INFORMATION ASSURANCE SECURITY+ LAB SERIES

CSSIA
National Resource
Center for Systems Security
and Information Assurance

Table of Contents

Lab 1: Network Devices and Technologies - Capturing Network Traffic

Lab 2: Secure Network Administration Principles - Log Analysis

Lab 3: Protocols and Default Network Ports - Transferring Data Using TCP/IP

Lab 4: Protocols and Default Network Ports - Connecting to a Remote System

Lab 5: Secure Implementation of Wireless Networking

Lab 6: Incident Response Procedures

Lab 7: Analyze and Differentiate Types of Malware

Lab 8: Analyze and Differentiate Types of Attacks Using Window Commands

Lab 9: Analyze and Differentiate Types of Application Attacks

Lab 10: Mitigation and Deterrent Techniques - Anti Forensic

Lab 11: Mitigation and Deterrent Techniques - Password Cracking

Lab 12: Discovering Security Threats and Vulnerabilities

Lab 13: Importance of Data Security - Data Theft

Lab 14: Importance of Data Security - Securing Data Using Encryption Software

Lab 15: Authentication, Authorization and Access Control

Lab 16: General Cryptography Concepts

CompTIA Security+® Lab Series

Lab 1: Network Devices and Technologies - Capturing Network Traffic

CompTIA Security+® Domain 1 - Network Security

Objective 1.1: Explain the security function and purpose of network devices and technologies

Document Version: 2012-08-15 (Beta)

Lab Author: Jesse Varsalone
Assistant Professor
Cyber Security

Organization: Community College of Baltimore County

The development of this document is funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) is an entity of Moraine Valley Community College.

Contents

1 Introduction 3
2 Objective: Explain the security function and purpose of network devices and technologies 3
3 Pod Topology 4
4 Lab Settings 5
Task 1 Using tcpdump to Capture Network Traffic 9
Task 1.1 Using tcpdump 9
Task 1.2 Conclusion 20
Task 1.3 Discussion Questions 20
Task 2 Capturing and Analyzing Traffic with Wireshark 21
Task 2.1 Using Wireshark 21
Task 2.2 Conclusion 28
Task 2.3 Discussion Questions 28
Task 3 Capturing and Analyzing Traffic with Network Miner 29
Task 3.1 Using Network Miner 29
Task 3.2 Conclusion 33
Task 3.3 Discussion Questions 33
5 References 34

1 Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By performing this lab, students will learn the process of capturing network traffic using three different methods, the tcpdump command, Wireshark, and Network Minor. The tcpdump command has no Graphical User Interface (GUI) and is only utilized within a Linux terminal. Wireshark shows you the raw output of network traffic captures and allows you to analyze them. Network Miner will allow you to capture data, and it will also pull out items like clear text messages and pictures.

This lab includes the following tasks:

- Task 1 - Using tcpdump to capture Network Traffic
- Task 2 - Capturing and Analyzing Traffic with Wireshark
- Task 3 - Capturing and Analyzing Traffic with Network Miner

2 Objective: Explain the security function and purpose of network devices and technologies

An essential part of network administration is the ability to capture and analyze network traffic. This can be important in order to identify the cause of bottlenecks, determining who is responsible for certain download activity, or analyzing an intrusion.

Wireshark [1] – A protocol analyzer that reads binary capture files. Wireshark will also allow you to capture network traffic and runs on Windows, Linux, and on Mac OS X.

Network Miner [2] – Network Miner allows you to capture and analyze network traffic. It is an NFAT, or Network Forensics Tool, that runs on the Windows operating system.

tcpdump [3] – A Linux/UNIX program that allows you to capture network traffic.

Sniffer – A sniffer is used to capture network traffic on a Network. Software programs like tcpdump, Wireshark, and Network Miner can be used to sniff traffic.

PCAP File – Programs that can sniff network traffic such as tcpdump, Wireshark, and Network Miner allow you to save the network capture to a PCAP file format. In order to read the PCAP format, you need a tool like Wireshark or Network Miner.

3 Pod Topology

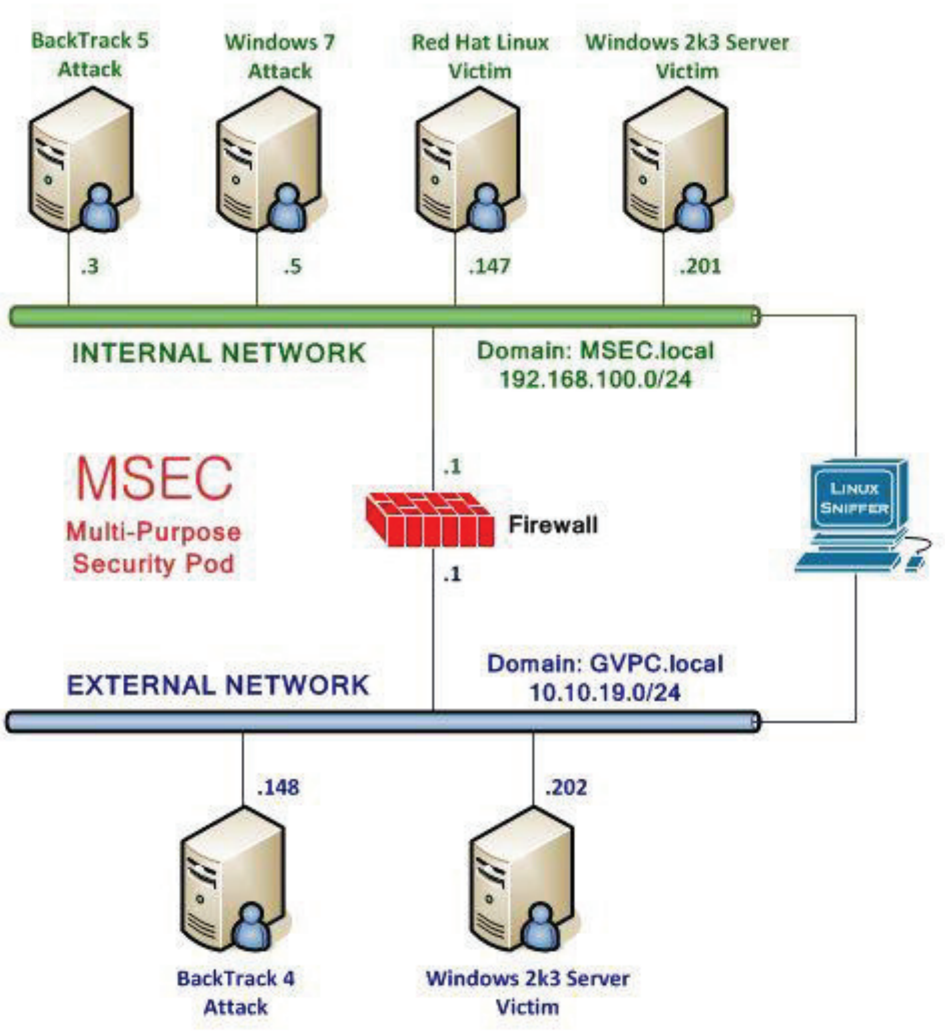


Figure 1: MSEC Network Topology

4 Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

Windows 7 Internal Attack Machine	192.168.100.5
Windows 7 student password	password
Linux Sniffer	No IP Addresses
Linux Sniffer root password	toor
BackTrack 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password
Windows 2k3 Server Internal Victim Machine	192.168.100.201
Windows 2k3 Server administrator password	password
BackTrack 4 External Attack Machine	10.10.19.148
BackTrack 4 External root password	password
Windows 2k3 Server External Victim	10.10.19.202
Windows 2k3 Server administrator password	password

Windows 7 Login:

1. Click on the Windows 7 icon on the topology.
2. Enter the username, **student** (verify the username with your instructor).
3. Type in the password, **password** and hit enter to log in (verify the password with your instructor).

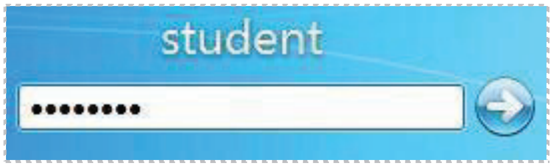


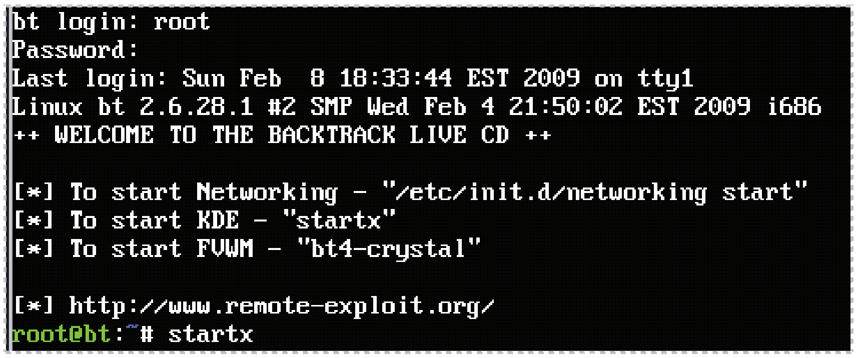
Figure 2: Windows 7 login

Linux Sniffer Login:

1. Click on the Linux Sniffer icon on the topology.
2. Type **root** at the **bt login:** username prompt.
3. At the password prompt, type **toor**.

For security purposes, the password will not be displayed.

4. To start the GUI, type **startx** at the root@bt:~# prompt and hit **enter**.

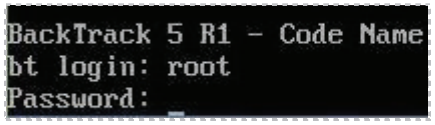


```
bt login: root
Password:
Last login: Sun Feb  8 18:33:44 EST 2009 on tty1
Linux bt 2.6.28.1 #2 SMP Wed Feb 4 21:50:02 EST 2009 i686
++ WELCOME TO THE BACKTRACK LIVE CD ++

[*] To start Networking - "/etc/init.d/networking start"
[*] To start KDE - "startx"
[*] To start FVWM - "bt4-crystal"

[*] http://www.remote-exploit.org/
root@bt:~# startx
```

Figure 3: Linux Sniffer login

BackTrack 5 Login:

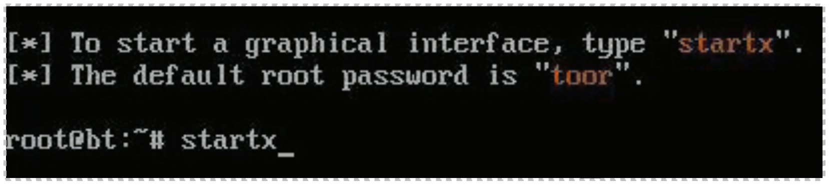
1. Click on the BackTrack 5 icon on the topology.
2. Type **root** at the bt login: username prompt.
3. Type **password** at the Password: prompt.



```
BackTrack 5 R1 - Code Name
bt login: root
Password: _
```

Figure 4: BackTrack 5 login

4. To start the GUI, type **startx** at the root@bt:~# prompt.

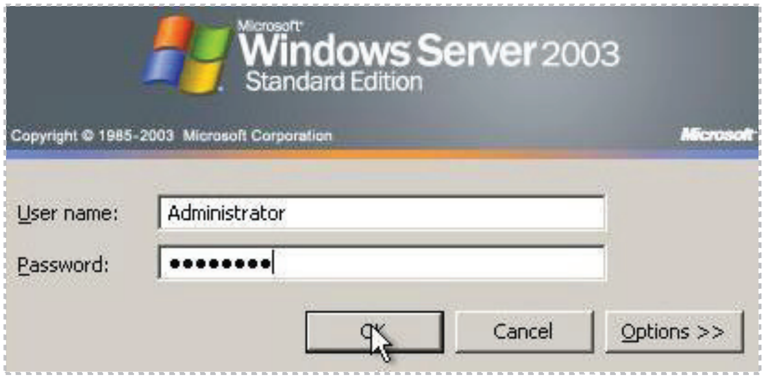


```
[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".

root@bt:~# startx_
```

Figure 5: BackTrack 5 GUI start up

Windows 2003 Server Login:

1. Click on the Windows 2k3 Server icon on the topology (these instructions will work for both internal and external victim machines).
2. Enter the User name, **Administrator** (verify the username with your instructor).
3. Type in the password: **password** and click the **OK** button (verify the password with your instructor).



Microsoft Windows Server 2003
Standard Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft

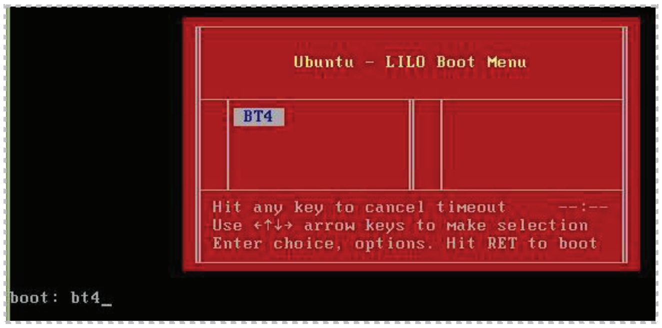
User name: Administrator

Password: ••••••••

Figure 6: Windows 2k3 login

BackTrack 4 Login:

1. Click on the BackTrack 4 icon on the topology.
2. At the Ubuntu boot menu, type **bt4** to select the BackTrack 4 system.



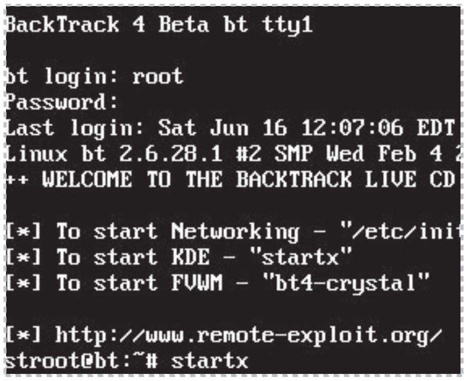
```
Ubuntu - LILO Boot Menu

BT4

Hit any key to cancel timeout      --:--
Use ←↑↓→ arrow keys to make selection
Enter choice, options. Hit RET to boot

boot: bt4_
```

Figure 7: Ubuntu Boot Menu

3. Type **root** at the bt login: username prompt.
4. Type **password** at the Password: prompt.

For security purposes, the password will not be displayed.

5. To start the GUI, type **startx** at the stroot@bt:~# prompt.



```
BackTrack 4 Beta bt tty1

bt login: root
Password:
Last login: Sat Jun 16 12:07:06 EDT
Linux bt 2.6.28.1 #2 SMP Wed Feb 4 2
++ WELCOME TO THE BACKTRACK LIVE CD

[*] To start Networking - "/etc/init
[*] To start KDE - "startx"
[*] To start FVWM - "bt4-crystal"

[*] http://www.remote-exploit.org/
stroot@bt:~# startx
```

Figure 8: BackTrack 4 login

Task 1 Using tcpdump to Capture Network Traffic

Part of a network administrator's job can be to capture and analyze network traffic. This is done for a variety of reasons, including the identification of the cause of bottlenecks, determining who is responsible for certain download activity, or analyzing an intrusion. There are many tools that can be utilized to capture network traffic, including tcpdump.

Task 1.1 Using tcpdump

The Linux distribution BackTrack is installed on the sniffer machine. BackTrack is a distribution used by security professionals for penetration testing and forensics.

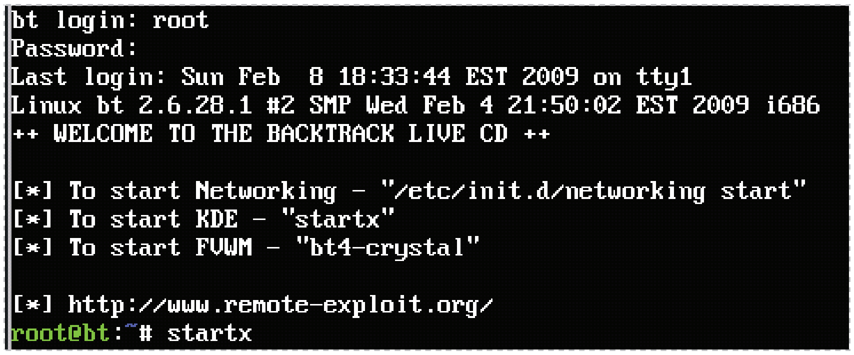
Log on to the sniffer.

If you have already logged into the Linux Sniffer as described in Lab Settings, section 4, skip this first step and begin this task at Step 2.

1. Log into the Linux Sniffer with the username of **root** with the password of **toor**.

For security purposes, the password will not be displayed.

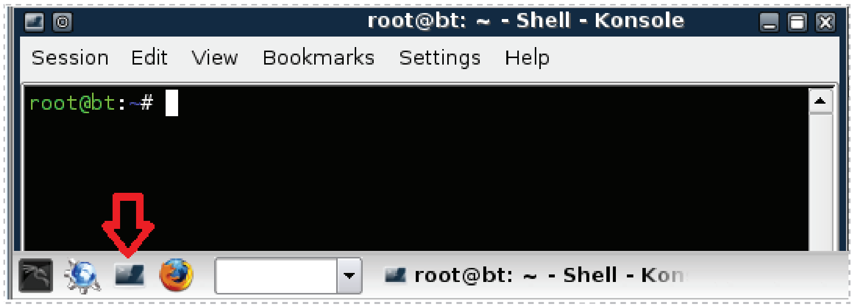
Type the following command to initialize the GUI (Graphical User Interface):
root@bt:~#**startx**



```
bt login: root
Password:
Last login: Sun Feb  8 18:33:44 EST 2009 on tty1
Linux bt 2.6.28.1 #2 SMP Wed Feb 4 21:50:02 EST 2009 i686
++ WELCOME TO THE BACKTRACK LIVE CD ++

[*] To start Networking - "/etc/init.d/networking start"
[*] To start KDE - "startx"
[*] To start FVWM - "bt4-crystal"

[*] http://www.remote-exploit.org/
root@bt:~# startx
```

Figure 9:   Logging on to the Sniffer

2. Open a terminal on the Sniffer system by clicking on the image to the left of Firefox in the task bar, in the bottom of the screen.

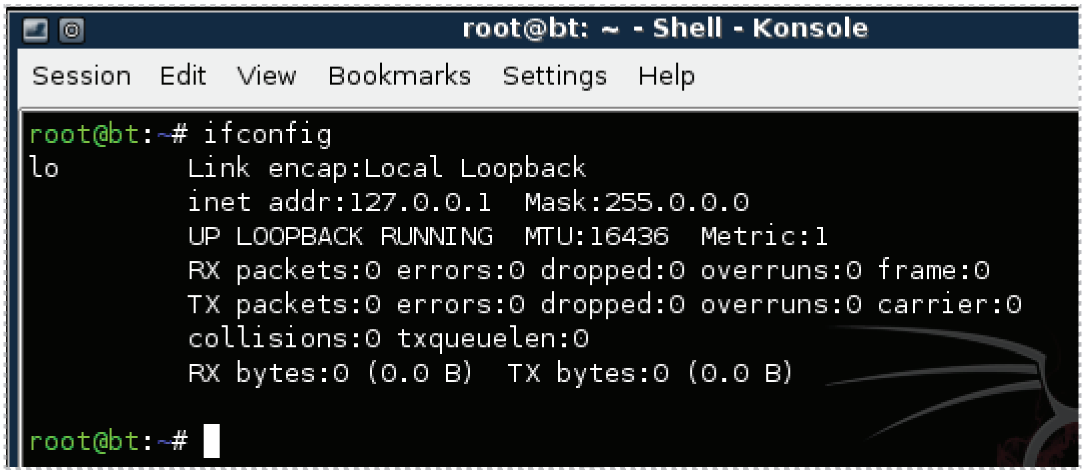

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt: ~ - Shell - Kon

```
root@bt:~# 
```

Figure 10:   The Terminal Windows within BackTrack

One of the nice features of some versions of BackTrack is that they are not automatically assigned IP Addresses though the use of DHCP, or Dynamic Host Configuration Protocol. The idea is to come on the network quietly, without being detected.

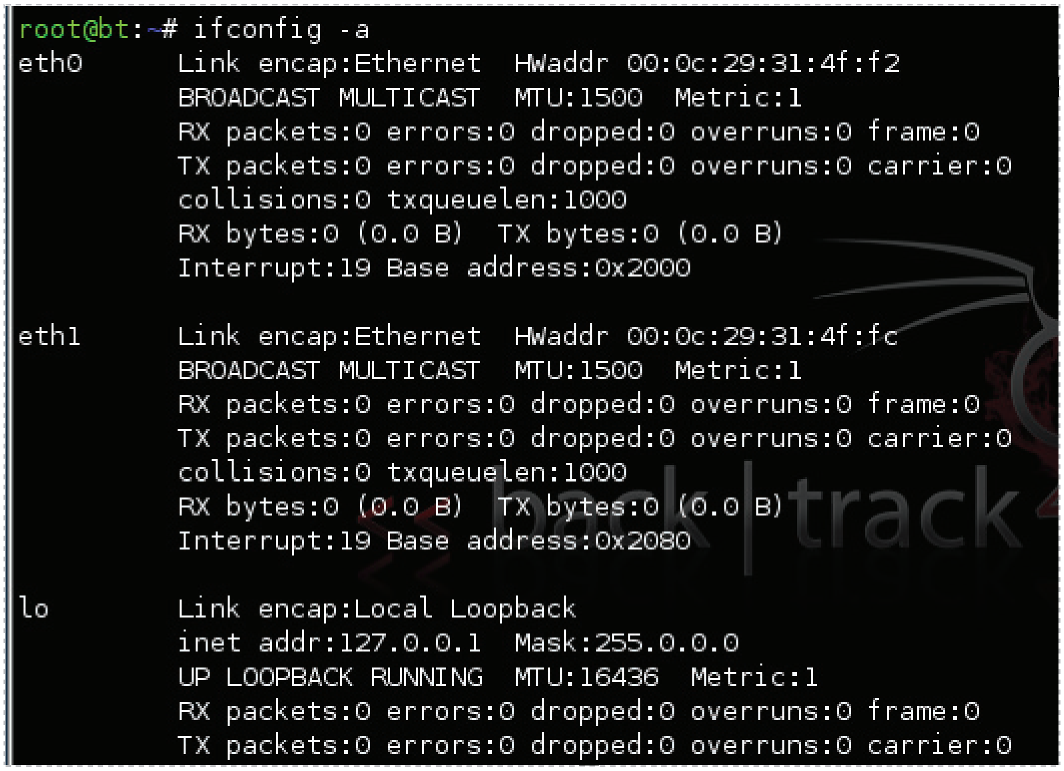
3. Only the loopback address, 127.0.0.1, is displayed when you type: root@bt:~#**ifconfig**


root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

```
root@bt:~# ifconfig
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:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@bt:~# 
```

Figure 11:   No IP Address, other than the Loopback Address of 127.0.0.1, is Displayed

4. Type the following command to view all available interfaces on the system: root@bt:~#**ifconfig -a**



```
root@bt:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:31:4f:f2
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2000

eth1      Link encap:Ethernet  HWaddr 00:0c:29:31:4f:fc
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2080

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:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
```

Figure 12: All Available Interfaces on the System

Neither of the interfaces, eth0 or eth1, are assigned IP Addresses on their respective networks. The reason the sniffer has two interfaces is that it is located on two networks.

Note: The pfSense Firewall also has 2 interfaces and is also connected to both networks.

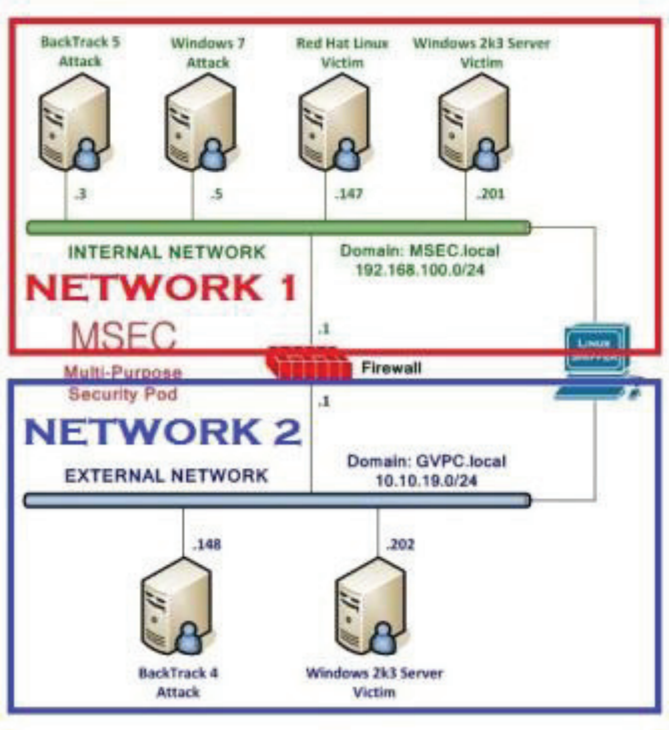


Figure 13: The Sniffer is Connected to Two Networks

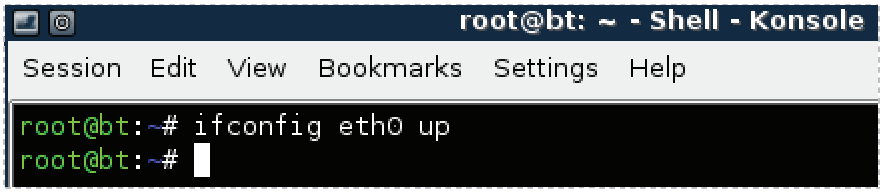
A sniffer should be operating in promiscuous mode so it can see all network traffic. To put the interfaces into promiscuous mode, type the following commands:

root@bt:~# **ifconfig eth0 -promisc**
root@bt:~# **ifconfig eth1 -promisc**

Two ways to ensure that a sniffer will capture all traffic on a network segment are:

- Connect the Sniffer and other devices on the Network to a Hub
- Connect the Sniffer to a switch's SPAN port, Switched Analyzed Network Port

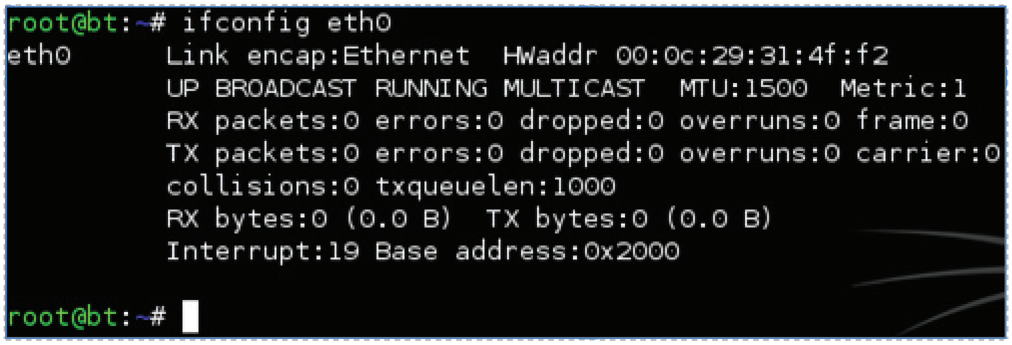
5. To activate the first interface, type the following command:
 root@bt:~#**ifconfig eth0 up**



```
root@bt:~# ifconfig eth0 up
root@bt:~#
```

Figure 14: Activating the First Interface

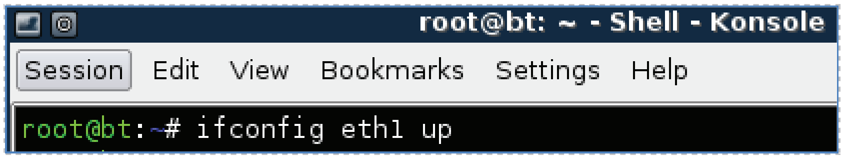
To verify the first interface, type the following command:
 root@bt:~#**ifconfig eth0**



```
root@bt:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:31:4f:f2
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2000

root@bt:~#
```

Figure 15: The Interface is activated without an IP Address

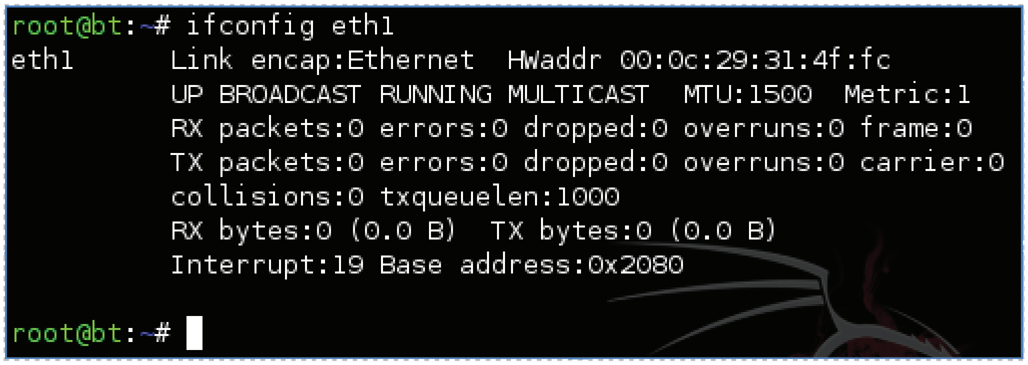
6. To activate the second interface, type the following command:
root@bt:~#**ifconfig eth1 up**



```
root@bt:~# ifconfig eth1 up
```

Figure 16: Activating the Second Interface

7. To verify the second interface, type the following command:
   root@bt:~#**ifconfig eth1**

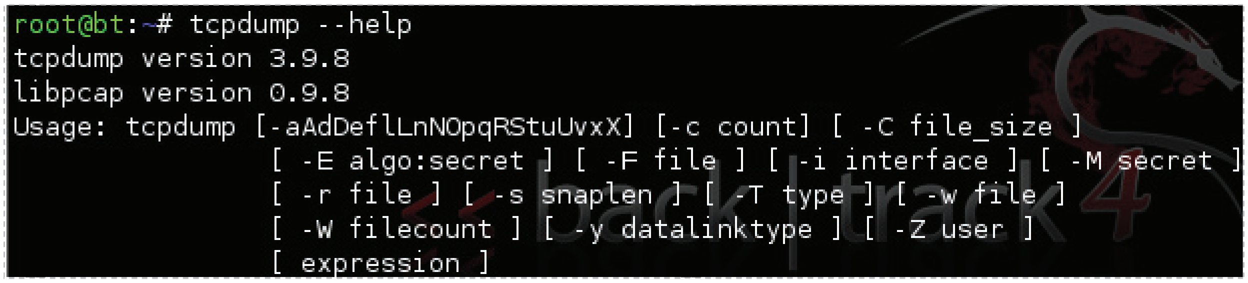


```
root@bt:~# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:0c:29:31:4f:fc
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2080

root@bt:~# 
```

Figure 17: The Interface is activated without an IP Address

The Linux/UNIX utility tcpdump is commonly used by network administrators to capture network traffic on a sniffer. Many sniffer machines do not have GUI, or Graphical User Interfaces, so running GUI based tools like Wireshark or Network Miner is not possible. Another benefit to using tcpdump is that it handles very large capture files with no problem.

8. Type the following command to view several available switches for tcpdump:
   root@bt:~#**tcpdump --help**

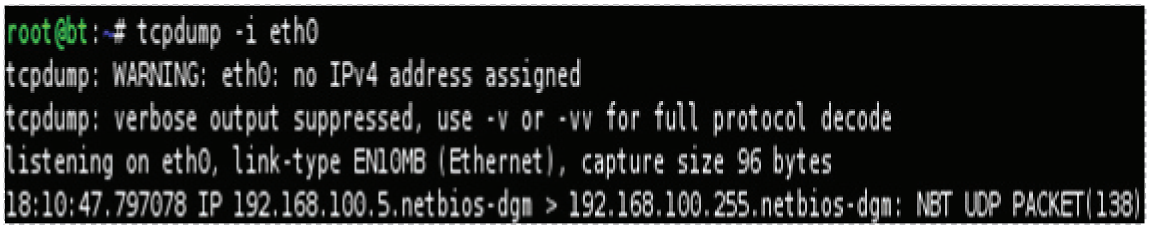


```
root@bt:~# tcpdump --help
tcpdump version 3.9.8
libpcap version 0.9.8
Usage: tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c count] [ -C file_size ]
               [ -E algo:secret ] [ -F file ] [ -i interface ] [ -M secret ]
               [ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]
               [ -W filecount ] [ -y datalinktype ] [ -Z user ]
               [ expression ]
```

Figure 18: The Available Options for tcpdump

9. To run tcpdump on the network segment interface eth0 is connected to, type:
   root@bt:~#**tcpdump –i eth0**

Wait until at least one packet is displayed before stopping the capture.



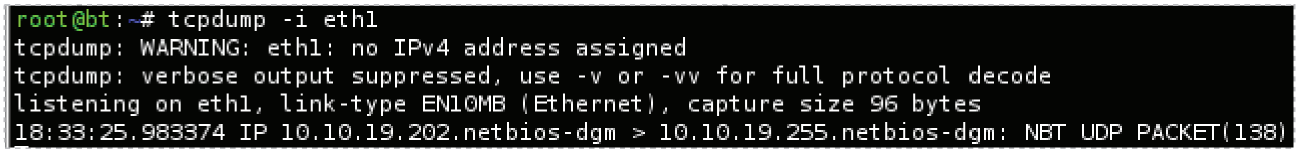
```
root@bt:~# tcpdump -i eth0
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
18:10:47.797078 IP 192.168.100.5.netbios-dgm > 192.168.100.255.netbios-dgm: NBT UDP PACKET(138)
```

Figure 19: The output of tcpdump on the network segment interface eth0 is connected

After one packet or more is displayed, hit **CTRL-C** to stop the network capture.
If the network 192.168.100.0/24 is displayed, eth0 is located on the first network.
If the network 10.10.19.0/24 is displayed, eth0 is located on the second network.
Also, notice that the default for tcpdump is to capture only the first 96 bytes.

10. To run tcpdump on the network segment interface eth1 is connected to, type:
    root@bt:~#**tcpdump –i eth1**

Wait until at least one packet is displayed before stopping the capture.

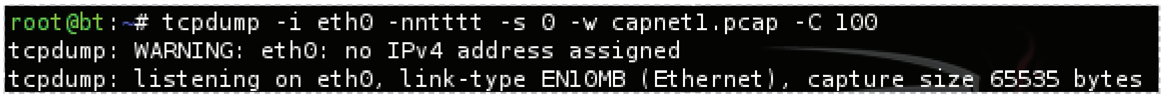


```
root@bt:~# tcpdump -i eth1
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
18:33:25.983374 IP 10.10.19.202.netbios-dgm > 10.10.19.255.netbios-dgm: NBT UDP PACKET(138)
```

Figure 20: The output of tcpdump on the network segment interface eth1 is connected

After one packet or more is displayed, hit **CTRL-C** to stop the network capture.
If the network 192.168.100.0/24 is displayed, eth1 is located on the first network.
If the network 10.10.19.0/24 is displayed, eth1 is located on the second network.

11. To capture traffic on the 192.168.100.0/24 network and send it to a file, type:
    root@bt:~#**tcpdump –i eth0 -nntttt -s 0 -w capnet1.pcap -C 100**

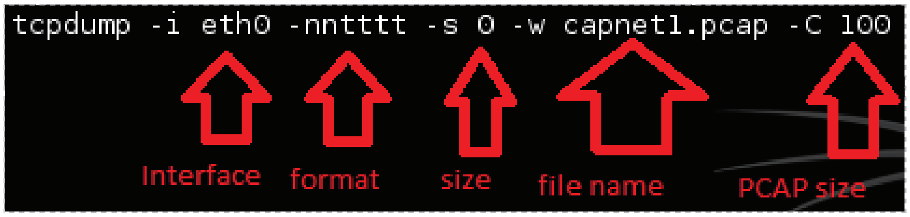


```
root@bt:~# tcpdump -i eth0 -nntttt -s 0 -w capnet1.pcap -C 100
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```

Figure 21: tcpdump syntax

The following table lists details of the switches used with the tcpdump command:

-i eth0	Use interface zero
-nntttt	Disable DNS resolution, date and time format
-s 0	Disables default packet size of 96 bytes, full packet size
-w	Write to a capture file, instead of displaying to the screen
-C	Split the captures into files of this size

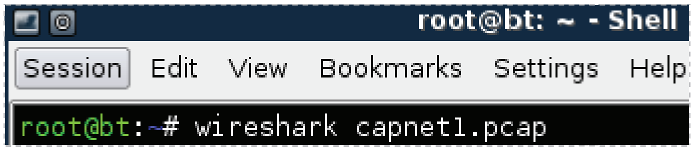


```
tcpdump -i eth0 -nntttt -s 0 -w capnet1.pcap -C 100
```

Figure 22: Detailed tcpdump Syntax Explained

Wait about 5 minutes so that your capture file will have some generated traffic. Press **CTRL-C** to stop tcpdump from running and discontinue the network capture.

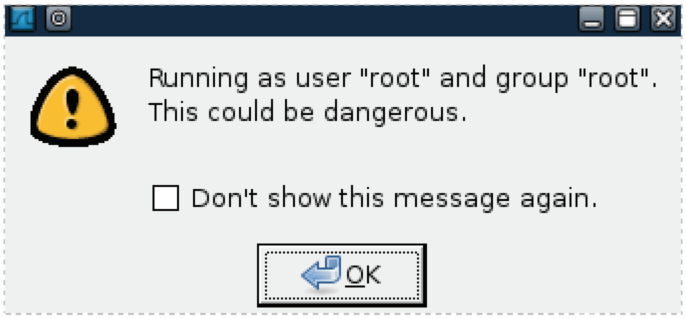
12. To view the capture file, type the following command at the BackTrack terminal: root@bt:~#**wireshark capnet1.pcap**



```
root@bt:~# wireshark capnet1.pcap
```

Figure 23: Opening the tcpdump capture with Wireshark

13. Check the **Don't show the message again** box and click the **OK** button.

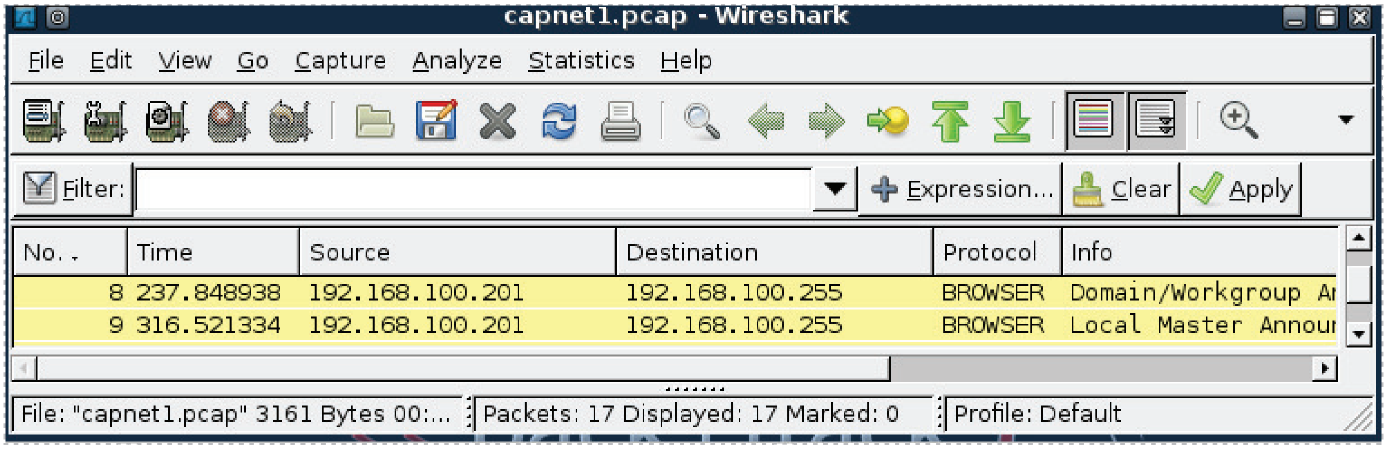


Running as user "root" and group "root". This could be dangerous.

□ Don't show this message again.

Figure 24: Opening the tcpdump capture with Wireshark

Wireshark will open and the capture file will appear, similar to the one seen below: Notice that the traffic listed takes place on the 192.168.100.0/24 network.

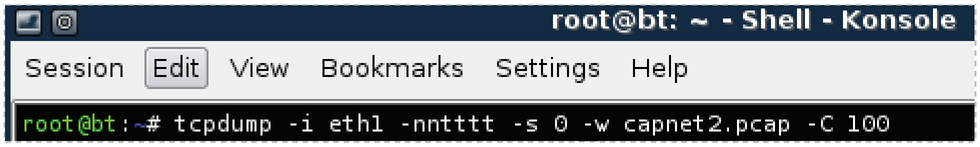

capnet1.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time         Source            Destination       Protocol  Info
    8  237.848938   192.168.100.201   192.168.100.255   BROWSER   Domain/Workgroup Ar
    9  316.521334   192.168.100.201   192.168.100.255   BROWSER   Local Master Annour
```

File: "capnet1.pcap" 3161 Bytes 00:... Packets: 17 Displayed: 17 Marked: 0 Profile: Default

Figure 25: The tcpdump Capture is Displayed within Wireshark

14. Close Wireshark.
15. To capture traffic on the 10.10.19.0/24 network and send it to a file, type:
    root@bt:~#**tcpdump –i eth1 -nntttt -s 0 -w capnet2.pcap -C 100**

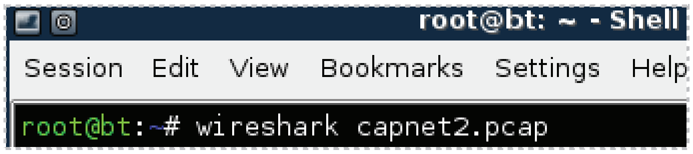

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

```
root@bt:~# tcpdump -i eth1 -nntttt -s 0 -w capnet2.pcap -C 100
```

Figure 26: tcpdump syntax

Wait about 5 minutes so that your capture file will have some generated traffic. Press **CTRL-C** to stop tcpdump from running and discontinue the network capture.

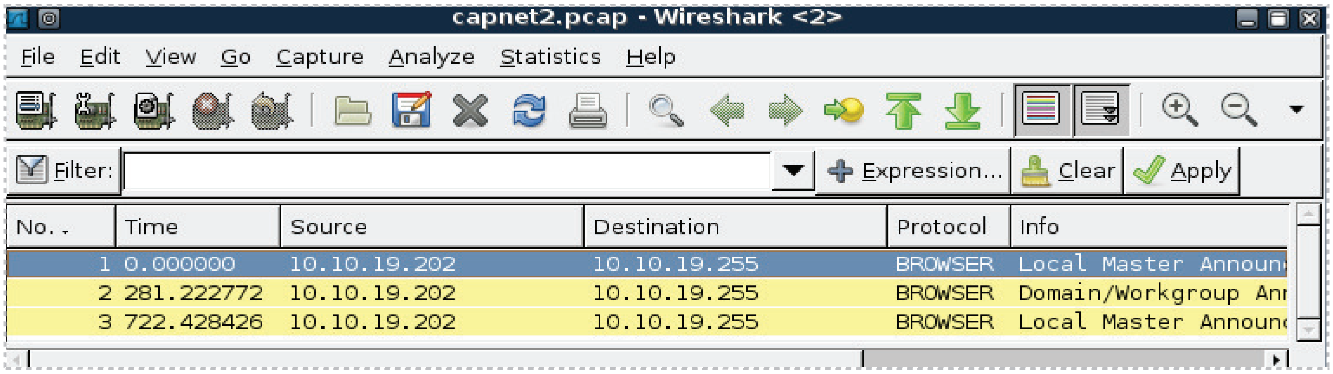
16. To view the capture file, type the following command at the BackTrack terminal:
    root@bt:~#**wireshark capnet2.pcap**



```
root@bt:~# wireshark capnet2.pcap
```

Figure 27: Opening the tcpdump capture with Wireshark

Wireshark will open and the capture file will appear similar to the one seen below: Notice that the traffic listed takes place on the 10.10.19.0/24 network. Exit Wireshark when finished.

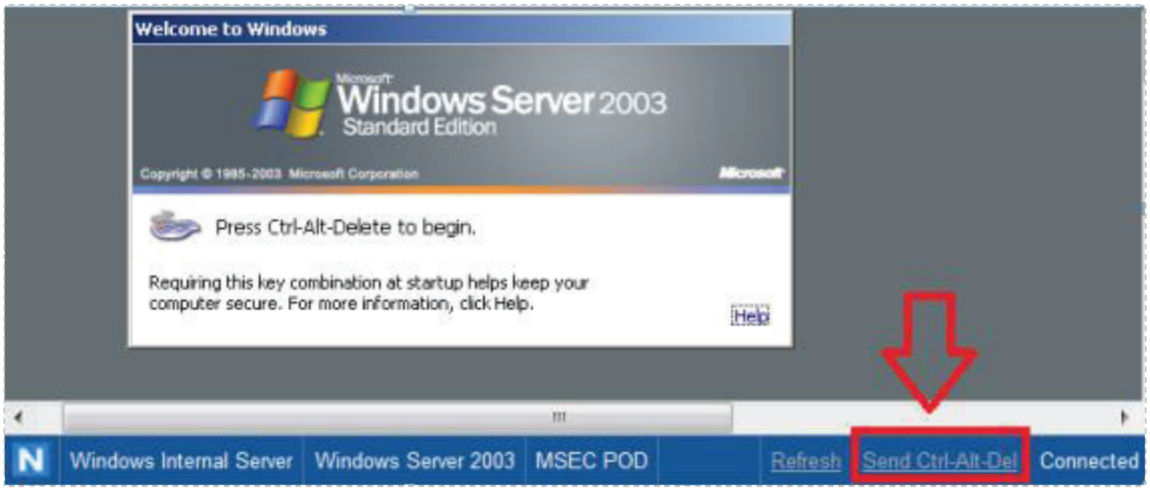

capnet2.pcap - Wireshark <2>
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.10.19.202	10.10.19.255	BROWSER	Local Master Announ
2	281.222772	10.10.19.202	10.10.19.255	BROWSER	Domain/Workgroup Ann
3	722.428426	10.10.19.202	10.10.19.255	BROWSER	Local Master Announ

Figure 28: The tcpdump Capture is Displayed within Wireshark

You can also filter which type of traffic you want to see with tcpdump. For example, if you just want to see ICMP traffic, you can filter tcpdump for that type of traffic.

17. Log on to the Windows Internal 2003 Server by clicking the **Send Ctrl-Alt-Del** link in the bottom right hand corner of the browser window. Log on to the 2003 server with the username of **Administrator** and the password of **password**.


Welcome to Windows

Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Figure 29: Send Ctrl-Alt-Del to the Windows 2003 Server

18. Click the shortcut to the command prompt icon on the Windows 2003 Desktop.

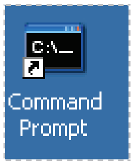
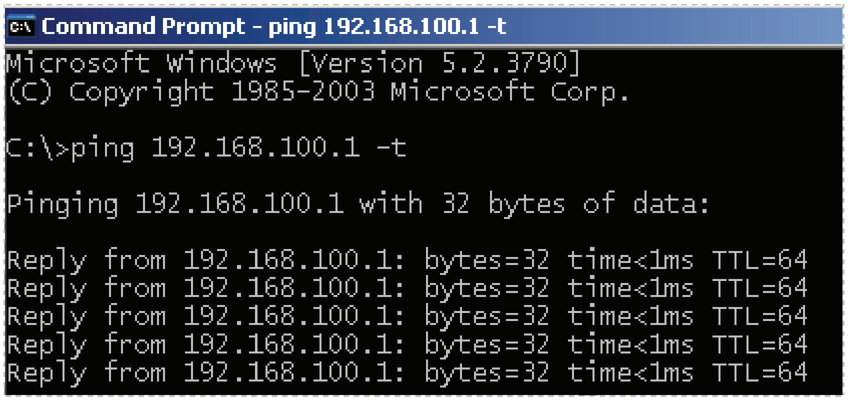


Figure 30: Windows 2003 Command Prompt

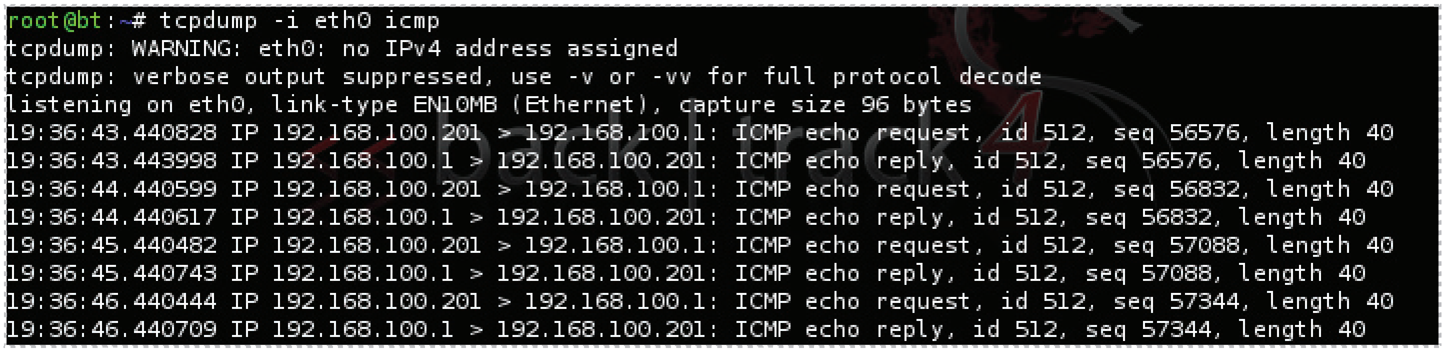
19. Type the following command to initiate a continuous ping of the gateway:
C:\ping 192.168.100.1 –t



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>ping 192.168.100.1 -t

Pinging 192.168.100.1 with 32 bytes of data:

Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
Reply from 192.168.100.1: bytes=32 time<1ms TTL=64
```

Figure 31: Pinging the Gateway

20. On the Sniffer Machine, type the following to capture ICMP traffic on Network 1:
    root@bt:~#**tcpdump –i eth0 icmp**

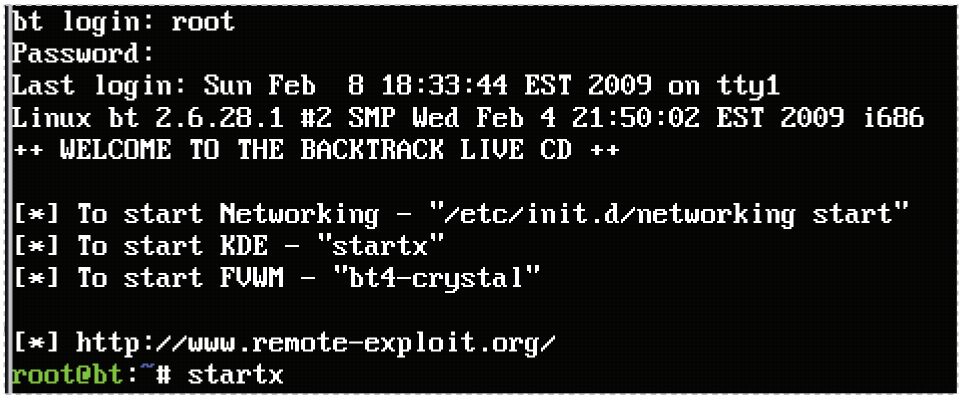


```
root@bt:~# tcpdump -i eth0 icmp
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
19:36:43.440828 IP 192.168.100.201 > 192.168.100.1: ICMP echo request, id 512, seq 56576, length 40
19:36:43.443998 IP 192.168.100.1 > 192.168.100.201: ICMP echo reply, id 512, seq 56576, length 40
19:36:44.440599 IP 192.168.100.201 > 192.168.100.1: ICMP echo request, id 512, seq 56832, length 40
19:36:44.440617 IP 192.168.100.1 > 192.168.100.201: ICMP echo reply, id 512, seq 56832, length 40
19:36:45.440482 IP 192.168.100.201 > 192.168.100.1: ICMP echo request, id 512, seq 57088, length 40
19:36:45.440743 IP 192.168.100.1 > 192.168.100.201: ICMP echo reply, id 512, seq 57088, length 40
19:36:46.440444 IP 192.168.100.201 > 192.168.100.1: ICMP echo request, id 512, seq 57344, length 40
19:36:46.440709 IP 192.168.100.1 > 192.168.100.201: ICMP echo reply, id 512, seq 57344, length 40
```

Figure 32: Capturing ICMP Traffic with tcpdump

Press **CTRL-C** to stop tcpdump from running and discontinue the network capture. On the Windows 2003 Server system, type **CTRL-C** to stop the continuous ping.

21. Log into the External BackTrack 4 machine with the username of **root** and the password of **password**. For security purposes, the password won't be displayed. Type the following command to initialize the GUI, Graphical User Interface:
    root@bt:~#**startx**



```
bt login: root
Password:
Last login: Sun Feb  8 18:33:44 EST 2009 on tty1
Linux bt 2.6.28.1 #2 SMP Wed Feb 4 21:50:02 EST 2009 i686
++ WELCOME TO THE BACKTRACK LIVE CD ++

[*] To start Networking - "/etc/init.d/networking start"
[*] To start KDE - "startx"
[*] To start FVWM - "bt4-crystal"

[*] http://www.remote-exploit.org/
root@bt:~# startx
```

Figure 33: Logging on to the External BackTrack machine

22. Log on to the Windows External 2003 Server by clicking the **Send Ctrl-Alt-Del** link in the bottom right hand corner of the browser window. Log on to the 2003 server with the username of **Administrator** and the password of **password**.

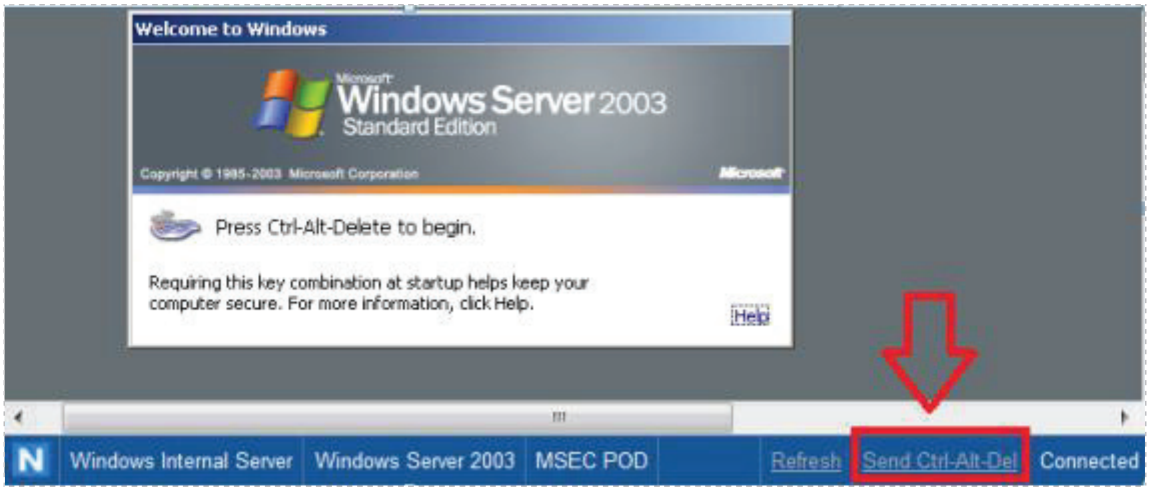

Welcome to Windows
Microsoft Windows Server 2003
Standard Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
Press Ctrl-Alt-Delete to begin.
Requiring this key combination at startup helps keep your computer secure. For more information, click Help.
Help
Windows Internal Server
Windows Server 2003
MSEC POD
Refresh
Send Ctrl-Alt-Del
Connected

Figure 34: Send Ctrl-Alt-Del to the Windows 2003 Server

23. Click the shortcut to the command prompt icon on the Windows 2003 Desktop.

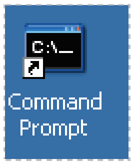
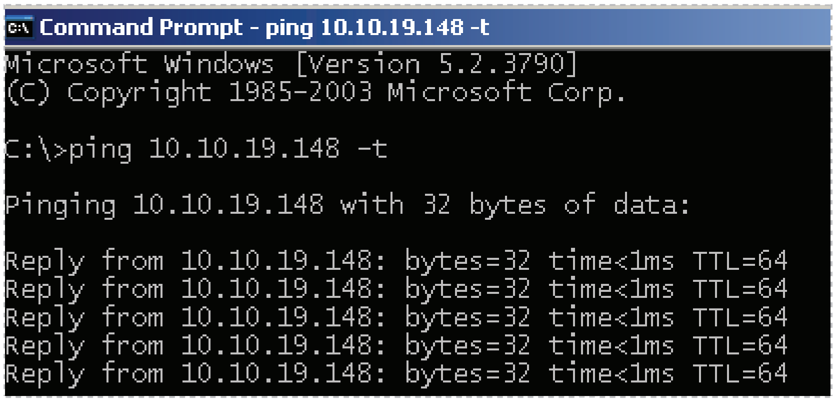


Figure 35: Windows 2003 Command Prompt

24. Type the following command to continuously ping the External BackTrack VM: C:\ping 10.10.19.148 –t

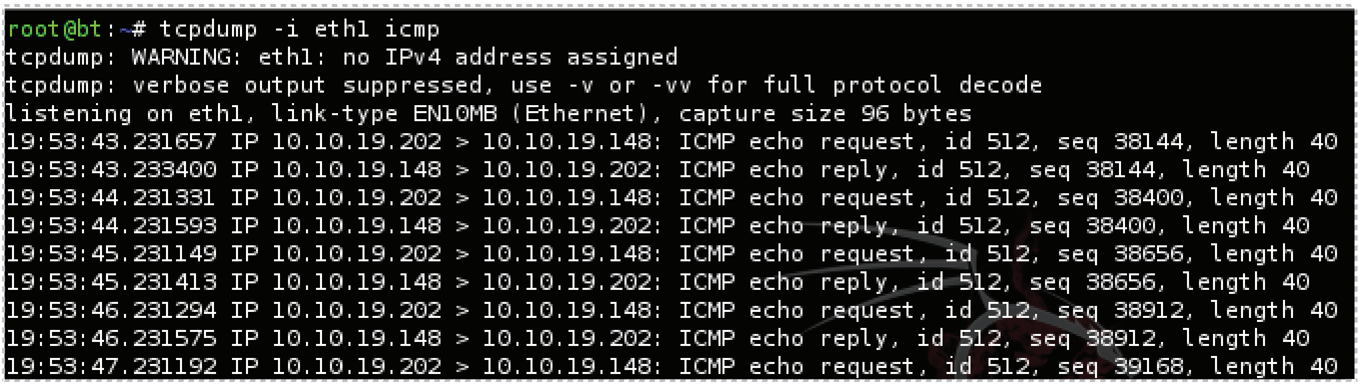


Command Prompt - ping 10.10.19.148 -t

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>ping 10.10.19.148 -t

Pinging 10.10.19.148 with 32 bytes of data:

Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
```

Figure 36: Pinging the External BackTrack Machine

25. On the Sniffer Machine, type the following to capture ICMP traffic on Network 2: root@bt:~#**tcpdump –i eth1 icmp**



```
root@bt:~# tcpdump -i eth1 icmp
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
19:53:43.231657 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 512, seq 38144, length 40
19:53:43.233400 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 512, seq 38144, length 40
19:53:44.231331 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 512, seq 38400, length 40
19:53:44.231593 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 512, seq 38400, length 40
19:53:45.231149 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 512, seq 38656, length 40
19:53:45.231413 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 512, seq 38656, length 40
19:53:46.231294 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 512, seq 38912, length 40
19:53:46.231575 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 512, seq 38912, length 40
19:53:47.231192 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 512, seq 39168, length 40
```

Figure 37: Capturing ICMP Traffic with tcpdump

26. Press **CTRL-C** to stop tcpdump from running and discontinue the network capture.
27. In the Windows 2003 Server system, press **CTRL-C** to stop the continuous ping.

Task 1.2 Conclusion

The tcpdump command is built into the Linux and Unix operating systems. It can be used to capture network traffic. The benefits of using tcpdump include the fact that many sniffer machines do not have GUI, or Graphical User Interfaces, so running GUI based tools like Wireshark is not possible. Another benefit to using tcpdump is that it handles very large capture files with no problem, and it allows you to filter for specific traffic.

Task 1.3 Discussion Questions

1. Does a network interface on a sniffer machine require an IP Address?
2. In what mode does a sniffer's network interface operate?
3. How do you determine available switches for tcpdump?
4. How can you display all of the network interfaces in Linux?

Task 2 Capturing and Analyzing Traffic with Wireshark

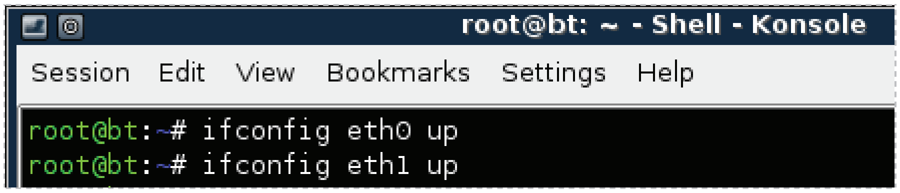
Wireshark is a GUI, or Graphical User Interface, tool that will allow you to capture and analyze network traffic. Wireshark runs on Windows, Linux, and on Mac OS X. Wireshark can be downloaded from the following link: http://www.wireshark.org/download.html.

Task 2.1 Using Wireshark

Before using Wireshark, it is important to bring the sniffer interfaces up. Even though this was done in Task 1, it is a good idea to start over to practice all of the required steps.

1. On the Linux Sniffer system, bring both of the Sniffer interfaces up by typing the following two commands:

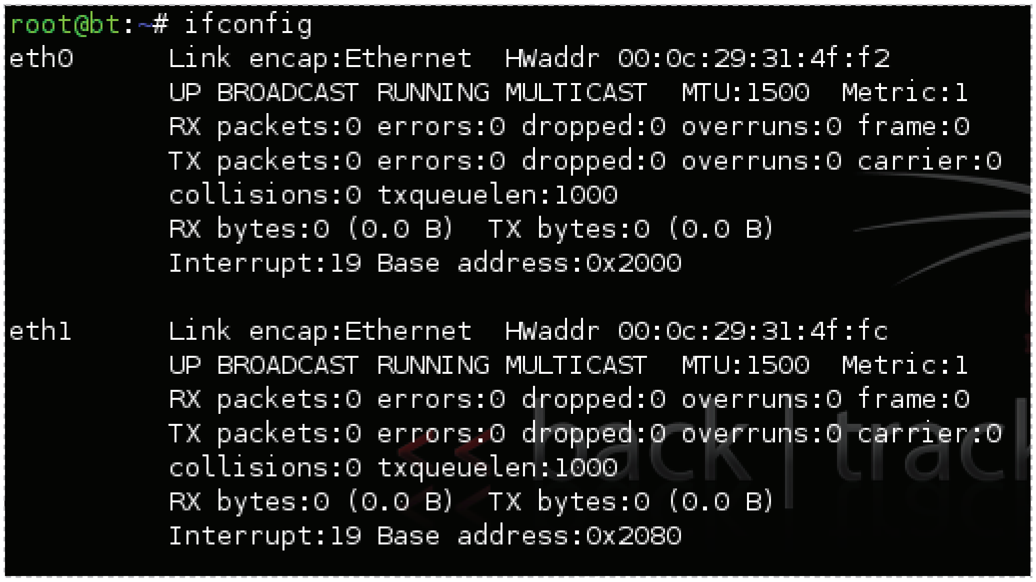
   root@bt:~#**ifconfig eth0 up**
   root@bt:~#**ifconfig eth1 up**


root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

```
root@bt:~# ifconfig eth0 up
root@bt:~# ifconfig eth1 up
```

Figure 38: Turning both Sniffer Interfaces on

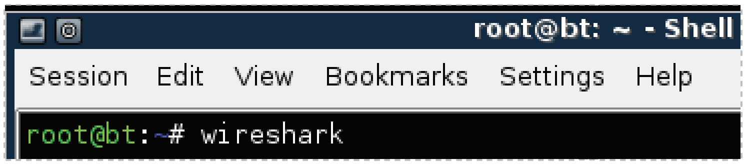
2. Type the following to verify that no IP Address has been set for either interface: root@bt:~#**ifconfig**



```
root@bt:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:31:4f:f2
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2000

eth1      Link encap:Ethernet  HWaddr 00:0c:29:31:4f:fc
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:19 Base address:0x2080
```

Figure 39: Verifying that the Sniffer Interfaces do not have IP Addresses

3. In the Sniffer terminal, type the following command to start Wireshark: root@bt:~#**wireshark**



```
root@bt:~# wireshark
```

Figure 40: Opening Wireshark

4. To view the available interfaces, select **Capture** then go down to **Interfaces.**

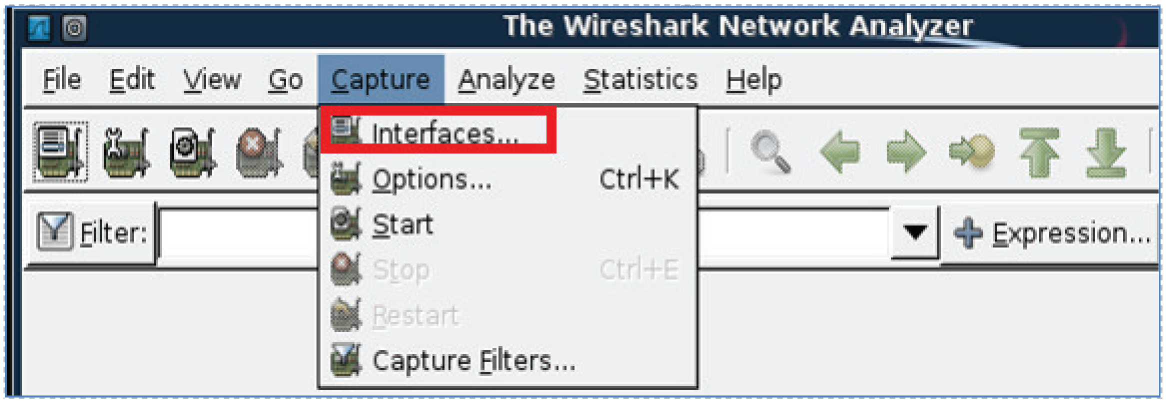
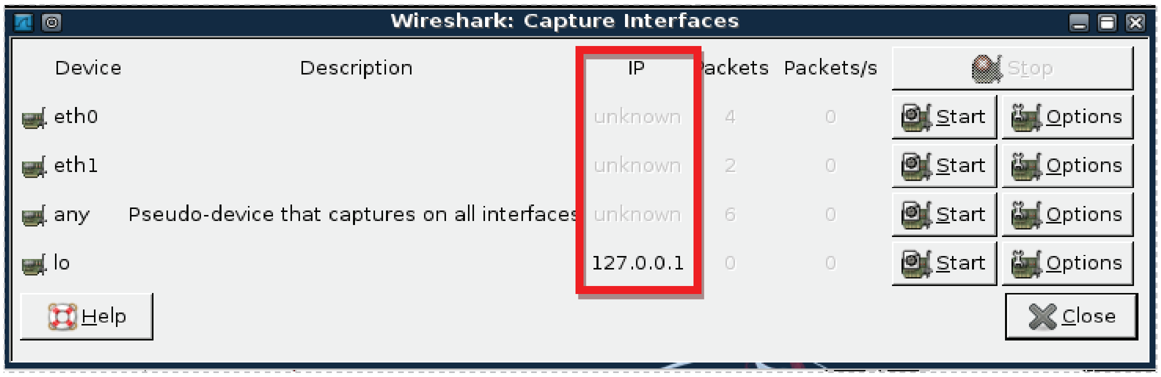


Figure 41: Selecting Interfaces from the Capture Menu

The **Wireshark: Capture Interfaces** pop-up box will be displayed on the sniffer.

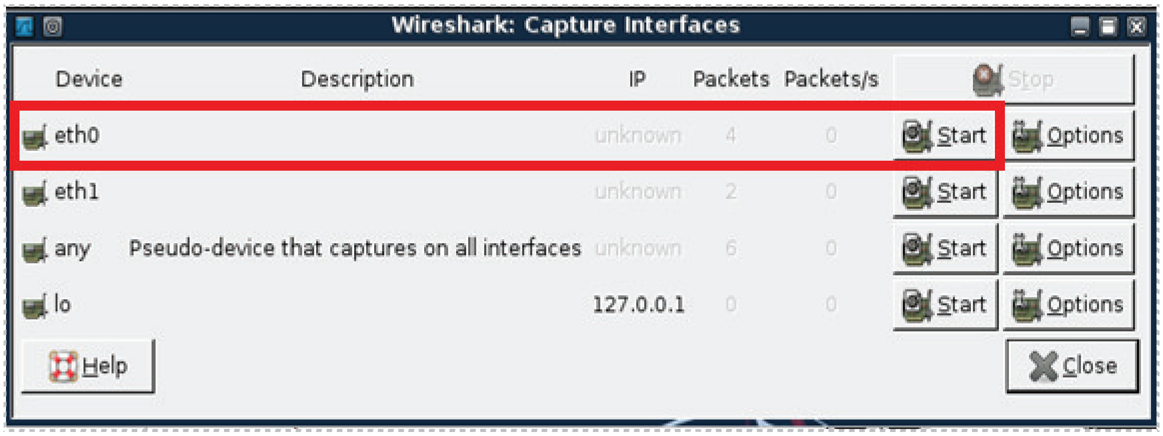


Device	Description	IP	ackets	Packets/s
eth0		unknown	4	0
eth1		unknown	2	0
any	Pseudo-device that captures on all interfaces	unknown	6	0
lo		127.0.0.1	0	0

Figure 42: The Devices eth0 and eth1 do not have IP Addresses listed

Notice that eth0 and eth1 do not have IP Addresses listed under the IP column.

5. Within the **Capture Interfaces** menu, click **Start** for the eth0 network device.



Device	Description	IP	Packets	Packets/s
eth0		unknown	4	0
eth1		unknown	2	0
any	Pseudo-device that captures on all interfaces	unknown	6	0
lo		127.0.0.1	0	0

Figure 43: Starting a Capture on the Network using Interface eth0

During this exercise, we will be capturing plain text FTP, or File Transfer Protocol, traffic from the Windows 7 Internal Machine to the Windows 2003 Internal machine.

6. Open a command prompt on the Windows 7 machine by double clicking on the **cmd-Shortcut** on the desktop.

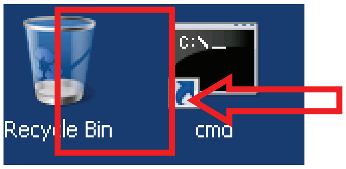
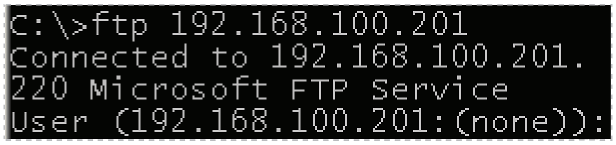


Figure 44: Opening a Command Prompt on Windows 7

7. Type the following command to connect to the Windows 2003 FTP Server: C:\ftp 192.168.100.201

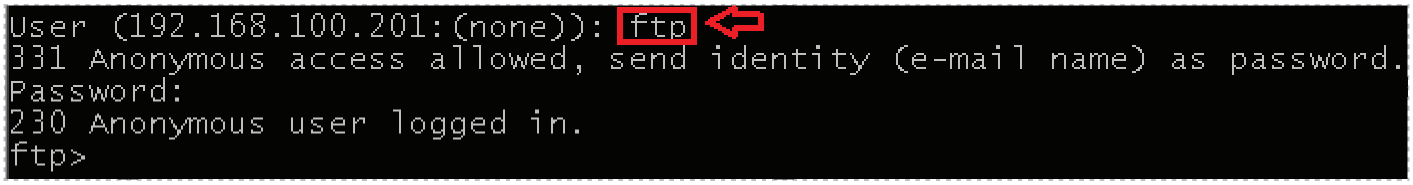


```
C:\>ftp 192.168.100.201
Connected to 192.168.100.201.
220 Microsoft FTP Service
User (192.168.100.201:(none)):
```

Figure 45: Connecting to the FTP Server 192.168.100.201

You should receive the message, *connected to 192.168.100.201.*

8. For the username, type **ftp** and hit enter. For the password, type **mysecurepass**. Note: For security purposes, the password will not be displayed when you type it

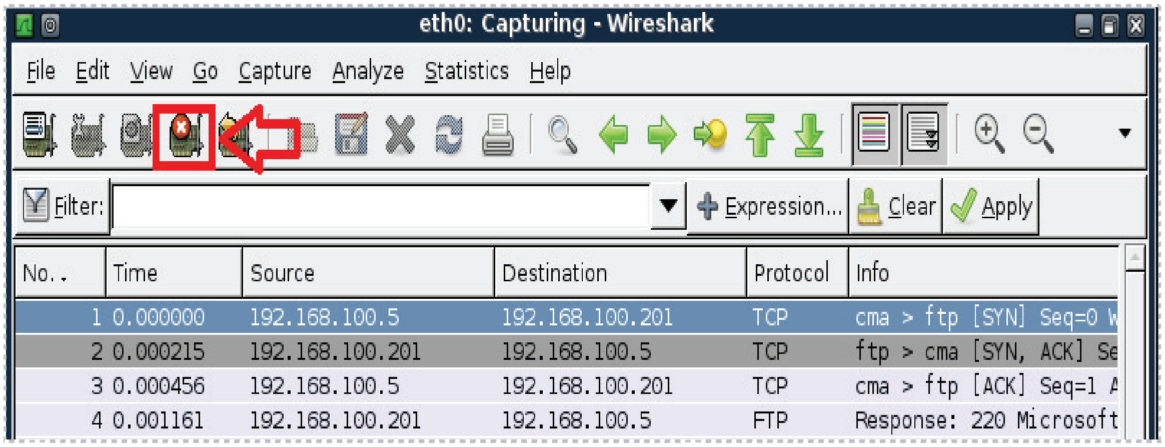


```
User (192.168.100.201:(none)): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp>
```

Figure 46: Logging in to the FTP Server

You should receive the message, *230 Anonymous user logged in*.

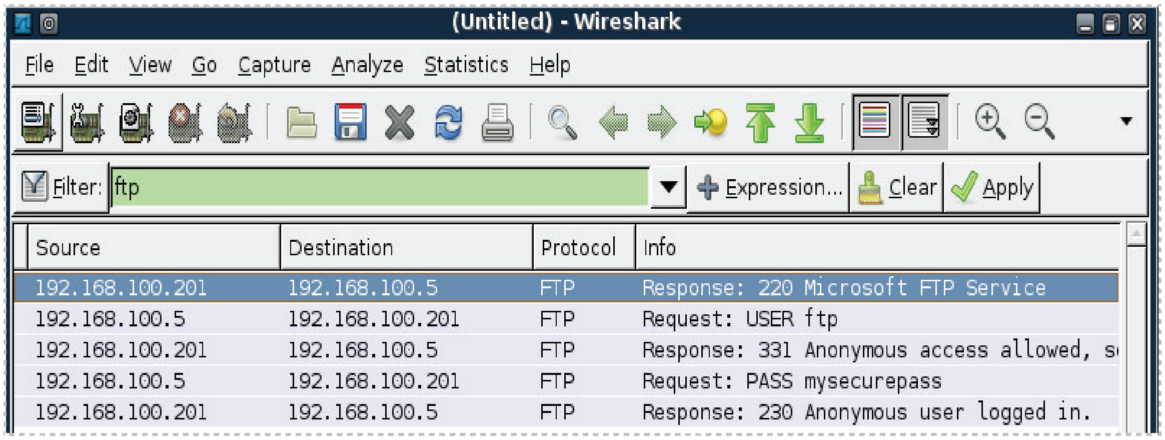
9. On the sniffer machine, click the **stop** button on Wireshark to stop the capture.



```
No. .  Time       Source           Destination      Protocol  Info
    1 0.000000   192.168.100.5    192.168.100.201  TCP       cma > ftp [SYN] Seq=0 W
    2 0.000215   192.168.100.201  192.168.100.5    TCP       ftp > cma [SYN, ACK] Se
    3 0.000456   192.168.100.5    192.168.100.201  TCP       cma > ftp [ACK] Seq=1 A
    4 0.001161   192.168.100.201  192.168.100.5    FTP       Response: 220 Microsoft
```

Figure 47: Stopping the Wireshark capture

10. On the Sniffer machine, type **ftp** in the filter pane and click **Apply**.

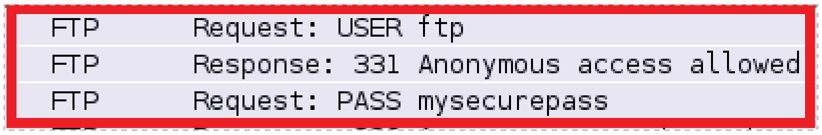


Filter: ftp

```
Source           Destination      Protocol  Info
192.168.100.201  192.168.100.5    FTP       Response: 220 Microsoft FTP Service
192.168.100.5    192.168.100.201  FTP       Request: USER ftp
192.168.100.201  192.168.100.5    FTP       Response: 331 Anonymous access allowed, s
192.168.100.5    192.168.100.201  FTP       Request: PASS mysecurepass
192.168.100.201  192.168.100.5    FTP       Response: 230 Anonymous user logged in.
```

Figure 48: Typing ftp in the Wireshark filter pane

If you scroll over, you can see the username of **ftp** and the password of **mysecurepass**.



```
FTP    Request: USER ftp
FTP    Response: 331 Anonymous access allowed
FTP    Request: PASS mysecurepass
```

Figure 49: The FTP username and password appear in clear text.

Now, we will capture FTP traffic on the external network using interface eth1.

11. To view the available interfaces, select **Capture** then go down to **Interfaces.**

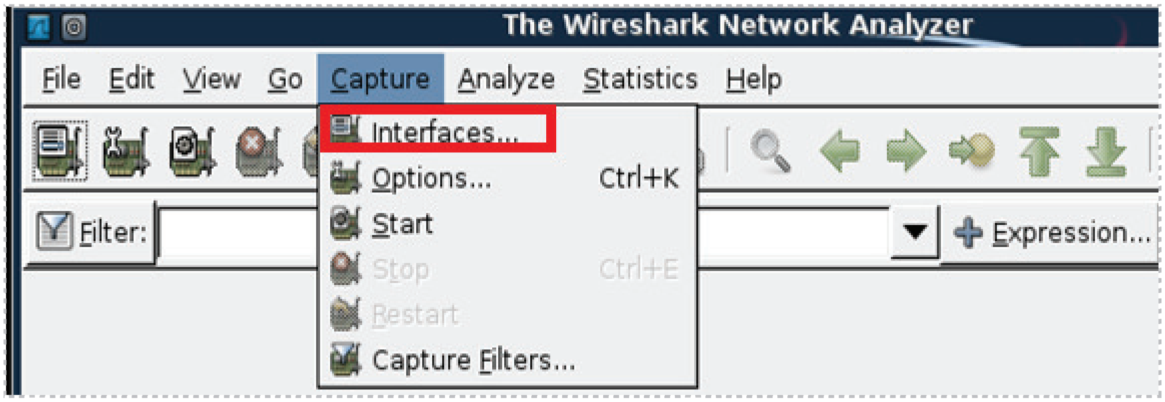
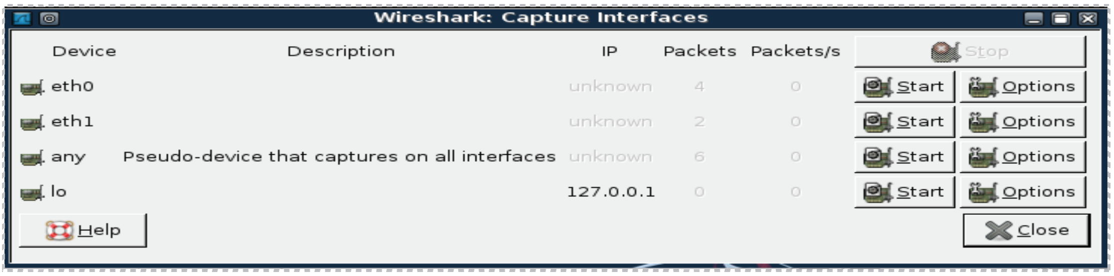


Figure 50: Selecting Interfaces from the Capture Menu

The **Wireshark: Capture Interfaces** pop-up box will be displayed on the sniffer.

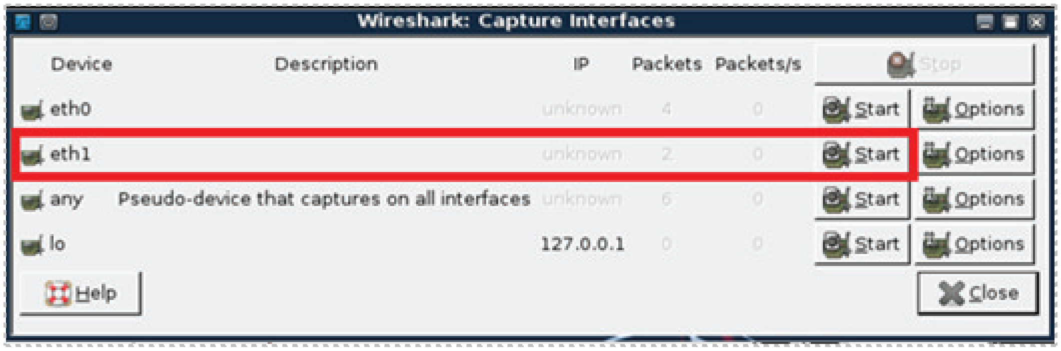

Wireshark: Capture Interfaces

Device	Description	IP	Packets	Packets/s	Stop	
eth0		unknown	4	0	Start	Options
eth1		unknown	2	0	Start	Options
any	Pseudo-device that captures on all interfaces	unknown	6	0	Start	Options
lo		127.0.0.1	0	0	Start	Options

Figure 51: The Devices eth0 and eth1 do not have IP Addresses listed

Notice that eth0 and eth1 do not have IP Addresses listed under the IP column.

12. Within the **Capture Interfaces** menu, click Start for the eth1 network device.

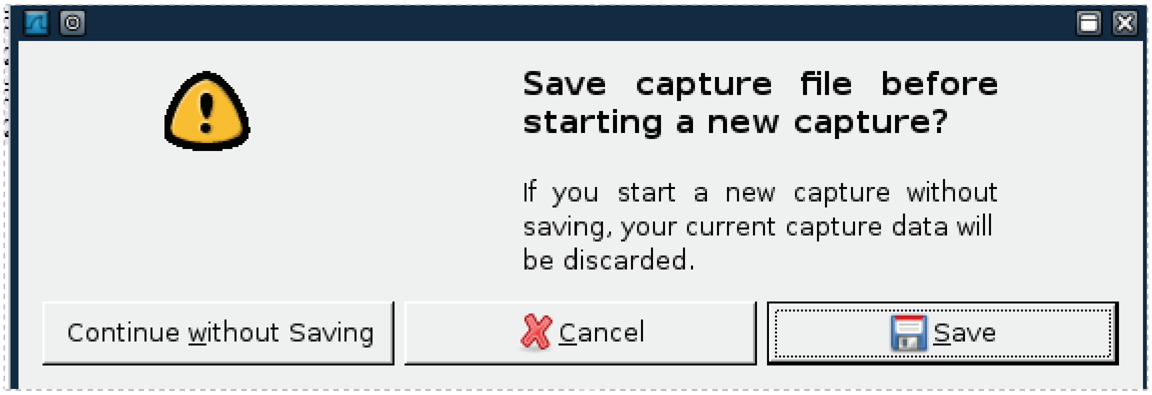

Wireshark: Capture Interfaces

Device	Description	IP	Packets	Packets/s	Stop	
eth0		unknown	4	0	Start	Options
eth1		unknown	2	0	Start	Options
any	Pseudo-device that captures on all interfaces	unknown	6	0	Start	Options
lo		127.0.0.1	0	0	Start	Options

Figure 52: Starting a Capture on the Network using Interface eth1

During this exercise, we will be capturing plain text FTP, or File Transfer Protocol, traffic from the BackTrack 4 External Machine to the Windows 2003 Server External machine.

13. Click **Continue without Saving** if you receive a warning message.

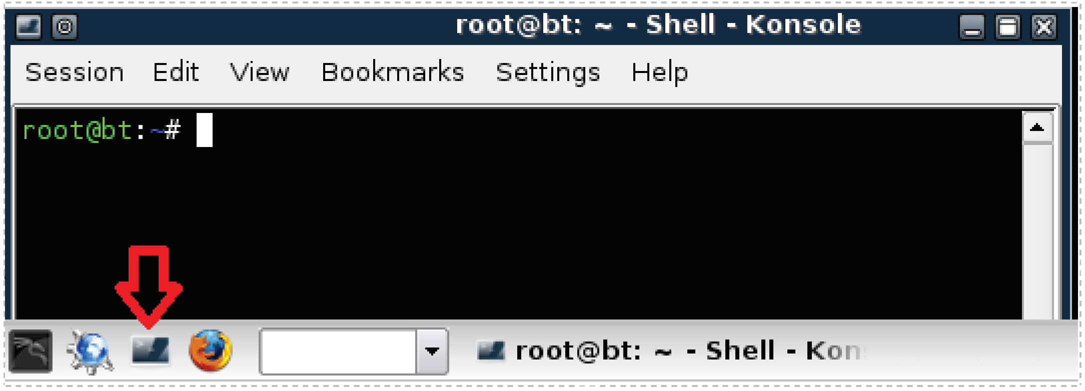


Save capture file before starting a new capture?

If you start a new capture without saving, your current capture data will be discarded.

Figure 53: Continue Without Saving

14. In the Sniffer's terminal, type the command **bye** to exit the ftp connection.
15. Open a terminal on the Backtrack 4 system by clicking on the image to the left of Firefox in the task bar, in the bottom of the screen.

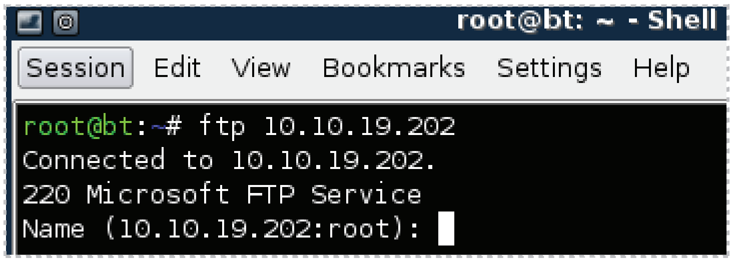


root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt: ~ - Shell - Kon

```
root@bt:~#
```

Figure 54: The BackTrack Terminal

16. Type the following command to connect to the Windows 2003 FTP Server:
root@bt:~#**ftp 10.10.19.202**



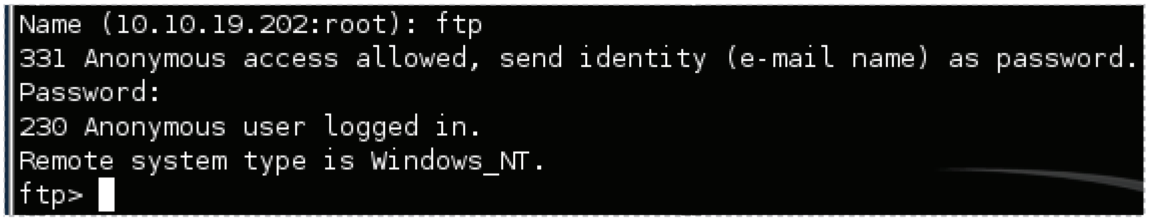
```
root@bt:~# ftp 10.10.19.202
Connected to 10.10.19.202.
220 Microsoft FTP Service
Name (10.10.19.202:root):
```

Figure 55: Connecting to the FTP Server 192.168.100.201

You should receive the message, *Connected to 10.10.19.202.*

17. For the username, type **ftp** and hit enter. For the password, type **supersecure**.

For security purposes, the password will not be displayed when you type it.

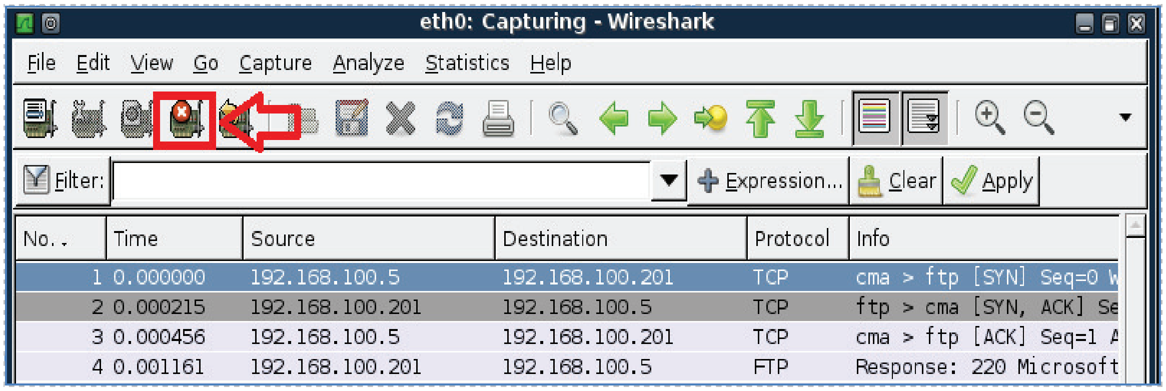


```
Name (10.10.19.202:root): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
Remote system type is Windows_NT.
ftp> 
```

Figure 56: Logging in to the FTP Server

You should receive the message, *230 Anonymous user logged in*.

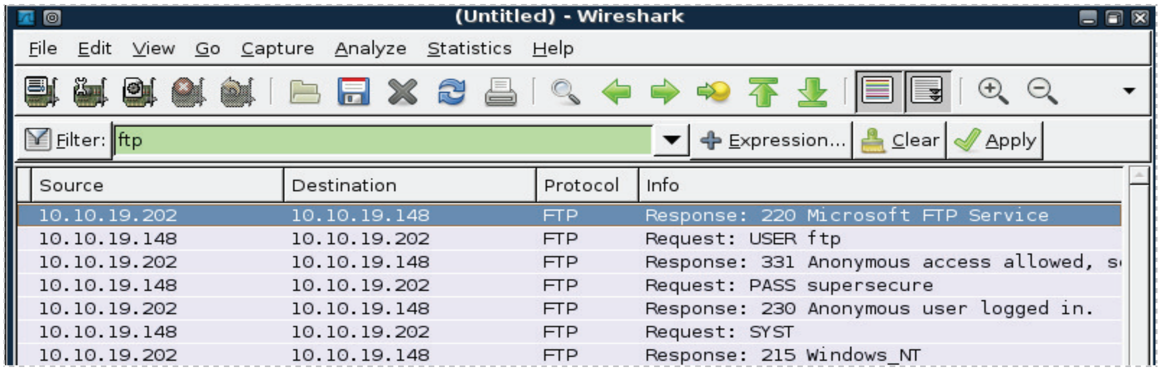
18. On the Sniffer machine, click the stop button on Wireshark to stop the capture.


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.100.5	192.168.100.201	TCP	cma > ftp [SYN] Seq=0 W
2	0.000215	192.168.100.201	192.168.100.5	TCP	ftp > cma [SYN, ACK] Se
3	0.000456	192.168.100.5	192.168.100.201	TCP	cma > ftp [ACK] Seq=1 A
4	0.001161	192.168.100.201	192.168.100.5	FTP	Response: 220 Microsoft

Figure 57: Stopping the Wireshark capture

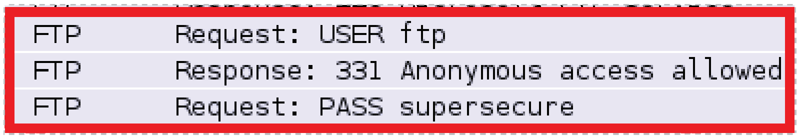
19. On the Sniffer machine, type **ftp** in the filter pane and click apply. (if needed)



Source	Destination	Protocol	Info
10.10.19.202	10.10.19.148	FTP	Response: 220 Microsoft FTP Service
10.10.19.148	10.10.19.202	FTP	Request: USER ftp
10.10.19.202	10.10.19.148	FTP	Response: 331 Anonymous access allowed, s
10.10.19.148	10.10.19.202	FTP	Request: PASS supersecure
10.10.19.202	10.10.19.148	FTP	Response: 230 Anonymous user logged in.
10.10.19.148	10.10.19.202	FTP	Request: SYST
10.10.19.202	10.10.19.148	FTP	Response: 215 Windows_NT

Figure 58: Typing ftp in the Wireshark filter pane

If you scroll over, you will see the username of **ftp** and the password of **supersecure**.



```
FTP      Request: USER ftp
FTP      Response: 331 Anonymous access allowed
FTP      Request: PASS supersecure
```

Figure 59: The FTP username and password appear in clear text.

20. Exit Wireshark. In the BackTrack 4 terminal, type the command **bye** to exit the ftp connection.

Task 2.2 Conclusion

Wireshark is a GUI, or Graphical User Interface, tool that will allow you to capture and analyze network traffic. Wireshark runs on Windows, Linux, and on Mac OS X. Wireshark can be used to capture network traffic on an interface on the sniffer without an IP Address. The Wireshark filter pane can be used to filter for various types of traffic.

Task 2.3 Discussion Questions

1. Do FTP usernames and passwords appear in clear text?
2. How do you choose the interface to capture on within Wireshark?
3. How do you filter for a certain protocol within the Wireshark program?
4. How do you open the Wireshark program from the terminal in Linux?

Task 3 Capturing and Analyzing Traffic with Network Miner

Network Miner is an NFAT, or Network Forensic Analysis Tool, that runs on Windows operating systems. The tcpdump command has no Graphical User Interface and is only utilized within a Linux terminal. Wireshark shows you the raw output of network traffic captures and allows you to analyze them. Network Miner will allow you to capture data, and it will also pull out items like clear text messages and pictures.

Task 3.1 Using Network Miner

Open Network Miner

1. Open Network Miner on the Windows 7 machine by double clicking on the desktop shortcut.

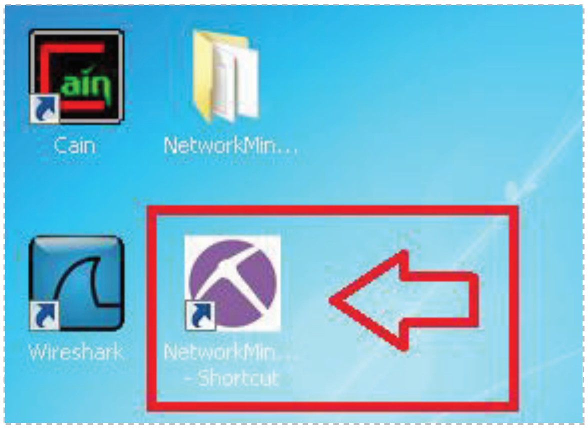
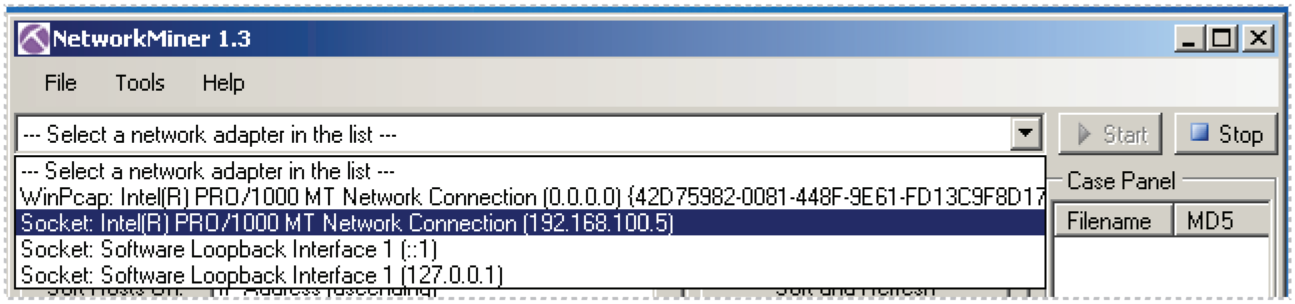


Figure 60: Opening Network Miner

2. Click the arrow to the right of the words **Select a network adapter in the list** and select: **Socket: Intel® PRO/1000MT Network Connection(192.168.100.5)**

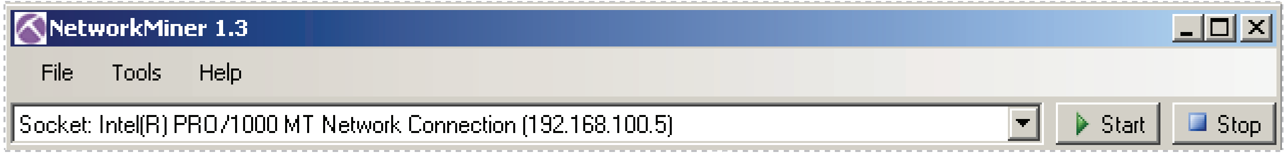


--- Select a network adapter in the list ---

--- Select a network adapter in the list ---
WinPcap: Intel(R) PRO/1000 MT Network Connection (0.0.0.0) {42D75982-0081-448F-9E61-FD13C9F8D17
Socket: Intel(R) PRO/1000 MT Network Connection (192.168.100.5)
Socket: Software Loopback Interface 1 (::1)
Socket: Software Loopback Interface 1 (127.0.0.1)

Figure 61: Selecting the Appropriate Interface

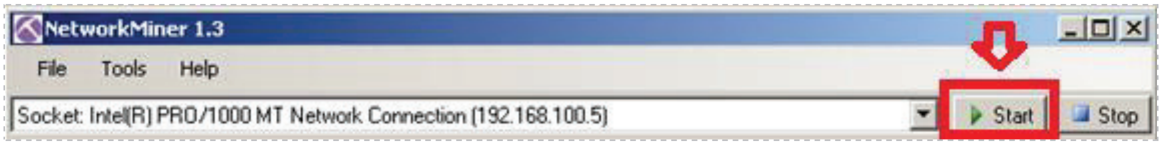
Verify that the correct Interface has now been selected within Network Miner.



Socket: Intel(R) PRO/1000 MT Network Connection (192.168.100.5)

Figure 62: The Correct Interface has been selected within Network Miner

3. Click the **Start** button, located on the right, to start a network capture.



Socket: Intel(R) PRO/1000 MT Network Connection (192.168.100.5)

Figure 63: Staring the Capture

4. Click on the **Internet Explorer Icon** in the Windows Taskbar.

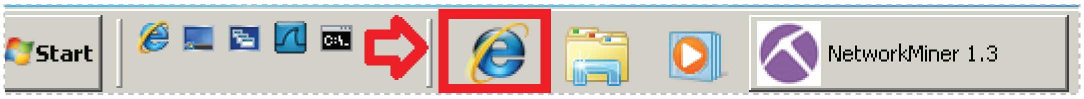


Figure 64: Opening Internet Explorer

Internet Explorer should open to a Blank Page with **about:blank** in the URL bar.

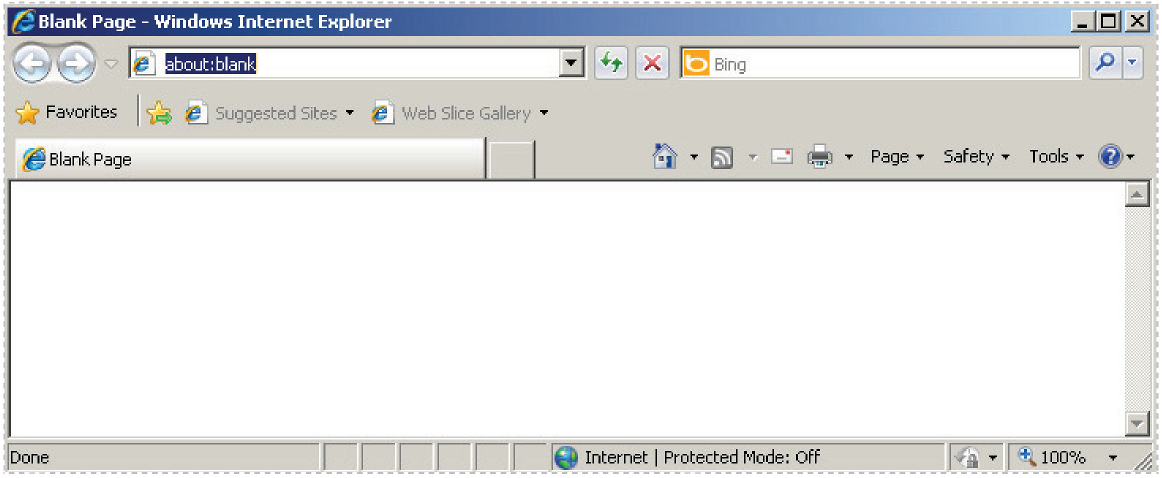


Figure 65: A Blank Page in Internet Explorer

5. In the URL bar, type the following to connect to the Windows 2003 Server's Web Page: http://192.168.100.201/

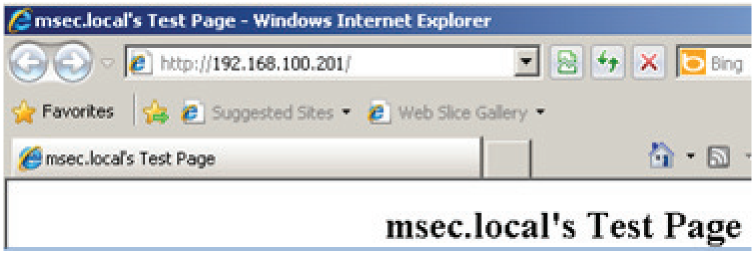


Figure 66: The Windows 2003 Web Page

You should see the **msec.local's Test Page** when connecting to the Windows 2003 Server.

6. In the URL bar, type the following to connect to the RHEL Web Page: http://192.168.100.147/

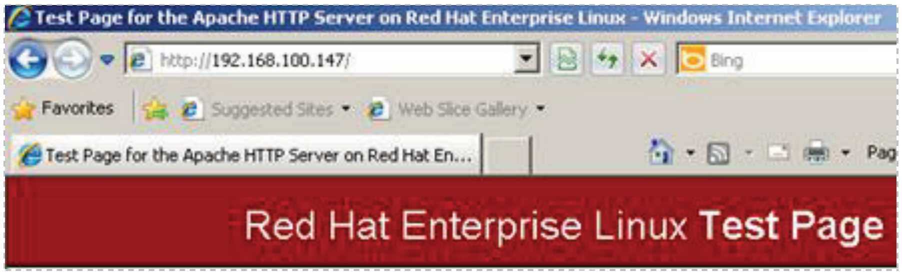

Test Page for the Apache HTTP Server on Red Hat Enterprise Linux - Windows Internet Explorer
http://192.168.100.147/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Test Page for the Apache HTTP Server on Red Hat En...
Pag
Red Hat Enterprise Linux Test Page

Figure 67: The RHEL Web Site

7. Click on the **Stop** button to end the Network Miner capture.

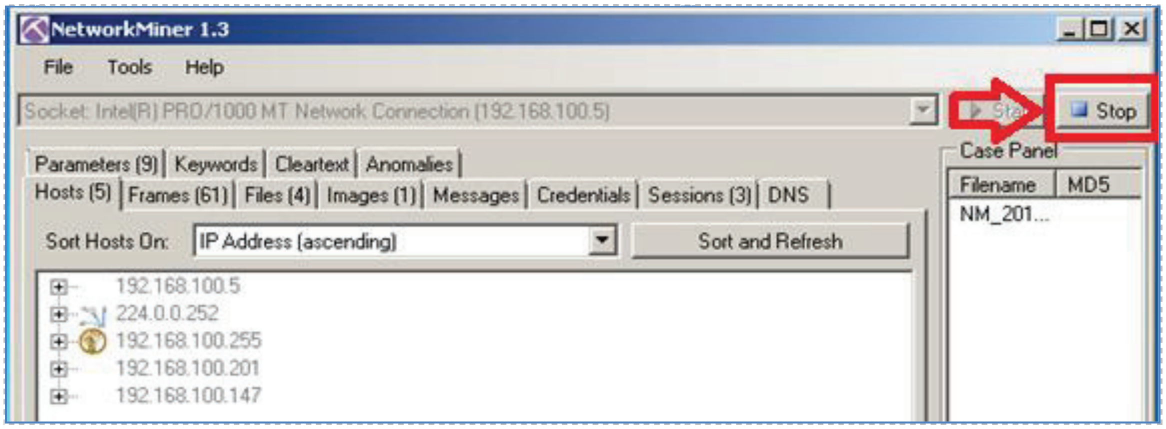
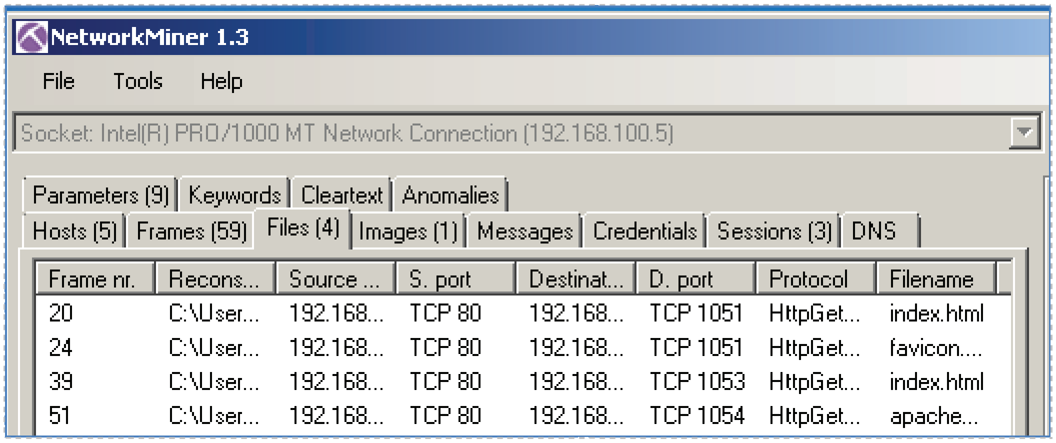


Figure 68: Files within the Network Capture

8. Click on the **Files** tab within the Network Miner Program.

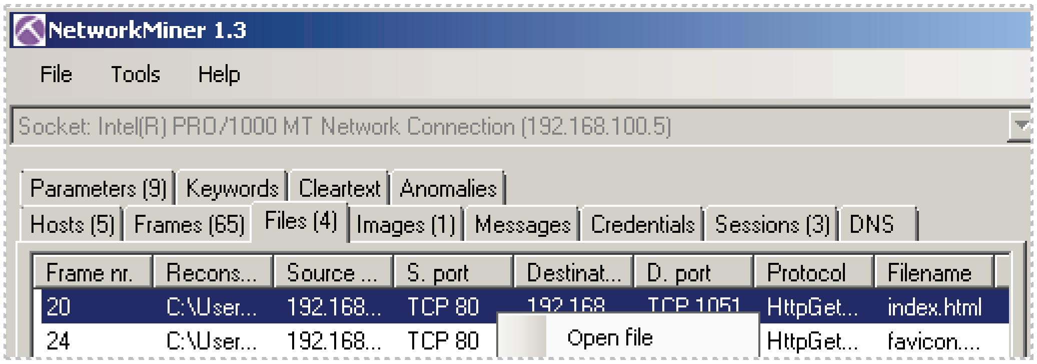


Socket: Intel(R) PRO/1000 MT Network Connection (192.168.100.5)

Frame nr.	Recons...	Source ...	S. port	Destinat...	D. port	Protocol	Filename
20	C:\User...	192.168...	TCP 80	192.168...	TCP 1051	HttpGet...	index.html
24	C:\User...	192.168...	TCP 80	192.168...	TCP 1051	HttpGet...	favicon....
39	C:\User...	192.168...	TCP 80	192.168...	TCP 1053	HttpGet...	index.html
51	C:\User...	192.168...	TCP 80	192.168...	TCP 1054	HttpGet...	apache...

Figure 69: Files within the Network Capture

9. Right click on the first **index.html** file and select open file.

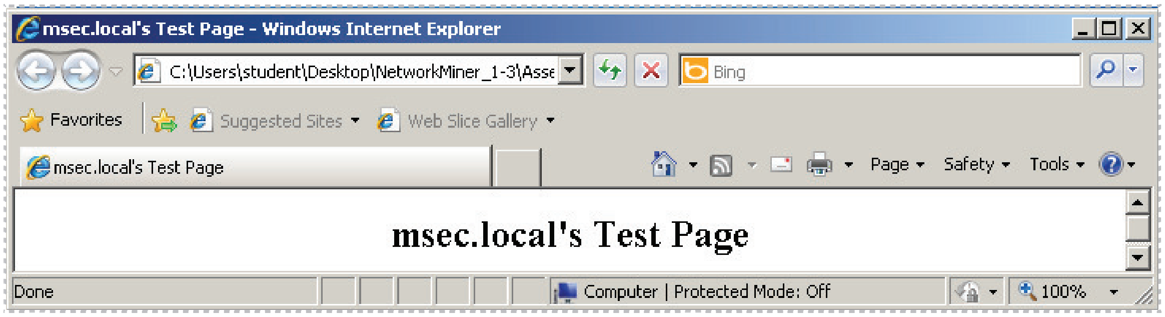


Socket: Intel(R) PRO/1000 MT Network Connection (192.168.100.5)

Frame nr.	Recons...	Source ...	S. port	Destinat...	D. port	Protocol	Filename
20	C:\User...	192.168...	TCP 80	192.168...	TCP 1051	HttpGet...	index.html
24	C:\User...	192.168...	TCP 80			HttpGet...	favicon....

Figure 70: The index.html file saved within the Network Capture

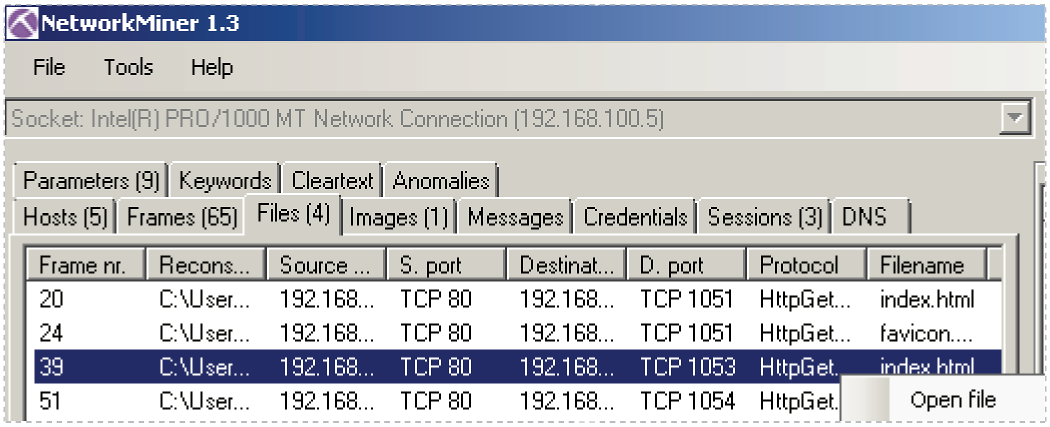
You should see msec.local's test page.


msec.local's Test Page - Windows Internet Explorer
C:\Users\student\Desktop\NetworkMiner_1-3\Asse
Bing
Favorites
Suggested Sites
Web Slice Gallery
msec.local's Test Page
Page
Safety
Tools
Done
Computer | Protected Mode: Off
100%

msec.local's Test Page

Figure 71: Opening a Local Copy of the Index.html file

10. Right click on the second **index.html** file and select open file.


NetworkMiner 1.3
File Tools Help
Socket: Intel(R) PRO/1000 MT Network Connection (192.168.100.5)
Parameters (9) Keywords Cleartext Anomalies
Hosts (5) Frames (65) Files (4) Images (1) Messages Credentials Sessions (3) DNS
Open file

Frame nr.	Recons...	Source ...	S. port	Destinat...	D. port	Protocol	Filename
20	C:\User...	192.168...	TCP 80	192.168...	TCP 1051	HttpGet...	index.html
24	C:\User...	192.168...	TCP 80	192.168...	TCP 1051	HttpGet...	favicon....
39	C:\User...	192.168...	TCP 80	192.168...	TCP 1053	HttpGet.	index.html
51	C:\User...	192.168...	TCP 80	192.168...	TCP 1054	HttpGet.	

Figure 72: The index.html file saved within the Network Capture

You should see the Red Hat Enterprise Linux Test Page.

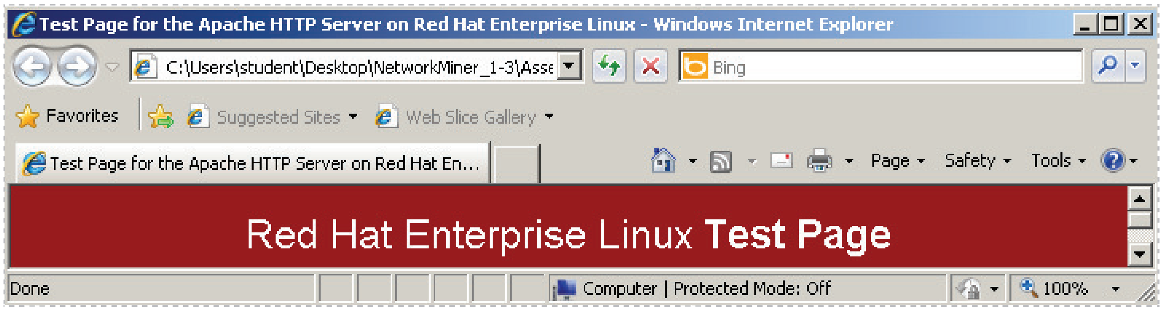

Test Page for the Apache HTTP Server on Red Hat Enterprise Linux - Windows Internet Explorer
C:\Users\student\Desktop\NetworkMiner_1-3\Asse
Bing
Favorites
Suggested Sites
Web Slice Gallery
Test Page for the Apache HTTP Server on Red Hat En...
Page
Safety
Tools
Red Hat Enterprise Linux Test Page
Done
Computer | Protected Mode: Off
100%

Figure 73: Opening a Local Copy of the Index.html file

Task 3.2 Conclusion

Network Miner is an NFAT, or Network Forensic Analysis Tool, that runs on Windows operating systems. Network Miner will allow you to capture data and will also pull out items like clear text messages, pictures, and web pages from visited sites.

Task 3.3 Discussion Questions

1. What kind of tool is Network Miner?
2. On what operating systems will the Network Miner program run?
3. How do you parse out web pages of visited sites in Network Miner?
4. What needs to be configured within Network Miner prior to capturing data?

5 References

1. Wireshark:
   http://www.wireshark.org/

2. Network Miner:
   http://www.netresec.com/?page=NetworkMiner

3. Man Page of tcpdump:
   http://www.tcpdump.org/tcpdump_man.html

4. Wireshark Download:
   http://www.wireshark.org/download.html

5. Network Miner Download:
   http://sourceforge.net/projects/networkminer/files/latest/download

CompTIA Security+® Lab Series

Lab 2: Secure Network Administration Principles - Log Analysis

CompTIA Security+® Domain 1 - Network Security

Objective 1.2: Apply and implement secure network administration principles

Document Version: 2012-08-15 (Beta)

Lab Author: Jesse Varsalone
Assistant Professor
Cyber Security

Organization: Community College of Baltimore County

The development of this document is funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) is an entity of Moraine Valley Community College. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation. A copy of this license can be found at http://www.gnu.org/licenses/fdl.html.

Contents

1 Introduction 3
2 Objective: Apply and implement secure network administration principles 3
3 Pod Topology 4
4 Lab Settings 5
Task 1 Log Analysis in Linux Using grep 8
Task 1.1 Using grep 8
Task 1.2 Conclusion 14
Task 1.3 Discussion Questions 14
Task 2 Log Analysis in Linux Using gawk 15
Task 2.1 Using gawk 15
Task 2.2 Conclusion 21
Task 2.3 Discussion Questions 21
Task 3 Log Analysis in Windows Using find 22
Task 3.1 Using find in Windows 22
Task 3.2 Conclusion 28
Task 3.3 Discussion Questions 28
5 References 29

1 Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will be able to parse log files within Linux and Windows for information pertinent to security events on their system. Students will perform administration on Linux and Windows machines and view the logs from these tasks.

This lab includes the following tasks:

- Task 1 - Log Analysis in Linux Using grep
- Task 2 - Log Analysis in Linux Using gawk
- Task 3 - Log Analysis in Windows Using find

2 Objective: Apply and implement secure network administration principles

You may have read articles online describing situations where someone's passwords were stolen and then used to gain access to an account in order to steal money. The use of strong passwords is critical to protecting your accounts, as well as data and resources within an organization.

grep [1] –Stands for Global Regular Expression Print. The GREP utility allows you to search through a large number of files and folders for specified text.

gawk [2] – The Linux/UNIX gawk command will allow you to display output in an easy to display human readable format. Typing **gawk –help** in Linux will display gawk options.

find [3] – This command can be used within Linux and Windows. The find command in Windows will allow you to search for a specific string within a large group of values.

secure [4] – This log file tracks SSH, or Secure Shell, connections. It provides information such as IP Addresses, and date and time stamps. It also tracks other events related to security, such as the creation of new user accounts and new group accounts.

access_log – This log file tracks HTTP, or Hyper Text Transfer Protocol, connections. It provides information such as IP addresses, user Agents, and date and time stamps.

3 Pod Topology

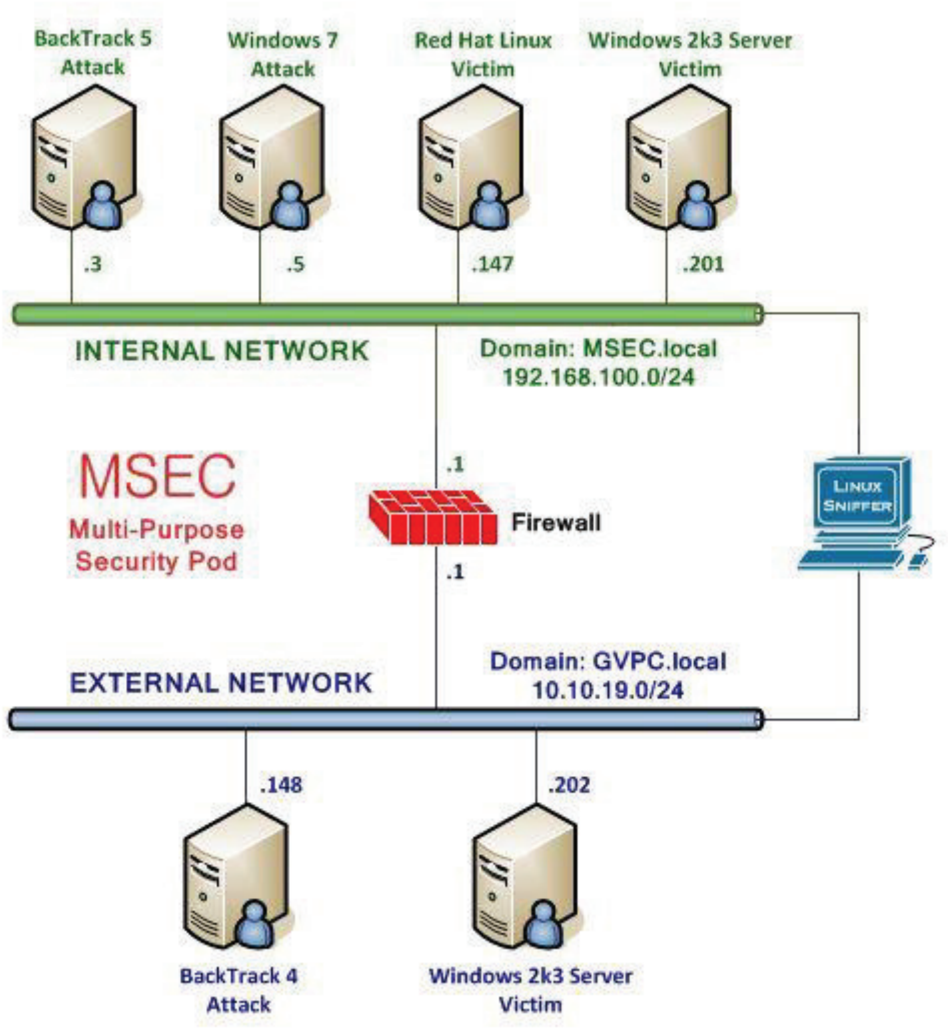


Figure 1: MSEC Network Topology

4 Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

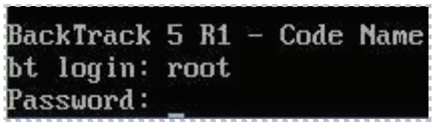
Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

BackTrack 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password
RHEL Internal Victim Machine	192.168.100.147
RHEL root password	password
BackTrack 4 External Attack Machine	10.10.19.148
BackTrack 4 root password	password
Windows 2k3 Server External Victim Machine	10.10.19.202
Windows 2k3 Server administrator password	password

BackTrack 5 Login:

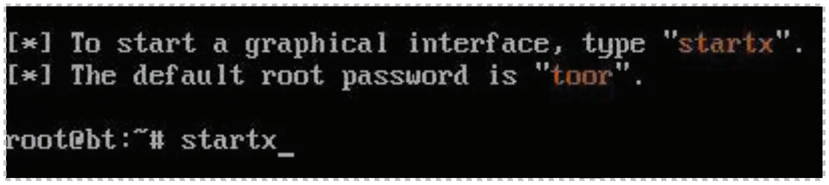
1. Click on the BackTrack 5 icon on the topology.
2. Type **root** at the **bt login:** username prompt.
3. Type **password** at the **Password:** prompt.



```
BackTrack 5 R1 - Code Name
bt login: root
Password: _
```

Figure 2: BackTrack 5 login

4. To start the GUI, type **startx** at the root@bt:~# prompt.



```
[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".

root@bt:~# startx_
```

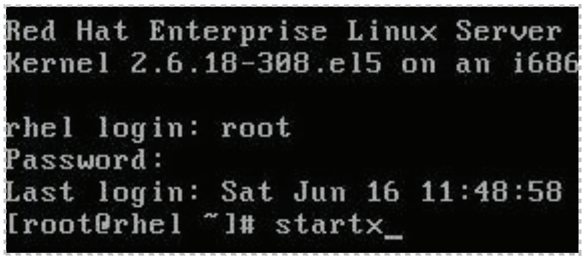
Figure 3: BackTrack 5 GUI start up

Red Hat Enterprise Linux Login:

1. Click on the Red Hat Linux icon on the topology.
2. Type **root** at the rhel login: prompt.
3. Type **password** at the Password: prompt.

For security purposes, the password will not be displayed.

4. To start the GUI, type **startx** at the [root@rhe ~]# prompt.

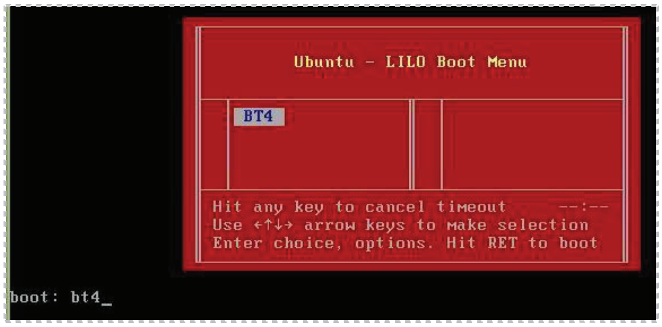


```
Red Hat Enterprise Linux Server
Kernel 2.6.18-308.el5 on an i686

rhel login: root
Password:
Last login: Sat Jun 16 11:48:58
[root@rhel ~]# startx_
```

Figure 4: RHEL login

BackTrack 4 Login:

1. Click on the BackTrack 4 icon on the topology.
2. At the Ubuntu boot menu, type **bt4** to select the BackTrack 4 system.



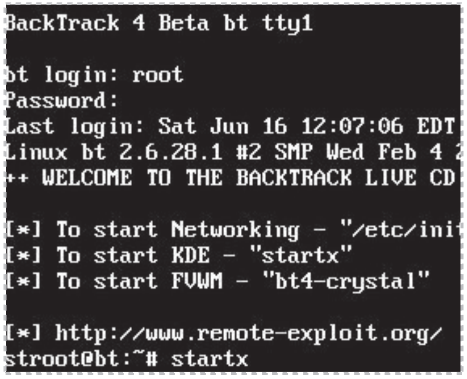
```
Ubuntu - LILO Boot Menu

BT4

Hit any key to cancel timeout     --:--
Use ←↑↓→ arrow keys to make selection
Enter choice, options. Hit RET to boot

boot: bt4_
```

Figure 5: Ubuntu Boot Menu

3. Type **root** at the bt login: username prompt.
4. Type **password** at the Password: prompt.

For security purposes, the password will not be displayed.

5. To start the GUI, type **startx** at the stroot@bt:~# prompt.

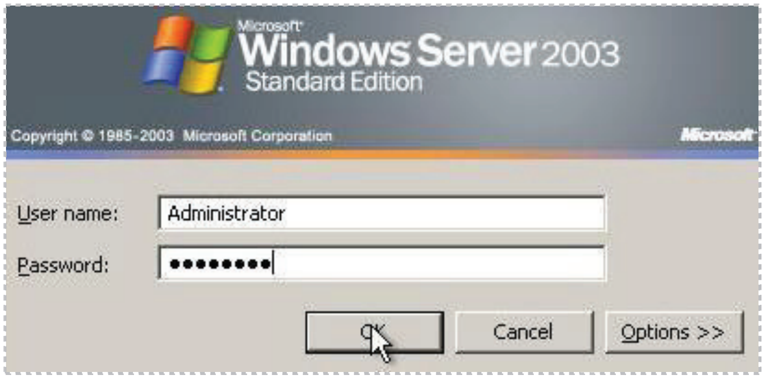


```
BackTrack 4 Beta bt tty1

bt login: root
Password:
Last login: Sat Jun 16 12:07:06 EDT
Linux bt 2.6.28.1 #2 SMP Wed Feb 4 2
++ WELCOME TO THE BACKTRACK LIVE CD

[*] To start Networking - "/etc/init
[*] To start KDE - "startx"
[*] To start FVWM - "bt4-crystal"

[*] http://www.remote-exploit.org/
stroot@bt:~# startx
```

Figure 6: BackTrack 4 login

Windows 2003 Server Login:

1. Click on the Windows 2k3 Server icon on the topology (these instructions will work for both internal and external victim machines).
2. Enter the User name, **Administrator** (verify the username with your instructor).
3. Type in the password: **password** and click the **OK** button (verify the password with your instructor).



User name: Administrator

Password: ••••••••

Figure 7: Windows 2k3 login

Task 1 Log Analysis in Linux Using grep

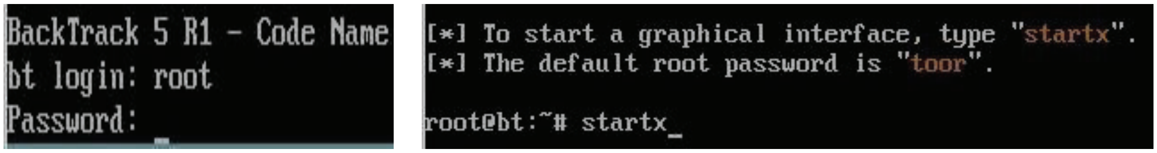
Within Network Administration, it is very important to check the system logs every day to monitor who is logging on and what type of activity is happening on a system. Log files can become extremely large, so tools like grep can be valuable in allowing the Network Administrator to filter for certain values. There are many log analysis jobs that can be run using grep that will provide the Network Administrator with information on the status of a system.

Task 1.1 Using grep

Open a Terminal to Get Started

If you have already logged in and started the GUI interface, as described in the Lab Settings section, you may start immediately at Step 1.

When starting the BackTrack 5 system, you must first enter in the username **root** followed by the password, **password**. At the initial start up screen, type the following command to start the GUI interface:
root@bt.~#**startx**.

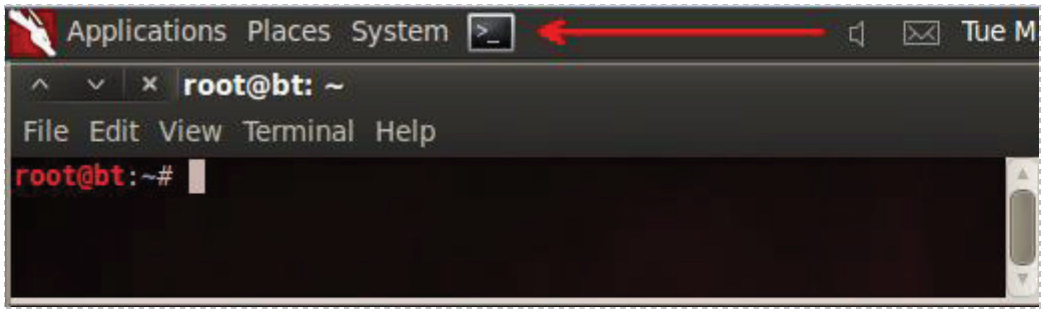


```
BackTrack 5 R1 - Code Name
bt login: root
Password: _
```

```
[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".

root@bt:~# startx_
```

Figure 8: Linux Initial Startup Screens

1. Open a terminal on the BackTrack 5 Internal Attack system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.

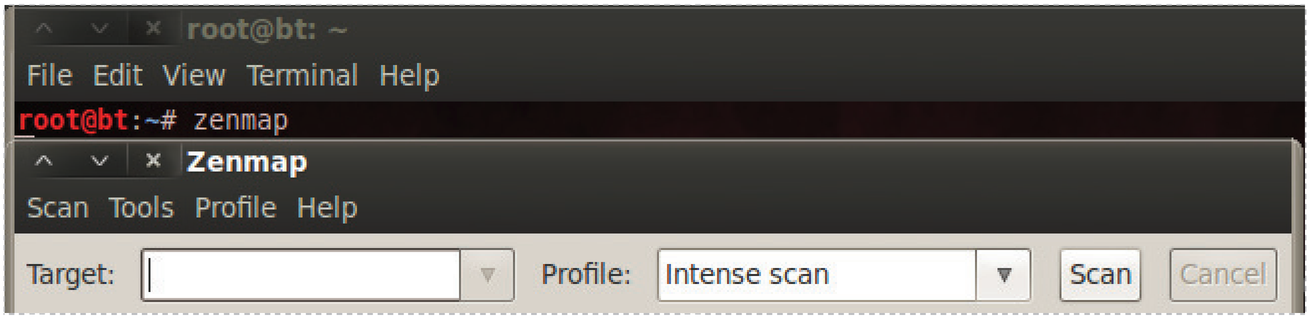


```
root@bt:~#
```

Figure 9: The Terminal Windows within BackTrack

Nmap, or network mapper, allows you to determine which TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) ports are open on a remote system. Zenmap is a GUI, Graphical User Interface, front-end for nmap. Zenmap is packaged with nmap.

2. Type the following command to perform a TCP nmap scan of the Red Hat Linux Victim: root@bt:~#**zenmap**



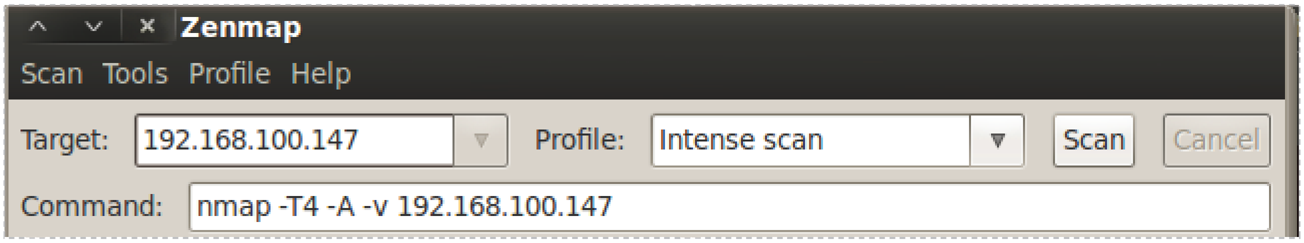
```
root@bt:~# zenmap
```

Target:

Profile: Intense scan

Figure 10: Zenmap can be Launched by Typing the Zenmap Command within the Terminal

3. In the target box, type the IP Address of **192.168.100.147** (the Linux victim).



Target: 192.168.100.147

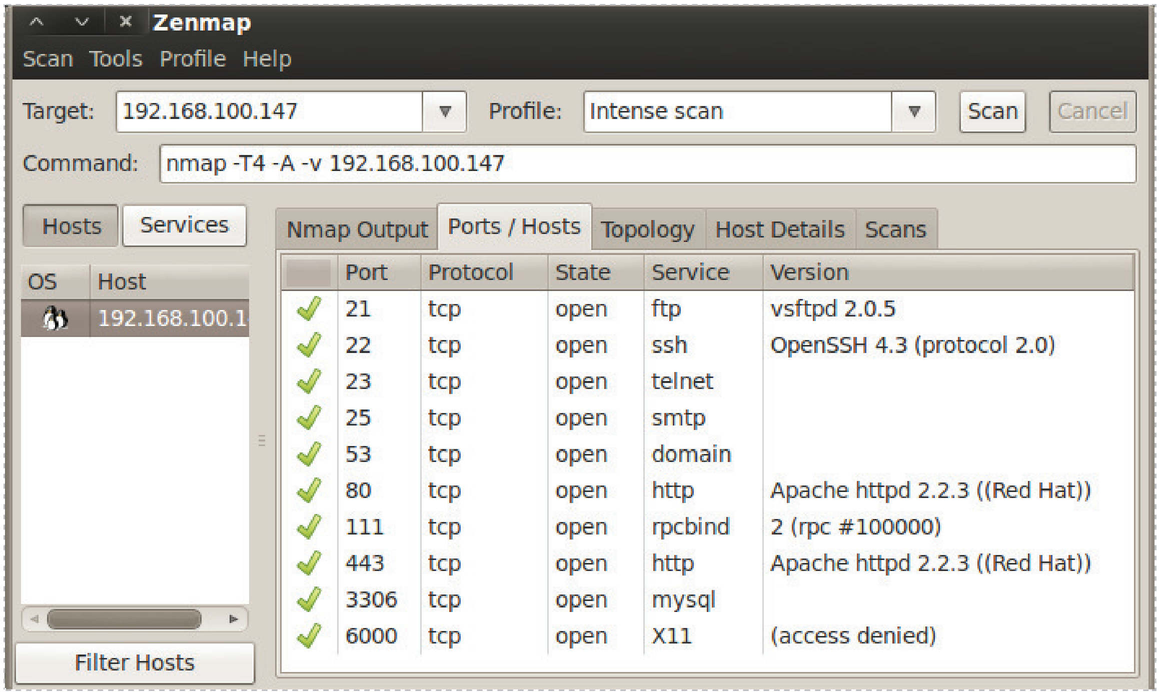
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.100.147

Figure 11: Entering the IP Address of the Target Machine

Notice that the switches for nmap are automatically added in the box directly below.

4. After a few seconds, click on the **Ports/Hosts** tab to display the open TCP ports.



Target: 192.168.100.147

Profile: Intense scan

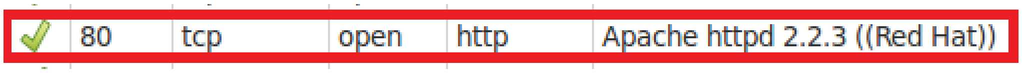
Command: nmap -T4 -A -v 192.168.100.147

OS	Host
	192.168.100.1

	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	vsftpd 2.0.5
✓	22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
✓	23	tcp	open	telnet	
✓	25	tcp	open	smtp	
✓	53	tcp	open	domain	
✓	80	tcp	open	http	Apache httpd 2.2.3 ((Red Hat))
✓	111	tcp	open	rpcbind	2 (rpc #100000)
✓	443	tcp	open	http	Apache httpd 2.2.3 ((Red Hat))
✓	3306	tcp	open	mysql	
✓	6000	tcp	open	X11	(access denied)

Figure 12: The Open TCP Ports on the Remote System

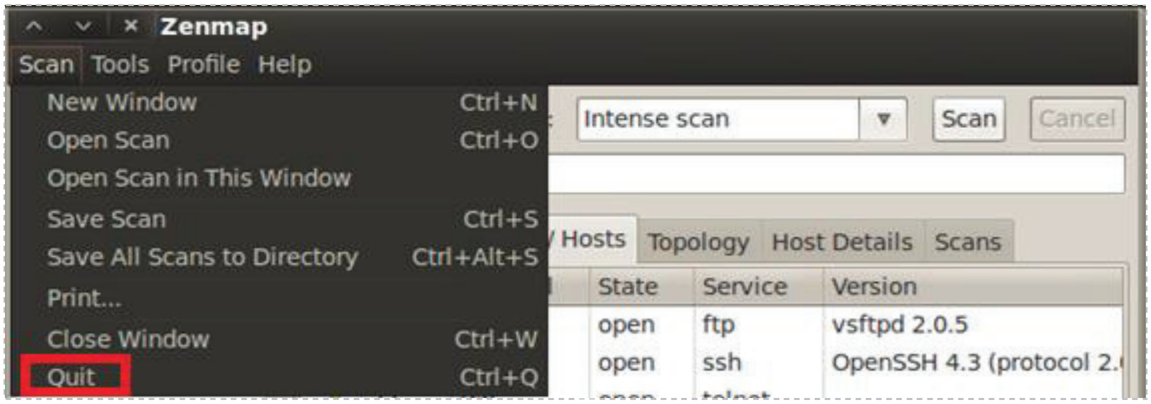
Notice that port 80 is open, which likely means the remote system is running a Web Server. The zenmap scan indicates that the web server is Apache 2.2.3.



✓	80	tcp	open	http	Apache httpd 2.2.3 ((Red Hat))

Figure 13: The Remote System is a Web Server

5. Close the Zenmap tool by selecting **Scan** from the menu bar, and select **Quit**. Click **Close Anyway** if you receive a warning indicating that the scan is not saved.



State	Service	Version
open	ftp	vsftpd 2.0.5
open	ssh	OpenSSH 4.3 (protocol 2.

Figure 14: Closing Zenmap

Now that we know port 80 is open, we can attempt to connect to the target web site.

6. Open Firefox on the BackTrack 5 machine, by performing the following steps: Click **Applications** from the Menu bar, select **Internet**, then **Firefox Web Browser**.

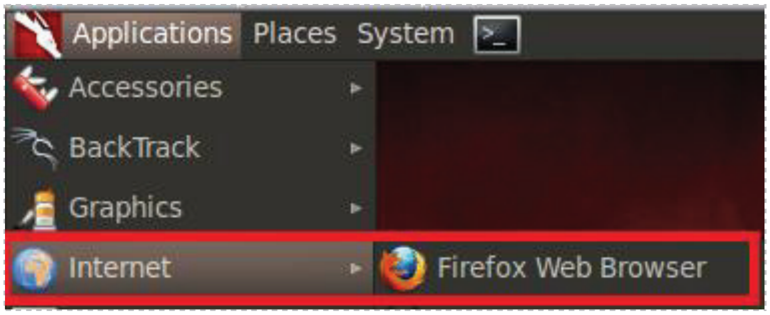
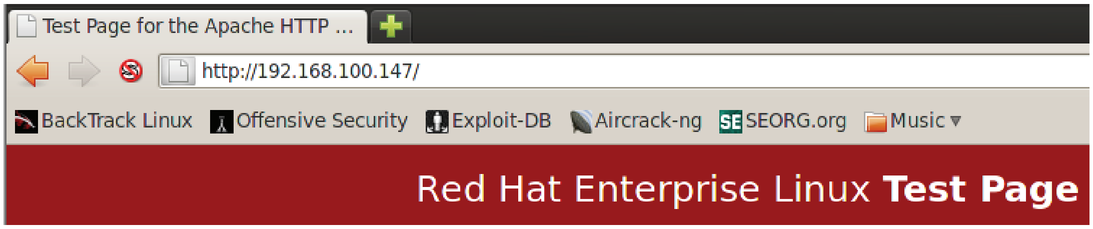


Figure 15: Opening Firefox on BackTrack

7. In the URL bar, type the address: http://192.168.100.147

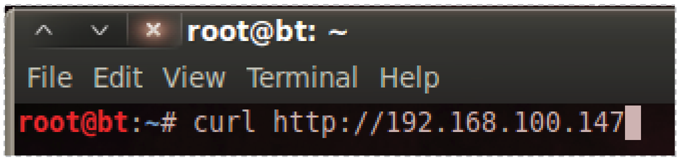


Red Hat Enterprise Linux **Test Page**

Figure 16: The Web Site of the Red Hat System

The test page likely indicates that the web site has not been configured. Close Firefox. Although you can view the HTML code of a web page in Firefox, there is also a Linux utility called curl, which stands for client Uniform Resource Locator.

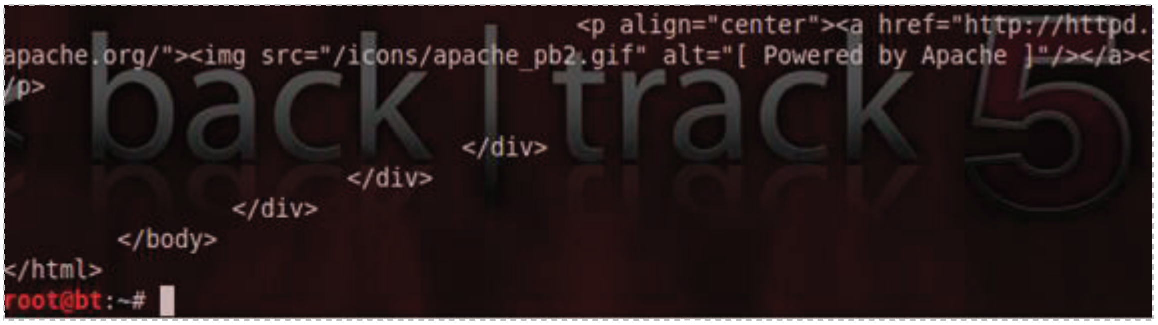
8. **Curl** can be used to make a copy of the website. On the BackTrack 5 terminal, type: root@bt:~#**curl http://192.168.100.147**



```
root@bt:~# curl http://192.168.100.147
```

Figure 17: The curl command

The output from running the curl command will look similar to that below:

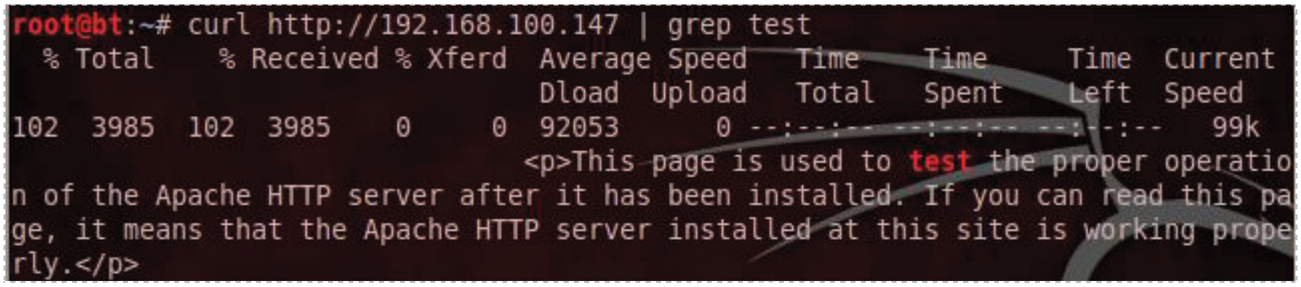


```
                                                    <p align="center"><a href="http://httpd.
apache.org/"><img src="/icons/apache_pb2.gif" alt="[ Powered by Apache ]"/></a><
/p>
                                            </div>
                                    </div>
                            </div>
                    </body>
</html>
root@bt:~# 
```

Figure 18: The Output from the curl command

Since the results from curl are large, you will find it helpful to filter them using the **grep** command.

9. On the BackTrack5 terminal, type the following to view HTML code and look for the word **test:**
root@bt:~#**curl** http://192.168.100.147 **| grep test**



```
root@bt:~# curl http://192.168.100.147 | grep test
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
102  3985  102  3985    0     0  92053      0 --:--:-- --:--:-- --:--:--   99k
                                <p>This page is used to test the proper operatio
n of the Apache HTTP server after it has been installed. If you can read this pa
ge, it means that the Apache HTTP server installed at this site is working prope
rly.</p>
```

Figure 19: Using GREP to filter the results for the word test

The word **test** is highlighted in red within the paragraph of the HTML text that contains the word.

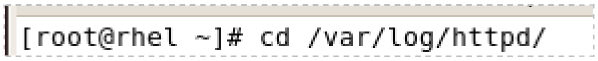
The Apache Server keeps records of the connections made to the website, including:

- IP Addresses
- User Agents
- Date/Time Stamps

The access_log is located in the /var/log/httpd directory and will have evidence of:

- The scan of the target website with Zenmap
- The connection made with Firefox
- The connection made with the curl command

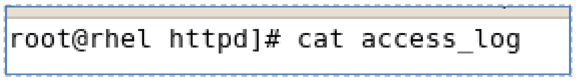
10. Switch over to the Red Hat 9 Enterprise Linux Internal Victim machine. To view the access_log, type the following command on the Red Hat system:
    [root@rhel ~]# **cd /var/log/httpd**



```
[root@rhel ~]# cd /var/log/httpd/
```

Figure 20: Switching to the Directory where the access_log is located

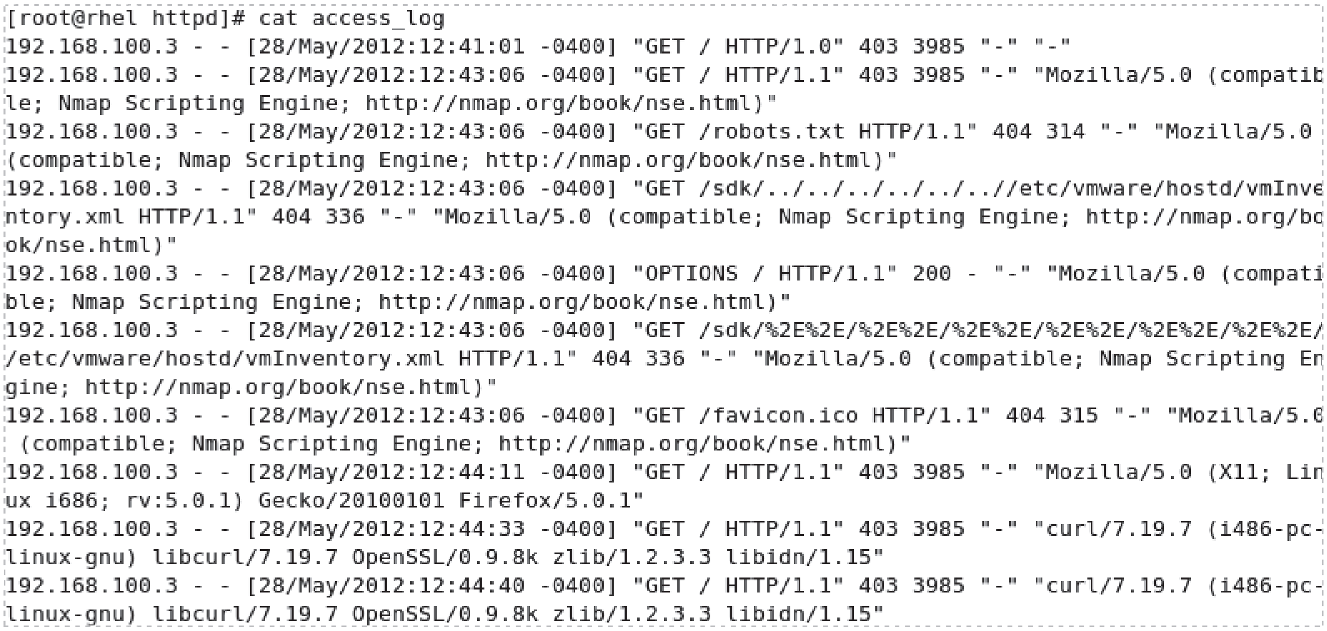
11. To view the connections in the log file, type the following command:
    [root@rhel httpd]# **cat access_log**



```
root@rhel httpd]# cat access_log
```

Figure 21: Using the cat command to view the access_log

The results will appear similar to the results in the picture below.

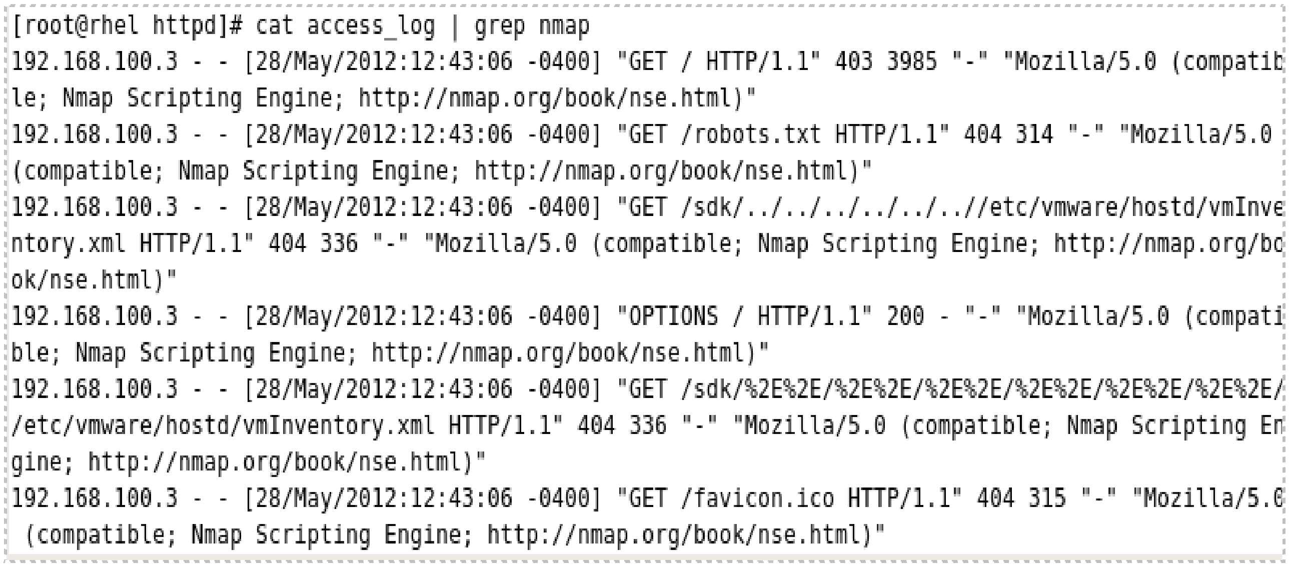


```
[root@rhel httpd]# cat access_log
192.168.100.3 - - [28/May/2012:12:41:01 -0400] "GET / HTTP/1.0" 403 3985 "-" "-"
192.168.100.3 - - [28/May/2012:12:43:06 -0400] "GET / HTTP/1.1" 403 3985 "-" "Mozilla/5.0 (compatib
le; Nmap Scripting Engine; http://nmap.org/book/nse.html)"
192.168.100.3 - - [28/May/2012:12:43:06 -0400] "GET /robots.txt HTTP/1.1" 404 314 "-" "Mozilla/5.0
(compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"
192.168.100.3 - - [28/May/2012:12:43:06 -0400] "GET /sdk/../../../../../..//etc/vmware/hostd/vmInve
ntory.xml HTTP/1.1" 404 336 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/bo
ok/nse.html)"
192.168.100.3 - - [28/May/2012:12:43:06 -0400] "OPTIONS / HTTP/1.1" 200 - "-" "Mozilla/5.0 (compati
ble; Nmap Scripting Engine; http://nmap.org/book/nse.html)"
192.168.100.3 - - [28/May/2012:12:43:06 -0400] "GET /sdk/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/
/etc/vmware/hostd/vmInventory.xml HTTP/1.1" 404 336 "-" "Mozilla/5.0 (compatible; Nmap Scripting En
gine; http://nmap.org/book/nse.html)"
192.168.100.3 - - [28/May/2012:12:43:06 -0400] "GET /favicon.ico HTTP/1.1" 404 315 "-" "Mozilla/5.0
 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"
192.168.100.3 - - [28/May/2012:12:44:11 -0400] "GET / HTTP/1.1" 403 3985 "-" "Mozilla/5.0 (X11; Lin
ux i686; rv:5.0.1) Gecko/20100101 Firefox/5.0.1"
192.168.100.3 - - [28/May/2012:12:44:33 -0400] "GET / HTTP/1.1" 403 3985 "-" "curl/7.19.7 (i486-pc-
linux-gnu) libcurl/7.19.7 OpenSSL/0.9.8k zlib/1.2.3.3 libidn/1.15"
192.168.100.3 - - [28/May/2012:12:44:40 -0400] "GET / HTTP/1.1" 403 3985 "-" "curl/7.19.7 (i486-pc-
linux-gnu) libcurl/7.19.7 OpenSSL/0.9.8k zlib/1.2.3.3 libidn/1.15"
```

Figure 22: The access_log file

In Linux, the access_log file can be extremely long. The GREP, or Global Regular Expression Print command can be used to filter the results of an access log or other output.

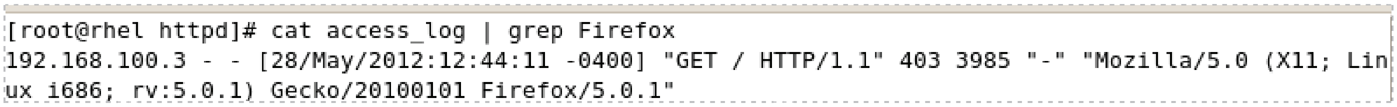
12. Type the following to filter the access_log file for the word nmap using grep:
    [root@rhel httpd]# **cat access_ log | grep nmap**



```
[root@rhel httpd]# cat access_log | grep nmap
192.168.100.3 - - [28/May/2012:12:43:06 -0400] "GET / HTTP/1.1" 403 3985 "-" "Mozilla/5.0 (compatib
le; Nmap Scripting Engine; http://nmap.org/book/nse.html)"
192.168.100.3 - - [28/May/2012:12:43:06 -0400] "GET /robots.txt HTTP/1.1" 404 314 "-" "Mozilla/5.0
(compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"
192.168.100.3 - - [28/May/2012:12:43:06 -0400] "GET /sdk/../../../../../..//etc/vmware/hostd/vmInve
ntory.xml HTTP/1.1" 404 336 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/bo
ok/nse.html)"
192.168.100.3 - - [28/May/2012:12:43:06 -0400] "OPTIONS / HTTP/1.1" 200 - "-" "Mozilla/5.0 (compati
ble; Nmap Scripting Engine; http://nmap.org/book/nse.html)"
192.168.100.3 - - [28/May/2012:12:43:06 -0400] "GET /sdk/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/
/etc/vmware/hostd/vmInventory.xml HTTP/1.1" 404 336 "-" "Mozilla/5.0 (compatible; Nmap Scripting En
gine; http://nmap.org/book/nse.html)"
192.168.100.3 - - [28/May/2012:12:43:06 -0400] "GET /favicon.ico HTTP/1.1" 404 315 "-" "Mozilla/5.0
 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)"
```

Figure 23: GREPing for the word nmap

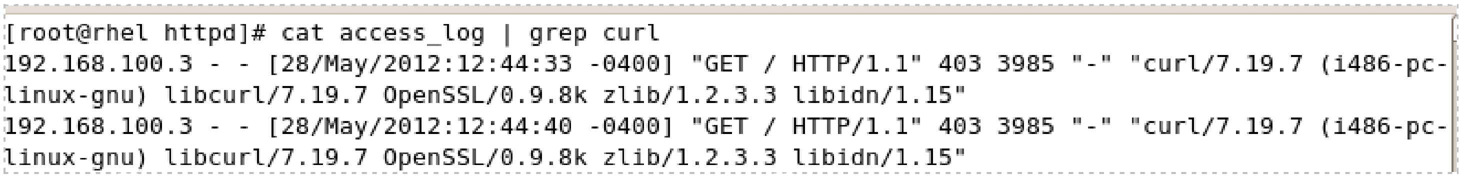
13. Type the following to filter the access_log file for the word Firefox using grep:
    [root@rhel httpd]# **cat access_ log | grep Firefox**



```
[root@rhel httpd]# cat access_log | grep Firefox
192.168.100.3 - - [28/May/2012:12:44:11 -0400] "GET / HTTP/1.1" 403 3985 "-" "Mozilla/5.0 (X11; Lin
ux i686; rv:5.0.1) Gecko/20100101 Firefox/5.0.1"
```

Figure 24: GREPing for the word Firefox

14. Type the following to filter the access_log file for the word curl using grep:
    [root@rhel httpd]# **cat access_log | grep curl**



```
[root@rhel httpd]# cat access_log | grep curl
192.168.100.3 - - [28/May/2012:12:44:33 -0400] "GET / HTTP/1.1" 403 3985 "-" "curl/7.19.7 (i486-pc-
linux-gnu) libcurl/7.19.7 OpenSSL/0.9.8k zlib/1.2.3.3 libidn/1.15"
192.168.100.3 - - [28/May/2012:12:44:40 -0400] "GET / HTTP/1.1" 403 3985 "-" "curl/7.19.7 (i486-pc-
linux-gnu) libcurl/7.19.7 OpenSSL/0.9.8k zlib/1.2.3.3 libidn/1.15"
```

Figure 25: GREPing for the word curl

Task 1.2 Conclusion

The access_log file within Linux provides information about connections to the server, including IP addresses, user agents, and date and time stamps. Log files can be extremely long and may contain a large amount of information about the connections made to the server. Linux utilities like grep can be used to filter the results of the file output.

Task 1.3 Discussion Questions

1. Where is the access_log file located on a Linux system?
2. What is contained within the access_log file?
3. What does curl stand for?
4. How do you grep for the word nmap within the access_log?

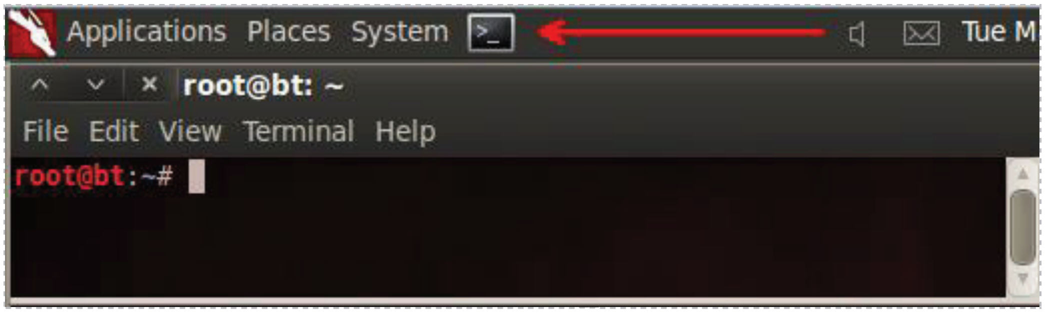
Task 2 Log Analysis in Linux Using gawk

While grep will allow you to filter the results of the file output, it will not really allow you to display the output differently. This is where gawk comes in; the Linux gawk command can be used to display the output of a text file in a more readable form.

Task 2.1 Using gawk

Perform the following steps to generate security incidents on the Linux Victim system.

1. Open a terminal on the BackTrack 5 system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.



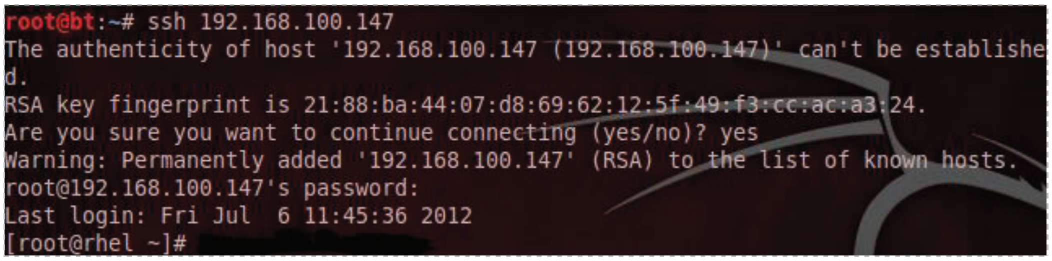
```
root@bt:~#
```

Figure 26: The Terminal Windows within BackTrack 5

2. Type the following command to SSH, to Secure Shell, to the remote system: [root@rhel ~]# **ssh 192.168.100.147**

   a. Type **yes** when asked "Are you sure you want to continue connecting (yes/no)?

   b. Type **password** for the password for root@192.168.100.147.



```
root@bt:~# ssh 192.168.100.147
The authenticity of host '192.168.100.147 (192.168.100.147)' can't be establishe
d.
RSA key fingerprint is 21:88:ba:44:07:d8:69:62:12:5f:49:f3:cc:ac:a3:24.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.100.147' (RSA) to the list of known hosts.
root@192.168.100.147's password:
Last login: Fri Jul  6 11:45:36 2012
[root@rhel ~]#
```

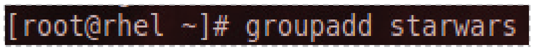
Figure 27:

You should receive a message indicating your last login time on the system.

In order to create more security events, we will be creating the group **starwars**. We will create a total of three users. After creating each of the users and putting them in the group starwars, we will assign each user account a password. The chart below lists the users and passwords for our accounts in the starwars group.

Group: starwars	
User	**Password**
luke	son
vader	dad
yoda	green

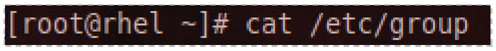
3. Type the following command to add the group **starwars**:
   [root@rhel ~]# **groupadd starwars**



```
[root@rhel ~]# groupadd starwars
```

Figure 28: Adding the Group starwars

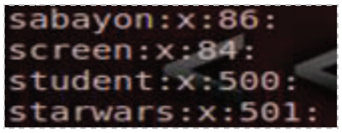
4. Type the following command to view the group file:
   [root@rhel ~]# **cat /etc/group**



```
[root@rhel ~]# cat /etc/group
```

Figure 29: Viewing the Group File

If you scroll to the bottom of the group file, you will see the group that was created along with its corresponding unique group number. Note: The root group has an id of zero.

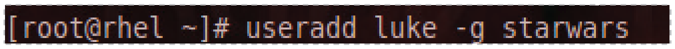


```
sabayon:x:86:
screen:x:84:
student:x:500:
starwars:x:501:
```

Figure 30: The group file

You can add users to the system in Linux by typing the **useradd** command. The **useradd** command will automatically create a directory with that user's name within the */home* directory. When the user logs in, they will be placed into their directory within */home*.

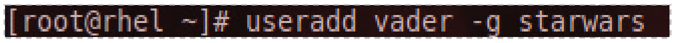
5. To add a user named **luke** and put him in the **starwars** group, type:
   [root@rhel ~]# **useradd luke –g starwars**



```
[root@rhel ~]# useradd luke -g starwars
```

Figure 31: Adding the user luke

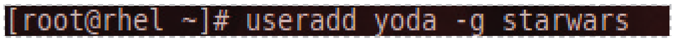
6. To add a user named **vader** and put him in the **starwars** group, type:
   [root@rhel ~]# **useradd vader –g starwars**



```
[root@rhel ~]# useradd vader -g starwars
```

Figure 32: Adding the user vader

7. To add a user named **yoda** and put him in the **starwars** group, type:
   [root@rhel ~]# **useradd yoda   –g starwars**



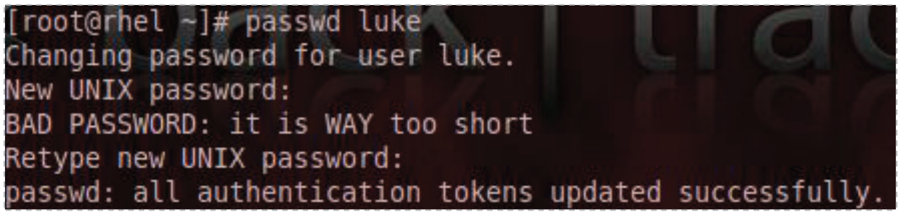
```
[root@rhel ~]# useradd yoda -g starwars
```

Figure 33: Adding the user yoda

Next, we will give each user a password. We will use simple passwords for this exercise, but that should never be done on a production system. Avoid dictionary words because attackers can use programs like John the Ripper to crack short passwords or passwords that are found in a dictionary. Stick to passwords with a minimum of eight characters, uppercase and lowercase letters, and special characters. When you use a simple password with the **passwd** command, you will be warned that the password is a “BAD PASSWORD: it is WAY too short”. Retype the password again and it will be accepted.

For security reasons, the password will not be displayed when you type it.

8. Type the following to give luke a password. Type **son** twice for the password:
   [root@rhel ~]# **passwd luke**

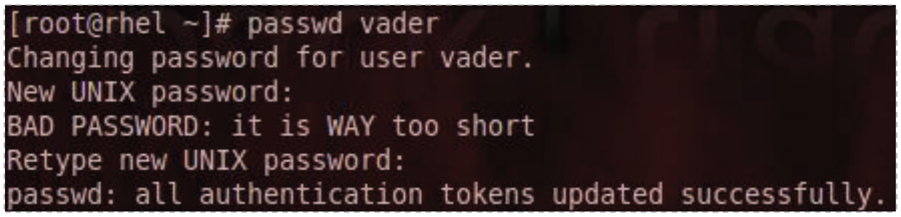


```
[root@rhel ~]# passwd luke
Changing password for user luke.
New UNIX password:
BAD PASSWORD: it is WAY too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Figure 34: Giving the user a Password

You should receive the message, *all authentication tokens updated successfully*.

9. Type the following to give vader a password. Type **dad** twice for the password:
   [root@rhel ~]# **passwd vader**

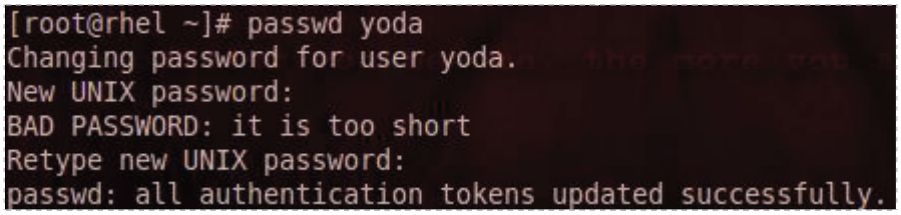


```
[root@rhel ~]# passwd vader
Changing password for user vader.
New UNIX password:
BAD PASSWORD: it is WAY too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Figure 35: Giving the user a Password

You should receive the message, *all authentication tokens updated successfully*.

10. Type the following to give yoda a password. Type **green** twice for the password:
    [root@rhel ~]# **passwd yoda**



```
[root@rhel ~]# passwd yoda
Changing password for user yoda.
New UNIX password:
BAD PASSWORD: it is too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

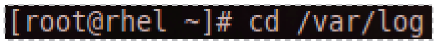
Figure 36: Giving the user a Password

You should receive the message, *all authentication tokens updated successfully*.

When you perform administrative tasks that are directly related to the security on a Linux system, they will show up in the secure log in the */var/log* directory. Examples of security incidents that will be recorded to the secure log include the following:

- Adding a user
- Logging on from a remote system
- Adding a group
- Changing a user’s password.

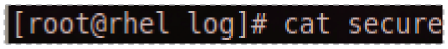
11. To view the secure log, type the following command on the Red Hat system:
    [root@rhel ~]# **cd /var/log/**



```
[root@rhel ~]# cd /var/log
```

Figure 37: Switching to the Directory where the secure log is located

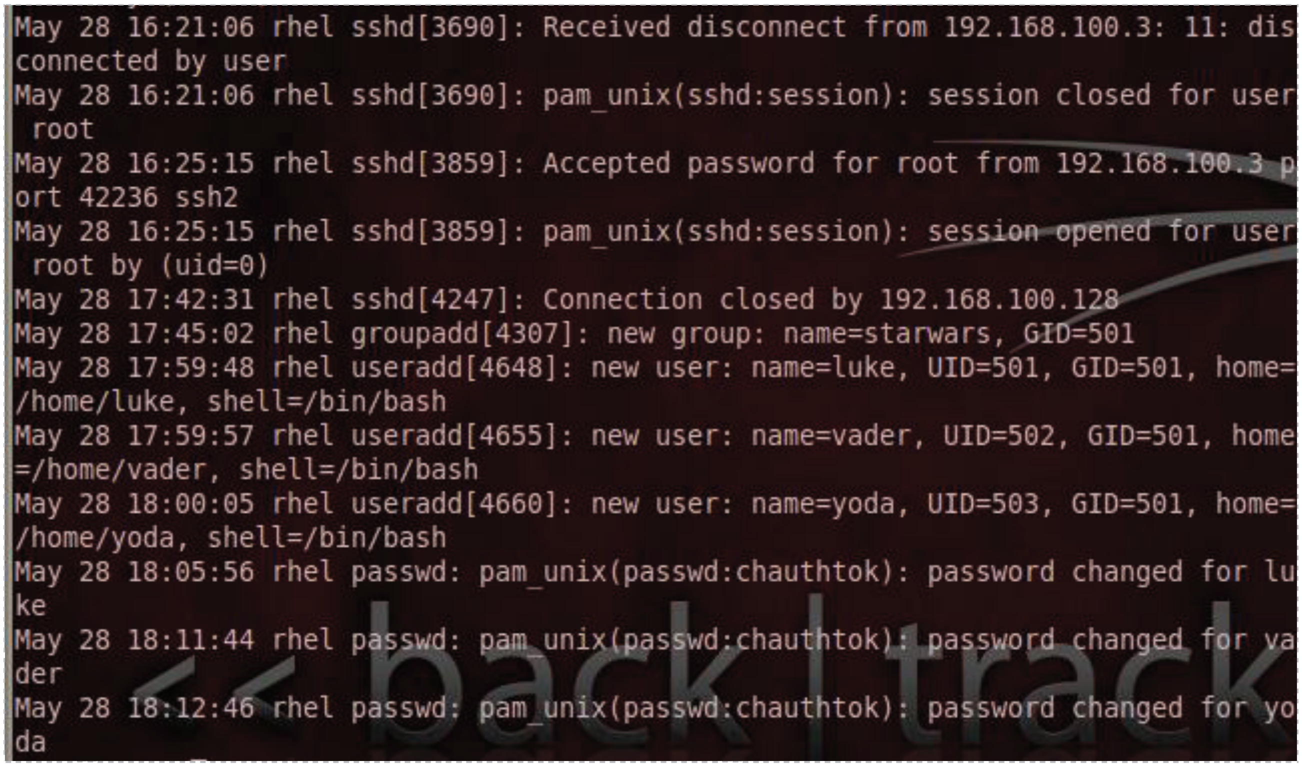
12. To view the connections in the log file, type the following command:
    [root@rhel log]# **cat secure**



```
[root@rhel log]# cat secure
```

Figure 38: Using the cat command to view the secure log

The results will appear similar to the results shown in the picture below.

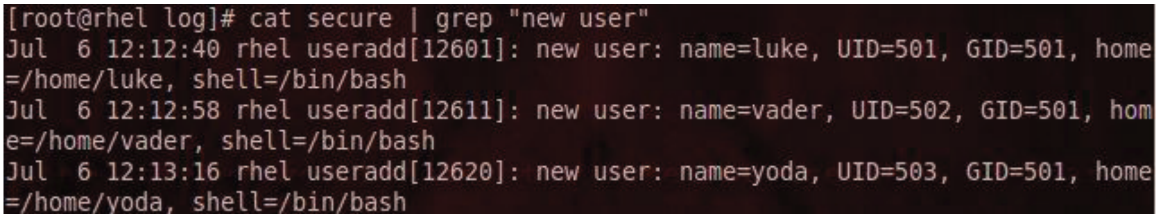


```
May 28 16:21:06 rhel sshd[3690]: Received disconnect from 192.168.100.3: 11: dis
connected by user
May 28 16:21:06 rhel sshd[3690]: pam_unix(sshd:session): session closed for user
 root
May 28 16:25:15 rhel sshd[3859]: Accepted password for root from 192.168.100.3 p
ort 42236 ssh2
May 28 16:25:15 rhel sshd[3859]: pam_unix(sshd:session): session opened for user
 root by (uid=0)
May 28 17:42:31 rhel sshd[4247]: Connection closed by 192.168.100.128
May 28 17:45:02 rhel groupadd[4307]: new group: name=starwars, GID=501
May 28 17:59:48 rhel useradd[4648]: new user: name=luke, UID=501, GID=501, home=
/home/luke, shell=/bin/bash
May 28 17:59:57 rhel useradd[4655]: new user: name=vader, UID=502, GID=501, home
=/home/vader, shell=/bin/bash
May 28 18:00:05 rhel useradd[4660]: new user: name=yoda, UID=503, GID=501, home=
/home/yoda, shell=/bin/bash
May 28 18:05:56 rhel passwd: pam_unix(passwd:chauthtok): password changed for lu
ke
May 28 18:11:44 rhel passwd: pam_unix(passwd:chauthtok): password changed for va
der
May 28 18:12:46 rhel passwd: pam_unix(passwd:chauthtok): password changed for yo
da
```

Figure 39: The secure file on the Victim

Notice the file has information about new users and a new group created on the system, password changes, and contains information about incoming SSH connections.

13. Search for the instances of new user creation in secure by typing the following:
    [root@rhel log]# **cat secure | grep "new user"**



```
[root@rhel log]# cat secure | grep "new user"
Jul  6 12:12:40 rhel useradd[12601]: new user: name=luke, UID=501, GID=501, home
=/home/luke, shell=/bin/bash
Jul  6 12:12:58 rhel useradd[12611]: new user: name=vader, UID=502, GID=501, hom
e=/home/vader, shell=/bin/bash
Jul  6 12:13:16 rhel useradd[12620]: new user: name=yoda, UID=503, GID=501, home
=/home/yoda, shell=/bin/bash
```

Figure 40: GREPing for the new user events in the secure file.

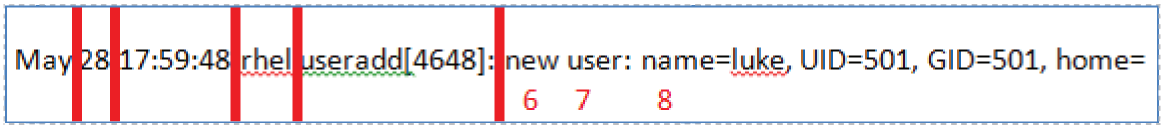
When **gawk** is used, the default field separator is a space. With the following command, everything to the right of the first space will be printed.

gawk '{print $1}' secure

In this case, it would be the word May because that word is to the left of the first space.

May 28 17:59:48 rhel useradd[4648]: new user: name=luke, UID=501, GID=501, home=

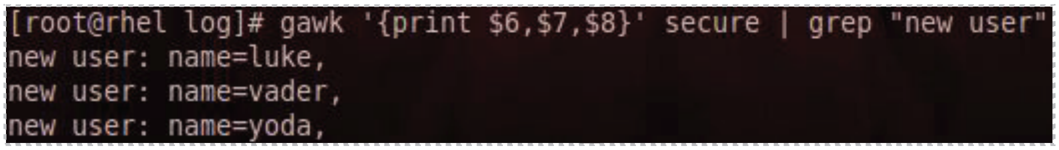
To determine users created, use gawk to print values to the left of 6th, 7th, and 8th space.



```
May 28 17:59:48 rhel useradd[4648]: new user: name=luke, UID=501, GID=501, home=
```

Figure 41: The Space as a Filed Separator

14. To determine the name of the new user created, we can use **grep** and **gawk**:
    [root@rhel log]# **gawk '{print $6,$7,$8}' secure | grep "new user"**



```
[root@rhel log]# gawk '{print $6,$7,$8}' secure | grep "new user"
new user: name=luke,
new user: name=vader,
new user: name=yoda,
```

Figure 42: Using the GAWK command

Task 2.2 Conclusion

The secure file in the /var/log directory will alert you to events related directly to the security on a Linux system, including account and password changes. The gawk command allows you to send specific output to the screen. The default delimiter for gawk is a space. As the secure log on a Linux system can become quite lengthy, the use of grep in conjunction with the gawk command will allow you to parse for certain events.

Task 2.3 Discussion Questions

1. What are the results from typing the following command?
   gawk –F= '{print $2}' /var/log/secure

2. What are the results from typing the following command?
   gawk '{print $2}' /var/log/secure

3. What are the results from typing the following command?
   gawk –F= '{print $1}' /var/log/secure

4. What are the results from typing the following command?
   gawk '{print $1}' /var/log/secure

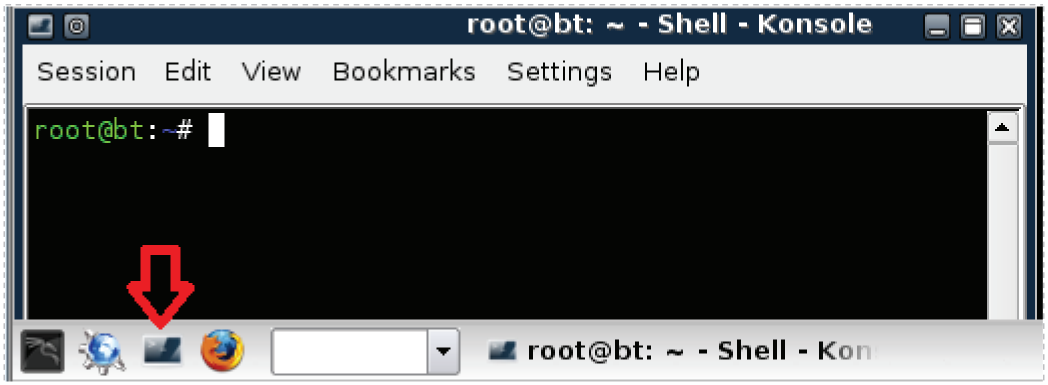
Task 3 Log Analysis in Windows Using find

Windows also has many logs, including the IIS, or Internet Information Services logs, which are text based logs. Neither gawk nor grep are part of Windows, although you can download third party versions. Windows has find, which will perform similar functions.

Task 3.1 Using find in Windows

Open a Terminal to Get Started

1. Open a terminal on the BackTrack 4 External Attack system by clicking the picture to the left of Firefox in the task bar, located at the bottom of the screen.

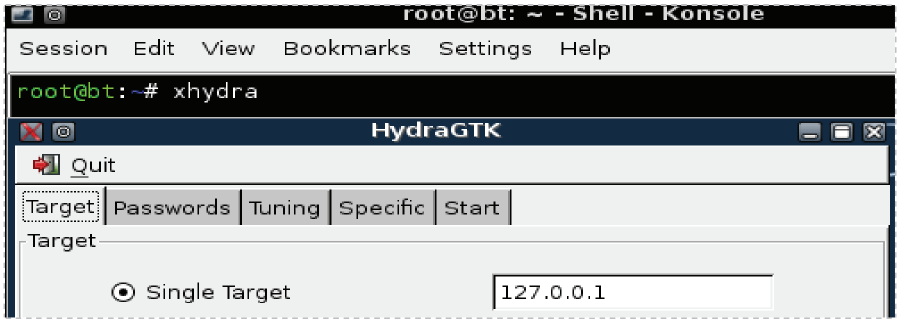

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt: ~ - Shell - Kon

```
root@bt:~#
```

Figure 43: The Terminal Windows within BackTrack

The **xHydra** tool included with BackTrack will allow you to perform a dictionary attack against a remote system. We will be performing a dictionary attack on the FTP server with xHydra in order to generate a large amount of entries into the FTP log files.

2. Type the following command to launch the **xHydra** program on BackTrack 4 system:
   root@bt:~#**xhydra**

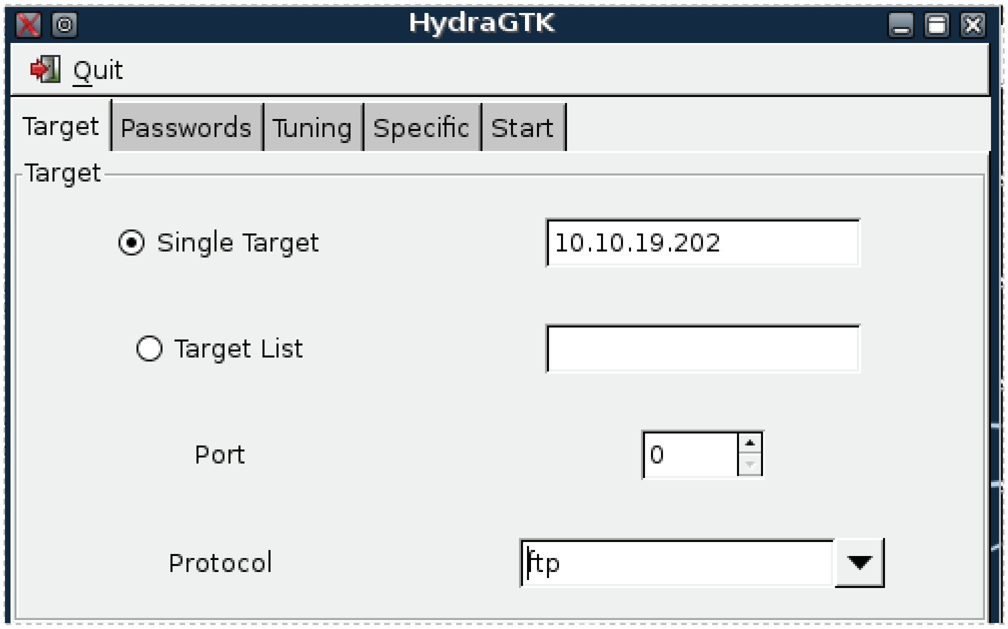

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
HydraGTK
Quit
Target
Passwords
Tuning
Specific
Start
Target

```
root@bt:~# xhydra
```

● Single Target 127.0.0.1

Figure 44: xHydra can be launched by typing the xhydra command within the Terminal

3. On the Target Tab, type **10.10.19.202**. Select **ftp** for the protocol.



Target

● Single Target 10.10.19.202

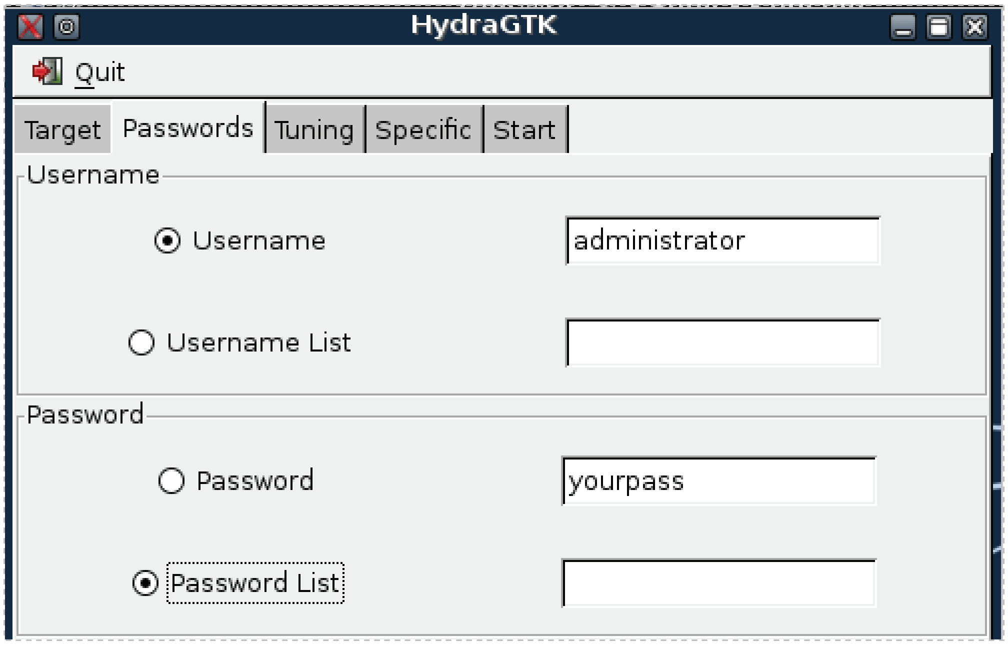
○ Target List

Port 0

Protocol ftp

Figure 38: The Target Tab of xHydra

4. Click on the **Passwords** tab. Type **administrator** for the username. Under the password category, click on the **Password List** button.



Username

● Username administrator

○ Username List

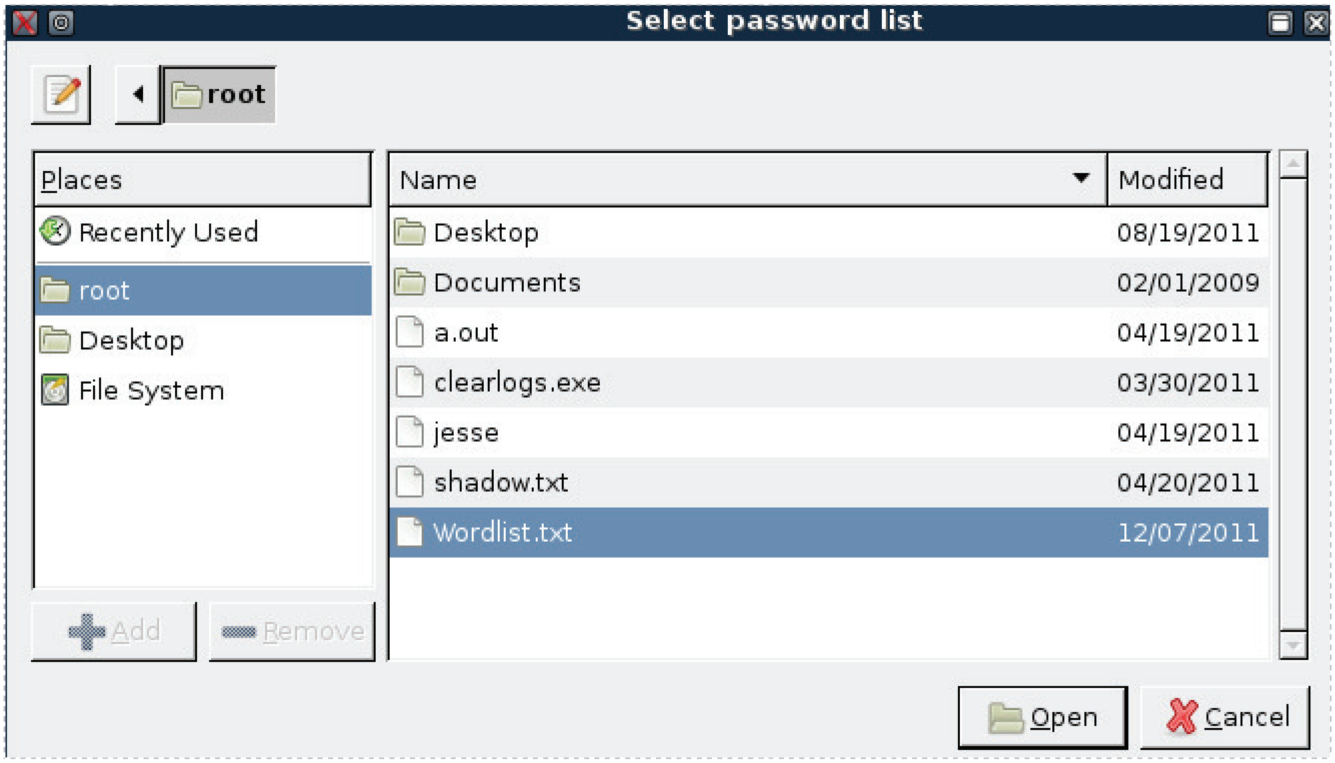
Password

○ Password yourpass

● Password List

Figure 45: The Passwords Tab of xHydra

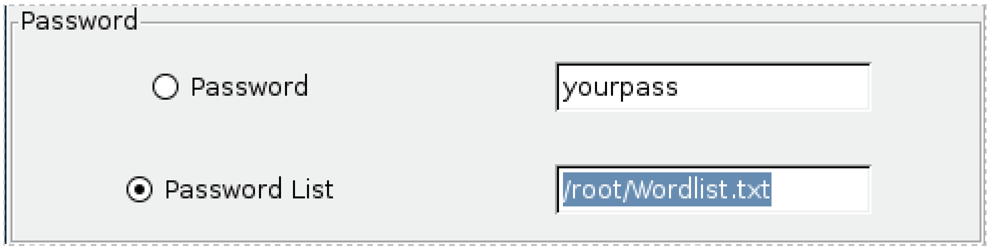
5. Click in the white space to the left of the words **Password List** in xHydra. Click the root directory, the click on **Wordlist.txt** and click the **Open** button.



Name	Modified
Desktop	08/19/2011
Documents	02/01/2009
a.out	04/19/2011
clearlogs.exe	03/30/2011
jesse	04/19/2011
shadow.txt	04/20/2011
Wordlist.txt	12/07/2011

Figure 46: Selecting the Password File

/root/Wordlist.txt should now be listed in the Password List box.

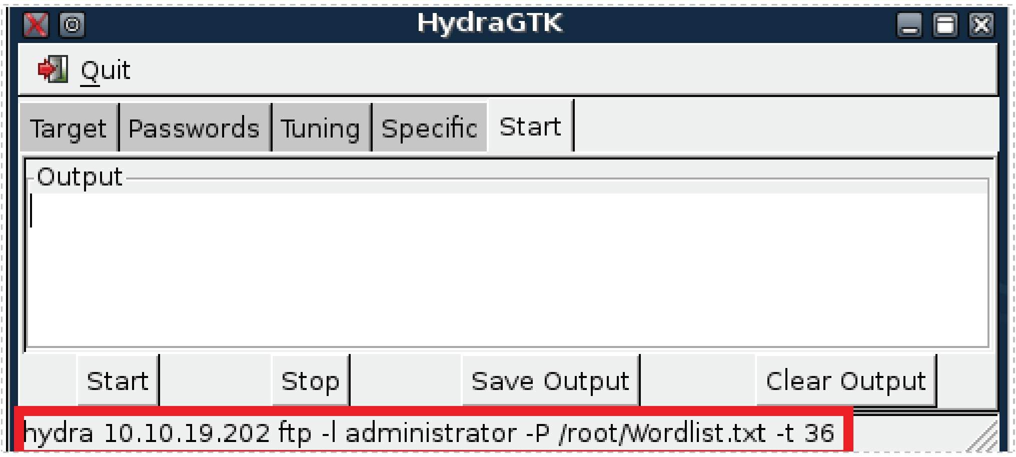


○ Password yourpass

● Password List /root/Wordlist.txt

Figure 47: The Password List

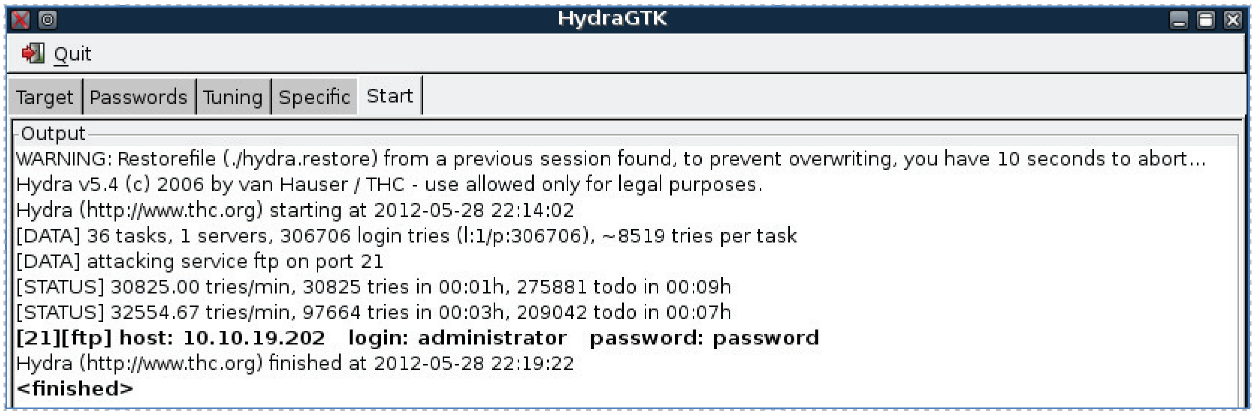
6. Click on the **Start** tab. At the bottom of the screen, verify that your xHydra program displays the options as shown in the picture below.



```
hydra 10.10.19.202 ftp -l administrator -P /root/Wordlist.txt -t 36
```

Figure 48: Verifying xHydra Options

7. Click **Start**. It will take about 10-20 minutes to crack the administrator password.



```
WARNING: Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2012-05-28 22:14:02
[DATA] 36 tasks, 1 servers, 306706 login tries (l:1/p:306706), ~8519 tries per task
[DATA] attacking service ftp on port 21
[STATUS] 30825.00 tries/min, 30825 tries in 00:01h, 275881 todo in 00:09h
[STATUS] 32554.67 tries/min, 97664 tries in 00:03h, 209042 todo in 00:07h
[21][ftp] host: 10.10.19.202   login: administrator   password: password
Hydra (http://www.thc.org) finished at 2012-05-28 22:19:22
<finished>
```

Figure 49: The password is cracked

8. Log on to the Microsoft Windows 2003 Server by clicking the **Send Ctrl-Alt-Del** link in the bottom right hand corner of the browser window. Log on to the 2003 server with the username of **Administrator** and the password of **password**.

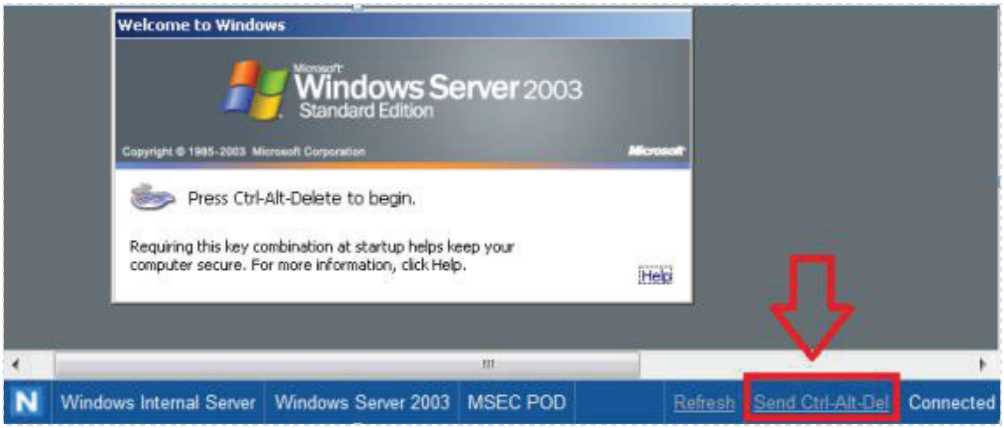

Welcome to Windows
Microsoft Windows Server 2003 Standard Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
Press Ctrl-Alt-Delete to begin.
Requiring this key combination at startup helps keep your computer secure. For more information, click Help.
Help
N
Windows Internal Server
Windows Server 2003
MSEC POD
Refresh
Send Ctrl-Alt-Del
Connected

Figure 50: Send Ctrl-Alt-Del to the Windows 2003 Server

9. On the Windows 2k3 Server Victim Machine, open a command prompt by clicking on the Command Prompt Shortcut located on the administrator's desktop.

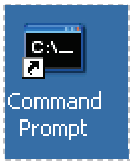
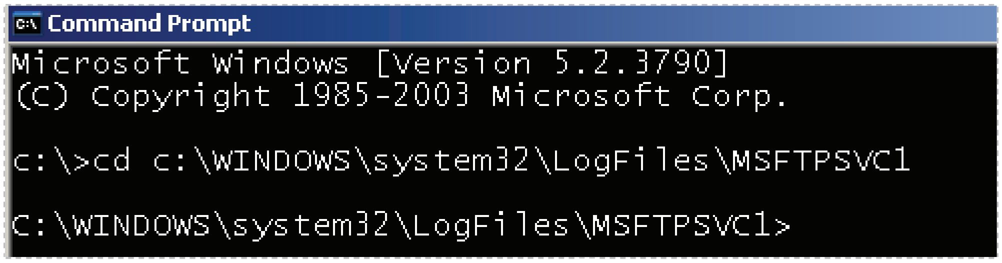


Figure 51: Opening a Command Prompt

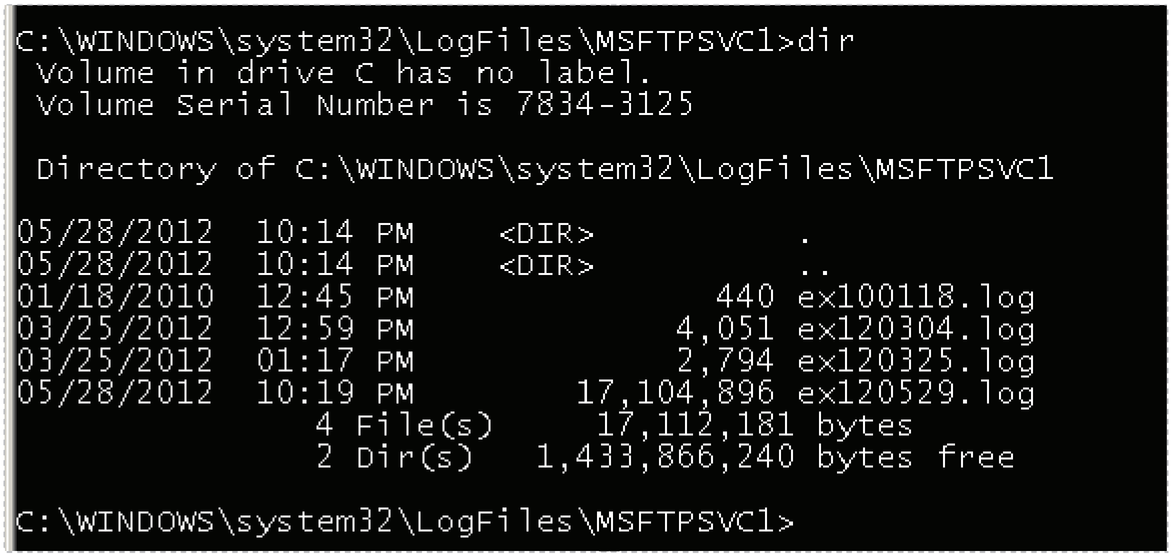
10. Navigate to the FTP Logfiles directory by typing the following command: C:\cd c:\Windows\System32\Logfiles\msftpsvc1



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\>cd c:\WINDOWS\system32\LogFiles\MSFTPSVC1

C:\WINDOWS\system32\LogFiles\MSFTPSVC1>
```

Figure 52: Navigating to the FTP Log files Directory

11. Type the following command to view all of the files in the directory:
    C:\WINDOWS\system32\LogFiles\MSFTPSVC1>**dir**



```
C:\WINDOWS\system32\LogFiles\MSFTPSVC1>dir
 Volume in drive C has no label.
 Volume Serial Number is 7834-3125

 Directory of C:\WINDOWS\system32\LogFiles\MSFTPSVC1

05/28/2012  10:14 PM    <DIR>          .
05/28/2012  10:14 PM    <DIR>          ..
01/18/2010  12:45 PM               440 ex100118.log
03/25/2012  12:59 PM             4,051 ex120304.log
03/25/2012  01:17 PM             2,794 ex120325.log
05/28/2012  10:19 PM        17,104,896 ex120529.log
               4 File(s)     17,112,181 bytes
               2 Dir(s)   1,433,866,240 bytes free

C:\WINDOWS\system32\LogFiles\MSFTPSVC1>
```

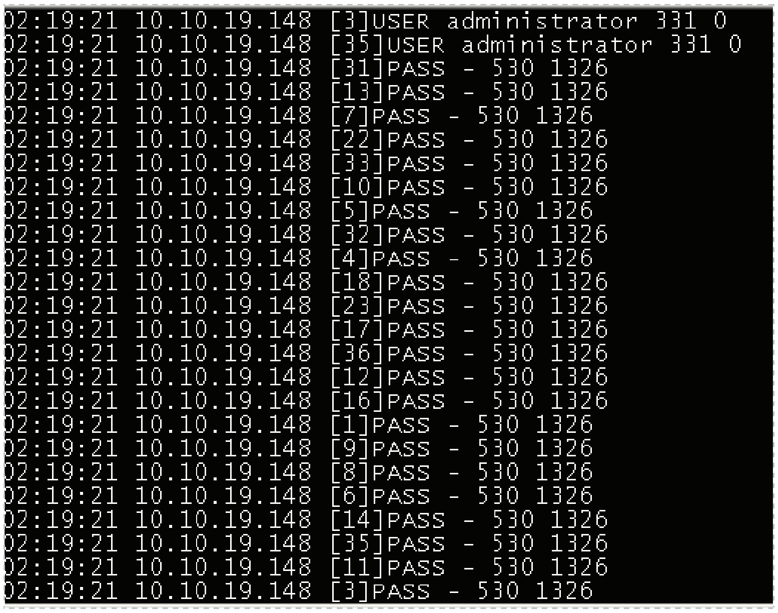
Figure 53: The FTP Log files

Notice how large today's log file is, because of the Hydra Dictionary attack.

12. Type the following command to view the contents of the file:
    C:\WINDOWS\system32\LogFiles\MSFTPSVC1>**type ex<todays date>.log**

Use the file with today's date. The format for the log files is year, month, day.

The results will appear similar to that of the results in the picture below.



```
02:19:21 10.10.19.148 [3]USER administrator 331 0
02:19:21 10.10.19.148 [35]USER administrator 331 0
02:19:21 10.10.19.148 [31]PASS - 530 1326
02:19:21 10.10.19.148 [13]PASS - 530 1326
02:19:21 10.10.19.148 [7]PASS - 530 1326
02:19:21 10.10.19.148 [22]PASS - 530 1326
02:19:21 10.10.19.148 [33]PASS - 530 1326
02:19:21 10.10.19.148 [10]PASS - 530 1326
02:19:21 10.10.19.148 [5]PASS - 530 1326
02:19:21 10.10.19.148 [32]PASS - 530 1326
02:19:21 10.10.19.148 [4]PASS - 530 1326
02:19:21 10.10.19.148 [18]PASS - 530 1326
02:19:21 10.10.19.148 [23]PASS - 530 1326
02:19:21 10.10.19.148 [17]PASS - 530 1326
02:19:21 10.10.19.148 [36]PASS - 530 1326
02:19:21 10.10.19.148 [12]PASS - 530 1326
02:19:21 10.10.19.148 [16]PASS - 530 1326
02:19:21 10.10.19.148 [1]PASS - 530 1326
02:19:21 10.10.19.148 [9]PASS - 530 1326
02:19:21 10.10.19.148 [8]PASS - 530 1326
02:19:21 10.10.19.148 [6]PASS - 530 1326
02:19:21 10.10.19.148 [14]PASS - 530 1326
02:19:21 10.10.19.148 [35]PASS - 530 1326
02:19:21 10.10.19.148 [11]PASS - 530 1326
02:19:21 10.10.19.148 [3]PASS - 530 1326
```

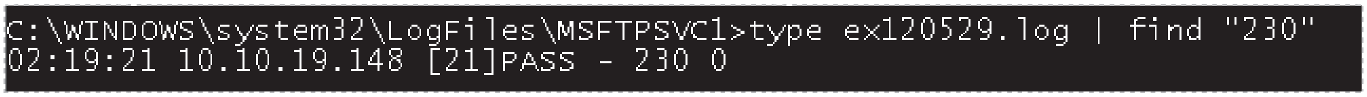
Figure 54: Today's FTP Log File

An incorrect password results in a 530 message. A 230 means the password was correct.

We can now use the find command to see if the user logged in successfully.

13. Type the following command to see if the attacker's login was successful:
    C:\WINDOWS\system32\LogFiles\MSFTPSVC1> **type ex<today's date>.log | find "230"**

Use the file with today's date. The format for the log files is year, month, day.



```
C:\WINDOWS\system32\LogFiles\MSFTPSVC1>type ex120529.log | find "230"
02:19:21 10.10.19.148 [21]PASS - 230 0
```

Figure 55: Today's FTP Log File

We now know the date and time that the hacker successfully logged into the victim system.

14. Close all open windows and terminals.

Task 3.2 Conclusion

The xHydra program allows an attacker to perform a dictionary attack against a variety of protocols, including FTP, File Transfer Protocol. A Windows system keeps logs of connection attempts in the C:\WINDOWS\system32\LogFiles\MSFTPSVC1 directory. These logfiles can be extremely long, so a user can use the find command to parse them.

Task 3.3 Discussion Questions

1. What is xHydra?
2. Where are FTP Log files stored in Windows?
3. What is the code for a successful FTP login?
4. How can the find command be used to locate the number 230 within a logfile?

5 References

1. GREP man Pages:
   http://unixhelp.ed.ac.uk/CGI/man-cgi?grep

2. Understanding /etc/shadow file The GNU Awk User's Guide:
   http://www.gnu.org/software/gawk/manual/gawk.html

3. Windows Find Command:
   http://www.computerhope.com/findhlp.htm

4. Files and Linux:
   http://www.irongeek.com/i.php?page=security/linuxlogs1

5. THC-Hydra:
   http://www.thc.org/thc-hydra/

CompTIA Security+® Lab Series

Lab 3: Protocols and Default Network Ports - Transferring Data Using TCP/IP

CompTIA Security+® Domain 1 - Network Security

Objective 1.4: Implement and use common protocols
Objective 1.5: Identify commonly used default network ports

Document Version: 2012-08-15 (Beta)

Lab Author: Jesse Varsalone
Assistant Professor
Cyber Security
Organization: Community College of Baltimore County

The development of this document is funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) is an entity of Moraine Valley Community College.

Contents

1 Introduction ... 3
2 Objectives: Implement and Use Common Protocols ... 3
Identify Commonly Used Default Network Ports ... 3
3 Pod Topology ... 5
4 Lab Settings ... 6
Task 1 Using Hyper Text Transfer Protocol (HTTP) to Transfer Files ... 8
Task 1.1 Transferring Files with HTTP ... 8
Task 1.2 Conclusion ... 15
Task 1.3 Discussion Questions ... 15
Task 2 Using File Transfer Protocol (FTP) to Transfer Files ... 16
Task 2.1 Using FTP ... 16
Task 2.2 Conclusion ... 23
Task 2.3 Discussion Questions ... 23
Task 3 Transferring Files Securely Using SCP ... 24
Task 3.1 Using SCP ... 24
Task 3.2 Conclusion ... 25
Task 3.3 Discussion Questions ... 25
5 References ... 26

1 Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will be able to transfer files using the FTP, HTTP, and SCP protocols. Protocols like HTTP, FTP, and SCP can be used to transfer files from one computer to another. File transfers are unencrypted by default when the FTP or HTTP protocols are used. File transfers will be encrypted if SCP is used. In this lab, the student will have the opportunity to configure servers and utilize file transfer client utilities.

This lab includes the following tasks:

- Task 1 - Using Hyper Text Transfer Protocol (HTTP) to transfer files
- Task 2 - Using File Transfer Protocol (FTP) to transfer files
- Task 3 - Transferring Files Securely Using SCP

2 Objectives: Implement and Use Common Protocols Identify Commonly Used Default Network Ports

It is important to know how files can be uploaded, downloaded, and securely transferred using protocols within the TCP/IP suite. Windows, Linux, UNIX, and the Mac OS X operating systems can be used as HTTP, FTP, and SSH servers. Some of the operating systems have the ability to run these servers without needing any third party applications. Windows comes with FTP and HTTP clients, while Linux, UNIX, and Mac OS come with clients for HTTP, FTP, and SCP. The third party application pscp.exe can be used on the Windows operating systems to perform secure file copies.

For this lab, the following terms and concepts will be of use:

FTP [1] – File Transfer Protocol, or FTP, can be used to transfer files from one computer to another. The FTP protocol uses the Transmission Control Protocol (TCP) and two ports, 20 and 21. Port 21 is used for the commands and port 20 is used for the data transfer. Credential and files that are transferred using FTP are sent in clear text.

HTTP – Hyper Text Transfer Protocol, or HTTP, can be used to download files. The HTTP protocol uses the Transmission Control Protocol (TCP) and port 80. HTTP clients include browsers and wget.exe. Web Server software includes Microsoft's Internet Information Services (IIS) and Apache. This is web server software, commonly used on Linux machines. However, Apache can be utilized on Windows, Mac OS X, and UNIX.

SCP [2] – The Secure Copy Protocol, or SCP, can be used encrypt file transmissions. In order to use the SCP protocol, the destination server must be running the SSH protocol. The SSH protocol uses the Transmission Control Protocol (TCP) and port 22. Credential and files that are transferred using SCP are encrypted.

IIS [3] – Microsoft's Internet Information Services, or IIS, is available on their server and some of their client operating systems. The administrator can configure various servers within IIS, such as FTP and HTTP servers. When IIS was first introduced there were many vulnerabilities. However, Microsoft has improved the security of IIS over the years.

Apache [4] – This is web server software, commonly used on Linux machines. However, Apache can be utilized on Windows, Mac OS X, and UNIX. The name Apache came from the Native American tribe and the software can be used to host a website.

3 Pod Topology

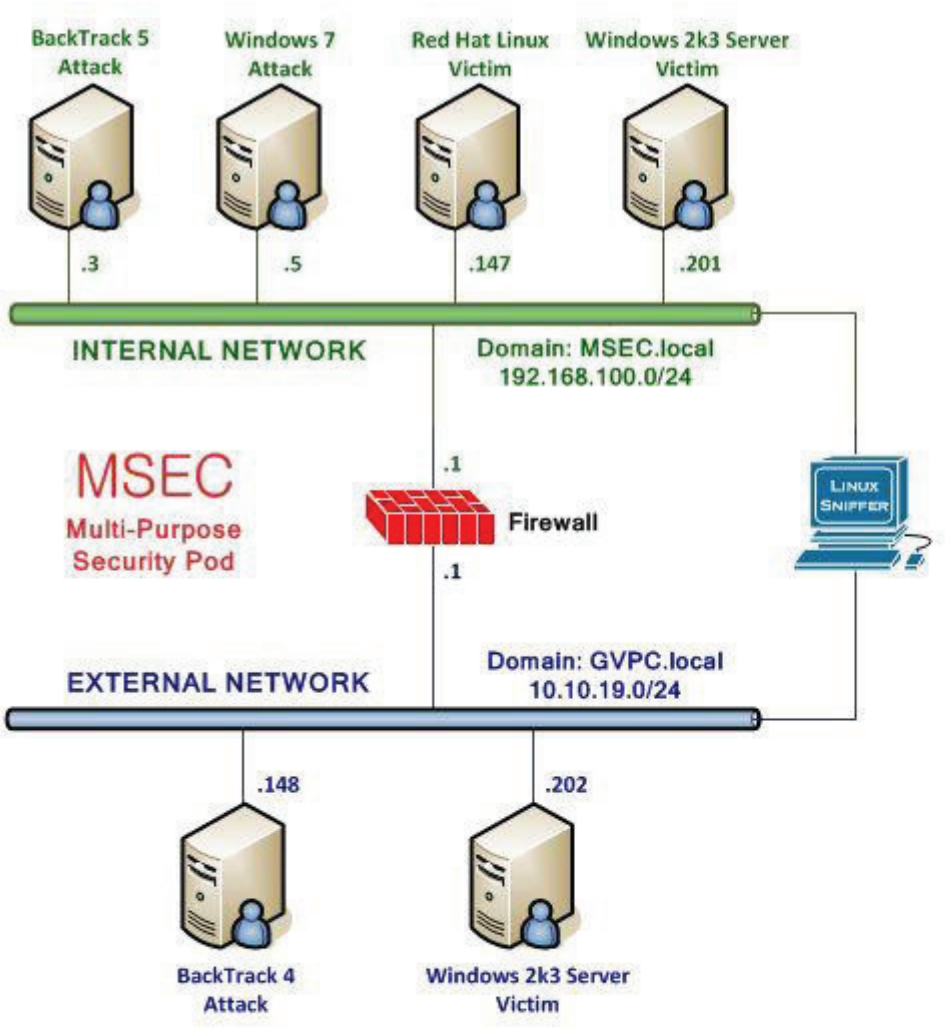


Figure 1: MSEC Network Topology

4 Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

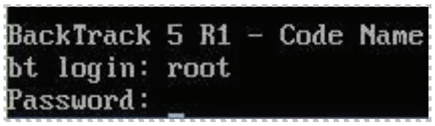
Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

BackTrack 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password
RHEL 9 Internal Victim Machine	192.168.100.147
RHEL 9 root password	password
Windows 2k3 Server Internal Victim Machine	192.168.100.201
Windows 2k3 Server administrator password	password

BackTrack 5 Login:

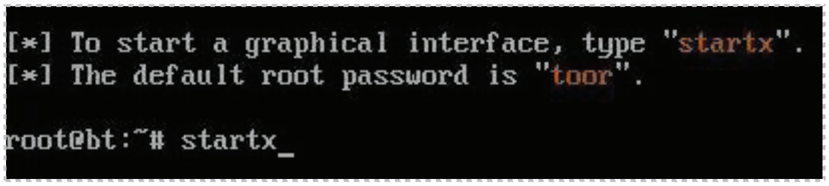
1. Click on the BackTrack 5 icon on the topology.
2. Type **root** at the **bt login:** username prompt.
3. Type **password** at the Password: prompt.



```
BackTrack 5 R1 - Code Name
bt login: root
Password: _
```

Figure 2: BackTrack 5 login

4. To start the GUI, type **startx** at the root@bt:~# prompt.



```
[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".

root@bt:~# startx_
```

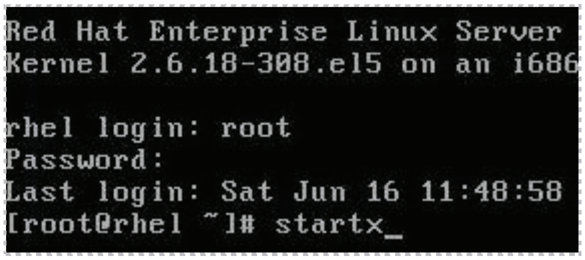
Figure 3: BackTrack 5 GUI start up

Red Hat Enterprise Linux Login:

1. Click on the Red Hat Linux icon on the topology.
2. Type **root** at the rhel login: prompt.
3. Type **password** at the Password: prompt.

For security purposes, the password will not be displayed.

4. To start the GUI, type **startx** at the [root@rhe ~]# prompt.

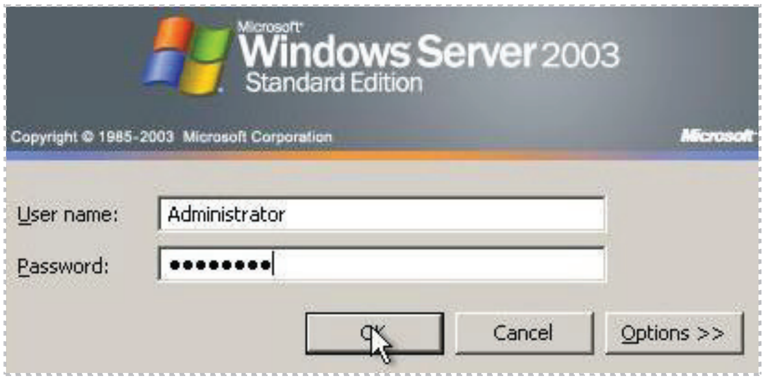


```
Red Hat Enterprise Linux Server
Kernel 2.6.18-308.el5 on an i686

rhel login: root
Password:
Last login: Sat Jun 16 11:48:58
[root@rhel ~]# startx
```

Figure 4: RHEL login

Windows 2003 Server Login:

1. Click on the Windows 2k3 Server icon on the topology (these instructions will work for both internal and external victim machines).
2. Enter the User name, **Administrator** (verify the username with your instructor).
3. Type in the password: **password** and click the **OK** button (verify the password with your instructor).



User name: Administrator

Password: ••••••••

Figure 5: Windows 2k3 login

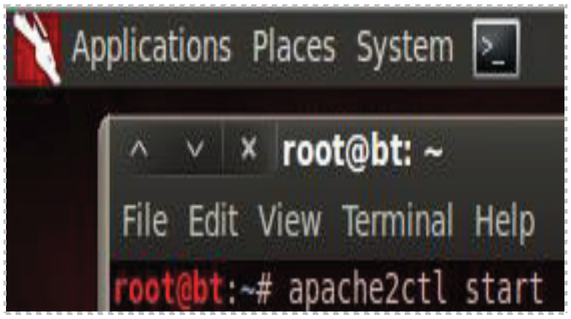
Task 1 Using Hyper Text Transfer Protocol (HTTP) to Transfer Files

Most people are familiar with the process of how to download a file from a web server. However, people who don't do network administration might not know how to configure a HTTP server. In this exercise, you will configure an Apache server on a Linux machine so that a client can download files to their machine. Apache is web server software which runs on a variety of operating systems. A version of Apache is included with BackTrack so the machine can perform web server functions.

Task 1.1 Transferring Files with HTTP

Start the Apache Server on the Attack machine

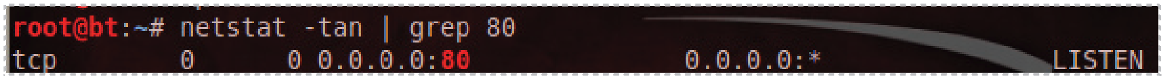
1. Open a terminal on the in BackTrack 5 Internal Attack system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen. Start the Apache server by typing the following command at the terminal: root@bt:~#**apache2ctl start**



```
root@bt:~# apache2ctl start
```

Figure 6: Starting Apache

2. To verify that the Apache server is listening on port 80, type the following: root@bt:~#**netstat –tan | grep 80**

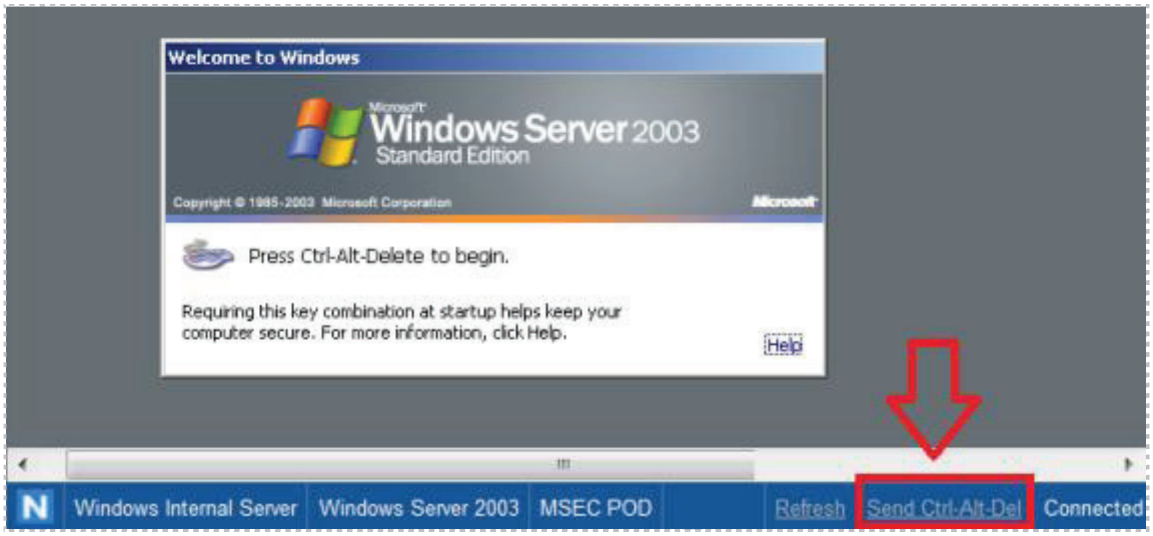


```
root@bt:~# netstat -tan | grep 80
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
```

Figure 7: Verifying that the Apache Web Server is Running

To test that the web server is functioning with a valid home page, you can attempt to connect to it from the Windows 7 machine by connecting to it from your browser.

3. Log on to the Microsoft Windows 2003 Server by clicking the **Send Ctrl-Alt-Del** link in the bottom right hand corner of the browser window. Log on to the 2003 server with the username of **Administrator** and the password of **password**.



Welcome to Windows

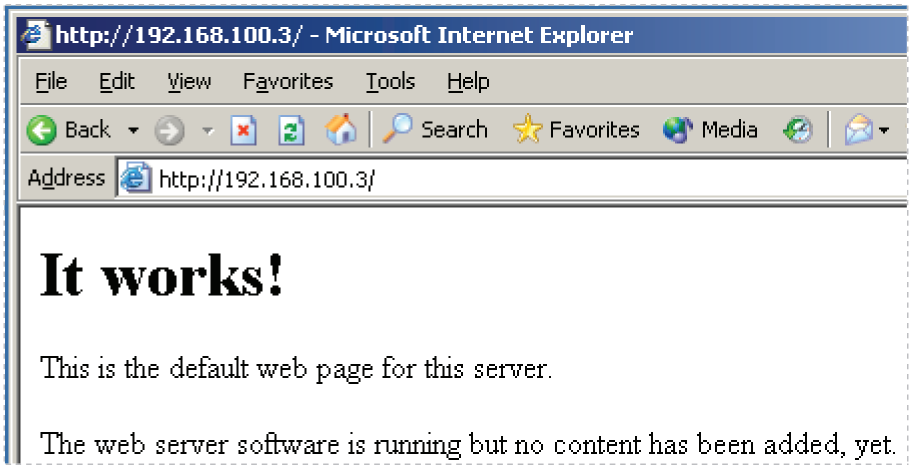
Copyright © 1985-2003 Microsoft Corporation

Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Figure 8: Logging on to Windows 2003

4. On the Windows 2003 machine, open Internet Explorer , by clicking on the shortcut to Internet Explorer on the desktop, and type the following URL: http://192.168.100.3 - You should see the message, *It works!,* on the webpage.



http://192.168.100.3/ - Microsoft Internet Explorer

Address: http://192.168.100.3/

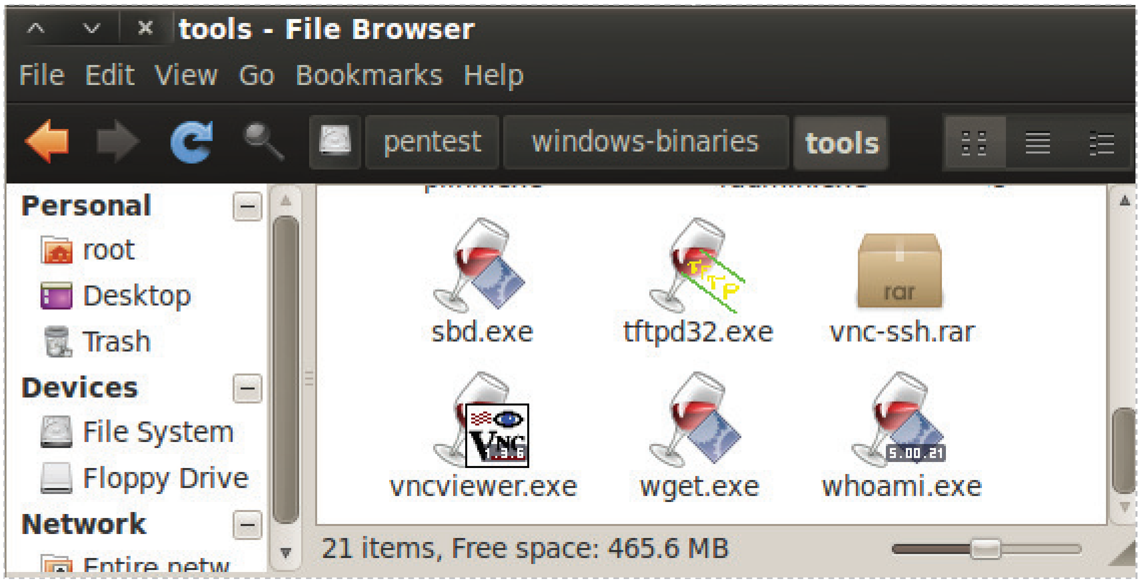
It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

Figure 9: Viewing the Default Web Page

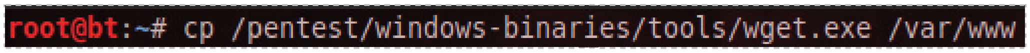
BackTrack comes with wget and several other Window's executables in the /pentest/windows-binaries directory. A binary file is an executable file.



21 items, Free space: 465.6 MB

Figure 10: Windows Binaries on the BackTrack Distribution

5. To copy **wget.exe** to the Apache directory, type the following at the terminal: root@bt:~#**cp /pentest/windows- binaries/tools/wget.exe /var/www**

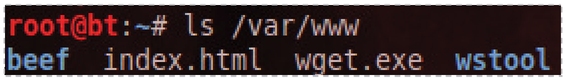


```
root@bt:~# cp /pentest/windows-binaries/tools/wget.exe /var/www
```

Figure 11: Copying wget.exe to the WWW Directory

You will not receive a message that the file was successfully copied over.

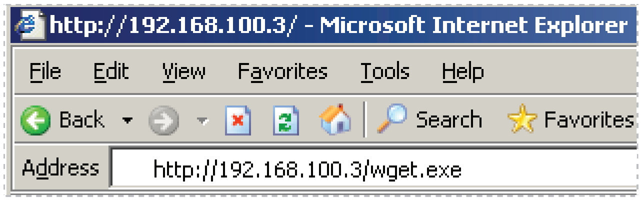
6. To verify that the file in present in the destination directory, type the following: root@bt:~#**ls /var/www**



```
root@bt:~# ls /var/www
beef  index.html  wget.exe  wstool
```

Figure 12: Contents of the WWW Directory

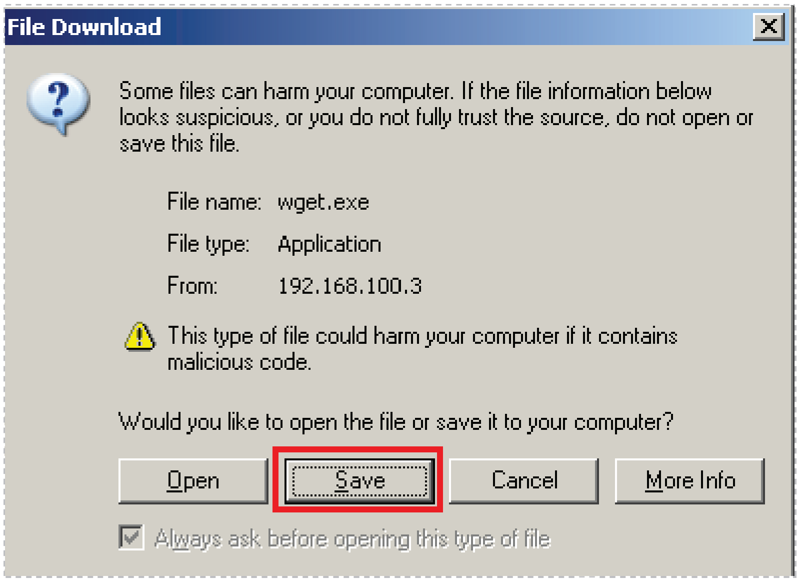
7. Download the wget file from the BackTrack Linux machine running Apache by typing the following URL in your browser: http://192.168.100.3/wget.exe


http://192.168.100.3/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites

Address http://192.168.100.3/wget.exe

Figure 13: The URL in the Browser

8. Click the **Save** button at the File Download Screen.



Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: wget.exe

File type: Application

From: 192.168.100.3

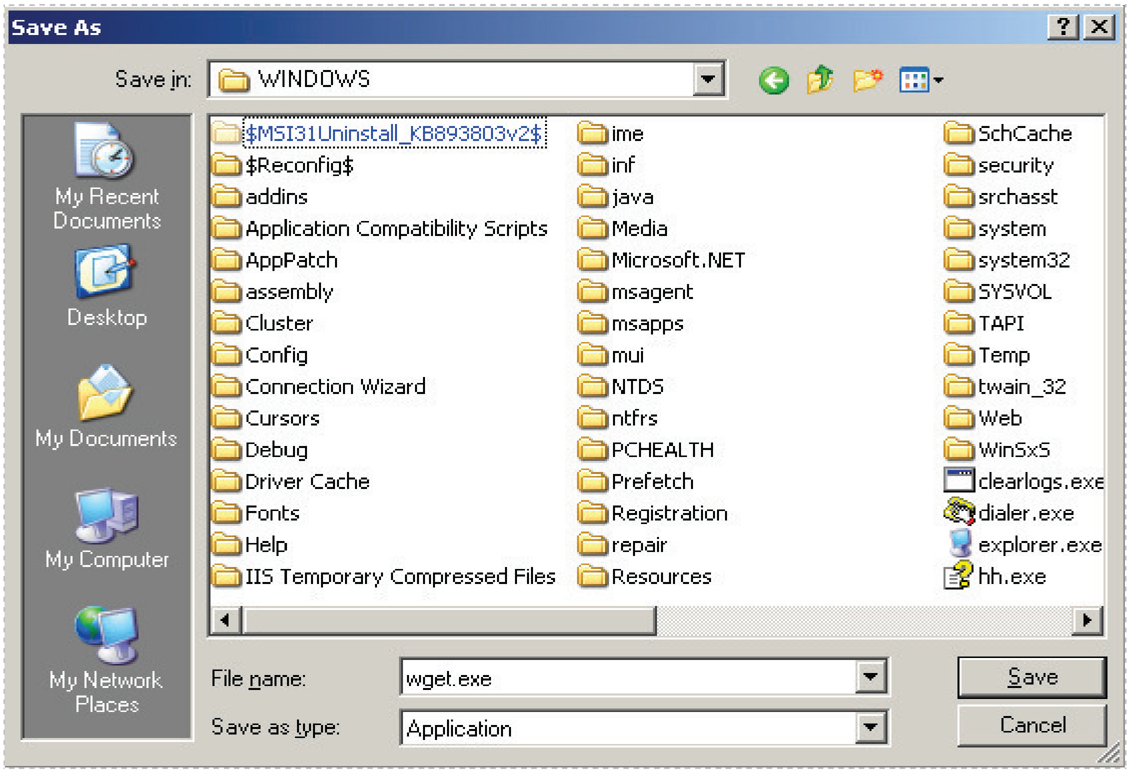
This type of file could harm your computer if it contains malicious code.

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

Figure 14: File Download Security Box

9. Click on **My Computer**, then **Local Disk (C:)**, and then select **Windows**. Click **Save**.



Save in: WINDOWS

File name: wget.exe

Save as type: Application

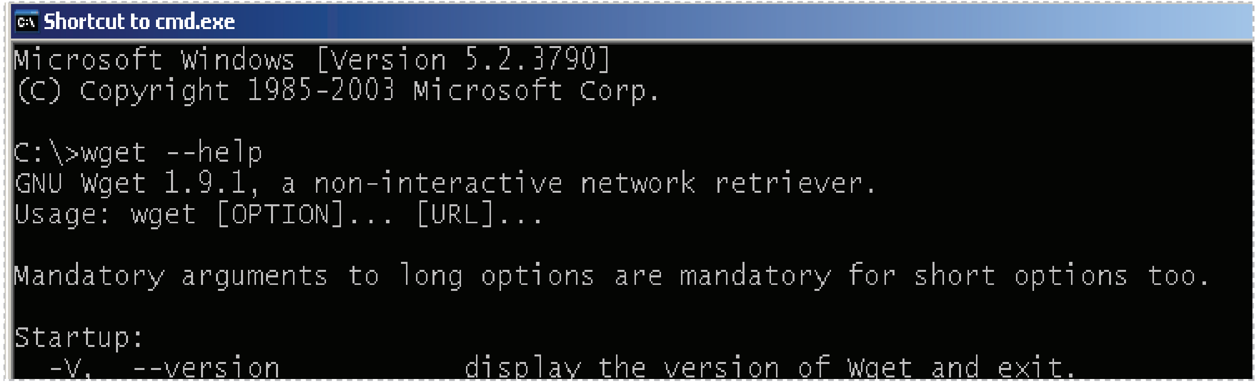
Figure 15: Downloading the Executable to the Windows Directory

Click **Close** to close the download complete dialog box. Downloading executables to the Windows or Windows\system32 directory is a good idea because that will place the executable in the path. If an executable is in the path, you will be able to type the command from any directory on the system.

10. Open a command prompt on the Windows 2003 machine by double clicking on the cmd.exe on the desktop.

Figure 16: Opening a Command Prompt on Windows 2003

11. Type the following command to verify that the wget file transferred correctly:
C:\wget --help

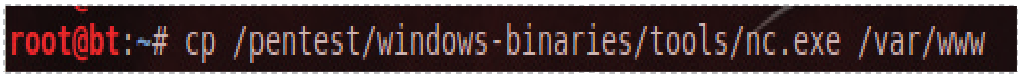


```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>wget --help
GNU Wget 1.9.1, a non-interactive network retriever.
Usage: wget [OPTION]... [URL]...

Mandatory arguments to long options are mandatory for short options too.

Startup:
  -V,  --version           display the version of Wget and exit.
```

Figure 17: Displaying the options for the wget command

Wget is a command line utility that allows you to download web pages and files.

12. To copy **netcat** to the Apache directory on the BackTrack 5 system, type the following at the terminal:
root@bt:~#**cp /pentest/windows-binaries/tools/nc.exe /var/www**

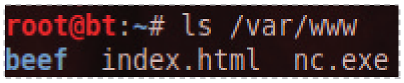


```
root@bt:~# cp /pentest/windows-binaries/tools/nc.exe /var/www
```

Figure 18: Copying Netcat to the WWW Directory

You will not receive a message that the file was successfully copied over.

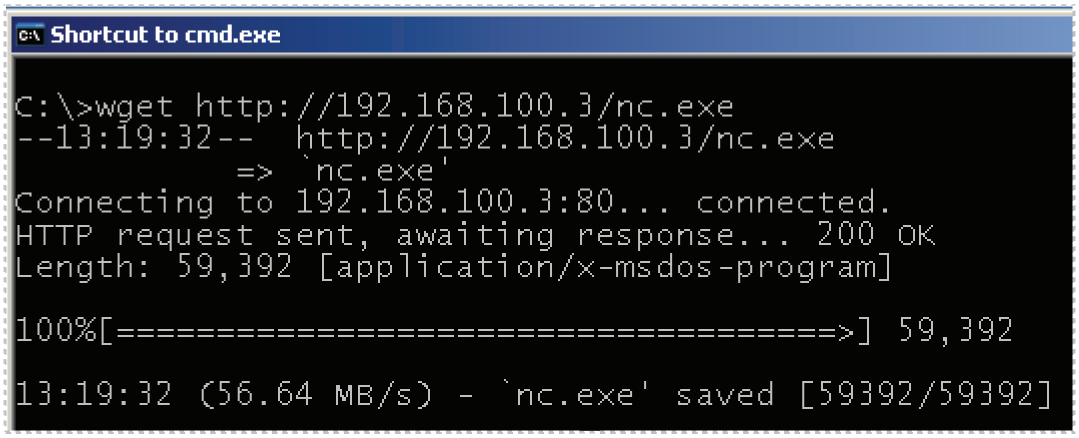
13. To verify that the file in present in the destination directory, type the following:
    root@bt:~#**ls /var/www**



```
root@bt:~# ls /var/www
beef  index.html  nc.exe
```

Figure 19: Verifying that Netcat is in the WWW Directory

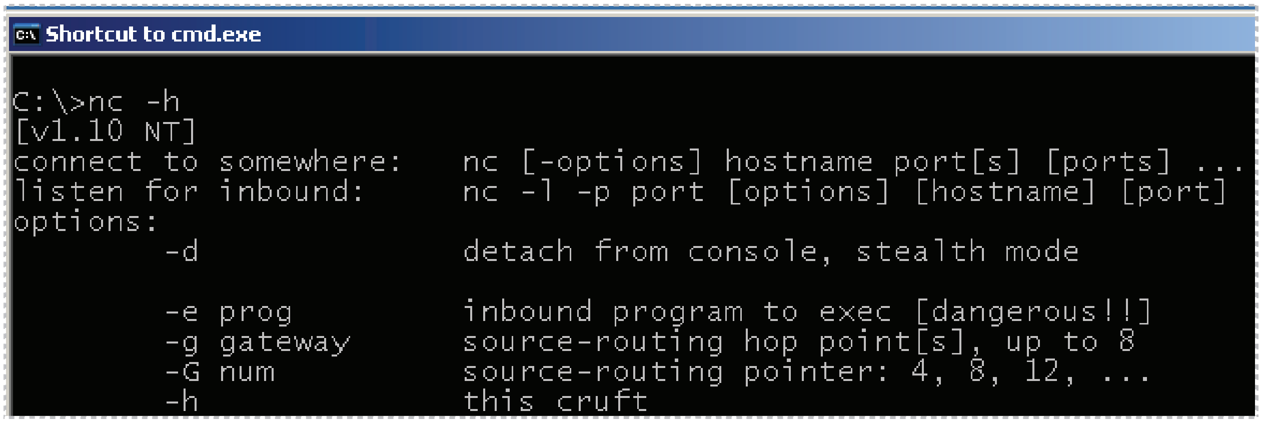
14. On the Windows 2003 system, type the following command to download **nc.exe**
    C:\wget http://192.168.100.3/nc.exe



```
C:\>wget http://192.168.100.3/nc.exe
--13:19:32--  http://192.168.100.3/nc.exe
           => `nc.exe'
Connecting to 192.168.100.3:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 59,392 [application/x-msdos-program]

100%[====================================>] 59,392

13:19:32 (56.64 MB/s) - `nc.exe' saved [59392/59392]
```

Figure 20: Starting a Netcat Listener on Port 443

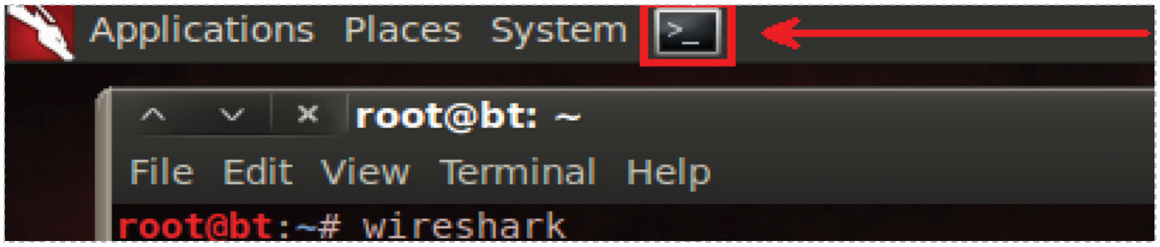
15. Type the following command to verify that the netcat file transferred correctly:
    C:\nc -h



```
C:\>nc -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth 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
```

Figure 21: Displaying the Options for the Netcat Command

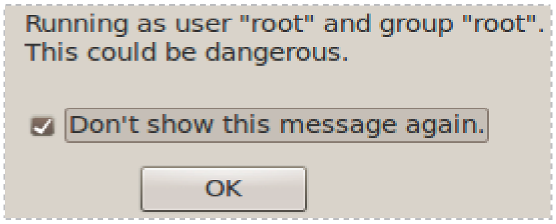
16. In the BackTrack 5 terminal, type **wireshark** (all lowercase) to bring up the wireshark program.



```
root@bt:~# wireshark
```

Figure 22: The Terminal Windows within BackTrack

17. Click the button that says **Don't show this message again**, and click **OK**.



Running as user "root" and group "root".
This could be dangerous.

☑ Don't show this message again.

Figure 23: Allow Wireshark to run as root

Wireshark is a protocol analyzer that allows you to capture network traffic in real time. You can also use it to analyze network traffic that you have captured previously.

18. Select **file** from the Wireshark menu and select **open**.
    Double click on the **root** folder, and then double click on the **lab3** folder.
    Double click on the file **lab3.pcap**

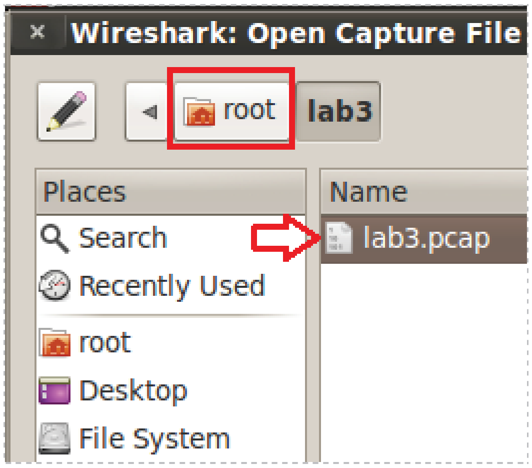
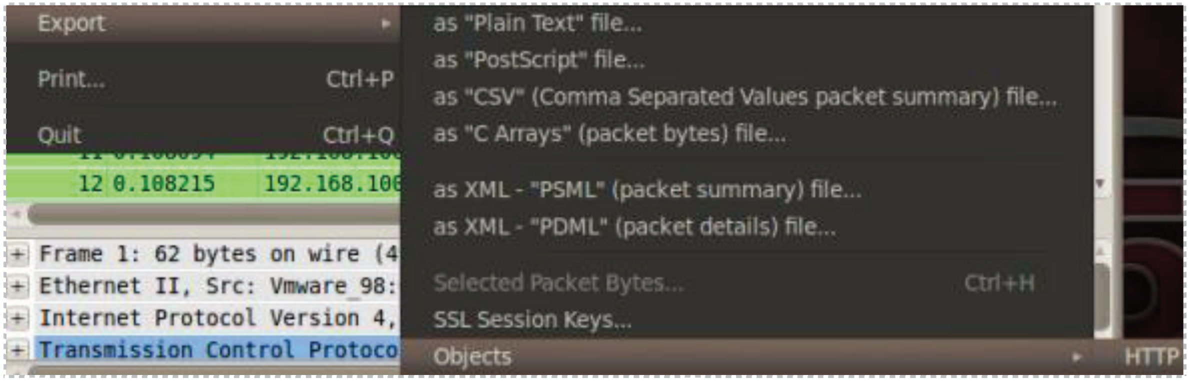


Figure 24: Selecting the lab3.pcapfile

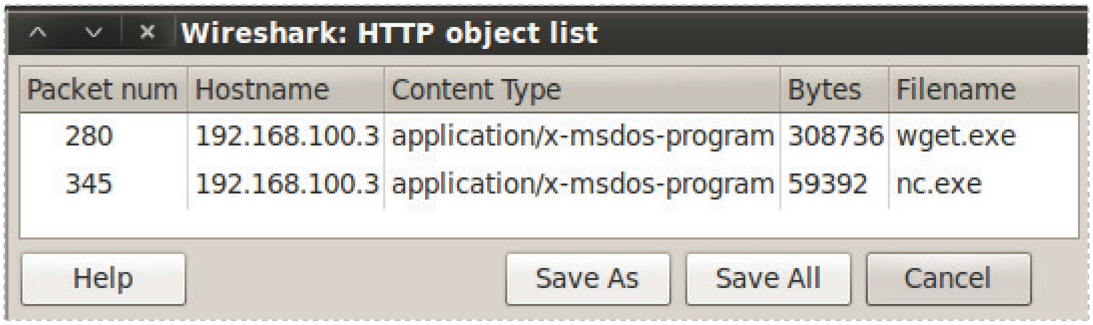
19. From the Wireshark menu, select **File**, **Export**, **Objects**, **HTTP**.


Export
Print... Ctrl+P
Quit Ctrl+Q
as "Plain Text" file...
as "PostScript" file...
as "CSV" (Comma Separated Values packet summary) file...
as "C Arrays" (packet bytes) file...
as XML - "PSML" (packet summary) file...
as XML - "PDML" (packet details) file...
Selected Packet Bytes... Ctrl+H
SSL Session Keys...
Objects
HTTP

```
12 0.108215   192.168.10
+ Frame 1: 62 bytes on wire (4
+ Ethernet II, Src: Vmware_98:
+ Internet Protocol Version 4,
+ Transmission Control Protoco
```

Figure 25: Parsing HTTP Objects

20. A new window will open with hostnames and filenames. You can see the names of the two files that were downloaded, wget.exe and nc.exe. When finished, click Cancel and exit Wireshark.



Packet num	Hostname	Content Type	Bytes	Filename
280	192.168.100.3	application/x-msdos-program	308736	wget.exe
345	192.168.100.3	application/x-msdos-program	59392	nc.exe

Figure 26: The HTTP Object List

Task 1.2 Conclusion

Apache is web server software that is included with the BackTrack Linux distribution. The HTTP protocol uses port 80, and files can be downloaded from an HTTP server with a browser, such as Internet Explorer, or a command line utility like wget. You can parse out objects that were transferred via the HTTP protocol over port 80 within Wireshark.

Task 1.3 Discussion Questions

1. What is the command to check to see if the web server is running on Linux?
2. How do you parse HTTP objects out of Wireshark?
3. How can you display all of the options for the wget command?
4. What does HTTP stand for and what port does it use?

Task 2 Using File Transfer Protocol (FTP) to Transfer Files

File Transfer Protocol, or FTP, uses Transmission Control Protocol and ports 20 and 21. FTP can be used to upload or download files. FTP sends everything across the wire in clear text by default, so its use should be avoided in favor of SCP if at all possible.

Task 2.1 Using FTP

You can use FTP from a browser or from the command line. FTP is more powerful from the command line and offers many more options. You can use FTP to upload or download files, as long as the account you are using has permission. Some ftp sites allow anonymous access, while others require a username and password. By default, all transmissions using the FTP protocol are sent over the wire in clear text.

1. Open a command prompt on the internal Windows 2003 machine by double clicking on the cmd-shortcut on the Desktop.

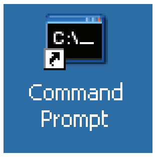
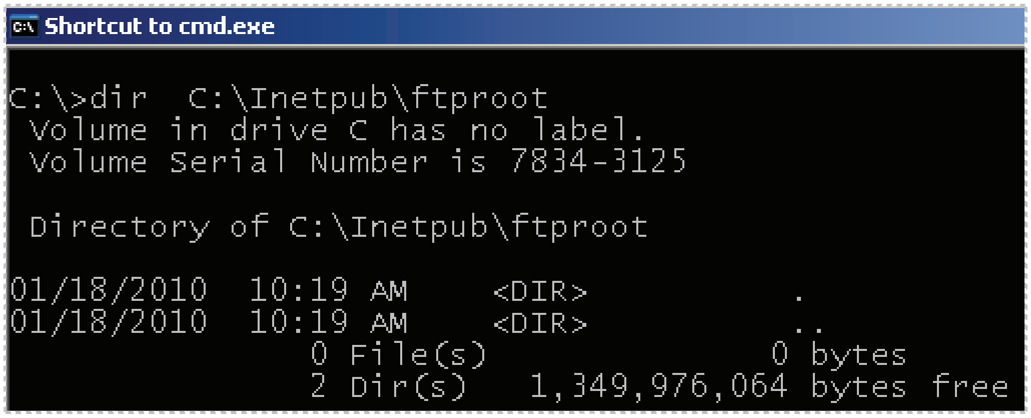


Figure 27: Opening a Command Prompt on Windows 2003

By default, users who connect to the FTP server on this Windows 2003 system will see the files and folders located within the **C:\Inetpub\ftproot** directory.

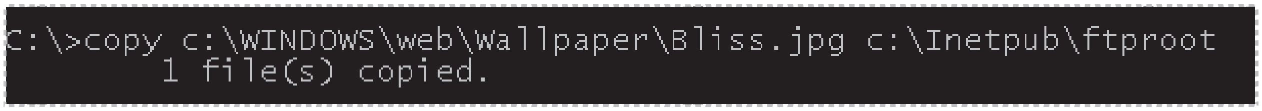
2. To view which files users will see when they connect to your FTP server, type C:\dir C:\Inetpub\ftproot



```
C:\>dir  C:\Inetpub\ftproot
 Volume in drive C has no label.
 Volume Serial Number is 7834-3125

 Directory of C:\Inetpub\ftproot

01/18/2010  10:19 AM    <DIR>          .
01/18/2010  10:19 AM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)   1,349,976,064 bytes free
```

Figure 28: Viewing the ftproot directory

3. Copy the Bliss file to the C:\Inetpub\ftproot directory by typing the following:
   C:\ **copy c:\WINDOWS\web\Wallpaper\Bliss.jpg c:\Inetpub\ftproot**



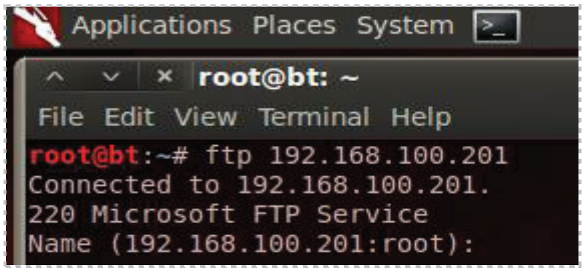
```
C:\>copy c:\WINDOWS\web\Wallpaper\Bliss.jpg c:\Inetpub\ftproot
        1 file(s) copied.
```

Figure 29: Copying a JPG file to the C:\Inetpub\ftproot directory

You should receive the message, *1 file(s) copied*, if your file is copied successfully.

Now, we will transfer the file from the Windows 2003 Server to the BackTrack 5 system.

4. Open a terminal on the BackTrack 5 system by clicking on the picture to the right of the word **System** in the task bar in the top of the. Connect to the FTP server by typing the following command:
   root@bt:~#**ftp 192.168.100.201**

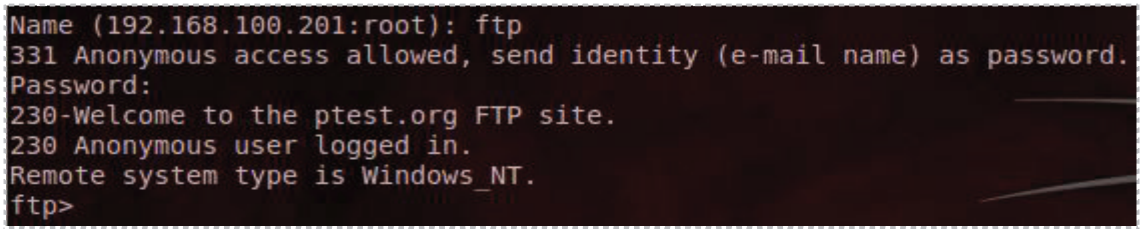

Applications Places System
root@bt: ~
File Edit View Terminal Help

```
root@bt:~# ftp 192.168.100.201
Connected to 192.168.100.201.
220 Microsoft FTP Service
Name (192.168.100.201:root):
```

Figure 30: FTP to a Remote Machine

5. For the username, type **ftp**. For the password, type **securityplus.**

For security reasons, the password will not be displayed when you type it.

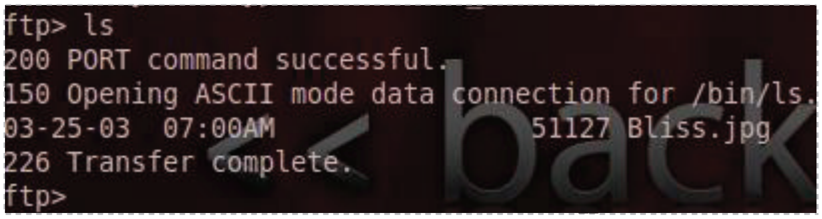


```
Name (192.168.100.201:root): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230-Welcome to the ptest.org FTP site.
230 Anonymous user logged in.
Remote system type is Windows_NT.
ftp>
```

Figure 31: Logging in as FTP

FTP Sites allowing anonymous connections will allow you to login as **ftp** or **anonymous**. Note: you should receive the message *Anonymous user logged in*.

6. Type the following command to view the files on the remote Windows system:
   ftp>**ls**

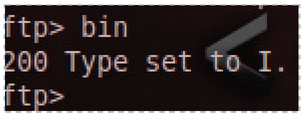


```
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
03-25-03  07:00AM                 51127 Bliss.jpg
226 Transfer complete.
ftp>
```

Figure 32: Viewing the files on the Remote FTP Site

Before the file can be transferred, you need to switch to binary mode if you are downloading anything that is not a text file, like a picture or an executable.

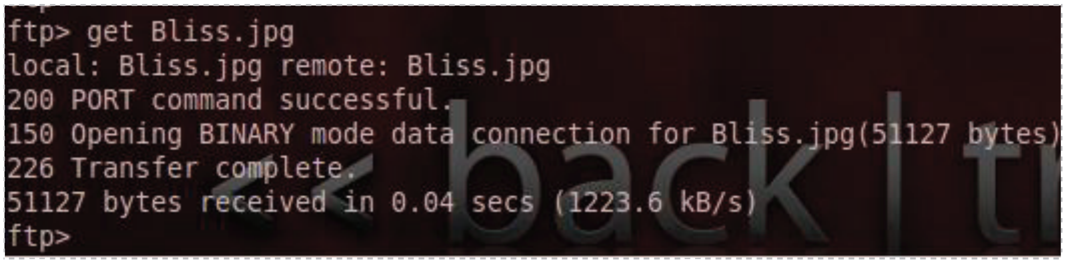
7. Type the following command to switch to binary mode:
   ftp>**bin**



```
ftp> bin
200 Type set to I.
ftp>
```

Figure 33: Switching to Binary Mode

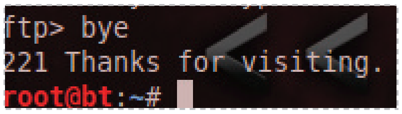
8. To download the file, type the following command (case sensitive):
   ftp>**get Bliss.jpg**



```
ftp> get Bliss.jpg
local: Bliss.jpg remote: Bliss.jpg
200 PORT command successful.
150 Opening BINARY mode data connection for Bliss.jpg(51127 bytes)
226 Transfer complete.
51127 bytes received in 0.04 secs (1223.6 kB/s)
ftp>
```

Figure 34: Downloading the File

9. Close the ftp session by typing the following command at the ftp prompt:
   ftp>**bye**



```
ftp> bye
221 Thanks for visiting.
root@bt:~#
```

Figure 35: Leaving the FTP Site

View the file by looking within root's home folder.

10. Click on **Places** from the menu bar and select **Home Folder**, view **Bliss.jpg**. Close the Home Folder when you are finished.

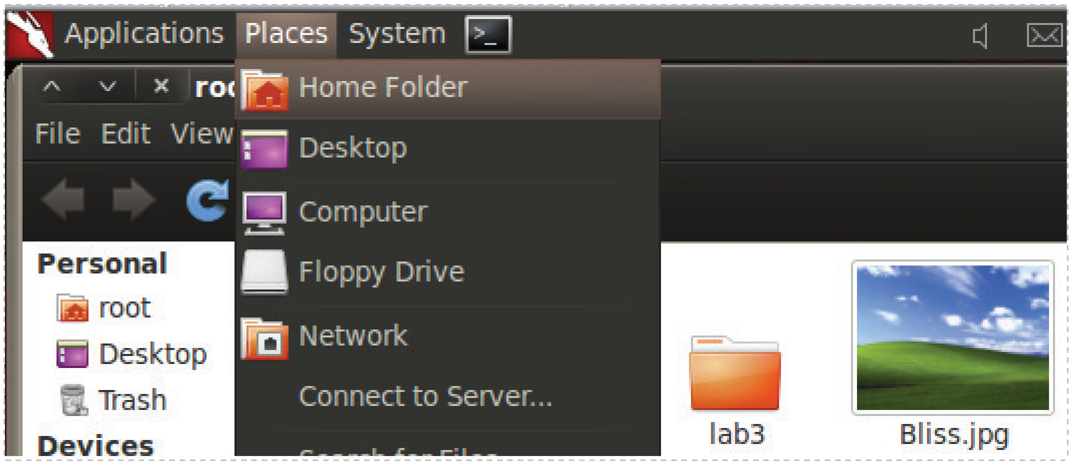


Figure 36: Viewing the Uploaded File

This Windows 2003 FTP Server allows users to download, but not upload files. In order to allow users to upload files, we must enable write permissions on the FTP server.

11. On the Windows 2003 server, click on the **Start** button, select **Administrative Tools**, and open **Internet Information Services (IIS) Manager**.

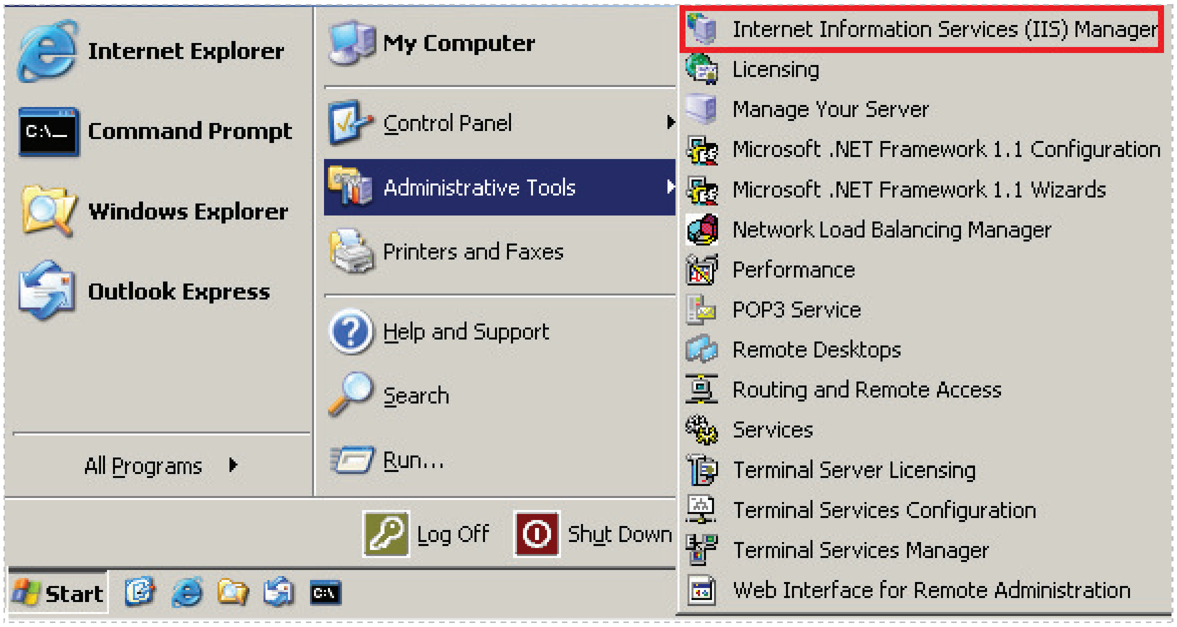
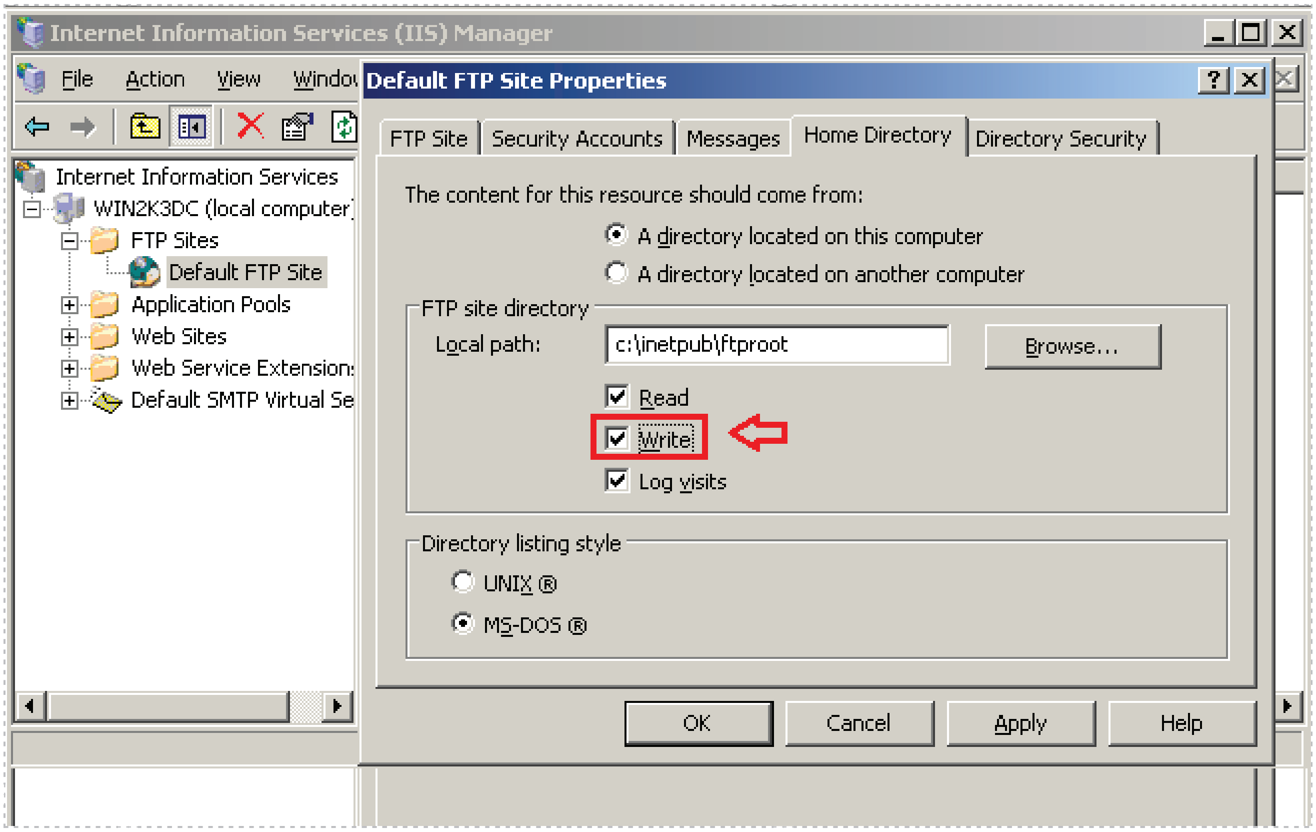

Internet Explorer
Command Prompt
Windows Explorer
Outlook Express
All Programs
My Computer
Control Panel
Administrative Tools
Printers and Faxes
Help and Support
Search
Run...
Log Off
Shut Down
Start
Internet Information Services (IIS) Manager
Licensing
Manage Your Server
Microsoft .NET Framework 1.1 Configuration
Microsoft .NET Framework 1.1 Wizards
Network Load Balancing Manager
Performance
POP3 Service
Remote Desktops
Routing and Remote Access
Services
Terminal Server Licensing
Terminal Services Configuration
Terminal Services Manager
Web Interface for Remote Administration

Figure 37: Opening Internet Information Services (IIS) Manager

12. Expand FTP Sites by clicking the plus (+) sign next to it. Right click on Default FTP Site and go to Properties. Click on the Home Directory Tab. Check the **Write** box and click **OK**. Close the **Default FTP Site Properties** window. Close the Internet Information Services (IIS) Manager.



The content for this resource should come from:

● A directory located on this computer

○ A directory located on another computer

FTP site directory

Local path: c:\inetpub\ftproot

☑ Read

☑ Write

☑ Log visits

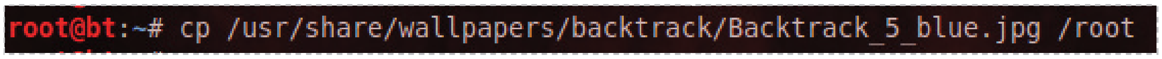
Directory listing style

○ UNIX ®

● MS-DOS ®

Figure 38: Allowing Write Access for the FTP Site

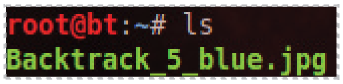
13. On the BackTrack 5 system, copy the BackTrack wallpaper to the root directory by typing the following:
root@bt:~#**cp /usr/share/wallpapers/backtrack/Backtrack_5_blue.jpg /root**



```
root@bt:~# cp /usr/share/wallpapers/backtrack/Backtrack_5_blue.jpg /root
```

Figure 39: Copying the Wallpaper file

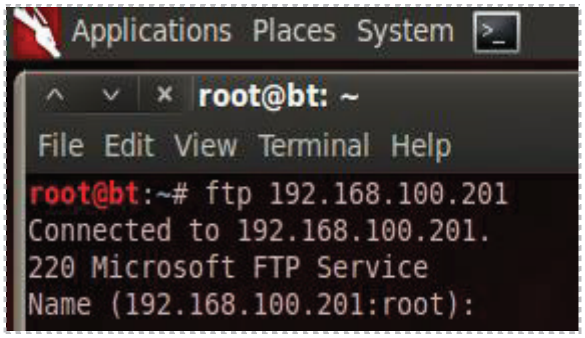
14. Type the following command to view the file in the root directory:
root@bt:~#**ls**



```
root@bt:~# ls
Backtrack_5_blue.jpg
```

Figure 40: Listing the File with the ls command

15. Connect to the FTP server by typing the following command:
    root@bt:~#**ftp 192.168.100.201**

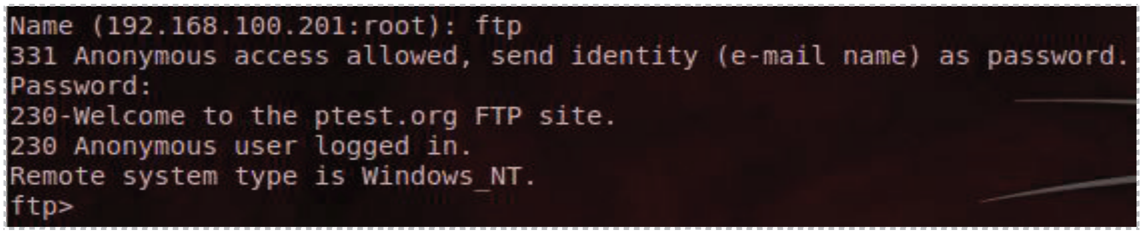


```
root@bt:~# ftp 192.168.100.201
Connected to 192.168.100.201.
220 Microsoft FTP Service
Name (192.168.100.201:root):
```

Figure 41: Copying a JPG file to the C:\Inetpub\ftproot directory

16. For the username, type **ftp**. For the password, type **securityplus.**

For security reasons, the password will not be displayed when you type it.

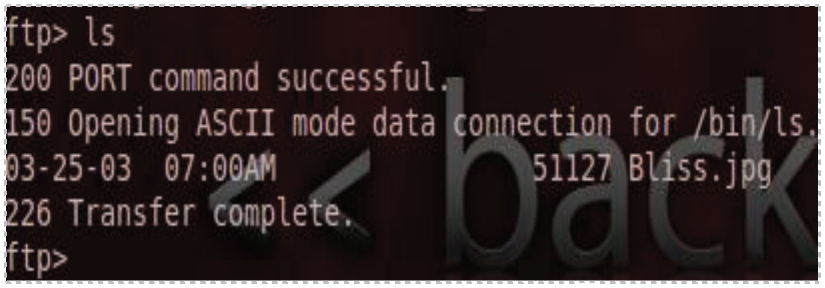


```
Name (192.168.100.201:root): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230-Welcome to the ptest.org FTP site.
230 Anonymous user logged in.
Remote system type is Windows_NT.
ftp>
```

Figure 42: Logging in as FTP

FTP Sites allowing anonymous connections will allow you to login as **ftp** or **anonymous**. Note: you should receive the message, *Anonymous user logged in*.

17. Type the following command to view the files on the remote Windows system:
    ftp>**ls**

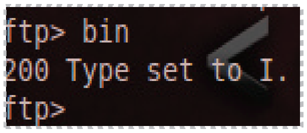


```
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
03-25-03  07:00AM              51127 Bliss.jpg
226 Transfer complete.
ftp>
```

Figure 43: Viewing the files on the Remote FTP Site

Before the file can be transferred, you need to switch to binary mode if you are downloading anything that is not a text file, like a picture or an executable.

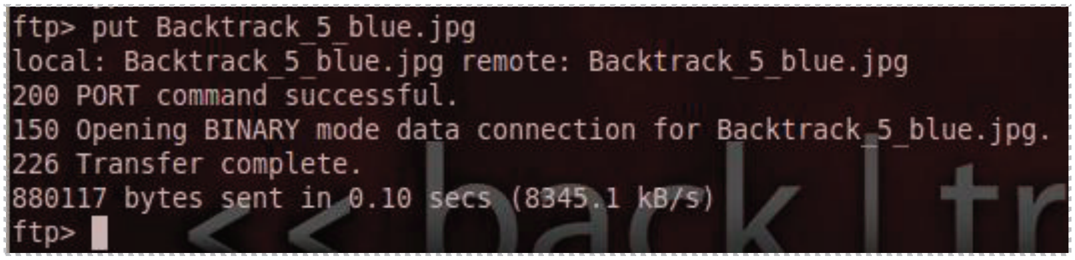
18. Type the following command to switch to binary mode:
    ftp>**bin**



```
ftp> bin
200 Type set to I.
ftp>
```

Figure 44: Switching to Binary Mode

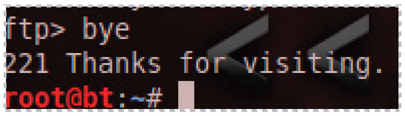
19. To upload the file, type the following command (case sensitive):
    ftp>**put Backtrack_5_blue.jpg**



```
ftp> put Backtrack_5_blue.jpg
local: Backtrack_5_blue.jpg remote: Backtrack_5_blue.jpg
200 PORT command successful.
150 Opening BINARY mode data connection for Backtrack_5_blue.jpg.
226 Transfer complete.
880117 bytes sent in 0.10 secs (8345.1 kB/s)
ftp>
```

Figure 45: Uploading the File

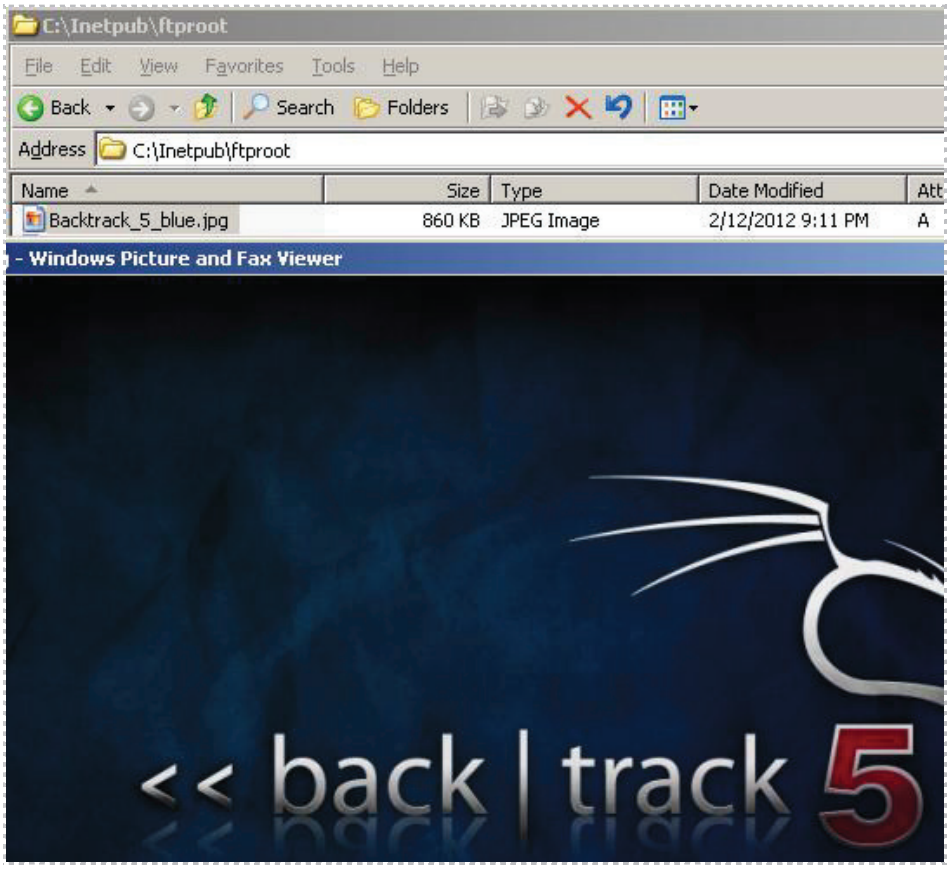
20. Close the ftp session by typing the following command at the ftp prompt:
    ftp>**bye**



```
ftp> bye
221 Thanks for visiting.
root@bt:~#
```

Figure 46: Leaving the FTP Site

21. On the Windows 2003 Machine, double click on **My Computer**, double click on **local disk (C:)**. Double click on the **Inetpub** directory, then double click on **ftproot**. Double click on the **Backtrack_5_blue.jpg** file to open it.


C:\Inetpub\ftproot
File Edit View Favorites Tools Help
Back
Search
Folders
Address C:\Inetpub\ftproot
- Windows Picture and Fax Viewer
<< back | track 5

Name	Size	Type	Date Modified	Att
Backtrack_5_blue.jpg	860 KB	JPEG Image	2/12/2012 9:11 PM	A

Figure 47: The Uploaded FTP File

22. Close all open windows.

Task 2.2 Conclusion

Like HTTP, the FTP protocol can be used to download file. FTP also can be used to upload files is the user has permission to do so. Many ftp sites allow users to login anonymously. FTP uses Ports 20 and 21 and transmits data in clear text by default.

Task 2.3 Discussion Questions

1. What are the two ports that FTP uses?
2. What is the command to upload a file to an FTP server?
3. Which ftp command should be used before uploading a picture file?
4. What is the default directory where Windows FTP files are stored?

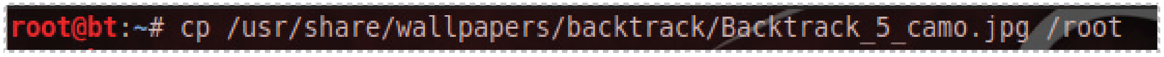
Task 3 Transferring Files Securely Using SCP

In this section, you will securely copy a file from the BackTrack Linux machine to the Linux machine running Redhat Enterprise Linux (RHEL) using SCP. Unlike FTP transmissions, SCP transmissions are encrypted. Port 22, Secure Shell is used for SCP.

Task 3.1 Using SCP

SCP can be used to securely send a file to a remote system.

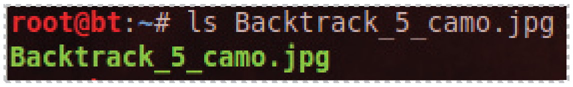
1. Open a terminal on the BackTrack 5 system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen. Copy the BackTrack wallpaper to the root directory by typing the following:
   root@bt:~#**cp /usr/share/wallpapers/backtrack/Backtrack_5_camo.jpg /root**



```
root@bt:~# cp /usr/share/wallpapers/backtrack/Backtrack_5_camo.jpg /root
```

Figure 48: Copying the BackTrack Wallpaper

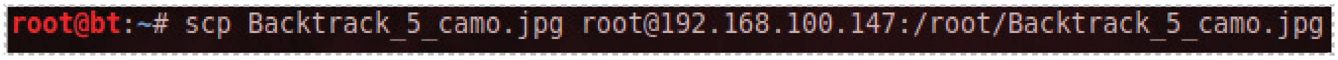
2. Type the following command to view the file in the root directory:
   root@bt:~#**ls Backtrack_5_camo.jpg**



```
root@bt:~# ls Backtrack_5_camo.jpg
Backtrack_5_camo.jpg
```

Figure 49: The Wallpaper File in root's Home Directory

3. Copy the file to the root directory of the RHEL machine by typing the following:
root@bt:~#**scp Backtrack_5_camo.jpg root@192.168.100.147:/root/Backtrack_5_camo.jpg**

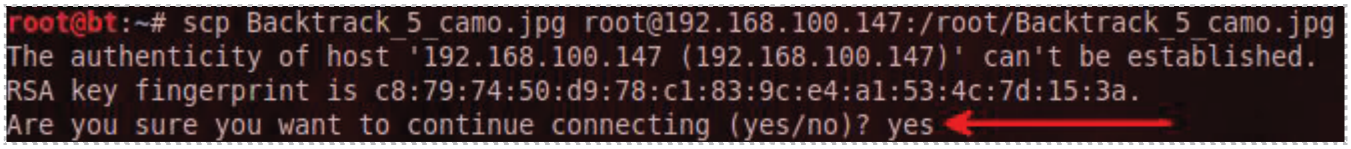


```
root@bt:~# scp Backtrack_5_camo.jpg root@192.168.100.147:/root/Backtrack_5_camo.jpg
```

Figure 50: Using the scp command

Hit the Enter key after you type the scp command on your BackTrack Linux machine.

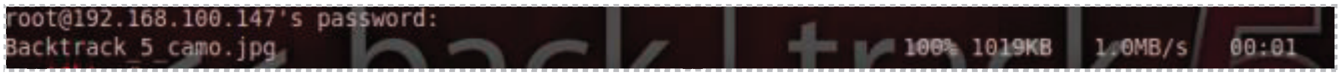
4. If prompted, type **yes** when you are asked if you are sure you want to continue connecting. If you do not receive the prompts (as seen below), continue to #5.



```
root@bt:~# scp Backtrack_5_camo.jpg root@192.168.100.147:/root/Backtrack_5_camo.jpg
The authenticity of host '192.168.100.147 (192.168.100.147)' can't be established.
RSA key fingerprint is c8:79:74:50:d9:78:c1:83:9c:e4:a1:53:4c:7d:15:3a.
Are you sure you want to continue connecting (yes/no)? yes
```

Figure 51: Connection Warning

5. Type the password of **password**. The file transfer status should go to 100%.



```
root@192.168.100.147's password:
Backtrack_5_camo.jpg                          100% 1019KB   1.0MB/s   00:01
```

Figure 52: Transferred File Status

6. On the Red Hat system, click on **Places** and select **Home Folder** to view the copied file. Close the window when you are finished.

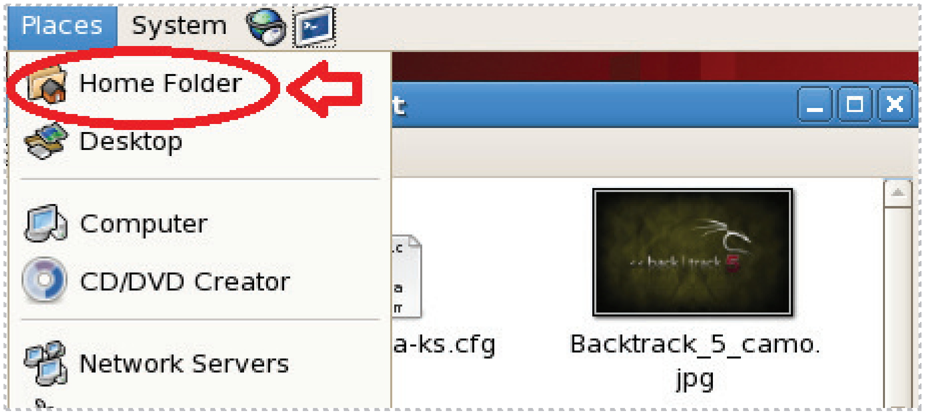


Figure 53: Transferred File

Task 3.2 Conclusion

The Secure Copy Protocol is a way to securely transfer files from one system to another. Unlike FTP, SCP encrypts the transmission so usernames and passwords will not be seen going across the wire like they can be with FTP. Use SCP rather than FTP whenever possible.

Task 3.3 Discussion Questions

1. What port does SSH and SCP use by default?
2. What does SCP stand for?
3. How is SCP different from the FTP protocol?
4. What benefits does using SCP provide over other protocols?

5 References

1. FTP Commands:
   http://unixhelp.ed.ac.uk/CGI/man-cgi?ftp

2. SCP:
   http://kb.iu.edu/data/agye.html

3. Internet Information Services:
   http://www.iis.net/

4. Apache:
   http://www.apache.org/

5. BackTrack Linux:
   http://www.backtrack-linux.org/

CompTIA Security+® Lab Series

Lab 4: Protocols and Default Network Ports - Connecting to a Remote System

CompTIA Security+® Domain 1 - Network Security

Objective 1.4: Implement and use common protocols
Objective 1.5: Identify commonly used default network ports

Document Version: 2012-08-15 (Beta)

Lab Author: Jesse Varsalone
Assistant Professor
Cyber Security
Organization: Community College of Baltimore County

The development of this document is funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) is an entity of Moraine Valley Community College. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation. A copy of this license can be found at http://www.gnu.org/licenses/fdl.html.

Contents

1 Introduction 3
2 Objectives: Implement and Use Common Protocols 3
Identify Commonly Used Default Network Ports 3
3 Pod Topology 5
4 Lab Settings 6
Task 1 Connecting to a Windows System through the Command Line 9
Task 1.1 Using TELNET to Perform Remote Administration 9
Task 1.2 Conclusion 16
Task 1.3 Discussion Questions 16
Task 2 Connecting to a Linux System through the Command Line 17
Task 2.1 Using SSH to Connect to a Remote Linux System 17
Task 2.2 Conclusion 24
Task 2.3 Discussion Questions 24
Task 3 Analyzing Remote Connections in Network Traffic 25
Task 3.1 Using Wireshark to Connect to a Remote Linux System 25
Task 3.2 Conclusion 30
Task 3.3 Discussion Questions 30
5 References 31

1 Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will be able to connect to remote systems running Windows and Linux and run commands to perform administrative tasks. Students will use the TELNET protocol to connect to remote Windows system and the SSH protocol to connect to a system running Linux. Students will then analyze both protocols within network traffic to determine whether the protocol uses encryption or clear text.

This lab includes the following tasks:

- Task 1 - Connecting to a Windows System through the Command Line
- Task 2 - Connecting to a Linux System through the Command Line
- Task 3 - Analyzing Remote Connections in Network Traffic

2 Objectives: Implement and Use Common Protocols Identify Commonly Used Default Network Ports

Network Administrators often have to perform maintenance on servers from remote locations. The server could be on a system within the same building or across the globe. Network administration can be done remotely through a GUI based program like Microsoft Terminal Services or Virtual Network Connector (VNC), but the use of command line tools like TELNET and SSH is extremely common. It is very common to have a Linux system running without a GUI, and there are even some distributions of Windows, like Server Core, that have no GUI interface. It is critically important for network administrators to understand command line utilities in order to have a good grasp of computer security concepts.

TELNET – The TELNET protocol, which uses port 23, allows someone to remotely administrator a computer, router, and switch. All traffic sent using the TELNET protocol is sent in clear text, which means usernames and passwords will be visible to anyone examining the traffic. For security reasons, the use of TELNET should be avoided.

SSH [1] – Secure Shell, which uses port 22, allows a user to securely connect to a remote machine. Unlike TELNET connections that are in clear text, SSH connections are encrypted. While Linux and Mac have support for SSH natively, Windows does not.

Windows Command Shell – The Windows command shell allows users to interact with the operating system from a command line environment. Virtually anything that can be done in the Graphical User Interface, or GUI, in Windows can be done from the command line. TELNET can be used to perform remote command line administration.

Linux Bash Shell – The Linux Bourne Again Shell, or Bash shell, is one of many shells that are available in a Linux environment. Linux servers are often managed from the command line; therefore network administrators need to be comfortable with bash.

Wireshark [2] – Wireshark is a protocol analyzer that will allow you to capture traffic as well as analyze network traffic. Wireshark can be used to inspect traffic and examine the clear text communication of TELNET and encrypted communication of SSH.

3 Pod Topology

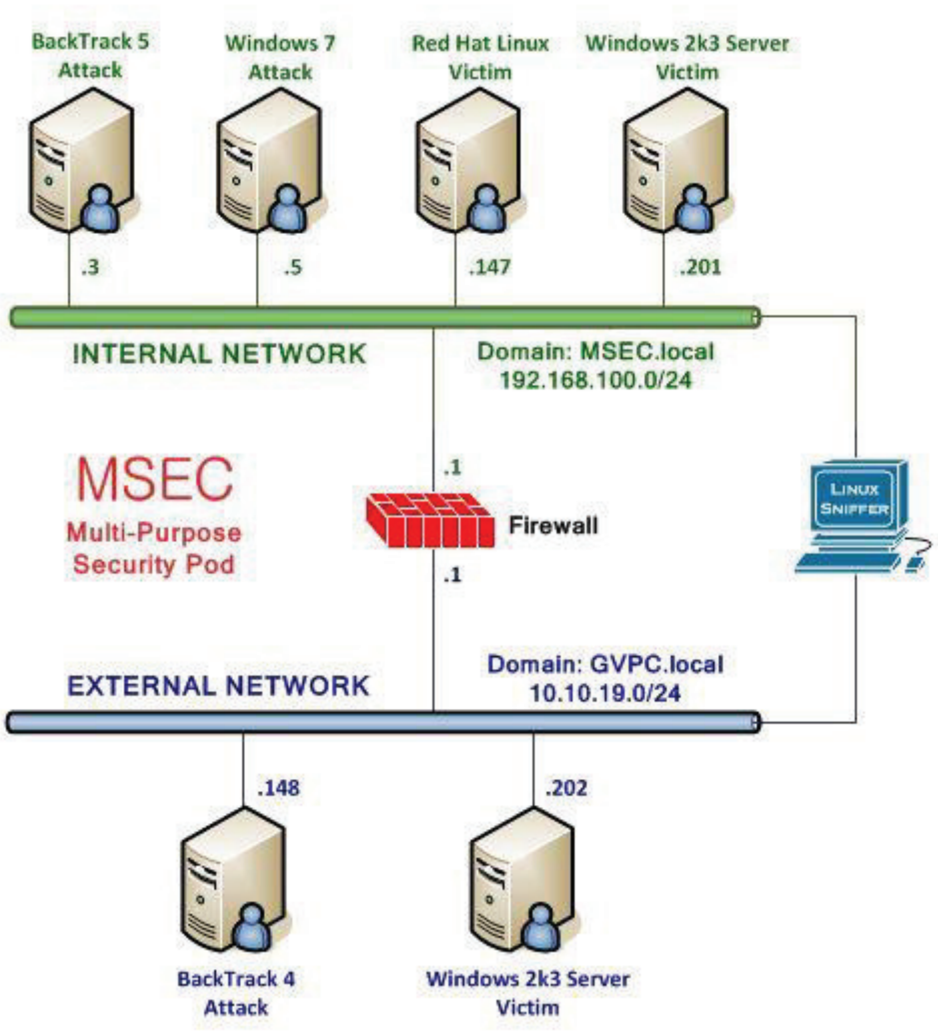


Figure 1: MSEC Network Topology

4 Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

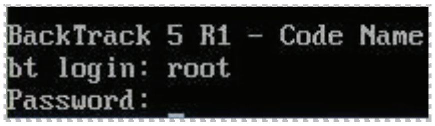
Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

BackTrack 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password
Windows 2k3 Server Internal Victim Machine	192.168.100.201
Windows 2k3 Server administrator password	password
Red Hat Enterprise Internal Victim Machine	192.168.100.3
Red Hat Enterprise root password	password
Win7 Internal Attack Machine	192.168.100.201
Win7 Attack Machine student password	password

BackTrack 5 Login:

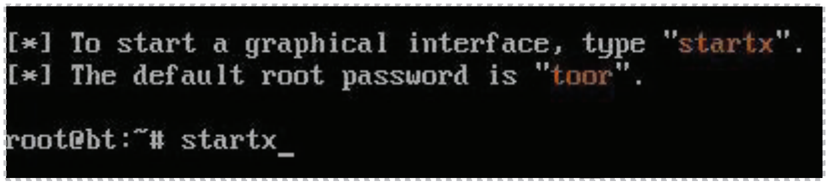
1. Click on the BackTrack 5 icon on the topology.
2. Type **root** at the **bt login:** username prompt.
3. Type **password** at the Password: prompt.



```
BackTrack 5 R1 - Code Name
bt login: root
Password: _
```

Figure 2: BackTrack 5 login

4. To start the GUI, type **startx** at the root@bt:~# prompt.

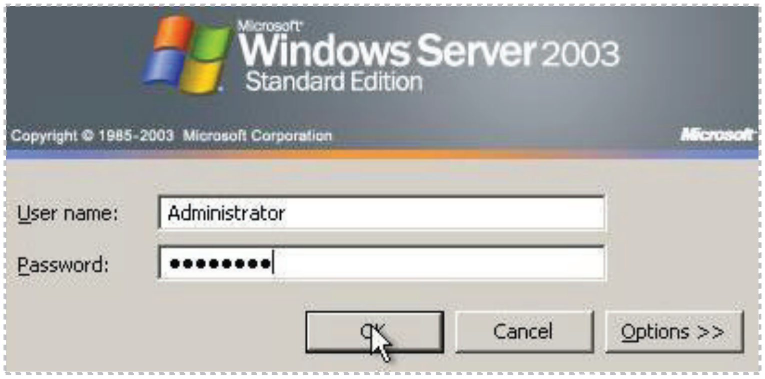


```
[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".

root@bt:~# startx_
```

Figure 3: BackTrack 5 GUI start up

Windows 2003 Server Login:

1. Click on the Windows 2k3 Server icon on the topology (these instructions will work for both internal and external victim machines).
2. Enter the User name, **Administrator** (verify the username with your instructor).
3. Type in the password: **password** and click the **OK** button (verify the password with your instructor).



User name: Administrator

Password: ••••••••

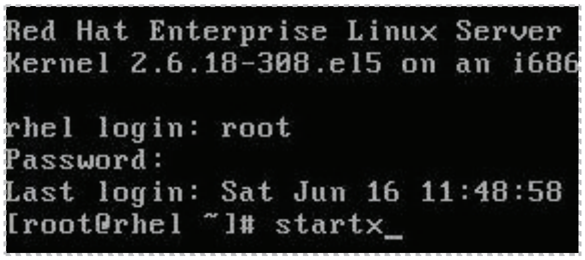
Figure 4: Windows 2k3 login

Red Hat Enterprise Linux Login:

1. Click on the Red Hat Linux icon on the topology.
2. Type **root** at the rhel login: prompt.
3. Type **password** at the Password: prompt.

For security purposes, the password will not be displayed.

4. To start the GUI, type **startx** at the [root@rhe ~]# prompt.



```
Red Hat Enterprise Linux Server
Kernel 2.6.18-308.el5 on an i686

rhel login: root
Password:
Last login: Sat Jun 16 11:48:58
[root@rhel ~]# startx_
```

Figure 5: RHEL login

Windows 7 Login:

1. Click on the Windows 7 icon on the topology.
2. Enter the username, **student** (verify the username with your instructor).
3. Type in the password, **password** and hit enter to log in (verify the password with your instructor).

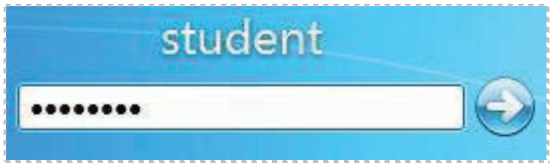


Figure 6: Windows 7 login

Task 1 Connecting to a Windows System through the Command Line

For a variety of reasons, network administrators may need to perform tasks on a remote system. TELNET can be used to perform remote administration on computers, routers, switches, and other devices. The disadvantage of using TELNET is that it sends everything across the wire in clear text including usernames, passwords, and commands. For this reason, the use of TELNET should be avoided if possible.

First, we will scan the victim machine to determine if the TELNET port is open. We will specify the default TELNET port of 23 when conducting the nmap scan.

Task 1.1 Using TELNET to Perform Remote Administration

Open a Command Prompt to Get Started

1. Open a command prompt on the Windows 7 machine by double clicking on the **cmd.exe** icon on the Desktop.

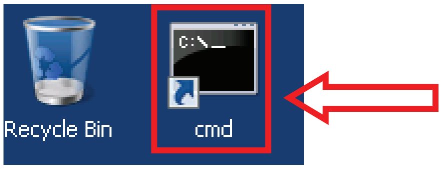
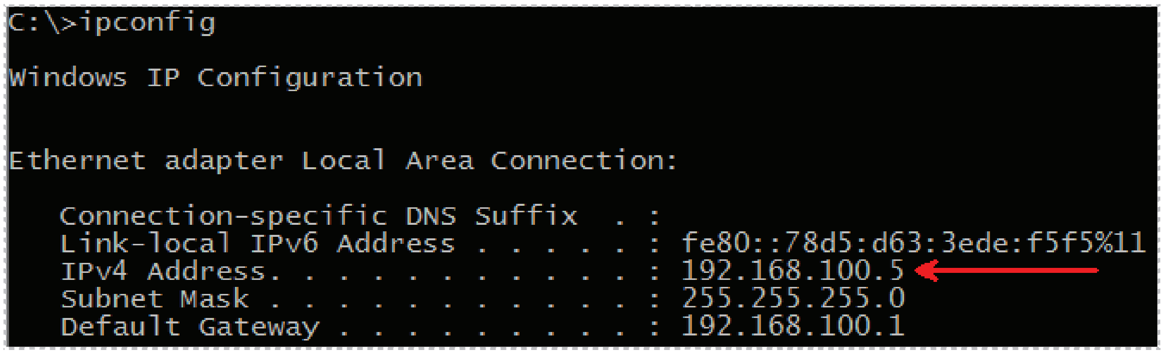


Figure 7: Opening a Command Prompt on Windows 7

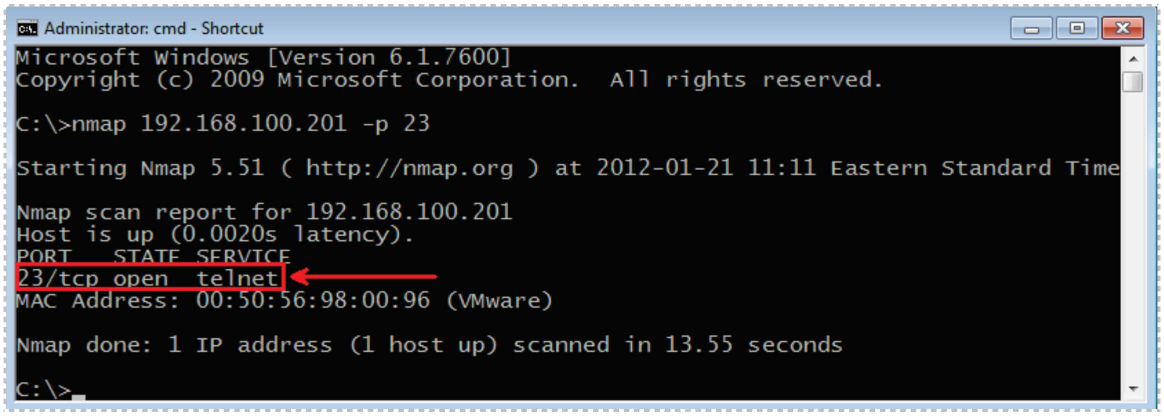
2. Before you start, determine the IP Address of the Windows 7 machine by typing: C:\ipconfig



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::78d5:d63:3ede:f5f5%11
   IPv4 Address. . . . . . . . . . . : 192.168.100.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.1
```

Figure 8: The IP Address Information of the Windows 7 Machine

3. Type the following to determine if port 23 is open on the remote system.
   C:\nmap 192.168.100.201 –p 23



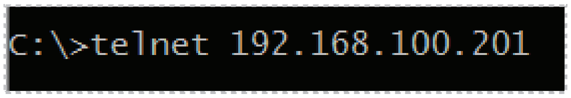
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>nmap 192.168.100.201 -p 23

Starting Nmap 5.51 ( http://nmap.org ) at 2012-01-21 11:11 Eastern Standard Time

Nmap scan report for 192.168.100.201
Host is up (0.0020s latency).
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:50:56:98:00:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.55 seconds

C:\>
```

Figure 9: The Results of an Nmap Scan

The results of the Nmap scan indicate that the TELNET port is open on the remote system. In order to connect via TELNET, you need to have a user account and the password for the remote system. This information is sent over the network in clear text.

The TELNET client is not installed by default on Windows Vista or Windows 7. It must be added through the Add Programs and Features applet in the Control Panel.
We have already added the TELNET client feature on the Windows 7 Virtual Machine.

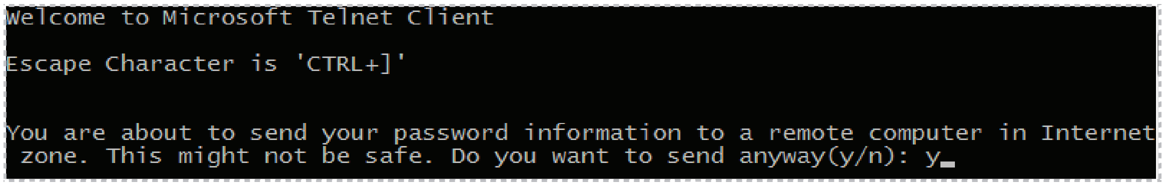
4. From the command prompt, type the following command
   C:\telnet 192.168.100.201



```
C:\>telnet 192.168.100.201
```

Figure 10: Using the TELNET command in Windows

5. You will be warned that it might not be safe to send your password. Type **y** to send it anyway.

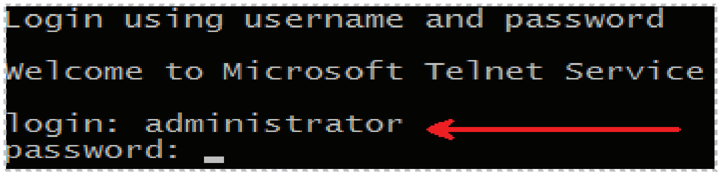


```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

You are about to send your password information to a remote computer in Internet
 zone. This might not be safe. Do you want to send anyway(y/n): y
```

Figure 11: Warnings about the Danger of Using Telnet

You will be prompted for the username and password. The username will be displayed as you type it, but the password is not displayed for security reasons.

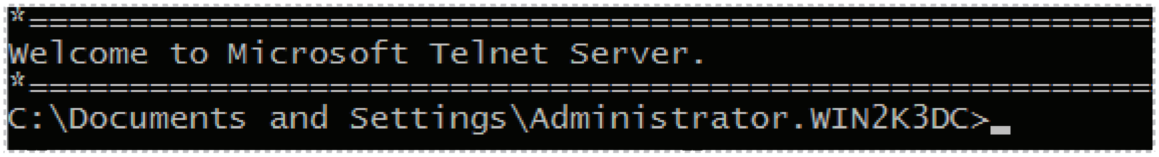
6. For the username, type **administrator** and for the password type **password.**



```
Login using username and password

Welcome to Microsoft Telnet Service

login: administrator
password: _
```

Figure 12: Inputting the Username and Password of the Remote System

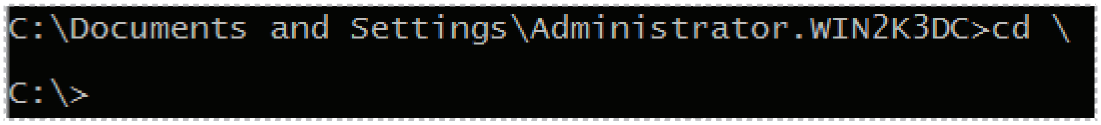
After a successful login, you will receive the message *Welcome to Microsoft Telnet Server.* You will start in the **Documents and Settings Folder** of the user's account.



```
*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================
C:\Documents and Settings\Administrator.WIN2K3DC>_
```

Figure 13: A Successful TELNET connection was made

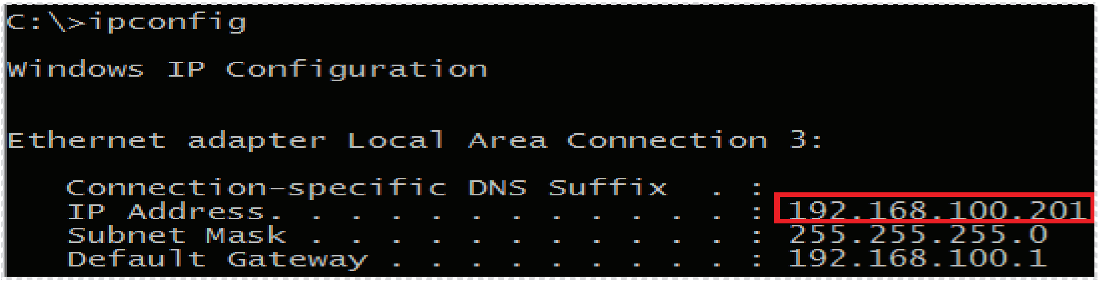
7. Type the following command to change directories to the root of the C drive: C:\Documents and Settings\Administrator.WIN2K3DC>**cd **



```
C:\Documents and Settings\Administrator.WIN2K3DC>cd \

C:\>
```

Figure 14 Changing Directories to the Root of C:

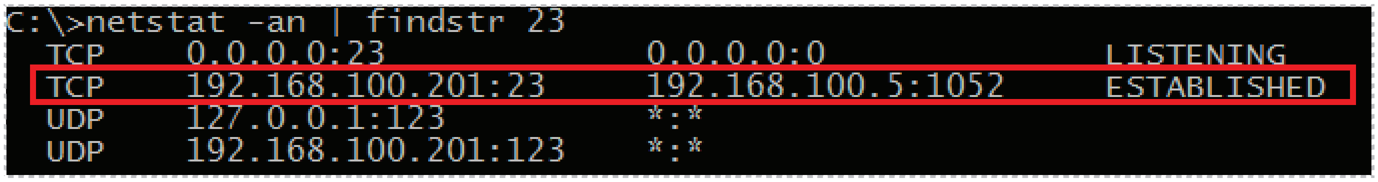
8. Type the following command to view the IP Address information of the remote system running Windows Server 2003 you are connected to through TELNET. C:\ >**ipconfig**



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.100.201
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.1
```

Figure 15: Displaying the IP Address of the Remote machine

9. To view the active telnet connection from the Windows 7 machine to the Windows Server 2003 machine in the network connections, type the following: C:\netstat –an | findstr 23



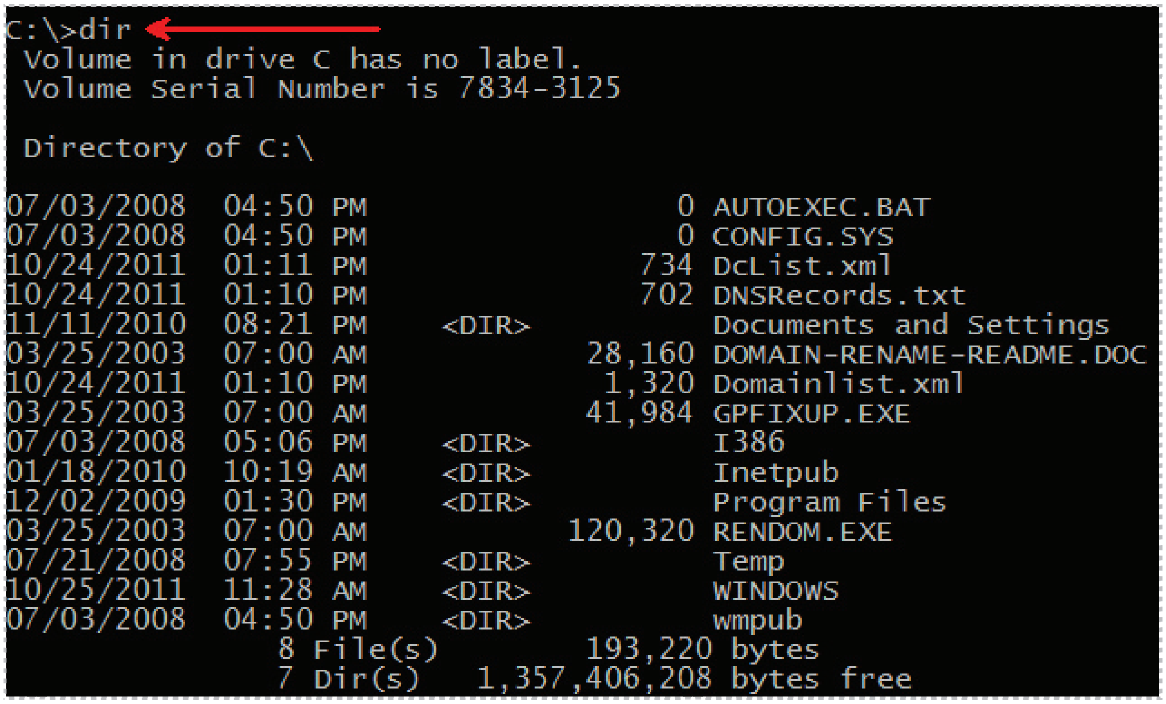
```
C:\>netstat -an | findstr 23
  TCP    0.0.0.0:23             0.0.0.0:0              LISTENING
  TCP    192.168.100.201:23     192.168.100.5:1052     ESTABLISHED
  UDP    127.0.0.1:123          *:*
  UDP    192.168.100.201:123    *:*
```

Figure 16: Viewing the TELNET Network Connection from Windows 7 to Server 2003

The netstat data first indicates that the Windows Server 2003 is listening on port 23:
TCP   0.0.0.0:23   0.0.0.0:0   LISTENING

The second connection indicates a TELNET connection from the Windows 7 with the IP Address of 192.168.100.5 to Windows Server 2003 with IP Address 192.168.100.201. The other two connections displayed are dealing with Network Time Protocol, which uses UDP and port 123. TELNET, on the other hand, uses TCP and port 23.

10. Type the following command to view the files on the root of the C drive. These are the files on the C: Drive of the remote Windows 2003 Server system. C:\dir

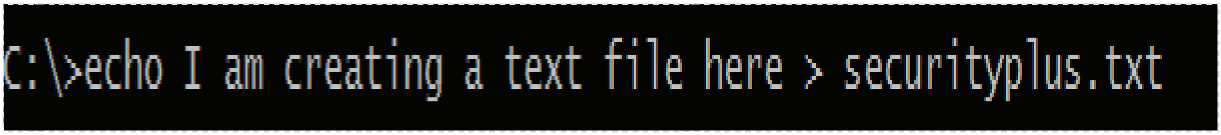


```
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 7834-3125

 Directory of C:\

07/03/2008  04:50 PM                 0 AUTOEXEC.BAT
07/03/2008  04:50 PM                 0 CONFIG.SYS
10/24/2011  01:11 PM               734 DcList.xml
10/24/2011  01:10 PM               702 DNSRecords.txt
11/11/2010  08:21 PM    <DIR>          Documents and Settings
03/25/2003  07:00 AM            28,160 DOMAIN-RENAME-README.DOC
10/24/2011  01:10 PM             1,320 Domainlist.xml
03/25/2003  07:00 AM            41,984 GPFIXUP.EXE
07/03/2008  05:06 PM    <DIR>          I386
01/18/2010  10:19 AM    <DIR>          Inetpub
12/02/2009  01:30 PM    <DIR>          Program Files
03/25/2003  07:00 AM           120,320 RENDOM.EXE
07/21/2008  07:55 PM    <DIR>          Temp
10/25/2011  11:28 AM    <DIR>          WINDOWS
07/03/2008  04:50 PM    <DIR>          wmpub
               8 File(s)        193,220 bytes
               7 Dir(s)   1,357,406,208 bytes free
```

Figure 17: Displaying the Files on the Remote System

In the next step, we will make a text file on a remote system through the command line. Notepad and Wordpad are GUI applications and cannot be utilized in a TELNET session. Using the **edit** command is not a good idea either because there is a good likelihood you will get stuck in the editor. In order to create a text file, we will use the echo command along with a redirect (>). This technique can be used in Windows or Linux.

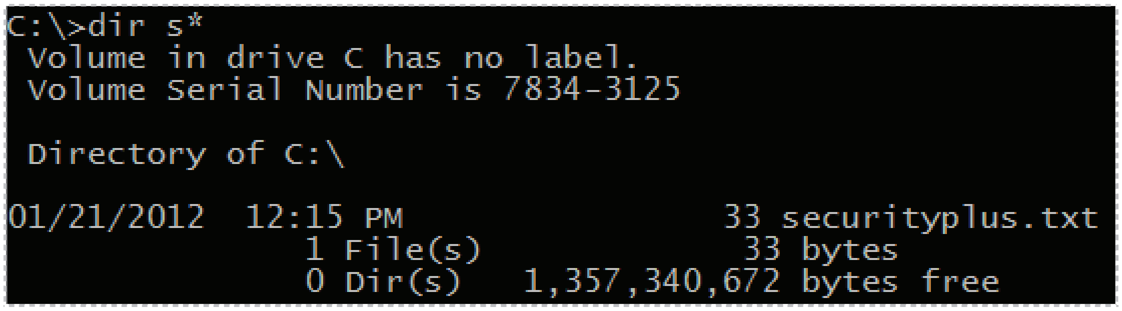
11. Type the following command to create a text file through the command line:
    C:\echo I am creating a text file here > securityplus.txt



```
C:\>echo I am creating a text file here > securityplus.txt
```

Figure 18: Creating a Text File Using Echo

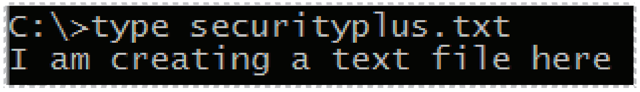
12. Type the following command to view the newly created file.
    C:\**dir s***



```
C:\>dir s*
 Volume in drive C has no label.
 Volume Serial Number is 7834-3125

 Directory of C:\

01/21/2012  12:15 PM                33 securityplus.txt
               1 File(s)             33 bytes
               0 Dir(s)   1,357,340,672 bytes free
```

Figure 19: Listing the File Created on the Remote System

13. To view what is written inside the file, type the following command:
    C:\type securityplus.txt



```
C:\>type securityplus.txt
I am creating a text file here
```

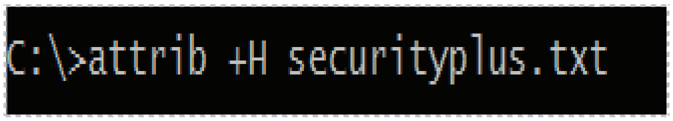
Figure 20: Displaying the Contents of the Text File on the Remote System

There are attributes you can add to a file from the command line, including:

- Hidden – File is not displayed in a directory listing.
- Read Only – File is readable, but cannot be changed or deleted.
- System – File is used by the operating system.
- Archive – File is used for backup purposes.

Attributes can be applied to files by using the **attrib** command. The attrib command followed by a plus (+) and the name of the file will add the attribute to the file. The attrib command followed by a minus sign (-)and the name of the file will remove the attribute from the file. A directory (**dir**) command along with a forward slash and the symbol representing the attribute will display the files with those attributes.

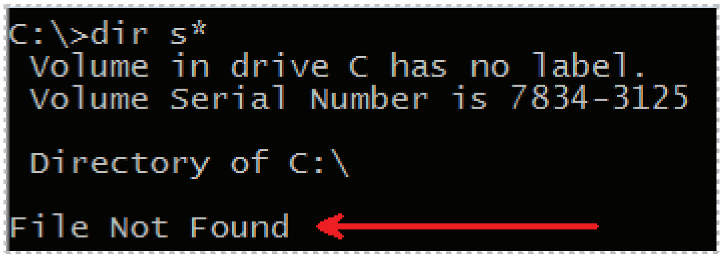
14. To hide the text file, type the following command
    C:**attrib +H securityplus.txt**



```
C:\>attrib +H securityplus.txt
```

Figure 21: Hiding a File on the Remote System using the attrib Command

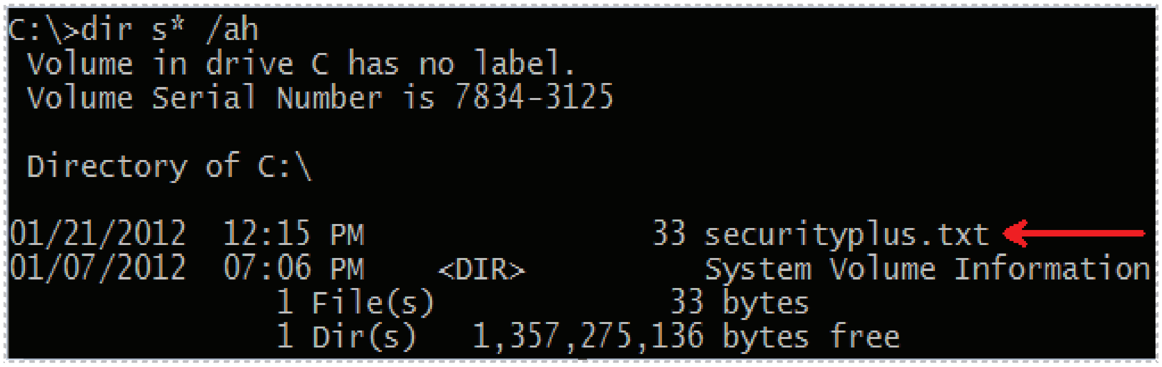
15. After applying the attribute, try to view the hidden securityplus.txt file
    C:**dir s***



```
C:\>dir s*
 Volume in drive C has no label.
 Volume Serial Number is 7834-3125

 Directory of C:\

File Not Found
```

Figure 22: The Hidden File is not displayed on the Remote System

16. To display the hidden securityplus.txt file, type the following command:
    C:**dir s* /ah**

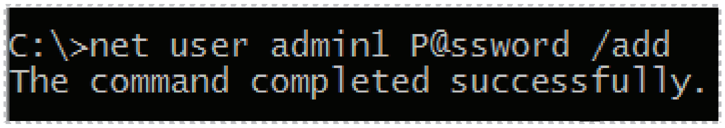


```
C:\>dir s* /ah
 Volume in drive C has no label.
 Volume Serial Number is 7834-3125

 Directory of C:\

01/21/2012  12:15 PM                33 securityplus.txt
01/07/2012  07:06 PM    <DIR>          System Volume Information
               1 File(s)             33 bytes
               1 Dir(s)   1,357,275,136 bytes free
```

Figure 23: Displaying the Hidden File on the Remote System

Displaying, creating, and hiding files can be done on a remote system using TELNET. An Administrator can also perform other tasks, such as account and service maintenance

17. To create a user on the remote system type the following command:
    C:\net user admin1 P@ssword /add

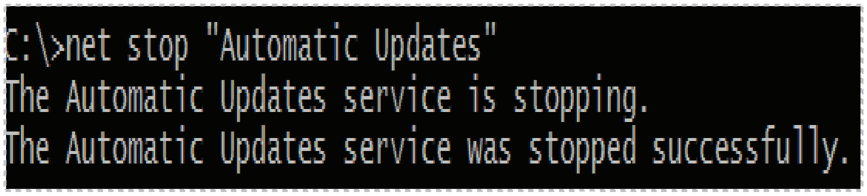


```
C:\>net user admin1 P@ssword /add
The command completed successfully.
```

Figure 24: Adding a User through the Command Line

You should receive the message that *the command completed successfully*. The user created will have an account named **admin1** and a password of **P@ssw0rd**.
The administrator logged into the system remotely through the command line can also view, stop, and start services by using the **net start** and **net stop** commands. One service that should not be stopped is the TELNET service or the connection will die.

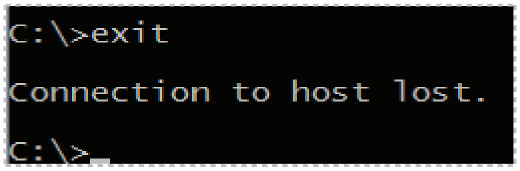
18. To stop the **Automatic Updates** service on the remote machine, type:
    C:\ **net stop "Automatic Updates"**



```
C:\>net stop "Automatic Updates"
The Automatic Updates service is stopping.
The Automatic Updates service was stopped successfully.
```

Figure 25: Stopping the Automatic Updates Service

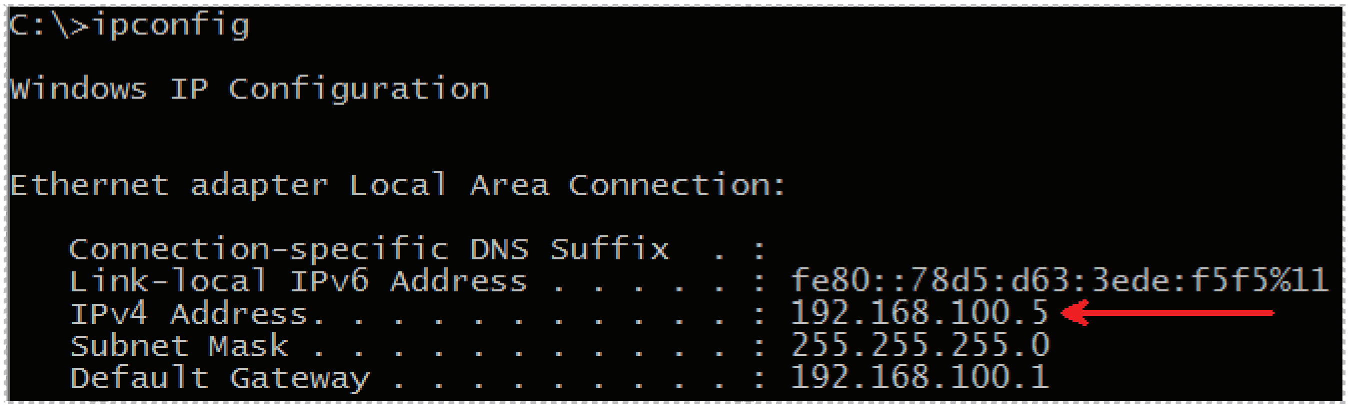
19. Type **exit** to leave the command prompt session on the remote machine



```
C:\>exit

Connection to host lost.

C:\>_
```

Figure 26: Leaving the TELNET session

20. To be sure that your TELNET session to the Windows Server is disconnected, type ipconfig and the IP Address of the Windows 7 System should be displayed again.
    C:\ipconfig



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::78d5:d63:3ede:f5f5%11
   IPv4 Address. . . . . . . . . . . : 192.168.100.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.1
```

Figure 27: The IP Address Information of the Windows 7 Machine

Task 1.2 Conclusion

A network administrator can use TELNET to remotely connect to a computer to run commands. A TELNET connection can be used to display and create files on the remote system, as well as perform other administrative tasks, like maintenance of accounts and services. TELNET uses TCP port 23 and sends information over the network in clear text.

Task 1.3 Discussion Questions

1. What command can be used to show an active TELNET connection?
2. What is the command that can be used to display files on a remote system when an administrator is connected via a TELNET session?
3. How can you create a file on a remote system during a TELNET session?
4. What command can be used to determine if a remote system is running TELNET?

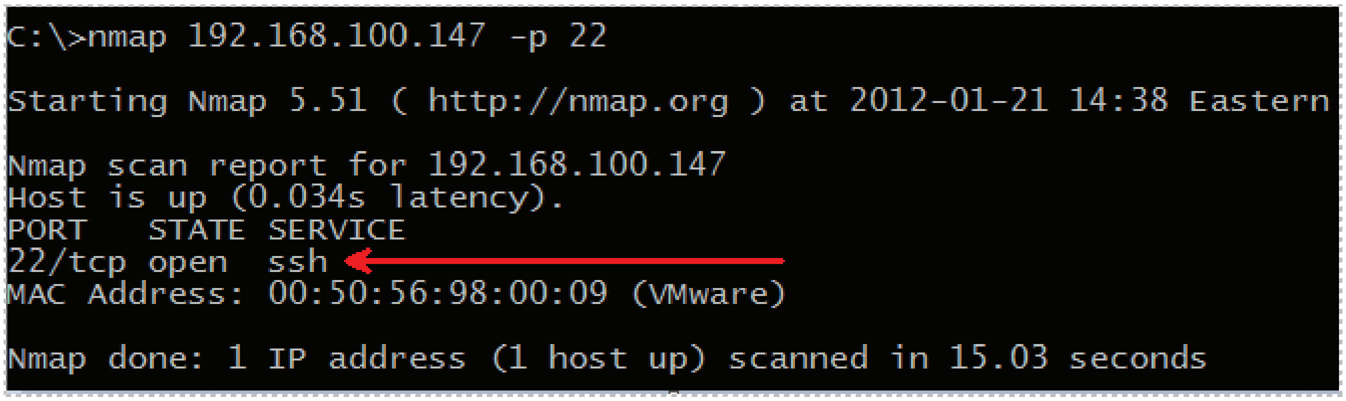
Task 2 Connecting to a Linux System through the Command Line

Most people would agree with the fact that since its inception, Linux has always been an operating system that took security seriously. Most distributions of Linux come with a built in SSH server as well as an SSH client that will allow you to connect to servers running SSH. The SSH, or secure shell, protocol, use Transmission Control Protocol port 22. Unlike TELNET, everything sent over the wire using SSH is encrypted.

Task 2.1 Using SSH to Connect to a Remote Linux System

Warning - This must be done before starting Task 2:
The Red Hat 9 Enterprise Linux Internal Victim machine needs to be logged into using the **root** username with the password: **password** (the password will not be displayed for security reasons). Once you have logged in, issue the command **startx** to start the GUI (Graphical User Interface). See Lab Settings, section 4 for details. **Until this procedure has been performed, Task 2 cannot be started.**

1. From a command prompt on the Windows 7 virtual machine, type the following to determine if port 22 is open on the remote Linux system:
   C:\>**nmap 192.168.100.201 –p 22**



```
C:\>nmap 192.168.100.147 -p 22

Starting Nmap 5.51 ( http://nmap.org ) at 2012-01-21 14:38 Eastern

Nmap scan report for 192.168.100.147
Host is up (0.034s latency).
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:50:56:98:00:09 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.03 seconds
```

Figure 28: Determining if SSH Port 22 is Open on the Remote Machine

Microsoft Windows does not have a Secure Shell (SSH) client built into the operating system. However, third party SSH client and server applications can be used to make SSH connections to other systems, or to allow incoming SSH connections. PuTTY is a 3rd party application that will allow you to connect to a remote system running SSH.

2. Double click on putty.exe to launch the third party SSH client application.

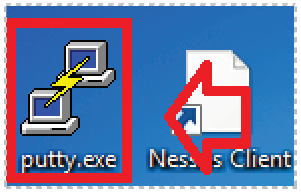


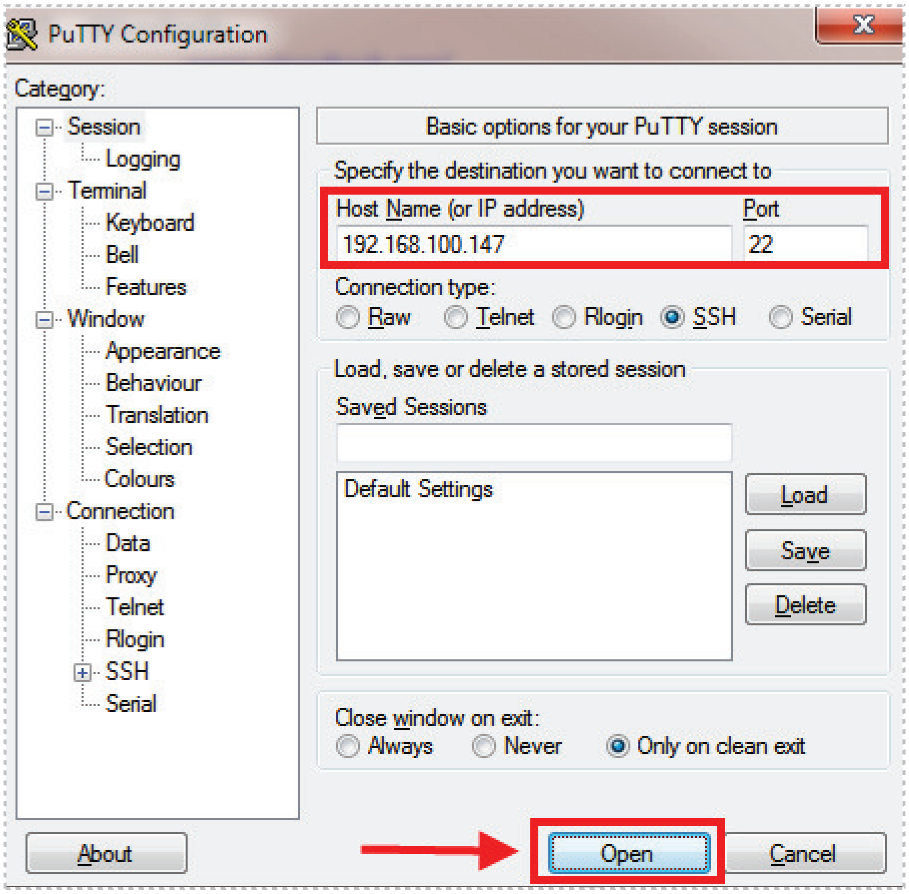
Figure 29: Launching putty.exe on the Windows 7 Machine

The PuTTY Configuration will open. Users can choose the following connection types:

- Raw
- Telnet
- Rlogin
- SSH
- Serial

PuTTY makes a great choice for Windows Vista and Windows 7 users who need to connect to Cisco devices because Windows no longer comes with HyperTerminal.

3. In the Host Name (or IP Address) box, type IP **192.168.100.147**



Host Name (or IP address): 192.168.100.147
Port: 22

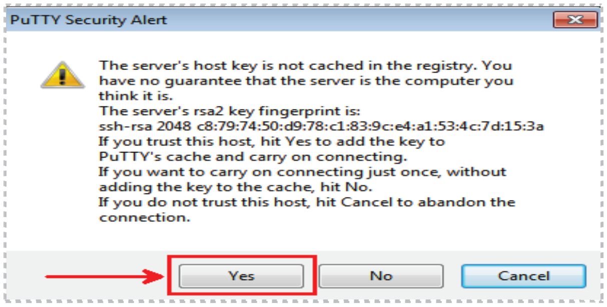
Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions:
Default Settings

Close window on exit:
○ Always ○ Never ● Only on clean exit

Figure 30: PuTTY Configuration Dialog Box

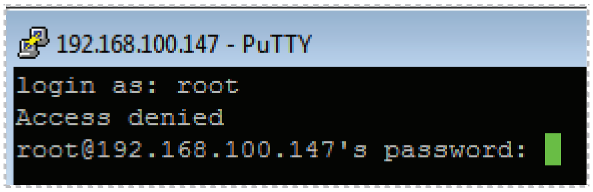
4. A PuTTY Security Alert Dialog will pop up. Click **Yes** to the Warning.



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 c8:79:74:50:d9:78:c1:83:9c:e4:a1:53:4c:7d:15:3a
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

Figure 31: Security Alert Dialog

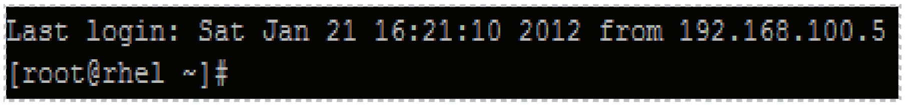
5. When you receive the login prompt, type **root**. The password is **password**. Note: the password will not appear when you type it for security reasons.



```
login as: root
Access denied
root@192.168.100.147's password:
```

Figure 32: Logging in to the Remote Machine via SSH

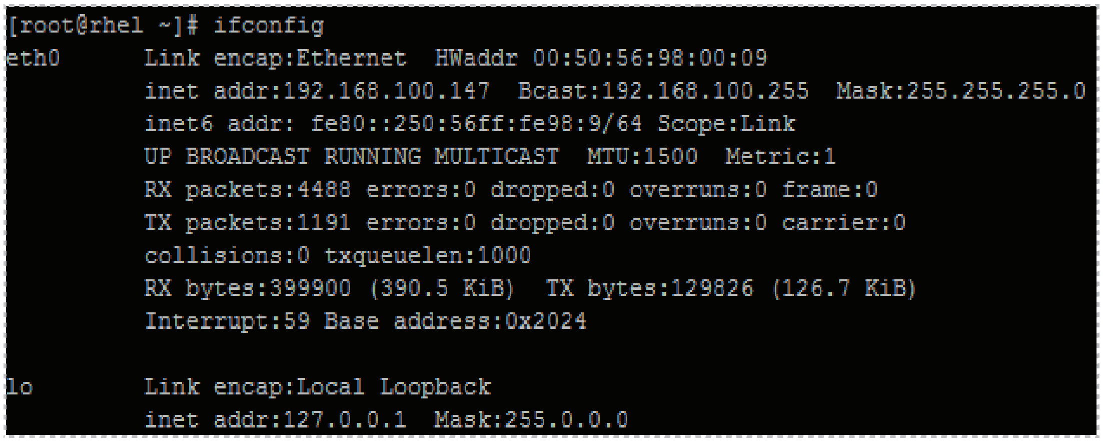
After a successful login, you will receive a *Last Login* message and a prompt.



```
Last login: Sat Jan 21 16:21:10 2012 from 192.168.100.5
[root@rhel ~]#
```

Figure 33: A Successful Login to the SSH Server Displays the Last Login Time

6. Checking the IP Address of the machine you are connecting to remotely is never a bad idea. To display IP Address information in Linux, type the following: [root@rhel ~]#**ifconfig**

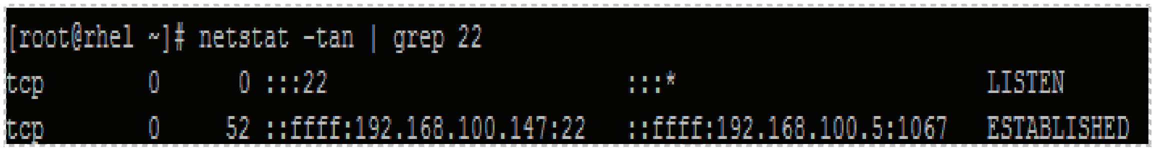


```
[root@rhel ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:98:00:09
          inet addr:192.168.100.147  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe98:9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4488 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1191 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:399900 (390.5 KiB)  TX bytes:129826 (126.7 KiB)
          Interrupt:59 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
```

Figure 34: Displaying the IP Address of the Remote Linux Machine

The first IP Address shown is for the first NIC in the system. The second is the loopback address.

7. To view the TCP secure shell (SSH) connection between the Windows 7 machine and the Linux machine, type the following command:
   [root@rhel ~]#**netstat –tan | grep 22**



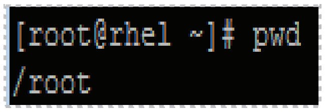
```
[root@rhel ~]# netstat -tan | grep 22
tcp        0      0 :::22                       :::*                        LISTEN
tcp        0     52 ::ffff:192.168.100.147:22   ::ffff:192.168.100.5:1067   ESTABLISHED
```

Figure 35: Viewing the Established SSH connection

The **netstat** command, which works in Windows and Linux, displays active network connections. By using the –tan switch, you will only display TCP connections. You can narrow down the output by piping the command into a GREP, Global regular Expressions Print, and using port 22. The first line of the netstat output tells you that the Linux machine is listening on port 22. The second line of the netstat output shows the established connection between the Windows 7 system with the IP Address of 192.168.100.5 and the Red Hat Linux system with the IP Address of 192.168.100.147.

To find out what directory you reside in on the Linux file system, type **pwd**. The command pwd is short for both *print working directory* and *present working directory*. The tilde (~) symbol tells you the current user is in their home directory.

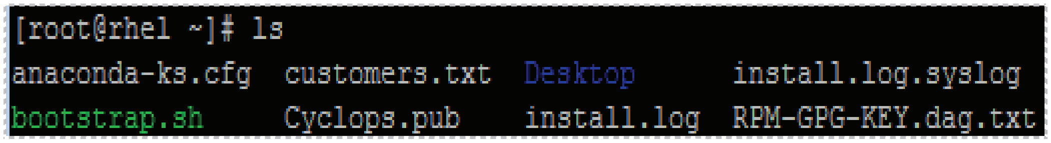
8. To view your current location on the file system in Linux, type:
   [root@rhel ~]#**pwd**



```
[root@rhel ~]# pwd
/root
```

Figure 36: Printing the Present Working Directory

9. List files in the root’s home directory by typing the following:
   [root@rhel ~]#**ls**

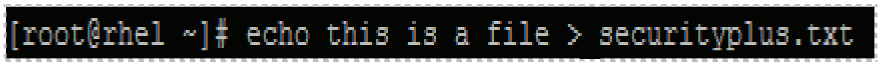


```
[root@rhel ~]# ls
anaconda-ks.cfg  customers.txt  Desktop      install.log.syslog
bootstrap.sh     Cyclops.pub    install.log  RPM-GPG-KEY.dag.txt
```

Figure 37: Using the ls command in Linux to View Files and Folders

The **ls** command usually display files as different colors than folders. Also, files with executable permissions are typically displayed using a green font color. Another common practice is to have folders start with a capital letter, although this is not a requirement.

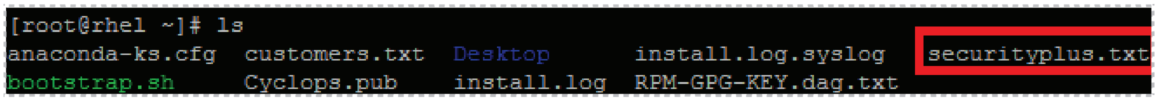
10. Creating a file in Linux can be done by using the vi editor or by using the echo command and a redirect symbol (>), like in Microsoft Windows. To make a file called **securityplus.txt** with the phrase "*this is a file*" in it, type the following:
    [root@rhel ~]#**echo this is a file > securityplus.txt**



```
[root@rhel ~]# echo this is a file > securityplus.txt
```

Figure 38: Creating a File in Linux

11. Type ls to view the created securityplus.txt file within root's home directory.
    [root@rhel ~]#**ls**

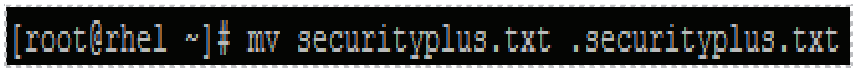


```
[root@rhel ~]# ls
anaconda-ks.cfg  customers.txt  Desktop      install.log.syslog  securityplus.txt
bootstrap.sh     Cyclops.pub    install.log  RPM-GPG-KEY.dag.txt
```

Figure 39: Displaying Files with the ls Command

In Linux, the **mv** (move) command is used to rename a file. By placing a period (.) at the beginning of a file name, that file will be hidden.

12. To hide the file, rename it using the mv command and put a period in the front.
    [root@rhel ~]#**mv securityplus.txt .securityplus.txt**

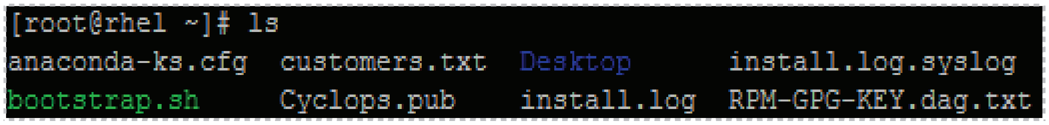


```
[root@rhel ~]# mv securityplus.txt .securityplus.txt
```

Figure 40: Renaming and Hiding a File

The file is now hidden and will not be displayed when **ls** is used without any switches.

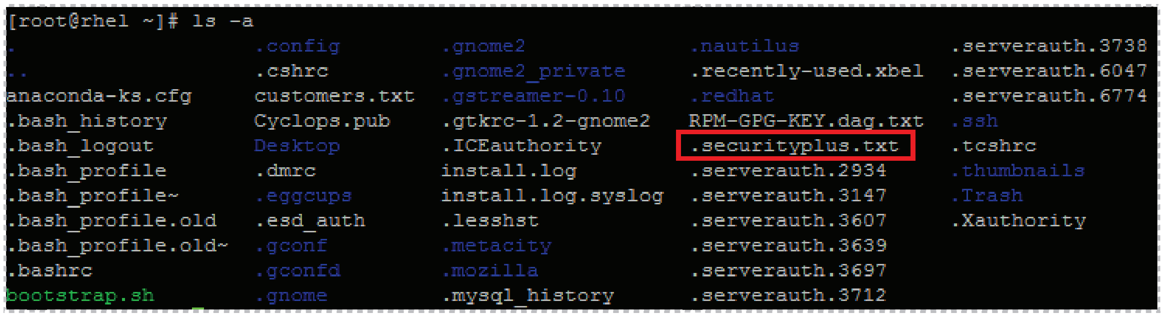
13. Type ls to see that the securityplus.txt file is no longer displayed.
    [root@rhel ~]#**ls**



```
[root@rhel ~]# ls
anaconda-ks.cfg  customers.txt  Desktop      install.log.syslog
bootstrap.sh     Cyclops.pub    install.log  RPM-GPG-KEY.dag.txt
```

Figure 41: The Hidden File is not Displayed with ls

14. To view hidden files within the root's home directory, the following:
    [root@rhel ~]#**ls -a**

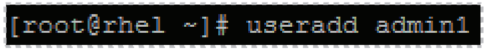


```
[root@rhel ~]# ls -a
.                   .config        .gnome2             .nautilus            .serverauth.3738
..                  .cshrc         .gnome2_private     .recently-used.xbel  .serverauth.6047
anaconda-ks.cfg     customers.txt  .gstreamer-0.10     .redhat              .serverauth.6774
.bash_history       Cyclops.pub    .gtkrc-1.2-gnome2   RPM-GPG-KEY.dag.txt  .ssh
.bash_logout        Desktop        .ICEauthority       .securityplus.txt    .tcshrc
.bash_profile       .dmrc          install.log         .serverauth.2934     .thumbnails
.bash_profile~      .eggcups       install.log.syslog  .serverauth.3147     .Trash
.bash_profile.old   .esd_auth      .lesshst            .serverauth.3607     .Xauthority
.bash_profile.old~  .gconf         .metacity           .serverauth.3639
.bashrc             .gconfd        .mozilla            .serverauth.3697
bootstrap.sh        .gnome         .mysql_history      .serverauth.3712
```

Figure 42: Displaying Hidden Files in Linux

Displaying, creating, and hiding files can be done on a remote system using SSH. The root account can also perform other tasks, such as account and service maintenance

15. To add a user to the Remote Linux system, type the following:
    [root@rhel ~]#**useradd admin1**

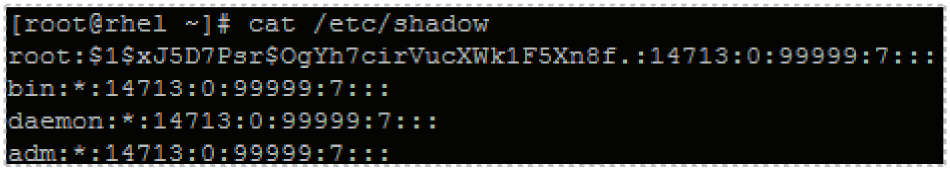


```
[root@rhel ~]# useradd admin1
```

Figure 43: Adding a User to the Remote Linux System

The **passwd** and **shadow** files in the /etc directory store the names of the users. The shadow file contains also stores the user's password hash. Linux users can cat, which stands for concatenate, to display the contents of a file like the shadow file.

16. To view the newly created user, type the following command:
    [root@rhel ~]#**cat /etc/shadow**

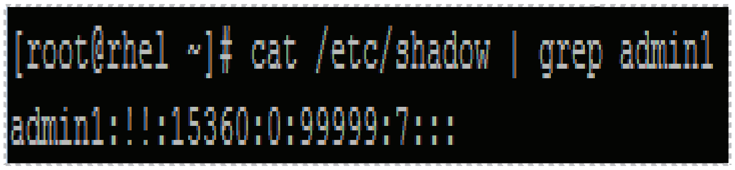


```
[root@rhel ~]# cat /etc/shadow
root:$1$xJ5D7Psr$OgYh7cirVucXWk1F5Xn8f.:14713:0:99999:7:::
bin:*:14713:0:99999:7:::
daemon:*:14713:0:99999:7:::
adm:*:14713:0:99999:7:::
```

Figure 44: Viewing the Shadow File on the Remote Linux System

Some files can contain pages of information. To narrow the display results, the grep command can be used. GREP, which stands for Global Regular Expressions Print, can be used to search for a character or a string of characters within a given output set.

17. To view the admin1 user created within the shadow file, type the following:
    [root@rhel ~]#**cat /etc/shadow | grep admin1**

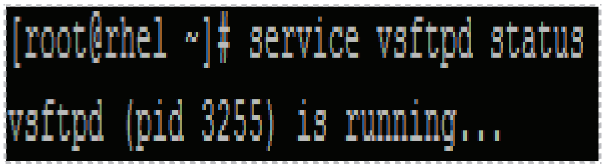


```
[root@rhel ~]# cat /etc/shadow | grep admin1
admin1:!!:15360:0:99999:7:::
```

Figure 45: Using GREP to Filter Search Results

The service command can be used to stop, start, and view server status.

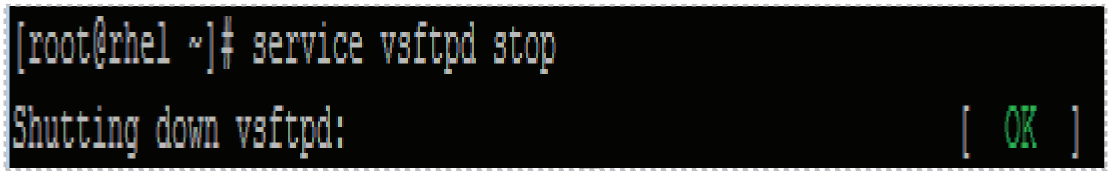
18. To view the status of the **Very Secure FTP Daemon9** (vsftpd), type the following:
    [root@rhel ~]#**service vsftpd status**



```
[root@rhel ~]# service vsftpd status
vsftpd (pid 3255) is running...
```

Figure 46: Viewing the Status of the vftpd Service

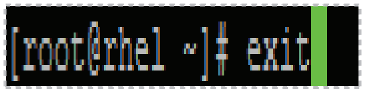
19. To stop the **vsftpd** service on the remote Linux system, type the following:
    [root@rhel ~]#**service vsftpd stop**



```
[root@rhel ~]# service vsftpd stop
Shutting down vsftpd:                                      [  OK  ]
```

Figure 47: Shutting Down the vsftpd service

20. To end the SSH session on the Remote Linux system, type the following:
    [root@rhel ~]#**exit**



```
[root@rhel ~]# exit
```

Figure 48: Typing Exit to Leave the SSH Session

The PuTTY Window will close and the SSH session will be terminated.

Task 2.2 Conclusion

Secure Shell, or SSH, allows users to remotely connect and administer computers running the Linux, Unix, and Mac operating systems as well other network devices such as routers and switches. Secure Shell encrypts the traffic, unlike TELNET, so the usernames, passwords, and commands will not be visible to anyone inspecting network traffic. It is strongly recommended that SSH be used instead of TELNET when possible.

Task 2.3 Discussion Questions

1. What port does Secure Shell use?
2. Is there a native SSH client or server on Microsoft Windows system?
3. What is the file in Linux that contains the password hash?
4. What are two methods that can be used for creating a file during a remote secure shell (SSH) connection within Linux?

Task 3 Analyzing Remote Connections in Network Traffic

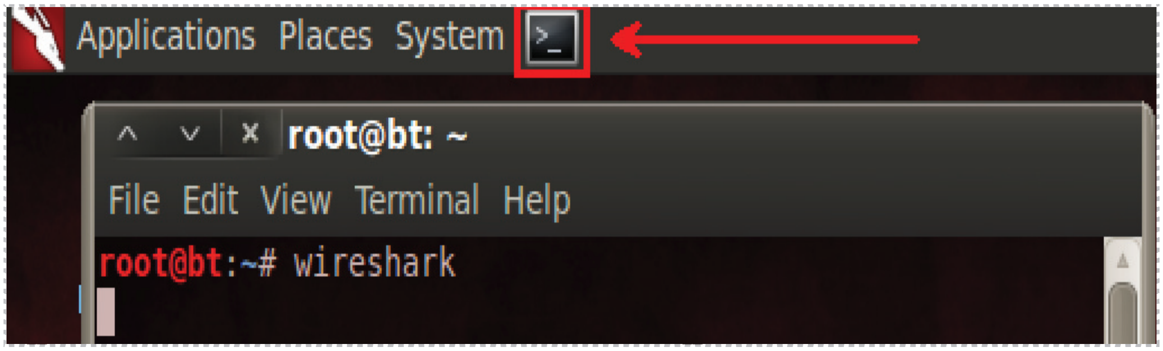
In this section, you will analyze a network capture file with TELNET and SSH traffic. You will be able to view the clear text communication during the TELNET session, but you will be unable to view the encrypted communication of the SSH connection.

Task 3.1 Using Wireshark to Connect to a Remote Linux System

Wireshark is a protocol analyzer, which will allow you to inspect and capture network traffic. The 32-bit and 64-bit versions can be downloaded from www.wireshark.org.

Open a Terminal to Get Started

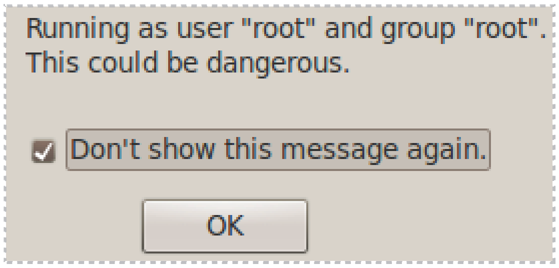
1. Open a terminal on the BackTrack 5 system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen. Type **wireshark** (all lowercase) to bring up the Wireshark program.



```
root@bt:~# wireshark
```

Figure 49: The Terminal Windows within BackTrack

2. If you receive a message about running Wireshark as root can be dangerous, click the button that says **Don't show this message again**, and click **OK**.

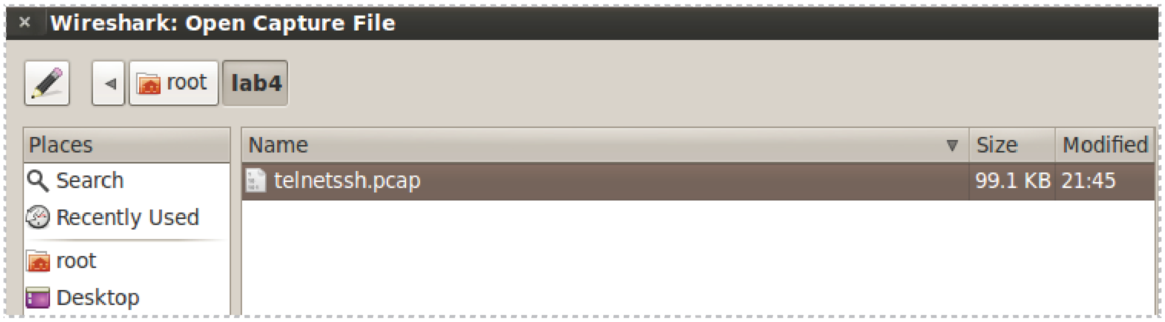


Running as user "root" and group "root". This could be dangerous.

☑ Don't show this message again.

Figure 50: Allow Wireshark to run as root

3. Select **file** from the Wireshark menu and select **open**. Double click on the **root** folder, then double click on the **lab4** folder. Double click on the file **telnetssh.pcap**



Name	Size	Modified
telnetssh.pcap	99.1 KB	21:45

Figure 51: Opening the Wireshark file

Examining TELNET traffic can be done by using either of the two filters within Wireshark:

- telnet
- tcp.port == 23

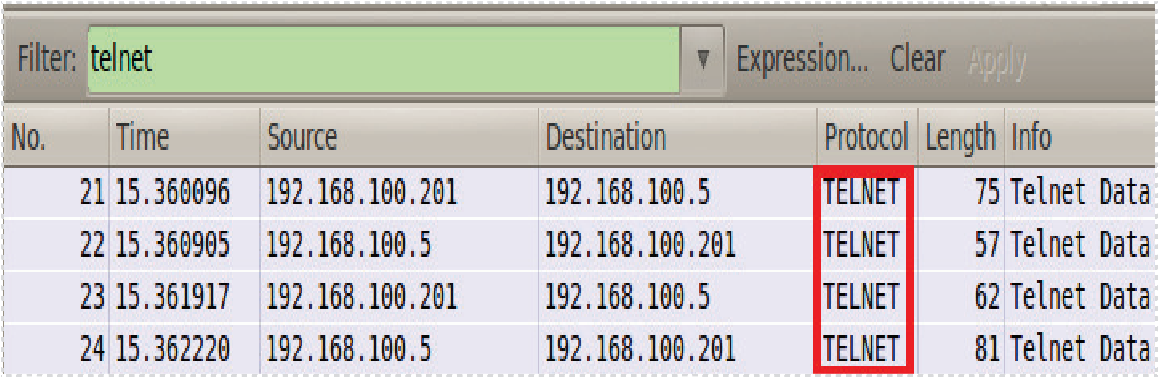
If TELNET is used on a Windows system, the following filter can be used (case sensitive):

- frame contains Microsoft Windows

Examining SSH traffic can be done by using either of the two filters within Wireshark:

- ssh
- tcp.port == 22

4. To examine the TELNET traffic, type telnet in the filter pane and click **Apply**.

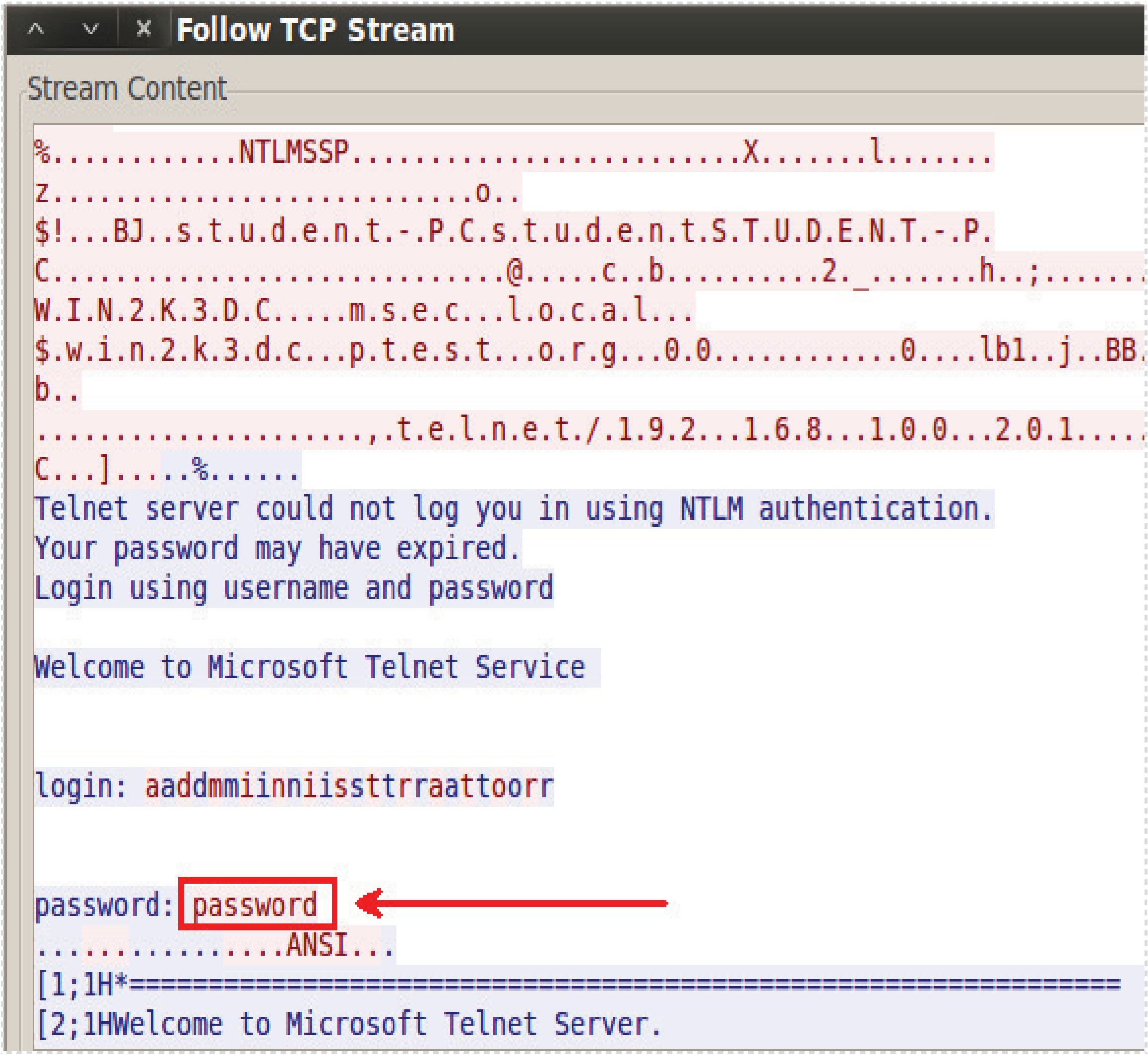


Filter: telnet

No.	Time	Source	Destination	Protocol	Length	Info
21	15.360096	192.168.100.201	192.168.100.5	TELNET	75	Telnet Data
22	15.360905	192.168.100.5	192.168.100.201	TELNET	57	Telnet Data
23	15.361917	192.168.100.201	192.168.100.5	TELNET	62	Telnet Data
24	15.362220	192.168.100.5	192.168.100.201	TELNET	81	Telnet Data

Figure 52: The telnet Filter in the Wireshark Pane

5. Right click on the first frame in the list and select **Follow TCP Stream**.



```
%...........NTLMSSP........................X.......l.......
z..........................o..
$!...BJ..s.t.u.d.e.n.t.-.P.C.s.t.u.d.e.n.t.S.T.U.D.E.N.T.-.P.
C...........................@.....c..b.........2._.......h..;.......
W.I.N.2.K.3.D.C.....m.s.e.c...l.o.c.a.l...
$.w.i.n.2.k.3.d.c...p.t.e.s.t...o.r.g...0.0...........0....lb1..j..BB.
b..
.....................,.t.e.l.n.e.t./.1.9.2...1.6.8...1.0.0...2.0.1....
C...].....%......
Telnet server could not log you in using NTLM authentication.
Your password may have expired.
Login using username and password

Welcome to Microsoft Telnet Service


login: aaddmmiinniissttrraattoorr


password: password
................ANSI...
[1;1H*==========================================================
[2;1HWelcome to Microsoft Telnet Server.
```

Figure 53: Following a TCP Stream

You can scroll down through the conversation to try to interpret what was happening. Notice how you can view the traffic because TELNET transmits in clear text. Both sides of the conversation between the TELNET server and client are displayed. To see a specific side of the conversation, click the arrow to the right of Entire conversation.

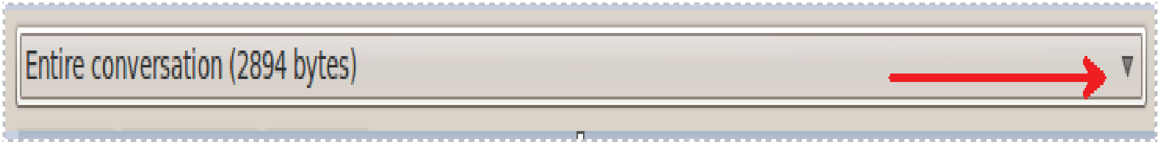
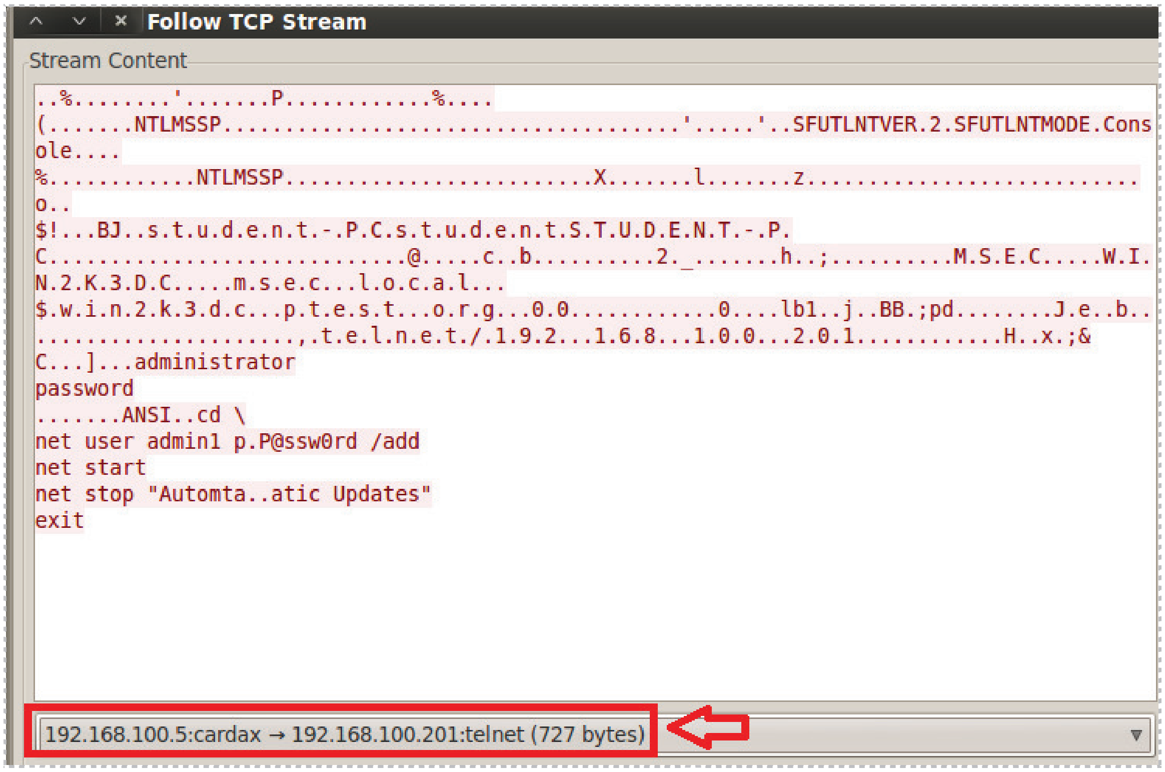


Figure 54: The telnet Filter in the Wireshark Pane

6. Select the conversation from the client with the IP Address of 192.168.100.5 to the telnet server of 192.168.100.201 by clicking the arrow to the right of **Entire conversation**, and selecting the first conversation in the drop box.



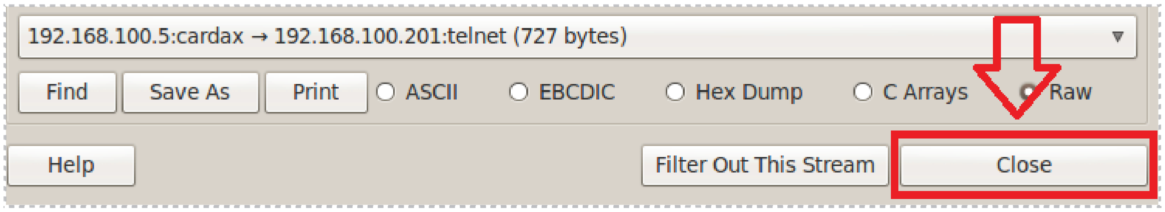
```
..%........'.......P............%....
(.......NTLMSSP.....................................'.....'..SFUTLNTVER.2.SFUTLNTMODE.Cons
ole....
%............NTLMSSP.........................X.......l.......z...........................
o..
$!...BJ..s.t.u.d.e.n.t.-.P.C.s.t.u.d.e.n.t.S.T.U.D.E.N.T.-.P.
C.............................@....c..b.........2._.......h..;.........M.S.E.C.....W.I.
N.2.K.3.D.C.....m.s.e.c...l.o.c.a.l...
$.w.i.n.2.k.3.d.c...p.t.e.s.t...o.r.g...0.0...........0....lb1..j..BB.;pd........J.e..b..
......................,.t.e.l.n.e.t./.1.9.2...1.6.8...1.0.0...2.0.1...........H..x.;&
C...]...administrator
password
.......ANSI..cd \
net user admin1 p.P@ssw0rd /add
net start
net stop "Automta..atic Updates"
exit
```

192.168.100.5:cardax → 192.168.100.201:telnet (727 bytes)

Figure 55: The Commands Sent to the TELNET Server

The client sent the username of *administrator* and password of *password* to the TELNET server. The client sent the command to add a user called *admin1* with the password of *P@ssw0rd*. The client also sent a net start command to the server to list the services, and then stopped the Automatic Updates service. The session terminated with the command exit. Viewing the details of this conversation illustrates why the use of TELNET should not be avoided. When SSH traffic is examined, it will be unreadable.

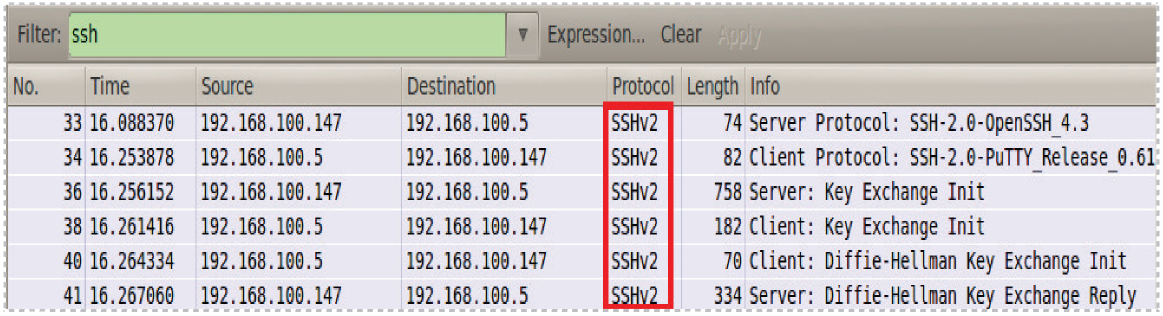
7. Click the **Close** button in the bottom right of Wireshark to close the TCP stream.


192.168.100.5:cardax → 192.168.100.201:telnet (727 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

Figure 56: Closing the TCP Stream

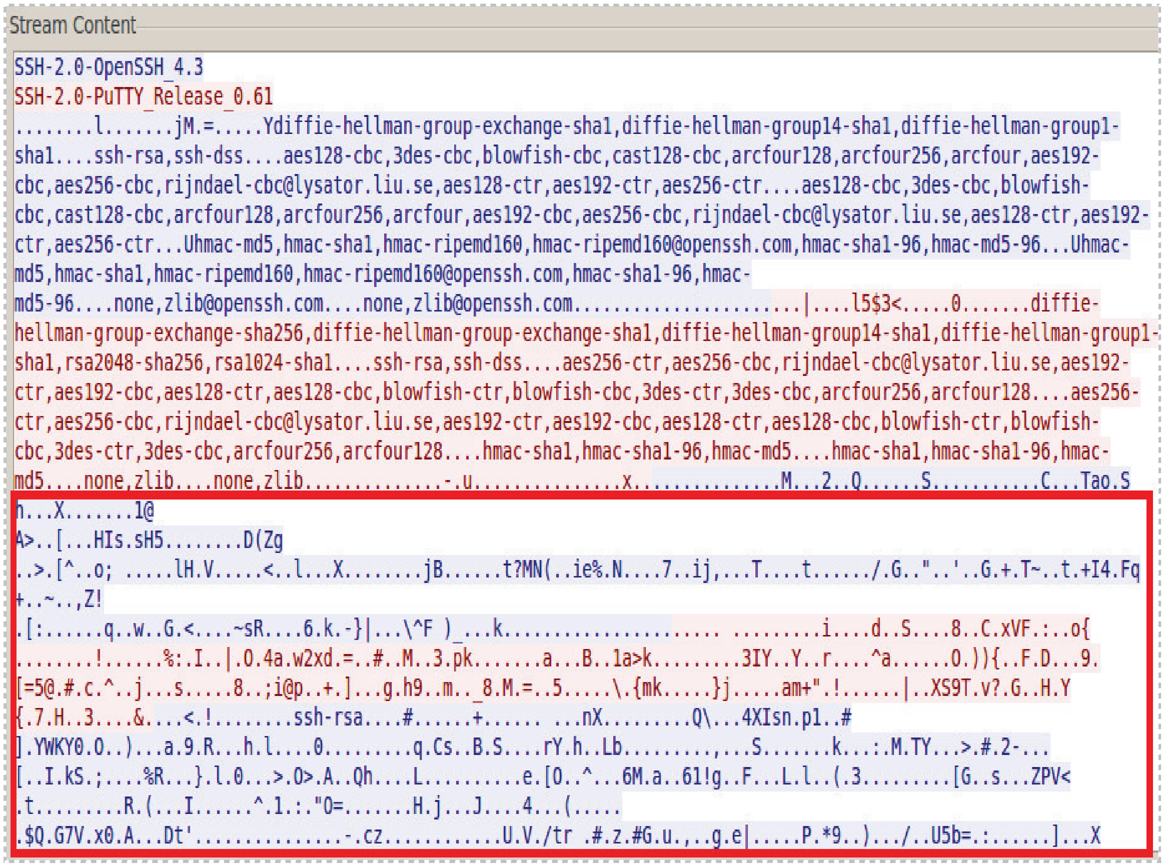
8. In the Wireshark filter Pane, type **ssh** then click the Apply button.



No.	Time	Source	Destination	Protocol	Length	Info
33	16.088370	192.168.100.147	192.168.100.5	SSHv2	74	Server Protocol: SSH-2.0-OpenSSH_4.3
34	16.253878	192.168.100.5	192.168.100.147	SSHv2	82	Client Protocol: SSH-2.0-PuTTY_Release_0.61
36	16.256152	192.168.100.147	192.168.100.5	SSHv2	758	Server: Key Exchange Init
38	16.261416	192.168.100.5	192.168.100.147	SSHv2	182	Client: Key Exchange Init
40	16.264334	192.168.100.5	192.168.100.147	SSHv2	70	Client: Diffie-Hellman Key Exchange Init
41	16.267060	192.168.100.147	192.168.100.5	SSHv2	334	Server: Diffie-Hellman Key Exchange Reply

Figure 57: Viewing SSH Traffic

9. Right click on the first frame in the list and select *Follow TCP Stream*.



```
SSH-2.0-OpenSSH_4.3
SSH-2.0-PuTTY_Release_0.61
........l.......jM.=.....Ydiffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-
sha1....ssh-rsa,ssh-dss....aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes192-
cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr....aes128-cbc,3des-cbc,blowfish-
cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-
ctr,aes256-ctr...Uhmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96...Uhmac-
md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-
md5-96....none,zlib@openssh.com....none,zlib@openssh.com......................|....l5$3<.....0.......diffie-
hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-
sha1,rsa2048-sha256,rsa1024-sha1....ssh-rsa,ssh-dss....aes256-ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-
ctr,aes192-cbc,aes128-ctr,aes128-cbc,blowfish-ctr,blowfish-cbc,3des-ctr,3des-cbc,arcfour256,arcfour128....aes256-
ctr,aes256-cbc,rijndael-cbc@lysator.liu.se,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,blowfish-ctr,blowfish-
cbc,3des-ctr,3des-cbc,arcfour256,arcfour128....hmac-sha1,hmac-sha1-96,hmac-md5....hmac-sha1,hmac-sha1-96,hmac-
md5....none,zlib....none,zlib.............-.u..............x..............M...2..Q.....S..........C...Tao.S
h...X.......1@
A>..[...HIs.sH5........D(Zg
..>.[^..o; .....lH.V.....<..l...X........jB......t?MN(..ie%.N....7..ij,...T....t...../.G.."..'..G.+.T~..t.+I4.Fq
+..~..,Z!
.[:......q..w..G.<....~sR....6.k.-}|...\^F )_...k....................... .........i....d..S....8..C.xVF.:..o{
........!......%:.I..|.0.4a.w2xd.=..#..M..3.pk.......a...B..1a>k.........3IY..Y..r....^a......0.)){..F.D...9.
[=5@.#.c.^..j...s.....8..;i@p..+.]...g.h9..m.._8.M.=..5.....\.{mk.....}j.....am+".!......|..XS9T.v?.G..H.Y
{.7.H..3....&....<.!........ssh-rsa....#......+...... ...nX.........Q\...4XIsn.pl..#
].YWKY0.O..)...a.9.R...h.l....0.........q.Cs..B.S....rY.h..Lb.........,...S.......k...:.M.TY...>.#.2-...
[..I.kS.;....%R...}.l.0...>.O>.A..Qh....L..........e.[0..^...6M.a..61!g..F...L.l..(.3.........[G..s...ZPV<
.t.........R.(...I......^.1.:."O=.......H.j...J....4...(.....
.$Q.G7V.x0.A...Dt'...............-.cz............U.V./tr .#.z.#G.u.,..g.e|.....P.*9..).../..U5b=.:......]...X
```

Figure 58: Viewing the Encrypted SSH Communication

Although you are able to see the names of ciphers used for encrypting the SSH session, you will not be able to see any of the communication between the client and server. Click the **Close** Button in the bottom right of Wireshark to close the TCP stream.

10. Close all open windows and terminals.

Task 3.2 Conclusion

TELNET uses TCP port 23 and sends everything over the network in clear text. When examining TELNET traffic, you are able to see usernames, passwords, and commands. Secure Shell (SSH) uses TCP port 22 and provides a secure channel for remote administration tasks. Examining SSH traffic provides you with no details of what occurred during the session between the SSH client and the SSH server.

Task 3.3 Discussion Questions

1. Type **frame contains PuTTY** in the Wireshark filter pane and click Apply. Determine which version of PuTTY is in use.
2. If you type **frame contains shadow** in the Wireshark filter pane, why are there no results in the root account viewed the shadow file remotely?

Type **frame contains "Microsoft Windows"** in the Wireshark filter pane and click Apply. Right click on the first frame and select *Follow TCP Stream* to answer questions 3 and 4.

3. Name a user account that was displayed in the clear text traffic.
4. Name the file that was created, and then hidden.

5 References

1. SSH MAN Page:
   http://linux.die.net/man/1/ssh

2. Wireshark:
   www.wireshark.org/

3. PuTTY home Page:
   http://www.chiark.greenend.org.uk/~sgtatham/putty/

4. BackTrack Linux:
   http://www.backtrack-linux.org/

5. Telnet Commands for Windows:
   http://technet.microsoft.com/en-us/library/c.aspx