



## Ethical Hacking Lab Series

### Lab 2: Conducting Active and Passive Reconnaissance against a Target

**Certified Ethical Hacking Domains:**  
Introduction to Ethical Hacking,  
Footprinting and Reconnaissance,  
Scanning Networks,  
Social Engineering

**Document Version: 2013-07-18 (Beta)**

**Organization:** Moraine Valley Community College  
**Author:** Jesse Varsalone

**Copyright © National Information Security, Geospatial Technologies Consortium (NISGTC)**

The development of this document is 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 work is licensed under the Creative Commons Attribution 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.



*The Center for Systems Security and Information Assurance (CSSIA), in partnership with the Network Development Group (NDG) is given a perpetual worldwide waiver to distribute per US Law this lab and future derivatives of these works.*

## Contents

Introduction .....	3
Domains: Introduction to Ethical Hacking, Footprinting and Reconnaissance, Scanning Networks, Social Engineering .....	3
Pod Topology .....	4
Lab Settings .....	5
1 Performing External Active Reconnaissance .....	6
1.1 Performing Active Reconnaissance Against an External Target .....	6
1.2 Conclusion .....	17
1.3 Discussion Questions.....	17
2 Performing Internal Active Reconnaissance.....	18
2.1 Performing an Internal Scan.....	18
2.2 Conclusion .....	25
2.3 Discussion Questions.....	25
3 Performing Internal and External Passive Reconnaissance .....	26
3.1 Passive Reconnaissance Using tcpdump and Wireshark .....	26
3.2 Conclusion .....	29
3.3 Discussion Questions.....	29
References .....	30

## Introduction

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, students will perform passive and active reconnaissance on systems.

This lab includes the following tasks:

- 1 – Performing External Active Reconnaissance
- 2 – Performing Internal Active Reconnaissance
- 3 – Performing Internal and External Passive Reconnaissance

## Domains: Introduction to Ethical Hacking, Footprinting and Reconnaissance, Scanning Networks, Social Engineering

Hackers will use various tools to find hosts on the network. After hosts are discovered and detailed information is gathered, the next step usually involves attacking systems.

**Nmap** – Nmap is a program that can be used in Linux, Mac, or Windows to locate machines on a network. After Nmap is used to discover machines on a network, it can also be utilized to determine which Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports the machine has open. Nmap will give an indication of the operating system the remote machine is using. Zenmap is a GUI frontend for Nmap.

**Metasploit** – Metasploit is an exploitation framework. Version 3 of Metasploit is written in Ruby and has exploits for Microsoft Windows, Mac OS X, Linux, and UNIX. Some exploits are for the operating systems themselves and others are for application software like Adobe Reader and Internet Explorer. There is a detailed description of each exploit, which explains which version of the operating system, or application software is vulnerable.

**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.

**Armitage** – Metasploit is a very powerful exploitation framework but it requires that the user be comfortable using the command line. Armitage is a GUI frontend for Metasploit that has many powerful capabilities. An attacker can use Armitage to identify and exploit victim machines within an easy to use graphical environment.

## Pod Topology

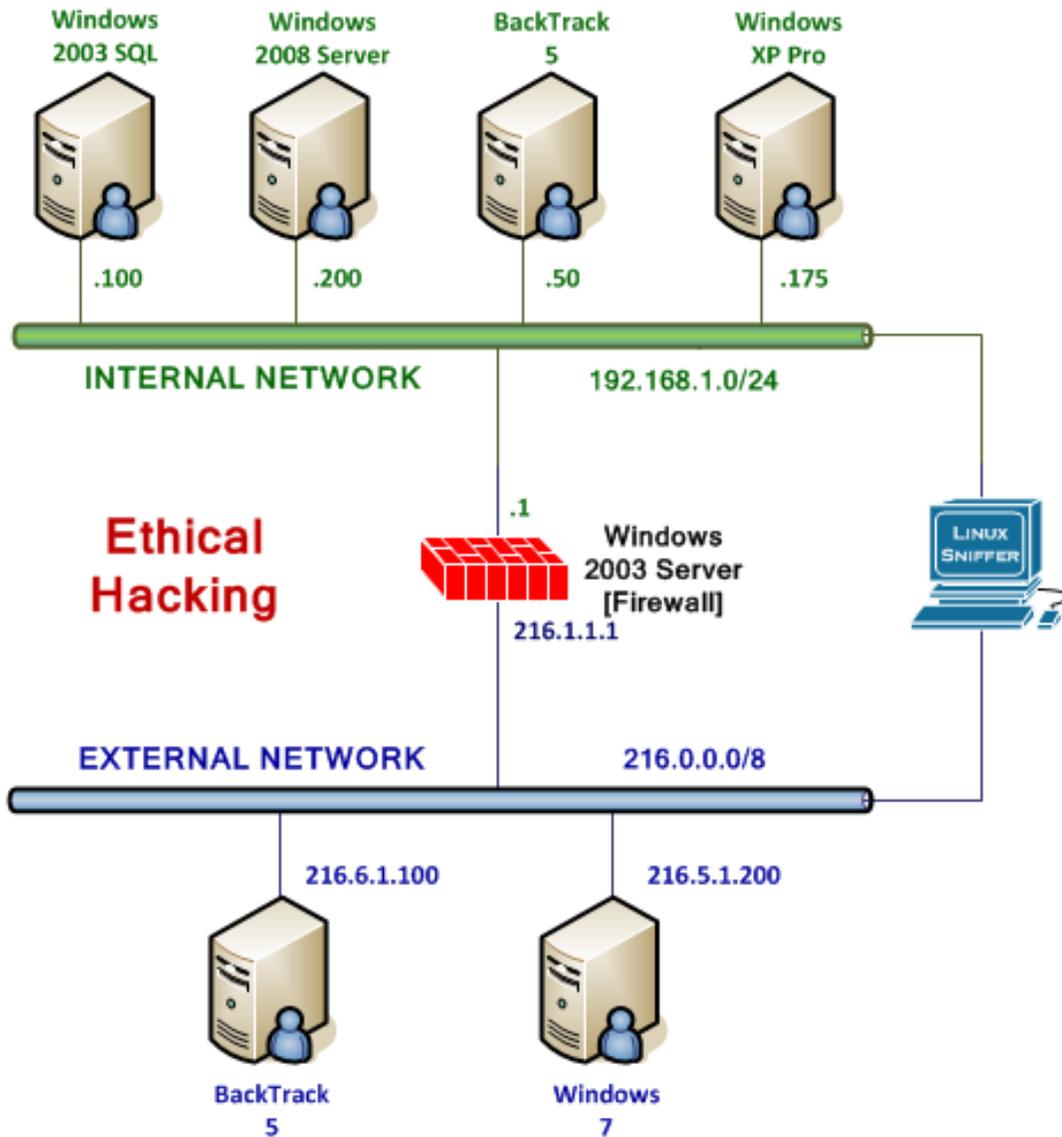


Figure 1: Lab Topology

## 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.

### Required Virtual Machines and Applications

This lab requires the use of the Linux Internal and External BackTrack 5 R3 machines.

External BackTrack 5	216.6.1.100
External BackTrack 5 <b>root</b> password	toor
Internal BackTrack 5	192.168.1.50
Internal BackTrack 5 <b>root</b> password	toor
Windows 2003 SQL	192.168.1.100
Windows 2003 <b>Administrator</b> password	P@ssw0rd

## 1 Performing External Active Reconnaissance

The purpose of performing active reconnaissance against an external target is to learn about the configuration of the systems connected to the Internet. Active Reconnaissance can provide information including which ports are open, the target operating system, as well as the version of the web server software the site is utilizing.

Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

### 1.1 Performing Active Reconnaissance Against an External Target

1. Open the *External BackTrack 5* attack machine, running BackTrack Linux (version 5 R3), type **root** for the login and **toor** for the password.

```
bt login: root
Password:
Last login: Thu Jan 24 11:19:02 EST 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

System information as of Fri Feb 22 09:04:41 EST 2013

System load: 0.12           Memory usage: 4%    Processes:      69
Usage of /:  57.9% of 19.06GB  Swap usage:  0%    Users logged in: 0

Graph this data and manage this system at https://landscape.canonical.com/
root@bt:~# _
```

Figure 2: Logging in as root

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

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

Figure 3: The startx command

3. Open a terminal on the Linux system by clicking on the picture to the right of the word **System** in the taskbar at the top of the screen in BackTrack 5 R3.

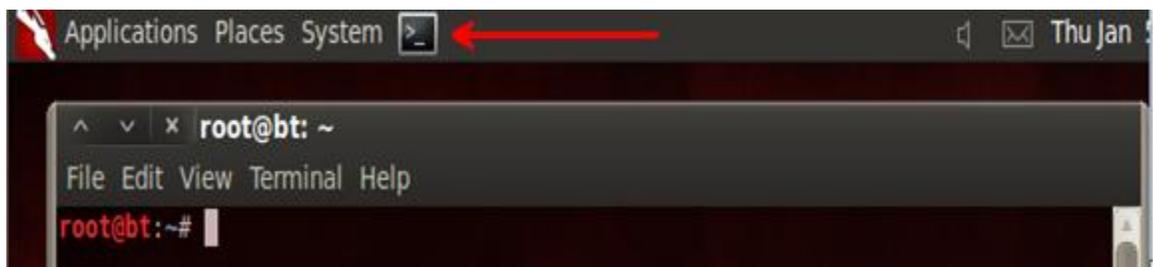


Figure 4: The Linux Terminal

Before we start scanning, it is important to know some information about how networks attached to the Internet commonly function. Our attack machine is using a Public IP address of 216.6.1.100 and the organization we are scanning has a public IP address of 216.1.1.1. The Firewall machine itself does not have any webserver software installed. Web services, such as FTP or HTTP, are actually running on the Windows 2003 SQL server, not the Firewall itself. When requests come in for those services, the firewall redirects those requests to the Windows 2003 SQL server running on the internal network. So, even though the Windows 2003 SQL server is not directly connect to the Internet, users from the Internet can utilize services on the machine because of the firewall redirection.

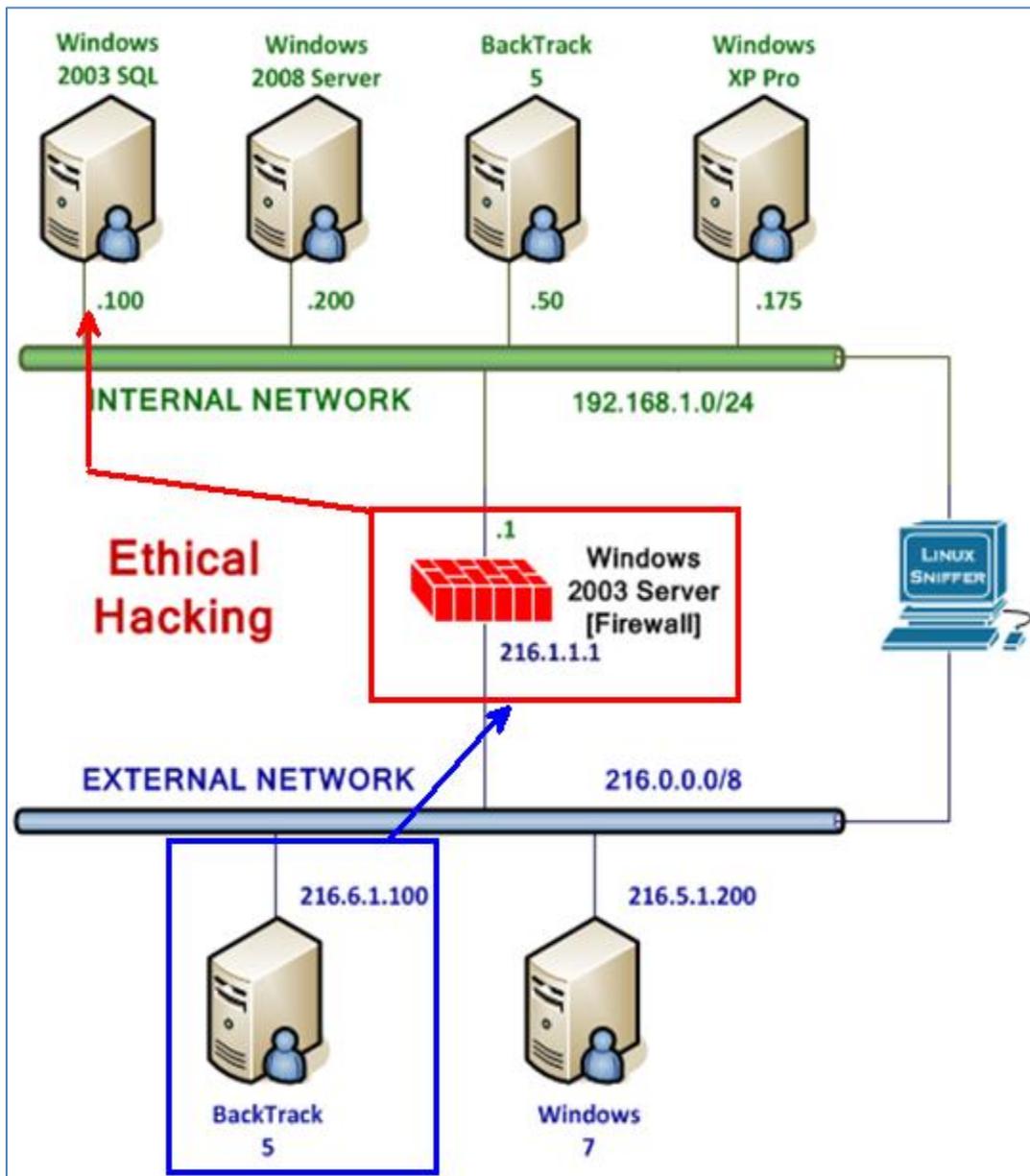


Figure 5: Diagram Explaining Firewall Redirection

Before you start scanning a system, you can perform a banner grab against the target. A banner grab is nothing more than connecting to a remote IP address and a corresponding port. You can use telnet or netcat to perform a banner grab. Note: If you are using Windows Vista, 7, or 8, the telnet client needs to be installed in Programs and Features.

An example using telnet to grab a banner by connecting to a port on a remote system:



Figure 6: Example Banner Grab

Here is a list of common ports that you can try to connect to when you grab banners.

Service Name	Port Number
File Transfer Protocol (FTP)	21
Secure Shell (SSH)	22
Simple Mail Transfer Protocol (SMTP)	25
Hyper Text Transfer Protocol (HTTP)	80
Post Office Protocol Version 3 (POP3)	110
Secure Hyper Text Transfer Protocol (HTTPS)	443
Remote Desktop Protocol (RDP)	3389

4. Type the following to determine if port 21 is open on the remote system:  
**root@bt:~# telnet 216.1.1.1 21**

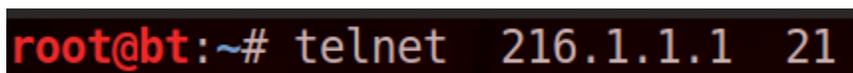


Figure 7: Determining if Port 21 is Open on the Remote System

5. The following message below will appear, indicating that the port is open and that the system is utilizing a Microsoft FTP Service. Type **quit** to end the session.

```
root@bt:~# telnet 216.1.1.1 21
Trying 216.1.1.1...
Connected to 216.1.1.1.
Escape character is '^]'.
220 Microsoft FTP Service
quit
221 See you later
Connection closed by foreign host.
```

Figure 8: A Banner Message Appears

6. Type the following to determine if port 22 is open on the remote system:

```
root@bt:~# telnet 216.1.1.1 22
```

```
root@bt:~# telnet 216.1.1.1 22
Trying 216.1.1.1...
telnet: Unable to connect to remote host: Connection timed out
```

Figure 9: The port is closed

The port is closed on the remote system, so we receive a connection time out message.

7. Type the following to determine if port 25 is open on the remote system:

```
root@bt:~# telnet 216.1.1.1 25
```

```
root@bt:~# telnet 216.1.1.1 25
Trying 216.1.1.1...
Connected to 216.1.1.1.
Escape character is '^]'.
220 server.XYZCOMPANY.COM Microsoft ESMTMP MAIL Service, Version: 6.0.3790.0
ready at Fri, 22 Feb 2013 10:05:56 -0500
quit
221 2.0.0 server.XYZCOMPANY.COM Service closing transmission channel
Connection closed by foreign host.
```

Figure 10: Determining if Port 25 is Open on the Remote System

A simple Google search of Microsoft ESMTMP MAIL Service, Version: 6.0.3790.0 indicates that the system is likely running Microsoft Exchange Server 2003, which it actually is.

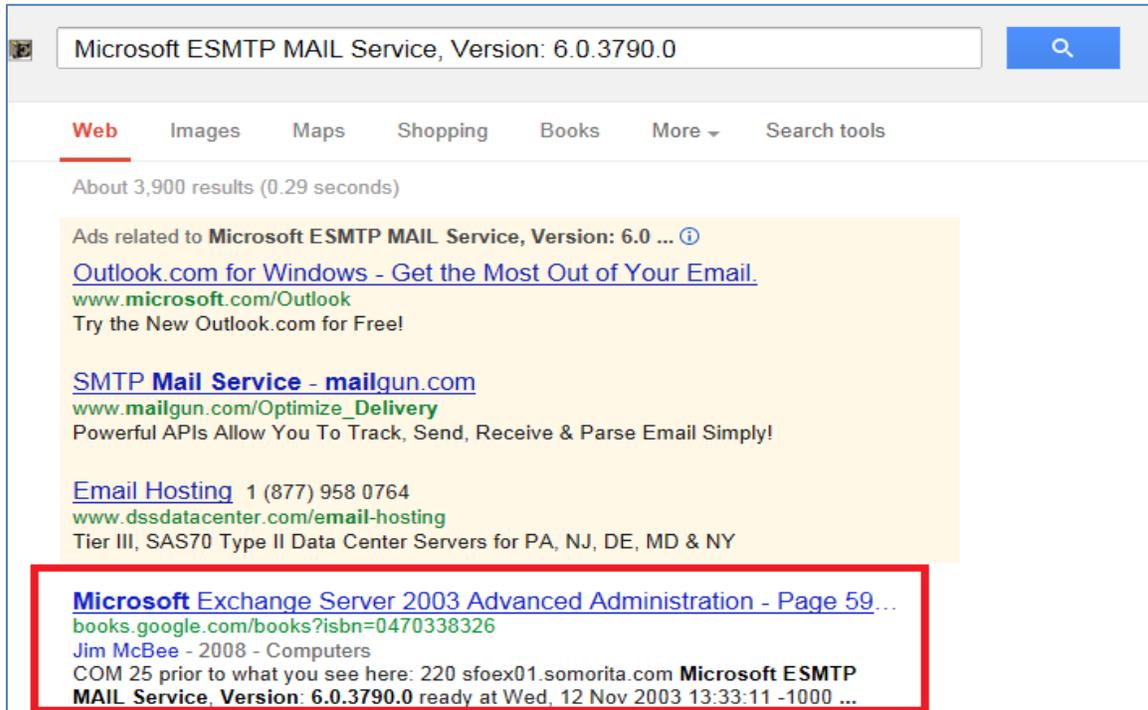


Figure 11: Googling the Banner Message

It is also important to know that banner grabbing is not just something that works in this isolated NETLAB+ environment, it is a technique that is used by people working in the field, such as network administrators, to test connectivity to a port on a remote system.

When you work in IT, you sometimes become the de facto help desk for your family. For instance, my sister called me and reported that she could not send email messages. So, I performed a banner grab to test to see if her ISP's mail server was functioning.

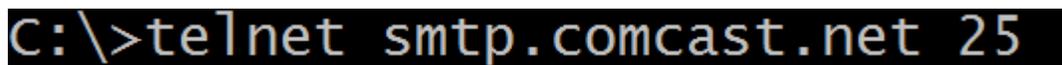


Figure 12: Banner Grab

At that moment, the port was closed. I advised her to tell the help desk that the SMTP server was down. After she called, they had it back up and running quickly. When I try to perform a banner grab several minutes later, the port responded fine.

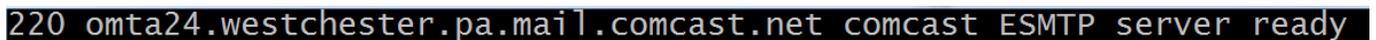


Figure 13: SMTP Banner

8. Type the following to determine if port 80 is open on the remote system:  
root@bt:~# telnet 216.1.1.1 80

```
root@bt:~# telnet 216.1.1.1 80
Trying 216.1.1.1...
Connected to 216.1.1.1.
Escape character is '^]'.

```

Figure 14: Determining if Port 80 is Open on the Remote System

9. While connected to the remote system, type the following to get a response, **hit enter twice after the command**:  
HEAD / HTTP/1.0 <enter> <enter>

```
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 1432
Content-Type: text/html
Content-Location: http://192.168.1.100/Default.htm
Last-Modified: Tue, 08 Jan 2013 02:16:10 GMT
Accept-Ranges: bytes
ETag: "2691da1f46edcd1:100c"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Fri, 22 Feb 2013 15:49:26 GMT
Connection: close

Connection closed by foreign host.

```

Figure 15: Port 80 is Open

Notice that several things are reported during the banner grab of port 80, including:

Server Response	What This Indicates
Server: Microsoft-IIS/6.0	The Version of Internet Information Services that is Running
http://192.168.1.100/Default.htm	The Internal IP address in Use
X-Powered-By: ASP.NET	Active Server Pages (ASP) are in use
Last-Modified: Tue, 08 Jan 2013	Last Modified Date of the Webpage

Banner grabbing allows you to determine if a port is open and possibly reveal information about the application and operating system software. And, it will also leave a much smaller footprint than when a scan is performed with a tool like Nmap or Zenmap.

10. Type the following command to scan the remote system using Nmap:

```
root@bt:~# nmap 216.1.1.1

Starting Nmap 6.01 ( http://nmap.org ) at 2013-02-22 13:32 EST
Nmap scan report for 216.1.1.1
Host is up (0.00045s 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: 00:0C:29:31:57:28 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 25.83 seconds
```

Figure 16: The Results of the Nmap

Keep in mind a few things about this Nmap scan you performed against 216.1.1.1:

- Nmap without any switches will work against machines blocking ICMP.
- A default Nmap scan will scan a large amount of the ports (not all).
- When you scan a machine that is on the Internet, you will not see a MAC address.

Notice that only the following 5 ports are open:

Port Number	Service
21	File Transfer Protocol (FTP)
23	TELNET
25	Simple Mail transfer Protocol (SMTP)
80	Hyper Text Transfer Protocol (HTTP)
110	Post Office Protocol Version 3 (POP3)

11. Type the following command to open Zenmap, the GUI front-end for Nmap:

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

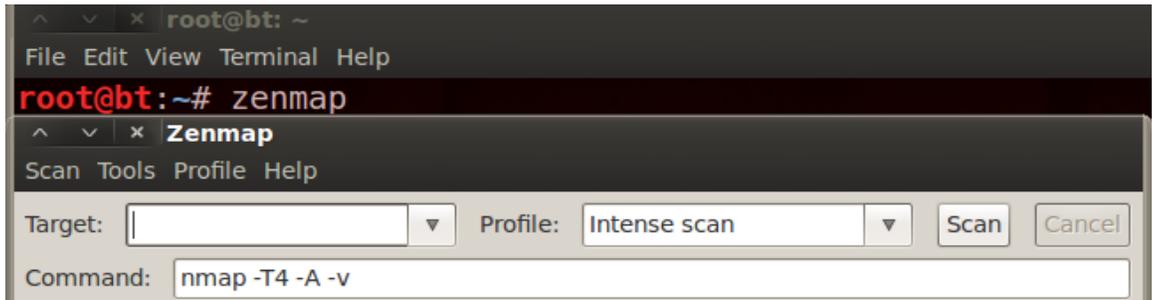


Figure 17: Open Zenmap

12. In the target box, type the public IP address for XYZcompany: 216.1.1.1. Click **Scan**.

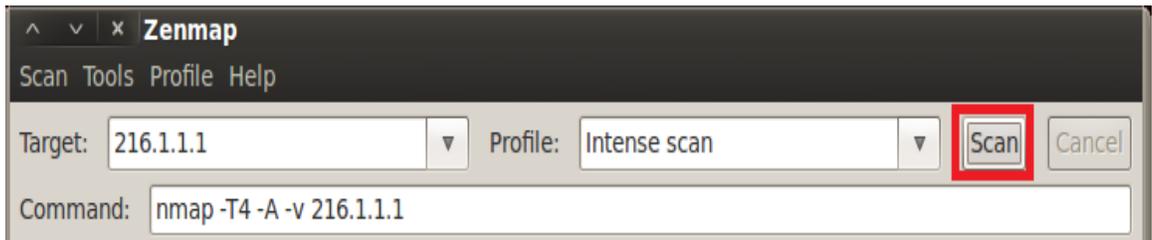


Figure 18: The Target IP

13. After the scan is completed, click on the **Ports/Hosts** tab to view the open ports.

	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	Microsoft ftpd
✓	23	tcp	open	telnet	Microsoft Windows XP telnetd
✓	25	tcp	open	smtp	Microsoft ESMTP 6.0.3790.0
✓	80	tcp	open	http	Microsoft IIS httpd 6.0
✓	110	tcp	open	pop3	MS Exchange 2003 pop3d 6.5.

Figure 19: Open Ports

Notice that the banner message is displayed in the version column of Zenmap. To demonstrate how a scan with Zenmap is much noisier than a simple banner grab, we will log on to the Windows server and check the log files for artifacts.

14. Log on to the **Windows 2003 SQL** machine. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer). Log on with the username **Administrator** and the password **P@ssw0rd**.



Figure 20: Send Ctrl-Alt-Del to the Windows 2003 Server

15. Click on **My Computer** on the Start Menu.



Figure 21: My Computer

16. Double-click on Local Disk (C:)



Figure 22: Local Disk (C:)

17. Double-click on the Windows directory.

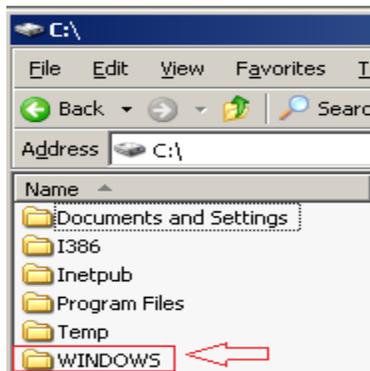


Figure 23: Windows Directory

18. Double click on the System32 directory.

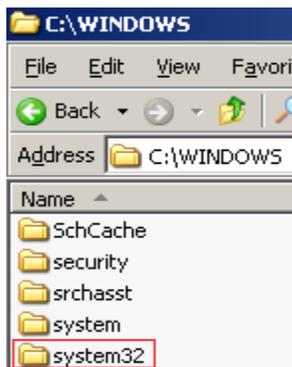


Figure 24: System32 Directory

19. Double-click on the Logfiles directory.



Figure 25: The Logfiles folder in System32

20. Double-click on W3SVC1.

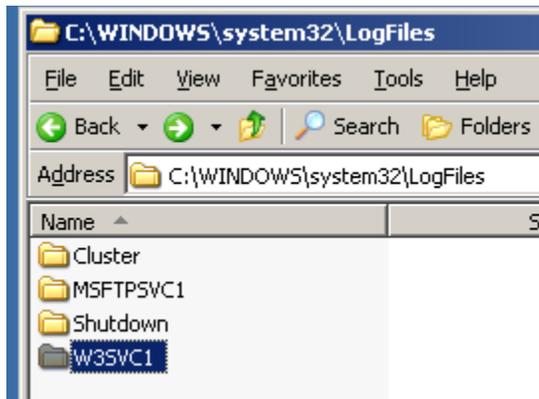


Figure 26: The Web Logs Directory

21. Double-click on the Logfile with today's date. The format is Year/Month/Day (YYMMDD)..

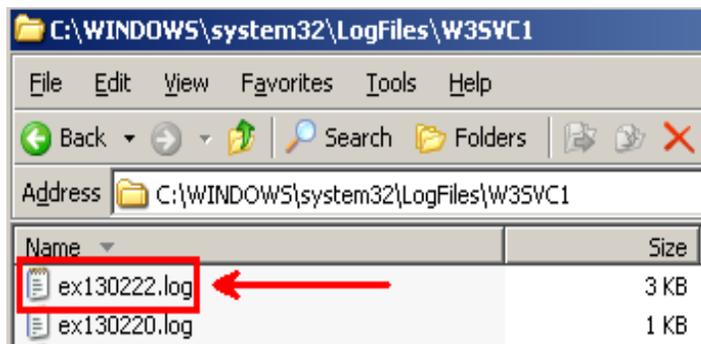


Figure 27: The Web Log files

While there is a single entry from the banner grab on the first line, there are multiple entries from the scans with Zenmap. The word Nmap in the user agent string is usually a red flag for people conducting log analysis and that IP address will be watched carefully.

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2013-02-22 20:28:25
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc
2013-02-22 20:28:25 192.168.1.100 HEAD /Default.htm - 80 - 216.6.1.100 - 200 0 0
2013-02-22 20:28:56 192.168.1.100 GET /Default.htm - 80 - 216.6.1.100 - 200 0 0
2013-02-22 20:29:03 192.168.1.100 GET /Default.htm - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+
2013-02-22 20:29:03 192.168.1.100 GET /robots.txt - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+
2013-02-22 20:29:03 192.168.1.100 GET /Default.htm - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+
2013-02-22 20:29:03 192.168.1.100 GET /Favicon.ico - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
2013-02-22 20:29:03 192.168.1.100 OPTIONS / - 80 - 216.6.1.100 Mozilla/5.0+(compatible;+Nmap+Scripting+Engine;
```

Figure 28: The Web Log file

## 1.2 Conclusion

A banner grab will allow you to determine if a port is open on a remote system. Sometimes banner messages provide you with information about the operating system or the applications in use. Scanners like Nmap and Zenmap can also be utilized to get information about open ports and banner messages. However, the scans with Nmap and Zenmap will leave more artifacts in the web logs and in network traffic captures.

## 1.3 Discussion Questions

1. Name two utilities that can be used to perform a banner grab.
2. Is there ever a need for someone besides a hacker to perform banner grabbing?
3. How do you check to see if port 110 is open on the remote system 216.1.1.1?
4. What message will you receive when you perform a banner grab against a remote system that has a closed port?

## 2 Performing Internal Active Reconnaissance

The purpose of performing active reconnaissance against one or more internal targets is also to learn about the configuration of the systems. With an internal scan, you are likely to be able to detect more machines and it is highly probable that systems will have more ports open on the LAN as opposed to systems connected to a the WAN. Insiders can be a big threat to companies because they have access to many more resources.

### 2.1 Performing an Internal Scan

1. Open the Internal **BackTrack 5** attack machine, type **root** for the login and **toor** for the password.

```
bt login: root
Password:
Last login: Thu Jan 24 11:19:02 EST 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

System information as of Fri Feb 22 09:04:41 EST 2013

System load: 0.12          Memory usage: 4%    Processes:      69
Usage of /:  57.9% of 19.06GB  Swap usage:  0%    Users logged in: 0

Graph this data and manage this system at https://landscape.canonical.com/
root@bt:~# _
```

Figure 29: Logging in as root

2. Type the following command to start the Graphical User Interface (GUI).

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

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

Figure 30: The startx command

3. Open a terminal on the Linux system by clicking on the picture to the right of the word **System** in the taskbar at the top of the screen.

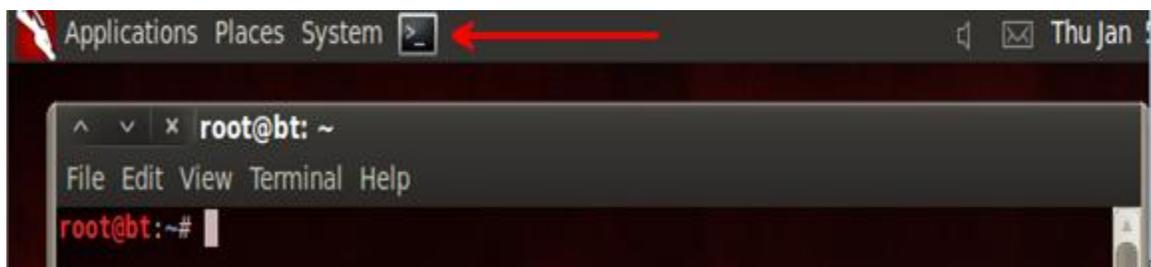


Figure 31: The Linux Terminal

We are on the Internal Network, so we have a lot more access than those machines trying to attack the company from the Internet. Right now we have 3 other IP addresses that we can scan, while the Internet attackers need to target a single IP address (the firewall: 216.1.1.1).

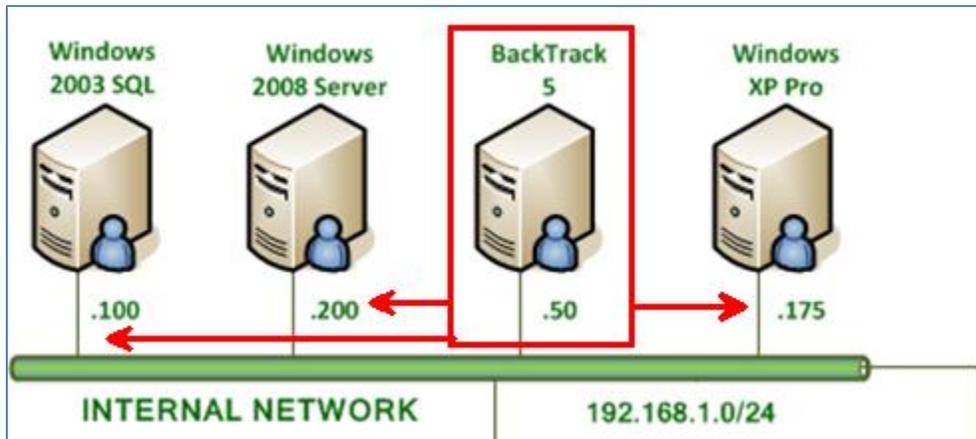


Figure 32: The Internal Network

4. On the Internal BackTrack machine, type the following to launch Metasploit:  
root@bt:~# msfconsole

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

Figure 33: Launching Metasploit

A random Metasploit banner message will appear with the current version number. Note: It may take a moment for the Metasploit banner to appear.

```
IIIIII      dTb.dTb
 II         4'  v  'B
 II         6.   .P
 II         'T; .;P'
 II         'T; ;P'
 II         'YvP'
IIIIII

I love shells --egypt

      =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 949 exploits - 505 auxiliary - 152 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf > █
```

Figure 34: Metasploit Banner

5. Type the following to perform an Nmap scan and send the output to a database:  
`msf > db_nmap 192.168.1.0/24`

```
msf > db_nmap 192.168.1.0/24
```

Figure 35: Nmap information Sent to Database

Watch as the Nmap runs a scan on hosts in the 192.168.1.0/24 network. Open ports are displayed on the screen as they are discovered.

6. Type the following to view hosts that were enumerated during the Nmap scan:  
`msf > hosts -u`

```
msf > hosts -u

Hosts
=====

address          mac
-----          -
192.168.1.1      00:0C:29:31:57:1E
192.168.1.50
192.168.1.100    00:0C:29:43:C9:0D
192.168.1.175    00:0C:29:E0:09:3F
192.168.1.200    00:0C:29:C4:99:4B
```

Figure 36: Listed Hosts

7. Type the following command to search for the SMB Scanner auxiliary module:  
`msf > search smb_version`

```
msf > search smb_version

Matching Modules
=====

Name                               Disclosure Date  Rank  Description
----                               -
auxiliary/scanner/smb/smb_version  normal          SMB Version Detection
```

Figure 37: Searching for the SMB Scanner

- Type the following command to use the SMB Scanner auxiliary module:  
msf > **use auxiliary/scanner/smb/smb\_version**

```
msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) >
```

Figure 38: Using the Scanner

If typed correctly, your sub-prompt will change to msf auxiliary(smb\_version) >

- Type the following command to view a list of module options:  
msf auxiliary(smb\_version) > **show options**

```
msf auxiliary(smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    RHOSTS           yes       The target address range or CIDR identifier
  SMBDomain WORKGROUP        no        The Windows domain to use for authentication
  SMBPass    SMBPass          no        The password for the specified username
  SMBUser    SMBUser          no        The username to authenticate as
  THREADS   1                yes       The number of concurrent threads
```

Figure 39: Showing the Options

- Type the following to load the hosts from the database as RHOSTS values.  
msf auxiliary(smb\_version) > **hosts -R**

```
msf auxiliary(smb_version) > hosts -R

Hosts
=====
address      mac              name  os_name  os_flavor  os_sp  purpose  info  comments
-----
192.168.1.1  00:0C:29:31:57:1E  Unknown  Unknown  Unknown  device
192.168.1.50  00:0C:29:43:C9:0D  Unknown  Unknown  Unknown  device
192.168.1.100 00:0C:29:E0:09:3F  Unknown  Unknown  Unknown  device
192.168.1.175 00:0C:29:C4:99:4B  Unknown  Unknown  Unknown  device
192.168.1.200 00:0C:29:C4:99:4B  Unknown  Unknown  Unknown  device

RHOSTS => 192.168.1.1 192.168.1.50 192.168.1.100 192.168.1.175 192.168.1.200
```

Figure 40: Setting the RHOSTS

11. Type the following command to view the options with the RHOSTS set:  
`msf auxiliary(smb_version) > show options`

```
msf auxiliary(smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):
  Name      Current Setting
  ----      -
  RHOSTS    192.168.1.1 192.168.1.100 192.168.1.175 192.168.1.200
  SMBDomain WORKGROUP
  SMBPass
  SMBUser
  THREADS   1
```

Figure 41: Showing the Options

The value for RHOSTS should be set to the multiple hosts on the 192.168.1.0/24 subnet.

12. Type the following to discover information about the hosts' operating systems.  
`msf auxiliary(smb_version) > run`

```
msf auxiliary(smb_version) > run
[*] 192.168.1.1:445 is running Windows 2003 No Service Pack (language: Unknown) (name:FW) (dom
[*] Scanned 1 of 4 hosts (025% complete)
[*] 192.168.1.100:445 is running Windows 2003 No Service Pack (language: Unknown) (name:SERVER
[*] Scanned 2 of 4 hosts (050% complete)
[*] 192.168.1.175:445 is running Windows XP Service Pack 2 (language: English) (name:WINXP) (d
[*] Scanned 3 of 4 hosts (075% complete)
[*] 192.168.1.200:445 is running Windows 2008 Standard without Hyper-V Service Pack 1 (languag
[*] Scanned 4 of 4 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 42: OS Information about the Remote Hosts is Disclosed

IP address	Operating Systems
192.168.1.1	Microsoft Windows 2003 NO Service Pack
192.168.1.100	Microsoft Windows 2003 NO Service Pack
192.168.1.175	Microsoft Windows XP SP2
192.168.1.200	Microsoft Windows 2008 Without Hyper V

13. Type the following to list the hosts and their corresponding operating systems.  
msf auxiliary(smb\_version) > **hosts -R**

```
msf auxiliary(smb_version) > hosts -u

Hosts
=====
address      mac          name  os_name  os_flavor
-----
192.168.1.1  00:0C:29:31:57:1E  Microsoft Windows 2003
192.168.1.50  Unknown
192.168.1.100 00:0C:29:43:C9:0D  Microsoft Windows 2003
192.168.1.175 00:0C:29:E0:09:3F  Microsoft Windows XP
192.168.1.200 00:0C:29:C4:99:4B  Microsoft Windows 2008 Standard
```

Figure 43: Relisting the Hosts with the OS Identified

14. Type **quit** to return to the **root@bt:~#** prompt.
15. Type the following to launch Armitage:  
root@bt:~# **armitage**

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

Figure 44: Launching Armitage

16. Click **Connect** to connect to the localhost as user msf with the password test.

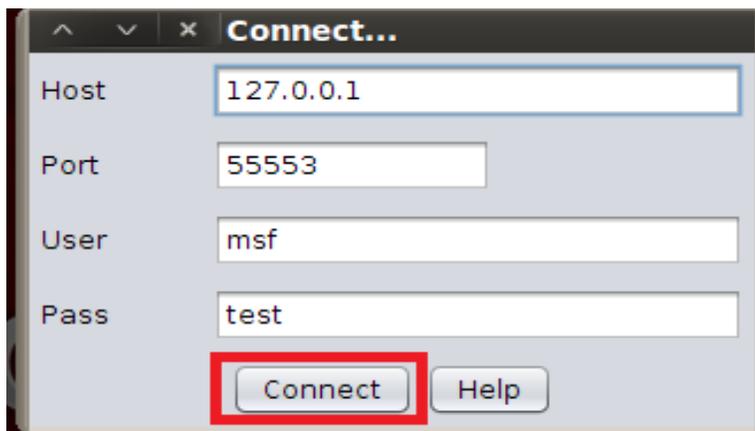


Figure 45: Connecting Armitage

17. Click **Yes** to start Metasploit's Remote Procedure Call(RPC) Server.

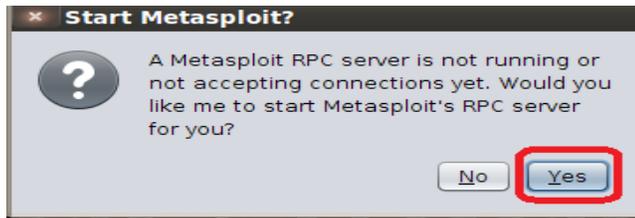


Figure 46: Start Metasploit RPC Server

You will initially get a java.net connection error. Do not click cancel, just wait briefly...

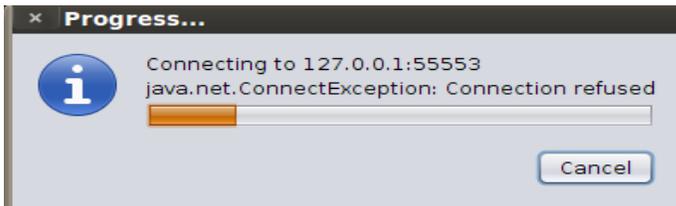


Figure 47: Java Connection Message

The Armitage windows will appear. Notice the Metasploit console on the bottom left.

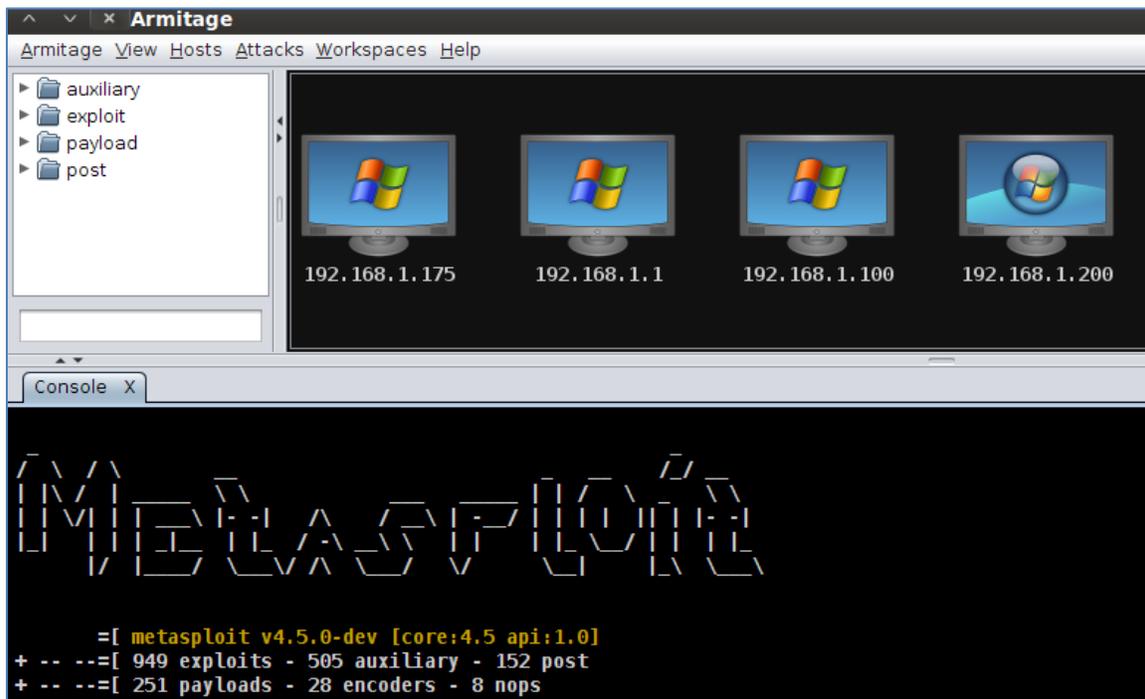


Figure 48: Armitage

Armitage is a front end for Metasploit, so the hosts are already identified because their information was loaded into the database when you ran commands in the msfconsole.

18. Hover over any of the Windows machines to get an exact OS determination.

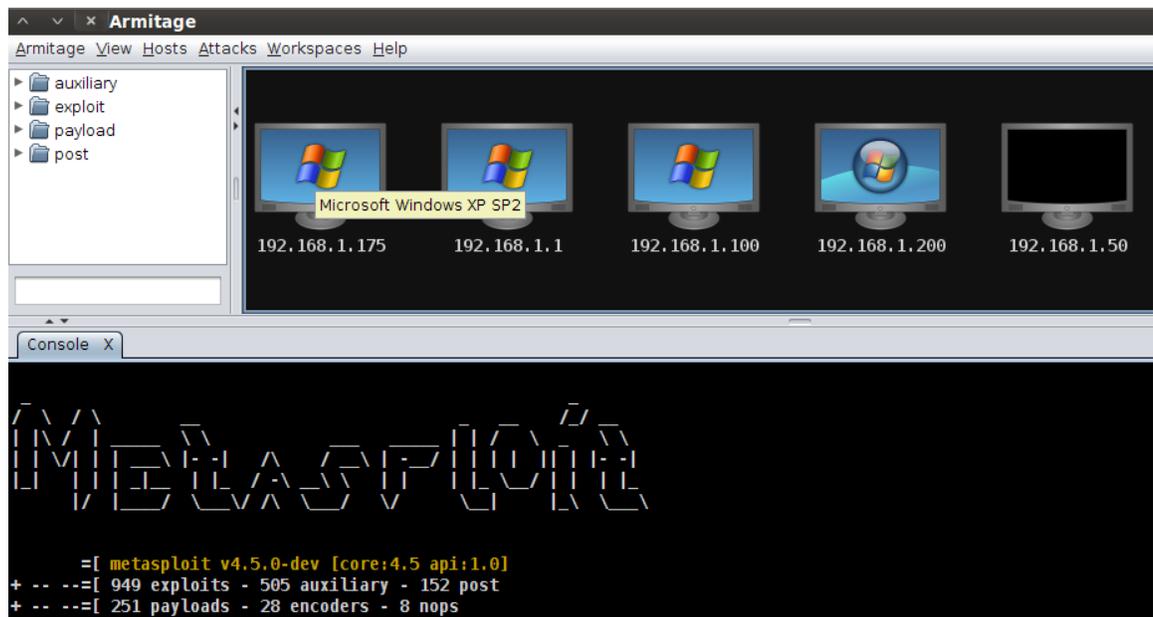


Figure 49: Operating System Identification

## 2.2 Conclusion

Scanning devices is much easier when you are on the inside of a network. There are more ports open and there is usually access to a greater number of machines. For this reason, insiders can be a huge threat and internal network traffic should be monitored.

## 2.3 Discussion Questions

1. What is the command to start Metasploit?
2. What will the hosts command do within msfconsole?
3. What is the command to set all of the computers listed in hosts to the RHOST?
4. How do you determine the exact OS fingerprint within Armitage?

### 3 Performing Internal and External Passive Reconnaissance

Performing reconnaissance of external and internal hosts and achieving very accurate depictions of what ports were open and what operating systems the remote machines were running, using any kind of active tools may get us caught. The use of passive tools like Wireshark or tcpdump will not be noticed on the network.

#### 3.1 Passive Reconnaissance Using tcpdump and Wireshark

1. On the *internal Backtrack 5* machine, type the following to view tcpdump switches:

```
root@bt:~# tcpdump --help
```

```
root@bt:~# tcpdump -help
tcpdump version 4.2.1
libpcap version 1.0.0
Usage: tcpdump [-aAbdDefhHIKlLnNOpqRStuUvxxX] [-B size] [-c count]
              [-C file_size] [-E algo:secret] [-F file] [-G seconds]
              [-i interface] [-M secret]
              [-r file] [-s snaplen] [-T type] [-w file]
              [-W filecount] [-y datalinktype] [-z command]
              [-Z user] [expression]
```

Figure 50: The tcpdump command

On the Internal 192.168.1.0/24 network, broadcasts are sent to 192.168.1.255.

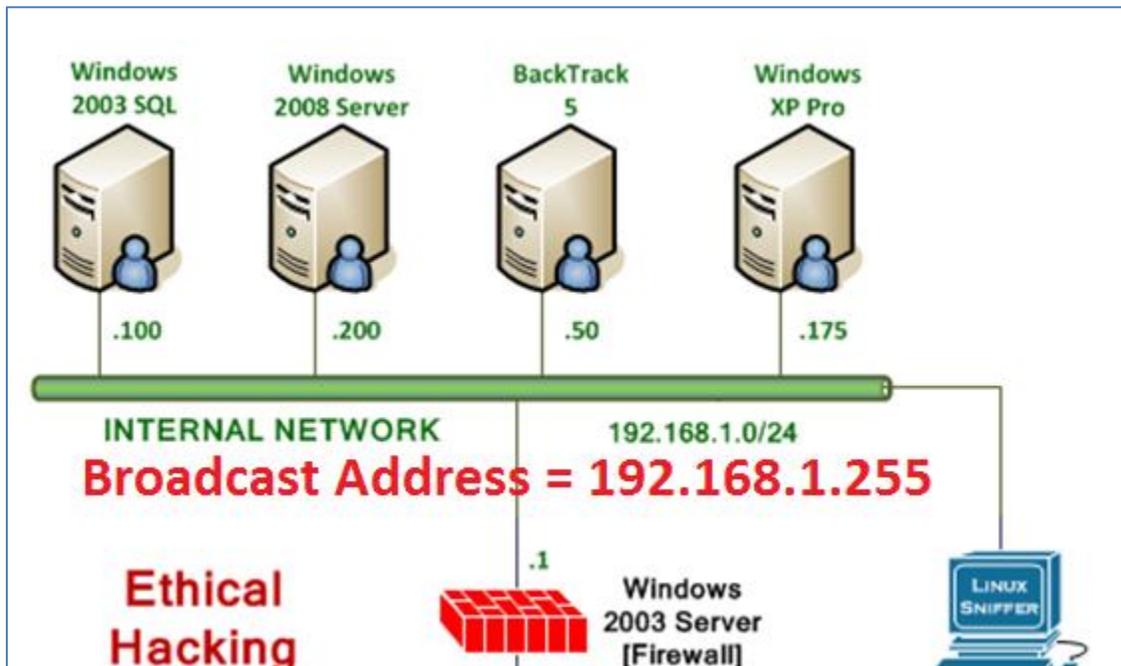
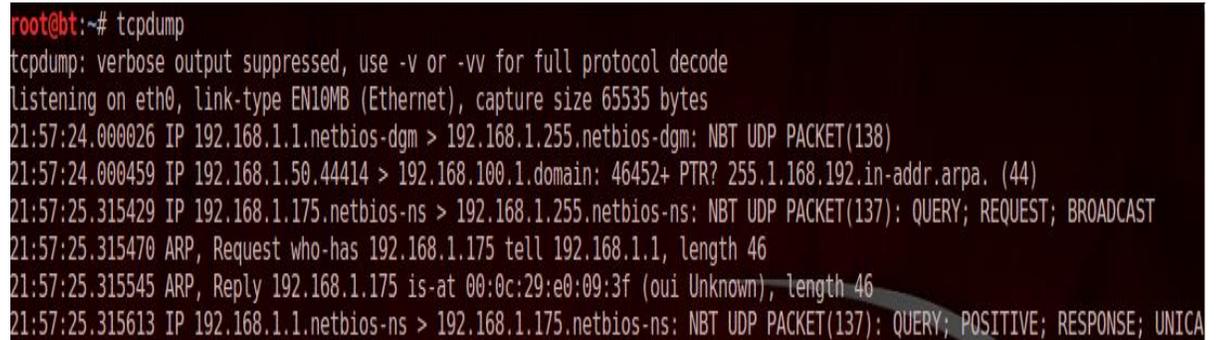


Figure 51: The Broadcast Address is 192.168.1.255.

2. Type the following command to passively sniff traffic on interface eth0:

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

A terminal window showing the execution of the tcpdump command. The output displays network traffic on interface eth0, including NetBIOS Datagram (NBT) UDP packets and ARP requests and replies. The first line shows a NetBIOS Datagram from 192.168.1.1 to 192.168.1.255. The second line shows a PTR record for 255.1.168.192. The third line shows a NetBIOS Name Service (NBT) UDP packet query. The fourth line shows an ARP request for 192.168.1.1. The fifth line shows an ARP reply for 192.168.1.175. The sixth line shows another NetBIOS Datagram query.

```
root@bt:~# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
21:57:24.000026 IP 192.168.1.1.netbios-dgm > 192.168.1.255.netbios-dgm: NBT UDP PACKET(138)
21:57:24.000459 IP 192.168.1.50.44414 > 192.168.100.1.domain: 46452+ PTR? 255.1.168.192.in-addr.arpa. (44)
21:57:25.315429 IP 192.168.1.175.netbios-ns > 192.168.1.255.netbios-ns: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
21:57:25.315470 ARP, Request who-has 192.168.1.175 tell 192.168.1.1, length 46
21:57:25.315545 ARP, Reply 192.168.1.175 is-at 00:0c:29:e0:09:3f (oui Unknown), length 46
21:57:25.315613 IP 192.168.1.1.netbios-ns > 192.168.1.175.netbios-ns: NBT UDP PACKET(137): QUERY; POSITIVE; RESPONSE; UNICA
```

Figure 52: Passive Sniffing

Most of the IP addresses announce themselves on the network, without doing any type of scan. User Datagram Protocol (UDP) NetBIOS Datagrams are sent to the network broadcast address of 192.168.1.255. Address Resolution Protocol (ARP) uses the broadcast MAC address of FF:FF:FF:FF:FF:FF. These broadcasts are sent to all machines within a single broadcast domain; meaning ARP broadcasts are not forwarded off a LAN segment.

Another way we can listen passively on the internal network is by using Wireshark.

3. On the sniffer machine, type the following command to launch Wireshark:

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

A terminal window showing the command 'wireshark' being typed at the root prompt.

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

Figure 53: Typing Wireshark

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



Figure 54: Wireshark Message

5. Select Capture from the Wireshark menu bar, and choose Interfaces.



Figure 55: Capture Sub-Menu

6. Check the box in front of eth0. Click the **Start** button at the bottom of the screen.

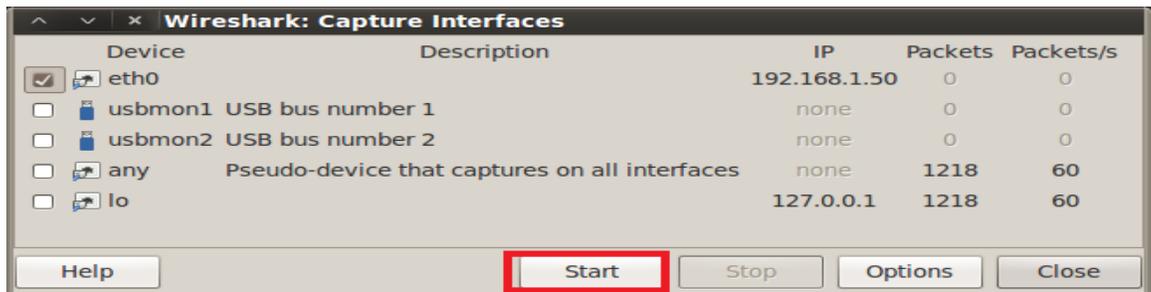


Figure 56: Starting Wireshark on the Internal Interface

You will notice IP addresses appear in the list after some time elapses.

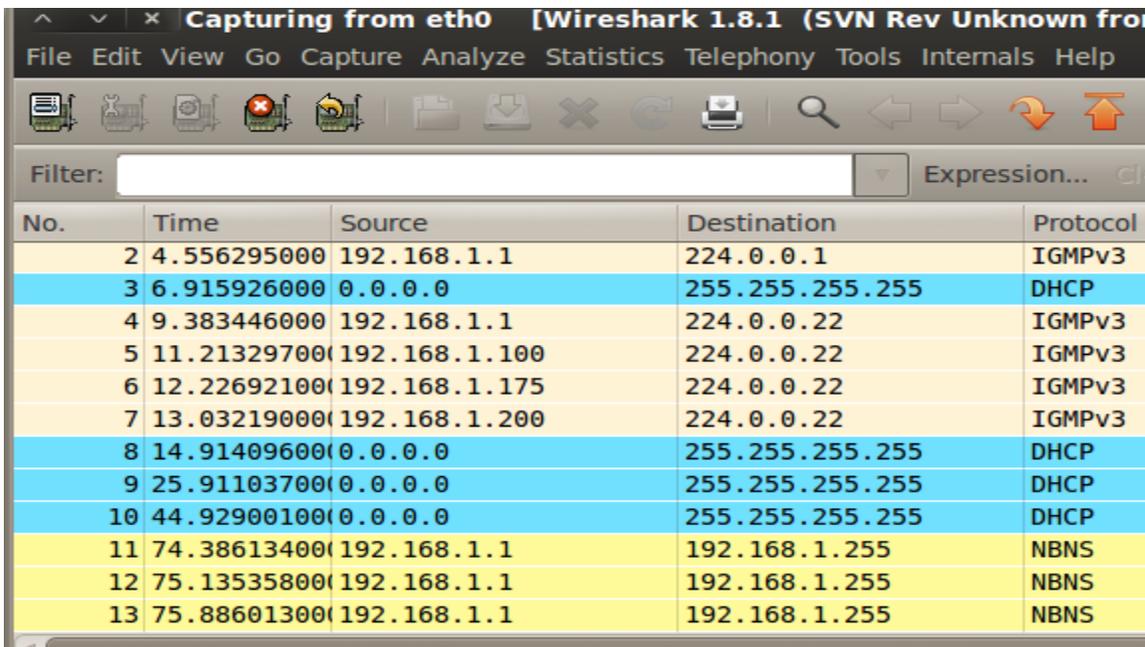


Figure 57: Passively Discovering IP addresses

There are also passive ways to discover information about hosts on the Internet. One way is to use a site that already aggregated the information you need. Sites, such as netcraft.com, will identify information such as the IP address, operating system, and version of the web server software that the remote host is utilizing.

The screenshot displays the Netcraft website interface. At the top, there are logos for VeriSign SSL (now from Symantec) and Symantec. The main heading is "Site report for www.towson.edu". On the left, there is a navigation menu with links like "Home", "Download Now!", "Report a Phish", "Top Reporters", "Phishiest TLDs", "Phishiest Countries", "Phishiest Hosters", "Phishing Map", "Most Popular Websites", "Branded Extensions", "Tell a Friend", "Phishing & Fraud", "Phishing Site Feed", "Hosting Phishing Alerts", "SSL CA Phishing Alerts", "Registry Phishing Alerts", "Domain Registration Risk", "Bank Fraud Detection", "Phishing Site Countermeasures", and "Version Support".

The main content area is divided into three sections:

- Background:**

Site title	Towson University	Date first seen	August 1995
Site rank	91714	Primary language	English
Description	Towson University, a top public university located near Baltimore, Maryland, offers nationally recognized academic programs that prepare students with the leadership and professional skills necessary for today's world.		
Keywords	teacher education, teacher training, elementary education, special education, deaf studies, audiology, occupational therapy, occupational science, kinesiology, small business development, accounting programs, economic education, reading programstigers, applied learning, nursing		
- Network:**

Site	http://www.towson.edu	Last Reboot	2 days ago <span>🔍</span>
Domain	towson.edu	Netblock Owner	COMBNET
IP address	136.160.171.30	Nameserver	ns1.towson.edu
IPv6 address	Not Present	DNS admin	postmaster@towson.edu
Domain registrar	educause.net	Reverse DNS	www1.towson.edu
Organisation	Towson University, Cook Library Room 28, Towson, 21252, United States	Nameserver organisation	whois.educause.net
Top Level Domain	Educational entities (.edu)	Hosting company	towson.edu
Hosting country	🇺🇸 US	DNS Security Extensions	unknown
- Hosting History:**

Netblock owner	IP address	OS	Web server	Last changed
COMBNET 3300 Metzerott Road Adelphi MD US 21783	136.160.171.30	Windows Server 2003	Microsoft-IIS/6.0	15-Feb-2013

Figure 58: The Netcraft Website

### 3.2 Conclusion

While performing active reconnaissance against targets provides the attacker with valuable information, it can set off network sensors and be detected within logs. Passive reconnaissance gives an attacker the ability to gain information without being detected.

### 3.3 Discussion Questions

1. What is a good website to get information about the version of the operating system and the web server software that the site is utilizing?
2. What are two good tools that can be used to collect information passively?
3. What is the command to see all of the available options for tcpdump?
4. What type of traffic will you see when you listen on the network with Wireshark?

## References

1. Wireshark:  
[www.wireshark.org](http://www.wireshark.org)
2. tcpdump:  
<http://www.tcpdump.org/>
3. Banner Grabbing (Ethical Hack):  
[http://www.firewalls.com/blog/banner\\_grab\\_ethical\\_hack/](http://www.firewalls.com/blog/banner_grab_ethical_hack/)
4. Banner Grabbing:  
<http://wcosughacking.blogspot.com/2011/06/banner-grabbing.html>
5. Metasploit:  
[www.metasploit.com](http://www.metasploit.com)