Ethical Hacking Lab Series

Lab 6: Utilizing Malware - Dark Comet

Certified Ethical Hacking Domains:
System Hacking,
Trojans and Backdoors,
Viruses and Worms

Document Version: 2013-07-18 (Beta)

Organization: Moraine Valley Community College
Author: Jesse Varsalone

.

The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

Contents

Introduction

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

By performing this lab, students will learn how to use Dark Comet.

This lab includes the following tasks:

- 1 – Setting up the Dark Comet Client (Server)
- 2 – Using the xp_cmd shell to upload and launch a Malicious Payload
- 3 – Exploiting the Victim Machine

Domains: System Hacking, Trojans and Backdoors, Viruses and Worms

Hackers often utilize user-friendly malware programs like the Dark Comet Trojan that will allow them to perform a variety of post exploitation tasks, including:

- Uploading Malware
- Running Programs
- Dumping Hashes
- Uninstalling Software
- Disabling Services
- Killing Processes
- Stealing Data
- DNS Manager
- Key Logger

Dark Comet is an extremely dangerous piece of malware that will allow attackers to maintain a persistent connection on a victim's machine through an encrypted connection. While SharK has not been updated since 2007, Dark Comet has been updated recently. Dark Comet works on the newer version of Windows operating systems. Programs like this are often referred to as command and control.

Remote Access Trojan – A program that will allow a remote user, likely an attacker to connect to a victim's machine and perform harmful actions to the computer's operating system. A Remote Access Trojan, or RAT, may allow the attacker to perform such tasks as uploading or downloading files and stealing a user's credentials.

Dark Comet – Remote Access Trojan that has a Graphical User Interface, or GUI, that allows the hacker to perform malicious tasks against a victim machine over an encrypted connection. Dark Comet includes two components, the server and the client.

Dark Comet Client – Although it may seem counterintuitive, the Dark Comet client is configured on the machine that will act as the server and accept client connections. Any port may be used for the "client", but a common port like 80 (Hyper Text Transfer Protocol) or 443 (Hyper Text Transfer Protocol Secure) or 443 will make the connection from the victim to the attacker seem a bit less conspicuous than a port like 12345.

Dark Comet Server – A server executable or payload is created and then distributed to one or more victims. Once the victim executes the payload, the malware will infect their machine and they will connect to the computer running the Dark Comet software.

Wrapper – This program allows you to add more than one executable and combine them into a single executable. From a malicious standpoint, an attacker could package a malicious executable with a legitimate one and use this to launch an attack.

Pod Topology

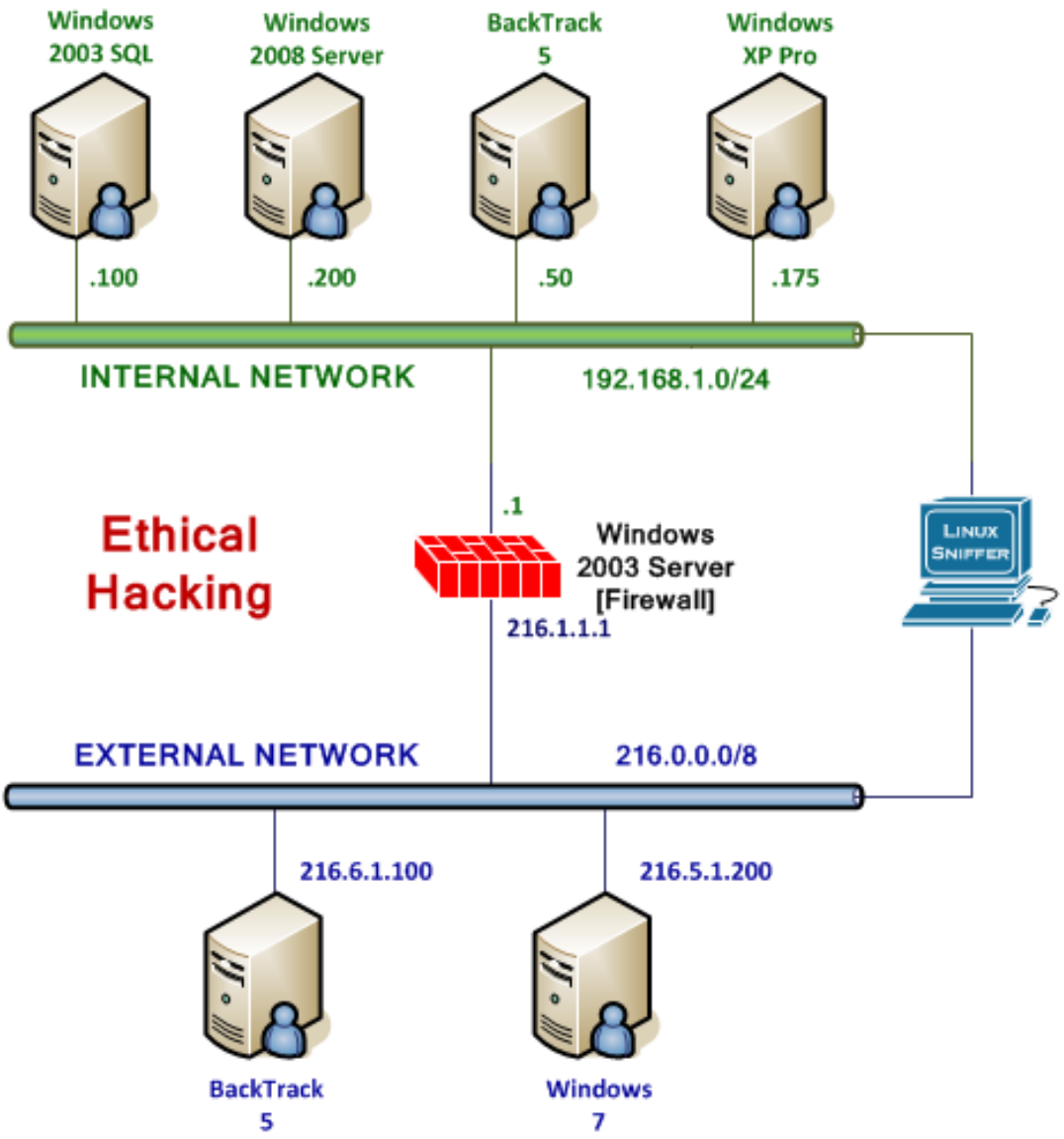

Figure 1: Lab Topology

Lab Settings

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

Required Virtual Machines and Applications

This lab requires the use of the machine running Windows XP and Windows 7.

Although you will not be logging on to the Firewall or the Windows 2003 Exchange, these machines being utilized are used during the lab.

Windows 7	216.5.1.200 (Public IP)
Windows 7 **student** password	password

1 Setting up the Dark Comet Client (Server)

Although it may seem counterintuitive, the Dark Comet client is configured on the machine that will act as the server and accept client connections. In this case, our Windows 7 machine will be the machine running the Dark Comet Software. We will configure the Windows 7 machine to run the Dark Comet software and accept incoming connections from victim machines that execute the malicious payloads.

1.1 Configuring the Dark Comet Client

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

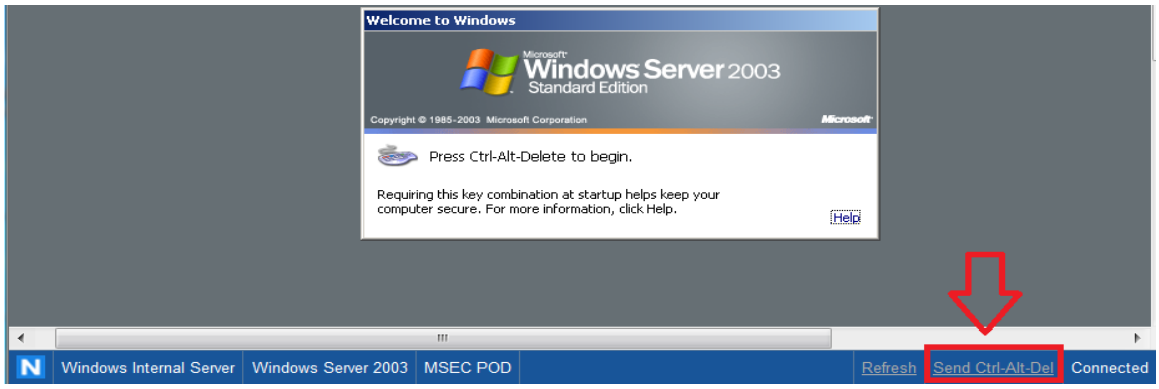

Figure 2: Send Ctrl-Alt-Del to the Windows 2003 SQL

Next, we will open the command prompt on the Windows 2003 SQL. In order to fully understand how the attack will be carried out, we must further investigate how the Network Address Translation, or NAT, process works and its relationship to attacks. Note that your Windows XP machine has a private IP address and is on the Local Area Network, or LAN, of the XYZcompany's network, which has a range of 192.168.1.0/24.

2. Open the command prompt on the Windows XP machine by clicking the desktop shortcut.

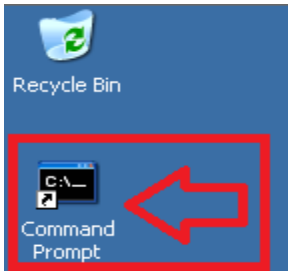

Figure 3: A Shortcut to the Command Prompt

3. On the 2003 server, type the following command to view your private IP address:
   C:\>**ipconfig**

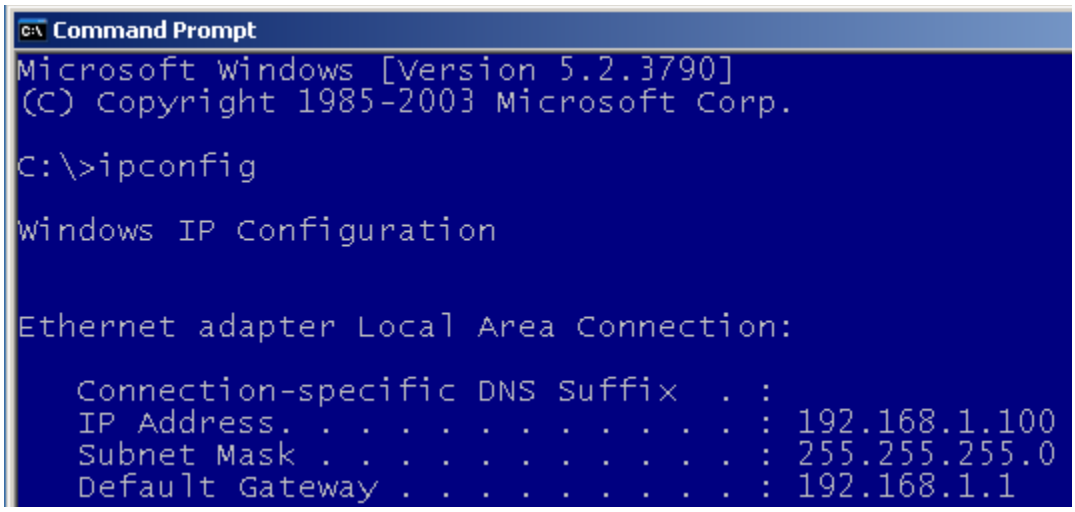

Figure 4: The ipconfig command

The IP address of the Windows 2003 SQL Server should be set to **192.168.1.100**.

4. Now, ping the Windows 7 machine on the external network by typing:
   C:\>**ping 216.5.1.200**

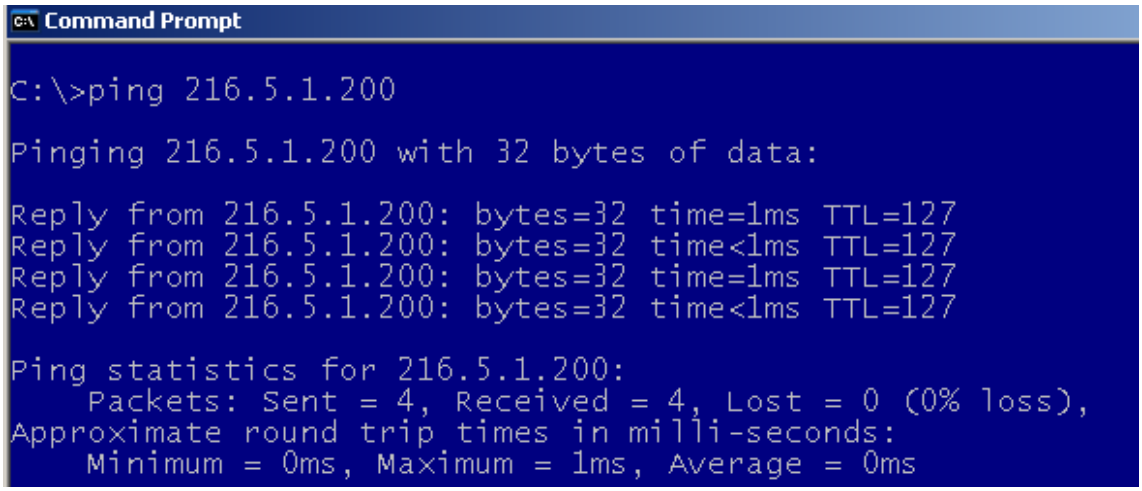

Figure 5: Successful ping of the Windows 7 machine

You should receive 4 successful replies from the Windows 7 machine with the IP address of 216.5.1.200. In some cases, you can ping machines on the Internet. However, some sites, like www.microsoft.com block ping. Also, some administrators do not allow pings through the firewall. In those cases, you will not be able to ping public addresses.

5. Log on to the Windows 7 machine as **student** with the password of **password.**

Figure 6: Logging on to Windows 7

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

Figure 7: Opening a Command Prompt on Windows 7

7. On the Windows 7 system, type the following to view your Public IP address C:\>**ipconfig**

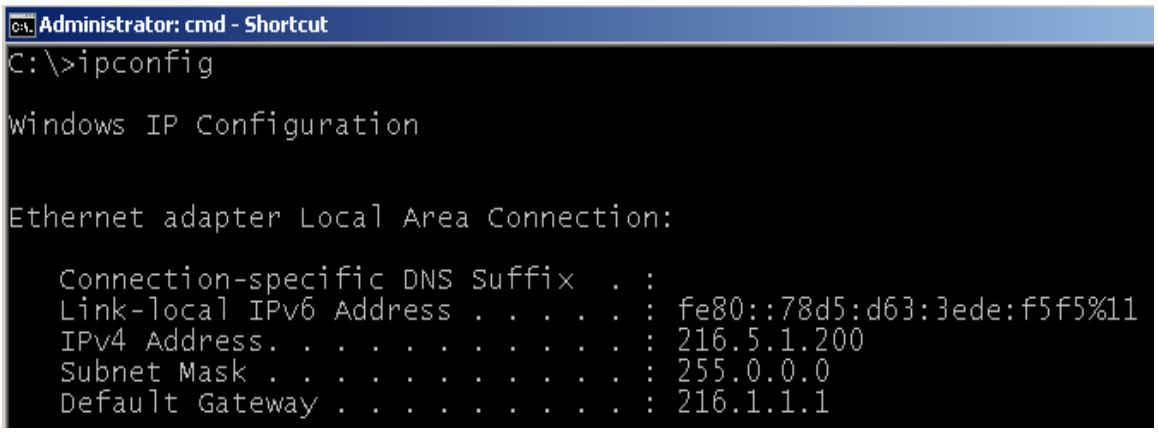

Figure 8: IP address Information on Windows 7

8. From Windows 7 on the public Internet (simulated), attempt to ping the Windows 2003 machine on the internal network by typing:
   C:\>**ping 192.168.1.100**

Notice that this attempt will fail.

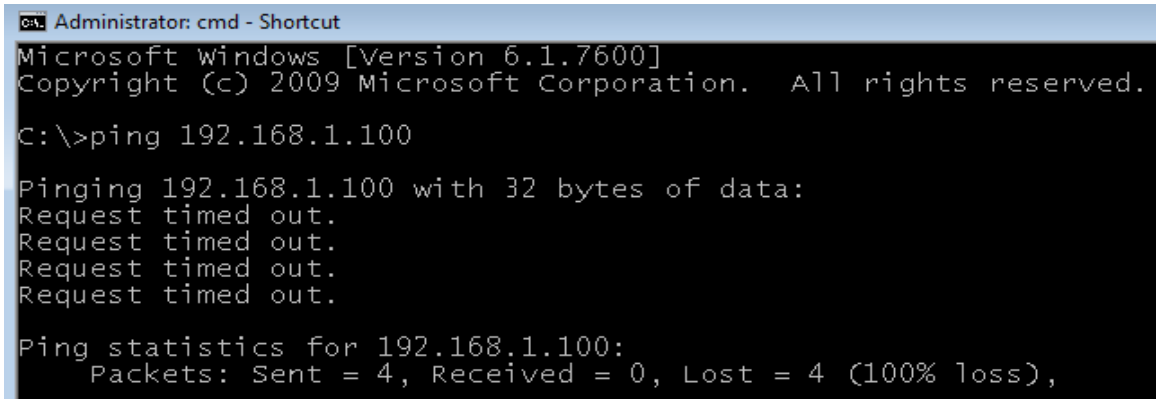

Figure 9: Failed Pings to the Machine on the Internal Network

Windows 7 is using a public IP address and is on the Wide Area Network, or WAN. Attackers trying to get on your internal network cannot directly attack the Windows 2003 machine because it is NATed behind the Firewall. The 2003 SQL Server machine is not sitting on the Internet (simulated) with a public IP address. However, the firewall is redirecting traffic to the internal SQL, and we will leverage that during our attack.

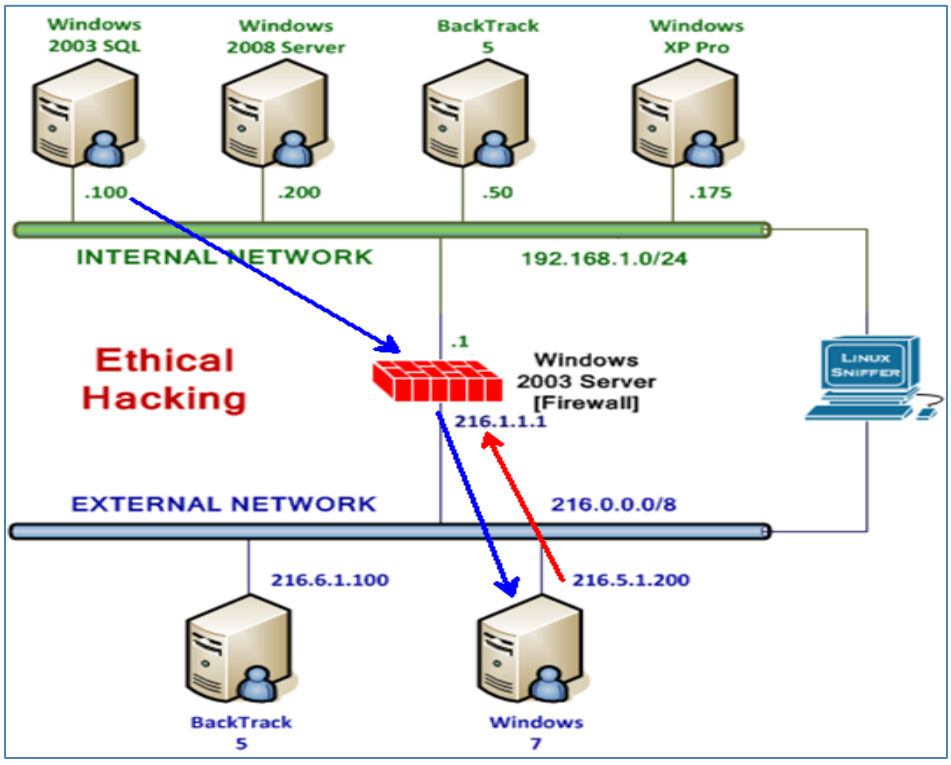

Figure 10: Internal Machines on Private Network are Unreachable from WAN

9. Open the Malware folder on the Win7 Desktop. Right-click on the DarkComet.7z file, select 7-zip and select the fourth choice down, **Extract to "DarkComet\"**.

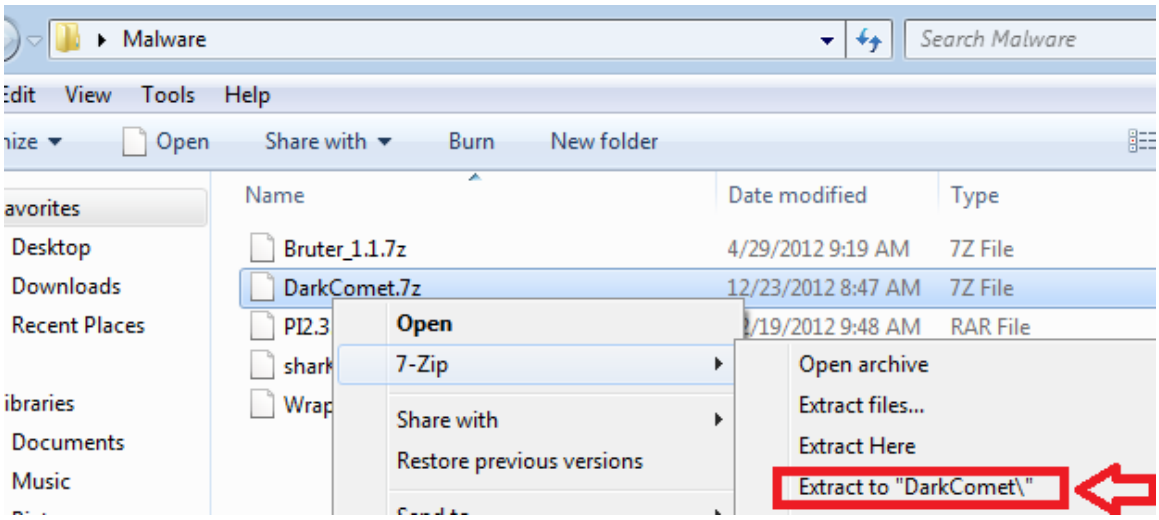

Figure 11: Extracting the file with 7-zip

10. Traverse thorough the Dark Comet folders until you see Dark Comet.exe. Double-click on the **Dark Comet.exe** file to launch the program.

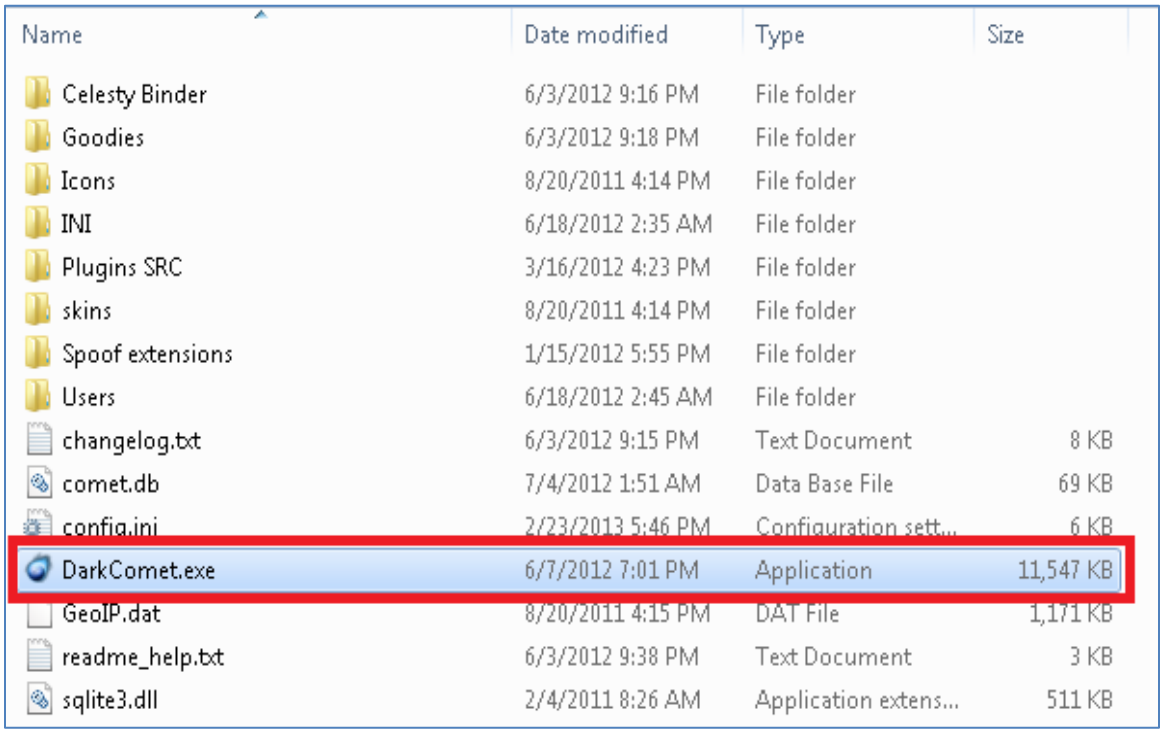

Figure 12: Extracting the file with 7-zip

First, we need to set the listen port to something other than the default port of 1601.

11. From the Dark Comet Menu bar, click File and select **Listen to new port**.

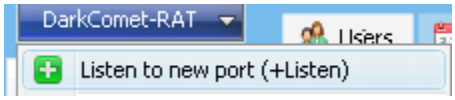

Figure 13: Listen to New Port

Any port may be used for the "client", but a common port like 80 (Hyper Text Transfer Protocol) or 443 (Hyper Text Transfer Protocol Secure) will make the connection from the victim to the attacker seem a bit less conspicuous than a port like the default port of 1604. In this example, we will set up Dark Comet to listen on port 443.

12. In the **Listen port** box, type 443. Click Start to begin listening on that port.

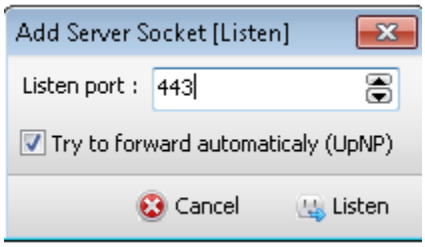

Figure 14: Listing on Port 443

The netstat command can be used to determine which ports the machine is listening on.

13. To verify that the attack machine is listening on port 443, type the following:
C:\>**netstat -an**

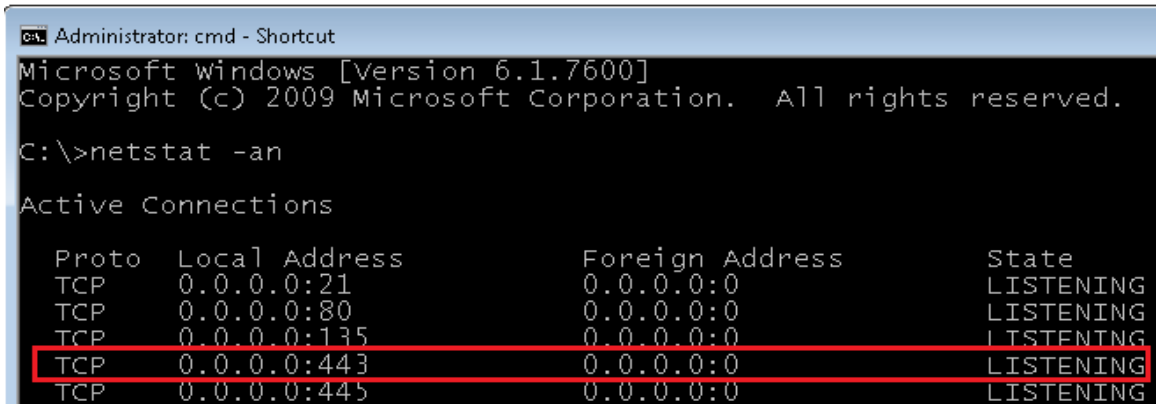

Figure 15: Dark Comet is listening on Port 443

14. To create a new server (client), Click on the DarkComet-RAT menu in the top left hand corner, select **Server module**, then select **Minimalist (Quick)** from the menu.

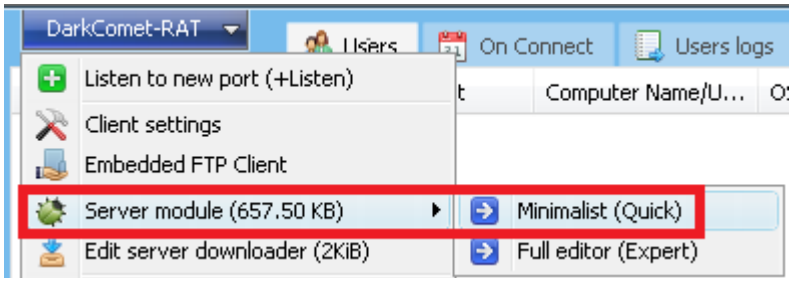

Figure 16: Creating a "Server"

15. For the IP/DNS address, type **216.5.1.200**. For the port, type **443**.

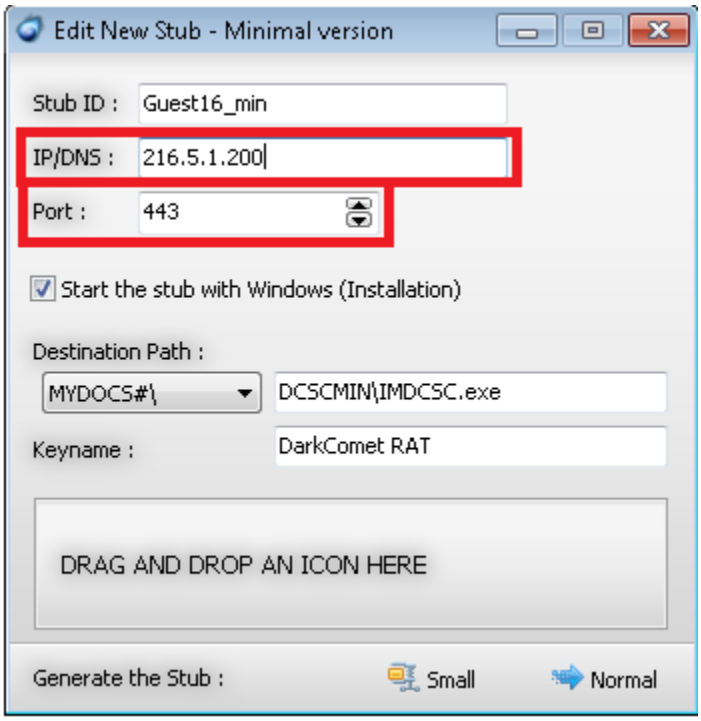

Figure 17: Changing the Port and IP address

16. Click on Start and select **Student** on the top right side of the menu.

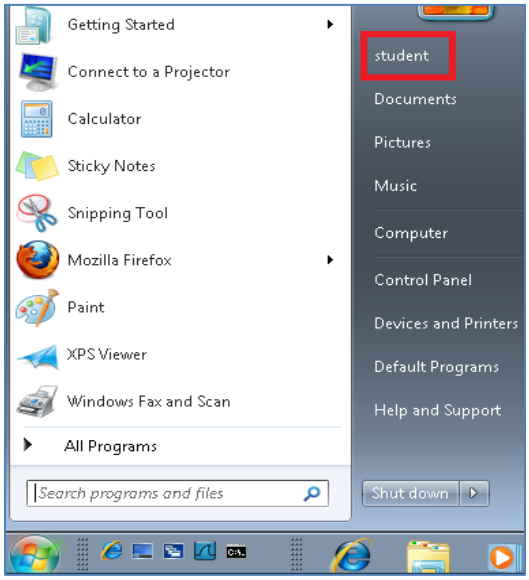

Figure 18: Entering the Student Folder

17. Double-click on the Desktop folder, then double-click on the malware folder. Navigate through the DarkComet folders until you arrive at the Icons folder. Double-click on the Icons folder. Find iexplore.exe and drag it to the section indicating **DRAG AND DROP AN ICON HERE**.

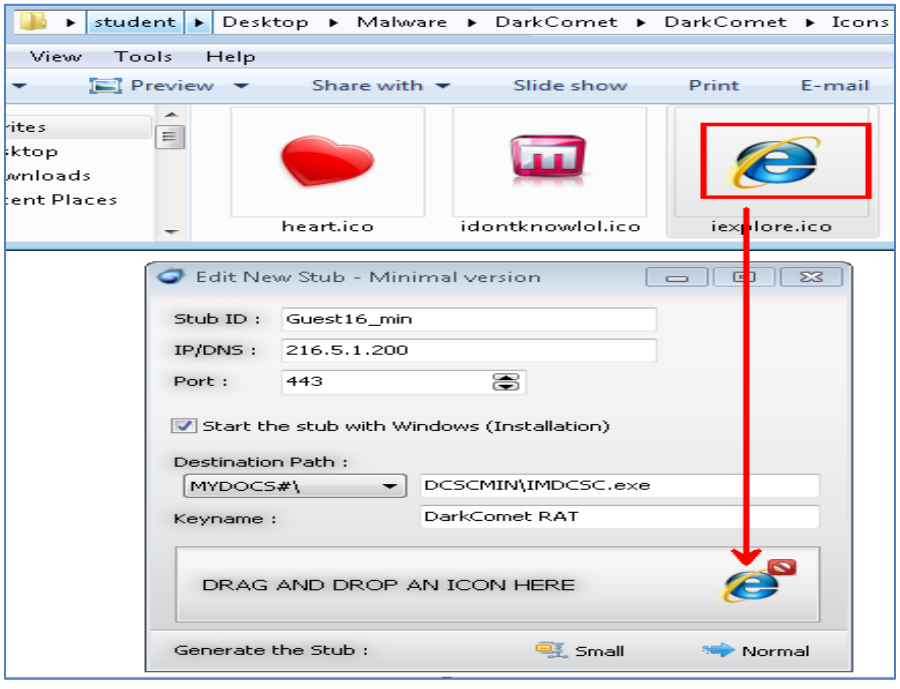

Figure 19: Dragging in the Icon

18. For the Generate the Stub choice, click the **Normal** button.

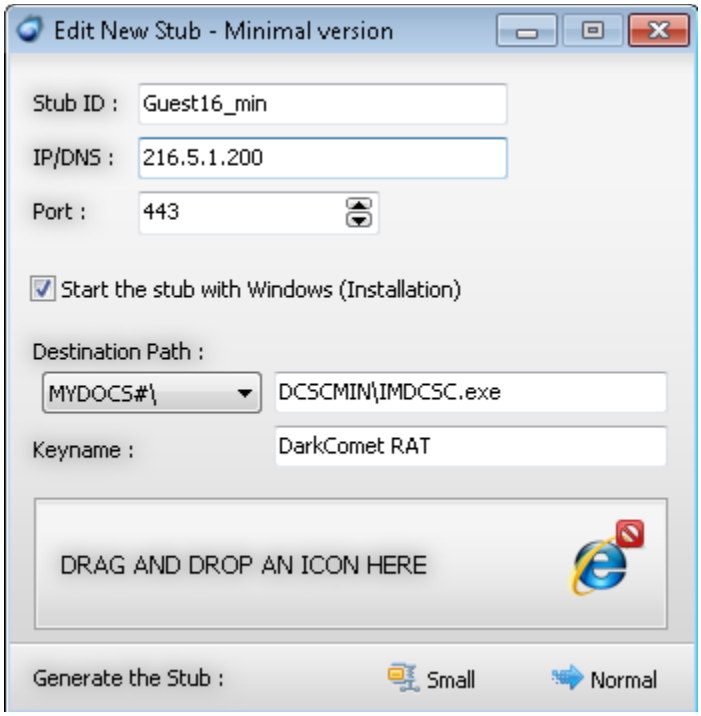

Figure 20: Generating the Payload

19. In the Save As box, Click **Computer > Local Disk C: > Inetpub > ftproot**. For the filename, type **iexplore** and then click the Save button to save the file.

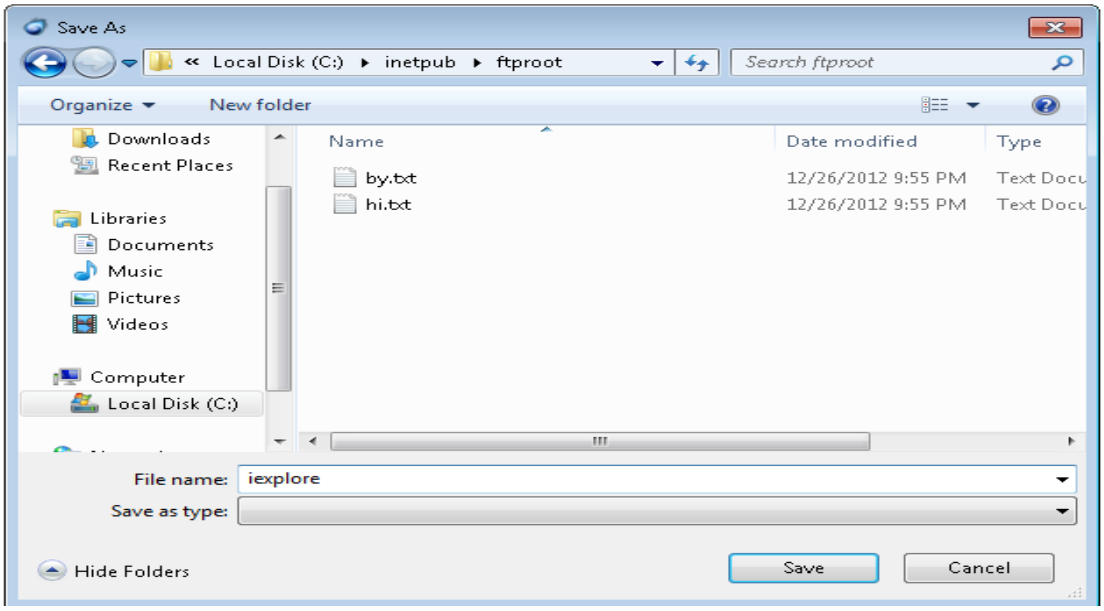

Figure 21: Saving the File

20. You will see the message that the stub was successfully generated. The file path should be **C:\inetpub\ftproot\iexplore.exe** for the generated stub. Click **OK**.

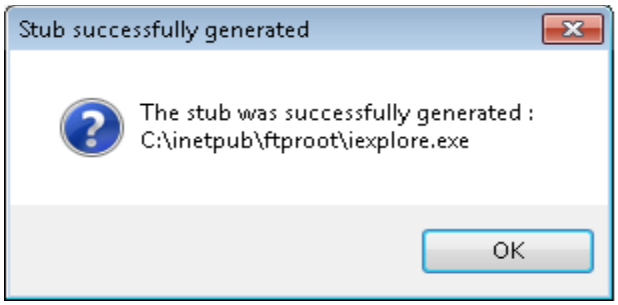

Figure 22: The File is Generated

21. Click on Start, Computer, Local Disk C:, Inetpub, Ftproot. The iexplore.exe file should be in the directory. Notice the actual Internet Explorer icon is used.

Figure 23: Legitimate Icon

1.2 Conclusion

Dark Comet is malware that has a server and a client component. The attacker first sets up the client, which will listen on a port and wait for connections. Attackers on the Internet cannot directly attack internal machines on an internal network. Rather, they need them to get users on an internal network with private IP addresses to launch a program so they will be able to connect to an external IP address on the Internet. If a malicious program has a legitimate looking icon, it will help to hide its detection.

1.3 Discussion Questions

1. How does someone on the Internet attack a machine with a private IP address?
2. What is the command to determine if your machine is listening on port 443?
3. Why might the default listening port of 1601 be a bad choice for the attacker?
4. Name a technique that can be used to increase the likelihood a malicious file will not be detected.

2 Using the xp_cmd shell to upload and launch a Malicious Payload

In this exercise, we will upload the malicious payload to the victim machine using the stored procedure xp_cmd shell. We will upload the svhost.exe file, which is actually a Dark Comet payload, by creating an ftp answer file and executing the ftp command. After uploading the file, we will launch it to get the victim to connect to the attacker.

2.1 Upload and Launch a Malicious Payload to the Victim Machine

The web application is using JavaScript to check for input validation. This is a form of client side validation. So, what we will do is disable JavaScript within our browser. Perform the following steps on the External **Windows 7** attack machine:

1. To disable JavaScript, select Tools from the Firefox menu bar and go down to Options. Click on the **Content** button. Uncheck **Enable JavaScript**, then click OK.

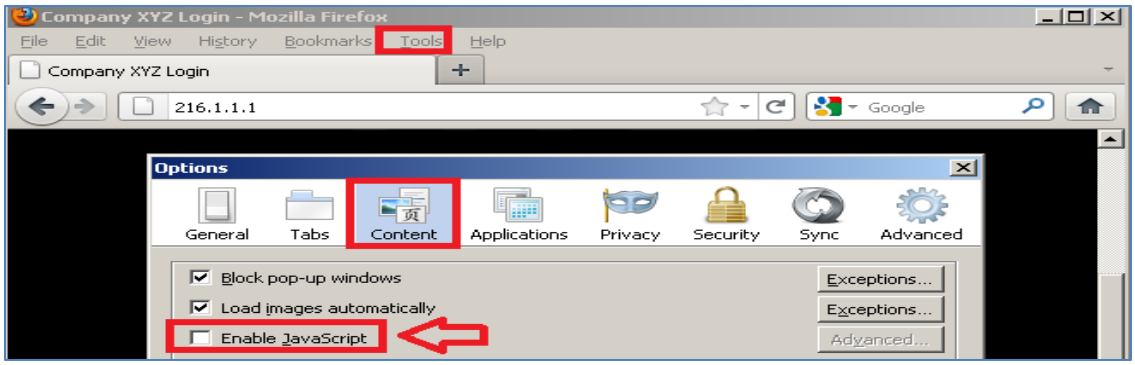

Figure 24: Disable JavaScript

2. Go to the Public IP address of XYZ Company by typing this URL in your browser: http://216.1.1.1

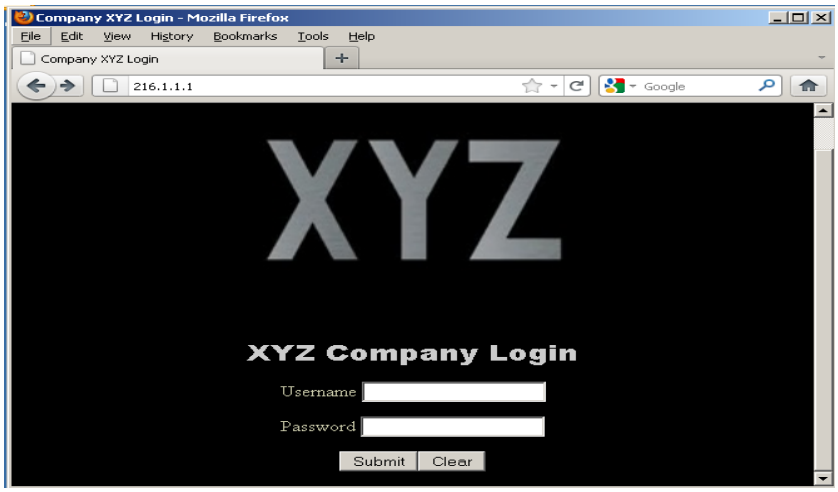

Figure 25: Public Facing Website

3. Open the sql.txt file on the Desktop. Highlight the fifth line in the sql.txt file. Select edit, then **Copy** from the menu.

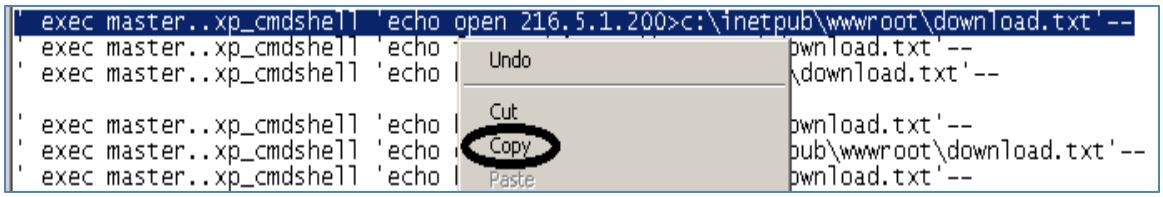

Figure 26: Copying a Line of Text

4. Right-click in the username field and select **Paste**. Click the Submit button.

Figure 27: Inputting the Information into the Username Field

You should see a web page with the response displayed in the figure below:

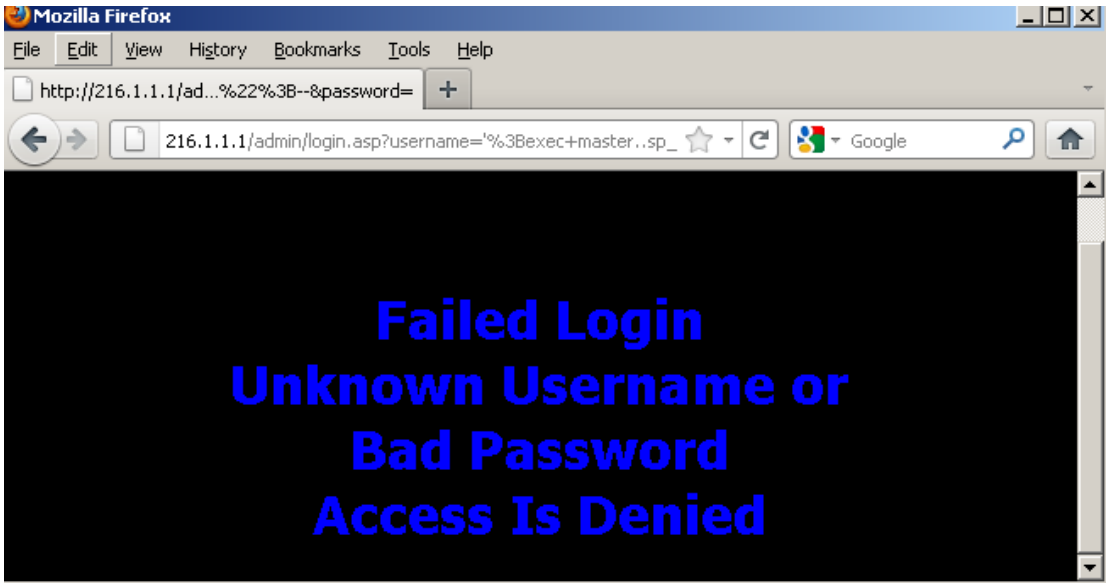

Figure 28: Inputting the Information into the Username Field

5. Click the down arrow to the right of the URL bar and drop down to **216.1.1.1**.

Figure 29: Returning to the Home Page

6. Highlight the sixth line of the sql.txt file. Select Edit, then **Copy** from the menu.

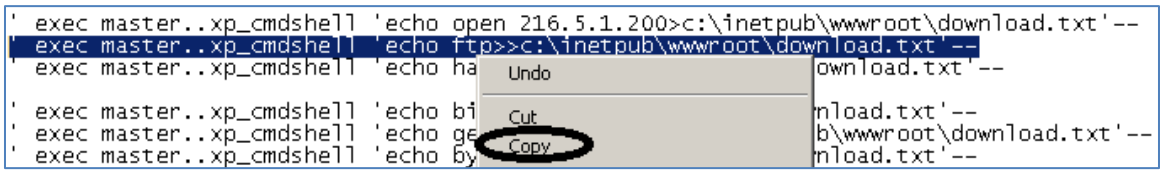

Figure 30: Copying a Line of Text

7. Right-click in the username field and select paste. Click the submit button.

Figure 31: Inputting the Information into the Username Field

You should see a web page with the response displayed in the figure below:

Figure 32: Inputting the Information into the Username Field

8. Click the down arrow to the right of the URL bar and drop down to **216.1.1.1**.

Figure 33: Returning to the Home Page

9. Highlight the seventh line in sql.txt. Select Edit, then Copy from the menu.

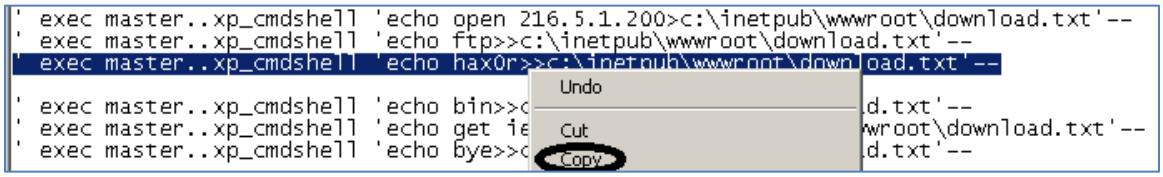

Figure 34: Copying a Line of Text

10. Right-click in the username field and select **Paste**. Click the Submit button.

Figure 35: Inputting the Information into the Username Field

You should see a web page with the response displayed in the figure below:

Figure 36: Inputting the Information into the Username Field

11. Click the down arrow to the right of the URL bar and drop down to **216.1.1.1**.

Figure 37: Returning to the Home Page

12. Highlight the eighth line in the sql.txt file. Select Edit, then **Copy** from the menu.

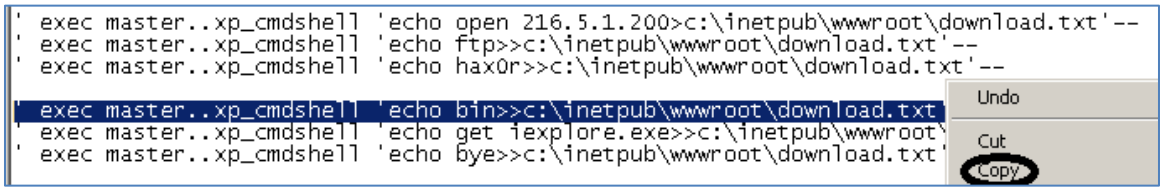

Figure 38: Copying a Line of Text

13. Right-click in the Username field and select Paste. Click the Submit button.

Figure 39: Inputting the Information into the Username Field

You should see a web page with the response displayed in the figure below:

Figure 40: Inputting the Information into the Username Field

14. Click the down arrow to the right of the URL bar and drop down to **216.1.1.1**.

Figure 41: Returning to the Home Page

15. Highlight the ninth line in the sql.txt file. Select Edit, then **Copy** from the menu.

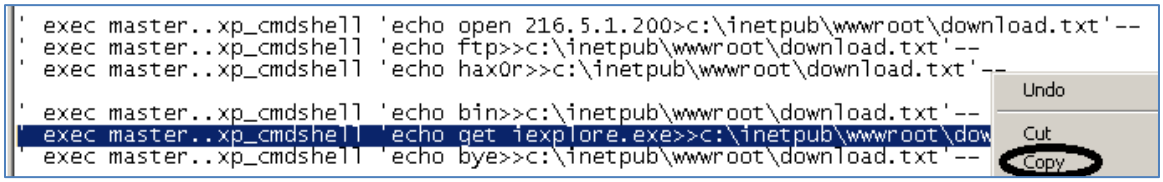

Figure 42: Copying a Line of Text

16. Right-click in the username field and select paste. Click the submit button.

Figure 43: Inputting the Information into the Username Field

You should see a web page with the response displayed in the figure below:

Figure 44: Inputting the Information into the Username Field

17. Click the down arrow to the right of the URL bar and drop down to **216.1.1.1**.

Figure 45: Returning to the Home Page

18. Highlight the tenth line in the sql.txt file. Select Edit, then **Copy** from the menu.

Figure 46: Copying a Line of Text

19. Right-click in the username field and select paste. Click the submit button.

Figure 47: Inputting the Information into the Username Field

You should see a web page with the response displayed in the figure below:

Figure 48: Inputting the Information into the Username Field

20. Click the down arrow to the right of the URL bar and drop down to 216.1.1.1.

Figure 49: Returning to the Home Page

21. Go to the Public IP address of XYZ Company by typing this URL in your browser: http://216.1.1.1/download.txt

You should have the same 6 lines in the figure below. If not, return to Step 3 of this task.

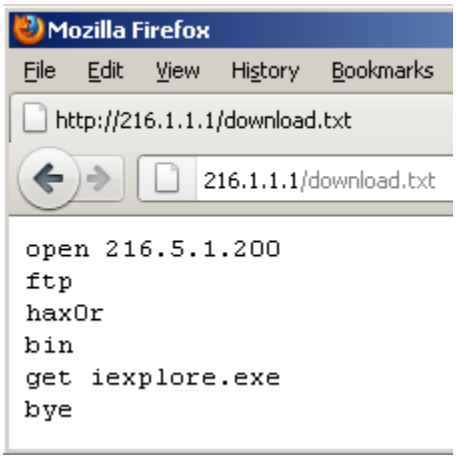

Figure 50: The Created FTP file

22. Open Wireshark on Windows 7 by clicking the shortcut on the desktop.

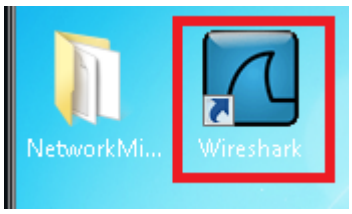

Figure 51: Opening Wireshark

23. Select **Capture** from the Wireshark menu bar and go down to **Interfaces**.

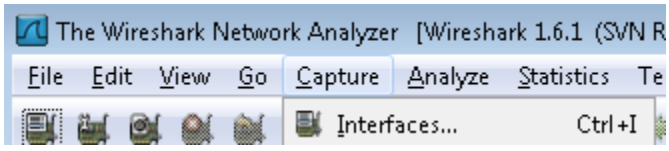

Figure 52: Selecting Interfaces from the Capture Menu

24. Click on the IPv6 Address to change it to an IPv4 Address. Click **Start**.

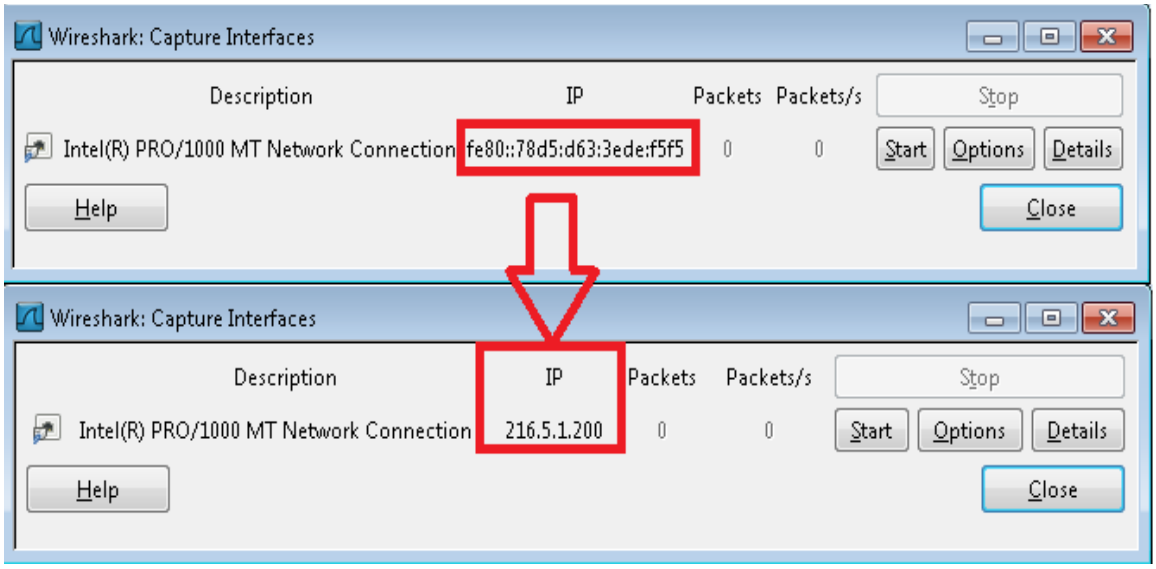

Figure 53: Changing IPv6 to IPv4

25. Type ftp (all lowercase) in the Wireshark filter pane and click **Apply** to the filter.

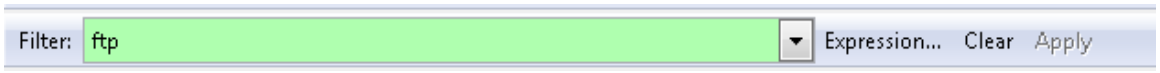

Figure 54: ftp Filter in Wireshark

26. Click the down arrow to the right of the URL bar and drop down to **216.1.1.1**.

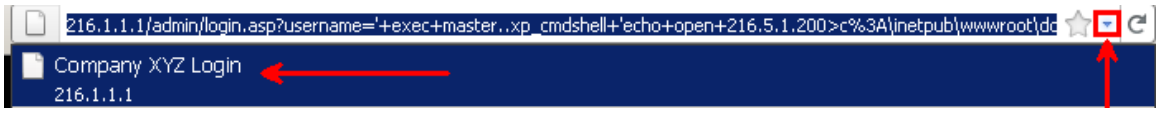

Figure 55: Returning to the Home Page

27. Highlight the eleventh line in sql.txt. Select Edit, then **Copy** from the menu.

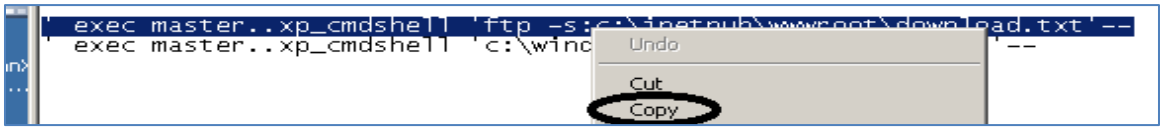

Figure 56: Copying a Line of Text

28. Right-click in the **Username** field and select Paste. Click the Submit button.

Figure 57: Inputting the Information into the Username Field

You should see a web page with the response displayed in the figure below:

Figure 58: Inputting the Information into the Username Field

In the Wireshark capture, you should see the transfer complete response. Notice **RETR iexplore.exe**.

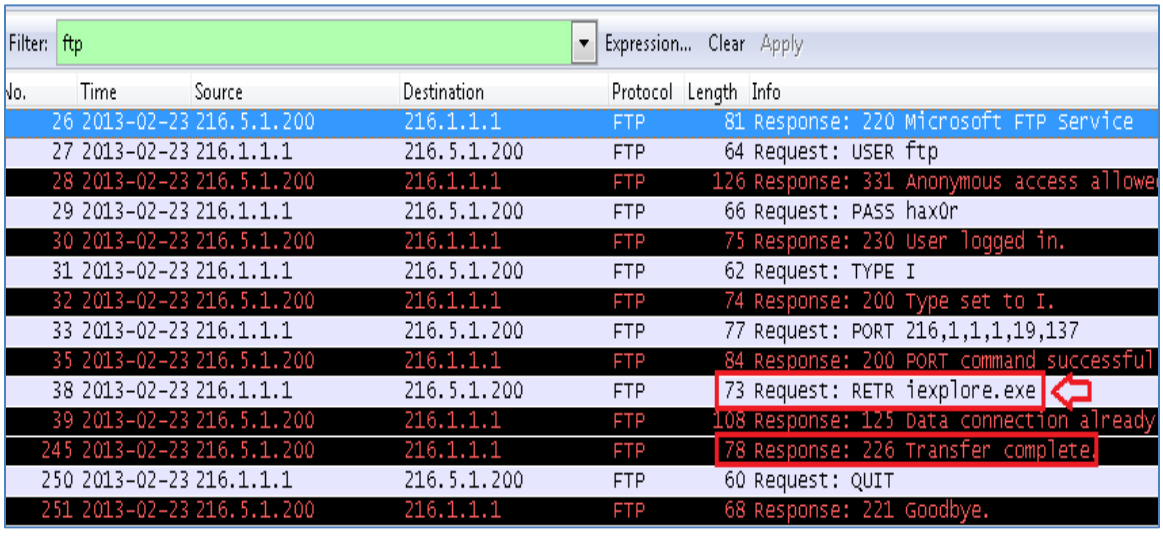

Figure 59: Inputting the Information into the Username Field

29. Click the down arrow to the right of the URL bar and drop down to **216.1.1.1**.

Figure 60: Returning to the Home Page

30. Highlight the eleventh line in sql.txt. Select edit, then copy from the menu.

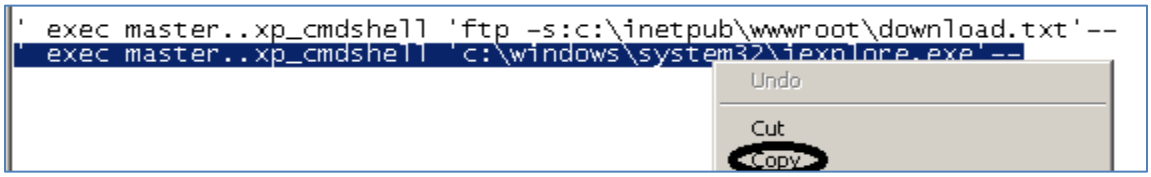

Figure 61: Copying a Line of Text

31. Right-click in the username field and select Paste. Click the Submit button.

Figure 62: Inputting the Information into the Username Field

You should now have a Dark Comet connection to the victim SQL server machine.

Figure 63: A Dark Comet Connection to the Victim (Thanks to SQL Injection)

32. Examine the Dark Comet program and notice the Public and Private IP address.

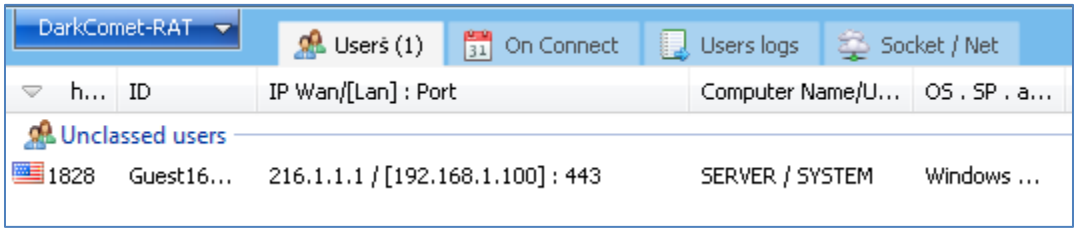

Figure 64: A Dark Comet Connection to the Victim (Thanks to SQL Injection)

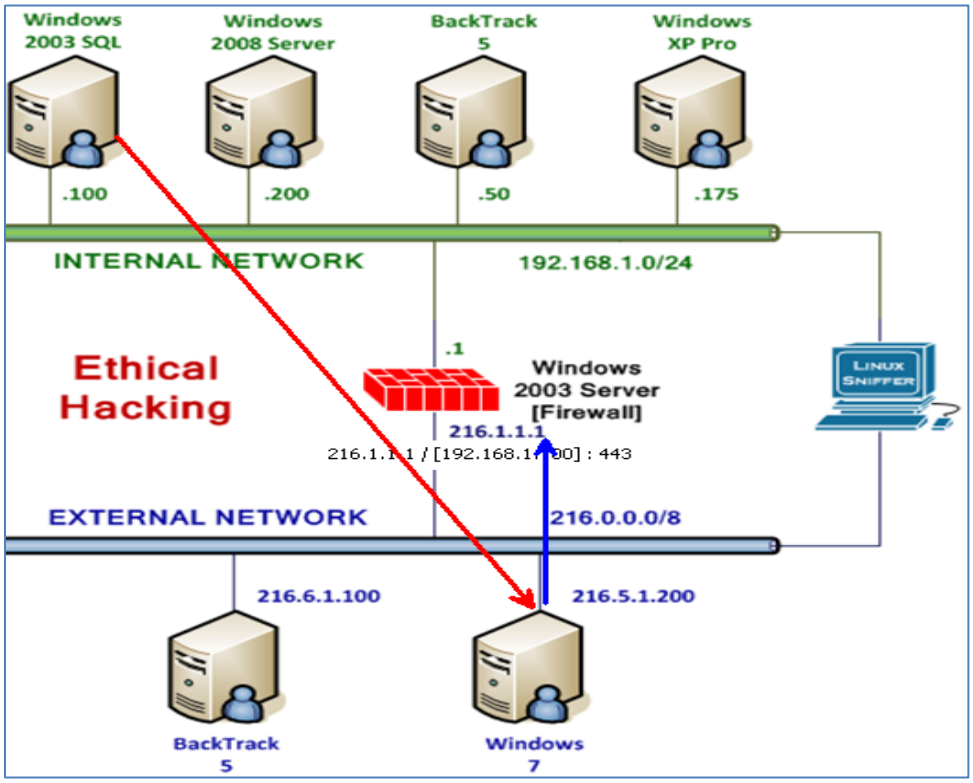

Figure 65: The WAN/LAN connections

2.2 Conclusion

A malicious Dark Comet payload is coded with the IP address and listening port of the attacking machine. In this case, SQL injection was utilized to upload the malware.

2.3 Discussion Questions

1. How do you change the Interface in Wireshark from IPv6 to IPv4?
2. How does Network Address Translation, or NAT, affect Dark Comet?
3. What is the procedure to disable JavaScript in Firefox ?
4. What would be a good name for a piece of malware to help disguise its presence?

3 Exploiting the Victim Machine

In this section, you will be using Dark Comet to exploit the victim. Only some of Dark Comet's capabilities will not be covered in this lesson, so it is recommended that you consider performing additional experimentation with the software within the isolated environment.

Never use Dark Comet or perform SQL injection outside of the isolated virtual environment.

3.1 Exploiting the Victim Machine with Dark Comet

1. On the Windows 7 machine, double click on the connection. A window will open with a large number of actions that you can perform against the victim machine.

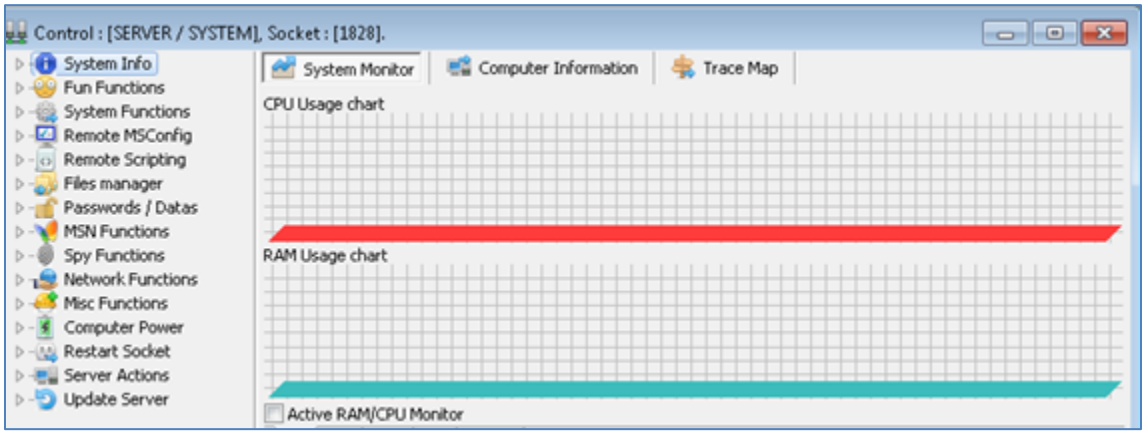

Figure 66: The connection to the Victim

2. Click the **Computer Information** tab to display information about the victim.

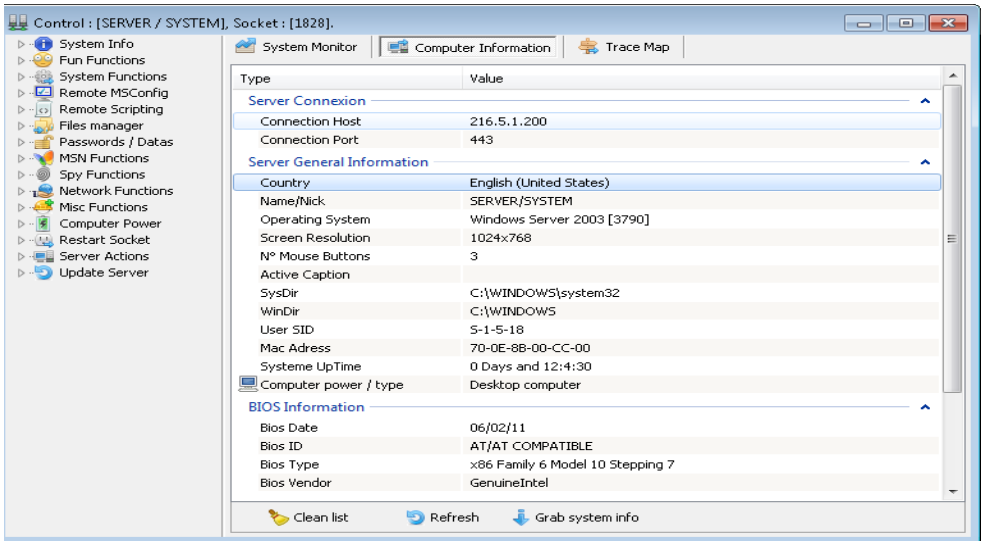

Figure 67: Information Screen of Dark Comet

3. Click on **Files Manager > Explorer files**. The left pane represents your Windows 7 machine and the right pane shows the drives on the victim machine. You can use this section to upload and download files over Dark Comet's encrypted network connection.

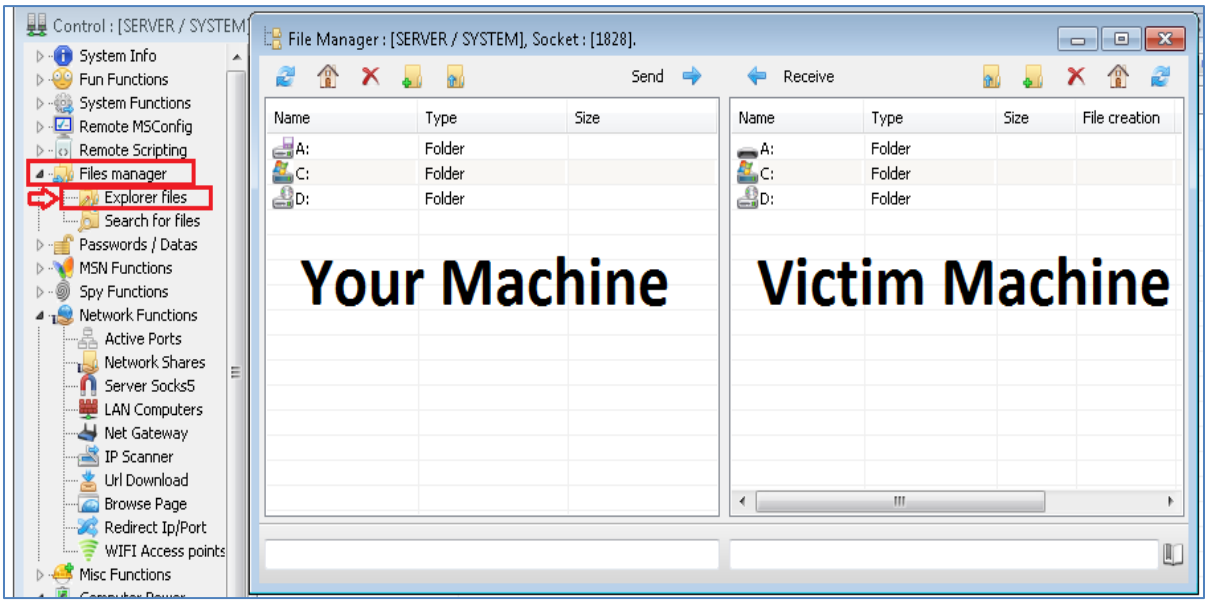

Figure 68: Managing Files on the Remote Machine

4. Double-click on the C: Drive on the victim's machine to view the drive's contents.

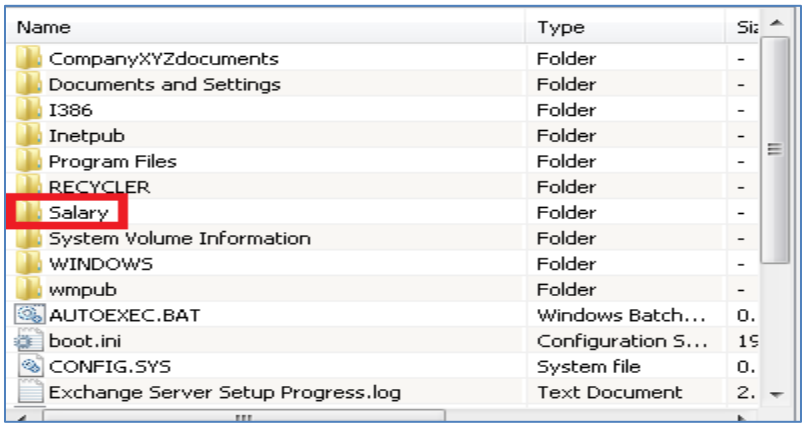

Figure 69: Folders on the Remote Machine

Many of the folders are common to all Windows distributions like the Windows and Program Files. The I386 directory holds install files. While Documents and Settings (Now Users on Vista and Higher) often stores documents, this is a server, so it is unlikely much is stored there. Two folders of interest are CompanyXYZdocuments and Salary.

5. In the right pane, (Your Windows 7 Machine) **click C: > Users > Student > Desktop.** In the left pane, (the victim machine) go into the Salary folder. Click on the spreadsheet file located in the Salary folder. Click the **Receive** button to exfiltrate the XLSX Spreadsheet from the victim.

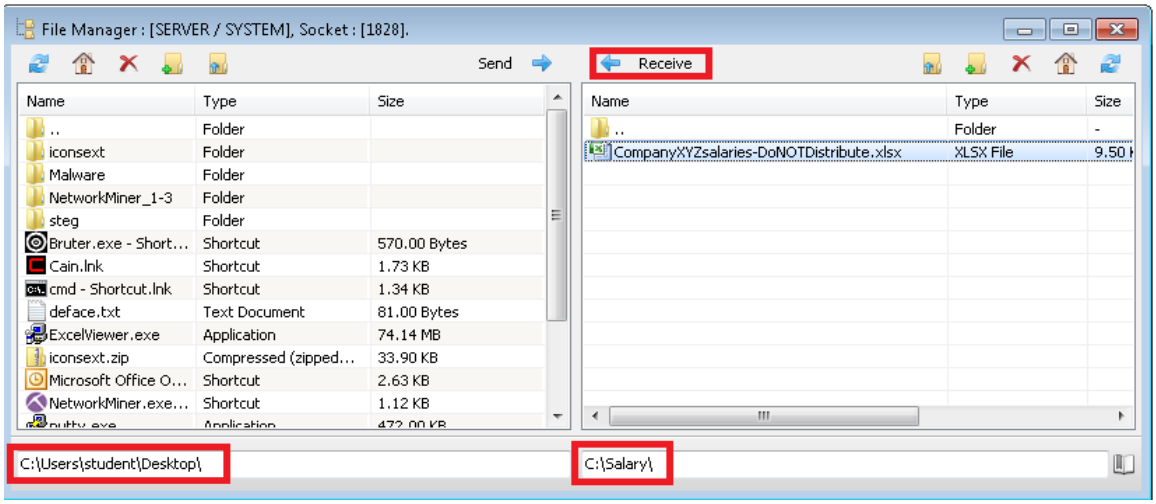

Figure 70: Exfiltrate the Data

6. Open the CompanyXYZsalaries-DoNOTDistribute.xlsx file on your desktop.

	A	B
1	Employee	Salary
2		
3	Amanda Anderson	47,000
4	Baron Beetle	39,000
5	Robert Carington	56,000
6	Charile Casington	78,000
7	Dana Dantfield	64,500
8	Eddy Frome	33,115
9	Gary Garrison	88,771
10	Andy Meterson	99,122
11	Raymond Miller	179,995
12	Steve Perkins	45,551
13	Al Teeing	61,123
14	Zachery Yickson	12,345

Figure 71: The Exfiltrated Spreadsheet

3.2 Conclusion

Dark Comet is a Graphical User Interface, or GUI, that allows the hacker to perform malicious tasks against a victim machine, like data-theft over an encrypted connection.

3.3 Discussion Questions

1. Name the folders located on C:, which are common to all Windows distributions.
2. What is the purpose of the i386 folder?
3. On what machines would the Documents and Settings folder be rarely used?
4. Why is it difficult to detect the Excel file being stolen if Dark Comet is utilized?

References

1. Dark Comet RAT:
   http://darkcomet-rat.com/

2. Malware Analysis - Dark Comet RAT:
   http://www.contextis.com/research/blog/malware-analysis-dark-comet-rat/

3. DarkComet RAT Pulled by Developer:
   http://www.securityweek.com/darkcomet-rat-pulled-developer

4. Dark Comet 2: Electric Boogaloo:
   blog.malwarebytes.org/intelligence/2012/10/dark-comet-2-electric-boogaloo/

5. DarkComet RAT Flames Out:
   http://threatpost.com/en_us/blogs/darkcomet-rat-flames-out-070912

