Ethical Hacking Lab Series

Lab 4: Poison Ivy - Remote Access Trojan

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

Document Version: 2013-07-18 (Beta)

Organization: Moraine Valley Community College
Author: Jesse Varsalone

.

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

Contents

Introduction 3
Domains: System Hacking ,Trojans and Backdoors, Viruses and Worms 3
Pod Topology 5
Lab Settings 6
1 Setting up the Poison Ivy Client (Server) 7
1.1 Configuring the Poison Ivy Client 7
1.2 Conclusion 13
1.3 Discussion Questions 13
2 Convincing the Victim to Launch the Malicious File 14
2.1 Creating the Payload 14
2.2 Conclusion 26
2.3 Discussion Questions 26
3 Exploiting the Victim Machine with Poison Ivy 27
3.1 Exploitation with Poison Ivy 27
3.2 Conclusion 30
3.3 Discussion Questions 30
References 31

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 Poison Ivy Client (Server)
2 - Convincing the Victim to Launch the Malicious File
3 - Exploiting the Victim Machine with Poison Ivy

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

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

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

Poison Ivy is an extremely dangerous piece of malware that will allow attackers to maintain a persistent connection on a victim's machine through an encrypted connection. There have been several high profile cases where Poison Ivy was used as an attack tool during an intrusion, including the attack against RSA's (a division of EMC Corporation) network in 2011.

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

Poison Ivy – Remote Access Trojan that has been used frequently in many high profile intrusion cases. The tool has a Graphical User Interface, or GUI, that allows the hacker to perform malicious tasks against a victim machine over an encrypted connection. Poison Ivy consists of two components, the server and the client.

Poison Ivy Client – Although it may seem counterintuitive, the Poison Ivy client is configured on the machine that will act as the server and accept client connections. Any port may be used for the "client", but a common port like 80 (Hyper Text Transfer

Protocol) or 443 (Hyper Text Transfer Protocol Secure) or 443 will make the connection from the victim to the attacker seem a bit less conspicuous than a port like 12345.

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

Wrapper – A program that allows you to combine multiple executable files into a single executable. From a malicious standpoint, an attacker could package a malicious executable with a legitimate one and use this to launch an attack.

Pod Topology

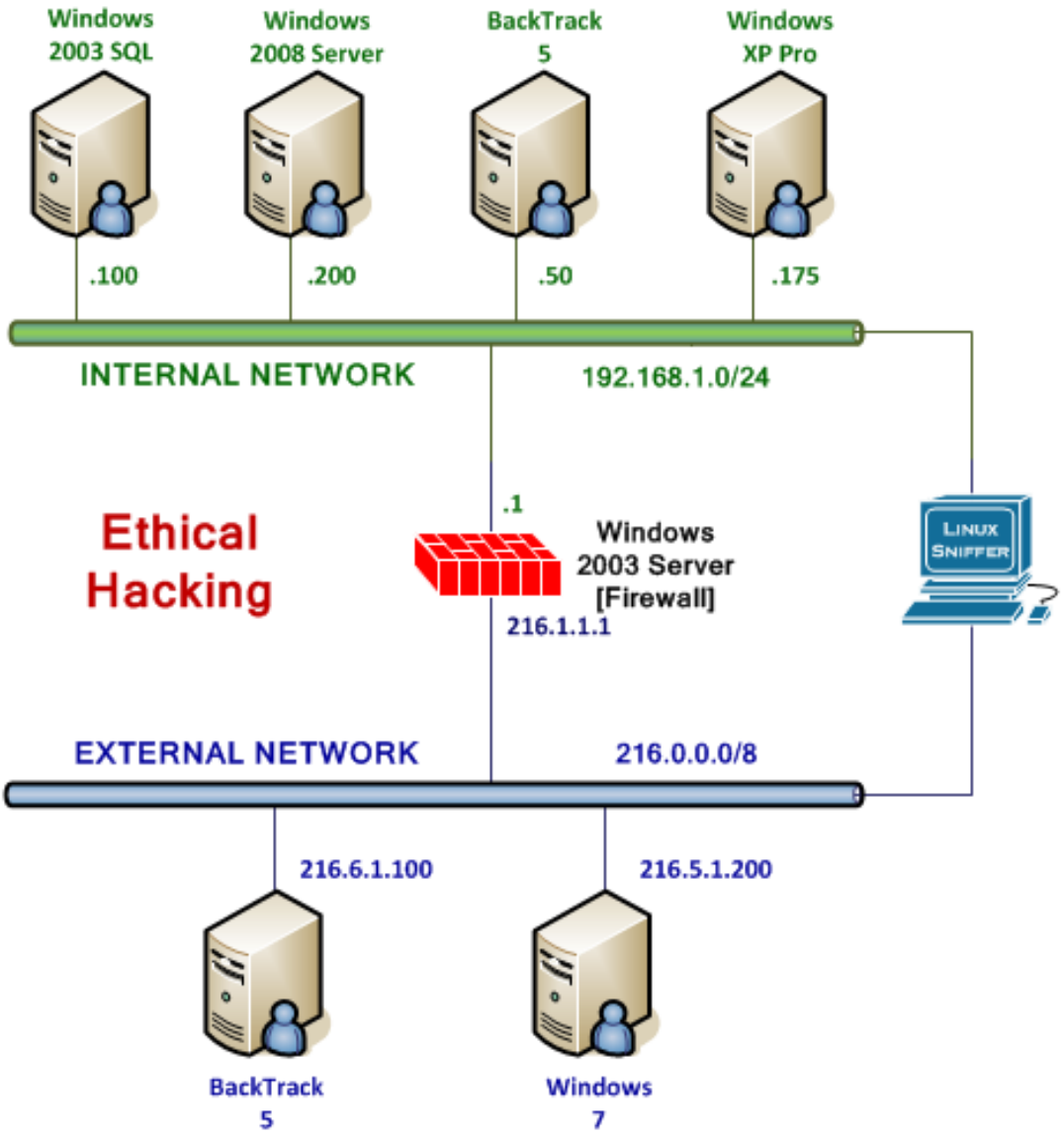

Figure 1: Lab Topology

Lab Settings

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

Required Virtual Machines and Applications

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

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

Windows XP Pro	192.168.1.175
Windows XP **Administrator** password	Ethicalhackin&
Windows 7	216.5.1.200 (Public IP)
Windows 7 **student** password	password

1 Setting up the Poison Ivy Client (Server)

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

1.1 Configuring the Poison Ivy Client

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

Figure 2: Logging in as Administrator

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

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

Figure 3: A Shortcut to the Command Prompt

3. On the XP system, type the following command to view your private IP address:
C:**ipconfig**

Figure 4: The ipconfig command

4. Now, ping the Windows 7 machine on the External Network by typing:
C:**ping 216.5.1.200**

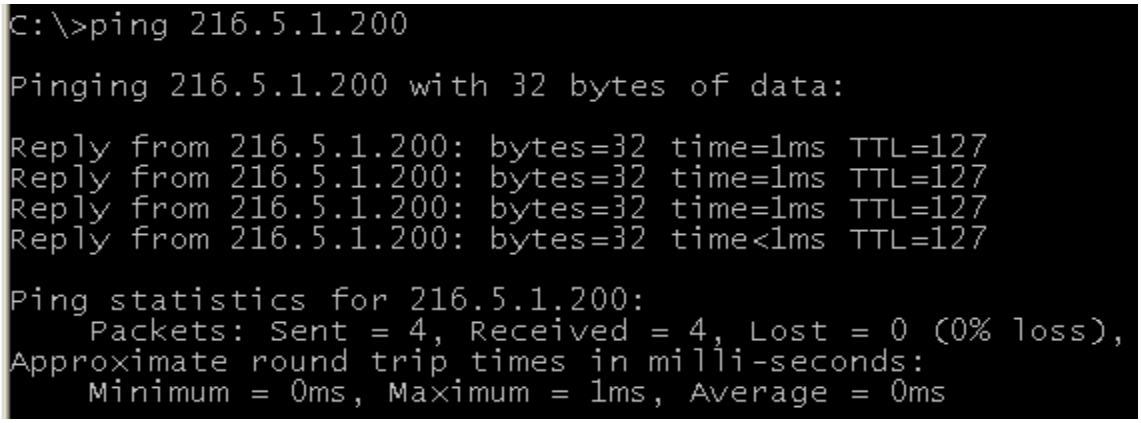

Figure 5: Successful ping of the Windows 7 machine

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

Figure 6: Opening a Command Prompt on Windows 7

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

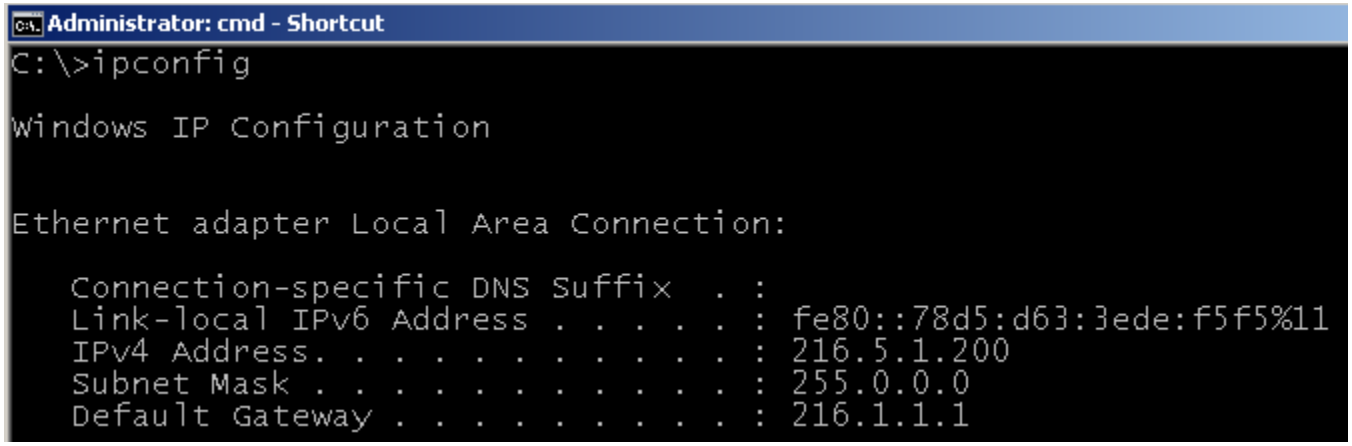

Figure 7: IP address Information on Windows 7

7. From the Windows 7 machine on the Public Internet (simulated), attempt to ping the Windows XP machine on the Internal Network by typing:
   C:**ping 192.168.1.175**

Notice, this will fail.

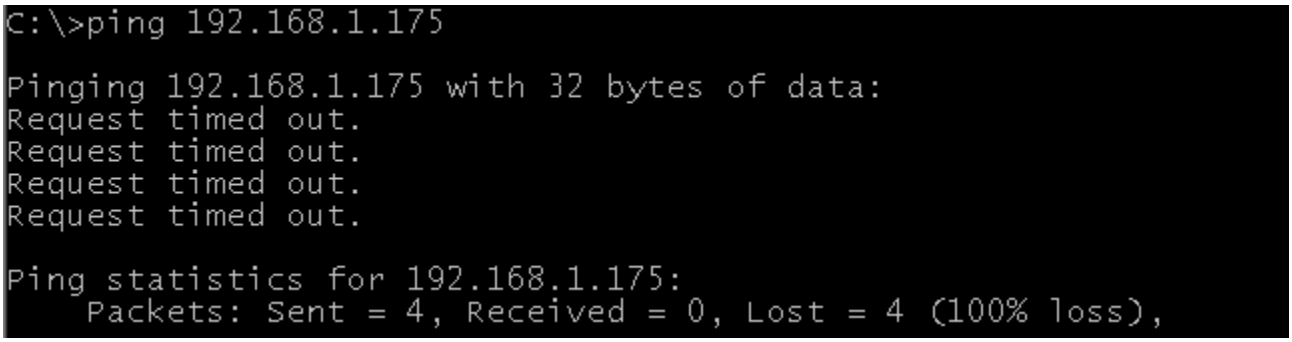

Figure 8: Failed Pings to the Machine on the Internal Network

The Windows 7 machine is using a Public IP address and is on the Wide Area Network, or WAN. Attackers trying to get on your internal network cannot directly attack the Windows XP machine because it is NATed behind the Firewall. The XP machine is not sitting on the Internet (simulated) with a Public IP address. The firewall is not redirecting any incoming traffic to the Windows XP machine.

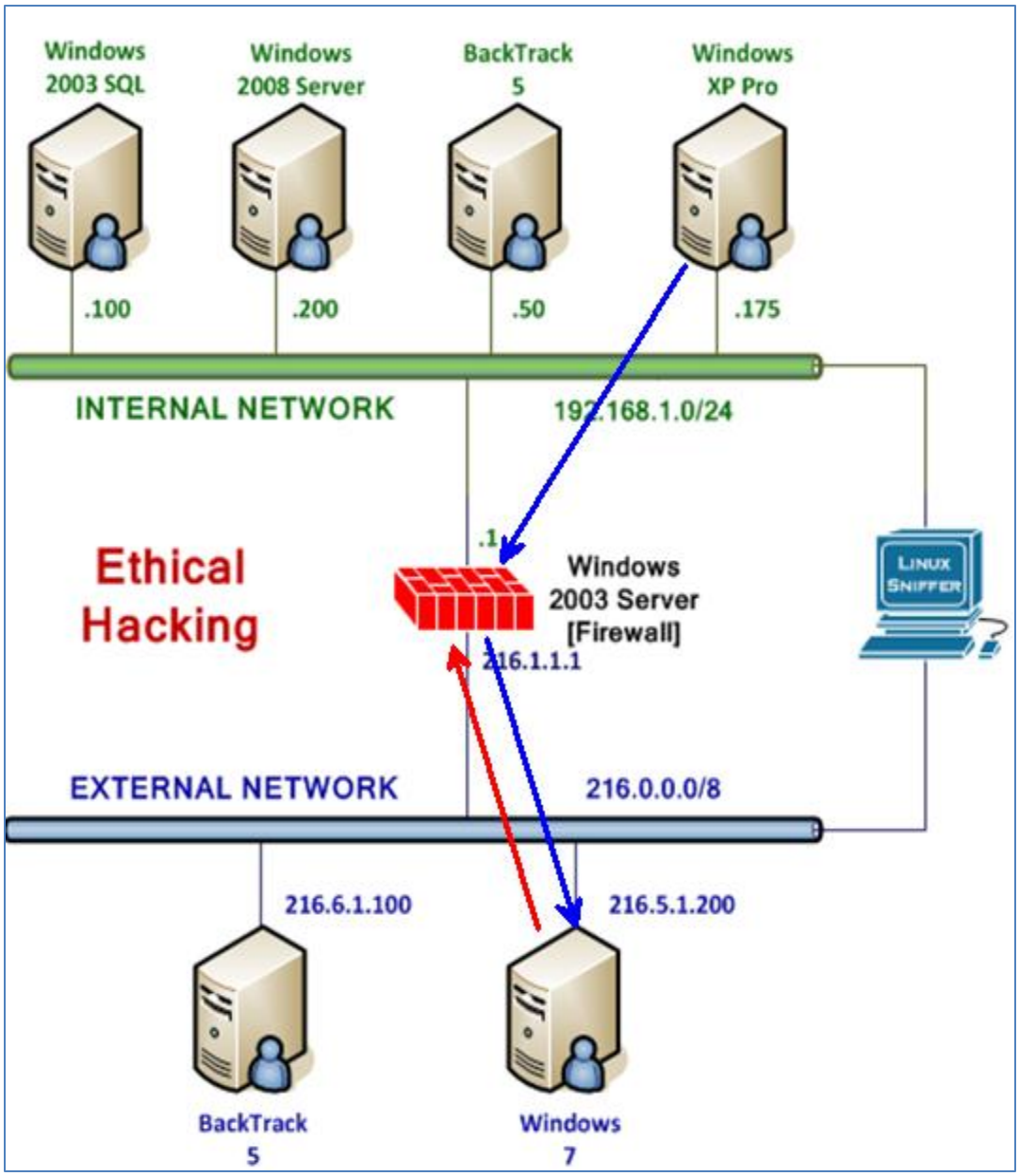

Figure 9: Internal Machines on Private Network are Unreachable from WAN

The only way for the attacker to get to the Windows XP machine is to have that machine on the internal network make a connection to the Public IP address of the Attacker.

8. Open the Malware folder on the Windows 7 desktop. Right-click on the PI2.3.2.rar file, select 7-zip and select the 4th choice down, **Extract to "PI2.3.2\"**.

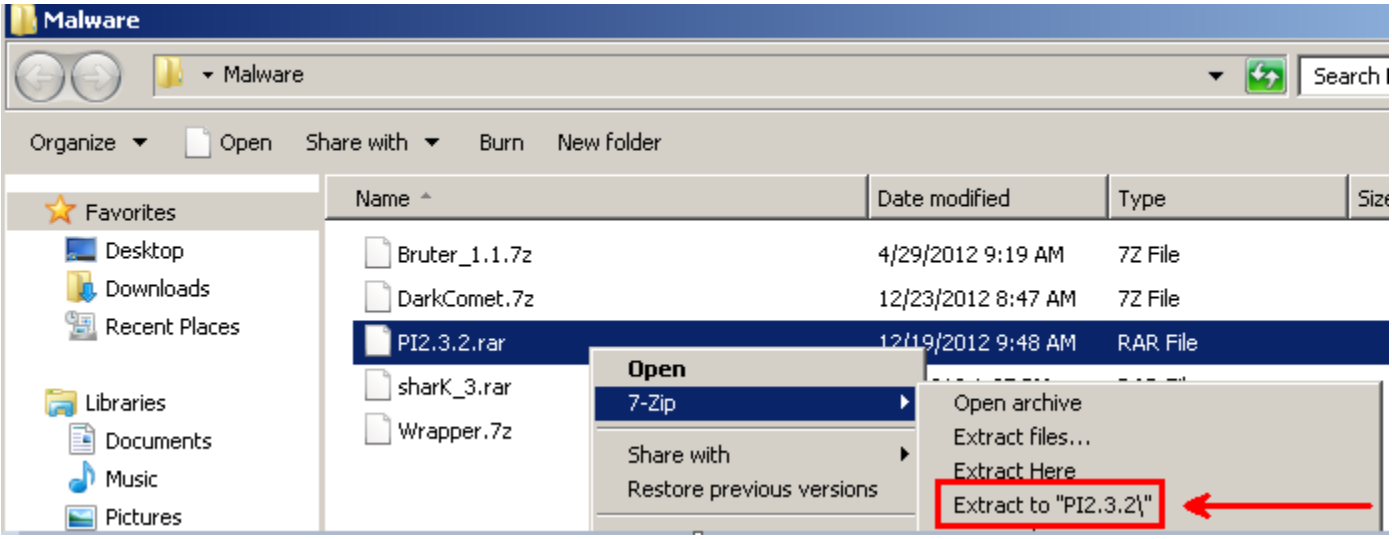

Figure 10: Extracting the file with 7-zip

9. Double-click on the PI2.3.2 folder and double-click on Poison Ivy 2.3.2.exe. Wait 10 seconds, click "Don't show this in the future" and click **I Agree**.

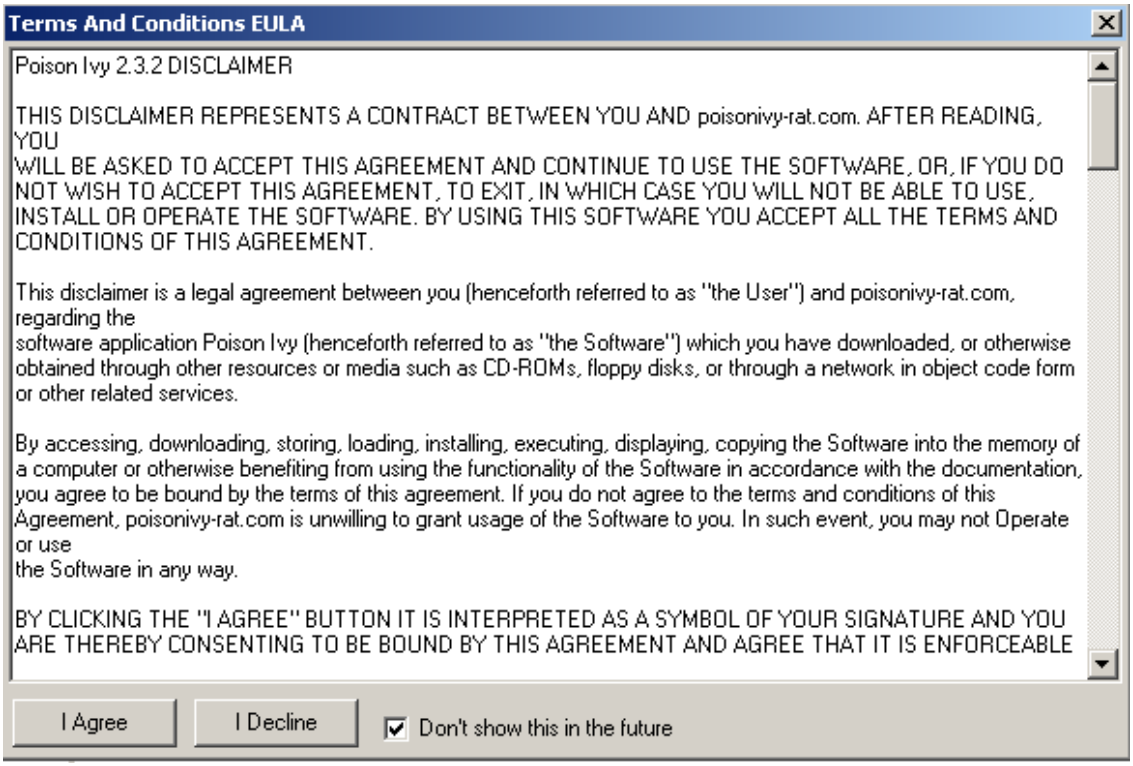

Figure 11: The Poison Ivy License Agreement

Although it may seem counterintuitive, the Poison Ivy client is configured on the machine that will act as the server and accept client connections. We will be configuring the Windows 7 VM to be the Poison Ivy Client (or Server, as it might be referred to).

10. From the Poison Ivy Menu bar, click File and select **New Client** from the list.

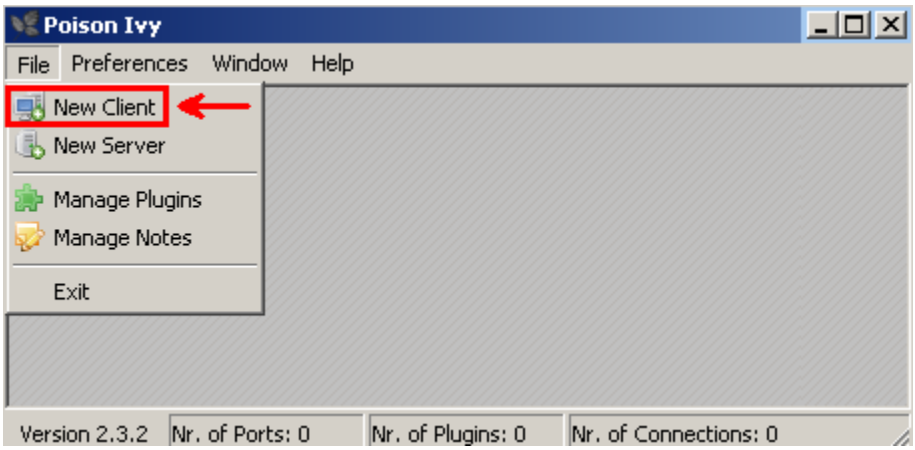

Figure 12: Select New Client

Any port may be used for the "client", but a common port like 80 (Hyper Text Transfer Protocol) or 443 (Hyper Text Transfer Protocol Secure) or 443 will make the connection from the victim to the attacker seem a bit less conspicuous than a port like 12345, or the default port of 3460. In this example, we will set up Poison Ivy to listen on port 443.

11. In the listen on Port box, type 443. Click **Start** to begin listening on that port.

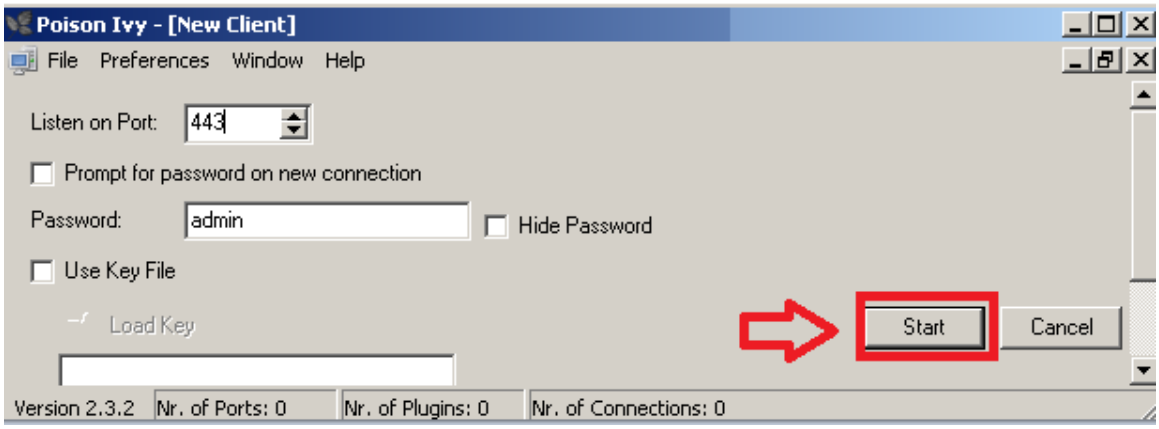

Figure 13: Listing Files with Hidden Attributes on the Root of C

The net stat command can be used to determine which ports the machine is listening on. If the –anb switch is added to the netstat command, the processes associated with each listening port will also be listed. The find command can be used to filter your results.

12. To verify that the attack machine is listening on port 443, type the following:
    C:\>**netstat -an | find "443" && netstat -anb | find "Poison"**

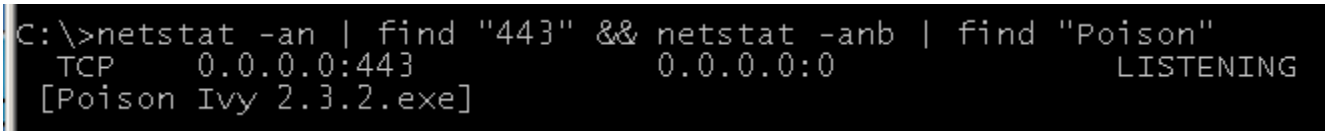

Figure 14: Poison Ivy is listening on Port 443

1.2 Conclusion

Poison Ivy is malware that has a server and a client component. The attacker first sets up the client, which will listen on a port and wait for connections. Attackers on the Internet cannot directly attack internal machines on an internal network. The only way for the attacker to get to the victim machine is to have that machine on the internal network launch a program so that will connect to an External IP address on the Internet.

1.3 Discussion Questions

1. How does someone on the Internet attack a machine with a private IP address?
2. What needs to be done after the Poison Ivy software is initially launched?
3. What is the command to determine if your machine is listening on port 443?
4. What is the command to determine the port Poison Ivy process is listening on?

2 Convincing the Victim to Launch the Malicious File

In this exercise, you will create the malicious Poison Ivy payload, and then convince the victim to launch the malware. We will package the malicious payload with a legitimate file in order to get the victim to "bite". We will do this by using a program called a wrapper. Wrappers are often used on the Internet to create special versions of open source software that have a bonus file or program that causes harm to a user's system.

2.1 Creating the Payload

1. From the Poison Ivy Menu bar, click File and select **New Server** from the list.

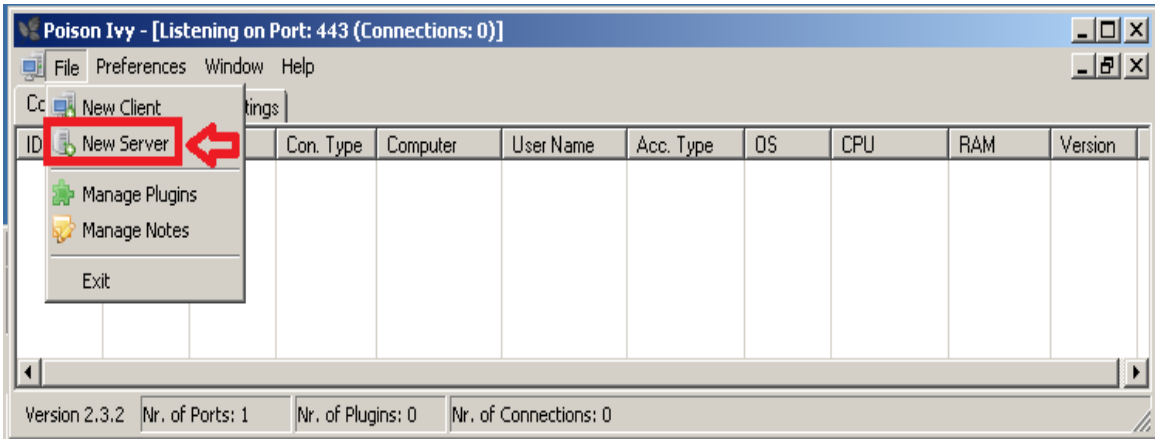

Figure 15: Creating the Poison Ivy "Server"

2. From the Profiles screen, click Create Profile. Name the Profile CEH and click OK.

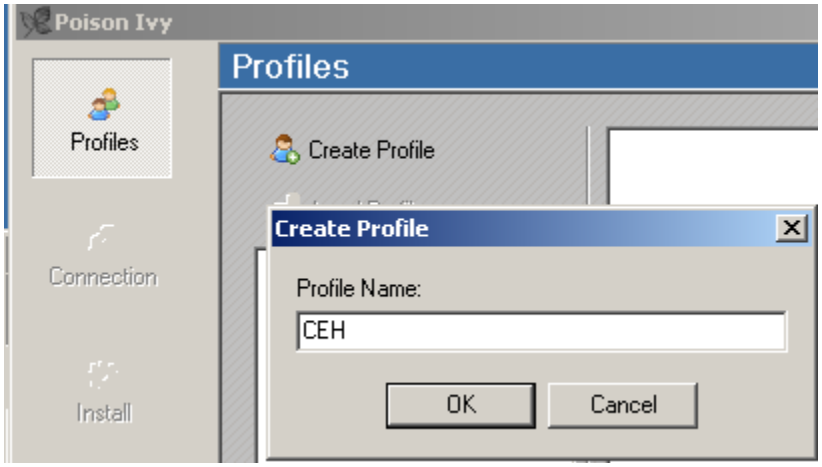

Figure 16: Creating a Profile within Poison Ivy

3. In the DNS/Port box, carefully type **216.5.1.200:443:0,** and click Next.

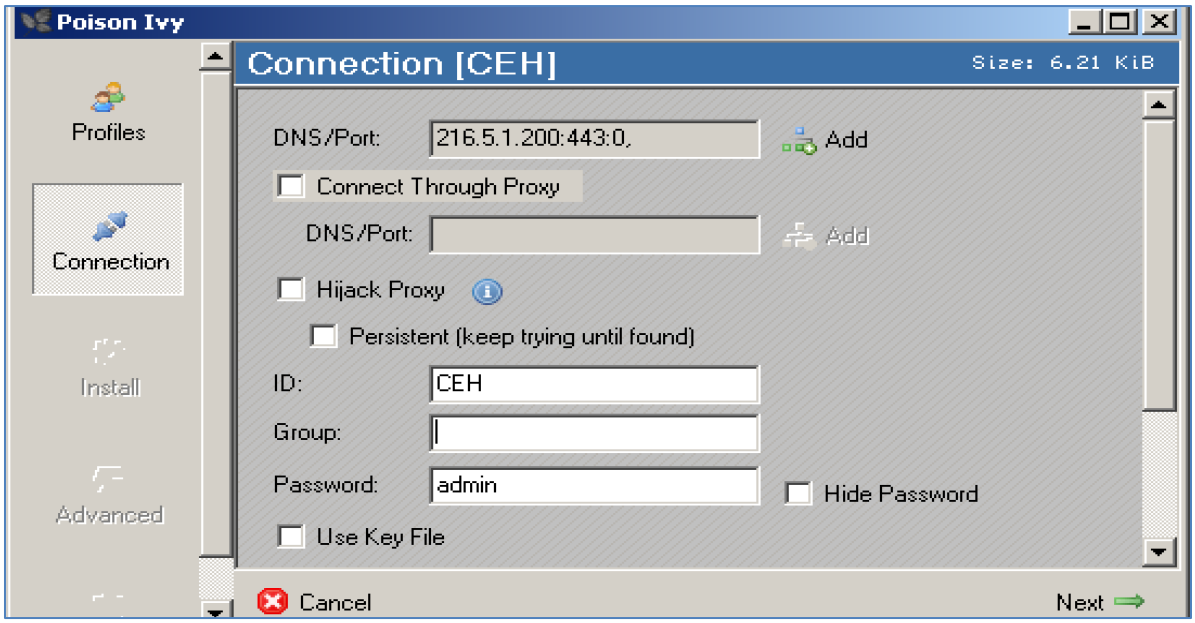

Figure 17: The Connection Screen in Poison Ivy

4. Check the box that states Start on system startup. Name the HKLM/Run Name **Norton** to disguise its presence. Then, click the next arrow to advance.

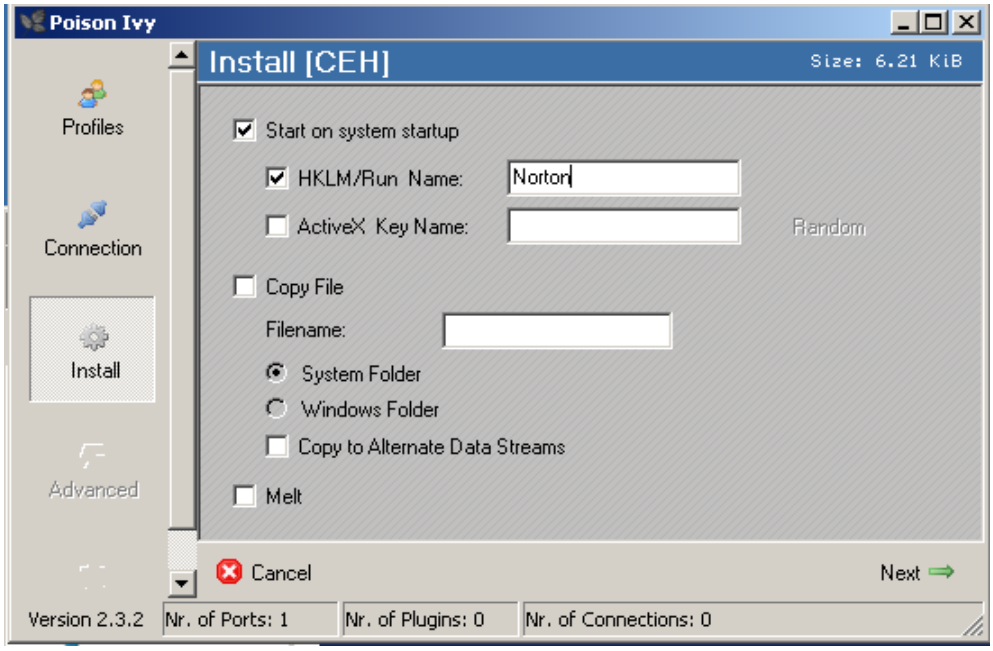

Figure 18: The Install Screen in Poison Ivy

5. At the Advanced Screen, leave all of the default options. Click Next to advance.

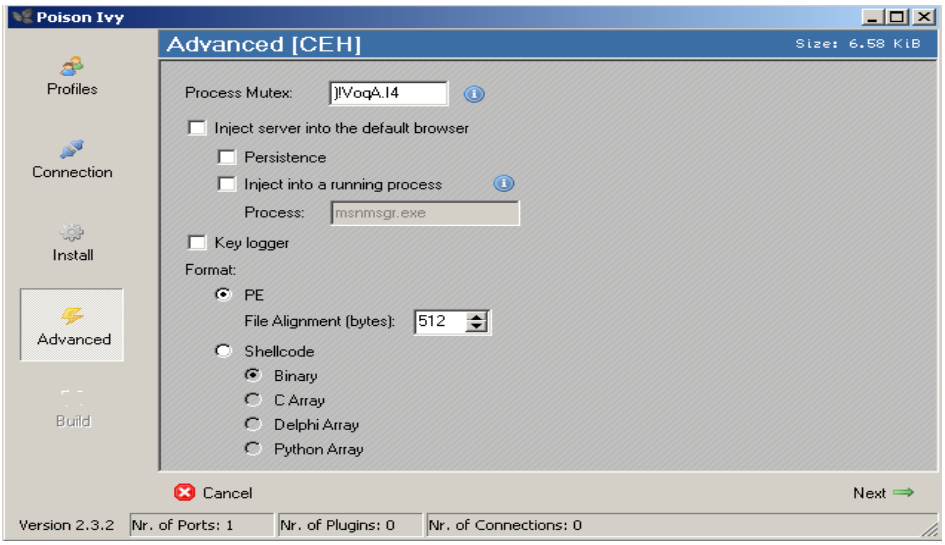

Figure 19: The Advanced Screen of Poison Ivy

6. First, click **Generate**. Then, click the desktop icon on the left in the **Save in** box. Name the file **iexplorer** and click save to save the generated payload.

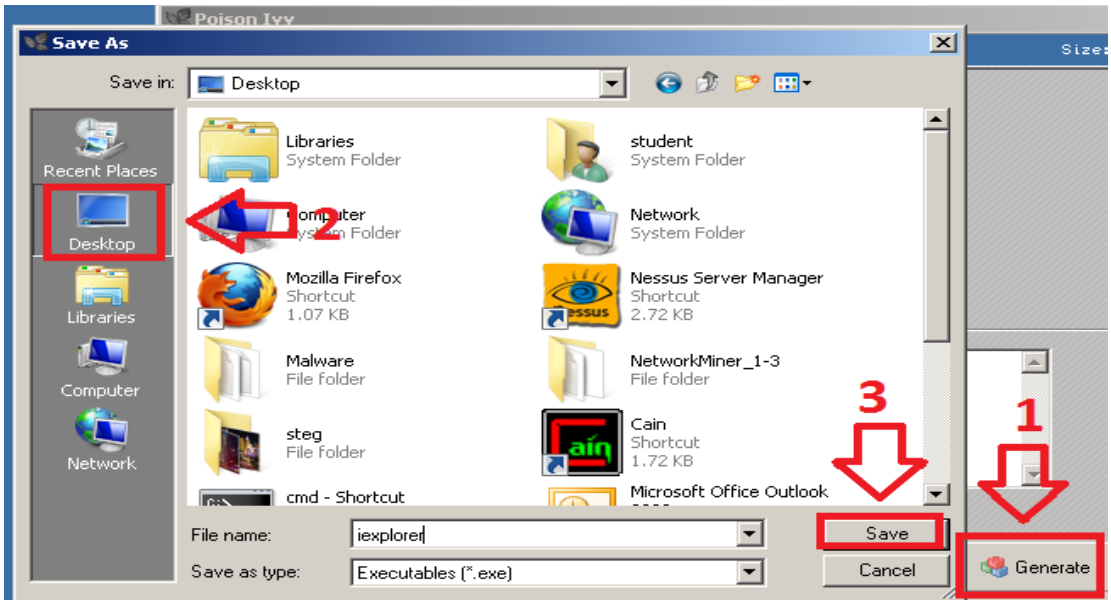

Figure 20: Generating the Payload

The name of the executable for Internet Explorer is iexplore.exe. The name of the executable for the Windows explorer is explorer.exe. We are using a similar file name. After you click OK, Poison Ivy will return to the screen that indicates it is listening on port 443.

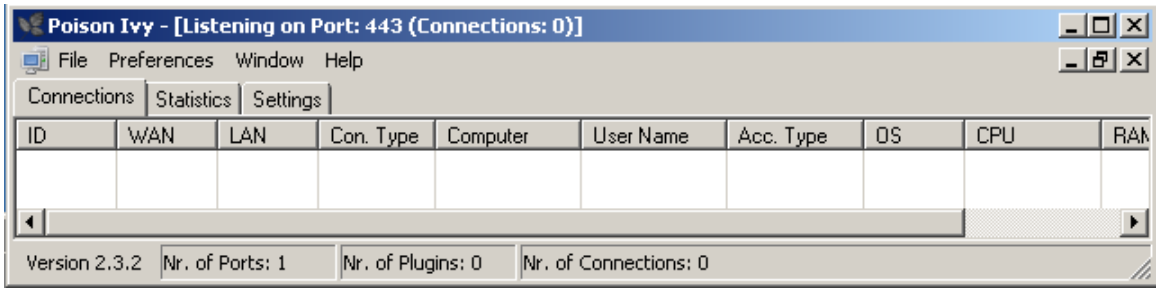

Figure 21: Listening on port 443

7. Open the Malware folder on the Windows 7 Desktop. Right-click on the wrapper.7z file, select 7-zip and select the 4th choice down, **Extract to Wrapper**.

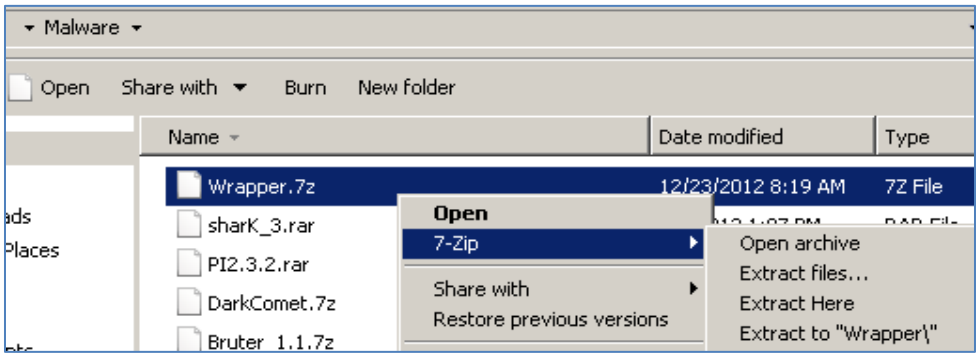

Figure 22: Extracting the program.

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

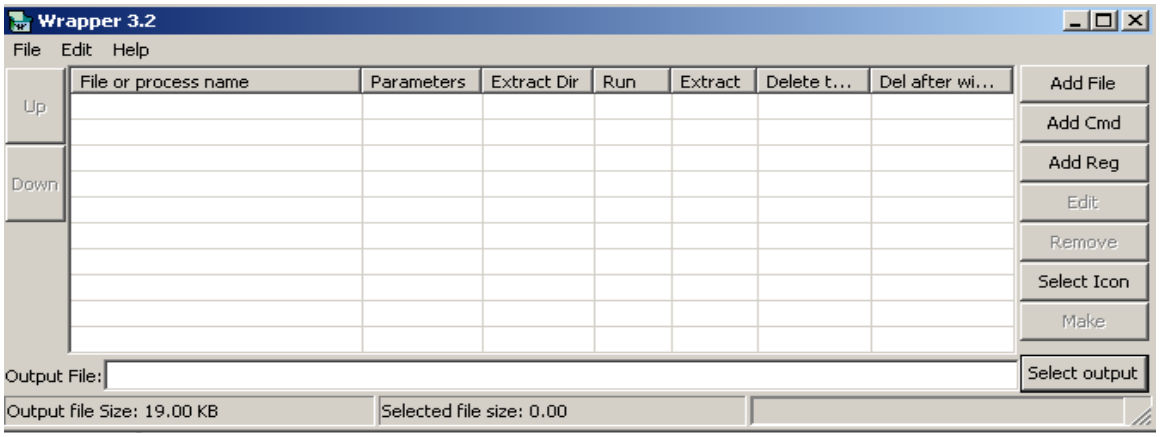

Figure 23: The Wrapper Program

9. Click **Add File**. Click the box to the right of the world filename. Browse to the desktop of your machine and select the iexplore.exe file. Click the OK button.

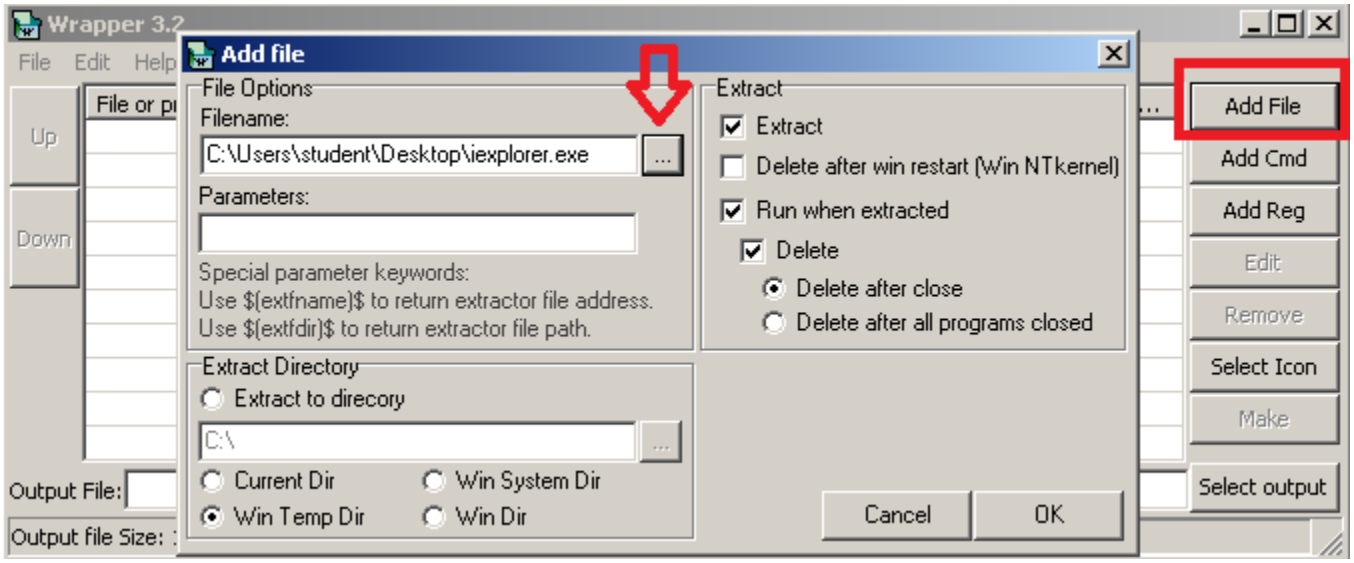

Figure 24: Adding a file

10. Click **Add file**. Click the box to the right of the world filename. Browse to the desktop of your machine and select the putty.exe file. Click the OK button.

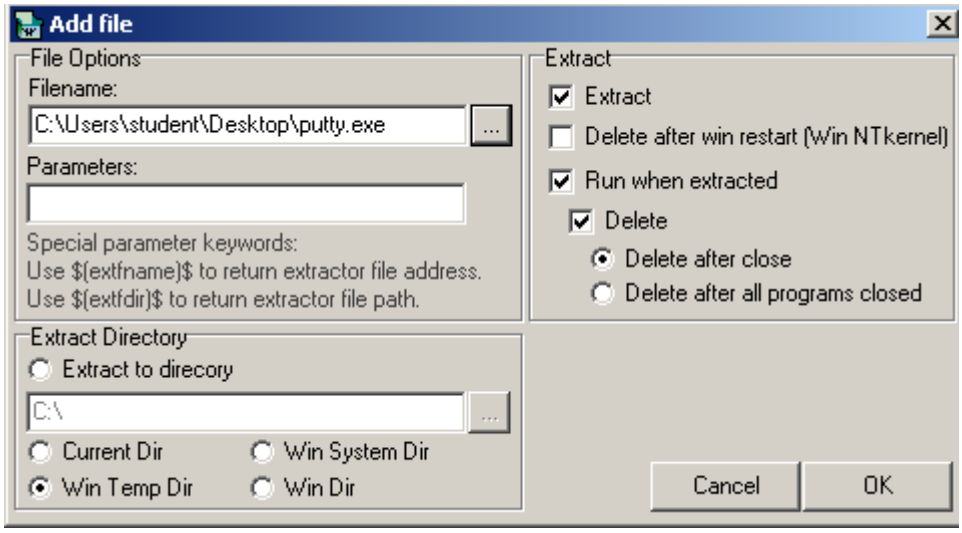

Figure 25: Adding an Additional file

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

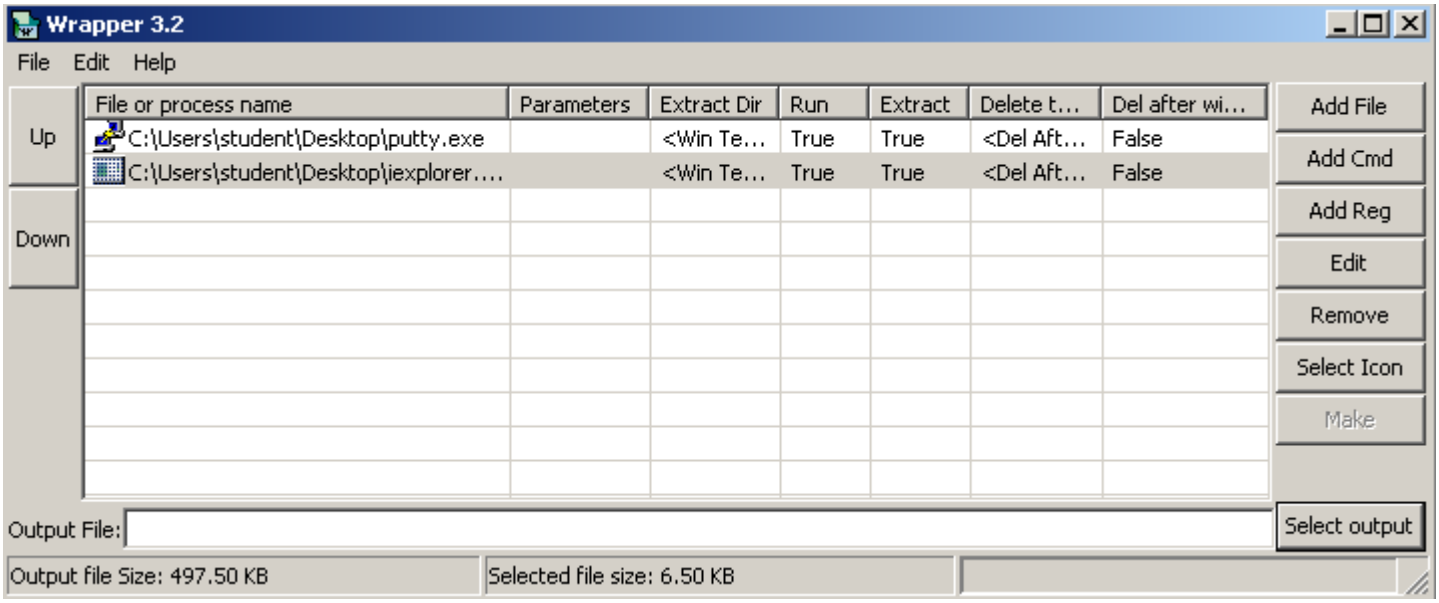

Figure 26: Two Files are Listed

11. Click the select output button in the lower right hand corner of wrapper. Navigate to **Local Disk (C:) > inetpub > ftproot**. Name the file **ssh**. Click Save.

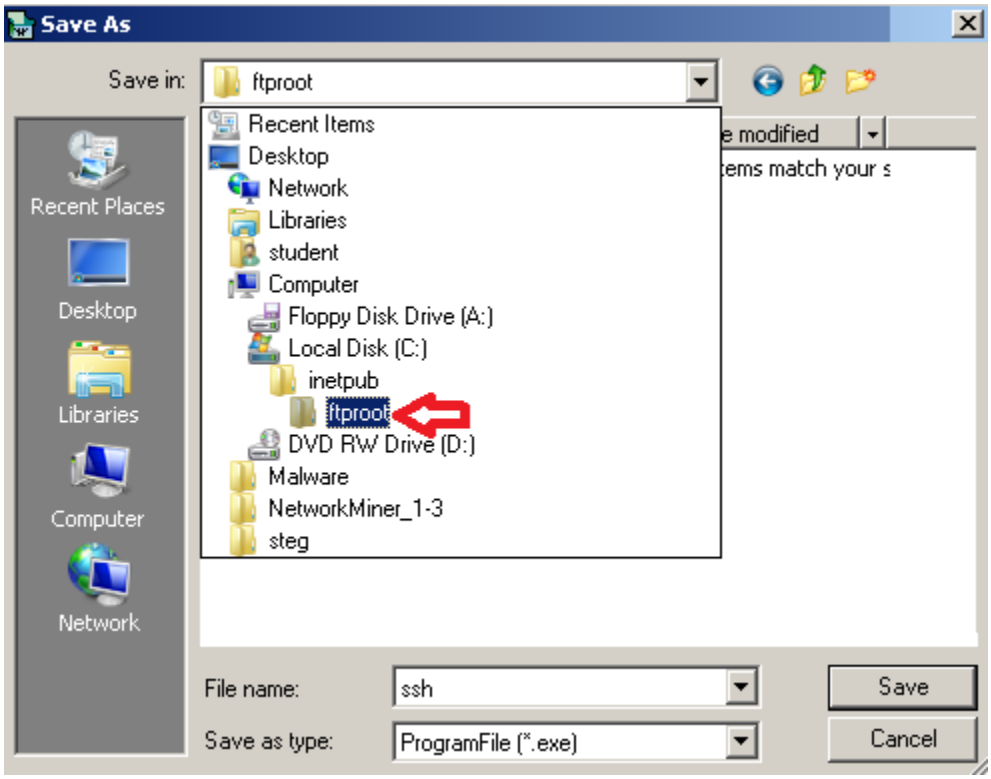

Figure 27: Saving the File to the FTProot Directory

12. Verify that the path is C:\Inetpub\ftproot\ssh.exe and click the **Make** button.

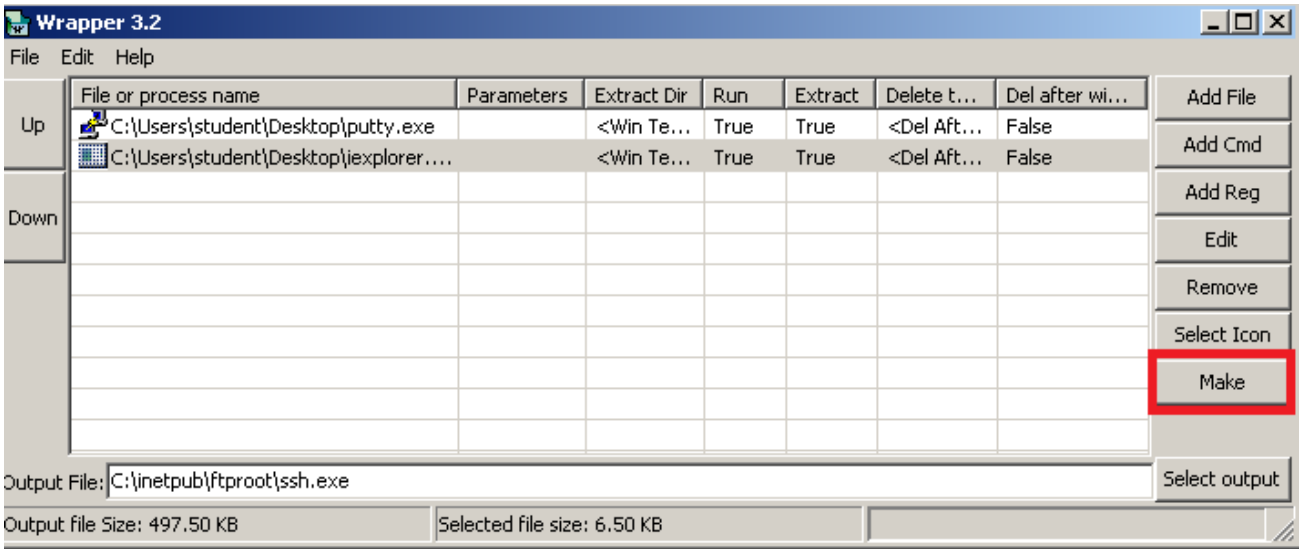

Figure 28: Making the Single File

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

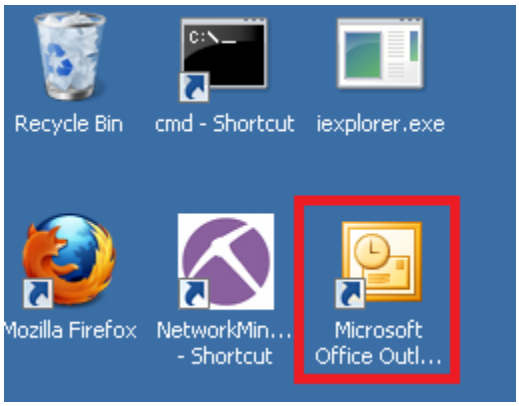

Figure 29: Opening Outlook

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

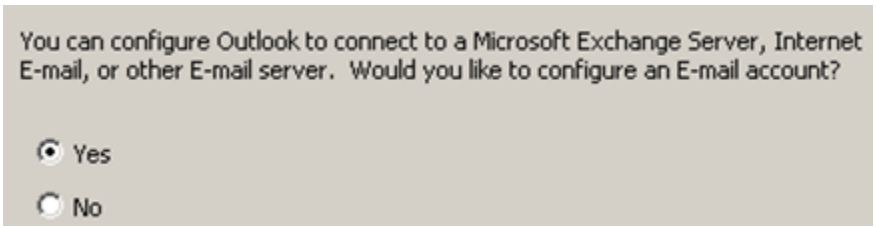

Figure 30: Opening Outlook

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

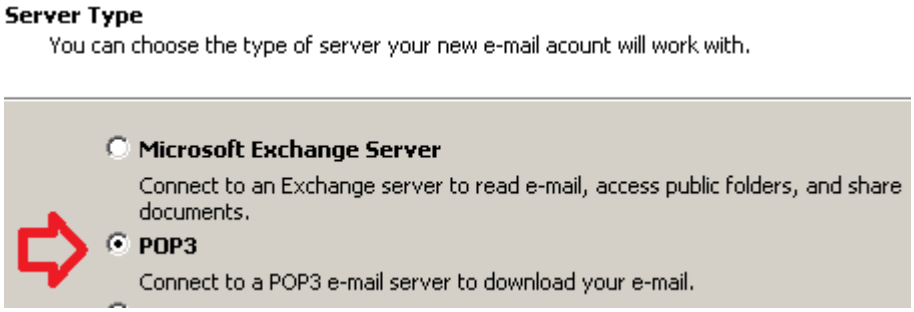

Figure 31: POP 3 Server

16. 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.

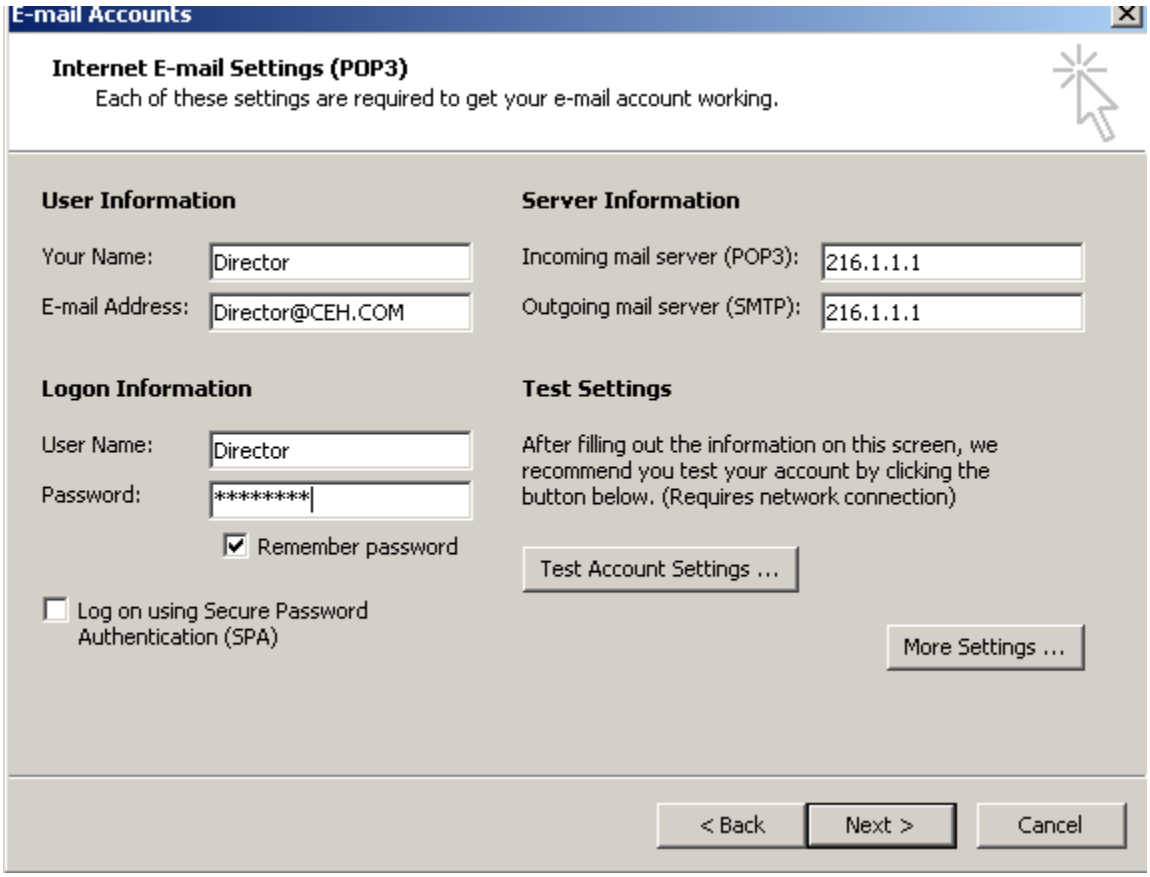

Figure 32: Mail Settings

In the next step, we will use a spear-phish attack, to get the administrator to open our ssh.exe software, which is putty wrapped with the iexplorer.exe Poison Ivy payload.

17. Click the new button in the top Left corner of Outlook.
18. Follow the steps below to send the email to rmiller.
    a. In the To box, type rmiller@XYZCOMPANY.COM
    b. In the Subject type, **Great SSH Utility**
    c. 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

    d. Click **Send** to send the email.

Do not click the **Send/Receive** button. The director email account does not exist.

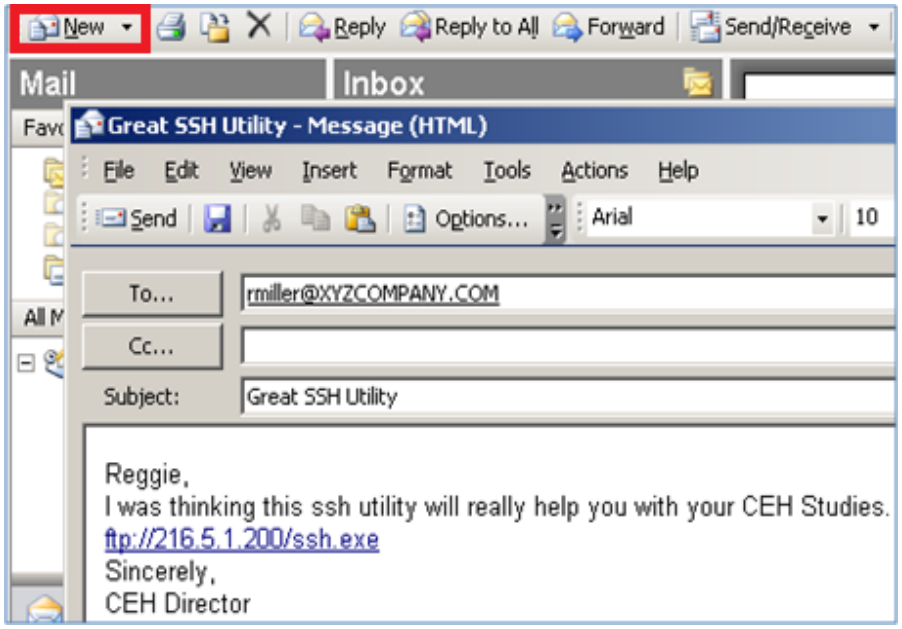

Figure 33: Spear Phish Email

19. Click on the start button on XP and then select Email from the Start menu.

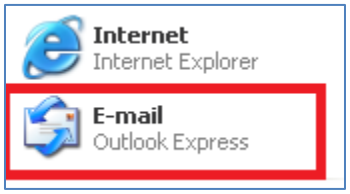

Figure 34: Opening Outlook Express

20. On the **Windows XP Pro** machine, Click the **Send/Receive** button to ensure that the email is received.

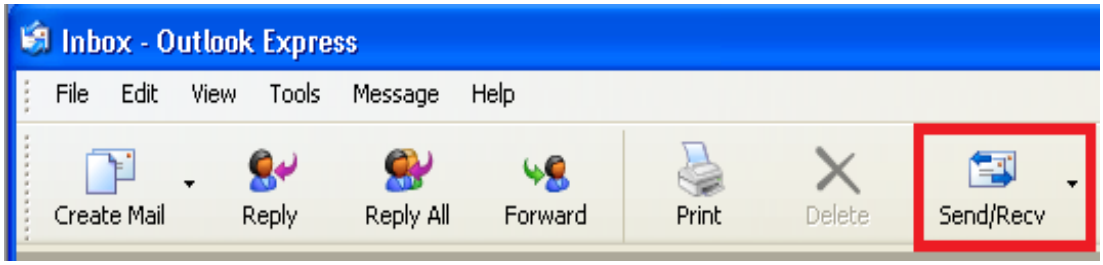

Figure 35: Send/Receive Button on Outlook Express

21. The email should appear in rmiller's inbox. Click on the hyperlink.

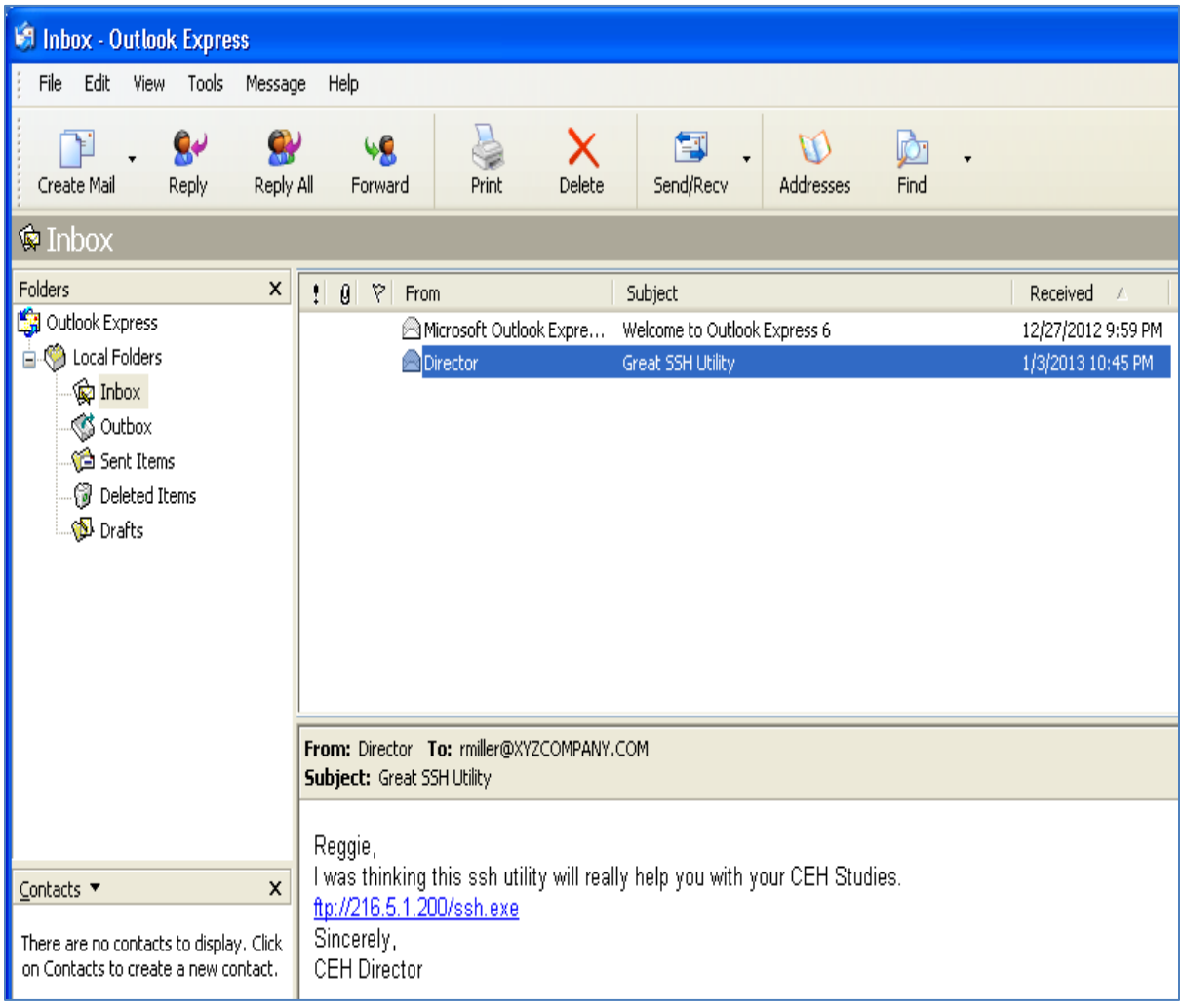

Figure 36: Spear Phish Email in the Inbox

22. Click on the link. Save the file to your Windows XP desktop.

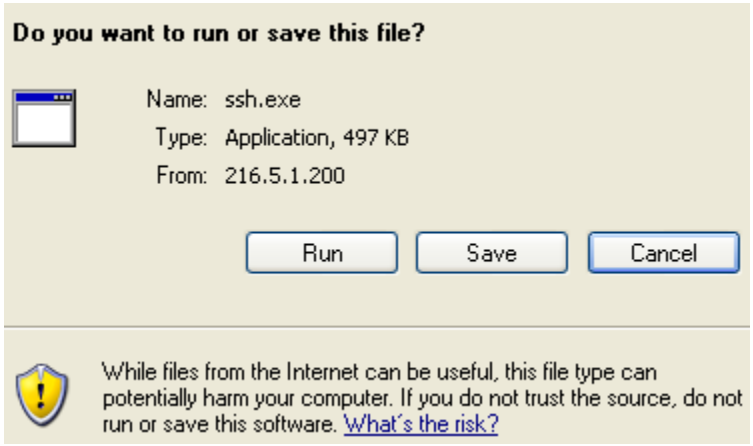

Figure 37: Save the ssh.exe file

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

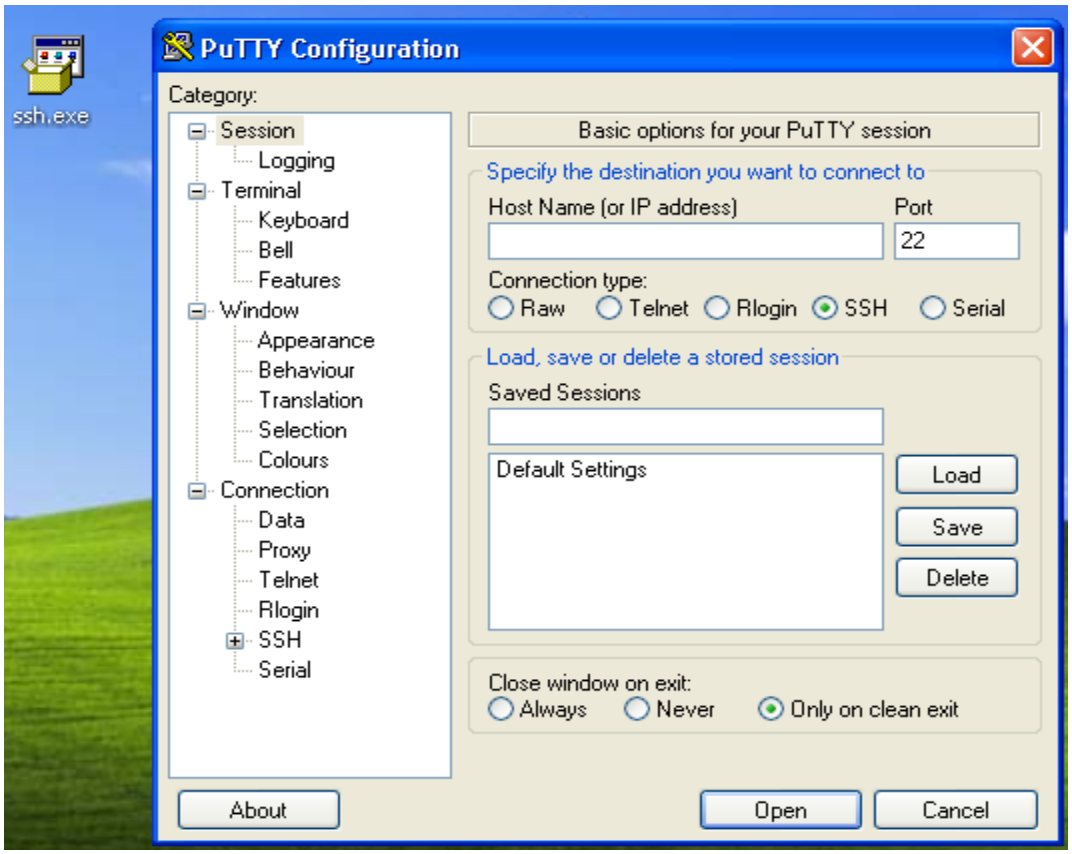

Figure 38: The Putty Program (With a Special Bonus)

On the **Windows 7** machine, you will notice a connection in the Poison Ivy window.

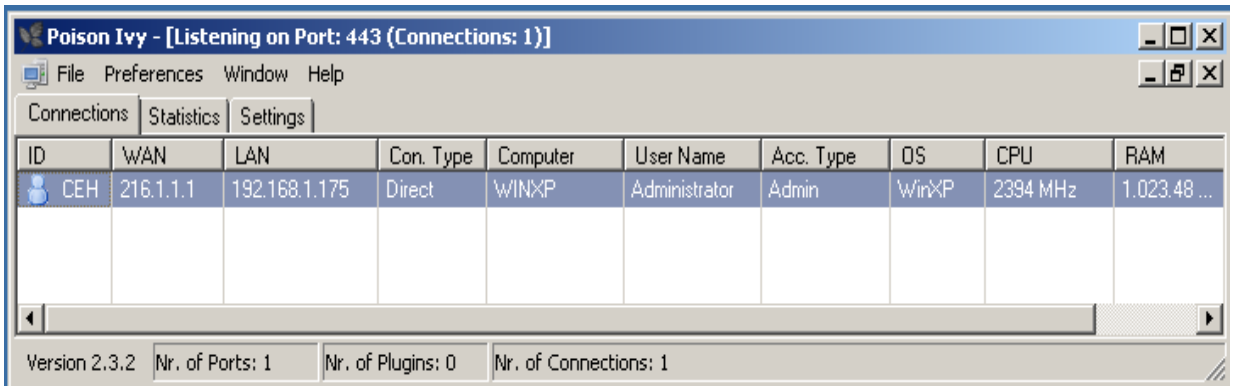

Figure 39: A connection from the Victim

Notice that Poison Ivy 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 under the Local Area Network (LAN) connection column.

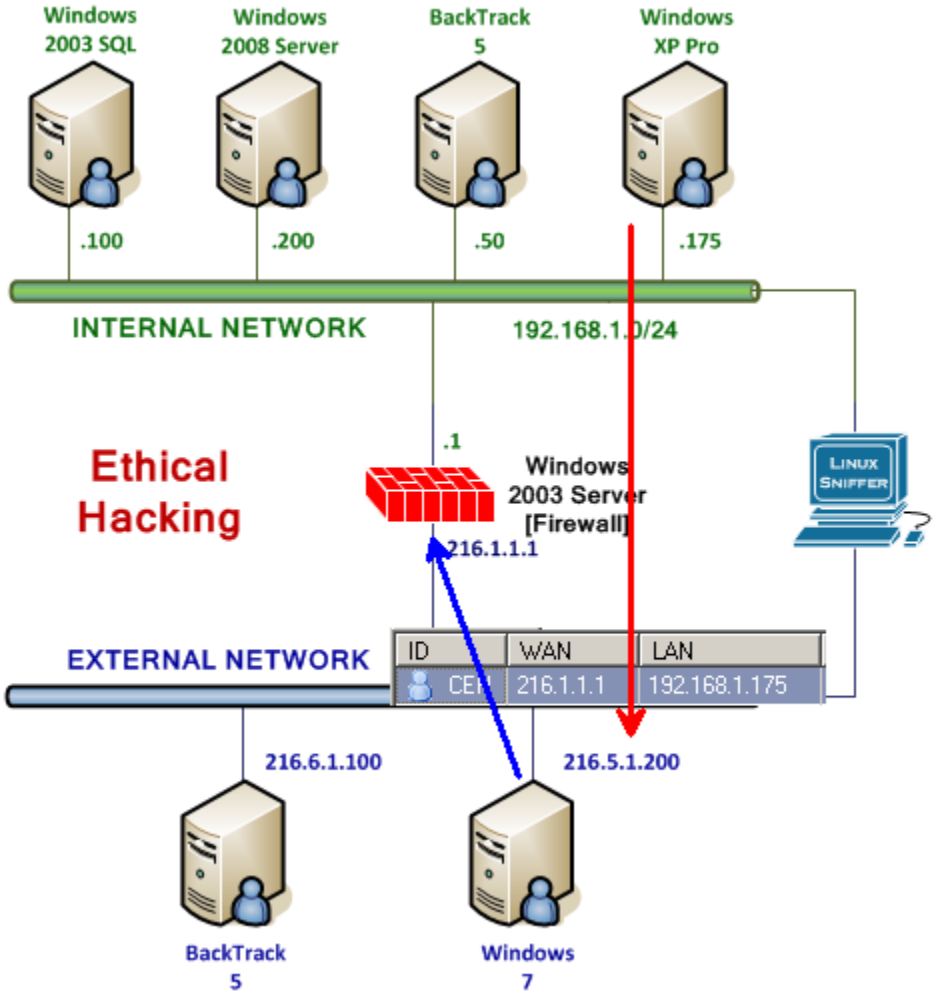

Figure 40: The WAN/LAN connections

2.2 Conclusion

A malicious Poison Ivy payload 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. Do not close the Poison Ivy window, as it will be used in the next section.

2.3 Discussion Questions

1. What is the function of a wrapper program?
2. How does Network Address Translation, or NAT, affect Poison Ivy?
3. What does the acronym POP stand for?
4. What is a good name for a piece of malware to help disguise its presence?

3 Exploiting the Victim Machine with Poison Ivy

In this section, you will be using Poison Ivy to exploit the victim. Since not all of the capabilities will be covered in this lesson, it is recommended that you consider performing additional experimentation with the software within the isolated environment.

Never use Poison Ivy or the Wrapper software outside of the isolated virtual environment.

3.1 Exploitation with Poison Ivy

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

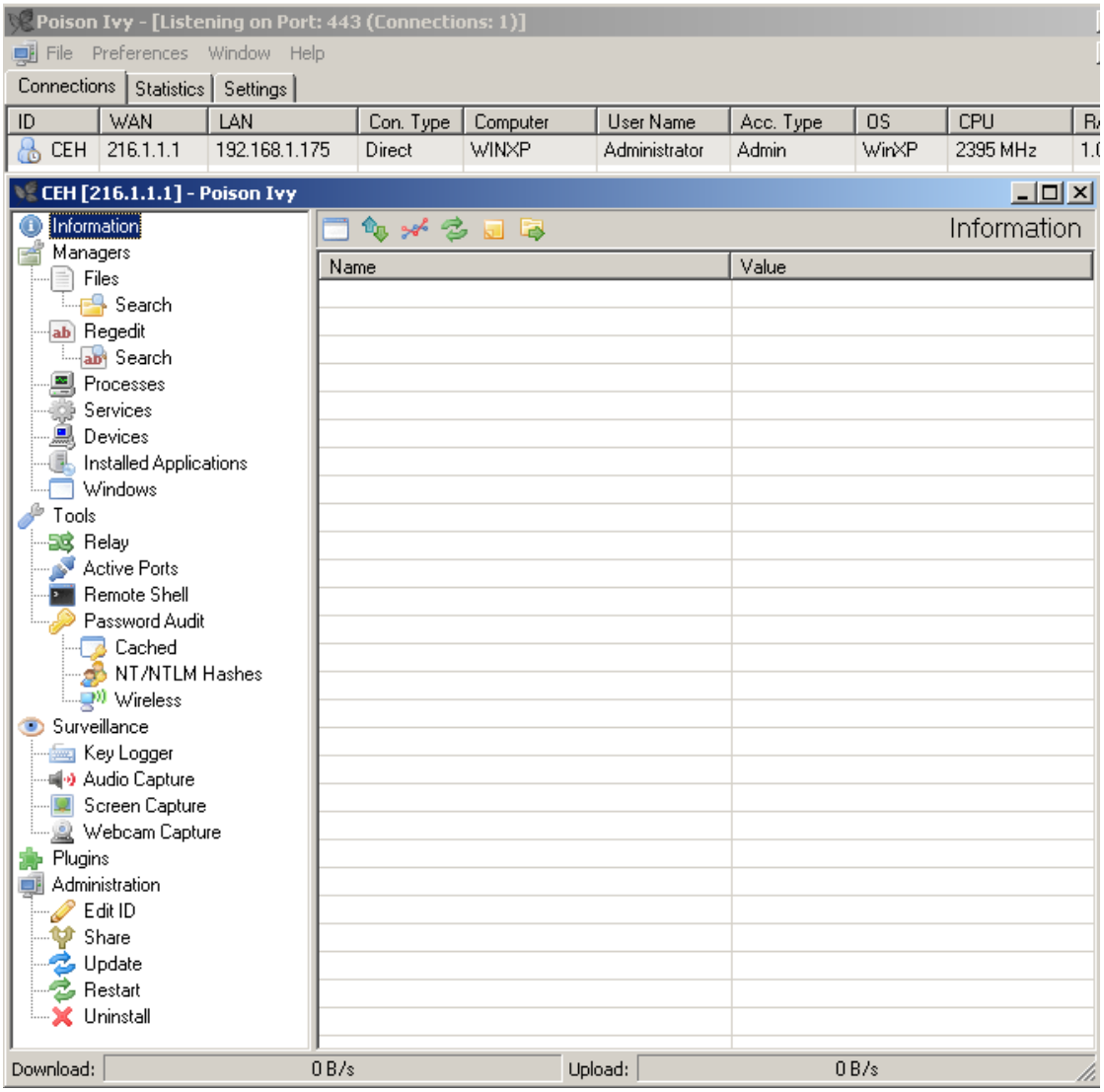

Figure 41: The connection to the Victim

2. Right-click on the Information Pane and select Refresh. The Information of the remote victim computer, such as operating system and patch level are displayed.

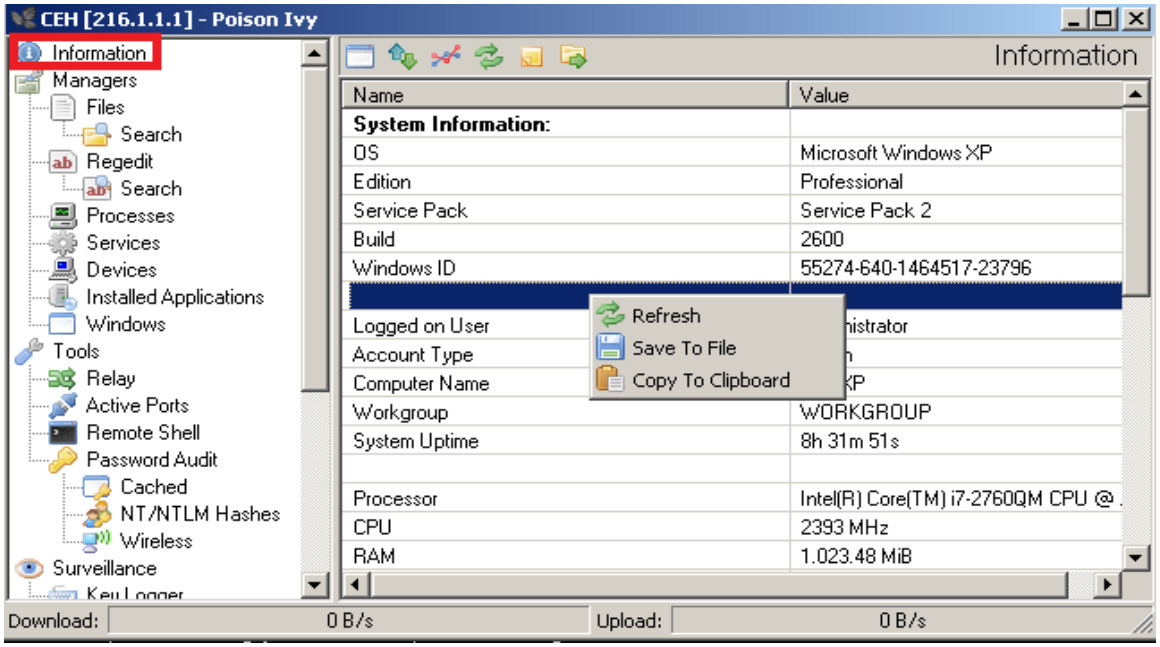

Figure 42: Information Screen of Poison Ivy

3. Click on Files and then click refresh folder in the right most pane. You can use this section to upload and download files over Poison Ivy's encrypted channel. You also can execute files (with switches) and securely delete files.

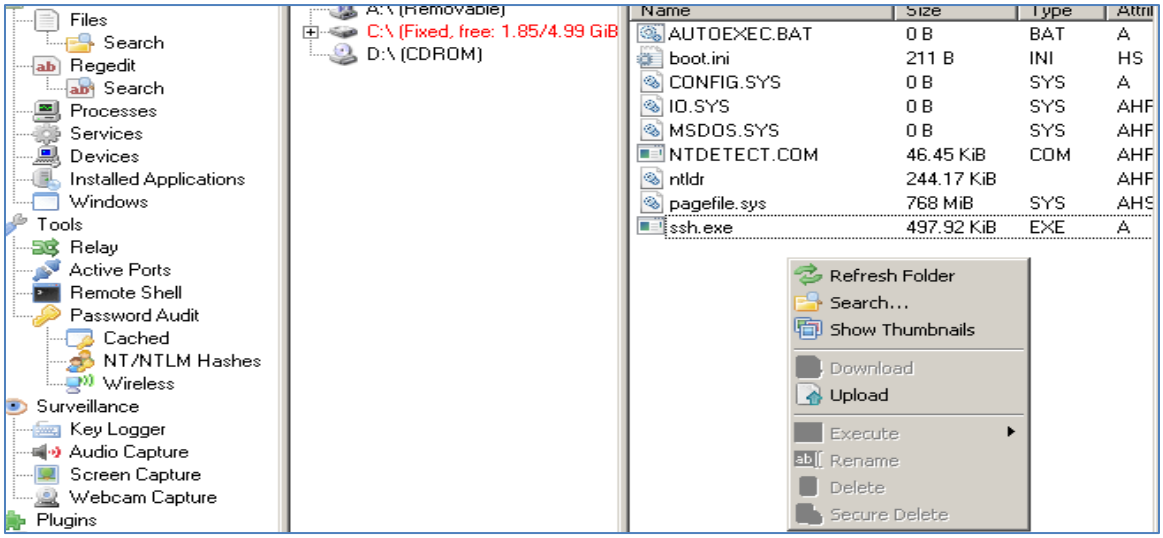

Figure 43: Managing Files on the Remote Machine

4. Click the Processes Selection on the left and click refresh in the right pane.

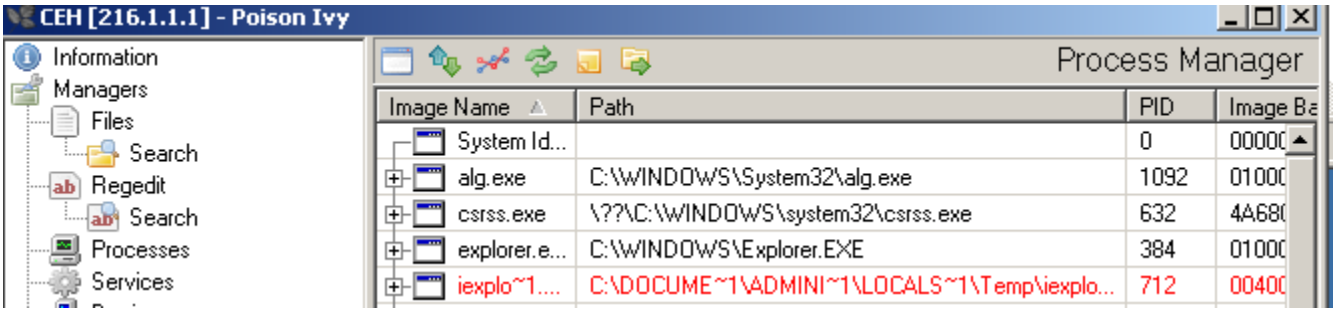

Figure 44: Processes on the Victim Machine

Processes can be killed. An attacker's strategy may include killing processes associated with anti-virus. The red process is the Poison Ivy payload running on the victim. As the attacker, that is one process you do not want to kill on the victim machine. Services can also be stopped, started, and uninstalled. Applications can also be uninstalled.

5. Click the Services Selection on the left and click refresh in the right pane. Find Automatic Updates in the list of services. Right-click and select Stop. This will prevent the machine from receiving windows updates and service packs.

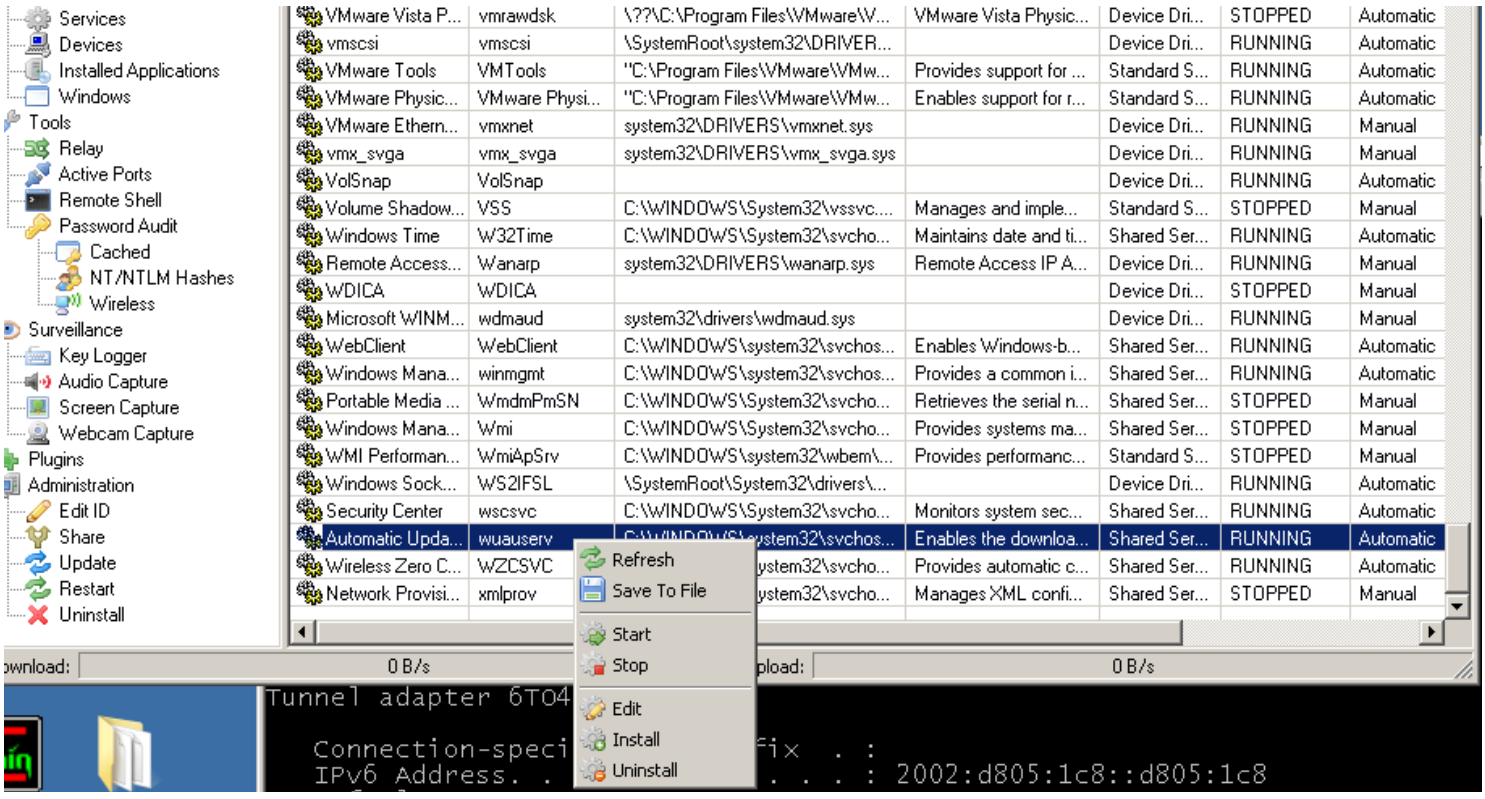

Figure 45: Stopping Automatic Updates

6. Right-click and refresh the Services pane. Automatic Updates should be stopped.

Automatic Upda...	wuauserv	C:\WINDOWS\system32\svchos...	Enables the downloa...	Shared Ser...	STOPPED	Automatic

Figure 46: Automatic Updates are Stopped

Poison Ivy also allows you to interact with a command prompt and dump hashes.

7. To dump the hashes on the remote machine. Select NT/NTLM Hashes in the left hand pane. Right click in the white space on the right pane and click refresh.

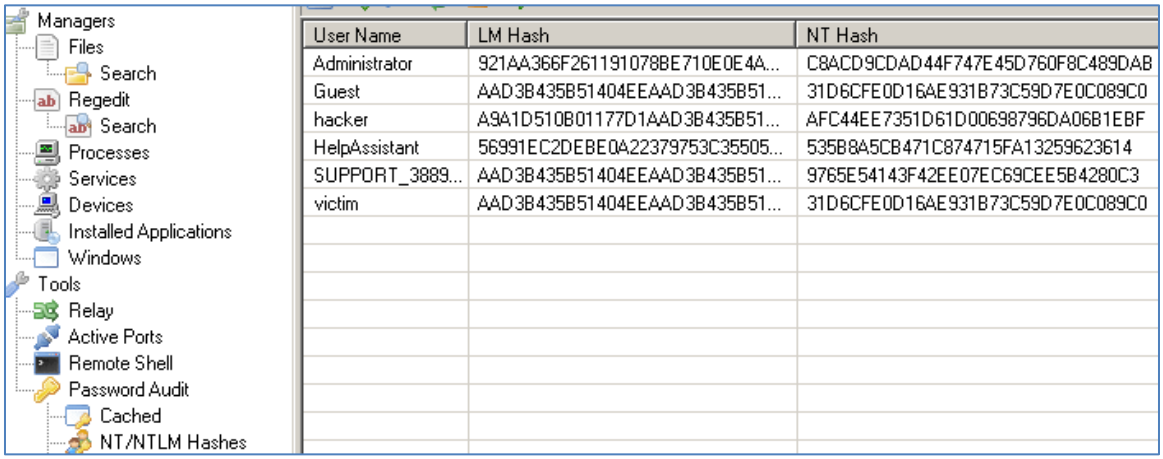

Figure 47: Dumping the Password Hashes

3.2 Conclusion

Poison Ivy provides a Graphical User Interface (GUI) through which users may perform malicious tasks against a victim machine over an encrypted connection. The attacker can perform tasks such as uploading and downloading files, dumping hashes, as well as killing processes and stopping services. Poison Ivy 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 red colored process in Poison Ivy's list of processes indicate?
2. How do you dump hashes within Poison Ivy?
3. In what section of Poison Ivy would you stop Automatic Updates?
4. Is it advisable to use Poison Ivy outside of an isolated lab environment?

References

1. Poison Ivy RAT:
   http://www.poisonivy-rat.com

2. Threat Description: Backdoor:W32/Poison Ivy:
   http://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml

3. How to detect and mitigate Poison Ivy RAT malware-style attacks:
   http://searchsecurity.techtarget.com/answer/How-to-detect-and-mitigate-Poison-Ivy-RAT-malware-style-attacks

4. Poison Ivy RAT Still Giving Users a Rash:
   http://threatpost.com/en_us/blogs/poison-ivy-rat-still-giving-users-rash-110311

5. Poison Ivy Used Against RSA:
   http://blogs.rsa.com/anatomy-of-an-attack/

