Malware Threats

Module 06

Malware

Malware (a contraction of "malicious software") is a type of program that contains malicious or harmful code embedded in apparently harmless programming or data in such a way that it can take control of a system and/or its operations and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Malware poses a major security threat to the information security. Malware writers explore new attack vectors to exploit vulnerabilities in information systems. This leads to ever more sophisticated malware attacks, including drive-by malware, "maladvertising" (or "malvertising"), Advanced Persistent Threats, and so on. Though organizations try hard to defend themselves using comprehensive security policies and advanced anti-malware controls, the current trend indicates that malware applications are targeting "lower-hanging fruit": undersecured smartphones, mobile applications, social media, and cloud services. The problem is further complicated because of threat predictions. As McAfee stated in its Threats Report published in February 2015, "Small nation states and foreign terror groups will take to cyberspace to conduct warfare against their enemies. They will attack by launching crippling distributed denial of service attacks or using malware that wipes the master boot record to destroy their enemies' networks."

Assessing an organization's information system against malware threats is a major challenge today because of the quickly-changing nature of malware threats. You need to be well versed in the latest developments in the field and understand the basic functioning of malware to select and implement controls appropriate to your organization and its needs.

The labs in this module will provide a first-hand experience with various techniques that attackers use to write and propagate malware. You will also learn how to effectively select security controls to protect your information assets from malware threats.

Lab Objectives

The objective of this lab includes:

- Creating and using different types of malware, such as Trojans, Viruses, and Worms, and exploiting a target machine as proof of concept
- Detecting malware

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Environment

To complete this lab, you will need:

- A computer running Windows Server 2012 as a host machine
- A computer running Window Server 2008 virtual machine
- Window 8.1 running as a virtual machine
- Windows 7 running as a virtual machine
- Kali Linux running as a virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 175 Minutes

Overview of Malware

With the help of a malicious application, an attacker gets access to stored passwords in a computer and would be able to read personal documents, delete files, display pictures, and/or display messages on the screen.

According to a recent report by Symantec, more than 317 million new pieces of malware—computer viruses or other malicious software—were created in the year 2014. That means nearly one million new threats were released each day. Malware has the ability to perform various malicious activities that might range from simple email advertising to complex identity theft and password stealing. Malware programmers create it to:

- Attack browsers and track websites visited
- Affect system performance, making it very slow
- Cause hardware failure, rendering the computer inoperable
- Steal personal information (including contacts, etc.)
- Erase important information, resulting in potential huge loss of data
- Attack other computers from a single compromised system
- Spam inboxes with advertising emails

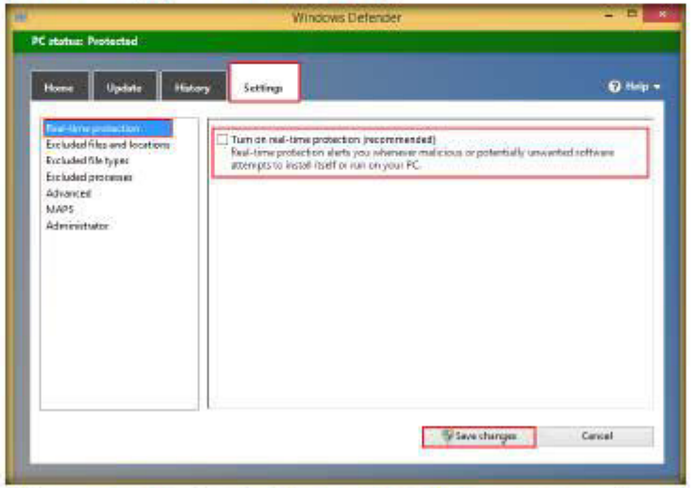
Lab Tasks

TASK 1

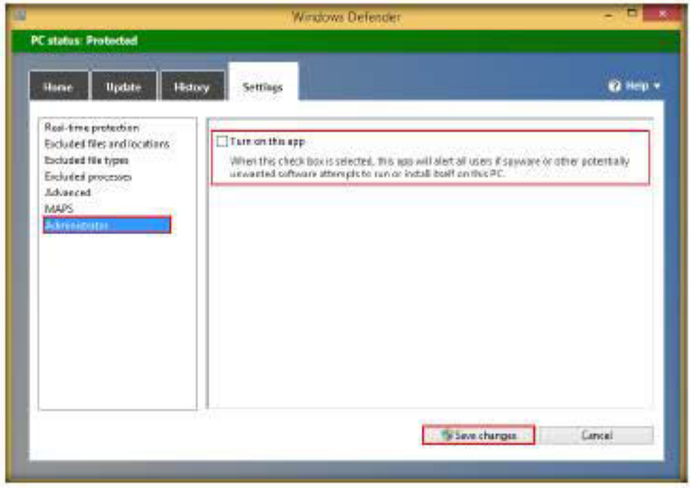
Overview

Note: **Turn off Windows Defender** in the machines you are using for the labs in this module, as it blocks and deletes malware as soon as it is executed.

To turn off **Windows Defender**, Go to **Control Panel** and select **Windows Defender**. In **Windows Defender** window, click on **Settings** tab, select **Real-time protection** from the left pane, uncheck **Turn on real-time protection (recommended)** option and click **Save changes**.



Select **Administrator** from the left pane, uncheck **Turn on this app** option, and click **Save changes**.



HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FIY

Recommended labs to assist you with malware threats:

- Creating a **HTTP Trojan** and Remote Controlling a Target Machine Using HTTP RAT
- Creating a Trojan Server Using the GUI Trojan **MoSucker**
- Gaining Control over a Victim machine Using **njRAT**
- Obfuscating a Trojan Using **SwayzCryptor** and making it Undetectable from Various **Anti-Virus Programs**
- Creating a Server Using the **ProRat** Tool
- Creating a Server Using the **Theef**
- Attaining Remote Access Using **Atelier Web Remote Commander**
- Building a Botnet Infrastructure Using **Umbra Loader**
- Creating a Virus Using the **JPS Virus Maker Tool**
- Creating a Worm Using **Ghost Eye Worm** and maintaining a Persistent Connection Using **njRAT**
- Creating a Worm Using the **Internet Worm Maker Thing**
- Virus analysis using **IDA Pro**
- Virus analysis using **Virus Total**
- Virus Analysis Using **OllyDbg**
- **Detecting Trojans**
- Monitoring TCP/IP Connections Using the **CurrPorts**

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FIY
HaCkRhInO-TeaM !

Lab 1

Creating an HTTP Trojan and Remotely Controlling a Target Machine Using HTTP RAT

A Trojan is a program that contains malicious or harmful code hidden inside apparently harmless programming or data, enabling it to take over system control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

HTTP/HTTPS Trojans can bypass any firewall, and work as kind of a straight HTTP tunnel, but one that works in reverse. They use web-based interfaces and port 80 to gain access. The execution of these Trojans takes place on the internal host and spawns a "child" at a predetermined time. The child program appears to be a user to the firewall so it allows the program access to the Internet. However, this child executes a local shell, connects to the web server that the attacker owns on the Internet through a legitimate-looking HTTP request, and sends it a ready signal. The legitimate-looking answer from the attacker's web server is in reality a series of commands that the child can execute on the machine's local shell.

Auditing a network against HTTP RATs is generally more difficult as well as essential, as most firewalls and other perimeter security devices cannot detect traffic generated by a HTTP RAT Trojan. As an ethical hacker and pen-tester, you must understand the working of HTTP Trojans to protect your networks against such malware.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Objectives

In this lab, you will learn how to:

- Run HTTP Trojan on Windows Server 2008 and create a Server
- Execute the Server from Windows 8.1 Machine
- Control Windows 8.1 machine Remotely from Windows Server 2008

Lab Environment

To carry out this, you will need:

- HTTP RAT located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Trojans Types\HTTP HTTPS Trojans\HTTP RAT TROJAN**
- Windows Server 2008 running in Virtual Machine (attacker machine)
- Windows 8.1 running in Virtual Machine (victim machine)
- You need a web browser to access Internet
- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

Overview of The Lab

Remote Access Trojans (RATs) are malicious programs that run invisibly on the host's PC and permit an intruder remote access and control. A RAT can provide a back door for administrative control over the target computer. Upon compromising target system, the attacker can use it to distribute RATs to other vulnerable computers and establish a botnet.

Lab Tasks

TASK 1

Create a Trojan

1. Log on to **Windows Server 2008** virtual machine.
2. Navigate to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\HTTP HTTPS Trojans\HTTP RAT TROJAN**, and double-click **httprat.exe**.
3. If **Open File - Security Warning** pop-up appears, click **Run**.
4. **HTTP RAT** main window appears as shown in the following screenshot:

FIGURE 1.1: HTTP RAT main window

5. Uncheck **send notification with ip address to mail** option, enter server port number as **84,** and click **Create** to create a **httpserver.exe** file.

FIGURE 1.2: Create backdoor

6. Once the httpserver.exe file is created, a pop-up will display. Click **OK**.

FIGURE 1.3: Backdoor server created successfully

The created httpserver will be placed in the tool directory.

7. The **httpserver.exe** file should be created in the folder **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\HTTP HTTPS Trojans\HTTP RAT TROJAN**.

8. Double click the file to run the Trojan.
9. If **Open File - Security Warning** pop-up appears, click **Run**.

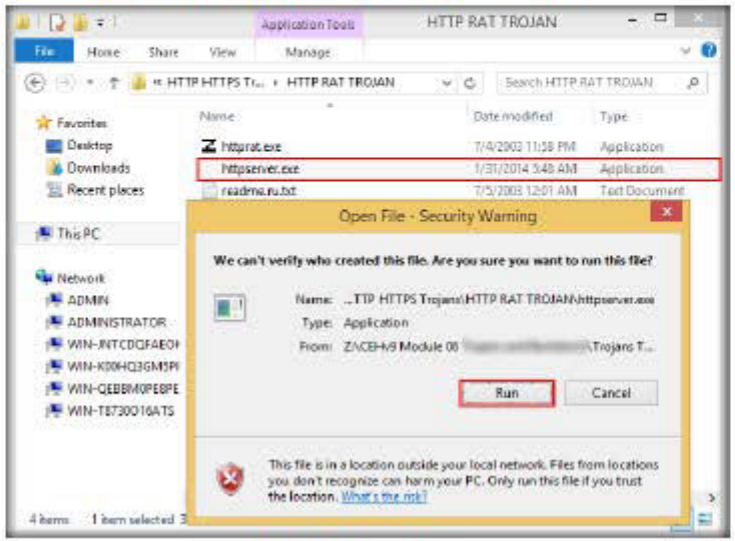


FIGURE 1.4: Running the Backdoor

10. Now, launch **Task Manager** to check whether the process is running on the machine.
11. To launch Task Manager, right-click the **Windows** icon, and click **Task manager**.

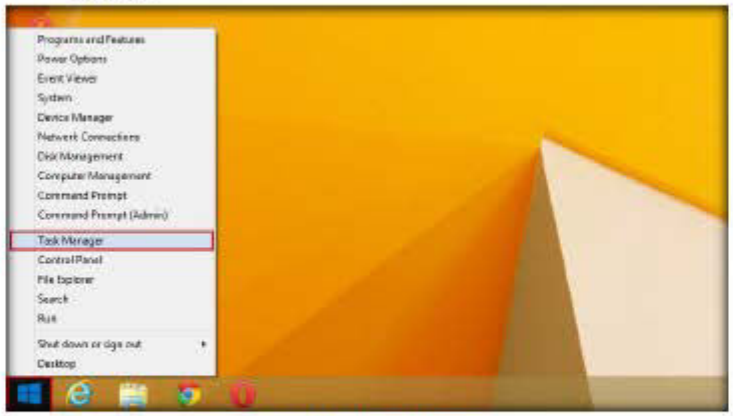


FIGURE 1.5: Launching Task Manager

12. You will be able to see the **Httpserver** process in the task manager window.

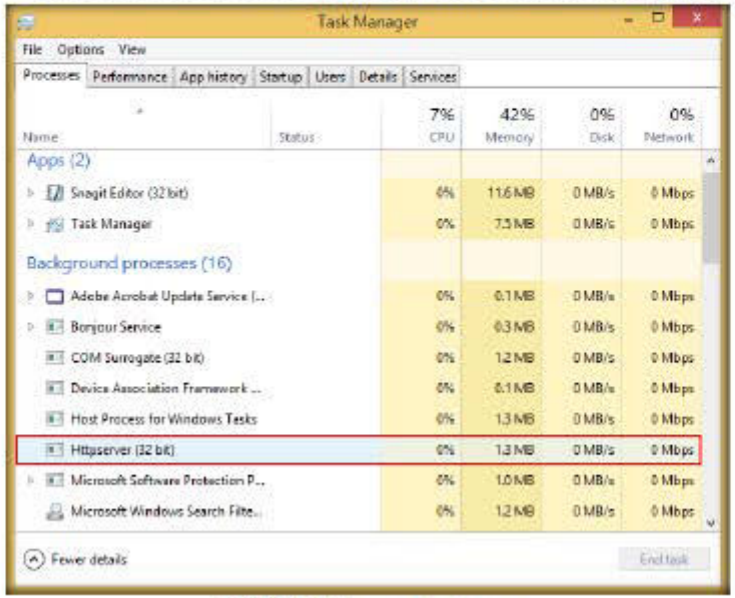


FIGURE 1.6: Backdoor running in task manager

TASK 2

Analyze the Victim machine's resources

13. Log in to **Windows Server 2008** virtual machine, and launch a **Web browser**.

14. Enter the IP address of Windows 8.1 (**10.0.0.10**) in the address bar to access the **Windows 8.1** virtual machine.

Note: Very often, the browser fails to connect to the Windows 8.1 virtual machine and displays an error on the webpage. If you receive the error, simply reload the webpage.

IP address may vary in your classroom lab environment.

FIGURE 1.7: Access the backdoor in Host web browser

15. Click on the **running processes** link to list down the processes running on the **Windows 8.1** machine.
16. You can kill any **running process** from here.
17. Click **browse,** and under **Browse**, click **Drive C**.

FIGURE 1.8: Access a drive in Host web browser

18. You can browse the contents in this drive (**C:**) by clicking on the respective links.

FIGURE 1.9: Accessing the Contents in C:\

19. Click **computer info** link to view the information of the **computer, users,** and **hardware**.

FIGURE 1.10: Obtaining the Computer information

20. In real time, attackers run this tool in the target machine, create a server in that machine, and execute it. By doing so, they obtain data contained in that machine as well as the information related to its hardware and software.
21. On completion of the lab, end the **Httpserver** process in **Windows 8.1**.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Creating a Trojan Server Using the GUI Trojan MoSucker

MoSucker is a visual basic Trojan. MoSucker's edit server program. It has a client with the same layout as subSeven's client.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

MoSucker is a powerful backdoor–hacker's remote access tool. The backdoor renames NETSTAT.EXE to NETSTAT.OLD when it is first activated and renames the file back when it is uninstalled. The backdoor also can install itself in a system with modification of startup keys in the Registry or INI files.

You are a Security Administrator of your company, and your job responsibilities include protecting the network from malware, Trojan attacks, theft of valuable network data, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

- Creating a server and testing the network for attack
- Access the victim machine remotely

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Environment

To complete this lab, you will need:

- The MoSucker tool, located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\MoSucker**
- A computer running Windows Server 2012 as Host Machine
- A computer running Window 8.1 Virtual Machine (Attacker)
- Windows Server 2008 running in Virtual Machine (Victim)
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

Overview of Malware

When activated on an infected system, malware allows more than one hacker to connect to a system and to perform the following actions:

1. Control the server—configure, restart, remove, close;
2. Open/close CD-ROM tray;
3. List and kill processes;
4. Shutdown/restart a system;
5. Log activities and control mouse and keyboard;
6. Upload, download, run, rename of move files;
7. List, create, remove directories;
8. Control Windows interface: popup start menu, minimize all windows, show/hide system tray, hide/show Start button, change wallpaper, change resolution, change system colors, flip screen, get opened windows list;
9. Copy/read text from clipboard;
10. Open/close chat session;
11. Administrator of a backdoor server can control other users' server rights;
12. Play sound files;
13. Create log file of backdoor activities;
14. Send text to a printer;
15. Obtain the OS system type and version;
16. Modify the Windows Registry;
17. Update server from Internet;
18. Change date and time;
19. Show picture;
20. Steal users' ICQ information;
21. Obtain information about users' local and network drives;
22. Show message boxes;
23. Notify a hacker when infected user is on line; and
24. Obtain general information about infected systems.

Lab Tasks

TASK 1

Create Server with MoSucker

1. Launch Windows 8.1 Virtual Machine, and navigate to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\MoSucker**.
2. Double click **CreateServer.exe** file to create a server.
3. If an **Open File - Security Warning** pop-up appears, click **Run**.

4. If the **VB6 Runtimes** pop-up appears, click **OK**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

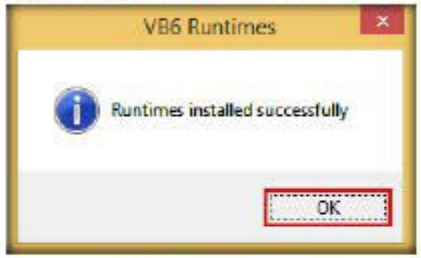


FIGURE 2.1: VB6 Runtimes pop-up

5. The MoSucker **Server Creator/Editor** window appears; leave the default settings, and click **OK**.

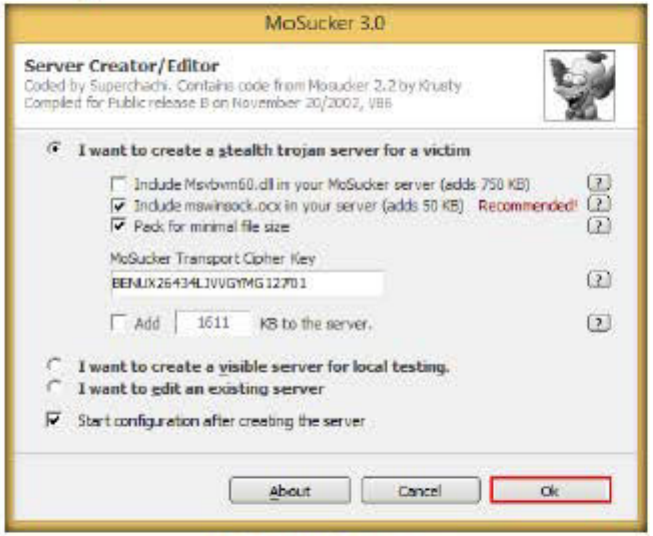


FIGURE 2.2: Install createServer.exe

6. Choose a location (**Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\MoSucker**) to save the file, specify a file name (server.exe), and click **Save**.

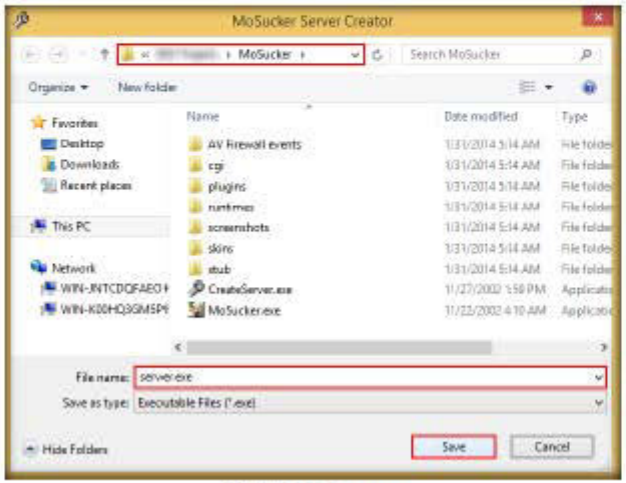


FIGURE 2.3: Save Server.exe

7. MoSucker will generate a server with all the complete settings in the specified directory.

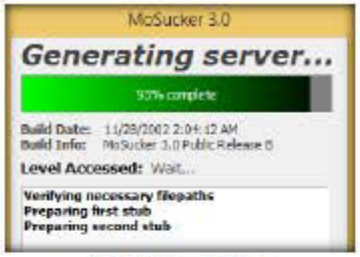


FIGURE 2.4 Generating Server

8. Once the server is created, an **Edit Server** pop-up appears; click **OK**.

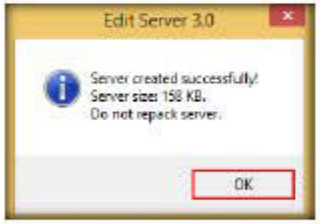


FIGURE 2.5: Server created successfully

9. In MoSucker wizard, change **Victim's Name,** or leave all the settings to default. Make a note of the **Connection-port** number (**4288**).

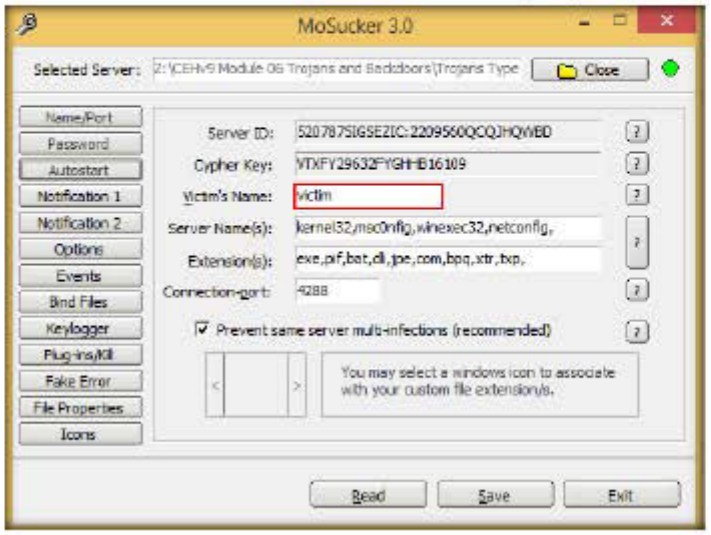


FIGURE 2.6: MoSucker wizard

10. Now, select **Keylogger** button in the left pane, check **Enable off-line keylogger,** and leave the other settings at their defaults. Click **Save**.

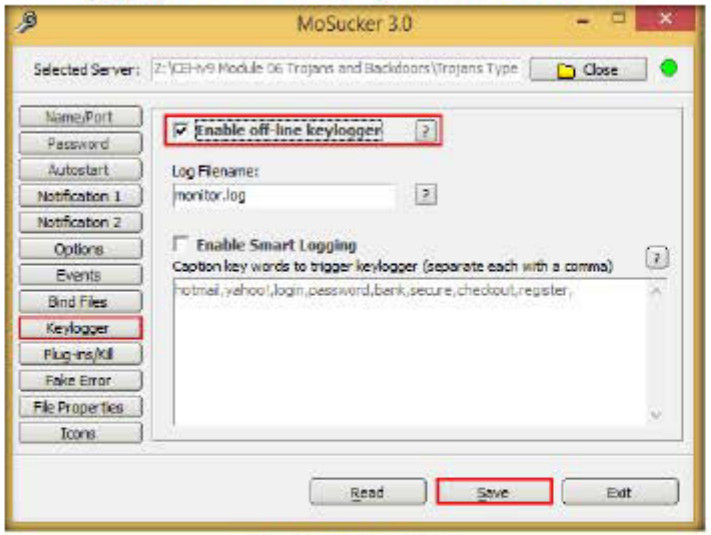


FIGURE 2.7: Enabling the Keylogger

11. Once the Trojan server is saved successfully, a **MoSucker EditServer** pop-up appears; click **OK**.

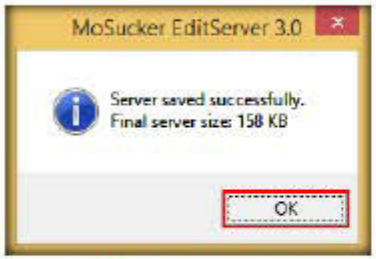


FIGURE 2.8: Server saved successfully

12. Exit the MoSucker Configuration wizard by clicking **Exit**.
13. Switch to **Windows Server 2008** virtual machine, and navigate to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\MoSucker**. Double-click **server.exe** to execute the trojan.
14. If the **Open File - Security Warning** pop-up appears, click **Run**.
15. If an administrator error pop-up appears, click **OK** to close it.

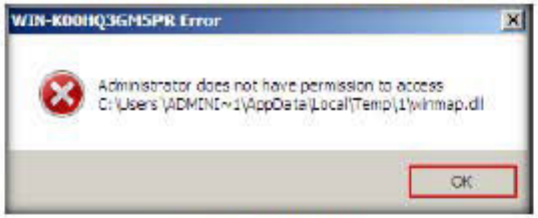


FIGURE 2.9: Administrator error

16. Switch back to **Windows 8.1** virtual machine and navigate to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\MoSucker**.
17. Double-click **MoSucker.exe** to launch MoSucker.
18. The **Open File - Security Warning** pop-up appears; click **Run**.
19. If the **VB6 Runtimes** pop-up appears, click **OK** to close it.

FIGURE 2.10: VB6 Runtimes pop-up

20. The **WARNING** dialog-box, regarding the license agreement, appears; click **Yes** to close it.

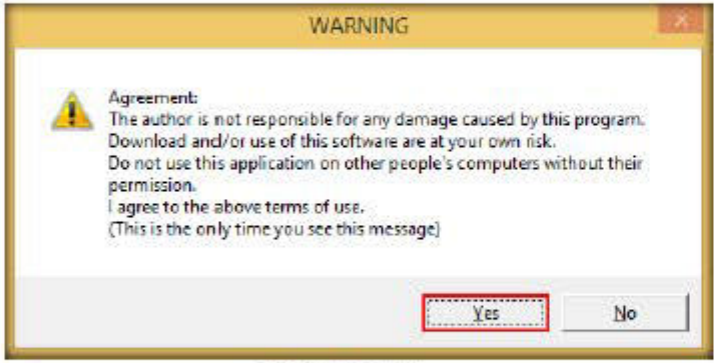


FIGURE 2.11: WARNING pop-up

21. The MoSucker main window appears, as shown in the following screenshot:

FIGURE 2.12: MoSucker main window

22. Enter the IP address of the **Windows Server 2008** (**10.0.0.11**) and port number (which you noted down in **Step no. 9**, here **4288**). Click **Connect**.
23. You can even specify other port numbers during server configuration.

Note: The IP address and port number might differ in your lab environment.

FIGURE 2.13: Connecting to victim machine

24. Now the **Connect** button automatically changes to **Disconnect** after establishing a connection to the victim machine, as shown in the screenshot:

FIGURE 2.14: Connection established

25. Now, click on **Misc stuff** in the left pane. MoSucker displays different options an attacker can use to perform different actions remotely.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

FIGURE 2.15: setting server options

26. Click **Server options** to view different options related to the server.

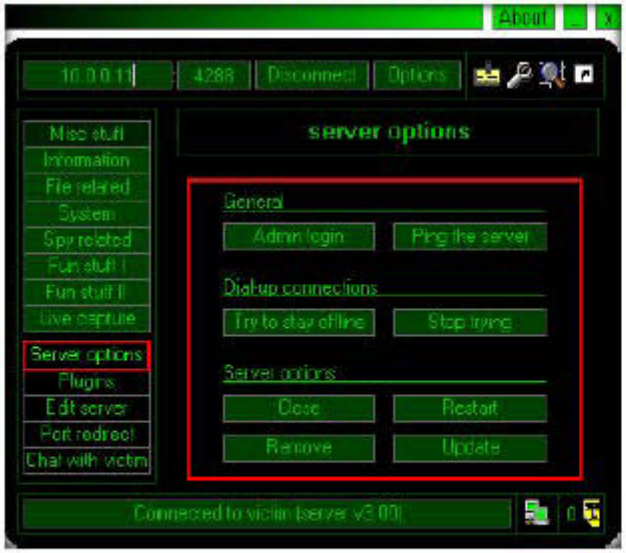


FIGURE 2.16: Setting Server Options

27. In the same way, you can explore other options that help you perform several other actions on the victim machine.
28. You can also access the victim machine remotely by clicking **Live capture** in the left pane.
29. In Live capture, click on **Start**.

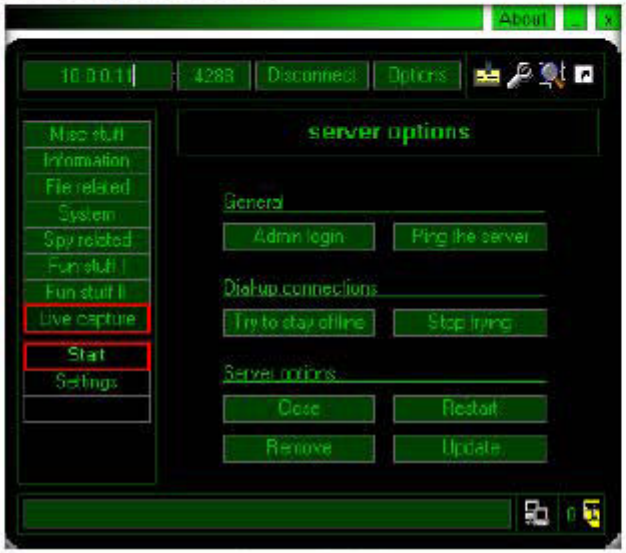


FIGURE 2.17: Start Capturing

30. A **DLL missing** prompt appears; click **Yes** to upload the DLL plugin.

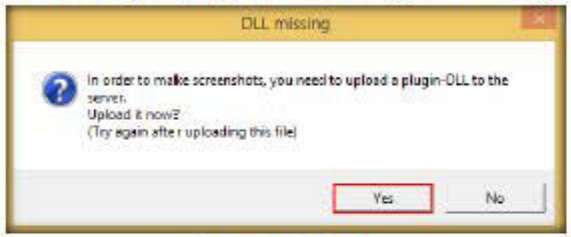


FIGURE 2.18: DLL missing pop-up

31. Click Start again in the MoSucker window if the capture doesn't being.
32. You will be able to access the victim machine remotely.

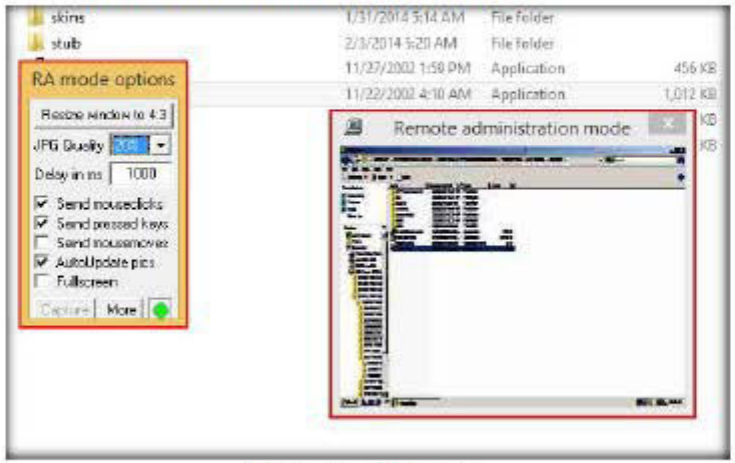


FIGURE 2.19: Accessing victim machine

33. In the **RA mode options**, set **JPG Quality** to **90%**, and select **Fullscreen**.

FIGURE 2.20: RA mode options

34. The remote administration mode appears in full screen, as shown in the screenshot:

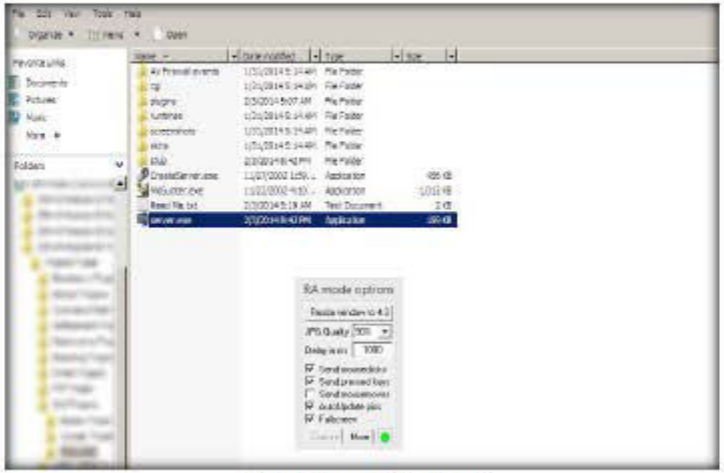


FIGURE 2.21: Remote administration mode

35. You can access files, modify them, and so on, in this mode.

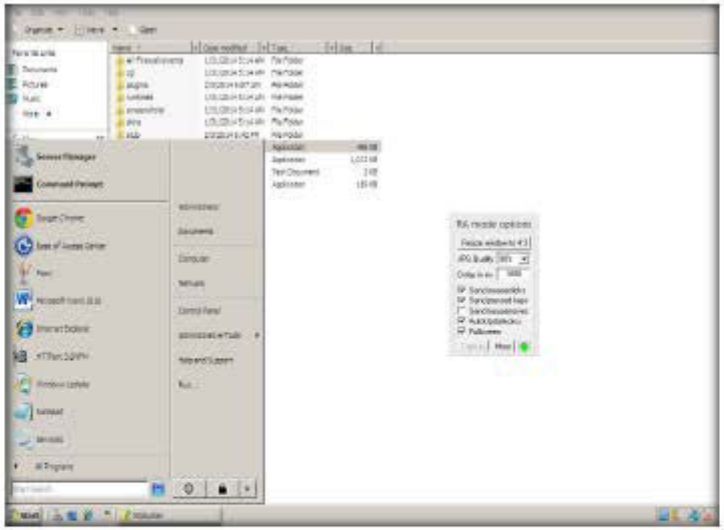


FIGURE 2.22: Accessing victim machine

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

36. Similarly, you can use other functionalities in MoSucker, such as keyloggers, the registry editor, and window manager.
37. In real-time, attackers send a crafted server/backdoor file to the victim, which upon execution on victim machines, allow attackers to view/access all information related to those machines.
38. On completion of the lab, end the **server.exe** process on the **Windows Server 2008** machine.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 3

Gaining Control over a Victim Machine Using njRAT

njRAT is a Remote Access Trojan (RAT) intensive in its data-stealing capabilities. In addition to logging keystrokes, this malware is capable of accessing target computers' cameras, stealing credentials stored in browsers, uploading/downloading files, manipulating processes and files, and viewing their desktops.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The njRAT, developed in .NET, allows attackers to take complete control of an infected device. The malware is capable of logging keystrokes, downloading and executing files, providing remote desktop access, stealing application credentials, and accessing the infected computer's webcam and microphone.

PhishMe reports that njRAT has been distributed over the past period with the aid of spam emails advertising a car changer hack for the "Need for Speed: World" video game. Zscaler also noted that video game cracks and application key generators are often used as lures.

Being a security administrator or an ethical hacker, your job responsibilities include finding machines vulnerable to Trojan attacks, protecting the network from malware, Trojan attacks, stealing valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn how to:

- Create a Server using njRAT
- Access the victim machine remotely

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Environment

To complete this lab, you will need:

- njRAT tool located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**
- A computer running Windows Server 2012 as Host Machine

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FIY
HaCkRhInO-TeaM !

- A computer running Window 8.1 Virtual Machine (Attacker)
- A computer running Window 7 Virtual Machine (Victim)
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of Malware

The njRAT Trojan remains one of the most successful RATs in the wild because of the widespread online support and tutorials available to cyber-criminals. There are a variety of .NET obfuscation tools that make detection difficult for antivirus solutions and hinders analysis by security researchers. njRAT utilizes dynamic DNS for command and control (C2) servers and communicates using a custom TCP protocol over a configurable port.

- The C&C callback from the infected system includes following information:
- Bot identifier (based off configurable string in builder and volume serial number)
- Computer name (base-64 encoded)
- Operating system information
- Existence of attached webcam ("Yes"/"No")
- Bot version
- Country code
- Title of the active process window

Note: The versions of the created Client or Host and appearance of the website may differ from what it is in the lab. But the actual process of creating the server and the client is the same one shown in this lab.

Lab Tasks

Before running the lab, Turn on Windows Firewall in the victim machine (i.e. Windows 7). Firewall is configured in this machine to show that this lab can be performed even if a victim machine has the Firewall configured in it.

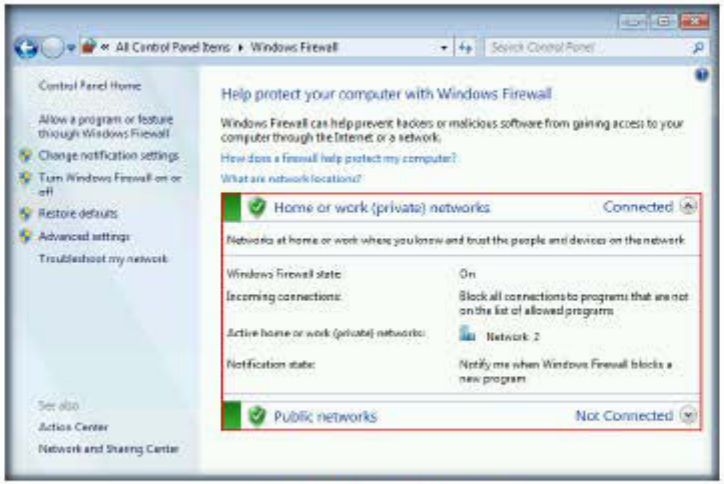


FIGURE 3.1: Turning on Windows Firewall

TASK 1

Create an Executable Server with njRAT

1. Log in to the **Windows 8.1** virtual machine, and navigate to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.
2. Double click on **njRAT v0.7d.exe** to launch the RAT.
3. If **Open File - Security Warning** pop-up appears, click **Run**.
4. njRAT GUI appears along with a **njRAT** pop-up, where you need to specify the port you want to use to interact with the victim machine. Enter the port number, and click **Start**.
5. In this lab, default port number **5552** has been chosen.

FIGURE 3.2: njRAT GUI along with a njRAT pop-up

6. The njRAT GUI appears; click the **Builder** link located at the lower-left corner of the GUI.

FIGURE 3.3: njRAT GUI

7. The **Builder** dialog-box appears; enter the IP address of **Windows 8.1** (attacker machine) virtual machine, check the options **Copy To StartUp** and **Registry StartUp,** and click **Build**.

Note: In this lab, the IP address of **Windows 8.1** virtual machine **10.0.0.4**. This IP address might vary in your lab environment.

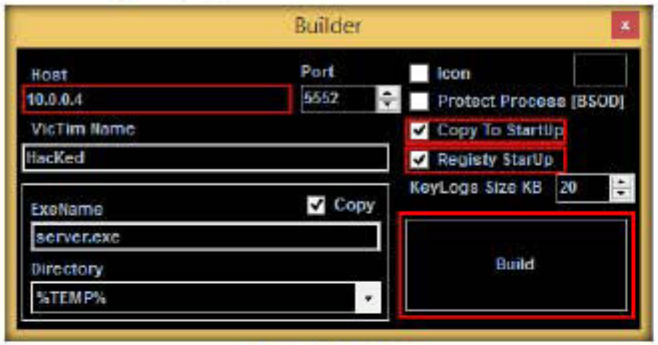


FIGURE 3.4: Builder dialog-box

8. The **Save As** dialog-box appears; specify a location to store the server, rename it, and click **Save**.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

9. In this lab, the destination location chosen is **Desktop,** and the file is named **Test.exe**.

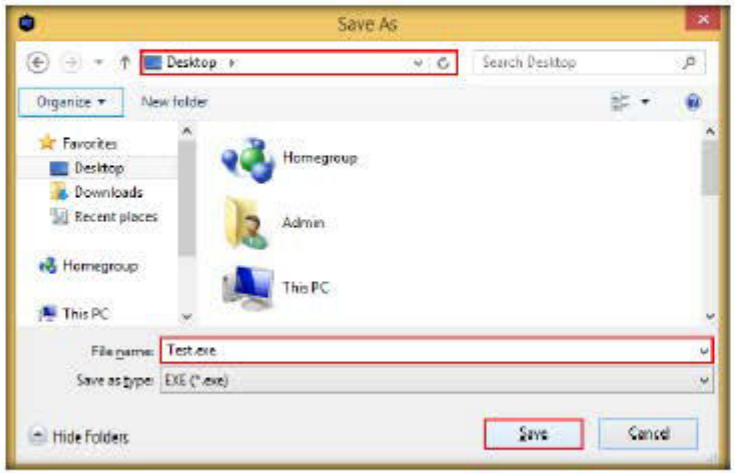


FIGURE 3.5: Save As dialog box

10. Once the server is created, the **DONE!** pop-up appears; click **OK**.

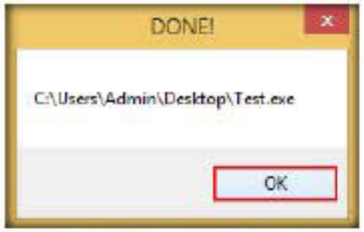


FIGURE 3.6: Server created successfully

11. Now, use any technique to send this server to the intended target through mail or any other source (in real time, attackers send this server to the victim).

TASK 2

Execute the Server on Windows 7

12. Log in to **Windows 7** virtual machine as a legitimate user. Download the file from the source through which the attacker (in this case, **you**) has sent the server executable and save it in a location.
13. In this lab, the server has been saved to **Desktop** on the **Windows 7** virtual machine.
14. Here, you are acting as an **attacker** who logged into the **Windows 8.1** machine to create a malicious server; and also as a **victim** who logged into **Windows 7** virtual machine and downloaded the server.

15. Double-click the server to run this malicious executable.

FIGURE 3.7: Executing the server

16. Switch back to **Windows 8.1**. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in Windows 8.1 establishes a persistent connection with the victim machine as shown in the screenshot:

FIGURE 3.8: Connection established successfully

17. Unless the attacker working on the Windows 8.1 machine disconnects the server on his own, the victim machine remains under his/her control.
18. The GUI displays the machine's basic details such as the IP address, User name, Type of Operating system and so on.

TASK 3

Manipulate Files on Victim Machine

19. Right-click on the detected victim name and click **Manager**.

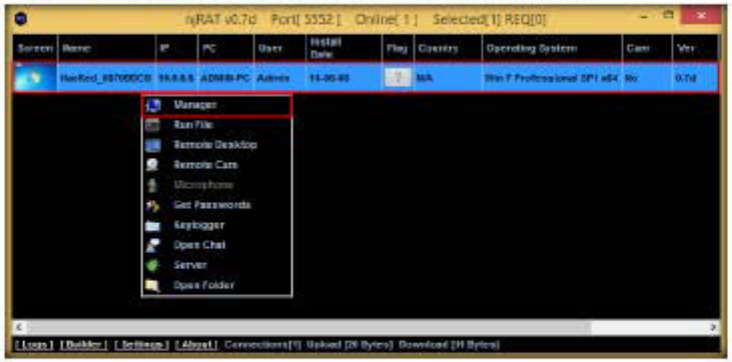


FIGURE 3.9: Managing the victim machine

20. Manager window appears, where **File Manager** is selected by default.

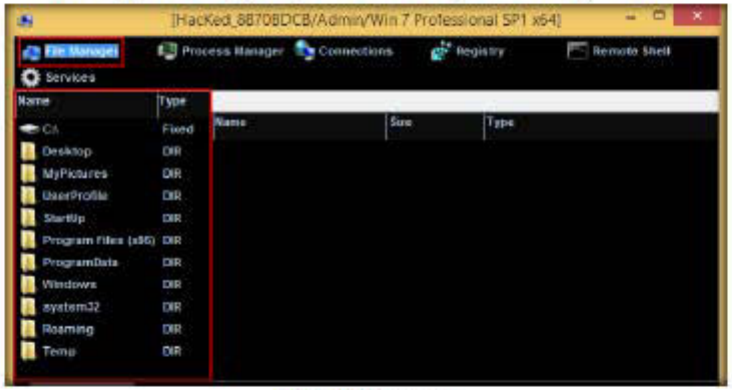


FIGURE 3.10: Manager window

21. Double-click any directory in the left pane (**ProgramData**); all its associated files/directories are displayed in the right pane. You can right-click a selected directory and manipulate it using the contextual options.

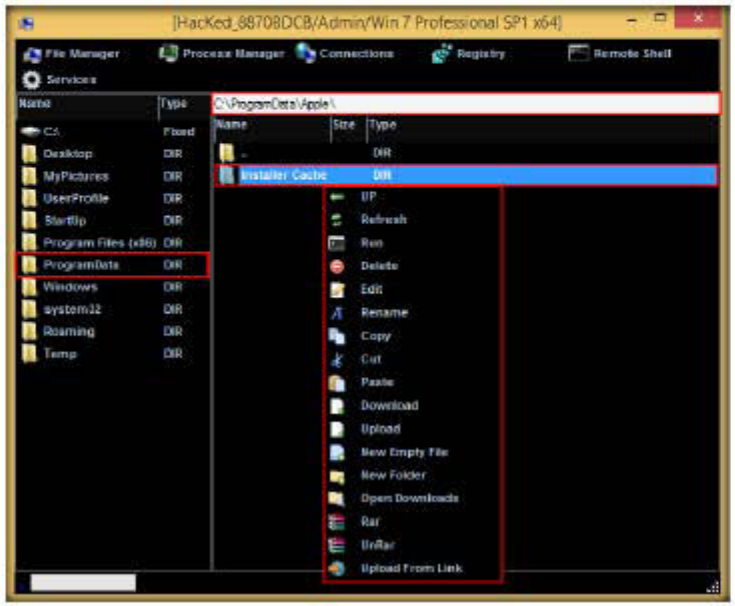


FIGURE 3.11: Accessing directories

TASK 4

Manage the Processes

22. Hover the mouse on **Process Manager**. You will be redirected to the Process Manager, where you can right-click on a selected process and perform actions such as **Kill**, **Delete**, and **Restart**.

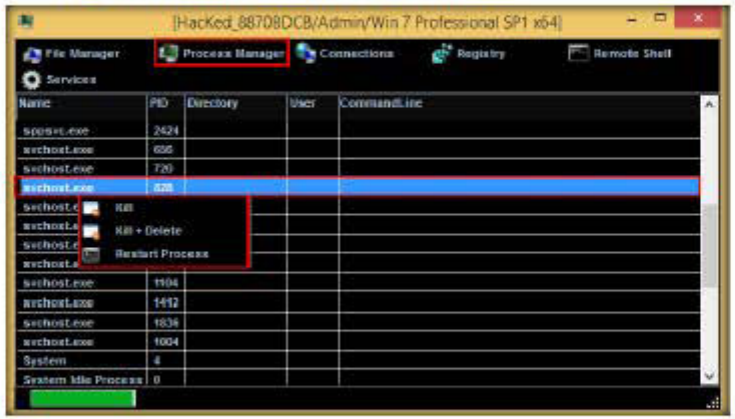


FIGURE 3.12: Process Manager Section

TASK 5

Manage the Connections

23. Click **Connections**, select a specific connection, right-click on it, and click **Kill Connection**. This kills the connection between two machines communicating through a particular port.

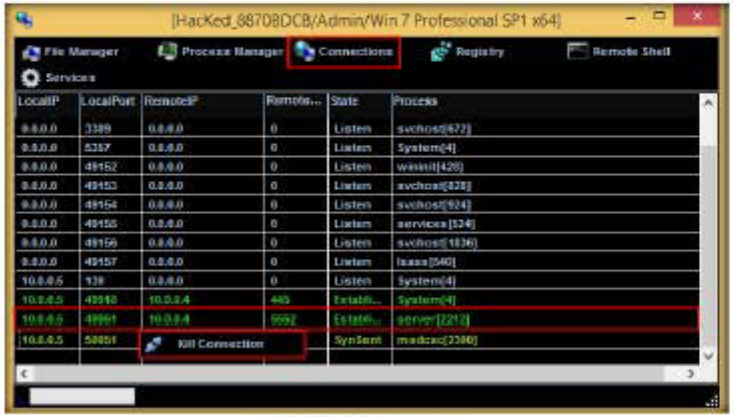


FIGURE 3.13: Managing connections

TASK 6

Manage the Registries

24. Click **Registry**, choose a registry directory from the left pane, and right-click on its associated registry files.
25. A few options appear for the files using which you can manipulate them.

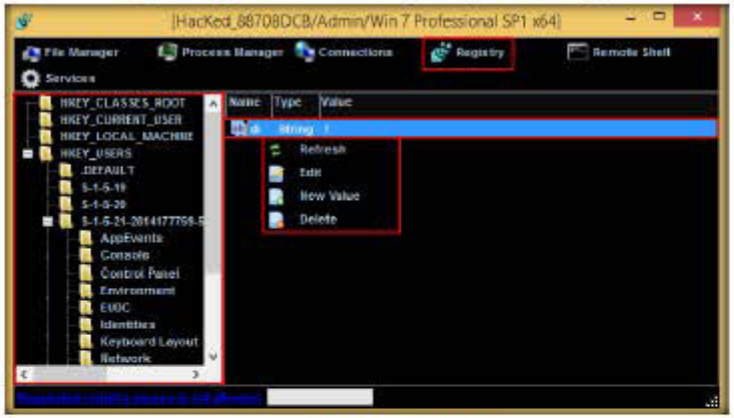


FIGURE 3.14: Managing Registries

TASK 7

Launch a Remote Shell

26. Click **Remote Shell**. This launches a remote command prompt of the victim machine (**Windows 7**).
27. Type the command **ipconfig /all** and press **Enter**.

FIGURE 3.15: Launch a Remote Shell

28. This displays all the interfaces related to the victim machine, as shown in the screenshot:

FIGURE 3.16: Launch a Remote Shell

29. Similarly, you can issue all the other commands that can be executed in the command prompt of the victim machine.

30. In the same way, click **Services**. You will be able to view all the services running in the victim machine. In this section, you can use options to **start**, **pause**, or **stop** a service.
31. Close the **Manager** window.
32. Now right-click on the victim name, click **Run File** and choose an option from the drop-down list.

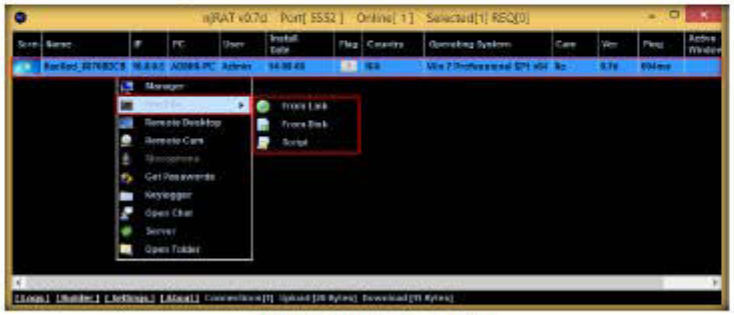


FIGURE 3.17: Launch a Remote Shell

33. An attacker makes use of these options to execute scripts or files remotely from his/ her machine.

TASK 8

Launch a Remote Desktop Connection

34. Right-click on the victim name, and select **Remote Desktop**.

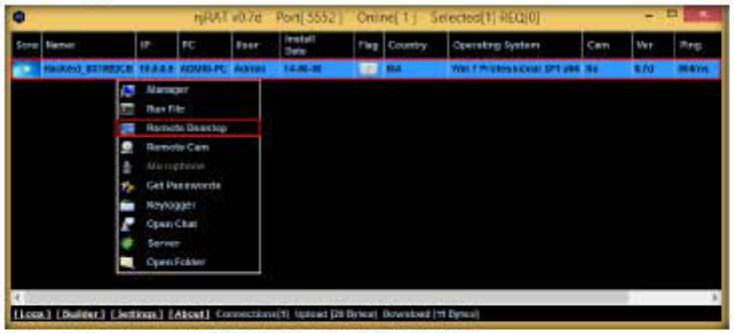


FIGURE 3.18: Launching a Remote Desktop Connection

35. This launches a remote desktop connection without the victim being aware of it.

36. **Remote Desktop** window appears, hover the mouse cursor to the top-center part of the window. A down arrow appears, click it.

FIGURE 3.19: Remote Desktop window

37. A remote desktop control panel appears; check the **Mouse** option.

FIGURE 3.20: Remote Desktop Control Panel

38. Now, you will be able to remotely interact with the victim machine using the mouse.

Note: If you want to create any files or write any scripts in the victim machine, you need to check the **Keyboard** option.

39. On completing the task, close the **Remote Desktop** window.

40. In the same way, right-click on the victim name, and select **Remote Cam** and **Microphone** to spy on the victim and track voice conversations.

FIGURE 3.21: Accessing Remote Cam and Microphone

TASK 9

Perform Key Logging

41. Switch to **Windows 7** virtual machine. Assume that you are the legitimate user and perform a few activities such as logging into any websites or typing text in some text documents.

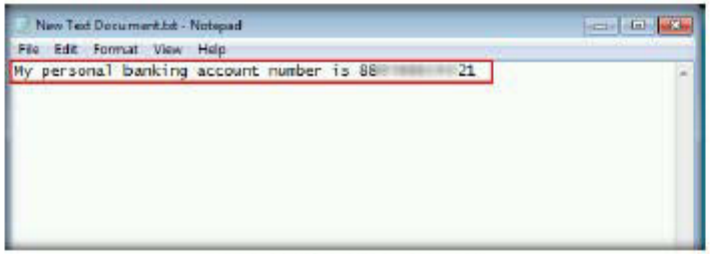


FIGURE 3.22: Entering Sensible Information

42. Switch back to Windows 8.1 virtual machine, right-click on the victim name, and click **Keylogger**.

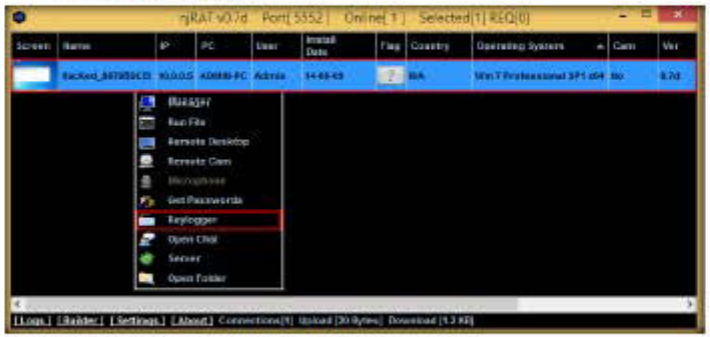


FIGURE 3.23: Launching Keylogger

43. The Keylogger window appears; wait for the window to load.
44. The window displays all the keystrokes performed by the victim on the **Windows 7** virtual machine, as shown in the screenshot:

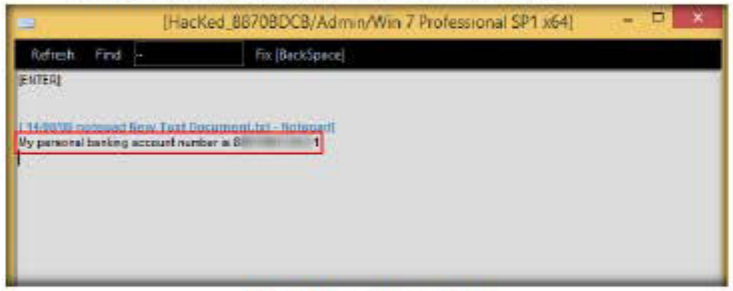


FIGURE 3.24: Keystrokes logged by njRAT

45. Close the Keylogger window.

TASK 10

Chat With the Victim

46. Right-click on the victim name, and click **Open Chat**.

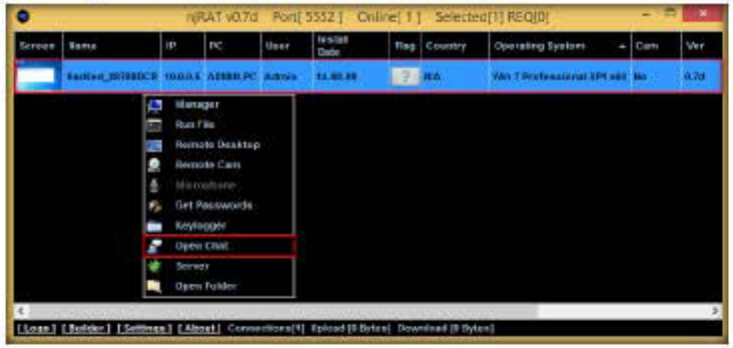


FIGURE 3.25: Opening Chat

47. A **Chat** pop-up appears; enter a nickname (here, **Hacker**), and click **OK**.

FIGURE 3.26: Entering a nickname

48. A chat box appears; type a message, and click **Send**.

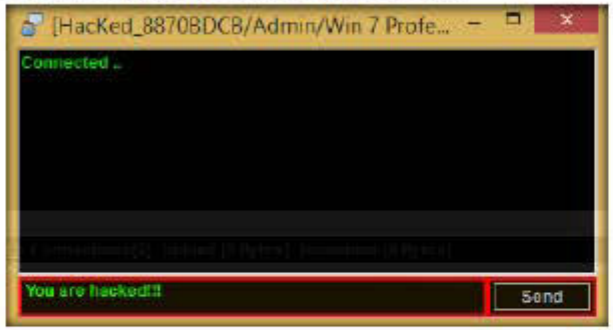


FIGURE 3.27: Typing a message

49. In real time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (**Windows 7**), as shown in the screenshot:

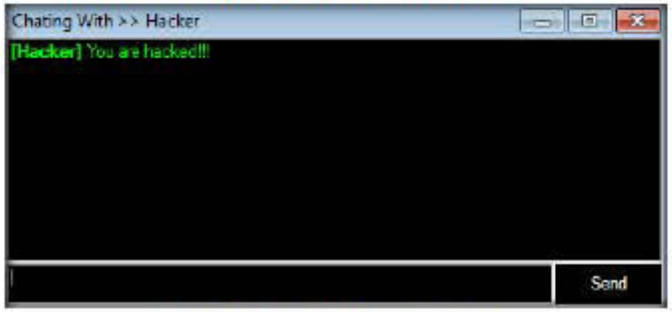


FIGURE 3.28: Message displayed on the victim's desktop

50. Seeing this, the victim becomes alert and attempts to close the chat box. No matter whatever the victim does, the chat box remains opened as long as the attacker uses it.
51. Surprised by the behavior, the victim (you) attempts to break the connection by restarting the machine. As soon as he/she does so, njRAT loses connection with Windows 7, as the machine gets shut down in the process of restarting.

FIGURE 3.29: Shutting down the victim machine

FIGURE 3.30: Connection closed in njRAT GUI

52. However, as soon as the victim logs in to his/her machine, the njRAT client automatically establishes a connection with the victim, as shown in the screenshot:

FIGURE 3.31: Logging in to victim machine

FIGURE 3.32: Connection established automatically

53. The attacker, as usual, makes use of the connection to access the victim machine remotely and perform malicious activity.
54. On completion of the lab, end the **Test.exe** process on the **Windows Server 7** machine.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 4

Obfuscating a Trojan Using SwayzCryptor and Making it Undetectable to Various Anti-Virus Programs

SwayzCryptor is a encrypter (or "crypter") that that allows users to encrypt the source code of their program.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

At present, there have been numerous anti-virus software programs configured to detect malware such as Trojans, viruses and worms. Though security specialists keep updating the virus definitions, hackers try to evade/bypass them by some or the other means. One method which attackers use to bypass AVs is to "crypt" (an abbreviation of "encrypt") the malicious files using fully undetectable crypters (FUDs). Crypting these files allow them to achieve their objectives and thereby taking complete control over the victim machine.

As an expert security auditor or ethical hacker, you need to ensure that your organization's network is secure from such encrypted malware files, and anti-virus tools are properly configured to detect and delete such files.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Objectives

The objective of this lab is to make students learn and understand how to crypt a Trojan and make it partially/completely undetectable.

Lab Environment

To carry out the lab, you need:

- SwayzCryptor located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Crypters\SwayzCryptor**
- A computer running Windows Server 2012 as host machine

- A computer running Window 8.1 Virtual Machine (Attacker)
- A computer running Window 7 Virtual Machine (Victim)
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Crypters

A crypter is software used to hide viruses, keyloggers, or any RAT tool from antiviruses so that they are not detected and deleted by antiviruses. It simply assigns hidden values to each individual code within source code. Thus, the source code becomes hidden, making it difficult for the anti-virus tools to scan it.

Lab Tasks

TASK 1

Scan with VirusTotal

1. Log into **Windows 8.1** virtual machine.
2. Launch a Web browser, and enter the URL https://www.virustotal.com in the address bar.
3. The **VirusTotal** main analysis site appears; click **Choose File** to upload a virus file.

FIGURE 4.1: VirusTotal webpage

4. An **Open** dialog box appears; navigate to the location where you have saved the Trojan file **Test.exe** in the previous lab (**Desktop**), select it, and click **Open**.

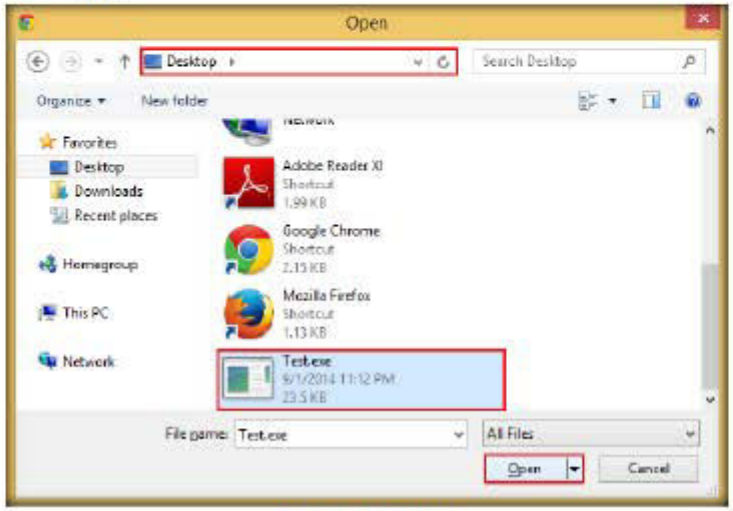


FIGURE 4.2: Open dialog-box

5. On selecting the file, click **Scan it!**

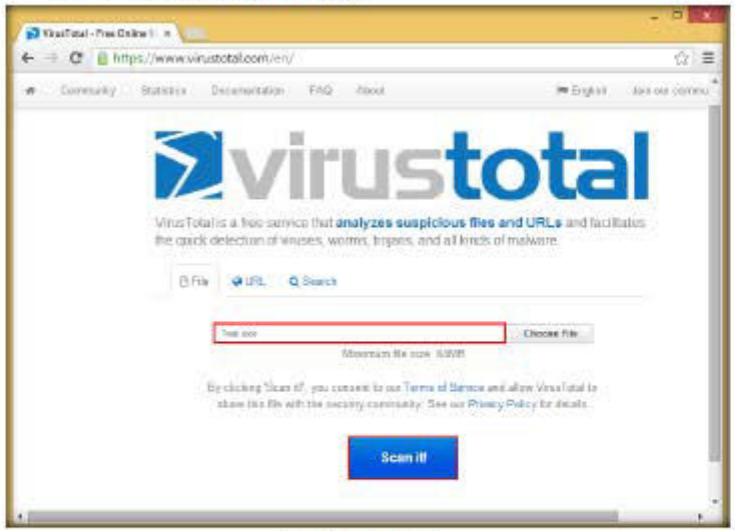


FIGURE 4.3: Scanning the file

6. VirusTotal uploads the file and begins to scan it with various anti-virus programs in its database, and displays the scan result shown in the screenshot:

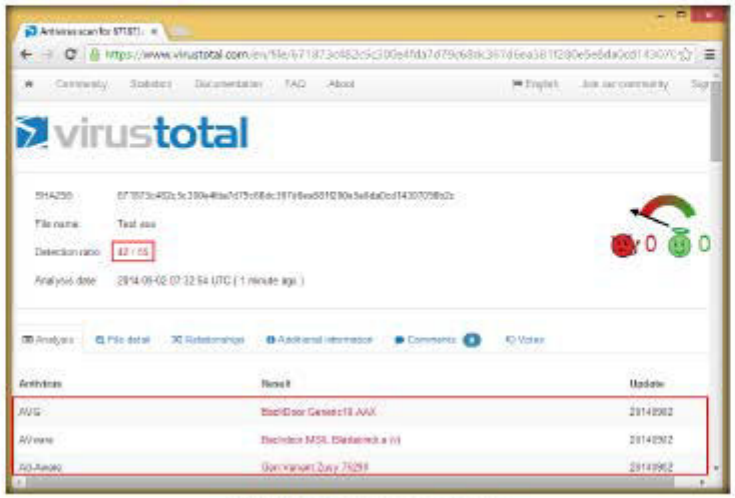


FIGURE 4.4: File detected by various anti-viruses

7. You can see that **42** anti-virus programs out of **55** have detected Test.exe as a malicious file.

Note: The detection ratio might vary in your lab environment.

TASK 2

Crypt a Trojan Using SwayzCryptor

8. Browse to **Z:\CEHv9 Module 06 Malware Threats\Crypters\SwayzCryptor**, and double-click **SwayzCryptor.exe**.
9. The **SwayzCryptor** GUI appears; click [...] below **File** to select the Trojan file:

FIGURE 4.5: Uploading the malicious file

10. The **Select a File** dialog-box appears; navigate to the location of **Test.exe** (**Desktop**), select it, and click **Open**.

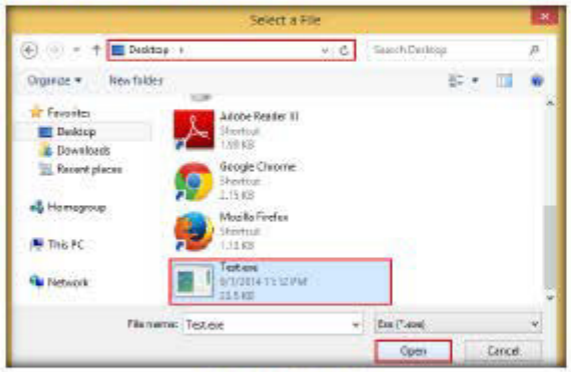


FIGURE 4.6: Selecting the File

11. Once the file is selected, check the options **Start up**, **Mutex,** and **Disable UAC,** and click **Encrypt**.

FIGURE 4.7: Configuring options

12. The **Save File** dialog-box appears; select a location where you want to store the crypted file (here, the **Desktop**), leave the file name set to its default (**CryptedFile**), and click **Save**.

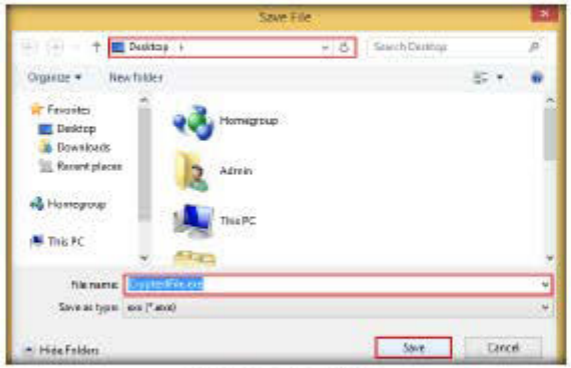


FIGURE 4.8: Save File dialog-box

13. Once the encryption is finished, click **Close**.

FIGURE 4.9: Closing the GUI

TASK 3

Scan with VirusTotal

14. Launch web browser and enter the URL https://www.virustotal.com in the address bar.
15. The **VirusTotal** main analysis site appears; click **Choose File** to upload a virus file.
16. An **Open** dialog-box appears; navigate to the location where you have saved the encrypted file **CryptedFile.exe** (**Desktop**), select the file, and click **Open**.

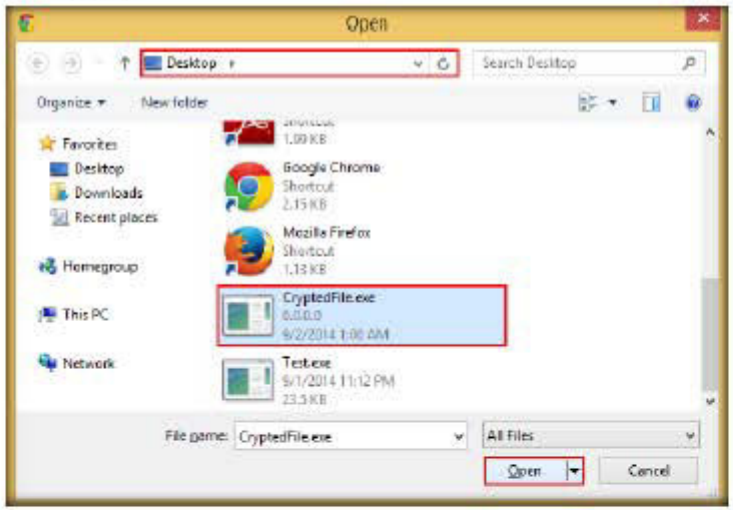


FIGURE 4.10: Open dialog-box

17. On selecting the file, click **Scan it!**

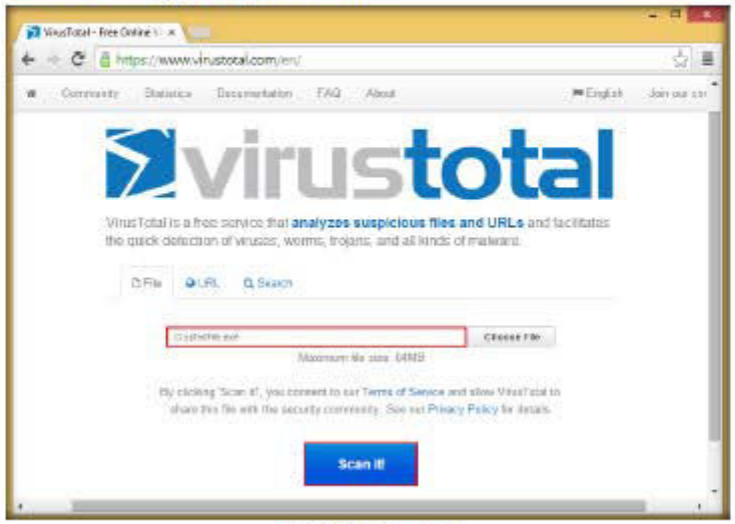


FIGURE 4.11: Scanning the file

18. VirusTotal uploads the file and begins to scan it with various anti-virus programs in its database. It displays the scan result shown in the screenshot:

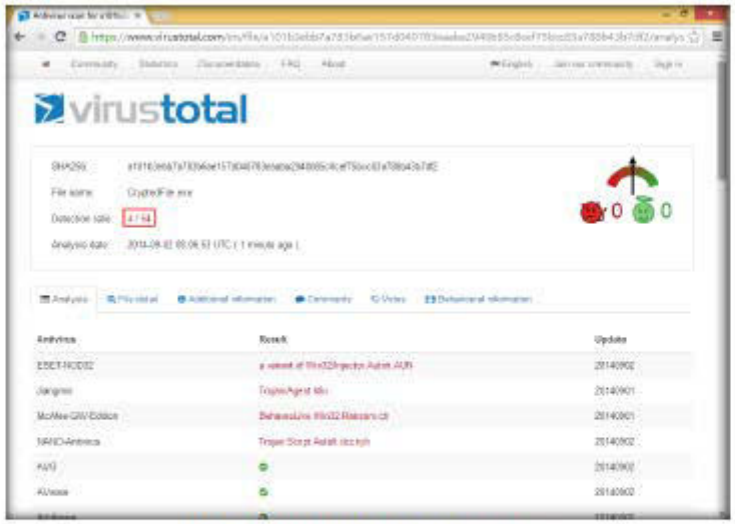


FIGURE 4.12: File detected by very few anti-virus programs

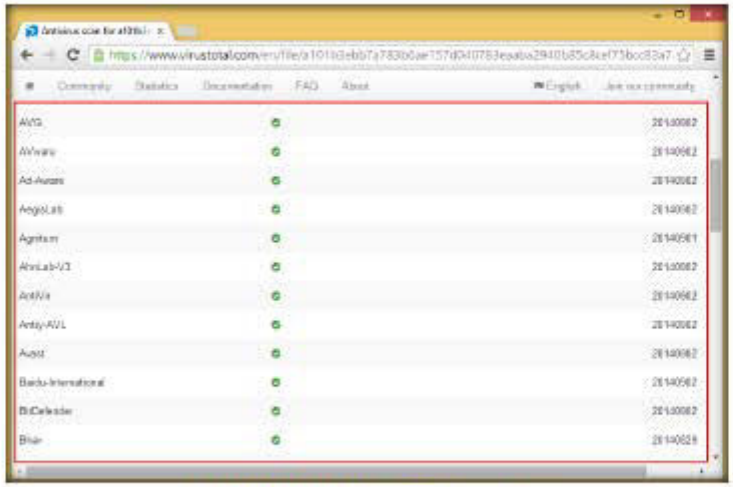


FIGURE 4.13: File detected by very few anti-virus programs

19. You can see that very few anti-virus programs have detected **CryptedFile.exe** as a malicious file, while others failed to detect.

Note: The scan result might vary in your lab environment.

TASK 4

Test the Crypted File

20. To test the functioning of the Crypted file, follow these steps:
21. Browse to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**, and launch njRAT by choosing the default port number **5552**.

FIGURE 4.14: Start njRAT

22. Use any technique to send **CryptedFile.exe** to the intended target, through mail or any other source.

23. Log in to **Windows 7** virtual machine as a legitimate user. Download the file from the source through which the attacker (here, **you**) has sent the server executable and save it in a location.
24. In this lab, the server has been saved to **Desktop** in **Windows 7** virtual machine.
25. Here, you are acting as an **attacker** who logged in to **Windows 8.1** machine to create a malicious server, and as a **victim** who logged into **Windows 7** virtual machine and downloaded the server.
26. Double-click **CryptedFile.exe** to run this malicious executable.

FIGURE 4.15: Executing the Crypted file

27. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in Windows 8.1 establishes a persistent connection with the victim machine, as shown in the screenshot:

FIGURE 4.16: Connection established by njRAT

Note: If njRAT fails to establish a connection, delete temporary files in both **Windows 8.1** and **Windows 7** virtual machines, end **Test.exe** process in Windows 7 virtual machine's task manager (if you haven't done it in the previous lab), and again double-click **CryptedFile.exe**.

28. Unless the attacker working on **Windows 8.1** machine disconnects the server on his own, the victim machine remains under his/her control.
29. Thus, you have created an undetectable Trojan, which can be used to maintain a persistent connection with the victim, as well as bypass the anti-virus and firewall programs.
30. On completing the lab, end the **CryptedFile.exe** process in Windows 7.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Lab 5

Creating a Server Using the ProRat Tool

ProRat is a Remote Administration Tool written in C programming language and capable of working with all Windows operating systems.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers use malware to steal personal information, financial data, and business information from target systems. ProRat is a "remote administration tool" made by PRO Group. ProRat was written in C programming language and capable of working with all Windows operating systems. ProRat was designed to allow users to control their own computers remotely from other computers. However, attackers have co-opted it for their own nefarious purposes. Some hackers take control of remote computer systems to conduct a denial of service (DoS) attack, which renders the target system unavailable for normal personal or business use. These targeted systems have included high-profile web servers such as banks and credit card gateways.

You, as an ethical hacker or pen-tester, can use ProRat to audit your own network against remote access Trojans.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of this lab include:

- Creating a server and testing the network for attack
- Detecting Malware
- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab Environment

To complete this lab, you will need:

- **Prorat** tool located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat**
- A computer running Windows Server 2012 as Host Machine
- A computer running Windows 8.1 (Virtual Machine)
- Windows Server 2008 running in Virtual Machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of the Malware

ProRat is a remote administration tool (RAT) written in C programming language and is capable of working with all Windows operating systems. The main purpose of this RAT is to access one's own computers remotely. As with other Trojan horses, ProRat uses a client and server. It opens a port on the computer, which allows the client to perform numerous operations on the server (the victim machine).

Some of the ProRat's malicious actions on the victim's machine:

- Logging keystrokes
- Stealing passwords
- Full control over files
- Drive formatting
- Open/close CD tray
- Hide taskbar, desktop, and start button
- View system information

Note: The versions of the created client or host and appearance of the website may differ from what it is in the lab. But the actual process of creating the server and client is as shown in this lab.

Lab Tasks

TASK 1

Create Server with ProRat

1. Launch **Windows 8.1** virtual machine.
2. Navigate to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat** and double-click on **Prorat 1.9 SE.exe** in **Windows 8.1** virtual machine.
3. If an **Open File - Security Warning** pop-up appears, click **Run**.

4. **ProRat** main window appears, click **Create**.

FIGURE 5.1: ProRat main window

5. Click **Create ProRat Server (342 Kbayt)** to create a ProRat server.

FIGURE 5.2: Creating a ProRat Server

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

6. **Create Server** window appears.

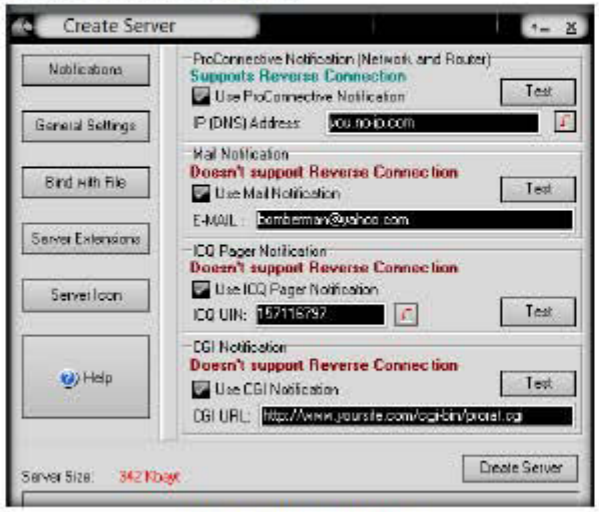


FIGURE 5.3: Create Server window

Password button: Retrieve passwords from many services, such as pop3 accounts, messenger, IE, mail, etc.

7. Click on **General Settings** button to configure features such as **Server Port**, **Server Password**, **Victim Name**, and the **port number**. In this lab, default settings are chosen. Note down the **Server password**.
8. Uncheck the highlighted **options,** as shown in the screenshot:

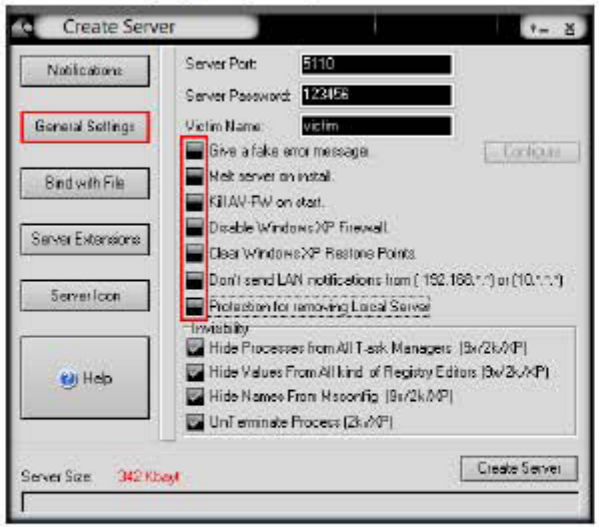


FIGURE 5.4: Configure the server

Note: you can use Dynamic DNS to connect over the Internet by using no-ip account registration.

9. Click on **Bind with file** button to bind sever with a file. In this lab, we are using **.jpg** file to bind the server.

Clipboard: To read data from random access memory.

10. Check **Bind server with a file** option, click **Select File** button, and navigate to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat\Images**.

VNC Trojan starts a VNC server daemon in the infected system.

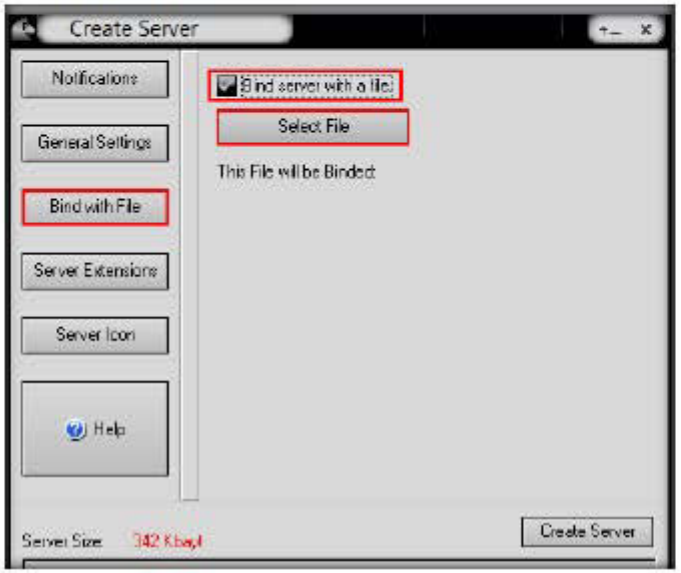


FIGURE 5.5: ProRat Binding with a file

11. Select **Car.jpg** in browse window, and click **Open** to bind the file.

File manager: To manage victim directory for add, delete, and modify.

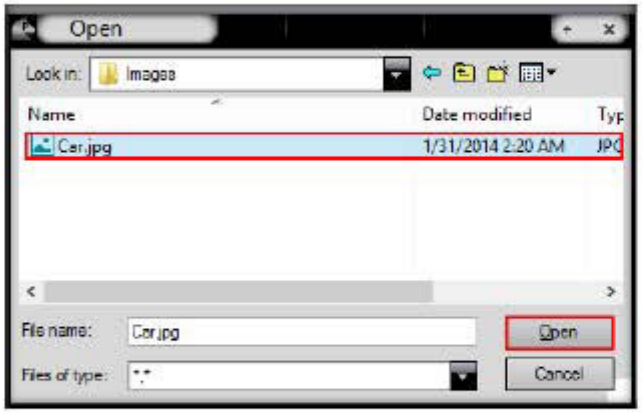


FIGURE 5.6: ProRat binding an image

12. A pop-up displays the prompt: **ProRat server will bind with Car.jpg**. Click **OK**.

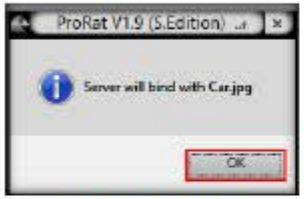


FIGURE 5.7: ProRat Pop-up

13. Click **Server Extensions**.
14. Under **Select Server Extension**, check **EXE (Has icon support)**.

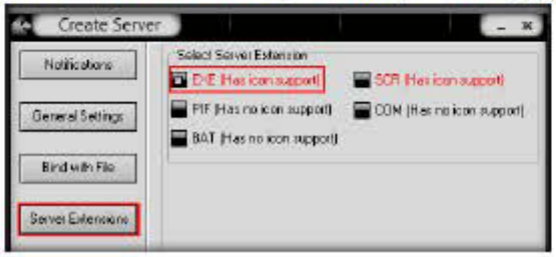


FIGURE 5.8: ProRat Server Extensions Settings

15. Click **Server Icon**.
16. Under Server Icon, select any icon, and click **Create Server**.

FIGURE 5.9: ProRat creating a server

Give Damage: To format the entire system files.

It connects to the victim using any VNC viewer with the password "secret."

17. A pop-up states that the server has been created. Click **OK**.

FIGURE 5.10: ProRat Server has created in the same current directory

18. The created server will be saved in **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat**. This server is named **binded_server** by default.

SHTTPD is a small HTTP server that can be embedded inside any program. It can be wrapped with a genuine program (game chess.exe). When executed, it turns a computer into an invisible web server.

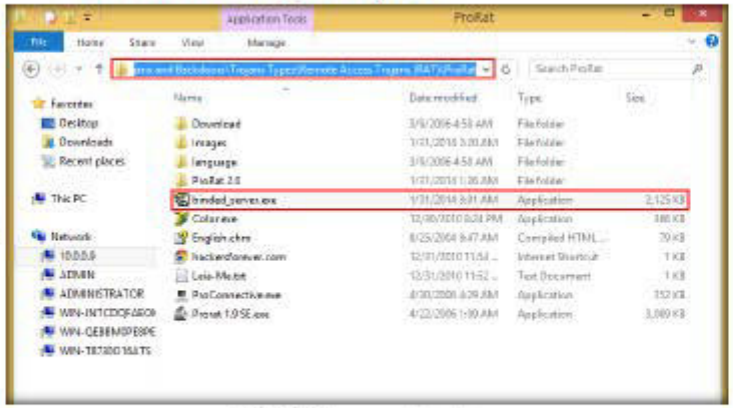


FIGURE 5.11: Server saved to the location

19. In real time, hackers may craft such servers and send them **by mail** or any communication media to the **victim's** machine.

Note: You need to **zip** the file before mailing it, as you cannot attach **.exe** files on some mail servers.

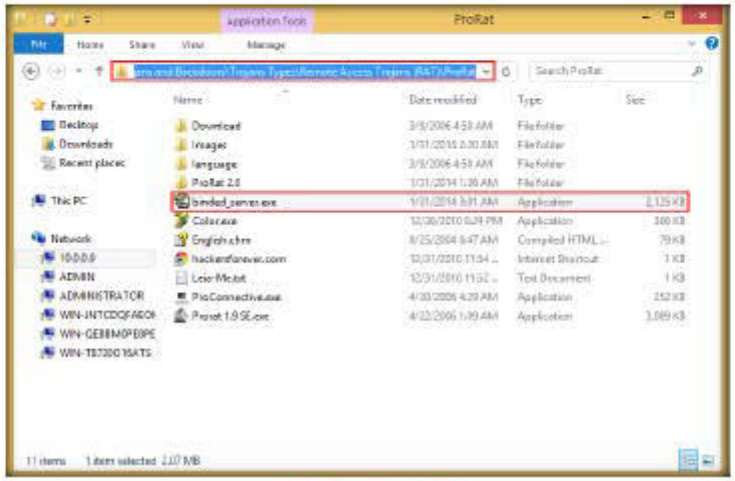


FIGURE 5.12: Sending the file

20. Launch **Windows Server 2008**, navigate to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat,** and double-click **binder_server.exe**.

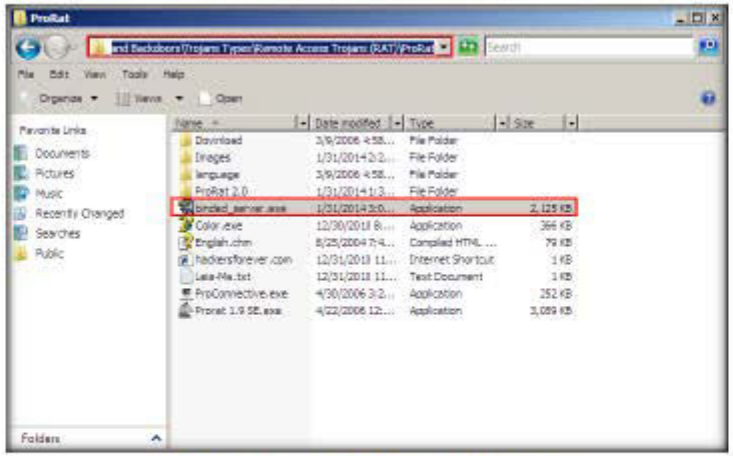


FIGURE 5.13: Executing the file sent from Windows 8.1 machine

21. If the **Open File - Security Warning** pop-up appears, click **Run**.
22. Switch back to the **Windows 8.1** virtual machine, and enter the IP address of **Windows Server 2008**; keep the default port number in the ProRat main window, and click **Connect.**
23. In this lab, the IP address of Windows Server 2008 is (**10.0.0.11**).

Note: The IP address of Windows Server 2008 may differ in your lab environment.

FIGURE 5.14: ProRat Connecting Infected Server

ICMP Trojan: Covert channels are methods in which an attacker can hide data in a protocol that is undetectable.

24. Enter the **password** you noted down at the time of creating Server and click **OK**.

FIGURE 5.15: Entering the password

Covert channels rely on techniques called tunneling, which allow one protocol to be carried over another protocol.

25. Now you are **connected** to the victim machine.
26. ProRat begins to monitor the user activities. It records all passwords, keystrokes, and so on.

27. To test the connection, click **PC Info,** and choose **System Information**.
28. ProRat displays the information of the victim machine, as shown in the screenshot:

FIGURE 5.16: ProRat connected computer window

TASK 2

Log all the Keystrokes

29. Click on **Keylogger** to **steal** user passwords for the online system.

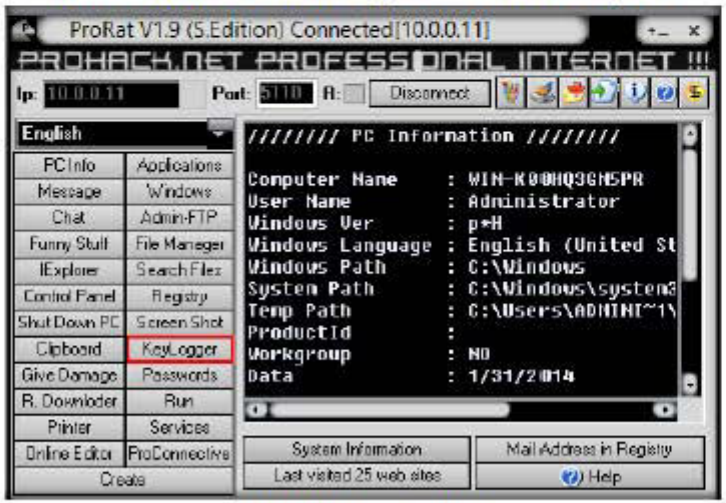


FIGURE 5.17: ProRat KeyLogger button

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

30. **KeyLogger** window appears, click **Read Log** to view the keylogs performed by the target user on the victim machine.

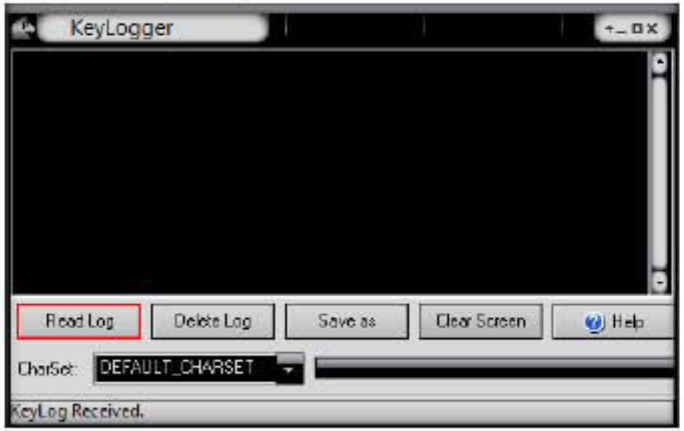


FIGURE 5.18: ProRat KeyLogger window

This Trojan works like a remote desktop access. The hacker gains complete GUI access of the remote system:

- Infect victim's computer with server.exe and plant Reverse Connecting Trojan.
- The Trojan connects to victim's Port to the attacker and establishing a reverse connection.
- Attacker then has complete control over victim's machine.

31. Switch to **Windows Server 2008** machine and open a browser, or Notepad, and type any text.

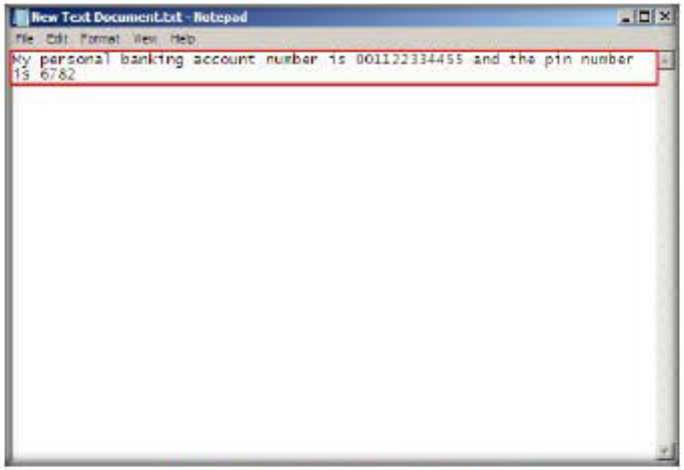


FIGURE 5.19: Text typed in Windows Server 2008 Notepad

Banking Trojans are program that steals data from infected computers via web browsers and protected storage.

32. While the victim is writing a **message** or entering a **username** and password, you can capture the log entity.

33. Now, switch to **Windows 8.1** Virtual Machine, and click **Read Log** from time to time to check for keystrokes logged from the victim machine.

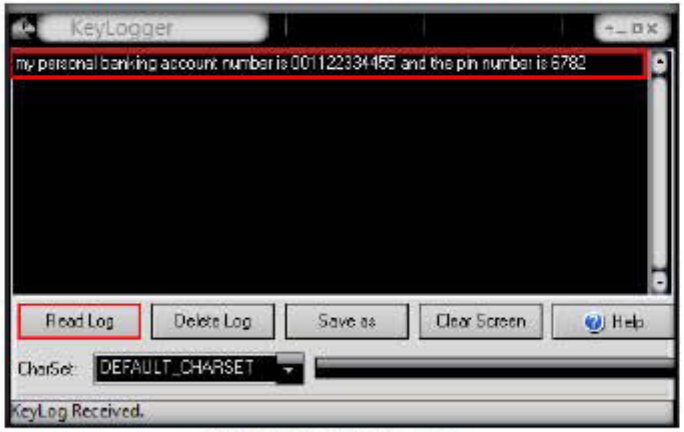


FIGURE 5.20: ProRat KeyLogger window

34. In the same way, you can make use of the other options that allow you to explore and control the victim machine.

Note: ProRat Keylogger will not read special characters.

35. On completing the lab, end the **binder_server.exe** process on the **Windows Server 2008** machine.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 6

Creating a Trojan Server Using Theef

Theef is a Windows-based application for both a client and a server. The Theef server is a virus that you install on a target computer, and the Theef client is what you then use to control the virus.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A backdoor Trojan provides remote, usually surreptitious, access to affected systems. A backdoor Trojan may be used to conduct distributed denial of service (DDoS) attacks, or it may be used to install additional Trojans or other forms of malicious software. For example, a backdoor Trojan may be used to install a downloader or dropper Trojan, which may in turn install a proxy Trojan used to relay spam or a keylogger Trojan that monitors and sends keystrokes to remote attackers. A backdoor Trojan may also open ports on the affected system, and can thus potentially lead to further compromise by other attackers.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks. The objectives of this lab include:

- Creating a server and testing the network for attack
- Detecting Malware
- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Environment

To complete this lab, you will need:

- **Theef** tool located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef**
- A computer running Windows Server 2012 as Host Machine
- A computer running Window 8.1 Virtual Machine (Attacker)

- A computer running Window Server 2008 Virtual Machine (Victim)
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

Overview of Trojans

Theef is a Remote Access Trojan written in Delphi, which gives remote attackers system access via port 9871. It is a Windows-based application for both a client and a server. The Theef server is a virus installed on a target system, and using Theef client, an attacker can control the virus.

Note: The versions of the created client or host, and the appearance of its website, may differ from that of the lab. But the actual process of creating the server and the client is the same.

Lab Tasks

TASK 1

Execute Server in the Victim Machine

1. Generally, an attacker might send a server executable to the victim machine and entice the victim to run it. In this lab, for demonstration purpose, we are directly executing the file in the victim machine, **Windows Server 2008**.
2. Launch the **Windows Server 2008** virtual machine (as **victim**), and navigate to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef**.
3. Double click **Server210.exe** to run the Trojan on the victim's machine.

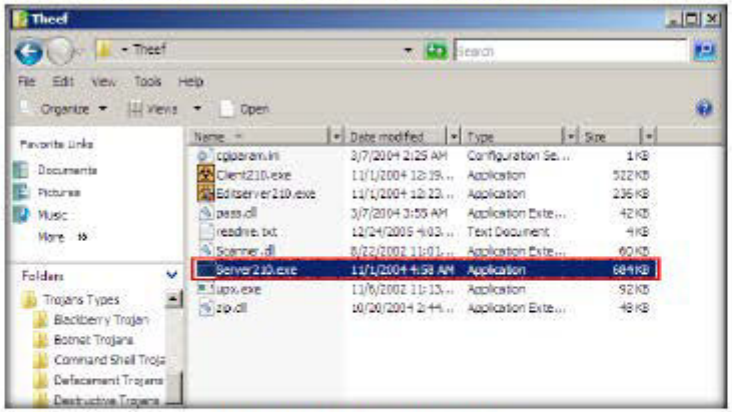


FIGURE 6.1: Windows Server 2008-Theef Folder

4. If the **Open File - Security Warning** pop-up appears, click **Run**.

5. Now log into **Windows 8.1** virtual machine (as **attacker**), and navigate to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef**.

TASK 2

Establish Connection with the Target

6. Double click **Client210.exe** to access the victim machine remotely.

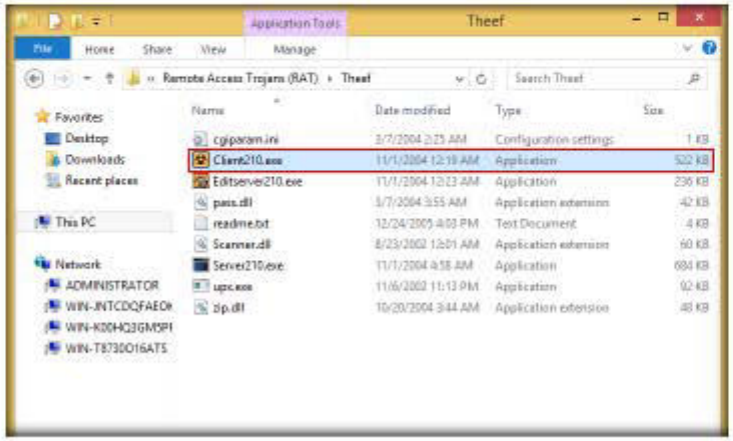


FIGURE 6.2: Windows 8.1-Running Client210.exe

7. If the **Open File - Security Warning** pop-up appears, click **Run**.
8. The main window of Theef appears as shown in the screenshot:

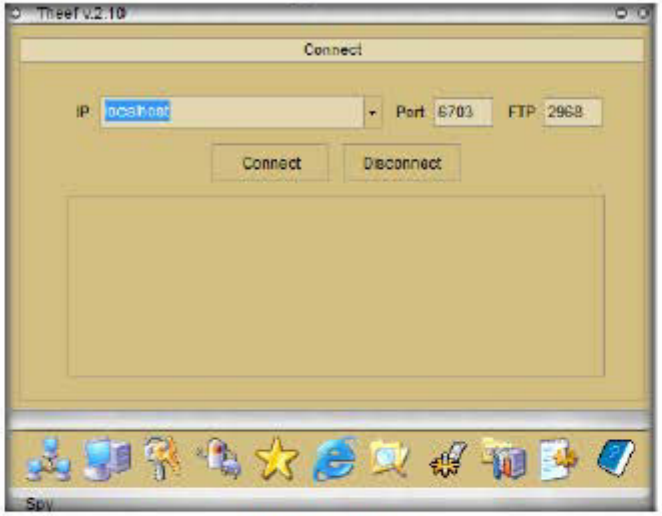


FIGURE 6.3: Theef Main Screen

9. Enter the target (**Windows Server 2008**) IP Address in the **IP** field (**10.0.0.12**), and leave the **Port** and **FTP** fields set to default. Click **Connect**.

Note: The target IP address may vary in your lab environment.

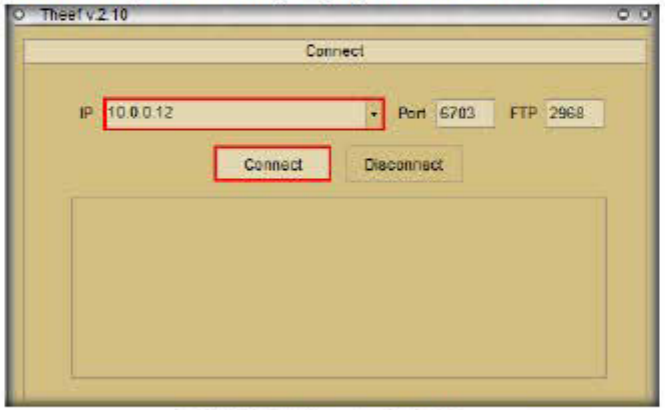


FIGURE 6.4: Thief Connecting to Victim Machine

10. Now, in **Windows 8.1** you have successfully established a remote connection with **Windows Server 2008**.
11. To view the Computer Information, click on **Computer Information** in the lower part of the window.

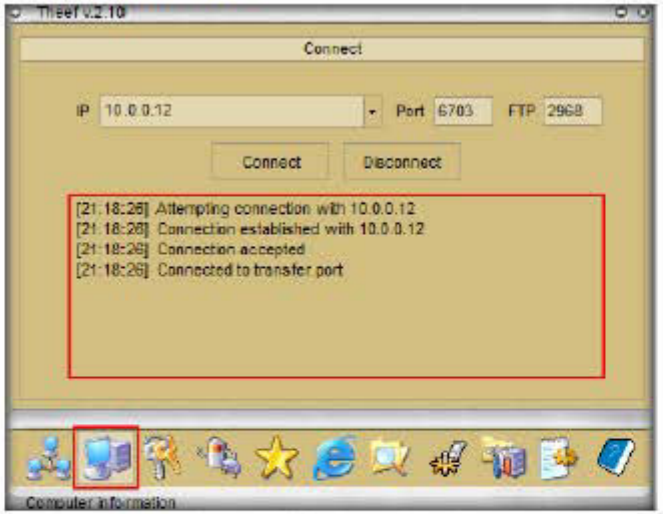


FIGURE 6.5: Thief Gained access to Victim Machine

TASK 3

Extract System Information

12. In Computer Information, you can view **PC Details**, **OS Info**, **Home**, and **Network** by clicking their respective buttons.
13. Here, for instance, **PC Details** has been selected to view computer-related information.

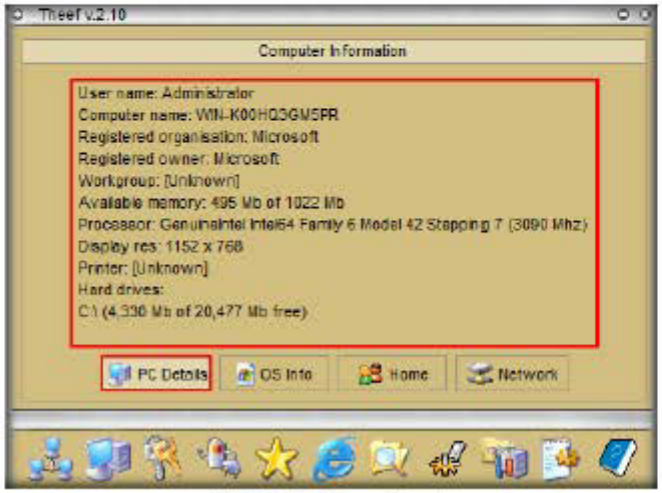


FIGURE 6.6: Theef Computer Information

14. Click **Spy** to capture screens, Keyloggers, etc. of the victim machine.

FIGURE 6.7: Theef Spy

TASK 4

Manipulate Tasks in the Task Manager

15. Select **Task Manager** to view the tasks running on the target machine.

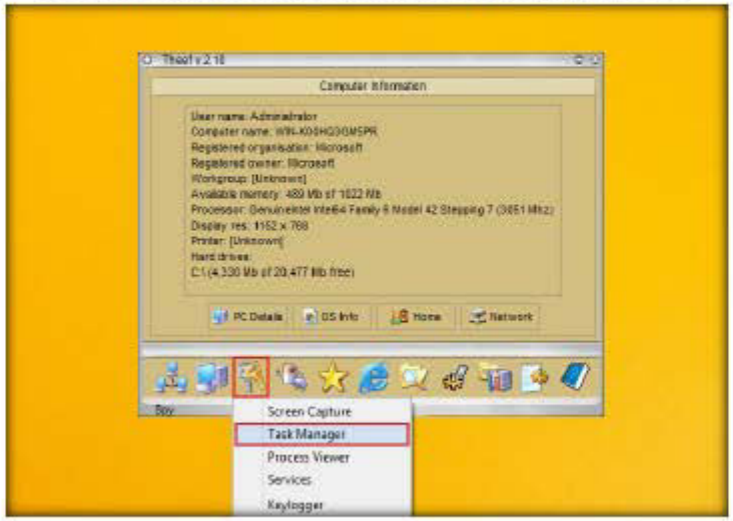


FIGURE 6.8 Selecting the Task Manager

16. In the Task Manager window, select a process (task), and click **Close window** to end the task in the target machine.

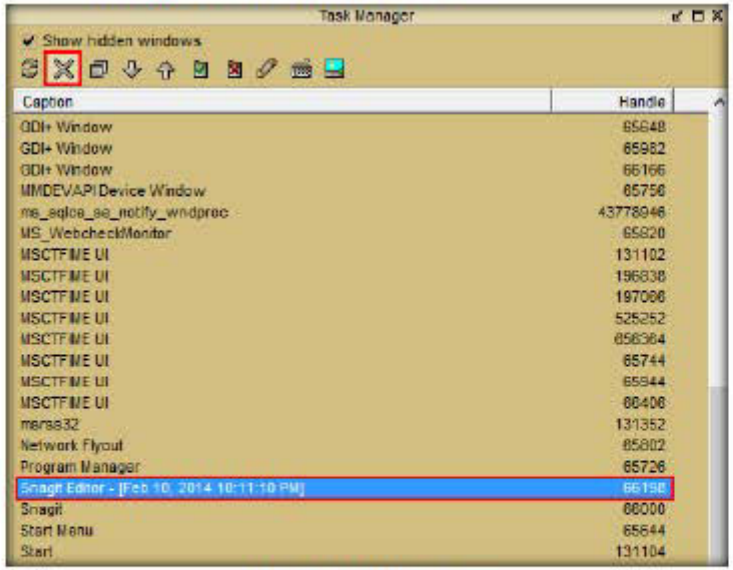


FIGURE 6.9: Thief Task Manager Window

Note: The tasks running in the task manager may vary in your lab environment.

17. Similarly, you can access the details of the victim machine by clicking on respective icons.
18. On completing the lab, end the **Server210.exe** process on the Windows Server 2008 machine.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 7

Attaining Remote Access Using Atelier Web Remote Commander

A Trojan is a program that contains a malicious or harmful code inside apparently harmless programming or data in such a way that it can assume control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Scenario

Atelier Web Remote Commander enables you to connect to other computers without installing any software on the remote machine. It allows you to remotely gather and manipulate information. You, as an ethical hacker or security administrator, can use AWRC to remotely audit and inventory software you can find.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of this lab include:

- Gain access to a remote computer
- Acquire sensitive information of the remote computer

Lab Environment

To complete this lab, you will need:

- **Atelier Web Remote Commander,** at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Atelier Web Remote Commander**
- A computer running Window Server 2012 (attacker)
- Windows Server 2008 running in virtual machine (victim)
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A web browser with access Internet

- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

Overview of the Lab

AWRCP lets you manage servers and workstations from your local computer. AWRCP does not require that you install any software on the remote machine. This turns the software particularly useful for accessing remote machines without any previous preparation. AWRCP provides lots of powerful tools for remote management and audit. With such tools you will be able to perform operations on the remote system that privileged remote interactive users himself could only dream about. With AWRCP you have the knowledge and capabilities to do virtually anything on the remote computer.

TASK 1

Install Atelier Web Remote Commander

Lab Tasks

1. Before beginning the lab, launch **Windows Server 2008** virtual machine.
2. Switch back to the host machine, and navigate to **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Atelier Web Remote Commander.**
3. Double-click **setup.exe,** and follow the wizard-driven installation steps to install the application.

FIGURE 7.1: Atelier Web Remote Commander Installation Wizard

4. On completing the installation, launch **AW Remote Commander** application from the **Apps** screen.
5. Main window of **AWRC** appears, as shown in the screenshot:

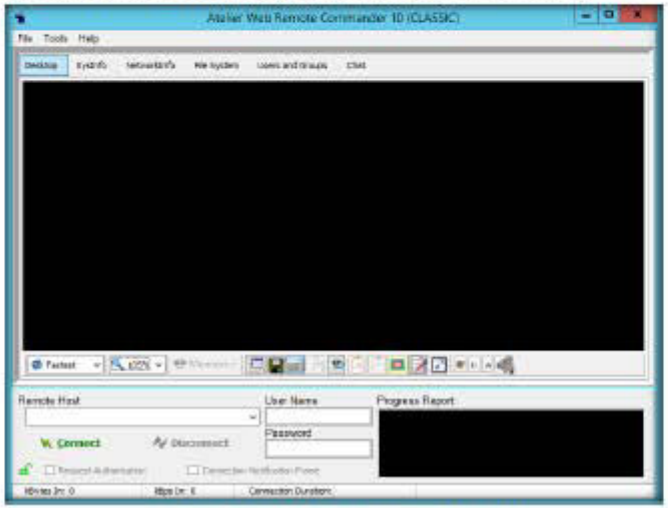


FIGURE 7.2: Atelier Web Remote Commander main window

This tool is used to gain access to all the information of the Remote system

TASK 2

Connect to a Victim Machine

6. Input the **IP address**, **Username**, and **Password** of the target computer.
7. In this lab, we have used **Windows Server 2008** (**10.0.0.11**)
   - Username: **Administrator**
   - Password: **qwerty@123**

Note: The IP addresses and credentials might vary in your lab environment.

8. Click **Connect** to access the machine remotely.

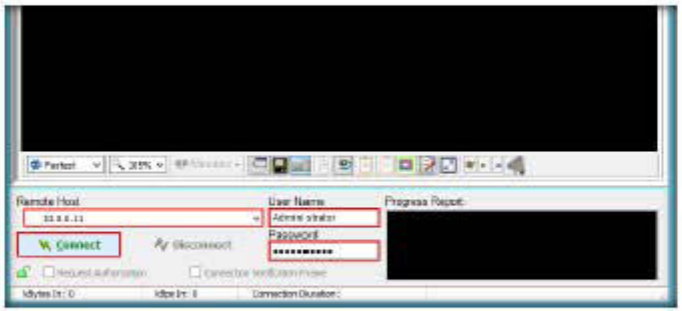


FIGURE 7.3: Providing remote computer details

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

9. You will be able to successfully login to the victim machine remotely, as shown in the screenshot.

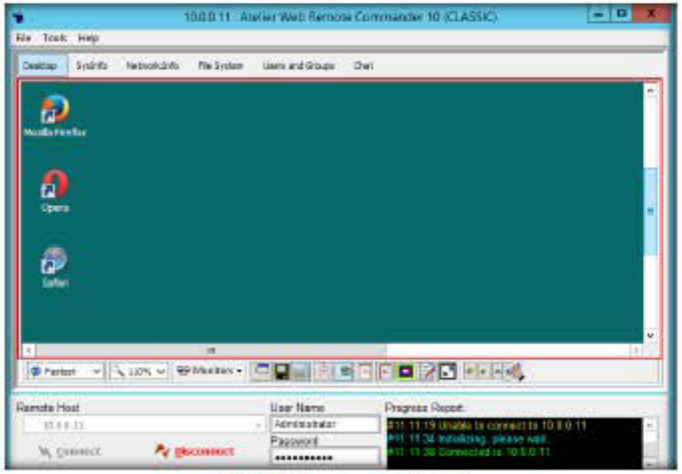


FIGURE 7.4: Remote computer Accessed

TASK 3

Extract Information of the Victim Machine

10. The Commander is now connected to the remote system; click the **SysInfo** tab to view the **General** virtual machine information.

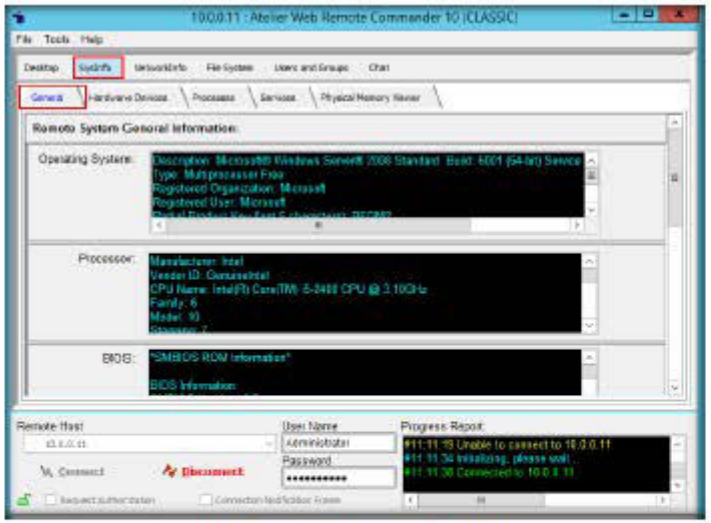


FIGURE 7.5: Information of the remote computer

11. Click the **Processes** tab, under Sysinfo section to view the processes running on the remote machine.

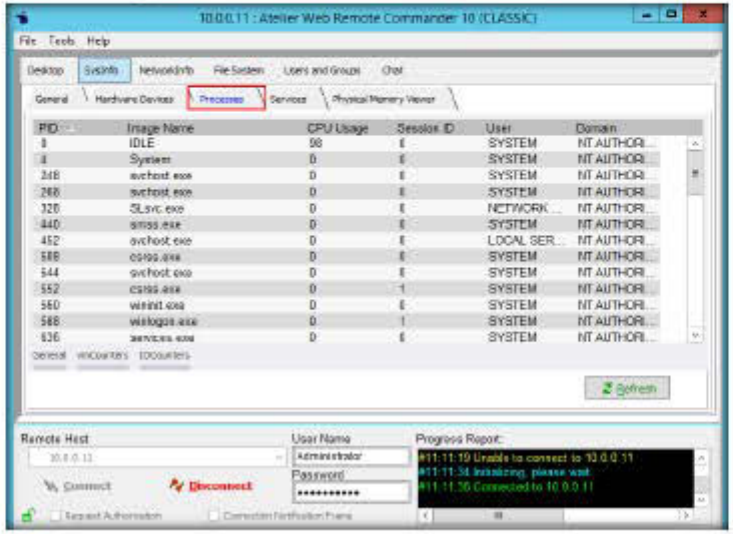


FIGURE 7.6: Processes running on the victim machine

12. In the same way, choose the other tabs to retrieve more information about the target machine.
13. Click the **NetworkInfo** tab to view the network information, such as the shared resources, routing information and so on.

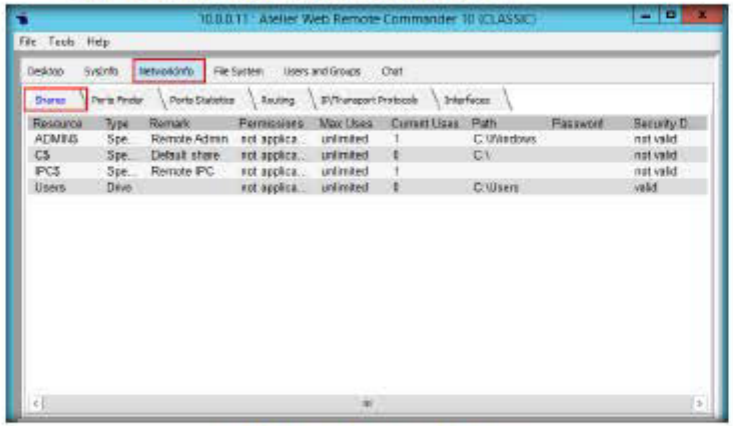


FIGURE 7.7: Viewing the Network Information

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

14. Click the **Routing** tab, under NetworkInfo, to view the **Active Routes**, **Netmask**, **Gateway,** as well as the **DNS Servers**.

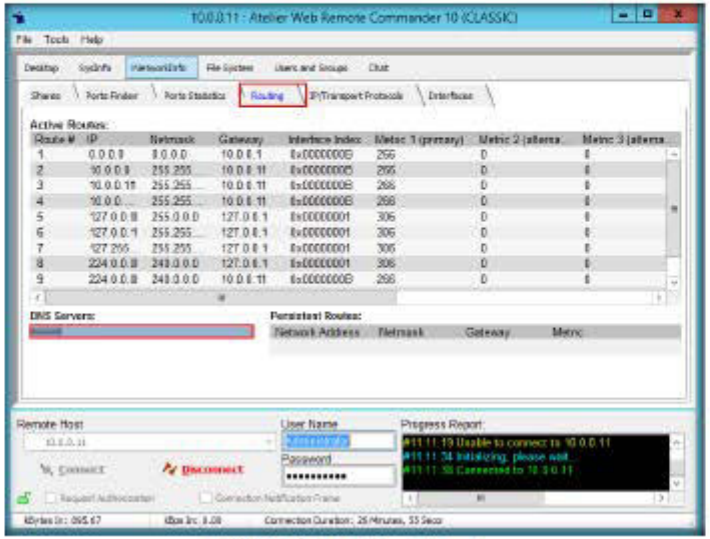


FIGURE 7.8. Viewing the Routing information

15. Click the other tabs to retrieve more information about the network.
16. Click the **File System** tab, choose **C:** from the drop-down list, and click **Get**.

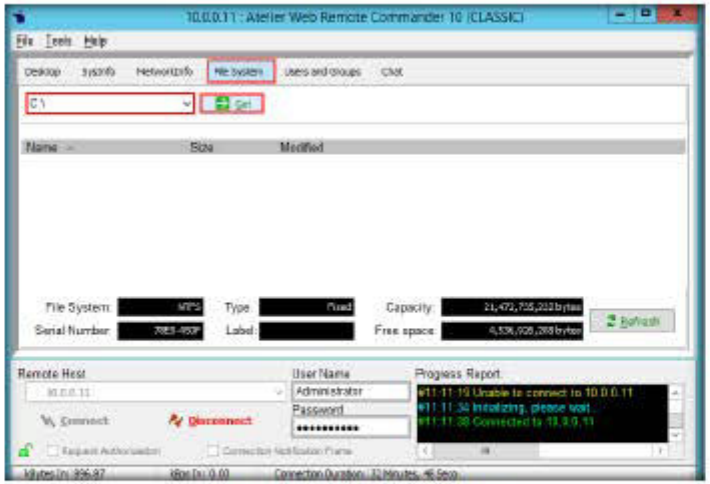


FIGURE 7.9. Obtaining the Files in the machine

17. AWRC lists all the files located in the directory, as shown in the screenshot:

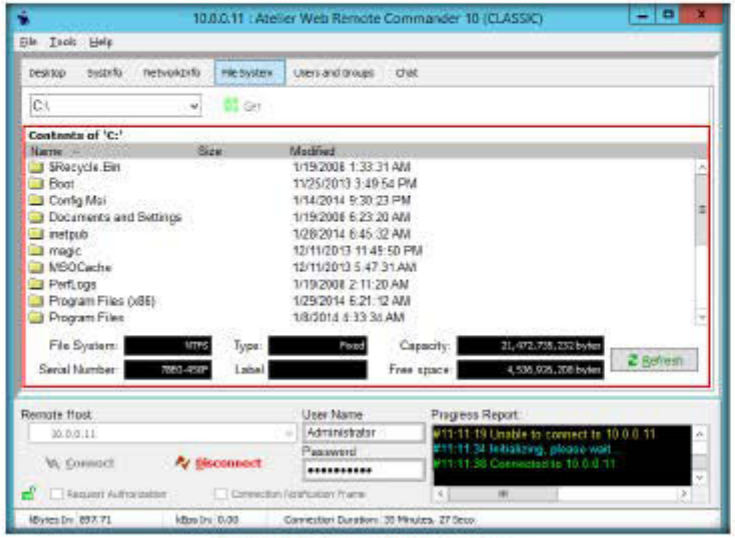


FIGURE 7.10: Viewing the Files in the machine

18. This way, you can choose the other drives and view the files in them.
19. Select **Users and Groups**. AWRC displays **Administrator** information by default.

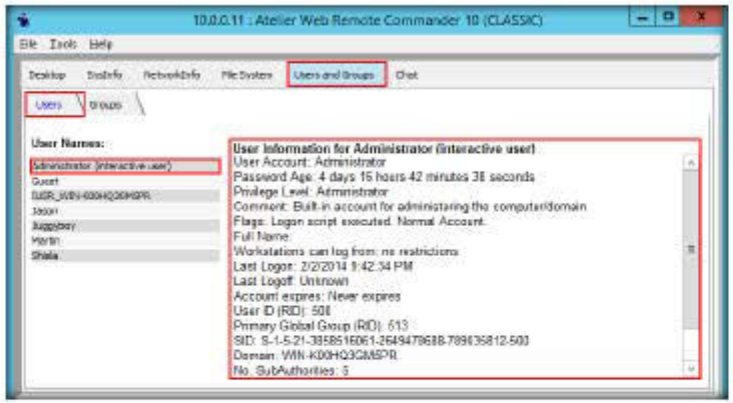


FIGURE 7.11: Users Information of the remote computer

20. You can click the other usernames to view their respective user-account information.

21. Click the **Groups** tab to view all local and global groups.

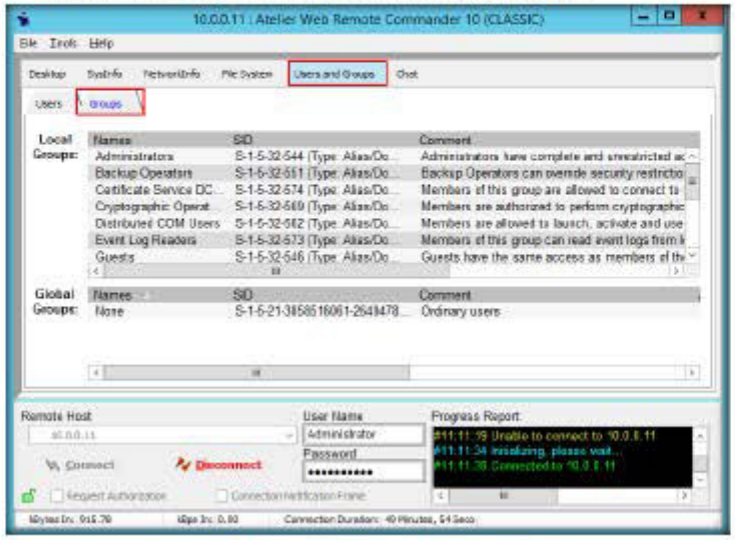


FIGURE 7.12: Groups Information of the remote computer

22. Analyze the results of the remote computer. In real time, attackers attempt to obtain the user credentials, and then directly establish a connection with the remote machine, without the need to send any crafted Trojan/backdoor to the victim, which needs to be executed.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 8

Building a Botnet Infrastructure Using Umbra Loader

Umbra Loader is an open-source HTTP botnet project that allows you to control victim machines (bots) remotely through http channel.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Today, most of the large information security attacks involve botnets in some ways. Attackers, also known as bot herder, use botnet Trojans to infect a large number of computers across a large geographical area to create a network of bots, also known as "bot herd" that can be in control through a Command and Control (C&C) center. They trick normal computer users to download Trojan infected files to their systems through phishing, SEO hacking, URL redirection, and so on. Once the user downloads and executes this botnet Trojan in the system, it connects back to the attacker using IRC channels and waits for instruction. This lab will help you understand how attackers set up a botnet infrastructure. This will enable you to protect your organization's system from being a part of a botnet.

Lab Objectives

The objective of this lab is to help students learn how to:

- Create a botnet using Umbra Loader
- Execute Applications from the Command and Control Center

Lab Environment

To perform the lab, you need:

- Windows Server 2012 host machine
- Windows Server 2008 running as a virtual machine
- Windows 8.1 running as a virtual machine
- Windows 7 running as a virtual machine

- Umbra Loader Botnet located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Botnets**
- Web Browsers
- Administrative Privileges to run the tool

Lab Duration

Time: 20 Minutes

Overview of the Lab

This lab demonstrates how to host the Umbra Loader web panel of WampServer and create a botnet, thereby executing applications on the bots remotely using the command and control center present in Umbra Loader.

Lab Tasks

TASK 1

Start WampServer

1. Launch **Windows Server 2008** virtual machine from Hyper-V Manager and log in to **Administrator** user account.

Note: Before installing WampServer, you need to stop IIS admin service and World Wide Web Publishing Service. To stop the service, go to **Start → Administrative Tools → Services**, right-click **IIS Admin Service,** and click **Stop**, right-click **World Wide Web Publishing Service,** and click **Stop**.

While stopping IIS admin service, if a **Stop Other Services** dialog-box appears stating that other services will also stop, click **Yes**.

2. Click **Start** at the lower-left corner of the screen, and click **start WampServer** to launch WampServer.

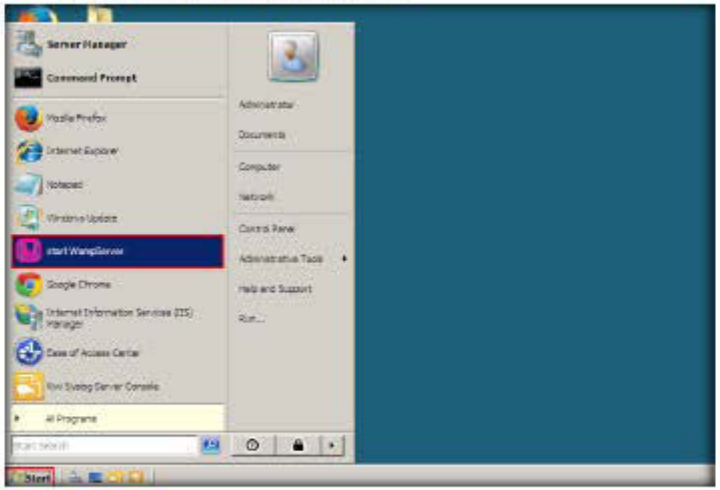


FIGURE 8.1: Launching WampServer

TASK 2

Host the Umbra Loader Website

3. Navigate to **Z:\CEHv9 Module 06 Malware Threats\Botnets**, and copy the **Umbra Loader** folder.

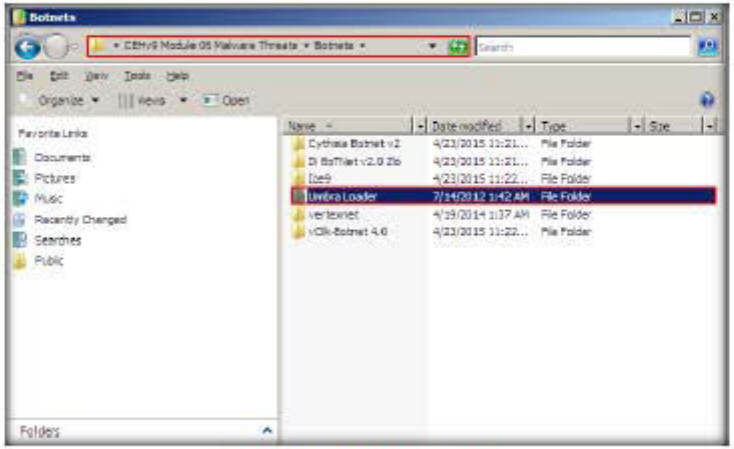


FIGURE 8.2: Copying Umbra Loader Folder

4. Paste the copied **Umbra Loader** folder onto the **Desktop**.

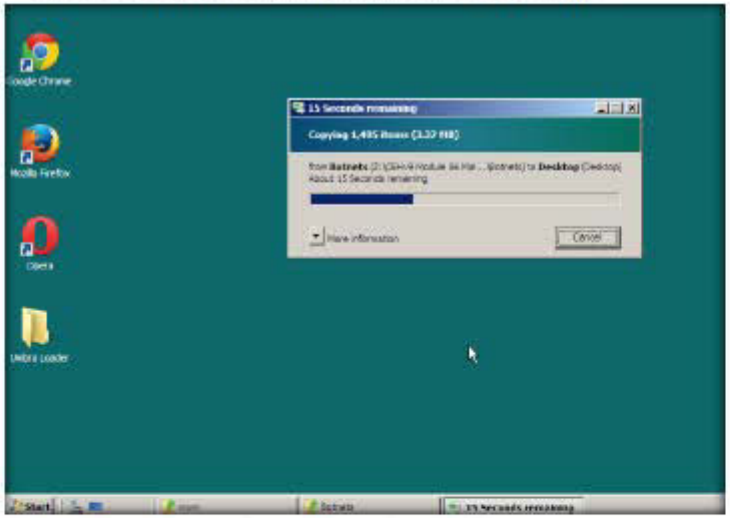


FIGURE 8.3: Pasting Umbra Loader Folder

5. Navigate to **Desktop**, go to **Umbra Loader → Panel,** and copy all the files in the location.

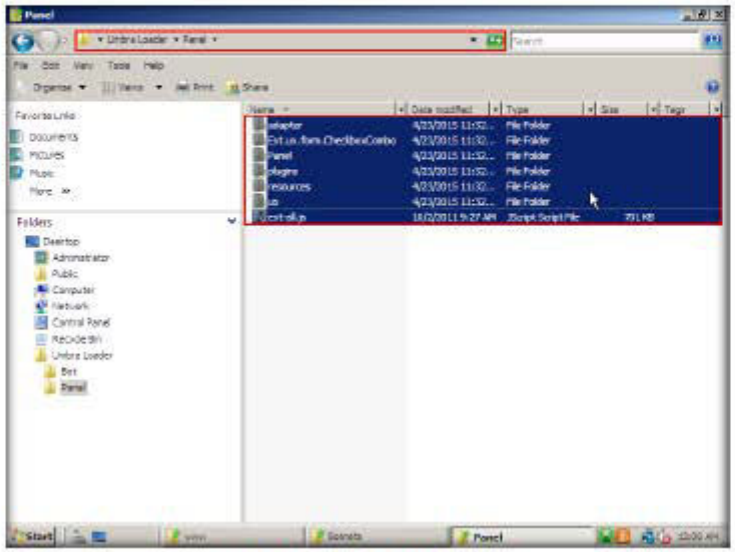


FIGURE 8.4: Pasting Umbra Loader Folder

6. Navigate to **C:\wamp\www,** and create a folder named **umbra.**

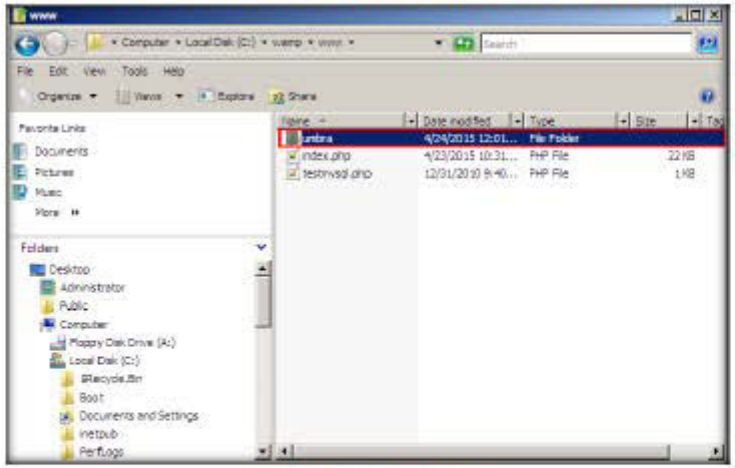


FIGURE 8.5: Creating umbra Folder

7. Open the created **umbra** folder, and paste all files that were copied in **step 5**.

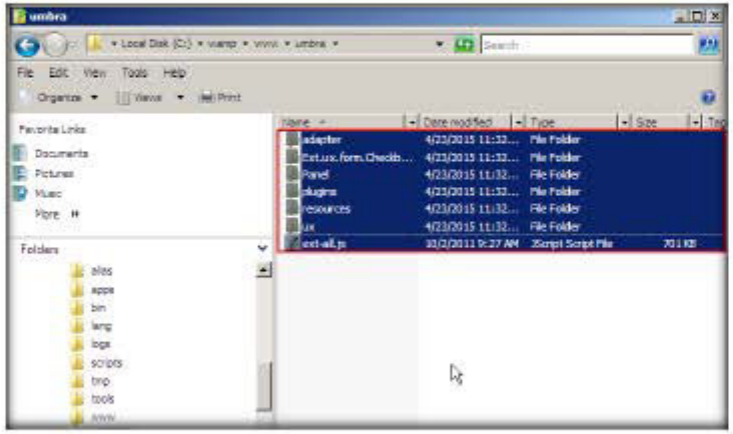


FIGURE 8.6: Pasting the Files

8. Now, we shall create a database for hosting umbra botnet. To create, launch a web browser, type the URL **http://localhost/phpmyadmin** and press **Enter**.
9. **phpMyAdmin** webpage appears. Click **Databases** tab.

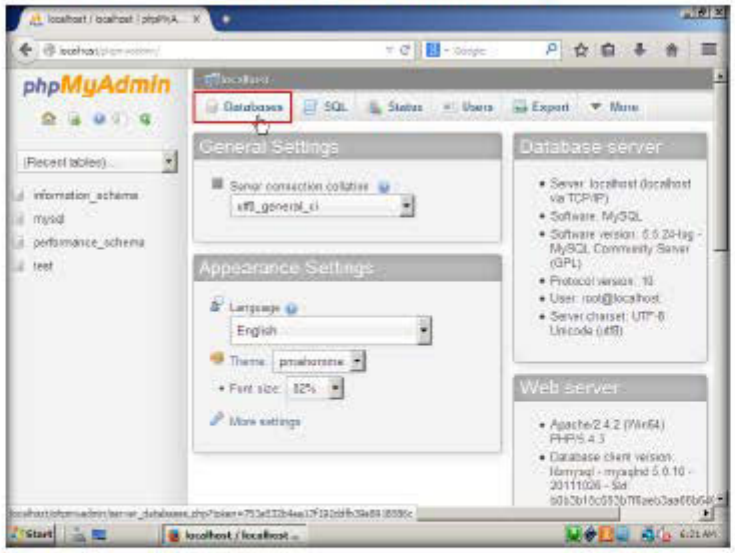


FIGURE 8.7: Creating Database

10. **Databases** webpage appears, type **umbra** in the **Create database** text field, leave the drop-down list set to default as **Collation** and click **Create** to create the new database.

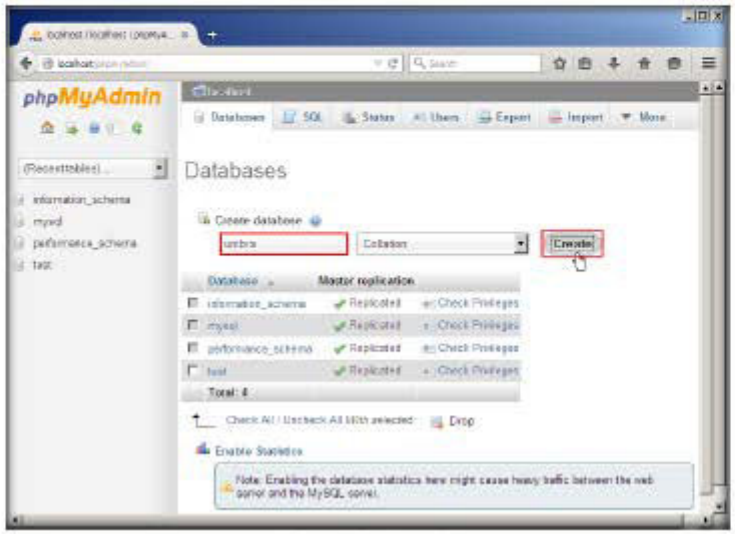


FIGURE 8.8: Creating Database

11. The newly added database appears in the left pane; click on it.

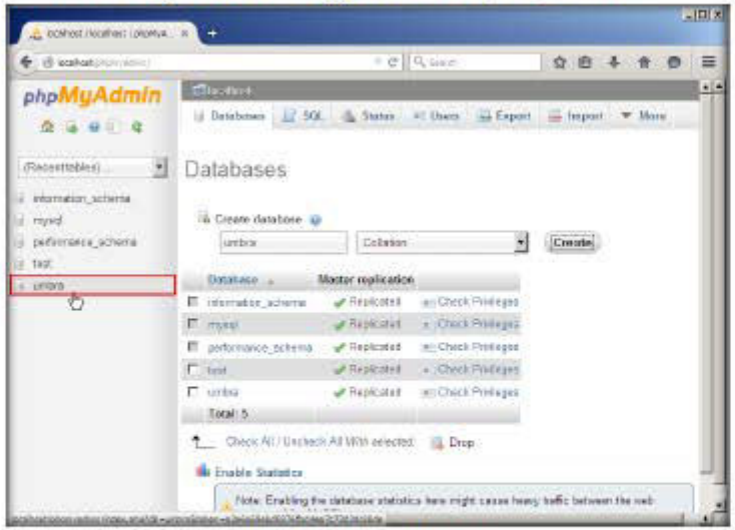


FIGURE 8.9: Assigning User Privileges

12. The umbra database's webpage appears; click **Privileges**.

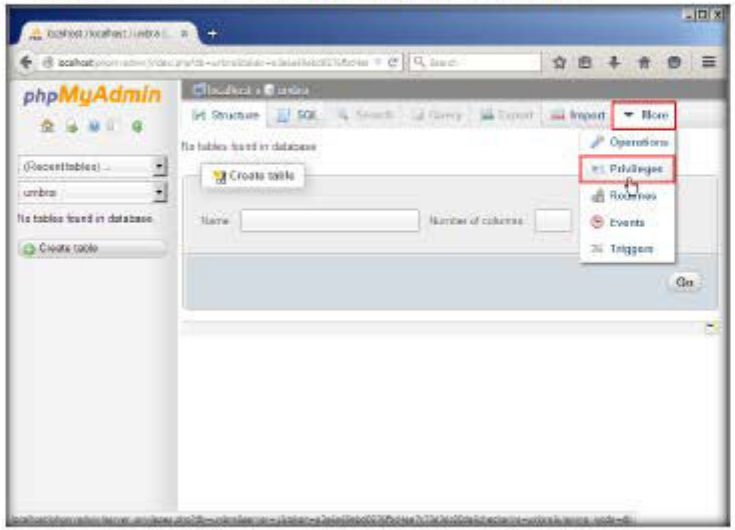


FIGURE 8.10: Assigning User Privileges

13. Here, you will be adding a user to the database. To add, click the **Add user** link.

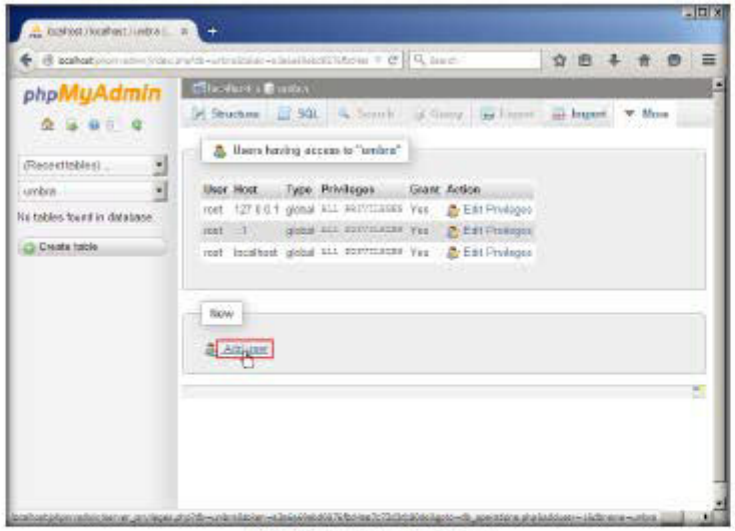


FIGURE 8.11: Assigning User Privileges

14. The **Add user** page appears under **Login Information** section:
    a. Type **umbra** in the **User name** text field.
    b. Select **Local** from the **Host** drop-down list.
    c. Type the password **test@123** in the **Password** and **Re-type** password fields.

    In the **Global privileges** section:

    d. Click the **Check All** link.
15. Click **Add User**.

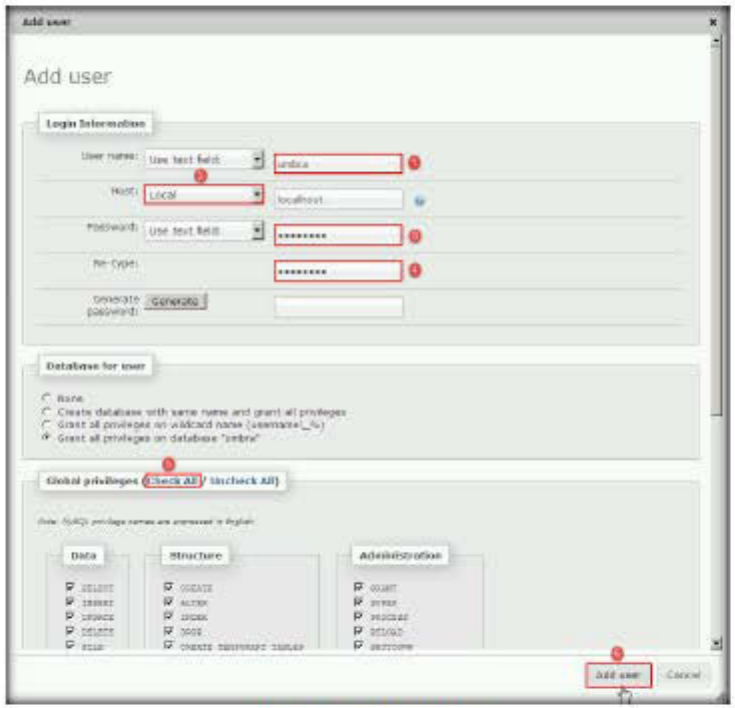


FIGURE 8.12: Assigning User Privileges

16. Minimize the browser, navigate to **C:\wamp\www\umbra\Panel\inc,** and open the **config.php** file in **Notepad++**.

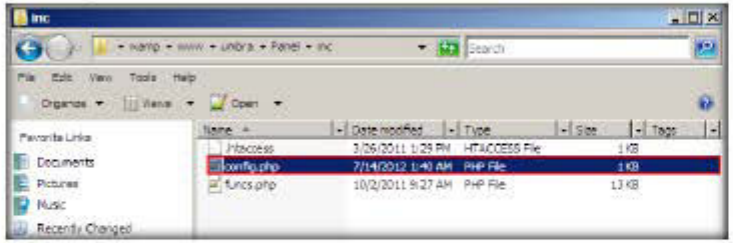


FIGURE 8.13: Opening config.php File

17. The **config.php** file opens in Notepad++. Now:
    a. In **line no. 2**, assign the user name as **admin** in double quotes. This would be the username to log in to umbra loader web application.
    b. In **line no. 3**, assign the password as **password** in double quotes. This would be the password to log in to umbra loader web application.
    c. In **line no. 5**, assign the mysql server host as **localhost** in double quotes.
    d. In **line no. 6**, assign the mysql username as **umbra** in double quotes.
    e. In **line no. 7**, assign the mysql password as **test@123** in double quotes.
    f. In **line no. 8**, assign the mysql database as **umbra** in double quotes.

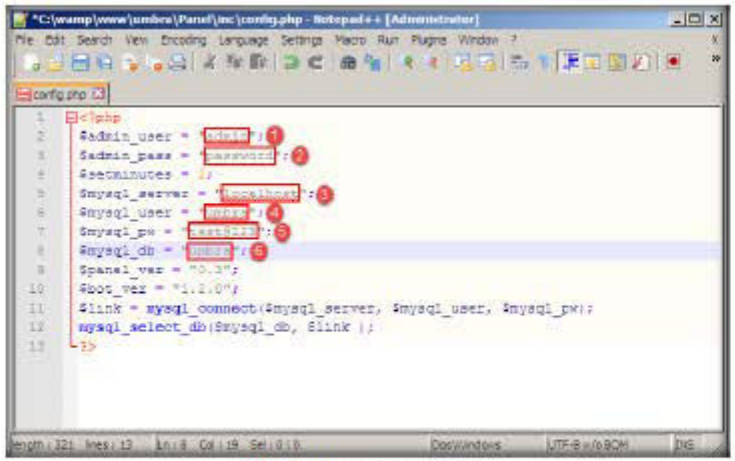


FIGURE 8.14: Editing config.php File

18. Once completed, save the file.

19. Maximize the web browser, open a new tab, type the URL **http://localhost/umbra/panel/install.php** in the address bar, and press **Enter**.
20. Wait for Umbra Loader installation to complete.
21. On completion of installation, the following screenshot is displayed.

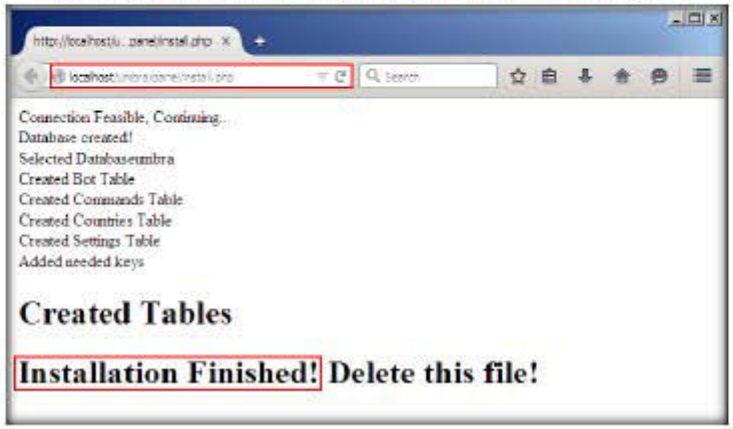


FIGURE 8.15: Installing Umbra Loader

22. Open a new tab, type **http://localhost/umbra/panel** in the address bar, and press **Enter**.

TASK 3

Create a Server

23. The **Login** page appears; type the username **admin**, the password **password**, and click **Login**.

FIGURE 8.16: Logging in to the Web Panel

24. On a successful login, a **Status** pop-up states: "**Login Successful.**" Click **OK**.

FIGURE 8.17: Log in Successful

25. Umbra Loader panel appears, as shown in the screenshot:

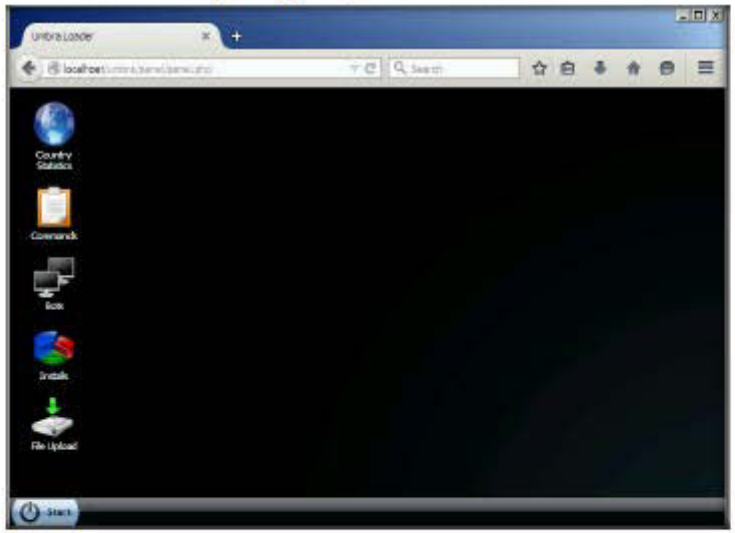


FIGURE 8.18: Umbra Loader Web Panel

26. Here, you will be able to view all the affected machines (bots) along with their statistics. The **command and control center** allows you to execute applications on the bots.

27. Now, we shall create a server using the umbra loader's botnet builder. When a user runs this server, the botnet attains connection to the victim machine and it is updated in the Bots list (in the web panel).
28. Navigate to **Desktop**, go to **Umbra Loader → Bot,** and double-click **Builder.exe**.

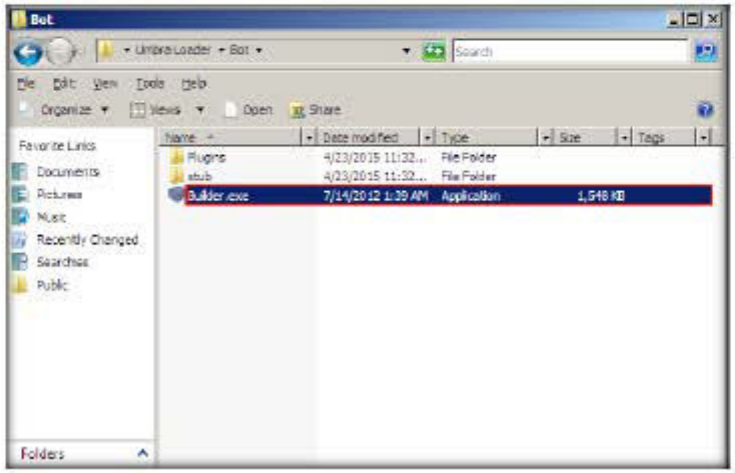


FIGURE 8.19: Loading the Builder

29. The Umbra Loader Builder window appears, displaying the Connection tab by default. In the tab, right-click in the window, and click **Add Host**.

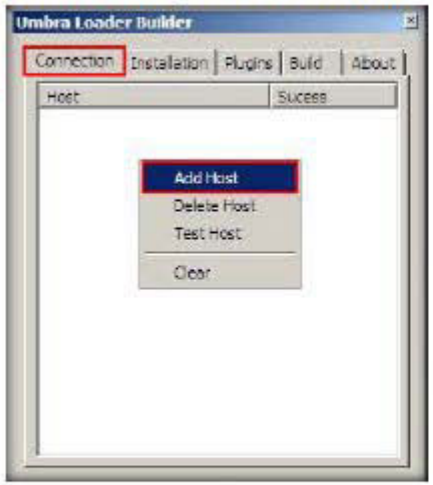


FIGURE 8.20: Adding a Host

30. The **New Host** pop-up appears; enter **http://[IP Address of windows Server 2008]/umbra/panel/bot.php** in the text field, and click **OK**.

Note: In this lab, the IP Address of **Windows Server 2008** is **10.0.0.9,** which might vary in your lab environment.

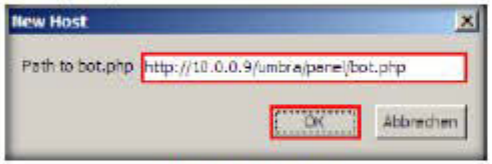


FIGURE 8.21: Adding a Host

31. To test whether the URL can connect successfully to the botnet database (when a victim runs the server being created), right-click on the added host, and click **Test Host**.

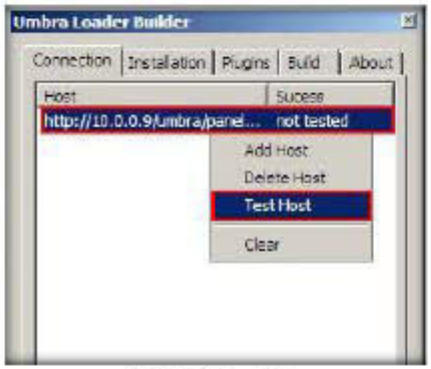


FIGURE 8.22: Testing Host

32. The status should change from **not tested** to **works!** as shown in the screenshot:

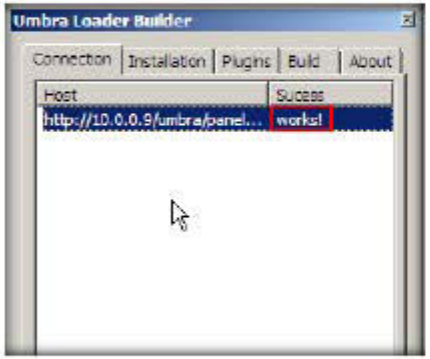


FIGURE 8.23: Test Successful

33. Now, click the Plugins tab, right-click in the window, and click **Add Plugin**.

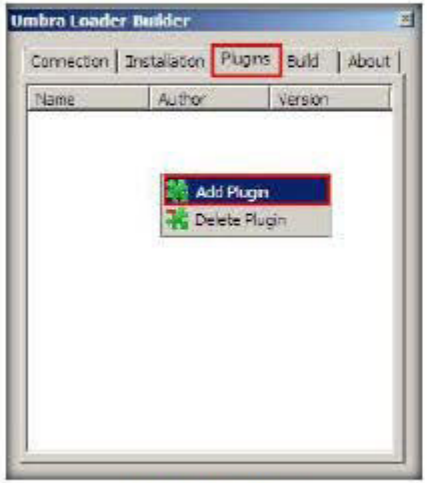


FIGURE 8.24: Adding Plugin

34. The **Open** Window appears; navigate to **Desktop → Umbra Loader → Bot → Plugins**, select **usbspreader.umbplg**, and click **Open**.

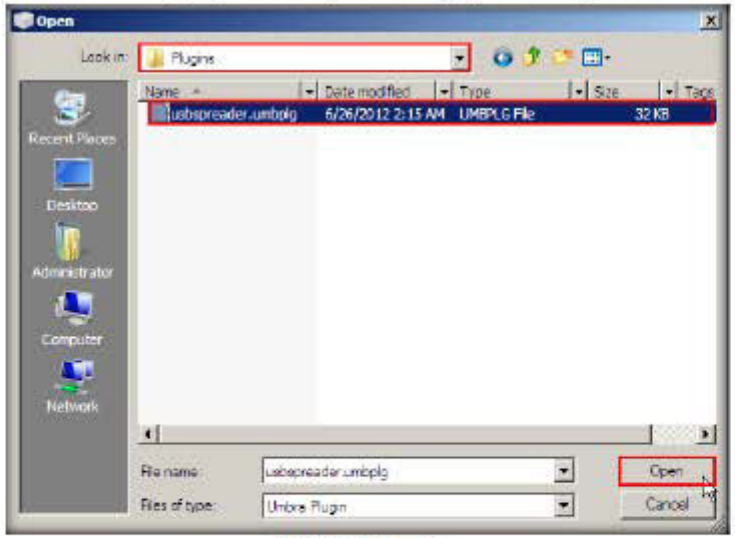


FIGURE 8.25: Adding Plugin

35. In the **Umbra Loader Builder** window, click the **Build** tab, and then click **Build**.

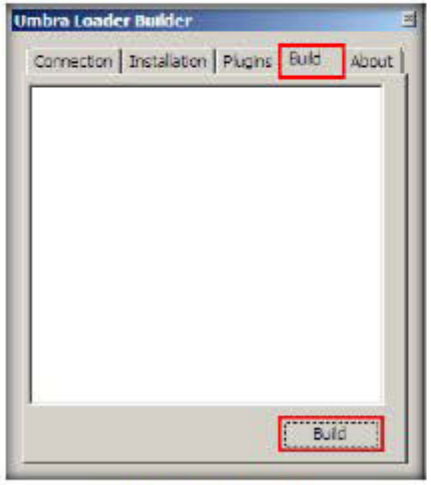


FIGURE 8.26: Building Server

36. This builds the server successfully.

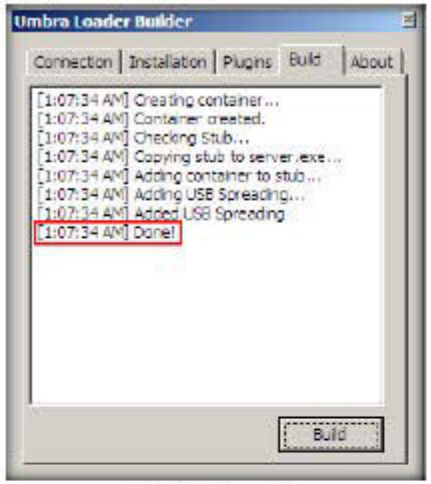


FIGURE 8.27: Server Built

37. Close the Umbra Loader Builder window.

TASK 4

Share the Server

38. The created **server.exe** file is stored in **Desktop → Umbra Loader → Bot**.

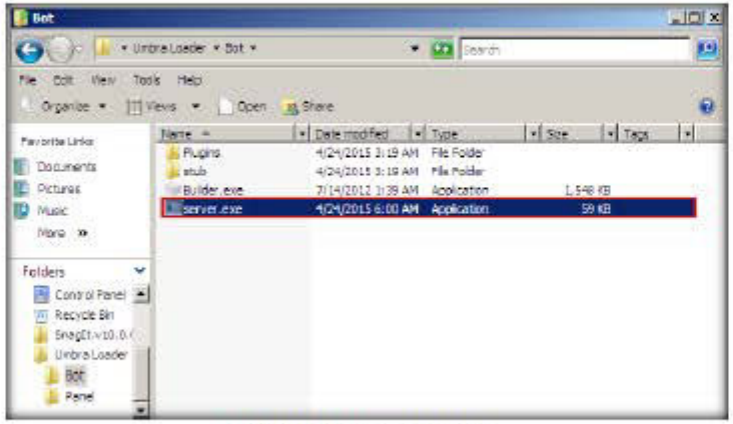


FIGURE 8.28: Viewing the Created Server

39. Now, let us share this file through a shared network drive.

40. So, copy **server.exe** file stored in the location **Desktop → Umbra Loader → Bot** and paste it in **Z:\CEHv9 Module 06 Malware Threats\Botnets\Umbra Loader**.

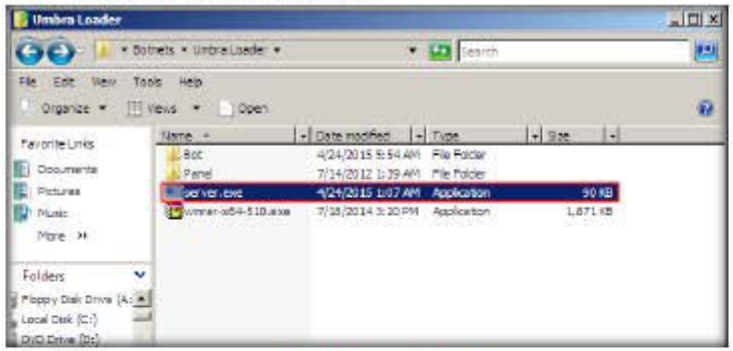


FIGURE 8.29: Sharing the Server

41. Now, log in to **Windows 7** virtual machine (as a victim), navigate to the location **Z:\CEHv9 Module 06 Malware Threats\Botnets\Umbra Loader**, and double-click **server.exe**.

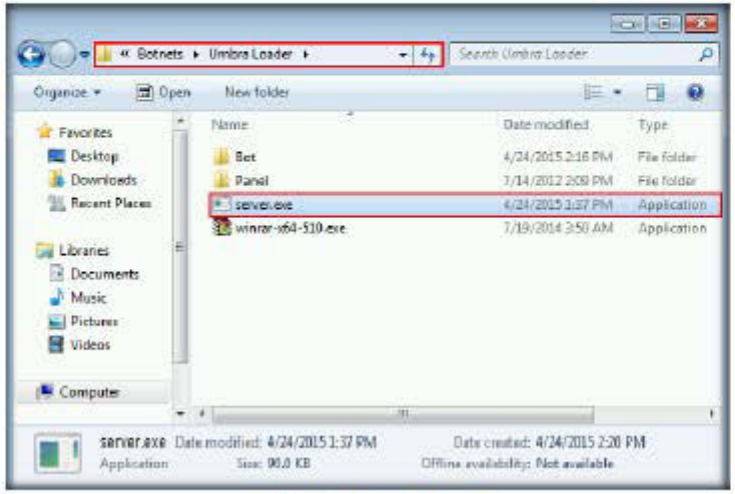


FIGURE 8.30: Executing the Server File

42. If the **Open File - Security Warning** pop-up appears, click **Run**.
43. In the same way, log in to **Windows 8.1** virtual machine (as a victim), navigate to the location **Z:\CEHv9 Module 06 Malware Threats\Botnets\Umbra Loader**, and double-click **server.exe**.
44. If the **User Account Control** pop-up appears, click **Run**.

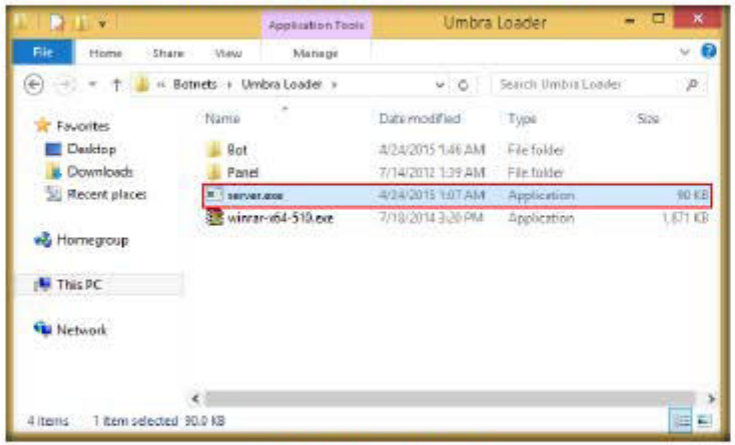


FIGURE 8.31: Executing the Server File

45. Now, these two machines have become victims of the botnet.
46. Switch to the **Windows Server 2008** virtual machine.

TASK 5

Execute Applications on the Bots

47. Maximize the web browser and click **Bots** icon. A **Bots** window appear displaying the added bots as shown in the following screenshot:

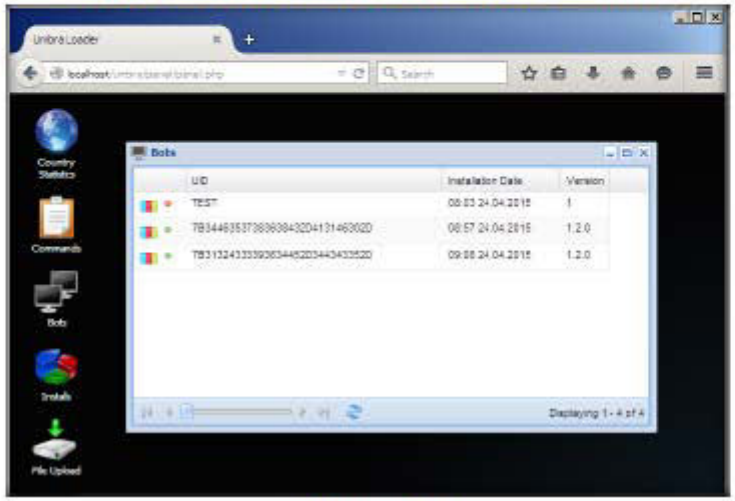


FIGURE 8.32: Viewing Bots

Note: If you do not find the bots, close the window, and re-launch it.

48. Now, you have control over these bots and you can use command and control center of Umbra Loader to execute any application remotely.
49. Let us execute an application for instance. So, to execute an application, we first need to place it in C:\www\umbra\Panel\uploads location.
50. In this lab, we shall be executing WinRAR application. Go to **Desktop → Umbra Loader**, copy **winrar-x64-510.exe,** and place it in **C:\www\umbra\Panel\uploads**.

FIGURE 8.33: Uploading an Application

51. To view the uploaded file, maximize the web browser, type the URL **http://localhost/umbra/Panel/uploads** in the address bar, and press **Enter**.
52. You can view the uploaded file as shown in the following screenshot:

FIGURE 8.34: Application Uploaded

53. Now, let us execute this application on the victim machines (i.e., bots). To execute, switch to the Umbra Loader panel tab and click **Commands** icon.
54. Commands window appears:
    a. Select **Download&Execute** from the **Command** drop-down list.
    b. Type **http://[IP Address of Windows Server 2008]/umbra/panel/uploads/winrar-x64-510.exe** in the **Parameters** field.
    c. Check all the options in the **Countries** drop-down list.
    d. Type **1** in the **Max. Executions** field, and click **Add**.

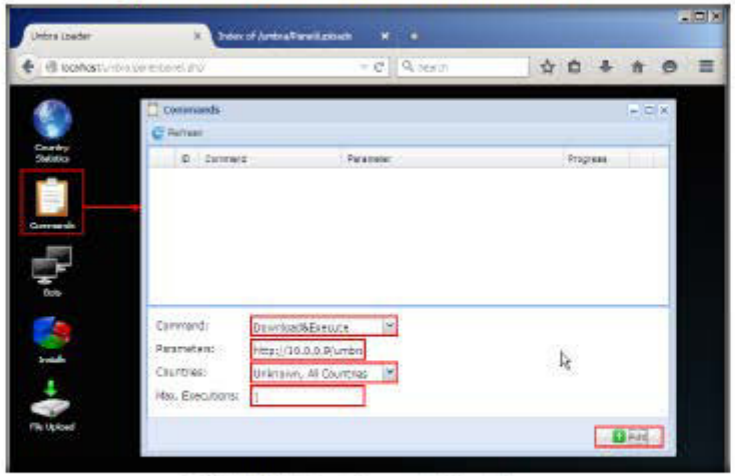


FIGURE 8.35: Configuring Command and Control Center

55. By setting these values, you are about to execute the **winrar-x64-510.exe** file, located in **http://[IP Address of Windows Server 2008]/umbra/panel/uploads/** only once.
56. You may execute the applications ***N*** number of times, where ***N*** is a number you specify in the **Max. Executions** field.
57. Umbra Loader begins to execute the application on the machines and displays the progress. You may click the **Refresh** button to view the updated progress of the command execution.

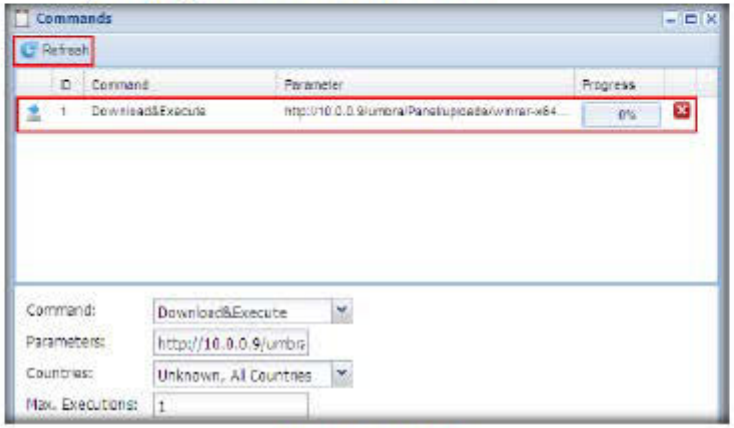


FIGURE 8.36: Viewing the Progress

58. After a while, switch to **Windows 7** machine. You will observe a **User Account Control** pop-up, which infers that the Umbra Loader botnet has successfully attempted to execute the application.

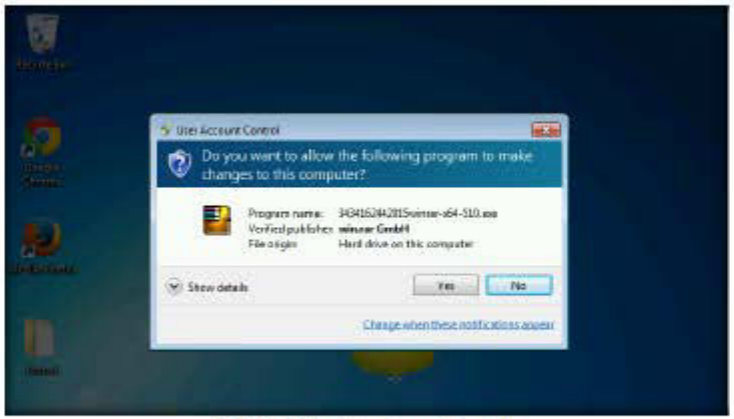


FIGURE 8.37: Application Executed Successfully

59. In the same way, switch to the **Windows 7** machine. You will observe a **User Account Control** pop-up, which infers that the Umbra Loader botnet has successfully attempted to execute the application.

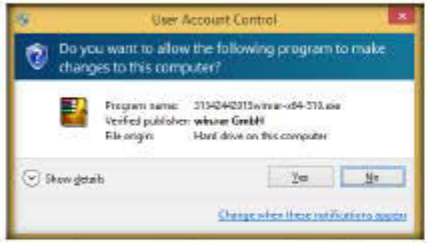


FIGURE 8.38: Application Executed Successfully

60. If you execute an application that can bypass the UAC setting, then the **User Account Control** pop-up does not appear and the application automatically executes.
61. Thus, in real-time, an attacker can execute applications on the affected machines (bots) and might also attempt to perform attacks such as denial of service.
62. On completing the lab, end the **server.exe** process in both **Windows 7** and **Windows 8.1** machines.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 9

Creating a Virus Using the JPS Virus Maker Tool

JPS Virus Maker is a tool to create viruses. It also has a feature for converting a virus into a worm.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Viruses are the scourges of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce itself. Therefore, attackers design every virus code in such a manner that the virus replicates itself *n* number of times, where *n* is a number specified by the attacker.

In recent years, there has been considerable growth in Internet traffic generated by malware. This traffic usually only impinges on the user when either their machine gets infected or, during the epidemic stage of a new worm, when the internet becomes unusable due to overloaded routers. What is less well known is that there is a background level of malware traffic at times of non-epidemic growth, and that anyone connecting an un-firewalled machine into the Internet today will see a steady stream of port scans, back-scatter from attempted distributed denial-of-service attacks, and host scans. Thus, it is necessary to continue to build better firewalls, to protect the Internet router infrastructure and provide early-warning mechanisms for new attacks.

As an ethical hacker and pen-tester, during an audit of a target organization, you have to determine whether viruses and worms can damage or steal the organization's information. You might need to construct viruses and worms, try to inject them into your target network, and check their behavior, whether an anti-virus will detect them, and whether they bypass the firewall.

Lab Objectives

Tools demonstrated in this lab are available in **D:\CEH-Tools\CEHv9 Module 06 Malware Threats**

The objective of this lab is to make students learn and understand how to make viruses and worms.

Lab Environment

To complete this lab, you will need:

- JPS tool located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Virus Maker\JPS Virus Maker**
- A computer running Windows Server 2012 as host machine
- Windows Server 2008 running on virtual machine as guest machine
- Run this tool on Windows Server 2008
- Administrative privileges to run tools

Lab Duration

Time: 5 Minutes

Overview of Virus and Worms

A virus is a self-replicating program that produces its own code by attaching copies of it onto other executable codes. Some viruses affect computers as soon as their codes are executed; others lie dormant until a predetermined logical circumstance is met.

Lab Tasks

TASK 1

Make a Virus

1. Launch **Windows Server 2008** virtual machine.
2. Navigate to **Z:\CEHv9 Module 06 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **jps.exe**.
3. If an **Open File - Security Warning** pop-up appears, click **Run**.
4. If a **Connect to** *** pop-up appears, enter the credentials of the host machine (**Windows Server 2012**) and click **OK**.

5. The **JPS (Virus Maker 3.0)** virus maker main window appears, as shown in the screenshot:

Note: Take a Snapshot of the virtual machine before launching the JPS Virus Maker tool.

The option, Auto Startup is always checked by default and start the virus whenever the system boots on.

FIGURE 9.1: JPS Virus Maker main window

6. The window displays various features/options that can be chosen while creating a virus file.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

7. JPS lists the **Virus Options**; check the **options** that you want to embed in a new virus file.
8. In this lab, the options embedded in the virus file are Disable Yahoo, Disable Internet Explorer, Disable Norton Anti Virus, Disable McAfee Anti Virus, Disable Taskbar, Disable Security Center, Disable Control Panel, Hide Windows Clock, Hide All Tasks in Taskmgr, Change Explorer Caption, Destroy Taskbar, Destroy Offlines (YIMessenger), Destroy Audio Service, Terminate Windows and Auto Startup.

This creation of a virus is only for knowledge purposes, don't misuse this tool.

A list of names for the virus after install is shown in the Name after Install drop-down list.

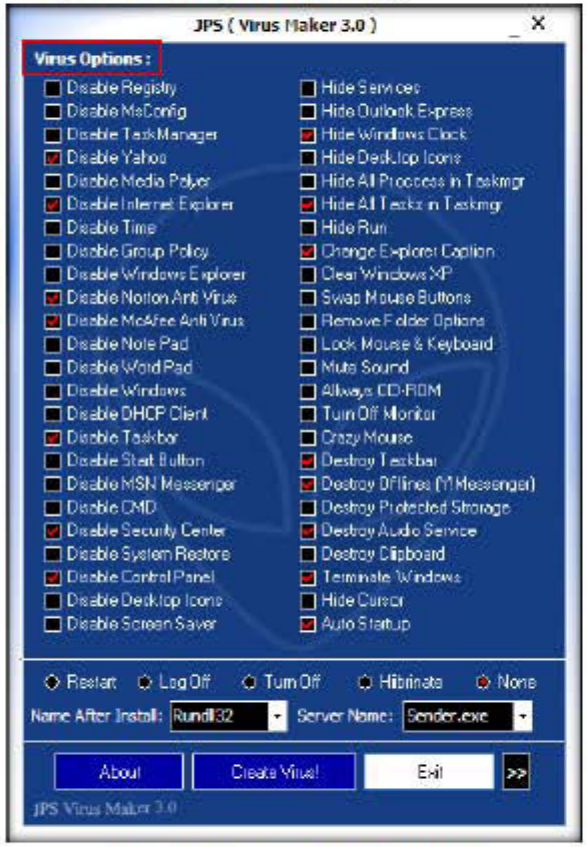


FIGURE 9.2: JPS Virus Maker main window with options selected

9. Click a **radio** button (here, **Restart**) to specify when the virus should **start attacking** the system after its creation.

FIGURE 9.3: JPS Virus Maker main window with Restart selected

A list of server names is present in the Server Name drop-down list. Select any server name.

10. From the **Name after Install** drop-down list, choose the name of the **service** (here, **Rundll32**) you want the virus to mimic.

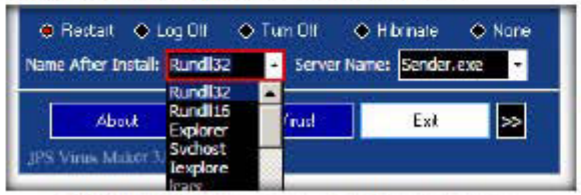


FIGURE 9.4: JPS Virus Maker main window with the Name After Install option

11. Choose a **server** name (here, **Svchost.exe**) for the virus from the **Server Name** drop-down list.

FIGURE 9.5: JPS Virus Maker main window with Server Name option

Don't forget to change the settings for every new virus creation. Otherwise, by default, it takes the same name as an earlier virus.

12. Now, before clicking on **Create Virus!**, click  icon to configure the virus options.

FIGURE 9.6: Configuring the Virus option

TASK 2

Make a Worm

13. A Virus options window appears, as shown in the screenshot:

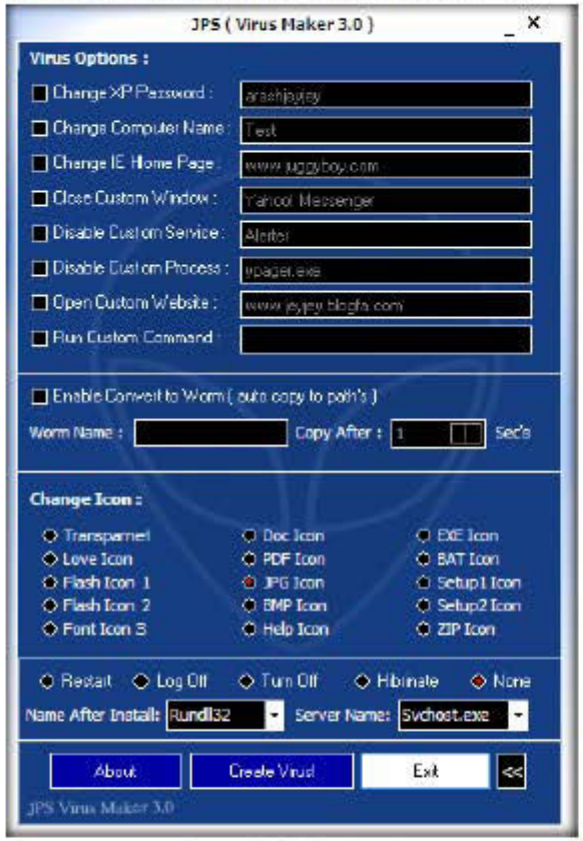


FIGURE 9.7: Configuring the Virus options

Make sure to check all the options and settings before clicking on Create Virus!

14. Check the **Change XP Password** option, and enter a **password** (here, **qwerty**) in the text field. Check **Change Computer Name** option, and type **Test** in the text field. Check **Change IE Home Page** option, and type a **website url** in the text field.
15. You can even configure the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox, and provide a **Worm Name** (here, **fedevi**).
16. For the worm to self-replicate after a particular time period, specify the time (in seconds; here, **1 second**) in the **Copy after** field.

17. Select **JPG Icon** radio button in the **Change Icon** section, and click **Restart** radio button, in the lower part of the window.

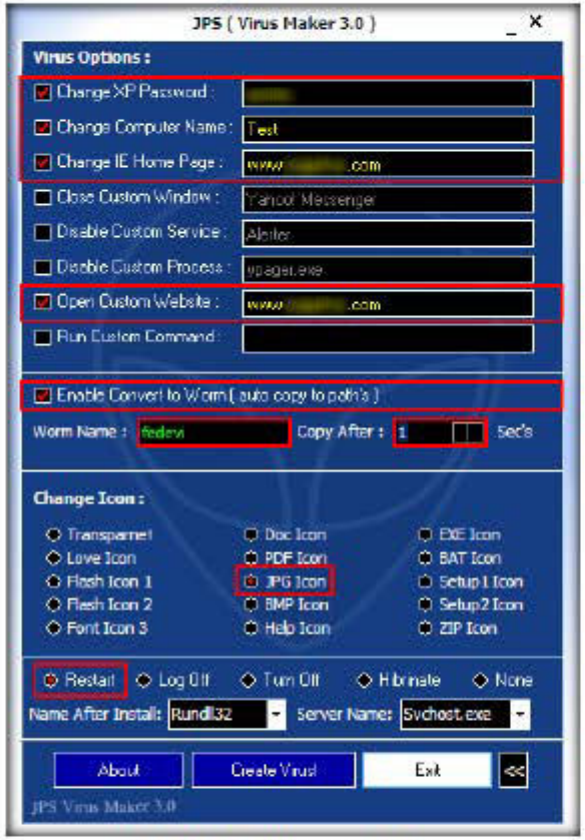


FIGURE 9.8: JPS Virus Maker main window with Options

Features
Change XP Password
Change Computer Name
Change IE Home Page
Close Custom Windows
Disable Custom Service
Disable Process
Open Custom Website
Run Custom Command
Enable Convert To Worm - Auto Copy Server To Active Path With Custom Name & Time
Change Custom Icon For your created Virus (15 Icons)

18. After **completing** your selection of options, click on **Create Virus!**

FIGURE 9.9: JPS Virus Maker Main window with Create Virus! Button

19. A pop-up window states: **Server Created Successfully...** Click **OK**.

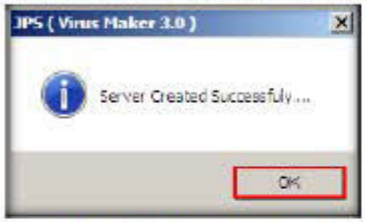


FIGURE 9.10: JPS Virus Maker Server Created successfully message

20. The newly created virus (server) is placed automatically in the **folder** where **jps.exe** is located, but with the name **Svchost.exe**.
21. Now, pack this virus with a **binder** or **virus packager,** and send it to the victim machine through emails, chats, mapped network drives, and so on.

Lab Analysis

Document all the files, created viruses, and worms in a separate location.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 10

Creating a Worm Using Ghost Eye Worm and Maintaining a Persistent Connection Using njRAT

Ghost Eye Worm is a "worm" hacking program that spreads random messages on Facebook, Steam, or chat sites.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Scenario

Worms are self-replicating hacking programs that spread malicious links (that have Trojans/backdoors embedded in them) which, when clicked, download the Trojans and install them on the victims' machines. These Trojans and worms may be crafted in such a way, that even anti-virus and firewalls fail to detect and block them.

As an expert Ethical Hacker or Penetration Tester, you need to ensure that proper security measures are taken to avoid worms and Trojans from entering a network.

Lab Objectives

The objective of this lab is to make students learn how to configure a worm, embed a Trojan in it and spread it through social Networking websites.

Lab Environment

To carry out this lab, you will need:

- Ghost Eye Worm located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Worm Maker\Ghost Eye Worm**
- A computer running Windows Server 2012 as host machine
- A computer running Windows 8.1 virtual machine as attacker machine
- A computer running Windows 7 virtual machine as victim machine

- A computer running Windows Server 2008 virtual machine as victim machine
- Administrative privileges to run tools

Lab Duration

Time: 30 Minutes

Overview of Worms

Computer worms are malicious programs that replicate, execute, and spread across the network connections independently without human interaction.

Lab Tasks

TASK 1

Create and Configure a Worm

1. Before running this lab, you need to log in to Windows 8.1 and Windows 7 virtual machines.
2. Ensure that you have an active **Dropbox** account. If you don't have, create one.
3. Navigate to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.

Note: Take a Snapshot of the virtual machine before launching the Ghost Eye Worm tool.

4. Double click on **njRAT v0.7d.exe** to launch the RAT.
5. If the **Open File - Security Warning** pop-up appears, click **Run**.
6. The njRAT GUI appears along with an **njRAT** pop-up where you need to mention the port you want to use in order to interact with the victim machine. Enter the port number and click **Start**.
7. In this lab, default port number **5552** has been chosen.

FIGURE 10.1: njRAT GUI

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

8. The njRAT GUI appears, click **Builder** link located at the lower left corner of the GUI.

FIGURE 10.2: Building a server

9. The **Builder** dialog-box appears; enter the IP address of **Windows 8.1** (attacker machine) virtual machine, check the options **Copy To StartUp** and **Registry StartUp,** and click **Build**.

Note: In this lab, the IP address of the **Windows 8.1** virtual machine is **10.0.0.4**, which might vary in your lab environment.

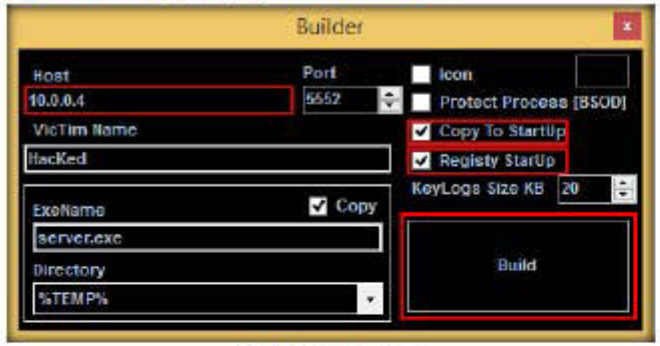


FIGURE 10.3: Building a server

10. The **Save As** dialog-box appears; specify a location to store the server, rename it, and click **Save**.
11. In this lab, the destination location chosen is **Desktop** and the file is named **Test.exe**.

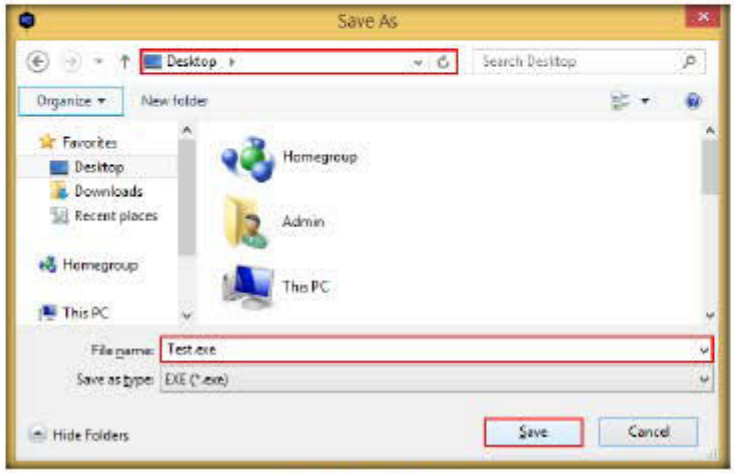


FIGURE 10.4: Building a server

12. Once the server is created, the **DONE!** pop-up appears; click **OK**.

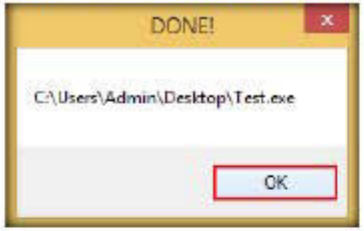


FIGURE 10.5: Server built successfully

Note: Leave **njRAT** running throughout this lab.

13. To make the trojan undetectable, you need to crypt it.

TASK 2

Crypt Trojan Using SwayzCryptor

14. Navigate to **Z:\CEHv9 Module 06 Malware Threats\Crypters\SwayzCryptor**, and double-click **SwayzCryptor.exe**.
15. **SwayzCryptor** GUI appears, click [...], below **File,** to select the Trojan file:

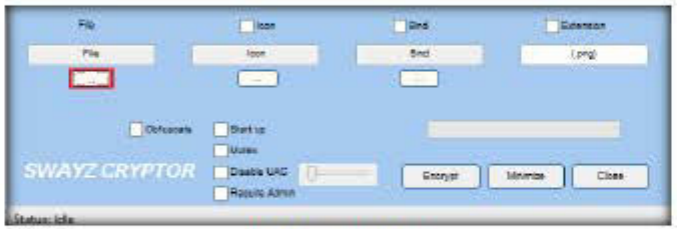


FIGURE 10.6: Selecting a File

16. The **Select a File** dialog-box appears; navigate to the location of **Test.exe** (**Desktop**), select it, and click **Open**.

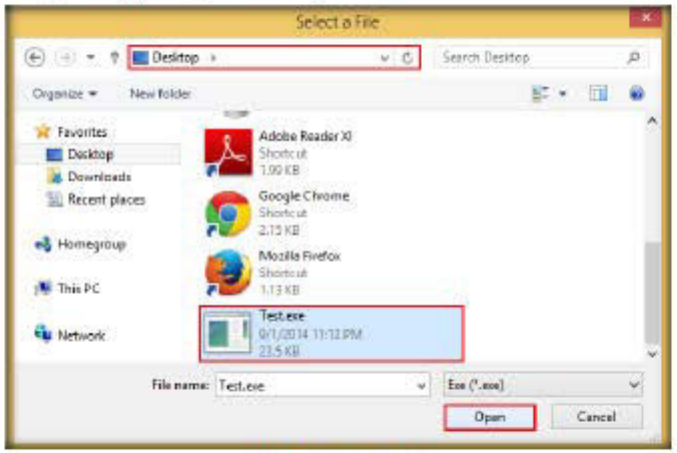


FIGURE 10.7: Selecting a File

17. Once the file is selected, check the options **Start up**, **Mutex,** and **Disable UAC;** then click **Encrypt**.

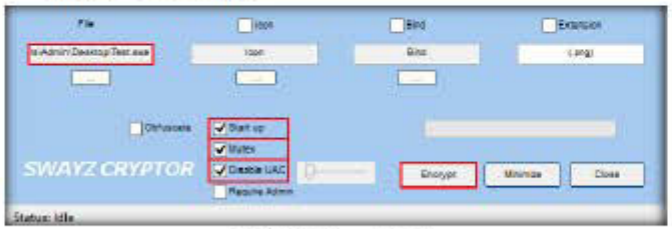


FIGURE 10.8: Encrypting the File

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

18. The **Save File** dialog-box appears; select a location where you want to store the crypted file (here, **Desktop**), leave the file name set to default (**CryptedFile**), and click **Save**.

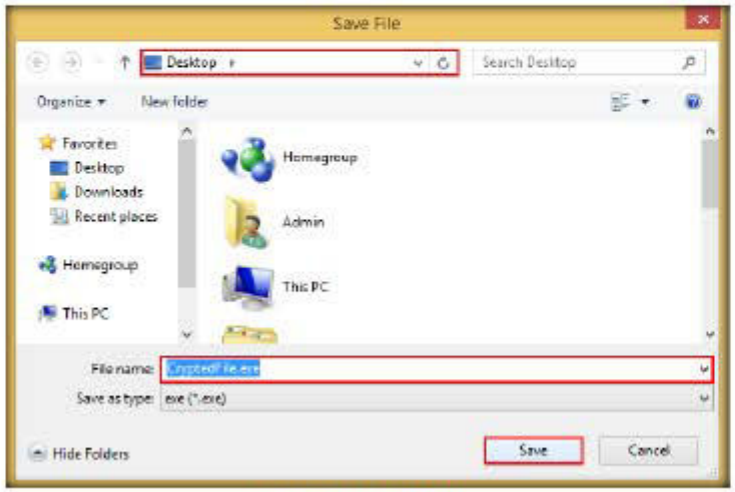


FIGURE 10.9: Encrypting the File

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

19. Once the encryption is finished, click **Close**.

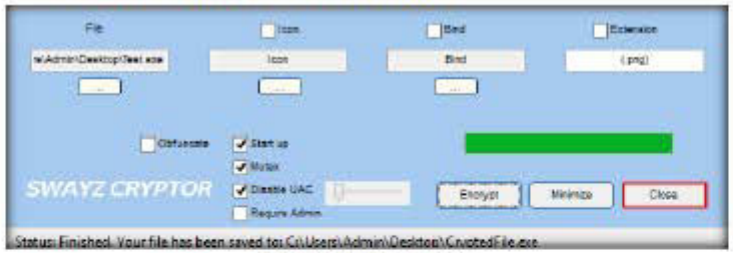


FIGURE 10.10: Exiting the application

TASK 3

Upload the File to Dropbox

20. Log into your Dropbox account, drag **CryptedFile.exe** (located on the **Desktop**) onto the Dropbox webpage.

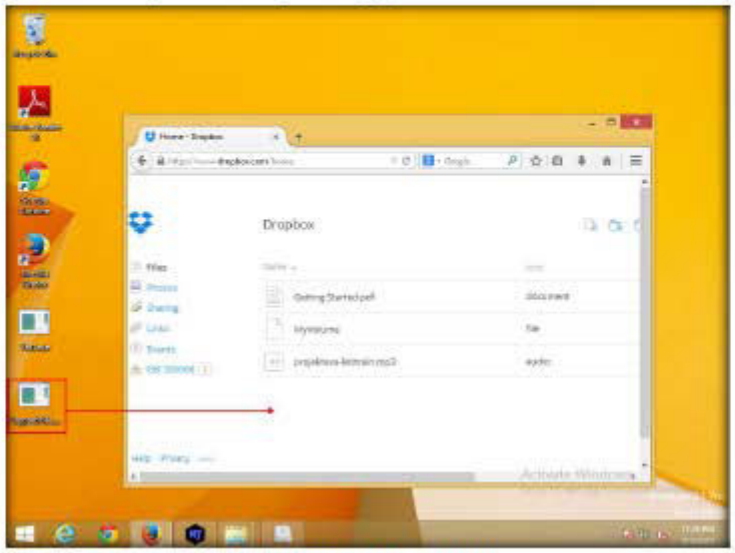


FIGURE 10.11: Dropping the Crypted file into Dropbox

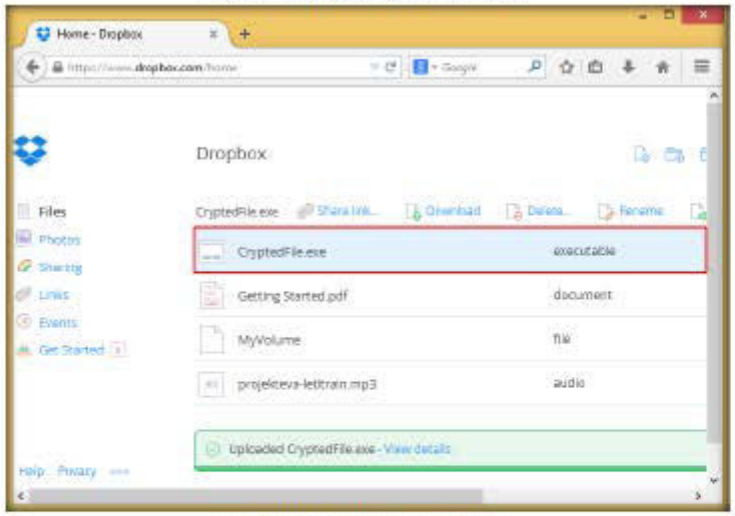


FIGURE 10.12: Crypted File dropped into Dropbox

21. Click on the uploaded **CryptedFile.exe** link.

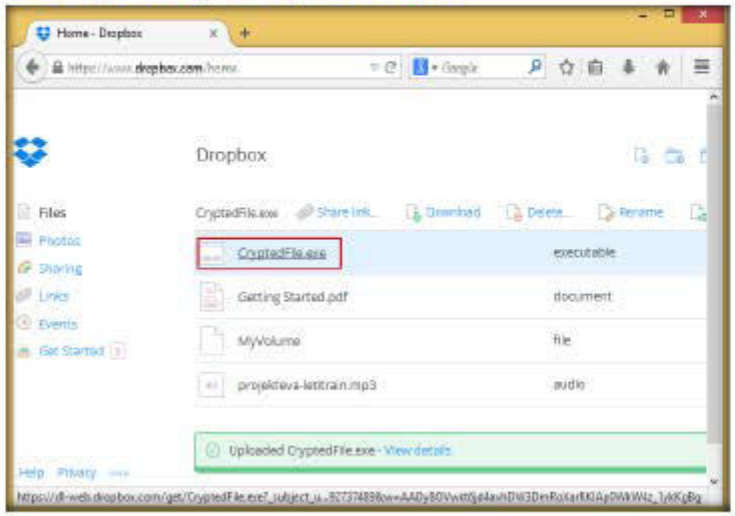


FIGURE 10.13 Crypted File dropped into Dropbox

22. The **CryptedFile.exe** pop-up appears on the webpage; click **Share**.

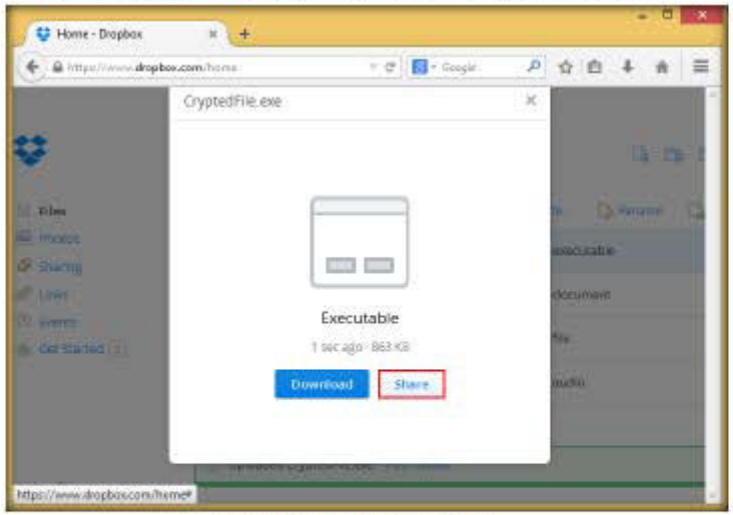


FIGURE 10.14 Crypted File dropped into Dropbox

23. The **Share link to 'CryptedFile.exe'** pop-up appears; copy the link and make a note of it.

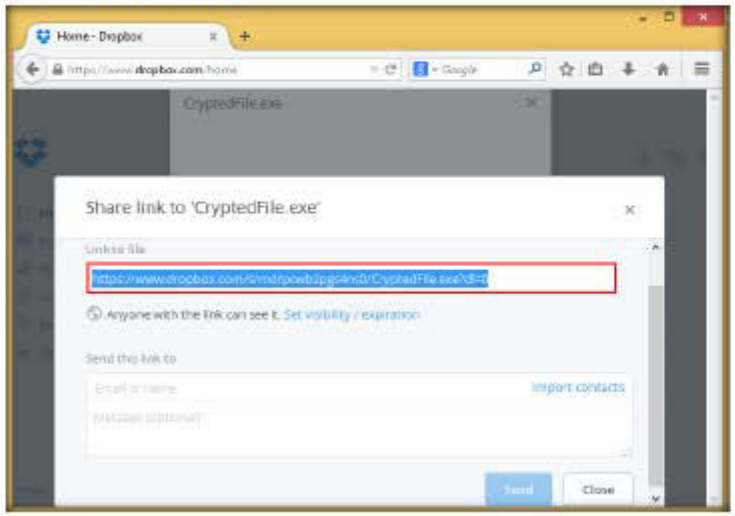


FIGURE 10.15: Dropbox link associated with the Crypted file

TASK 4

Launch and Configure Ghost Eye Worm

24. Navigate to **Z:\CEHv9 Module 06 Malware Threats\Worm Maker\Ghost Eye Worm** on the **Windows 8.1** virtual machine, and double-click **Ghost Eye Worm.exe**.
25. The **Ghost Eye - Worm** pop-up appears; click **OK**.

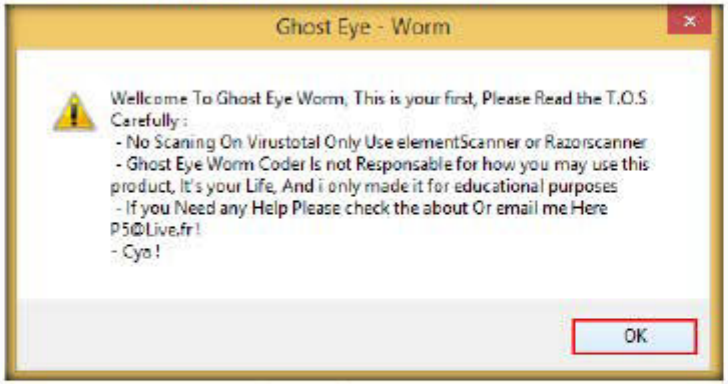


FIGURE 10.16: Ghost Eye - Worm pop-up

26. The **Ghost Eye - Worm** dialog - box appears; enter **Ghosteyeismael** in the **Password** field, and then click **Browse**.

FIGURE 10.17: Browsing the stub

27. The **Open** dialog - box appears; navigate to **Z:\CEHv9 Module 06 Malware Threats\Worm Maker\Ghost Eye Worm**, select **Stub.exe**, and click **Open**.

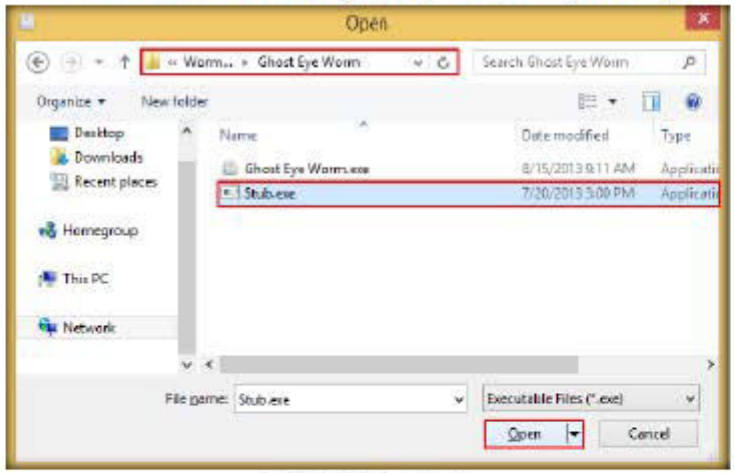


FIGURE 10.18: Browsing the stub

28. Wait 15 to 20 seconds, after which the **Ghost Eye Worm** pop-up appears; click **OK**.

29. The **Ghost Eye - Worm** GUI appears, as shown in the screenshot:

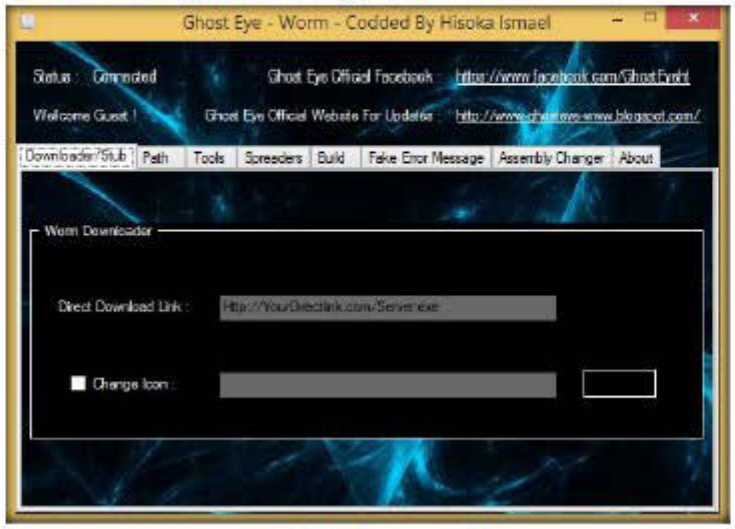


FIGURE 10.19: Ghost Eye - Worm GUI

30. Paste the link you copied from Dropbox into the **Direct Download Link** field, and replace **www** with **dl**, so that the **CryptedFile.exe** file is downloaded directly onto the victim machine when the worm is executed.

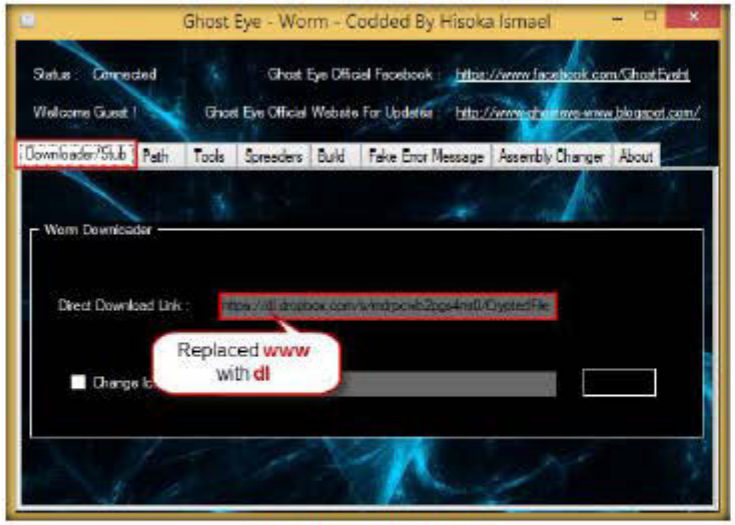


FIGURE 10.20: Replacing www with dl

31. Click the **Path** tab. Name the server as **Windows** (or other name), and choose the extension **.exe**.
32. Click the **%temp%** radio button to set the path of the server file (**Windows.exe**) to the **Temp** folder.

FIGURE 10.21: Setting the path of the file to temp folder

33. Click the **Spreaders** tab.
34. Check **Steam/Facebook/Skype/Chatwebsites,** and write a description, followed by the direct download link of the Trojan file **CryptedFile.exe,** shown in **step 30** (**https://dl.dropbox.com/...**).

    The reason for the direct download link here is that, when a victim executes the worm, it starts spreading the link (mentioned in this field) on the Internet. When a general user clicks the link, the trojan file (**CryptedFile.exe**) runs on that machine, and njRAT establishes a connection with that user.
35. Check **Notify Me By email For Each Successfully Installed Server.**
36. Enter your **email ID** in the email field, followed by its respective password in the **Password** field. Enter the **Subject** as **Victim Trapped**.

37. Whenever a victim runs the worm, you receive a notification to your mail ID with the subject **Victim Trapped**.

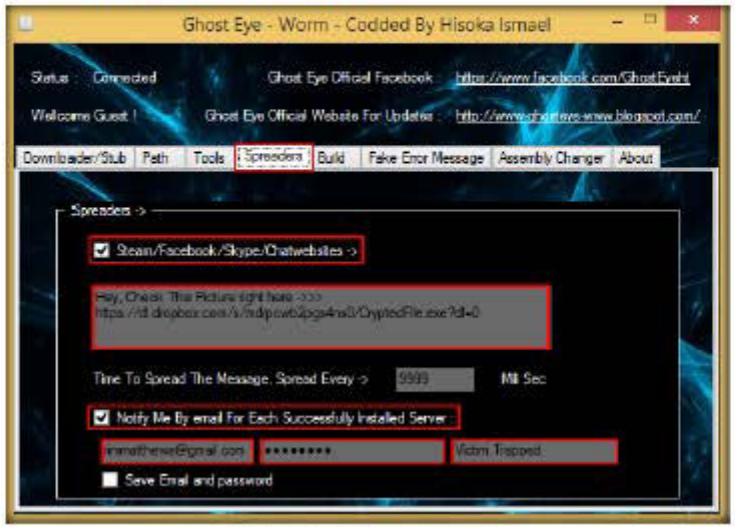


FIGURE 10.22: Configuring the Spreaders tab

38. Click the **Fake Error Message** tab, check **Enable Fake Error Message** option, enter **Alert!!** (or anything of your choice) in the **Fake Title** field, and type the message **You are my Victim!!!** (or similar) in the **Message Here ....** field.
39. Click **Exclamation**.

40. This displays an exclamation on the victim machine's screen when the worm runs.

FIGURE 10.23: Setting a Fake Error Message

41. Click the **Assembly Changer** tab, check **Change Assembly** option, and click **Generate** button twice or thrice.

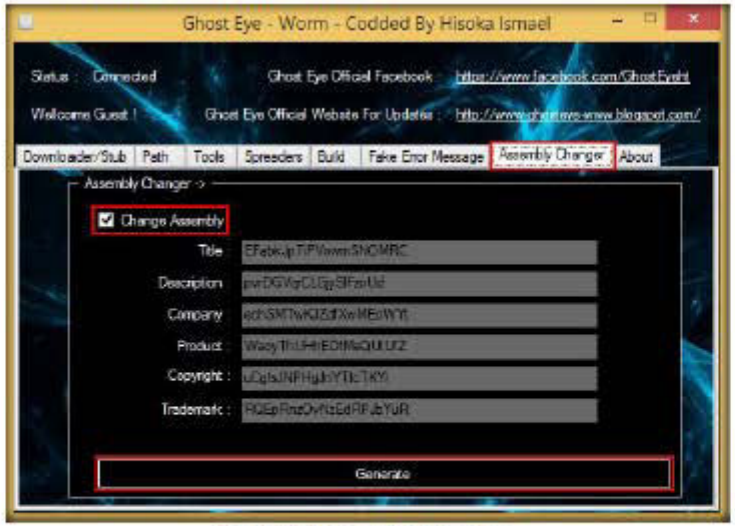


FIGURE 10.24: Configuring the Assembly Changer

42. Click the **Build** tab, and click **Build**.

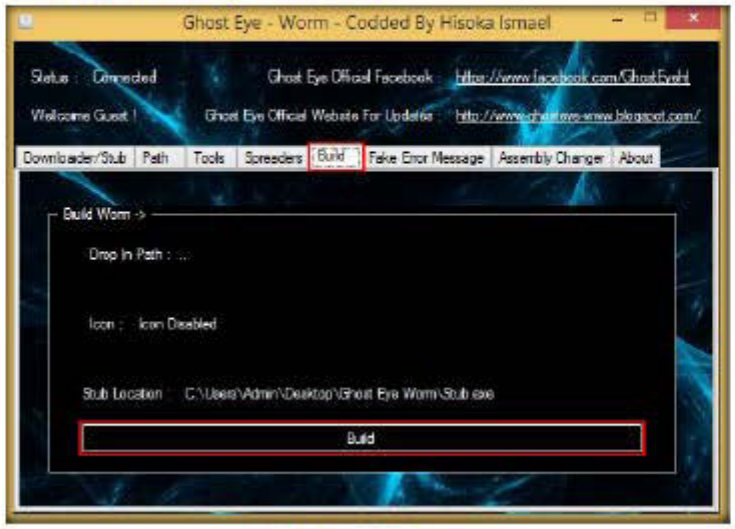


FIGURE 10.25: Building the Worm

43. The **Save As** dialog-box appears; select the destination location (here, **Desktop**) in which you want to save the generated worm, name it **worm** (or similar), and click **Save**.

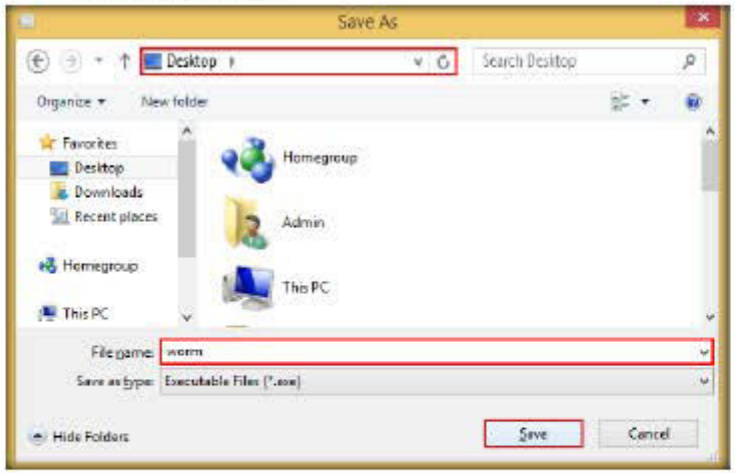


FIGURE 10.26: Saving the Worm

TASK 5

Crypt the worm Using SwayzCryptor

44. Once the worm is created, the **Ghost Eye - Worm** pop-up appears, stating that the worm has been built successfully. Click **OK**.
45. Navigate to **Z:\CEHv9 Module 06 Malware Threats\Crypters\SwayzCryptor**, and double-click **SwayzCryptor.exe**.
46. **SwayzCryptor** GUI appears, click [...], under **File,** to select the Trojan file:

FIGURE 10.27: Saving the Worm

47. The **Select a File** dialog-box appears; navigate to **worm.exe** (**Desktop**), select it, and click **Open**.

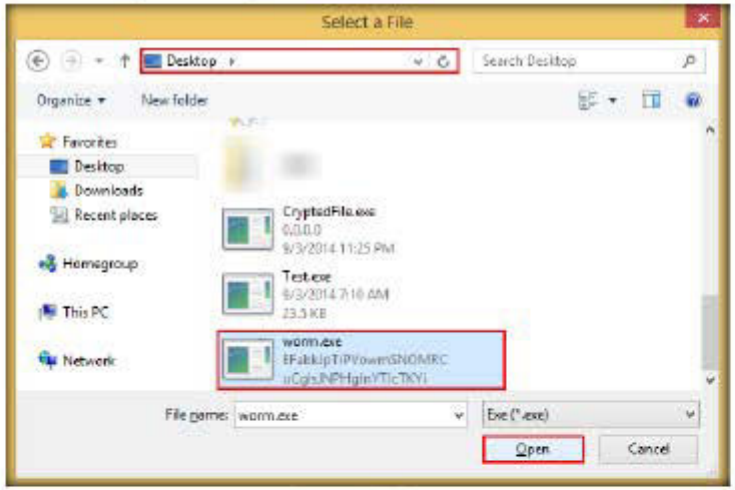


FIGURE 10.28: Saving the Worm

48. Once the file is selected, check the options **Start up**, **Mutex,** and **Disable UAC;** then click **Encrypt**.

FIGURE 10.29: Crypting the Worm

49. The **Save File** dialog-box appears; select a location where you want to store the crypted file (here, **Desktop**), name the file as **Crypted Worm** and click **Save**.

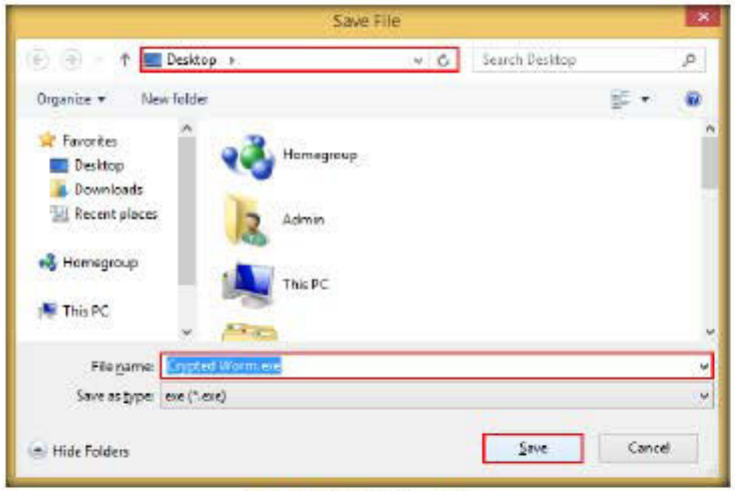


FIGURE 10.30: Saving the Crypted Worm

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

50. Once the encryption is finished, click **Close**.

FIGURE 10.31: Exiting the SwayzCryptor Application

51. Send this Crypted Worm to the intended victim through mail, a shared network drive, or any other means.
52. In this lab, you will be using shared network drive to download the crypted worm.
53. To share the file through shared network drive, you need to copy the **Crypted Worm.exe** file on the **Desktop** to **Z:\CEHv9 Module 06 Malware Threats\Worm Maker\Ghost Eye Worm**.

FIGURE 10.32: Crypted Worm saved to Desktop

54. Assume that you are the victim and you are logged into the **Windows 7** virtual machine.

55. Click **Checkpoint** in the Hyper-V toolbar to create a checkpoint, so that when the machine gets affected by the worm, you can restore this checkpoint and return to the previous working state, before the worm was executed.

FIGURE 10.33: Creating a checkpoint

56. The **Checkpoint Name** dialog-box appears; specify a name (here, **Check 1**), and click **Yes**.

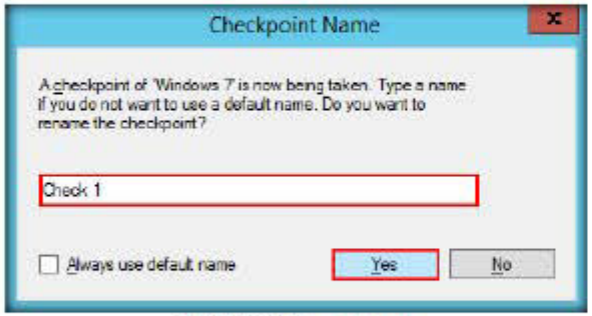


FIGURE 10.34: Naming the checkpoint

57. Log into a social networking website such as **Facebook,** and minimize the window.

Note: In this lab, you need two Facebook accounts, one yours, and one a dummy account. Create a dummy account and add it as a "friend" in the current account (yours).

Note: Do not use the account of a legitimate account holder.

Delete the dummy account after performing this lab.

FIGURE 10.35: Logging in to Facebook

58. Because we will be using shared network drive to download the worm, navigate to **Z:\CEHv9 Module 06 Malware Threats\Worm Maker\Ghost Eye Worm**, copy **Crypted Worm.exe** file from the location, and save it to the Windows 7 machine's **Desktop**.

59. Double-click **Crypted Worm.exe** file.

FIGURE 10.36: Naming the checkpoint

60. As soon as you double-click the **Crypted worm.exe** file, the worm activates and an **Alert!!** pop-up appears, stating **You are my Victim!!!**. Click **OK**.

FIGURE 10.37: Alert! pop-up

61. Switch to the **Windows 8.1** virtual machine, and log into your mail account, whose email ID and password were provided in Ghost Eye Worm during the worm's creation.

62. You will observe an email in the inbox, with the subject **Victim Trapped**:

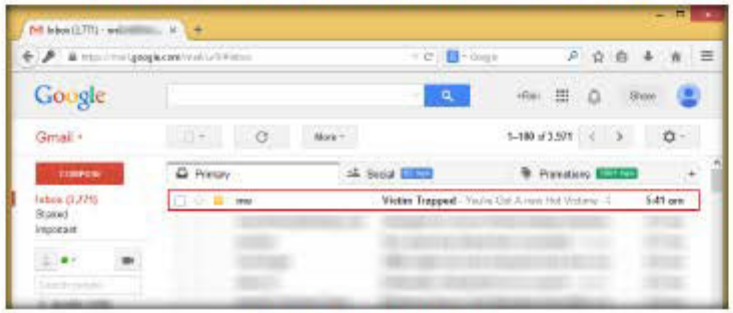


FIGURE 10.38: Mail received in inbox

63. When you open the mail, you will observe the details of victim machine, such as computer name, operating system, IP address and so on, as shown in the screenshot:

FIGURE 10.39: Mail containing the victim's information

64. Maximize the njRAT GUI. Observe that the njRAT client (njRAT GUI) running in Windows 8.1 establishes a persistent connection with the victim machine, as shown in the screenshot.

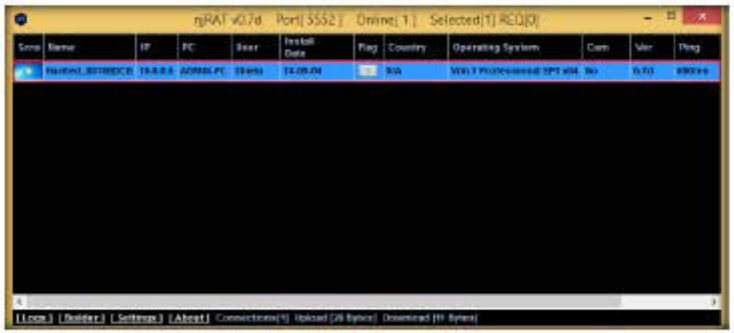


FIGURE 10.40: Connection established

65. Unless the attacker working on the Windows 8.1 machine disconnects the server on his own, the victim machine remains under his/her control.
66. The GUI displays the machine's basic details such as the IP address, User name, Type of Operating system, and so on.
67. Now, you can use njRAT to monitor keystrokes, establish remote desktop connection, and so on.
68. Switch back to the **Windows 7** virtual machine as a victim (here, you), maximize **Facebook** window, open chat list, select the dummy account, type a random message, and press **Enter**.

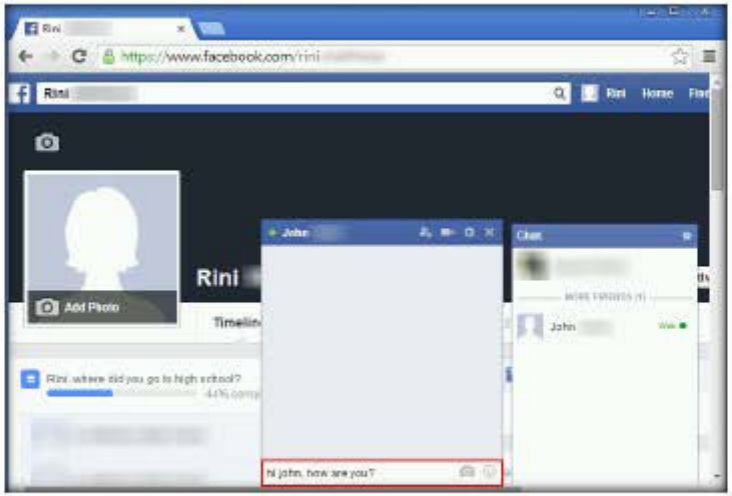


FIGURE 10.41: Entering a chat message

69. As soon as you press **Enter**, the spreader message is automatically entered into the chat box, and a **Security Check** dialog-box appears over the **Facebook** webpage. Type the correct **CAPTCHA** in the text box, and click **Submit**.

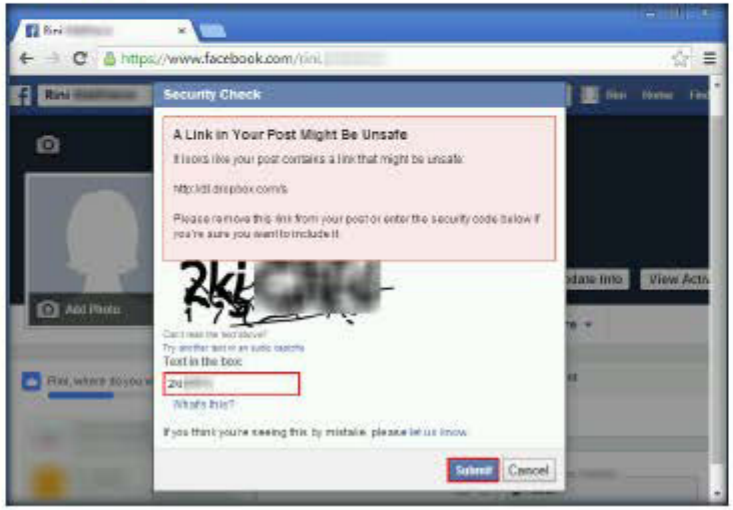


FIGURE 10.42: Entering the CAPTCHA

70. The spreader message is successfully posted in the chat box, as shown in the screenshot:

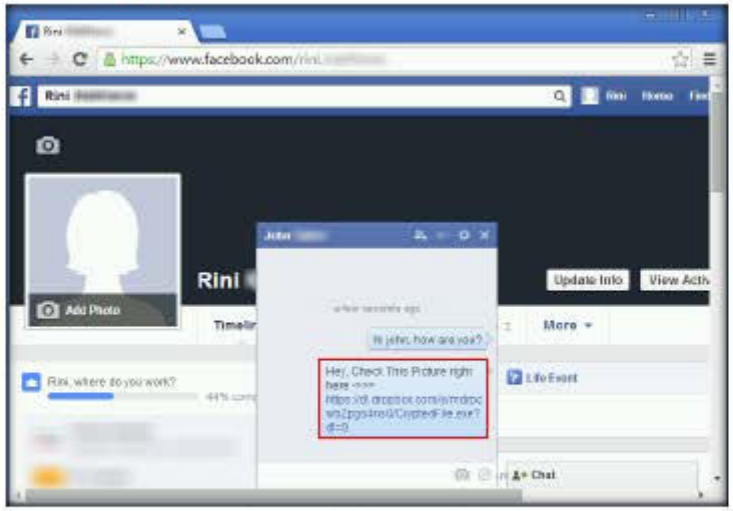


FIGURE 10.43: Spreader message posted in chat

Note: The spreader message gets activated whenever/wherever you press **Enter**, irrespective of the window on which you are navigating.

71. Now, log into the **Windows Server 2008** virtual machine as a general user, and follow **steps 55** and **56** to create a checkpoint.

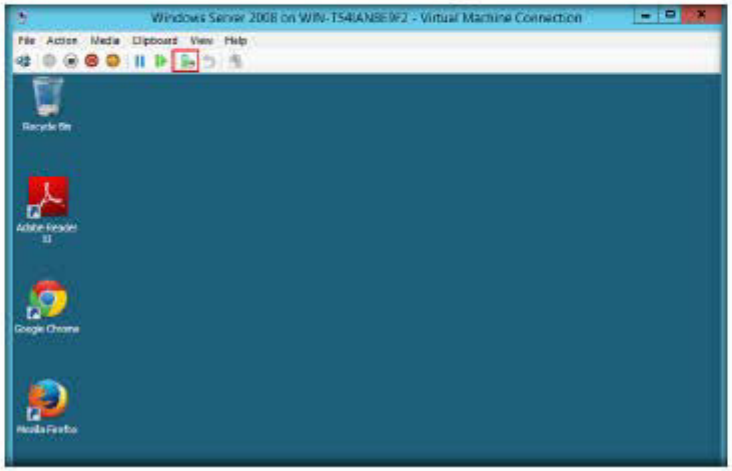


FIGURE 10.44: Creating a snapshot

72. Launch the Firefox web browser, and sign into **Facebook** with the recently created dummy account.

FIGURE 10.45: Logging in to Facebook

73. Click the **Messages** icon, and then click the **Inbox message** that you received from the victim's account (here, you).

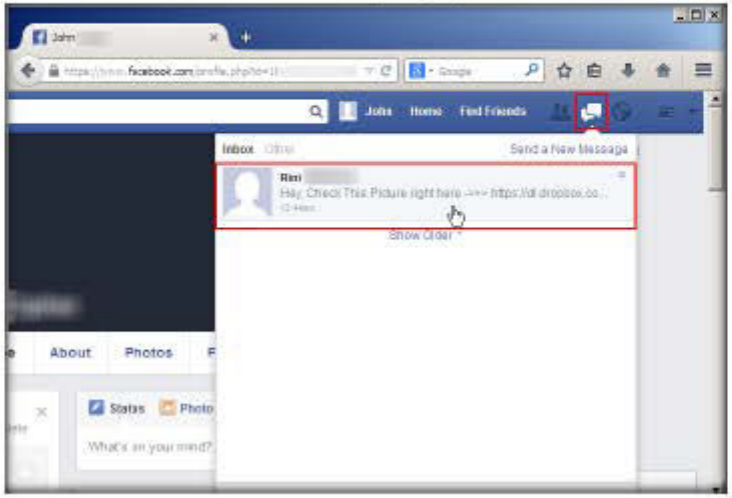


FIGURE 10.46: Opening the message

74. In real time, a general user holding an account in Facebook clicks the link sent by the victim. Here, you are only acting as the general user as well as the victim.

75. Chat box appears; click the Dropbox download link.

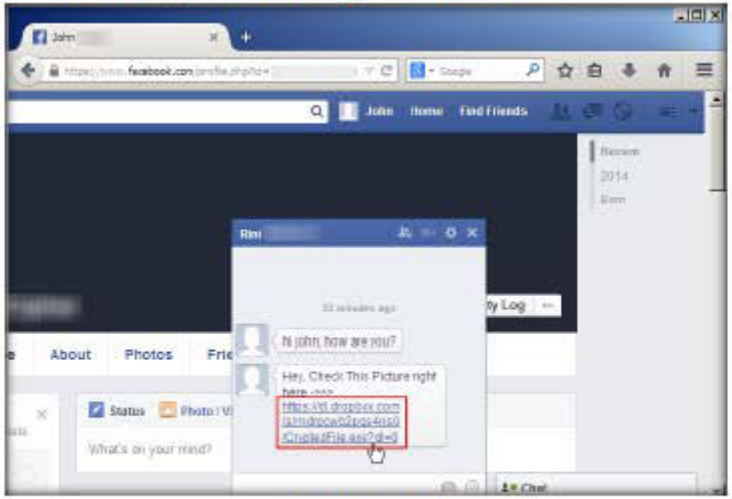


FIGURE 10.47: Clicking the link

76. **Opening CryptedFile.exe** pop-up appears; click **Save File**.

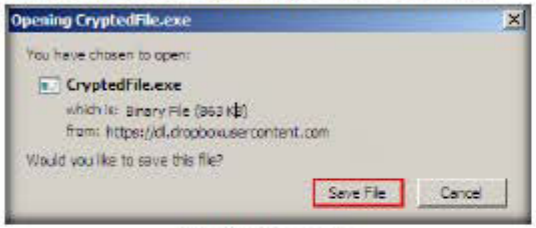


FIGURE 10.48: Saving the file

77. Click the **download** icon (down-arrow) on the top-right corner of the browser window, and then click on **CryptedFile.exe**.
78. If the **Open File - Security Warning** pop-up appears, click **Run**.
79. In real time, attackers create Trojan files in jpg or other format as the victim becomes alert seeing the file (trojan) in exe format. Because this is just a demonstration of the attack, we are creating Trojan directly in .exe format.

FIGURE 10.49: Executing the file

80. As soon as the file (trojan) is executed, the njRAT client establishes a connection with the Windows Server 2008 machine, and the user working on this machine has become a victim.
81. Switch to the Windows 8.1 virtual machine. You will be able to see a connection being established on njRAT, as shown in the screenshot.

FIGURE 10.50: Connection established

82. This way, when a person receives a spreader message from the first victim who is affected by the worm, and he/she downloads and installs the file, the njRAT client running on the attacker's machine establishes a connection, and the attacker will be able to remotely access the client machine.
83. Now, switch to the **Windows 7** virtual machine.
84. Click **Revert** on the toolbar.

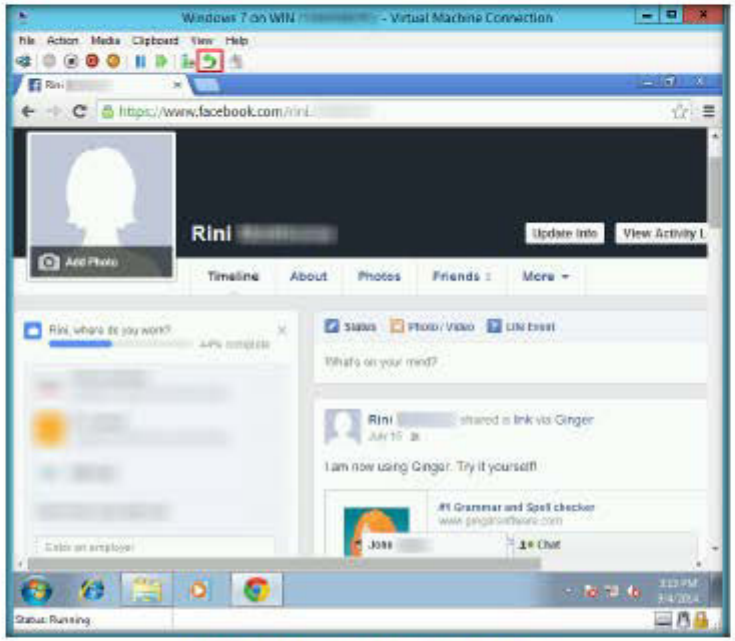


FIGURE 10.51: Reverting back to the previous checkpoint

85. The **Revert Virtual Machine** dialog-box appears; click **Revert**.

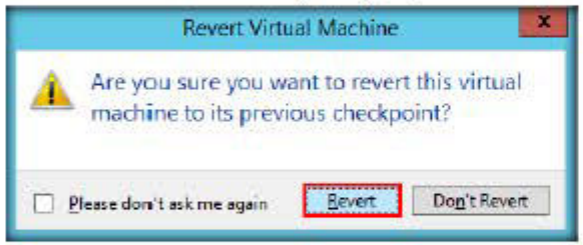


FIGURE 10.52: Reverting back to the previous checkpoint

86. You will be reverted to the previous checkpoint, as shown in the screenshot:

FIGURE 10.53: Checkpoint reverted back

87. In the same way, follow **steps 84** and **85** to revert **Windows Server 2008** virtual machine to its previous checkpoint.

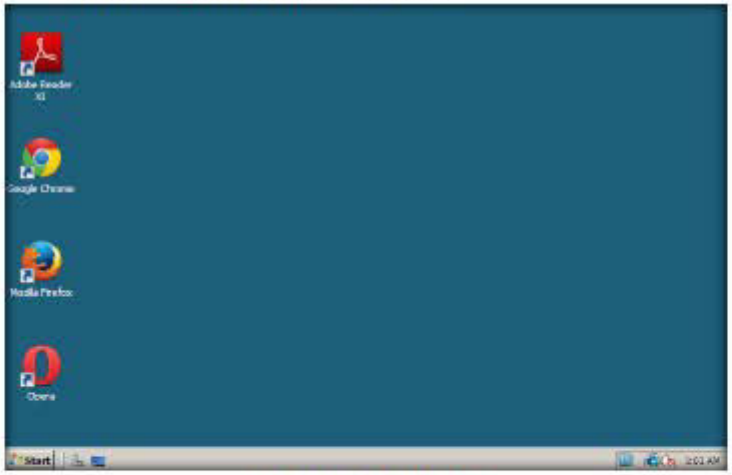


FIGURE 10.54: Checkpoint reverted back

88. This way, an attacker uses worms and Trojans in real-time to establish connection with the target machines and develop a botnet.

Lab Analysis

Document all the files, created viruses, and worms in a separate location.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 11

Creating a Worm Using Internet Worm Maker Thing

Internet Worm Maker Thing is a tool to used create worms. It can also convert a virus into a worm.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Scenario

Internet Worm Maker Thing is an automated scripting tool used to generate malicious code. It enables you to specify criteria down to the most basic element, including the actions you want it to perform, its display language, and its launch date. This lab demonstrates how easily an attacker can create a worm. As an ethical hacker and pen-tester, you can use Internet Worm Maker Thing as a proof of concept to audit perimeter security controls in your organization.

Lab Objectives

The objective of this lab is to make students learn and understand how to make viruses and worms.

Lab Environment

To carry out this lab, you will need:

- Internet Worm Maker Thing, located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Worm Maker\Internet Worm Maker Thing**
- A computer running Windows Server 2012 as host machine
- Run this tool on Windows Server 2012
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Virus and Worms

Computer worms are standalone malicious programs that replicate, execute, and spread across the network connections independently without human interaction. Intruders create most of the worms to replicate and to spread across a network, consuming available computing resources, thereby causing network servers, web servers and individual computer systems to stop responding. However, some worms carry a payload to damage the host system.

Lab Tasks

TASK 1

Make a Worm

1. Navigate to **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Worm Maker\Internet Worm Maker Thing**, and double-click **Generator.exe** file.
2. The **Internet Worm Maker Thing** main window appears, as shown in the screenshot:

Note: Take a Snapshot of the virtual machine before launching the Internet Worm Maker Thing tool.

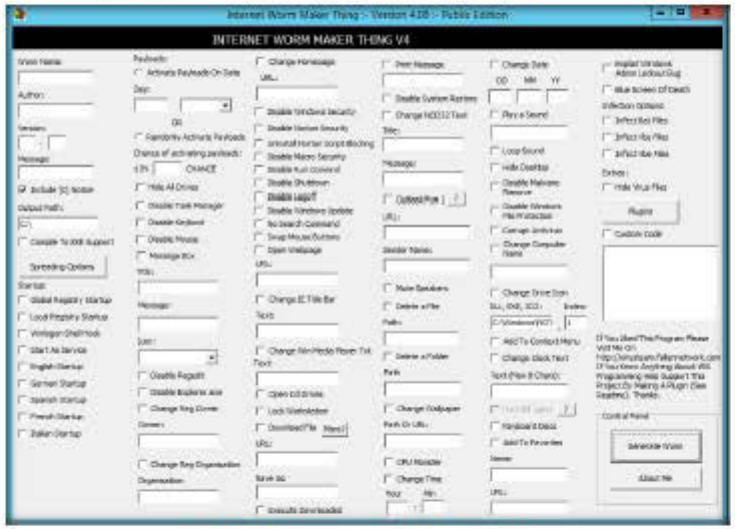


FIGURE 11.1: Internet Worm maker thing main window

The option, Auto Startup is always checked by default and start the virus whenever the system boots on.

3. Enter a **Worm name**, **author**, **version**, **message** and **output path** for the created worm.
4. Click the **Compile To EXE Support** check box.

5. In the **Startup** section, click the **English Startup** check box.

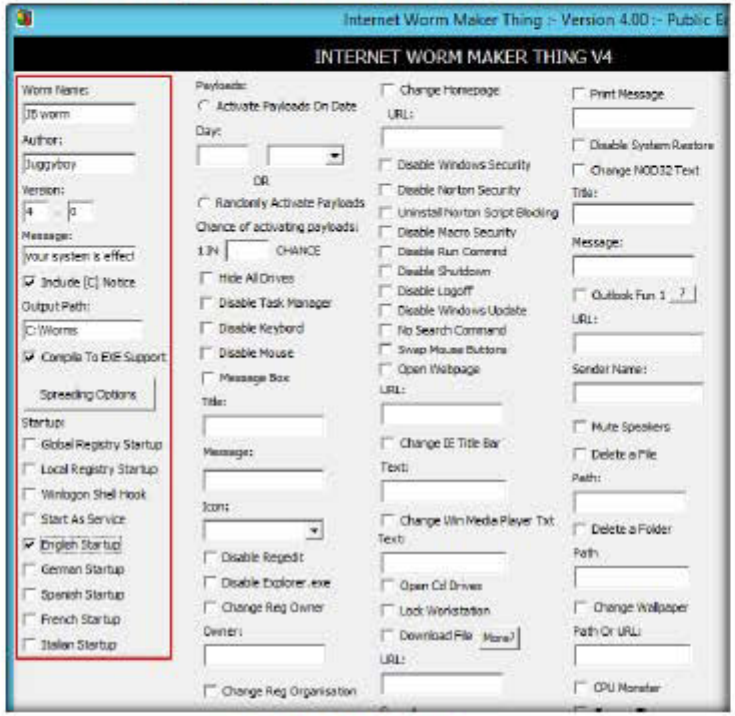


FIGURE 11.2 Select the options for creating Worm

6. Select the **Activate Payloads on Date** radio button, under **Payloads**; and enter the **Chance of activating payloads** value of **5**.

A list of names for the virus after install is shown in the Name after Install drop-down list.

7. Select the **Hide All Drives**, **Disable Task Manager**, **Disable keyboard**, **Disable Mouse**, and **Massage Box** check boxes.
8. Enter a **Title** and a **Message**, and select **Information** from the **Icon** drop-down list.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

9. Select the **Disable Regedit**, **Disable Explorer.exe** and **change Reg owner** check boxes.

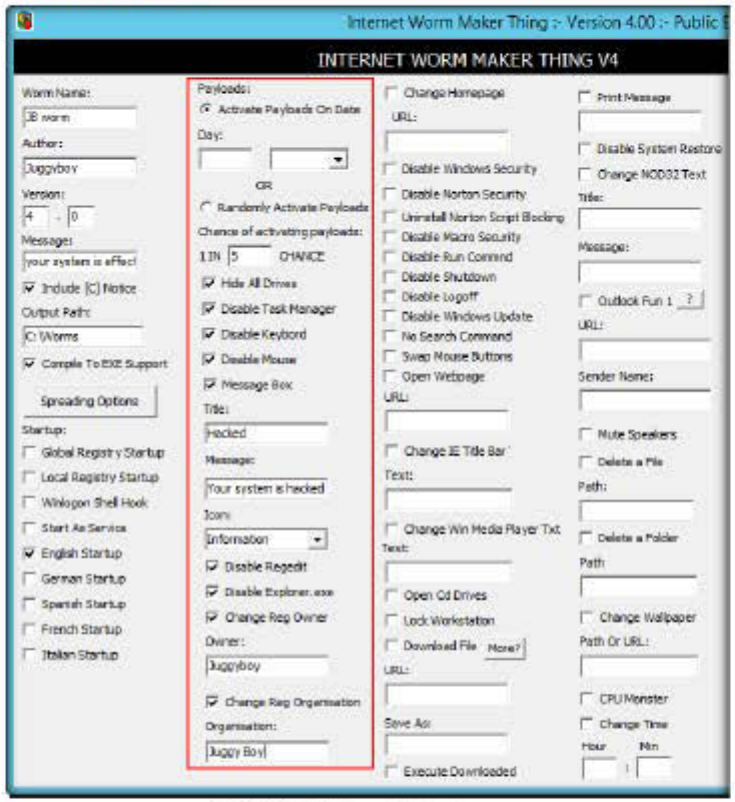


FIGURE 11.3: Select the options for creating worm

Don't forget to change the settings for every new virus creation. Otherwise, by default, it takes the same name as an earlier virus.

10. Select the **change Homepage** check box, and type http://www.juggyboy.com in the **URL** field.
11. Select the **Disable Windows Security**, **Disable Norton Security**, **Uninstall Norton Script Blocking**, **Disable Micro Security**, **Disable Run command**, **Disable shutdown**, **Disable Logoff**, **Disable windows Updates**, **No Search Command**, **Swap Mouse Button**, and **Open Web Page** check boxes.

12. Select the **Change IE Title Bar**, **Change Win Media Player Txt**, **Open Cd Drives**, and **Lock Workstation** check boxes.

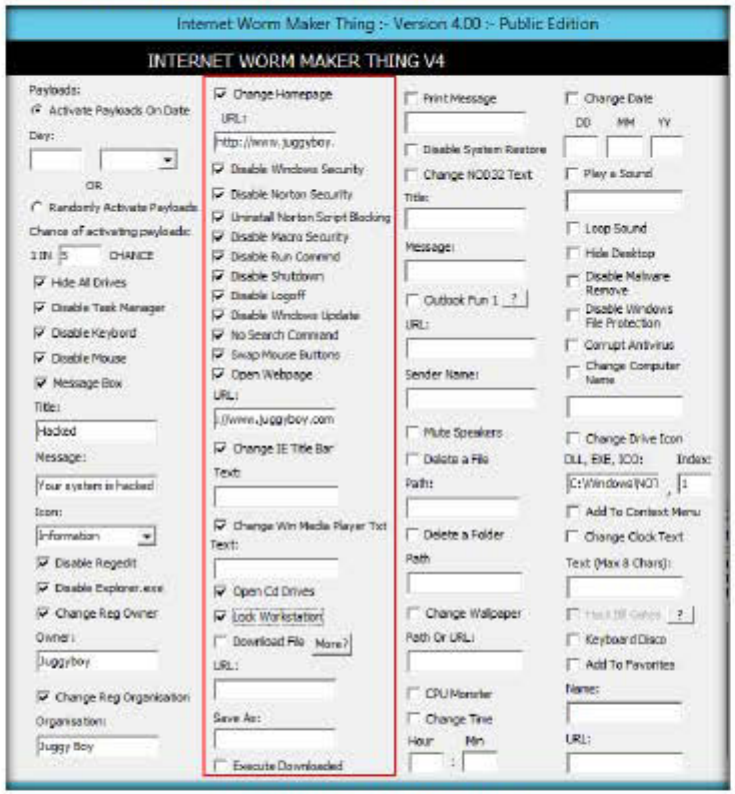


FIGURE 11.4 Select the options for creating worm

13. Select the **Print Message**, **Disable System Restore**, and **Change NOD32 Text** check boxes.
14. Enter a **Title** and a **Message** in their respective fields.
15. Enter the **URL** as http://www.juggyboy.com and **sender Name** as **juggyboy**.
16. Select the **Mute Speakers**, **Delete a Folder**, **Change Wallpaper**, and **CPU Monster** check boxes.

17. Select the **Change Time** check box, and enter a time in the **Hour** and **Min** fields.

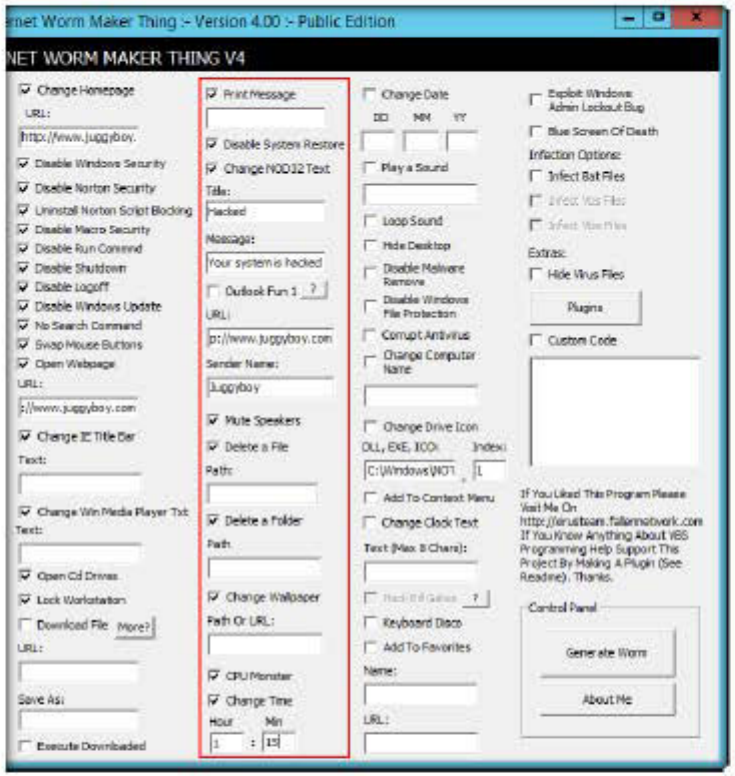


FIGURE 11.5: Select the options for creating worm

18. Select the **Change Date** check box, and enter a date in the **DD**, **MM**, and **YY** fields.

19. Select the **Loop Sound**, **Hide Desktop**, **Disable Malware Remove**, **Disable Windows File Protection**, **Corrupt Antivirus**, and **Change Computer Name** check boxes.

20. Select the **Change Drive icon**, **Add To Context Menu**, **Change Clock Text**, **Keyboard Disco**, and **Add To Favorites** check boxes.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

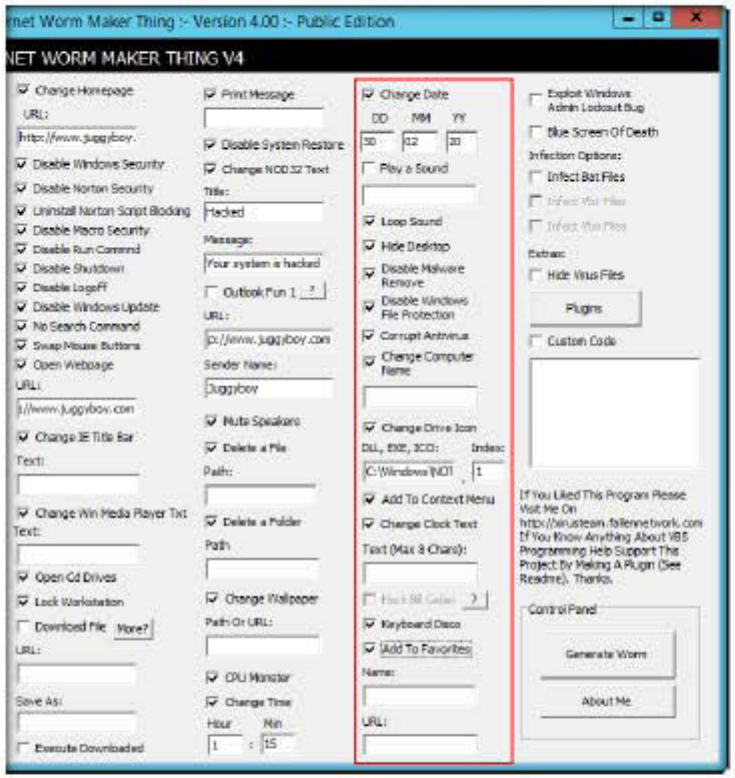


FIGURE 11.6 Select the options for creating worm

21. Select the **Exploit Windows Admin Lockout Bug** and **Blue Screen of Death** check boxes.

22. Select the **Infect Bat Files** check box, under **Infection Options**; select the **Hide Virus Files** check box, under **Extras**; and click **Generate Worm**, under **Control Panel**.

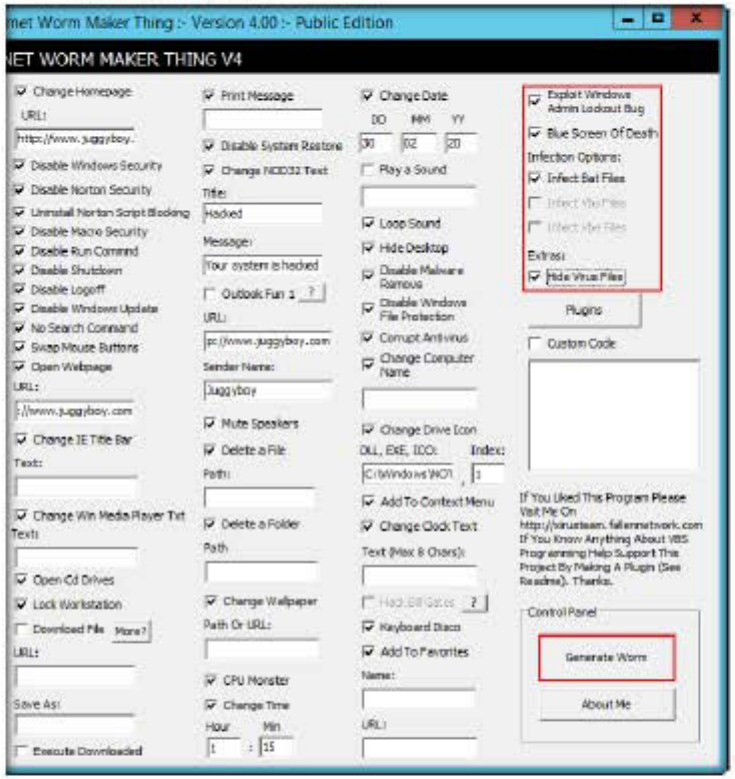


FIGURE 11.7: Select the options for creating worm

23. Once the worm is successfully created, an **Information!** dialog box appears. Click **OK** to close the pop-up.

FIGURE 11.8: Successful creation of worm pop-up window

24. The created **worm.vbs** is saved to the output path you provide, while configuring the Internet Worm Maker Thing. In this lab, the worm is saved to the location **C:/Worms**.

FIGURE 11.9: Created worm in a folder

25. In this way, attackers might craft worms using any of the above options and send them to the intended victims. When the victim runs the worm, the options configured in the worm start acting upon the victim's machine, which might also affect its performance.

Lab Analysis

Document all the files, created viruses, and worms in a separate location.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 12

Virus Analysis using IDA Pro

Computer worms are malicious programs that replicate, execute, and spread themselves across network connections independently, without human interaction.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Malware analysis provides in-depth understanding of each individual sample and identifies emerging technical trends from the large collections of malware samples without actually executing them. The samples of malware are mostly compatible with the Windows binary executable. There are a variety of goals in performing Malware analysis. As an ethical hacker and pen tester you have to perform malware analysis to understand the working of the malware and assess the damage that a malware may cause to the information system.

Lab Objectives

The objective of this lab is to make students learn and understand how to make viruses and worms to test the organization's firewall and antivirus programs.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Environment

To complete this lab, you will need:

- IDA Pro located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Malware Analysis Tools\IDA Pro**
- A computer running Windows Server 2012 as host machine
- Windows Server 2008 running on virtual machine as guest machine
- Run this tool on Windows Server 2008
- You can also download the latest version of IDA Pro from the link http://www.hex-rays.com/products/ida/index.shtml
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of the Lab

As a disassembler, IDA Pro explores binary programs, for which source code might not be available, to create maps of their execution. The primary purpose of a disassembler is to display the instructions actually executed by the processor in a symbolic representation called "assembly language." But in real life, things aren't always simple. Hostile code usually does not cooperate with the analyst. Viruses, worms, and Trojans are often armored and obfuscated. More powerful tools are required. The debugger in IDA Pro complements the static analysis capabilities of the disassembler by allowing an analyst to single step through the code being investigated, the debugger often bypasses the obfuscation and helps obtain data that the more powerful static disassembler will be able to process in depth.

Lab Tasks

TASK 1

IDA Pro

1. Log into the **Windows Server 2008** virtual machine.
2. Navigate to **Z:\CEHv9 Module 06 Malware Threats\Malware Analysis Tools\IDA Pro** and double-click **idademo66_windows.exe**.
3. If the **Open File - Security Warning** pop-up appears, click **Run**.
4. The IDA installation wizard appears; click on **Next** to continue with the installation.

Read the License Agreement carefully before accepting

FIGURE 12.1: IDA Pro Setup

Reload the input file

This command reloads the same input file into the database. IDA tries to retain as much information as possible in the database. All the names, comments, segmentation information and similar will be retained.

5. Select the **I accept the agreement** radio button for IDA Pro license agreement, and then follow the wizard driven installation steps to install IDA.

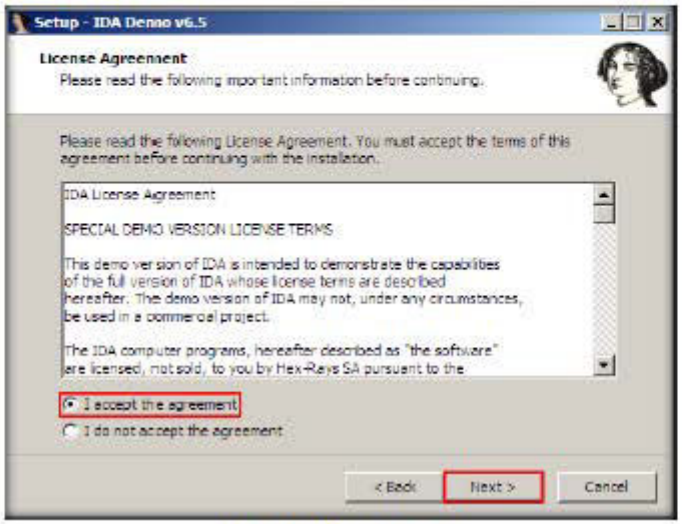


FIGURE 12.2: IDA Pro license agreement

Trace window

In this window, you can view some information related to all traced events. The tracing events are the information saved during the execution of a program. Different type of trace events are available: instruction tracing events, function tracing events and write, read/write or execution tracing events.

6. On completing the installation, ensure that **Launch IDA Demo** is checked, and then click **Finish**.

FIGURE 12.3: IDA Pro installation completed

Add breakpoint

This command adds a breakpoint at the current address. If an instruction exists at this address, an instruction breakpoint is created. Or else, IDA offers to create a hardware breakpoint, and allows the user to edit breakpoint settings.

7. If the **IDA License** window appears, click on **I Agree**.

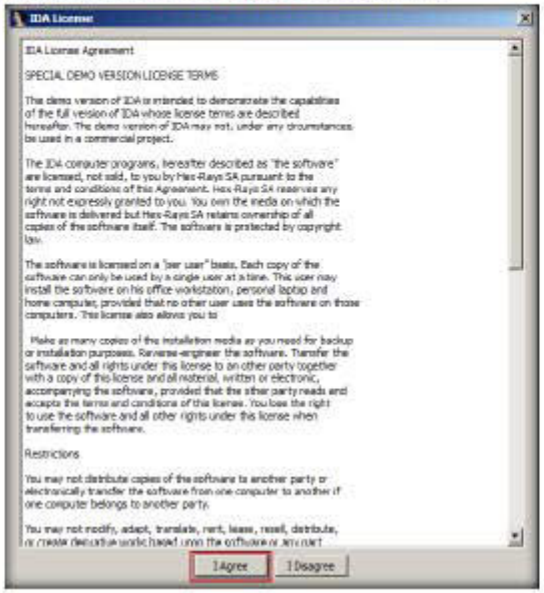


FIGURE 12.4 IDA Pro License accepts

8. The **IDA: Quick start** pop-up appears; click on **New**.

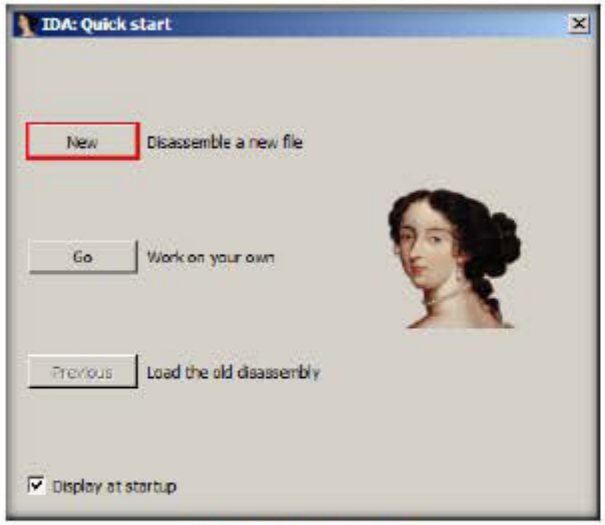


FIGURE 12.5 IDA Pro Welcome window

The configuration files are searched in the IDA.EXE directory. In the configuration files, you can use C, C++ style comments and include files. If no file is found, IDA uses default values.

Add execution trace

This command adds an execution trace to the current address.

// Compile an IDC script.
// The input should not contain functions that are
// currently executing - otherwise the behavior of the replaced
// functions is undefined.
// input - if isfile != 0, then this is the name of file to compile
// otherwise it hold the text to compile
// returns 0 - ok, otherwise it returns an error message.

string CompileEx(string input, long isfile);

// Convenience macro:

#define Compile(file) CompileEx(file, 1)

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

9. The IDA main window appears, along with the "Select file to disassemble" window. Navigate to **Z:\CEHv9 Module 06 Malware Threats\Viruses\Klez Virus Live!**, select **face.exe,** and click **open**.

Function tracing

This command starts function tracing. You can then use all debugger commands as usual: the debugger will save all addresses where a call to a function or a return from a function occurred.

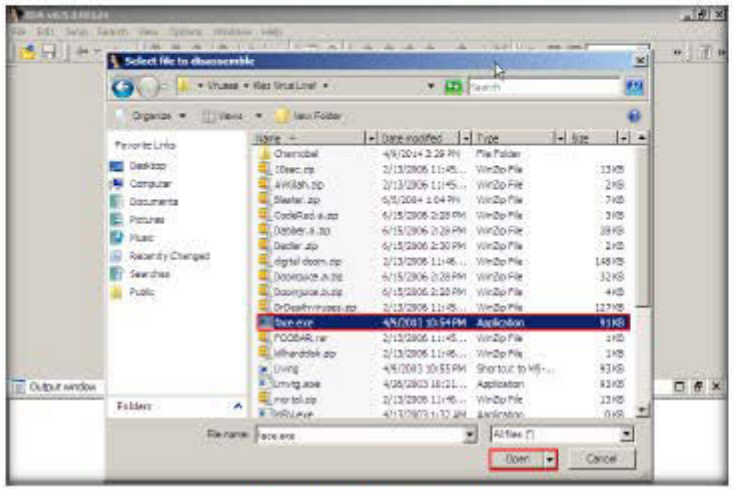


FIGURE 12.6: IDA Pro file browse window

10. The **Load a new file** window appears; keep the current settings, and click **OK**.

Add/Edit an enum

Action name: AddEnum

Action name: EditEnum

These commands allow you to define and to edit an enum type. You need to specify:

- name of enum
- its serial number (1,2...)
- representation of enum members

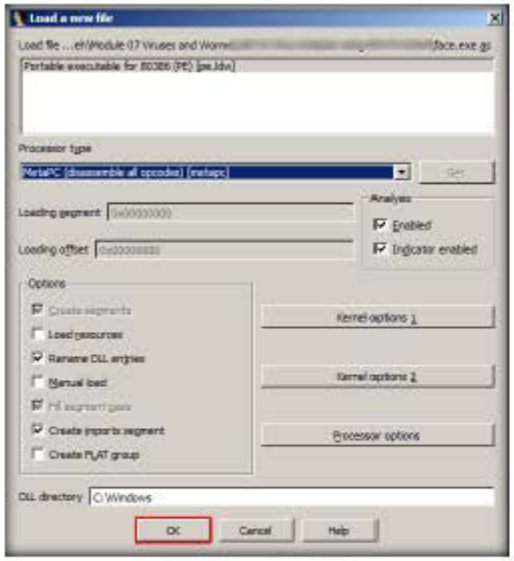


FIGURE 12.7: Load a new file window

11. If a **Warning** pop-up appears, click **OK**.
12. The **Please confirm** dialog-box appears; read the instructions carefully, and click **Yes**.

FIGURE 12.8 Confirmation wizard

Select appropriate options as per your requirement.

TMP or TEMP: Specifies the directory where the temporary files will be created.

Add read/write trace

This command adds a read/write trace to the current address.

Each time the given address will be accessed in read or write mode, the debugger will add a trace event to the Trace window.

13. The final window appears after the analysis is complete, as shown in the screenshot:

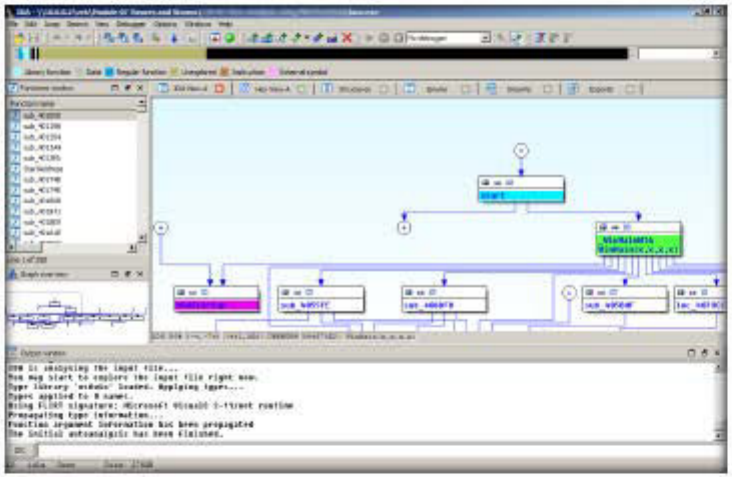


FIGURE 12.9: IDA Pro window after analysis

14. Go to **View → Graphs** and click **Flow Chart** from menu bar.

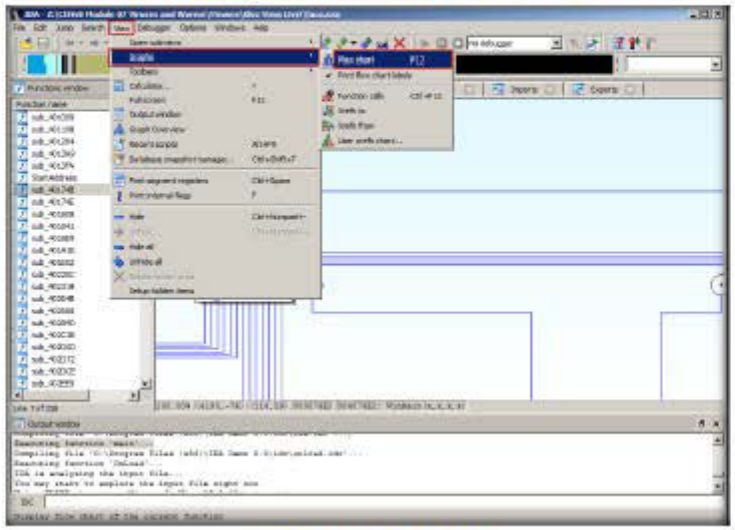


FIGURE 12.10: IDA Pro flow chart menu

Create alignment directive

Action name: Make Alignment

This command allows you to create an alignment directive.

15. A **Graph window** appears with the flow. You may zoom in to view clearly.

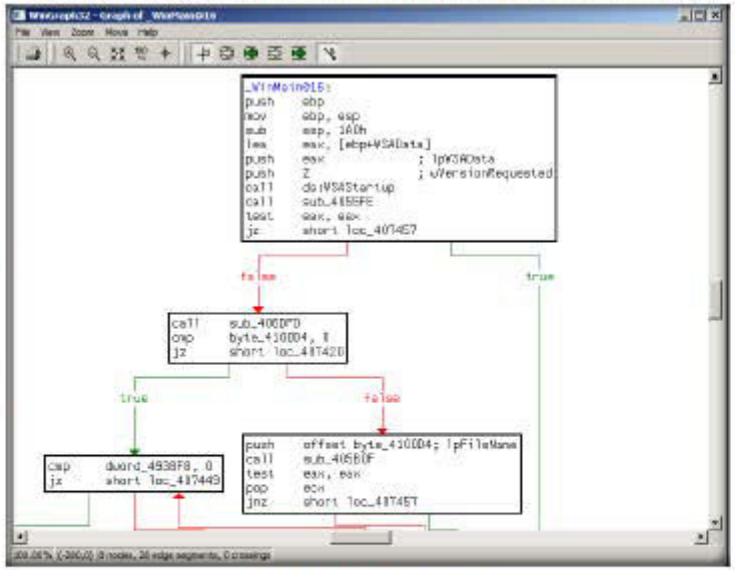


FIGURE 12.11: IDA Pro flow chart

Empty input file

The input file doesn't contain any instructions or data, i.e. there is nothing to disassemble.

Some file formats allow the situation when the file is not empty but it doesn't contain anything to disassemble. For example, COFF/OMF/EXE formats could contain a file header which just declares that there are no executable sections in the file.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Zoom in to have a better view of the details.

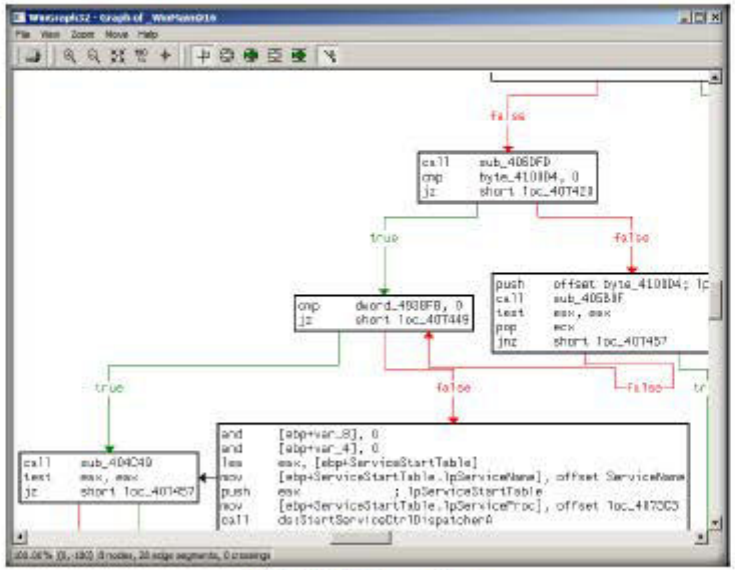


FIGURE 12.12: IDA Pro zoom flow chart

Zoom in to have a better view of the details.

Instruction tracing

This command starts instruction tracing. You can then use all the debugger commands as usual: the debugger will save all the modified register values for each instruction. When you click on an instruction trace event in the trace window, IDA displays the corresponding register values preceding the execution of this instruction. In the Result column of the Trace window, you can also see which registers were modified by this instruction.

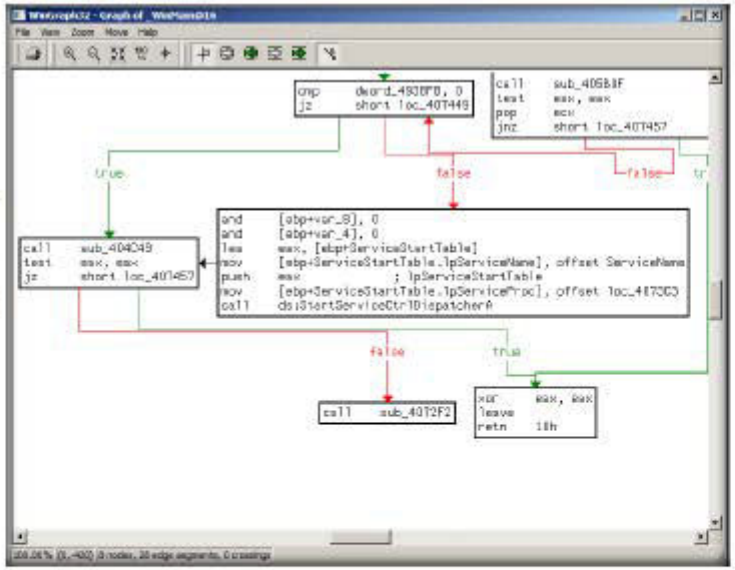


FIGURE 12.13: IDA Pro zoom flow chart

16. Go to **View → Graphs** and click **Function Calls** from menu bar.

FIGURE 12.14: IDA Pro Function calls menu

17. Window showing **call flow** appears; zoom in for a better view.

FIGURE 12.15: IDA Pro call flow of face

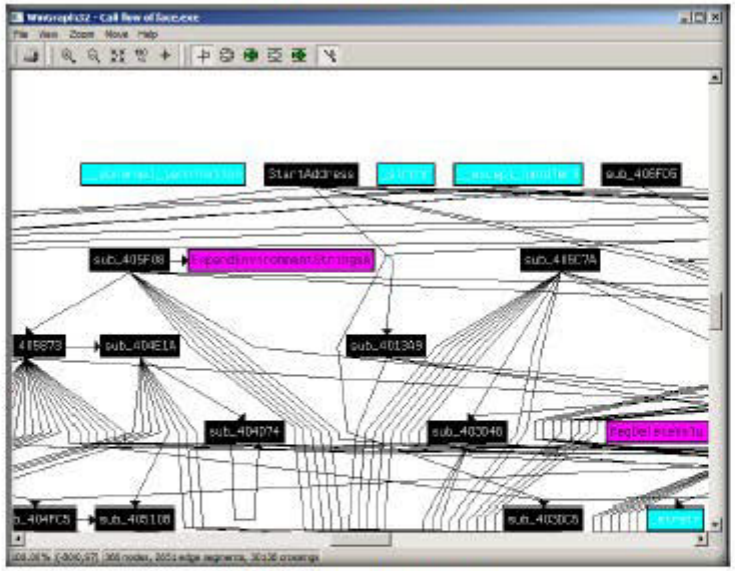


FIGURE 12.16: IDA Pro call flow of face with zoom

Empty input file

The input file doesn't contain any instructions or data, i.e. there is nothing to disassemble.

Some file formats allow the situation when the file is not empty but it doesn't contain anything to disassemble. For example, COFF/OMF/EXE formats could contain a file header which just declares that there are no executable sections in the file.

18. Click **Windows** on the menu bar, and select **Hex View-A**.

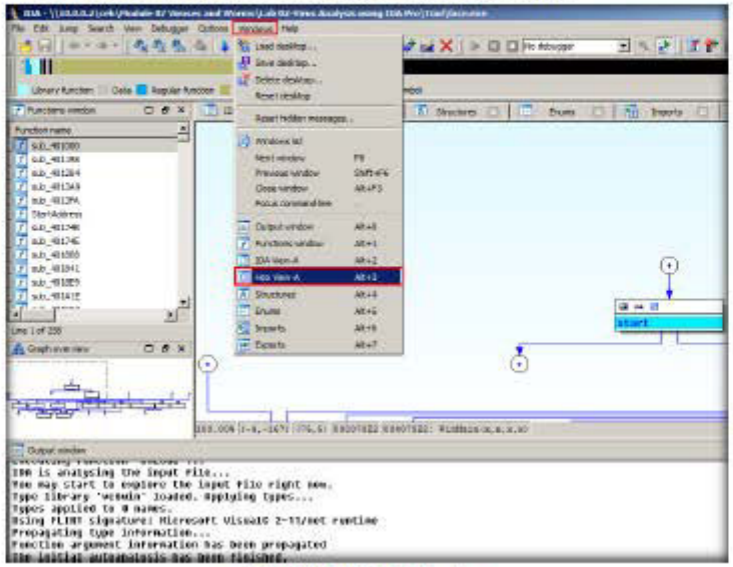


FIGURE 12.17: IDA Pro Hex View-A menu

19. IDA displays the hex values, as shown in the screenshot:

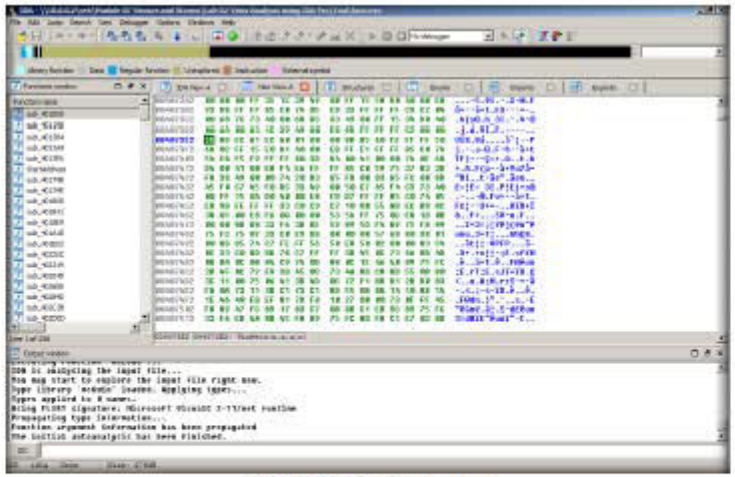


FIGURE 12.18: IDA Pro Hex View-A result

20. Click **Windows** from the menu bar, and select **Structures**.

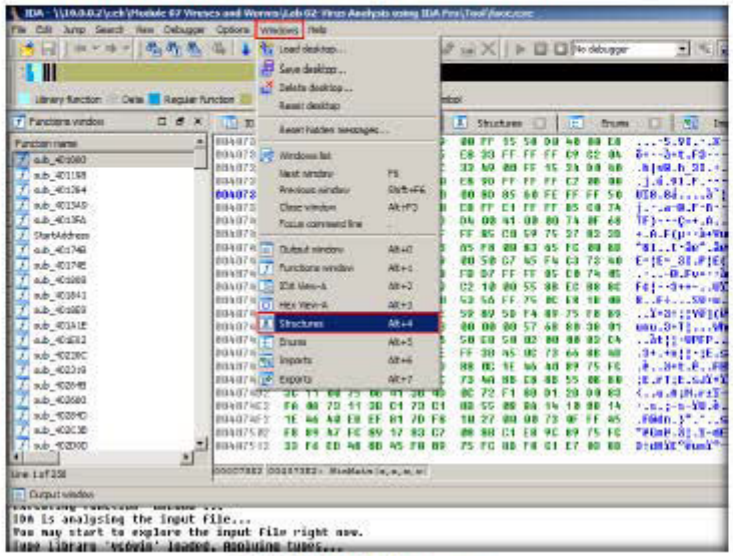


FIGURE 12.19: IDA Pro Hex Structure menu

21. IDA displays all the **Structures** (to expend structures, click on **Ctrl** and **+**), as shown in the screenshot:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

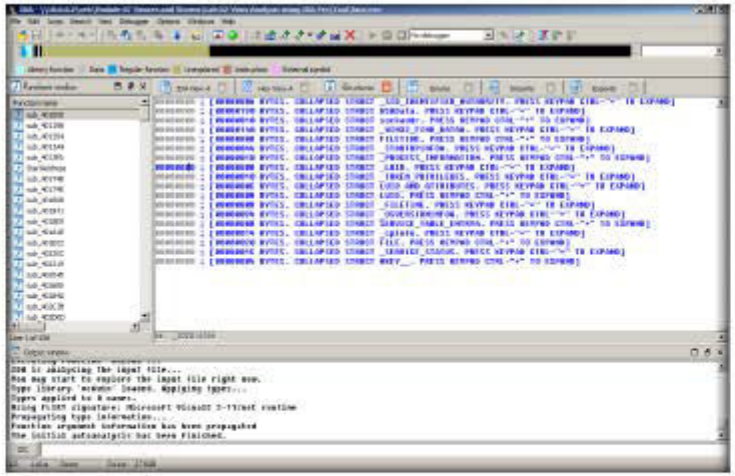


FIGURE 12.20: IDA Pro Hex Structure result

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

22. Click **Windows** from the menu bar, and select **Enum**.

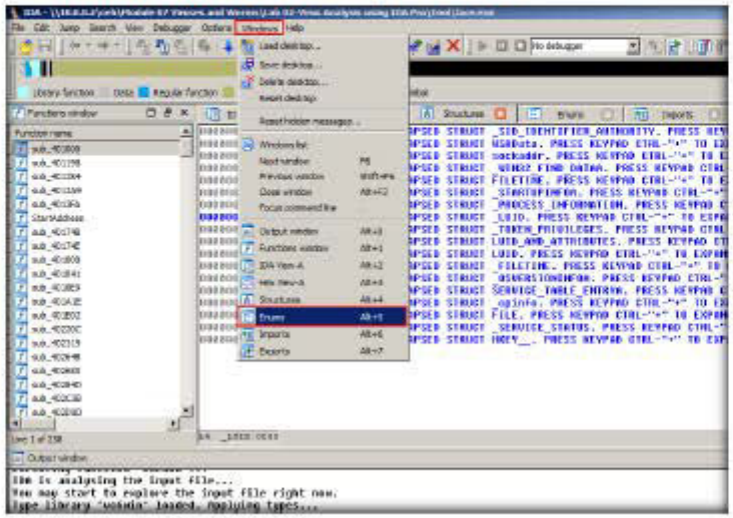


FIGURE 12.21: IDA Pro Enums menu

23. IDA displays the Windows Enum results, as shown in the screenshot:

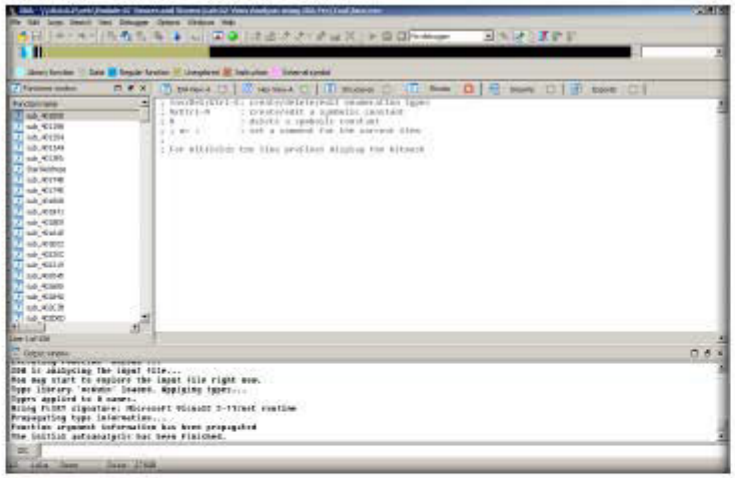


FIGURE 12.22: IDA Pro Enums result

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Lab 13

Virus Analysis Using VirusTotal

VirusTotal is a free service that analyzes suspicious files and URLs, and facilitates the quick detection of viruses, worms, Trojans, and other kinds of malware.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In today's online environment, it's important to know what risks lie ahead at each click. Every day millions of people go online to find information, to do business, to have a good time. There have been many warnings about the potential for data theft, such as identity theft, phishing scams, and pharming. We have at least heard of denial-of-service attacks and "zombie" computers, and now yet another type of online attack has emerged: holding data for ransom.

VirusTotal helps you, an expert Ethical Hacker and Penetration Tester, to analyze files and URLs enabling the identification of viruses, worms, Trojans, and other kinds of malicious content detected by anti-virus engines and website scanners. In this lab, you will see how you can analyze malware using online virus analysis services.

Lab Objectives

The objective of this lab is to learn and understand how to make viruses and worms to test an organization's firewall and anti-virus programs.

- Analyze virus files over the Internet

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Environment

To complete this lab, you will need:

- A computer running Windows Server 2012 as host machine
- A web browser with Internet access

Lab Duration

Time: 5 Minutes

Overview of VirusTotal

VirusTotal's stated mission is to help improve the anti-virus and security industry and make the Internet a safer place through the development of free tools and services. VirusTotal simply acts as an information aggregator. The aggregated data are the output of different antivirus engines, website scanners, file and URL analysis tools, and user contributions. The malware signatures of antivirus solutions present in VirusTotal are periodically updated as they are developed and distributed by anti-virus companies. The update polling frequency is 15 minutes—thus ensuring that these products are using the latest signature sets. Website scanning is done via API queries to the different companies providing the particular solution; hence, the most updated version of their dataset is always used.

Lab Tasks

TASK 1

VirusTotal Scanning service

1. Log into the **Windows Server 2012** host machine.
2. Launch a web browser (here, **Firefox**), type **http://www.virustotal.com** in the address bar, and press **Enter**.
3. The **VirusTotal** webpage appears in the browser; click **Choose File**.

FIGURE 13.1: Virus Total Home Page

4. The **File Upload** window appears; navigate to **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.

You can upload any infected file to analyze.

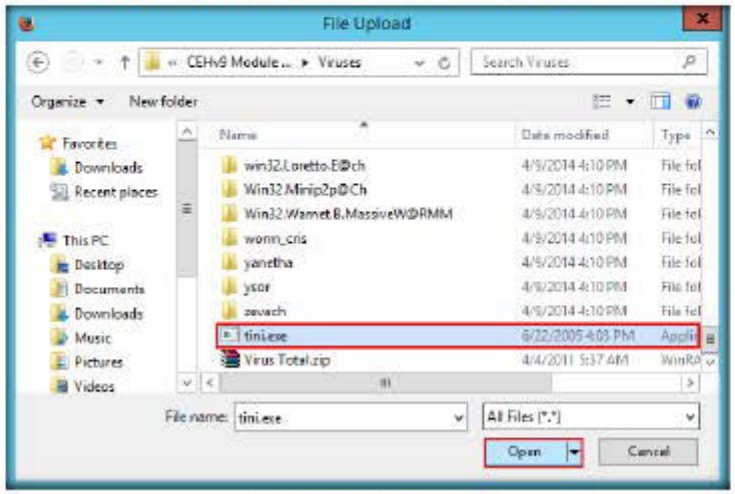


FIGURE 13.2: Select a file for Virus analysis

5. Click on **Scan it!**

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

FIGURE 13.3: Click Send button to send the files for analysis

6. The selected file will be sent to the VirusTotal server to analyze.
7. If a pop-up appears stating that the file has already been analyzed, click on **Reanalyse**.

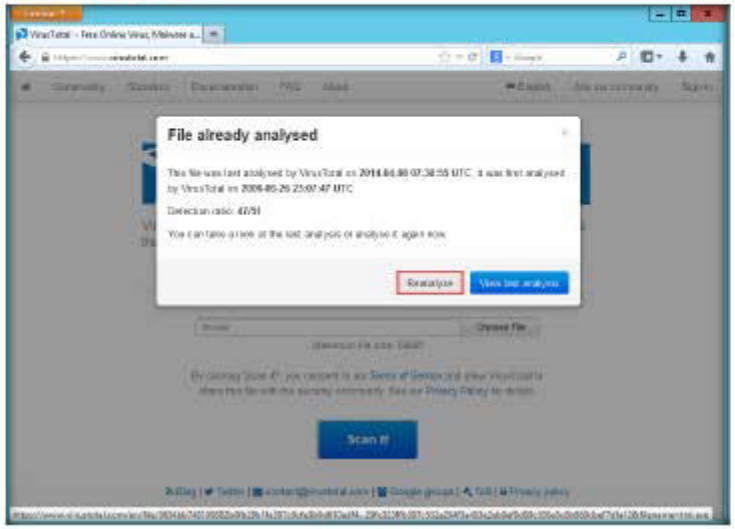


FIGURE 13.4: Sending File

8. Selected file analysis queues are scanned, as shown in the screenshot:

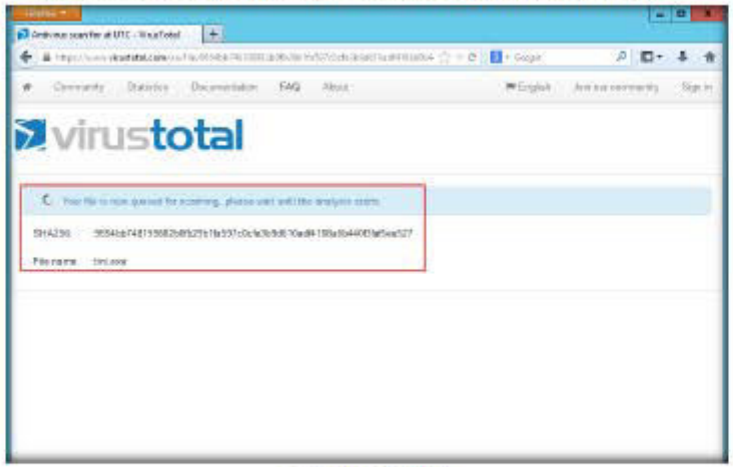


FIGURE 13.5: Scanned File

9. VirusTotal returns a detailed report displaying the result of each anti-virus for the selected **tini.exe** malicious file, as shown in the screenshot:

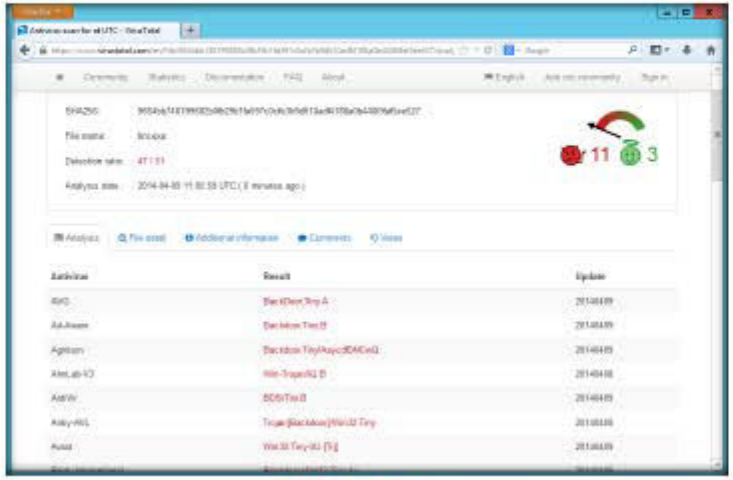


FIGURE 13.6: Analyzing the file

Lab Analysis

Analyze and document the results of this lab exercise. Provide your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Lab 14

Virus Analysis Using OllyDbg

OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is not available. It traces registers, recognizes procedures, API calls, switches, tables, constants, and strings, and locates routines from object files and libraries.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

There are literally thousands of malicious logic programs and new ones come out by the numbers, so that's why it's important to keep up to date with new ones that come out each day. Many websites keep track of this. There is no known method for providing 100% protection for any computer or computer network from computer viruses, worms, and Trojan horses, but people can take several precautions to significantly reduce their chances of being infected by any of these malicious programs.

In this lab, OllyDbg is used to analyze virus registers, procedures, API calls, tables, libraries, constants, and strings.

Lab Objectives

The objective of this lab is to make students learn and understand analysis of the viruses.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Environment

To complete this lab, you need:

- OllyDbg tool, located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Malware Analysis Tools\OllyDbg**
- A computer running Windows Server 2012 as host machine
- You can also download the latest version of OllyDbg from the link http://www.ollydbg.de/
- Run this tool on Windows Server 2012
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of OllyDbg

This debugging engine is now more stable, especially if one steps into the exception handlers. There is a new debugging option, "Set permanent breakpoints on system calls." When active, it requests OllyDbg to set breakpoints on KERNEL32.UnhandledExceptionFilter (), NTDLL.KiUserExceptionDispatcher(), NTDLL.ZwContinue() and NTDLL.NtQueryInformationProcess().

Lab Tasks

TASK 1

Debug a Virus

1. Navigate to **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Malware Analysis Tools\OllyDbg**, and double-click **OLLYDBG.EXE**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. If the **UDD Directory Absent** dialog box appears, click **OK**.
4. The **OllyDbg** main window appears, as shown in the screenshot:

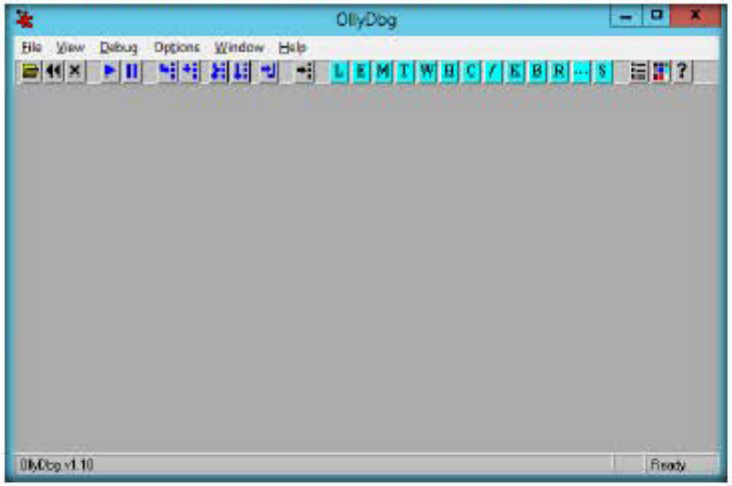


FIGURE 14.1: OllyDbg main window

You can also download the latest version of OllyDbg from the link http://www.ollydbg.de.

Note: When you launch OllyDbg for the first time, a number of sub-windows might appear in the main window of OllyDbg; close all of them.

5. Choose **File** in menu bar, and choose **Open...**
6. The **Open 32-bit executable** window appears; navigate to **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.

Data formats. Dump windows display data in all common formats: hexadecimal, ASCII, UNICODE, 16-and 32-bit signed/unsigned/hexadecimal integers, 32/64/80-bit floats, addresses, disassembly (MASM, IDEAL, HLA or AT&T).

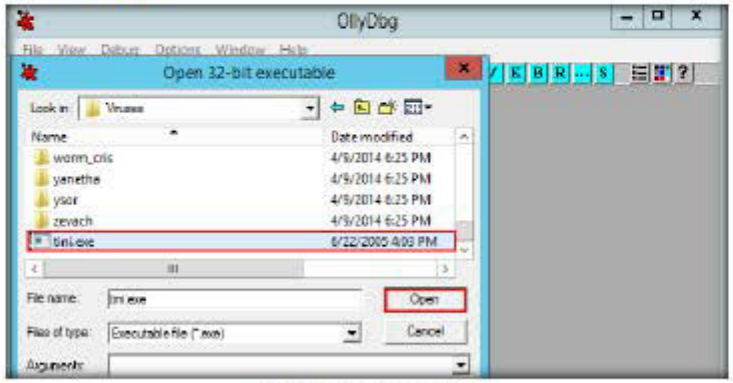


FIGURE 14.2 Select tini.exe Virus

7. The output appears in a window named **CPU - main thread, module ntdll**, as shown in the screenshot:

OllyDbg can debug multithread applications. You can switch from one thread to another, suspend, resume and kill threads or change their priorities.

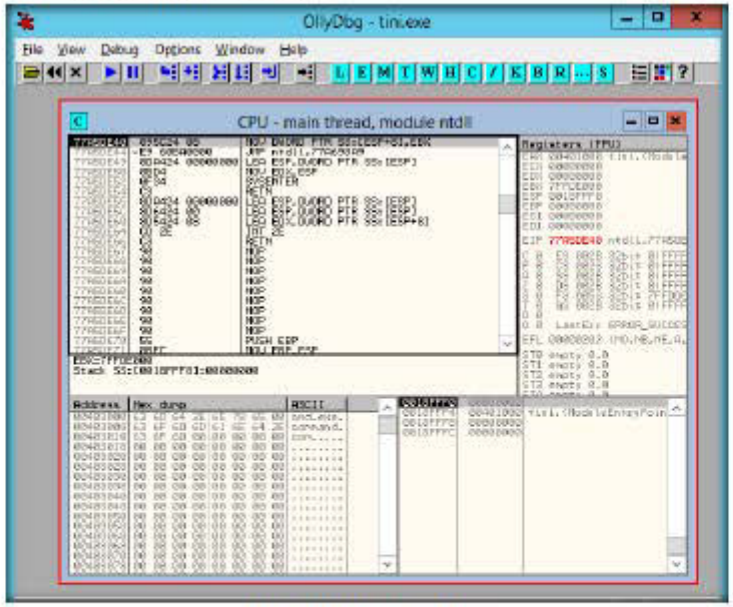


FIGURE 14.3: CPU utilization of tini.exe

8. Choose **View** in menu bar, and choose **Log**.

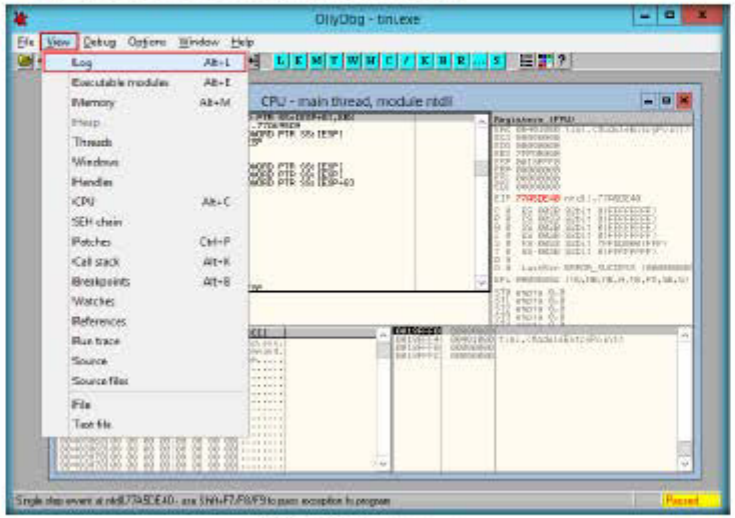


FIGURE 14.4 Select log information

Full UNICODE support. All operations available for ASCII strings are also available for UNICODE, and vice versa. OllyDbg is able to recognize UTF-8 strings.

9. A window named **Log data** appears in OllyDbg (**Log data**), displaying the log details shown in the screenshot:

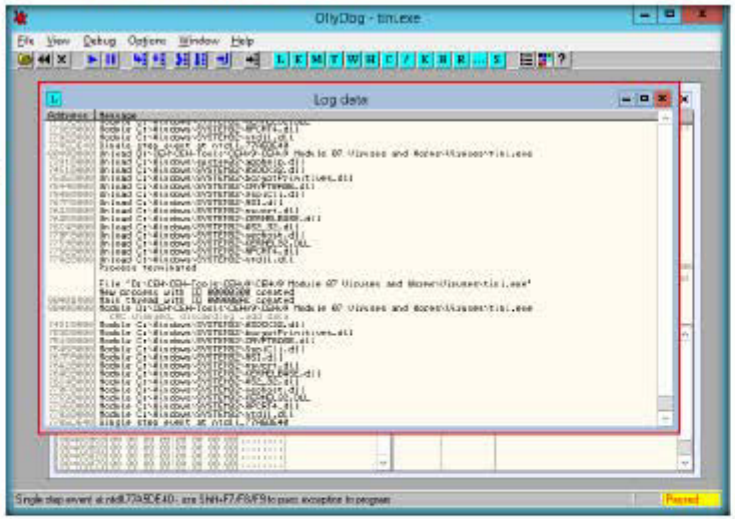


FIGURE 14.5 Output of Log data information of tini.exe

Breakpoints: OllyDbg supports all common kinds of breakpoints: INT3, memory and hardware. You may specify number of passes and set conditions for pause

10. Choose **View** in the menu bar, and then choose **Executable module**.

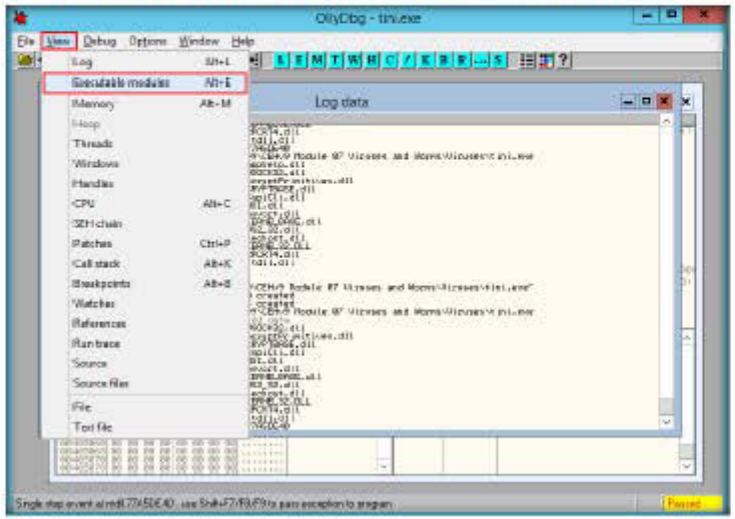


FIGURE 14.6: Viewing executable modules

11. A window appears in OllyDbg (Executable modules), displaying all the executable modules as shown in the following screenshot:

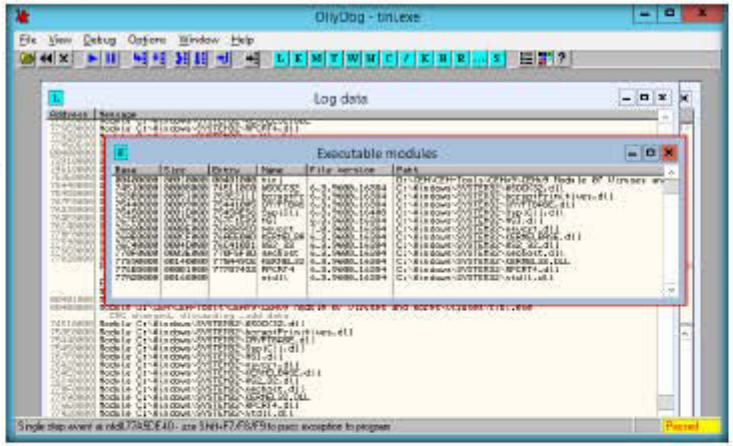


FIGURE 14.7: Output of executable modules of tini.exe

Watches: Watch is an expression evaluated each time the program pauses. You can use registers, constants, address expressions, Boolean and algebraical operations of any complexity.

12. Choose **View** in menu bar, and then choose **Memory**.

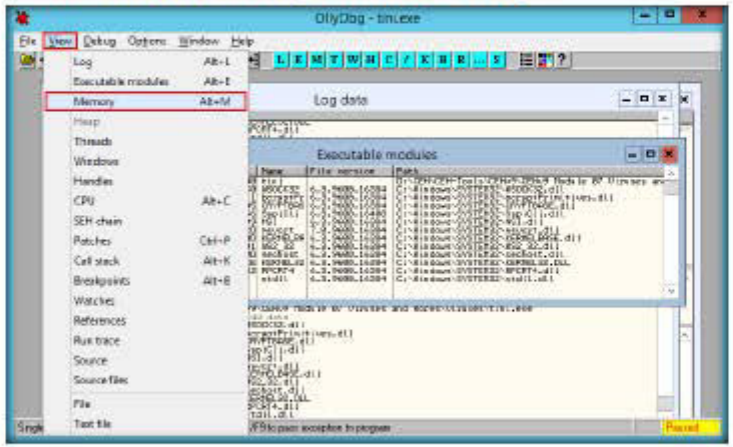
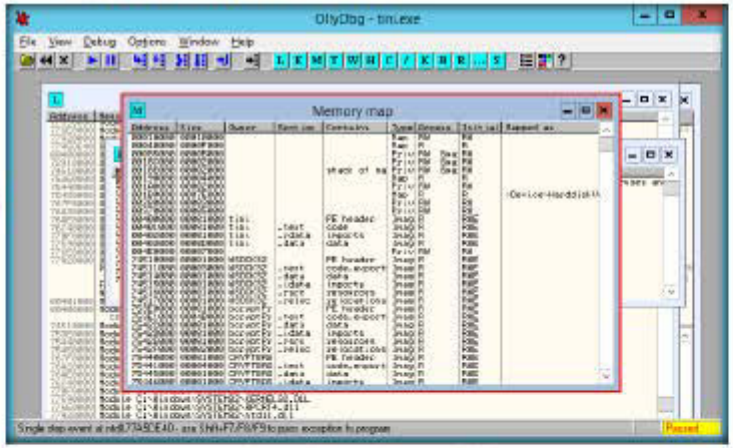


FIGURE 14.8: Viewing memory mappings

13. A window appears in OllyDbg (**Memory map**), displaying all memory mappings, as shown in the screenshot:



OllyDbg supports four different decoding modes: MASM, Ideal, HLA and AT&T

FIGURE 14.9: Output of Memory map of tini.exe

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

14. Choose **View** in menu bar, and then choose **Threads**.

FIGURE 14.10: Viewing the threads

15. A window appears in OllyDbg (**Threads**), displaying all threads, as shown in the screenshot:

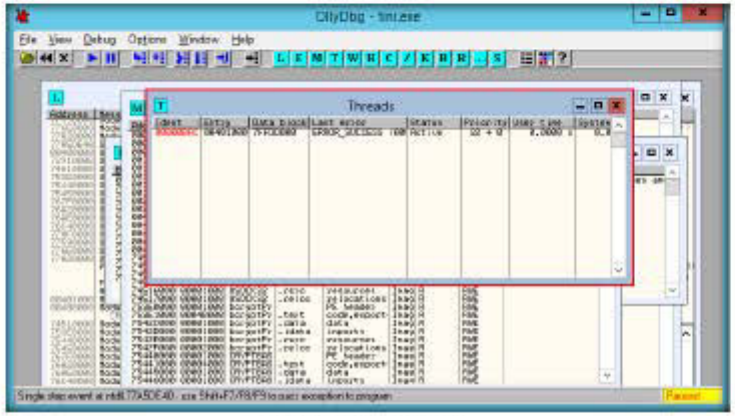


FIGURE 14.11: Output of threads

16. This way, you can scan a file and analyze the output using OllyDbg.

Lab Analysis

Document all the files, created viruses, and worms in a separate location.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Lab 15

Detecting Trojans

A Trojan is a program that contains malicious or harmful code hidden inside apparently harmless programming or data, in such a way that it can take over system control and cause damage such as ruining the file allocation table on a hard drive.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Nature of malware makes them difficult to detect. Unlike viruses, Trojans do not delete or corrupt files or applications that a victim might notice; they do their best to stay out of the victim's sight, thus escaping detection. Malware detection helps in addressing this problem on infected systems, and thus serves to protect them and them resources from further loss.

You are a Security Administrator of your company, and your job responsibilities include protecting the network from Malware, Trojan attacks, theft of valuable network data, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of this lab include system monitoring, using tools such as:

- Port Monitor
- Process Monitor
- Registry Monitor
- Startup Program Monitor, etc.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats

Lab Environment

To carry out this, you need:

- **Tepview,** located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Port Monitoring Tools\TCPView**
- **Autoruns,** located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Process Monitoring Tools\Autoruns**

- **Jv16 power tool,** located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Registry Entry Monitoring Tools\jv16 PowerTools**
- A computer running Window Server 2012 (host machine)
- Windows Server 2003 running in virtual machine
- If you decide to download the latest version, then screenshots shown in the lab might differ
- You need a web browser to access Internet
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of the Lab

Trojans are malicious programs that masquerade as a useful or legitimate file, but their actual purpose is to take complete control over the computer, thereby accessing files and confidential information. To protect files and personal information from such unauthorized access, an anti-virus product has to be used, which automatically scans and detects the presence of Trojans on the system, or one can also manually detect the Trojans installed on the system.

Lab Tasks

1. Log in to **Windows Server 2012** host machine.
2. Double-click **Tcpview.exe** located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Port Monitoring Tools\TCPView** in order to launch the application.
3. If a **TCPView License Agreement** window appears, click **Agree** button to agree to the terms and conditions.

TASK 1

Analyze the Processes running on each port using TCPView

4. TCPView main window appears, displaying the details, such as **Process**, **ProcessId**, **Protocol**, **Local address**, **Local Port**, **Remote Address**, and **Remote Port**.

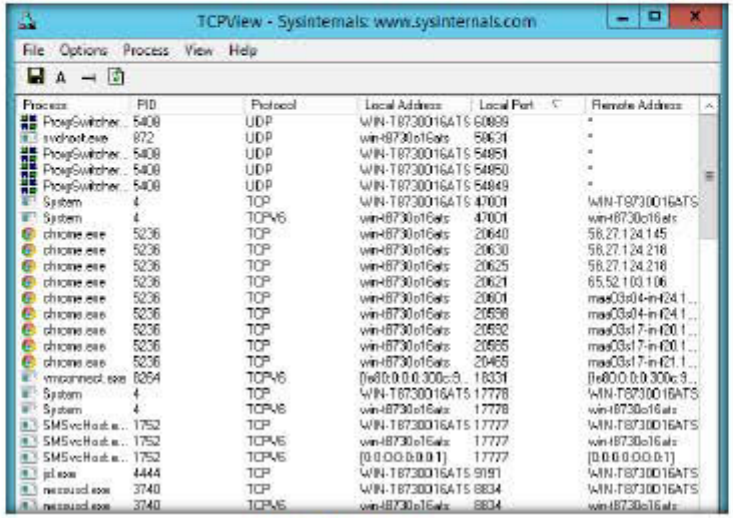


FIGURE 15.1: Tcpview Main window

5. TCPView performs **Port monitoring**. Click **Local Port** tab to view the ports in serial order.

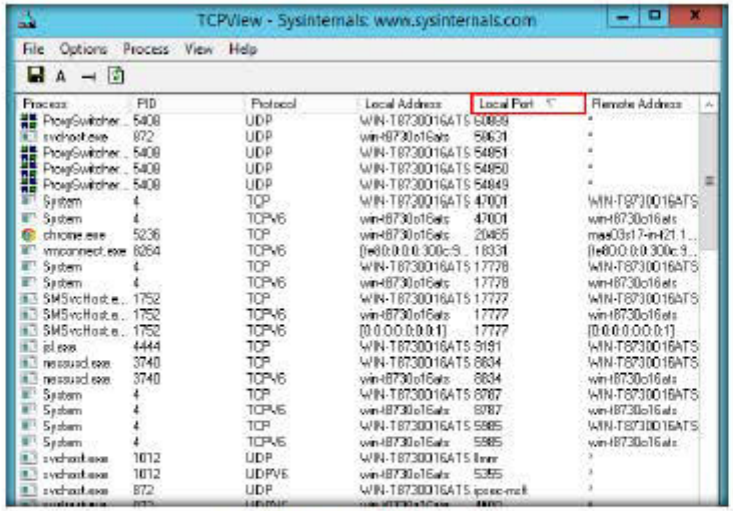


FIGURE 15.2: Tcpview Main analyzing ports

Should delete items that you do not wish to ever execute. Do so by choosing **Delete** in the **Entry** menu. Only the currently selected item will be deleted.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

6. TCPView helps you analyze TCP and other ports. Click the **Protocol** tab to view the Protocol in serial order.

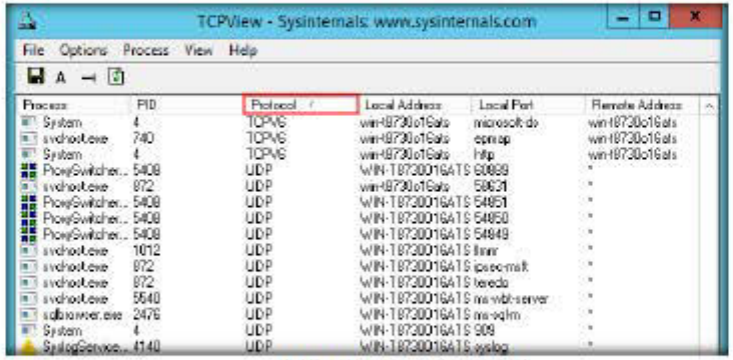


FIGURE 15.3: Tcpview analyzing protocols

7. You can also end a process by double-clicking the respective process, and then click **End Process**.

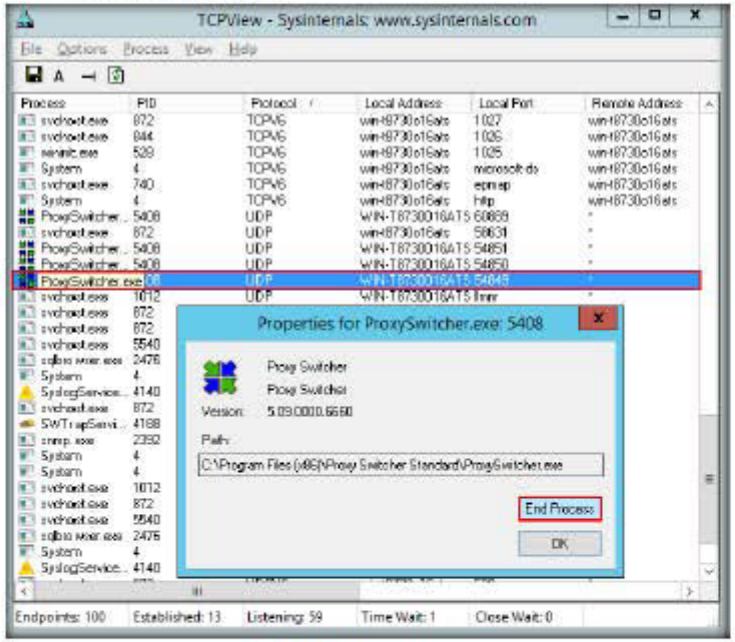


FIGURE 15.4: Tcpview killing a process

Disabling and Deleting Entries

If you don't want an entry to active the next time you boot or login you can either disable or delete it. To disable an entry uncheck it. Autoruns will store the startup information in a backup location so that it can reactivate the entry when you recheck it. For items stored in startup folders Autoruns creates a subfolder named Autoruns disabled. Check a disabled item to re-enable it.

8. If a **TCPView** dialog box appears, click **Yes** to terminate the process.

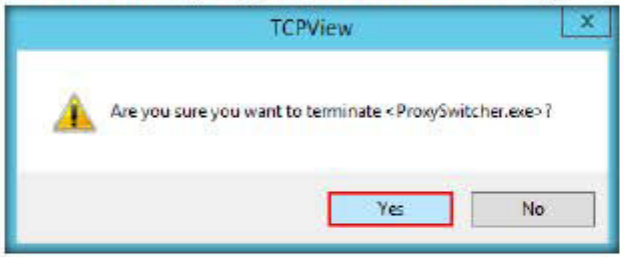


FIGURE 15.5: Killing Processes

9. This way, you can view all the processes running on the machine and stop unwanted/malicious processes that may affect your system. If you are unable to stop a process, then you can view the port on which it is running and add a firewall rule to block the port.

TASK 2

Examine the Results in AutoRuns

10. Log into the **Windows Server 2012** host machine.
11. Navigate to **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Process Monitoring Tools\Autoruns**, and double-click **autoruns.exe**.
12. The **AutoRuns License Agreement** window appears; click **Agree**.

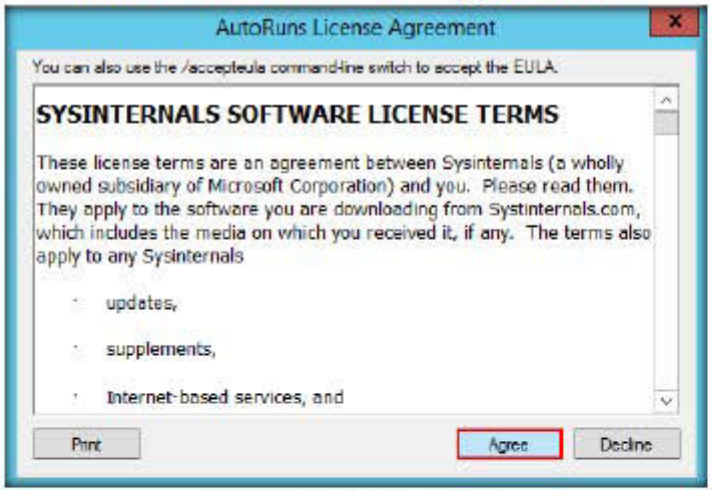
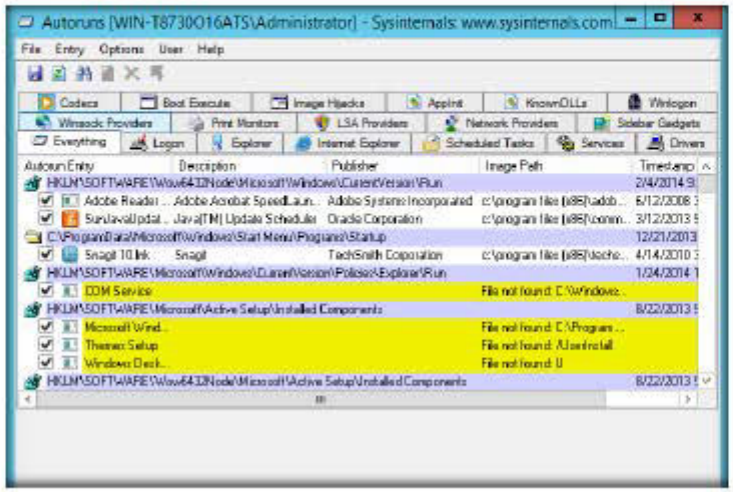


FIGURE 15.6: AutoRuns License Agreement window

You can view Explorer's file properties dialog for an entry's image file by choosing **Properties** in the **Entry** menu. You can also have Autoruns automatically execute an Internet search in your browser by selecting **Search Online** in the **Entry** menu.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

13. Autoruns displays all the **processes, dll's, services,** and so on, as shown in the screenshot:

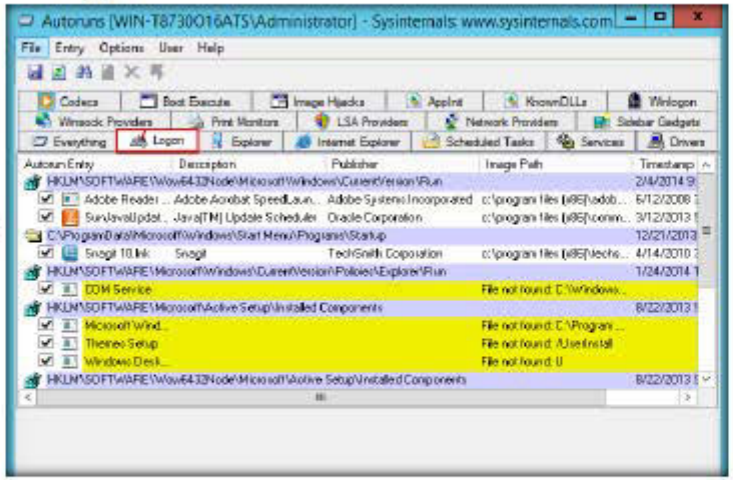


Simply run Autoruns and it shows you the currently configured auto-start applications in the locations that most directly execute applications. Perform a new scan that reflects changes to options by refreshing the display.

FIGURE 15.7: Autoruns Main Window

Note: The application lists displayed under all the tabs may vary in your lab environment.

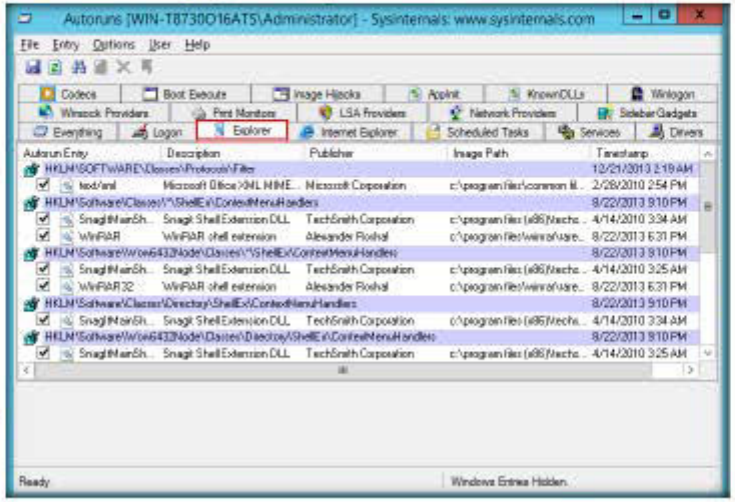
14. Click the **Logon** tab to view the applications that run automatically during logon.



Internet Explorer This entry shows Browser Helper Objects (BHO's), Internet Explorer toolbars and extensions.

FIGURE 15.8: Autoruns Logon list

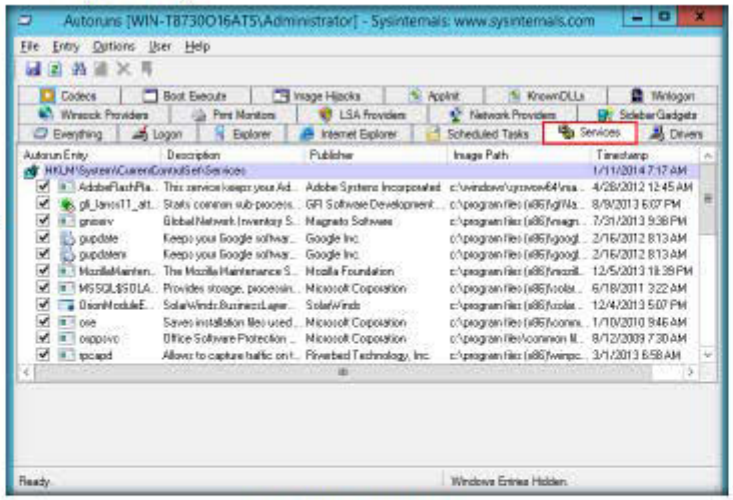
15. Click the **Explorer** tab to view the explorer applications that run automatically at system startup.



There are several ways to get more information about an autorun location or entry. To view a location or entry in **Explorer** or **Regedit** chose Jump To in the **Entry** menu or double-click on the entry or location's line in the display.

FIGURE 15.9: Autoruns Explorer list

16. Clicking the **Services** tab displays all the services that run automatically at system startup.



Services All Windows services are configured to start automatically when the system boots.

Drivers This displays all kernel-mode drivers registered on the system except those that are disabled.

FIGURE 15.10: Autoruns Services list

17. Click the **Drivers** tab to view all the applications' drivers that run automatically at system startup.
18. For example, here **airpcap** is selected. Clicking this driver displays the size, version and time at which it was run automatically at system startup (for the first time).

Note: The list displayed under this tab may vary in your lab environment.

If you are running Autoruns without administrative privileges on Windows Vista and attempt to change the state of a global entry, you'll be denied access.

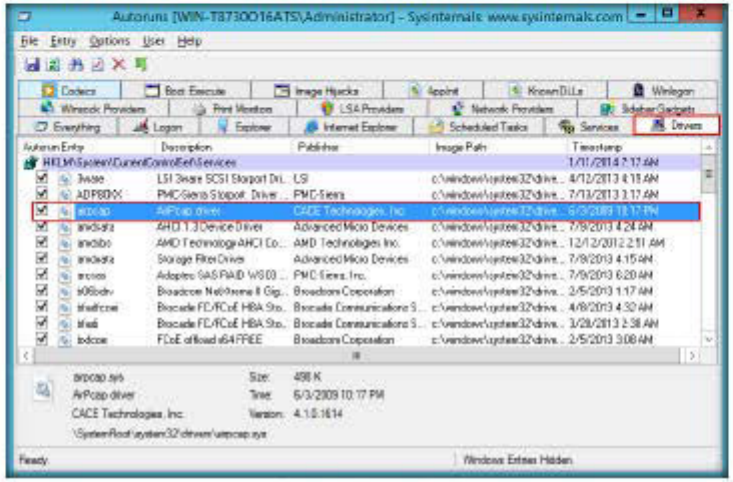


FIGURE 15.11: Autoruns Drivers list.

19. Click **Known DLLs** tab to view all the known DLLs that start automatically at system startup.

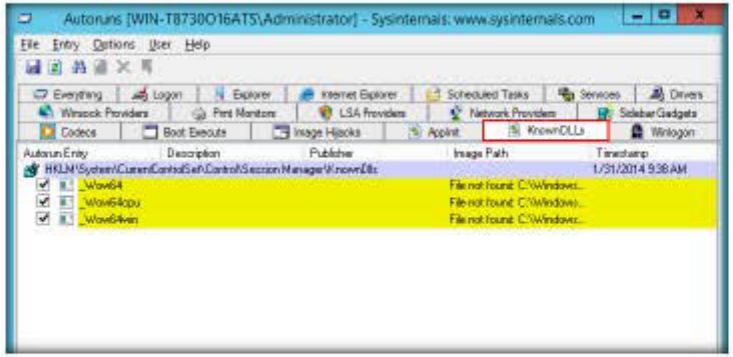


FIGURE 15.12: Autoruns Known DLLs list.

20. By examining all these tabs, you can find any unwanted process/application running on the machine and stop/delete them manually.

TASK 3

Perform intensive scan for unwanted resources using jv16 Power Tools

21. Log into the **Windows Server 2012** host machine.
22. Navigate to **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Registry Entry Monitoring Tools\jv16 PowerTools**, and double-click **jv16pt_setup.exe**.
23. Follow the wizard-driven installation steps to install jv16 Power Tools.

FIGURE 15.13: Jv16 Power Tools installation wizard

24. Click **jv16 PowerTools** on the **Apps** screen to launch the application.

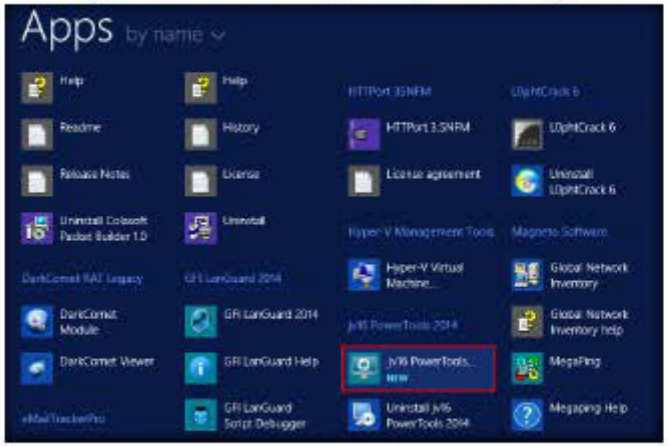


FIGURE 15.14: Launching the application

Winlogon Notifications Shows DLLs that register for Winlogon notification of logon events.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

Winsock Providers
Shows registered Winsock protocols, including Winsock service providers. Malware often installs itself as a Winsock service provider because there are few tools that can remove them. Autoruns can uninstall them, but cannot disable them.

25. The **jv16 PowerTools Quick Tutorial** window appears; click **Next**.

FIGURE 15.15: Jv16 PowerTools Quick Tutorial window

26. Choose a language (here, **English**), and click **Next**.

FIGURE 15.16: Choosing a language

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

27. The **Tips** section of the tutorial appears; click **Next**.

FIGURE 15.17: Tips section

28. Click **Next** in the **subscription** section.

FIGURE 15.18: Subscription section

29. Select the **Show me a simplified user interface** radio button in the **user interface** section, and click **Next**.

FIGURE 15.19: User Interface section

30. The application begins to set up, as shown in the screenshot:

FIGURE 15.20: Application setup

31. On completion of the setup, a pop-up appears states that the tool will restart. Click **OK**.

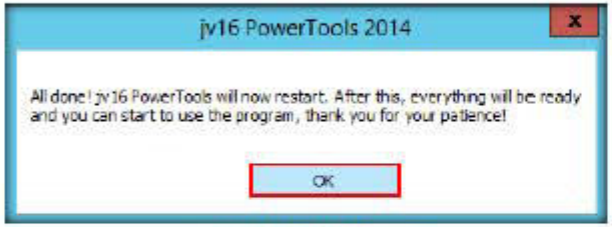


FIGURE 15.21: Tool restart pop-up

32. The **jv16 PowerTools** main window appears on the screen.
33. Click **Clean and fix my computer**.

FIGURE 15.22: jv16 main window

34. The **Clean and fix my computer** dialogue box appears. Click the **Settings** tab, and click **Start**.

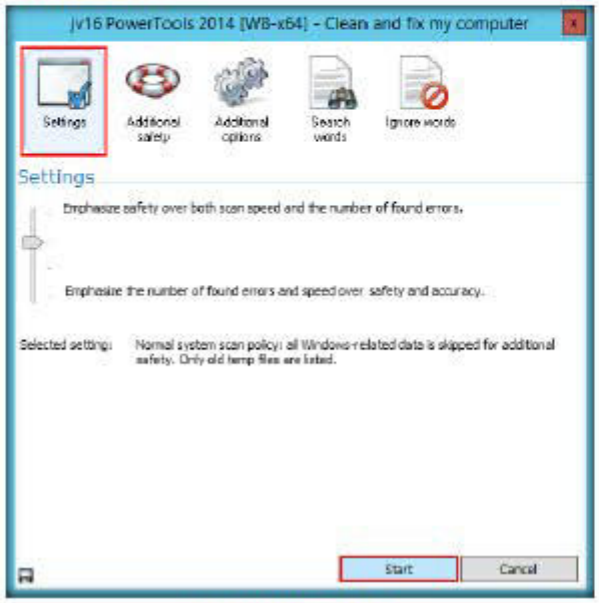


FIGURE 15.23: Beginning the analysis

35. This starts analyzing the machine. It takes a few minutes.

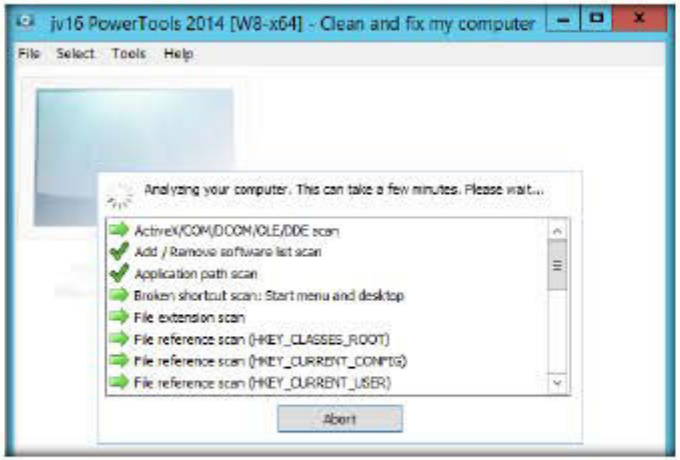


FIGURE 15.24: jv16 Analyzing the system

LSA Providers Shows registers Local Security Authority (LSA) authentication, notification and security packages.

Printer Monitor Drivers Displays DLLs that load into the print spooling service. Malware has used this support to autostart itself.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

36. Once the scanning is complete, jv16 PowerTools displays the **Registry Errors**, **Temp Files**, etc.

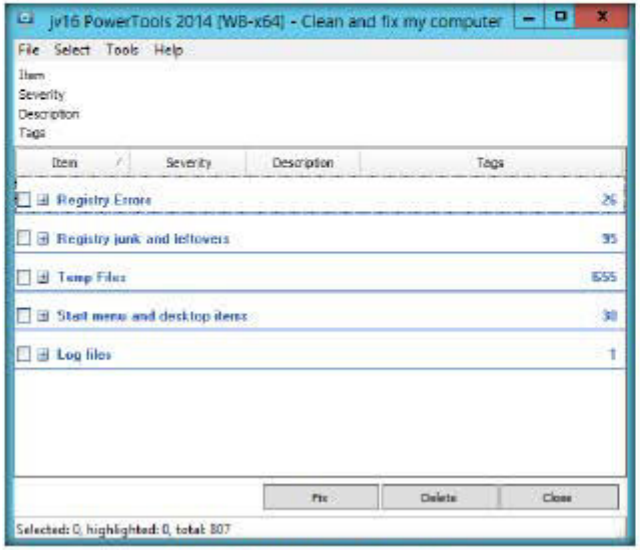


FIGURE 15.25: jv16 displaying the analysis results

You can save the results of a scan with **File->Save** and load a saved scan with **File->Load.** These commands work with native Autoruns file formats, but you can use File->Export to save a text-only version of the scan results. You can also automate the generation of native Autoruns export files with command line options.

37. To view the Registry Errors, expand the **Registry Errors** node, and expand the **Invalid file or directory reference** node.

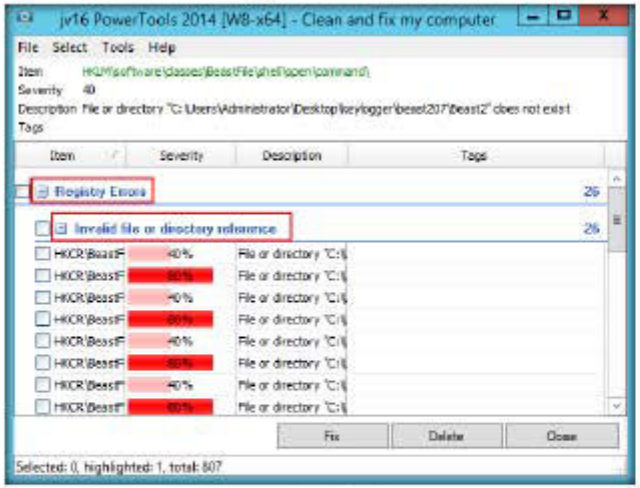
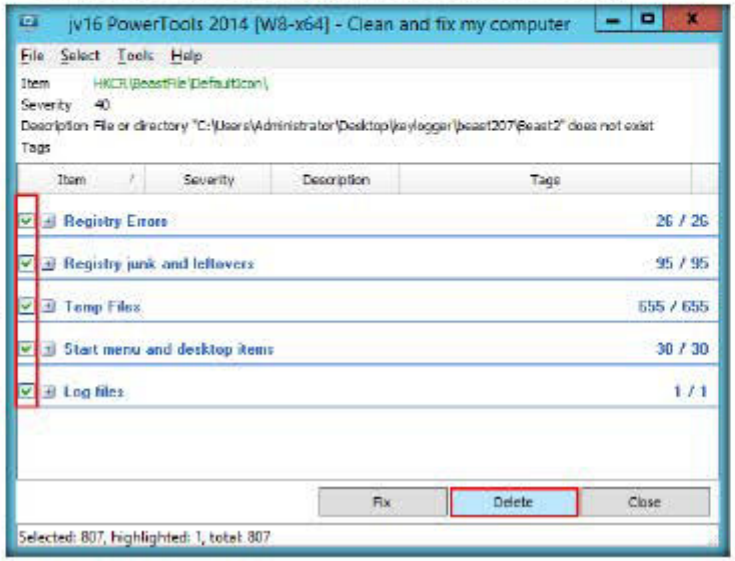


FIGURE 15.26: Viewing the registry errors

If you are running Autoruns without administrative privileges on Windows Vista and attempt to change the state of a global entry, you'll be denied access. Autoruns will display a dialog with a button that enables you to re-launch Autoruns with administrative rights.

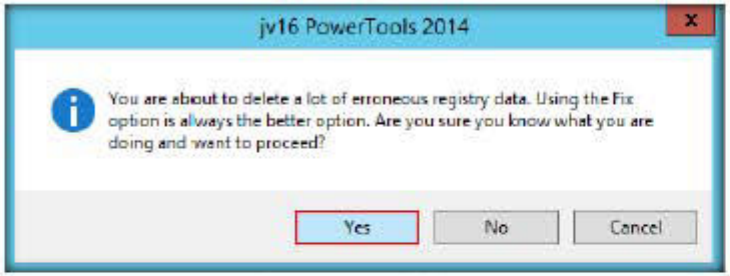
38. In the same way, expand the other items in the list to view all the temporary files, log files, etc.
39. Check all the items in the application window, and click **Delete**.



Compare the current Autoruns display with previous results that you've saved. Select **File | Compare** and browse to the saved file. Autoruns will display in green any new items, which correspond to entries that are not present in the saved file. Note that it does not show deleted items.

FIGURE 15.27: Deleting all the files

40. The **jv16 PowerTools** pop-up appears; click **Yes**.



Unless the **Include Empty Locations** selection in the **Options** menu is checked Autoruns doesn't show locations with no entries.

FIGURE 15.28: jv16 PowerTools pop-up

41. This deletes all the unwanted/harmful registries, logs, temporary files, etc., ensuring the safety of your computer.
42. If the **jv16 Power Tools** pop-up appears, asking you to restart the computer, click **OK**.
43. If the **Clean and Fix My Computer** dialogue-box still appears, close it.

44. Click **Home**, and select **Control which programs start automatically**.

FIGURE 15.29: Selecting Control which programs start automatically

45. Check the software of your choice in **Startup manager,** and select the appropriate action on the software you check.

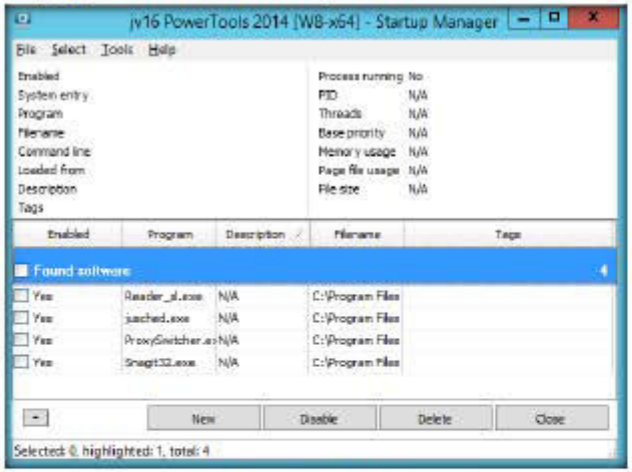


FIGURE 15.30: jv16 Startup Manager Dialogue

46. Thus, you could find any Trojans or malicious files running at system startup and choose appropriate actions against them.

47. Select **Registry Tools** to view Registry-related icons.

The **Verify Signatures** option appears in the **Options** menu on systems that support image signing verification and can result in Autoruns querying certificate revocation list (CRL) web sites to determine if image signatures are valid.

The **Hide Microsoft Entries** selection omits images that have been signed by Microsoft if **Verify Signatures** is selected and omits images that have Microsoft in their resource's company name field if **Verify Signatures** is not selected.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

48. This section helps you to find, manage, monitor, compress, clean, or replace **registry files**.

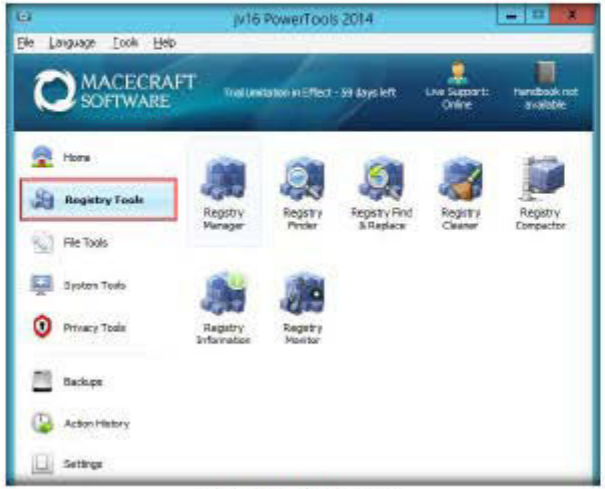


FIGURE 15.31: jv16 Registry tools

Use the Hide Microsoft Entries or Hide Windows Entries in the Options menu to help you identify software that's been added to a system since installation. Autoruns prefixes the name of an image's publisher with "(Not verified)" if it cannot verify a digital signature for the file that's trusted by the system.

49. Click **File Tools** to view file-related icons.

50. This section helps you to find, recover, clean, organize, or merge **files** or **directories**.

FIGURE 15.32: jv16 File tools

Use the **Hide Windows Entries** omits images signed by Windows if **Verify Signatures** is selected. If **Verify Signatures** is not selected, **Hide Windows Entries** omits images that have Microsoft in their resource's company name field and the image resides beneath the %SystemRoot% directory.

51. Select the **System Tools** menu to view system-related applications with which you can uninstall software, manage services, etc.

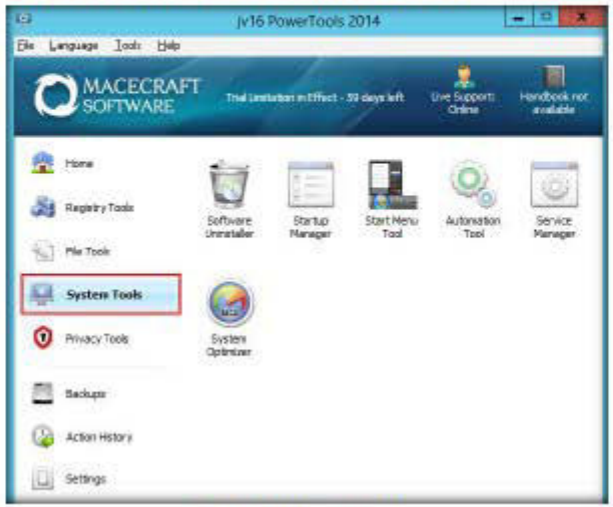


FIGURE 15.33: jv16 System tools

52. Select **Privacy tools** to view **History cleaner** and **Disk Wiper** options.

FIGURE 15.34: jv16 Privacy tools

53. The first option helps in cleaning the history, while the other wipes the disk—which is *not* recommended.

54. Select **Backups** to view the system-related backups.

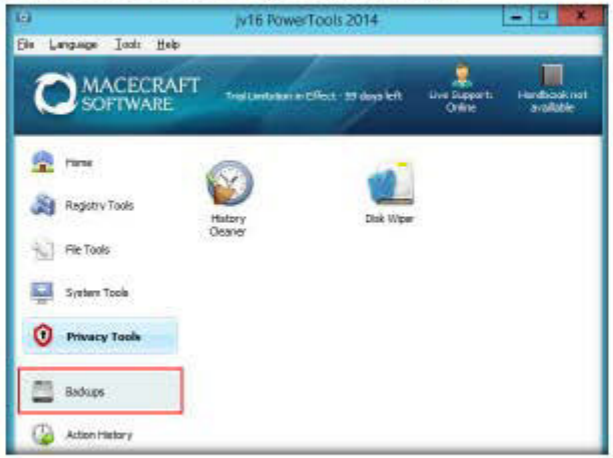


FIGURE 15.35: jv16 Backup tools

55. The **Jv16 Powertools Backup Tool** window appears, displaying backups such as **registry**, **file**, and **other** backups.

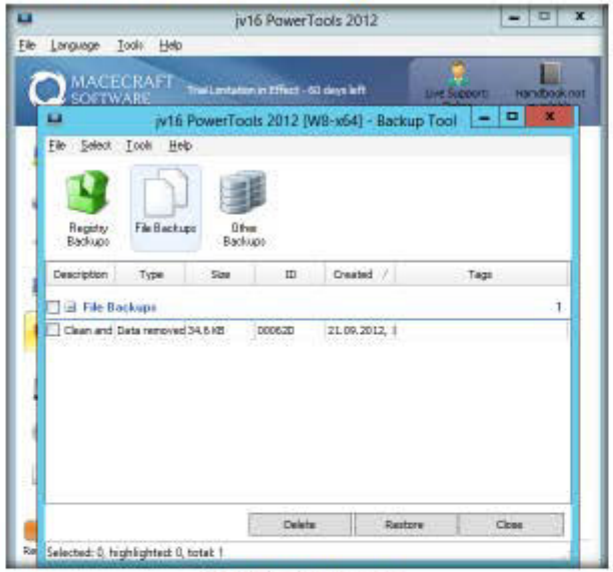


FIGURE 15.36: jv16 Backup tools

56. You can choose whether to delete or restore backups in this window.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 16

Monitoring TCP/IP Connections Using the CurrPorts

CurrPorts is network monitoring software that displays a list of all currently opened TCP/IP and UDP ports on a local computer, along with the processes running on its ports.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 06 Malware Threats and D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

Lab Scenario

You already know that the Internet uses a software protocol named TCP/IP to format and transfer data. An attacker can monitor ongoing TCP connections and have all the information in the IP and TCP headers and packet payloads with which to hijack the connection. The attacker, having all the information on the network, can create false packets in the TCP connection.

As a Network Administrator, your daily task is to check the TCP/IP connections of each server you manage. You have to monitor all TCP and UDP ports, and list all the established IP addresses of the server using the CurrPorts tool, and kill any suspicious processes you might find.

Lab Objectives

The objective of this lab is to help students analyze the processes running on the machine, and analyze the ports on which they are running.

Lab Environment

To complete this lab, you will need:

- **njRAT,** located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**
- CurrPorts, located at **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Port Monitoring Tools\CurrPorts**
- You can also download the latest version of CurrPorts from the link http://www.nirsoft.net/utils/cports.html
- If you decide to download the latest version, then screenshots shown in the lab might differ

- A computer running Windows Server 2012
- Windows 8.1 running as a virtual machine
- Administrator privileges to run the CurrPorts application

You can download CurrPorts tool from http://www.nirsoft.net.

Lab Duration

Time: 10 Minutes

Overview of the Lab

The lab demonstrates how to analyze malicious processes running on a machine using CurrPorts. Here, you will first create a server using njRAT, and then execute this server from another machine. Later, you will run CurrPorts application on that machine and find that the process associated with the server is running on it.

Lab Tasks

TASK 1

Create a Server and Execute it on Remote Machine

1. Log into **Windows 8.1** virtual machine, and navigate to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**
2. Launch njRAT, create a server, and save it to **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.
3. While building the server, assign the server name as **Trojan.exe** for demonstration purposes.

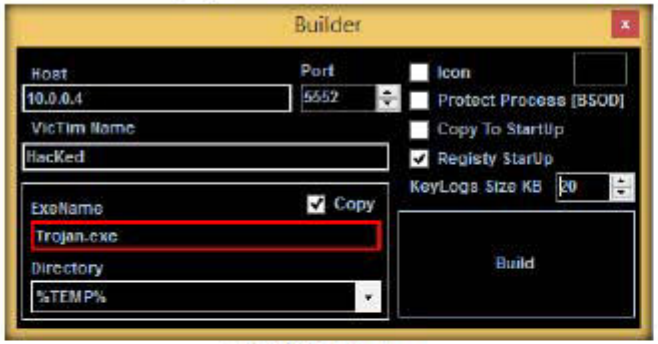


FIGURE 16.1: Building a Server

4. In this lab, we are naming the server **Trojan.exe**.

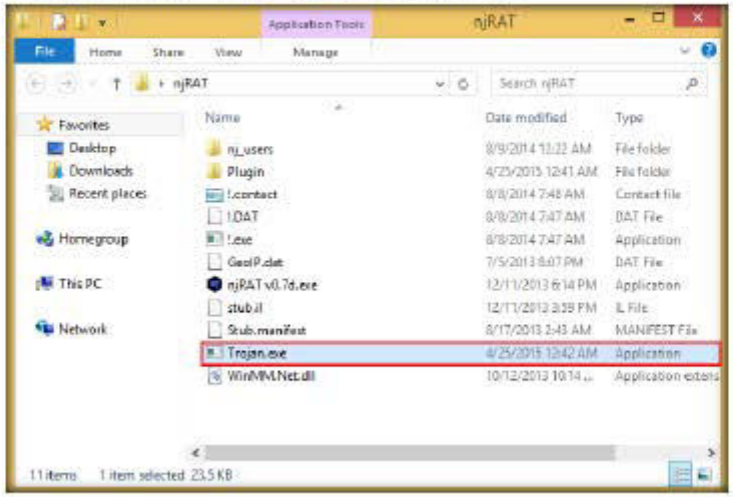


FIGURE 16.2: Server Built

5. Now, place this **Trojan.exe** file in **Z:\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.

6. Switch to the **Windows Server 2012** machine, navigate to **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**, and double-click **Trojan.exe**.

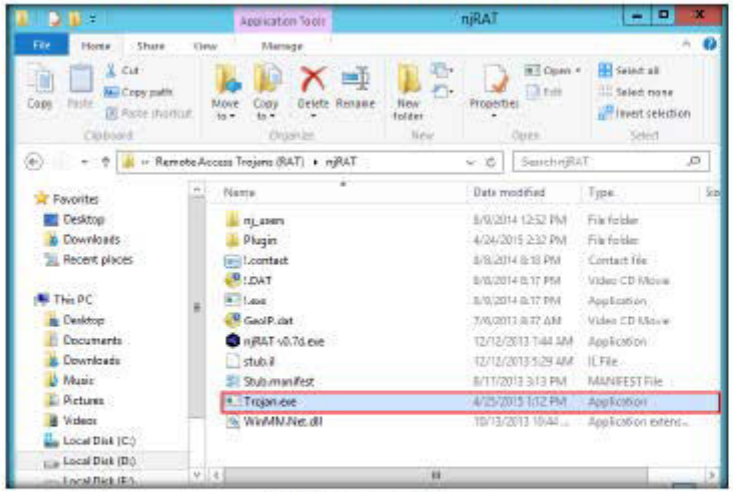


FIGURE 16.3: Sharing the Server

7. Observe that a connection has been established by the njRAT client running on the **Windows 8.1** machine.

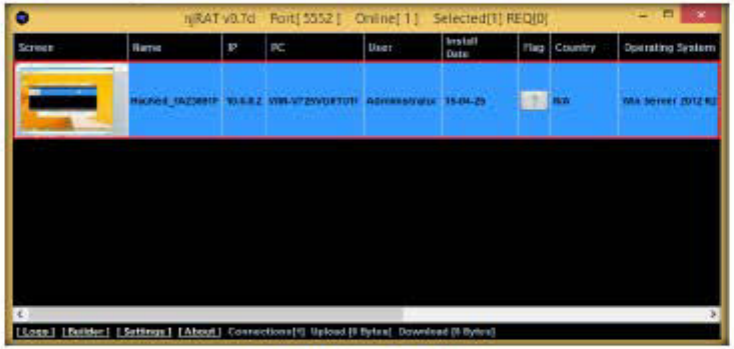


FIGURE 16.4: Connection Established

TASK 2

Examine the Malicious Processes Using CurrPorts

8. Now, let us analyze this process on **Windows Server 2012** using CurrPorts.
9. Switch back to **Windows Server 2012**, navigate to **D:\CEH-Tools\CEHv9 Module 06 Malware Threats\Port Monitoring Tools\CurrPorts**, and double-click **cports.exe**.
10. The CurrPorts window appears, displaying a list of currently opened TCP/IP and UDP ports on the machine. Here, you can observe the **Trojan.exe** process running on the machine, as shown in the screenshot:

CurrPorts utility is a standalone executable, which doesn't require any installation process or additional DLLs.

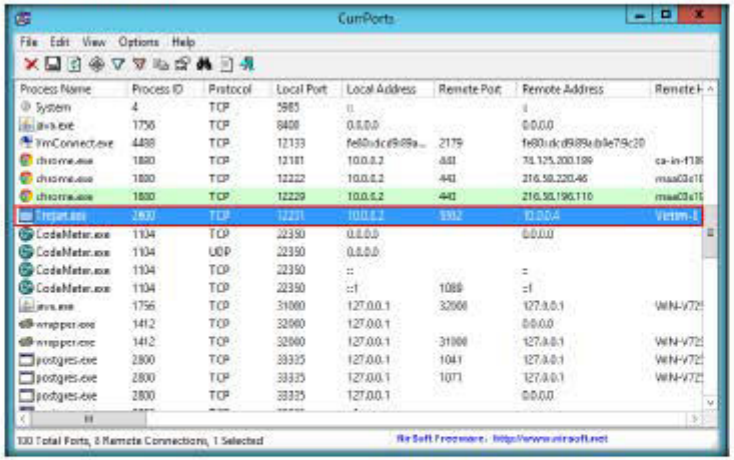


FIGURE 16.5: Viewing the Process

11. It is evident from the above screenshot that the process is connected to the machine on **port 5552**.
12. You can view the properties of the process by right-clicking on the process, and clicking **Properties** in the **Context** menu.

In the lower-left corner of the CurrPorts window, the status of total ports and remote connections is displayed.

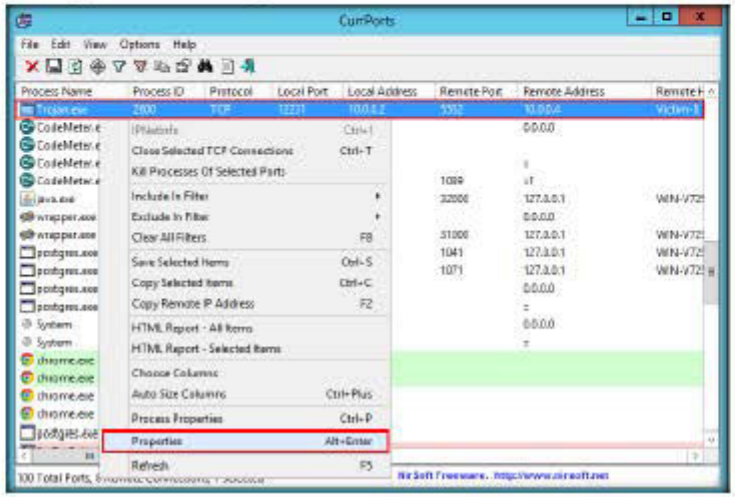
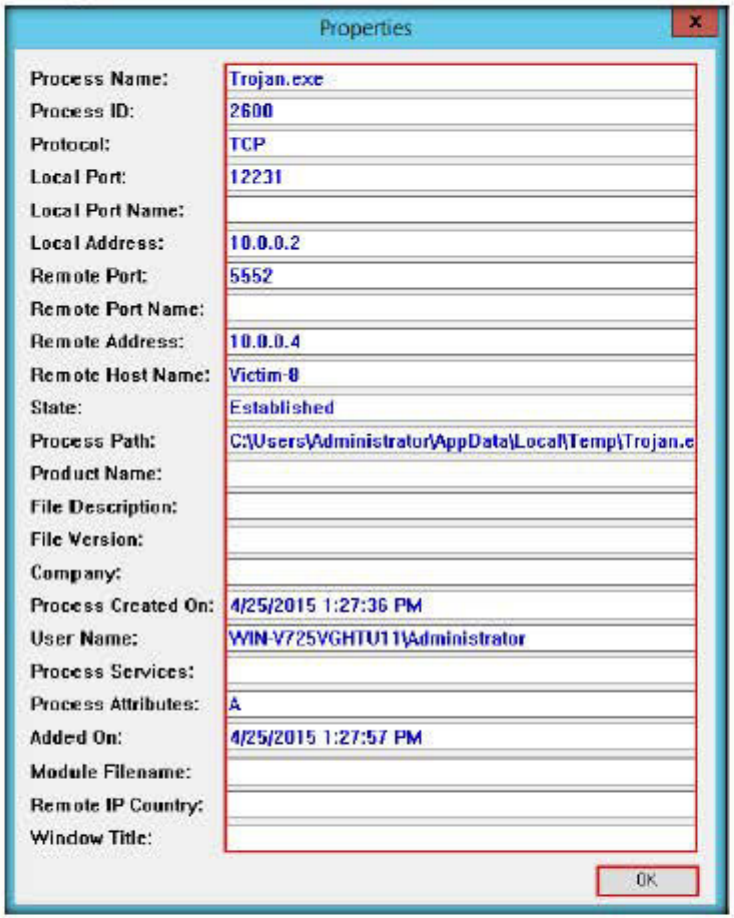


FIGURE 16.6: Viewing the Properties

13. The Properties window appears displaying information related to the process, such as the name of the process, process ID, Remote Address, Process Path, Remote Host name, and so on.

14. Once you are done examining the properties associated with the process, click **OK**.



CurrPorts Features:

Free network monitoring software for Windows.

Displays extensive information on TCP/IP and UDP connections on your system.

Displays all kind of ports (established, listening, or closed).

Lets you kill specific processes with just one click.

Displays process properties on double click on its table entry.

FIGURE 16.7: Examining the Properties

TASK 3

Kill the Malicious Process

15. Because **Trojan.exe** is a malicious process, you may end the process by right-clicking on it, and selecting **Kill Processes Of Selected Ports** in the context menu.
16. Alternatively, you may even select **Close Selected TCP Connections**, so that the port closes, and the attacker can never attain connection through the port, unless you open it.

In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP ports information to HTML file, XML file, or to tab-delimited text file.

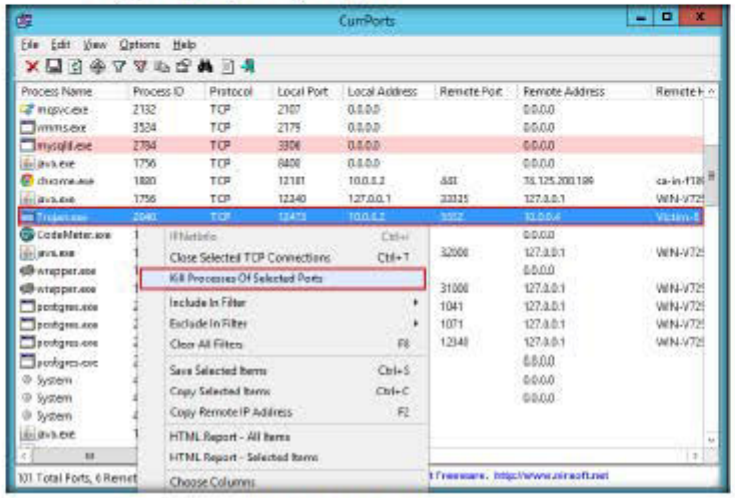


FIGURE 16.8: Killing the Process

17. The **CurrPorts** dialog-box appears; click **Yes** to close the connection.

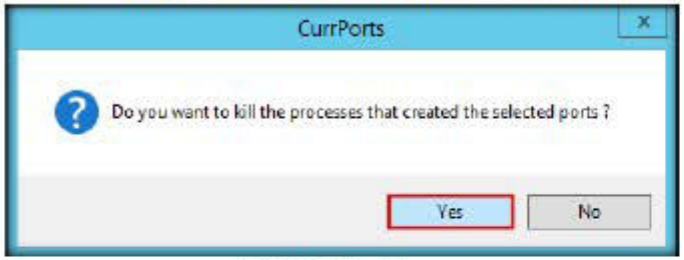


FIGURE 16.9: Killing the Process

18. This way, you can analyze the ports open on a machine and analyze the processes running on it.
19. If the process is found to be suspicious, you may either kill the process or close the port.

Lab Analysis

Document all the IP addresses, open ports and their running applications, and protocols discovered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs