System Hacking

Module 06

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)

- 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.

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		√	√

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.

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

- 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.

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.

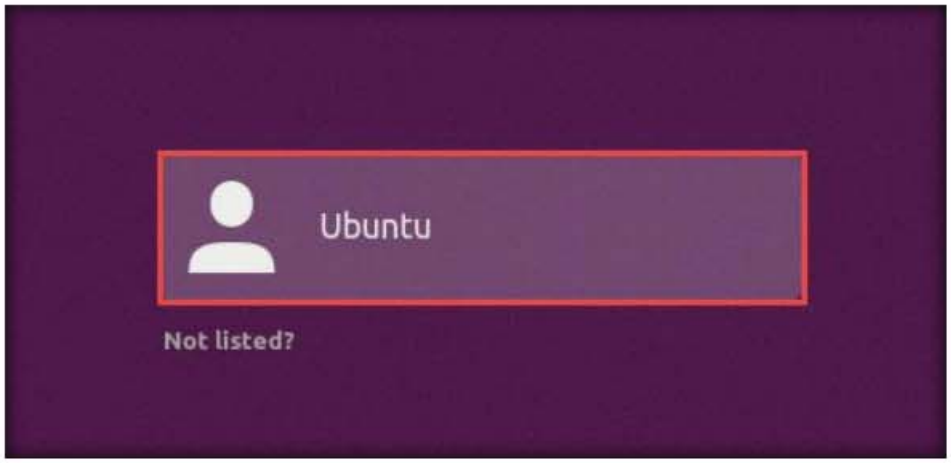

Figure 1.1.1: Click on Ubuntu button to login

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.

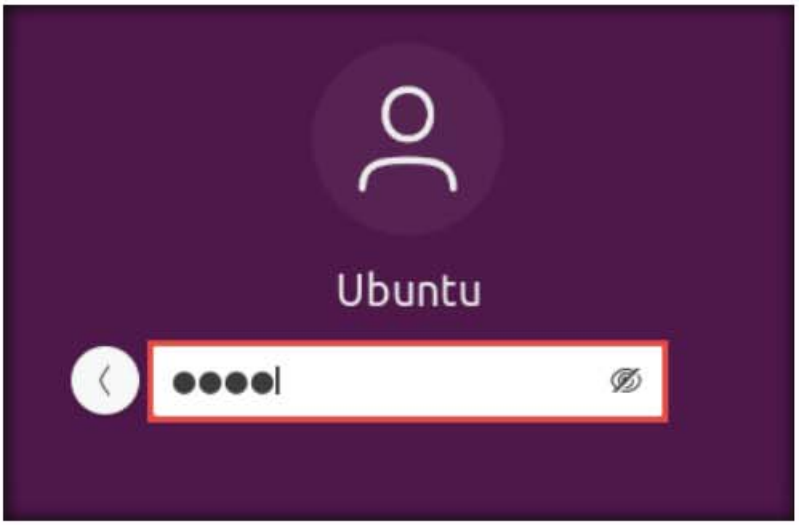

Figure 1.1.2: Login as the root user

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.

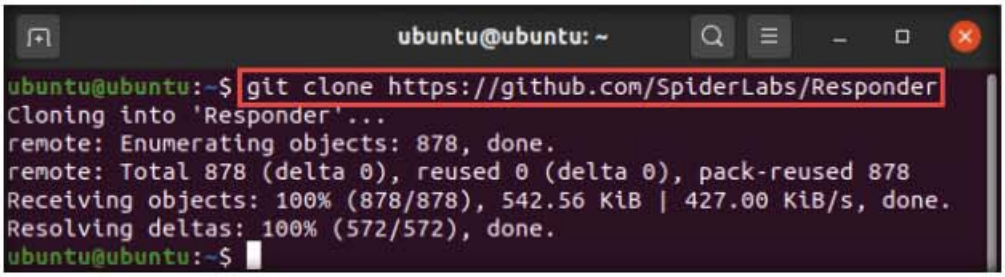

Figure 1.1.4: Cloning Responder tool

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:

- 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.

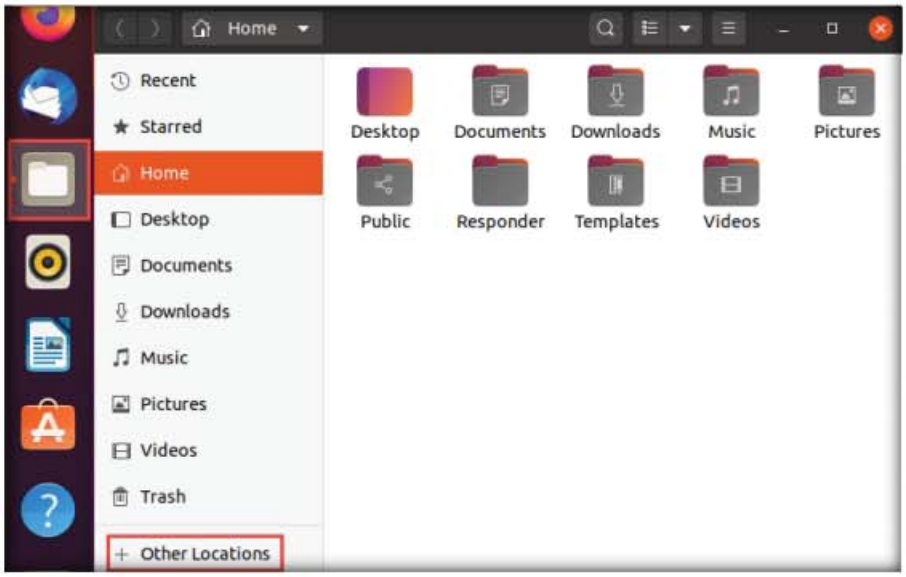

Figure 1.1.5: Open Other Locations

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

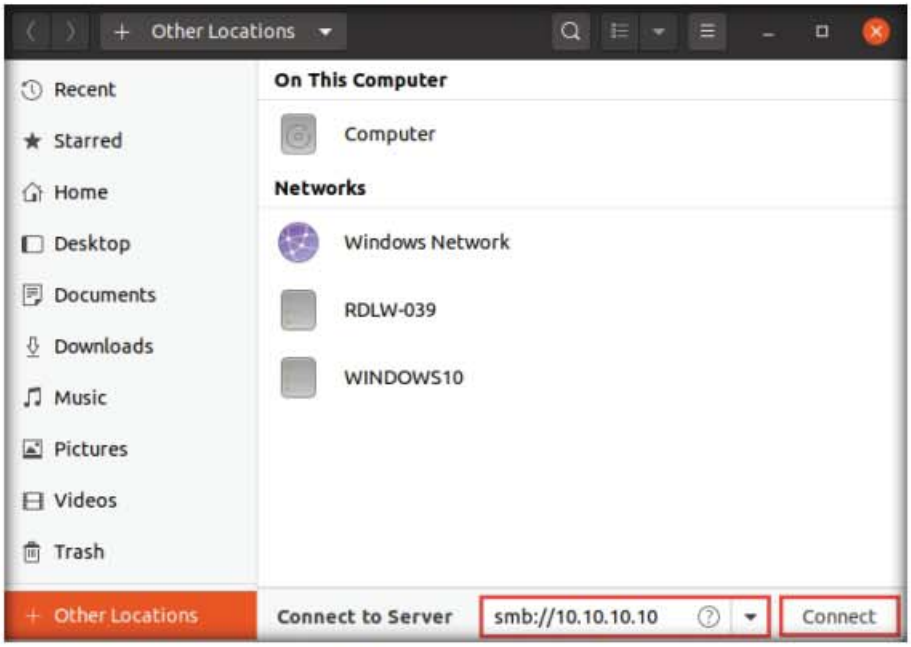

Figure 1.1.6: + Other Locations window

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

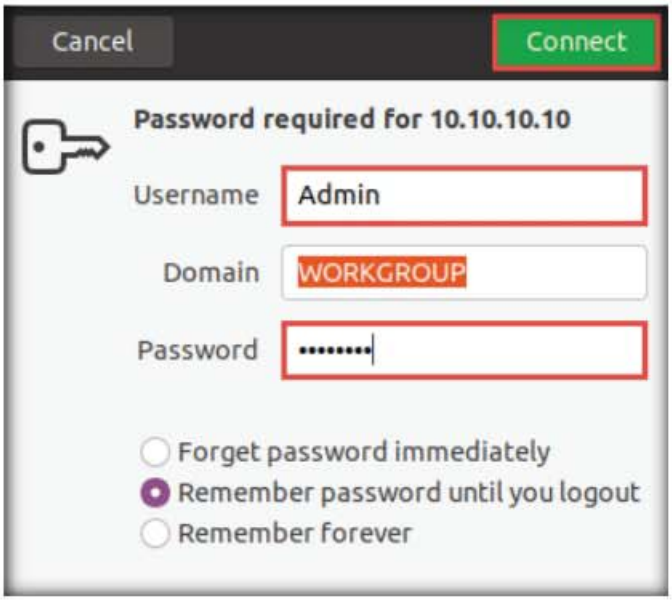

Figure 1.1.7: Security pop-up

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.

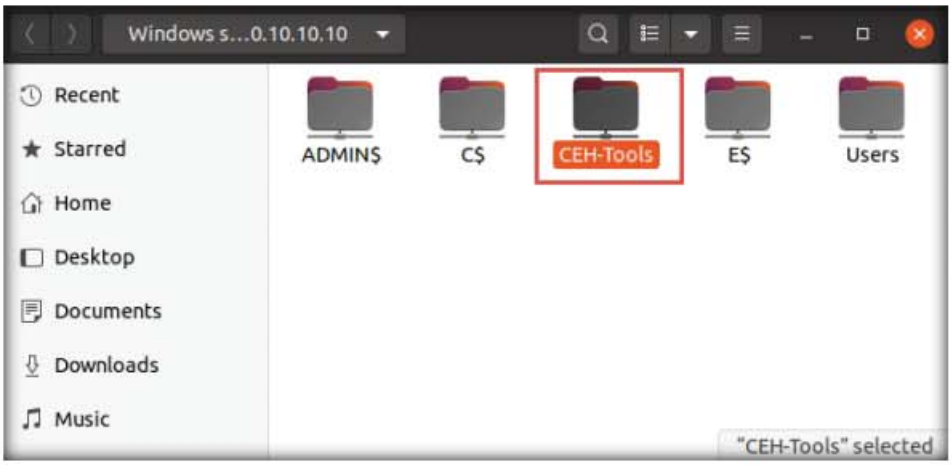

Figure 1.1.8: Windows 10: shared folders

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

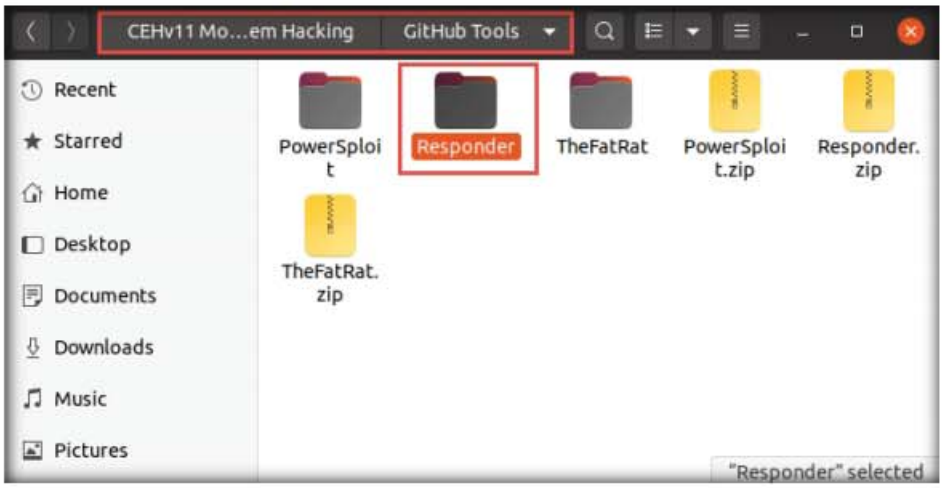

Figure 1.1.9: Copy Responder folder

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

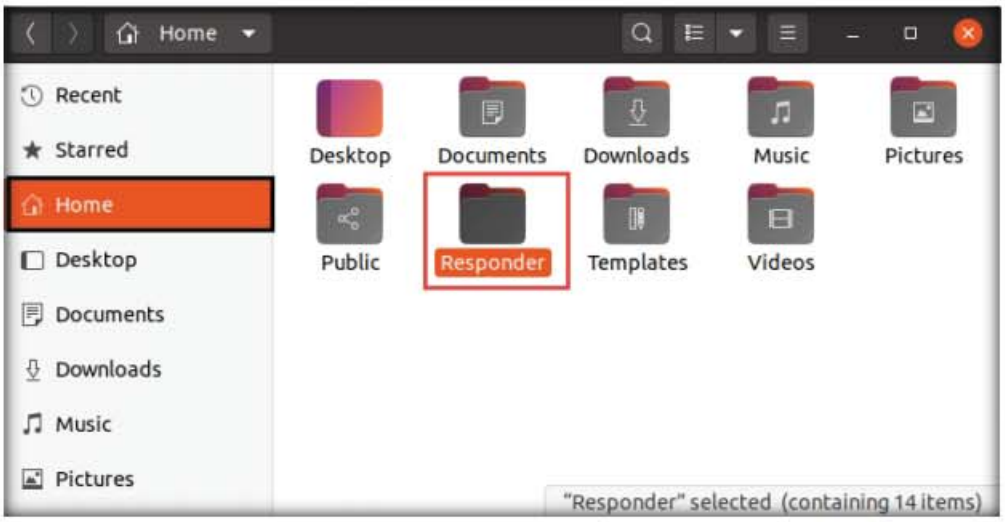

Figure 1.1.10: Paste Responder folder

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**.

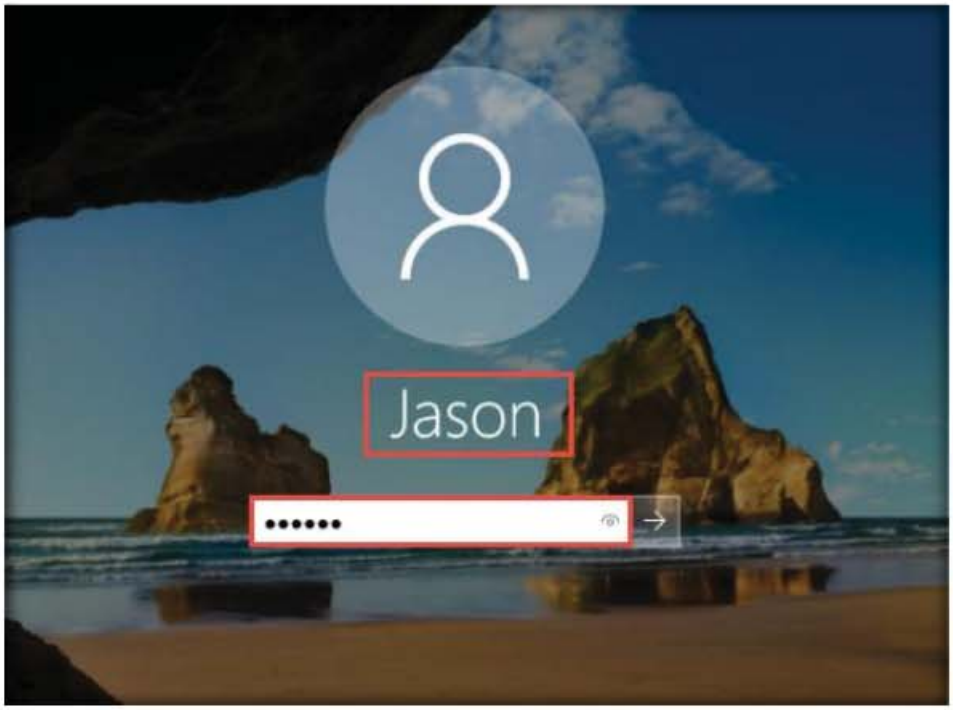

Figure 1.1.11: Login as Jason

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.

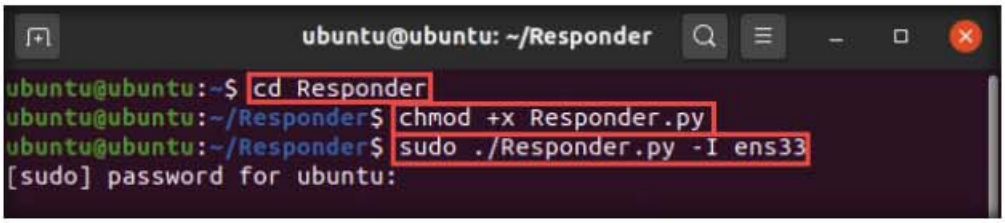

Figure 1.1.12: Running Responder tool

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

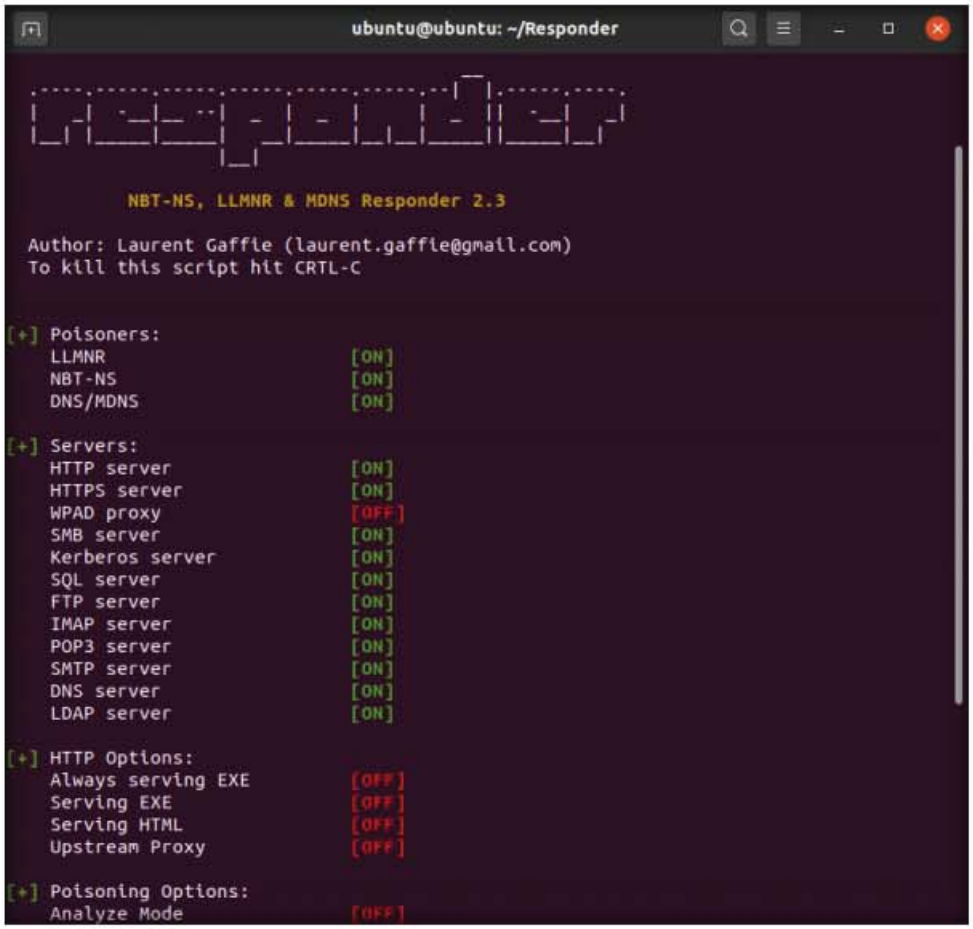

Figure 1.1.13: Responder starts listening

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**.

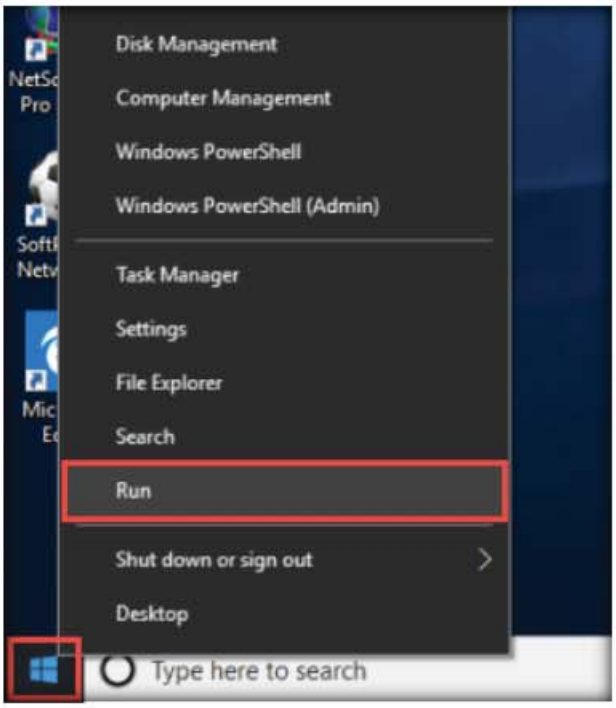

Figure 1.1.14: Launching the Run window

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

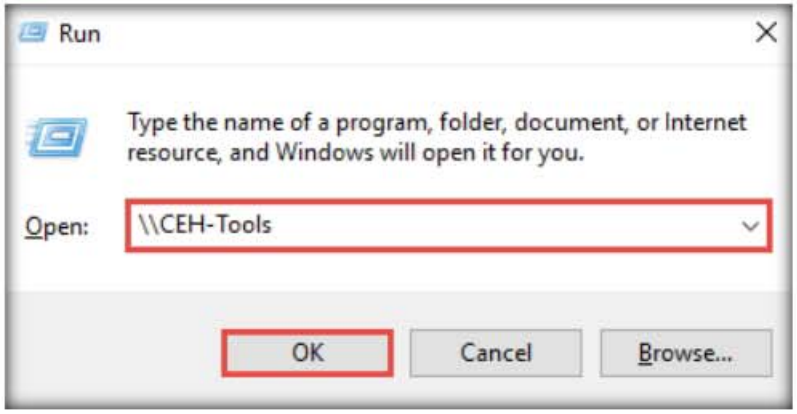

Figure 1.1.15: Run window

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

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.

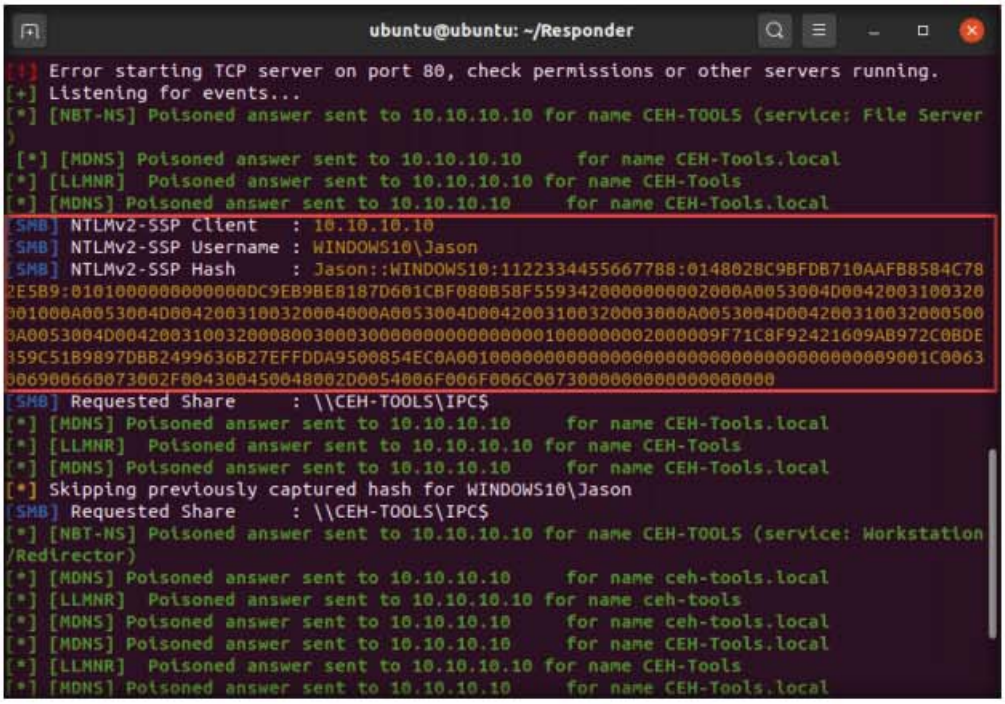

Figure 1.1.16: Hash obtained by Responder

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.

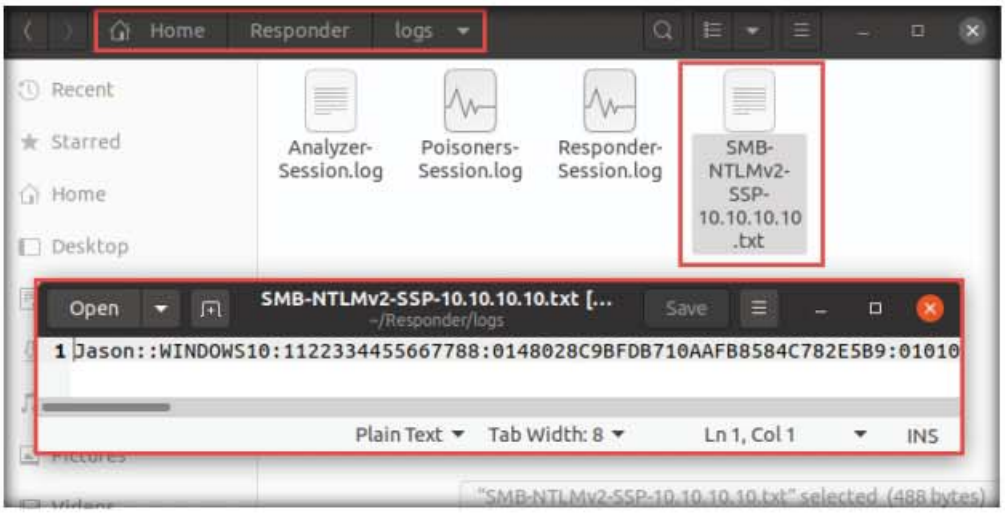

Figure 1.1.17: Responder log file

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.

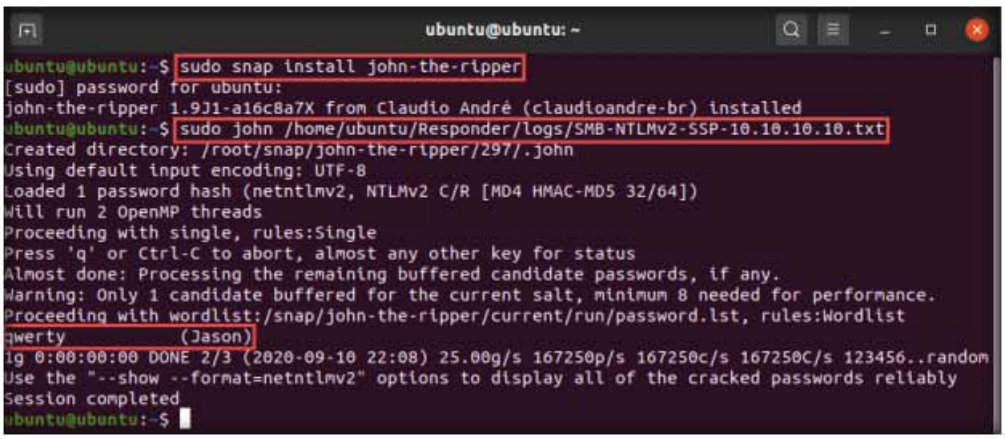

Figure 1.1.18: Password cracked successfully

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.

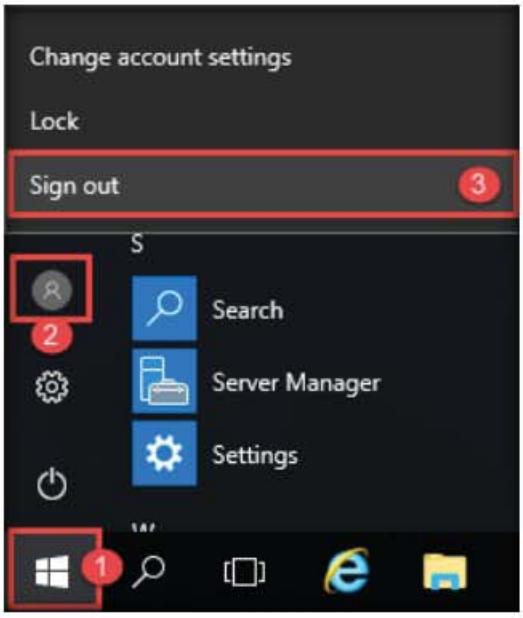

Figure 1.1.19: Sign out

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

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**.

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.

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

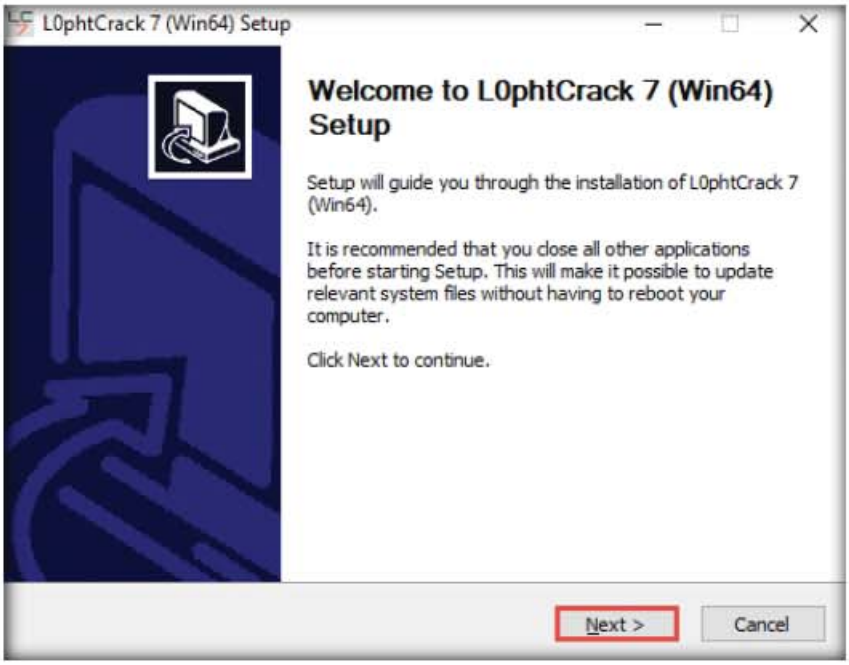

Figure 1.2.1: L0phtCrack Setup window

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.

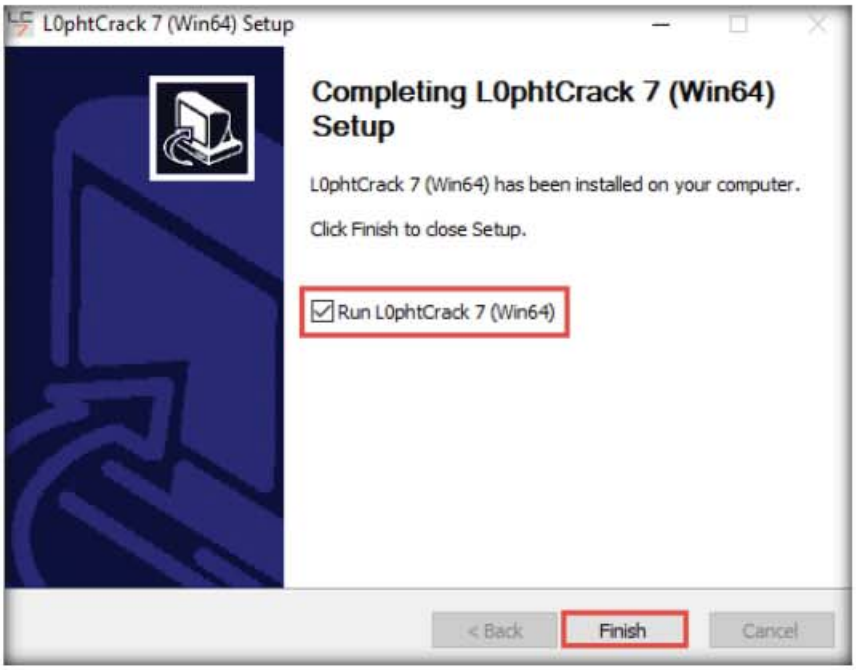

Figure 1.2.2: L0phtCrack Setup window: click Finish

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

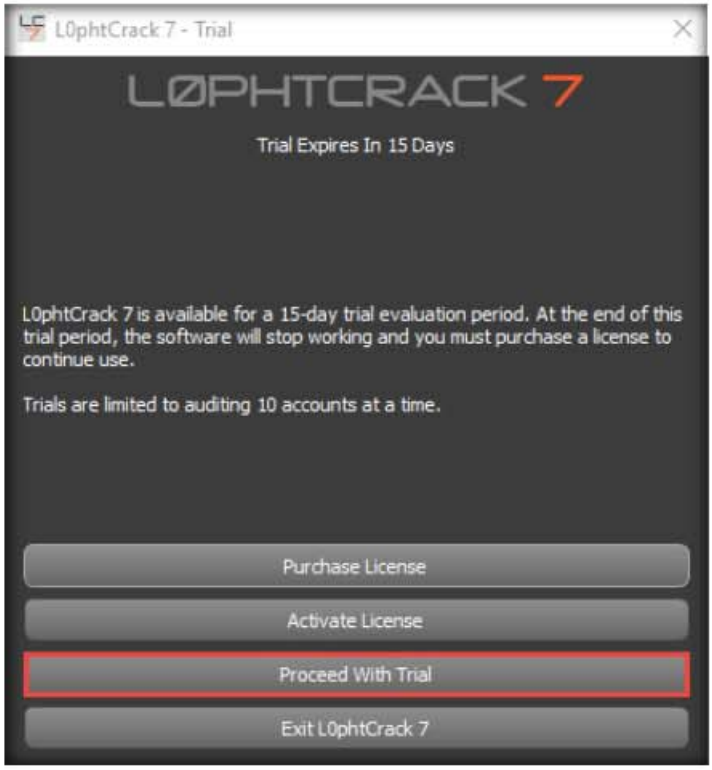

Figure 1.2.3: L0phtCrack7-Trial window

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

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

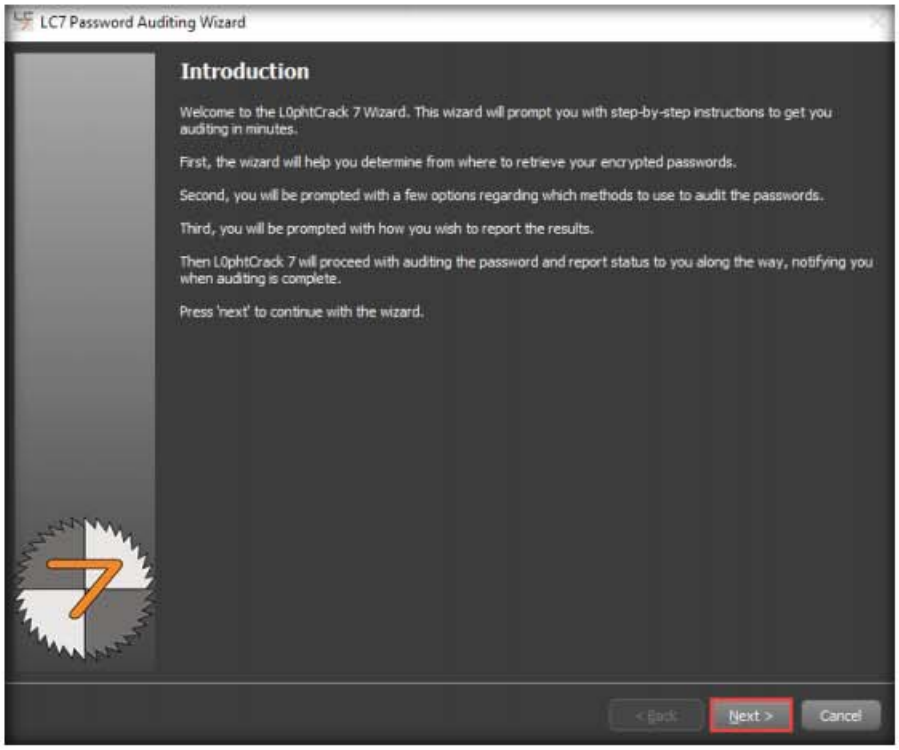

Figure 1.2.5: Password auditing wizard window

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

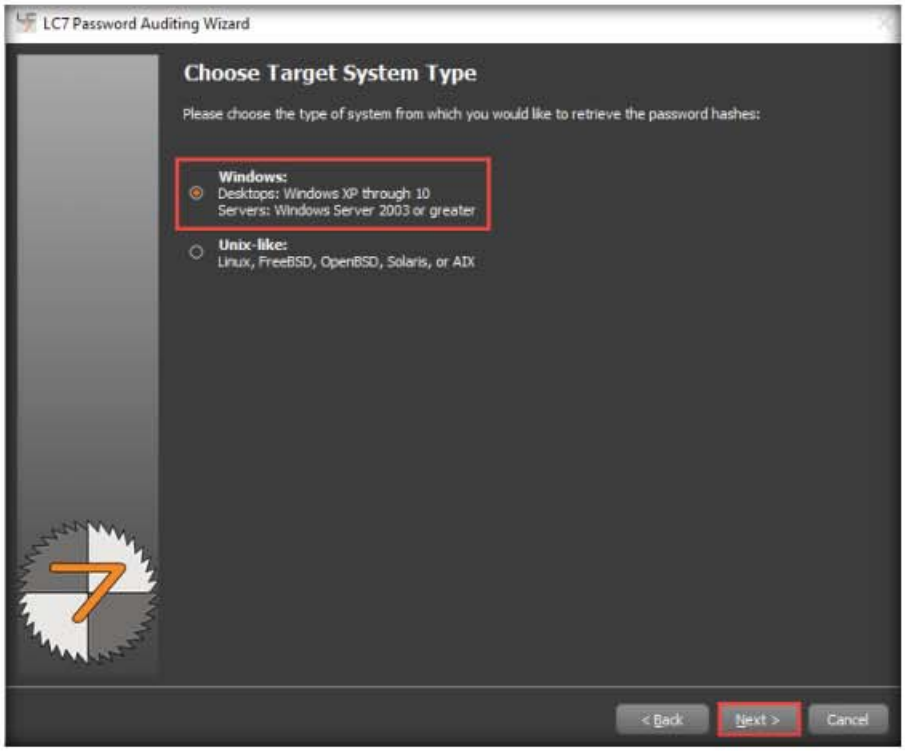

Figure 1.2.6: Choose target system type option

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

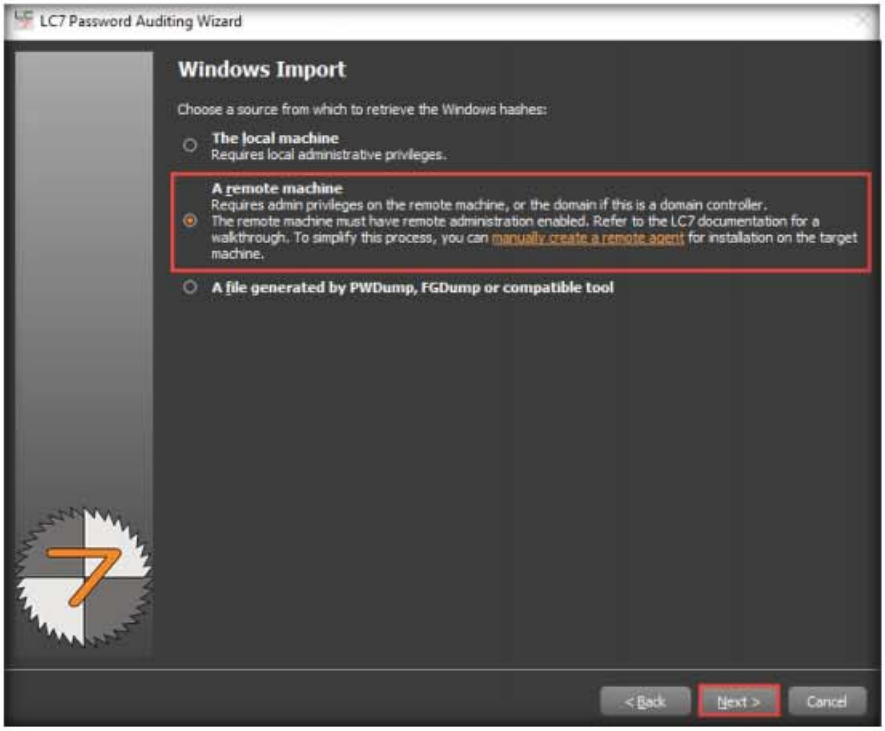

Figure 1.2.7: Windows import option

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.

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

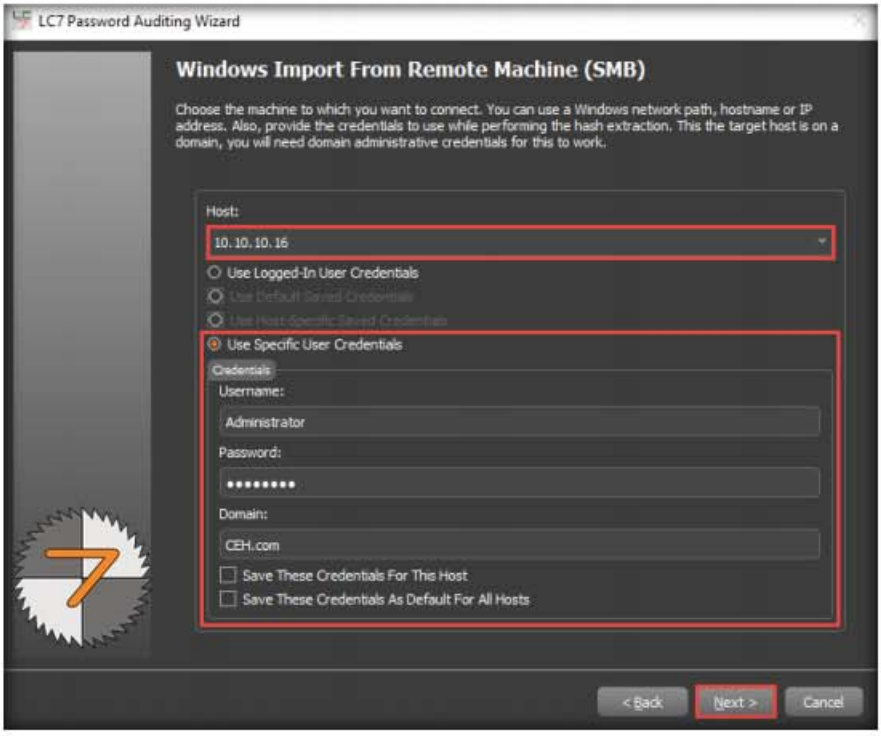

Figure 1.2.8: Windows import from remote machine (SMB) menu

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

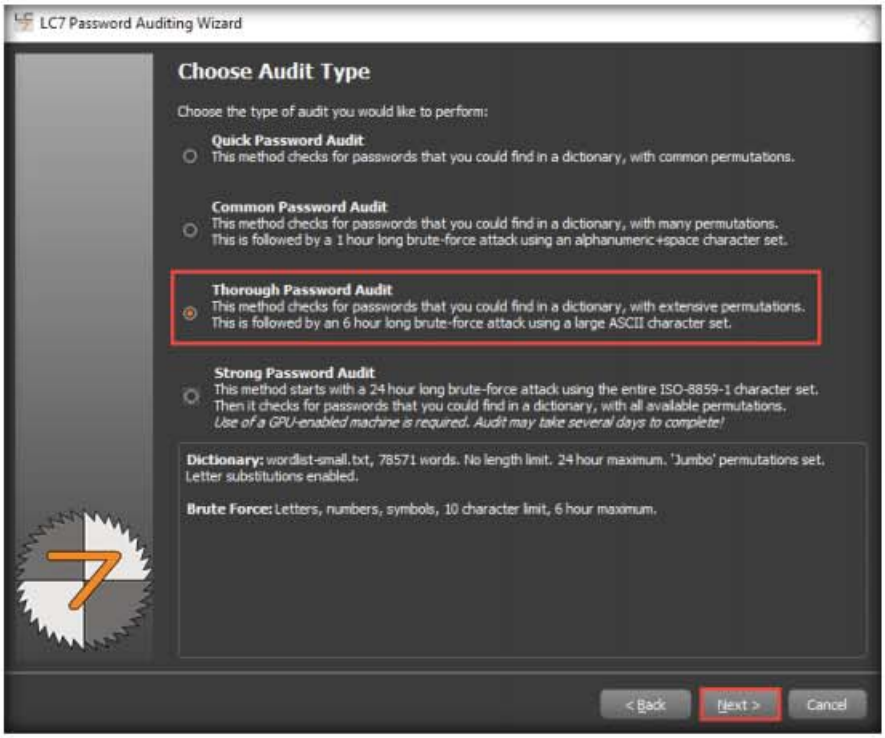

Figure 1.2.9: Choose the audit type section of the LC7 wizard

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.

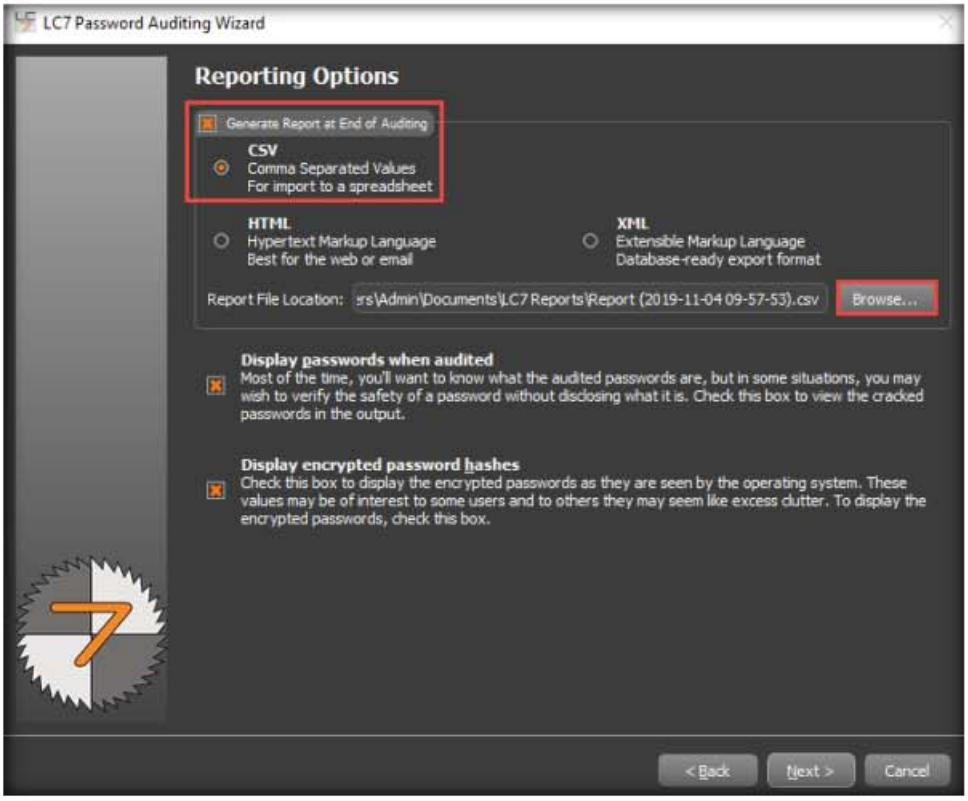

Figure 1.2.10: Reporting options section

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

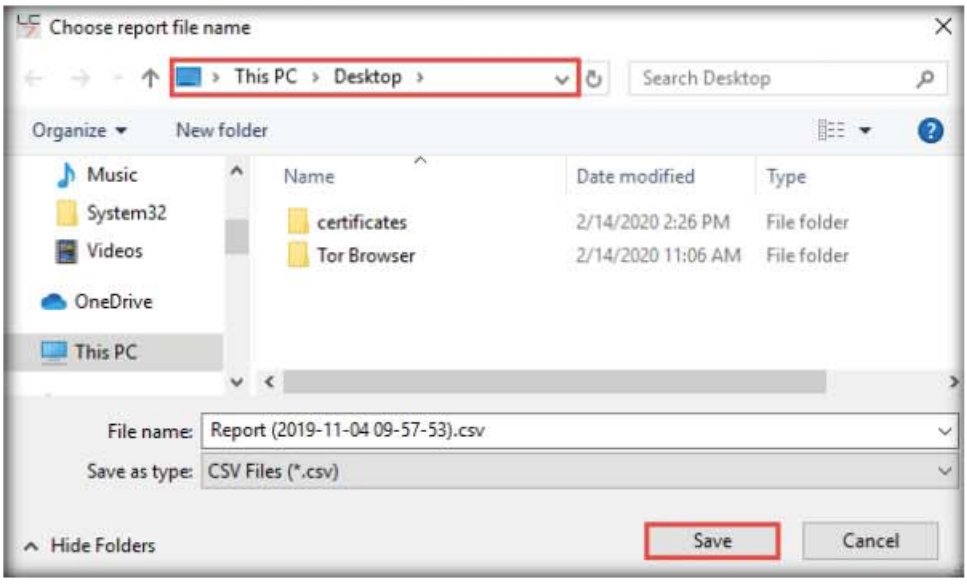

Figure 1.2.11: Choose report filename window

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

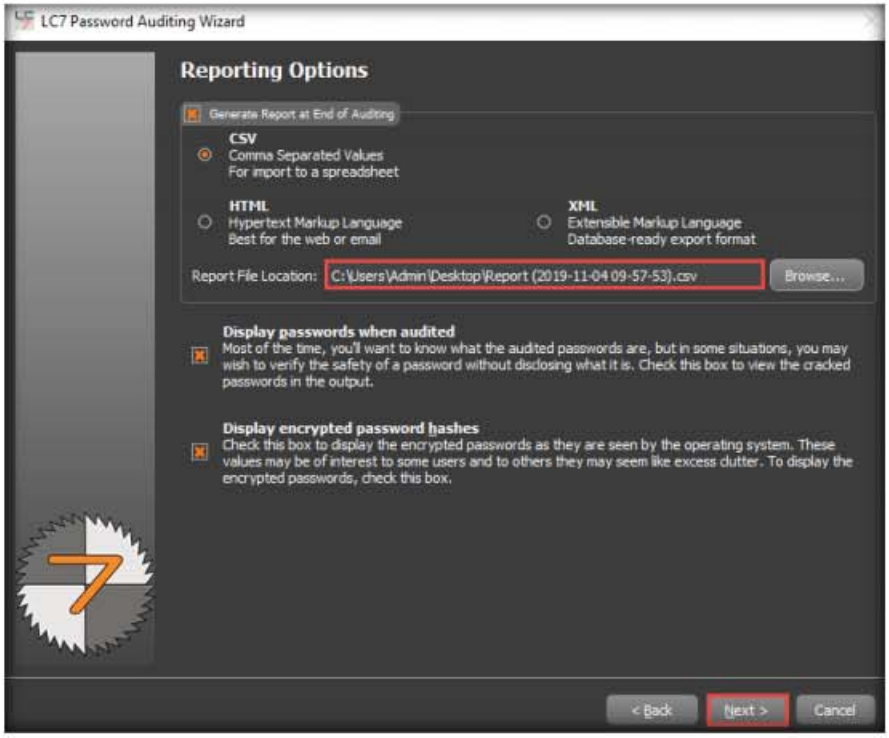

Figure 1.2.12: Reporting options section

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

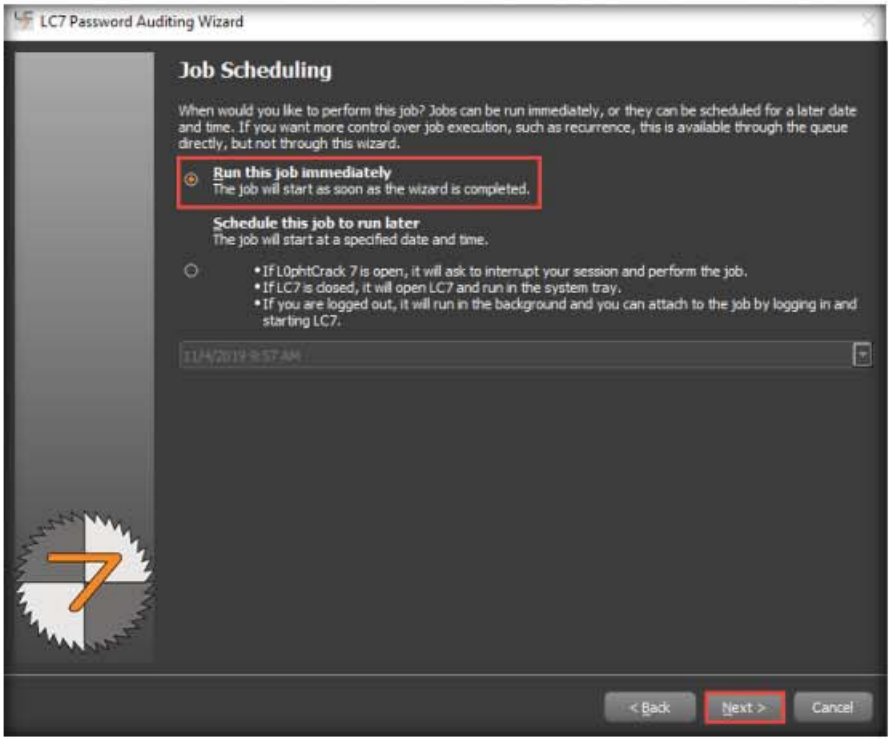

Figure 1.2.13: Job scheduling option

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

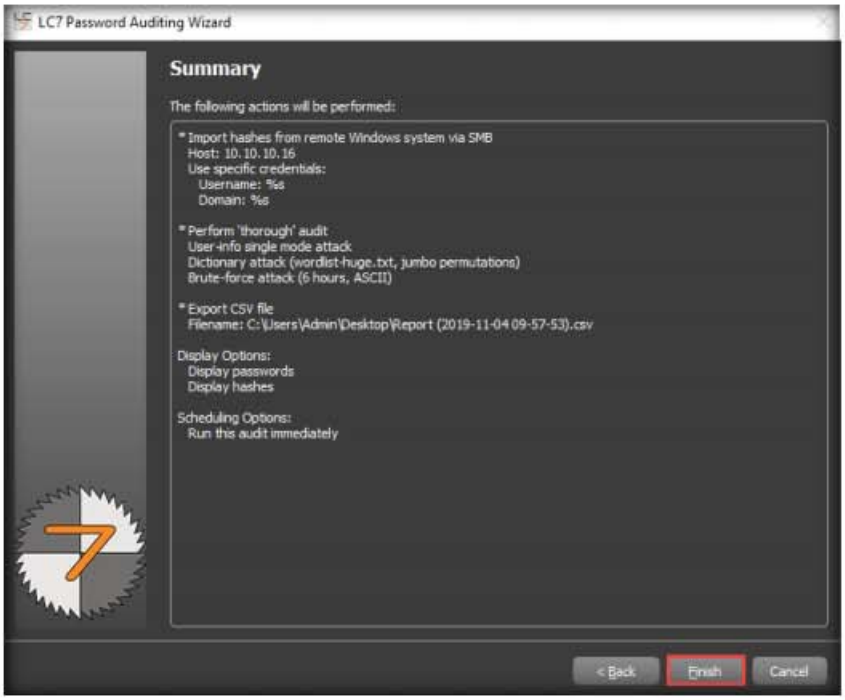

Figure 1.2.14: Summary option

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.

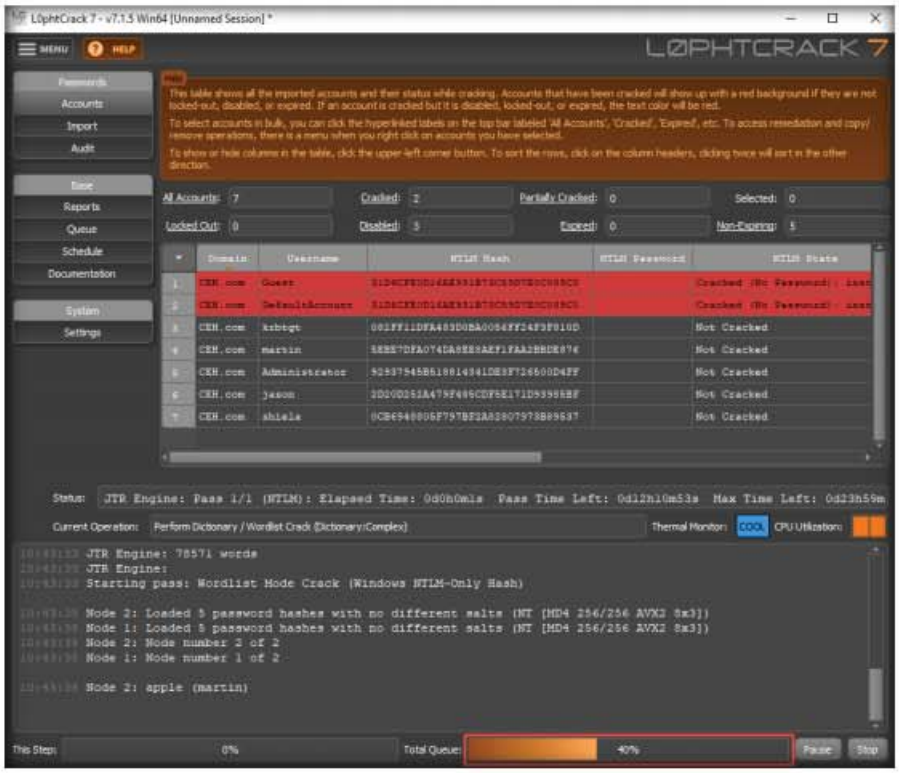

Figure 1.2.15: Cracking password in progress

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.

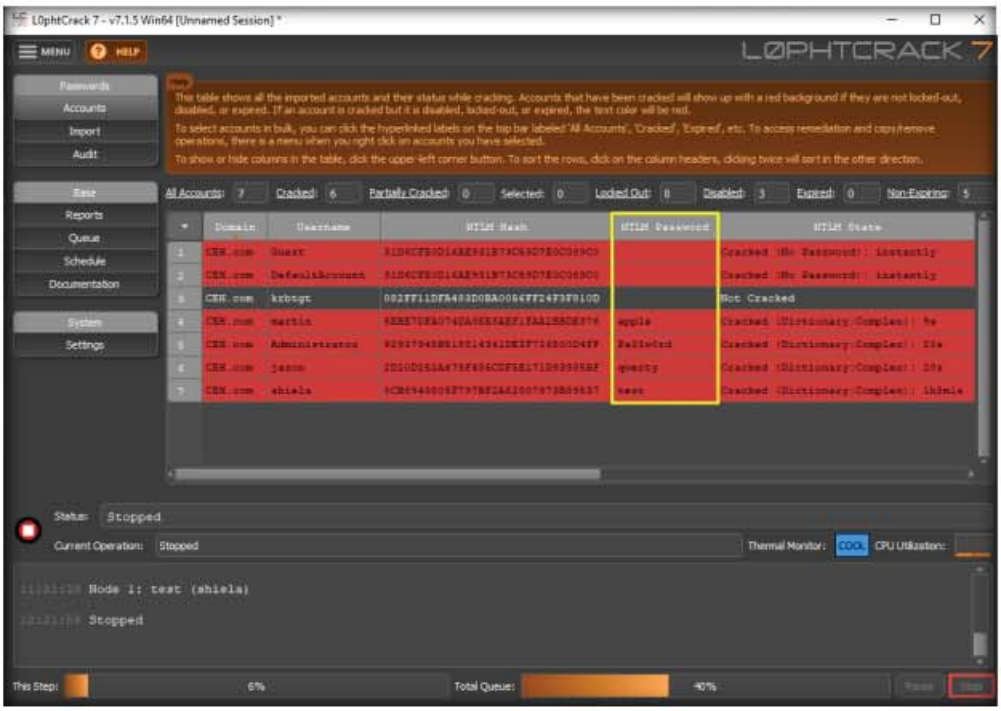

Figure 1.2.16: Passwords successfully cracked

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/**.