Enumeration

Module 04

Enumeration

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system, and is conducted in an intranet environment.

Lab Scenario

With the development of network technologies and applications, network attacks are greatly increasing both in number and severity. Attackers always look for Service vulnerabilities: Application vulnerabilities on a network or servers. If attackers find a flaw or loophole in a service run over the Internet, they will immediately use it to compromise the entire system and other data found, and thus compromise other network systems. Similarly, if they find a workstation with administrative privileges with faults in that workstation's applications, they can execute an arbitrary code or implant viruses to intensify the damage to the network.

As a key technique in the network security domain, an Intrusion Detection System (IDS) plays a vital role in detecting various kinds of attacks and securing the networks. Therefore, as an administrator, you should make sure that services do not run as the root user, and you should be cautious of patches and updates for applications from vendors or security organizations such as CERT and CVE. Safeguards can be implemented so that email client software does not automatically open or execute attachments.

In the first step of a security assessment and penetration testing of your organization, you have collected open-source information about your organization. Now, you need to perform enumeration on the network. In this step, you have to probe the target network further to collect more details, such as network machines, users, and shared folders. As an Expert Ethical Hacker and Penetration Tester you must know how to enumerate target networks and extract lists of computers, user names, user groups, ports, operating systems, machine names, network resources, and services, using various enumeration techniques.

Lab Objectives

The objective of this lab is to provide expert knowledge on network enumeration and other responsibilities that include:

- User name and user groups
- Lists of computers, their operating systems, and ports
- Machine names, network resources, and services
- Lists of shares on individual hosts on the network
- Policies and passwords

Lab Environment

To complete this lab, you will need:

- Windows Server 2016, Windows Server 2012, Windows 10, Windows 8 and Kali Linux as virtual machines
- A Web browser with an Internet connection
- Administrative privilege to run tools

Lab Duration

Time: 80 Minutes

Overview of Enumeration

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system, and is conducted in an intranet environment.

Lab Tasks

Recommended labs to assist you in enumeration are:

- NetBIOS Enumeration using **Global Network Inventory**
- Enumerating Network Resources using **Advanced IP Scanner**
- Performing Network Enumeration using **SuperScan**
- Enumerating Resources in a Local Machine using **Hyena**
- Performing Network Enumeration using **NetBIOS Enumerator**
- Enumerating a Network using **SoftPerfect Network Scanner**
- Enumerating a Target Network using **Nmap** and **Net Use**
- Enumerating Services on a **Target Machine**
- SNMP Enumeration using **snmp_enum**
- LDAP Enumeration using **Active Directory Explorer** (**ADExplorer**)
- Enumerating Information from Windows and Samba Host using **Enum4linux**

Lab Analysis

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

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

Lab 1

NetBIOS Enumeration using Global Network Inventory

Global Network Inventory is used as an audit scanner in zero deployment and agent-free environments. It scans computers by IP range, by domain, and single or multiple computers, as defined by the Global Network Inventory host file.

Lab Scenario

The first step of enumeration is to collect the names of the machines in the network, including switches, network printers, document centers, and so on. Later, you will probe these machines for detailed information about the network and host resources. In this lab, you will learn how networks are scanned using the Global Network Inventory tool.

Lab Objectives

This lab will show you how networks can be scanned and how to use Global Network Inventory.

Lab Environment

To complete this lab, you will need:

- Global Network Inventory, located at **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory**
- You can download the latest version of Global Network Inventory from this link **http://www.magnetosoft.com/products/global_network_inventory/gni_features.htm/**
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2016 as the attacker machine
- Another computer running Window Server 2012 as the victim machine
- A Web browser with Internet access

- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Global Network Inventory

Global Network Inventory is one of the de facto tools for security auditing and testing of firewalls and networks. It is also used for Idle Scanning.

Lab Tasks

1. Navigate to **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory** and double-click **gni_setup.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. The **Global Network Inventory Installation Wizard** appears. Follow the steps to install the application.

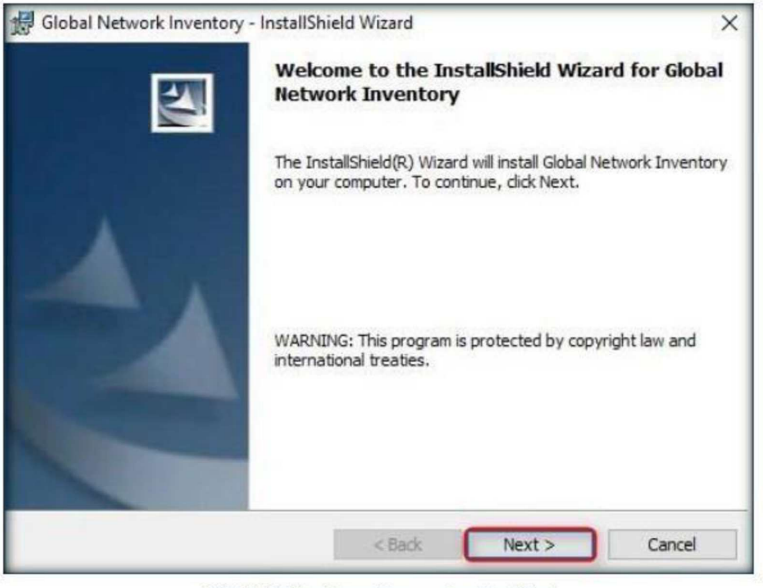

FIGURE 1.1: Global Network Inventory Installation Wizard

4. On completing the installation, launch **Global Network Inventory** from the **Apps** screen.

Note: If the application launches automatically after installation, skip to **step 5**.

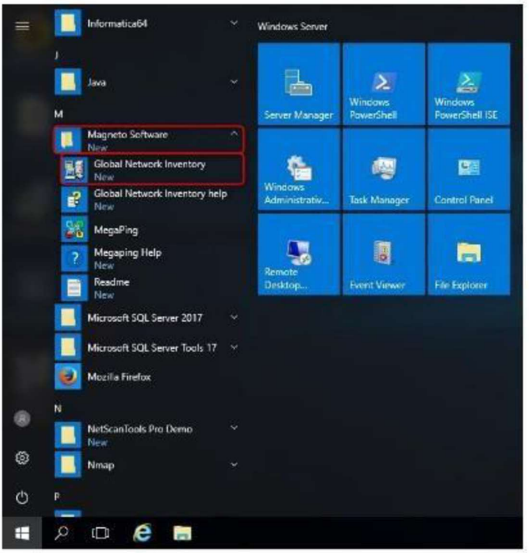

FIGURE 1.2: Run Global Network Inventory from start menu

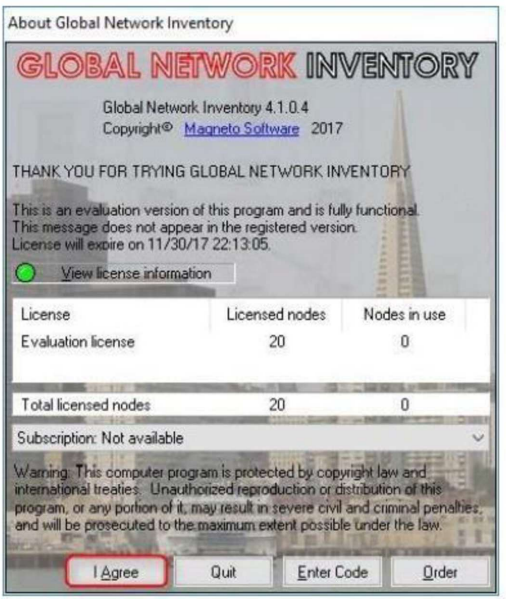

FIGURE 1.3: Global Network Inventory License information screen

5. The **Global Network Inventory** GUI appears, along with a **Tip of the Day** pop-up; click **Close**.

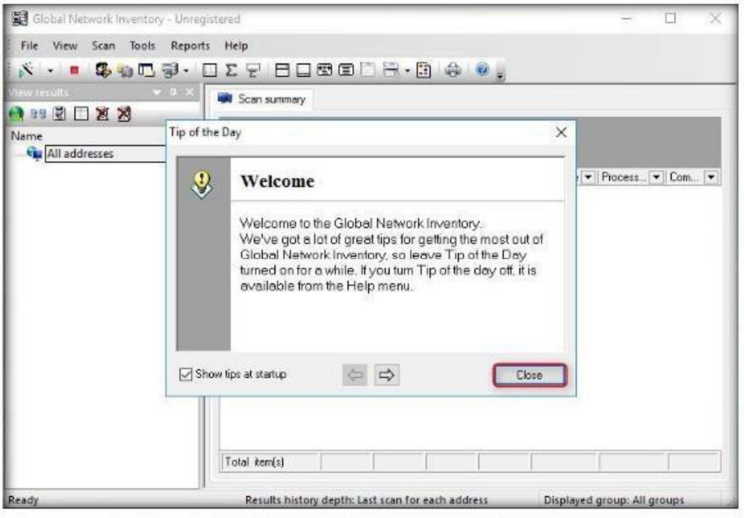

FIGURE 1.4: Global Network Inventory main window

6. Log into the **Windows Server 2012** virtual machine from Vmware Workstation.

7. Now, switch back to the host machine. The **New Audit Wizard** window appears; click **Next**.

FIGURE 1.5: Global Network Inventory new audit wizard

8. The **Audit Scan Mode** section appears; select **IP range scan** and click **Next**.

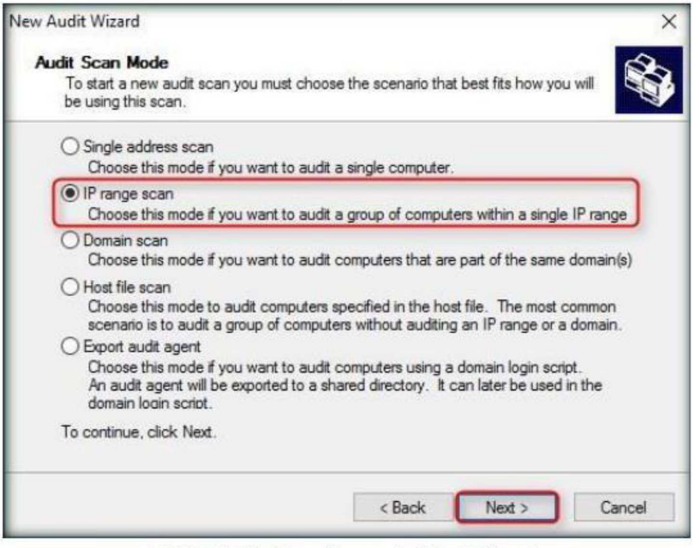

FIGURE 1.6: Global Network Inventory Audit Scan Mode section

9. The **IP Range Scan** section appears. Set an **IP range** and click **Next**.

Note: The IP range might differ in your lab environment.

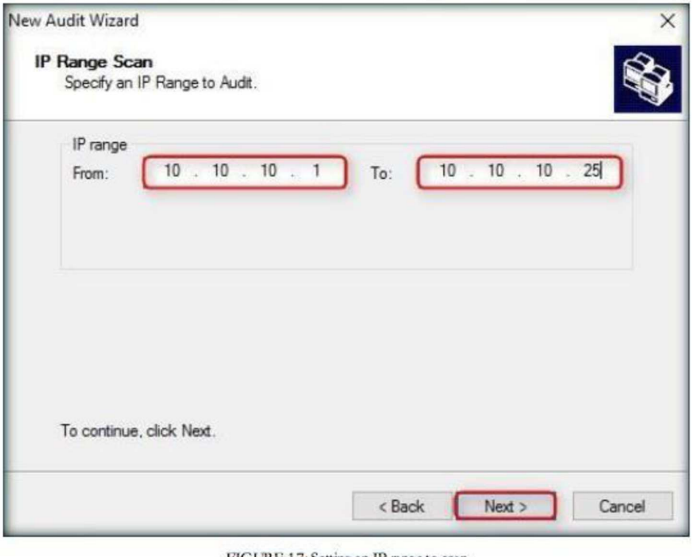

FIGURE 1.7: Setting an IP range to scan

10. The **Authentication Settings** section appears; select **Connect as,** enter the credentials of **Windows Server 2012** virtual machine, and click **Next.**

Note: In real time, attackers do not know the credentials of the remote machine/machines. In such case, they simply choose the **Connect as currently logged on user** option and perfom a scan to determine which mahcines are active in the network. In such case, they will not be able to extract information about the target except its IP and MAC addresses. So, they might use tools such as Nmap to gather information about open ports and services running on them. This lab is just for assessment purpose, so we have directly entered the credentials of the remote machine and are able to access the inventory Global Network Inventory application.

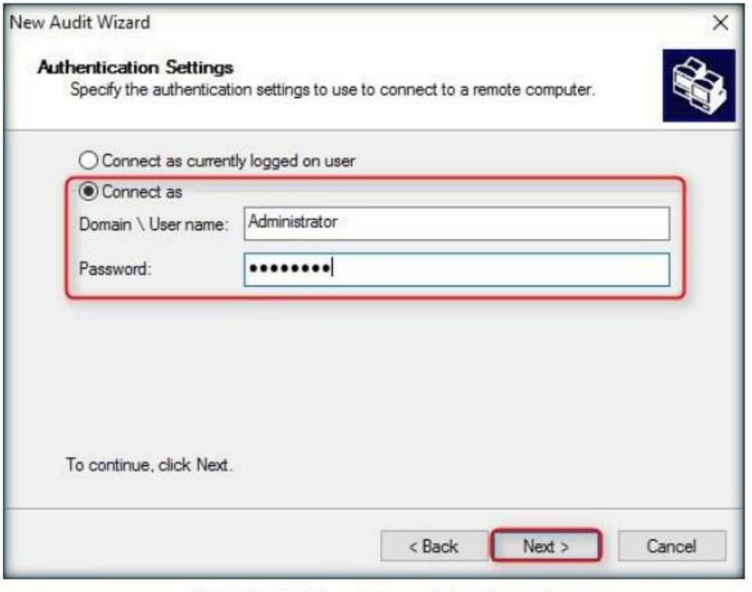

FIGURE 1.8: Global Network Inventory Authentication settings

11. Leave the default settings and click **Finish** in the final step of the wizard.

FIGURE 1.9: Global Network Inventory final Audit wizard

12. It displays the **Scanning progress** in the **Scan progress** window.

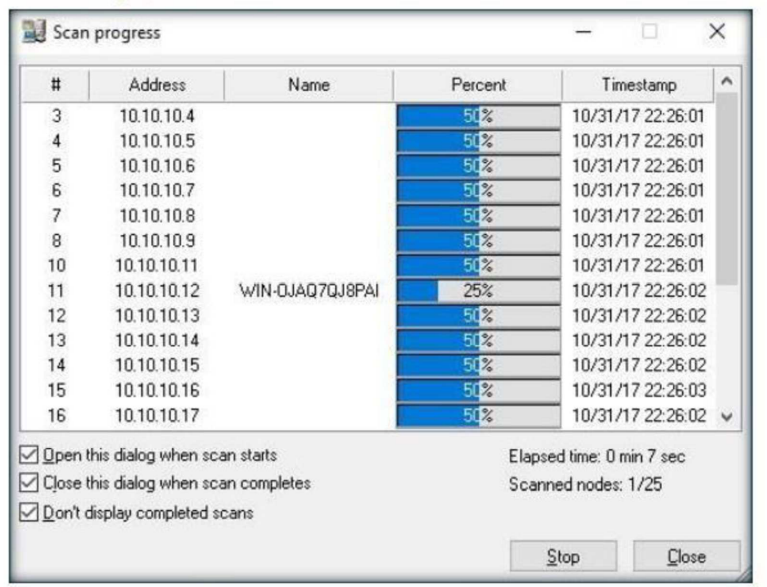

FIGURE 1.10: Global Network Inventory Scanning Progress

13. Once scanning is completed, the scanning results are displayed, as shown in the following screenshot:

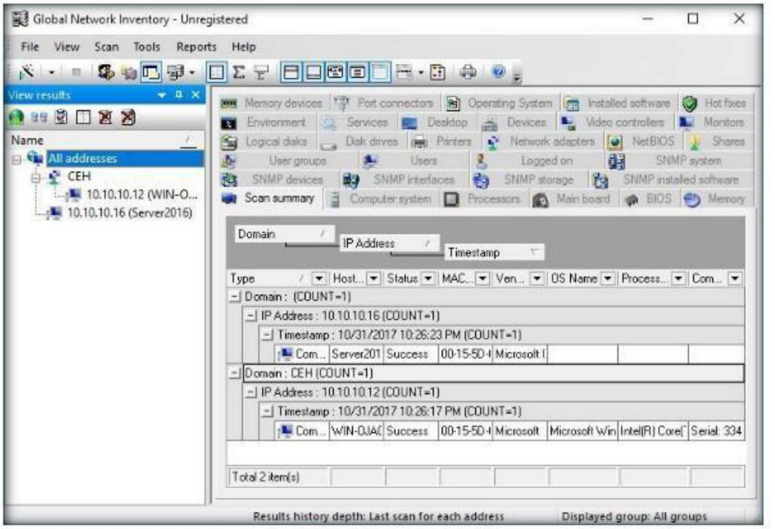

FIGURE 1.11: Global Network Inventory result window

Note: The scan result and the summary of the scan in each tab might vary in your lab environment.

14. Now select the IP address of **Windows Server 2012** (**10.10.10.12**) virtual machine in the left pane, under **View results**, to view individual results.

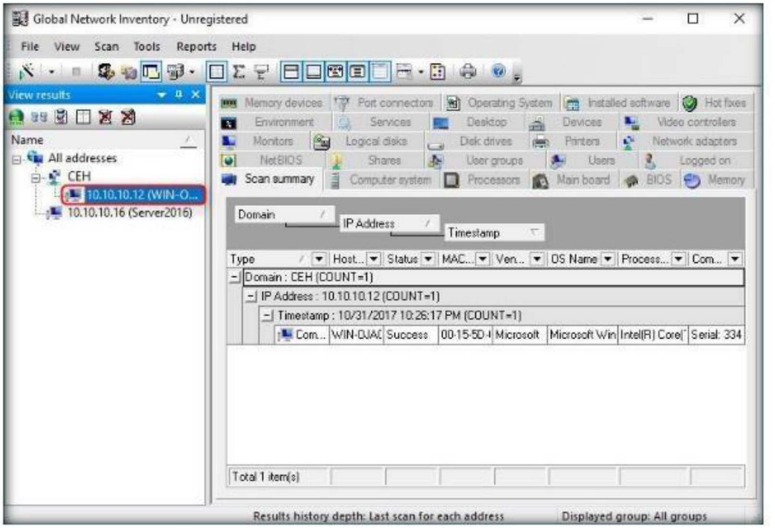

FIGURE 1.12: Global Network Inventory Individual machine results

15. The **Scan summary** tab displays a brief summary of machine that has been scanned.

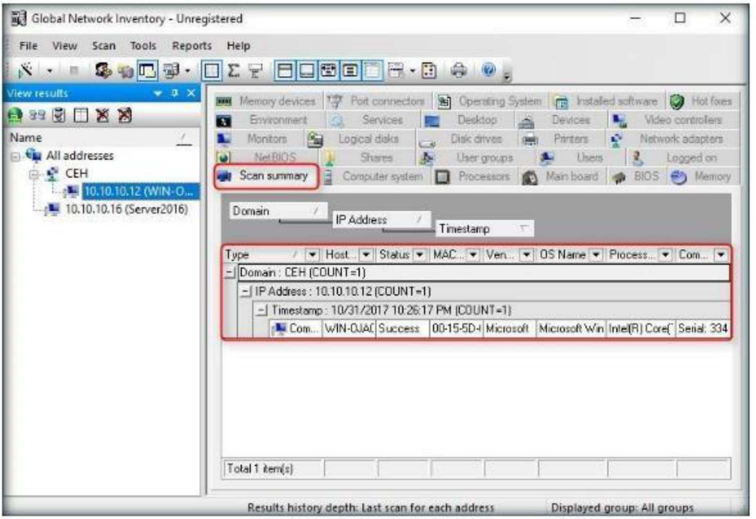

FIGURE 1.13: Global Inventory Scan Summary tab

16. You can even hover the mouse cursor over the computer details tab to view the scan summary, as shown in the following screenshot:

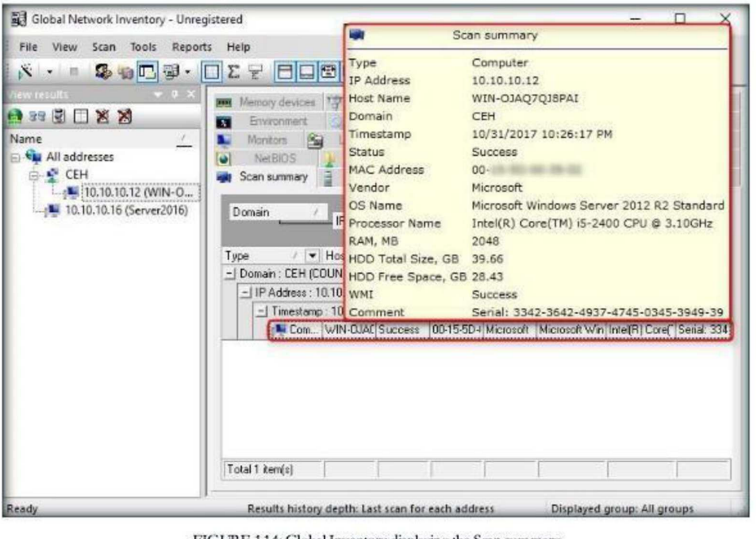

FIGURE 1.14: Global Inventory displaying the Scan summary

17. The **Operating System** tab displays the operating system details of the virtual machine.

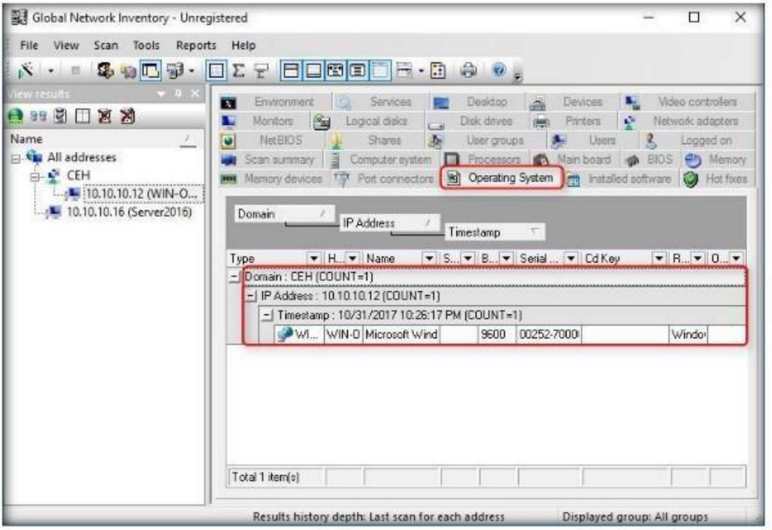

FIGURE 1.15: Global Inventory Operating System tab

18. Hover the mouse over the windows details tab to view the complete details of the machine.

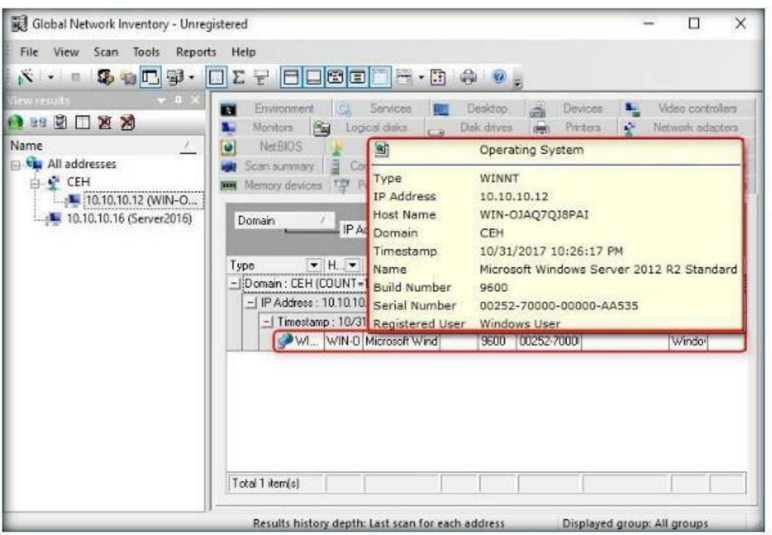

FIGURE 1.16: Global Inventory displaying the operating system details

19. The **BIOS** section gives details of BIOS settings.

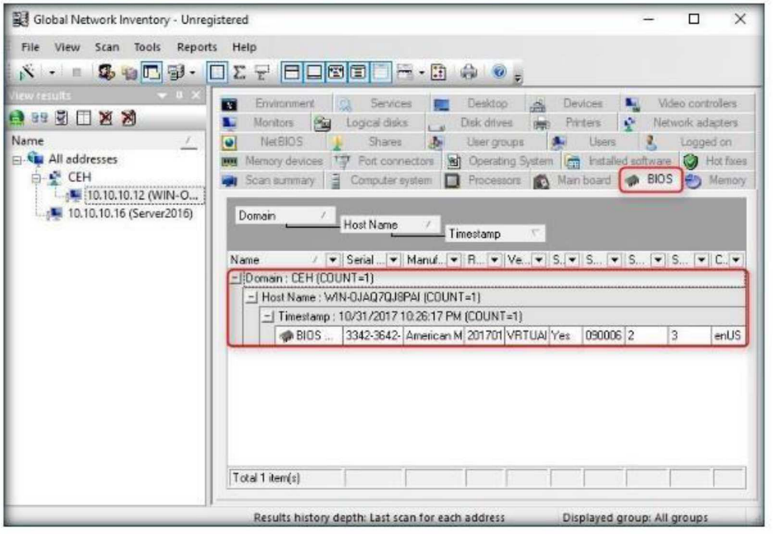

FIGURE 1.17: Global Network Inventory Bios summary tab

20. Hover the mouse cursor over the tab containing the BIOS information, shown in the following screenshot:

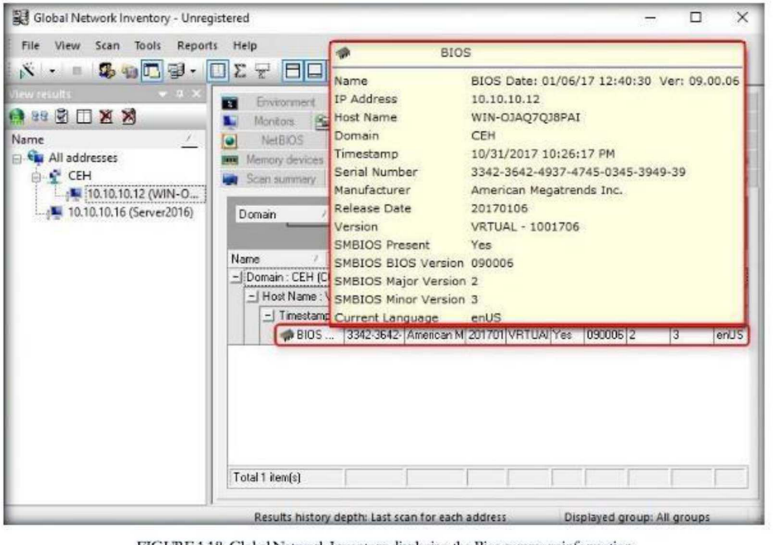

FIGURE 1.18: Global Network Inventory displaying the Bios summary information

21. Under **NetBIOS**, complete details of NetBIOS applications are displayed.

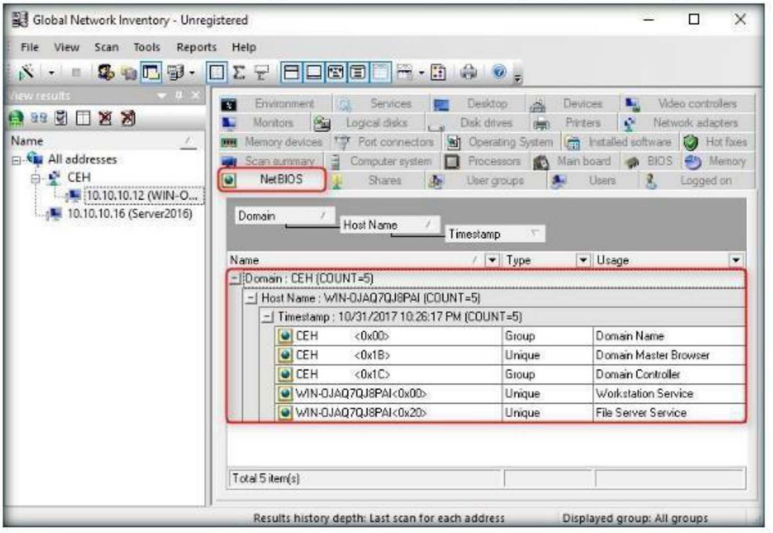

FIGURE 1.19: Global Network Inventory NetBIOS tab

22. Click each NetBIOS application to view its details.

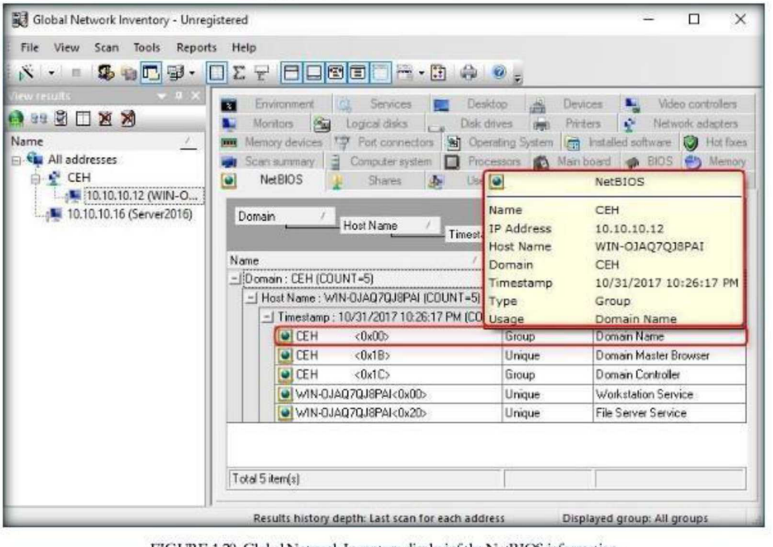

FIGURE 1.20: Global Network Inventory displayinf the NetBIOS information

23. The **User groups** tab shows user account details by work group.

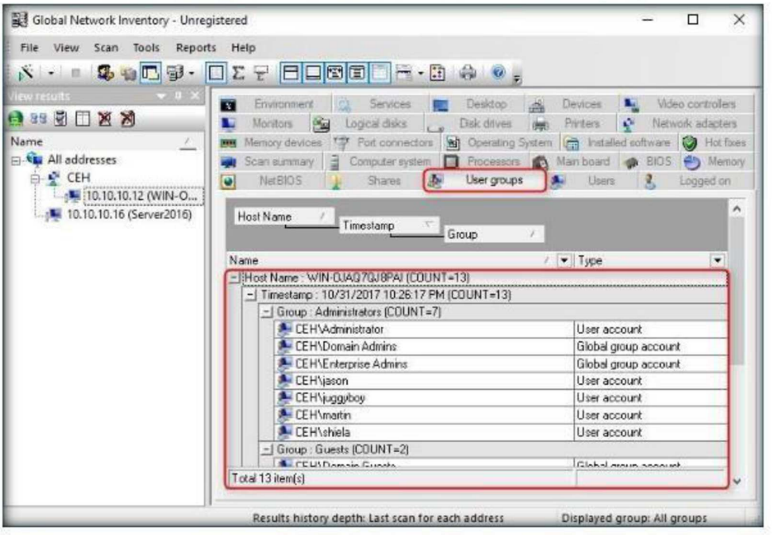

FIGURE 1.21: Global Network Inventory User groups tab

24. Hover the mouse cursor over each work group to view its information.

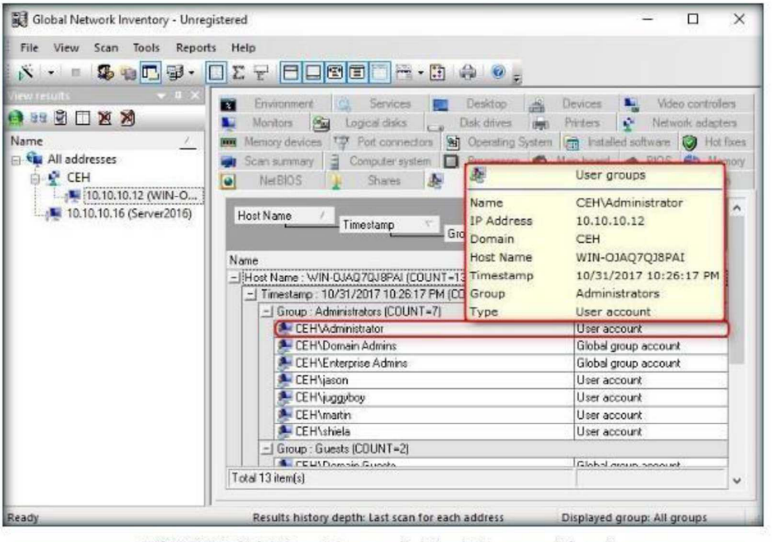

FIGURE 1.22: Global Network Inventory displaying the User groups information

25. The **Logged on** tab shows detailed information of the logged on machine.

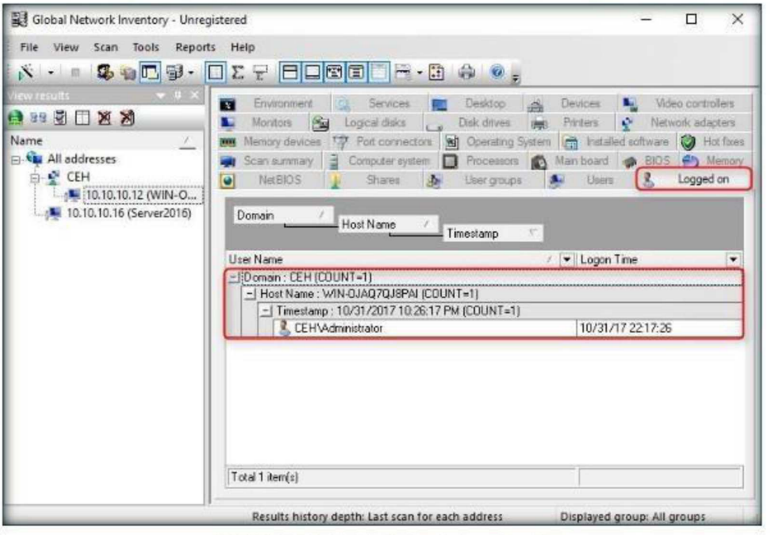

FIGURE 1.23: Global Network Inventory Logged on tab

26. Hover the mouse cursor over the domain name to view log-on details.

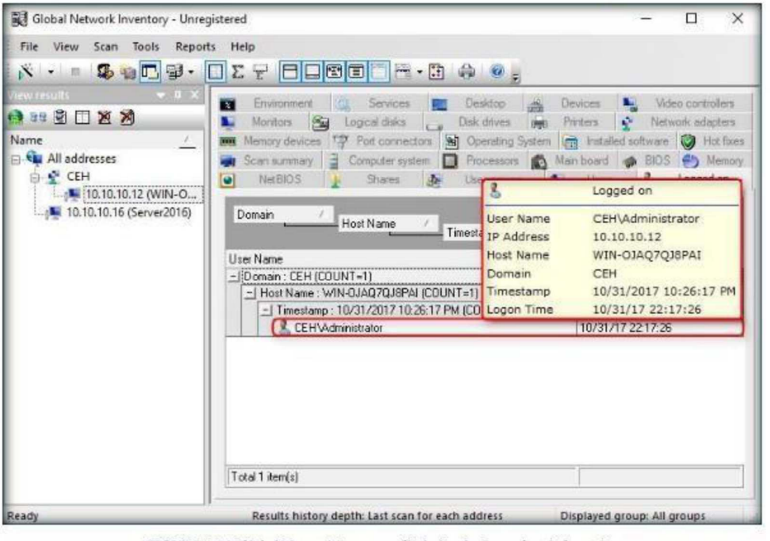

FIGURE 1.24: Global Network Inventory displaying the Logged on information

27. The **Services** section give the details of the services installed on the machine.

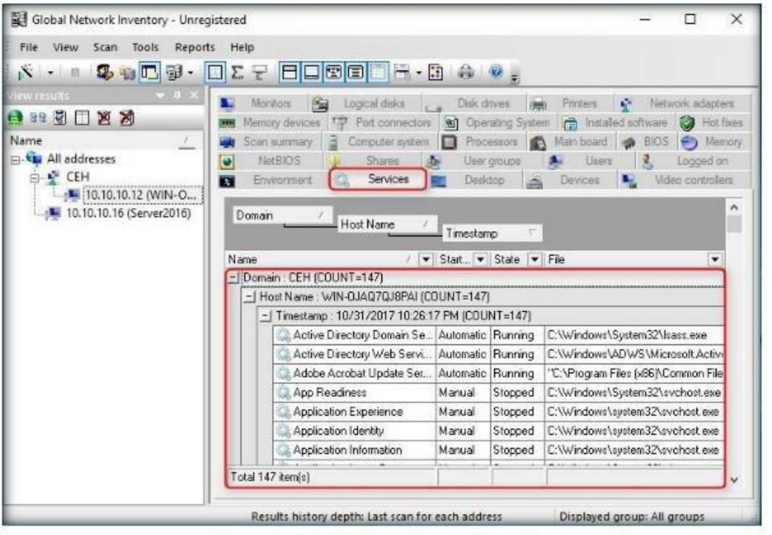

FIGURE 1.25: Global Network Inventory Services tab

28. Hover the mouse cursor over any service to view its details.

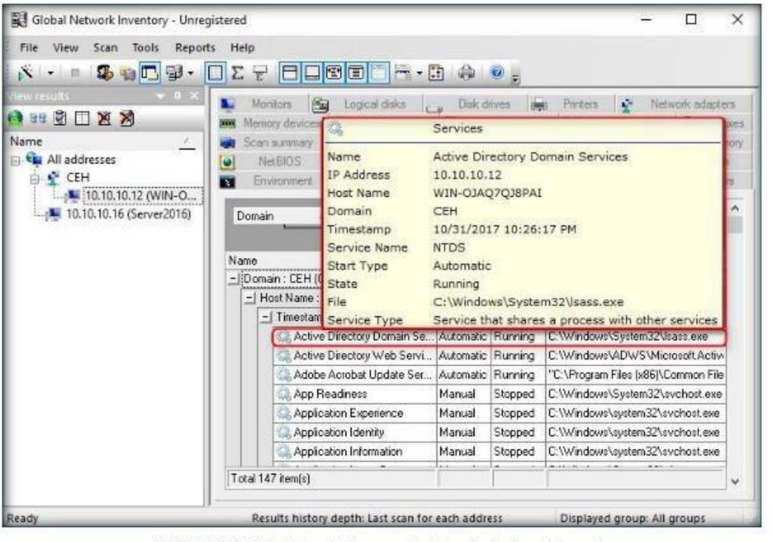

FIGURE 1.26: Global Network Inventory displaying the Services information

29. The **Installed software** section displays details of software installed on the virtual machine.

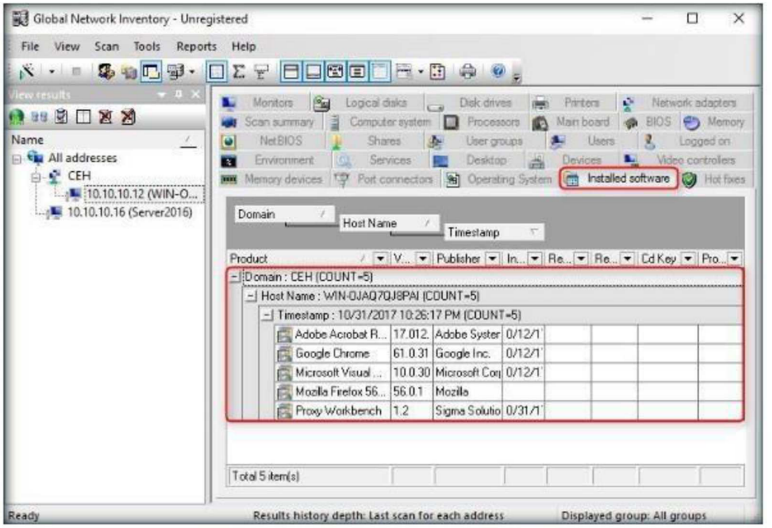

FIGURE 1.27: Global Network Inventory Installed software tab

30. Hover over software names to view their details.

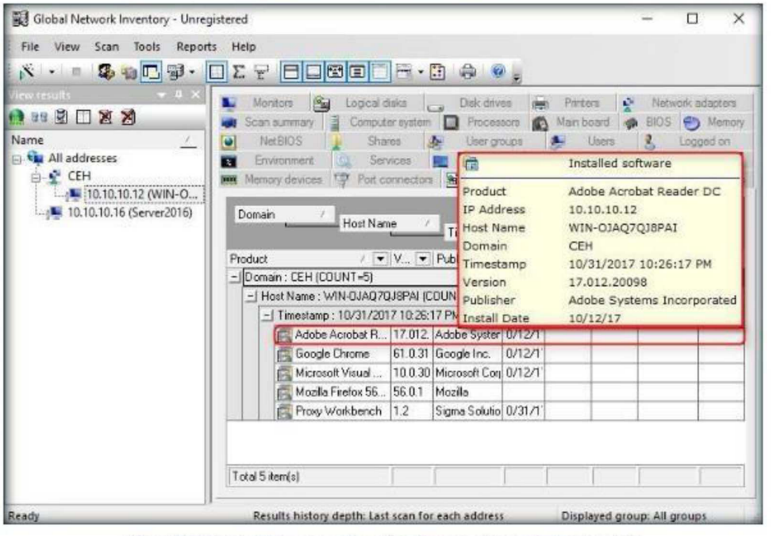

FIGURE 1.28: Global Network Inventory displaying the Installed software information

Lab Analysis

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

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

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

Lab

2

Enumerating Network Resources using Advanced IP Scanner

Advanced IP Scanner is a free network scanner that provides various types of information regarding local network computers.

Lab Scenario

It becomes very important to perform vulnerability scanning to find network flaws and vulnerabilities, and patch it up before attackers can intrude into it. The goal of running a scanner is to identify devices on your network that are open to known vulnerabilities.

Lab Objectives

The objective of this lab is to help students perform a local network scan and discover all network resources.

You need to:

- Perform a system and network scan
- Enumerate user accounts
- Execute remote penetration
- Gather information about local network computers

Lab Environment

In this lab, you will need:

- Advanced IP Scanner located at **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Ping Sweep Tools\Advanced IP Scanner**
- You can download the latest version of Advanced IP Scanner from the link **http://www.advanced-ip-scanner.com**
- If you decide to download the latest version, then screenshots shown in the lab might differ

- A computer running Windows Server 2016 as the attacker machine
- A computer running Windows server 2012 as the victim machine
- A computer running Windows 10 as the victim machine
- A Web browser with Internet access
- Administrative privileges to run this tool

Lab Duration

Time: 5 Minutes

Overview of Network Scanning

Network scanning is performed to collect information about live systems, open ports, and network vulnerabilities. Gathered information is helpful in determining network threats and vulnerabilities, and to know whether there are any suspicious or unauthorized IP connections that could enable data theft and cause damage to resources.

Lab Tasks

1. Navigate to **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Ping Sweep Tools\Advanced IP Scanner**-and double-click **ipscan25.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. Select a language, and click **OK**.

FIGURE 2.1: Select Setup Language dialog-box

4. Select **Install**, and click **Next**.

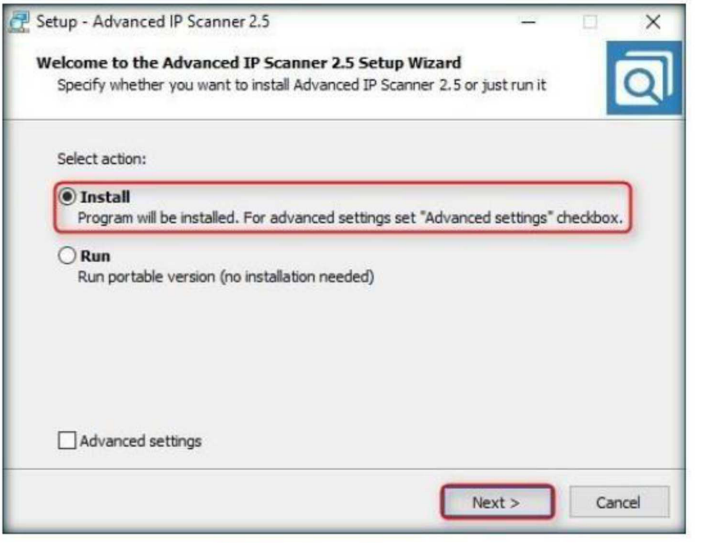

FIGURE 2.2: Advance IP Scanner setup

5. In the **License Agreement** step, select **I accept the agreement**, and click **Install**.

FIGURE 2.3: Advance IP Scanner setup

6. On completion of installation, launch **Advanced IP Scanner** from the Apps list.

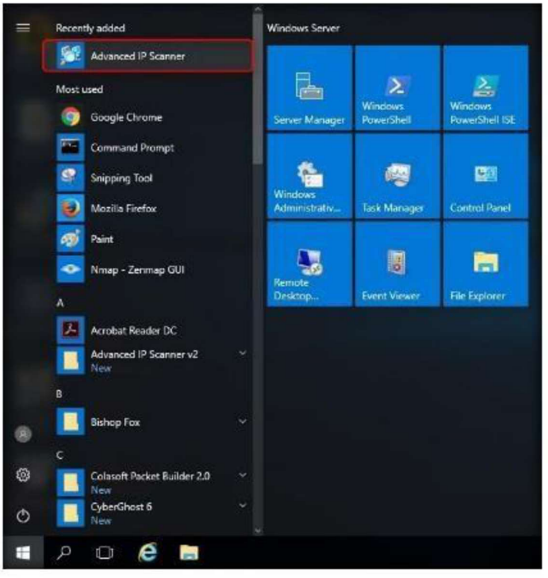

FIGURE 2.4: Launching the application from Apps list

7. The **Advanced IP Scanner** GUI appears, as shown in the following screenshot:

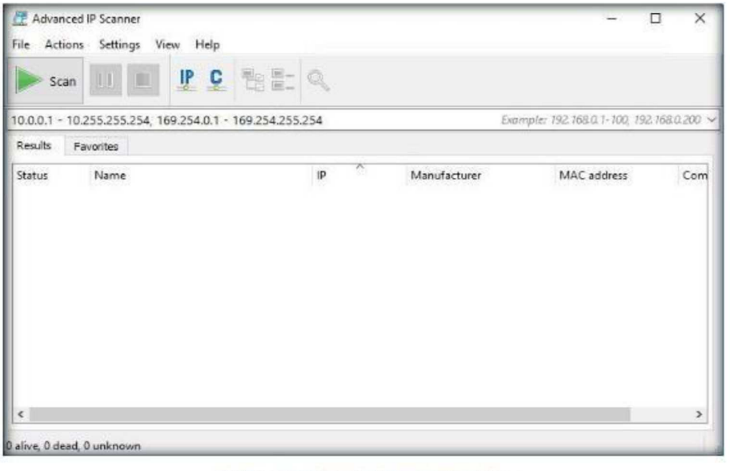

FIGURE 2.5: Advanced IP Scanner main window

8. Now, launch one or more virtual machines; in this lab we are logging into **Windows Server 2012** and **Windows 10**.

9. Switch back to the attacker machine (**Windows Server 2016**) and specify the IP address range in the **Select range** field.
10. Click the **Scan** button to begin the scan.

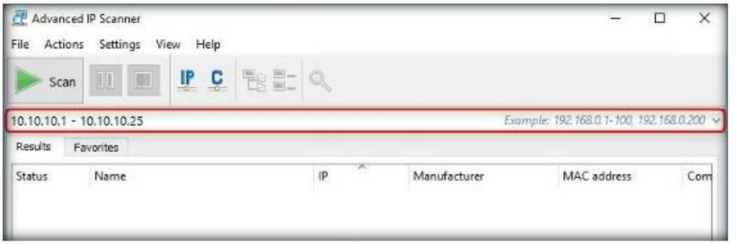

FIGURE 2.6: Scanning a Subnet

Note: The IP addresses range might differ in your lab environment.

11. **Advanced IP Scanner** scans all IP addresses within the range and displays the **scan results**.
12. It displays the status as **live** as shown in the following screenshot:

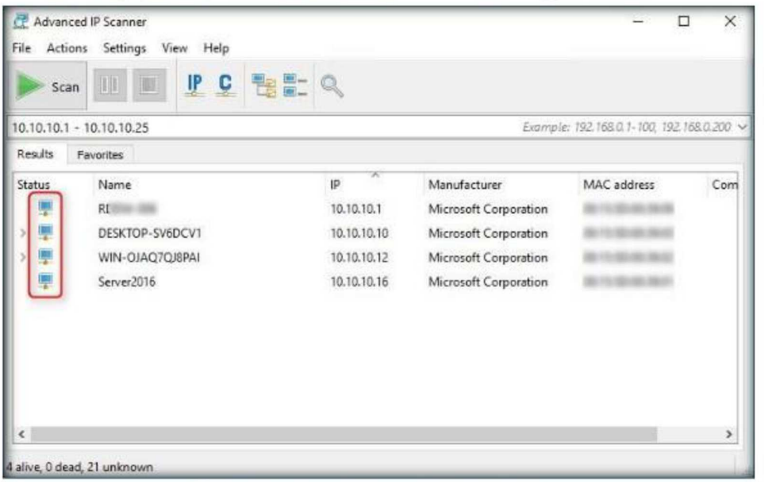

FIGURE 2.7: Advanced IP Scanner displaying Alive Host list

Note: The scan results might differ in your lab environment.

13. Now, you have the **IP address**, **Name**, **MAC address,** and **Manufacturer** information of the victim machine.

14. Click **Expand all** to view the shared folders and services running on the victim machine.

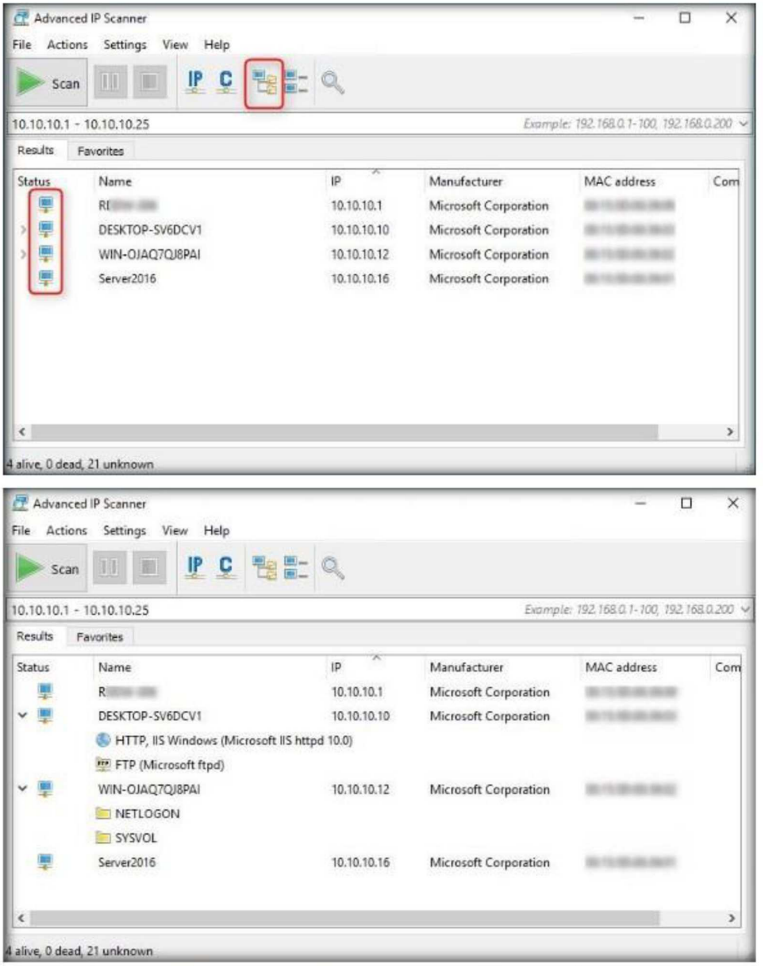

FIGURE 2.8: Advanced IP Scanner displaying shared folders and services

15. **Right-click** any of the detected IP addresses to list Wake-On-Lan, Shut down, Abort shut down, and other options.

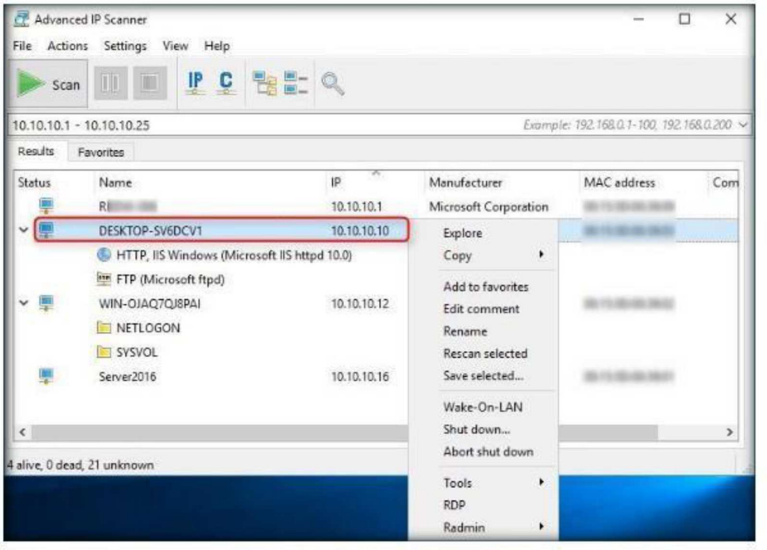

FIGURE 2.9: Exploring the victim machines

16. Using these options, you can ping, traceroute, transfer files, chat, send a message, connect to the victim's machine remotely (using **Radmin**), and so on.

Note: To use the Radmin option, you need to install Radmin viewer, which you can download at **www.radmin.com**.

17. An attacker can also make use of these options, and use various others (e.g., shutting down a remote machine) discussed below.

18. You can forcefully **Shutdown**, **Reboot**, and **Abort Shutdown** the selected victim machine.

19. Right-click **10.10.10.12** and select **Shut down...**.

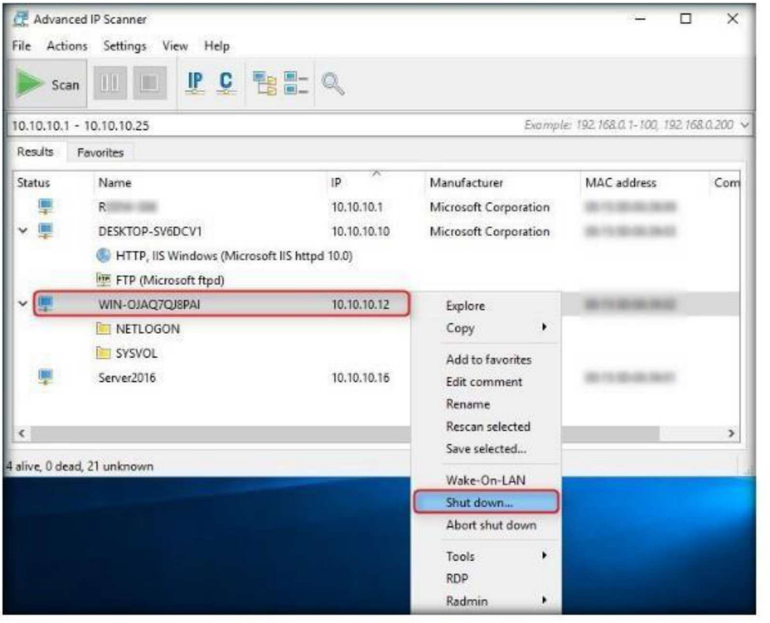

FIGURE 2.10: Shutting down a virtual machine

Note: 10.10.10.12 is the IP address of **Windows Server 2012** virtual machine, which might differ in your lab environment.

20. The **Shutdown options** window opens; set a **Timeout** (here, **10 seconds**), and click **Shutdown** to shut down the virtual machine.

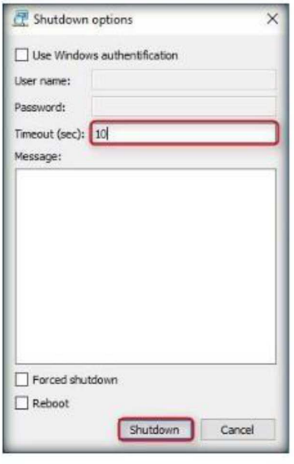

FIGURE 2.11: Shutting down a virtual machine remotely

21. The **Shutdown results** pop-up appears; click **Ok**.

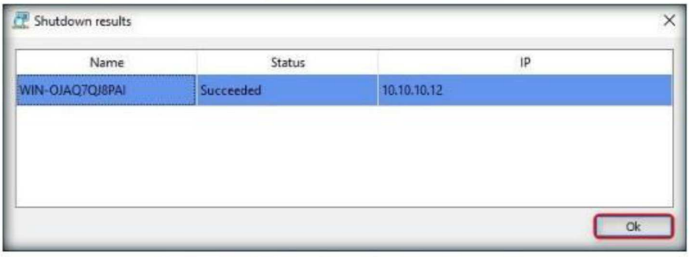

FIGURE 2.12: Shutting down a virtual machine remotely

22. The victim machine will shut down after the specified time out (i.e., 10 seconds).

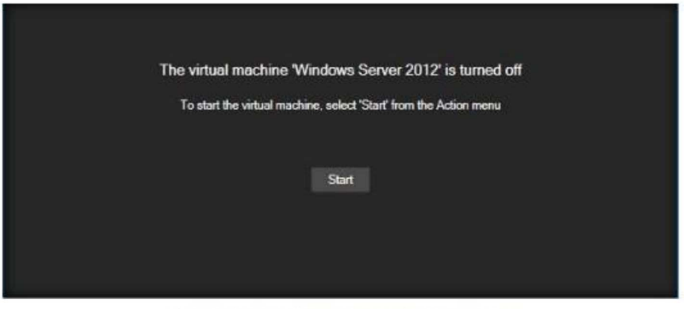

FIGURE 2.13: Victim machine successfully shutdown

23. Thus, an attacker might also discover machines in a network and use various options to retrieve shared files, view system related information, and so on.

Lab Analysis

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

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

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

Lab

3

Performing Network Enumeration using SuperScan

SuperScan is a TCP port scanner, pinger, and resolver. Its features include extensive Windows host enumeration capability, TCP SYN scanning, and UDP scanning.

Lab Scenario

During enumeration, information is systematically collected and individual systems are identified. Pen testers examine systems in their entirety to evaluate security weaknesses. In this lab, we extract NetBIOS information, User and Group Accounts, Network shares, and Trusted Domains and Services (running or stopped). SuperScan detects open TCP and UDP ports on target machines and determines which services are running on them, allowing attackers to exploit these open ports and hack target machines. As an Expert Ethical Hacker and Penetration Tester, you can thus use SuperScan to enumerate target networks and extract lists of computers, user names, user groups, machine names, network resources, and services.

Lab Objectives

The objective of this lab is to help students learn and perform NetBIOS enumeration, which is carried out to obtain:

- Lists of computers that belong to a domain
- Lists of shares on the individual hosts on the network
- Policies and passwords

Lab Environment

To complete this lab, you will need:

- SuperScan is located at **Z:\CEH-Tools\CEHv10 Module 04 Enumeration\NetBIOS Enumeration Tools\SuperScan**
- You can download the latest version of SuperScan from this link at **http://www.mcafee.com/us/downloads/free-tools/superscan.aspx**
- A computer running Windows Server 2016 machine
- Windows 10 running as target machine

- Administrative privileges to install and run tools
- A Web browser with an Internet connection

Lab Duration

Time: 5 Minutes

Overview of SuperScan

1. The purpose of SuperScan is to gather information such as: Account lockout threshold, Local groups and user accounts, Global groups and user accounts
2. Restrict anonymous bypass routine and also password checking:
   a. Checks for user accounts with blank passwords
   b. Checks for user accounts with passwords that are same as the usernames in lower case

Lab Tasks

1. Launch **Windows 10** virtual machine before beginning this lab.
2. Switch back to machine (Windows Server 2016), navigate to **Z:\CEH-Tools\CEHv10 Module 04 Enumeration\NetBIOS Enumeration Tools\SuperScan**, and double-click **SuperScan4.1.exe**.
3. If the **Open File - Security Warning** pop-up appears, click **Run**.
4. The SuperScan main window appears.

FIGURE 3.1: SuperScan main window

5. Click on the **Windows Enumeration** tab.
6. Enter the IP address of the target machine in the **Hostname/IP/URL** textbox. In this lab, we have entered **Windows 10** virtual machine IP address.

Note: This IP address may differ in your lab environment.

7. Check the types of **enumeration** you want to perform.
8. Now, click on **Enumerate**.

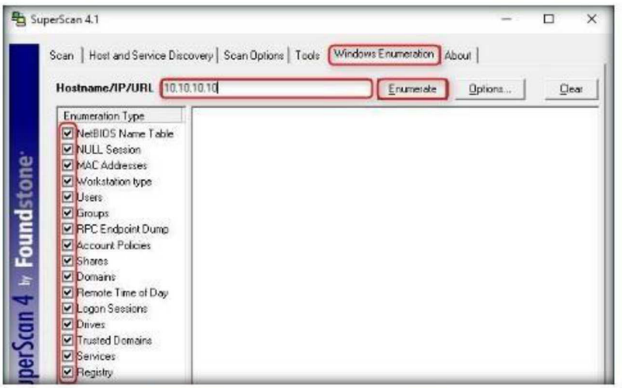

FIGURE 3.2: SuperScan main window with IP Address

9. SuperScan starts **enumerating** the provided hostname and displays the **results** as shown in the following screenshot:

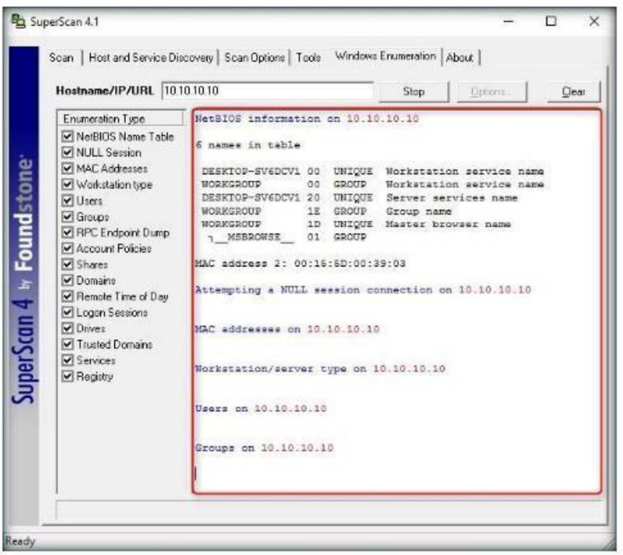

FIGURE 3.3: SuperScan main window with results

10. Wait for the enumeration process to complete.
11. After the completion of enumeration process, the stop button changes to **Enumerate**.
12. Scroll down the window. An **Enumeration complete** message will be displayed at the end of the enumeration result window.

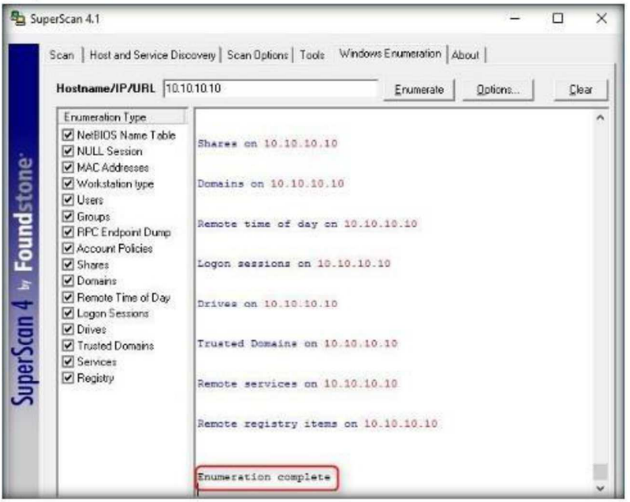

FIGURE 3.4: SuperScan Enumeration completed

13. Now, scroll the window to see the results of the enumeration.

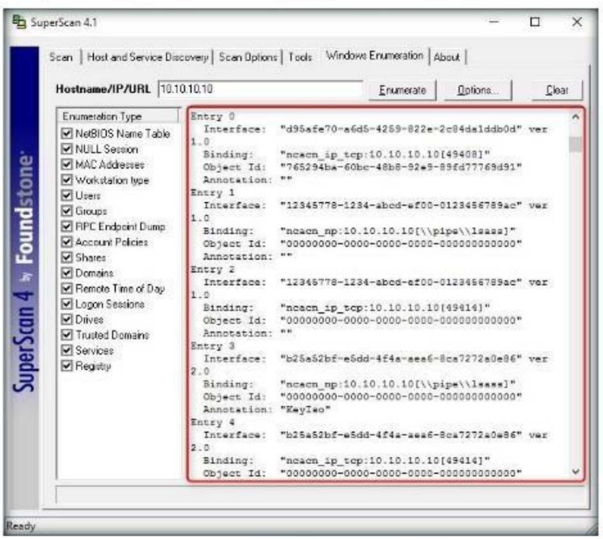

FIGURE 3.5: SuperScan Enumeration Results

14. To perform a new enumeration on another Hostname, click on the **Clear** button at the top right of the window. The option **erases** all the previous results.

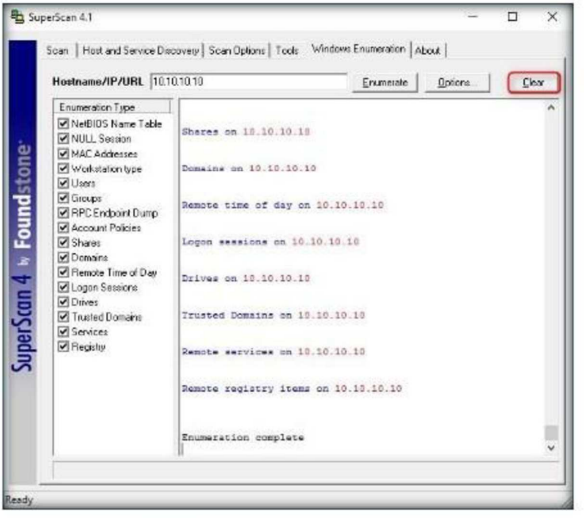

FIGURE 3.6: SuperScan main window with results

Lab Analysis

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

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

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	

Lab

4

Enumerating Resources in a Local Machine using Hyena

Hyena uses an Explorer-style interface for all operations, including right-click context menus for all objects. Management of users, groups (local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing are all supported.

Lab Scenario

Hackers enumerate applications and banners in addition to identifying user accounts and shared resources. In this lab, Hyena uses an Explorer-style interface for all operations. Management of users, groups (local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing are all supported. To be an Expert Ethical Hacker and Penetration Tester, you must have sound knowledge of enumeration, which requires an active connection to the machine being attacked.

Lab Objectives

The objective of this lab is to help students learn and perform network enumeration of:

- System user information
- Running system services

Lab Environment

To perform this lab, you need:

- A computer running Windows Server 2016
- Administrative privileges to install and run tools
- You can download this tool from the following link **http://www.systemtools.com**

- If you decide to download the latest version of this tool, the screenshots may differ

Lab Duration

Time: 5 Minutes

Overview of Enumeration

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an intranet environment.

Lab Tasks

1. Navigate to **Z:\CEH-Tools\CEHv10 Module 04 Enumeration\NetBIOS Enumeration Tools\Hyena** and double-click **Hyena_English_x86.exe**.
2. If an **Open File - Security Warning** pop-up appears, click **Run**.
3. Hyena installation wizard appears; click **Next**.

Note: If you are asked to install **C++ Redistribute**, click **Install**. After installation, if it requires a system restart, click **Yes** to restart the machine.

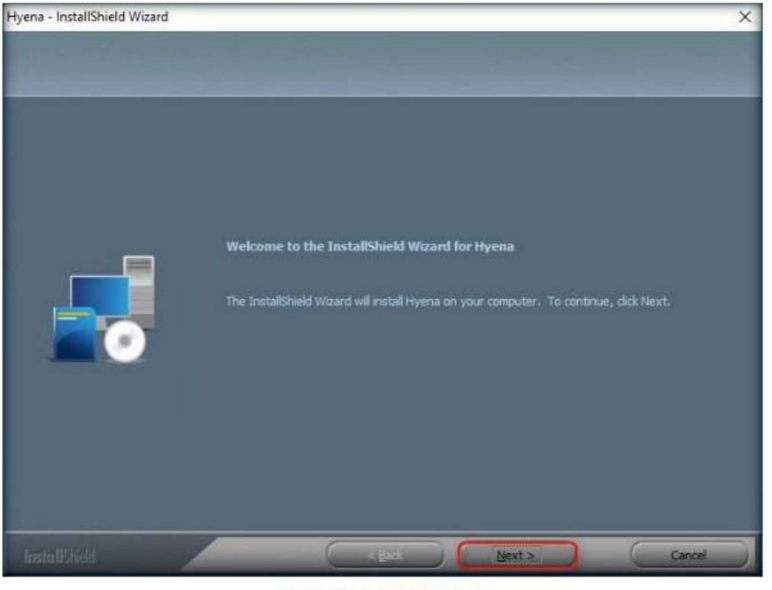

FIGURE 4.1: Installation of Hyena

4. Follow the steps to install Hyena.
5. On completion of installation, **Install Shield Wizard Complete** section appears; click **Finish** to complete the installation.

6. On completion of installation, launch **Hyena** application from the **Apps** list.

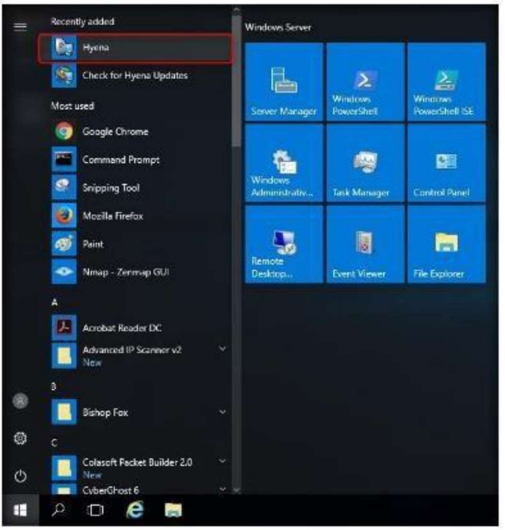

FIGURE 4.2: Windows Server 2012 Installed Apps

7. If the **System Tools Update Notification Utility** appears, click **Close**.
8. If the **Registration** window appears, click **OK** to continue.
9. If the **Hyena** dialog box appears, prompting you to register the application, click **No**.
10. The main window of **Hyena** appears, as shown in screenshot:

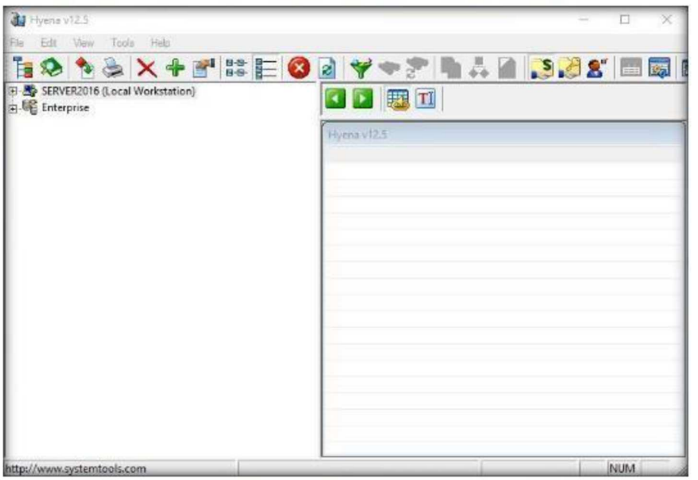

FIGURE 4.3: Main window of Hyena

11. Click the "**+**" node of the **Local Workstation** to expand section, then expand **Users** node to view all the users in the local machine.

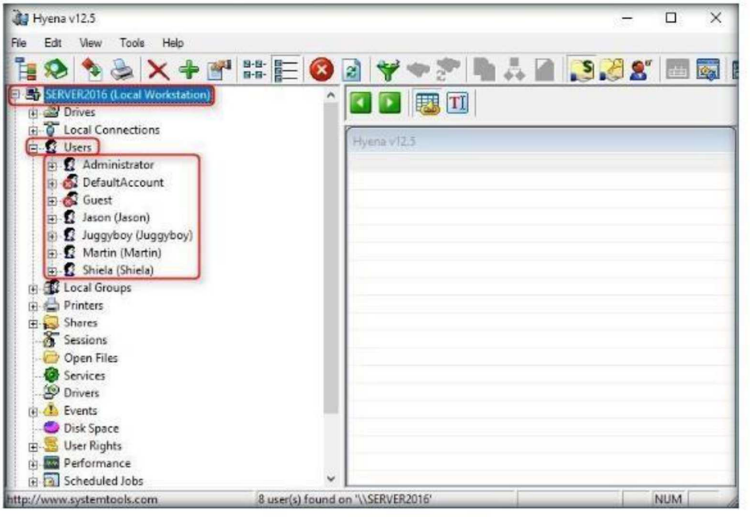

FIGURE 4.4: Expand the System users

12. To check the services running on the system, double-click **Services**.

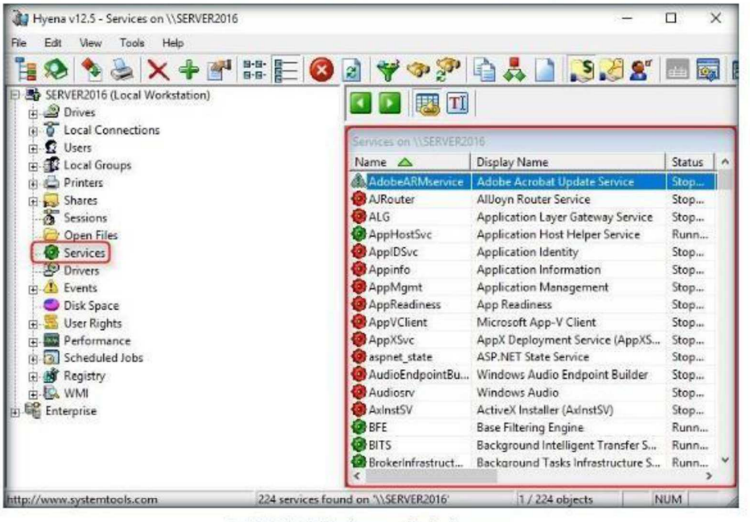

FIGURE 4.5: Services running in the system

13. Double-click **User Rights** to list the user rights.

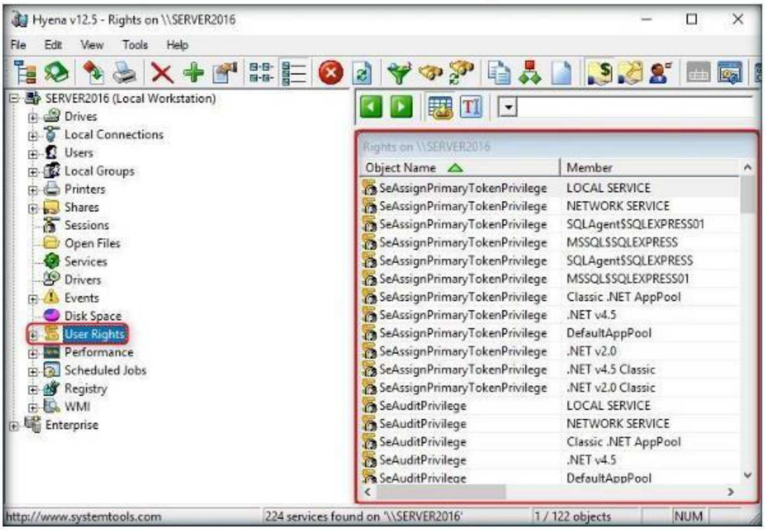

FIGURE 4.6: Users Rights

14. Double-click **Scheduled Jobs** to examine the scheduled jobs.

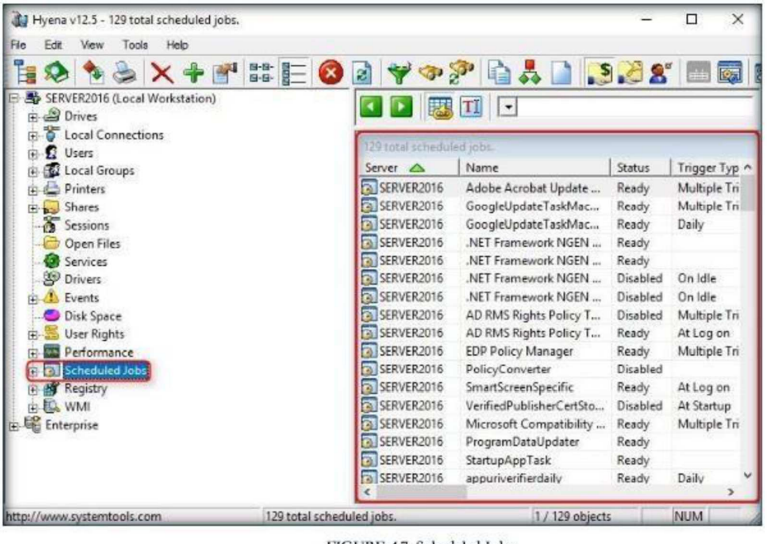

FIGURE 4.7: Scheduled Jobs

15. By observing all these options, you can check for any reasonable information discovered by Hyena that would prompt you to take proper security measures to safeguard the system.

Lab Analysis

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

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

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

Lab

5

Performing Network Enumeration using NetBIOS Enumerator

You can use NetBIOS to probe identified services for known weaknesses.

Lab Scenario

Enumeration is the first attack on a target network, used to gather information by actively connecting to it. You must have sound knowledge of enumeration, a process that requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources. In this lab, we enumerate a target's user name, MAC address, and domain group.

Lab Objectives

The objective of this lab is to help students learn and perform NetBIOS enumeration.

The purpose of NetBIOS enumeration is to gather the following information:

- Account lockout threshold
- Local groups and user accounts
- Global groups and user accounts

Lab Environment

To complete this lab, you will need:

- NETBIOS Enumerator tool is located at **Z:\CEH-Tools\CEHv10 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator**
- You can download the latest version of NetBIOS Enumerator from the link **http://nbtenum.sourceforge.net**
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A machine running Windows Server 2016 as an Attacker machine

- A virtual machine running Windows Server 2012 as a target machine
- A virtual machine running Windows 10 as a target machine
- Administrative privileges are required to run this tool

Lab Duration

Time: 5 Minutes

Overview of Enumeration

Enumeration involves making active connections, so that they can be logged. Typical information attackers look for in enumeration includes user account names for future password guessing attacks. NetBIOS Enumerator is an enumeration tool that shows how to use remote network support and to deal with some other interesting web techniques, such as SMB.

Lab Tasks

1. To launch NetBIOS Enumerator, go to **Z:\CEH-Tools\CEHv10 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double click **NetBIOS Enumerater.exe**.
2. If the **Open - File Security Warning** pop-up appears, click **Run**.
3. **NetBIOS Enumerator** main window appears, as shown in the screenshot:

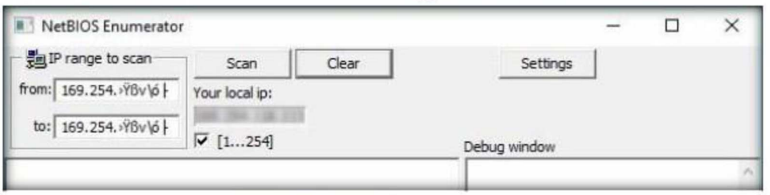

FIGURE 5.1: NetBIOS Enumerator main window

4. Under **IP range to scan**, enter an **IP range** in the **from** and **to** fields.

Note: The IP range might differ in your lab environment.

5. Click the **Scan** button to initiate the scan.

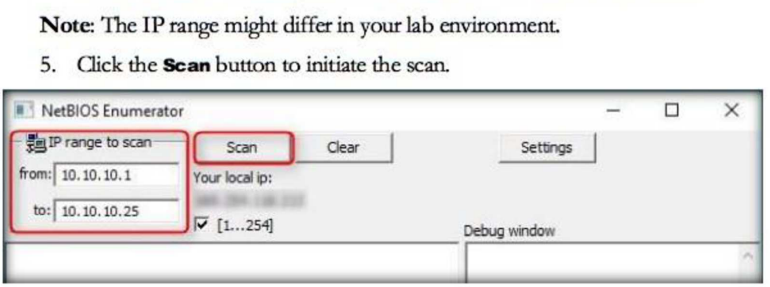

FIGURE 5.2: NetBIOS Enumerator with IP range to scan

6. NetBIOS Enumerator starts scanning for the range of **IP addresses** provided.

7. After the completion of scanning, the results are displayed in the **left pane**.
8. The **Debug window** section in the right pane shows the scanning range of IP addresses and displays **Ready!** after completion of the scan.

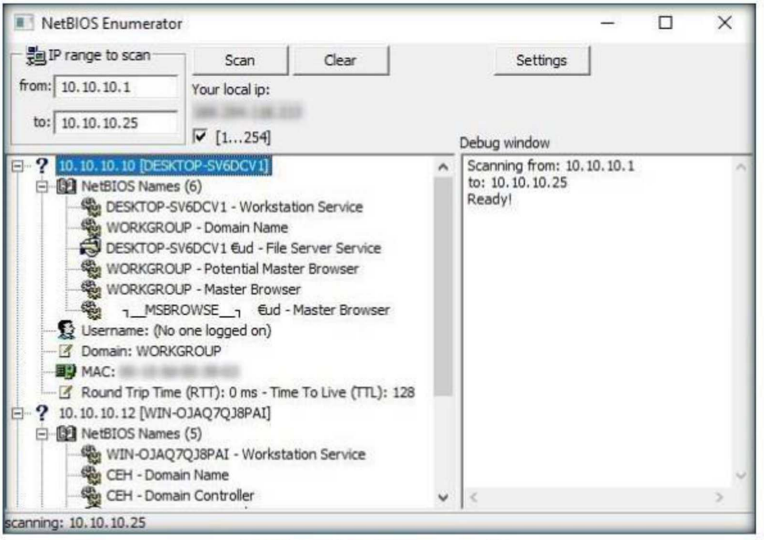

FIGURE 5.3: NetBIOS Enumerator results

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

9. Attackers may use the information obtained, such as enumerated usernames, and perform password guessing techniques to crack a user account.
10. To perform a new scan or to rescan the provided range of IP addresses, erase the previous scan results by clicking **Clear**.

Lab Analysis

Analyze and document the results related to this lab exercise.

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

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

Lab

6

Enumerating a Network using SoftPerfect Network Scanner

SoftPerfect Network Scanner is a free, multi-threaded IP, NetBIOS, and SNMP scanner with a modern interface and many advanced features.

Lab Scenario

To be an Expert Ethical Hacker and Penetration Tester, you must have sound knowledge of enumeration, which requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources. In this lab, we try to resolve host names and auto-detect your local and external IP range.

Lab Objectives

The objective of this lab is to help students learn and perform NetBIOS enumeration, which is carried out to detect:

- Hardware MAC addresses across routers
- Hidden shared folders and writable ones
- Internal and External IP address

Lab Environment

To complete this lab, you will need:

- SoftPerfect Network Scanner is located at **Z:\CEH-Tools\CEHv10 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner**
- You can download the latest version of SoftPerfect Network Scanner from the link **http://www.softperfect.com/products/networkscanner**
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A machine running Windows Server 2016

- A virtual machine running Windows Server 2012 as a target machine
- A virtual machine running Windows 10 as a target machine
- Administrative privileges are required to run this tool

Lab Duration

Time: 5 Minutes

Overview of Enumeration

Enumeration involves an active connection so that they can be logged. Typical information that attackers look for includes user account names for future password guessing attacks.

Lab Task

1. To launch SoftPerfect Network Scanner, navigate to **Z:\CEH-Tools\CEHv10 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner**, and double click **netscan_setup.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. If the **Network Scanner** dialog box appears, click **Continue**.

FIGURE 6.1: Network Scanner dialog-box

4. The **SoftPerfect Network Scanner** GUI appears on the screen.

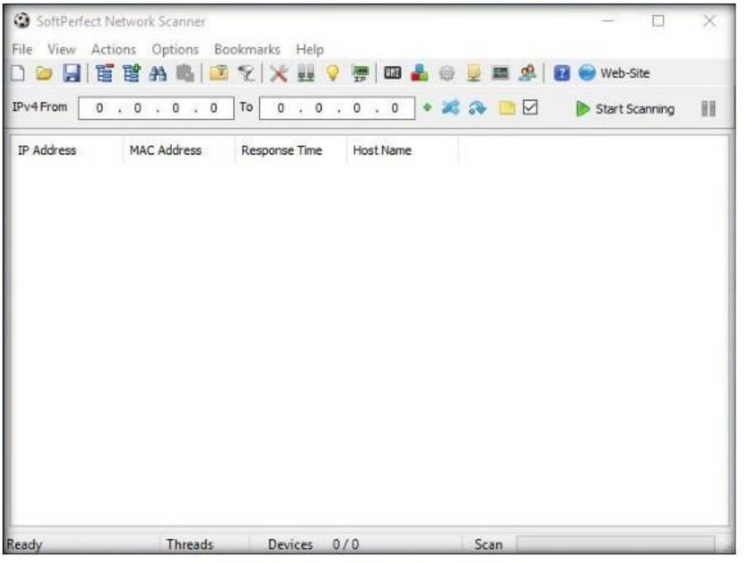

FIGURE 6.2: SoftPerfect Network Scanner main window

5. To start scanning your network, enter an IP range in the **IPv4 From** and **To** fields, and click **Start Scanning** button.

Note: The IP range might differ in your lab environment.

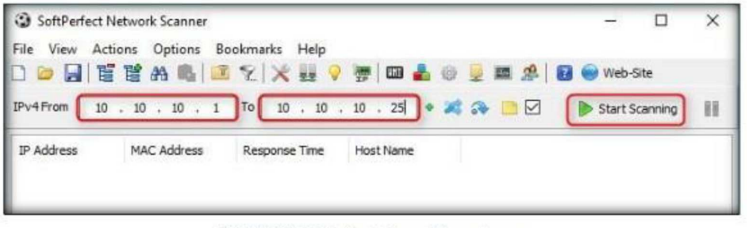

FIGURE 6.3: SoftPerfect setting an IP range to scan

6. The **status bar** displays the status of the scan at the lower-right corner of the GUI.

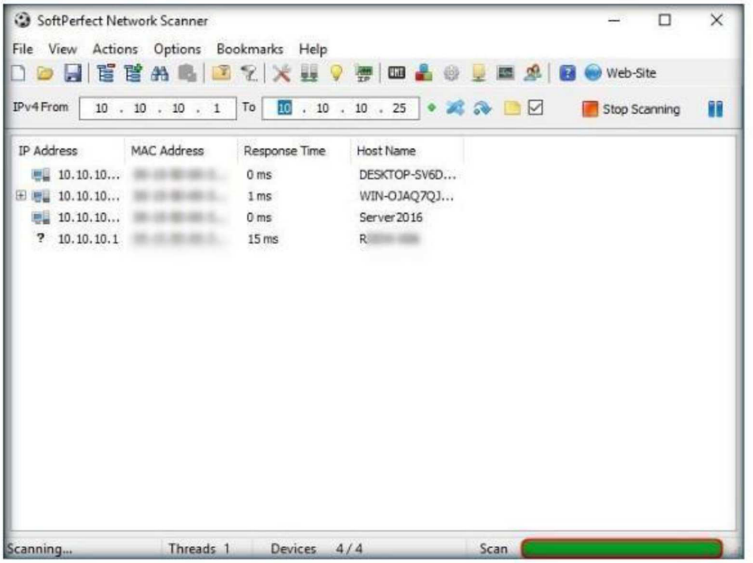

FIGURE 6.4: SoftPerfect status bar

7. To view the **properties** of an individual **IP address**, right-click a particular IP address, and select **Properties**.

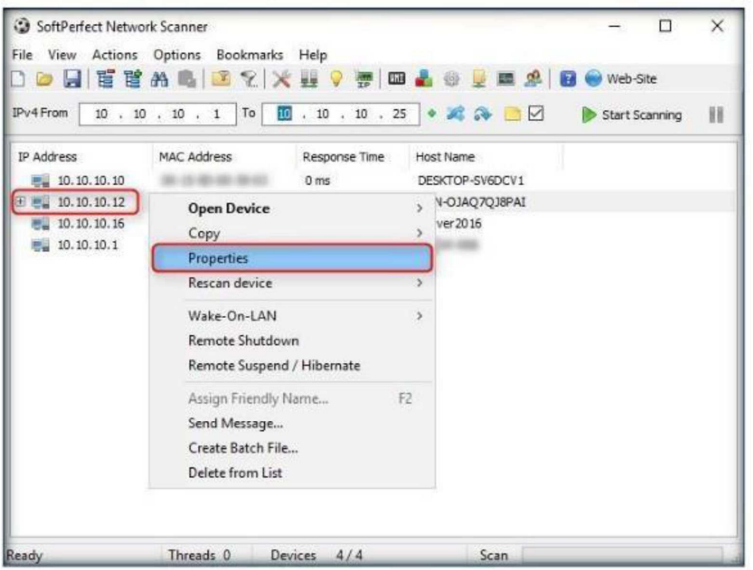

FIGURE 6.5: IP address scanned details

8. The **Properties** window appears, displaying the **Shared Resources** and **Basic Info** of the machine corresponding to the selected IP address.

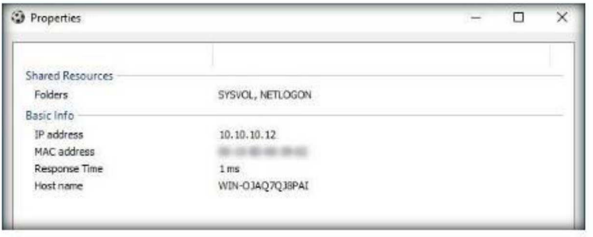

FIGURE 6.6: Properties window

9. To view the shared folders, notice the scanned hosts that have a **+** node before them. Expand the node to view all the shared folders.

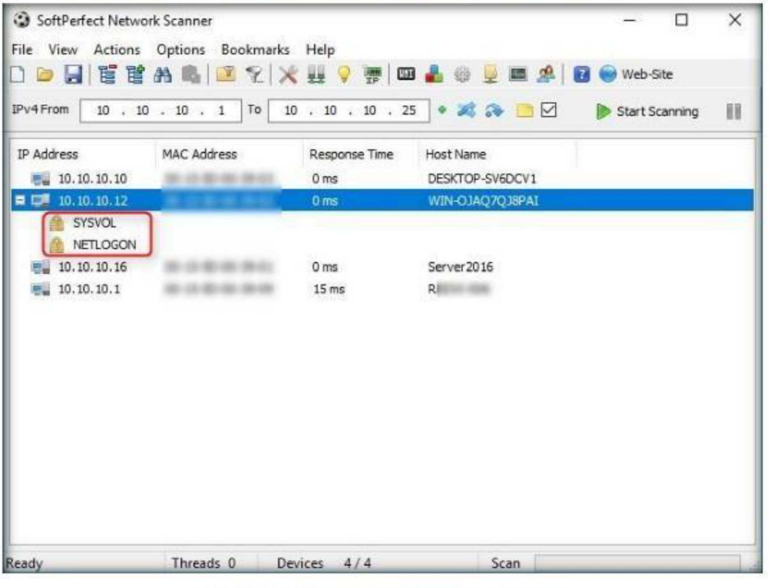

FIGURE 6.7: SoftPerfect Scanner displaying the shared folders

10. Right-click the selected host, and click **Open Device**. A drop-down list appears, containing options that allow you to connect to the remote machine as HTTP, HTTPS, Telnet and so on.

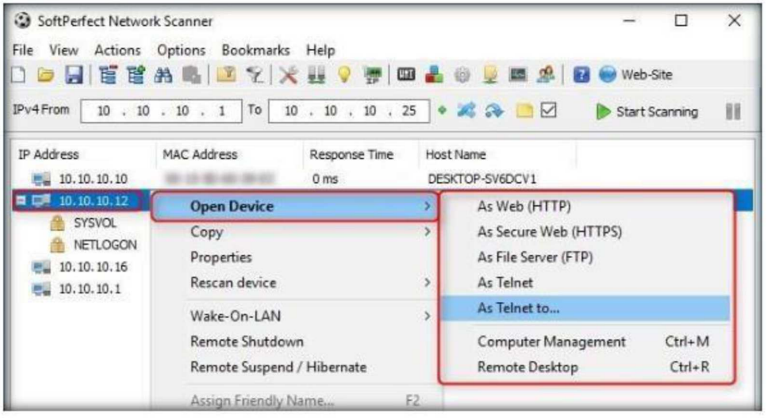

FIGURE 6.8: Various options in SoftPerfect Network Scanner

11. If the selected host is not secure enough, you can make use of these options to connect to the remote machines. You may also be able to perform activities such as sending a message, shutting down a computer remotely, and so on. These features are applicable only if the selected machine is built with a poor security configuration.

Lab Analysis

Analyze and document the results related to this lab exercise.

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

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

Lab

7

Enumerating a Target Network using Nmap and Net Use

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system.

Lab Scenario

In fact, a penetration test begins before penetration testers have made contact with victim systems. During enumeration, information is systematically collected and individual systems are identified. Pen testers examine the systems in their entirety to assess security weaknesses. In this lab, we discus Nmap, it uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, and what type of packet filters/firewalls are in use. It was designed to rapidly scan large networks. By using the open ports an attacker can easily attack the target machine to overcome this type of attacks on networks filled with IP filters, firewalls, and other obstacles.

As an Expert Ethical Hacker and Penetration Tester, you will need to enumerate a target network and extract a list of computers, user names, user groups, machine names, network resources, and services using various enumeration techniques.

Lab Objectives

The objective of this lab is to help students understand and perform enumeration on target network using various techniques to obtain:

- User names and user groups
- Lists of computers, their operating systems, and the ports on them
- Machine names, network resources, and services
- Lists of shares on the individual hosts on the network
- Policies and passwords

Lab Environment

To perform this lab, you will need:

- Nmap located at **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Scanning Tools\Nmap**
- You can download the latest version of Nmap from the link **http://nmap.org/download.html#windows**
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 Virtual Machine
- A computer running Windows Server 2016 Virtual machine
- Administrative privileges to install and run tools

Lab Duration

Time: 10 Minutes

Overview of Enumeration

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an intranet environment.

Lab Tasks

The basic idea in this section is to:

- Perform scans to find hosts with **NetBIOS** ports open (135, 137-139, 445)
- Do an **nbtstat** scan to find generic **information** (computer names, user names, MAC addresses) on the hosts
- Create a Null Session
- Install and Launch **Nmap** in Windows Server 2012 machine

Note: If Nmap is already installed in the Windows Server 2016 machine, skip to **step no. 5.**

1. Navigate to **Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks\Scanning Tools\Nmap** and double-click **nmap-7.60-setup.exe.**
2. If an **Open File - Security Warning** pop-up appears, click **Run.**

3. The **Nmap Setup** window appears; click **I Agree** and follow the steps to install Nmap.

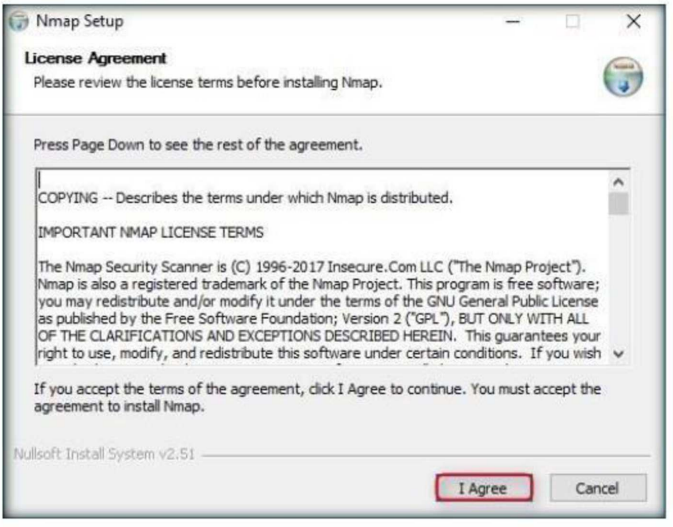

FIGURE 7.1: Nmap Setup window

4. During installation, a **WinPcap setup** pop-up appears. If a higher version of WinPcap is already installed, click **No,** and follow the steps to install WinPcap.

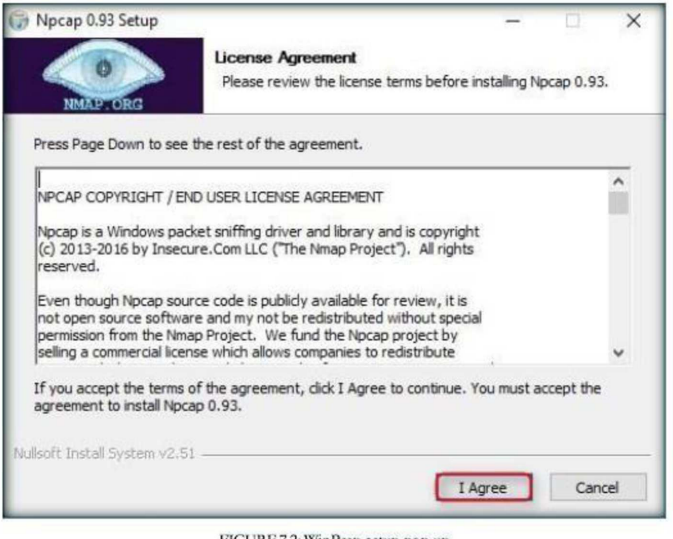

FIGURE 7.2: WinPcap setup pop-up

5. On completion of installation, launch Nmap application from the **Apps** list.

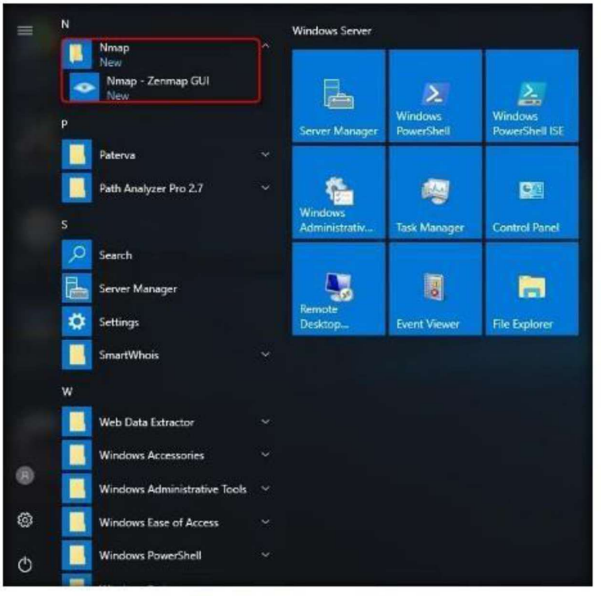

FIGURE 7.3: Windows Server 2012 Apps list

6. The **Nmap - Zenmap GUI** window appears, with the **Intense scan** profile set by default.

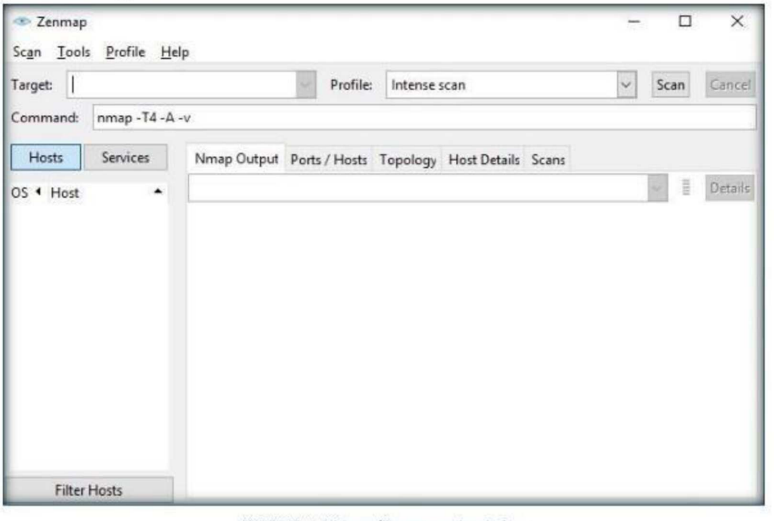

FIGURE 7.4: Nmap/Zenmap main window

7. Perform the **nmap -O** scan for the **Windows Server 2012** virtual machine network. This takes few minutes.

Note: IP address of Windows Server 2012 may differ in your lab environment.

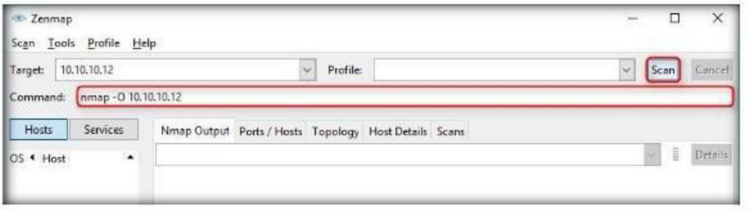

FIGURE 7.5: Configuring Nmap

8. Nmap performs a **scan** for the provided **target IP address** and outputs the results in the Nmap **Output** tab.

9. Your first target is the computer with a Windows OS, on which you can see ports **139** and **445** open. Remember, this usually works only **against Windows** but may partially succeed if other OSs have these ports open. There may be more than one system with **NetBIOS** open.

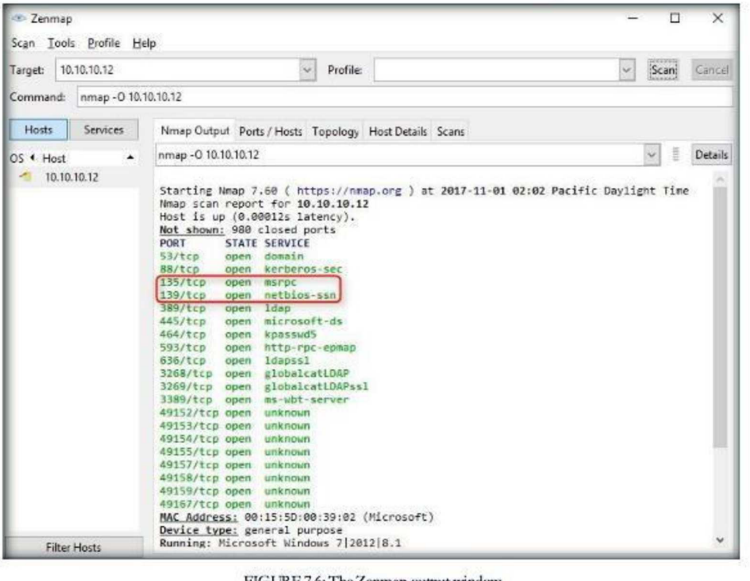

FIGURE 7.6: The Zenmap output window

10. Now you see that ports 135, 139, 445 and 5357 are open, and port **139** is using NetBIOS.

Note: The result displayed in Nmap might differ in your lab environment.

11. Now, launch the **command prompt** in the **Windows Server 2012** virtual machine, and perform **nbtstat** on port 139 of the Windows Server 2016 machine.

12. Run the command **nbtstat –A 10.10.10.16**.

Note: 10.10.10.16 is the IP address of the **Windows Server 2016** virtual machine. This IP address and result may differ in your lab environment.

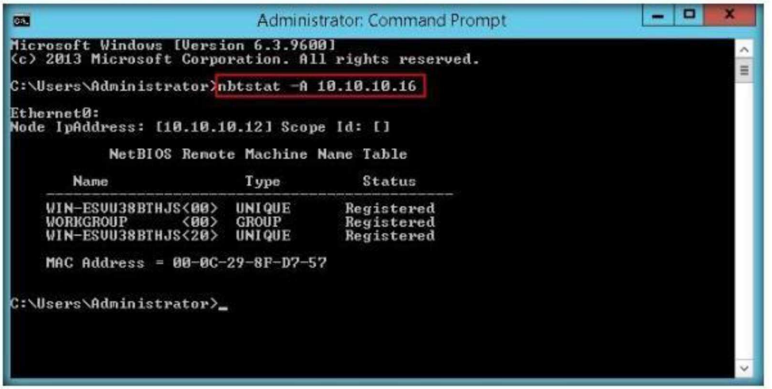

FIGURE 7.7: Command Prompt with the nbtstat command

13. We have not even created a **null session** (an unauthenticated session) yet, and we can still pull down this info.

14. Issue **net use** command to view the created null sessions/shared folders from your host:

FIGURE 7.8: Command Prompt with the net use command

Note: The IP address displayed in the result might differ in your environment.

Lab Analysis

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

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

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

Lab

8

Enumerating Services on a Target Machine

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system.

Lab Scenario

Various services run on a machine that contribute to its functioning. There may be older versions of these services, which contain vulnerabilities that can allow an attacker to exploit them. So, if an attacker obtains the version details, he/she might be able to exploit vulnerable services running on the machine and compromise it. As a Penetration tester, your duty is to enumerate the services running on a target machine and patch the vulnerable ones.

Lab Objectives

The objective of this lab is to help students understand and perform enumeration on a target network using various techniques to:

- Scan all the machines on a given network or a subnet
- List machines that are up and running
- Determine open ports on a given node
- Find if any port has firewall restriction
- Enumerate all the services running on the port along with their respective versions

Lab Environment

To perform this lab, you will need:

- A computer running with Windows Server 2016 machine
- Kali Linux running as a virtual machine
- Windows Server 2012 running as a virtual machine

Lab Duration

Time: 10 Minutes

Overview of Enumeration

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an intranet environment.

Lab Tasks

Note: Launch the **Windows Server 2012** virtual machine before running this lab.

1. Launch the **Kali Linux** virtual machine from VMware Workstation and log into it. The credentials to log in to the machine are Username: **root** and Password: **toor**.
2. The **Kali Linux** machine **Desktop** appears, as shown in the following screenshot:

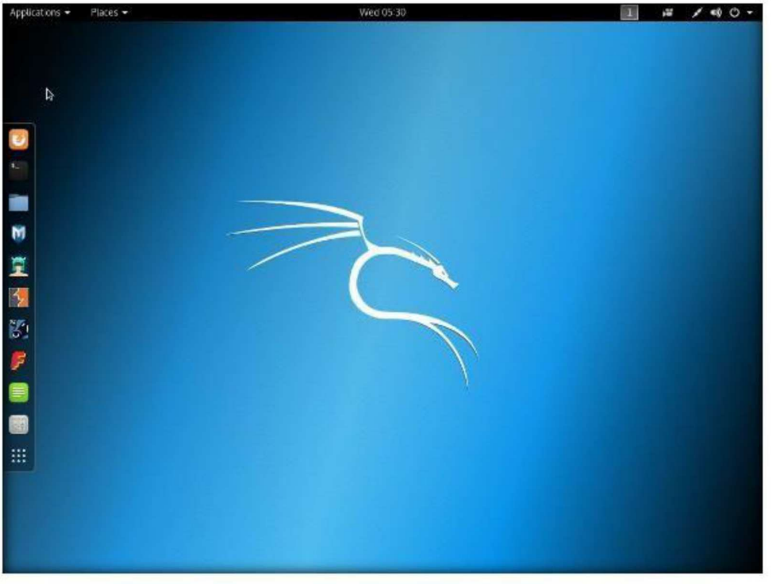

FIGURE 8.1: Kali Linux Machine

3. Select **Applications → 01- Information Gathering (drop-down list) → Network & Port Scanners → nmap**. This launches the Nmap application.

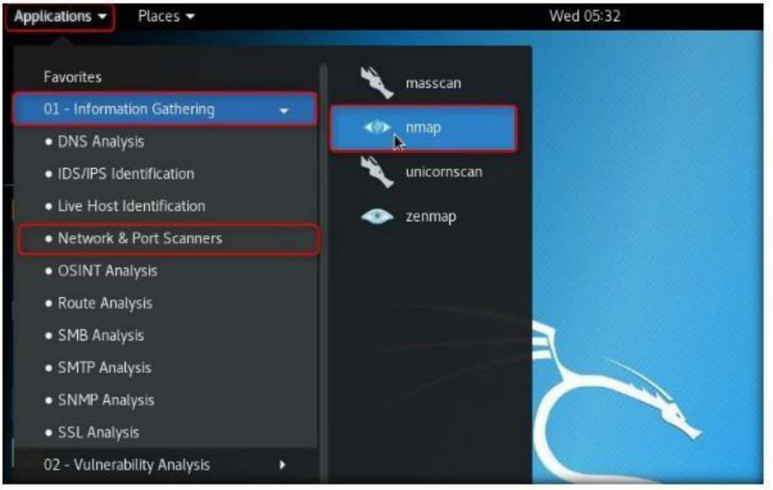

FIGURE 8.2: Launch Nmap in Kali Linux

4. The Nmap application appears in a command line terminal, displaying all the switches that can be used to perform scanning.

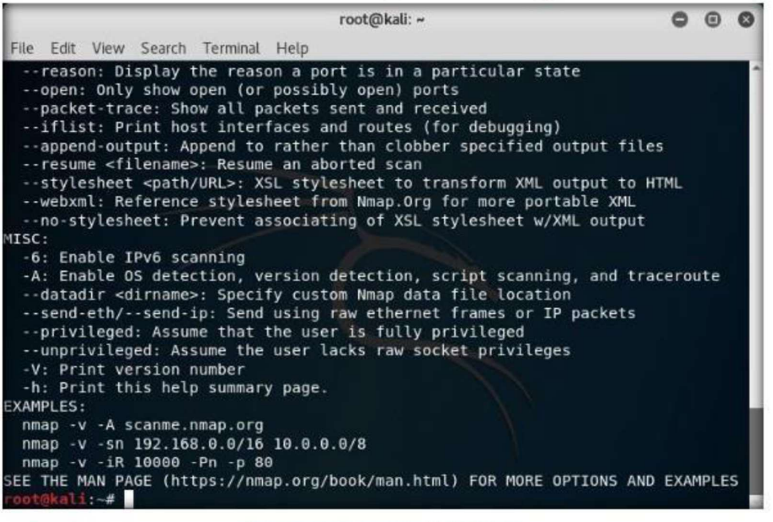

FIGURE 8.3: Nmap in Command Terminal

5. Type **nmap -sP 10.10.10.1/24** and press **Enter** to initiate the ping sweep scan on the entire subnet.

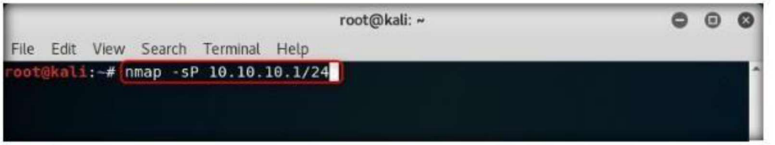

FIGURE 8.4: Nmap Ping Sweep scan

6. Nmap scans all the nodes on the subnet and starts displaying all the hosts that are up and running, along with their respective MAC Addresses and device information, as shown in the following screenshot:

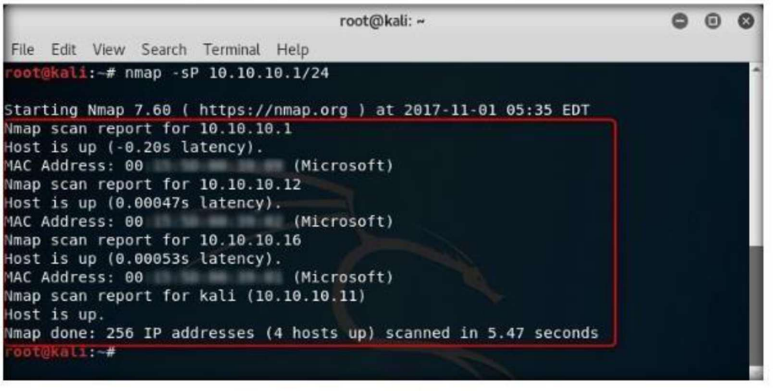

FIGURE 8.5: Nmap Ping Sweep scan results

7. The scan might take comparatively more time to complete. So, after obtaining sufficient number of machines in the scan result, you may terminate the scan by pressing **Ctrl+C**.

8. Now, choose an IP address from the scan result and perform a **stealthy syn scan**. To do so, type **nmap -sS [IP Address of Target Machine]** and press **Enter**. The IP address used in this lab is **10.10.10.12** and this address belongs to **Windows Server 2012**.

Note: The IP address of Windows Server 2012 may differ in your environment.

FIGURE 8.6: Nmap Stelthy Syn Scan

9. By issuing this command, a stealthy syn scan will be initiated.
10. Nmap performs stealthy syn scan and lists all the open ports running on the Windows Server 2012 machine, as shown in the screenshot:

Note: The result returned by Nmap might differ in your lab environment.

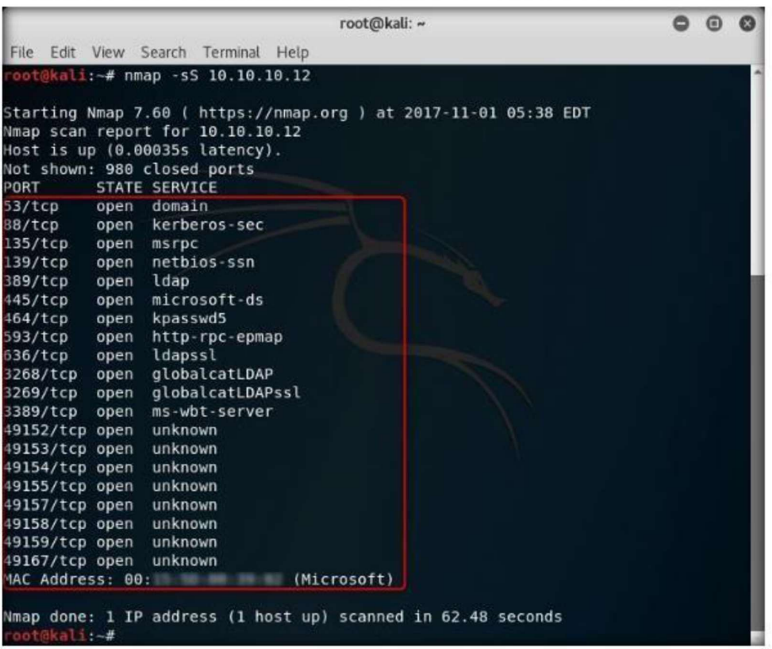

FIGURE 8.7: Nmap Stealthy Syn Scan Results

11. Now that we have obtained all the open ports, along with the services running on them, we will attempt to determine/enumerate the versions of each service running on the ports by performing a syn scan with the version detection switch enabled.

12. To enumerate the versions of the obtained services, type the command **nmap -sSV -O [IP Address of Target Machine]** and press **Enter**. The IP address used in this lab is **10.10.10.12,** and this address belongs to the **Windows Server 2012**.

Note: The IP address of Windows Server 2012 may differ in your lab environment.

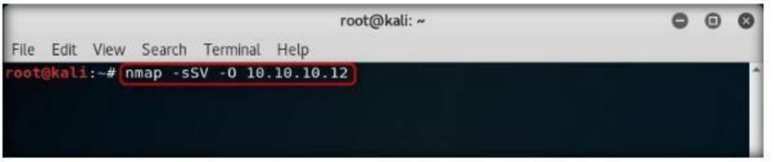

FIGURE 8.8: Nmap Stealthy Syn Scan Version Detection and OS Detection

13. By issuing this command, a stealthy syn scan with version detection along with OS detection will be initiated.

14. Nmap performs the scan and displays the versions of the services, along with an OS fingerprint, as shown in the screenshot:

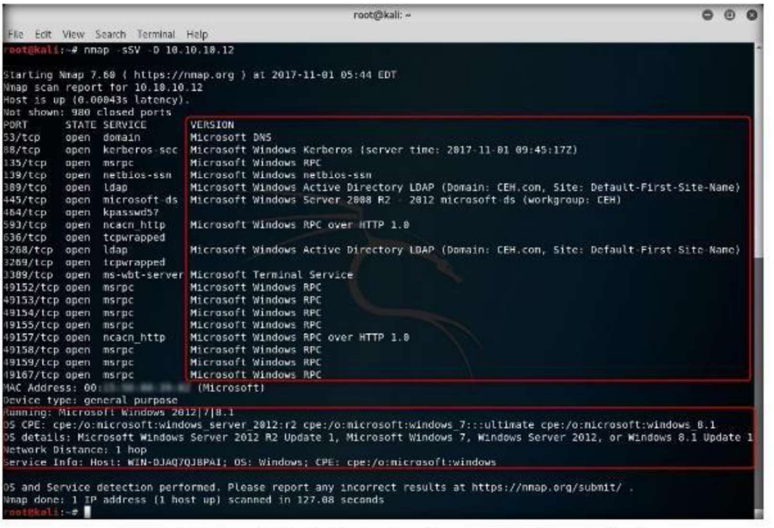

FIGURE 8.9: Nmap Stealthy Syn Scan Version Detection and OS Detection Result

15. Now that you have obtained the enumerated result, you can save this scan result for future reference.

16. Type **nmap -sSV -O [IP Address of Target Machine] -oN Enumeration.txt** and press **Enter**. The IP address used in this lab is **10.10.10.12,** which is assigned to **Windows Server 2012**.

FIGURE 8.10: Nmap Saving Stealthy Syn Scan Result

17. This command performs the **Stealthy Syn Scan with Version Detection and OS Detection** and saves the result to home (root) directory with the name **Enumeration.txt**.

18. On completion of the lab, navigate to **Places → Home** folder.

FIGURE 8.11: Kali Linux Home Folder

19. The **Home** folder appears, displaying the saved **Enumeration.txt** file. You can instead double-click the file to view the same result.

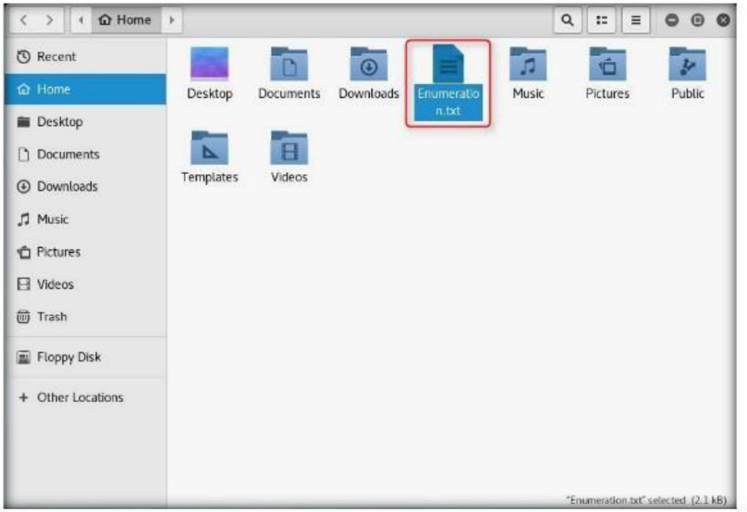

FIGURE 8.12: Stealthy Syn Scan Result File

20. The scan result appears in a text file, as shown in the following screenshot:

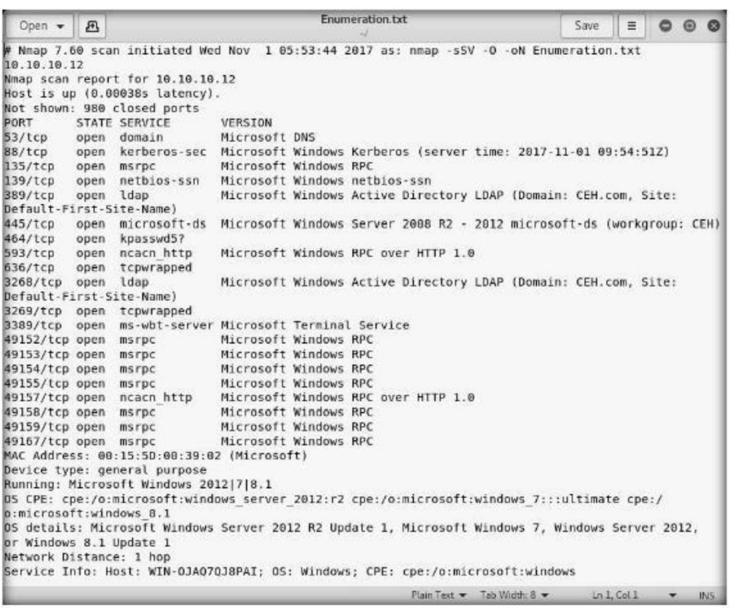

FIGURE 8.13: Stealthy Scan Result

21. Alternatively, you can issue the command **cat Enumeration.txt** in a command-line terminal to view the result:

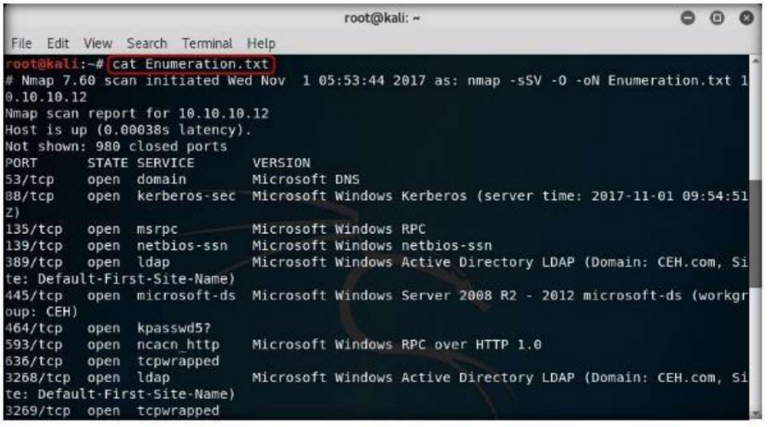

FIGURE 8.14: Stealthy Syn Scan Result viewing by using cat command

22. By performing services enumeration, an attacker might attempt to find vulnerabilities associated with that particular application and exploit them to gain access to the target machine.

Lab Analysis

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

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

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

Lab

9

SNMP Enumeration using snmp_enum

snmp_enum module in Metasploit allows enumeration of any devices with SNMP protocol support. It supports hardware, software, and network information. The default community used is "public".

Lab Scenario

SNMP enumeration is the process of enumerating the users' accounts and devices on a SNMP enabled computer. SNMP service comes with two passwords, which are used to configure and access the SNMP agent from the management station. They are: Read community string and Read/Write community string. These strings (passwords) come with a default value, which is same for all the systems. Hence, they become easy entry points for attackers if left unchanged by the administrator. Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, shares, etc., and network information such as ARP tables, routing tables, device specific information, and traffic statistics.

As an ethical hacker or an information security officer, it is imperative for you to find the default community strings and patch them up.

Lab Objectives

The objective of this lab is to help students understand and enforce various enumeration techniques to:

- Connected Devices
- Hostname and information
- Domain
- Hardware and storage information
- Software Components
- Total Memory

Lab Environment

To perform this lab, you will need:

- Kali Linux running as the Attacker Machine
- WindowsServer2012 as the Victim Machine
- Administrative privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Lab

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system. These techniques are conducted in an intranet environment.

Lab Tasks

1. Before starting SNMP enumeration, first we need to find out whether the SNMP port is opened. SNMP uses port 161 by default; to check whether this port is opened, we first need to run Nmap port scan.
2. Launch a command terminal, type **nmap -sU -p 161 <Target machine IP address>** and press **Enter** (in the **Kali Linux** attacker machine).
3. In this lab, our victim machine is the **Windows Server 2012** machine, with IP address **10.10.10.12**.

   Note: The IP addresses shown in this lab may differ in your lab environment.

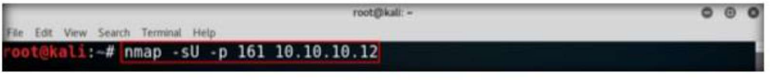

FIGURE 9.1: Performing Nmap UDP scan

4. Now you can see that port **161** is open and is used by **SNMP,** as shown in the following screenshot.

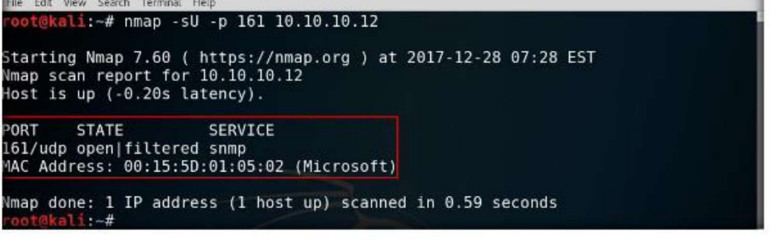

FIGURE 9.2: Nmap UDP scan result

5. Type **nmap -sU -p 161 --script=snmp-brute <Target machine IP Address>** and press **Enter**.
6. This script will extract the SNMP community string from the target machine.
7. It will search pcap socket in parallel threads. The sending sockets sends the SNMP probes along with the community strings with valid credentials.

FIGURE 9.3: Nmap finding SNMP community string

8. The script output will be displayed as shown in the screenshot. Now the extracted SNMP port is used by the public (community string) and with valid credentials.
9. If the target machine doesn't have a valid account, no output will be displayed.

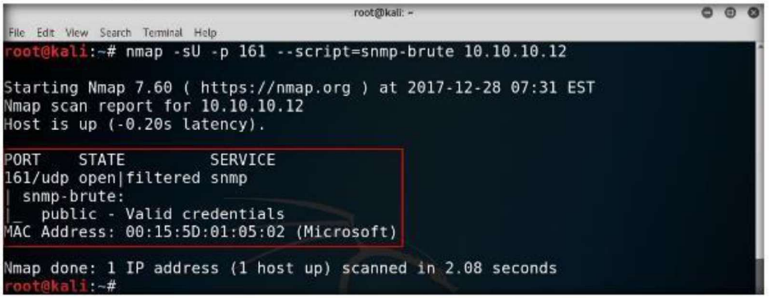

FIGURE 9.4: SNMP Community String found with Valid Credentials

10. Now perform **SNMP** enumeration on the target machine. In a command-line terminal, type **msfconsole** and press **Enter**.

FIGURE 9.5: Launching Metasploit Framework

11. Now, type **use auxiliary/scanner/snmp/snmp_login** and press **Enter**.

FIGURE 9.6: Launching snmp_login module

12. Now, to see what are the options available with snmp_login, type **show options** and press **Enter**. This will list out all the commands and usage.

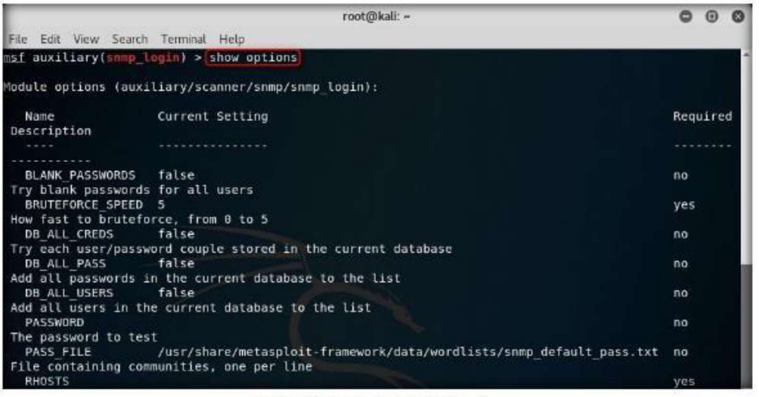

FIGURE 9.7: Viewing Module Options

13. Now, type **setg RHOSTS 10.10.10.12** and press **Enter**.

Note: In this lab, **10.10.10.12** is the IP Address of the **Windows Server 2012** and this might vary in your lab environment.

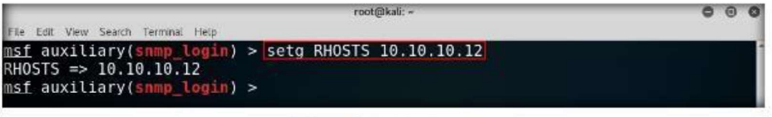

FIGURE 9.8: Setting Options

14. We have set the all the required options for SNMP enumeration. Now, type **exploit** and press **Enter**.

15. Once you press **Enter**, you can see that the victim machine (Windows Server 2012) has given access to the community '**public**' as shown in the screenshot.

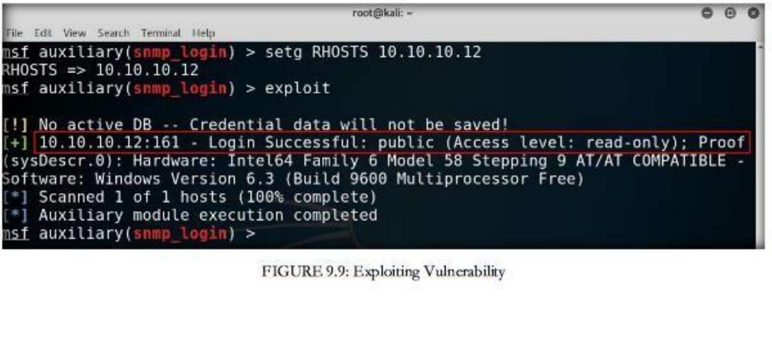

FIGURE 9.9: Exploiting Vulnerability

16. Now, type **use auxiliary/scanner/snmp/snmp_enum** and press **Enter**.

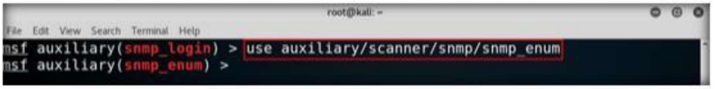

FIGURE 9.10: Launching snmp_enum Auxiliary Module

17. Now, type **exploit** and press **Enter**. This will enumerate the target machine and list down all the required sensitive information.

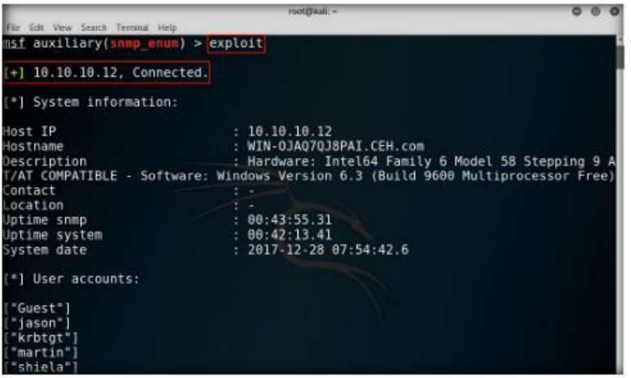

FIGURE 9.11: Exploiting Vulnerability

18. **snmp_enum** enumerates the target machine information, as shown in the screenshot.
19. First, it displays the **System Information**:
    a. Host IP
    b. Host Name
    c. Hardware Description
    d. System Uptime
    e. SNMP Uptime
    f. Domain if system is connected in Domain

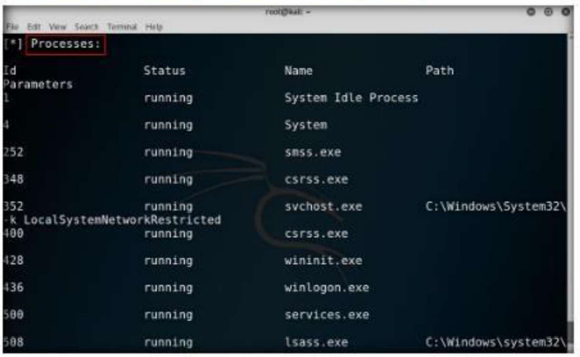

FIGURE 9.12: System Information Obtained

20. It also displays the **User accounts** associated with the target machine. Scroll down to view more sensitive information like Network Information, MAC Address, Running Processes, Installed Applications and Softwares, etc.

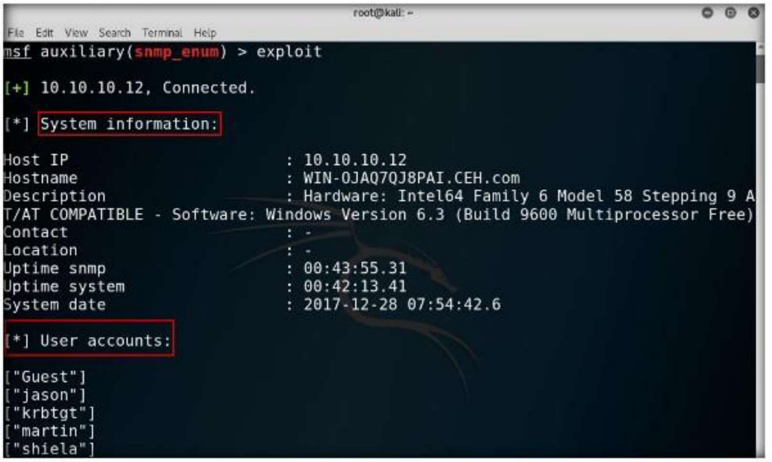

FIGURE 9.13: Viewing Other Information

Lab Analysis

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

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

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

Lab

10

LDAP Enumeration using Active Directory Explorer (ADExplorer)

The Lightweight Directory Access Protocol (LDAP) is used to get to catalog postings inside active directory or other directory services. A directory is generally ordered in a various leveled and sensible arrangement, rather like the levels of administration and representatives in an organization. LDAP is often tied into the domain name system to allow incorporated brisk lookups and quick determination of questions.

Lab Scenario

A penetration test begins before testers have even made contact with victim systems. During enumeration, information is systematically collected and individual systems are identified. Pen testers examine the systems in their entirety, which allows them to evaluate security weaknesses. In this lab, we discuss Nmap, which uses raw IP packets in novel ways to determine what hosts are available on a network, what services (application names and versions) those hosts are offering, what OSs (and versions) they are running, and what type of packet filters/firewalls are in use. Nmap was designed to rapidly scan large networks; by using open ports, attackers can easily attack target machines. To protect against this type of attack, networks are typically bolstered with IP filters, firewalls, and other obstacles.

As an Expert Ethical Hacker and Penetration Tester, you will need to enumerate a target network and extract a list of computers, user names, user groups, machine names, network resources, and services using various enumeration techniques.

Lab Objectives

The objective of this lab is to help students understand and perform enumeration on a target network using various techniques to obtain:

- User names and user groups
- Attributes

Lab Environment

To perform this lab, you will need:

- Active Directory Explorer located at **Z:\CEH-Tools\CEHv10 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer**
- You can download the latest version of Active Directory Explorer from the link **https://technet.microsoft.com/en-us/library/bb963907.aspx**
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running a Windows Server 2012 Machine
- A computer running with Windows Server 2016 machine
- Administrative privileges to install and run tools

Lab Duration

Time: 5 Minutes

Overview of Enumeration

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an intranet environment.

Lab Tasks

The basic idea in this section is to:

- Perform LDAP Enumeration on an Active Directory Domain system
- Modifying Domain User Accounts

1. Now switch to Windows Server 2016 machine and navigate to **Z:\CEH-Tools\CEHv10 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer**, and double-click **ADExplorer.exe**.
2. **Active Directory Explorer License Agreement** window appears; click **Agree**.

FIGURE 10.1: Open File – Security Warning

3. The **Connect to Active Directory** pop-up appears; type the IP address of the Windows Server 2012 IP (**10.10.10.12**) and click **OK**.

   Note: IP Addresses may differ in your lab environment.

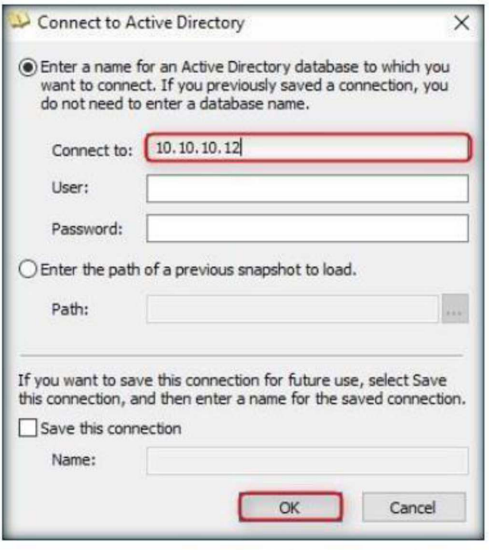

FIGURE 10.2: ADExplorer Connect to Active Directory

4. The **Active Directory Explorer** displays the active directory structure in the left pane, as shown in the following figure.

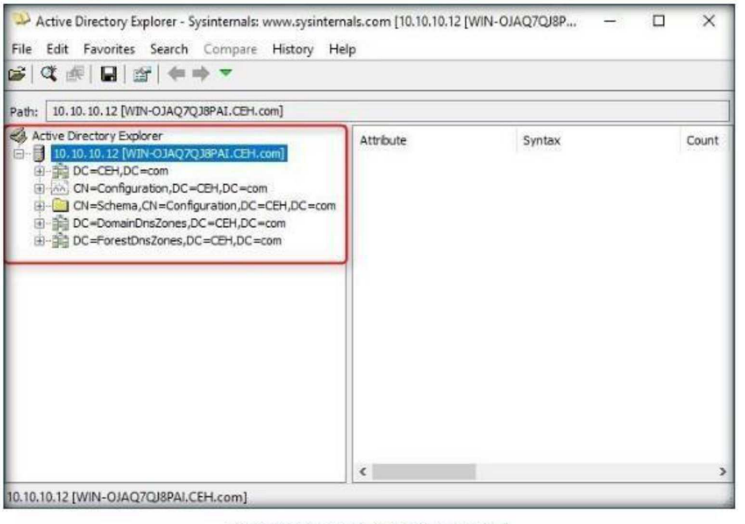

FIGURE 10.3: ADExplorer Main Window

5. Now, expand **DC=CEH,DC=com** and **CN=Users** to explore domain user details.

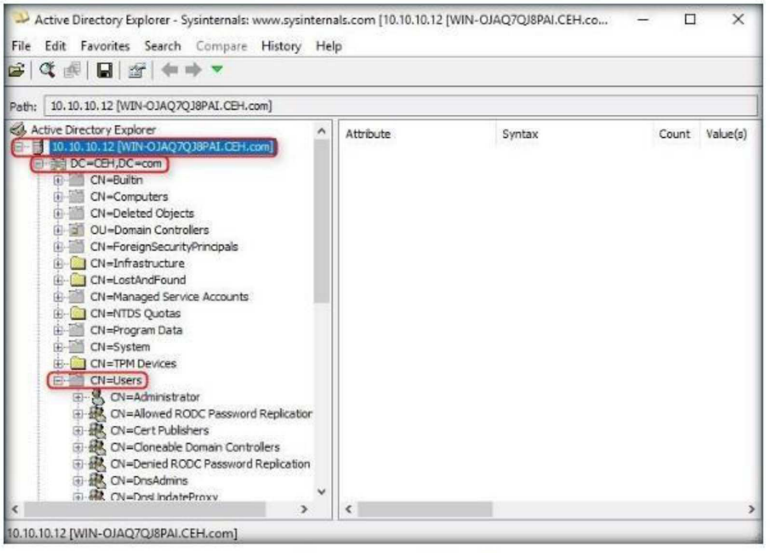

FIGURE 10.4: ADExplorer Domain Users Node

6. Click any **user name** (in the left pane) to display its properties in the right pane.

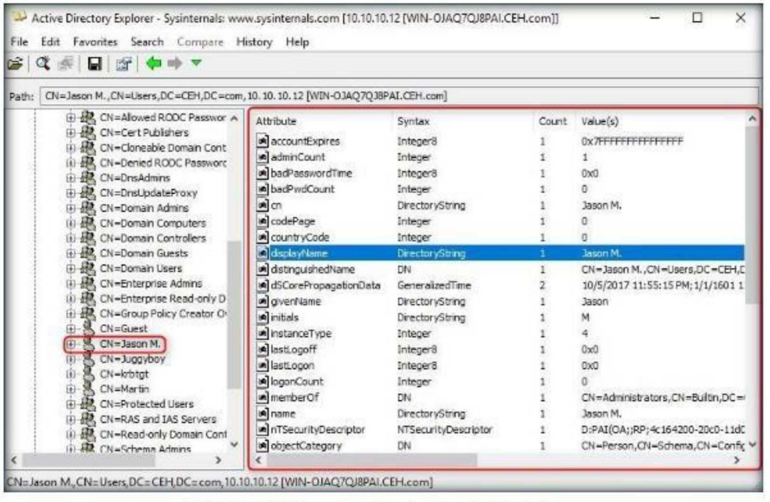

FIGURE 10.5: ADExplorer Domain Users Profile Attributes

7. Right-click any attribute (in the right pane), and click **Modify...** from the context menu to modify that user's profile.

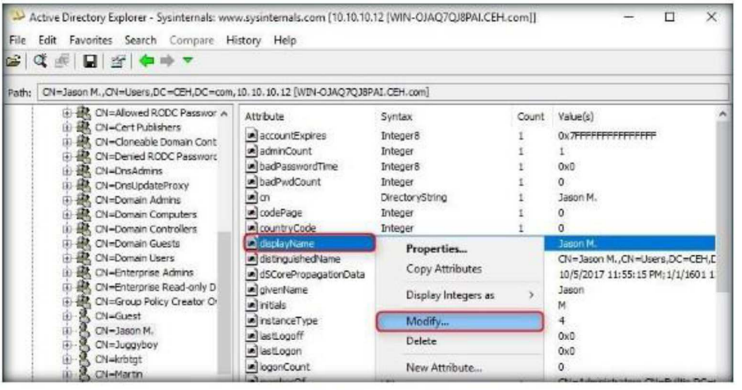

FIGURE 10.6: ADExplorer User Profile Modification

8. The **Modify Attribute** window appears where you can modify the user profile.

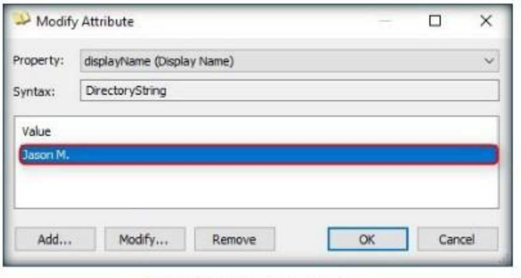

FIGURE 10.7: Modifying Attributes

9. Similarly, you can check with the other user profile attributes.

Lab Analysis

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

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

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

Lab

11

Enumerating Information from Windows and Samba Host using Enum4linux

A Linux alternative to enum.exe for enumerating data from Windows and Samba hosts.

Lab Scenario

Enum4linux is a tool for enumerating information from Windows and Samba systems. As a security expert you have to secure process where the attacker can establish an active connection with the victim and try to discover as many attack vectors as possible, which can be used to exploit the systems further. You should know what info is available to the attacker and secure that info before anyone misuses it.

Lab Objectives

The objective of this lab is to help students understand and enforce various enumeration techniques to enumerate:

- Connected Devices
- Hostname and information
- Domain
- Hardware and storage information
- Software Components
- Total Memory

Lab Environment

To perform this lab, you will need:

- Kali Linux running as the Attacker Machine
- Windows Server 2012 as the Victim Machine

- Administrative privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Lab

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system. These techniques are conducted in an intranet environment.

Lab Tasks

Before starting this lab, turn on the Windows Server 2012 machine and login.

1. Now start the **Kali Linux** machine and open a **Terminal** window. In the terminal window type **enum4linux -h** and hit **Enter** to get the help options of enum4linux.

FIGURE 11.1: Enum4linux help command

2. Help options appear as shown in the screenshot. Now in this lab we will only demonstrate only a few options to conduct enumeration on the target machine.

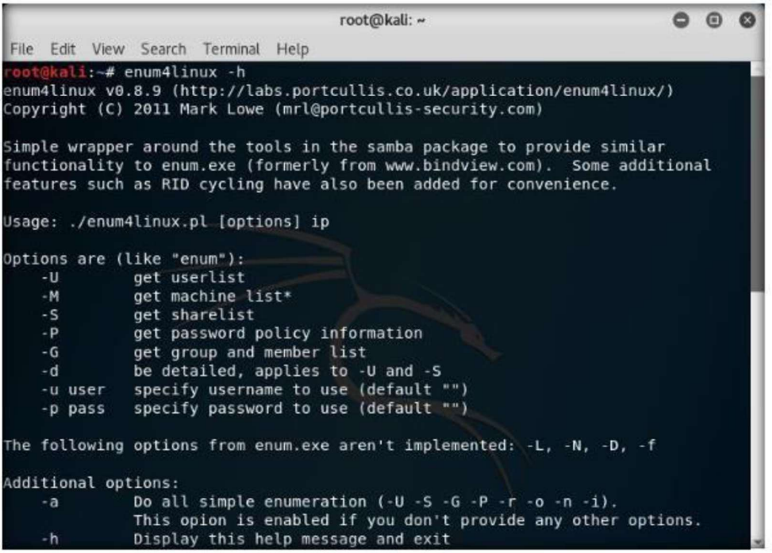

FIGURE 11.2: Enum4linux help options

3. In the terminal window type **enum4linux -u martin -p apple -U 10.10.10.12** and hit **Enter** to run this tool using the User list option.

   Note: Here 10.10.10.12 is the IP address of the Windows Server 2012; this might be different for your lab environment.

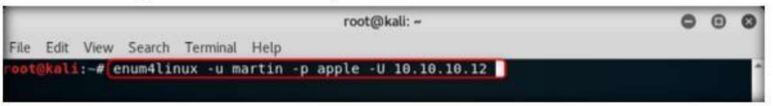

FIGURE 11.3: Enum4linux command with User list option enabled

4. Enum4linux starts enumerating the workgroups/domains first and displays the results as shown in the screenshot.

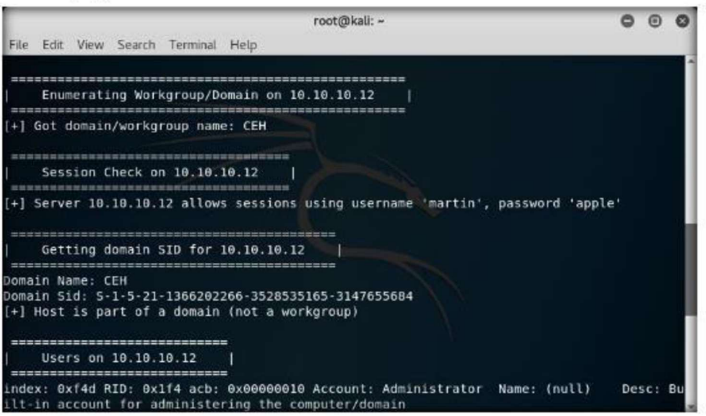

FIGURE 11.4: Enum4linux enumerating the domain information of the target

5. Then it lists out the Users info with their respective RIDs as shown in the screenshot.

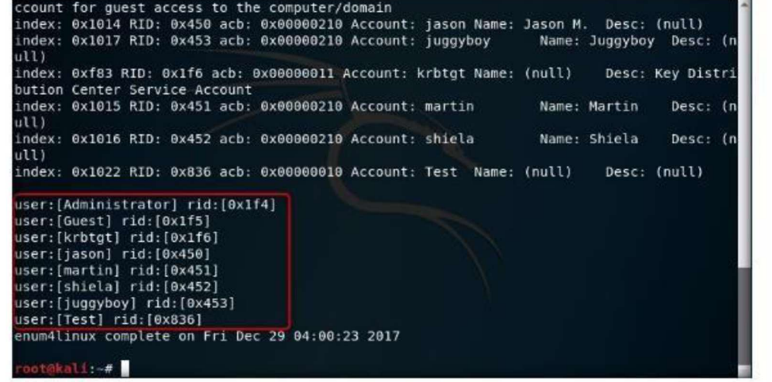

FIGURE 11.5: User info with their respective RIDs

6. Now to get the OS information of the target, type **enum4linux -u martin -p apple -o 10.10.10.12** and hit **Enter**.

FIGURE 11.6: Enum4linux command for enumerating OS information

7. The tool enumerates the target system and lists out its OS details as shown in the screenshot.

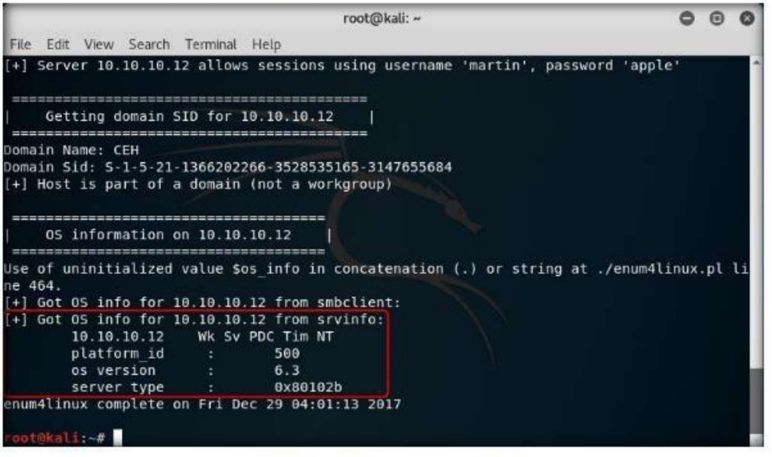

FIGURE 11.7: OS information of the target

8. Now we will enumerate the password policy information of our target machine. In the terminal window, type **enum4linux -u martin -p apple -P 10.10.10.12** and hit **Enter**.

FIGURE 11.8: Enum4linux command to enumerate password policy information

9. The tool enumerates the target system and displays its password policy information as shown in the screenshot.

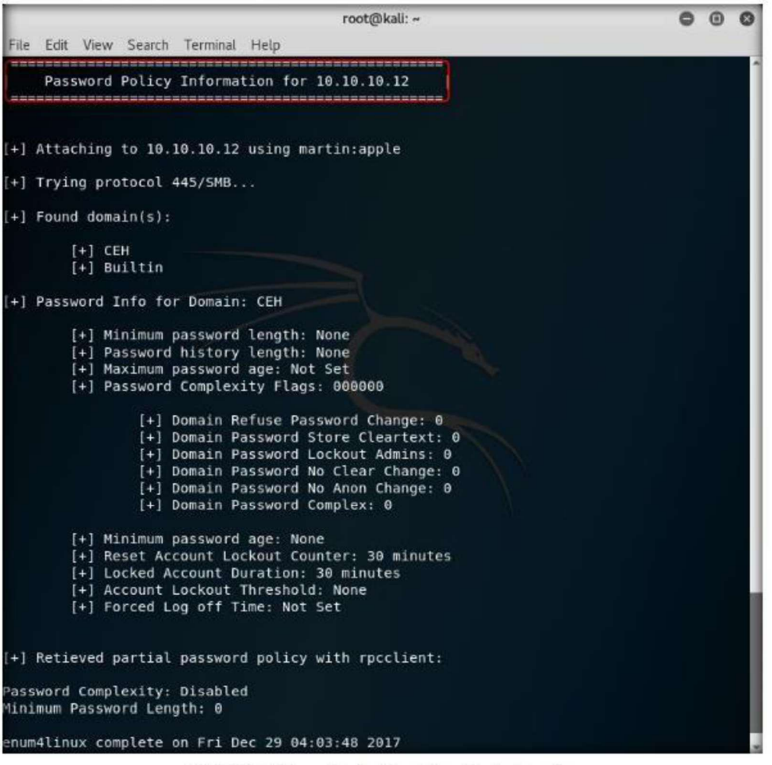

FIGURE 11.9: Password policy information of the target machine

10. Now we will enumerate the group policy information of our target machine. In the terminal window, type **enum4linux -u martin -p apple -G 10.10.10.12** and hit **Enter**.

FIGURE 11.10: Enum4linux command for group and domain info

11. The tool enumerates the target system and displays the group policy information as shown in the screenshot.

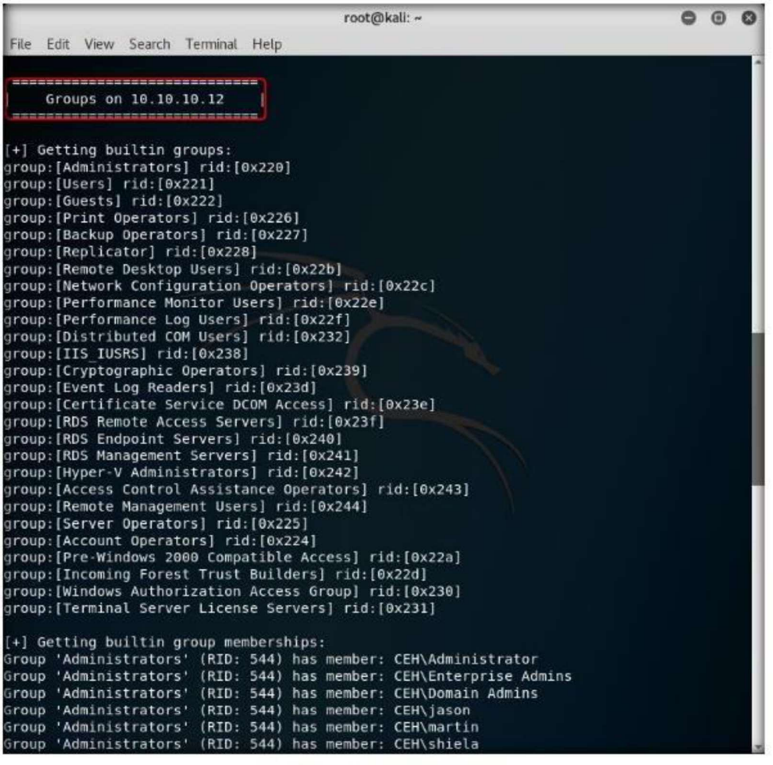

FIGURE 11.11: Group info of the target

12. It further enumerates the local and domain group memberships and displays them as given in the screenshot.

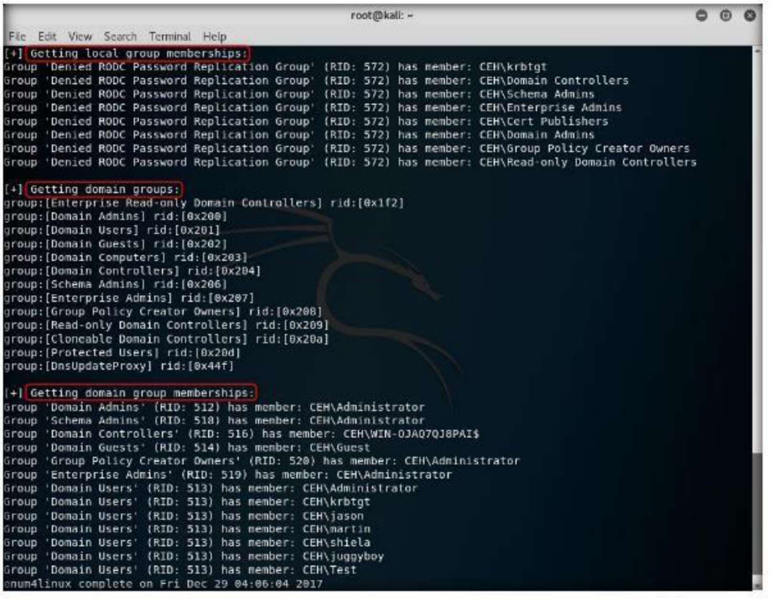

FIGURE 11.12: Domain and group memberships of the target system

13. To enumerate the share policy information of our target machine, type **enum4linux -u martin -p apple -S 10.10.10.12** and hit **Enter**.

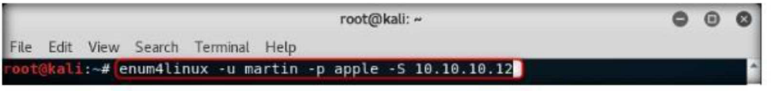

FIGURE 11.13: Enum4linux command to get the share info

14. The tool conducts share enumeration on the target system and displays the share information as shown in the screenshot.

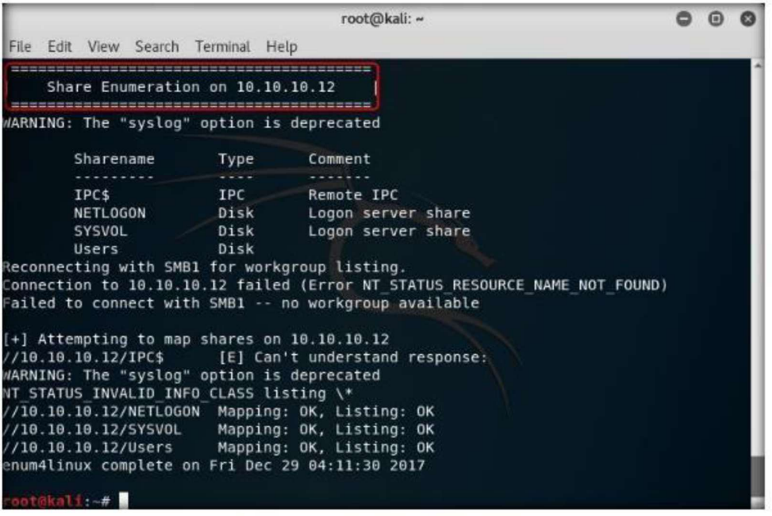

FIGURE 11.14: Share info of the target system

Lab Analysis

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

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

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