





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.

ICON KEY

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

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

 **Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 04 Enumeration**

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.

TASK 1

Overview

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 (ADEplorer)**
- 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.





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.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

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

 **Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks**

Module 04 – Enumeration

- 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

TASK 1

Install Global Network Inventory

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.

Scan computers by IP range, by domain, single computers, or computers, defined by the Global Network Inventory host file.

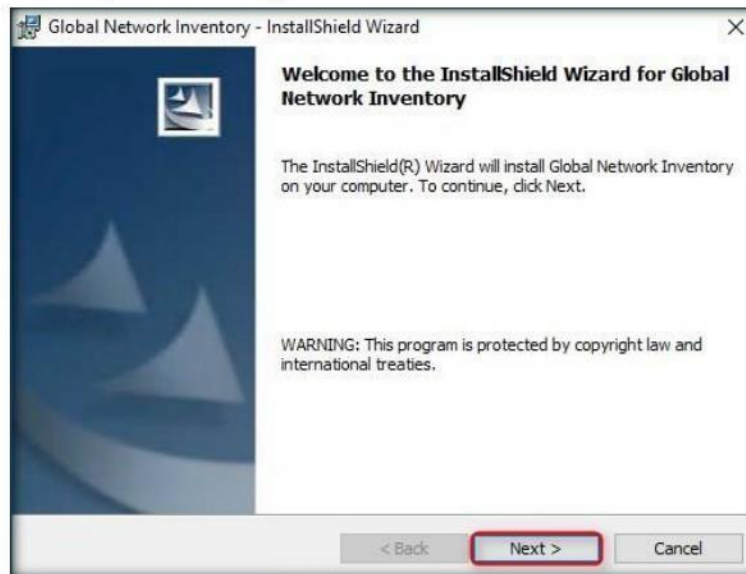


FIGURE 1.1: Global Network Inventory Installation Wizard

Module 04 – Enumeration

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

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

Fully customizable layouts and color schemes on all views and reports. Export data to HTML, XML, Microsoft Excel, and text formats.

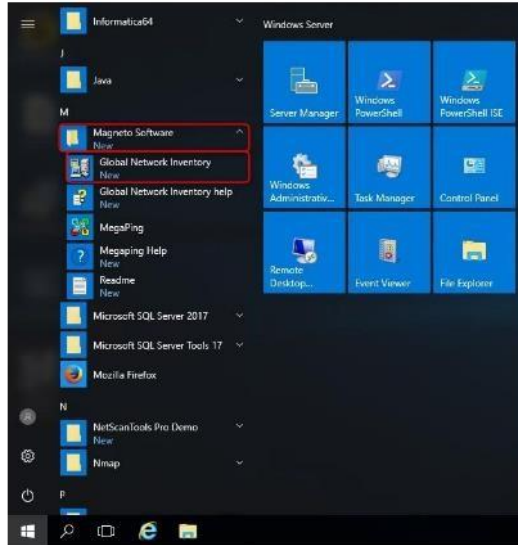


FIGURE 1.2: Run Global Network Inventory from start menu



FIGURE 1.3: Global Network Inventory License information screen

Module 04 – Enumeration

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

Scan only items that you need by customizing scan elements.

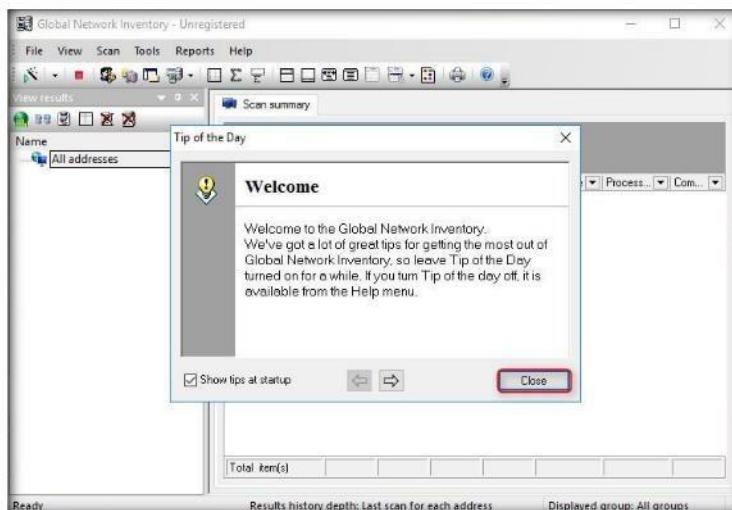


FIGURE 1.4: Global Network Inventory main window

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**.

TASK 2
Configure Global Inventory Scanner

Views scan results, including historic results for all scans, individual machines, or selected number of addresses.



FIGURE 1.5: Global Network Inventory new audit wizard

Module 04 – Enumeration

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

Fully customizable layouts and color schemes on all views and reports.

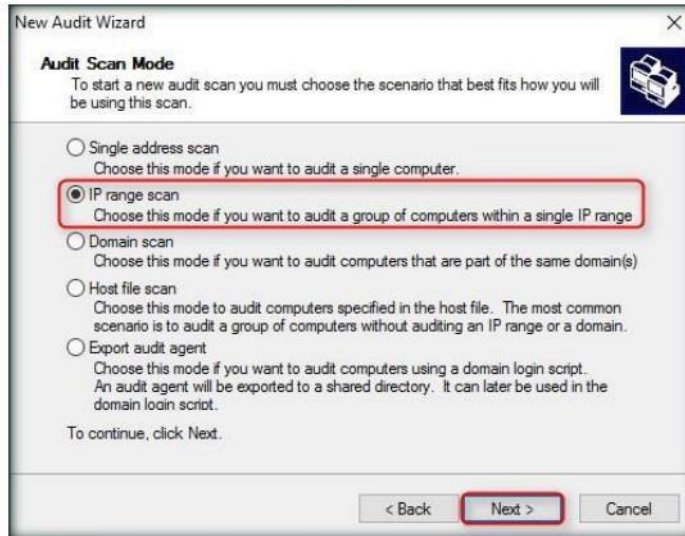


FIGURE 16: Global Network Inventory Audit Scan Mode section

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

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

Licenses are network-based rather than user-based. In addition, extra licenses to cover additional addresses can be purchased at any time if required.

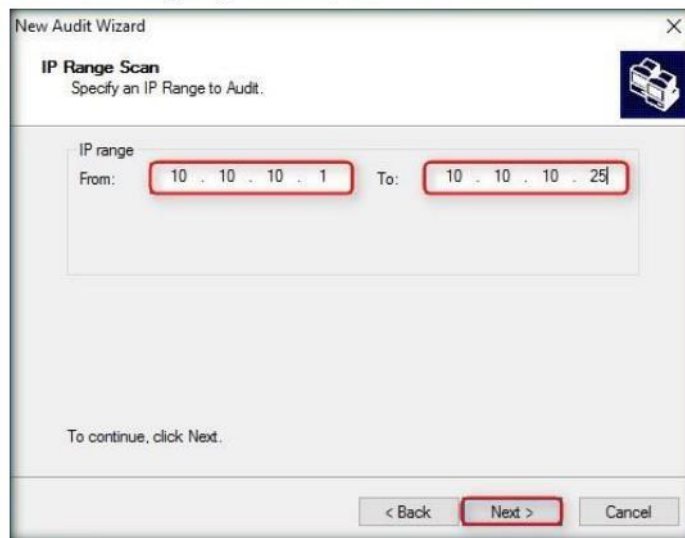


FIGURE 17: Setting an IP range to scan

Module 04 – Enumeration

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

The program comes with dozens of customizable reports. New reports can be easily added through the user interface.

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 perform a scan to determine which machines 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.

Ability to generate reports on schedule after every scan, daily, weekly, or monthly.



FIGURE 1.8 Global Network Inventory Authentication settings

Module 04 – Enumeration

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

To configure reports, choose **Reports** | **Configure reports** from the main menu and select a report from a tree control on the left. Each report can be configured independently.



FIGURE 1.9: Global Network Inventory final Audit wizard

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

Filtering is a quick way to find a subset of data within a dataset. A filtered grid displays only the nodes that meet the criteria you specified for a column(s).

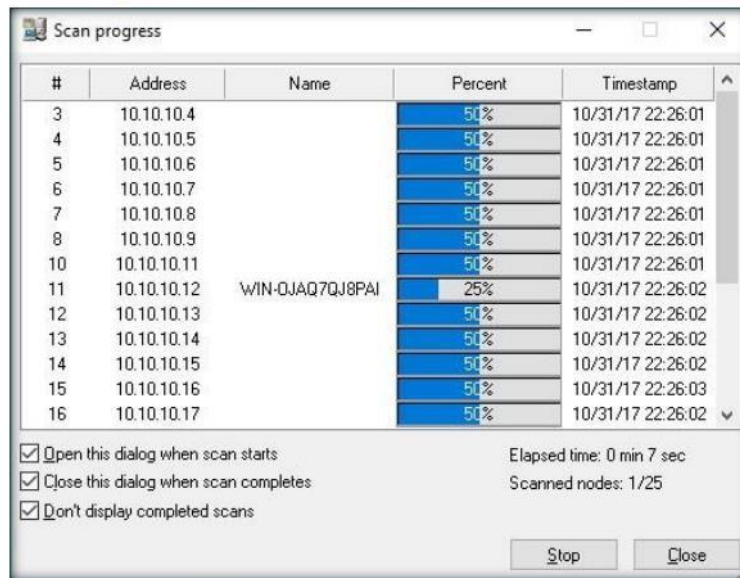


FIGURE 1.10: Global Network Inventory Scanning Progress

Module 04 – Enumeration

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

Global Network Inventory lets you change grid layout simply by dragging column headers using the mouse. Dropping a header onto the Grouping pane groups data according to the values stored within the "grouped" column.

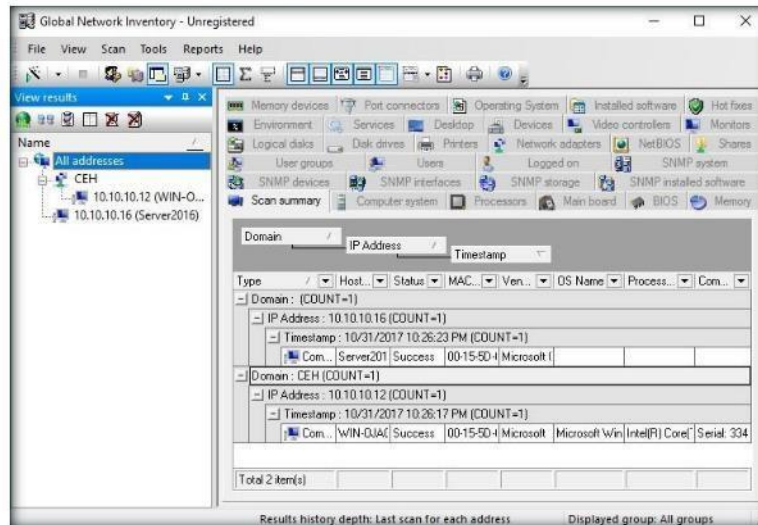


FIGURE 1.11: Global Network Inventory result window

TASK 3
Examine the Scanned Machine

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.

Global Network Inventory grid color scheme is completely customizable. You can change Global Network Inventory colors by selecting **Tools | Grid colors** from main menu and changing colors.

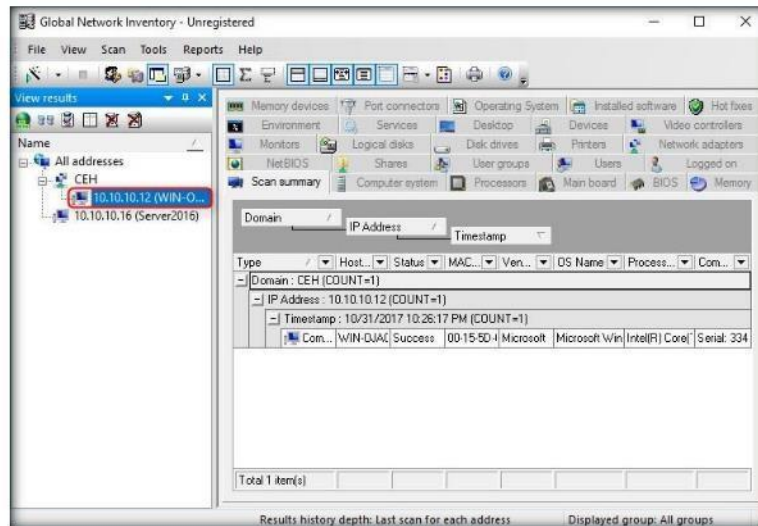


FIGURE 1.12: Global Network Inventory Individual machine results

Module 04 – Enumeration

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

To configure results history level choose Scan | Results history level from the main menu and set the desired history level.

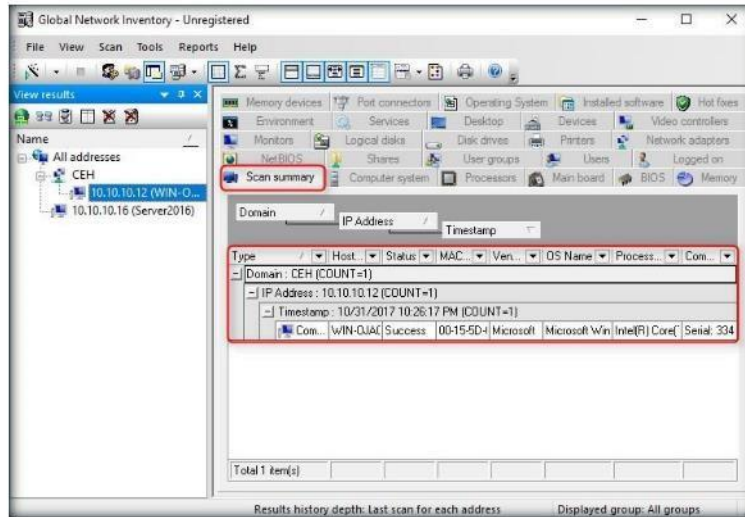


FIGURE 1.13: Global Inventory Scan Summary tab

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

Reliable IP detection and identification of network appliances such as network printers, document centers, hubs, and other devices.

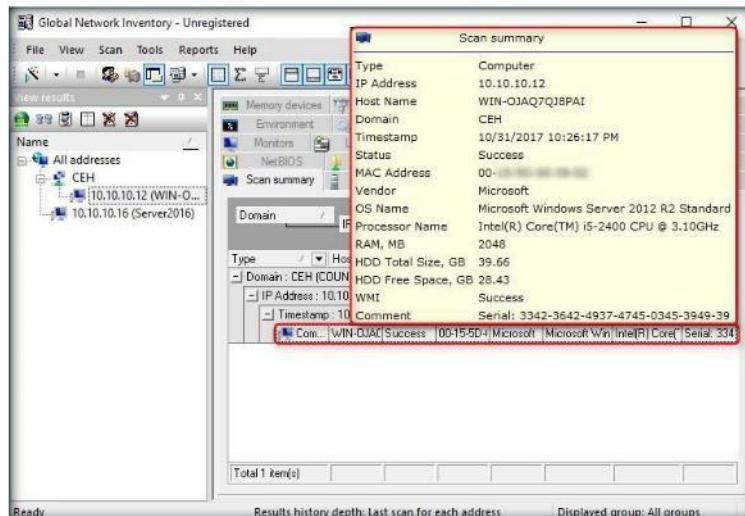


FIGURE 1.14: Global Inventory displaying the Scan summary

Module 04 – Enumeration

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

Export data to HTML, XML, Microsoft Excel, and text formats.

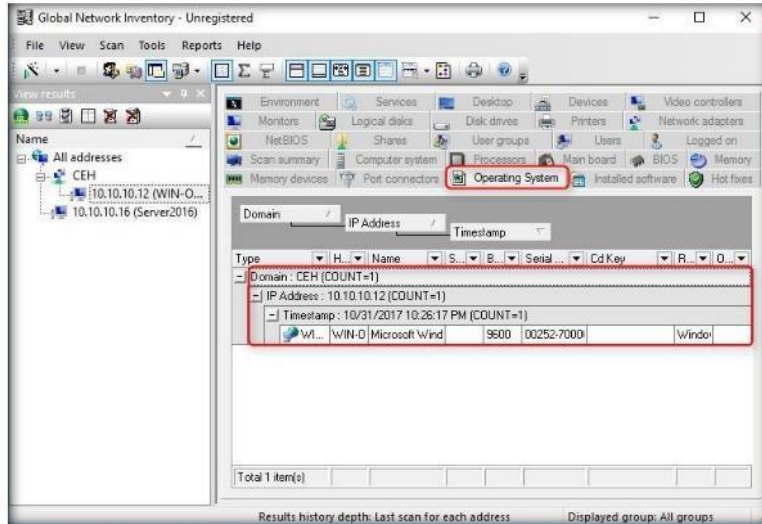


FIGURE 1.15: Global Inventory Operating System tab

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

Schedule inventory scans to run at specified times, hourly, daily, weekly, monthly, and annually. Ability to generate reports on schedule after every scan, daily, weekly, or monthly.

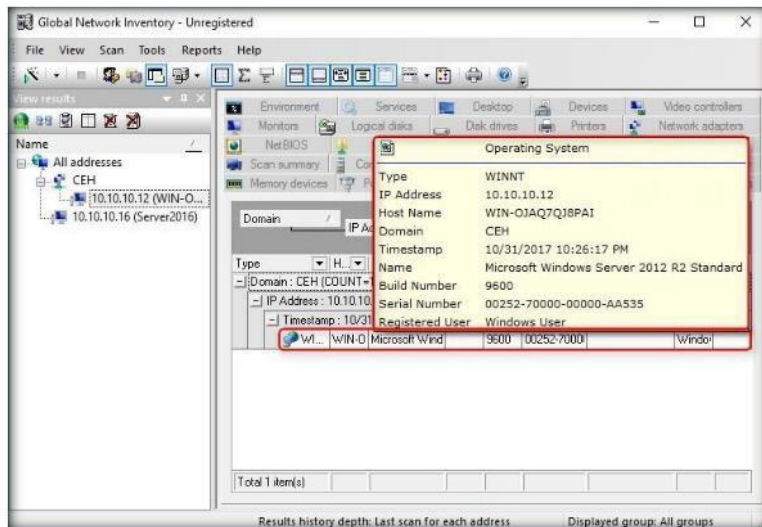


FIGURE 1.16: Global Inventory displaying the operating system details

Module 04 – Enumeration

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

Scan only items that you need by customizing scan elements.

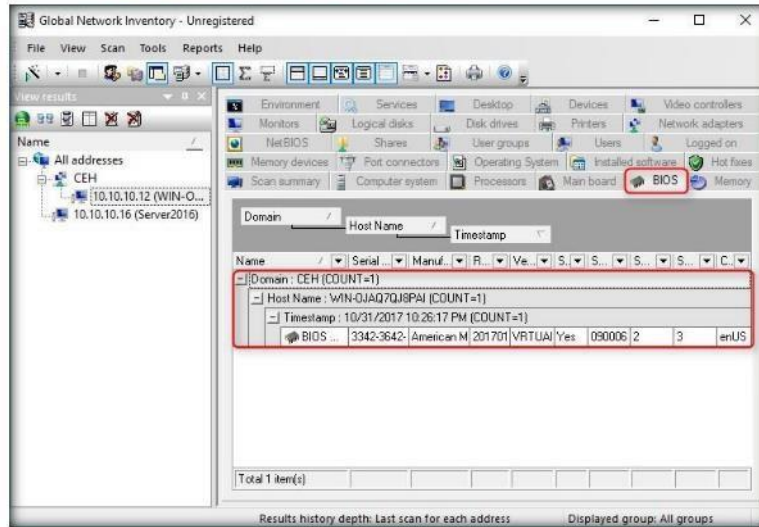


FIGURE 1.17: Global Network Inventory BIOS summary tab

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

E-mail address - Specifies the e-mail address that people should use when sending e-mail to you at this account. The e-mail address must be in the format name@company—for example, someone@mycompany.com.

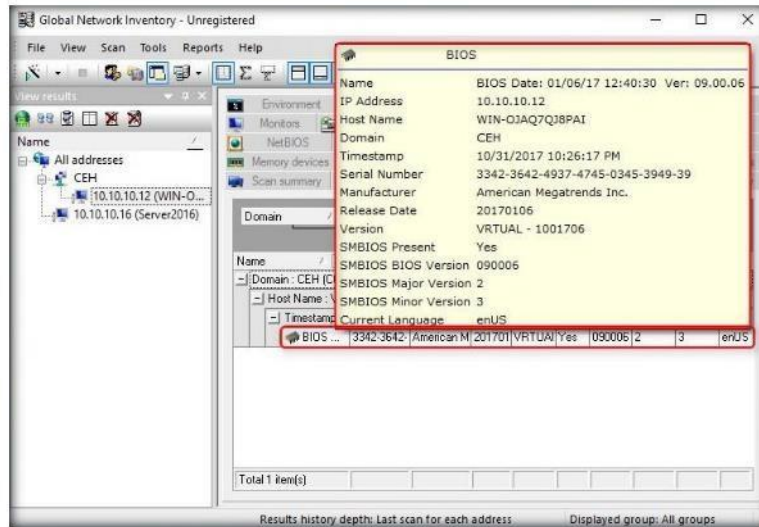


FIGURE 1.18: Global Network Inventory displaying the Bios summary information

Module 04 – Enumeration

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

NetBIOS provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network.

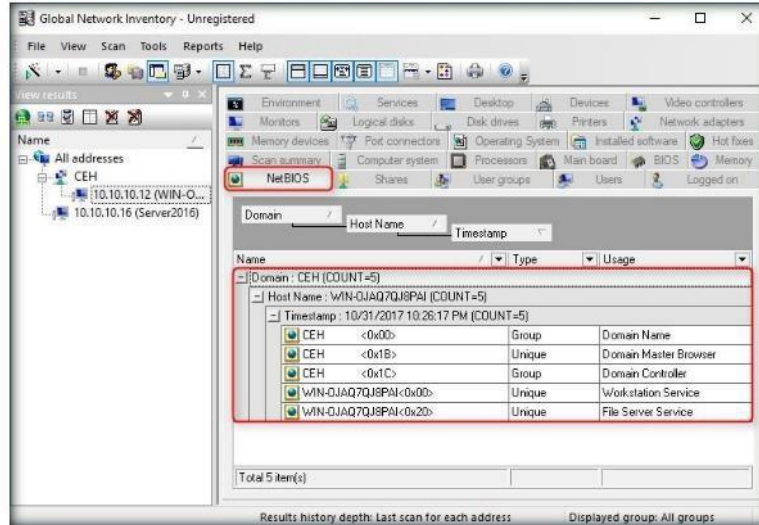


FIGURE 1.19: Global Network Inventory NetBIOS tab

22. Click each NetBIOS application to view its details.

Message subject - Type the Subject of your message. Global Network Inventory cannot post a message that does not contain a subject.

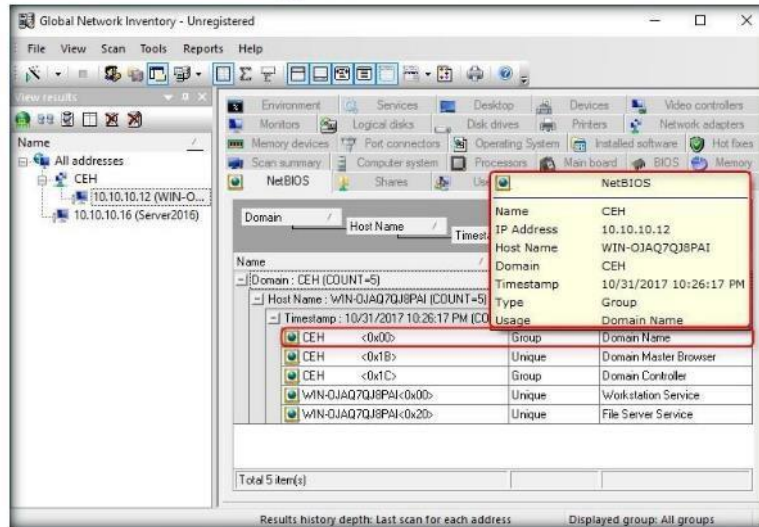


FIGURE 1.20: Global Network Inventory displaying the NetBIOS information

Module 04 – Enumeration

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

Name - Specifies the friendly name associated with your e-mail address. When you send messages, this name appears in the From box of your outgoing messages.

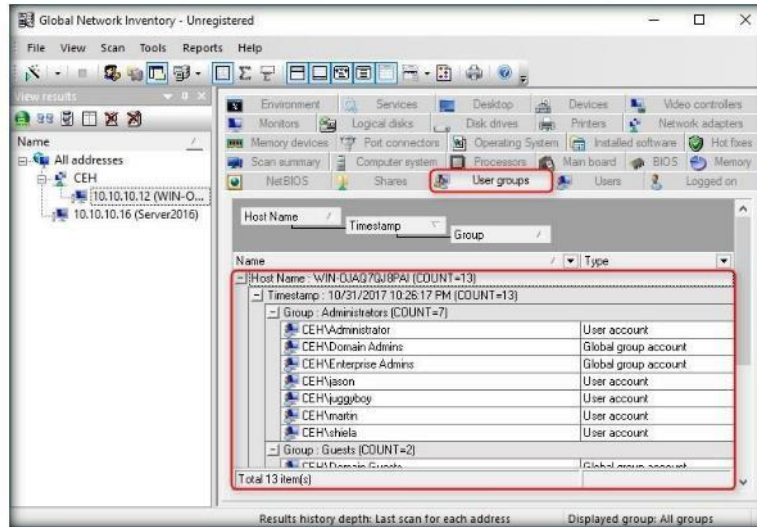


FIGURE 1.21: Global Network Inventory User groups tab

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

Global Network Inventory agent can also be deployed to perform regular audits initiated through the domain login script when your users log on the network. In this scenario, Global Network Inventory agent is exported to a shared network directory, and audit results are collected in audit repository directory as snap files and later merged into the main database.

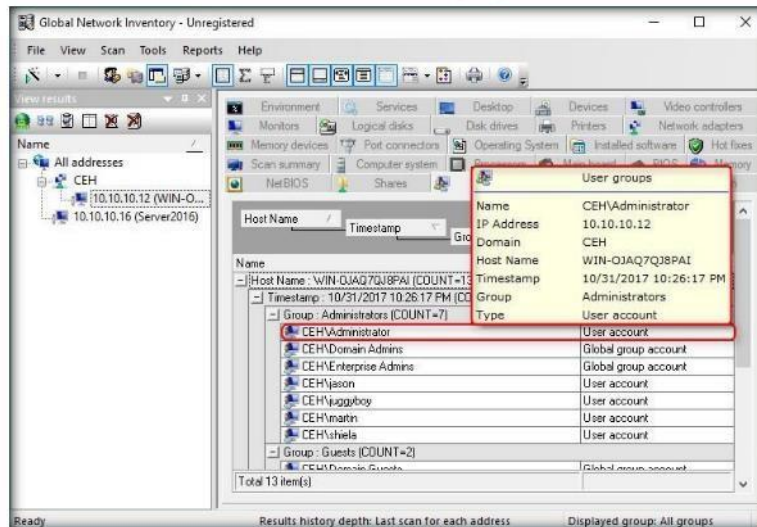


FIGURE 1.22: Global Network Inventory displaying the User groups information

Module 04 – Enumeration

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

Port - Specifies the port number you connect to on your outgoing e-mail (SMTP) server. This port number is usually 25.

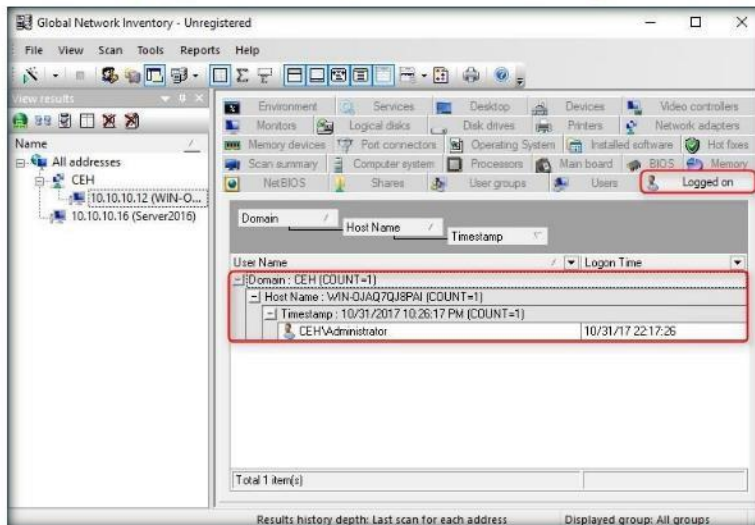


FIGURE 1.23: Global Network Inventory Logged on tab

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

Outgoing mail (SMTP) - Specifies your Simple Mail Transfer Protocol (SMTP) server for outgoing messages.

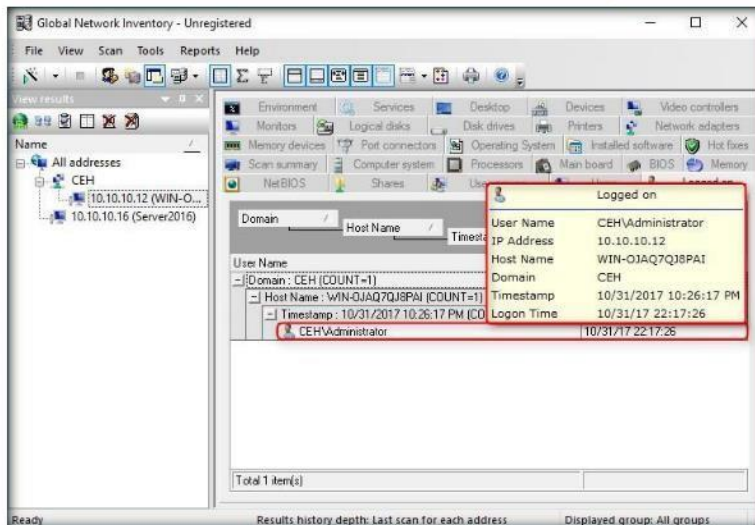


FIGURE 1.24: Global Network Inventory displaying the Logged on information

Module 04 – Enumeration

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

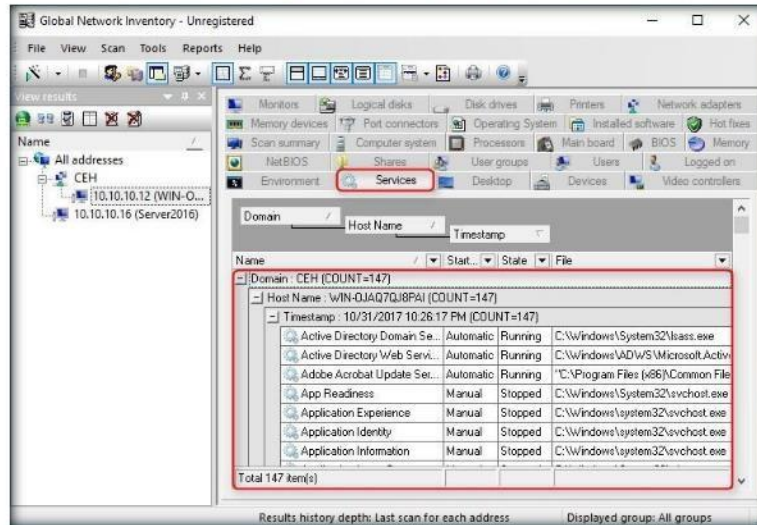


FIGURE 1.25: Global Network Inventory Services tab

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

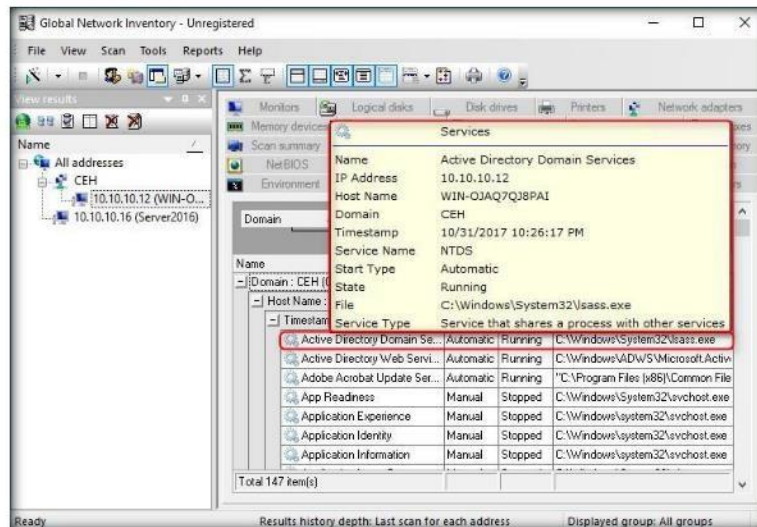
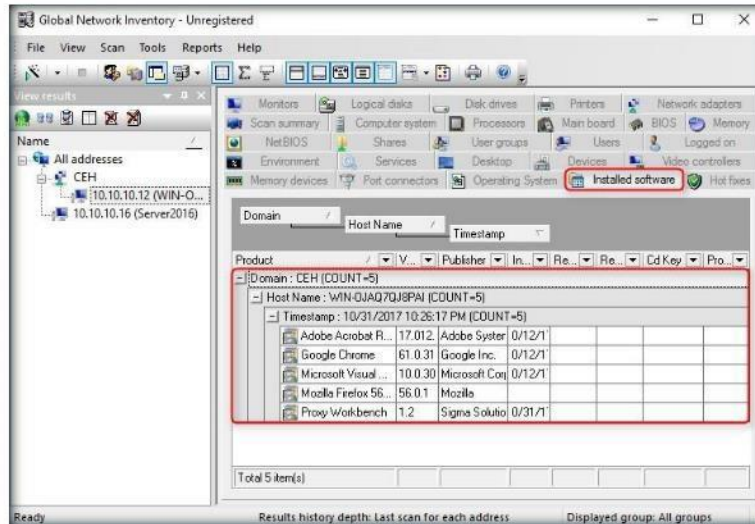


FIGURE 1.26: Global Network Inventory displaying the Services information

To create a new custom report that includes more than one scan element, click choose Reports | Configure reports from the main menu, click the Add button on the reports dialog, customize settings as desired, and click the OK button.

Module 04 – Enumeration

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



ⓘ A security account password is created to make sure that no other user can log on to Global Network Inventory. By default, Global Network Inventory uses a blank password.

FIGURE 1.27: Global Network Inventory Installed software tab

30. Hover over software names to view their details.

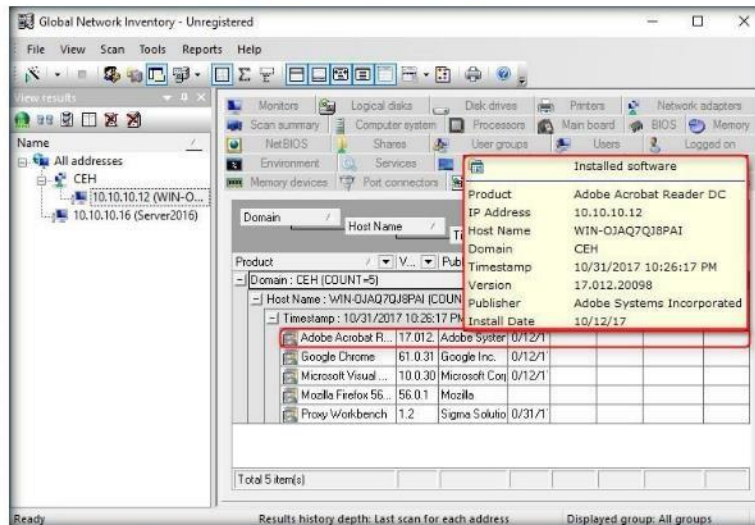


FIGURE 1.28: Global Network Inventory displaying the Installed software information

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

Lab 2

Enumerating Network Resources using Advanced IP Scanner

ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

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

 **Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 03 Scanning Networks**

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

Module 04 – Enumeration

- 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

TASK 1
**Install Advanced
IP Scanner**

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

Module 04 – Enumeration

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

 You can also download Advanced IP Scanner from <http://www.advanced-ip-scanner.com>.

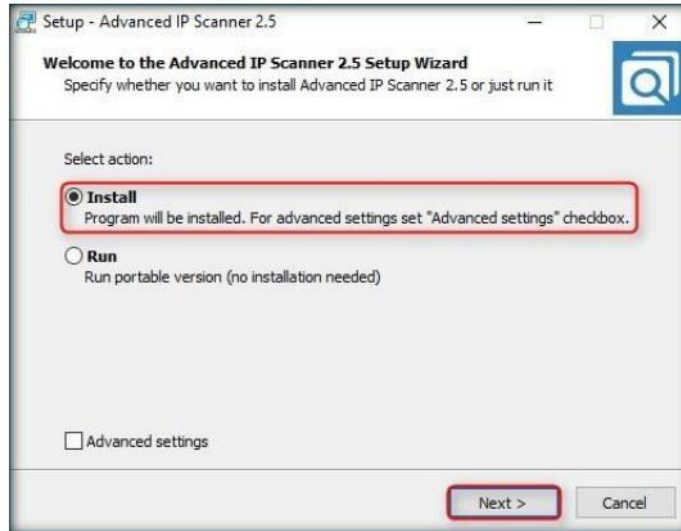


FIGURE 2.2: Advance IP Scanner setup

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



 With Advanced IP Scanner, you can scan hundreds of IP addresses simultaneously.



FIGURE 2.3: Advance IP Scanner setup

Module 04 – Enumeration

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

 You can wake any machine remotely with Advanced IP Scanner, if the Wake-on-LAN feature is supported by your network card.

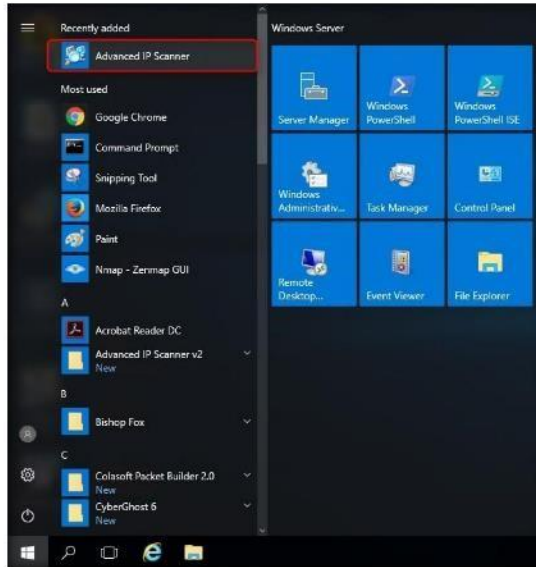



FIGURE 2.4: Launching the application from Apps list

 You have to guess a range of IP address of the victim machine.

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

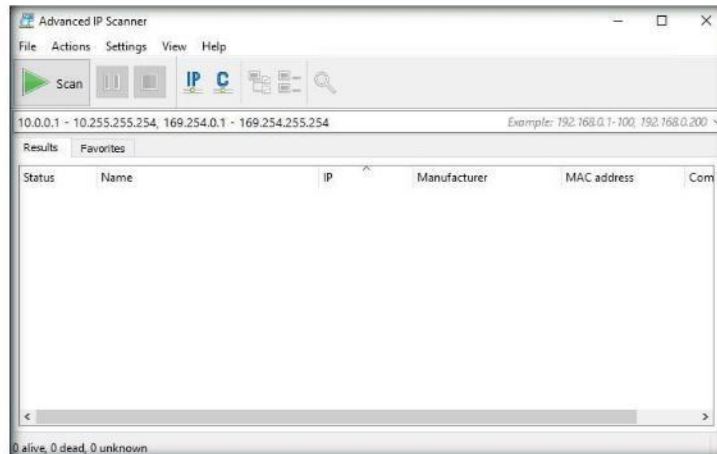



FIGURE 2.5: Advanced IP Scanner main window

 Radmin 2.x and 3.x Integration enable you to connect (if Radmin is installed) to remote computers with just one click.

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

Module 04 – Enumeration

TASK 2

Scan a Network to Discover Hosts

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

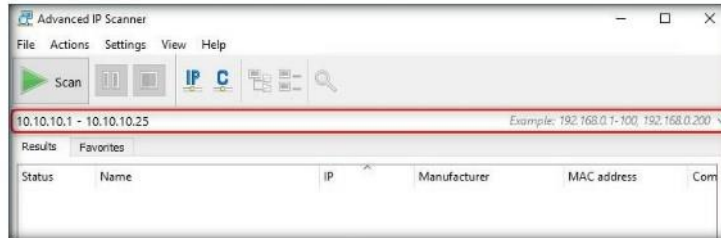


FIGURE 2.6: Scanning a Subnet

The status of scan is shown at the bottom left side of the window.

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

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

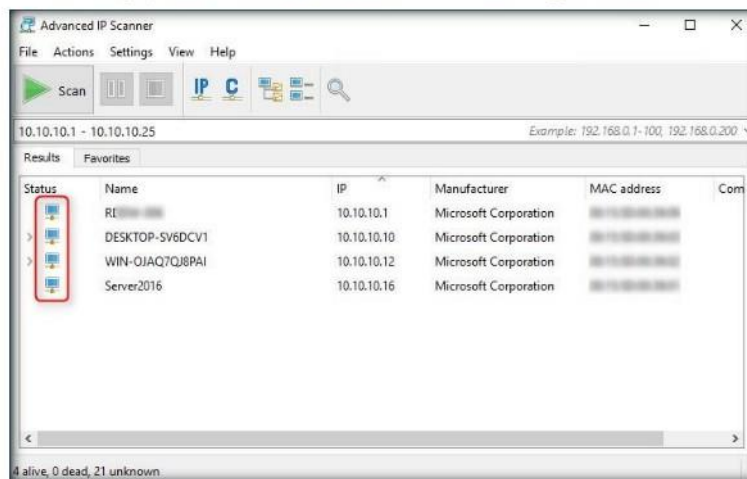


FIGURE 2.7: Advanced IP Scanner displaying Alive Host list


Lists of computers saving and loading enable you to perform operations with a specific list of computers. Just save a list of machines you need and Advanced IP Scanner loads it at startup automatically.

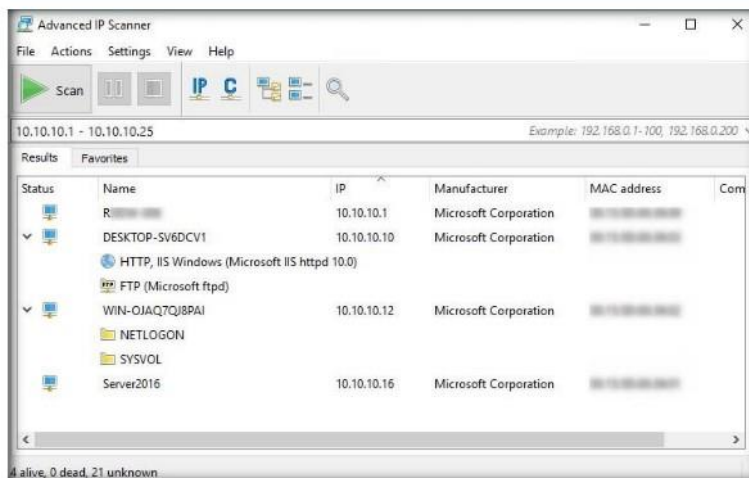
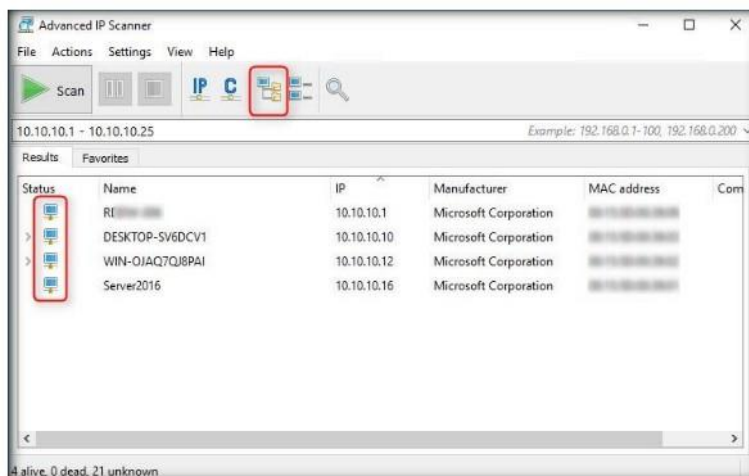
Note: The scan results might differ in your lab environment.

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

Module 04 – Enumeration

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

 **Group Operations:** Any feature of Advanced IP Scanner can be used with any number of selected computers. For example, you can remotely shut down a complete computer class with a few clicks.




 Advanced IP Scanner works on Windows Server 2003/Server 2008 and on Windows 7 (32 bit, 64 bit).

FIGURE 2.8: Advanced IP Scanner displaying shared folders and services

Module 04 – Enumeration

TASK 3

Examine the Options

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

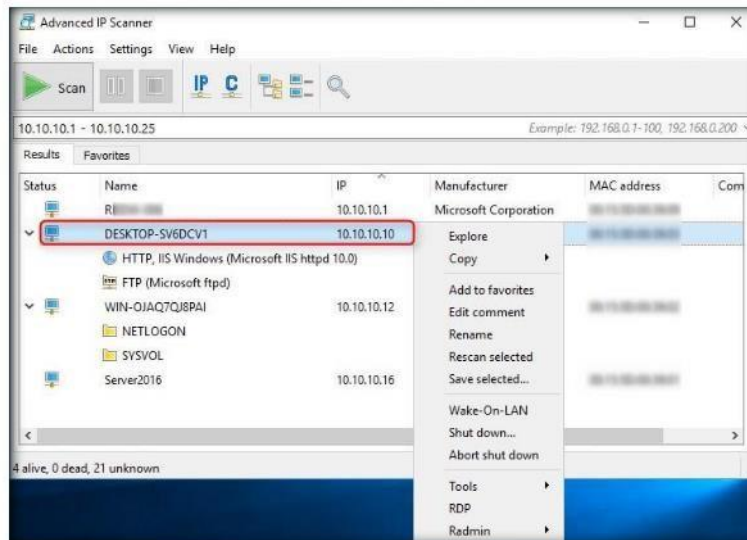



FIGURE 2.9: Exploring the victim machines

 Wake-on-LAN: You can wake any machine remotely with Advanced IP Scanner, if Wake-on-LAN feature is supported by your network card.

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.

Module 04 – Enumeration

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

This shuts down any remote machine or group of machines running a Windows operating system. You can use your default access rights or specify a login and password for shutdown. This feature is very handy for system administrators since it enables all computers in a customized list to be turned off in a single operation at the end of the working day.

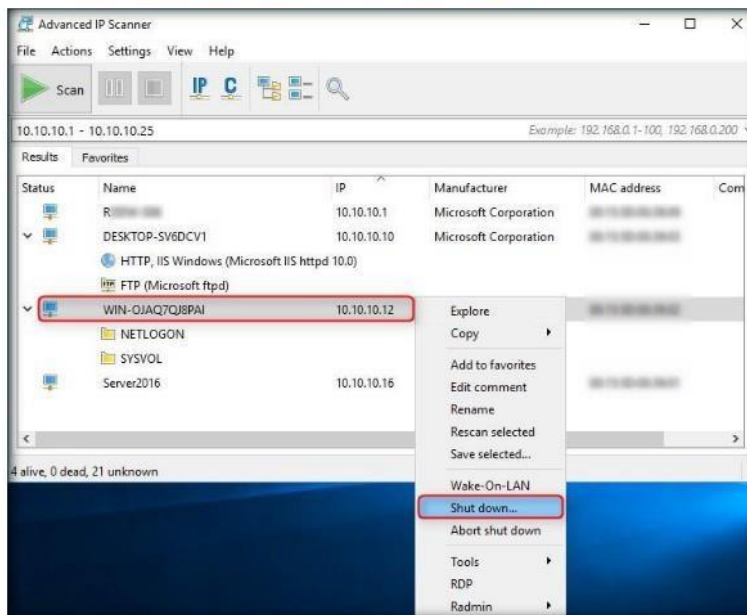


FIGURE 2.10: Shutting down a virtual machine

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.

Winfingerprint Input Options:

- IP Range (Netmask and Inverted Netmask supported) IP List(Single Host Neighborhood)



FIGURE 2.11: Shutting down a virtual machine remotely

Module 04 – Enumeration

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

There is the opportunity to run quick commands (ping, tracer, telnet and SSH) on a selected computer.

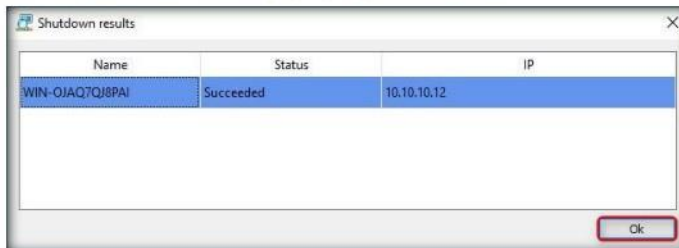


FIGURE 2.12: Shutting down a virtual machine remotely

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

The software scans ports of network computers and finds HTTP, HTTPS, FTP and shared folders.

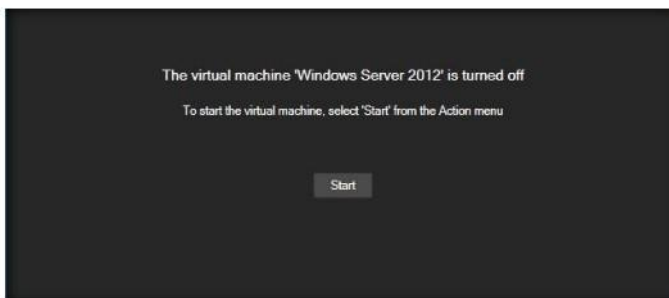


FIGURE 2.13: Victim machine successfully shutdown

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> 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.

ICON KEY

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

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

 **Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 04 Enumeration**


Module 04 – Enumeration

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

Lab Duration

Time: 5 Minutes

Overview of SuperScan

 SuperScan is not supported by Windows 95/98/ME.

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

TASK 1

Launch SuperScan

 SuperScan features:

- Superior scanning speed
- Support for unlimited IP ranges
- Improved host detection using multiple ICMP methods
- TCP SYN scanning
- UDP scanning (two methods)
- IP address import supporting ranges and CIDR formats

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.

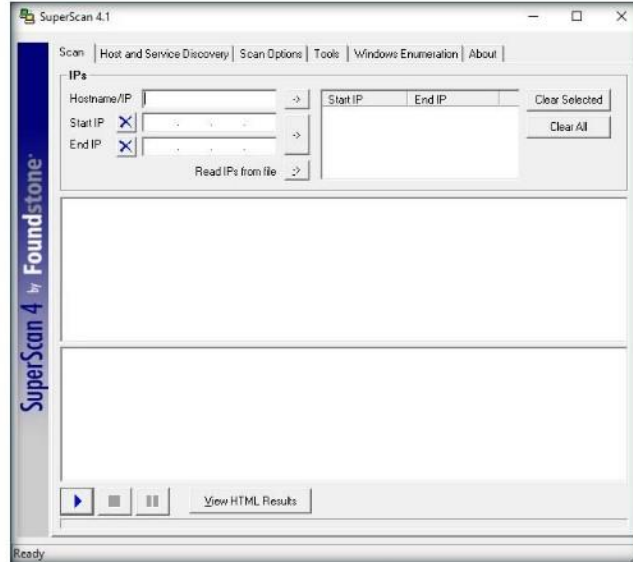


FIGURE 3.1: SuperScan main window

Module 04 – Enumeration

- Click on the **Windows Enumeration** tab.
 - 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.
- Check the types of **enumeration** you want to perform.
 - Now, click on **Enumerate**.

TASK 2

Perform Enumeration

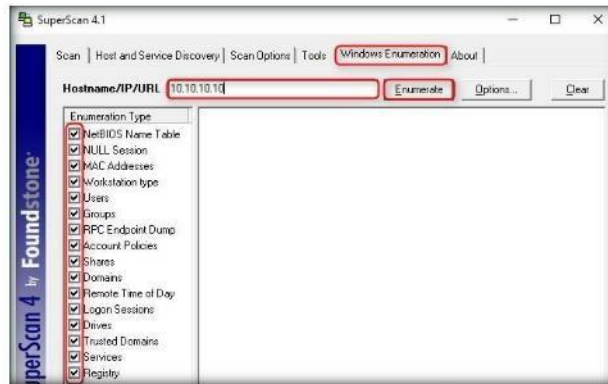



FIGURE 3.2: SuperScan main window with IP Address

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

 You can use SuperScan to perform port scans, retrieve general network information, such as name lookups and traceroutes, and enumerate Windows host information, such as users, groups, and services.

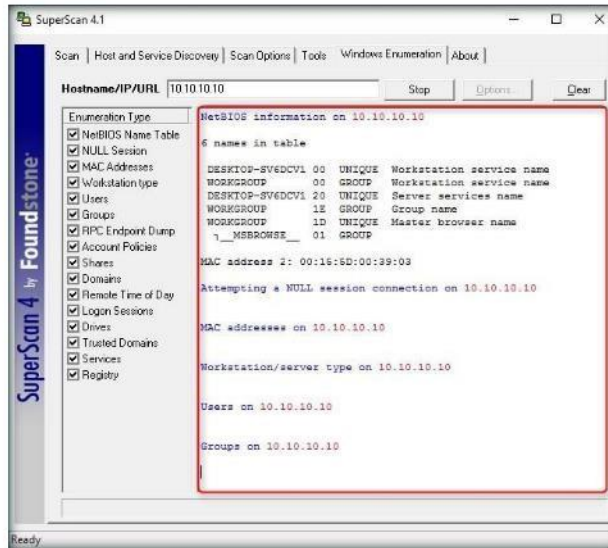


FIGURE 3.3: SuperScan main window with results

Module 04 – Enumeration

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.

Windows XP Service Pack 2 has removed raw sockets support, which now limits SuperScan and many other network scanning tools. Some functionality can be restored by running the net stop Shared Access at the Windows command prompt before starting SuperScan.

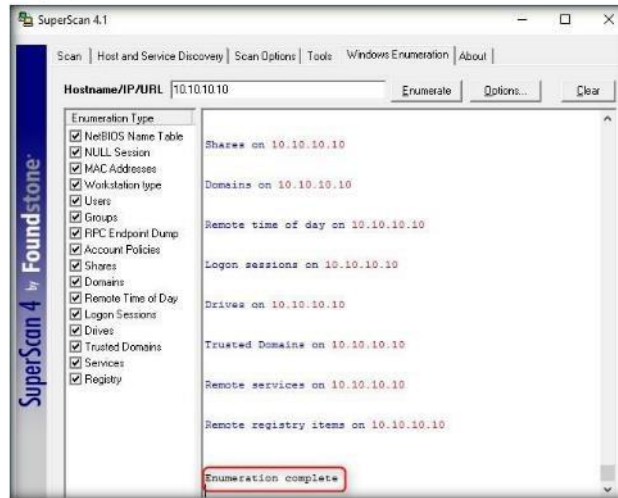


FIGURE 3.4: SuperScan Enumeration completed

TASK 3

Analyze the Results

You can also download SuperScan from <http://www.foundstone.com>.

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

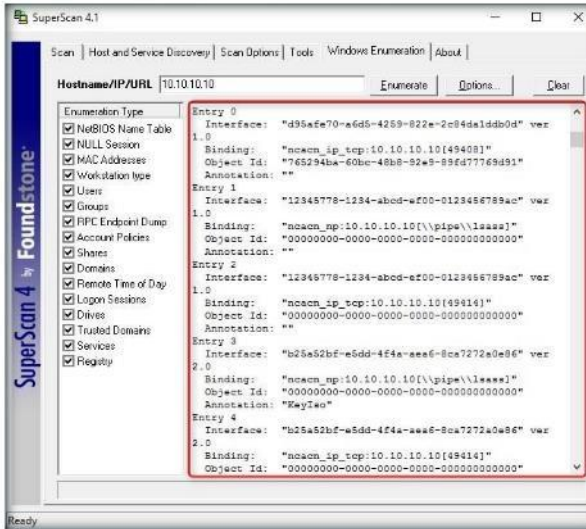



FIGURE 3.5: SuperScan Enumeration Results

Module 04 – Enumeration

- 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.

 SuperScan has four different ICMP host discovery methods available. This is useful, because while a firewall may block ICMP echo requests, it may not block other ICMP packets, such as timestamp requests. SuperScan gives you the potential to discover more hosts.

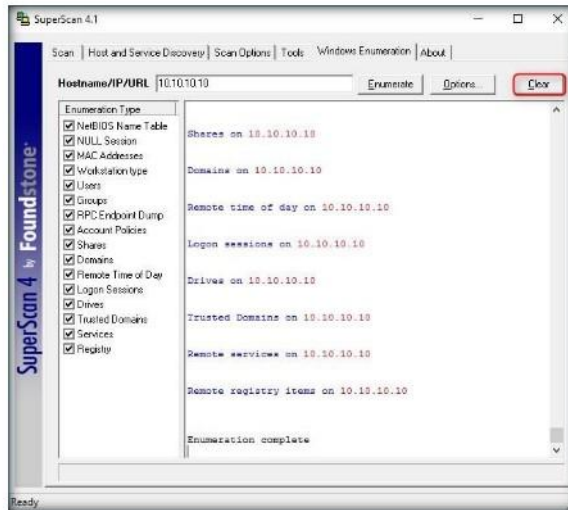


FIGURE 3.6: SuperScan main window with results

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> 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.

ICON KEY

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

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>

 **Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 04 Enumeration**

Module 04 – Enumeration

- 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

TASK 1

Install Hyena

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.

Hyena can be used on any Windows client to manage any Windows NT, Windows 2000, Windows XP/Vista, Windows 7, or Windows Server 2003/2008/2012 installation.

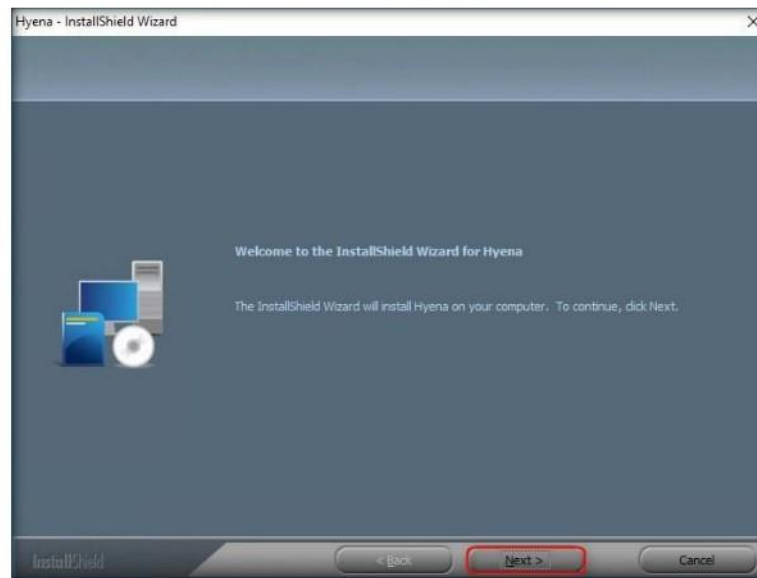


FIGURE 4.1: Installation of Hyena

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

Module 04 – Enumeration

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

In addition to supporting standard Windows system management functions, Hyena also includes extensive Active Directory integration.

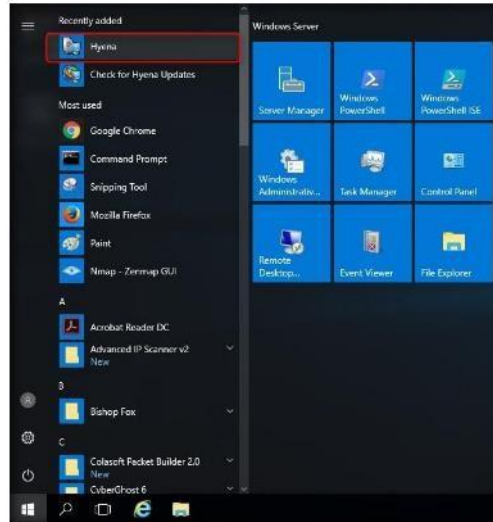


FIGURE 4.2: Windows Server 2012 Installed Apps

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

Additional command-line options were added to allow starting Hyena and automatically inserting and selecting/expanding a domain, server, or computer.

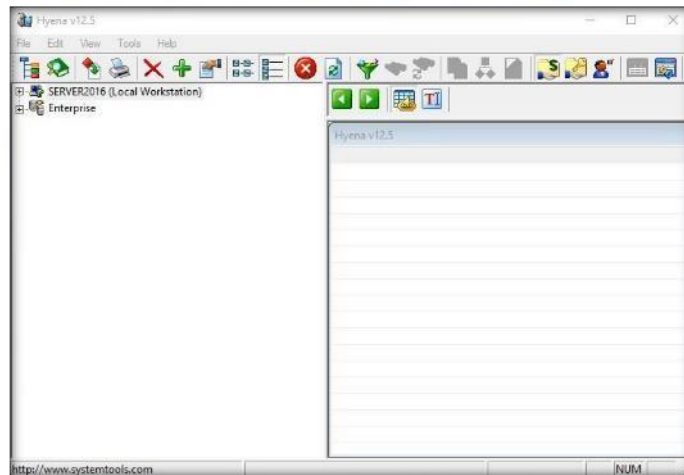


FIGURE 4.3: Main window of Hyena

Module 04 – Enumeration

TASK 2

Enumerate System Information

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

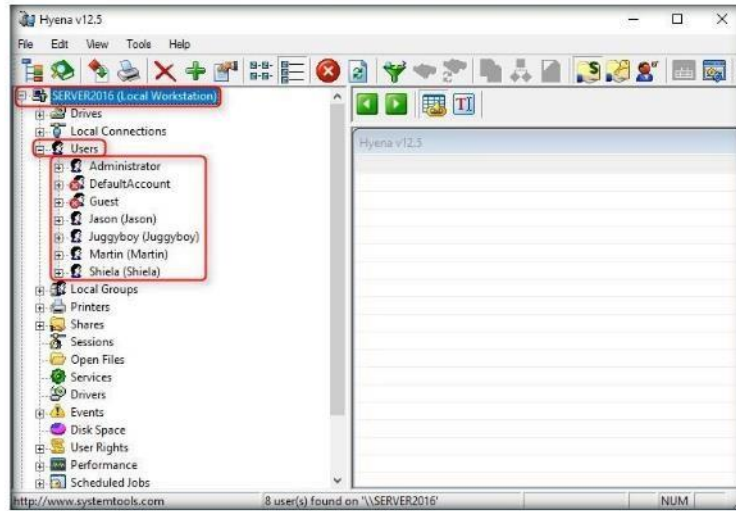


FIGURE 4.4: Expand the System users

TASK 3

Examine the Results

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

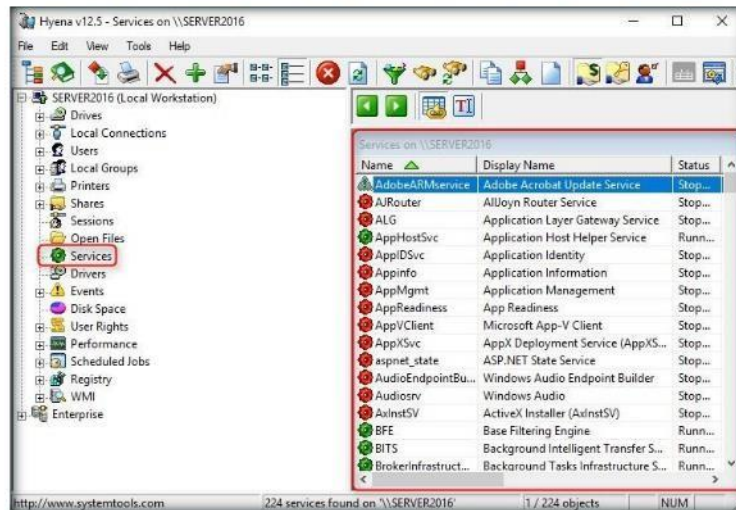


FIGURE 4.5: Services running in the system

Module 04 – Enumeration

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

Hyena also includes full exporting capabilities and both Microsoft Access and Excel reporting and exporting options

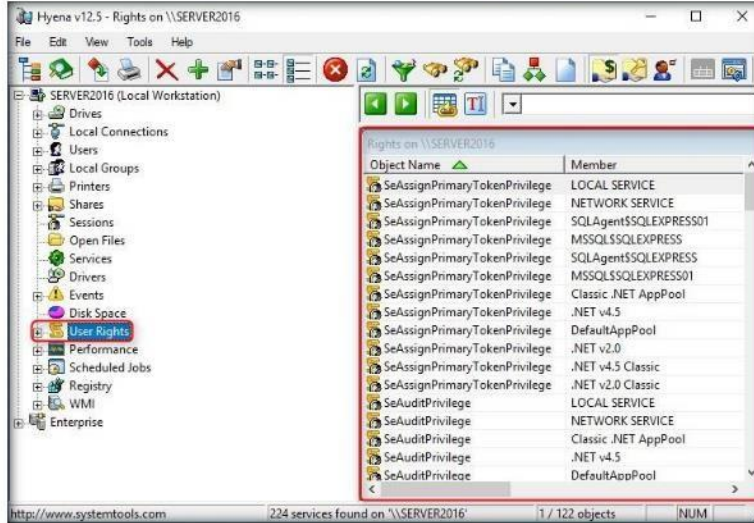


FIGURE 4.6: Users Rights

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

Hyena will execute the most current Group Policy editor, GPMEMSC, if it is present on the system.

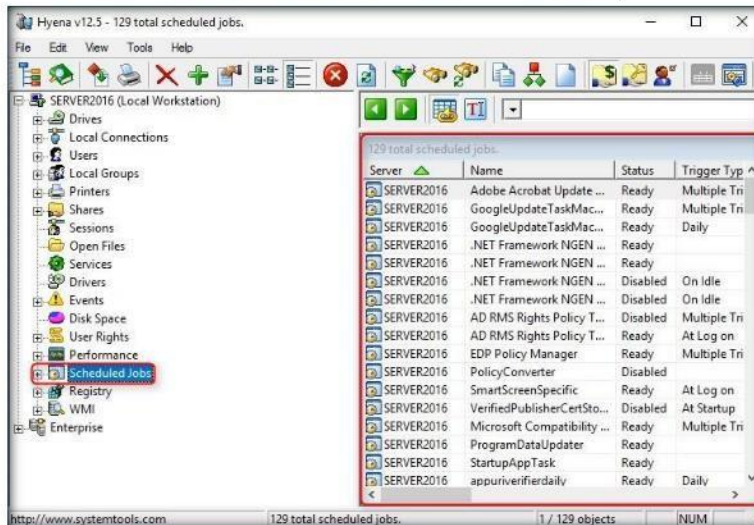


FIGURE 4.7: Scheduled Jobs

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.

Module 04 – Enumeration

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs





Performing Network Enumeration using NetBIOS Enumerator


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


ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

 **Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 04 Enumeration**

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

Module 04 – Enumeration

- 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

TASK 1

Launch NetBIOS Enumerator

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

NetBIOS is designed to help troubleshoot NetBIOS name resolution problems. When a network is functioning normally, NetBIOS over TCP/IP (NetBT) resolves NetBIOS names to IP addresses.

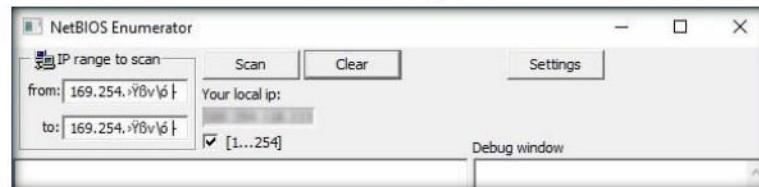


FIGURE 5.1: NetBIOS Enumerator main window

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.

Feature:

- Added port scan
- GUI - ports can be added, deleted, edited
- Dynamic memory management
- Threaded work (64 ports scanned at once)

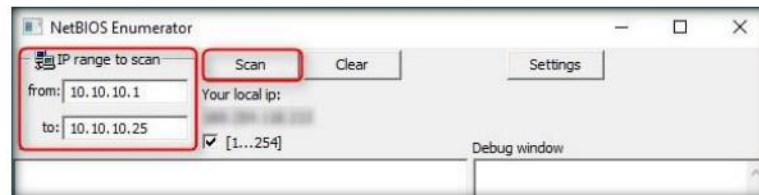


FIGURE 5.2: NetBIOS Enumerator with IP range to scan

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

Module 04 – Enumeration

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.

TASK 2
Examine the Results

The network function, NetServerGetInfo, is also implemented in this tool.

The protocol SNMP is implemented and running on all versions of Windows.

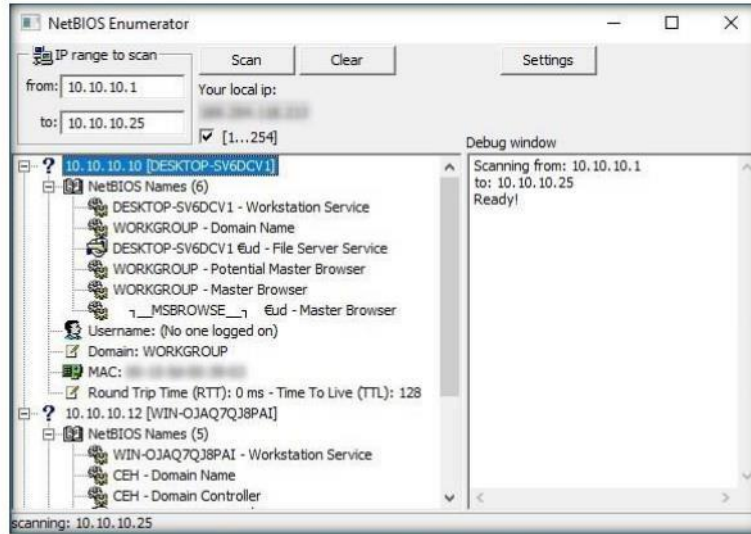


FIGURE 5.3: NetBIOS Enumerator results

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs





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.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

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

 **Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 04 Enumeration**

Module 04 – Enumeration

 You can also download SoftPerfect Network Scanner from <http://www.SoftPerfect.com>.

- 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

TASK 1

**Launch
SoftPerfect
Network Scanner**

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**.

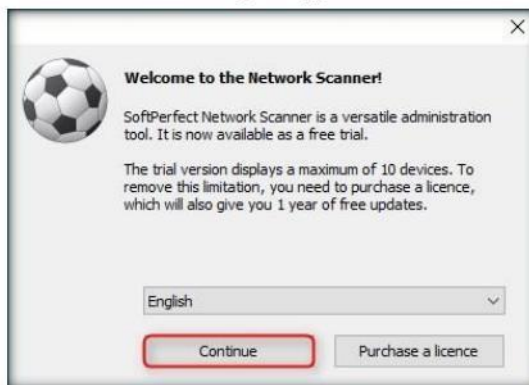


FIGURE 6.1: Network Scanner dialog-box

Module 04 – Enumeration

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

TASK 2

Perform Enumeration

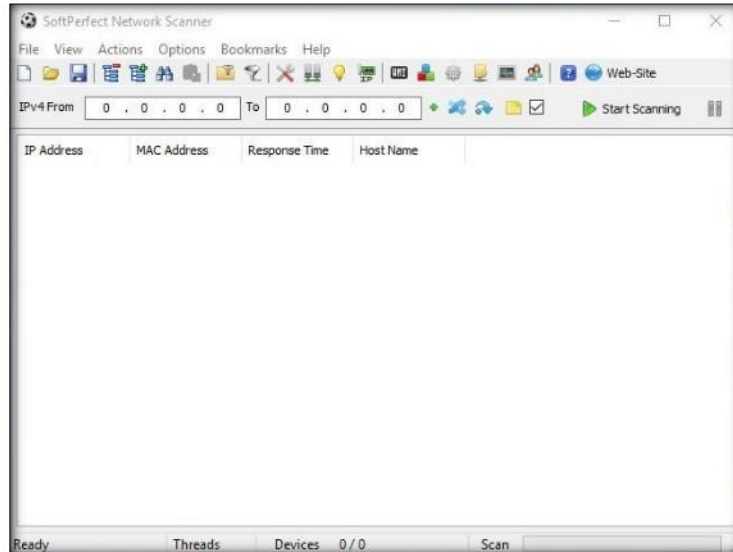


FIGURE 6.2: SoftPerfect Network Scanner main window

- 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.

Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 04 Enumeration

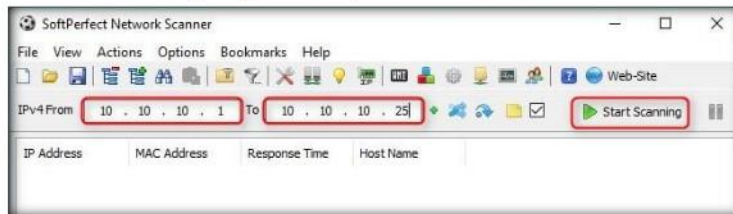


FIGURE 6.3: SoftPerfect setting an IP range to scan

Module 04 – Enumeration

TASK 3

Examine the Enumerated Results

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

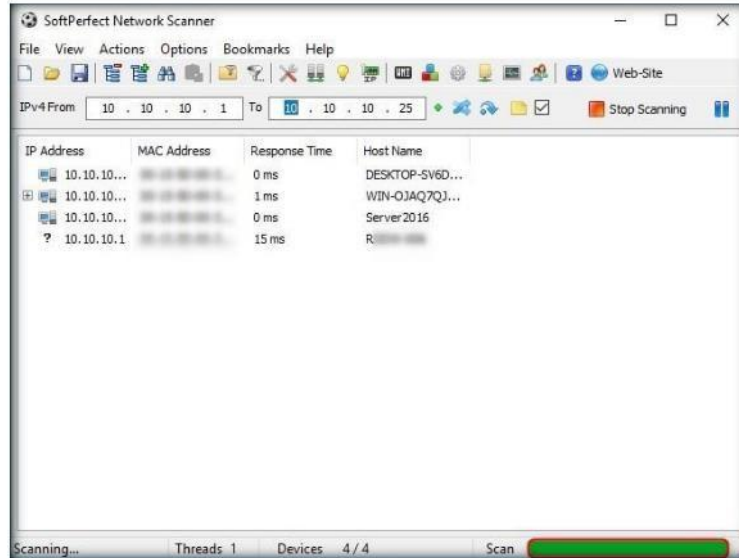


FIGURE 6.4: SoftPerfect status bar

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

SoftPerfect Network Scanner can also check for a user-defined port and report if one is open. It can also resolve host names and auto-detect your local and external IP range. It supports remote shutdown and Wake-On-LAN.

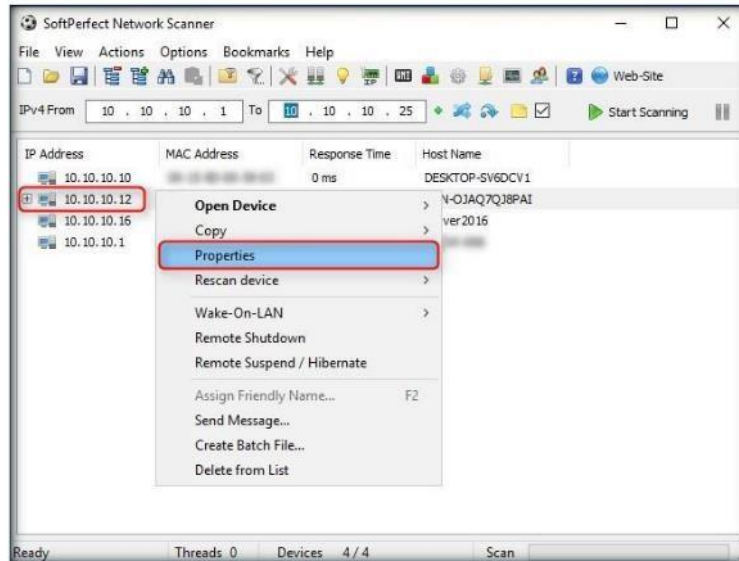


FIGURE 6.5: IP address scanned details

Module 04 – Enumeration

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

SoftPerfect allows you to mount shared folders as network drives, browse them using Windows Explorer, and filter the results list.

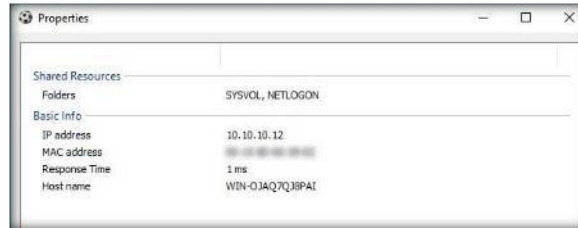


FIGURE 6.6: Properties window

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.

In addition, it can retrieve practically any information about network computers via WMI, SNMP, HTTP, NetBIOS, and a bunch of other features.

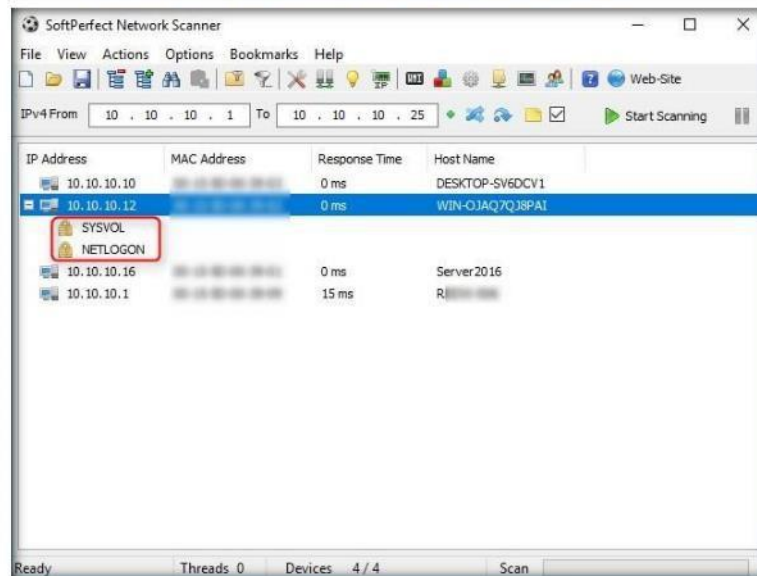


FIGURE 6.7: SoftPerfect Scanner displaying the shared folders

Module 04 – Enumeration

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.

It can also resolve host names and auto-detect the local and external IP address range. To assist with network administration, it supports remote shutdown and Wake-On-LAN.

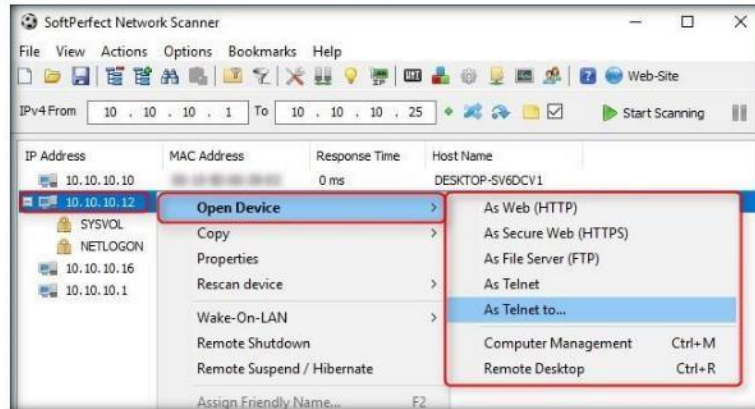


FIGURE 6.8: Various options in SoftPerfect Network Scanner

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs





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.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

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 discuss 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

 **Tools**
demonstrated in
this lab are
available in
Z:\CEH-
Tools\CEHv10
Module 04
Enumeration

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 **nbstat** 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**.

TASK 1

Install Nmap

Module 04 – Enumeration

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

📁 Zenmap file installs the following files:

- Nmap Core Files
- Nmap Path
- WinPcap 4.1.1
- Network Interface Import
- Zenmap (GUI frontend)
- Ncat (Modern Netcat)
- Ndiff



FIGURE 7.1: Nmap Setup window

- 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.

📸 Take a snapshot (a type of quick backup) of your virtual machine before each lab, because if something goes wrong, you can go back to it.

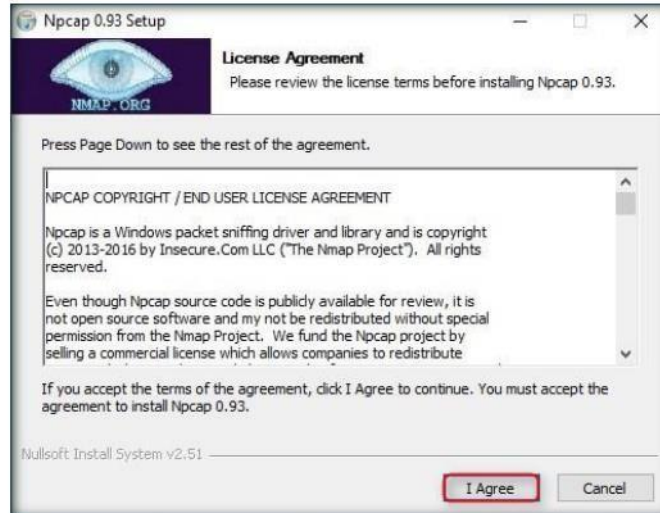



FIGURE 7.2: WinPcap setup pop-up

Module 04 – Enumeration

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

 Nmap Syntax: nmap [Scan Type(s)] [Options] {target specification}.

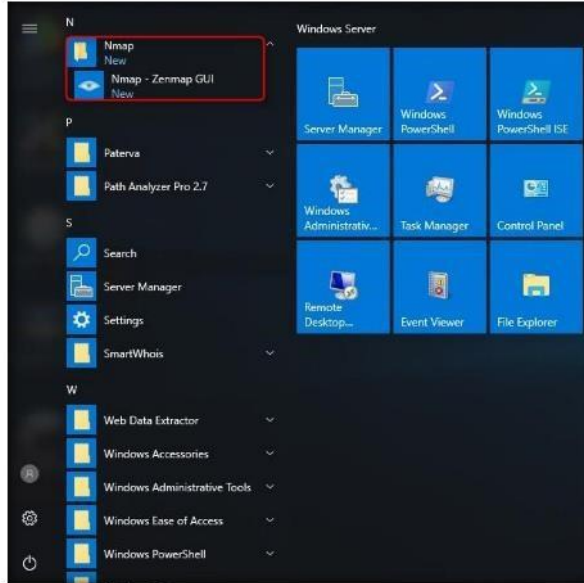



FIGURE 7.3: Windows Server 2012 Apps list

TASK 2
Perform Nmap Scan

 While Nmap attempts to produce accurate results, keep in mind that all of its insights are based on packets returned by the target machines or the firewalls in front of them.

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

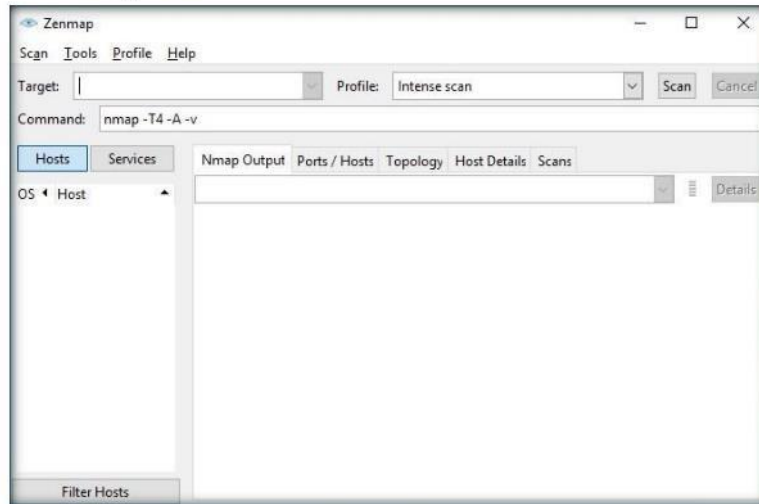


FIGURE 7.4: Nmap/Zenmap main window

Module 04 – Enumeration

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.

Use the `--osscan-guess` option for best results in Nmap.

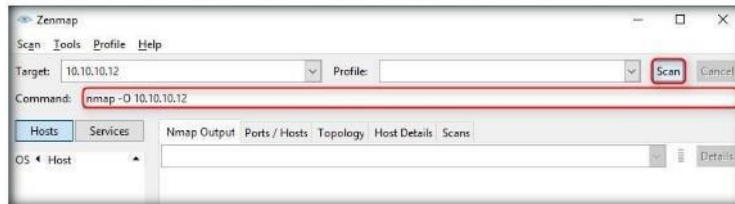


FIGURE 7.5: Configuring Nmap

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.

TASK 3

Find Open NetBIOS Ports

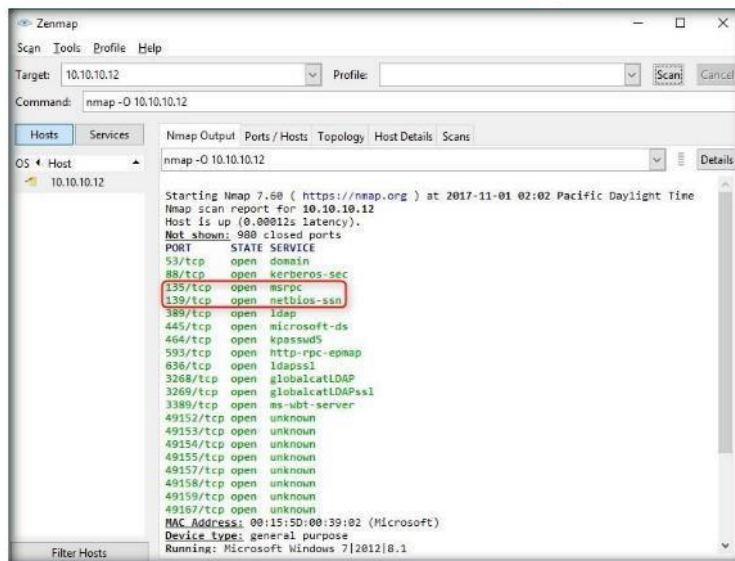



FIGURE 7.6: The Zenmap output window

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.

Nmap.org is the official source for downloading Nmap source code and binaries for Nmap and Zenmap.

Module 04 – Enumeration

 Nmap has traditionally been a command-line tool run from a UNIX shell or (more recently) a Windows command prompt.

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.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>nbtstat -A 10.10.10.16
Ethernet0:
Node IpAddress: [10.10.10.12] Scope Id: []

NetBIOS Remote Machine Name Table

Name                Type               Status
-----
WIN-ESUU38BTHJS<00> UNIQUE            Registered
WORKGROUP           <00>              GROUP             Registered
WIN-ESUU38BTHJS<20> UNIQUE            Registered

MAC Address = 00-0C-29-8F-D7-57

C:\Users\Administrator>_
```

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:

 Net Command
Syntax: NET [ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP | HELPMMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION | SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW]



```
Administrator: Command Prompt
C:\Users\Administrator>net use
New connections will be remembered.

Status      Local        Remote              Network
-----
Z:          \\vmware-host\Shared Folders  VMware Shared Folders

The command completed successfully.

C:\Users\Administrator>_
```

FIGURE 7.8: Command Prompt with the net use command

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

Module 04 – Enumeration

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs





Enumerating Services on a Target Machine

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

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

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.

TASK 1
Launch Kali Linux Virtual Machine

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

Module 04 – Enumeration

TASK 2

Launch Nmap

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

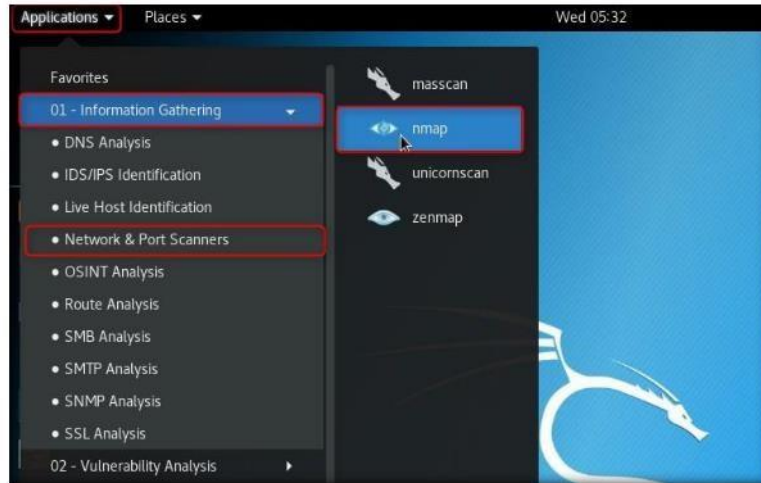


FIGURE 8.2: Launch Nmap in Kali Linux

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

The Nmap module is an interface with Nmap's internal functions and data structures. The API provides target host details such as port states and version detection results.

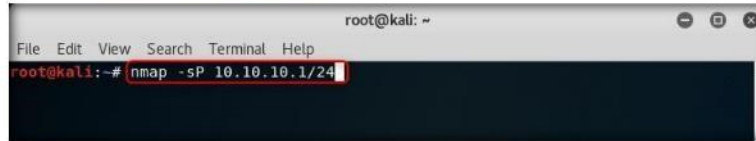
```
root@kali: ~  
File Edit View Search Terminal Help  
--reason: Display the reason a port is in a particular state  
--open: Only show open (or possibly open) ports  
--packet-trace: Show all packets sent and received  
--iflist: Print host interfaces and routes (for debugging)  
--append-output: Append to rather than clobber specified output files  
--resume <filename>: Resume an aborted scan  
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML  
--webxml: Reference stylesheet from Nmap.Org for more portable XML  
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output  
MISC:  
-6: Enable IPv6 scanning  
-A: Enable OS detection, version detection, script scanning, and traceroute  
--datadir <dirname>: Specify custom Nmap data file location  
--send-eth/--send-ip: Send using raw ethernet frames or IP packets  
--privileged: Assume that the user is fully privileged  
--unprivileged: Assume the user lacks raw socket privileges  
-V: Print version number  
-h: Print this help summary page.  
EXAMPLES:  
nmap -v -A scanme.nmap.org  
nmap -v -sn 192.168.0.0/16 10.0.0.0/8  
nmap -v -iR 10000 -Pn -p 80  
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES  
root@kali:~#
```

FIGURE 8.3: Nmap in Command Terminal

Module 04 – Enumeration

TASK 3 Perform Ping Sweep


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

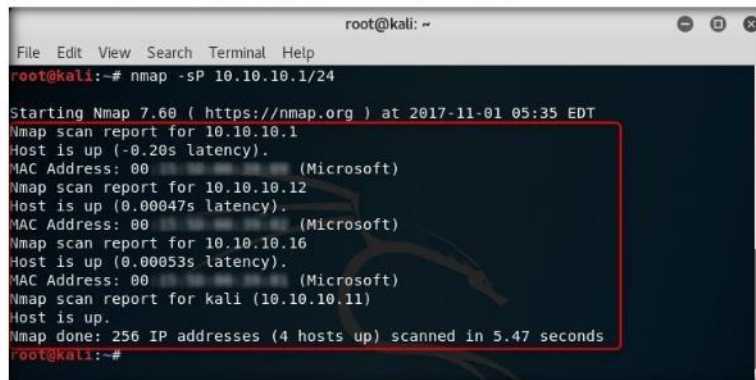


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sP 10.10.10.1/24
```

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:

 -sP this scan type lists the hosts within the specified range that responded to a ping. It allows you to detect which computers are online, rather than which ports are open. Four methods exist within Nmap for ping sweeping.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sP 10.10.10.1/24  
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-01 05:35 EDT  
Nmap scan report for 10.10.10.1  
Host is up (-0.20s latency).  
MAC Address: 00 (Microsoft)  
Nmap scan report for 10.10.10.12  
Host is up (0.00047s latency).  
MAC Address: 00 (Microsoft)  
Nmap scan report for 10.10.10.16  
Host is up (0.00053s latency).  
MAC Address: 00 (Microsoft)  
Nmap scan report for kali (10.10.10.11)  
Host is up.  
Nmap done: 256 IP addresses (4 hosts up) scanned in 5.47 seconds  
root@kali:~#
```

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**.

TASK 4
Perform Stealthy Syn Scan

- 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.

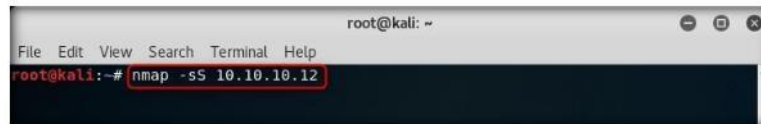


FIGURE 8.6: Nmap Stealthy Syn Scan

- By issuing this command, a stealthy syn scan will be initiated.
- 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.

A stealth scan (-sS) is often picked up by most firewalls and IDS systems now days. It was originally designed to prevent logging of a scan in the logs for whatever server is running on the port the scanner connects to.

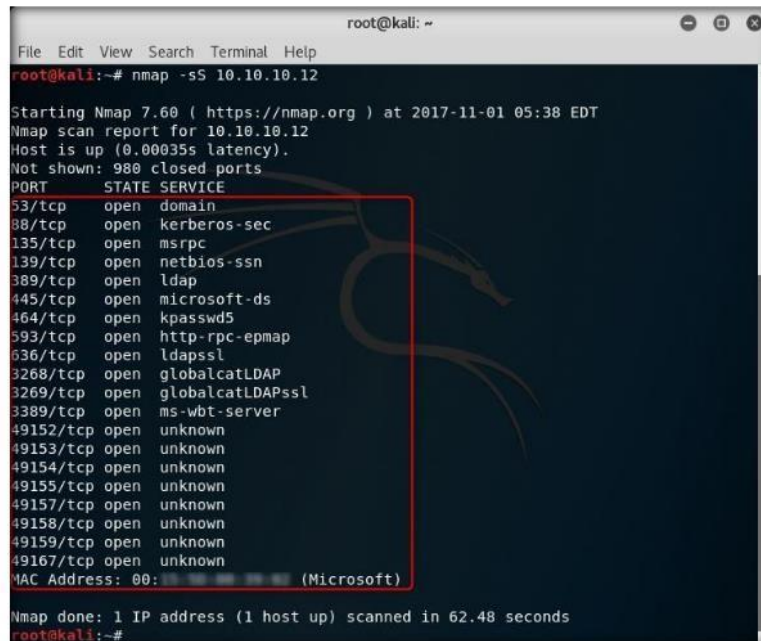


FIGURE 8.7: Nmap Stealthy Syn Scan Results

- 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.

Module 04 – Enumeration

TASK 5

Perform Stealthy Syn Scan with Version Detection and OS Detection

- 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.

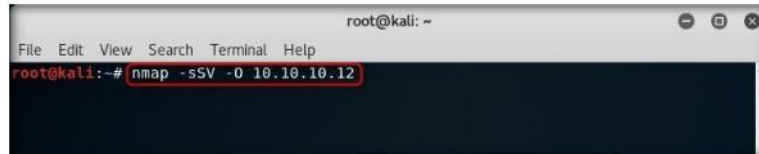


FIGURE 8.8: Nmap Stealthy Syn Scan Version Detection and OS Detection

- By issuing this command, a stealthy syn scan with version detection along with OS detection will be initiated.
- Nmap performs the scan and displays the versions of the services, along with an OS fingerprint, as shown in the screenshot:

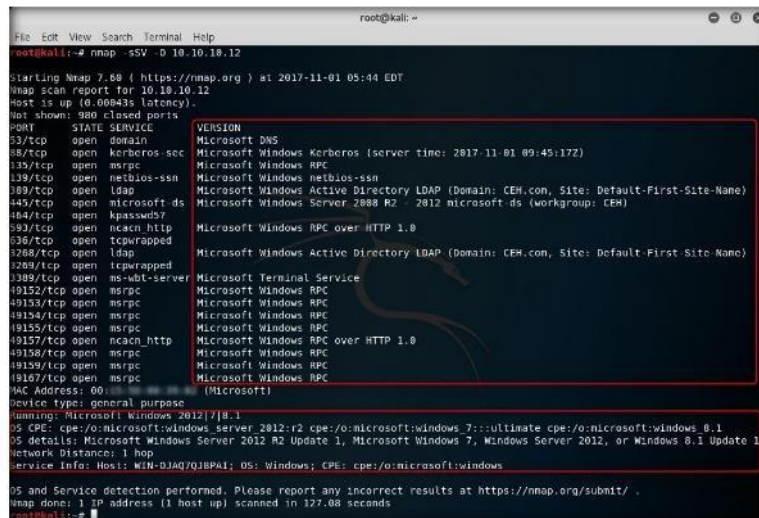


FIGURE 8.9: Nmap Stealthy Syn Scan Version Detection and OS Detection Result

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

Version Detection collects information about the specific service running on an open port, including the product name and version number. This information can be critical in determining an entry point for an attack.

Module 04 – Enumeration

TASK 6

Save the Scan Result

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**.

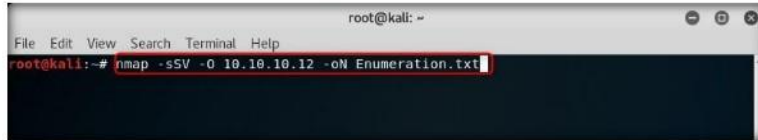


FIGURE 8.10: Nmap Saving Stealthy Syn Scan Result

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

The `-sSV` option enables version detection, and the `-A` option enables both OS fingerprinting and version detection, as well as any other advanced features.

Module 04 – Enumeration

TASK 7

View the Scan Result

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

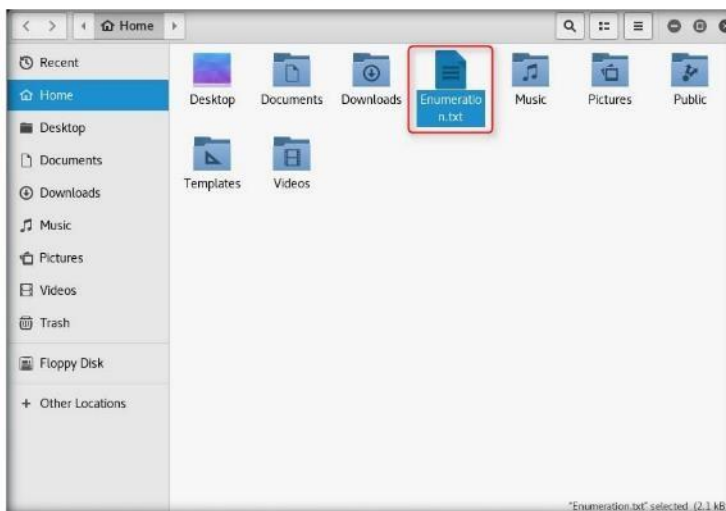


FIGURE 8.12: Stealthy Syn Scan Result File

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

Nmap adjusts its timings automatically depending on network speed and response times of the victim. However, you may want more control over the timing in order to create a more stealthy scan, or to get the scan over and done with quicker.

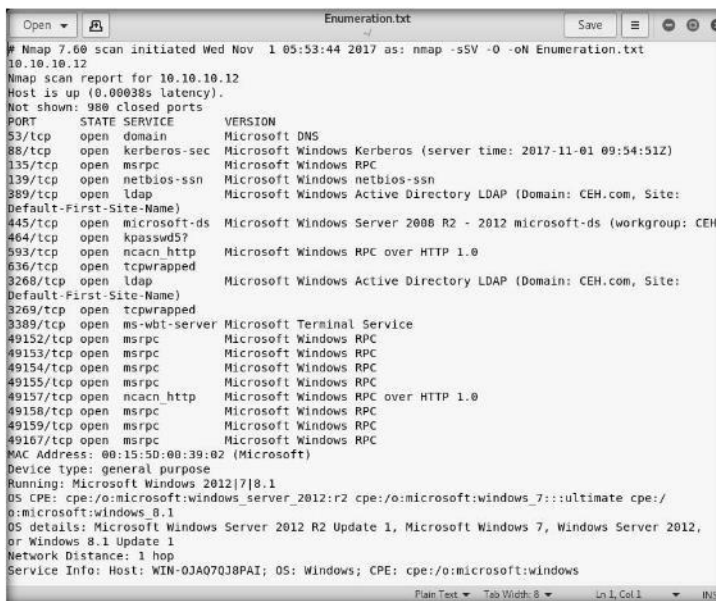
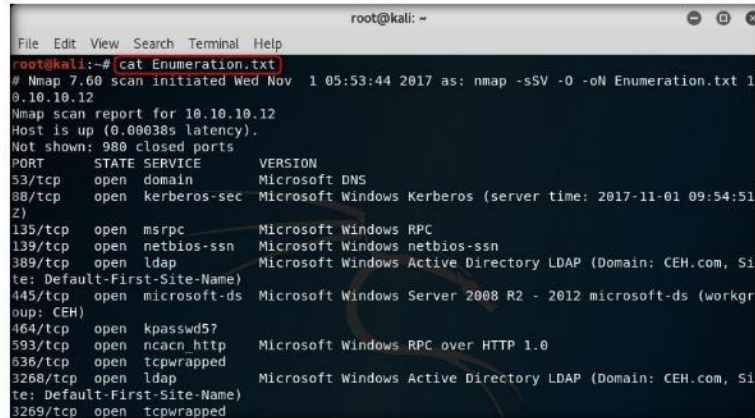


FIGURE 8.13: Stealthy Scan Result

Module 04 – Enumeration

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

SYN or Stealth scanning makes use of this procedure by sending a SYN packet and looking at the response. If SYN/ACK is sent back, the port is open and the remote end is trying to open a TCP connection.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# cat Enumeration.txt
# Nmap 7.60 scan initiated Wed Nov  1 05:53:44 2017 as: nmap -sSV -O -oN Enumeration.txt 10.10.10.12
Nmap scan report for 10.10.10.12
Host is up (0.00038s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Microsoft DNS
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2017-11-01 09:54:51Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (Domain: CEH.com, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CEH)
464/tcp   open  kpasswd57        Microsoft Windows RPC
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: CEH.com, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
```

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



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".

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

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

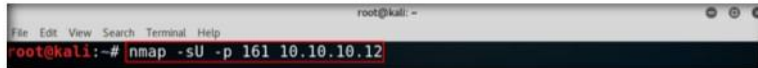
TASK 1

Test for SNMP Port Status

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.

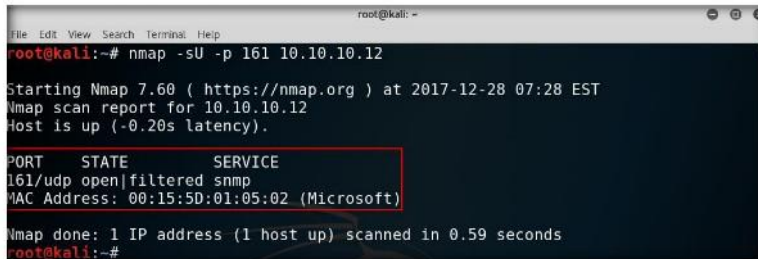
 -sU Scans UDP port.
-p <port ranges>: Only scan specified ports.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sU -p 161 10.10.10.12
```

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.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sU -p 161 10.10.10.12  
Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-28 07:28 EST  
Nmap scan report for 10.10.10.12  
Host is up (-0.20s latency).  
PORT      STATE      SERVICE  
161/udp  open|filtered  snmp  
MAC Address: 00:15:5D:01:05:02 (Microsoft)  
Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds  
root@kali:~#
```

FIGURE 9.2: Nmap UDP scan result

TASK 2
Find SNMP Community String

```
nmap -sU --script snmp-brute <target> [--script-args snmp-brute.communitiesb=<wordlist>]
```

If not defined, the default wordlist used to brute-force the SNMP community strings is nseclib/data/snmpcommunities.lst.

In case this wordlist does not exist, the script falls back to nseclib/data/passwords.lst.

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.

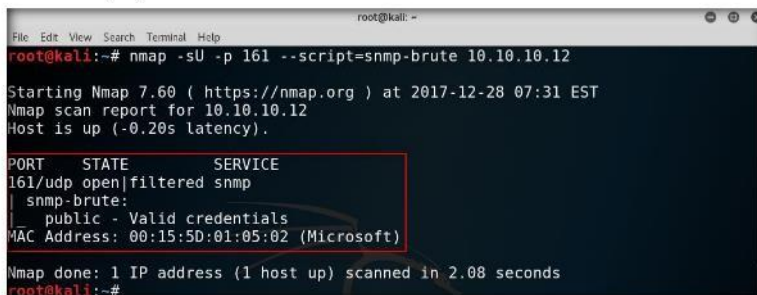


FIGURE 9.4: SNMP Community String found with Valid Credentials

TASK 3
Enumerate Community String

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

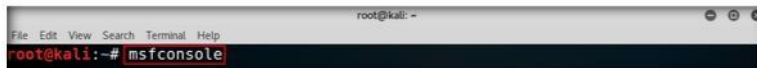


FIGURE 9.5: Launching Metasploit Framework

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

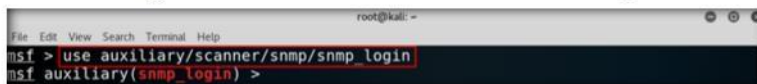
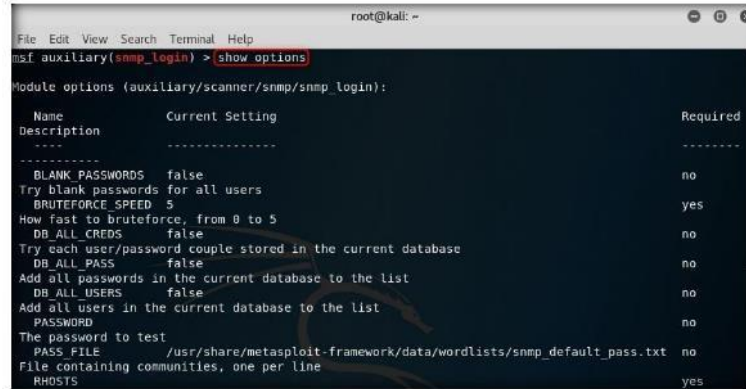


FIGURE 9.6: Launching snmp_login module

Module 04 – Enumeration

- 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.



```
root@kali: ~  
msf auxiliary(snmp_login) > show options  
Module options (auxiliary/scanner/snmp/snmp_login):  


| Name             | Current Setting                                                      | Required |
|------------------|----------------------------------------------------------------------|----------|
| BLANK_PASSWORDS  | false                                                                | no       |
| Description      | Try blank passwords for all users                                    |          |
| BRUTEFORCE_SPEED | 5                                                                    | yes      |
| Description      | How fast to bruteforce, from 0 to 5                                  |          |
| DB_ALL_CREDS     | false                                                                | no       |
| Description      | Try each user/password couple stored in the current database         |          |
| DB_ALL_PASS      | false                                                                | no       |
| Description      | Add all passwords in the current database to the list                |          |
| DB_ALL_USERS     | false                                                                | no       |
| Description      | Add all users in the current database to the list                    |          |
| PASSWORD         |                                                                      | no       |
| Description      | The password to test                                                 |          |
| PASS_FILE        | /usr/share/metasploit-framework/data/wordlists/snmp_default_pass.txt | no       |
| Description      | File containing communities, one per line                            |          |
| RHOSTS           |                                                                      | yes      |


```

FIGURE 9.7: Viewing Module Options

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

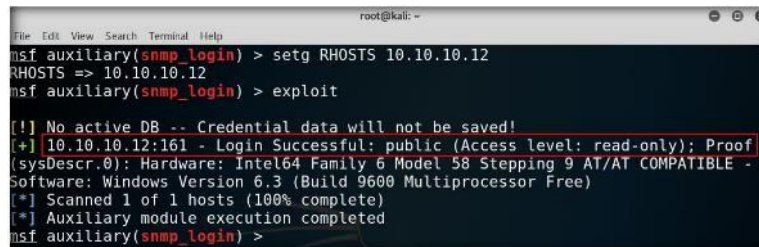
Note: In this lab, **10.10.10.12** is the IP Address of the **Windows Server 2012** and this might vary in your lab environment.



```
root@kali: ~  
msf auxiliary(snmp_login) > setg RHOSTS 10.10.10.12  
RHOSTS => 10.10.10.12  
msf auxiliary(snmp_login) >
```

FIGURE 9.8: Setting Options

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

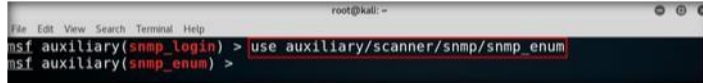


```
root@kali: ~  
msf auxiliary(snmp_login) > setg RHOSTS 10.10.10.12  
RHOSTS => 10.10.10.12  
msf auxiliary(snmp_login) > exploit  
[!] No active DB -- Credential data will not be saved!  
[+] 10.10.10.12:161 - Login Successful: public (Access level: read-only); Proof  
(sysDescr.0): Hardware: Intel64 Family 6 Model 58 Stepping 9 AT/AT COMPATIBLE -  
Software: Windows Version 6.3 (Build 9600 Multiprocessor Free)  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf auxiliary(snmp_login) >
```

FIGURE 9.9: Exploiting Vulnerability

Module 04 – Enumeration

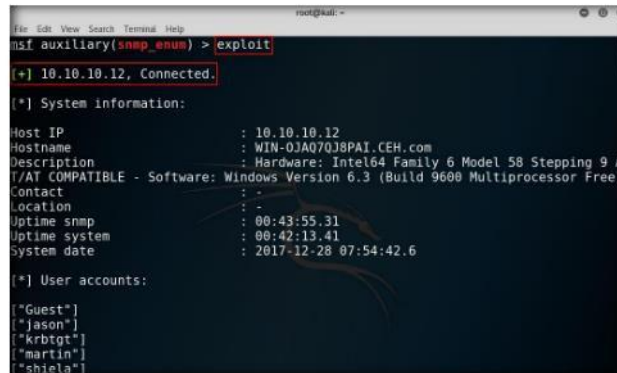
16. Now, type **use auxiliary/scanner/snmp/snmp_enum** and press **Enter**.



```
root@kali: ~  
msf auxiliary(snmp_login) > use auxiliary/scanner/snmp/snmp_enum  
msf auxiliary(snmp_enum) >
```

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.



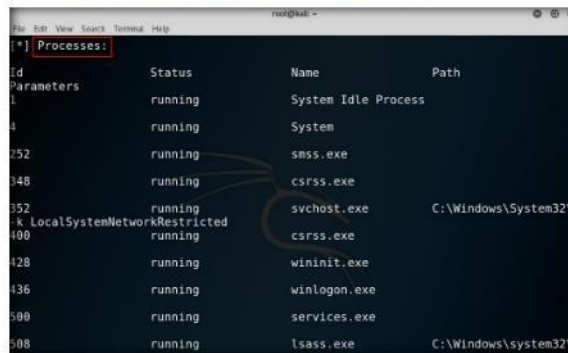
```
msf auxiliary(snmp_enum) > exploit  
[*] 10.10.10.12, Connected.  
[*] System information:  
Host IP           : 10.10.10.12  
Hostname          : WIN-0JA070J8PAI.CEH.com  
Description       : Hardware: Intel64 Family 6 Model 58 Stepping 9 A  
T/AT COMPATIBLE - Software: Windows Version 6.3 (Build 9600 Multiprocessor Free)  
Contact           : -  
Location          : -  
Uptime snmp       : 00:43:55.31  
Uptime system     : 00:42:13.41  
system date       : 2017-12-28 07:54:42.6  
[*] User accounts:  
["Guest"]  
["jason"]  
["krbtgt"]  
["martin"]  
["shielda"]
```

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

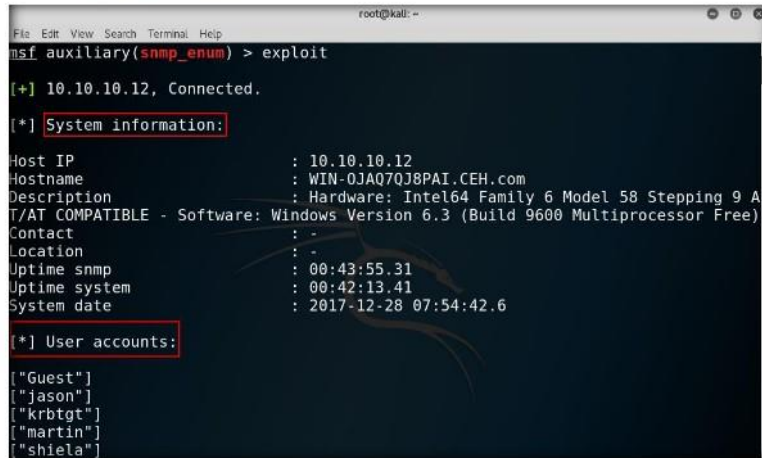


```
msf auxiliary(snmp_enum) > exploit  
[*] Processes:  
ID      Status      Name      Path  
-----  
0       running     System Idle Process  
4       running     System  
252     running     smss.exe  
348     running     csrss.exe  
352     running     svchost.exe      C:\Windows\System32\svchost.exe  
400     running     csrss.exe  
428     running     wininit.exe  
436     running     winlogon.exe  
500     running     services.exe  
508     running     lsass.exe        C:\Windows\system32\lsass.exe
```

FIGURE 9.12: System Information Obtained

Module 04 – Enumeration

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.



```
root@kali: ~
File Edit View Search Terminal Help
msf auxiliary(sntp_enum) > exploit

[+] 10.10.10.12, Connected.

[*] System information:

Host IP           : 10.10.10.12
Hostname          : WIN-0JA070J8PAI.CEH.com
Description       : Hardware: Intel64 Family 6 Model 58 Stepping 9 A
T/AT COMPATIBLE - Software: Windows Version 6.3 (Build 9600 Multiprocessor Free)
Contact           : -
Location          : -
Uptime snmp       : 00:43:55.31
Uptime system     : 00:42:13.41
System date       : 2017-12-28 07:54:42.6

[*] User accounts:

["Guest"]
["jason"]
["krbtgt"]
["martin"]
["shielal"]
```

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> 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.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

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

 **Tools**
demonstrated in
this lab are
available in
Z:\CEH-
Tools\CEHv10
Module 04
Enumeration

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**.

 **TASK 1**

**Launch
ADExplorer**

 Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor.

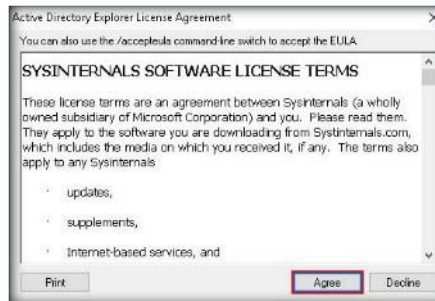


FIGURE 10.1: Open File – Security Warning

TASK 2
Connect to Active Directory Machine

Connect to your Active Directory database by entering the server details.

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.

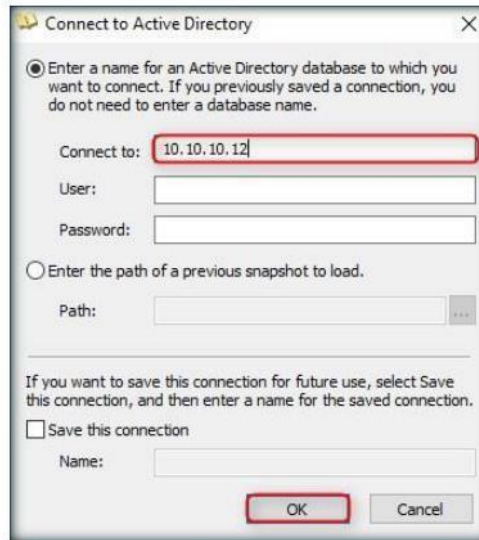


FIGURE 10.2: ADExplorer Connect to Active Directory

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

Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 04 Enumeration

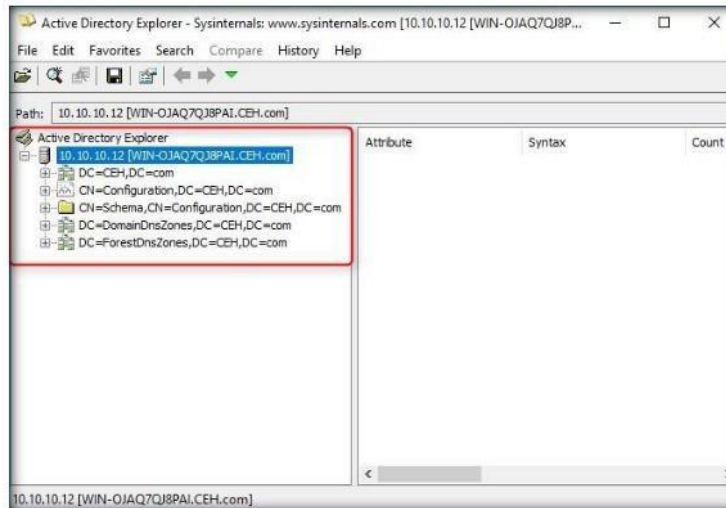


FIGURE 10.3: ADExplorer Main Window

Module 04 – Enumeration

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

AD Explorer also includes the ability to save snapshots of an AD database for off-line viewing and comparisons.

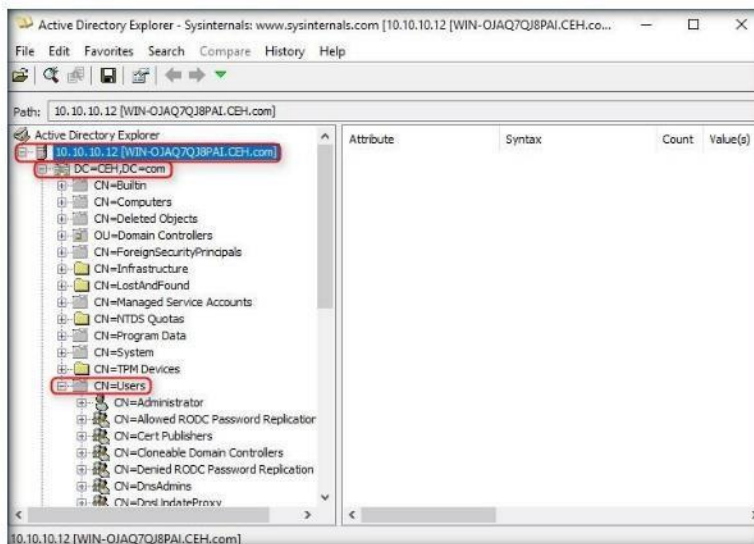


FIGURE 10.4: ADEplorer Domain Users Node

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

AD Explorer to easily navigate an AD database, define favorite locations, view object properties and attributes without having to open dialog boxes.

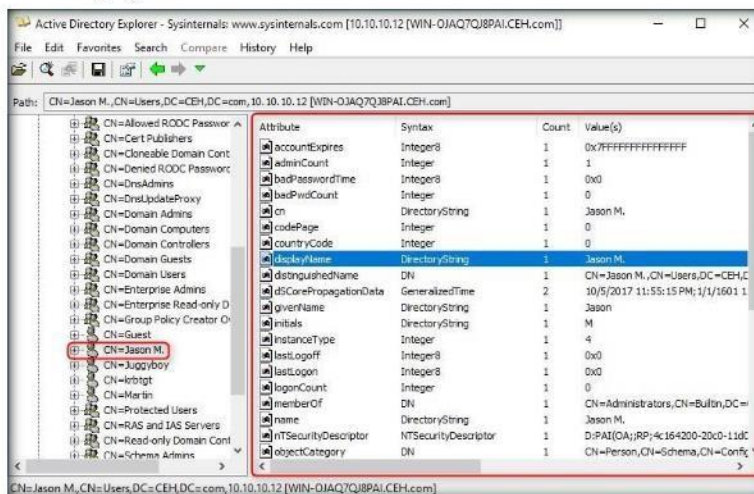


FIGURE 10.5: ADEplorer Domain Users Profile Attributes

TASK 3

Modifying User Attributes

AD Explorer enables the XenClient Enterprise Synchronizer Administrator to avoid most AD configuration problems, which are caused by typos or improper order of elements in a Distinguished Name (DN).

LDAP generally runs on port 389 and like other protocols tends to usually conform to a distinct set of rules (RFC's).

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

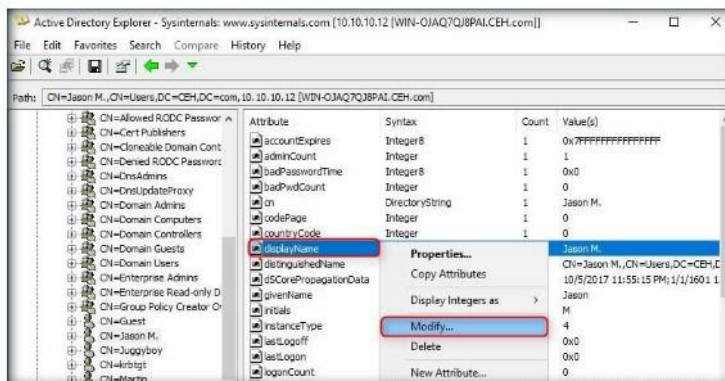


FIGURE 10.6: ADEplorer User Profile Modification

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

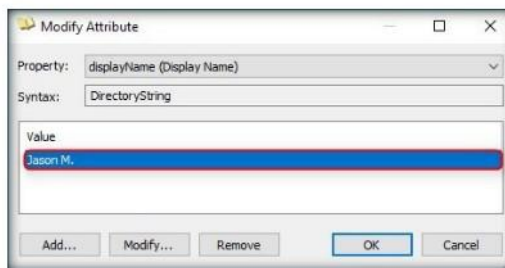


FIGURE 10.7: Modifying Attributes

- 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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs





Enumerating Information from Windows and Samba Host using Enum4linux

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

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

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

Module 04 – Enumeration

- Administrative privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Lab

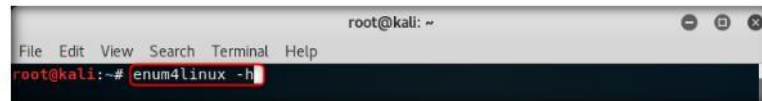
Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system. These techniques are conducted in an intranet environment.

Lab Tasks

TASK 1 Test for User Info

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

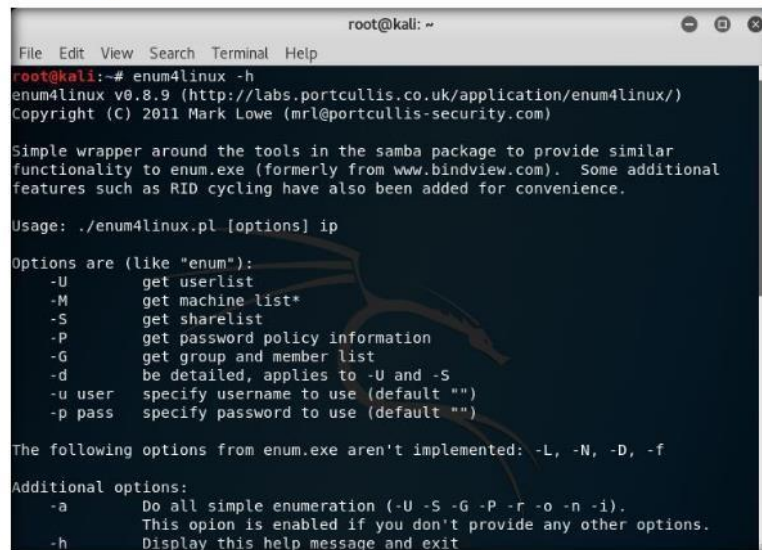
1. Now start the **Kali Linux** machine and open a **Terminal** window. In the terminal window type **enum4linux -h** and hit **Enter** to get the help options of enum4linux.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# enum4linux -h
```

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.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# enum4linux -h  
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)  
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)  
  
Simple wrapper around the tools in the samba package to provide similar  
functionality to enum.exe (formerly from www.bindview.com). Some additional  
features such as RID cycling have also been added for convenience.  
  
Usage: ./enum4linux.pl [options] ip  
  
Options are (like "enum"):  
-U get userlist  
-M get machine list*  
-S get sharelist  
-P get password policy information  
-G get group and member list  
-d be detailed, applies to -U and -S  
-u user specify username to use (default "")  
-p pass specify password to use (default "")  
  
The following options from enum.exe aren't implemented: -L, -N, -D, -f  
  
Additional options:  
-a Do all simple enumeration (-U -S -G -P -r -o -n -i).  
This option is enabled if you don't provide any other options.  
-h Display this help message and exit
```

FIGURE 11.2: Enum4linux help options

Module 04 – Enumeration

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.

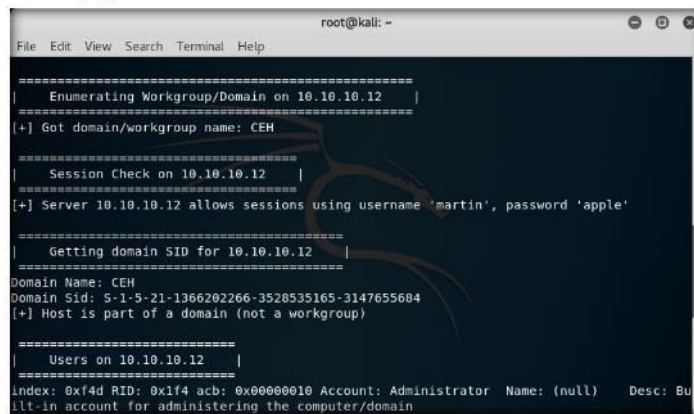
Note: Here 10.10.10.12 is the IP address of the Windows Server 2012; this might be different for your lab environment.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# enum4linux -u martin -p apple -U 10.10.10.12
```

FIGURE 11.3: Enum4linux command with User list option enabled

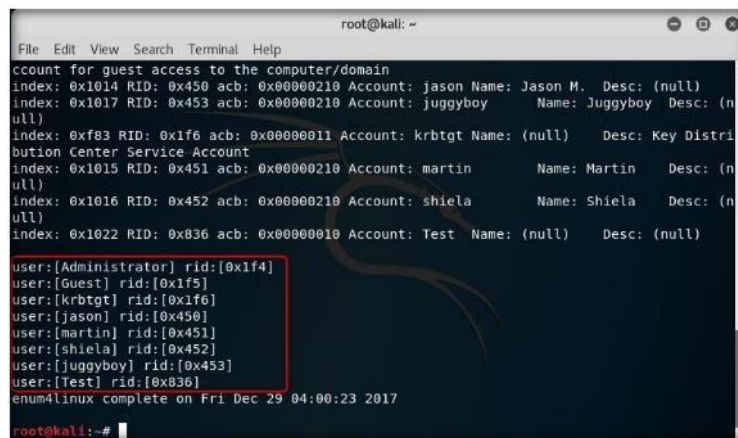
4. Enum4linux starts enumerating the workgroups/domains first and displays the results as shown in the screenshot.



```
root@kali: ~  
File Edit View Search Terminal Help  
=====  
| Enumerating Workgroup/Domain on 10.10.10.12 |  
=====  
[+] Got domain/workgroup name: CEH  
=====  
| Session Check on 10.10.10.12 |  
=====  
[+] Server 10.10.10.12 allows sessions using username 'martin', password 'apple'  
=====  
| Getting domain SID for 10.10.10.12 |  
=====  
Domain Name: CEH  
Domain Sid: 5-1-5-21-1366202266-3528535165-3147655684  
[+] Host is part of a domain (not a workgroup)  
=====  
| Users on 10.10.10.12 |  
=====  
Index: 0x1f4 RID: 0x1f4 acb: 0x0000010 Account: Administrator Name: (null) Desc: Bu  
ilt-in account for administering the computer/domain
```

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.



```
root@kali: ~  
File Edit View Search Terminal Help  
ccount for guest access to the computer/domain  
Index: 0x1014 RID: 0x450 acb: 0x00000210 Account: jason Name: Jason M. Desc: (null)  
Index: 0x1017 RID: 0x453 acb: 0x00000210 Account: juggyboy Name: Juggyboy Desc: (n  
ull)  
Index: 0xf83 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null) Desc: Key Distri  
bution Center Service Account  
Index: 0x1015 RID: 0x451 acb: 0x00000210 Account: martin Name: Martin Desc: (n  
ull)  
Index: 0x1016 RID: 0x452 acb: 0x00000210 Account: shiela Name: Shiela Desc: (n  
ull)  
Index: 0x1022 RID: 0x836 acb: 0x00000010 Account: Test Name: (null) Desc: (null)  
  
user:[Administrator] rid:[0x1f4]  
user:[Guest] rid:[0x1f5]  
user:[krbtgt] rid:[0x1f6]  
user:[jason] rid:[0x450]  
user:[martin] rid:[0x451]  
user:[shiela] rid:[0x452]  
user:[juggyboy] rid:[0x453]  
user:[Test] rid:[0x836]  
enum4linux complete on Fri Dec 29 04:00:23 2017  
root@kali:~#
```

FIGURE 11.5: User info with their respective RIDs

Module 04 – Enumeration

TASK 2

Test for OS Info

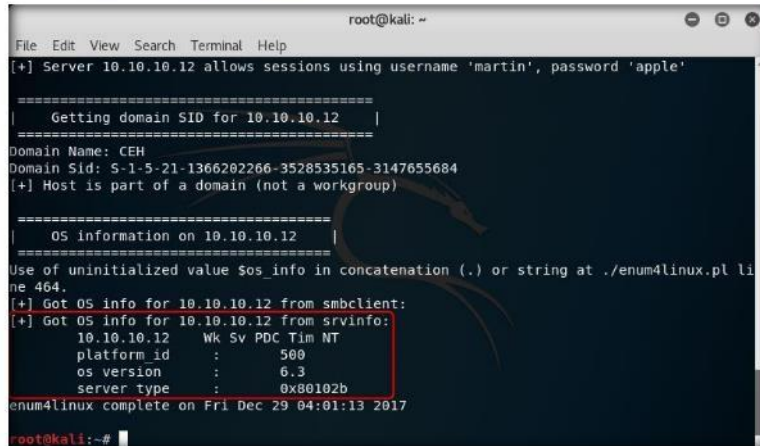
- Now to get the OS information of the target, type **enum4linux -u martin -p apple -o 10.10.10.12** and hit **Enter**.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# enum4linux -u martin -p apple -o 10.10.10.12
```

FIGURE 11.6: Enum4linux command for enumerating OS information

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



```
root@kali: ~  
File Edit View Search Terminal Help  
[+] Server 10.10.10.12 allows sessions using username 'martin', password 'apple'  
=====|  
| Getting domain SID for 10.10.10.12 |  
=====|  
Domain Name: CEH  
Domain Sid: S-1-5-21-1366202266-3528535165-3147655684  
[+] Host is part of a domain (not a workgroup)  
=====|  
| OS information on 10.10.10.12 |  
=====|  
Use of uninitialized value $os info in concatenation (.) or string at ./enum4linux.pl line 464.  
[+] Got OS info for 10.10.10.12 from smbclient:  
[+] Got OS info for 10.10.10.12 from srvinfo:  
10.10.10.12 Wk Sv PDC Tim NT  
platform_id : 500  
os version : 6.3  
server type : 0x80102b  
enum4linux complete on Fri Dec 29 04:01:13 2017  
root@kali:~#
```

FIGURE 11.7: OS information of the target

TASK 3

Test for Password Policy Info

- 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**.

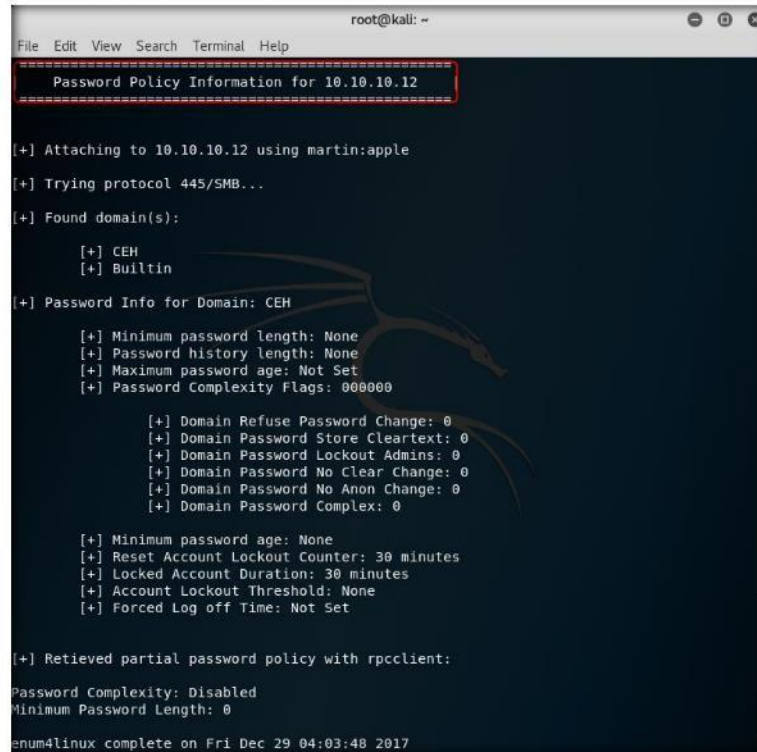


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# enum4linux -u martin -p apple -P 10.10.10.12
```

FIGURE 11.8: Enum4linux command to enumerate password policy information

Module 04 – Enumeration

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



```
root@kali: ~
File Edit View Search Terminal Help
=====
Password Policy Information for 10.10.10.12
=====

[+] Attaching to 10.10.10.12 using martin:apple
[+] Trying protocol 445/SMB...
[+] Found domain(s):
    [+] CEH
    [+] Bulltin
[+] Password Info for Domain: CEH
    [+] Minimum password length: None
    [+] Password history length: None
    [+] Maximum password age: Not Set
    [+] Password Complexity Flags: 000000

        [+] Domain Refuse Password Change: 0
        [+] Domain Password Store Cleartext: 0
        [+] Domain Password Lockout Admins: 0
        [+] Domain Password No Clear Change: 0
        [+] Domain Password No Anon Change: 0
        [+] Domain Password Complex: 0

    [+] Minimum password age: None
    [+] Reset Account Lockout Counter: 30 minutes
    [+] Locked Account Duration: 30 minutes
    [+] Account Lockout Threshold: None
    [+] Forced Log off Time: Not Set

[+] Retrieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 0

enum4linux complete on Fri Dec 29 04:03:48 2017
```

FIGURE 11.9: Password policy information of the target machine

TASK 4

Test for Group Info

- 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**.

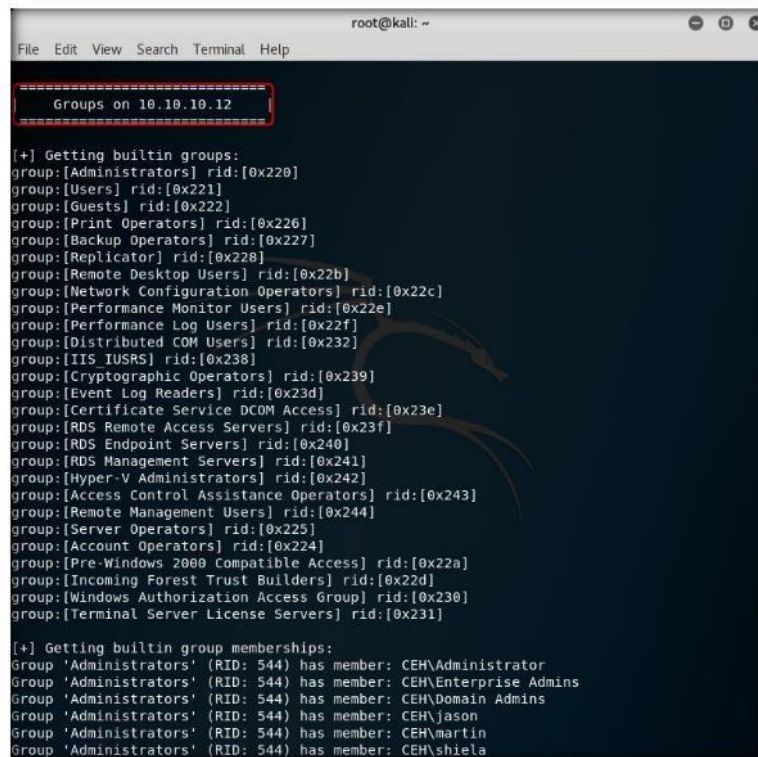


```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# enum4linux -u martin -p apple -G 10.10.10.12
```

FIGURE 11.10: Enum4linux command for group and domain info

Module 04 – Enumeration

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

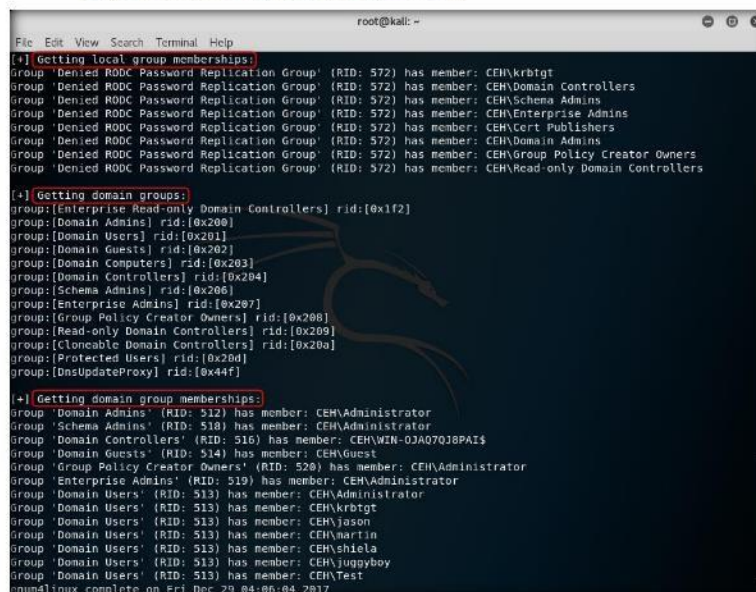
A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the output of a command to enumerate groups on the target IP 10.10.10.12. The output is divided into two sections: 'Getting builtin groups' and 'Getting builtin group memberships'. The first section lists various built-in Windows groups with their respective RIDs. The second section shows the members of the 'Administrators' group, including 'Administrator', 'Enterprise Admins', 'Domain Admins', 'jason', 'martin', and 'shielia'.

```
root@kali: ~  
File Edit View Search Terminal Help  
-----  
Groups on 10.10.10.12  
-----  
[+] Getting builtin groups:  
group:[Administrators] rid:[0x220]  
group:[Users] rid:[0x221]  
group:[Guests] rid:[0x222]  
group:[Print Operators] rid:[0x226]  
group:[Backup Operators] rid:[0x227]  
group:[Replicator] rid:[0x228]  
group:[Remote Desktop Users] rid:[0x22b]  
group:[Network Configuration Operators] rid:[0x22c]  
group:[Performance Monitor Users] rid:[0x22e]  
group:[Performance Log Users] rid:[0x22f]  
group:[Distributed COM Users] rid:[0x232]  
group:[IIS IUSRS] rid:[0x238]  
group:[Cryptographic Operators] rid:[0x239]  
group:[Event Log Readers] rid:[0x23d]  
group:[Certificate Service DCOM Access] rid:[0x23e]  
group:[RDS Remote Access Servers] rid:[0x23f]  
group:[RDS Endpoint Servers] rid:[0x240]  
group:[RDS Management Servers] rid:[0x241]  
group:[Hyper-V Administrators] rid:[0x242]  
group:[Access Control Assistance Operators] rid:[0x243]  
group:[Remote Management Users] rid:[0x244]  
group:[Server Operators] rid:[0x225]  
group:[Account Operators] rid:[0x224]  
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]  
group:[Incoming Forest Trust Builders] rid:[0x22d]  
group:[Windows Authorization Access Group] rid:[0x230]  
group:[Terminal Server License Servers] rid:[0x231]  
  
[+] Getting builtin group memberships:  
Group 'Administrators' (RID: 544) has member: CEH\Administrator  
Group 'Administrators' (RID: 544) has member: CEH\Enterprise Admins  
Group 'Administrators' (RID: 544) has member: CEH\Domain Admins  
Group 'Administrators' (RID: 544) has member: CEH\jason  
Group 'Administrators' (RID: 544) has member: CEH\martin  
Group 'Administrators' (RID: 544) has member: CEH\shielia
```

FIGURE 11.11: Group info of the target

Module 04 – Enumeration

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



```
root@kali: ~
File Edit View Search Terminal Help
[+] Getting local group memberships:
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\krbtgt
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Domain Controllers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Schema Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Enterprise Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Cert Publishers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Domain Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Group Policy Creator Owners
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Read-only Domain controllers
[+] Getting domain groups:
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[DnsupdateProxy] rid:[0x44f]
[+] Getting domain group memberships:
Group 'Domain Admins' (RID: 512) has member: CEH\Administrator
Group 'Schema Admins' (RID: 518) has member: CEH\Administrator
Group 'Domain Controllers' (RID: 516) has member: CEH\WIN-OJA07QJ8PA1$
Group 'Domain Guests' (RID: 514) has member: CEH\Guest
Group 'Group Policy Creator Owners' (RID: 528) has member: CEH\Administrator
Group 'Enterprise Admins' (RID: 519) has member: CEH\Administrator
Group 'Domain Users' (RID: 513) has member: CEH\Administrator
Group 'Domain Users' (RID: 513) has member: CEH\krbtgt
Group 'Domain Users' (RID: 513) has member: CEH\jason
Group 'Domain Users' (RID: 513) has member: CEH\martin
Group 'Domain Users' (RID: 513) has member: CEH\chiela
Group 'Domain Users' (RID: 513) has member: CEH\juggpyboy
Group 'Domain Users' (RID: 513) has member: CEH\Test
enum4linux complete on Fri Dec 29 04:06:04 2017
```

FIGURE 11.12: Domain and group memberships of the target system

TASK 5

Test for Share Info

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**.

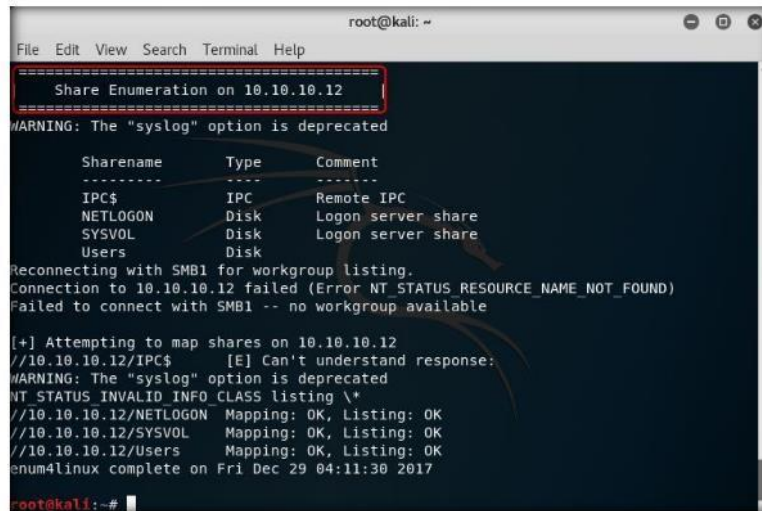


```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# enum4linux -u martin -p apple -S 10.10.10.12
```

FIGURE 11.13: Enum4linux command to get the share info

Module 04 – Enumeration

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



```
root@kali: ~
File Edit View Search Terminal Help
=====
Share Enumeration on 10.10.10.12
=====
WARNING: The "syslog" option is deprecated

Sharename      Type      Comment
-----
IPC$           IPC       Remote IPC
NETLOGON      Disk     Logon server share
SYSVOL        Disk     Logon server share
Users         Disk

Reconnecting with SMB1 for workgroup listing.
Connection to 10.10.10.12 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.12
//10.10.10.12/IPC$ [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_INVALID_INFO_CLASS listing \*
//10.10.10.12/NETLOGON Mapping: OK, Listing: OK
//10.10.10.12/SYSVOL Mapping: OK, Listing: OK
//10.10.10.12/Users Mapping: OK, Listing: OK
enum4linux complete on Fri Dec 29 04:11:30 2017
root@kali:~#
```

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs