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 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 D:\CEH-Tools\CEHv9 Module 04 Enumeration

Lab Environment

To complete this lab, you will need:

- Windows Server 2012 as host machine
- Windows Server 2008, Windows 8.1, Windows 7 and Kali Linux as virtual machines
- A Web browser with an Internet connection
- Administrative privilege to run tools

Lab Duration

Time: 85 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 **SNMPCHECK**
- LDAP Enumeration Using **Active Directory Explorer** (**ADExplorer**)
- Performing Network Enumeration Using Various **DNS Interrogation Tools**

Lab Analysis

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

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

Lab 1

NetBIOS Enumeration Using Global Network Inventory

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

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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

To complete this lab, you will need:

- Global Network Inventory, located at **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory Scanner**
- You can also 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 2012 as attacker (host machine)
- Another computer running Window Server 2008 as victim (virtual machine)

- A Web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Global Network Inventory

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

Lab Tasks

TASK 1

Install Global Network Inventory

1. Navigate to **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory Scanner** 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.

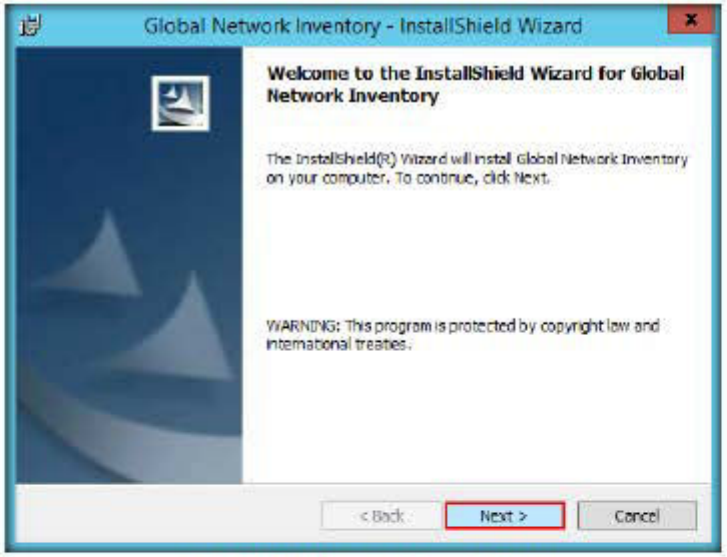


FIGURE 1.1: Global Network Inventory Installation Wizard

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

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

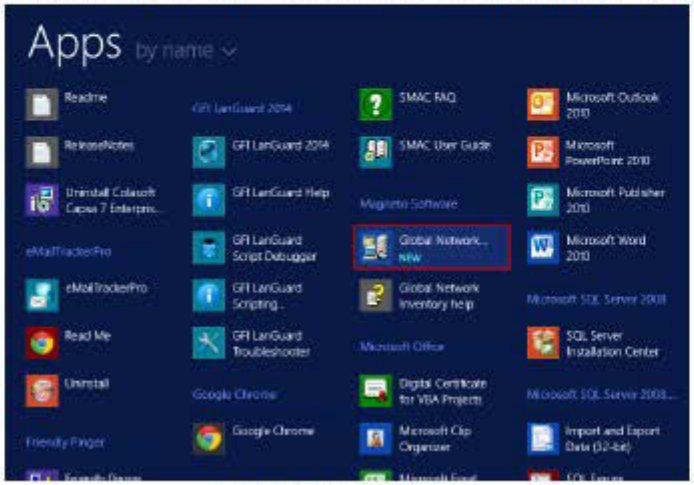


FIGURE 1.2 Windows Server 2012 Apps screen

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

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

Scan only items that you need by customizing scan elements.

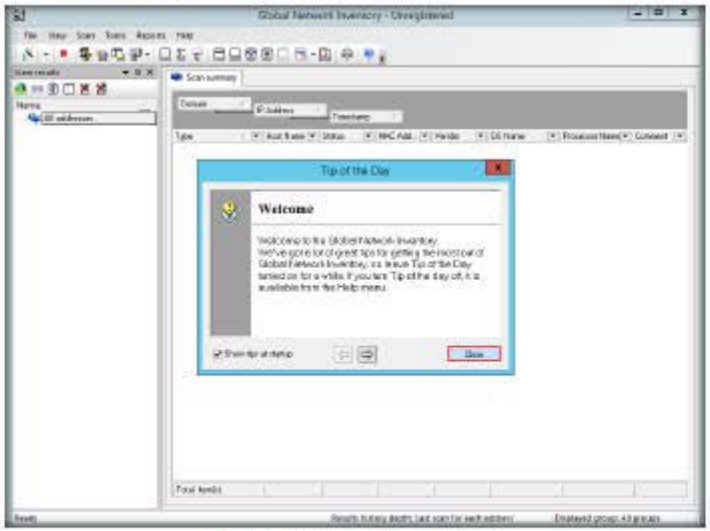


FIGURE 1.3: Global Network Inventory main window

TASK 2

Configure Global Inventory Scanner

6. Log into the **Windows Server 2008** virtual machine from Hyper-V Manager
7. Now, switch back to the host machine. The **New Audit Wizard** window appears, click **Next**.

FIGURE 1.4: Global Network Inventory new audit wizard

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

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

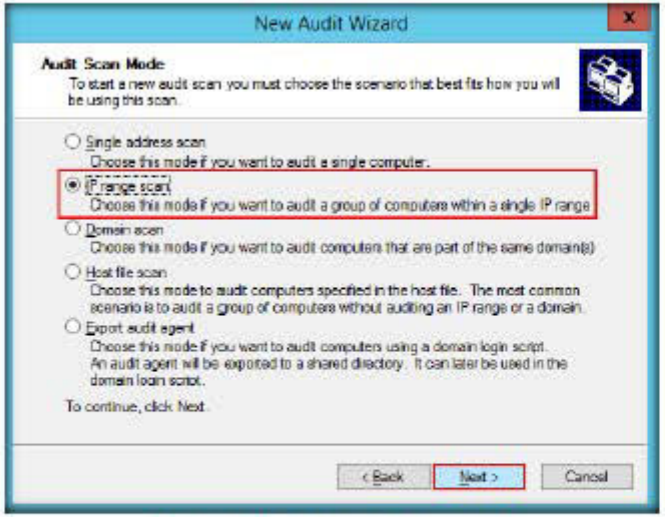


FIGURE 1.5: Global Network Inventory Audit Scan Mode section

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

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FIY
HaCkRhInO-TeaM !

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

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

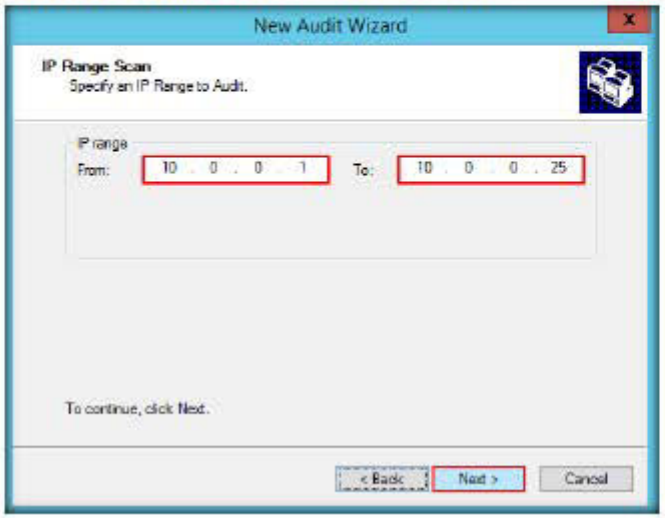


FIGURE 1.6: Setting an IP range to scan

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

10. The Authentication Settings section appears; select **Connect as,** enter the credentials of **Windows Server 2008 Virtual Machine,** and click **Next**.

Note: In real time, attackers do not know the credentials of the remote machine/machines. In such case, they simply choose the **Connect as currently logged on user** option and 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.

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

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

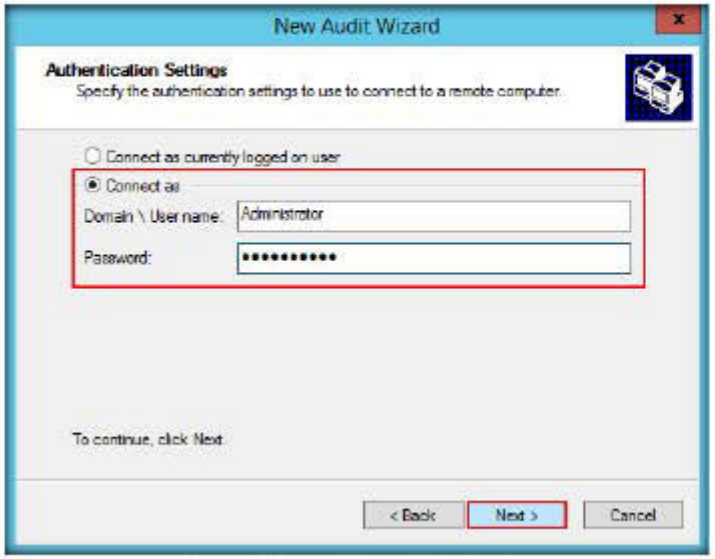


FIGURE 1.7: Global Network Inventory Authentication settings

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

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

FIGURE 1.8: Global Network Inventory final Audit wizard

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

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

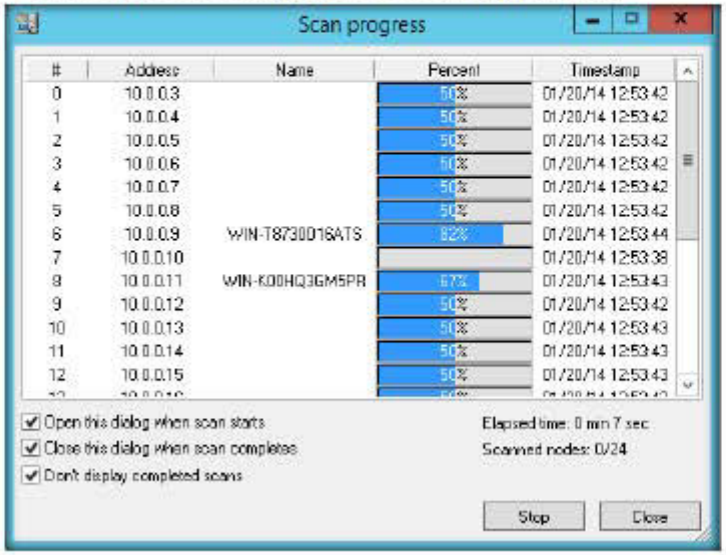


FIGURE 1.9: Global Network Inventory Scanning Progress

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).

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

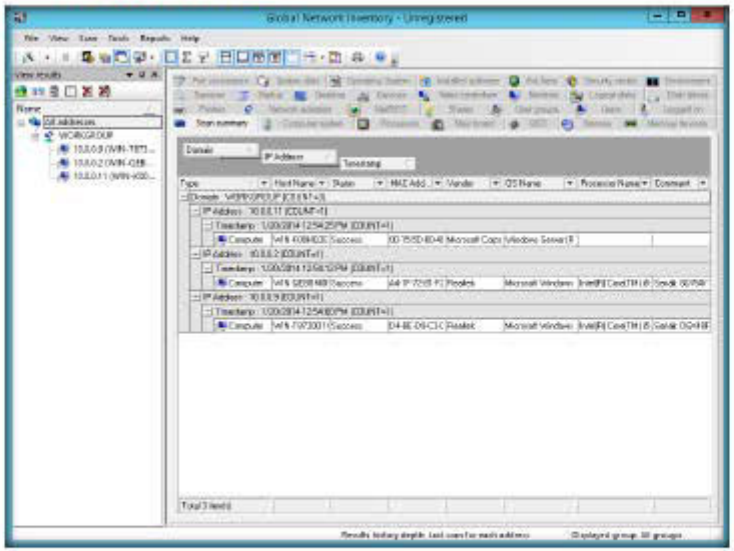


FIGURE 1.10: Global Network Inventory result window

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.

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 2008** (**10.0.0.11**) 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.

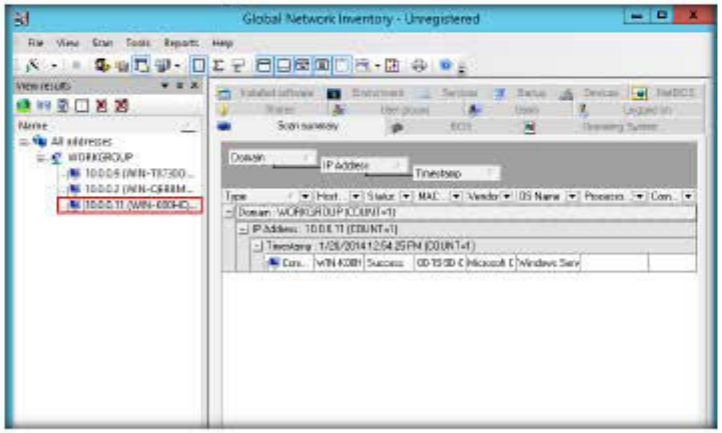


FIGURE 1.11: Global Network Inventory Individual machine results

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.

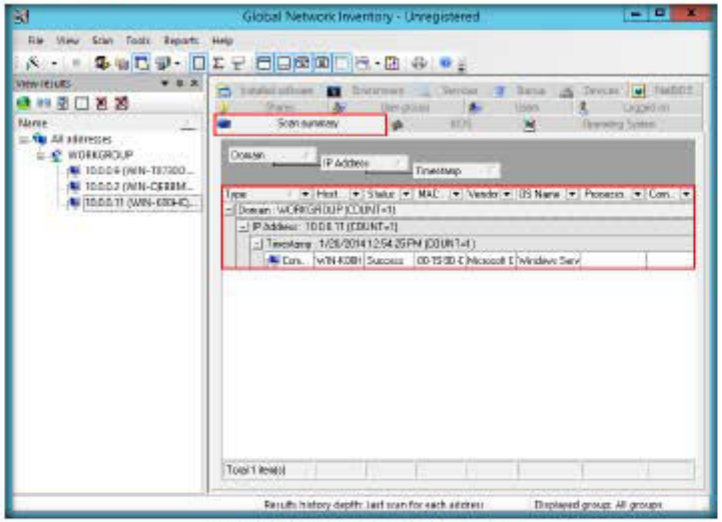
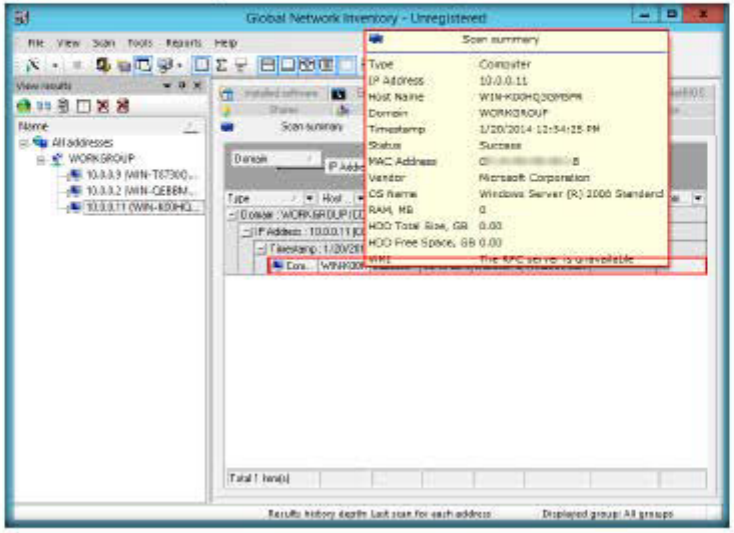


FIGURE 1.12: Global Inventory Scan Summary tab

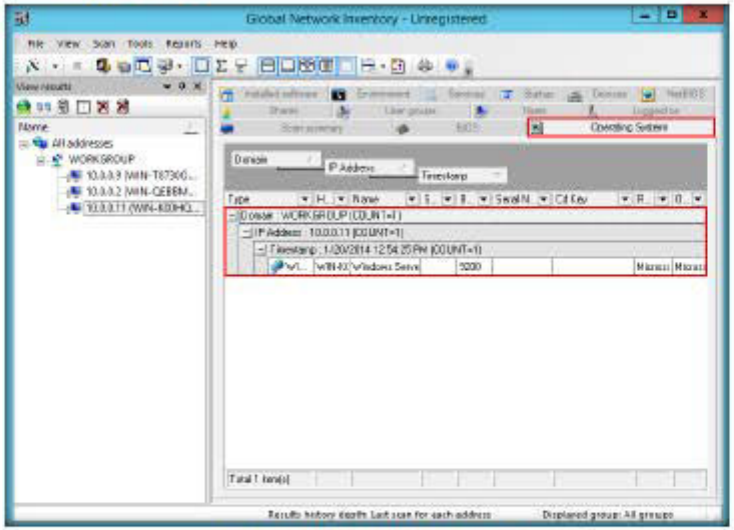
16. You can even hover the mouse cursor over the computer details tab to view the scan summary, as shown in the following screenshot:



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

FIGURE 1.13: Global Inventory displaying the Scan summary

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 1.14: Global Inventory Operating System tab

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

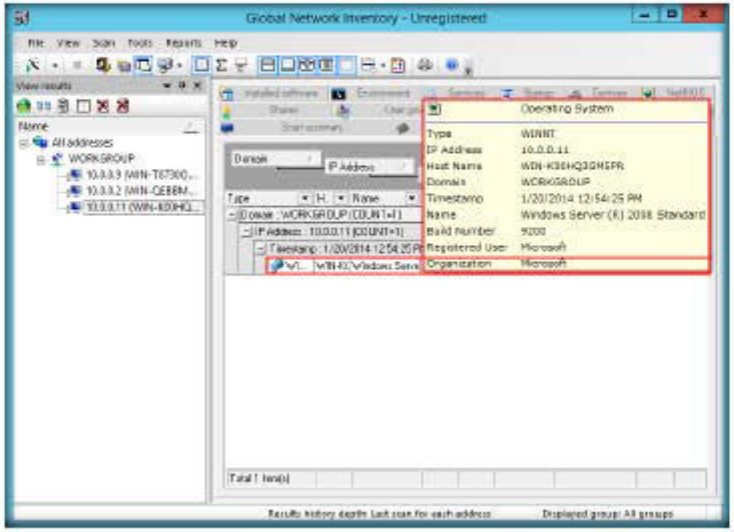


FIGURE 1.15: Global Inventory displaying the operating system details

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

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

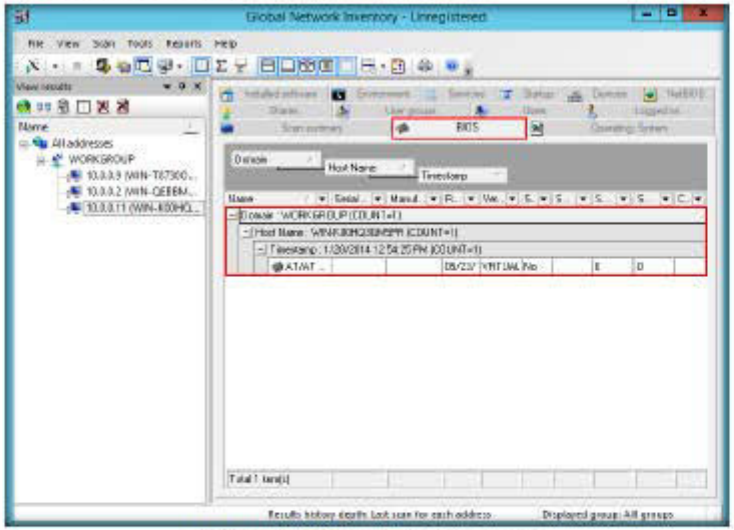


FIGURE 1.16: Global Network Inventory Bios summary tab

Scan only items that you need by customizing scan elements.

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.

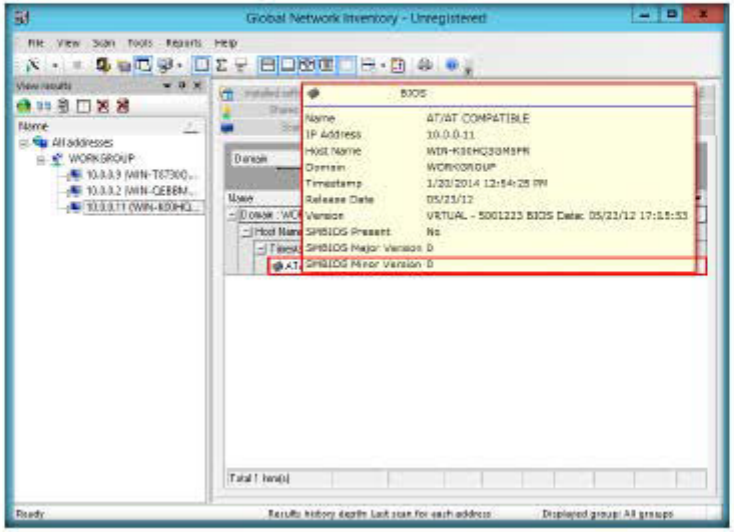


FIGURE 1.17: Global Network Inventory displaying the Bios summary information

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.

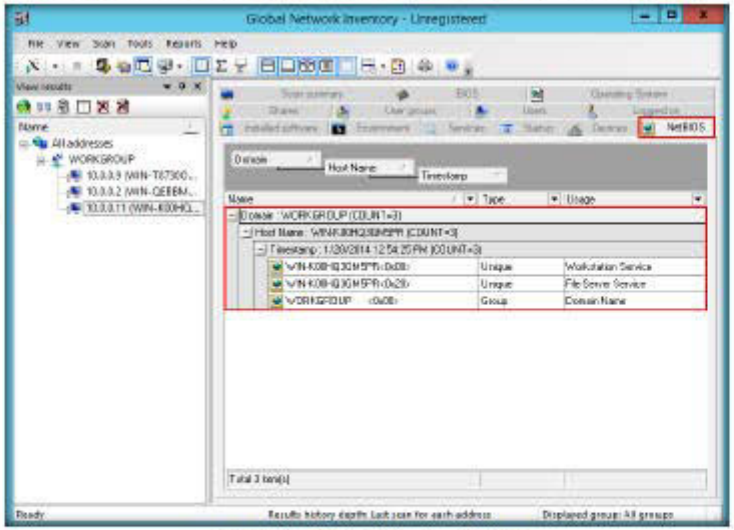
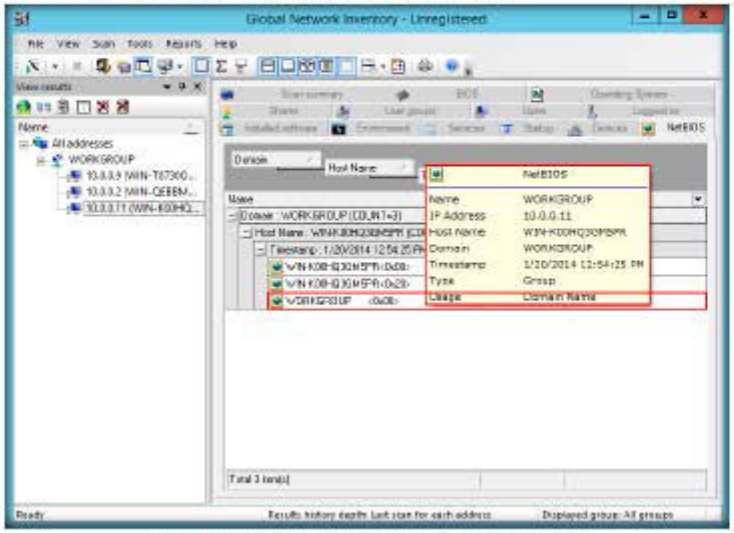


FIGURE 1.18: Global Network Inventory NetBIOS tab

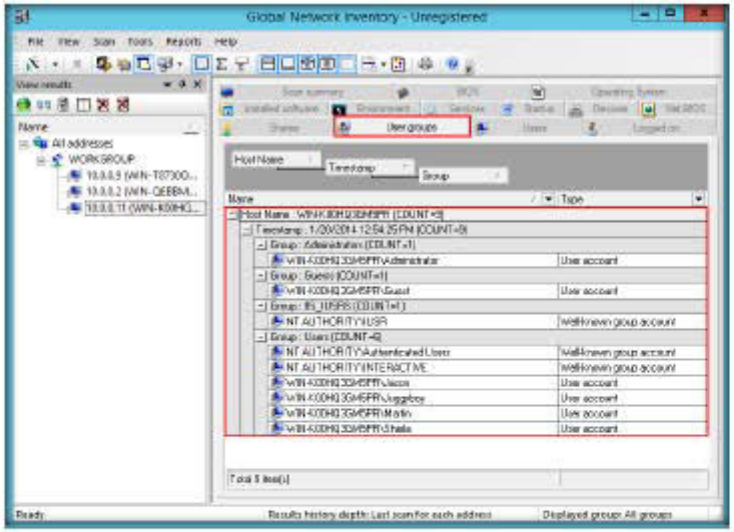
22. Click each NetBIOS application to view its details.



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

FIGURE 1.19: Global Network Inventory displaying the NetBIOS information

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 1.20: 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.

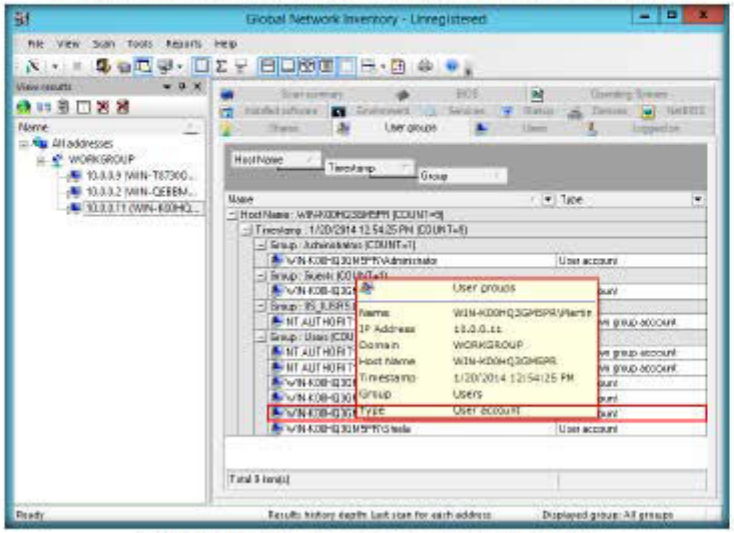


FIGURE 1.21: Global Network Inventory displaying the User groups information

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.

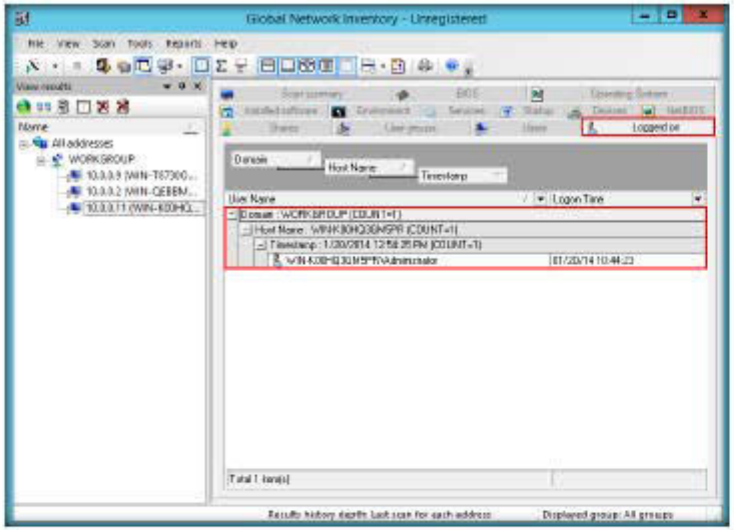


FIGURE 1.22: Global Network Inventory Logged on tab

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

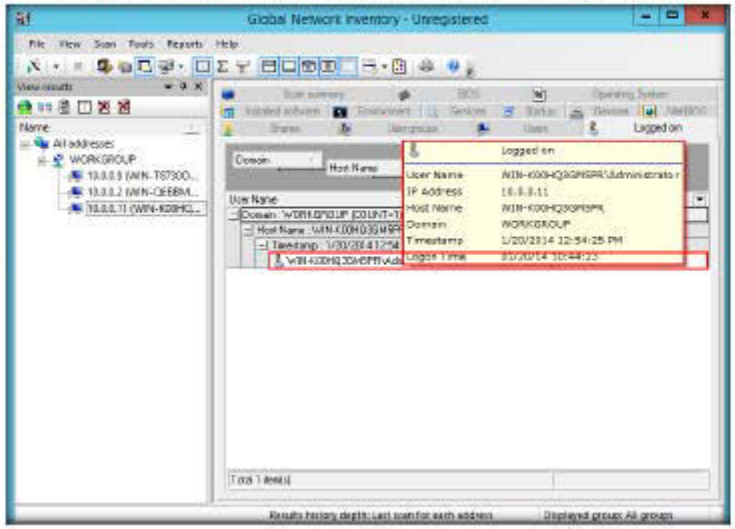


FIGURE 1.23: Global Network Inventory displaying the Logged on information

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

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

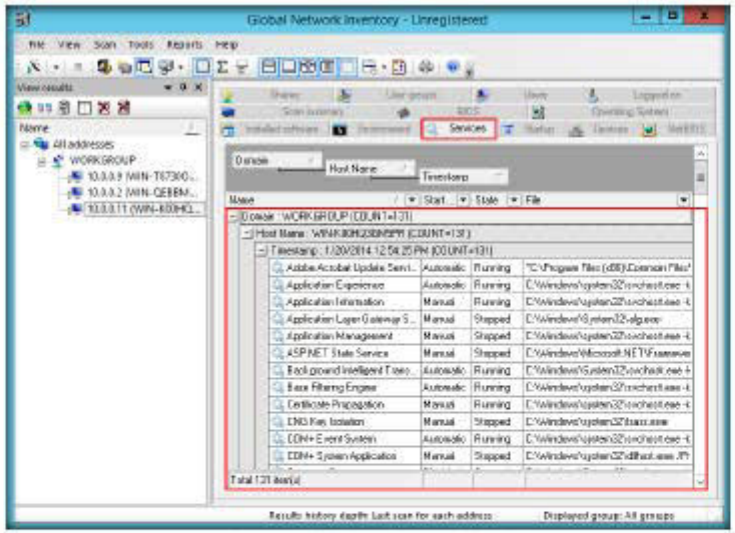


FIGURE 1.24: Global Network Inventory Services tab

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.

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

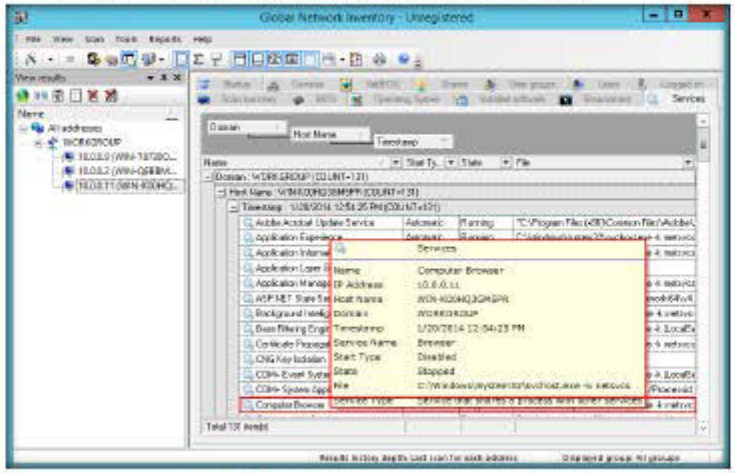
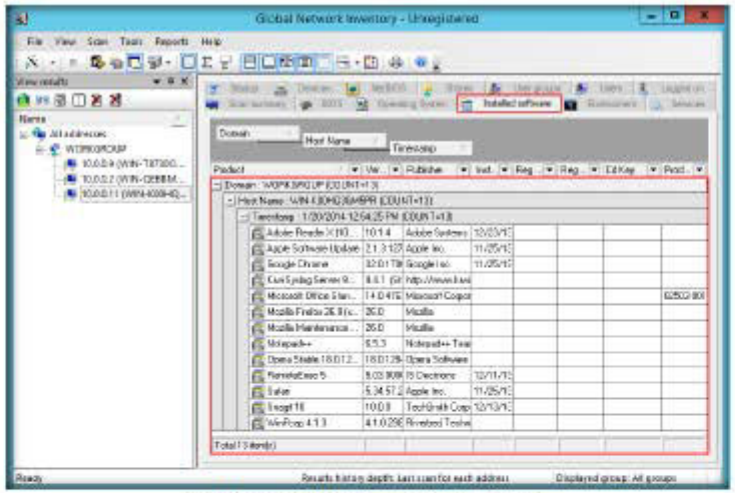


FIGURE 1.25: Global Network Inventory displaying the Services information

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 1.26: Global Network Inventory Network Adapter tab

30. Hover over software names to view their details.

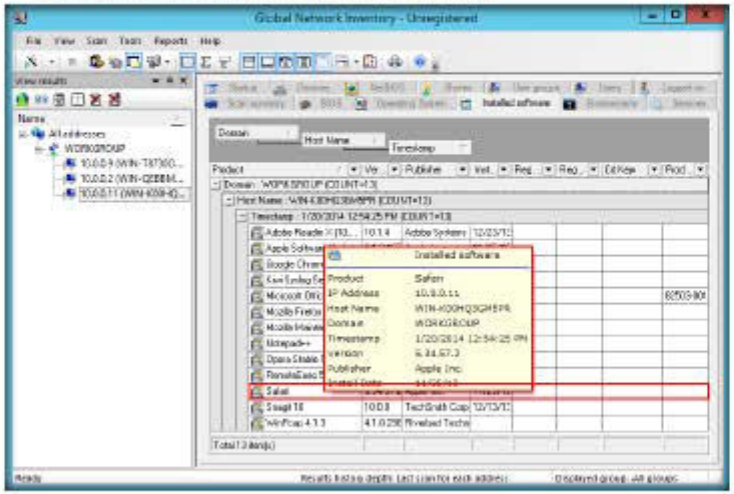


FIGURE 1.27: Global Network Inventory displaying the Network Adapter information

Lab Analysis

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

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

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

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FIY
HaCkRhInO-TeaM !

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 intrudes 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 D:\CEH-Tools\CEHv9 Module 03 Scanning Networks

Lab Environment

In this lab, you will need:

- Advanced IP Scanner located at **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Ping Sweep Tools\Advanced IP Scanner**
- You can also download the latest version of Advanced IP Scanner from the link http://www.advanced-ip-scanner.com
- If you decide to download the latest version, then screenshots shown in the lab might differ

- A computer running Windows Server 2012 as attacker (host machine)
- A computer running Windows server 2008 as victim (virtual machine)
- A computer running Windows 8.1 as victim (virtual 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 **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Ping Sweep Tools\Advanced IP Scanner** and double-click **ipscan23.exe**.
2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. Select a language, and click **OK**.

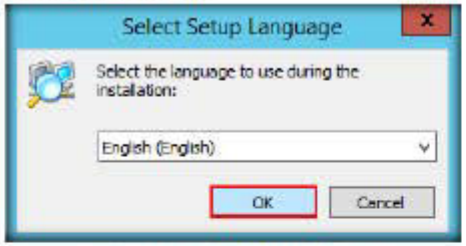


FIGURE 2.1: Select Setup Language dialog-box

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

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

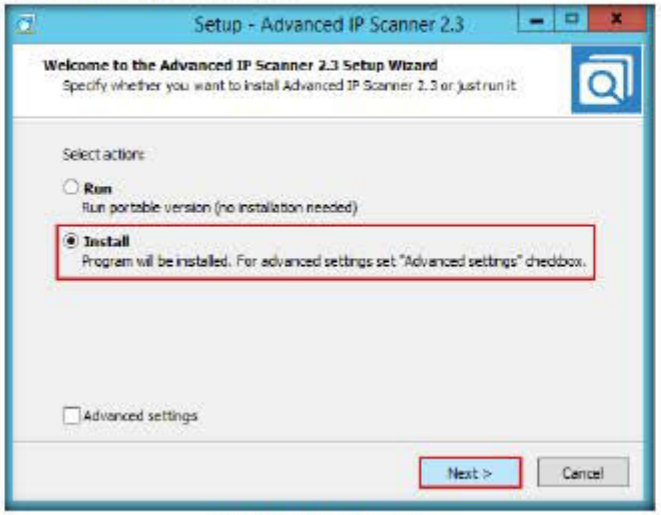


FIGURE 2.2: Advance IP Scanner setup

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.

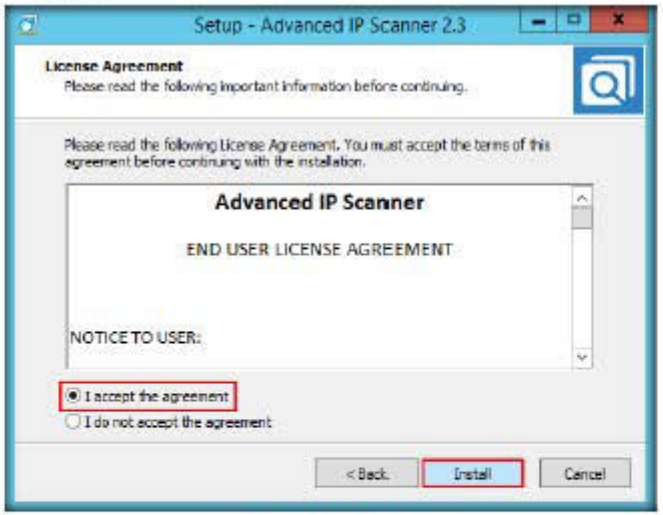


FIGURE 2.3: Advance IP Scanner setup

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

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 Screen

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

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

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

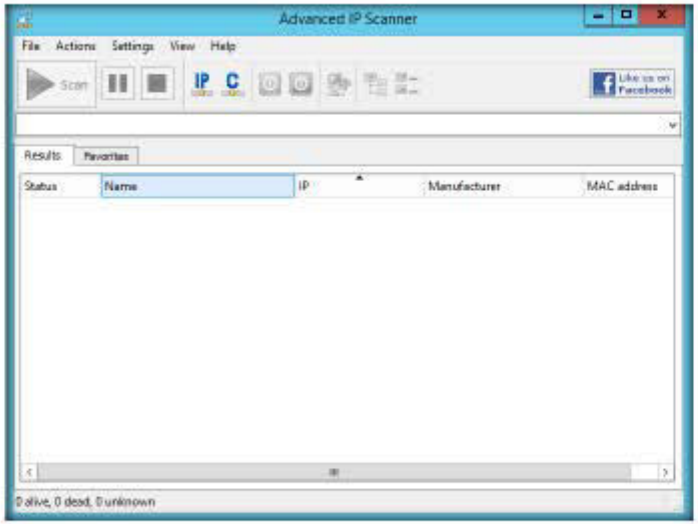


FIGURE 2.5: Advanced IP Scanner main window

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

TASK 2

Scan a Network to Discover hosts

8. Now, launch one or more virtual machines; in this lab we are logging into **Windows Server 2008** and **Windows 8.1**.
9. Switch back to the attacker machine (**Windows Server 2012**) and specify the IP address range in the **Select range** field.
10. Click **Scan** button to begin the scan.

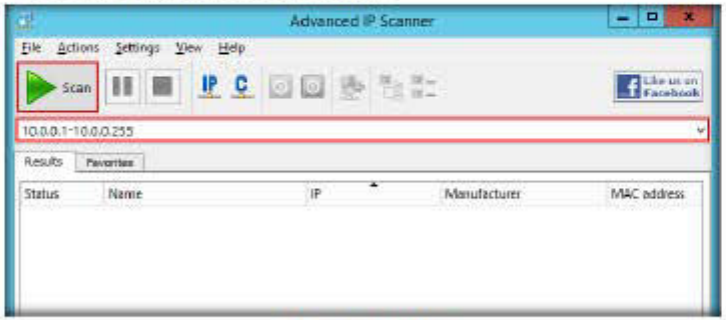


FIGURE 2.6: Scanning a Subnet

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.

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

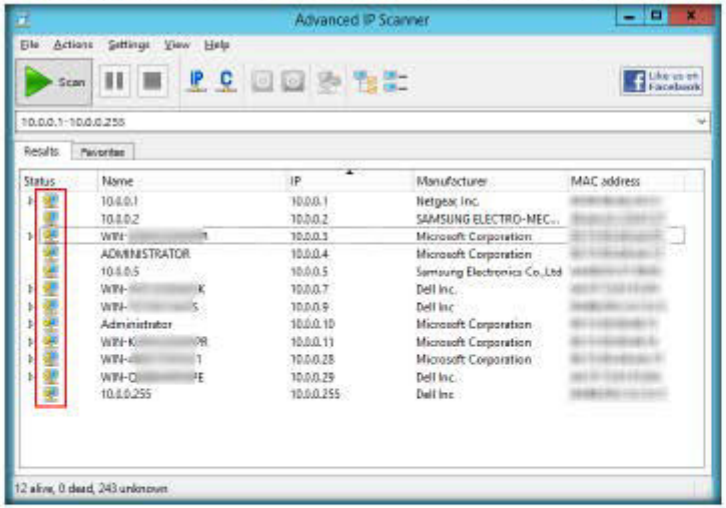


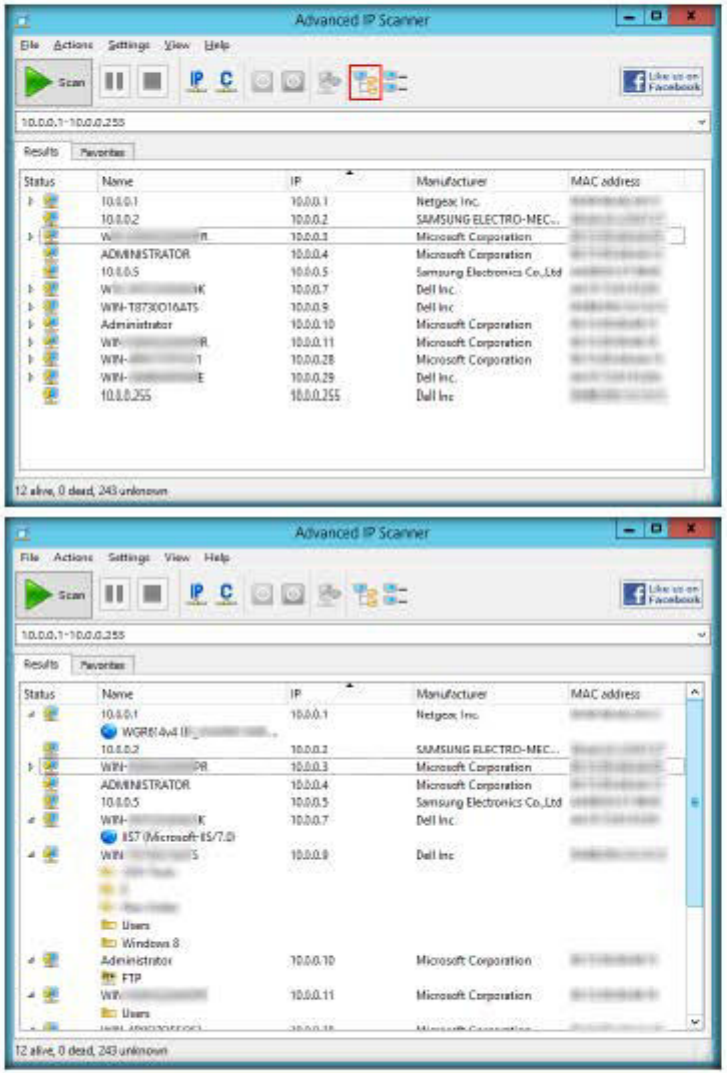
FIGURE 2.7: Advanced IP Scanner displaying Alive Host list

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.

13. Now, you have the **IP address**, **Name**, **MAC address**, and **Manufacturer** information of the victim machine.
14. Click **Expand all** to view the shared folders and services running on the victim machine.

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

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.

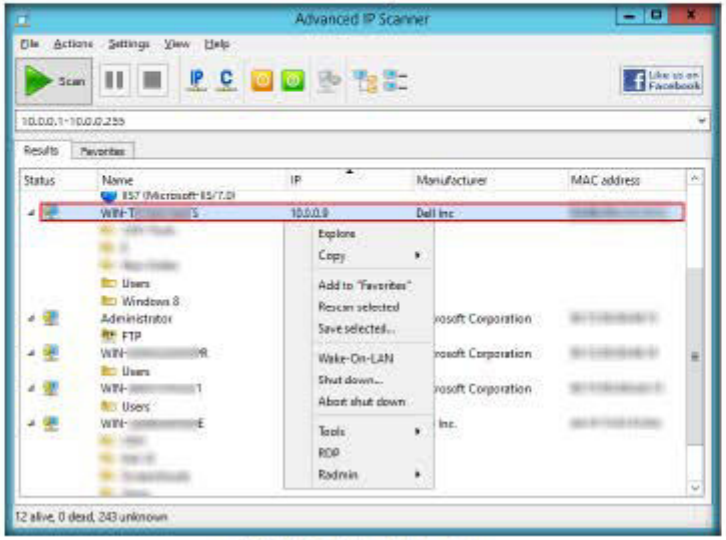


FIGURE 2.9: Exploring the victim machines

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.

19. Right-click **10.0.0.11** and select **Shut down...**.

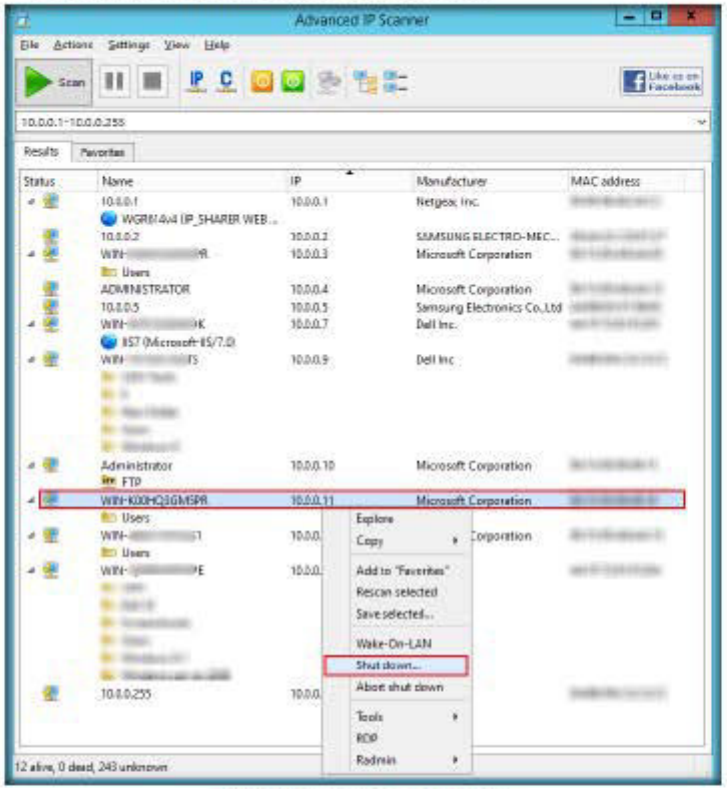


FIGURE 2.10: Shutting down a virtual machine

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.

Note: 10.0.0.11 is the IP address of **Windows Server 2008** 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 ListSingle Host Neighborhood

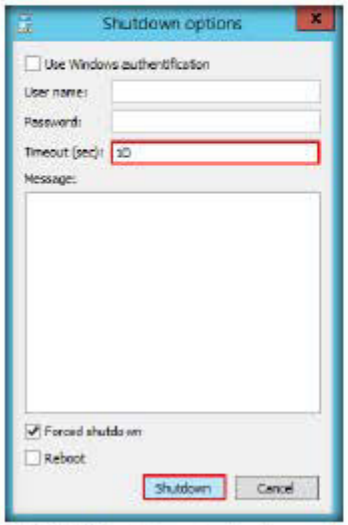


FIGURE 2.11: Shutting down a virtual machine remotely

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

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

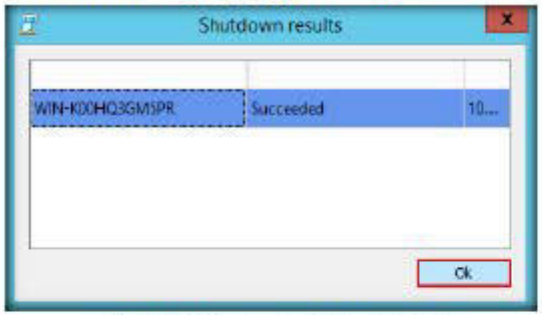


FIGURE 2.12: Shutting down a virtual machine remotely

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

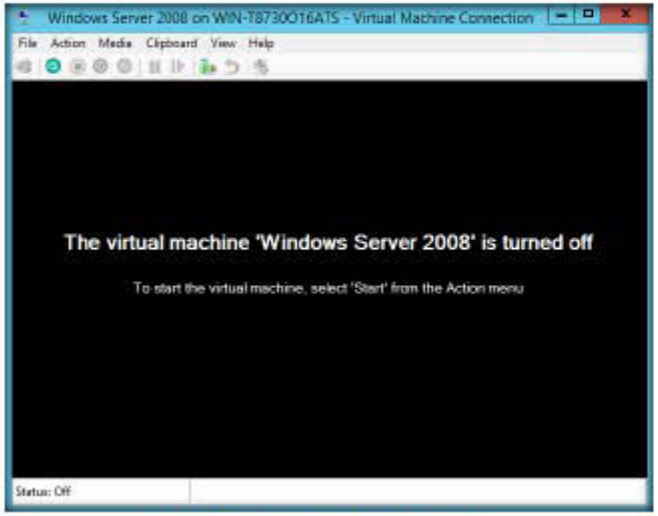


FIGURE 2.13: Victim machine successfully shutdown

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.

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

Lab Analysis

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

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

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

Lab 3

Performing Network Enumeration Using SuperScan

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

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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 04 Enumeration

To complete this lab, you will need:

- SuperScan is located at **D:\CEH-Tools\CEHv9 Module 04 Enumeration\NetBIOS Enumeration Tools\SuperScan**
- You can also download the latest version of SuperScan from this link http://www.mcafee.com/us/downloads/free-tools/superscan.aspx

- A computer running Windows Server 2012 as host machine
- Windows 8.1 running on a virtual machine as target machine
- Administrative privileges to install and run tools
- A Web browser with an Internet connection

Lab Duration

Time: 5 Minutes

Overview of SuperScan

1. The purpose of SuperScan is to gather information such as:
   a. Account lockout threshold
   b. Local groups and user accounts
   c. 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

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

Lab Tasks

TASK 1

Launch SuperScan

1. Launch **Windows 8.1** virtual machine before beginning this lab.
2. Switch back to host machine (Windows Server 2012), navigate to **D:\CEH-Tools\CEHv9 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, as shown in the following screenshot:

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
- Simple HTML report generation
- Source port scanning
- Fast hostname resolving
- Extensive banner grabbing
- Massive built-in port list description database
- IP and port scan order randomization
- A collection of useful tools (ping, traceroute, Whois etc.)
- Extensive Windows host enumeration capability

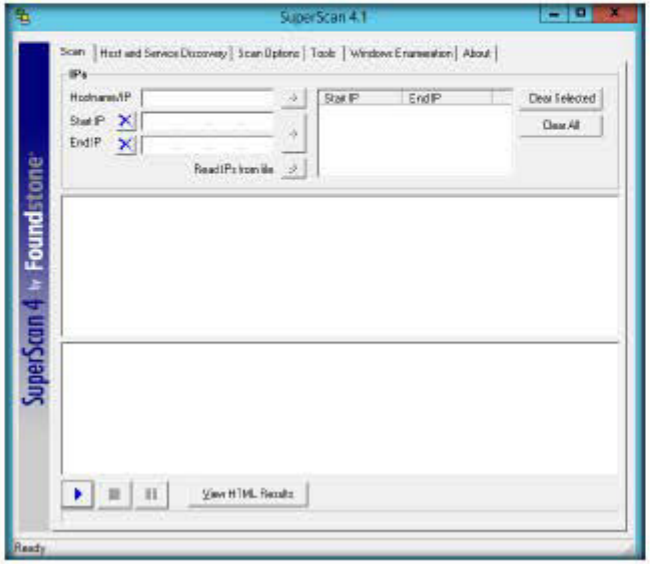


FIGURE 3.1: SuperScan main window

5. Click on the **Windows Enumeration** tab.
6. Enter the IP address of the target machine in the **Hostname/IP/URL** textbox. In this lab, we have entered **Windows 8.1** virtual machine IP address.

Note: This IP address may differ in lab environment.

TASK 2

Perform Enumeration

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

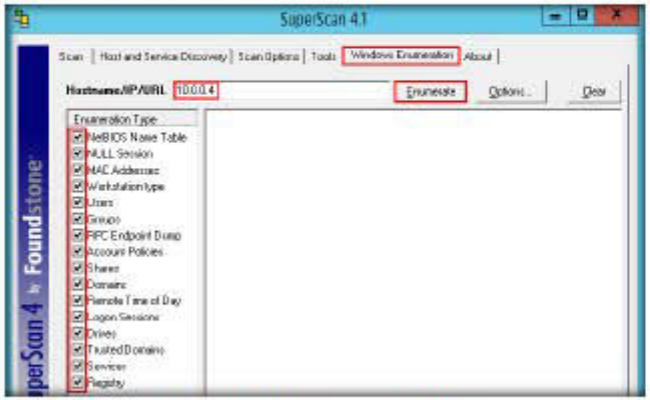


FIGURE 3.2: SuperScan main window with IP Address

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

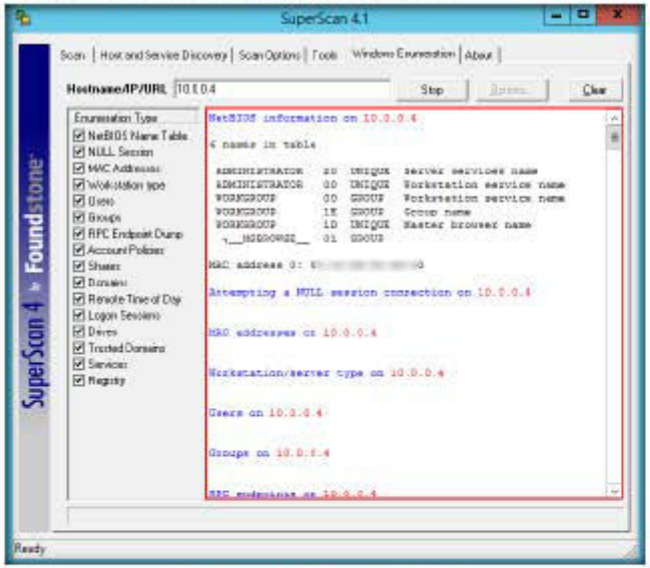


FIGURE 3.3: SuperScan main window with results

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.

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.

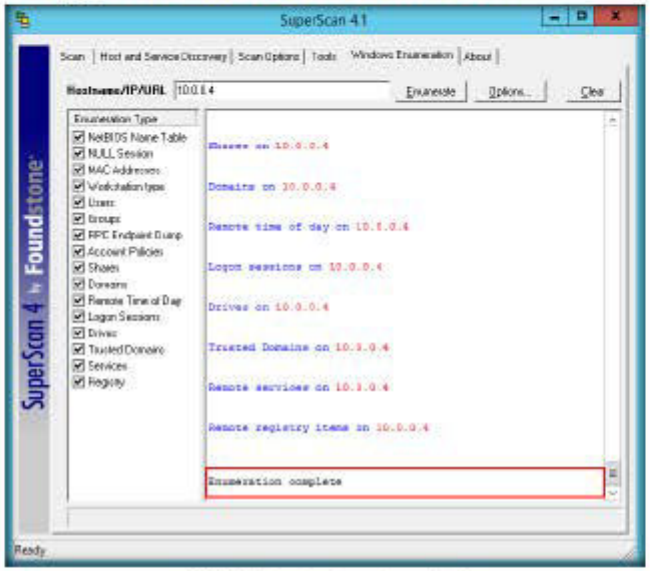


FIGURE 3.4: SuperScan Enumeration completed

TASK 3

Analyze the Results

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

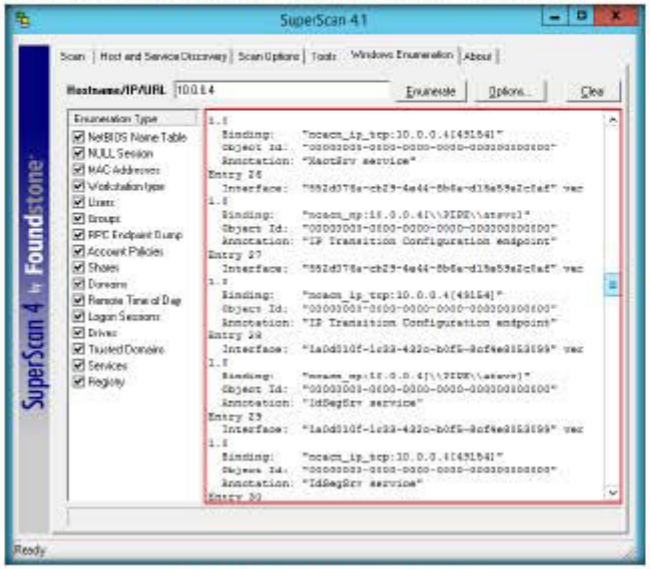


FIGURE 3.5: SuperScan Enumeration Results

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

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

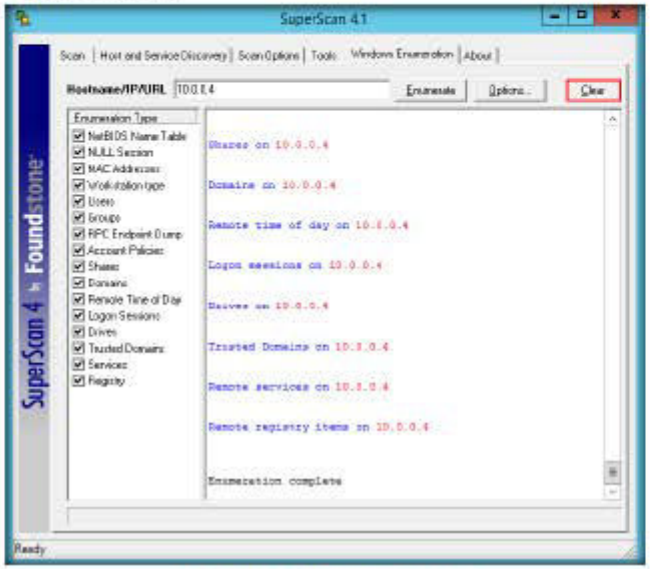


FIGURE 3.6: SuperScan main window with results

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.

Lab Analysis

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

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

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

Lab 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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 04 Enumeration

Lab Environment

To perform this lab, you need:

- A computer running Windows Server 2012
- Administrative privileges to install and run tools
- You can also download this tool from following link: http://www.systemtools.com/hyena/download.htm

- 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 **D:\CEH-Tools\CEHv9 Module 04 Enumeration\NetBIOS Enumeration Tools\Hyena** and double-click **Hyena_English_x64.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.

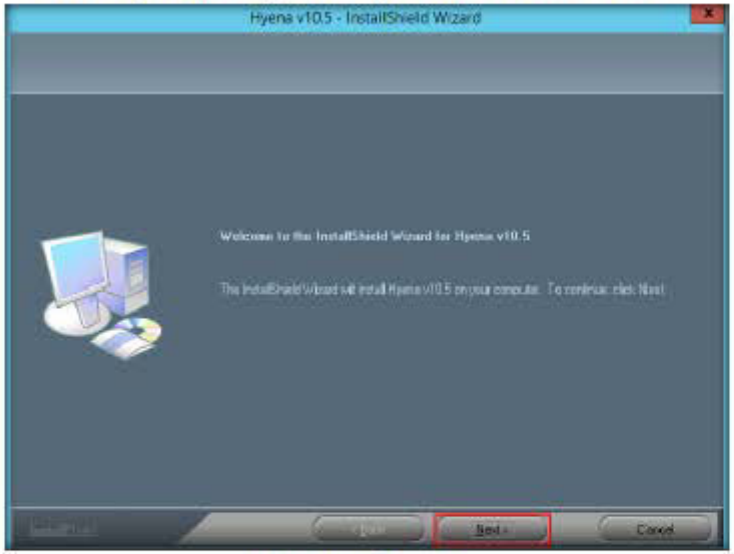


FIGURE 4.1: Installation of Hyena

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

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

FIGURE 4.2: Windows Server 2012 Installed Apps

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

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

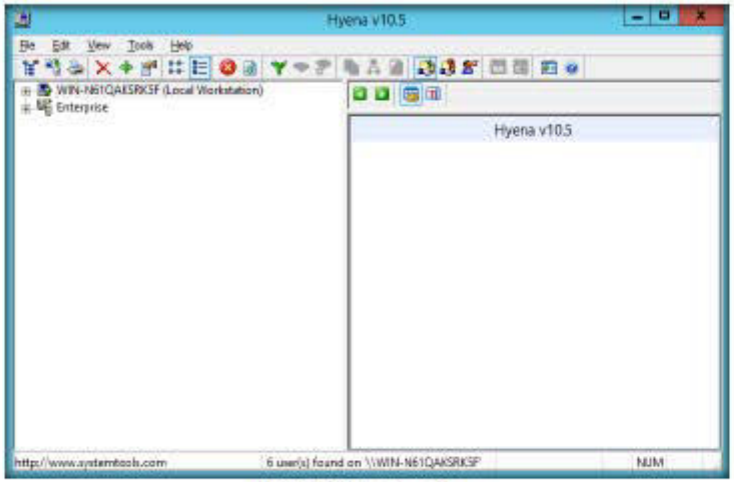


FIGURE 4.3: Main window of Hyena

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

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.

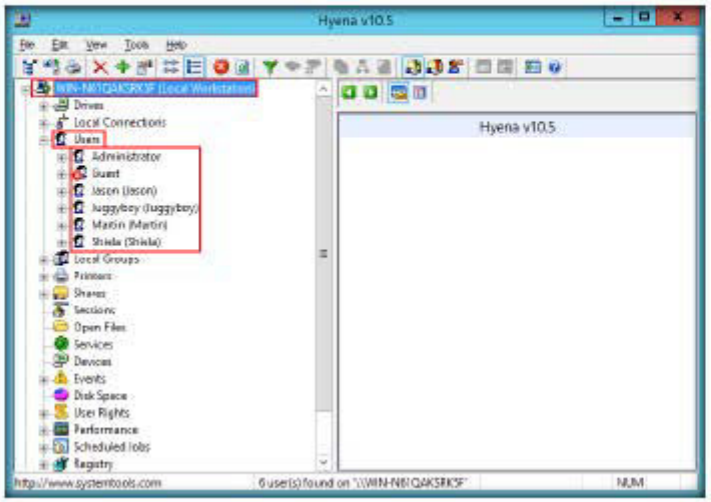


FIGURE 4.4: Expand the System users

TASK 3

Examine the Results

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

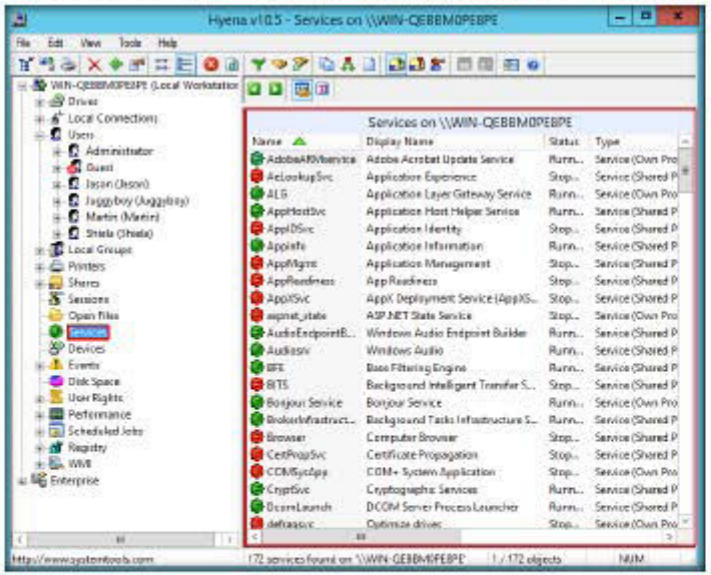


FIGURE 4.5: Services running in the system

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

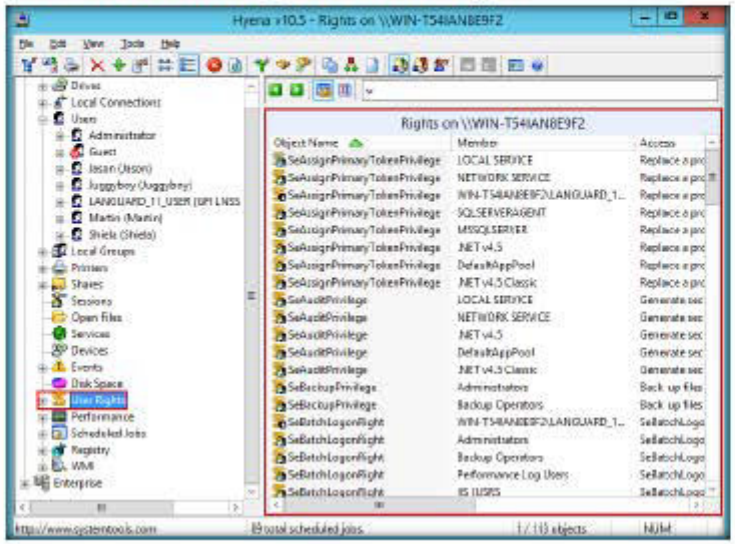


FIGURE 4.6: Users Rights

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

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

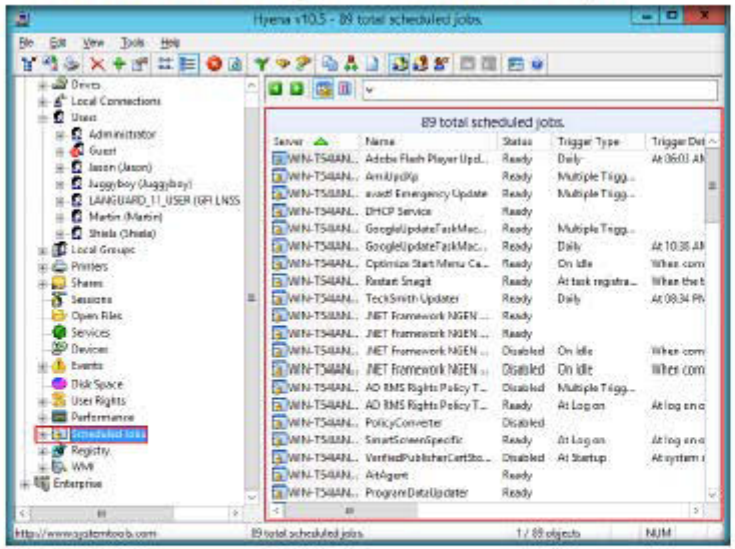


FIGURE 4.7: Scheduled Jobs

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

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

Lab Analysis

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

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

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

Lab 5

Performing Network Enumeration Using NetBIOS Enumerator

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

ICON KEY

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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 04 Enumeration

Lab Scenario

Enumeration is the first attack on a target network, used to gather the 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 **D:\CEH-Tools\CEHv9 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator**
- You can also 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 2012 as an Attacker machine

- A virtual machine running Windows Server 2008 as a target machine
- A virtual machine running Windows 8.1 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 **D:\CEH-Tools\CEHv9 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double click **NetBIOS Enumerater.exe**.
2. If the **Open - File Security Warning** pop-up appears, click **Run**.
3. NetBIOS Enumerator main window appears, as shown in the screenshot:

FIGURE 5.1: NetBIOS Enumerator main window

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.

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

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

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

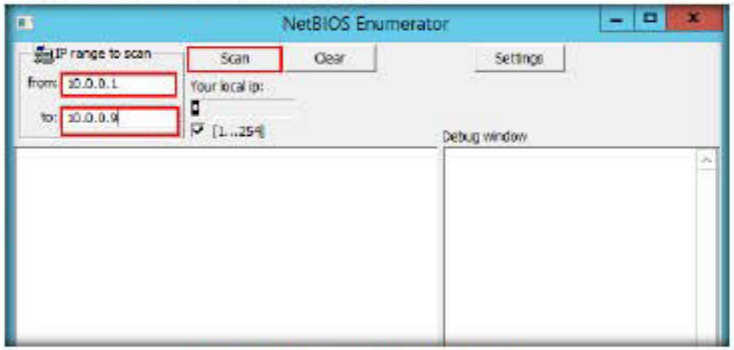


FIGURE 5.2: NetBIOS Enumerator with IP range to scan

Feature:

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

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

TASK 2

Examine the Results

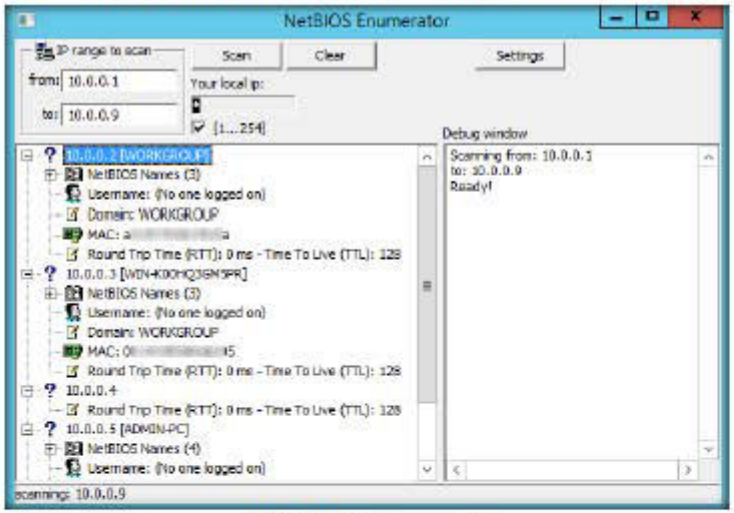


FIGURE 5.3: NetBIOS Enumerator results

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

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.

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

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

10. To perform a new scan or to rescan the provided range of IP addresses, erase the previous scan results by clicking **Clear**.

Lab Analysis

Analyze and document the results related to this lab exercise.

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

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

Lab 6

Enumerating a Network Using SoftPerfect Network Scanner

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

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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 04 Enumeration

Lab Environment

To complete this lab, you will need:

- SoftPerfect Network Scanner is located at **D:\CEH-Tools\CEHv9 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner\64-bit**
- You can also 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 2012 server

- A virtual machine running Windows Server 2008 as a target machine
- A virtual machine running Windows 8.1 as a target machine
- Administrative privileges are required to run this tool

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

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 **D:\CEH-Tools\CEHv9 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner\64-bit**, and double click **netscan.exe**.

Note: If the host machine (Windows Server 2012) is 32-bit, you need to navigate to **D:\CEH-Tools\CEHv9 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner\32-bit** and double click **netscan.exe**.

2. If the **Open File - Security Warning** pop-up appears, click **Run**.
3. If the **Network Scanner** dialog box appears, click **No**.

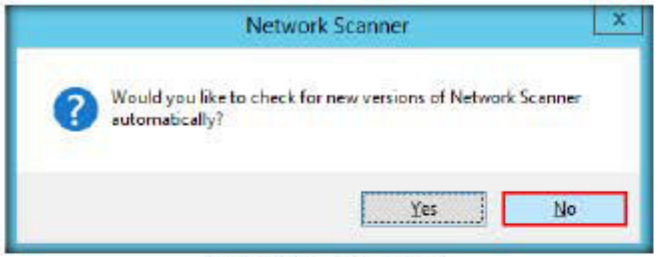


FIGURE 6.1: Network Scanner dialog-box

TASK 2

Perform Enumeration

4. The SoftPerfect Network Scanner GUI appears on the screen. **Close** the ad pop-up that appears at the lower end of the GUI.

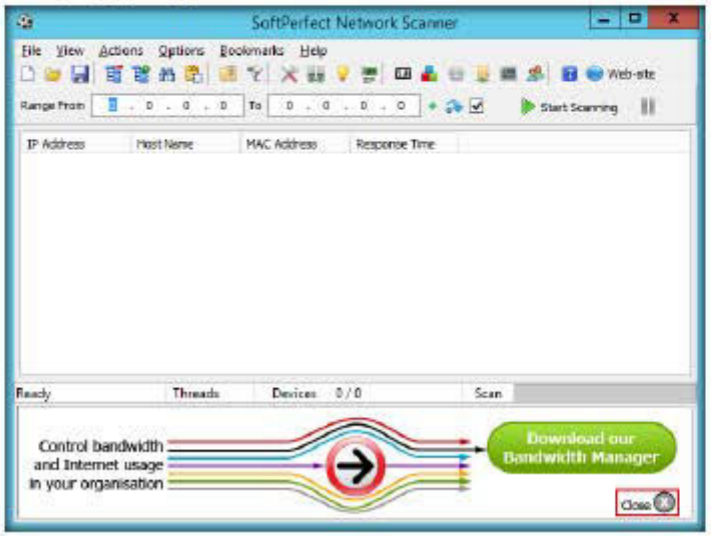


FIGURE 6.2: SoftPerfect Network Scanner main window

5. To start scanning your network, enter an IP range in the **Range 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 D:\CEH-Tools\CEHv9 Module 04 Enumeration

FIGURE 6.3: SoftPerfect setting an IP range to scan

TASK 3

Examine the Enumerated Results

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

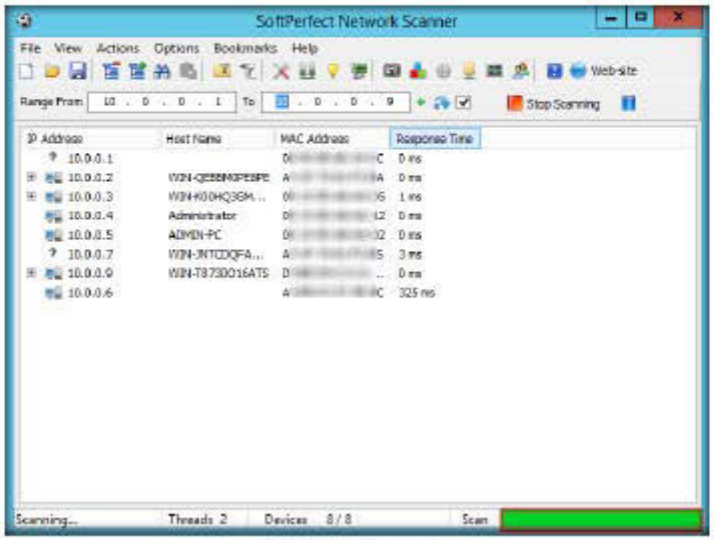


FIGURE 6.4: SoftPerfect status bar

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.

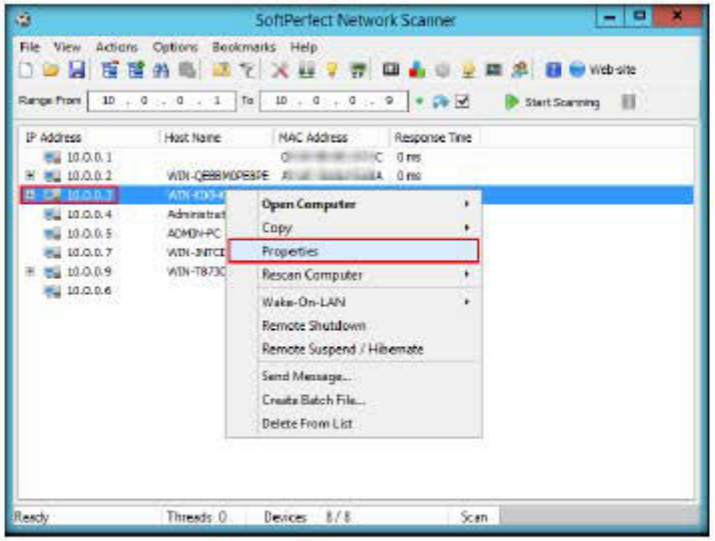


FIGURE 6.5: IP address scanned details

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

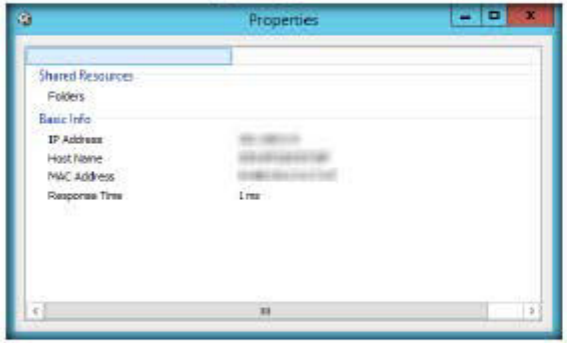


FIGURE 6.6: Properties window

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

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

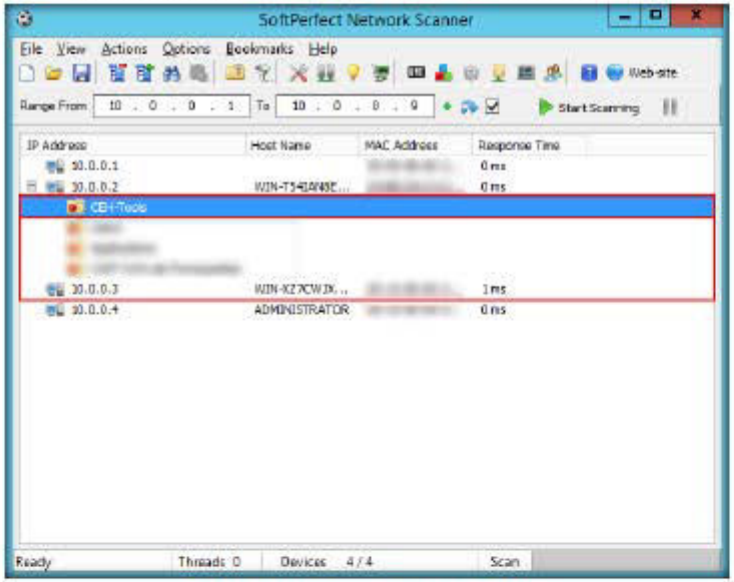


FIGURE 6.7: SoftPerfect Scanner displaying the shared folders

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

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

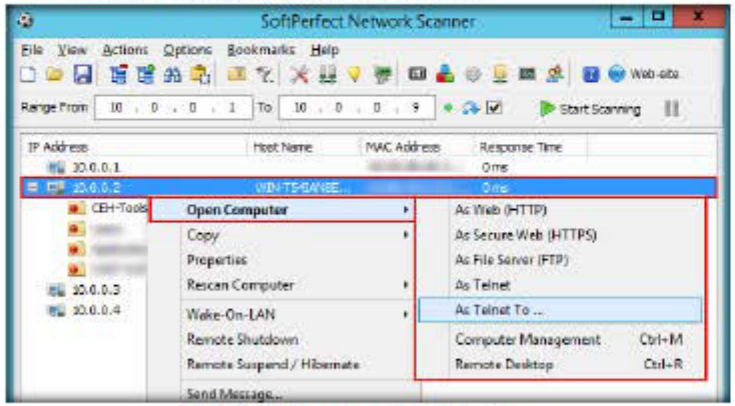


FIGURE 6.8 Various options in SoftPerfect Network Scanner

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.

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

Lab Analysis

Analyze and document the results related to this lab exercise.

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

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

Lab 7

Enumerating a Target Network using Nmap and Net Use

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

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 discus Nmap, it uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, it was designed to rapidly scan large networks. By using the open ports attacker can easily attack the target machine to overcome this type of attacks network 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 **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Scanning Tools\Nmap**
- You can also 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 2008 Virtual Machine
- A computer running with Windows Server 2012 as Host machine
- Administrative privileges to install and run tools

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 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 **nbtstat** scan to find generic **information** (computer names, user names, MAC addresses) on the hosts
- Create a Null Session
- Install and Launch **Nmap** in Windows Server 2012 machine

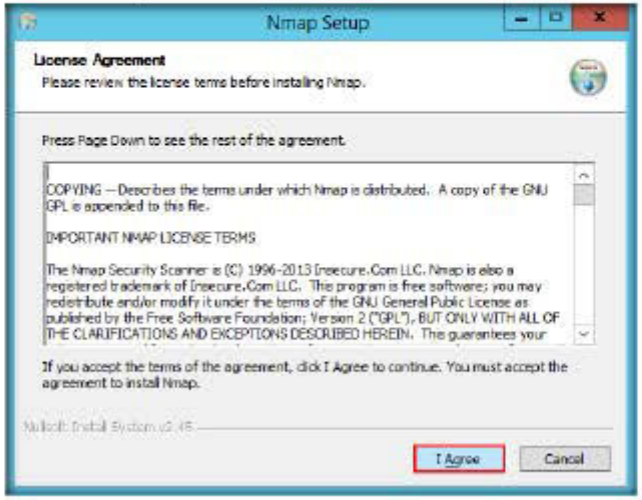
TASK 1

Install Nmap

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

1. Navigate to **D:\CEH-Tools\CEHv9 Module 03 Scanning Networks\Scanning Tools\Nmap** and double-click **nmap-6.40-setup.exe**.
2. If an **Open File - Security Warning** pop-up appears, click **Run**.

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

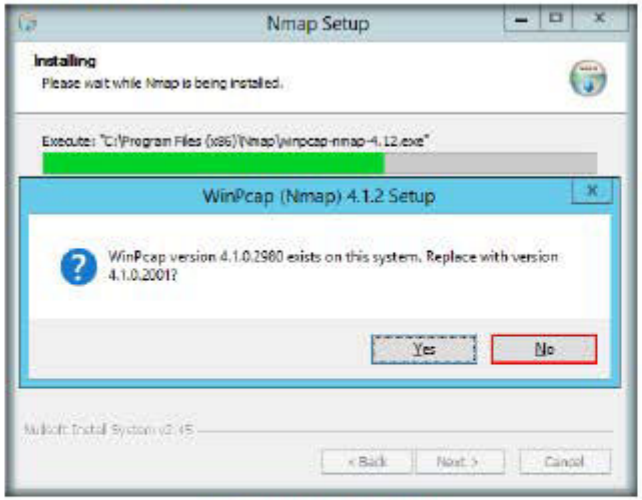


Zenmap file installs the following files:

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

FIGURE 7.1: Nmap Setup window

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



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

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

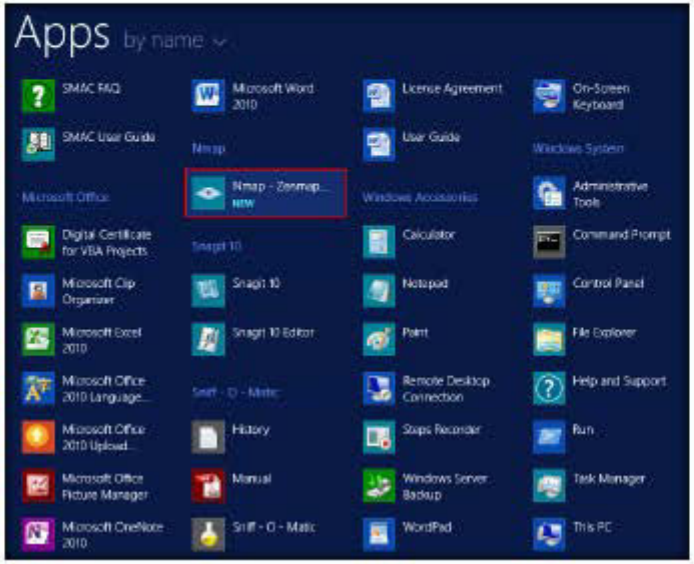


FIGURE 7.3: Windows Server 2012 Apps screen

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

TASK 2

Perform Nmap Scan

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

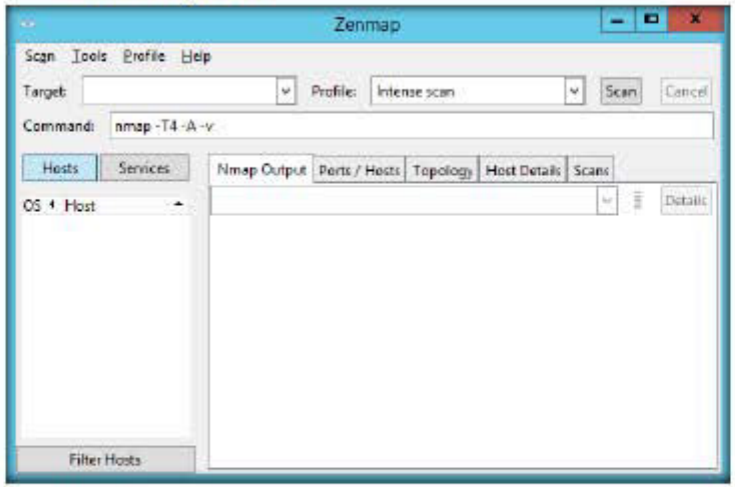


FIGURE 7.4: Nmap/Zenmap main window

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.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

7. Perform the **nmap -O** scan for the **Windows Server 2008** Virtual machine network. This takes few minutes.

Note: IP address of Windows Server 2008 may differ in your lab environment.

Use the –osscan-guess option for best results in nmap.

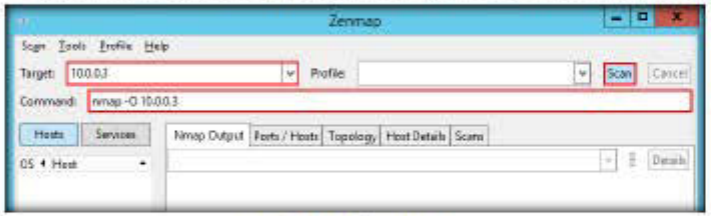


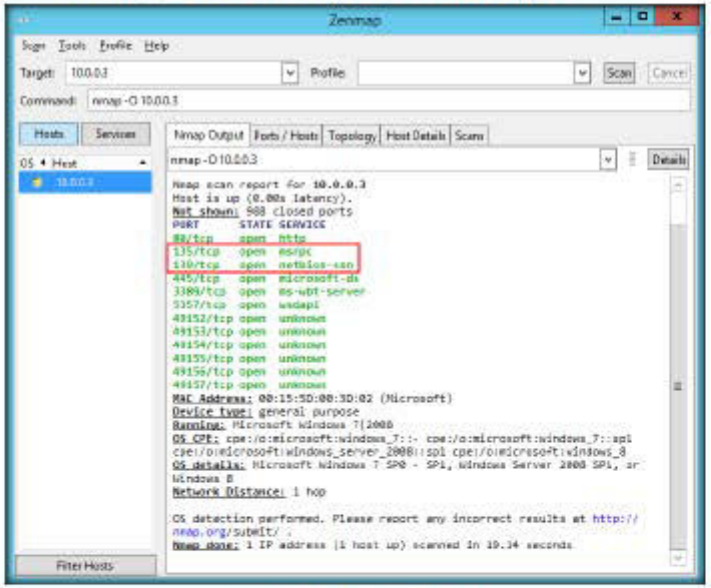
FIGURE 7.5: Configuring Nmap

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

TASK 3

Find Open NetBIOS Ports

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.



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

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 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 **Windows Server 2008** virtual machine, and perform **nbtstat** on port 139 of the target machine.
12. Run the command **nbtstat –A 10.0.0.2**.

Note: **10.0.0.2** is the IP address of **Windows Server 2012** virtual machine. This IP address and result may differ in your lab environment.

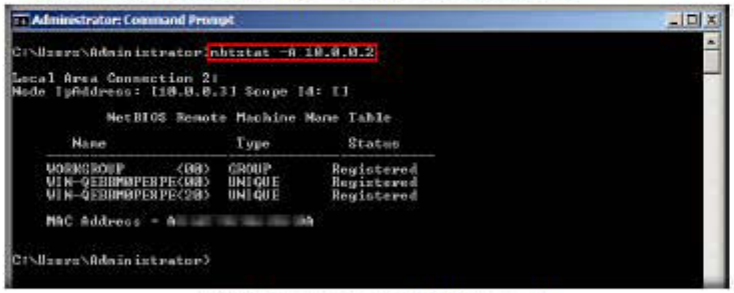


FIGURE 7.7: Command Prompt with the nbtstat command

TASK 4

Create Null Sessions

13. We have not even created a **null session** (an unauthenticated session) yet, and we can still pull down this info.
14. Issue **net use** command to view the created null sessions/shared folders from your host:

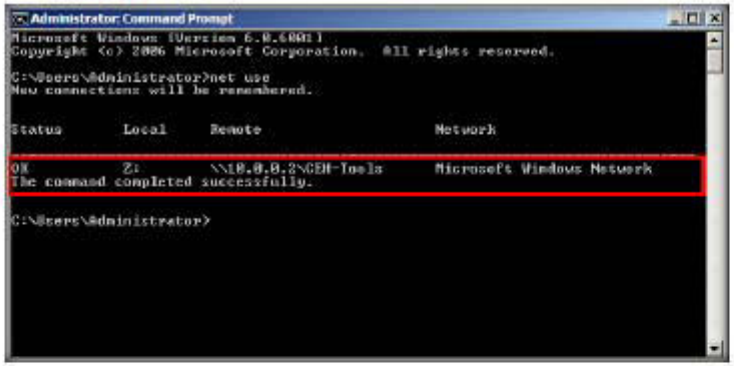


FIGURE 7.8: Command Prompt with the net use command

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

15. Now, issue the command **net use \\X.X.X.X\CEH-Tools ""/user:""** (where **X.X.X.X** is the address of the Host machine from which the folder CEH-Tools has been shared, and there are no spaces between the double quotes).
16. This **creates/ connects** a null session.

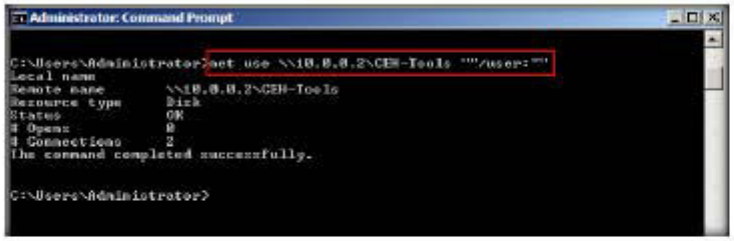


FIGURE 7.9: The command prompt with the net use command

17. **Confirm** it by issuing a generic **net use** command to see connected null sessions from your host.

Net Command

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

18. To confirm, type **net use**, which should list your **newly created** null session.
19. You will observe that a null session has been created on the name of CEH-Tools, as shown in the screenshot:

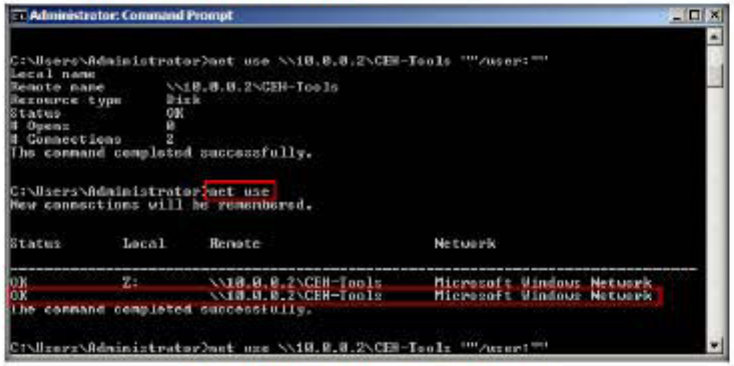


FIGURE 7.10: The command prompt with the net use command

Lab Analysis

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

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

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

Lab 8

Enumerating Services on a Target Machine

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

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 maybe 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 of 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 2012 as Host machine
- Kali Linux running as a virtual machine
- Windows Server 2008 running as a virtual machine

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

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 **Windows Server 2008** virtual machine before running this lab.

TASK 1

Launch Kali Linux Virtual Machine

1. Launch **Kali Linux** virtual machine from Hyper-V Manager 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

TASK 2

Launch nmap

3. Select **Applications → Kali Linux → Top 10 Security Tools → nmap**. This launches the nmap application.

FIGURE 8.2: Launch nmap in Kali Linux

4. 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.

FIGURE 8.3: nmap in Command Terminal

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

TASK 3

Perform Ping Sweep

5. Type **nmap -sP 10.0.0.0/10** and press **Enter** to initiate the ping sweep scan.

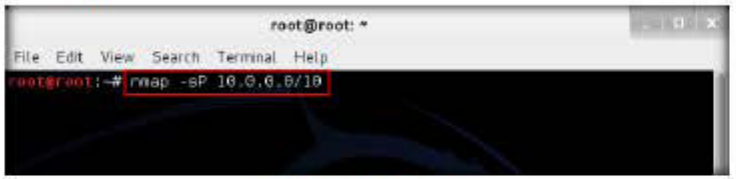


FIGURE 8.4: nmap Ping Sweep scan

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

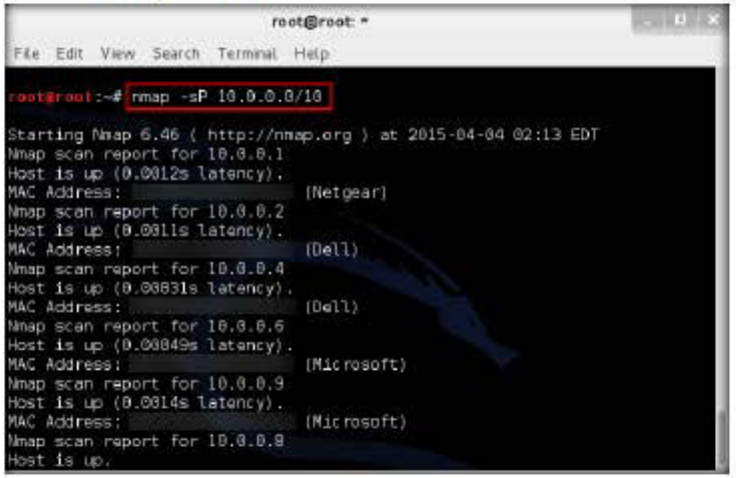


FIGURE 8.5: nmap Ping Sweep scan results

-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.

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

8. Now, choose an IP address from the scan result and perform a **stealthy syn scan**. To do so, type **nmap -sS [IPAddressofTargetMachine]** and press **Enter**. The IP address used in this lab is **10.0.0.6** and this address belongs to **Windows Server 2008**.

Note: The IP address of Windows Server 2008 may differ in your environment.

FIGURE 8.6: nmap Stealthy Syn Scan

9. By issuing this command, a stealthy syn scan will be initiated.
10. Nmap performs stealthy syn scan and lists all the open ports running on Windows Server 2008 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 nowdays. 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.

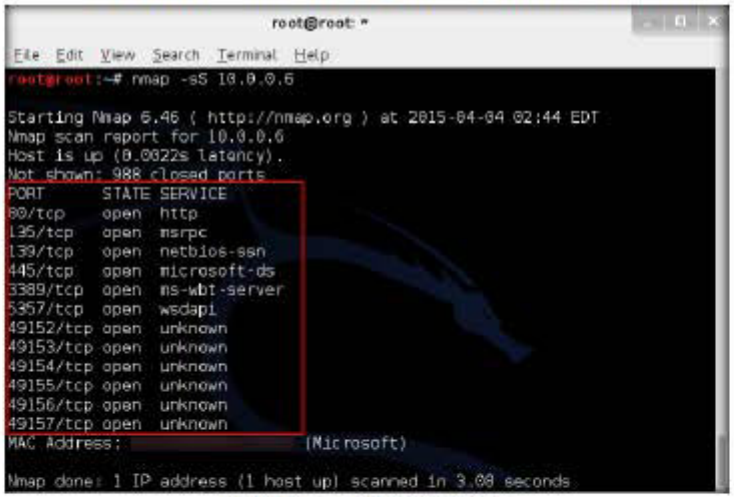


FIGURE 8.7: nmap Stealthy Syn Scan Results

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

TASK 5

Perform Stealthy Syn Scan with Version Detection and OS Detection

12. To enumerate the versions of the obtained services, type the command **nmap -sSV -O [IPAddressofTargetMachine]** and press **Enter**. The IP address used in this lab is **10.0.0.6,** and this address belongs to **Windows Server 2008**.

Note: The IP address of Windows Server 2008 may differ in your lab environment.

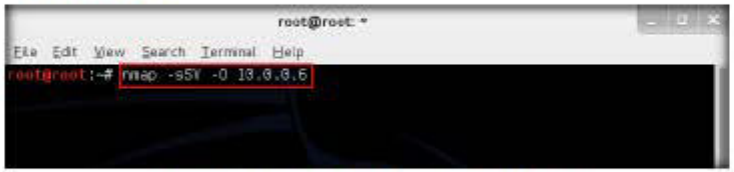


FIGURE 8.8: nmap Stealthy Syn Scan Version Detection and OS Detection

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

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

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.

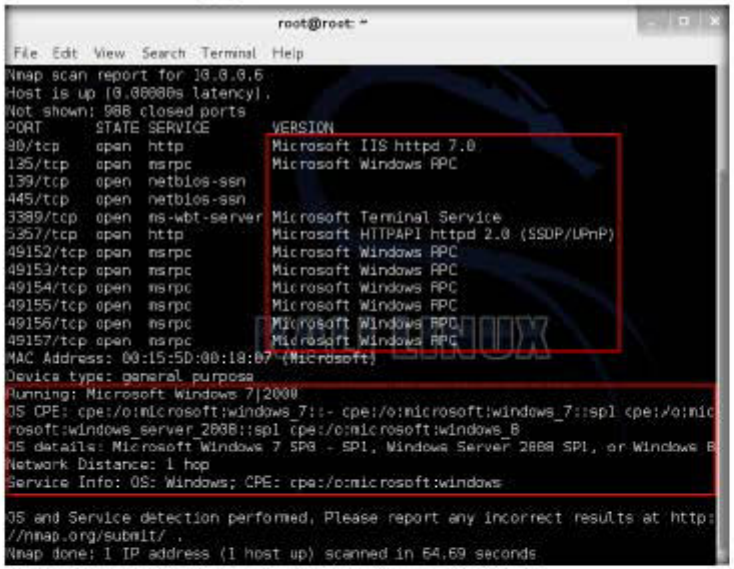


FIGURE 8.9: nmap Stealthy Syn Scan Version Detection and OS Detection Result

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

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

TASK 6

Save the Scan Result

16. Type **nmap -sSV -O [IPAddressofTargetMachine] -oN Enumeration.txt** and press **Enter**. The IP address used in this lab is **10.0.0.6,** which is assigned to **Windows Server 2008**.

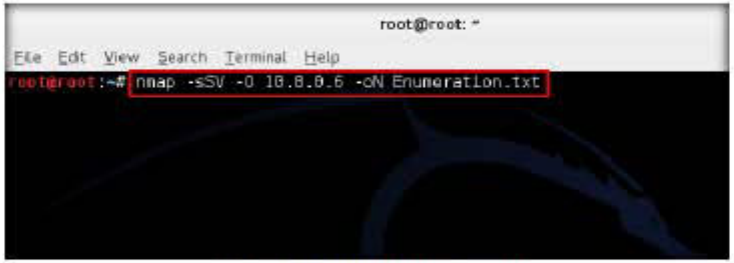


FIGURE 8.10: nmap Saving Stealthy Syn Scan Result

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.

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.

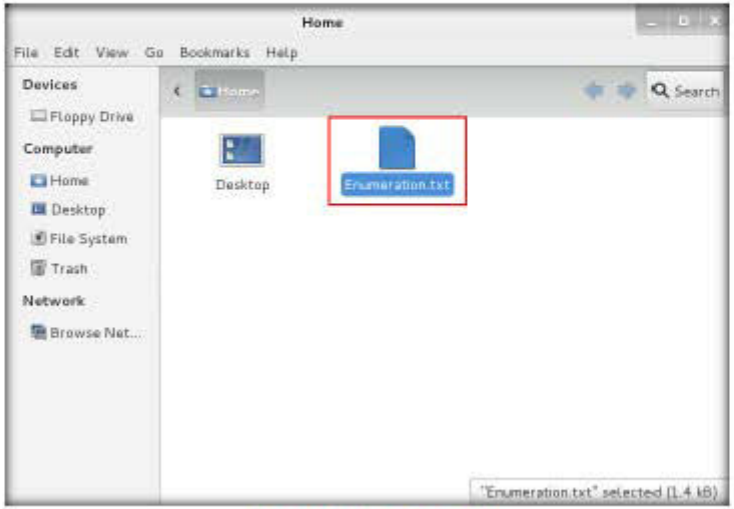


FIGURE 8.12: Stealthy Syn Scan Result File

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

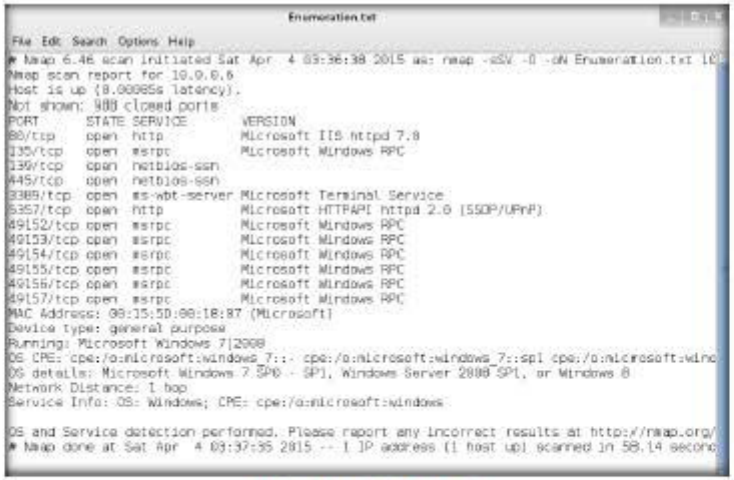


FIGURE 8.13: Stealthy Scan Result

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.

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.

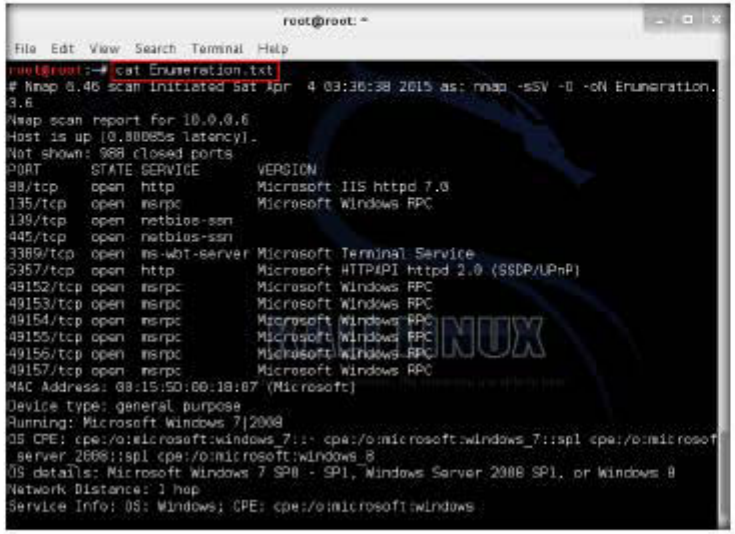


FIGURE 8.14: Stealthy Syn Scan Result viewing by using cat command

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

Lab Analysis

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

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

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

Lab 9

SNMP Enumeration Using SNMPCHECK

snmpcheck permits you to list the SNMP devices and spots the yield in an extremely comprehensible cordial arrangement. It could be valuable for entrance testing or frameworks checking. Conveyed under GPL permit and taking into account the "Athena-2k" script by jshaw.

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:

- A computer running with Windows Server 2012 as Host machine
- Kali Linux running as a virtual machine (Attacker Machine)
- Windows Server 2008 as a virtual machine (Victim Machine)
- An 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 2008** machine, with IP address **10.0.0.10**.

   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.

FIGURE 9.1: Performing nmap UDP scan

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

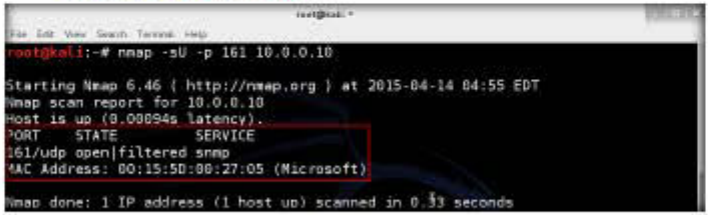


FIGURE 9.2: nmap UDP scan result

TASK 2

Find SNMP Community String

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

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.

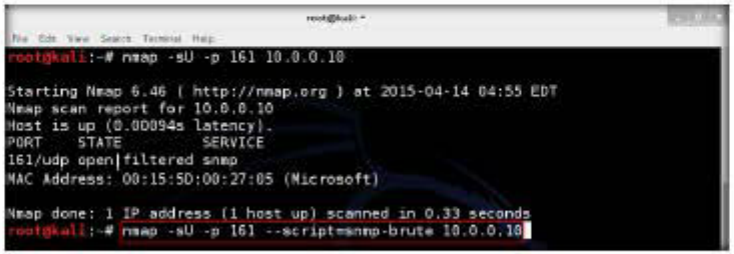


FIGURE 9.3: nmap finding SNMP community string

8. The script output will display as shown in the screenshot. Now the extracted SNMP port is used by the public (community string) and with valid credentials.

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

9. If the target machine doesn't have a valid account, no output will display.

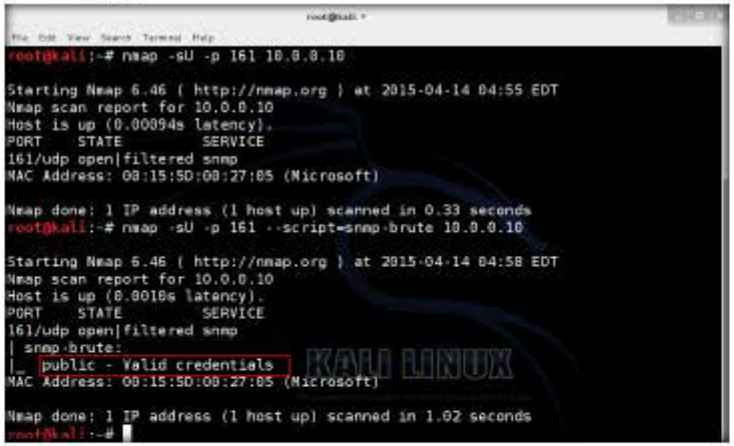


FIGURE 9.4: SNMP Community String found with Valid Credentials

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

10. Now perform SNMP enumeration on the target machine: in a command-line terminal, type **snmpcheck** and press **Enter** to display snmpcheck commands and their uses.

11. **snmpcheck** is a tool that allows you to enumerate the SNMP devices, placing the output in a simple format.
12. **snmpcheck** can be mainly used for penetration testing or for systems monitoring purposes.

snmpcheck should not be used against machines you do not own or administrator. This tool might create IDS warnings. The author can't be held responsible for the use and/or misuse of this program.

FIGURE 9.5: snmpcheck commands list

TASK 3

Enumerate Community String

13. Type **snmpcheck -t <Target machine IP Address> -c <community string> | more** and press **Enter**.
14. Here, the **-t** switch is to set Target host and the **-c** switch is the SNMP community.

FIGURE 9.6: Enumerating Community String using snmpcheck

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

snmpcheck enumerated System Information.

17. If you want to view more information enumerated by snmpcheck, press **Enter**.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

18. In the screenshot, you can see the **More** option is highlighted to view additional system information.

The managed devices records information and by use of the deployed agent communicate with the overarching Network Management System.

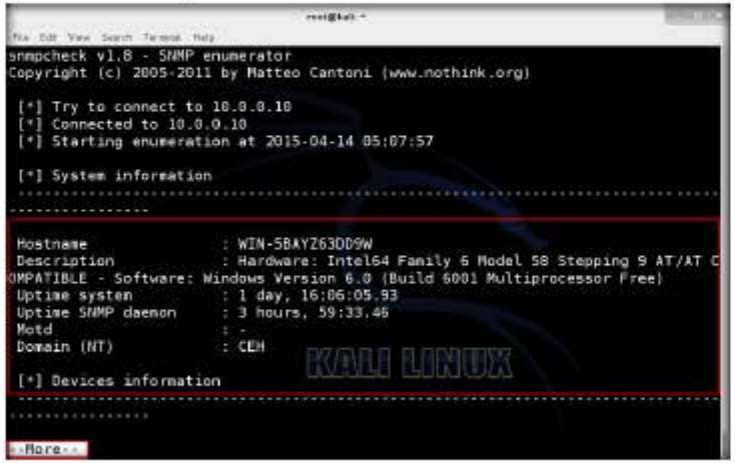


FIGURE 9.7: snmpcheck enumerated System Information

19. The following screenshot shows the information for all devices connected to the network.

snmpcheck extracted the device information for everything connected to the Target machine.

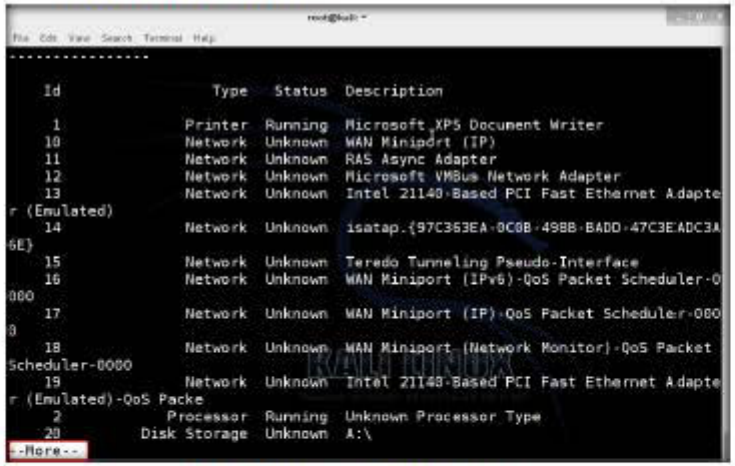


FIGURE 9.8: snmpcheck enumerated Devices Information

20. **Storage Information** displays the target-machine drive data, as shown in the screenshots.

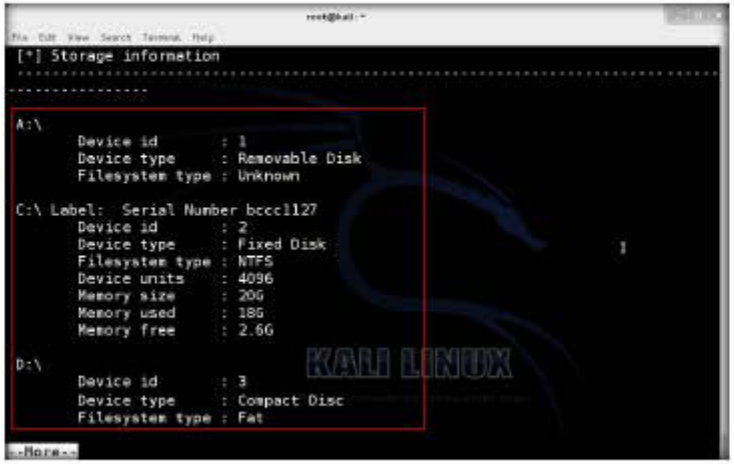


FIGURE 9.9: snmpcheck enumerated Storage Information

SNMP is dangerous as it is a clear text protocol and as such could potentially provide valuable information to an attacker.

21. Press **Enter** to view **More** information about the enumerated system.

Lab Analysis

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

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

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

Lab

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

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

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

Lab Objectives

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

- User names and user groups
- Attributes

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 04 Enumeration

To perform this lab, you will need:

- Active Directory Explorer located at **D:\CEH-Tools\CEHv9 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer**
- You can also 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 Windows Server 2008 Virtual Machine
- A computer running with Windows Server 2012 as Host 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 Active Directory Domain system
- Modifying Domain User Accounts

TASK 1

Launch ADExplorer

1. Now switch to Windows Server 2012 machine and navigate to **D:\CEH-Tools\CEHv9 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer**, and double-click **ADExplorer.exe**.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

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

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

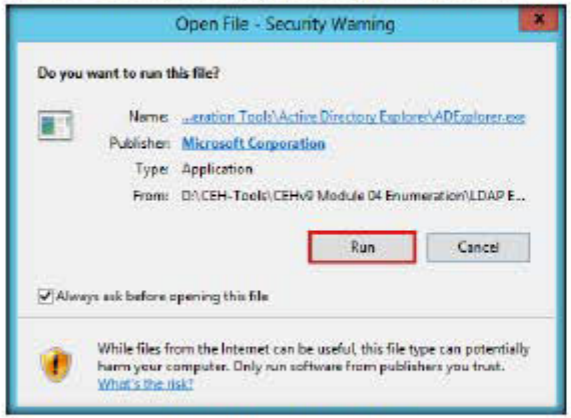


FIGURE 10.1: Open File – Security Warning

TASK 2

Connect to Active Directory Machine

3. The Connect to Active Directory pop-up appears; type the IP address of Windows Server 2008 IP (**10.0.0.10**) and click **OK**.

Note: IP Addresses may differ in your lab environment.

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

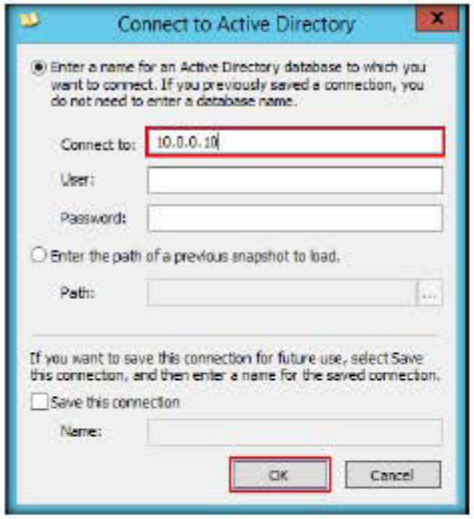


FIGURE 10.2: ADExplorer Connect to Active Directory

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

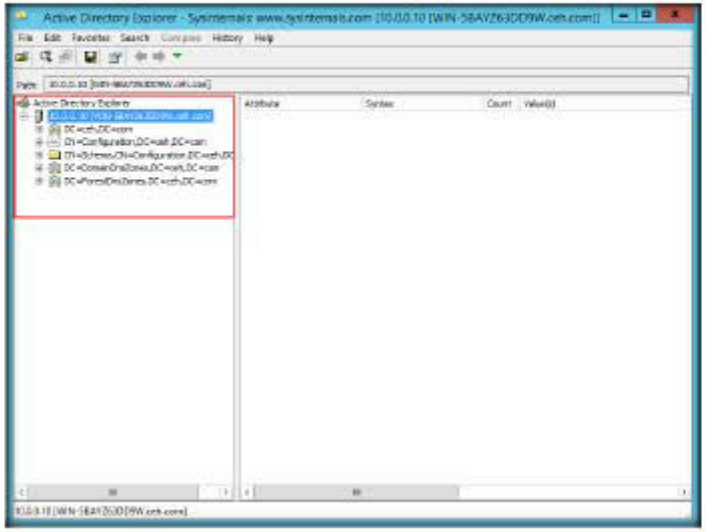
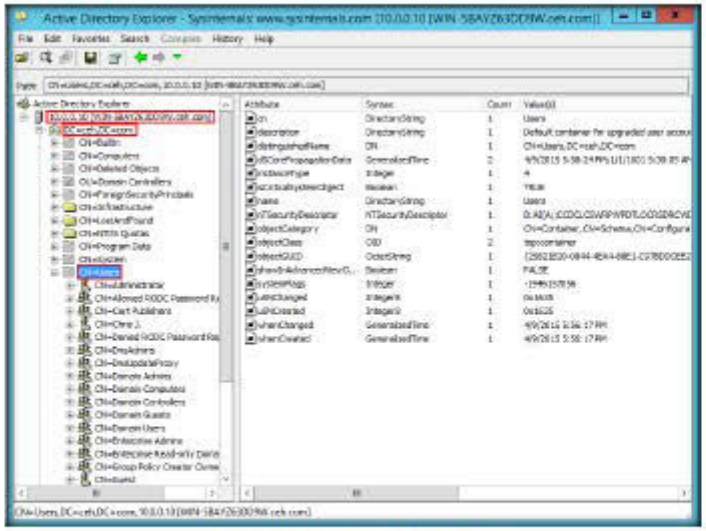


FIGURE 10.3: ADExplorer Main Window

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv9 Module 04 Enumeration

5. 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: ADExplorer Domain Users Node

6. 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.

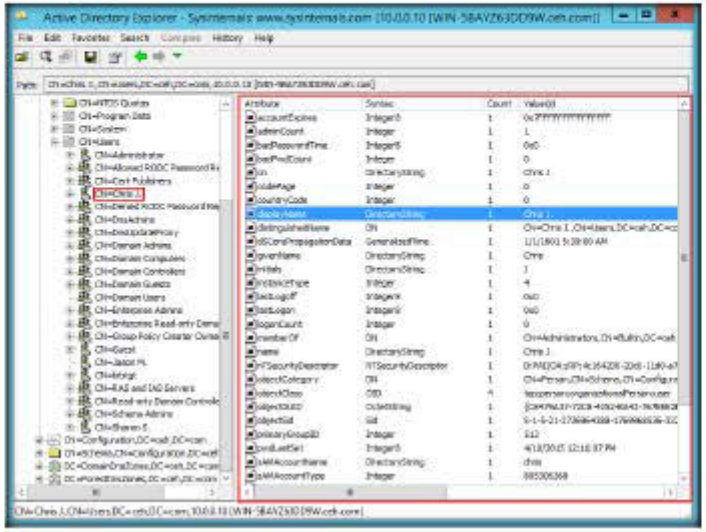


FIGURE 10.5: ADExplorer Domain Users Profile Attributes

TASK 3

Modifying User Attributes

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

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).

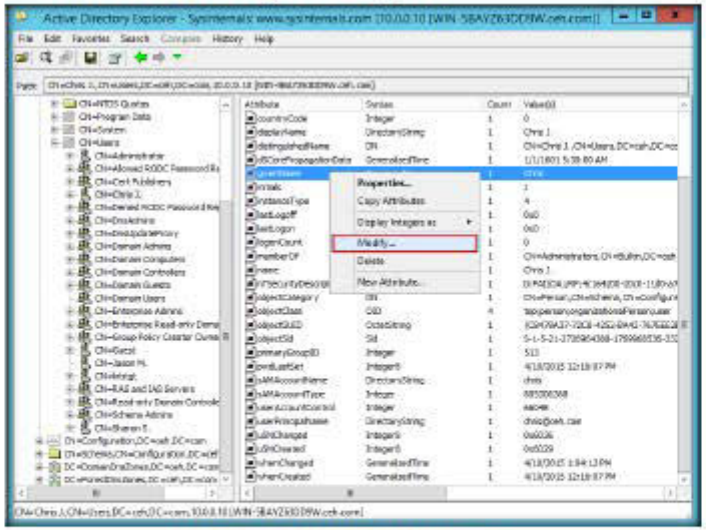


FIGURE 10.6: ADExplorer User Profile Modification

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

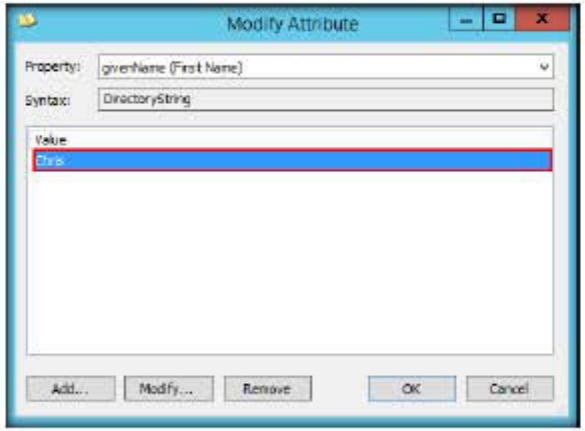


FIGURE 10.7: Modifying Attributes

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

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

Lab Analysis

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

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

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

Lab 11

Performing Network Enumeration Using Various DNS Interrogation Tools

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

Attackers enforce various DNS enumeration techniques like Zone Transfer, Domain and Host Brute-Force, and Cache Snooping to obtain information associated with DNS servers and network infrastructure of organizations.

As an ethical hacker or an information security officer, you need to compromise the network information using DNS enumeration techniques; and then implement DNS enumeration countermeasures for data protection.

Lab Objectives

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

- Extract Whois information

Lab Environment

To complete this lab, you will need:

- A computer running with Windows Server 2012 as Host machine
- Kali Linux running as a virtual machine
- An active website

Lab Duration

Time: 15 Minutes

Overview of Enumeration

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

Lab Tasks

TASK 1

Launch Kali Linux Virtual Machine

1. Launch **Kali Linux** virtual machine from Hyper-V Manager, and log into it (Username: **root**; Password: **toor**).
2. The Kali Linux **Desktop** appears, as shown in the following screenshot:

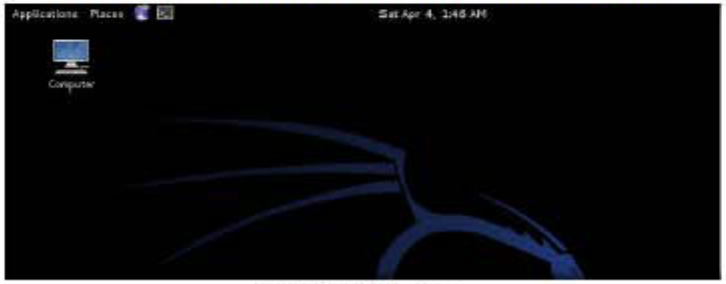


FIGURE 11.1: Kali Linux Machine

TASK 2

Launch Command Line Terminal

3. Select **Applications** → **Accessories** → **Terminal** to launch the command-line terminal.
4. Alternatively, you can click the Command Line Terminal icon, located in the taskbar.

FIGURE 11.2: Launching Command Terminal

TASK 3

Enumerate Whois Information

5. The target used in this lab is www.certifiedhacker.com; its corresponding domain name is certifiedhacker.com.
6. Type **whois certifiedhacker.com** in the command-line terminal, and press **Enter**

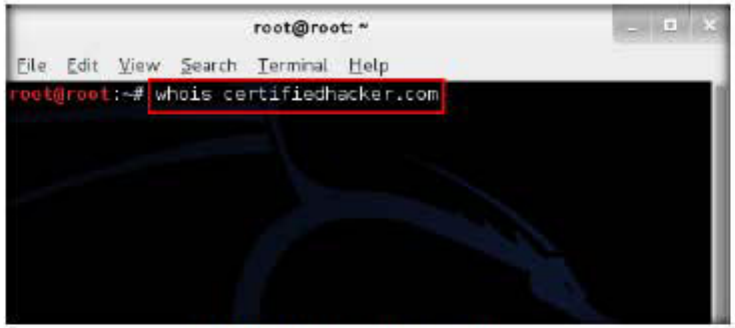


FIGURE 11.3: Whois information of certifiedhacker.com

7. This returns whois-related information from the certifiedhacker.com domain.

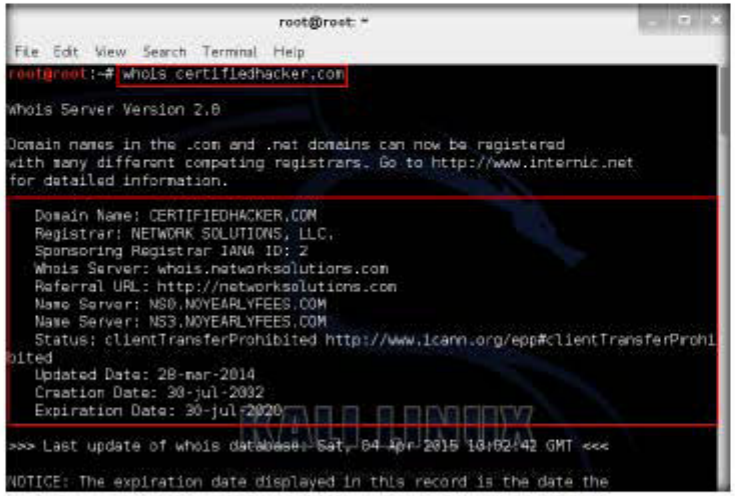


FIGURE 11.4: Whois information result of certifiedhacker.com

The usage of the 'whois' varies widely from system to system, but nevertheless a common ground is established where you have you give the IP address after the command.

HaCkRhInO-TeaM !
Y0uR SeCuiTy iS N0t En0Ugh
wE FrEE t0 FlY
HaCkRhInO-TeaM !

8. Scroll down the terminal window to view the registrar-related information:

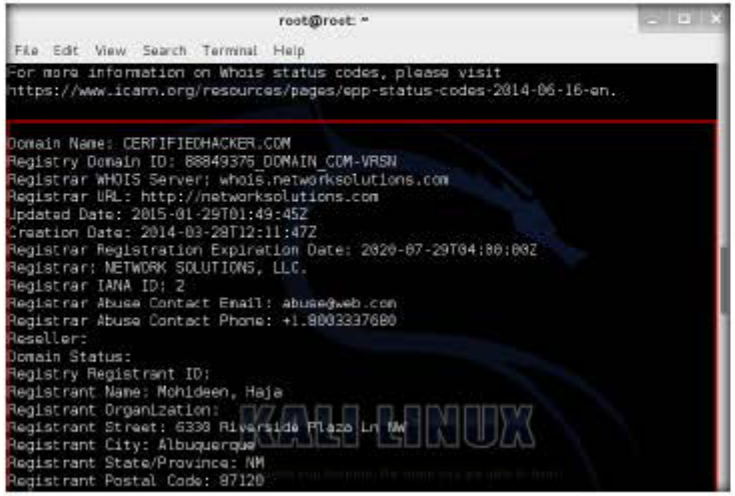


FIGURE 11.5: Registration Information of Certifiedhacker.com

TASK 4

Enumerate IP Addresses

9. Type **host www.certifiedhacker.com** to enumerate the IP addresses of www.certifiedhacker.com website.

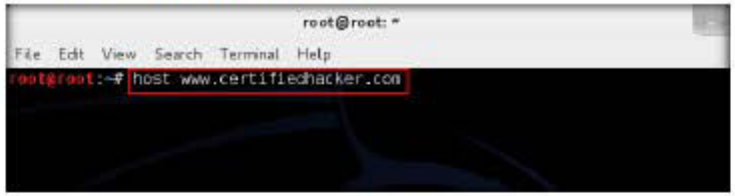


FIGURE 11.6: Host command to find IP address

10. You will be provided with all IP addresses associated with the target website, as shown in the following screenshot:

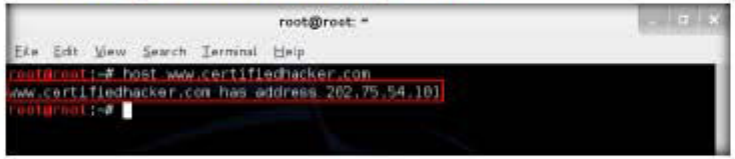


FIGURE 11.7: IP address of the Target

TASK 5

Enumerate DNS Records Using host

11. Type **host -a certifiedhacker.com** and press **Enter** to display DNS records associated with the website, as shown in the screenshot:

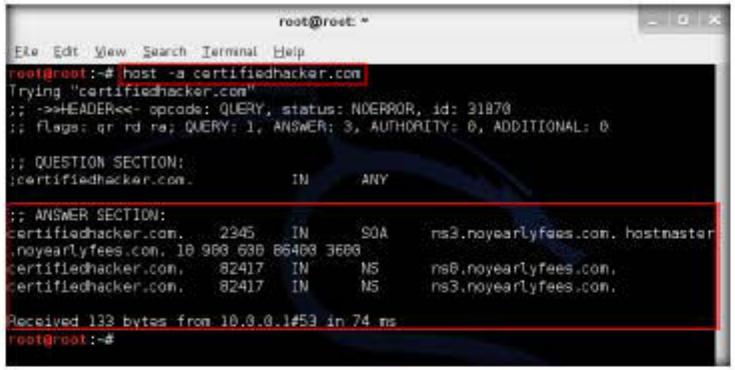


FIGURE 11.8: DNS records of the Target

TASK 6

Enumerate DNS Records Using dnsenum

12. Type **dnsenum certifiedhacker.com** and press **Enter** to display the IP address, name servers, mail servers, and others related to the website, as shown in the screenshot:

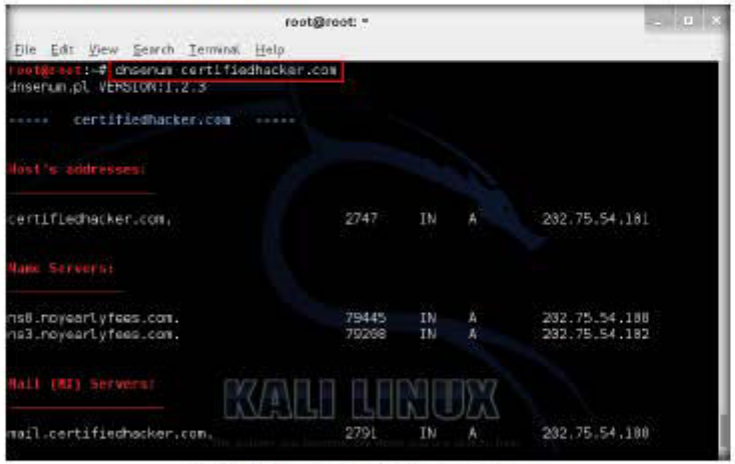


FIGURE 11.9: Enumerating DNS Records using dnsenum

13. dnsenum also tries to perform zone transfers for the domain on its associated nameservers, in an attempt to obtain subdomains, as shown in the screenshot:

This List of DNS record types provides an overview of types of resource records (database records) stored in the zone files of the domain name system (DNS).

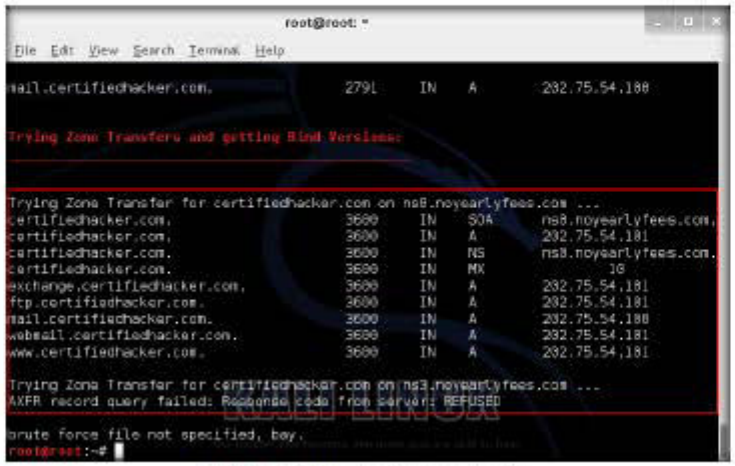


FIGURE 11.10: dnsenum performing zone transfers

The DNS implements a distributed, hierarchical, and redundant database for information associated with Internet domain names and addresses. In these domain servers, different record types are used for different purposes.

14. In case a zone transfer fails, you could brute-force an attack on the target website by issuing the command **dnsenum -f /usr/share/dnsenum/dns.txt [domain name of the target website]** and pressing Enter. In this lab, the target domain is **certifiedhacker.com**.

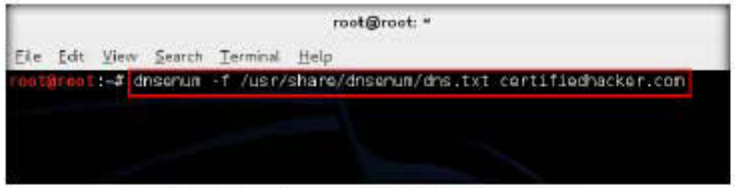


FIGURE 11.11: Performing brute-forcing on target using dnsenum

15. dnsenum attempts brute-forcing on the website to extract its subdomain, class c IP addresses, and so on associated with the website.

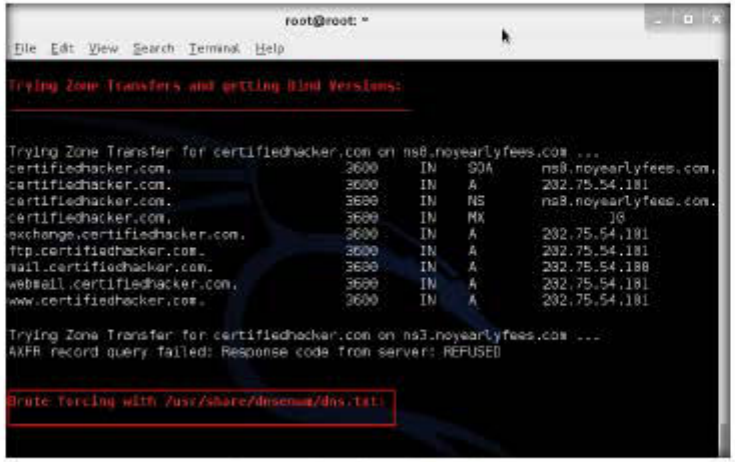


FIGURE 11.12 Brute-force results using dnsenum

TASK 7

Enumerate DNS Records Using dnsdict

16. Type the command **dnsdict6 -d -4 certifiedhacker.com** and press **Enter**.
17. This:
    a. Enumerates the subdomains in certifiedhacker.com associated with IPv4 addresses
    b. Obtains dns-related information, as shown in the screenshot:

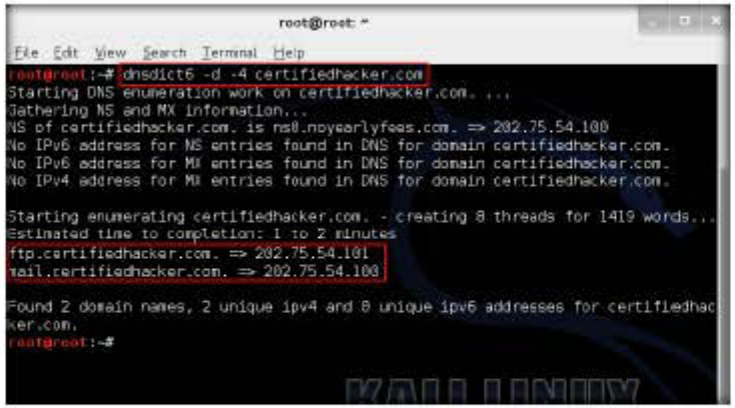


FIGURE 11.13: dnsdict – enumerating subdomains in target

TASK 8

Enumerate DNS Records Using fierce

18. Type **fierce -dns certifiedhacker.com** and press **Enter**. This enumerates the name server related information, along with subdomains associated with the website, as shown in the screenshot:

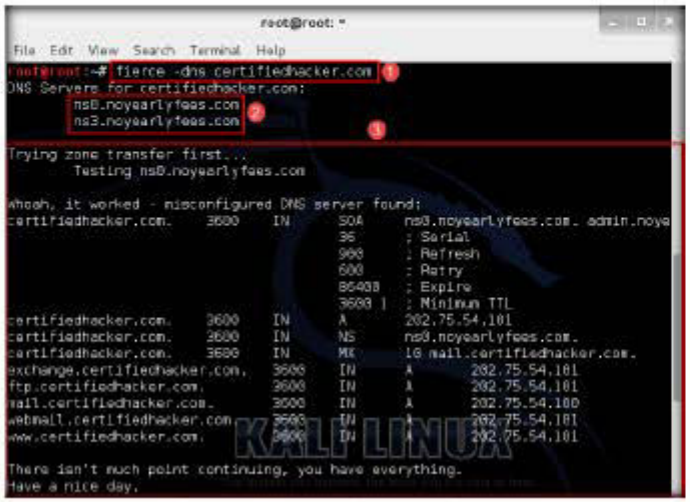


FIGURE 11.14: Fierce command to enumerate the name server

Lab Analysis

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

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

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