

## **CEH Lab Manual**

---

# **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

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 \(ADEExplorer\)](#)
- 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.

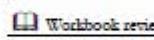
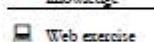
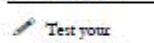
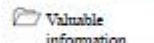
PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS  
RELATED TO THIS LAB.



## 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



### 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/](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.



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.

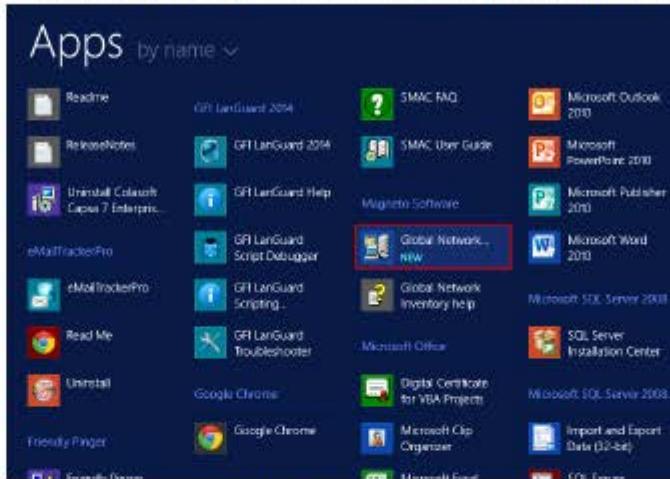


FIGURE 1.2 Windows Server 2012 Apps screen

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

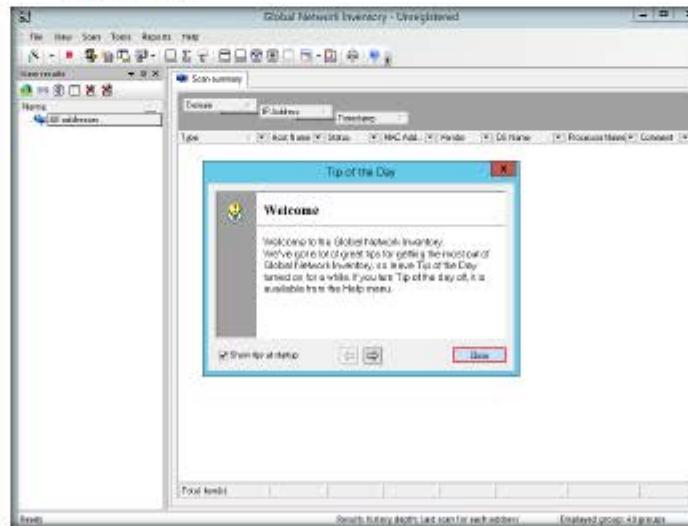


FIGURE 1.3 Global Network Inventory main window

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

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

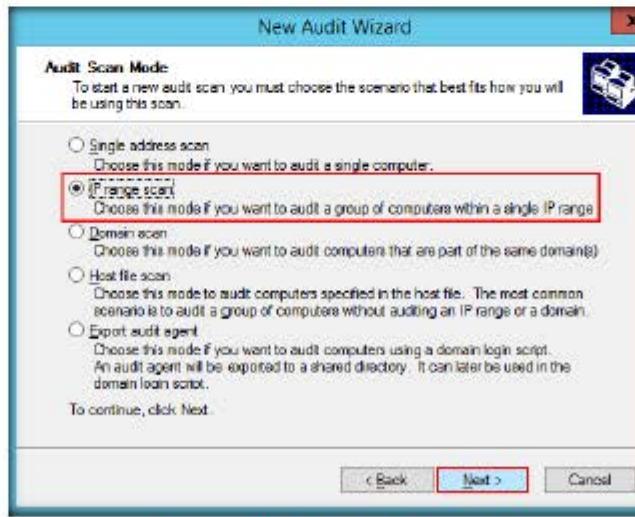


FIGURE 1.5 Global Network Inventory Audit Scan Mode section

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

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



FIGURE 1.6 Setting an IP range to scan

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

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

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

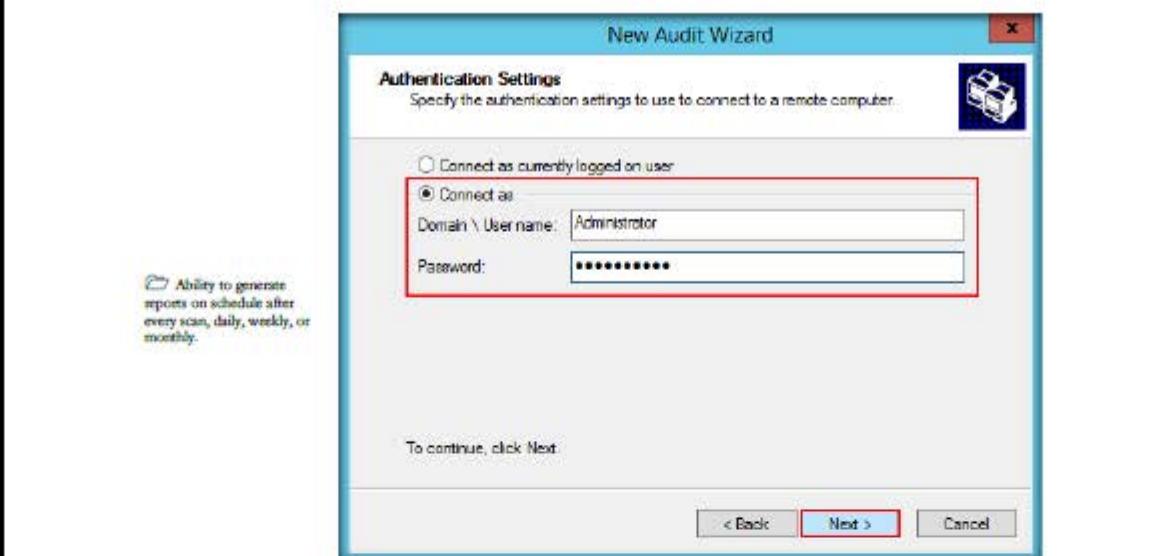


FIGURE 1.7: Global Network Inventory Authentication settings

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



FIGURE 1.8: Global Network Inventory final Audit wizard

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

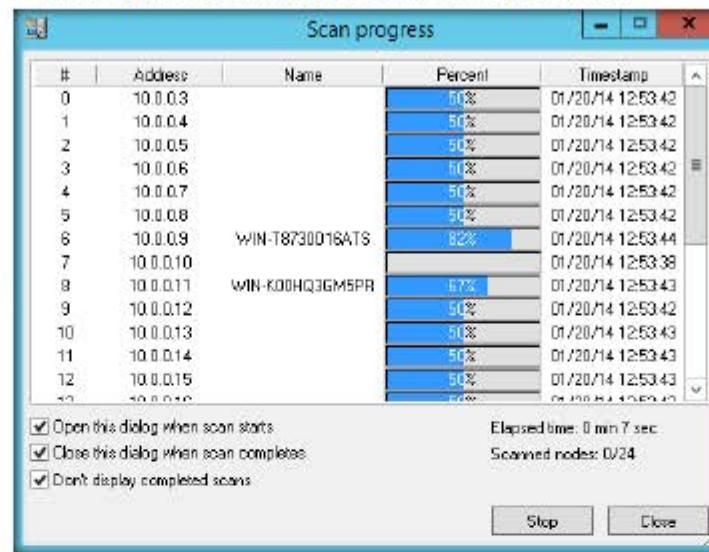


FIGURE 1.9: Global Network Inventory Scanning Progress

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

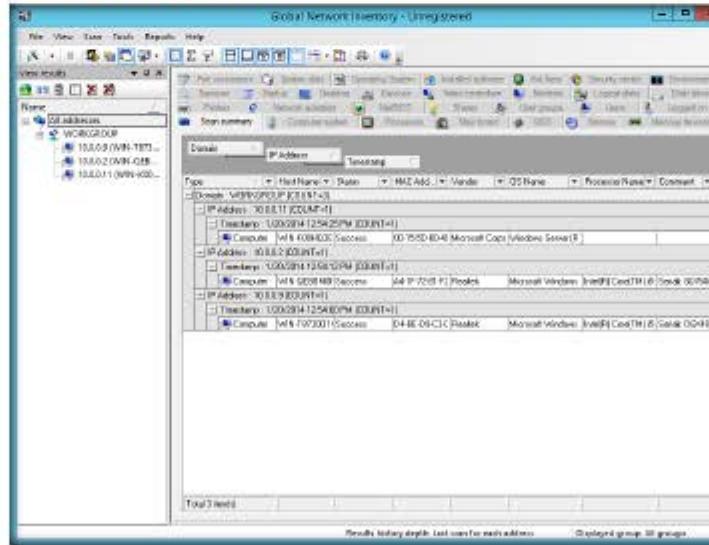


FIGURE 1.10: Global Network Inventory result window

**TASK 3****Examine the Scanned Machine**

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

14. Now select the IP address of **Windows Server 2008 (10.0.0.11)** virtual machine in the left pane, under View results, to view individual results.

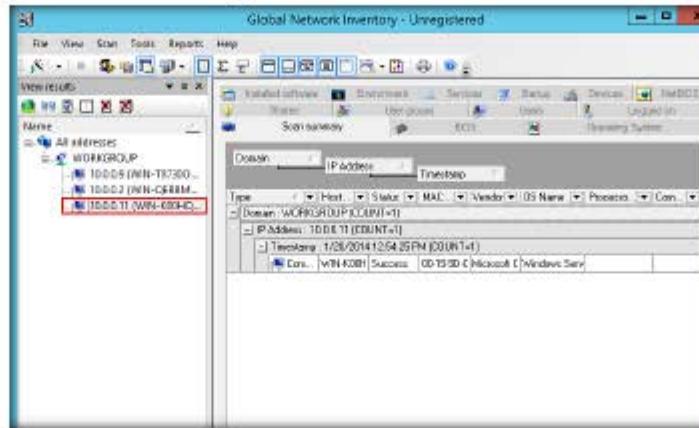


FIGURE L11: Global Network Inventory Individual machine results

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

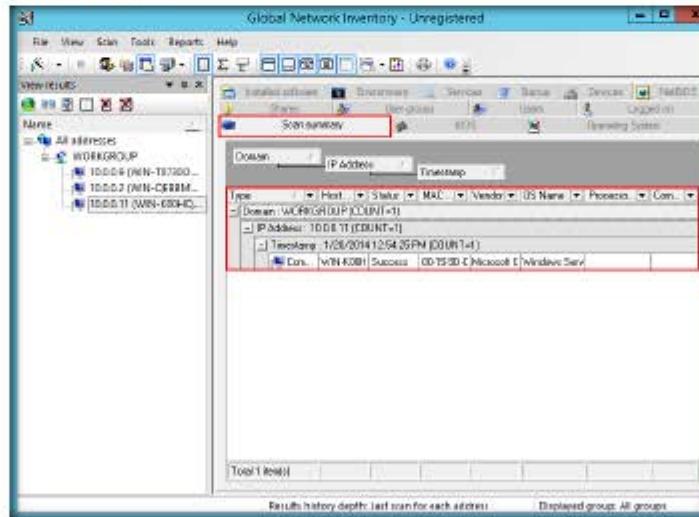


FIGURE L12: Global Inventory Scan Summary tab

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

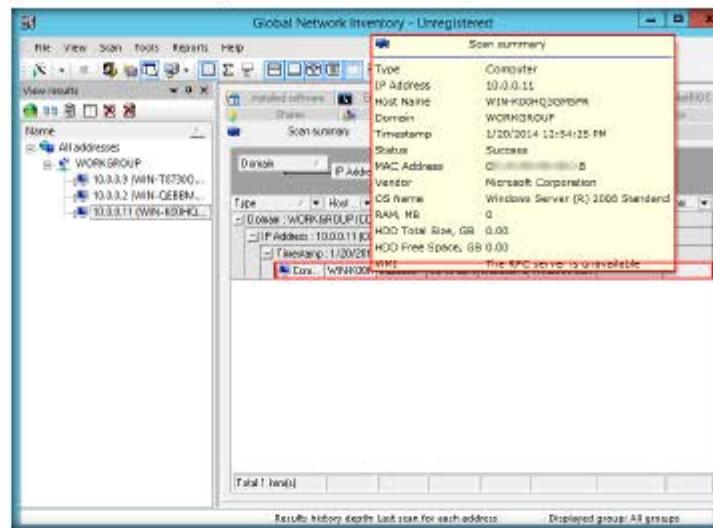


FIGURE 1.13: Global Inventory displaying the Scan summary

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

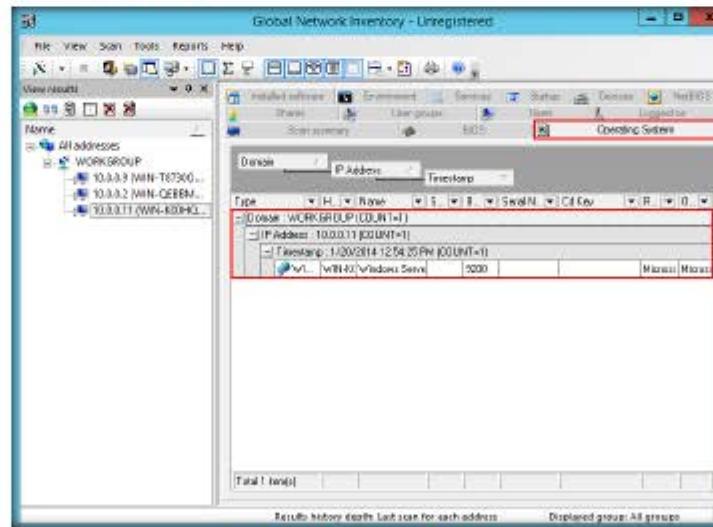


FIGURE 1.14: Global Inventory Operating System tab

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

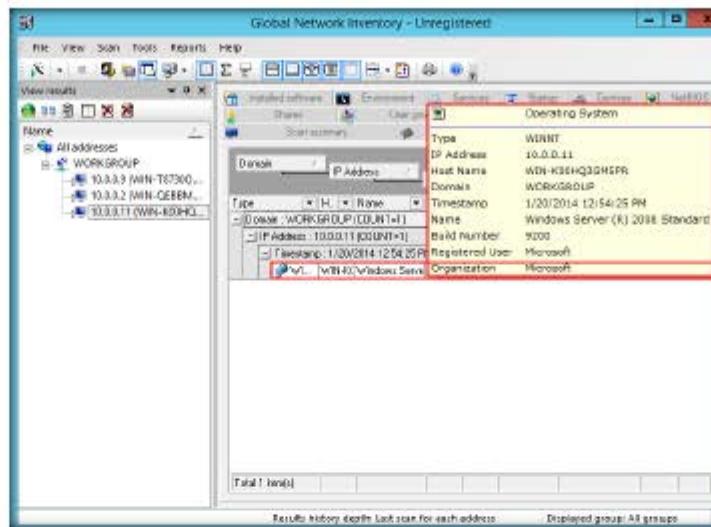


FIGURE 1.15: Global Inventory displaying the operating system details

19. The Bios section gives details of Bios settings.

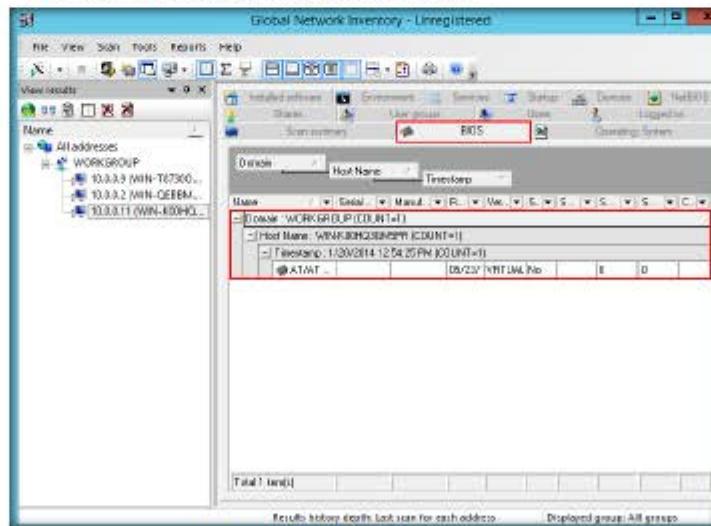


FIGURE 1.16: Global Network Inventory Bios summary tab

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

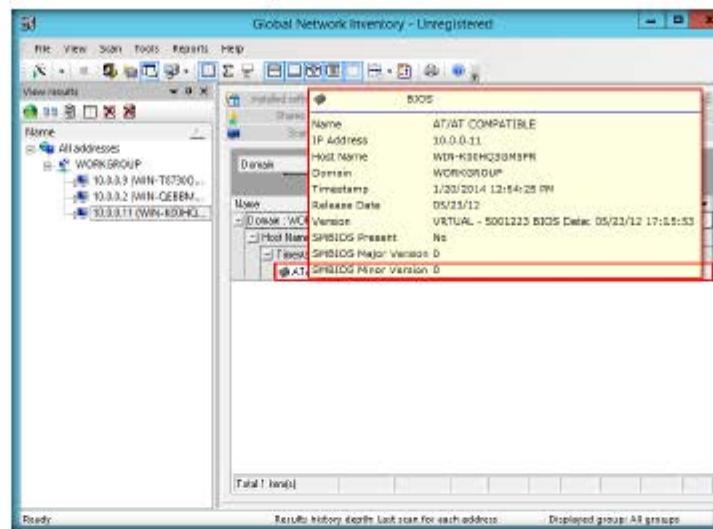


FIGURE L17: Global Network Inventory displaying the Bios summary information

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

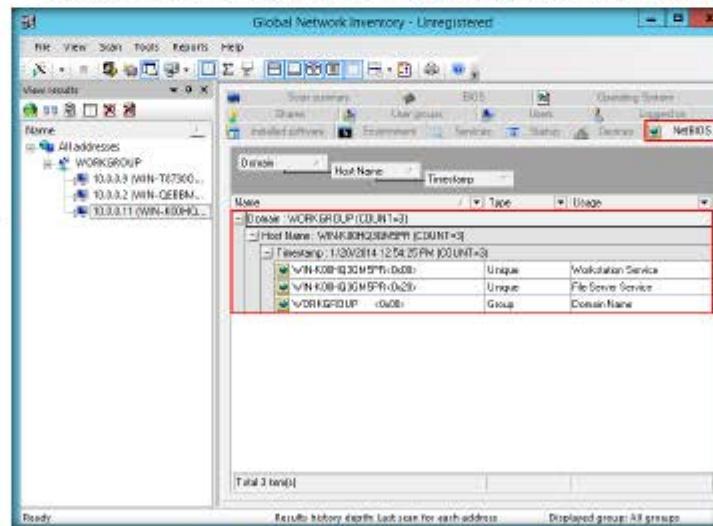


FIGURE L18: Global Network Inventory NetBIOS tab

22. Click each NetBIOS application to view its details.

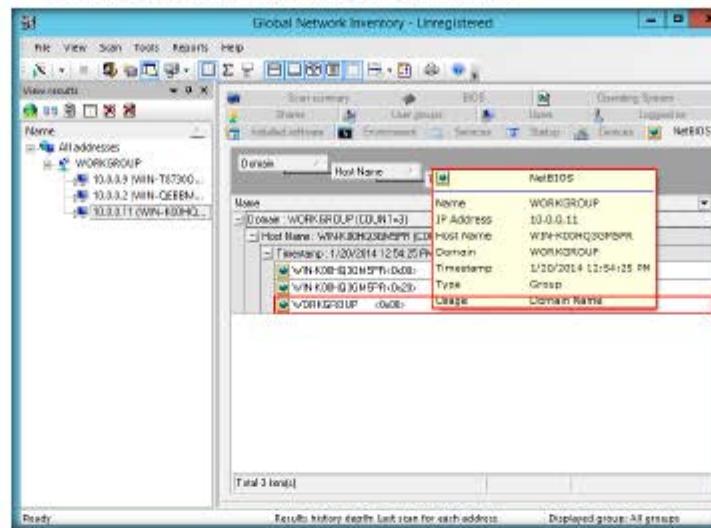


FIGURE 119: Global Network Inventory displaying the NetBIOS information

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

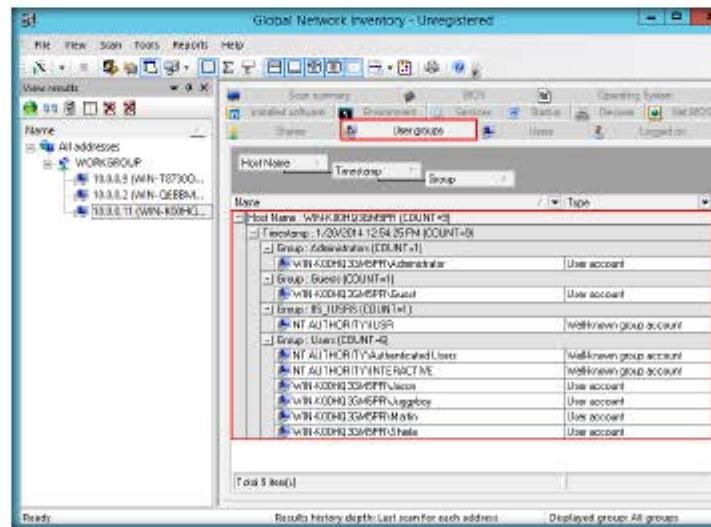


FIGURE 120: Global Network Inventory User groups tab

HaCkRhInO-TeaM !

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

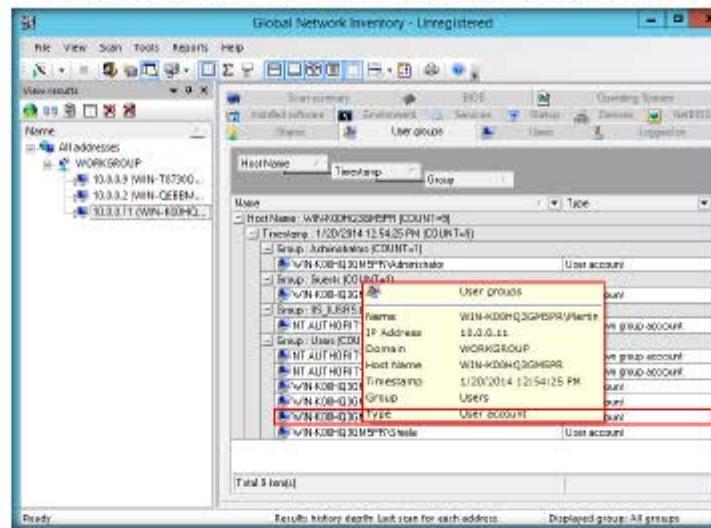


FIGURE 1.21: Global Network Inventory displaying the User groups information

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

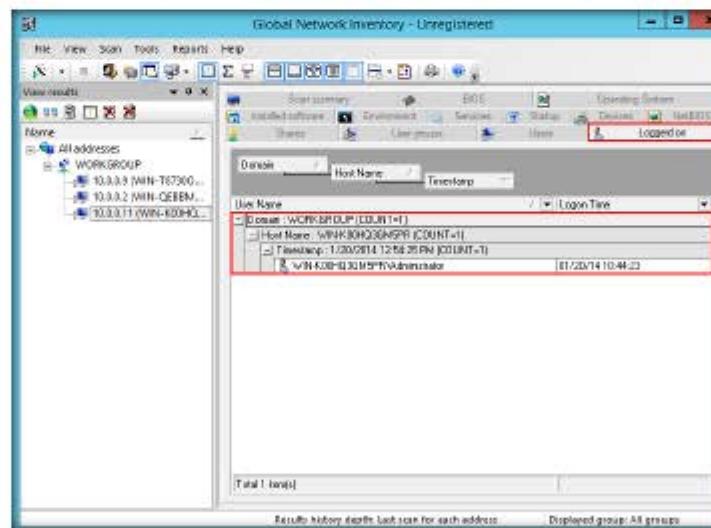


FIGURE 1.22: Global Network Inventory Logged on telnet

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

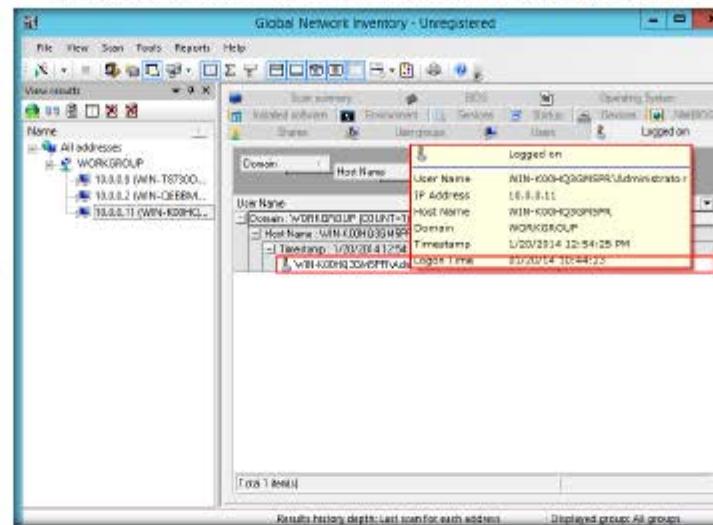


FIGURE 1.23: Global Network Inventory displaying the Logged on information

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

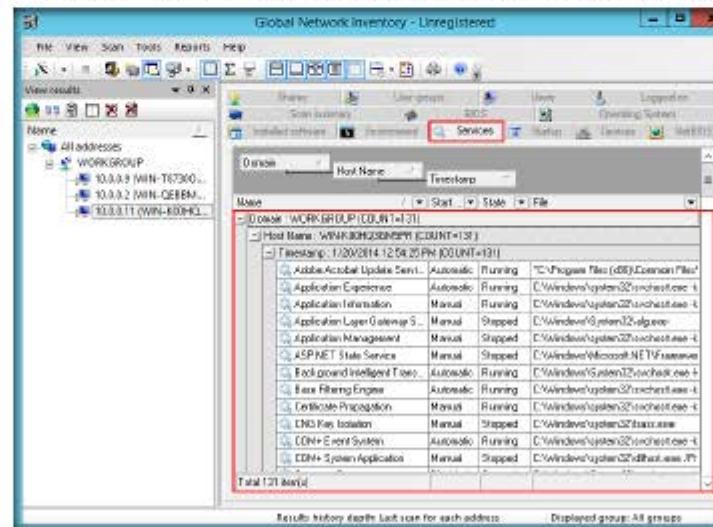


FIGURE 1.24: Global Network Inventory Services tab

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

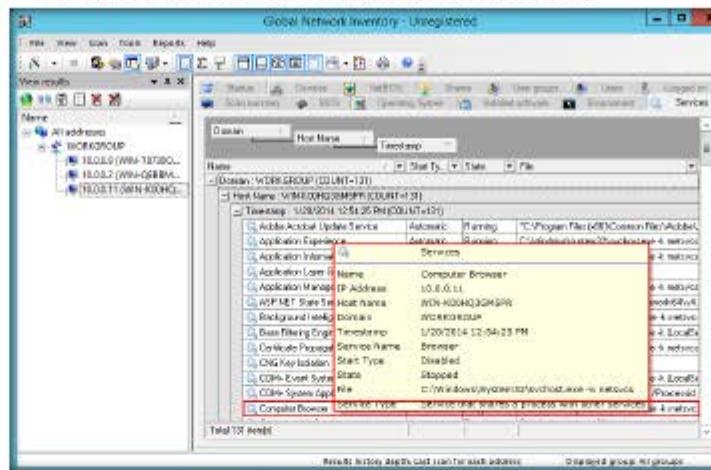


FIGURE 1.25: Global Network Inventory displaying the Services information

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

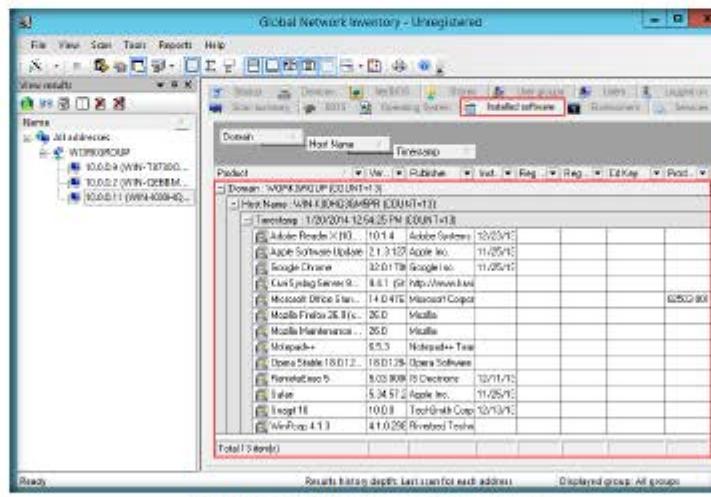


FIGURE 1.26: Global Network Inventory Network Adapter tab

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.

30. Hover over software names to view their details.

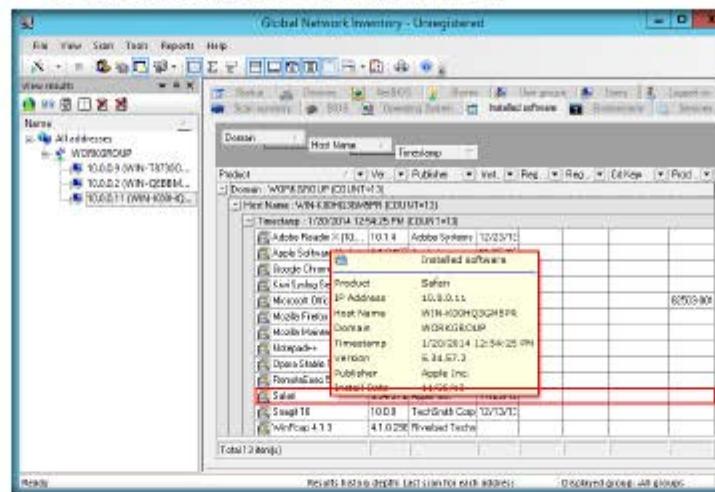


FIGURE 1.27: Global Network Inventory displaying the Network Adapter information

## Lab Analysis

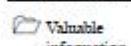
Document all the IP addresses, open ports and running applications, and protocols you discovered during this lab.

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

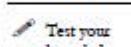
<b>Internet Connection Required</b>	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
<b>Platform Supported</b>	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



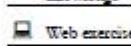
## Enumerating Network Resources Using Advanced IP Scanner

**ICON KEY**

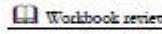
Valuable information



Test your knowledge



Web exercise



Workbook review

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

### Lab Scenario

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

### Lab Objectives

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

You need to:

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

Tools demonstrated in this lab are available in 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

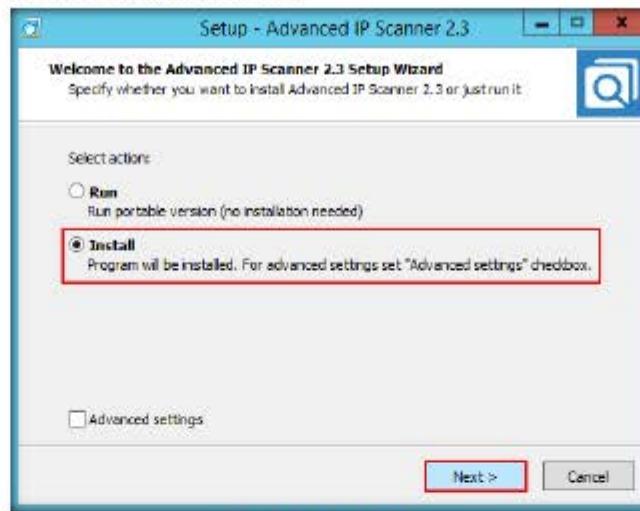
4. Select **Install**, and click **Next**.

FIGURE 2.2: Advance IP Scanner setup

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

FIGURE 2.3: Advance IP Scanner setup

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



FIGURE 2.4 Launching the application from Apps Screen

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

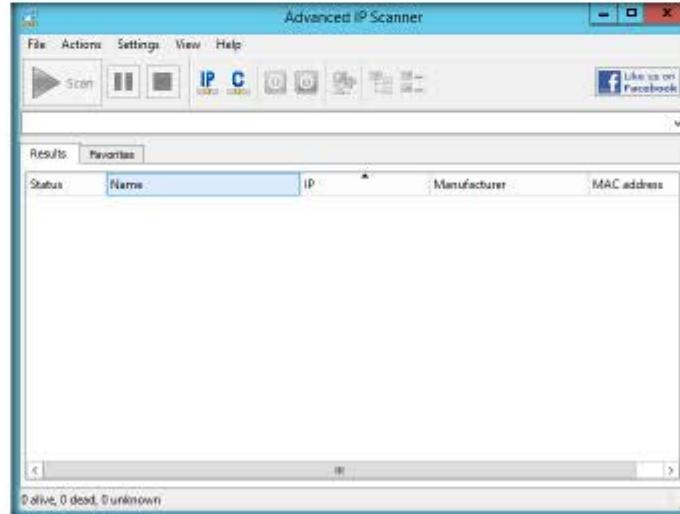


FIGURE 2.5 Advanced IP Scanner main window

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

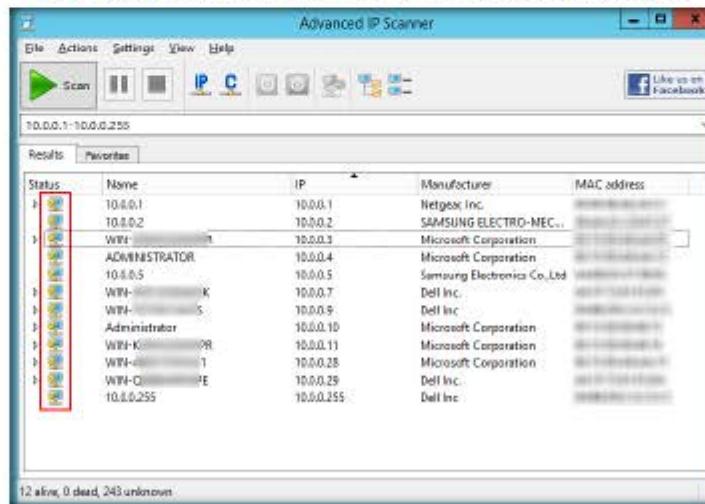


FIGURE 2.7 Advanced IP Scanner displaying Alive Host list

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

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

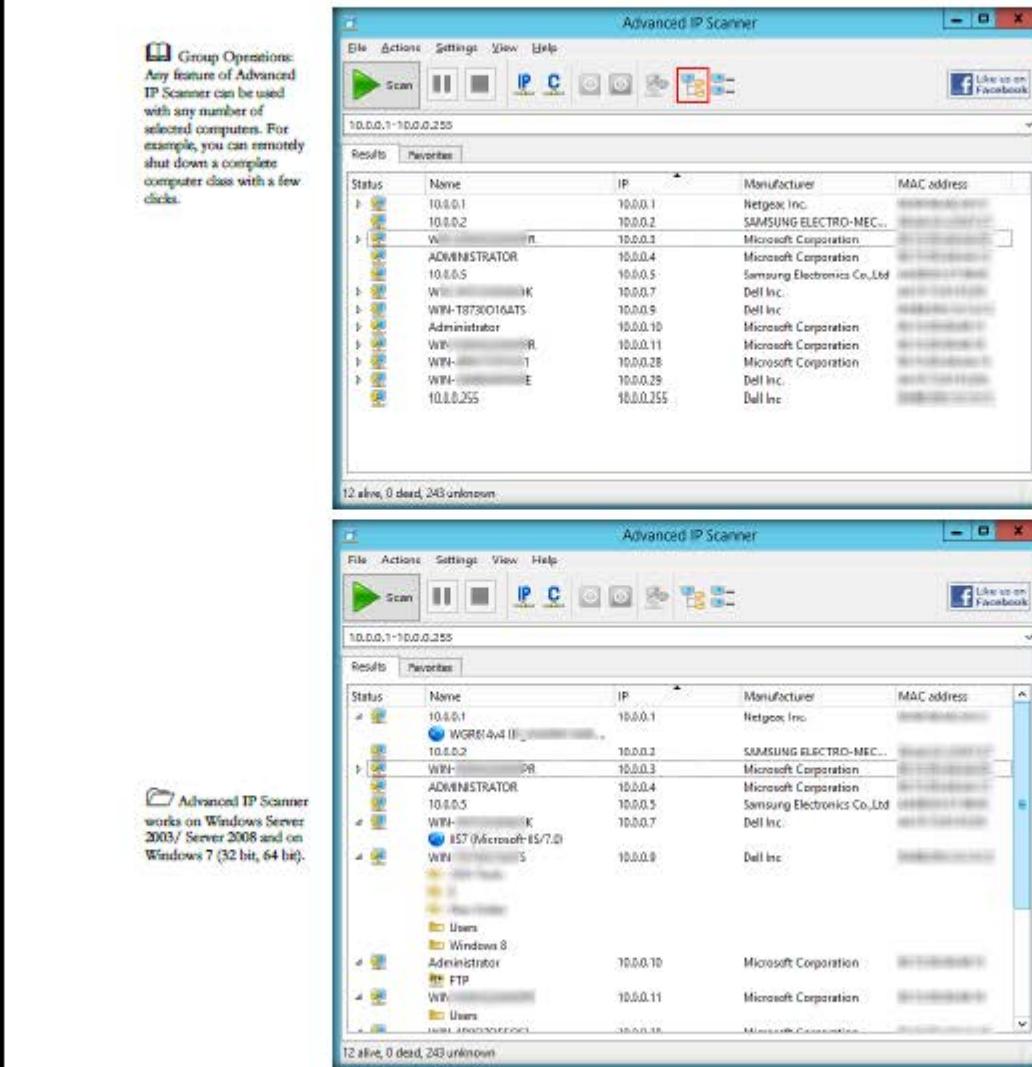


FIGURE 2.8 Advanced IP Scanner displaying shared folders and services

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

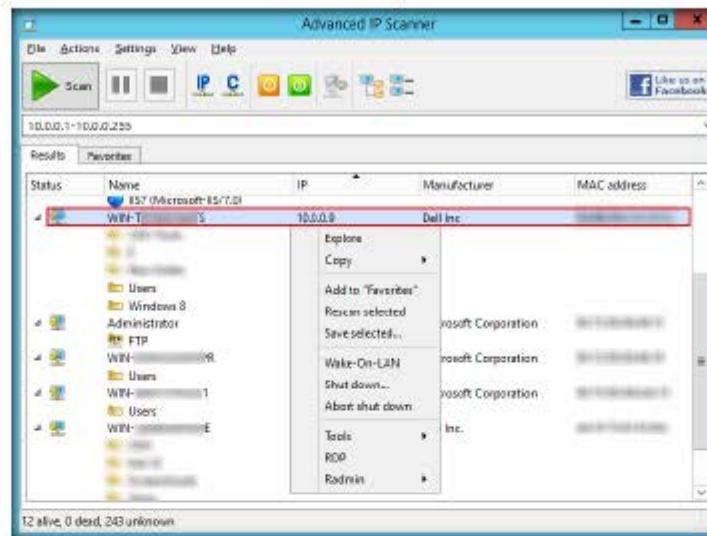


FIGURE 2.9 Exploring the victim machine

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](http://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.

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

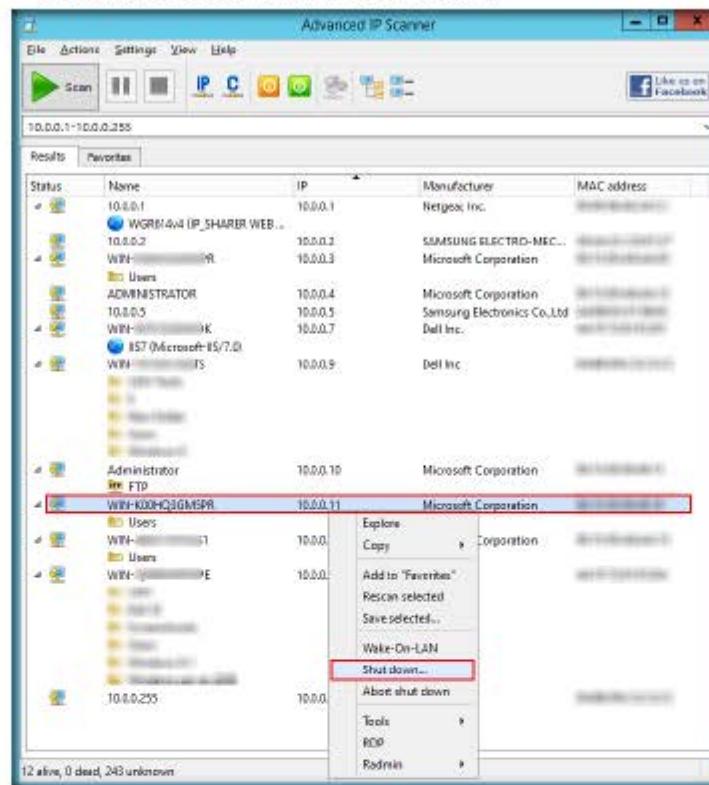
19. Right-click 10.0.0.11 and select **Shut down...**

FIGURE 2.10: Shutting down a virtual machine

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.

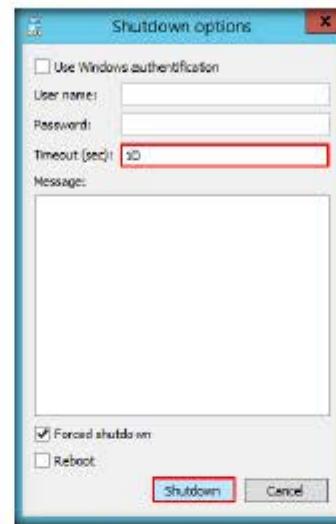


FIGURE 2.11: Shutting down a virtual machine remotely

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

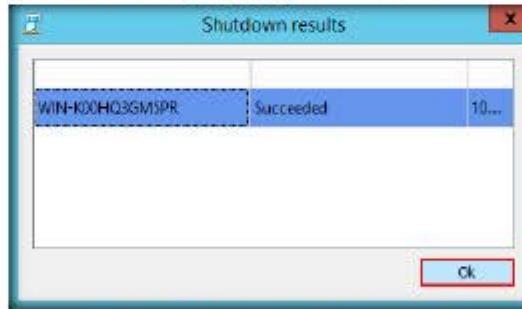


FIGURE 2.12: Shutting down a virtual machine remotely

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

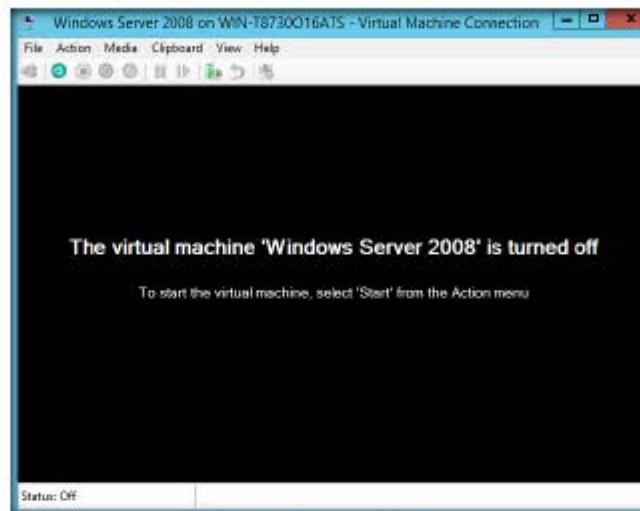


FIGURE 2.13: Victim machine successfully shutdown

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

## Lab Analysis

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

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

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



## Performing Network Enumeration Using 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 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

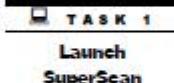
Time: 5 Minutes

### 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



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:

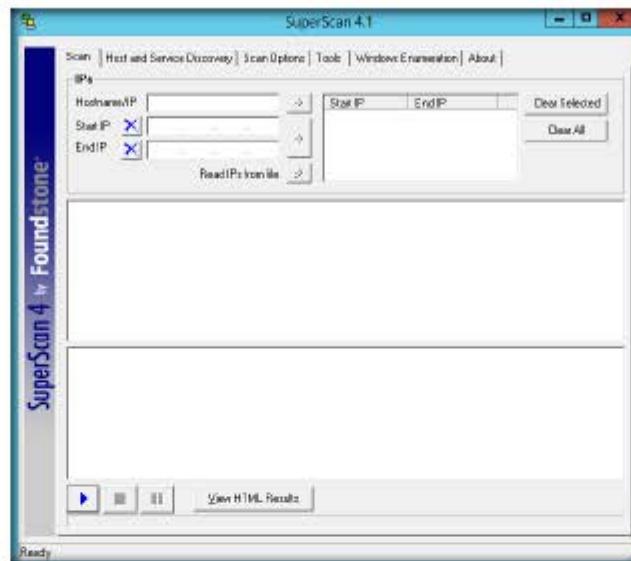


FIGURE 3.1: SuperScan main window

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.

7. Check the types of **enumeration** you want to perform.

8. Now, click on **Enumerate**.

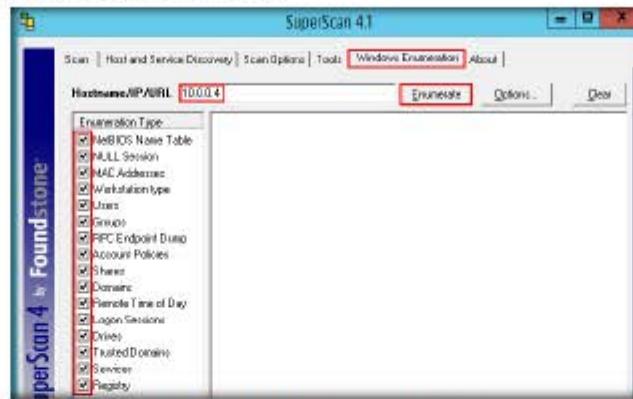


FIGURE 3.2: SuperScan main window with IP Address

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

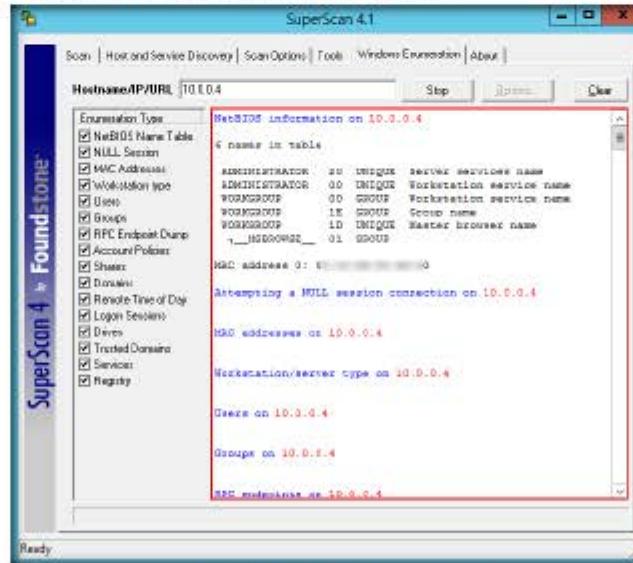


FIGURE 3.3: SuperScan main window with results

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

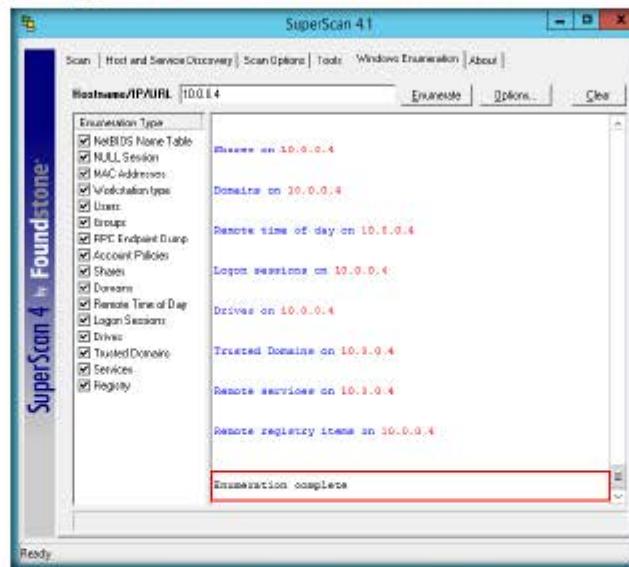
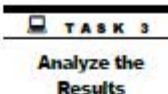


FIGURE 3.4 SuperScan Enumeration completed



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

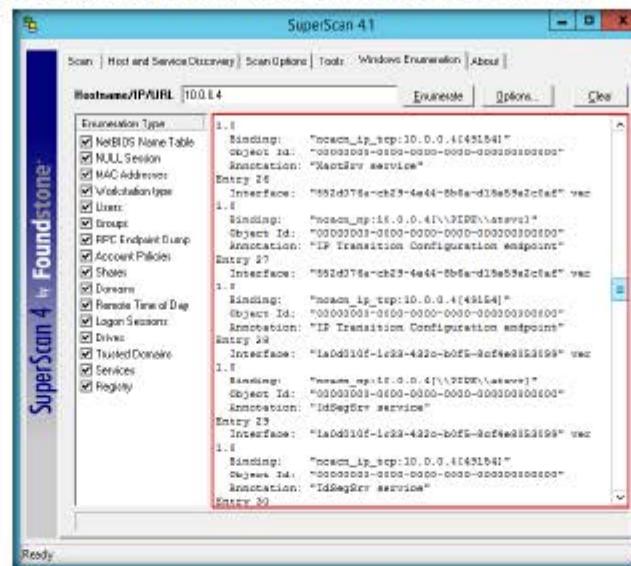


FIGURE 3.5: SuperScan Enumeration Results

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

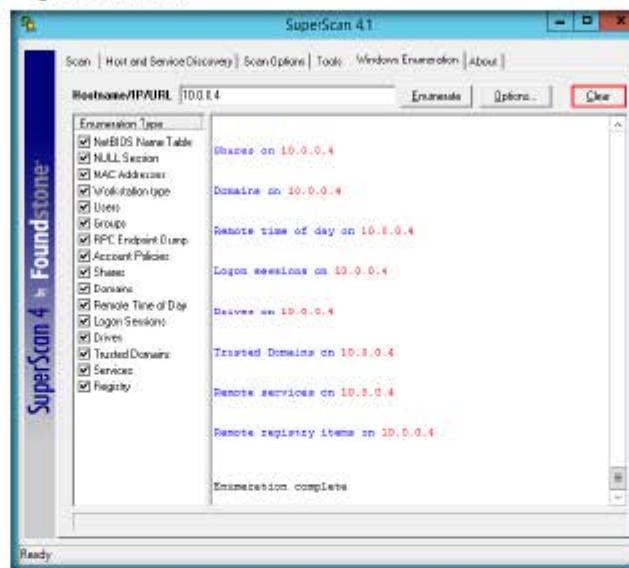


FIGURE 3.6: SuperScan main window with results

## Lab Analysis

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

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

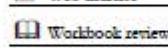
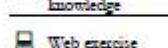
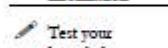
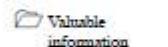
<b>Internet Connection Required</b>	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
<b>Platform Supported</b>	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



## 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



### 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

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.

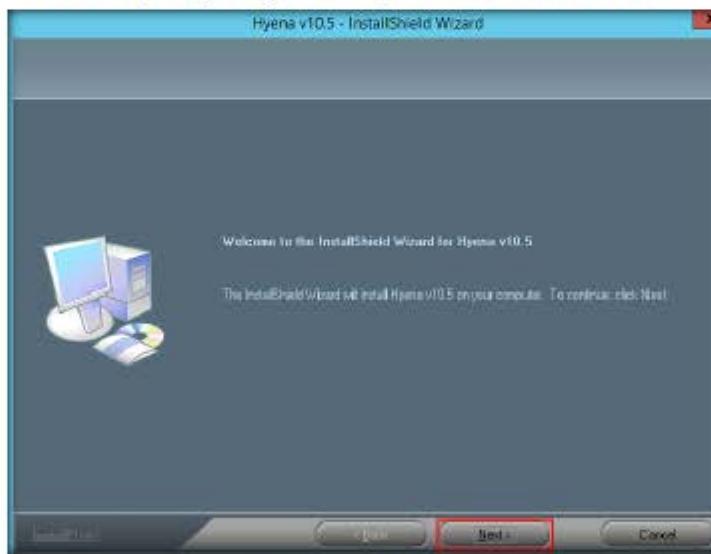


FIGURE 4.1: Installation of Hyena

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

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:

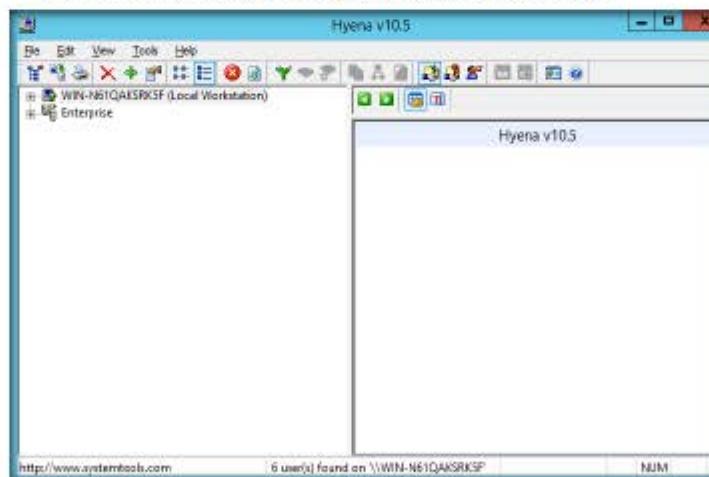


FIGURE 4.3 Main window of Hyena

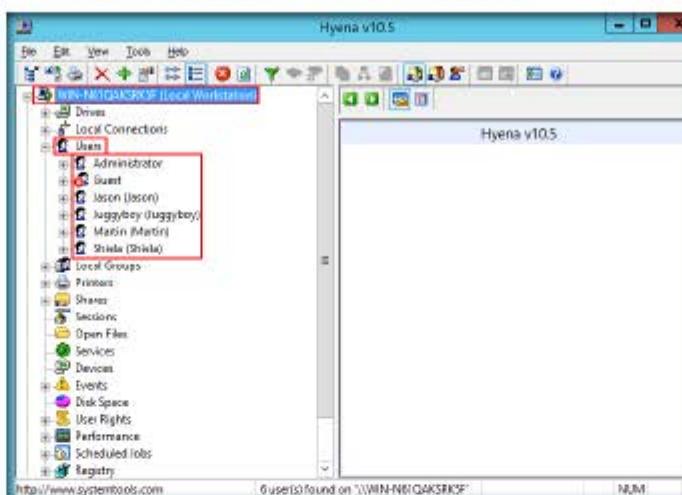
**T A S K 2****Enumerate System Information**

FIGURE 4.4: Expand the System users

**T A S K 3****Examine the Results**

Name	Display Name	Status	Type
AdobeAcrobatUpdateService	Adobe Acrobat Update Service	Runn.	Service (Own Pro)
ActionLogSvc	ActionLog Service	Stop.	Service (Shared P)
ALG	Application Layer Gateway Service	Runn.	Service (Own Pro)
AppHostSvc	Application Host Helper Service	Runn.	Service (Shared P)
AppDsvc	Application Identity	Stop.	Service (Shared P)
AppInfo	Application Information	Runn.	Service (Shared P)
AppMgmt	Application Management	Stop.	Service (Shared P)
AppReadiness	App Readiness	Stop.	Service (Shared P)
AppSVC	AppX Deployment Service (AppXSvc)	Stop.	Service (Shared P)
aspnet_state	ASP .NET State Service	Stop.	Service (Own Pro)
AudioEndpointB...	Windows Audio Endpoint Builder	Runn.	Service (Shared P)
Audiosrv	Windows Audio	Runn.	Service (Shared P)
BaseF	Base Filtering Engine	Runn.	Service (Shared P)
BITS	Background Intelligent Transfer S...	Stop.	Service (Shared P)
Bonjour Service	Bonjour Service	Runn.	Service (Own Pro)
BrokerInfrastructure	Background and Tasks Infrastructure S...	Runn.	Service (Shared P)
Browser	Computer Browser	Stop.	Service (Shared P)
CertPropSvc	Certificate Propagation	Stop.	Service (Shared P)
CDMSystemAppl...	COM+ System Application	Stop.	Service (Own Pro)
CryptSvc	Cryptographic Services	Runn.	Service (Shared P)
DcomLaunch	DCOM Server Process Launcher	Runn.	Service (Shared P)
DefragSrvc	Defragmentation driver	Stop.	Service (Own Pro)

The screenshot shows the 'Hyena v10.5 - Services on \\WIN-QEBBM0PEBPE' interface. The left sidebar shows the 'Local Connection' node. The 'SERVICES' node is selected and highlighted with a red box. The right pane displays a list of services with their names, display names, statuses, and types. Below the sidebar, the URL 'http://www.systemtools.com' is visible.

FIGURE 4.5: Services running in the system

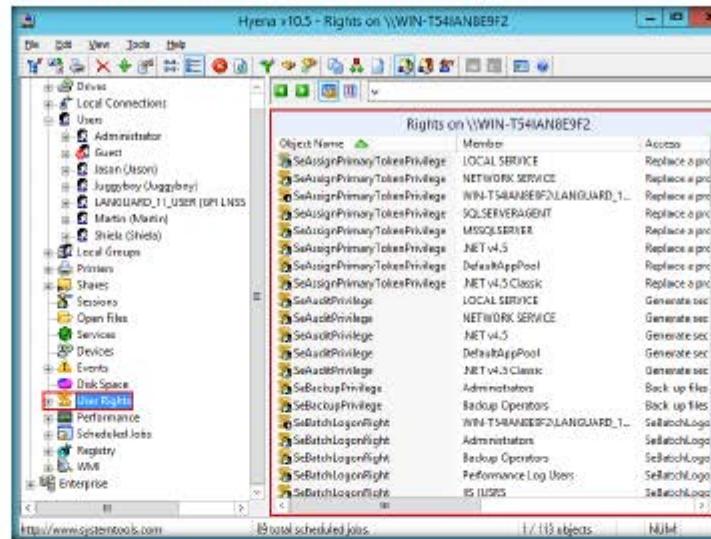
13. Double-click **User Rights** to list the User Rights.

FIGURE 4.6: Users Rights

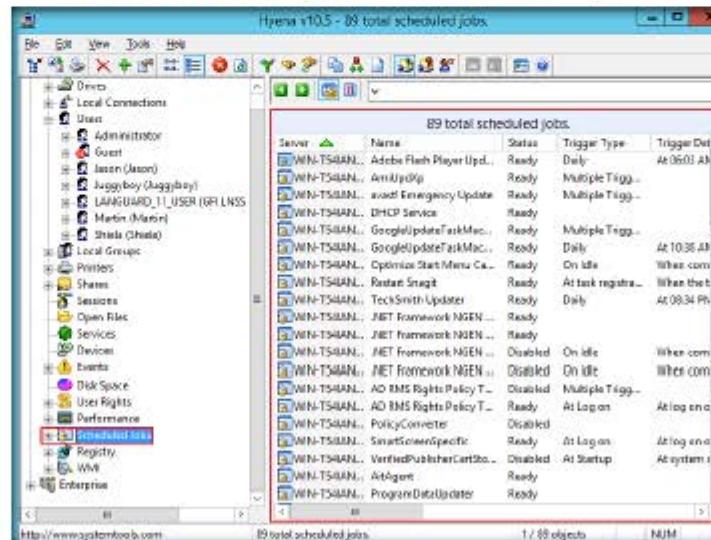
14. Double-click **Scheduled jobs** to examine the Scheduled jobs.

FIGURE 4.7: Scheduled Jobs

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

### Lab Analysis

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

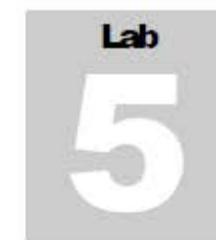
PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS  
RELATED TO THIS LAB.

#### Internet Connection Required

Yes       No

#### Platform Supported

Classroom       iLabs



## 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\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://nbrenum.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



1. To launch NetBIOS Enumerator go to **D:\CEH-Tools\CEHv9 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double click **NetBIOS Enumerator.exe**.
2. If the **Open - File Security Warning** pop-up appears, click **Run**.
3. NetBIOS Enumerator main window appears, as shown in the screenshot:

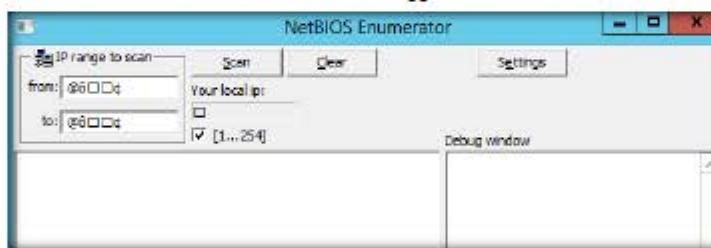


FIGURE 5.1: NetBIOS Enumerator main window

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

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

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.

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

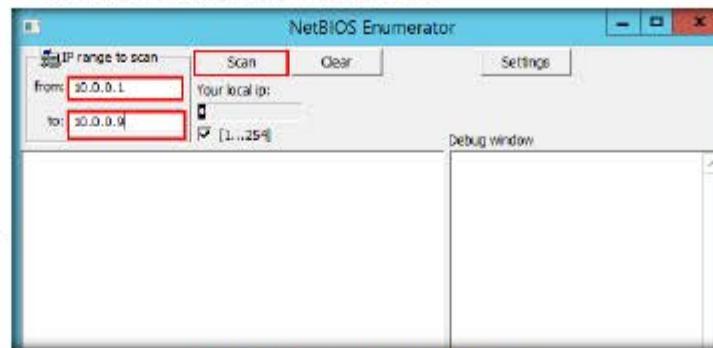


FIGURE 5.2: NetBIOS Enumerator with IP range to scan

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

## TASK 2

### Examine the Results

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

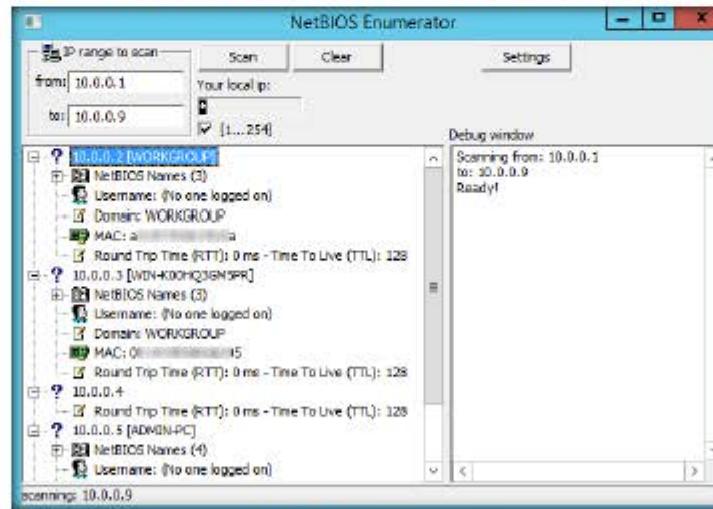


FIGURE 5.3: NetBIOS Enumerator results

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

- Attackers may use the information obtained, such as enumerated usernames, and perform password guessing techniques to crack a user account.

10. To perform a new scan or to reread 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.

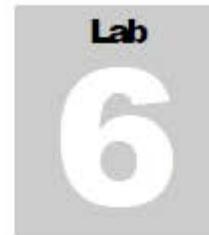
PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS  
RELATED TO THIS LAB.

#### Internet Connection Required

Yes       No

#### Platform Supported

Classroom       iLabs



## 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

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.

#### Workbook reviews

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

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

- 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 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

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

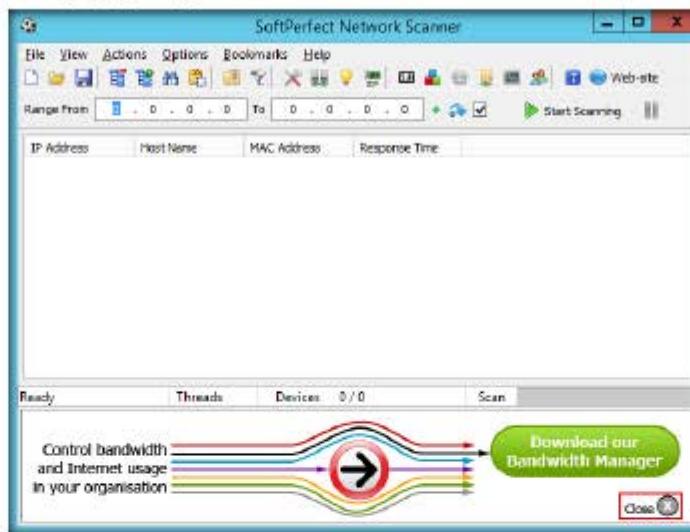


FIGURE 6.2 SoftPerfect Network Scanner main window

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.



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.

IP Address	Host Name	MAC Address	Response Time
10.0.0.1		00:0c:29	0 ms
10.0.0.2	WIN-Q8BBHQBEPF	A0:B1:C2	0 ms
10.0.0.3	WIN-K0DHQ3GM...	00:0c:29	1 ms
10.0.0.4	Administrator	00:0c:29	12 ms
10.0.0.5	ADMIN-PC	00:0c:29	32 ms
10.0.0.7	WIN-JNTDDQFA...	00:0c:29	5 ms
10.0.0.9	WIN-T8730016ATS	00:0c:29	0 ms
10.0.0.6		00:0c:29	325 ms

Scanning... Threads 2 Devices 8 / 8 Scan [Green Progress Bar]

FIGURE 6.4 SoftPerfect status bar

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



FIGURE 6.5 IP address scanned details

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

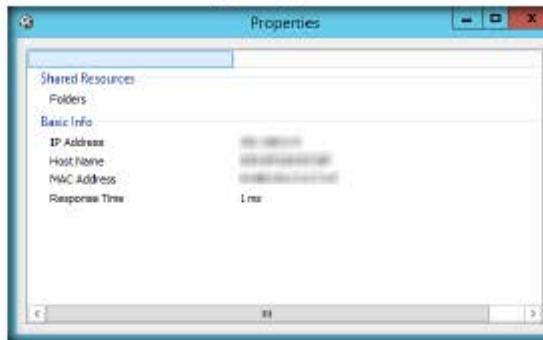


FIGURE 6.6 Properties window

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

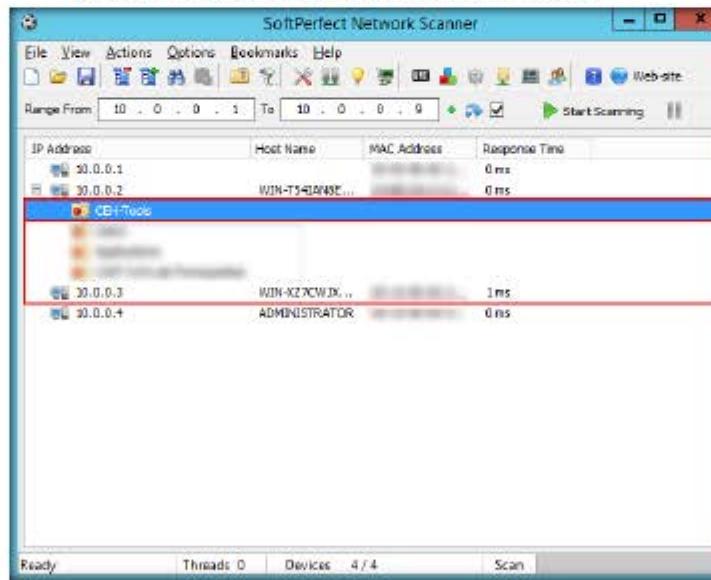


FIGURE 6.7 SoftPerfect Scanner displaying the shared folders

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

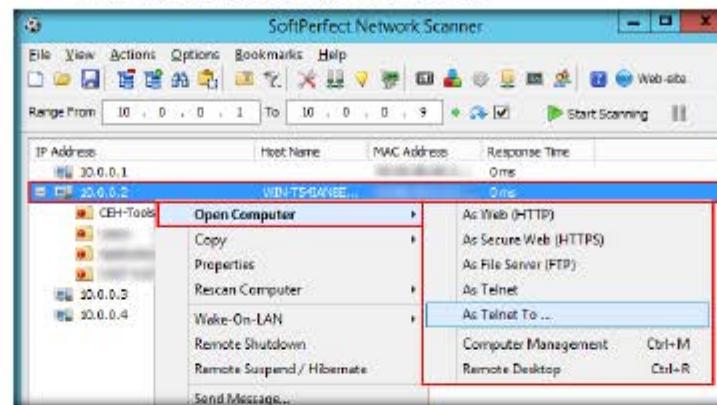


FIGURE 6.8 Various options in SoftPerfect Network Scanner

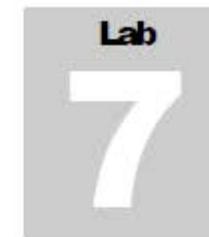
11. If the selected host is not secure enough, you can make use of these options to connect to the remote machines. You may also be able to perform activities such as sending a message, shutting down a computer remotely, and so on. These features are applicable only if the selected machine is built with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

<b>Internet Connection Required</b>	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
<b>Platform Supported</b>	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs



## Enumerating a Target Network using Nmap and Net Use

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

### ICON KEY

	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

### Lab Scenario

In fact a penetration test begins before penetration testers have made contact with victim systems. During enumeration, information is systematically collected and individual systems are identified. Pen testers examine the systems in their entirety to assess security weaknesses. In this lab, we discuss Nmap, it uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, 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 networks filled with IP filters, firewalls, and other obstacles.

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

### Lab Objectives

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

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

## Lab Environment

To perform this lab, you will need:

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

- 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

## Lab Duration

Time: 10 Minutes

## Overview of Enumeration

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

## Lab Tasks

The basic idea in this section is to:

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

Note: If Nmap is already installed in the 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**.

 TASK 1

Install Nmap

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

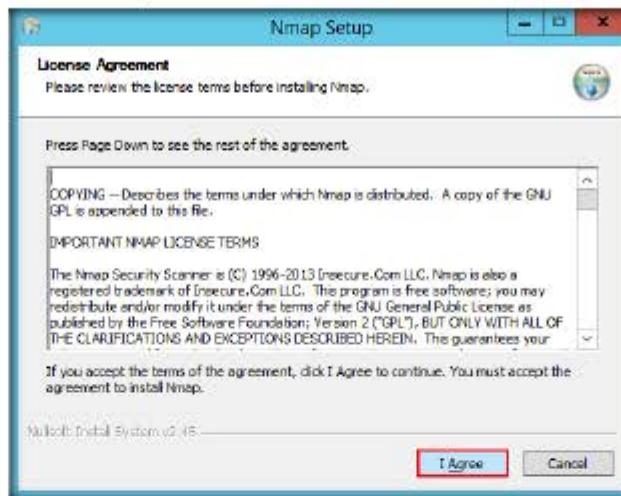


FIGURE 7.1: Nmap Setup window

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

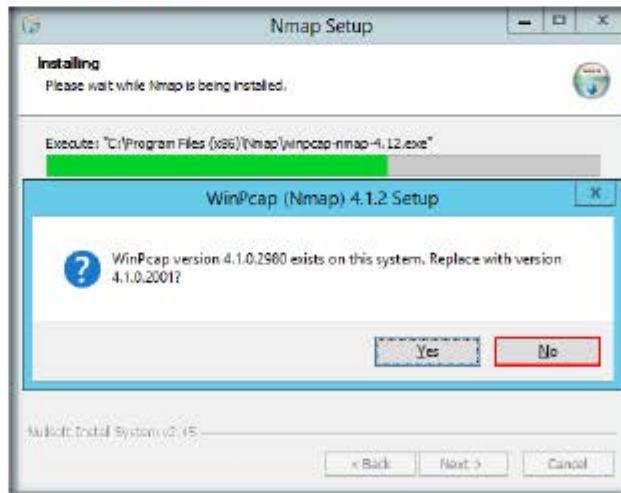


FIGURE 7.2: WinPcap setup pop-up

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

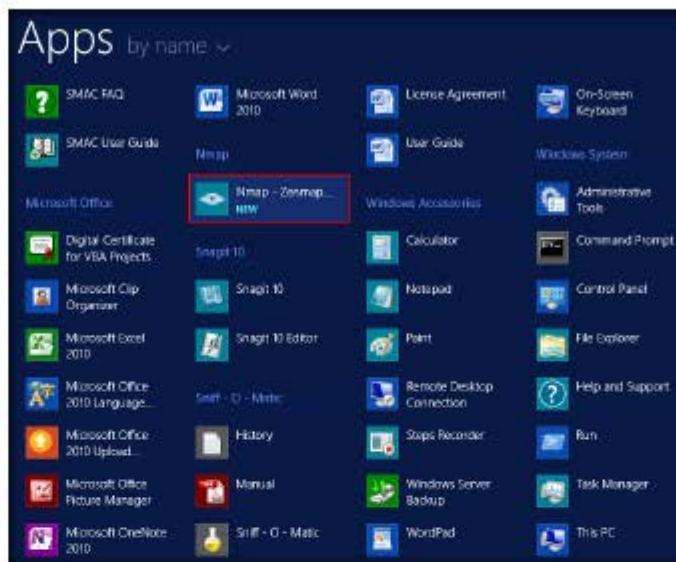


FIGURE 7.3: Windows Server 2012 Apps screen

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

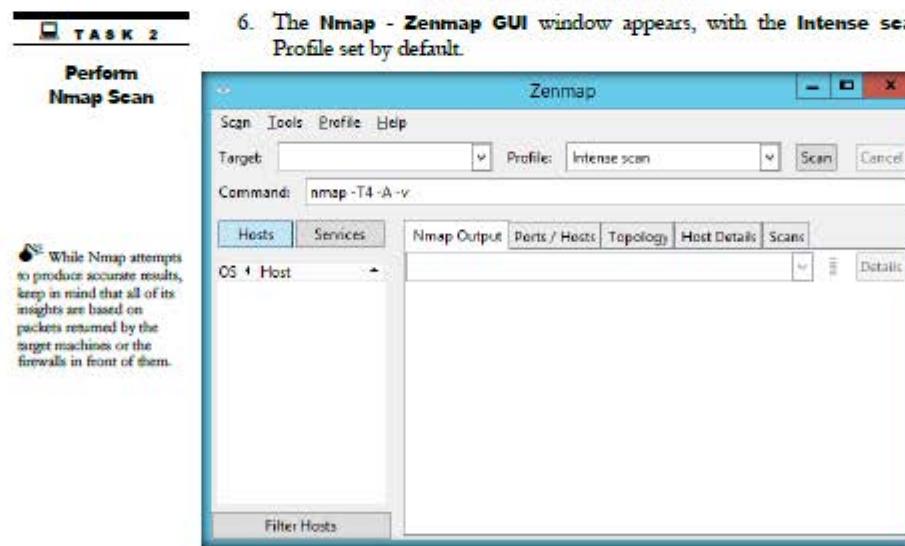


FIGURE 7.4: Nmap/Zenmap main window

 Use the `--script=gross` option for best results in nmap.

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.

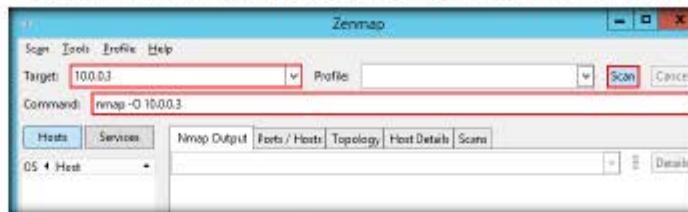


FIGURE 7.5 Configuring Nmap

### TASK 3

#### Find Open NetBIOS Ports

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

8. Nmap performs a **scan** for the provided **target IP address** and outputs the results in the **Nmap Output** tab.
9. Your first target is the computer with a Windows OS, on which you can see ports **139** and **445** open. Remember, this usually works only against **Windows** but may partially succeed if other OSs have these ports open. There may be more than one system with **NetBIOS** open.

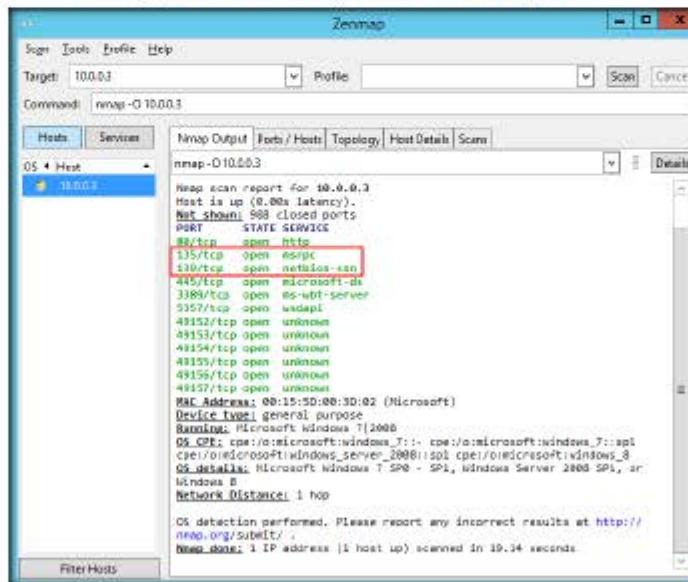


FIGURE 7.6 The Zenmap output window

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

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

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

- Now, launch the **command prompt** in **Windows Server 2008** virtual machine, and perform **nbtstat** on port 139 of the target machine.

- 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.



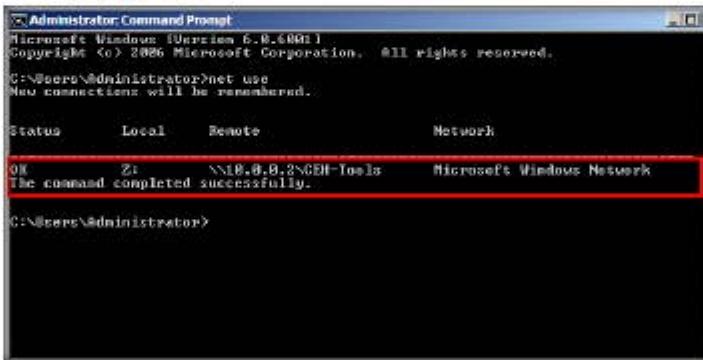
```
C:\Windows\system32\cmd.exe /k nbtstat -A 10.0.0.2
Local Area Connection 2
Node IpAddress: (10.0.0.3) Scope Id: 11
NetBIOS Remote Machine Name Table
  Name          Type      Status
MORMOGROUP    <00>    GROUP    Registered
UNN-QE80MPPEPEK<00> UNIQUE   Registered
UNN-QE80MPPEPEK<00> UNIQUE   Registered
MAC Address = 00:0c:29:00:00:00
C:\Windows\system32\cmd.exe
```

FIGURE 7.7: Command Prompt with the nbtstat command

#### TASK 4

##### Create Null Sessions

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



```
C:\Windows\system32\cmd.exe /k net use
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

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

Status       Local           Remote           Network
OK          Z:\           \\10.0.0.2\CEH-Tools   Microsoft Windows Network
The command completed successfully.

C:\Users\Administrator>
```

FIGURE 7.8: Command Prompt with the net use command

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

- 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).
- This **creates/ connects** a null session.

```
C:\Users\Administrator>net use \\192.168.0.2\CEH-Tools ""<user>""
Local name      Remote name
Resource type   Resource type
Status         OK
# O/Ses       0
# Connections  2
The command completed successfully.

C:\Users\Administrator>
```

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.
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:

```
C:\Users\Administrator>net use \\192.168.0.2\CEH-Tools ""<user>""
Local name      Remote name
Resource type   Resource type
Status         OK
# O/Ses       0
# Connections  2
The command completed successfully.

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

Status          Local      Remote           Network
OK             Z:        \\192.168.0.2\CEH-Tools Microsoft Windows Network
OK             Z:        \\192.168.0.2\CEH-Tools Microsoft Windows Network
The command completed successfully.

C:\Users\Administrator>net use \\192.168.0.2\CEH-Tools ""<user>"
```

Status	Local	Remote	Network
OK	Z:	\\192.168.0.2\CEH-Tools	Microsoft Windows Network
OK	Z:	\\192.168.0.2\CEH-Tools	Microsoft Windows Network

FIGURE 7.10: The command prompt with the net use command

## Lab Analysis

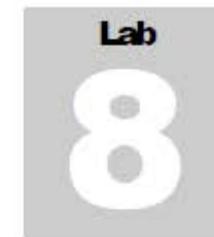
Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

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

---

<b>Internet Connection Required</b>	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
<b>Platform Supported</b>	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs

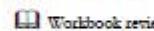
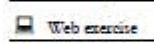
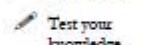
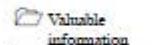
---



## Enumerating Services on a Target Machine

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

### ICON KEY



### 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

## 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.

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

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.

```
root@root: ~
File Edit View Search Terminal Help
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--log-errors: Log errors/warnings to the normal-format output file
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  -datadir <dirname>: Specify custom Nmap data file location
  -sendETH/-send-ip: Send using raw ethernet frames or IP packets
  -privileged: Assume that the user is fully privileged
  -unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/18 10.0.0.0/8
  nmap -v -PR 10000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@root: ~#
```

The terminal window shows the usage information for the nmap command. It includes sections for options like --open, --packet-trace, and --iflist, as well as a 'MISC' section with flags like -6, -A, and -privileged. Examples of command-line usage are provided at the bottom, such as 'nmap -v -A scanme.nmap.org' and 'nmap -v -PR 10000 -Pn -p 80'.

FIGURE 8.3: nmap in Command Terminal

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

```
root@root: ~
File Edit View Search Terminal Help
root@root:~# nmap -sP 10.0.0.0/10
```

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:

```
root@root: ~
File Edit View Search Terminal Help
root@root:~# nmap -sP 10.0.0.0/10

Starting Nmap 6.46 ( http://nmap.org ) at 2015-04-04 02:13 EDT
Nmap scan report for 10.0.0.1
Host is up (0.0012s latency).
MAC Address: [REDACTED] (Netgear)
Nmap scan report for 10.0.0.2
Host is up (0.0011s latency).
MAC Address: [REDACTED] (Dell)
Nmap scan report for 10.0.0.4
Host is up (0.00031s latency).
MAC Address: [REDACTED] (Dell)
Nmap scan report for 10.0.0.6
Host is up (0.00049s latency).
MAC Address: [REDACTED] (Microsoft)
Nmap scan report for 10.0.0.8
Host is up (0.0014s latency).
MAC Address: [REDACTED] (Microsoft)
Nmap scan report for 10.0.0.9
Host is up.
```

FIGURE 8.5: nmap Ping Sweep scan results

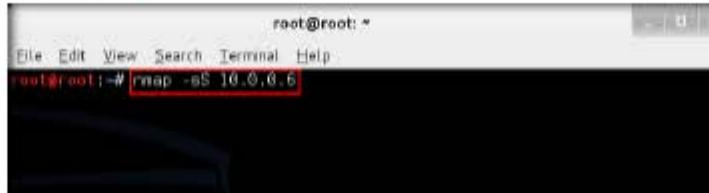
-sP this scan type lists the hosts within the specified range that responded to a ping. It allows you to detect which computers are online, rather than which ports are open. Four methods exist within Nmap for ping sweeping.

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 [IP Address of Target Machine]` 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.

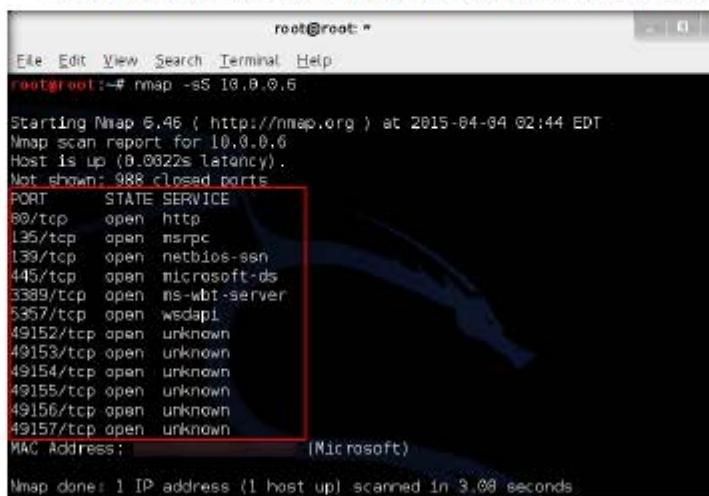


```
root@root: ~
File Edit View Search Terminal Help
root@root:~# nmap -sS 10.0.0.6
```

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.



```
root@root: ~
File Edit View Search Terminal Help
root@root:~# nmap -sS 10.0.0.6

Starting Nmap 6.46 ( http://nmap.org ) at 2015-04-30 02:44 EDT
Nmap scan report for 10.0.0.6
Host is up (0.0022s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3889/tcp  open  ms-wbt-server
5357/tcp  open  wwdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 3.08 seconds
```

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 -sV -O [IP Address of Target Machine]` 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.

```
root@root: ~
File Edit View Search Terminal Help
root@root:~# nmap -sV -O 10.0.0.6
```

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:

```
root@root: ~
File Edit View Search Terminal Help
Nmap scan report for 10.0.0.6
Host is up (0.00000s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE VERSION
38/tcp    open  http   Microsoft IIS httpd 7.0
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
5257/tcp  open  http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc
49153/tcp open  msrpc
49154/tcp open  msrpc
49155/tcp open  msrpc
49156/tcp open  msrpc
49157/tcp open  msrpc
MAC Address: 00:15:5D:00:18:B7 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 7 [2008]
OS CPE: cpe:/o:microsoft:windows_7::*-cpe:/o:microsoft:windows_7::spl-cpe:/o:microsoft:windows_server_2008::spl-cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SPL, Windows Server 2008 SPL, or Windows 8
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

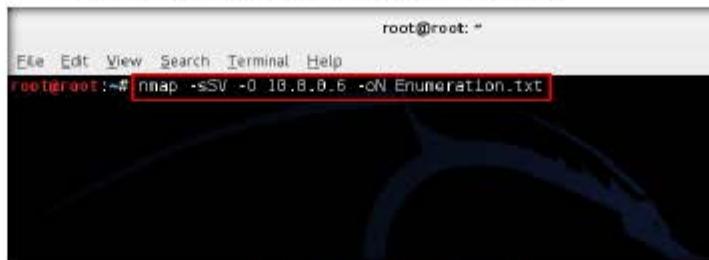
Nmap done: 1 IP address (1 host up) scanned in 64.69 seconds
```

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.

**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.



```
root@root:~# nmap -sSV -o 10.0.0.6 -oN Enumeration.txt
```

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**.

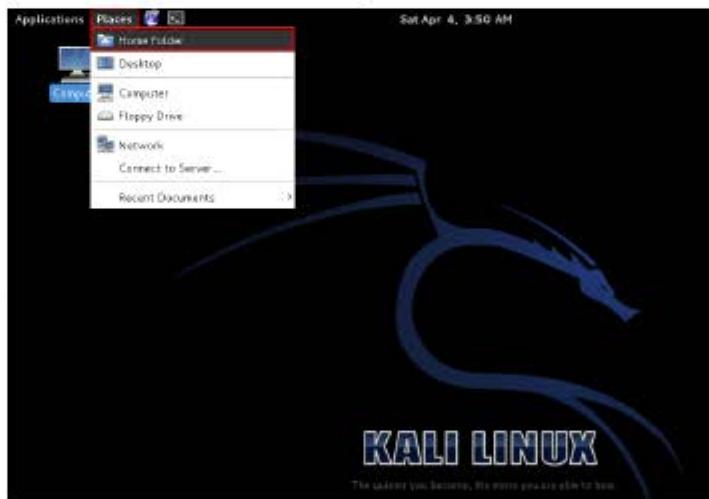


FIGURE 8.11: Kali Linux Home Folder

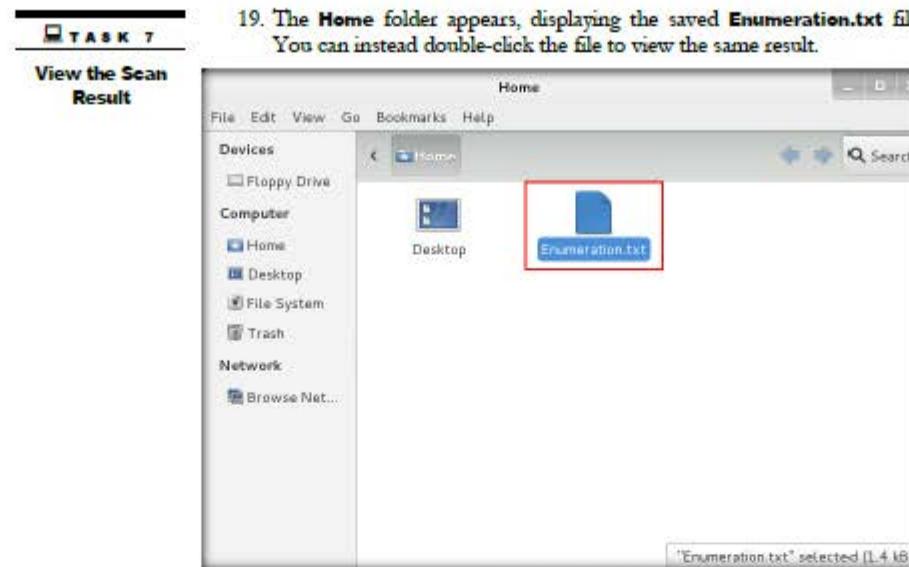


FIGURE 8.12: Stealthy Syn Scan Result File

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

```

* Nmap 6.46 scan initiated Sat Apr 4 09:36:38 2015 as: nmap -sV -O -oN Enumeration.txt ICD
Nmap scan report for 19.0.0.6
Host is up (0.00085s latency).
Not shown: 909 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft IIS httpd 7.0
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49156/tcp open  msrpc       Microsoft Windows RPC
49157/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 08:35:5D:00:1B:87 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 7 [2008]
OS: CPE: cpe:/microsoft:windows_7::; cpe:/microsoft:windows_7::sp1 cpe:/microsoft:win
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/microsoft:windows

OS and Service detection performed. Please report any incorrect results at http://nmap.org/
* Nmap done at Sat Apr 4 09:37:35 2015 -- 1 IP address (1 host up) scanned in 58.14 seconds

```

FIGURE 8.13: Stealthy Scan Result

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

```

root@root:~#
File Edit View Search Terminal Help
root@root:~# cat Enumeration.txt
# Nmap 6.46 scan initiated Sat Apr  4 03:36:38 2015 as: nmap -sSV -O -oN Enumeration
3.6
Nmap scan report for 10.0.0.6
Host is up [0.00005s latency].
Not shown: 988 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 7.0
135/tcp   open  msrpc   Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
5357/tcp  open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc   Microsoft Windows RPC
49153/tcp open  msrpc   Microsoft Windows RPC
49154/tcp open  msrpc   Microsoft Windows RPC
49155/tcp open  msrpc   Microsoft Windows RPC
49156/tcp open  msrpc   Microsoft Windows RPC
49157/tcp open  msrpc   Microsoft Windows RPC
MAC Address: 08:15:5D:00:18:07 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::; cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

root@root:~#

```

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.

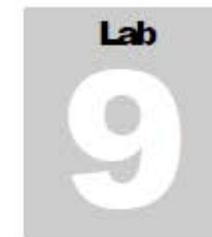
PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

### Internet Connection Required

Yes       No

### Platform Supported

Classroom       iLabs



## 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.

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

```
root@kali:~# nmap -sU -p 161 10.0.0.10
```

FIGURE 9.1: Performing nmap UDP scan

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

```
root@kali:~# nmap -sU -p 161 10.0.0.10
Starting Nmap 6.46 ( http://nmap.org ) at 2015-04-14 04:55 EDT
Nmap scan report for 10.0.0.10
Host is up (0.00094s latency).
PORT      STATE      SERVICE
161/udp  open|filtered  snmp
MAC Address: 00:15:5D:00:27:05 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

FIGURE 9.2: nmap UDP scan result

**TASK 2****Find SNMP Community String**

**NS** nmap -sU --script snmp-brute <target> [-scriptargs snmp-communityfile=<wordlist>]

```
root@kali:~# nmap -sU -p 161 10.0.0.10
Starting Nmap 6.46 ( http://nmap.org ) at 2015-04-14 04:55 EDT
Nmap scan report for 10.0.0.10
Host is up (0.00094s latency).
PORT      STATE      SERVICE
161/udp  open|filtered  snmp
MAC Address: 00:15:5D:00:27:05 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
root@kali:~# nmap -sU -p 161 --script=snmp-brute 10.0.0.10
```

FIGURE 9.3: nmap finding SNMP community string

**NS** If not defined, the default wordlist used to brute-force the SNMP community strings is /usr/share/snmp/communities.txt.

- Type `nmap -sU -p 161 --script=snmp-brute <Target machine IP Address>` and press **Enter**.
- This script will extract the SNMP community string from the target machine.
- It will search pcap socket in parallel threads. The sending sockets sends the SNMP probes along with the community strings with valid credentials.
- 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 the target machine doesn't have a valid account, no output will display.

```
root@kali:~# nmap -sU -p 161 10.0.0.10
Starting Nmap 6.46 ( http://nmap.org ) at 2015-04-14 04:55 EDT
Nmap scan report for 10.0.0.10
Host is up (0.00094s latency).
PORT      STATE      SERVICE
161/udp  open|filtered  snmp
MAC Address: 00:15:5D:00:27:05 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
root@kali:~# nmap -sU -p 161 --script=snmp-brute 10.0.0.10

Starting Nmap 6.46 ( http://nmap.org ) at 2015-04-14 04:58 EDT
Nmap scan report for 10.0.0.10
Host is up (0.0010s latency).
PORT      STATE      SERVICE
161/udp  open|filtered  snmp
|_ snmp-brute:
|_ public - Valid credentials
MAC Address: 00:15:5D:00:27:05 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
root@kali:~#
```

FIGURE 9.4: SNMP Community String found with Valid Credentials

**NS** In case this wordlist does not exist, the script falls back to /usr/share/snmp/passwords.txt.

- 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.

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

```
root@kali:~# snmpcheck
snmpcheck v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

Usage: snmpcheck [-t <IP address>
                  -p : target host;
                  -p : SNMP port; default port is 161;
                  -c : SNMP community; default is public;
                  -v : SNMP version {1,2}; default is 1;
                  -r : request retries; default is 0;
                  -w : detect write access (separate action by enumeration);
                  -d : disable 'TCP connections' enumeration!
                  -T : force timeout in seconds; default is 20. Max is 60;
                  -D : enable debug;
                  -h : show help menu;

root@kali:~#
```

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.

```
root@kali:~# snmpcheck -t 10.0.0.10 -c public | more
```

FIGURE 9.6: Enumerating Community String using **snmpcheck**

**snmpcheck** enumerated System Information.

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

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

```

root@kali:~# snmpcheck v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org).

[*] Try to connect to 10.0.0.10
[*] Connected to 10.0.0.10
[*] Starting enumeration at 2015-04-14 05:07:57

[*] System information
-----
Hostname : WIN-SBAYZ63DD9W
Description : Hardware: Intel64 Family 6 Model 58 Stepping 9 AT/AT Compatible - Software: Windows Version 6.0 (Build 6001 Multiprocessor Free)
Uptime system : 1 day, 16:06:05.93
Uptime SNMP daemon : 3 hours, 59:33.46
Moid :
Domain (NT) : CEM

[*] Devices information
-----
[*] More ...

```

FIGURE 9.7: snmpcheck enumerated System Information

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

Id	Type	Status	Description
1	Printer	Running	Microsoft XPS Document Writer
10	Network	Unknown	MAN Miniprt (IP)
11	Network	Unknown	RAS Async Adapter
12	Network	Unknown	Microsoft VMBus Network Adapter
13	Network	Unknown	Intel 21140-Based PCI Fast Ethernet Adapter
14	Network	Unknown	isatap.{97C3B3EA-0C0B-49BB-BADD-47C3EADC3A6E}
15	Network	Unknown	Teredo Tunneling Pseudo-Interface
16	Network	Unknown	MAN Miniport (IPv6)-QoS Packet Scheduler-0000
17	Network	Unknown	MAN Miniport (IP)-QoS Packet Scheduler-0000
18	Network	Unknown	MAN Miniport (Network Monitor)-QoS Packet Scheduler-0000
19	Network	Unknown	Intel 21140-Based PCI Fast Ethernet Adapter
2	Processor	Running	Unknown Processor Type
20	Disk Storage	Unknown	A:\

FIGURE 9.8: snmpcheck enumerated Devices Information

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

The screenshot shows a terminal window titled '[\*] Storage information' with the command 'root@kali: ~'. It lists the following storage details:

Drive	Device id	Device type	Filesystem type
A:\	1	Removable Disk	Unknown
C:\	2	Fixed Disk	NTFS
D:\	3	Compact Disc	Fat

A note on the left side of the terminal window states: 'SNMP is dangerous as it is a clear text protocol and as such could potentially provide valuable information to an attacker.'

FIGURE 9.9: `snmpcheck` enumerated Storage Information

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 (ADEExplorer)

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

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

## Lab Environment

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

---

**T A S K 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**.

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



FIGURE 10.1: Open File – Security Warning

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.

**TASK 2**  
Connect to Active  
Directory Machine

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

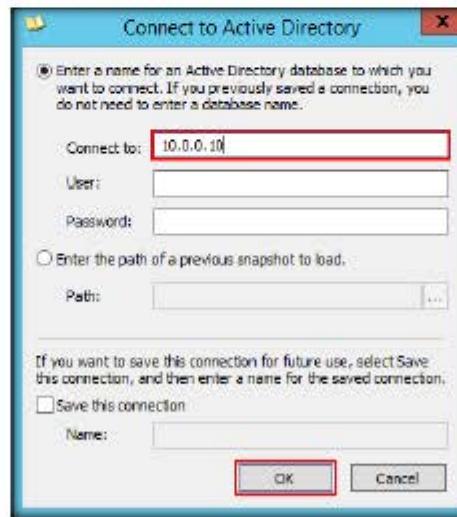


FIGURE 10.2: ADEplorer Connect to Active Directory

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

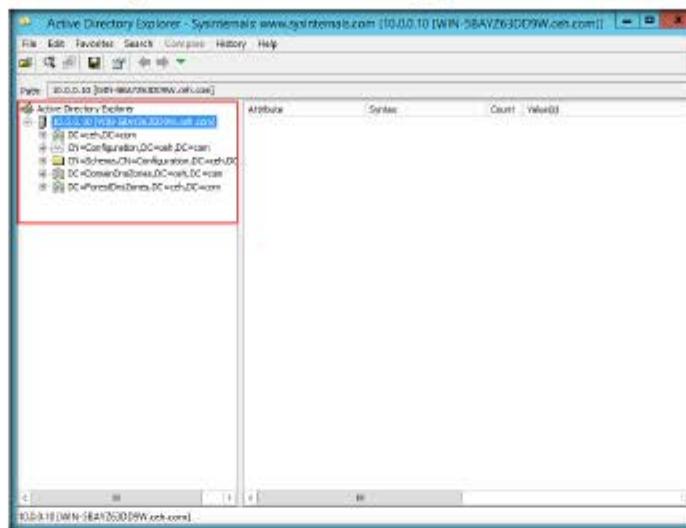


FIGURE 10.3: ADExplorer Main Window

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

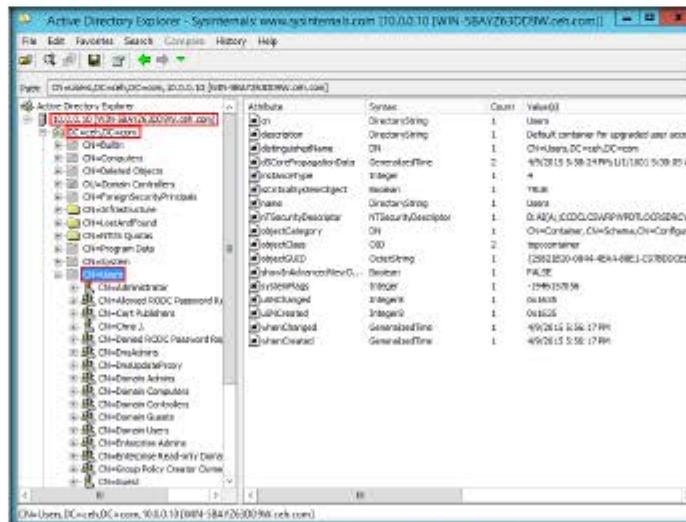


FIGURE 10.4: ADExplorer Domain Users Node

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

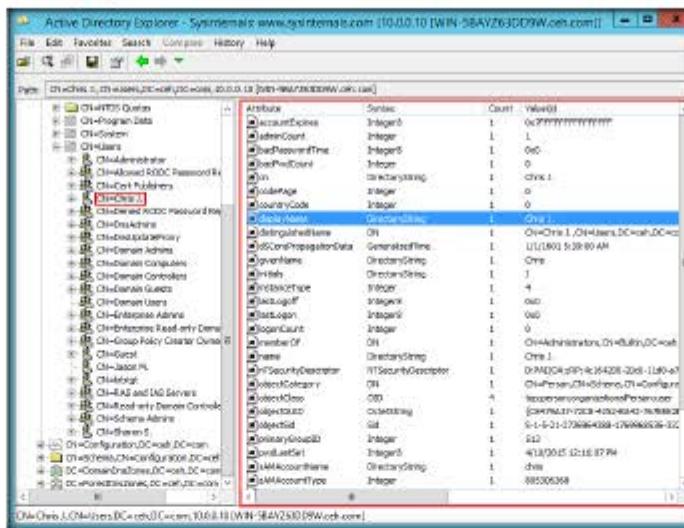


FIGURE 10.5: AD Explorer Domain Users Profile Attributes

 **TASK 3**

## Modifying User Attributes

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

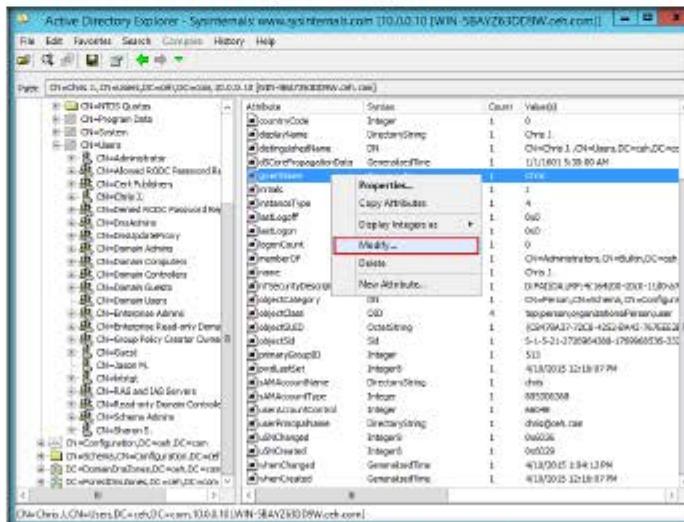


FIGURE 10.6: ADEplorer User Profile Modifications

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

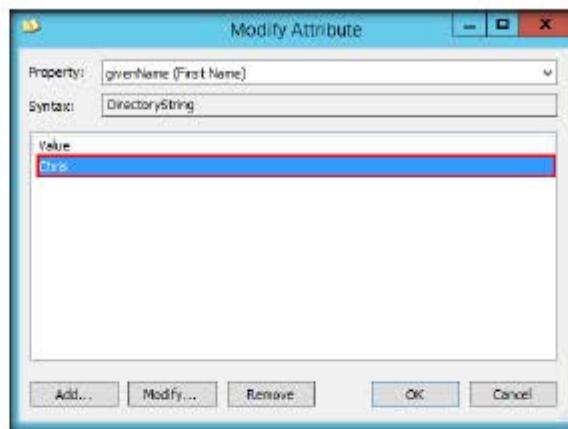


FIGURE 10.7: Modifying Attributes

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

## Lab Analysis

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

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

### Internet Connection Required

Yes       No

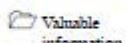
### Platform Supported

Classroom       iLabs

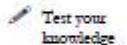
**Lab****11**

## Performing Network Enumeration Using Various DNS Interrogation Tools

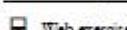
*Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system.*

**ICON KEY**

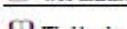
Valuable information



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



FIGURE 11.1 Kali Linux Machine

#### TASK 2

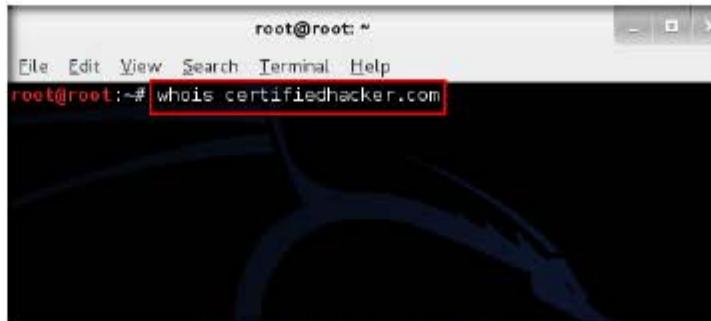
##### Launch Command Line Terminal



FIGURE 11.2 Launching Command Terminal

**TASK 3****Enumerate Whois Information**

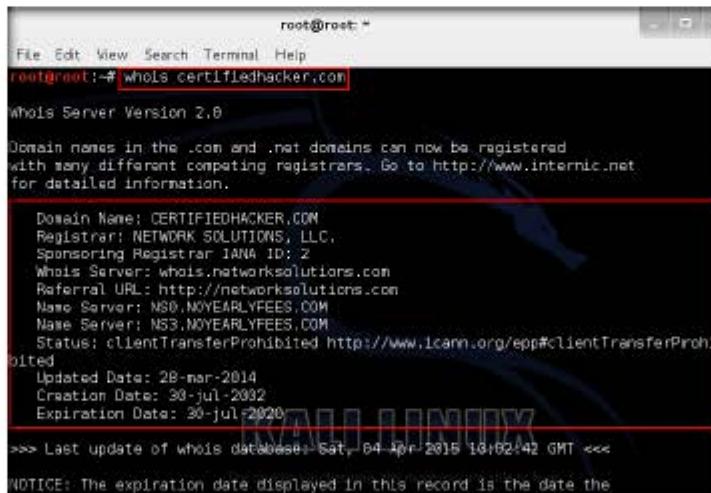
5. The target used in this lab is [www.certifiedhacker.com](http://www.certifiedhacker.com); its corresponding domain name is `certifiedhacker.com`.
6. Type `whois certifiedhacker.com` in the command-line terminal, and press **Enter**



```
root@root:~#
File Edit View Search Terminal Help
root@root:~# whois certifiedhacker.com
```

FIGURE 11.3: Whois information of certifiedhacker.com

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



```
root@root:~#
File Edit View Search Terminal Help
root@root:~# whois certifiedhacker.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: CERTIFIEDHACKER.COM
Registrar: NETWORK SOLUTIONS, LLC.
Sponsoring Registrar IANA ID: 2
Whois Server: whois.networksolutions.com
Referral URL: http://networksolutions.com
Name Server: NS0.NOVEARLYFEES.COM
Name Server: NS3.NOVEARLYFEES.COM
Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Updated Date: 28-mar-2014
Creation Date: 08-jul-2002
Expiration Date: 08-jul-2020

>>> Last update of whois database: Sat, 04 Apr 2015 10:02:42 GMT <<<

NOTICE: The expiration date displayed in this record is the date the
```

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 to give the IP address after the command.

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

The terminal window shows the WHOIS results for the domain CERTIFIEDHACKER.COM. The information includes:

- Domain Name: CERTIFIEDHACKER.COM
- Registry Domain ID: 88849376 DOMAIN\_COM-VRSN
- Registrar WHOIS Server: whois.networksolutions.com
- Registrar URL: http://networksolutions.com
- Updated Date: 2015-01-29T01:49:45Z
- Creation Date: 2014-03-28T12:11:47Z
- Registrar Registration Expiration Date: 2026-07-29T04:00:00Z
- Registrar: NETWORK SOLUTIONS, LLC.
- Registrar IANA ID: 2
- Registrar Abuse Contact Email: abuse@web.com
- Registrar Abuse Contact Phone: +1.8003337680
- Reseller:
- Domain Status:
- Registry Registrant ID:
- Registrant Name: Mohideen, Haja
- Registrant Organization:
- Registrant Street: 6338 Riverside Plaza Ln NW
- Registrant City: Albuquerque
- Registrant State/Province: NM
- Registrant Postal Code: 87120

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.

The terminal window shows the command "host www.certifiedhacker.com" being run. The output is:

```
root@root:~# host www.certifiedhacker.com
```

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:

The terminal window shows the output of the "host" command for the website www.certifiedhacker.com. The output is:

```
root@root:~# host www.certifiedhacker.com
www.certifiedhacker.com has address 202.75.54.101
root@root:~#
```

FIGURE 11.7: IP address of the Target

**TASK 5****Enumerate DNS Records Using host**

```
root@root:~# host -a certifiedhacker.com
Trying "certifiedhacker.com"
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 31870
;; Flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;certifiedhacker.com.      IN      ANY
;; ANSWER SECTION:
certifiedhacker.com.    2345    IN      SOA     ns3.noearlyfees.com. hostmaster
.noearlyfees.com. 10 900 600 86400 3600
certifiedhacker.com.    82417   IN      NS      ns8.noearlyfees.com.
certifiedhacker.com.    82417   IN      NS      ns3.noearlyfees.com.

Received 133 bytes from 10.0.0.1#53 in 74 ms
root@root:~#
```

FIGURE 11.8: DNS records of the Target

**TASK 6****Enumerate DNS Records Using dnsenum**

```
root@root:~# dnsenum certifiedhacker.com
dnsenum.pl VERSION 0.1.2.3

----- certifiedhacker.com -----

Host's addresses:
certifiedhacker.com.          2747    IN      A       232.75.54.181

Name Servers:
ns8.noearlyfees.com.         79445   IN      A       232.75.54.188
ns3.noearlyfees.com.          79268   IN      A       232.75.54.182

Mail (MX) Servers:
mail.certifiedhacker.com.    2791    IN      A       232.75.54.180
```

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:

```
root@root: ~
File Edit View Search Terminal Help
mail.certifiedhacker.com. 2791 IN A 232.75.54.180

Trying Zone Transfers and getting Bind Versions
Trying Zone Transfer for certifiedhacker.com on ns1.noearlyfees.com ...
certifiedhacker.com. 3600 IN SOA ns0.noearlyfees.com.
certifiedhacker.com. 3600 IN A 232.75.54.181
certifiedhacker.com. 3600 IN NS ns0.noearlyfees.com.
certifiedhacker.com. 3600 IN MX 10
exchange.certifiedhacker.com. 3600 IN A 232.75.54.181
ftp.certifiedhacker.com. 3600 IN A 232.75.54.181
mail.certifiedhacker.com. 3600 IN A 232.75.54.180
webmail.certifiedhacker.com. 3600 IN A 232.75.54.181
www.certifiedhacker.com. 3600 IN A 232.75.54.181

Trying Zone Transfer for certifiedhacker.com on ns3.noearlyfees.com ...
AXFR record query failed: Recipient code from server: REFUSED
brute force file not specified, bay.
root@root: ~#
```

FIGURE 11.10: `dnsenum` performing zone transfer

**NOTE** 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).

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**.

```
root@root: ~
File Edit View Search Terminal Help
root@root: ~# dnsenum -f /usr/share/dnsenum/dns.txt 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.

```

root@root:~#
File Edit View Search Terminal Help
Trying Zone Transfers and getting Bind Versions:
Trying Zone Transfer for certifiedhacker.com on ns0.noyearlyfees.com ...
certifiedhacker.com.          3600  IN  SOA   ns0.noyearlyfees.com.
certifiedhacker.com.          3600  IN  A    202.75.54.101
certifiedhacker.com.          3600  IN  NS   ns0.noyearlyfees.com.
certifiedhacker.com.          3600  IN  MX   10
exchange.certifiedhacker.com. 3600  IN  A    202.75.54.101
ftp.certifiedhacker.com.      3600  IN  A    202.75.54.101
mail.certifiedhacker.com.     3600  IN  A    202.75.54.108
webmail.certifiedhacker.com.  3600  IN  A    202.75.54.101
www.certifiedhacker.com.     3600  IN  A    202.75.54.101

Trying Zone Transfer for certifiedhacker.com on ns3.noyearlyfees.com ...
AXFR record query failed: Response code from server: REFUSED

Brute Forcing with /usr/share/dnsenum/dns.txt

```

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:

- Enumerates the subdomains in **certifiedhacker.com** associated with IPv4 addresses
- Obtains dns-related information, as shown in the screenshot:

```

root@root:~#
File Edit View Search Terminal Help
root@root:~# dnsdict6 -d -4 certifiedhacker.com
Starting DNS enumeration work on certifiedhacker.com. ...
Gathering NS and MX Information...
NS of certifiedhacker.com. is ns0.noyearlyfees.com. => 202.75.54.100
No IPv6 address for NS entries found in DNS for domain certifiedhacker.com.
No IPv6 address for MX entries found in DNS for domain certifiedhacker.com.
No IPv4 address for MX entries found in DNS for domain certifiedhacker.com.

Starting enumerating certifiedhacker.com. - creating 8 threads for 1419 words...
Estimated time to completion: 1 to 2 minutes
ftp.certifiedhacker.com. => 202.75.54.101
mail.certifiedhacker.com. => 202.75.54.108

Found 2 domain names, 2 unique ipv4 and 0 unique ipv6 addresses for certifiedhacker.com.
root@root:~#

```

FIGURE 11.13: dnsdict – enumerating subdomains in target

**T A S K 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:

```

root@root:~# fierce -dns certifiedhacker.com
DNS Servers for certifiedhacker.com:
    ns0.noyearlyfees.com
    ns1.noyearlyfees.com
    ns2.noyearlyfees.com

Trying zone transfer first...
Testing ns0.noyearlyfees.com

Whooh, it worked - misconfigured DNS server found:
certifiedhacker.com. 3600 IN SOA ns0.noyearlyfees.com. admin.noya
36          ; Serial
960        ; Refresh
600        ; Retry
86400     ; Expire
3600      ; Minimum TTL
certifiedhacker.com. 3600 IN A 202.75.54.101
certifiedhacker.com. 3600 IN NS ns0.noyearlyfees.com.
certifiedhacker.com. 3600 IN MX 10 mail.certifiedhacker.com.
exchange.certifiedhacker.com. 3600 IN A 202.75.54.101
ftp.certifiedhacker.com. 3600 IN A 202.75.54.101
mail.certifiedhacker.com. 3600 IN A 202.75.54.101
webmail.certifiedhacker.com. 3600 IN A 202.75.54.101
www.certifiedhacker.com. 3600 IN A 202.75.54.101

There isn't much point continuing, you have everything.
Have a nice day.

```

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.

<b>Internet Connection Required</b>	
<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
<b>Platform Supported</b>	
<input checked="" type="checkbox"/> Classroom	<input type="checkbox"/> iLabs