Enumeration

Module 04

Enumeration

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

ICON KEY

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

Lab Scenario

Penetration testing is much more than just running exploits against vulnerable systems like we learned in the previous module. In fact a penetration test begins before penetration testers have even made contact with the victim systems.

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\CEHv8 Module 04 Enumeration

Lab Environment

To carry out the lab, you need:

- **Windows Server 2012** as host machine
- **Windows Server 2008, Windows 8 and Windows 7 as** virtual machine
- A web browser with an **Internet** connection
- Administrative privileges to run tools

Lab Duration

Time: 60 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.

TASK 1

Overview

Lab Tasks

Recommended labs to assist you in Enumeration:

- Enumerating a Target Network Using **Nmap** Tool
- Enumerating NetBIOS Using the **SuperScan** Tool
- Enumerating NetBIOS Using the **NetBIOS Enumerator Tool**
- Enumerating a Network Using the **SoftPerfect Network Scanner**
- Enumerating a Network Using **SolarWinds Toolset**
- Enumerating the System Using **Hyena**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

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

Lab 1

Enumerating a Target Network Using Nmap

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

As an **expert ethical hacker** and **penetration teste**r 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

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

To perform the lab, you need:

- A computer running **Windows Server 2008** as a virtual machine
- A computer running with **Windows Server 2012** as a host machine
- Nmap is located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\Additional Enumeration Pen Testing Tools\Nmap**
- Administrative privileges to install and run tools

Lab Duration

Time: 10 Minutes

Overview of Enumeration

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

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** to these hosts to gain more information
- Install and Launch **Nmap** in a Windows Server 2012 machine

TASK 1

Nbstat and Null Sessions

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

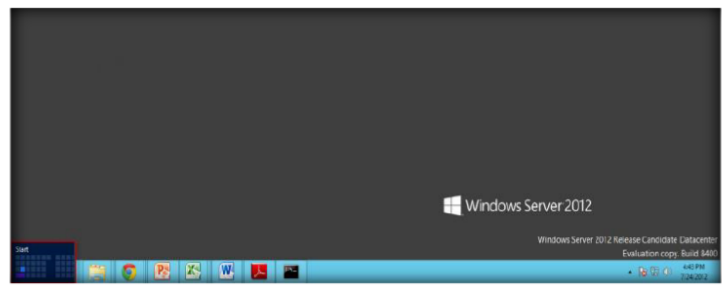


FIGURE 1.1: Windows Server 2012 – Desktop view

Zenmap file installs the following files:

- Nmap Core Files
- Nmap Path
- WinPcap 4.1.1
- Network Interface Import
- Zenmap (GUI frontend)

2. Click the **Nmap-Zenmap GUI** app to open the **Zenmap** window.

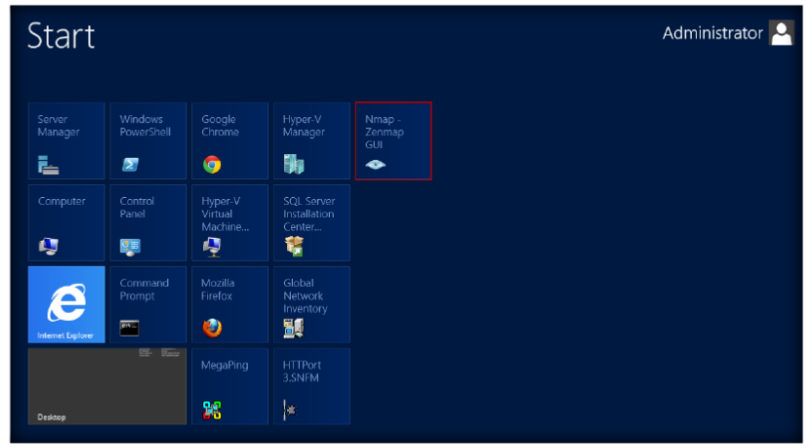


FIGURE 1.2: Windows Server 2012 – Apps

3. Start your virtual machine running **Windows Server 2008**
4. Now launch the **nmap** tool in the **Windows Server 2012** host machine.
5. Perform **nmap –O scan** for the Windows Server 2008 virtual machine (**10.0.0.6**) network. This takes a few minutes.

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

Note: IP addresses may vary in your lab environment.

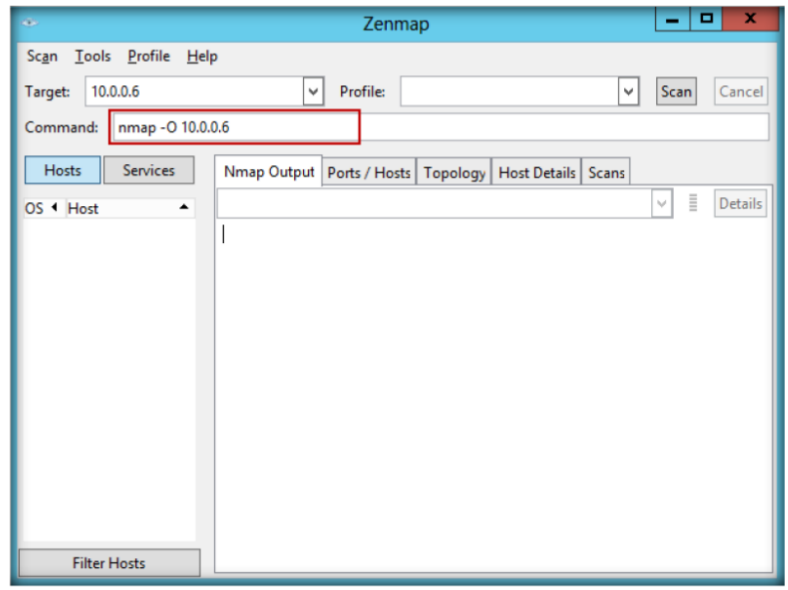


FIGURE 1.3: The Zenmap Main window

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

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

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

TASK 2

Find hosts with NetBIOS ports open

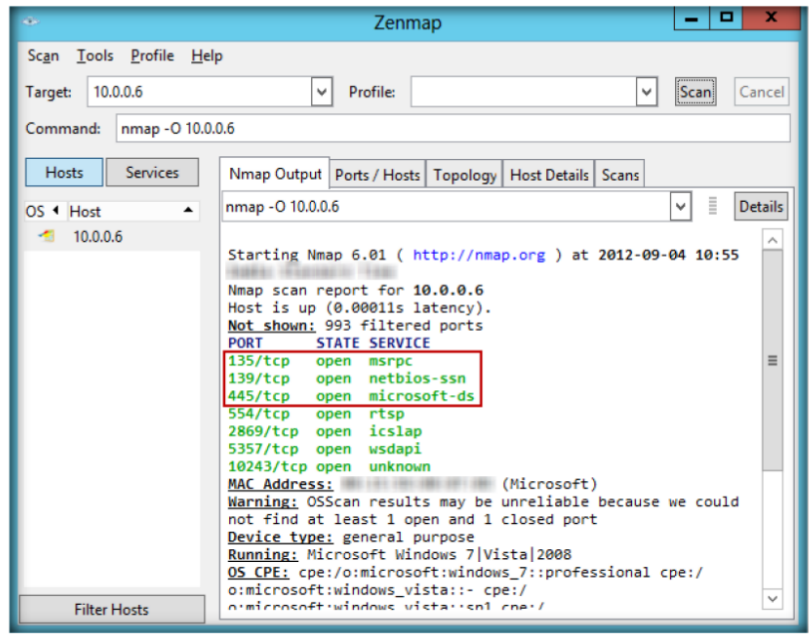


FIGURE 1.4: The Zenmap output window

8. Now you see that ports 139 and 445 are open and port **139** is using NetBIOS.
9. Now launch the **command prompt** in **Windows Server 2008** virtual machine and perform **nbtstat** on port 139 of the target machine.
10. Run the command **nbtstat –A 10.0.0.7**.

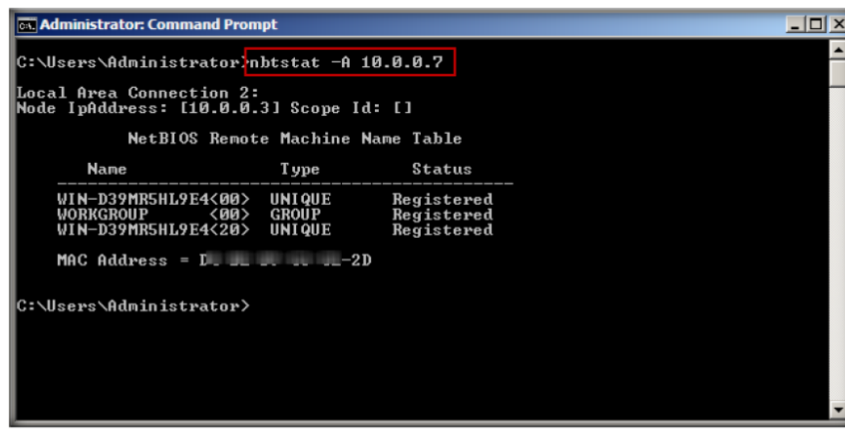


FIGURE 1.5: Command Prompt with the nbtstat command

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

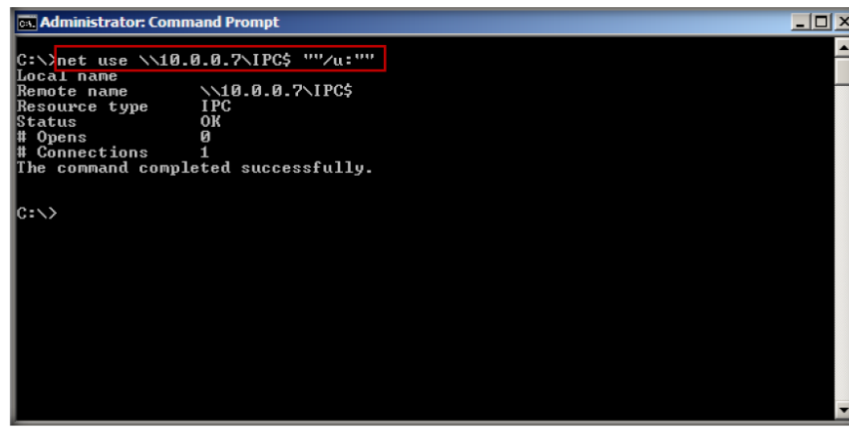
11. We have not even created a **null session** (an unauthenticated session) yet, and we can still pull this info down.

TASK 3

Create a Null Session

12. Now **create** a null session.

13. In the command prompt, type **net use \\X.X.X.X\IPC$ “” /u:””** (where **X.X.X.X** is the address of the host machine, and there are no spaces between the double quotes).



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

FIGURE 1.6: The command prompt with the net use command

14. **Confirm** it by issuing a generic **net use** command to see connected null sessions from your host.
15. To confirm, type **net use**, which should list your **newly created** null session.

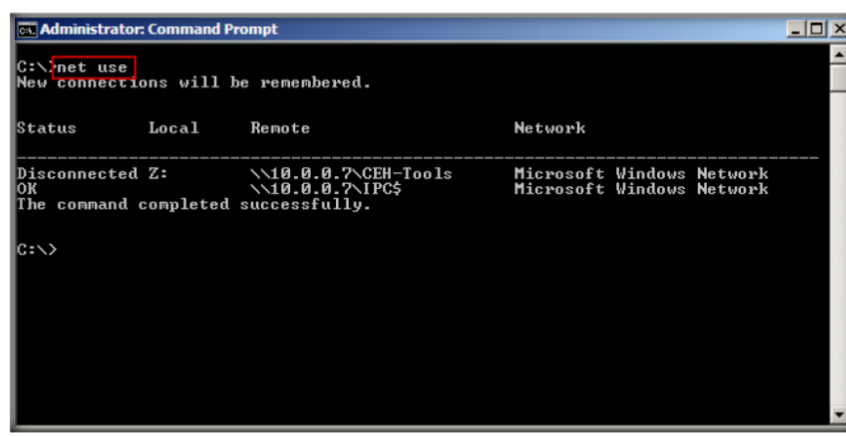


FIGURE 1.7: The command prompt with the net use command

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target’s security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
Nmap	**Target Machine:** 10.0.0.6
	List of Open Ports: 135/tcp, 139/tcp, 445/tcp, 554/tcp, 2869/tcp, 5357/tcp, 10243/tcp
	NetBIOS Remote machine IP address: 10.0.0.7
	Output: Successful connection of Null session

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

Questions

1. Evaluate what **nbtstat –A** shows us for each of the Windows hosts.
2. Determine the other options of **nbtstat** and what each option outputs.
3. Analyze the **net use** command used to establish a null session on the target machine.

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

Lab 2

Enumerating NetBIOS Using the SuperScan Tool

SuperScan is a TCP port scanner, pinger, and resolver. The tool's 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. The pen testers examine the systems in their entirety; this allows evaluating security weaknesses. In this lab we extract the information of NetBIOS information, user and group accounts, network shares, trusted domains, and services, which are either running or stopped. SuperScan detects open TCP and UDP ports on a target machine and determines which services are running on those ports; by using this, an attacker can exploit the open port and hack your machine. As an expert ethical hacker and penetration tester, you need to enumerate target networks and extract lists 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 learn and perform NetBIOS enumeration. NetBIOS enumeration is carried out to obtain:

- List of computers that belong to a domain
- List 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\CEHv8 Module 04 Enumeration

To carry out the lab, you need:

- SuperScan tool is located at **D:\CEH-Tools\CEHv8 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** running on a virtual machine as target machine
- Administrative privileges to install and run tools
- A web browser with an Internet connection

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

Lab Duration

Time: 10 Minutes

Overview of NetBIOS Enumeration

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

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

Lab Tasks

TASK 1

Perform Enumeration

1. Double-click the **SuperScan4** file. The **SuperScan** window appears.

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

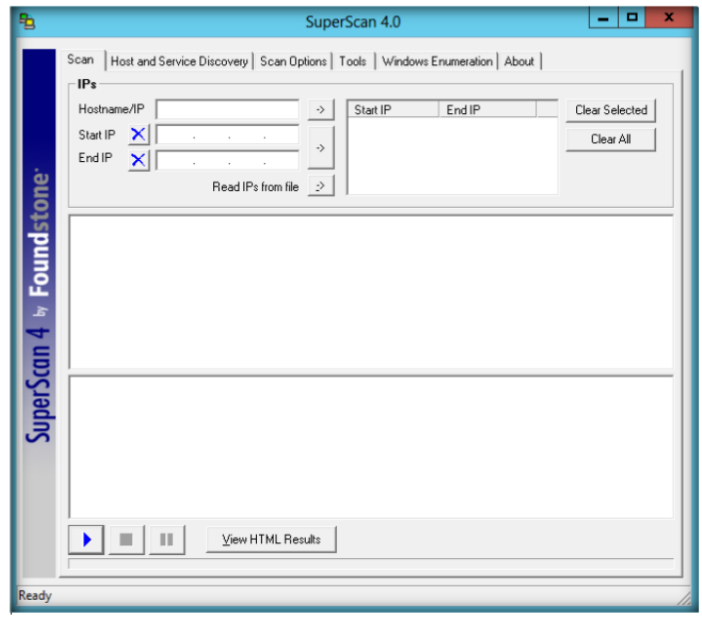


FIGURE 2.1: SuperScan main window

SuperScan features:

- Superior scanning speed
- Support for unlimited IP ranges
- Improved host detection using multiple ICMP methods
- TCP SYN scanning
- UDP scanning (two methods)
- IP address import supporting ranges and CIDR formats
- Simple HTML report generation
- Source port scanning
- Fast hostname resolving
- Extensive banner grabbing
- Massive built-in port list description database
- IP and port scan order randomization
- A collection of useful tools (ping, traceroute, Whois etc.)
- Extensive Windows host enumeration capability

2. Click the **Windows Enumeration** tab located on the top menu.
3. Enter the **Hostname/IP/URL** in the text box. In this lab, we have a Windows 8 virtual machine IP address. These IP addresses may vary in lab environments.
4. Check the types of **enumeration** you want to perform.
5. Now, click **Enumerate**.

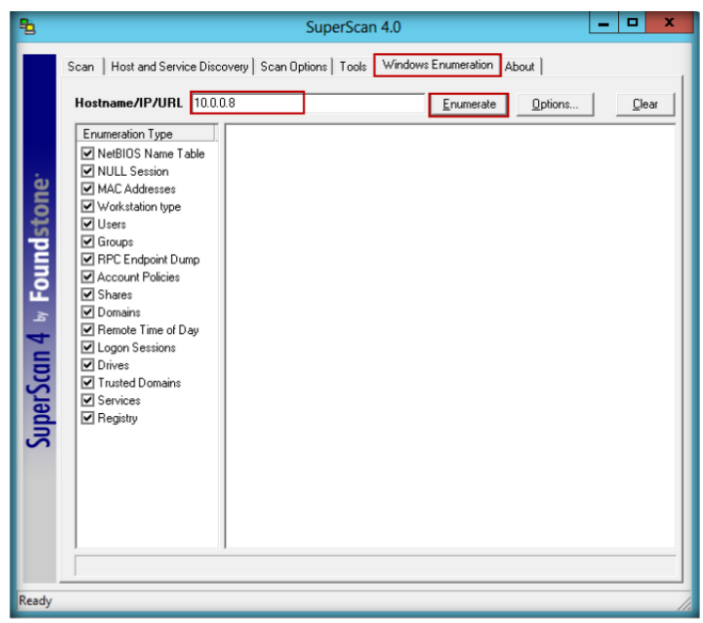


FIGURE 2.2: SuperScan main window with IP address

6. SuperScan starts **enumerating** the provided hostname and displays the **results** in the right pane of the window.

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

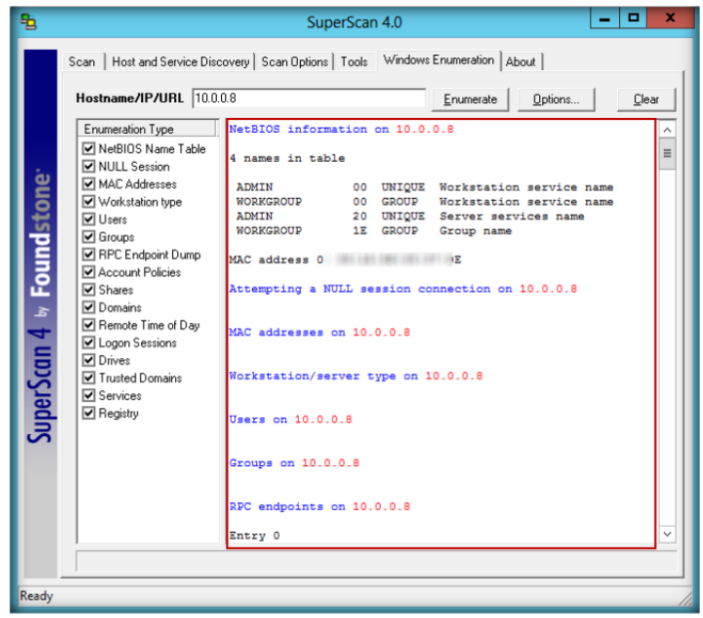


FIGURE 2.3: SuperScan main window with results

7. Wait for a while to **complete** the enumeration process.
8. After the completion of the enumeration process, an **Enumeration completion** message displays.

Your scan can be configured in the Host and Service Discovery and Scan Options tabs. The Scan Options tab lets you control such things as name resolution and banner grabbing.

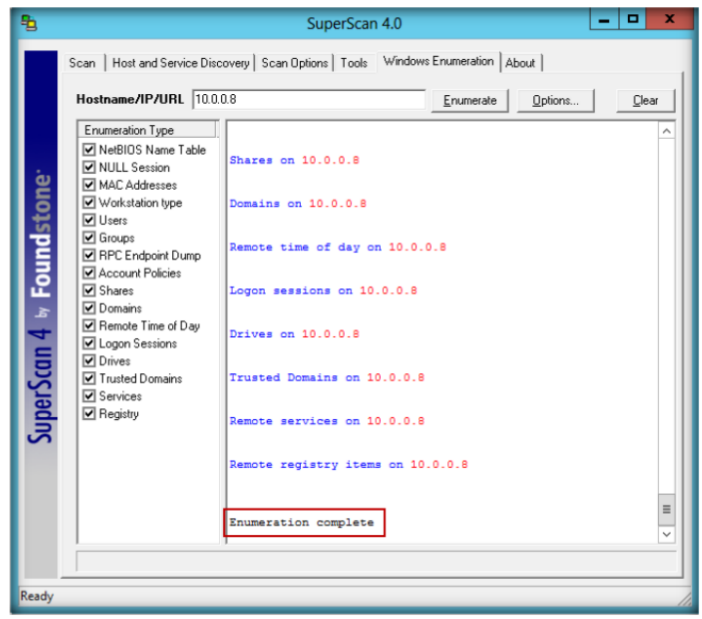


FIGURE 2.4: SuperScan main window with results

9. Now move the scrollbar up to see the **results** of the enumeration.

TASK 2

Erase Results

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

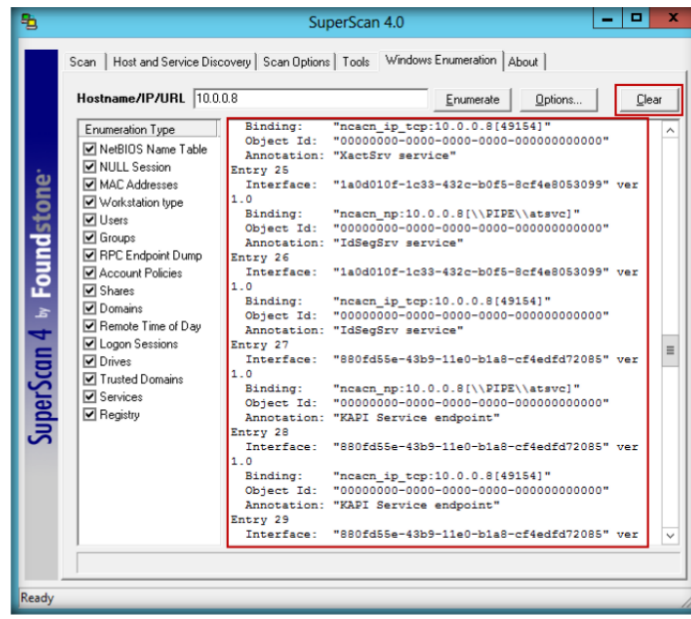


FIGURE 2.5: SuperScan main window with results

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

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
SuperScan Tool	**Enumerating Virtual Machine IP address:** 10.0.0.8
	Performing Enumeration Types: ▪ Null Session ▪ MAC Address ▪ Work Station Type ▪ Users ▪ Groups ▪ Domain ▪ Account Policies ▪ Registry
	Output: Interface, Binding, Objective ID, and Annotation

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

Questions

1. Analyze how remote registry enumeration is possible (assuming appropriate access rights have been given) and is controlled by the provided registry.txt file.
2. As far as stealth is concerned, this program, too, leaves a rather large footprint in the logs, even in SYN scan mode. Determine how you can avoid this footprint in the logs.

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

Lab 3

Enumerating NetBIOS Using the NetBIOS Enumerator Tool

Enumeration is the process of probing identified services for known weaknesses.

ICON KEY

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

Lab Scenario

Enumeration is the first attack on a target network; enumeration is the process of gathering the information about a target machine by actively connecting to it. Discover NetBIOS name enumeration with NBTscan. Enumeration means to identify the user account, system account, and admin account. In this lab, we enumerate a machine's user name, MAC address, and domain group. 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.

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
- To restrict anonymous bypass routine and also password checking for user accounts with:
  - Blank passwords
  - Passwords that are same as the username in lower case

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

Lab Environment

To carry out the lab, you need:

- NETBIOS Enumerator tool is located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator**
- You can also download the latest version of **NetBIOS Enumerator** from the link http://nbtenum.sourceforge.net/
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Run this tool in **Windows Server 2012**
- Administrative privileges are required to run this tool

Lab Duration

Time: 10 Minutes

Overview of Enumeration

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

Lab Tasks

TASK 1

Performing Enumeration using NetBIOS Enumerator

1. To launch NetBIOS Enumerator go to **D:\CEH-Tools\CEHv8 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator**, and double-click **NetBIOS Enumerater.exe**.

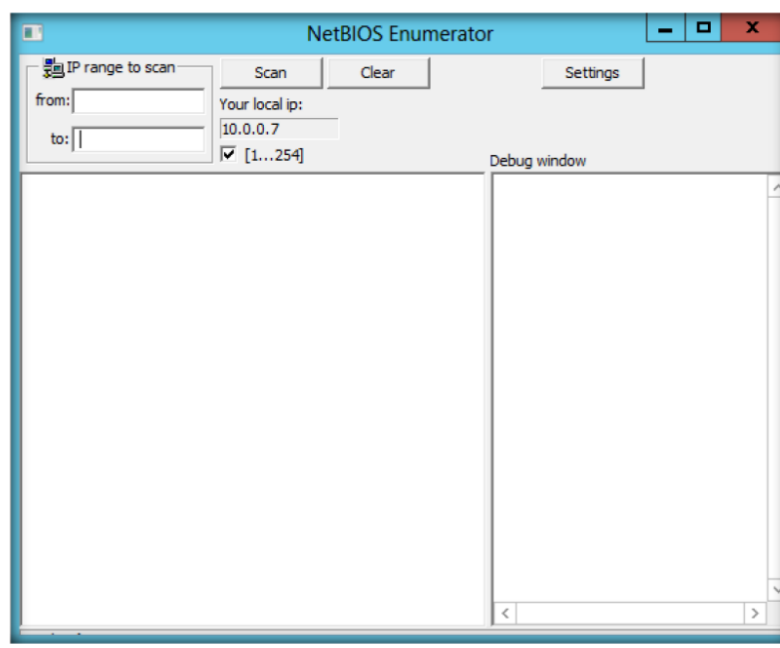


FIGURE 3.1: NetBIOS Enumerator main window

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

2. In the **IP range to scan** section at the top left of the window, enter an **IP range** in **from** and **to** text fields.
3. Click **Scan**.

Feature:

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

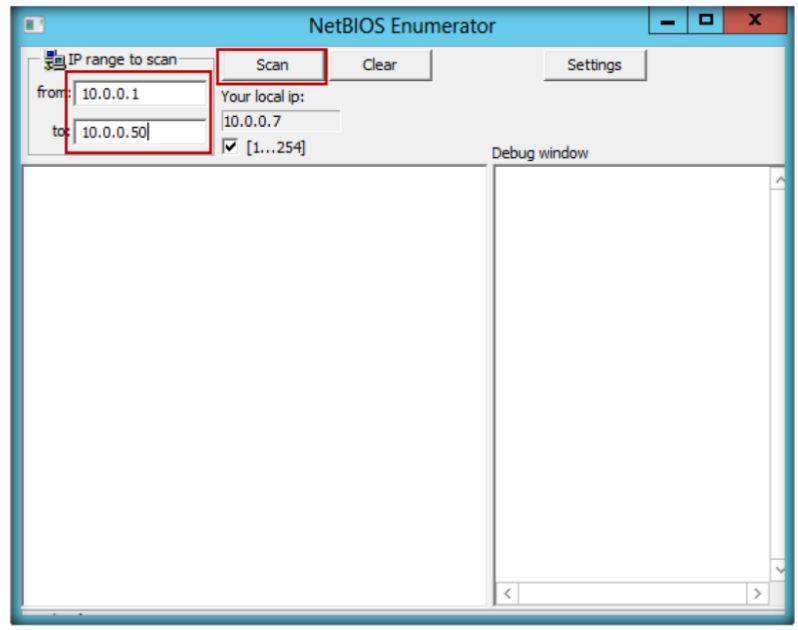


FIGURE 3.2: NetBIOS Enumerator with IP range to scan

Network function SMB scanning is also implemented and running.

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

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

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

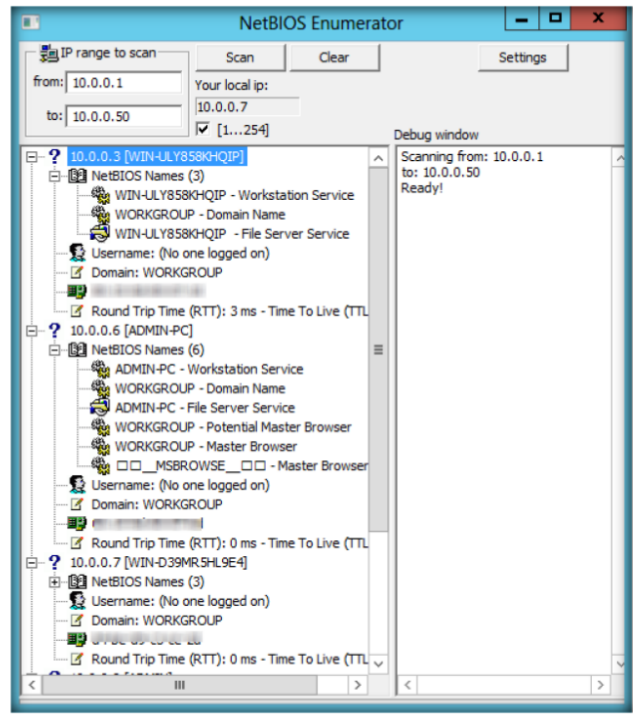


FIGURE 3.3: NetBIOS Enumerator results

7. To perform a **new scan** or rescan, click **Clear**.
8. If you are going to perform a new scan, the previous scan results are **erased**.

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
NetBIOS Enumerator Tool	**IP Address Range:** 10.0.0.1 – 10.0.0.50 **Result:** ▪ Machine Name ▪ NetBIOS Names ▪ User Name ▪ Domain ▪ MAC Address ▪ Round Trip Time (RTT)

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

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

Lab 4

Enumerating a Network Using SoftPerfect Network Scanner

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

ICON KEY

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

Lab Scenario

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

Lab Objectives

The objective of this lab is to help students learn and perform NetBIOS enumeration. NetBIOS enumeration 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\CEHv8 Module 04 Enumeration

Lab Environment

To carry out the lab, you need:

- SoftPerfect Network Scanner is located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner**
- 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
- Run this tool in **Windows 2012 server**
- Administrative privileges are required to run this tool

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

Lab Duration

Time: 5 Minutes

Overview of Enumeration

Enumeration involves an **active connection** so that it can be logged. Typical information that attackers are looking for includes user **account names** for future password-guessing attacks.

Lab Task

TASK 1

Enumerate Network

1. To launch SoftPerfect Network Scanner, navigate to **D:\CEH-Tools\CEHv8 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner**
2. Double-click **netscan.exe**

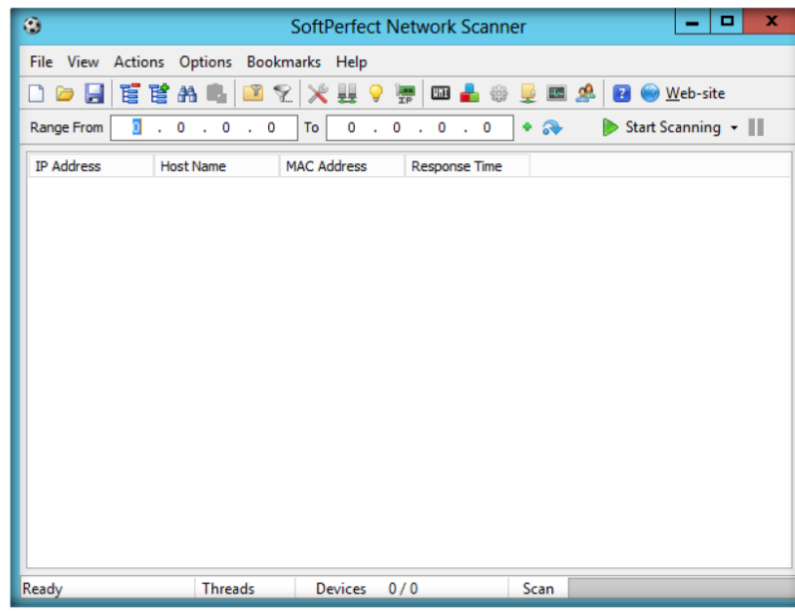


FIGURE 4.1: SoftPerfect Network Scanner main window

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

3. To start scanning your network, enter an IP range in the **Range From** field and click **Start Scanning**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

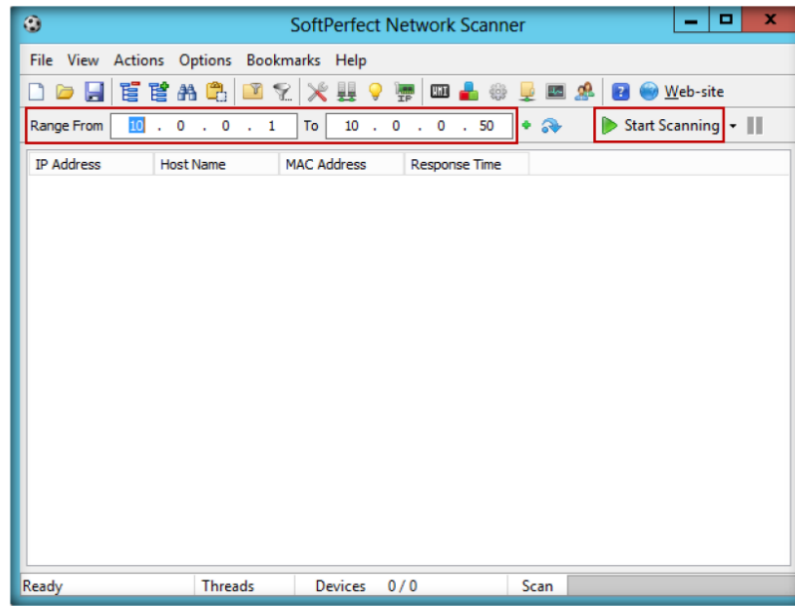


FIGURE 4.2: SoftPerfect setting an IP range to scan

4. The **status bar** displays the status of the scanned IP addresses at the bottom of the window.

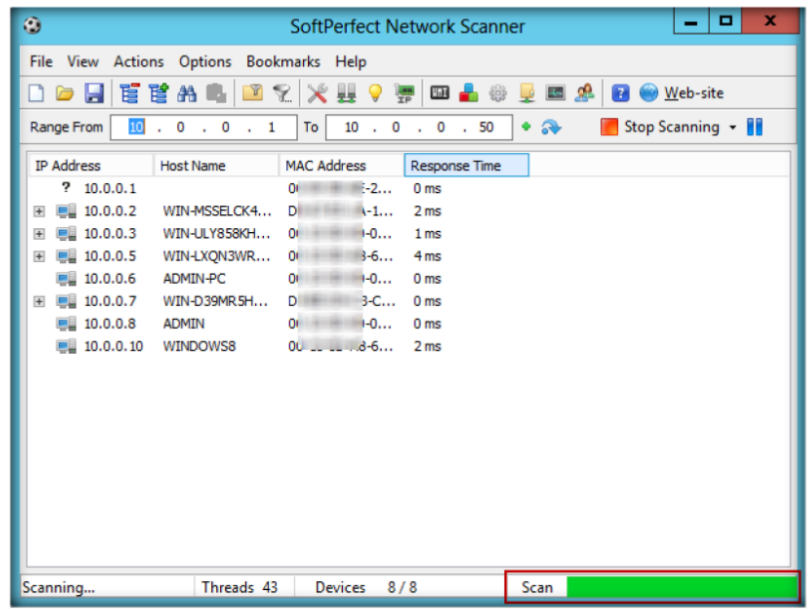


FIGURE 4.3: SoftPerfect status bar

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

5. To view the **properties** of an individual **IP address**, right-click that particular IP address.

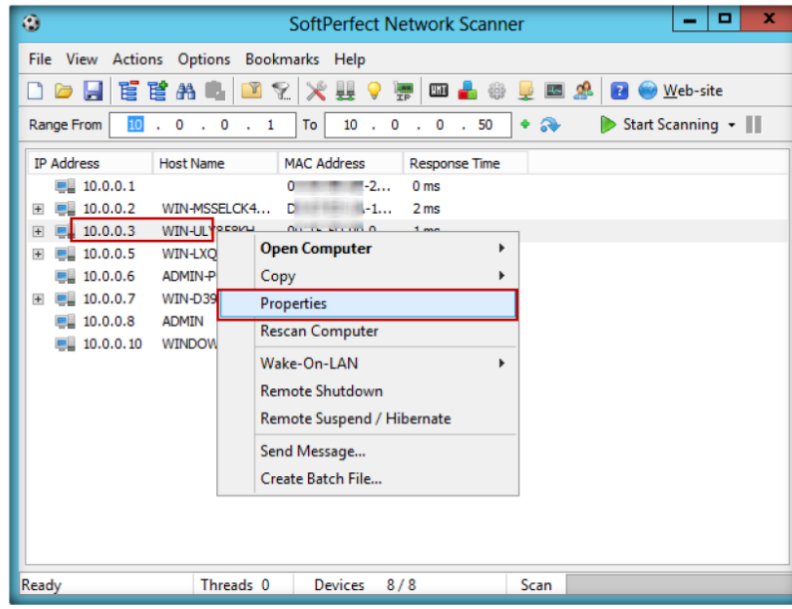


FIGURE 4.4: SoftPerfect IP address scanned details

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
SoftPerfect Network Scanner	**IP Address Range:** 10.0.0.1 – 10.0.0.50
	Result: ▪ IP Address ▪ Host Names ▪ MAC Address ▪ Response Time

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

Questions

1. Examine the detection of the IP addresses and MAC addresses across routers.

2. Evaluate the scans for listening ports and some UDP and SNMP services.

3. How would you launch external third-party applications?

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

Lab 5

Enumerating a Network Using SolarWinds Toolset

The SolarWinds Toolset provides the tools you need as a network engineer or network consultant to get your job done. Toolset includes best-of-breed solutions that work simply and precisely, providing the diagnostic, performance, and bandwidth measurements you want, without extraneous, unnecessary features.

ICON KEY

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

Lab Scenario

Penetration testing is much more than just running exploits against vulnerable systems like we learned in the previous module. In fact a penetration test begins before penetration testers have even made contact with the victim systems. Rather than blindly throwing out exploits and praying that one of them returns a shell, penetration tester meticulously study the environment for potential weaknesses and their mitigating factors. By the time a penetration tester runs an exploit, he or she is nearly certain that it will be successful. Since failed exploits can in some cases cause a crash or even damage to a victim system, or at the very least make the victim un-exploitable in the future, penetration testers won't get the best results. In this lab we enumerate target system services, accounts, hub ports, TCP/IP network, and routes. 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.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

Lab Objectives

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

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

Lab Environment

To carry out the lab, you need:

- **SolarWinds-Toolset-V10** located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\SNMP Enumeration Tools\SolarWind's IP Network Browser**
- You can also download the latest version of **SolarWinds Toolset Scanner** from the link http://www.solarwinds.com/
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Run this tool in **Windows Server 2012** Host machine and **Windows Server 2008** virtual machine
- Administrative privileges are required to run this tool
- Follow the **wizard-driven** installation instructions

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

Lab Duration

Time: 5 Minutes

Overview of Enumeration

Enumeration involves an **active connection** so that it can be logged. Typical information that attackers are looking for includes user **account names** for future password guessing attacks.

Lab Task

TASK 1

Enumerate Network

1. Configure **SNMP services** and select **Start → Control Panel → Administrative Tools → Services**.

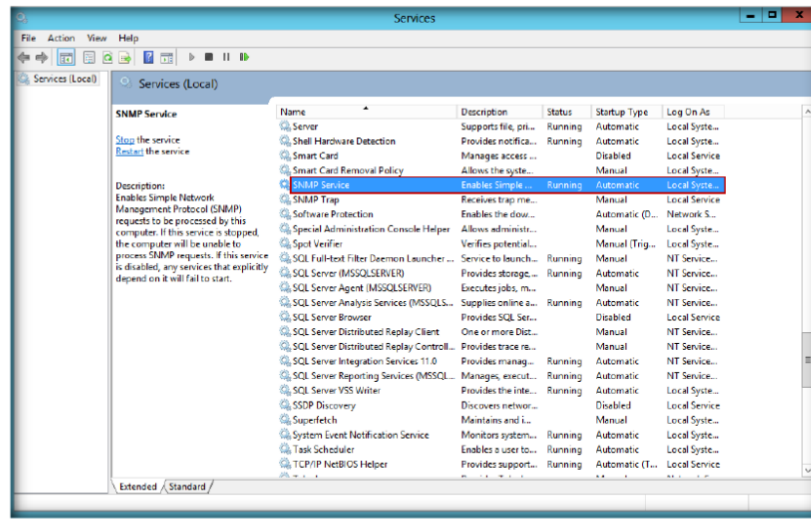


FIGURE 5.1: Setting SNMP Services

Cut troubleshooting time in half using the Workspace Studio, which puts the tools you need for common situations at your fingertips

2. Double-click **SNMP** service.
3. Click the **Security** tab, and click **Add...** The **SNMP Services Configuration** window appears. Select **READ ONLY** from **Community rights** and **Public** in **Community Name**, and click **Add**.

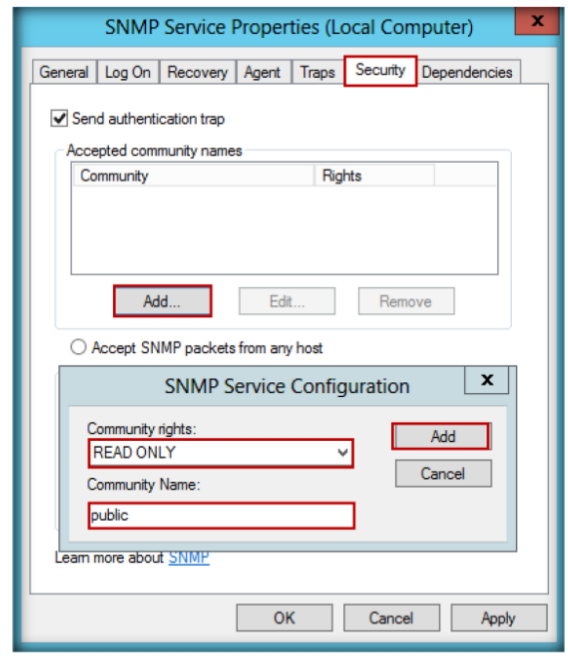


FIGURE 5.2: Configuring SNMP Services

Monitor and alert in real time on network availability and health with tools including Real-Time Interface Monitor, SNMP Real-Time Graph, and Advanced CPU Load

4. Select **Accept SNMP packets from any host**, and click **OK**.

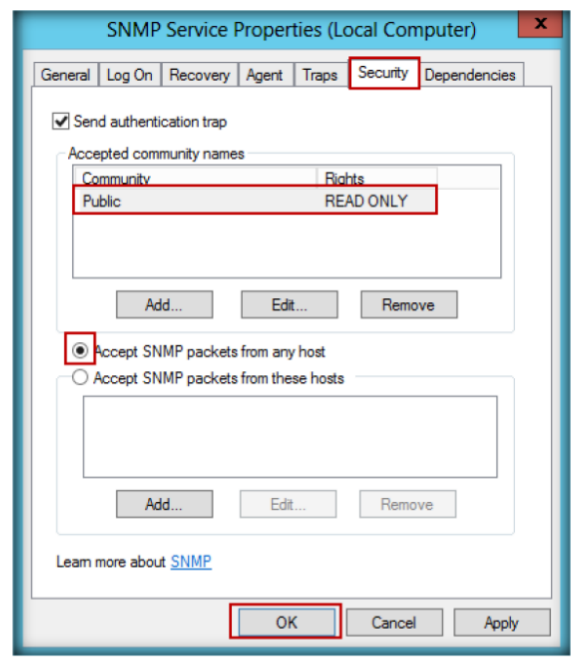


FIGURE 5.3: setting SNMP Services

5. Install **SolarWinds-Toolset-V10**, located in **D:\CEH-Tools\CEHv8 Module 04 Enumeration\SNMP Enumeration Tools\SolarWind's IP Network Browser**.
6. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

FIGURE 5.4: Windows Server 2012 – Desktop view

Perform robust network diagnostics for troubleshooting and quickly resolving complex network issues with tools such as Ping Sweep, DNS Analyzer, and Trace Route

7. Click the **Workspace Studio** app to open the **SolarWinds Workspace Studio** window.

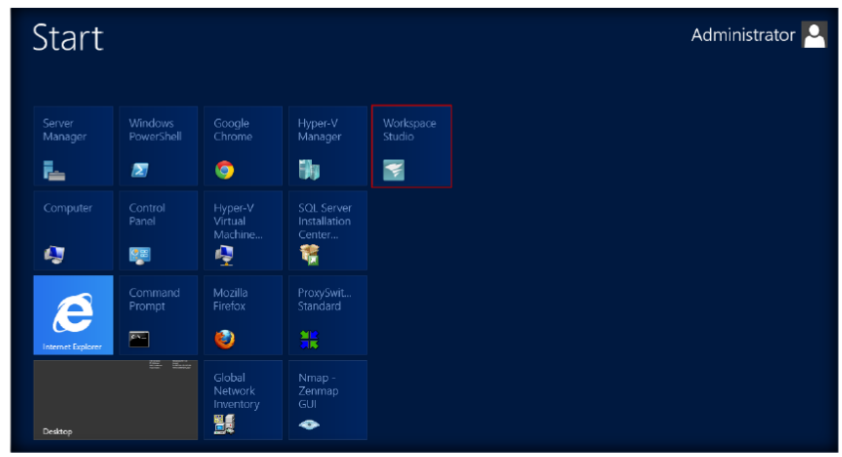


FIGURE 5.5: Windows Server 2012 – Apps

6. The main window of **SolarWinds Workspace Studio** is shown in the following figure.

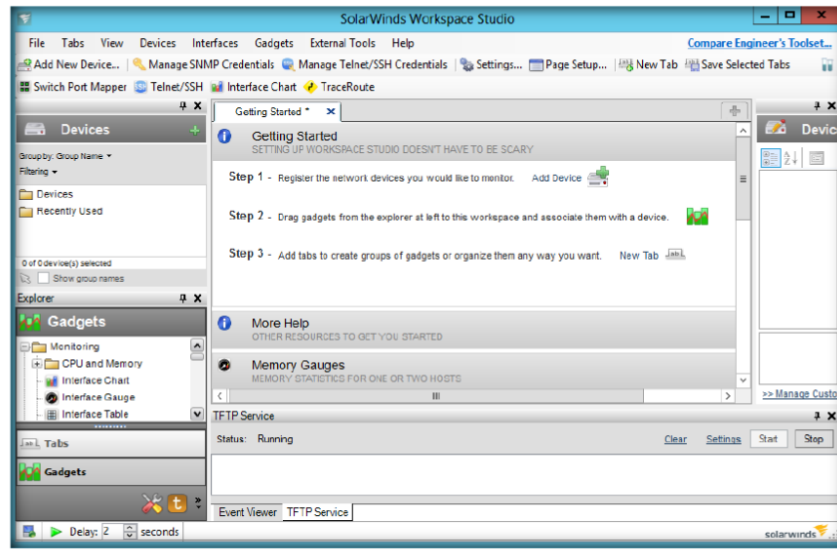


FIGURE 5.6 Solarwinds workspace studio main window

7. Click **External Tools**, and then select **Classic tools → Network Discovery → IP Network Browser**.

Deploy an array of **network discovery tools** including Port Scanner, Switch Port Mapper, and Advanced Subnet Calculator.

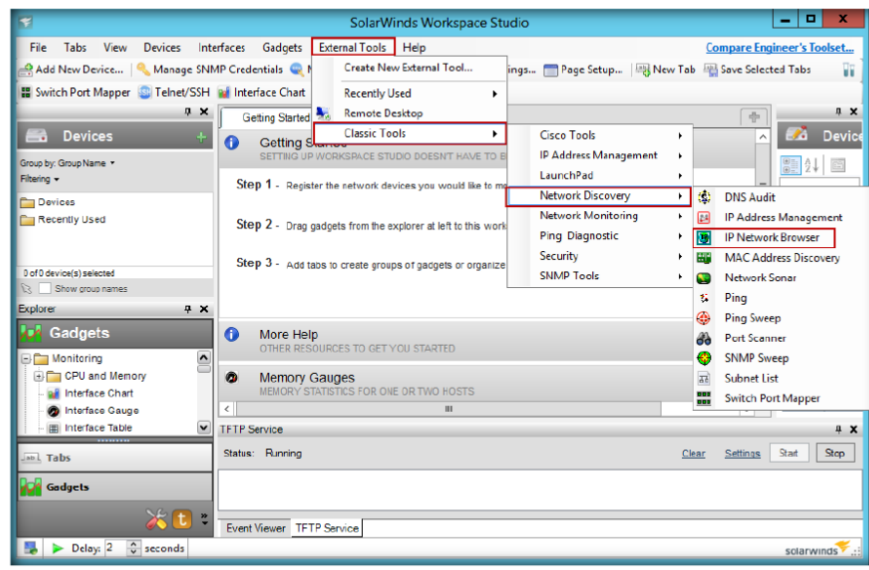


FIGURE 5.7: Menu Escalation for IP network browser

8. **IP Network Browser** will be shown. Enter the **Windows 8 Virtual Machine IP address (10.0.0.7)** and click **Scan Device** (the IP address will be different in your network).

SolarWinds Toolset applications use several methods to collect data about the health and performance of your network, including ICMP, SNMPv3, DNS and Syslog. Toolset does NOT require deployment of proprietary agents, appliances, or garden gnomes on the network.

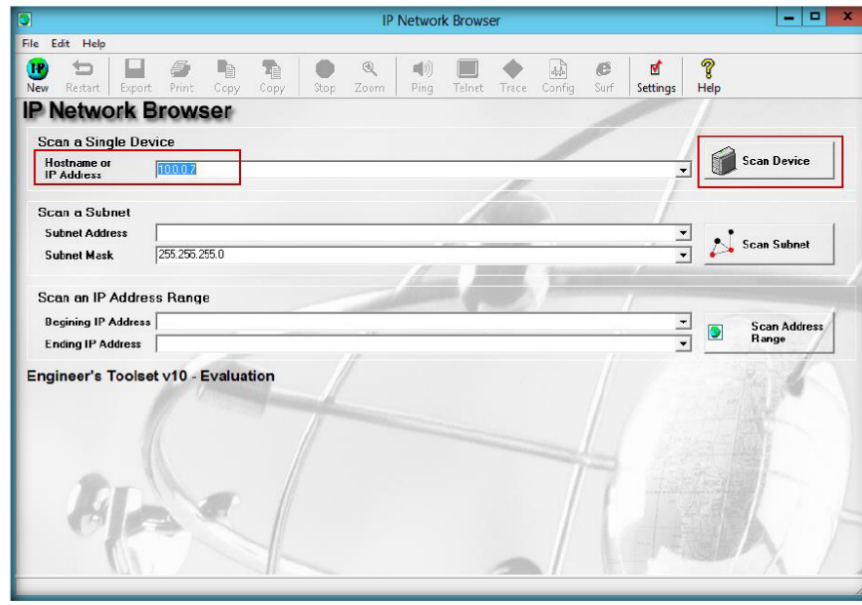


FIGURE 5.8: IP Network Browser windows

9. It will show the result in a line with the **IP address** and name of the computer that is being scanned.
10. Now click the **Plus (+)** sign before the IP address.

NetFlow Realtime is intended for granular, real-time troubleshooting and analysis of NetFlow statistics on single interface and is limited to a 1 hour capture

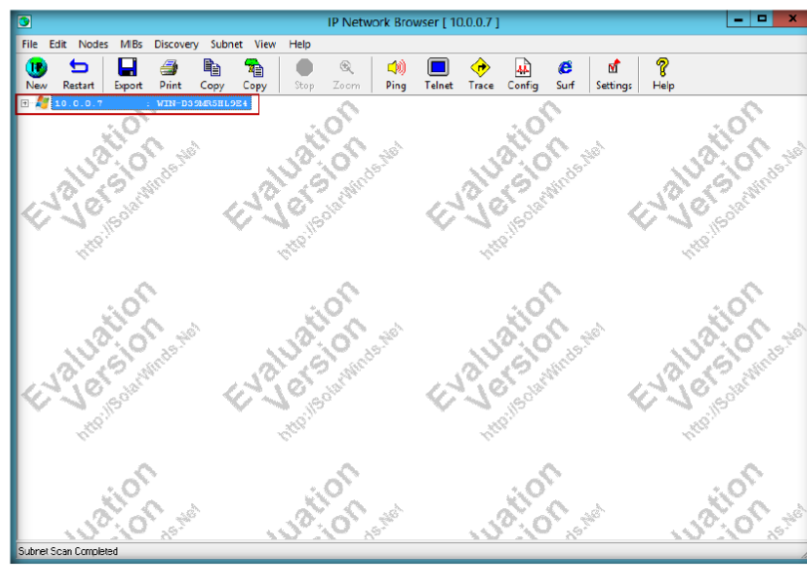


FIGURE 5.9: IP Network Browser windows results page

11. It will list all the information of the targeted IP address.

🗁 To start a new tab, go to 'tabs' on the menu bar and choose 'new tab.' Right-click on a tab to bring up options (Import, Export, Rename, Save, Close). You can add tools to tabs from the Gadgets box in the lower left or directly from the gadgets menu. A good way to approach it is to collect all the tools you need for a given task (troubleshooting Internet connectivity, for example) on one tab. Next time you face that situation simply open that tab

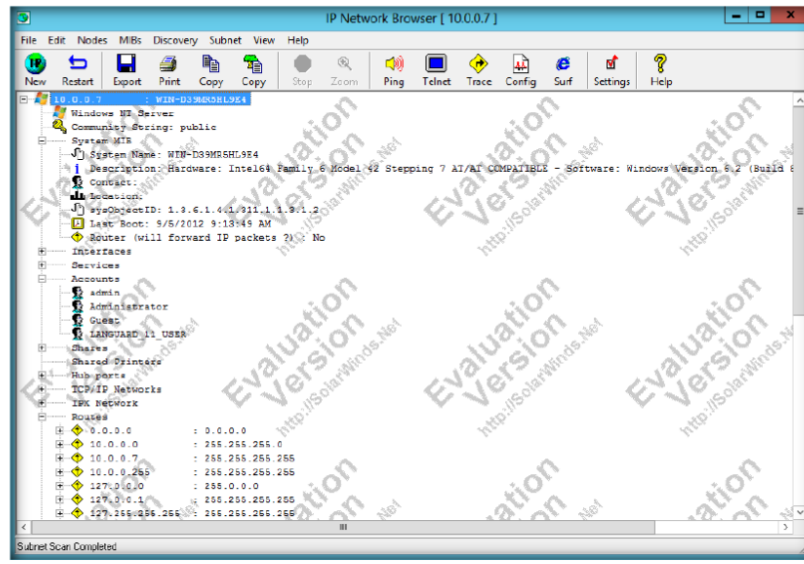


FIGURE 5.10: IP Network Browser windows results page

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
SolarWinds Tool Set	**Scan Device IP Address:** 10.0.0.7 **Output:** ▪ Interfaces ▪ Services ▪ Accounts ▪ Shares ▪ Hub Ports ▪ TCP/IP Network ▪ IPX Network ▪ Routes

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

Questions

1. Analyze the details of the system such as user accounts, system MSI, hub ports, etc.

2. Find the IP address and Mac address of the system.

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

Lab 6

Enumerating the System Using Hyena

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

ICON KEY

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

Lab Scenario

The hacker enumerates 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 (both 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:

- Users information in the system
- Services running in the system

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

Lab Environment

To perform the 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 decided to download latest version of this tool screenshots may differ

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:

TASK 1

Installation of Hyena

1. Navigate to **D:\CEH-Tools\CEHv8 Module 04 Enumeration\NetBIOS Enumeration Tools\Hyena**
2. Double-click **Hyena_English_x64.exe**. You can see the following window. Click **Next**.

You can download the Hyena from *http://www.systemtools.com/hyena/hyena_new.htm*

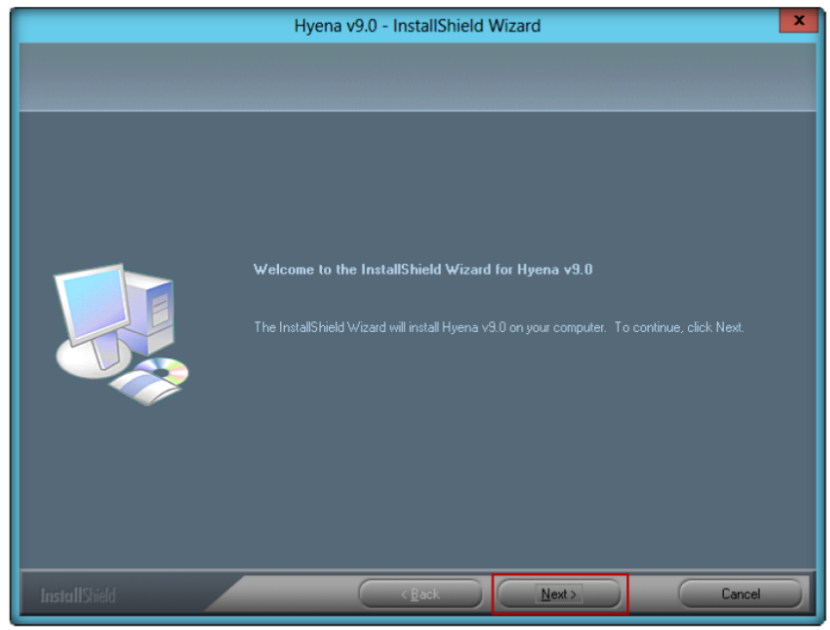


FIGURE 6.1: Installation of Hyena

3. The **Software License Agreement** window appears, you must accept the agreement to install Hyena.
4. Select **I accept the terms of the license agreement** to continue and click **Next**.

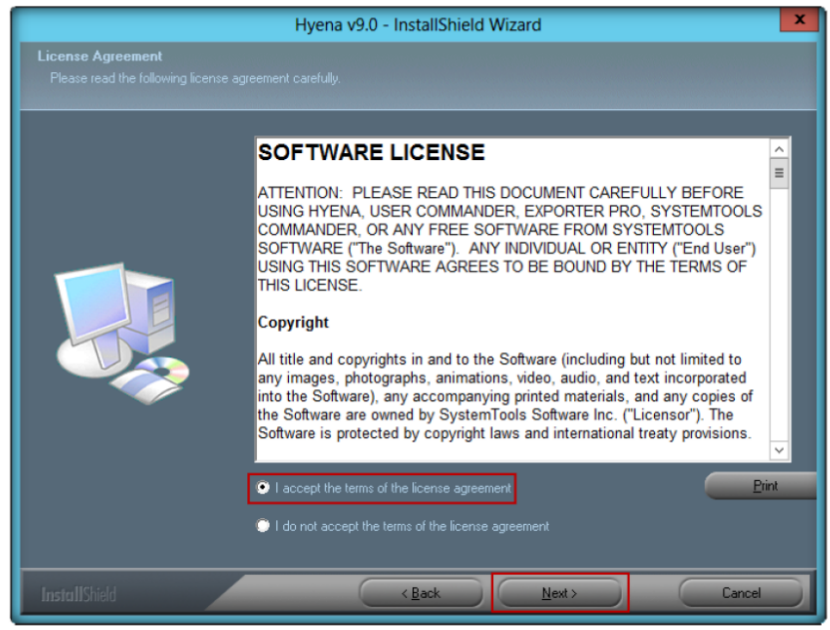


FIGURE 6.2: Select the Agreement

5. Choose the **destination location** to install Hyena.
6. Click **Next** to continue the installation.

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

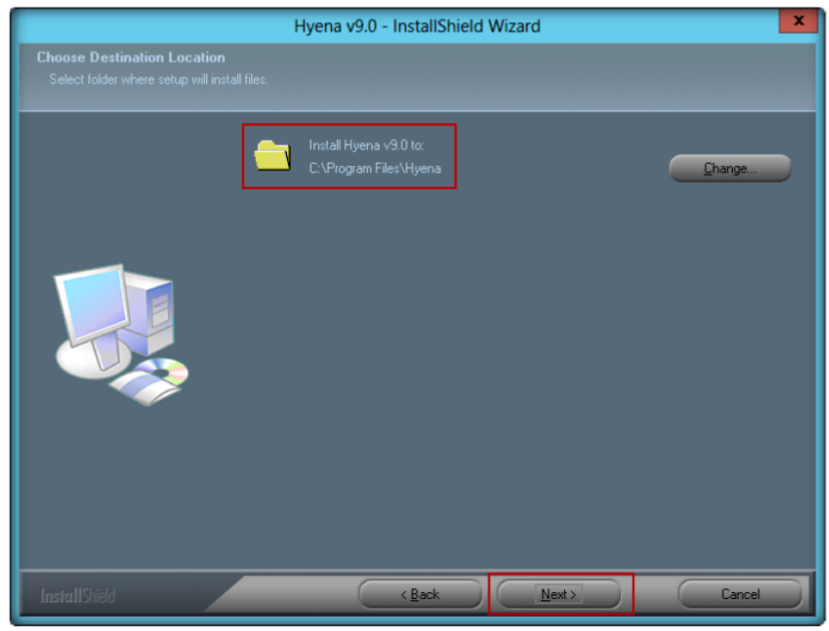


FIGURE 6.3: Selecting folder for installation

7. The **Ready to install the Program** window appears. Click **Install**.

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

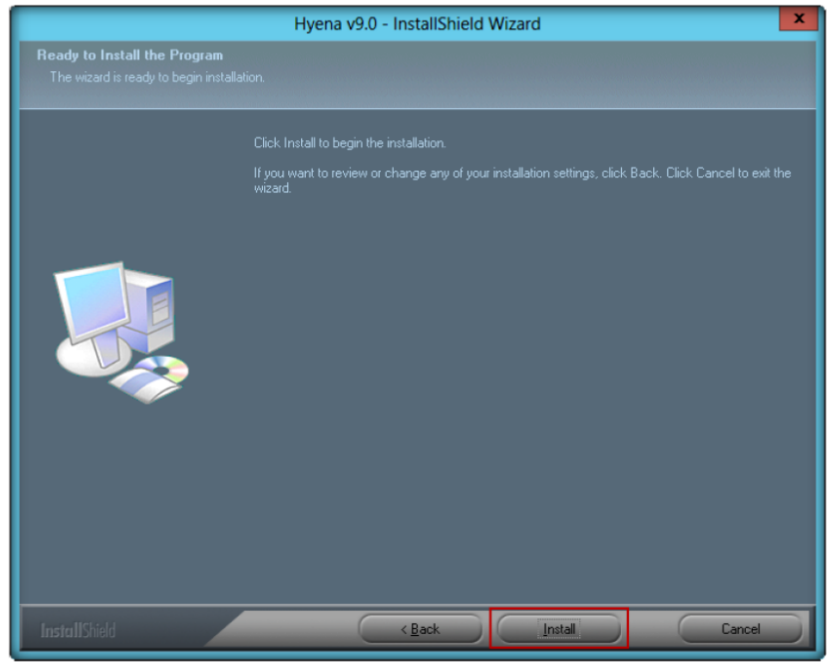


FIGURE 6.4: selecting installation type

8. The **InstallShield Wizard complete** window appears. Click **Finish** to complete the installation.

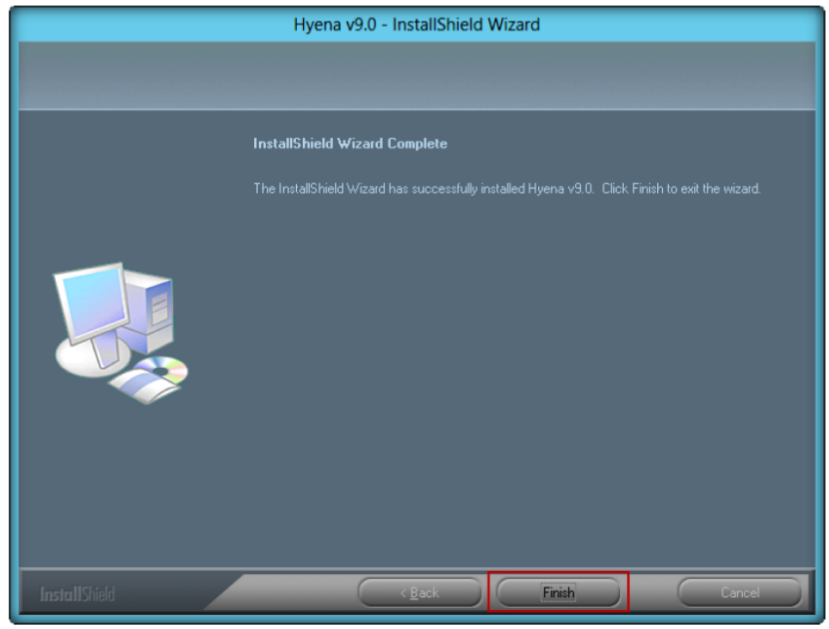


FIGURE 6.5: Ready to install window

TASK 2

Enumerating system Information

9. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

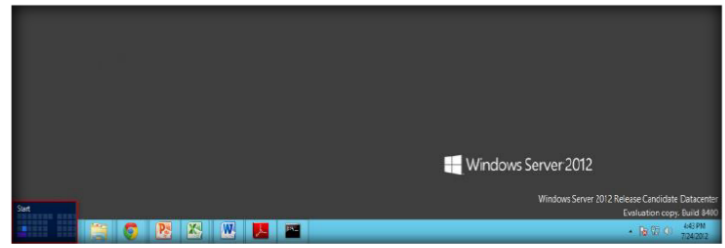


FIGURE 6.6: Windows Server 2012 – Desktop view

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

10. Click the **Hyena** app to open the **Hyena** window.

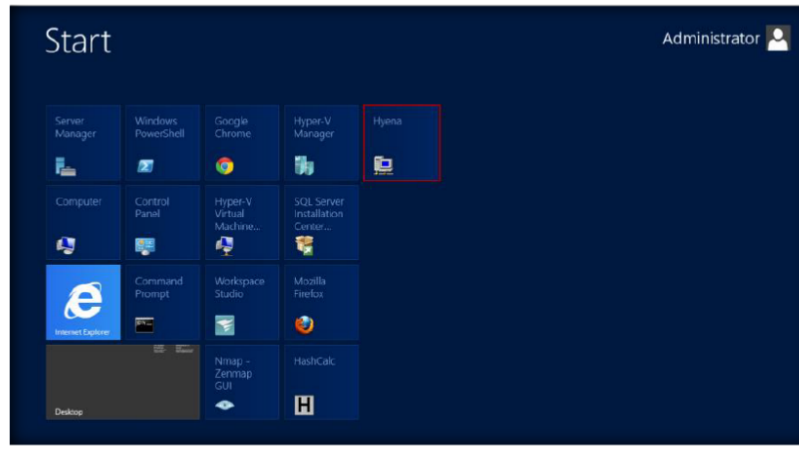


FIGURE 6.7: Windows Server 2012 – Apps

11. The **Registration** window will appear. Click **OK** to continue.
12. The main window of **Hyena** is shown in following figure.

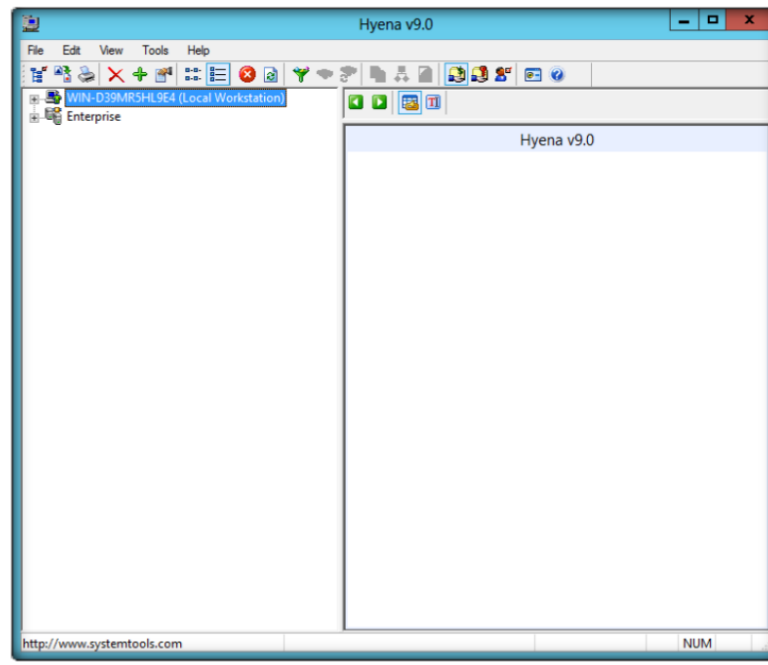


FIGURE 6.8: Main window of Hyena

13. Click **+** to expand **Local workstation**, and then click **Users**.

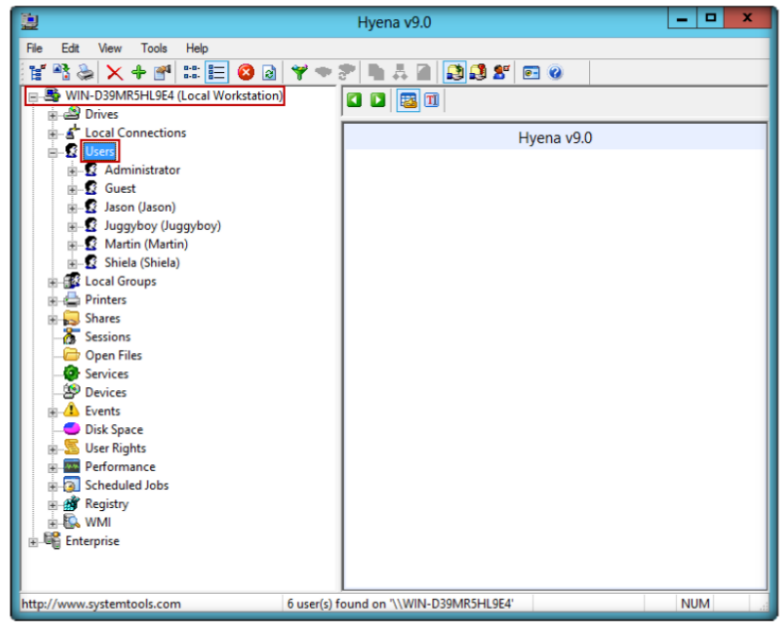


FIGURE 6.9: Expand the System users

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

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

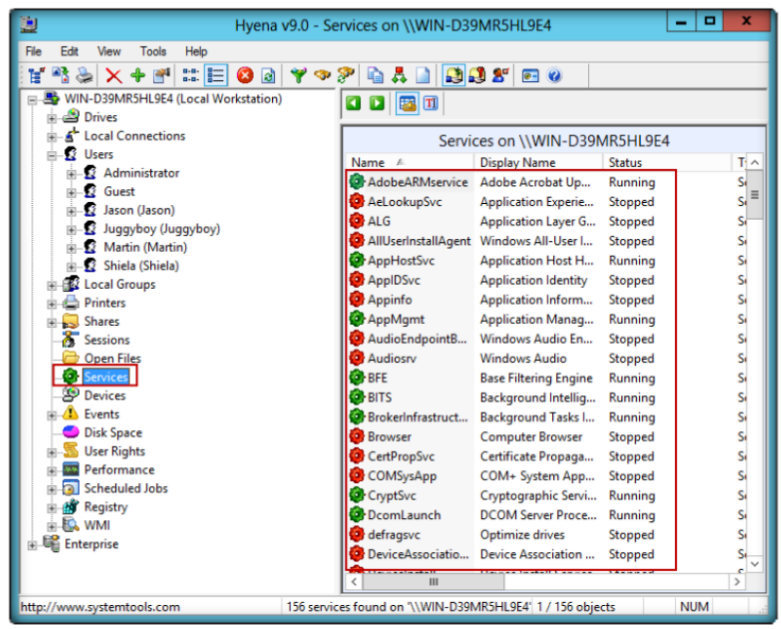


FIGURE 6.10: Services running in the system

15. To check the **User Rights**, click **+** to expand it.

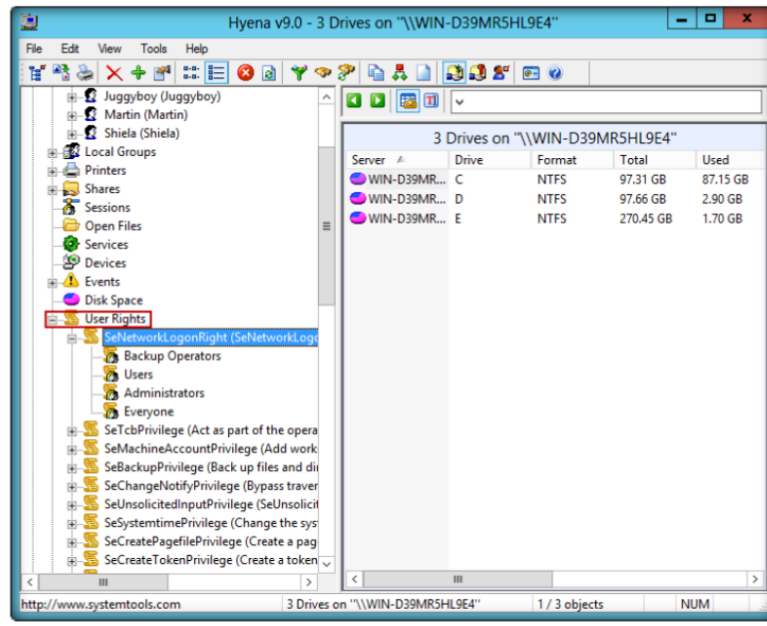


FIGURE 6.11: Users Rights

16. To check the **Scheduled jobs**, click **+** to expand it.

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

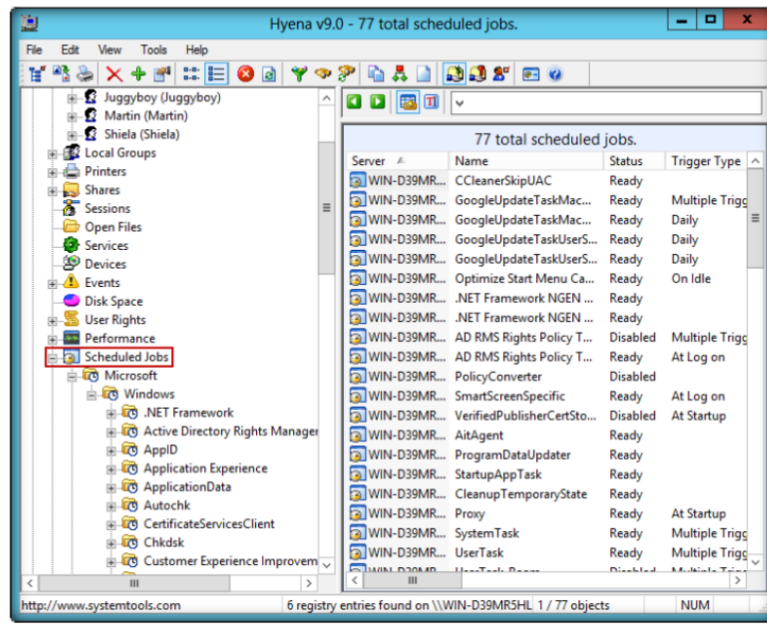


FIGURE 6.12: Scheduled jobs

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
Hyena	**Intention :** Enumerating the system
	Output: ▪ Local Connections ▪ Users ▪ Local Group ▪ Shares ▪ Shares ▪ Sessions ▪ Services ▪ Events ▪ User Rights ▪ Performance ▪ Registry ▪ WMI

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

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