Module 05

Enumeration

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.

ICON KEY


Important Information

Quiz


CPTE Labs


Course Review

Enumeration means to identify the user account, system account and admin account. We find out this information by enumerating Windows' active directory.

Discover NetBIOS name enumeration by using NBTscan and establishing null sessions and connections. Null session tools like Dumpsec, Winfo, Sid2User and more may be used to perform this attack.

Lab Objectives

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

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

Lab Scenario

You have proven yourself a quick study and your boss has asked you to continue your great work. Now that you have found the targets and open ports, you have been asked to find some additional information regarding those targets. We are not ready to exploit yet, just find more information; please stay within the scope of work on this module.

As an expert ethical hacker and penetration testing engineer, 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 Environment

This lab requires:

- **Windows 7**
- **Kali Linux VM**
- A Firefox web browser with Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 60 Minutes

Overview of Enumeration

The enumeration phase is the phase where the information of the reconnaissance phase will be in use the first time. The enumeration procedure impacts, for example, active actions taken by cyber attackers to gain system access and, of course, the important attack vectors or schemes. Information and data captured through the reconnaissance phase build a review and overview about the target company. In special test cases or topics, the captured information plays a significant role in the enumeration or exploitation phase.

During the enumeration phase, date and information will be systematically captured or tracked. In special cases, individual systems, infrastructures or environments are completely identified by our security team during the enumeration phase simulation.

Lab Tasks

Recommended labs to assist you in Enumeration:

- **Lab 1: Enumerating a Target Network Using ZeNmap Tool**
- **Lab 2: Make use of the telnet utility to perform banner grabbing**
- **Lab 3: Enumerating NetBIOS Using the SuperScan Tool**
- **Lab 4: Enumerating NetBIOS Using the NetBIOS Enumerator Tool**
- **Lab 5: Enumerating system using Hyena tools**
- **Lab 6. Perform SMTP Enumeration**

Lab Analysis

Analyze and document the results related to the lab. Give your opinion on your target's security posture and exposure through public and free information.

Lab 1

Scanning a Target Using Zenmap Tools

ZeNmap Overview

Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

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 pentesters examine the systems in their entirety, which allows evaluating 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 biters/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 attack on a network filled with IP filters, firewalls and other obstacles.

Your goal, as an expert ethical hacker and penetration tester, is 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.

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
- 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 Resources

To run this lab, you need the following:

- Nmap located on Desktop

Zenmap works on Windows versions after and including Windows 7, and Server 2003/2008.

- A computer running Windows 7 VM
- Windows Server 2008 running on a virtual machine as a guest
- A Firefox web browser with Internet access
- Administrative privileges to run the ZeNmap tool

Lab Duration

Time: 10 Minutes

Lab Tasks

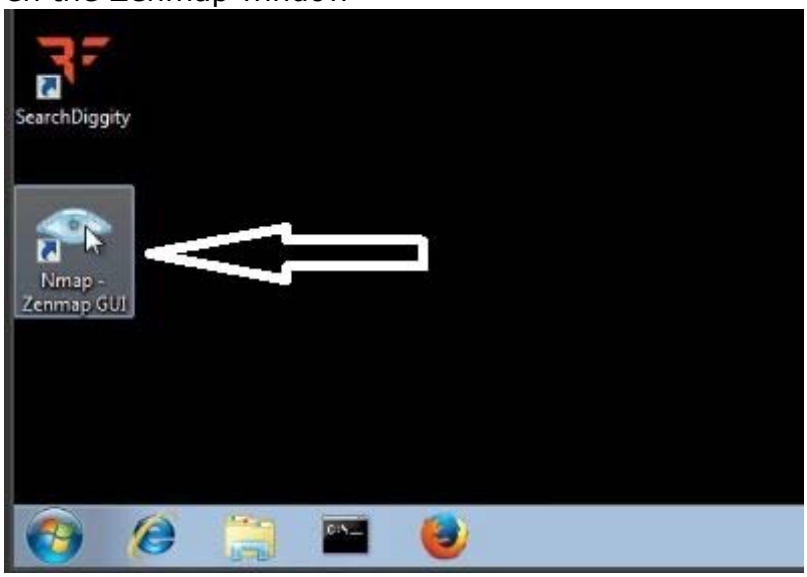
The basic idea in this lab is to:

- 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

Task 1

Intense Scan

1. On Windows 7 VM, click the Nmap-Zenmap GUI icon on the Desktop to open the Zenmap window



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

2. Start your virtual machine running Windows Server 2008.

3. Now launch the Zenmap tool in the Windows 7 VM

NOTE: Target is typically Windows 2008 VM.

4. Perform **nmap -O** scan for your Windows Server 2008 virtual machine (192.168.1.105, in our example) network. This takes a few minutes. Note: IP addresses may vary in your lab environment.

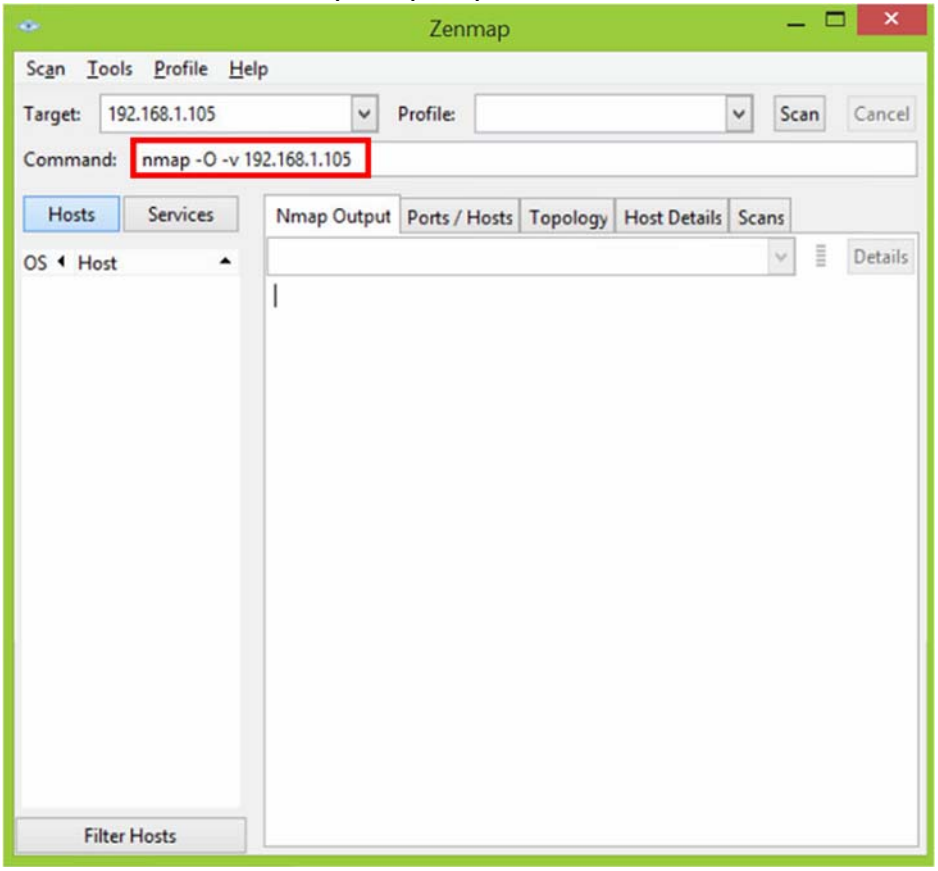


Figure: 1.3- Zenmap GUI main window

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

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

6. 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 in other OSes that have these ports open. There may be more than one system that has NetBIOS open.

Task 2

Find hosts with NetBIOS ports open

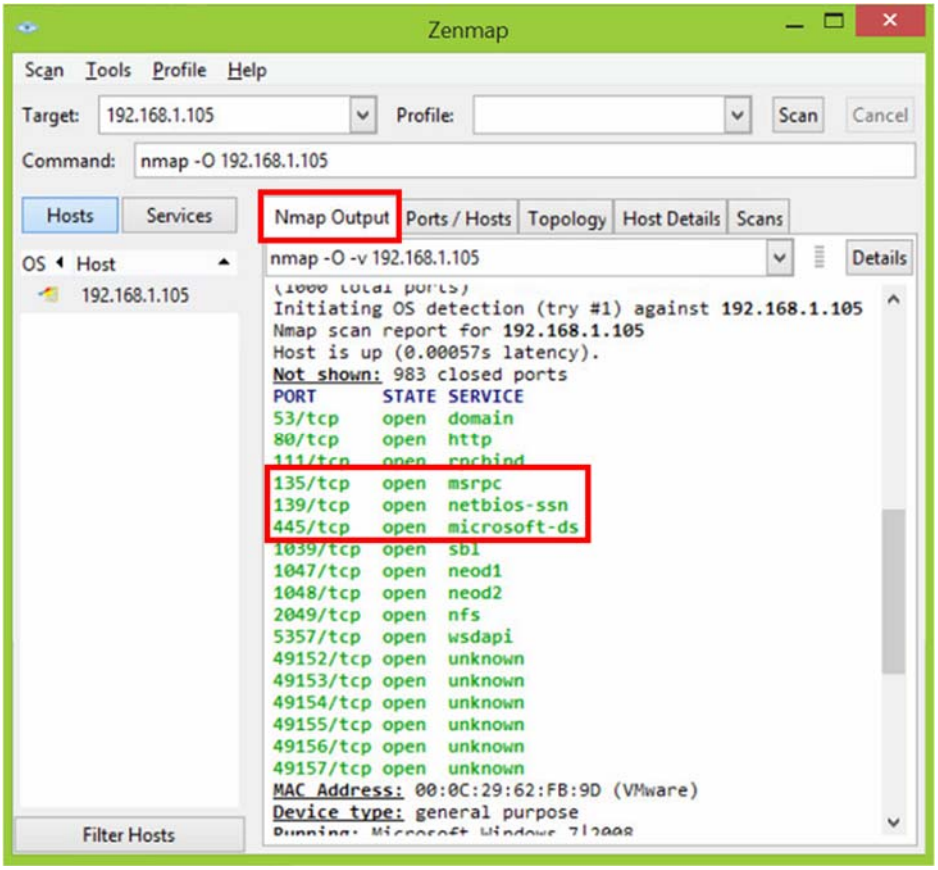


Figure: 1.4- Zenmap GUI output window

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

7. Now you see that ports 139 and 445 are open and port 139 is using NetBIOS.
8. Now launch the command prompt in your Windows Server 2008 virtual machine and perform nbtstat on port 139 to the target machine.
9. Run the command nbtstat -A 192.168.1.105

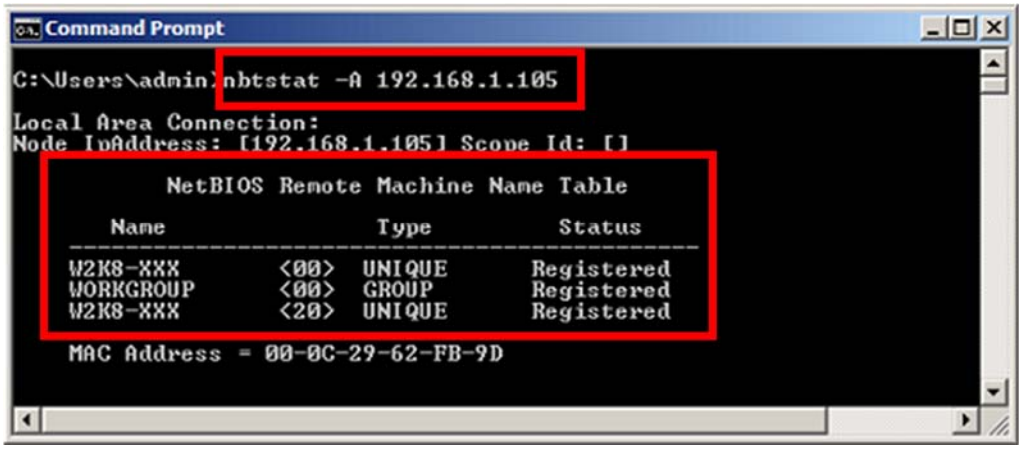


Figure: 1.5- Command Prompt with the nbtstat command

Task 3

Create a Null Session

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]

10. We have not even created a null session (an unauthenticated session) yet.
11. Now create a null session.
12. In the command prompt, type net use \\a.b.c.d\IPC$ “” /u:”” (where a.b.c.d is the address of the host machine or Windows server 2008 vm, and there are no spaces between the double quotes).
13. Confirm it by issuing a generic net use command to see connected null sessions from your host.
14. To confirm, type net use, which should list your newly created null session. (Run from Windows 7 connecting to Windows server 2008)

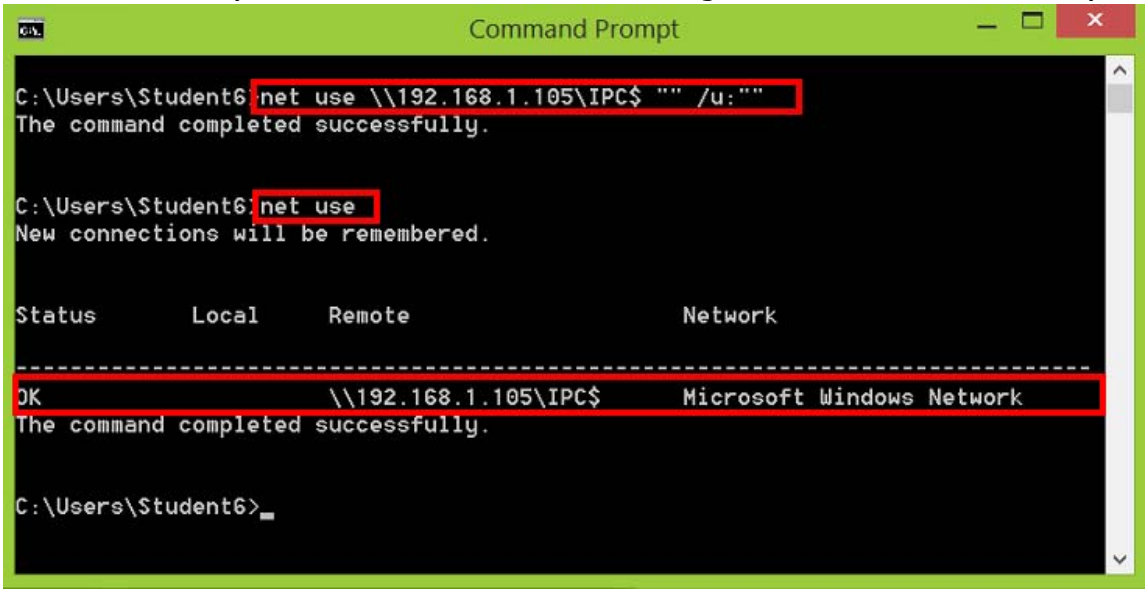


Figure: 1.6- The command prompt with the net use command

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

Tool / Utility	Information Collected / Objectives Achieved
Nmap tools	Target Machine: 192.168.1.105 List of Open Ports: 135/tcp, 139/tcp, 445/tcp, 554/tcp, 2869/tcp, 5357/tcp, 10243/tcp NetBIOS Remote machine IP address: 192.168.1.105 Output: Successful connection of Null session

Quiz

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.

Lab 2

Make use of the telnet utility to perform banner grabbing

Banner Grabbing Overview

In the context of Computer Networking, Banner Grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports. Administrators can use this to take inventory of the systems and services on their network. An intruder, however, can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits.

Some examples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 respectively. Tools commonly used to perform banner grabbing are Telnet, which is included with most operating systems, and Netcat.

Lab Scenario

We will use the Telnet utility to enumerate service by using banner grabbing techniques:

- Perform a GET Request against your Windows 2008 Server.
  - Open a command prompt
  - Type: telnet <ipaddress> 80
  - Hit enter once
  - At the prompt, type: GET / HTTP/1.0
  - Then hit enter 2 or 3 times and your banner will appear!
- Perform a HEAD Request against your Windows 2008 Server.
  - Type: telnet <ipaddress> 80
  - Hit enter once
  - At the prompt, type: HEAD / HTTP/1.0
  - Then hit enter 2 more times.

Lab Resources

To run this lab, you need the following:

- Kali Linux Virtual Machine
- Telnet utility

Lab Duration

Time: 5 Minutes

Lab Tasks

Task 1

Banner Grabbing using Telnet and HTTP GET Request

1. Open a shell in the Kali Linux Virtual Machine:
2. Type: telnet <ip address of Windows 2008 VM> 80
3. Hit enter once
4. At the prompt, type: GET / HTTP/1.0 (Note: if this is done from Windows command prompt you will not see what you enter)
5. Then hit enter 2 or 3 times and your banner will appear!

```
root@kali:~# telnet 192.168.1.105 80
Trying 192.168.1.105...
Connected to 192.168.1.105.
Escape character is '^]'.
GET / HTTP /1.0
HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 19 Aug 2014 14:46:12 GMT
Connection: close
Content-Length: 311

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/str
ict.dtd">
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Bad Request</h2>
<hr><p>HTTP Error 400. The request is badly formed.</p>
</BODY></HTML>
Connection closed by foreign host.
root@kali:~#
```

Figure: 2.1- Banner Grabbing using Telnet and HTTP GET Request

Task 2

Banner Grabbing using Telnet and HTTP HEAD Request

6. Type: telnet <ip address of Windows 2012 VM> 80
7. Hit enter once
8. At the prompt, type: HEAD / HTTP/1.0
9. Then hit enter 2 more times.

```
root@kali:~# telnet 192.168.1.105 80
Trying 192.168.1.105...
Connected to 192.168.1.105.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 689
Content-Type: text/html
Last-Modified: Wed, 18 Sep 2013 18:55:58 GMT
Accept-Ranges: bytes
ETag: "b2c6f1b5a0b4ce1:0"
Server: Microsoft-IIS/7.0
X-Powered-By: ASP.NET
Date: Tue, 19 Aug 2014 14:48:48 GMT
Connection: close

Connection closed by foreign host.
root@kali:~#
```

Figure: 2.2- Banner Grabbing using Telnet and HTTP HEAD Request

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

Tool / Utility	Information Collected / Objectives Achieved
Banner Grabbing using telnet utility	Target Machine: 192.168.1.105 Telnet Target with TCP/80 Uses HTTP GET and HEAD request to grab the banner of the Web Server Output: Web Server version and type

Quiz

1. Use other HTTP methods to grab the banner of the target
2. Try different TCP ports
3. Why didn't banner grabbing work with UPD port and Telnet?
4. Almost all HTTP servers differ in the way they implement the HTTP protocol. In the case where the HTTP request is well formed and legitimate, the response returned by all HTTP servers is more or less compliant with the specifications laid out in the RFCs for HTTP. However, when confronted with malformed HTTP requests, these servers differ in their responses. Differences in the way the HTTP protocol is handled by various HTTP servers forms the basis of the HTTP fingerprinting technique.
   Fill the following table:

HTTP Test	What to expect
HEAD / HTTP/1.0	
DELETE / HTTP/1.0	
GET / HTTP/3.0	
GET / JUNK/1.1	

Answer:

HTTP Test	What to expect
HEAD / HTTP/1.0	Normal HTTP header response
DELETE / HTTP/1.0	Response when operations such as DELETE aren't generally allowed
GET / HTTP/3.0	Response to a request with an improper HTTP protocol number
GET / JUNK/1.1	Response to a request with an improper protocol specification

Lab 3

Enumerating NetBIOS Using the SuperScan Tool

SuperScan Overview

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.

Lab Scenario

During enumeration, information is systematically collected and individual systems are identified. The pen testers examine the systems in their entirety; this allows for evaluating security weaknesses. In this lab, we extract the information of NetBIOS, user and group accounts, network shares, hosted 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.

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 Resources

To run this lab, you need the following:

- SuperScan tool located on Desktop
- A computer running Windows 7
- Any Windows VM as the target
- Administrative privileges to install and run tools
- A web browser with an Internet connection

Lab Duration

Time: 10 Minutes

Lab Tasks

Task 1

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

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

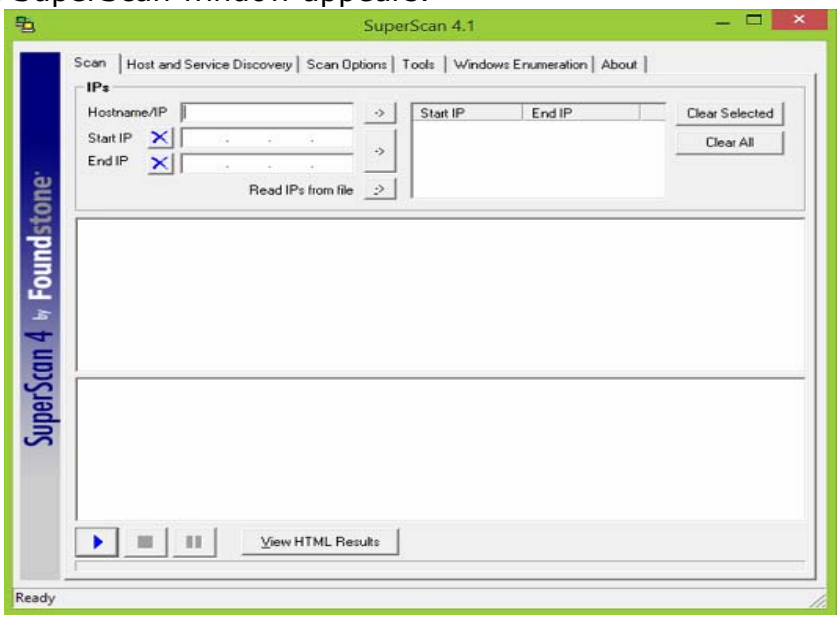


Figure: 4.1- SuperScan Main Window

2. Click the Windows Enumeration tab located on the top menu.
3. Enter the Hostname/IP/URL in the text box.
   In our example, we are using 192.168.1.105 (Windows 2008 VM)
4. Check the types of enumeration you want to perform.
5. Now, click Enumerate.

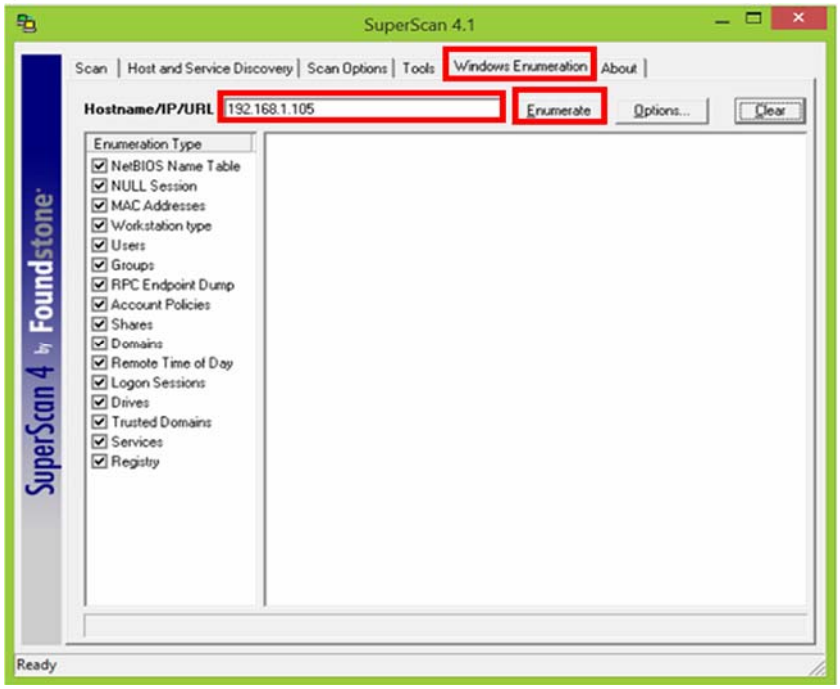


Figure: 4.2- SuperScan Main Window with IP address

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.

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

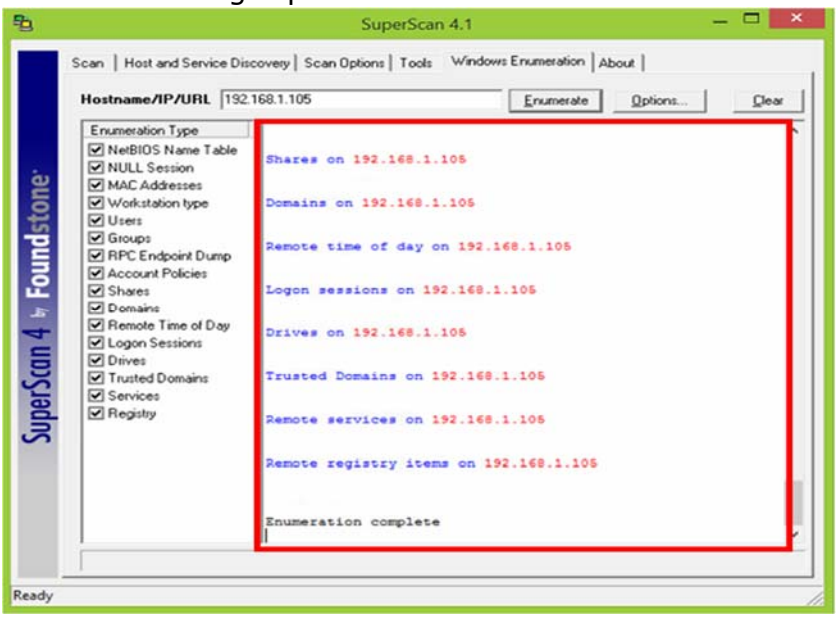


Figure: 4.3- SuperScan Main Window with IP address

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

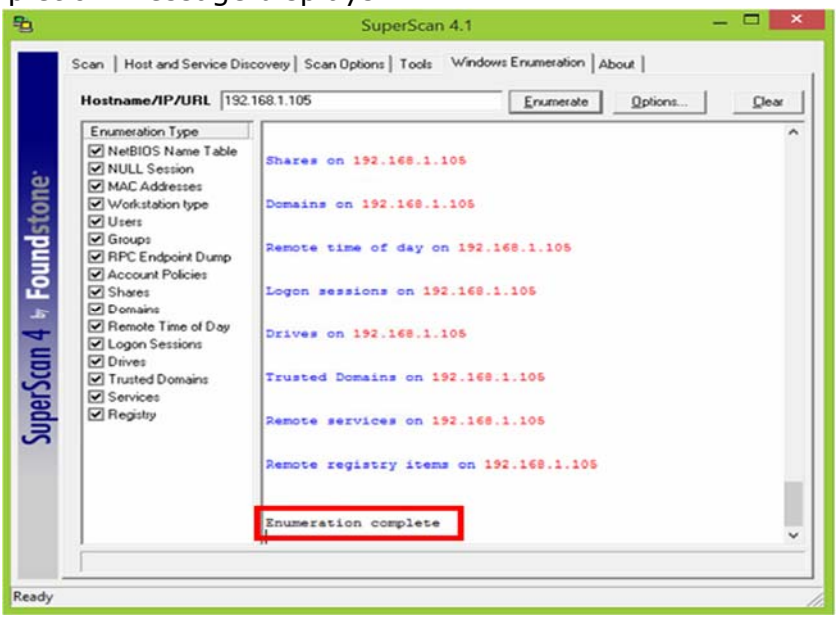


Figure: 4.4- SuperScan Main Window with results

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

Task 2

Erase Results

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

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

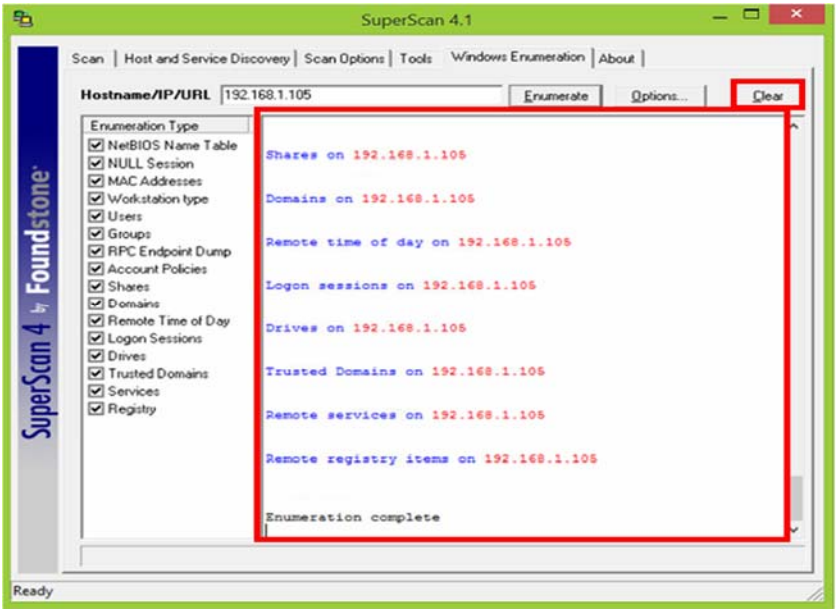


Figure: 4.5- SuperScan Main Window with IP address

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

Tool / Utility	Information Collected / Objectives Achieved
SuperScan Tool	**Enumerating Virtual Machine IP address:** 192.168.1.105 **Performing Enumeration Types:** • Null Session • MAC Address • Work Station Type • Users • Groups • Domain • Account Policies • Registry **Output:** Interface, Binding, Objective ID, and Annotation

Quiz

1. Analyze how remote registry enumeration is possible 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.

Lab 4

Enumerating NetBIOS Using the NetBIOS Enumerator Tool

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 the same as the usernames in lower case

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.

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.

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

Lab Resources

To run this lab, you need the following:

- NETBIOS Enumerator tool on Desktop
- Run this tool in **Windows 7**
- Administrative privileges are required to run this tool

Lab Duration

Time: 10 Minutes

Lab Tasks

1. To launch NetBIOS Enumerator, go to Desktop and double-click NetBIOS Enumerator.exe. (on your Windows 7 VM)

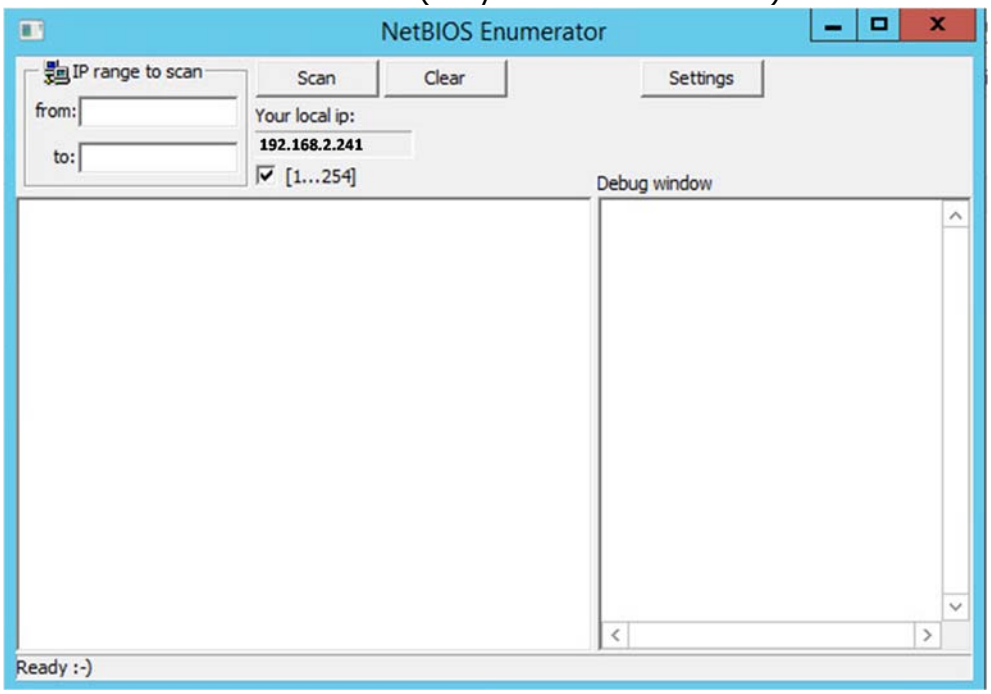


Figure: 4.1- NetBIOS Enumerator main window

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.

Task 1

Performing Enumeration using NetBIOS Enumerator

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.

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

Network function SMB scanning is also implemented and running.

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

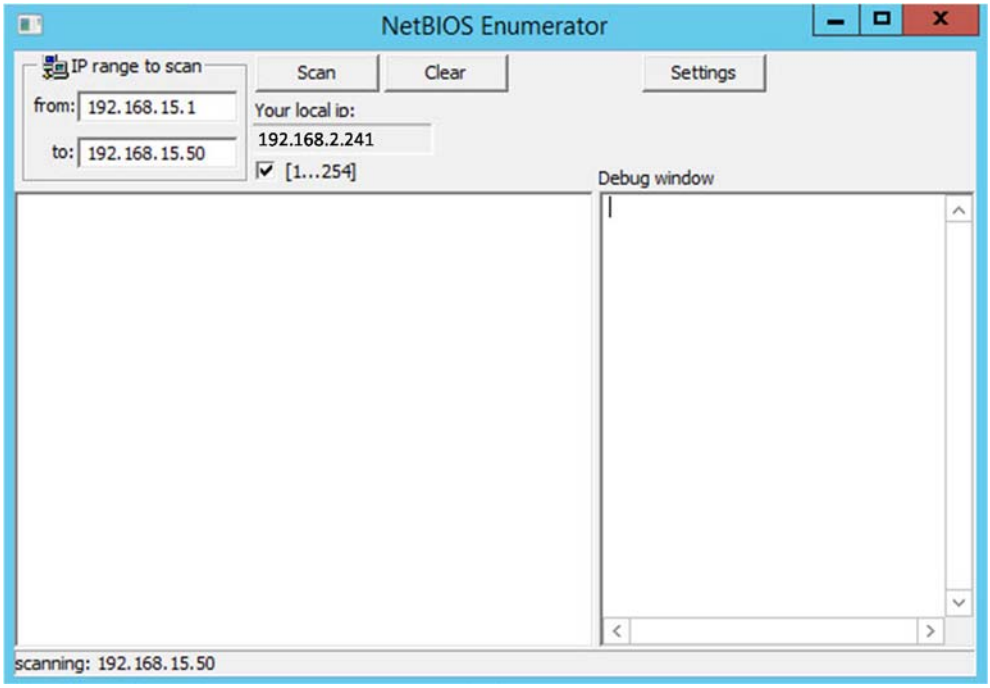


Figure: 4.2- NetBIOS Enumerator with IP range to scan

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

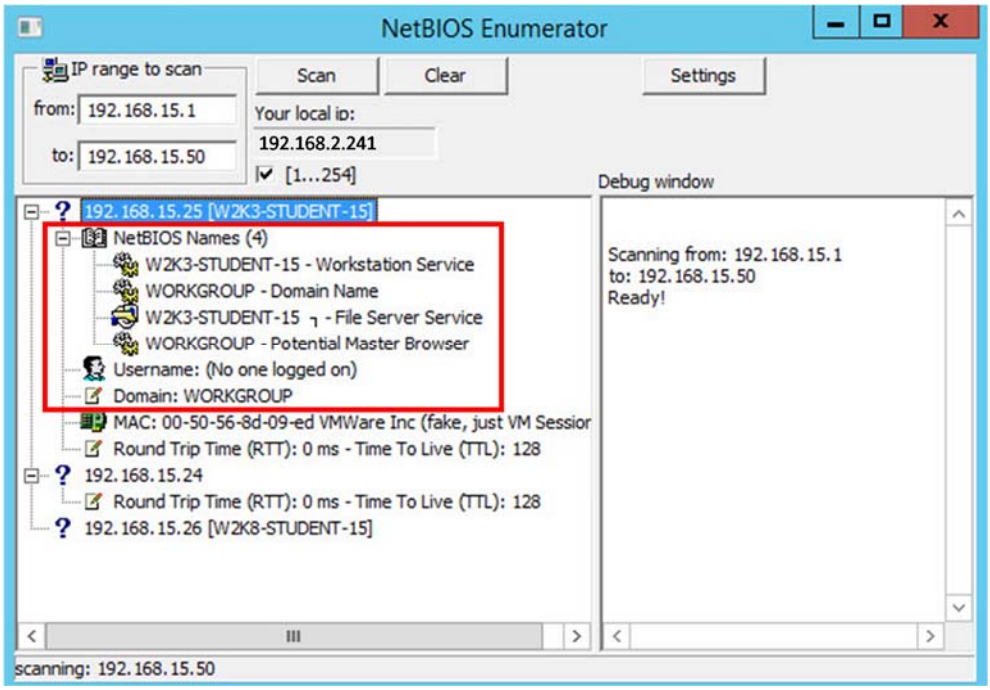


Figure: 4.3- NetBIOS Enumerator results

7. To perform a new scan 01- rescan, click Clear.
8. If you are going to perform a new scan, the previous scan results are erased.

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

Tool / Utility	Information Collected / Objectives Achieved
NetBIOS Enumerator Tool	**IP Address Range:** 192.168.15.1-92.168.15.50 **Result:** • Machine Name • NetBIOS Names • User Name • Domain • MAC Address • Round Trip Time (RTT)

Lab 5

Enumerating the System Using Hyena

Overview of 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.

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

The key new feature in v11.0 is the **'Active Task'**. Hyena's new 'Active Task' will provide the functionality for mass importing and updating of most Active Directory attributes from a delimited text input file.

All task settings are saved in a 'task file', allowing for easy repetitive task executions, including command line and scheduling support. For Active Directory user tasks, home directory creation can be automated using Hyena's existing user home directory templates.

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, tiles, printers and print jobs, sessions, open tiles, 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.

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

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

Lab Resources

To run this lab, you need the following:

- A computer running Windows 7
- Administrative privileges to install and run tools

Lab Duration

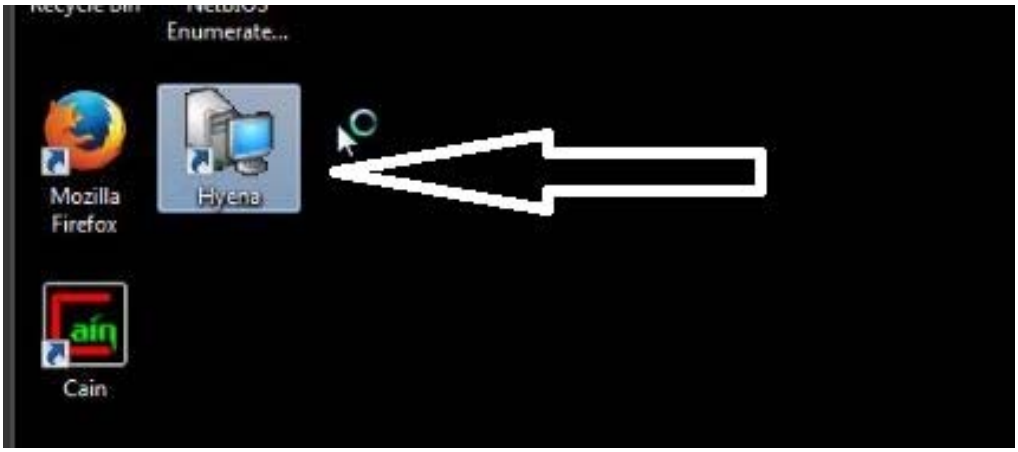
Time: 10 Minutes

Lab Tasks

Task 1

Launch Hyena tools

1. To launch Hyena go to Desktop and Double-click the **Hyena_English_x64.exe**. icon. (in Windows 7 VM)



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

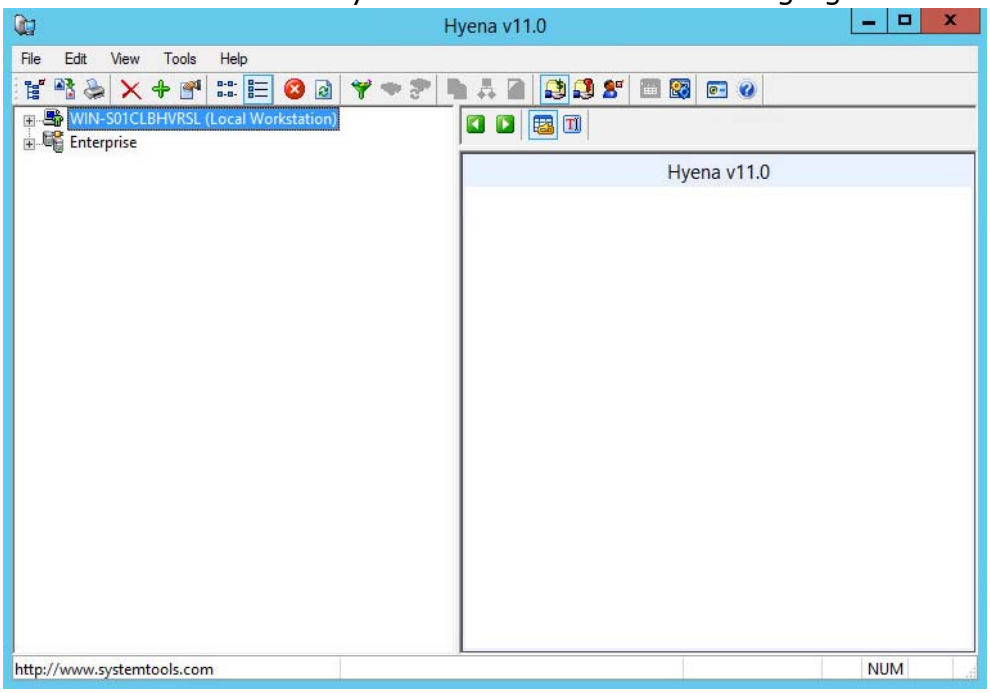
2. The Registration window will appear. Click **OK** to continue.

Task 2

Enumerating System Information

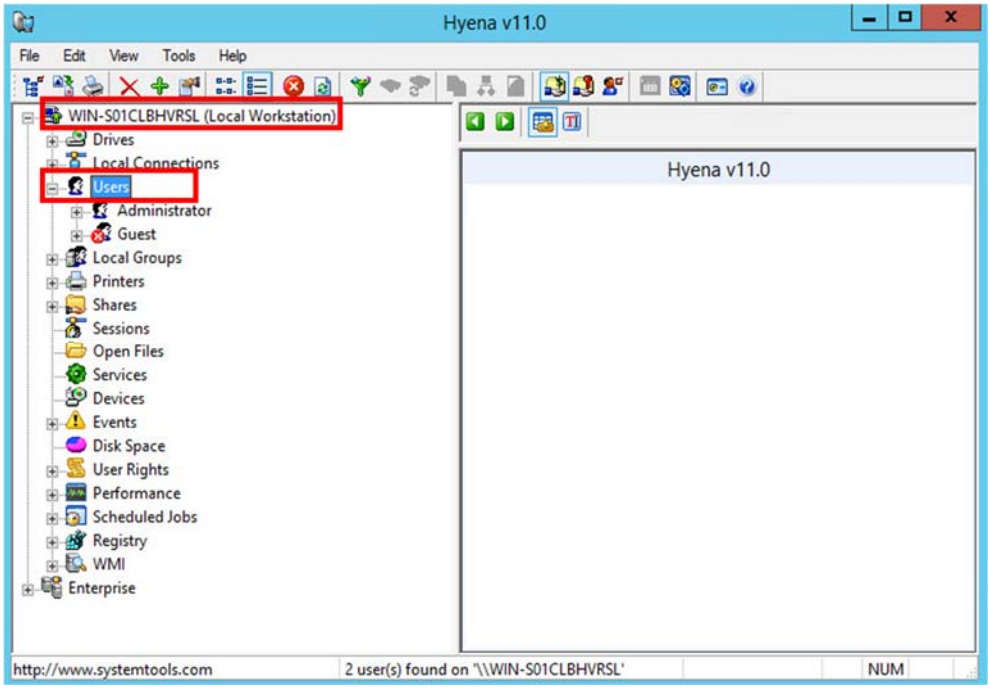
Additional command-line options were added to allow starting Hyena and automatically inserting and selecting/ expanding a domain, server, or computer.

3. The main window of Hyena is shown in the following figure.



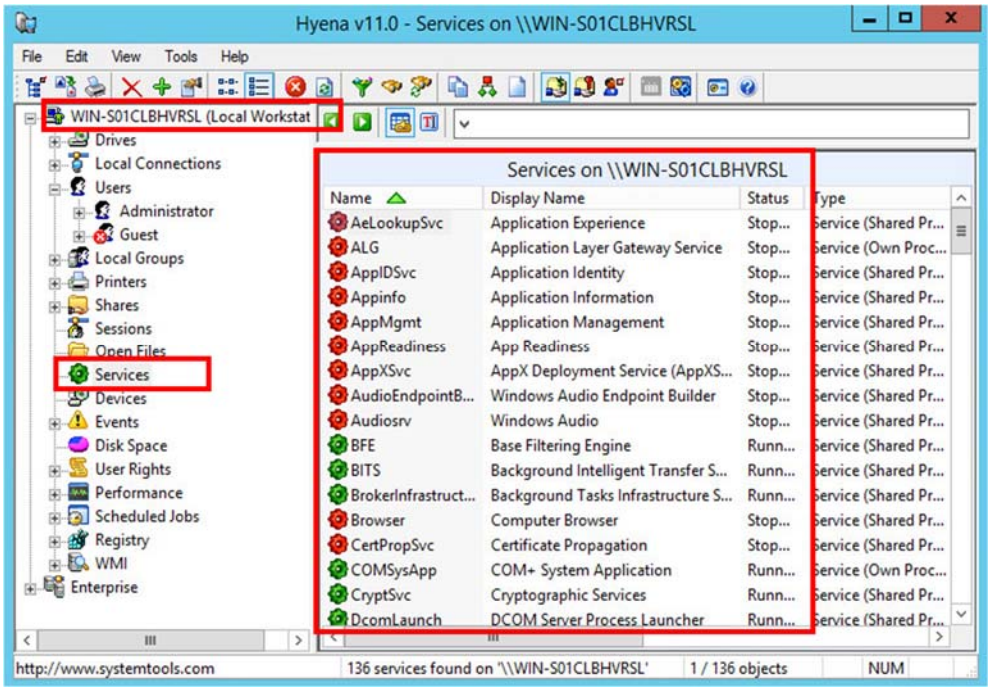
Main Windows of Hyena

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



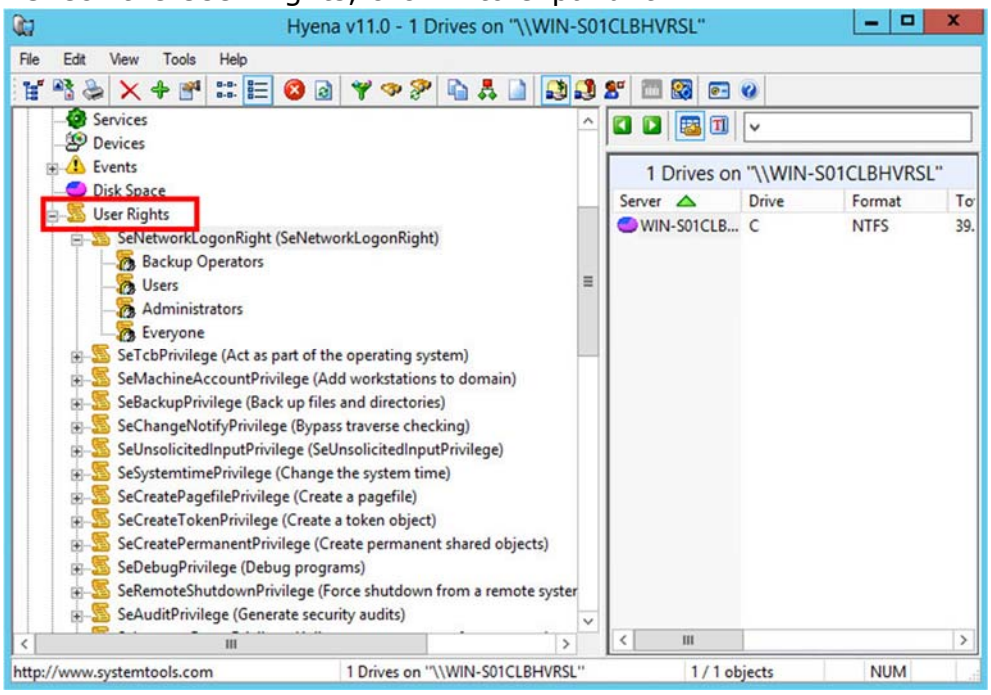
Expand the System users

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



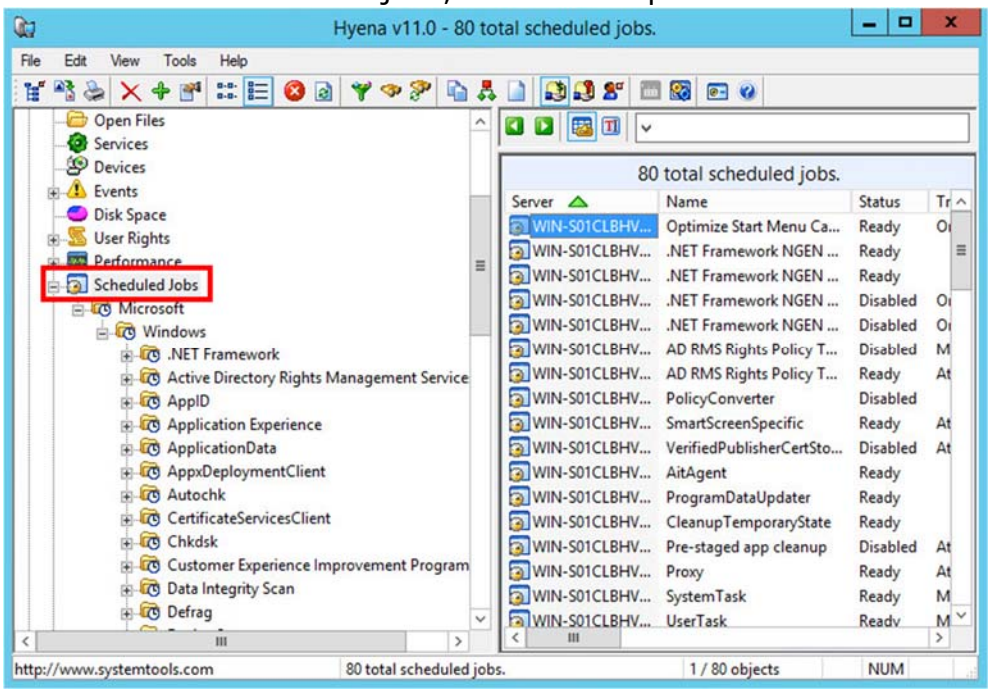
Services running in the system

6. Check the User Rights, click + to expand it.



User Rights

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



Scheduled jobs

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

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