

5. Which of the following tool is capable of performing a customized scan? A. nmap
B. wireshark
C. Netcraft
D. Airpcap
6. Which of the following is not a TCP Flag? A. URG
B. PSH
C. FIN
D. END
7. Successful three-way handshaking consists of: A. SYN, SYN-ACK, ACK
B. SYN, SYN-ACK, END
C. SYN, FIN, RST
D. SYN, RST, ACK
8. Method of pinging a range of IP address is called: A. Ping
B. Ping Sweep
C. Hping
D. SSDP Scanning
9. Scanning technique, in which TCP three-way handshaking session, initiated and completed is called:
A. TCP Connect (Full-open Scan)
B. TCP Connect (Half-open Scan)
C. Stealth Scan (Half-open Scan)
D. Stealth Scan (Full-open Scan)
10. Xmas Scan is a type of Inverse TCP Flag scanning, in which: A. Flags such as URG, FIN, PSH are set
B. Flags are not set
C. Only FIN flag is set
D. Only SYN flag is set

Chapter 4: Enumeration

Technology Brief

In the earlier sections on Footprinting and Scanning, we looked at how to collect information about any organization, and how to target a website or a particular network. We also discussed several tools that can be helpful in collecting general information about a target. Now we are moving on to observing the target more closely in order to obtain detailed information. This includes sensitive information such as network information, network resources, routing paths, SNMP, DNS, other protocol-related information, user and group information, etc. This sensitive information is required to gain access to a system. This information is gathered by using different tools and techniques.

Enumeration Concepts

Enumeration

In the Enumeration phase, an attacker initiates active connections with the target system. Through this active connection, direct queries are generated to gain more information. This information helps to identify the system's attack points. Once an attacker discovers attack points, he/she can gain unauthorized access to reach the assets by using the collected information.

The information enumerated in this phase is:

- Routing Information
- SNMP Information
- DNS Information
- Machine Name
- User Information
- Group Information
- Application and Banners
- Network Sharing Information
- Network Resources

In previous phases, the information being found did not concern legal issues. However, using the tools required for the enumeration phase may cross legal boundaries and carries chances of being traced. You must have proper permission to perform these actions.

Techniques for Enumeration

Enumeration Using Email ID

Using an Email ID to extract information can provide useful information such as username, domain name, etc. An email address usually contains in it the username and domain name.

Enumeration Using Default Password

Another way of enumeration is by using default passwords. Every device and software has default credentials and settings. It is recommended that these default settings and configurations are changed. Some administrators keep using default passwords and settings, making it very easy for an attacker to gain unauthorized access by using default credentials. Finding default settings, configurations, and passwords of devices is no longer difficult.

Enumeration using SNMP

Enumeration using SNMP is a process of collecting information through SNMP. The attacker uses default community strings or guesses the string to extract information about a device. The SNMP protocol was developed to allow administrators to manage devices such as servers, routers, switches, and workstations on an IP network. It allows network administrators to manage network performance, troubleshoot and resolve network problems, as well as design a highly available and scalable plan for network growth. SNMP is an application layer protocol. It provides communication between managers and agents. The SNMP system consists of three elements:

- SNMP Manager
- SNMP Agents (managed node)
- Management Information Base (MIB)

Brute Force Attack on Active Directory

Active Directory (AD) provides centralized command and control of domain users, computers, and network printers. It restricts access to network resources to defined users and computers. The AD is a big target as it is a good source of sensitive information for an attacker.

Brute forcing or generating queries to LDAP services helps to gather information such as username, address, credentials, privileges information, etc.

Enumeration through DNS Zone Transfer

Enumeration through the DNS zone transfer process includes extracting information such as the location of the DNS Server, DNS Records, and other valuable network related information like hostname, IP address, username, etc. A zone transfer is a process of updating DNS servers; a zone file carries valuable information that can be retrieved by an attacker. UDP port 53 is used for DNS requests. TCP 53 is used for DNS zone transfers to ensure that the transfer went through.

Services and Ports to Enumerate

Services	Ports	DNS Zone Transfer	TCP 53	DNS Queries	UDP 53
SNMP	UDP 161	SNMP Trap	TCP/UDP 162	Microsoft RPC Endpoint Mapper	TCP/UDP 135
LDAP	TCP/UDP 389	NBNS	UDP 137	Global Catalog Service	TCP/UDP 3268
NetBIOS	TCP 139	SMTP	TCP 25		

Table 4-01: Services and Ports to Enumerate

Lab 4- 1: Services Enumeration using Nmap

Case Study: In this Lab, consider the network 10. 10. 10.0/24, on which different devices are running. We will enumerate services, ports, and Operating System's information using the Nmap utility with Kali Linux.

Note: Nmap is a free open source network scanner tool by Gordon Lyon. It is popularly used to discover hosts and services on a network by sending packets and analyzing the responses. It provides a number of features for probing computer networks, including host discovery and service and Operating System detection.

Procedure & Commands:

Open the terminal of Kali Linux

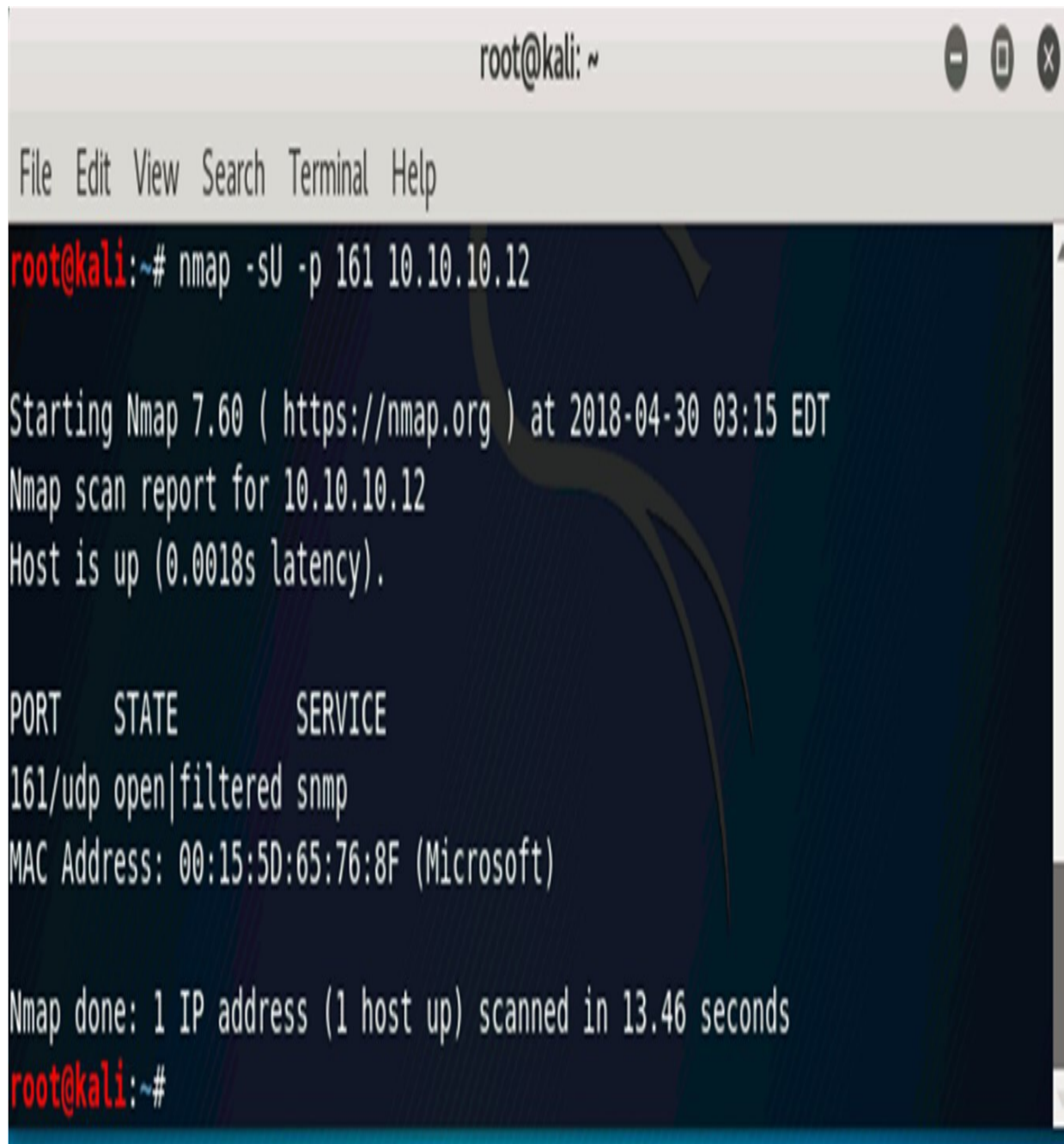
Enter the command: root@kali:~# nmap -sP 10. 10. 10.0/24


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sP 10.10.10.0/24  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-30 03:12 EDT  
Nmap scan report for 10.10.10.8  
Host is up (0.0024s latency).  
MAC Address: 00:15:5D:65:76:92 (Microsoft)  
Nmap scan report for 10.10.10.9  
Host is up (0.00074s latency).  
MAC Address: 00:15:5D:65:76:94 (Microsoft)  
Nmap scan report for 10.10.10.10  
Host is up (0.0011s latency).  
MAC Address: 00:15:5D:65:76:91 (Microsoft)  
Nmap scan report for 10.10.10.12  
Host is up (0.0034s latency).  
MAC Address: 00:15:5D:65:76:8F (Microsoft)  
Nmap scan report for www.goodshopping.com (10.10.10.16)  
Host is up (0.00049s latency).  
MAC Address: 00:15:5D:28:73:23 (Microsoft)  
Nmap scan report for 10.10.10.11  
Host is up.  
Nmap done: 256 IP addresses (6 hosts up) scanned in 28.01 seconds  
root@kali:~#
```

Figure 4-01: Ping Sweep

Figure 4-01: Ping Sweep

To perform Ping Sweep on the subnet, check live host and other basic information. Enter the command: `root@kali:~# nmap -sU -p 10. 10. 10. 12`

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the command 'root@kali:~# nmap -sU -p 161 10.10.10.12' being entered. The output indicates that Nmap 7.60 is starting at 2018-04-30 03:15 EDT, reports the scan for 10.10.10.12, and confirms the host is up with a latency of 0.0018s. A table shows the scan results for port 161/udp, which is open|filtered and associated with the snmp service. The MAC address 00:15:5D:65:76:8F (Microsoft) is also listed. The scan completed in 13.46 seconds, scanning 1 IP address (1 host up). The prompt returns to 'root@kali:~#'.

```
root@kali:~# nmap -sU -p 161 10.10.10.12

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-30 03:15 EDT
Nmap scan report for 10.10.10.12
Host is up (0.0018s latency).

PORT      STATE      SERVICE
161/udp   open|filtered snmp
MAC Address: 00:15:5D:65:76:8F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
root@kali:~#
```

Figure 4-02: UDP Port Scanning

The result shows SNMP UDP port 16 1 is open and filtered. Now, enter the command: `root@kali:~# nmap -sS 10. 10. 10. 12` to perform a stealth scan on target host 10. 10. 10. 12.


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sS 10.10.10.12  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-30 03:17 EDT  
Nmap scan report for 10.10.10.12  
Host is up (0.010s latency).  
Not shown: 975 closed ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
88/tcp    open  kerberos-sec  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
593/tcp   open  http-rpc-epmap  
636/tcp   open  ldapssl  
1025/tcp  open  NFS-or-IIS  
1026/tcp  open  LSA-or-nterm  
1027/tcp  open  IIS  
1028/tcp  open  unknown  
1030/tcp  open  iad1  
1031/tcp  open  iad2  
1032/tcp  open  iad3  
1040/tcp  open  netsaint  
1043/tcp  open  boinc  
1048/tcp  open  neod2  
1069/tcp  open  cognex-insight  
3268/tcp  open  globalcatLDAP  
3269/tcp  open  globalcatLDAPssl  
3306/tcp  open  mysql  
3389/tcp  open  ms-wbt-server
```

Figure 4-22: Stealth Scan

Figure 4-03. Stearn Scan

The result shows a list of open ports and services running on the target host. Enter the command: root@kali:~# nmap -sSV -O 10. 10. 10. 12

This command performs operating system and version scanning on target host 10. 10. 10. 12.

root@kali: ~

File Edit View Search Terminal Help

root@kali:~# nmap -sSV -O 10.10.10.12

Starting Nmap 7.60 (<https://nmap.org>) at 2018-04-30 03:20 EDT

Nmap scan report for 10.10.10.12

Host is up (0.0025s latency).

Not shown: 975 closed ports

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS
88/tcp	open	kerberos-sec	Microsoft Windows Kerberos (server time: 2018-04-30 07:20:28Z)
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
389/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: CEH.com, Site: Default-First-Site-Name)
445/tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CEH)
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
1025/tcp	open	msrpc	Microsoft Windows RPC
1026/tcp	open	msrpc	Microsoft Windows RPC
1027/tcp	open	msrpc	Microsoft Windows RPC
1028/tcp	open	msrpc	Microsoft Windows RPC
1030/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1031/tcp	open	msrpc	Microsoft Windows RPC
1032/tcp	open	msrpc	Microsoft Windows RPC
1040/tcp	open	msrpc	Microsoft Windows RPC
1043/tcp	open	msrpc	Microsoft Windows RPC
1048/tcp	open	msrpc	Microsoft Windows RPC
1069/tcp	open	msrpc	Microsoft Windows RPC
3268/tcp	open	ldap	Microsoft Windows Active Directory LDAP (Domain: CEH.com, Site: Default-First-Site-Name)
3269/tcp	open	tcpwrapped	
3306/tcp	open	mysql	MySQL (unauthorized)

Figure 4-04: OS and Version Scanning NetBIOS Enumeration

NetBIOS stands for Network Basic Input/Output System. It is a program that allows communication between different applications running on different systems within a local area network. NetBIOS uses a unique 16-ASCII character string to identify the network devices over TCP/IP. The initial 15 characters are for identifying the device, the 16th character is to identify the service. NetBIOS service uses TCP port 139. NetBIOS over TCP (NetBT) uses the following TCP and UDP ports:

- UDP port 137 (name services)
- UDP port 138 (datagram services)
- TCP port 139 (session services)

Using NetBIOS enumeration, an attacker can discover:

- List of machines within a domain
- File sharing
- Printer sharing
- Username
- Group information
- Password
- Policies

NetBIOS names are classified into the following types:

- Unique
- Group
- Domain Name • Internet Group • Multihomed

Name Hex Code 00<computername>

Type Information U Workstation Service <computername> 0 1

0 1<WW-
__MSBROWSE__>

<computername> 03
<computername> 06
<computername> 1F <computername> 20
<computername> 2 1 <computername> 22

<computername> 23
<computername> 24
<computername> 30
<computername> 3 1 <computername> 43
<computername> 44
<computername> 45
<computername> 46
<computername> 4C

<computername> 42 <computername> 52

<computername> 87 <computername> 6A U Messenger Service G
Master Browser

U Messenger Service U RAS Server Service U NetDDE Service
U File Server Service
U RAS Client Service

U Microsoft Exchange Interchange(MSMail Connector)

U Microsoft Exchange Store
U Microsoft Exchange Directory
U Modem Sharing Server Service
U Modem Sharing Client Service
U SMS Clients Remote Control
U SMS Administrators Remote Control Tool U SMS Clients Remote Chat
U SMS Clients Remote Transfer

U DEC Pathworks TCPIP service on Windows NT
U mccafee anti-virus
U DEC Pathworks TCPIP service on Windows NT
U Microsoft Exchange MTA

U Microsoft Exchange IMC

<computename> BE U Network Monitor Agent

<computename> BF U <username> 03 U <domain> 00 G Network
Monitor Application Messenger Service Domain Name

<domain> 1B U Domain Master Browser <domain> 1C G Domain
Controllers

<domain> 1D U <domain> 1E G Master Browser Browser Service
Elections

<Inet~Services> 1C G <IS~computer 00 U name>

<computename> [2B] U IRISMULTICAST [2F] G IRISNAMESERVER
[33] G Forte_\$ND800ZA [20] U IIS IIS

Lotus Notes Server Service Lotus Notes Lotus Notes DCA ImaLan
Gateway Server Service

Table 4-02: NetBIOS Names NetBIOS Enumeration Tool

The *nbtstat* command is a useful tool for displaying information about NetBIOS over TCP/IP statistics. It is also used to display information such as NetBIOS name tables, name cache, and other information. The command that uses nbtstat utility is shown below:

```
nbtstat.exe -a "NetBIOS name of the remote system".
```

```
nbtstat -A 192. 168. 1. 10
```

The nbtstat command can be used along with several options. Available options for the nbtstat command are listed below:

Option Description

-a Displays the NetBIOS name table and MAC address information. This option is used with hostname in syntax

-A Displays the NetBIOS name table and MAC address information. This option is used with IP Address in syntax

-c Displays NetBIOS name-cache information

-n Displays the names registered locally by NetBIOS applications such as the server and redirector
-r Displays a count of all resolved names by broadcast or the WINS server

-s Lists the NetBIOS sessions table and converts destination IP addresses to computer NetBIOS names

-S Lists the current NetBIOS sessions, status, along with the IP address *Table 4-03: Nbtstat Options*

Lab 4-2: Enumeration using SuperScan Tool Procedure:

Open the SuperScan Software, go to the “Windows Enumeration” tab

Windows Enumeration

. Enter the Hostname or IP address of the targeted Windows machine. Go to the “Options” button to customize the enumeration. Select the enumeration type from the

left section. After configuring, click “ Enumerate”

Enumerate

to initiate the enumeration process.

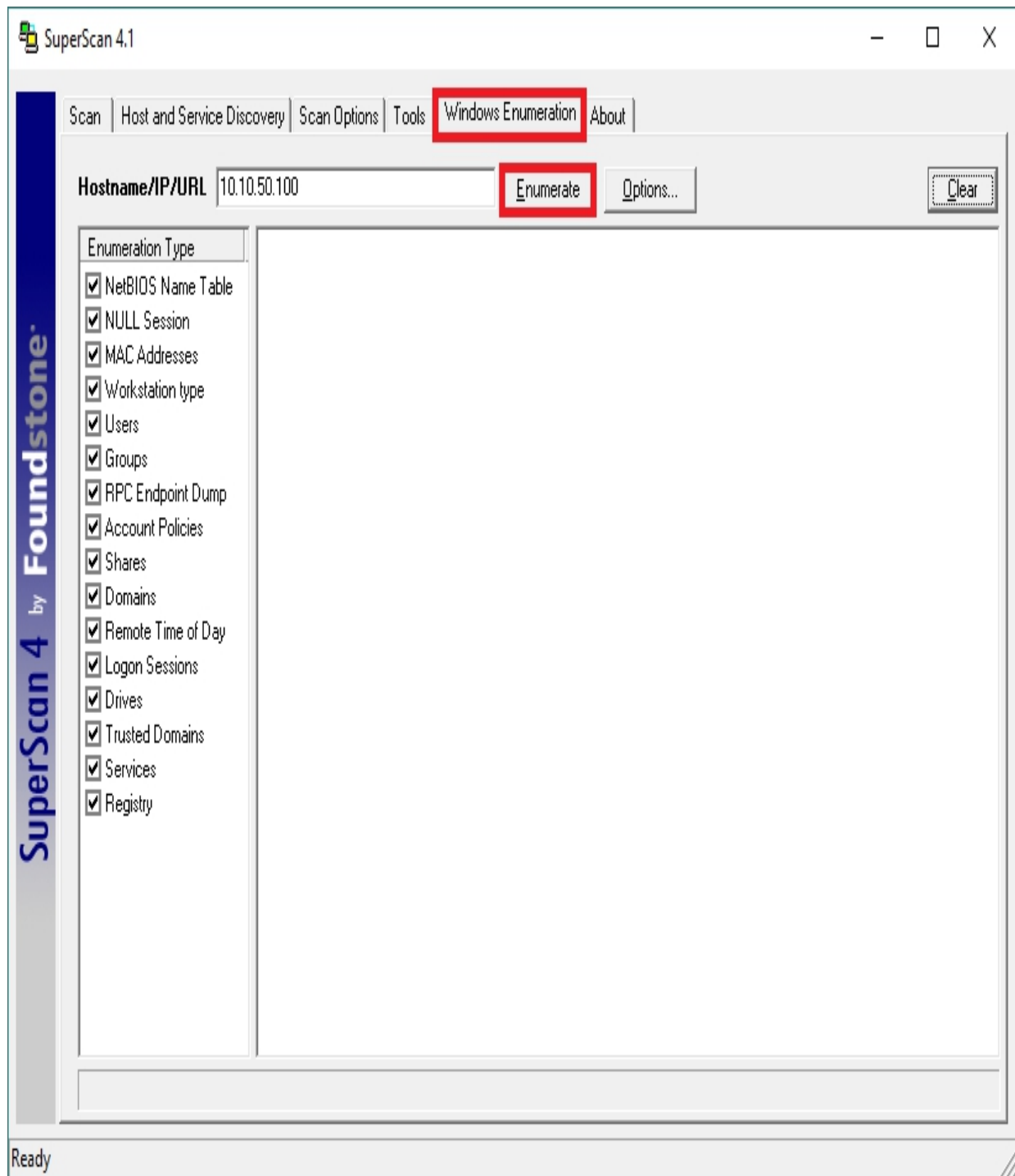


Figure 4-05: Super Scan Enumeration Tool

The enumeration process can gather information about the target machine such as MAC address, Operating System, and other information depending upon the type of enumeration selected before initiating the process.

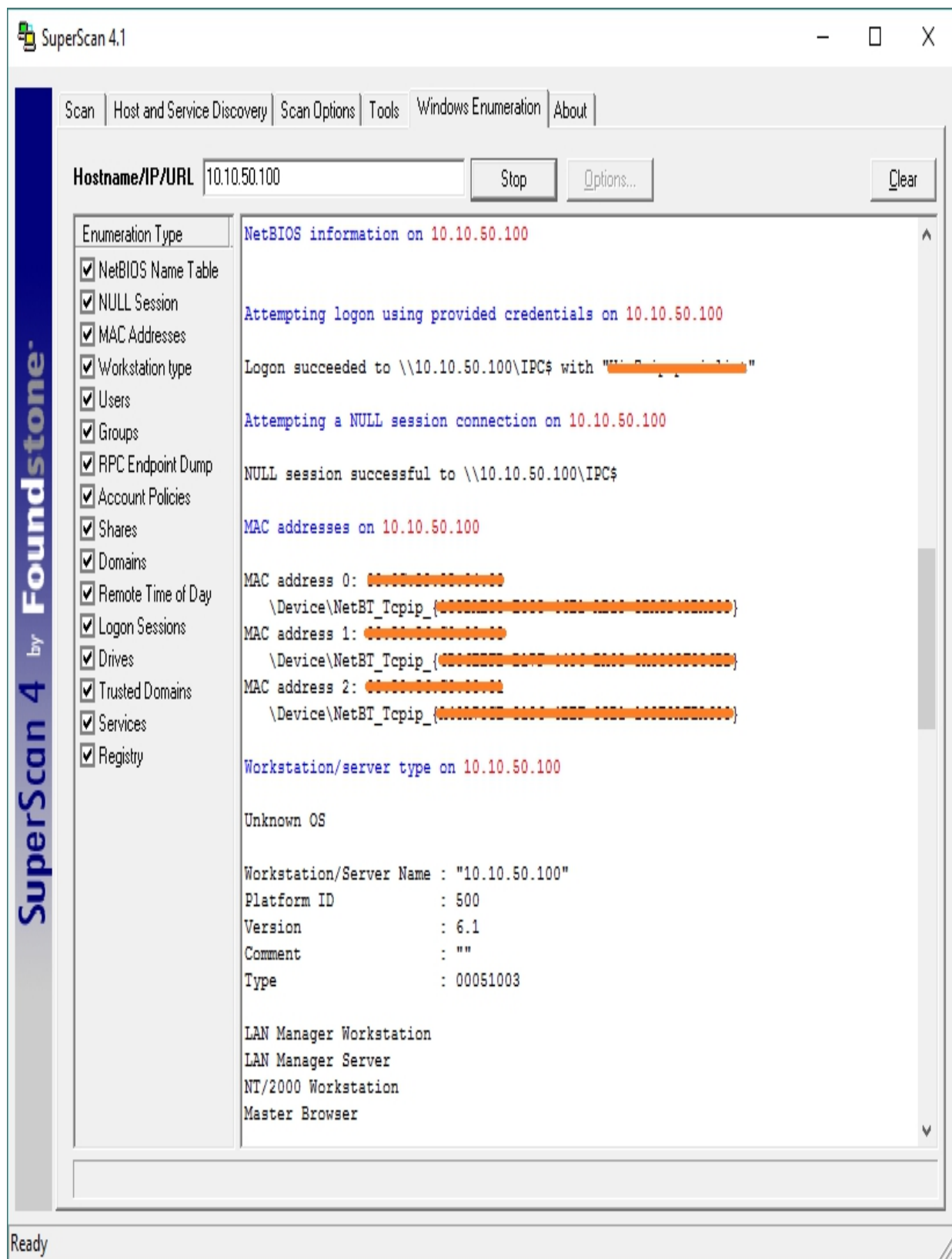


Figure 4-06: Windows Enumeration

In the figure below, User information of target machine along with full name, system comments, last login information, password expiry information, password change information, number of logins, and invalid password count information are fetched.

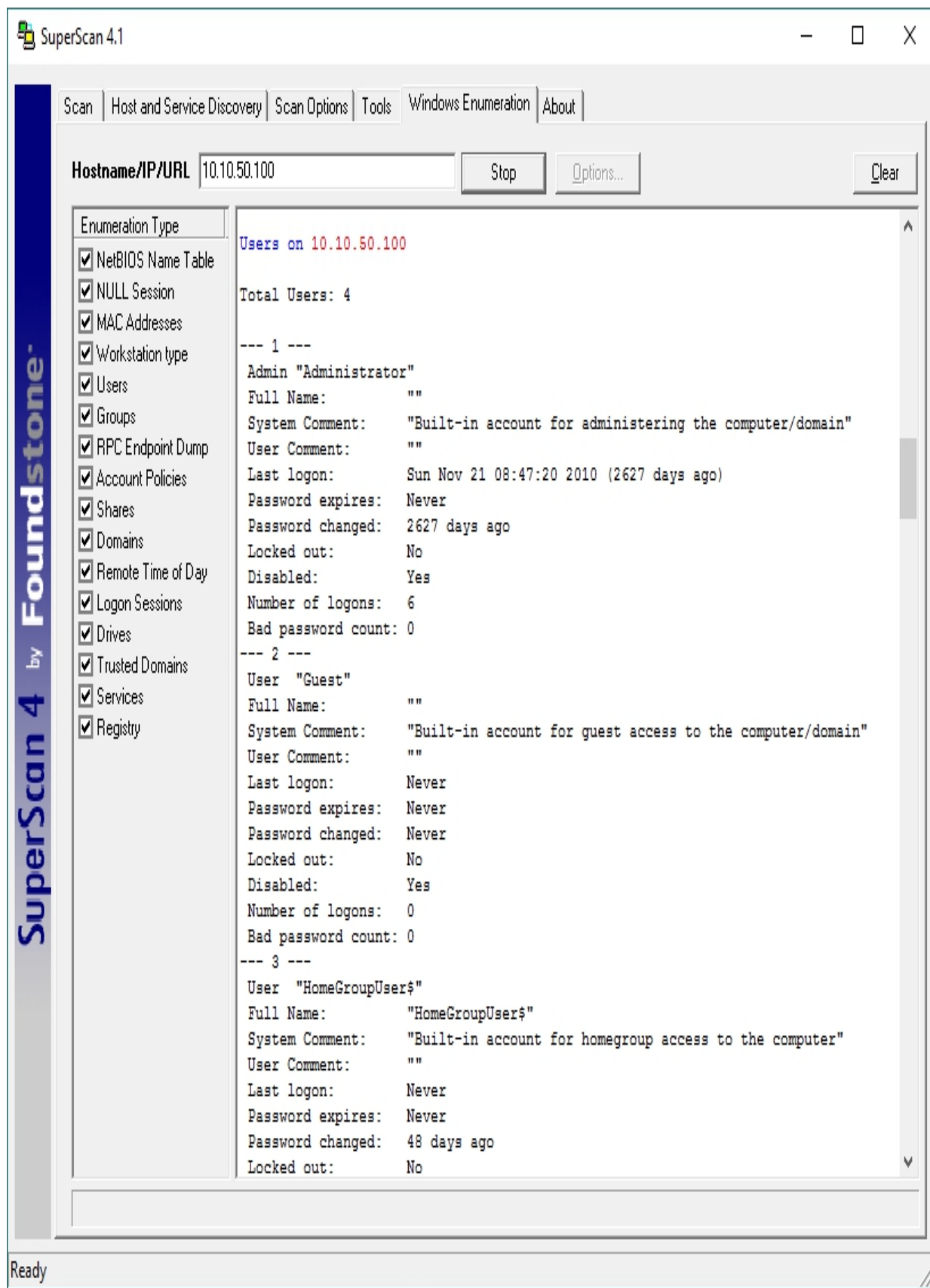


Figure 4-27: Windows Enumeration

Figure 4-07: Windows Enumeration

The result shows the password and account policies' information, shares' information, remote login information, etc.

Hostname/IP/URL 10.10.50.100

Enumerate

Options...

Clear

Enumeration Type

- ☒ NetBIOS Name Table
- ☒ NULL Session
- ☒ MAC Addresses
- ☒ Workstation type
- ☒ Users
- ☒ Groups
- ☒ RPC Endpoint Dump
- ☒ Account Policies
- ☒ Shares
- ☒ Domains
- ☒ Remote Time of Day
- ☒ Logon Sessions
- ☒ Drives
- ☒ Trusted Domains
- ☒ Services
- ☒ Registry

Object Id: "765294ba-60bc-48b8-92e9-89fd77769d91"

Annotation: ""

Password and account policies on 10.10.50.100

Account lockout threshold is 0
Account lockout duration is 30 mins
Minimum password length is 0
Maximum password age is 42 days

Shares on 10.10.50.100

Disk: ADMIN\$ (Remote Admin)
Disk: C\$ (Default share)
IPC: IPC\$ (Remote IPC)
Disk: Users ()

Domains on 10.10.50.100

Remote time of day on 10.10.50.100

Date: 07/08/2008
Time: 11:49:35
Timezone: GMT-05:00
Uptime: 38 days, 18 hours, 10 minutes

Logon sessions on 10.10.50.100

Total Sessions: 1

\\\\192.168.95.24 Win7 Uptime: 0:03:35 Idle: 0:00:00

Drives on 10.10.50.100

Trusted Domains on 10.10.50.100

Figure 4–08: Windows Enumeration

Some other useful tools are:

NetBIOS Enumeration Tool

Hyena
Winfingerprint
NetBIOS
Enumerator

Description

Hyena is a GUI based—NetBIOS Enumeration tool that shows shares, user's login information, and other related information

Winfingerprint is a NetBIOS Enumeration tool that is capable of providing information such as Operating System information, User and Group information, shares, sessions and services, SIDs, etc.

NetBIOS Enumerator is a GUI based NetBIOS Enumeration tool that is capable of providing port scanning, Dynamic Memory management, OS determination, traceroute, DNS information, host information, and many features depending upon the version of the software

Nsauditor Network Security Auditor

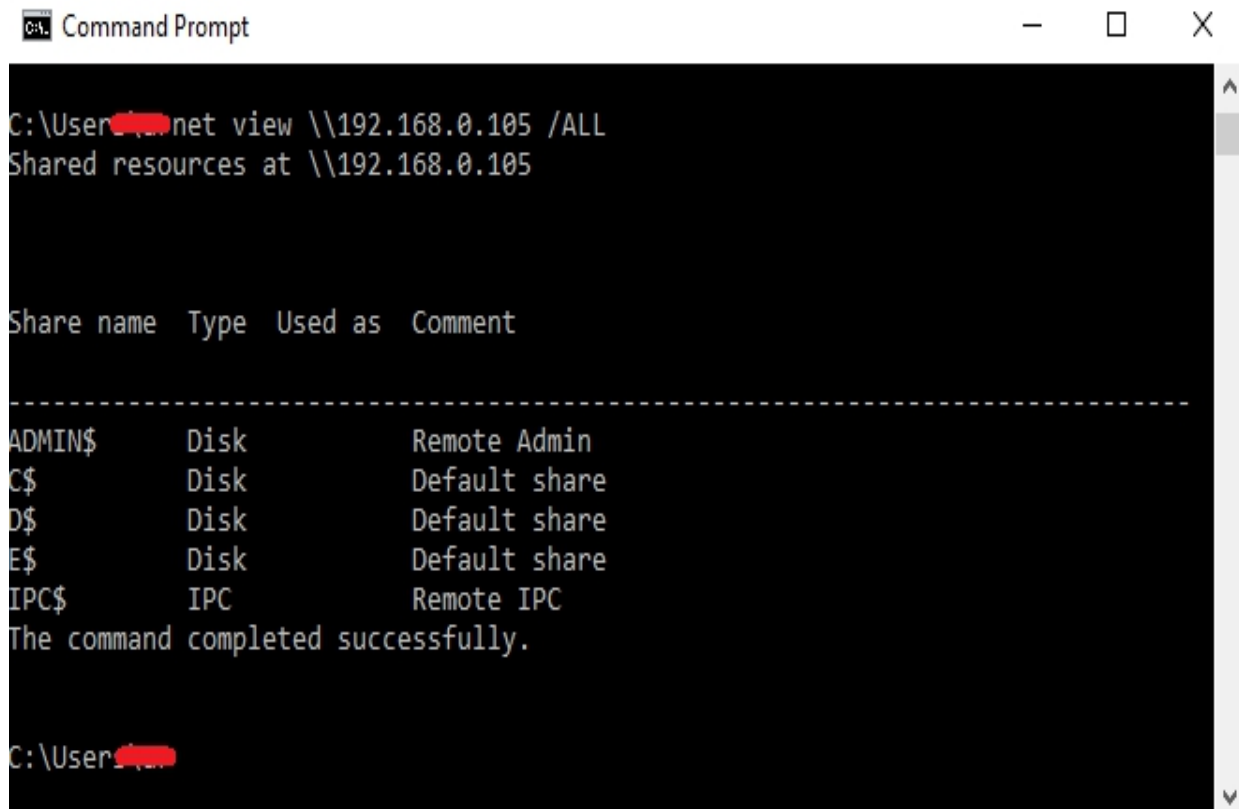
Nsauditor network monitoring provides some insight into services running locally, with options to dig down into each connection and analyze the remote system, terminate connections, and view data

Table 4–04: NetBIOS Enumeration Tools

Enumerating Shared Resources Using Net View

Net View is the utility that is used to display information about all shared resources of the remote host or workgroup. Following is the command syntax for the Net View utility:

```
C:\Users\Wa>net view [\\computername [/CACHE] | [/ALL] |  
/DOMAIN[:domain name]]
```



```
C:\User>net view \\192.168.0.105 /ALL
Shared resources at \\192.168.0.105

Share name  Type  Used as  Comment
-----
ADMIN$      Disk      Remote Admin
C$          Disk      Default share
D$          Disk      Default share
E$          Disk      Default share
IPC$        IPC       Remote IPC
The command completed successfully.

C:\User>
```

Figure 4–09: Net View

Lab 4–3: Enumeration using SoftPerfect Network Scanner Tool Procedure:

Download and install SoftPerfect Network Scanner tool. In this lab, we are using Windows Server 20 16 to perform scanning using SoftPerfect Network Scanner to scan shared resources in a network.

After installation, run the application and enter the range of IP addresses you want to scan.

Figure 4–10: SoftPerfect Network Scanner

Now, click on the “Start Scanning” button.

File View Actions Options Bookmarks Help















IPv4 From To

IP Address	MAC Address	Response Time	Host Name
10.10.50.1	C0-67-AF-C7-D9-80	0 ms	
? 10.10.50.10	F8-72-EA-A4-A1-CC	0 ms	
? 10.10.50.11	F8-72-EA-A4-A1-2C	2 ms	
10.10.50.20	00-0C-29-72-4A-C1	0 ms	
10.10.50.100	00-0C-29-95-04-33	1 ms	WIN7-PC
10.10.50.200	00-0C-29-CF-4F-DD	0 ms	
10.10.50.202	00-0C-29-20-C4-A9	0 ms	WIN7-1-PC
10.10.50.211	00-0C-29-BA-AC-AA	0 ms	WIN-2HMGPM3UAD7
10.10.50.210	00-0C-29-EA-BD-DF	3 ms	

Figure 4-11: Scanning

SoftPerfect scans for hosts in the determined range.

IPv4 From To      Start Scanning 

IP Address	MAC Address	Response Time	Host Name
 10.10.50.1	C0-67-AF-C7-D9-80	0 ms	
 10.10.50.10	F8-72-EA-A4-A1-CC	0 ms	
 10.10.50.11	F8-72-EA-A4-A1-2C	2 ms	
 10.10.50.20	00-0C-29-72-4A-C1	0 ms	
 10.10.50.100	00-0C-29-95-04-33	1 ms	WIN7-PC
 10.10.50.200	00-0C-29-CF-4F-DD	0 ms	
 10.10.50.202	00-0C-29-20-C4-A9	0 ms	WIN7-1-PC
 10.10.50.214	00-0C-29-84-18-A4	0 ms	WIN-2HMGPM3UAD7
 10.10.50.215	00-0C-29-84-18-A5	0 ms	

Open Device >

Copy >

Properties

Rescan device >

Wake-On-LAN >

Remote Shutdown

Remote Suspend / Hibernate

Assign Friendly Name... F2

Send Message...

Create Batch File...

Delete from List

Figure 4–12: Exploring Results

After scanning, select your target host and right click on it. Go to “Properties” .

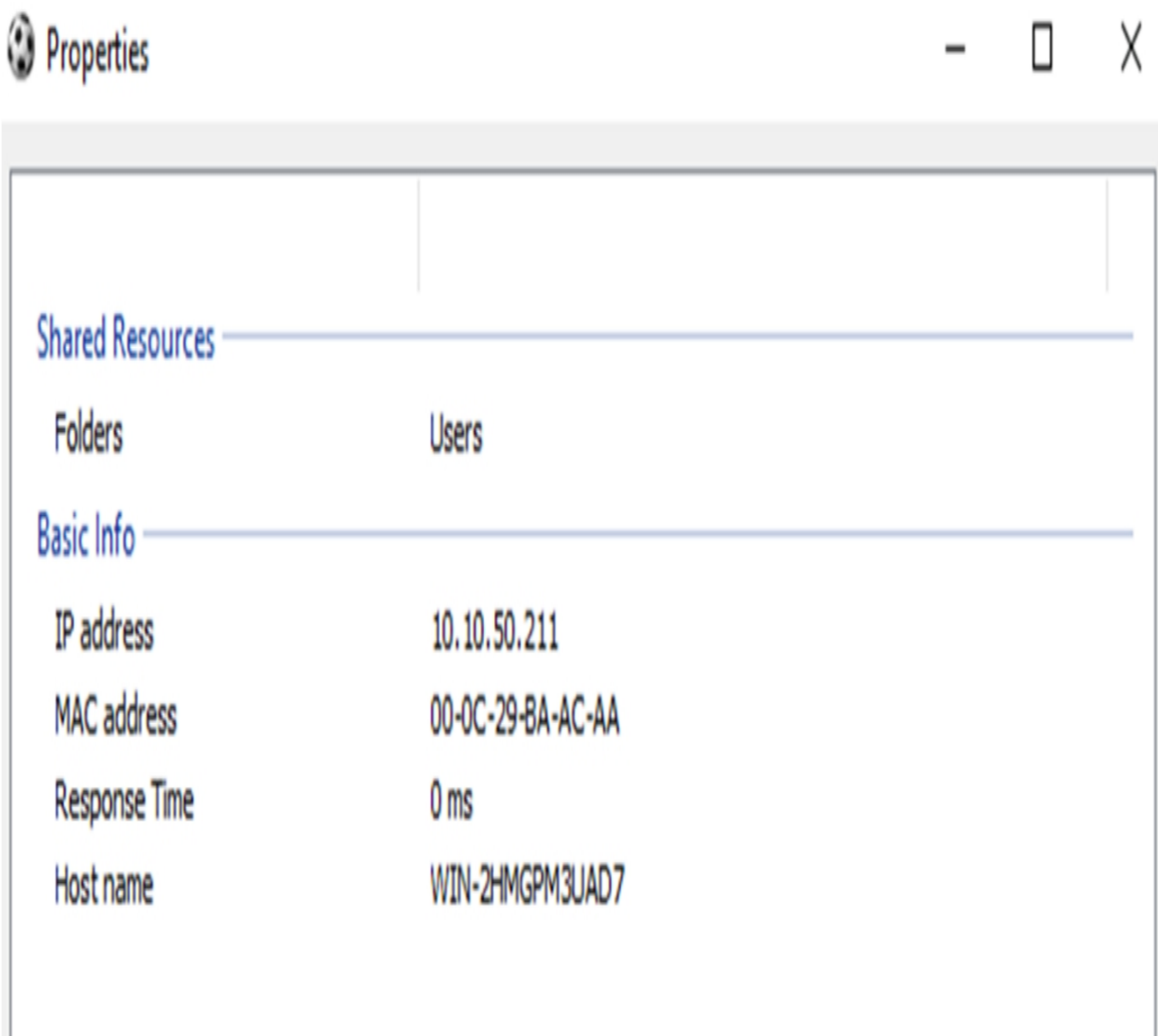


Figure 4–13: Exploring Results

The output shows shared resources and basic information about the host. This host has shared folders with different users.

Figure 4–14: Exploring Results

Now select another host and go to “Properties” .

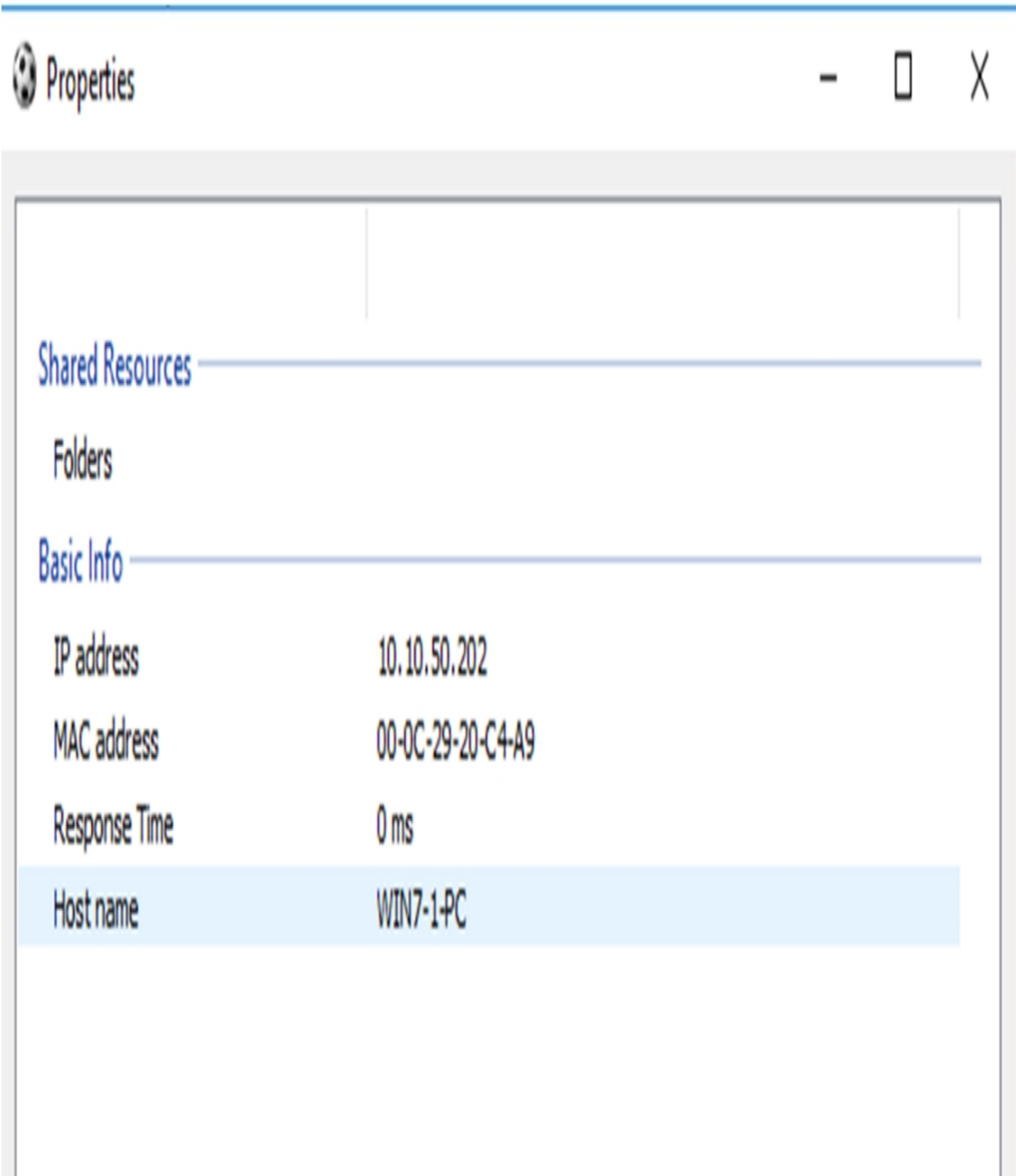


Figure 4–15: Exploring Results

This host does not have any shared resource with anyone.

SNMP Enumeration

Simple Network Management Protocol (SNMP) enumeration is a technique in which information regarding user accounts and devices is

targeted using the most widely used network management protocol, SNMP. SNMP requires a community string to authenticate the management station.

replies sends

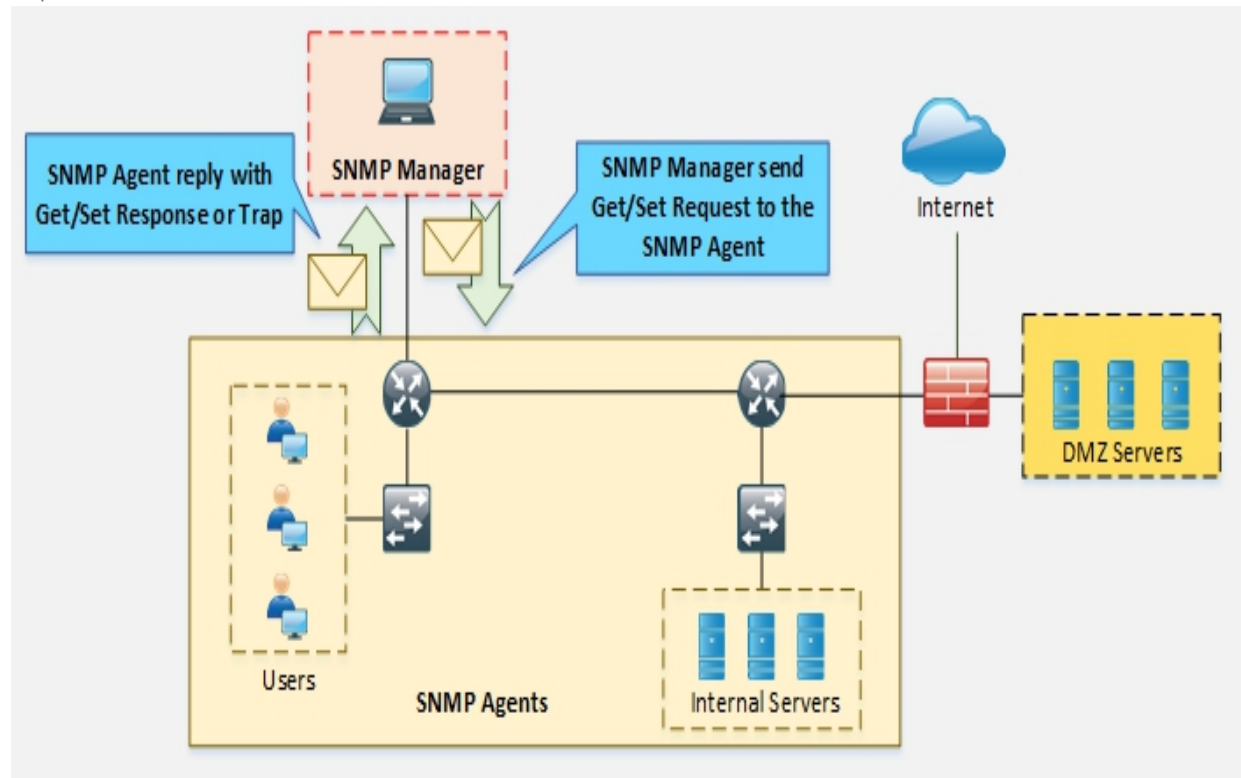


Figure 4-16: SNMP Working

There are different forms of community string in different versions of SNMP. By guessing the default community string and gaining unauthorized access, attackers can extract information such as host, devices, shares, network information, etc.

Community Strings Description SNMP Read-only

Community String
SNMP Read-Write
Community String

SNMP Trap Community Enables a remote device to retrieve "read-only" information from a device

Used for requesting information from a device and to modify settings on that device

Sends SNMP Traps to InterMapper

String *Table 4-05: SNMP Community String Types*

Simple Network Management Protocol

In a production environment where thousands of networking devices such as routers, switches, servers, and endpoints are deployed, Network Operation Center (NOC) has to play a very important role. Almost every single vendor supports Simple Network Management Protocol (SNMP). Initially, SNMP deployment requires a Management Station. A management station collects information about different aspects of network devices. Next is configuration and software support by networking devices themselves. A configuration like the type of encryption and hashing being run on a management station's software must match the SNMP settings on networking devices. Technically three components are involved in deploying SNMP in a network:

SNMP Manager

This is a software application running on the management station for displaying the

collected information from networking devices in a clear and representable manner. Commonly used SNMP software are PRTG, Solarwinds, OPManager, etc.

SNMP Agent

This software runs on networking nodes whose different components need to be monitored. Examples include CPU/RAM usage, interface status, etc. UDP port number 161 is used for communication between the SNMP agent and SNMP manager. *Management Information Base*

MIB stands for Management Information Base: a collection of information organized

hierarchically in a virtual database. These databases are accessed using a protocol like SNMP.

There are two types of MIBs:

MIB Types **Description** **Scaler** This defines a single object instance
Tabular This defines multiple related object instances *Table 4-06: MIB Types*

Scalar objects define a single object instance whereas tabular objects define multiple related object instances grouped in MIB tables. MIBs are collections of definitions that define the properties of the managed object within the device to be managed.

This collection of information is addressed through Object Identifiers (OIDs). These OIDs include MIB objects like string, address, counter, access level and other information.

MIB example: The typical objects to monitor on a printer are the different cartridge states and maybe the number of printed files, and the typical objects of interest are the inbound and outbound traffic as well as the rate of packet loss or the number of packets addressed to a broadcast address.

The features of available SNMP variants are:

Version Features

No Support for encryption and hashing. Plain text community string is used for v1 authentication

No support for encryption and hashing either. Some great functions, for example, v2c the ability to get data in bulk from agents, are implemented in version 2c
Support for both encryption (DES) and hashing (MD5 or SHA).

Implementation

of version 3 has three models. NoAuthNoPriv means no encryption and hashing v3 will be used. AuthNoPriv means only MD5 or SHA based hashing will be used. AuthPriv means both encryption and hashing will be used for SNMP traffic *Table 4-07: SNMP Versions*

SNMP Enumeration Tool

OpUtils

OpUtils is a network monitoring and troubleshooting tool for network engineers. OpUtils is powered by Manage Engines, which supports a number of tools for switch port and IP address management. It helps network engineers to manage their devices and IP address space with

ease. It performs network monitoring, detection of a rogue device intrusion, bandwidth usage monitoring, etc.

Download Website: [https://www.manageengine.com/SolarWinds Engineer's Toolset](https://www.manageengine.com/SolarWinds_Engineer's_Toolset)

SolarWinds Engineer's Toolset is a network administrator's tool that offers hundreds of networking tools for troubleshooting and for diagnosing the performance of the network.

Download Website: <https://www.solarwinds.com/>
Key features are:

- Automated network detection
- Monitoring and alerting in real time • Powerful diagnostic capabilities
- Improved network security
- Configuring and managing logs
- Monitoring of IP addresses and DHCP scope

LDAP Enumeration

The Lightweight Directory Access Protocol LDAP is an open standard, internet protocol. LDAP is used for accessing and maintaining distributed directory information services in a hierarchical and logical structure. A directory service plays an important role by allowing information such as user, system, network, service information, etc. to be shared throughout the network. LDAP provides a central place to store usernames and passwords. Applications and services connect to the LDAP server to validate users. The client initiates an LDAP session by sending an operation request to the Directory System Agent (DSA) using TCP port 389. The communication between client and server uses Basic Encoding Rules (BER). Directory services using LDAP include:

- Active Directory
- Open Directory
- Oracle iPlanet
- Novell eDirectory
- OpenLDAP

LDAP Enumeration Tool

LDAP Enumeration Tools that can be used for the enumeration of LDAP-enabled systems and services include:

LDAP Enumeration Tool Website JXplorer www.jxplorer.org LDAP Admin Tool www.ldapsoft.com LDAP Account Manager www.ldap-account-manager.org Active Directory Explorer technet.microsoft.com LDAP Administration Tool sourceforge.net LDAP Search securityexploded.com Active Directory Domain Services Management Pack www.microsoft.com LDAP Browser/Editor www.novell.com *Table 4-08: LDAP Enumeration Tools*

NTP Enumeration

Network Time Protocol (NTP)

NTP stands for Network Time Protocol and is used in a network to synchronize the clocks across the hosts and network devices. NTP is an important protocol, as directory services, network devices, and hosts rely on clock settings for login and logging purposes to keep a record of events. NTP helps in correlating events by time system logs are received by Syslog servers. NTP uses UDP port number 123, and its whole communication is based on Coordinated Universal Time (UTC).

NTP uses a term known as **stratum** to describe the distance between the NTP server and device. It is just like a TTL number that decreases with every hop when a packet passes by. The stratum value, starting from one, increases with every hop. For example, if we see stratum number 10 on a local router, it means that the NTP server is nine hops away. Securing NTP is also an important aspect, as the attacker may alter timings to mislead the forensic teams who investigate and correlate the events to find the root cause of the attack.

NTP Authentication

NTP version 3 (NTPv3), and advanced versions support a cryptographic authentication technique between NTP peers. This authentication can be used to mitigate an attack. Three commands are used in the NTP master and the NTP client:

```
Router(config)# ntp authenticate
```

```
Router(config)# ntp authentication-key key-number md5 key-value
```

```
Router(config)# ntp trusted-key key-number
```

Even without NTP authentication configuration, network time information is still exchanged between servers and clients. The difference is that these NTP clients do not consider the NTP server as a secure source because of the possibilities of the legitimate NTP server going down and a fake NTP server taking over the real NTP server are high.

NTP Enumeration

Another important aspect of collecting information is the time at which a specific event occurs. Attackers may try to change the timestamp settings of the router or may introduce a rogue NTP server to the network to mislead the forensic teams. Thanks to the creators of NTP v3, it supports authentication with NTP server and its peers. It is possible to gather information from NTP using different tools such as

commands, Nmap, and NSE script. In the process of enumerating through NTP, an attacker generates queries to the NTP server to extract valuable information from the responses, such as:

- Information of the host connected to NTP server
 - Client's IP address, machine's name, Operating System information •
- Network information such as internal IPs or topology map may be disclosed from

NTP packets depending upon the deployment of NTP server, i.e., if NTP server is deployed in DMZ

NTP Enumeration Commands

`ntpdc` is used for questioning the `ntpd` daemon regarding the current state and requested changes in state.

```
root@kali:~# ntpdc [ -<flag> [<val>] | --<name> [{=| }<val>] ]...
```

[host...] `ntpdc` command can be used with the following options:

Options Description

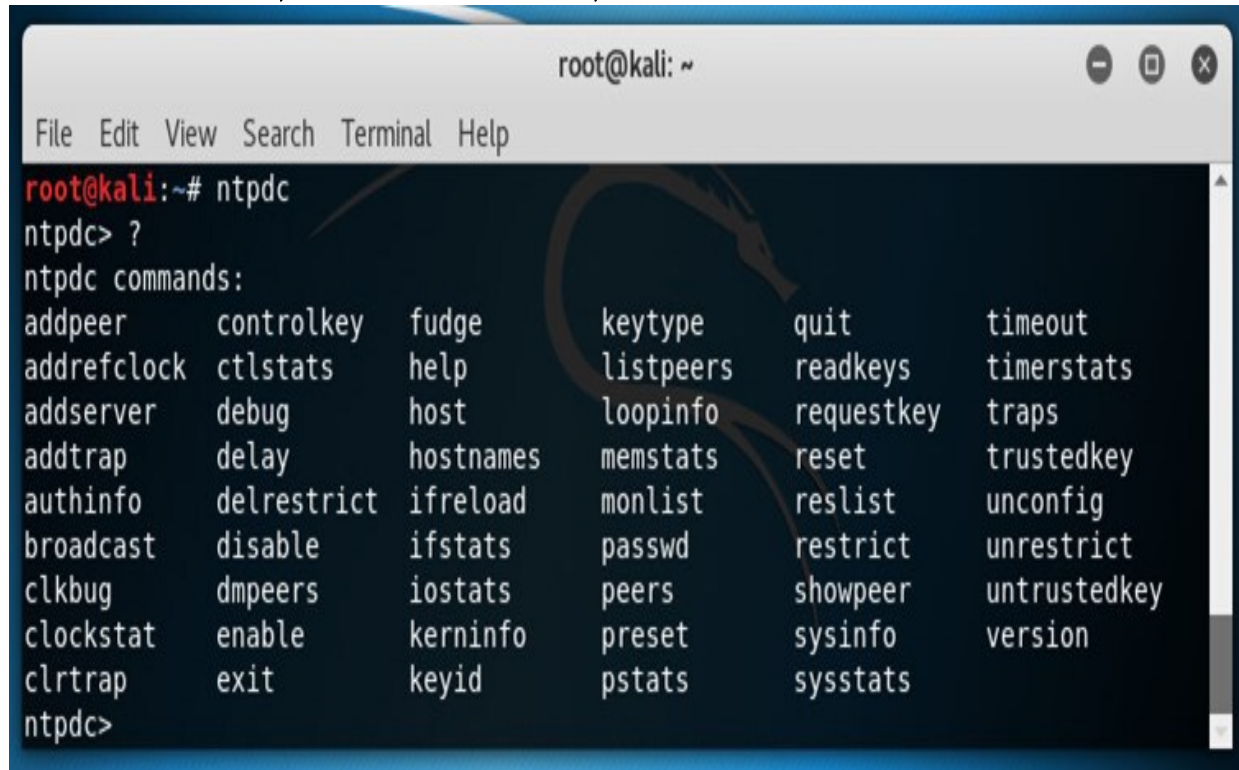
- i This option forces operation in interactive mode
- n Displays host addresses in the dotted-quad numeric format

-l Displays the list of peers known to the server(s)
-p Displays the list of the peers known to the server, additionally,
displays the

summary of their state

-s Displays list of peers known to the server, a summary of their state,
in a different format, equivalent to -c dmpeers

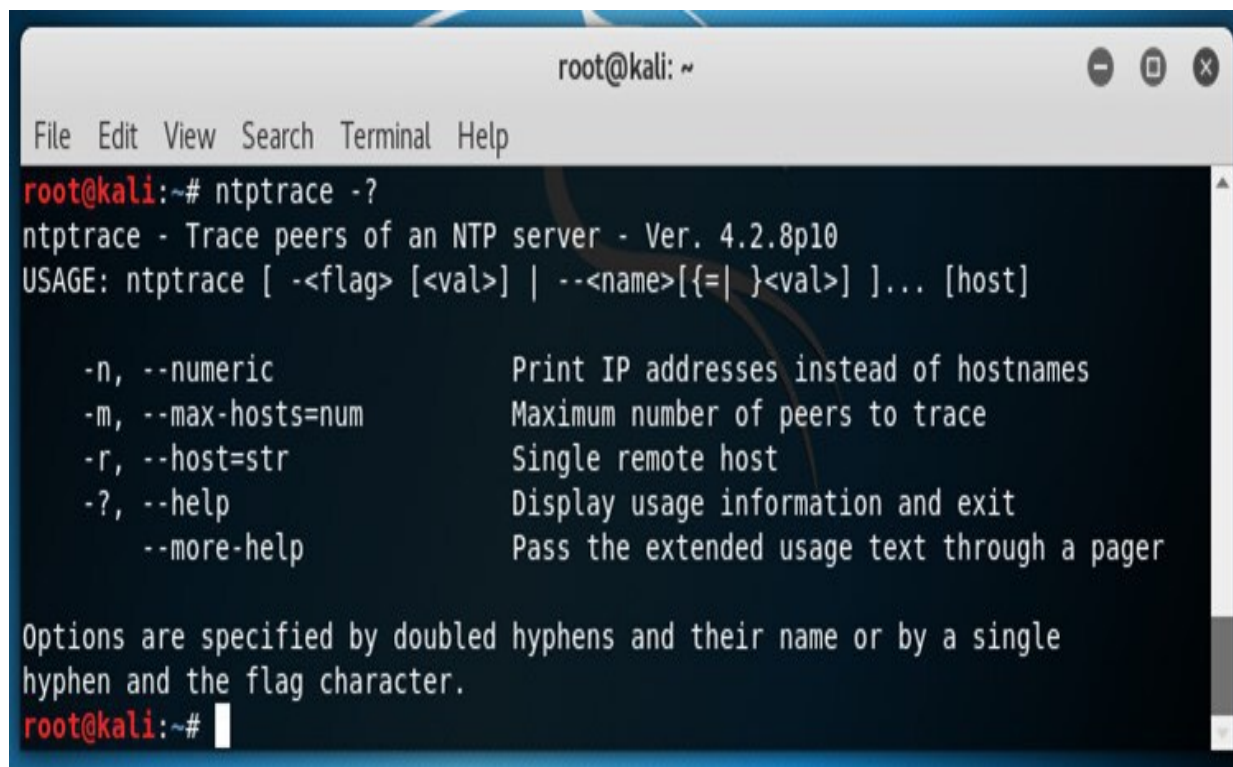
Table 4-09: ntpdc Command Options

A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the command 'ntpdc' being entered at the prompt 'root@kali:~#'. Below this, the prompt changes to 'ntpdc>' and the user enters '?'. The terminal then displays a list of ntpdc commands in a grid-like format. The commands are: addpeer, addrefclock, addserver, addtrap, authinfo, broadcast, clkbug, clockstat, clrtap, controlkey, ctlstats, debug, delay, delrestrict, disable, dmpeers, enable, exit, fudge, help, host, hostnames, ifreload, ifstats, iostats, kerninfo, keyid, keytype, listpeers, loopinfo, memstats, monlist, passwd, peers, preset, pstats, quit, readkeys, requestkey, reset, reslist, restrict, showpeer, sysinfo, sysstats, timeout, timerstats, traps, trustedkey, unconfig, unrestrict, untrustedkey, and version.

```
root@kali:~# ntpdc
ntpdc> ?
ntpdc commands:
addpeer      controlkey  fudge      keytype    quit        timeout
addrefclock  ctlstats   help       listpeers  readkeys    timerstats
addserver    debug      host       loopinfo   requestkey  traps
addtrap      delay      hostnames  memstats   reset       trustedkey
authinfo     delrestrict ifreload   monlist    reslist     unconfig
broadcast    disable    ifstats    passwd     restrict    unrestrict
clkbug       dmpeers    iostats    peers      showpeer    untrustedkey
clockstat    enable     kerninfo   preset     sysinfo     version
clrtap       exit       keyid      pstats     sysstats
ntpdc>
```

Figure 4-17: ntpdc Commands

ntptrace is a Perl script, which uses ntpq to follow the chain of NTP servers from a given host back to the primary time source. ntptrace requires implementation of the NTP Control and Monitoring Protocol specified in RFC 1305, and NTP Mode 6 packets enabled to work properly.

A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the command 'ntptrace -?' being executed. The output displays the version '4.2.8p10' and the usage: 'ntptrace [-<flag> [<val>] | --<name>[={<val>}]]... [host]'. A list of options follows: '-n, --numeric' (Print IP addresses instead of hostnames), '-m, --max-hosts=num' (Maximum number of peers to trace), '-r, --host=str' (Single remote host), '-?, --help' (Display usage information and exit), and '--more-help' (Pass the extended usage text through a pager). A note states: 'Options are specified by doubled hyphens and their name or by a single hyphen and the flag character.' The prompt 'root@kali:~#' is visible at the bottom with a cursor.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ntptrace -?
ntptrace - Trace peers of an NTP server - Ver. 4.2.8p10
USAGE: ntptrace [ -<flag> [<val>] | --<name>[={<val>}] ]... [host]

-n, --numeric          Print IP addresses instead of hostnames
-m, --max-hosts=num    Maximum number of peers to trace
-r, --host=str         Single remote host
-?, --help             Display usage information and exit
--more-help            Pass the extended usage text through a pager

Options are specified by doubled hyphens and their name or by a single
hyphen and the flag character.
root@kali:~#
```

Figure 4-18: ntptrace Commands

ntpq is a command line utility that is used for inquiring the NTP server. The ntpq is used to monitor NTP daemon ntpd operations and determine performance. It uses the standard NTP mode 6 control message formats.

Ntpq command can be used with the following options:

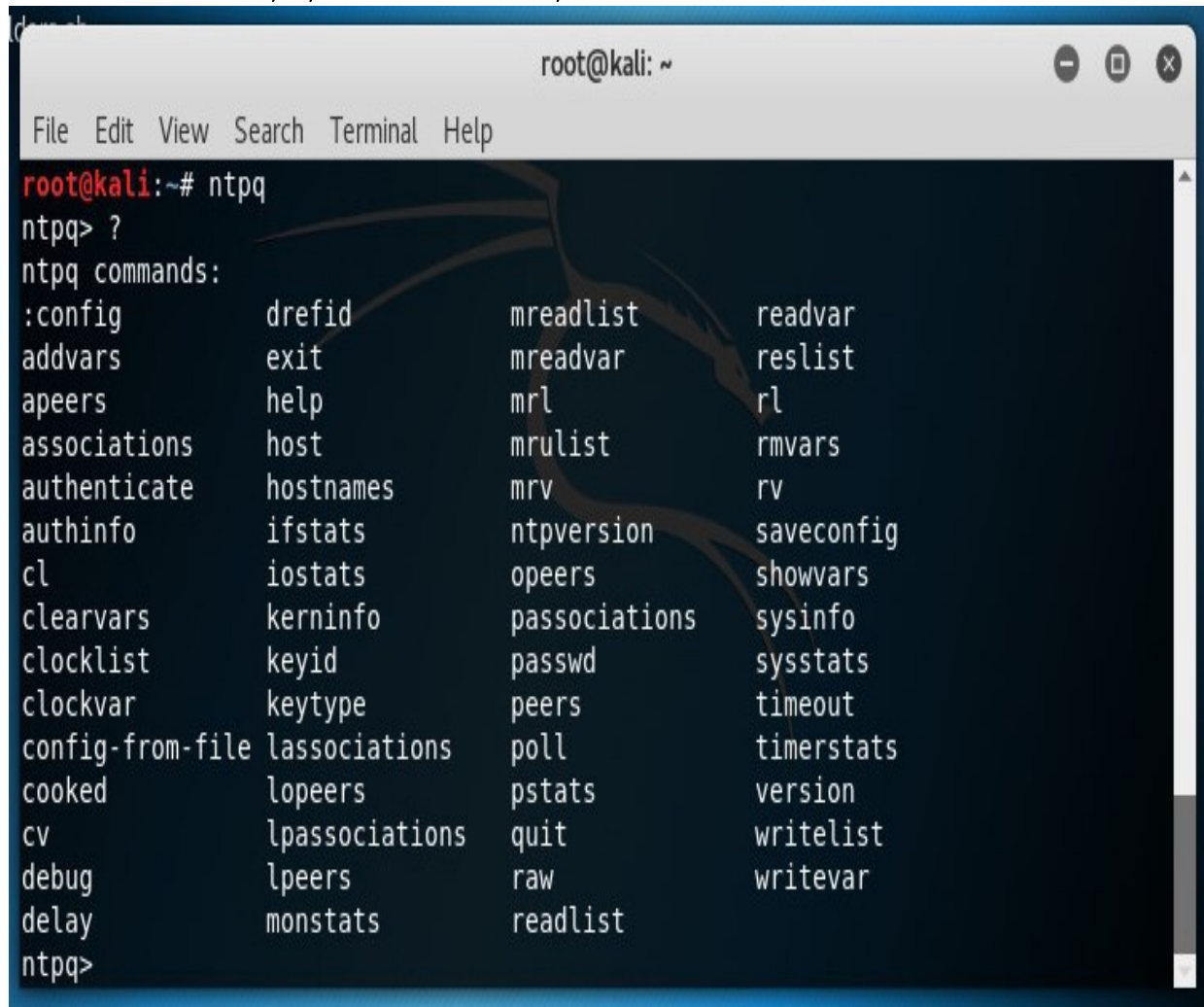
Options Description

- c The following argument is interpreted as an interactive format command and is added to the list of commands to be executed on the specified host(s). Multiple -c options may be given
- d Turns on debugging mode
- i Forces ntpq to operate in interactive mode. Prompts will be written to the standard output and commands read from the standard input
- n Outputs all host addresses in the dotted-quad numeric format rather than converting to the canonical host names
- p Prints a list of the peers known to the server as well as a summary of their state. This is equivalent to the peer's interactive command

-4 Forces DNS resolution of the following host names on the command line to the IPv4 namespace

-6 Forces DNS resolution of the following host names on the command line to the IPv6 namespace

Table 4-10: ntpq Command Options

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the command 'ntpq' being executed, followed by the prompt 'ntpq> ?'. The output lists various ntpq commands in a four-column format. The commands listed are: :config, drefid, mreadlist, readvar, addvars, exit, mreadvar, reslist, a peers, help, mrl, rl, associations, host, mrulist, rmvars, authenticate, hostnames, mrv, rv, authinfo, ifstats, ntpversion, saveconfig, cl, iostats, o peers, showvars, clearvars, kerninfo, passociations, sysinfo, clocklist, keyid, passwd, sysstats, clockvar, keytype, peers, timeout, config-from-file, lassociations, poll, timerstats, cooked, lo peers, pstats, version, cv, lpassociations, quit, writelist, debug, l peers, raw, writevar, delay, monstats, readlist, and ntpq>.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ntpq
ntpq> ?
ntpq commands:
:config      drefid      mreadlist   readvar
addvars      exit        mreadvar    reslist
a peers      help        mrl          rl
associations host        mrulist     rmvars
authenticate hostnames   mrv          rv
authinfo     ifstats     ntpversion   saveconfig
cl           iostats     o peers      showvars
clearvars    kerninfo    passociations sysinfo
clocklist    keyid       passwd       sysstats
clockvar     keytype     peers        timeout
config-from-file lassociations poll          timerstats
cooked       lo peers    pstats       version
cv           lpassociations quit          writelist
debug        l peers     raw          writevar
delay        monstats    readlist
ntpq>
```

*Figure 4-19: ntpq Commands
NTP Enumeration Tools*

- Nmap
- NTP server scanner • Wireshark
- NTPQuery

SMTP Enumeration

Simple Mail Transfer Protocol (SMTP)

SMTP Enumeration is another way to extract information about the target by using Simple Mail Transfer Protocol (SMTP). SMTP Protocol ensures the mail communication between email servers and recipients over internet port 25. SMTP is one of the most popular TCP/IP protocols widely used by most of the email servers, now defined in RFC 821.

SMTP Enumeration Technique

Following are some of the SMTP commands that can be used for enumeration. SMTP server responses for commands such as VRFY, RCPT TO, and EXPN are different. By inspecting and comparing the responses for valid and invalid users through interacting with the SMTP server via telnet, valid users can be determined.

Command Function

HELO To identify the domain name of the sender EXPN To verify Mailbox on local host

MAIL FROM To identify the sender of the email RCPT TO To specify the message recipients

SIZE To specify Maximum Supported Size Information DATA To define data

RSET To reset the connection and buffer of SMTP VRFY To verify the availability of Mail Server HELP To show help.

QUIT To terminate a session.

Table 4-11: SMTP Commands SMTP Enumeration Tool

- NetScan Tool Pro
- SMTP-user-enum
- Telnet

DNS Zone Transfer Enumeration Using Nslookup

In the enumeration process through DNS Zone transfer, an attacker finds the target's TCP port 53, as TCP port 53 is used by DNS, and Zone transfer uses this port by default. Using port scanning techniques, you can find out whether the port is open or not.

DNS Zone Transfer

DNS Zone transfer is the process that is performed by DNS. In the process of Zone transfer, DNS passes a copy containing database records to another DNS server. The DNS Zone transfer process provides support for resolving queries, as more than one DNS server can respond to the queries.

Consider a scenario, in which both primary and secondary DNS servers are responding to queries. The secondary DNS server gets the copy of the DNS records to update the information in its database.

DNS Zone Transfer Using Nslookup Command

1. Go to Windows command line (CMD), type “nslookup” and press “Enter”.



```
C:\Users\tbi>nslookup
Default Server: UnKnown
Address: fe80::1

> www.example.com
Server: UnKnown
Address: fe80::1

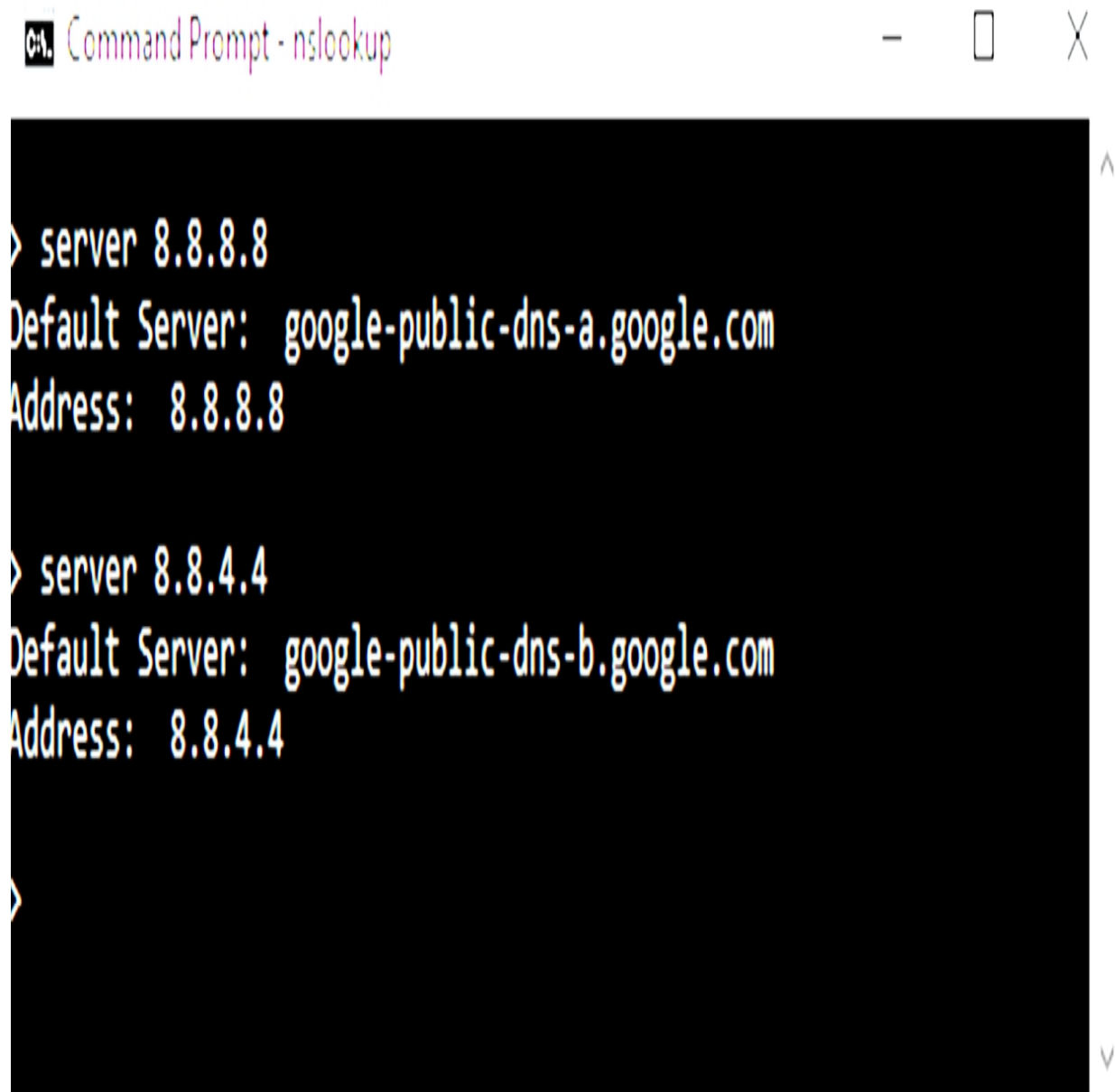
Non-authoritative answer:
Name:    www.example.com
Addresses: 2606:2800:220:1:248:1893:25c8:1946
          93.184.216.34

>
```

Figure 4-20: nslookup Command

2. Command prompt will proceed to the ">" symbol.
3. Enter "server <DNS Server Name>" or "server <DNS Server

Address>".



```
Command Prompt - nslookup

> server 8.8.8.8
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

> server 8.8.4.4
Default Server: google-public-dns-b.google.com
Address: 8.8.4.4

>
```

Figure 4-21: NsLookup Command

4. Enter “set type=any” and press “Enter”. It will retrieve all records from a DNS server.
5. Enter “ls -d <Domain>”, this will display the information from the target domain (if allowed).



```
Command Prompt - nslookup

> set type=any
> ls -d ipspecialist.net
[google-public-dns-a.google.com]
ipspecialist.net.      MX      10      ipspecialist.net.
ipspecialist.net.      NS      1      ipspecialist.net.
ipspecialist.net.      NS      2      ipspecialist.net.
ipspecialist.net.      A       1      192.168.1.1
```

Figure 4-22: Nslookup Command

6. If not allowed, it will show “request failed”.



```
Command Prompt - nslookup

> ls -d ipspecialist.net
[google-public-dns-a.google.com]
*** Can't list domain ipspecialist.net: Server failed
The DNS server refused to transfer the zone ipspecialist.net to your computer. If this
is incorrect, check the zone transfer security settings for ipspecialist.net on the DNS
server at IP address 8.8.8.8.

>
```

Figure 4-23: Nslookup Command

7. Linux supports the dig command. At the command prompt, enter “dig <domain.com> axfr”.

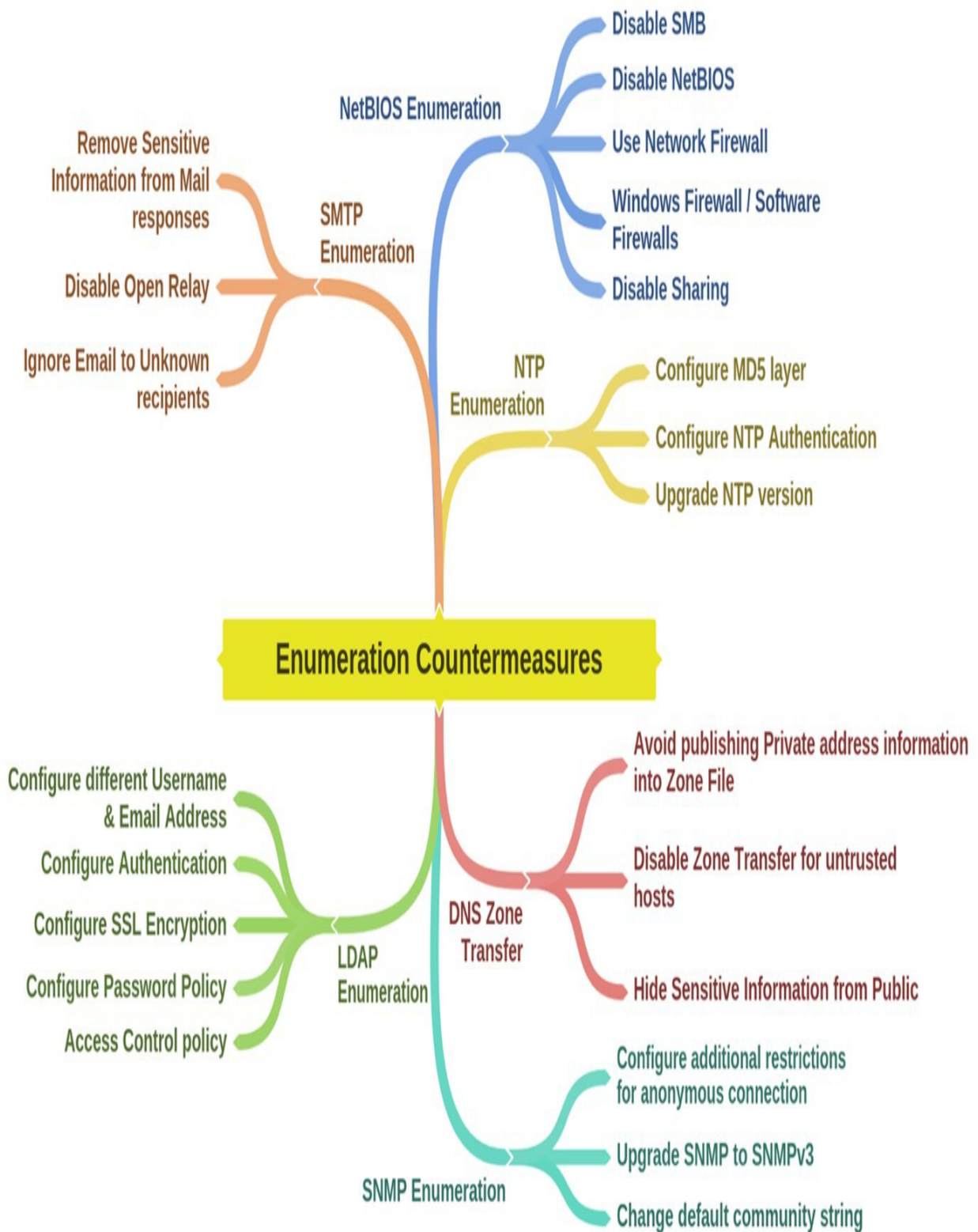
Enumeration Countermeasures

Countermeasures for preventing enumeration are as follows:

1. Use advanced security techniques.
2. Install advanced security software.

3. Use updated versions of protocols.
4. Implement strong security policies.
5. Use unique and difficult passwords.
6. Ensure strong encrypted communication between client and server.
7. Disable unnecessary ports, protocols, sharing, and default enabled services.

Mind Map



Practice Questions

1. What is true about Enumeration?

- A. In the phase of Enumeration, an attacker initiates active connections with the target system to extract more information
- B. In the phase of Enumeration, an attacker collects information about target using Social Engineering
- C. In the phase of Enumeration, an attacker collects information about target using the passive connection
- D. In the phase of Enumeration, an attacker collects information about target using Scanning

2. NetBIOS is basically:

- A. Input / Output System Program
- B. Networking System
- C. Operating System
- D. Graphics Program

3. Which of the following does not belong to NetBIOS Enumeration? A.

- File Sharing Information
- B. Username & Password Information
- C. Group Information
- D. Port Information

4. The command nbstat with the option "-a" extracts the information of:

- A. With hostname, displays the NetBIOS name table and MAC address information
- B. With IP address, display the NetBIOS name table and MAC address information
- C. NetBIOS name cache information
- D. Displays the names registered locally by NetBIOS applications such as the server and redirector

5. The command nbstat with the option "-A" extract the information of:

- A. With hostname, displays the NetBIOS name table and MAC address information