Chapter 4: Enumeration

Technology Brief

In the earlier processes like Footprinting and Scanning, we have understood how to collect information about any organization, target website, or a particular network. We have also discussed several tools that can be helpful in collecting the general information regarding the target. Now we are moving to observe the target more closely in order to gain detailed information. This information is sensitive such as network information, network resources, routing paths, SNMP, DNS and 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 actively.

Enumeration Concepts

Enumeration

In the phase of Enumeration, An attacker initiates active connections with the target system. With this active connection, direct queries are generated to gain more information. These information helps to identify the system attack points. Once attacker discovers attack points, it can gain unauthorized access using this collected information to reach assets.

Information that is enumerated in this phase are: -

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

In the previous phases, the finding was not too concerned with any legal issues. Using the tools required for enumeration phase may cross legal boundaries and chances to being traced as using active connections with the target. You must have proper permission to perform these actions.

Techniques for Enumeration

Enumeration Using Email ID

Extraction of information using Email ID can provide useful information like username, domain name, etc. An Email address contains username and domain name in it.

Enumeration using Default Password

Another way of enumeration is using default passwords. Every device and software has its default credentials and settings. This default setting and configuration are recommended to be changed. Some administrators keep using default passwords and settings. It became so easy for an attacker to gain unauthorized access using default credentials. Finding default settings, configuration and password of a device is not a big deal.

Enumeration using SNMP

Enumeration using SNMP is a process of gaining information through SNMP. The attacker uses default community strings or guesses the string to extract information about a device. SNMP protocol was developed to allow the manageability of devices by the administrator, such as servers, routers, switches, workstations on an IP network. It allows the network administrators to manage network performance of a network, finds, troubleshoots and solve network problems, design, and plan for network growth. SNMP is an application layer protocol. It provides communication between managers and agents. The SNMP system is consisting 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 the access to network resources only to the defined users and computers. The AD is a big target, a greater source of sensitive information for an attacker. Brute force attack to exploit, or generating queries to LDAP services are performed to gather information such as username, address, credentials, privileges information, etc.

Enumeration through DNS Zone Transfer

Enumeration through DNS zone transfer process includes extracting information like locating DNS Server, DNS Records, Other valuable network related information such as hostname, IP address, username, etc. A zone transfer is a process to update DNS servers; Zone file carries valuable information which is retrieved by the attacker. UDP 53 is used for DNS requests from DNS servers. TCP 53 is used for DNS zone transfers to ensure 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 Port to Enumerate

Lab 4-1: Services Enumeration using Nmap

Case Study: In this Lab, consider a network 10.10.10.0/24 where different devices are running. We will enumerate services, ports and operating system information using nmap utility with Kali Linux.

Procedure & Commands:
Open the terminal of Kali Linux Enter the command: root@kali:~# **nmap –sP 10.10.10.0/24**

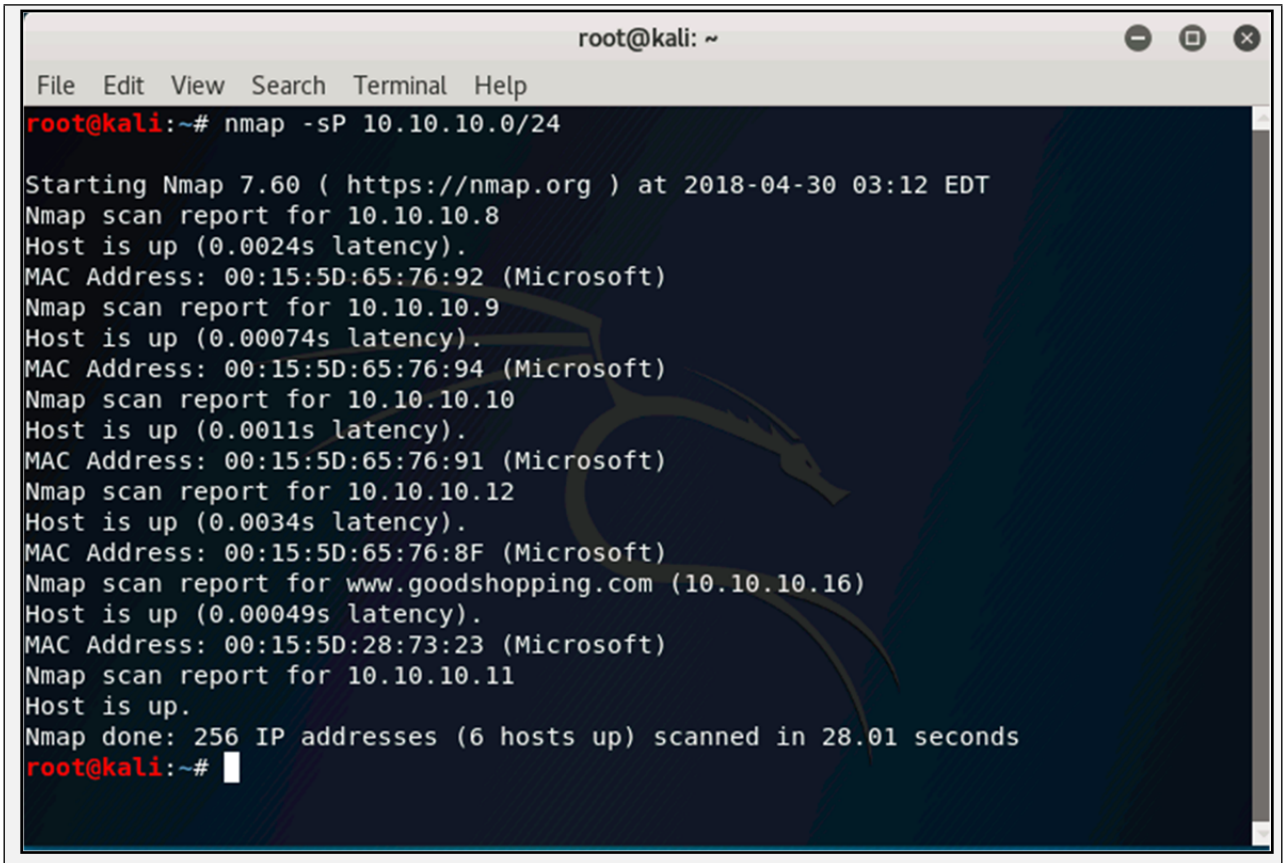


Figure 4-01: Ping Sweep

Performing Ping Sweep on the subnet to check live host and other basic information. Enter the command: root@kali:~# **nmap –sU -p 10.10.10.12**

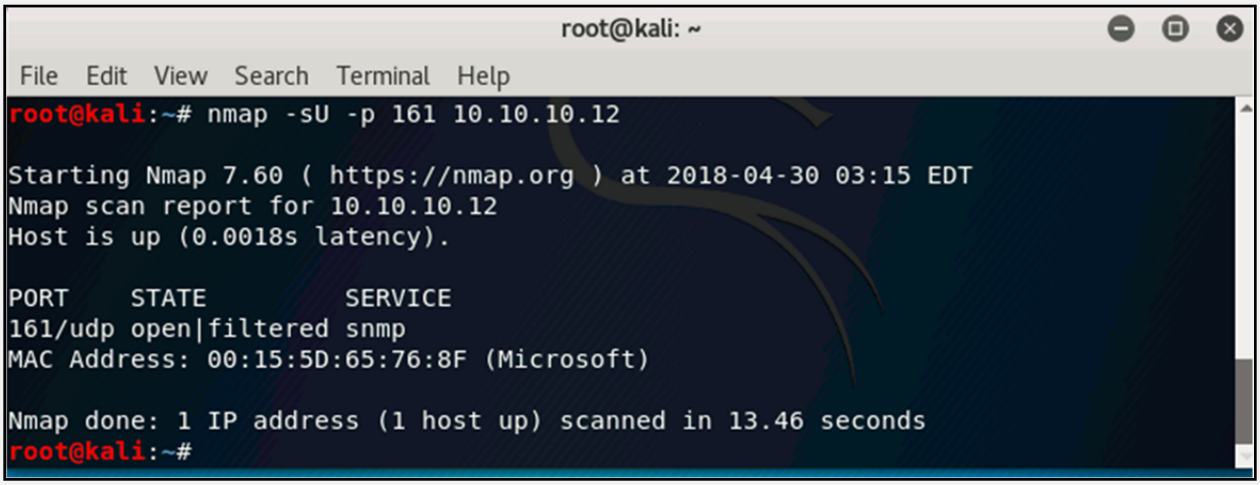


Figure 4-02 UDP Port Scanning

UDP port scanning for port 161 (SNMP Port) for the target host 10.10.10.12. The result shows SNMP port 161 is open & filtered. Now enter the command: root@kali:~# **nmap –sS 10.10.10.12** to perform a Stealthy scan on target host 10.10.10.12

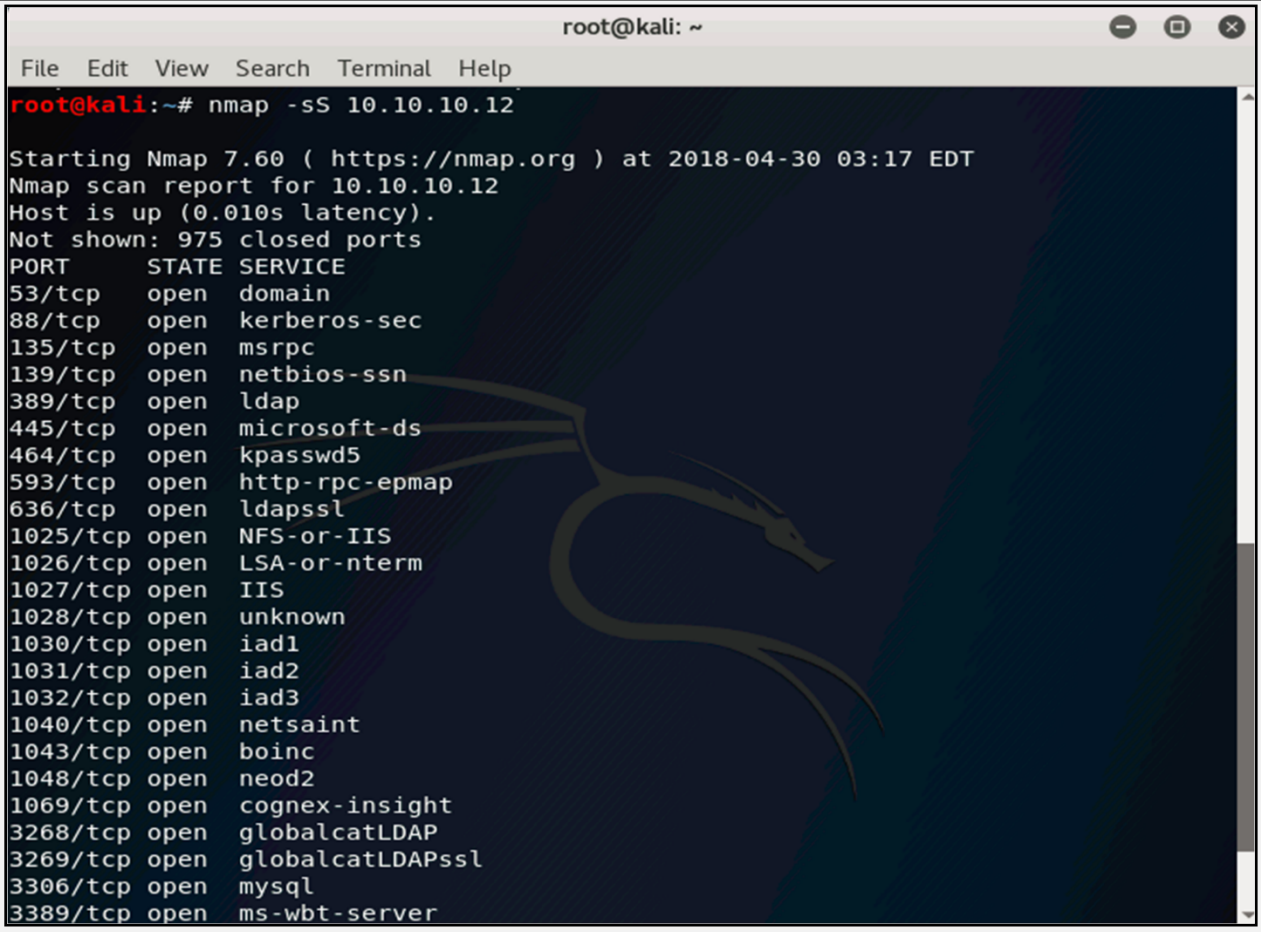


Figure 4-03 Stealth Scan

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**
Operating System & Version scanning on target host 10.10.10.12.

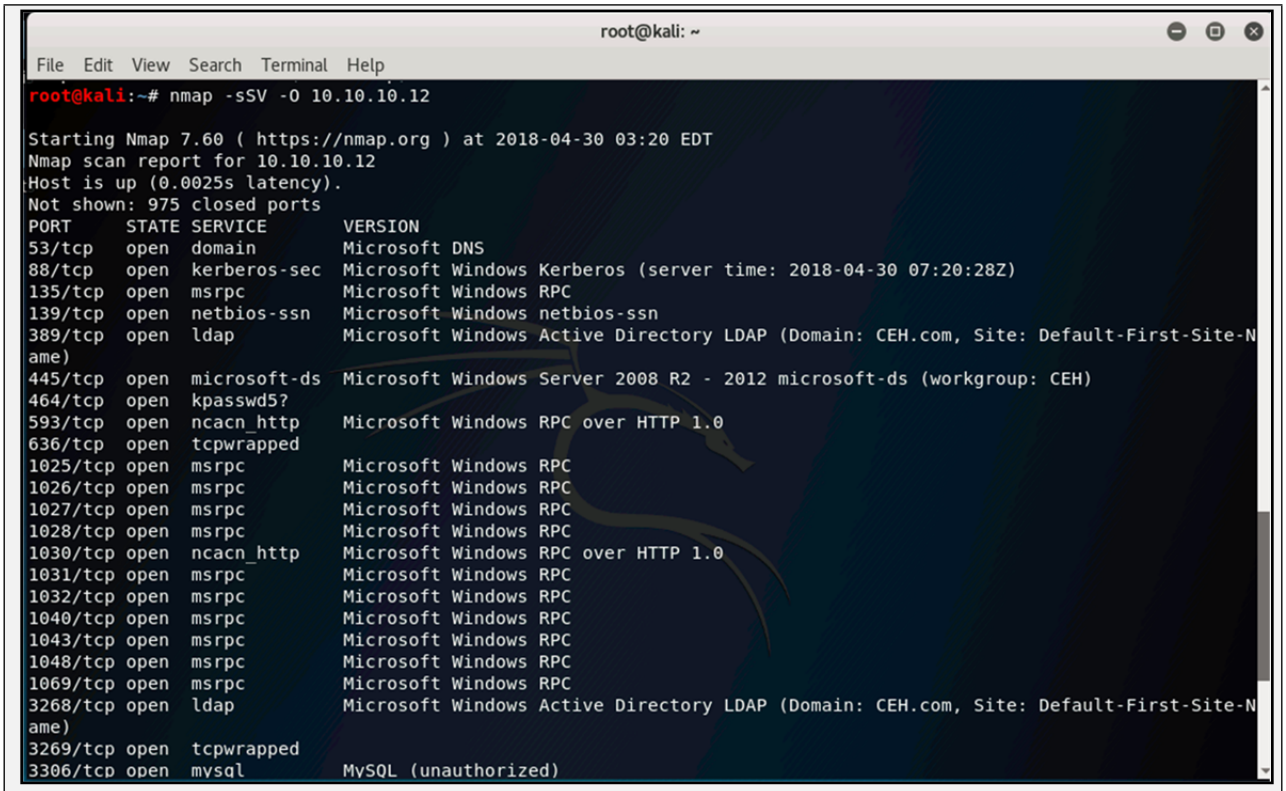


Figure 4-04 OS and Version Scanning

NetBIOS Enumeration

NetBIOS is Network Basic Input / Output System program that allows the communication in between different applications running on different systems within a local area network. NetBIOS service uses a unique 16-ASCII Character string in order to identify the network devices over TCP/IP. The Initial 15 Characters are for identifying the device, 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	Type	Information
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
<\\--__MSBROWSE__>	01	G	Master Browser
<computername>	03	U	Messenger Service
<computername>	06	U	RAS Server Service
<computername>	1F	U	NetDDE Service
<computername>	20	U	File Server Service
<computername>	21	U	RAS Client Service
<computername>	22	U	Microsoft Exchange Interchange(MSMail Connector)
<computername>	23	U	Microsoft Exchange Store
<computername>	24	U	Microsoft Exchange Directory
<computername>	30	U	Modem Sharing Server Service
<computername>	31	U	Modem Sharing Client Service
<computername>	43	U	SMS Clients Remote Control
<computername>	44	U	SMS Administrators Remote Control Tool
<computername>	45	U	SMS Clients Remote Chat
<computername>	46	U	SMS Clients Remote Transfer
<computername>	4C	U	DEC Pathworks TCPIP service on Windows NT
<computername>	42	U	mccaffee anti-virus
<computername>	52	U	DEC Pathworks TCPIP service on Windows NT
<computername>	87	U	Microsoft Exchange MTA
<computername>	6A	U	Microsoft Exchange IMC
<computername>	BE	U	Network Monitor Agent
<computername>	BF	U	Network Monitor Application
<username>	03	U	Messenger Service

<domain>	00	G	Domain Name
<domain>	1B	U	Domain Master Browser
<domain>	1C	G	Domain Controllers
<domain>	1D	U	Master Browser
<domain>	1E	G	Browser Service Elections
<INet~Services>	1C	G	IIS
<IS~computer name>	00	U	IIS
<computername>	[2B]	U	Lotus Notes Server Service
IRISMULTICAST	[2F]	G	Lotus Notes
IRISNAMESERVER	[33]	G	Lotus Notes
Forte_$ND800ZA	[20]	U	DCA IrmaLan Gateway Server Service

Table 4-02 NetBIOS Names

NetBIOS Enumeration Tool

The ***nbstat*** command is a useful tool to display information about NetBIOS over TCP/IP statistics. It is also used to display information such as NetBIOS name tables, name cache, and other information. Command using nbstat utility is shown below: -

```
nbtstat.exe –a "NetBIOS name of the remote system."
nbtstat -A 192.168.1.10
```

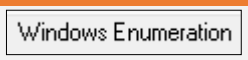
the nbstat command can be used along with several options, list the options available for the nbstat command are as below: -

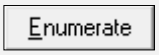
Option	Description
-a	With hostname, Display the NetBIOS name table, MAC address information.
-A	With IP Address, Display the NetBIOS name table, MAC address information.
-c	NetBIOS name cache information.
-n	Displays the names registered locally by NetBIOS applications such as the server and redirector.
-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 nbstat options

Lab 4-2: Enumeration using SuperScan Tool

Procedure:

Open the SuperScan Software, Go to the Windows Enumeration tab 

. Enter the Hostname or IP address of target Windows machine. Go to **Options**/button to customize the Enumeration. Select the Enumeration type from the left section. After configuring, to start enumeration process, Click **Enumerate** 

to initiate the process.

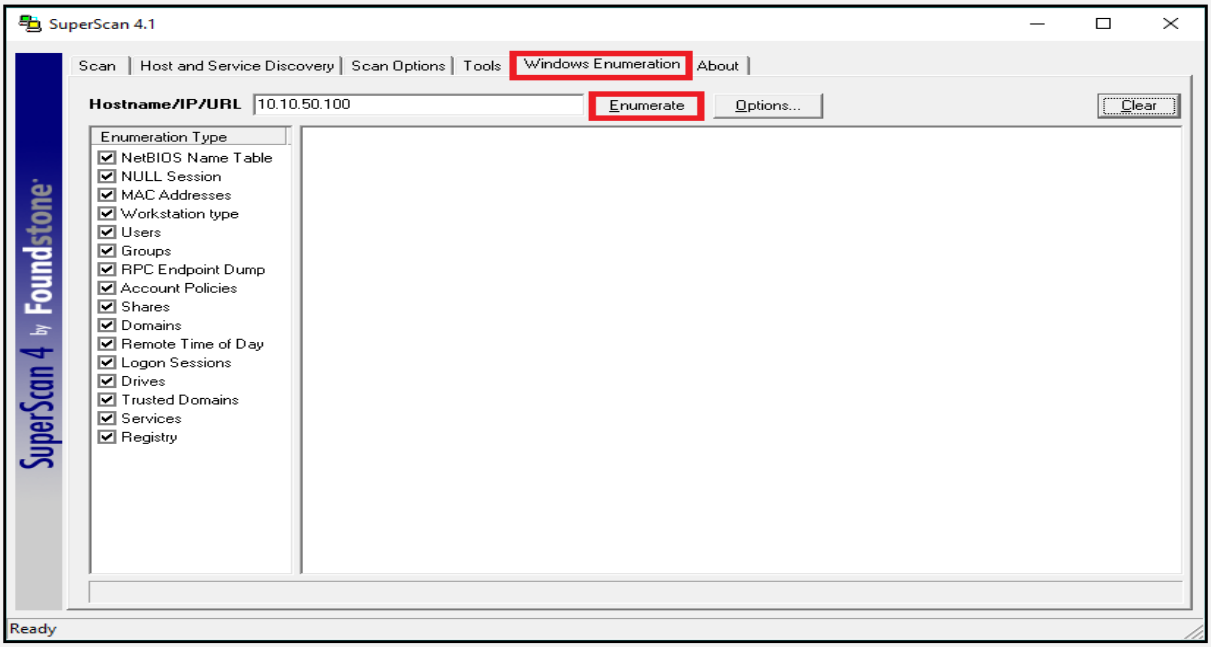


Figure 4-05 Super Scan Enumeration tool

After starting the Enumeration, it will gather the information about the target machine such as MAC address information, operating system information and other information depending upon the type of enumeration selected before initiating the process.

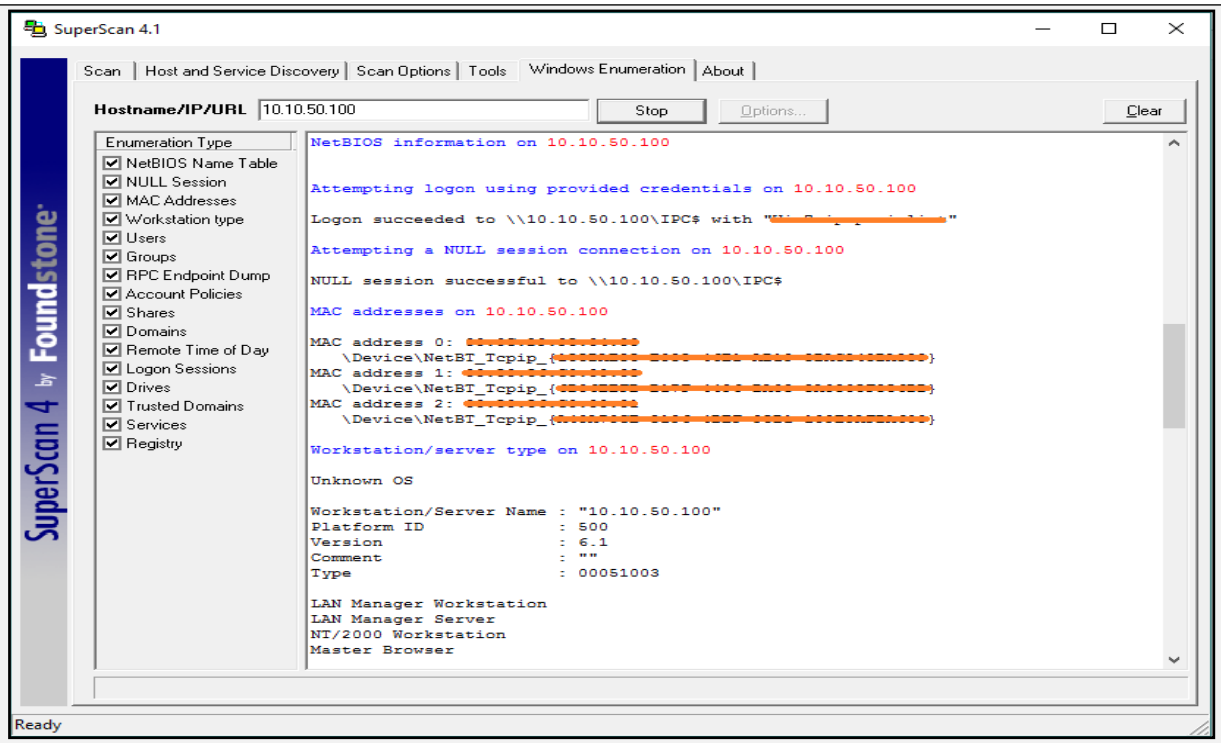


Figure 4-06 Windows Enumeration

Displaying 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, etc.

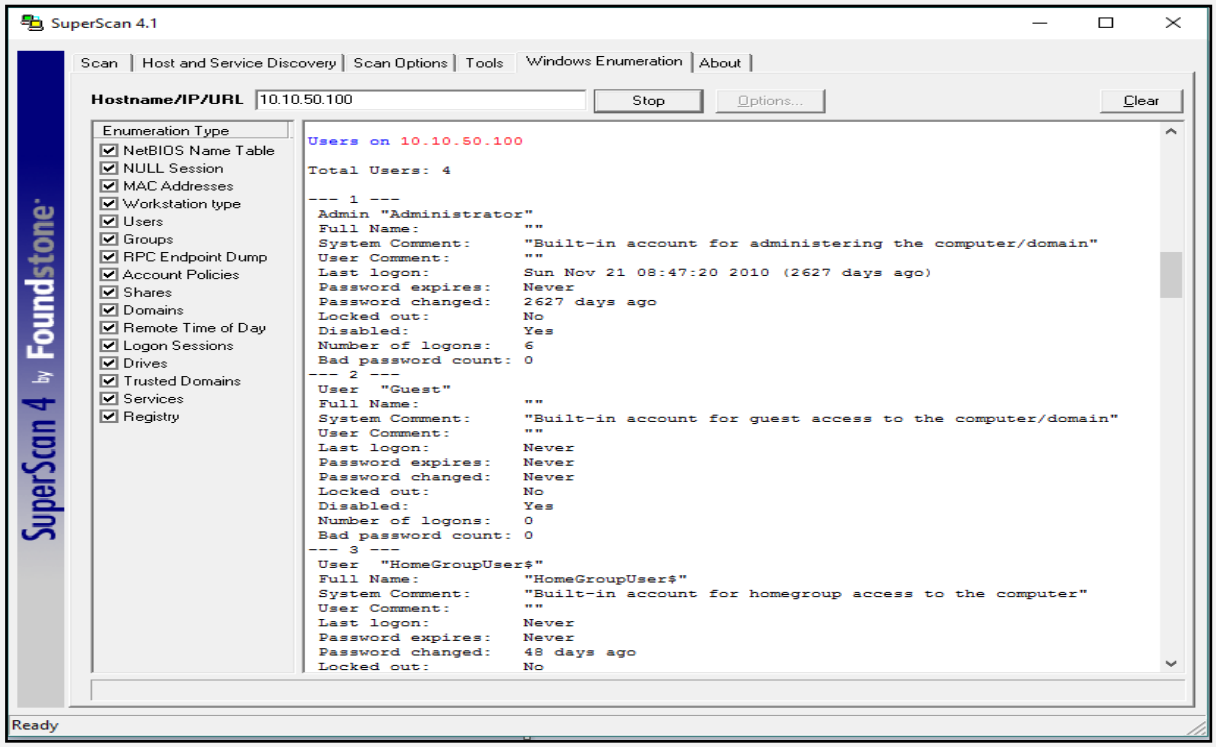


Figure 4-07 Windows Enumeration

The result is showing password and Account policies information, shares information, Remote login information, etc.

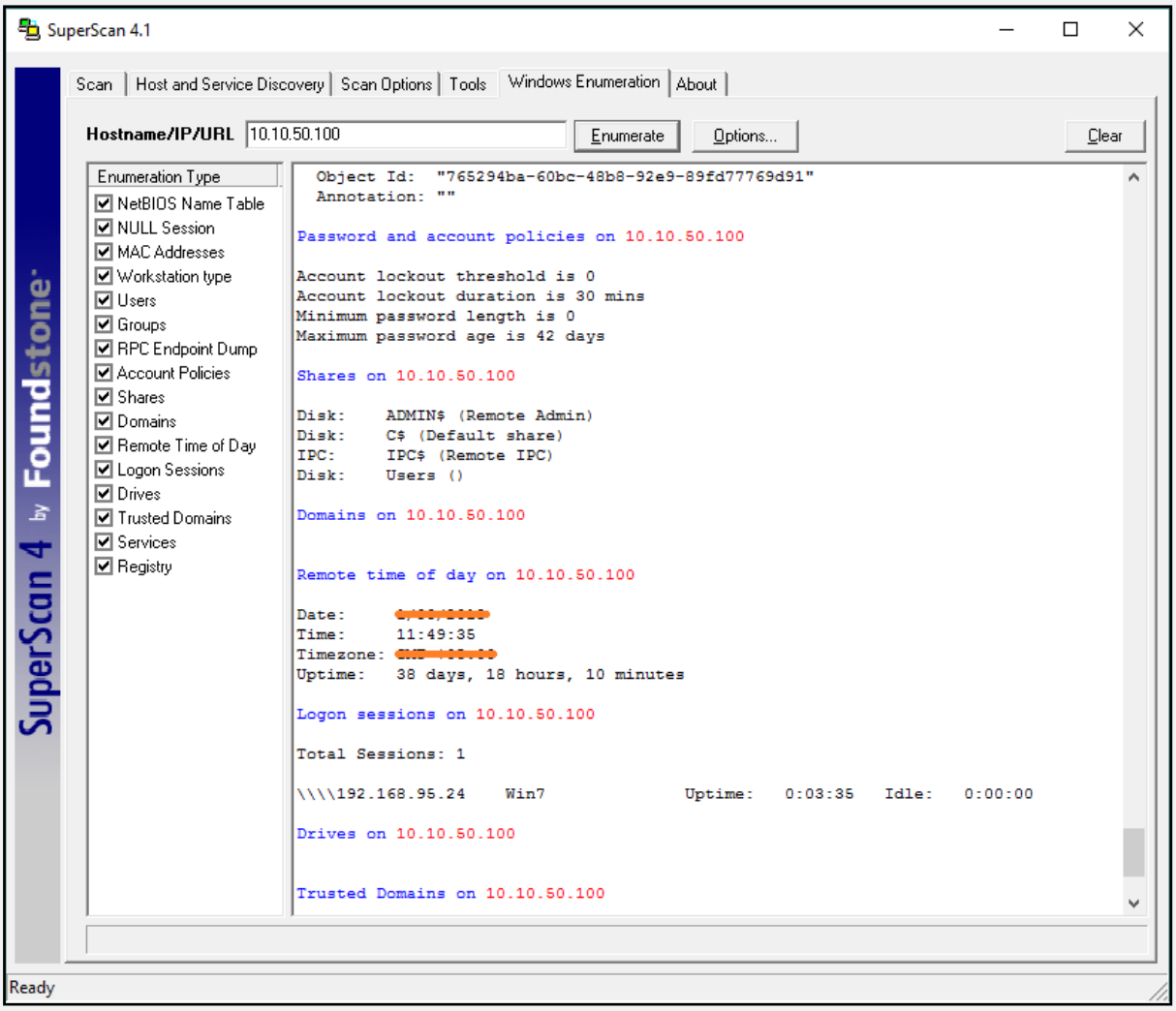


Figure 4-08 Windows Enumeration

Some of the other useful tools are: -

NetBIOS Enumeration Tool	Description
Hyena	Hyena is GUI based, NetBIOS Enumeration tool that shows Shares, User login information and other related information
Winfingerprint	Winfingerprint is NetBIOS Enumeration tool that is capable of providing information such as Operating System, User & Group information, shares, sessions and Services, SIDs, and much more information.
NetBIOS Enumerator	NetBIOS Enumerator is 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 remote host or workgroup. Command Syntax for the Net View utility is: -

```
C:\Users\a>net view [\\computername [/CACHE] | [/ALL] | /DOMAIN[:domainname]]
```

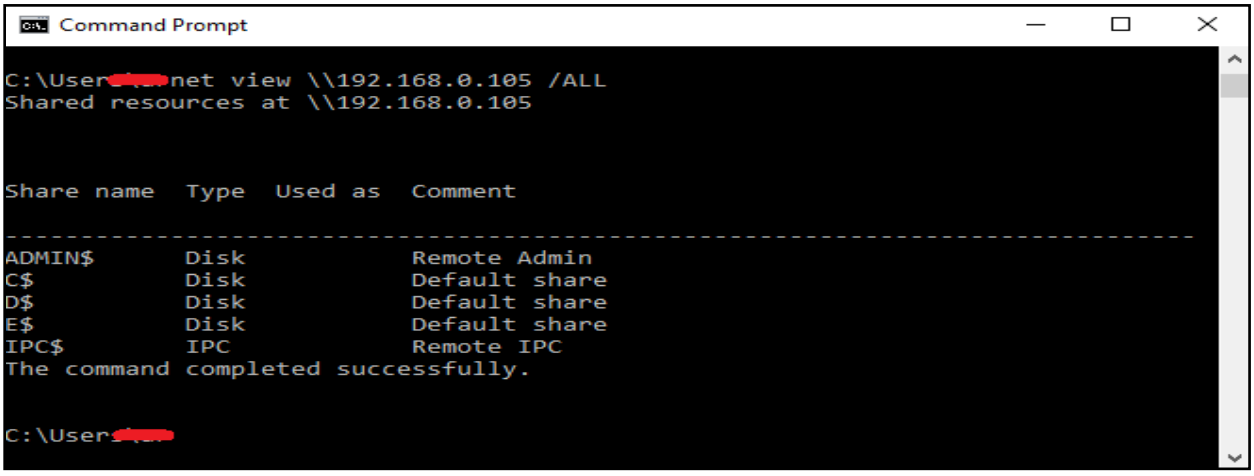


Figure 4-09 Net View

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 2016 to perform scanning using SoftPerfect Network Scanner to scan shared resources in a network.

After Installation, run the application & enter the range of IP address to scan.

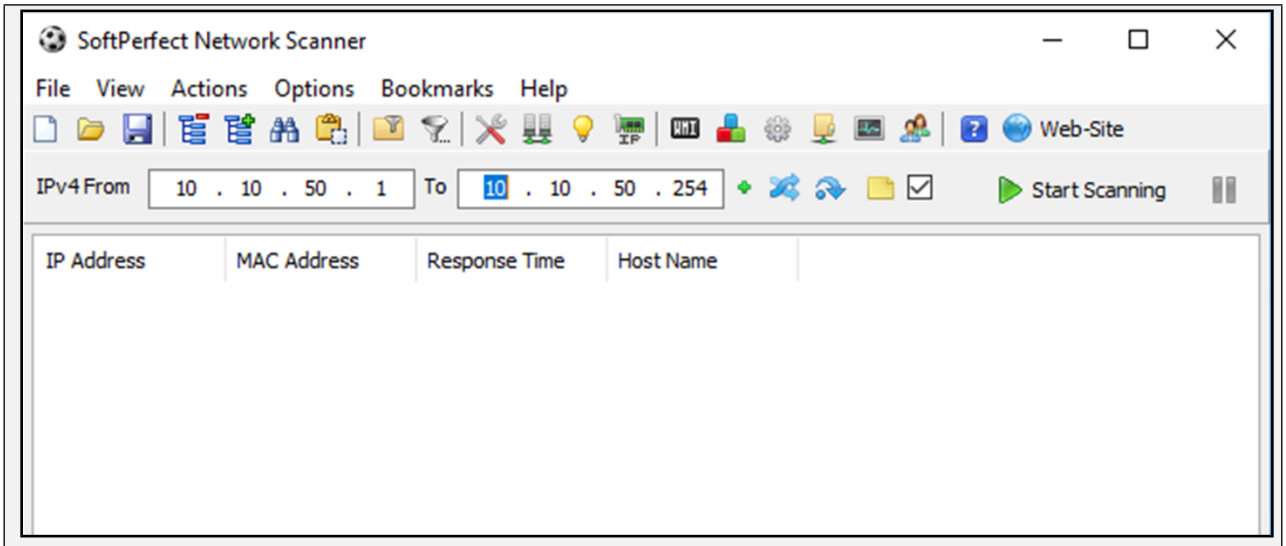


Figure 4-10 SoftPerfect Network Scanner

Now, Click on **Start Scanning** button.

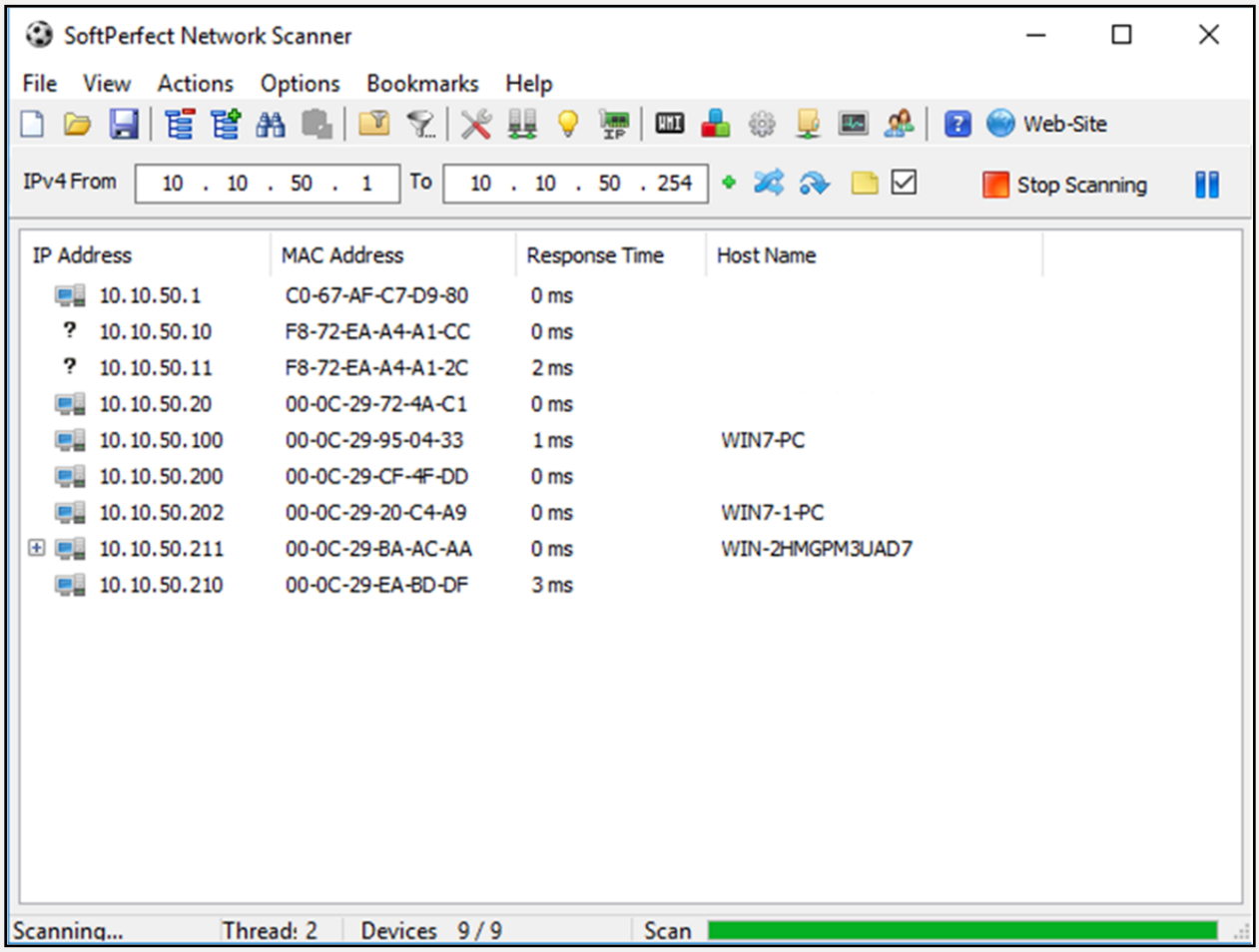


Figure 4-11 Scanning

SoftPerfect Network Scanning tool is scanning for hosts in a given range.

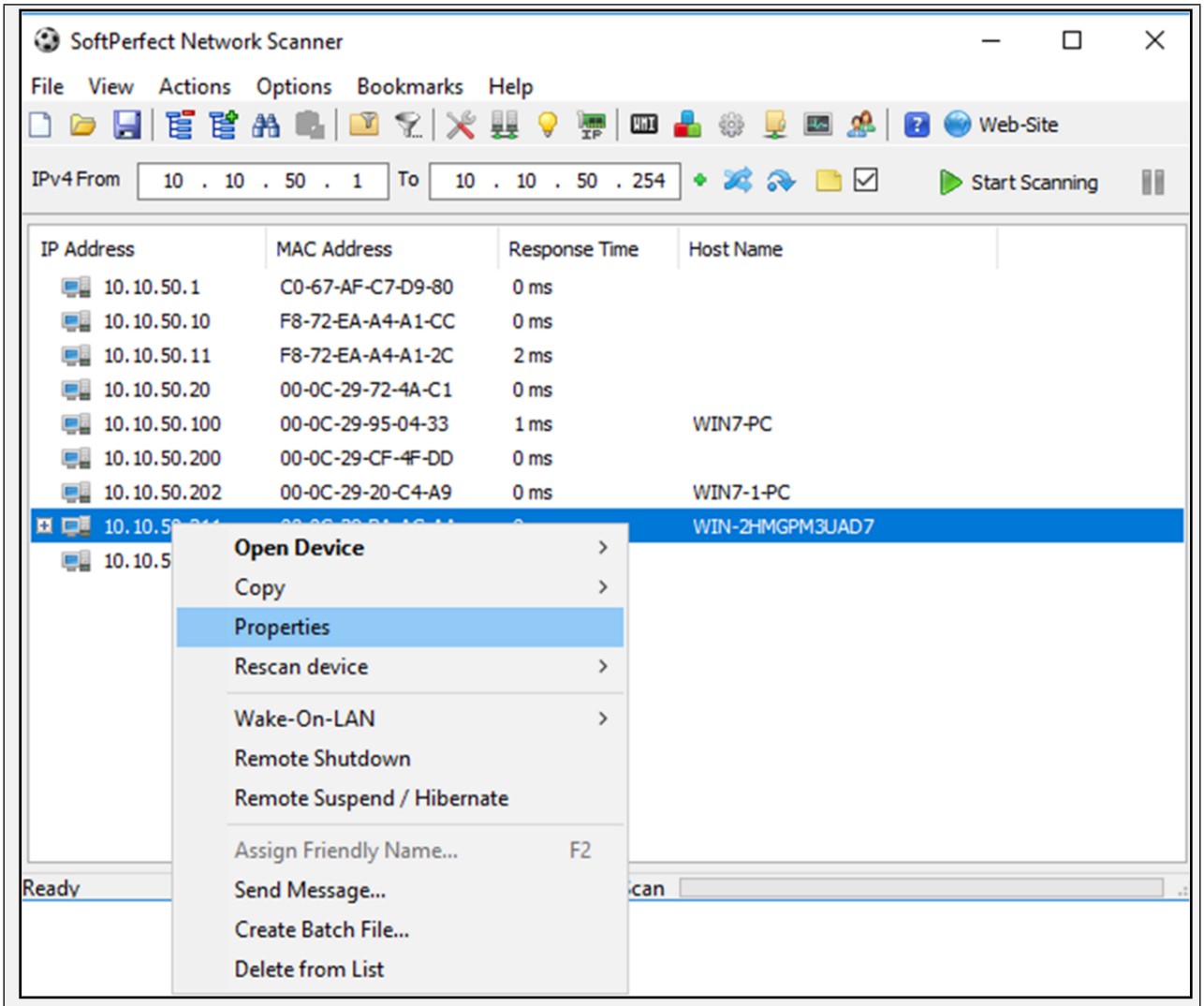


Figure 4-12 Exploring results

After Scanning, select your target host and right click on it.
Go to **Properties**.

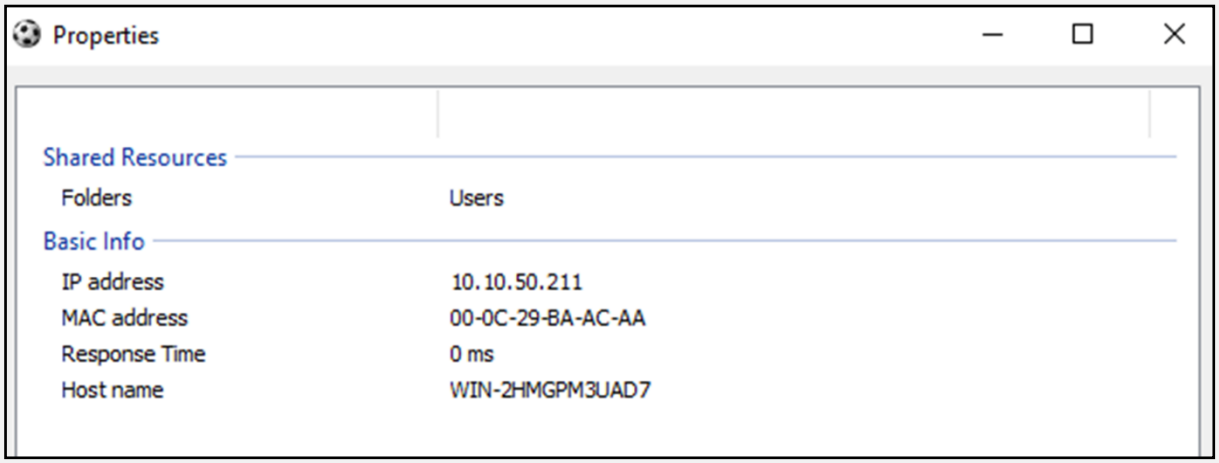


Figure 4-13 Exploring Results

The output is showing shared resource & basic information about the host. This host has shared folders with different users.

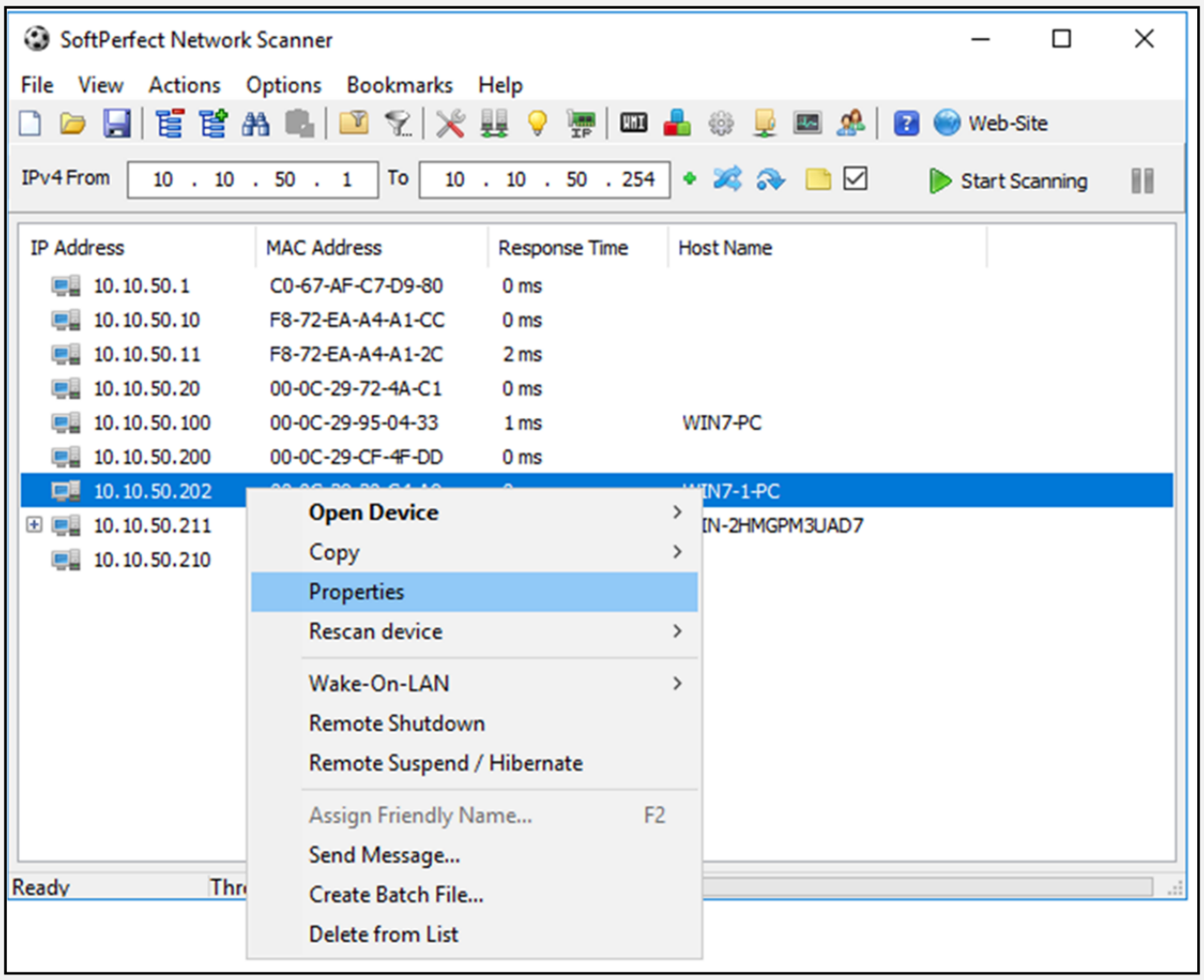


Figure 4-14 Exploring Results

Now select other host and go to properties.

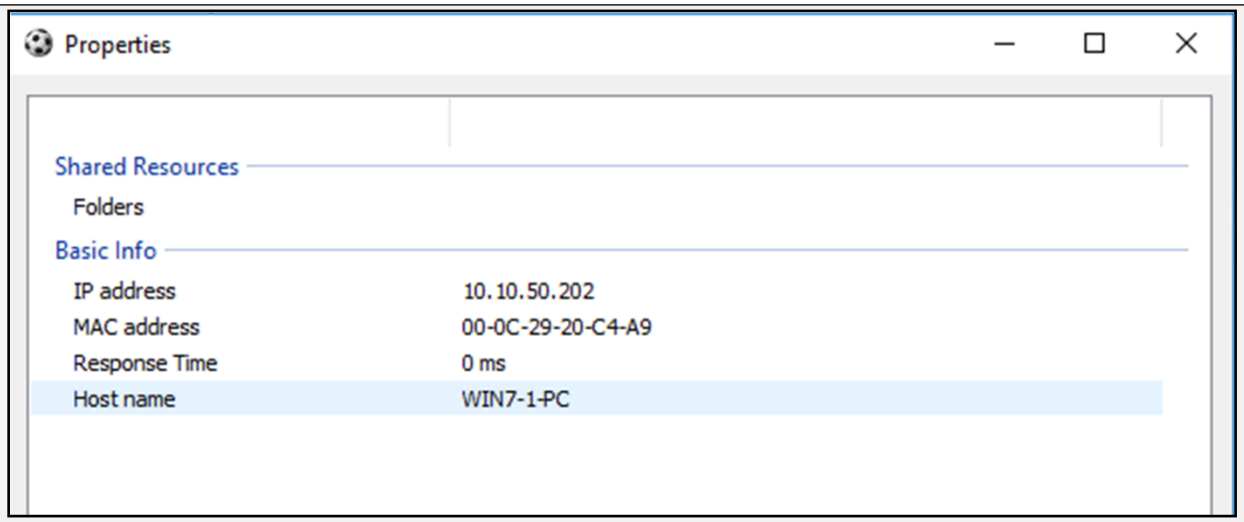


Figure 4-15 Exploring Results

This host does not have any shared resource with anyone.

SNMP Enumeration

SNMP Enumeration

Simple Network Management Protocol (SNMP) Enumeration is a technique of enumeration using most widely used network management protocol SNMP. In SNMP Enumeration, user accounts and device information is targeted using SNMP. SNMP requires community string to authenticate the management station.

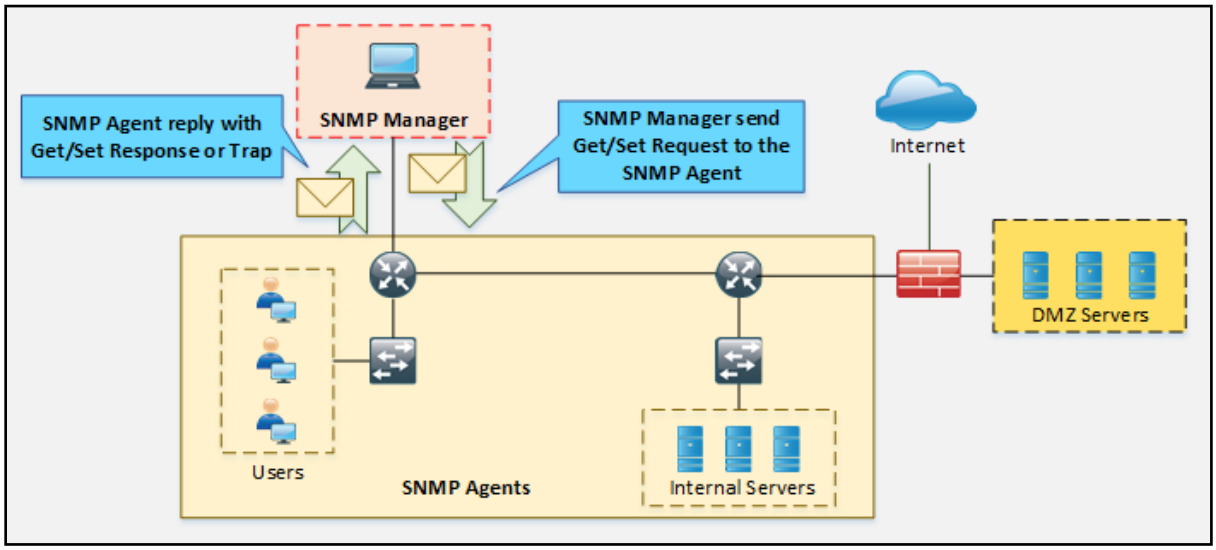


Figure 4-16 SNMP Working

This community string is in a different form in different versions of SNMP. Using the default community string, by guessing the community string, attacker extracts the

information such as Host, devices, shares, network information and much more by gaining unauthorized access.

Community Strings	Description
SNMP Read-only community string	Enables a remote device to retrieve "read-only" information from a device.
SNMP Read-Write community string	Used in requests for information from a device and to modify settings on that device.
SNMP Trap community string	Sends SNMP Traps to InterMapper.

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 Management Station. Management station collects the information regarding different aspects of network devices. The second thing is configuration and software support by networking devices itself. A configuration like the type of encryption and hashing running on management station's software must match with SNMP settings on networking devices.

Technically three components are involved in deploying SNMP in a network: -

SNMP Manager:

A software application running on the management station to display the collected information from networking devices in a nice and representable manner. Commonly used SNMP software are PRTG, Solarwinds, OPManager, etc.

SNMP Agent:

The software is running 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 SNMP agent and SNMP manager.

Management Information Base:

MIB stands for Management Information Base and is a collection of information organized hierarchically in a virtual database. These are accessed using a protocol such as SNMP.

There are two types of MIBs: -

There are two types of MIBs: -

MIB Types	Description

Scaler	It defines a single object instance.
Tabular	It defines multiple related objects 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, which define the properties of the managed object within the device to be managed.

This collection of information such as a description of network objects that are organized & managed hierarchically in MIB using SNMP is addressed through Object identifiers (OIDs). These Object identifiers (OIDs) includes 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 on a switch, the typical objects of interest are the incoming and outgoing 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
V1	No Support for encryption and hashing. Plain text community string is used for authentication
V2c	No support for encryption and hashing either. Some great functions like the ability to get data in bulk from agents are implemented in version 2c
V3	Support for both encryption (DES) and hashing (MD5 or SHA). Implementation of version 3 has three models. NoAuthNoPriv means no encryption and hashing 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, support number of tools for Switch Port & 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 and more.

Download Website: https://www.manageengine.com/

SolarWinds Engineer's Toolset

SolarWinds Engineer's Toolset is a network administrator's tool offers hundreds of networking tools for detection and troubleshooting and network diagnostics.

Download Website: https://www.solarwinds.com/

Key features

- Automated network detection
- Monitoring and alerts in real time
- Powerful diagnostic capabilities
- Improved network security
- Registry configuration and administration
- Monitoring of IP addresses and DHCP scopes

LDAP Enumeration

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol LDAP is an open standard, Internet protocol. LDAP is for accessing and maintaining distributed directory information services in a hierarchical and logical structure. A directory service plays an important role by allowing the sharing of information like user, system, network, service, etc. 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 Directory System Agent (DSA) using TCP port 389. Communication between Client and Server uses Basic Encoding Rules (BER).

Directory services using LDAP includes:

- 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 & 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 is Network Time Protocol used in a network to synchronize the clocks across the hosts and network devices. The NTP is an important protocol, as directory services, network devices and host rely on clock settings for login purposes and logging to keep a record of events. NTP helps in correlating events by the 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 NTP server and device. It is just like TTL number that decreases every hop a packet passes by. Stratum value, starting from one, increases by every hop. For example, if we see stratum number 10 on local router, it means that NTP server is nine hops away. Securing NTP is also an important aspect as the attacker may change time at first place 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 later versions support a cryptographic authentication technique between NTP peers. This authentication can be used to mitigate an attack.

Three commands are used on 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
```

Without NTP Authentication configuration, Network time information still exchanges between server and clients, but the difference is these NTP clients do not authenticate the NTP server as a secure source such as what if the legitimate NTP server goes down and Fake NTP server overtake the real NTP server.

NTP Enumeration

Another important aspect of collecting information is the time at which that specific event occurs. Attackers may try to change the timestamps setting of the router or may introduce rough NTP server in the network to mislead the forensic teams. Thanks to the

creators of NTP v3, it has support for authentication with NTP server before considering its time to be authenticated one.

It is possible to gather information from NTP using different tools such as NTP commands, Nmap and an NSE script. In the process of Enumeration through NTP, attacker generates queries to NTP server to extract valuable information from the responses such as: -

- Host information connected to NTP server
- Client IP address, Machine name, Operating System information
- Network information such as Internal IPs depends upon deployment of NTP server, i.e., if NTP server is deployed in DMZ.

NTP Enumeration Commands

ntpdc is used to query the ntpd daemon regarding current state & request 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 force to operate in interactive mode.
-n	Display host addresses in the dotted-quad numeric format
-l	Display the list of peers which are known to the server(s).
-p	Display the list of the peers known to the server, additionally, display the summary of their state.
-s	Display 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

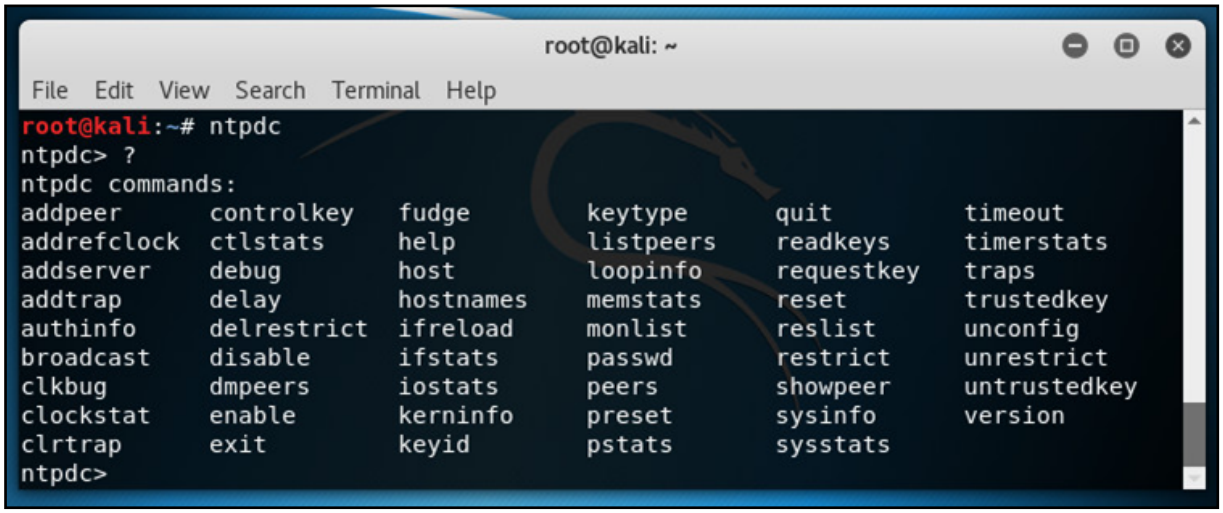


Figure 4-17 ntpdc commands

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

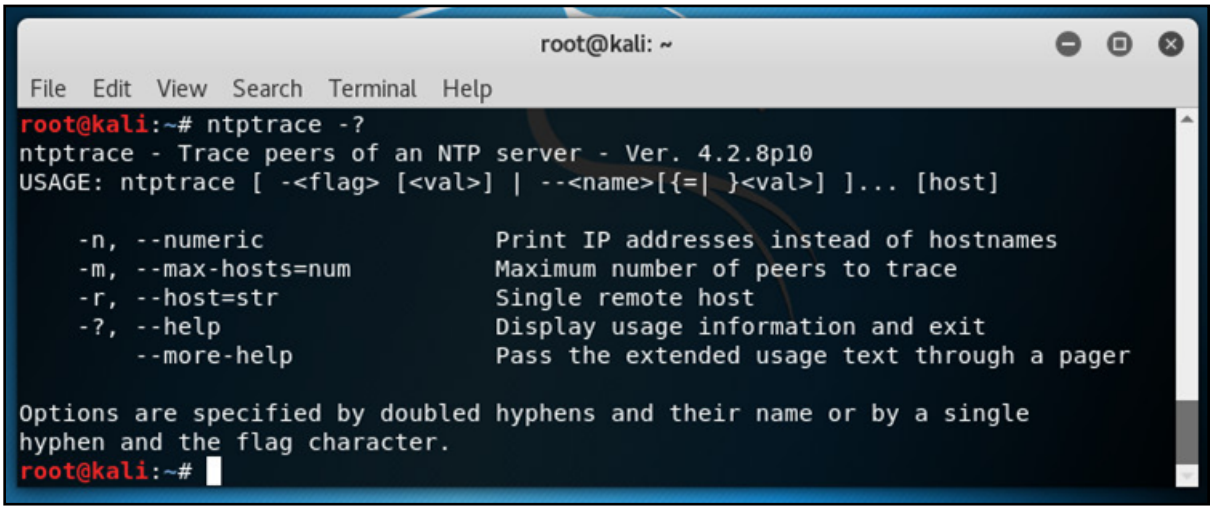


Figure 4-18 ntptrace commands

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

Ntpq command can be used with 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	Turn on debugging mode.
-i	Force ntpq to operate in interactive mode. Prompts will be written to the standard output and commands read from the standard input.
-n	Output all host addresses in the dotted-quad numeric format rather than converting to the canonical host names.
-p	Print 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	Force DNS resolution of following host names on the command line to the IPv4 namespace.
-6	Force DNS resolution of following host names on the command line to

	the IPv6 namespace.

Table 4-10 ntpq command options

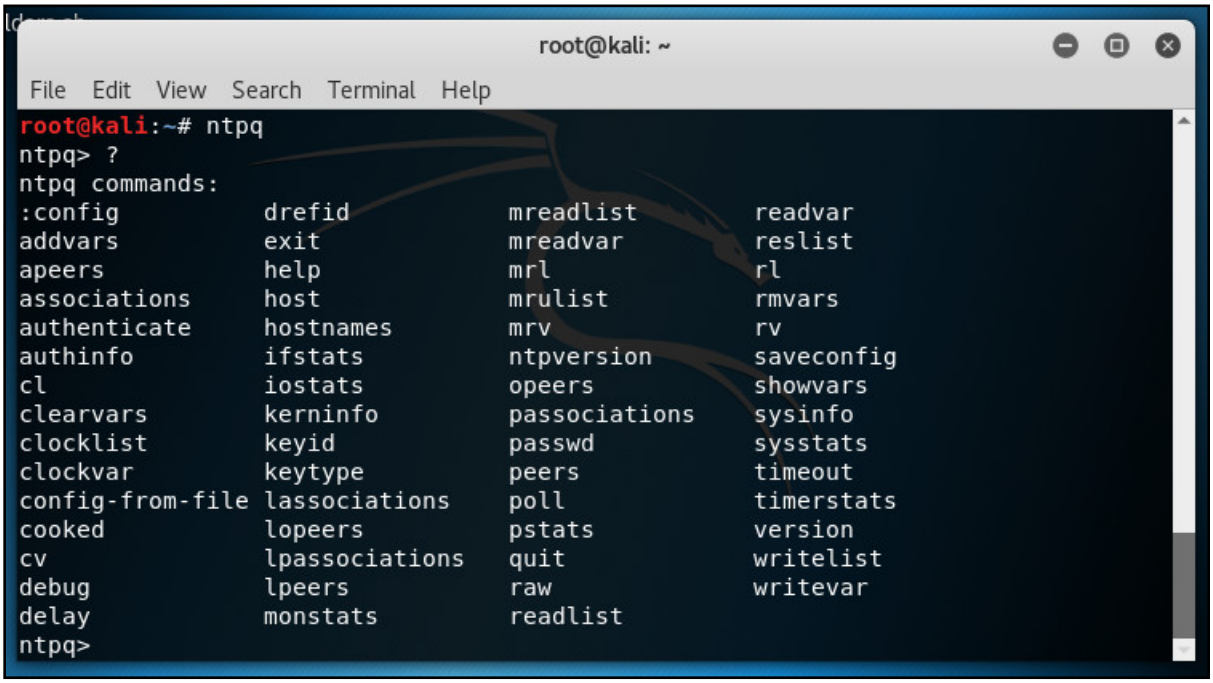


Figure 4-19 ntpq commands

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 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 popular TCP/IP protocol widely used by most of the email servers now defined in RFC 821.

SMTP Enumeration Technique

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

Command	Function

HELO	To identify the domain name of the sender.
EXPN	Verify Mailbox on localhost
MAIL FROM	To identifies the sender of the email.
RCPT TO	Specify the message recipients.
SIZE	To specify Maximum Supported Size Information.
DATA	To define data.
RSET	Reset the connection & buffer of SMTP.
VRFY	Verify the availability of Mail Server.
HELP	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, attacker find 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 if the port is open.

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. 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 the queries. Secondary DNS server gets the DNS records copy to update the information in its database.

DNS Zone Transfer using nslookup command

1. Go to Windows command line (CMD) and enter Nslookup and press Enter.

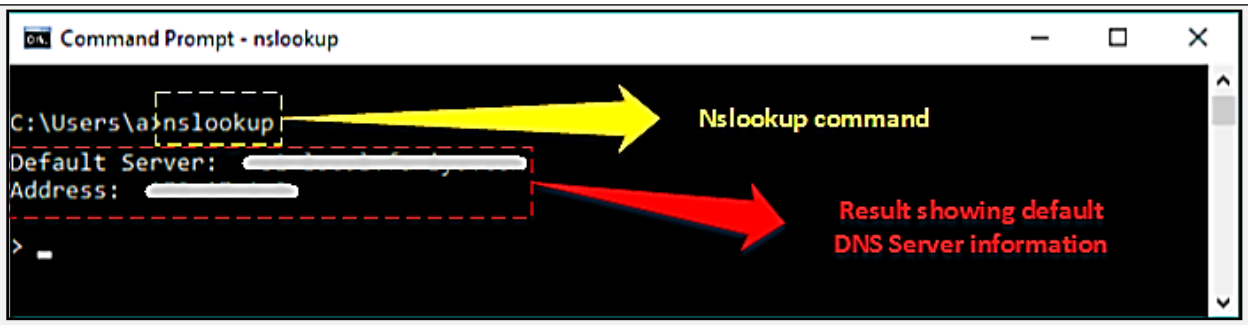


Figure 4-20 nslookup command

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

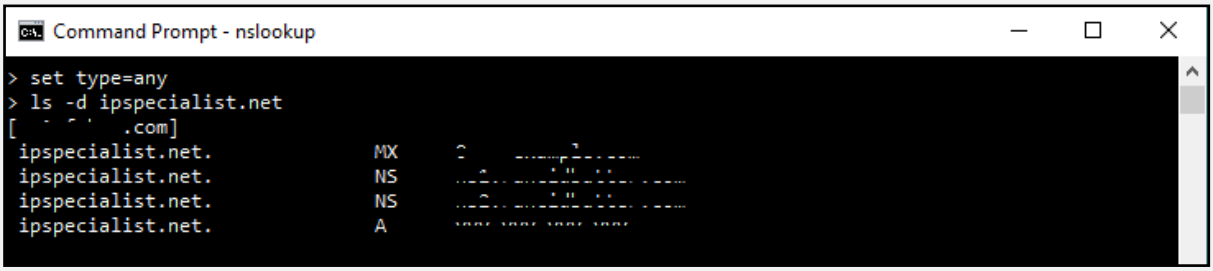


Figure 4-21 nslookup command

6. If not allowed, it will show the request failed.

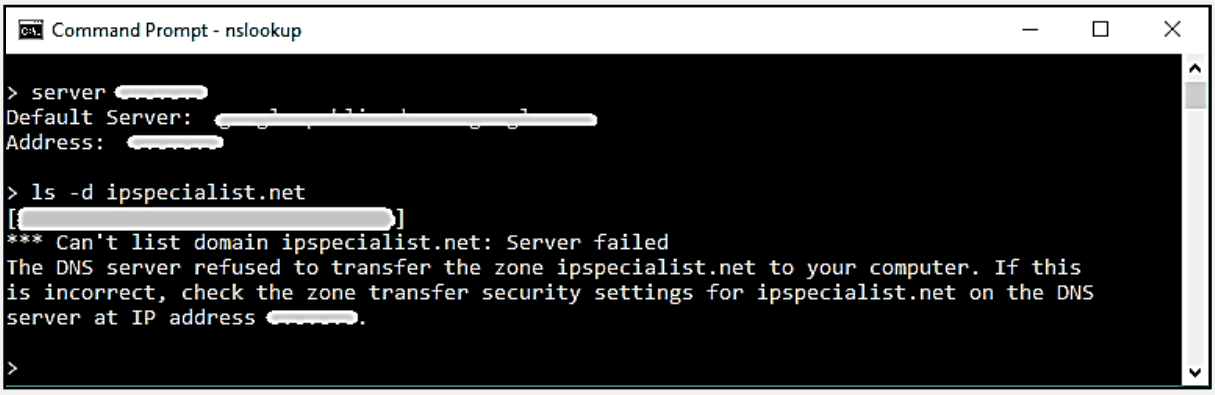


Figure 4-22 nslookup command

7. Linux support dig command, At a command prompt enter dig <domain.com> axfr.

Enumeration Countermeasures

Using advance security techniques, advanced security softwares, updated versions of protocols, strong security policies, unique, and difficult password, strong encrypted

communication between client and server, disabling unnecessary ports, protocols, sharing and default enabled services can prevent from enumeration at a certain level.

Mind Map