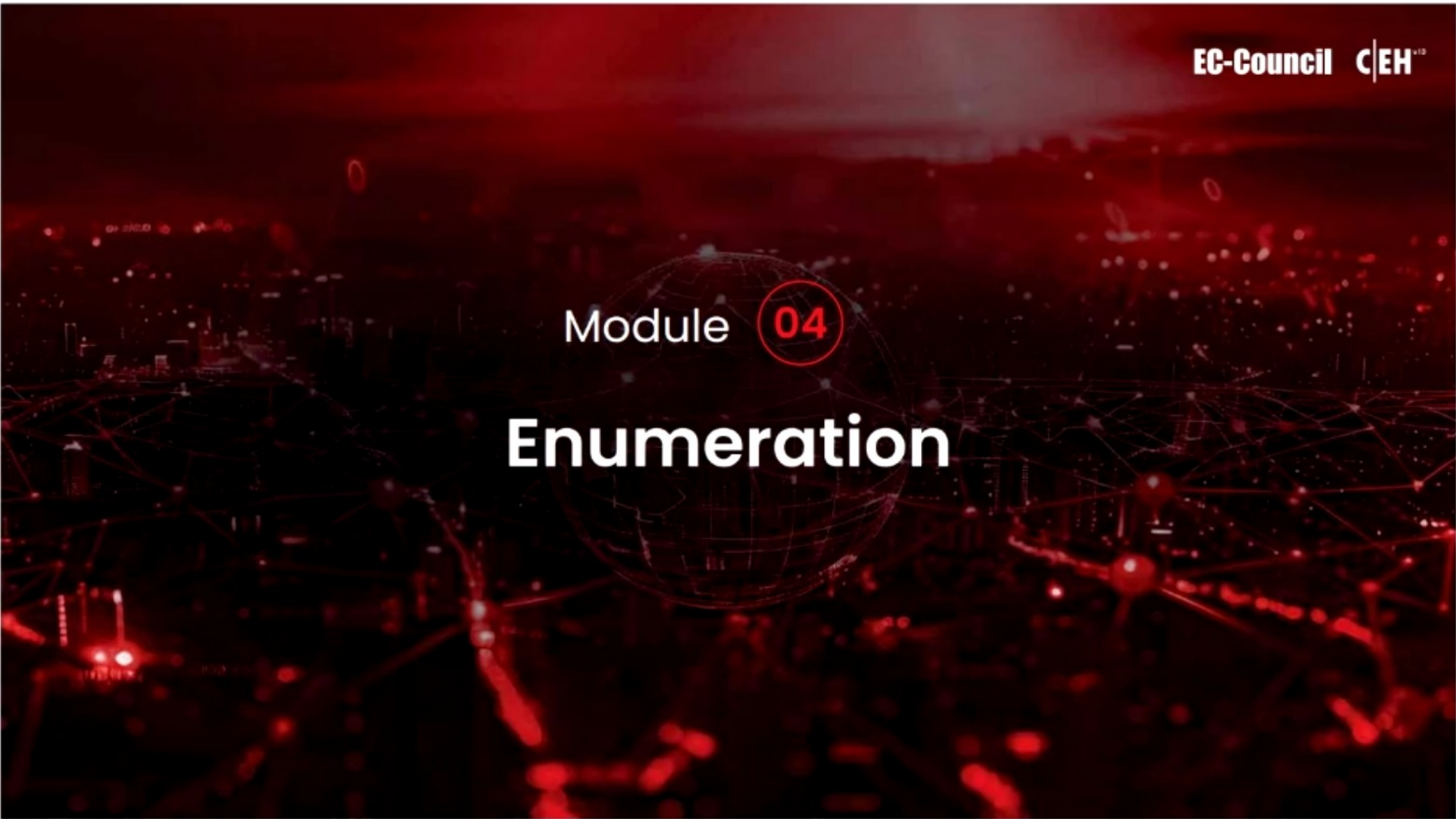

EC-Council C|EH
Module 04
Enumeration

Learning Objectives

01 Explain Enumeration Concepts

02 Demonstrate Different Techniques for NetBIOS Enumeration

03 Demonstrate Different Techniques for SNMP Enumeration and LDAP Enumeration

04 Use Different Techniques for NTP and NFS Enumeration

05 Demonstrate Different Techniques for SMTP and DNS Enumeration

06 Demonstrate IPsec, VoIP, RPC, Unix/Linux, and SMB Enumeration

07 Explain Enumeration Countermeasures

Objective 01

Explain Enumeration Concepts

What is Enumeration?

Enumeration involves an attacker **creating active connections with a target system** and **performing directed queries** to gain more information about the target

Attackers use the extracted information to **identify points for a system attack** and **perform password attacks** to gain unauthorized access to information system resources

Enumeration techniques are conducted in an **intranet environment**

Information Enumerated by Intruders

Network resources

Network shares

Routing tables

Audit and service settings

SNMP and FQDN details

Machine names

Users and groups

Applications and banners

Objective 02

Demonstrate Different Techniques for NetBIOS Enumeration

NetBIOS Enumeration

- A NetBIOS name is a unique 16 ASCII character string used to **identify the network devices** over TCP/IP; fifteen characters are used for the **device name**, and the sixteenth character is reserved for the **service or name record type**

Attackers use the NetBIOS enumeration to obtain

- **The list of computers that belong to a domain**
- **The list of shares on the individual hosts in the network**
- **Policies and passwords**

NetBIOS name list

Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for the computer
<username>	<03>	UNIQUE	Messenger service running for the logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, identifies the primary domain controller (PDC) for the domain

Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

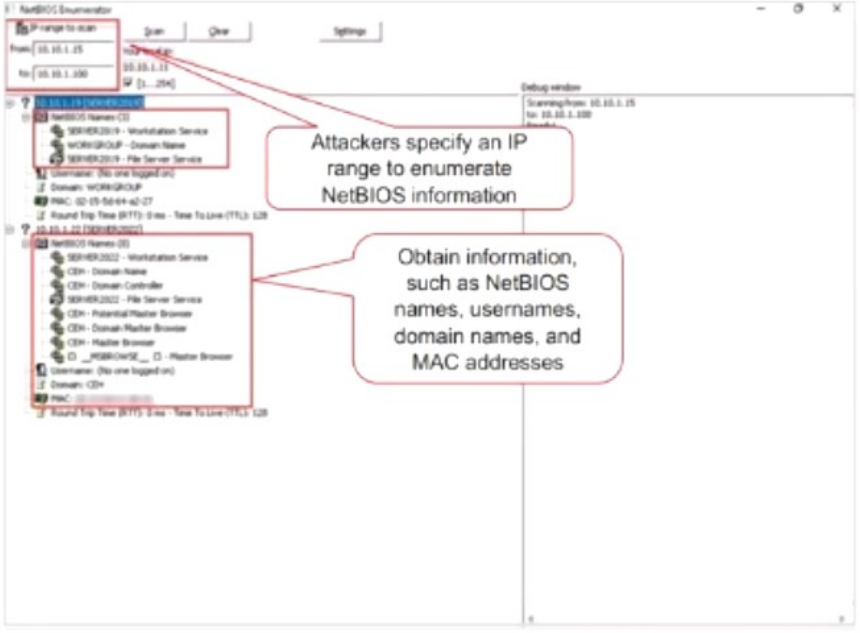
NetBIOS Enumeration (Cont'd)

Nbtstat Utility

Run the `nbtstat` command "**`nbtstat -a <IP address of the remote machine>`**" to obtain the NetBIOS name table of a remote computer

https://learn.microsoft.com

NetBIOS Enumerator



https://nbtenum.sourceforge.net

Other NetBIOS Enumeration Tools:

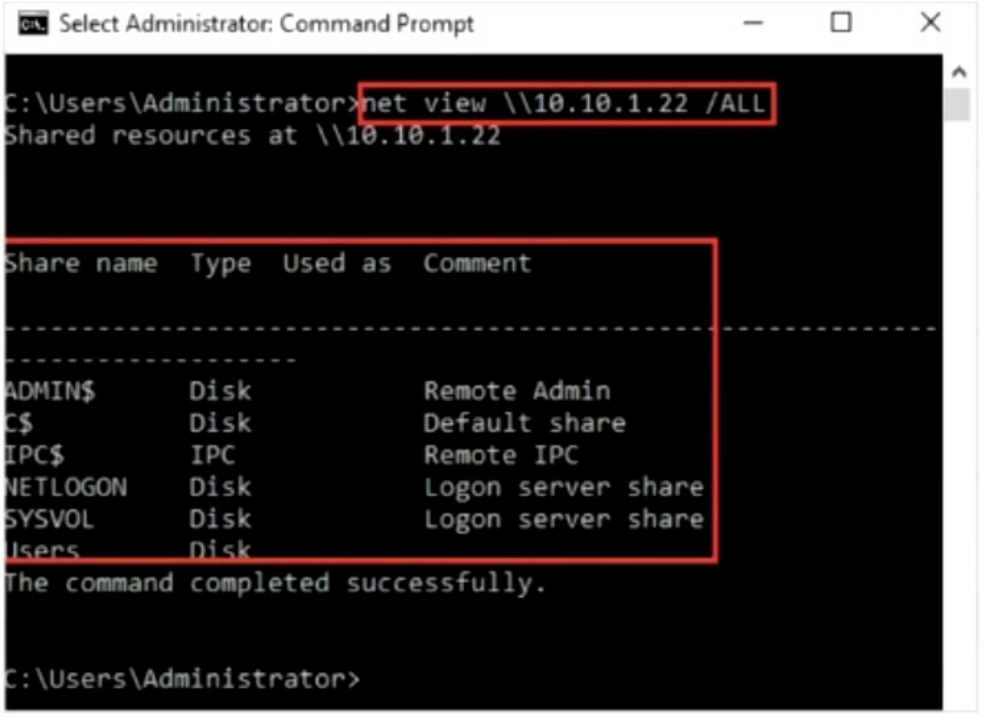
- **Nmap** — *https://nmap.org*
- **Global Network Inventory** — *https://magnetosoft.com*
- **Advanced IP Scanner** — *http://www.advanced-ip-scanner.com*
- **Hyena** — *https://www.systemtools.com*

Enumerating Shared Resources Using Net View

- The Net View utility is used to obtain a list of all the **shared resources of a remote host or workgroup**

Net View Commands

- **net view \\<computername>**
- **net view /domain:<domain name>**



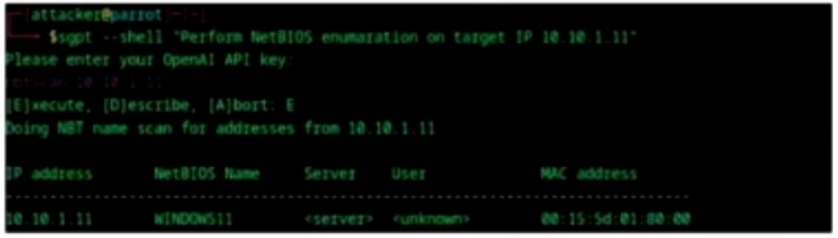
NetBIOS Enumeration using AI

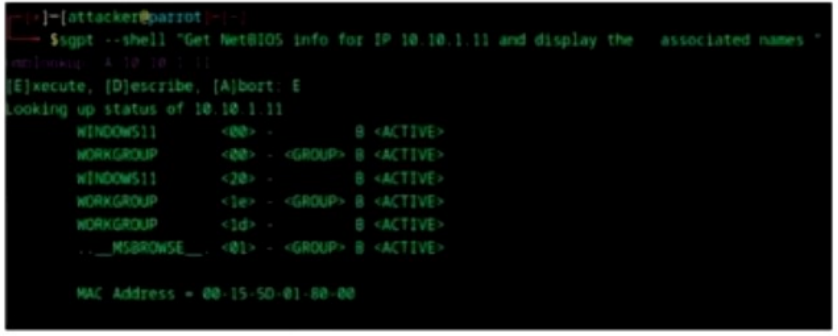
- Attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using appropriate prompt such as

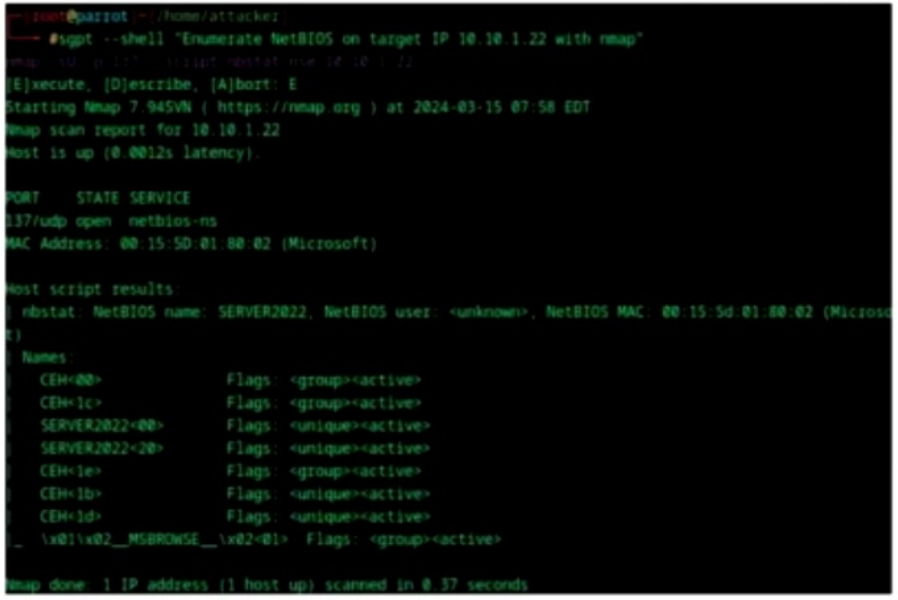
  "Perform NetBIOS enumeration on target IP 10.10.1.11"

  "Get NetBIOS info for IP 10.10.1.11 and display the associated names"

  "Enumerate NetBIOS on target IP 10.10.1.22 with nmap"







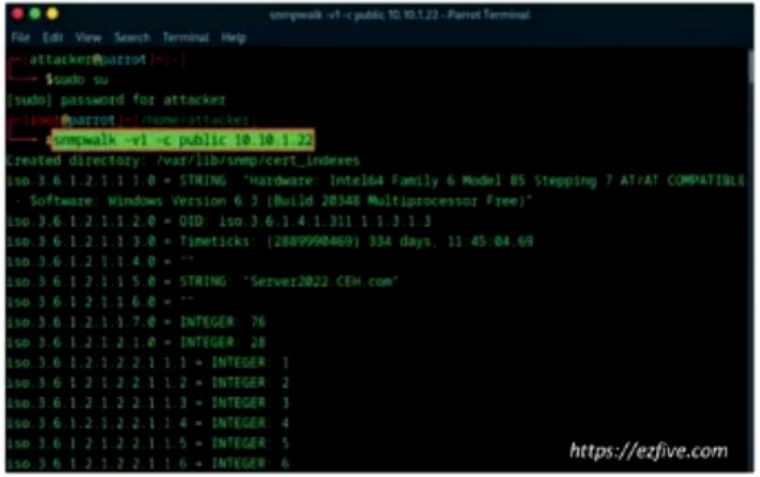
Objective 03

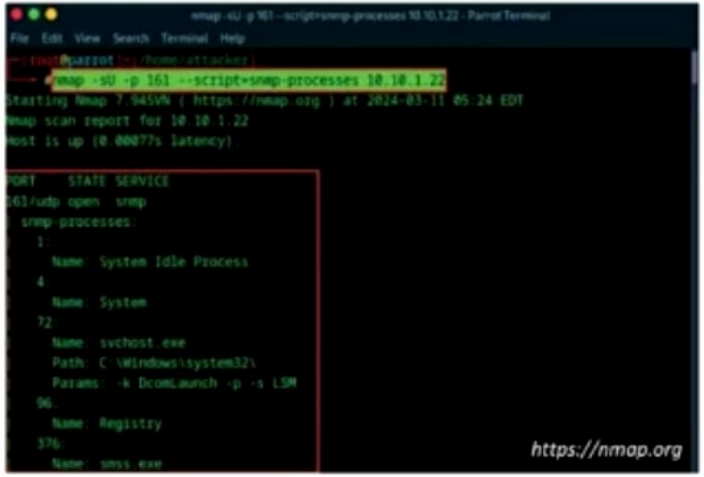
Demonstrate Different Techniques for SNMP Enumeration and LDAP Enumeration

SNMP (Simple Network Management Protocol) Enumeration

- Attackers use SNMP **default community strings** to extract information about a device
- Attackers enumerate SNMP to extract information about **network resources**, such as hosts, routers, devices, and shares, and **network information**, such as ARP tables, routing tables, and traffic

Enumerating SNMP using SnmpWalk and Nmap



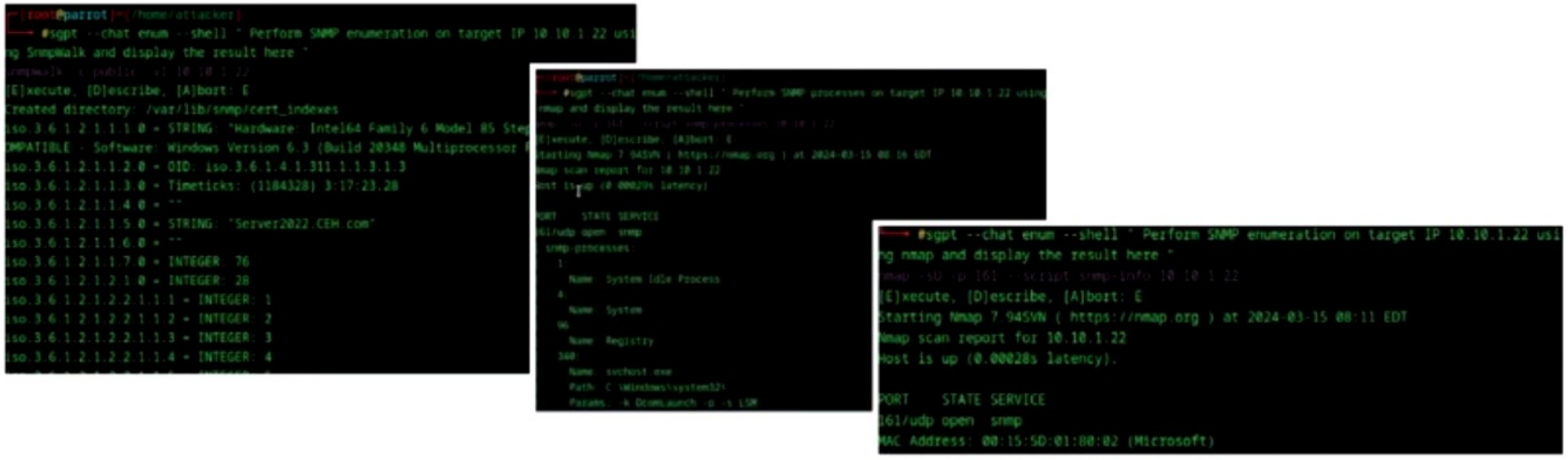


Other SNMP Enumeration Tools:

snmp-check	**SoftPerfect Network Scanner**	**Network Performance Monitor**	**OpUtils**
https://www.nothink.org	*https://www.softperfect.com*	*https://www.solarwinds.com*	*https://www.manageengine.com*

SNMP Enumeration with SnmpWalk and Nmap using AI

- Attacker can also leverage AI powered ChatGPT or other generative AI technology to perform this task by using appropriate prompt such as
- "Perform SNMP enumeration on target IP 10.10.1.22 using SnmpWalk and display the result here"
- "Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here"



LDAP Enumeration

Lightweight directory access protocol (LDAP) is an **Internet protocol** for accessing distributed directory services

A client starts a LDAP session by connecting to a **directory system agent** (DSA) on TCP port 389 and then sends an operation request to the DSA

Attackers query the LDAP service to gather information, such as **valid usernames**, **addresses**, and **departmental details**, which can be further used to perform attacks

Other LDAP Enumeration Tools:

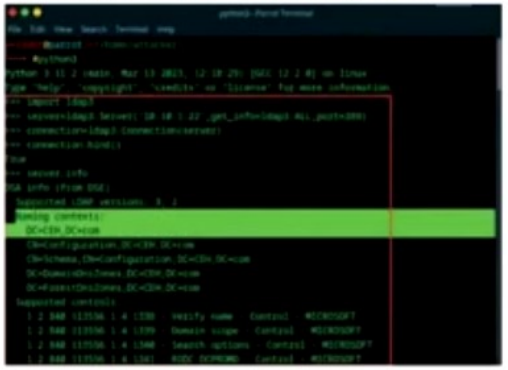
Softerra LDAP Administrator
https://www.ldapadministrator.com

ldapsearch
https://linux.die.net

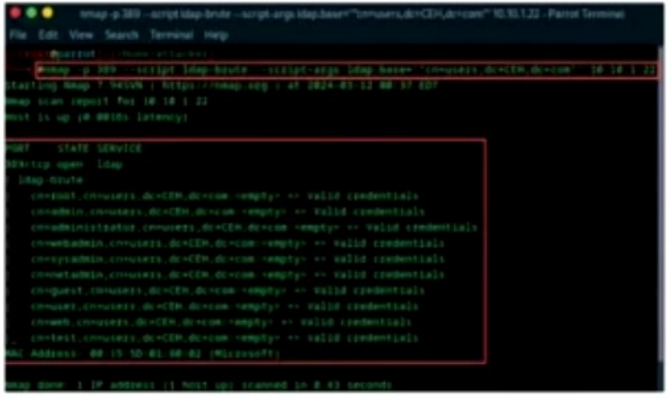
AD Explorer
https://docs.microsoft.com

LDAP Admin Tool
https://www.ldapsoft.com

Manual LDAP Enumeration



Automated LDAP Enumeration



Objective 04

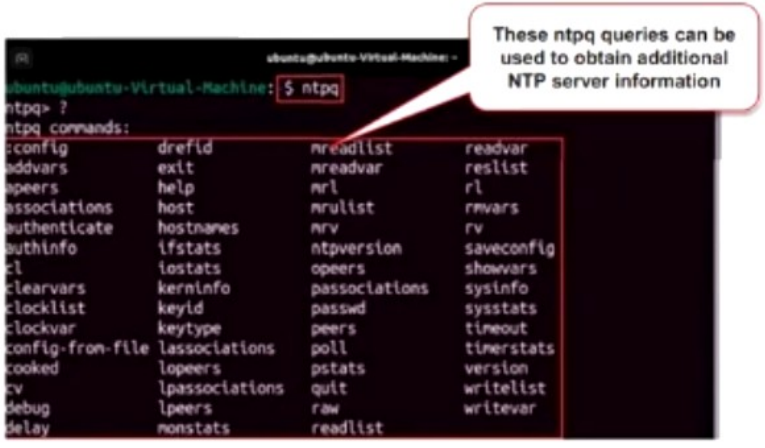
Use Different Techniques for NTP and NFS Enumeration

NTP Enumeration and NTP Enumeration Commands

Attackers query the NTP server to gather valuable information, such as list of **connected hosts** and **Clients' IP addresses** in a network, their system names, and OSs

- **ntptrace**
  - Traces a chain of NTP servers back to the primary source
  - **ntptrace [-n] [-m maxhosts] [servername/IP_address]**
- **ntpdc**
  - Monitors operation of the NTP daemon, ntpd
  - **ntpdc [-ilnps] [-c command] [host] [...]**

- **ntpq**
  - Monitors NTP daemon (ntpd) operations and determines performance
  - **ntpq [-inp] [-c *command*] [*host*] [...]**



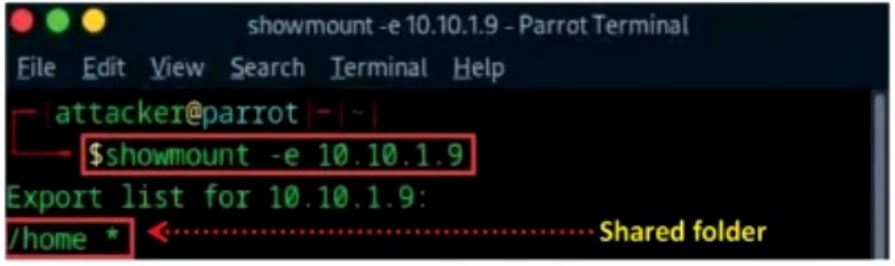
NFS Enumeration

The NFS system is generally implemented on the computer network, where the **centralization of data** is required for critical resources

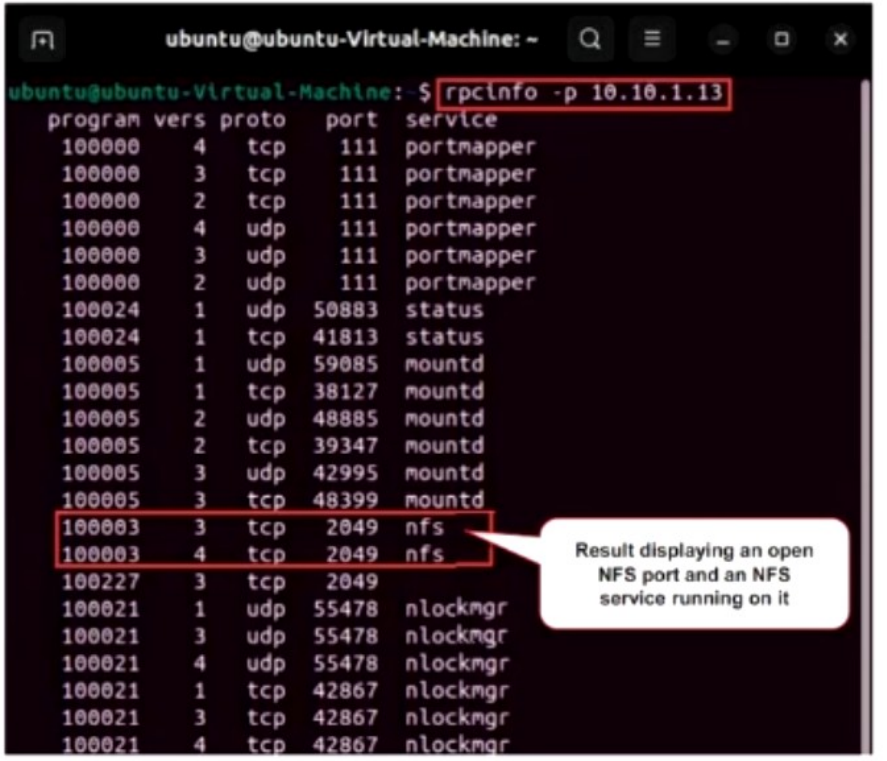
NFS enumeration enables attackers to identify the **exported directories**, **list of clients** connected to the NFS server along with their **IP addresses**, and the **shared data** associated with the IP addresses

Attackers use tools such as **RPSCan** and **SuperEnum** to perform NFS enumeration

showmount command



rpcinfo command



Objective 05

Demonstrate Different Techniques for SMTP and DNS Enumeration

SMTP Enumeration

- SMTP provides 3 built-in-commands:
  - **VRFY** - Validates users
  - **EXPN** - Shows the actual delivery addresses of aliases and mailing lists
  - **RCPT TO** - Defines the recipients of a message
- SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users, based on which we can **determine valid users on the SMTP server**
- Attackers can directly interact with SMTP via the telnet prompt and collect a **list of valid users** on the SMTP server

Using the SMTP VRFY Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
VRFY Jonathan
250 Super-User
<Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

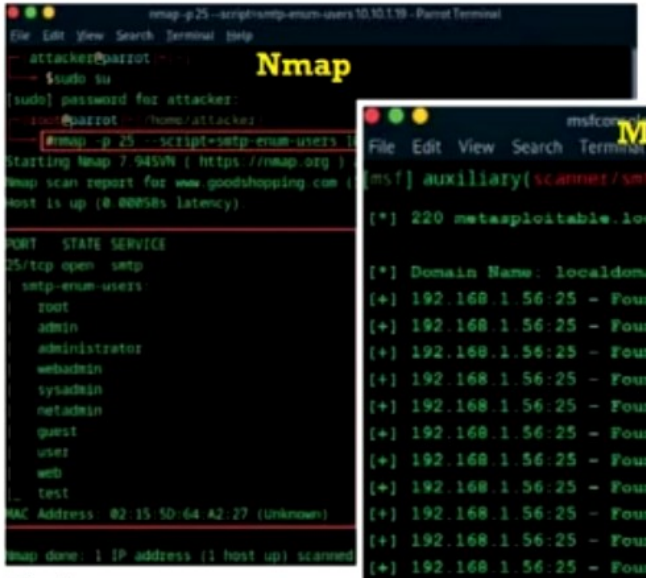
Using the SMTP EXPN Command

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
EXPN Jonathan
250 Super-User
<Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

Using the SMTP RCPT TO Command

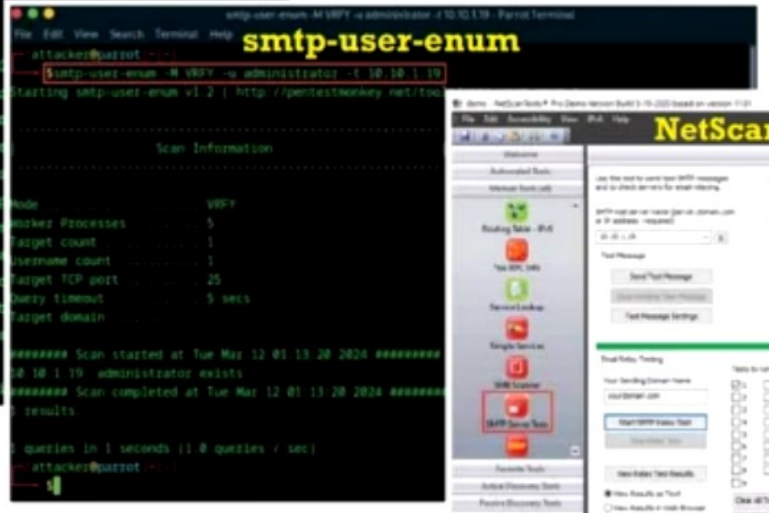
```
$ telnetl 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86],
pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

SMTP Enumeration (Cont'd)

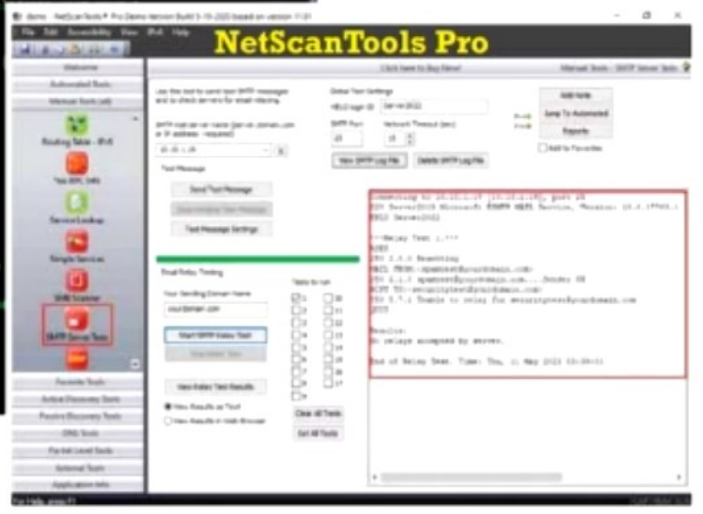


https://nmap.org

https://www.metasploit.com



https://pentestmonkey.net

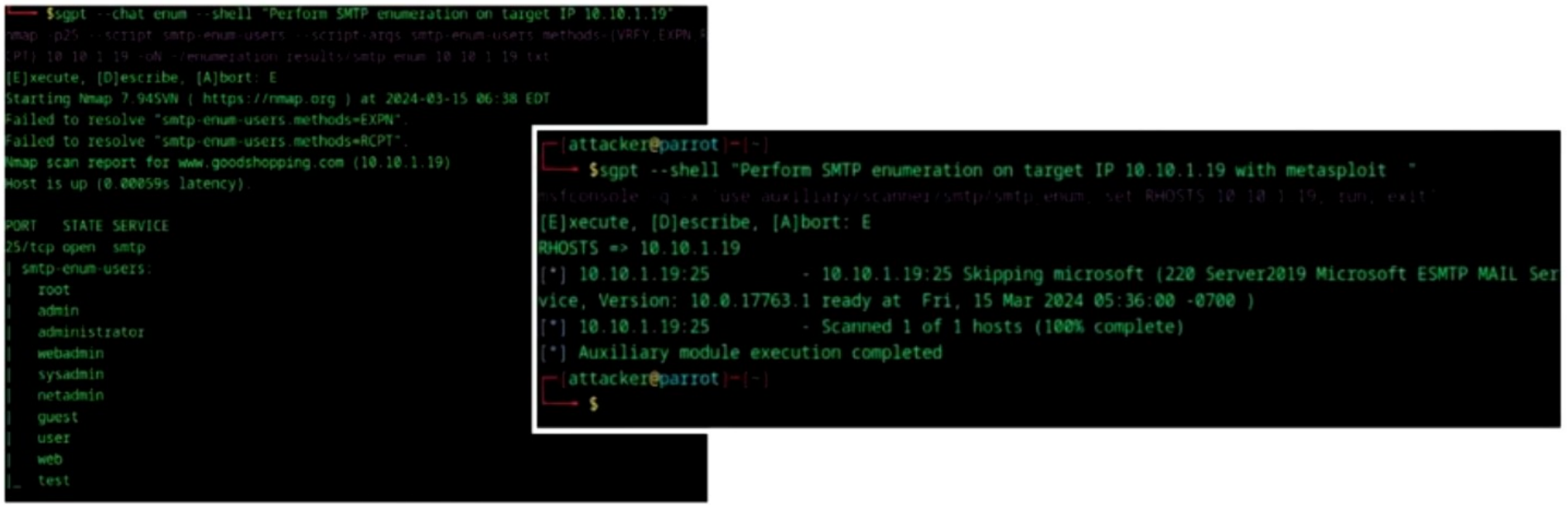


https://www.netscantools.com

SMTP Enumeration using AI

An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using appropriate prompt such as

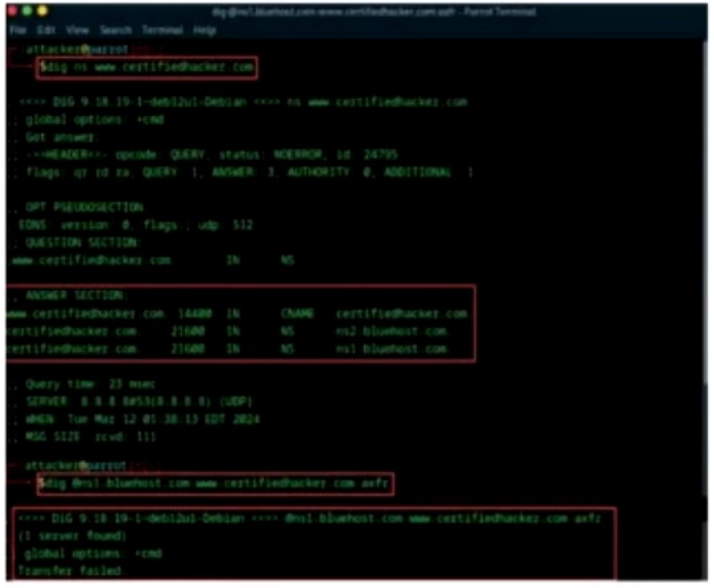
- *"Perform SMTP enumeration on target IP 10.10.1.19."*
- *"Perform SMTP enumeration on target IP 10.10.1.19 with metasploit"*



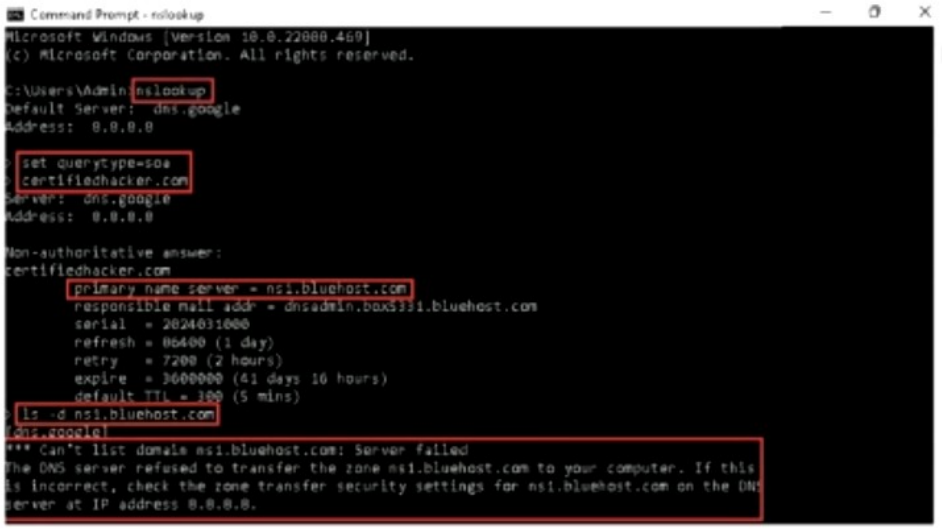
DNS Enumeration using Zone Transfer

- If the target DNS server allows zone transfers, then attackers use this technique to obtain **DNS server names**, **hostnames**, **machine names**, **usernames**, **IP addresses**, **aliases**, etc. assigned within a target domain
- Attackers perform DNS zone transfer using tools, such as **nslookup**, **dig**, and **DNSRecon**; if DNS transfer setting is enabled on the target name server, it will provide DNS information, or else it will return an error saying it has failed or refuses the zone transfer

Linux DNS zone transfer using dig command



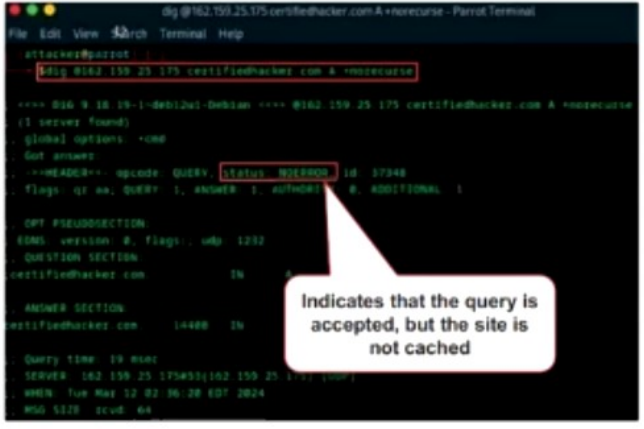
Windows DNS zone transfer using nslookup command

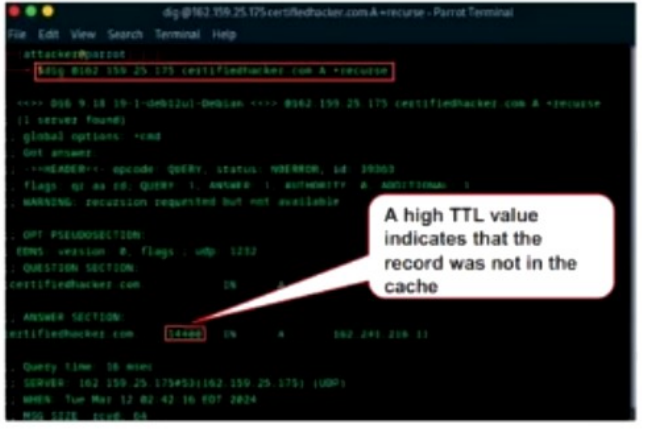


DNS Cache Snooping

- DNS cache snooping is a **DNS enumeration** technique whereby an **attacker queries** the **DNS server** for a specific cached DNS record

Non-recursive Method	Attackers send a **non-recursive query** by setting the **Recursion Desired** (RD) bit in the query header to zero
Recursive Method	Attackers send a recursive query to **determine the time** the **DNS record** resides in the cache

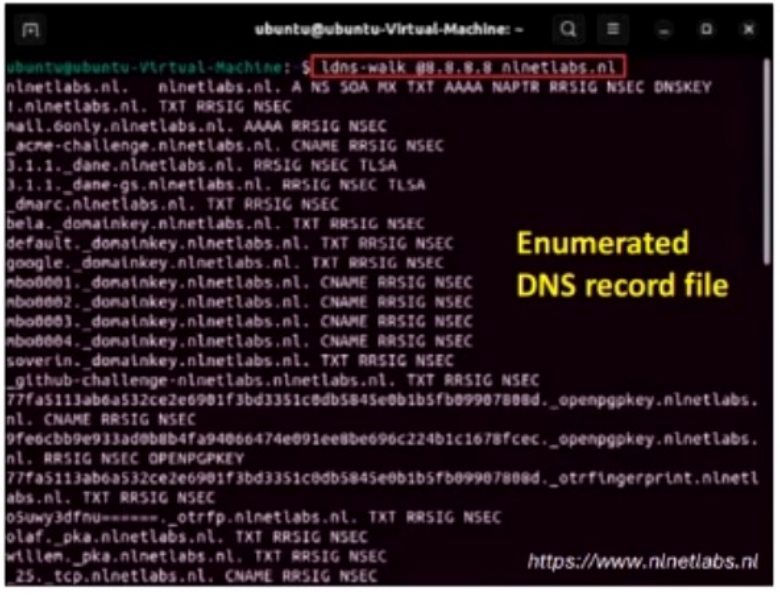




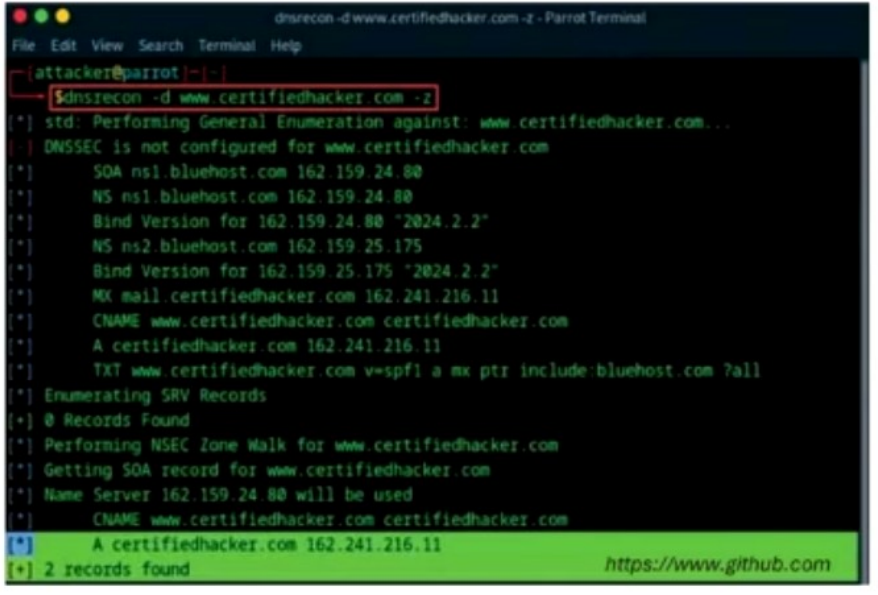
DNSSEC Zone Walking

- DNSSEC zone walking is a DNS enumeration technique where an attacker attempts to **obtain internal records of the DNS server** if the DNS zone is not properly configured
- Attackers use tools, such as **LDNS** and **DNSRecon**, to exploit this vulnerability and **obtain the network information** of a target domain and further launch Internet-based attacks

LDNS

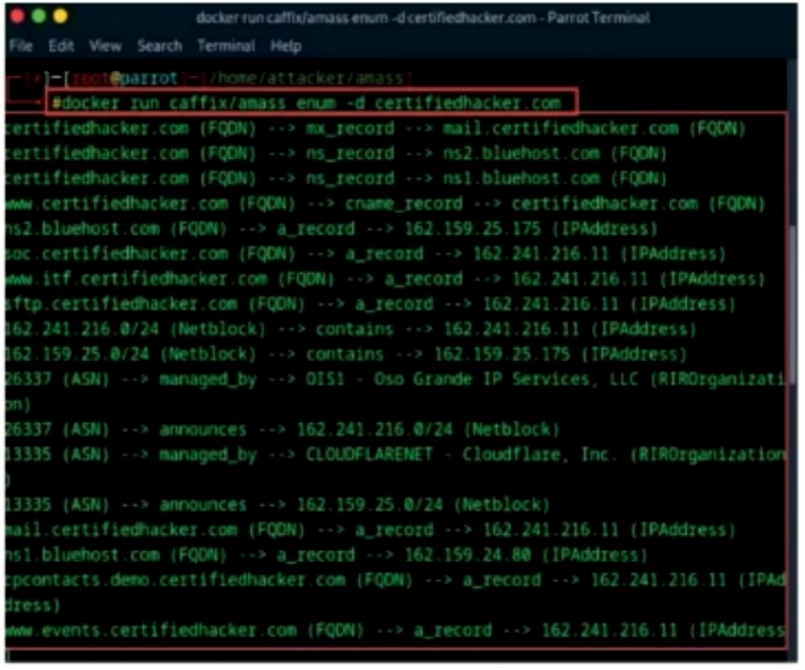


DNSRecon



DNS Enumeration Using OWASP Amass

OWASP Amass is a DNS enumeration tool that allows attackers to **map the target network** and **discover potential attack surfaces**



OWASP Amass commands for DNS Enumeration

- Command to perform a passive enumeration:

  ```
  amass enum -passive -d <Target Domain> -src
  ```

- Command to perform an active enumeration through brute-forcing :

  ```
  amass enum -active -d <Target Domain> -brute -w
  /usr/share/wordlists/amass/all.txt
  ```

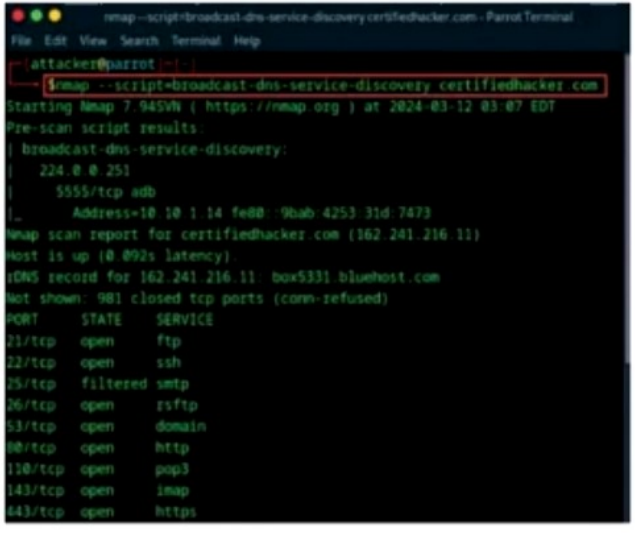
- Command to track or compare the last two enumeration scans :

  ```
  amass track -config /root/amass/config.ini -dir
  amass4owasp -d <Target Domain> -last 2
  ```

DNS and DNSSEC Enumeration Using Nmap

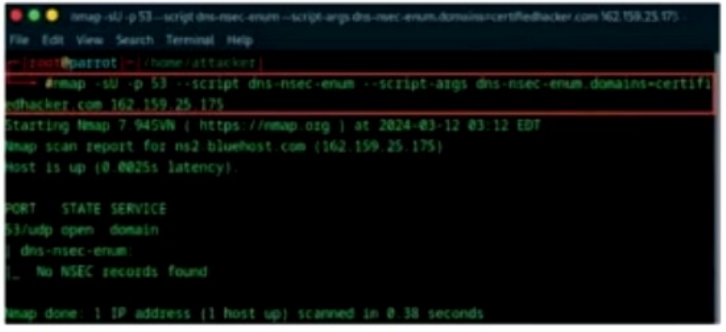
DNS Enumeration

Attackers use Nmap for scanning domains and obtaining a **list of subdomains**, **records**, **IP addresses**, and other valuable information from the target host



DNSSEC Enumeration

Attackers enumerate DNSSEC using Nmap **dns-nsec-enum.nse** or **dns-nsec3-enum.nse** scripts to obtain information related to domains and their sub-domains



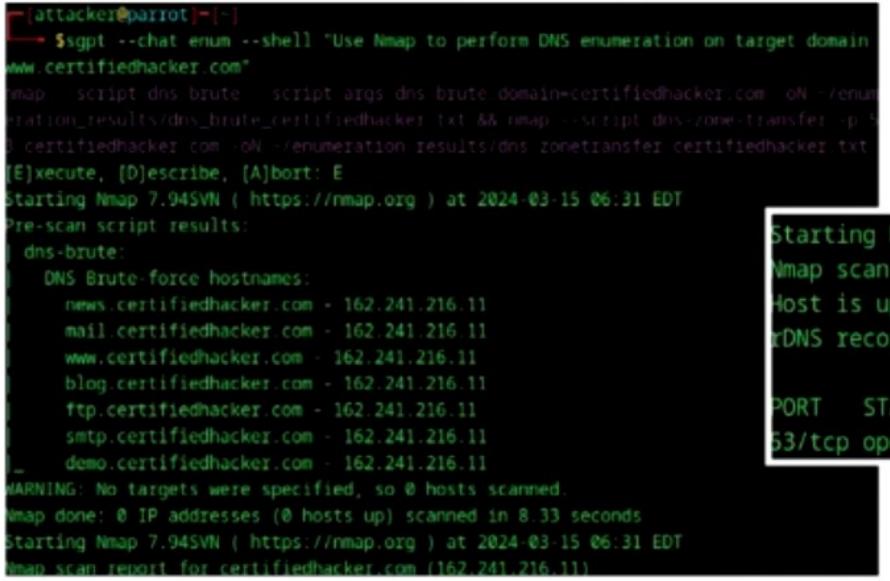
DNS Enumeration Tools

- **Knock** — *https://github.com*
- **Subfinder** — *https://github.com*
- **Raccoon** — *https://github.com*
- **Turbolist3r** — *https://github.com*

DNS Enumeration with Nmap Using AI

An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as

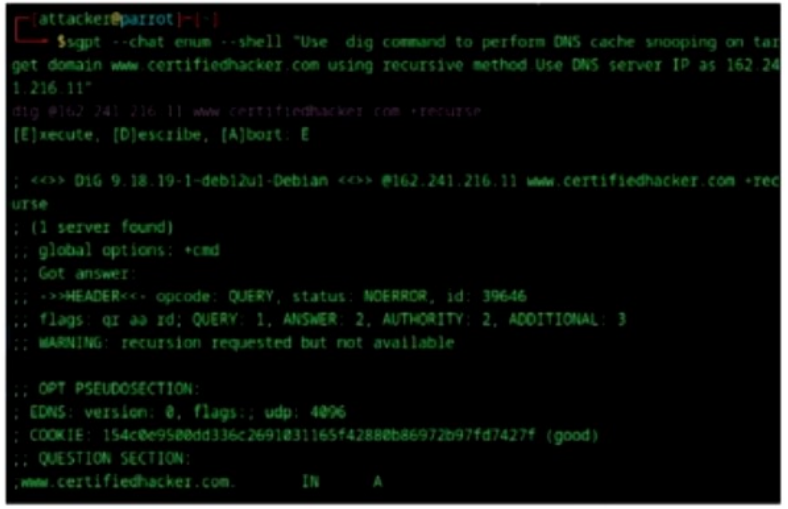
- *"Use Nmap to perform DNS Enumeration on target domain www.certifiedhacker.com"*

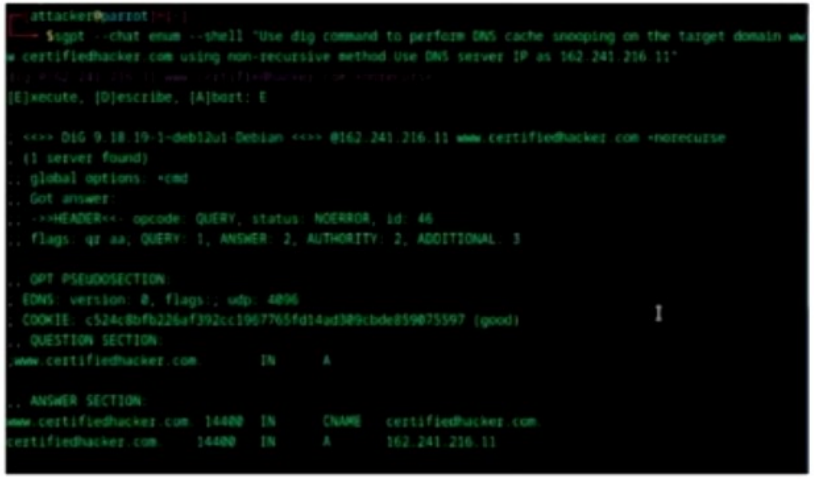


DNS Cache Snooping using AI

An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as

- *"Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method. Use DNS server IP as <DNS server IP>"*
- *"Use dig command to perform DNS cache snooping on the target domain www.certifiedhacker.com using non-recursive method. Use DNS server IP as <DNS server IP>"*





Objective 06

Demonstrate IPsec, VoIP, RPC, Unix/Linux, and SMB Enumeration

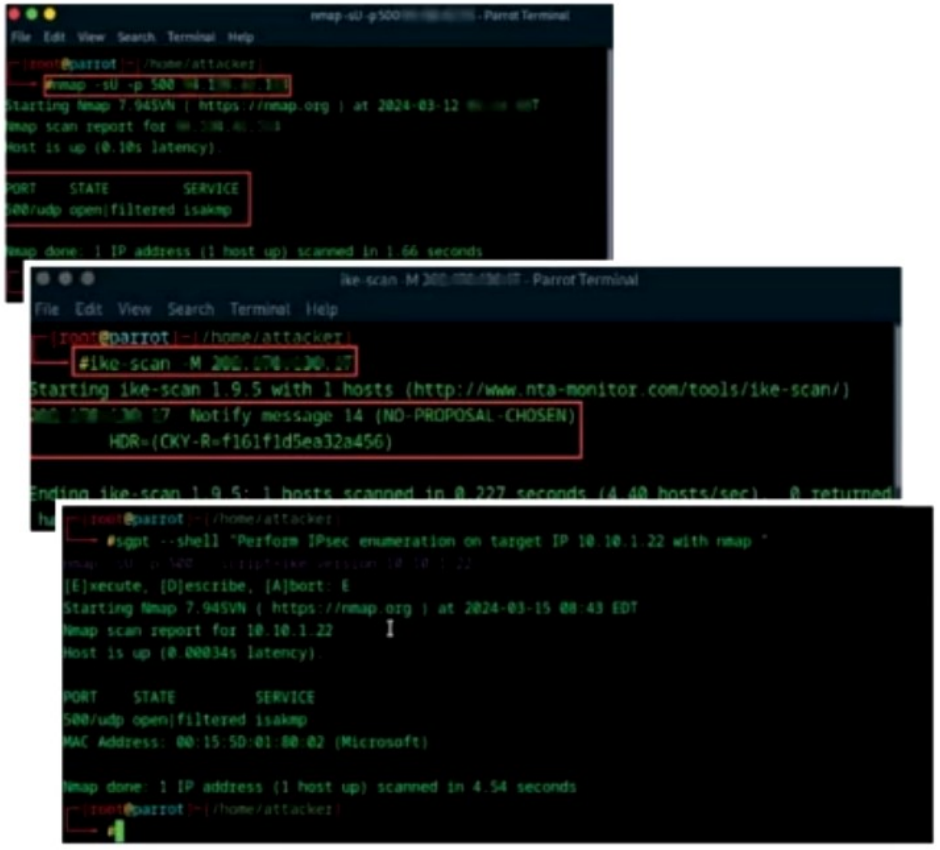
IPsec Enumeration

Most IPsec based **VPNs use ISAKMP**, a part of IKE, to establish, negotiate, modify, and delete Security Associations (SA) and cryptographic keys in a VPN environment

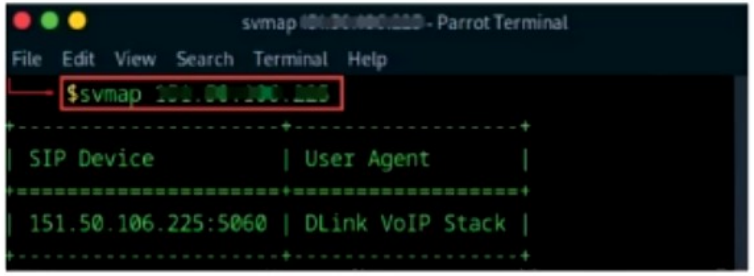
A simple **scanning for ISAKMP at UDP port 500** can indicate the presence of a VPN gateway

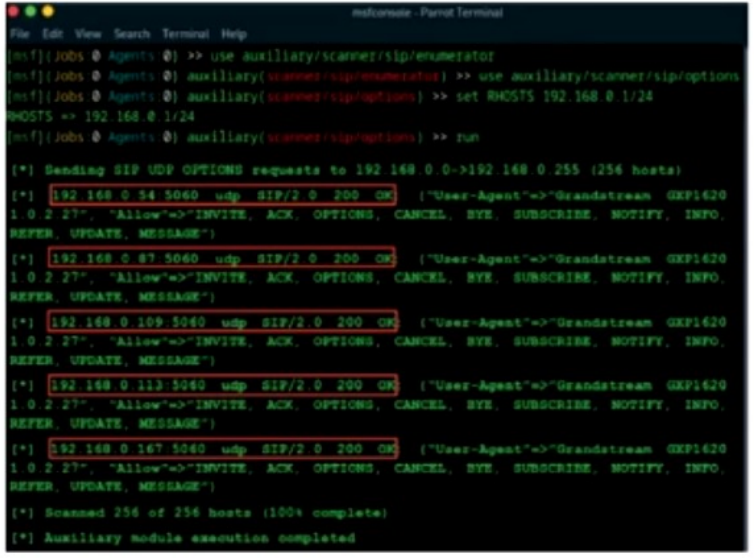
Attackers can probe further using a tool, such as **ike-scan**, to enumerate sensitive information, including encryption and hashing algorithm, authentication type, key distribution algorithm, and SA LifeDuration

An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as "***Perform IPsec enumeration on target IP 10.10.1.22 with nmap***"



VoIP Enumeration





VoIP uses **Session Initiation Protocol (SIP)** protocol to enable voice and video calls over an IP network

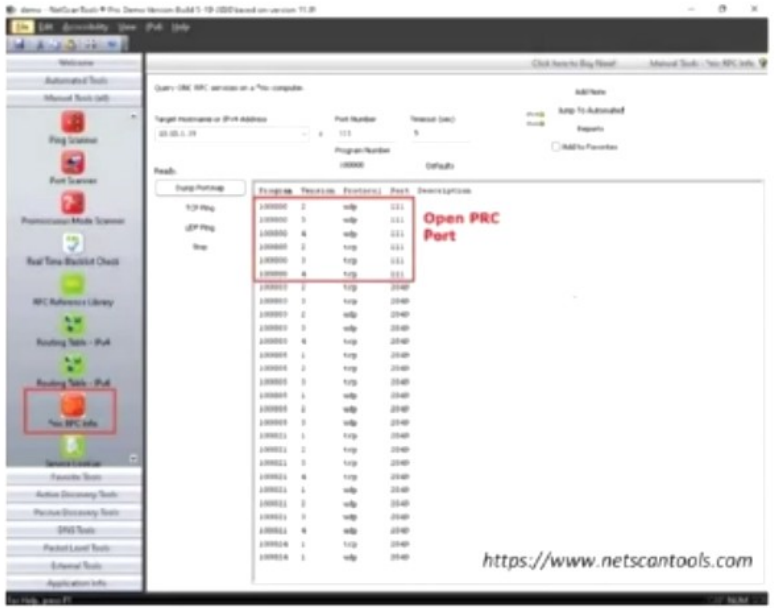
SIP service generally uses UDP/TCP ports 2000, 2001, 5060, and 5061

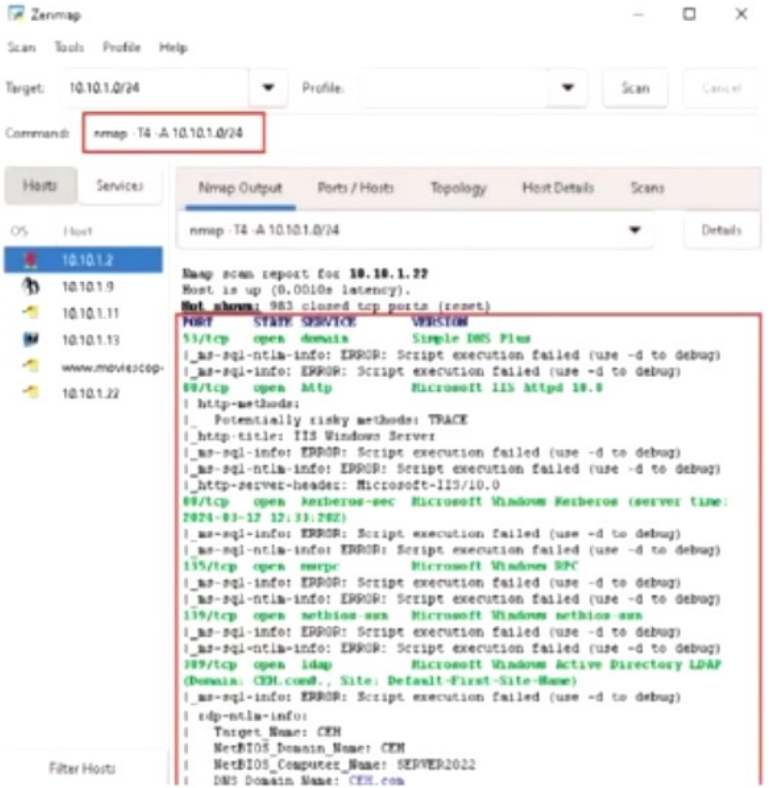
VoIP enumeration provides sensitive information, such as VoIP gateway/servers, IP-PBX systems, client software (softphones)/VoIP phones, User-agent IP addresses, and user extensions

This information can be used to launch various VoIP attacks, such as Denial-of-Service (DoS), Session Hijacking, Caller ID spoofing, Eavesdropping, Spamming over Internet Telephony (SPIT), and VoIP phishing (Vishing)

RPC Enumeration

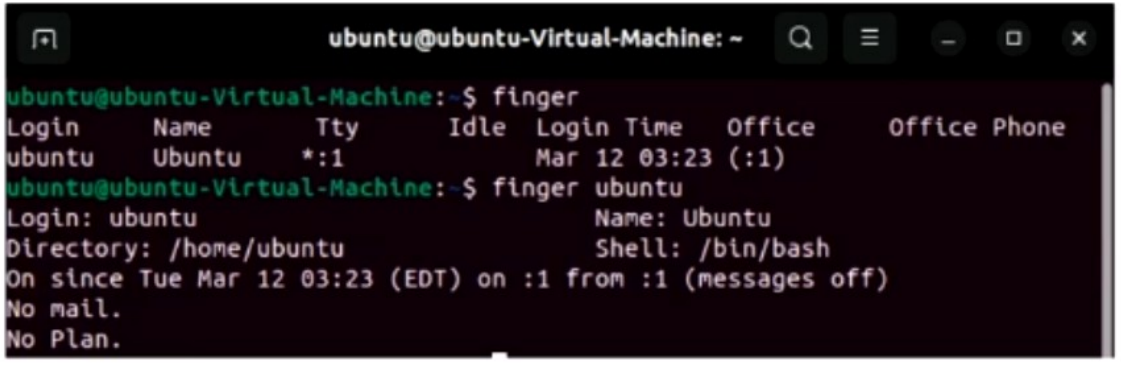
- Remote Procedure Call (RPC) allows clients and servers to communicate in **distributed client/server programs**
- Enumerating RPC endpoints enables attackers to **identify any vulnerable services** on these service ports





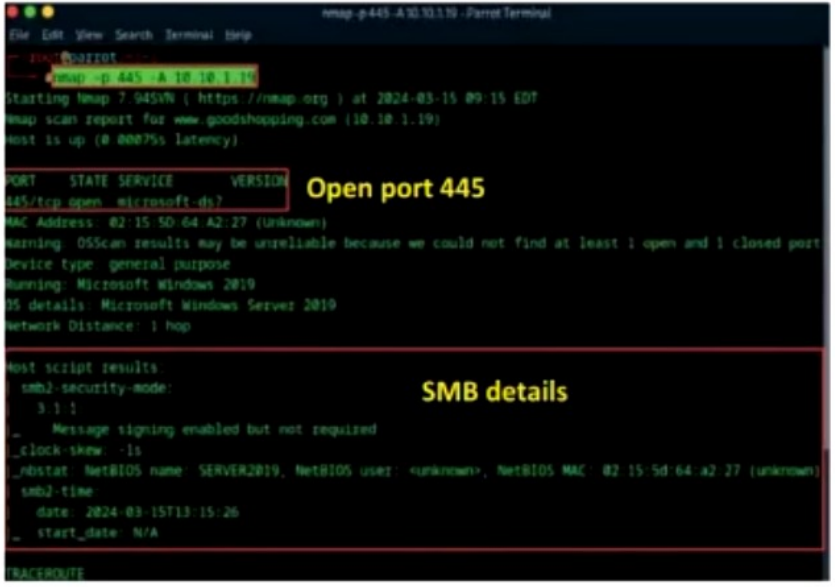
Unix/Linux User Enumeration

rusers	Displays a list of users who are logged on to remote machines or machines on local network **Syntax:** `/usr/bin/rusers [-a] [-l] [-u| -h| -i] [Host ...]`
rwho	Displays a list of users who are logged on to hosts on the local network **Syntax:** `rwho [ -a]`
finger	Displays information about system users, such as login name, real name, terminal name, idle time, login time, office location, and office phone numbers **Syntax:** `finger [-l] [-m] [-p] [-s] [user ...] [user@host ... ]`



SMB Enumeration

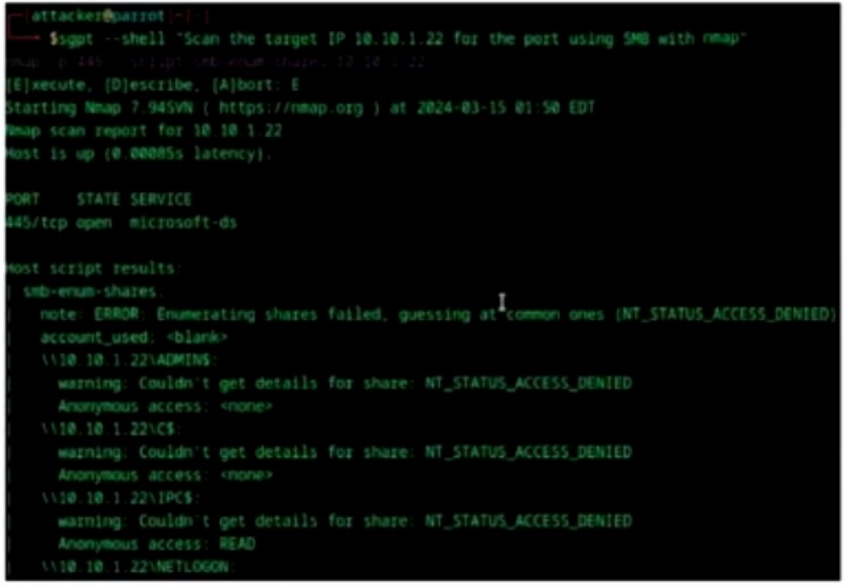
- Attackers use SMB enumeration tools, such as **Nmap**, **SMBMap**, **enum4linux**, and **nullinux**, to perform a directed scan on the SMB service running on port 445
- SMB enumeration helps attackers to perform **OS banner grabbing** on the target



SMB Enumeration with AI

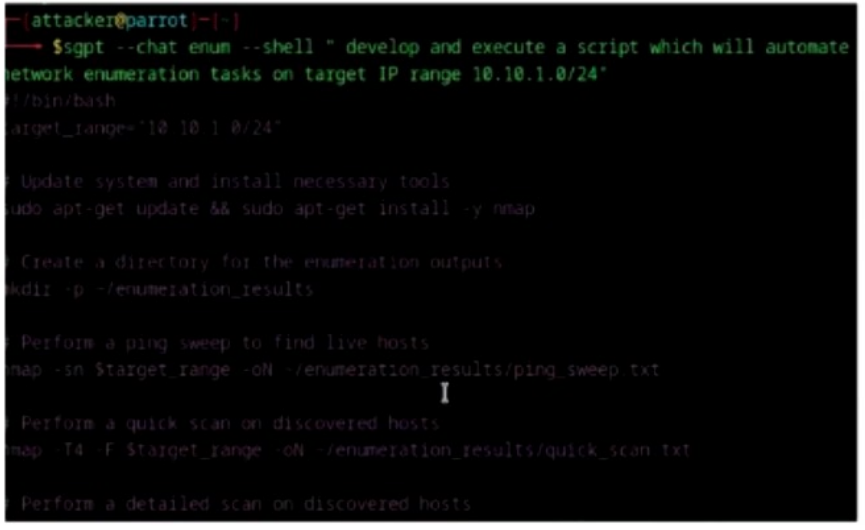
- An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as

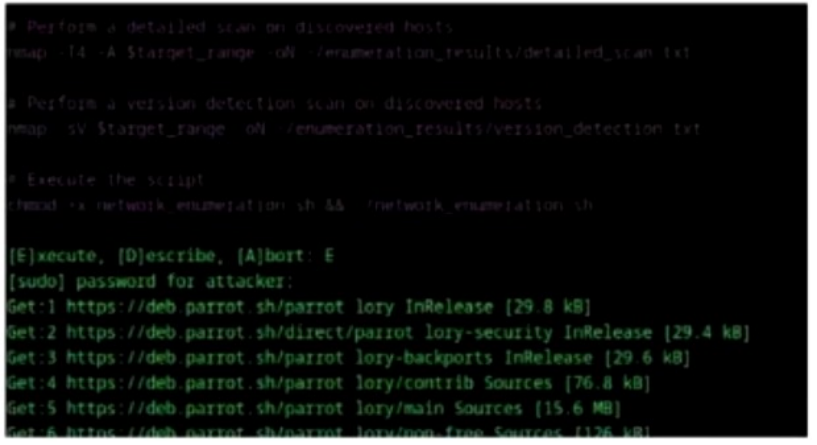
  "Scan the target IP 10.10.1.22 for the port using SMB with nmap"



Create and Run Custom Script to Automate Network Enumeration Tasks with AI

- An attacker can also leverage AI-powered ChatGPT or other generative AI technology to automate various network enumeration tasks by create custom script that will run automatically and fetch the desired result. They can use appropriate prompts to create custom scripts, such as the one below:
  - *"Develop and execute a script which will automate network enumeration tasks on target IP range 10.10.1.0/24"*





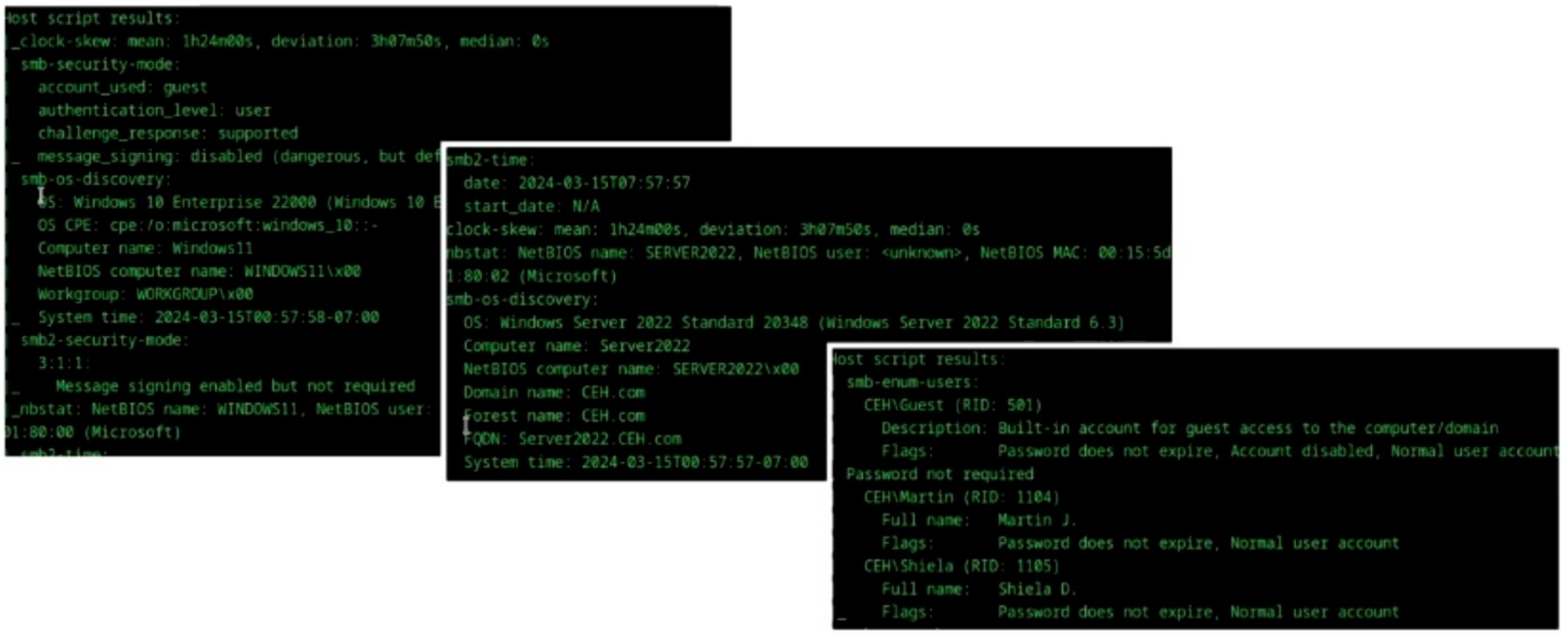
Create and Run Custom Script to Automate Network Enumeration Tasks with AI (Cont'd)

```
_Not valid after:  2024-09-13T08:50:47
 rdp-ntlm-info:
   Target_Name: WINDOWS11
   NetBIOS_Domain_Name: WINDOWS11
   NetBIOS_Computer_Name: WINDOWS11
   DNS_Domain_Name: Windows11
   DNS_Computer_Name: Windows11
   Product_Version: 10.0.22000
_  System_Time: 2024-03-15T07:57:56+00:00
_ssl-date: 2024-03-15T07:58:38+00:00; 0s from scanner time.
ervice Info: Host: WINDOWS11; OS: Windows; CPE: cpe:/o:microsoft:windows

ost script results:
_clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s
 smb-security-mode:
   account_used: guest
   authentication_level: user
   challenge_response: supported
_  message_signing: disabled (dangerous, but default)
 smb-os-discovery:
   OS: Windows 10 Enterprise 22000 (Windows 10 Enterprise 6.3)
   OS CPE: cpe:/o:microsoft:windows_10::-
```

```
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-03-15T07:58:38+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Server2019
| Not valid before: 2024-03-14T07:50:45
|_Not valid after:  2024-09-13T07:50:45
| rdp-ntlm-info:
|   Target_Name: SERVER2019
|   NetBIOS_Domain_Name: SERVER2019
|   NetBIOS_Computer_Name: SERVER2019
|   DNS_Domain_Name: Server2019
|   DNS_Computer_Name: Server2019
|   Product_Version: 10.0.17763
|_  System_Time: 2024-03-15T07:57:56+00:00
```

Create and Run Custom Script to Automate Network Enumeration Tasks with AI (Cont'd)



Objective 07

Explain Enumeration Countermeasures

Enumeration Countermeasures

SNMP

- **Remove the SNMP agent** or turn off the SNMP service
- If turning off SNMP is not an option, then change the default **community string names**
- **Upgrade to SNMP3**, which encrypts passwords and messages
- Implement the Group Policy security option called "**Additional restrictions for anonymous connections**"

LDAP

- By default, LDAP traffic is transmitted unsecured; **use SSL or STARTTLS technology** to encrypt the traffic
- Select a **username different** from your email address and enable **account lockout**
- Use **NT LAN Manager (NTLM)**, **Kerberos**, or any basic authentication mechanism to limit access to legitimate users

NFS

- Implement **proper permissions** (read/write must be restricted to specific users) on exported file systems
- Implement **firewall rules** to block NFS port 2049
- Ensure **proper configuration** of files, such as **/etc/smb.conf**, **/etc/exports** and **etc/hosts.allow**, to protect the data stored in servers
- **Log the requests** to access the system files on the NFS server

Enumeration Countermeasures (Cont'd)

SMTP

Configure SMTP servers to

- Exclude sensitive **mail server** and **local host information** in mail responses
- Disable **open relay** feature
- **Limit the number of accepted connections** from a source to prevent brute-force attacks
- Provide **limited information** in error messages

SMB

- Disable SMB protocol on **Web and DNS Servers**
- Disable SMB protocol on **Internet facing servers**
- Disable ports **TCP 139** and **TCP 445** used by the SMB protocol
- Restrict anonymous access through **RestrictNullSessAccess** parameter from the **Windows Registry**

DNS

- Ensure that the resolver can be accessed only by the hosts **inside the network**
- Ensure that the request packets exiting the network use **random ports**
- Audit **DNS zones** to identify vulnerabilities in domains and subdomains
- Update and **patch nameservers** with the most recent versions of software

Module Summary

- In this module, we have discussed the following:
  - Enumeration concepts along with techniques, services, and ports used for enumeration
  - How attackers perform enumeration using different techniques (NetBIOS, SNMP, LDAP, AD, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Linux/Unix, and SMB enumeration) to gather more information about a target
  - How organizations can defend against enumeration activities
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen testers, perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems