Module 04

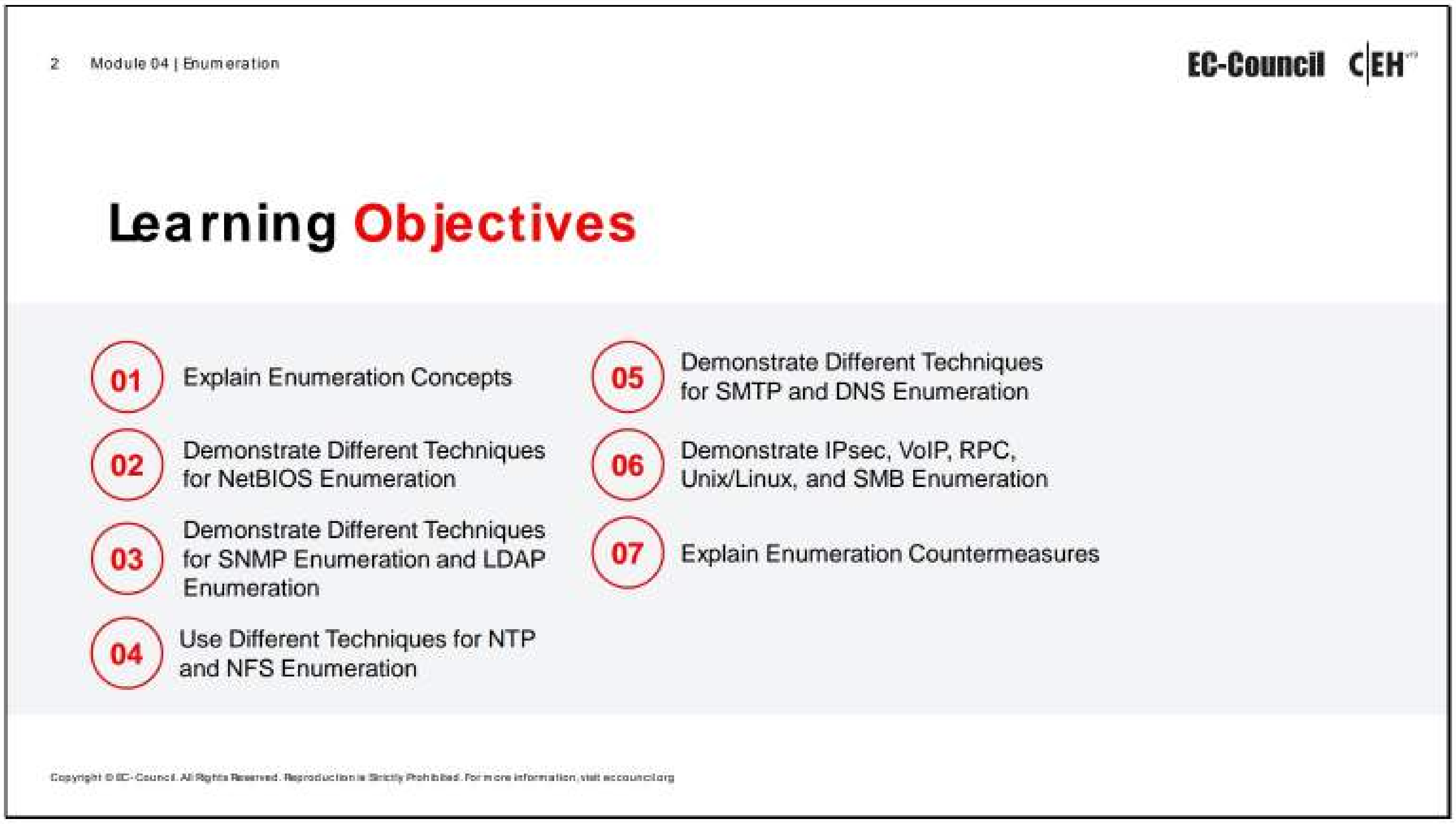
Enumeration

EC-Council
Official Curricula

EC-Council C|EH v13

Certified Ethical Hacker

This page is intentionally left blank.



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

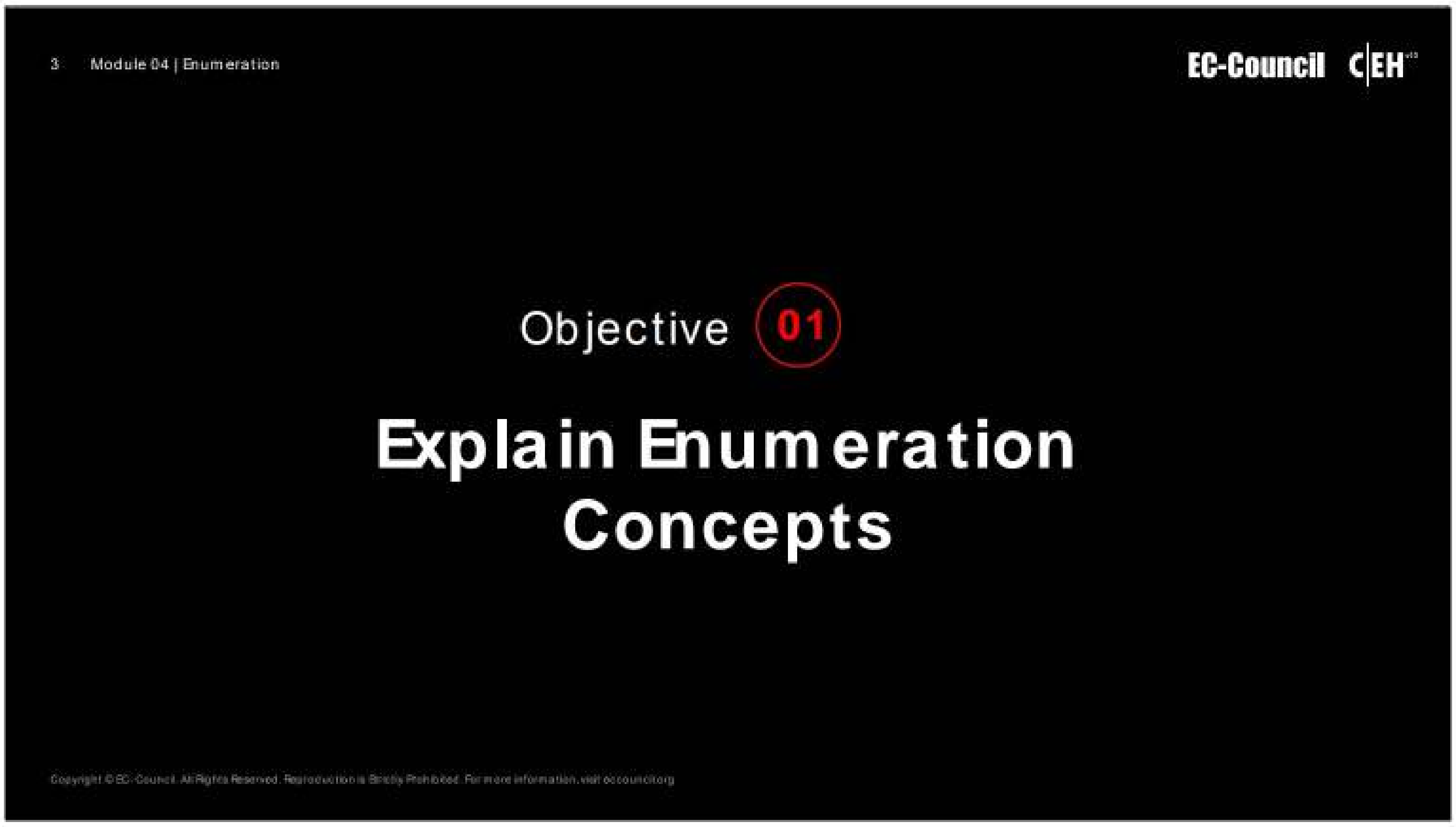
Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Learning Objectives

In the previous modules, you learned about footprinting and network scanning. This module covers the next phase, enumeration. We start with an introduction to enumeration concepts. Subsequently, the module provides insight into different techniques for Network Basic Input/Output System (NetBIOS), Simple Network Management Protocol (SNMP), Lightweight Directory Access Protocol (LDAP), Network Time Protocol (NTP), Network File System (NFS), Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), Internet Protocol Security (IPsec), Voice over Internet Protocol (VoIP), remote procedure call (RPC), Linux/Unix, and Server Message Block (SMB) enumeration. The module ends with an overview of enumeration countermeasures.

At the end of this module, you will be able to:

- Describe enumeration concepts
- Explain different techniques for NetBIOS enumeration
- Explain different techniques for SNMP enumeration
- Explain different techniques for LDAP and active directory (AD) enumeration
- Explain different techniques for NTP enumeration
- Explain different techniques for NFS enumeration
- Explain different techniques for SMTP and DNS enumeration
- Explain other enumeration techniques such as IPsec, VoIP, RPC, Linux/Unix, and SMB enumeration
- Apply enumeration countermeasures



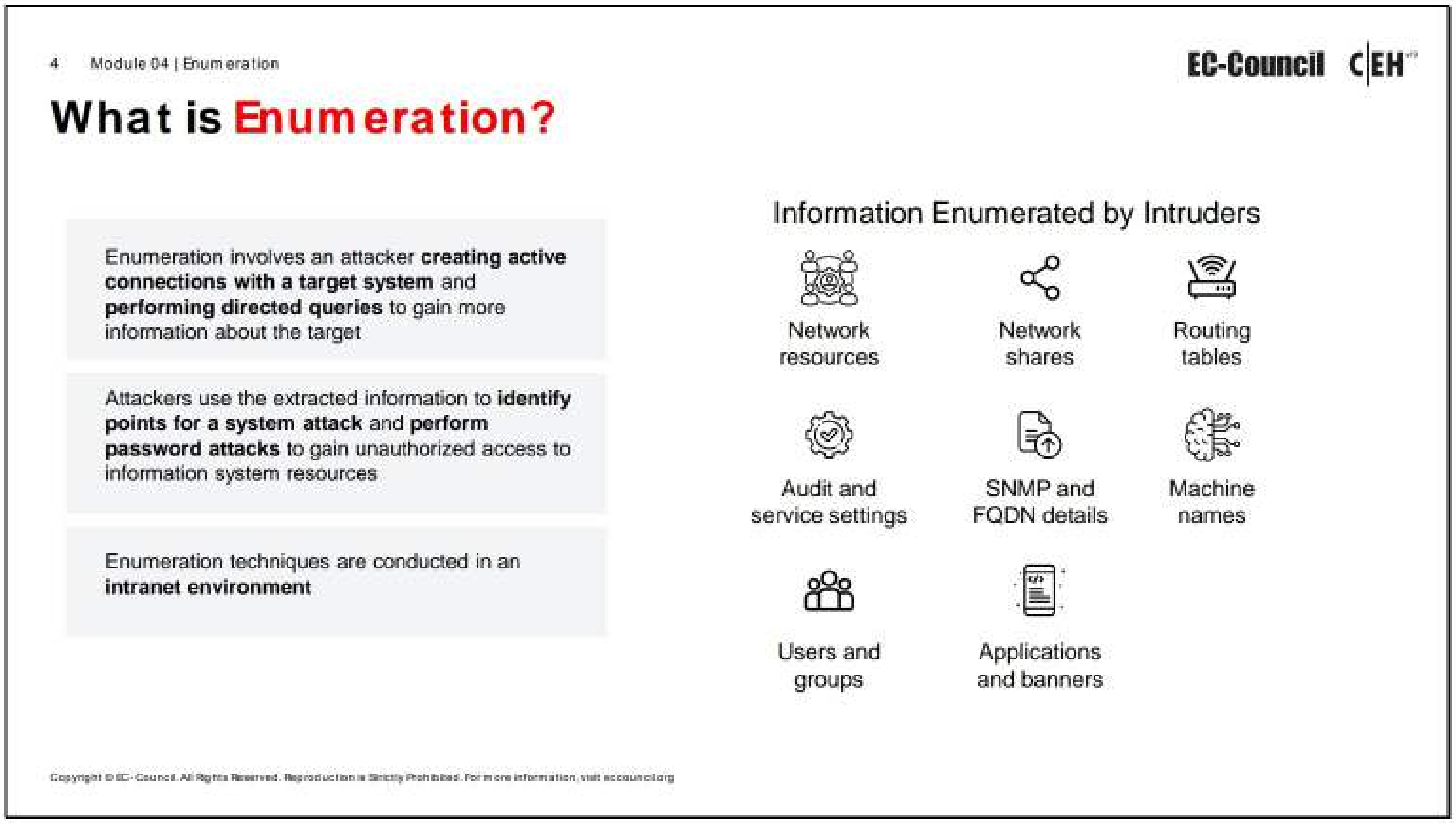
Objective 01

Explain Enumeration Concepts

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Enumeration Concepts

Different sections of this module deal with the enumeration of different services and ports. Before discussing the actual enumeration process, we introduce concepts related to enumeration.



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

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

What is Enumeration?

Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network. In the enumeration phase, an attacker creates active connections with the system and sends directed queries to gain more information about the target. The attacker uses the information collected using enumeration to identify vulnerabilities in the system security, which help them exploit the target system. In turn, enumeration allows the attacker to perform password attacks to gain unauthorized access to information system resources. Enumeration techniques work in an intranet environment.

In particular, enumeration allows the attacker to collect the following information:

- Network resources
- Network shares
- Routing tables
- Audit and service settings
- SNMP and fully qualified domain name (FQDN) details
- Machine names
- Users and groups
- Applications and banners

During enumeration, attackers may stumble upon a remote inter-process communication (IPC) share, such as IPC$ in Windows, which they can probe further to connect to an administrative share by brute-forcing admin credentials and obtain complete information about the file-system listing that the share represents.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The previous modules highlighted how attackers gather necessary information about a target without any illegal activity. However, enumeration activities may be illegal depending on the organization's policies and the laws that are in effect. An ethical hacker or pen tester should always acquire proper authorization before performing enumeration.

Techniques for Enumeration

The following techniques are used to extract information about a target.

- **Extract usernames using email IDs**

  Every email address contains two parts, a username and a domain name, in the format "username@domainname."

- **Extract information using default passwords**

  Many online resources provide a list of default passwords assigned by manufacturers to their products. Users often ignore recommendations to change the default usernames and passwords provided by the manufacturer or developer of a product. This eases an attacker's task of enumerating and exploiting the target system.

- **Brute force Active Directory**

  Microsoft Active Directory is susceptible to username enumeration at the time of user-supplied input verification. This is a design error in the Microsoft Active Directory implementation. If a user enables the "logon hours" feature, then all the attempts at service authentication result in different error messages. Attackers take advantage of this to enumerate valid usernames. An attacker who succeeds in extracting valid usernames can conduct a brute-force attack to crack the respective passwords.

- **Extract information using DNS Zone Transfer**

  A network administrator can use DNS zone transfer to replicate DNS data across several DNS servers or back up DNS files. For this purpose, the administrator needs to execute a specific zone-transfer request to the name server. If the name server permits zone transfer, it will convert all the DNS names and IP addresses hosted by that server to ASCII text.

  If the network administrators did not configure the DNS server properly, the DNS zone transfer can be an effective method to obtain information about the organization's network. This information may include lists of all named hosts, sub-zones, and related IP addresses. A user can perform DNS zone transfer using nslookup and dig commands.

- **Extract user groups from Windows**

  To extract user groups from Windows, the attacker should have a registered ID as a user in the Active Directory. The attacker can then extract information from groups in which the user is a member by using the Windows interface or command-line method.

- **Extract usernames using SNMP**

  Attackers can easily guess read-only or read-write community strings by using the SNMP application programming interface (API) to extract usernames.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Extract network resources and topology using SNMP**

  Attackers can methodically query the SNMP tree to gather detailed information about network resources and topology.

Services and Ports to Enumerate

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) manage data communications between terminals in a network.

TCP is a connection-oriented protocol capable of carrying messages or emails over the Internet. It provides a reliable multi-process communication service in a multi-network environment. The features and functions of TCP include the following:

- Supports acknowledgement for receiving data through a sliding window acknowledgement system
- Offers automatic retransmission of lost or acknowledged data
- Allows addressing and multiplexing of data
- A connection can be established, managed, or terminated
- Offers quality-of-service transmission
- Offers congestion management and flow control

UDP is a connectionless protocol that carries short messages over a computer network. It provides unreliable service. The applications of UDP include the following:

- Audio streaming
- Videoconferencing and teleconferencing

Services and TCP/UDP ports that can be enumerated include the following.

- **TCP/UDP 53: DNS Zone Transfer**

  The DNS resolution process establishes communication between DNS clients and DNS servers. DNS clients send DNS messages to DNS servers listening on UDP port 53. If the DNS message size exceeds the default size of UDP (512 octets), the response contains only the data that UDP can accommodate, and the DNS server sets a flag to indicate the truncated response. The DNS client can now resend the request via TCP over port 53 to the DNS server. In this approach, the DNS server uses UDP as a default protocol. In the case of lengthy queries for which UDP fails, TCP is used as a failover solution. Malware such as ADM worm and Bonk Trojan uses port 53 to exploit vulnerabilities within DNS servers, helping intruders launch attacks.

- **TCP/UDP 135: Microsoft RPC Endpoint Mapper**

  Source: *https://docs.microsoft.com*

  RPC is a protocol used by a client system to request a service from a server. An endpoint is the protocol port on which the server listens for the client's RPCs. The RPC Endpoint Mapper enables RPC clients to determine the port number currently assigned to a specific

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

RPC service. There is a flaw in the part of RPC that exchanges messages over TCP/IP. The incorrect handling of malformed messages causes failure. This affects the RPC Endpoint Mapper, which listens on TCP/IP port 135. This vulnerability could allow an attacker to send RPC messages to the RPC Endpoint Mapper process on a server to launch a denial-of-service (DoS) attack.

- **UDP 137: NetBIOS Name Service (NBNS)**

  NBNS, also known as the Windows Internet Name Service (WINS), provides a name-resolution service for computers running NetBIOS. NetBIOS name servers maintain a database of the NetBIOS names for hosts and the corresponding IP address the host is using. NBNS aims to match IP addresses with NetBIOS names and queries. Attackers usually attack the name service first. Typically, NBNS uses UDP 137 as its transport protocol. It can also use TCP 137 as its transport protocol for a few operations, though this might never occur in practice.

- **TCP 139: NetBIOS Session Service (SMB over NetBIOS)**

  TCP 139 is perhaps the most well-known Windows port. It is used to transfer files over a network. Systems use this port for both null-session establishment as well as file and printer sharing. A system administrator considering the restriction of access to ports on a Windows system should make the restriction of TCP 139 a top priority. An improperly configured TCP 139 port can allow an intruder to gain unauthorized access to critical system files or the complete file system, resulting in data theft or other malicious activities.

- **TCP/UDP 445: SMB over TCP (Direct Host)**

  Windows supports file- and printer-sharing traffic using the SMB protocol directly hosted on TCP. In earlier OSs, SMB traffic required the NetBIOS over TCP (NBT) protocol to work on TCP/IP transport. Directly hosted SMB traffic uses port 445 (TCP and UDP) instead of NetBIOS.

- **UDP 161: Simple Network Management Protocol (SNMP)**

  SNMP is widely used in network management systems to monitor network-attached devices such as routers, switches, firewalls, printers, and servers. It consists of a manager and agents. The agent receives requests on port 161 from the managers and responds to the managers on port 162.

- **TCP/UDP 389: Lightweight Directory Access Protocol (LDAP)**

  LDAP is a protocol for accessing and maintaining distributed directory information services over an IP network. By default, LDAP uses TCP or UDP as its transport protocol over port 389.

- **TCP 2049: Network File System (NFS)**

  NFS protocol is used to mount file systems on a remote host over a network, and users can interact with the file systems as if they are mounted locally. NFS servers listen to its client systems on TCP port 2049. If NFS services are not properly configured, then attackers may exploit the NFS protocol to gain control over a remote system, perform privilege escalation, inject backdoors or malware on a remote host, etc.

- **TCP 25: Simple Mail Transfer Protocol (SMTP)**

  SMTP is a TCP/IP mail delivery protocol. It transfers email across the Internet and across local networks. It runs on the connection-oriented service provided by TCP and uses the well-known port number 25. Below table lists some commands used by SMTP and their respective syntaxes.

Hello	HELO <sending-host>
From	MAIL FROM:<from-address>
Recipient	RCPT TO:<to-address>
Data	DATA
Reset	RESET
Verify	VRFY<string>
Expand	EXPN<string>
Help	HELP[string]
Quit	QUIT

Table 4.1: SMTP commands and their respective syntaxes

- **TCP/UDP 162: SNMP Trap**

  An SNMP trap uses TCP/UDP port 162 to send notifications such as optional variable bindings and the sysUpTime value from an agent to a manager.

- **UDP 500: Internet Security Association and Key Management Protocol (ISAKMP)/Internet Key Exchange (IKE)**

  Internet Security Association and Key Management Protocol (ISAKMP)/Internet Key Exchange (IKE) is a protocol used to set up a security association (SA) in the IPsec protocol suite. It uses UDP port 500 to establish, negotiate, modify, and delete SAs and cryptographic keys in a virtual private network (VPN) environment.

- **TCP 22: Secure Shell (SSH) / Secure File Transfer Protocol (SFTP)**

  Secure Shell (SSH) is a command-level protocol mainly used for managing various networked devices securely. It is generally used as an alternative protocol to the unsecure Telnet protocol. SSH uses the client/server communication model, and the SSH server, by default, listens to its client on TCP port 22. Attackers may exploit the SSH protocol by brute-forcing SSH login credentials.

  SFTP, by default, uses port 22, facilitating the secure exchange of data over a single Internet connection. This designated port for SFTP enhances its security and simplicity compared to protocols such as FTP/S that require multiple ports for operation. SFTP's reliance on just one port makes its use more straightforward while it continues to secure data transfers through SSH encryption. Attackers enumerate SFTP to gather information about user accounts, file and directory permissions, and the server's configuration.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **TCP/UDP 3268: Global Catalog Service**

  Microsoft's Global Catalog server, a domain controller that stores extra information, uses port 3268. Its database contains rows for every object in the entire organization, instead of rows for only the objects in one domain. Global Catalog allows one to locate objects from any domain without having to know the domain name. LDAP in the Global Catalog server uses port 3268. This service listens to port 3268 through a TCP connection. Administrators use port 3268 for troubleshooting issues in the Global Catalog by connecting to it using LDP.

- **TCP/UDP 5060, 5061: Session Initiation Protocol (SIP)**

  The Session Initiation Protocol (SIP) is a protocol used in Internet telephony for voice and video calls. It typically uses TCP/UDP port 5060 (non-encrypted signaling traffic) or 5061 (encrypted traffic with TLS) for SIP to servers and other endpoints.

- **TCP 20/21: File Transfer Protocol**

  FTP is a connection-oriented protocol used for transferring files over the Internet and private networks. FTP is controlled on TCP port 21, and for data transmission, FTP uses TCP port 20 or some dynamic port numbers depending on the server configuration. If attackers identify that FTP server ports are open, then they perform enumeration on FTP to find information such as the software version and state of existing vulnerabilities to perform further exploitations such as the sniffing of FTP traffic and FTP brute-force attacks.

- **TCP 23: Telnet**

  The Telnet protocol is used for managing various networked devices remotely. It is an unsecure protocol because it transmits login credentials in the cleartext format. Therefore, it is mostly used in private networks. The Telnet server listens to its clients on port 23. Attackers can take advantage of the Telnet protocol to perform banner grabbing on other protocols such as SSH and SMTP, brute-forcing attacks on login credentials, port-forwarding attacks, etc.

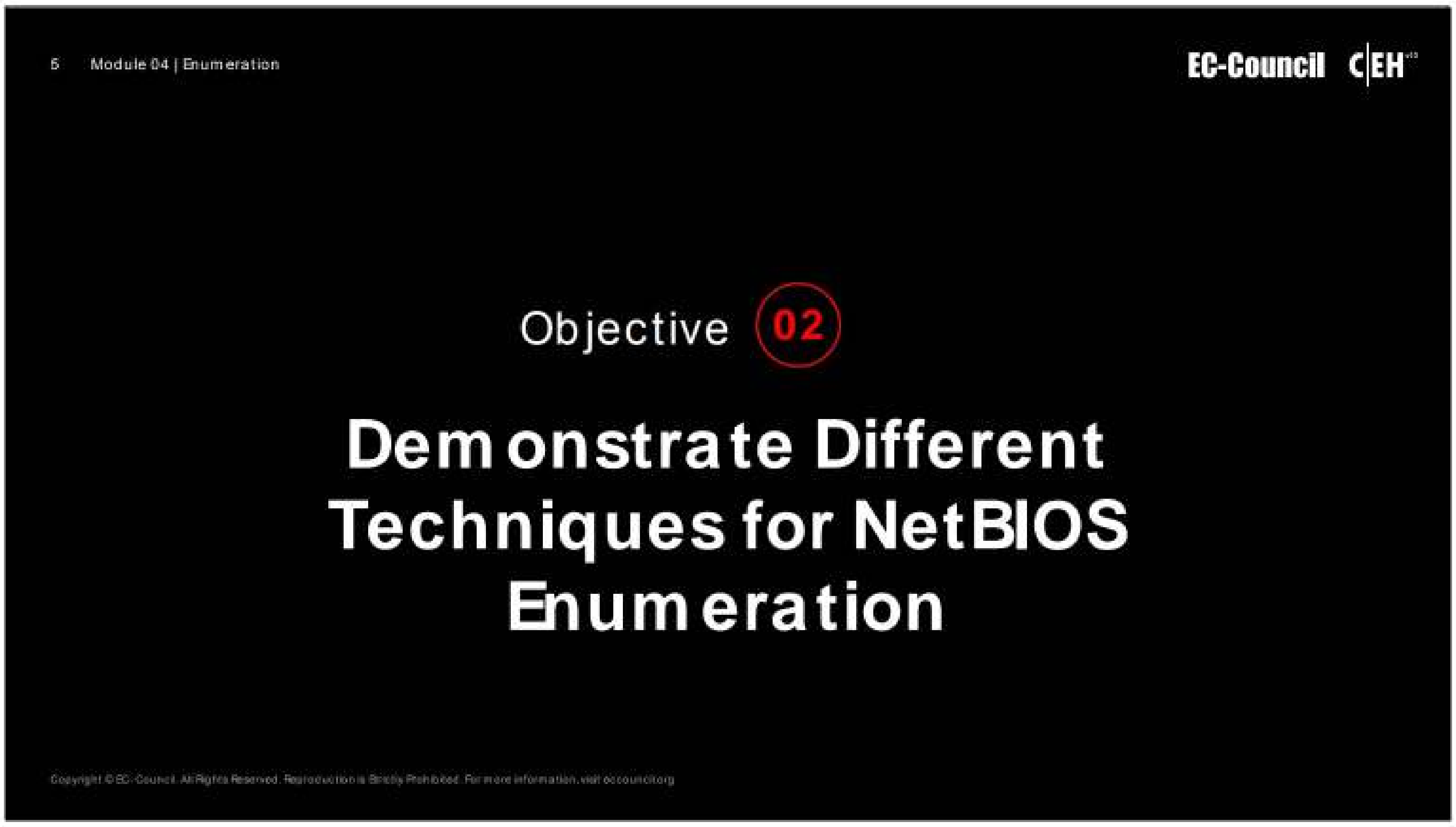
- **UDP 69: Trivial File Transfer Protocol (TFTP)**

  TFTP is a connectionless protocol used for transferring files over the Internet. TFTP depends on connectionless UDP; therefore, it does not guarantee the proper transmission of the file to the destination. TFTP is mainly used to update or upgrade software and firmware on remote networked devices. It uses UDP port 69 for transferring files to a remote host. Attackers may exploit TFTP to install malicious software or firmware on remote devices.

- **TCP 179: Border Gateway Protocol (BGP)**

  BGP is widely used by Internet service providers (ISPs) to maintain huge routing tables and for efficiently processing Internet traffic. BGP routers establish sessions on TCP port 179. The misconfiguration of BGP may lead to various attacks such as dictionary attacks, resource-exhaustion attacks, flooding attacks, and hijacking attacks.

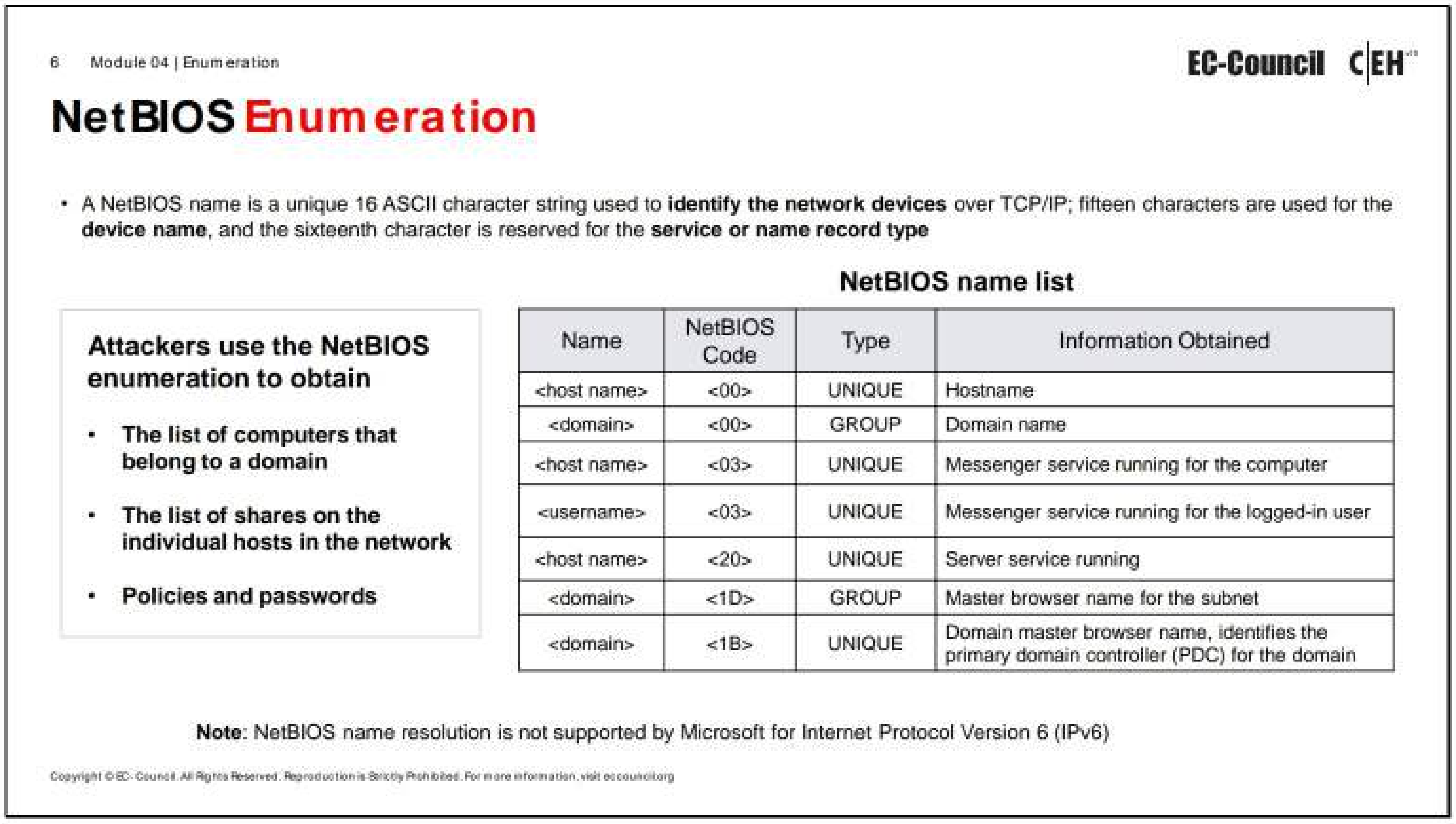
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Objective 02

Demonstrate Different Techniques for NetBIOS Enumeration

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org



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

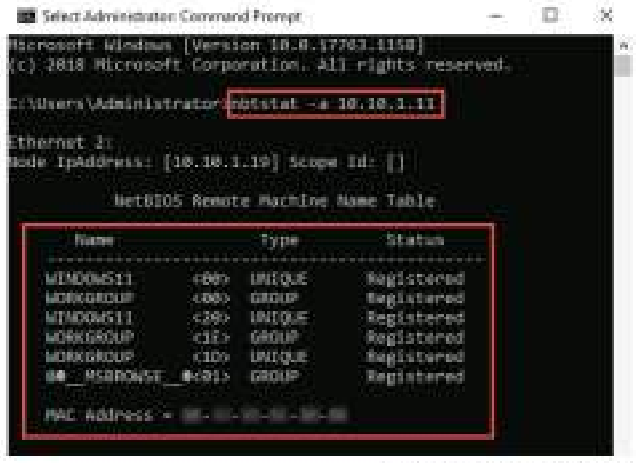
Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

NetBIOS Enumeration (Cont'd)

Nbtstat Utility

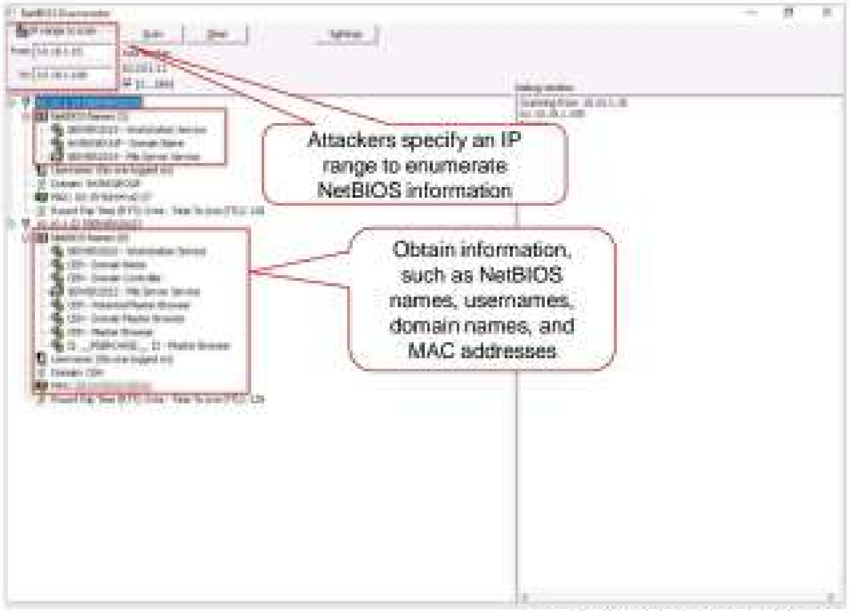
Run the `nbtstat` command "`nbtstat -a <IP address of the remote machine>`" to obtain the NetBIOS name table of a remote computer



```
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.1.11

Ethernet 2:
Node IpAddress: [10.10.1.19] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WINDOWS11      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WINDOWS11      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ☻☻__MSBROWSE__☻<01>  GROUP       Registered

    MAC Address = [redacted]
```

https://learn.microsoft.com

NetBIOS Enumerator



Attackers specify an IP range to enumerate NetBIOS information

Obtain information, such as NetBIOS names, usernames, domain names, and MAC addresses

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

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

NetBIOS Enumeration

This section describes NetBIOS enumeration, the information obtained, and various NetBIOS enumeration tools. NetBIOS is considered first for enumeration because it extracts a large amount of sensitive information about the target network, such as users and network shares.

The first step in enumerating a Windows system is to take advantage of the NetBIOS API. NetBIOS was originally developed as an API for client software to access local area network (LAN) resources. Windows uses NetBIOS for file and printer sharing. The NetBIOS name is a unique 16-character ASCII string assigned to Windows systems to identify network devices over TCP/IP; 15 characters are used for the device name, and the 16th is reserved for the service or record type. NetBIOS uses UDP port 137 (name services), UDP port 138 (datagram services), and TCP port 139 (session services). Attackers usually target the NetBIOS service because it is easy to exploit and run on Windows systems even when not in use.

Attackers use NetBIOS enumeration to obtain the following:

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

An attacker who finds a Windows system with port 139 open can check to see which resources can be accessed or viewed on a remote system. However, to enumerate the NetBIOS names, the remote system must have enabled file and printer sharing. NetBIOS enumeration may allow an attacker to read or write to a remote computer system, depending on the availability of shares, or launch a DoS attack.

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, which identifies the primary domain controller (PDC) for the domain
<domain>	<1E>	GROUP	Browser service elections

Table 4.2: NetBIOS name list

Note that Microsoft does not support NetBIOS name resolution for IPv6.

Nbtstat Utility

Source: *https://learn.microsoft.com*

Nbtstat is a Windows utility that helps in troubleshooting NETBIOS name resolution problems. The `nbtstat` command removes and corrects preloaded entries using several case-sensitive switches. Attackers use Nbtstat to enumerate information such as NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both local and remote computers, and the NetBIOS name cache.

The syntax of the nbtstat command is as follows:

```
nbtstat [-a <remotename>] [-A <IPaddress>] [-c] [-n] [-r] [-R] [-RR] [-
s] [-S] [<interval>][-?]
```

The table shown below lists various Nbtstat parameters and their respective functions.

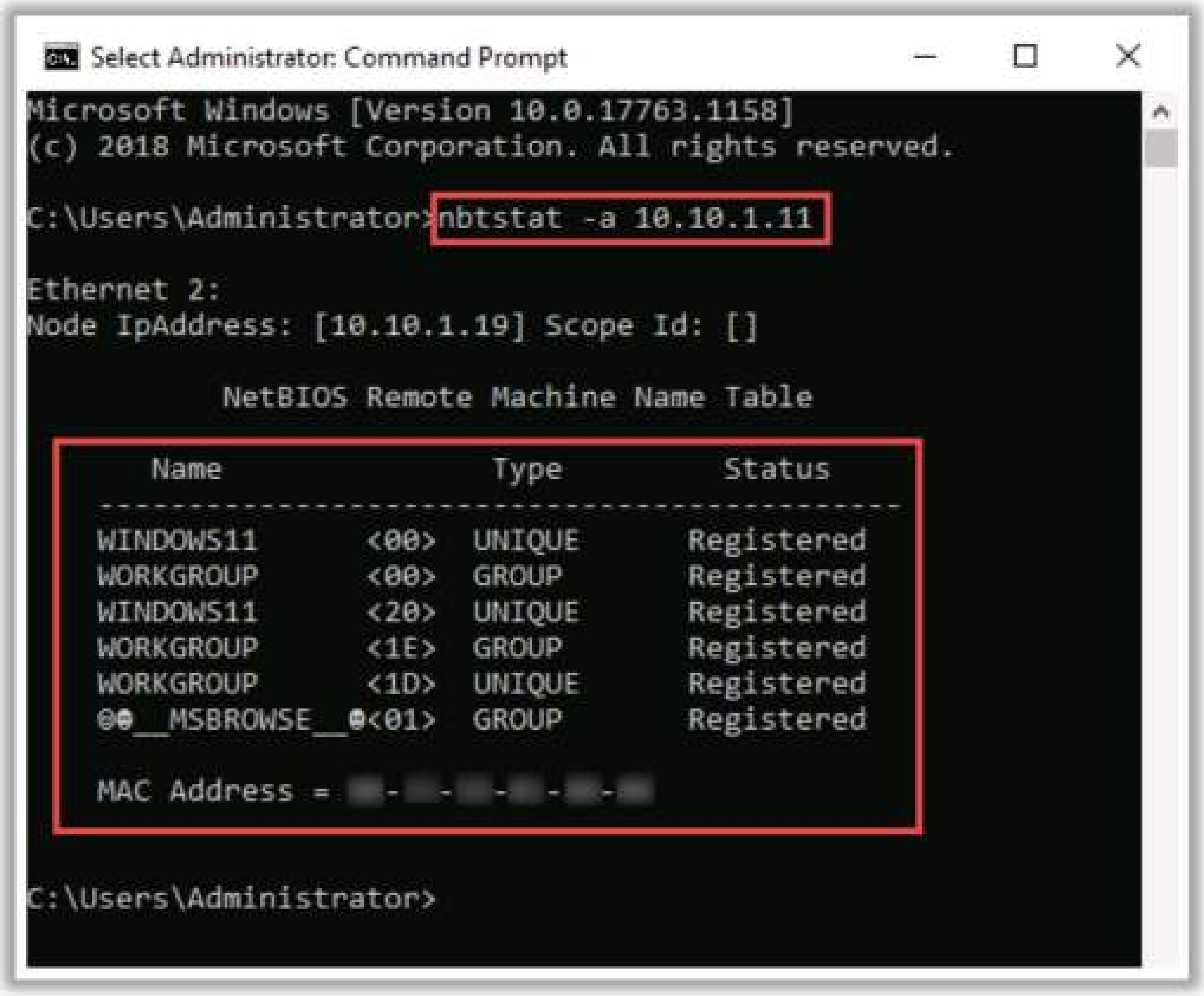
Nbtstat Parameter	Function
`-a <remotename>`	Displays the NetBIOS name table of a remote computer, where <remotename> is the NetBIOS computer name of the remote computer
`-A <IPaddress>`	Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer
`-c`	Lists the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses
`-n`	Displays the names registered locally by NetBIOS applications such as the server and redirector
`-r`	Displays a count of all names resolved by a broadcast or WINS server

`-R`	Purges the name cache and reloads all #PRE-tagged entries from the Lmhosts file
`-RR`	Releases and re-registers all names with the name server
`-s`	Lists the NetBIOS sessions table converting destination IP addresses to computer NetBIOS names
`-S`	Lists the current NetBIOS sessions and their status with the IP addresses
`<interval>`	Re-displays selected statistics, pausing at each display for the number of seconds specified in Interval
`-?`	Displays help

Table 4.3: Nbtstat parameters and their respective functions

The following are some examples for nbtstat commands.

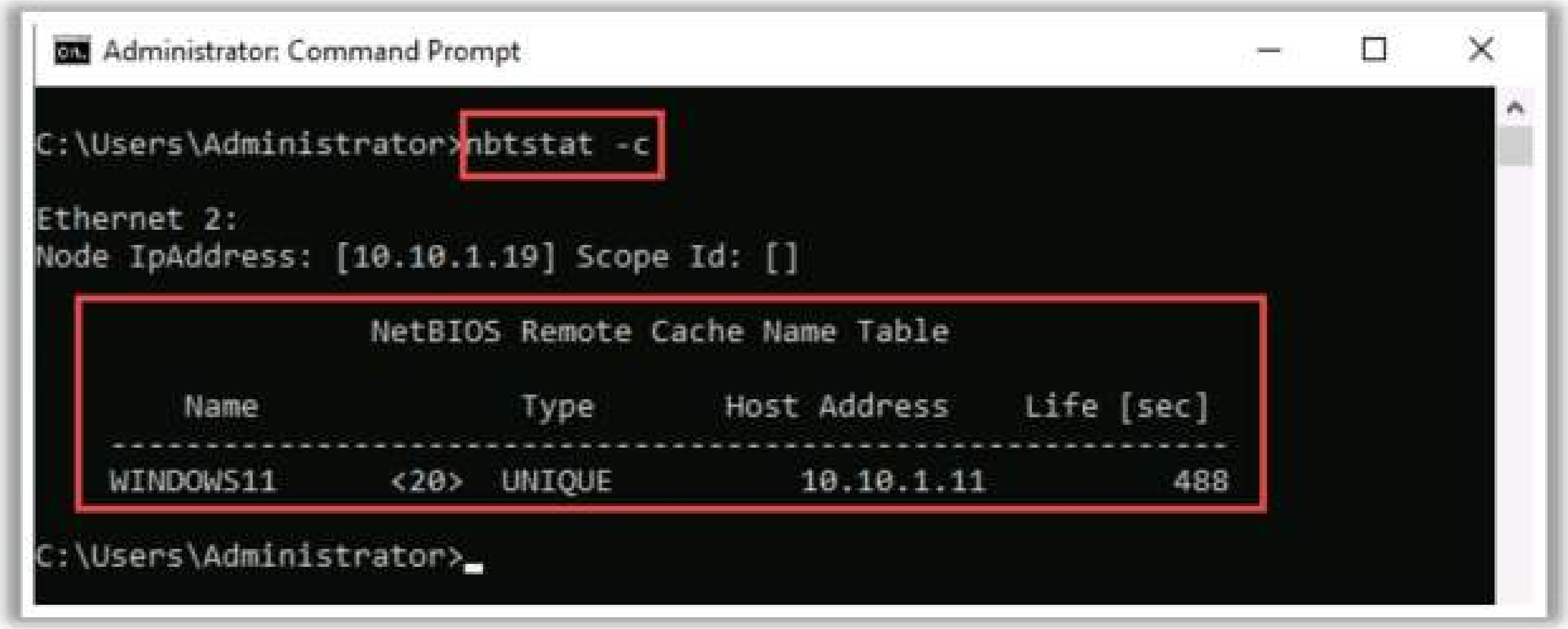
- The nbtstat command "**`nbtstat –a <IP address of the remote machine>`**" can be executed to obtain the NetBIOS name table of a remote computer.



```
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.1.11

Ethernet 2:
Node IpAddress: [10.10.1.19] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WINDOWS11      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WINDOWS11      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ☺☻__MSBROWSE__☻<01>  GROUP       Registered

    MAC Address = [redacted]

C:\Users\Administrator>
```

Figure 4.1: Nbtstat command to obtain the name table of a remote system

- The nbtstat command "**`nbtstat –c`**" can be executed to obtain the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.



```
C:\Users\Administrator>nbtstat -c

Ethernet 2:
Node IpAddress: [10.10.1.19] Scope Id: []

                NetBIOS Remote Cache Name Table

    Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    WINDOWS11      <20>  UNIQUE          10.10.1.11          488

C:\Users\Administrator>
```

Figure 4.2: Nbtstat command to obtain the contents of the NetBIOS name table

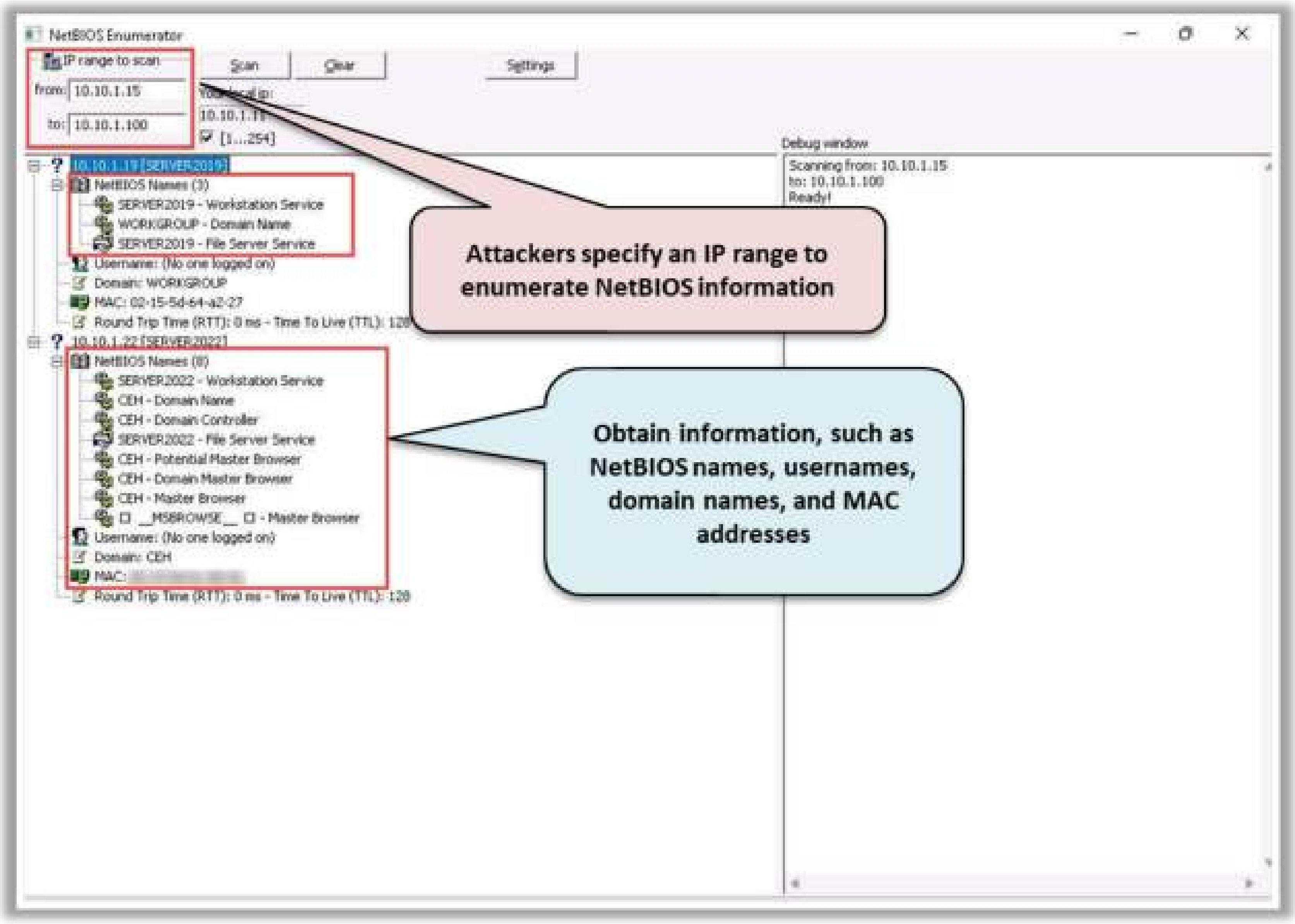
NetBIOS Enumeration Tools

NetBIOS enumeration tools explore and scan a network within a given range of IP addresses and lists of computers to identify security loopholes or flaws in networked systems. These tools also enumerate operating systems (OSs), users, groups, Security Identifiers (SIDs), password policies, services, service packs and hotfixes, NetBIOS shares, transports, sessions, disks and security event logs, etc.

- **NetBIOS Enumerator**

  Source: *https://nbtenum.sourceforge.net*

  NetBIOS Enumerator is an enumeration tool that shows how to use remote network support and to deal with some other web protocols, such as SMB. As shown in the screenshot, attackers use NetBIOS Enumerator to enumerate details such as NetBIOS names, usernames, domain names, and media access control (MAC) addresses for a given range of IP addresses.



```
from: 10.10.1.15
to: 10.10.1.100
10.10.1.11
☑ [1...254]
```

```
? 10.10.1.19 [SERVER2019]
    NetBIOS Names (3)
        SERVER2019 - Workstation Service
        WORKGROUP - Domain Name
        SERVER2019 - File Server Service
    Username: (No one logged on)
    Domain: WORKGROUP
    MAC: 02-15-5d-64-a2-27
    Round Trip Time (RTT): 0 ms - Time To Live (TTL): 128
? 10.10.1.22 [SERVER2022]
    NetBIOS Names (8)
        SERVER2022 - Workstation Service
        CEH - Domain Name
        CEH - Domain Controller
        SERVER2022 - File Server Service
        CEH - Potential Master Browser
        CEH - Domain Master Browser
        CEH - Master Browser
        __MSBROWSE__ - Master Browser
    Username: (No one logged on)
    Domain: CEH
    MAC: [redacted]
    Round Trip Time (RTT): 0 ms - Time To Live (TTL): 128
```

```
Scanning from: 10.10.1.15
to: 10.10.1.100
Ready!
```

Attackers specify an IP range to enumerate NetBIOS information

Obtain information, such as NetBIOS names, usernames, domain names, and MAC addresses

Figure 4.3: Screenshot of NetBIOS Enumerator

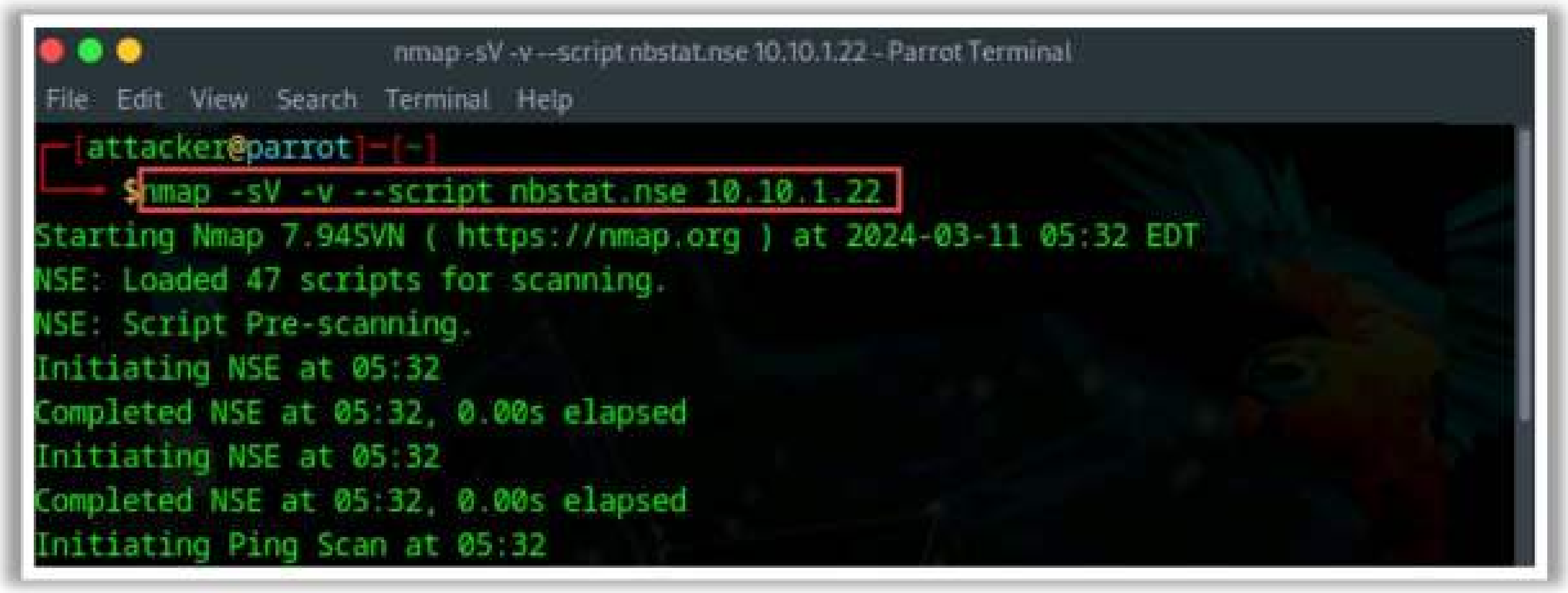
- **Nmap**

  Source: *https://nmap.org*

  Attackers use the Nmap Scripting Engine (NSE) for discovering NetBIOS shares on a network. The NSE nbstat script allows attackers to retrieve the target's NetBIOS names and MAC addresses. By default, the script displays the name of the computer and the logged-in user. However, if the verbosity is turned up, it displays all names related to that system.

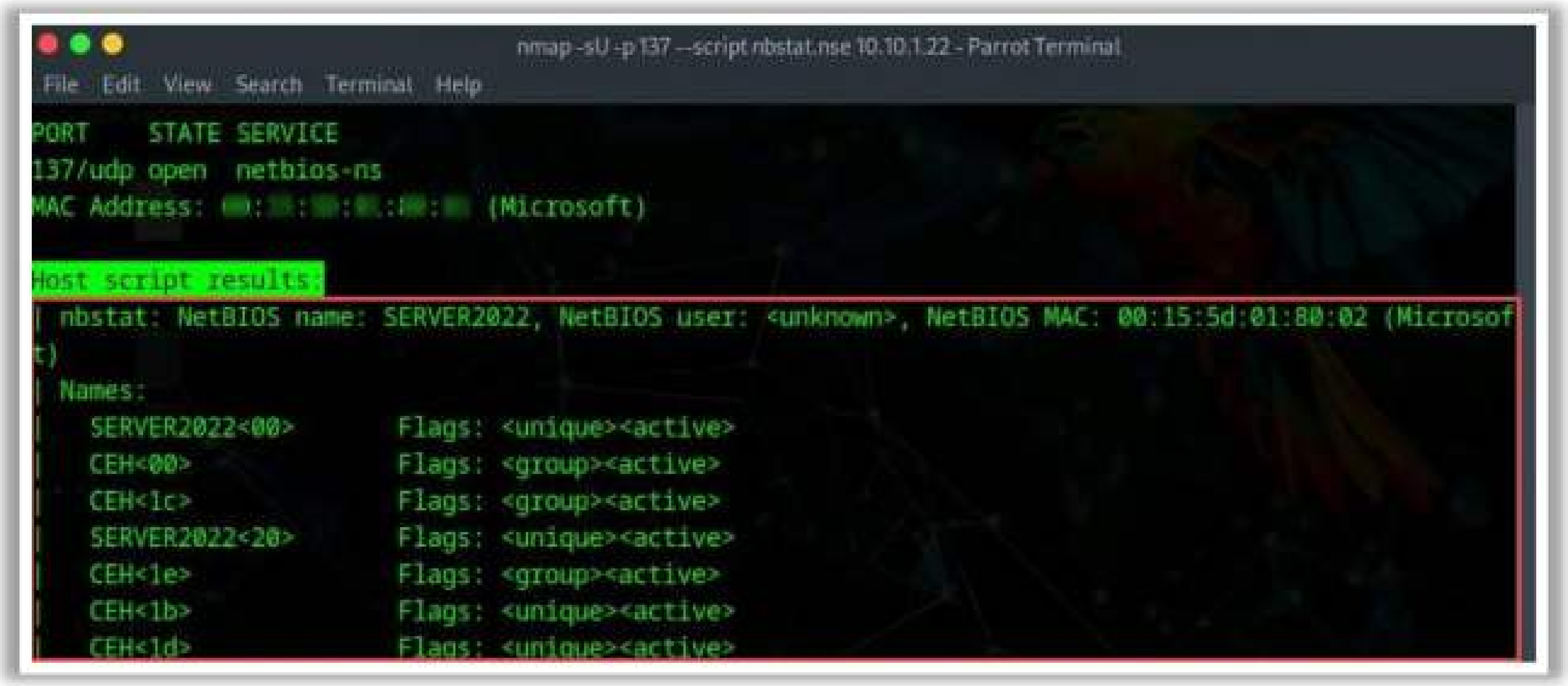
  As shown in the screenshot, an attacker uses the following Nmap command to perform NetBIOS enumeration on a target host:

  `nmap -sV -v --script nbstat.nse <target IP address>`


nmap -sV -v --script nbstat.nse 10.10.1.22 - Parrot Terminal
File
Edit
View
Search
Terminal
Help

```
┌─[attacker@parrot]─[~]
└──╼ $nmap -sV -v --script nbstat.nse 10.10.1.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 05:32 EDT
NSE: Loaded 47 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:32
Completed NSE at 05:32, 0.00s elapsed
Initiating NSE at 05:32
Completed NSE at 05:32, 0.00s elapsed
Initiating Ping Scan at 05:32
```

Figure 4.4: Screenshot of Nmap command for NetBIOS enumeration


nmap -sU -p 137 --script nbstat.nse 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help

```
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: [redacted] (Microsoft)

Host script results:
| nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:01:80:02 (Microsof
t)
| Names:
|   SERVER2022<00>       Flags: <unique><active>
|   CEH<00>              Flags: <group><active>
|   CEH<1c>              Flags: <group><active>
|   SERVER2022<20>       Flags: <unique><active>
|   CEH<1e>              Flags: <group><active>
|   CEH<1b>              Flags: <unique><active>
|   CEH<1d>              Flags: <unique><active>
```

Figure 4.5: Screenshot of Nmap NetBIOS enumeration output

The following are some additional NetBIOS enumeration tools:

- Global Network Inventory (*https://magnetosoft.com*)
- Advanced IP Scanner (*https://www.advanced-ip-scanner.com*)
- Hyena (*https://www.systemtools.com*)
- Nsauditor Network Security Auditor (*https://www.nsauditor.com*)

Enumerating User Accounts

Source: *https://learn.microsoft.com*

Enumerating user accounts using the PsTools suite helps in controlling and managing remote systems from the command line. The following are some commands for enumerating user accounts.

- **PsExec**

  PsExec is a lightweight Telnet replacement that can execute processes on other systems, complete with full interactivity for console applications, without having to install client software manually. PsExec's most powerful use case is the launch of interactive command prompts on remote systems and remote-enabling tools such as ipconfig that otherwise cannot show information about remote systems. The syntax of the PsExec command is as follows:

  ```
  psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd][-n s][-r servicename][-h][-l][-s|-e][-x][-i [session]][-c executable [-f|-v]][-w directory][-d][-<priority>][-a n,n,...] cmd [arguments]
  ```

- **PsFile**

  PsFile is a command-line utility that shows a list of files on a system that opened remotely, and it can close opened files either by name or by a file identifier. The default behavior of PsFile is to list the files on the local system opened by remote systems. Typing a command followed by "- " displays information on the syntax for that command. The syntax of the PsFile command is as follows:

```
psfile [\\RemoteComputer [-u Username [-p Password]]] [[Id | path]
[-c]]
```

- **PsGetSid**

  PsGetSid translates SIDs to their display name and vice versa. It works on built-in accounts, domain accounts, and local accounts. It also displays the SIDs of user accounts and translates an SID into the name that represents it. It works across the network to query SIDs remotely. The syntax of the PsGetSid command is as follows:

```
psgetsid [\\computer[,computer[,...] | @file] [-u username [-p
password]]] [account|SID]
```

- **PsKill**

  PsKill is a kill utility that can kill processes on remote systems and terminate processes on the local computer. Running PsKill with a process ID directs it to kill the process of that ID on the local computer. If a process name is specified, PsKill will kill all processes that have that name. One need not install a client on the target computer to use PsKill to terminate a remote process. The syntax of the PsKill command is as follows:

```
pskill [- ] [-t] [\\computer [-u username] [-p password]] <process
name | process id>
```

- **PsInfo**

  PsInfo is a command-line tool that gathers key information about local or remote legacy Windows systems, including the type of installation, kernel build, registered organization and owner, number of processors and their type, amount of physical memory, installation date of the system, and expiration date in the case of a trial version. By default, PsInfo shows information for the local system. A remote computer name can be specified to obtain information for a remote system. The syntax of the PsInfo command is as follows:

```
psinfo [[\\computer[,computer[,..] | @file [-u user
[-p psswd]]] [-h] [-s] [-d] [-c [-t delimiter]] [filter]
```

- **PsList**

  PsList is a command-line tool that displays central processing unit (CPU) and memory information or thread statistics. Tools in the Resource Kits, pstat and pmon, show different types of data only for the processes on the system on which the tools are run.

- **PsLoggedOn**

  PsLoggedOn is an applet that displays both the locally logged-in users and users logged in via resources for either the local computer or a remote one. If a username is specified instead of a computer, PsLoggedOn searches the computers in the network neighborhood and reveals if the user currently logged in. PsLoggedOn defines a locally logged-in user is one that has a profile loaded into the registry. Therefore, PsLoggedOn determines who is logged in by scanning the keys under the HKEY_USERS key. For each key that has a name

All Rights Reserved. Reproduction is Strictly Prohibited.

or user SID, PsLoggedOn looks up the corresponding username and displays it. To determine who logged into a computer via resource shares, PsLoggedOn uses the NetSessionEnum API. The syntax of the PsLoggedOn command is as follows:

```
psloggedon [- ] [-l] [-x] [\\computername | username]
```

- **PsLogList**

  The elogdump utility dumps the contents of an Event Log on a local or remote computer. PsLogList is a clone of elogdump except that PsLogList can log in to remote systems in situations where the user's security credentials would not permit access to the Event Log, and PsLogList retrieves message strings from the computer on which the event log is stored. The default function of PsLogList is to display the contents of the System Event Log on the local computer with visually friendly formatting. The syntax of the PsLogList command is as follows:

```
psloglist [- ] [\\computer[,computer[,...] | @file [-u username [-
p password]]] [-s [-t delimiter]] [-m #|-n #|-h #|-d #|-w][-c][-
x][-r][-a mm/dd/yy][-b mm/dd/yy][-f filter] [-i ID[,ID[,...] | -e
ID[,ID[,...]]] [-o event source[,event source][,..]]] [-q event
source[,event source][,..]]] [-l event log file] <eventlog>
```

- **PsPasswd**

  PsPasswd can change an account password on local or remote systems, and administrators can create batch files that run PsPasswd on the computers they manage to perform a mass change of the administrator password. PsPasswd uses Windows password reset APIs; therefore, it does not send passwords over the network in the cleartext. The syntax of the PsPasswd command is as follows:

```
pspasswd [[\\computer[,computer[,..] | @file [-u user [-p psswd]]]
Username [NewPassword]
```

- **PsShutdown**

  PsShutdown can shut down or reboot a local or remote computer. It requires no manual installation of client software. The syntax of the PsShutdown command is as follows:

```
psshutdown [[\\computer[,computer[,..] | @file [-u user [-p
psswd]]] -s|-r|-h|-d|-k|-a|-l|-o [-f] [-c] [-t nn|h:m] [-n s] [-v
nn] [-e [u|p]:xx:yy] [-m "message"]
```

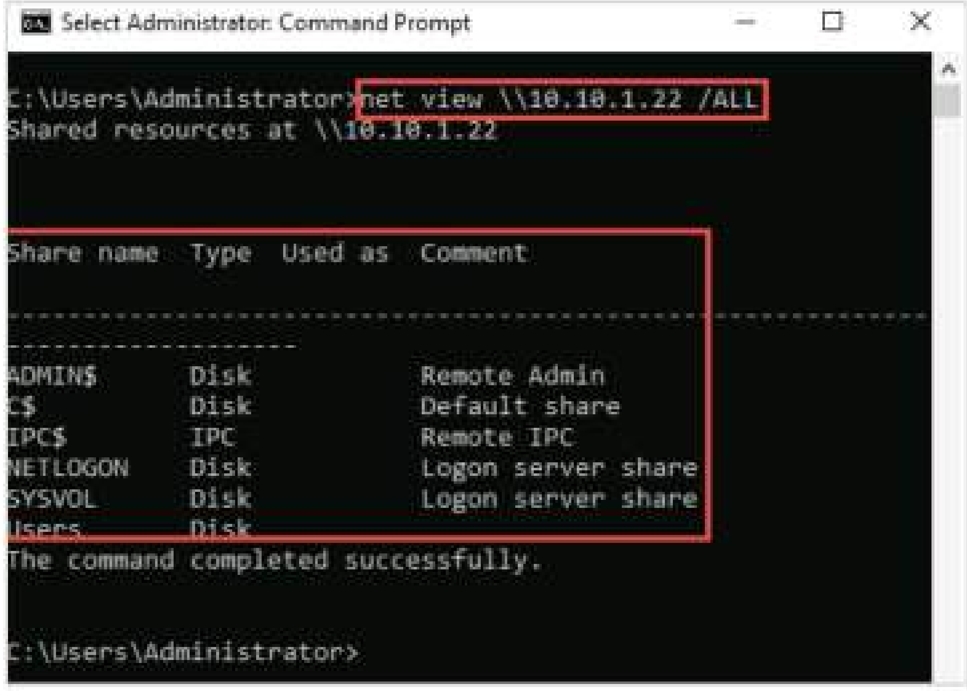
All Rights Reserved. Reproduction is Strictly Prohibited.

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>**



```
C:\Users\Administrator>net view \\10.10.1.22 /ALL
Shared resources at \\10.10.1.22



Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
ADMIN$      Disk           Remote Admin
C$          Disk           Default share
IPC$        IPC            Remote IPC
NETLOGON    Disk           Logon server share
SYSVOL      Disk           Logon server share
Users       Disk
The command completed successfully.


C:\Users\Administrator>
```

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Enumerating Shared Resources Using Net View

Net View is a command-line utility that displays a list of computers in a specified workgroup or shared resources available on a specified computer. It can be used in the following ways.

```
net view \\<computername>
```

In the above command, `<computername>` is the name or IP address of a specific computer, the resources of which are to be displayed.

```
net view \\<computername> /ALL
```

The above command displays all the shares on the specified remote computer, along with hidden shares.

```
net view /domain
```

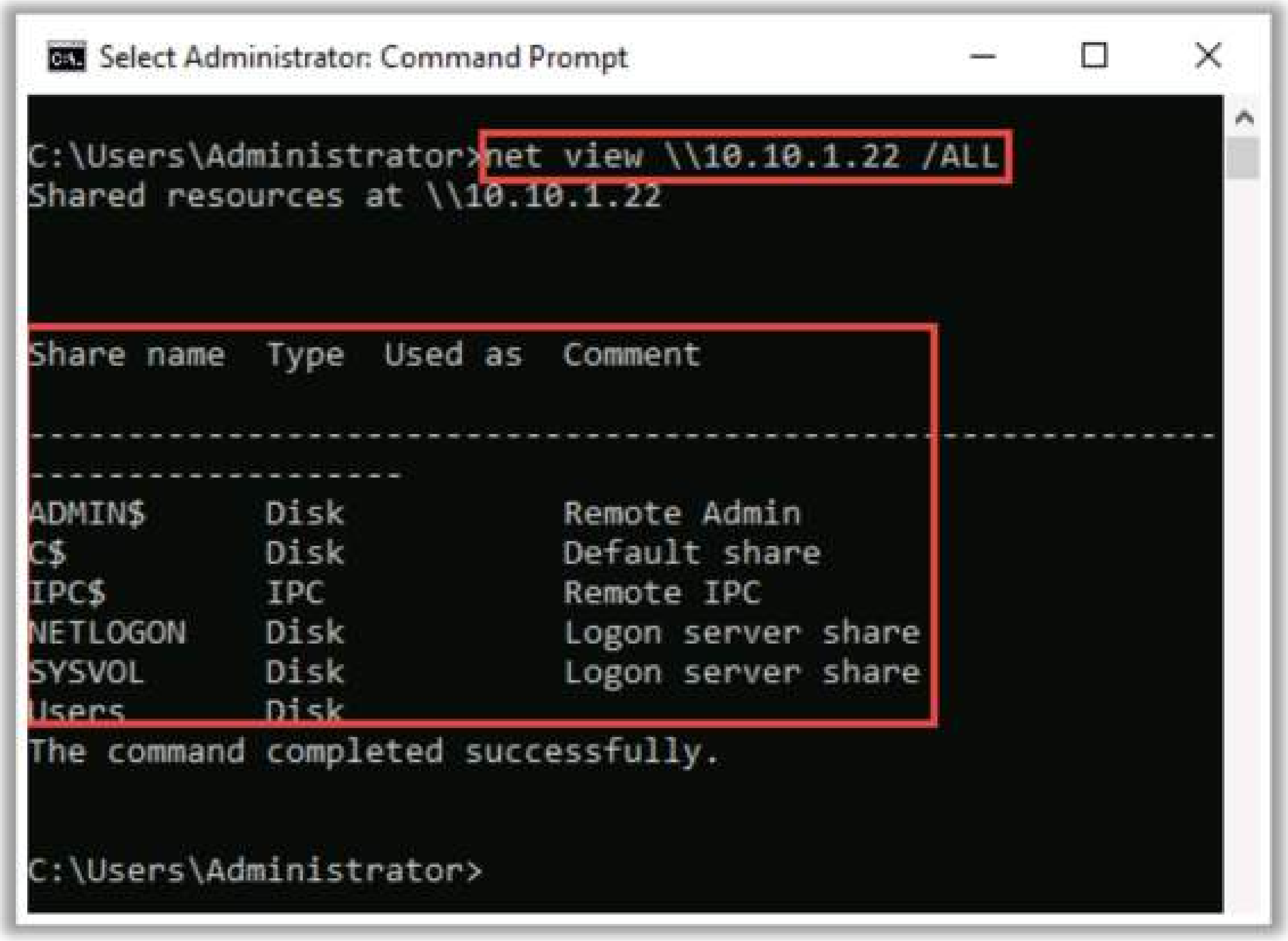
The above command displays all the shares in the domain.

```
net view /domain:<domain name>
```

The above command displays all the shares on the specified domain.

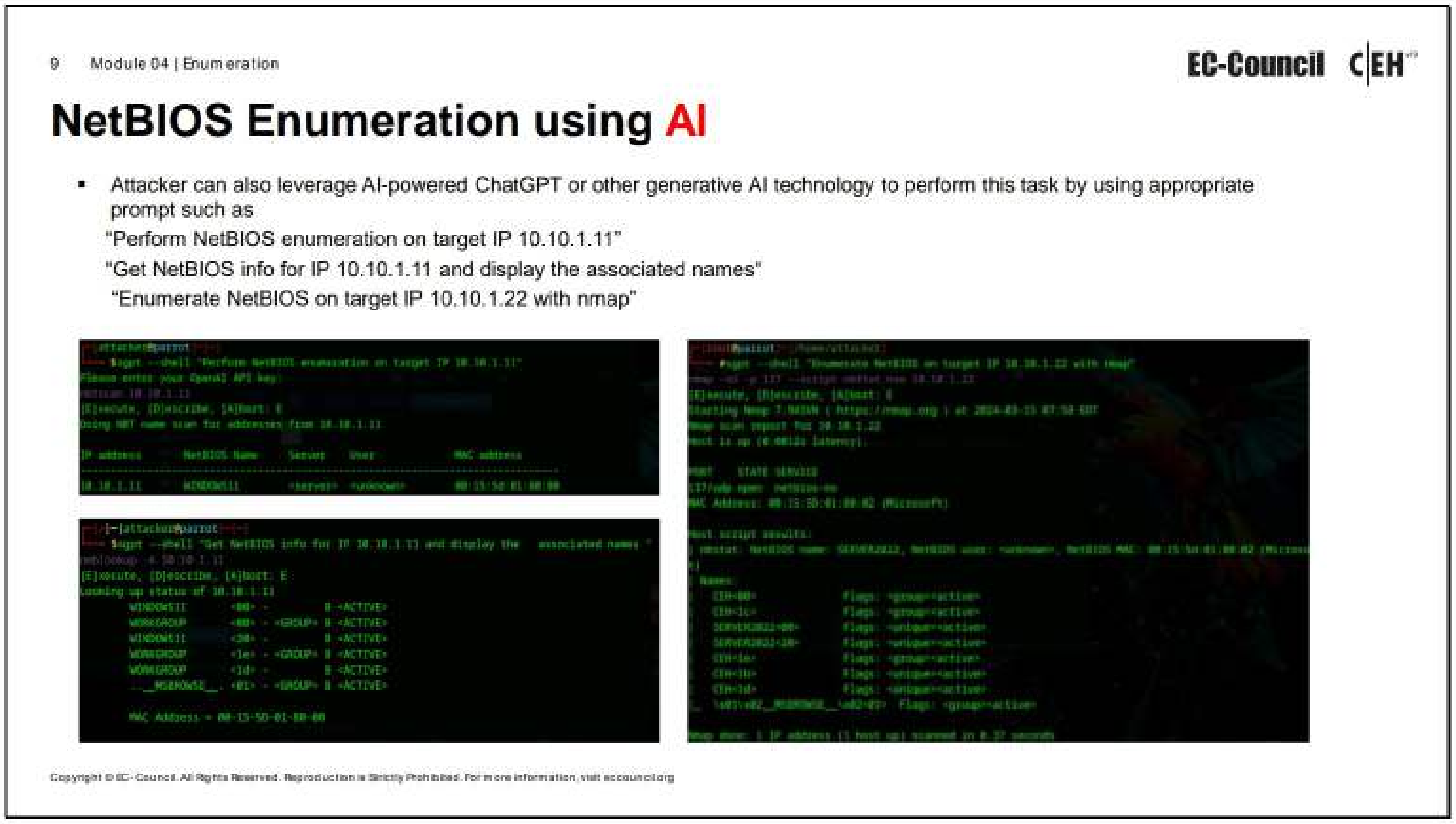
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The screenshot shows the shared resources available on the specified computer.



```
C:\Users\Administrator>net view \\10.10.1.22 /ALL
Shared resources at \\10.10.1.22



Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
ADMIN$      Disk           Remote Admin
C$          Disk           Default share
IPC$        IPC            Remote IPC
NETLOGON    Disk           Logon server share
SYSVOL      Disk           Logon server share
Users       Disk
The command completed successfully.


C:\Users\Administrator>
```

Figure 4.6: Output of Net View command



9 Module 04 | Enumeration

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"

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

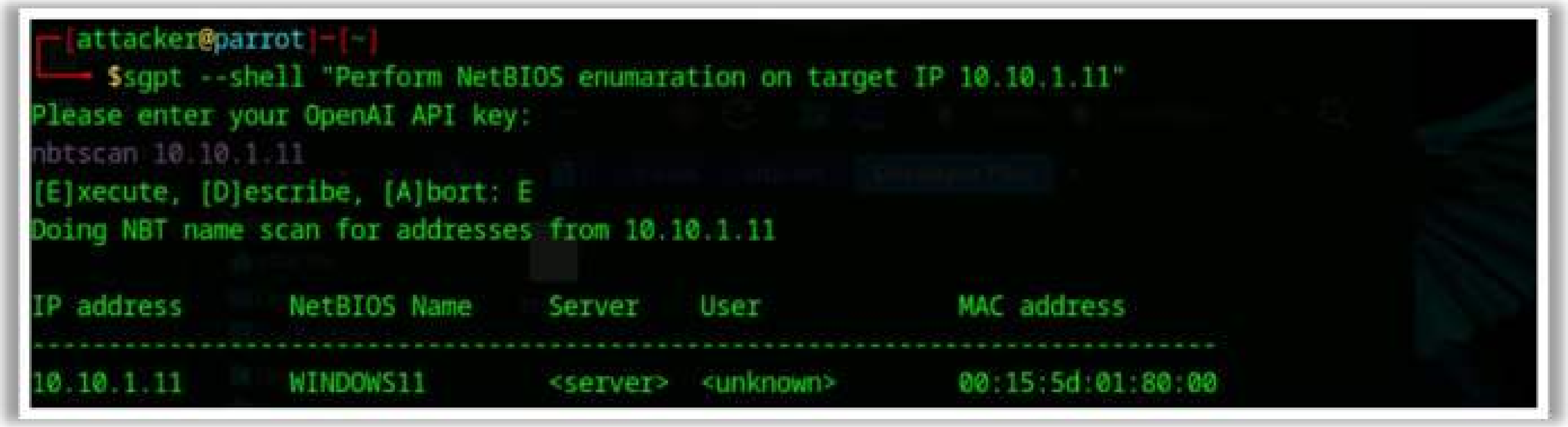
NetBIOS Enumeration using AI

Attackers can leverage AI-powered technologies to enhance and automate their network enumeration tasks. With the aid of AI, attackers can effortlessly perform NetBIOS enumeration to acquire NetBIOS information, associated names, and enumerate NetBIOS services on target IP addresses.

Attackers can use ChatGPT to perform this task by using appropriate prompts such as:

Example #1:

- **"Perform NetBIOS enumeration on target IP 10.10.1.11"**



```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --shell "Perform NetBIOS enumaration on target IP 10.10.1.11"
Please enter your OpenAI API key:
nbtscan 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Doing NBT name scan for addresses from 10.10.1.11

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
10.10.1.11       WINDOWS11        <server>  <unknown>        00:15:5d:01:80:00
```

Figure 4.7: Perform NetBIOS enumeration on target IP

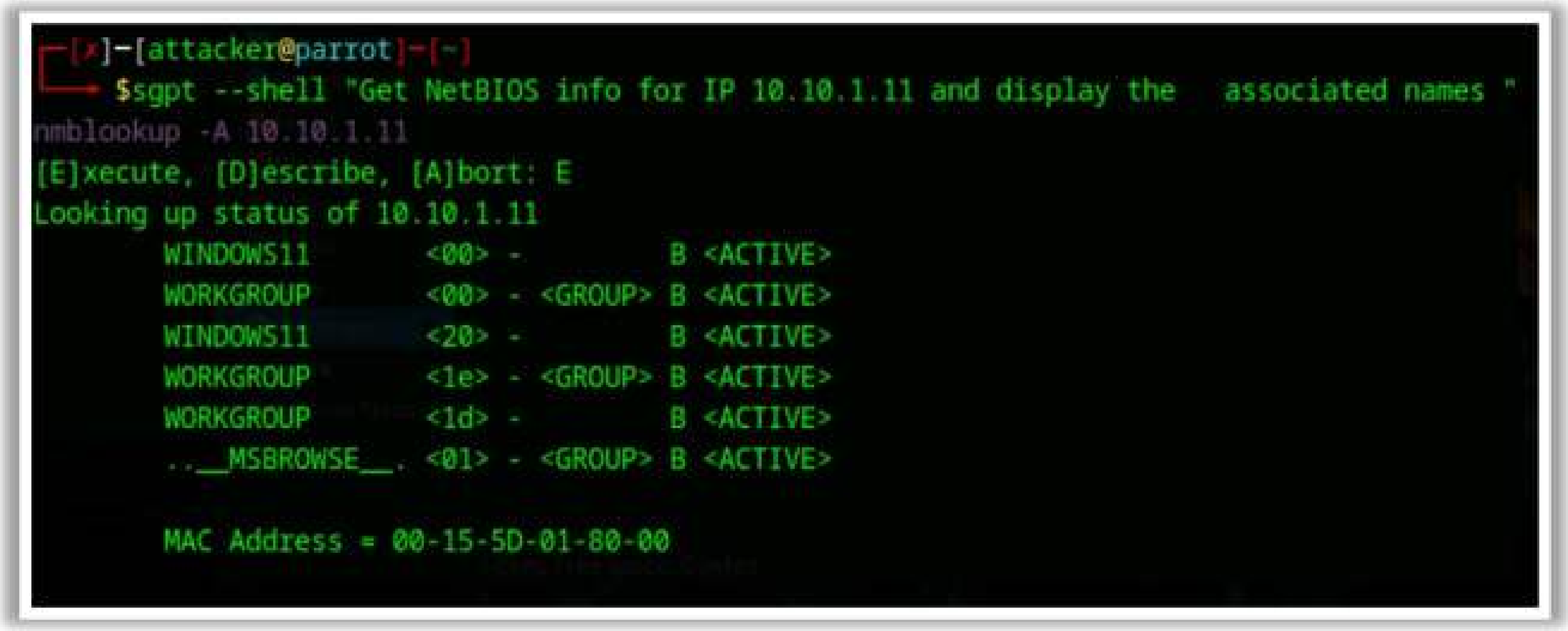
The following prompt is designed to automate NetBIOS enumeration on the specified target IPs:

`nbtscan 10.10.1.11`

The **`nbtscan`** command is used to perform NetBIOS enumeration on the target IP 10.10.1.11.

Example #2:

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



```
┌─[✗]─[attacker@parrot]─[~]
└──╼ $sgpt --shell "Get NetBIOS info for IP 10.10.1.11 and display the   associated names "
nmblookup -A 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Looking up status of 10.10.1.11
        WINDOWS11       <00> -         B <ACTIVE>
        WORKGROUP       <00> - <GROUP> B <ACTIVE>
        WINDOWS11       <20> -         B <ACTIVE>
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>
        WORKGROUP       <1d> -         B <ACTIVE>
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>

        MAC Address = 00-15-5D-01-80-00
```

Figure 4.8: Perform NetBIOS enumeration on target IP and display the names

The following prompt is designed to automate NetBIOS enumeration on the specified target IPs:

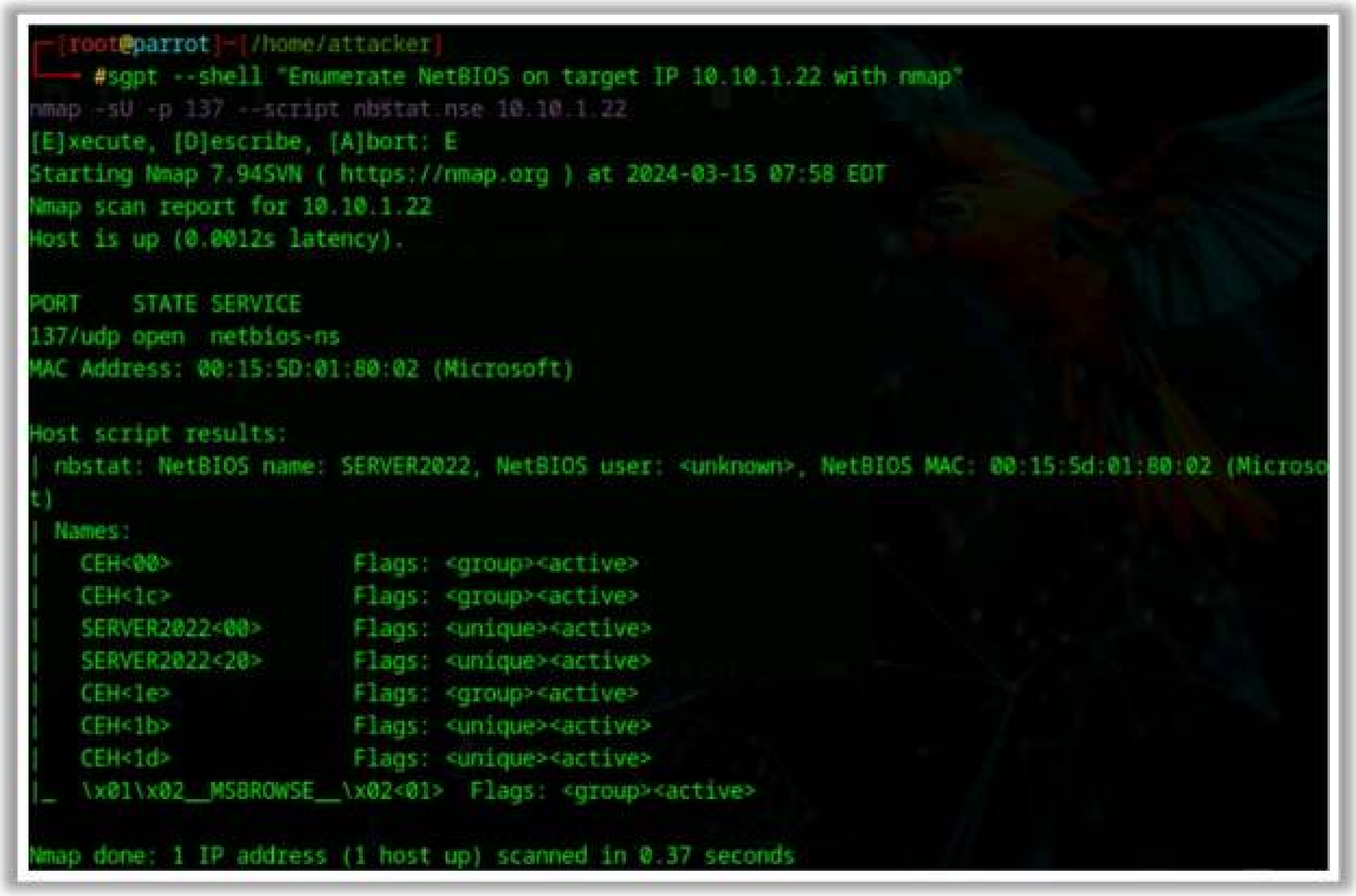
`nmblookup -A 10.10.1.11`

Explanation:

The `nmblookup` command with the `-A` option is used to get NetBIOS information for the target IP 10.10.1.11 and display the associated names.

Example #3:

- **"Enumerate NetBIOS on target IP 10.10.1.22 with nmap"**



```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --shell "Enumerate NetBIOS on target IP 10.10.1.22 with nmap"
nmap -sU -p 137 --script nbstat.nse 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 07:58 EDT
Nmap scan report for 10.10.1.22
Host is up (0.0012s latency).

PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Host script results:
| nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:01:80:02 (Microso
t)
| Names:
|   CEH<00>              Flags: <group><active>
|   CEH<1c>              Flags: <group><active>
|   SERVER2022<00>       Flags: <unique><active>
|   SERVER2022<20>       Flags: <unique><active>
|   CEH<1e>              Flags: <group><active>
|   CEH<1b>              Flags: <unique><active>
|   CEH<1d>              Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Figure 4.9: Perform NetBIOS enumeration on target IP with nmap

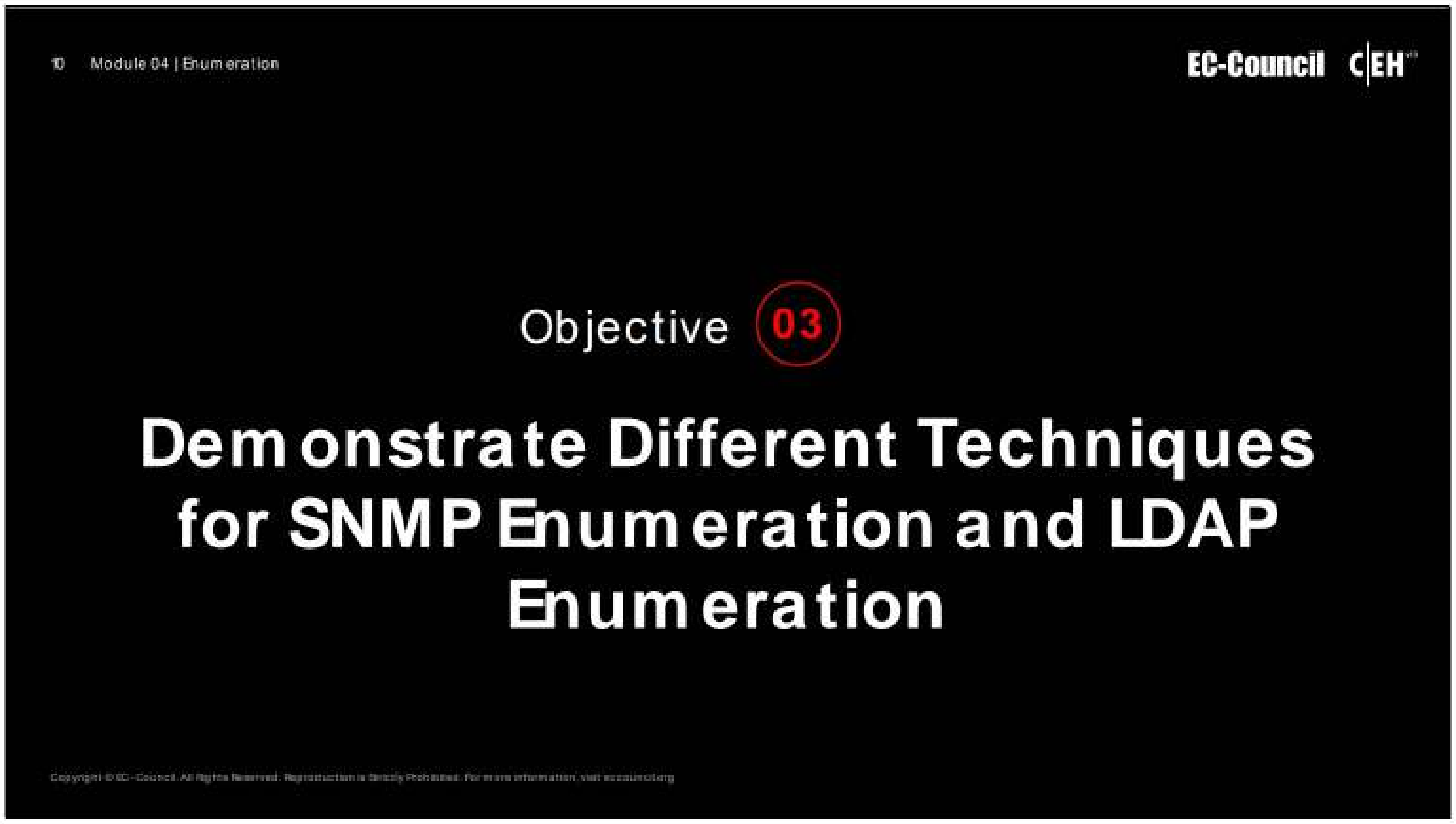
The following prompt is designed to automate NetBIOS enumeration on the specified target IPs:

```
nmap -sU -p 137 --script nbstat.nse 10.10.1.22
```

- The `nmap` command with specific options
- script (`nbstat.nse`) is used to enumerate NetBIOS services on the target IP 10.10.1.22.

These commands automate NetBIOS enumeration tasks and provide detailed information about NetBIOS services on the specified target IPs.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

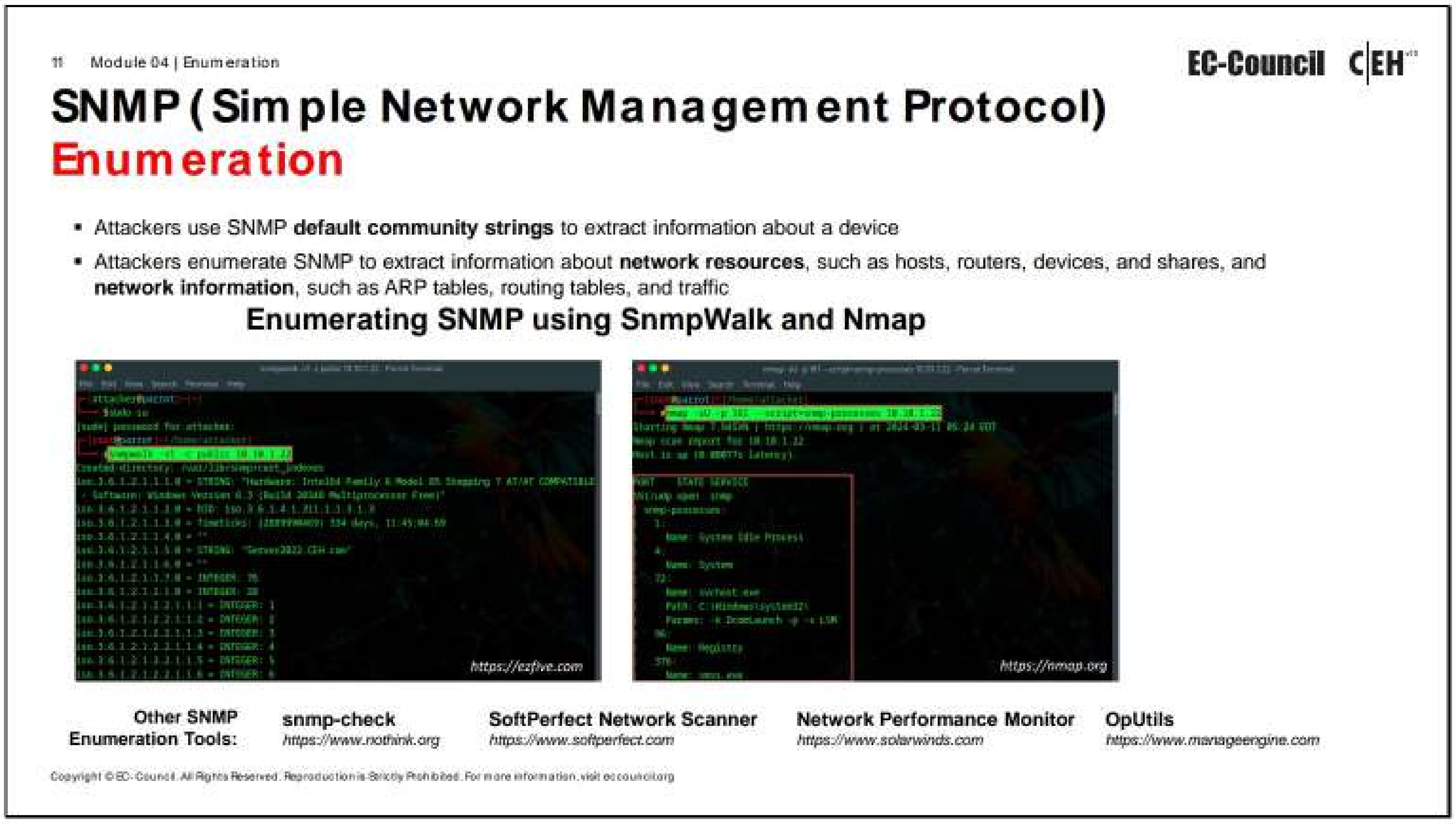


EC-Council C|EH

Objective 03

Demonstrate Different Techniques for SNMP Enumeration and LDAP Enumeration

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org



EC-Council C|EH

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

https://ezfive.com

https://nmap.org

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

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

SNMP Enumeration

Simple Network Management Protocol (SNMP) allows network administrators to manage network devices from a remote location. However, SNMP has many security vulnerabilities, such as a lack of auditing. Attackers may take advantage of these vulnerabilities to perform account and device enumeration. This section describes SNMP enumeration, the information extracted via SNMP enumeration, and various SNMP enumeration tools used to enumerate user accounts and devices on a target system.

SNMP is an application-layer protocol that runs on UDP and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on Windows and Unix networks on networking devices.

SNMP enumeration is the process of creating a list of the user's accounts and devices on a target computer using SNMP. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates with the agent.

Almost all the network infrastructure devices such as routers and switches contain an SNMP agent for managing the system or devices. The SNMP management station sends requests to the agent; after receiving the request, the agent replies. Both requests and replies are configuration variables accessible by the agent software. SNMP management stations send requests to set values to some variables. Traps let the management station know if an abnormal event such as a reboot or an interface failure has occurred at the agent's side.

SNMP contains the following two passwords for configuring and accessing the SNMP agent from the management station.

- **Read Community String**
    - The configuration of the device or system can be viewed with the help of this password.
    - These strings are public.
- **Read/Write Community String**
    - The device configuration can be changed or edited using this password.
    - These strings are private.

When administrators leave the community strings at the default setting, attackers can use these default community strings (passwords) for changing or viewing the configuration of the device or system. Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, and shares as well as network information such as ARP tables, routing tables, device-specific information, and traffic statistics.

Commonly used SNMP enumeration tools include OpUtils (*https://www.manageengine.com*) and Network Performance Monitor (https://www.solarwinds.com).

Working of SNMP

SNMP uses a disturbed architecture comprising SNMP managers, SNMP agents, and several related components. The communication process between an SNMP manager and SNMP agent is as follows.

1. **Initialization**
   - **Start-Up**

     When a network device boots up, the SNMP agent on the device initializes its configuration and prepares to communicate with the SNMP manager by listening on the designated port (usually UDP port 161).

2. **Discovery**
   - **Manager Discovers Agents**

     The SNMP manager discovers SNMP-enabled devices on the network by sending a request to the broadcast address or specific IP addresses where agents are known to reside.

3. **Information Exchange**

   The communication between an SNMP manager and agent involves several types of operations, primarily using SNMP messages called Protocol Data Units (PDUs). The key operations include:

   a. **Get Request**

   The SNMP manager sends a Get Request to an SNMP agent to retrieve the value of a specific variable, such as the status of a router interface or the bandwidth usage on a network link.

   b. **GetNext Request**

   This request is used to fetch the next variable in the MIB (Management Information Base) tree. It allows the manager to query a sequence of variables without knowing their exact names.

   c. **Set Request**

   The SNMP manager uses Set Requests to modify the value of a variable in the agent's MIB, effectively changing the configuration or behavior of the network device.

   d. **GetBulk Request**

   Introduced in SNMPv2, this operation allows the retrieval of large volumes of data with a single request, improving efficiency over multiple GetNext Requests.

   e. **Response**

   After receiving a Get, GetNext, Set, or GetBulk request, the SNMP agent processes the request, performs the necessary actions, and sends back a Response PDU containing the requested values or an acknowledgment of the action taken.

All Rights Reserved. Reproduction is Strictly Prohibited.

f. Inform Request

An SNMP agent uses Inform Requests to send unsolicited information to the SNMP manager, usually about significant events or errors. This mechanism is used for manager-to-manager communication as well.

g. Trap

Traps are unsolicited messages sent from an SNMP agent to the manager to alert it of significant events or changes in the network, such as a device reboot or a link failure. SNMPv3 introduced the concept of Notifications, which encompasses both Traps and Informs, adding authentication and encryption.

4. Monitoring and Management

The SNMP manager uses the information collected from SNMP agents to monitor network performance, detect and diagnose issues, and configure network devices remotely. This ongoing process involves regular polling (sending Get Requests) and listening for Traps or Inform Requests from agents.

Management Information Base (MIB)

MIB is a virtual database containing a formal description of all the network objects that SNMP manages. It is a collection of hierarchically organized information. It provides a standard representation of the SNMP agent's information and storage. MIB elements are recognized using object identifiers (OIDs). An OID is the numeric name given to an object and begins with the root of the MIB tree. The OID can uniquely identify the object in the MIB hierarchy.

MIB-managed objects include scalar objects, which define a single object instance, and tabular objects, which define a group of related object instances. OIDs include the object's type (such as counter, string, or address), access level (such as read or read/write), size restrictions, and range information. The SNMP manager converts the OIDs into a human-readable display using the MIB as a codebook.

A user can access the contents of the MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. For example, http://IP.Address/Lseries.mib or http://library_name/Lseries.mib.Microsoft provides the list of MIBs that are installed with the SNMP service in the Windows resource kit. The major MIBs are .as follows:

- **DHCP.MIB**: Monitors network traffic between DHCP servers and remote hosts
- **HOSTMIB.MIB**: Monitors and manages host resources
- **LNMIB2.MIB**: Contains object types for workstation and server services
- **MIB_II.MIB:** Manages TCP/IP-based Internet using a simple architecture and system
- **WINS.MIB**: For the Windows Internet Name Service (WINS)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerating SNMP using SnmpWalk

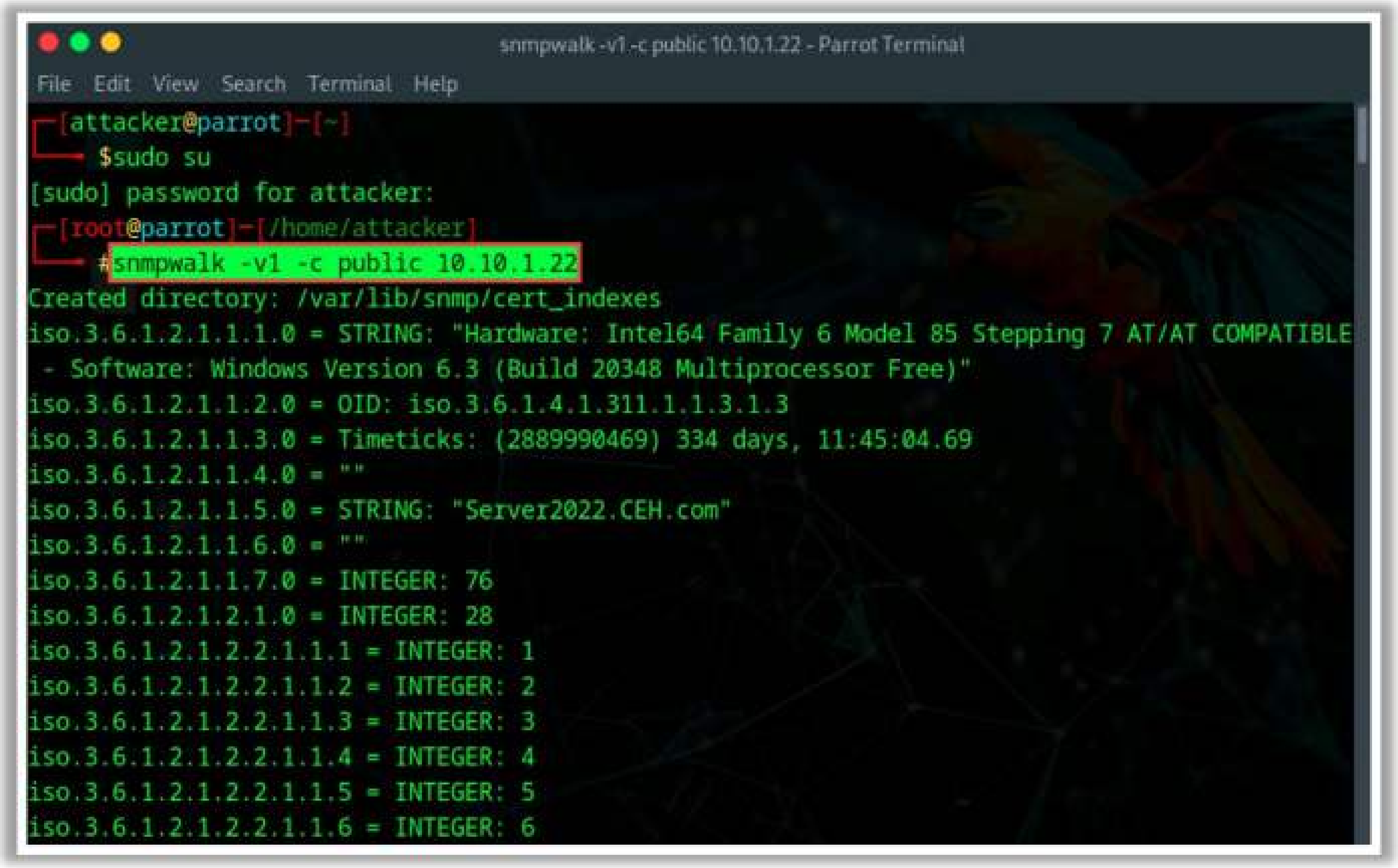
Source: *https://ezfive.com*

SnmpWalk is a command-line tool that allows attackers to scan numerous Simple Network Management Protocol (SNMP) nodes instantly and identify a set of variables that are available for accessing the target network. Using this tool, attackers target the root node so that information from all the sub-nodes such as routers and switches can be fetched. The information can be retrieved in the form of an object identifier (OID), which is part of the management information base (MIB) associated with the devices having SNMP enabled.

Attackers execute the following command to retrieve SNMP information from the target device:

```
snmpwalk -v1 -c public <Target IP Address>
```

The above command allows attackers to view all the OIDs, variables, and other associated information. Using this command, attackers can also retrieve all the data in transit to the SNMP server from the SNMP agent, including the server being used, user credentials, and other parameters.


snmpwalk -v1 -c public 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #snmpwalk -v1 -c public 10.10.1.22
Created directory: /var/lib/snmp/cert_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE
 - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (2889990469) 334 days, 11:45:04.69
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "Server2022.CEH.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 28
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
```

Figure 4.10: Screenshot of SnmpWalk

Other SnmpWalk Commands:

- Command to enumerate SNMPv2 with a community string of public:

  `snmpwalk -v2c -c public <Target IP Address>`

- Command to search for installed software:

  `snmpwalk -v2c -c public <Target IP Address> hrSWInstalledName`

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Command to determine the amount of RAM on the host:

  `snmpwalk -v2c -c public <Target IP Address> hrMemorySize`

- Command to change an OID to a different value:

  `snmpwalk -v2c -c public <Target IP Address> <OID> <New Value>`

- Command to change the sysContact OID:

  `snmpwalk -v2c -c public <Target IP Address> sysContact <New Value>`

Enumerating SNMP using Nmap

Source: *https://nmap.org*

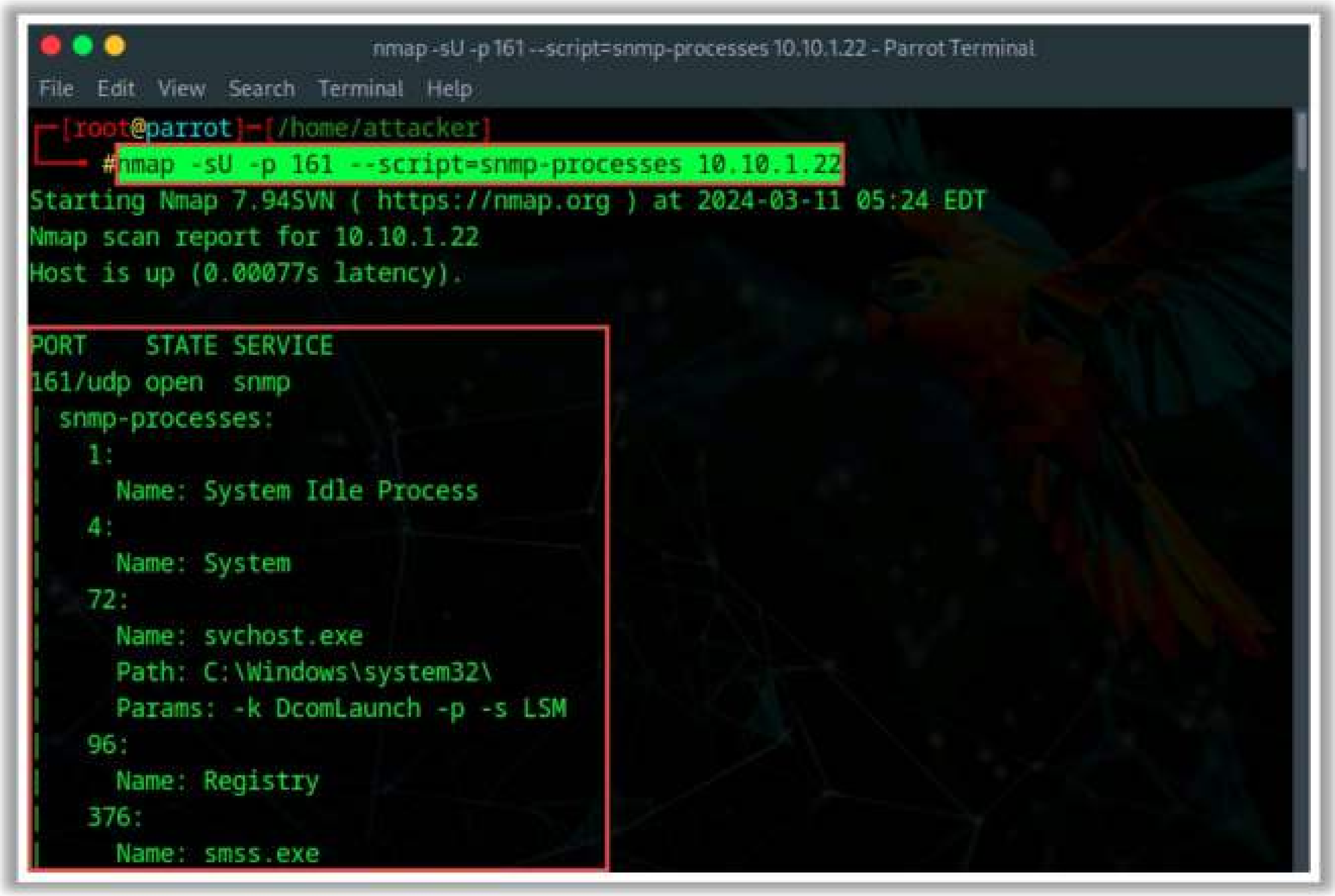
Attackers use the **`snmp-processes`** Nmap Scripting Engine (NSE) script against an SNMP remote server to retrieve information related to the hosted SNMP services.

```
nmap -sU -p 161 --script=snmp-processes <Target IP Address>
```

The above Nmap command, when executed, retrieves a list of all the running SNMP processes along with the associated ports on the target host.

Other Nmap commands to perform SNMP enumeration:

- **`nmap -sU -p 161 --script=snmp-sysdescr <Target IP Address>`** → Retrieves information regarding SNMP server type and operating system details.
- **`nmap -sU -p 161 --script=snmp-win32-software <Target IP Address>`** → Retrieves a list of all the applications running on the target machine.


nmap -sU -p 161 --script=snmp-processes 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -sU -p 161 --script=snmp-processes 10.10.1.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 05:24 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00077s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-processes:
|   1:
|     Name: System Idle Process
|   4:
|     Name: System
|   72:
|     Name: svchost.exe
|     Path: C:\Windows\system32\
|     Params: -k DcomLaunch -p -s LSM
|   96:
|     Name: Registry
|   376:
|     Name: smss.exe
```

Figure 4.11: Screenshot of Nmap using the snmp-processes NSE script

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SNMP Enumeration Tools

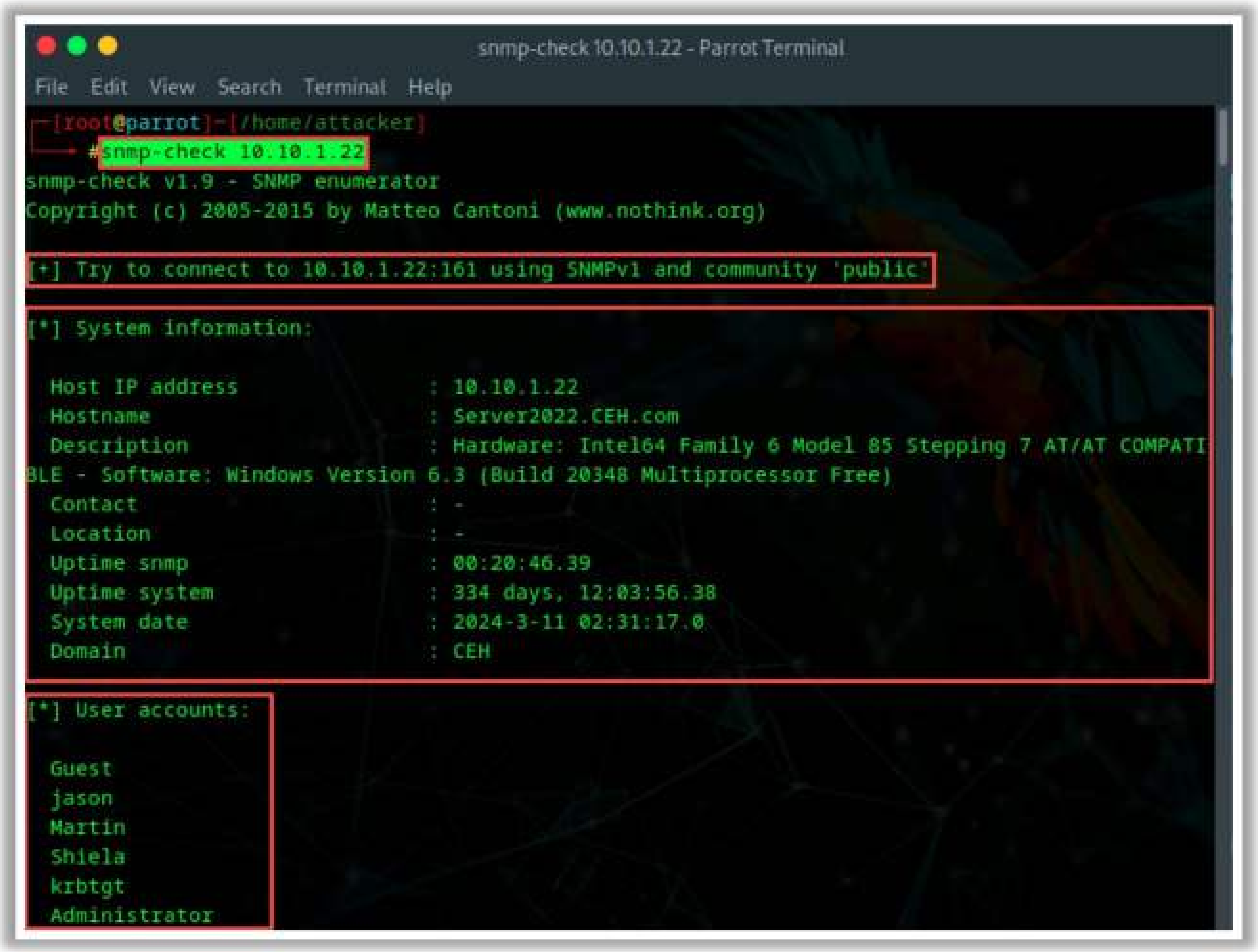
SNMP enumeration tools are used to scan a single IP address or a range of IP addresses of SNMP-enabled network devices to monitor, diagnose, and troubleshoot security threats.

- **snmp-check (snmp_enum Module)**

  Source: *https://www.nothink.org*

  snmp-check is an open-source tool distributed under the GNU General Public License (GPL). Its goal is to automate the process of gathering information on any device with SNMP support (Windows, Unix-like, network appliances, printers, etc.). snmp-check allows the enumeration of SNMP devices and places the output in a human-readable and user-friendly format. It could be useful for penetration testing or systems monitoring.

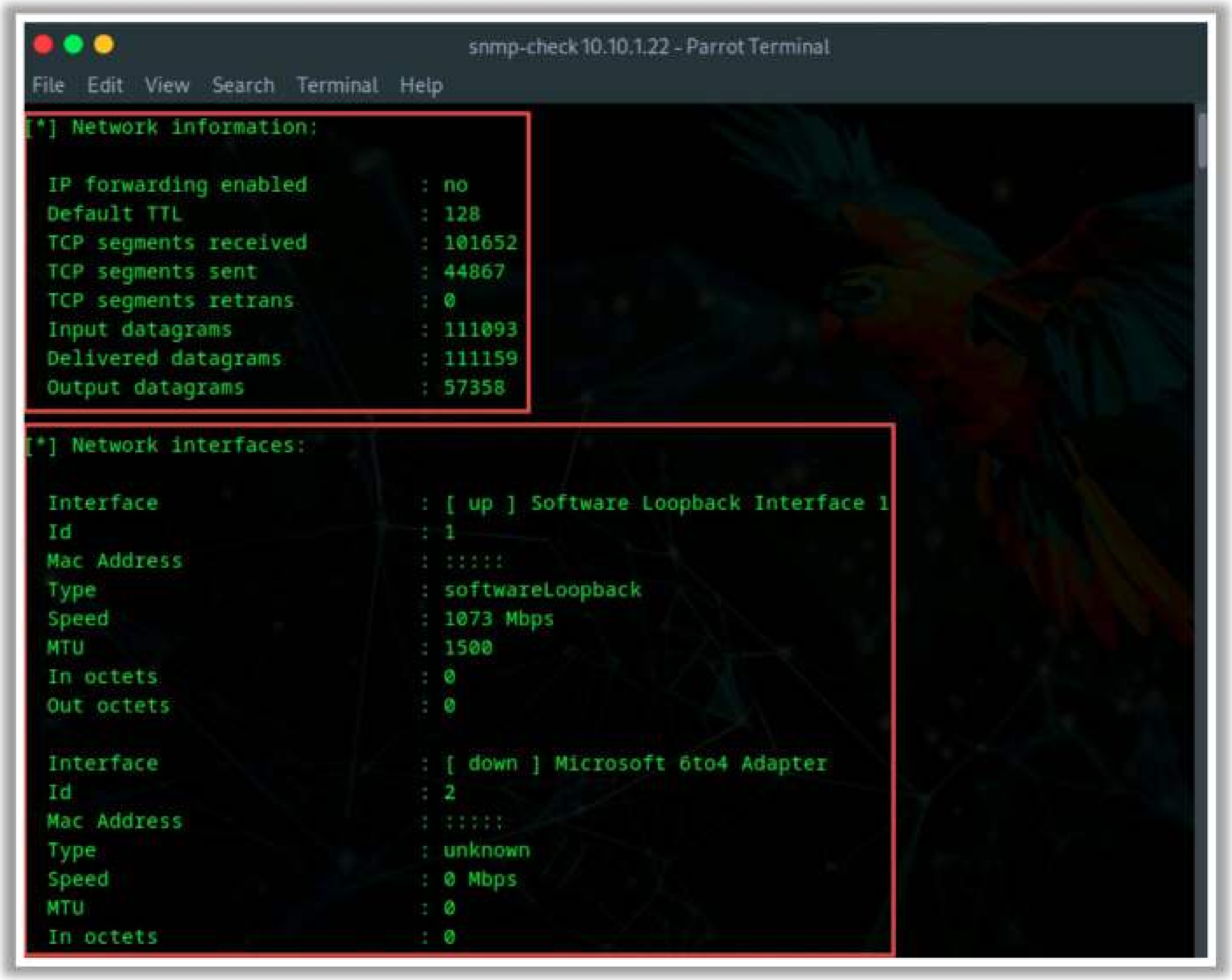
  Attackers use this tool to gather information about the target, such as contact, description, write access, devices, domain, hardware and storage information, hostname, Internet Information Services (IIS) statistics, IP forwarding, listening UDP ports, location, mountpoints, network interfaces, network services, routing information, software components, system uptime, TCP connections, total memory, uptime, and user accounts.


snmp-check 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[/home/attacker]
└──╼ #snmp-check 10.10.1.22
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.10.1.22:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 10.10.1.22
  Hostname                      : Server2022.CEH.com
  Description                   : Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATI
BLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)
  Contact                       : -
  Location                      : -
  Uptime snmp                   : 00:20:46.39
  Uptime system                 : 334 days, 12:03:56.38
  System date                   : 2024-3-11 02:31:17.0
  Domain                        : CEH

[*] User accounts:

  Guest
  jason
  Martin
  Shiela
  krbtgt
  Administrator
```

Figure 4.12: Screenshot of snmp-check showing system information and user accounts

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.


snmp-check 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help

```
[*] Network information:

  IP forwarding enabled         : no
  Default TTL                   : 128
  TCP segments received         : 101652
  TCP segments sent             : 44867
  TCP segments retrans          : 0
  Input datagrams               : 111093
  Delivered datagrams           : 111159
  Output datagrams              : 57358

[*] Network interfaces:

  Interface                     : [ up ] Software Loopback Interface 1
  Id                            : 1
  Mac Address                   : :::::
  Type                          : softwareLoopback
  Speed                         : 1073 Mbps
  MTU                           : 1500
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ down ] Microsoft 6to4 Adapter
  Id                            : 2
  Mac Address                   : :::::
  Type                          : unknown
  Speed                         : 0 Mbps
  MTU                           : 0
  In octets                     : 0
```

Figure 4.13: Screenshot of snmp-check showing network information and interfaces

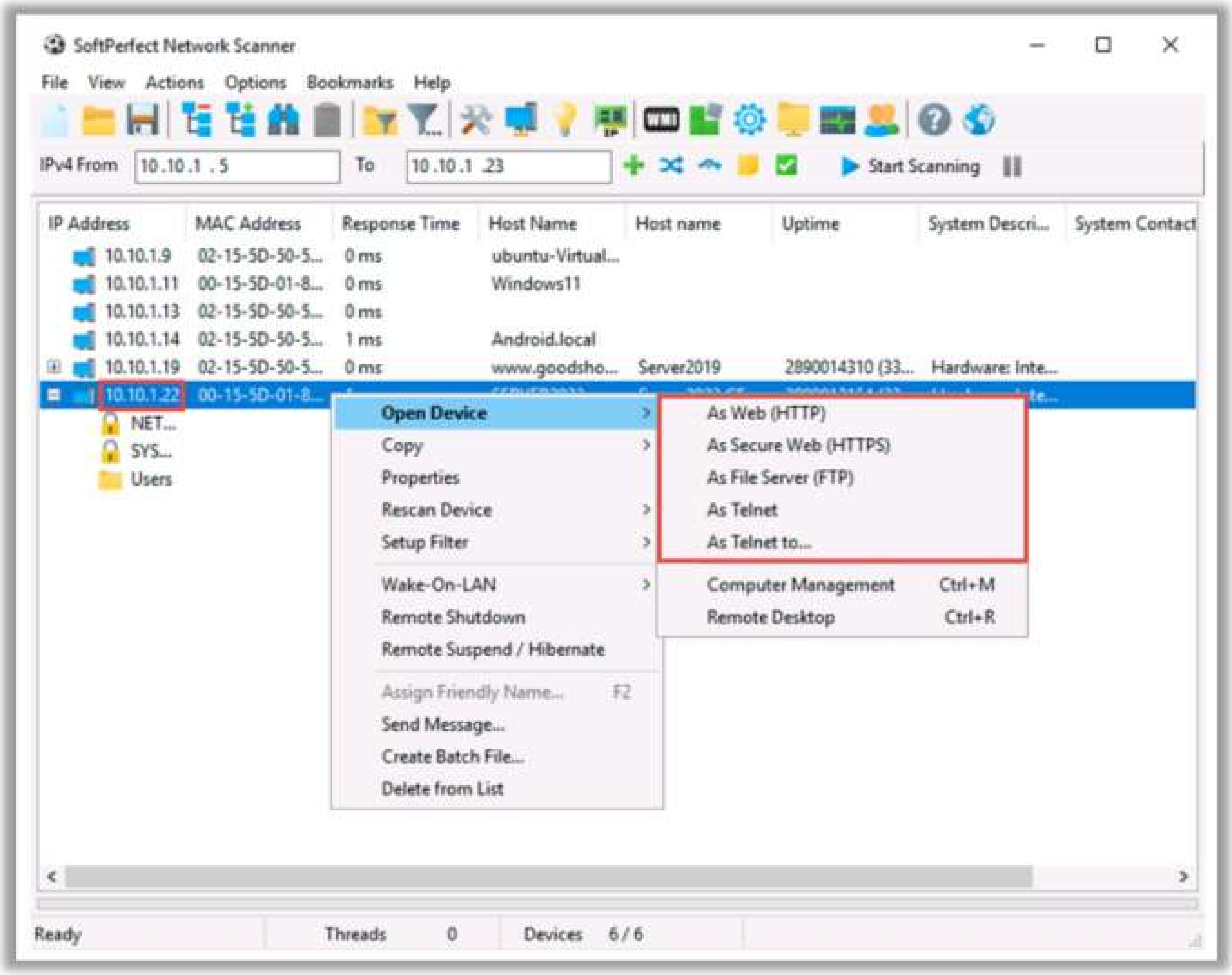
- **SoftPerfect Network Scanner**

  Source: *https://www.softperfect.com*

  SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices via Windows Management Instrumentation (WMI), SNMP, Hypertext Transfer Protocol (HTTP), SSH, and PowerShell. It also scans for remote services, registry, files, and performance counters; offers flexible filtering and display options; and exports NetScan results to a variety of formats ranging from Extensible Markup Language (XML) to JavaScript Object Notation (JSON).

  Moreover, SoftPerfect Network Scanner can check for a user-defined port and report if one is open. In addition, it can resolve host names and auto-detect the local and external IP range. It supports remote shutdown and Wake-on-LAN.

  Attackers uses this tool to gather information about a shared folder and network devices.



IPv4 From 10.10.1.5 To 10.10.1.23

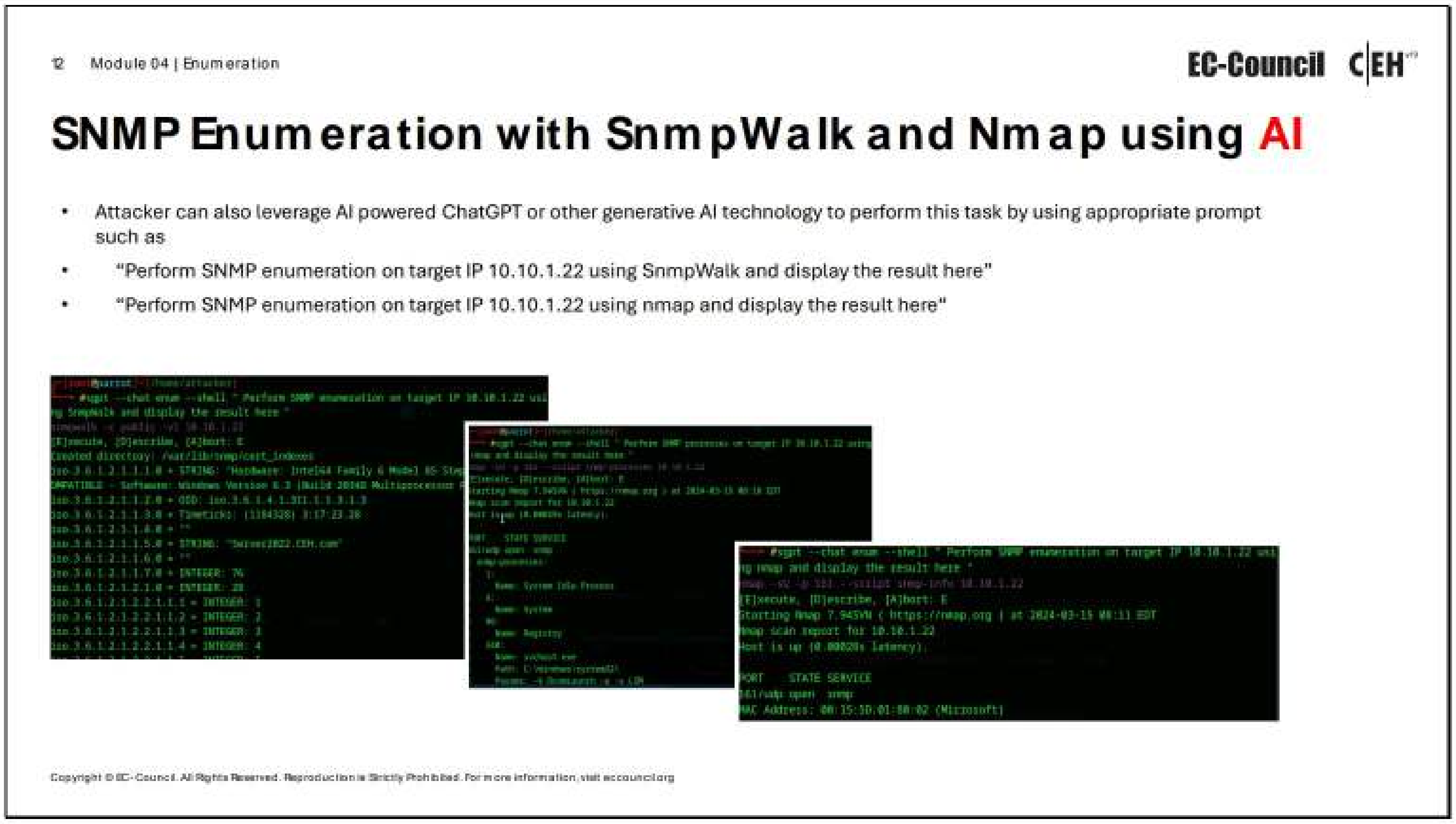
IP Address	MAC Address	Response Time	Host Name	Host name	Uptime	System Descri...	System Contact
10.10.1.9	02-15-5D-50-5...	0 ms	ubuntu-Virtual...				
10.10.1.11	00-15-5D-01-8...	0 ms	Windows11				
10.10.1.13	02-15-5D-50-5...	0 ms					
10.10.1.14	02-15-5D-50-5...	1 ms	Android.local				
10.10.1.19	02-15-5D-50-5...	0 ms	www.goodsho...	Server2019	2890014310 (33...	Hardware: Inte...	
10.10.1.22	00-15-5D-01-8...						

Ready Threads 0 Devices 6 / 6

Figure 4.14: Screenshot of SoftPerfect Network Scanner

The following are some additional SNMP enumeration tools:

- Network Performance Monitor (*https://www.solarwinds.com*)
- OpUtils (*https://www.manageengine.com*)
- PRTG Network Monitor (*https://www.paessler.com*)
- Engineer's Toolset (*https://www.solarwinds.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"

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

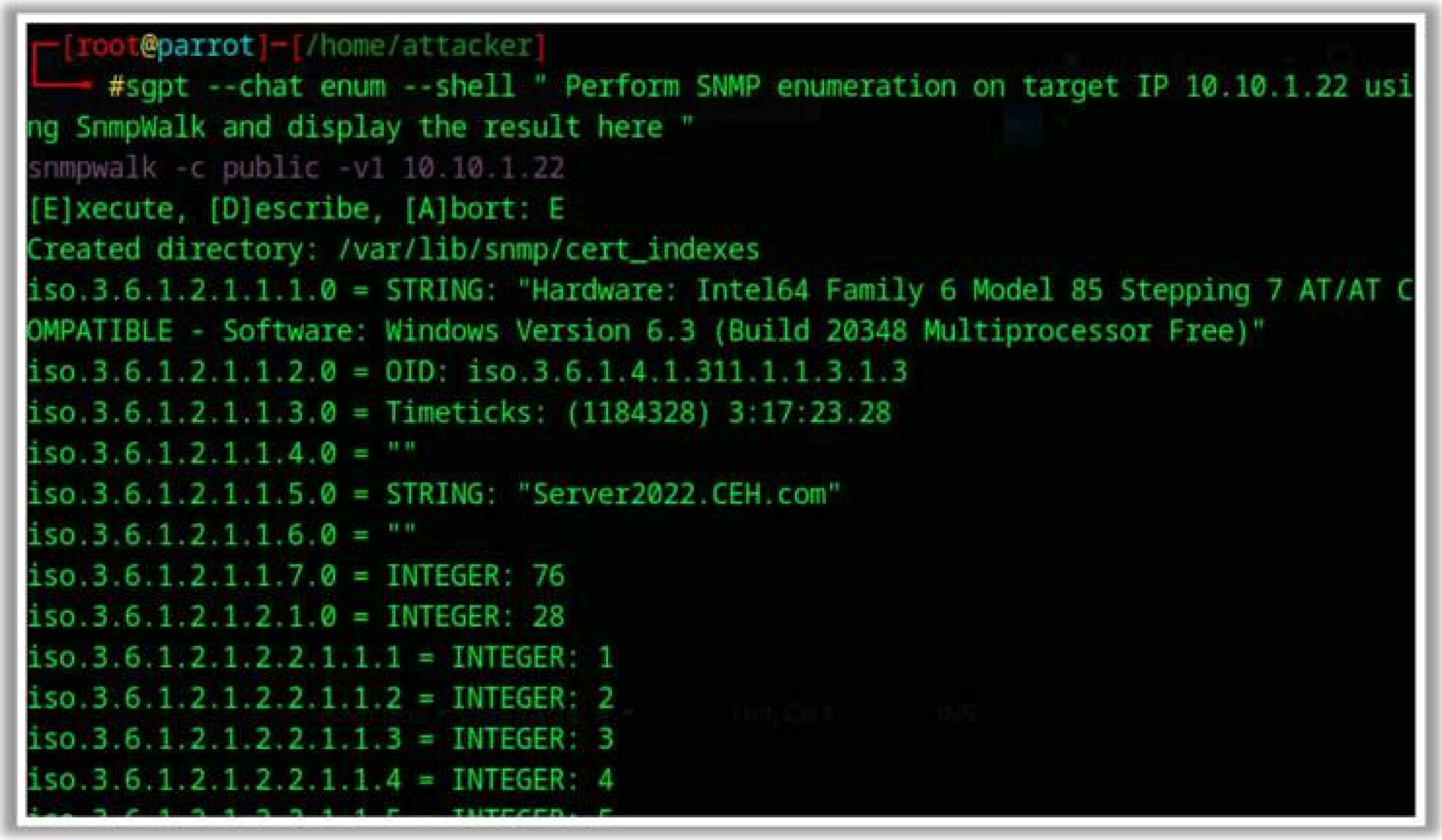
SNMP Enumeration with SnmpWalk and Nmap using AI

Attackers can leverage AI-powered technologies to enhance and automate their network enumeration tasks. With the aid of AI, attackers can effortlessly perform SNMP enumeration and gather SNMP information and processes on target IP addresses.

Attackers can use ChatGPT to perform this task by using appropriate prompts such as:

Example #1:

- **"Perform SNMP enumeration on target IP 10.10.1.22 using SnmpWalk and display the result here".**



```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat enum --shell " Perform SNMP enumeration on target IP 10.10.1.22 usi
ng SnmpWalk and display the result here "
snmpwalk -c public -v1 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Created directory: /var/lib/snmp/cert_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT C
OMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (1184328) 3:17:23.28
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "Server2022.CEH.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 28
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
```

Figure 4.15: Perform SNMP enumeration on target IP using SnmpWalk

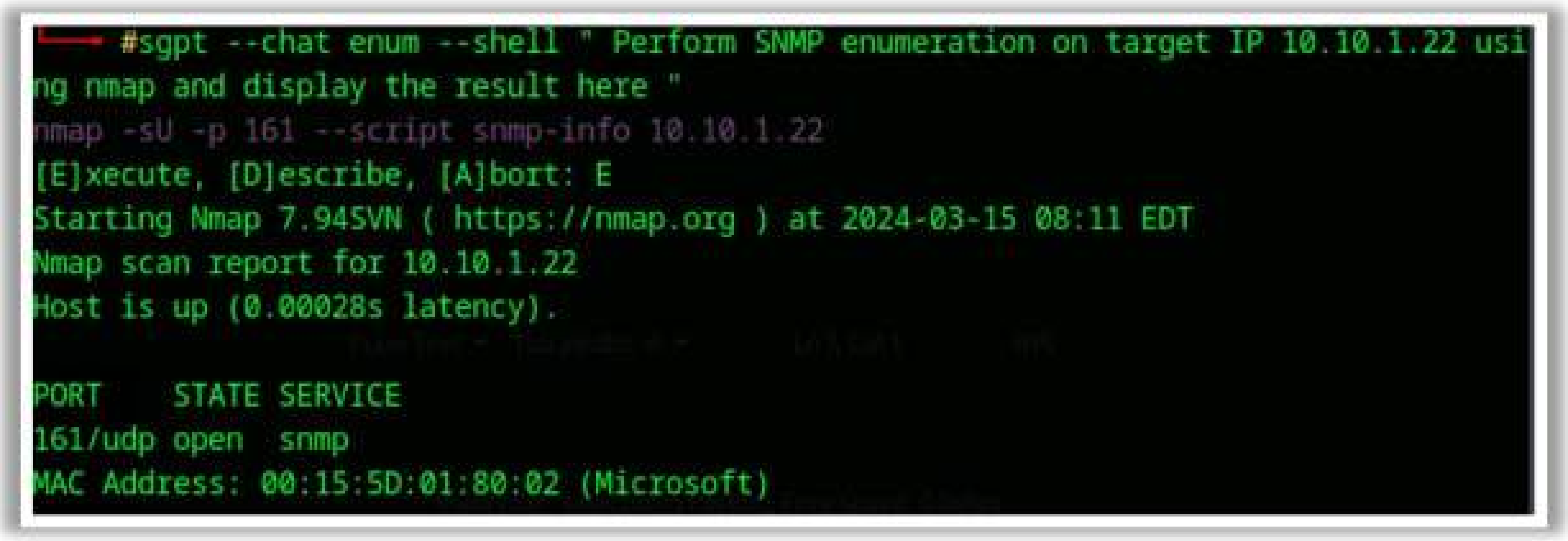
The following command is designed to automate SNMP enumeration tasks on the specified target IP:

```
snmpwalk -c public -v1 10.10.1.22
```

The `snmpwalk` command is used to perform SNMP enumeration on the target IP 10.10.1.22 using SnmpWalk.

Example #2:

- **"Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here".**



```
└──╼ #sgpt --chat enum --shell " Perform SNMP enumeration on target IP 10.10.1.22 usi
ng nmap and display the result here "
nmap -sU -p 161 --script snmp-info 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:11 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00028s latency).

PORT    STATE SERVICE
161/udp open  snmp
MAC Address: 00:15:5D:01:80:02 (Microsoft)
```

Figure 4.16: Perform SNMP enumeration on target IP using Nmap

The following command is designed to automate SNMP enumeration tasks on the specified target IP:

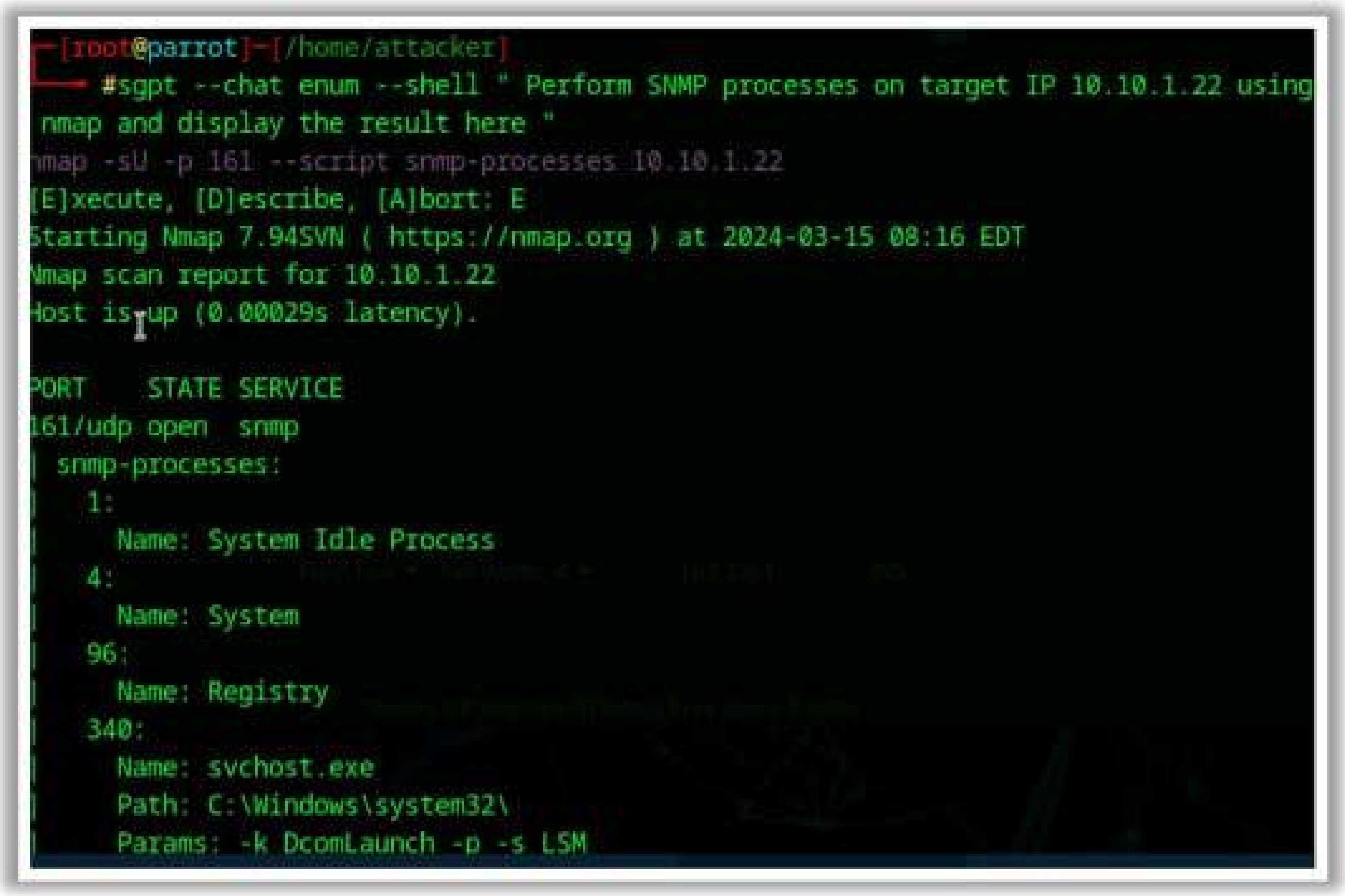
```
nmap -sU -p 161 --script snmp-info 10.10.1.22
```

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The `nmap` command with specific options and script (`snmp-info`) is used to perform SNMP enumeration on the target IP 10.10.1.22 using nmap.

Example #3:

- **"Perform SNMP processes on target IP 10.10.1.22 using nmap and display the result here".**



```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat enum --shell " Perform SNMP processes on target IP 10.10.1.22 using
 nmap and display the result here "
nmap -sU -p 161 --script snmp-processes 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:16 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00029s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-processes:
|   1:
|     Name: System Idle Process
|   4:
|     Name: System
|   96:
|     Name: Registry
|   340:
|     Name: svchost.exe
|     Path: C:\Windows\system32\
|     Params: -k DcomLaunch -p -s LSM
```

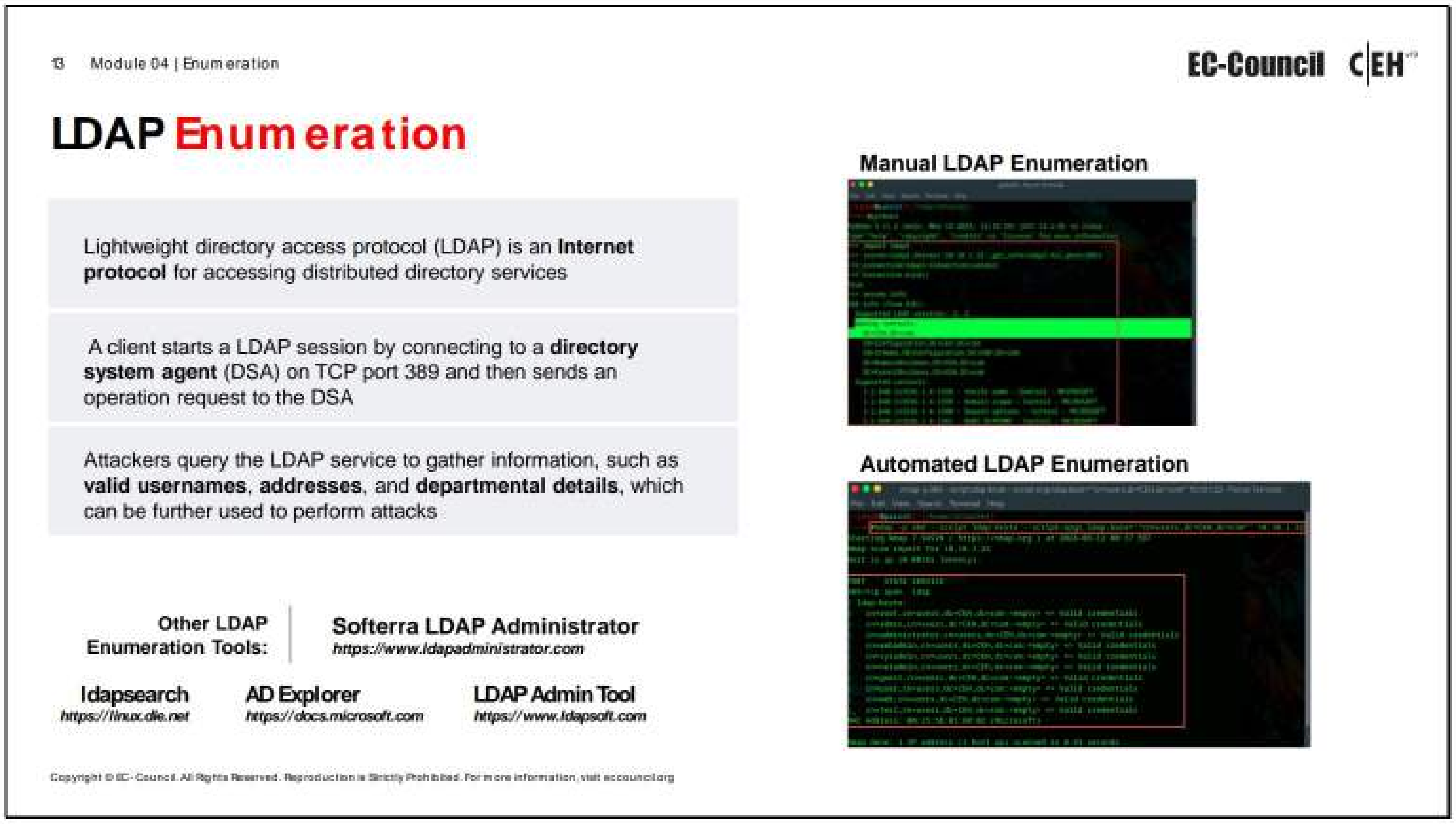
Figure 4.17: Perform SNMP processes on target IP

The following command is designed to automate SNMP enumeration tasks on the specified target IP:

```
nmap -sU -p 161 --script snmp-processes 10.10.1.22
```

Another `nmap` command with specific options and script (`snmp-processes`) is used to perform SNMP processes on the target IP 10.10.1.22 using nmap.

These commands automate SNMP enumeration tasks and display the results for each command executed on the specified target IP 10.10.1.22.



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

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

LDAP Enumeration

Various protocols enable communication and manage data transfer between network resources. All these protocols carry valuable information about network resources along with the data. An external user who successfully enumerates that information by manipulating the protocols can break into the network and may misuse the network resources. The Lightweight Directory Access Protocol (LDAP) is one such protocol that accesses the directory listings. This section focuses on LDAP enumeration, the information extracted via LDAP enumeration, and LDAP enumeration tools.

LDAP is an Internet protocol for accessing distributed directory services. LDAP accesses directory listings within Active Directory or from other directory services. LDAP is a hierarchical or logical form of a directory, similar to a company's organizational chart. Directory services may provide any organized set of records, often in a hierarchical and logical structure, such as a corporate email directory. It uses DNS for quick lookups and the fast resolution of queries. A client starts an LDAP session by connecting to a Directory System Agent (DSA), typically on TCP port 389, and sends an operation request to the DSA. The Basic Encoding Rules (BER) format is used to transmit information between the client and server.

An attacker can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names, which an attacker can use to launch attacks.

Manual and Automated LDAP Enumeration

Attackers can use both manual and automated approaches for LDAP enumeration. Some of the commands that can be used for LDAP enumeration are as follows.

Manual LDAP Enumeration

Attackers can perform manual LDAP enumeration using Python. Follow the steps given below to perform manual LDAP enumeration using Python.

1. Using Nmap, check whether the target LDAP server is listening on port 389 for LDAP and port 636 for secure LDAP.
2. If the target server is listening on the specified ports, initiate the enumeration process by installing LDAP using the following command:

   ```
   pip3 install ldap3
   ```

3. As shown in the code given below, create a server object (`server`), specify the target IP address or hostname and port number. If the target server is listening on secure LDAP, specify `use_ssl = True`.
4. Retrieve the Directory System Agent (DSA)–specific entry (DSE) naming contexts by specifying `get_info = ldap3.ALL`.
5. Now, create a connection object, `connection`, and initiate a call to `bind()`.
6. If the connection is successful, `True` is displayed on the screen as follows:

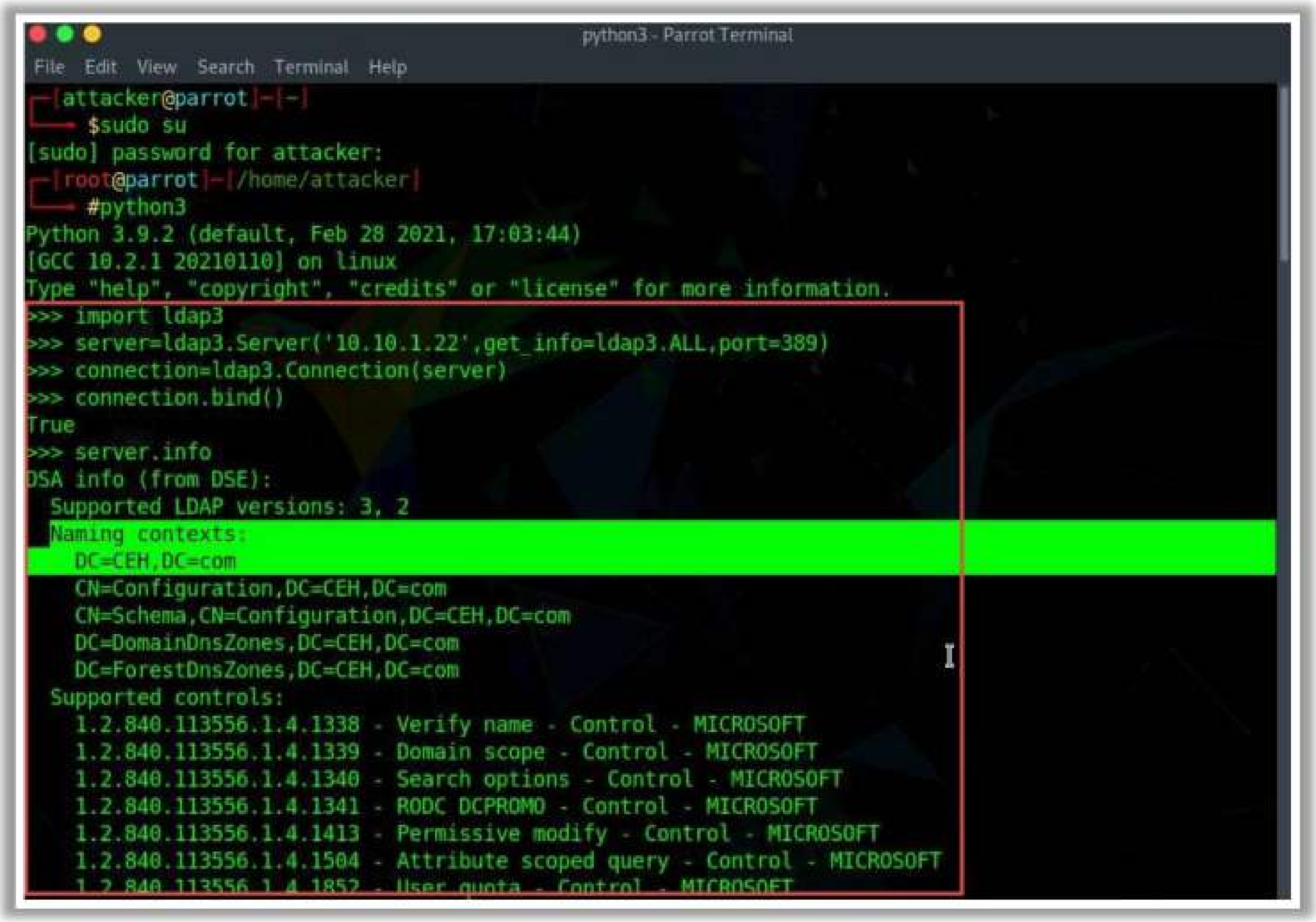
   ```
   >>> import ldap3
   >>> server = ldap3.Server('Target IP Address', get_info = ldap3.ALL, port =389)
   >>> connection = ldap3.Connection(server)
   >>> connection.bind()
   True
   ```

7. Now, one can fetch information such as the domain name and naming context using the following script:

   ```
   >>> server.info
   ```

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24



python3 - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import ldap3
>>> server=ldap3.Server('10.10.1.22',get_info=ldap3.ALL,port=389)
>>> connection=ldap3.Connection(server)
>>> connection.bind()
True
>>> server.info
DSA info (from DSE):
  Supported LDAP versions: 3, 2
  Naming contexts:
    DC=CEH,DC=com
    CN=Configuration,DC=CEH,DC=com
    CN=Schema,CN=Configuration,DC=CEH,DC=com
    DC=DomainDnsZones,DC=CEH,DC=com
    DC=ForestDnsZones,DC=CEH,DC=com
  Supported controls:
    1.2.840.113556.1.4.1338 - Verify name - Control - MICROSOFT
    1.2.840.113556.1.4.1339 - Domain scope - Control - MICROSOFT
    1.2.840.113556.1.4.1340 - Search options - Control - MICROSOFT
    1.2.840.113556.1.4.1341 - RODC DCPROMO - Control - MICROSOFT
    1.2.840.113556.1.4.1413 - Permissive modify - Control - MICROSOFT
    1.2.840.113556.1.4.1504 - Attribute scoped query - Control - MICROSOFT
    1.2.840.113556.1.4.1852 - User quota - Control - MICROSOFT
```

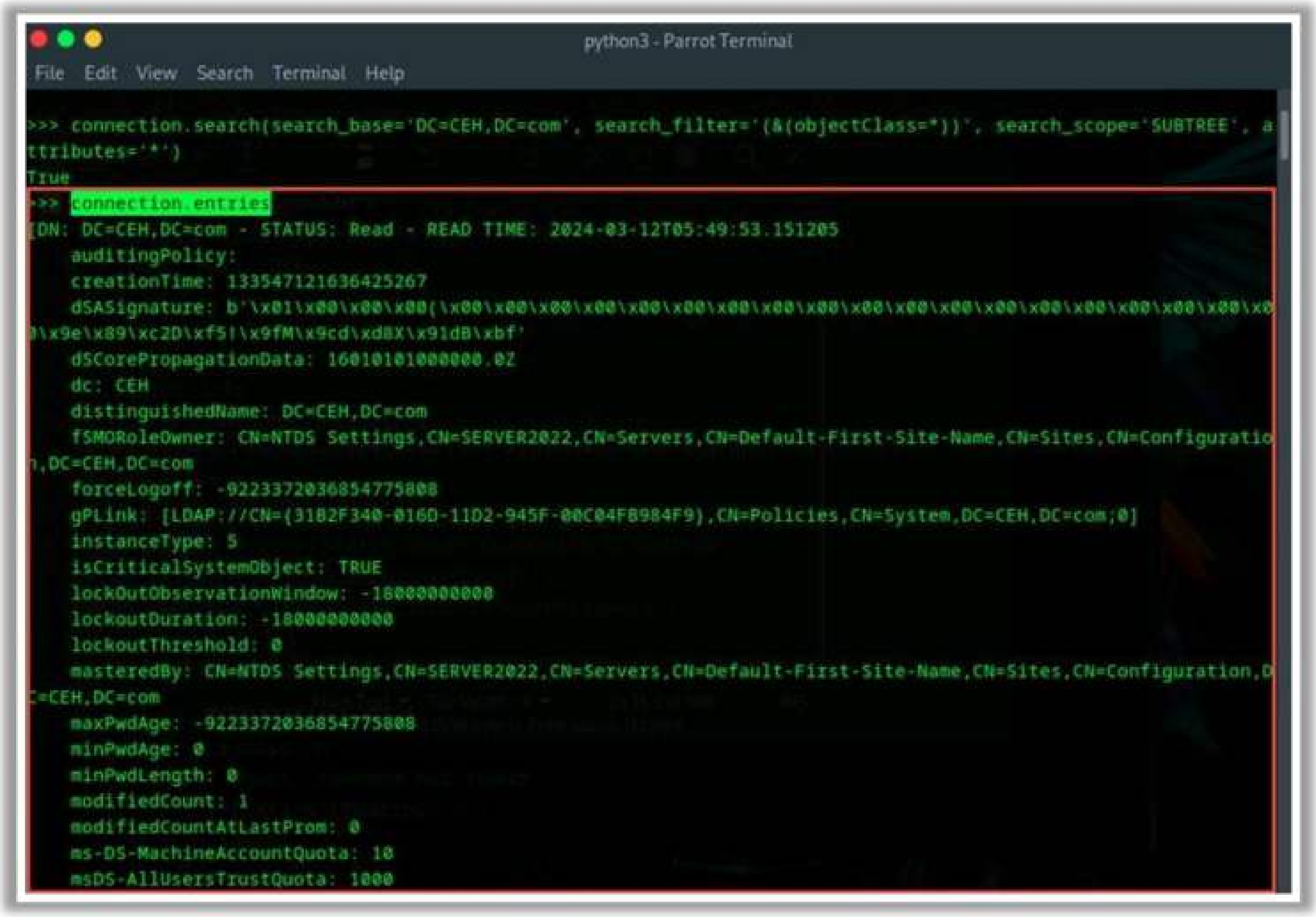
Figure 4.18: Screenshot showing LDAP enumeration using Python script

8. After obtaining the naming context, retrieve all the directory objects using the script given below:

```
>>> connection.search(search_base='DC=DOMAIN,DC=DOMAIN',
search_filter='(&(objectClass=*))', search_scope='SUBTREE',
attributes='*')
```

```
True
```

```
>> connection.entries
```


python3 - Parrot Terminal
File Edit View Search Terminal Help

```
>>> connection.search(search_base='DC=CEH,DC=com', search_filter='(&(objectClass=*))', search_scope='SUBTREE', a
ttributes='*')
True
>>> connection.entries
[DN: DC=CEH,DC=com - STATUS: Read - READ TIME: 2024-03-12T05:49:53.151205
    auditingPolicy:
    creationTime: 133547121636425267
    dSASignature: b'\x01\x00\x00\x00(\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x9e\x89\xc2D\xf5!\x9fM\x9cd\xd8X\x91dB\xbf'
    dSCorePropagationData: 16010101000000.0Z
    dc: CEH
    distinguishedName: DC=CEH,DC=com
    fSMORoleOwner: CN=NTDS Settings,CN=SERVER2022,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuratio
n,DC=CEH,DC=com
    forceLogoff: -9223372036854775808
    gPLink: [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=CEH,DC=com;0]
    instanceType: 5
    isCriticalSystemObject: TRUE
    lockOutObservationWindow: -18000000000
    lockoutDuration: -18000000000
    lockoutThreshold: 0
    masteredBy: CN=NTDS Settings,CN=SERVER2022,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,D
C=CEH,DC=com
    maxPwdAge: -9223372036854775808
    minPwdAge: 0
    minPwdLength: 0
    modifiedCount: 1
    modifiedCountAtLastProm: 0
    ms-DS-MachineAccountQuota: 10
    msDS-AllUsersTrustQuota: 1000
```

Figure 4.19: Screenshot showing output of LDAP enumeration

9. Now, use the following script to dump the entire LDAP:

```
>> connection.search(search_base='DC=DOMAIN,DC=DOMAIN',
search_filter='(&(objectClass=person))', search_scope='SUBTREE',
attributes='userPassword')

True

>>> connection.entries
```

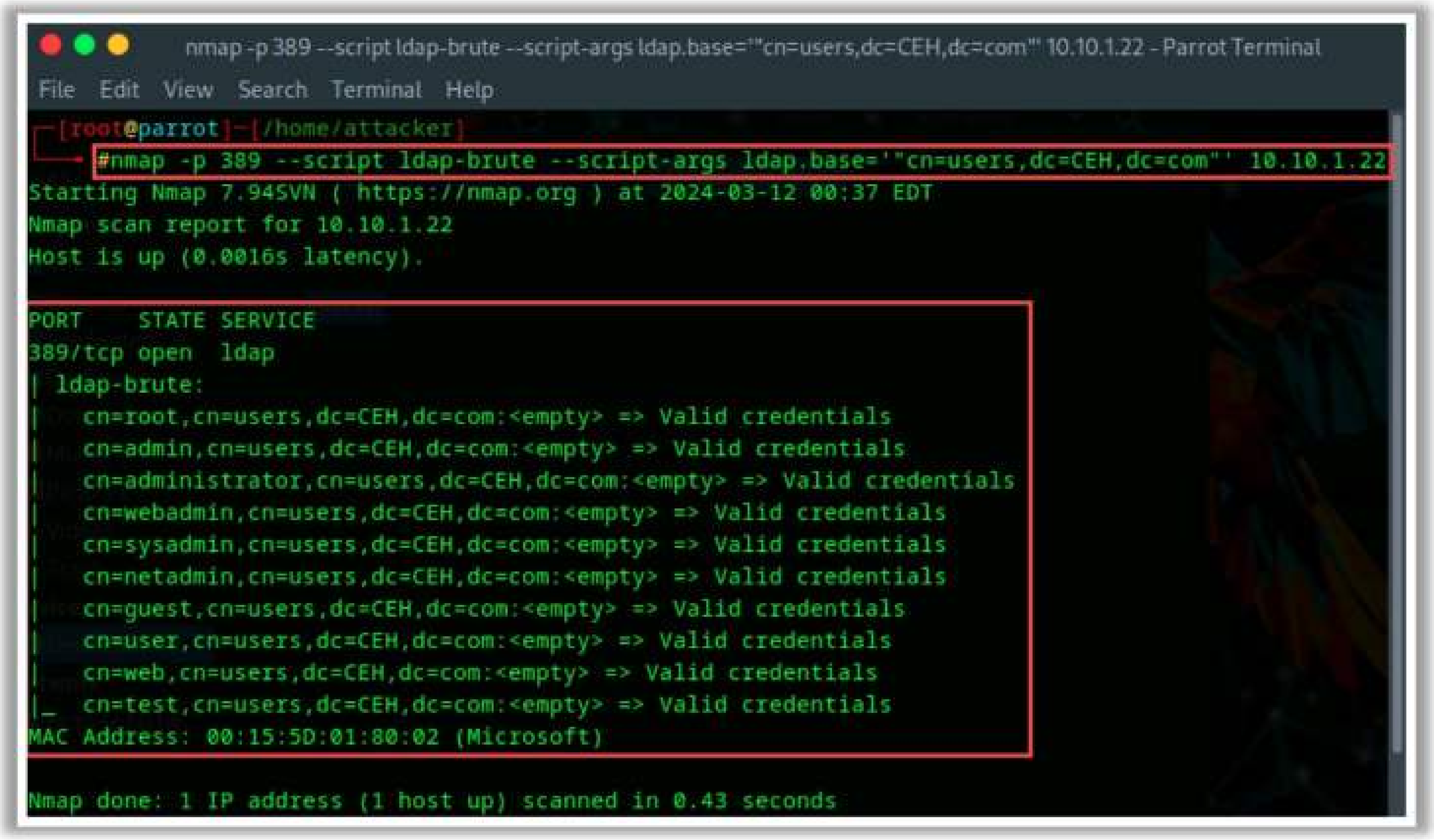
Automated LDAP Enumeration

Source: *https://nmap.org*

Attackers use the `ldap-brute NSE script` to brute-force LDAP authentication. By default, it uses the built-in username and password lists. The `userdb` and `passdb` script arguments can be employed to use custom lists.

```
nmap -p 389 --script ldap-brute --script-args
ldap.base='"cn=users,dc=CEH,dc=com "' <Target IP Address>
```

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



nmap -p 389 --script ldap-brute --script-args ldap.base='"cn=users,dc=CEH,dc=com"' 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -p 389 --script ldap-brute --script-args ldap.base='"cn=users,dc=CEH,dc=com"' 10.10.1.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 00:37 EDT
Nmap scan report for 10.10.1.22
Host is up (0.0016s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-brute:
|   cn=root,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=admin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=administrator,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=webadmin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=sysadmin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=netadmin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=guest,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=user,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=web,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|_  cn=test,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

Figure 4.20: Screenshot showing output of the Nmap ldap-brute NSE script

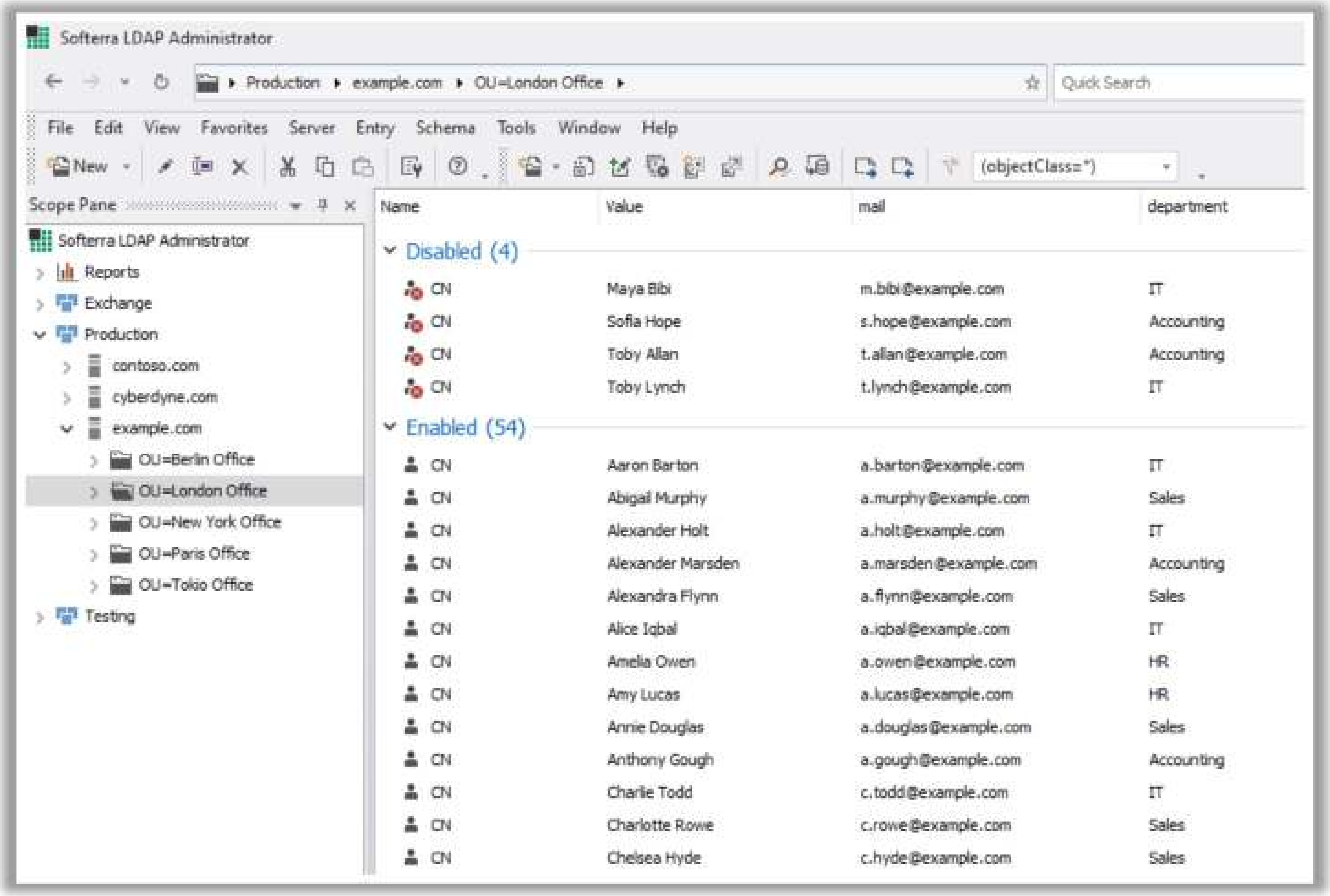
LDAP Enumeration Tools

There are many LDAP enumeration tools that access directory listings within Active Directory (AD) or other directory services. Using these tools, attackers can enumerate information such as valid usernames, addresses, and departmental details from different LDAP servers.

- **Softerra LDAP Administrator**

  Source: *https://www.ldapadministrator.com*

  Softerra LDAP Administrator is an LDAP administration tool that works with LDAP servers such as Active Directory (AD), Novell Directory Services, and Netscape/iPlanet. It browses and manages LDAP directories. As shown in the screenshot, attackers use Softerra LDAP Administrator to enumerate user details such as the username, email address, and department.



Name	Value	mail	department
Disabled (4)			
CN	Maya Bibi	m.bibi@example.com	IT
CN	Sofia Hope	s.hope@example.com	Accounting
CN	Toby Allan	t.allan@example.com	Accounting
CN	Toby Lynch	t.lynch@example.com	IT
Enabled (54)			
CN	Aaron Barton	a.barton@example.com	IT
CN	Abigail Murphy	a.murphy@example.com	Sales
CN	Alexander Holt	a.holt@example.com	IT
CN	Alexander Marsden	a.marsden@example.com	Accounting
CN	Alexandra Flynn	a.flynn@example.com	Sales
CN	Alice Iqbal	a.iqbal@example.com	IT
CN	Amelia Owen	a.owen@example.com	HR
CN	Amy Lucas	a.lucas@example.com	HR
CN	Annie Douglas	a.douglas@example.com	Sales
CN	Anthony Gough	a.gough@example.com	Accounting
CN	Charlie Todd	c.todd@example.com	IT
CN	Charlotte Rowe	c.rowe@example.com	Sales
CN	Chelsea Hyde	c.hyde@example.com	Sales

Figure 4.21: Screenshot of Softerra LDAP Administrator

- **ldapsearch**

  Source: *https://linux.die.net*

  `ldapsearch` is a shell-accessible interface for the **`ldap_search_ext(3)`** library call. **`ldapsearch`** opens a connection to an LDAP server, binds it, and performs a search using the specified parameters. The filter should conform to the string representation of the search filters, as defined in RFC 4515. If not provided, the default filter, (**`objectClass=*`**), is used.

  If **`ldapsearch`** finds one or more entries, the attributes specified by **`attrs`** are returned. If **`*`** is listed, all user attributes are returned. If **`+`** is listed, all operational attributes are returned. If no **`attrs`** are listed, all user attributes are returned. If only **`1.1`** is listed, no attributes are returned.

  The search results are displayed using an extended version of the LDAP Data Interchange Format (LDIF). The option **`-L`** controls the output format.

  Attackers use **`ldapsearch`** to enumerate AD users. This allows attackers to establish connections with an LDAP server to perform different searches using specific filters. The following command can be used to perform an LDAP search using simple authentication:

  ```
  ldapsearch -h <Target IP Address> -x
  ```

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

If the above command is executed successfully, the following command can be executed to obtain additional details related to the naming contexts:

`ldapsearch -h <Target IP Address> -x -s base namingcontexts`

For example, from the output of the above command, if the primary domain component can be identified as `DC=htb,DC=local`, the following command can be used to obtain more information about the primary domain:

`ldapsearch -h <Target IP Address> -x -b "DC=htb,DC=local"`

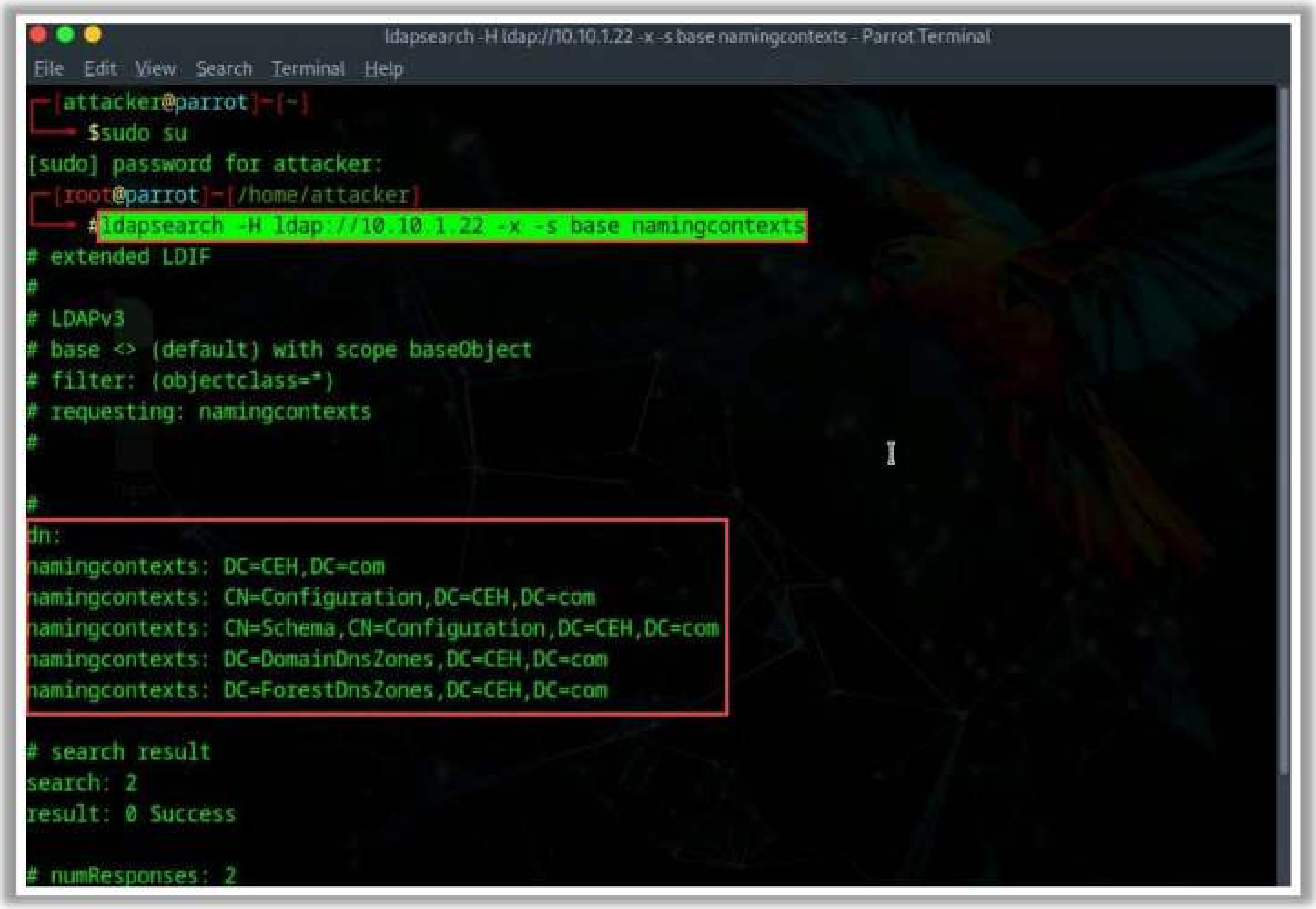
The following commands can be used to retrieve information about a specific object or all the objects in a directory tree:

`ldapsearch -h <Target IP Address> -x -b "DC=htb,DC=local" '(objectClass=Employee)'`→ retrieves information related to the object class Employee.

`ldapsearch -x -h <Target IP Address> -b "DC=htb,DC=local" "objectclass=*"` → retrieves information related to all the objects in the directory tree.

The following command retrieves a list of users belonging to a particular object class:

`ldapsearch -h <Target IP Address> -x -b "DC=htb,DC=local" '(objectClass= Employee)' sAMAccountName sAMAccountType`


ldapsearch -H ldap://10.10.1.22 -x -s base namingcontexts - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #ldapsearch -H ldap://10.10.1.22 -x -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingcontexts: DC=CEH,DC=com
namingcontexts: CN=Configuration,DC=CEH,DC=com
namingcontexts: CN=Schema,CN=Configuration,DC=CEH,DC=com
namingcontexts: DC=DomainDnsZones,DC=CEH,DC=com
namingcontexts: DC=ForestDnsZones,DC=CEH,DC=com

# search result
search: 2
result: 0 Success

# numResponses: 2
```

Figure 4.22: Screenshot of ldapsearch

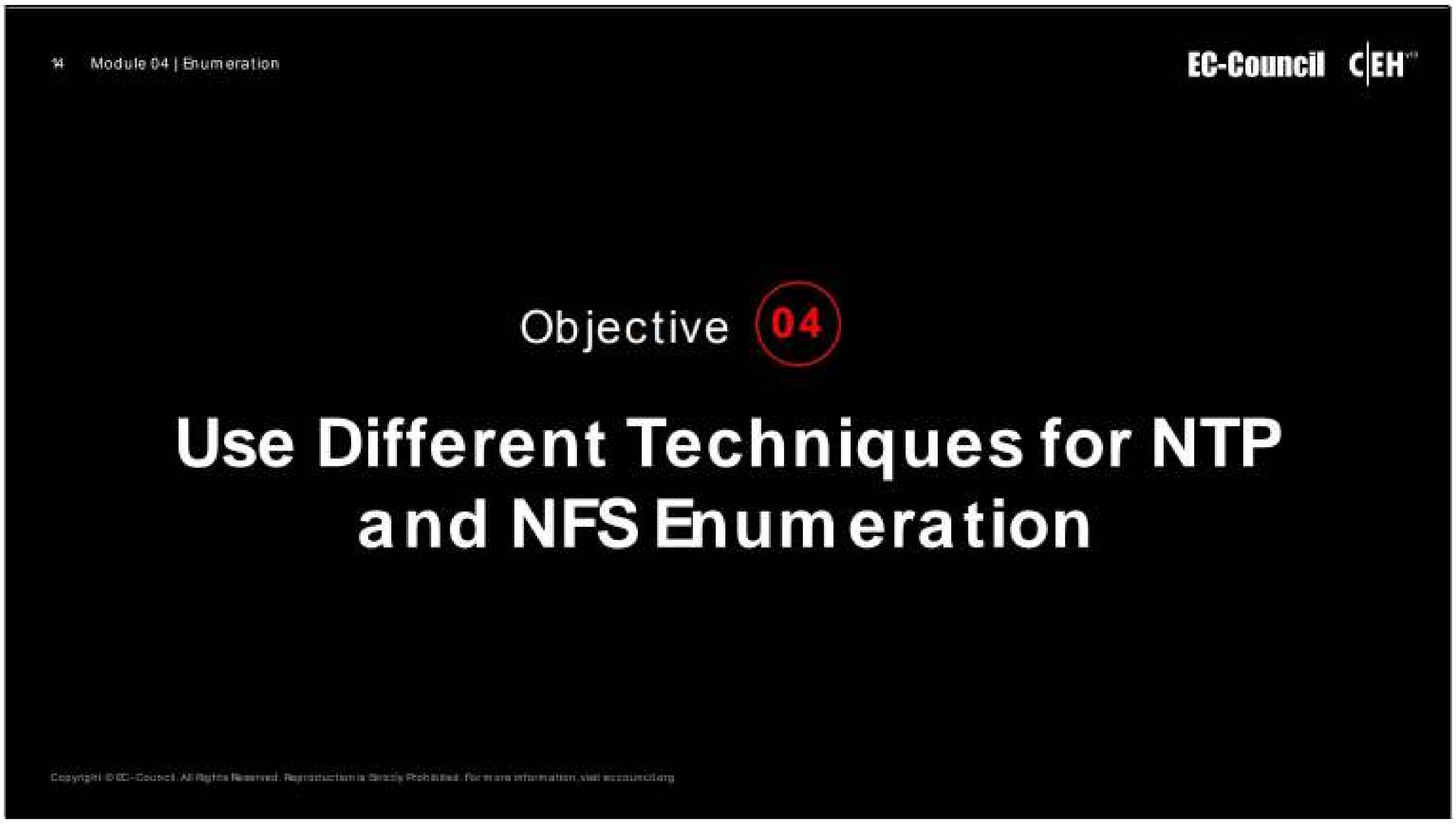
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some additional LDAP enumeration tools:

- AD Explorer (*https://docs.microsoft.com*)
- LDAP Admin Tool (*https://www.ldapsoft.com*)
- LDAP Account Manager (*https://www.ldap-account-manager.org*)
- LDAP Search (*https://securityxploded.com*)

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24



Objective 04

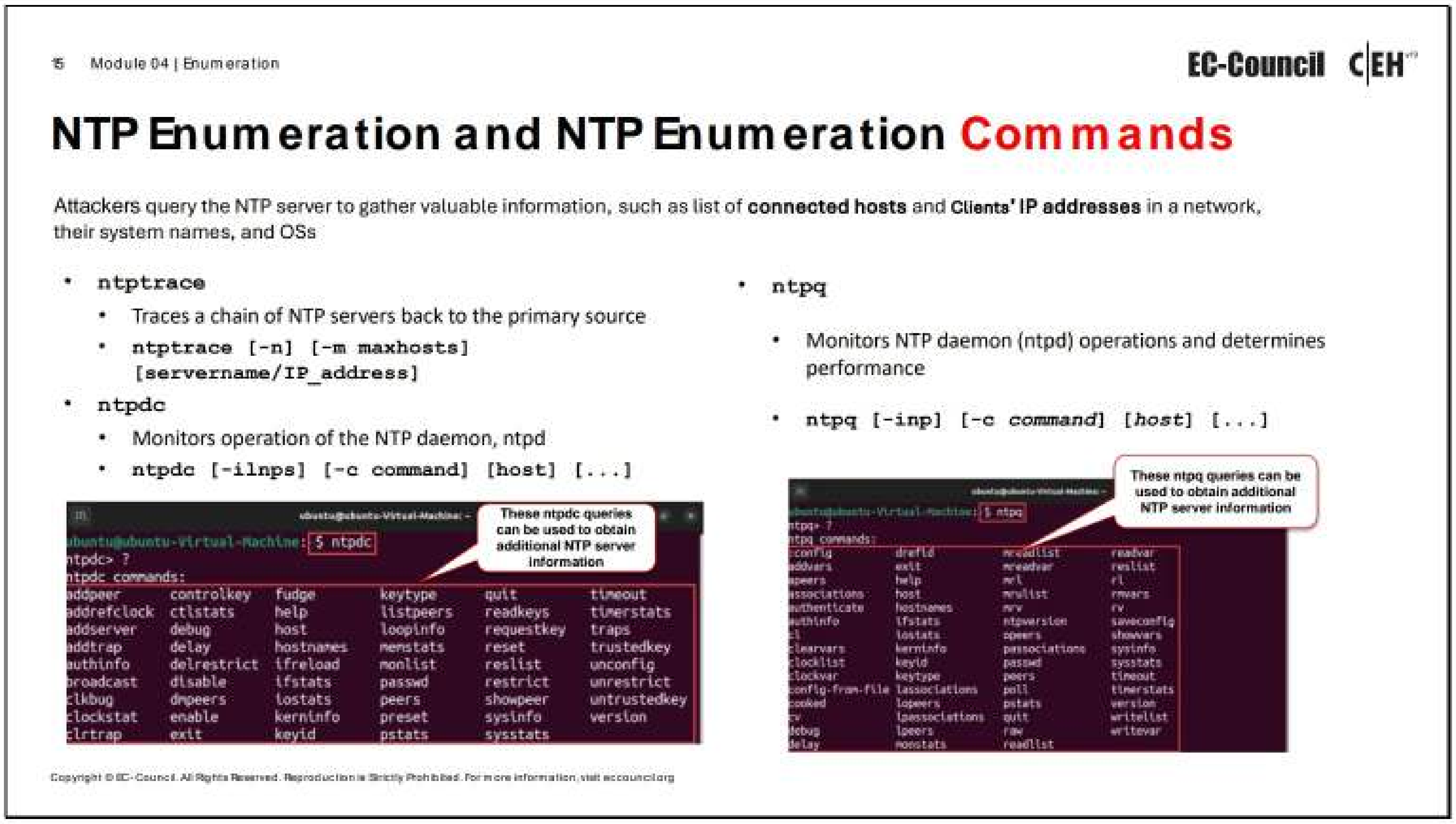
Use Different Techniques for NTP and NFS Enumeration

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

NTP and NFS Enumeration

Administrators often overlook the Network Time Protocol (NTP) server when considering security. However, if queried properly, it can provide valuable network information to an attacker. Therefore, it is necessary to know what information an attacker can obtain about a network through NTP enumeration. The Network File System (NFS) is used for the management of remote file access. NFS enumeration helps attackers to gather information such as a list of clients connected to the NFS server, along with their IP addresses, and exported directories.

This section describes NTP enumeration, the information extracted via NTP enumeration, various NTP enumeration commands, NTP enumeration tools, and NFS enumeration techniques and tools.



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] [...]`**

```
ubuntu@ubuntu-Virtual-Machine: $ 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
clrtrap      exit         keyid        pstats       sysstats
```

These ntpdc queries can be used to obtain additional NTP server information

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

```
ubuntu@ubuntu-Virtual-Machine: $ ntpq
ntpq> ?
ntpq commands:
:config          drefid           mreadlist        readvar
addvars          exit             mreadvar         reslist
apeers           help             mrl              rl
associations     host             mrulist          rmvars
authenticate     hostnames        mrv              rv
authinfo         ifstats          ntpversion       saveconfig
cl               iostats          opeers           showvars
clearvars        kerninfo         passociations    sysinfo
clocklist        keyid            passwd           sysstats
clockvar         keytype          peers            timeout
config-from-file lassociations    poll             timerstats
cooked           lopeers          pstats           version
cv               lpassociations   quit             writelist
debug            lpeers           raw              writevar
delay            monstats         readlist
```

These ntpq queries can be used to obtain additional NTP server information

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

NTP Enumeration

NTP is designed to synchronize clocks of networked computers. It uses UDP port 123 as its primary means of communication. NTP can maintain time within an error of 10 ms over the public Internet. Furthermore, it can achieve an accuracy of 200 µs or better in LANs under ideal conditions.

The following are some pieces of information an attacker can obtain by querying an NTP server:

- List of hosts connected to the NTP server
- Clients' IP addresses in the network, their system names, and OSs
- Internal IPs, if the NTP server is in the demilitarized zone (DMZ)

NTP Enumeration Commands

NTP enumeration commands such as **`ntpdate`**, **`ntptrace`**, **`ntpdc`**, and **`ntpq`** are used to query an NTP server for valuable information.

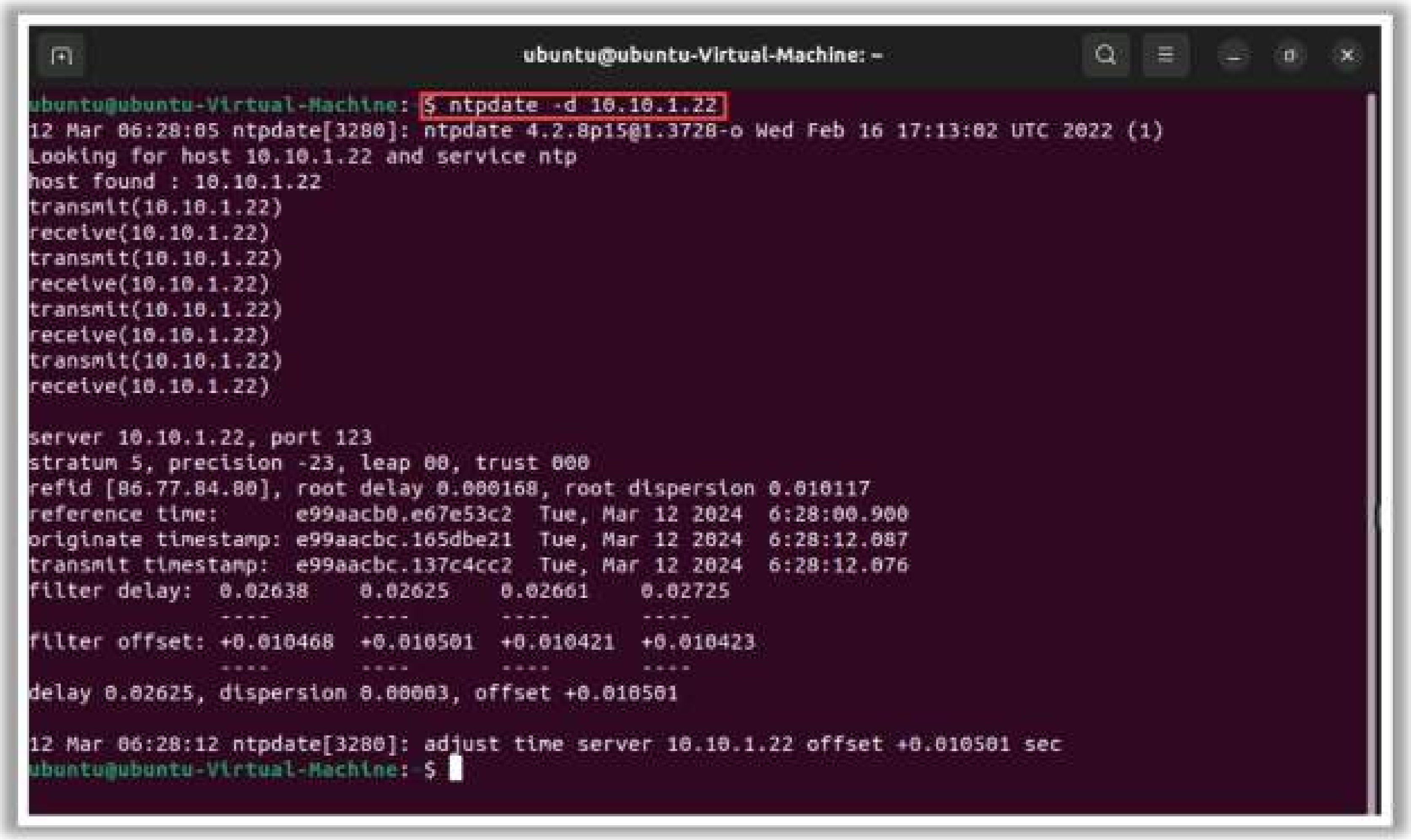
- **ntpdate**

  This command collects the number of time samples from several time sources. Its syntax is as follows:

  ```
  ntpdate [-46bBdqsuv] [-a key] [-e authdelay] [-k keyfile] [-o version] [-p samples] [-t timeout] [ -U user_name] server [...]
  ```

`-4`	Force DNS resolution of given host names to the IPv4 namespace
`-6`	Force DNS resolution of given host names to the IPv6 namespace
`-a key`	Enable the authentication function/specify the key identifier to be used for authentication
`-B`	Force the time to always be slewed
`-b`	Force the time to be stepped
`-d`	Enable debugging mode
`-e authdelay`	Specify the processing delay to perform an authentication function
`-k keyfile`	Specify the path for the authentication key file as the string “keyfile”; the default is /etc/ntp/keys
`-o version`	Specify the NTP version for outgoing packets as an integer version, which can be 1 or 2; the default is 4
`-p samples`	Specify the number of samples to be acquired from each server, with values ranging from 1–8; the default is 4
`-q`	Query only; do not set the clock
`-s`	Divert logging output from the standard output (default) to the system syslog facility
`-t timeout`	Specify the maximum wait time for a server response; the default is 1 s
`-u`	Use an unprivileged port for outgoing packets
`-v`	Be verbose; logs ntpdate’s version identification string

Table 4.4: ntpdate parameters and their respective functions



```
ubuntu@ubuntu-Virtual-Machine: $ ntpdate -d 10.10.1.22
12 Mar 06:28:05 ntpdate[3280]: ntpdate 4.2.8p15@1.3728-o Wed Feb 16 17:13:02 UTC 2022 (1)
Looking for host 10.10.1.22 and service ntp
host found : 10.10.1.22
transmit(10.10.1.22)
receive(10.10.1.22)
transmit(10.10.1.22)
receive(10.10.1.22)
transmit(10.10.1.22)
receive(10.10.1.22)
transmit(10.10.1.22)
receive(10.10.1.22)

server 10.10.1.22, port 123
stratum 5, precision -23, leap 00, trust 000
refid [86.77.84.80], root delay 0.000168, root dispersion 0.010117
reference time:      e99aacb0.e67e53c2  Tue, Mar 12 2024  6:28:00.900
originate timestamp: e99aacbc.165dbe21  Tue, Mar 12 2024  6:28:12.087
transmit timestamp:  e99aacbc.137c4cc2  Tue, Mar 12 2024  6:28:12.076
filter delay:  0.02638    0.02625    0.02661    0.02725
               ----       ----       ----       ----
filter offset: +0.010468  +0.010501  +0.010421  +0.010423
               ----       ----       ----       ----
delay 0.02625, dispersion 0.00003, offset +0.010501

12 Mar 06:28:12 ntpdate[3280]: adjust time server 10.10.1.22 offset +0.010501 sec
ubuntu@ubuntu-Virtual-Machine: $ 
```

Figure 4.23: Screenshot of the ntpdate command, showing debugging information for a given IP

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **ntptrace**

  This command determines where the NTP server obtains the time from and follows the chain of NTP servers back to its primary time source. Attackers use this command to trace the list of NTP servers connected to the network. Its syntax is as follows:

  ```
  ntptrace [-n] [-m maxhosts] [servername/IP_address]
  ```

`-n`	Do not print host names and show only IP addresses; may be useful if a name server is down
`-m maxhosts`	Set the maximum number of levels up the chain to be followed

Table 4.5: ntptrace parameters and their respective functions

  Example:

  ```
  # ntptrace
  localhost: stratum 4, offset 0.0019529, synch distance 0.143235
  10.10.0.1: stratum 2, offset 0.01142
  73, synch distance 0.115554
  10.10.1.1: stratum 1, offset 0.0017698, synch distance 0.011193
  ```

- **ntpdc**

  This command queries the ntpd daemon regarding its current state and requests changes in that state. Attackers use this command to retrieve the state and statistics of each NTP server connected to the target network. Its syntax is as follows:

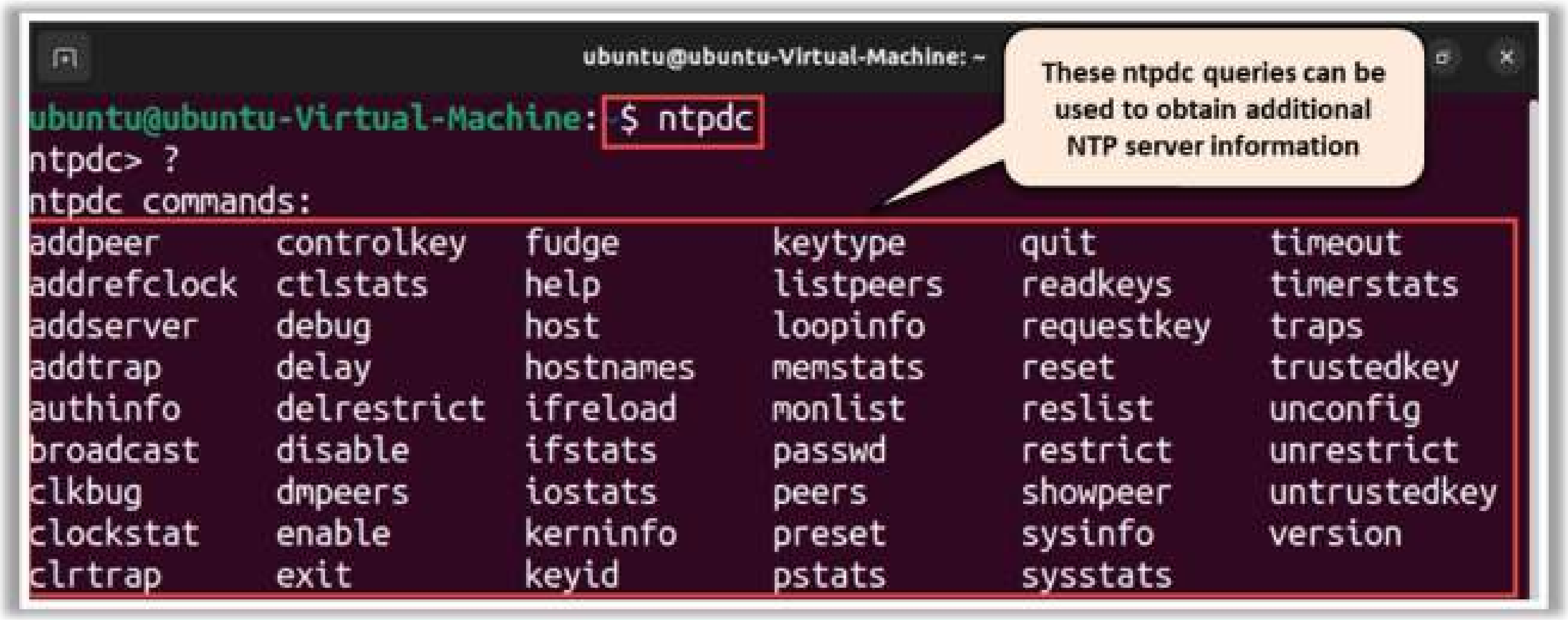
  ```
  ntpdc [ -46dilnps ] [ -c command] [hostname/IP_address]
  ```

`-4`	Force DNS resolution of the given host name to the IPv4 namespace
`-6`	Force DNS resolution of the given host name to the IPv6 namespace
`-d`	Set the debugging mode to on
`-c`	Following argument is interpreted as an interactive format command; multiple -c options may be given
`-i`	Force ntpdc to operate in the interactive mode
`-l`	Obtain a list of peers known to the server(s); this switch is equivalent to -c listpeers
`-n`	Output all host addresses in the dotted-quad numeric format, rather than host names
`-p`	Print a list of the peers as well as a summary of their states; this is equivalent to -c peers
`-s`	Print a list of the peers as well as a summary of their states, but in a slightly different format from that for the -p switch; this is equivalent to -c dmpeers

Table 4.6: ntpdc parameters and their respective functions

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24



```
ubuntu@ubuntu-Virtual-Machine:~$ 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
clrtrap      exit         keyid        pstats       sysstats
```

These ntpdc queries can be used to obtain additional NTP server information

Figure 4.24: Screenshot of the ntpdc command

- **ntpq**

  This command monitors the operations of the NTP daemon **`ntpd`** and determines its performance. Its syntax is as follows:

  `ntpq [-46dinp] [-c command] [host/IP_address]`

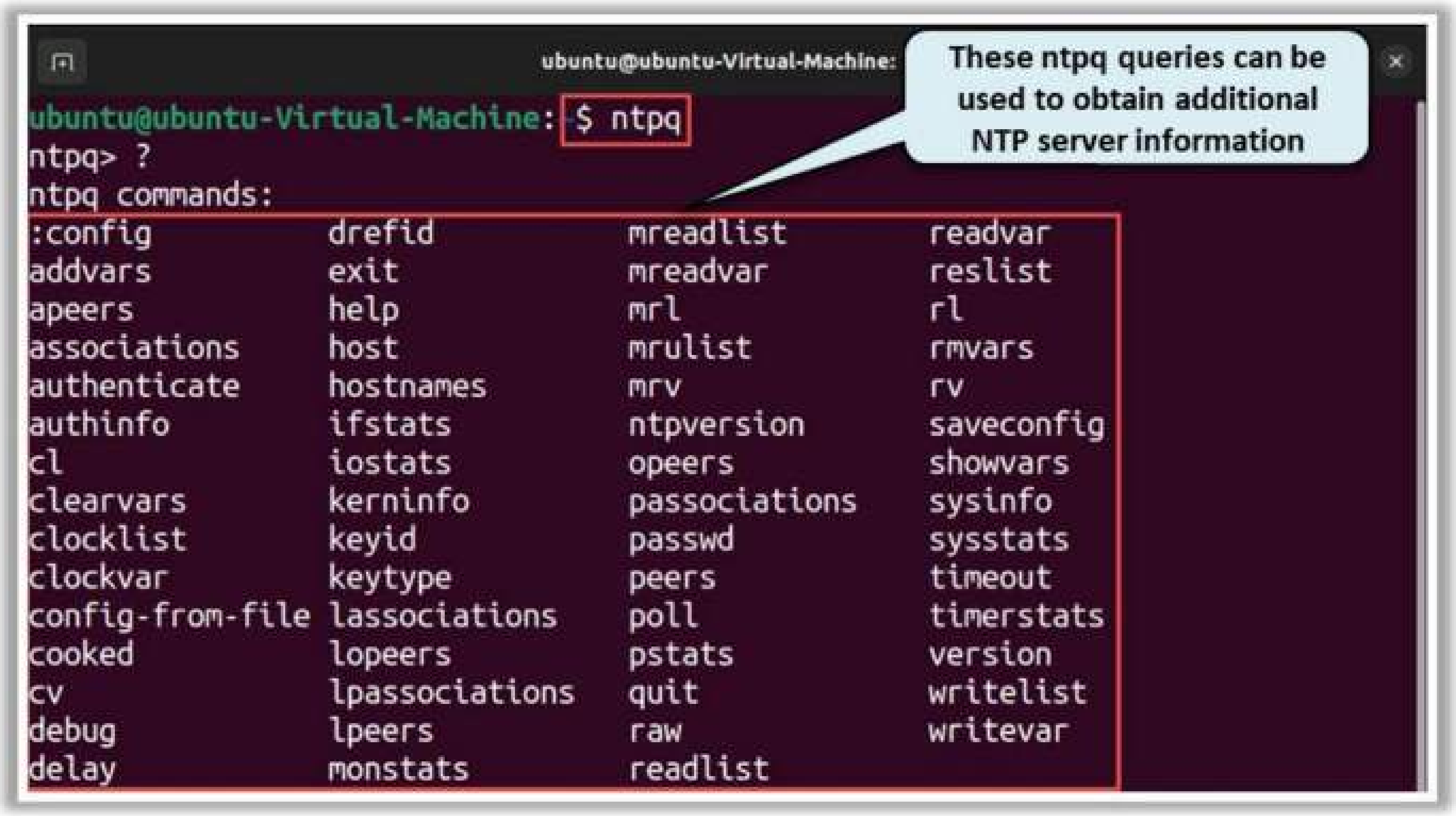
`-4`	Force DNS resolution of the given host name to the IPv4 namespace
`-6`	Force DNS resolution of the given host name to the IPv6 namespace
`-c`	Following argument is an interactive format command; multiple -c options may be given
`-d`	Debugging mode
`-i`	Force ntpq to operate in the interactive mode
`-n`	Output all host addresses in the dotted-quad numeric format, rather than host names
`-p`	Print a list of the peers as well as a summary of their states

Table 4.7: ntpq parameters and their respective functions

Example:

```
ntpq> version
ntpq 4.2.8p15@1.3728-o
ntpq> host
current host is localhost
```

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



These ntpq queries can be used to obtain additional NTP server information

```
ubuntu@ubuntu-Virtual-Machine:~$ ntpq
ntpq> ?
ntpq commands:
:config          drefid           mreadlist        readvar
addvars          exit             mreadvar         reslist
apeers           help             mrl              rl
associations     host             mrulist          rmvars
authenticate     hostnames        mrv              rv
authinfo         ifstats          ntpversion       saveconfig
cl               iostats          opeers           showvars
clearvars        kerninfo         passociations    sysinfo
clocklist        keyid            passwd           sysstats
clockvar         keytype          peers            timeout
config-from-file lassociations    poll             timerstats
cooked           lopeers          pstats           version
cv               lpassociations   quit             writelist
debug            lpeers           raw              writevar
delay            monstats         readlist
```

Figure 4.25: Screenshot of the ntpq command

Note: In many Linux distributions, the NTP daemon **`ntpd`** has been joined with Chrony, **`chronyd`**. Both the daemons synchronize the local system's time with a remote time server.

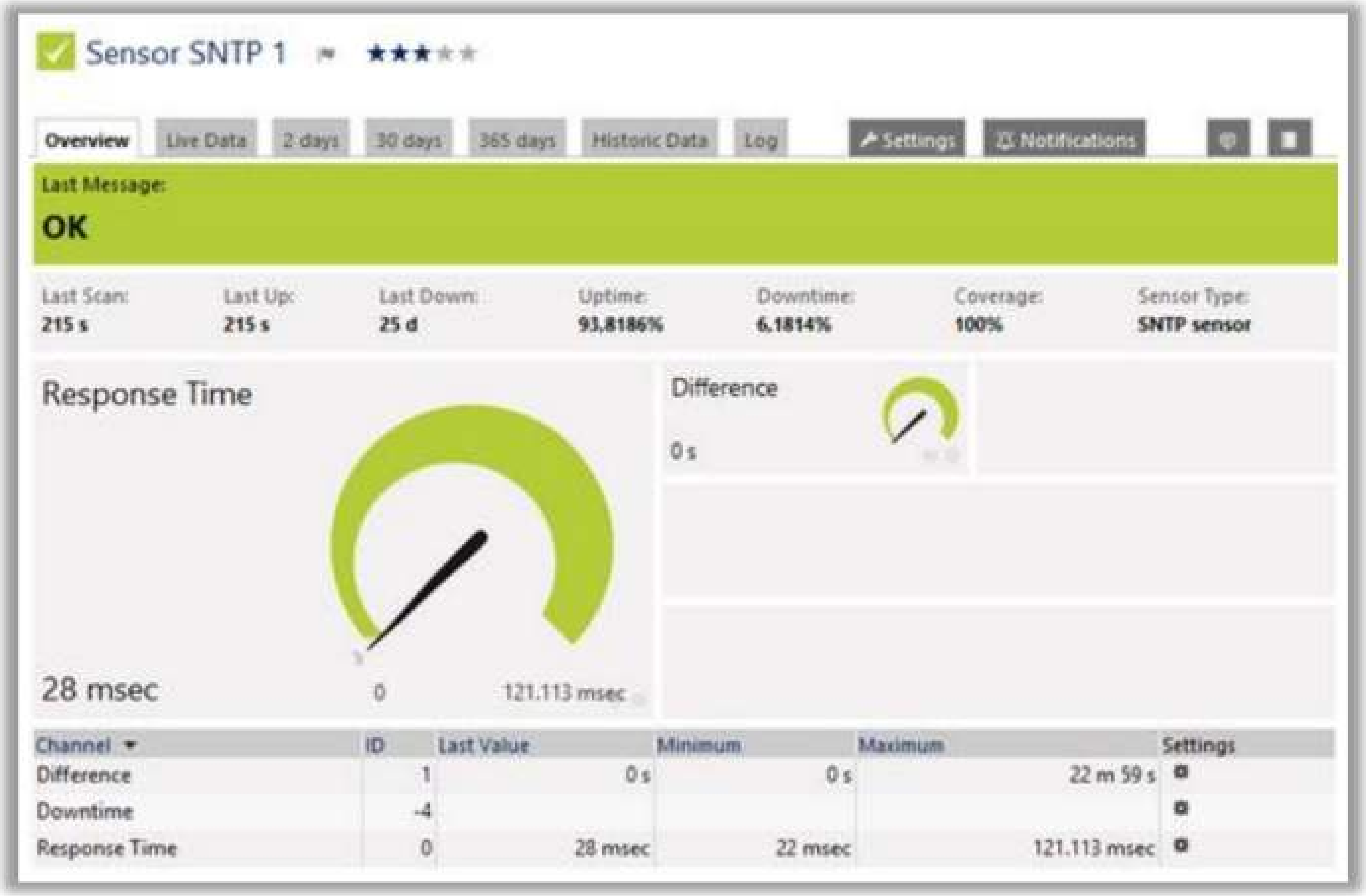
NTP Enumeration Tools

NTP enumeration tools are used to monitor the working of NTP and SNTP servers in the network and help in the configuration and verification of connectivity from the time client to the NTP servers.

- **PRTG Network Monitor**

  Source: *https://www.paessler.com*

  PRTG monitors all systems, devices, traffic, and applications of IT infrastructure by using various technologies such as SNMP, WMI, and SSH. Attackers use PRTG Network Monitor to retrieve SNTP server details such as the response time from the server, active sensors with the server, and synchronization time.



Last Message:
OK

Last Scan:	Last Up:	Last Down:	Uptime:	Downtime:	Coverage:	Sensor Type:
215 s	215 s	25 d	93,8186%	6,1814%	100%	SNTP sensor

Response Time 28 msec

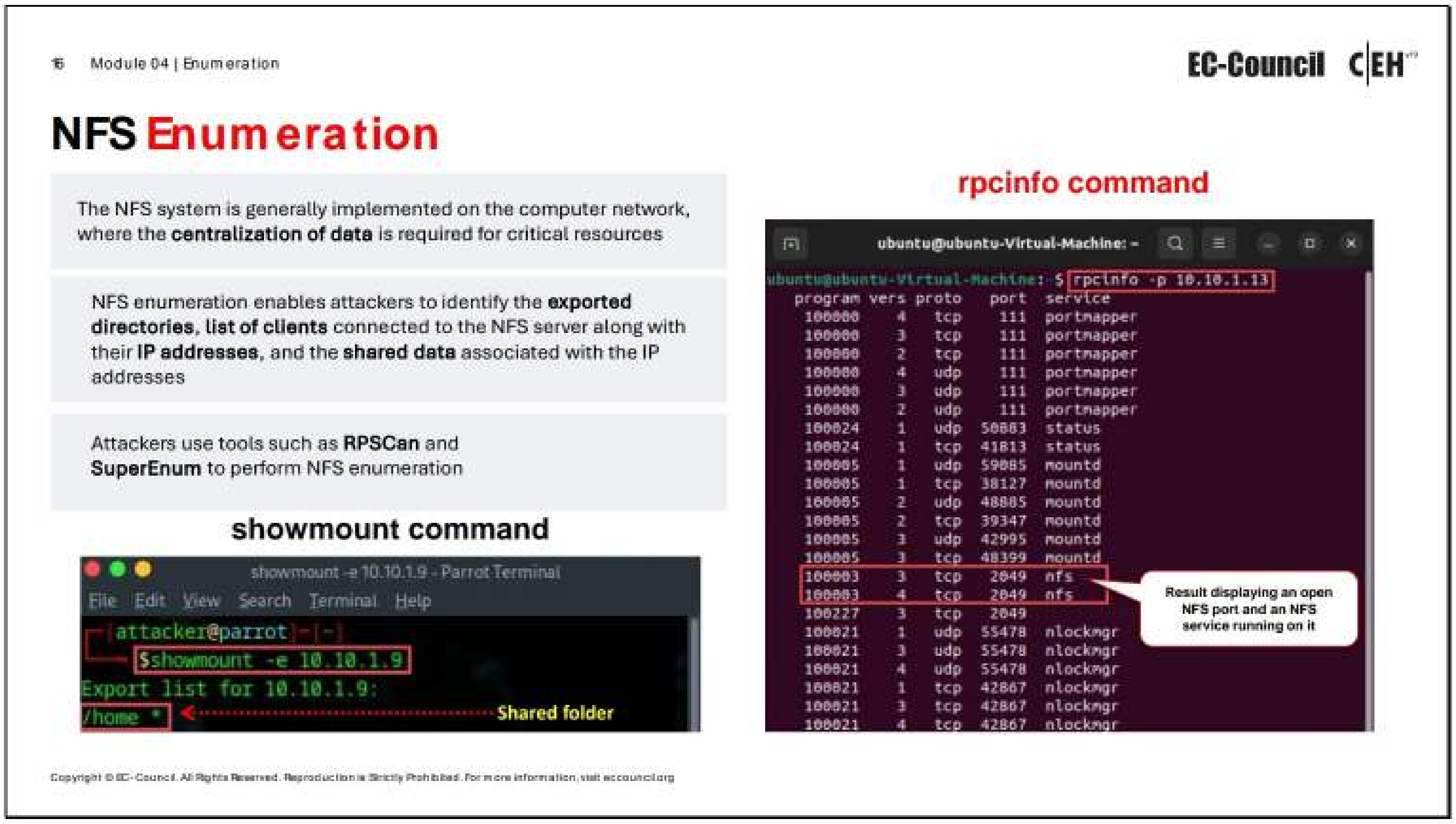
Difference 0 s

Channel ▾	ID	Last Value	Minimum	Maximum	Settings
Difference	1	0 s	0 s	22 m 59 s	⚙
Downtime	-4				⚙
Response Time	0	28 msec	22 msec	121.113 msec	⚙

Figure 4.26: Screenshot of PRTG Network Monitor

The following are some NTP enumeration tools:

- Nmap (*https://nmap.org*)
- Wireshark (*https://www.wireshark.org*)
- udp-proto-scanner (*https://labs.portcullis.co.uk*)
- NTP Server Scanner (*http://www.bytefusion.com*)



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

showmount -e 10.10.1.9 - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $showmount -e 10.10.1.9
Export list for 10.10.1.9:
/home *
```

rpcinfo command

```
ubuntu@ubuntu-Virtual-Machine:~$ rpcinfo -p 10.10.1.13
   program vers proto   port  service
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  50883  status
    100024    1   tcp  41813  status
    100005    1   udp  59085  mountd
    100005    1   tcp  38127  mountd
    100005    2   udp  48885  mountd
    100005    2   tcp  39347  mountd
    100005    3   udp  42995  mountd
    100005    3   tcp  48399  mountd
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100227    3   tcp   2049
    100021    1   udp  55478  nlockmgr
    100021    3   udp  55478  nlockmgr
    100021    4   udp  55478  nlockmgr
    100021    1   tcp  42867  nlockmgr
    100021    3   tcp  42867  nlockmgr
    100021    4   tcp  42867  nlockmgr
```

Result displaying an open NFS port and an NFS service running on it

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

NFS Enumeration

NFS is a type of file system that enables users to access, view, store, and update files over a remote server. These remote data can be accessed by the client in the same way it is accessed on the local system. Depending on the privileges assigned to the clients, they can either only read or both read and write the data.

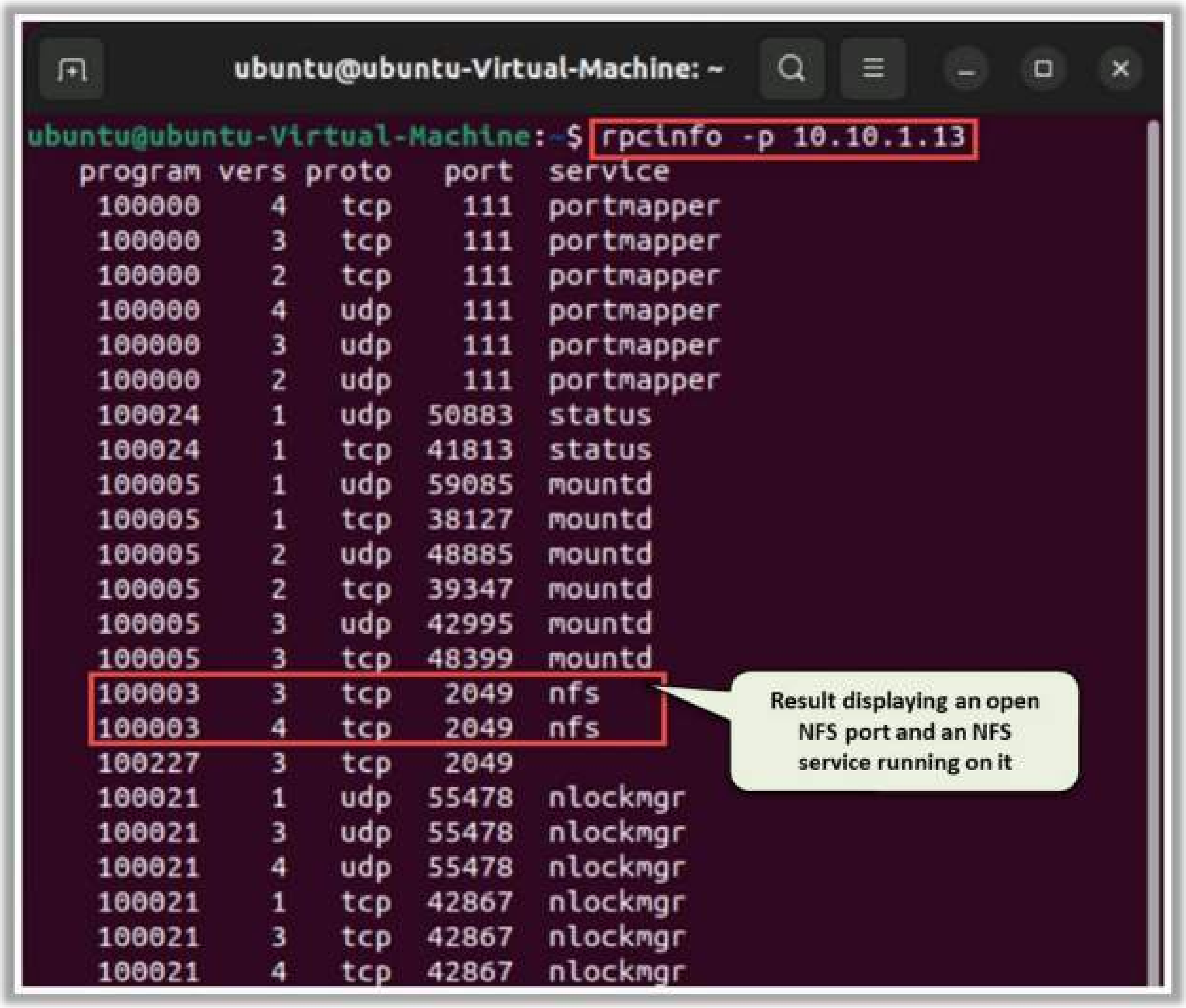
An NFS system is generally implemented on a computer network in which the centralization of data is required for critical resources. The remote procedure call (RPC) is used to route and process the request between clients and servers.

To accomplish the task of sharing files and directories over the network, the "exporting" process is used. However, the client first attempts to make the file available for sharing by using the "mounting" process. The **`/etc/exports`** location on the NFS server contains a list of clients allowed to share files on the server. In this approach, to access the server, the only credential used is the client's IP address. NFS versions before version 4 run on the same security specification.

Enumerating NFS services 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. After gathering this information, the attackers can spoof their IP addresses to gain full access to the shared files on the server.

As shown in the screenshot, an attacker runs the following **`rpcinfo`** command to scan the target IP address for an open NFS port (port 2049) and the NFS services running on it:

```
rpcinfo -p <Target IP Address>
```



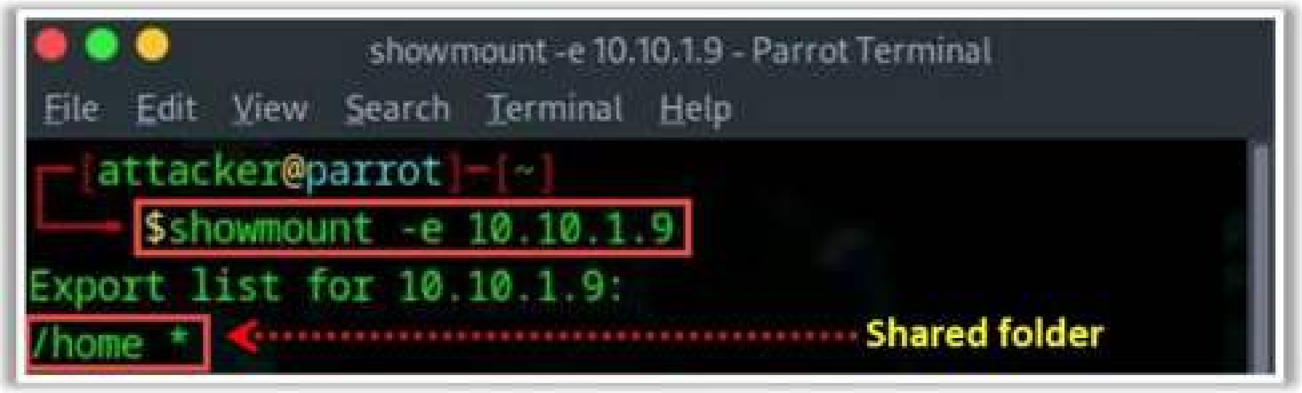
```
ubuntu@ubuntu-Virtual-Machine:~$ rpcinfo -p 10.10.1.13
   program vers proto   port  service
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  50883  status
    100024    1   tcp  41813  status
    100005    1   udp  59085  mountd
    100005    1   tcp  38127  mountd
    100005    2   udp  48885  mountd
    100005    2   tcp  39347  mountd
    100005    3   udp  42995  mountd
    100005    3   tcp  48399  mountd
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100227    3   tcp   2049
    100021    1   udp  55478  nlockmgr
    100021    3   udp  55478  nlockmgr
    100021    4   udp  55478  nlockmgr
    100021    1   tcp  42867  nlockmgr
    100021    3   tcp  42867  nlockmgr
    100021    4   tcp  42867  nlockmgr
```

Result displaying an open NFS port and an NFS service running on it

Figure 4.27: Screenshot of rpcinfo command displaying open NFS port and services

As shown in the screenshot, an attacker runs the following command to view the list of shared files and directories:

`showmount -e <Target IP Address>`



```
┌─[attacker@parrot]─[~]
└──╼ $showmount -e 10.10.1.9
Export list for 10.10.1.9:
/home *
```

Figure 4.28: Screenshot of the showmount command displaying a shared directory

Further, an attacker can use various other commands and tools to gain access to the NFS server and upload malicious files on the server to launch further attacks.

NFS Enumeration Tools

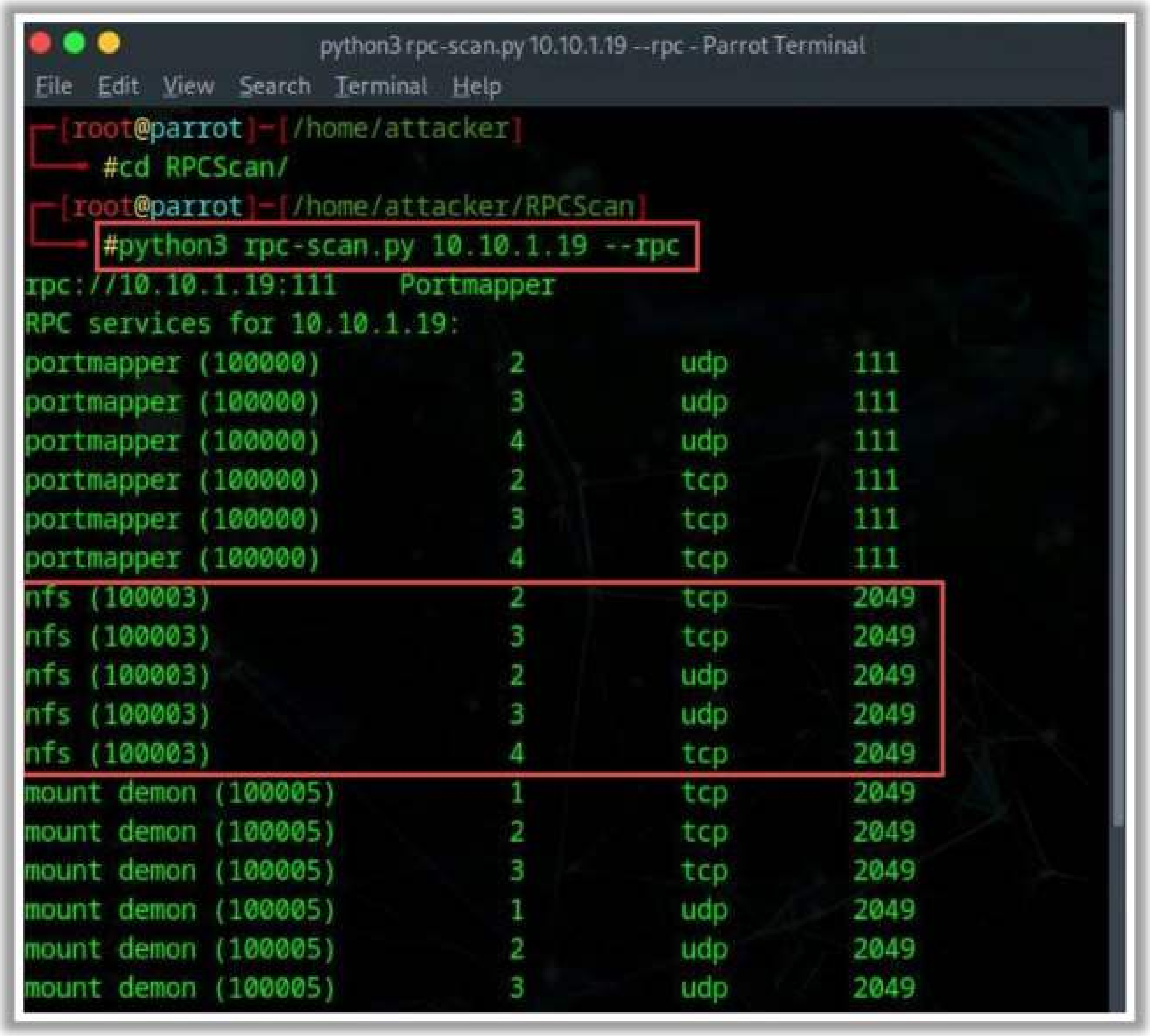
NFS enumeration tools scan a network within a given range of IP addresses or a single IP address to identify the NFS services running on it. These tools also assist in obtaining a list of RPC services using portmap, a list of NFS shares, and a list of directories accessible through NFS; further, they allow downloading a file shared through the NFS server. Attackers use tools such as RPCScan and SuperEnum to perform NFS enumeration.

- **RPCScan**

  Source: *https://github.com*

  RPCScan communicates with RPC services and checks misconfigurations on NFS shares. As shown in the screenshot, an attacker runs the following command to enumerate a target IP address for active NFS services:

  `python3 rpc-scan.py <Target IP Address> --rpc`


python3 rpc-scan.py 10.10.1.19 --rpc - Parrot Terminal
File Edit View Search Terminal Help

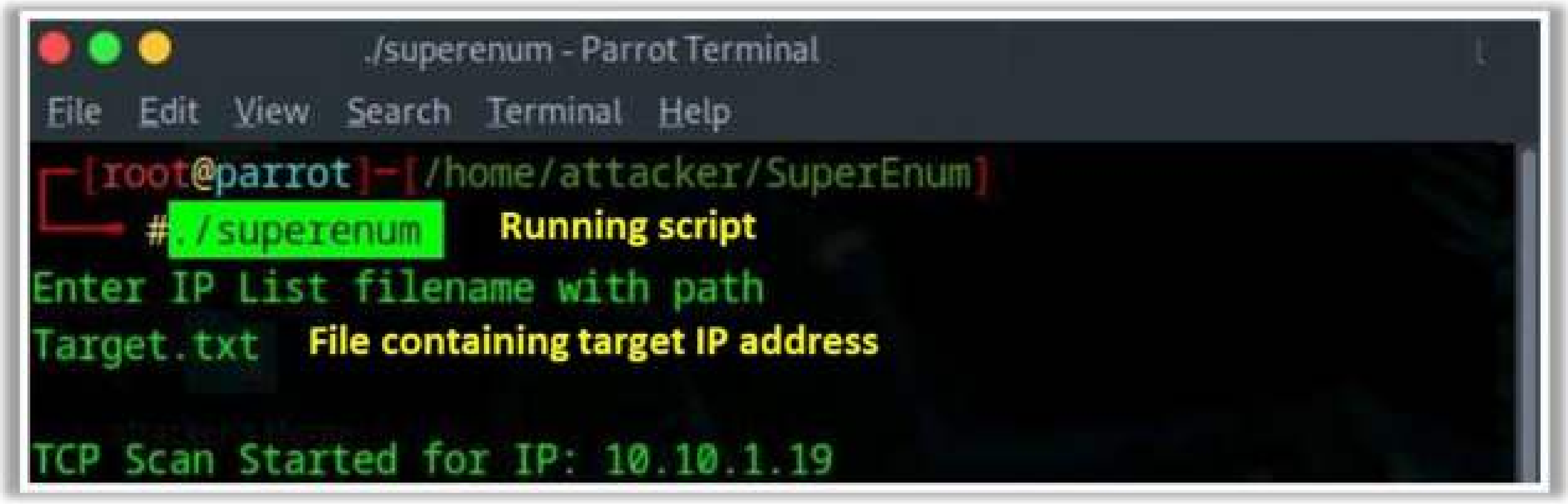
```
┌─[root@parrot]─[/home/attacker]
└──╼ #cd RPCScan/
┌─[root@parrot]─[/home/attacker/RPCScan]
└──╼ #python3 rpc-scan.py 10.10.1.19 --rpc
rpc://10.10.1.19:111    Portmapper
RPC services for 10.10.1.19:
portmapper (100000)           2         udp       111
portmapper (100000)           3         udp       111
portmapper (100000)           4         udp       111
portmapper (100000)           2         tcp       111
portmapper (100000)           3         tcp       111
portmapper (100000)           4         tcp       111
nfs (100003)                  2         tcp       2049
nfs (100003)                  3         tcp       2049
nfs (100003)                  2         udp       2049
nfs (100003)                  3         udp       2049
nfs (100003)                  4         tcp       2049
mount demon (100005)          1         tcp       2049
mount demon (100005)          2         tcp       2049
mount demon (100005)          3         tcp       2049
mount demon (100005)          1         udp       2049
mount demon (100005)          2         udp       2049
mount demon (100005)          3         udp       2049
```

Figure 4.29: Screenshot of RPCScan displaying open NFS ports and services

- **SuperEnum**

  Source: *https://github.com*

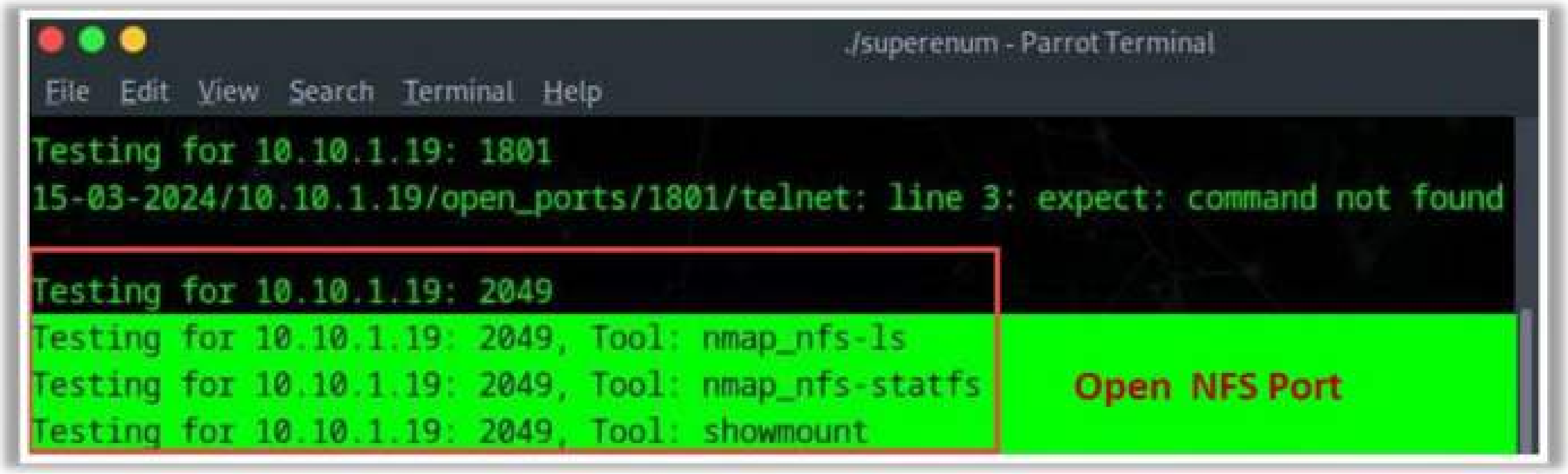
  SuperEnum includes a script that performs the basic enumeration of any open port. As shown in the screenshot, an attacker uses the **`./superenum`** script and then enters a text file name "**`Target.txt`**" having a target IP address or a list of IP addresses for enumeration.


./superenum - Parrot Terminal
File Edit View Search Terminal Help
Running script
File containing target IP address

```
┌─[root@parrot]─[/home/attacker/SuperEnum]
└──╼ #./superenum
Enter IP List filename with path
Target.txt

TCP Scan Started for IP: 10.10.1.19
```

Figure 4.30: Screenshot of SuperEnum running a script

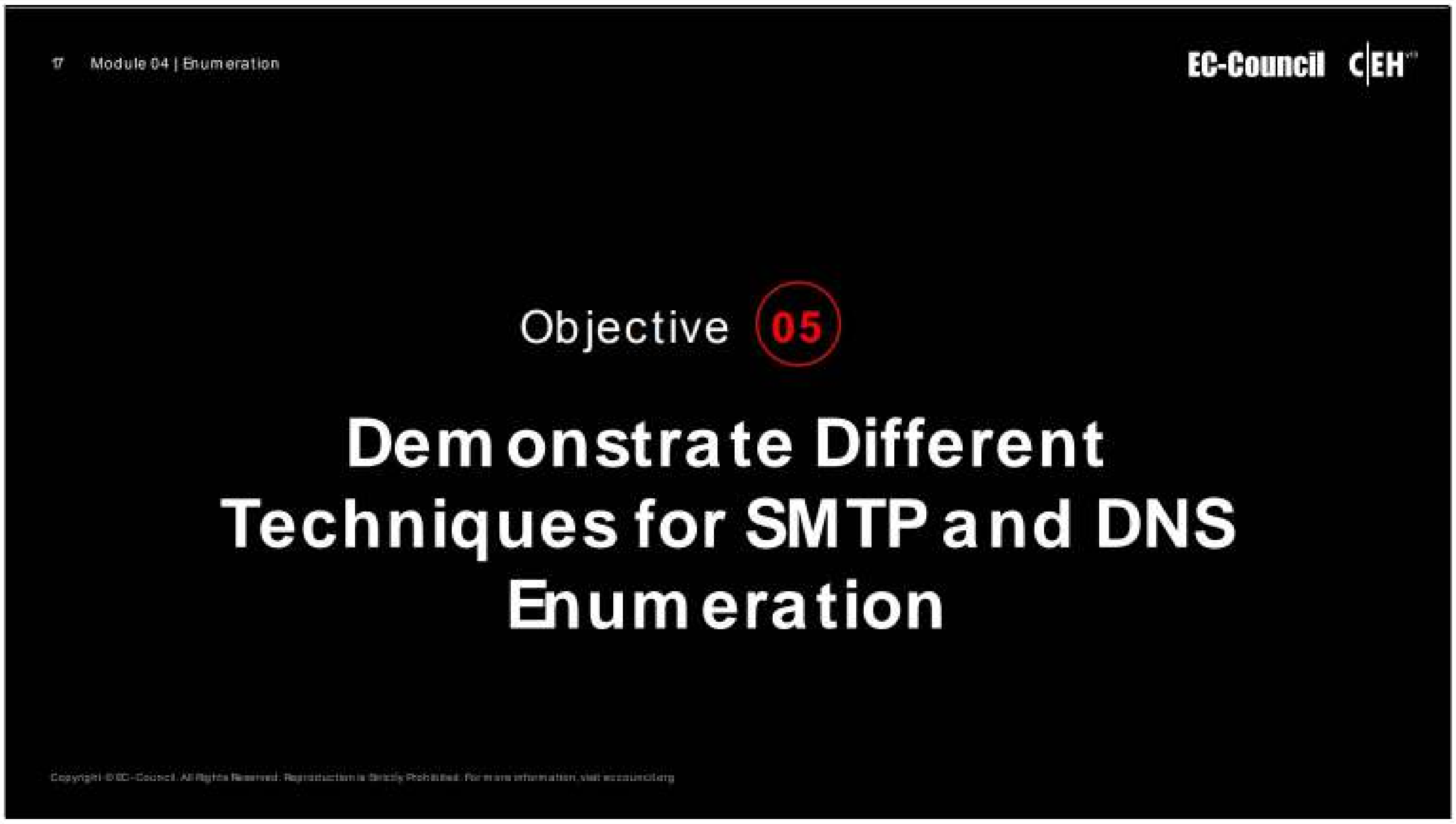
After scanning a target IP address, the script displays all the open ports, as shown in the below screenshot. Port 2049 has an NFS service running.


./superenum - Parrot Terminal
File Edit View Search Terminal Help
Open NFS Port

```
Testing for 10.10.1.19: 1801
15-03-2024/10.10.1.19/open_ports/1801/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2049
Testing for 10.10.1.19: 2049, Tool: nmap_nfs-ls
Testing for 10.10.1.19: 2049, Tool: nmap_nfs-statfs
Testing for 10.10.1.19: 2049, Tool: showmount
```

Figure 4.31: Screenshot of SuperEnum displaying open NFS ports

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



EC-Council C|EH

Objective 05

Demonstrate Different Techniques for SMTP and DNS Enumeration

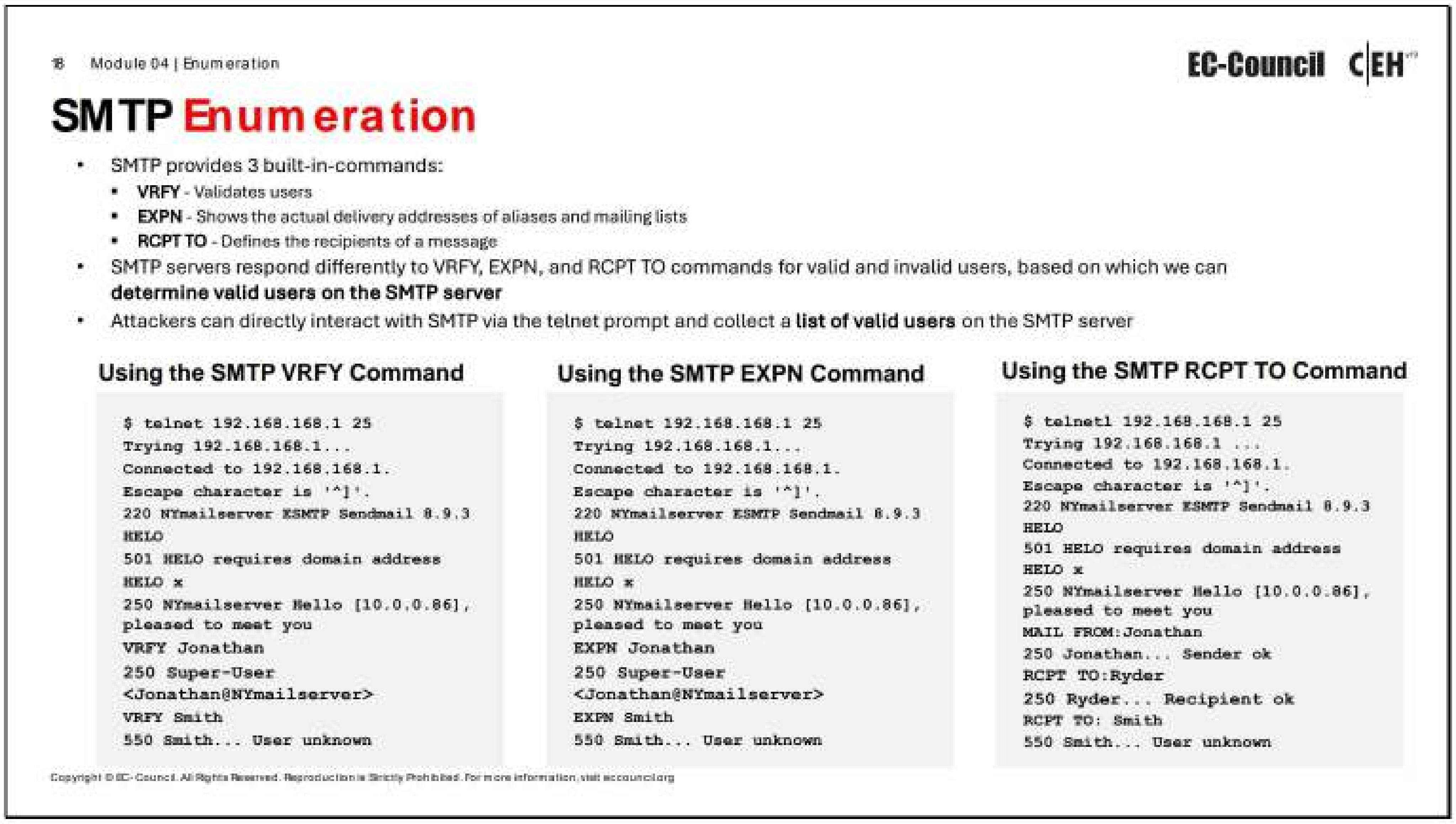
Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

SMTP and DNS Enumeration

This section describes enumeration techniques to extract information related to network resources. It also covers DNS enumeration techniques that yield information about the DNS servers and network infrastructure of the target organization. The section discusses both SMTP and DNS enumeration techniques, covering SMTP enumeration, the process of obtaining a list of valid users on an SMTP server, SMTP enumeration tools, DNS zone transfer enumeration, DNS cache snooping, and DNS zone walking.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24



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
```

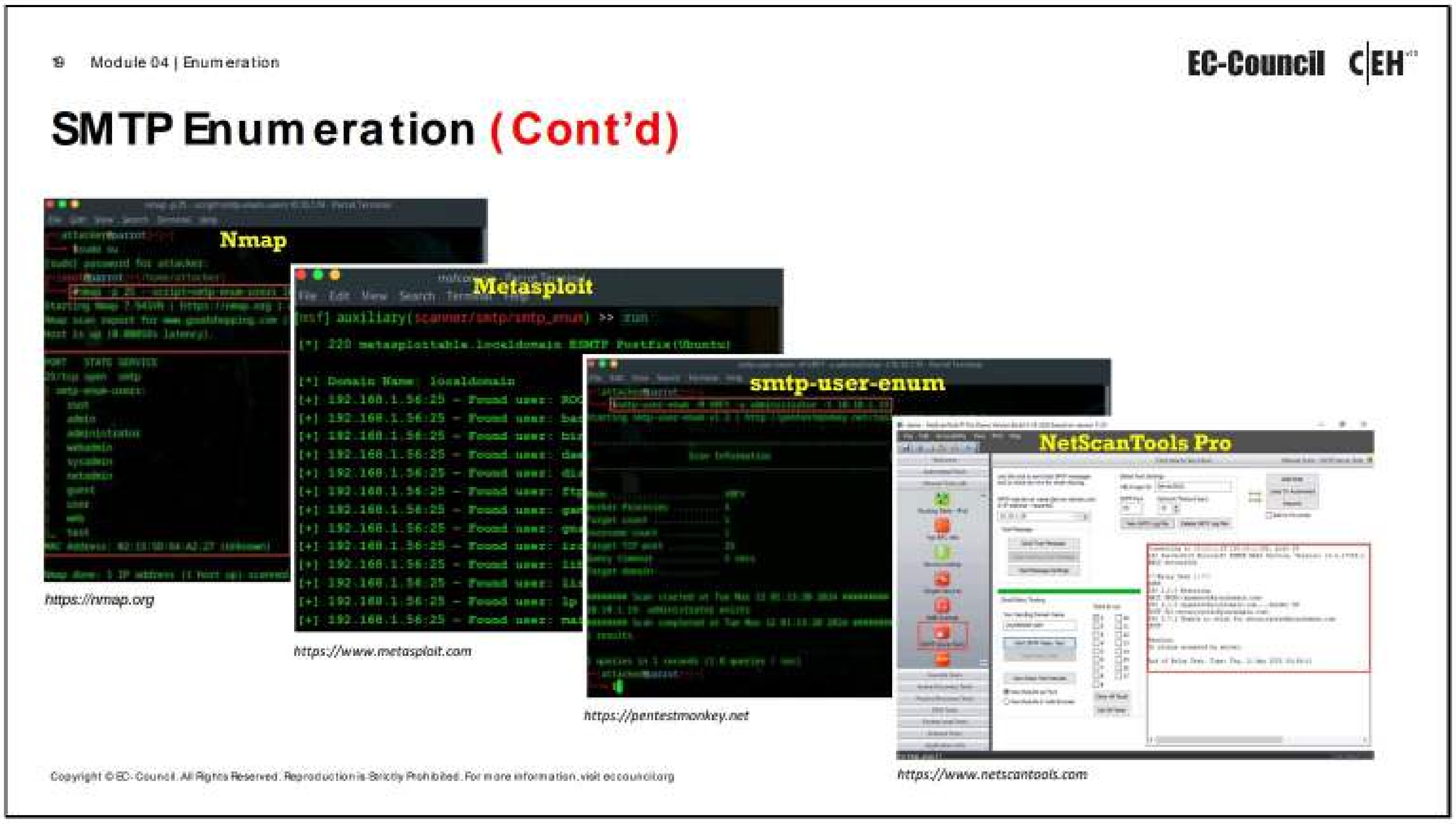
Using the SMTP EXPN Command

```
$ 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
```

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org



SMTP Enumeration (Cont'd)

```
msf] auxiliary(scanner/smtp/smtp_enum) >> run

[*] 220 metasploittable.localdomain ESMTP Postfix(Ubuntu)

[*] Domain Name: localdomain
[+] 192.168.1.56:25 - Found user: ROO
[+] 192.168.1.56:25 - Found user: bac
[+] 192.168.1.56:25 - Found user: bi
[+] 192.168.1.56:25 - Found user: da
[+] 192.168.1.56:25 - Found user: di
[+] 192.168.1.56:25 - Found user: ftp
[+] 192.168.1.56:25 - Found user: ga
[+] 192.168.1.56:25 - Found user: gn
[+] 192.168.1.56:25 - Found user: ir
[+] 192.168.1.56:25 - Found user: li
[+] 192.168.1.56:25 - Found user: li
[+] 192.168.1.56:25 - Found user: lp
[+] 192.168.1.56:25 - Found user: ma
```

https://nmap.org

https://www.metasploit.com

https://pentestmonkey.net

https://www.netscantools.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

SMTP Enumeration

Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail exchange (MX) servers to direct mail via DNS. It runs on TCP port 25, 2525, or 587.

SMTP provides the following three built-in commands.

- **VRFY:** Validates users

```
$ 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
```

- **EXPN:** Displays the actual delivery addresses of aliases and mailing lists

```
$ 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
```

- **RCPT TO:** Defines the recipients of the message

```
$ 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
```

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24

```
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 servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users; therefore, valid users on the SMTP server can be determined. Attackers can directly interact with SMTP via the Telnet prompt and collect a list of valid users on the SMTP server.

Administrators and pen testers can perform SMTP enumeration using command-line utilities such as Telnet and netcat or by using tools such as Metasploit, Nmap, NetScanTools Pro, and smtp-user-enum to collect a list of valid users, delivery addresses, message recipients, etc.

SMTP Enumeration using Nmap

Source: *https://nmap.org*

Attackers use Nmap to enumerate information from the target SMTP server. They enumerate the target SMTP server using various SMTP commands available with Nmap Scripting Engine (NSE) scripts.

- The following command, when executed, lists all the SMTP commands available in the Nmap directory:

  ```
  nmap -p 25, 365, 587 -script=smtp-commands <Target IP Address >
  ```

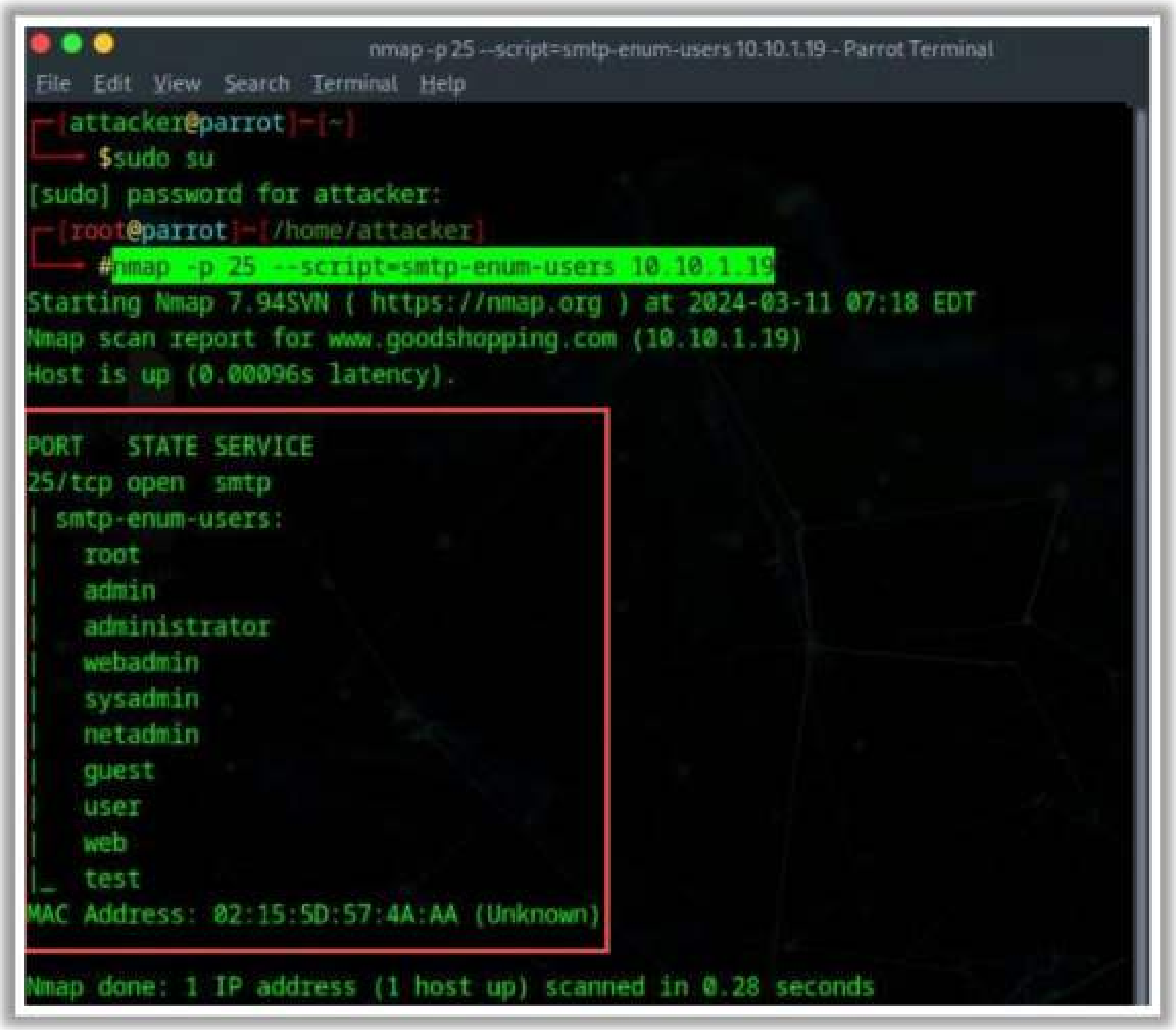
- Run the following command to identify SMTP open relays:

  ```
  nmap -p 25 -script=smtp-open-relay <Target IP Address>
  ```

- Run the following command to enumerate all the mail users on the SMTP server:

  ```
  nmap -p 25 –script=smtp-enum-users <Target IP Address>
  ```

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.


nmap -p 25 --script=smtp-enum-users 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -p 25 --script=smtp-enum-users 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-11 07:18 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00096s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| smtp-enum-users:
|   root
|   admin
|   administrator
|   webadmin
|   sysadmin
|   netadmin
|   guest
|   user
|   web
|_  test
MAC Address: 02:15:5D:57:4A:AA (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Figure 4.32: Screenshot showing output of the smtp-enum-users NSE script

SMTP Enumeration using Metasploit

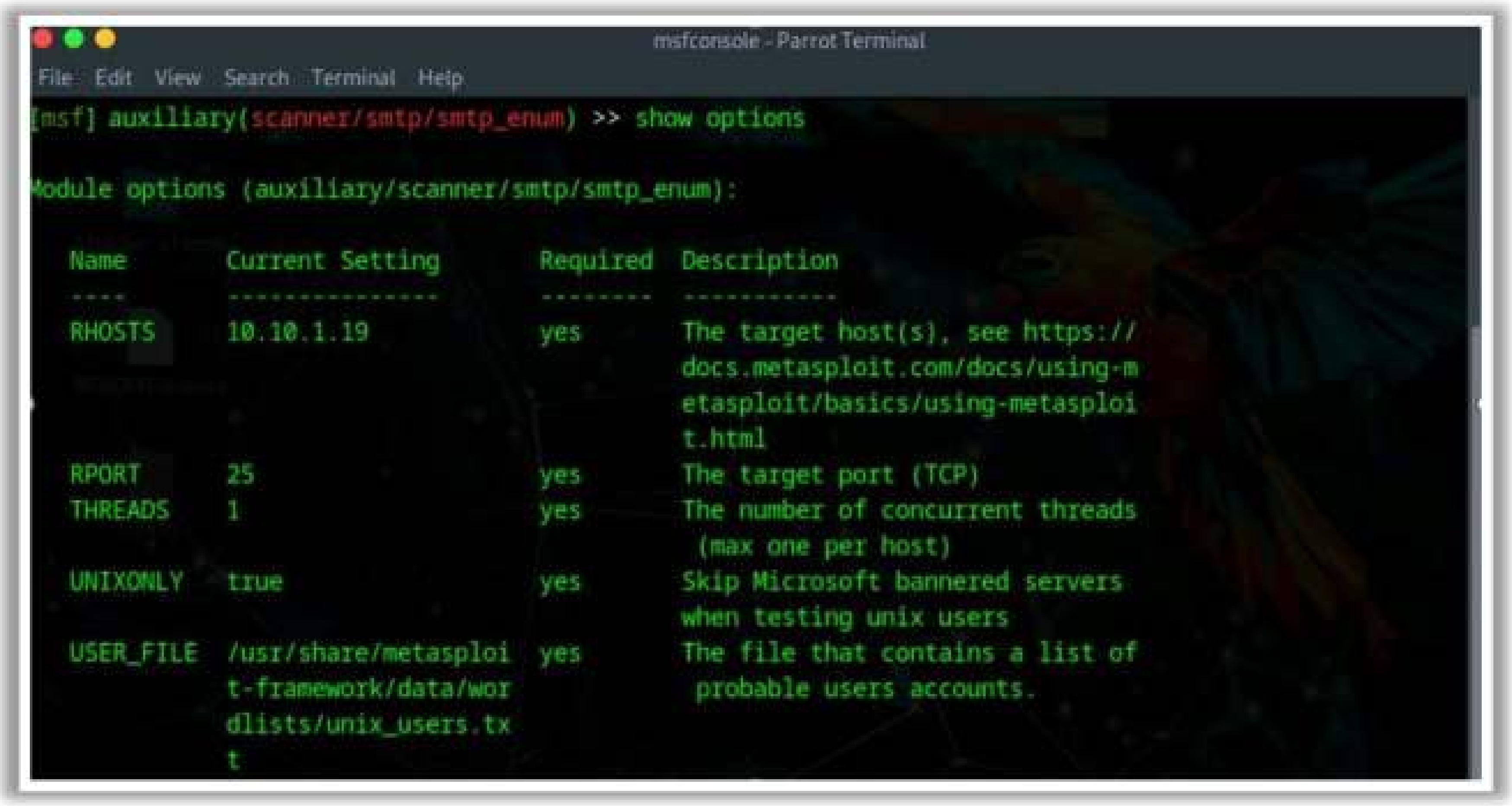
Attackers use the Metasploit framework to enumerate SMTP users. The framework contains an SMTP enumeration module that allows attackers to connect to the target SMTP server and enumerate usernames using predefined wordlists. The SMTP server uses its inbuilt method **VRFY** to validate the usernames in the wordlist file with the users present on the server and displays the matched list of users.

Steps to Enumerate SMTP Users Using Metasploit

- **Step 1**: Launch Metasploit `msfconsole` and switch to the relevant auxiliary scanner to initiate the process: `auxiliary/scanner/smtp/smtp_enum`.

  ```
  msf > use auxiliary/scanner/smtp/smtp_enum
  msf auxiliary(smtp_enum) >
  ```

- **Step 2**: Use the command `show options` to view the entire list of options required to perform this task. Alternatively, the command `show evasion` can be used to view the list of options to evade security solutions.


msfconsole - Parrot Terminal
File Edit View Search Terminal Help

```
[msf] auxiliary(scanner/smtp/smtp_enum) >> show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting      Required  Description
   ----       ---------------      --------  -----------
   RHOSTS     10.10.1.19           yes       The target host(s), see https://
                                             docs.metasploit.com/docs/using-m
                                             etasploit/basics/using-metasploi
                                             t.html
   RPORT      25                   yes       The target port (TCP)
   THREADS    1                    yes       The number of concurrent threads
                                              (max one per host)
   UNIXONLY   true                 yes       Skip Microsoft bannered servers
                                             when testing unix users
   USER_FILE  /usr/share/metasploi yes       The file that contains a list of
              t-framework/data/wor            probable users accounts.
              dlists/unix_users.tx
              t
```

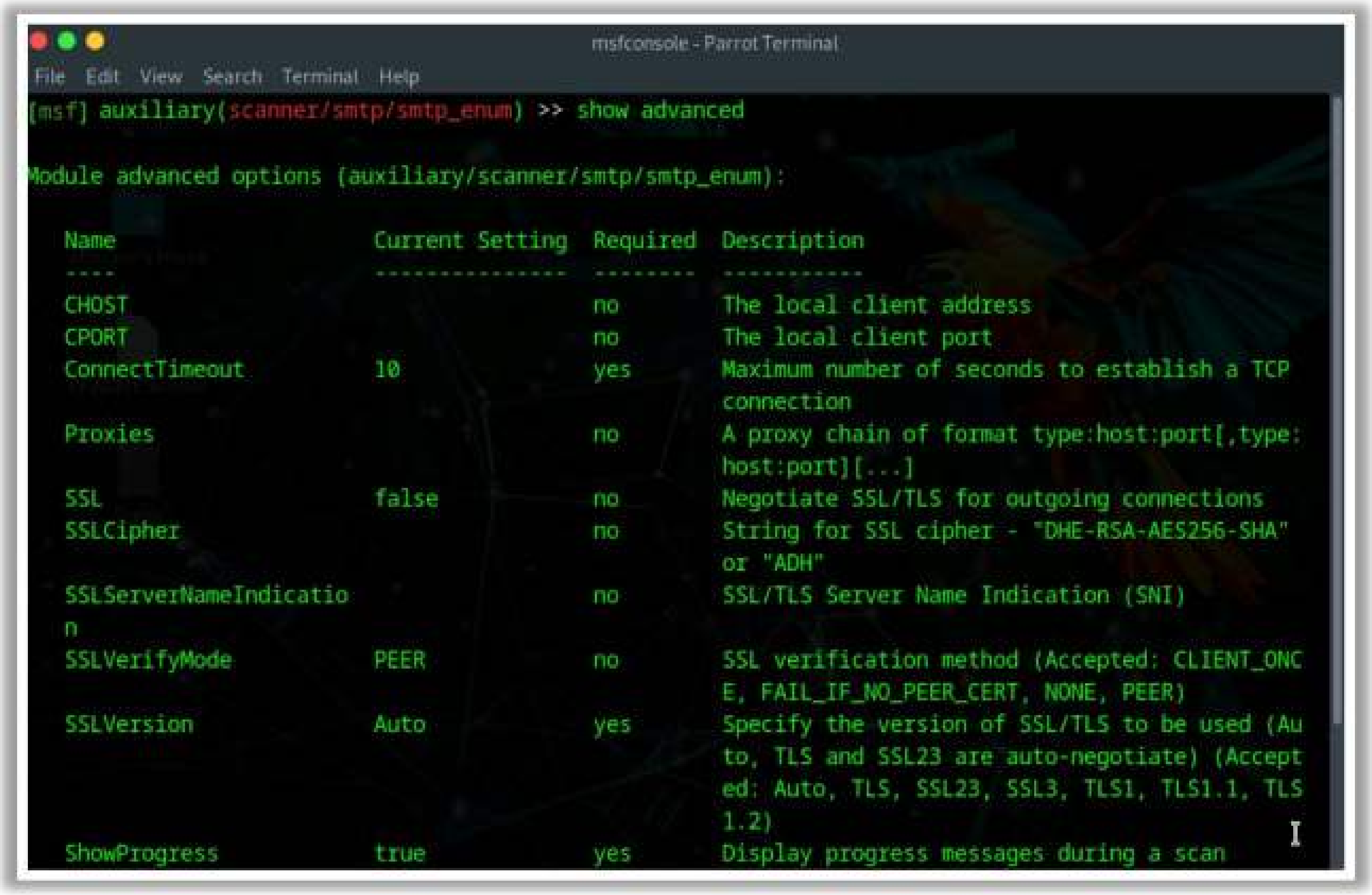
Figure 4.33: Screenshot of Metasploit showing smtp_enum options

- **Step 3:** Use the option `set RHOST` to set the target SMTP server's IP address or a range of IP addresses.

- **Step 4:** By default, the Metasploit framework uses default wordlists located at `/usr/share/60etasploit-framework/data/wordlists/unix_users.txt` to enumerate SMTP users. The `USER _FILE` option can be set to use custom wordlists.

  ```
  msf auxiliary(smtp_enum) > set USER_FILE <location of wordlists file>
  ```

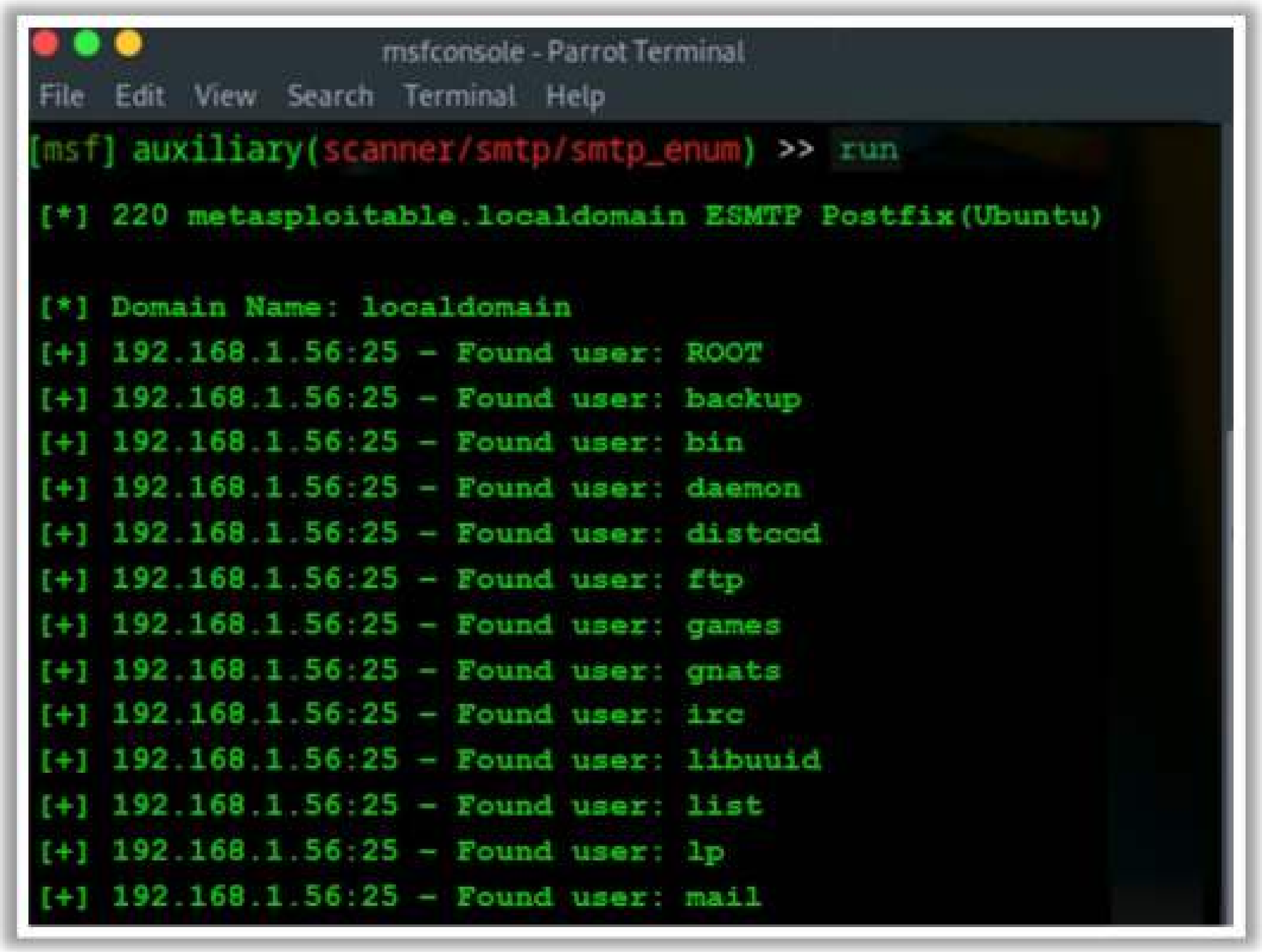
- **Step 5**: Use the command `show advanced` to view the complete list of available options in the SMTP user enumeration module.



```
[msf] auxiliary(scanner/smtp/smtp_enum) >> show advanced

Module advanced options (auxiliary/scanner/smtp/smtp_enum):

   Name                    Current Setting  Required  Description
   ----                    ---------------  --------  -----------
   CHOST                                    no        The local client address
   CPORT                                    no        The local client port
   ConnectTimeout          10               yes       Maximum number of seconds to establish a TCP
                                                      connection
   Proxies                                  no        A proxy chain of format type:host:port[,type:
                                                      host:port][...]
   SSL                     false            no        Negotiate SSL/TLS for outgoing connections
   SSLCipher                                no        String for SSL cipher - "DHE-RSA-AES256-SHA"
                                                      or "ADH"
   SSLServerNameIndicatio                   no        SSL/TLS Server Name Indication (SNI)
   n
   SSLVerifyMode           PEER             no        SSL verification method (Accepted: CLIENT_ONC
                                                      E, FAIL_IF_NO_PEER_CERT, NONE, PEER)
   SSLVersion              Auto             yes       Specify the version of SSL/TLS to be used (Au
                                                      to, TLS and SSL23 are auto-negotiate) (Accept
                                                      ed: Auto, TLS, SSL23, SSL3, TLS1, TLS1.1, TLS
                                                      1.2)
   ShowProgress            true             yes       Display progress messages during a scan
```

Figure 4.34: Screenshot of Metasploit showing smtp_enum advanced options

- **Step 6:** Execute the **`run`** command to begin the enumeration process. It scans the given wordlists with the SMTP server users and lists all the matched usernames.



```
[msf] auxiliary(scanner/smtp/smtp_enum) >> run

[*] 220 metasploitable.localdomain ESMTP Postfix(Ubuntu)

[*] Domain Name: localdomain
[+] 192.168.1.56:25 - Found user: ROOT
[+] 192.168.1.56:25 - Found user: backup
[+] 192.168.1.56:25 - Found user: bin
[+] 192.168.1.56:25 - Found user: daemon
[+] 192.168.1.56:25 - Found user: distccd
[+] 192.168.1.56:25 - Found user: ftp
[+] 192.168.1.56:25 - Found user: games
[+] 192.168.1.56:25 - Found user: gnats
[+] 192.168.1.56:25 - Found user: irc
[+] 192.168.1.56:25 - Found user: libuuid
[+] 192.168.1.56:25 - Found user: list
[+] 192.168.1.56:25 - Found user: lp
[+] 192.168.1.56:25 - Found user: mail
```

Figure 4.35: Screenshot of Metasploit retrieving SMTP users

As shown in the screenshot, attackers obtain a list of valid SMTP users from the target SMTP server and can use this information to initiate targeted attacks.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24

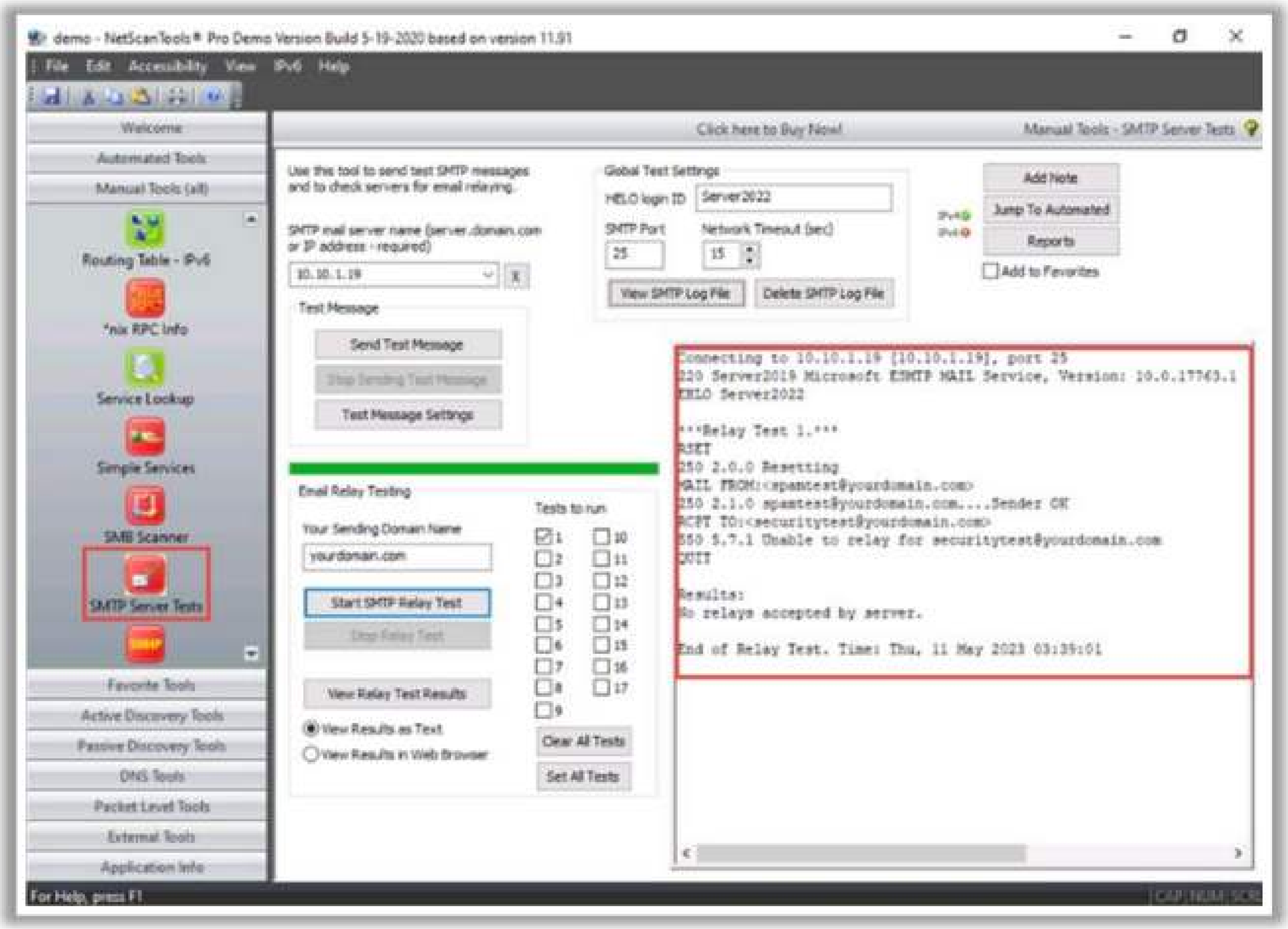
SMTP Enumeration Tools

SMTP enumeration tools are used to perform username enumeration. Attackers can use the usernames obtained from this enumeration to launch further attacks on other systems in the network.

- **NetScanTools Pro**

  Source: *https://www.netscantools.com*

  NetScanTools Pro's SMTP Email Generator tool tests the process of sending an email message through an SMTP server. Attackers use NetScanTools Pro for SMTP enumeration and extract all the email header parameters, including confirm/urgent flags. Attackers can also record the email session in a log file and then view the communications between NetScanTools Pro and the SMTP server in the log file.



Use this tool to send test SMTP messages and to check servers for email relaying.

SMTP mail server name (server.domain.com or IP address - required): 10.10.1.19

HELO login ID: Server2022

SMTP Port: 25

Network Timeout (sec): 15

☐ Add to Favorites

Your Sending Domain Name: yourdomain.com

☑ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16 ☐ 17

● View Results as Text
○ View Results in Web Browser

```
onnecting to 10.10.1.19 [10.10.1.19], port 25
20 Server2019 Microsoft ESMTP MAIL Service, Version: 10.0.17763.1
ELO Server2022

**Relay Test 1.***
SET
50 2.0.0 Resetting
AIL FROM:<spamtest@yourdomain.com>
50 2.1.0 spamtest@yourdomain.com....Sender OK
CPT TO:<securitytest@yourdomain.com>
50 5.7.1 Unable to relay for securitytest@yourdomain.com
UIT

esults:
o relays accepted by server.

nd of Relay Test. Time: Thu, 11 May 2023 03:35:01
```

Figure 4.36: Screenshot of NetScanTools Pro

- **smtp-user-enum**

  Source: *https://pentestmonkey.net*

  smtp-user-enum is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail). Enumeration is performed by inspecting the responses to VRFY, EXPN, and RCPT TO commands. As shown in the screenshot, smtp-user-enum needs to be passed on to a list of users and at least one target running an SMTP service.

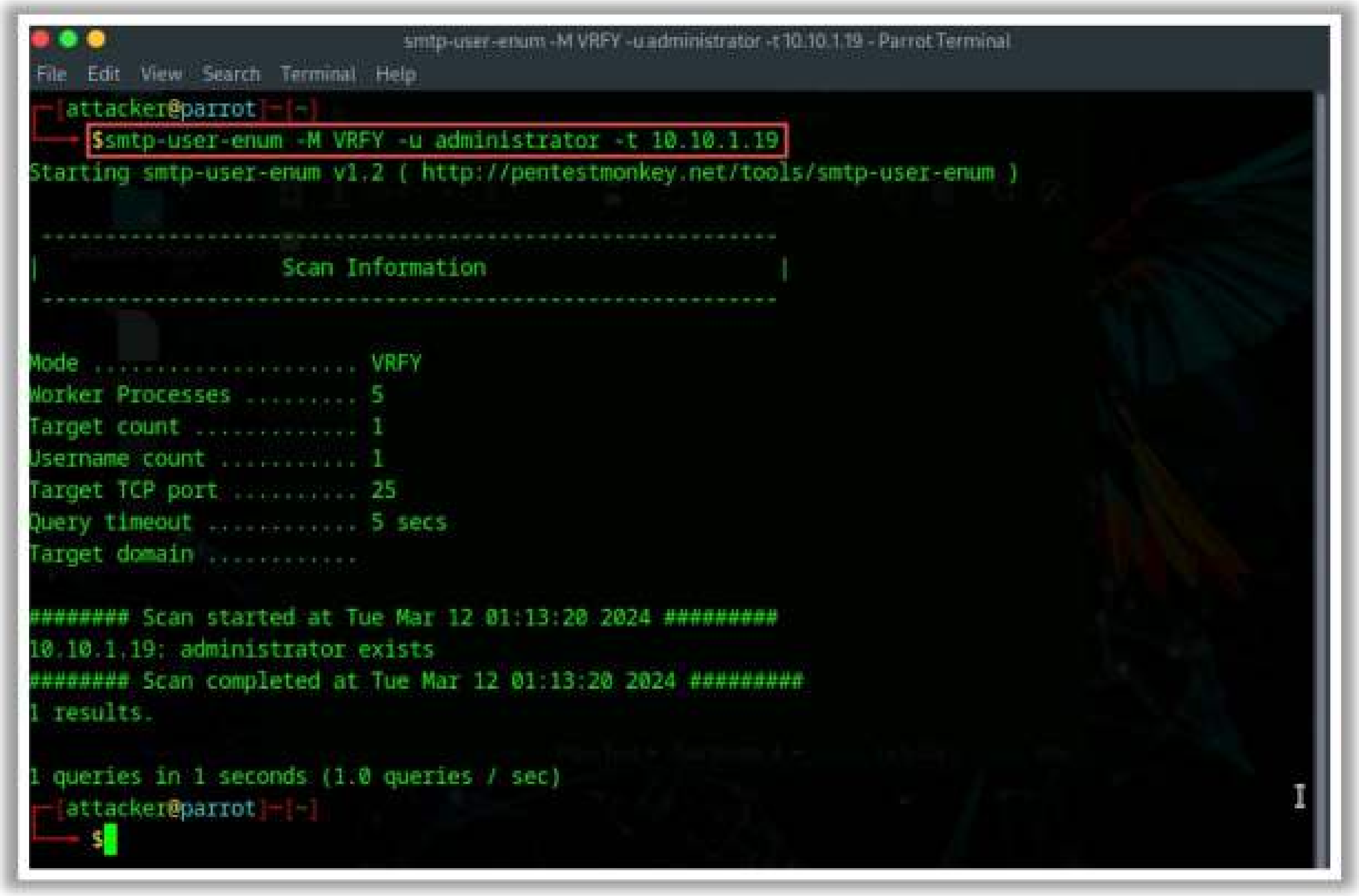
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The syntax for using smtp-user-enum is as follows:

```
smtp-user-enum.pl [options] (-u username|-U file-of-usernames) (-
t host|-T file-of-targets)
```

smtp-user-enum has the following options:

- **-m n**: Maximum number of processes (default: 5)
- **-M mode**: Specify the SMTP command to use for username guessing from among EXPN, VRFY, and RCPT TO (default: VRFY)
- **-u user**: Check if a user exists on the remote system
- **-f addr**: Specify the from email address to use for "RCPT TO" guessing (default: user@example.com)
- **-D dom**: Specify the domain to append to the supplied user list to create email addresses (default: none)
- **-U file**: Select the file containing usernames to check via the SMTP service
- **-t host**: Specify the server host running the SMTP service
- **-T file**: Select the file containing hostnames running the SMTP service
- **-p port**: Specify the TCP port on which the SMTP service runs (default: 25)
- **-d**: Debugging output
- **-t n**: Wait for a maximum of n seconds for the reply (default: 5)
- **-v**: Verbose
- **-h**: Help message

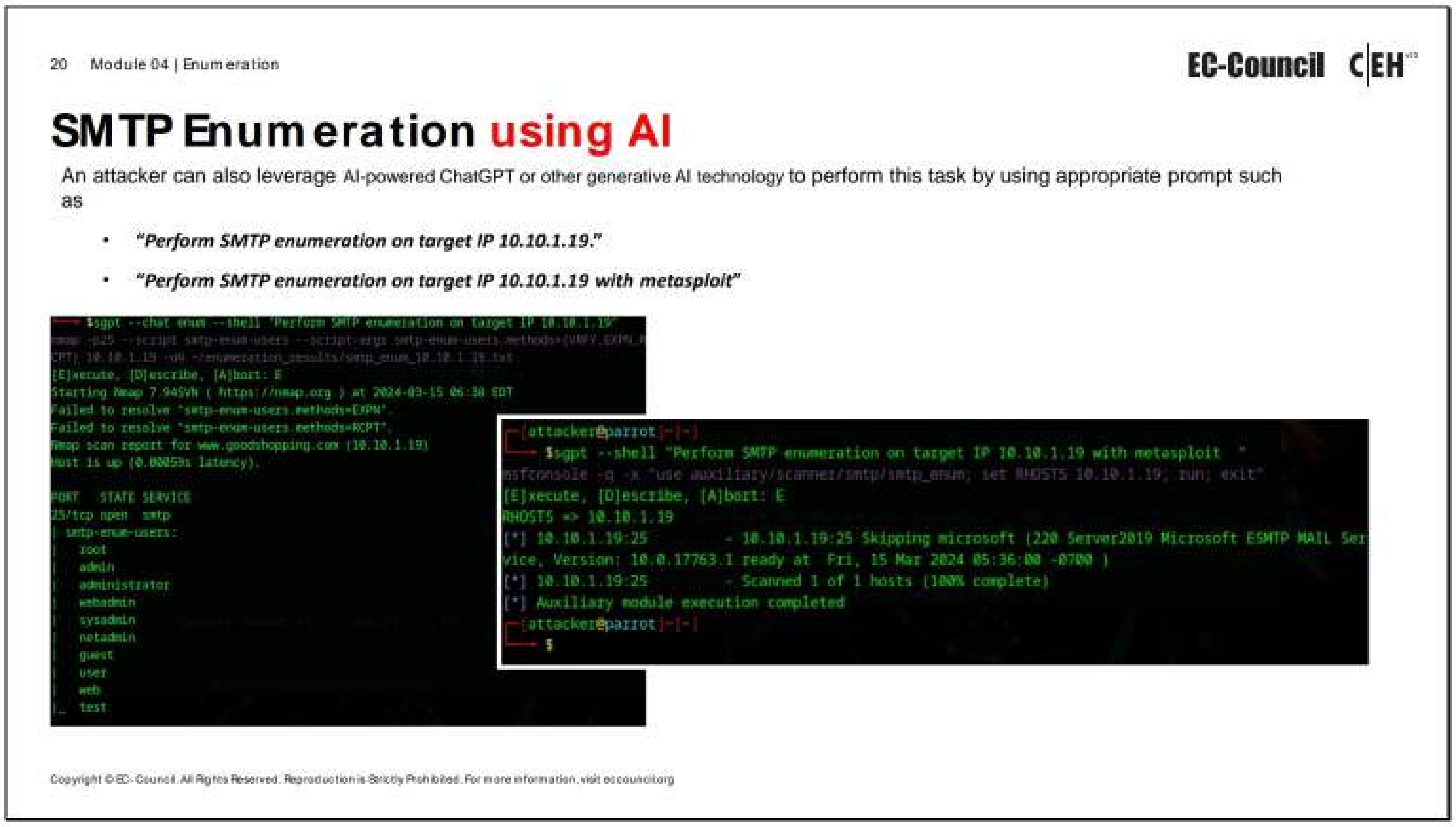

smtp-user-enum -M VRFY -u administrator -t 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $smtp-user-enum -M VRFY -u administrator -t 10.10.1.19
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Tue Mar 12 01:13:20 2024 #########
10.10.1.19: administrator exists
######## Scan completed at Tue Mar 12 01:13:20 2024 #########
1 results.

1 queries in 1 seconds (1.0 queries / sec)
┌─[attacker@parrot]─[~]
└──╼ $
```

Figure 4.37: Screenshot of smtp-user-enum

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24



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"*

```
$sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19"
nmap -p25 --script smtp-enum-users --script-args smtp-enum-users.methods={VRFY,EXPN,R
CPT} 10.10.1.19 -oN ~/enumeration_results/smtp_enum_10.10.1.19.txt
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 06:30 EDT
Failed to resolve "smtp-enum-users.methods=EXPN".
Failed to resolve "smtp-enum-users.methods=RCPT".
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00059s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| smtp-enum-users:
|   root
|   admin
|   administrator
|   webadmin
|   sysadmin
|   netadmin
|   guest
|   user
|   web
|_  test
```

```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --shell "Perform SMTP enumeration on target IP 10.10.1.19 with metasploit  "
msfconsole -q -x "use auxiliary/scanner/smtp/smtp_enum; set RHOSTS 10.10.1.19; run; exit"
[E]xecute, [D]escribe, [A]bort: E
RHOSTS => 10.10.1.19
[*] 10.10.1.19:25         - 10.10.1.19:25 Skipping microsoft (220 Server2019 Microsoft ESMTP MAIL Ser
vice, Version: 10.0.17763.1 ready at  Fri, 15 Mar 2024 05:36:00 -0700 )
[*] 10.10.1.19:25         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
┌─[attacker@parrot]─[~]
└──╼ $
```

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

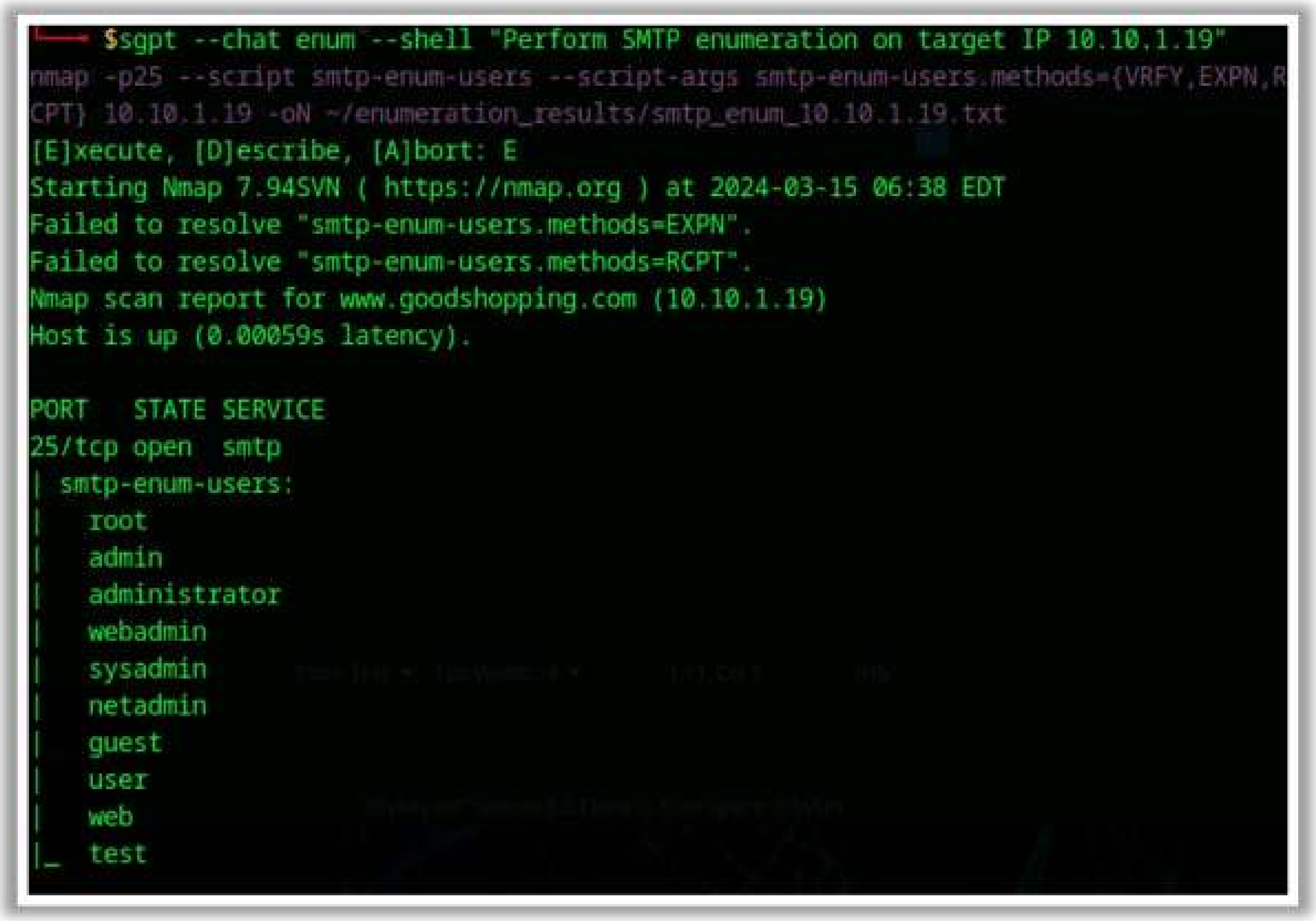
SMTP Enumeration using AI

Attackers can leverage AI-powered technologies to enhance and automate their network enumeration tasks. With the aid of AI, attackers can effortlessly perform SMTP enumeration and gather SMTP user information on target IP addresses.

Attackers can use ChatGPT to perform this task by using appropriate prompts such as:

Example #1:

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



```
└──╼ $sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19"
nmap -p25 --script smtp-enum-users --script-args smtp-enum-users.methods={VRFY,EXPN,R
CPT} 10.10.1.19 -oN ~/enumeration_results/smtp_enum_10.10.1.19.txt
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 06:38 EDT
Failed to resolve "smtp-enum-users.methods=EXPN".
Failed to resolve "smtp-enum-users.methods=RCPT".
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00059s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| smtp-enum-users:
|   root
|   admin
|   administrator
|   webadmin
|   sysadmin
|   netadmin
|   guest
|   user
|   web
|_  test
```

Figure 4.38: Perform SMTP enumeration on target IP with nmap

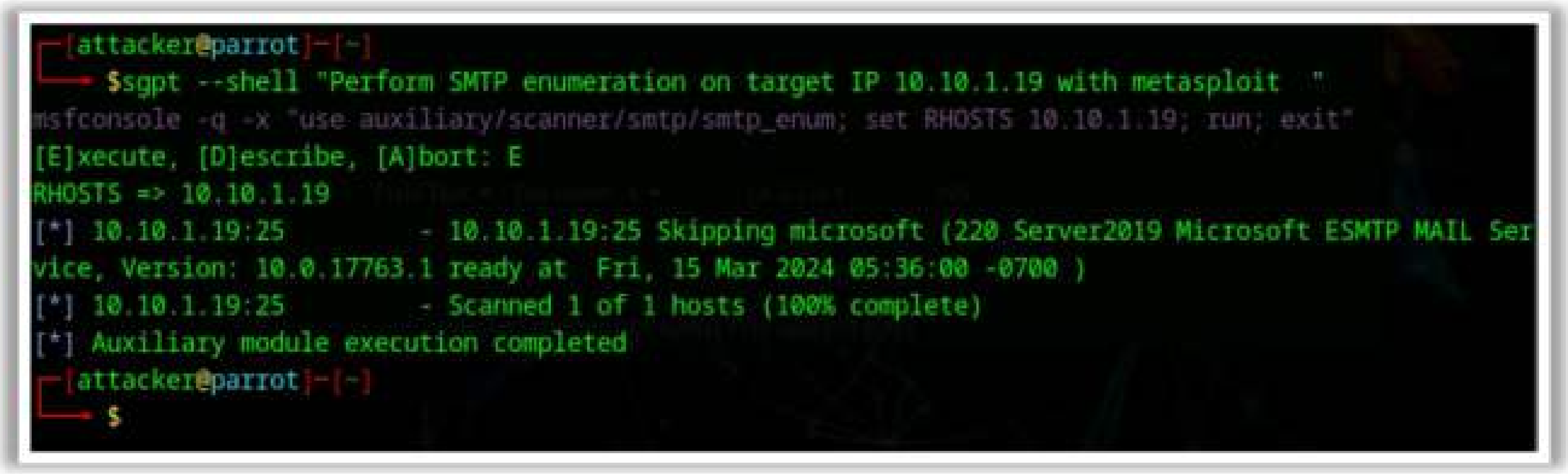
The following command is designed to automate SMTP enumeration tasks on the specified target IP:

`nmap -p25 --script smtp-enum-users --script-args smtp-enum-users.methods={VRFY, EXPN, RCPT} 10.10.1.19 -oN ~/enumeration_results/smtp_enum_10.10.1.19.txt`

This command uses **`nmap`** with specific options and script (**`smtp-enum-users`**) to perform SMTP enumeration on port 25 of the target IP 10.10.1.19. The results are saved to the file smtp_enum_10.10.1.19.txt in the ~/enumeration_results/ directory.

Example #2:

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



```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --shell "Perform SMTP enumeration on target IP 10.10.1.19 with metasploit  "
msfconsole -q -x "use auxiliary/scanner/smtp/smtp_enum; set RHOSTS 10.10.1.19; run; exit"
[E]xecute, [D]escribe, [A]bort: E
RHOSTS => 10.10.1.19
[*] 10.10.1.19:25         - 10.10.1.19:25 Skipping microsoft (220 Server2019 Microsoft ESMTP MAIL Ser
vice, Version: 10.0.17763.1 ready at  Fri, 15 Mar 2024 05:36:00 -0700 )
[*] 10.10.1.19:25         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
┌─[attacker@parrot]─[~]
└──╼ $
```

Figure 4.39: Perform SMTP enumeration on target IP with Metasploit

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following command is designed to automate SMTP enumeration tasks on the specified target IP:

```
msfconsole -q -x "use auxiliary/scanner/smtp/smtp_enum; set RHOSTS 10.10.1.19;
run; exit"
```

This command uses `msfconsole` with the `-q` option to run Metasploit in quiet mode. The `-x` option is used to specify the commands to execute within Metasploit. It sets the target IP as 10.10.1.19 and executes the `smtp_enum` auxiliary module, which performs SMTP enumeration.

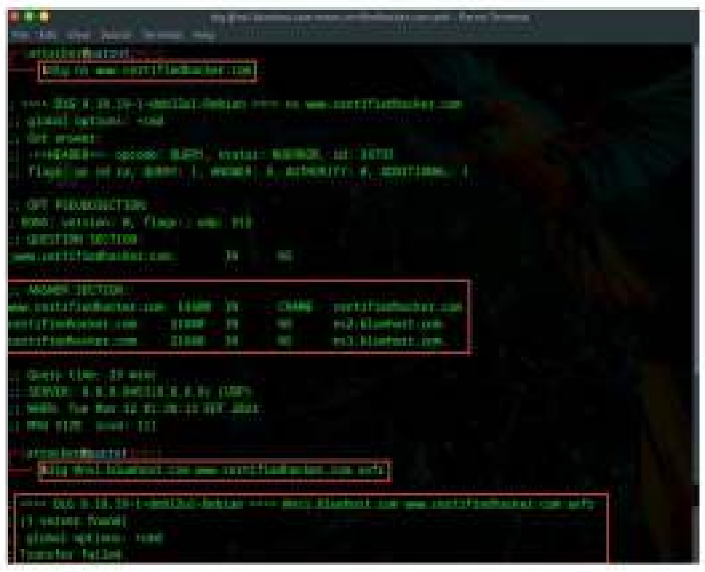
These commands automate SMTP enumeration tasks and display the results for each command executed on the specified target IP 10.10.1.19.

All Rights Reserved. Reproduction is Strictly Prohibited.

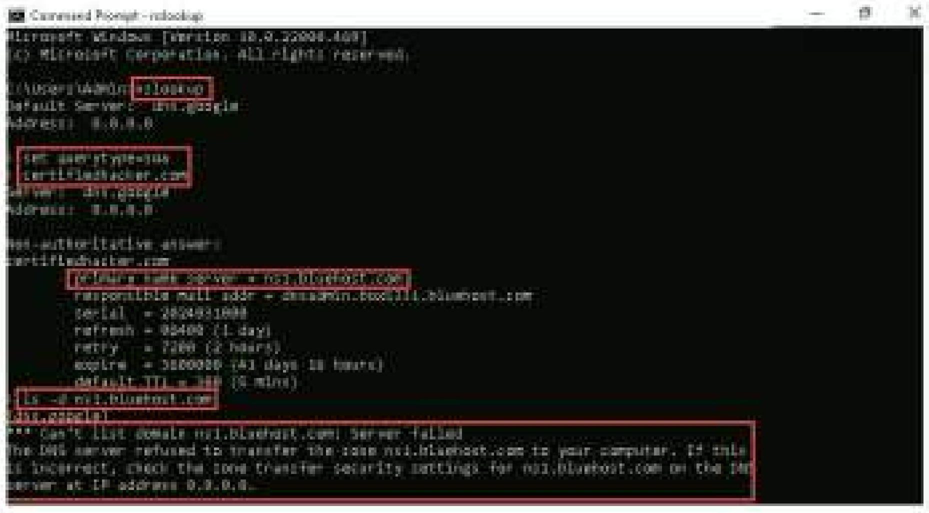
DNS Enumeration using Zone Transfer

- 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



Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

DNS Enumeration using Zone Transfer

DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. In most cases, the primary DNS server maintains a backup or secondary server for redundancy, which holds all the information stored in the primary server. The DNS server uses zone transfer to distribute changes made to the main server to the secondary server(s). An attacker performs DNS zone transfer enumeration to locate the DNS server and access records of the target organization. If the DNS server of the target organization allows zone transfers, then attackers can perform DNS zone transfer to obtain DNS server names, hostnames, machine names, usernames, IP addresses, aliases, etc. assigned within a target domain.

In DNS enumeration using zone transfer, an attacker attempts to retrieve a copy of the entire zone file for a domain from the DNS server. Attackers can perform DNS zone transfer using tools such as nslookup, dig command, and DNSRecon. If the DNS transfer setting is enabled on the target name server, it will provide the DNS information; else, it will return an error stating it has failed or refused the zone transfer.

To perform a DNS zone transfer, the attacker sends a zone-transfer request to the DNS server pretending to be a client; the DNS server then sends a portion of its database as a zone to the attacker. This zone may contain a large amount of information about the DNS zone network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

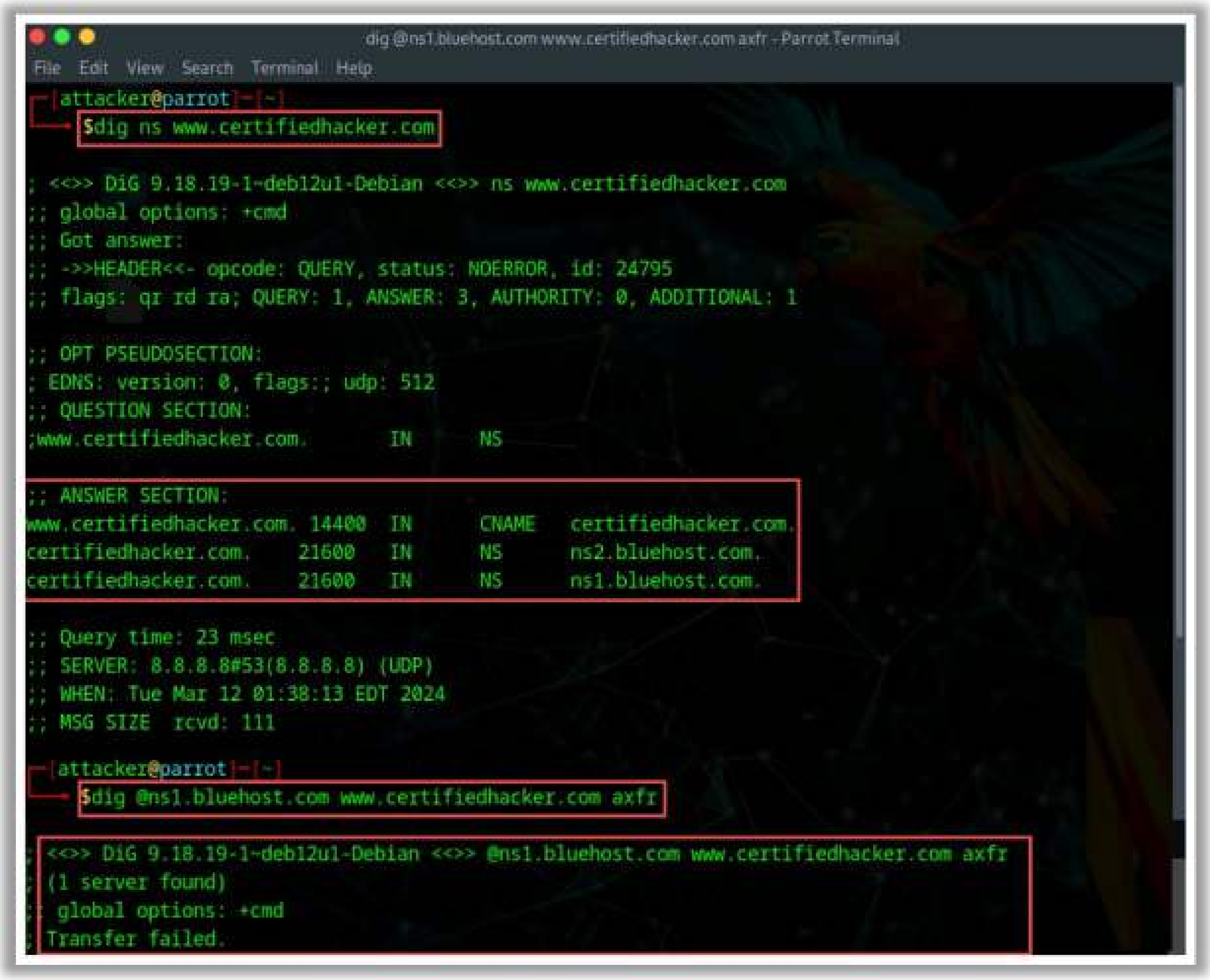
- **dig Command**

  Attackers use the `dig` command on Linux-based systems to query the DNS name servers and retrieve information about the target host addresses, name servers, mail exchanges, etc. As shown in the screenshot, attackers use the following command to perform DNS zone transfer:

  ```
  dig ns <target domain>
  ```

  The above command retrieves all the DNS name servers of the target domain. Next, attackers use one of the name servers from the output of the above command to test whether the target DNS allows zone transfers. They use the following command for this purpose:

  ```
  dig @<domain of name server> <target domain> axfr
  ```


dig @ns1.bluehost.com www.certifiedhacker.com axfr - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $dig ns www.certifiedhacker.com

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> ns www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24795
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com.       IN      NS

;; ANSWER SECTION:
www.certifiedhacker.com. 14400  IN      CNAME   certifiedhacker.com.
certifiedhacker.com.    21600   IN      NS      ns2.bluehost.com.
certifiedhacker.com.    21600   IN      NS      ns1.bluehost.com.

;; Query time: 23 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Tue Mar 12 01:38:13 EDT 2024
;; MSG SIZE  rcvd: 111

┌─[attacker@parrot]─[~]
└──╼ $dig @ns1.bluehost.com www.certifiedhacker.com axfr

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> @ns1.bluehost.com www.certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

Figure 4.40: Screenshot of Linux DNS zone transfer using dig command

- **nslookup Command**

  Source: *https://docs.microsoft.com*

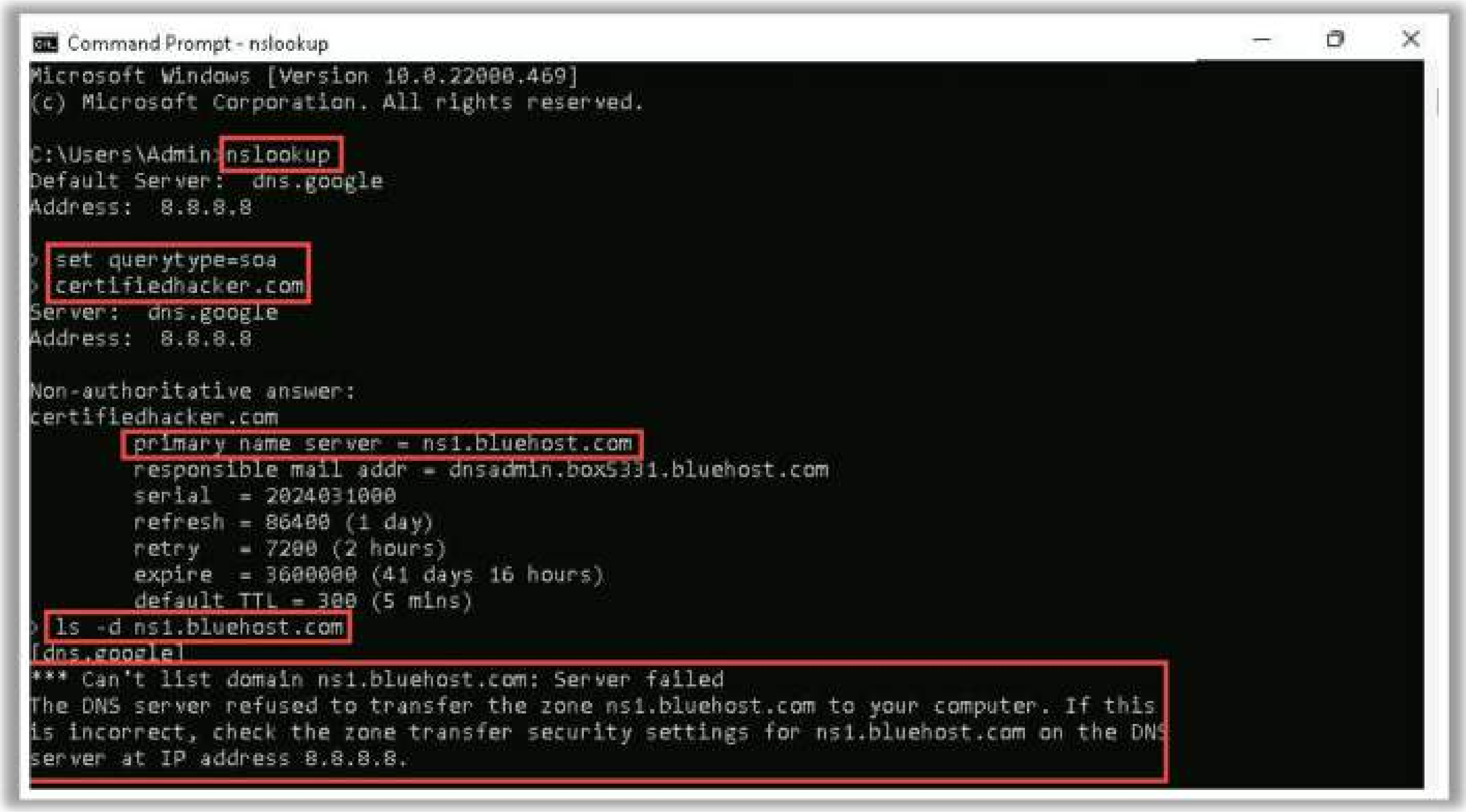
  Attackers use the nslookup command on Windows-based systems to query the DNS name servers and retrieve information about the target host addresses, name servers, mail exchanges, etc. As shown in the screenshot, attackers use the following command to perform DNS zone transfer:

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
nslookup
set querytype=soa
<target domain>
```

The above command sets the query type to the Start of Authority (SOA) record to retrieve administrative information about the DNS zone of the target domain **`certifiedhacker.com`**. The following command is used to attempt to transfer the zone of the specified name server:

```
/ls -d <domain of name server>
```



```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set querytype=soa
> certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
certifiedhacker.com
        primary name server = ns1.bluehost.com
        responsible mail addr = dnsadmin.box5331.bluehost.com
        serial  = 2024031000
        refresh = 86400 (1 day)
        retry   = 7200 (2 hours)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
> ls -d ns1.bluehost.com
[dns.google]
*** Can't list domain ns1.bluehost.com: Server failed
The DNS server refused to transfer the zone ns1.bluehost.com to your computer. If this
is incorrect, check the zone transfer security settings for ns1.bluehost.com on the DNS
server at IP address 8.8.8.8.
```

Figure 4.41: Screenshot of Windows DNS zone transfer using the nslookup command

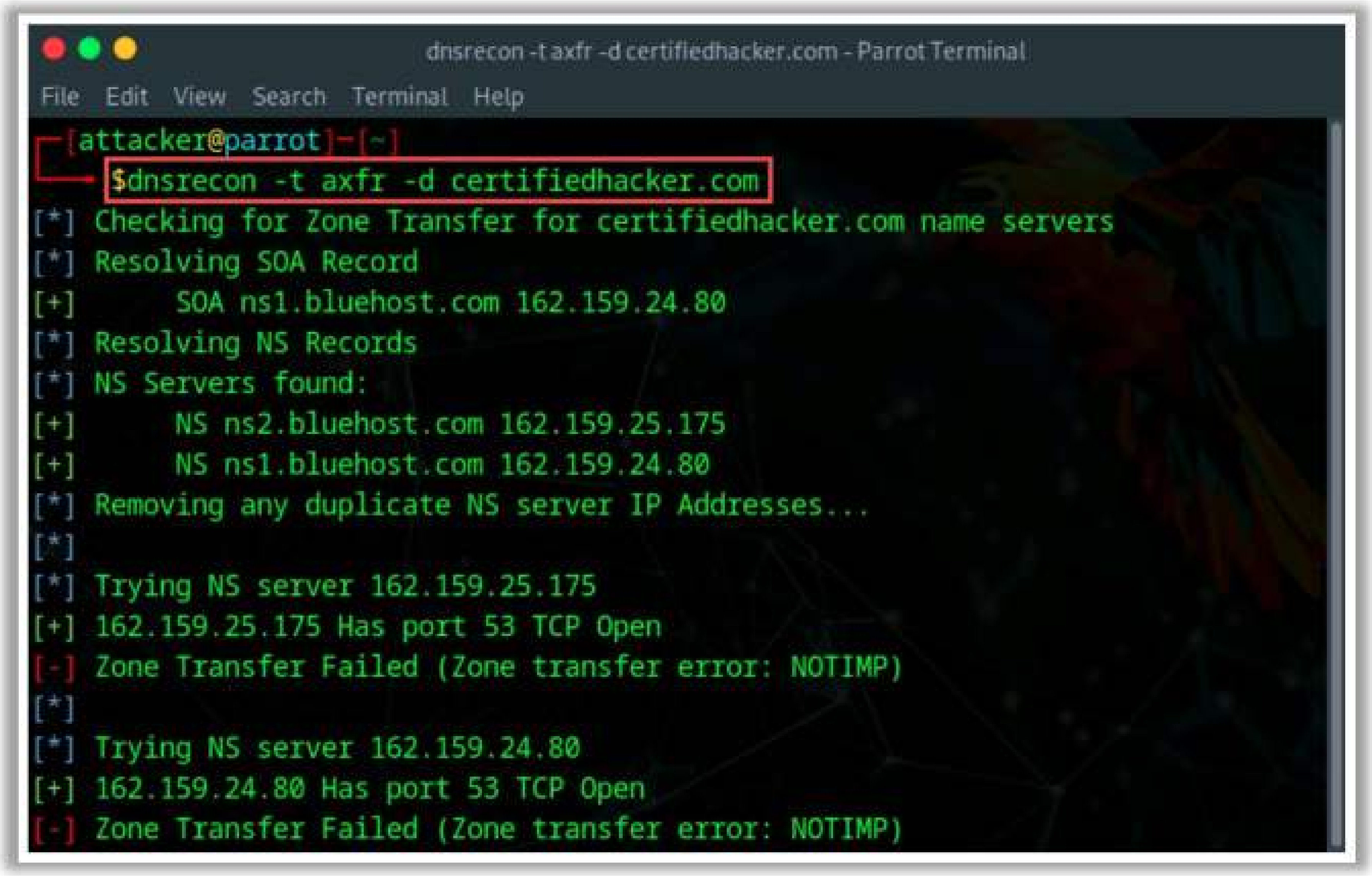
- **DNSRecon**

  Source: *https://github.com*

  Attackers use DNSRecon to check all NS records of the target domain for zone transfers. As shown in the screenshot, attackers use the following command for DNS zone transfer:

  ```
  dnsrecon -t axfr -d <target domain>
  ```

  In the above command, the **`-t`** option specifies the type of enumeration to be performed, **`axfr`** is the type of enumeration in which all NS servers are tested for a zone transfer, and the **`-d`** option specifies the target domain.


dnsrecon -t axfr -d certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $dnsrecon -t axfr -d certifiedhacker.com
[*] Checking for Zone Transfer for certifiedhacker.com name servers
[*] Resolving SOA Record
[+]      SOA ns1.bluehost.com 162.159.24.80
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS ns2.bluehost.com 162.159.25.175
[+]      NS ns1.bluehost.com 162.159.24.80
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 162.159.25.175
[+] 162.159.25.175 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: NOTIMP)
[*]
[*] Trying NS server 162.159.24.80
[+] 162.159.24.80 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: NOTIMP)
```

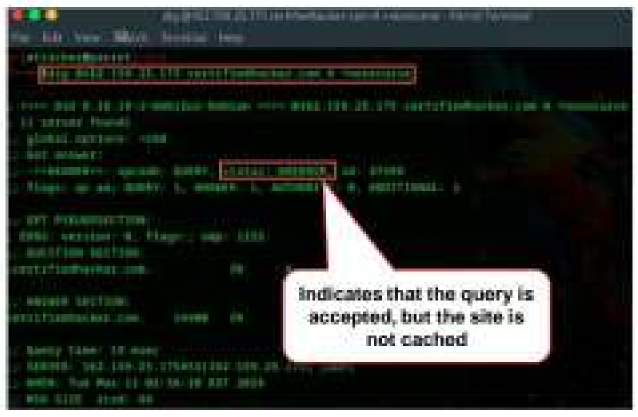
Figure 4.42: Screenshot of DNS zone transfer using DNSRecon

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

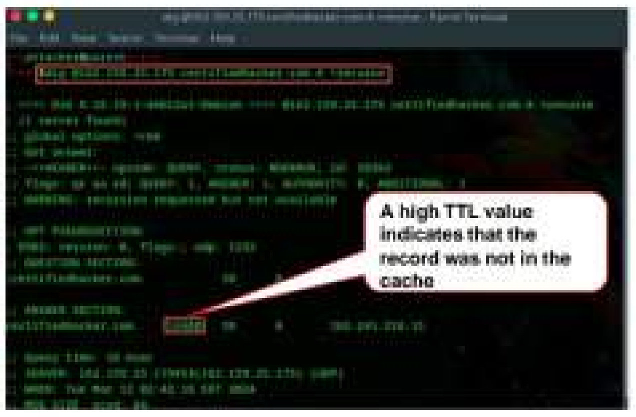
DNS Cache Snooping

- 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



Indicates that the query is accepted, but the site is not cached



A high TTL value indicates that the record was not in the cache

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

DNS Cache Snooping

DNS cache snooping is a type of DNS enumeration technique in which an attacker queries the DNS server for a specific cached DNS record. By using this cached record, the attacker can determine the sites recently visited by the user. This information can further reveal important information such as the name of the owner of the DNS server, its service provider, the name of its vendor, and bank details. By using this information, the attacker can perform a social engineering attack on the target user. Attackers perform DNS cache snooping using various tools such as the dig command, and DNSRecon.

Attackers use the following two DNS cache snooping methods to snoop on a target domain.

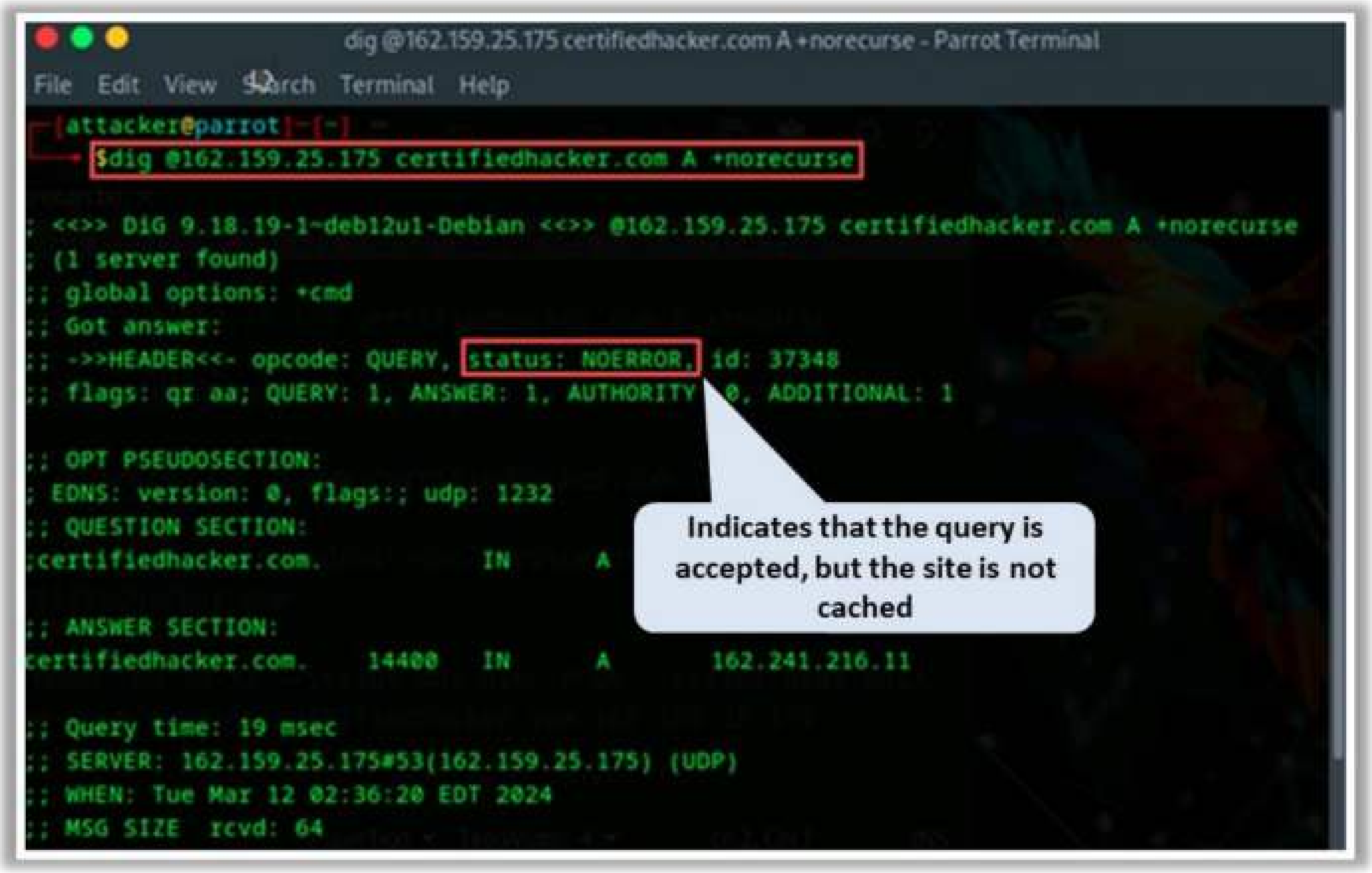
- **Non-recursive Method**

  In this method, to snoop on a DNS server, attackers send a non-recursive query by setting the Recursion Desired (RD) bit in the query header to zero. Attackers query the DNS cache for a specific DNS record such as A, CNAME, PTR, CERT, SRV, and MX. If the queried record is present in the DNS cache, the DNS server responds with the information indicating that some user on the system has visited a specific domain. Otherwise, the DNS server responds with the information about another DNS server that can return an answer to the query, or it replies with the `root.hints` file containing information about all root DNS servers.

  Attackers use the `dig` command followed by the name/IP address of the DNS server, domain name, and type of DNS record file. The `+norecurse` option is used to set the query to non-recursive.

  ```
  dig @<IP of DNS server> <Target domain> A +norecurse
  ```

As shown in the screenshot, the status `NOERROR` implies that the query was accepted but no answer was returned, thereby indicating that no user from the system had visited the queried site.


dig @162.159.25.175 certifiedhacker.com A +norecurse - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $dig @162.159.25.175 certifiedhacker.com A +norecurse

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> @162.159.25.175 certifiedhacker.com A +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37348
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY  0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;certifiedhacker.com.           IN      A

;; ANSWER SECTION:
certifiedhacker.com.    14400   IN      A       162.241.216.11

;; Query time: 19 msec
;; SERVER: 162.159.25.175#53(162.159.25.175) (UDP)
;; WHEN: Tue Mar 12 02:36:20 EDT 2024
;; MSG SIZE  rcvd: 64
```

Indicates that the query is accepted, but the site is not cached

Figure 4.43: Screenshot of a dig query for a site that is not cached

- **Recursive Method**

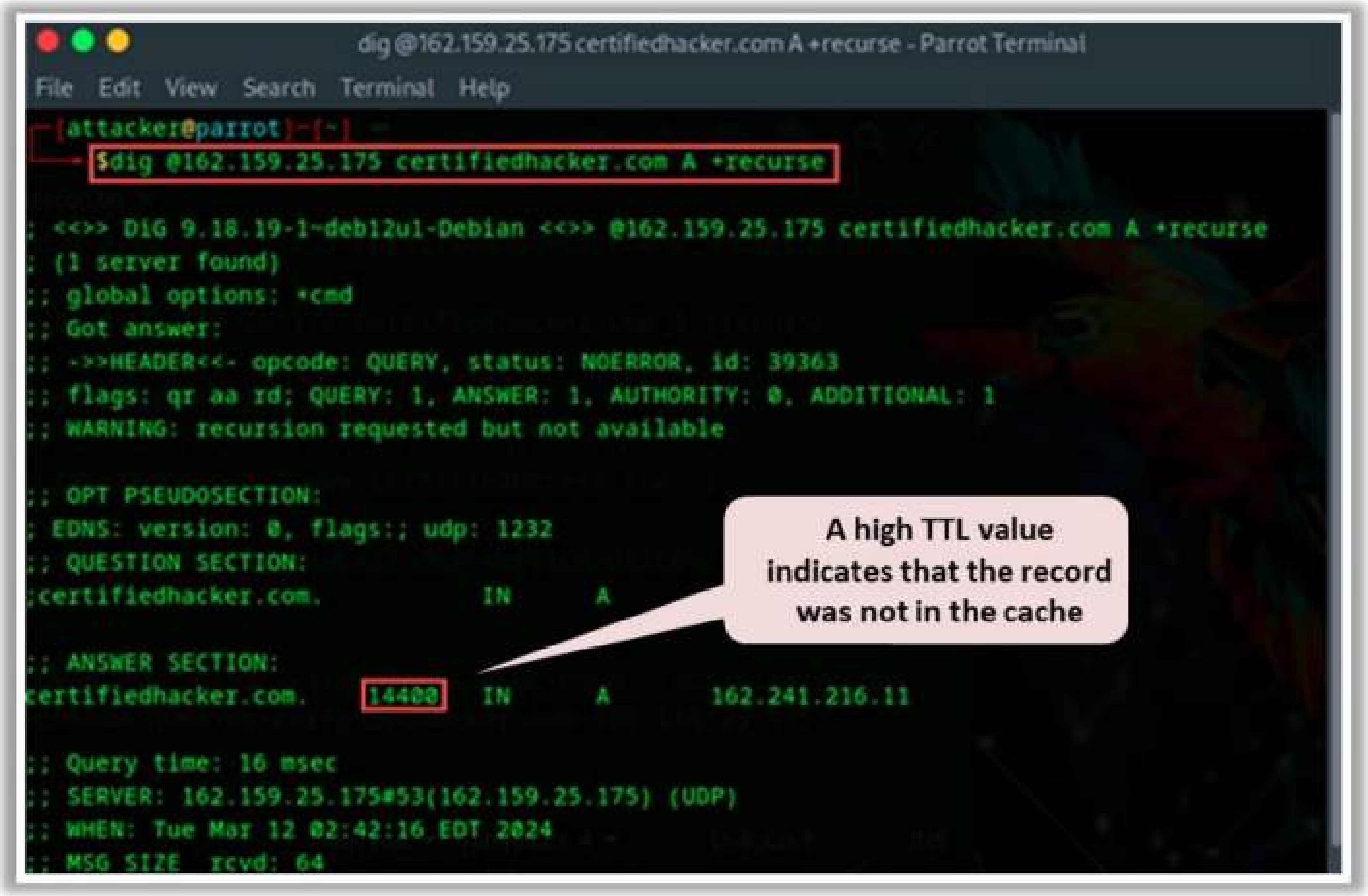
  In this method, to snoop on the DNS server, attackers send a recursive query by setting the `+recurse` option instead of the `+norecurse` option. Similar to the non-recursive method, the attackers query the DNS cache for a specific DNS record such as A, CNAME, PTR, CERT, SRV, and MX.

  In this method, the time-to-live (TTL) field is examined to determine the duration for which the DNS record remains in the cache. Here, the TTL value obtained from the result is compared with the TTL that was initially set in the TTL field. If the TTL value in the result is less than the initial TTL value, the record is cached, indicating that someone on the system has visited that site. However, if the queried record were not present in the cache, it will be added to the cache after the first query is sent.

  Attackers use the same `dig` command as in the non-recursive method but with the `+recurse` option instead of the `+norecurse` option:

  `dig @<IP of DNS server> <Target domain> A +recurse`

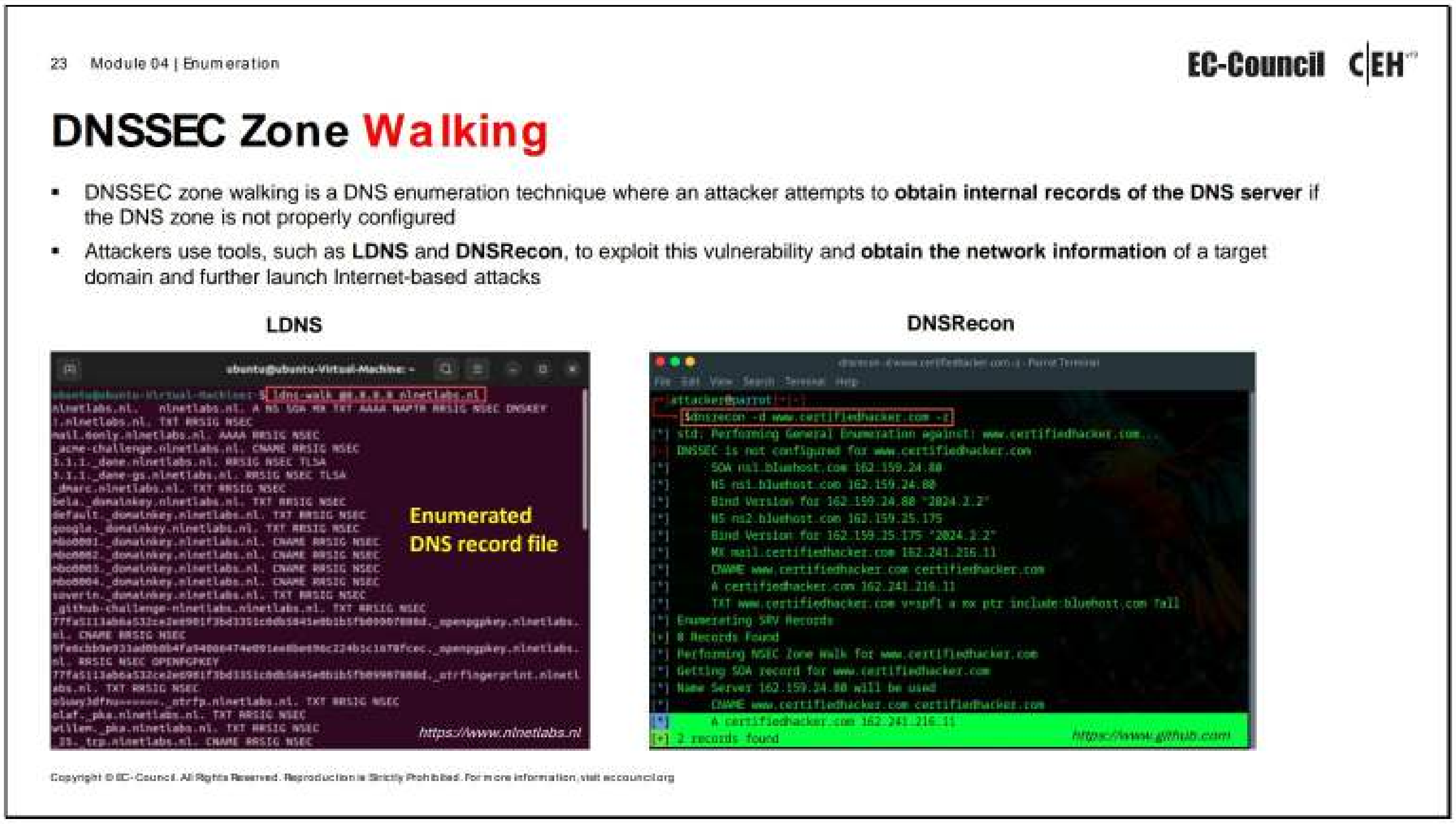
  As shown in the screenshot, the TTL value for the domain `certifiedhacker.com` is considerably high, which strongly suggests that the domain record was not in the cache when the query was issued.


dig @162.159.25.175 certifiedhacker.com A +recurse - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $dig @162.159.25.175 certifiedhacker.com A +recurse

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> @162.159.25.175 certifiedhacker.com A +recurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39363
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;certifiedhacker.com.           IN      A

;; ANSWER SECTION:
certifiedhacker.com.    14400   IN      A       162.241.216.11

;; Query time: 16 msec
;; SERVER: 162.159.25.175#53(162.159.25.175) (UDP)
;; WHEN: Tue Mar 12 02:42:16 EDT 2024
;; MSG SIZE  rcvd: 64
```

A high TTL value indicates that the record was not in the cache

Figure 4.44: Screenshot of a dig query for a cached site



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

```
ubuntu@ubuntu-Virtual-Machine:~$ ldns-walk @8.8.8.8 nlnetlabs.nl
nlnetlabs.nl.   nlnetlabs.nl. A NS SOA MX TXT AAAA NAPTR RRSIG NSEC DNSKEY
1.nlnetlabs.nl. TXT RRSIG NSEC
mail.6only.nlnetlabs.nl. AAAA RRSIG NSEC
_acme-challenge.nlnetlabs.nl. CNAME RRSIG NSEC
3.1.1._dane.nlnetlabs.nl. RRSIG NSEC TLSA
3.1.1._dane-gs.nlnetlabs.nl. RRSIG NSEC TLSA
_dmarc.nlnetlabs.nl. TXT RRSIG NSEC
bela._domainkey.nlnetlabs.nl. TXT RRSIG NSEC
default._domainkey.nlnetlabs.nl. TXT RRSIG NSEC
google._domainkey.nlnetlabs.nl. TXT RRSIG NSEC
mbo0001._domainkey.nlnetlabs.nl. CNAME RRSIG NSEC
mbo0002._domainkey.nlnetlabs.nl. CNAME RRSIG NSEC
mbo0003._domainkey.nlnetlabs.nl. CNAME RRSIG NSEC
mbo0004._domainkey.nlnetlabs.nl. CNAME RRSIG NSEC
soverin._domainkey.nlnetlabs.nl. TXT RRSIG NSEC
_github-challenge-nlnetlabs.nlnetlabs.nl. TXT RRSIG NSEC
77fa5113ab6a532ce2e0901f3bd3351c0db5845e0b1b5fb09907808d._openpgpkey.nlnetlabs.
nl. CNAME RRSIG NSEC
9fe6cbb9e933ad0b0b4fa94008474e091ee0be096c224b5c1878fcec._openpgpkey.nlnetlabs.
nl. RRSIG NSEC OPENPGPKEY
77fa5113ab6a532ce2e0901f3bd3351c0db5845e0b1b5fb09907808d._otrfingerprint.nlnetl
abs.nl. TXT RRSIG NSEC
o5uwy3dfnu======._otrfp.nlnetlabs.nl. TXT RRSIG NSEC
olaf._pka.nlnetlabs.nl. TXT RRSIG NSEC
willem._pka.nlnetlabs.nl. TXT RRSIG NSEC
_25._tcp.nlnetlabs.nl. CNAME RRSIG NSEC
```

Enumerated DNS record file

https://www.nlnetlabs.nl

DNSRecon

```
┌─[attacker@parrot]─[~]
└──╼ $dnsrecon -d www.certifiedhacker.com -z
[*] std: Performing General Enumeration against: www.certifiedhacker.com...
[-] DNSSEC is not configured for www.certifiedhacker.com
[*]      SOA ns1.bluehost.com 162.159.24.80
[*]      NS ns1.bluehost.com 162.159.24.80
[*]      Bind Version for 162.159.24.80 "2024.2.2"
[*]      NS ns2.bluehost.com 162.159.25.175
[*]      Bind Version for 162.159.25.175 "2024.2.2"
[*]      MX mail.certifiedhacker.com 162.241.216.11
[*]      CNAME www.certifiedhacker.com certifiedhacker.com
[*]      A certifiedhacker.com 162.241.216.11
[*]      TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[+] 0 Records Found
[*] Performing NSEC Zone Walk for www.certifiedhacker.com
[*] Getting SOA record for www.certifiedhacker.com
[*] Name Server 162.159.24.80 will be used
[*]      CNAME www.certifiedhacker.com certifiedhacker.com
[*]      A certifiedhacker.com 162.241.216.11
[+] 2 records found
```

https://www.github.com

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

DNSSEC Zone Walking

Domain Name System Security Extensions (DNSSEC) zone walking is a type of DNS enumeration technique in which an attacker attempts to obtain internal records if the DNS zone is not properly configured. The enumerated zone information can assist the attacker in building a host network map.

Organizations use DNSSEC to add security features to the DNS data and provide protection against known threats to the DNS. This security feature uses digital signatures based on public-key cryptography to strengthen authentication in DNS. These digital signatures are stored in the DNS name servers along with common records such as MX, A, AAAA, and CNAME.

While DNSSEC provides Internet security, it is also susceptible to a vulnerability called zone enumeration or zone walking. By exploiting this vulnerability, attackers can obtain network information of a target domain, based on which they may launch Internet-based attacks.

To overcome the zone enumeration vulnerability, a new version of DNSSEC that uses Next Secure version 3 (NSEC3) is used. The NSEC3 record provides the same functionality as NSEC records, except that it provides cryptographically hashed record names that are designed to prevent the enumeration of record names present in the zone.

To perform zone enumeration, attackers can use various DNSSEC zone enumerators such as LDNS, DNSRecon, nsec3map, nsec3walker, and DNSwalk.

DNSSEC Zone Walking Tools

DNSSEC zone walking tools are used to enumerate the target domain's DNS record files. These tools can also perform zone enumeration on NSEC and NSEC3 record files and further use the gathered information to launch attacks such as denial-of-service (DoS) attacks and phishing attacks.

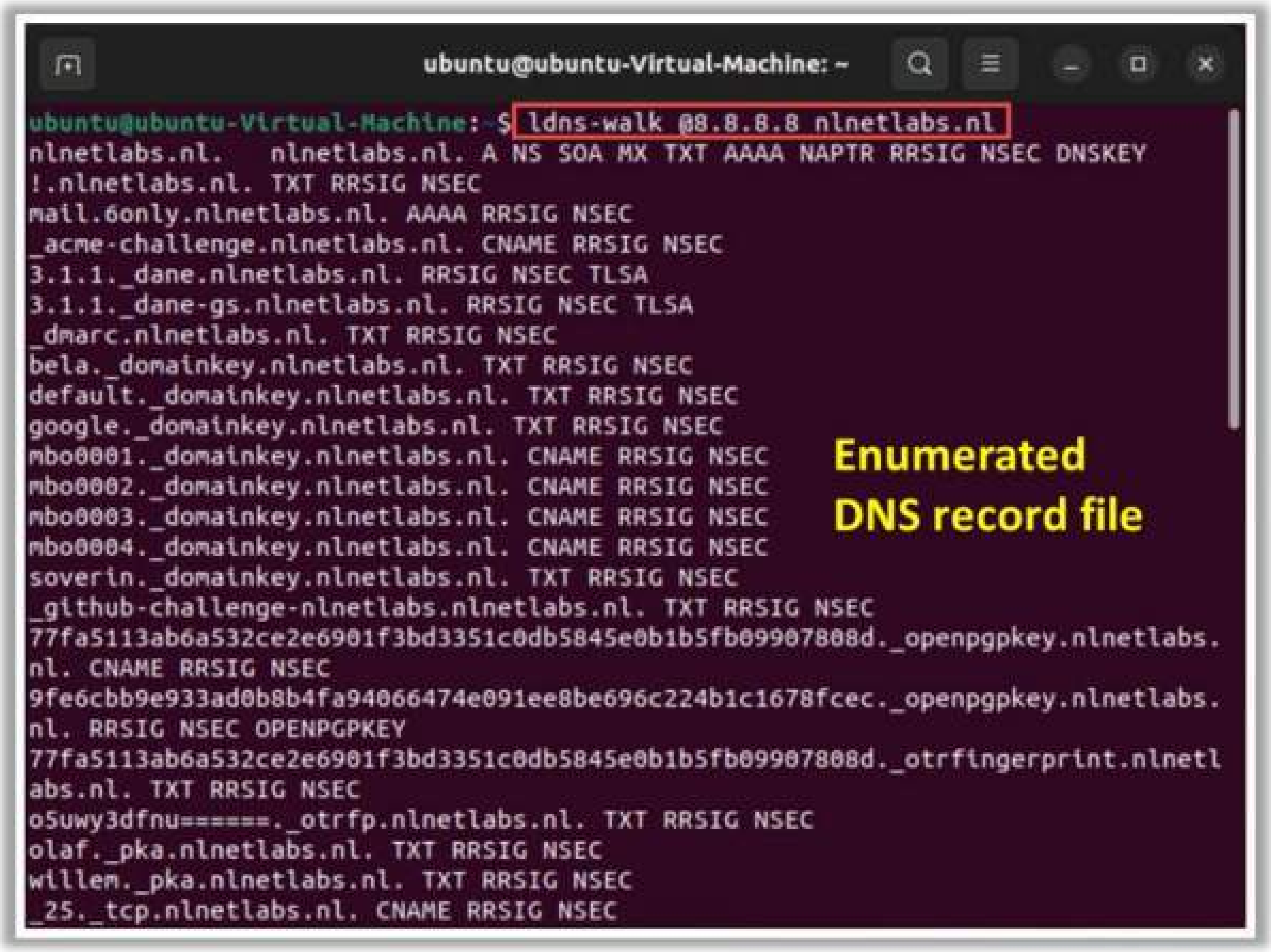
- **LDNS**

  Source: *https://www.nlnetlabs.nl*

  LDNS-walk enumerates the DNSSEC zone and obtains results on the DNS record files.

  As shown in the screenshot, attackers use the following query to enumerate a target domain **`iana.org`** using the DNS server **`8.8.8.8`** to obtain DNS record files:

  `ldns-walk @<IP of DNS Server> <Target domain>`



```
ubuntu@ubuntu-Virtual-Machine:~$ ldns-walk @8.8.8.8 nlnetlabs.nl
nlnetlabs.nl.   nlnetlabs.nl. A NS SOA MX TXT AAAA NAPTR RRSIG NSEC DNSKEY
!.nlnetlabs.nl. TXT RRSIG NSEC
mail.6only.nlnetlabs.nl. AAAA RRSIG NSEC
_acme-challenge.nlnetlabs.nl. CNAME RRSIG NSEC
3.1.1._dane.nlnetlabs.nl. RRSIG NSEC TLSA
3.1.1._dane-gs.nlnetlabs.nl. RRSIG NSEC TLSA
_dmarc.nlnetlabs.nl. TXT RRSIG NSEC
bela._domainkey.nlnetlabs.nl. TXT RRSIG NSEC
default._domainkey.nlnetlabs.nl. TXT RRSIG NSEC
google._domainkey.nlnetlabs.nl. TXT RRSIG NSEC
mbo0001._domainkey.nlnetlabs.nl. CNAME RRSIG NSEC
mbo0002._domainkey.nlnetlabs.nl. CNAME RRSIG NSEC
mbo0003._domainkey.nlnetlabs.nl. CNAME RRSIG NSEC
mbo0004._domainkey.nlnetlabs.nl. CNAME RRSIG NSEC
soverin._domainkey.nlnetlabs.nl. TXT RRSIG NSEC
_github-challenge-nlnetlabs.nlnetlabs.nl. TXT RRSIG NSEC
77fa5113ab6a532ce2e6901f3bd3351c0db5845e0b1b5fb09907808d._openpgpkey.nlnetlabs.
nl. CNAME RRSIG NSEC
9fe6cbb9e933ad0b8b4fa94066474e091ee8be696c224b1c1678fcec._openpgpkey.nlnetlabs.
nl. RRSIG NSEC OPENPGPKEY
77fa5113ab6a532ce2e6901f3bd3351c0db5845e0b1b5fb09907808d._otrfingerprint.nlnetl
abs.nl. TXT RRSIG NSEC
o5uwy3dfnu======._otrfp.nlnetlabs.nl. TXT RRSIG NSEC
olaf._pka.nlnetlabs.nl. TXT RRSIG NSEC
willem._pka.nlnetlabs.nl. TXT RRSIG NSEC
_25._tcp.nlnetlabs.nl. CNAME RRSIG NSEC
```

Figure 4.45: Screenshot of LDNS displaying results on the target domain

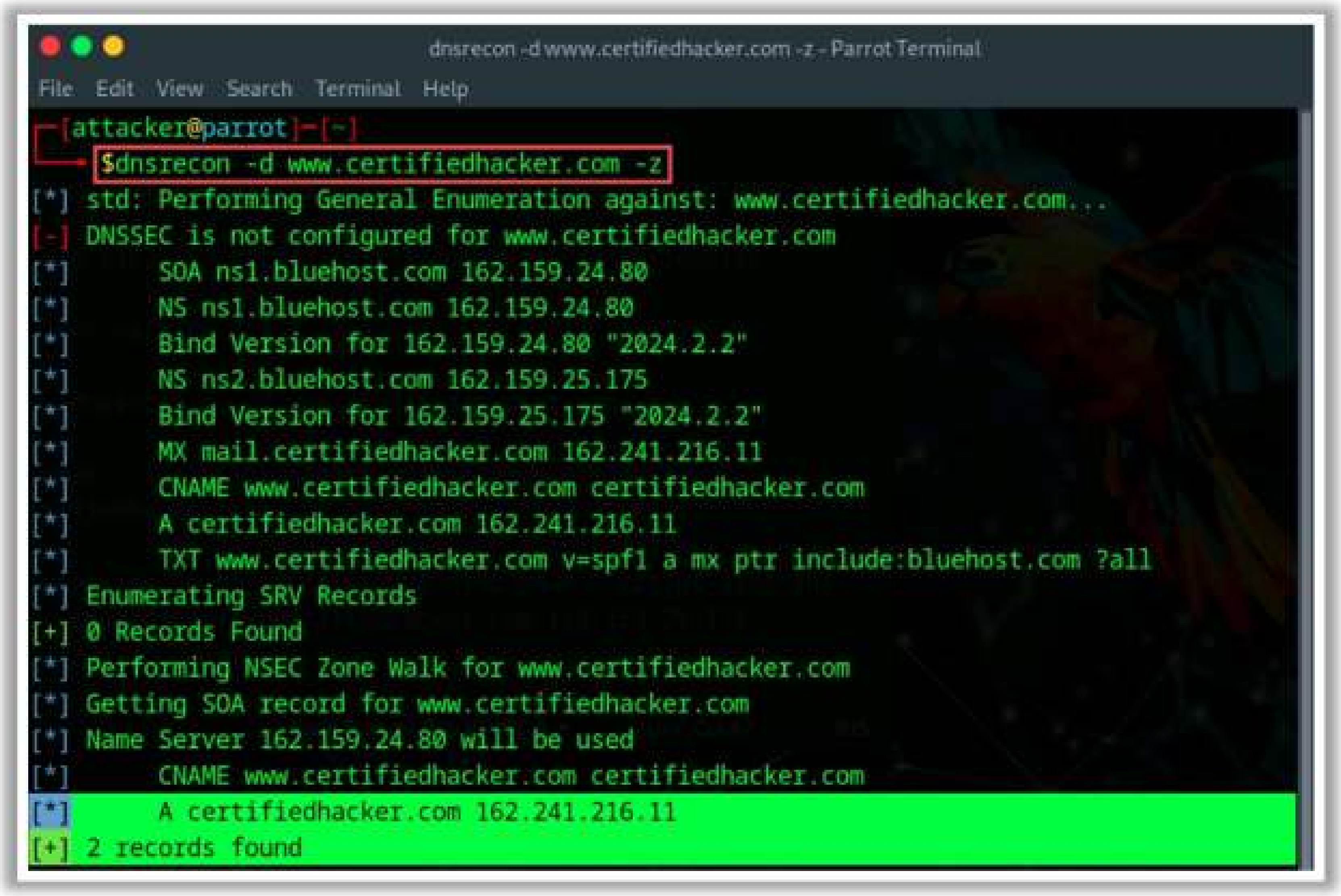
- **DNSRecon**

  Source: *https://www.github.com*

  DNSRecon is a zone enumeration tool that assists users in enumerating DNS records such as A, AAAA, and CNAME. It also performs NSEC zone enumeration to obtain DNS record files of a target domain.

  As shown in the screenshot, attackers use the following query to perform zone enumeration against a target domain **`certifiedhacker.com`**:

  `dnsrecon -d <target domain> -z`



dnsrecon -d www.certifiedhacker.com -z - Parrot Terminal
File Edit View Search Terminal Help

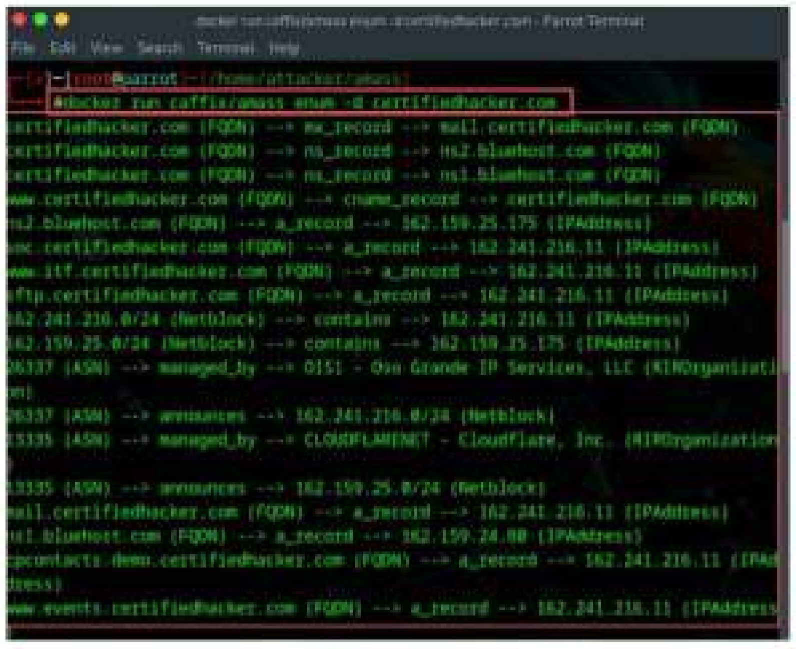
```
┌─[attacker@parrot]─[~]
└──╼ $dnsrecon -d www.certifiedhacker.com -z
[*] std: Performing General Enumeration against: www.certifiedhacker.com...
[-] DNSSEC is not configured for www.certifiedhacker.com
[*]      SOA ns1.bluehost.com 162.159.24.80
[*]      NS ns1.bluehost.com 162.159.24.80
[*]      Bind Version for 162.159.24.80 "2024.2.2"
[*]      NS ns2.bluehost.com 162.159.25.175
[*]      Bind Version for 162.159.25.175 "2024.2.2"
[*]      MX mail.certifiedhacker.com 162.241.216.11
[*]      CNAME www.certifiedhacker.com certifiedhacker.com
[*]      A certifiedhacker.com 162.241.216.11
[*]      TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[+] 0 Records Found
[*] Performing NSEC Zone Walk for www.certifiedhacker.com
[*] Getting SOA record for www.certifiedhacker.com
[*] Name Server 162.159.24.80 will be used
[*]      CNAME www.certifiedhacker.com certifiedhacker.com
[*]      A certifiedhacker.com 162.241.216.11
[+] 2 records found
```

Figure 4.46: Screenshot of DNSRecon displaying results on the target domain

All Rights Reserved. Reproduction is Strictly Prohibited.

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**



```
┌─[✗]─[root@parrot]─[/home/attacker/amass]
└──╼ #docker run caffix/amass enum -d certifiedhacker.com
ertifiedhacker.com (FQDN) --> mx_record --> mail.certifiedhacker.com (FQDN)
ertifiedhacker.com (FQDN) --> ns_record --> ns2.bluehost.com (FQDN)
ertifiedhacker.com (FQDN) --> ns_record --> ns1.bluehost.com (FQDN)
ww.certifiedhacker.com (FQDN) --> cname_record --> certifiedhacker.com (FQDN)
s2.bluehost.com (FQDN) --> a_record --> 162.159.25.175 (IPAddress)
nc.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
ww.itf.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
ftp.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
62.241.216.0/24 (Netblock) --> contains --> 162.241.216.11 (IPAddress)
62.159.25.0/24 (Netblock) --> contains --> 162.159.25.175 (IPAddress)
6337 (ASN) --> managed_by --> OIS1 - Oso Grande IP Services, LLC (RIROrganizati
on)
6337 (ASN) --> announces --> 162.241.216.0/24 (Netblock)
3335 (ASN) --> managed_by --> CLOUDFLARENET - Cloudflare, Inc. (RIROrganization

3335 (ASN) --> announces --> 162.159.25.0/24 (Netblock)
ail.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
s1.bluehost.com (FQDN) --> a_record --> 162.159.24.80 (IPAddress)
pcontacts.demo.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAd
dress)
ww.events.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress
```

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`

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

DNS Enumeration using OWASP Amass

Source: *https://github.com*

OWASP Amass is a DNS enumeration tool that allows attackers to map the target network and discover potential attack surfaces. Attackers use a combination of both active and passive reconnaissance techniques to gather information from DNS. This tool enables attackers to enumerate critical information without triggering any security alerts within the DNS environment of the targeted network.

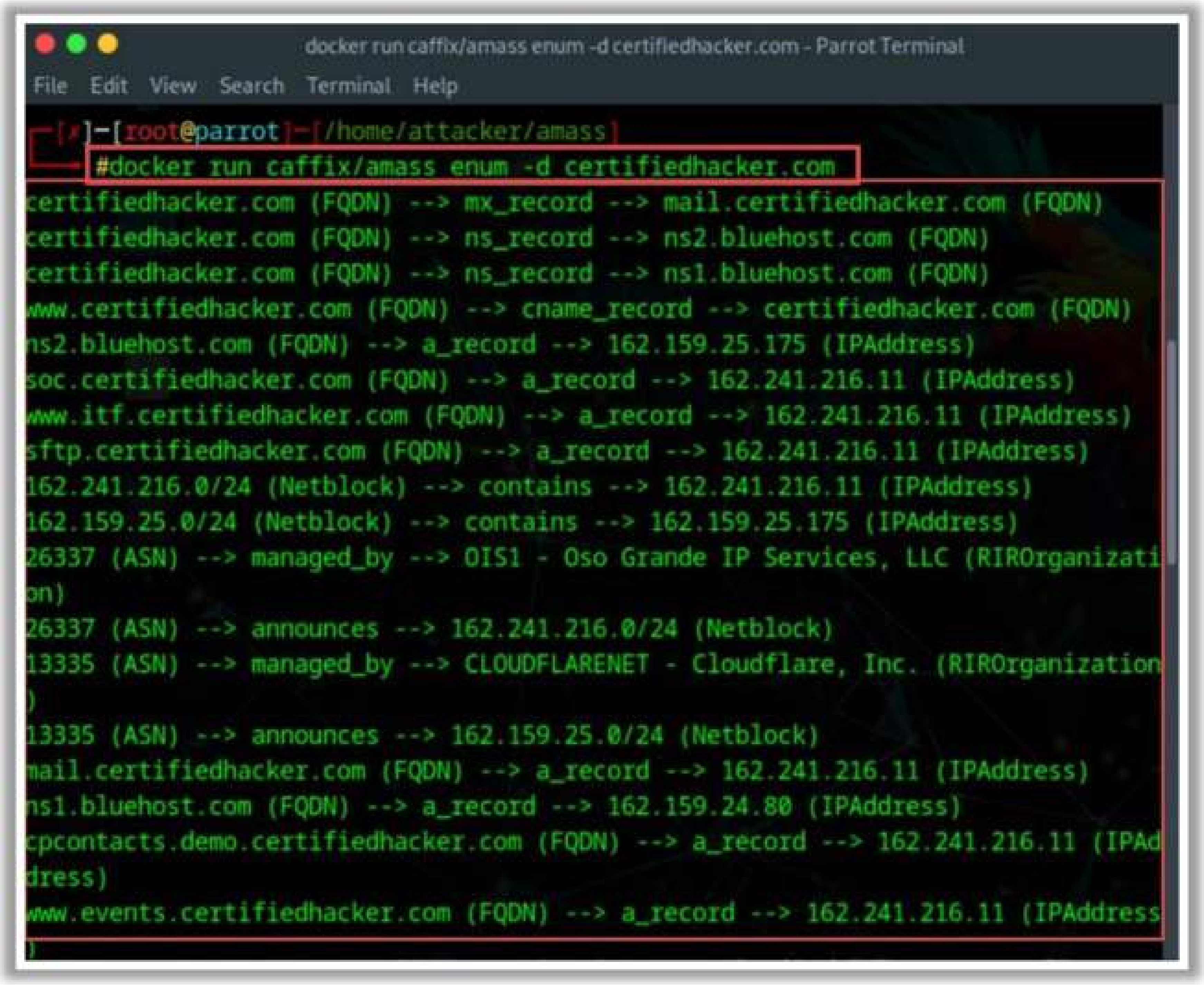
Attackers can execute the following command to enumerate DNS information from the target network:

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

The above command allows attackers to gather all the details of DNS, including its subdomains. Using this command, attackers can also enumerate details of IP addresses, SSL/TLS, HTTP, APIs, certificates, web archives, and data scraping incorporated with the target domain.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24


docker run caffix/amass enum -d certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help

```
[✗]-[root@parrot]-[/home/attacker/amass]
   #docker run caffix/amass enum -d certifiedhacker.com
certifiedhacker.com (FQDN) --> mx_record --> mail.certifiedhacker.com (FQDN)
certifiedhacker.com (FQDN) --> ns_record --> ns2.bluehost.com (FQDN)
certifiedhacker.com (FQDN) --> ns_record --> ns1.bluehost.com (FQDN)
www.certifiedhacker.com (FQDN) --> cname_record --> certifiedhacker.com (FQDN)
ns2.bluehost.com (FQDN) --> a_record --> 162.159.25.175 (IPAddress)
soc.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
www.itf.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
sftp.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
162.241.216.0/24 (Netblock) --> contains --> 162.241.216.11 (IPAddress)
162.159.25.0/24 (Netblock) --> contains --> 162.159.25.175 (IPAddress)
26337 (ASN) --> managed_by --> OIS1 - Oso Grande IP Services, LLC (RIROrganizati
on)
26337 (ASN) --> announces --> 162.241.216.0/24 (Netblock)
13335 (ASN) --> managed_by --> CLOUDFLARENET - Cloudflare, Inc. (RIROrganization
)
13335 (ASN) --> announces --> 162.159.25.0/24 (Netblock)
mail.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress)
ns1.bluehost.com (FQDN) --> a_record --> 162.159.24.80 (IPAddress)
cpcontacts.demo.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAd
dress)
www.events.certifiedhacker.com (FQDN) --> a_record --> 162.241.216.11 (IPAddress
)
```

Figure 4.47: Screenshot of OWASP Amass

Other OWASP Amass commands for DNS Enumeration:

- Run the following command to perform a passive enumeration:

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

- Run the following command to perform an active enumeration through brute-forcing with a specified wordlist:

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

- Run the following command to track or compare the last two enumeration scans performed on the target domain:

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

- Run the following command to display the results of enumeration stored in amass database (amass4owasp):

  `amass db -dir amass4owasp -list`

- Run the following command to create a d3-force HTML visual graph:

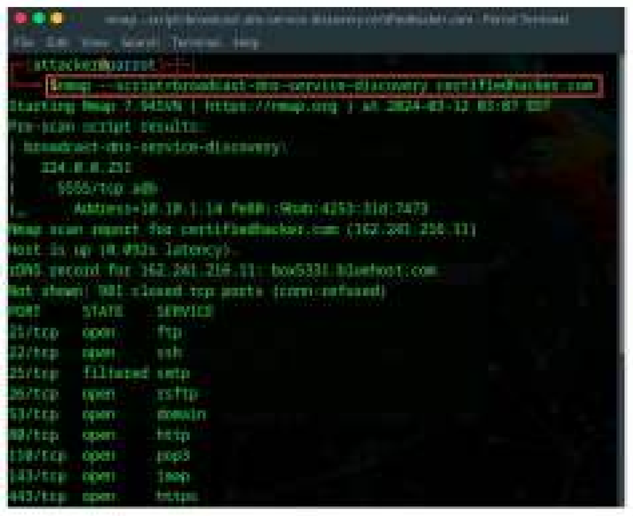
  `amass viz -d3 -dir amass4owasp`

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DNS and DNSSEC Enumeration Using Nmap

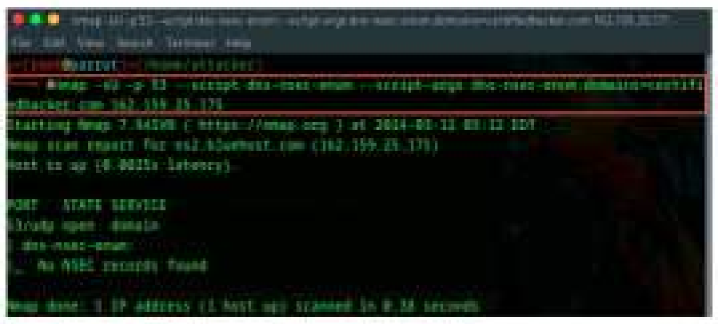
DNS Enumeration

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

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

DNS and DNSSEC Enumeration using Nmap

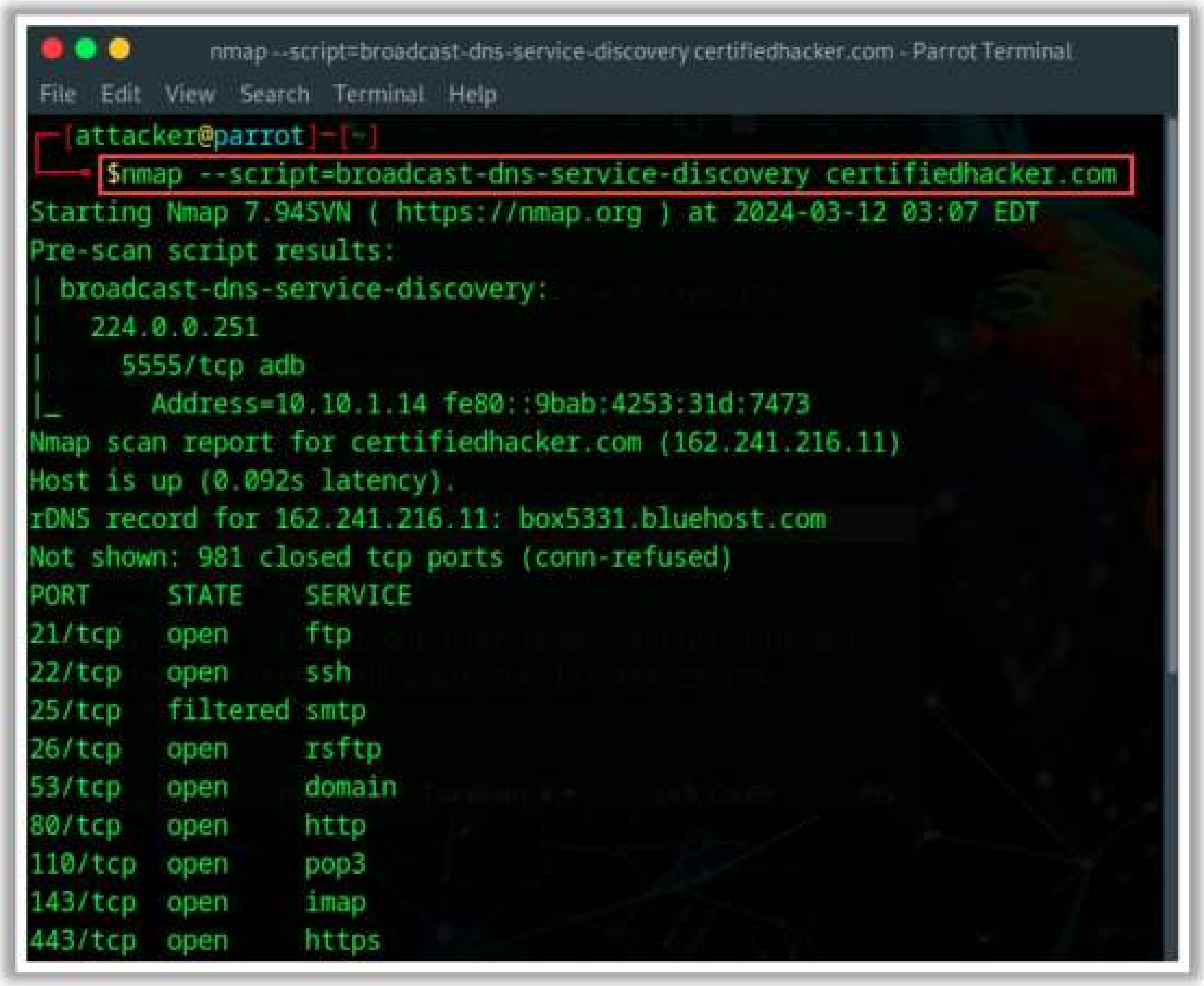
DNS Enumeration Using Nmap

Attackers use Nmap to scan domains and obtain a list of subdomains, records, IP addresses, and other valuable information from the target host.

- Run the following command to list all the available services on the target host:

  `nmap --script=broadcast-dns-service-discovery <Target Domain>`

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

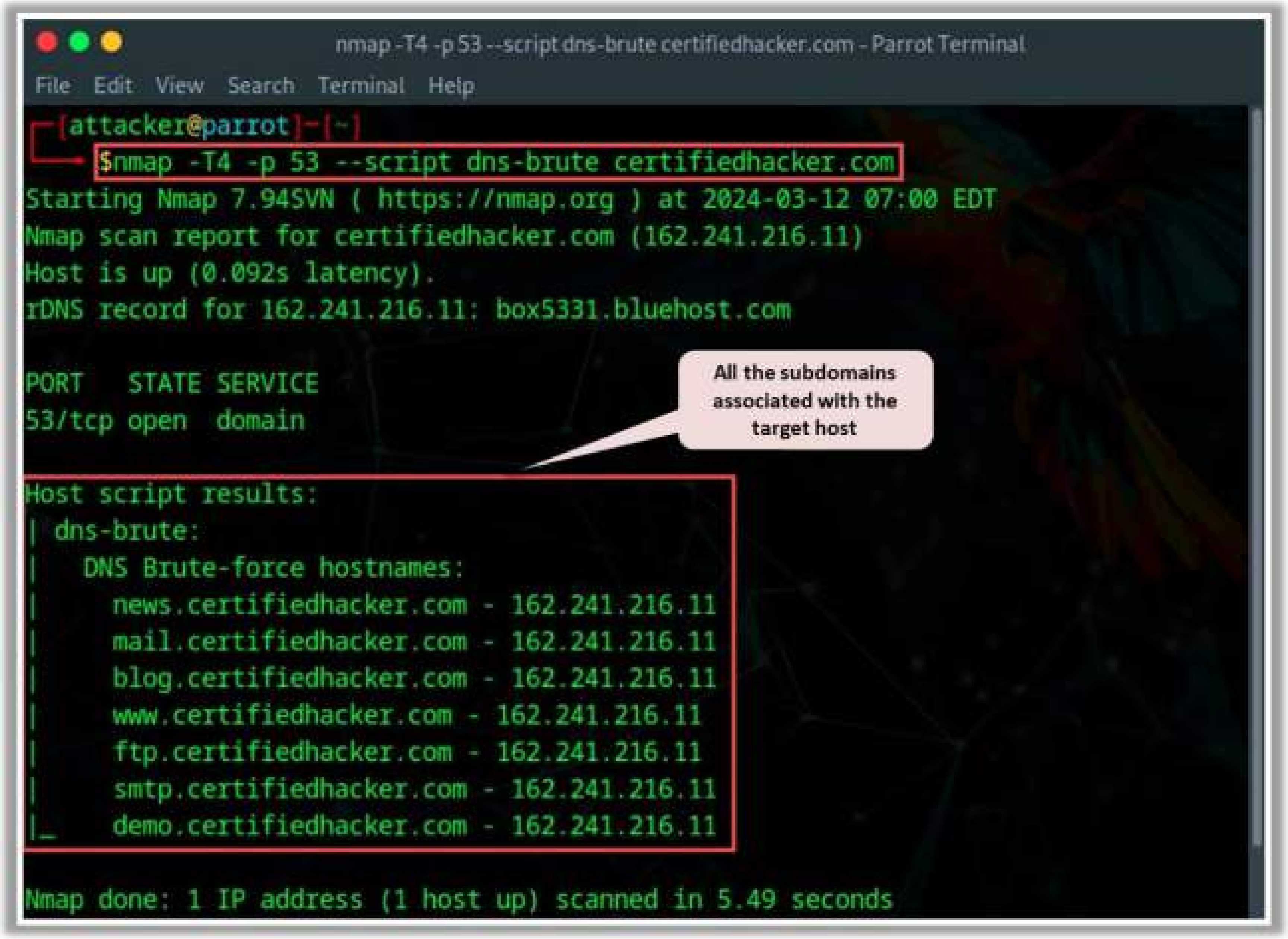

nmap --script=broadcast-dns-service-discovery certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[attacker@parrot]─[~]
└──╼ $nmap --script=broadcast-dns-service-discovery certifiedhacker.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 03:07 EDT
Pre-scan script results:
| broadcast-dns-service-discovery:
|   224.0.0.251
|     5555/tcp adb
|_      Address=10.10.1.14 fe80::9bab:4253:31d:7473
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.092s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 981 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   filtered smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
143/tcp  open     imap
443/tcp  open     https
```

Figure 4.48: Screenshot of Nmap DNS service discovery

- Execute the following command to retrieve all the subdomains associated with the target host:

  `nmap -T4 -p 53 --script dns-brute <Target Domain>`


nmap -T4 -p 53 --script dns-brute certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help

```
┌[attacker@parrot]-[~]
└──╼ $nmap -T4 -p 53 --script dns-brute certifiedhacker.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 07:00 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.092s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT   STATE SERVICE
53/tcp open  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     news.certifiedhacker.com - 162.241.216.11
|     mail.certifiedhacker.com - 162.241.216.11
|     blog.certifiedhacker.com - 162.241.216.11
|     www.certifiedhacker.com - 162.241.216.11
|     ftp.certifiedhacker.com - 162.241.216.11
|     smtp.certifiedhacker.com - 162.241.216.11
|_    demo.certifiedhacker.com - 162.241.216.11

Nmap done: 1 IP address (1 host up) scanned in 5.49 seconds
```

All the subdomains associated with the target host

Figure 4.49: Screenshot of the dns-brute NSE script

The above command provides a list of subdomains along with their IP addresses. If any wildcard entries are recorded, they are represented as **`*A*`** for IPv4 addresses and **`*AAAA*`** for IPv6 addresses.

- Run the following command to check whether DNS recursion is enabled on the target server:

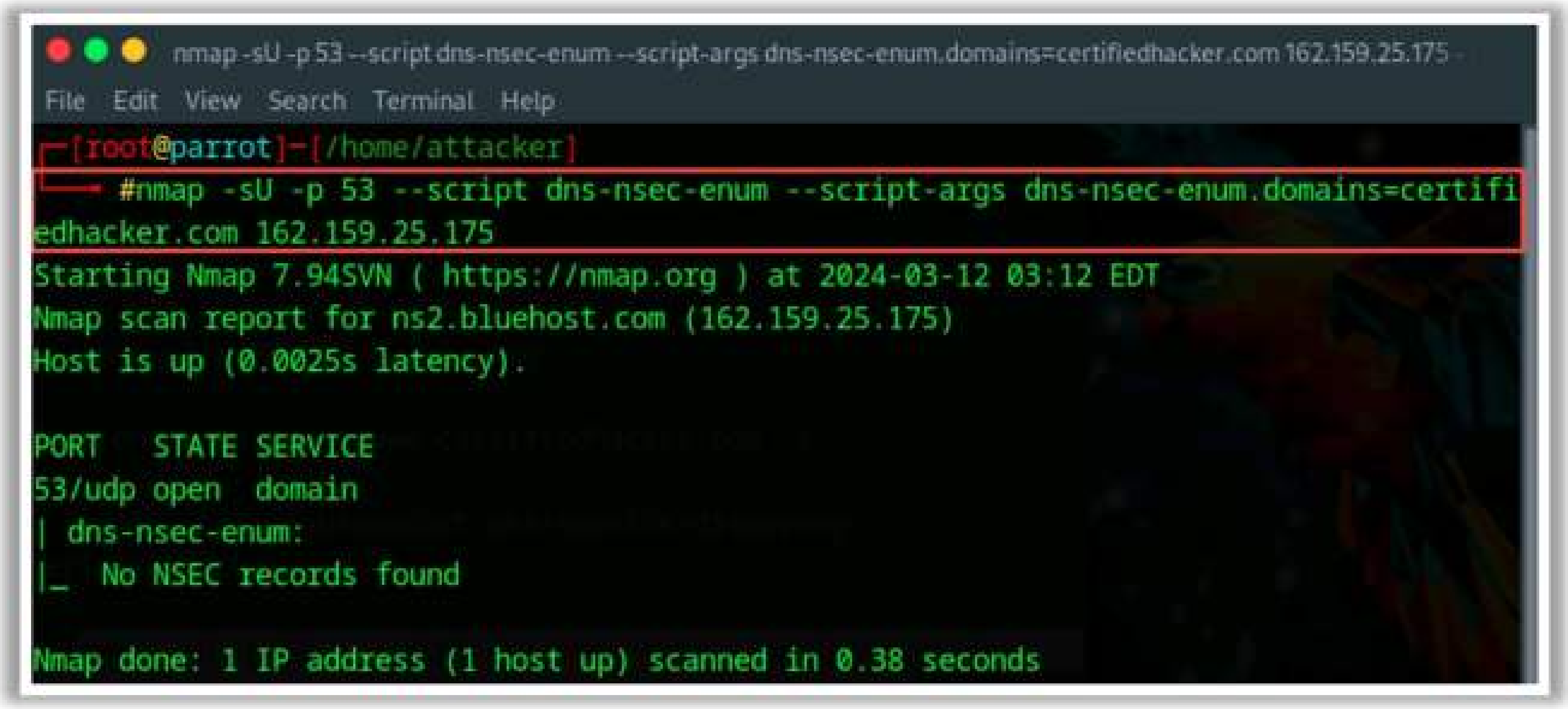
  `nmap -Pn -sU -p 53 --script=dns-recursion 192.168.1.150`

DNS Security Extensions (DNSSEC) Enumeration using Nmap

DNSSEC provides security for DNS queries and responses. Attackers enumerate DNSSEC using **`dns-nsec-enum.nse`** or **`dns-nsec3-enum.nse`** NSE scripts to obtain information related to domains and their subdomains.

- Execute the following command to retrieve the list of subdomains associated with the target domain:

  `nmap -sU -p 53 --script dns-nsec-enum --script-args dns-nsec-enum.domains= eccouncil.org <target>`



nmap -sU -p 53 --script dns-nsec-enum --script-args dns-nsec-enum.domains=certifiedhacker.com 162.159.25.175 -
File Edit View Search Terminal Help

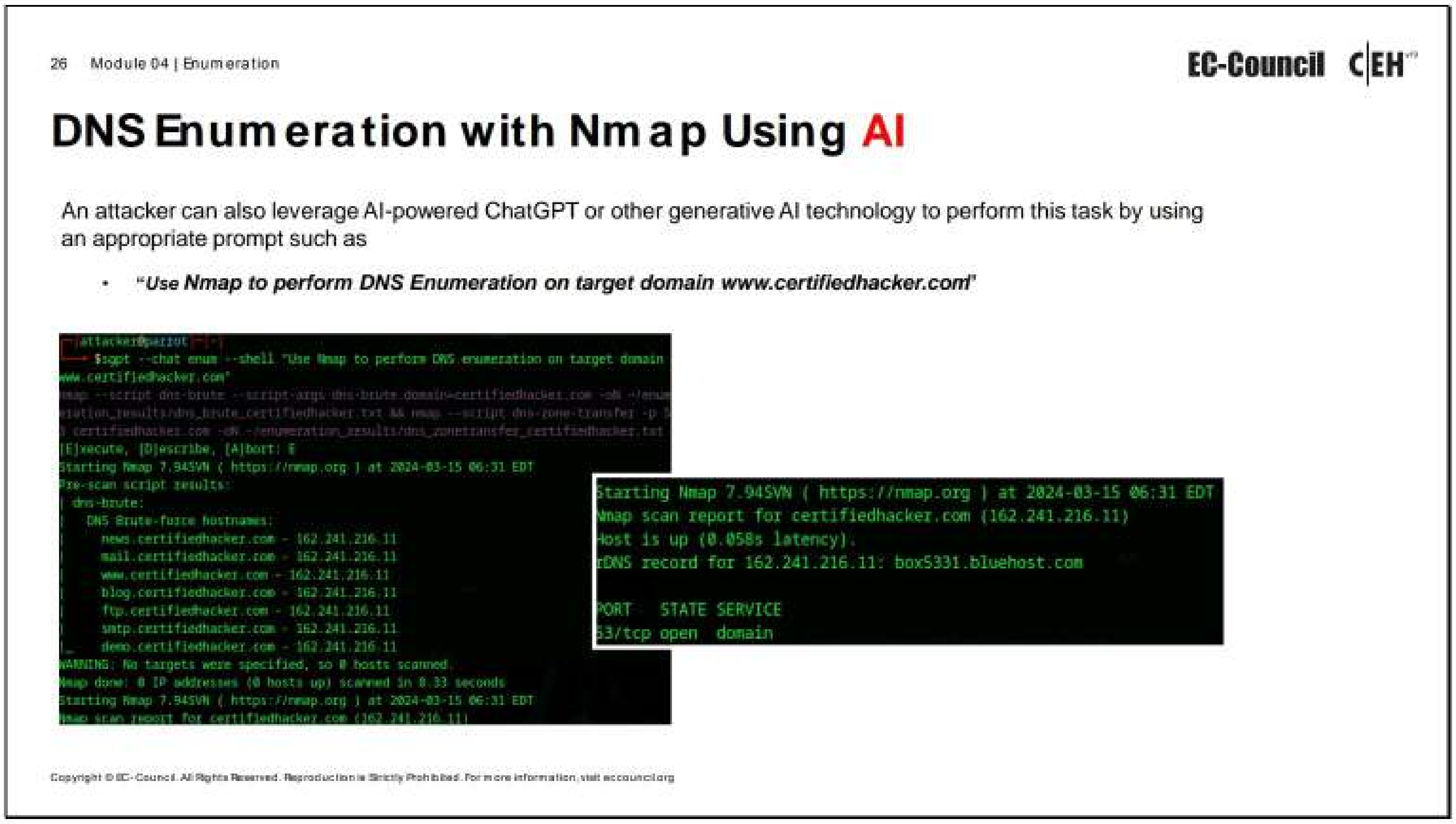
```
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -sU -p 53 --script dns-nsec-enum --script-args dns-nsec-enum.domains=certifi
edhacker.com 162.159.25.175
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 03:12 EDT
Nmap scan report for ns2.bluehost.com (162.159.25.175)
Host is up (0.0025s latency).

PORT   STATE SERVICE
53/udp open  domain
| dns-nsec-enum:
|_  No NSEC records found

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

Figure 4.50: Screenshot of Nmap dns-nsec-enum NSE script

The following are some of the additional DNS enumeration tools:

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

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



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"*

```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --chat enum --shell "Use Nmap to perform DNS enumeration on target domain
www.certifiedhacker.com"
nmap --script dns-brute --script-args dns-brute.domain=certifiedhacker.com -oN ~/enum
eration_results/dns_brute_certifiedhacker.txt && nmap --script dns-zone-transfer -p 5
3 certifiedhacker.com -oN ~/enumeration_results/dns_zonetransfer_certifiedhacker.txt
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 06:31 EDT
Pre-scan script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     news.certifiedhacker.com - 162.241.216.11
|     mail.certifiedhacker.com - 162.241.216.11
|     www.certifiedhacker.com - 162.241.216.11
|     blog.certifiedhacker.com - 162.241.216.11
|     ftp.certifiedhacker.com - 162.241.216.11
|     smtp.certifiedhacker.com - 162.241.216.11
|_    demo.certifiedhacker.com - 162.241.216.11
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 8.33 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 06:31 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 06:31 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.058s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT   STATE SERVICE
53/tcp open  domain
```

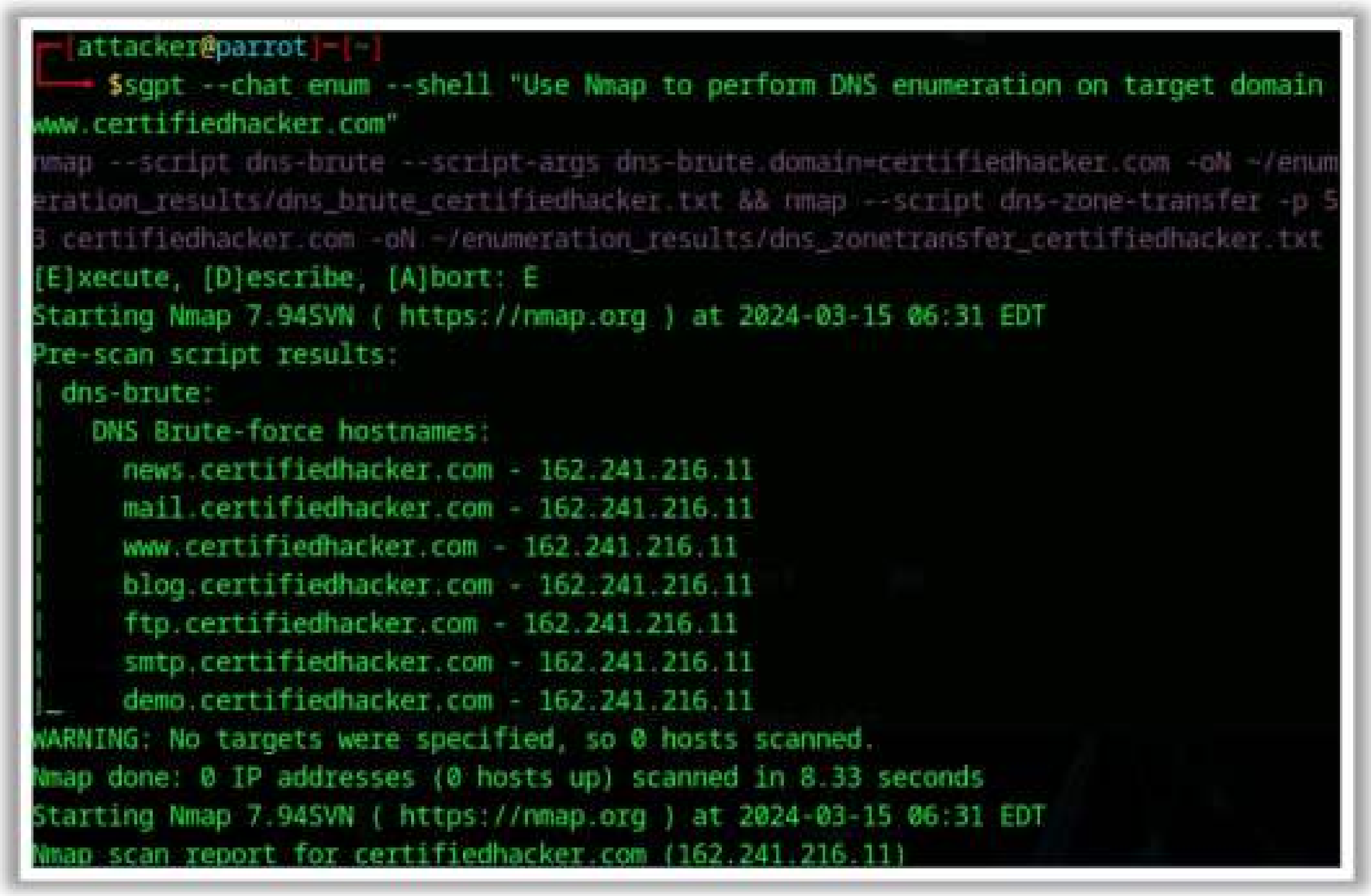
Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

DNS Enumeration with Nmap using AI

Attackers can leverage AI-powered technologies to enhance and automate their network enumeration tasks. With the aid of AI, attackers can effortlessly perform DNS enumeration and gather DNS information on target domains.

Attackers can use ChatGPT to perform this task by using appropriate prompts such as:

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



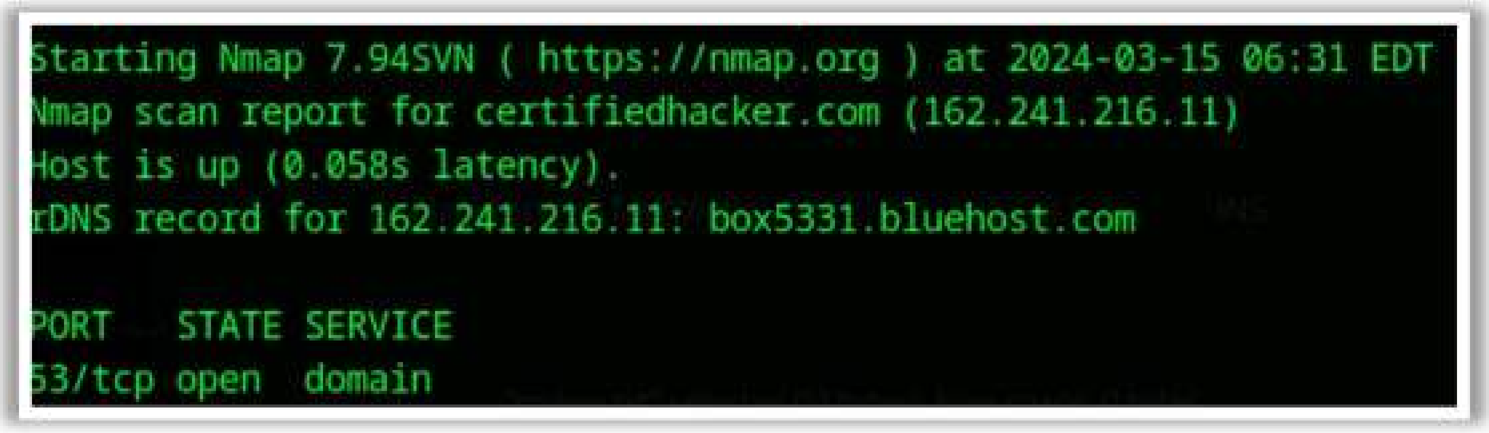
```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --chat enum --shell "Use Nmap to perform DNS enumeration on target domain
www.certifiedhacker.com"
nmap --script dns-brute --script-args dns-brute.domain=certifiedhacker.com -oN ~/enum
eration_results/dns_brute_certifiedhacker.txt && nmap --script dns-zone-transfer -p 5
3 certifiedhacker.com -oN ~/enumeration_results/dns_zonetransfer_certifiedhacker.txt
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 06:31 EDT
Pre-scan script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     news.certifiedhacker.com - 162.241.216.11
|     mail.certifiedhacker.com - 162.241.216.11
|     www.certifiedhacker.com - 162.241.216.11
|     blog.certifiedhacker.com - 162.241.216.11
|     ftp.certifiedhacker.com - 162.241.216.11
|     smtp.certifiedhacker.com - 162.241.216.11
|_    demo.certifiedhacker.com - 162.241.216.11
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 8.33 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 06:31 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
```

Figure 4.51: Perform DNS enumeration on target Domain with Nmap

Technet24

The following command is designed to automate DNS enumeration tasks on the specified target domain:

```
nmap --script dns-brute --script-args dns-brute.domain=certifiedhacker.com -oN
~/enumeration_results/dns_brute_certifiedhacker.txt && nmap --script dns-zone-
transfer -p 53 certifiedhacker.com -oN
~/enumeration_results/dns_zonetransfer_certifiedhacker.txt
```



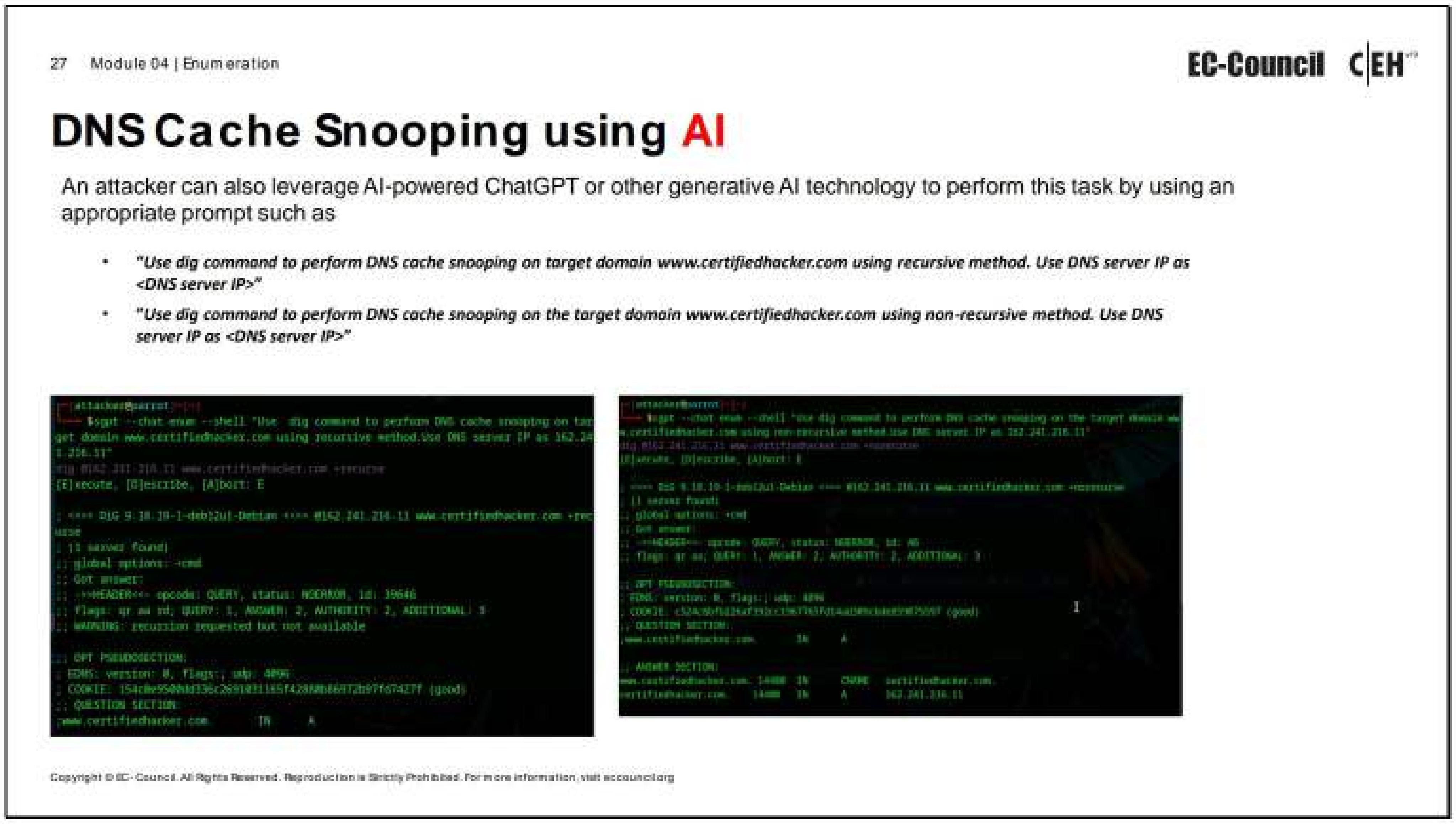
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 06:31 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.058s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT   STATE SERVICE
53/tcp open  domain
```

Figure 4.52: Perform DNS enumeration on target Domain with nmap

- The first command uses `nmap` with the `dns-brute` script to perform DNS brute-force enumeration on the domain `certifiedhacker.com`. The results are saved to the file `dns_brute_certifiedhacker.txt` in the `~/enumeration_results/` directory.
- The second command uses nmap with the `dns-zone-transfer` script to perform DNS zone transfer enumeration on port 53 of the domain `certifiedhacker.com`. The results are saved to the file `dns_zonetransfer_certifiedhacker.txt` in the `~/enumeration_results/` directory.

This command automates DNS enumeration tasks and saves the results for each command executed on the specified target domain www.certifiedhacker.com.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



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>"***

```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --chat enum --shell "Use  dig command to perform DNS cache snooping on tar
get domain www.certifiedhacker.com using recursive method.Use DNS server IP as 162.24
1.216.11"
dig @162.241.216.11 www.certifiedhacker.com +recurse
[E]xecute, [D]escribe, [A]bort: E

; <<>> DiG 9.18.19-1-deb12u1-Debian <<>> @162.241.216.11 www.certifiedhacker.com +rec
urse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39646
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: [illegible] (good)
;; QUESTION SECTION:
;www.certifiedhacker.com.       IN      A
```

```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on the target domain ww
w.certifiedhacker.com using non-recursive method.Use DNS server IP as 162.241.216.11"
dig @162.241.216.11 www.certifiedhacker.com +norecurse
[E]xecute, [D]escribe, [A]bort: E

; <<>> DiG 9.18.19-1-deb12u1-Debian <<>> @162.241.216.11 www.certifiedhacker.com +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: [illegible] (good)
;; QUESTION SECTION:
;www.certifiedhacker.com.       IN      A

;; ANSWER SECTION:
www.certifiedhacker.com. 14400  IN      CNAME   certifiedhacker.com.
certifiedhacker.com.    14400   IN      A       162.241.216.11
```

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

DNS Cache Snooping using AI

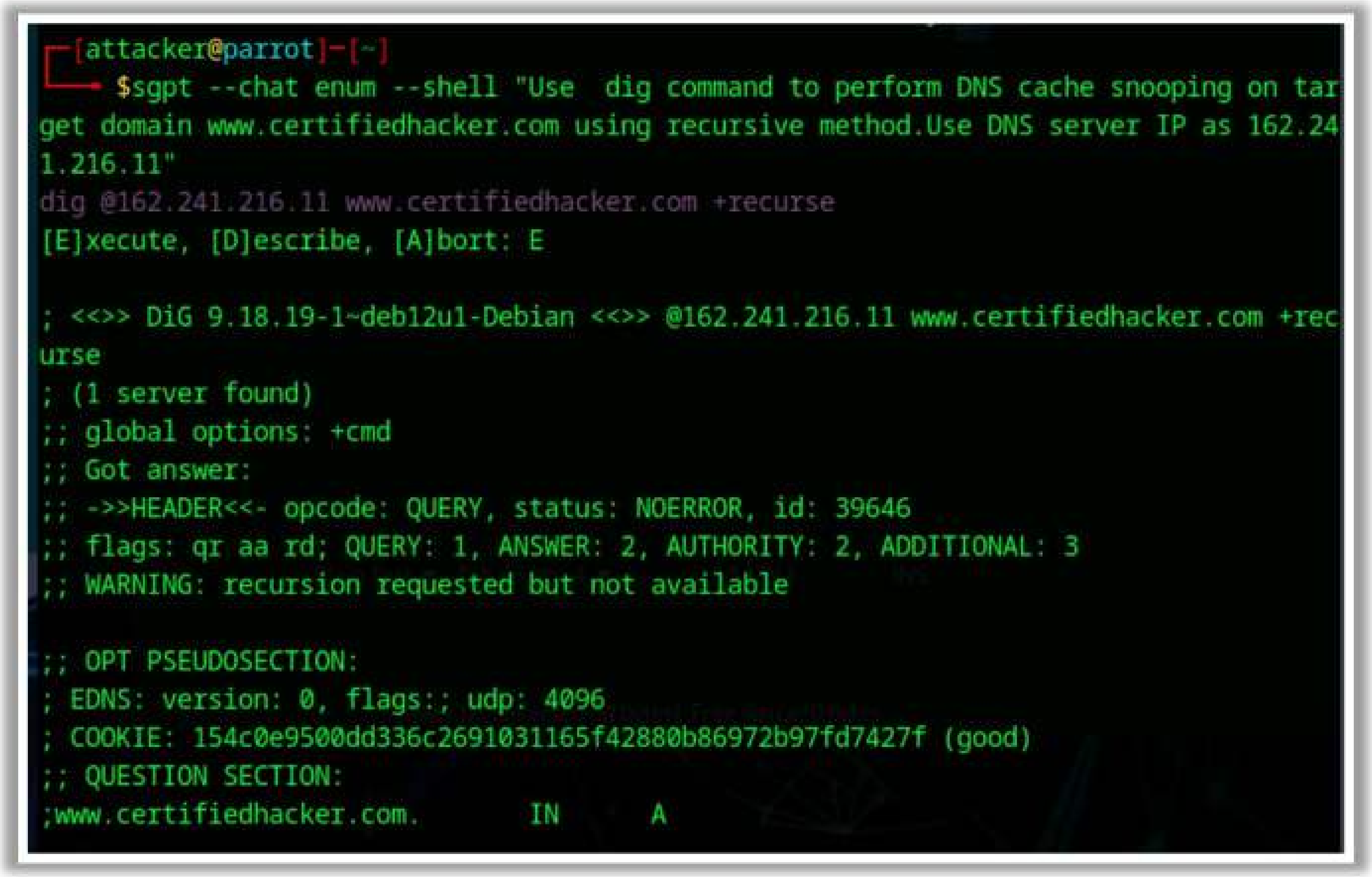
Attackers can leverage AI-powered technologies to enhance and automate their network enumeration tasks. With the aid of AI, attackers can effortlessly perform DNS cache snooping on target domain.

Example #1:

Attackers can use ChatGPT to perform this task by using appropriate prompts such as:

"Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method. Use DNS server IP as 162.241.216.11."

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --chat enum --shell "Use  dig command to perform DNS cache snooping on tar
get domain www.certifiedhacker.com using recursive method.Use DNS server IP as 162.24
1.216.11"
dig @162.241.216.11 www.certifiedhacker.com +recurse
[E]xecute, [D]escribe, [A]bort: E

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> @162.241.216.11 www.certifiedhacker.com +rec
urse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39646
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 154c0e9500dd336c2691031165f42880b86972b97fd7427f (good)
;; QUESTION SECTION:
;www.certifiedhacker.com.       IN      A
```

Figure 4.53: Perform DNS cache snooping on target Domain with dig

The following command is designed to automate DNS cache snooping on the specified target domain using the dig command:

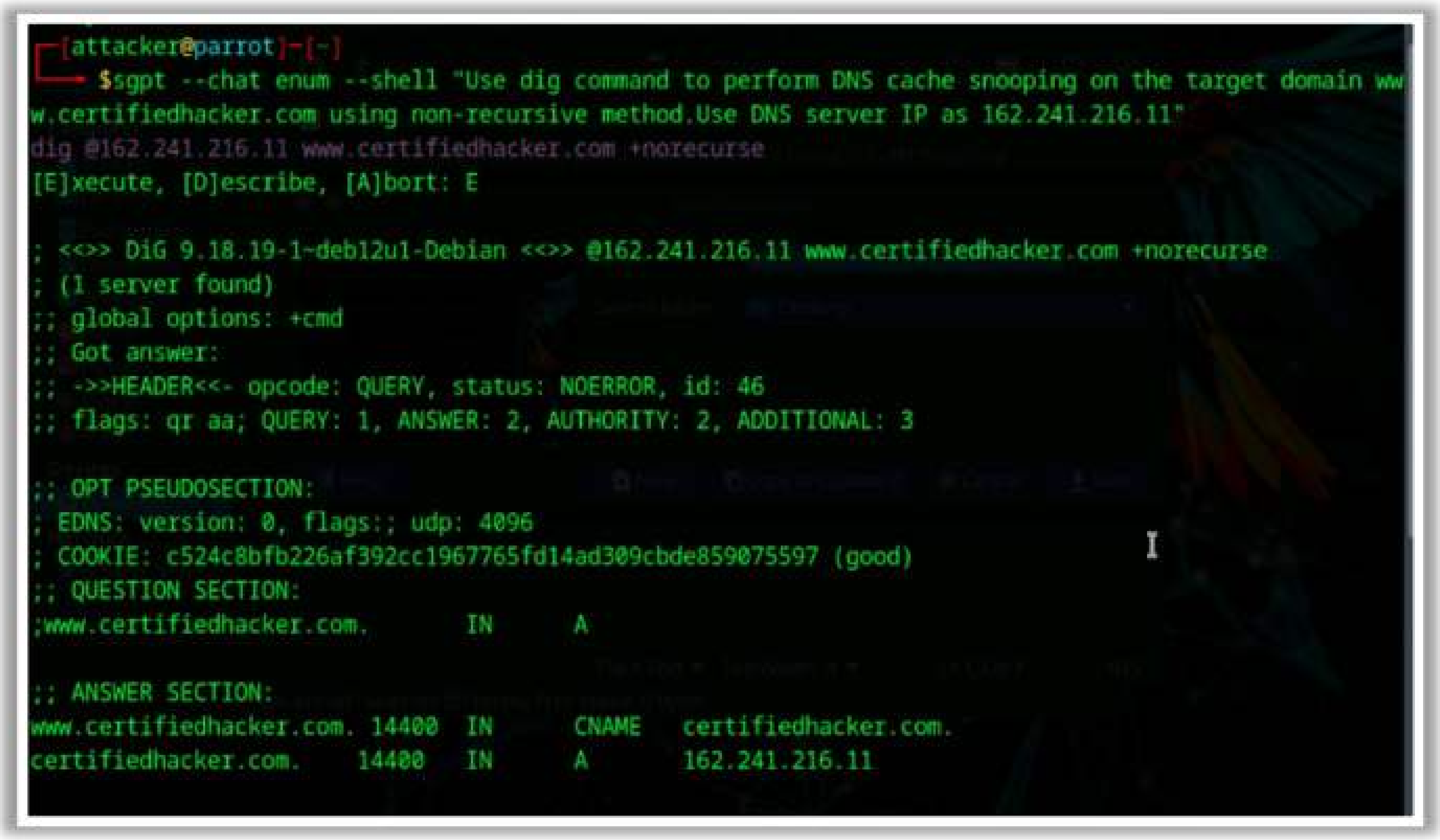
`dig @162.241.216.11 www.certifiedhacker.com +recurse`

- The command executes the `dig` command to perform DNS cache snooping on the target domain `www.certifiedhacker.com`.
- The `@162.241.216.11` argument specifies the DNS server IP address to query.
- The `www.certifiedhacker.com` argument specifies the target domain to query.
- The `+recurse` option indicates that recursive DNS resolution should be used to perform the query.

This command automates DNS cache snooping and displays the results for the specified target domain www.certifiedhacker.com using the recursive method.

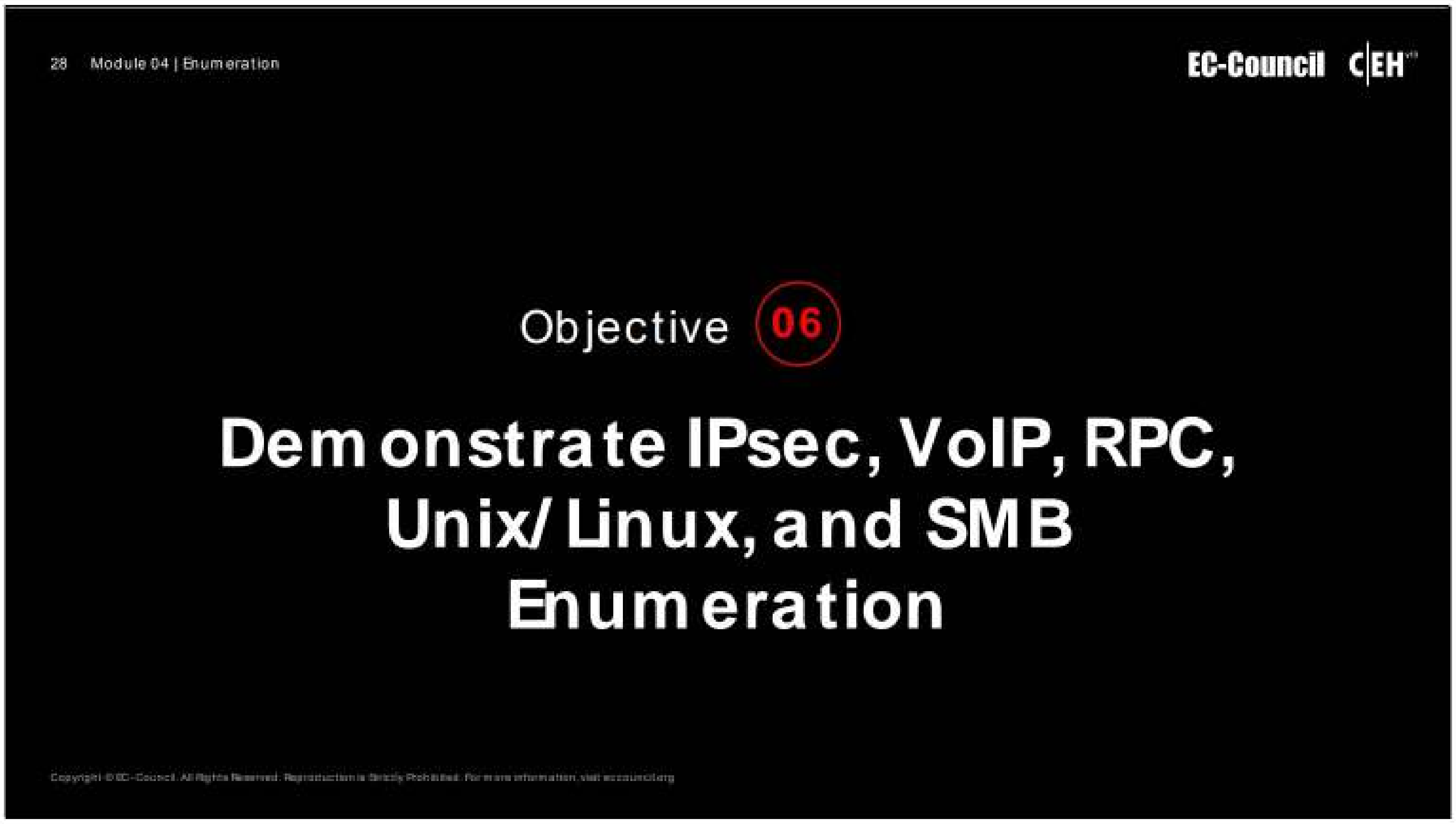
Example #2:

Similarly, attackers can automate DNS cache snooping on the specified target domain using the non-recursive method.



```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on the target domain ww
w.certifiedhacker.com using non-recursive method.Use DNS server IP as 162.241.216.11"
dig @162.241.216.11 www.certifiedhacker.com +norecurse
[E]xecute, [D]escribe, [A]bort: E

; <<>> DiG 9.18.19-1~deb12u1-Debian <<>> @162.241.216.11 www.certifiedhacker.com +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: c524c8bfb226af392cc1967765fd14ad309cbde859075597 (good)
;; QUESTION SECTION:
;www.certifiedhacker.com.       IN      A

;; ANSWER SECTION:
www.certifiedhacker.com. 14400  IN      CNAME   certifiedhacker.com.
certifiedhacker.com.    14400   IN      A       162.241.216.11
```

Figure 4.54: Perform DNS cache snooping on target Domain with dig – using non-recursive method



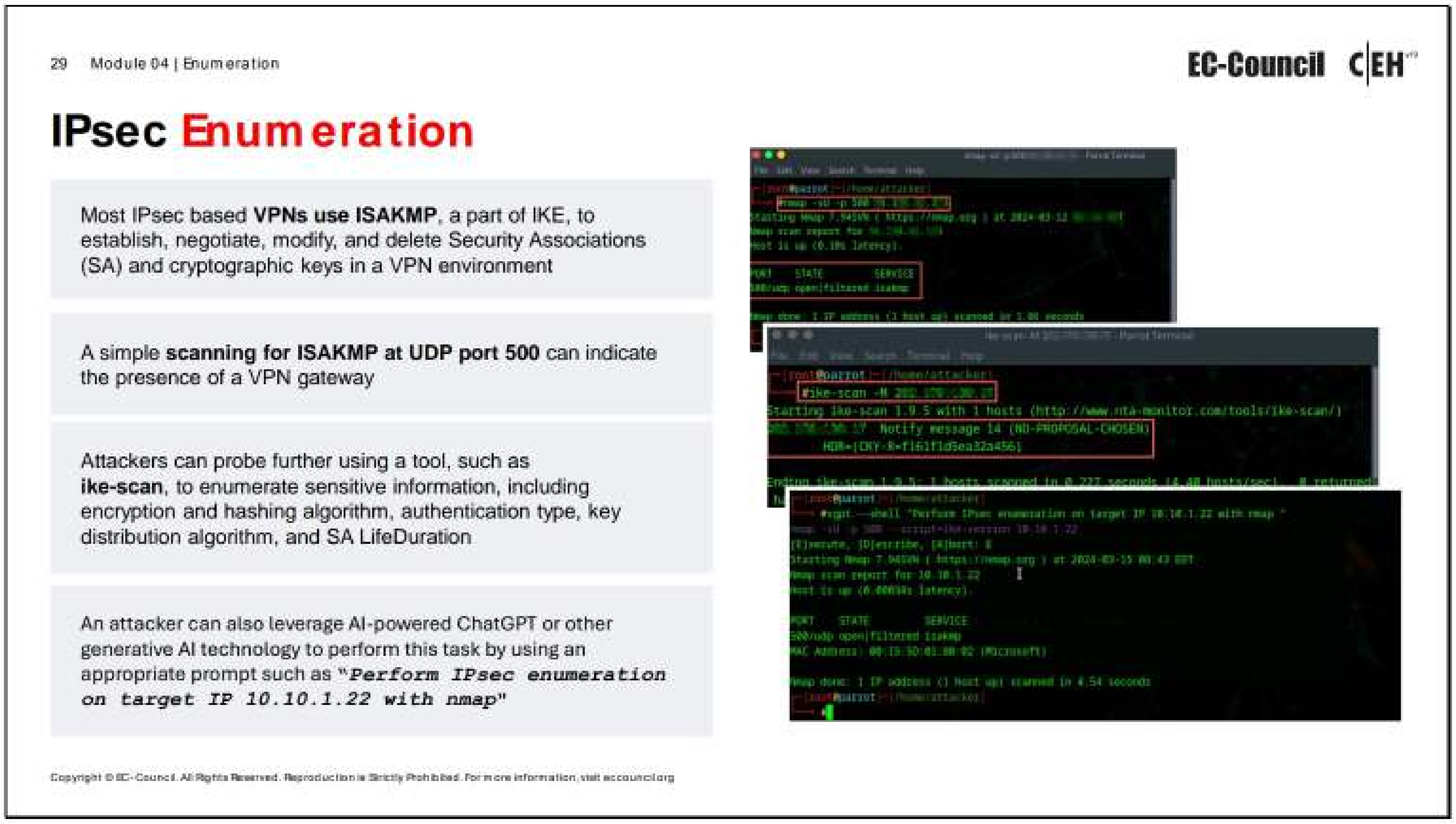
Objective 06

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

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Other Enumeration Techniques

This section discusses IPsec, VoIP, RPC, Unix/Linux user, Telnet, SSH user, 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***"

```
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -sU -p 500 [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 [redacted]
Nmap scan report for [redacted]
Host is up (0.10s latency).

PORT    STATE         SERVICE
500/udp open|filtered isakmp

Nmap done: 1 IP address (1 host up) scanned in 1.08 seconds
```

```
┌─[root@parrot]─[/home/attacker]
└──╼ #ike-scan -M [redacted]
Starting ike-scan 1.9.5 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
[redacted]  Notify message 14 (NO-PROPOSAL-CHOSEN)
        HDR=(CKY-R=f161f1d5ea32a456)

Ending ike-scan 1.9.5: 1 hosts scanned in 0.227 seconds (4.40 hosts/sec).  0 returned
```

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --shell "Perform IPsec enumeration on target IP 10.10.1.22 with nmap "
nmap -sU -p 500 --script=ike-version 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 00:43 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00034s latency).

PORT    STATE         SERVICE
500/udp open|filtered isakmp
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 4.54 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

IPsec Enumeration

IPsec is the most commonly implemented technology for both gateway-to-gateway (LAN-to-LAN) and host-to-gateway (remote access) enterprise VPN solutions. IPsec provides data security by employing various components such as Encapsulating Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE) to secure communication between VPN endpoints.

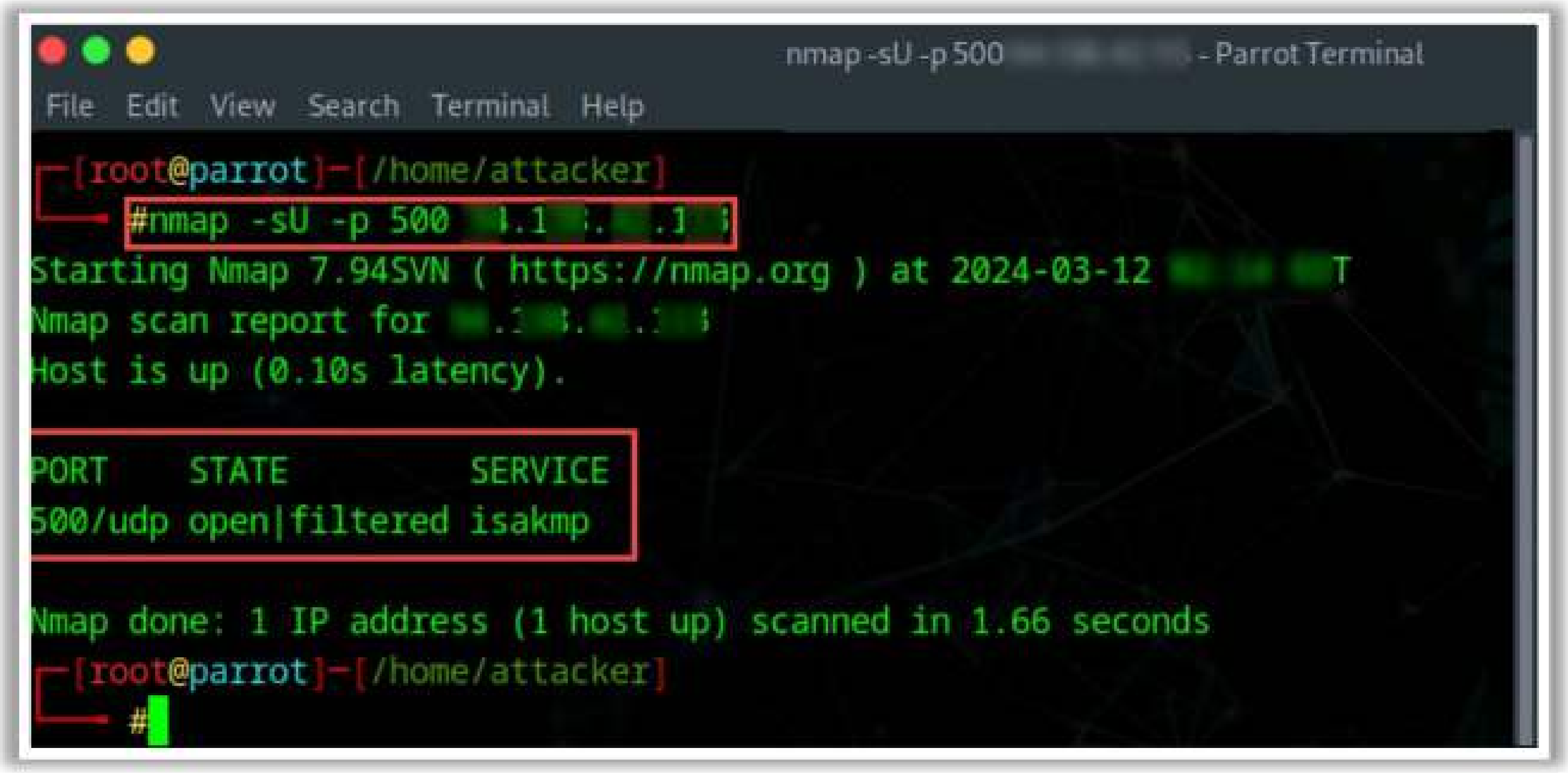
Most IPsec-based VPNs use the Internet Security Association Key Management Protocol (ISAKMP), a part of IKE, to establish, negotiate, modify, and delete Security Associations (SA) and cryptographic keys in a VPN environment.

Attackers can perform simple direct scanning for ISAKMP at UDP port 500 with tools such as Nmap to acquire information related to the presence of a VPN gateway.

The following command can be used to perform an Nmap scan for checking the status of ISAKMP over port 500:

```
# nmap –sU –p 500 <target IP address>
```

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.


nmap -sU -p 500 [redacted] - Parrot Terminal
File Edit View Search Terminal Help

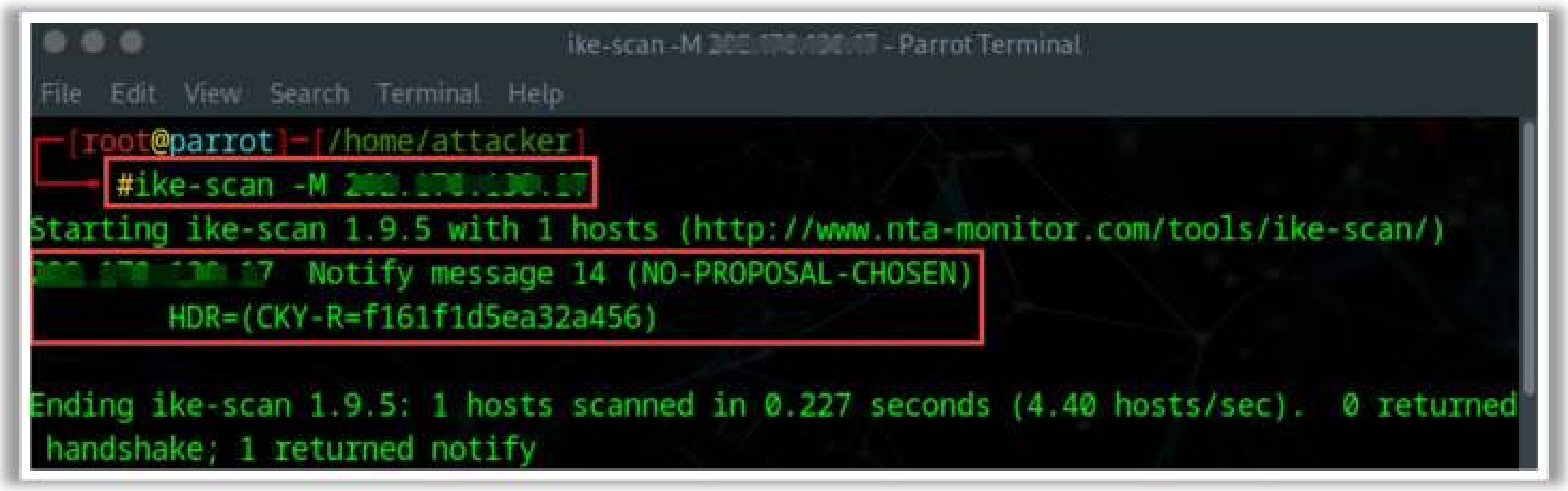
```
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -sU -p 500 [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 [redacted]T
Nmap scan report for [redacted]
Host is up (0.10s latency).

PORT    STATE         SERVICE
500/udp open|filtered isakmp

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

Figure 4.55: Screenshot displaying an Nmap scan over port 500 for ISAKMP

Attackers can probe further using fingerprinting tools such as ike-scan to enumerate sensitive information, including the encryption and hashing algorithm, authentication type, key distribution algorithm, and SA LifeDuration. In this type of scan, specially crafted IKE packets with an ISAKMP header are sent to the target gateway, and the responses are recorded.

The following command is used for initial IPsec VPN discovery with ike-scan tool:

```
# ike-scan -M <target gateway IP address>
```


ike-scan -M [redacted] - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[/home/attacker]
└──╼ #ike-scan -M [redacted]
Starting ike-scan 1.9.5 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
[redacted]  Notify message 14 (NO-PROPOSAL-CHOSEN)
        HDR=(CKY-R=f161f1d5ea32a456)

Ending ike-scan 1.9.5: 1 hosts scanned in 0.227 seconds (4.40 hosts/sec).  0 returned
 handshake; 1 returned notify
```

Figure 4.56: Screenshot displaying ike-scan enumeration

ike-scan

Source: *https://github.com*

ike-scan discovers IKE hosts and can fingerprint them using the retransmission backoff pattern. ike-scan can perform the following functions.

- **Discovery**: The hosts running IKE in a given IP range can be determined by displaying the hosts that respond to the IKE requests sent by ike-scan.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Fingerprinting**: The IKE implementation used by the hosts can be determined, and in some cases, the version of the software they are running can be determined. This is done in two ways: UDP backoff fingerprinting, which involves recording the times of arrival of the IKE response packets from the target hosts and comparing the observed retransmission backoff pattern against known patterns, and Vendor ID fingerprinting, which compares Vendor ID payloads from the VPN servers against known Vendor ID patterns.
- **Transform enumeration**: The transform attributes supported by the VPN server for IKE phase 1 (e.g., encryption algorithm and hash algorithm) can be determined.
- **User enumeration**: For some VPN systems, valid VPN usernames can be discovered.
- **Pre-shared key cracking**: Offline dictionary or brute-force password cracking can be performed for IKE Aggressive Mode with pre-shared key authentication. This uses ike-scan to obtain the hash and other parameters as well as psk-crack, which is a part of the ike-scan package, to perform the cracking.

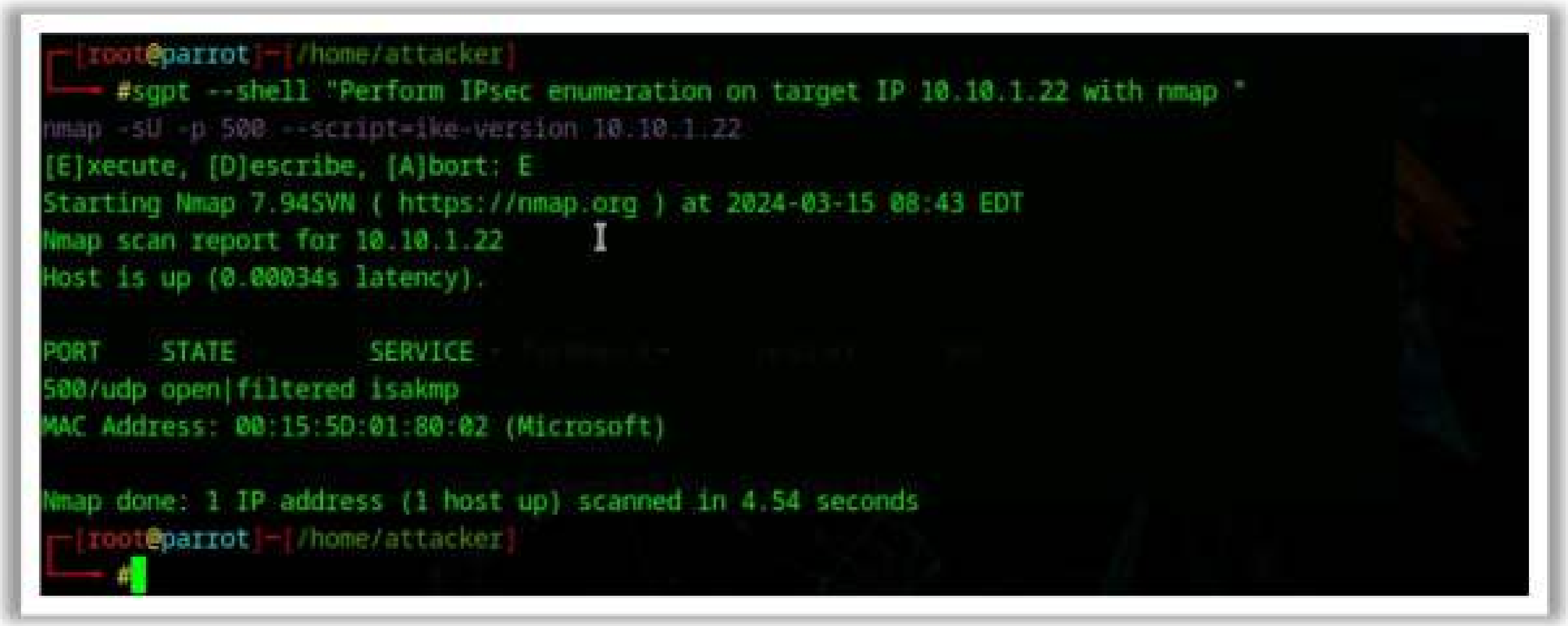
IPsec Enumeration with AI

Attackers can leverage AI-powered technologies to enhance and automate their network enumeration tasks. With the aid of AI, attackers can effortlessly perform IPsec enumeration on the target domain.

For example,

An attacker can use ChatGPT to perform this task by using an appropriate prompt such as:

- **"Perform IPsec enumeration on target IP 10.10.1.22 with nmap".**



```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --shell "Perform IPsec enumeration on target IP 10.10.1.22 with nmap "
nmap -sU -p 500 --script=ike-version 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:43 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00034s latency).

PORT    STATE         SERVICE
500/udp open|filtered isakmp
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 4.54 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

Figure 4.57: Perform IPsec enumeration on target IP

To perform an Internet Protocol Security (IPsec) enumeration on the target IP address 10.10.1.22 using Nmap, you can use the following command:

`nmap -sU -p 500 –script=ike-version 10.10.1.22`

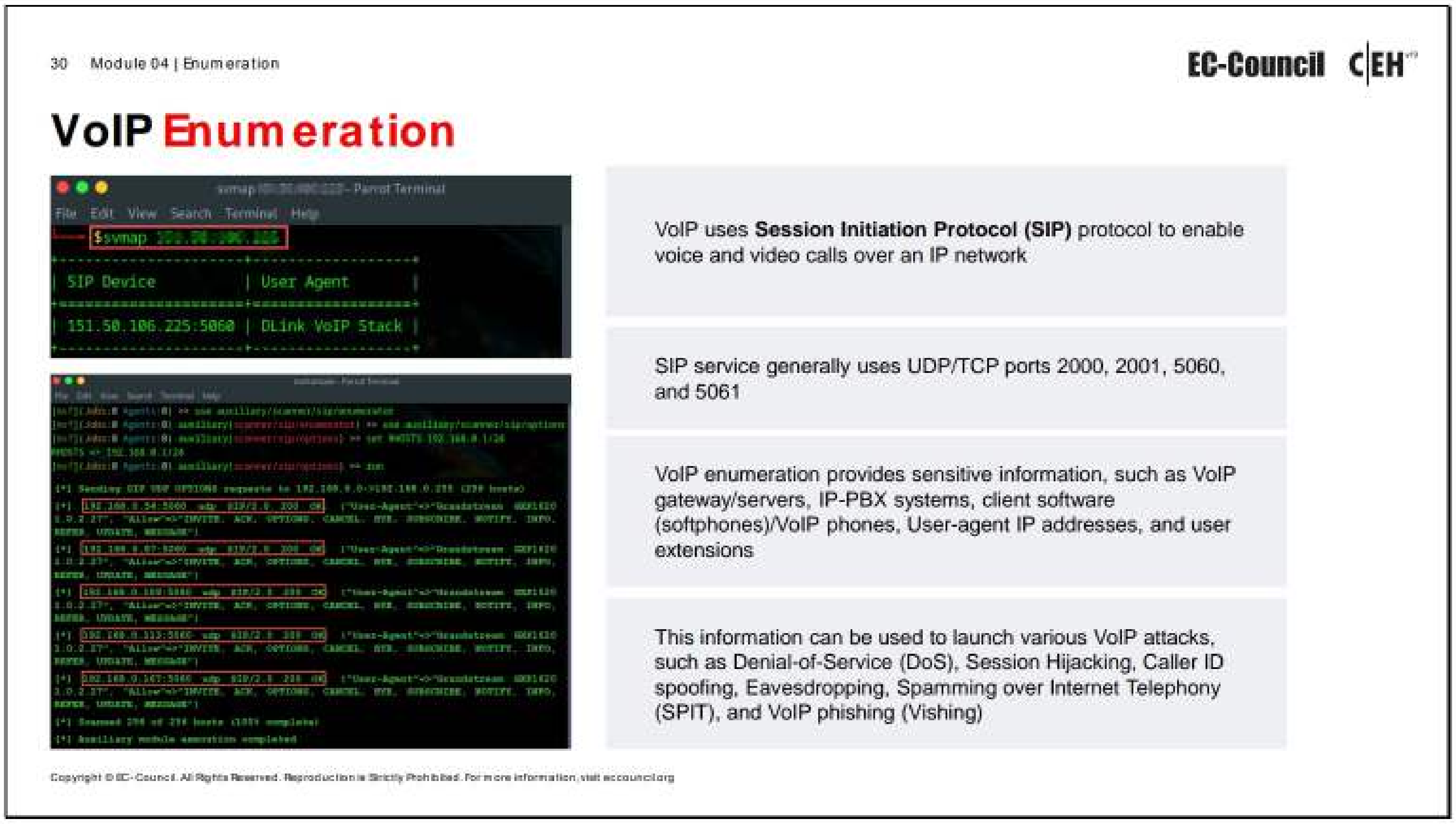
- **`nmap`**: This is the command to invoke Nmap, a network scanning tool.
- **`-sU`**: This option specifies a UDP scan (UDP packets) with no payload. This is typically used for scanning services that do not respond to ICMP requests.

Technet24

- `-p 500`: This option specifies the port number to scan. Port 500 is the default port used for Internet Key Exchange (IKE), a protocol used in IPsec VPNs.
- `--script=ike-version`: This option specifies the Nmap script to run. The `ike-version` script is used to detect the version of IKE running on the target.
- `10.10.1.22`: This is the target IP address you want to scan for IPsec enumeration.

This command instructs Nmap to perform a UDP scan on port 500 and run the `ike-version` script against the target IP address 10.10.1.22 to detect the version of IKE running, which can provide insights into the IPsec configuration.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



VoIP Enumeration

```
$svmap [redacted]
+--------------------+-------------------+
| SIP Device         | User Agent        |
+====================+===================+
| 151.50.106.225:5060 | DLink VoIP Stack |
+--------------------+-------------------+
```

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)

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

VoIP Enumeration

VoIP is an advanced technology that has replaced the conventional public switched telephone network (PSTN) in both corporate and home environments. VoIP uses Internet infrastructure to establish connections for voice calls; data are also transmitted on the same network. However, VoIP is vulnerable to TCP/IP attack vectors. Session Initiation Protocol (SIP) is one of the protocols used by VoIP for performing voice calls, video calls, etc. over an IP network. This SIP service generally uses UDP/TCP ports 2000, 2001, 5060, and 5061.

Attackers use Svmap and Metasploit tools to perform VoIP enumeration. Through VoIP enumeration, attackers can gather sensitive information such as VoIP gateway/servers, IP-private branch exchange (PBX) systems, and User-Agent IP addresses and user extensions of client software (softphones) or VoIP phones. This information can be used to launch various VoIP attacks such as DoS attacks, session hijacking, caller ID spoofing, eavesdropping, spam over Internet telephony (SPIT), and VoIP phishing (Vishing).

- **Svmap**

  Source: *https://github.com*

  Svmap is an open-source scanner that identifies SIP devices and PBX servers on a target network. It can be helpful for system administrators when used as a network inventory tool.

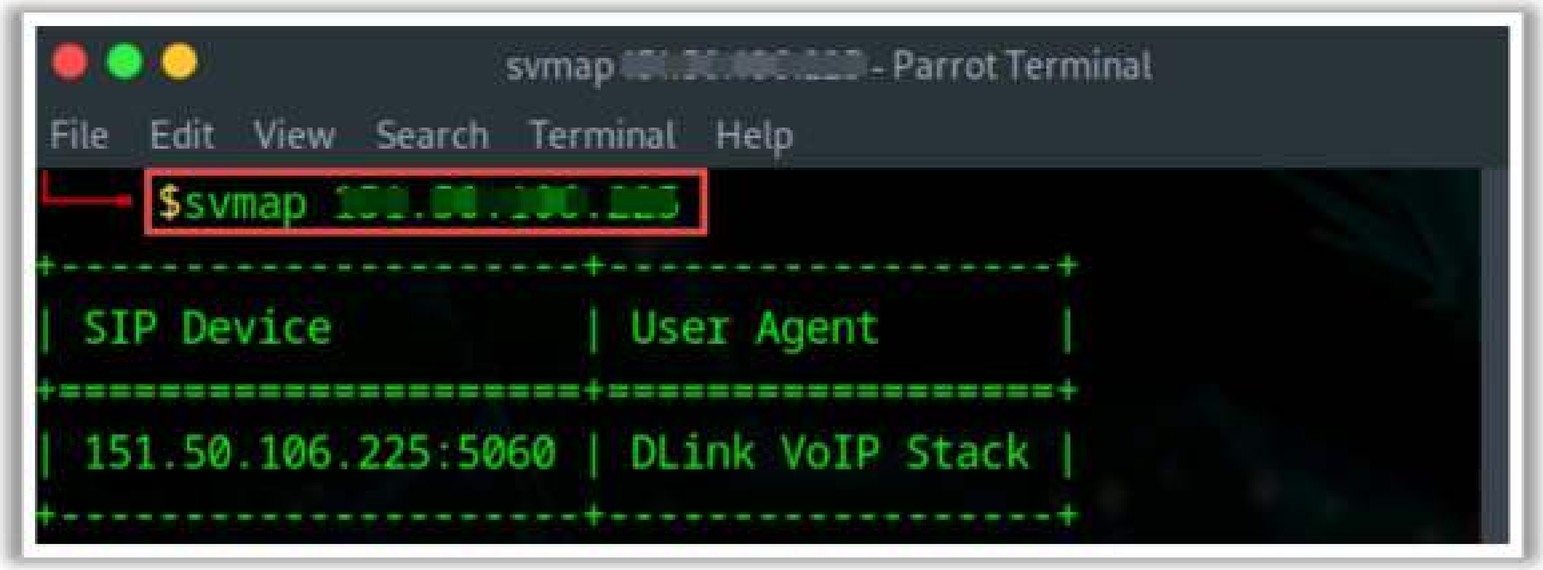
  Attackers use Svmap to perform the following:

  - Identify SIP devices and PBX servers on default and non-default ports
  - Scan large ranges of networks

- Scan one host on different ports for an SIP service on that host or multiple hosts on multiple ports
- Ring all the phones on a network simultaneously using the INVITE method

Below screenshot shows an example for the enumeration of SIP device details using the Svmap tool through the following command:

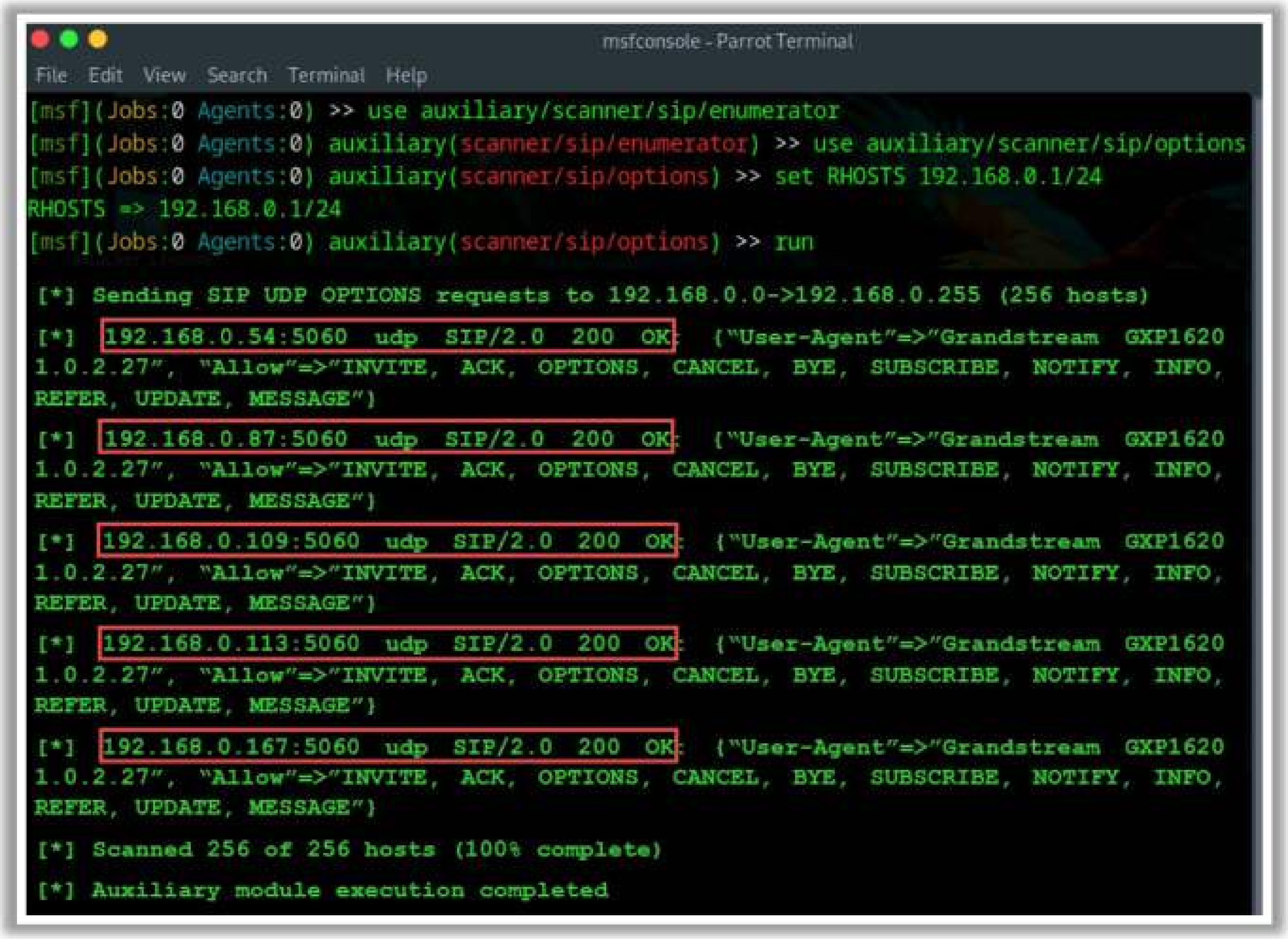
```
# svmap <target network range/IP Address>
```


svmap [redacted] - Parrot Terminal
File Edit View Search Terminal Help

```
$svmap [redacted]
+---------------------+------------------+
| SIP Device          | User Agent       |
+=====================+==================+
| 151.50.106.225:5060 | DLink VoIP Stack |
+---------------------+------------------+
```

Figure 4.58: Screenshot displaying Svmap scan for enumerating SIP details

Attackers use Metasploit's SIP Username Enumerator to scan numeric usernames/extensions of VoIP phones. Below screenshot shows an example for enumerating SIP using Metasploit.


msfconsole - Parrot Terminal
File Edit View Search Terminal Help

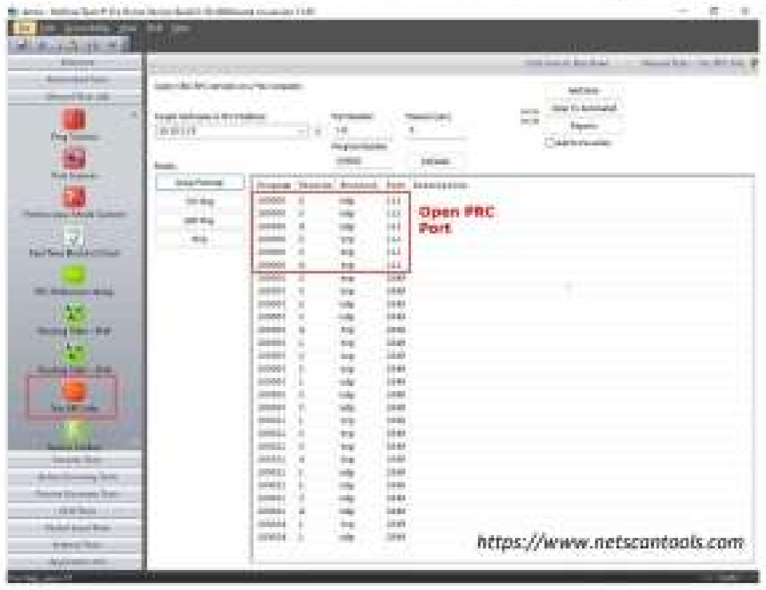
```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/sip/enumerator
[msf](Jobs:0 Agents:0) auxiliary(scanner/sip/enumerator) >> use auxiliary/scanner/sip/options
[msf](Jobs:0 Agents:0) auxiliary(scanner/sip/options) >> set RHOSTS 192.168.0.1/24
RHOSTS => 192.168.0.1/24
[msf](Jobs:0 Agents:0) auxiliary(scanner/sip/options) >> run

[*] Sending SIP UDP OPTIONS requests to 192.168.0.0->192.168.0.255 (256 hosts)
[*] 192.168.0.54:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620
1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] 192.168.0.87:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620
1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] 192.168.0.109:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620
1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] 192.168.0.113:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620
1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] 192.168.0.167:5060 udp SIP/2.0 200 OK: {"User-Agent"=>"Grandstream GXP1620
1.0.2.27", "Allow"=>"INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO,
REFER, UPDATE, MESSAGE"}
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 4.59: Screenshot displaying Metasploit exploit for SIP enumeration

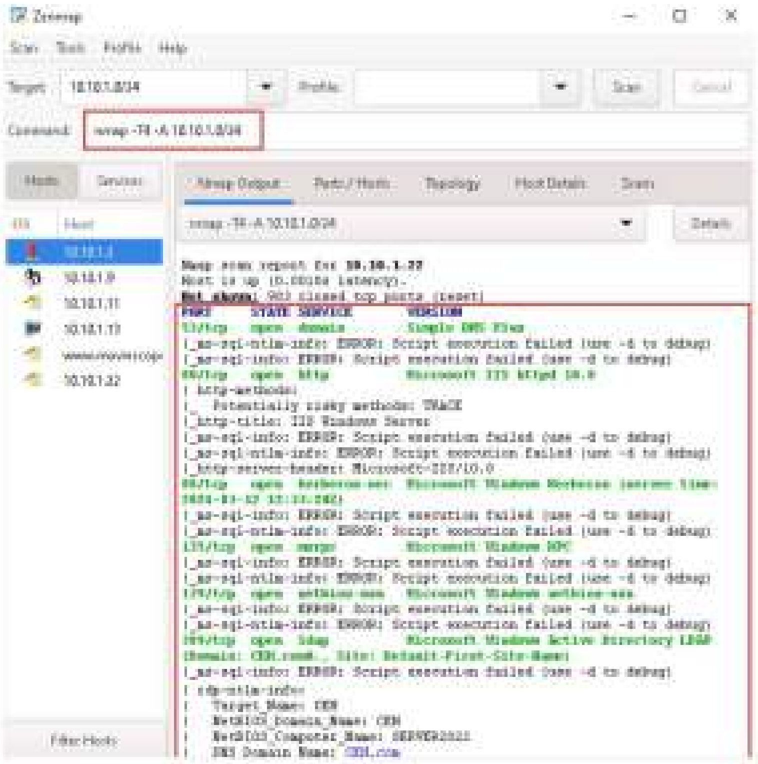
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



https://www.netscantools.com



```
Nmap scan report for 10.10.1.22
Host is up ([illegible] latency).
Not shown: [illegible] closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http         Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time:
[illegible])
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
135/tcp  open  msrpc        Microsoft Windows RPC
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP
(Domain: CEH.com0., Site: Default-First-Site-Name)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
| rdp-ntlm-info:
|   Target_Name: CEH
|   NetBIOS_Domain_Name: CEH
|   NetBIOS_Computer_Name: SERVER2022
|   DNS_Domain_Name: CEH.com
```

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

RPC Enumeration

The remote procedure call (RPC) is a technology used for creating distributed client/server programs. RPC allows clients and servers to communicate in distributed client/server programs. It is an inter-process communication mechanism, which enables data exchange between different processes. In general, RPC consists of components such as a client, a server, an endpoint, an endpoint mapper, a client stub, and a server stub, along with various dependencies.

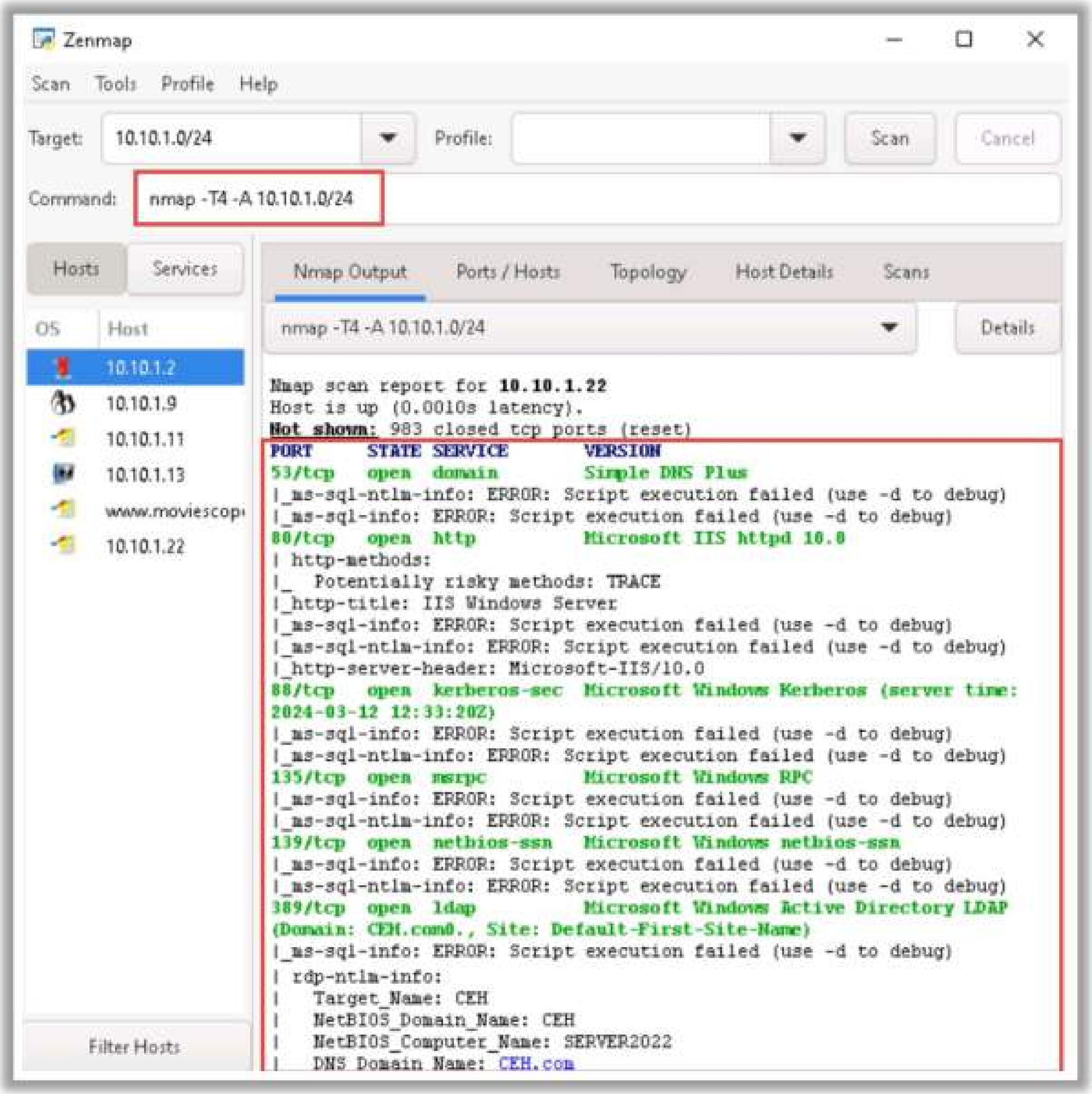
The portmapper service listens on TCP and UDP port 111 to detect the endpoints and present clients, along with details of listening RPC services. Enumerating RPC endpoints enables attackers to identify any vulnerable services on these service ports. In networks protected by firewalls and other security establishments, this portmapper is often filtered. Therefore, attackers scan wide port ranges to identify RPC services that are open to direct attack.

Attackers use the following Nmap scan commands to identify the RPC service running on the network:

```
# nmap -sR <target IP/network>
# nmap -T4 –A <target IP/network>
```

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24



Target: 10.10.1.0/24

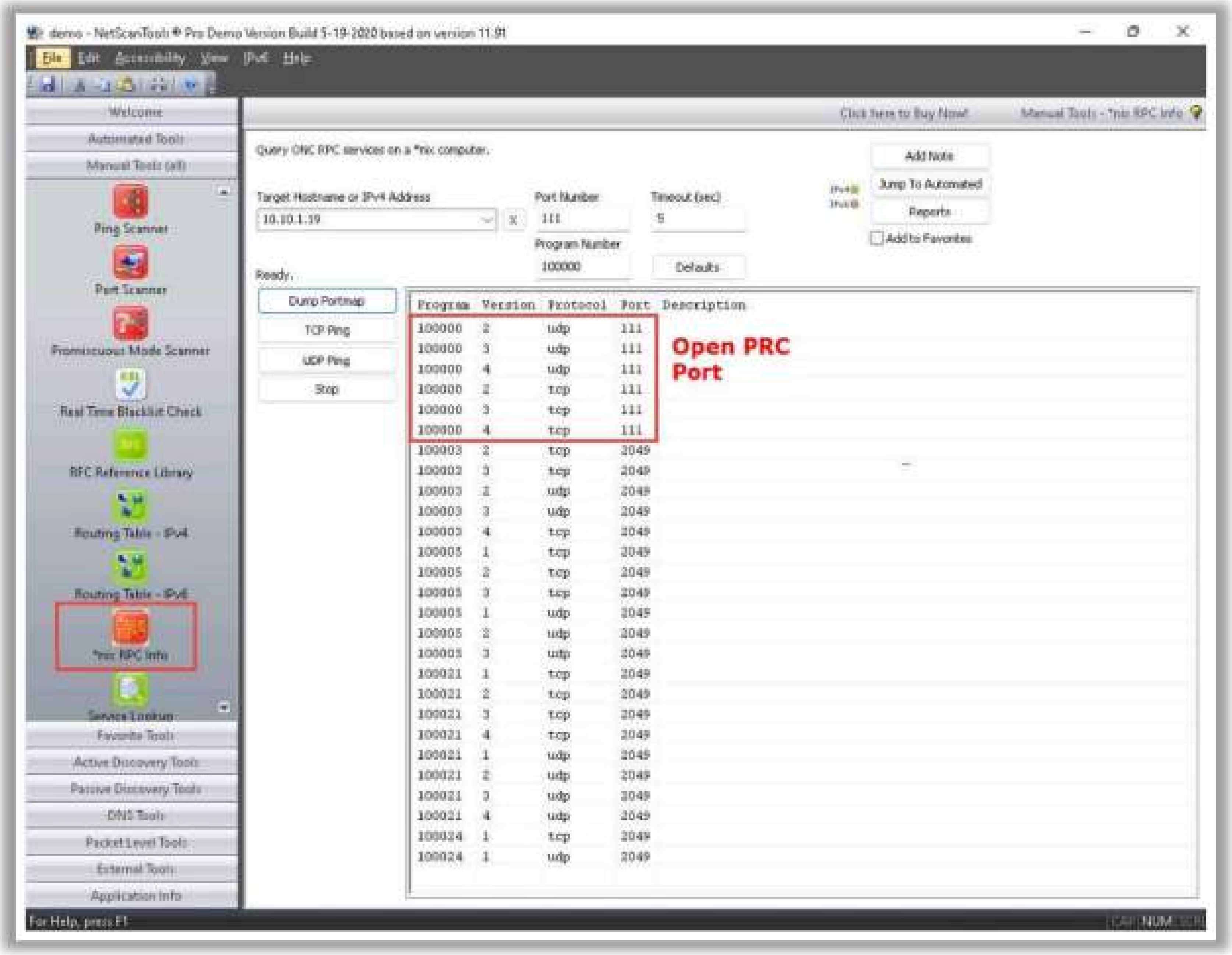
Command: nmap -T4 -A 10.10.1.0/24

nmap -T4 -A 10.10.1.0/24

```
Nmap scan report for 10.10.1.22
Host is up (0.0010s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time:
2024-03-12 12:33:20Z)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
135/tcp  open  msrpc         Microsoft Windows RPC
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP
(Domain: CEH.com0., Site: Default-First-Site-Name)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
| rdp-ntlm-info:
|   Target_Name: CEH
|   NetBIOS_Domain_Name: CEH
|   NetBIOS_Computer_Name: SERVER2022
|   DNS_Domain_Name: CEH.com
```

Figure 4.60: Screenshot displaying an Nmap scan result for RPC enumeration

Additionally, attackers use tools such as NetScanTools Pro to capture the RPC information of the target network. The NetScanTools Pro RPC Info tool helps attackers detect and access the portmapper daemon/service that typically runs on port 111 of Unix or Linux machines.



Query ONC RPC services on a *nix computer.

Target Hostname or IPv4 Address: 10.10.1.19

Port Number: 111

Timeout (sec): 5

Program Number: 100000

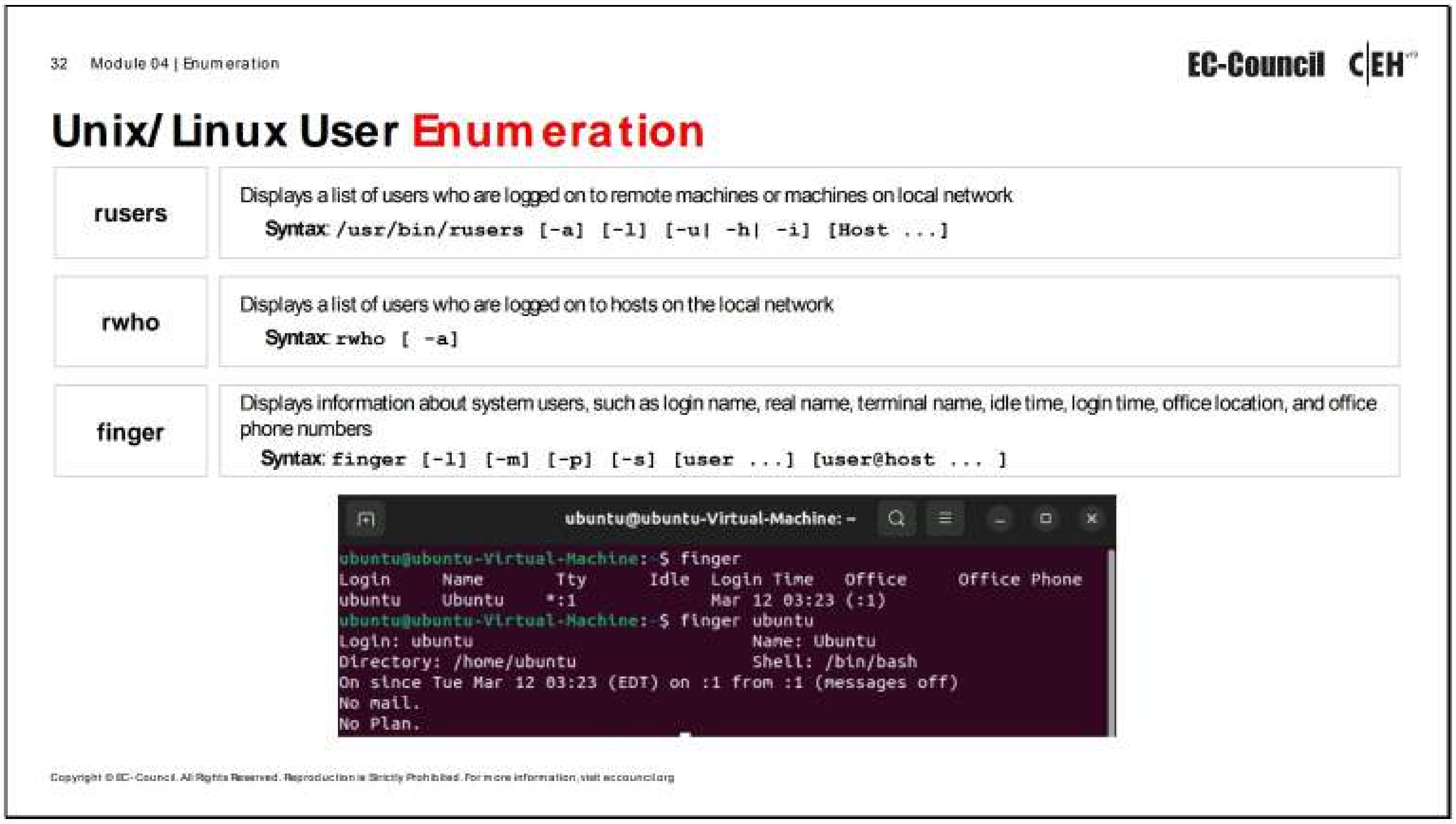
Ready.

```
Program  Version  Protocol  Port  Description
100000   2        udp       111
100000   3        udp       111
100000   4        udp       111
100000   2        tcp       111
100000   3        tcp       111
100000   4        tcp       111
100003   2        tcp       2049
100003   3        tcp       2049
100003   2        udp       2049
100003   3        udp       2049
100003   4        tcp       2049
100005   1        tcp       2049
100005   2        tcp       2049
100005   3        tcp       2049
100005   1        udp       2049
100005   2        udp       2049
100005   3        udp       2049
100021   1        tcp       2049
100021   2        tcp       2049
100021   3        tcp       2049
100021   4        tcp       2049
100021   1        udp       2049
100021   2        udp       2049
100021   3        udp       2049
100021   4        udp       2049
100024   1        tcp       2049
100024   1        udp       2049
```

Figure 4.61: Screenshot displaying NetScanTools Pro tool for RPC enumeration

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24



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 ... ]`

```
ubuntu@ubuntu-Virtual-Machine:~$ finger
Login     Name       Tty      Idle  Login Time   Office     Office Phone
ubuntu    Ubuntu     *:1            Mar 12 03:23 (:1)
ubuntu@ubuntu-Virtual-Machine:~$ finger ubuntu
Login: ubuntu                           Name: Ubuntu
Directory: /home/ubuntu                 Shell: /bin/bash
On since Tue Mar 12 03:23 (EDT) on :1 from :1 (messages off)
No mail.
No Plan.
```

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Unix/Linux User Enumeration

One of the important steps for enumeration is to perform Unix/Linux user enumeration. Unix/Linux user enumeration provides a list of users along with details such as the username, host name, and start date and time of each session.

The following command-line utilities can be used to perform Unix/Linux user enumeration.

- **rusers**

  rusers displays a list of users who are logged in to remote machines or machines on the local network. It displays an output similar to the who command, but for the hosts/systems on the local network. Its syntax is as follows:

  ```
  /usr/bin/rusers [-a] [-l] [-u| -h| -i] [Host ...]
  ```

  The options are as follows.

  - **-a**: Gives a report for a machine even if no users are logged in
  - **-h**: Sorts alphabetically by host name
  - **-l**: Gives a longer listing similar to the who command
  - **-u**: Sorts by the number of users
  - **-i**: Sorts by idle time

- **rwho**

  rwho displays a list of users who are logged in to hosts on the local network. Its output is similar to that of the who command and contains information about the username, host name, and start date and time of each session for all machines on the local network running the rwho daemon. Its syntax is as follows:

  `rwho [ -a]`

  It has the following option.

  - **-a**: Includes all users; without this flag, users whose sessions are idle for an hour or more are not included in the report

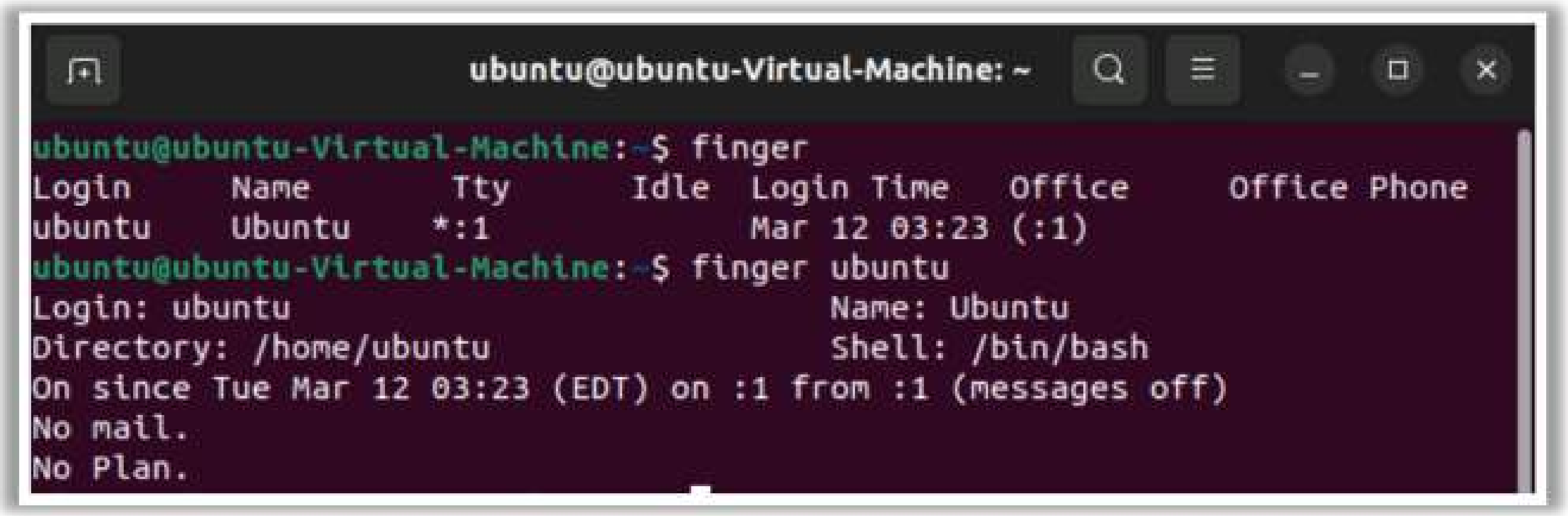
- **finger**

  finger displays information about system users such as the user's login name, real name, terminal name, idle time, login time, office location, and office phone numbers. Its syntax is as follows:

  `finger [-l] [-m] [-p] [-s] [user ...] [user@host ...]`

  The options are as follows.

  - **-s**: Displays the user's login name, real name, terminal name, idle time, login time, office location, and office phone number
  - **-l**: Produces a multi-line format displaying all of the information described for the **-s** option as well as the user's home directory, home phone number, login shell, mail status, and the contents of the files ".plan," ".project," ".pgpkey," and ".forward" from the user's home directory
  - **-p**: Prevents the **-l** option of finger from displaying the contents of the ".plan," ".project," and ".pgpkey" files.
  - **-m**: Prevents the matching of usernames.



```
ubuntu@ubuntu-Virtual-Machine:~$ finger
Login     Name       Tty      Idle  Login Time   Office     Office Phone
ubuntu    Ubuntu     *:1            Mar 12 03:23 (:1)
ubuntu@ubuntu-Virtual-Machine:~$ finger ubuntu
Login: ubuntu                           Name: Ubuntu
Directory: /home/ubuntu                 Shell: /bin/bash
On since Tue Mar 12 03:23 (EDT) on :1 from :1 (messages off)
No mail.
No Plan.
```

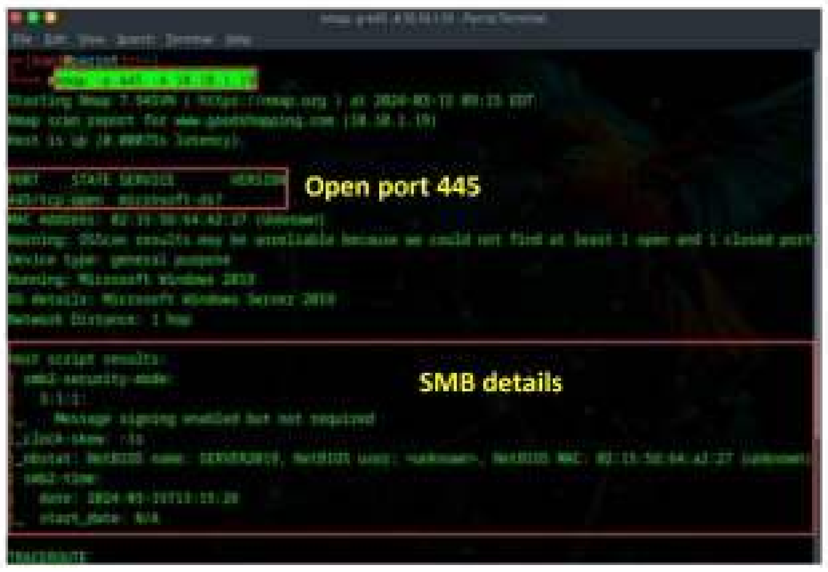
Figure 4.62: Screenshot displaying the execution of the finger command for user enumeration

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24

SMB Enumeration

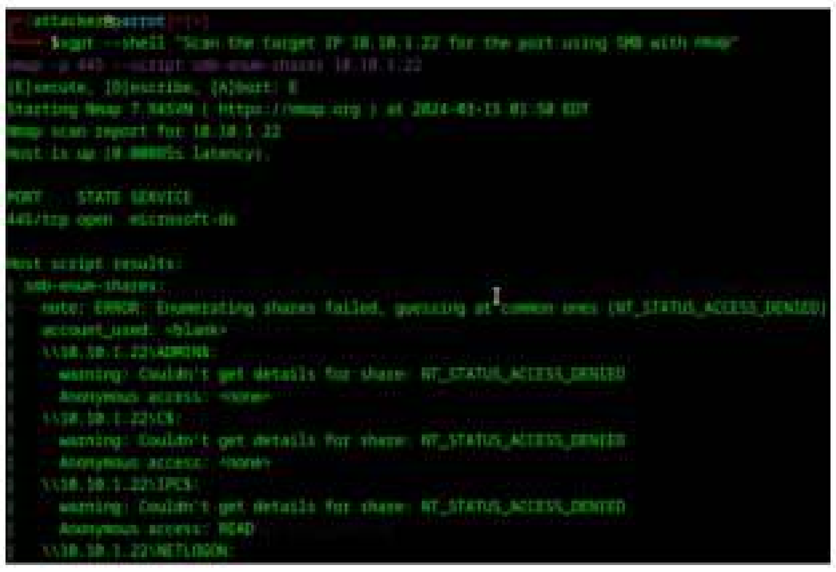
- Attackers use SMB enumeration tools, such as **Nmap**, **SMBMap**, **enum4linux**, and **nullinux**, to perform a directed scan on the SMB service running on port 445
- SMB enumeration helps attackers to perform **OS banner grabbing** on the target



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"



Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

SMB Enumeration

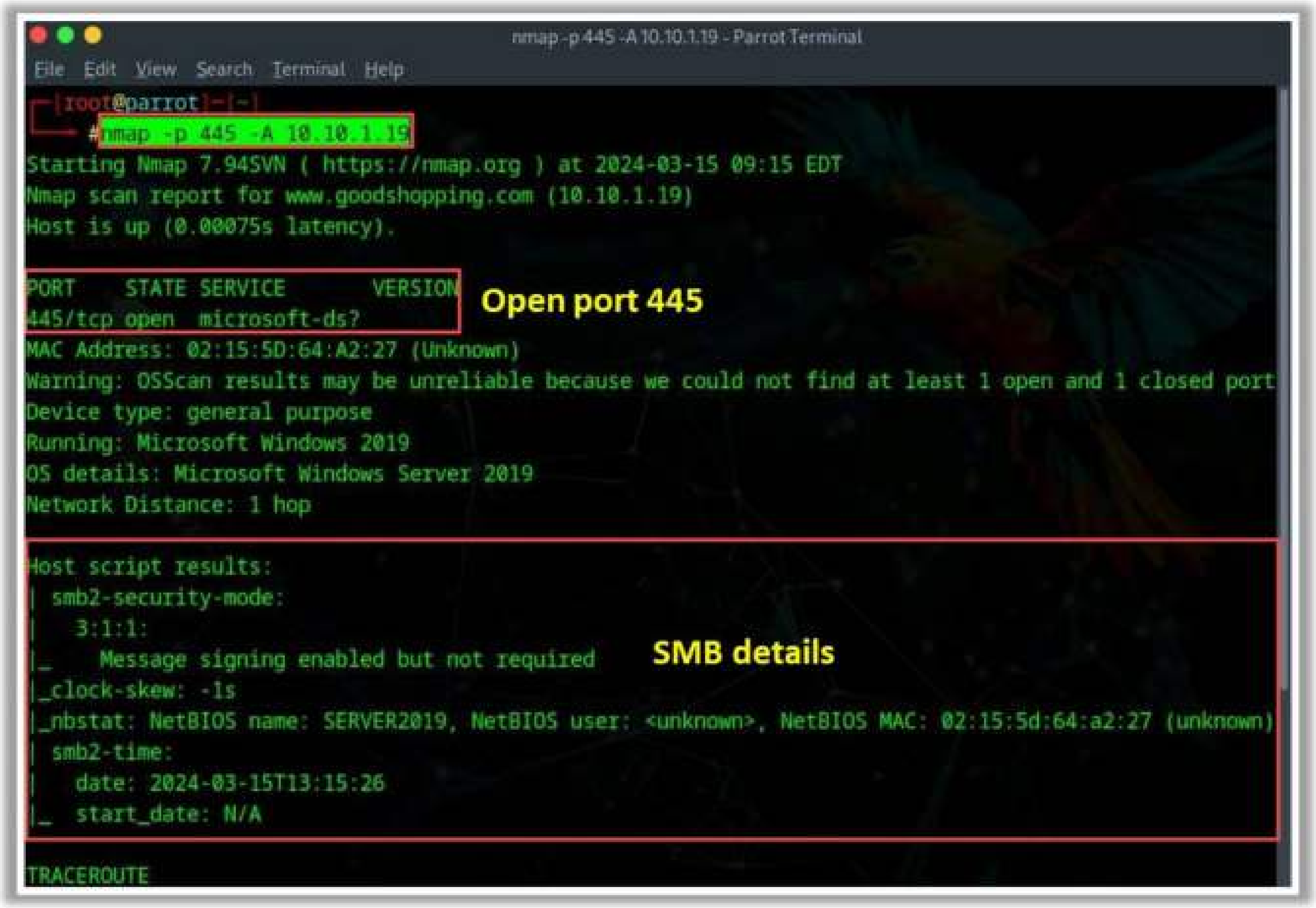
Server Message Block (SMB) is a transport protocol that is generally used by Windows systems for providing shared access to files, printers, and serial ports as well as remote access to Windows services. By default, SMB runs directly on TCP port 445 or via the NetBIOS API on UDP ports 137 and 138 and TCP ports 137 and 139. By using the SMB service, users can access files and other data stored at a remote server. The SMB service also allows application users to read, write, and modify the files on the remote server. A network running this service is highly vulnerable to SMB enumeration, which provides a good amount of information about the target.

In SMB enumeration, attackers generally perform banner grabbing to obtain information such as OS details and versions of services running. By using this information, attackers can perform various attacks such as SMB relay attacks and brute-force attacks. Attackers can also use SMB enumeration tools such as Nmap, SMBMap, enum4linux, nullinux, SMBeagle and NetScanTool Pro to perform a directed scan on the SMB service running on port 445.

As shown in the screenshot, attackers use the following Nmap command to enumerate the SMB service running on the target IP address:

```
# nmap -p 445 -A <target IP>
```

In the above command, the option `-p` specifies a port to scan (`445` in this case), and option `-A` is used for OS detection, version detection, script scanning, and traceroute information.


nmap -p 445 -A 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
Open port 445
SMB details

```
┌─[root@parrot]─[~]
└──╼ #nmap -p 445 -A 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 09:15 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00075s latency).

PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?
MAC Address: 02:15:5D:64:A2:27 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2019
OS details: Microsoft Windows Server 2019
Network Distance: 1 hop

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: -1s
|_nbstat: NetBIOS name: SERVER2019, NetBIOS user: <unknown>, NetBIOS MAC: 02:15:5d:64:a2:27 (unknown)
| smb2-time:
|   date: 2024-03-15T13:15:26
|_  start_date: N/A

TRACEROUTE
```

Figure 4.63: Screenshot of Nmap performing SMB enumeration

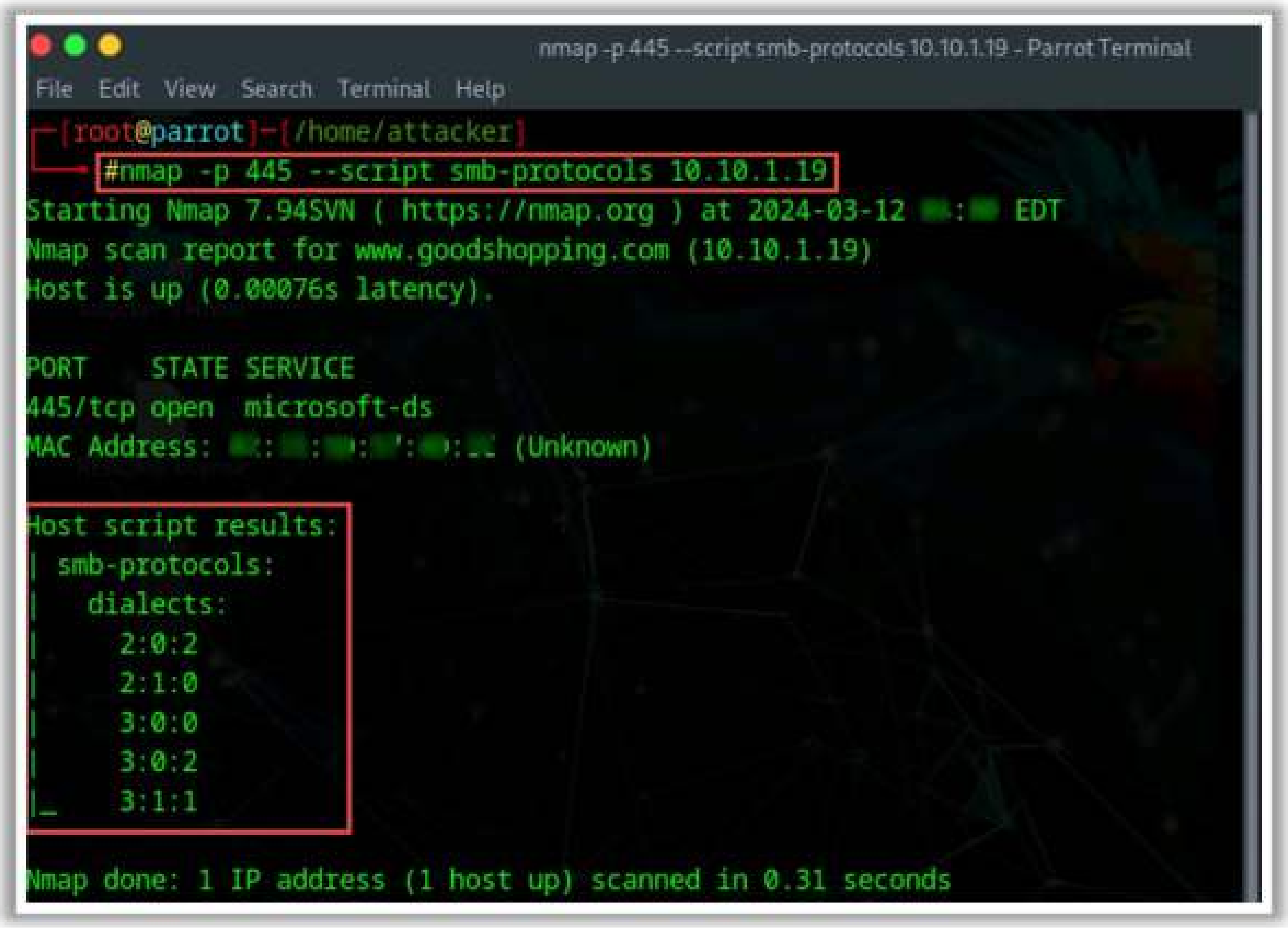
The `STATE` of `PORT 445/tcp` is `OPEN`, which indicates that port 445 is open and that the SMB service is running. By using this command, attackers can also obtain details on the OS and traceroute of the specified target.

As shown in the screenshot, attackers use the following Nmap commands to enumerate the supported protocols and versions of the target SMB server:

```
# nmap -p 445 --script smb-protocols <Target IP>
# nmap -p 139 --script smb-protocols <Target IP>
```

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24


nmap -p 445 --script smb-protocols 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -p 445 --script smb-protocols 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 [redacted]:[redacted] EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00076s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: [redacted]:[redacted]:[redacted]:[redacted]:[redacted]:[redacted] (Unknown)

Host script results:
| smb-protocols:
|   dialects:
|     2:0:2
|     2:1:0
|     3:0:0
|     3:0:2
|_    3:1:1

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

Figure 4.64: Screenshot of Nmap performing SMB enumeration

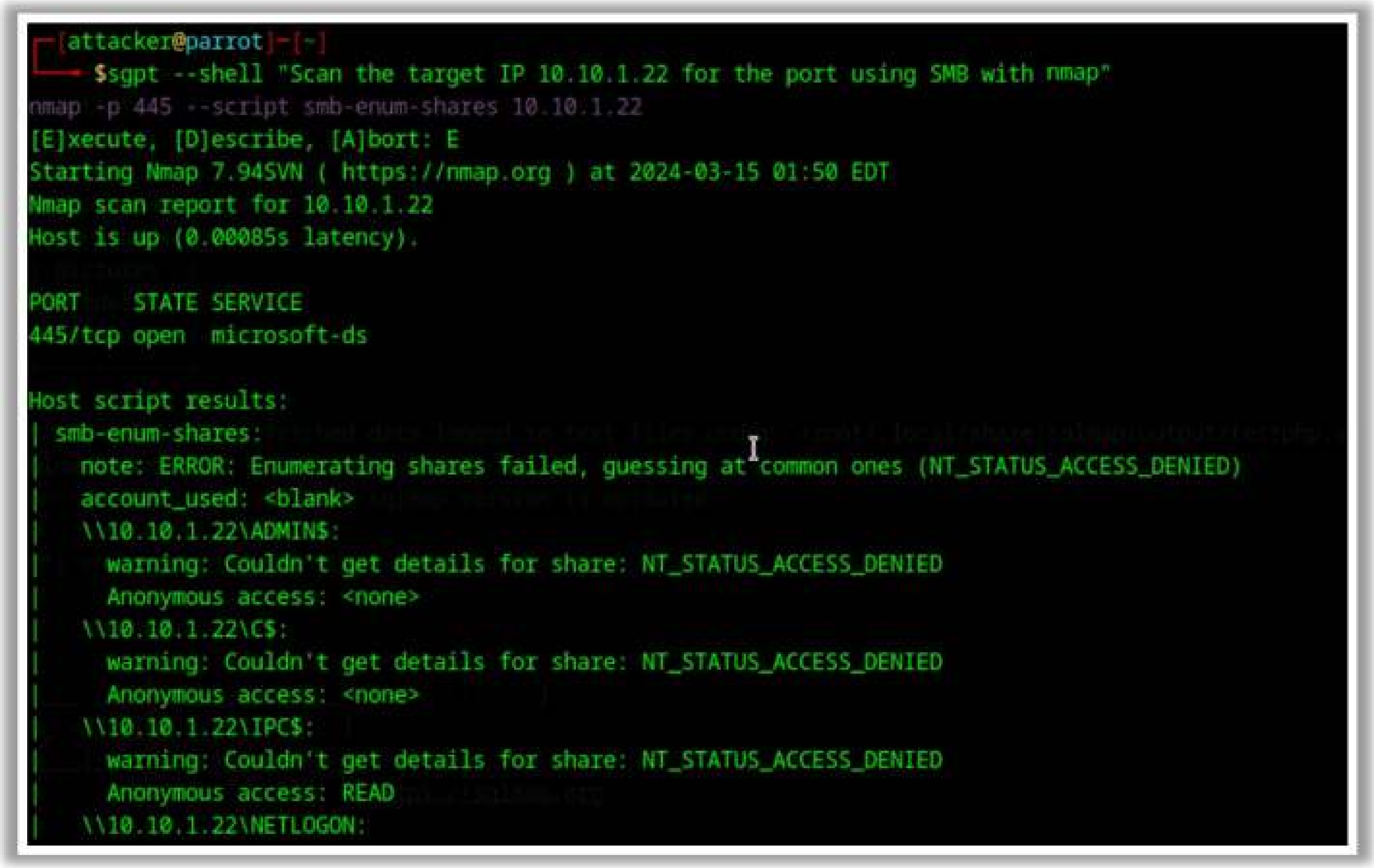
SMB Enumeration with AI

Attackers can leverage AI-powered technologies to enhance and automate their network enumeration tasks. With the aid of AI, attackers can effortlessly perform SMB enumeration on target domains.

For example,

An attacker can use ChatGPT 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".**



```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --shell "Scan the target IP 10.10.1.22 for the port using SMB with nmap"
nmap -p 445 --script smb-enum-shares 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 01:50 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00085s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\10.10.1.22\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.10.1.22\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.10.1.22\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: READ
|   \\10.10.1.22\NETLOGON:
```

Figure 4.65: Scan the target IP for the port using SMB with nmap

To scan a target IP for open SMB ports using Nmap, you can use the following command:

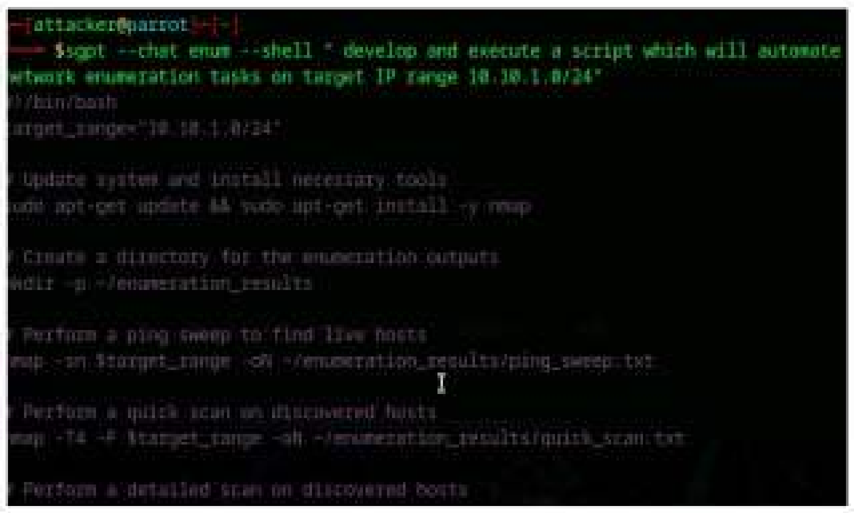
`nmap -p 445 --script smb-enum-shares 10.10.1.22`

- `` `nmap` ``: This is the command to invoke Nmap, a network scanning tool.
- `` `-p 445` ``: This option specifies the port number to scan. Port 445 is commonly associated with Server Message Block (SMB) protocol.
- `` `--script smb-enum-shares` ``: This option specifies the Nmap script to run. **`The`** `` `smb-enum-shares` `` script is used to enumerate shares available on SMB servers.
- `'10.10.1.22'`: This is the target IP address you want to scan for SMB ports.

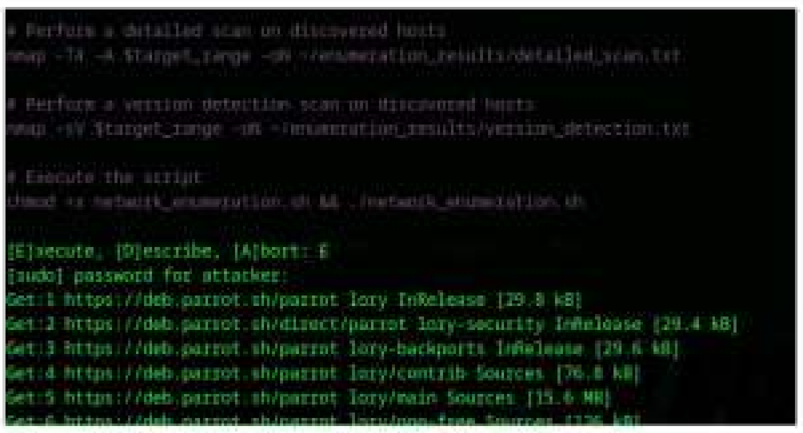
This command instructs Nmap to scan the specified target IP for port 445 (SMB) and to use the smb-enum-shares script to enumerate available shares on SMB servers.

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"***



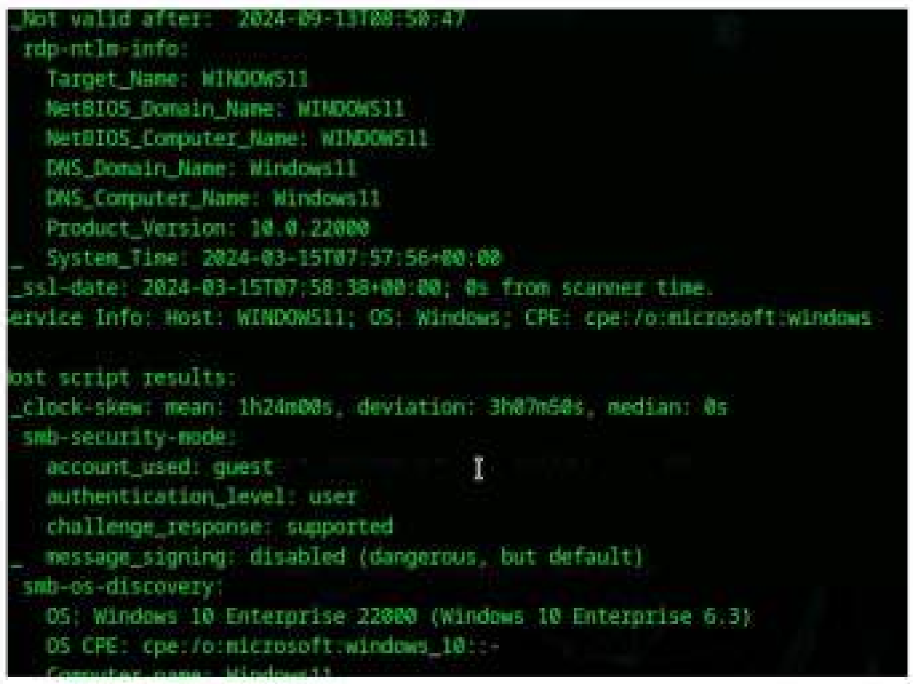
```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --chat enum --shell " develop and execute a script which will automate
etwork enumeration tasks on target IP range 10.10.1.0/24"
!/bin/bash
arget_range="10.10.1.0/24"

# Update system and install necessary tools
udo apt-get update && sudo apt-get install -y nmap

# Create a directory for the enumeration outputs
kdir -p ~/enumeration_results

# Perform a ping sweep to find live hosts
map -sn $target_range -oN ~/enumeration_results/ping_sweep.txt

# Perform a quick scan on discovered hosts
map -T4 -F $target_range -oN ~/enumeration_results/quick_scan.txt

# Perform a detailed scan on discovered hosts
```



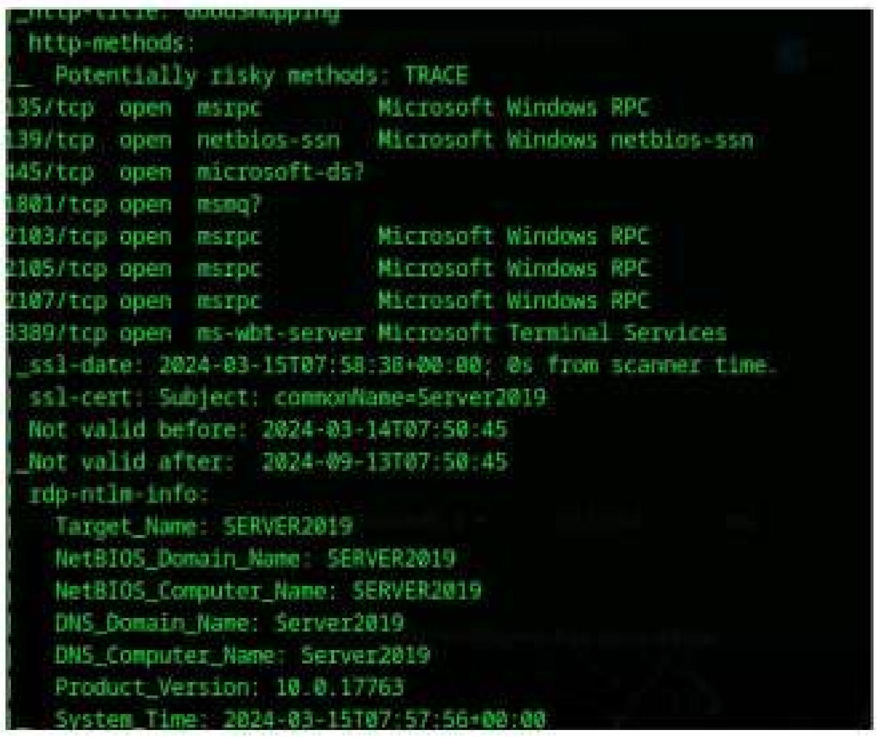
```
# Perform a detailed scan on discovered hosts
nmap -T4 -A $target_range -oN ~/enumeration_results/detailed_scan.txt

# Perform a version detection scan on discovered hosts
nmap -sV $target_range -oN ~/enumeration_results/version_detection.txt

# Execute the script
chmod +x network_enumeration.sh && ./network_enumeration.sh

[E]xecute, [D]escribe, [A]bort: E
[sudo] password for attacker:
Get:1 https://deb.parrot.sh/parrot lory InRelease [29.8 kB]
Get:2 https://deb.parrot.sh/direct/parrot lory-security InRelease [29.4 kB]
Get:3 https://deb.parrot.sh/parrot lory-backports InRelease [29.6 kB]
Get:4 https://deb.parrot.sh/parrot lory/contrib Sources [76.8 kB]
Get:5 https://deb.parrot.sh/parrot lory/main Sources [15.6 MB]
Get:6 https://deb.parrot.sh/parrot lory/non-free Sources [126 kB]
```

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

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

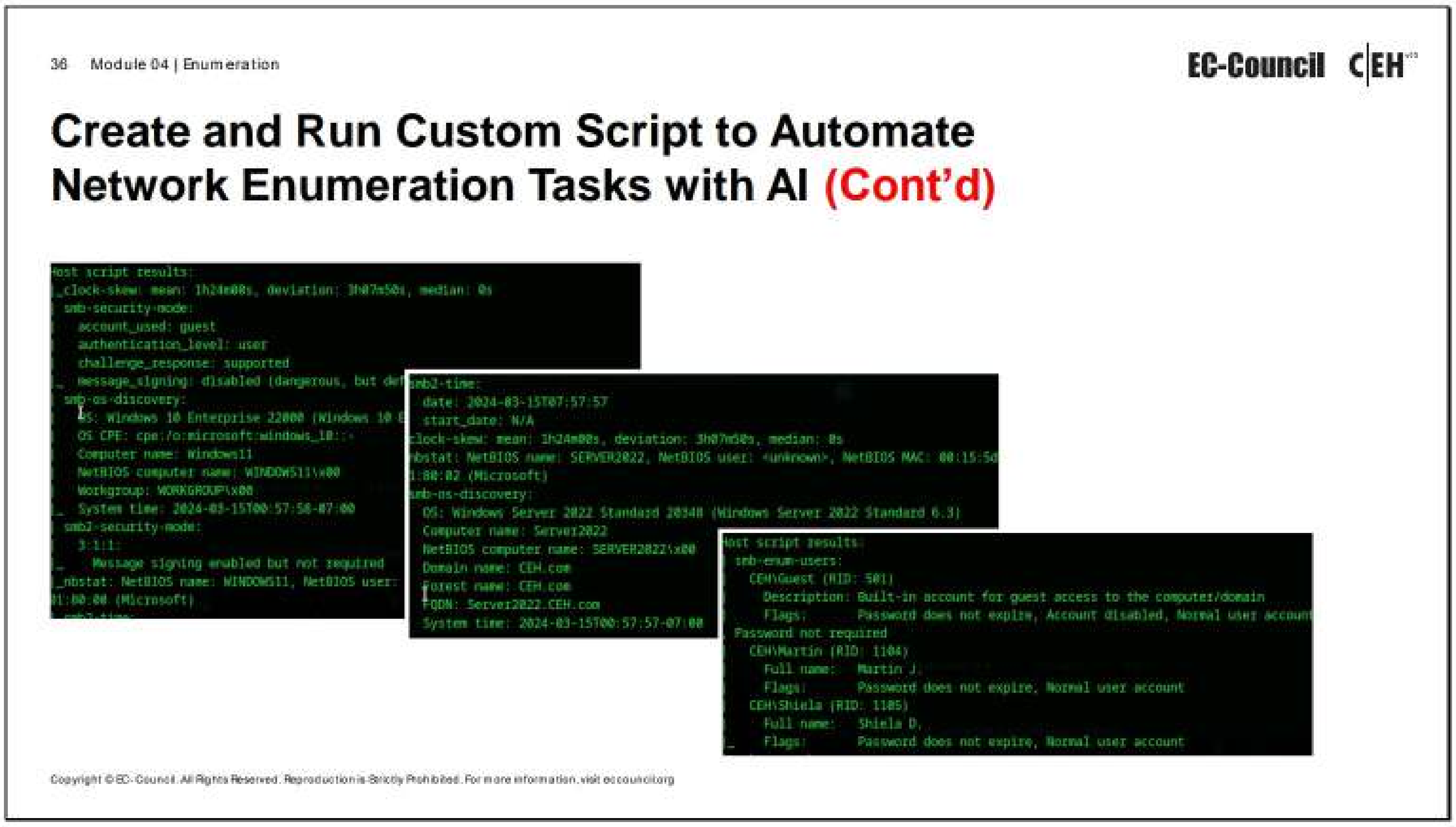


```
_Not valid after:  2024-09-13T08:50:47
 rdp-ntlm-info:
   Target_Name: WINDOWS11
   NetBIOS_Domain_Name: WINDOWS11
   NetBIOS_Computer_Name: WINDOWS11
   DNS_Domain_Name: Windows11
   DNS_Computer_Name: Windows11
   Product_Version: 10.0.22000
_  System_Time: 2024-03-15T07:57:56+00:00
_ssl-date: 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::-
   Computer name: Windows11
```



```
|_http-title: GoodShopping
| 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
```

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org



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

```
Host 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 def
| smb-os-discovery:
|   OS: Windows 10 Enterprise 22000 (Windows 10 E
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: Windows11
|   NetBIOS computer name: WINDOWS11\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-03-15T00:57:58-07:00
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: WINDOWS11, NetBIOS user:
01:00:00 (Microsoft)
```

```
smb2-time:
  date: 2024-03-15T07:57:57
  start_date: N/A
clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s
nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d
1:00:02 (Microsoft)
smb-os-discovery:
  OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
  Computer name: Server2022
  NetBIOS computer name: SERVER2022\x00
  Domain name: CEH.com
  Forest name: CEH.com
  FQDN: Server2022.CEH.com
  System time: 2024-03-15T00:57:57-07:00
```

```
Host script results:
| smb-enum-users:
|   CEH\Guest (RID: 501)
|     Description: Built-in account for guest access to the computer/domain
|     Flags:       Password does not expire, Account disabled, Normal user account
| Password not required
|   CEH\Martin (RID: 1104)
|     Full name:   Martin J.
|     Flags:       Password does not expire, Normal user account
|   CEH\Shiela (RID: 1105)
|     Full name:   Shiela D.
|_    Flags:       Password does not expire, Normal user account
```

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

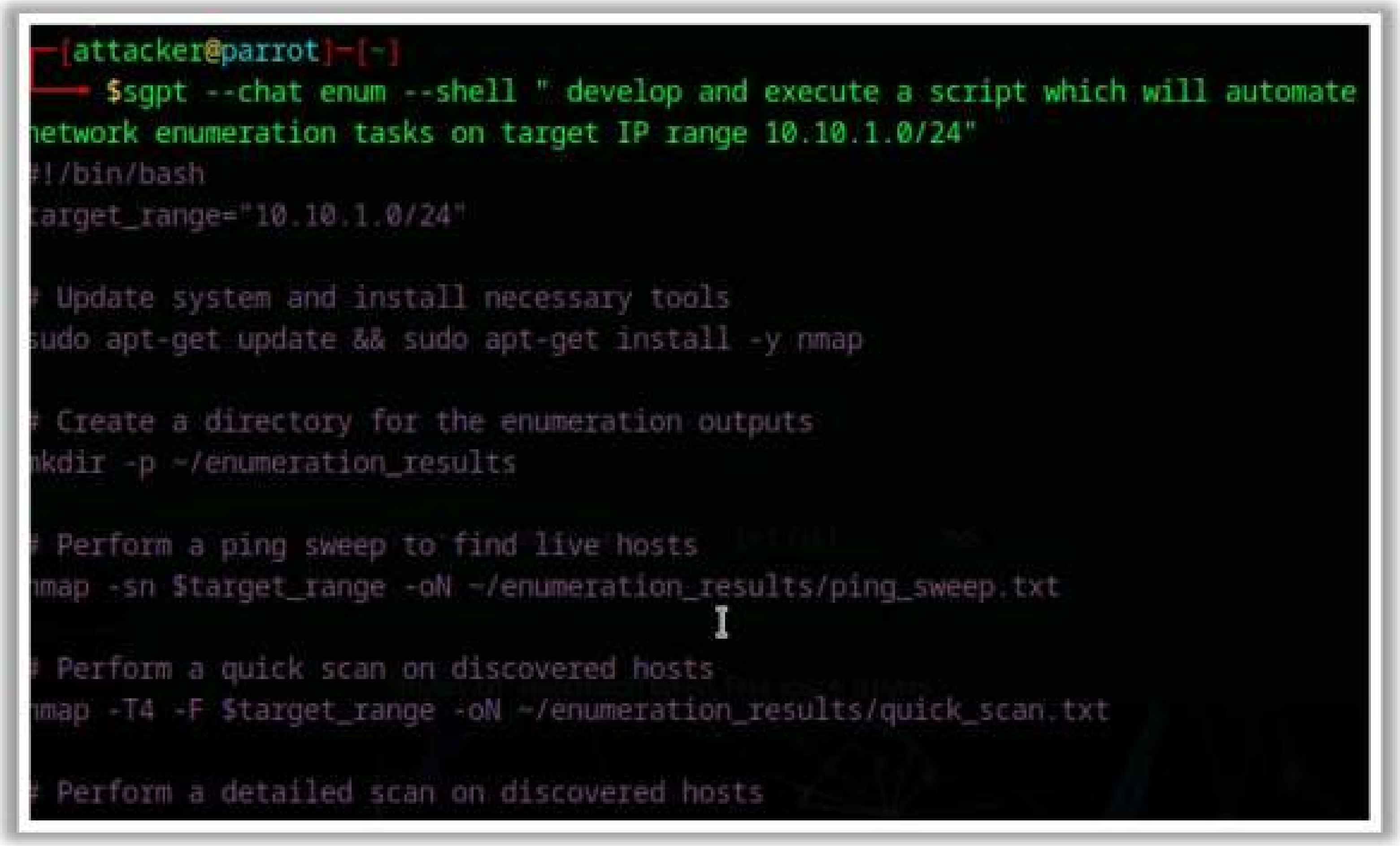
Create and Run Custom Script to Automate Network Enumeration Tasks with AI

Attackers can leverage AI-powered technologies to enhance and automate their network enumeration tasks. With the aid of AI, attackers can effortlessly create and run custom network enumeration scripts and acquire valuable insights about their targets. By developing such custom scripts, attackers can efficiently execute a series of network enumeration commands to gather information about a target domain.

For example,

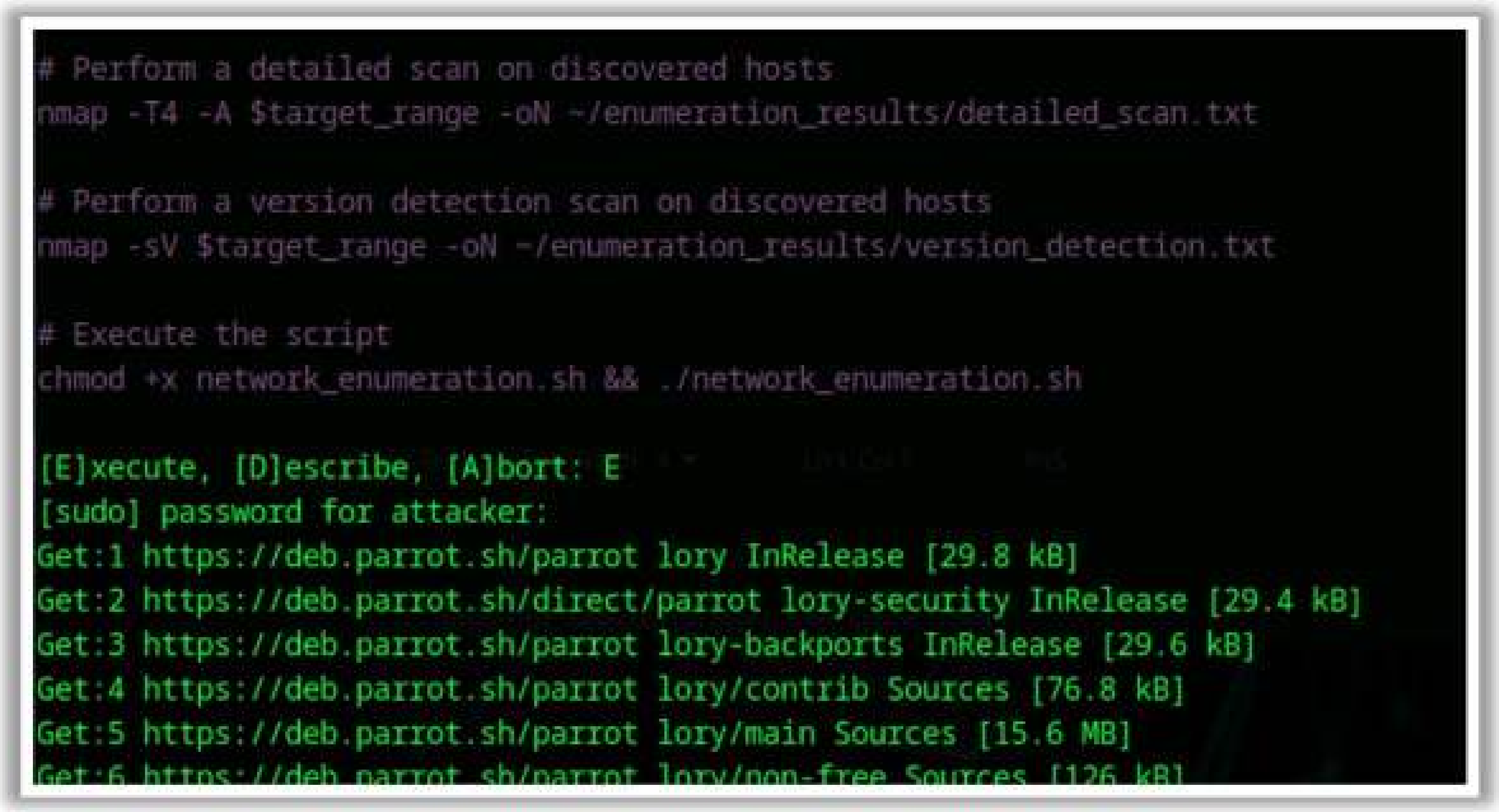
An attacker can use ChatGPT to perform this task by using an appropriate prompt such as:

→ ***"Develop and execute a script that will automate network enumeration tasks on target IP range 10.10.1.0/24".***



```
┌─[attacker@parrot]─[~]
└──╼ $sgpt --chat enum --shell " develop and execute a script which will automate
etwork enumeration tasks on target IP range 10.10.1.0/24"
#!/bin/bash
arget_range="10.10.1.0/24"

# Update system and install necessary tools
sudo apt-get update && sudo apt-get install -y nmap

# Create a directory for the enumeration outputs
kdir -p ~/enumeration_results

# Perform a ping sweep to find live hosts
map -sn $target_range -oN ~/enumeration_results/ping_sweep.txt

# Perform a quick scan on discovered hosts
map -T4 -F $target_range -oN ~/enumeration_results/quick_scan.txt

# Perform a detailed scan on discovered hosts
```

Figure 4.66: Script that will automate network enumeration tasks on target IP range



```
# Perform a detailed scan on discovered hosts
nmap -T4 -A $target_range -oN ~/enumeration_results/detailed_scan.txt

# Perform a version detection scan on discovered hosts
nmap -sV $target_range -oN ~/enumeration_results/version_detection.txt

# Execute the script
chmod +x network_enumeration.sh && ./network_enumeration.sh

[E]xecute, [D]escribe, [A]bort: E
[sudo] password for attacker:
Get:1 https://deb.parrot.sh/parrot lory InRelease [29.8 kB]
Get:2 https://deb.parrot.sh/direct/parrot lory-security InRelease [29.4 kB]
Get:3 https://deb.parrot.sh/parrot lory-backports InRelease [29.6 kB]
Get:4 https://deb.parrot.sh/parrot lory/contrib Sources [76.8 kB]
Get:5 https://deb.parrot.sh/parrot lory/main Sources [15.6 MB]
Get:6 https://deb.parrot.sh/parrot lory/non-free Sources [126 kB]
```

Figure 4.67: Script that will automate network enumeration tasks on target IP range

```
#!/bin/bash
target_range="10.10.1.0/24"
#Update system and install necessary tools
sudo apt-get update && sudo apt-get install -y nmap
#Create a directory for the enumeration outputs
mkdir -p ~/enumeration_results
#Perform a ping sweep to find live hosts
nmap -sn $target_range -oN ~/enumeration_results/ping_sweep.txt
#Perform a quick scan on discovered hosts
nmap -T4 -F $target_range -oN ~/enumeration_results/quick_scan.txt
```

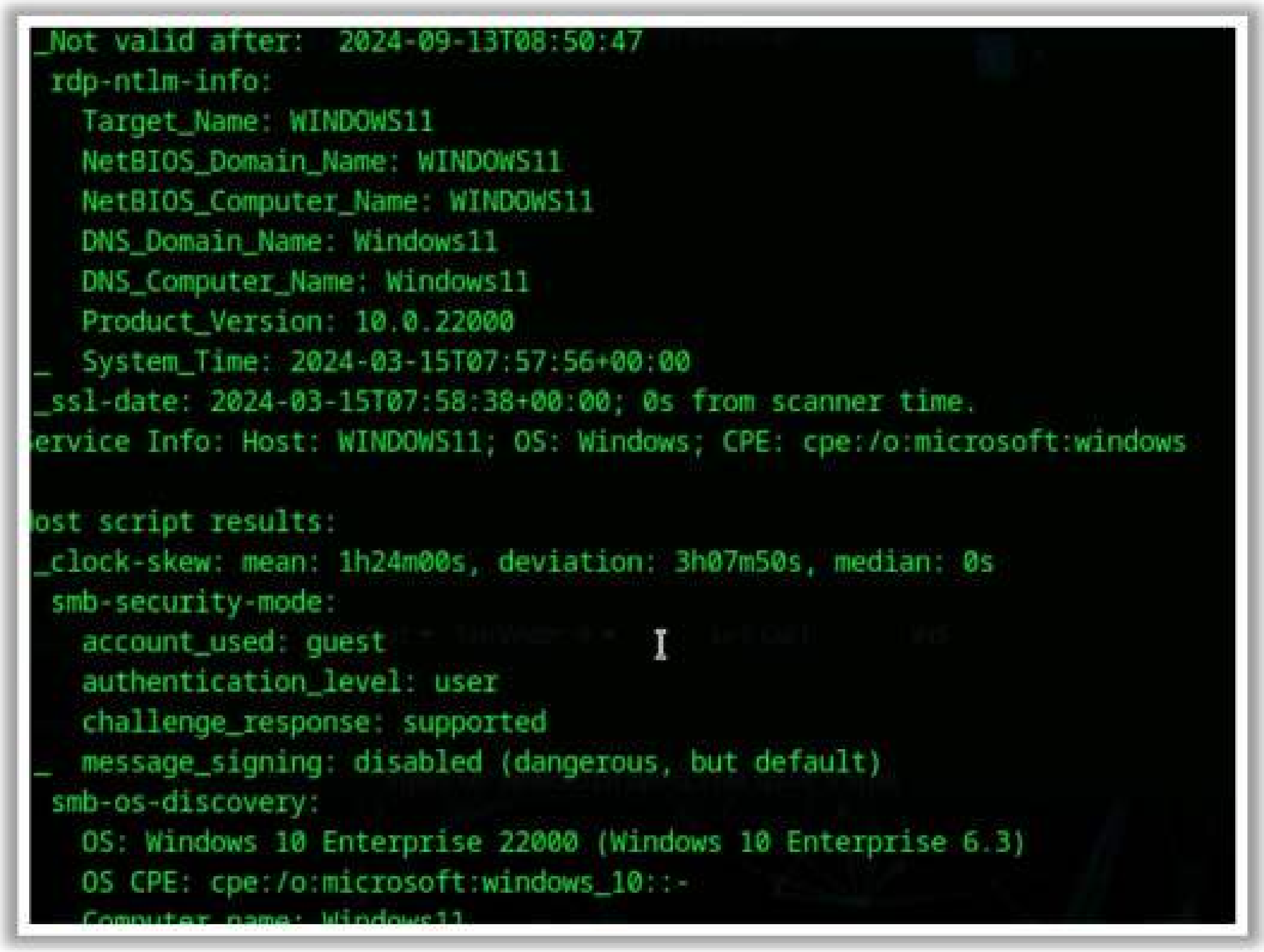
```
    #Perform a detailed scan on discovered hosts
    nmap -T4 -A $target_range -oN ~/enumeration_results/detailed_scan.txt
    #Perform a version detection scan on discovered hosts
    nmap -sV $target_range -oN ~/enumeration_results/version_detection.txt
    #Execute the script
   chmod +x network_enumeration.sh && ./network_enumeration.sh
```

The shell script is designed to perform network enumeration tasks using Nmap on a specified target range.

- `` `#!/bin/bash` ``: This line specifies the shebang, indicating that the script should be executed using the Bash shell.
- `` `target_range="10.10.1.0/24"` ``: This variable stores the target IP range to be scanned.
- `` `sudo apt-get update && sudo apt-get install -y nmap` ``: This command updates the system's package lists and installs Nmap if it is not already installed.
- `` `mkdir -p ~/enumeration_results` ``: This command creates a directory named "enumeration_results" in the user's home directory to store the enumeration outputs.
- `` `nmap -sn $target_range -oN ~/enumeration_results/ping_sweep.txt` ``: This command performs a ping sweep to find live hosts in the specified target range and saves the results to a file named "ping_sweep.txt".
- `` `nmap -T4 -F $target_range -oN ~/enumeration_results/quick_scan.txt` ``: This command performs a quick scan on discovered hosts, focusing on the most common ports, and saves the results to a file named "quick_scan.txt".
- `` `nmap -T4 -A $target_range -oN ~/enumeration_results/detailed_scan.txt` ``: This command performs a detailed scan on discovered hosts, including version detection and OS detection, and saves the results to a file named "detailed_scan.txt".
- `` `nmap -sV $target_range -oN ~/enumeration_results/version_detection.txt` ``: This command performs a version detection scan on discovered hosts and saves the results to a file named "version_detection.txt".
- `` `chmod +x network_enumeration.sh && ./network_enumeration.sh` ``: This line sets the script file as executable and then executes it.

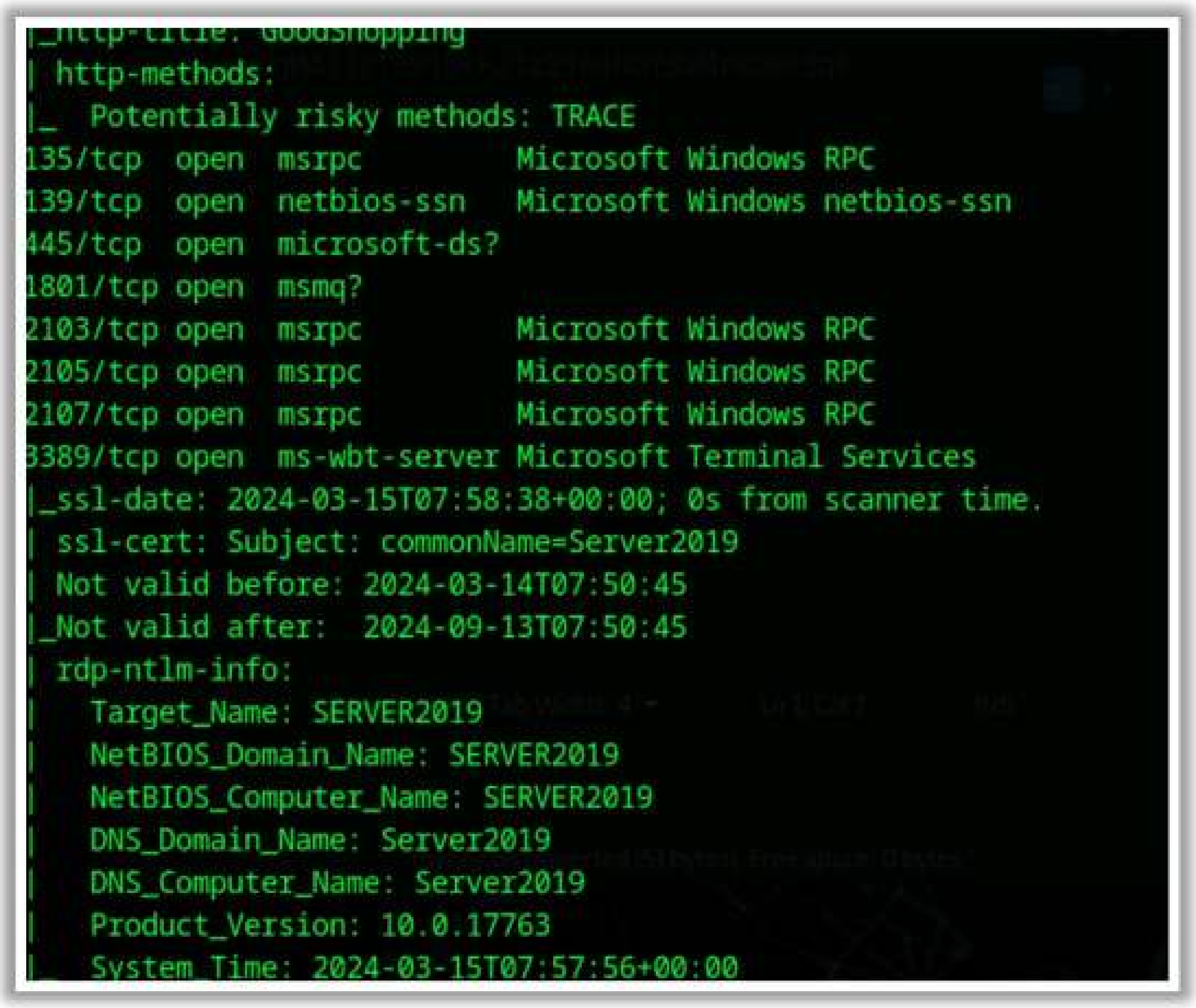
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24



```
_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::-
   Computer name: Windows11
```

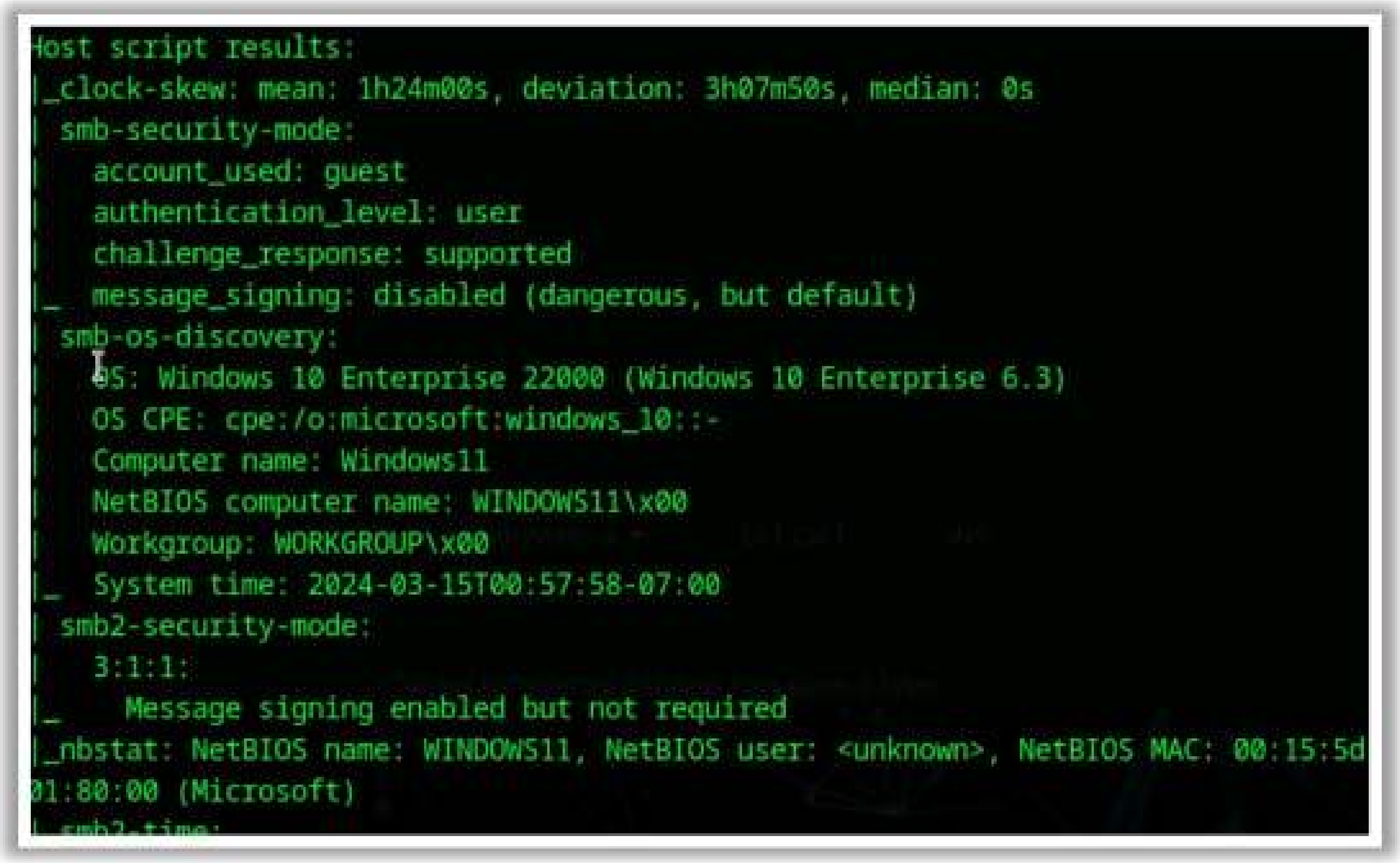
Figure 4.68: Output



```
|_http-title: Goodshopping
| 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
```

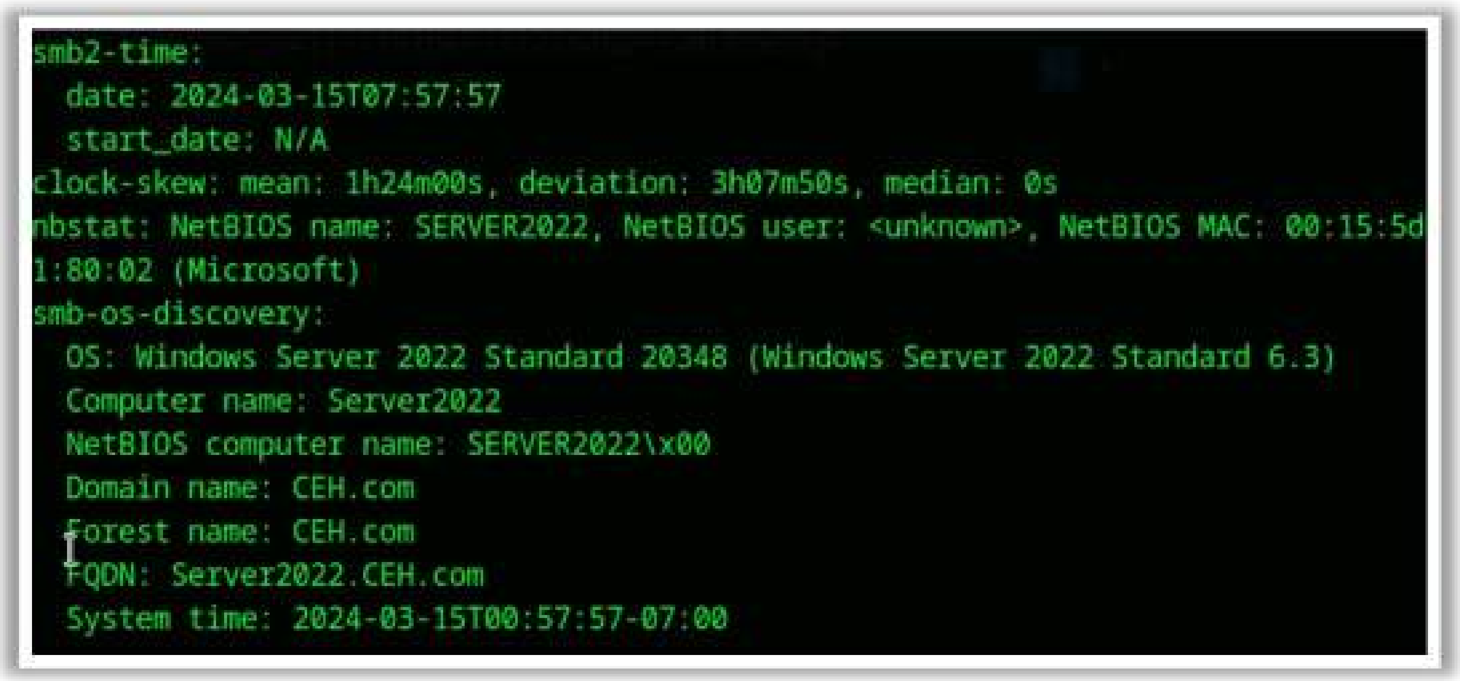
Figure 4.69: Output

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



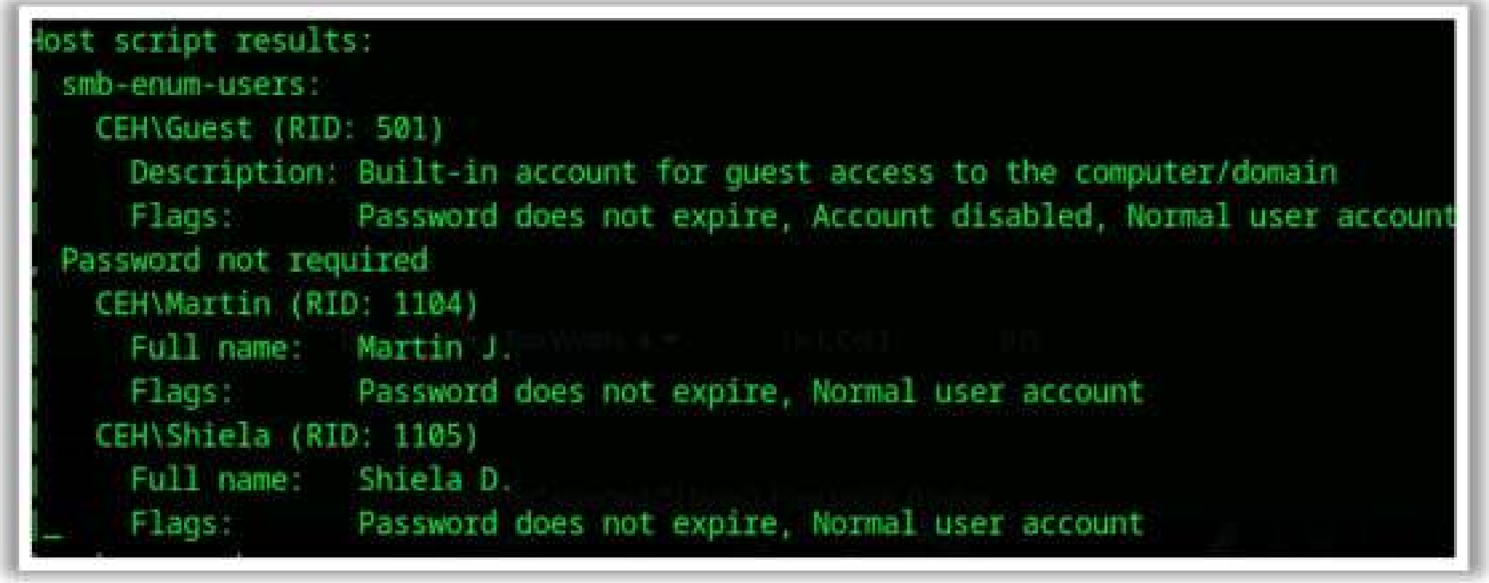
```
Host script results:
|_clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 10 Enterprise 22000 (Windows 10 Enterprise 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: Windows11
|   NetBIOS computer name: WINDOWS11\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-03-15T00:57:58-07:00
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: WINDOWS11, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d
01:80:00 (Microsoft)
| smb2-time:
```

Figure 4.70: Output



```
smb2-time:
  date: 2024-03-15T07:57:57
  start_date: N/A
clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s
nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d
1:80:02 (Microsoft)
smb-os-discovery:
  OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
  Computer name: Server2022
  NetBIOS computer name: SERVER2022\x00
  Domain name: CEH.com
  Forest name: CEH.com
  FQDN: Server2022.CEH.com
  System time: 2024-03-15T00:57:57-07:00
```

Figure 4.71: Output

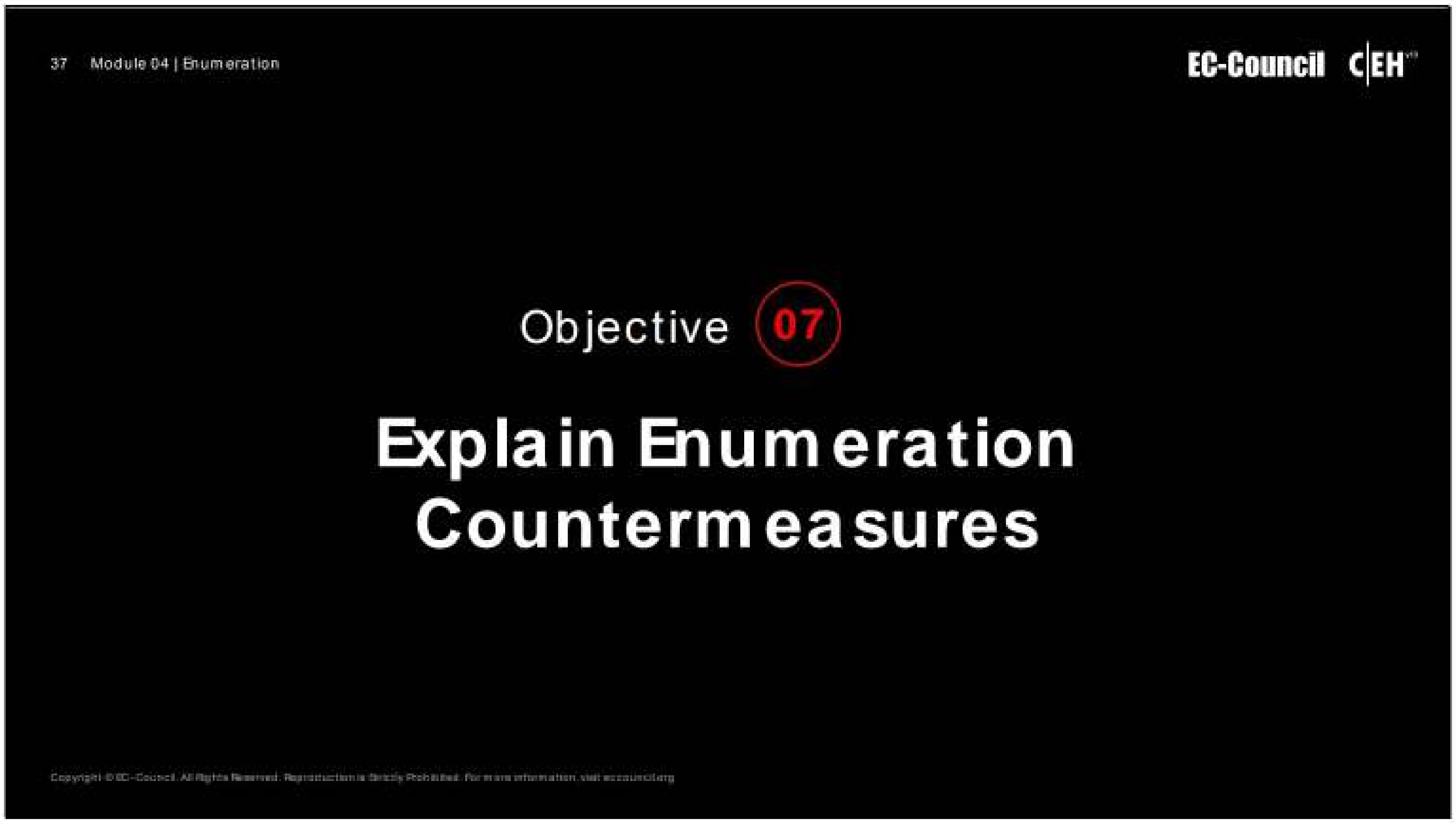


```
Host script results:
| smb-enum-users:
|   CEH\Guest (RID: 501)
|     Description: Built-in account for guest access to the computer/domain
|     Flags:       Password does not expire, Account disabled, Normal user account
 Password not required
|   CEH\Martin (RID: 1104)
|     Full name:   Martin J.
|     Flags:       Password does not expire, Normal user account
|   CEH\Shiela (RID: 1105)
|     Full name:   Shiela D.
|_    Flags:       Password does not expire, Normal user account
```

Figure 4.72: Output

This script automates the process of network enumeration by performing various Nmap scans on the specified target IP range and saving the results to separate files for analysis.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

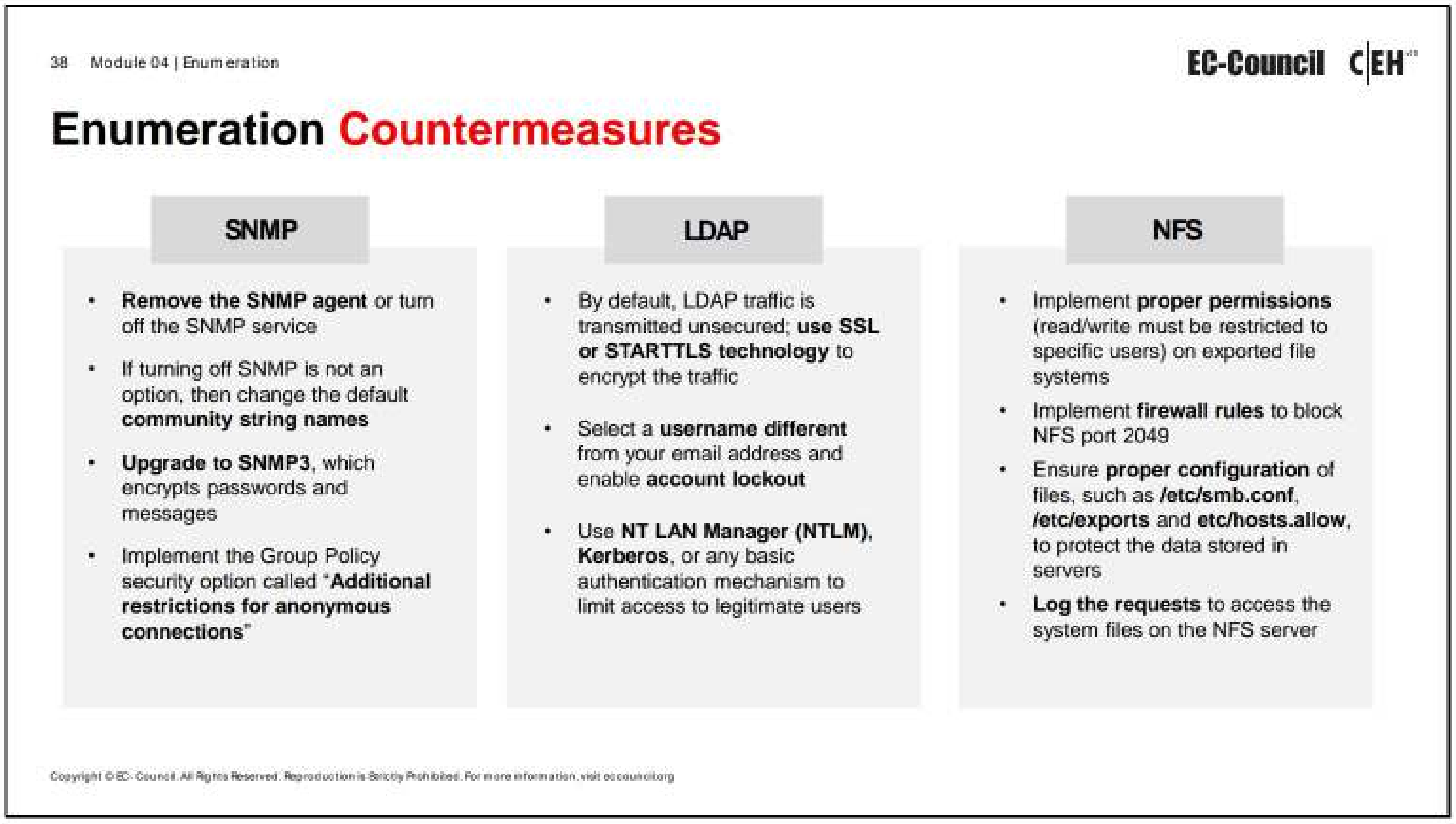


EC-Council C|EH

Objective 07

Explain Enumeration Countermeasures

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org



EC-Council C|EH

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**"

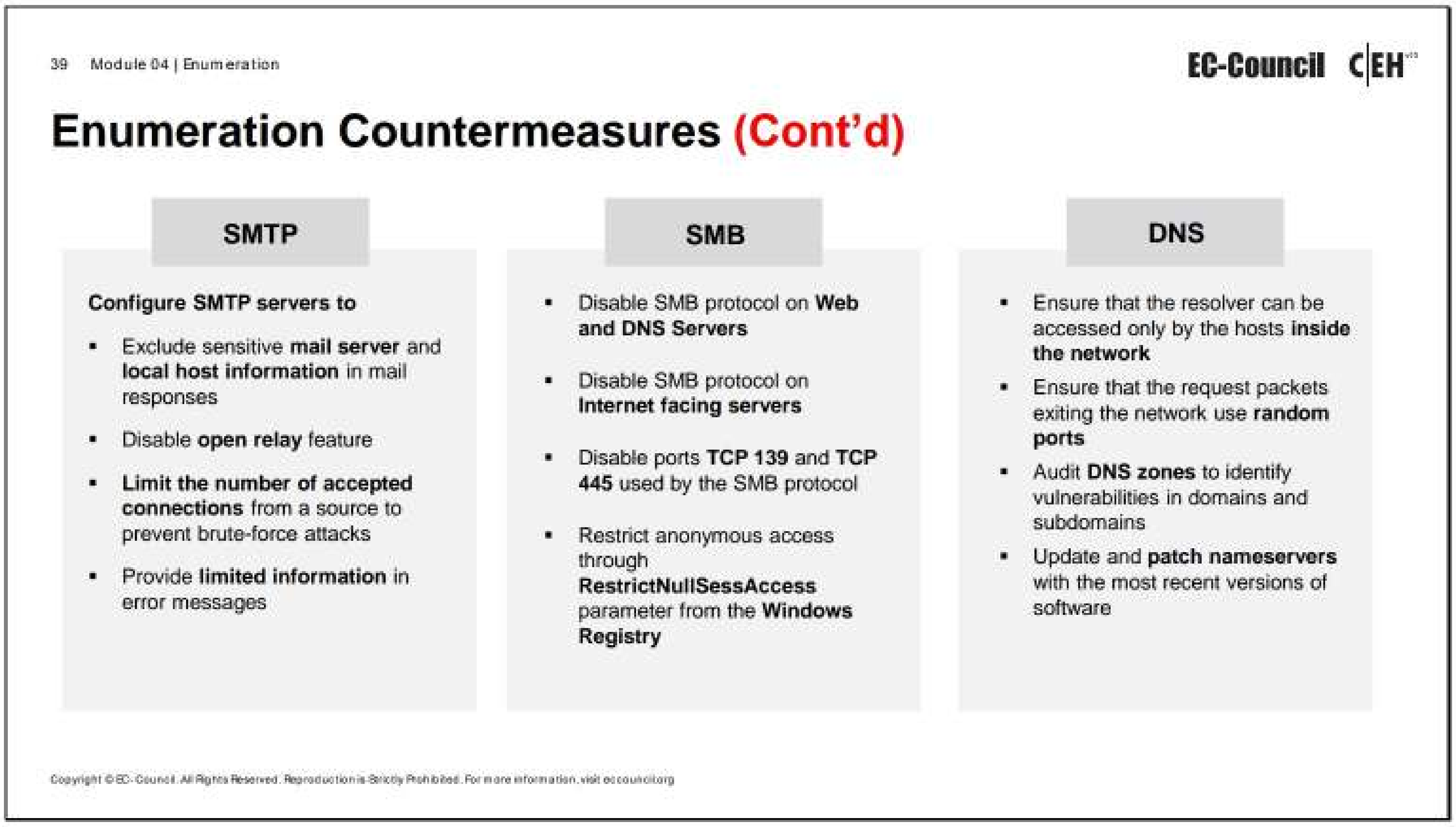
LDAP

- 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

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org



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

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Enumeration Countermeasures

Thus far, we have described the enumeration techniques and tools used to extract valuable information from targets. Next, we discuss countermeasures that can prevent attackers from enumerating sensitive information from a network or host. This section focuses on methods for avoiding information leakage through SNMP, DNS, SMTP, LDAP, SMB, and NFS enumeration.

SNMP Enumeration Countermeasures

- 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."
- Ensure that access to null session pipes, null session shares, and IPsec filtering is restricted.
- Block access to TCP/UDP port 161.
- Do not install the management and monitoring Windows component unless required.
- Encrypt or authenticate using IPsec.
- Do not misconfigure the SNMP service with read-write authorization.
- Configure access-control lists (ACLs) for all SNMP connections to allow only legitimate users to access SNMP devices.

- Limit SNMP access to only those IP addresses or networks that require it for legitimate management purposes. This can be achieved through access control lists (ACLs) on the devices themselves or through network firewalls.
- Regularly audit the network traffic.
- Encrypt credentials using the "AuthNoPriv" mode, which uses MD5 and SHA for additional protection.
- Modify the registry to allow only restricted or permitted access to the SNMP community name.
- Change the default password and periodically change the current password.
- Identify all the SNMP devices with read/write permissions and provide read-only permissions to specific devices that do not require read/write permissions.
- Avoid using the "NoAuthNoPriv" mode as it does not encrypt communications.
- Implement the role-based access control (RBAC) policies to SNMP communities or users.
- Configure SNMPv3 users in the cluster to enhance security with encryption and authentication.
- For devices still using SNMPv1 or SNMPv2c, change the default community strings (the equivalent of passwords for SNMP) from the default "public" and "private" to complex, unique values. Furthermore, restrict write access as much as possible.
- Keep management traffic, including SNMP, on a separate, secure VLAN or network segment. This limits the exposure of SNMP to potential eavesdroppers or attackers on the main network.
- If SNMP is not needed for network management tasks, consider disabling it entirely on devices. This eliminates the protocol as a potential source of information for attackers.
- Manufacturers often release updates that address security vulnerabilities in SNMP implementations. Regularly applying these updates can protect against exploitation.
- Implement monitoring and anomaly detection tools to alert on unusual SNMP traffic patterns, which could indicate enumeration or other malicious activities.
- Ensure SNMP access is logged, and regularly audit these logs for unauthorized access attempts or suspicious activities.

LDAP Enumeration Countermeasures

- By default, LDAP traffic is transmitted unsecured; therefore, use Secure Sockets Layer (SSL) or STARTTLS technology to encrypt the traffic.
- Select a username different from the email address and enable account lockout.
- Restrict access to Active Directory (AD) by using software such as Citrix.
- Use NT LAN Manager (NTLM), Kerberos, or any basic authentication mechanism to limit access to legitimate users.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Log access to Active Directory (AD) services.
- Block users from accessing certain AD entities by changing the permissions on those objects/attributes.
- Deploy canary accounts, which resemble real accounts, to mislead attackers.
- Create decoy groups with the word “Admin” in the name to mislead attackers. Attackers typically search for LDAP admin accounts.
- Enable multi-factor authentication (MFA) for accessing LDAP directories. This adds an additional layer of security, making it harder for attackers to gain unauthorized access using compromised credentials.
- Disable anonymous binds to the LDAP directory unless absolutely necessary for the organization's operation. This ensures that only authenticated users can query the LDAP server.
- Configure ACLs to limit what authenticated users can see and do. ACLs can restrict access to sensitive information based on the user’s credentials and their need to know.
- Ensure that all LDAP queries and modifications are logged. Regularly review these logs for unusual or unauthorized access patterns, which could indicate an enumeration attempt or other malicious activities.
- Employ monitoring tools capable of detecting abnormal LDAP query patterns. Such tools can alert administrators to potential enumeration or attack attempts in real-time.
- Place LDAP servers within a secure network segment, accessible only to those systems and users that require access. This can limit the attack surface and reduce the potential for unauthorized access.
- Configure firewalls to restrict LDAP traffic to and from authorized systems only. This includes blocking unnecessary external access to LDAP services.
- Enforce strong password policies for accounts that have access to LDAP. This minimizes the risk of brute-force or credential stuffing attacks.

NFS Enumeration Countermeasures

- Implement proper permissions (read/write must be restricted to specific users) in 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 the server.
- Review and update the /etc/exports file to ensure that only authorized hosts can access shared directories.
- Use /etc/hosts.allow and /etc/hosts.deny files to define which hosts or networks are allowed or denied access to NFS services.

Technet24

- Log the requests to access the system files on the NFS server.
- Keep the `root_squash` option in the `/etc/exports` file turned **ON** so that no requests made as root on the client are trusted.
- Implement NFS tunneling through SSH to encrypt the NFS traffic over the network.
- Implement the principle of least privileges to mitigate threats such as data modification, data addition, and the modification of configuration files by normal users.
- Ensure that users are not running `suid` and `sgid` on the exported file system.
- Ensure that the NIS netgroup has a fully defined hostname to prevent the granting of higher access to other hosts.
- Configure deep packet inspection (DPI) firewall to monitor all NFS traffic, irrespective of port number.
- Implement Kerberos authentication for NFS to ensure that both the client and server authenticate each other securely. This can help prevent unauthorized access.
- NFSv4 includes support for stronger security features than its predecessors, including the ability to use Kerberos for encryption and authentication. Migrating to NFSv4 can significantly enhance security.
- Keep NFS servers and clients within a secure, segmented part of the network to limit access from unauthorized network segments.
- Configure firewalls to restrict NFS traffic to and from authorized systems only. Blocking unnecessary external access to NFS services can prevent unauthorized discovery and access.
- Regularly monitor NFS server access logs for unusual access patterns or access attempts from unauthorized hosts. This can help in early detection of enumeration or attack attempts.
- Use file system auditing tools to monitor and log access to NFS shares. Auditing can help identify unauthorized access or modifications to sensitive files.
- Regularly update and patch the NFS server software and client systems to protect against known vulnerabilities that could be exploited during enumeration or attacks.

SMTP Enumeration Countermeasures

SMTP servers should be configured in the following manner:

- Ignore email messages to unknown recipients.
- Exclude sensitive information on mail servers and local hosts in mail responses.
- Disable the open relay feature.
- Limit the number of accepted connections from a source to prevent brute-force attacks.
- Disable the EXPN, VRFY, and RCPT TO commands or restrict them to authentic users.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ignore emails to unknown recipients by configuring SMTP servers.
- Identify spammers through machine learning (ML) solutions.
- Do not share internal IP/host information or mail relay system information.
- Implement sender policy framework (SPF), domain keys identified mail (DKIM), and domain-based message authentication and reporting & conformance (DMARC).
- Configure the SMTP server to provide limited information in error messages. Verbose responses can provide attackers with clues about the server configuration or valid user accounts.
- Use ACLs to restrict the use of certain SMTP commands to authorized users or IP addresses. This can prevent anonymous or unauthorized users from attempting to enumerate user information.
- Ensure that the SMTP server requires authentication before allowing access to any information or the ability to send emails. This can help prevent anonymous enumeration attempts.
- Use transport layer security (TLS) to encrypt communication with the SMTP server. This ensures that any data exchanged with the server, including authentication credentials, is encrypted.
- Ensure that the SMTP server logs access attempts and commands used. Regular review of these logs can help identify suspicious activity or attempted enumeration.
- Use security tools that can analyze log files and detect unusual patterns of behavior, such as a high number of failed login attempts, which may indicate an enumeration attempt.
- Use firewalls to control access to the SMTP server, allowing only trusted IP addresses or networks to connect.
- Implement rate limiting to restrict the number of requests that an IP address can make to the SMTP server within a certain timeframe. This can help mitigate brute-force attacks.

SMB Enumeration Countermeasures

Common sharing services or other unused services may provide entry points for attackers to evade network security. A network running SMB is at a high risk of enumeration. Because web and DNS servers do not require this protocol, it is advisable to disable it on them. The SMB protocol can be disabled by disabling the properties **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks** in **Network and Dial-up Connections**. On servers that are accessible from the Internet, also known as bastion hosts, SMB can be disabled by disabling the same two properties of the **TCP/IP properties** dialog box. Another method of disabling the SMB protocol on bastion hosts without explicitly disabling it is to block the ports used by the SMB service. These are TCP ports 139 and 445.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Technet24

Because disabling SMB services is not always a feasible option, other countermeasures against SMB enumeration may be required. Windows Registry can be configured to limit anonymous access from the Internet to a specified set of files. These files and folders are specified in the settings **Network access: Named pipes that can be accessed anonymously** and **Network access: Shares that can be accessed anonymously**. This configuration involves adding the **RestrictNullSessAccess** parameter to the registry key as follows:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

The **RestrictNullSessAccess** parameter takes binary values, where 1 denotes enabled and 0 denotes disabled. Setting this parameter to 1 or enabled restricts the access of anonymous users to the files specified in the **Network access** settings.

The following are additional countermeasures for defending against SMB enumeration.

- Ensure that Windows Firewall or similar endpoint protection systems are enabled on the system.
- Install the latest security patches for Windows and third-party software.
- Implement a proper authentication mechanism with a strong password policy.
- Implement strong permissions to keep the stored information safe.
- Perform regular audits of system logs.
- Perform active system monitoring to monitor the systems for any malicious incident.
- Implement secure VPNs to secure the organizational data during remote access.
- Employ file behavioral analysis systems such as next-generation firewalls (NGFWs) to observe traffic patterns and obtain timely analysis reports on SMB resources.
- Employ highly robust and secure monitoring systems such as global threat sensors for highly sensitive and top-secret data.
- Implement digitally signed data transmission and communication for accessing SMB resources.
- Block/disable TCP ports 88, 139, and 445 and UDP ports 88, 137, and 138 to prevent SMB attacks.
- Enable public profile settings in the firewall system.
- Block/disable the SMB protocol for Internet-facing servers.
- Ensure that SMB convention web confronting and DNS mainframes are disabled.
- Ensure that all systems are using SMBv3 or higher, which includes enhancements to security features, including encryption. Avoid using SMBv1, which is outdated and vulnerable.
- Configure ACLs to restrict access to SMB shares only to users who require it. Review and tighten permissions regularly.

- Use the least privilege principle to ensure users and services operate with the minimum necessary permissions, reducing the potential impact of compromised accounts.
- Configure SMB servers to log access attempts and changes to shared resources. Regularly review logs for suspicious activity.

DNS Enumeration Countermeasures

Discussed below are various measures to prevent DNS enumeration.

- **Restrict resolver access:** Ensure that the resolver can be accessed only by the hosts inside the network to prevent external cache poisoning.
- **Randomize source ports:** Ensure that the request packets exiting the network use random ports, rather than UDP port 53. In addition, randomize the query IDs and change the alphabet case of domain names to defend against cache poisoning.
- **Audit DNS zones:** Audit DNS zones to identify vulnerabilities in domains and subdomains and address DNS-related issues.
- **Patch known vulnerabilities:** Update and patch nameservers with the most recent versions of software such as BIND and Microsoft DNS.
- **Monitor nameservers:** Monitor the behavior of nameservers to identify malicious activities or unexpected behaviors at the earliest.
- **Restrict DNS zone transfers:** Restrict DNS zone transfers to specific slave nameserver IP addresses because the zone transfer may include a master copy of the primary server's database. Disable DNS zone transfers to untrusted hosts.
- **Use different servers for authoritative and resolving functions:** Separating the functions of the resolver and authoritative nameserver can reduce overload and prevent denial of service (DoS) attacks on domains.
- **Use isolated DNS servers:** Avoid hosting the application server along with the DNS server. Use an isolated and dedicated server for DNS services to minimize the risk of web application attacks.
- **Disable DNS recursion:** Disable DNS recursion in the DNS server configuration to recursively restrict queries from other or third-party domains and mitigate DNS amplification and poisoning attacks.
- **Harden the OS:** Harden the OS by closing unused ports and blocking unnecessary services.
- **Use VPN:** Use a VPN for secure communication. In addition, change default passwords.
- **Implement two-factor authentication:** Enforce two-factor authentication to provide secure access when a DNS server is managed by a third party.
- **Use DNS change lock:** Use DNS change lock or client lock to restrict the alteration of DNS settings without appropriate authorization.
- **Use DNSSEC:** Implement DNSSEC as an additional layer of security for the DNS server to allow only digitally signed DNS requests and mitigate DNS hijacking.

Technet24

- **Use premium DNS registration:** Use premium DNS registration services that hide sensitive information, such as host information (HINFO), from the public.
- **Secure DNS queries/encrypt DNS traffic:** Consider using DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT) to encrypt DNS queries and responses. This helps prevent eavesdropping and man-in-the-middle attacks that could facilitate DNS enumeration.
- **Enable DNS logging and monitoring:** Enable logging on DNS servers to record queries and responses. Regular monitoring and analysis of these logs can help identify suspicious patterns that may indicate enumeration attempts.
- **Employ anomaly detection:** Employ anomaly detection systems to automatically flag unusual DNS query volumes or patterns, which could signify enumeration or other DNS attacks.
- **Implement rate limiting:** Configure DNS servers to limit the rate of accepted queries from individual IP addresses. This can mitigate the effectiveness of brute-force enumeration techniques.
- **Split DNS architecture:** Implement a split DNS architecture, where internal DNS queries are handled by a separate DNS server from those coming from external sources. This limits the exposure of internal network structure to the outside world.
- **Use minimal DNS information:** Be cautious about the amount of information shared through DNS records. For instance, avoid using descriptive subdomain names that reveal internal network details or server purposes.

Other countermeasures to defend against DNS enumeration are as follows:

- Ensure that private hosts and their IP addresses are not published in the DNS zone files of the public DNS server.
- Use standard network admin contacts for DNS registrations to avoid social engineering attacks.
- Prune DNS zone files to avoid revealing unnecessary information.
- Maintain independent internal and external DNS servers.
- Ensure that old or unused DNS records are deleted periodically.
- Restrict **version.bind** request queries using ACLs. Remove or run **BIND** with the least privileges.
- Use **/etc/hosts** file for the development or staging of subdomains instead of using DNS records.
- Deploy DNS Firewalls to block malicious queries and protect against DNS-based threats by using threat intelligence to identify and prevent communication with known malicious domains.
- Periodically review and audit DNS configurations to ensure that they are secure and that only necessary DNS information is exposed to the public.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40 Module 04 | Enumeration

EC-Council C|EH

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

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org

Module Summary

In this module, we discussed the enumeration concepts along with the techniques, services, and ports used for enumeration. We have also discussed how attackers perform different enumeration techniques (NetBIOS, SNMP, LDAP, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Linux/Unix, and SMB enumeration) to gather information about the target. This module ended with a detailed discussion on the countermeasures that organizations can adopt to 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.

Technet24