C|EH Certified Ethical Hacker

EC-Council

MODULE 04

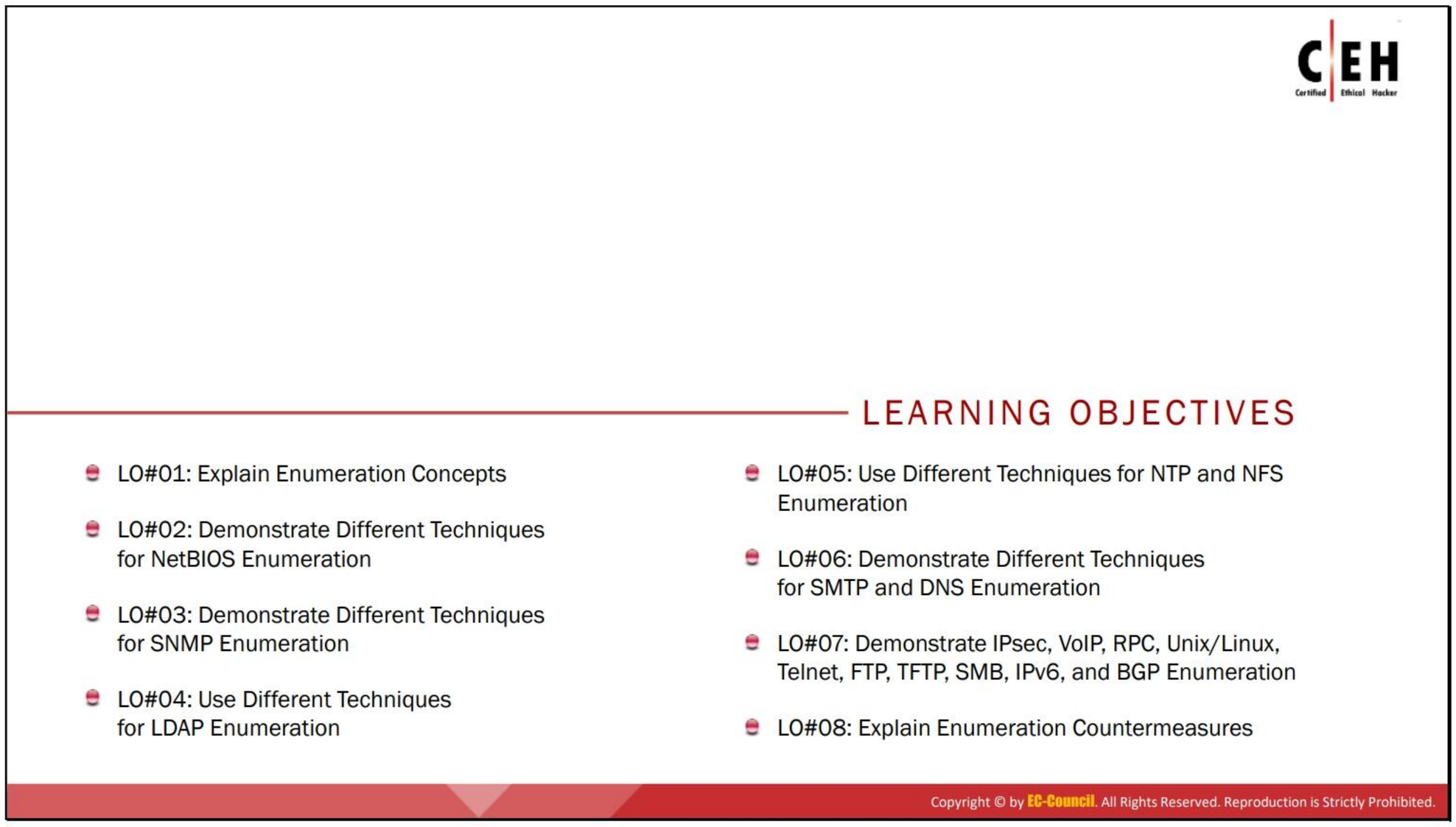
ENUMERATION

EC-COUNCIL OFFICIAL CURRICULA

https://t.me/learningnets

This page is intentionally left blank.

https://t.me/learningnets



Learning Objectives

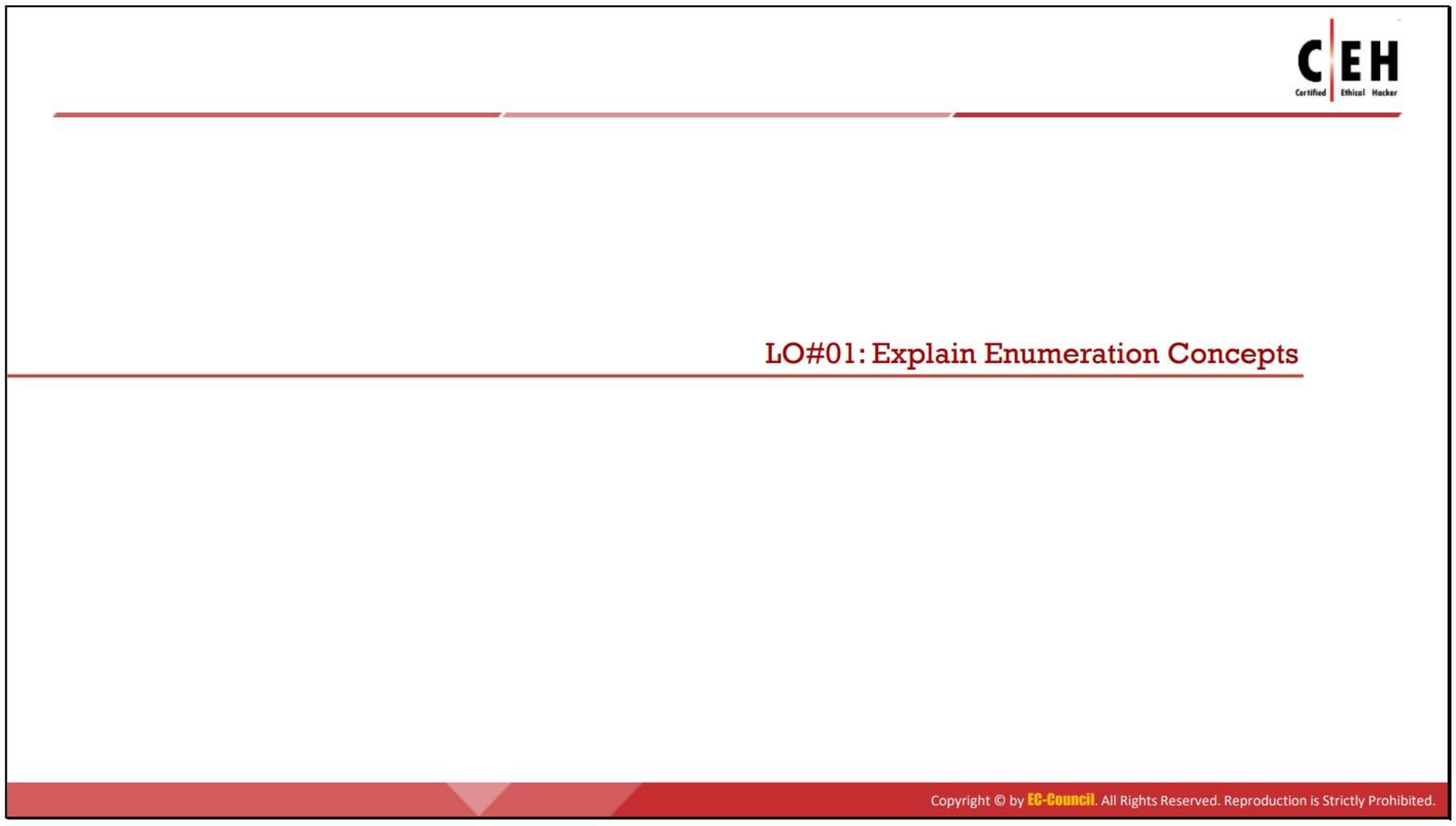
In the previous modules, you learned about footprinting and network scanning. This module covers the next phase, enumeration. We start with an introduction to enumeration concepts. Subsequently, the module provides insight into different techniques for Network Basic Input/Output System (NetBIOS), Simple 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, Telnet, File Transfer Protocol (FTP), Trivial FTP (TFTP), Server Message Block (SMB), Internet Protocol version 6 (IPv6), and Border Gateway Protocol (BGP) 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, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration
- Apply enumeration countermeasures

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

https://t.me/learningnets

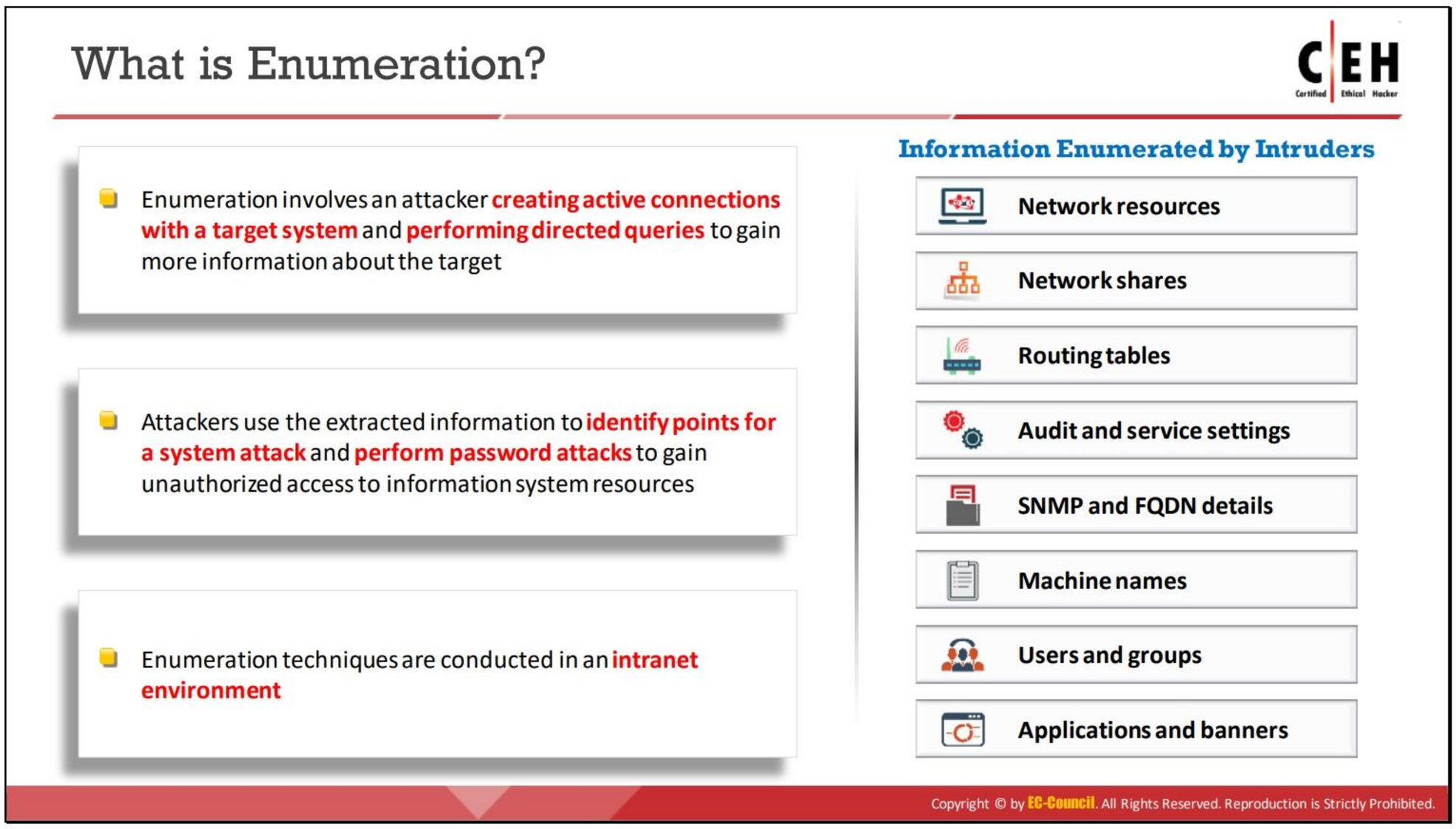


Enumeration Concepts

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.

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

https://t.me/learningnets



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.

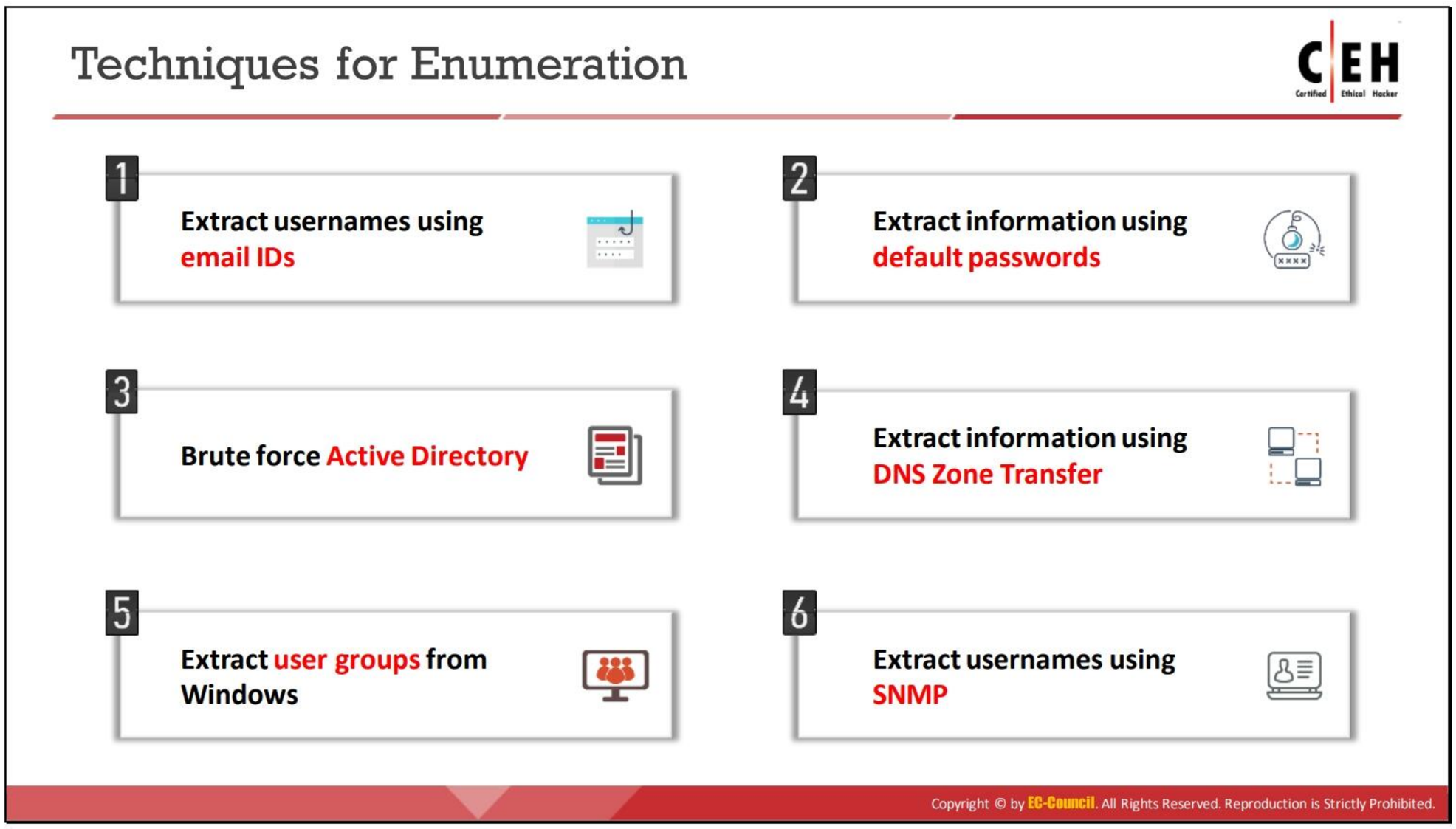
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

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.

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

https://t.me/learningnets



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

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

https://t.me/learningnets

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**

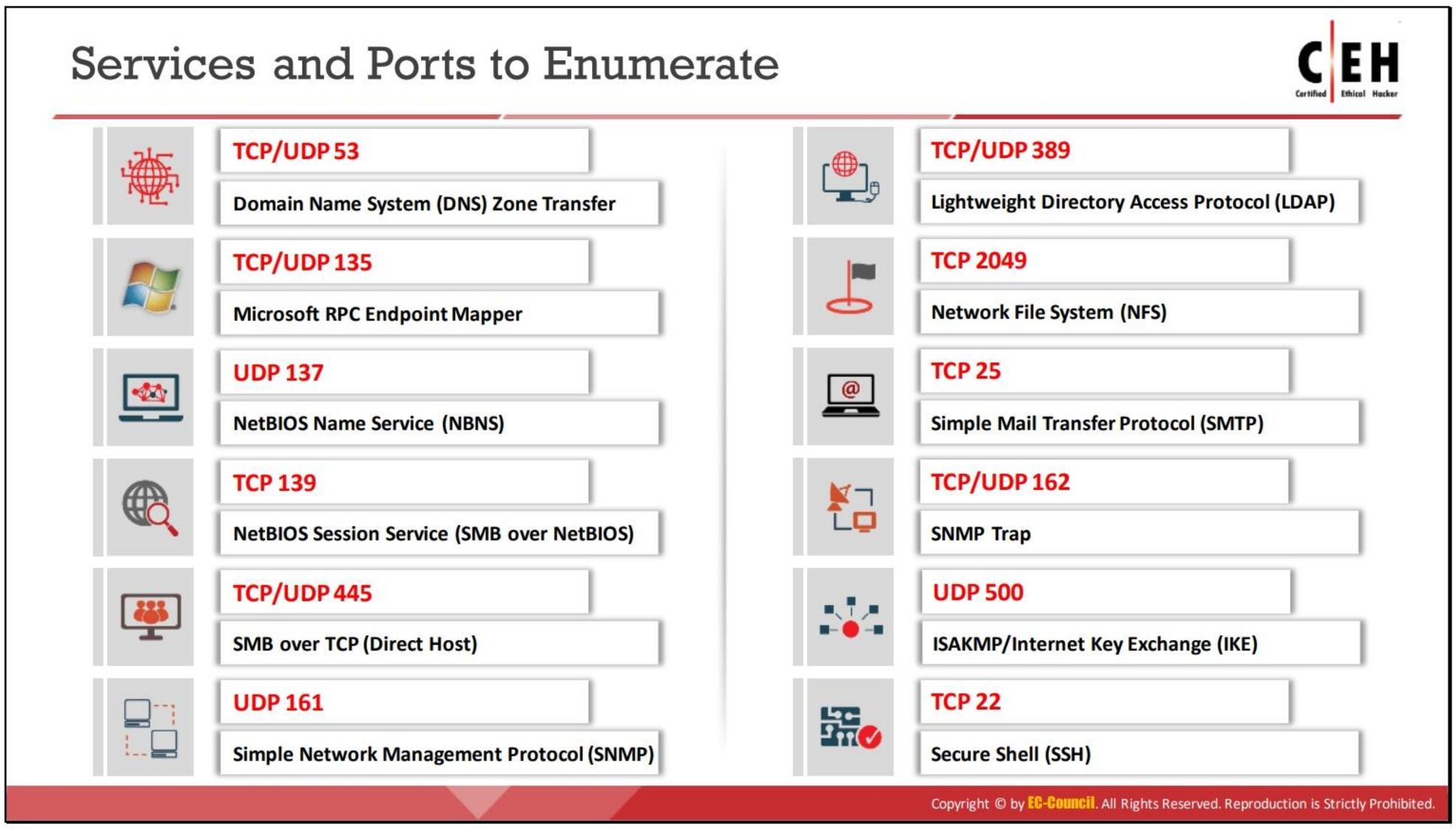
  To extract user groups from Windows, the attacker should have a registered ID as a user in the Active Directory. The attacker can then extract information from groups in which the user is a member by using the Windows interface or command-line method.

- **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.

https://t.me/learningnets



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

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

https://t.me/learningnets

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 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

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

https://t.me/learningnets

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.

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

https://t.me/learningnets

- **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 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.

- **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.

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

https://t.me/learningnets

- **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.

https://t.me/learningnets

LO#02: Demonstrate Different Techniques for NetBIOS Enumeration

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

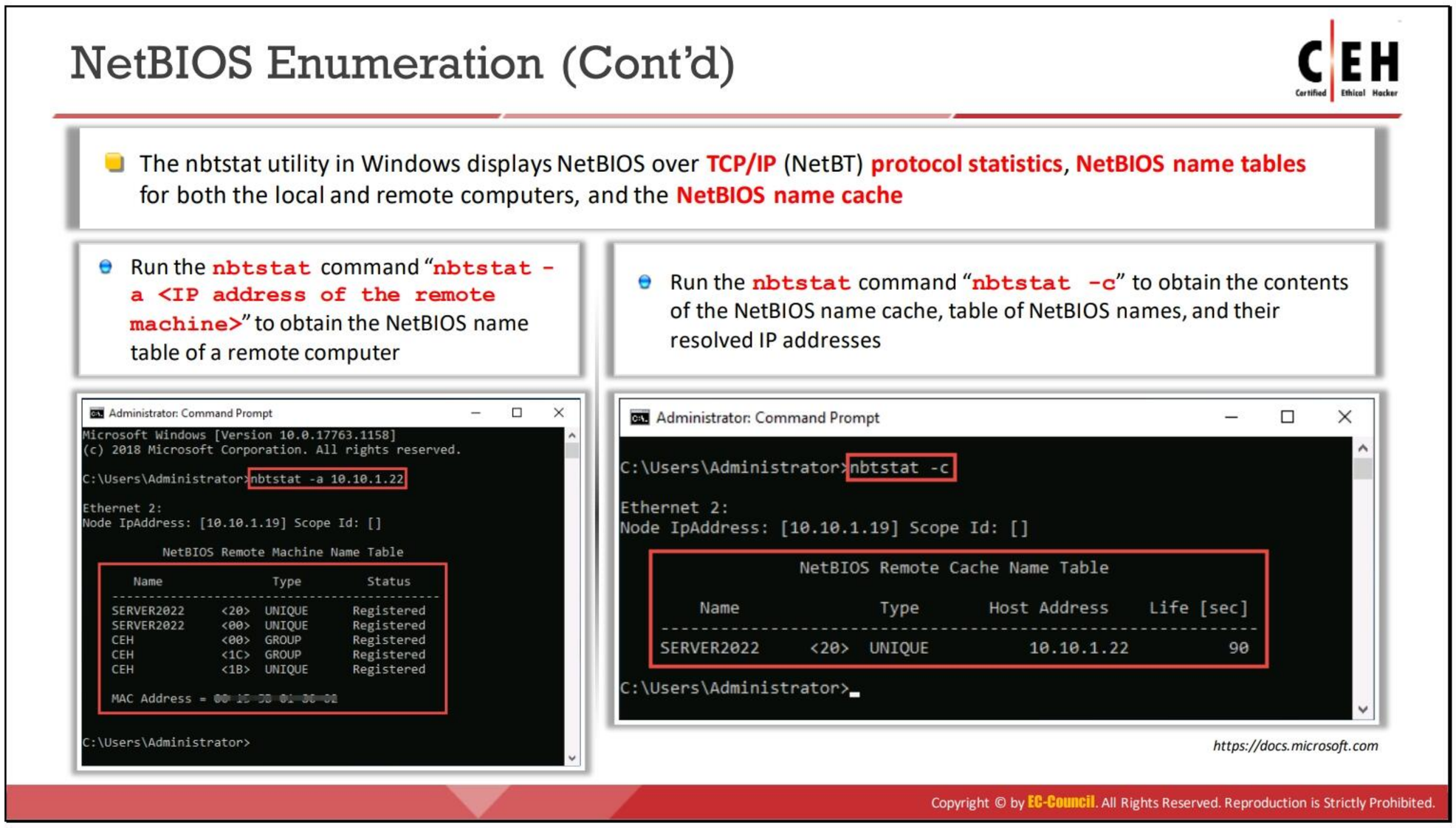
Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for the computer
<username>	<03>	UNIQUE	Messenger service running for the logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<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 © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

https://t.me/learningnets



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.

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

https://t.me/learningnets

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://docs.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 IP Address] [-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 IP Address`	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

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

https://t.me/learningnets

-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

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.

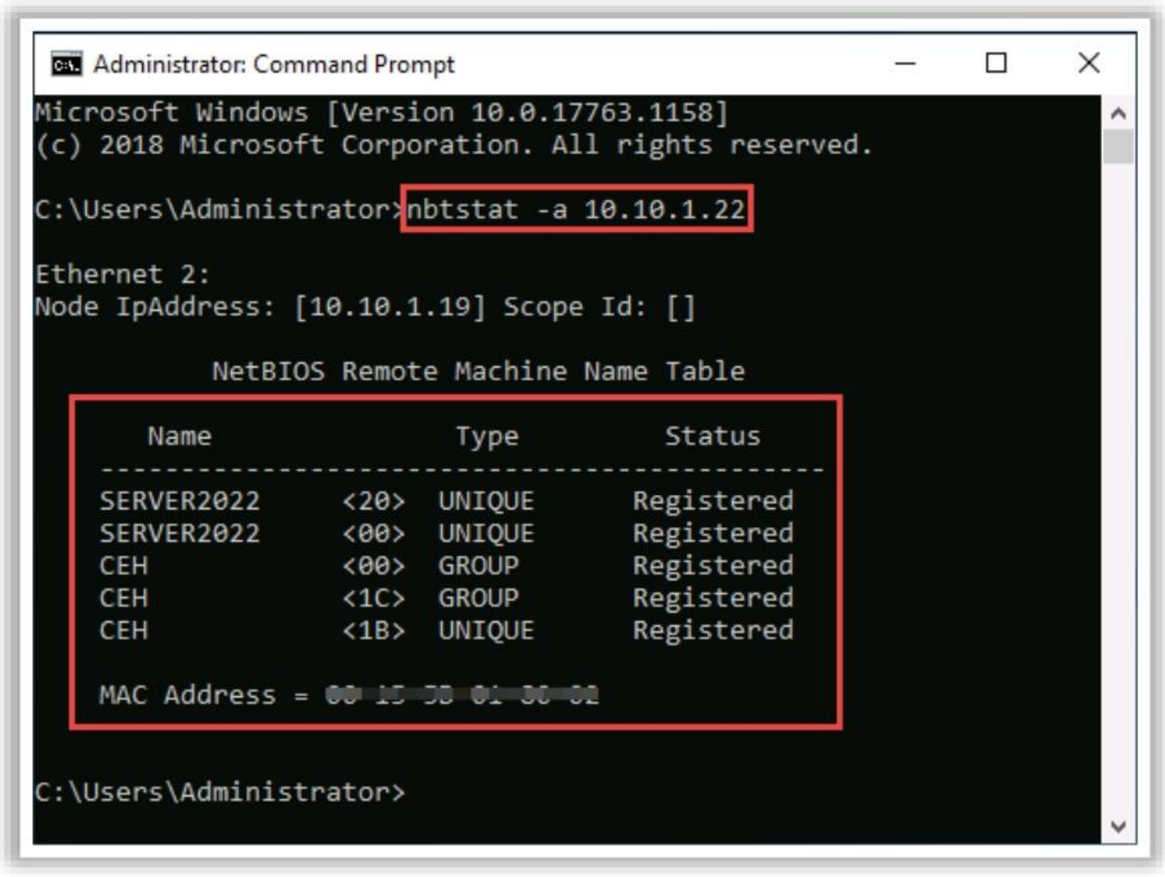


Figure 4.1: Nbtstat command to obtain the name table of a remote system

- 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.

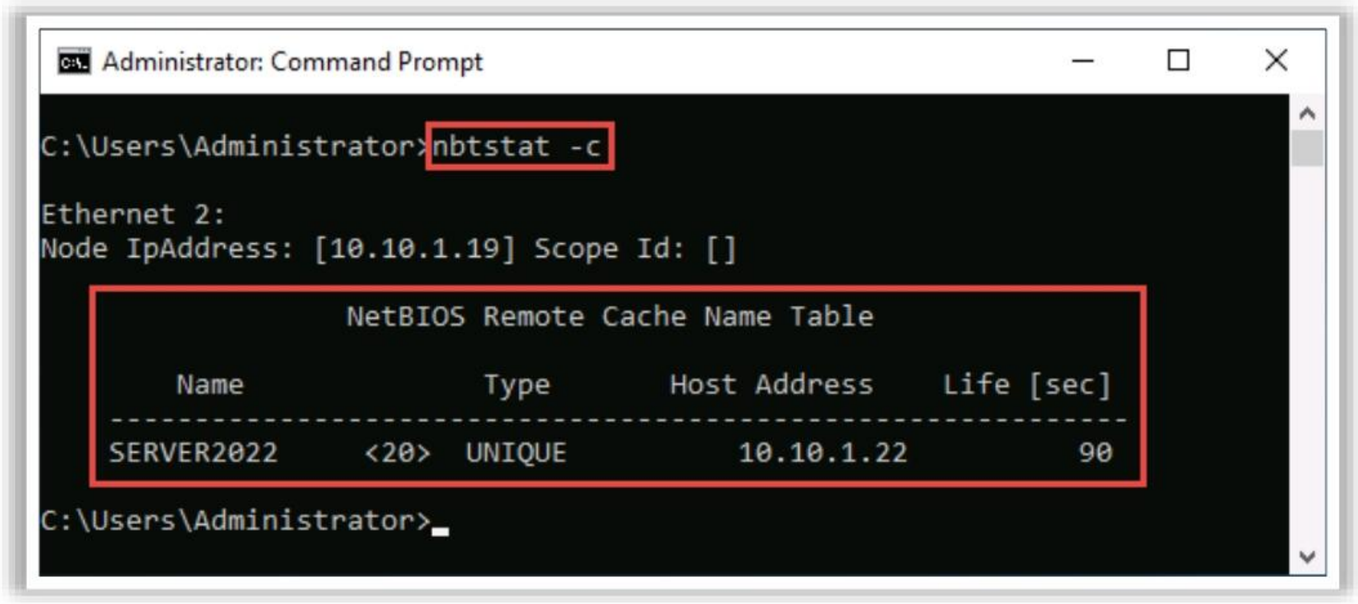
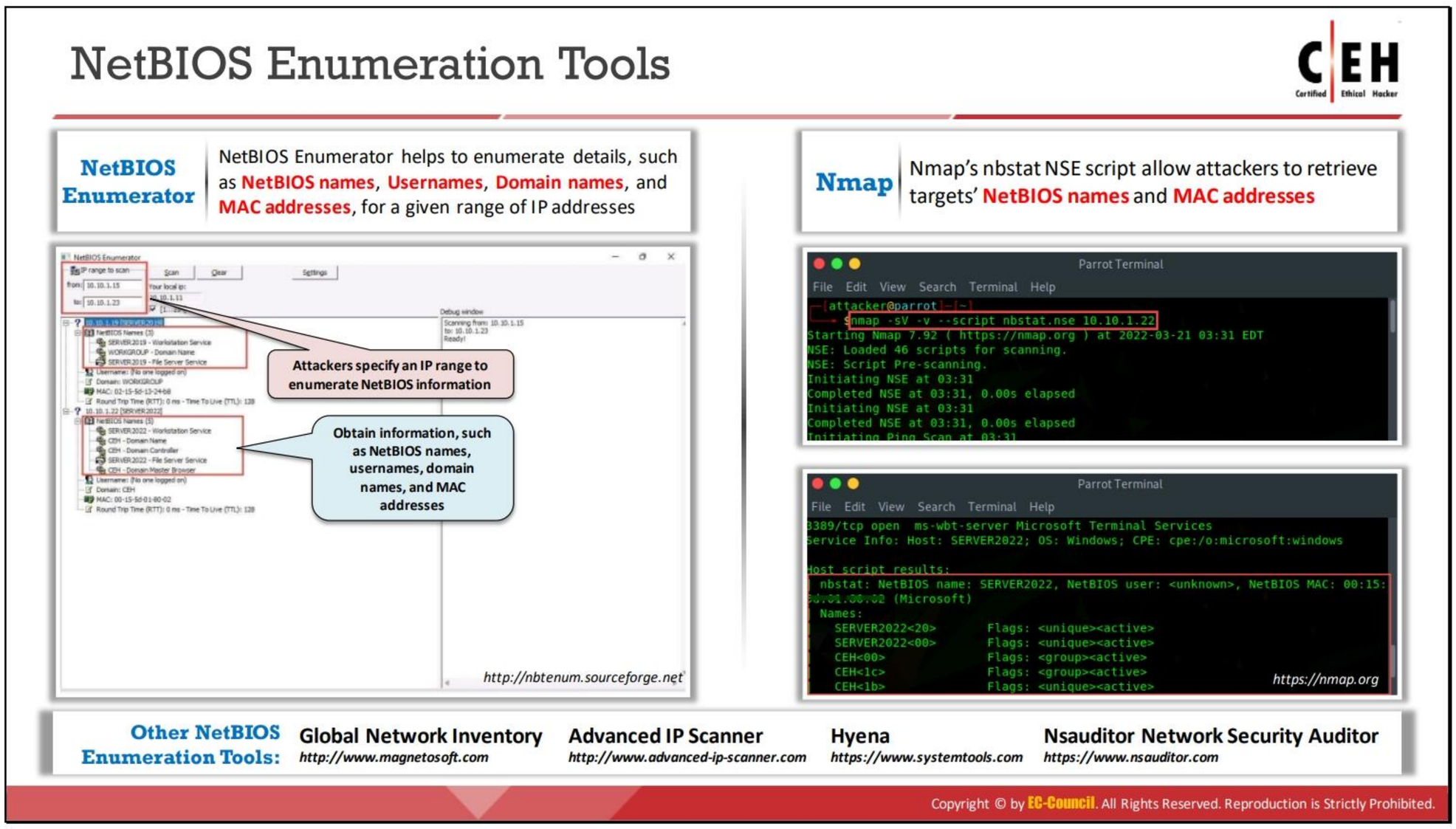


Figure 4.2: Nbtstat command to obtain the contents of the NetBIOS name table

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

https://t.me/learningnets



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: *http://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.

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

https://t.me/learningnets

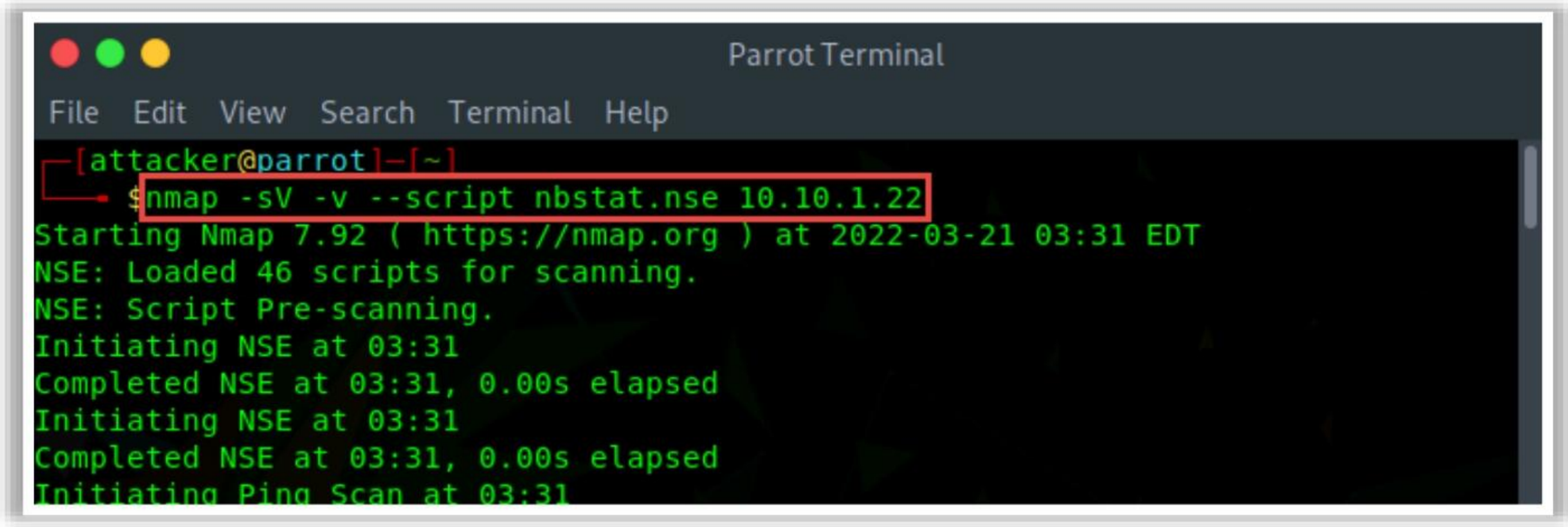


Figure 4.4: Screenshot of Nmap command for NetBIOS enumeration

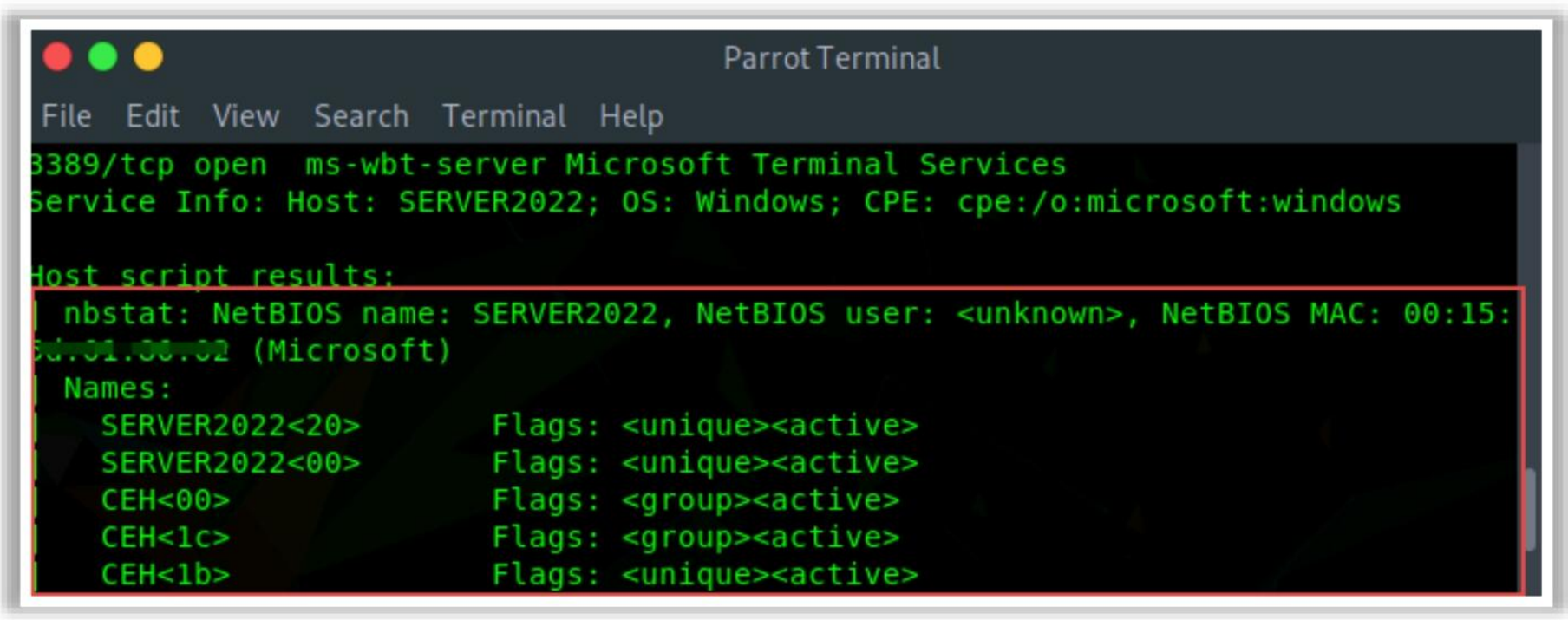


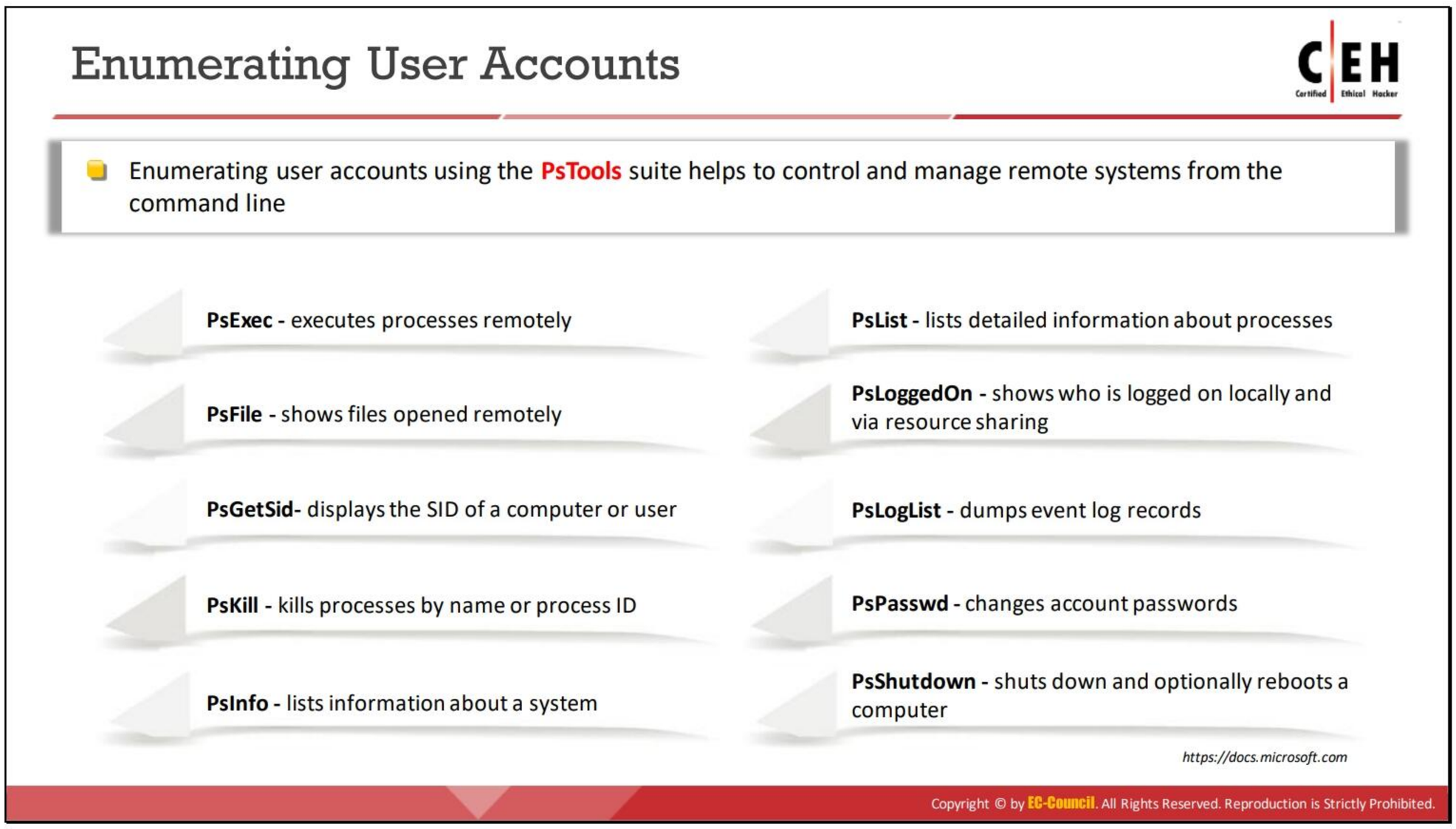
Figure 4.5: Screenshot of Nmap NetBIOS enumeration output

The following are some additional NetBIOS enumeration tools:

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

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

https://t.me/learningnets



Enumerating User Accounts

Source: *https://docs.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.

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

https://t.me/learningnets

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 or user SID, PsLoggedOn looks up the corresponding username and displays it. To

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

https://t.me/learningnets

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]
```

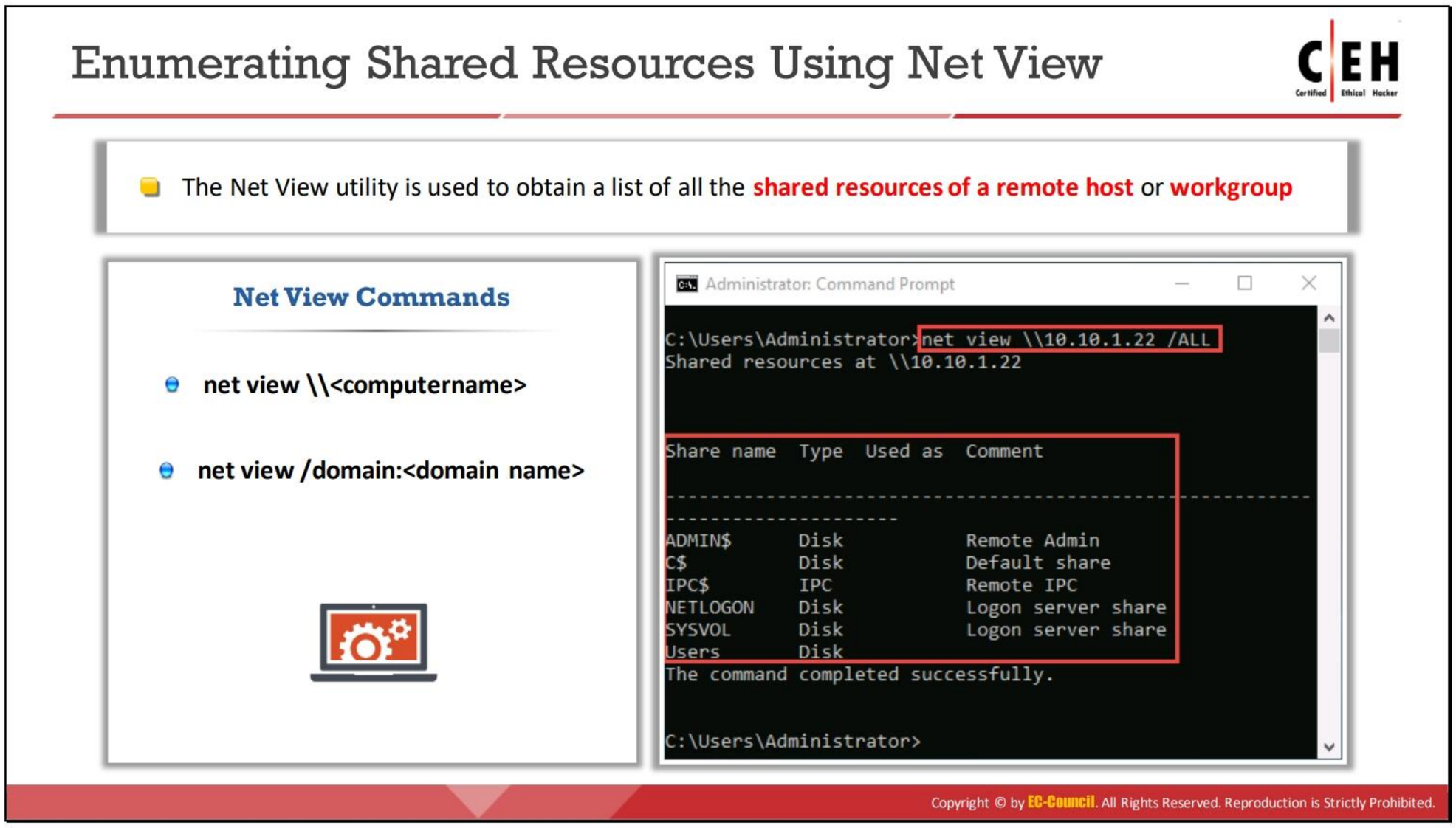
- **PsShutdown**

  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"]
```


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

https://t.me/learningnets



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.

https://t.me/learningnets

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

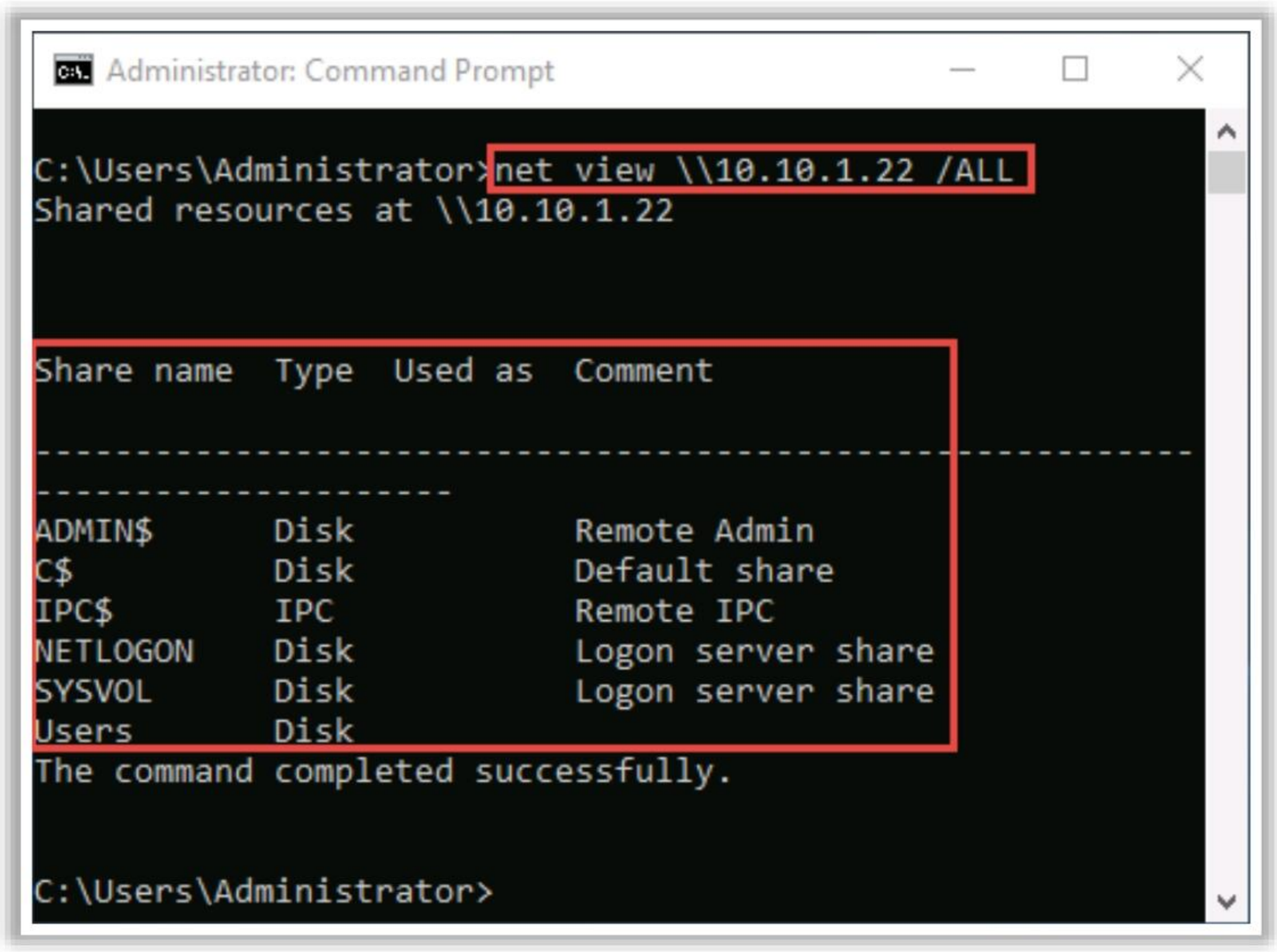


Figure 4.6: Output of Net View command

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

https://t.me/learningnets

LO#03: Demonstrate Different Techniques for SNMP Enumeration

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SNMP (Simple Network Management Protocol) Enumeration

- SNMP enumeration is the process of **enumerating user accounts and devices** on a target system using SNMP
- SNMP consists of a **manager** and an **agent**; agents are embedded on every network device, and the manager is installed on a separate computer

- SNMP holds **two passwords** to access and configure the SNMP agent from the management station
  - **Read community string**: It is public by default; it allows for the viewing of the device/system configuration
  - **Read/write community string**: It is private by default; it allows remote editing of configuration

- Attackers use these **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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

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

https://t.me/learningnets

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 following are some commands associated with SNMP.

- **GetRequest**: Used by the SNMP manager to request information from an SNMP agent
- **GetNextRequest**: Used by the SNMP manager continuously to retrieve all the data stored in an array or table

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

https://t.me/learningnets

- **GetResponse**: Used by an SNMP agent to satisfy a request made by the SNMP manager
- **SetRequest**: Used by the SNMP manager to modify the value of a parameter within an SNMP agent's management information base (MIB)
- **Trap**: Used by an SNMP agent to inform the pre-configured SNMP manager of a certain event

The communication process between an SNMP manager and SNMP agent is as follows.

- The SNMP manager (Host X, 10.10.2.1) uses the GetRequest command to send a request for the number of active sessions to the SNMP agent (Host Y, 10.10.2.15). To perform this step, the SNMP manager uses an SNMP service library such as the Microsoft SNMP Management API library (Mgmtapi.dll) or Microsoft WinSNMP API library (Wsnmp32.dll).
- The SNMP agent (Host Y) receives the message and verifies if the community string (Compinfo) is present on its MIB, checks the request against its list of access permissions for that community, and verifies the source IP address.
- If the SNMP agent does not find the community string or access permission in Host Y's MIB database and the SNMP service is set to send an authentication trap, it sends an authentication failure trap to the specified trap destination, Host Z.
- The master agent component of the SNMP agent calls the appropriate extension agent to retrieve the requested session information from the MIB.
- Using the session information retrieved from the extension agent, the SNMP service forms a return SNMP message that contains the number of active sessions and the destination IP address (10.10.2.1) of the SNMP manager, Host X.
- Host Y sends the response to Host X.

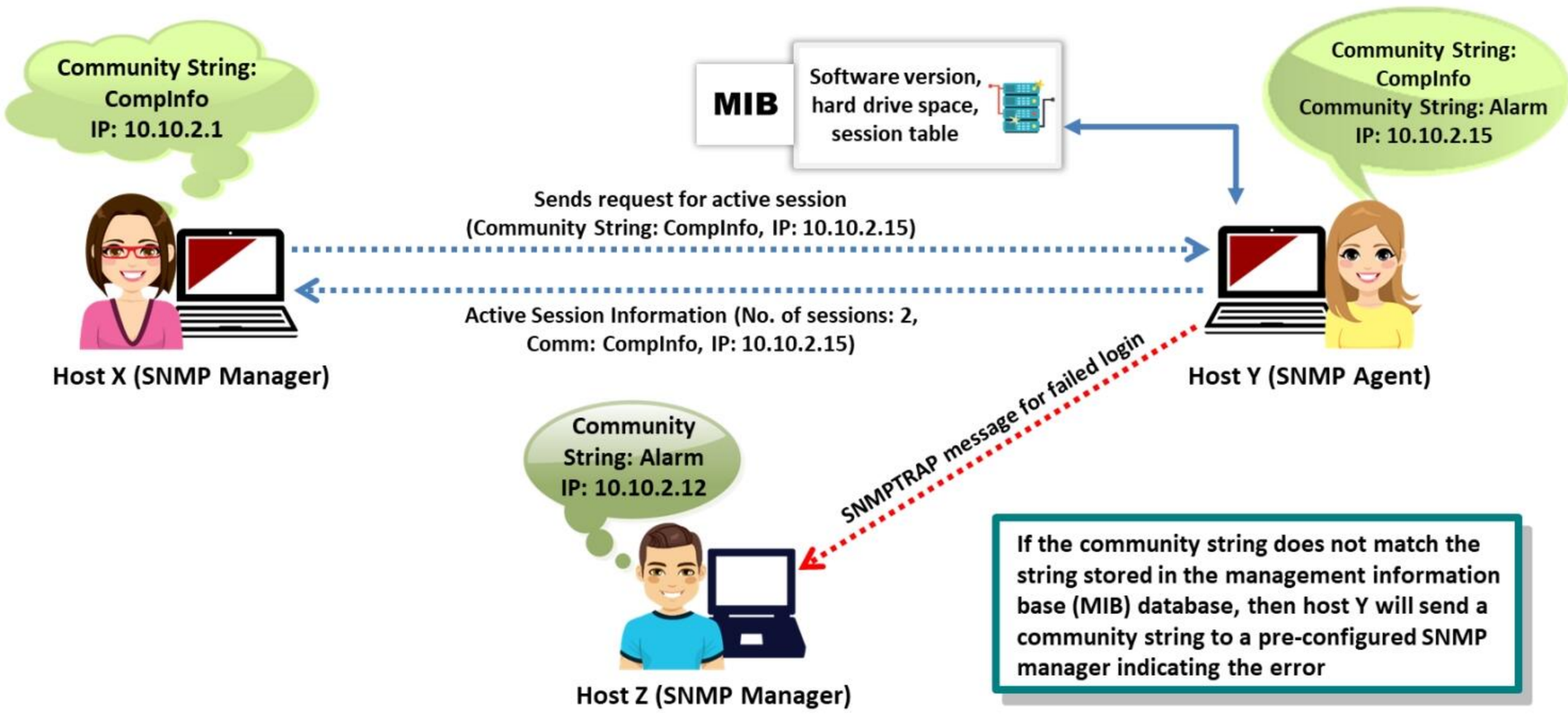


Figure 4.7: Illustration of the working of SNMP

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

https://t.me/learningnets

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.

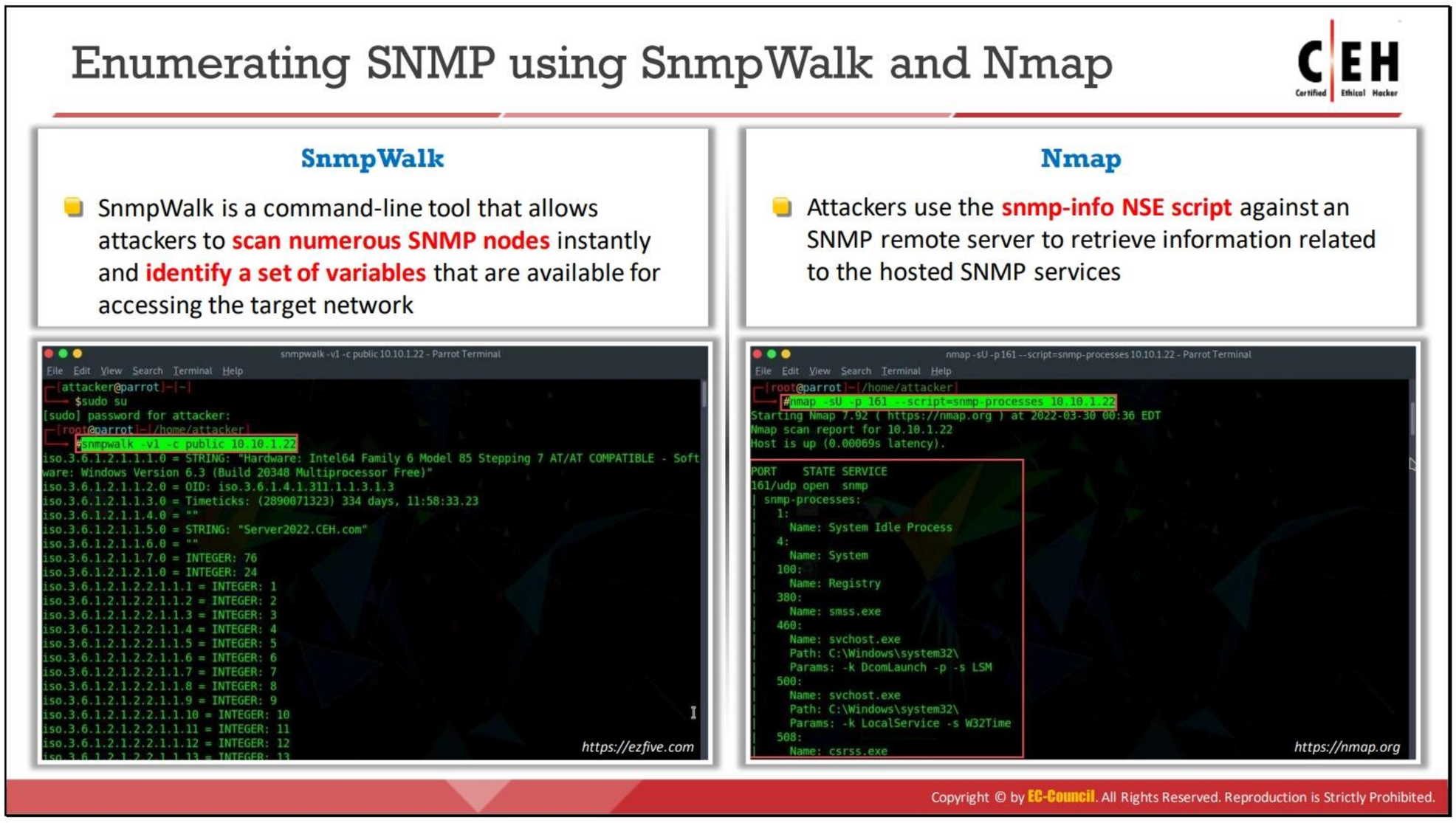
MIB-managed objects include scalar objects, which define a single object instance, and tabular objects, which define a group of related object instances. OIDs include the object's type (such as counter, string, or address), access level (such as read or read/write), size restrictions, and range information.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

https://t.me/learningnets



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.

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

https://t.me/learningnets

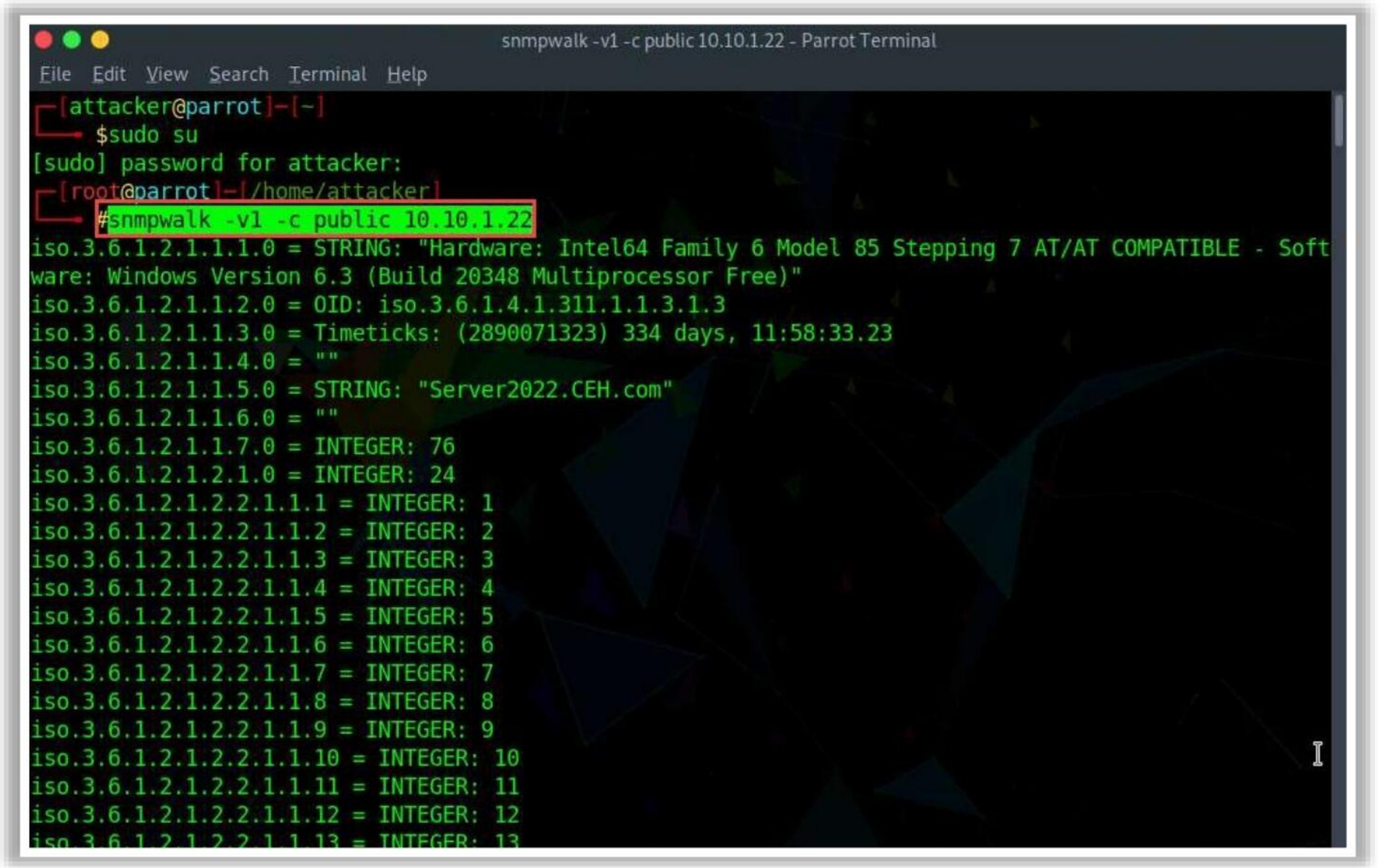


Figure 4.8: Screenshot of SnmpWalk

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`

- 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>`

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

https://t.me/learningnets

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.

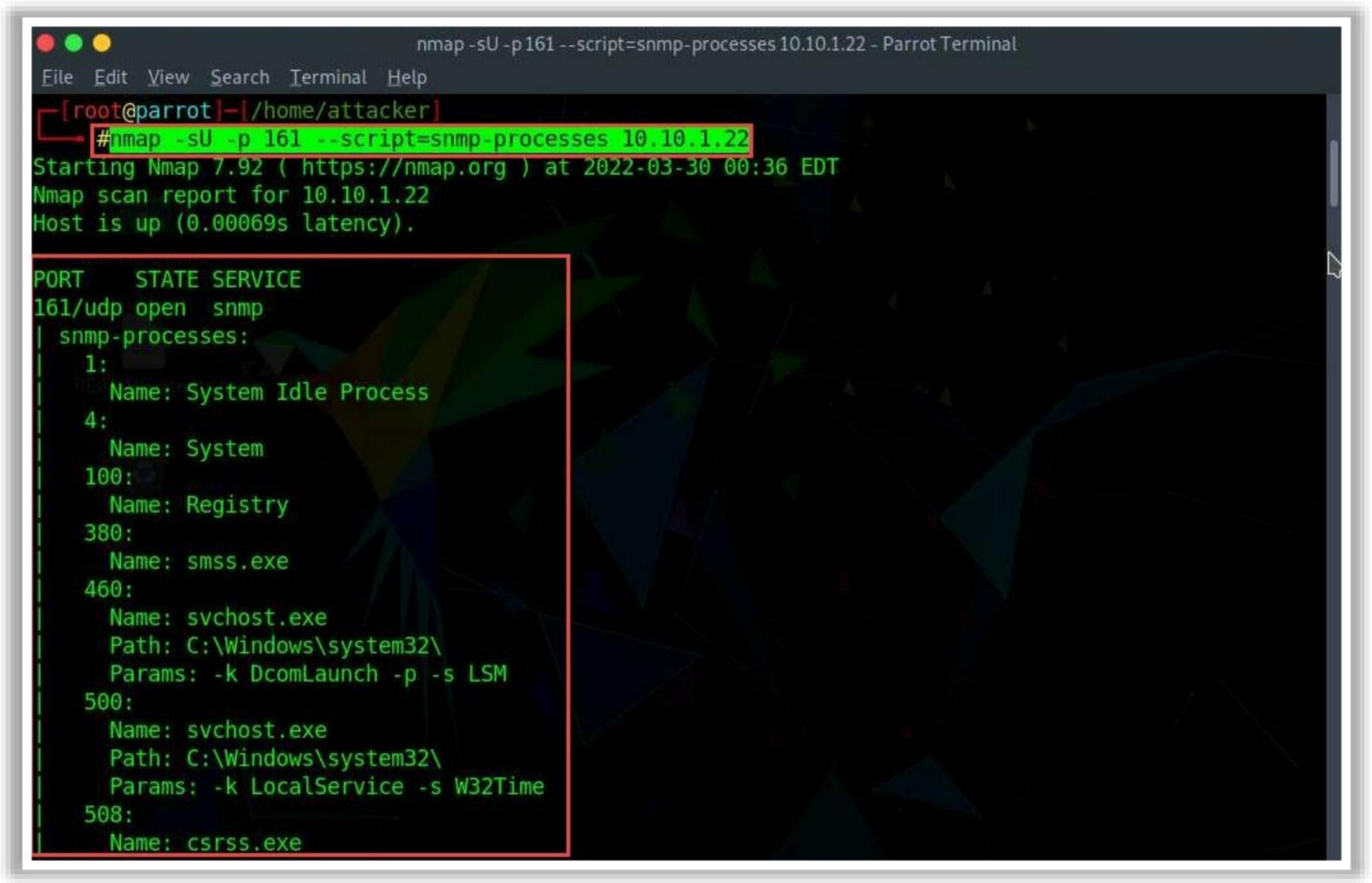
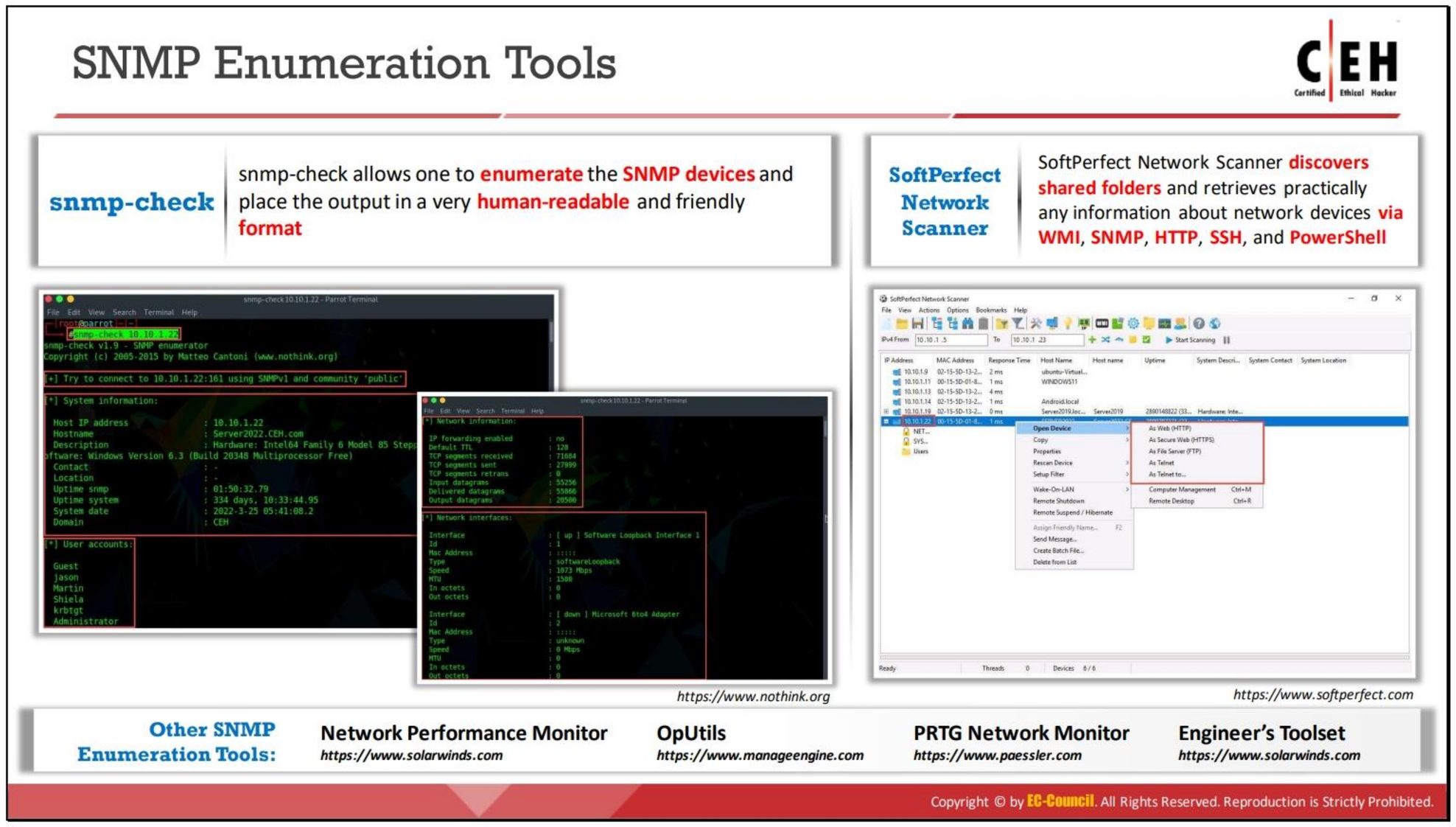


Figure 4.9: Screenshot of Nmap using the snmp-processes NSE script

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

https://t.me/learningnets



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.

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

https://t.me/learningnets

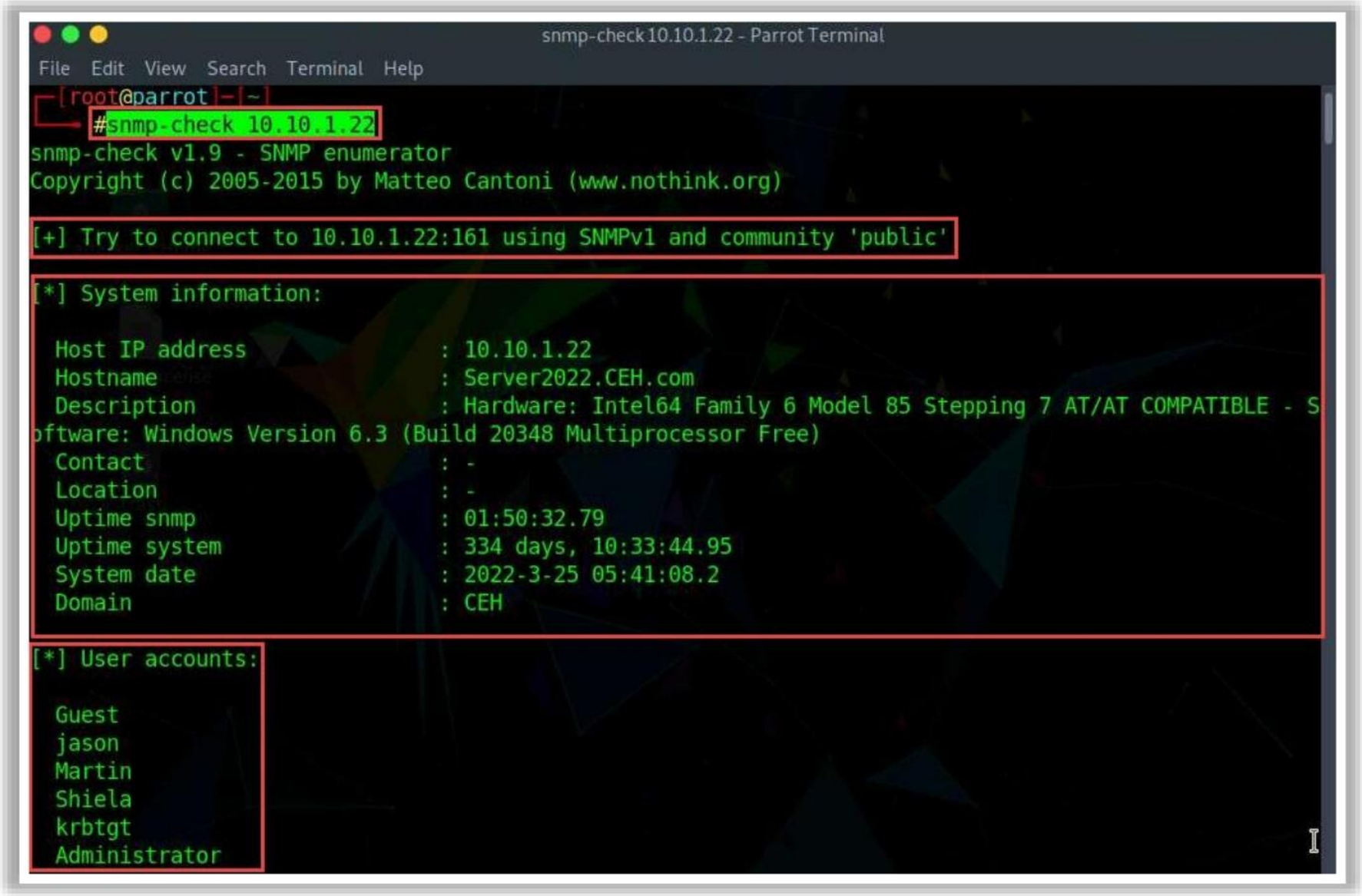


Figure 4.10: Screenshot of snmp-check showing system information and user accounts

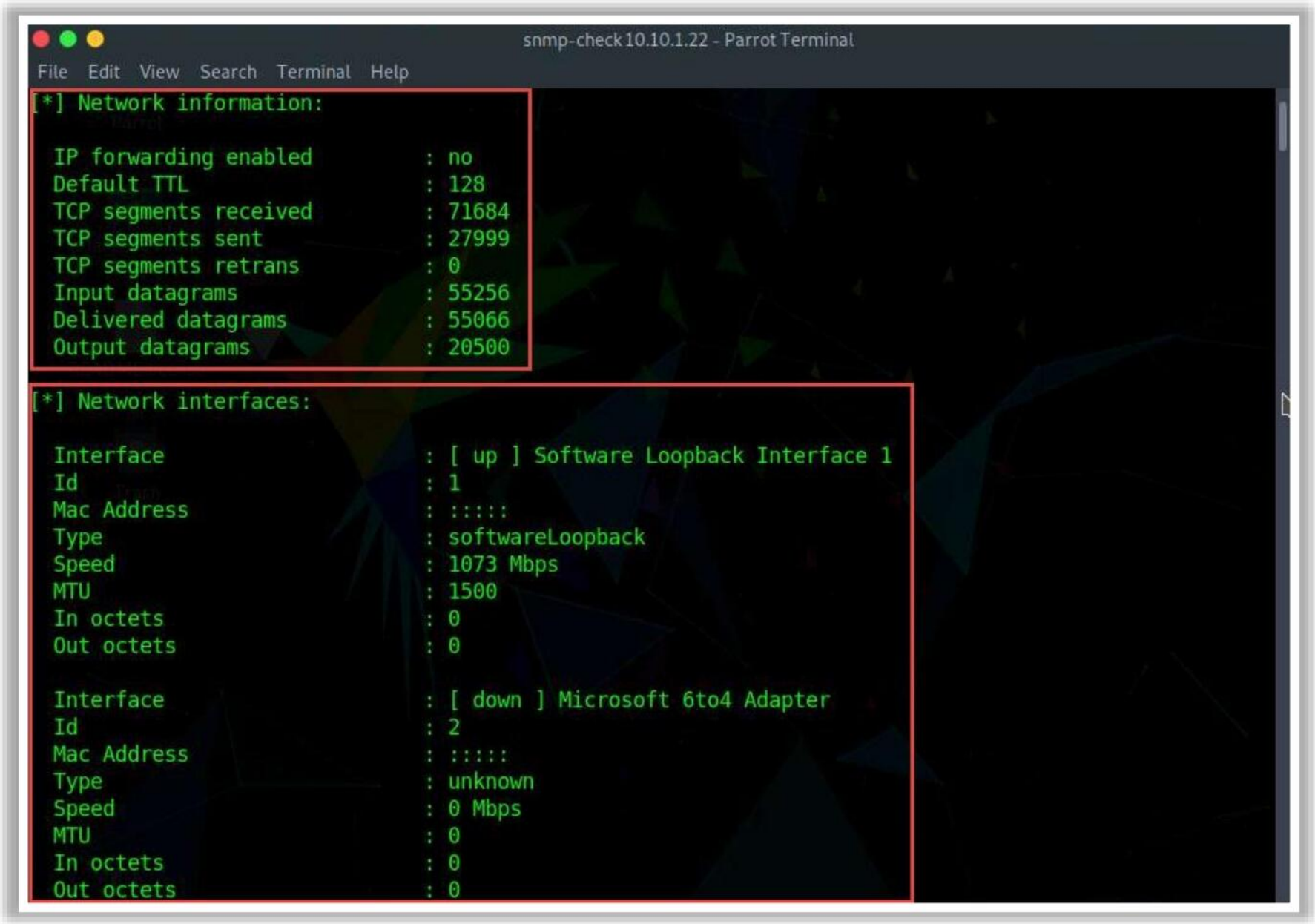


Figure 4.11: Screenshot of snmp-check showing network information and interfaces

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

https://t.me/learningnets

- **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.

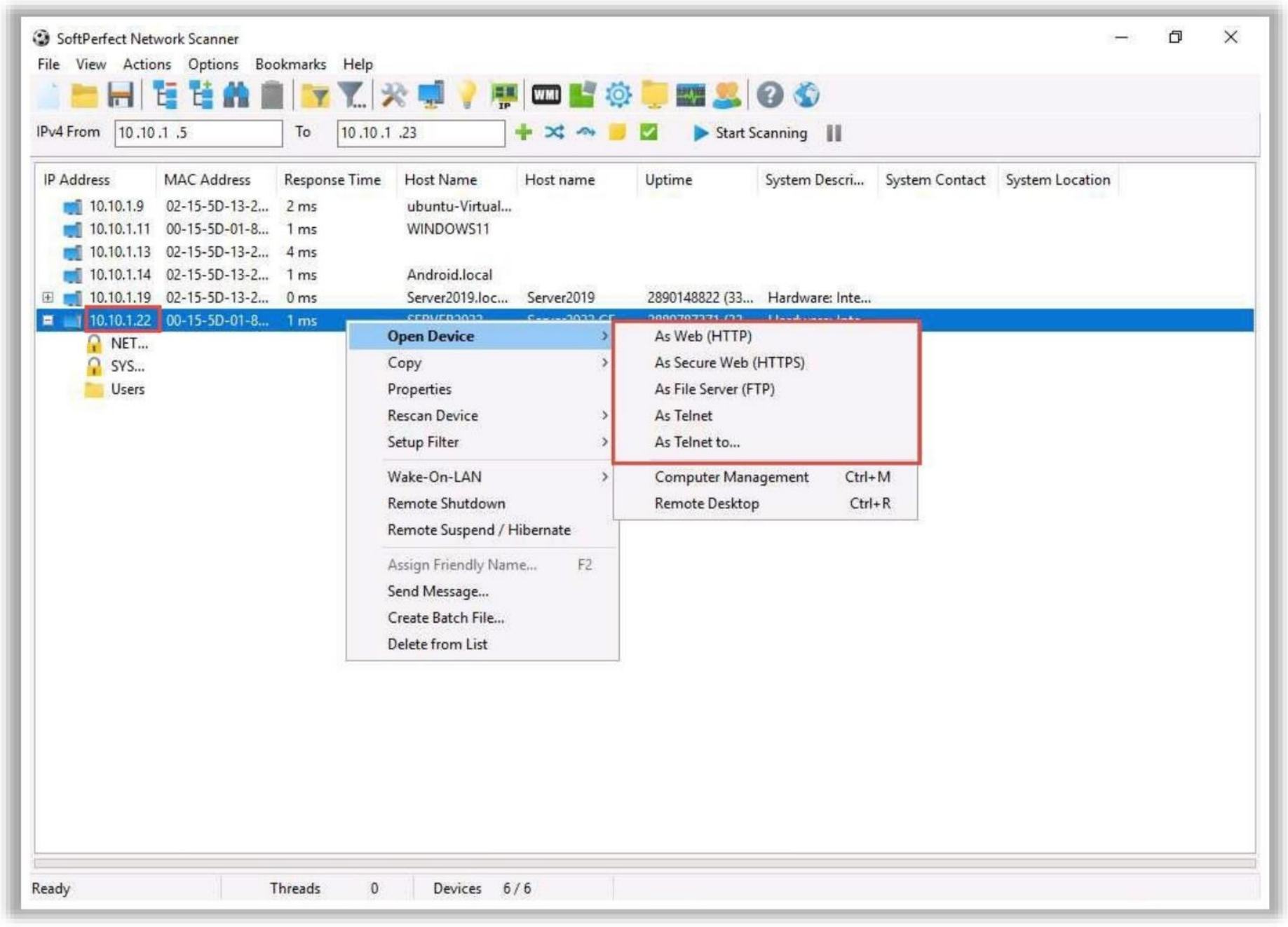


Figure 4.12: Screenshot of SoftPerfect Network Scanner

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*)

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

https://t.me/learningnets

LO#04: Use Different Techniques for LDAP Enumeration

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

LDAP Enumeration

1. Lightweight directory access protocol (LDAP) is an **Internet protocol** for accessing distributed directory services
2. Directory services may provide any organized set of records, often in a **hierarchical** and **logical structure**, such as a corporate email directory
3. 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
4. Information is transmitted between the client and server using **basic encoding rules** (BER)
5. Attackers query the LDAP service to gather information, such as **valid usernames**, **addresses**, and **departmental details**, which can be further used to perform attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

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

https://t.me/learningnets

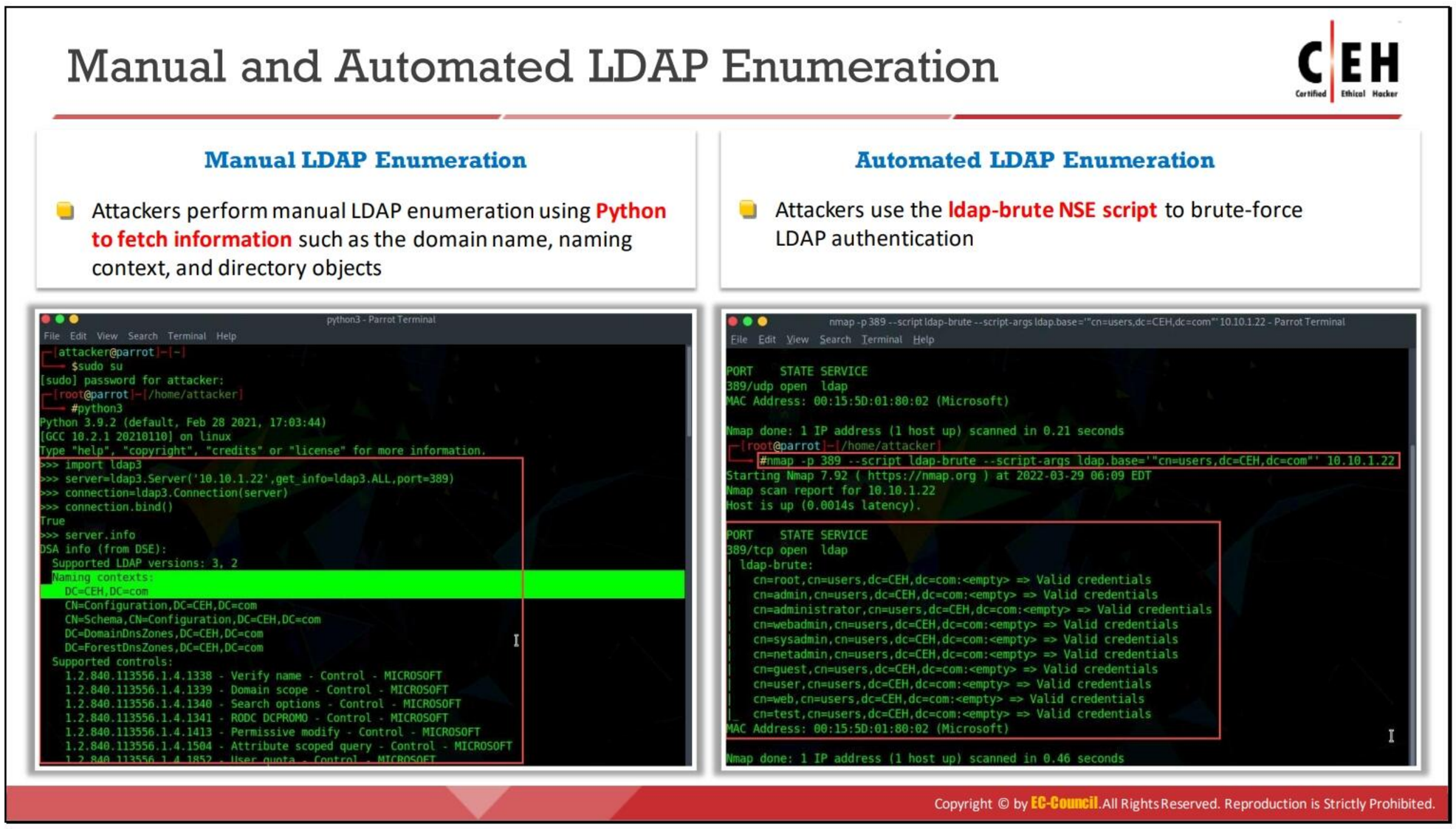
LDAP enumeration, the information extracted via LDAP enumeration, and LDAP enumeration tools.

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.

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

https://t.me/learningnets



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()`**.

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

https://t.me/learningnets

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
```

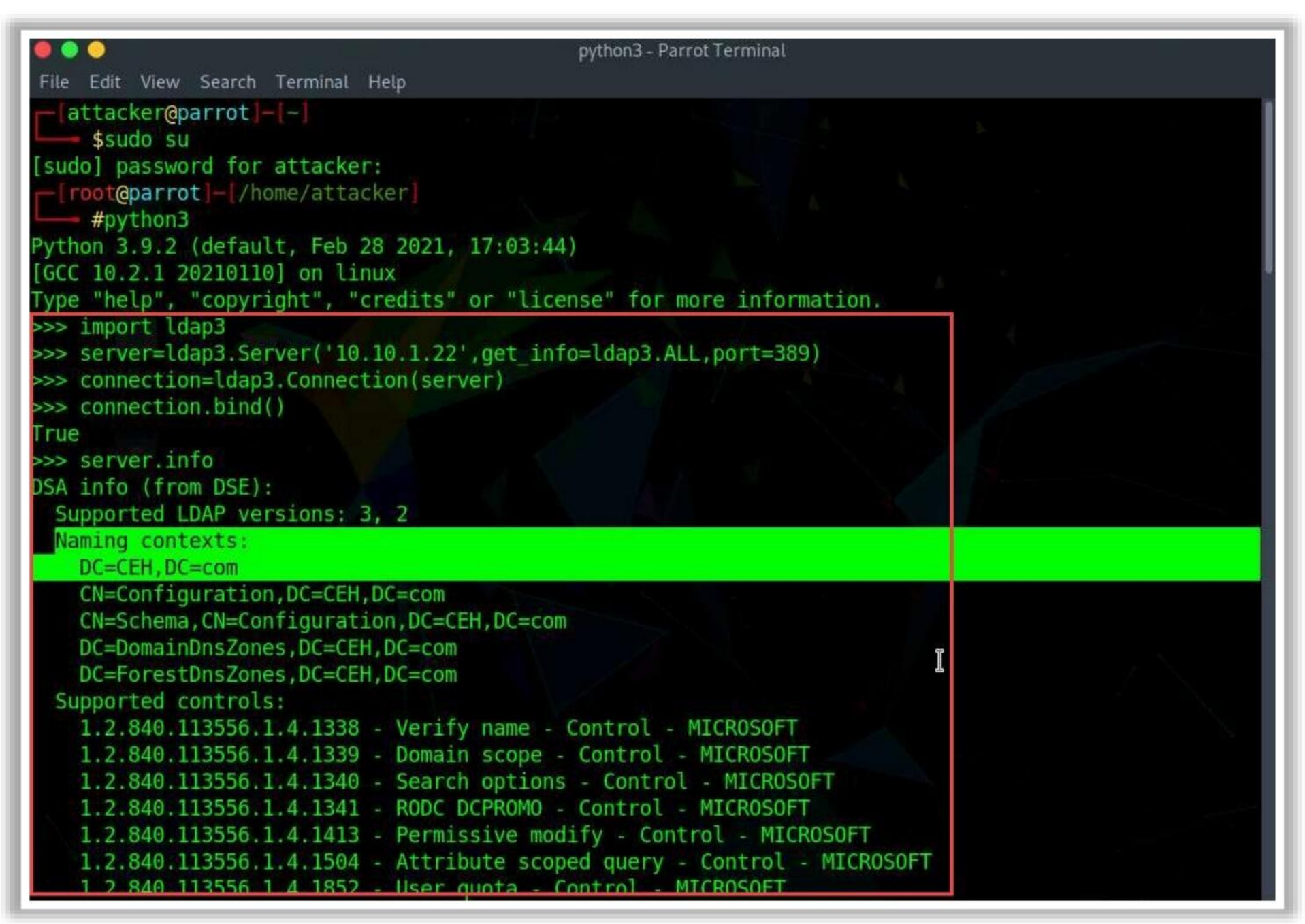


Figure 4.13: Screenshot showing LDAP enumeration using Python script

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

https://t.me/learningnets

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
```

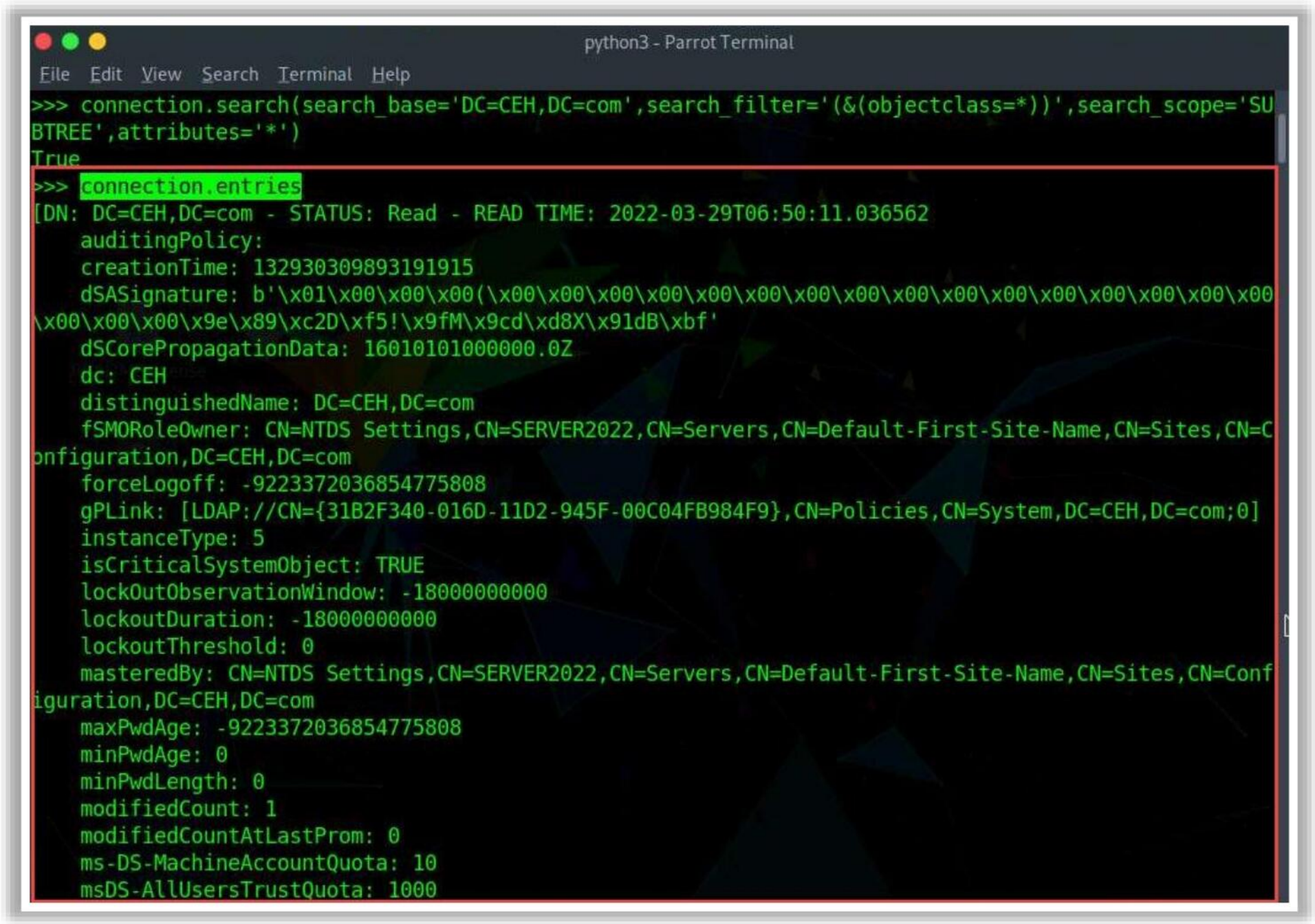


Figure 4.14: Screenshot showing output of LDAP enumeration

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
```


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

https://t.me/learningnets

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>
```

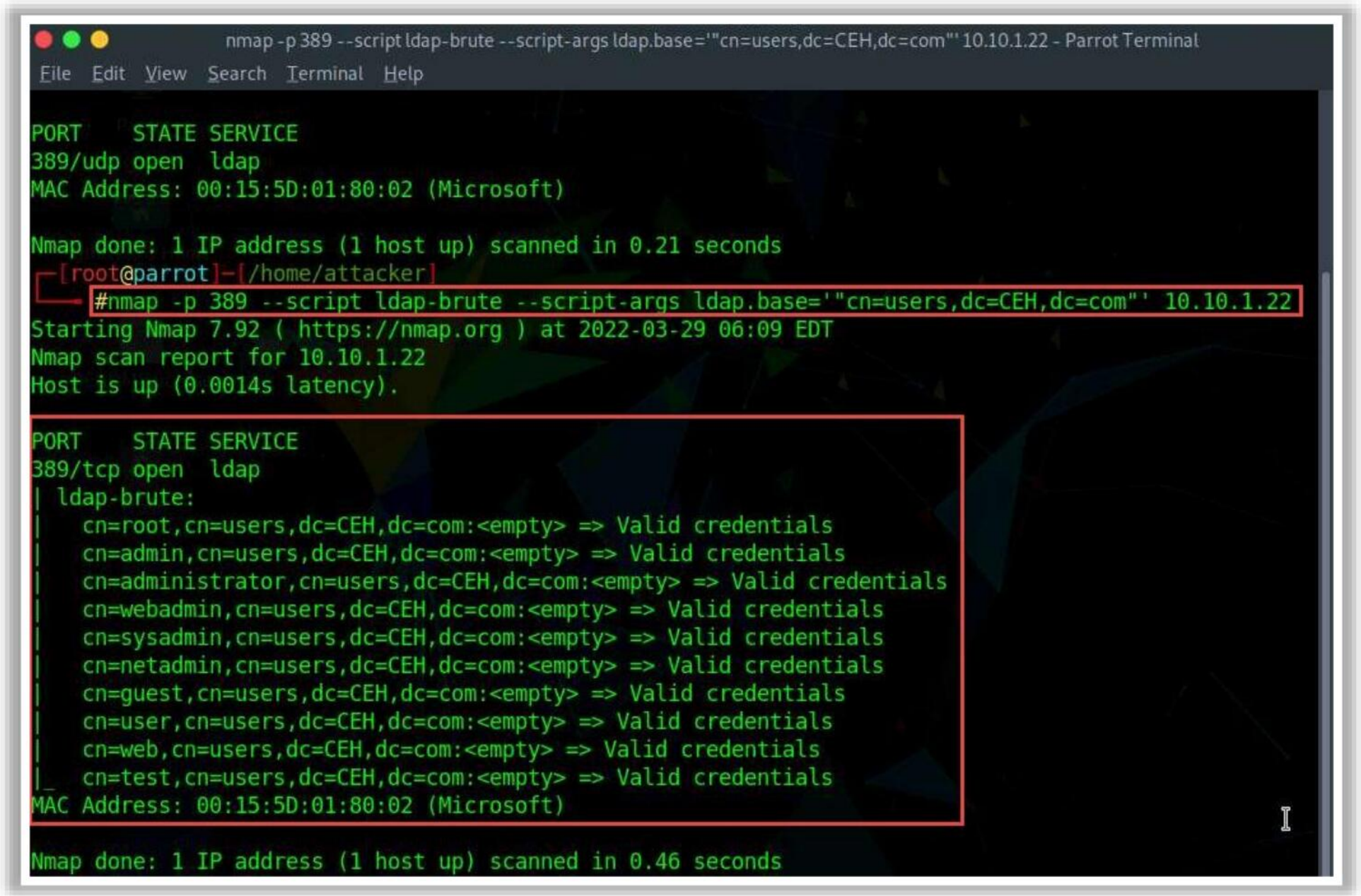
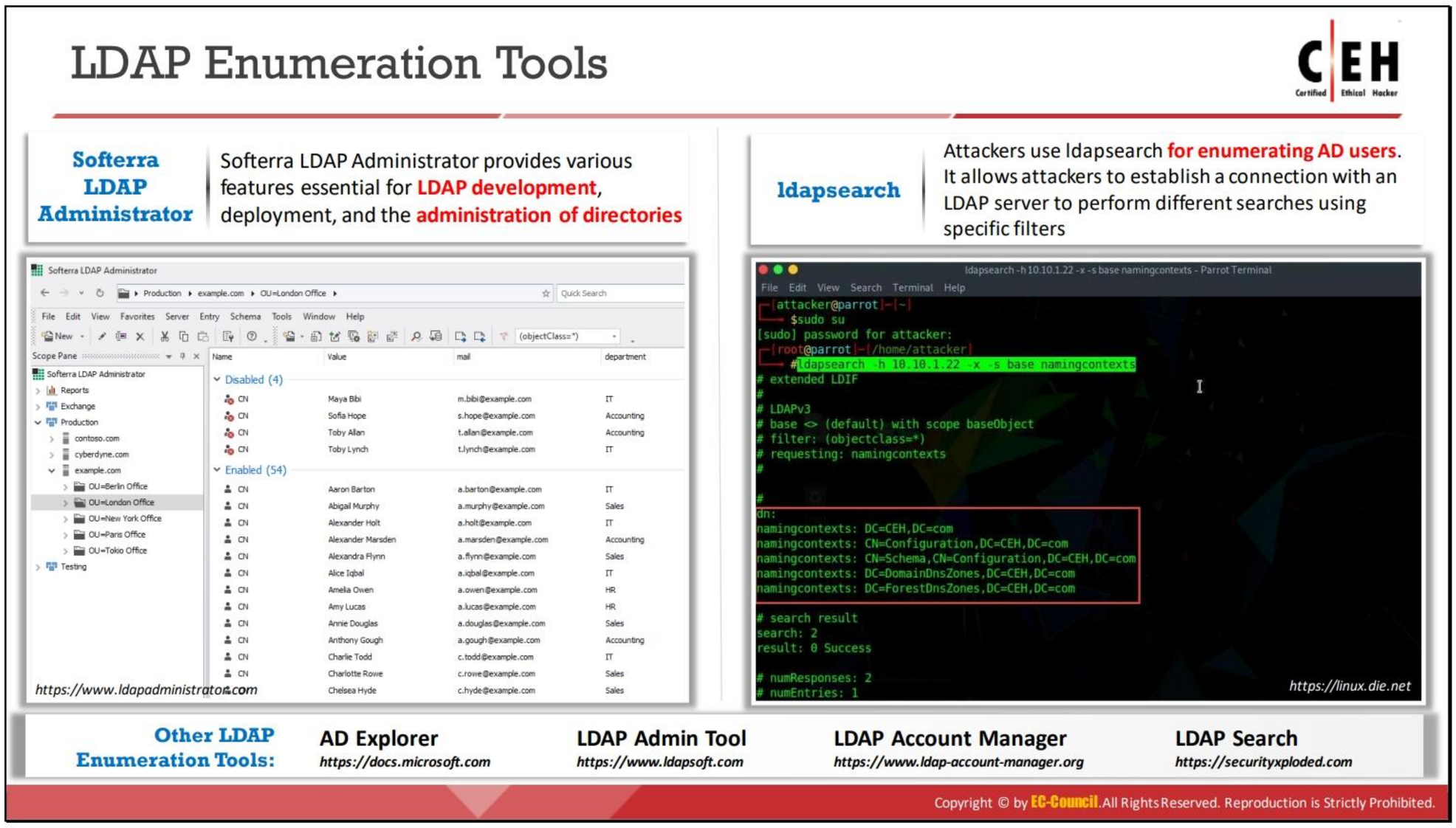


Figure 4.15: Screenshot showing output of the Nmap ldap-brute NSE script

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

https://t.me/learningnets



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.

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

https://t.me/learningnets

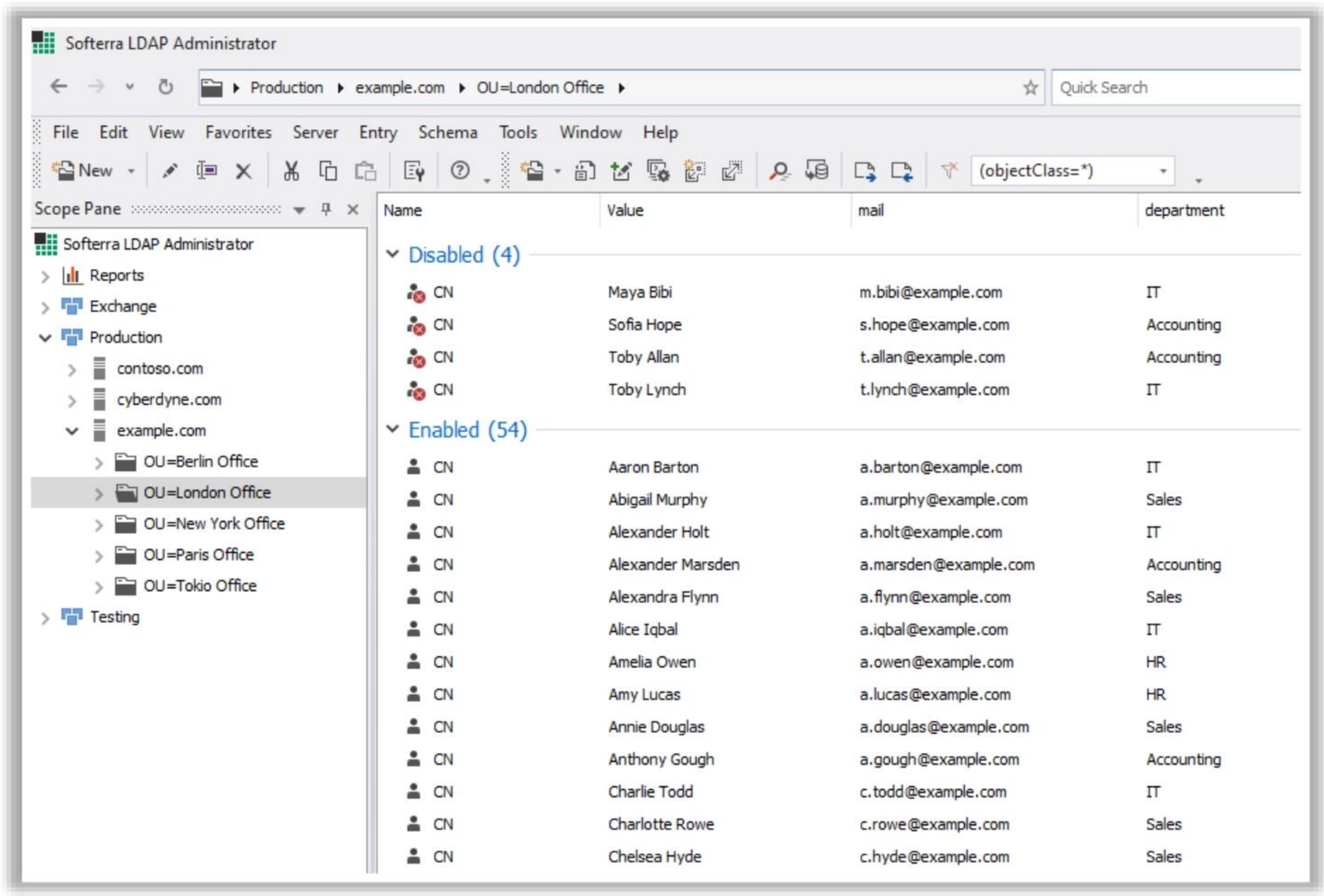


Figure 4.16: Screenshot of Softerra LDAP Administrator

- **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.

https://t.me/learningnets

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
```

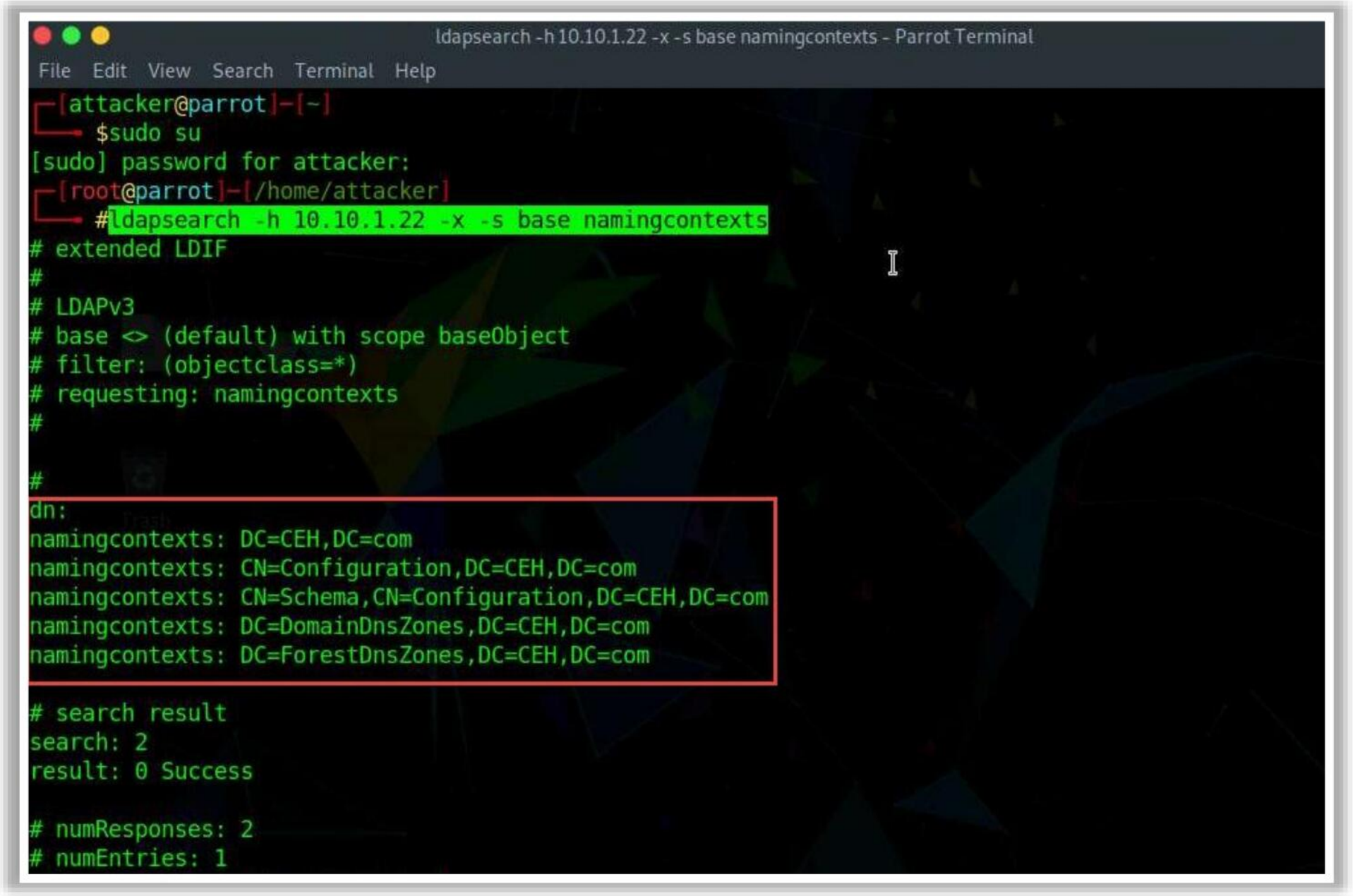


Figure 4.17: Screenshot of ldapsearch

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

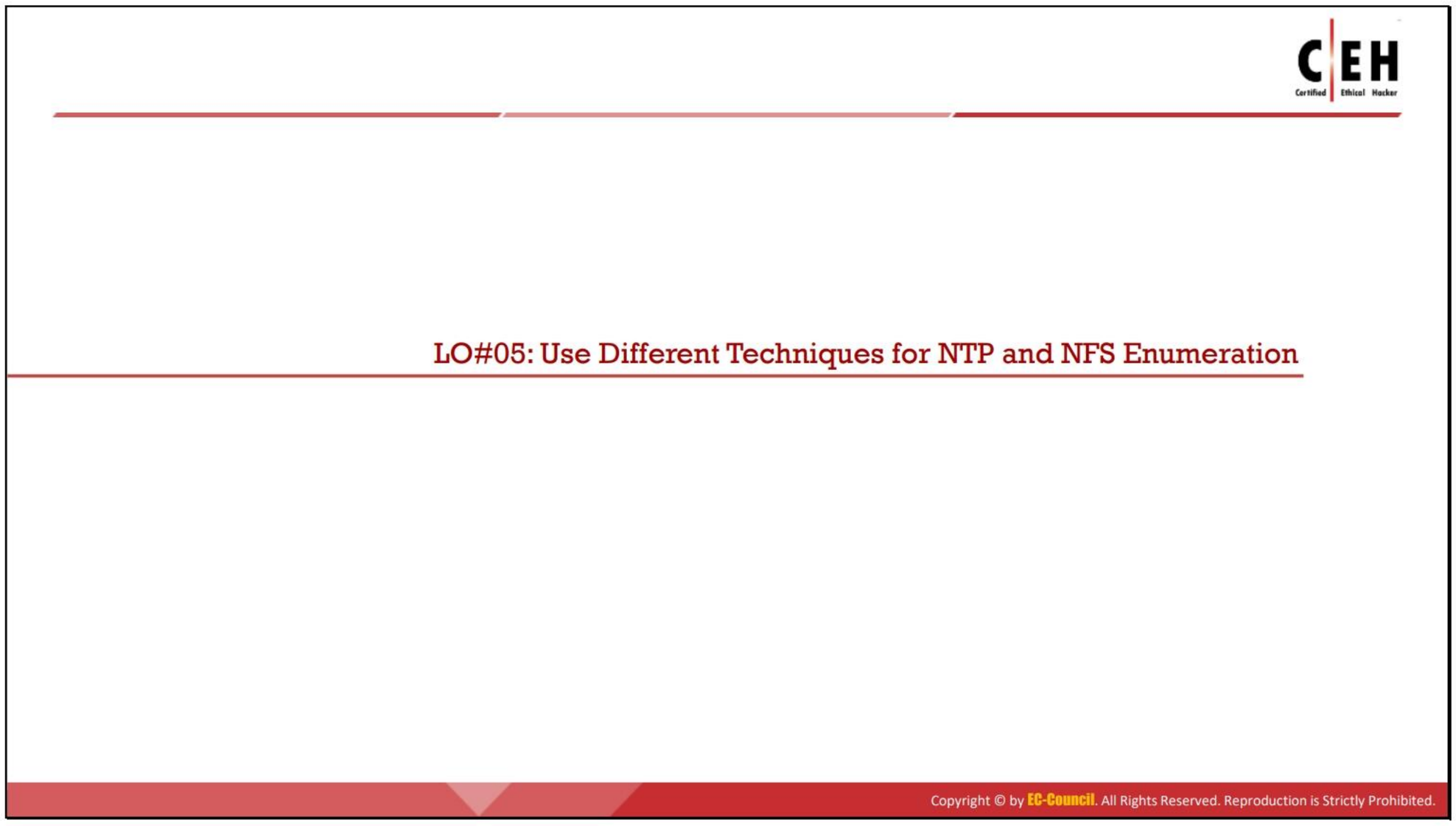
https://t.me/learningnets

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.

https://t.me/learningnets



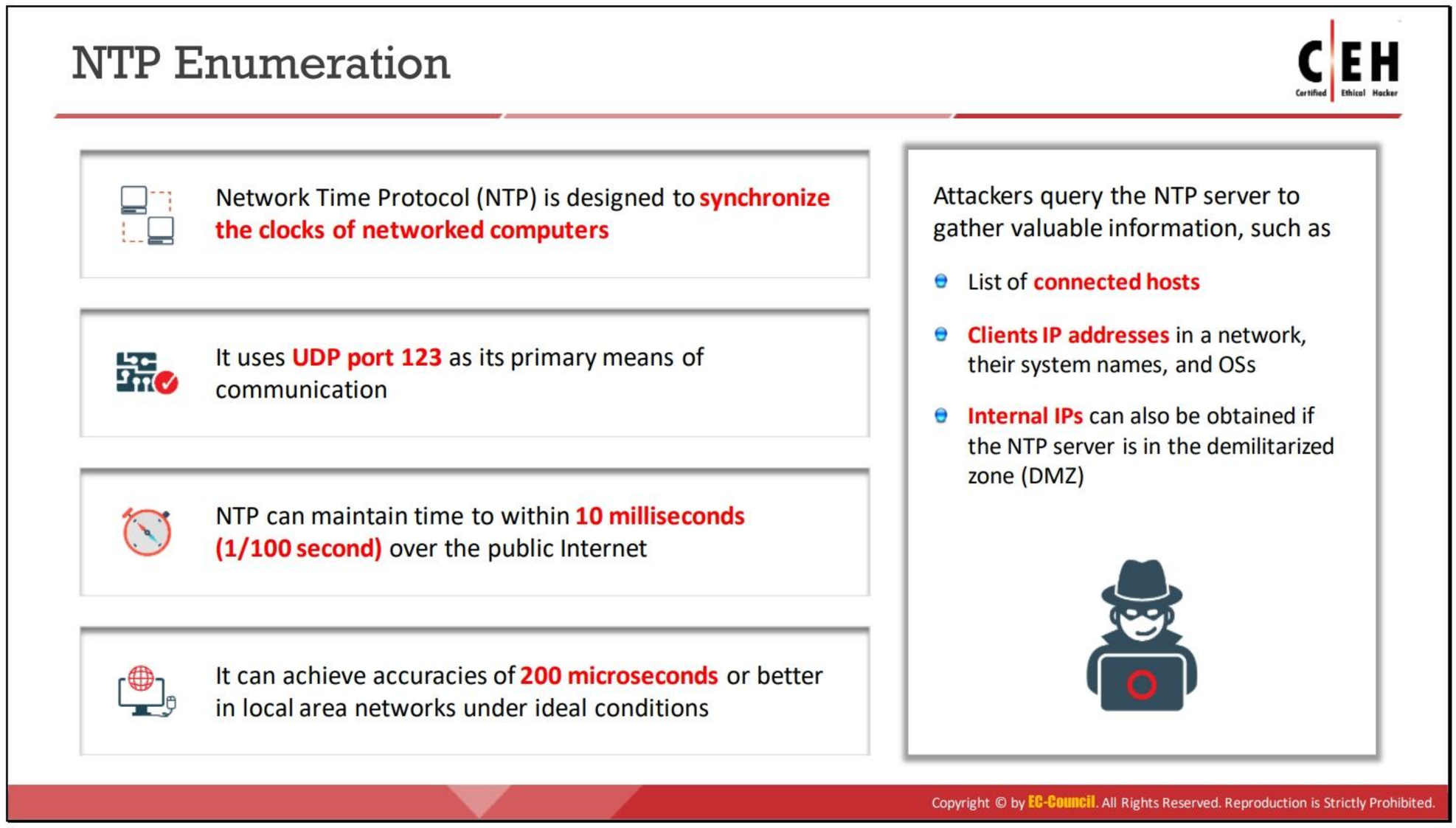
NTP and NFS Enumeration

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.

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

https://t.me/learningnets



NTP Enumeration

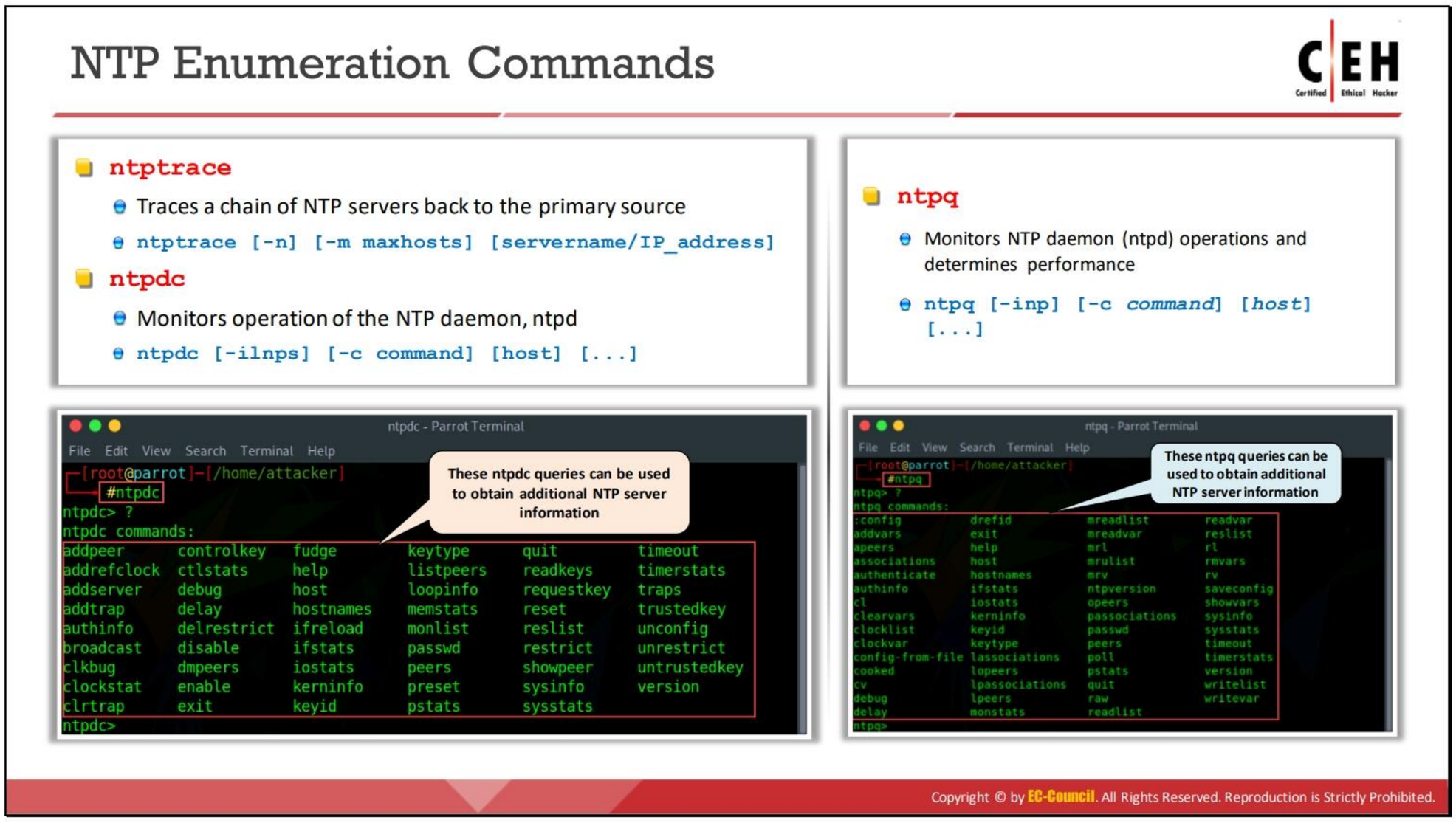
NTP is designed to synchronize clocks of networked computers. It uses UDP port 123 as its primary means of communication. NTP can maintain time within an error of 10 ms over the public Internet. Furthermore, it can achieve an accuracy of 200 µs or better in LANs under ideal conditions.

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)

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

https://t.me/learningnets



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

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

https://t.me/learningnets

-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

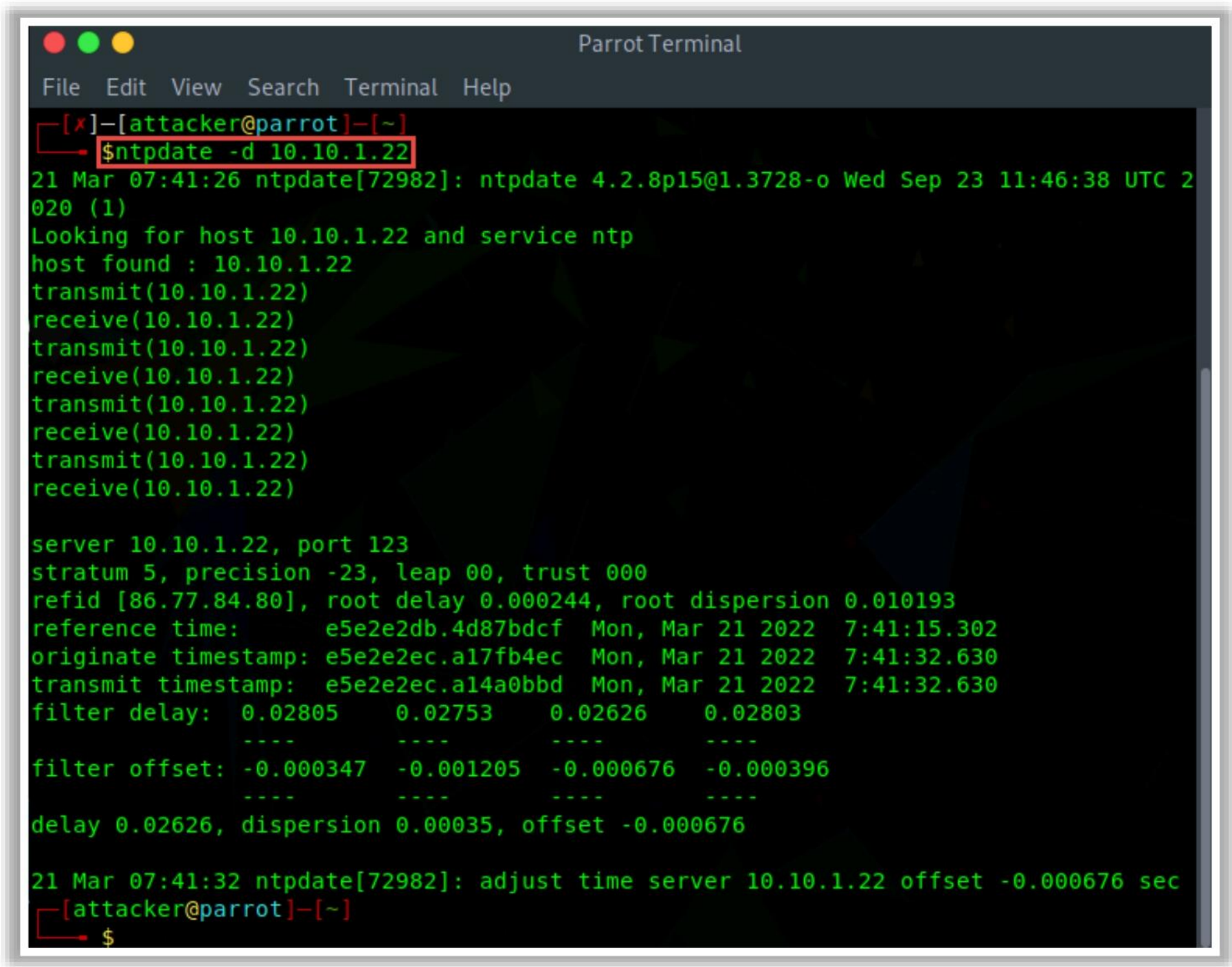


Figure 4.18: Screenshot of the ntpdate command, showing debugging information for a given IP

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

https://t.me/learningnets

- **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.

https://t.me/learningnets

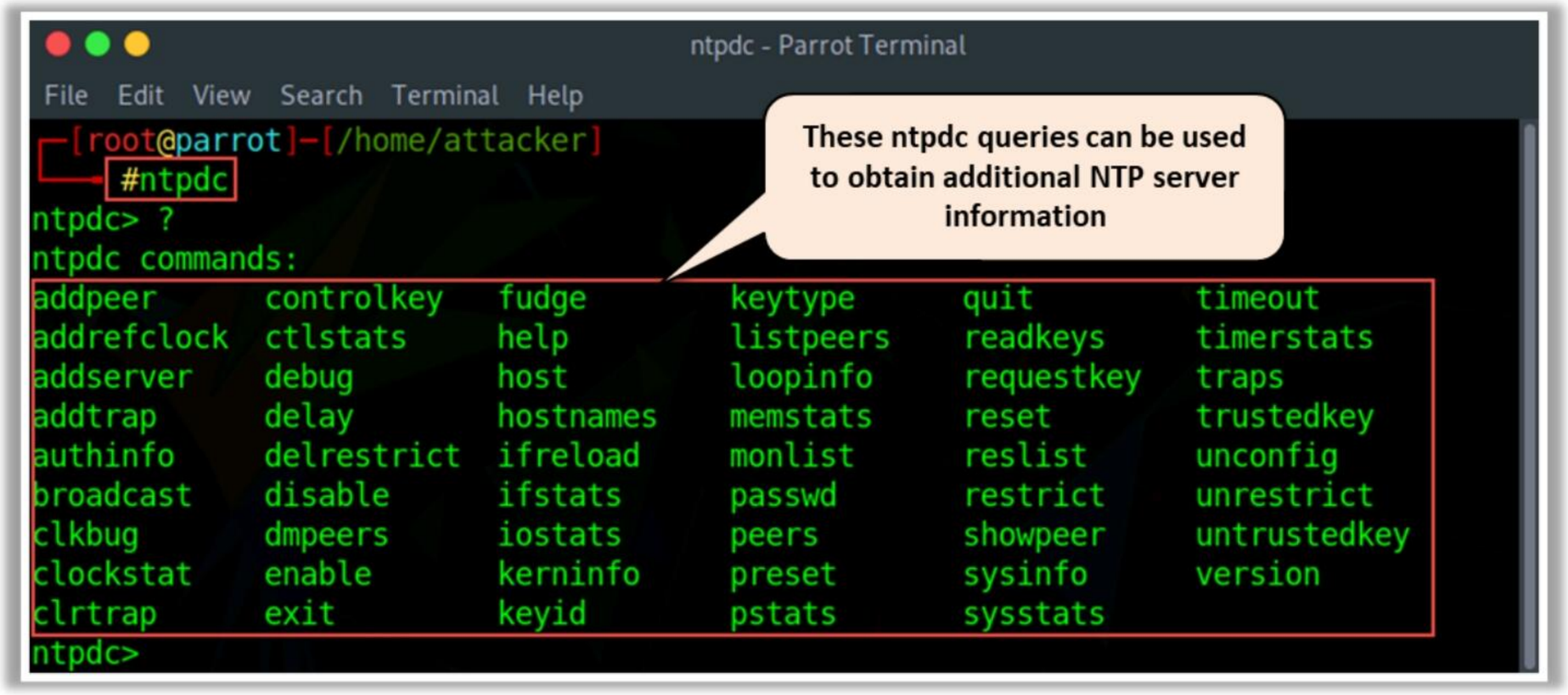


Figure 4.19: Screenshot of the ntpdc command

- **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.

https://t.me/learningnets

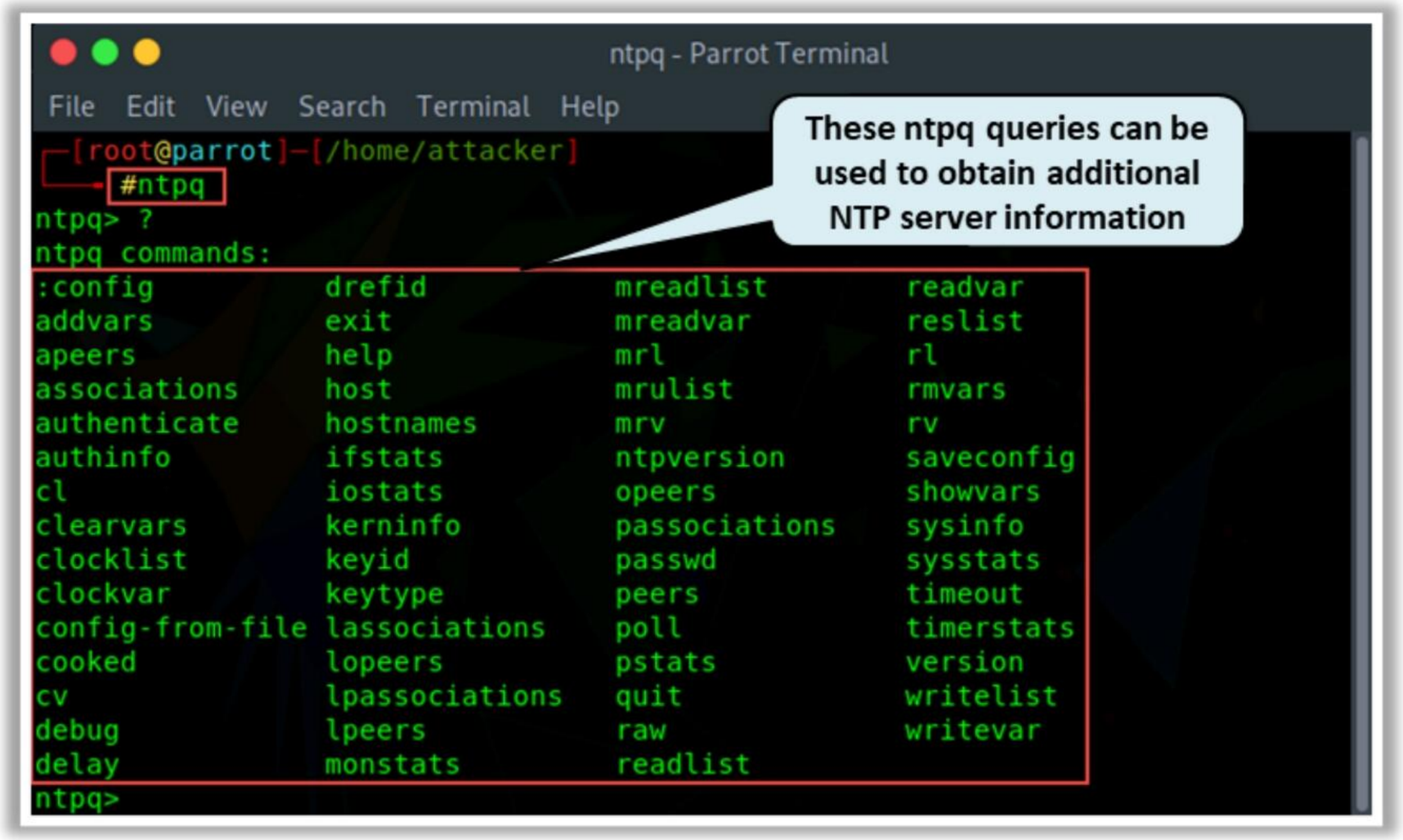
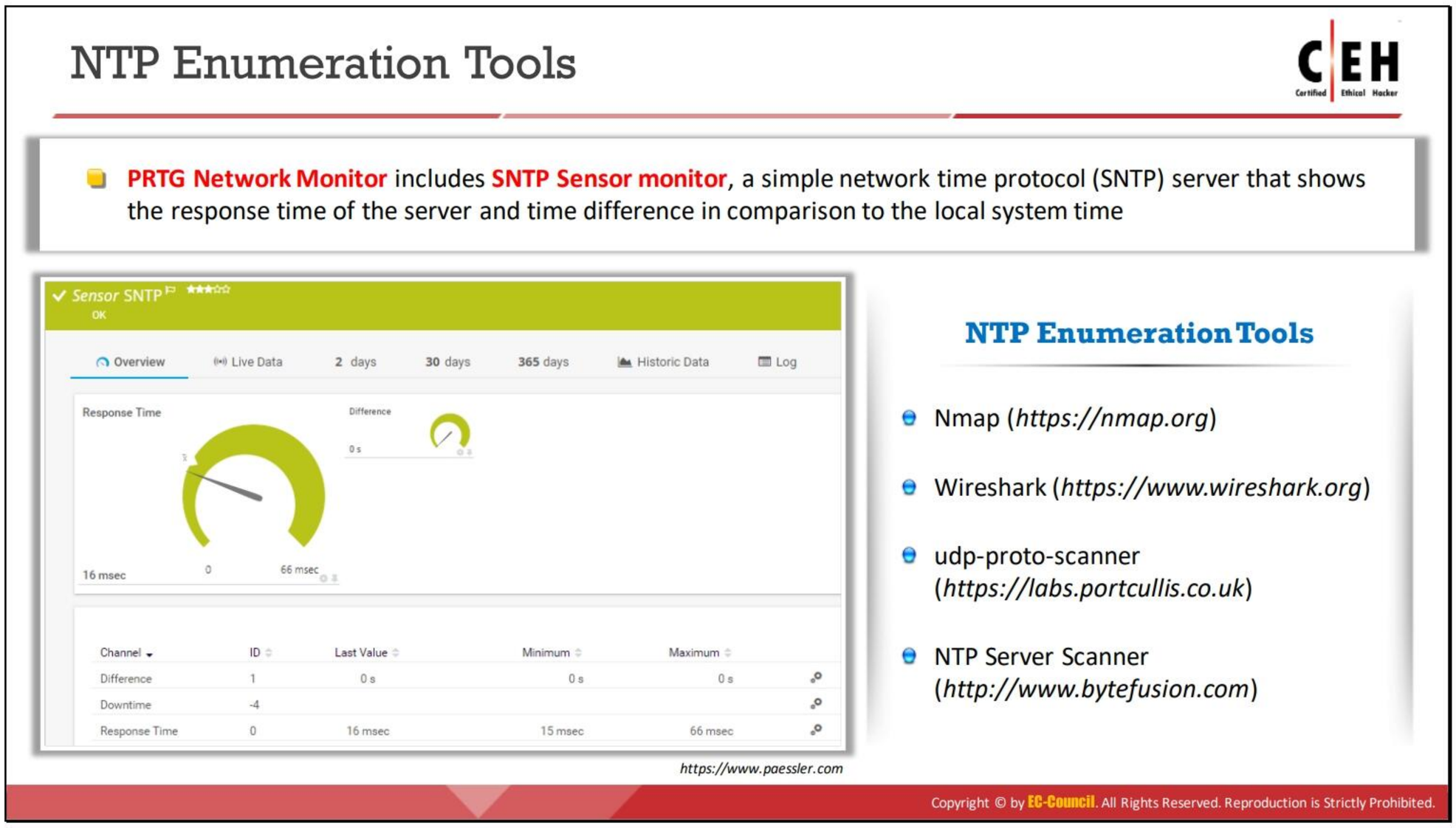


Figure 4.20: Screenshot of the ntpq command

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.

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

https://t.me/learningnets



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.

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

https://t.me/learningnets

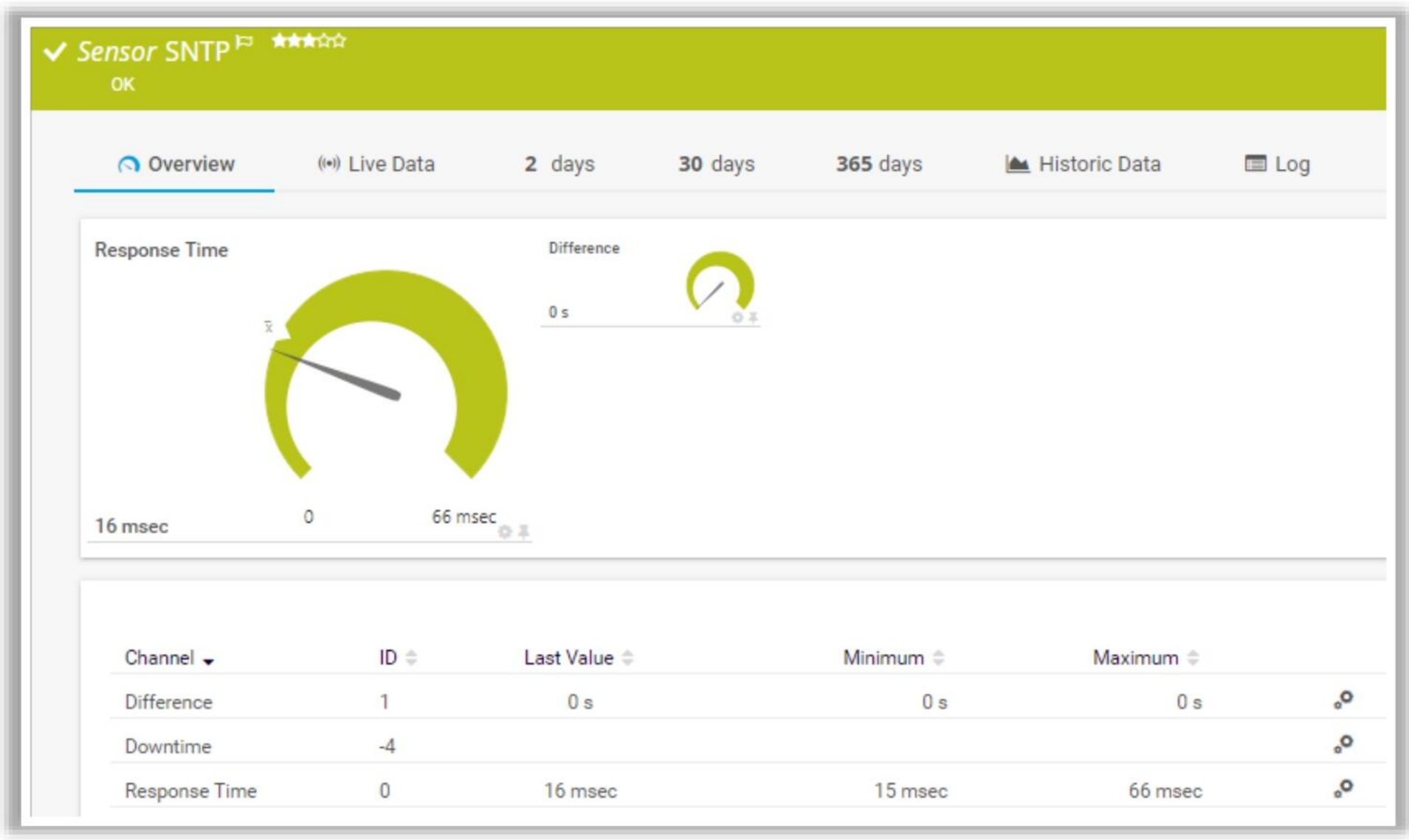


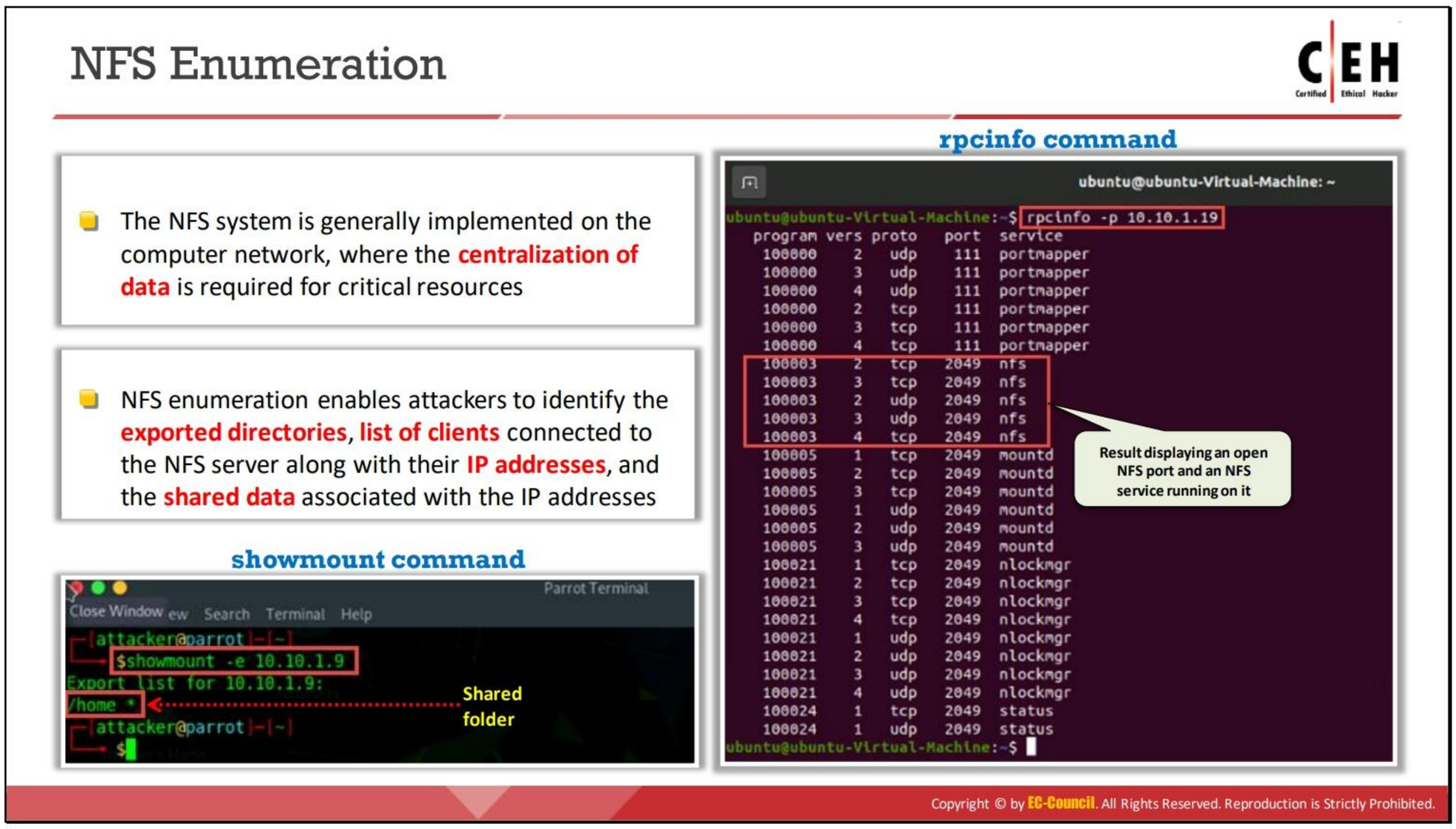
Figure 4.21: Screenshot of PRTG Network Monitor

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*)

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

https://t.me/learningnets



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>
```


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

https://t.me/learningnets

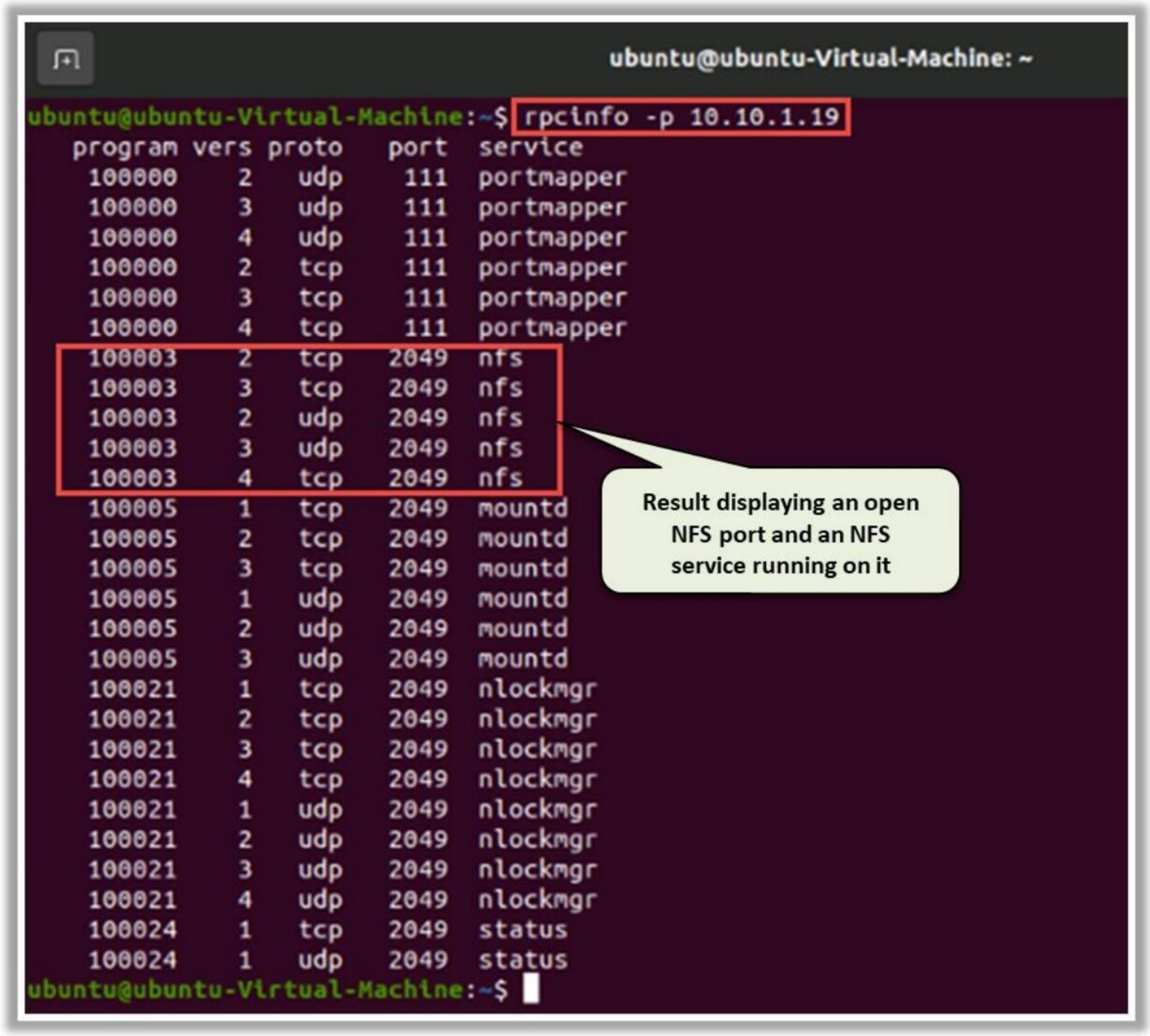


Figure 4.22: Screenshot of rpcinfo command displaying open NFS port and services

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>
```

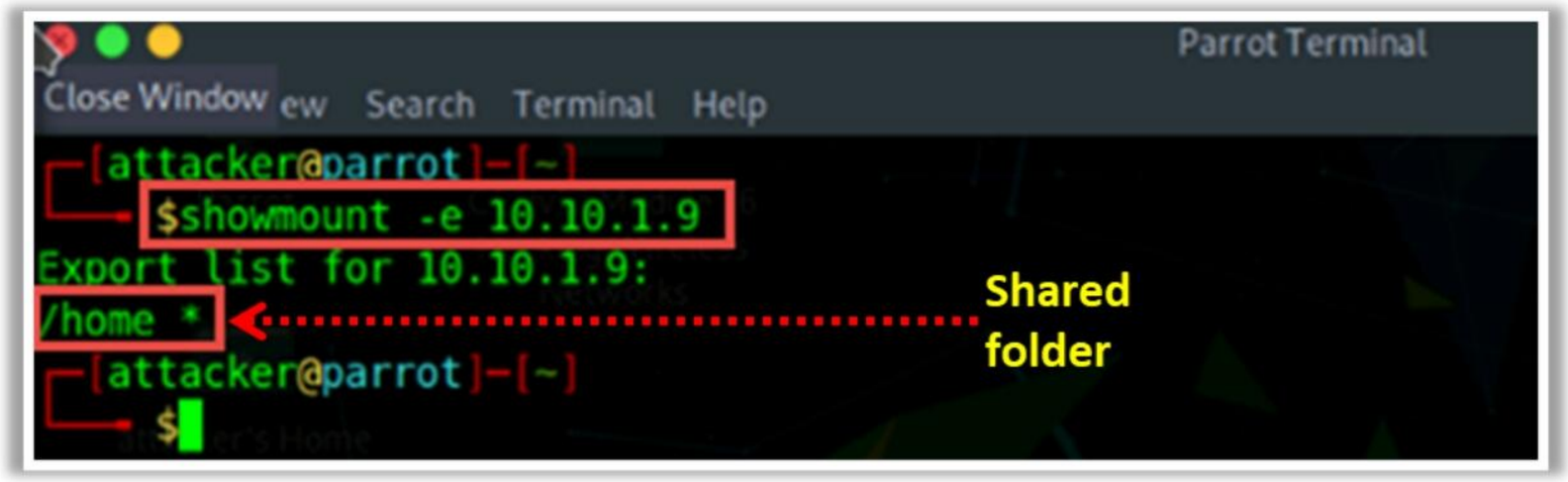
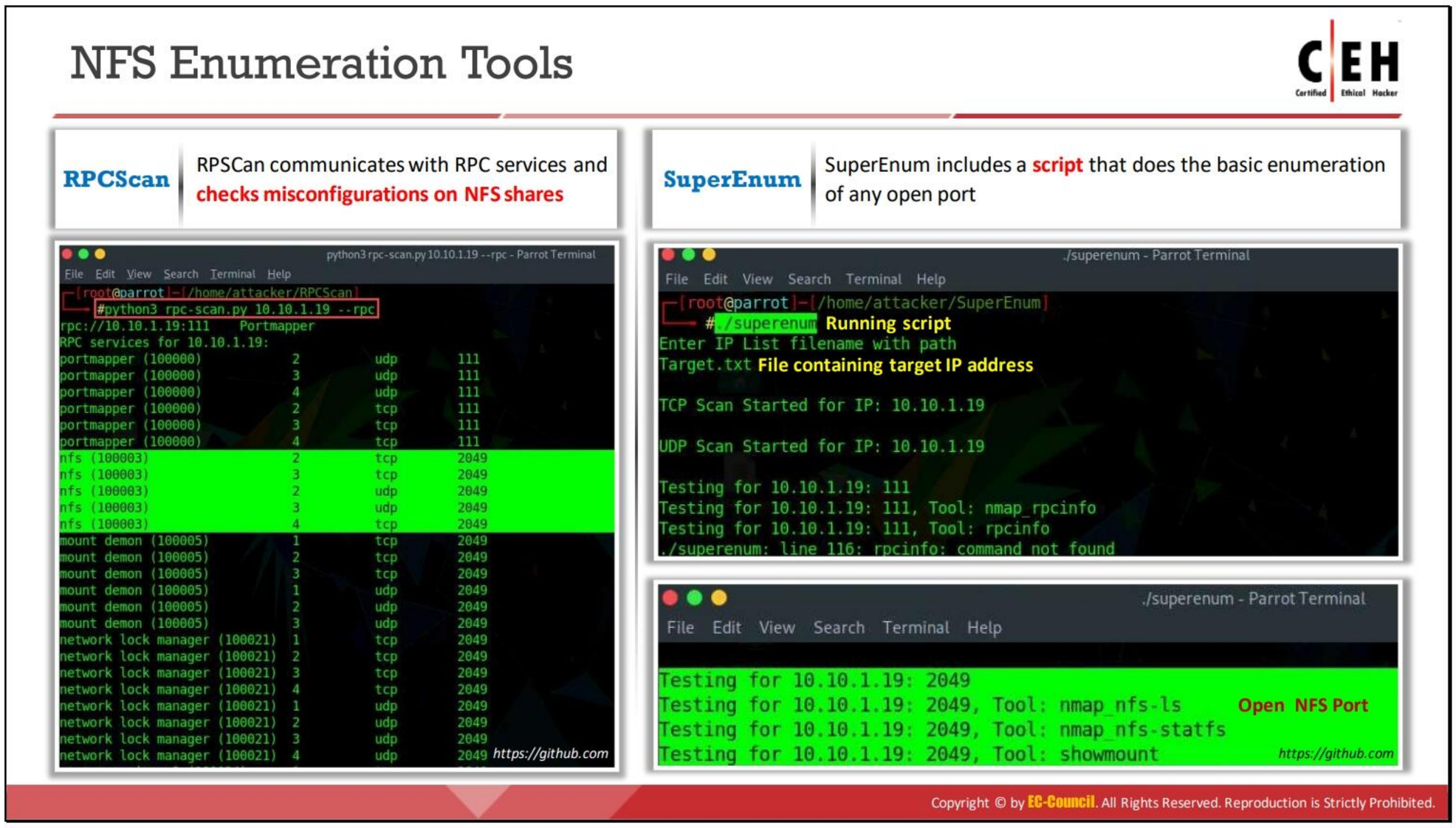


Figure 4.23: Screenshot of the showmount command displaying a shared directory

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.

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

https://t.me/learningnets



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
```


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

https://t.me/learningnets

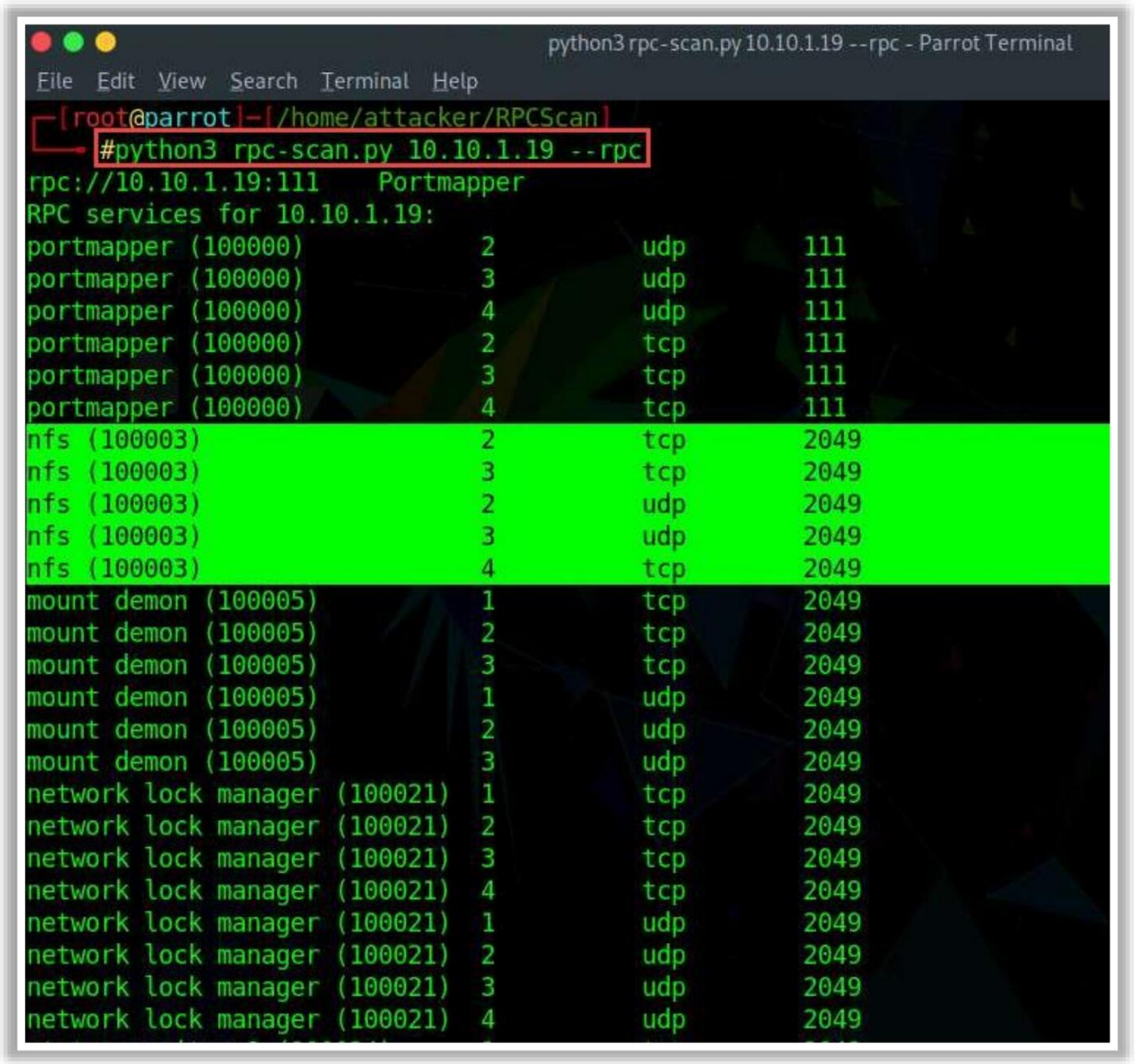


Figure 4.24: Screenshot of RPCScan displaying open NFS ports and services

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

https://t.me/learningnets

- **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.

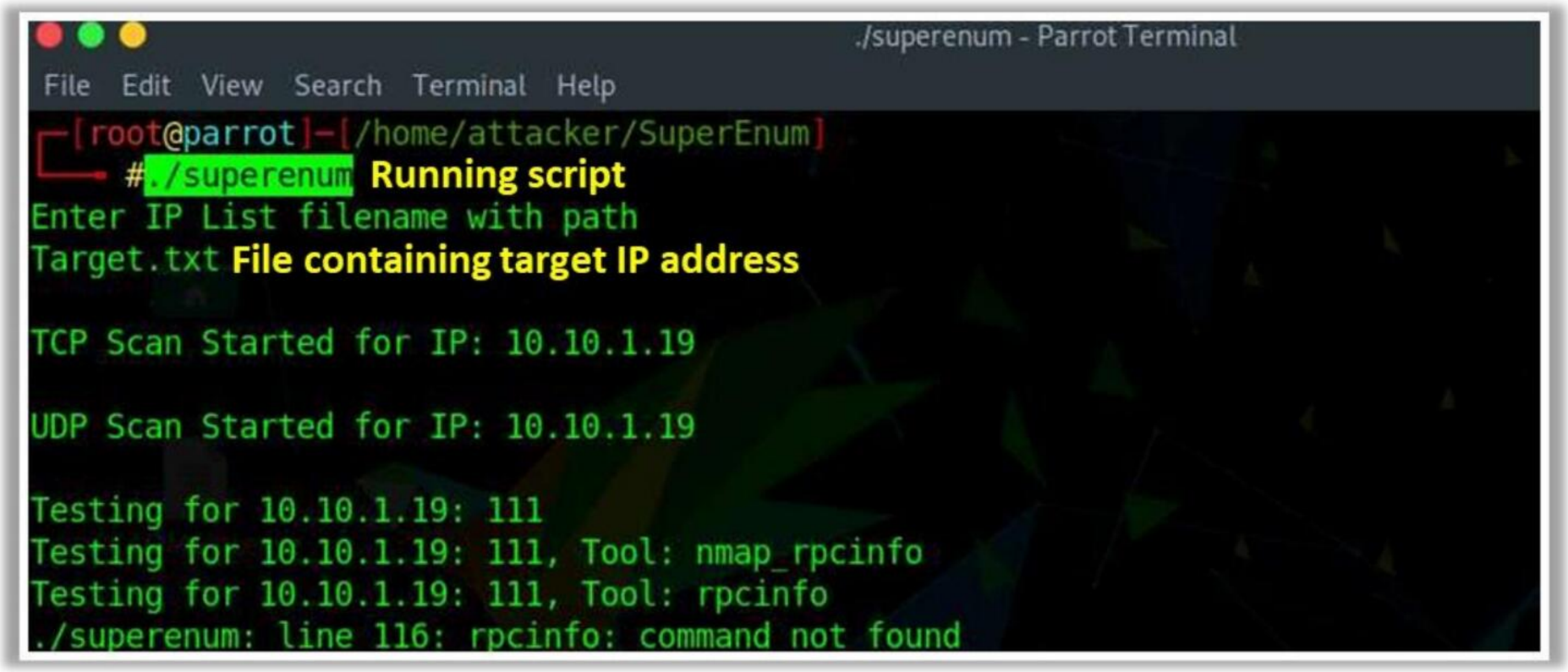


Figure 4.25: Screenshot of SuperEnum running a script

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.

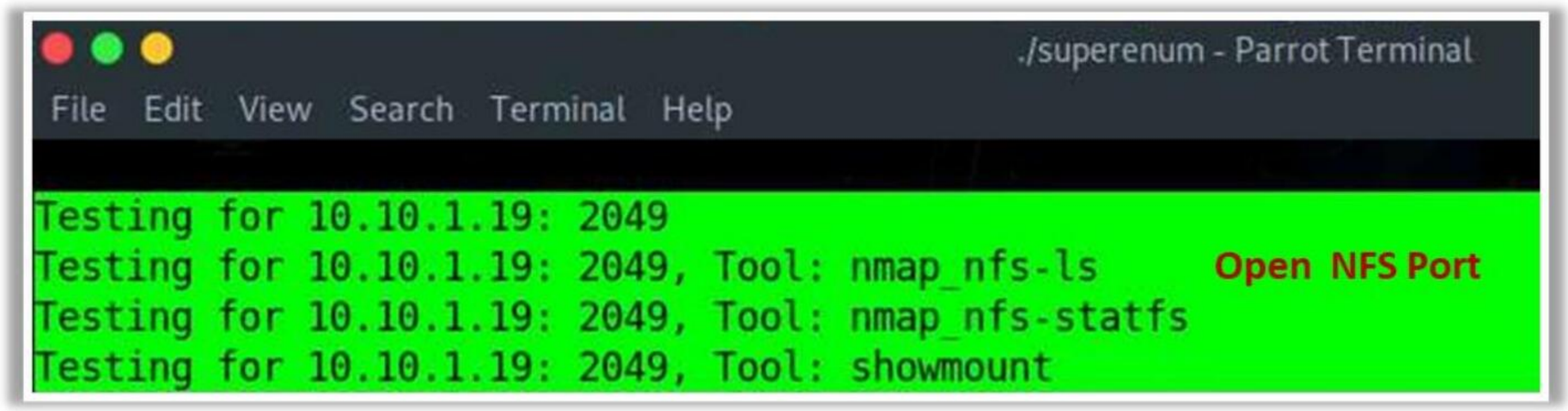


Figure 4.26: Screenshot of SuperEnum displaying open NFS ports

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

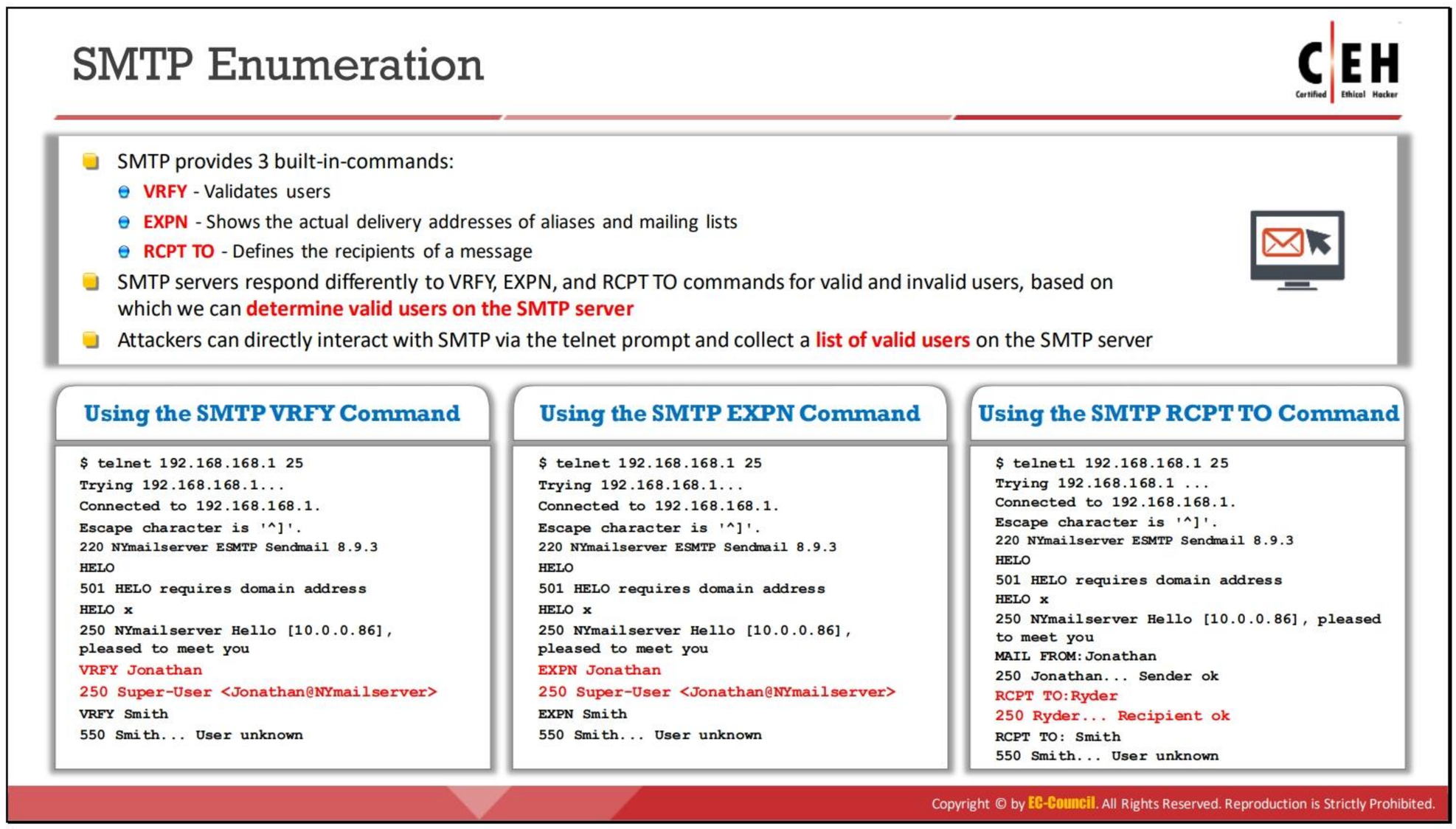
https://t.me/learningnets

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.

https://t.me/learningnets



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
```


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

https://t.me/learningnets

- **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

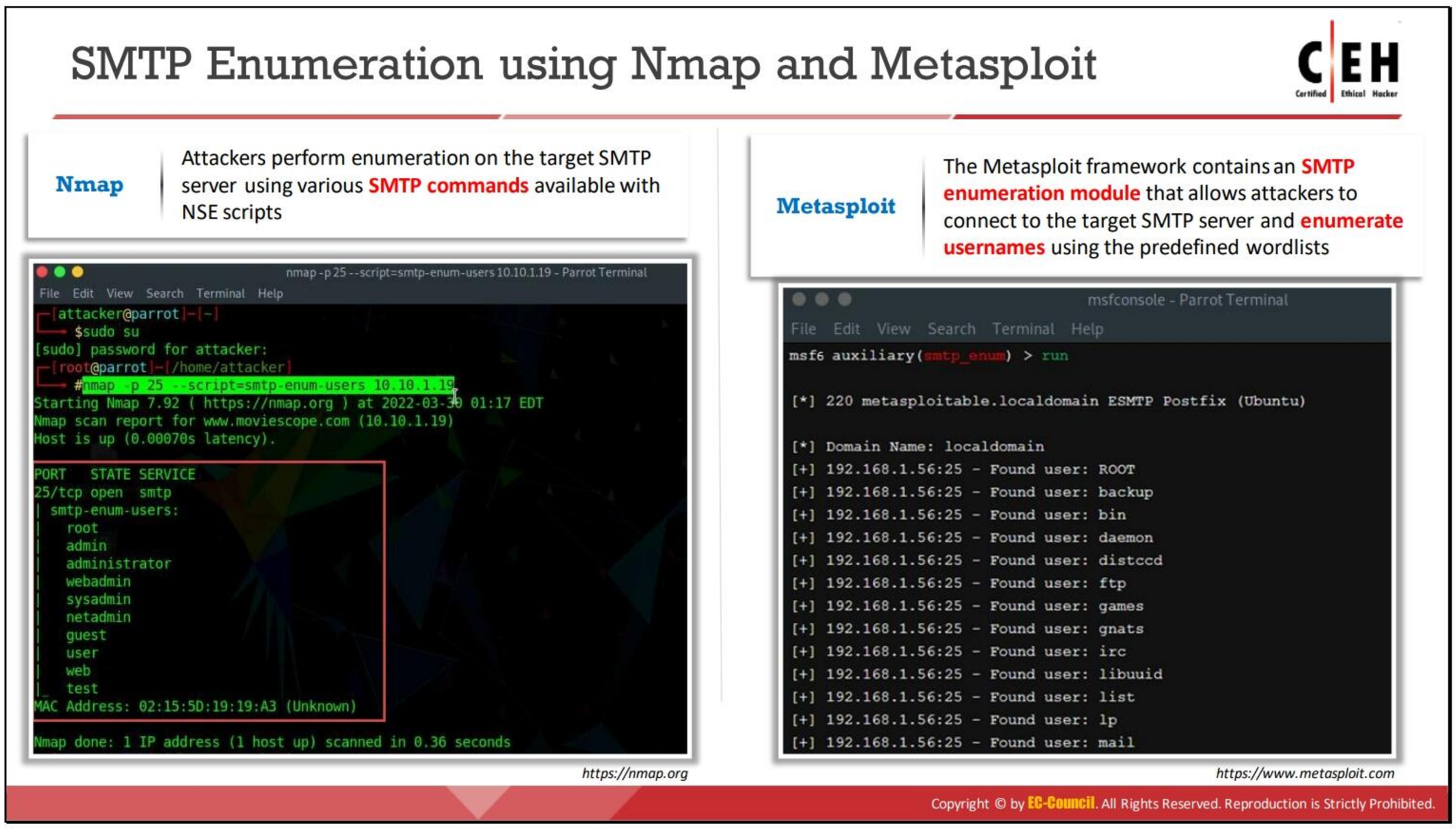
```
$ telnetl 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder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

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

https://t.me/learningnets



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.

https://t.me/learningnets

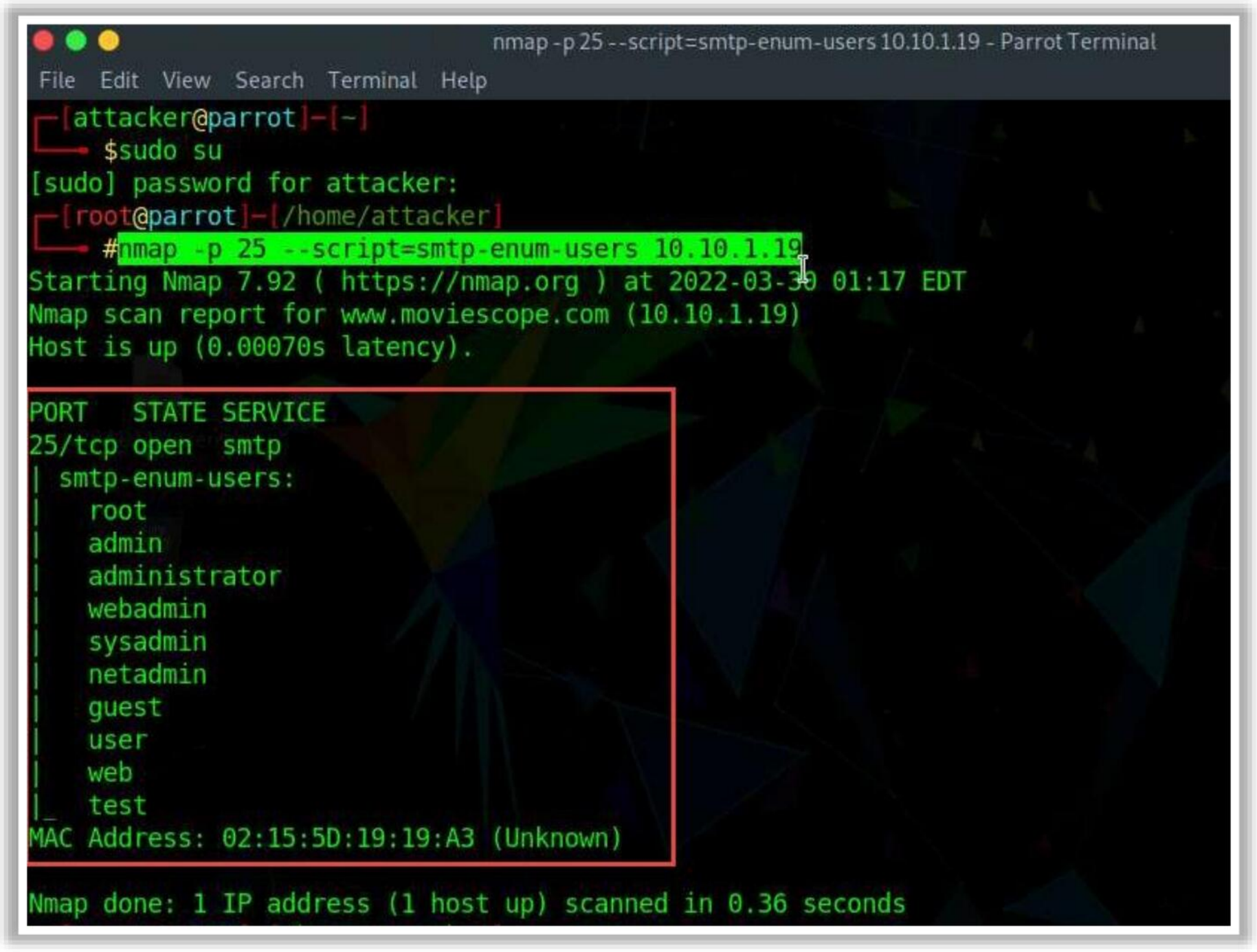


Figure 4.27: Screenshot showing output of the smtp-enum-users NSE script

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.

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

https://t.me/learningnets

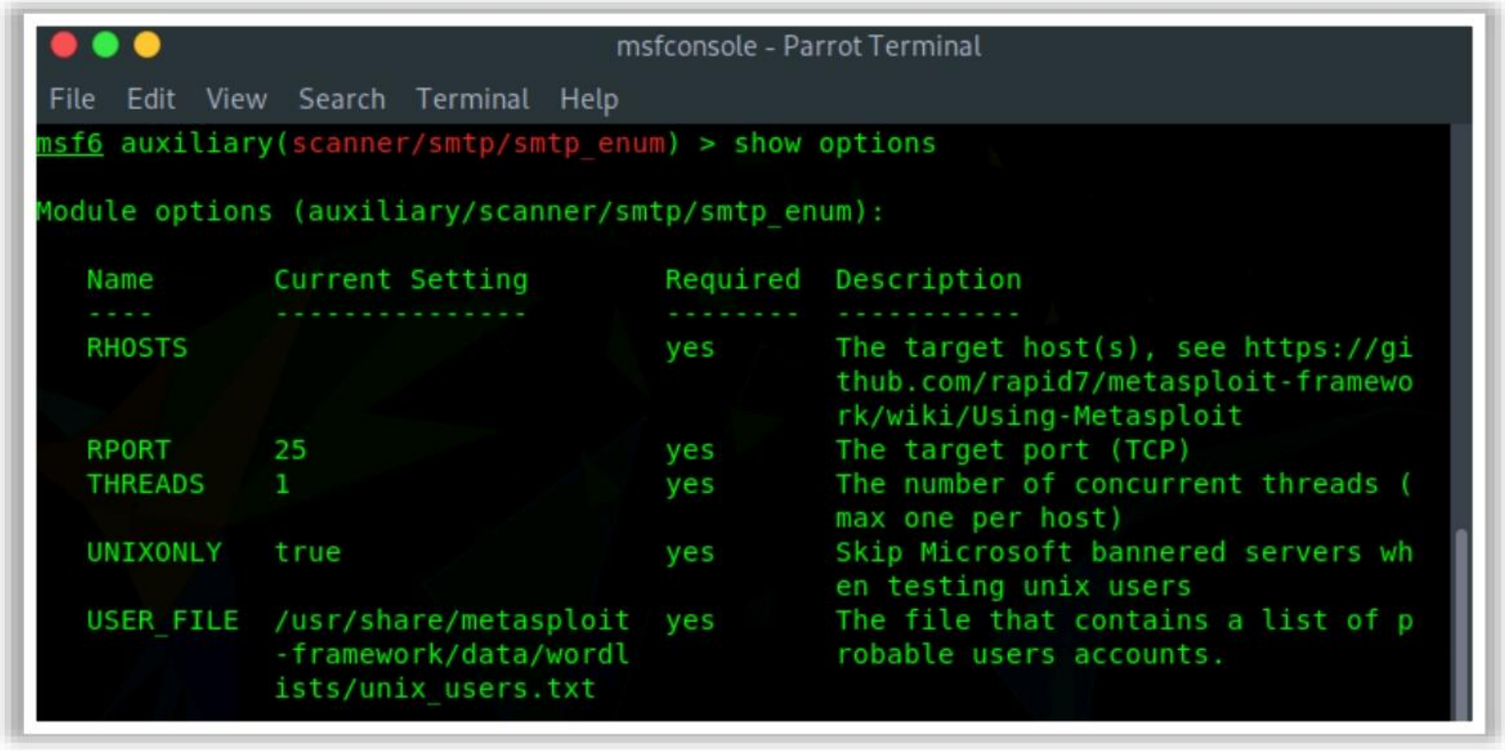


Figure 4.28: Screenshot of Metasploit showing smtp_enum options

- **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/64etasploit-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.

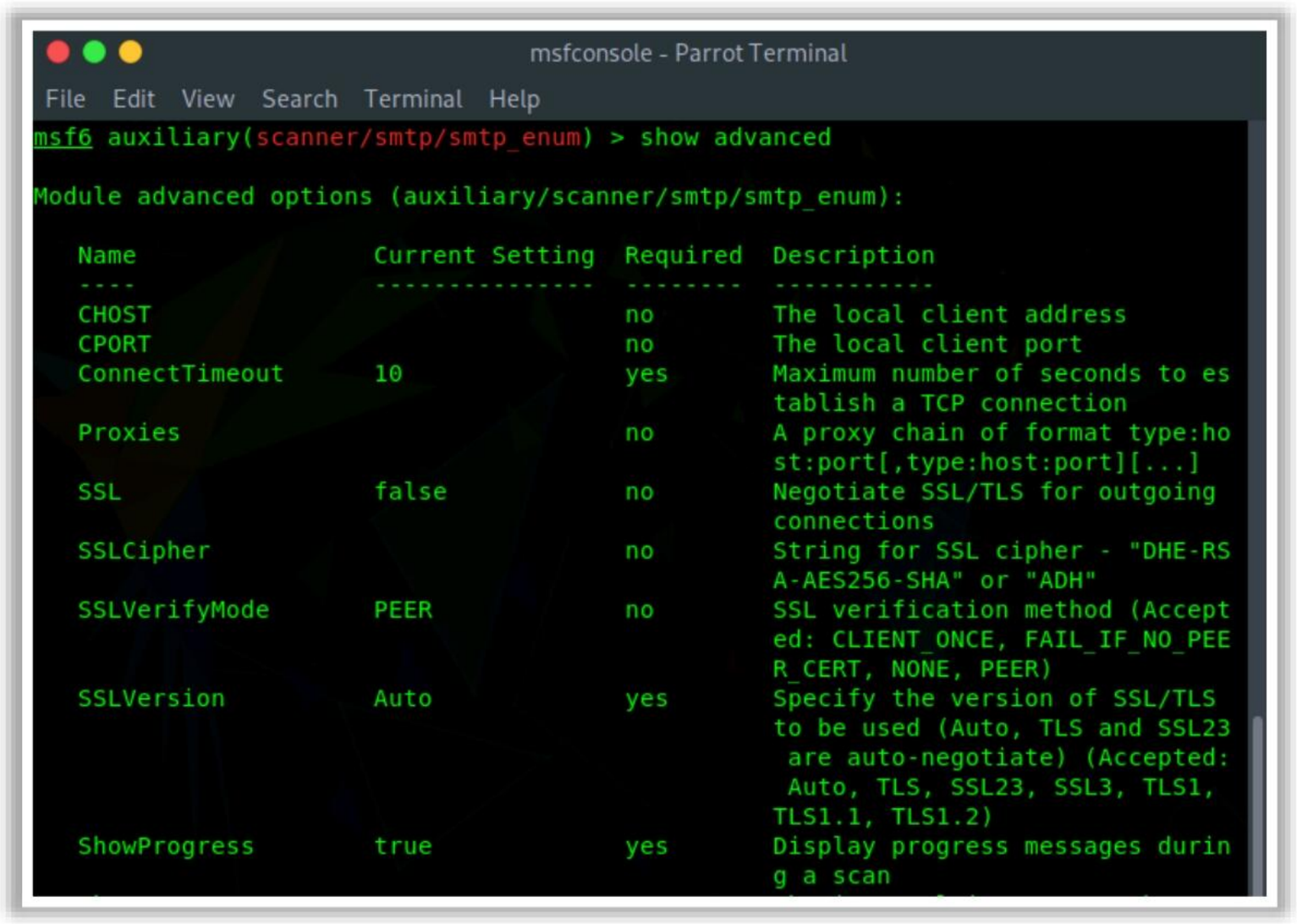


Figure 4.29: Screenshot of Metasploit showing smtp_enum advanced options

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

https://t.me/learningnets

- **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.

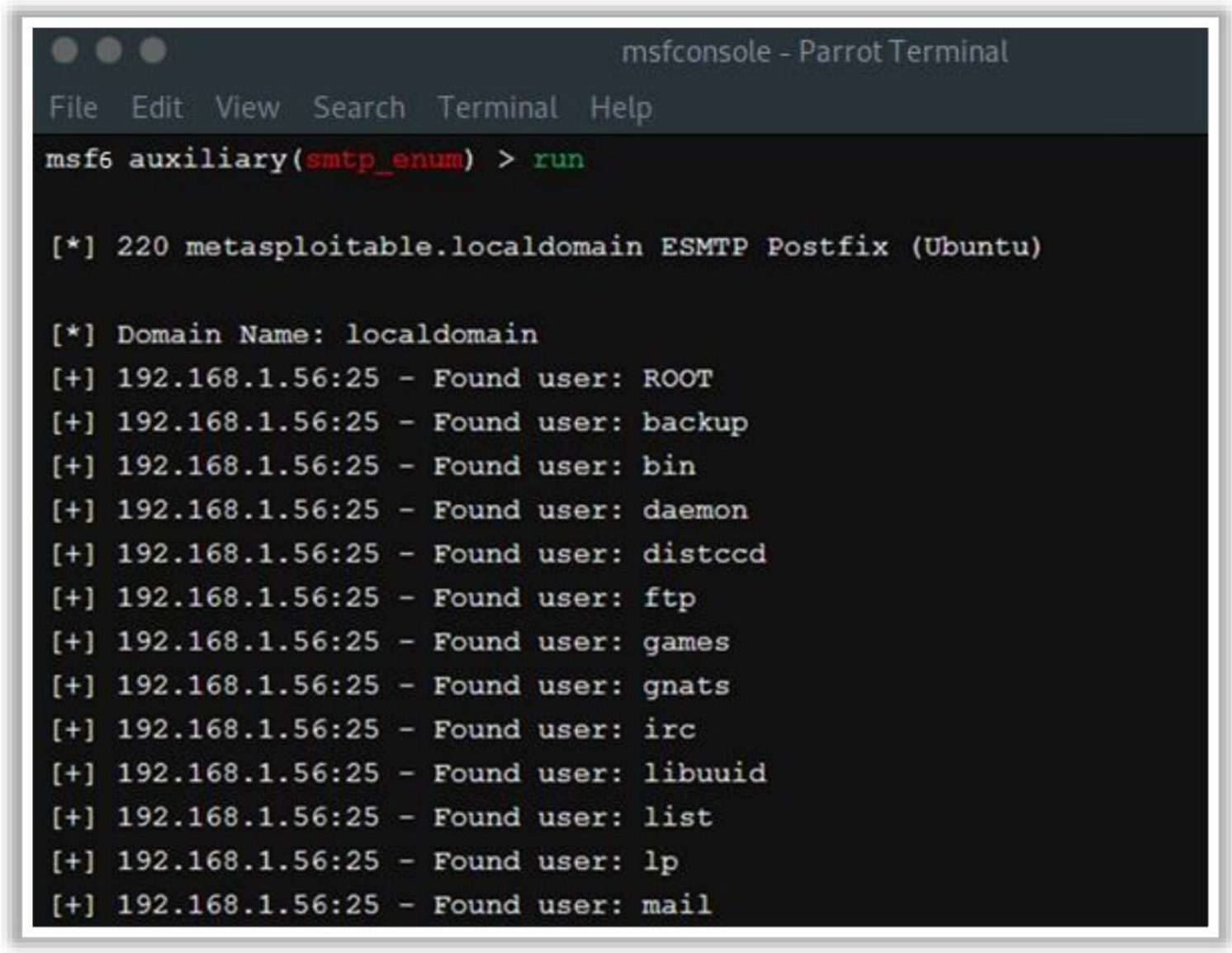
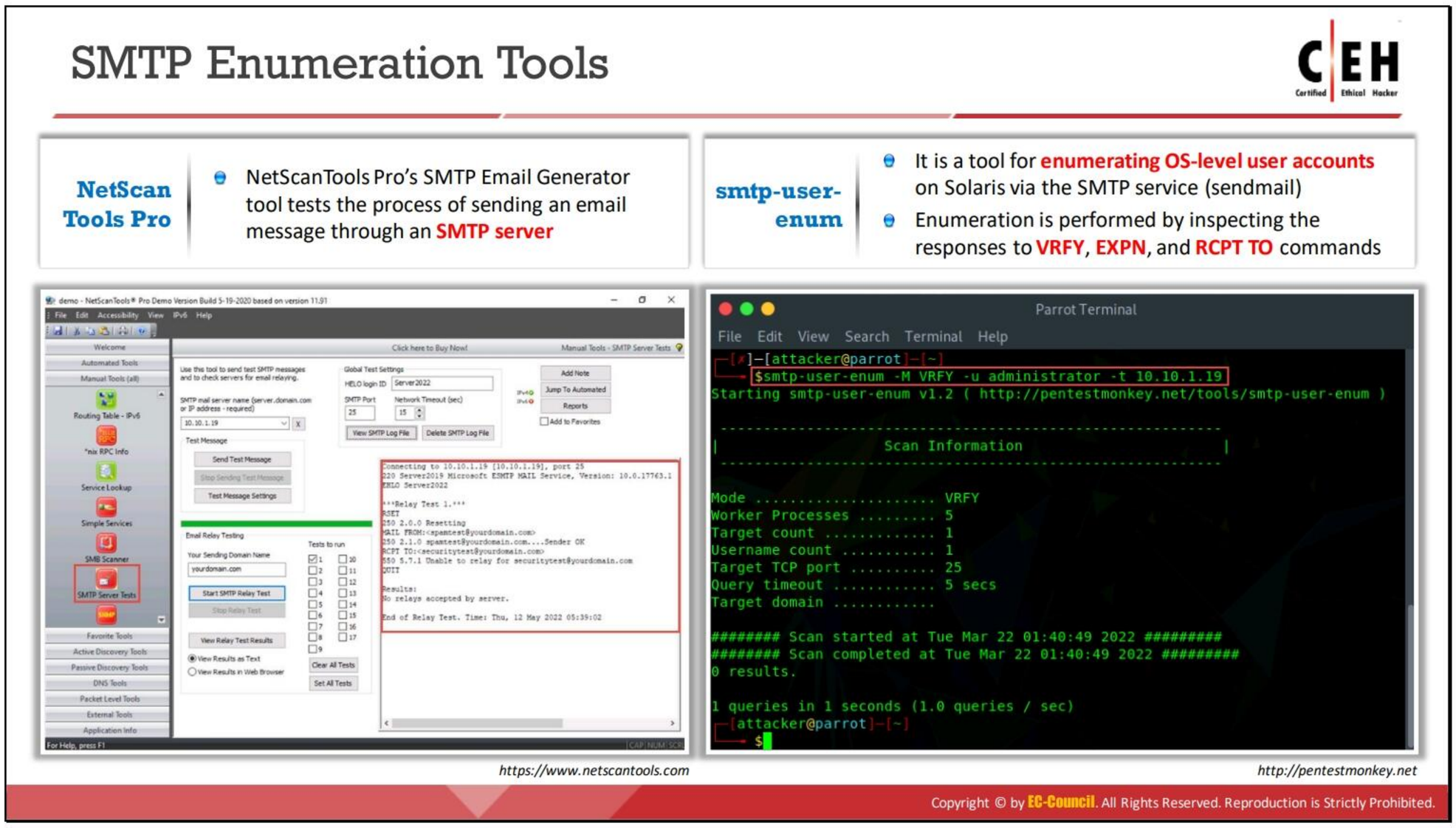


Figure 4.30: Screenshot of Metasploit retrieving SMTP users

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.

https://t.me/learningnets



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.

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

https://t.me/learningnets

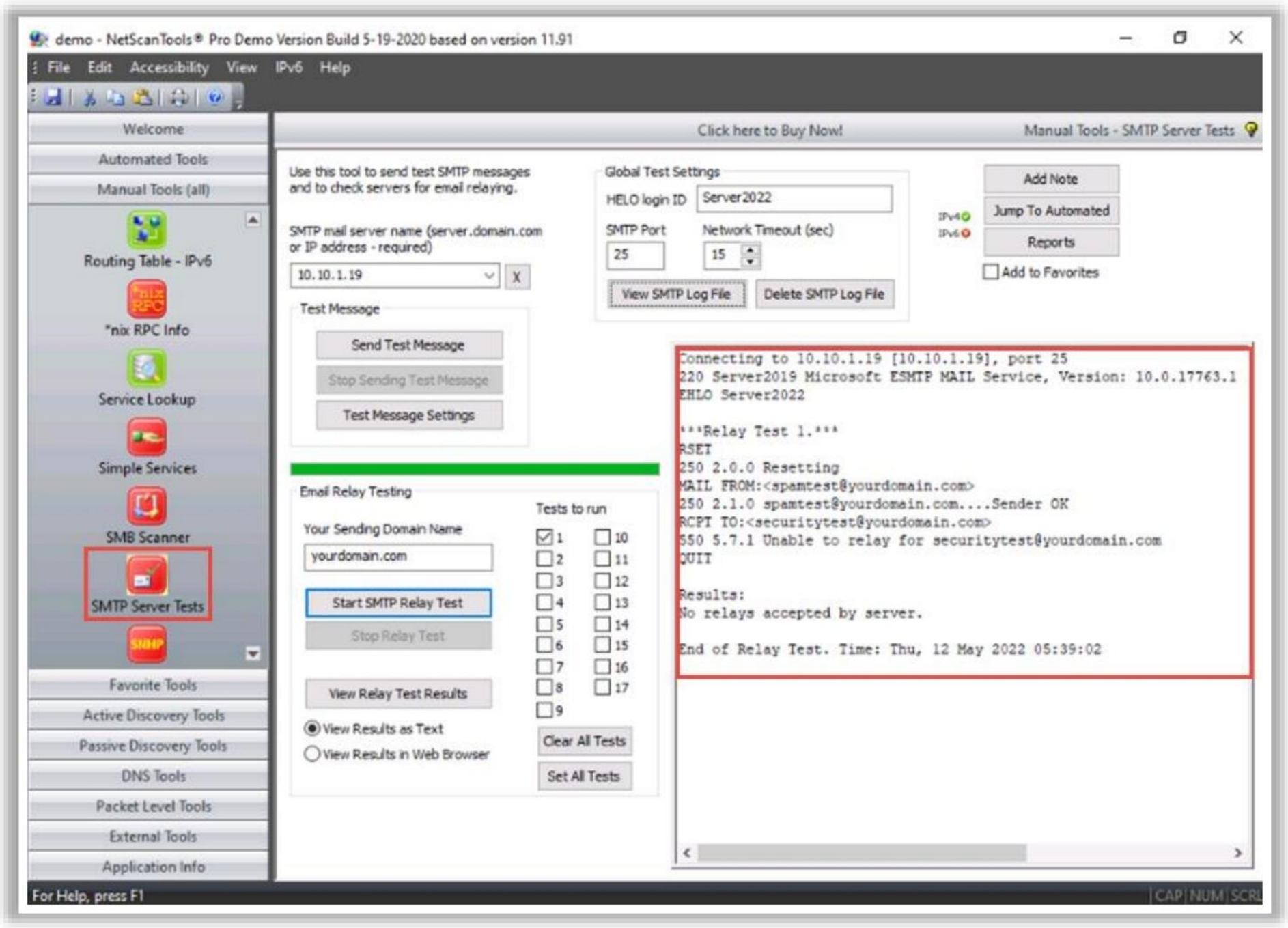


Figure 4.31: Screenshot of NetScanTools Pro

- **smtp-user-enum**

  Source: *http://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. 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)

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

https://t.me/learningnets

- **-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

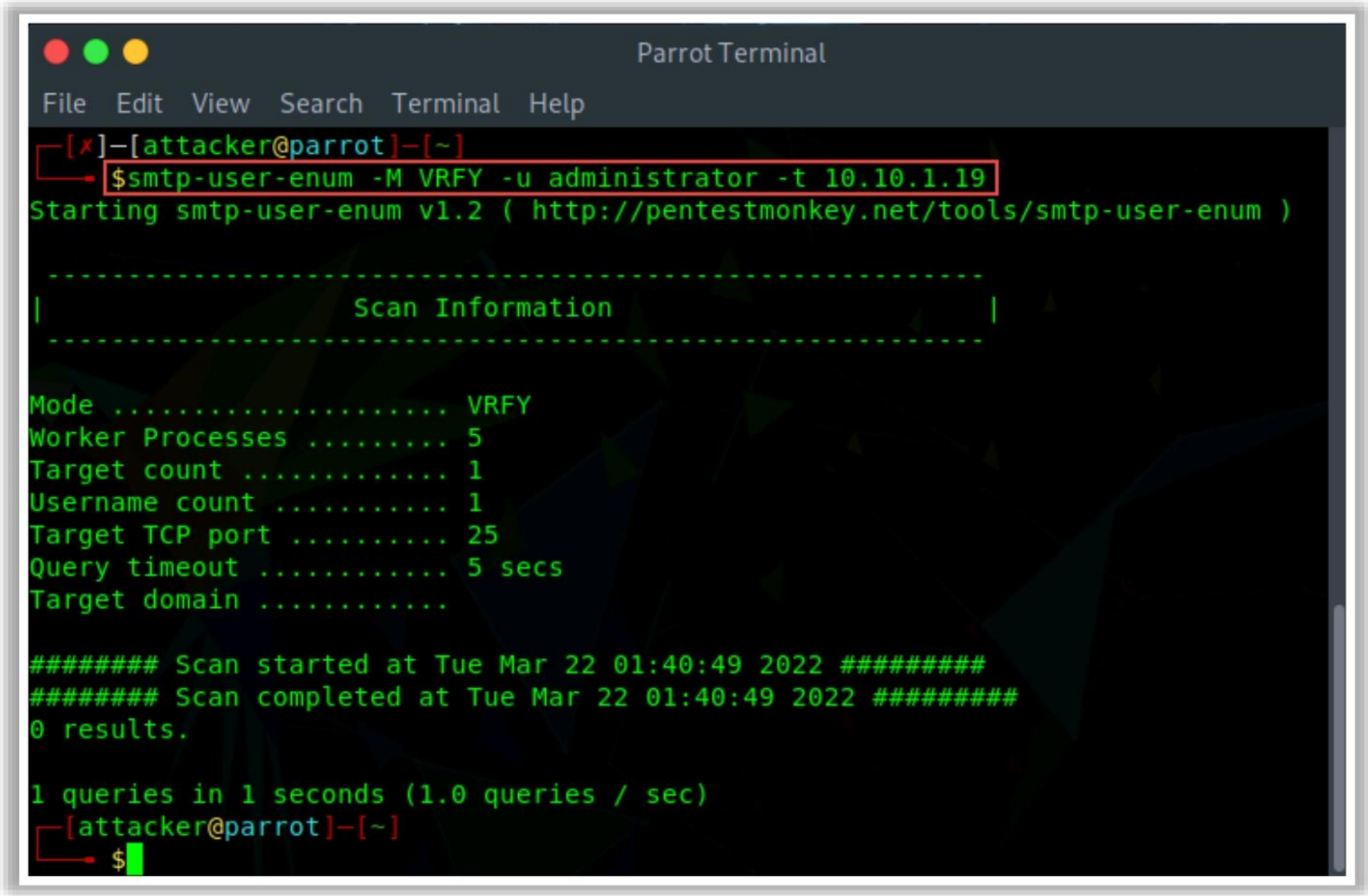
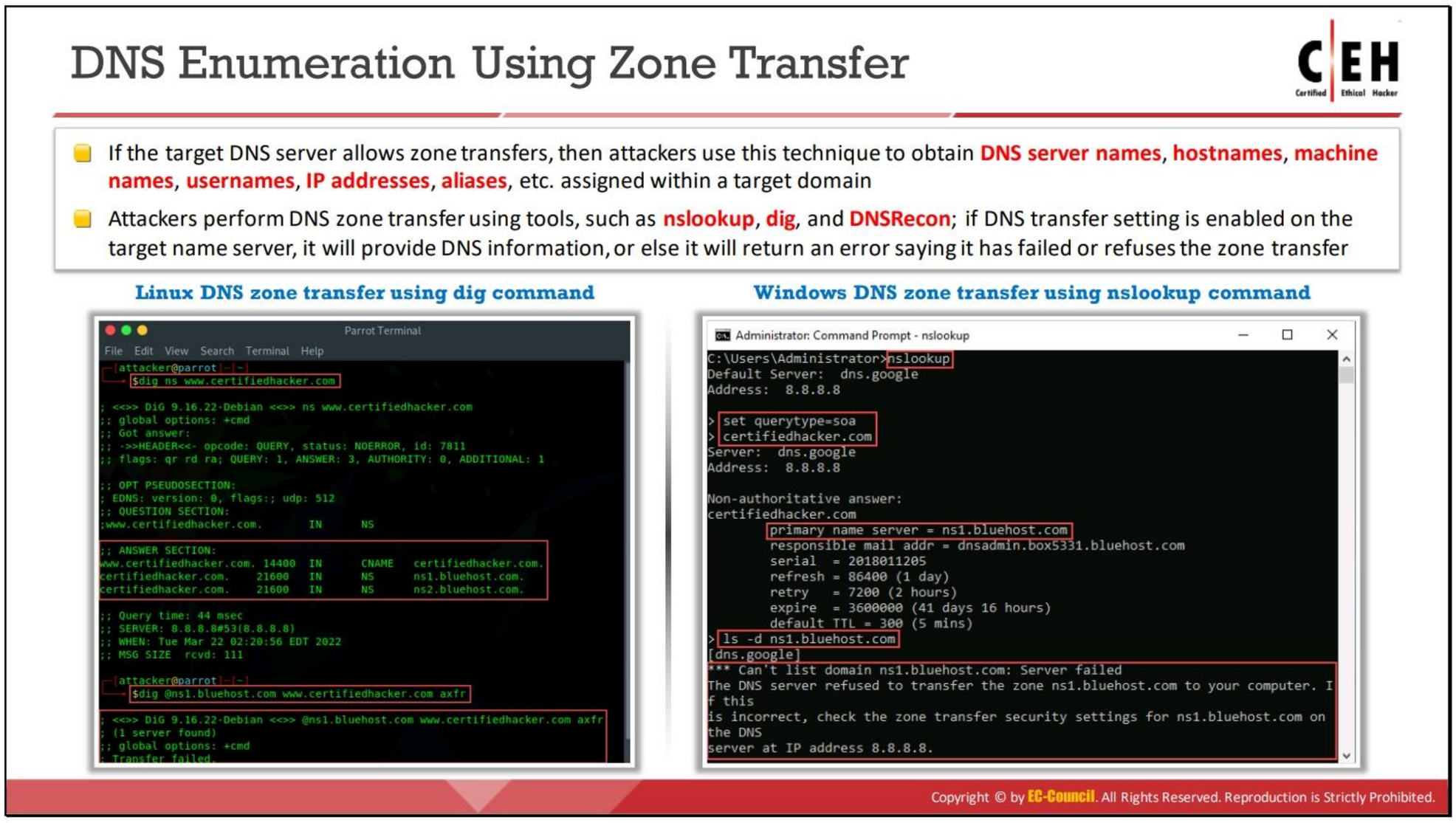


Figure 4.32: Screenshot of smtp-user-enum

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

https://t.me/learningnets



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.

https://t.me/learningnets

- **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

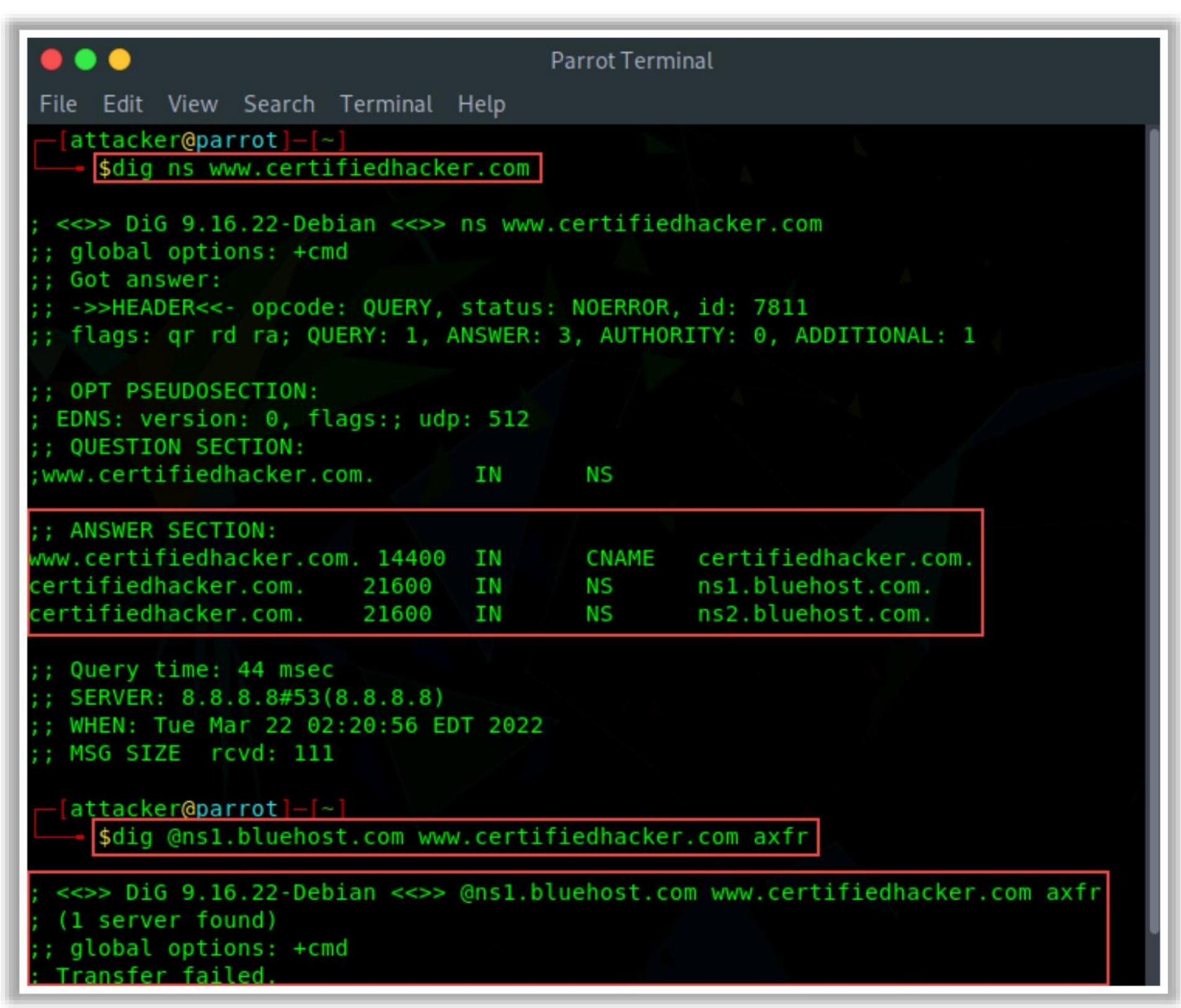


Figure 4.33: Screenshot of Linux DNS zone transfer using dig command

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

https://t.me/learningnets

- **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:

  `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>`

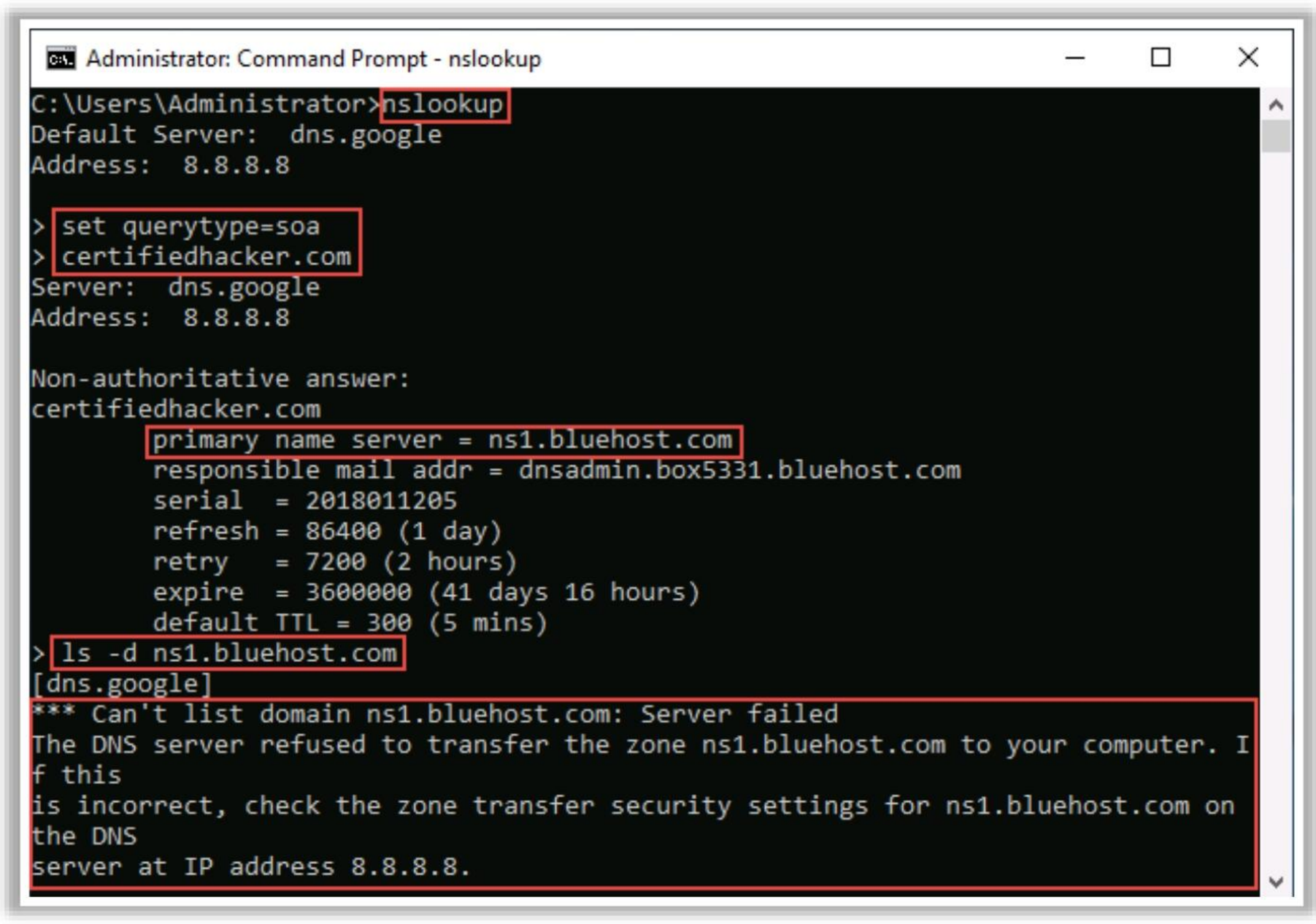


Figure 4.34: Screenshot of Windows DNS zone transfer using the nslookup command

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

https://t.me/learningnets

- **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.

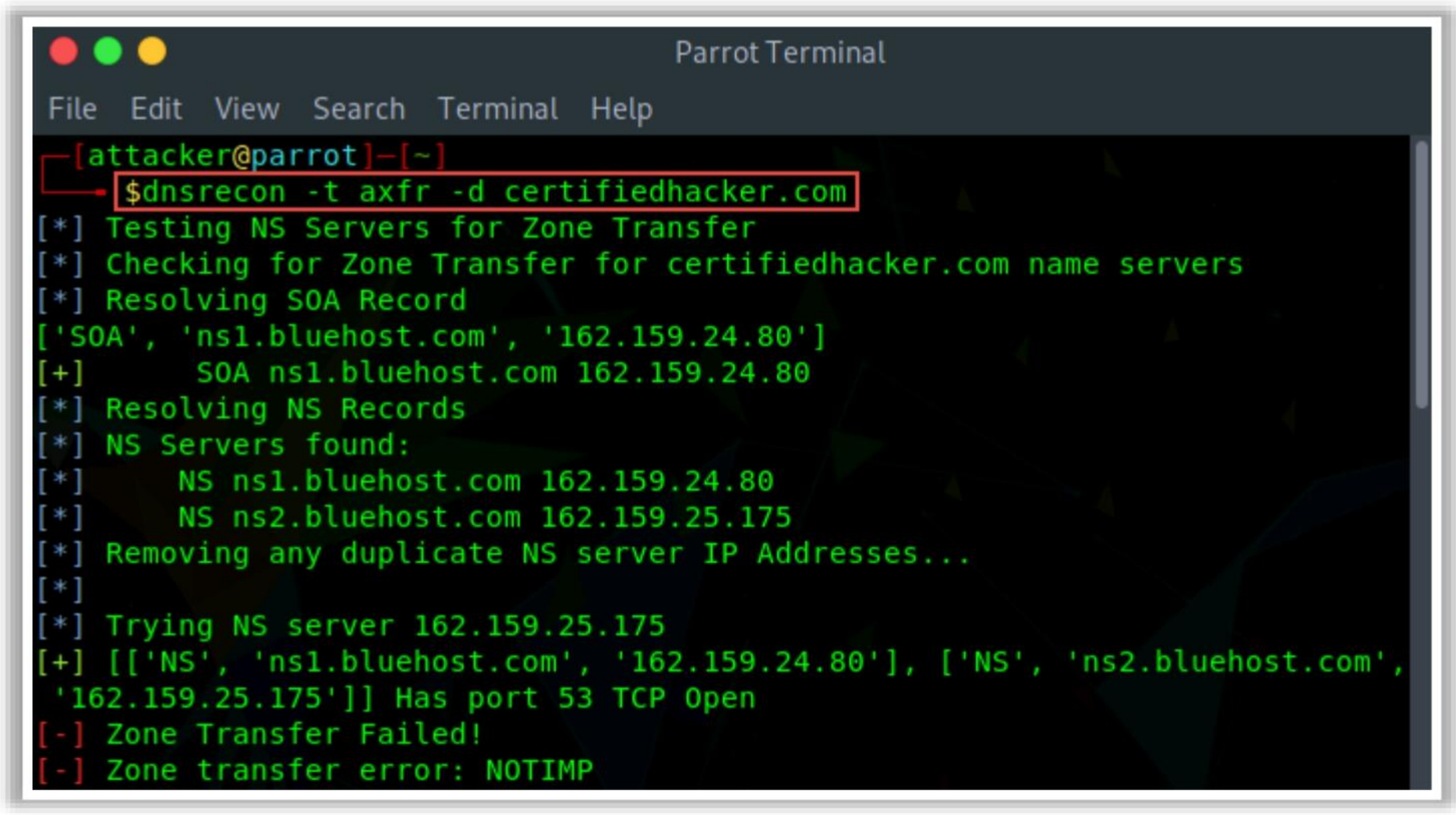
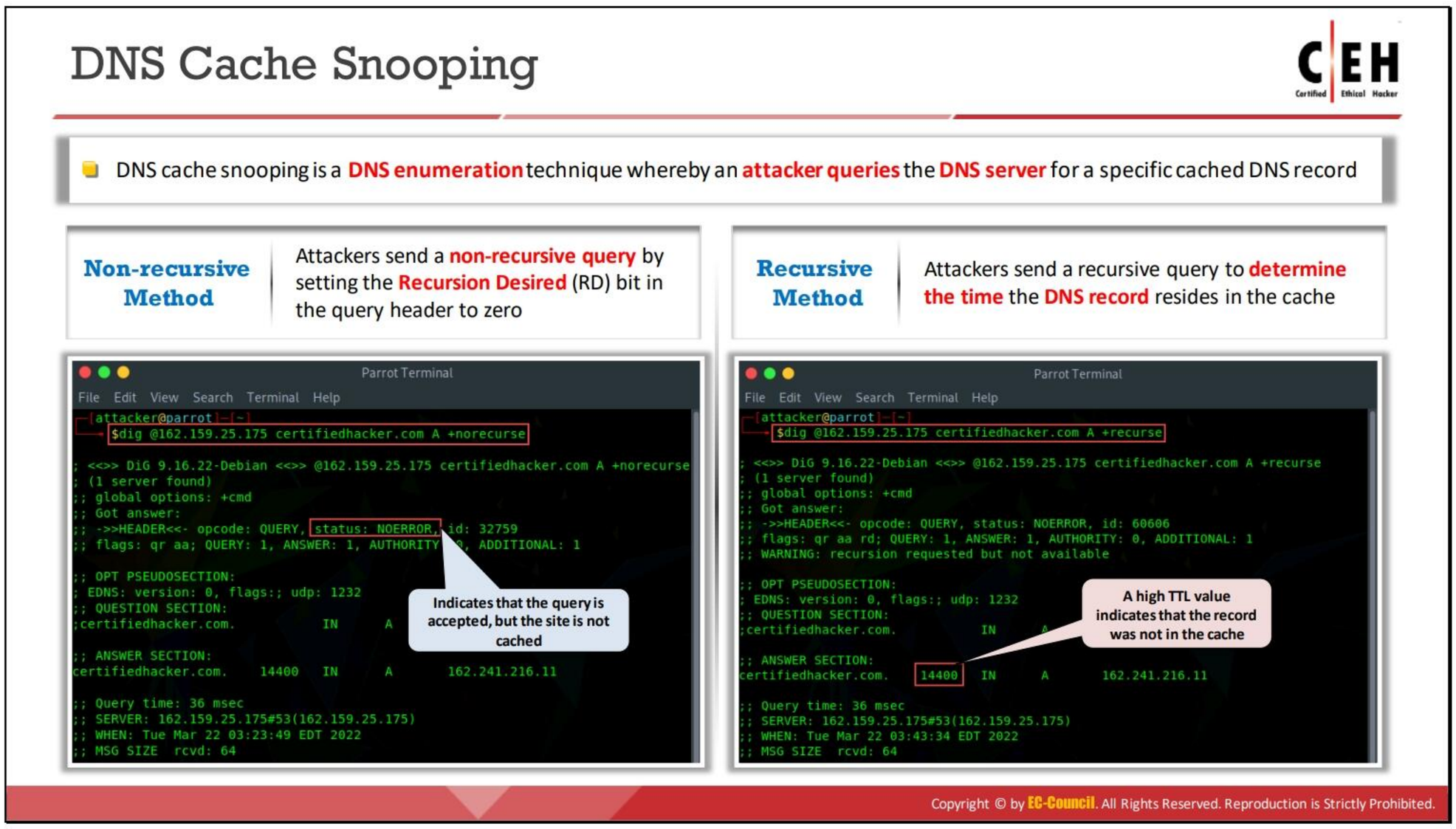


Figure 4.35: Screenshot of DNS zone transfer using DNSRecon

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

https://t.me/learningnets



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`

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

https://t.me/learningnets

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.

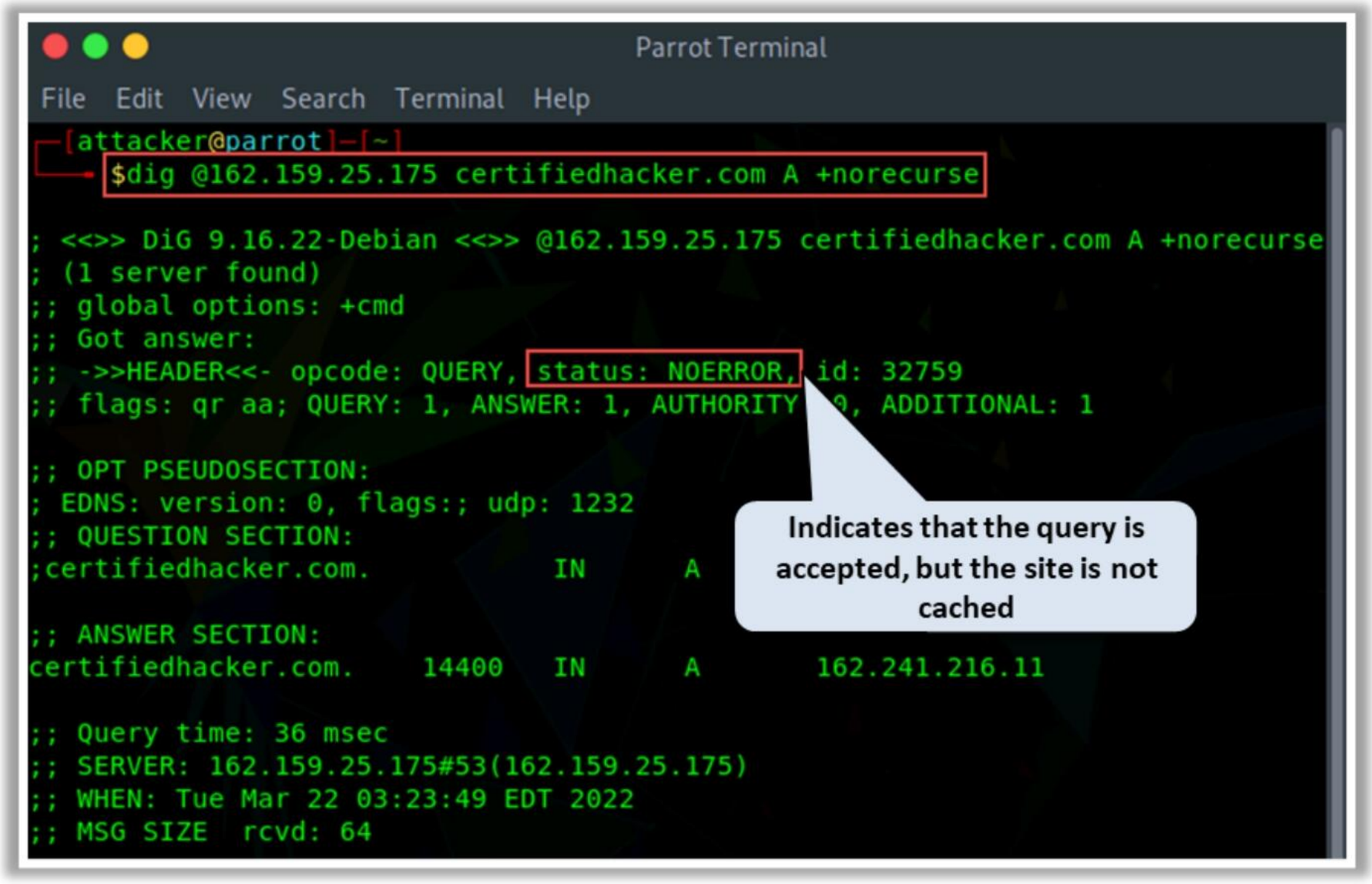


Figure 4.36: Screenshot of a dig query for a site that is not cached

- **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.

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

https://t.me/learningnets

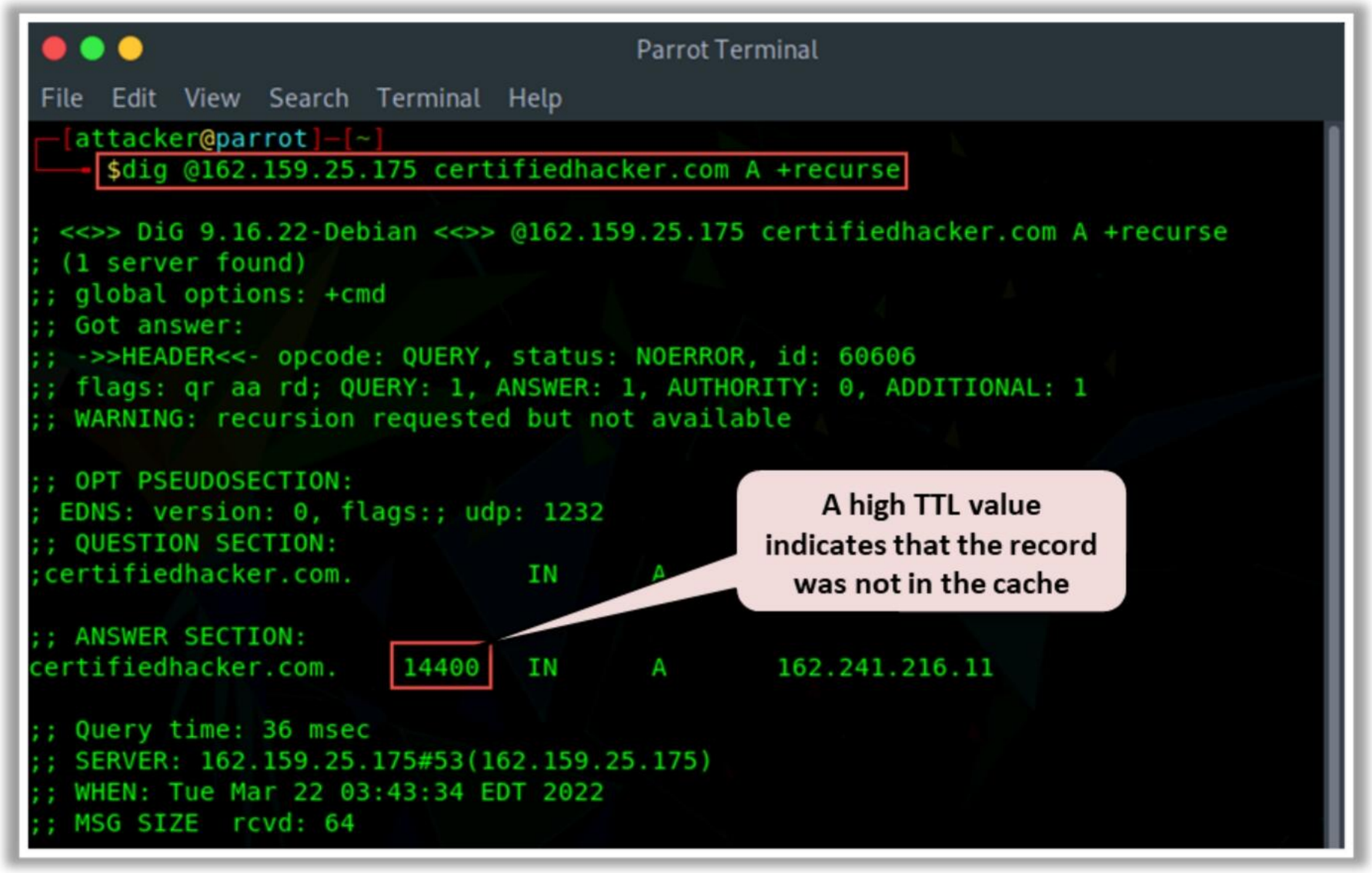
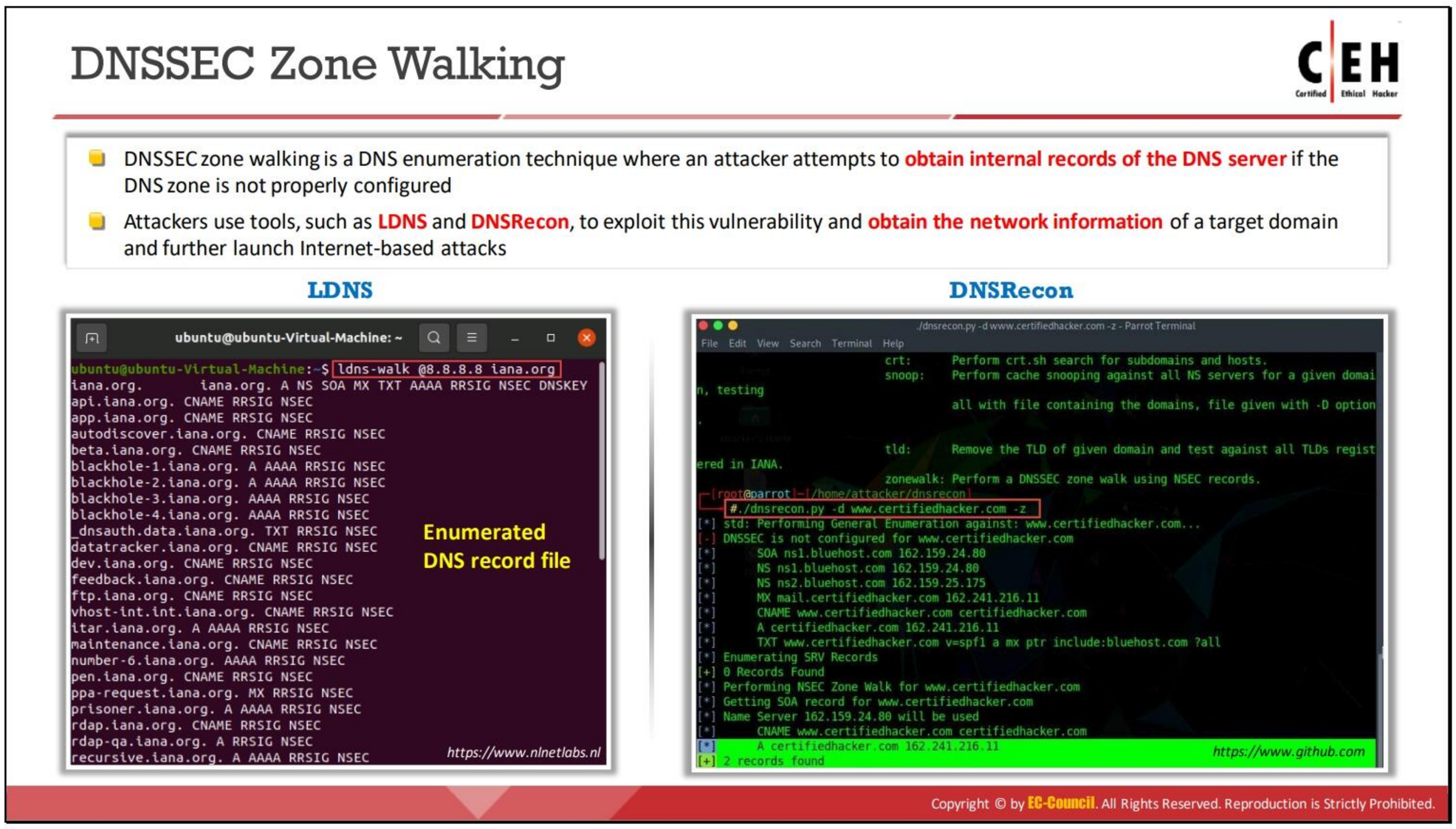


Figure 4.37: Screenshot of a dig query for a cached site

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

https://t.me/learningnets



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.

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

https://t.me/learningnets

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>`

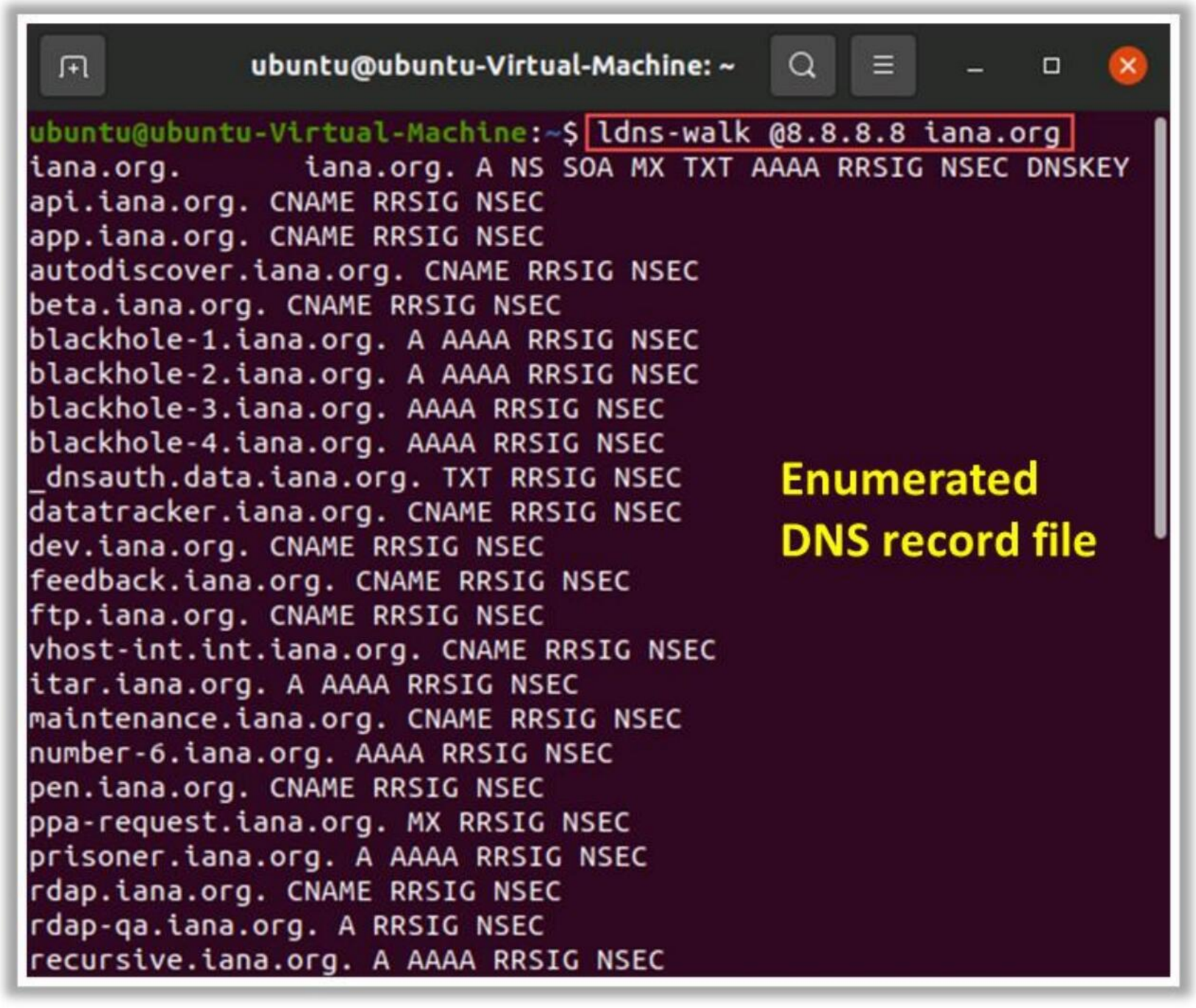


Figure 4.38: Screenshot of LDNS displaying results on the target domain

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

https://t.me/learningnets

- **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`

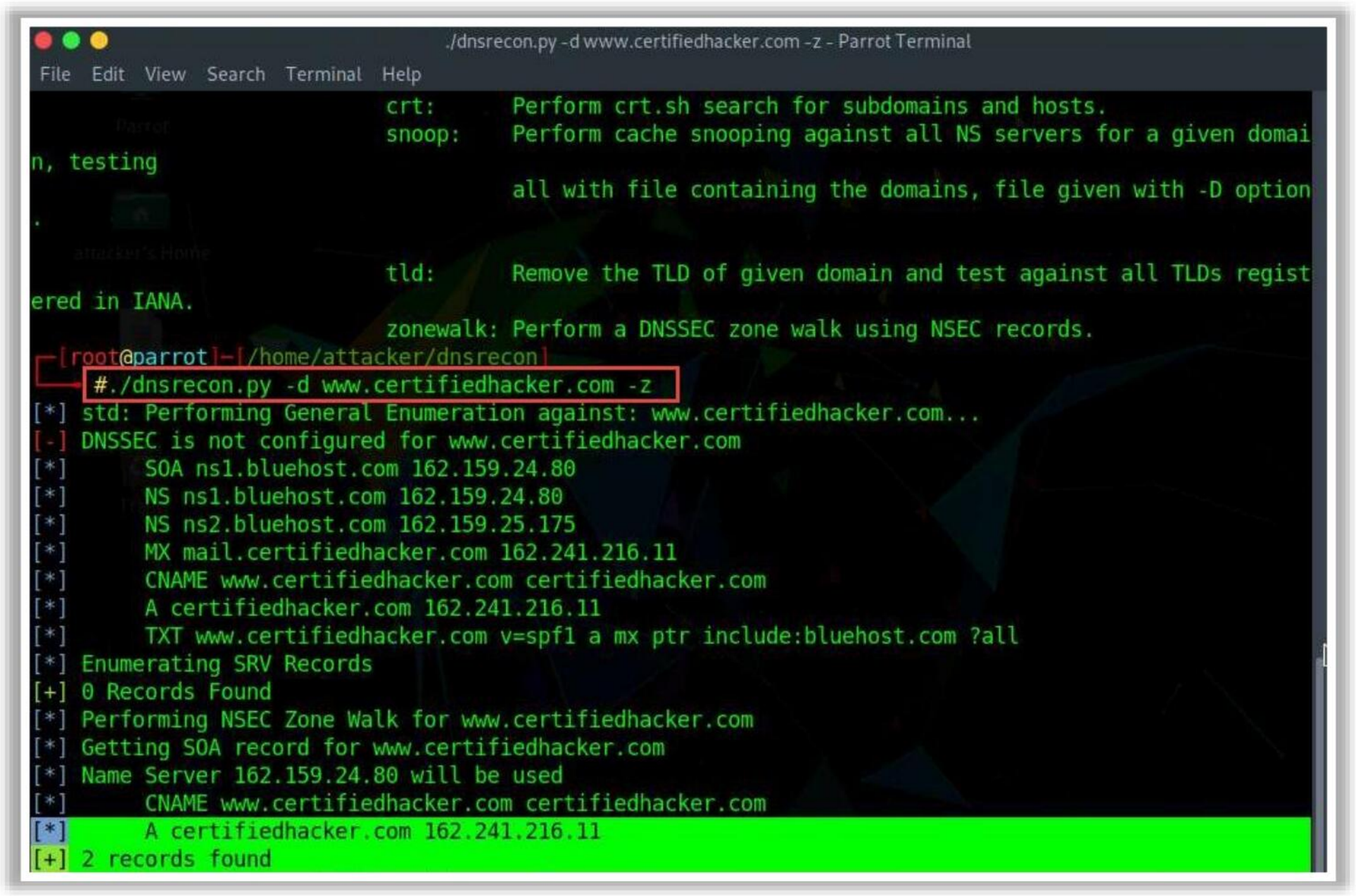
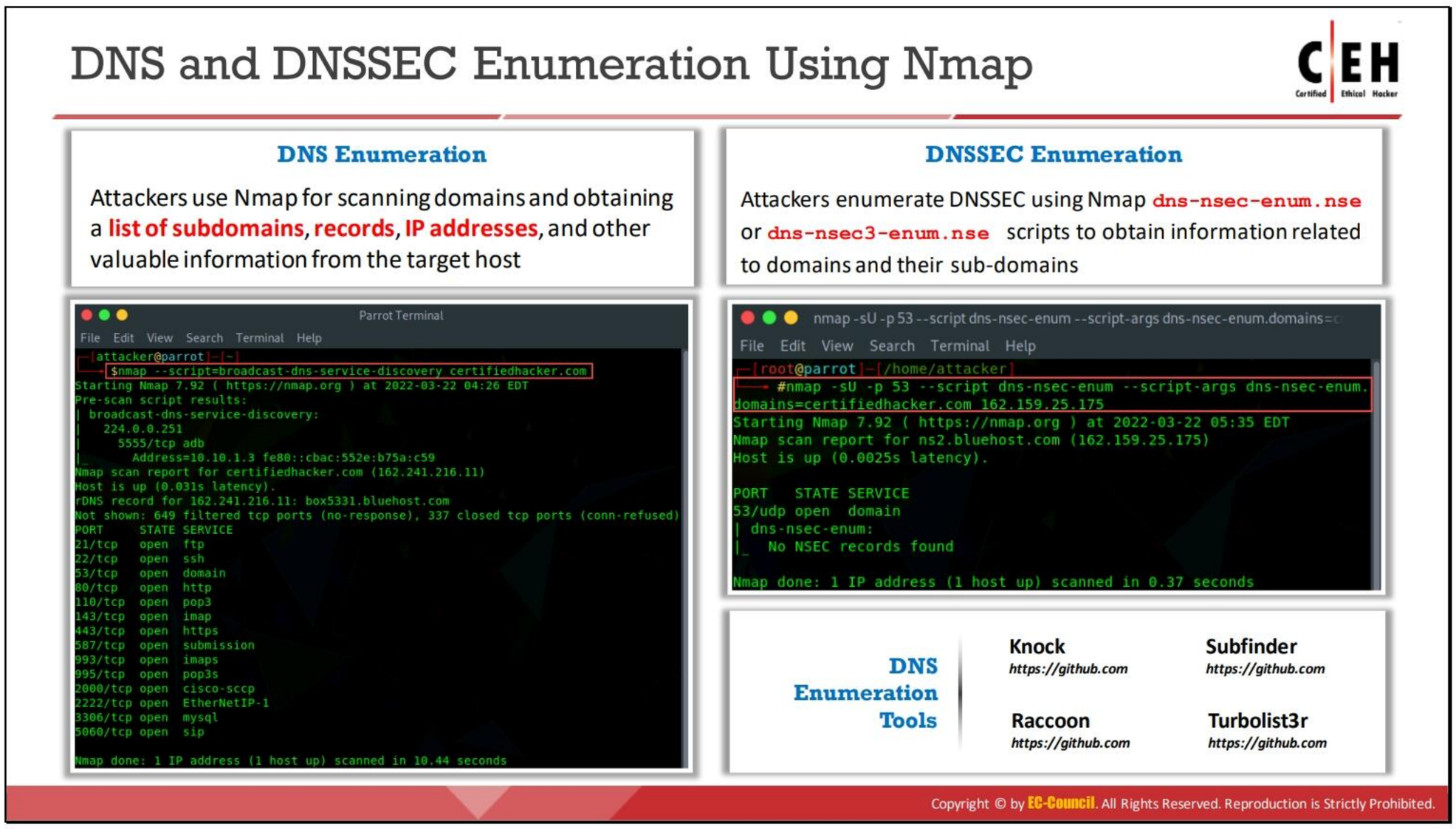


Figure 4.39: Screenshot of DNSRecon displaying results on the target domain

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

https://t.me/learningnets



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.

https://t.me/learningnets

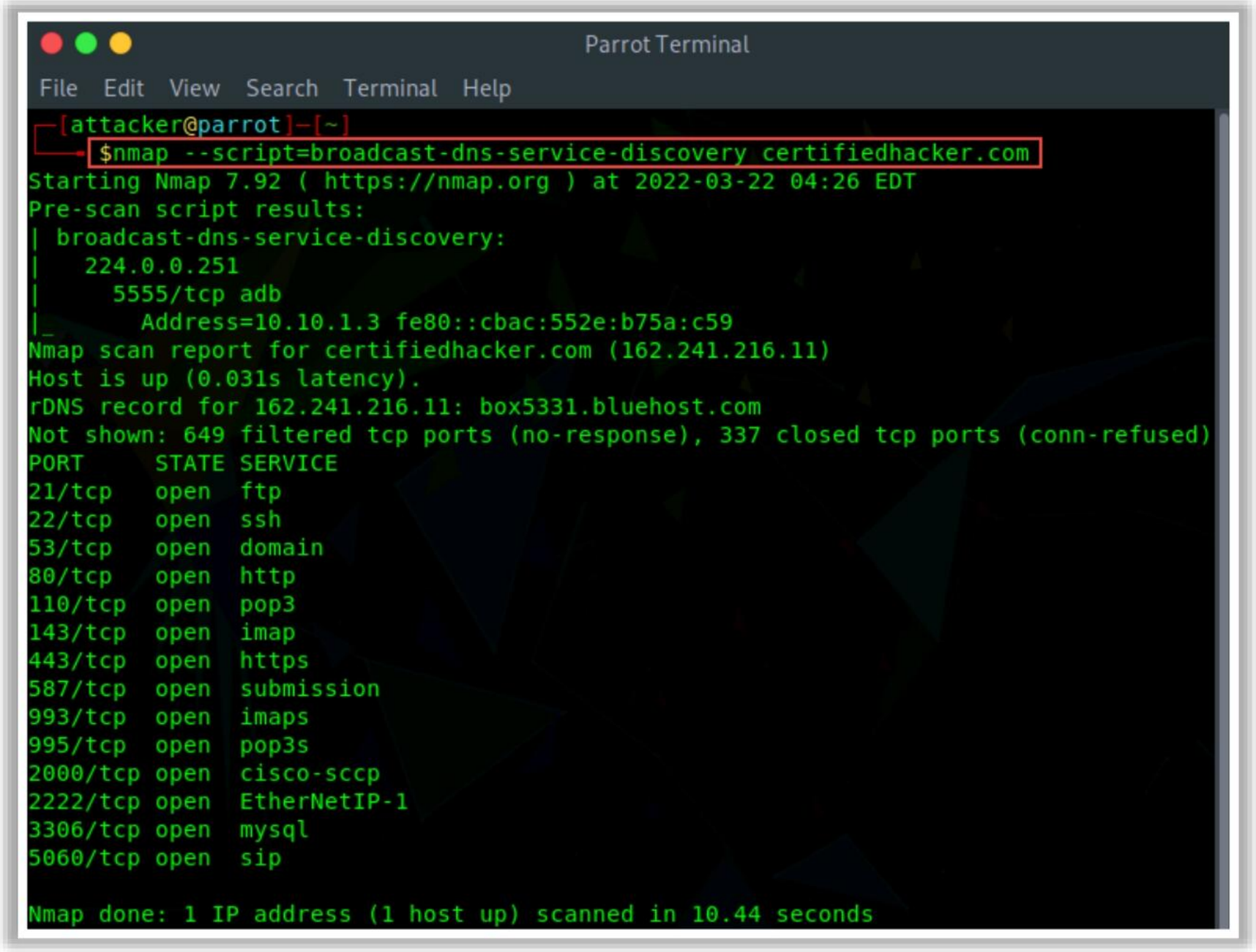


Figure 4.40: Screenshot of Nmap DNS service discovery

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

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

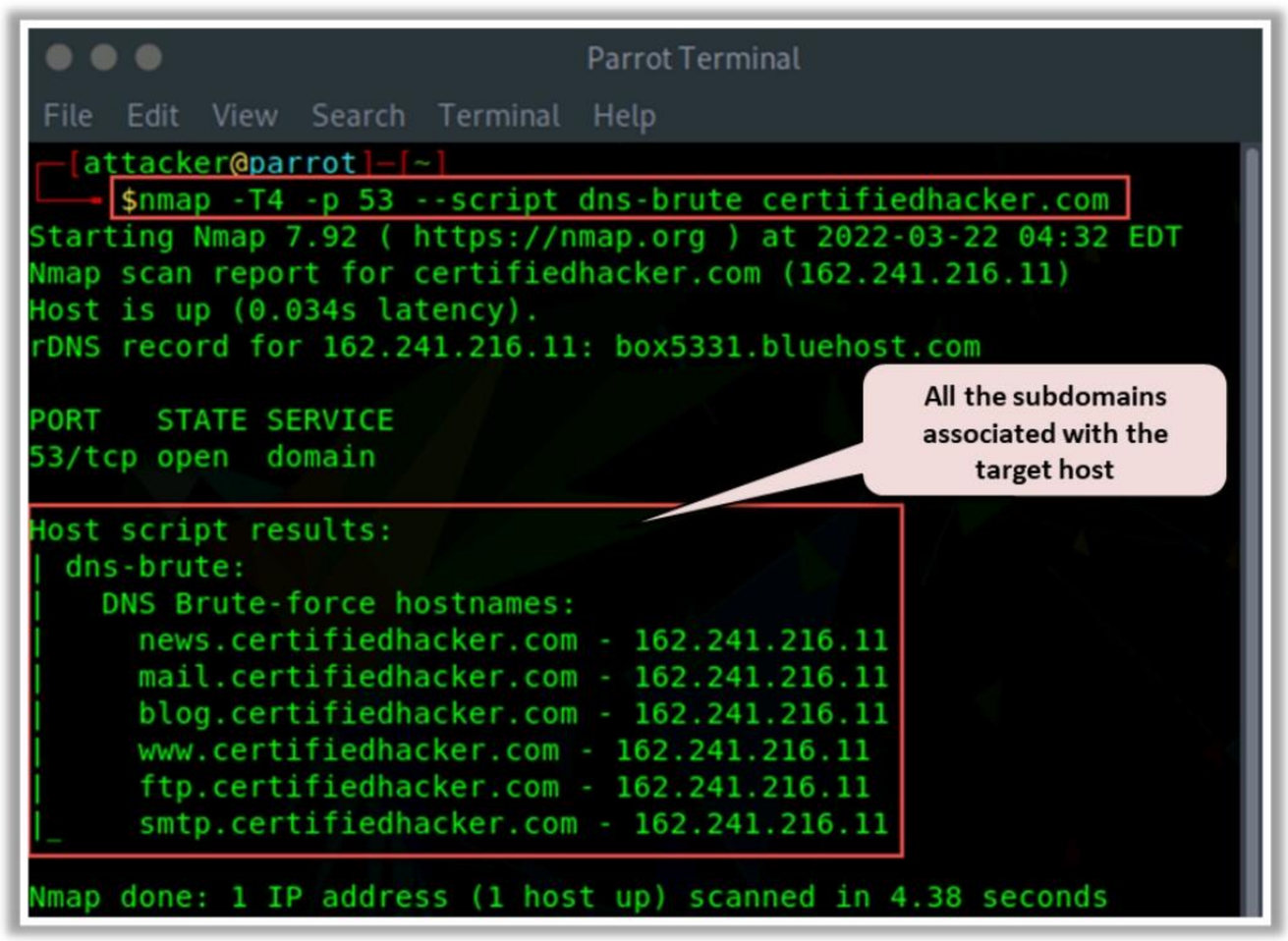


Figure 4.41: Screenshot of the dns-brute NSE script

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

https://t.me/learningnets

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>
```

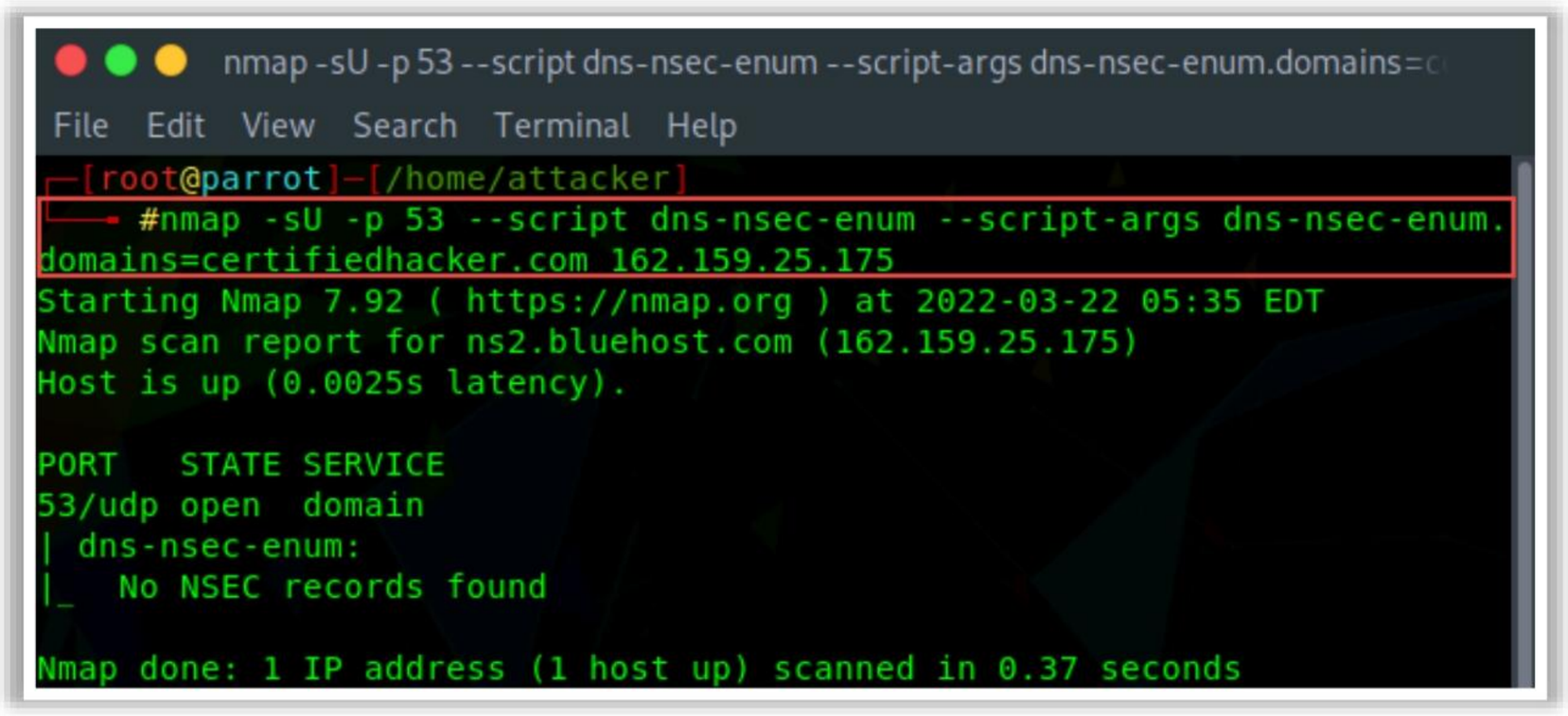


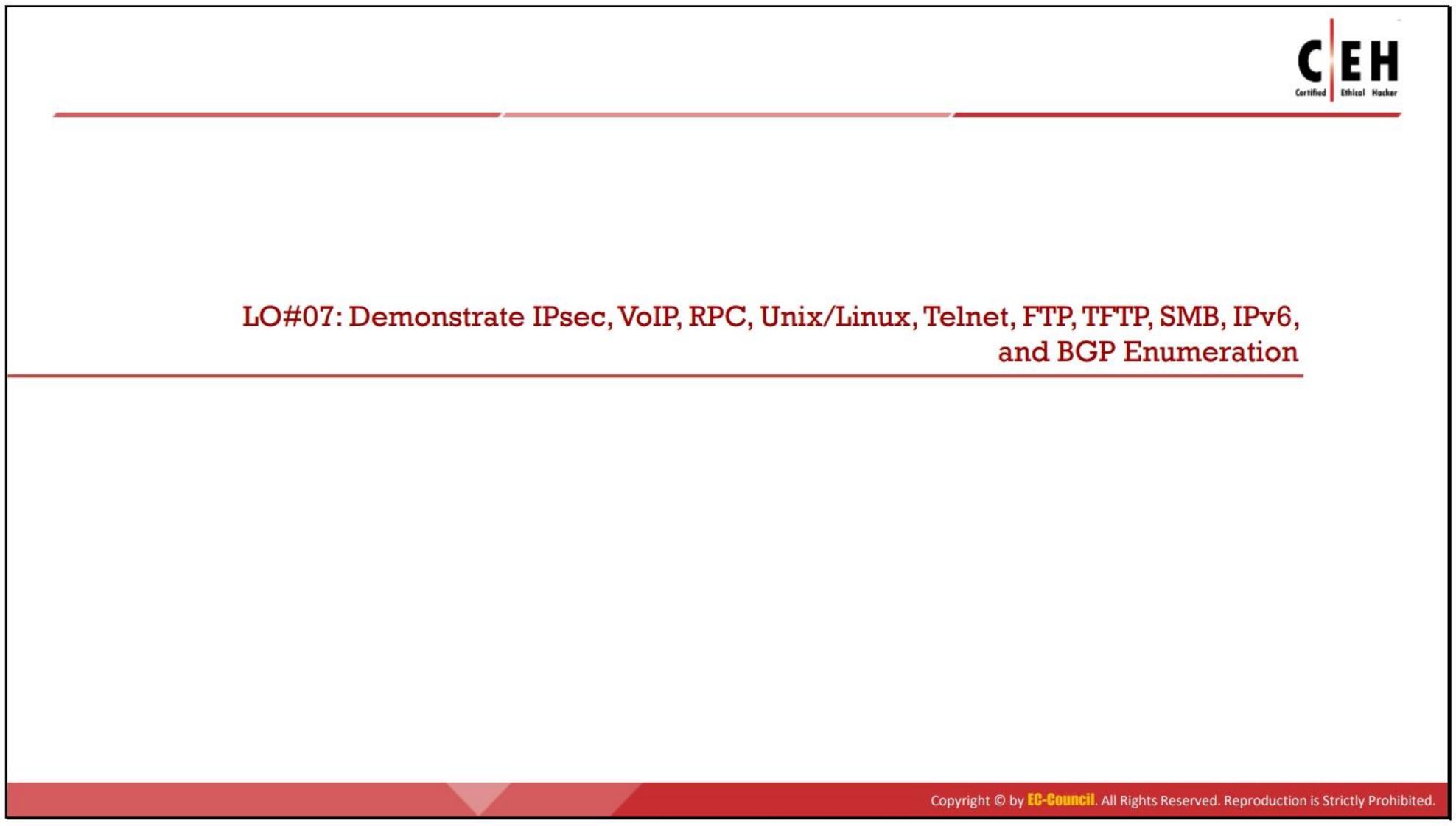
Figure 4.42: Screenshot of Nmap dns-nsec-enum NSE script

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.

https://t.me/learningnets

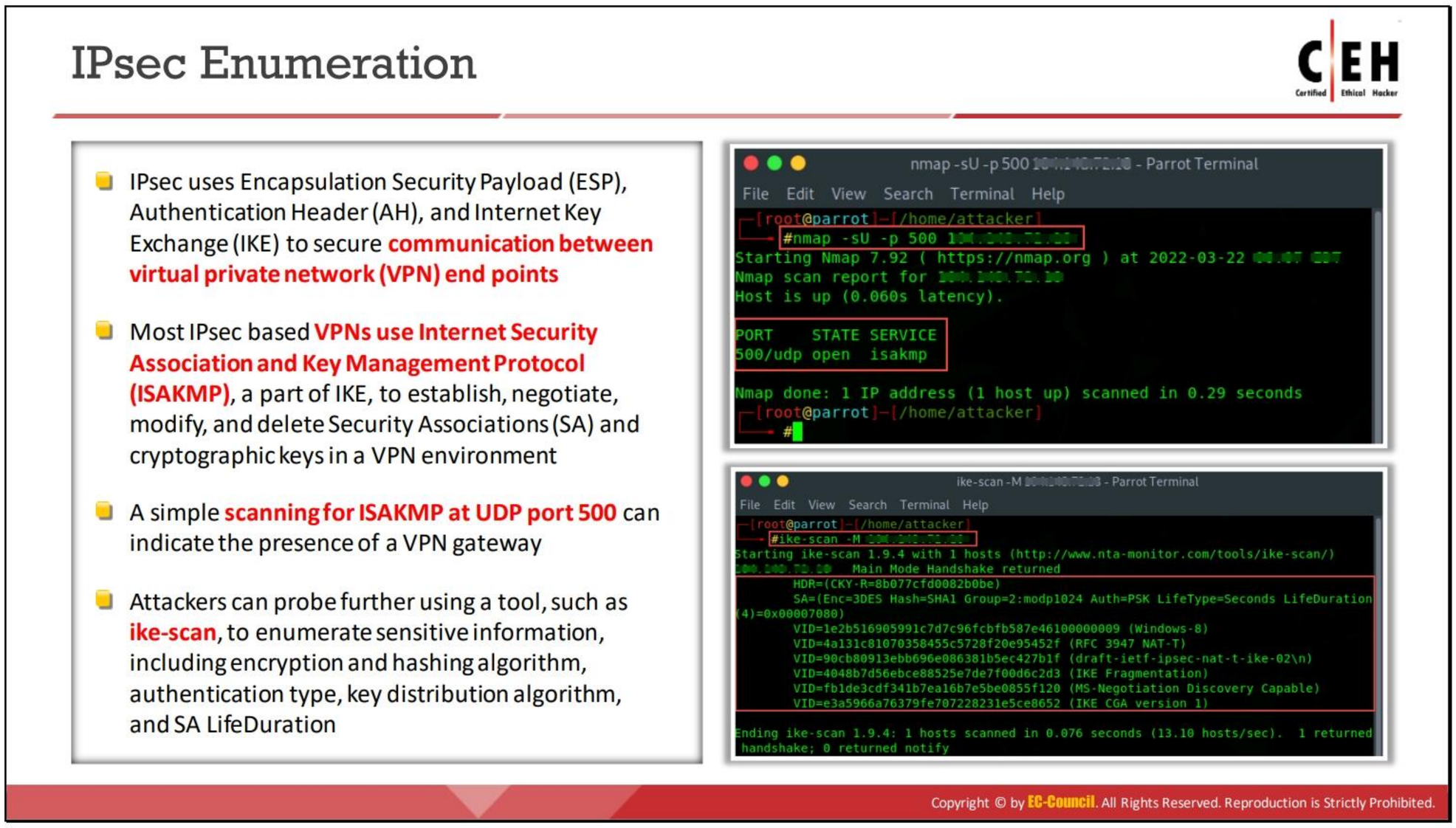


Other Enumeration Techniques

This section discusses IPsec, VoIP, RPC, Unix/Linux user, Telnet, SSH user, FTP, TFTP, SMB, IPv6, and BGP enumeration.

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

https://t.me/learningnets



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.

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

https://t.me/learningnets

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>
```

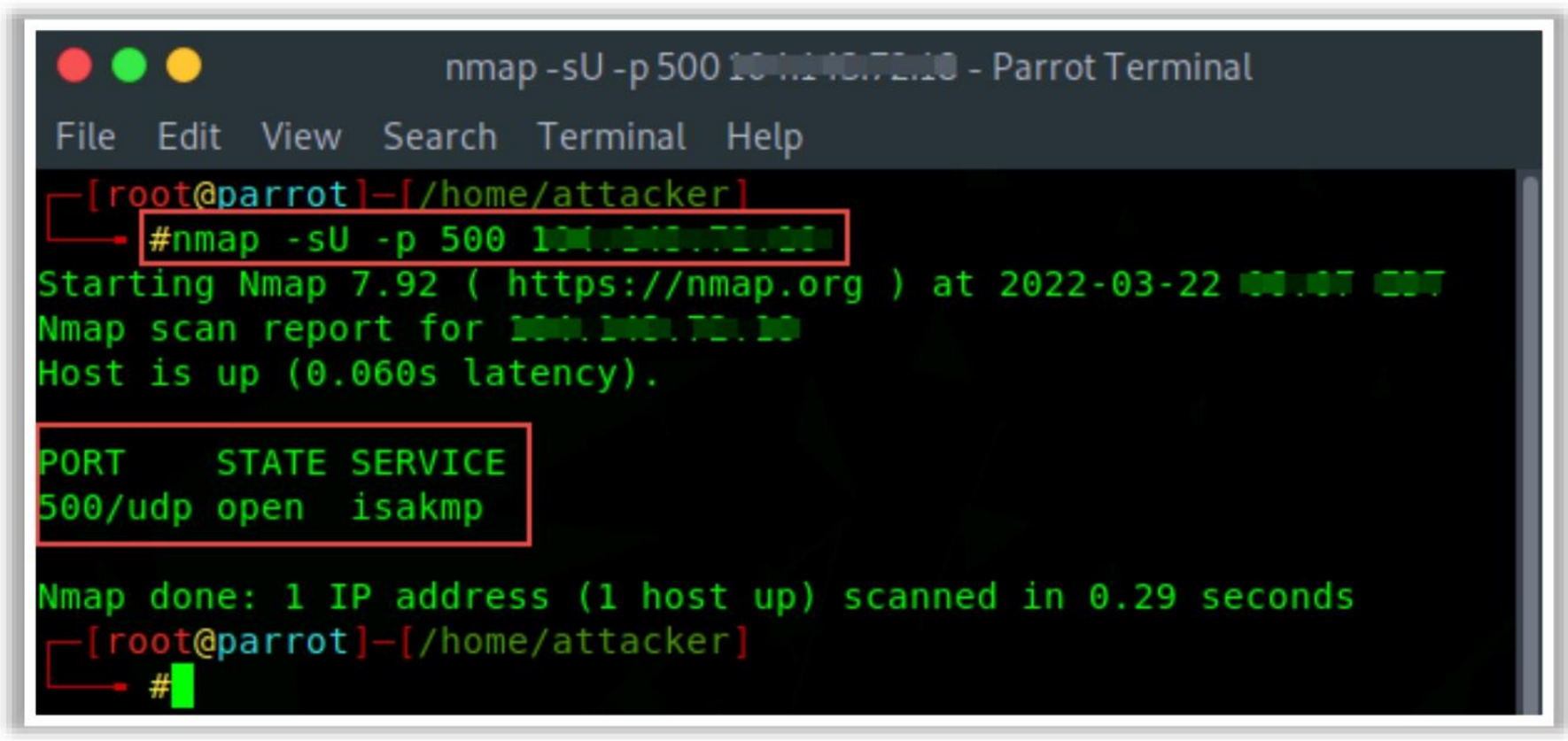


Figure 4.43: Screenshot displaying an Nmap scan over port 500 for ISAKMP

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>
```

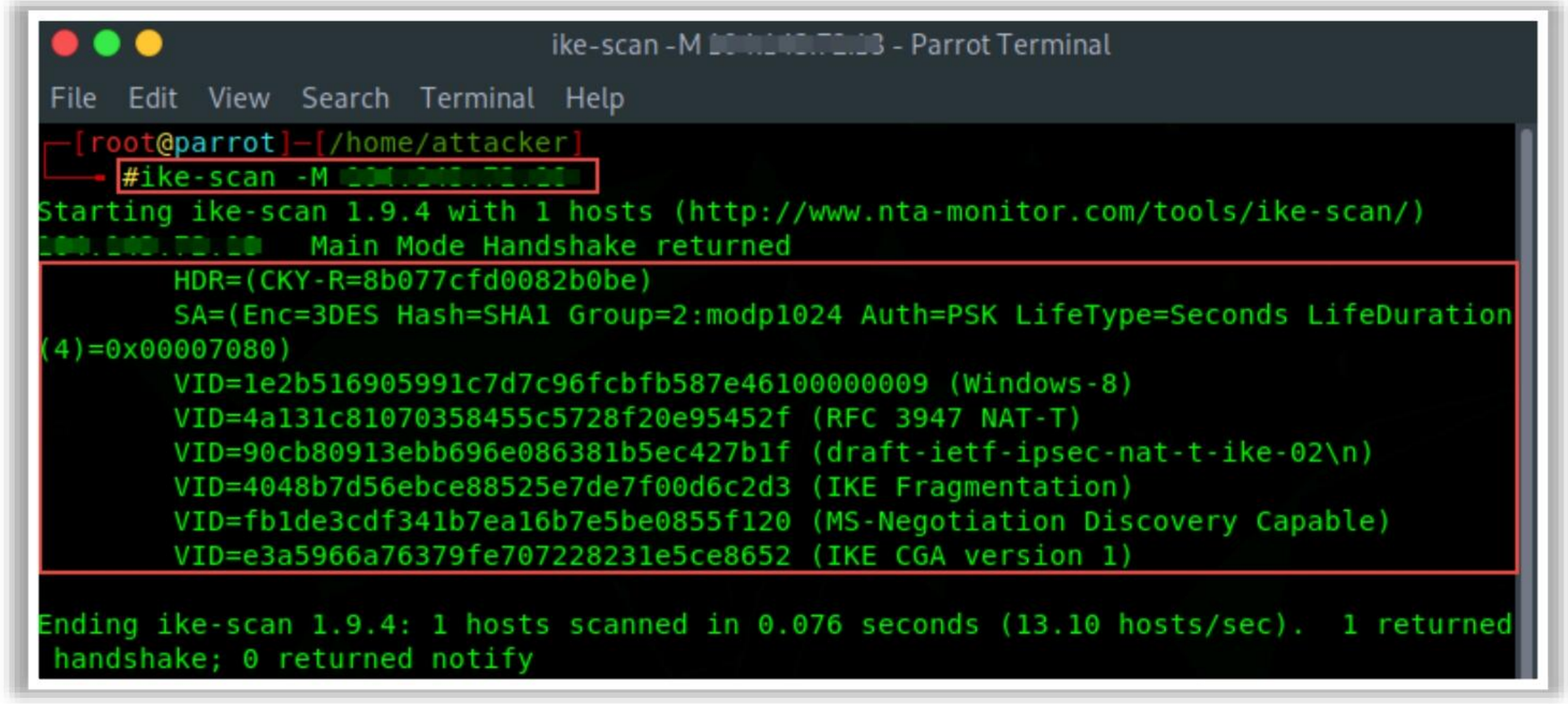


Figure 4.44: Screenshot displaying ike-scan enumeration

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

https://t.me/learningnets

ike-scan

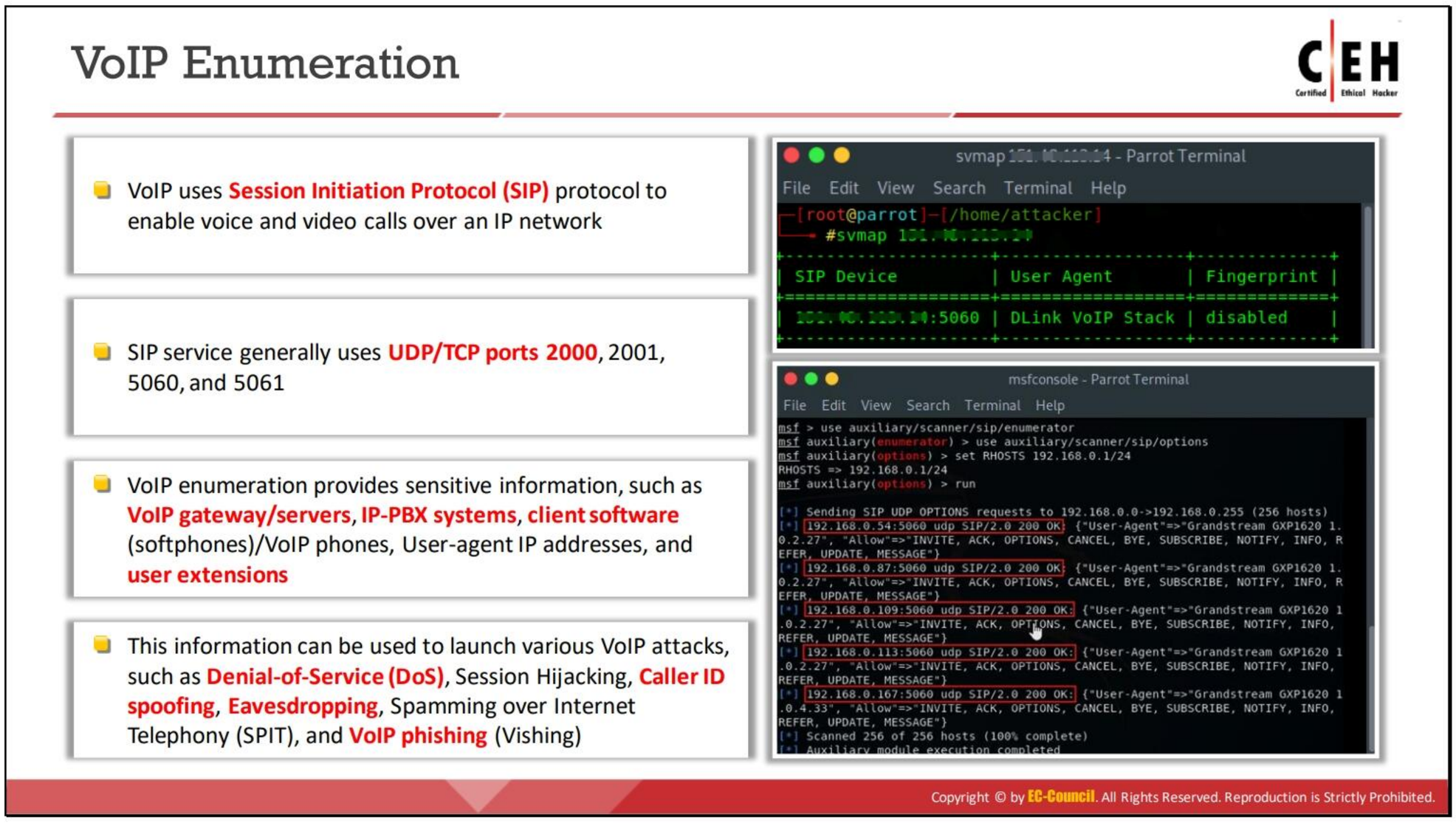
Source: *https://github.com*

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.
- **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.

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

https://t.me/learningnets



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

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

https://t.me/learningnets

- 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>

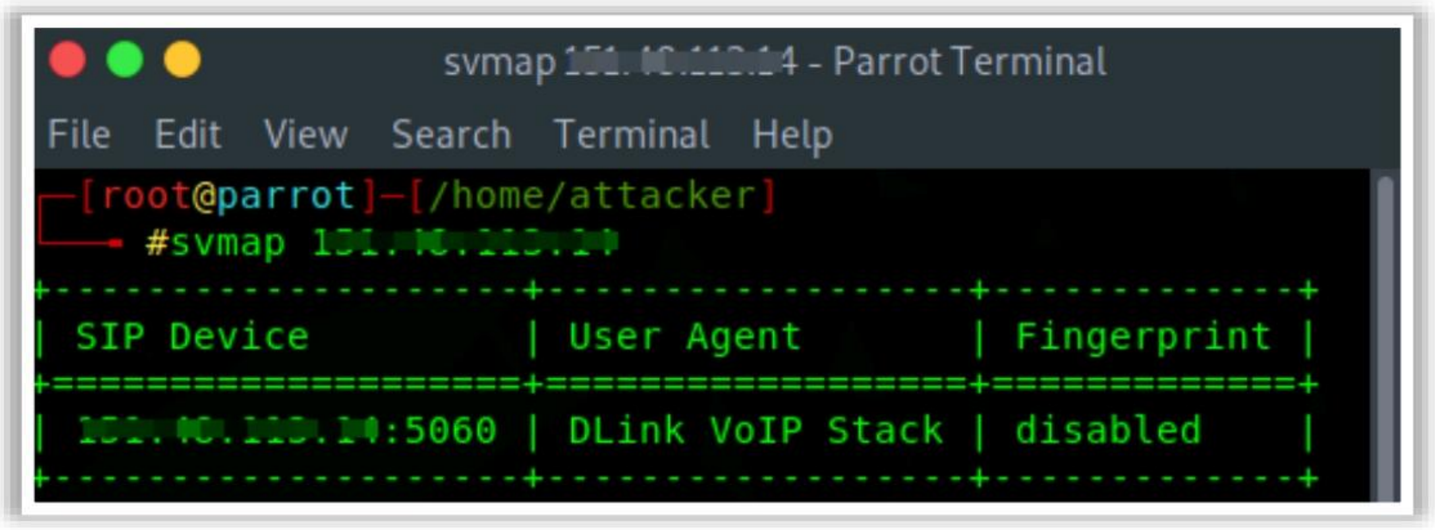


Figure 4.45: Screenshot displaying Svmap scan for enumerating SIP details

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.

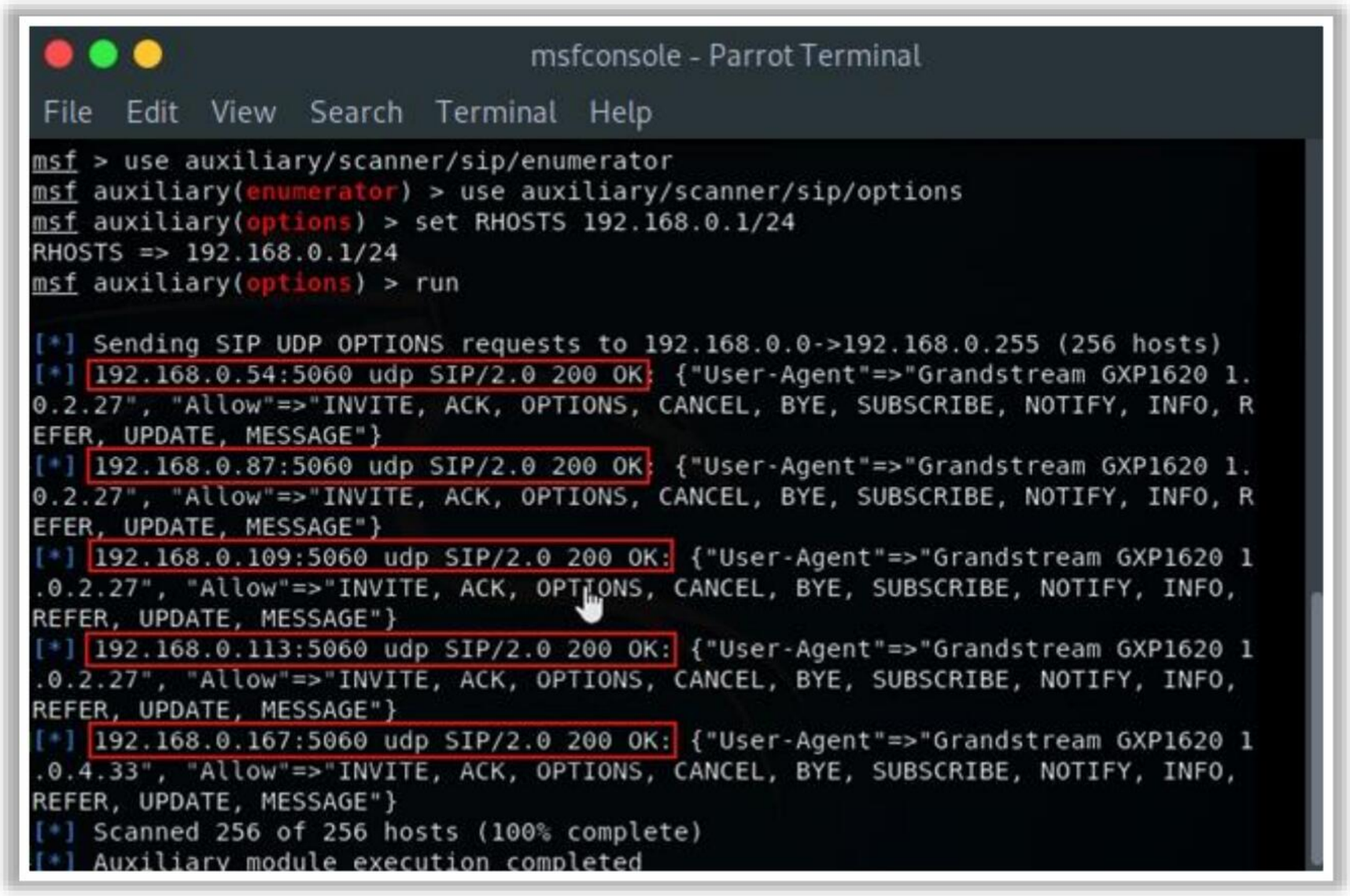
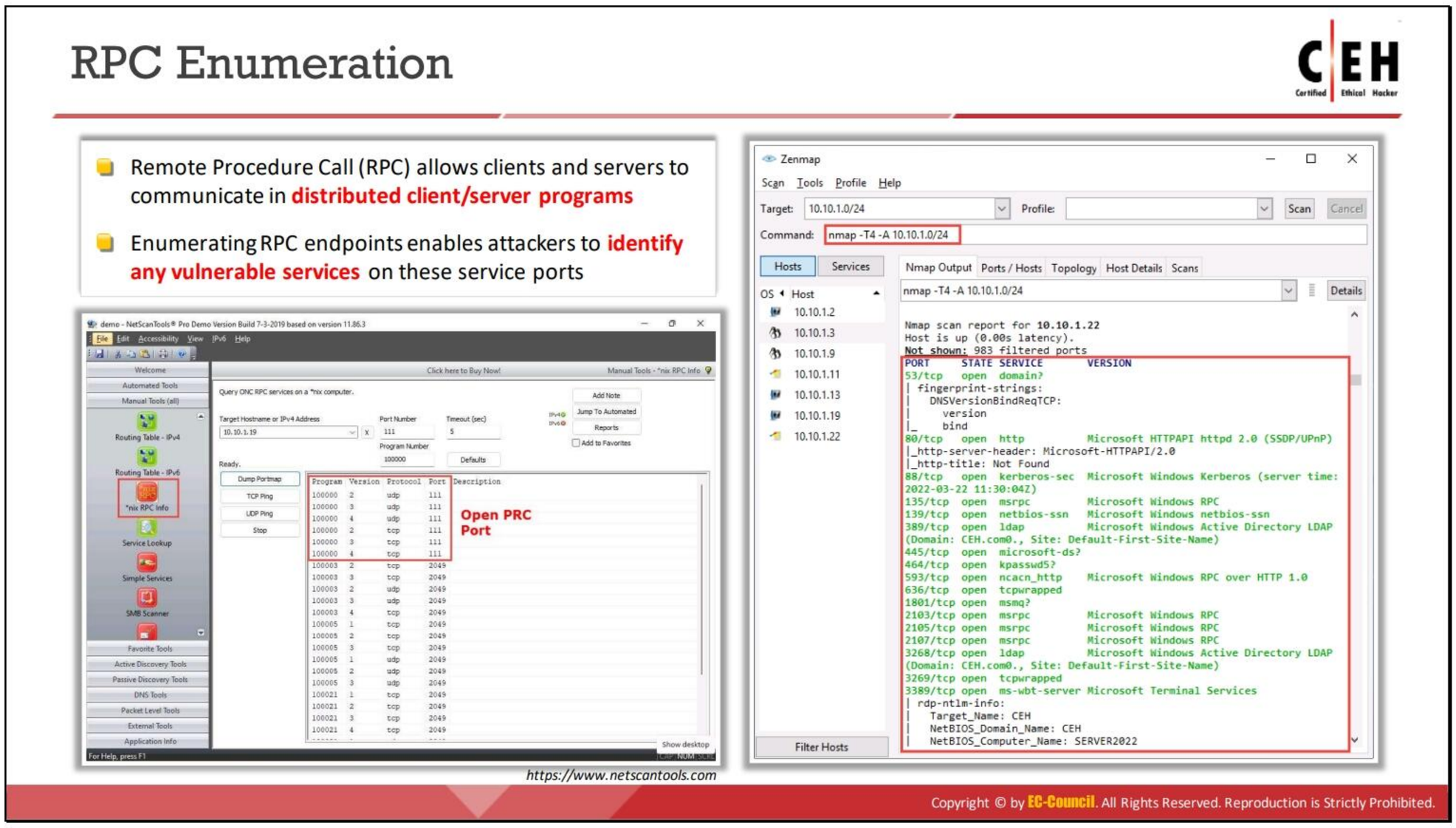


Figure 4.46: Screenshot displaying Metasploit exploit for SIP enumeration

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

https://t.me/learningnets



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.

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

https://t.me/learningnets

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>
```

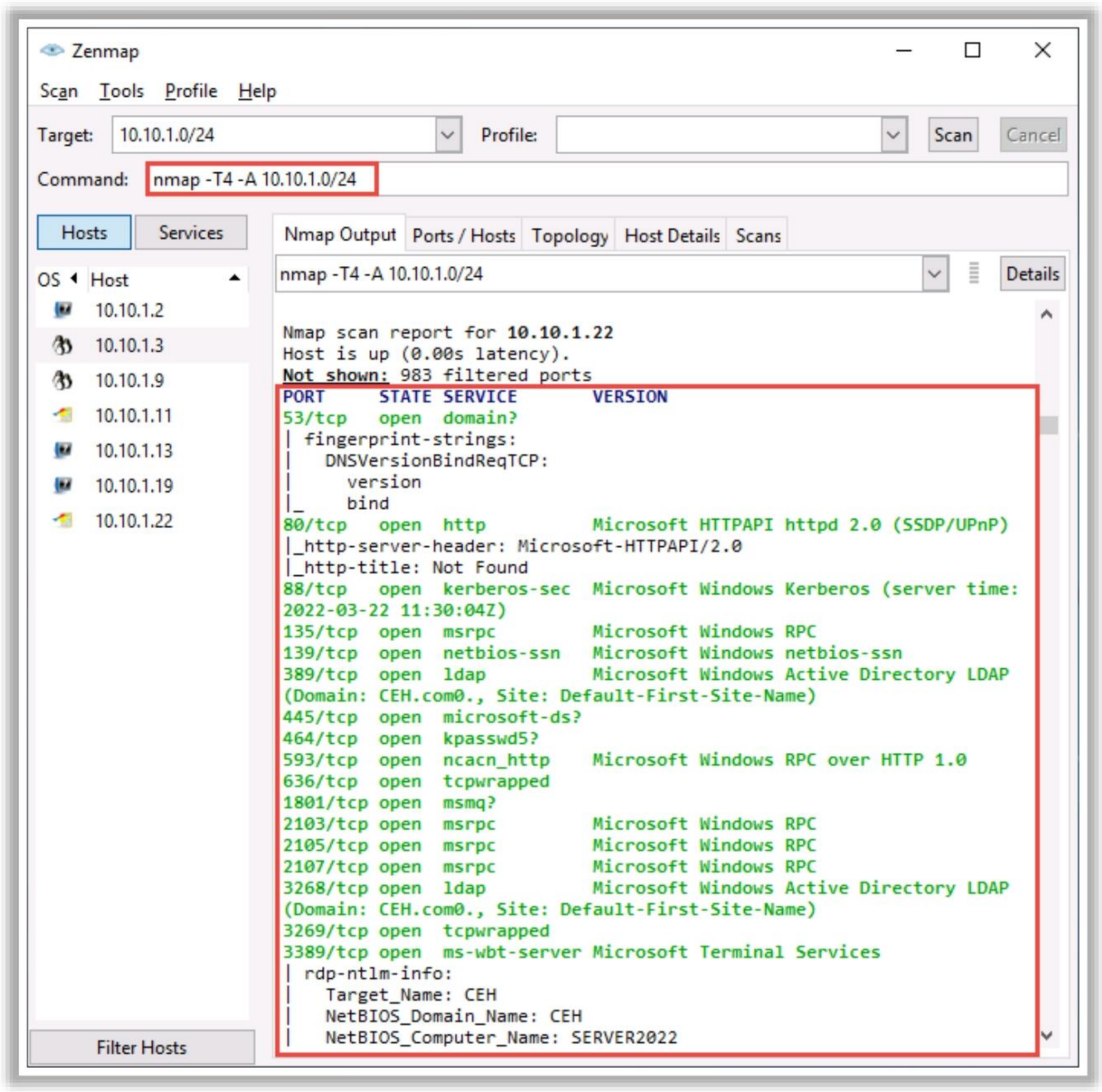


Figure 4.47: Screenshot displaying an Nmap scan result for RPC enumeration

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

https://t.me/learningnets

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.

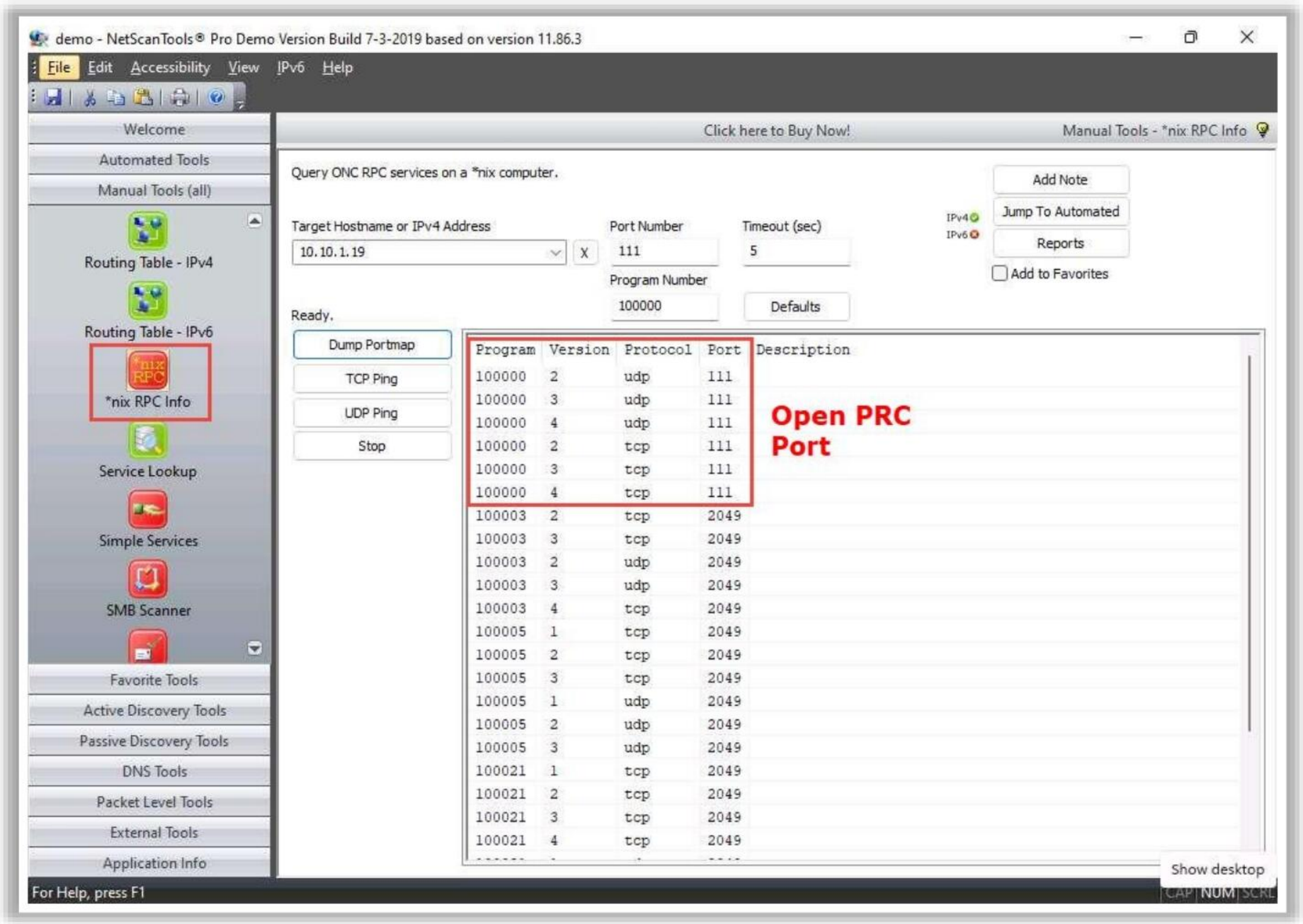
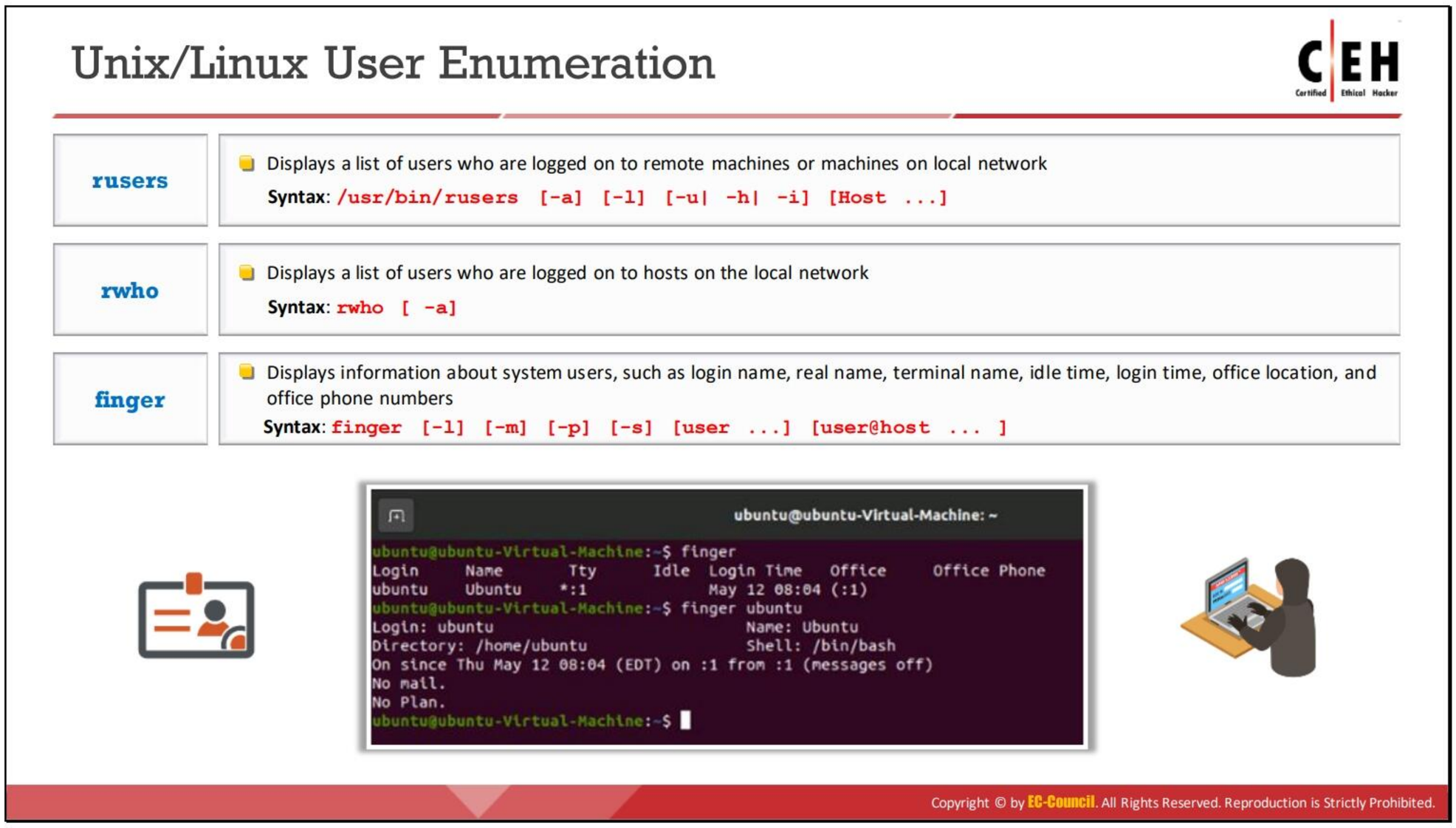


Figure 4.48: Screenshot displaying NetScanTools Pro tool for RPC enumeration

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

https://t.me/learningnets



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

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

https://t.me/learningnets

- **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.

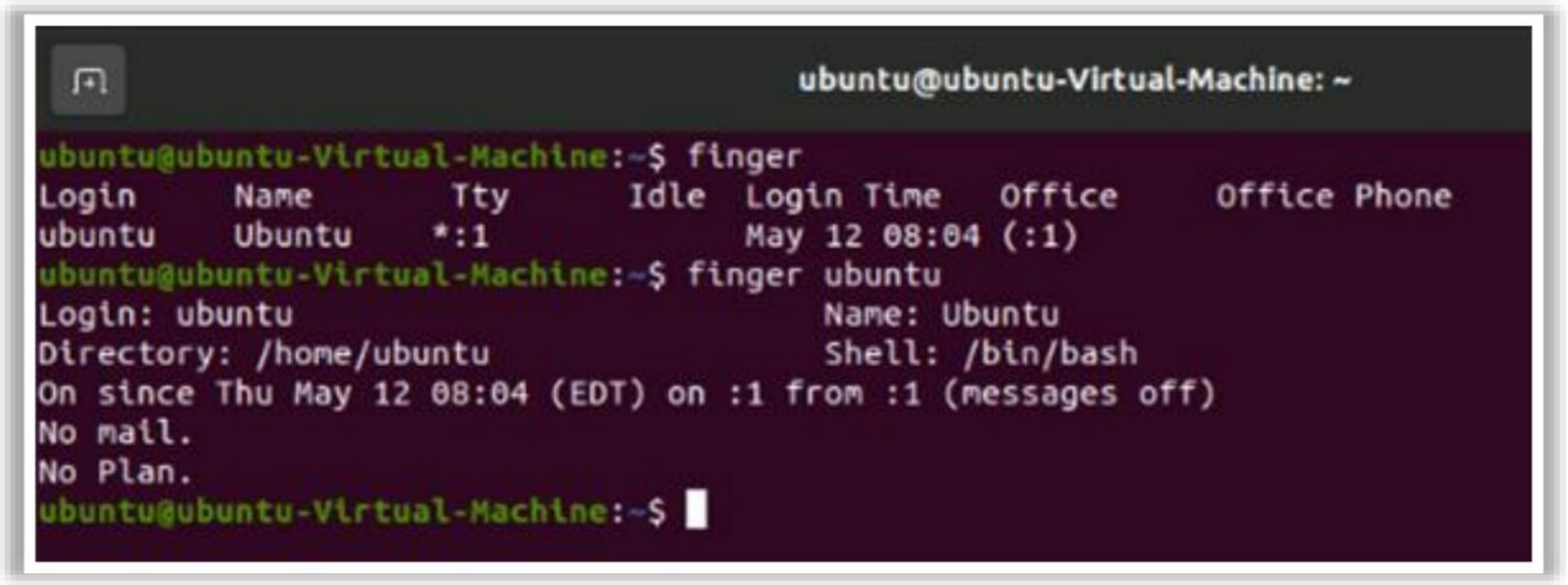
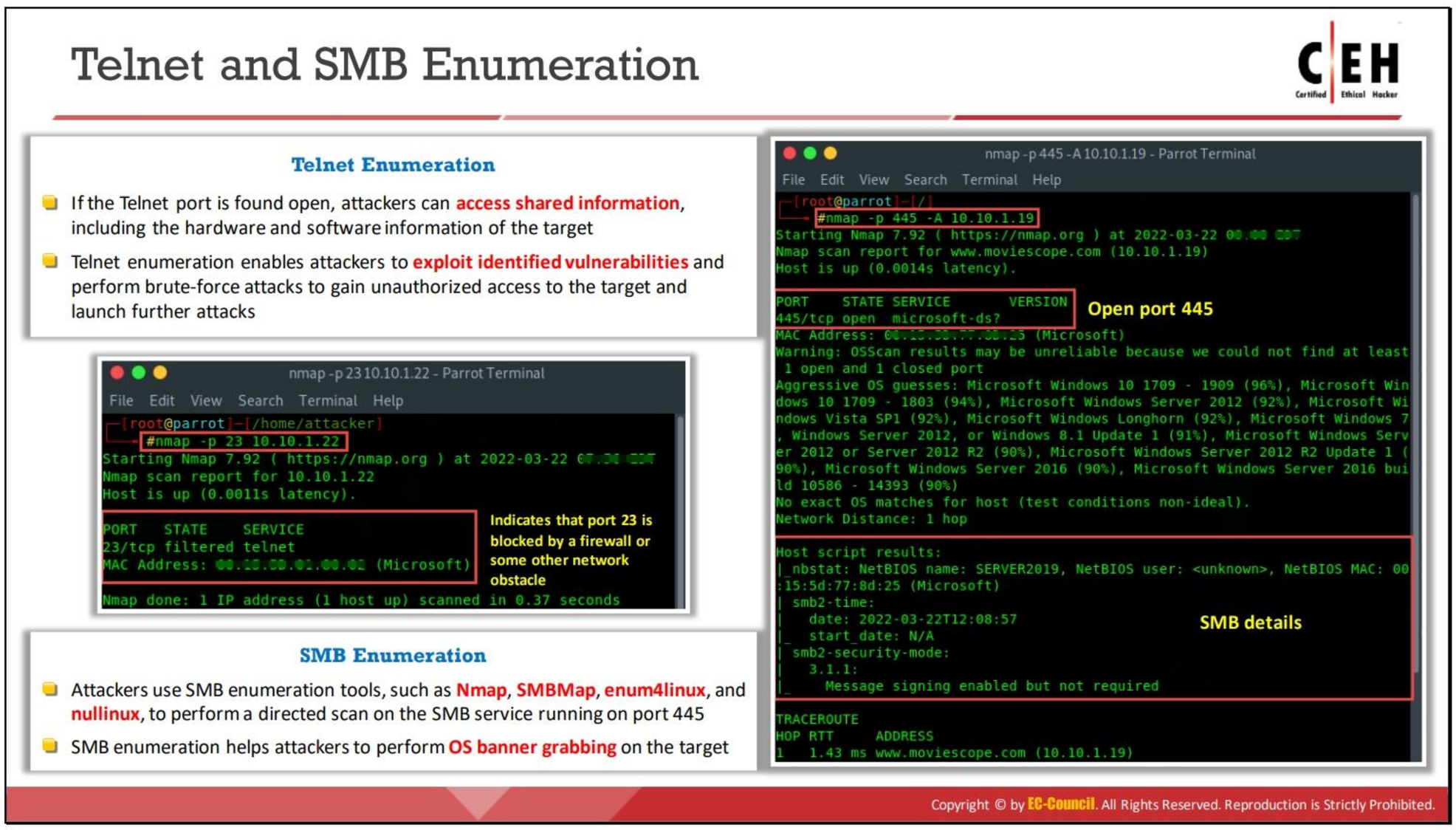


Figure 4.49: Screenshot displaying the execution of the finger command for user enumeration

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

https://t.me/learningnets



Telnet Enumeration

Telnet is a network terminal protocol that allows users to access remote computers or servers over the Internet. This protocol provides two-way interactive communication for computers on LANs and the Internet. Depending on the privileges assigned to the users, they can use Telnet to log in to the remote system to access specific files, services, data, etc.

Attackers perform port scanning to gather information regarding open ports and services on the target server. If the Telnet port is found to be open, attackers can learn about the information being shared, including hardware and software information of the target. By using this information, attackers can exploit their specific vulnerabilities and perform a brute-force attack to gain unauthorized access to the target system. Attackers can use the Nmap tool to perform simple direct scanning for Telnet port 23.

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

https://t.me/learningnets

As shown in the screenshot, the following Nmap command is used by attackers to enumerate the Telnet service running on the target system:

```
# nmap -p 23 <target domain/IP Address>
```

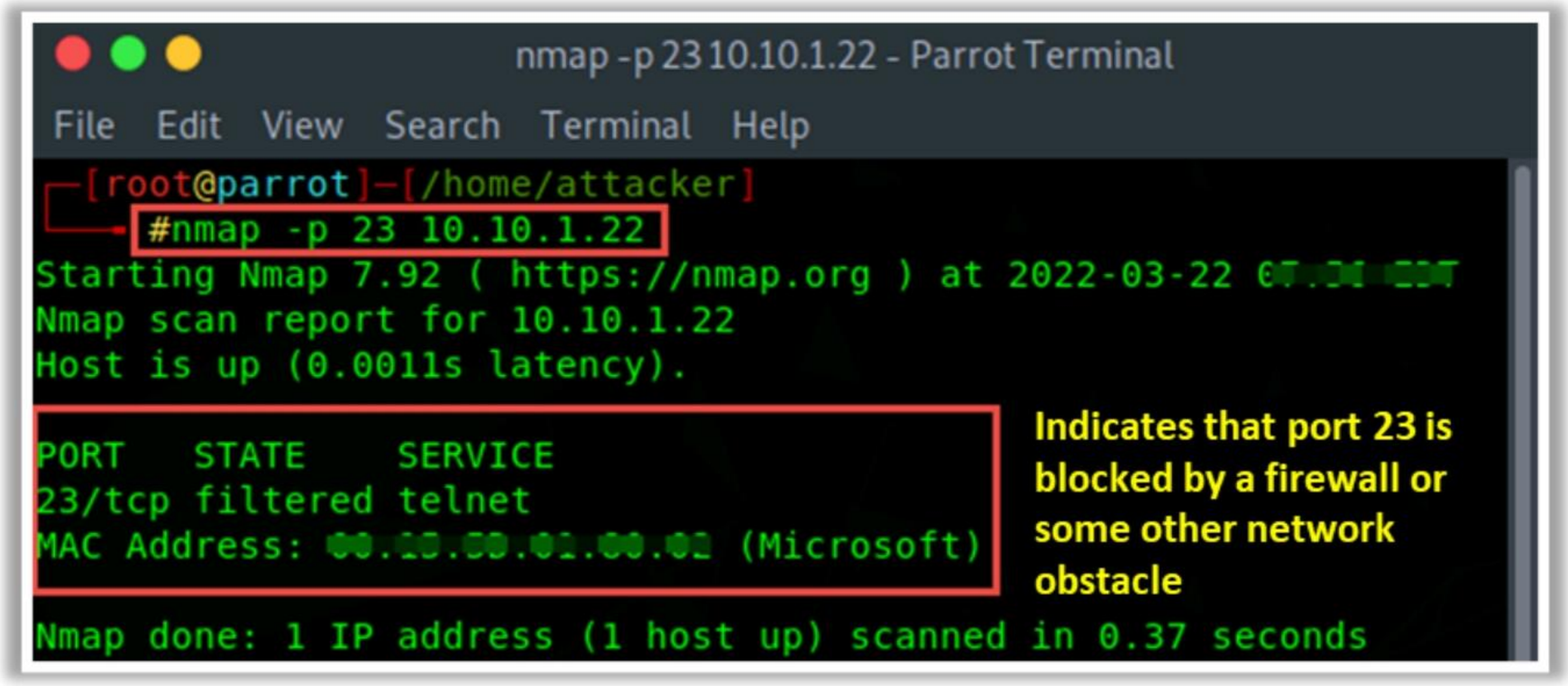


Figure 4.50: Screenshot of Nmap displaying a Telnet enumeration result

Attackers can further use the following script to enumerate information from remote Microsoft Telnet services with New Technology LAN Manager (NTLM) authentication enabled:

```
# nmap -p 23 --script telnet-ntlm-info <target IP>
```

Once the information about the target server is obtained, the attackers can use the following script to perform a brute-force attack against the Telnet server:

```
# nmap -p 23 –script telnet-brute.nse –script-args
userdb=/root/Desktop/user.txt,passdb=/root/Desktop/pass.txt <target
IP>
```

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, and NetScanTool Pro to perform a directed scan on the SMB service running on port 445.

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

https://t.me/learningnets

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.

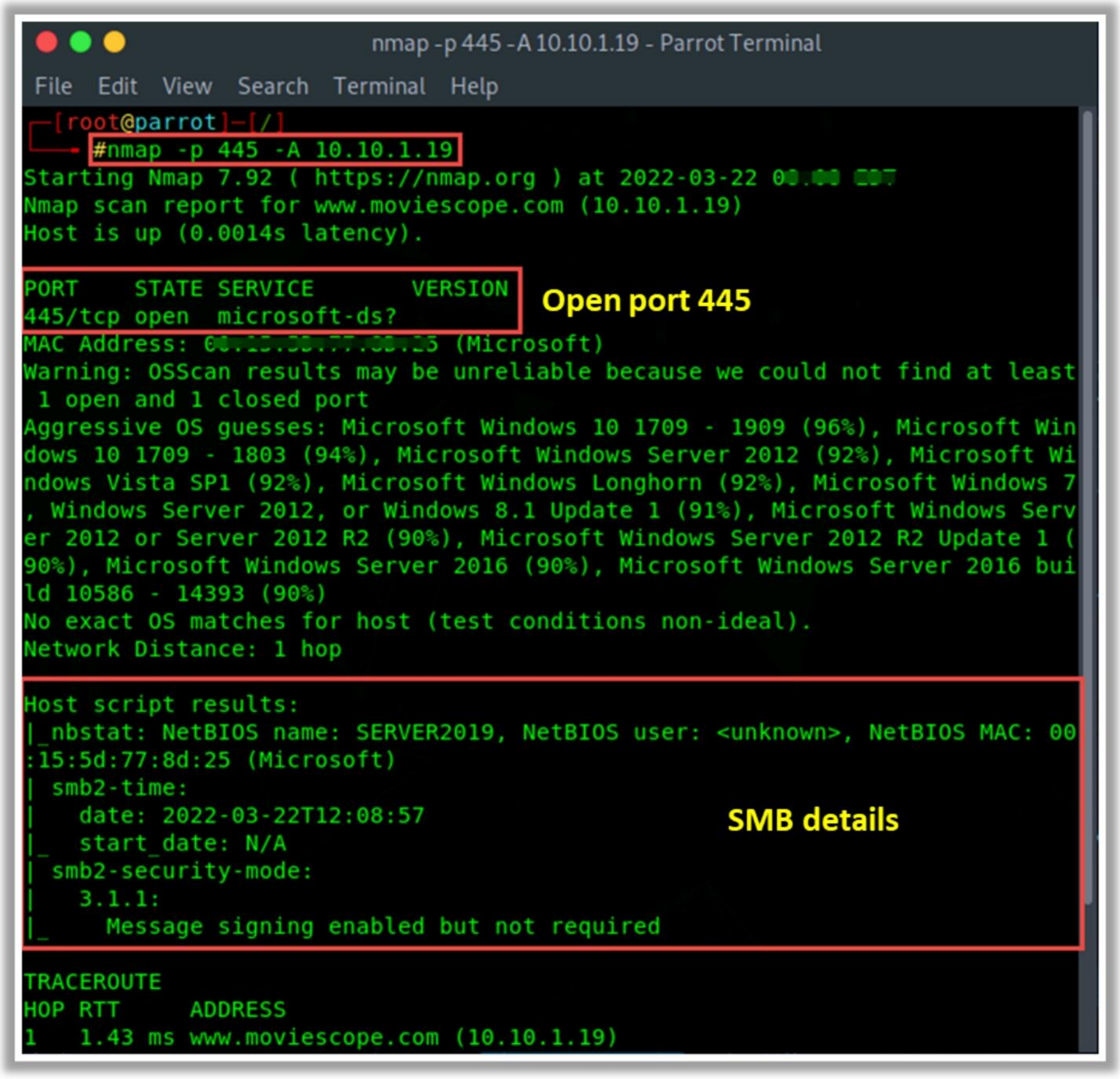


Figure 4.51: Screenshot of Nmap performing SMB enumeration

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.

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

https://t.me/learningnets

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>
```

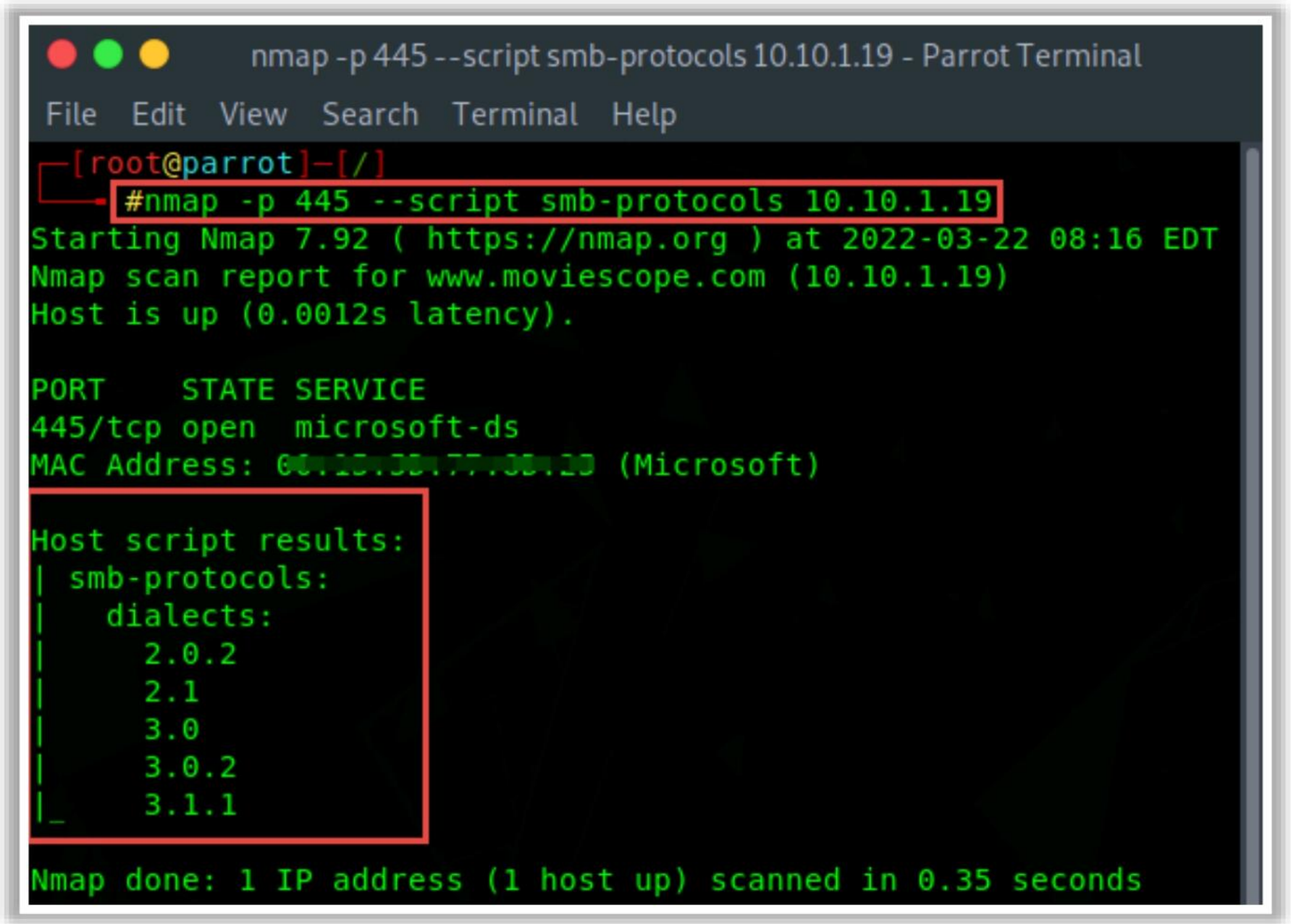
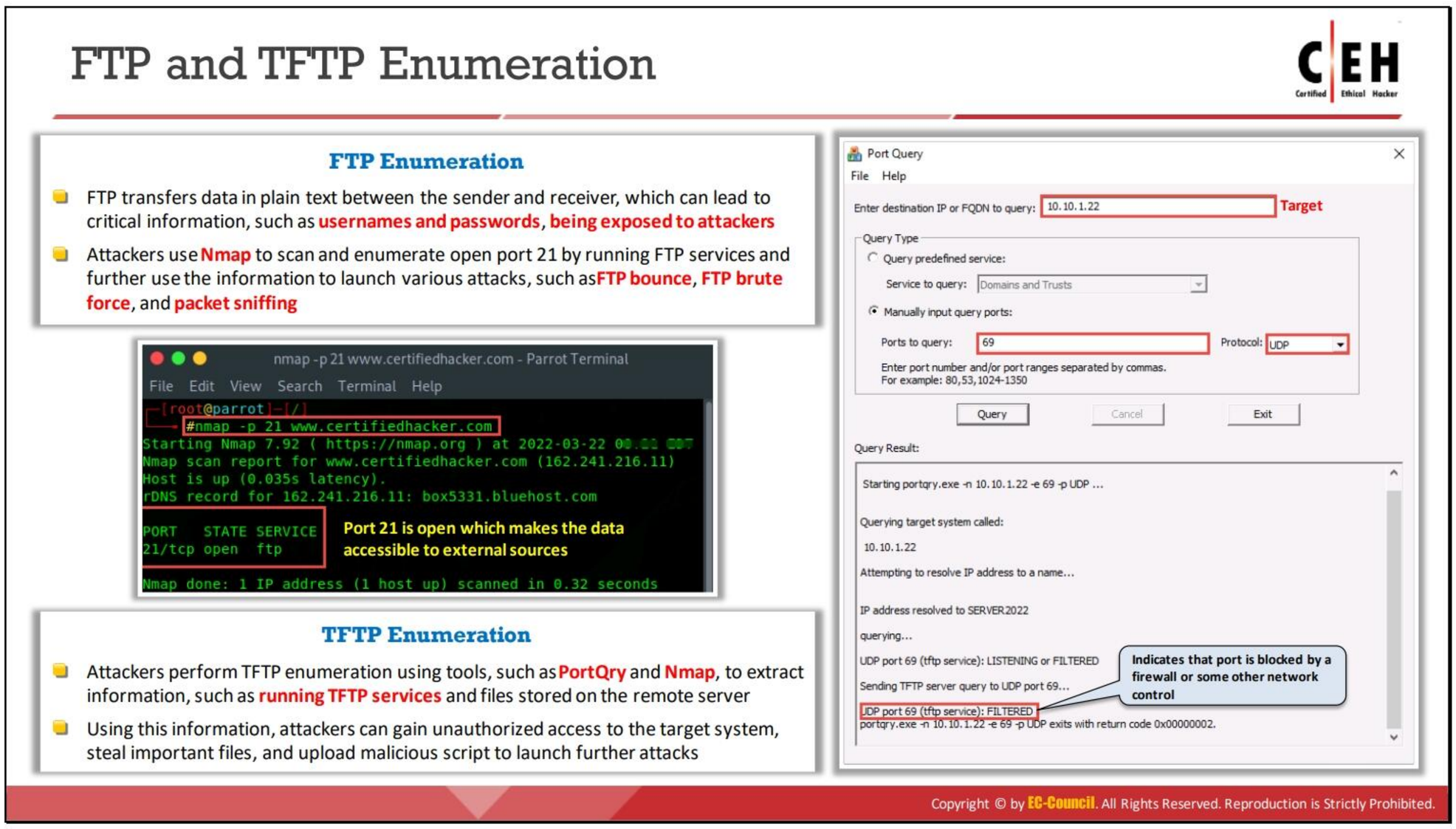


Figure 4.52: Screenshot of Nmap performing SMB enumeration

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

https://t.me/learningnets



FTP Enumeration

The File Transfer Protocol (FTP) is used to transfer files over TCP, and its default port is 21. In FTP, data are transferred between a sender and receiver in plaintext, exposing critical information such as usernames and passwords to attackers. FTP offers neither a secure network environment nor secure user authentication. Individuals do not need authentication to access an FTP server in a network. This provides an easy method for attackers to access network resources.

The implementation of FTP in an organization's network makes the data accessible to external sources. Attackers can scan and enumerate open port 21 running FTP services and further use this information to launch various attacks such as FTP bounce, FTP brute force, and packet sniffing.

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

https://t.me/learningnets

As shown in the screenshot, the following Nmap command is used by the attackers to enumerate the FTP service running on the target domain:

```
# nmap -p 21 <target domain>
```

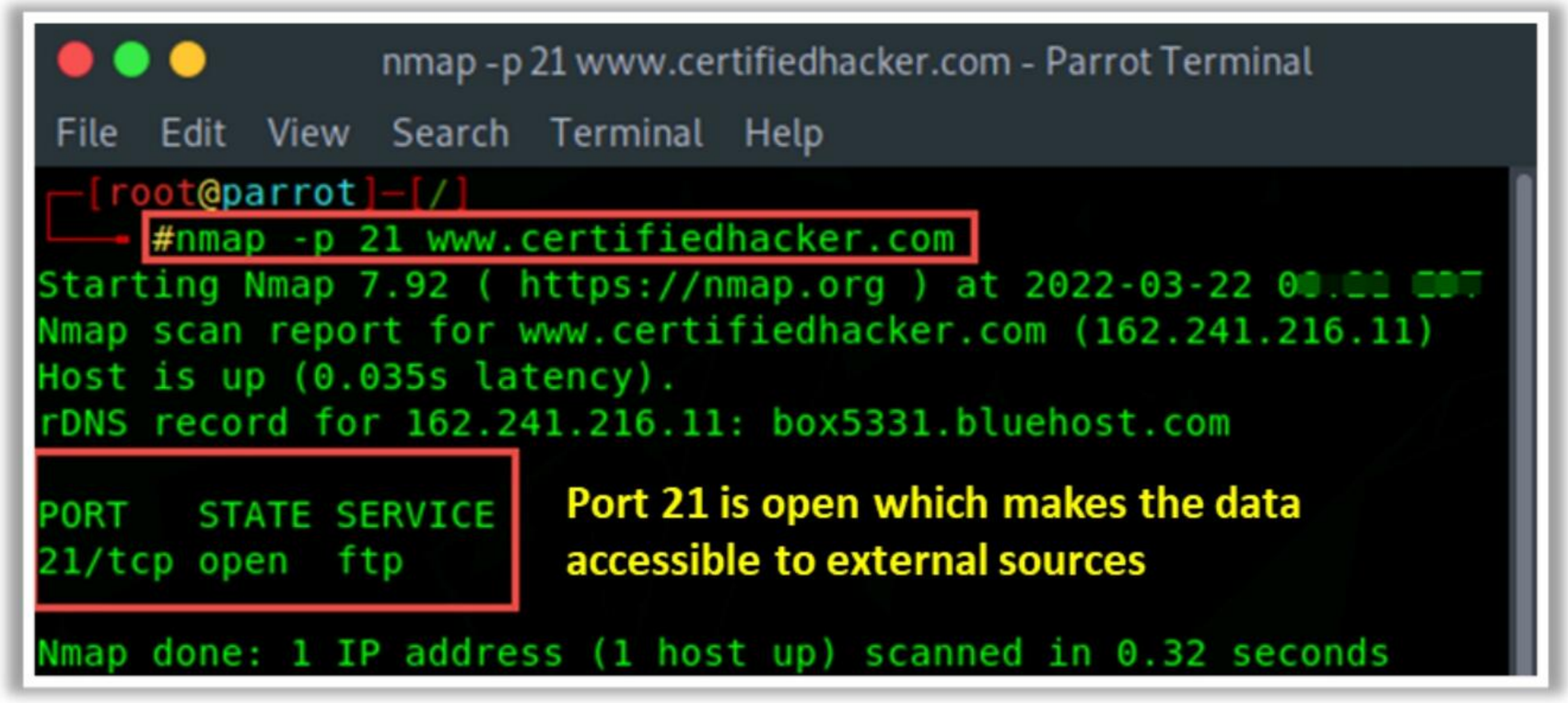


Figure 4.53: Screenshot of Nmap displaying a FTP enumeration result

Attackers also use Metasploit to enumerate FTP services running on remote hosts. The following commands can be used to detect the FTP version of the target server:

```
use auxiliary/scanner/ftp/ftp_version
msf auxiliary(scanner/ftp/ftp_version) > set RHOSTS <target IP>
msf auxiliary(scanner/ftp/ftp_version) > exploit
```

TFTP Enumeration

The Trivial File Transfer Protocol (TFTP) is a simplified version of FTP and is used for transferring files between network devices. By default, TFTP servers listen on UDP port 69. This protocol is used when directory visibility and user authentication are not required; therefore, it provides no security features.

To perform TFTP enumeration, attackers can use tools such as PortQry and Nmap to extract information such as running TFTP services and files stored on a remote server. By using the enumerated information, attackers can further gain unauthorized access to the target system, steal important files, and upload malicious scripts to launch further attacks. Furthermore, this information enables attackers to perform various attacks such as DNS amplification attacks, TFTP reflection attacks, and DDoS attacks.

- **PortQry**

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

  The PortQry utility reports the port status of TCP and UDP ports on a selected target. Attackers can use the PortQry tool to perform TFTP enumeration. This utility reports the port status of target TCP and UDP ports on a local or remote computer.

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

https://t.me/learningnets

In the PortQry tool, the attackers can specify the target to scan for a running TFTP service on open port 69. As shown in the screenshot, attackers perform TFTP enumeration on the target domain by setting the **`Ports to query:`** value to 69 and **`Protocol`** to UDP.

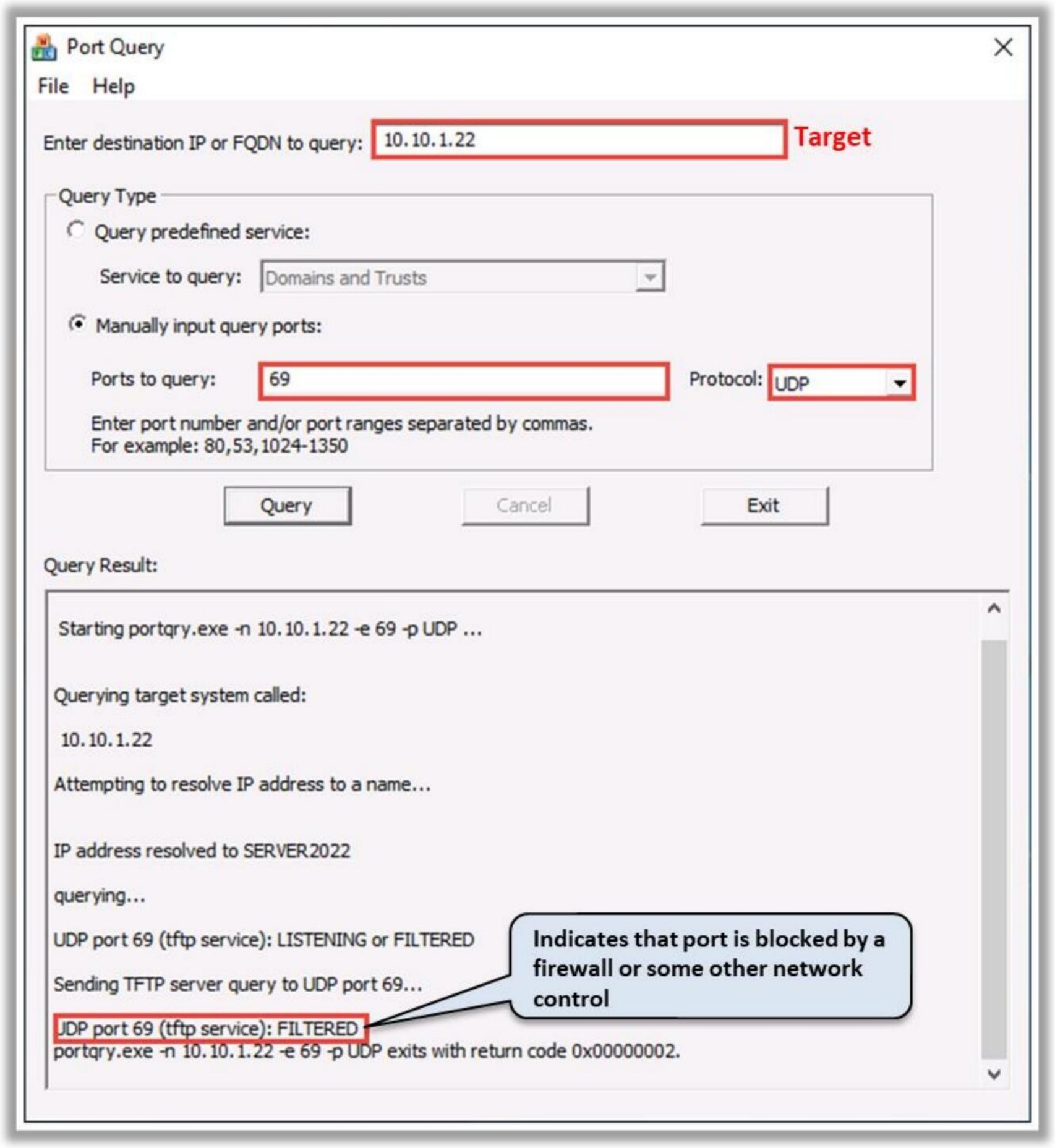


Figure 4.54: Screenshot of the PortQry tool displaying a TFTP scan result

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

https://t.me/learningnets

Attackers can also use the PortQry command-line utility to perform TFTP enumeration using the following command:

```
portqry -n <target domain/IP> -e 69 -p udp
```

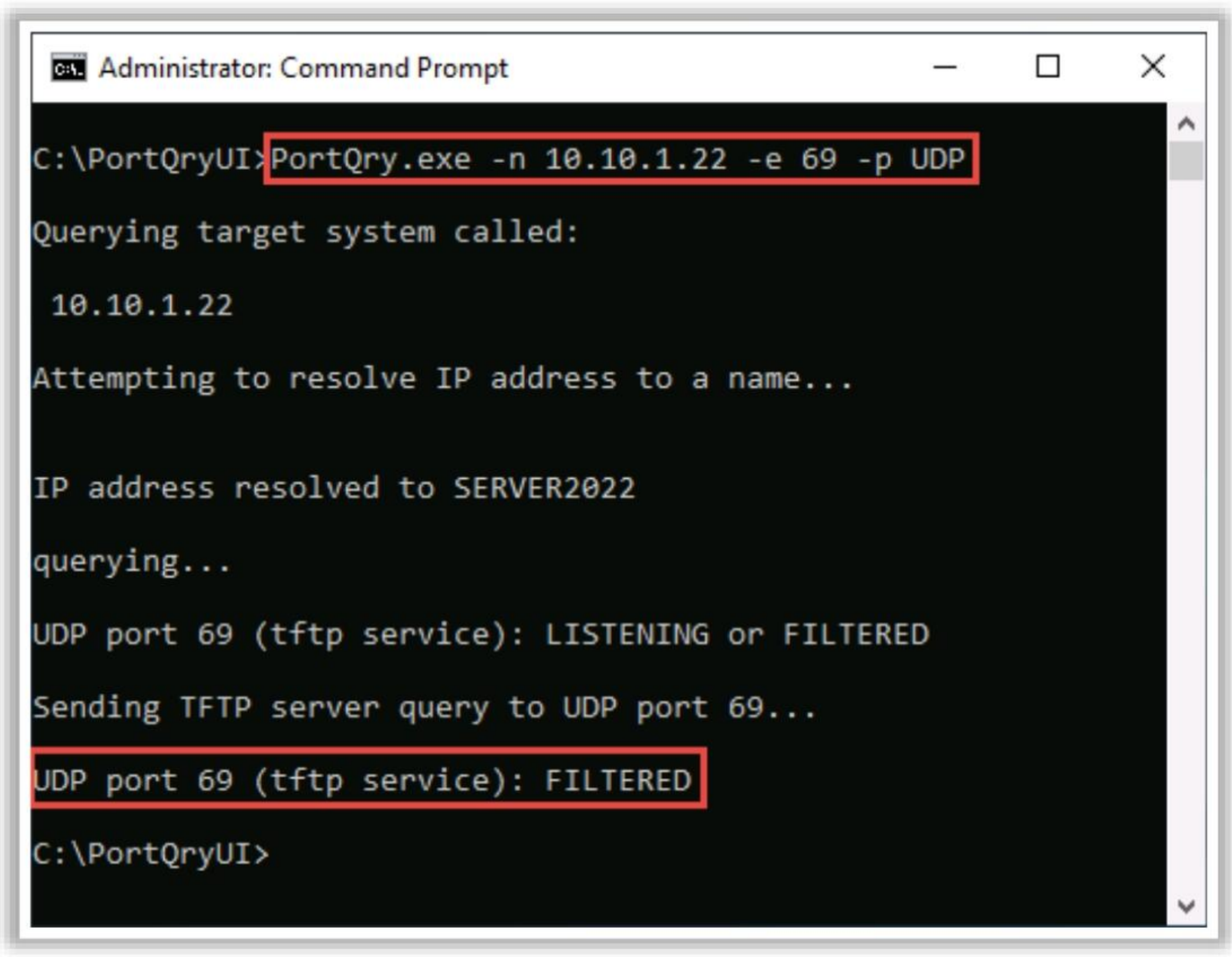


Figure 4.55: Screenshot of the PortQry command-line utility showing a TFTP scan result

- **Nmap**

  Source: *https://nmap.org*

  Attackers can use the Nmap tool to perform simple direct scanning for TFTP port 69. As shown in the screenshot, the following Nmap command is used by attackers to enumerate the TFTP service running on the target domain:

  ```
  # nmap -p 69 <target domain/IP>
  ```

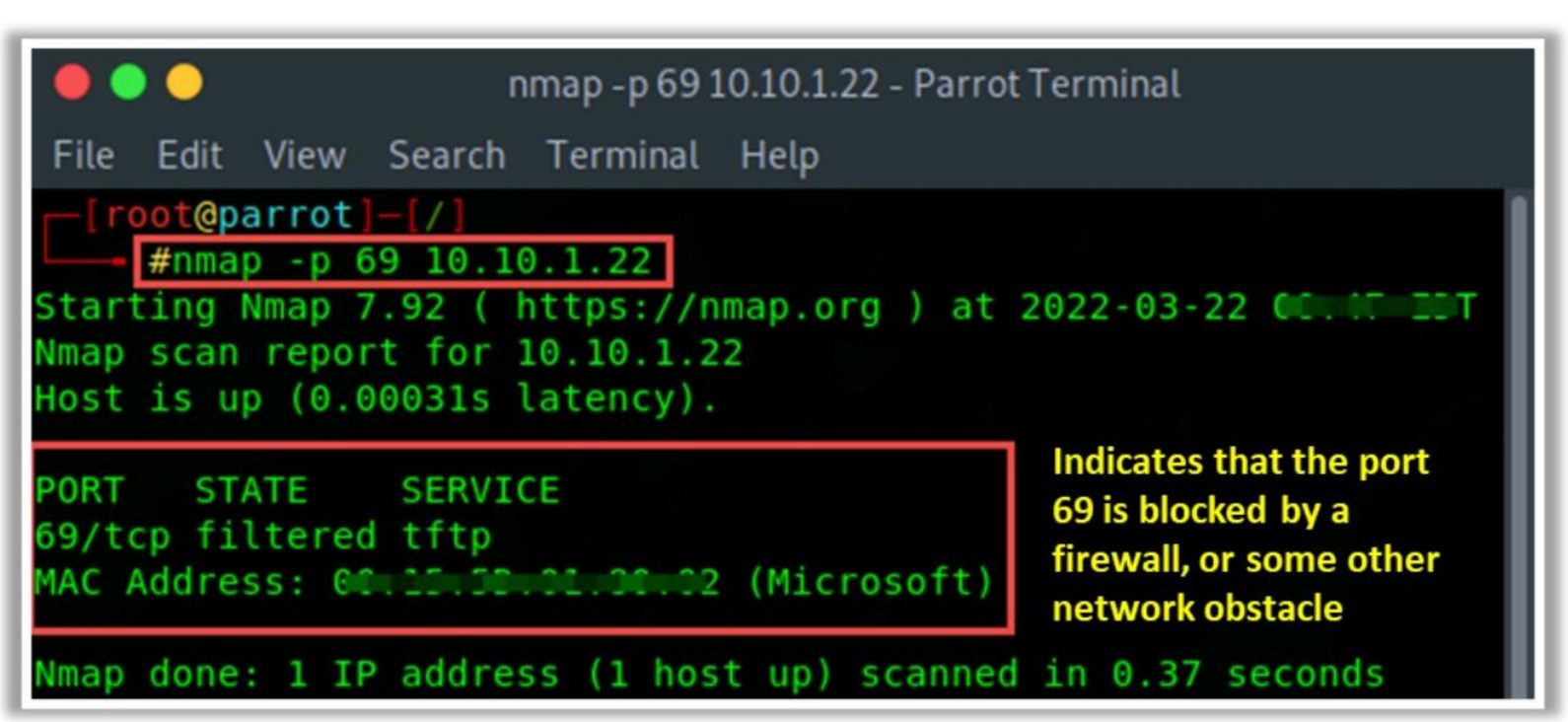
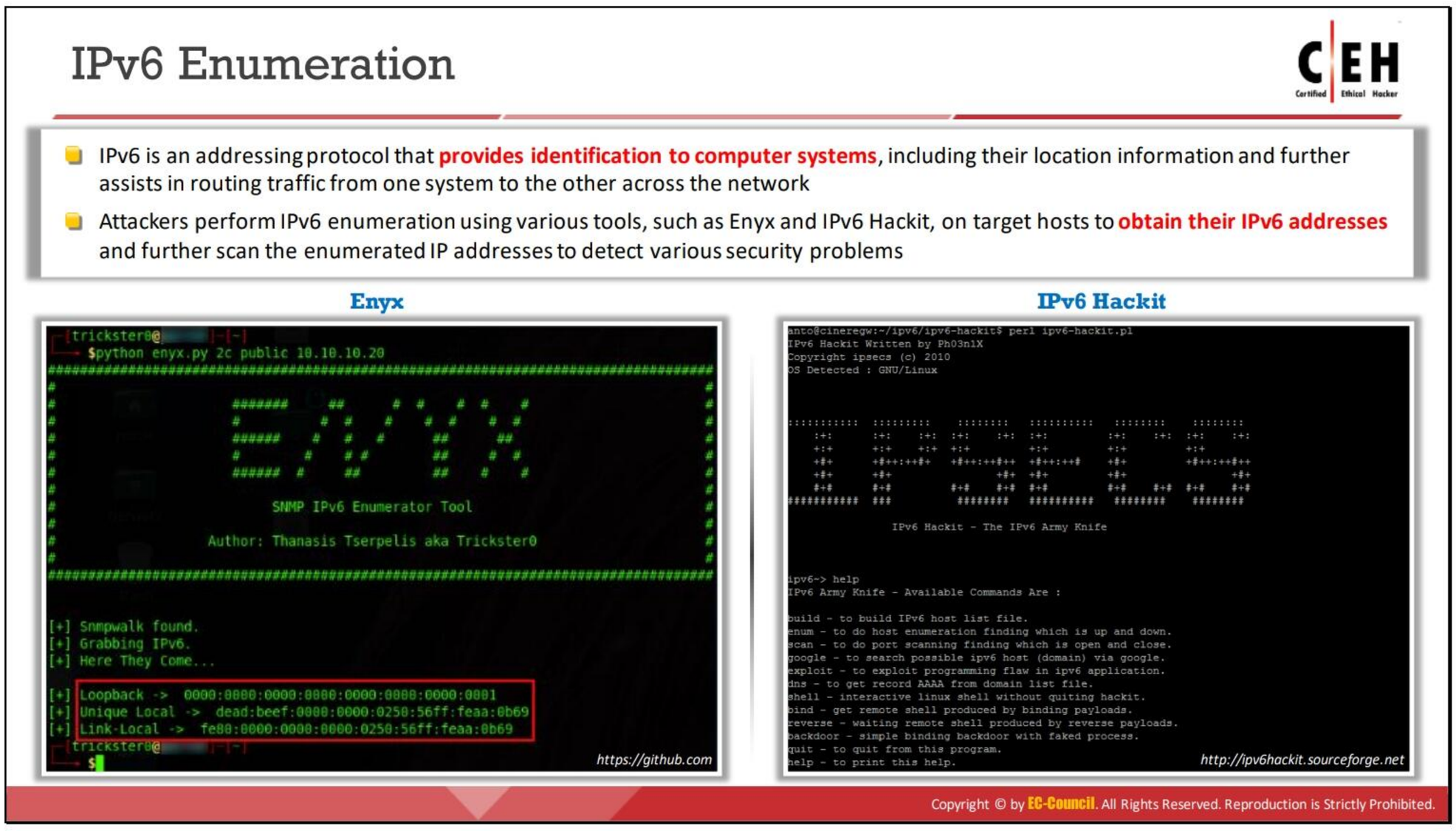


Figure 4.56: Screenshot of Nmap command displaying a TFTP scan result

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

https://t.me/learningnets



IPv6 Enumeration

Internet Protocol version 6 (IPv6) is an addressing protocol that identifies computer systems, including location information, and assists in routing traffic from one system to another system across a network. It is an advanced version of IPv4 and, therefore, supports a greater number of hosts as compared to IPv4. It was designed to overcome the problem of IPv4 address exhaustion.

Attackers perform IPv6 enumeration on target hosts to obtain their IPv6 addresses and further scan the enumerated IP addresses to detect various security problems such as access to routing structure, exposure of sensitive content, and users' access control lists. By using this information, attackers can launch various attacks such as SYN flood attacks, DNS amplification attacks, and DDoS attacks. Attackers can scan and enumerate the IPv6 address of a target machine in the network by using various tools such as Enyx and IPv6 Hackit.

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

https://t.me/learningnets

- **Enyx**

  Source: *https://github.com*

  Enyx is an enumeration tool that fetches the IPv6 address of a machine through SNMP.

  As shown in the screenshot, attackers use the following command to enumerate the IPv6 address of a target machine (`10.10.10.20`) by setting the SNMP version to `2c` and community string to `public`:

  `Python enyx.py 2c public <target IP>`

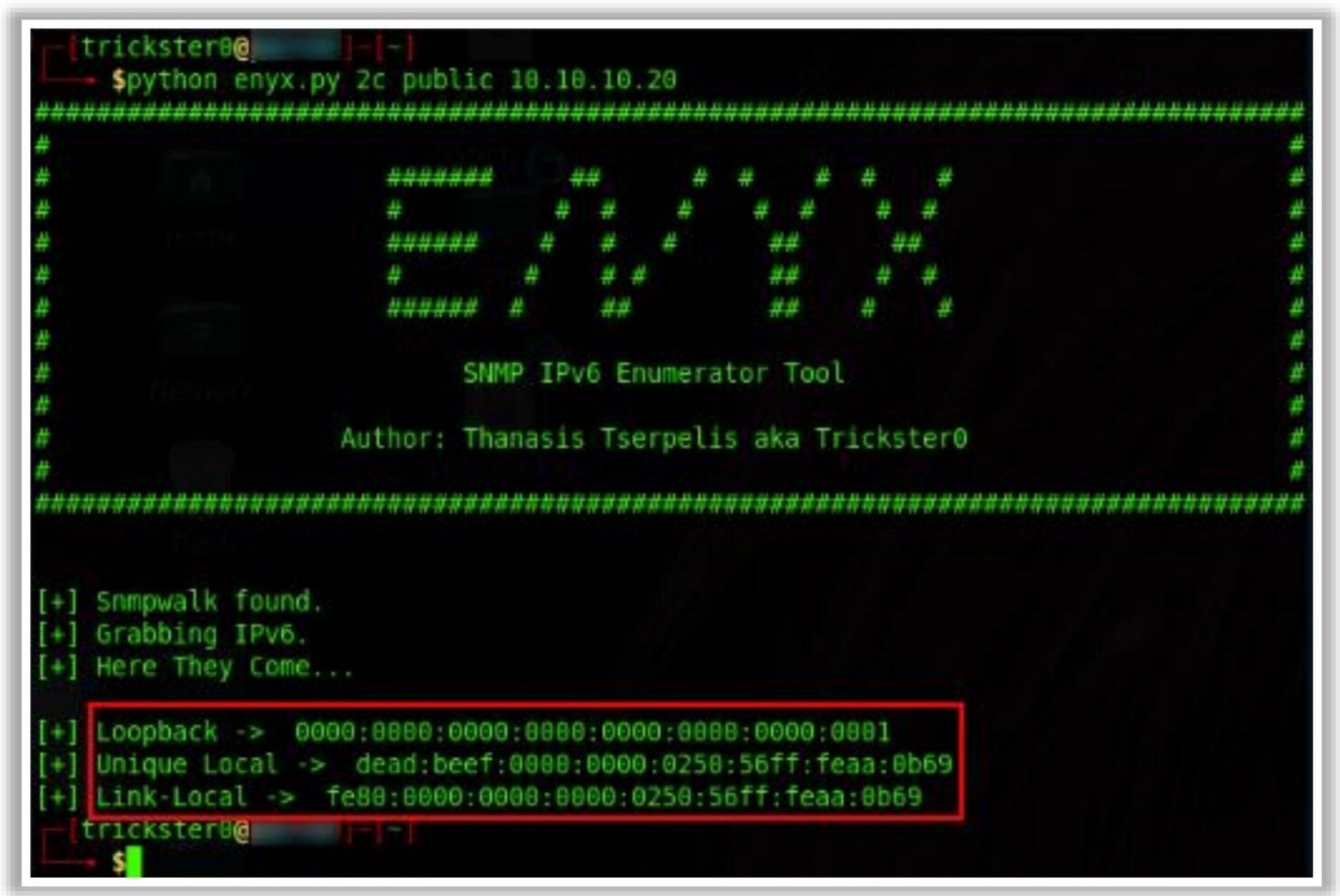


Figure 4.57: Screenshot of Enyx tool displaying enumerated results

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

https://t.me/learningnets

- **IPv6 Hackit**

  Source: *http://ipv6hackit.sourceforge.net*

  Hackit is a scanning tool that provides a list of active IPv6 hosts. It can perform TCP port scanning and identify AAAA IPv6 host records.

  As shown in the screenshot, attackers can specify the target machine and run a scan to enumerate the IPv6 information.

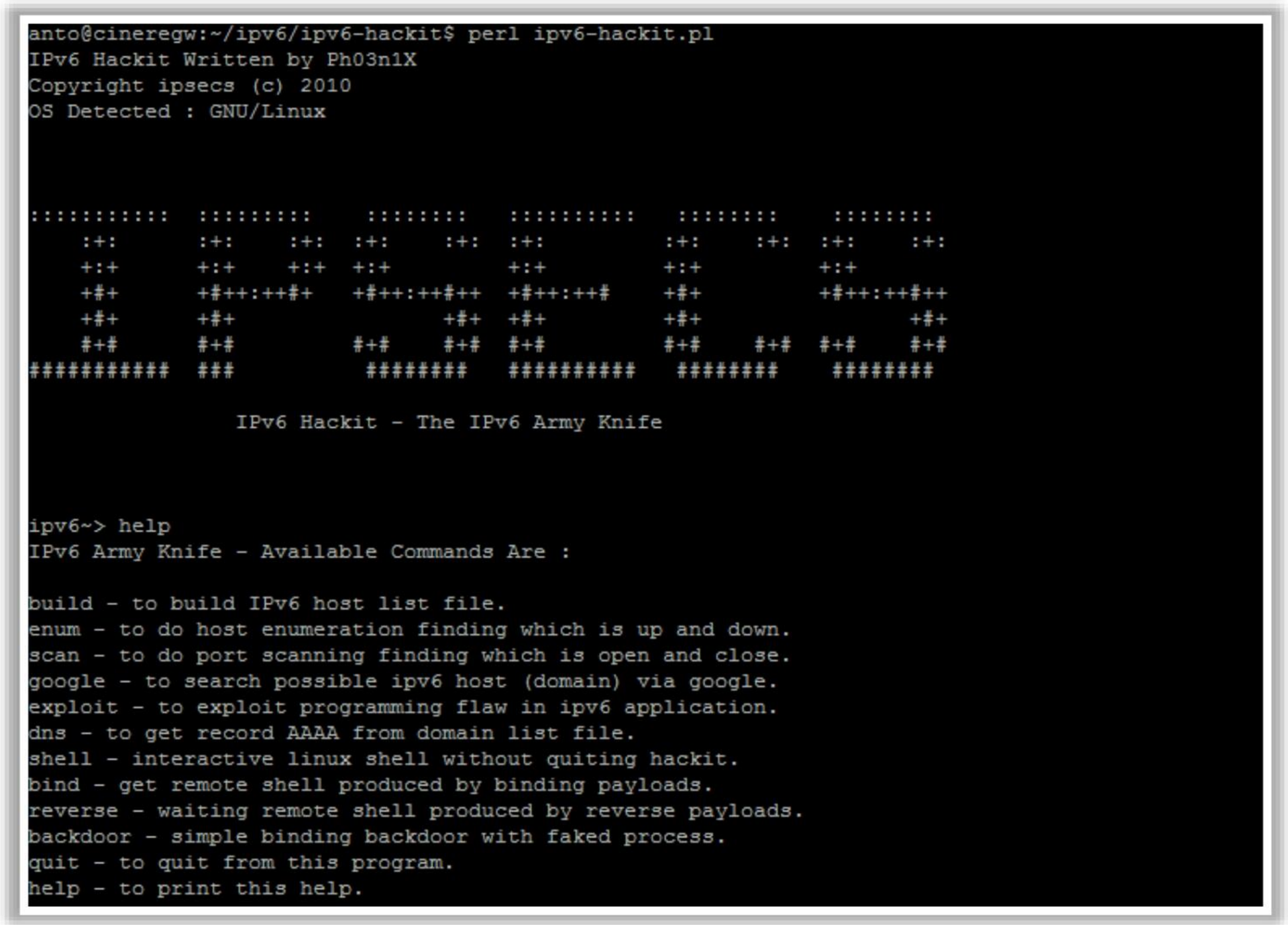
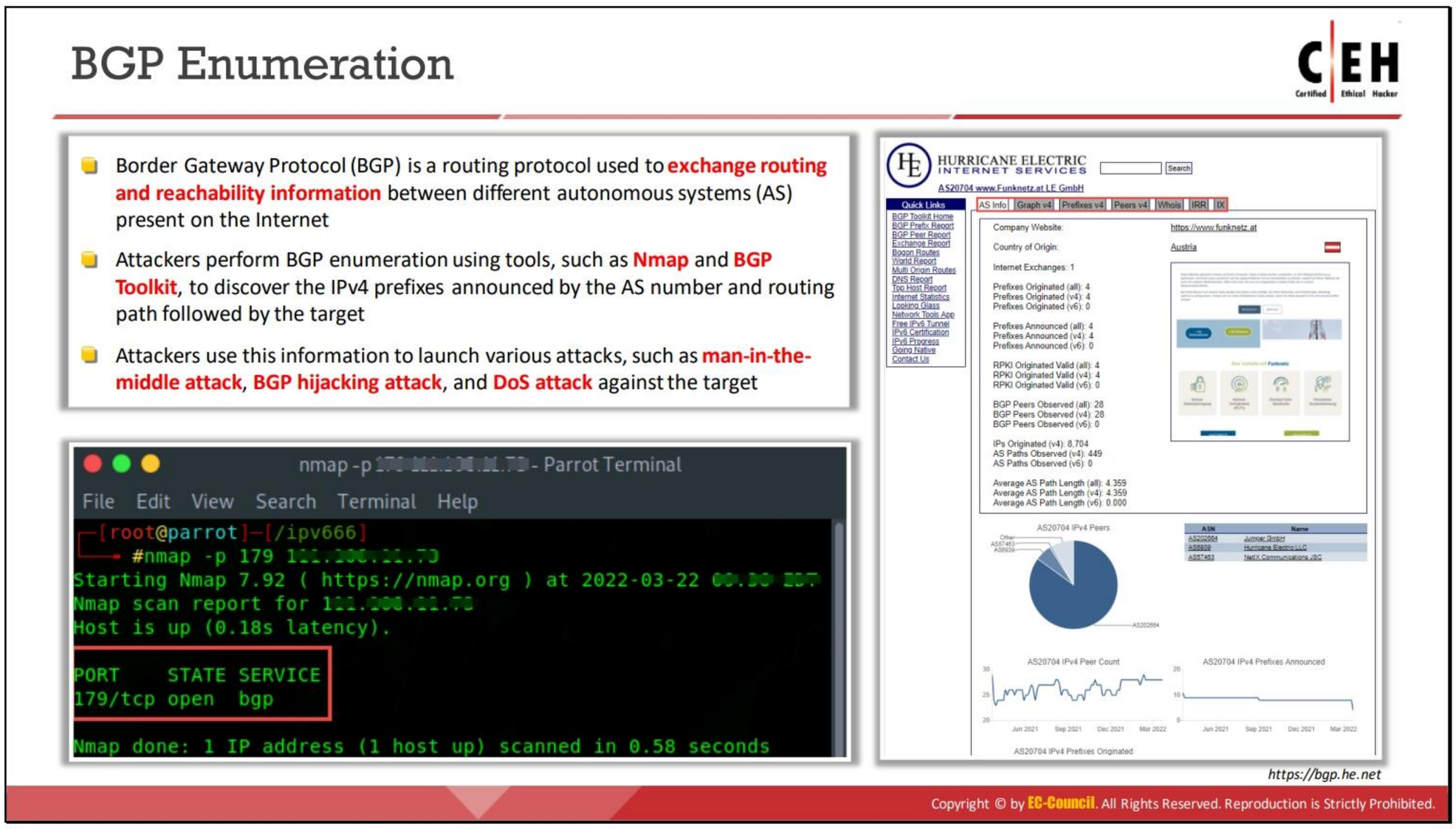


Figure 4.58: Screenshot displaying the IPv6 Hackit tool

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

https://t.me/learningnets



BGP Enumeration

The Border Gateway Protocol (BGP) is a routing protocol used to exchange routing and reachability information between different autonomous systems (AS) on the Internet. Because this protocol is used to connect one AS to other ASs, it is also called external BGP (eBGP). BGP finds the shortest path to route traffic from one IP address to another efficiently. BGP creates its TCP session on port 179.

Attackers perform BGP enumeration on the target using tools such as Nmap and BGP Toolkit to discover the IPv4 prefixes indicated by the AS number and the routing path followed by the target. Attackers use this information to launch various attacks against the target, such as man-in-the-middle attacks, BGP hijacking attacks, and DoS attacks.

As shown in the screenshot, attackers use the following Nmap command to enumerate BGP running on the target system:

```
# nmap -p 179 <target IP>
```

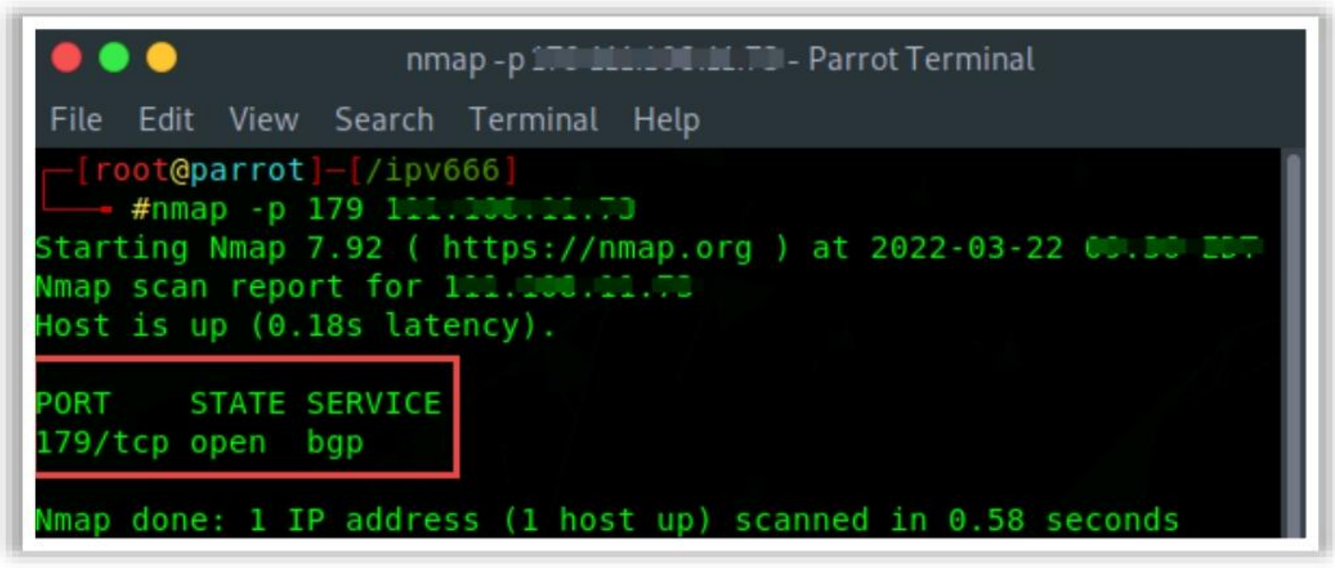


Figure 4.59: Screenshot of Nmap displaying a BGP enumeration result

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

https://t.me/learningnets

As shown in the screenshot, attackers use BGP Toolkit to perform BGP enumeration on the target domain. This online tool can be used to search for the target domain and obtain details such as DNS information, website information, IP information, AS information, and whois information. Based on the identified ASs, attackers can further enumerate details such as IPv4 prefixes, BGP routing graphs, and IPv4 peers.

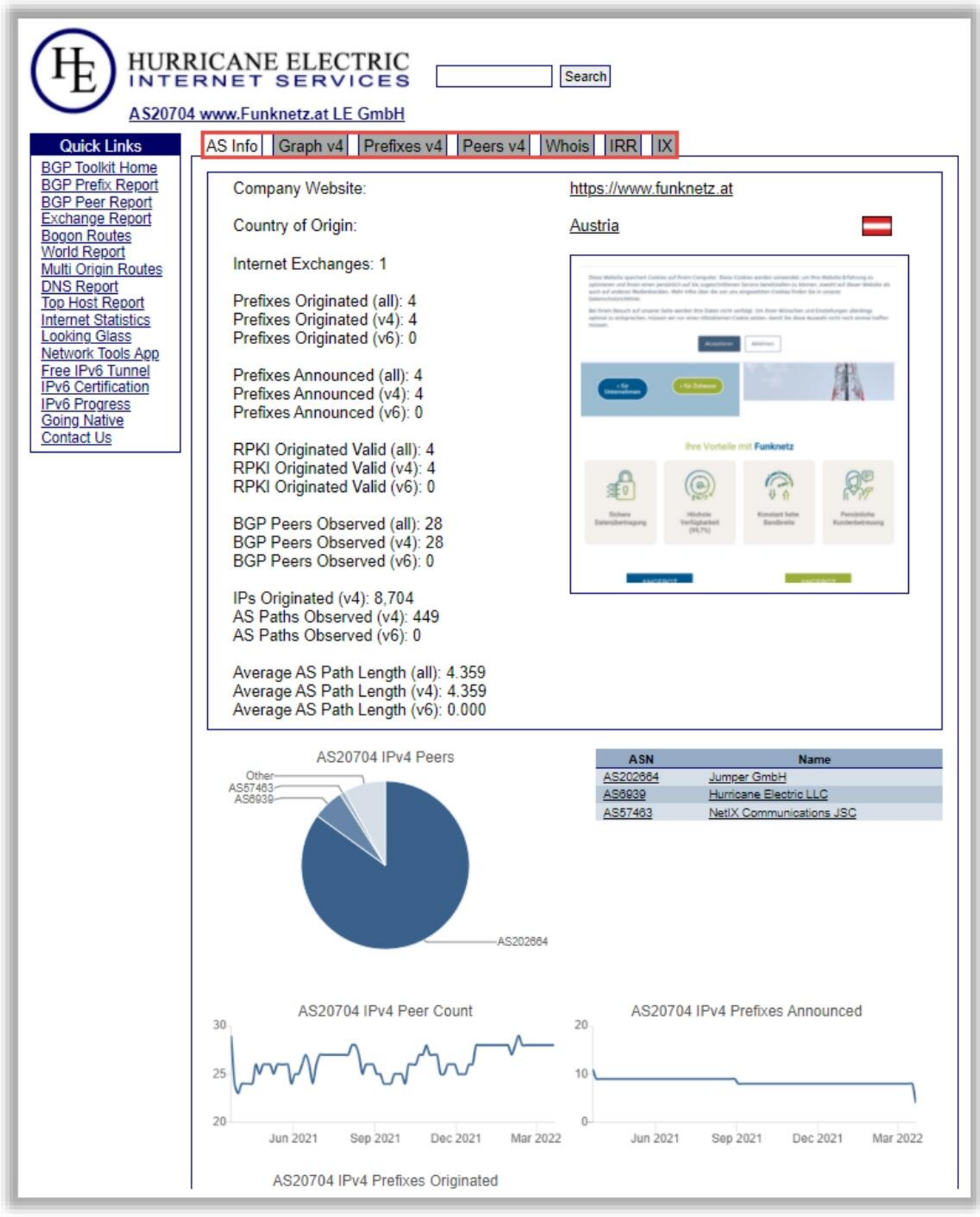


Figure 4.60: Screenshot of BGP Toolkit

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

https://t.me/learningnets

LO#08: Explain Enumeration Countermeasures

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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 © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

https://t.me/learningnets

Enumeration Countermeasures (Cont'd)

SMTP

Configure SMTP servers to

- Ignore **email messages** to unknown recipients
- 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

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**

FTP

- Implement **secure FTP** (SFTP) or FTP secure (FTPS) to encrypt the FTP traffic over the network
- Implement **strong passwords** or a certification-based authentication policy
- Ensure that **unrestricted uploading of files** on the FTP server is **not allowed**
- **Disable anonymous FTP accounts**; if not feasible, regularly monitor anonymous FTP accounts

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

DNS Enumeration Countermeasures

1	Restrict resolver access	6	Restrict DNS zone transfers	11	Use VPN
2	Randomize source ports	7	Separate resolver and authoritative nameserver	12	Implement two-factor authentication
3	Audit DNS zones	8	Use isolated DNS servers	13	Use DNS change lock
4	Patch known vulnerabilities	9	Disable DNS recursion	14	Use DNSSEC
5	Monitor nameservers	10	Harden the OS	15	Use premium DNS registration

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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, NFS, and FTP enumeration.

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

https://t.me/learningnets

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.
- 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.

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.
- 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.

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

https://t.me/learningnets

- Create decoy groups with the word "Admin" in the name to mislead attackers. Attackers typically search for LDAP admin accounts.

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.
- 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.

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.
- 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.

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

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

https://t.me/learningnets

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.

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.

FTP Enumeration Countermeasures

- Implement secure FTP (SFTP, which uses SSH) or FTP secure (FTPS, which uses SSL) to encrypt the FTP traffic over the network.
- Implement strong passwords or a certification-based authentication policy.
- Ensure that the unrestricted uploading of files on the FTP server is not allowed.

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

https://t.me/learningnets

- Disable anonymous FTP accounts. If this is not possible, monitor anonymous FTP accounts regularly.
- Restrict access by IP or domain name to the FTP server.
- Configure access controls on authenticated FTP accounts using access-control lists (ACLs).
- Restrict login attempts and time.
- Configure ingress and egress filtering rules for the FTP services.
- Use SSL/FTPS for authenticated FTP accounts.
- Do not run regular public services such as mail or the web on a single FTP server.
- Implement a Markov game-based analysis model for vulnerability assessment and penetration testing (VAPT) on cloud-based FTP servers.

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.

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

https://t.me/learningnets

- **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.
- **Use premium DNS registration:** Use premium DNS registration services that hide sensitive information, such as host information (HINFO), from the public.

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.

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

https://t.me/learningnets

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, Telnet, FTP, TFTP, SMB, IPv6, and BGP 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 © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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, Telnet, FTP, TFTP, SMB, IPv6, and BGP 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.

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

https://t.me/learningnets