

# Lab 8: Perform Enumeration using AI

## Lab Scenario

In this lab, you will use AI-assisted tools and techniques to perform enumeration on a target network. The goal is to gather detailed information about the network resources and infrastructure, which will help you identify potential vulnerabilities and plan further penetration testing activities.

## Lab Objectives

- Perform Enumeration using ShellGPT

## Overview of Enumeration using AI

Artificial Intelligence (AI) can significantly enhance the enumeration process by automating tasks, analyzing large datasets, and identifying patterns that might be missed by traditional tools. AI can streamline the enumeration process, making it faster, more efficient, and more accurate.

### Task 1: Perform Enumeration using ShellGPT

ShellGPT is a powerful tool leveraging AI, specifically GPT-4, to assist in various tasks, including network enumeration for penetration testing. By using ShellGPT, ethical hackers can automate the enumeration process, gain insightful data analysis, and identify potential vulnerabilities more efficiently.

Here, we will use the ShellGPT to perform enumeration on the target IP address.

The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the diverse environments in which it operates. As a result, you may observe differences in command syntax, execution, and results while performing this lab task.

1. Before starting this lab, click [Parrot Security](#) to switch to the **Parrot Security** machine and incorporate ShellGPT by following steps provided in [Integrate ShellGPT in Parrot Security Machine.pdf](#).

Alternatively, you can follow the steps to integrate ShellGPT provided in **Module 00: Integrate ShellGPT in Parrot Security Machine**.

2. After incorporating the ShellGPT API in Parrot Security Machine, in the terminal window run **sgpt -shell “Perform NetBIOS enumeration on target IP 10.10.1.11”** command to perform NetBIOS enumeration on target system.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "sgpt --shell \"Perform NetBIOS enumeration on target IP 10.10.1.11\" - Parrot Terminal". The command run is "nbtscan 10.10.1.11". The output shows a single entry for the target IP 10.10.1.11, which is identified as a Windows 11 server with the NetBIOS name "WINDOWS11". The user is listed as "<unknown>" and the MAC address is "00:15:5d:01:80:00".

```
[root@parrot]~[~/home/attacker]
└─# sgpt --shell "Perform NetBIOS enumeration on target IP 10.10.1.11"
nbtscan 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Doing NBT name scan for addresses from 10.10.1.11

IP address      NetBIOS Name    Server    User          MAC address
-----
10.10.1.11      WINDOWS11     <server>  <unknown>   00:15:5d:01:80:00
[root@parrot]~[~/home/attacker]
└─#
```

3. Run **sgpt --shell “Get NetBIOS info for IP 10.10.1.11 and display the associated names”** command to view the associated names of target system.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "sgpt --shell "Get NetBIOS info for IP 10.10.1.11 and display the associated names" - Parrot Terminal". The command run was "nmblookup -A 10.10.1.11". The output shows the following NetBIOS entries:

```
[root@parrot]~[/home/attacker]
└─# nmblookup -A 10.10.1.11
[E]ecute, [D]escribe, [A]bort: E
Looking up status of 10.10.1.11
  WINDOWS11      <00> -          B <ACTIVE>
  WORKGROUP     <00> - <GROUP> B <ACTIVE>
  WINDOWS11     <20> -          B <ACTIVE>
  WORKGROUP     <1e> - <GROUP> B <ACTIVE>
  WORKGROUP     <1d> -          B <ACTIVE>
  .__MSBROWSE__. <01> - <GROUP> B <ACTIVE>

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

[root@parrot]~[/home/attacker]
└─#
```

The terminal window has a dark background with a network graph watermark. The bottom status bar shows "CEHv13 Module 13 Hacking Web Servers".

4. To perform NetBIOS enumeration using Nmap run **sgpt --shell “Enumerate NetBIOS on target IP 10.10.1.22 with nmap”** command.

In the prompt type **E** and press **Enter** to execute the command.

```
[E]xecute, [D]escribe, [A]bort: E
sgpt --shell "Enumerate NetBIOS on target IP 10.10.1.22 with Nmap" - Parrot Terminal
File Edit View Search Terminal Help
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 01:21 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00061s latency).

PORT      STATE SERVICE
137/udp  open  netbios-ns

MAC Address: 00:15:5D:01:80:02 (Microsoft)

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

CEHV43 Module 18
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
[root@parrot]#
```

5. We will now perform SNMP enumeration using ShellGPT, to do so, run **sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using SnmpWalk and display the result here" command.**

In the prompt type **E** and press **Enter** to execute the command.

```
[root@parrot]~[/home/attacker]
└─#sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using SnmpWalk and d
isplay the result here"
snmpwalk -v2c -c public 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Created directory: /var/lib/snmp/cert_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE - Soft
ware: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (2887671485) 334 days, 5:18:34.85
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "Server2022.CEH.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 28
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10
iso.3.6.1.2.1.2.2.1.1.11 = INTEGER: 11
```

6. Run **sgpt --chat enum --shell “Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here”** command to perform SNMP enumeration using Nmap.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar indicates the command being run: "sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here" - Parrot Terminal". The terminal prompt is "[root@parrot]~[/home/attacker]". The output of the command is displayed, showing the results of an nmap scan for port 161 (SNMP) on host 10.10.1.22. The output includes a list of users found on the system, including "Administrator", "Guest", "Martin", "Shiela", "jason", and "krbtgt". It also lists shares such as "C:\Users", "SYSVOL", and "NETLOGON". System details like hardware (Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE), software (Windows Version 6.3 (Build 20348 Multiprocessor Free)), and system uptime (334d05h28m41.31s (2887732131 timeticks)) are also provided.

```
[root@parrot]~[/home/attacker]
#sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here"
nmap -sU -p 161 --script snmp-interfaces,snmp-netstat,snmp-processes,snmp-win32-shares,snmp-win32-users,snmp-win32-software,snmp-sysdescr 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 01:39 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00035s latency).

PORT      STATE SERVICE
161/udp    open   snmp
| snmp-win32-users:
|   Administrator
|   Guest
|   Martin
|   Shiela
|   jason
|_  krbtgt
| snmp-win32-shares:
|   Users: C:\Users
|   SYSVOL: C:\Windows\SYSVOL\sysvol
|_  NETLOGON: C:\Windows\SYSVOL\sysvol\CEH.com\SCRIPTS
| snmp-sysdescr: Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)
|_  System uptime: 334d05h28m41.31s (2887732131 timeticks)
```

- Run **sgpt --chat enum --shell "Perform SNMP processes on target IP 10.10.1.22 using nmap and display the result here" command.**

In the prompt type **E** and press **Enter** to execute the command.

The terminal window shows the following command and its output:

```
sgpt --chat enum --shell "Perform SNMP processes on target IP 10.10.1.22 using nmap and display the result here" - Parrot Terminal
```

```
[root@parrot]~[/home/attacker]
#sgpt --chat enum --shell "Perform SNMP processes on target IP 10.10.1.22 using nmap and display the result here"
nmap -sU -p 161 --script snmp-processes 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 01:42 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00084s latency).

PORT      STATE SERVICE
161/udp    open  snmp
| snmp-processes:
| 1:
|   Name: System Idle Process
| 4:
|   Name: System
| 72:
|   Name: svchost.exe
|   Path: C:\Windows\system32\
|   Params: -k DcomLaunch -p -s LSM
| 96:
|   Name: Registry
| 380:
|   Name: smss.exe
| 492:
|   Name: csrss.exe
```

8. To perform SMTP enumeration on a target IP run **sgpt --chat enum --shell “Perform SMTP enumeration on target IP 10.10.1.19.”** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19." - Parrot Terminal". The terminal prompt is "[root@parrot]~[/home/attacker]". The command run was "#sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19."". The output shows an Nmap scan report for www.goodshopping.com (10.10.1.19). The host is up with 0.0016s latency. It lists ports, states, and services, specifically port 25/tcp as open smtp. It details various SMTP commands supported by the server, including EHLO, STARTTLS, RCPT, DATA, RSET, MAIL, QUIT, HELP, AUTH, TURN, ETRN, BDAT, and VRFY. It also lists users found via SMTP-enum-users, including root, admin, administrator, webadmin, sysadmin, netadmin, and guest.

```
sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19." - Parrot Terminal
[ro...@parrot]~[/home/attacker]
#sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19."
nmap -p25,465,587 --script smtp-commands,smtp-enum-users,smtp-ntlm-info,smtp-open-relay,smtp-vuln-cve2010-4344,smtp-vuln-cve2011-1720,smtp-vuln-cve2011-1764 10.10.1.19
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 01:57 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.0016s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
|_smtp-open-relay: Server is an open relay (14/16 tests)
| smtp-commands: Server2019 Hello [10.10.1.13], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDST
ATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
  TURN ETRN BDAT VRFY
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
| smtp-enum-users:
| root
| admin
| administrator
| webadmin
| sysadmin
| netadmin
| guest

```

9. We will perform DNS enumeration with Nmap using ShellGPT, to do so run **sgpt --chat enum --shell "Use Nmap to perform DNS Enumeration on target domain www.certifiedhacker.com"** command.

In the prompt type **E** and press **Enter** to execute the command.

```
Applications Places System Mon May 20, 02:58
sgpt --chat enum --shell "Use Nmap to perform DNS Enumeration on target domain www.certifiedhacker.com" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#sgpt --chat enum --shell "Use Nmap to perform DNS Enumeration on target domain www.certifiedhacker.com"
nmap --script dns-brute,dns-zone-transfer,dns-service-discovery -p 53 www.certifiedhacker.com
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 02:57 EDT
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.14s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
PORT      STATE SERVICE
53/tcp    open  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     news.certifiedhacker.com - 162.241.216.11
|     blog.certifiedhacker.com - 162.241.216.11
|     mail.certifiedhacker.com - 162.241.216.11
|     www.certifiedhacker.com - 162.241.216.11
|     ftp.certifiedhacker.com - 162.241.216.11
|     smtp.certifiedhacker.com - 162.241.216.11
|     demo.certifiedhacker.com - 162.241.216.11
CEHv11 Module 14
Nmap done: 1 IP address (1 host up) scanned in 6.00 seconds
[root@parrot]~[/home/attacker]
Menu sgpt--chatenum--sh...
```

10. To perform DNS cache snooping on target domain run **sgpt --chat enum --shell “Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method. Use DNS server IP as 162.241.216.11”** command.

In the prompt type **E** and press **Enter** to execute the command.

```
[root@parrot]~[/home/attacker]
#sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method. Use DNS server IP as 162.241.216.11"
dig @162.241.216.11 www.certifiedhacker.com +recurse
[E]xecute, [D]escribe, [A]bort: E

; <>> DiG 9.18.24-1-Debian <>> @162.241.216.11 www.certifiedhacker.com +recurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 41420
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d7161237fea3794059ae9cf1664af985fb6cb25ced467996 (good)
;; QUESTION SECTION:
;www.certifiedhacker.com.      IN      A

;; ANSWER SECTION:
www.certifiedhacker.com. 14400  IN      CNAME   certifiedhacker.com.
certifiedhacker.com.       14400  IN      A       162.241.216.11
;; AUTHORITY SECTION:
certifiedhacker.com.     86400  IN      NS      ns2.bluehost.com.

[  ] Menu  sgpt--chatenum--sh...
```

11. Run **sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on the target domain www.certifiedhacker.com using non-recursive method. Use DNS server IP as 162.241.216.11"** command.

In the prompt type **E** and press **Enter** to execute the command.

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

; <>> DiG 9.18.24-1-Debian <>> @162.241.216.11 www.certifiedhacker.com +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23855
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: acfad99c8af6fc3dce0a3f4a664afbd4c556cc50fd4fd75f (good)
;; QUESTION SECTION:
;www.certifiedhacker.com.      IN      A

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

;; AUTHORITY SECTION:
certifiedhacker.com.    86400  IN      NS       ns2.bluehost.com.
certifiedhacker.com.    86400  IN      NS       ns1.bluehost.com.
```

12. To perform IPsec enumeration using ShellGPT run **sgpt --shell “Perform IPsec enumeration on target IP 10.10.1.22 with Nmap”** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "sgpt --shell \"Perform IPsec enumeration on target IP 10.10.1.22 with Nmap\" - Parrot Terminal". The command run was "nmap -sU -p 500 --script=ike-version 10.10.1.22". The output indicates the host is up and shows a single open|filtered port 500/udp for isakmp. The MAC address is 00:15:5D:01:80:02 (Microsoft). The scan took 4.69 seconds.

```
sgpt --shell "Perform IPsec enumeration on target IP 10.10.1.22 with Nmap" - Parrot Terminal
[roo...@parrot]~[/home/attacker]
└─# sgpt --shell "Perform IPsec enumeration on target IP 10.10.1.22 with Nmap"
nmap -sU -p 500 --script=ike-version 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 03:33 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00047s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 4.69 seconds
[roo...@parrot]~[/home/attacker]
└─#
```

13. We will now perform SMB enumeration using ShellGPT, to do so, run **sgpt --shell “Scan the target IP 10.10.1.22 for the port using SMB with Nmap”** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "sgpt --shell \"Scan the target IP 10.10.1.22 for the port using SMB with Nmap\" - Parrot Terminal". The terminal window displays a custom script named sgpt. The script uses the nmap command to scan port 445 of the target IP 10.10.1.22, specifically looking for SMB protocols and OS discovery. The output shows that the host is up and that port 445/tcp is open, serving the Microsoft-DS service. The host's MAC address is 00:15:5D:01:80:02 (Microsoft). The script then performs SMB protocol dialects enumeration, listing various versions from NT LM 0.12 to 3:1:1. It also performs OS discovery, identifying the target as Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3), with computer name Server2022, NetBIOS computer name SERVER2022\x00, and domain name CEH.com.

```
sgpt --shell "Scan the target IP 10.10.1.22 for the port using SMB with Nmap"
nmap -p 445 --script smb-protocols,smb-os-discovery 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 03:40 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00042s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2:0:2
|     2:1:0
|     3:0:0
|     3:0:2
|     3:1:1
| smb-os-discovery:
|   OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
|   Computer name: Server2022
|   NetBIOS computer name: SERVER2022\x00
|   Domain name: CEH.com
```

14. To create and execute a custom script to automate network enumeration tasks run **sgpt --chat enum --shell** “Develop and execute a script which will automate various network enumeration tasks on target IP range 10.10.1.0/24” command.

In the prompt type **E** and press **Enter** to execute the command.

```
Applications Places System Mon May 20, 03:50
sgpt --chat enum --shell "Develop and execute a script which will automate various network enumeration tasks on target IP range 10.10.1.0/24"
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#sgpt --chat enum --shell "Develop and execute a script which will automate various network enumeration tasks on target IP range 10.10.1.0/24"
cat << 'EOF' > network_enum.sh
#!/bin/bash
nmap -sn 10.10.1.0/24 -oG - | awk '/Up$/ {print $2}' > live_hosts.txt
nmap -sV -iL live_hosts.txt -oA service_scan
nmap -O -iL live_hosts.txt -oA os_scan
nmap -p- -iL live_hosts.txt -oA full_port_scan
EOF

chmod +x network_enum.sh && ./network_enum.sh
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 03:48 EDT
Nmap scan report for 10.10.1.2
Host is up (0.00061s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  Unbound
88/tcp    open  http   nginx
MAC Address: 02:15:5D:20:BB:86 (Unknown)

Nmap scan report for 10.10.1.9
Host is up (0.00055s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
Menu  sgpt--chatenum--sh...
```

15. We will perform LDAP enumeration using ShellGPT, to do so, run **sgpt --shell "Use nmap script to perform ldap-brute-force on IP 10.10.1.22"** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "sgpt --shell \"Use nmap script to perform ldap-brute-force on IP 10.10.1.22\" - Parrot Terminal". The terminal content is as follows:

```
[root@parrot]~[~/home/attacker]
└─# sgpt --shell "Use nmap script to perform ldap-brute-force on IP 10.10.1.22"
nmap -p 389 --script ldap-brute --script-args ldap-brute.hostname=10.10.1.22 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 05:17 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00042s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
[root@parrot]~[~/home/attacker]
└─#
```

16. To perform FTP enumeration, run **sgpt --shell "Use Nmap to perform FTP Enumeration on www.certifiedhacker.com"** command.

In the prompt type **E** and press **Enter** to execute the command.

The screenshot shows a terminal window titled "sgpt --shell \"Use Nmap to perform FTP Enumeration on www.certifiedhacker.com\" - Parrot Terminal". The command run was "nmap -sV --script=ftp-anon,ftp-bounce,ftp-libopie,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-vuln-cve2010-4221 www.certifiedhacker.com". The output indicates the host is up with 0.15s latency. It shows various open ports including 21/tcp (FTP), 22/tcp (SSH), 25/tcp (SMTP), 80/tcp (HTTP), and 443/tcp (SSL/TLS). The Apache server header is identified as "Apache/2.4.41". The SMTP service is Exim 4.96.2.

```
[root@parrot]~[~/home/attacker]
#sgpt --shell "Use Nmap to perform FTP Enumeration on www.certifiedhacker.com"
nmap -sV --script=ftp-anon,ftp-bounce,ftp-libopie,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-vuln-cve2010-4221 www.certifiedhacker.com
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 05:30 EDT
Nmap scan report for www.certifiedhacker.com (162.241.216.11)
Host is up (0.15s latency).

rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 981 closed tcp ports (reset)

PORT      STATE     SERVICE      VERSION
21/tcp    open      ftp         Pure-FTPD
22/tcp    open      ssh         OpenSSH 7.4 (protocol 2.0)
25/tcp    open      smtp        Exim smtpd 4.96.2
26/tcp    open      smtp        Exim smtpd 4.96.2
53/tcp    open      domain     ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp    open      http        Apache httpd
|_http-server-header: Apache
110/tcp   open      pop3       Dovecot pop3d
143/tcp   open      imap       Dovecot imapd
443/tcp   open      ssl/http   Apache httpd
| http-server-header:
|   Apache
|_ nginx/1.21.6
465/tcp   open      tcpwrapped
587/tcp   open      smtp       Exim smtpd 4.96.2
```

17. The result appears showing the open ports present on the website, you can see that the **port 21** on which FTP service is running is open.
18. Apart from the aforementioned commands, you can further explore additional options within the ShellGPT tool and utilize various other tools to conduct enumeration on the target.
19. This concludes the demonstration of performing enumeration using ShellGPT.
20. Close all open windows and document all the acquired information.

#### Question 4.8.1.1

In Parrot Security machine write a ShellGPT prompt and execute it to perform SMB enumeration on Windows Server 2022 machine (10.10.1.22), Identify the service that is running on port 445 in Windows Server 2022 machine.