Lab 6: Perform Network Scanning using AI

Lab Scenario

As ethical hackers and penetration testers, it is crucial to leverage advanced tools and techniques to uncover hidden vulnerabilities in target networks. This lab focuses on utilizing AI-powered network scanning tools like ShellGPT to gather comprehensive information about systems within the target network.

Lab Objectives

- Scan a target using ShellGPT

Overview of Network Scanning using AI

Network scanning using AI enhances cybersecurity by automating the detection of vulnerabilities and threats. AI-driven tools analyze network traffic, identify anomalies, and predict potential attacks with high accuracy, providing proactive defense mechanisms and reducing response times for cybersecurity teams.

Task 1: Scan a Target using ShellGPT

ShellGPT is an AI-powered tool that can assist in scanning networks by automating tasks such as identifying active devices, detecting open ports, and analyzing network vulnerabilities. It leverages advanced algorithms to provide efficient, real-time insights, ensuring network security and performance optimization.

Here, we will use ShellGPT to discover active hosts, open ports, services running, and OS details of systems present in the target network.

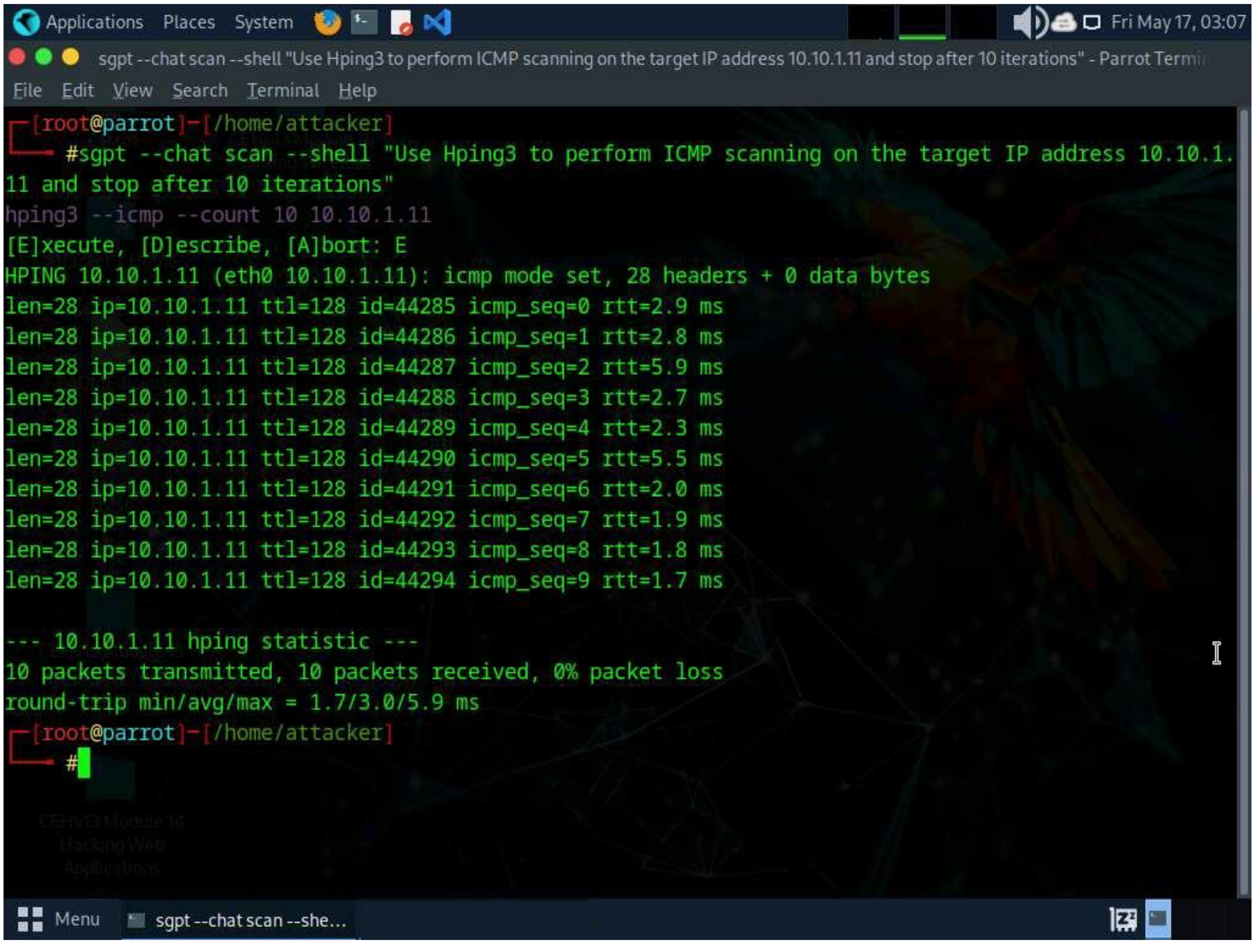
The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the 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** and login as **toor**. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**), 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 --chat scan --shell “Use hping3 to perform ICMP scanning on the target IP address 10.10.1.11 and stop after 10 iterations”** to perform ICMP scan on target IP address.

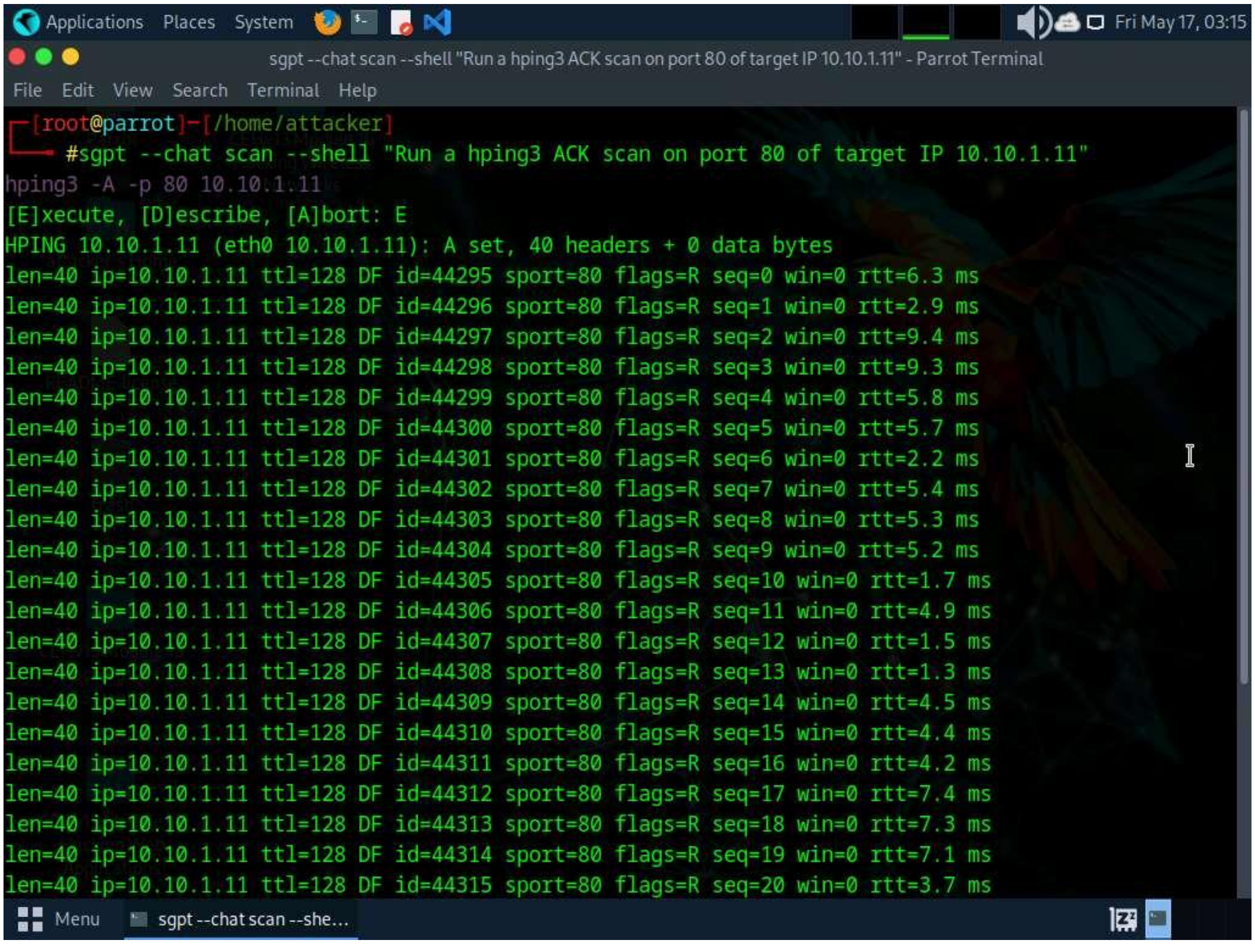
In the prompt type **E** and press **Enter** to execute the command.


Applications
Places
System
Fri May 17, 03:07
sgpt --chat scan --shell "Use Hping3 to perform ICMP scanning on the target IP address 10.10.1.11 and stop after 10 iterations" - Parrot Termi
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat scan --she...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Use Hping3 to perform ICMP scanning on the target IP address 10.10.1.
11 and stop after 10 iterations"
hping3 --icmp --count 10 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
HPING 10.10.1.11 (eth0 10.10.1.11): icmp mode set, 28 headers + 0 data bytes
len=28 ip=10.10.1.11 ttl=128 id=44285 icmp_seq=0 rtt=2.9 ms
len=28 ip=10.10.1.11 ttl=128 id=44286 icmp_seq=1 rtt=2.8 ms
len=28 ip=10.10.1.11 ttl=128 id=44287 icmp_seq=2 rtt=5.9 ms
len=28 ip=10.10.1.11 ttl=128 id=44288 icmp_seq=3 rtt=2.7 ms
len=28 ip=10.10.1.11 ttl=128 id=44289 icmp_seq=4 rtt=2.3 ms
len=28 ip=10.10.1.11 ttl=128 id=44290 icmp_seq=5 rtt=5.5 ms
len=28 ip=10.10.1.11 ttl=128 id=44291 icmp_seq=6 rtt=2.0 ms
len=28 ip=10.10.1.11 ttl=128 id=44292 icmp_seq=7 rtt=1.9 ms
len=28 ip=10.10.1.11 ttl=128 id=44293 icmp_seq=8 rtt=1.8 ms
len=28 ip=10.10.1.11 ttl=128 id=44294 icmp_seq=9 rtt=1.7 ms

--- 10.10.1.11 hping statistic ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 1.7/3.0/5.9 ms
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

3. Now, run **sgpt --chat scan --shell “Run a hping3 ACK scan on port 80 of target IP 10.10.1.11”** command to perform ACK scan on target IP address.

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


Applications
Places
System
Fri May 17, 03:15
sgpt --chat scan --shell "Run a hping3 ACK scan on port 80 of target IP 10.10.1.11" - Parrot Terminal
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat scan --she...

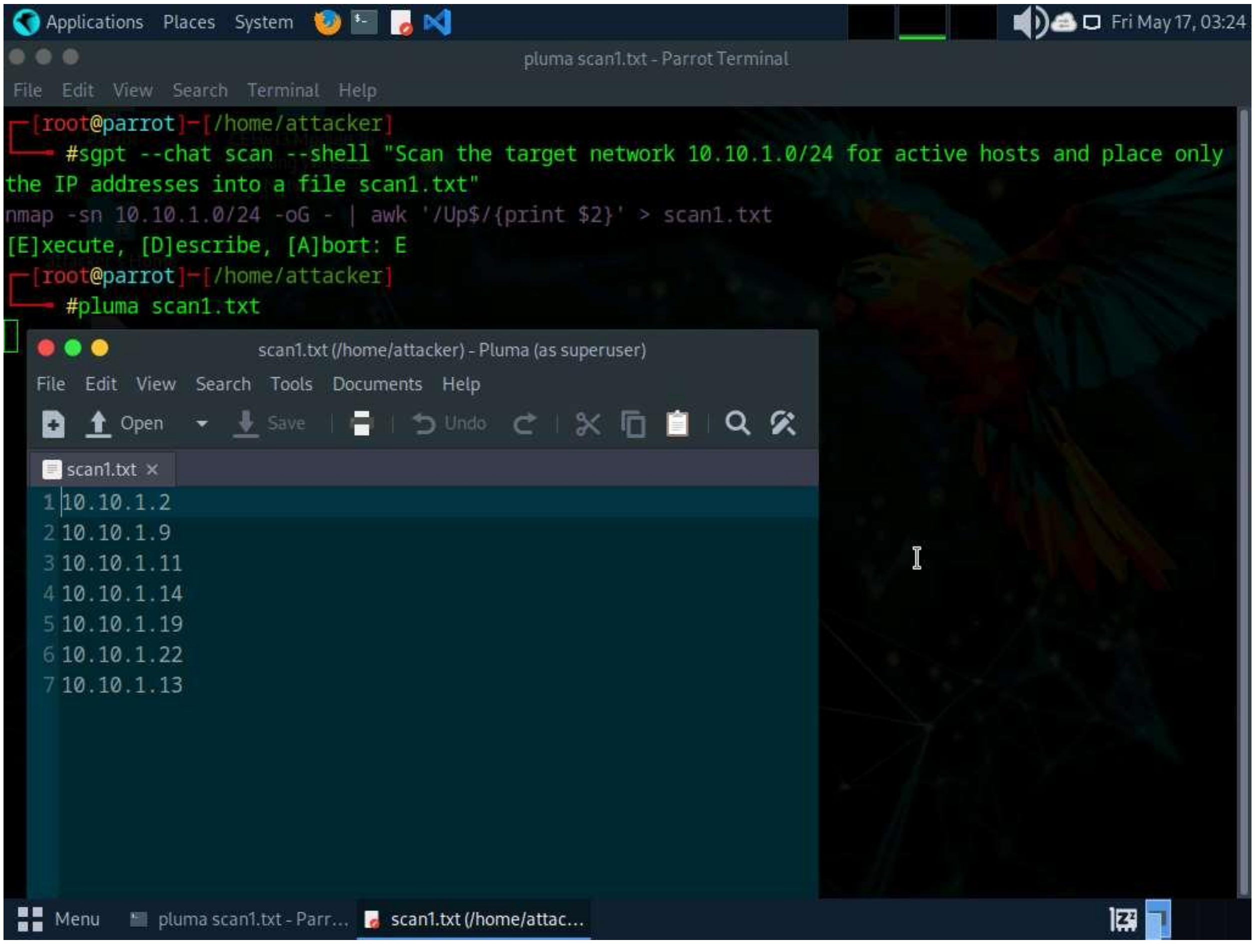
```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Run a hping3 ACK scan on port 80 of target IP 10.10.1.11"
hping3 -A -p 80 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
HPING 10.10.1.11 (eth0 10.10.1.11): A set, 40 headers + 0 data bytes
len=40 ip=10.10.1.11 ttl=128 DF id=44295 sport=80 flags=R seq=0 win=0 rtt=6.3 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44296 sport=80 flags=R seq=1 win=0 rtt=2.9 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44297 sport=80 flags=R seq=2 win=0 rtt=9.4 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44298 sport=80 flags=R seq=3 win=0 rtt=9.3 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44299 sport=80 flags=R seq=4 win=0 rtt=5.8 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44300 sport=80 flags=R seq=5 win=0 rtt=5.7 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44301 sport=80 flags=R seq=6 win=0 rtt=2.2 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44302 sport=80 flags=R seq=7 win=0 rtt=5.4 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44303 sport=80 flags=R seq=8 win=0 rtt=5.3 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44304 sport=80 flags=R seq=9 win=0 rtt=5.2 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44305 sport=80 flags=R seq=10 win=0 rtt=1.7 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44306 sport=80 flags=R seq=11 win=0 rtt=4.9 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44307 sport=80 flags=R seq=12 win=0 rtt=1.5 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44308 sport=80 flags=R seq=13 win=0 rtt=1.3 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44309 sport=80 flags=R seq=14 win=0 rtt=4.5 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44310 sport=80 flags=R seq=15 win=0 rtt=4.4 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44311 sport=80 flags=R seq=16 win=0 rtt=4.2 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44312 sport=80 flags=R seq=17 win=0 rtt=7.4 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44313 sport=80 flags=R seq=18 win=0 rtt=7.3 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44314 sport=80 flags=R seq=19 win=0 rtt=7.1 ms
len=40 ip=10.10.1.11 ttl=128 DF id=44315 sport=80 flags=R seq=20 win=0 rtt=3.7 ms
```

4. Press **Ctrl + C** to stop the scan.

5. Run **sgpt --chat scan --shell "Scan the target network 10.10.1.0/24 for active hosts and place only the IP addresses into a file scan1.txt”** to perform host discovery.

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

6. Now run **pluma scan1.txt** command to open scan1.txt file and view the IP addresses of active hosts in the target subnet.

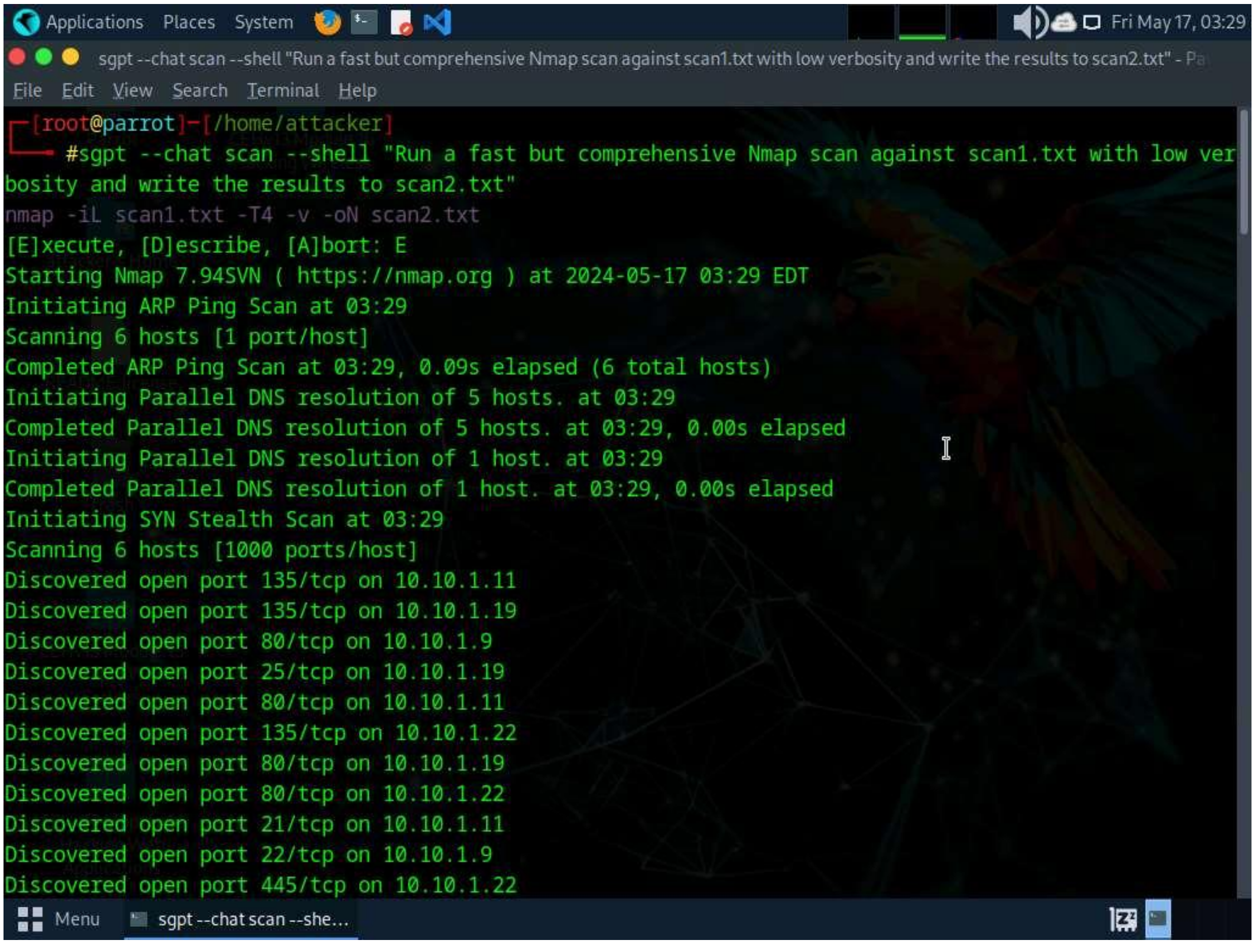

Applications
Places
System
Fri May 17, 03:24
pluma scan1.txt - Parrot Terminal
File Edit View Search Terminal Help
scan1.txt (/home/attacker) - Pluma (as superuser)
File Edit View Search Tools Documents Help
Open
Save
Undo
scan1.txt
Menu
pluma scan1.txt - Parr...
scan1.txt (/home/attac...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Scan the target network 10.10.1.0/24 for active hosts and place only the IP addresses into a file scan1.txt"
nmap -sn 10.10.1.0/24 -oG - | awk '/Up$/{print $2}' > scan1.txt
[E]xecute, [D]escribe, [A]bort: E
┌─[root@parrot]─[/home/attacker]
└──╼ #pluma scan1.txt
```

```
10.10.1.2
10.10.1.9
10.10.1.11
10.10.1.14
10.10.1.19
10.10.1.22
10.10.1.13
```

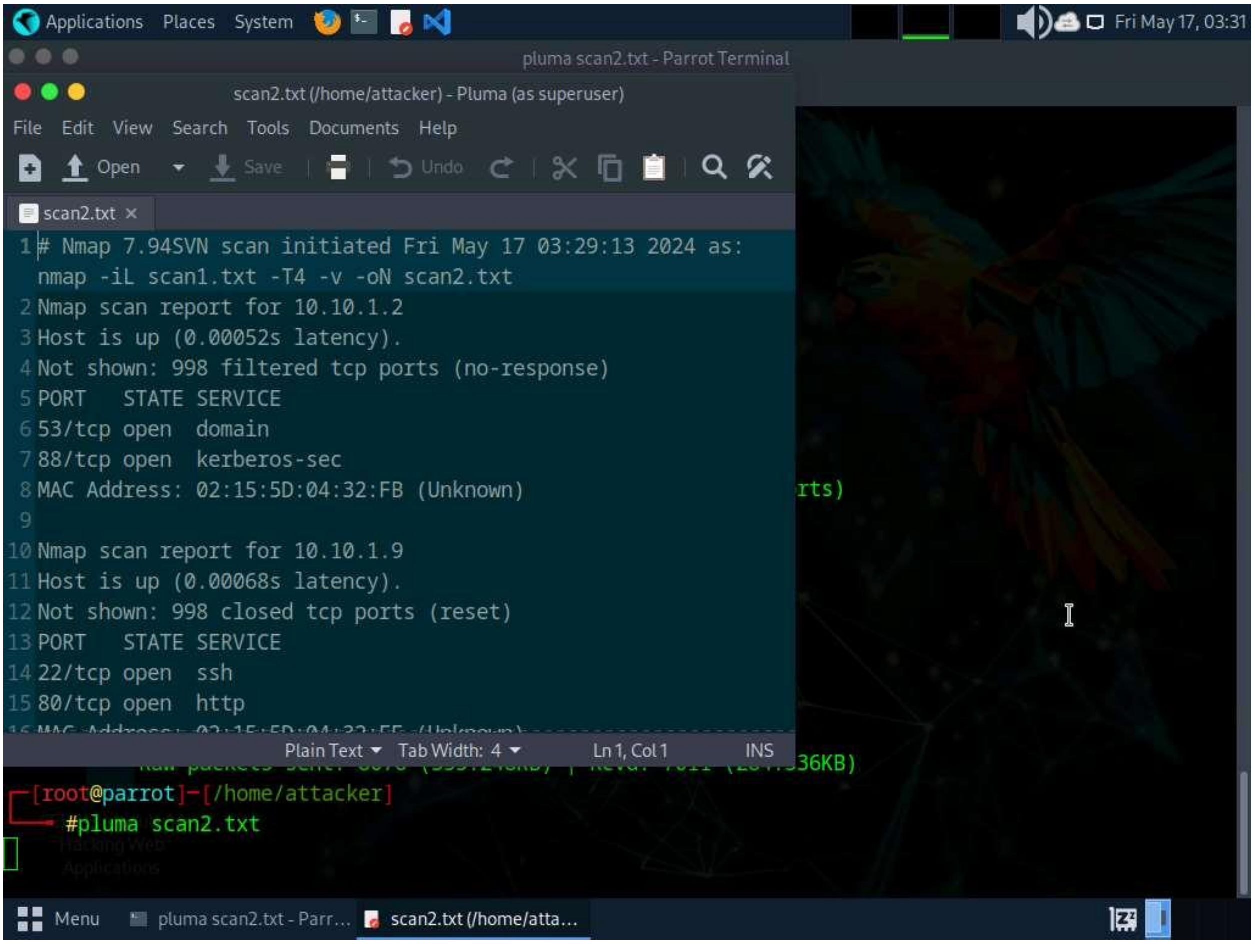
7. Close the text editor window.
8. To perform nmap scan against the IP addresses that were gathered in previous step run **sgpt --chat scan --shell "Run a fast but comprehensive nmap scan against scan1.txt with low verbosity and write the results to scan2.txt"** command.

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


Applications
Places
System
Fri May 17, 03:29
sgpt --chat scan --shell "Run a fast but comprehensive Nmap scan against scan1.txt with low verbosity and write the results to scan2.txt" - Pa
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat scan --she...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Run a fast but comprehensive Nmap scan against scan1.txt with low ver
bosity and write the results to scan2.txt"
nmap -iL scan1.txt -T4 -v -oN scan2.txt
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 03:29 EDT
Initiating ARP Ping Scan at 03:29
Scanning 6 hosts [1 port/host]
Completed ARP Ping Scan at 03:29, 0.09s elapsed (6 total hosts)
Initiating Parallel DNS resolution of 5 hosts. at 03:29
Completed Parallel DNS resolution of 5 hosts. at 03:29, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 03:29
Completed Parallel DNS resolution of 1 host. at 03:29, 0.00s elapsed
Initiating SYN Stealth Scan at 03:29
Scanning 6 hosts [1000 ports/host]
Discovered open port 135/tcp on 10.10.1.11
Discovered open port 135/tcp on 10.10.1.19
Discovered open port 80/tcp on 10.10.1.9
Discovered open port 25/tcp on 10.10.1.19
Discovered open port 80/tcp on 10.10.1.11
Discovered open port 135/tcp on 10.10.1.22
Discovered open port 80/tcp on 10.10.1.19
Discovered open port 80/tcp on 10.10.1.22
Discovered open port 21/tcp on 10.10.1.11
Discovered open port 22/tcp on 10.10.1.9
Discovered open port 445/tcp on 10.10.1.22
```

9. After the scan run **pluma scan2.txt** command to open scan2.txt file and view the scan results.

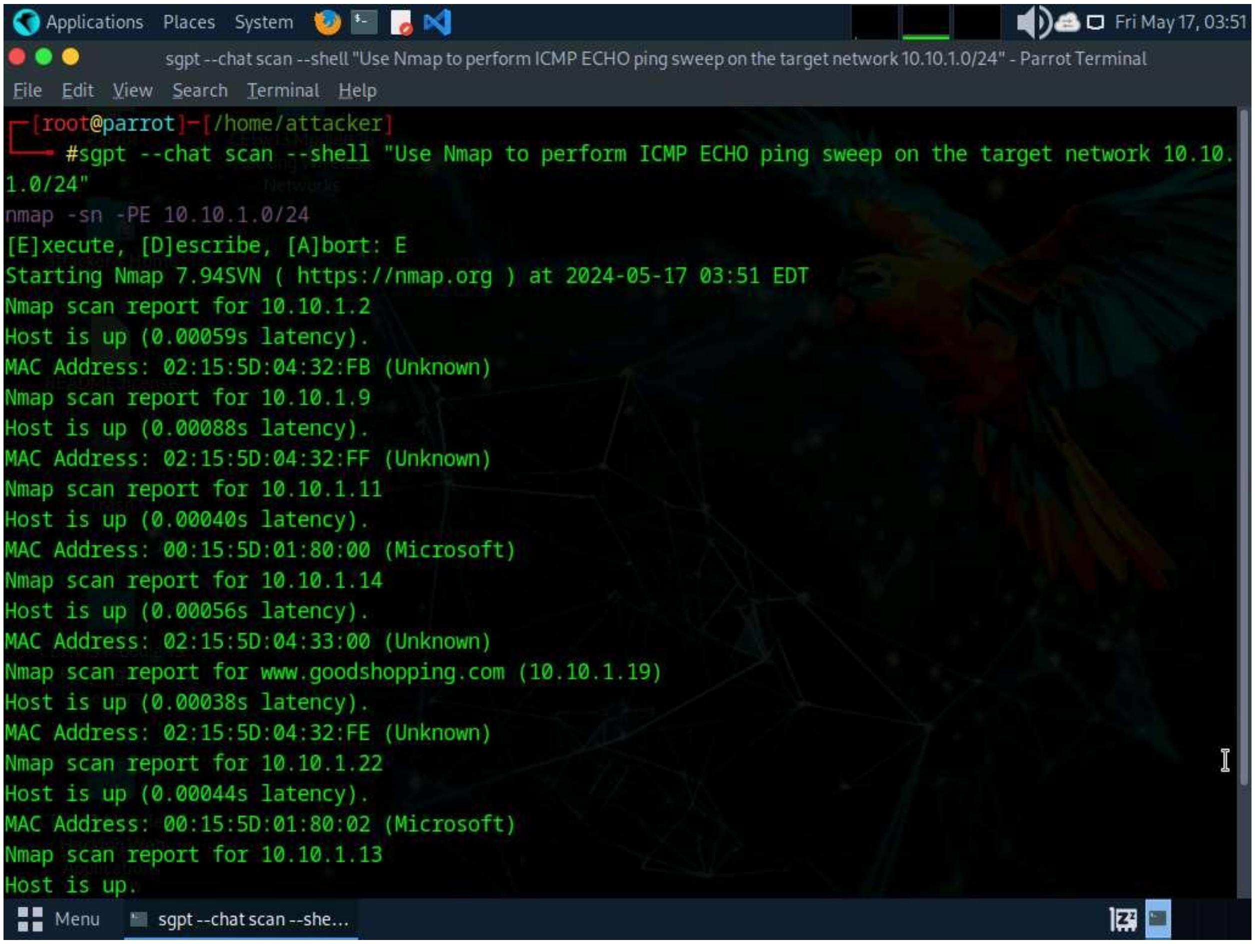


```
# Nmap 7.94SVN scan initiated Fri May 17 03:29:13 2024 as:
nmap -iL scan1.txt -T4 -v -oN scan2.txt
Nmap scan report for 10.10.1.2
Host is up (0.00052s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
88/tcp open  kerberos-sec
MAC Address: 02:15:5D:04:32:FB (Unknown)

Nmap scan report for 10.10.1.9
Host is up (0.00068s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

```
┌─[root@parrot]─[/home/attacker]
└──╼ #pluma scan2.txt
```

10. Close the text editor window.
11. Run **sgpt --chat scan --shell "Use nmap to perform ICMP ECHO ping sweep on the target network 10.10.1.0/24"** command to perform ICMP ECHO ping sweep on the target network.

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

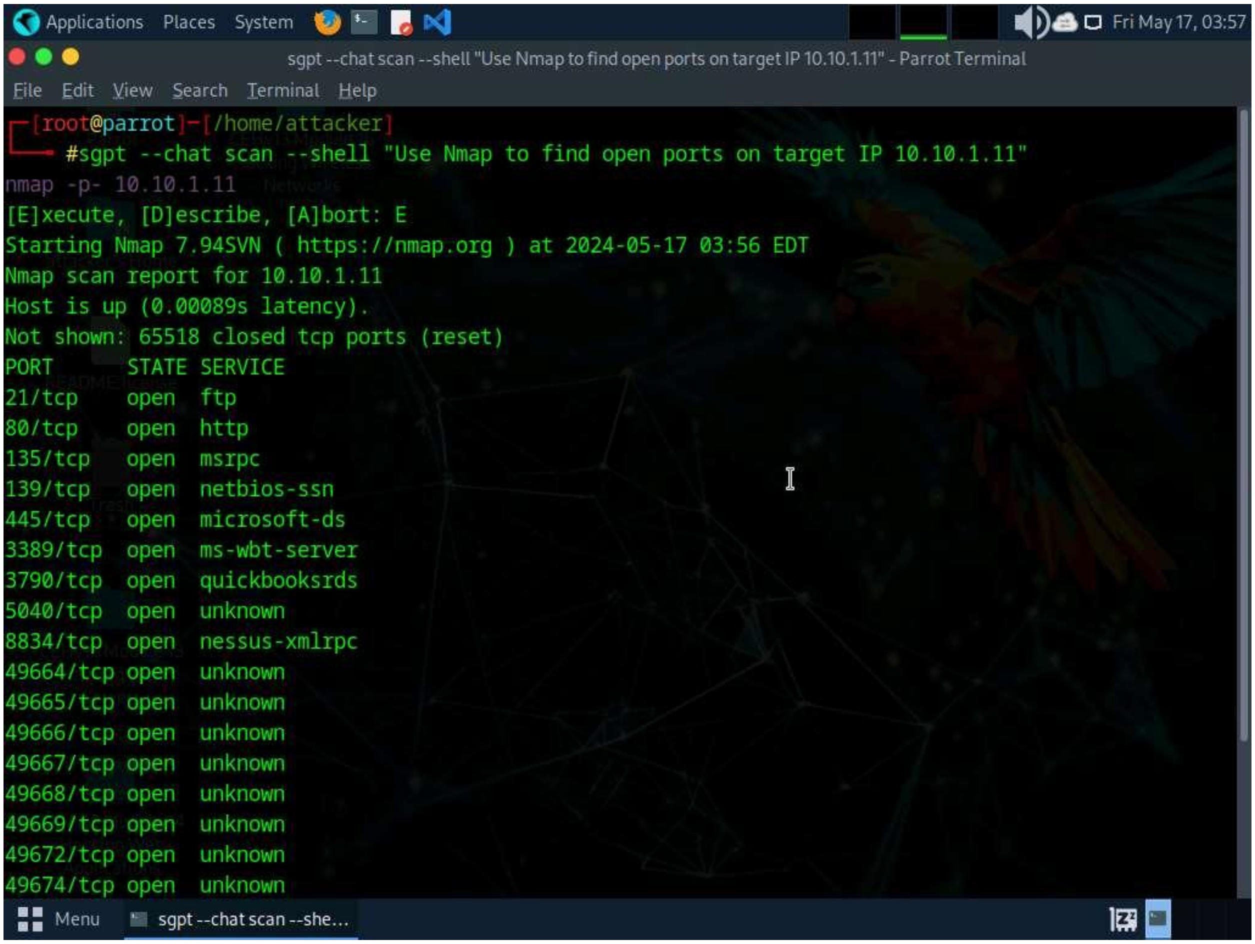

Applications Places System
Fri May 17, 03:51
sgpt --chat scan --shell "Use Nmap to perform ICMP ECHO ping sweep on the target network 10.10.1.0/24" - Parrot Terminal
File Edit View Search Terminal Help
Menu
sgpt --chat scan --she...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Use Nmap to perform ICMP ECHO ping sweep on the target network 10.10.
1.0/24"
nmap -sn -PE 10.10.1.0/24
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 03:51 EDT
Nmap scan report for 10.10.1.2
Host is up (0.00059s latency).
MAC Address: 02:15:5D:04:32:FB (Unknown)
Nmap scan report for 10.10.1.9
Host is up (0.00088s latency).
MAC Address: 02:15:5D:04:32:FF (Unknown)
Nmap scan report for 10.10.1.11
Host is up (0.00040s latency).
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap scan report for 10.10.1.14
Host is up (0.00056s latency).
MAC Address: 02:15:5D:04:33:00 (Unknown)
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00038s latency).
MAC Address: 02:15:5D:04:32:FE (Unknown)
Nmap scan report for 10.10.1.22
Host is up (0.00044s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap scan report for 10.10.1.13
Host is up.
```

12. Now, we will perform port scanning using ShellGPT to do so, run **sgpt --chat scan --shell "Use nmap to find open ports on target IP 10.10.1.11"** command.

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

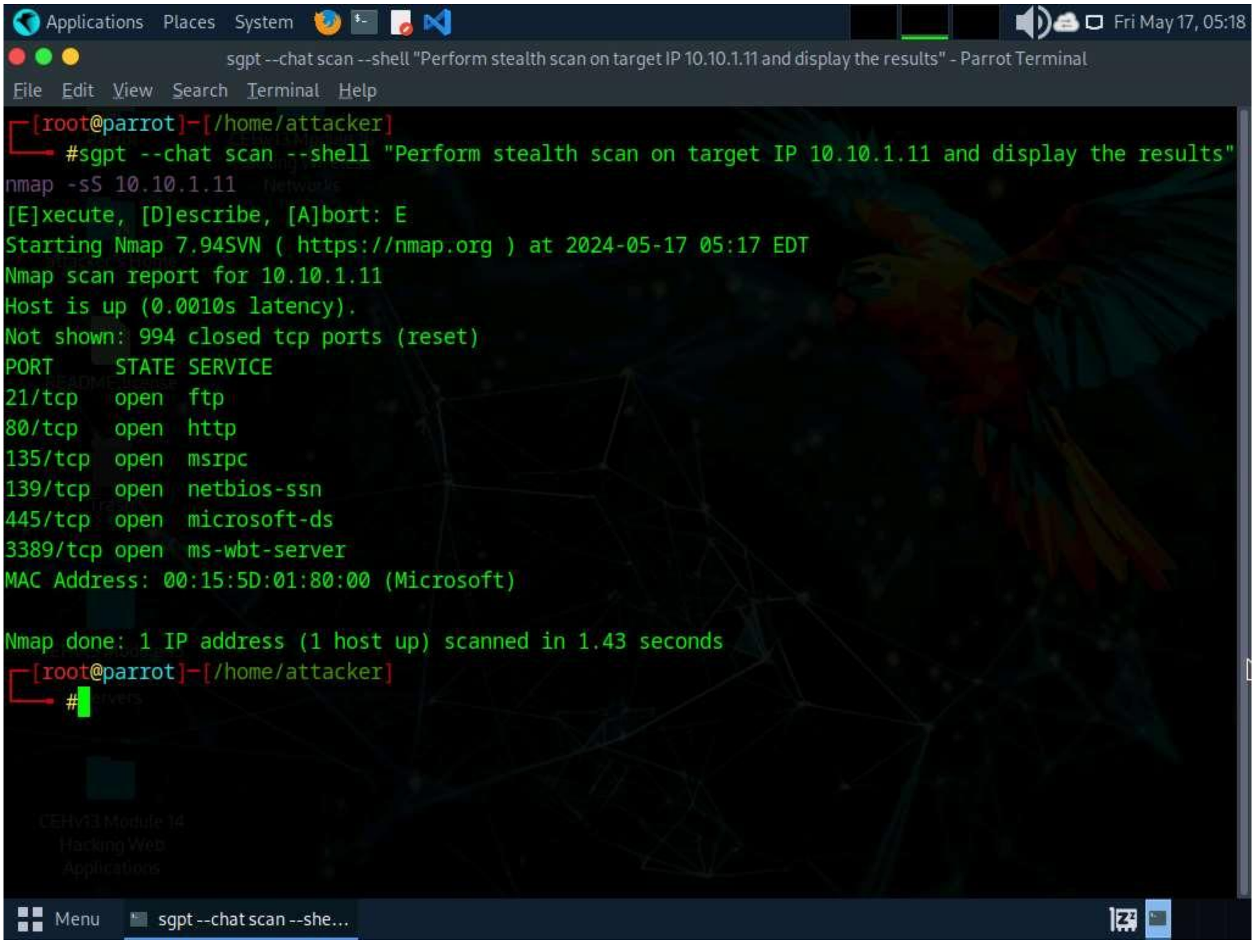
13. The scan results will appear displaying all the open ports, pertaining to the target IP address.


Applications
Places
System
Fri May 17, 03:57
sgpt --chat scan --shell "Use Nmap to find open ports on target IP 10.10.1.11" - Parrot Terminal
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat scan --she...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Use Nmap to find open ports on target IP 10.10.1.11"
nmap -p- 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 03:56 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00089s latency).
Not shown: 65518 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3790/tcp  open  quickbooksrds
5040/tcp  open  unknown
8834/tcp  open  nessus-xmlrpc
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49672/tcp open  unknown
49674/tcp open  unknown
```

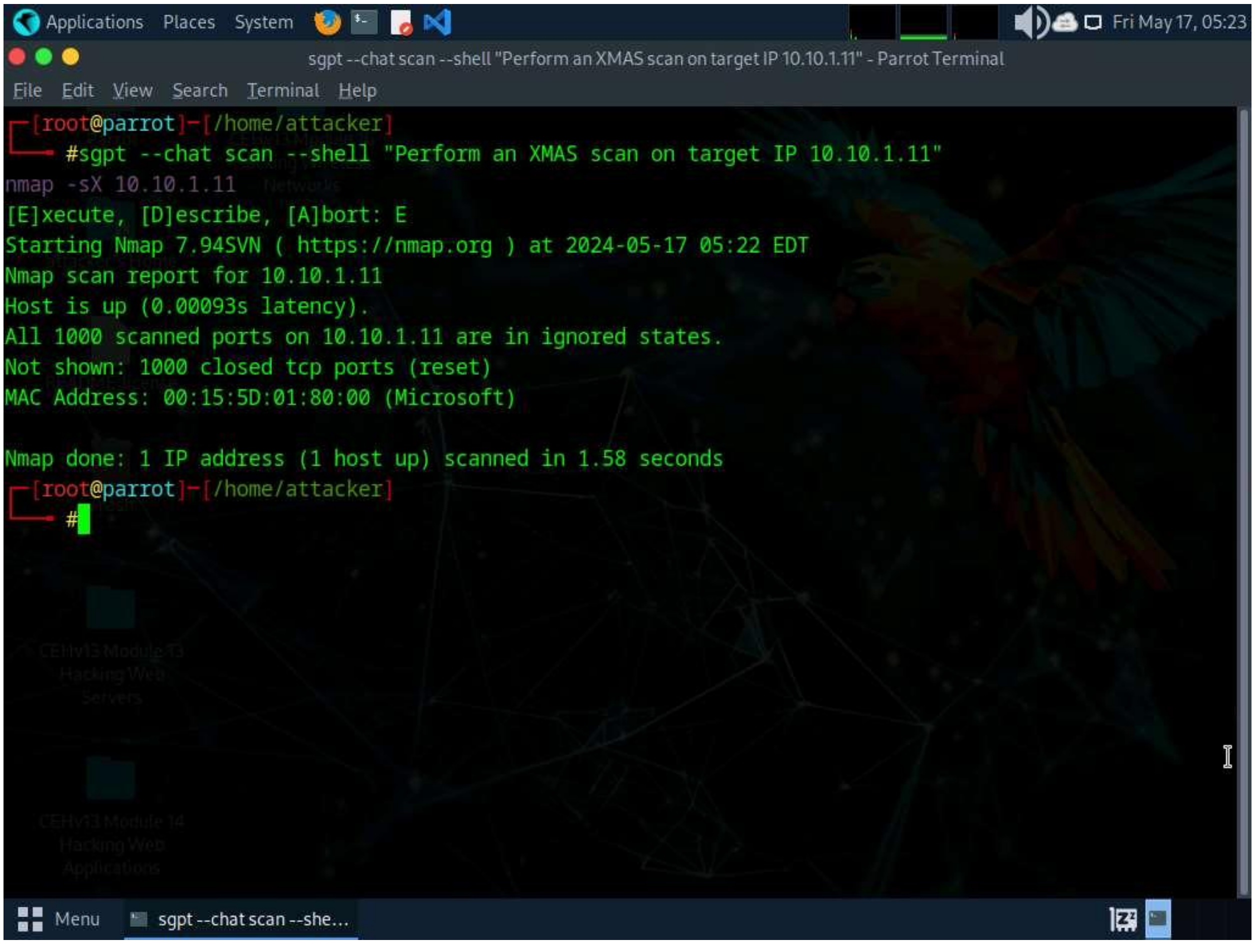
14. Now, we will perform stealth scan on a target IP, to do so, run **sgpt --chat scan --shell "Perform stealth scan on target IP 10.10.1.11 and display the results"** command.

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


Applications Places System
Fri May 17, 05:18
sgpt --chat scan --shell "Perform stealth scan on target IP 10.10.1.11 and display the results" - Parrot Terminal
File Edit View Search Terminal Help
Menu
sgpt --chat scan --she...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Perform stealth scan on target IP 10.10.1.11 and display the results"
nmap -sS 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 05:17 EDT
Nmap scan report for 10.10.1.11
Host is up (0.0010s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

15. To perform XMAS scan on a target IP address, run **sgpt --chat scan --shell "Perform an XMAS scan on target IP 10.10.1.11"** command.

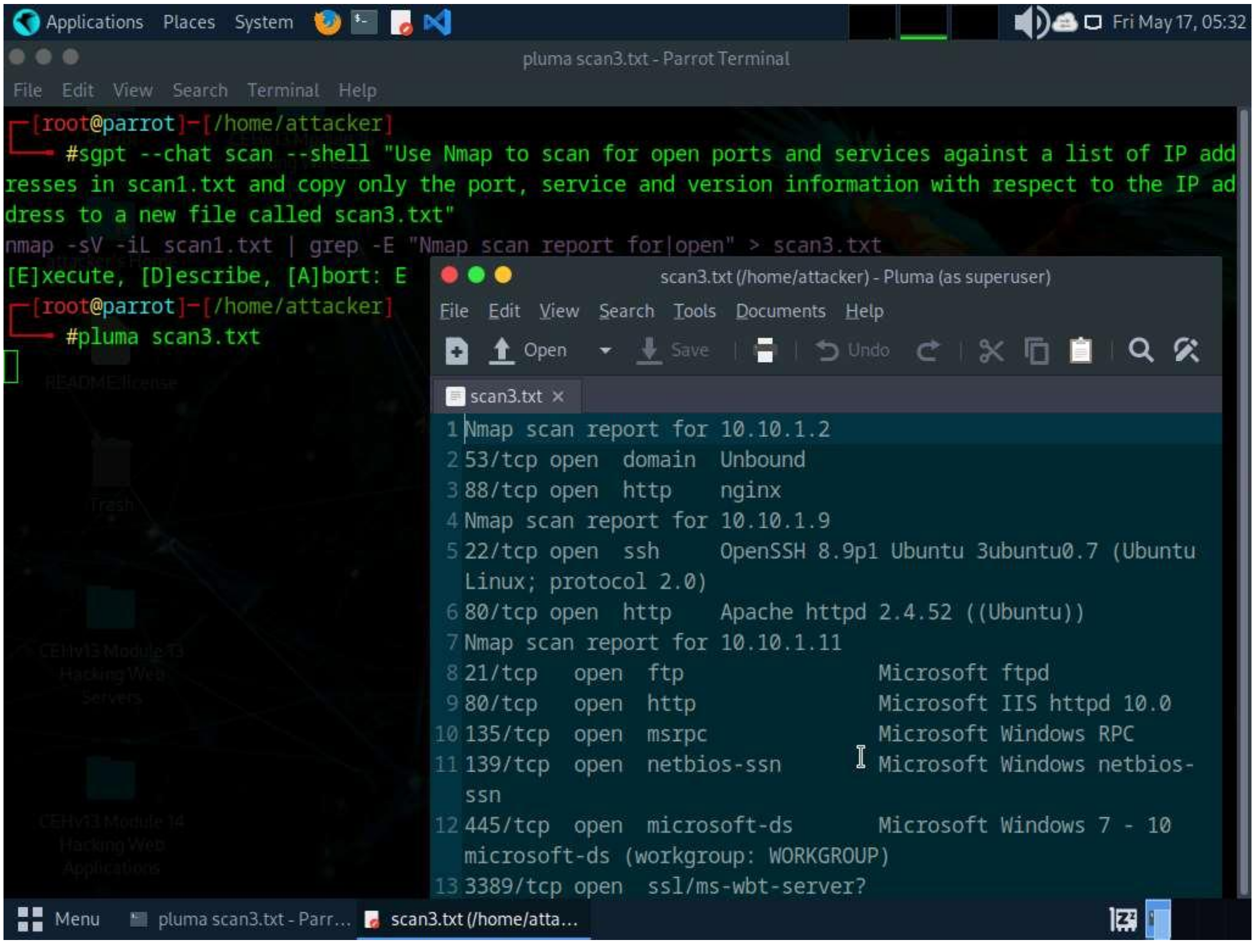

Applications
Places
System
Fri May 17, 05:23
sgpt --chat scan --shell "Perform an XMAS scan on target IP 10.10.1.11" - Parrot Terminal
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat scan --she...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Perform an XMAS scan on target IP 10.10.1.11"
nmap -sX 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 05:22 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00093s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

16. Run **sgpt --chat scan --shell “Use Nmap to scan for open ports and services against a list of IP addresses in scan1.txt and copy only the port, service and version information with the respective IP address to a new file called scan3.txt”** command to scan for open services and ports against the list of IP addresses acquired in **Step#6**.

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

17. Once the scan is finished run **pluma scan3.txt** command to view the scan results.

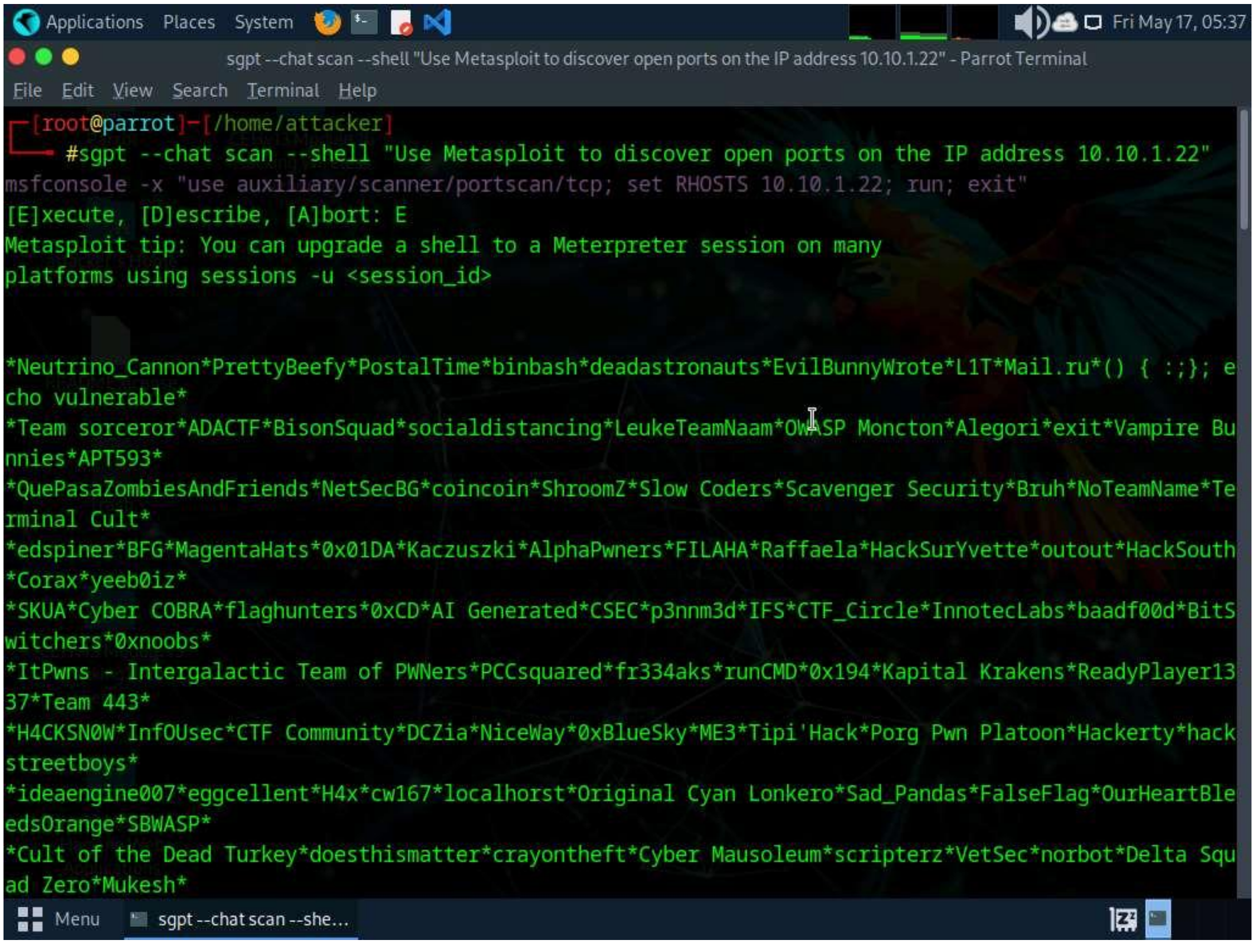

Applications Places System
Fri May 17, 05:32
pluma scan3.txt - Parrot Terminal
File Edit View Search Terminal Help
scan3.txt (/home/attacker) - Pluma (as superuser)
File Edit View Search Tools Documents Help
Open Save Undo
scan3.txt
Menu
pluma scan3.txt - Parr...
scan3.txt (/home/atta...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Use Nmap to scan for open ports and services against a list of IP add
resses in scan1.txt and copy only the port, service and version information with respect to the IP ad
dress to a new file called scan3.txt"
nmap -sV -iL scan1.txt | grep -E "Nmap scan report for|open" > scan3.txt
[E]xecute, [D]escribe, [A]bort: E
┌─[root@parrot]─[/home/attacker]
└──╼ #pluma scan3.txt
```

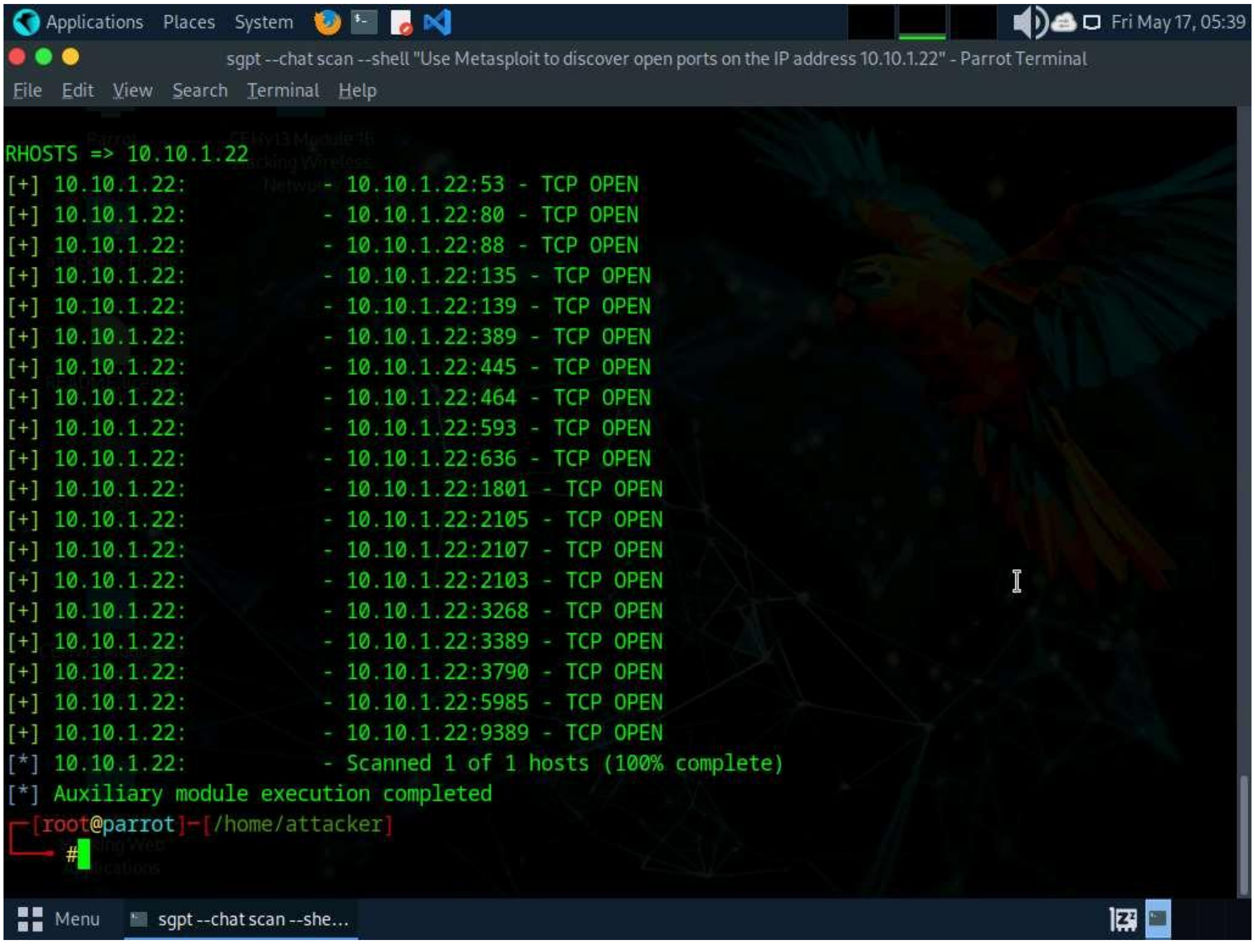
```
Nmap scan report for 10.10.1.2
53/tcp open  domain  Unbound
88/tcp open  http    nginx
Nmap scan report for 10.10.1.9
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
Nmap scan report for 10.10.1.11
21/tcp    open  ftp                Microsoft ftpd
80/tcp    open  http               Microsoft IIS httpd 10.0
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp open  ssl/ms-wbt-server?
```

18. Close the text editor window.
19. Now we will use Metasploit to discover open ports on a target system, run **sgpt --chat scan --shell "Use Metasploit to discover open ports on the IP address 10.10.1.22"** command.

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


Applications
Places
System
Fri May 17, 05:37
sgpt --chat scan --shell "Use Metasploit to discover open ports on the IP address 10.10.1.22" - Parrot Terminal
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat scan --she...

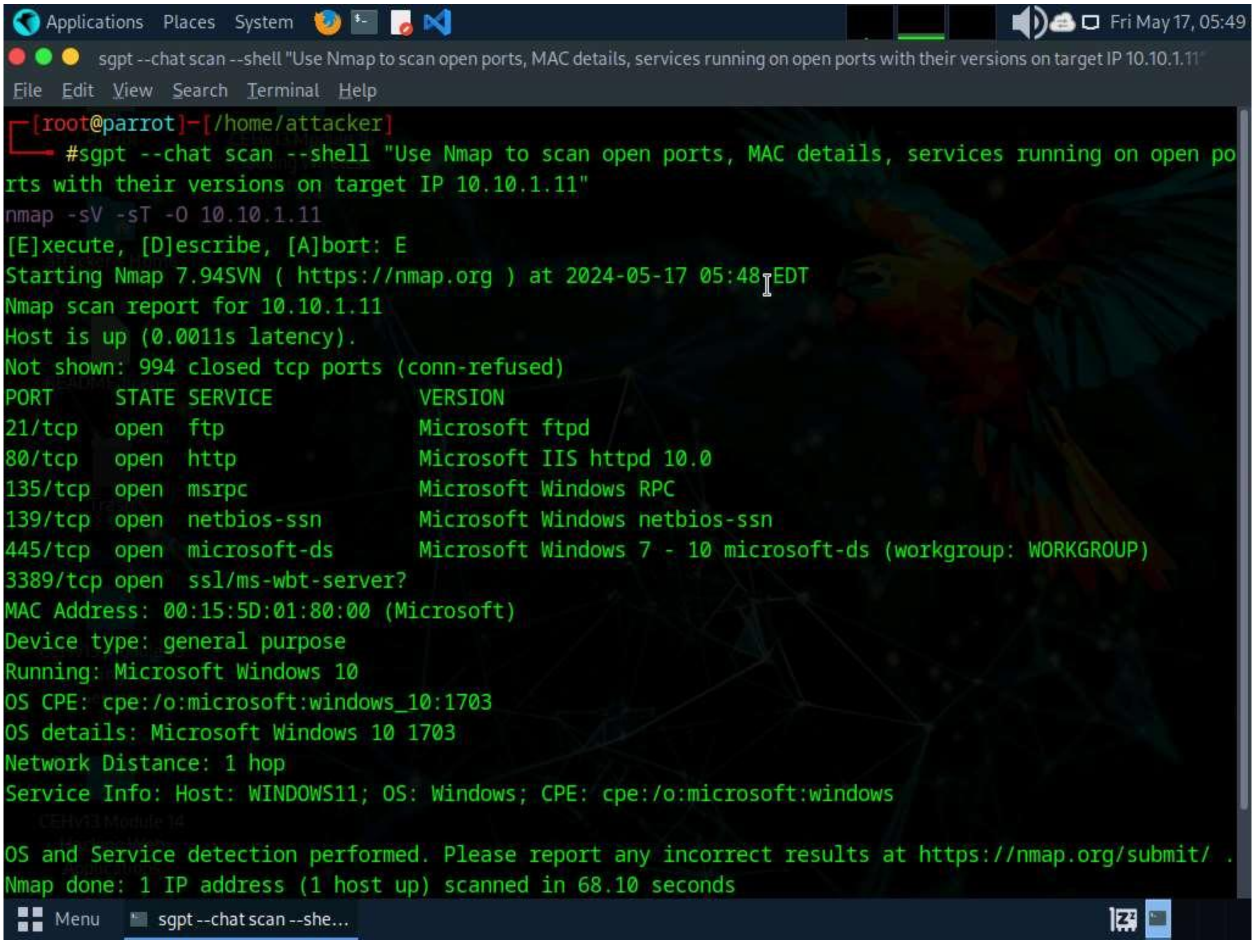
```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Use Metasploit to discover open ports on the IP address 10.10.1.22"
msfconsole -x "use auxiliary/scanner/portscan/tcp; set RHOSTS 10.10.1.22; run; exit"
[E]xecute, [D]escribe, [A]bort: E
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>


*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; e
cho vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bu
nnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Te
rminal Cult*
*edspiner*BFG*MagentaHats*0x01DA*Kaczuszki*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth
*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baadf00d*BitS
witchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer13
37*Team 443*
*H4CKSN0W*InfOUsec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hack
streetboys*
*ideaengine007*eggcellent*H4x*cw167*localhorst*Original Cyan Lonkero*Sad_Pandas*FalseFlag*OurHeartBle
edsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squ
ad Zero*Mukesh*
```


Applications Places System
Fri May 17, 05:39
sgpt --chat scan --shell "Use Metasploit to discover open ports on the IP address 10.10.1.22" - Parrot Terminal
File Edit View Search Terminal Help
Menu
sgpt --chat scan --she...

```
RHOSTS => 10.10.1.22
[+] 10.10.1.22:          - 10.10.1.22:53 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:80 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:88 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:135 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:139 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:389 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:445 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:464 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:593 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:636 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:1801 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:2105 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:2107 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:2103 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:3268 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:3389 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:3790 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:5985 - TCP OPEN
[+] 10.10.1.22:          - 10.10.1.22:9389 - TCP OPEN
[*] 10.10.1.22:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

20. To perform service version discovery on a target system run **sgpt --chat scan --shell “Use Nmap to scan open ports, MAC details, services running on open ports with their versions on target IP 10.10.1.11”** command.

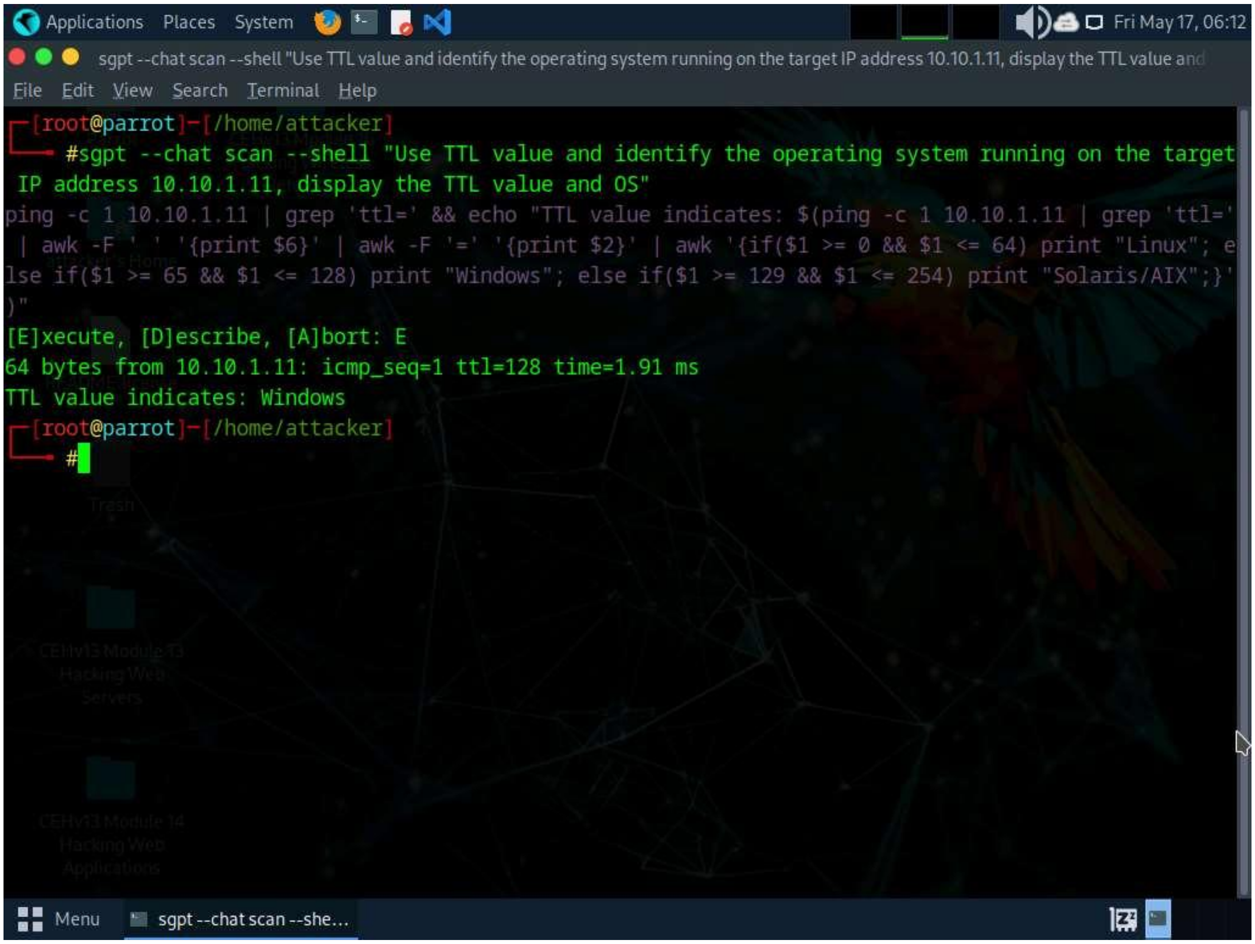
In the prompt type **E** and press **Enter** to execute the command.


Applications Places System
Fri May 17, 05:49
sgpt --chat scan --shell "Use Nmap to scan open ports, MAC details, services running on open ports with their versions on target IP 10.10.1.11
File Edit View Search Terminal Help
Menu
sgpt --chat scan --she...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Use Nmap to scan open ports, MAC details, services running on open po
rts with their versions on target IP 10.10.1.11"
nmap -sV -sT -O 10.10.1.11
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 05:48 EDT
Nmap scan report for 10.10.1.11
Host is up (0.0011s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE            VERSION
21/tcp   open  ftp                Microsoft ftpd
80/tcp   open  http               Microsoft IIS httpd 10.0
135/tcp  open  msrpc              Microsoft Windows RPC
139/tcp  open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds       Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp open  ssl/ms-wbt-server?
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
Network Distance: 1 hop
Service Info: Host: WINDOWS11; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.10 seconds
```

21. We will now perform OS discovery using ShellGPT, to do so run **sgpt --chat scan --shell "Use TTL value and identify the operating system running on the target IP address 10.10.1.11, display the TTL value and OS"** command.

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

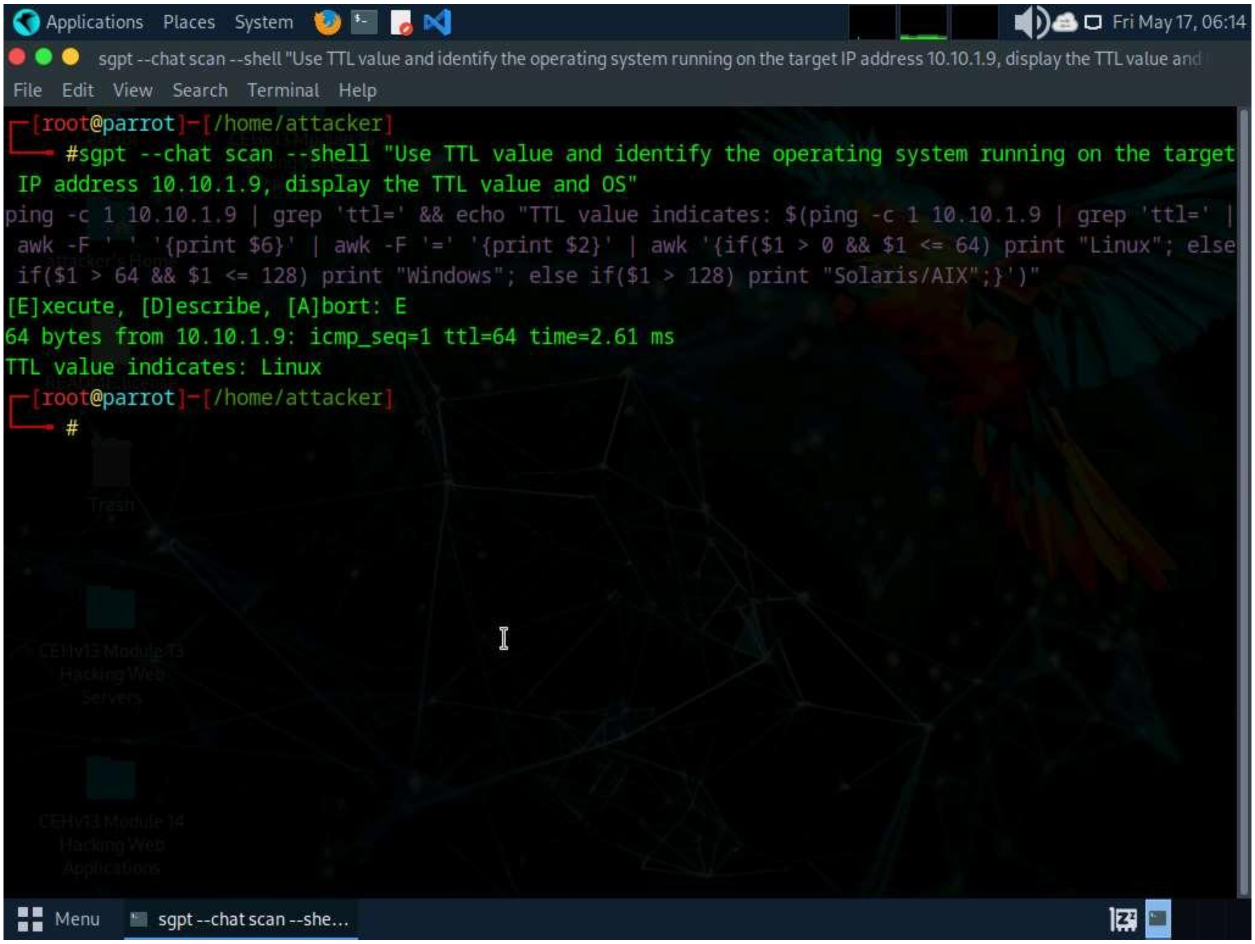


Applications Places System
Fri May 17, 06:12
sgpt --chat scan --shell "Use TTL value and identify the operating system running on the target IP address 10.10.1.11, display the TTL value and
File Edit View Search Terminal Help
Menu
sgpt --chat scan --she...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Use TTL value and identify the operating system running on the target
 IP address 10.10.1.11, display the TTL value and OS"
ping -c 1 10.10.1.11 | grep 'ttl=' && echo "TTL value indicates: $(ping -c 1 10.10.1.11 | grep 'ttl='
 | awk -F ' ' '{print $6}' | awk -F '=' '{print $2}' | awk '{if($1 >= 0 && $1 <= 64) print "Linux"; e
lse if($1 >= 65 && $1 <= 128) print "Windows"; else if($1 >= 129 && $1 <= 254) print "Solaris/AIX";}'
)"
[E]xecute, [D]escribe, [A]bort: E
64 bytes from 10.10.1.11: icmp_seq=1 ttl=128 time=1.91 ms
TTL value indicates: Windows
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

22. Run **sgpt --chat scan --shell "Use TTL value and identify the operating system running on the target IP address 10.10.1.9, display the TTL value and OS"**

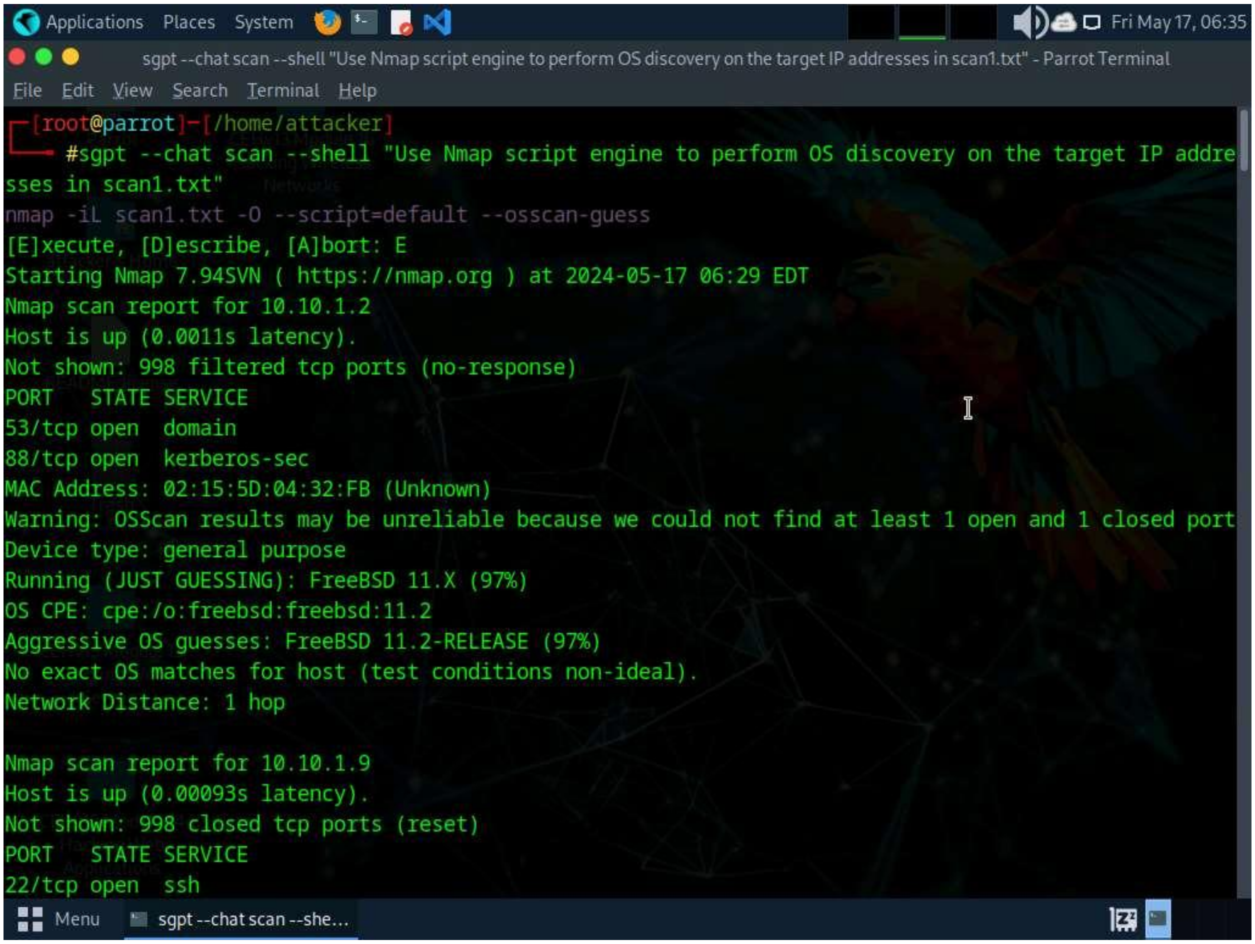
In the prompt type **E** and press **Enter** to execute the command.


Applications
Places
System
Fri May 17, 06:14
sgpt --chat scan --shell "Use TTL value and identify the operating system running on the target IP address 10.10.1.9, display the TTL value and
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat scan --she...

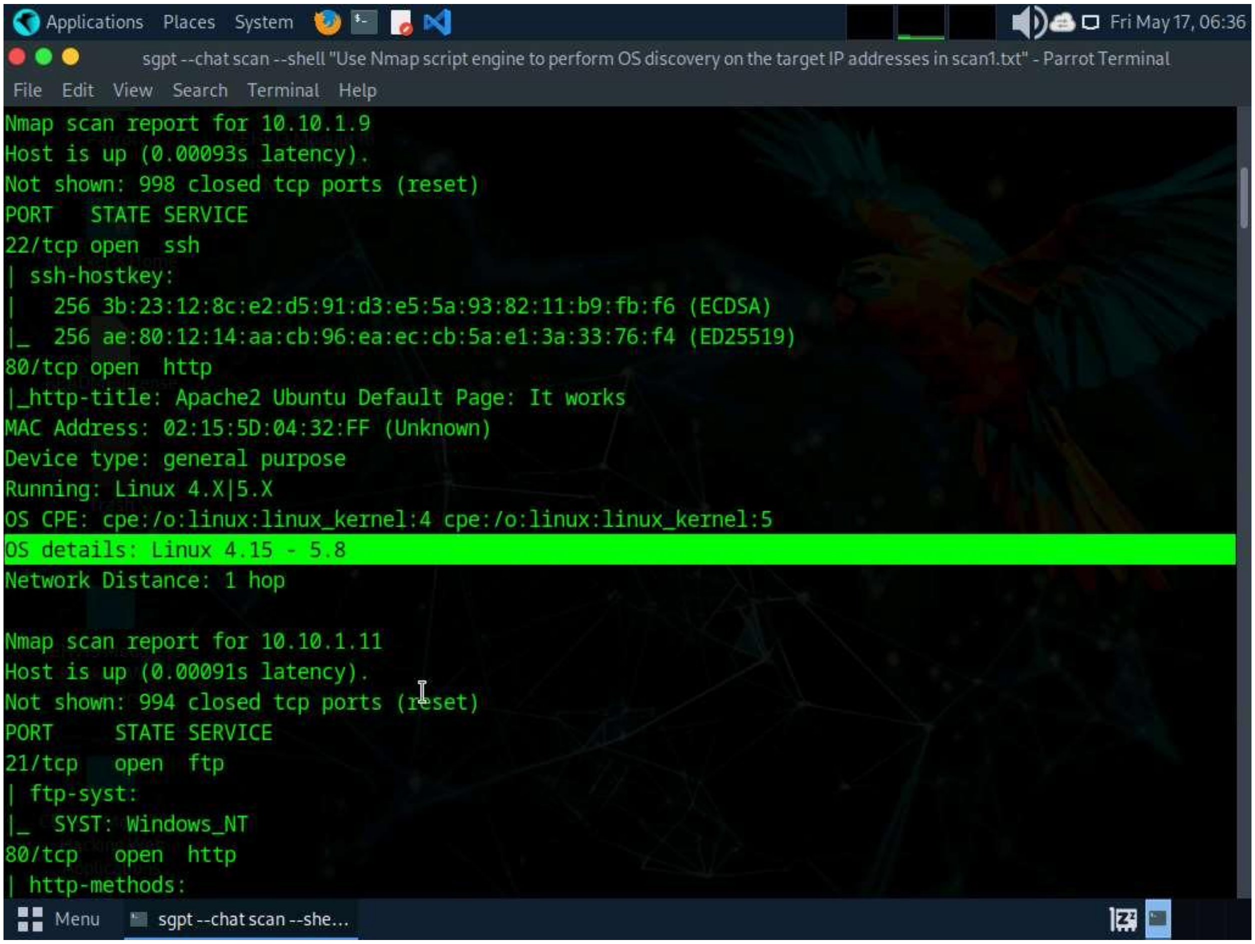
```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Use TTL value and identify the operating system running on the target
 IP address 10.10.1.9, display the TTL value and OS"
ping -c 1 10.10.1.9 | grep 'ttl=' && echo "TTL value indicates: $(ping -c 1 10.10.1.9 | grep 'ttl=' |
 awk -F ' ' '{print $6}' | awk -F '=' '{print $2}' | awk '{if($1 > 0 && $1 <= 64) print "Linux"; else
 if($1 > 64 && $1 <= 128) print "Windows"; else if($1 > 128) print "Solaris/AIX";}')"
[E]xecute, [D]escribe, [A]bort: E
64 bytes from 10.10.1.9: icmp_seq=1 ttl=64 time=2.61 ms
TTL value indicates: Linux
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

23. We will now perform OS discovery using Nmap on the list of IP addresses acquired in **Step#6**, to do so run **sgpt --chat scan --shell "Use Nmap script engine to perform OS discovery on the target IP addresses in scan1.txt"**

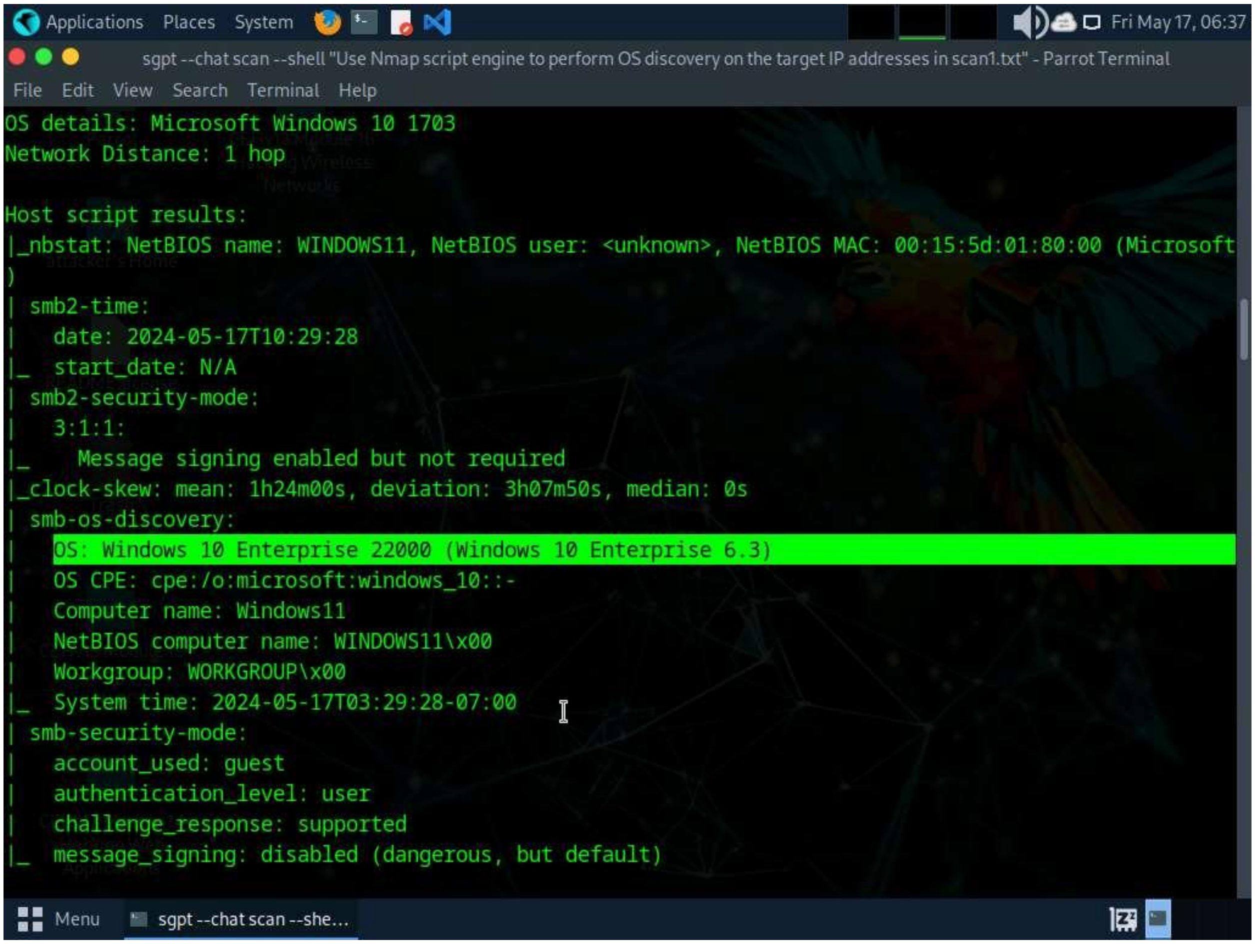
In the prompt type **E** and press **Enter** to execute the command.


Applications
Places
System
Fri May 17, 06:35
sgpt --chat scan --shell "Use Nmap script engine to perform OS discovery on the target IP addresses in scan1.txt" - Parrot Terminal
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat scan --she...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Use Nmap script engine to perform OS discovery on the target IP addre
sses in scan1.txt"
nmap -iL scan1.txt -O --script=default --osscan-guess
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 06:29 EDT
Nmap scan report for 10.10.1.2
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
88/tcp open  kerberos-sec
MAC Address: 02:15:5D:04:32:FB (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 10.10.1.9
Host is up (0.00093s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
```


Applications
Places
System
Fri May 17, 06:36
sgpt --chat scan --shell "Use Nmap script engine to perform OS discovery on the target IP addresses in scan1.txt" - Parrot Terminal
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat scan --she...

```
Nmap scan report for 10.10.1.9
Host is up (0.00093s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   256 3b:23:12:8c:e2:d5:91:d3:e5:5a:93:82:11:b9:fb:f6 (ECDSA)
|_  256 ae:80:12:14:aa:cb:96:ea:ec:cb:5a:e1:3a:33:76:f4 (ED25519)
80/tcp open  http
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:15:5D:04:32:FF (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

Nmap scan report for 10.10.1.11
Host is up (0.00091s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-syst:
|_  SYST: Windows_NT
80/tcp   open  http
| http-methods:
```

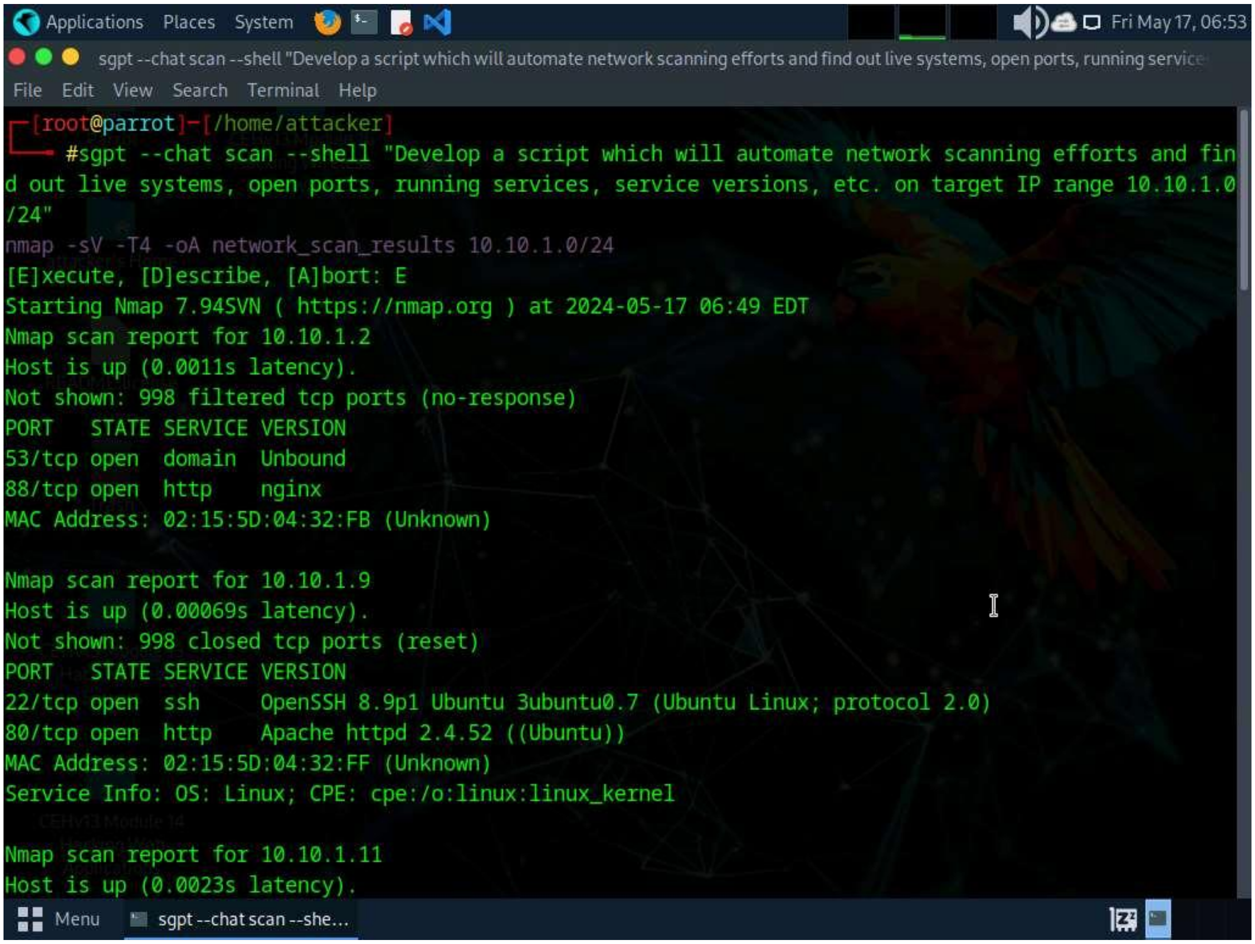

Applications Places System
Fri May 17, 06:37
sgpt --chat scan --shell "Use Nmap script engine to perform OS discovery on the target IP addresses in scan1.txt" - Parrot Terminal
File Edit View Search Terminal Help
Menu
sgpt --chat scan --she...

```
OS details: Microsoft Windows 10 1703
Network Distance: 1 hop

Host script results:
|_nbstat: NetBIOS name: WINDOWS11, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:01:80:00 (Microsoft
)
| smb2-time:
|   date: 2024-05-17T10:29:28
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s
| smb-os-discovery:
|   OS: Windows 10 Enterprise 22000 (Windows 10 Enterprise 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: Windows11
|   NetBIOS computer name: WINDOWS11\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-05-17T03:29:28-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

24. We will automate various network scanning tasks by create custom script that will run automatically and fetch the desired result.

25. In the terminal window run **sgpt --chat scan --shell "Develop a script which will automate network scanning efforts and find out live systems, open ports, running services, service versions, etc. on target IP range 10.10.1.0/24"** command.

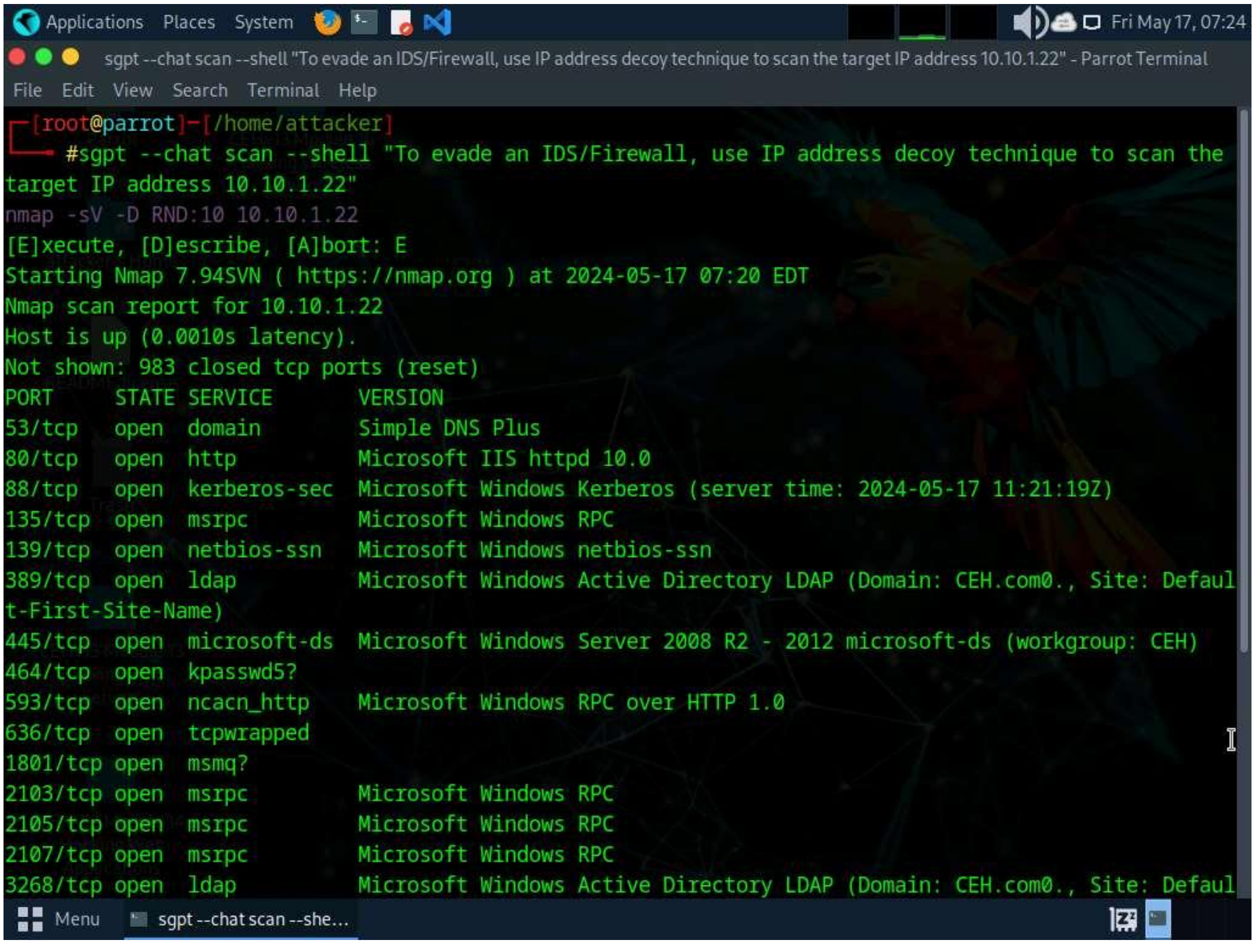
In the prompt type **E** and press **Enter** to execute the command.


Applications
Places
System
Fri May 17, 06:53
sgpt --chat scan --shell "Develop a script which will automate network scanning efforts and find out live systems, open ports, running service
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat scan --she...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Develop a script which will automate network scanning efforts and fin
d out live systems, open ports, running services, service versions, etc. on target IP range 10.10.1.0
/24"
nmap -sV -T4 -oA network_scan_results 10.10.1.0/24
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 06:49 EDT
Nmap scan report for 10.10.1.2
Host is up (0.0011s 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:04:32:FB (Unknown)

Nmap scan report for 10.10.1.9
Host is up (0.00069s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
MAC Address: 02:15:5D:04:32:FF (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.10.1.11
Host is up (0.0023s latency).
```

26. To use the IP Address Decoy technique to scan run **sgpt --chat scan --shell “To evade an IDS/Firewall, use IP address decoy technique to scan the target IP address 10.10.1.22”** command.

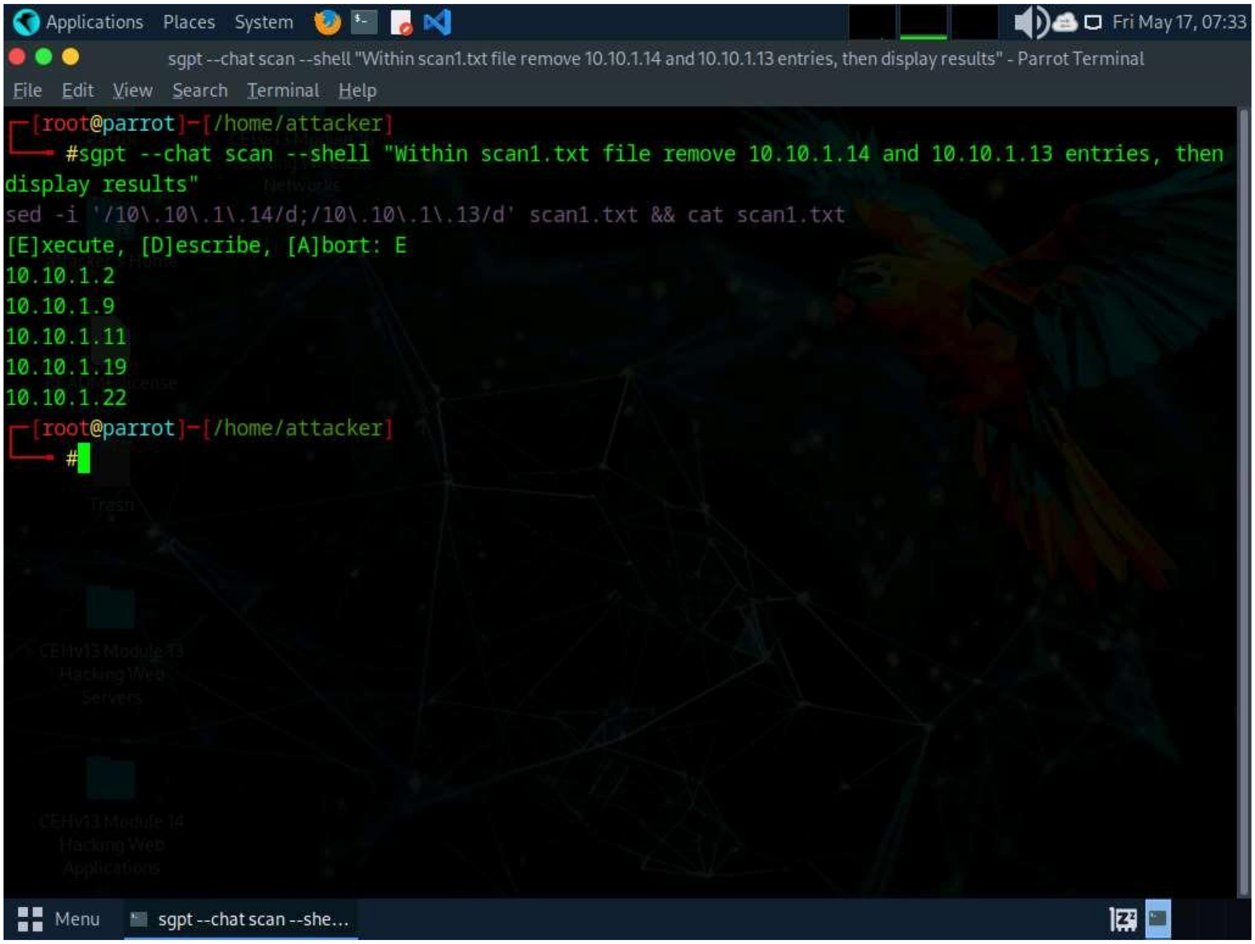
In the prompt type **E** and press **Enter** to execute the command.


Applications
Places
System
Fri May 17, 07:24
sgpt --chat scan --shell "To evade an IDS/Firewall, use IP address decoy technique to scan the target IP address 10.10.1.22" - Parrot Terminal
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat scan --she...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "To evade an IDS/Firewall, use IP address decoy technique to scan the
target IP address 10.10.1.22"
nmap -sV -D RND:10 10.10.1.22
[E]xecute, [D]escribe, [A]bort: E
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 07:20 EDT
Nmap scan report for 10.10.1.22
Host is up (0.0010s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-05-17 11:21:19Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: CEH.com0., Site: Defaul
t-First-Site-Name)
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CEH)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: CEH.com0., Site: Defaul
```

27. Now, run **sgpt --chat scan --shell “Within scan1.txt file remove 10.10.1.14 and 10.10.1.13 entries, then display results”** command to remove IP address from scan1.txt file and display result.

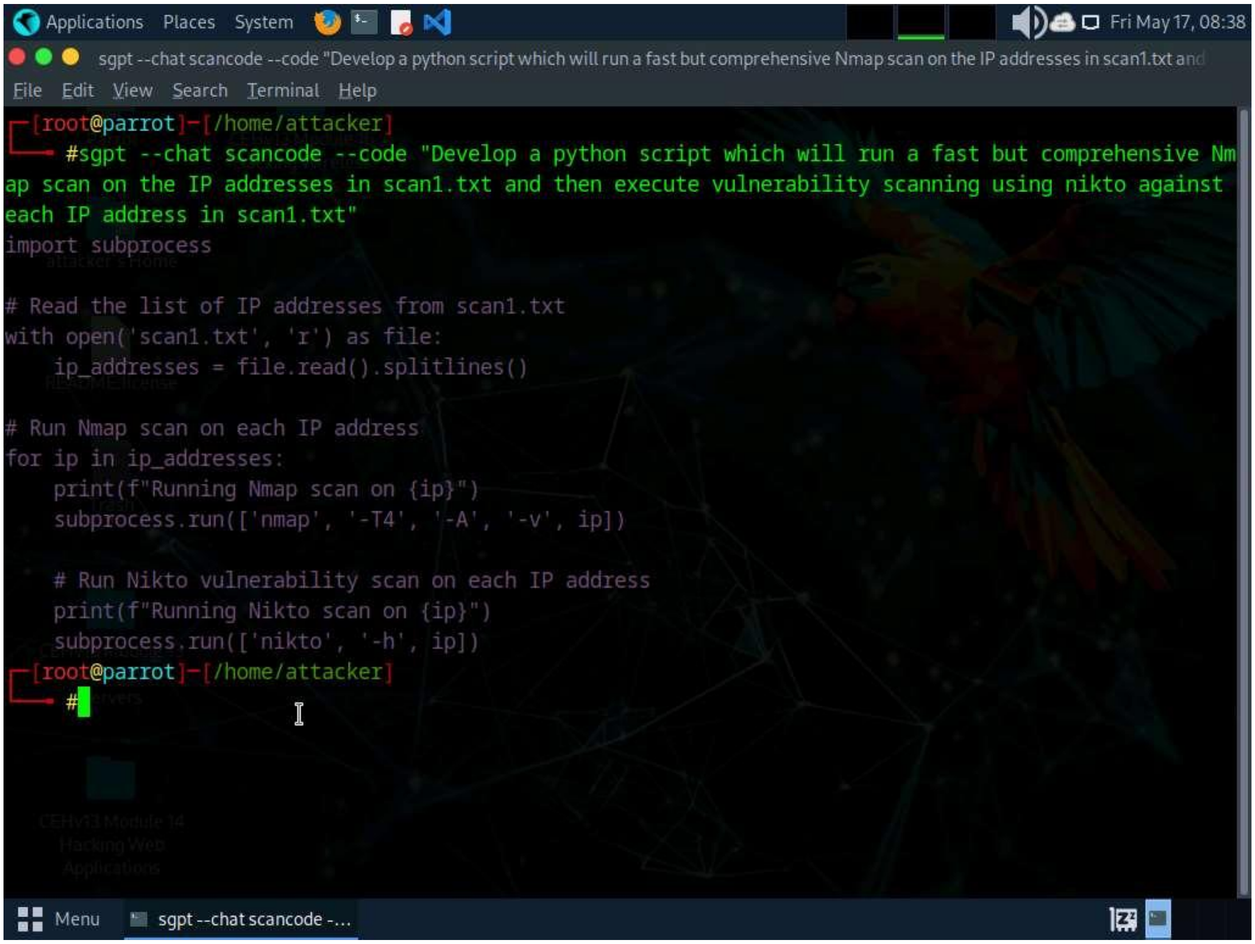
In the prompt type **E** and press **Enter** to execute the command.


Applications Places System
Fri May 17, 07:33
sgpt --chat scan --shell "Within scan1.txt file remove 10.10.1.14 and 10.10.1.13 entries, then display results" - Parrot Terminal
File Edit View Search Terminal Help
Menu
sgpt --chat scan --she...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scan --shell "Within scan1.txt file remove 10.10.1.14 and 10.10.1.13 entries, then
display results"
sed -i '/10\.10\.1\.14/d;/10\.10\.1\.13/d' scan1.txt && cat scan1.txt
[E]xecute, [D]escribe, [A]bort: E
10.10.1.2
10.10.1.9
10.10.1.11
10.10.1.19
10.10.1.22
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

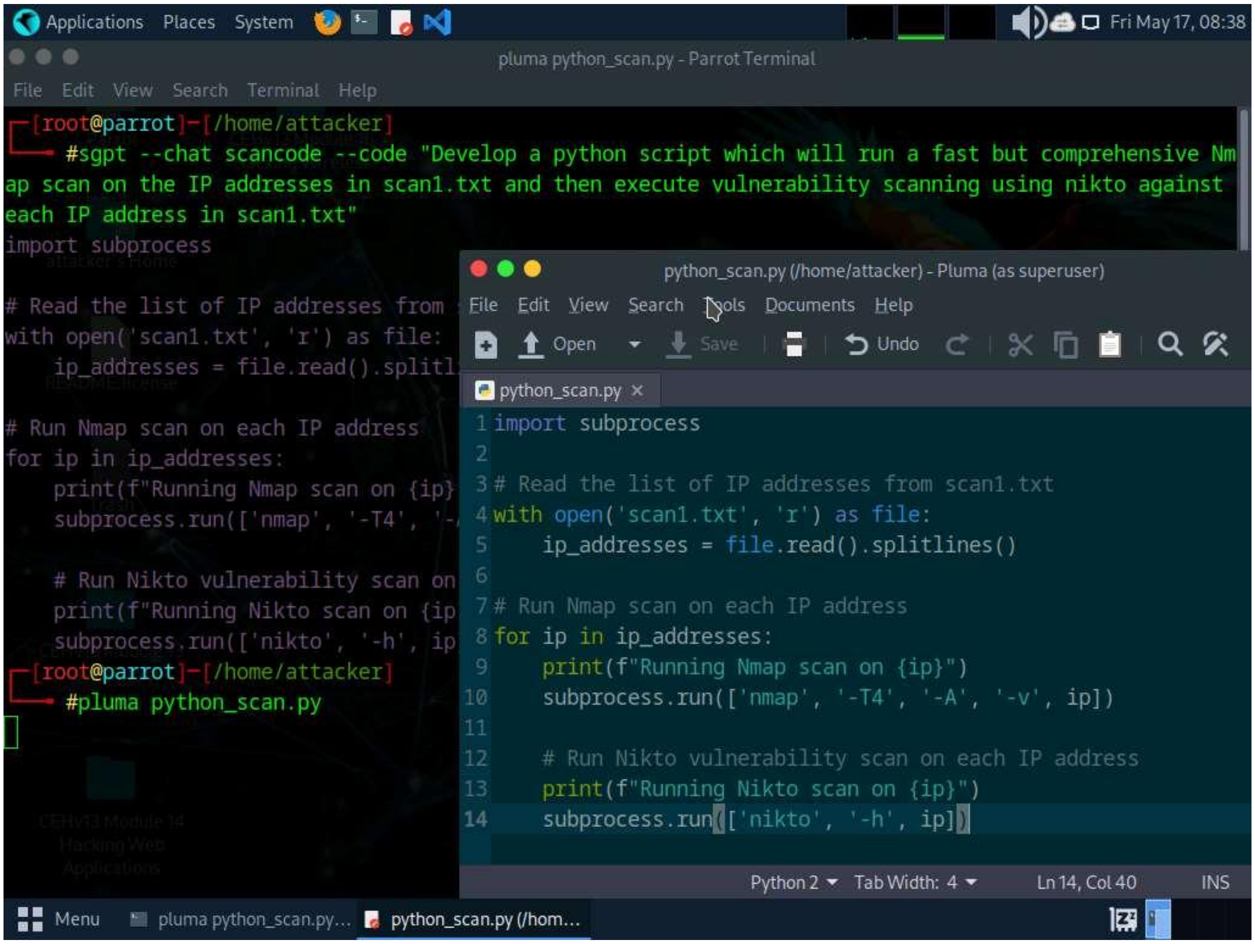
28. Run **sgpt --chat scancode --code "Create a python script to run a fast but comprehensive Nmap scan on the IP addresses in scan1.txt and then execute vulnerability scanning using nikto against each IP address in scan1.txt"** command to create a python script which performs Nmap scan.

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


Applications
Places
System
Fri May 17, 08:38
sgpt --chat scancode --code "Develop a python script which will run a fast but comprehensive Nmap scan on the IP addresses in scan1.txt and
File
Edit
View
Search
Terminal
Help
Menu
sgpt --chat scancode -...

```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scancode --code "Develop a python script which will run a fast but comprehensive Nm
ap scan on the IP addresses in scan1.txt and then execute vulnerability scanning using nikto against
each IP address in scan1.txt"
import subprocess

# Read the list of IP addresses from scan1.txt
with open('scan1.txt', 'r') as file:
    ip_addresses = file.read().splitlines()

# Run Nmap scan on each IP address
for ip in ip_addresses:
    print(f"Running Nmap scan on {ip}")
    subprocess.run(['nmap', '-T4', '-A', '-v', ip])

    # Run Nikto vulnerability scan on each IP address
    print(f"Running Nikto scan on {ip}")
    subprocess.run(['nikto', '-h', ip])
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

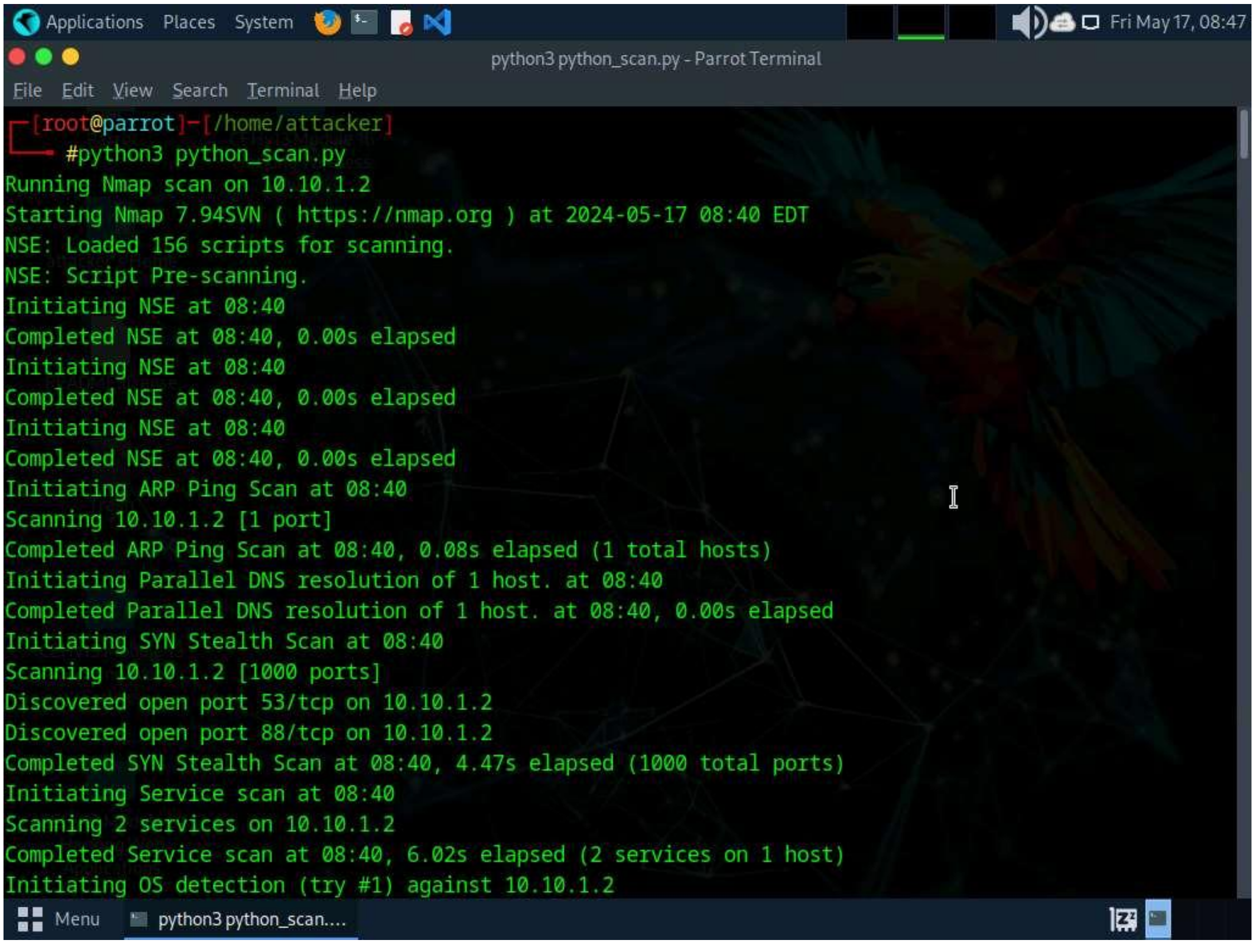
29. Now, copy the python code and type **pluma python_scan.py** in the terminal. A Text editor window opens paste the code in the text editor window, save the file and close it.


Applications Places System
Fri May 17, 08:38
pluma python_scan.py - Parrot Terminal
File Edit View Search Terminal Help
python_scan.py (/home/attacker) - Pluma (as superuser)
File Edit View Search Tools Documents Help
Open
Save
Undo
python_scan.py
Python 2
Tab Width: 4
Ln 14, Col 40
INS
Menu
pluma python_scan.py...
python_scan.py (/hom...

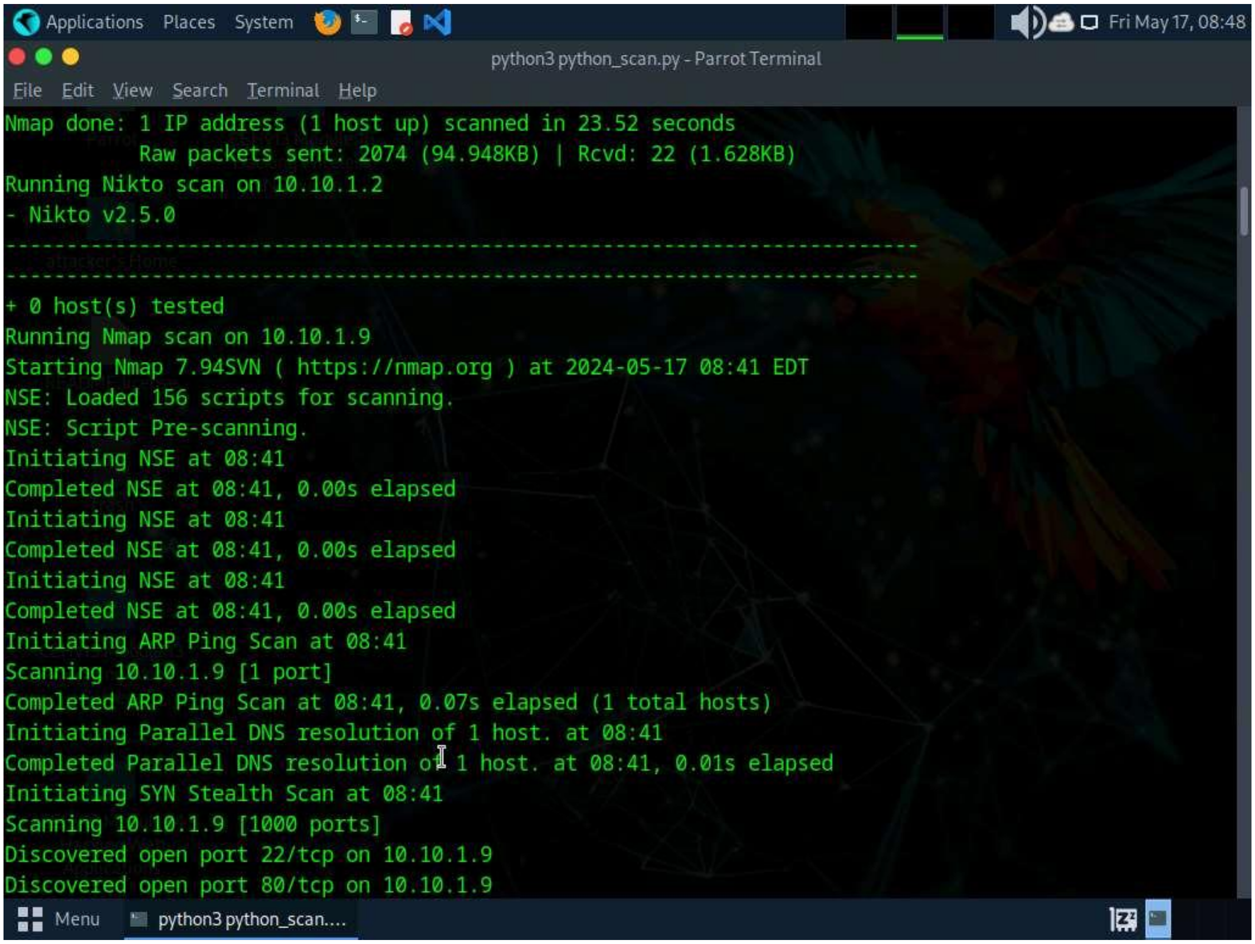
```
┌─[root@parrot]─[/home/attacker]
└──╼ #sgpt --chat scancode --code "Develop a python script which will run a fast but comprehensive Nmap scan on the IP addresses in scan1.txt and then execute vulnerability scanning using nikto against each IP address in scan1.txt"
import subprocess

# Read the list of IP addresses from
with open('scan1.txt', 'r') as file:
    ip_addresses = file.read().splitl

# Run Nmap scan on each IP address
for ip in ip_addresses:
    print(f"Running Nmap scan on {ip}
    subprocess.run(['nmap', '-T4', '-

    # Run Nikto vulnerability scan on
    print(f"Running Nikto scan on {ip
    subprocess.run(['nikto', '-h', ip
┌─[root@parrot]─[/home/attacker]
└──╼ #pluma python_scan.py
```

```python
import subprocess

# Read the list of IP addresses from scan1.txt
with open('scan1.txt', 'r') as file:
    ip_addresses = file.read().splitlines()

# Run Nmap scan on each IP address
for ip in ip_addresses:
    print(f"Running Nmap scan on {ip}")
    subprocess.run(['nmap', '-T4', '-A', '-v', ip])

    # Run Nikto vulnerability scan on each IP address
    print(f"Running Nikto scan on {ip}")
    subprocess.run(['nikto', '-h', ip])
```

30. Now, in the terminal window, type **python3 python_scan.py** to run the script.



```
┌─[root@parrot]─[/home/attacker]
└──╼ #python3 python_scan.py
Running Nmap scan on 10.10.1.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 08:40 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:40
Completed NSE at 08:40, 0.00s elapsed
Initiating NSE at 08:40
Completed NSE at 08:40, 0.00s elapsed
Initiating NSE at 08:40
Completed NSE at 08:40, 0.00s elapsed
Initiating ARP Ping Scan at 08:40
Scanning 10.10.1.2 [1 port]
Completed ARP Ping Scan at 08:40, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:40
Completed Parallel DNS resolution of 1 host. at 08:40, 0.00s elapsed
Initiating SYN Stealth Scan at 08:40
Scanning 10.10.1.2 [1000 ports]
Discovered open port 53/tcp on 10.10.1.2
Discovered open port 88/tcp on 10.10.1.2
Completed SYN Stealth Scan at 08:40, 4.47s elapsed (1000 total ports)
Initiating Service scan at 08:40
Scanning 2 services on 10.10.1.2
Completed Service scan at 08:40, 6.02s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.10.1.2
```


Applications Places System
Fri May 17, 08:48
python3 python_scan.py - Parrot Terminal
File Edit View Search Terminal Help
Menu
python3 python_scan....

```
Nmap done: 1 IP address (1 host up) scanned in 23.52 seconds
           Raw packets sent: 2074 (94.948KB) | Rcvd: 22 (1.628KB)
Running Nikto scan on 10.10.1.2
- Nikto v2.5.0
---------------------------------------------------------------------------
---------------------------------------------------------------------------
+ 0 host(s) tested
Running Nmap scan on 10.10.1.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 08:41 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:41
Completed NSE at 08:41, 0.00s elapsed
Initiating NSE at 08:41
Completed NSE at 08:41, 0.00s elapsed
Initiating NSE at 08:41
Completed NSE at 08:41, 0.00s elapsed
Initiating ARP Ping Scan at 08:41
Scanning 10.10.1.9 [1 port]
Completed ARP Ping Scan at 08:41, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:41
Completed Parallel DNS resolution of 1 host. at 08:41, 0.01s elapsed
Initiating SYN Stealth Scan at 08:41
Scanning 10.10.1.9 [1000 ports]
Discovered open port 22/tcp on 10.10.1.9
Discovered open port 80/tcp on 10.10.1.9
```

31. Apart from the aforementioned commands, you can further explore additional options within the ShellGPT tool and utilize various other tools to conduct Network Scanning on the target machine.

32. This concludes the demonstration of using ShellGPT to discover active hosts, open ports, services running, and OS details of systems present in the target network.

33. Close all open windows and document all the acquired information.

Question 3.6.1.1

Write a ShellGPT prompt and execute it on Parrot Security machine, to perform port scanning on Windows 11 virtual machine (10.10.1.11). Enter the name of the service that is running on port 139.