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.

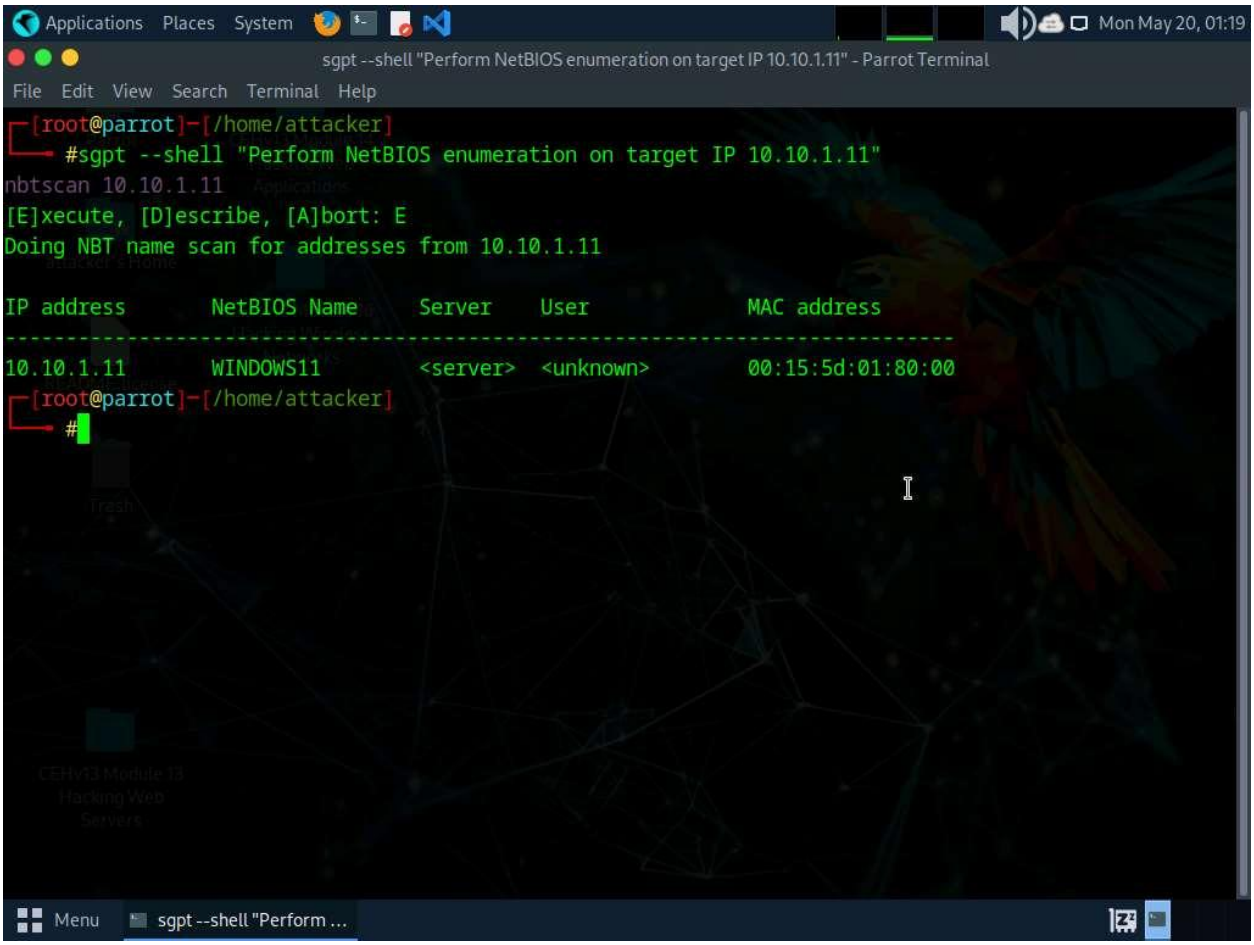
The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the 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**.

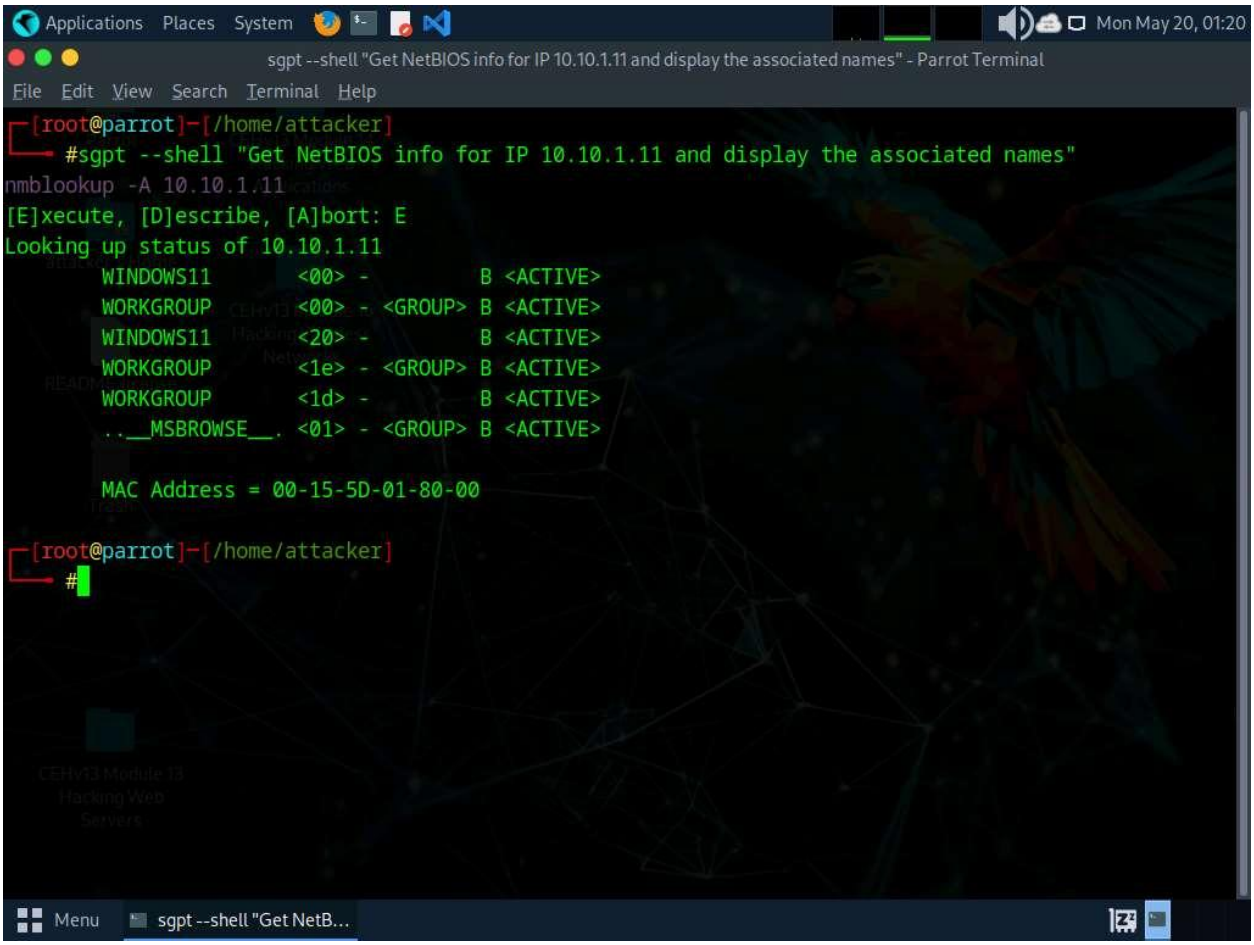
2. After incorporating the ShellGPT API in Parrot Security Machine, in the terminal window run **sgpt --shell "Perform NetBIOS enumeration on target IP 10.10.1.11"** command to perform NetBIOS enumeration on target system.

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



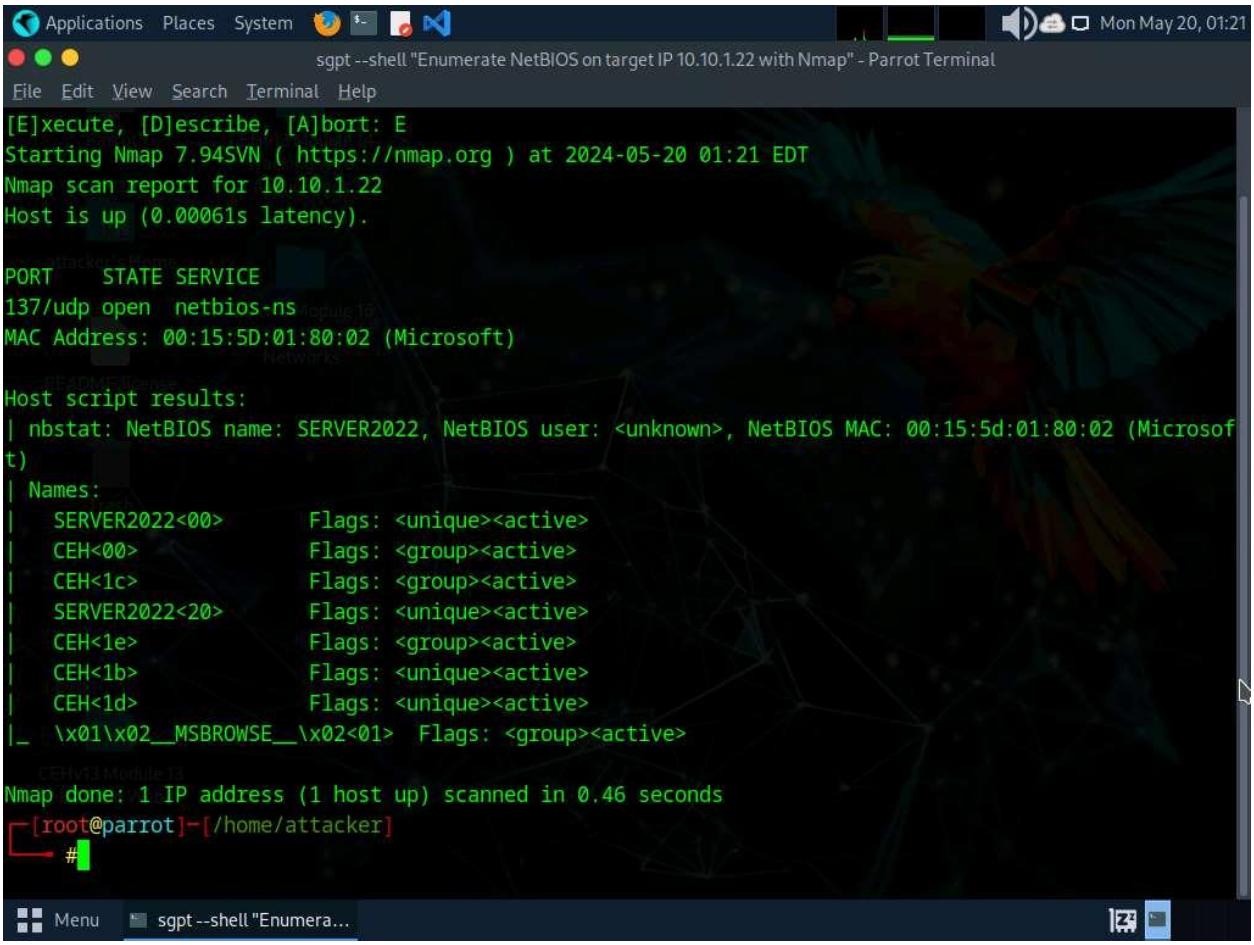
3. Run **sgpt --shell "Get NetBIOS info for IP 10.10.1.11 and display the associated names"** command to view the associated names of target system.

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



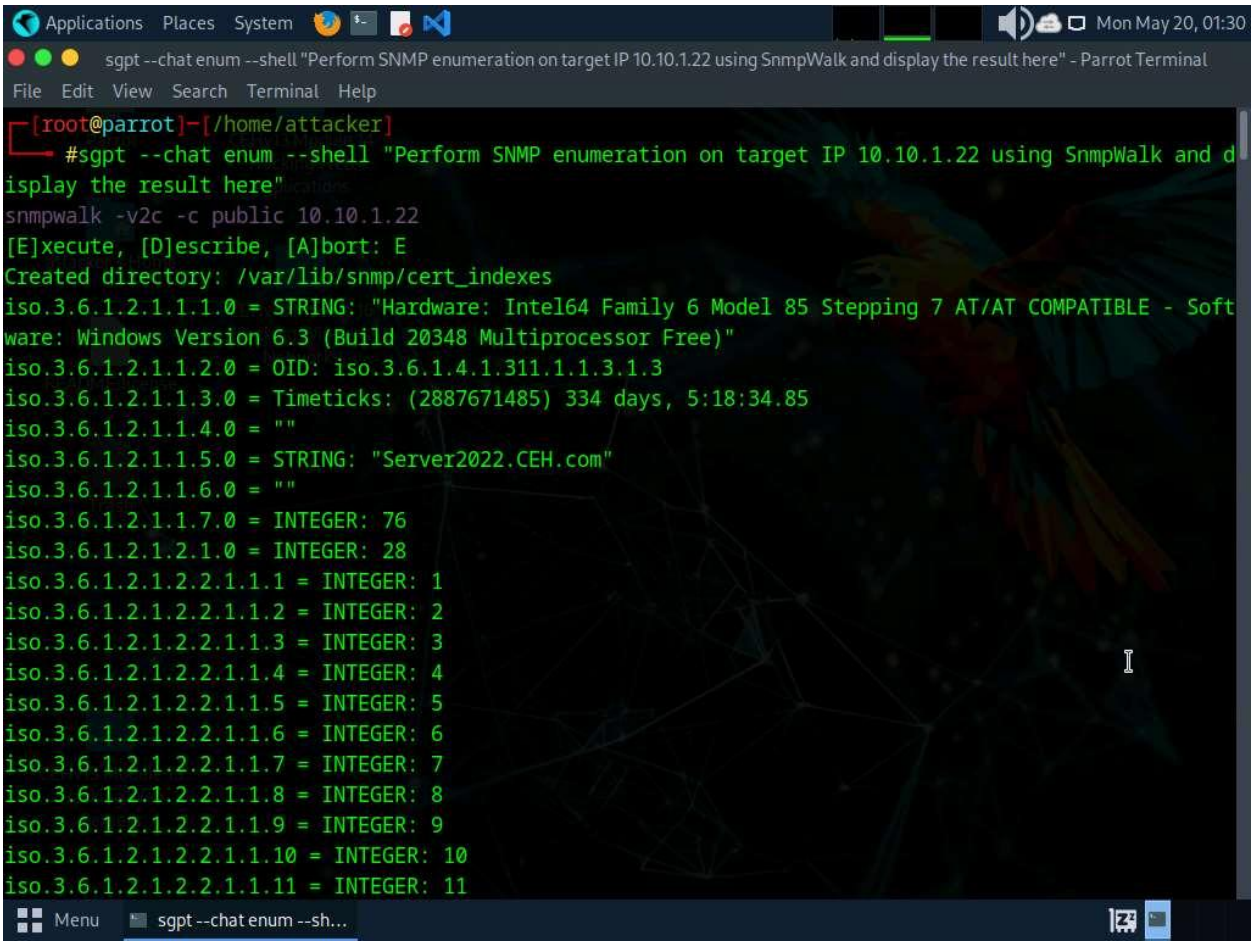
4. To perform NetBIOS enumeration using Nmap run **sgpt --shell "Enumerate NetBIOS on target IP 10.10.1.22 with nmap"** command.

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



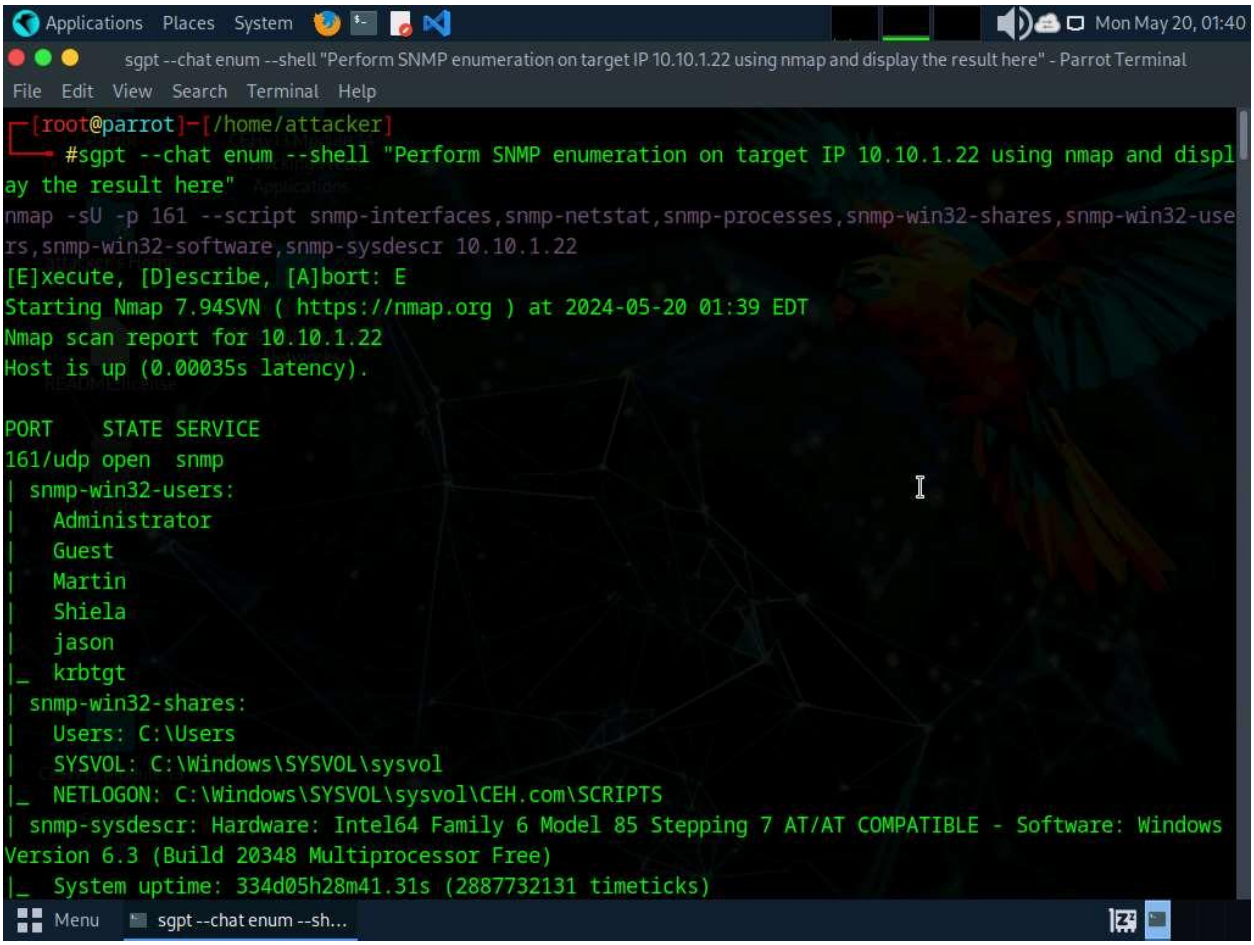
5. We will now perform SNMP enumeration using ShellGPT, to do so, run **sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using SnmpWalk and display the result here"** command.

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



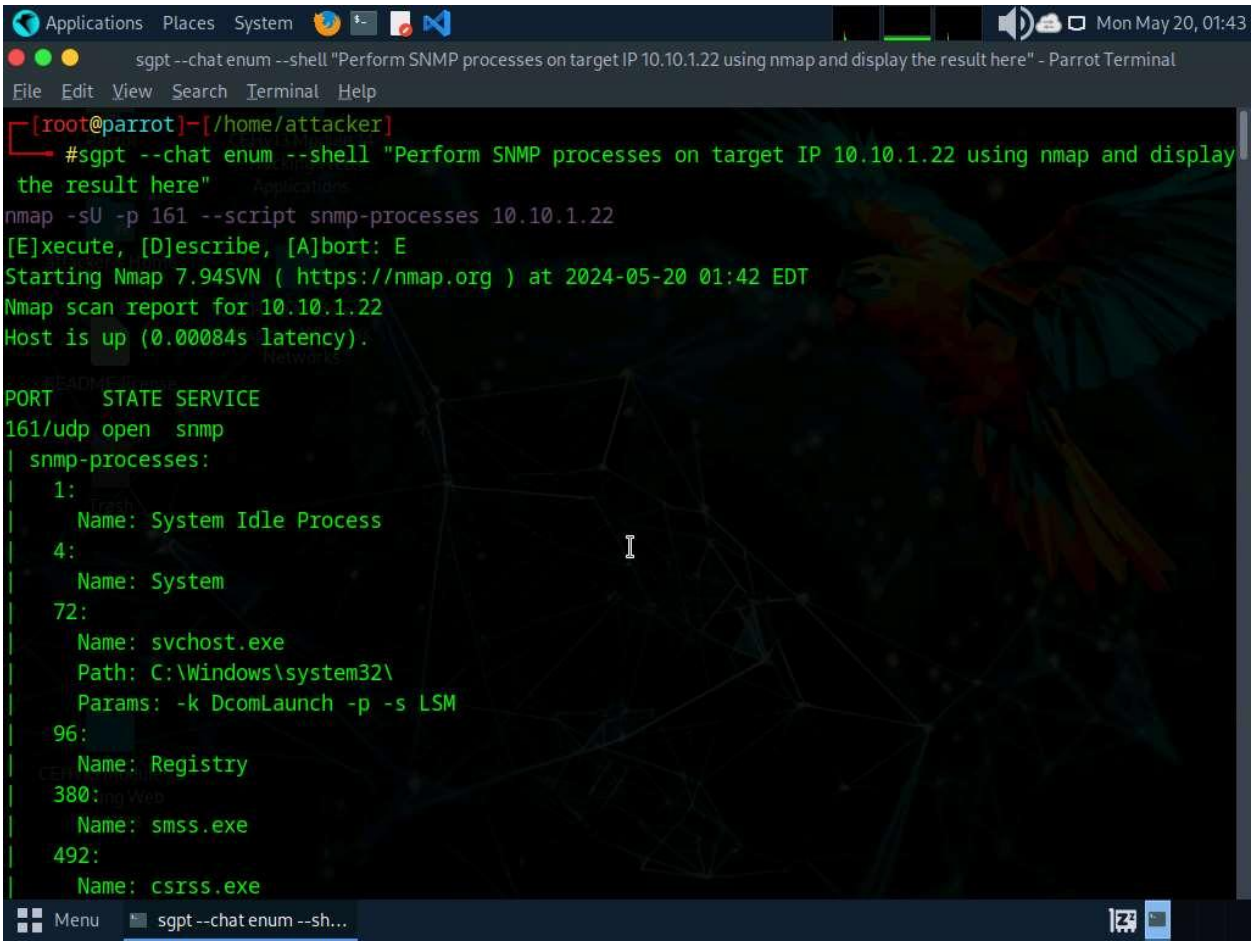
6. Run **sgpt --chat enum --shell "Perform SNMP enumeration on target IP 10.10.1.22 using nmap and display the result here"** command to perform SNMP enumeration using Nmap.

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



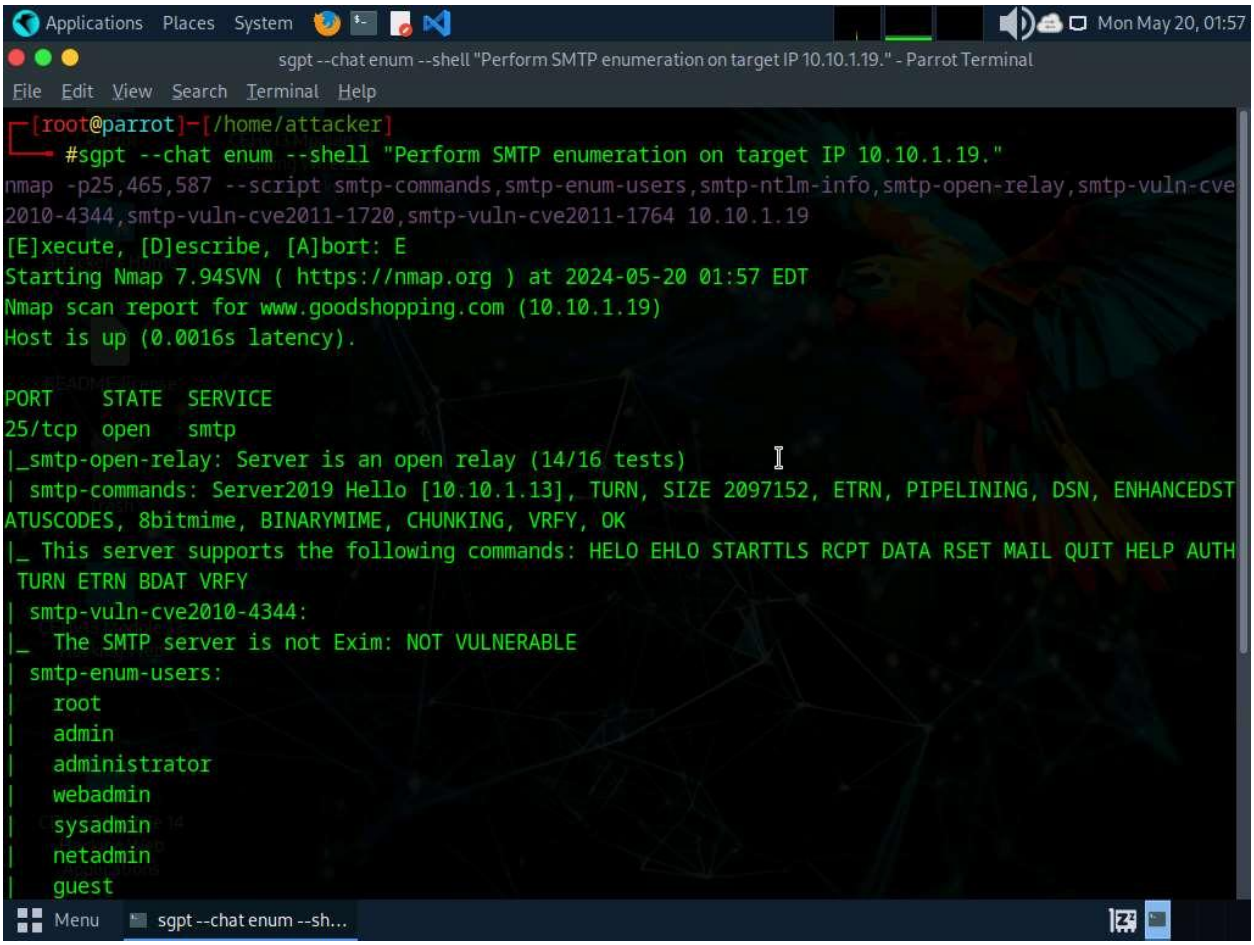
7. Run **sgpt --chat enum --shell "Perform SNMP processes on target IP 10.10.1.22 using nmap and display the result here"** command.

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



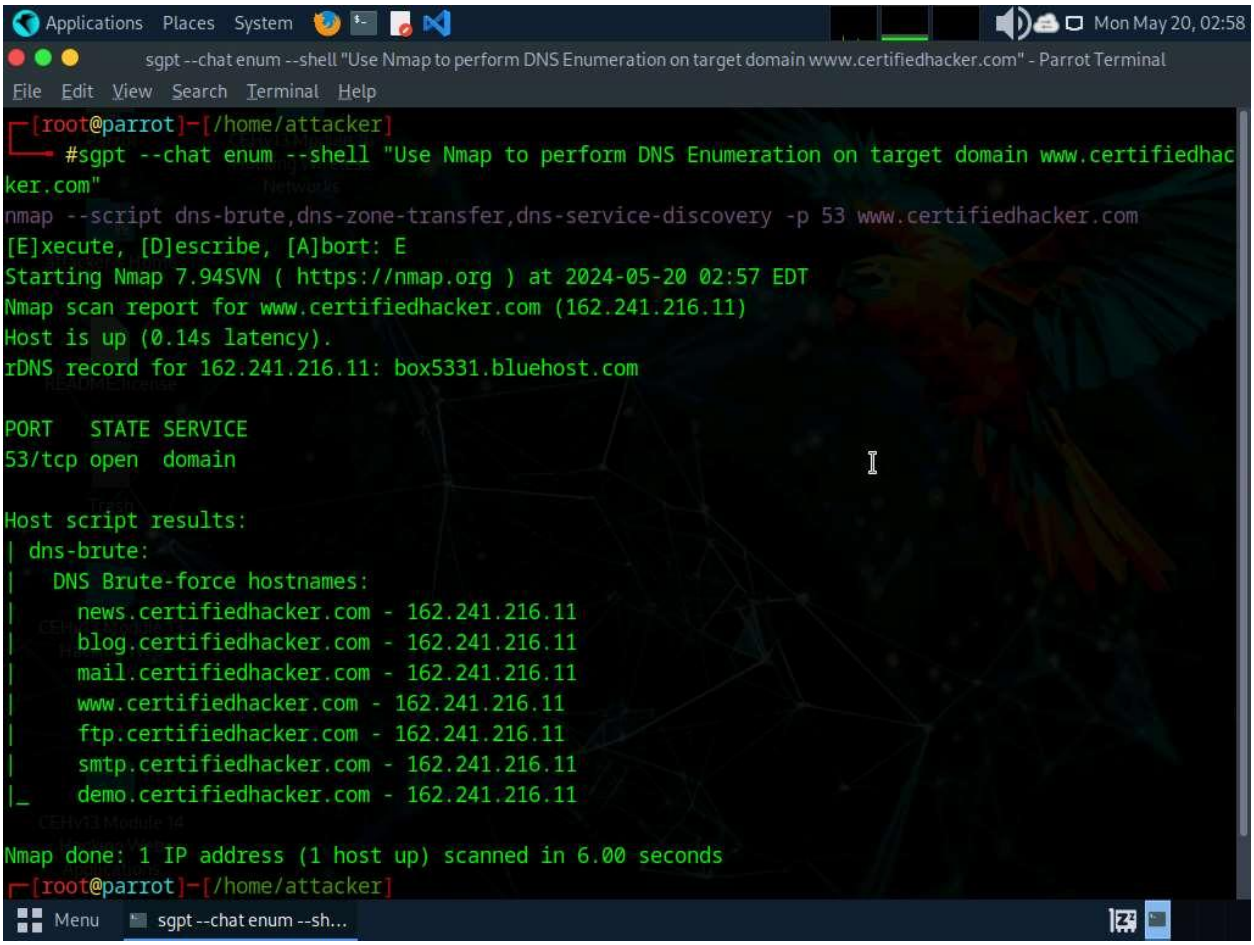
8. To perform SMTP enumeration on a target IP run **sgpt --chat enum --shell "Perform SMTP enumeration on target IP 10.10.1.19."** command.

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



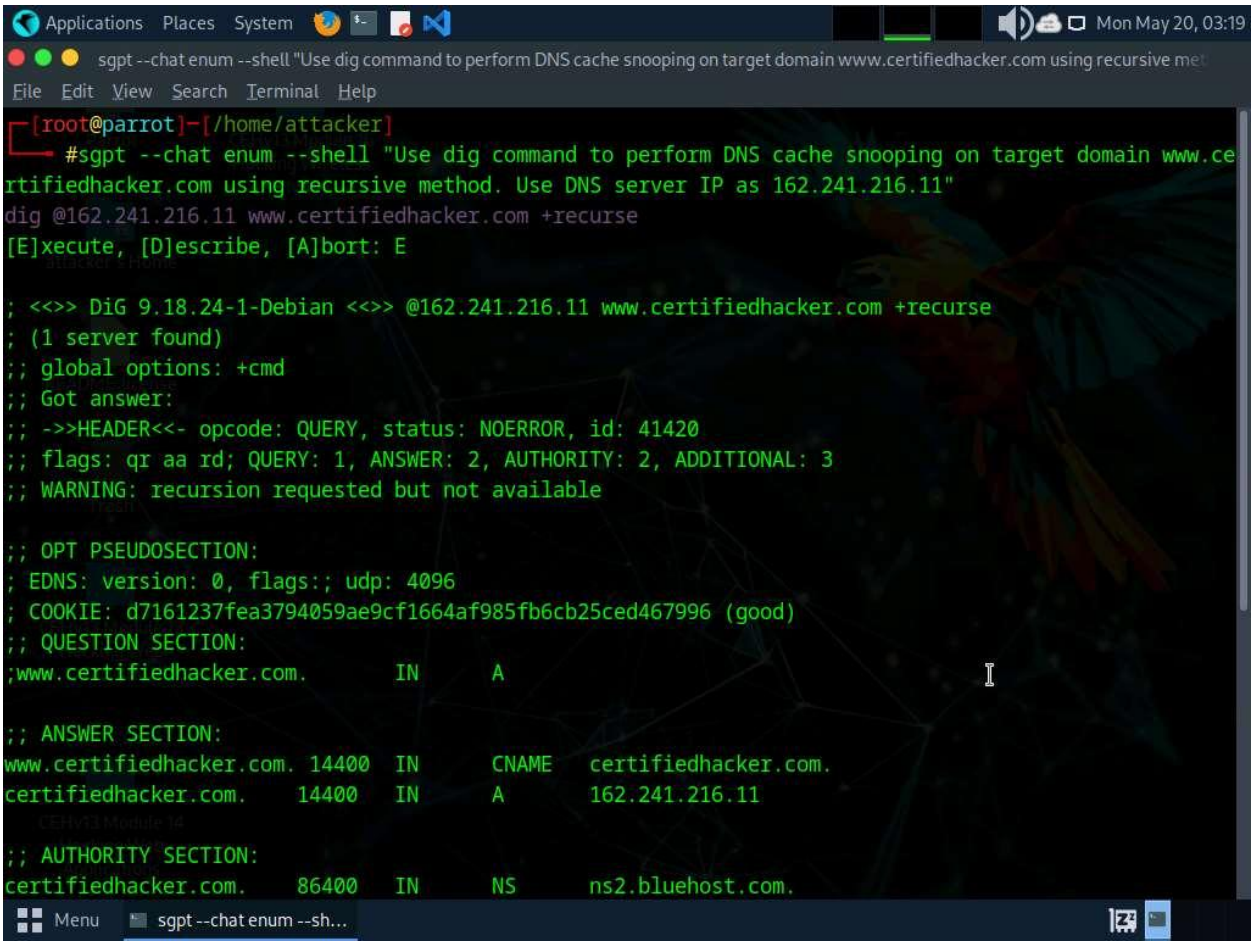
9. We will perform DNS enumeration with Nmap using ShellGPT, to do so run **sgpt --chat enum --shell "Use Nmap to perform DNS Enumeration on target domain www.certifiedhacker.com"** command.

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



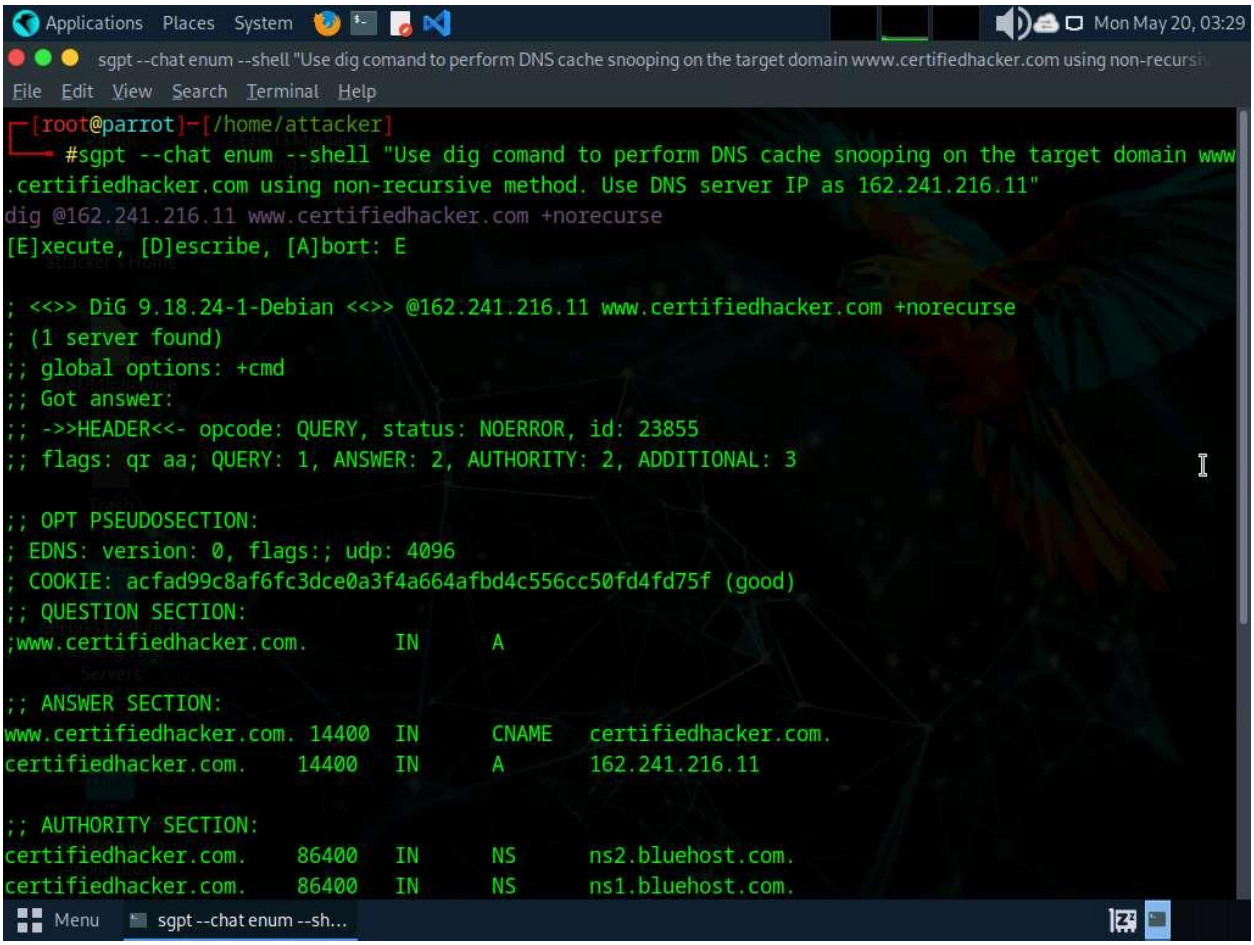
10. To perform DNS cache snooping on target domain run **sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on target domain www.certifiedhacker.com using recursive method. Use DNS server IP as 162.241.216.11"** command.

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



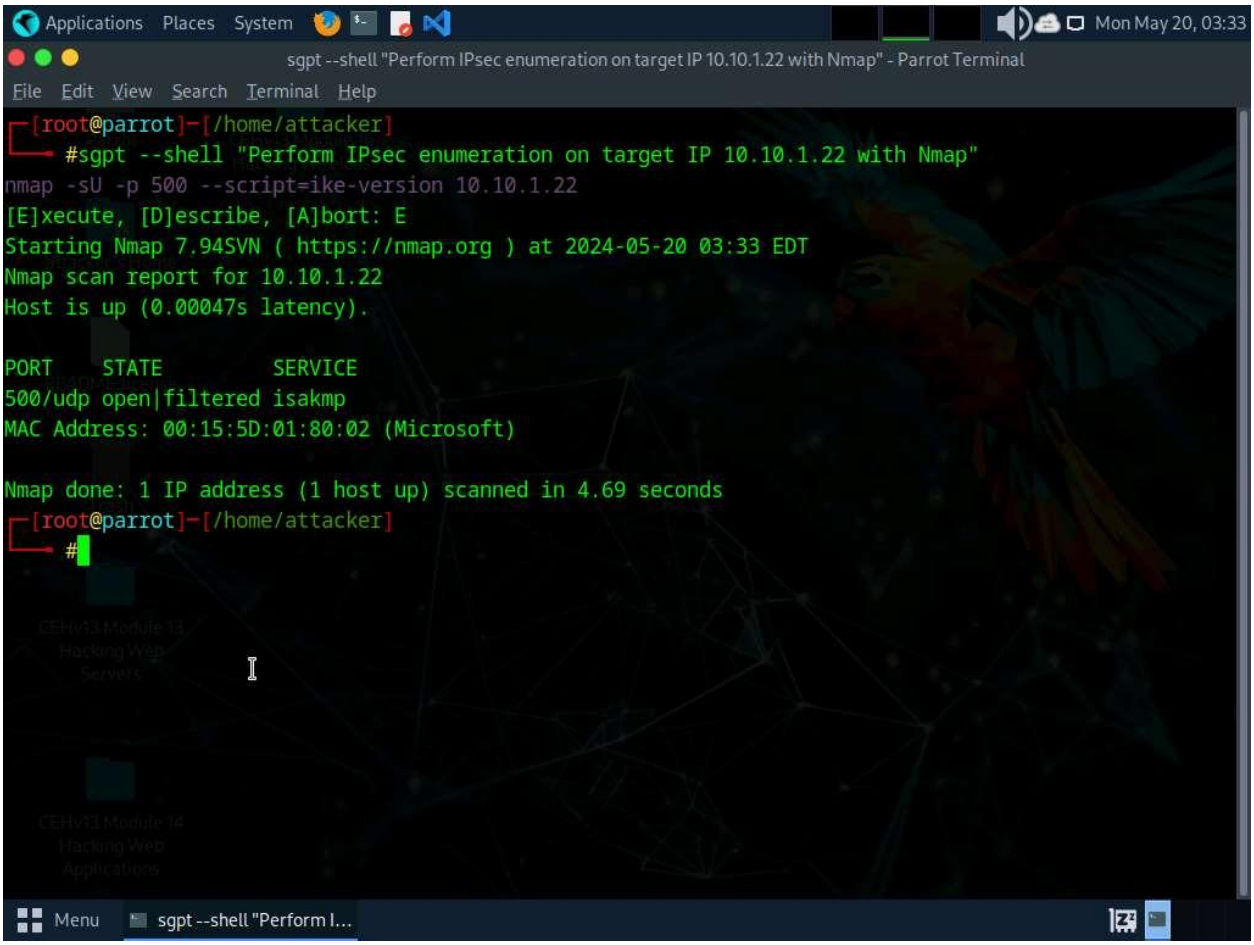
11. Run **sgpt --chat enum --shell "Use dig command to perform DNS cache snooping on the target domain www.certifiedhacker.com using non-recursive method. Use DNS server IP as 162.241.216.11"** command.

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



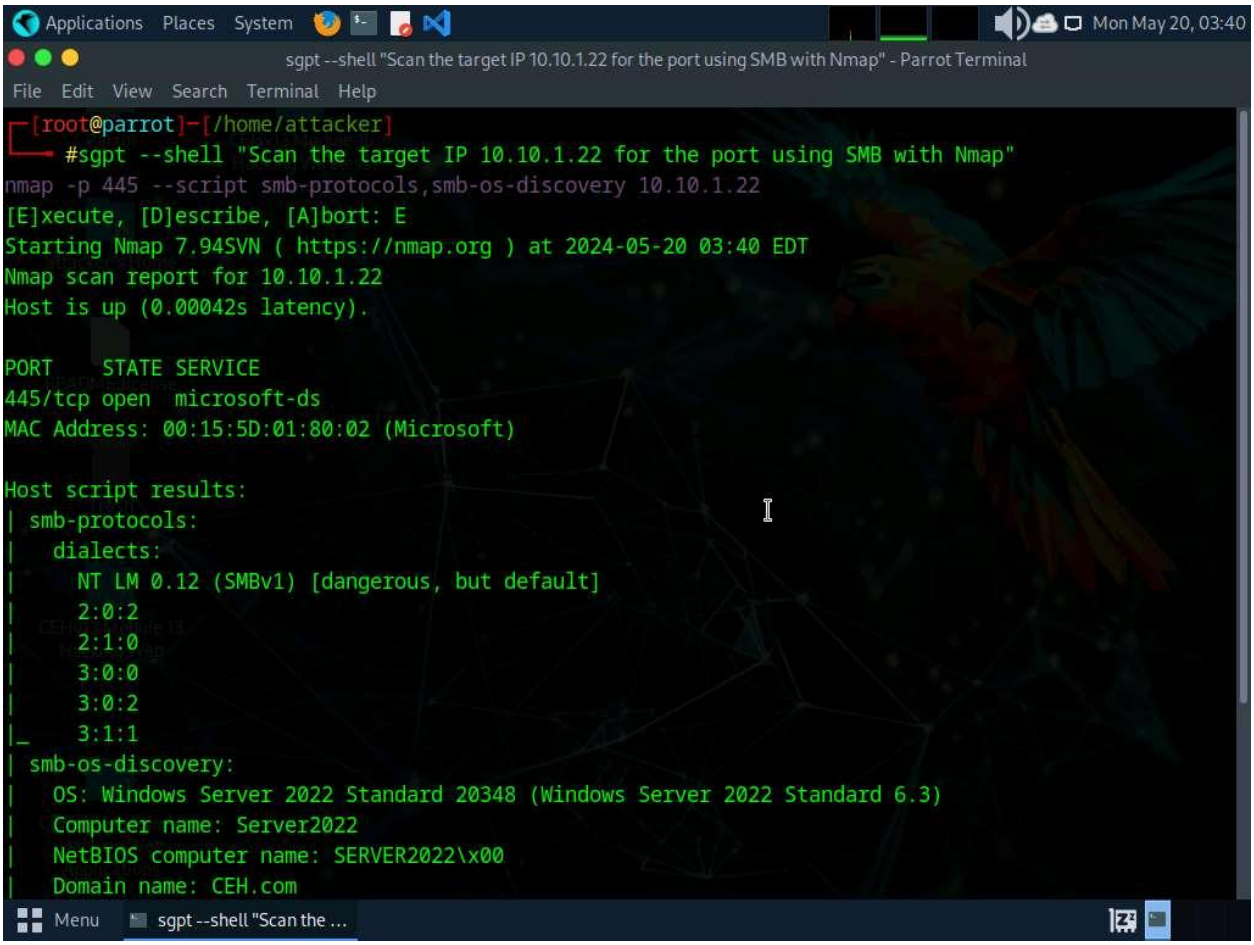
12. To perform IPsec enumeration using ShellGPT run **sgpt --shell "Perform IPsec enumeration on target IP 10.10.1.22 with Nmap"** command.

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



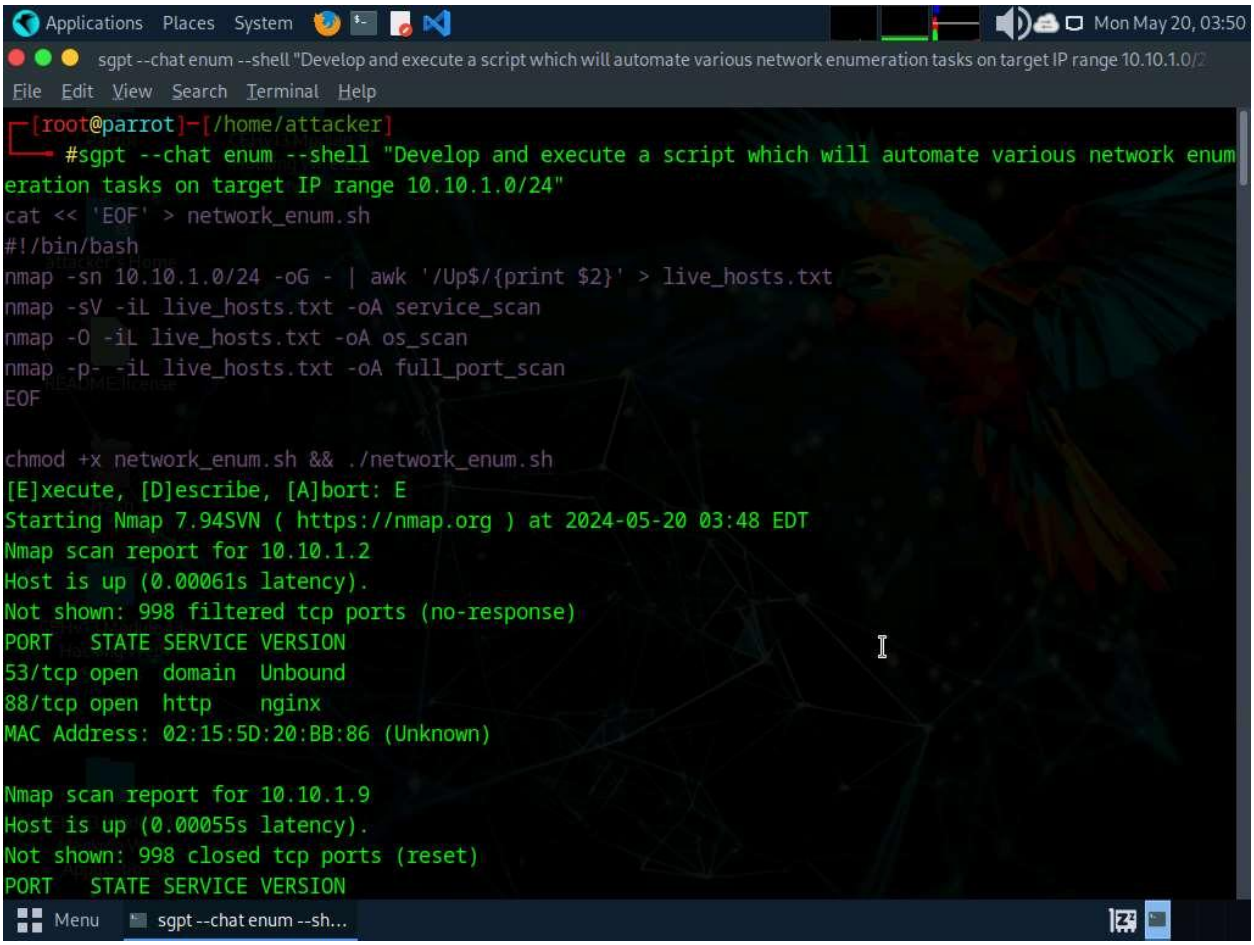
13. We will now perform SMB enumeration using ShellGPT, to do so, run **sgpt --shell "Scan the target IP 10.10.1.22 for the port using SMB with Nmap"** command.

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



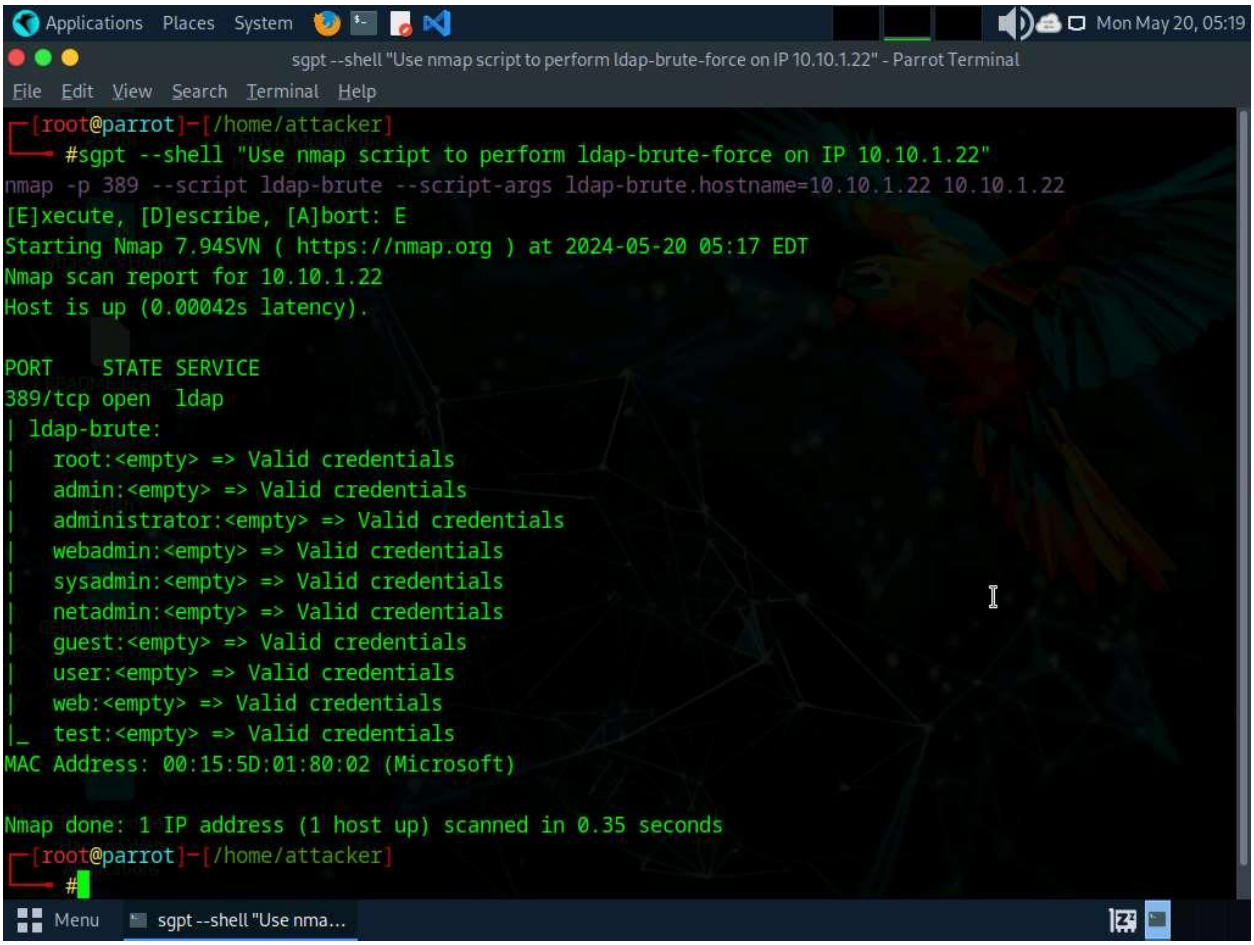
14. To create and execute a custom script to automate network enumeration tasks run **sgpt --chat enum --shell "Develop and execute a script which will automate various network enumeration tasks on target IP range 10.10.1.0/24"** command.

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



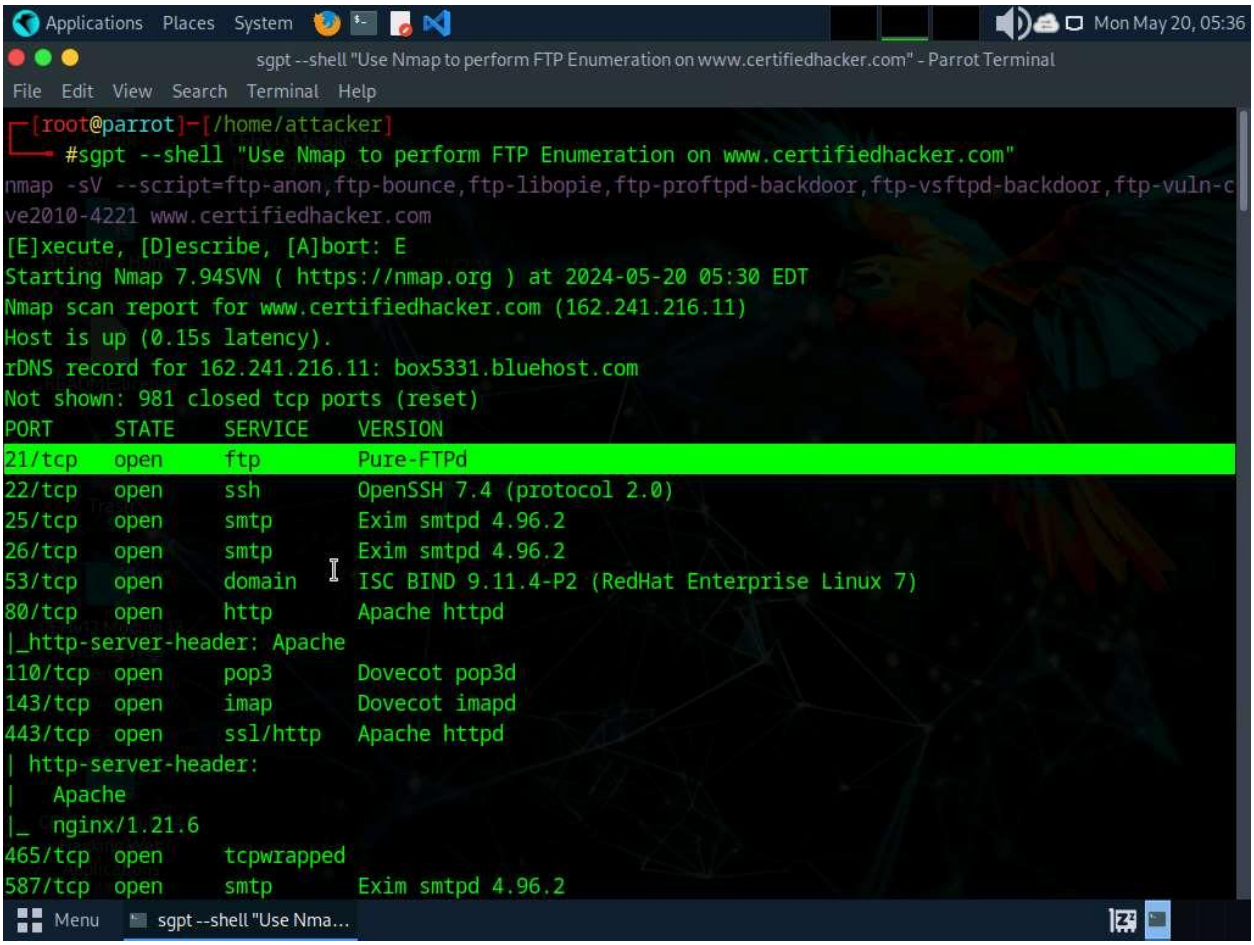
15. We will perform LDAP enumeration using ShellGPT, to do so, run **sgpt --shell "Use nmap script to perform ldap-brute-force on IP 10.10.1.22"** command.

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



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.



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.