Lab 3: Perform a Web Server Hacking using AI

Lab Scenario

The objective of this lab is to simulate the process of hacking a web server using AI-driven tools and techniques. This exercise will involve footprinting, fingerprinting, and exploiting vulnerabilities to understand the security posture of the target web server.

Lab Objectives

- Perform Web Server Footprinting and Attacks using ShellGPT

Overview of Web Server Hacking using AI

In the realm of cybersecurity, the role of artificial intelligence (AI) has become increasingly significant, especially in the domain of ethical hacking. AI-powered tools and techniques provide ethical hackers with enhanced capabilities to discover vulnerabilities, automate attacks, and strengthen defenses. Web server hacking, a critical aspect of penetration testing, leverages AI to perform footprinting, fingerprinting, and exploitation more efficiently and effectively.

Task 1: Perform Web Server Footprinting and Attacks using ShellGPT

Web server footprinting and subsequent attacks are critical steps in penetration testing or ethical hacking to assess the security posture of a target organization. ShellGPT, an AI-driven tool, enhances these processes by automating information gathering, fingerprinting, and vulnerability identification tasks.

Here we will use ShellGPT to perform Webserver footprinting and attacks using ShellGPT.

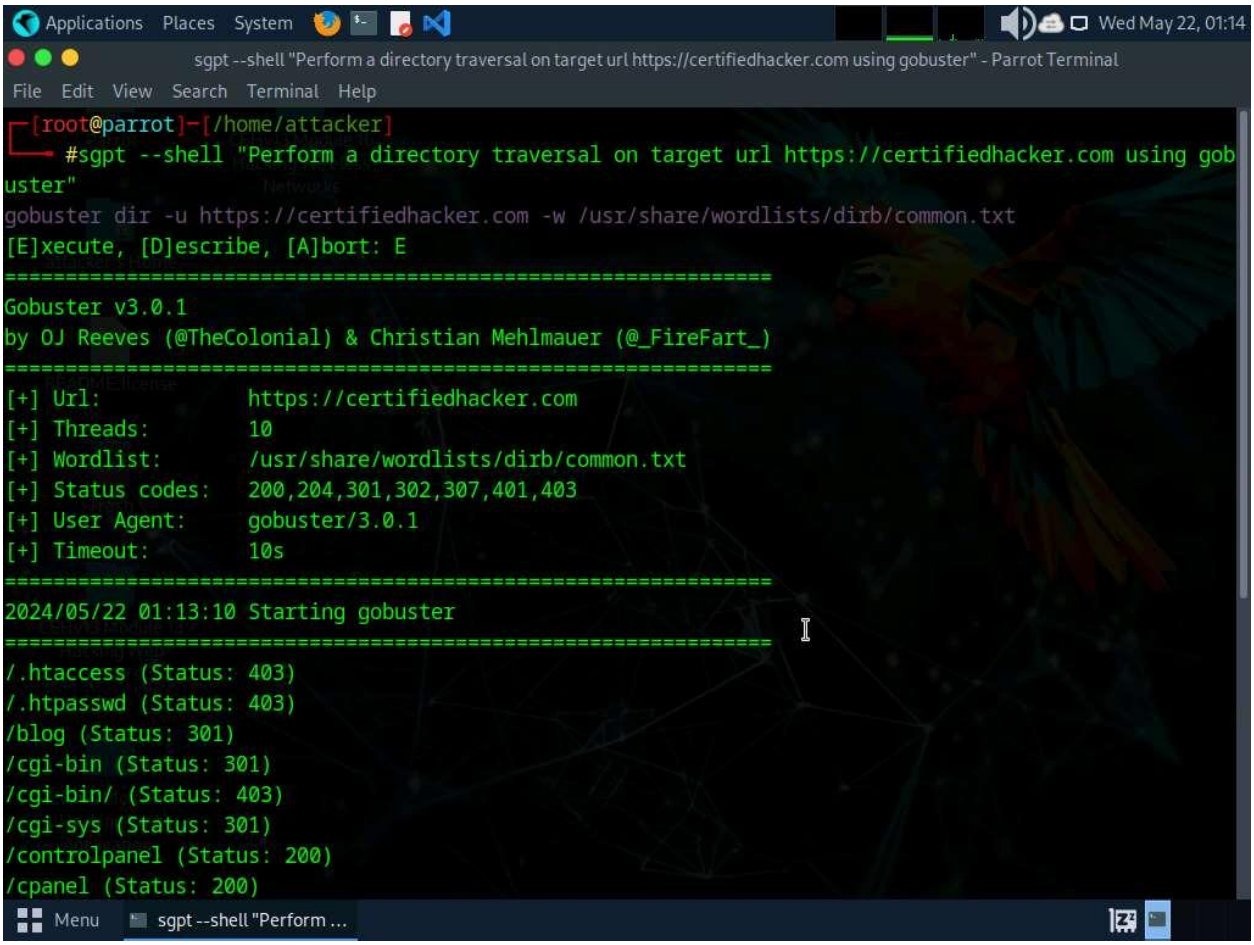
The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the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

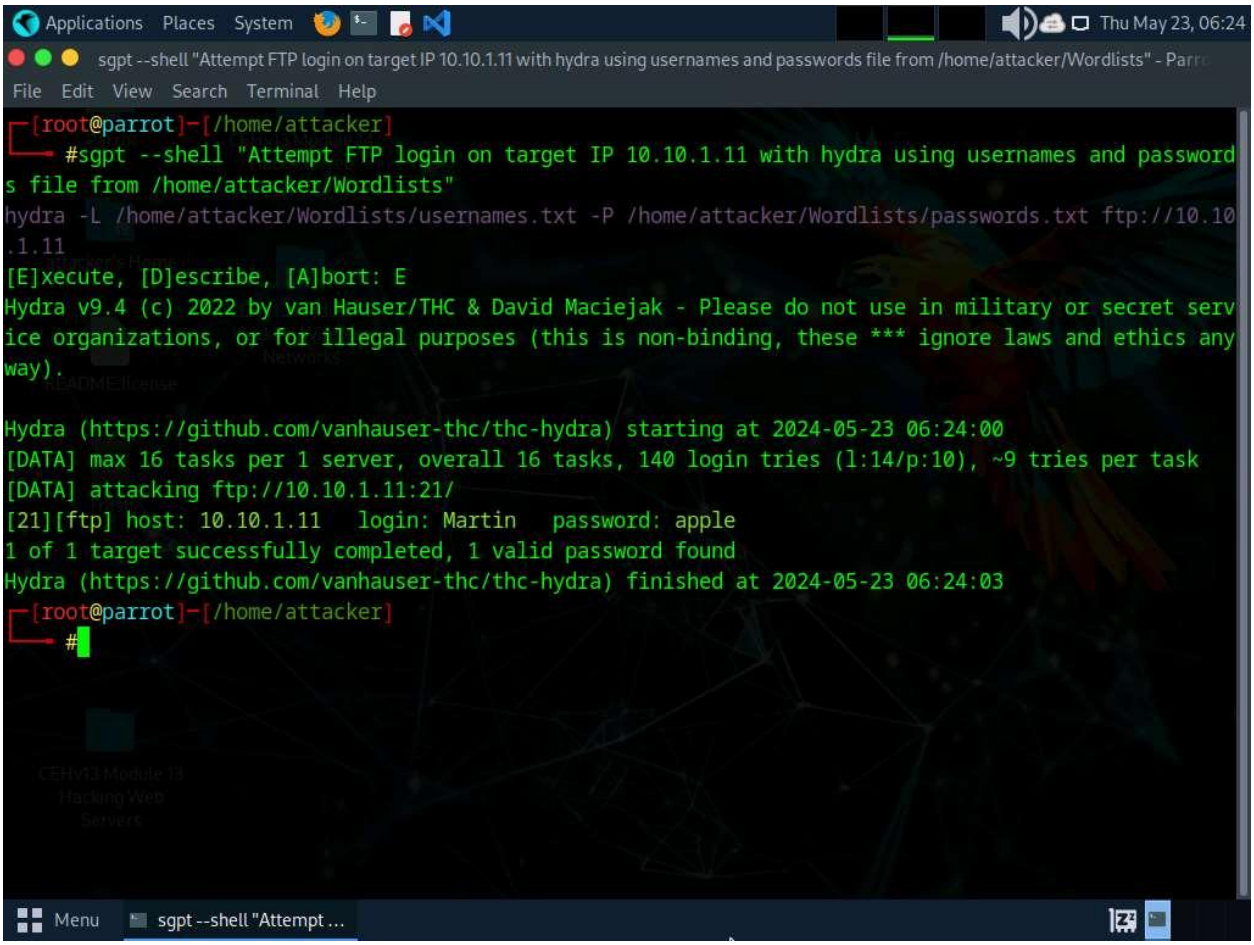
2. To perform directory traversal using ShellGPT, run **sgpt --shell "Perform a directory traversal on target url https://certifiedhacker.com using gobuster"** command.

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



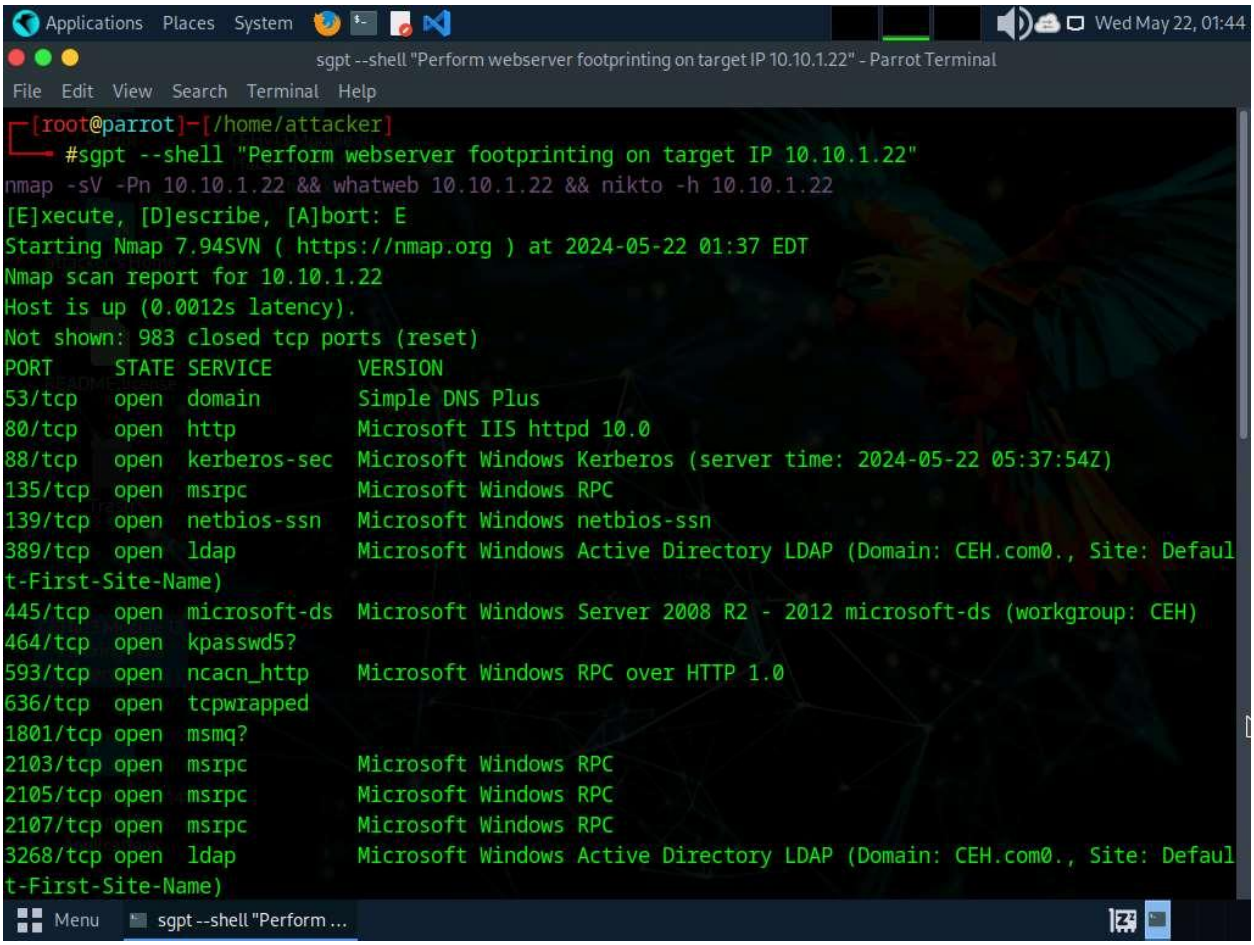
3. To perform FTP bruteforce attack run **sgpt --shell "Attempt FTP login on target IP 10.10.1.11 with hydra using usernames and passwords file from /home/attacker/Wordlists"** command.

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



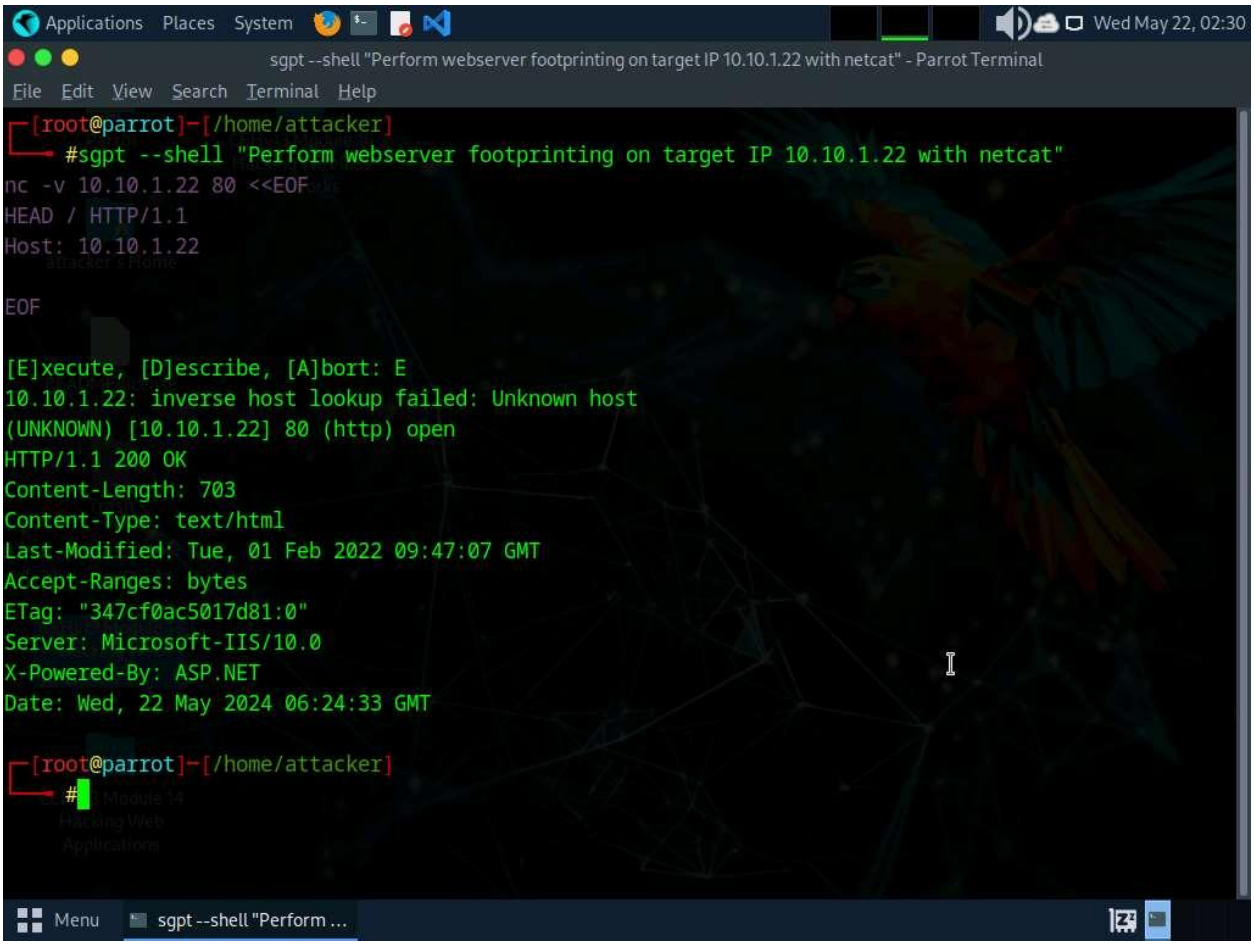
4. To perform webserver footprinting on target IP address using ShellGPT, run **sgpt --shell "Perform webserver footprinting on target IP 10.10.1.22"** command.

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



5. Run **sgpt --shell "Perform webserver footprinting on target IP 10.10.1.22 with netcat"** command to perform web server footprinting using netcat.

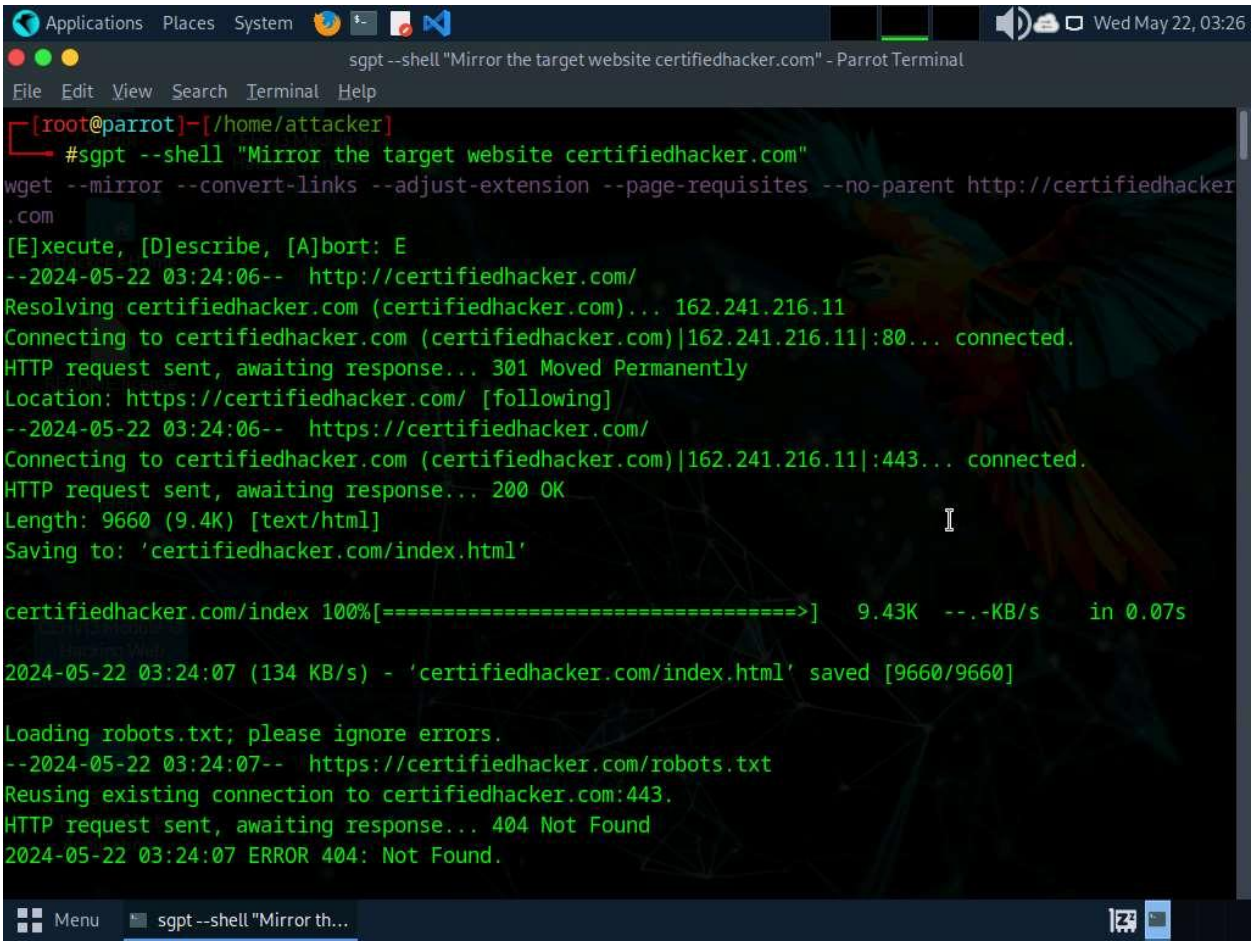
In the prompt type **E** and press **Enter** to execute the command.



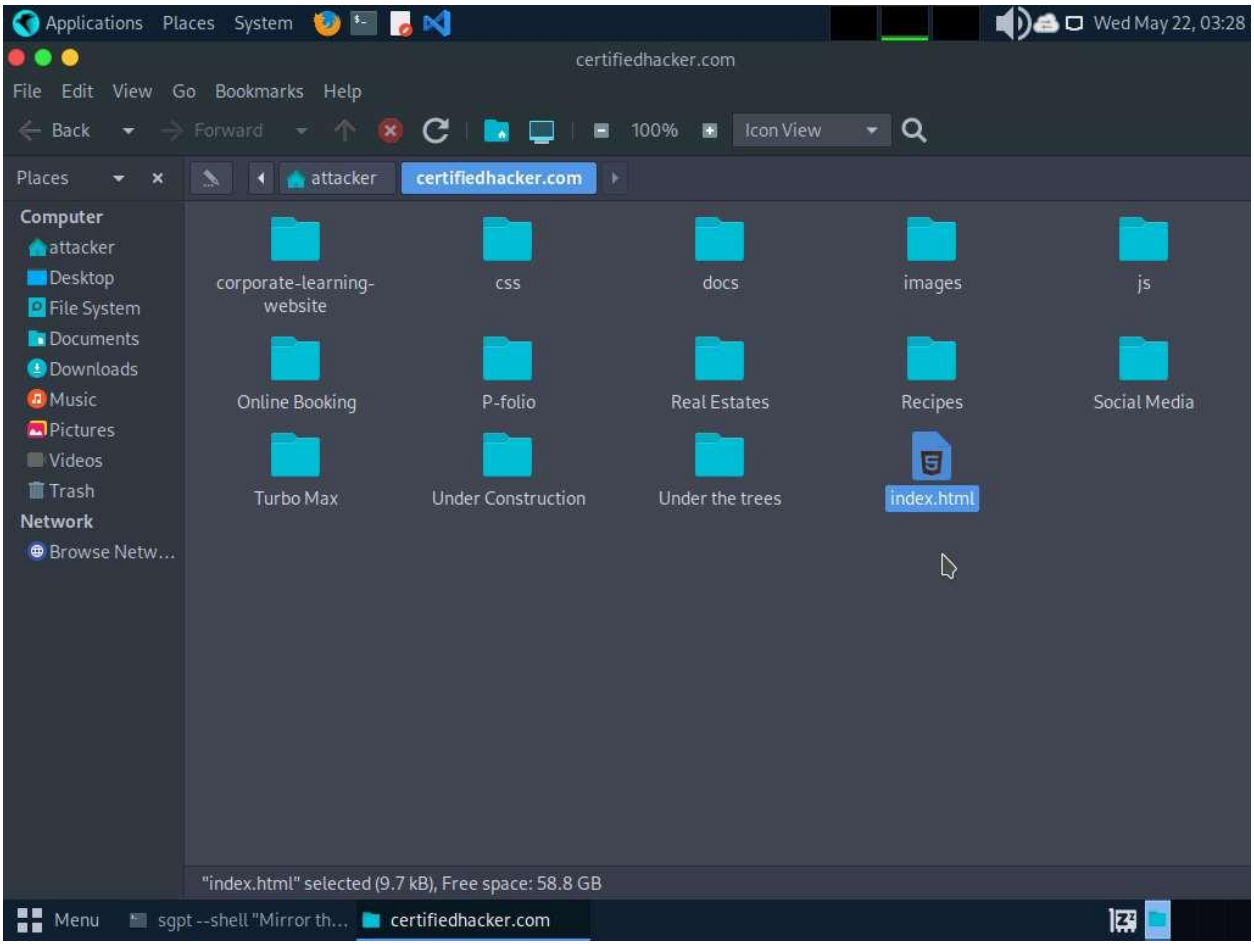
6. To perform website mirroring using ShellGPT, run **sgpt --shell "Mirror the target website certifiedhacker.com"** command.

Alternatively you can use Httrack to mirror a target website, to do so run **sgpt --shell "Mirror the target website https://certifiedhacker.com with httrack on desktop"** command.

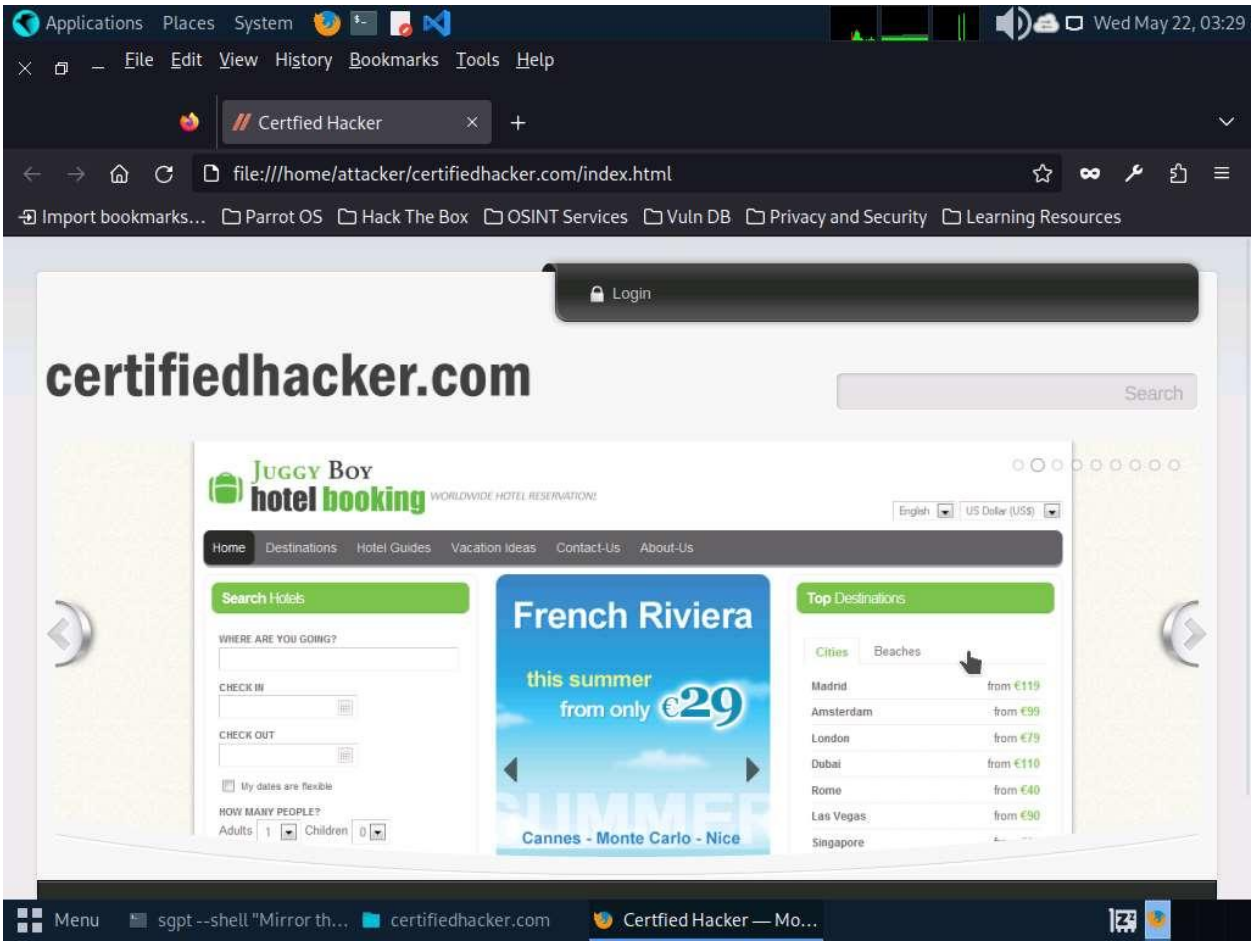
In the prompt type **E** and press **Enter** to execute the command.



7. To view the mirrored website navigate to **Places -> Home Folder -> certifiedhacker.com** location and double-click on **index.html** file.



8. The mirrored certifiedhacker.com website opens up in Firefox browser.



9. Apart from the aforementioned commands, you can further use ShellGPT prompts to perform Web Server Hacking.
10. This concludes the demonstration of webserver footprinting and attacks using ShellGPT.
11. Close all open windows and document all the acquired information.

Question 13.3.1.1

In Parrot Security machine, use ShellGPT to write and execute a prompt to perform directory traversal attack on https://certifiedhacker.com website using gobuster. Enter the status code of /docs directory of certifiedhacker.com that is displayed in the gobuster tool