Lab 9: Perform Footprinting using AI

Lab Scenario

In this lab, you will use AI to analyze and map digital footprints from social media data. The AI will identify patterns and highlight privacy risks. By comparing AI-generated insights with manual analysis, students will understand the power and limitations of AI in cybersecurity.

Lab Objectives

- Footprinting a target using ShellGPT

Overview of Footprinting using AI

Footprinting using AI accelerates the reconnaissance process by automating data collection and analysis, allowing security professionals to uncover vulnerabilities more efficiently. AI-powered footprinting enhances threat intelligence by identifying patterns and anomalies in vast amounts of data, providing deeper insights into potential risks. As an ethical hacker you should look for as much information as possible about the target using AI.

Task 1: Footprinting a Target using ShellGPT

Footprinting with ShellGPT involves leveraging shell scripting capabilities along with GPT's language processing prowess. By crafting tailored scripts, ShellGPT automates data gathering from various sources, including WHOIS databases and online forums. It parses and extracts relevant information such as domain registrations, IP addresses, and network configurations. ShellGPT streamlines the reconnaissance process, enabling efficient analysis and identification of potential security vulnerabilities. Its integration enhances the footprinting phase with automation and intelligent data processing.

Here, we will use ShellGPT to perform footprinting on a target.

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.

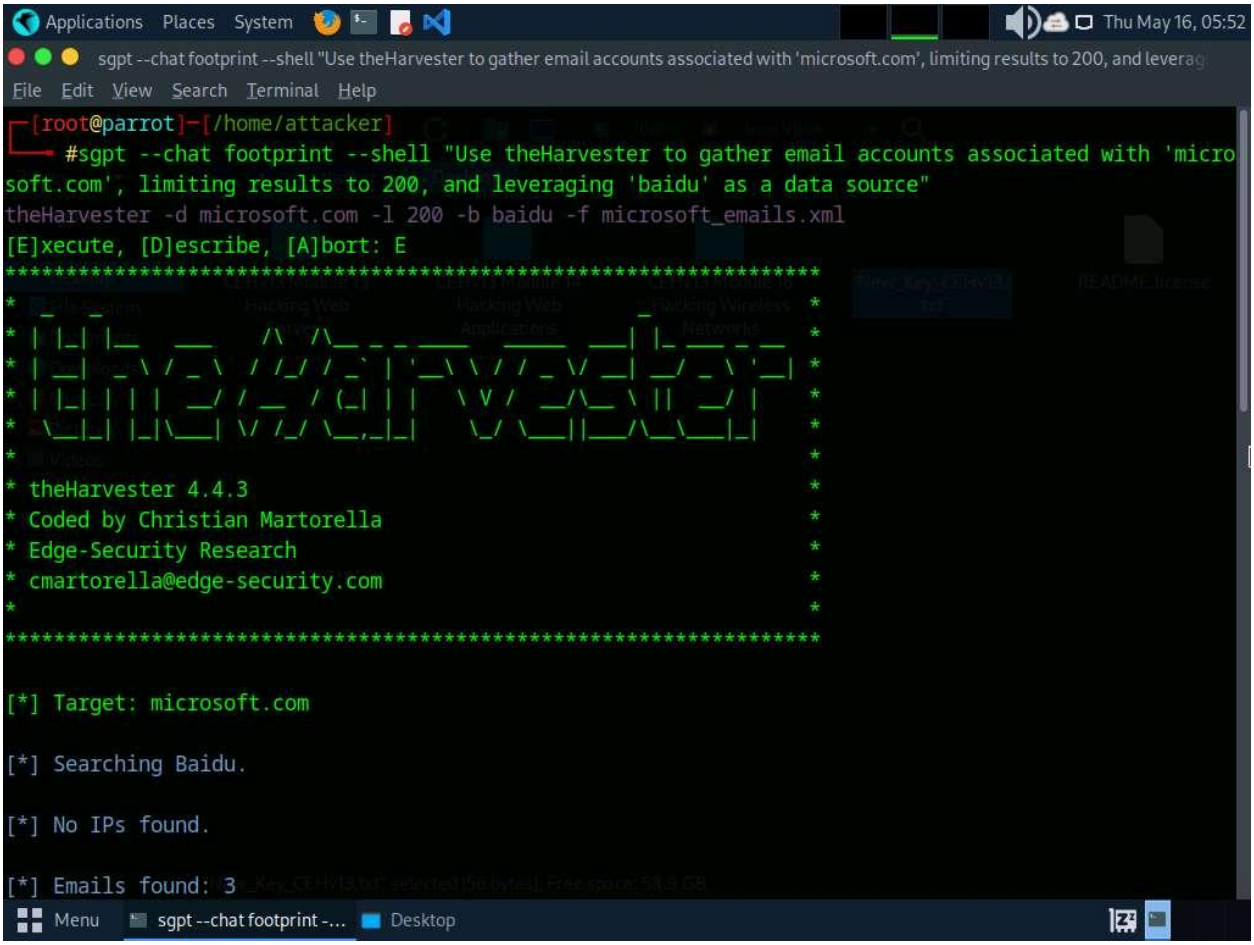
1. Before starting this lab, click Parrot Security to switch to the **Parrot Security** machine and incorporate ShellGPT by following steps provided in Integrate ShellGPT in Parrot Security Machine.pdf.

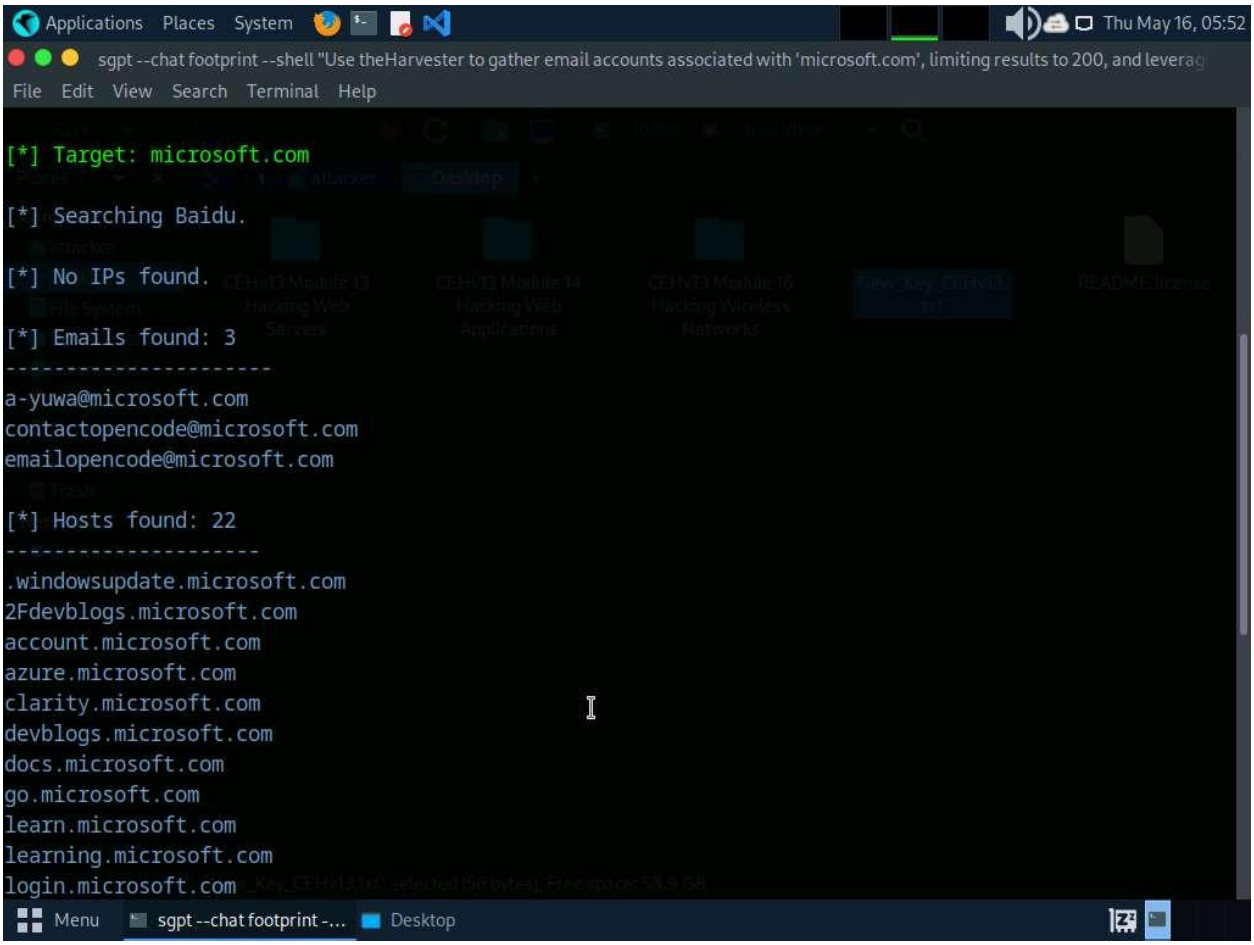
Alternatively, you can follow the steps to integrate **ShellGPT** provided in **Module 00: Integrate ShellGPT in Parrot Security Machine**.

2. After incorporating the ShellGPT API in **Parrot Security** machine, we will use ShellGPT for harvesting emails pertaining to a target organization. To do so, run **sgpt --chat footprint --shell "Use theHarvester to gather email accounts associated with 'microsoft.com', limiting results to 200, and leveraging 'baidu' as a data source"** command.

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

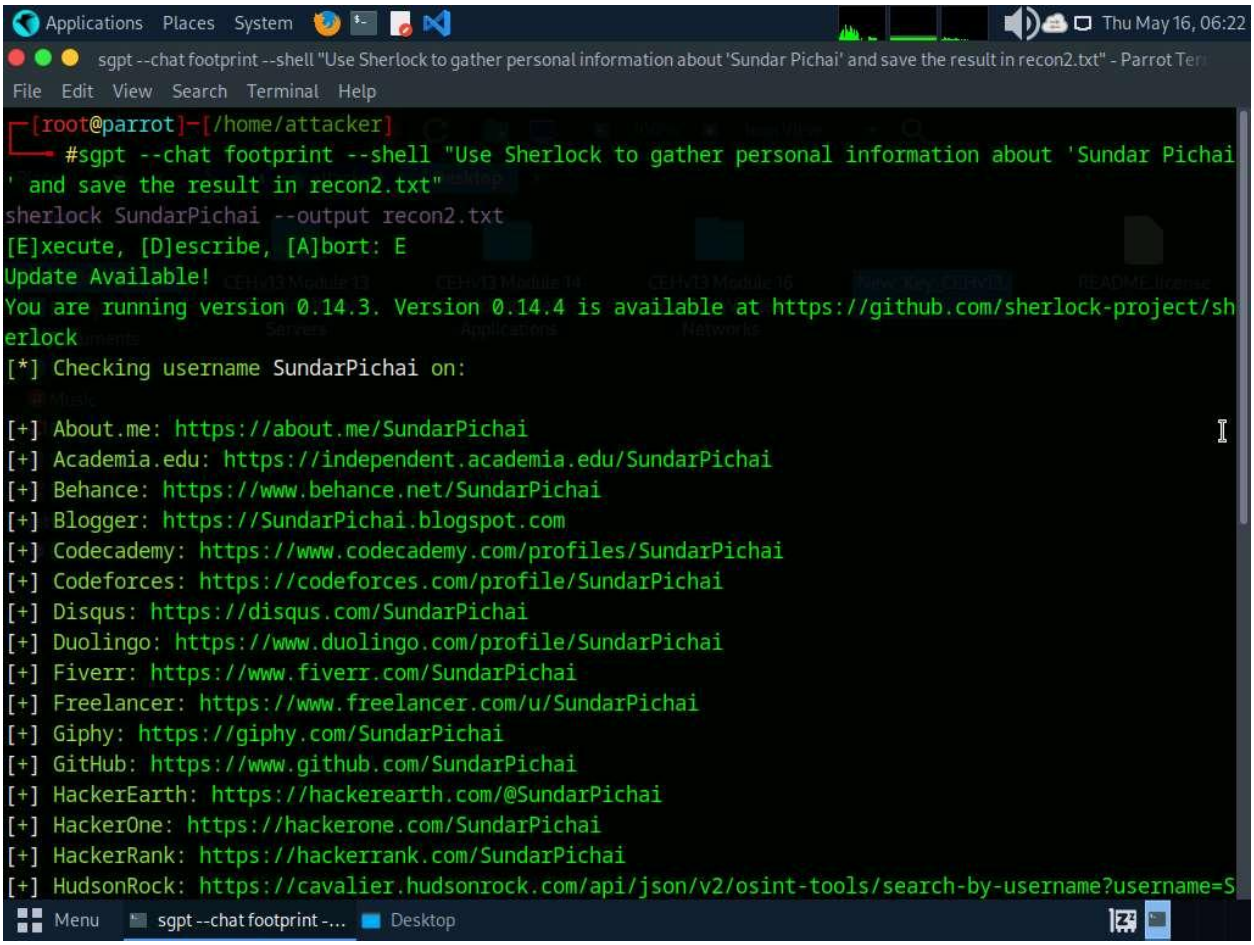
3. ShellGPT will harvest the emails using theHarvester tool and displays the email and host list.



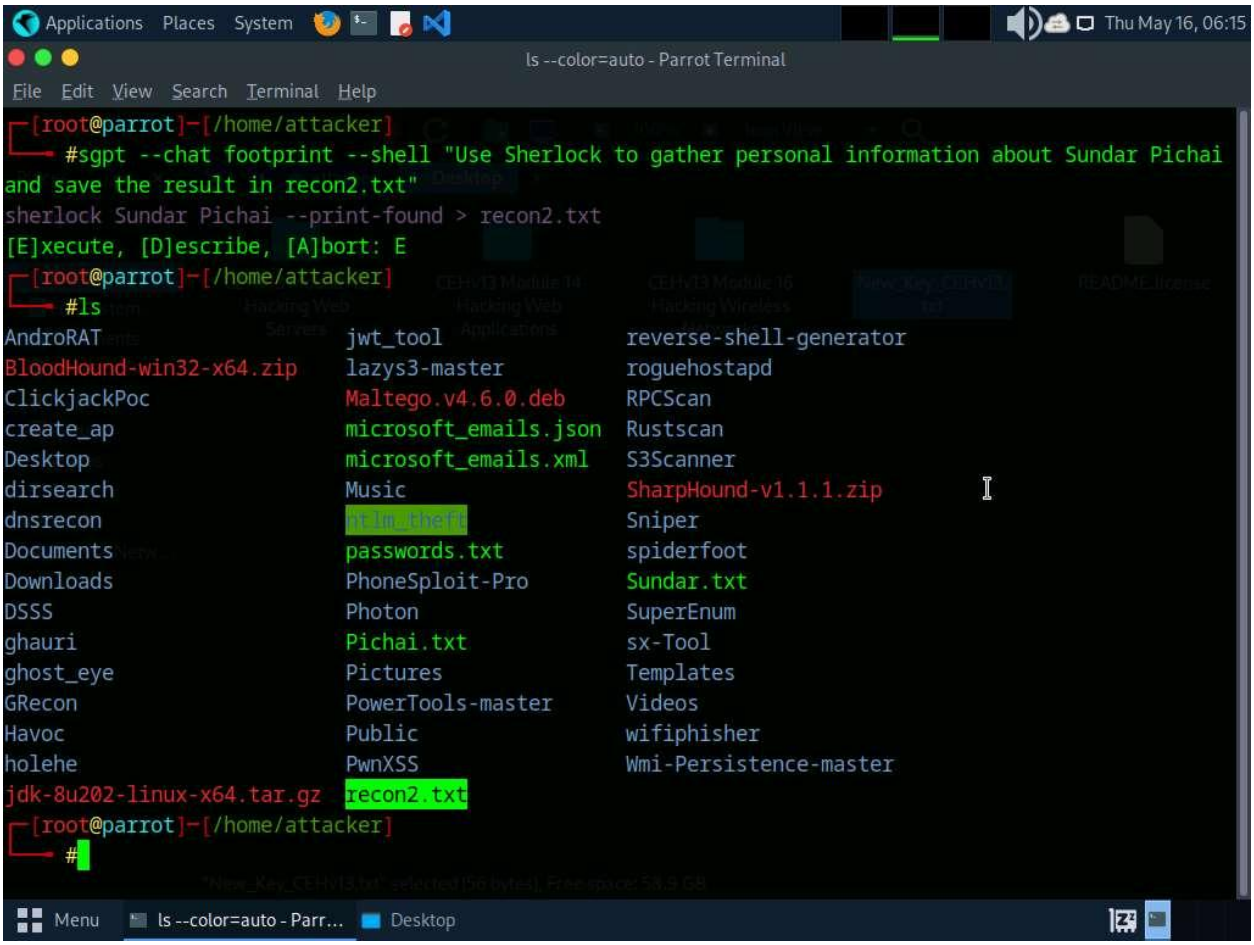


4. We will perform footprinting through social networking sites using ShellGPT, to do so run **sgpt --chat footprint --shell "Use Sherlock to gather personal information about 'Sundar Pichai' and save the result in recon2.txt"** command.

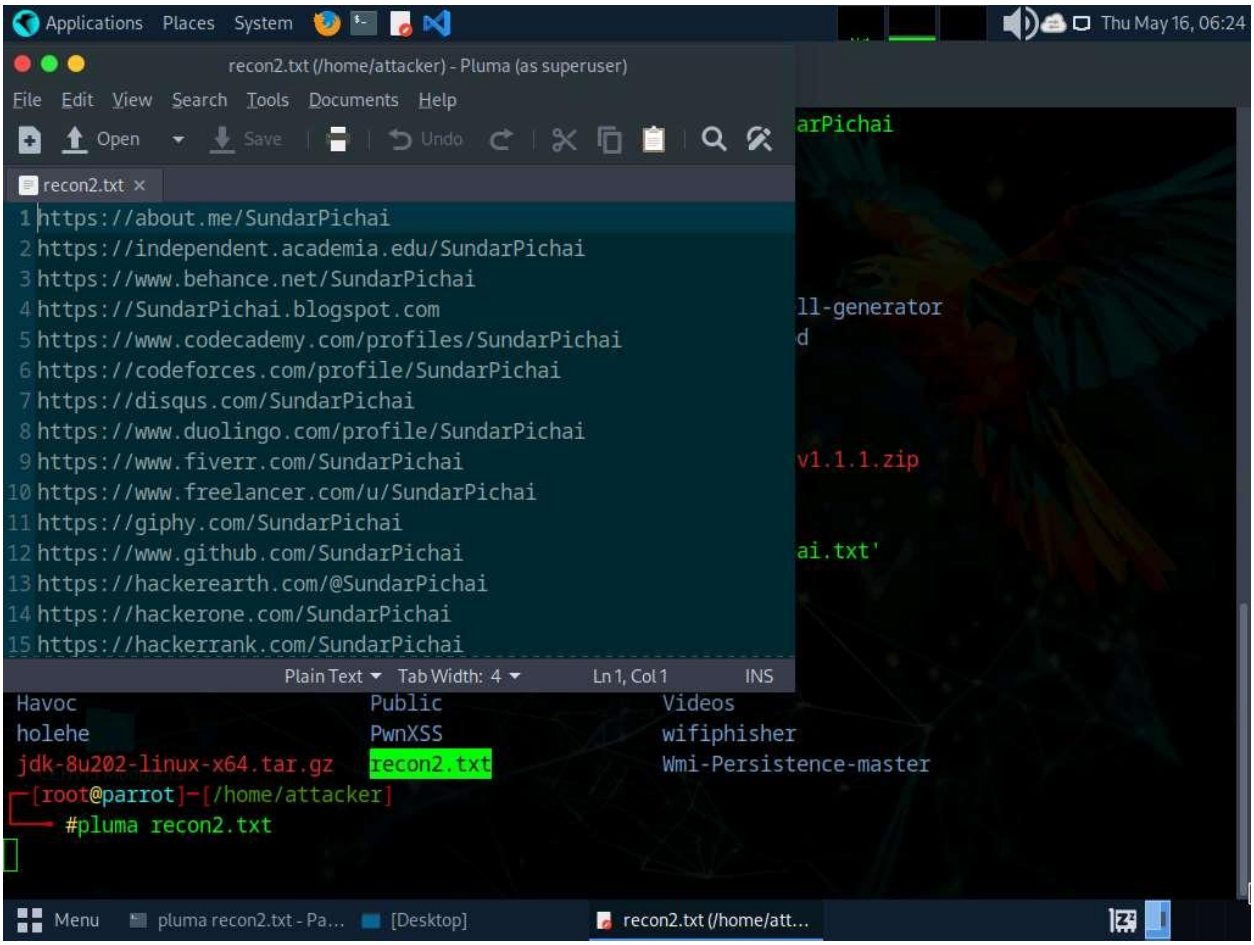
In the prompt type **E** and press **Enter** to execute the command.



5. After the execution of the command, in the terminal run **ls** command to view the contents in the present working directory.



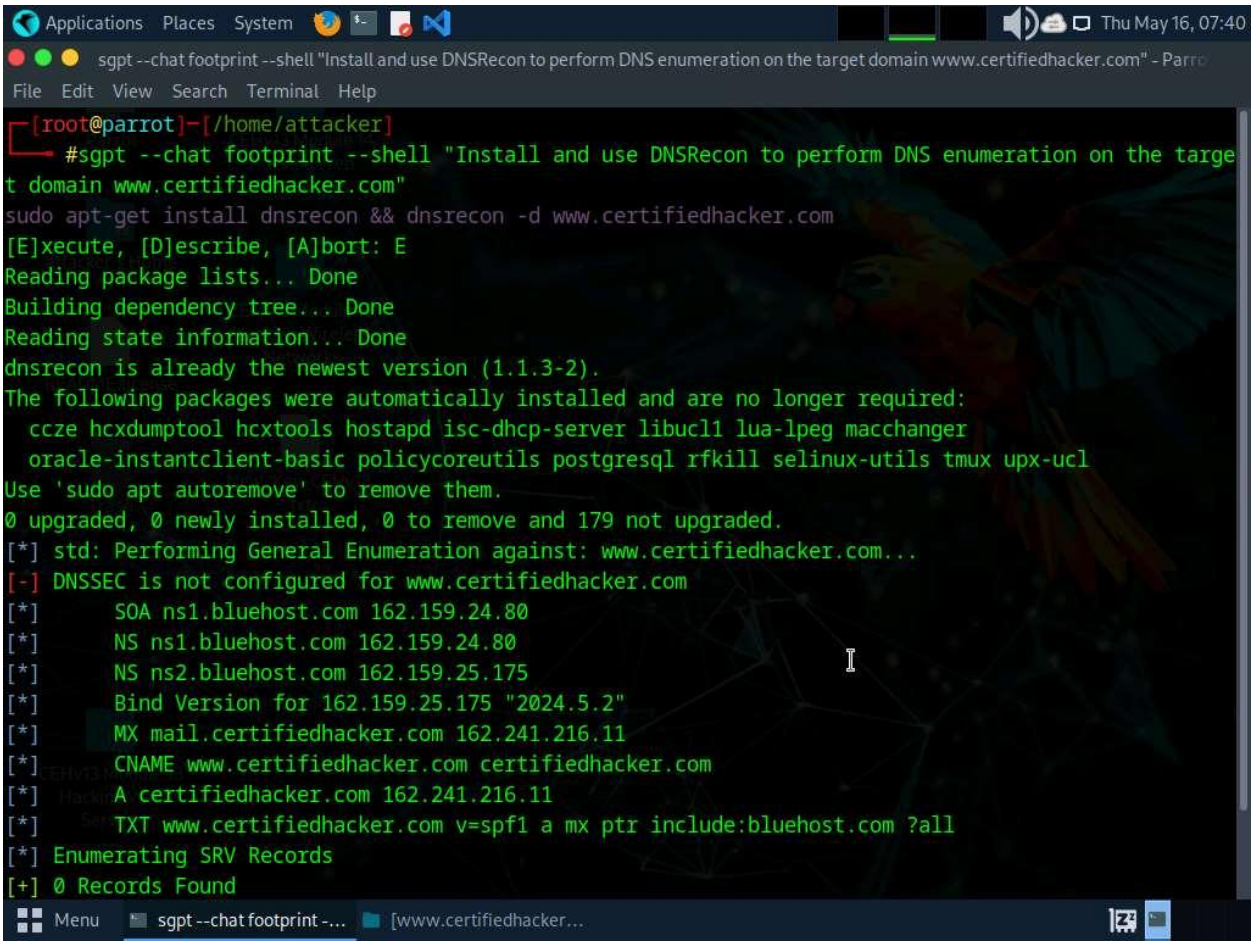
6. We can see that recon2.txt file is created by previous command. In the terminal window, run **pluma recon2.txt** command to view its contents. Close the text editor window.



ls

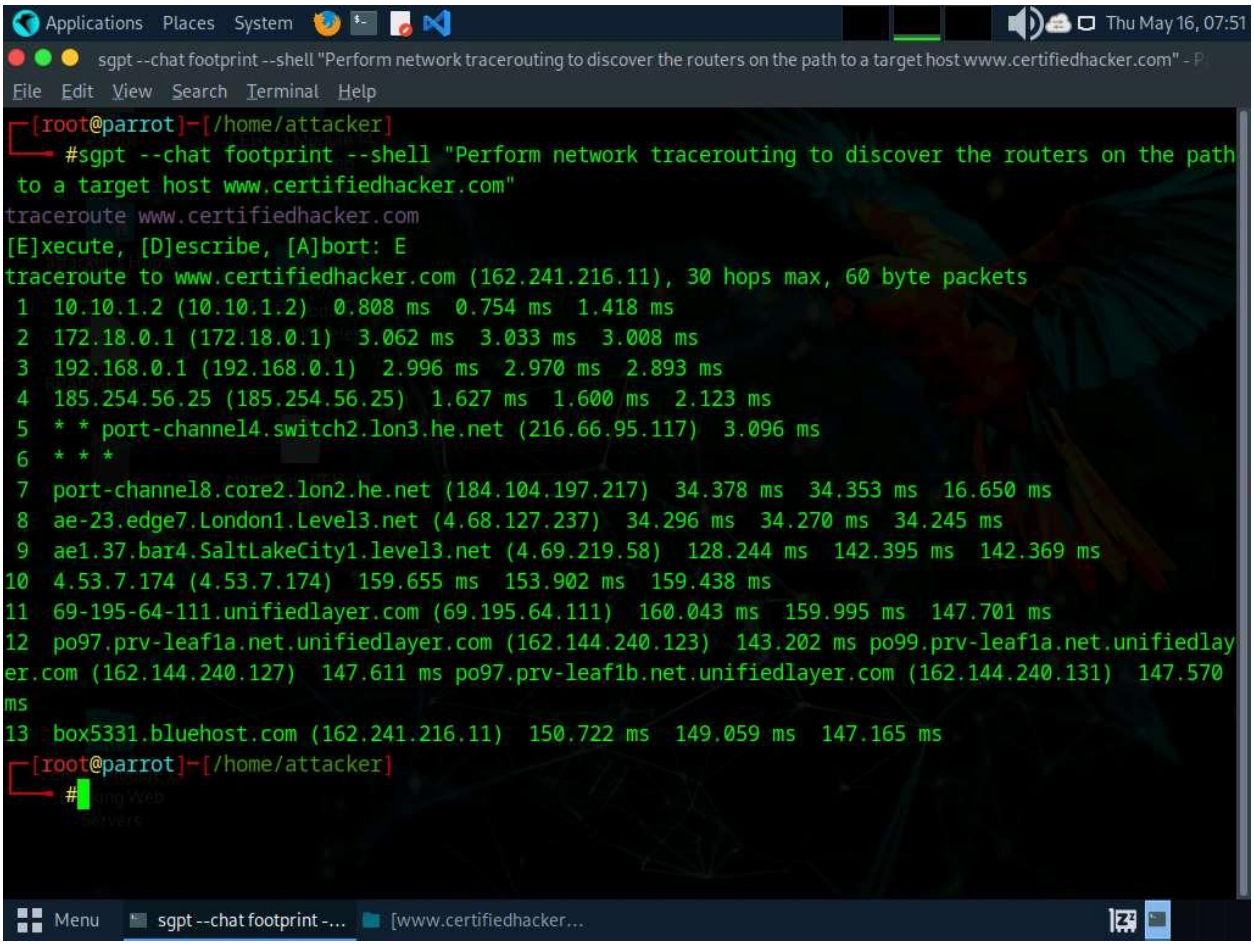
7. We will perform DNS lookup using ShellGPT, to do so, run **sgpt --chat footprint --shell "Install and use DNSRecon to perform DNS enumeration on the target domain www.certifiedhacker.com"** command.

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



8. In the terminal run **sgpt --chat footprint --shell "Perform network tracerouting to discover the routers on the path to a target host www.certifiedhacker.com"** command to perform Traceroute to a target.

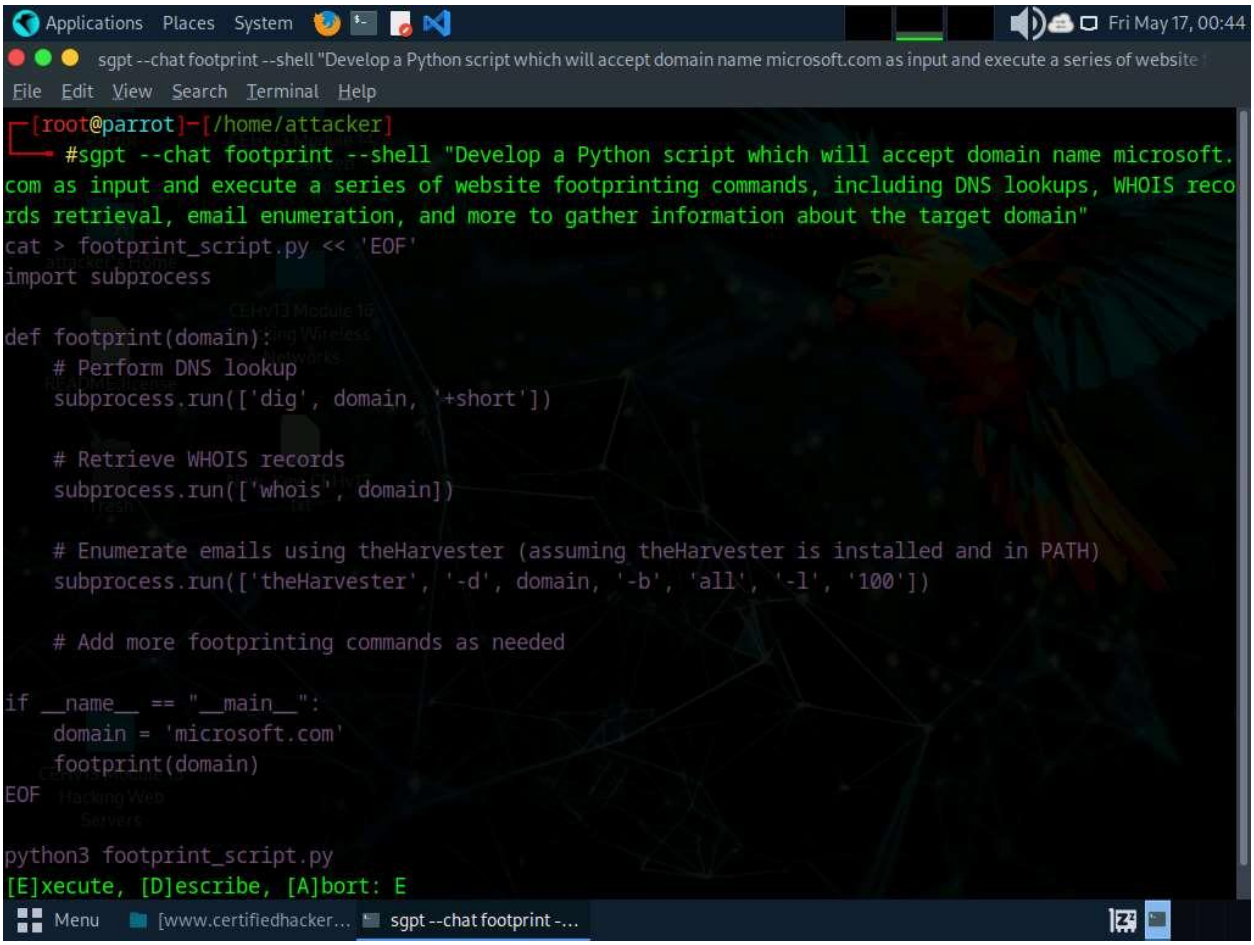
In the prompt type **E** and press **Enter** to execute the command.

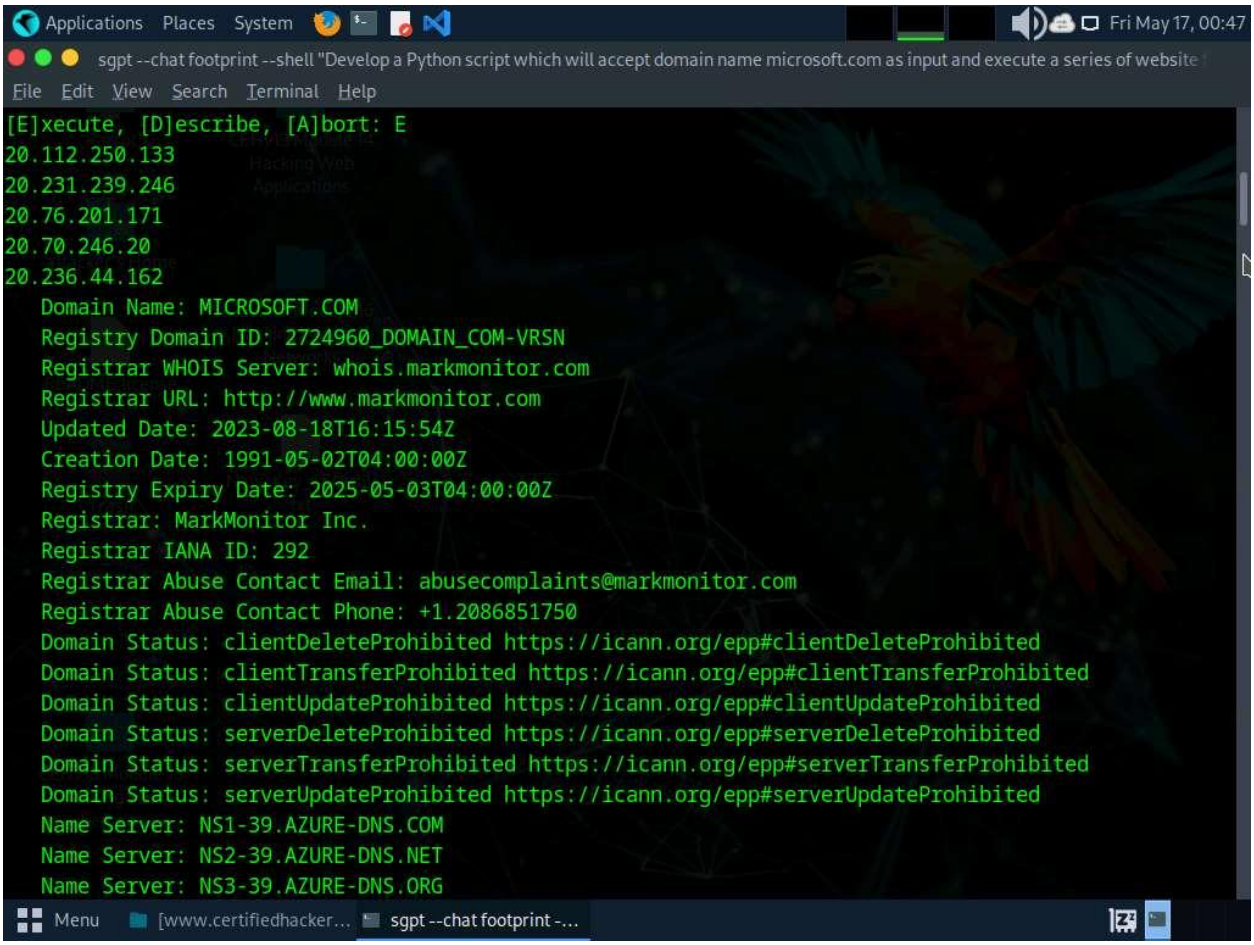


9. Now run **sgpt --chat footprint --shell "Develop a Python script which will accept domain name microsoft.com as input and execute a series of website footprinting commands, including DNS lookups, WHOIS records retrieval, email enumeration, and more to gather information about the target domain"** command to run a python script to automate footprinting tasks.

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

It might take some time develop and run the script.


Applications Places System
Fri May 17, 00:44
sgpt --chat footprint --shell "Develop a Python script which will accept domain name microsoft.com as input and execute a series of website
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#sgpt --chat footprint --shell "Develop a Python script which will accept domain name microsoft.com as input and execute a series of website footprinting commands, including DNS lookups, WHOIS records retrieval, email enumeration, and more to gather information about the target domain"
cat > footprint_script.py << 'EOF'
import subprocess
def footprint(domain):
# Perform DNS lookup
subprocess.run(['dig', domain, '+short'])
# Retrieve WHOIS records
subprocess.run(['whois', domain])
# Enumerate emails using theHarvester (assuming theHarvester is installed and in PATH)
subprocess.run(['theHarvester', '-d', domain, '-b', 'all', '-l', '100'])
# Add more footprinting commands as needed
if __name__ == "__main__":
domain = 'microsoft.com'
footprint(domain)
EOF
python3 footprint_script.py
[E]xecute, [D]escribe, [A]bort: E
Menu
[www.certifiedhacker...
sgpt --chat footprint -...



10. Apart from the aforementioned commands, you can further explore additional options within the ShellGPT tool and utilize various other tools to conduct footprinting on the target.
11. This concludes the demonstration of performing footprinting using the ShellGPT.
12. Close all open windows and document all the acquired information.