Module 02: Footprinting and Reconnaissance

Scenario

Reconnaissance refers to collecting information about a target, which is the first step in any attack on a system. It has its roots in military operations, where the term refers to the mission of collecting information about an enemy. Reconnaissance helps attackers narrow down the scope of their efforts and aids in the selection of weapons of attack. Attackers use the gathered information to create a blueprint, or "footprint," of the organization, which helps them select the most effective strategy to compromise the system and network security.
Similarly, the security assessment of a system or network starts with the reconnaissance and footprinting of the target. Ethical hackers and penetration (pen) testers must collect enough information about the target of the evaluation before initiating assessments. Ethical hackers and pen testers should simulate all the steps that an attacker usually follows to obtain a fair idea of the security posture of the target organization. In this scenario, you work as an ethical hacker with a large organization. Your organization is alarmed at the news stories concerning new attack vectors plaguing large organizations around the world. Furthermore, your organization was the target of a major security breach in the past where the personal data of several of its customers were exposed to social networking sites.
You have been asked by senior managers to perform a proactive security assessment of the company. Before you can start any assessment, you should discuss and define the scope with management; the scope of the assessment identifies the systems, network, policies and procedures, human resources, and any other component of the system that requires security evaluation. You should also agree with management on rules of engagement (RoE)-the "do's and don'ts" of assessment. Once you have the necessary approvals to perform ethical hacking, you should start gathering information about the target organization. Once you methodologically begin the footprinting process, you will obtain a blueprint of the security profile of the target organization. The term "blueprint" refers to the unique system profile of the target organization as the result of footprinting.
The labs in this module will give you a real-time experience in collecting a variety of information about the target organization from various open or publicly accessible sources.

Objective

The objective of the lab is to extract information about the target organization that includes, but is not limited to:

- **Organization Information**Employee details, addresses and contact details, partner details, weblinks, web technologies, patents, trademarks, etc.

Footprinting and Reconnaissance

- **Network Information**Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records, and other related information
- **System Information**Operating systems, web server OSes, location of web servers, user accounts and passwords, etc.

Overview of Footprinting

Footprinting refers to the process of collecting information about a target network and its environment, which helps in evaluating the security posture of the target organization's IT infrastructure. It also helps to identify the level of risk associated with the organization's publicly accessible information.
Footprinting can be categorized into passive footprinting and active footprinting:

- **Passive Footprinting**: Involves gathering information without direct interaction. This type of footprinting is principally useful when there is a requirement that the information-gathering activities are not to be detected by the target.
- **Active Footprinting**: Involves gathering information with direct interaction. In active footprinting, the target may recognize the ongoing information gathering process, as we overtly interact with the target network.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the target. Recommended labs that will assist you in learning various footprinting techniques include:

1. Perform footprinting through search engines
    - Gather information using advanced Google hacking techniques
2. Perform footprinting through Internet Research Services
    - Find the company's domains, sub-domains, and Hosts using Netcraft and DNSdumpster
3. Perform footprinting through social networking sites
    - Gather personal information from various social networking sites using Sherlock
4. Perform Whois footprinting
    - Perform Whois lookup using DomainTools
5. Perform DNS footprinting
    - Gather DNS information using nslookup command line utility and online tool
6. Perform network footprinting
    - Perform network tracerouting in Windows and Linux Machines
7. Perform email footprinting
    - Gather information about a target by tracing emails using eMailTrackerPro

8. Perform footprinting using various footprinting tools
    - Footprinting a target using Recon-ng
9. Perform Footprinting using AI
    - Footprinting a target using Shellgpt

Lab 1: Perform Footprinting Through Search Engines

Lab Scenario
As a professional ethical hacker or pen tester, your first step is to gather maximum information about the target organization by performing footprinting using search engines; you can perform advanced image searches, reverse image searches, advanced video searches, etc. Through the effective use of search engines, you can extract critical information about a target organization such as technology platforms, employee details, login pages, intranet portals, contact details, etc., which will help you in performing social engineering and other types of advanced system attacks.
Lab Objectives

- Gather information using advanced Google hacking techniques

Overview of Search Engines
Search engines use crawlers, automated software that continuously scans active websites, and add the retrieved results to the search engine index, which is further stored in a huge database. When a user queries a search engine index, it returns a list of Search Engine Results Pages (SERPs). These results include web pages, videos, images, and many different file types ranked and displayed based on their relevance. Examples of major search engines include Google, Bing, Yahoo, Ask, Aol, Baidu, WolframAlpha, and DuckDuckGo.

Task 1: Gather Information using Advanced Google Hacking Techniques

Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results. This can provide information about websites that are vulnerable to exploitation.

Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

1. By default, **Windows 11** machine selected, click Ctrl+Alt+Delete and login with **Admin/Pa$$w0rd**.
2. Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 11** machine thumbnail in the **Resources** pane.
3. more...
4. Alternatively, you can also click **Pa$$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane.
5. more...

6. Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

7. Launch any web browser, and go to **https://www.google.com** (here, we are using **Mozilla Firefox**).

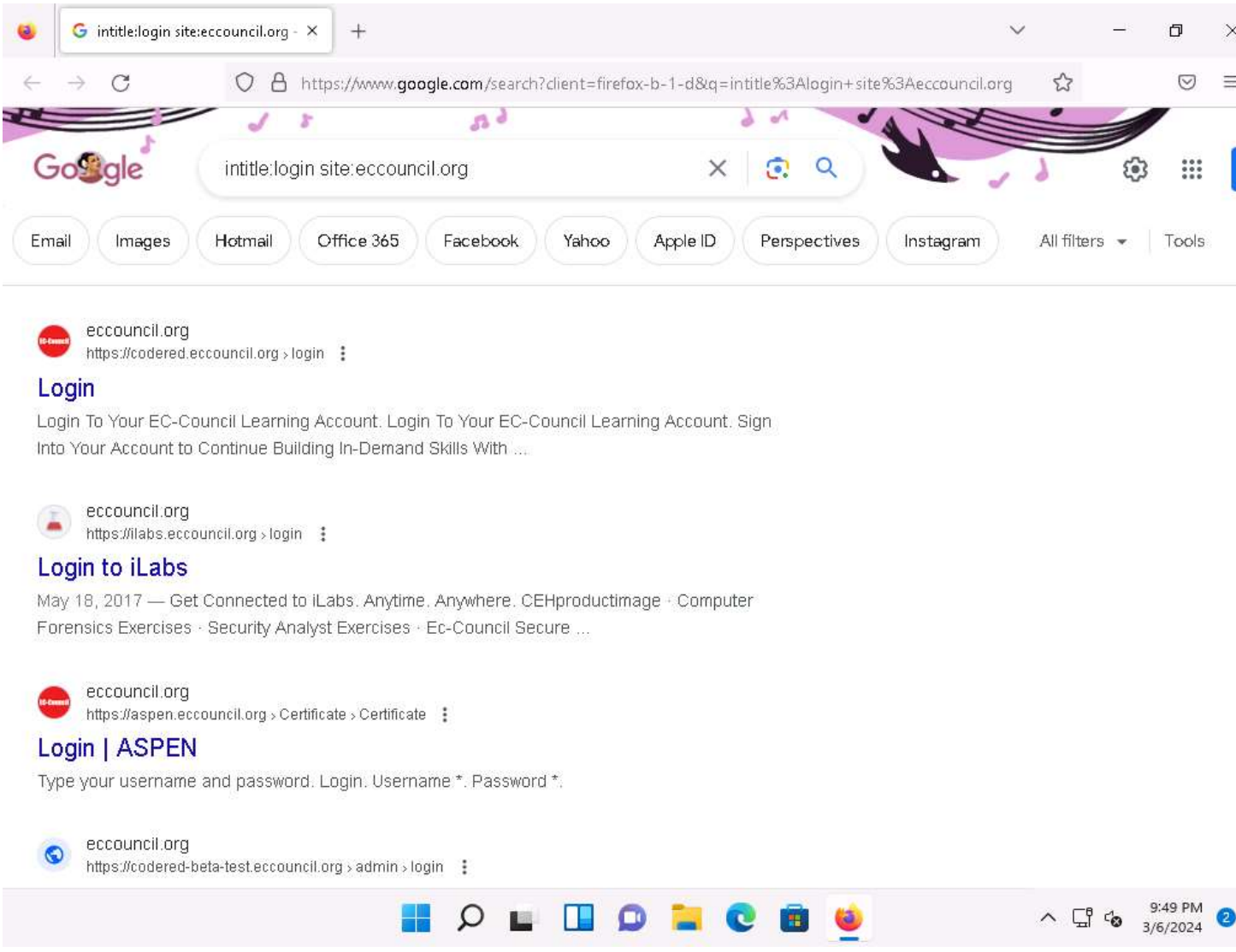
8. If a **Firefox Software Updater** window appears click **No**.

    - If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.
    - If a notification appears, click **Okay, Got it** to finish viewing the information.

9. In the search bar search for **intitle:login site:eccouncil.org**. This search command uses **intitle** and **site** Google advanced operators, which restrict results to pages on the **eccouncil.org** website that contain the **login** pages. An example is shown in the screenshot below.

10. Here, this Advanced Google Search operator can help attackers and pen testers to extract login pages of the target organization's website. Attackers can subject login pages to various attacks such as credential bruteforcing, injection attacks and other web application attacks. Similarly, assessing the login pages against various attacks is crucial for penetration testing.

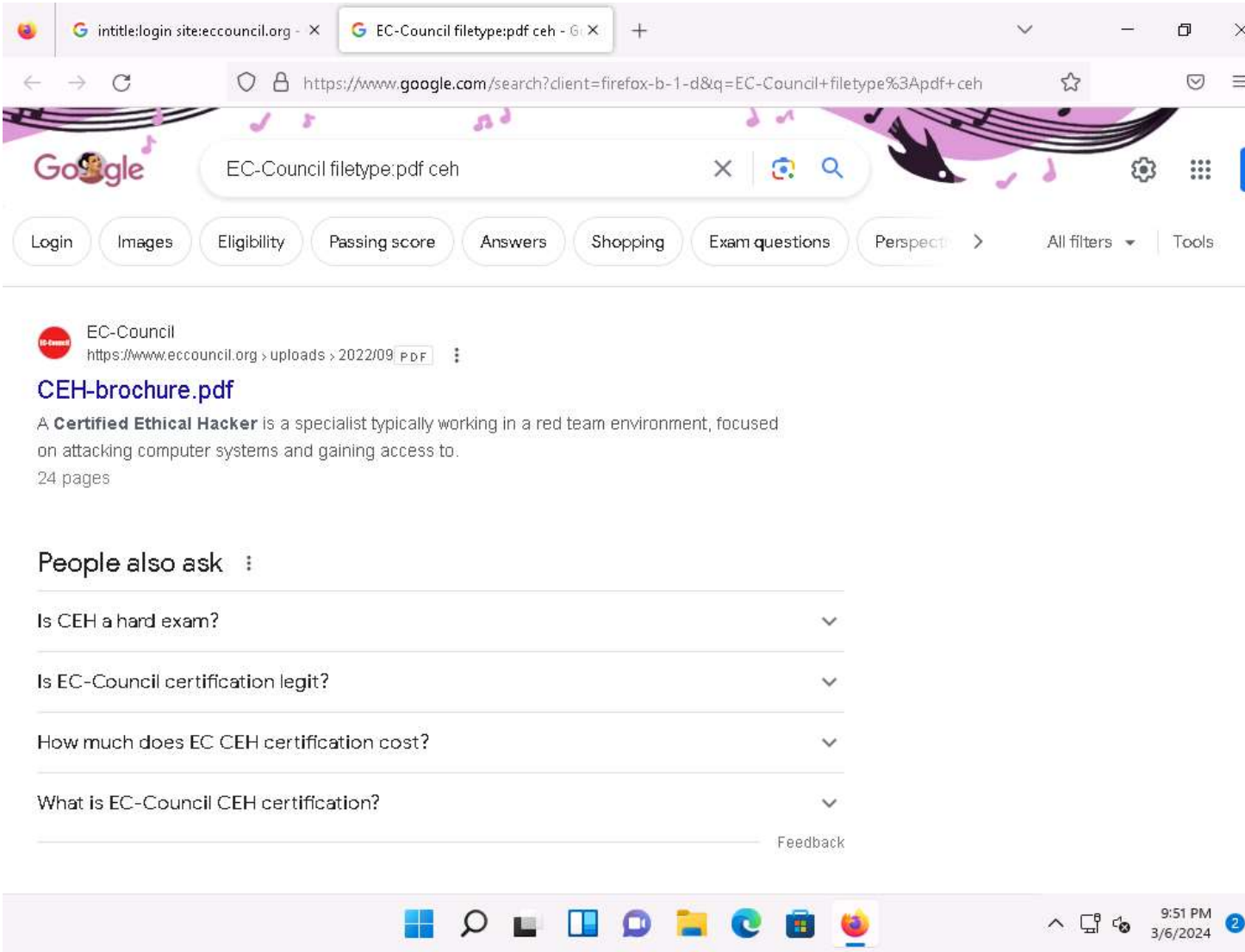
11.



12. Similarly, type the command **EC-Council filetype:pdf ceh** in the search bar to search your results based on the file extension and the keyword (here, **ceh**). Click on any link from the results (here, **CEH-brochure.pdf**) to view the pdf file.

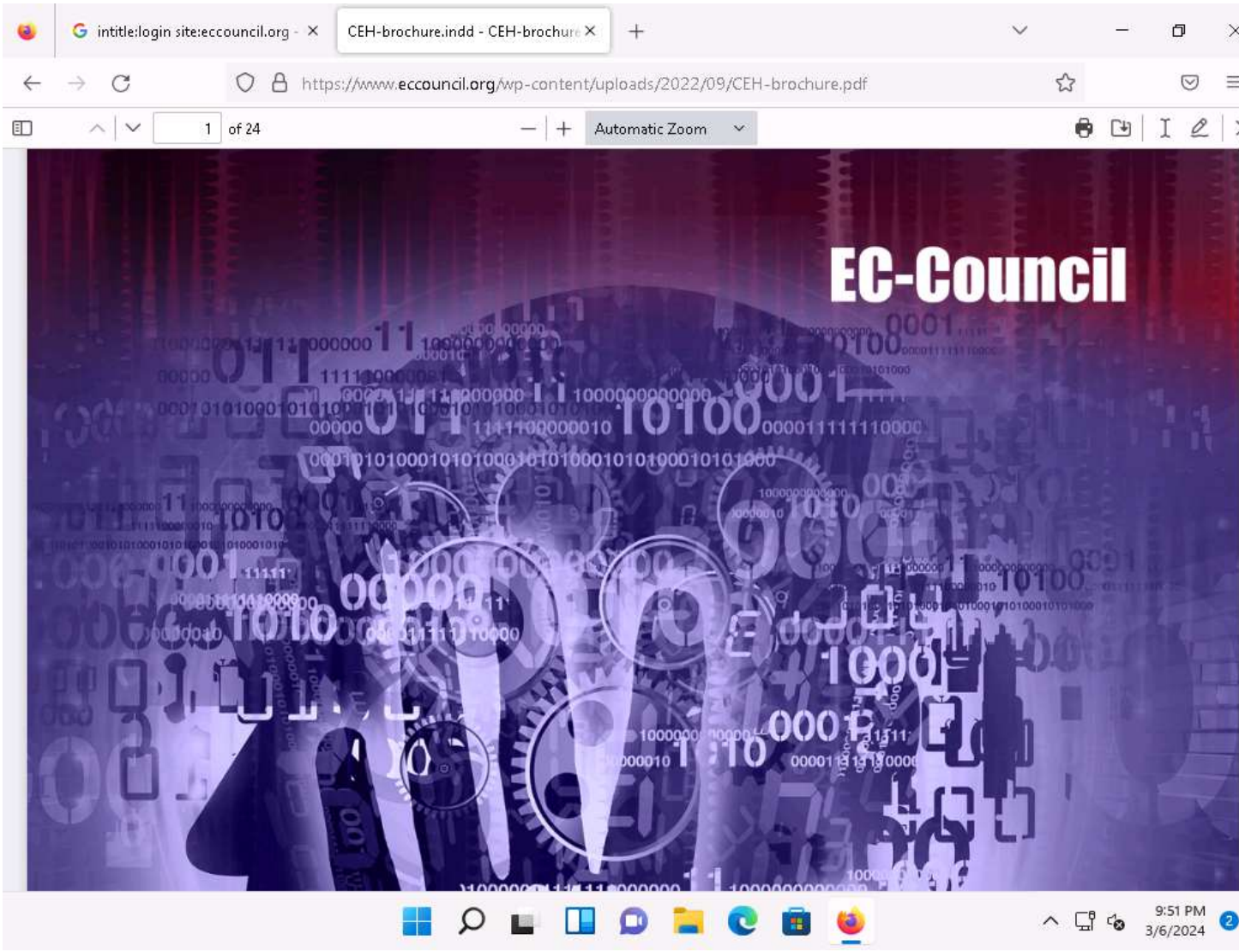
13. Here, the file type pdf is searched for the target organization EC-Council. The result might differ when you perform this task.
14. The PDF and other documents from a target website may provide sensitive information about the target's products and services. They may help attackers to determine an attack vector to exploit the target.

15.



16. The page appears displaying the PDF file, as shown in the screenshot.

17.



18. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.

- **cache**: This operator allows you to view cached version of the web page. [cache:www.eccouncil.org]- Query returns the cached version of the website www.eccouncil.org
- **allinurl**: This operator restricts results to pages containing all the query terms specified in the URL. [allinurl: EC-Council career]-Query returns only pages containing the words "EC-Council" and "career" in the URL
- **inurl**: This operator restricts the results to pages containing the word specified in the URL [inurl: copy site:www.eccouncil.org]-Query returns only pages in EC-Council site in which the URL has the word "copy"
- **allintitle**: This operator restricts results to pages containing all the query terms specified in the title. [allintitle: detect malware]-Query returns only pages containing the words "detect" and "malware" in the title
- **inanchor**: This operator restricts results to pages containing the query terms specified in the anchor text on links to the page. [Anti-virus inanchor:Norton]-Query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus"
- **allinanchor**: This operator restricts results to pages containing all query terms specified in the anchor text on links to the page. [allinanchor: best cloud service provider]-Query returns only pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider"

- **link**: This operator searches websites or pages that contain links to the specified website or page. [link:www.eccouncil.org]-Finds pages that point to EC-Council's home page
- **related**: This operator displays websites that are similar or related to the URL specified. [related:www.eccouncil.org]-Query provides the Google search engine results page with websites similar to eccouncil.org
- **info**: This operator finds information for the specified web page. [info:eccouncil.org]-Query provides information about the www.eccouncil.org home page
- **location**: This operator finds information for a specific location. [location: EC-Council]-Query give you results based around the term EC-Council

19. This concludes the demonstration of gathering information using advanced Google hacking techniques. You can conduct a series of queries on your own by using these advanced Google operators and gather the relevant information about the target organization.
20. Close all open windows and document all the acquired information.

Lab 2: Perform Footprinting Through Internet Research Services

---

Lab Scenario

As a professional ethical hacker or pen tester, you should be able to extract a variety of information about your target organization from Internet research services. By doing so, you can extract critical information such as a target organization's domains, subdomains, operating systems, geographic locations, employee details, emails, financial information, infrastructure details, hidden web pages and content, etc.

Using this information, you can build a hacking strategy to break into the target organization's network and can carry out other types of advanced system attacks.

Lab Objectives

- Find the company's domains and subdomains using Netcraft and DNSdumpster

Overview of Internet Research Services

Internet research services such as people search services, alerting services, financial services, and job sites, provide information about a target organization; for example, infrastructure details, physical location, employee details, etc. Moreover, groups, forums, and blogs may provide sensitive information about a target organization such as public network information, system information, and personal information. Internet archives may provide sensitive information that has been removed from the World Wide Web (WWW).

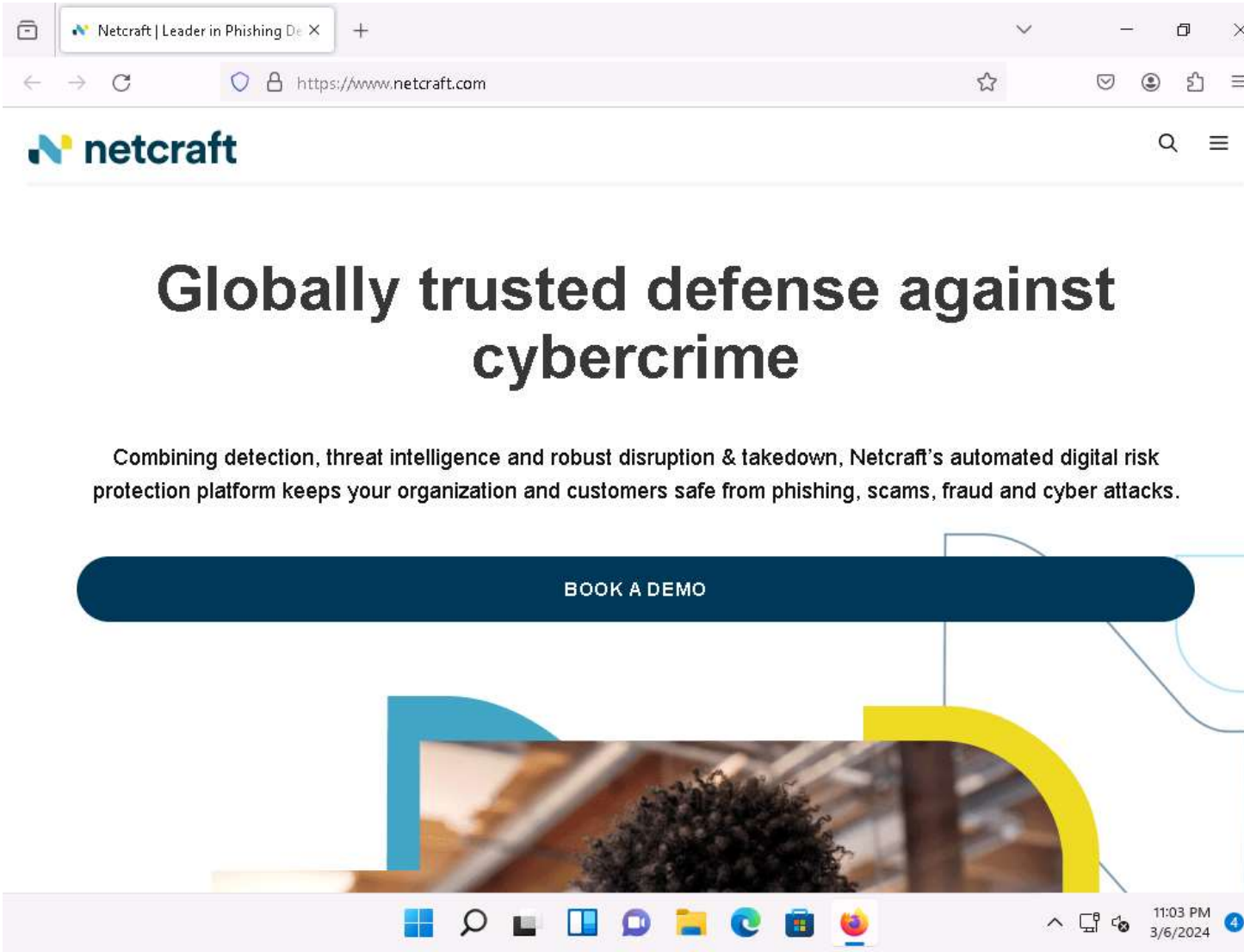
Task 1: Find the Company's Domains, Subdomains and Hosts using Netcraft and DNSdumpster

Domains and sub-domains are part of critical network infrastructure for any organization. A company's top-level domains (TLDs) and subdomains can provide much useful information such as organizational history, services and products, and contact information. A public website is designed to show the presence of an organization on the Internet, and is available for free access.

Here, we will extract the company's domains and subdomains using the Netcraft and DNSdumpster tools.

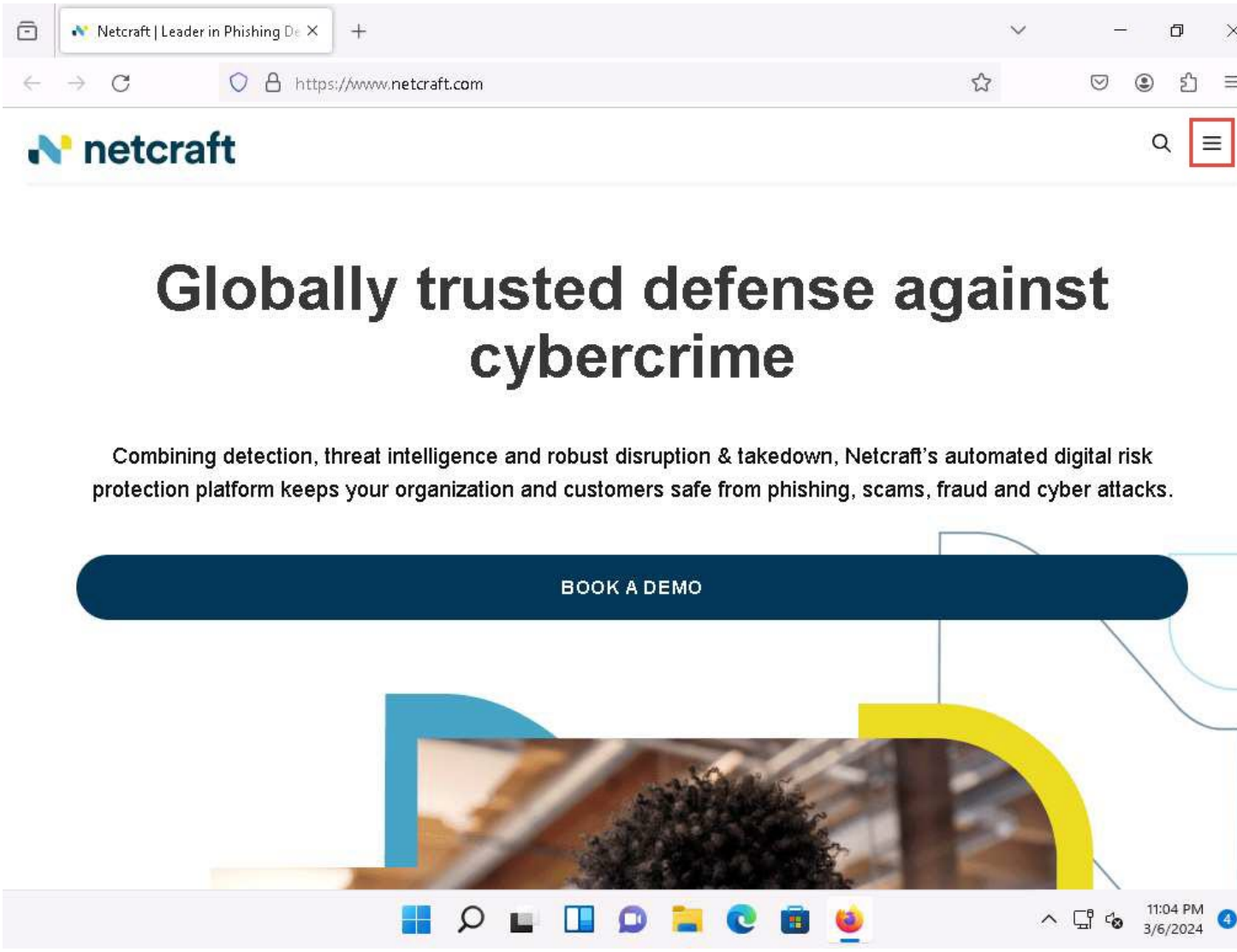
1. Launch any web browser, and go to **https://www.netcraft.com** (here, we are using **Mozilla Firefox**).
2. **Netcraft** page appears, as shown in the screenshot.

3. If cookie pop-up appears, click **Accept**.

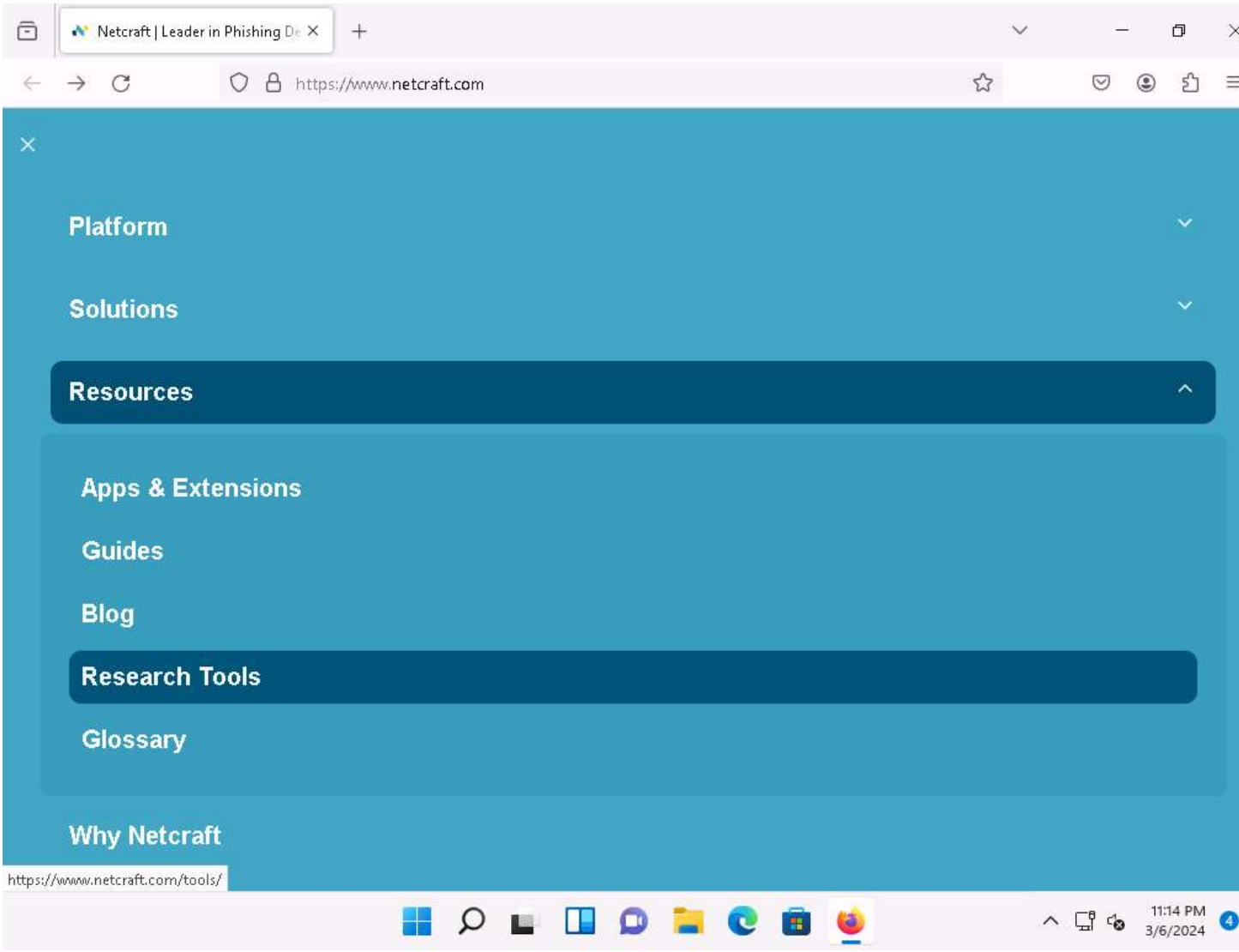
4. 

5. Click on menu icon from the top-right corner of the page and navigate to the **Resources** -> **Research Tools**.

6.


Netcraft | Leader in Phishing De
https://www.netcraft.com
netcraft
Globally trusted defense against cybercrime
Combining detection, threat intelligence and robust disruption & takedown, Netcraft's automated digital risk protection platform keeps your organization and customers safe from phishing, scams, fraud and cyber attacks.
BOOK A DEMO
11:04 PM
3/6/2024

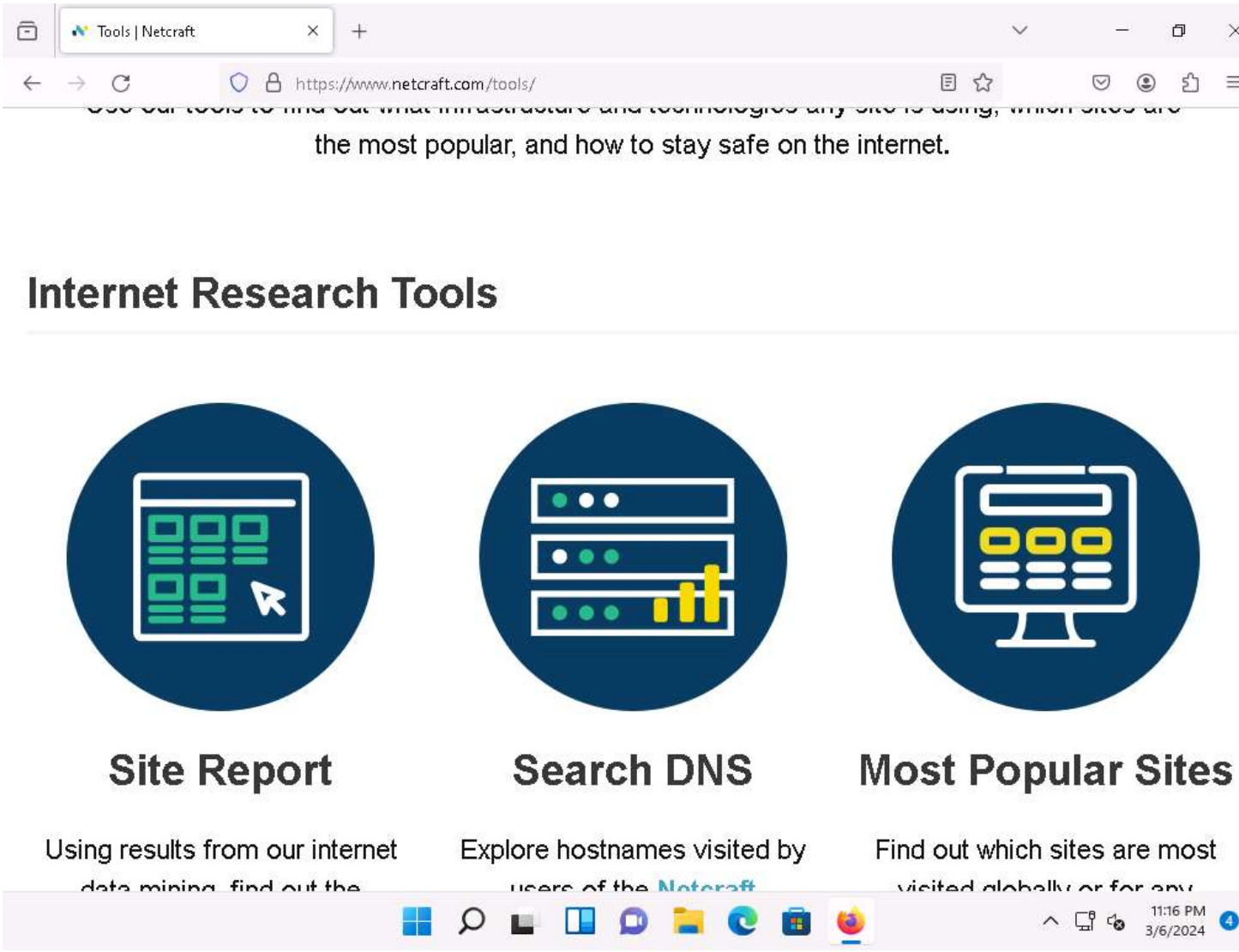
7.



8. In the **Tools | Netcraft** page, click on **Site Report** option.

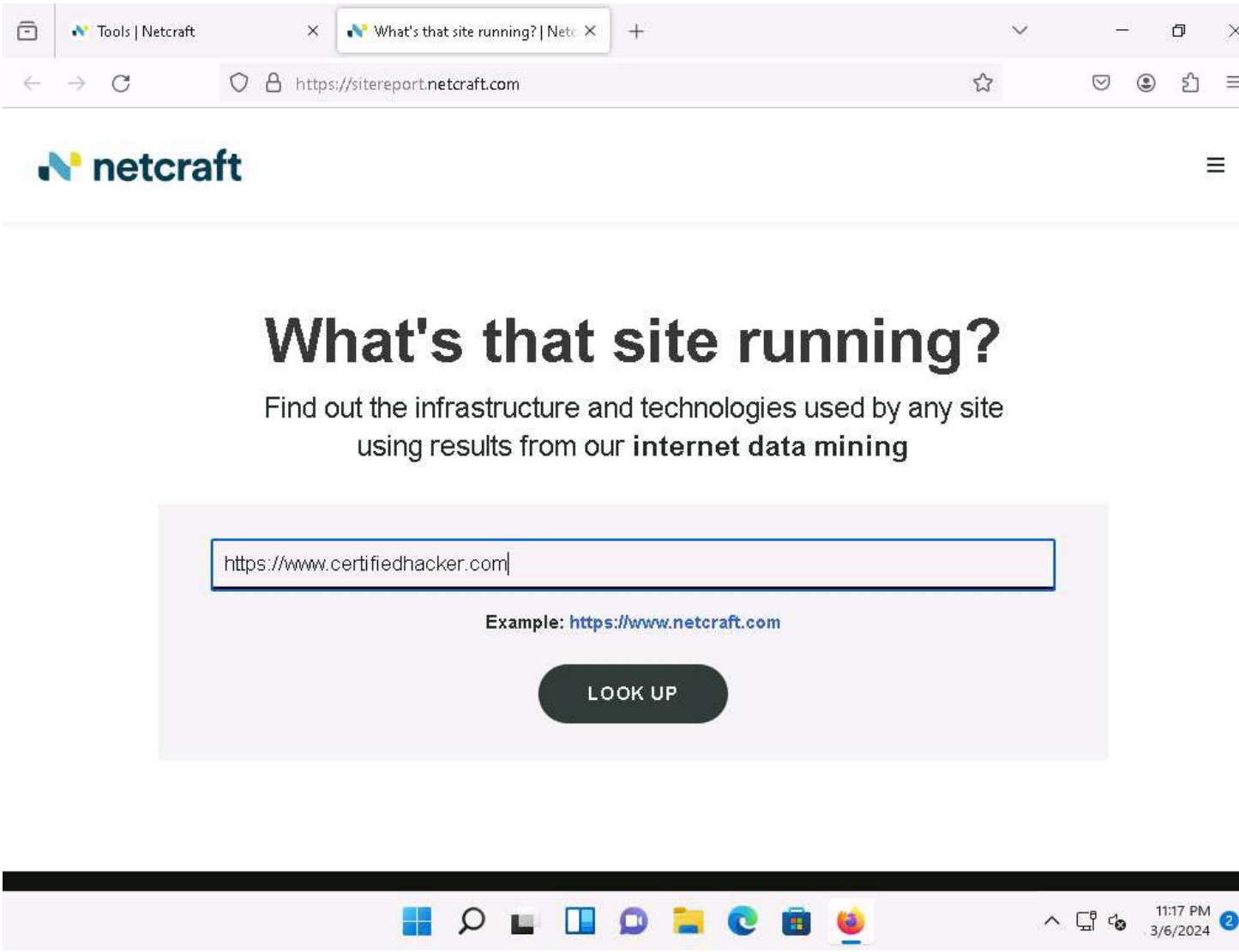
9. If a cookies pop-up appears, click on **ACCEPT COOKIES**.

10.



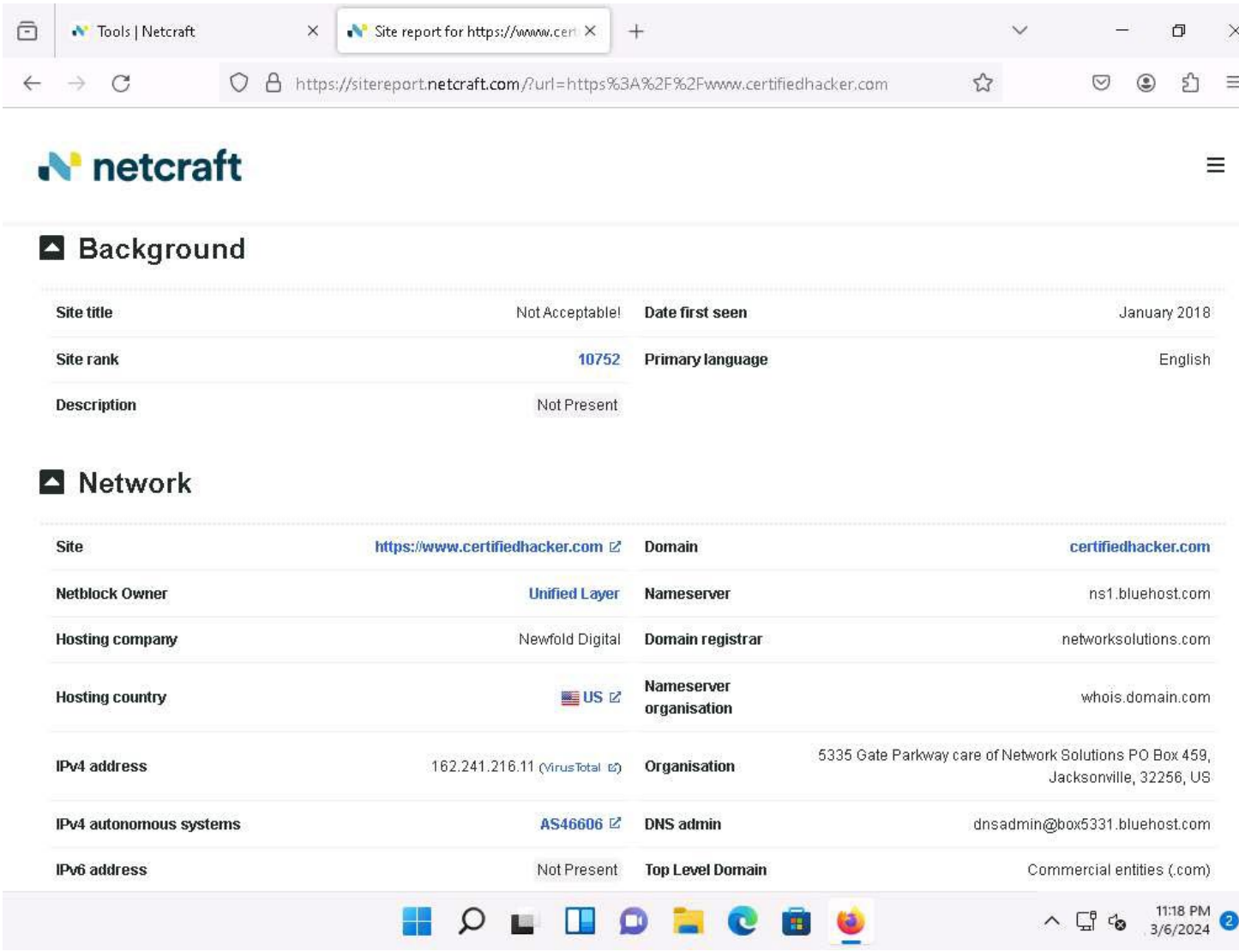
11. The **What's that site running?** page appears. To extract information associated with the organizational website such as infrastructure, technology used, sub domains, background, network, etc., type the target website's URL (here, **https://www.certifiedhacker.com**) in the text field, and then click the **LOOK UP** button, as shown in the screenshot.

12.



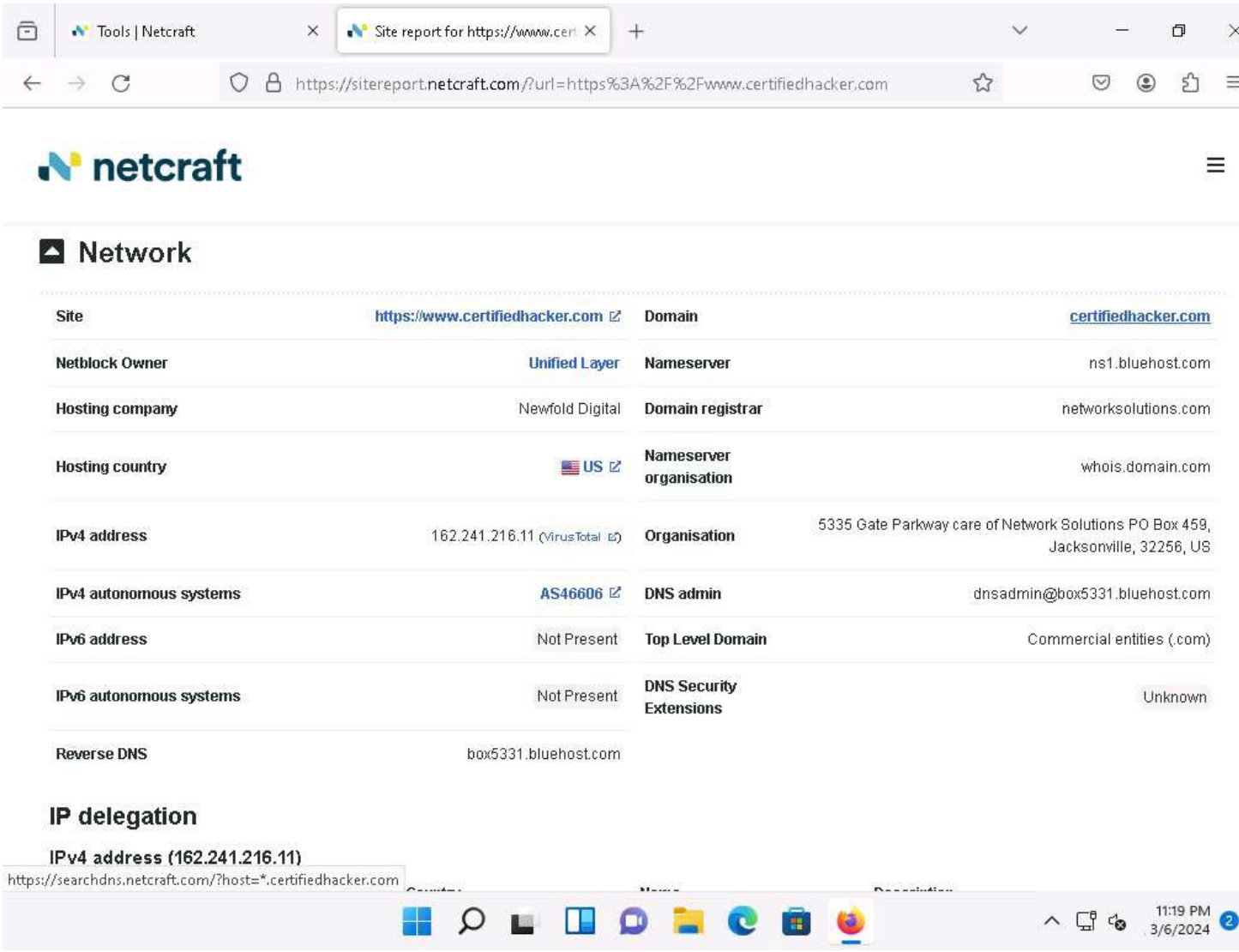
13. The **Site report for https://www.certifiedhacker.com** page appears, containing information related to **Background**, **Network**, **Hosting History**, etc., as shown in the screenshot.

14.



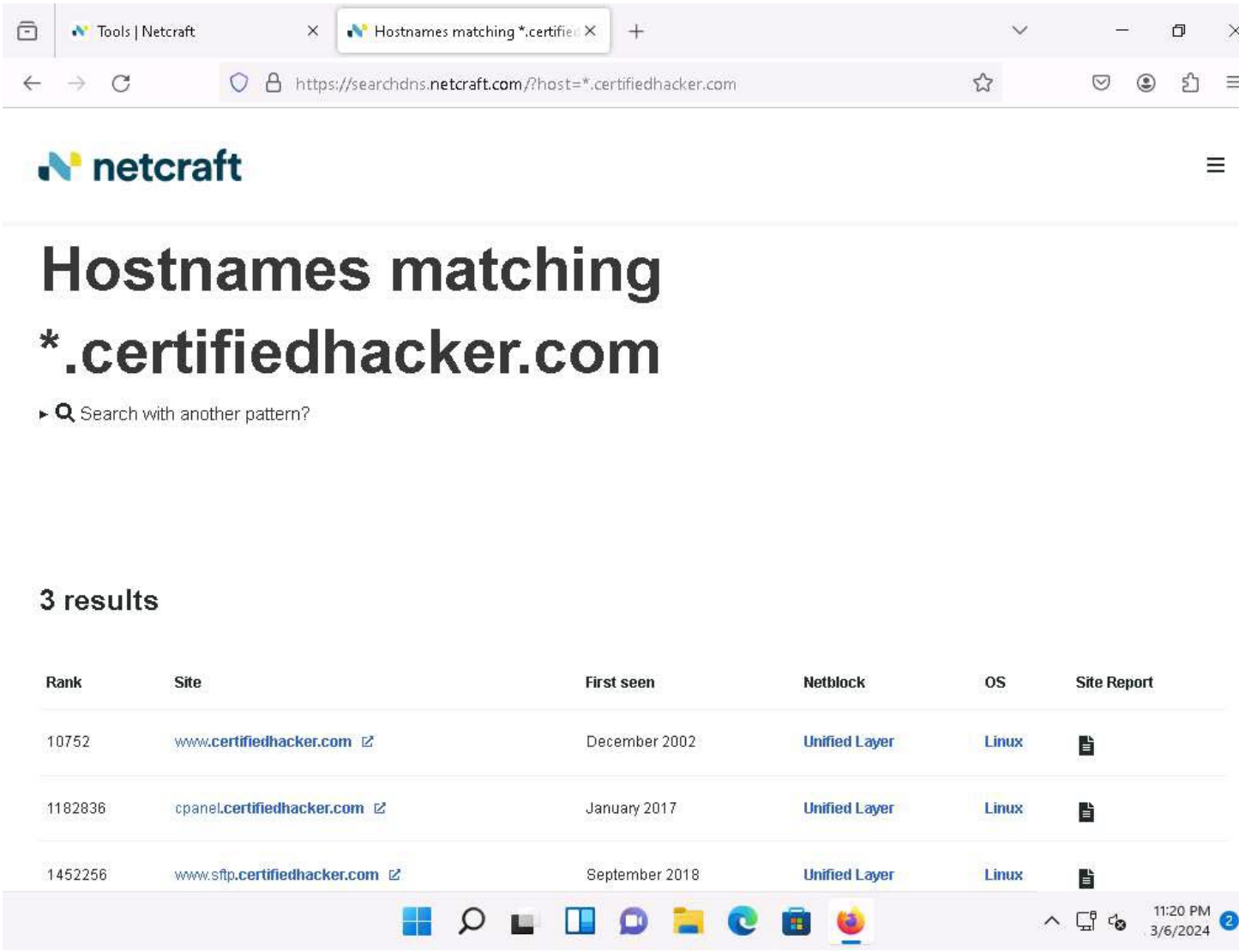
15. In the **Network** section, click on the website link (here, **certifiedhacker.com**) in the **Domain** field to view the subdomains.

16.



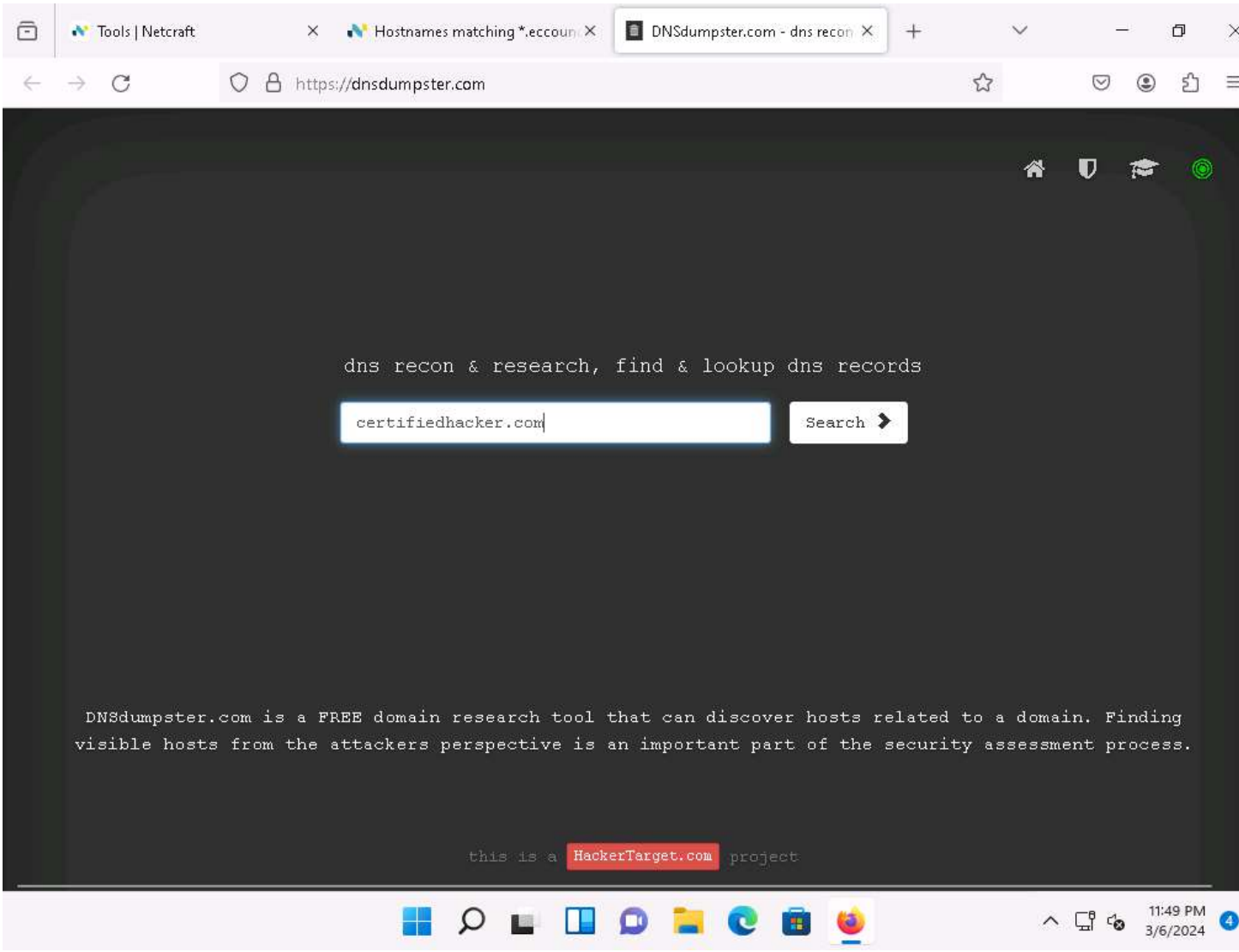
17. The result will display the subdomains of the target website along with netblock and operating system information, as shown in the screenshot.

18.



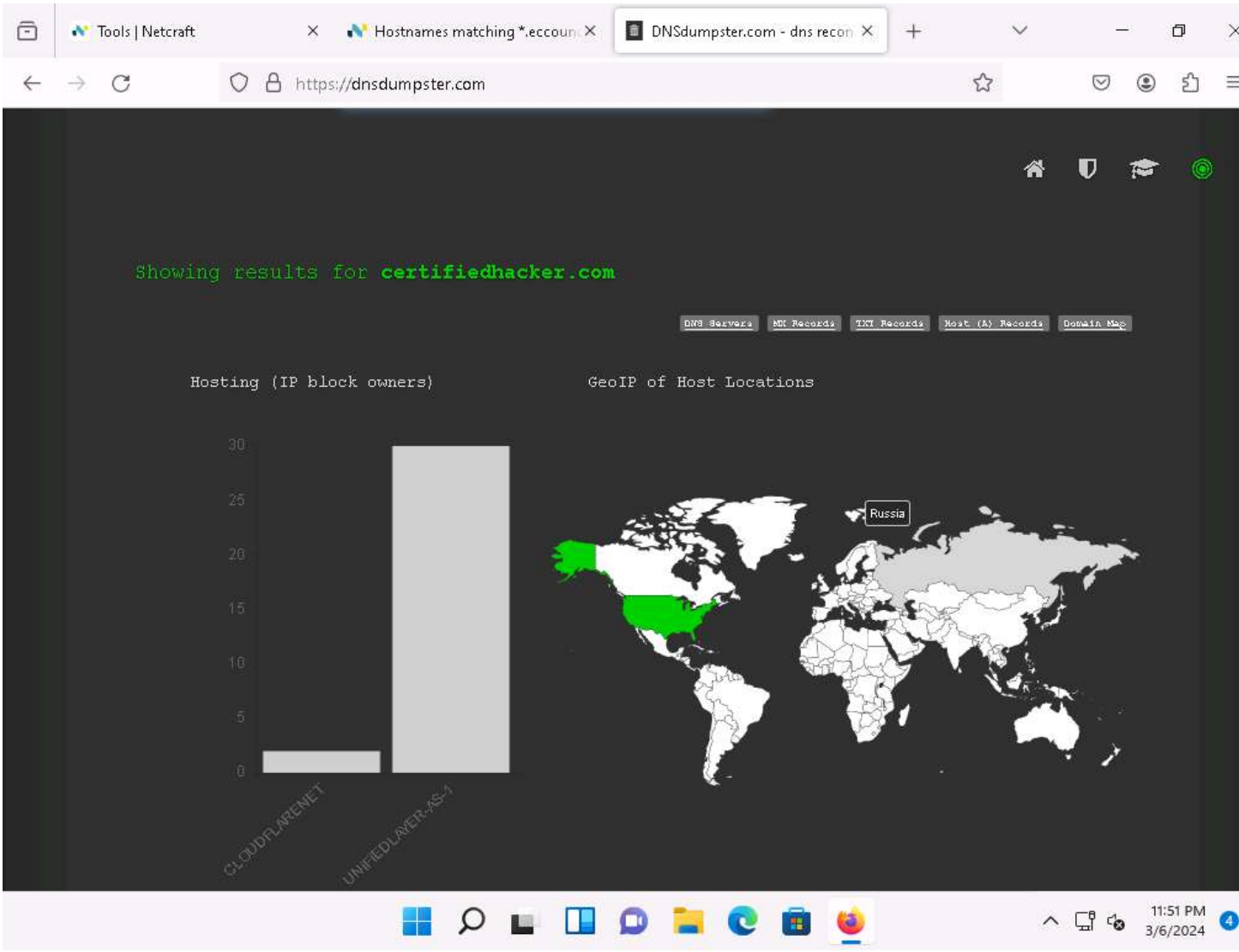
19. Now, we will find company's DNS Servers along with Geo IP and domain mapping using DNSdumpster website.
20. Open a new tab in **Firefox** browser and go to **https://dnsdumpster.com/**. Search for **certifiedhacker.com** in the search box.

21.



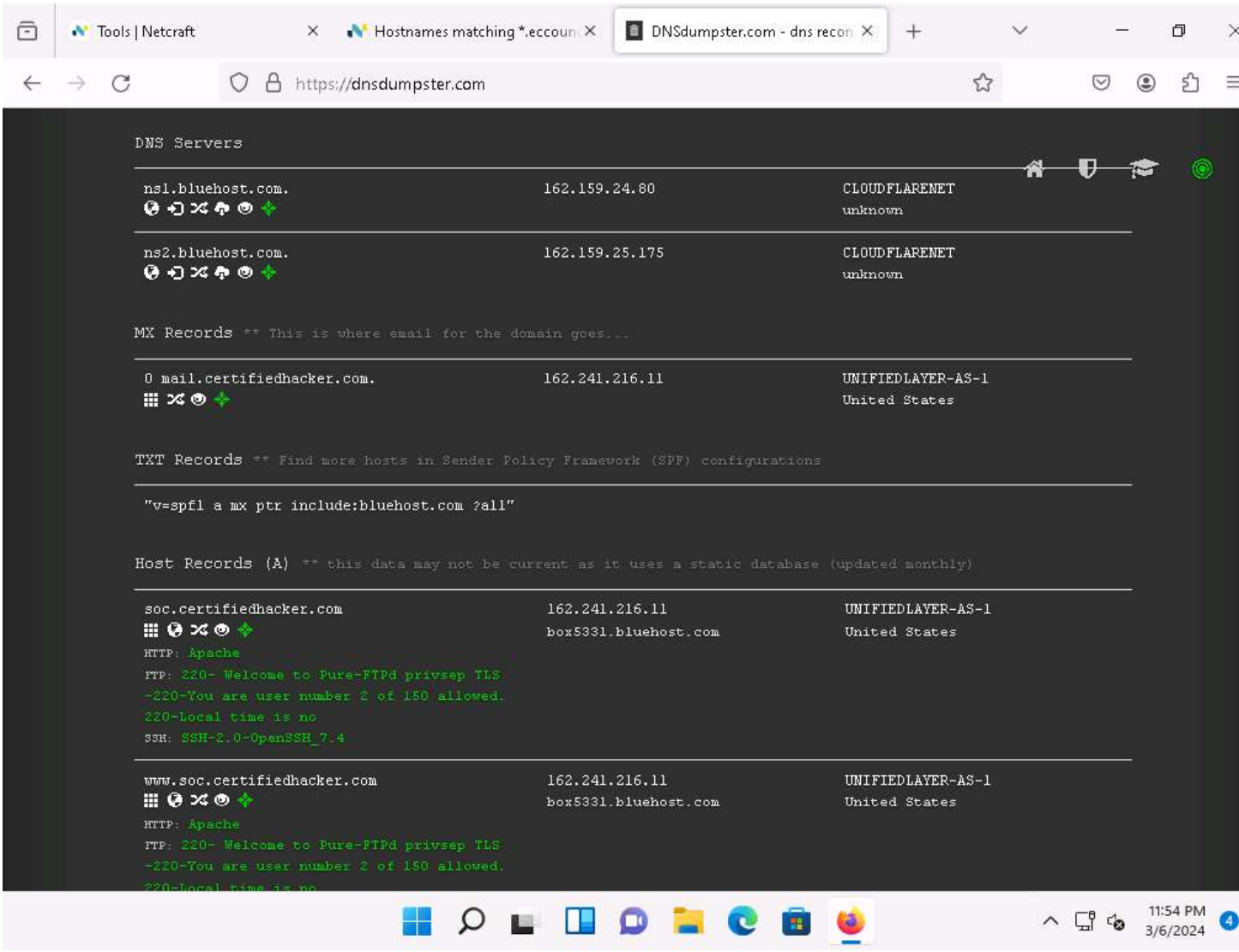
22. The website displays the **GEOIP of Host Locations**, as shown in the screenshot.

23.



24. Scroll down to view the list of **DNS Servers**, **MX Records**, **Host Record (A)** along with their IP addresses.

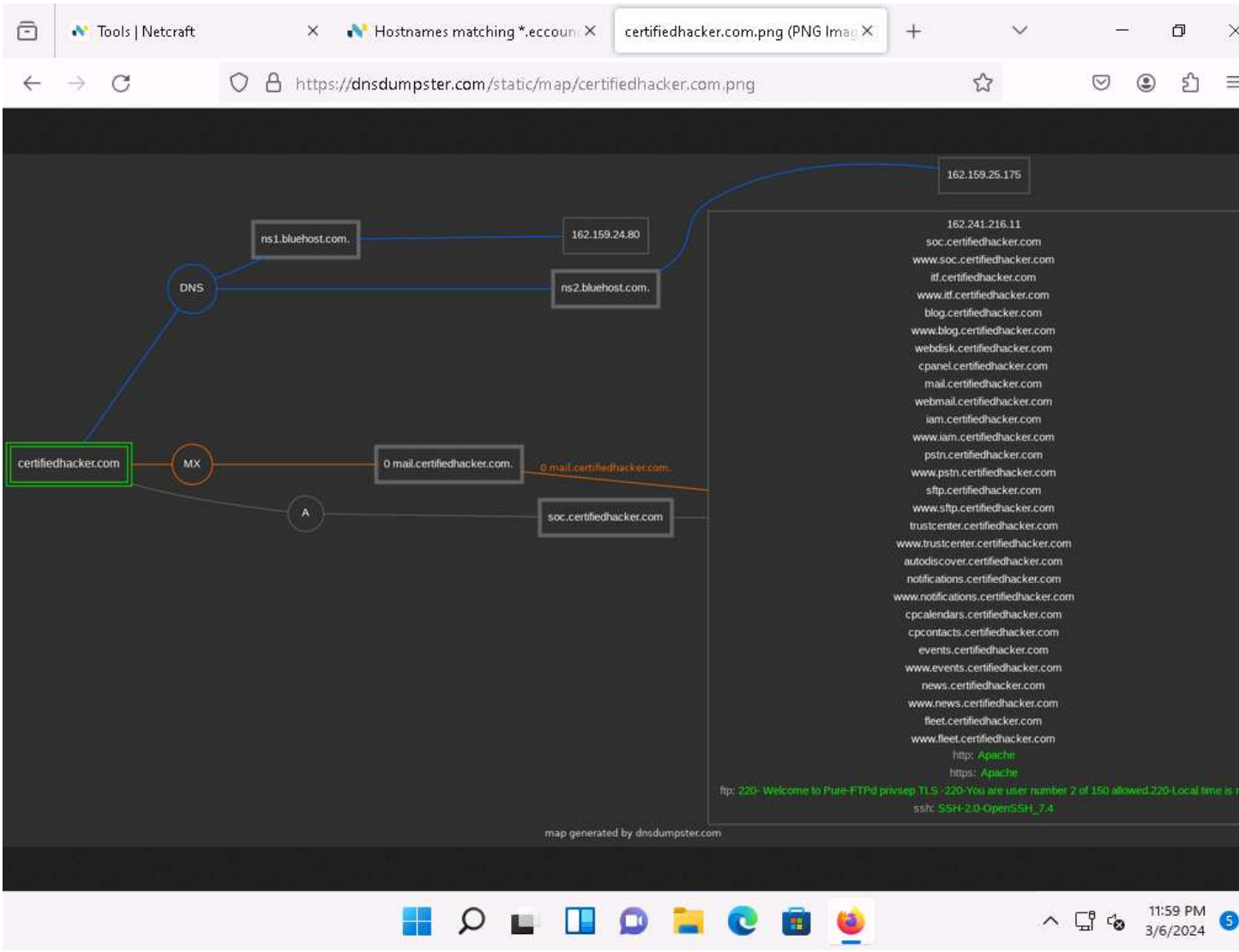
25.



26. Further, scroll down to view the domain mapping of the website.

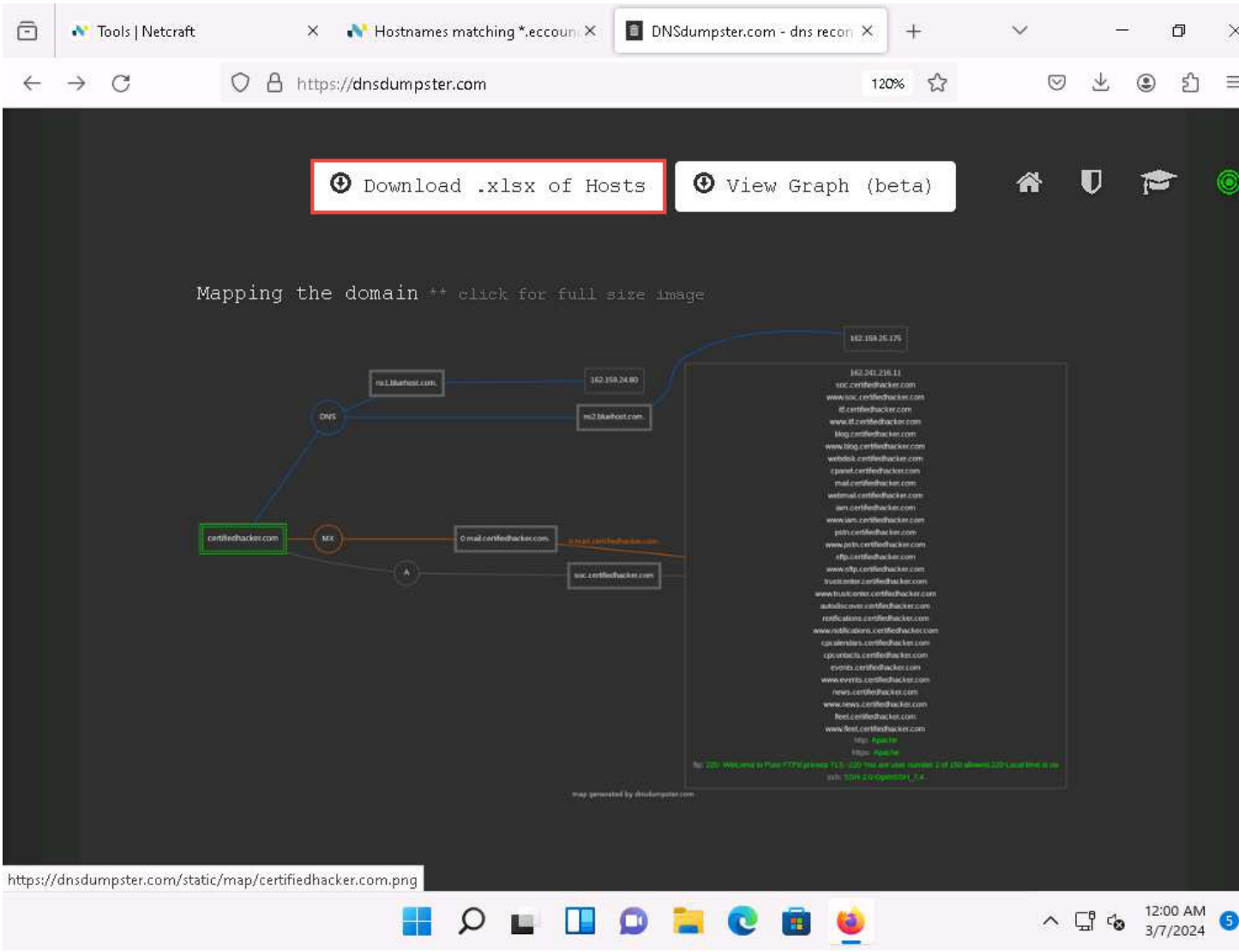
27. Click on the map to view the full-size image.
28. Click back to exit from full-size image.

29.



30. Click on **Download .xlsx of Hosts** button to download the list of hosts.

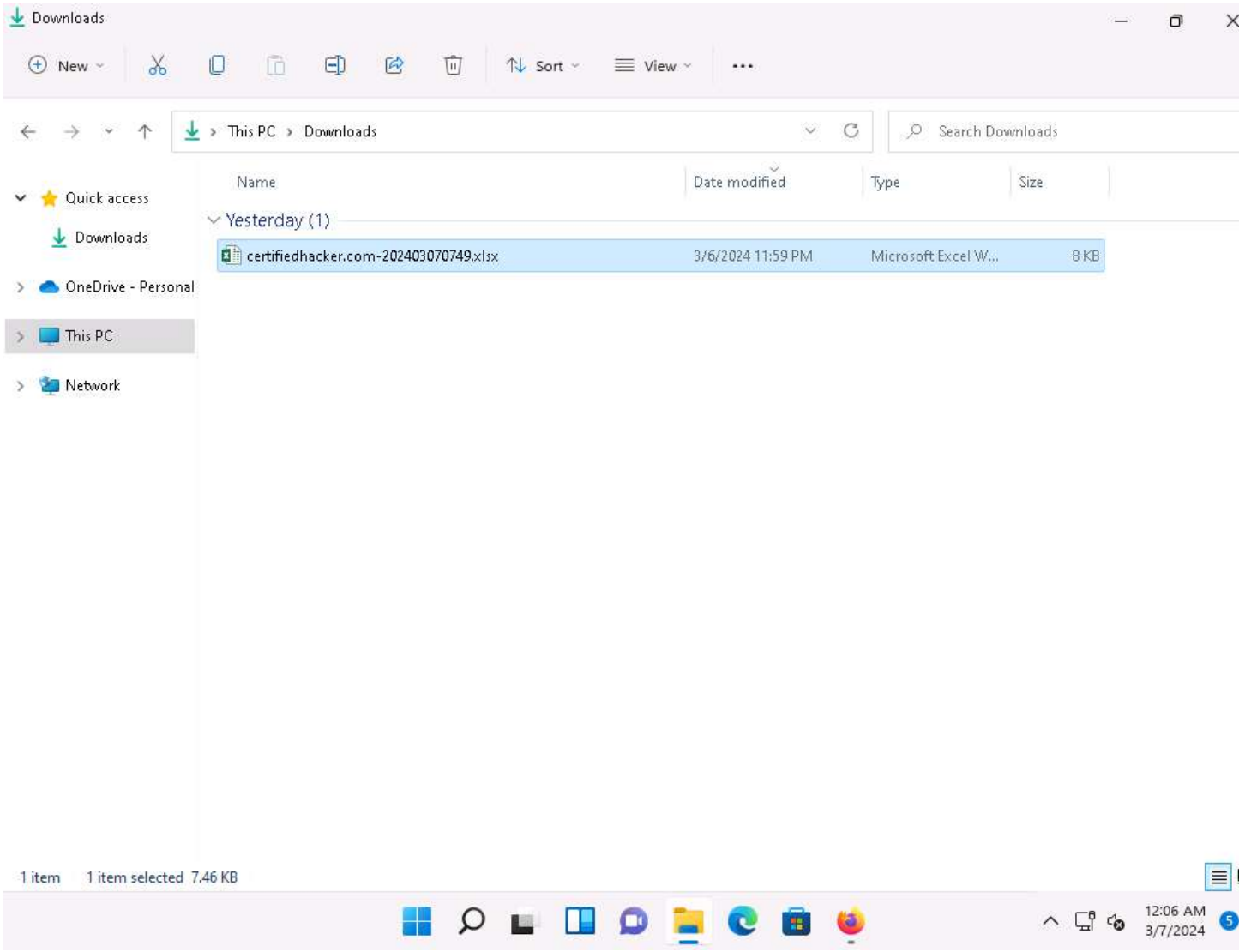
31.



32. Navigate to the **Downloads** folder and double-click on **certifiedhacker.com-xxxxxxx.xlsx** file to view the list of Hosts.

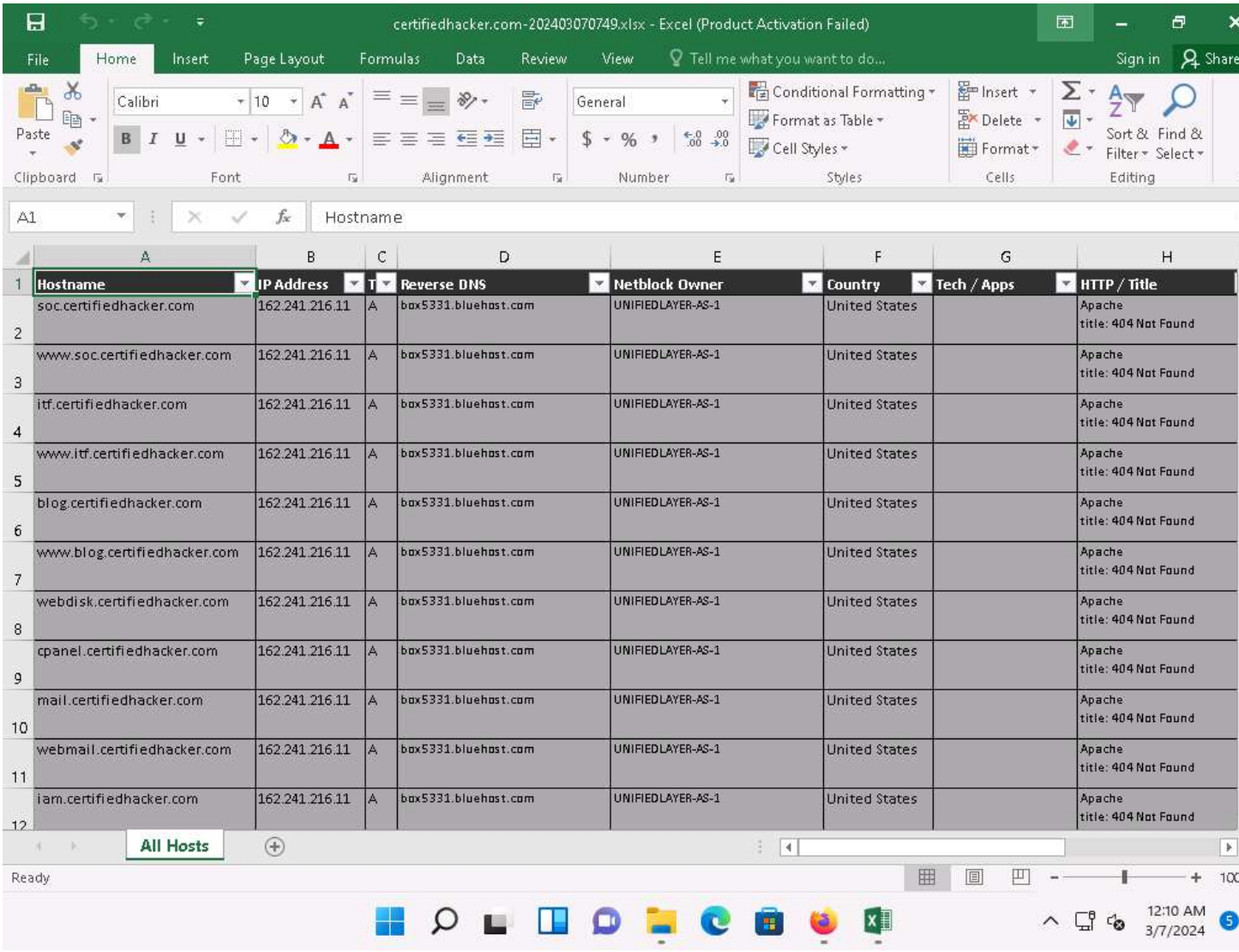
33. In the **Microsoft Office Activation Wizard** window, click on **Close**.
34. At the top of the Excel sheet, click on **Enable Editing**.

35.



36. The Excel sheet displays the details such as Hostname, IP Address, Reverse DNS, Netblock Owner, Country, HTTP /Title, etc.

37.



Hostname	IP Address	T	Reverse DNS	Netblock Owner	Country	Tech / Apps	HTTP / Title
soc.certifiedhacker.com	162.241.216.11	A	box5331.bluehost.com	UNIFIEDLAYER-AS-1	United States		Apache title: 404 Not Found
www.soc.certifiedhacker.com	162.241.216.11	A	box5331.bluehost.com	UNIFIEDLAYER-AS-1	United States		Apache title: 404 Not Found
itf.certifiedhacker.com	162.241.216.11	A	box5331.bluehost.com	UNIFIEDLAYER-AS-1	United States		Apache title: 404 Not Found
www.itf.certifiedhacker.com	162.241.216.11	A	box5331.bluehost.com	UNIFIEDLAYER-AS-1	United States		Apache title: 404 Not Found
blog.certifiedhacker.com	162.241.216.11	A	box5331.bluehost.com	UNIFIEDLAYER-AS-1	United States		Apache title: 404 Not Found
www.blog.certifiedhacker.com	162.241.216.11	A	box5331.bluehost.com	UNIFIEDLAYER-AS-1	United States		Apache title: 404 Not Found
webdisk.certifiedhacker.com	162.241.216.11	A	box5331.bluehost.com	UNIFIEDLAYER-AS-1	United States		Apache title: 404 Not Found
cpanel.certifiedhacker.com	162.241.216.11	A	box5331.bluehost.com	UNIFIEDLAYER-AS-1	United States		Apache title: 404 Not Found
mail.certifiedhacker.com	162.241.216.11	A	box5331.bluehost.com	UNIFIEDLAYER-AS-1	United States		Apache title: 404 Not Found
webmail.certifiedhacker.com	162.241.216.11	A	box5331.bluehost.com	UNIFIEDLAYER-AS-1	United States		Apache title: 404 Not Found
iam.certifiedhacker.com	162.241.216.11	A	box5331.bluehost.com	UNIFIEDLAYER-AS-1	United States		Apache title: 404 Not Found

38. This concludes the demonstration of finding the company's domains and subdomains and Hosts using the Netcraft tool and DNSdumpster. The attackers can use this collected list of subdomains to perform web application attacks on the target organization such as injection attacks, brute-force attack, and denial-of-service (DoS) attacks.
39. You can also use tools such as **Pentest-Tools Find Subdomains** (https://pentest-tools.com), to identify the domains and subdomains of any target website.
40. Close all open windows and document all the acquired information.

Question 2.2.1.1

Use the DNSdumpster website (https://dnsdumpster.com/) to obtain certifiedhacker.com domain's DNS Servers along with Geo IP and domain mapping. Enter the IP Address of the ns2.bluehost.com DNS Server of the target domain.

Score

Correct

Question 2.2.1.2

Search for www.eccouncil.org on Netcraft (https://www.netcraft.com) and identify the operating system of the web server hosting the website www.eccouncil.org.

Score

Correct

Lab 3: Perform Footprinting Through Social Networking Sites

Lab Scenario
As a professional ethical hacker, during information gathering, you need to gather personal information about employees working in critical positions in the target organization; for example, the Chief Information Security Officer, Security Architect, or Network Administrator. By footprinting through social networking sites, you can extract personal information such as name, position, organization name, current location, and educational qualifications. Further, you can find professional information such as company or business, current location, phone number, email ID, photos, videos, etc. The information gathered can be useful to perform social engineering and other types of advanced attacks.
Lab Objectives

- Gather personal information from various social networking sites using Sherlock

Overview of Social Networking Sites
Social networking sites are online services, platforms, or other sites that allow people to connect and build interpersonal relations. People usually maintain profiles on social networking sites to provide basic information about themselves and to help make and maintain connections with others; the profile generally contains information such as name, contact information (cellphone number, email address), friends' information, information about family members, their interests, activities, etc. On social networking sites, people may also post their personal information such as date of birth, educational information, employment background, spouse's names, etc. Organizations often post information such as potential partners, websites, and upcoming news about the company. Thus, social networking sites often prove to be valuable information resources. Examples of such sites include LinkedIn, Facebook, Instagram, Twitter, Pinterest, YouTube, etc.

Task 1: Gather Personal Information from Various Social Networking Sites using Sherlock

Sherlock is a python-based tool that is used to gather information about a target person over various social networking sites. Sherlock searches a vast number of social networking sites for a given target user, locates the person, and displays the results along with the complete URL related to the target person.
Here, we will use Sherlock to gather personal information about the target from the social networking sites.

Here, we are gathering information about **Elon Musk**. However, you can select a target of your choice.

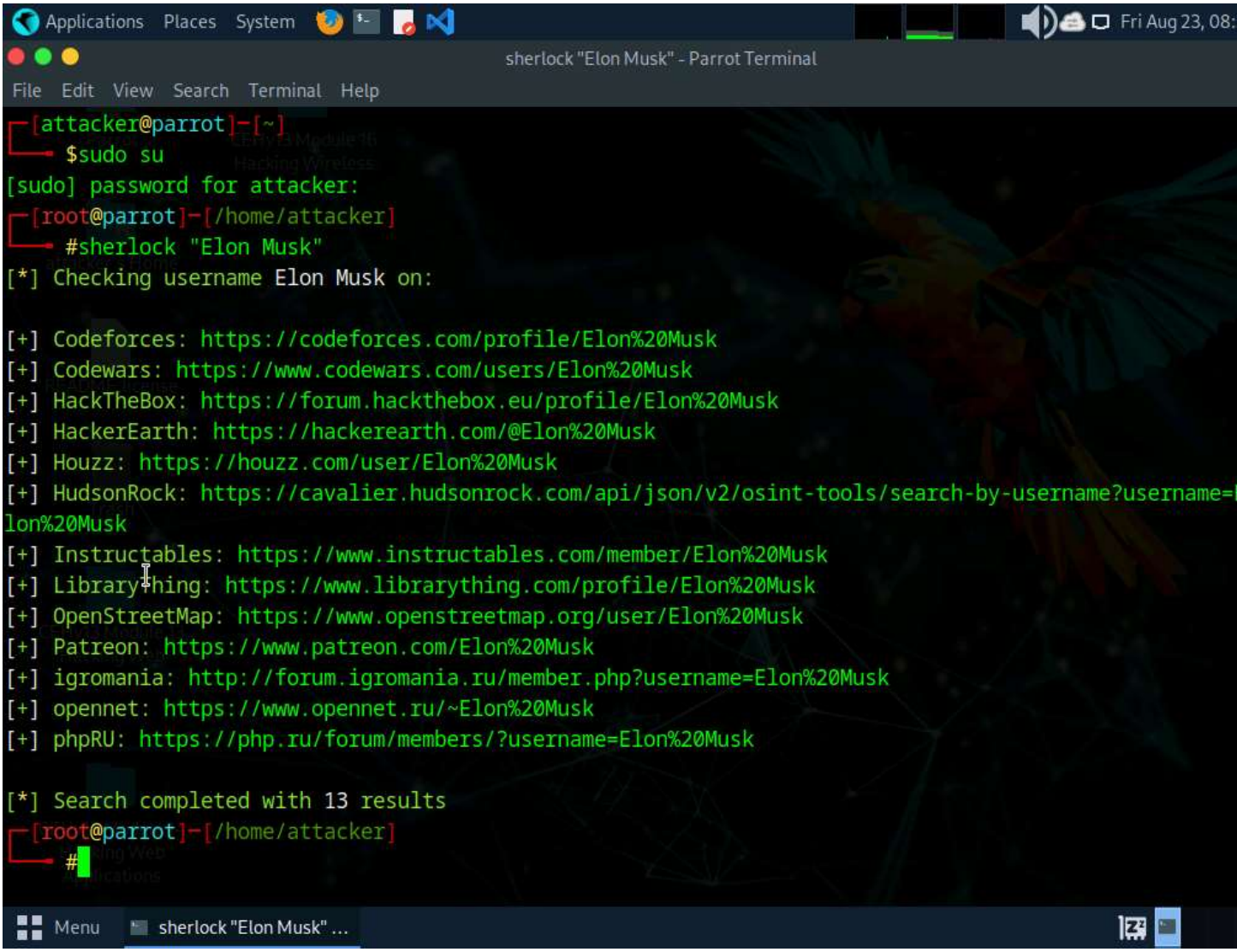
1. Turn on the Parrot Security virtual machine
2. Click Parrot Security to switch to **Parrot** machine, and login with attacker/toor. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

3. The password that you type will not be visible.

4. Run **sherlock "Elon Musk"** command and you will get all the URLs related to Elon Musk, as shown in the screenshot. Scroll-down to view all the results.

5. The results might differ when you perform this task. If you receive any error messages in between ignore them.

6.



7. The attackers can further use the gathered URLs to obtain sensitive information about the target such as DOB, employment status and information about the organization that they are working for, including the business strategy, potential clients, and upcoming project plans.
8. This concludes the demonstration of gathering personal information from various social networking sites using Sherlock.
9. You can also use tools such as **Social Searcher** (https://www.social-searcher.com) to gather additional information related to the target company and its employees from social networking sites.
10. Close all open windows and document all the acquired information.

Question 2.3.1.1

Use the Sherlock tool to gather all the URLs related to Elon Musk from various social networking sites. Enter the complete URL related to Elon Musk that is obtained from the social networking site Codewars.

Score

Correct

Lab 4: Perform Whois Footprinting

Lab Scenario
During the footprinting process, gathering information on the target IP address and domain obtained during previous information gathering steps is important. As a professional ethical hacker or penetration tester, you should be able to perform Whois footprinting on the target; this method provides target domain information such as the owner, its registrar, registration details, name server, contact information, etc. Using this information, you can create a map of the organization's network, perform social engineering attacks, and obtain internal details of the network.
Lab Objectives

- Perform Whois lookup using DomainTools

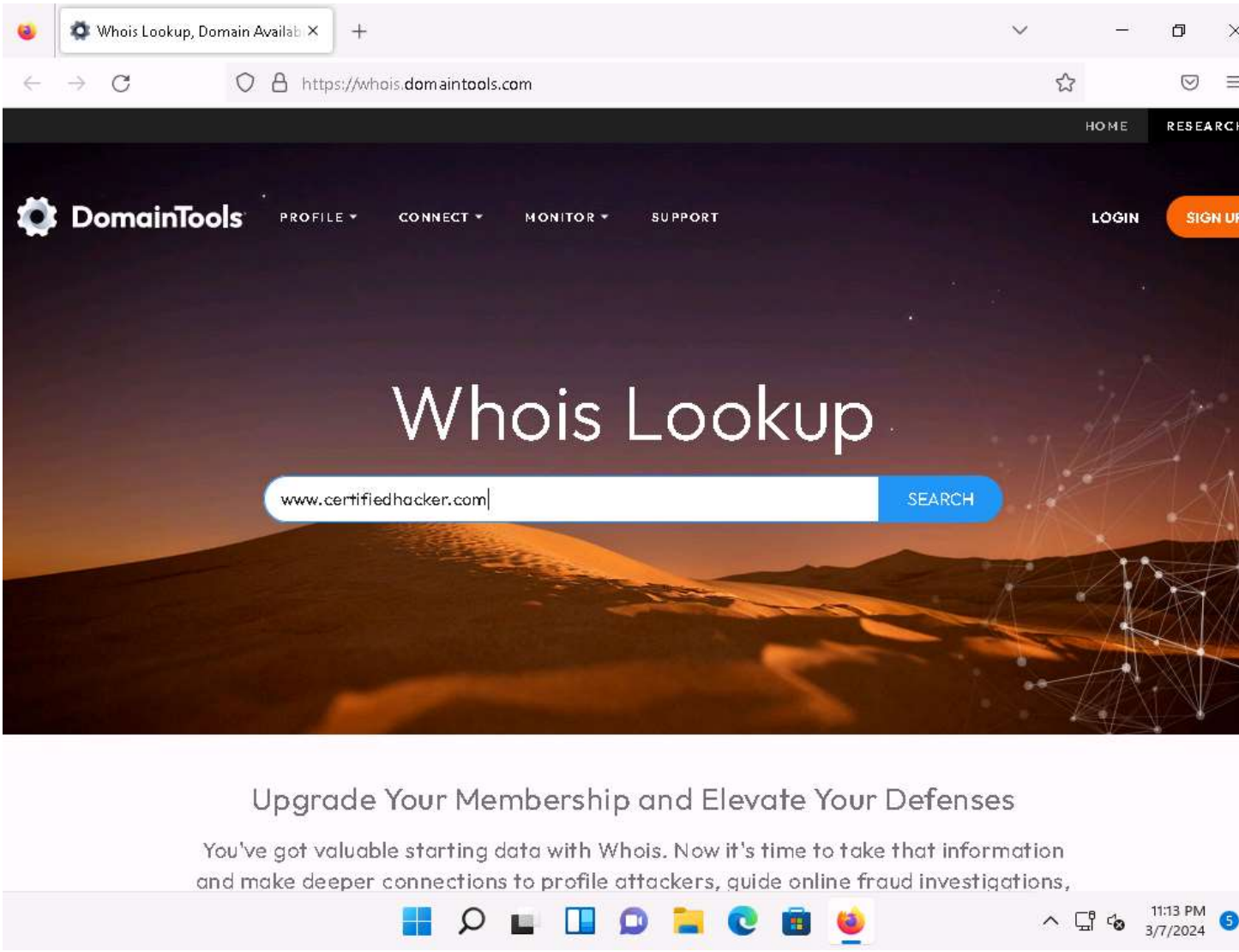
Overview of Whois Footprinting
This lab focuses on how to perform a Whois lookup and analyze the results. Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, and contains the personal information of domain owners. For each resource, the Whois database provides text records with information about the resource itself and relevant information of assignees, registrants, and administrative information (creation and expiration dates).

Task 1: Perform Whois Lookup using DomainTools

Here, we will gather target information by performing Whois lookup using DomainTools.

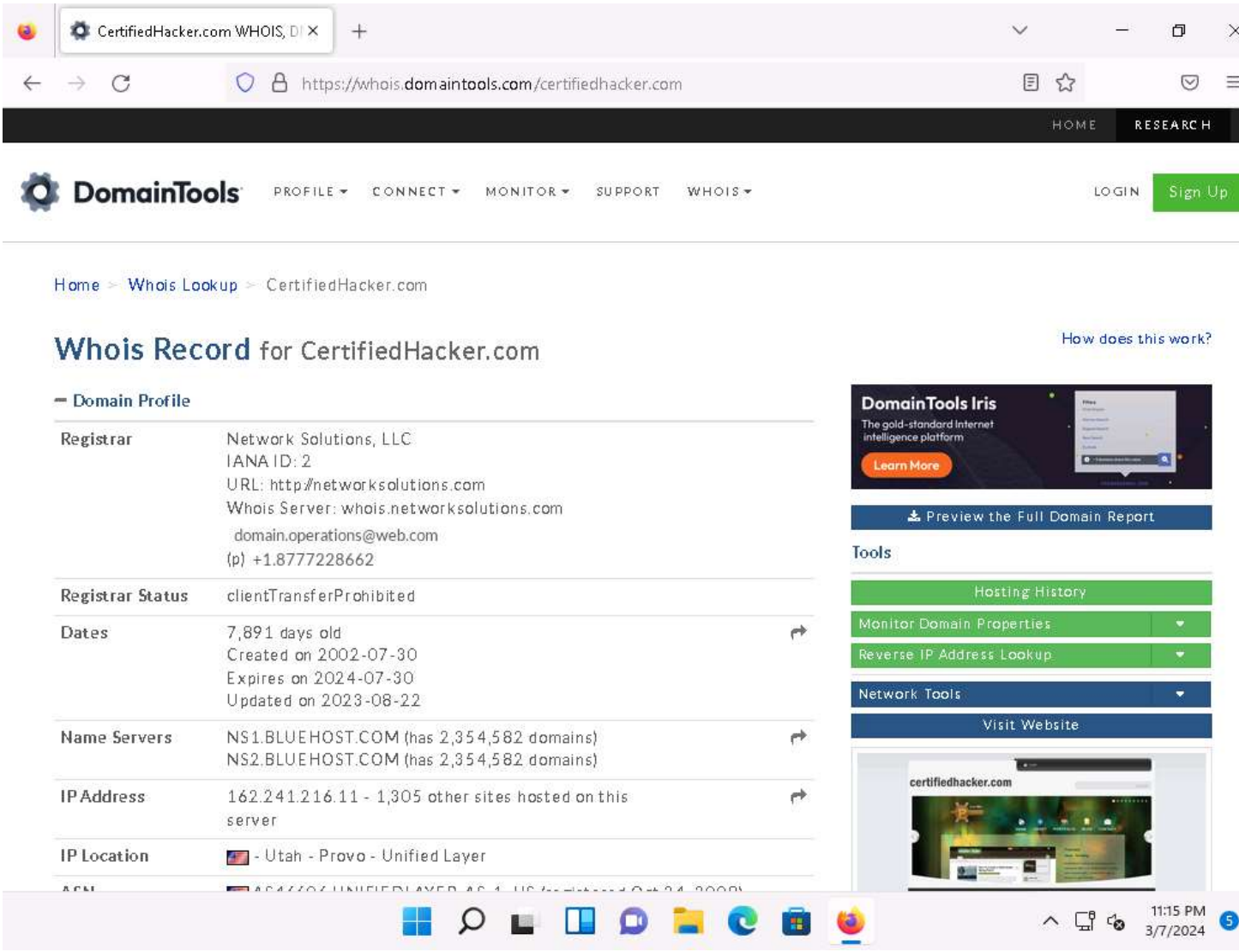
1. Click Windows 11 to switch to the **Windows 11** machine, open any web browser, and go to **https://whois.domaintools.com** (here, we are using **Mozilla Firefox**).
2. The Whois Lookup website appears, as shown in the screenshot. Now, in the search bar, search for **www.certifiedhacker.com**.

3.

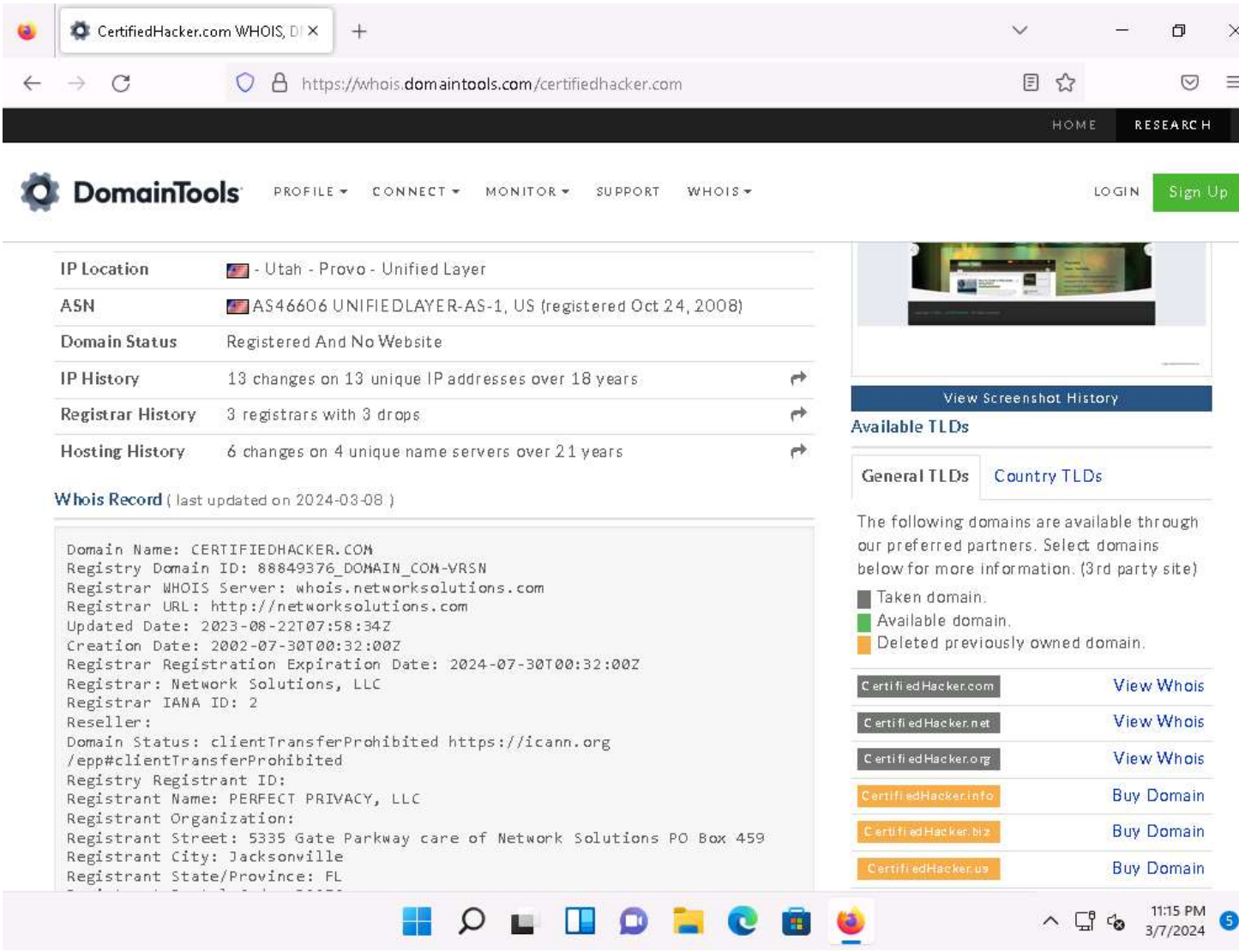


4. This search result reveals the details associated with the URL entered, **www.certifiedhacker.com**, which includes organizational details such as registration details, name servers, IP address, location, etc., as shown in the screenshots.

5.


CertifiedHacker.com WHOIS, D
https://whois.domaintools.com/certifiedhacker.com
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
WHOIS
LOGIN
Sign Up
Home > Whois Lookup > CertifiedHacker.com
Whois Record for CertifiedHacker.com
How does this work?
Domain Profile
Registrar
Network Solutions, LLC
IANA ID: 2
URL: http://networksolutions.com
Whois Server: whois.networksolutions.com
domain.operations@web.com
(p) +1.8777228662
Registrar Status
clientTransferProhibited
Dates
7,891 days old
Created on 2002-07-30
Expires on 2024-07-30
Updated on 2023-08-22
Name Servers
NS1.BLUEHOST.COM (has 2,354,582 domains)
NS2.BLUEHOST.COM (has 2,354,582 domains)
IP Address
162.241.216.11 - 1,305 other sites hosted on this server
IP Location
- Utah - Provo - Unified Layer
DomainTools Iris
The gold-standard Internet intelligence platform
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Visit Website
certifiedhacker.com
11:15 PM
3/7/2024

6.



7. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
8. Using this information, an attacker can create a map of the organization's network and further mislead domain owners with social engineering, and obtain internal details of the network.
9. You can also use other Whois lookup tools such as **SmartWhois** (https://www.tamos.com), **Batch IP Converter** (http://www.sabsoft.com), etc. to extract additional target Whois information.
10. Close all open windows and document all the acquired information.

Question 2.4.1.1

Perform a Whois lookup using DomainTools and find the URL that belongs to the registrar of the website www.certifiedhacker.com.

Score

Correct

Lab 5: Perform DNS Footprinting

Lab Scenario

As a professional ethical hacker, you need to gather the DNS information of a target domain obtained during the previous steps. You need to perform DNS footprinting to gather information about DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, and much more about a target network.

Using this information, you can determine key hosts connected in the network and perform social engineering attacks to gather even more information.

Lab Objectives

- Gather DNS information using nslookup command line utility and online tool

Overview of DNS

DNS considered the intermediary source for any Internet communication. The primary function of DNS is to translate a domain name to IP address and vice-versa to enable human-machine-network-internet communications. Since each device has a unique IP address, it is hard for human beings to memorize all IP addresses of the required application. DNS helps in converting the IP address to a more easily understandable domain format, which eases the burden on human beings.

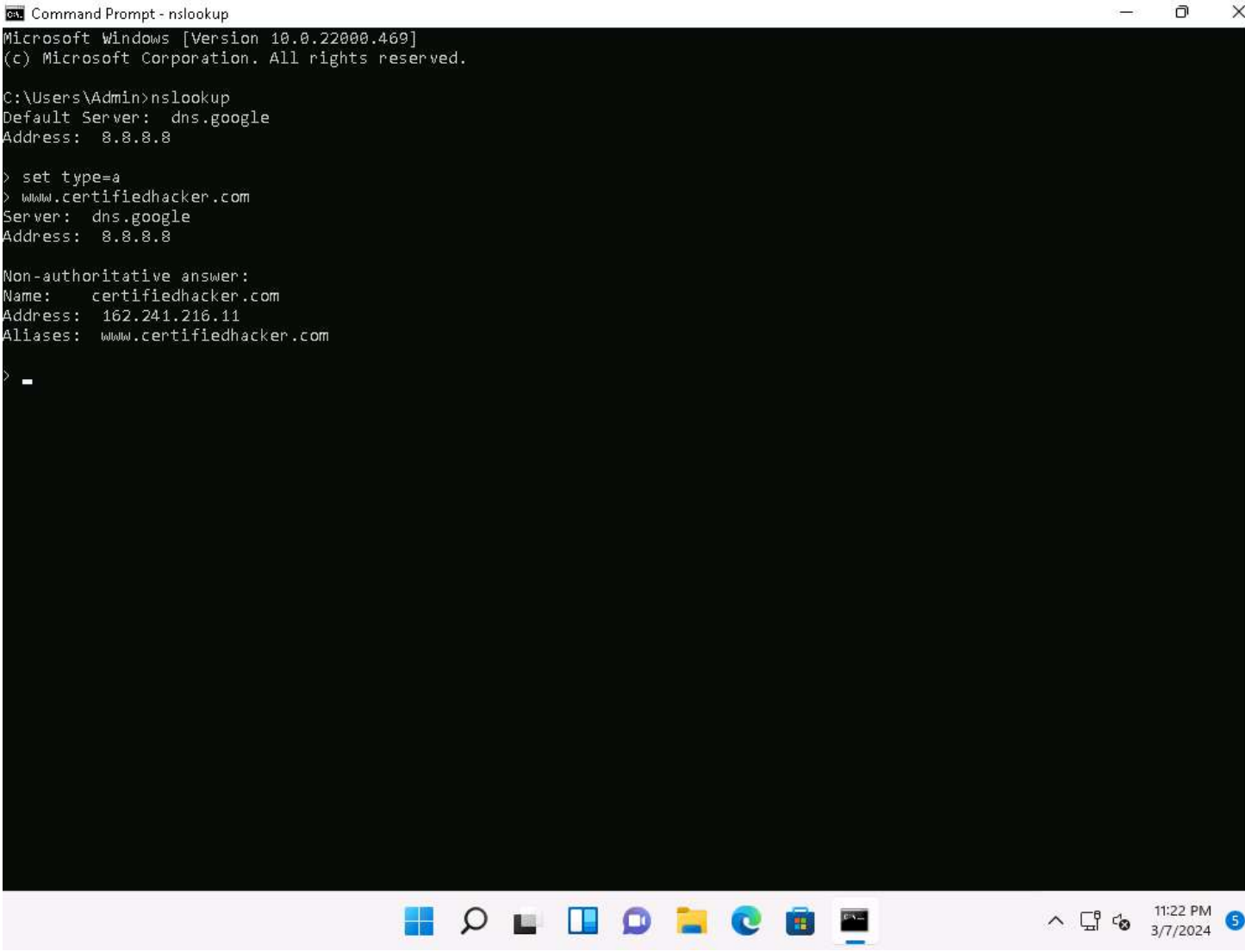
Task 1: Gather DNS Information using nslookup Command Line Utility and Online Tool

nslookup is a network administration command-line utility, generally used for querying the DNS to obtain a domain name or IP address mapping or for any other specific DNS record. This utility is available both as a command-line utility and web application.

Here, we will perform DNS information gathering about target organizations using the nslookup command-line utility and NSLOOKUP web application.

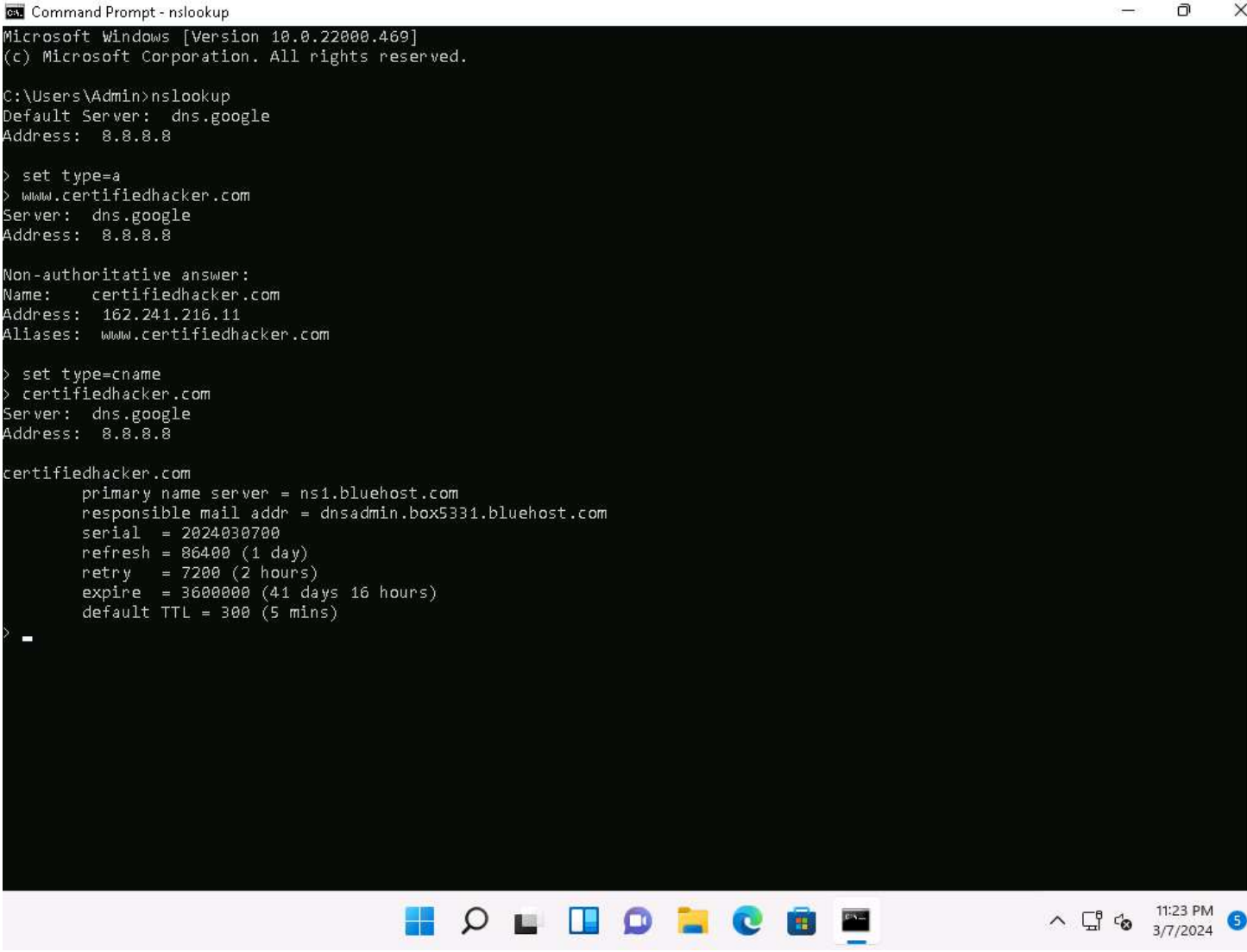
1. In the **Windows 11** machine, launch a **Command Prompt**, and run **nslookup** command. This displays the default server and its address assigned to the **Windows 11** machine.
2. In the nslookup **interactive** mode, type **set type=a** and press **Enter**. Setting the type as "**a"** configures nslookup to query for the IP address of a given domain.
3. Type the target domain **www.certifiedhacker.com** and press **Enter**. This resolves the IP address and displays the result, as shown in the screenshot.

4.



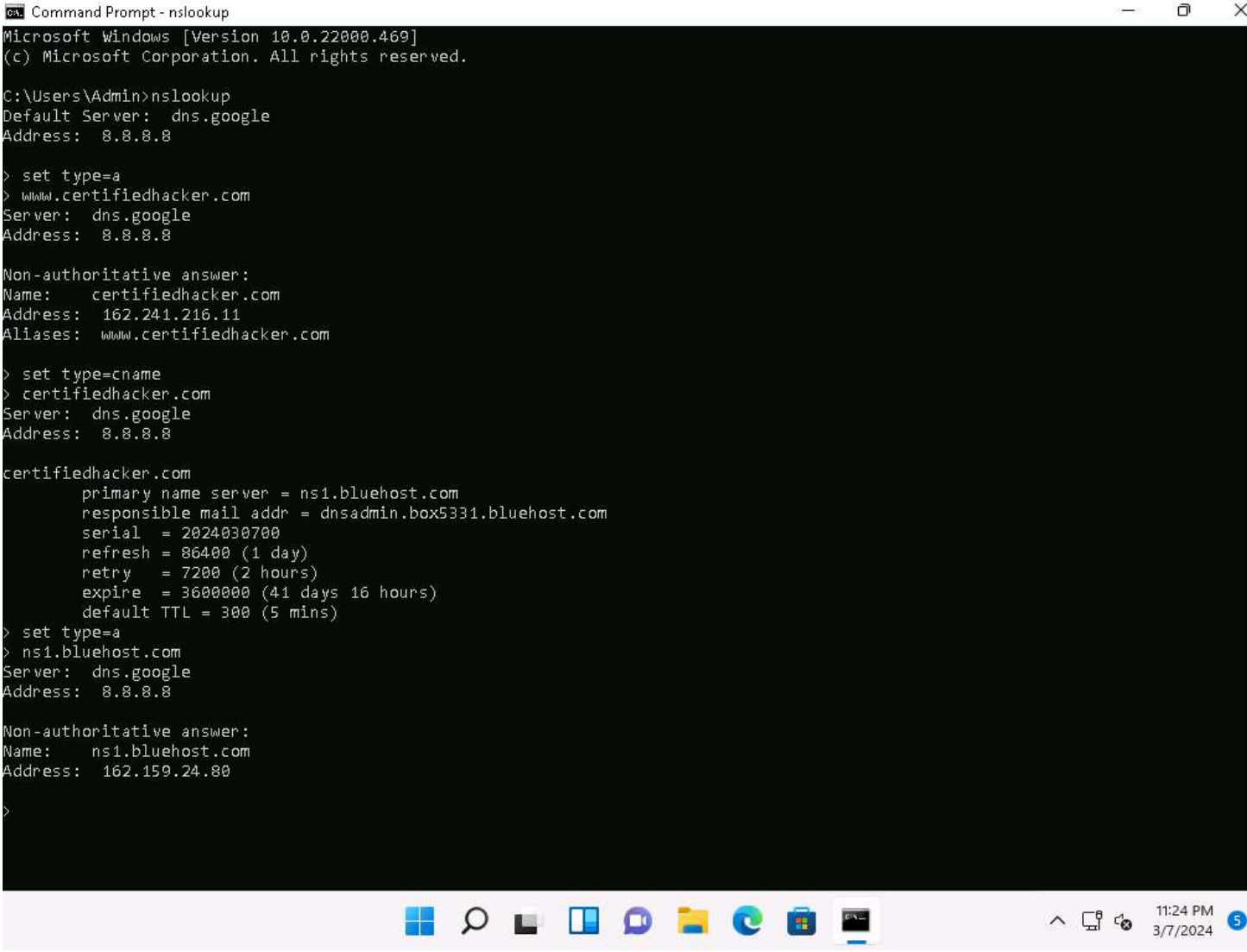
5. The first two lines in the result are:
6. Server: **dns.google** and Address: **8.8.8.8**
7. This specifies that the result was directed to the default server hosted on the local machine (**Windows 11**) that resolves your requested domain.
8. Thus, if the response is coming from your local machine's server (Google), but not the server that legitimately hosts the domain **www.certifiedhacker.com**; it is considered to be a non-authoritative answer. Here, the IP address of the target domain **www.certifiedhacker.com** is **162.241.216.11**.
9. Since the result returned is non-authoritative, you need to obtain the domain's authoritative name server.
10. Type **set type=cname** and press **Enter**. The CNAME lookup is done directly against the domain's authoritative name server and lists the CNAME records for a domain.
11. Type **certifiedhacker.com** and press **Enter**.
12. This returns the domain's authoritative name server (**ns1.bluehost.com**), along with the mail server address (**dnsadmin.box5331.bluehost.com**), as shown in the screenshot.

13.



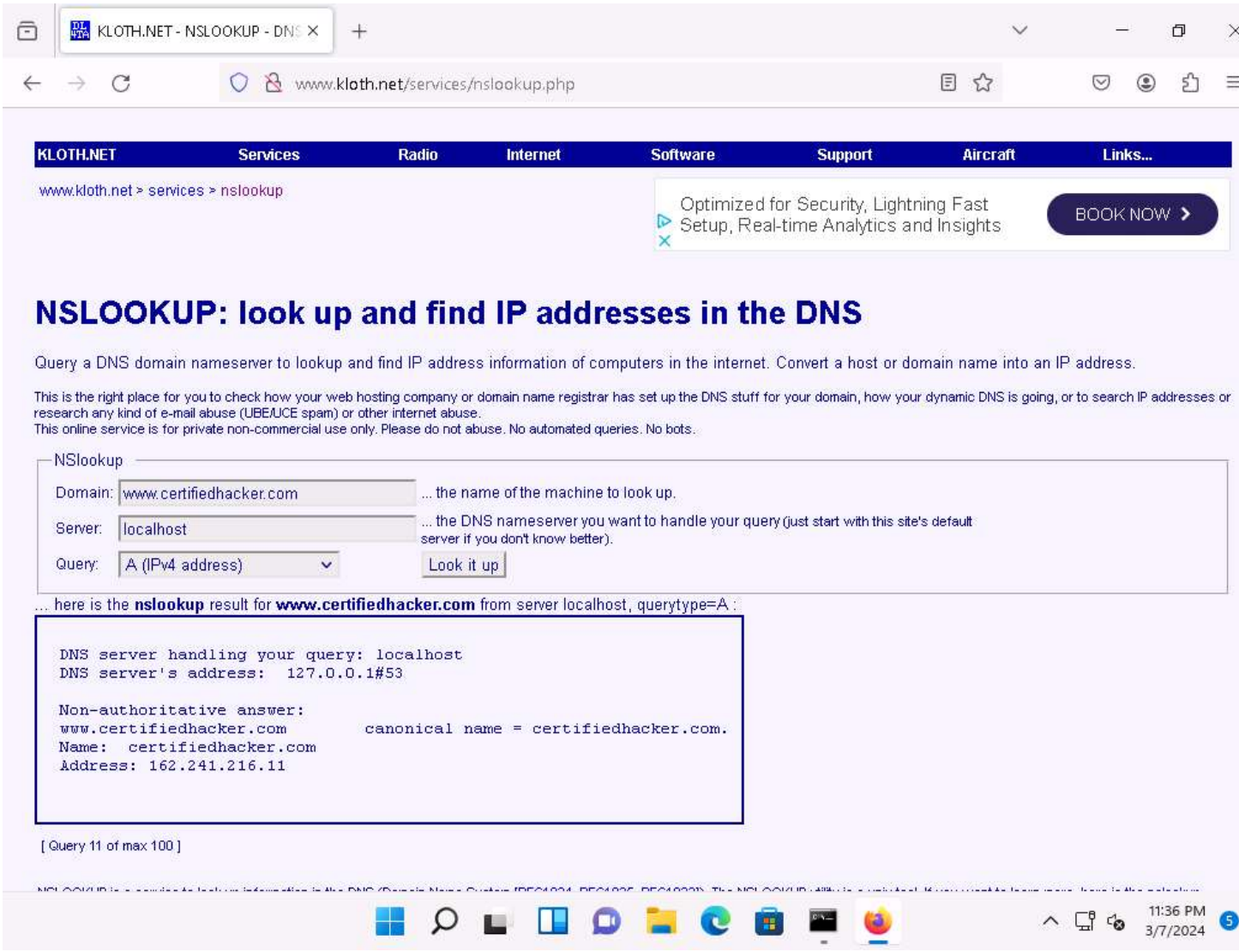
14. Since you have obtained the authoritative name server, you will need to determine the IP address of the name server.
15. Issue the command **set type=a** and press **Enter**.
16. Type **ns1.bluehost.com** (or the primary name server that is displayed in your lab environment) and press **Enter**. This returns the IP address of the server, as shown in the screenshot.

17.



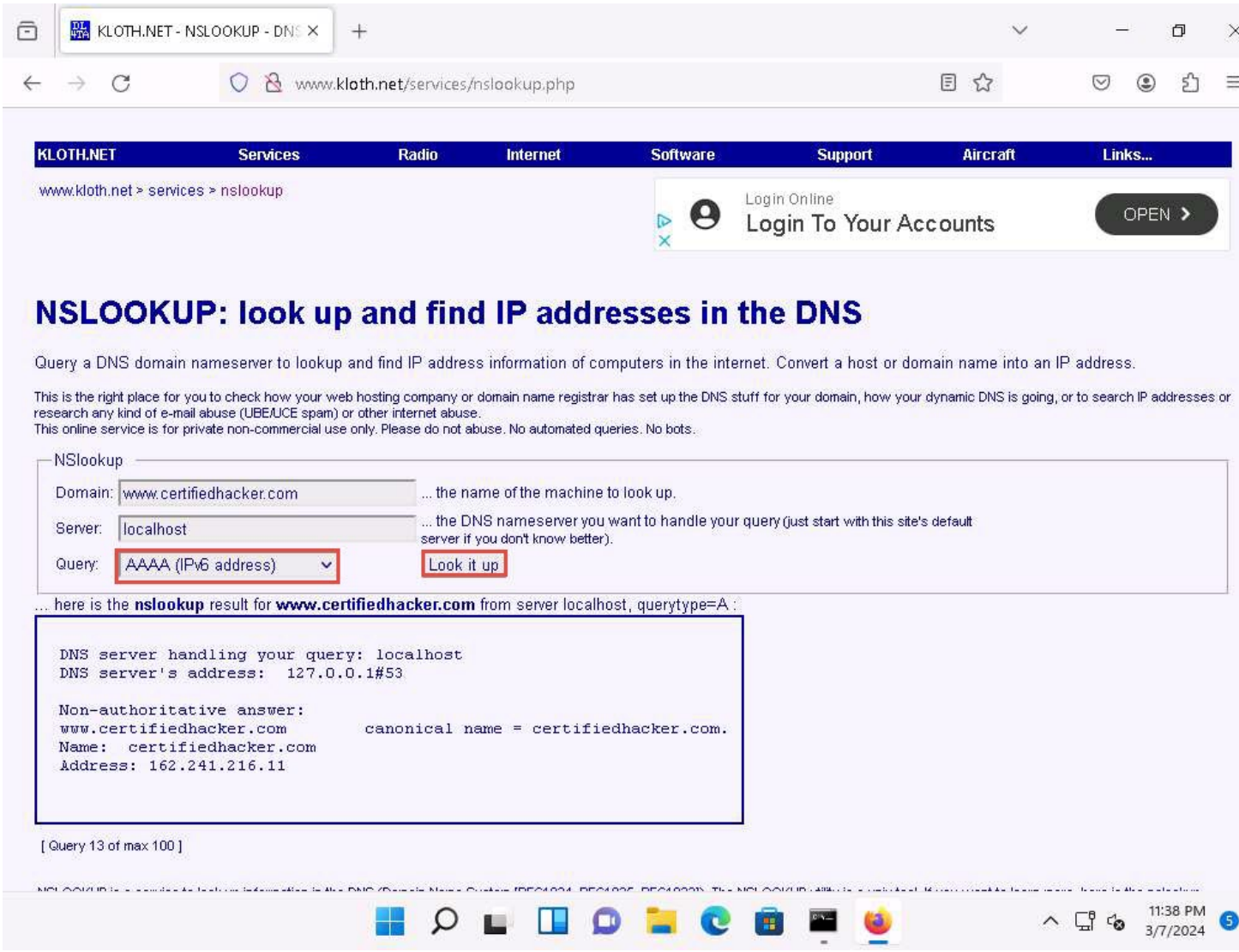
18. The authoritative name server stores the records associated with the domain. So, if an attacker can determine the authoritative name server (primary name server) and obtain its associated IP address, he/she might attempt to exploit the server to perform attacks such as DoS, DDoS, URL Redirection, etc.
19. You can also perform the same operations using the NSLOOKUP online tool. Conduct a series of queries and review the information to gain familiarity with the NSLOOKUP tool and gather information.
20. Now, we will use an online tool NSLOOKUP to gather DNS information about the target domain.
21. Open any web browser and go to **http://www.kloth.net/services/nslookup.php** (here, we are using **Mozilla Firefox**).
22. **NSLOOKUP** website appears, as shown in the screenshot.
23. Once the site opens, in the **Domain:** field, enter **www.certifiedhacker.com**. Set the **Query:** field to default [**A (IPv4 address)**] and click the **Look it up** button to review the results that are displayed.

24.

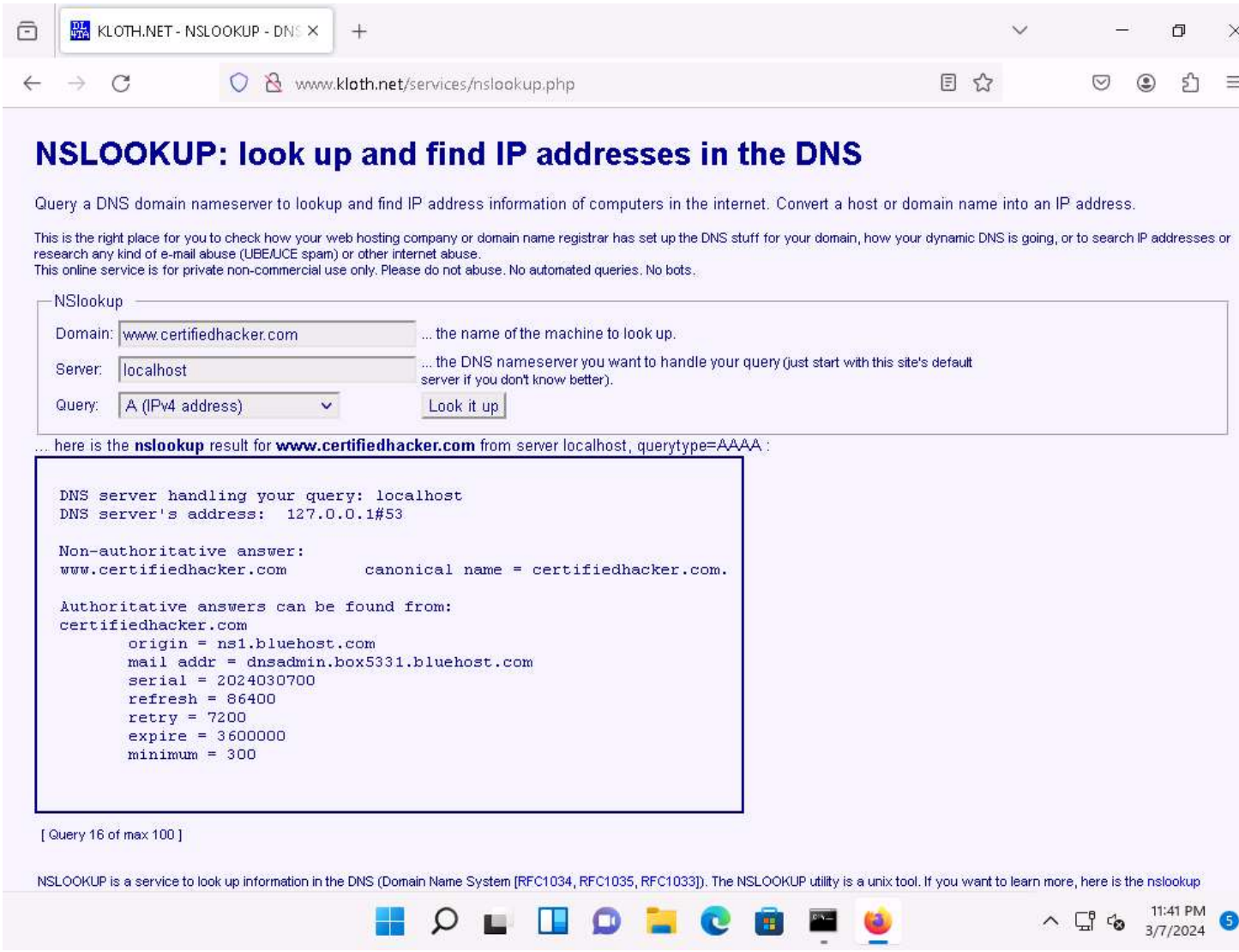


25. In the **Query:** field, click the drop-down arrow and check the different options that are available, as shown in the screenshot.
26. As you can see, there is an option for **AAAA (IPv6 address)**; select that and click **Look it up**. Perform queries related to this, since there are attacks that are possible over IPv6 networks as well.

27.


KLOTH.NET - NSLOOKUP - DNS
www.kloth.net/services/nslookup.php
KLOTH.NET
Services
Radio
Internet
Software
Support
Aircraft
Links...
www.kloth.net > services > nslookup
Login Online
Login To Your Accounts
OPEN
NSLOOKUP: look up and find IP addresses in the DNS
Query a DNS domain nameserver to lookup and find IP address information of computers in the internet. Convert a host or domain name into an IP address.
This is the right place for you to check how your web hosting company or domain name registrar has set up the DNS stuff for your domain, how your dynamic DNS is going, or to search IP addresses or research any kind of e-mail abuse (UBE/UCE spam) or other internet abuse.
This online service is for private non-commercial use only. Please do not abuse. No automated queries. No bots.
NSlookup
Domain: www.certifiedhacker.com
... the name of the machine to look up.
Server: localhost
... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).
Query: AAAA (IPv6 address)
Look it up
... here is the nslookup result for www.certifiedhacker.com from server localhost, querytype=A :
DNS server handling your query: localhost
DNS server's address: 127.0.0.1#53
Non-authoritative answer:
www.certifiedhacker.com canonical name = certifiedhacker.com.
Name: certifiedhacker.com
Address: 162.241.216.11
[Query 13 of max 100]
11:38 PM
3/7/2024

28.



29. This concludes the demonstration of DNS information gathering using the nslookup command-line utility and NSLOOKUP online tool.
30. You can also use DNS lookup tools such as **DNSdumpster** (https://dnsdumpster.com) to extract additional target DNS information.
31. Close all open windows and document all the acquired information.

Question 2.5.1.1

Use the nslookup command-line utility to find the primary name server of the website www.certifiedhacker.com.

Score

Lab 6: Perform Network Footprinting

Lab Scenario

With the IP address, hostname, and domain obtained in the previous information gathering steps, as a professional ethical hacker, your next task is to perform network footprinting to gather the network-related information of a target organization such as network range, traceroute, TTL values, etc. This information will help you to create a map of the target network and perform a man-in-the-middle attack.

Lab Objectives

- Perform network tracerouting in Windows and Linux Machines

Overview of Network Footprinting

Network footprinting is a process of accumulating data regarding a specific network environment. It enables ethical hackers to draw a network diagram and analyze the target network in more detail to perform advanced attacks.

Task 1: Perform Network Tracerouting in Windows and Linux Machines

The route is the path that the network packet traverses between the source and destination. Network tracerouting is a process of identifying the path and hosts lying between the source and destination. Network tracerouting provides critical information such as the IP address of the hosts lying between the source and destination, which enables you to map the network topology of the organization. Traceroute can be used to extract information about network topology, trusted routers, firewall locations, etc.

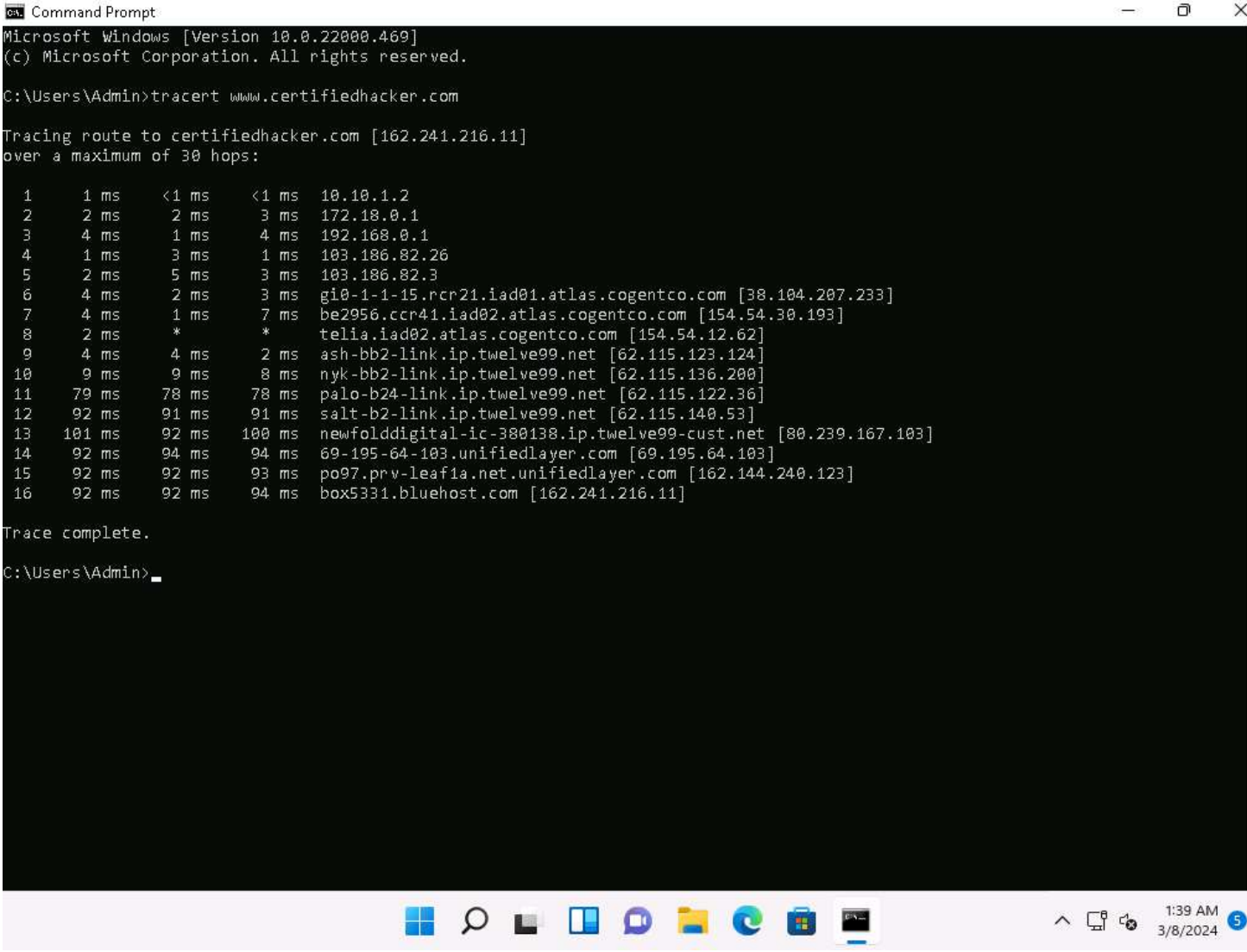
Here, we will perform network tracerouting using both Windows and Linux machines.

Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

1. In the **Windows 11** machine, open the **Command Prompt** window. Run **tracert www.certifiedhacker.com** command to view the hops that the packets made before reaching the destination.

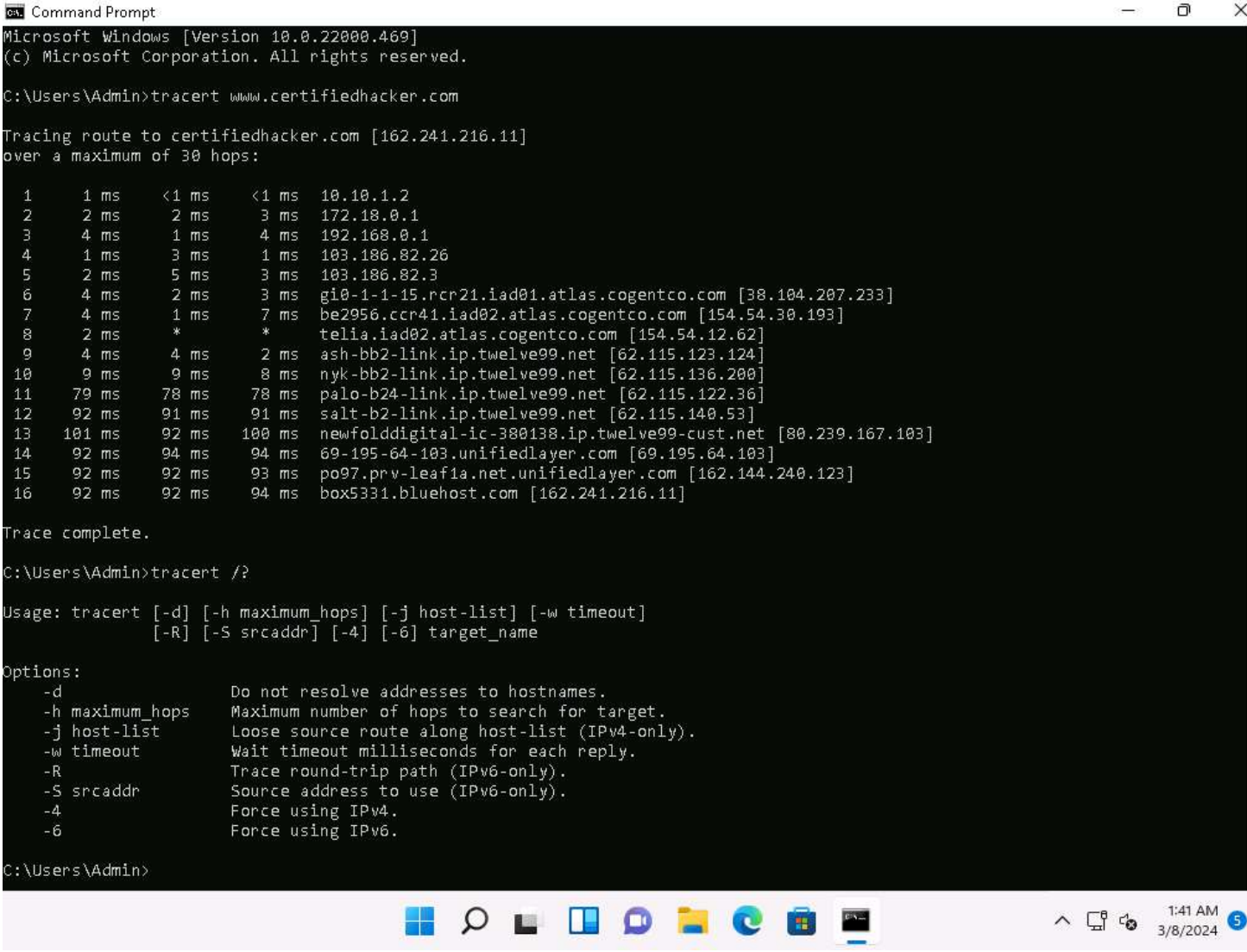
2. The results might differ when you perform the lab.

3.



4. Run **tracert /?** command to view the different options for the command, as shown in the screenshot.

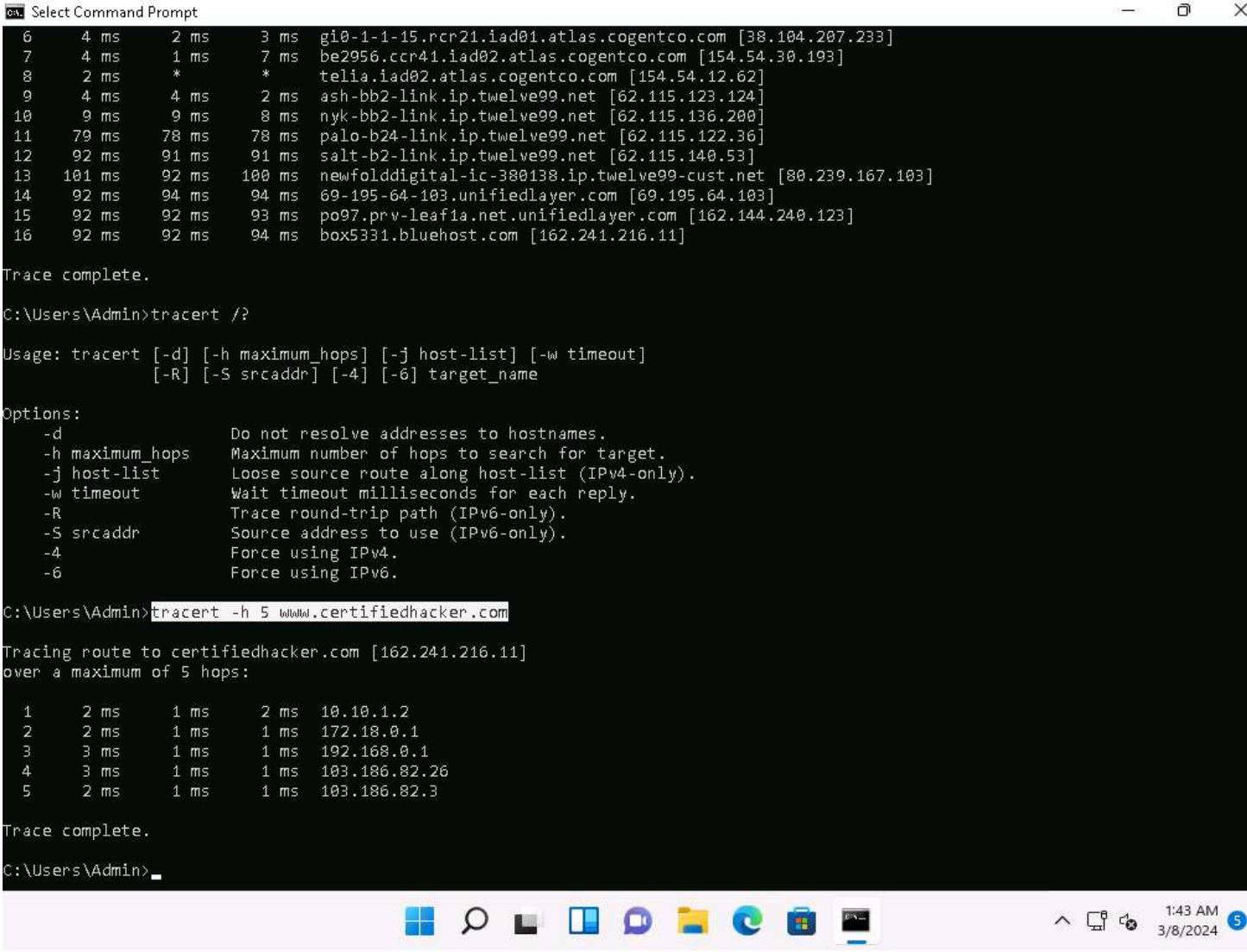
5.



6. Run **tracert -h 5 www.certifiedhacker.com** command to perform the trace, but with only 5 maximum hops allowed.

7. -h: Number of maximum hops.

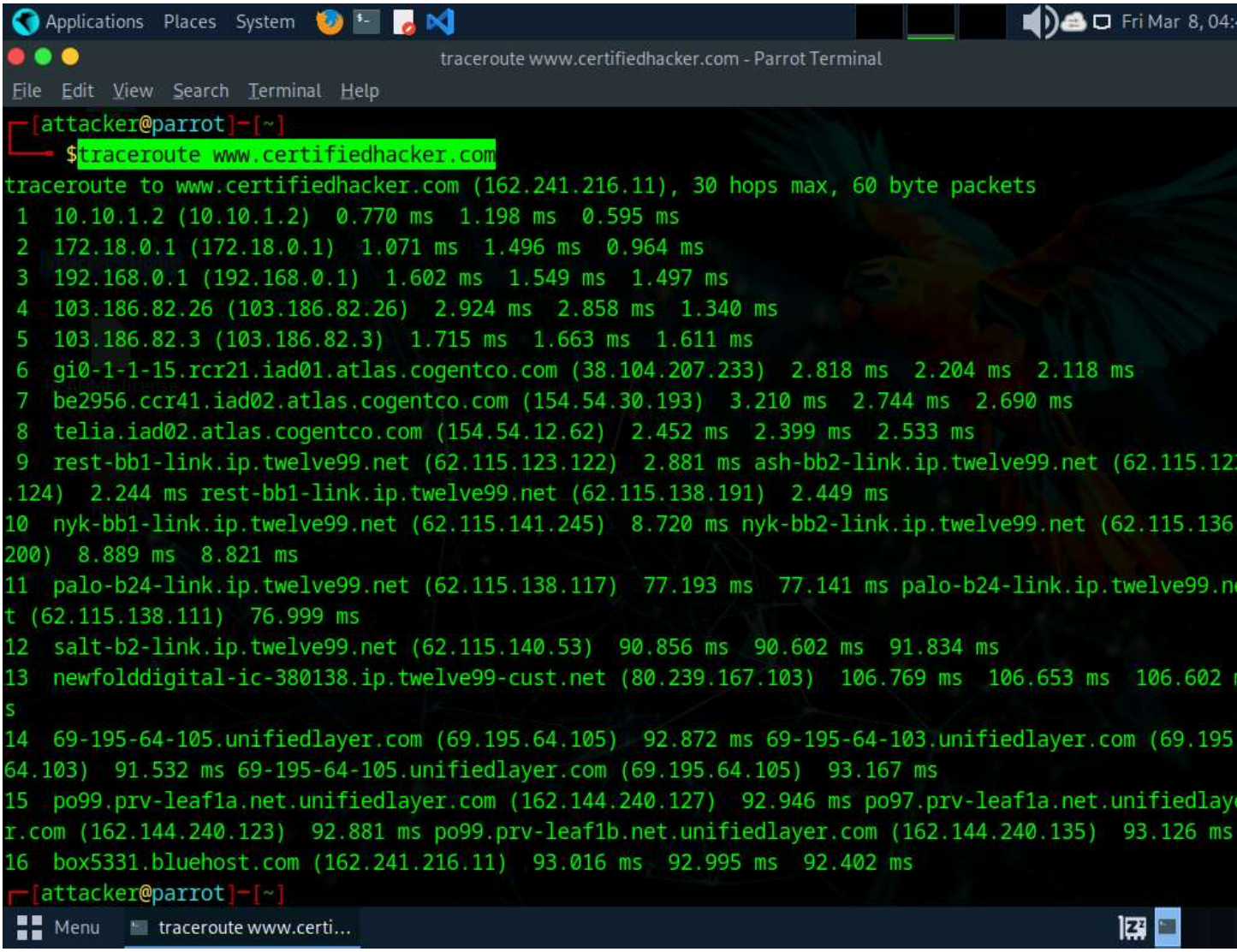
8.



9. After viewing the result, close the command prompt window.
10. Now, click Parrot Security to switch to the **Parrot Security** machine and open a **Terminal** window.
11. Run **traceroute www.certifiedhacker.com** command to view the hops that the packets made before reaching the destination.

12. Since we have set up a simple network, you can find the direct hop from the source to the target destination. However, screenshots may vary depending on the target destination.

13.



14. This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.
15. You can also use other traceroute tools such as **PingPlotter** (https://www.pingplotter.com/), **Traceroute NG** (https://www.solarwinds.com), etc. to extract additional network information of the target organization.
16. Close all open windows and document all acquired information.

Question 2.6.1.1

Perform network tracerouting using traceroute command on the Parrot machine for the www.certifiedhacker.com domain. Enter the IP address of the target domain.

Score

Lab 7: Perform Email Footprinting

Lab Scenario

As a professional ethical hacker, you need to be able to track emails of individuals (employees) from a target organization for gathering critical information that can help in building an effective hacking strategy. Email tracking allows you to collect information such as IP addresses, mail servers, OS details, geolocation, information about service providers involved in sending the mail etc. By using this information, you can perform social engineering and other advanced attacks.

Lab Objectives

- Gather information about a target by tracing emails using eMailTrackerPro

Overview of Email Footprinting

E-mail footprinting, or tracking, is a method to monitor or spy on email delivered to the intended recipient. This kind of tracking is possible through digitally time-stamped records that reveal the time and date when the target receives and opens a specific email.

Email footprinting reveals information such as:.

- Recipient's system IP address
- The GPS coordinates and map location of the recipient
- When an email message was received and read
- Type of server used by the recipient
- Operating system and browser information
- If a destructive email was sent
- The time spent reading the email
- Whether or not the recipient visited any links sent in the email
- PDFs and other types of attachments
- If messages were set to expire after a specified time

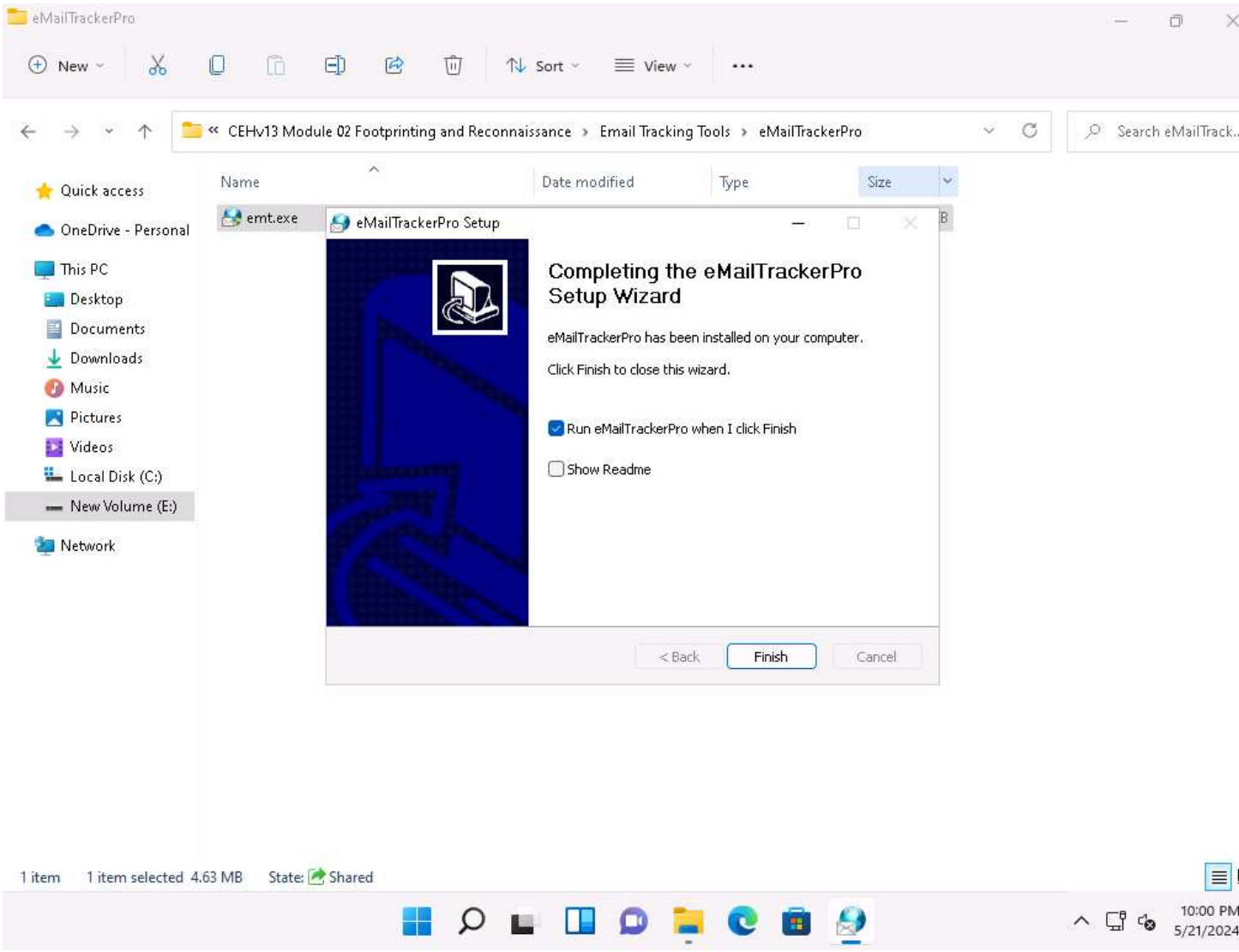
Task 1: Gather Information about a Target by Tracing Emails using eMailTrackerPro

The email header is a crucial part of any email and it is considered a great source of information for any ethical hacker launching attacks against a target. An email header contains the details of the sender, routing information, addressing scheme, date, subject, recipient, etc. Additionally, the email header helps ethical hackers to trace the routing path taken by an email before delivering it to the recipient.

Here, we will gather information by analyzing the email header using eMailTrackerPro.

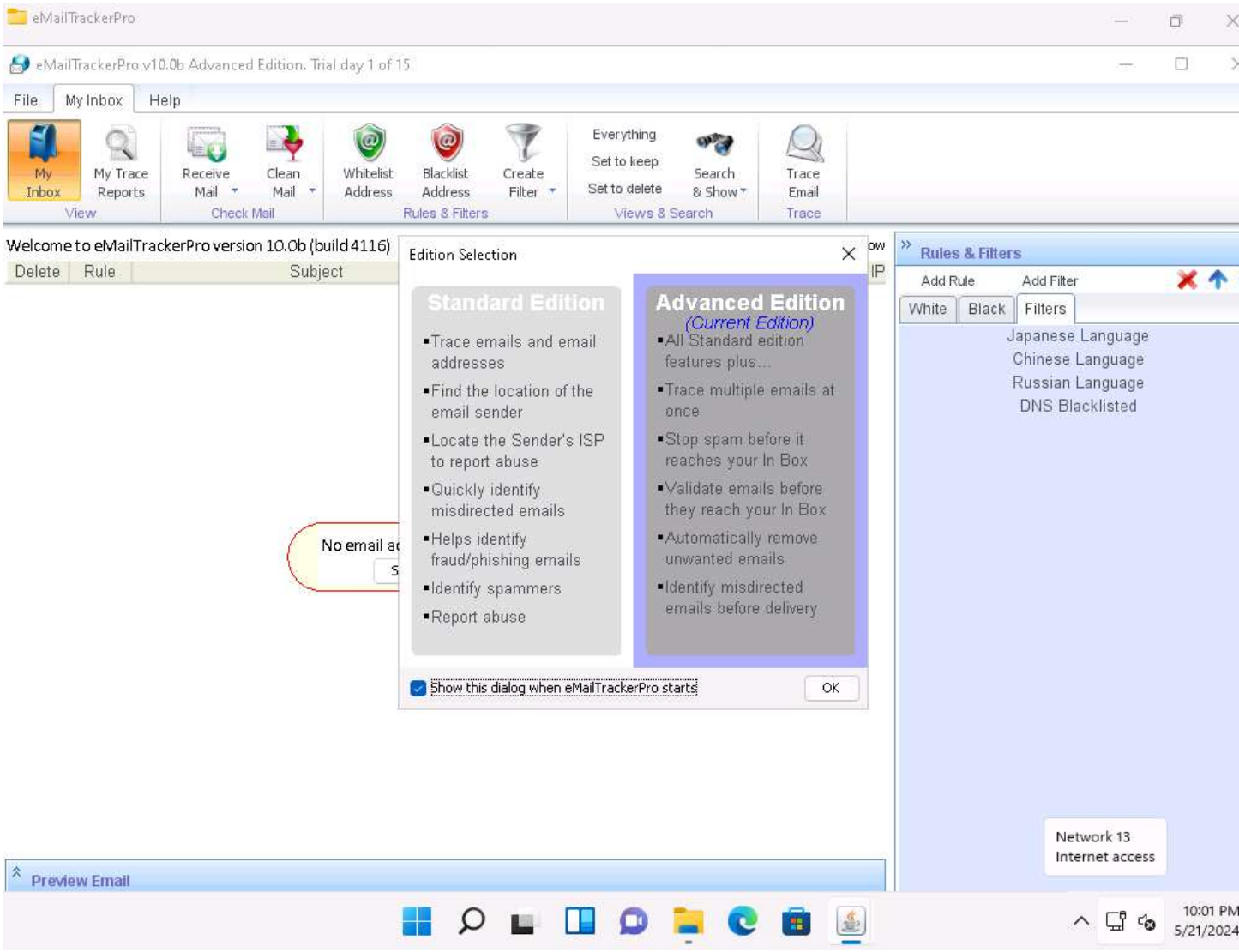
1. Click Windows 11 to switch to the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv13 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro** and double-click **emt.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.
3. The **eMailTrackerPro Setup** window appears. Follow the wizard steps (by selecting default options) to install eMailTrackerPro.
4. After the installation is complete, in the **Completing the eMailTrackerPro Setup Wizard**, uncheck the **Show Readme** check-box and click the **Finish** button to launch the eMailTrackerPro.

5.



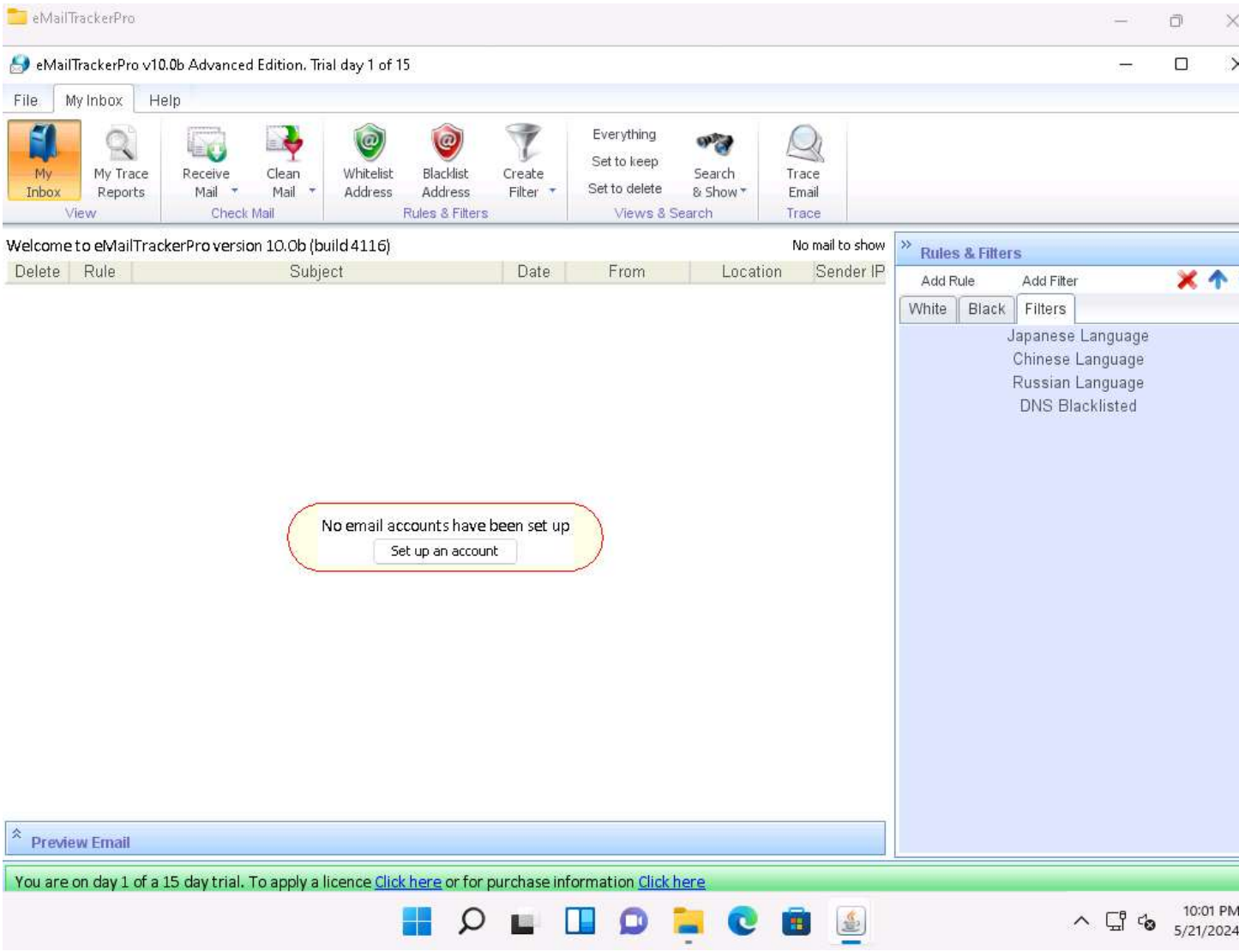
6. The main window of **eMailTrackerPro** appears along with the **Edition Selection** pop-up; click **OK**.

7.



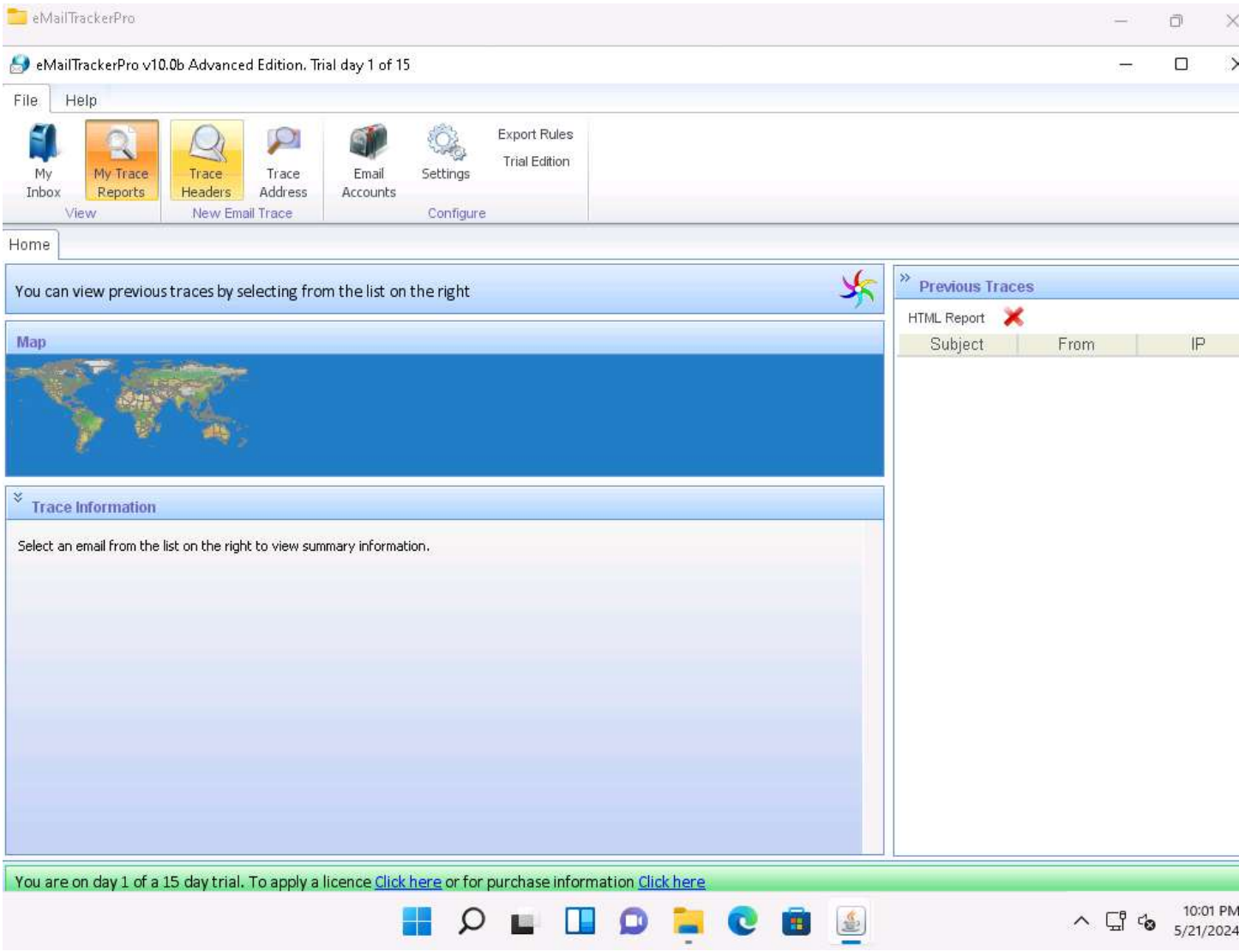
8. The **eMailTrackerPro** main window appears, as shown in the screenshot.

9.



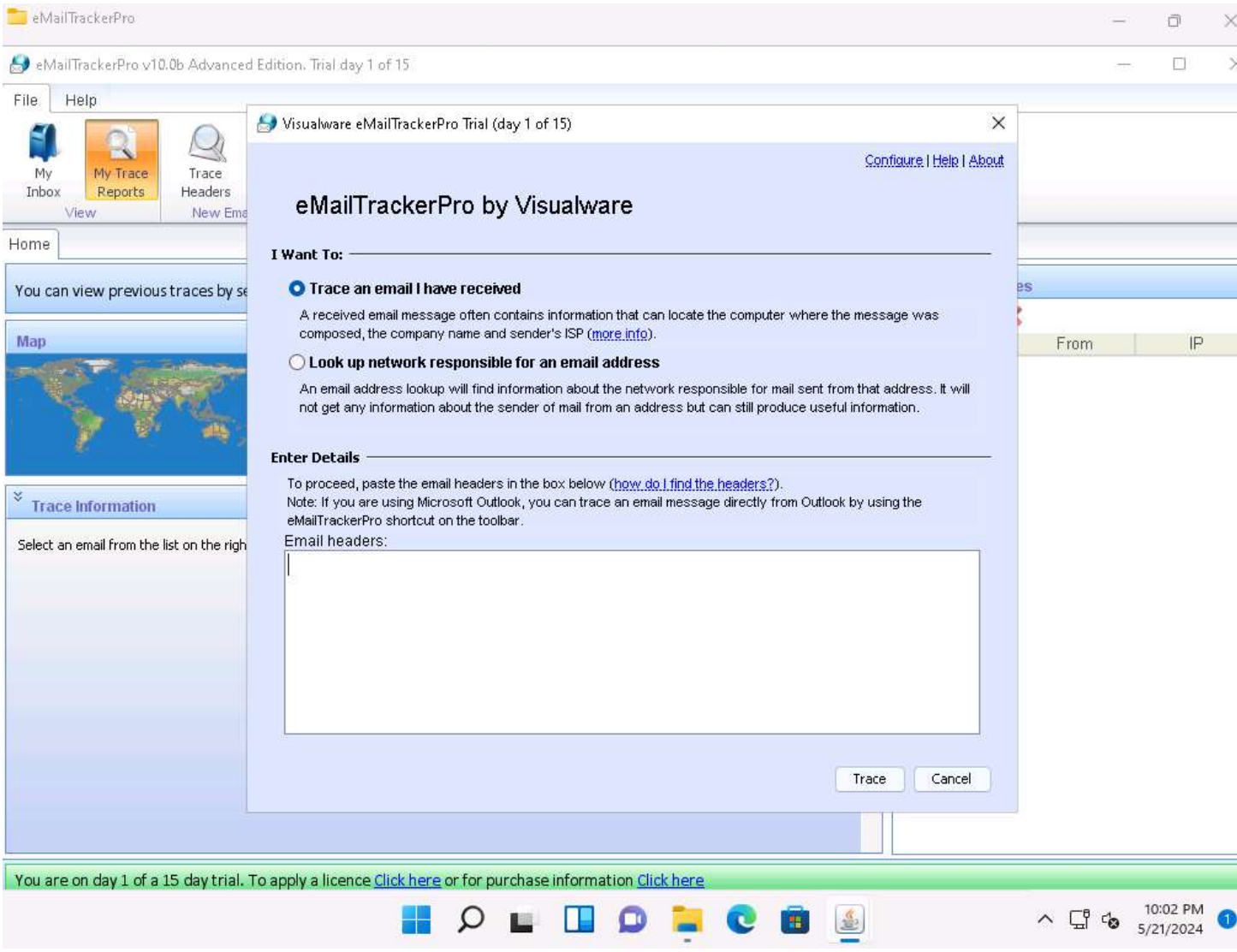
10. To trace email headers, click the **My Trace Reports** icon from the **View** section. (here, you will see the output report of the traced email header).
11. Click the **Trace Headers** icon from the **New Email Trace** section to start the trace.

12.



13. A pop-up window will appear; select **Trace an email I have received**. Copy the email header from the suspicious email you wish to trace and paste it in the **Email headers**: field under **Enter Details** section.

14.

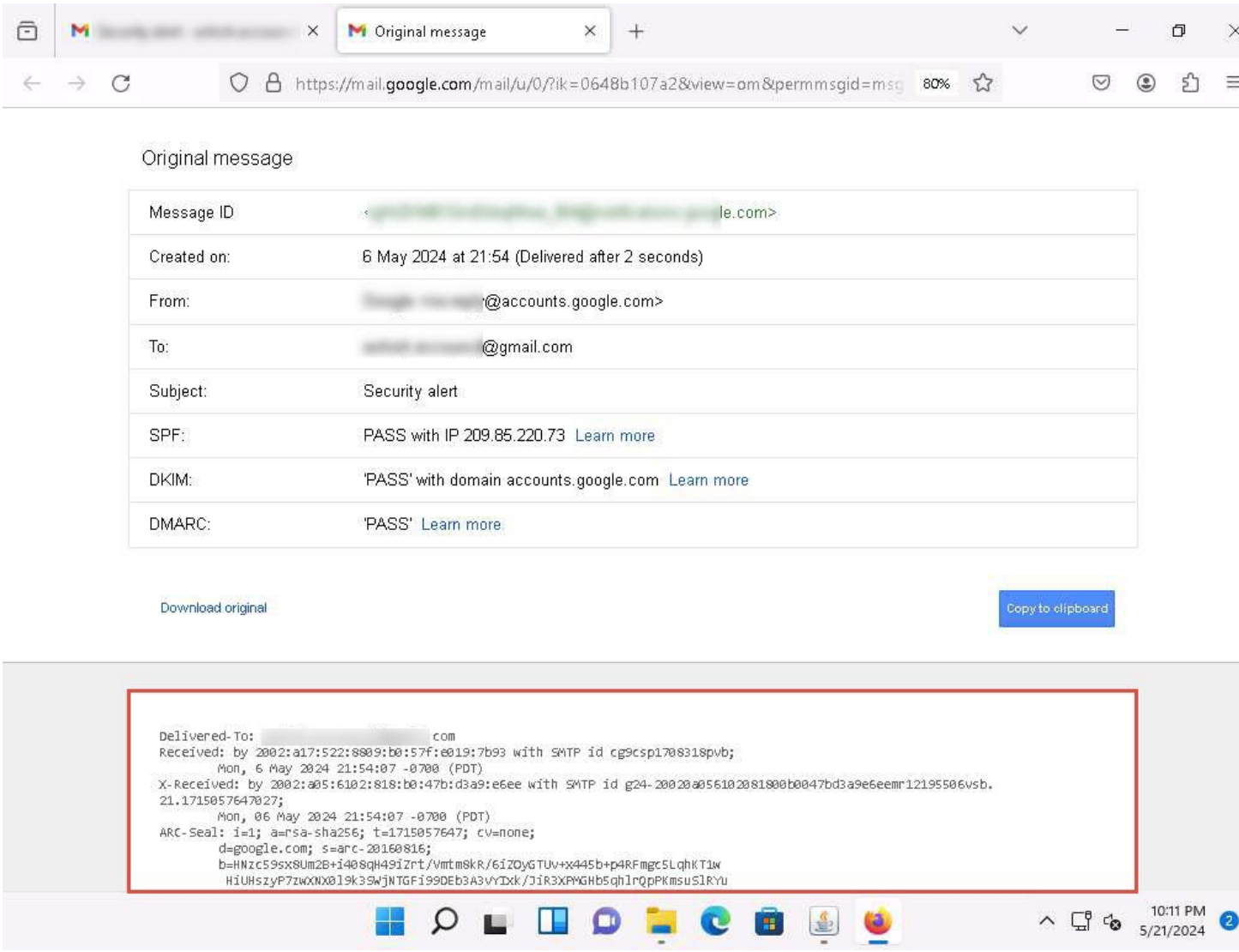


15. For finding email headers, open any web browser and log in to any email account of your choice; from the email inbox, open the message you would like to view headers for.

16. In **Gmail**, find the email header by following the steps:

    - Open an email; click the dots (**More**) icon arrow next to the **Reply** icon at the top-right corner of the message pane.
    - Select **Show original** from the list.
    - The **Original Message** window appears in a new browser tab with all the details about the email, including the email header

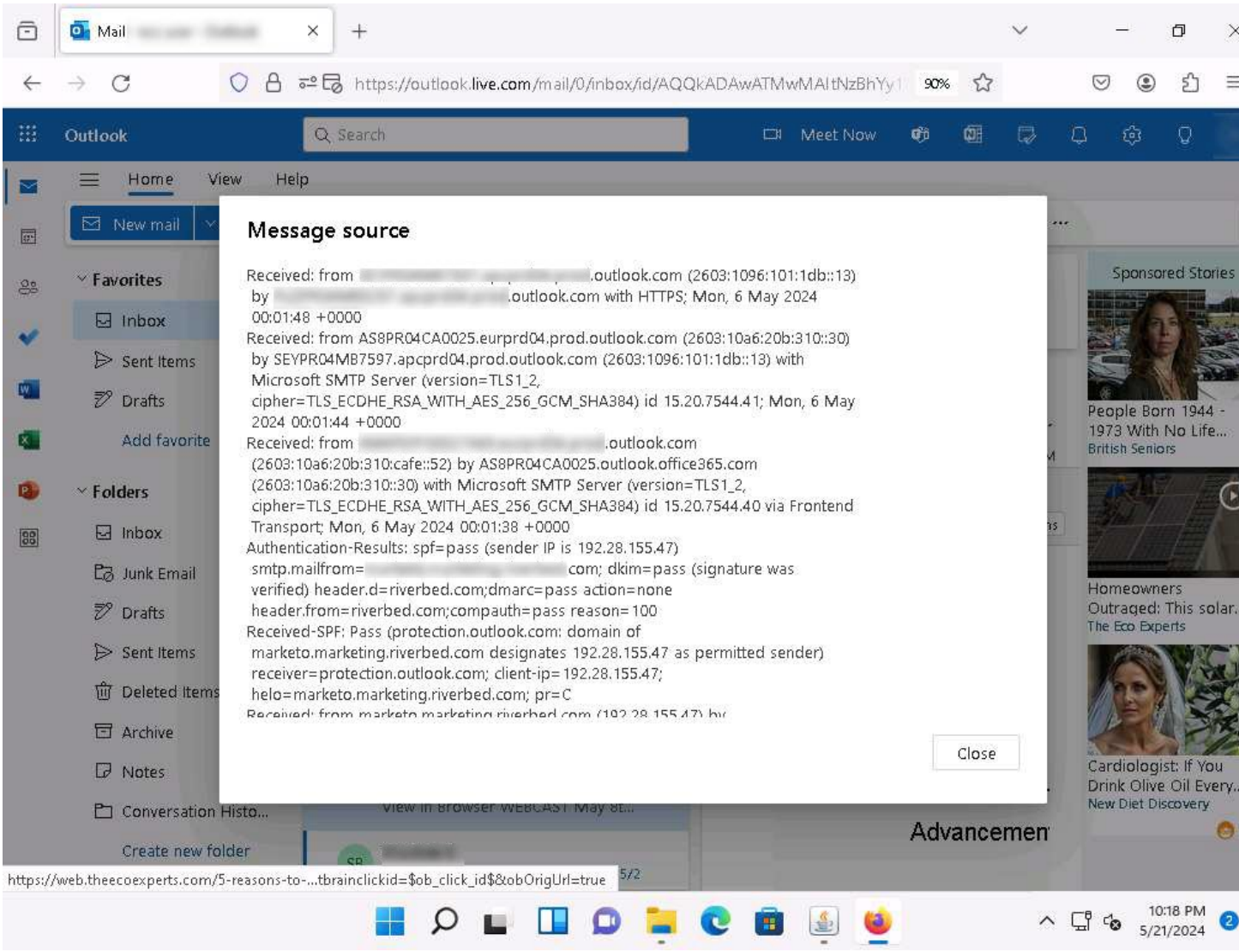
17.



18. In **Outlook**, find the email header by following the steps:

- Double-click the email to open it in a new window
- Click the **… (More actions)** icon present at the right of the message-pane to open message options
- From the options, click **View**
- The **view message source** window appears with all the details about the email, including the email header

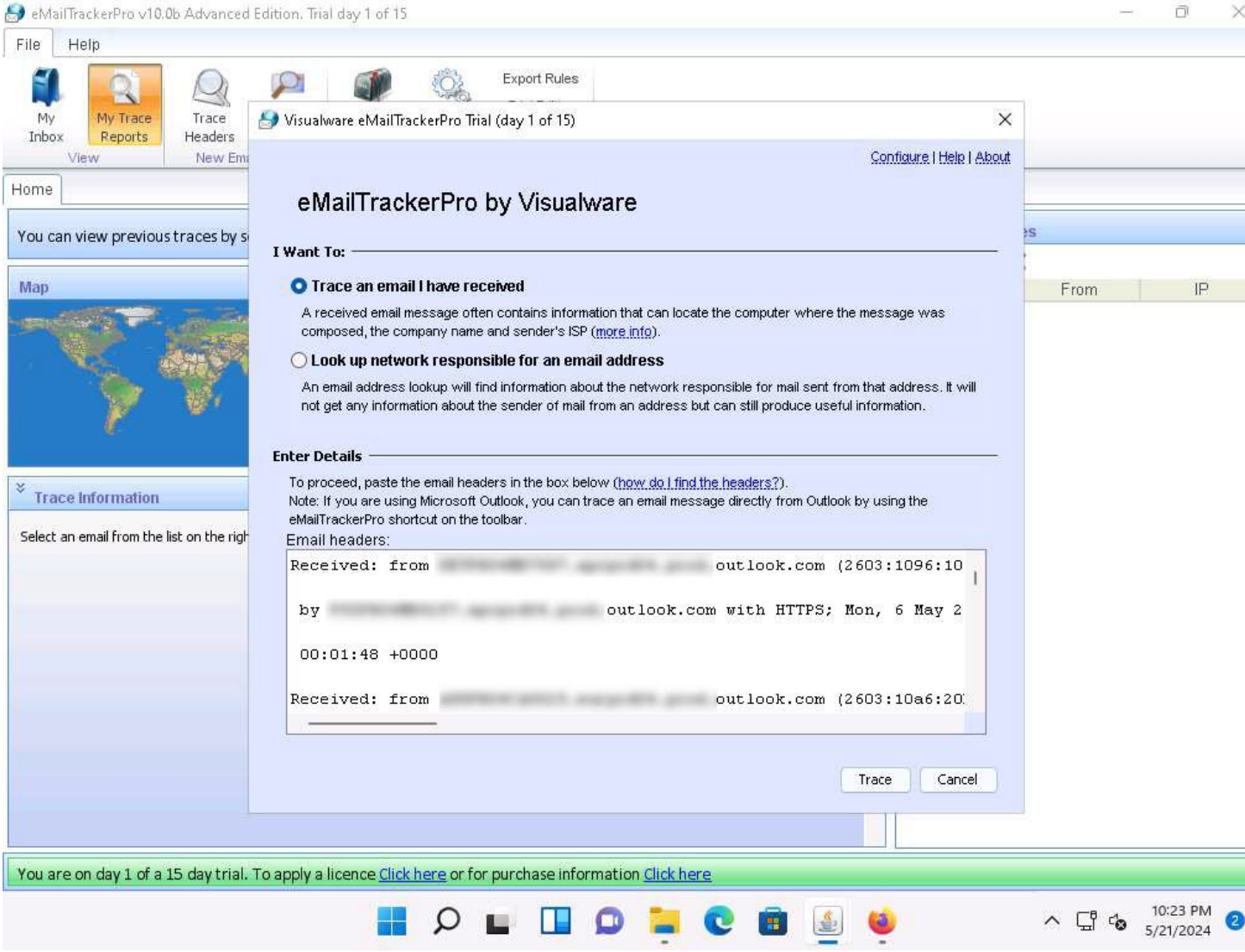
19.



20. Copy the entire email header text and paste it into the **Email headers**: field of eMailTrackerPro, and click **Trace**.

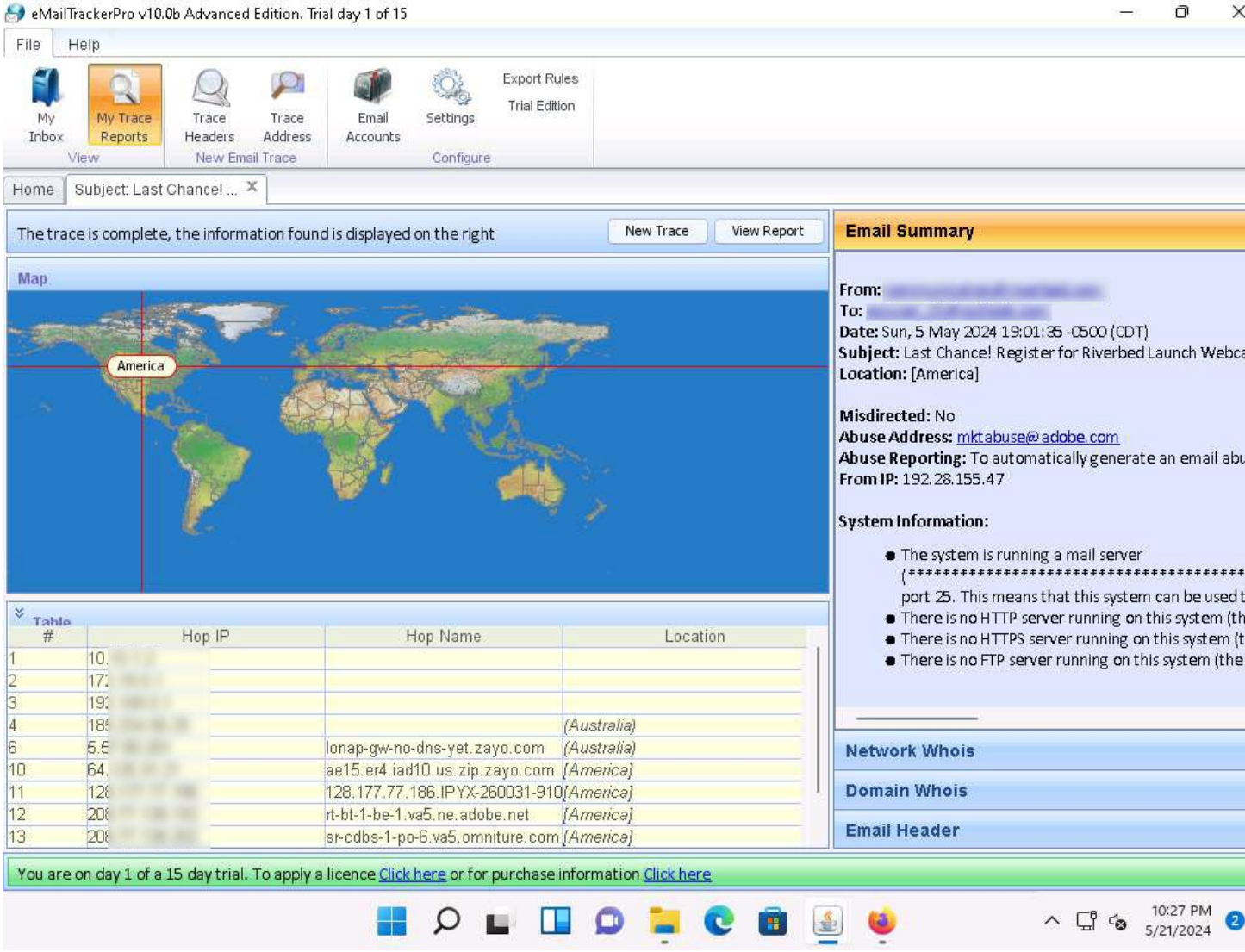
21. Here, we are analyzing the email header from gmail account. However, you can also analyze the email header from outlook account.

22.



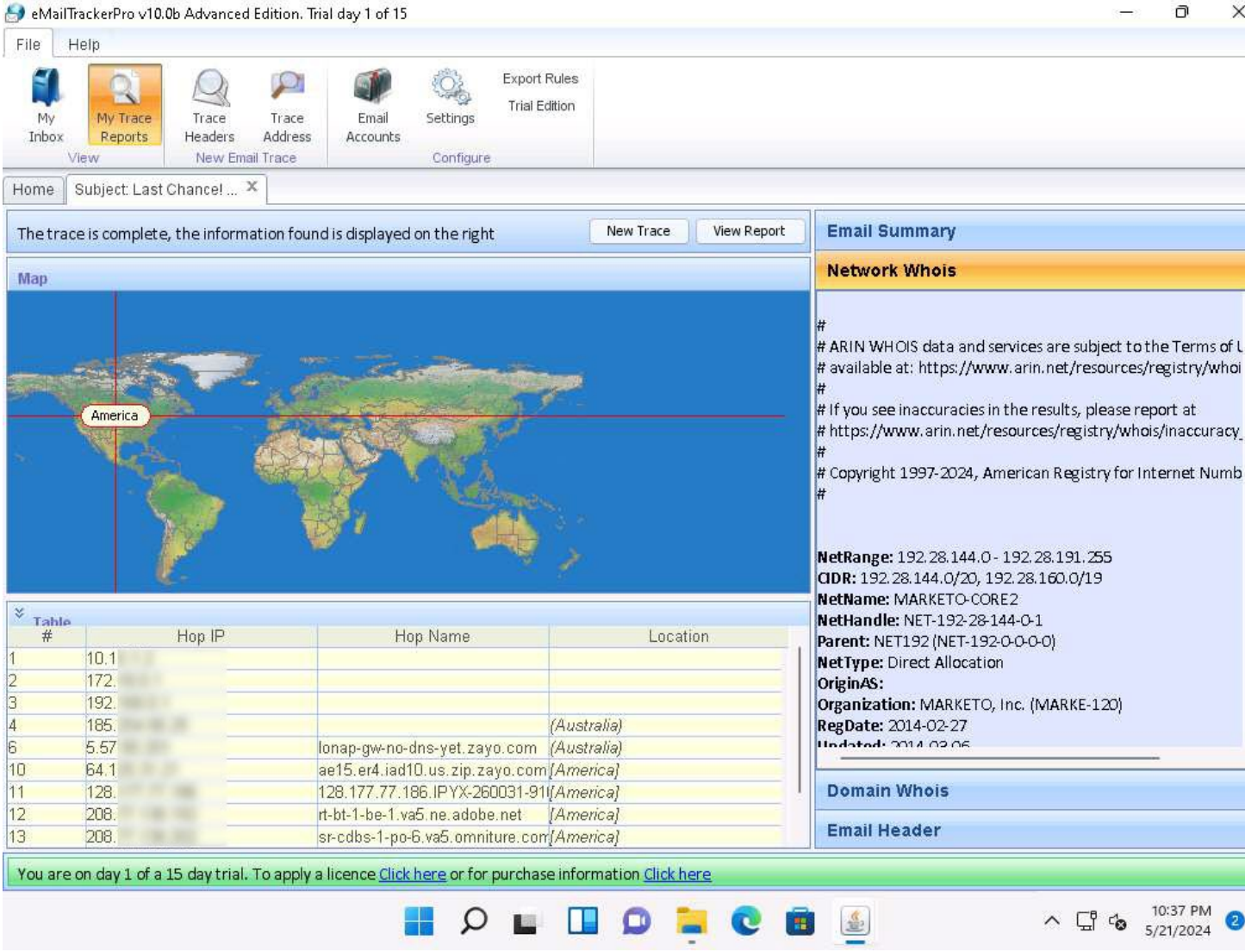
23. The **My Trace Reports** window opens.
24. The email location will be traced in a **Map** (world map GUI). You can also view the summary by selecting **Email Summary** on the right-hand side of the window. The **Table** section right below the Map shows the entire hop in the route, with the **IP** and suspected locations for each hop.

25.



26. To examine the Network Whois data, click the **Network Whois** button below **Email Summary** to view the Network Whois data.

27.



28. This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.
29. You can also use email tracking tools such as **MxToolbox** (https://mxtoolbox.com/), **Social Catfish** (https://socialcatfish.com/), **IP2Location Email Header Tracer** (https://www.ip2location.com/) etc. to track an email and extract target information such as sender identity, mail server, sender's IP address, location, etc.
30. Close all open windows and document all the acquired information.

Question 2.7.1.1

On the Windows 11 machine, use the eMailTrackerPro tool located at E:\CEH-Tools\CEHv13 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro to gather information about an email by analyzing the email header. Observe the output and enter YES if the tool contains the “Abuse Reporting” feature; else, enter NO.

Score

Lab 8: Perform Footprinting using Various Footprinting Tools

Lab Scenario

The information gathered in the previous steps may not be sufficient to reveal the potential vulnerabilities of the target. There could be more information available that could help in finding loopholes in the target. As an ethical hacker, you should look for as much information as possible about the target using various tools. This lab activity will demonstrate what other information you can extract from the target using various footprinting tools.

Lab Objectives

- Footprinting a target using Recon-ng

Overview of Footprinting Tools

Footprinting tools are used to collect basic information about the target systems in order to exploit them. Information collected by the footprinting tools contains the target's IP location information, routing information, business information, address, phone number and social security number, details about the source of an email and a file, DNS information, domain information, etc.

Task 1: Footprinting a Target using Recon-ng

Recon-ng is a web reconnaissance framework with independent modules and database interaction that provides an environment in which open-source web-based reconnaissance can be conducted. Here, we will use Recon-ng to perform network reconnaissance, gather personnel information, and gather target information from social networking sites.

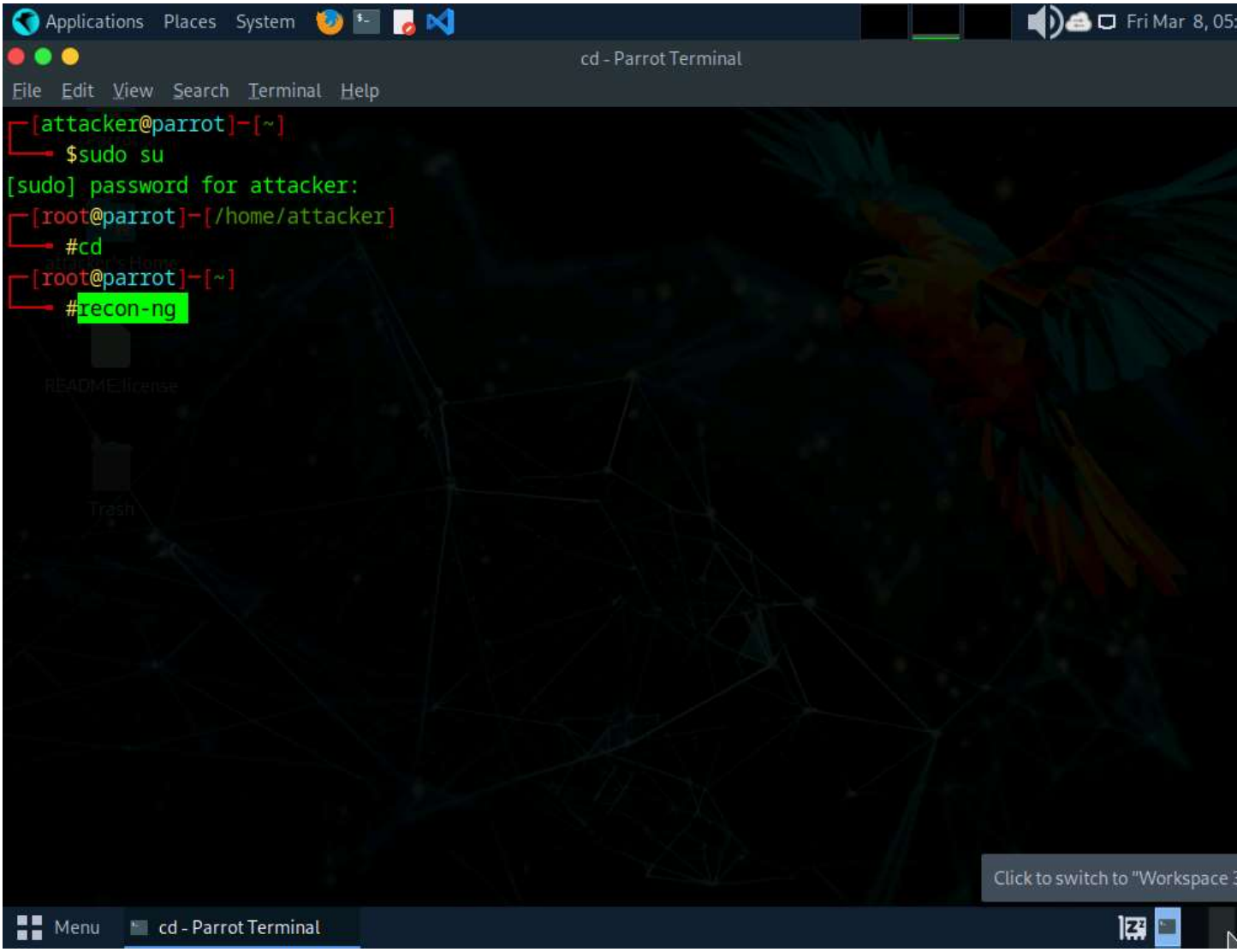
Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.
The results obtained might differ when you perform this lab task.

1. In the **Parrot Security** machine, open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

2. The password that you type will not be visible.

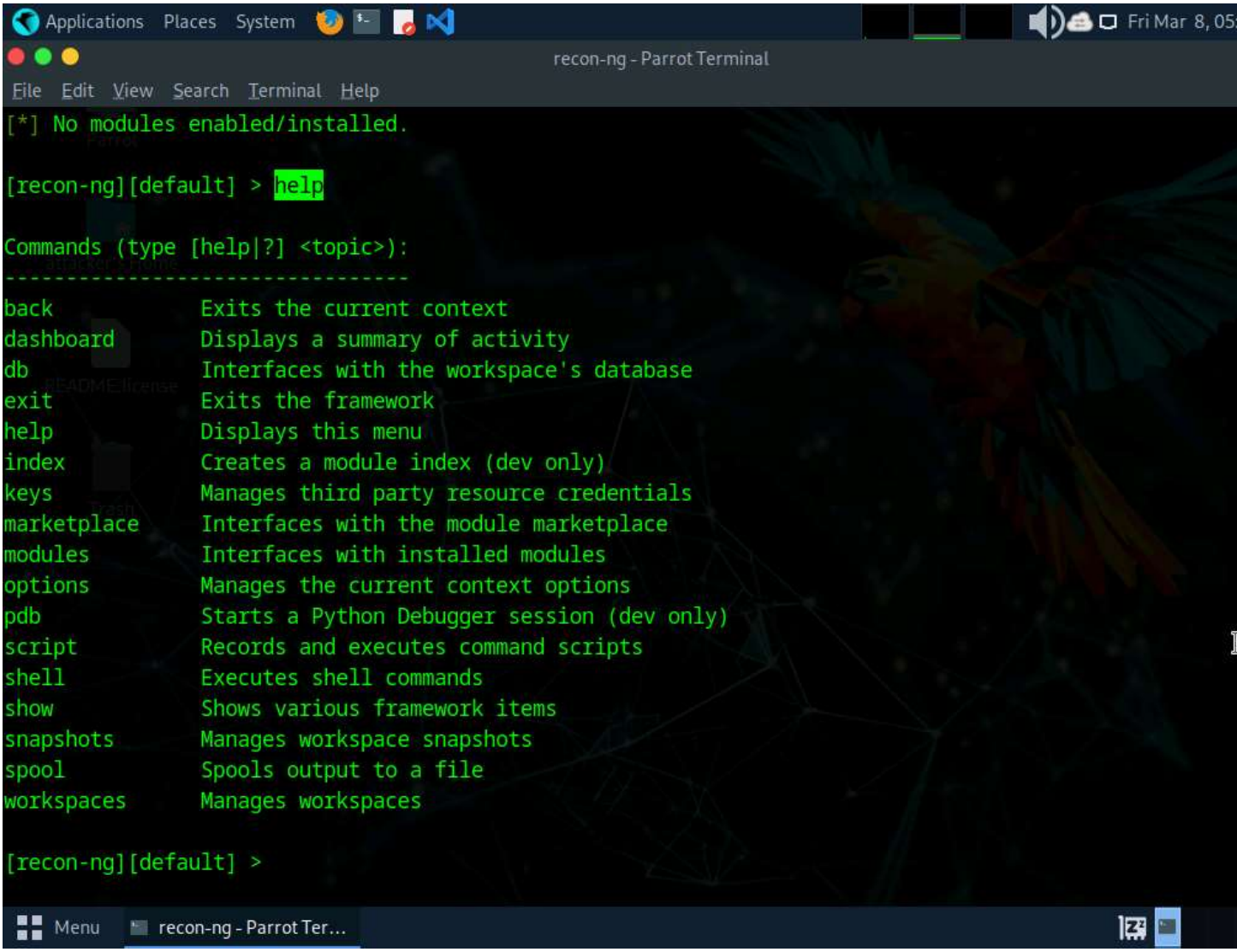
3. Now, run **cd** command to jump to the root directory and run **recon-ng** command to launch the application.

4.



5. Run **help** command to view all the commands that allow you to add/delete records to a database, query a database, etc.

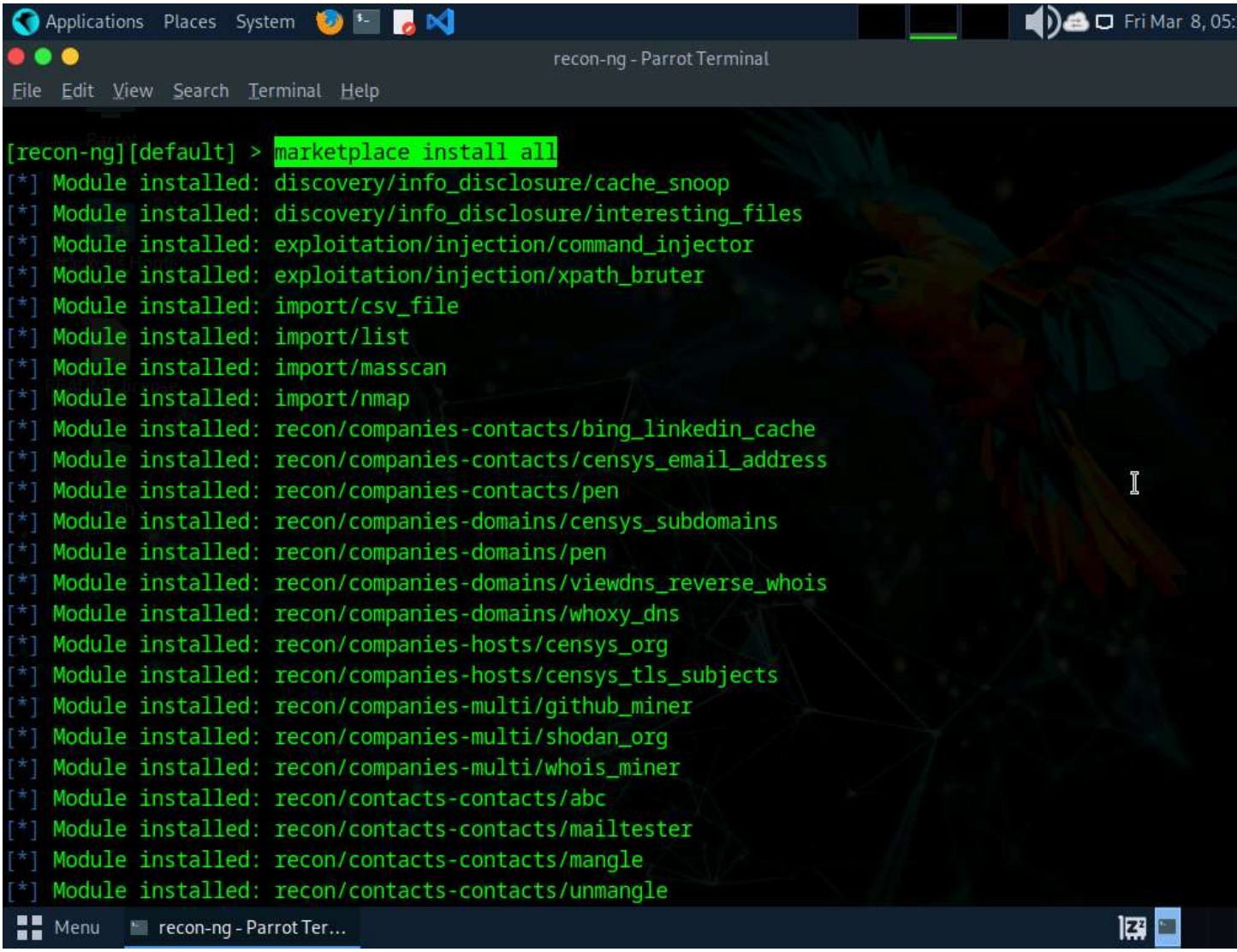
6.



7. Run **marketplace install all** command to install all the modules available in recon-ng.

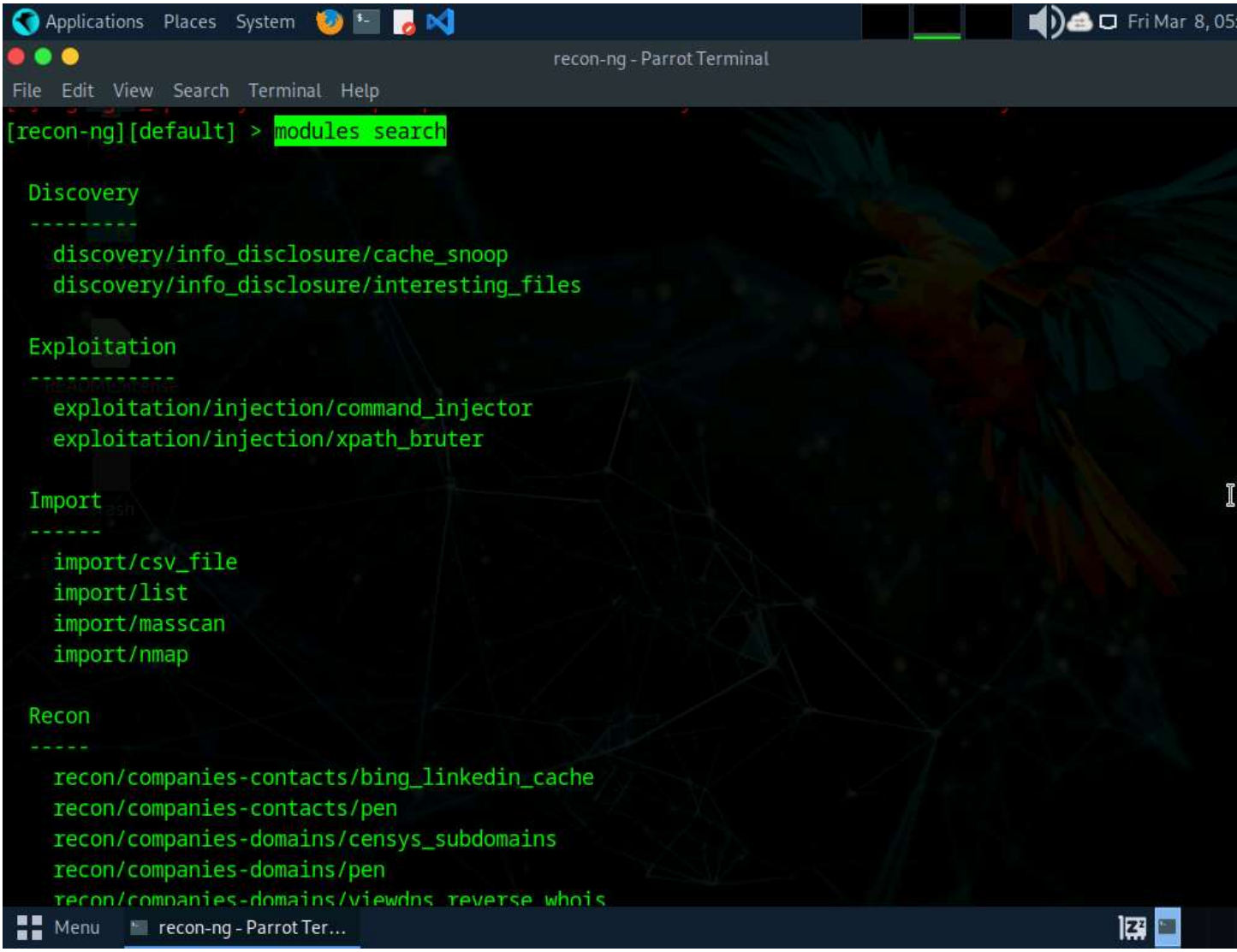
8. Ignore the errors while running the command.

9.



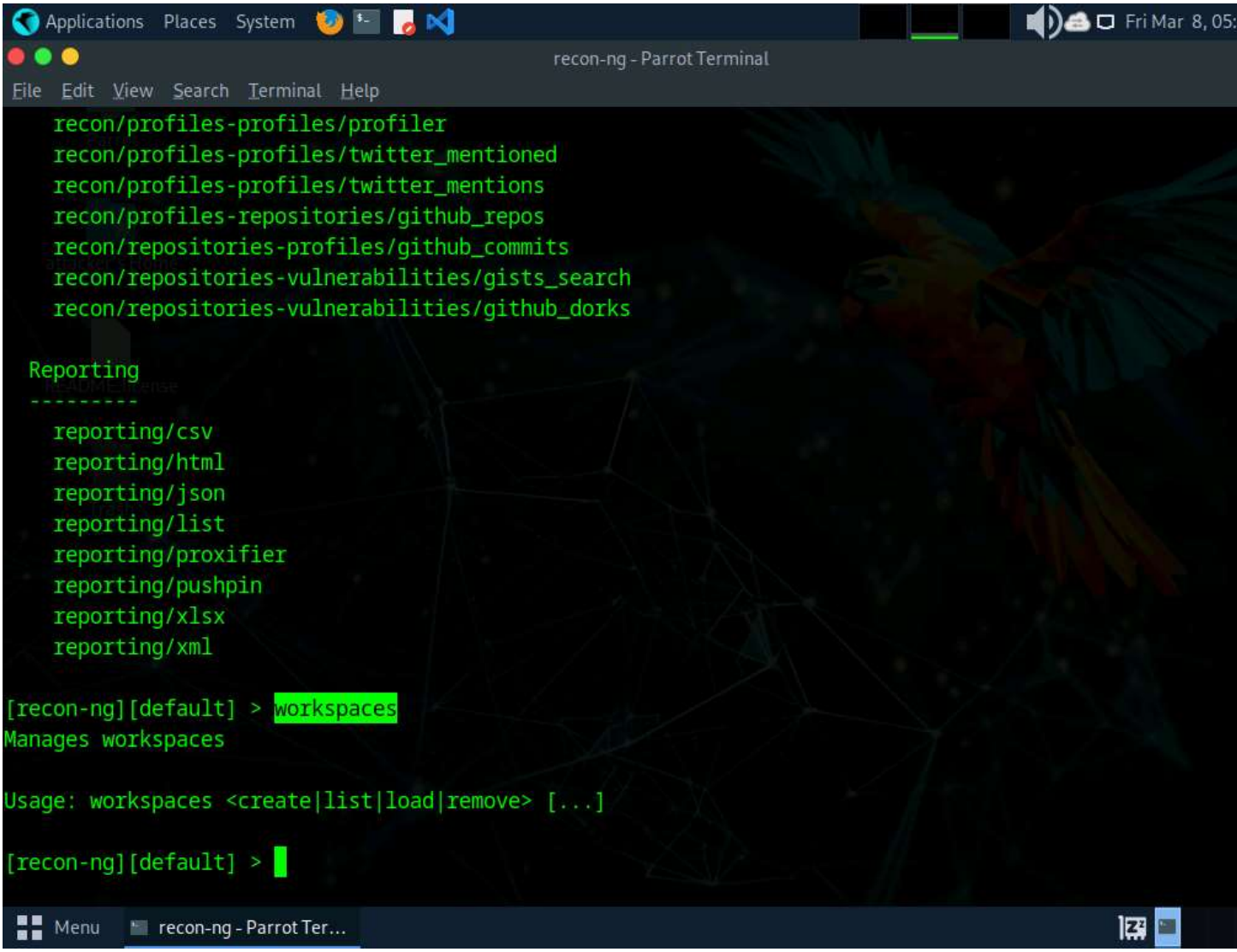
10. After the installation of modules, run **modules search** command. This displays all the modules available in recon-ng.

11.



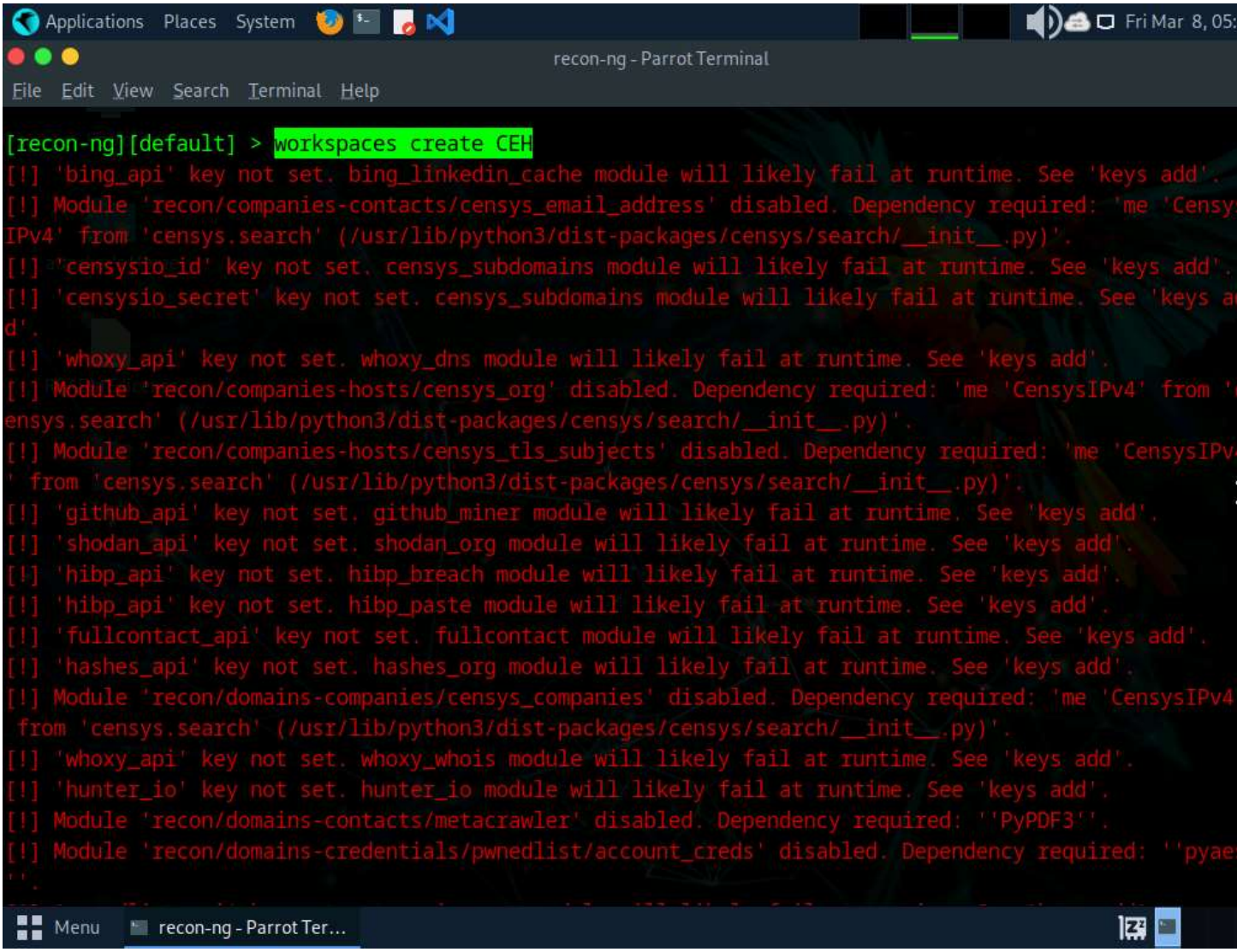
12. You will be able to perform network discovery, exploitation, reconnaissance, etc. by loading the required modules.
13. Run **workspaces** command to view the commands related to the workspaces.

14.



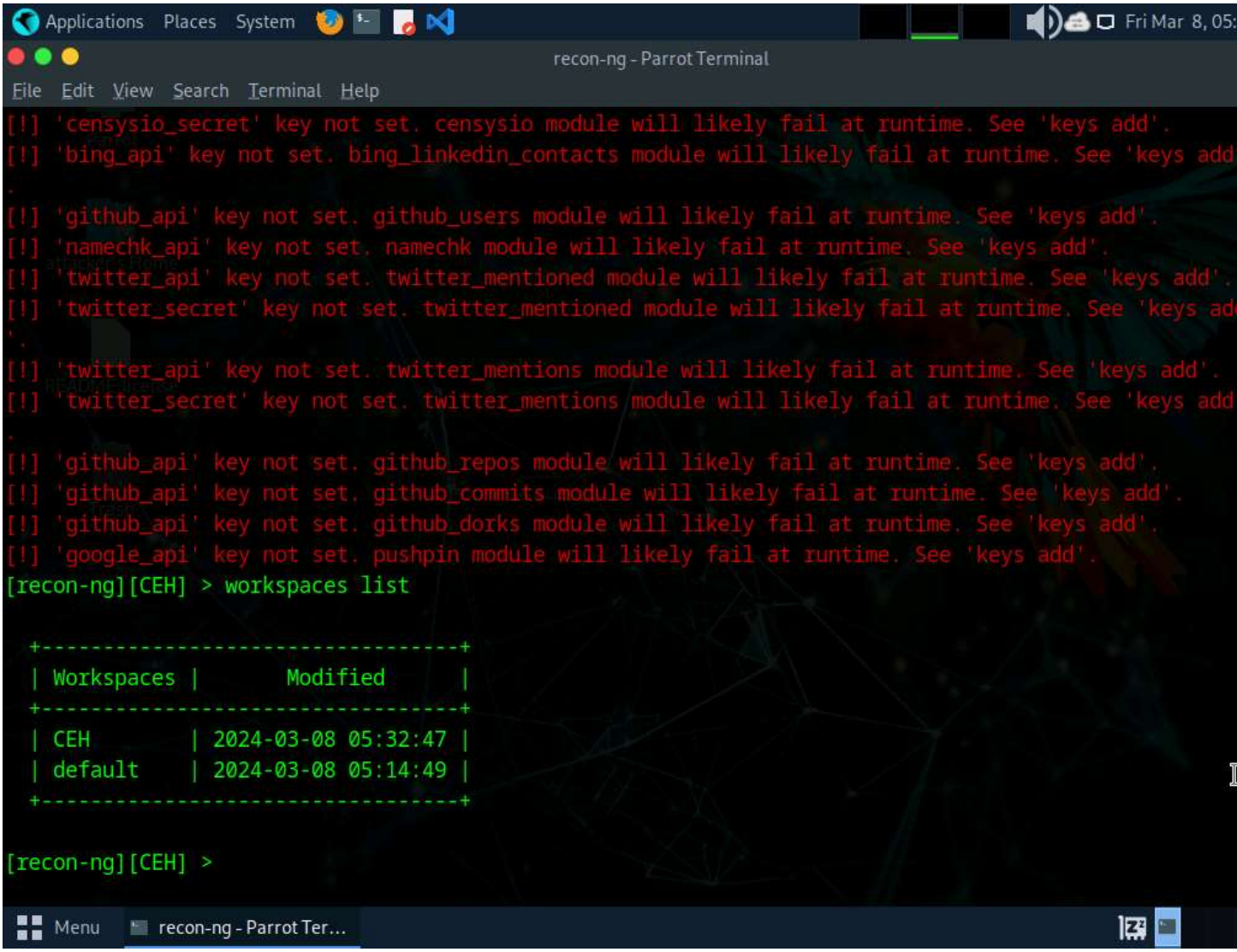
15. Create a workspace in which to perform network reconnaissance. In this task, we shall be creating a workspace named **CEH**.
16. To create the workspace, run **workspaces create CEH** command. This creates a workspace named CEH.

17.



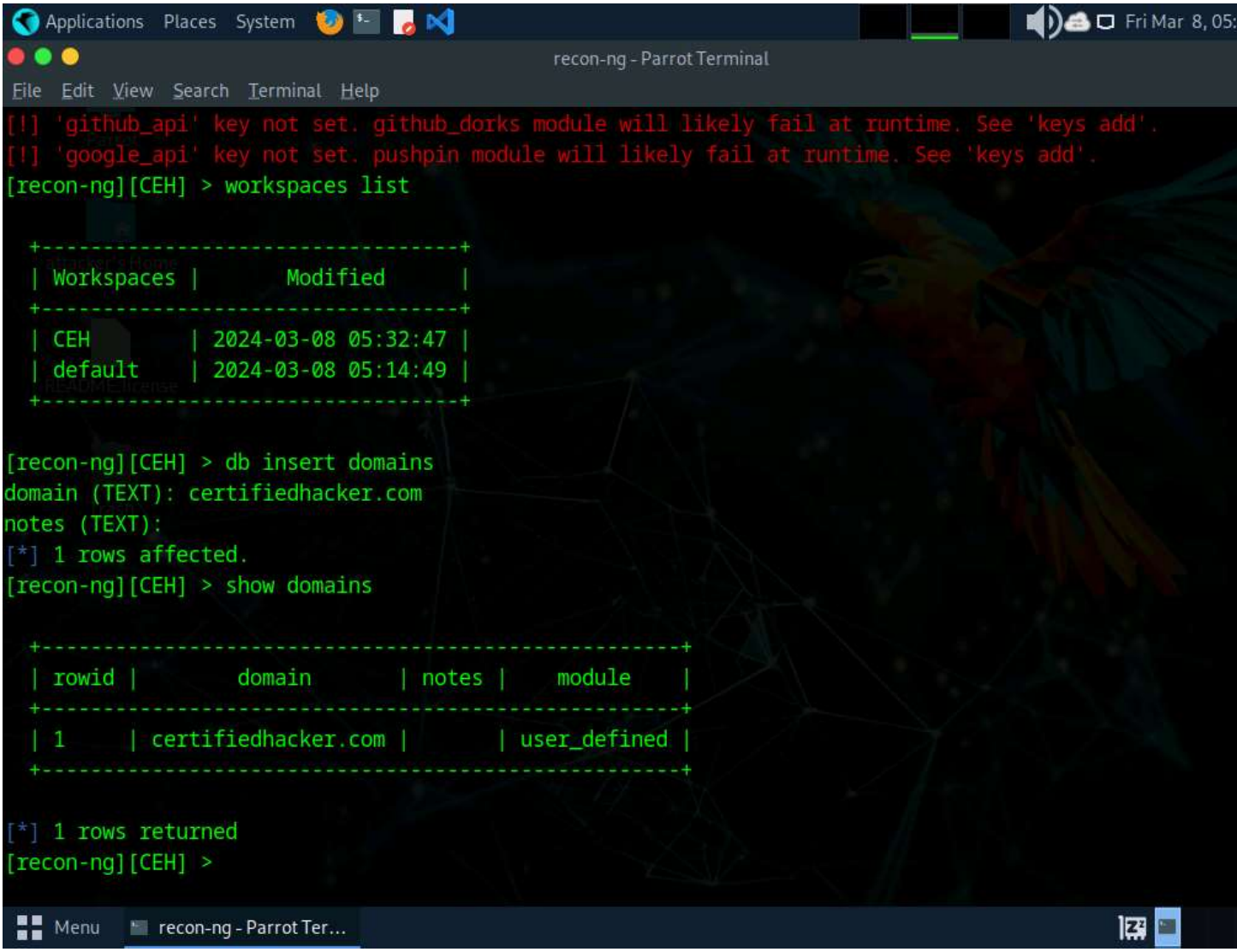
18. Enter **workspaces list**. This displays a list of workspaces (along with the workspace added in the previous step) that are present within the workspaces databases.

19.



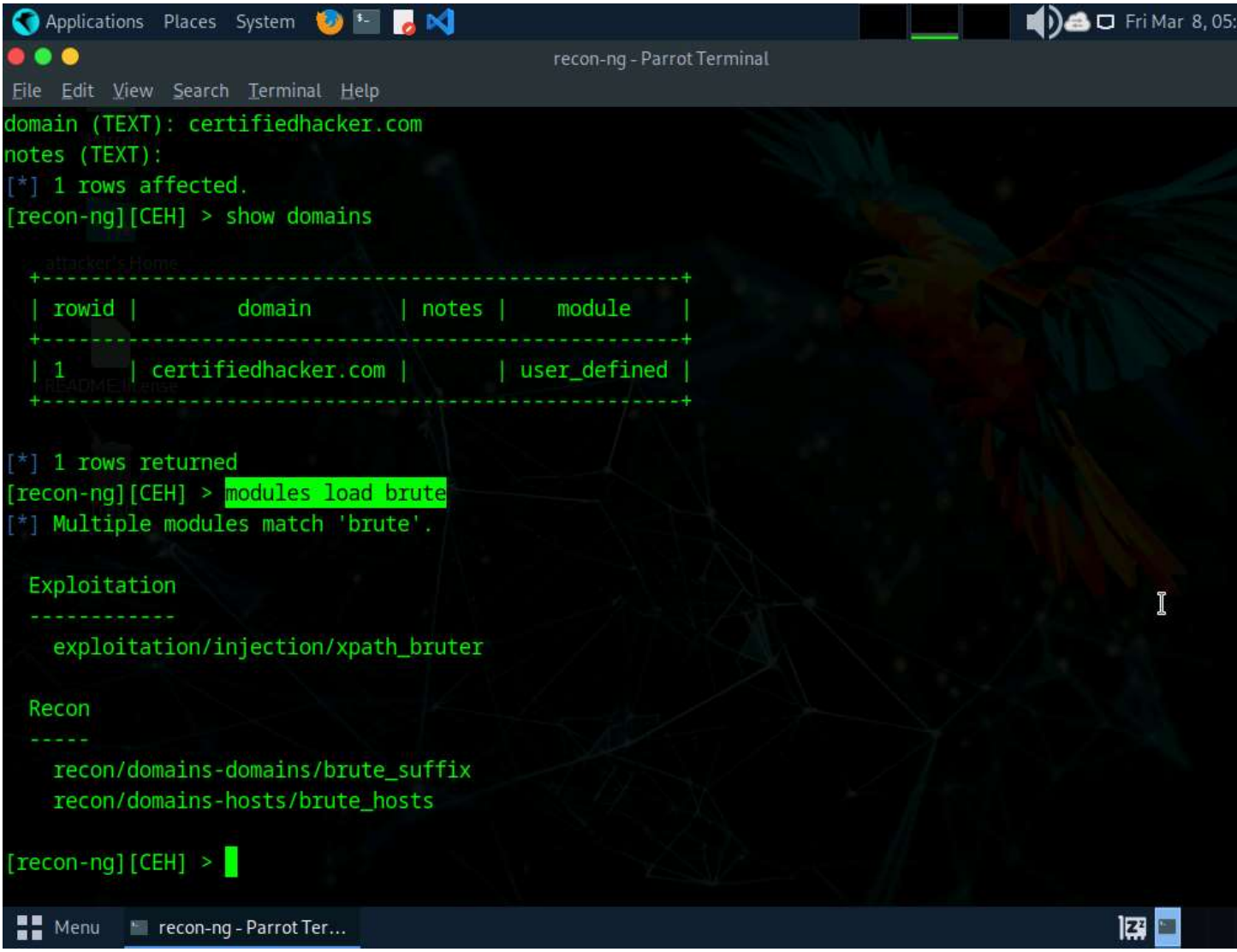
20. Add a domain in which you want to perform network reconnaissance.
21. Issue the command **db insert domains**.
22. Under **domain (TEXT)** option type **certifiedhacker.com** and press **Enter**. In the **notes (TEXT)** option press **Enter**. This adds certifiedhacker.com to the present workspace.
23. You can view the added domain by issuing the **show domains** command, as shown in the screenshot.

24.



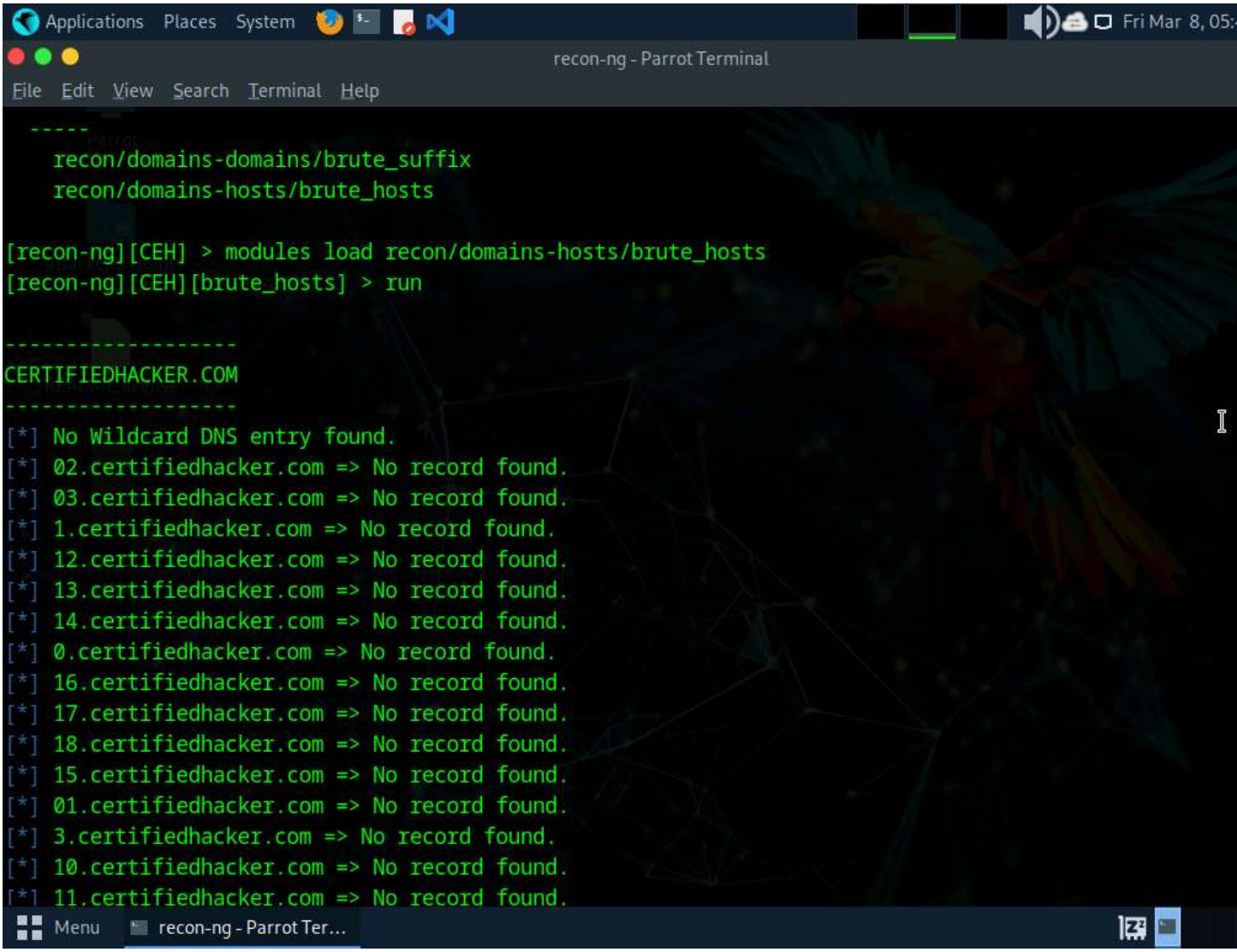
25. Harvest the hosts-related information associated with **certifiedhacker.com** by loading network reconnaissance modules such as brute_hosts, Netcraft, and Bing.
26. Issue **modules load brute** command to view all the modules related to brute forcing. In this task, we will be using the **recon/domains-hosts/brute_hosts** module to harvest hosts.

27.



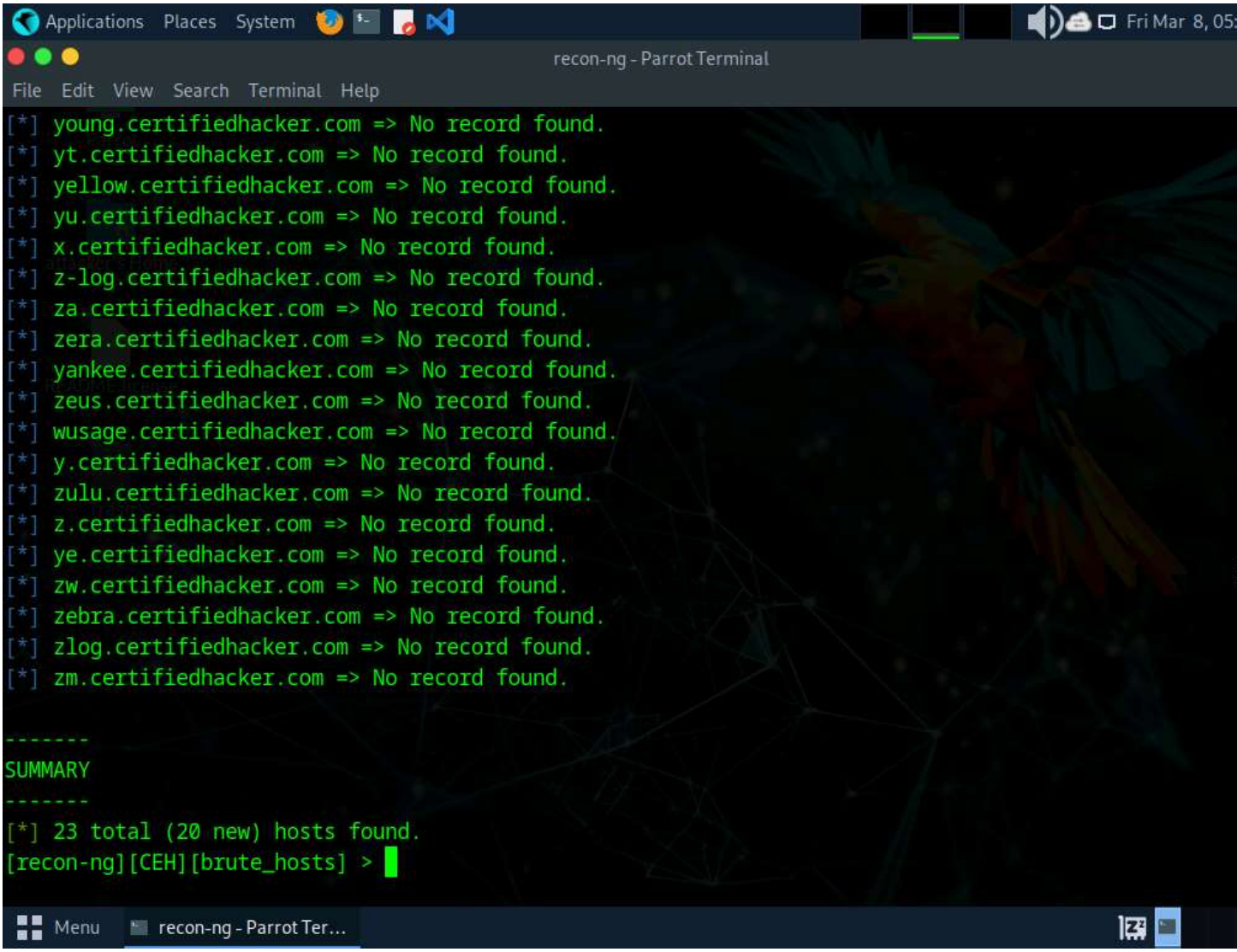
28. To load the **recon/domains-hosts/brute_hosts** module, issue **modules load recon/domains-hosts/brute_hosts** command.
29. Issue **run** command. This begins to harvest the hosts, as shown in the screenshot.

30.



31. Observe that hosts have been added by running the **recon/domains-hosts/brute_hosts** module.

32.



33. You have now harvested the hosts related to certifiedhacker.com using the brute_hosts module. You can use other modules such as Netcraft and Bing to harvest more hosts.

34. Use the **back** command to go back to the CEH attributes terminal.

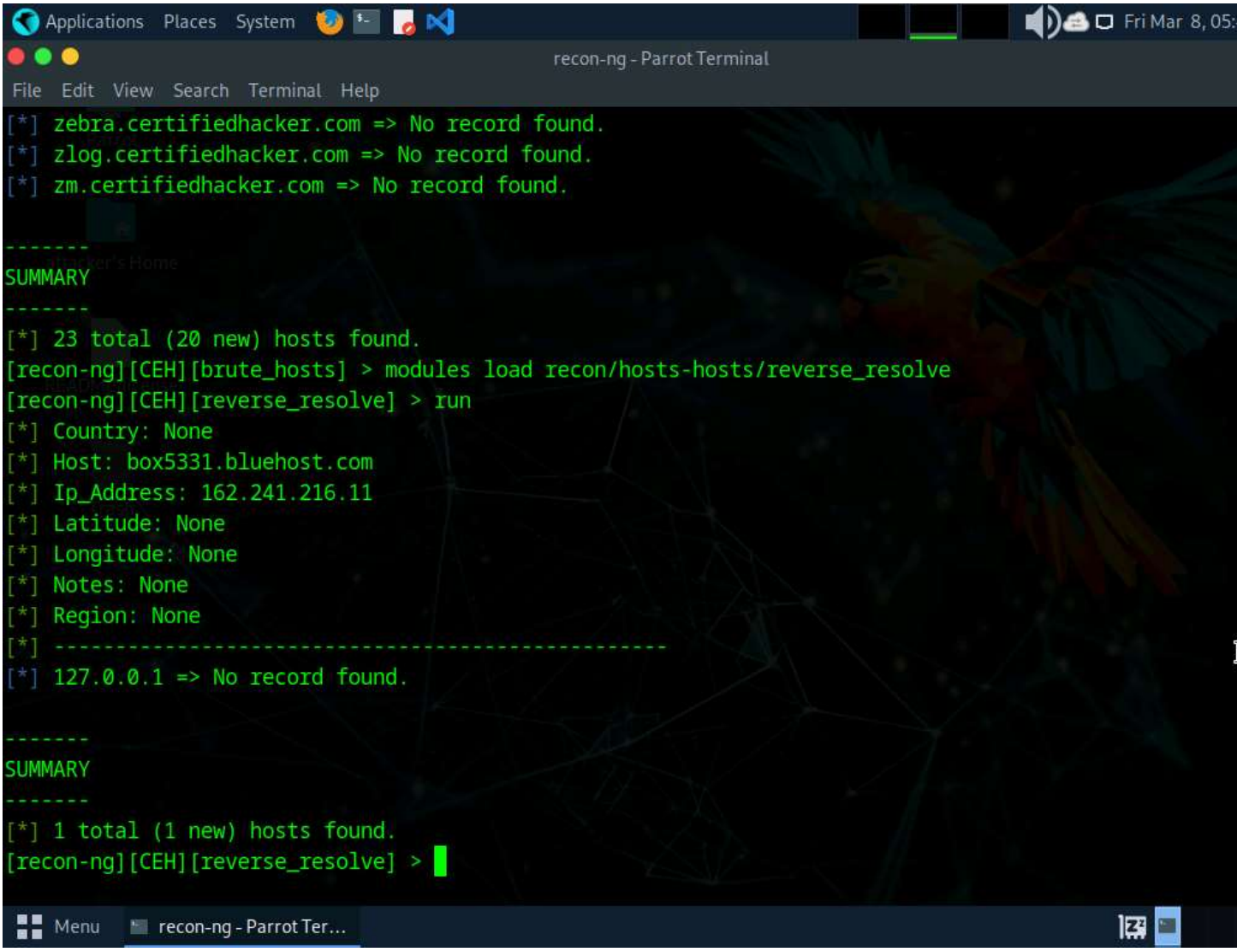
35. more...

36. To resolve hosts using the Bing module, use the following commands:

    - **back**
    - **modules load recon/domains-hosts/bing_domain_web**
    - **run**

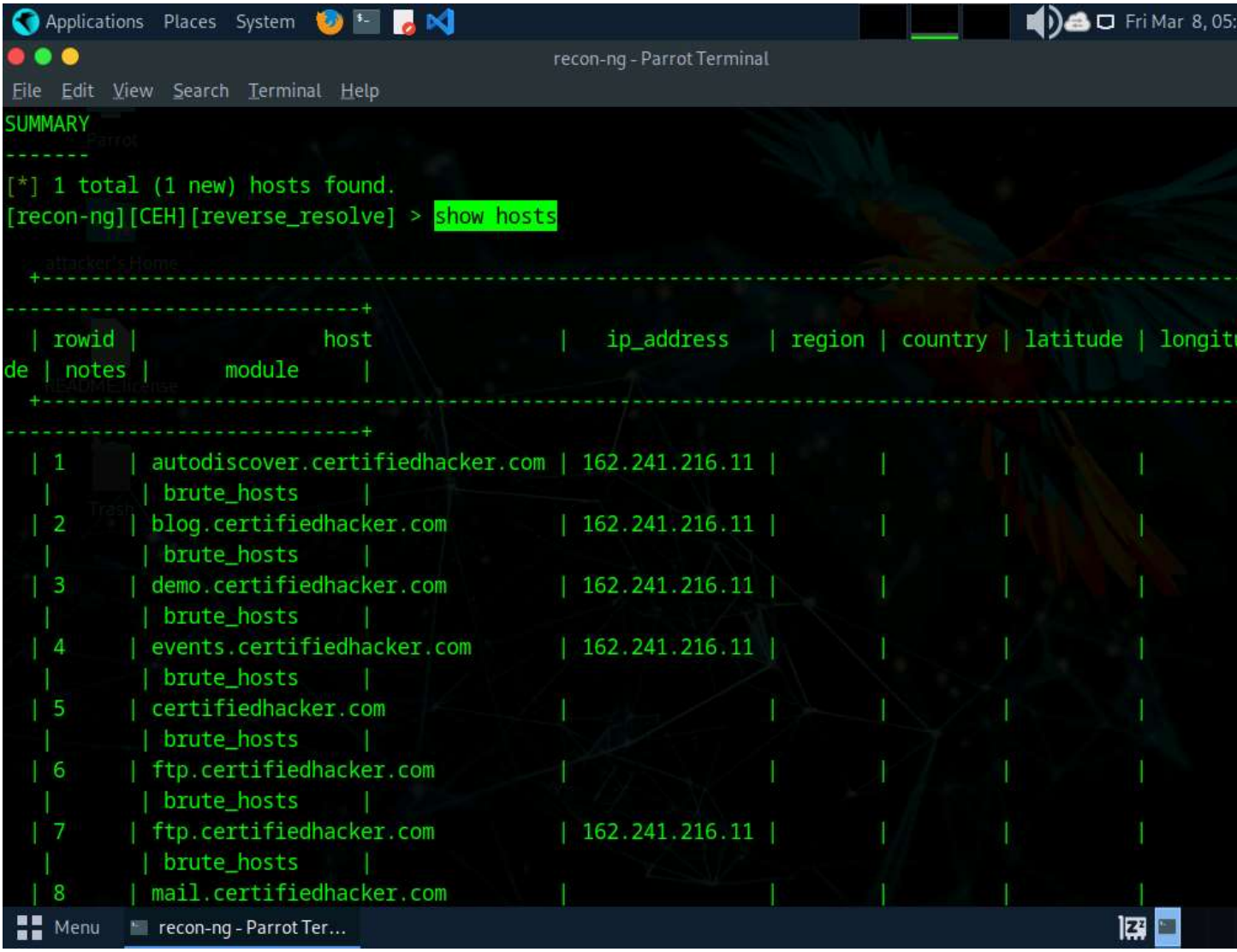
37. more...

38. Now, perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames.
39. Execute **modules load reverse_resolve** command to view all the modules associated with the reverse_resolve keyword. In this task, we will be using the **recon/hosts-hosts/reverse_resolve** module.
40. Run the **modules load recon/hosts-hosts/reverse_resolve** command to load the module.

41. Issue the **run** command to begin the reverse lookup.
42. 

43. Once done with the reverse lookup process, run the **show hosts** command. This displays all the hosts that are harvested so far, as shown in the screenshot.

44.

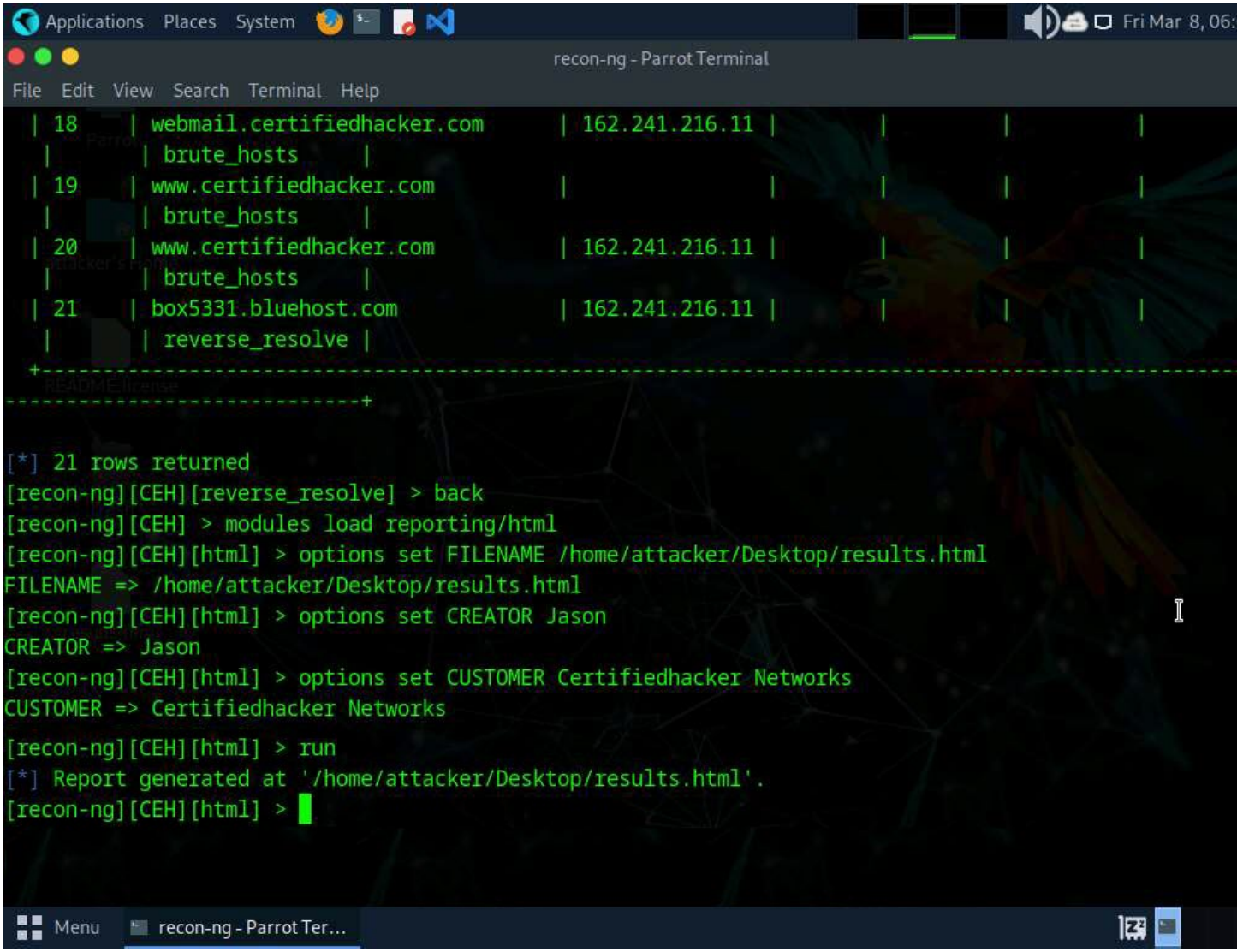


45. Now, use the **back** command to go back to the CEH attributes terminal.
46. Now, that you have harvested several hosts, we will prepare a report containing all the hosts.
47. Execute **modules load reporting** command to view all the modules associated with the reporting keyword. In this lab, we will save the report in HTML format. So, the module used is **reporting/html**.
48. Run the **modules load reporting/html** command.
49. Observe that you need to assign values for **CREATOR** and **CUSTOMER** options while the **FILENAME** value is already set, and you may change the value if required. To do so, run the below commands:

    - **options set FILENAME /home/attacker/Desktop/results.html**. By issuing this command, you are setting the report name as **results.html** and the path to store the file as **Desktop**.
    - **options set CREATOR [your name]** (here, **Jason**).
    - **options set CUSTOMER Certifiedhacker Networks** (since you have performed network reconnaissance on **certifiedhacker.com** domain).

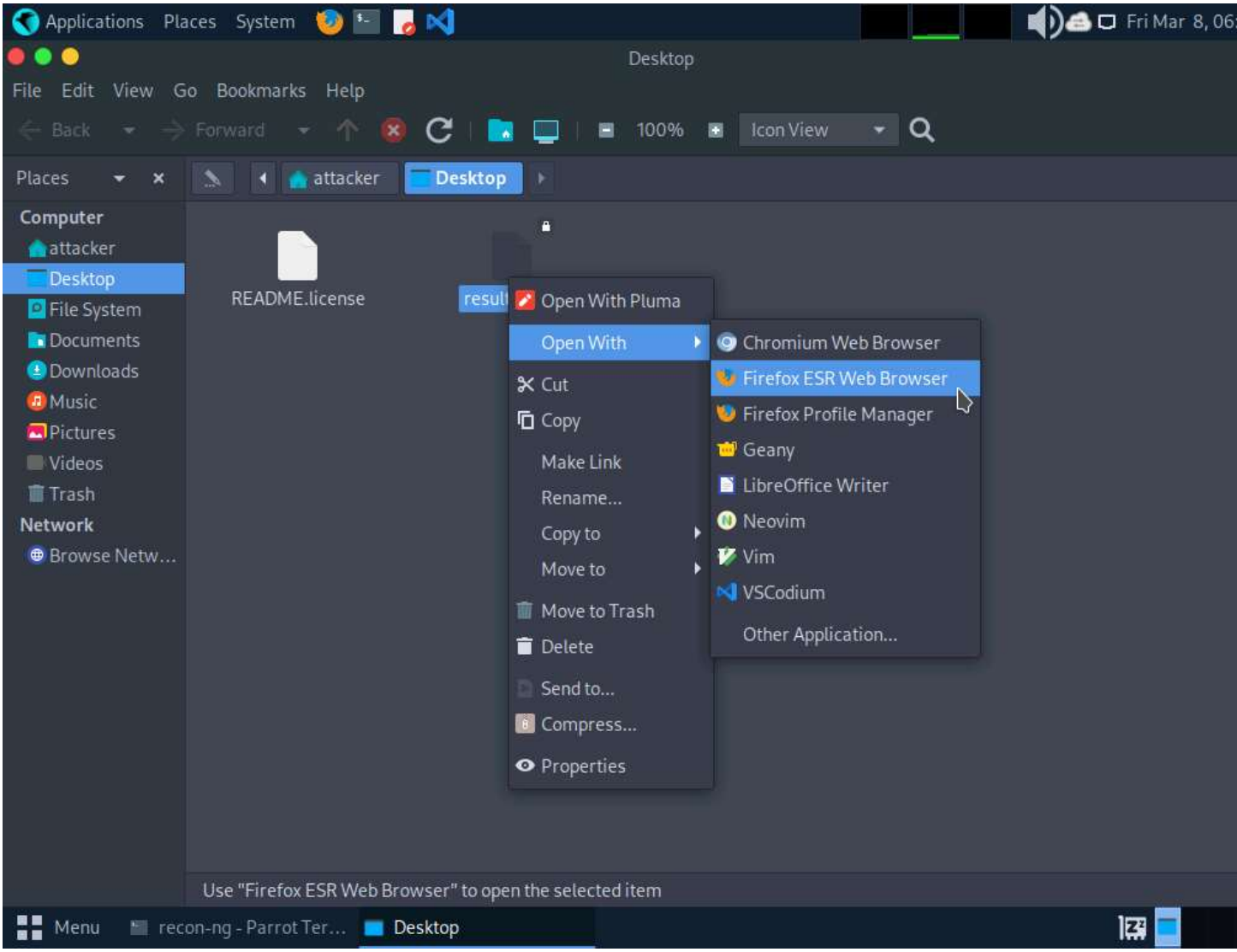
50. Use the **run** command and press **Enter** to create a report for all the hosts that have been harvested.

51.



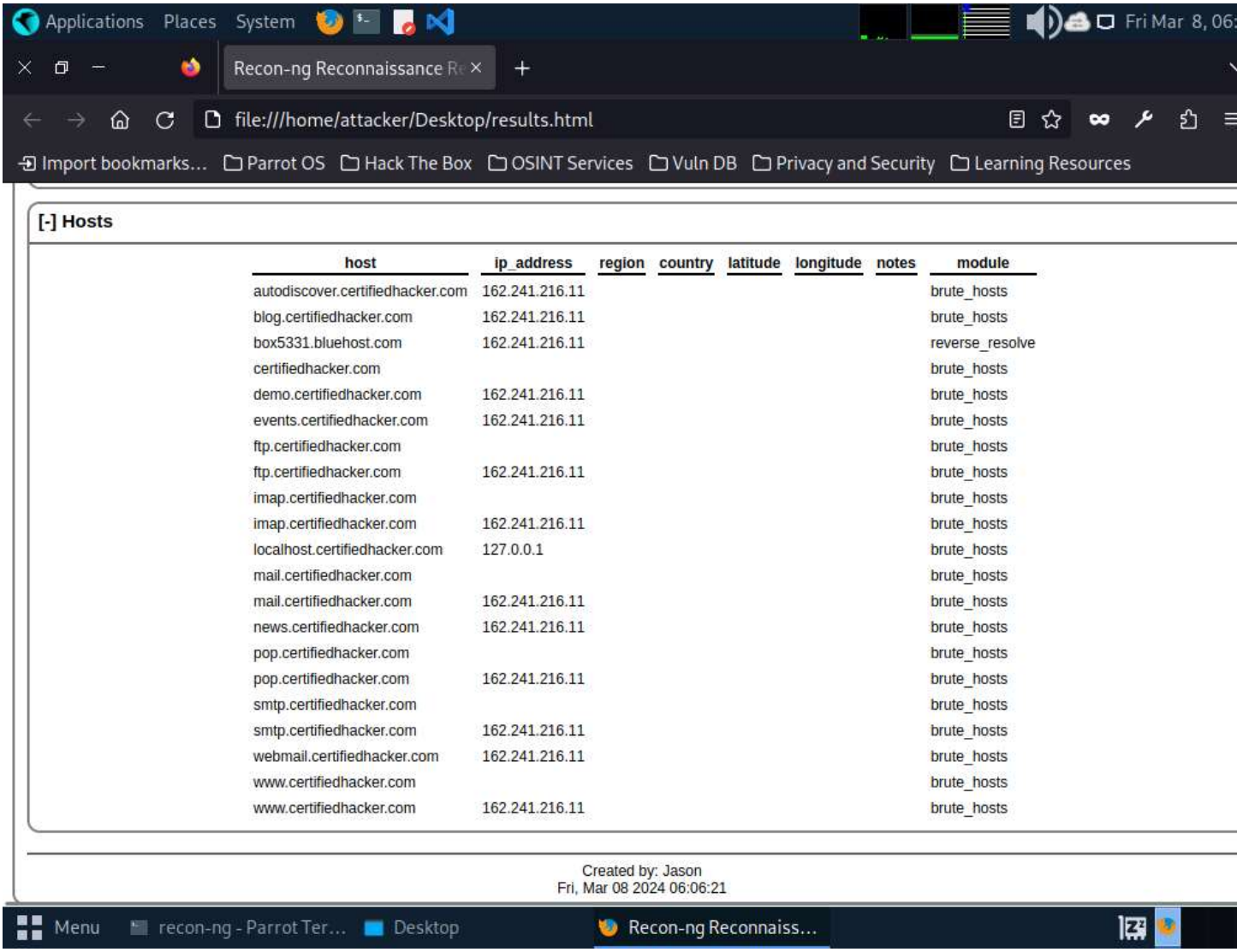
52. The generated report is saved to **/home/attacker/Desktop/**.
53. Navigate to **/home/attacker/Desktop/**, right-click on the **results.html** file, click on **Open With**, and select the **Firefox ESR Web Browser** browser from the available options.

54.



55. The generated report appears in the **Firefox** browser, displaying the summary of the harvested hosts.
56. You can expand the **Hosts** node to view all the harvested hosts, as shown in the screenshot.

57.

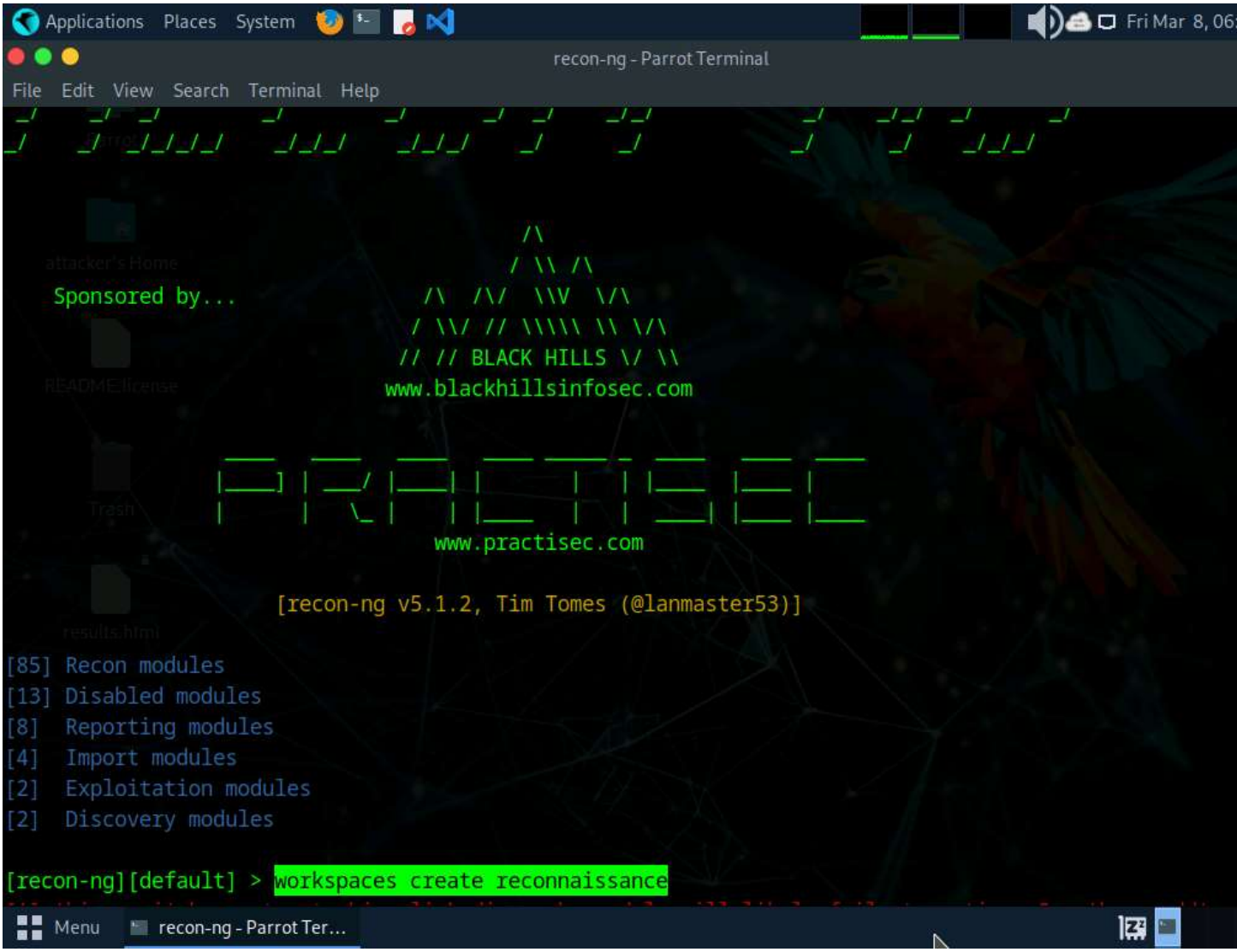


58. Close all open windows.
59. Until now, we have used the Recon-ng tool to perform network reconnaissance on a target domain
60. Now, we will use Recon-ng to gather personnel information.
61. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

62. The password that you type will not be visible.

63. Run **cd** command to jump to the root directory and run **recon-ng** command.
64. Add a workspace by issuing the command **workspaces create reconnaissance** and press **Enter**. This creates a workspace named reconnaissance.

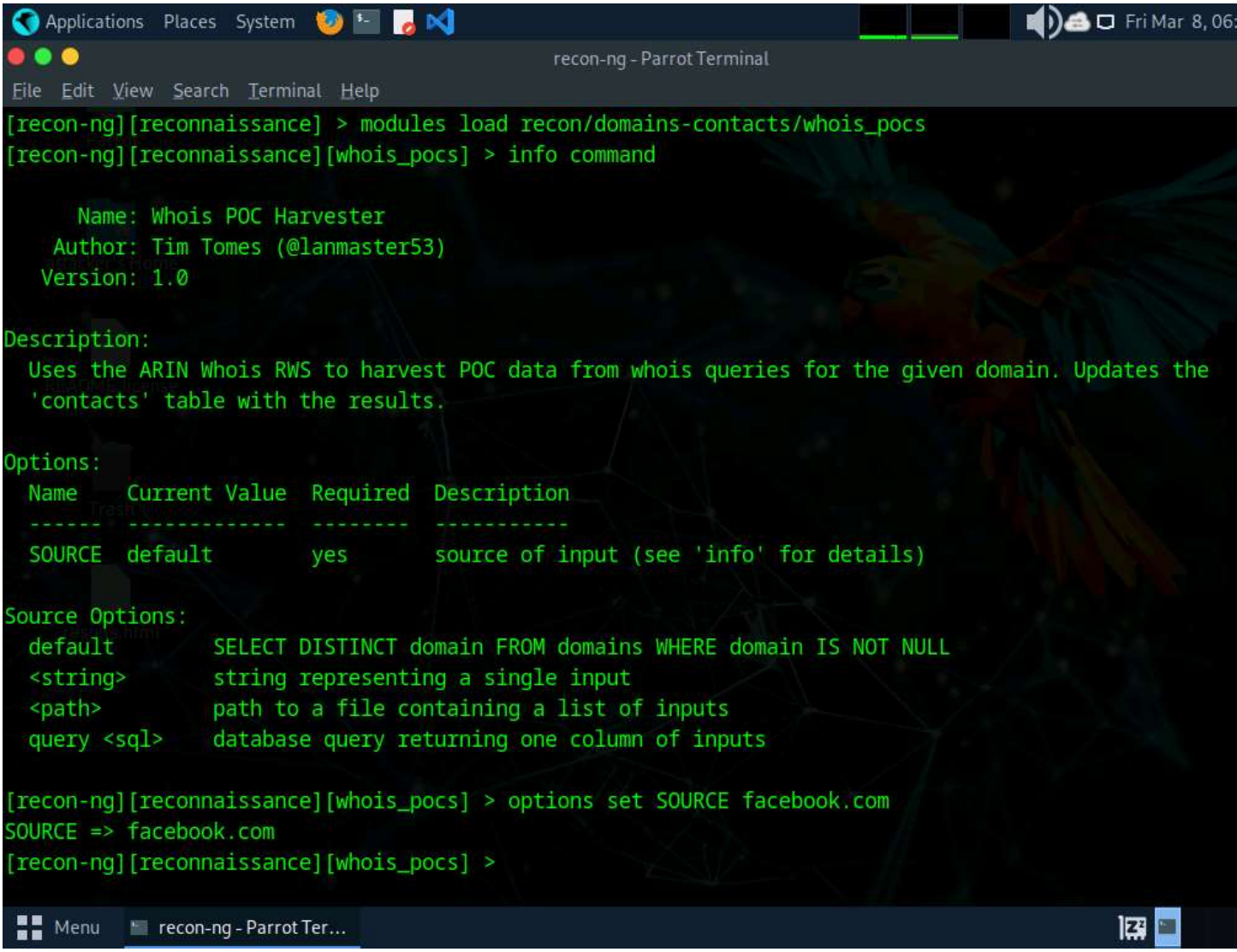
65.



66. Set a domain and perform footprinting on it to extract contacts available in the domain.
67. Execute **modules load recon/domains-contacts/whois_pocs** command. This module uses the ARIN Whois RWS to harvest POC data from Whois queries for the given domain.
68. Run the **info command** command to view the options required to run this module.
69. Run **options set SOURCE facebook.com** command to add facebook.com as a target domain.

70. Here, we are using facebook.com as a target domain to gather contact details.

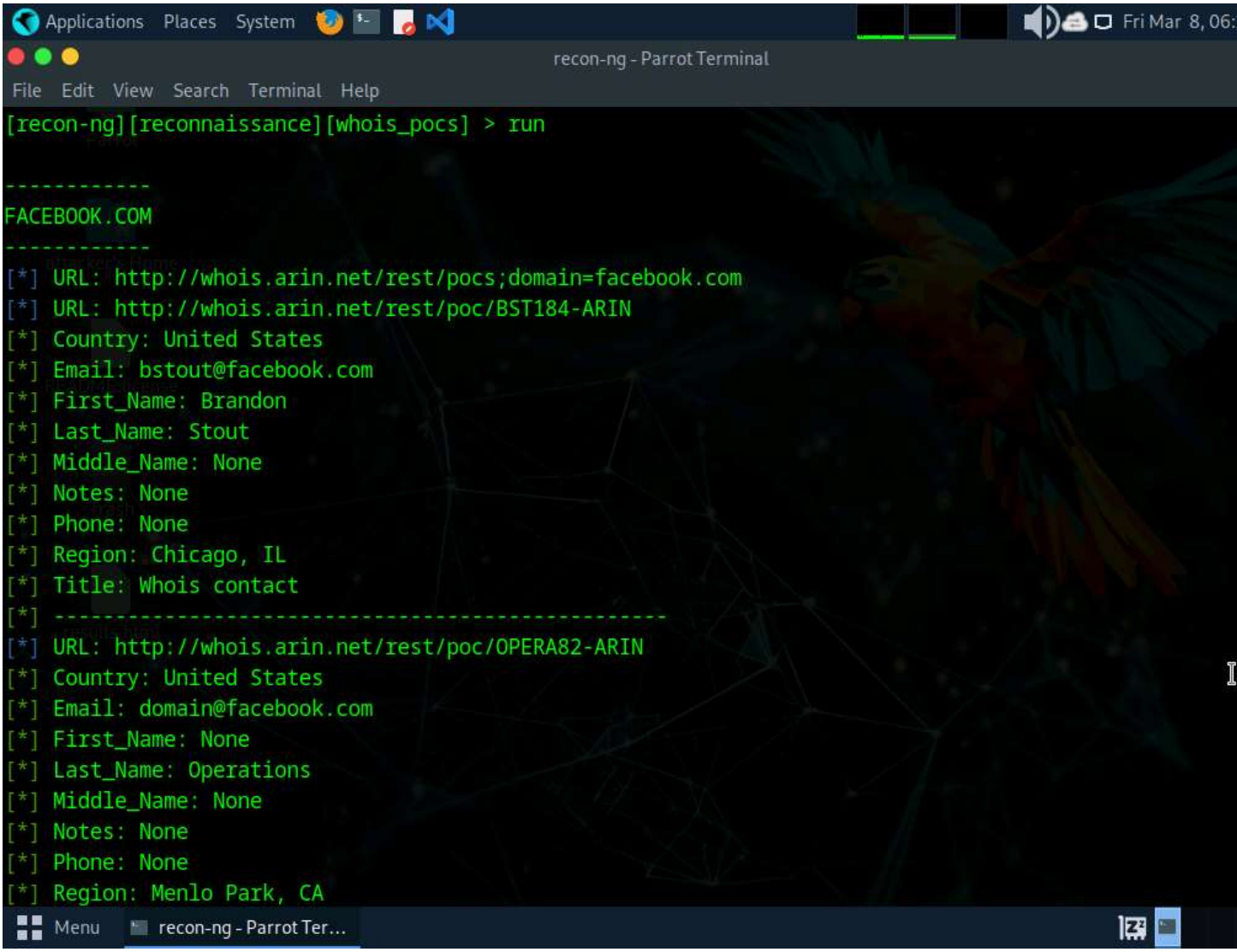
71.



72. Execute the **run** command. The **recon/domains-contacts/whois_pocs** module extracts the contacts associated with the domain and displays them, as shown in the screenshot

73. Results might differ when you perform the lab.

74.

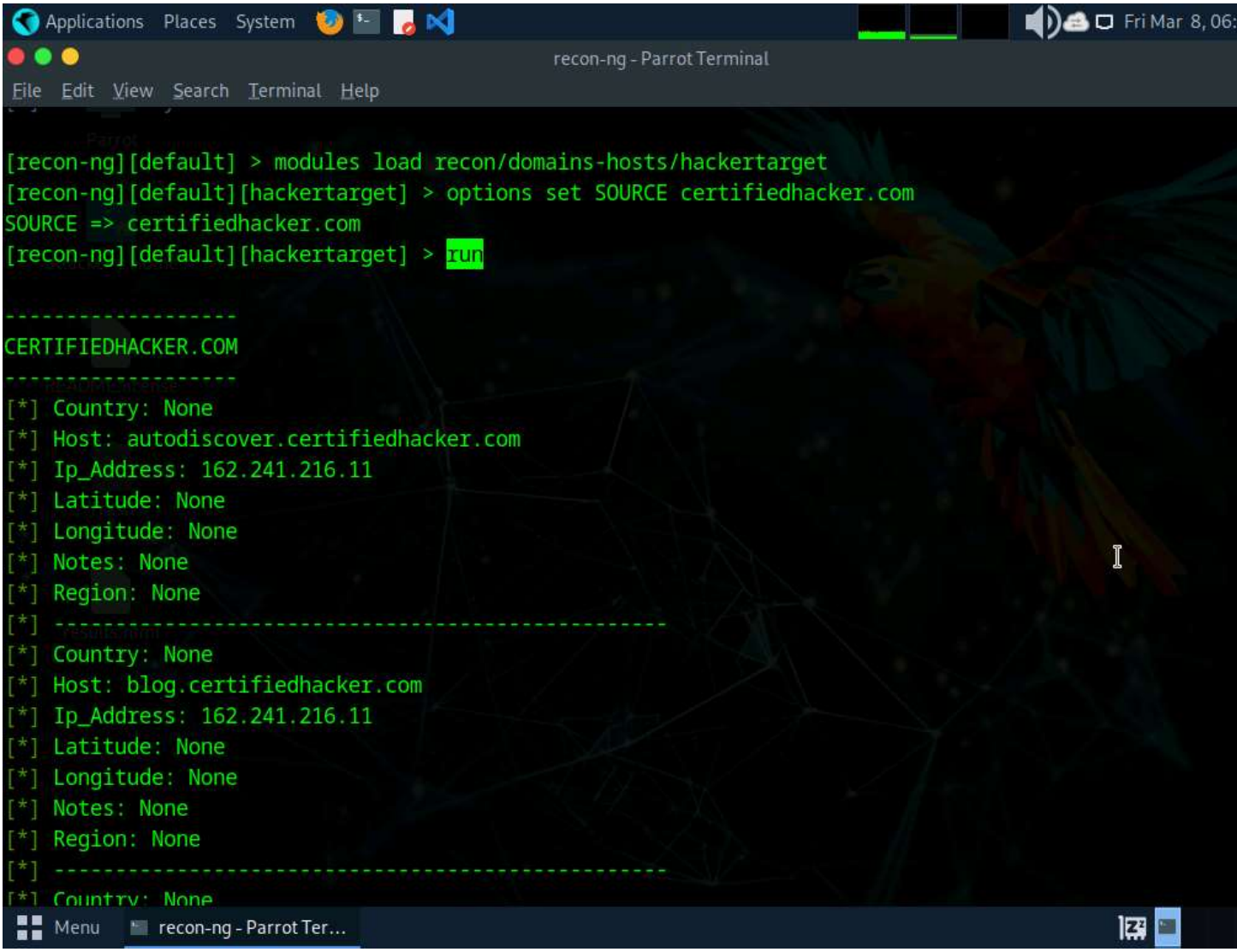


75. Until now, we have obtained contacts related to the domains. Note down these contacts' names. Close all the open windows.
76. Now, we will use Recon-ng to extract a list of subdomains and IP addresses associated with the target URL.
77. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

78. The password that you type will not be visible.

79. Now, run **cd** command to jump to the root directory and run **recon-ng** command.
80. To extract a list of subdomains and IP addresses associated with the target URL, we need to load the **recon/domains-hosts/hackertarget** module.
81. Run the **modules load recon/domains-hosts/hackertarget** command and run **options set SOURCE certifiedhacker.com** command.
82. Execute the **run** command. The **recon/domains-hosts/hackertarget** module searches for list of subdomains and IP addresses associated with the target URL and returns the list of subdomains and their IP addresses.

83.



84. This concludes the demonstration of gathering host information of the target domain and gathering personnel information of a target organization.
85. Close all open windows and document all the acquired information.

Question 2.8.1.1

Use the Recon-ng tool to gather personnel information. Enter the Recon-ng module name that extracts the contacts associated with the domain and displays them.

Score

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

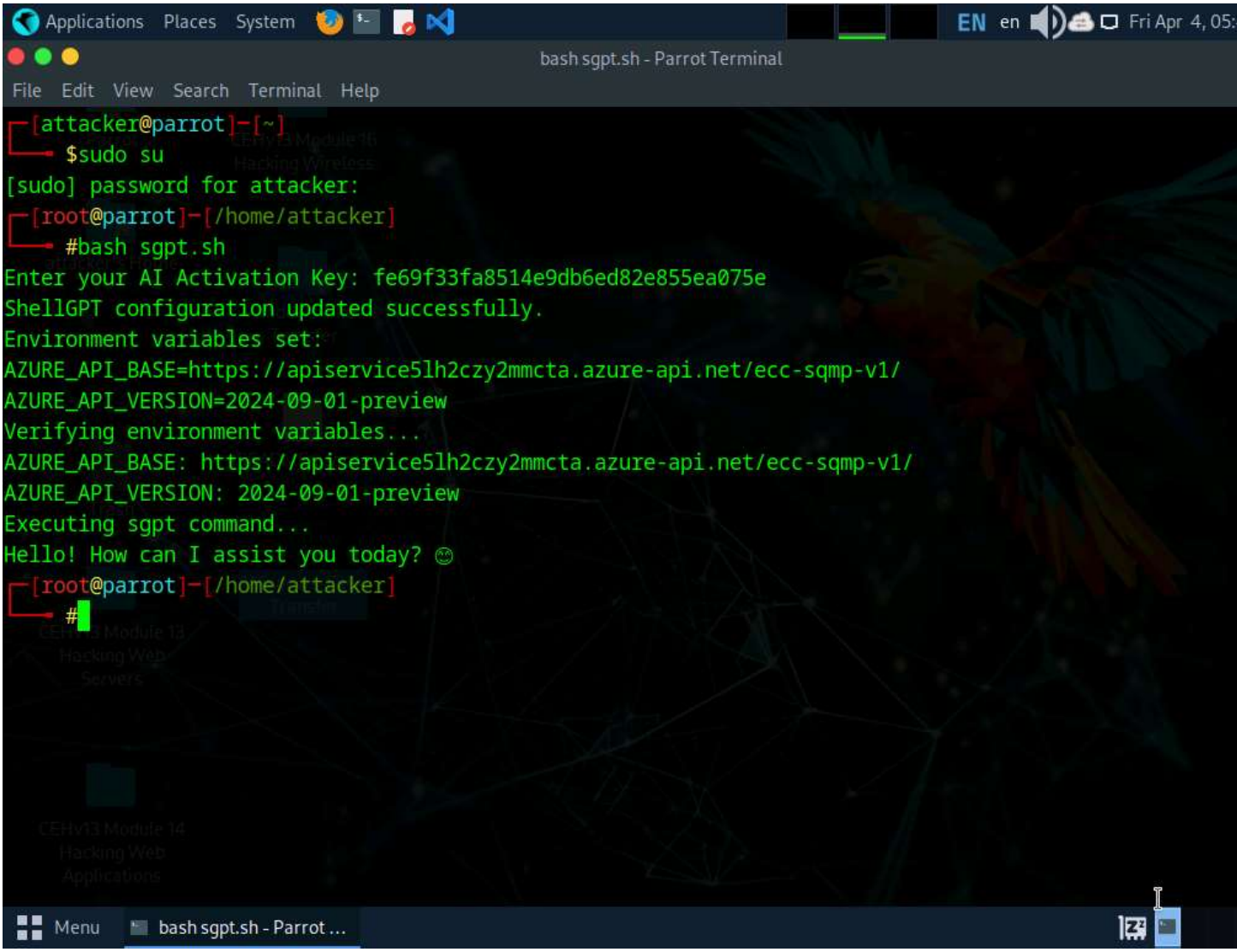
Footprinting with ShellGPT involves leveraging shell scripting capabilities along with GPT's language processing prowess. By crafting tailored scripts, ShellGPT automates data gathering from various sources, including WHOIS databases and online forums. It parses and extracts relevant information such 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. Click Parrot Security to switch to Parrot machine, and login with **attacker/toor**. Open a Terminal window and execute **sudo su** to run the program as a root user (When prompted, enter the password **toor**).
2. The password that you type will not be visible.
3. Run **bash sgpt.sh** command to configure ShellGPT and the AI activation key.
4. You can follow the **Instructions to Download your AI Activation Key** in **Module 00: CEH Lab Setup** to obtain the AI activation key. Alternatively, follow the instructions available in the file, Instructions to Download your AI_Activation_Key.pdf

5.

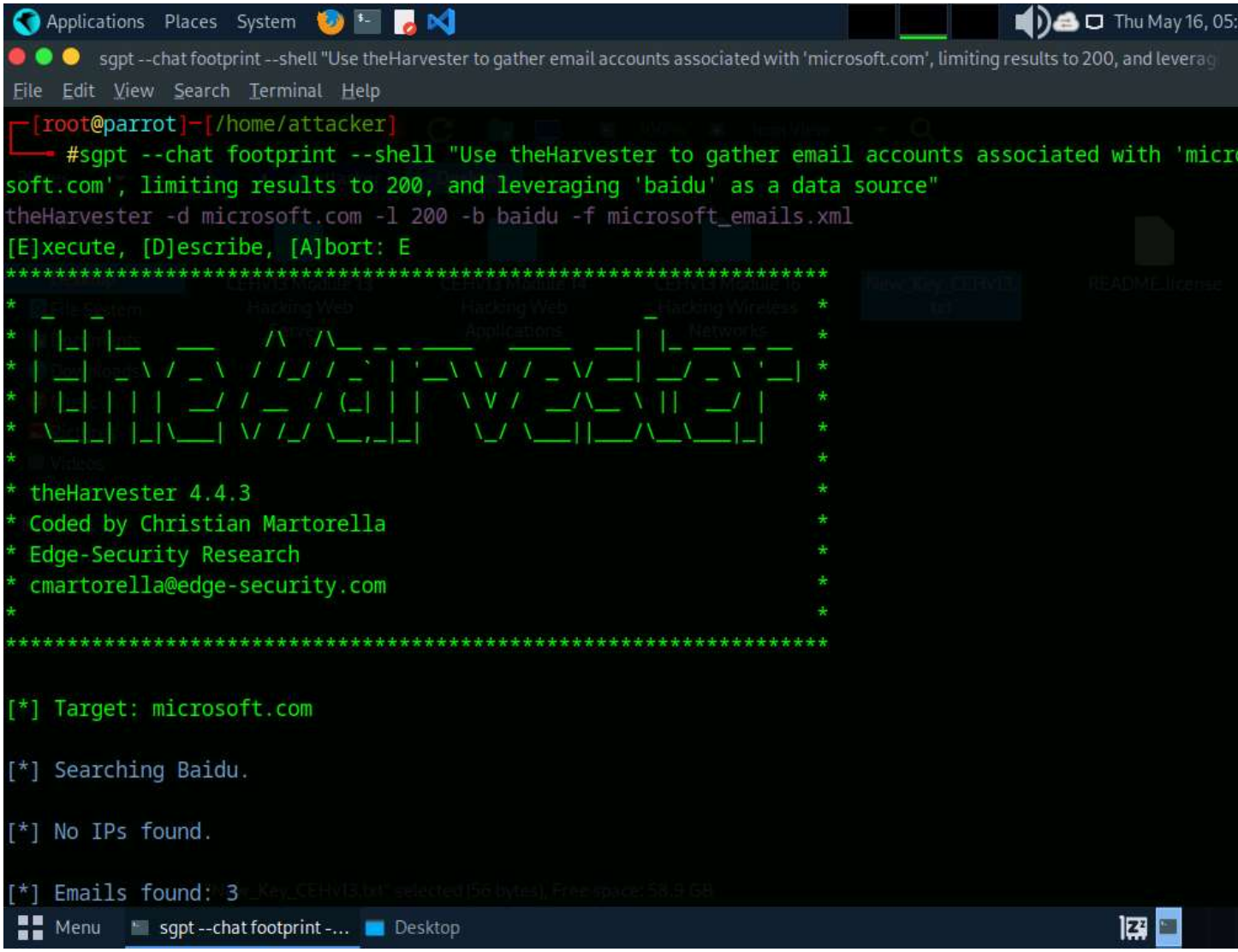


6. After configuring the ShellGPT in **Parrot Security** machine, we will use ShellGPT for harvesting emails pertaining to a target organization. To do so, run **sgpt --chat footprint --shell "Use theHarvester to gather email accounts associated with 'microsoft.com', limiting results to 200, and leveraging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

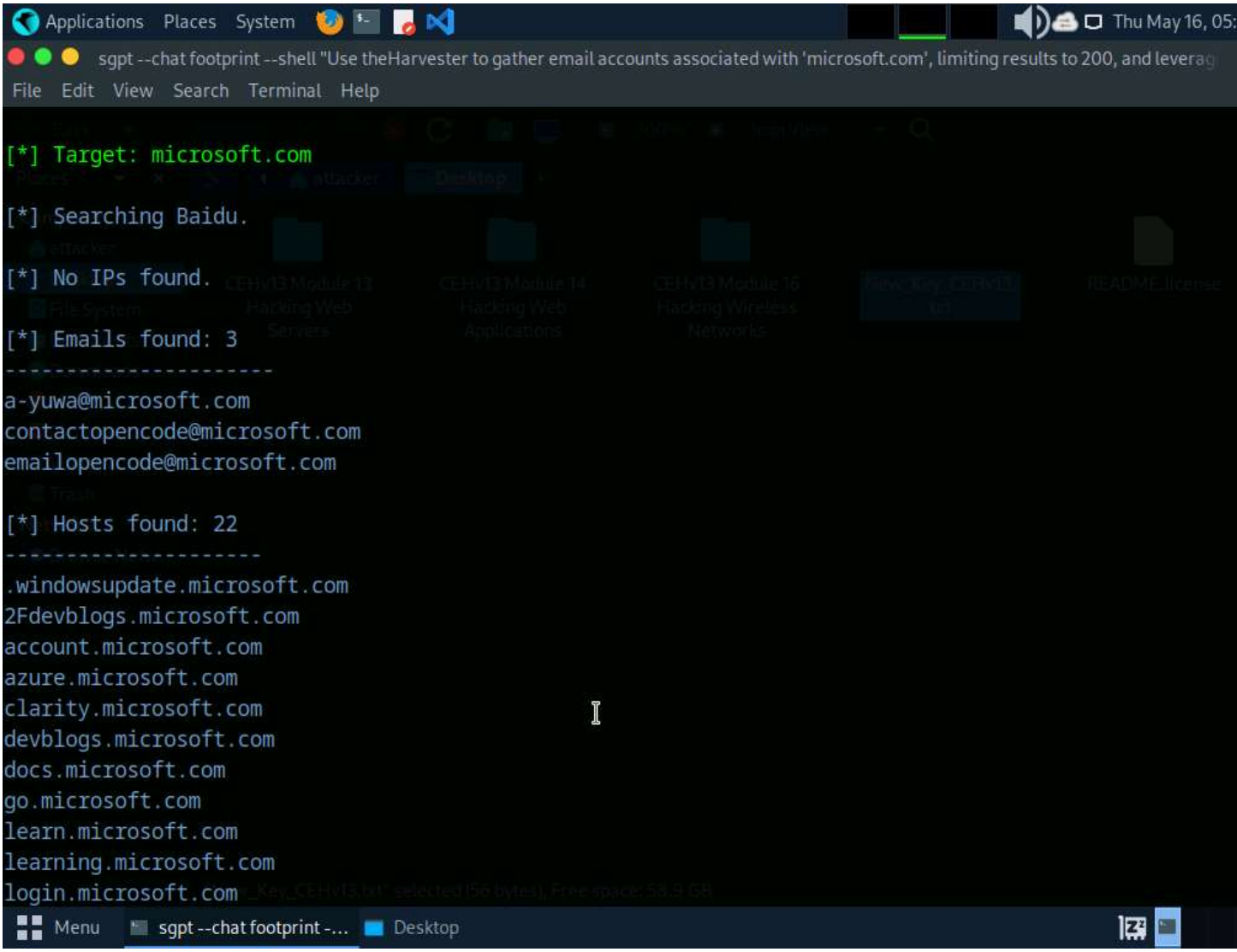
7. In the prompt type **E** and press **Enter** to execute the command.

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

9.


Applications Places System
Thu May 16, 05:
sgpt --chat footprint --shell "Use theHarvester to gather email accounts associated with 'microsoft.com', limiting results to 200, and leverag
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#sgpt --chat footprint --shell "Use theHarvester to gather email accounts associated with 'micr
soft.com', limiting results to 200, and leveraging 'baidu' as a data source"
theHarvester -d microsoft.com -l 200 -b baidu -f microsoft_emails.xml
[E]xecute, [D]escribe, [A]bort: E
theHarvester 4.4.3
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com
[*] Target: microsoft.com
[*] Searching Baidu.
[*] No IPs found.
[*] Emails found: 3
Menu
sgpt --chat footprint -...
Desktop

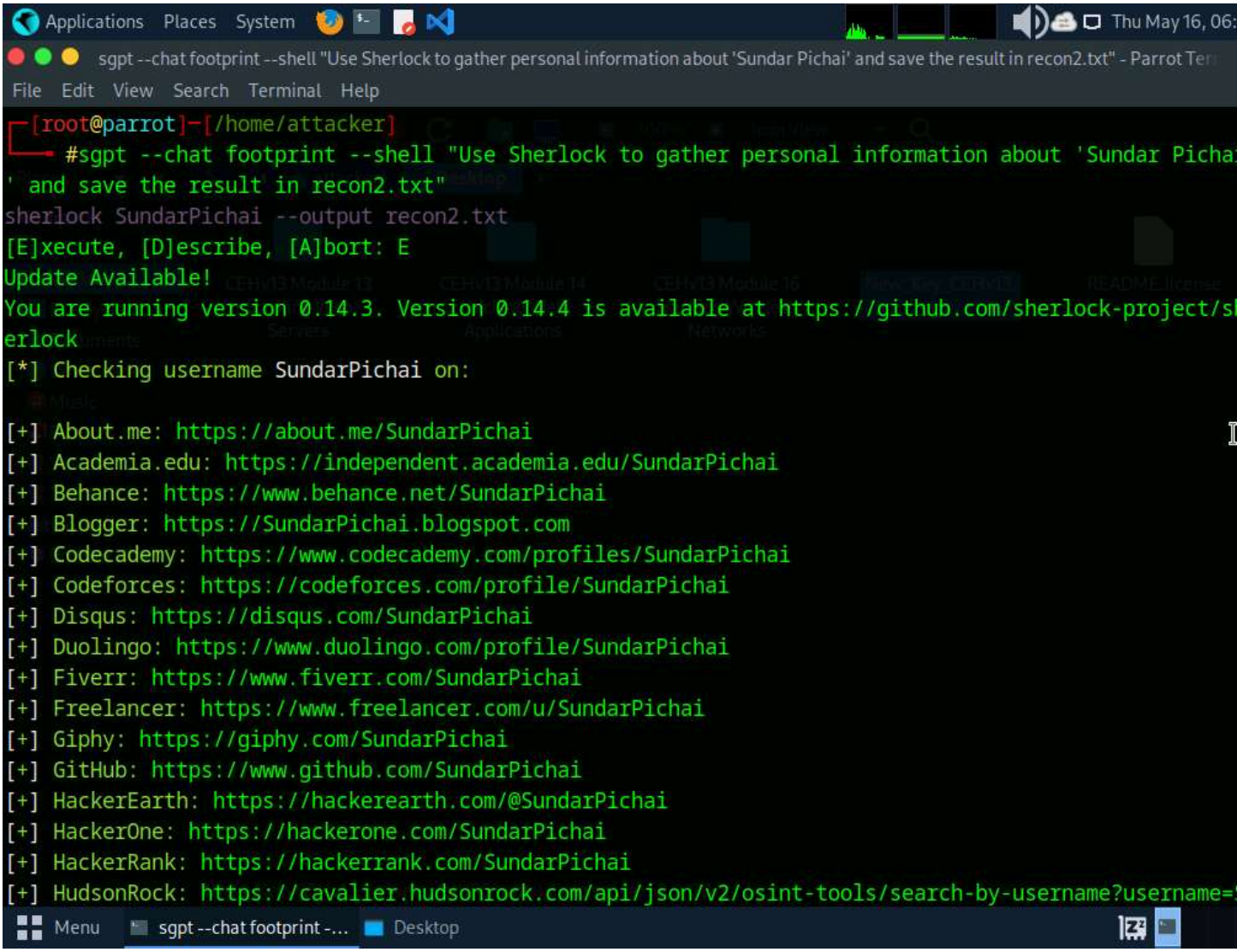
10.



11. 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.

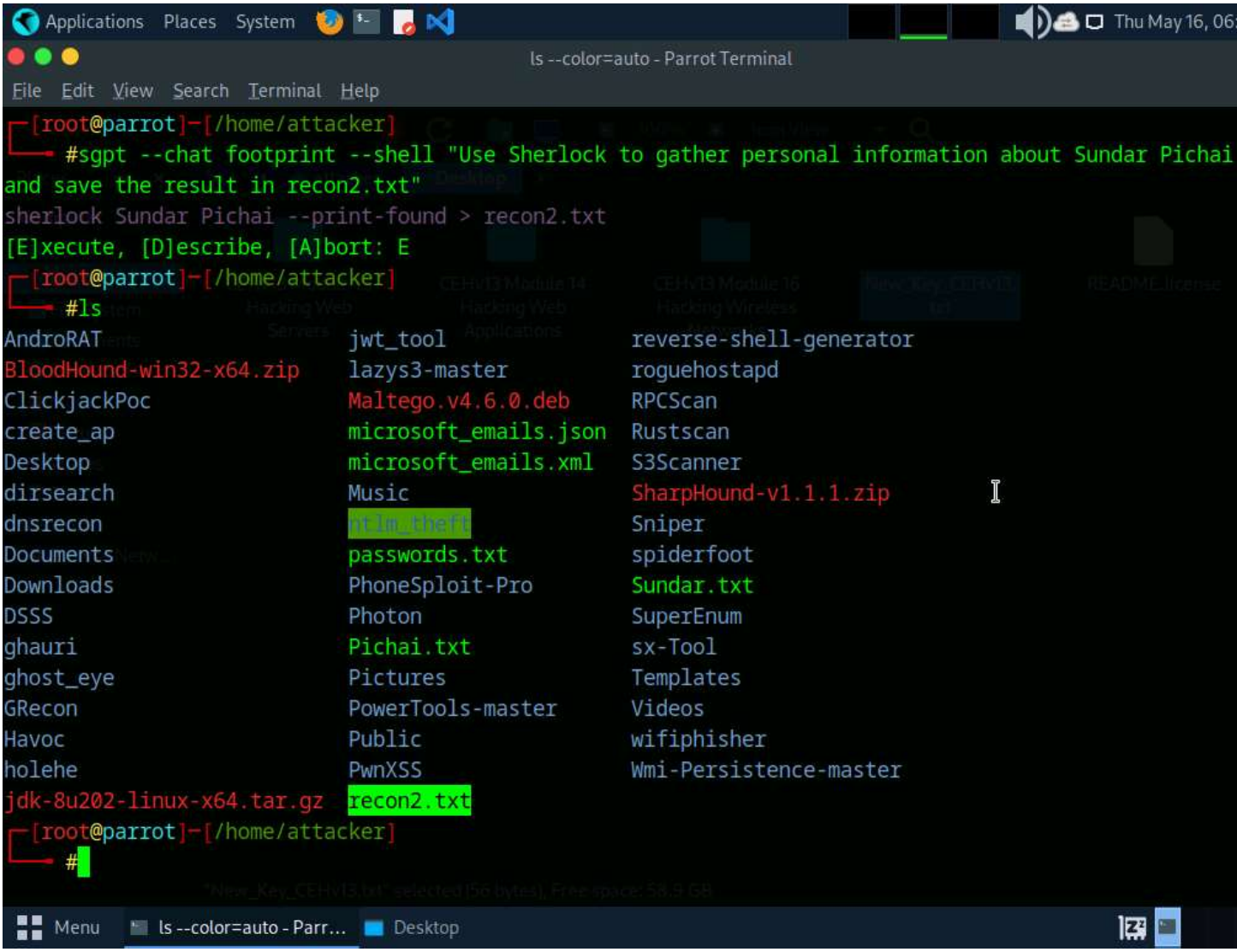
12. In the prompt type **E** and press **Enter** to execute the command.

13.

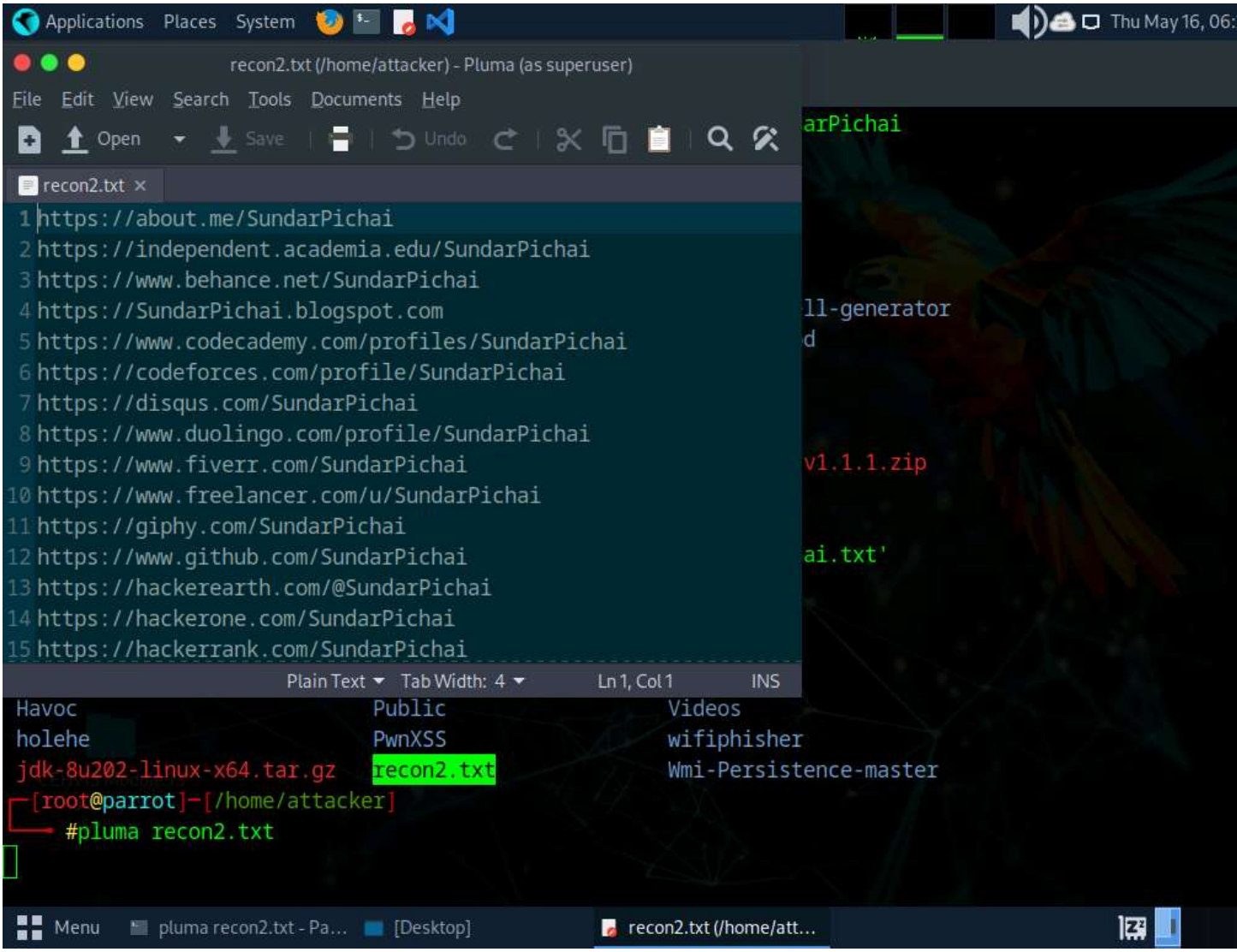


14. After the execution of the command, in the terminal run **ls** command to view the contents in the present working directory.

15.



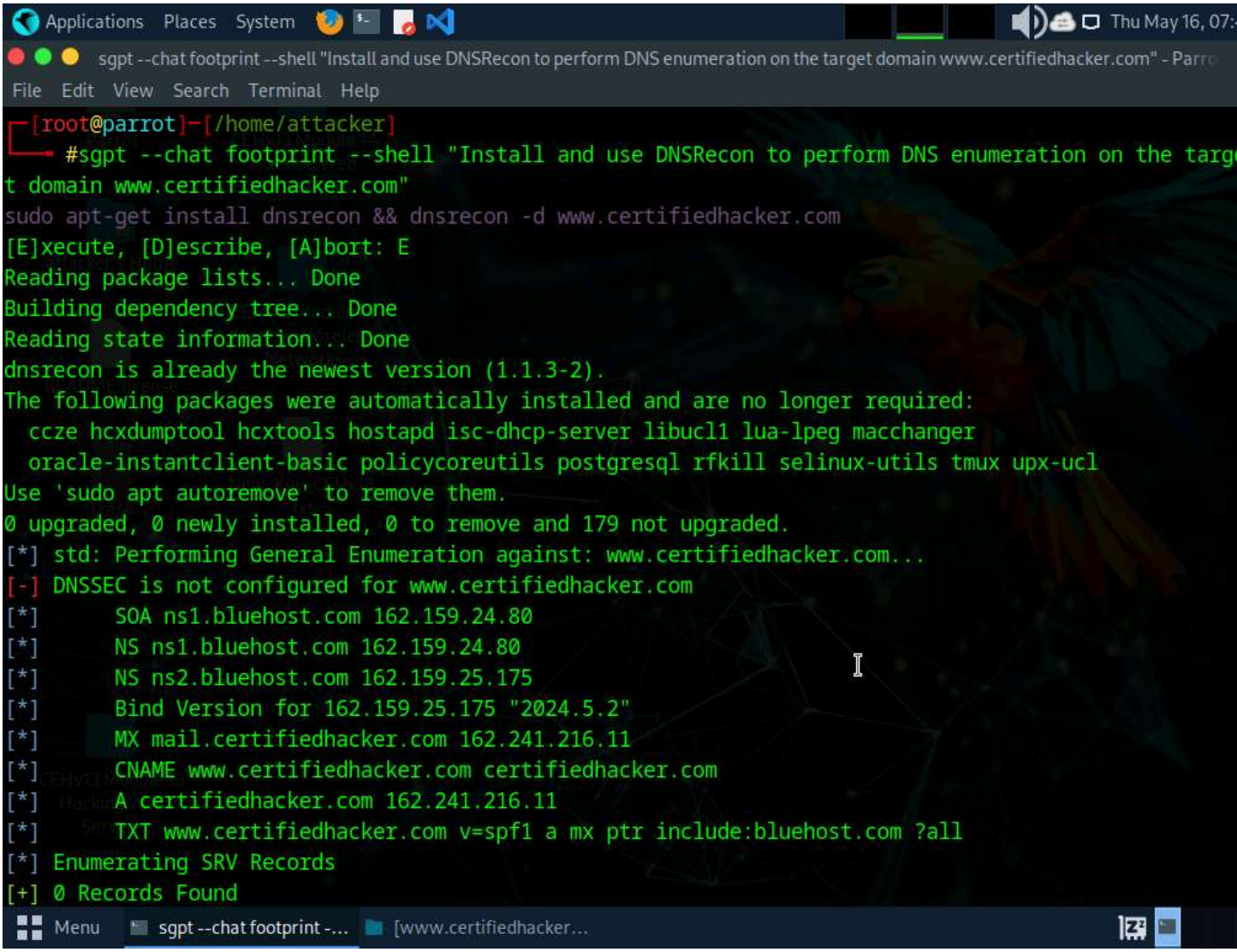
16. We can see that recon2.txt file is created by previous command. In the terminal window, run **pluma recon2.txt** command to view its contents. Close the text editor window.

17. 

ls
18. 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.

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

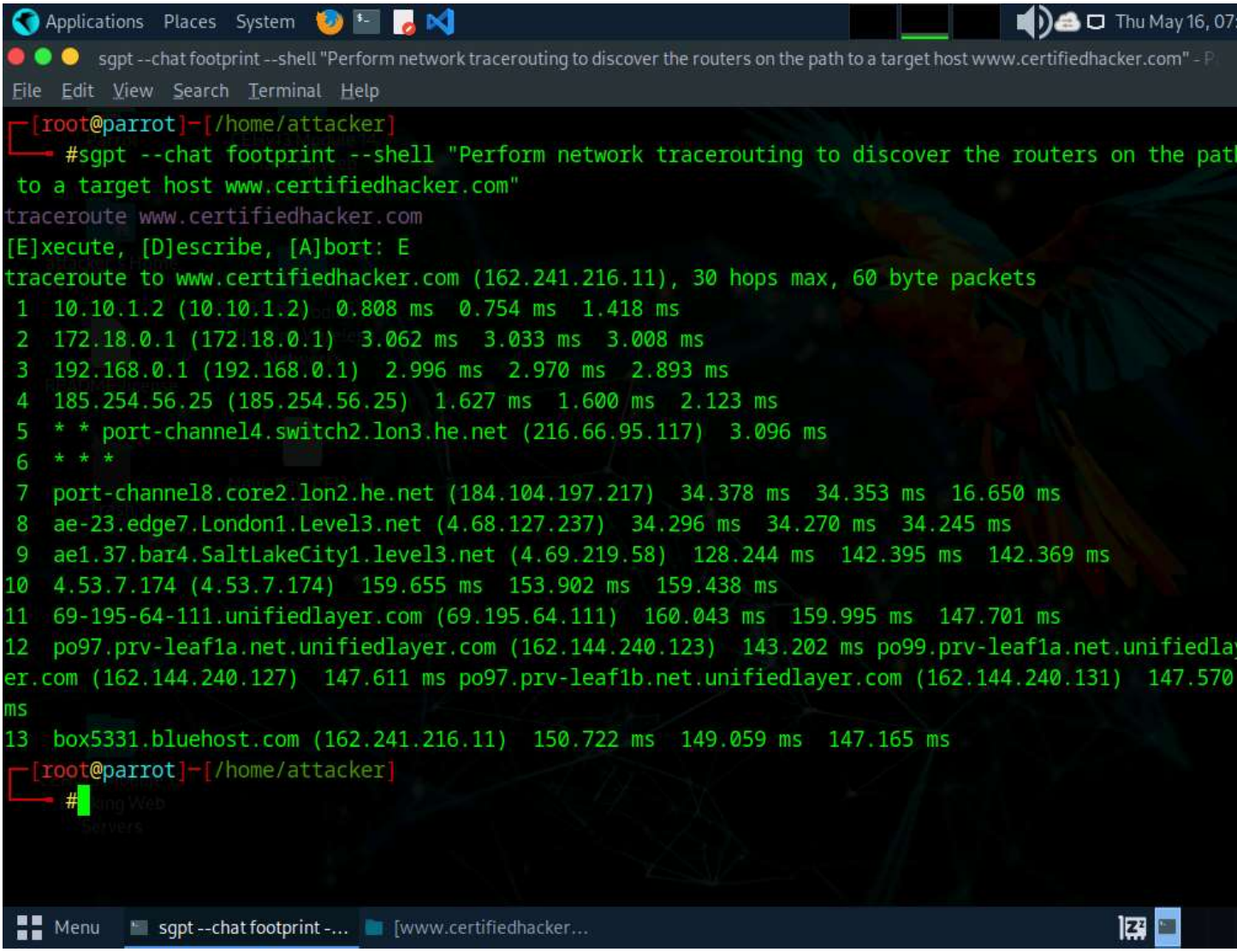
20.



21. 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.

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

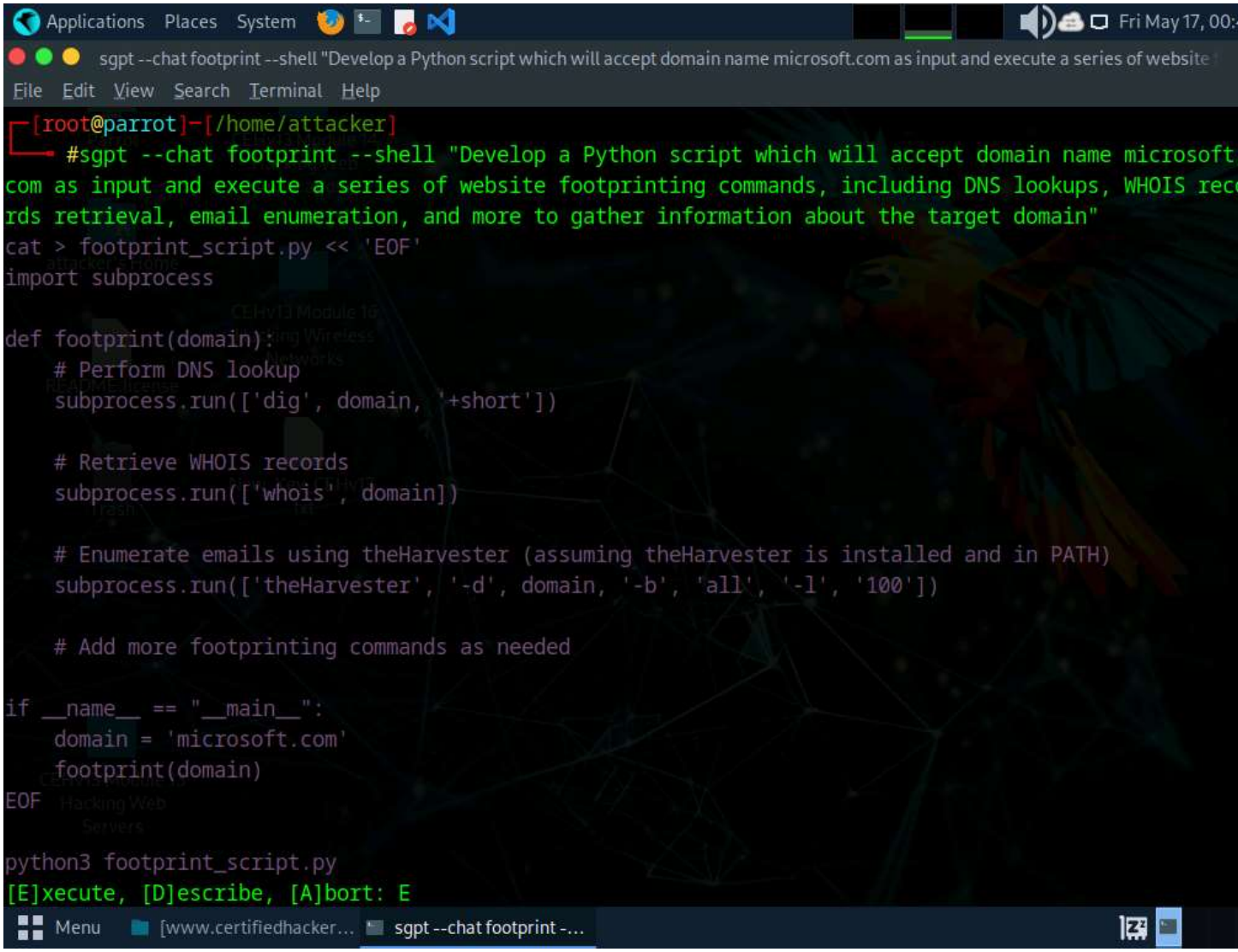
23.



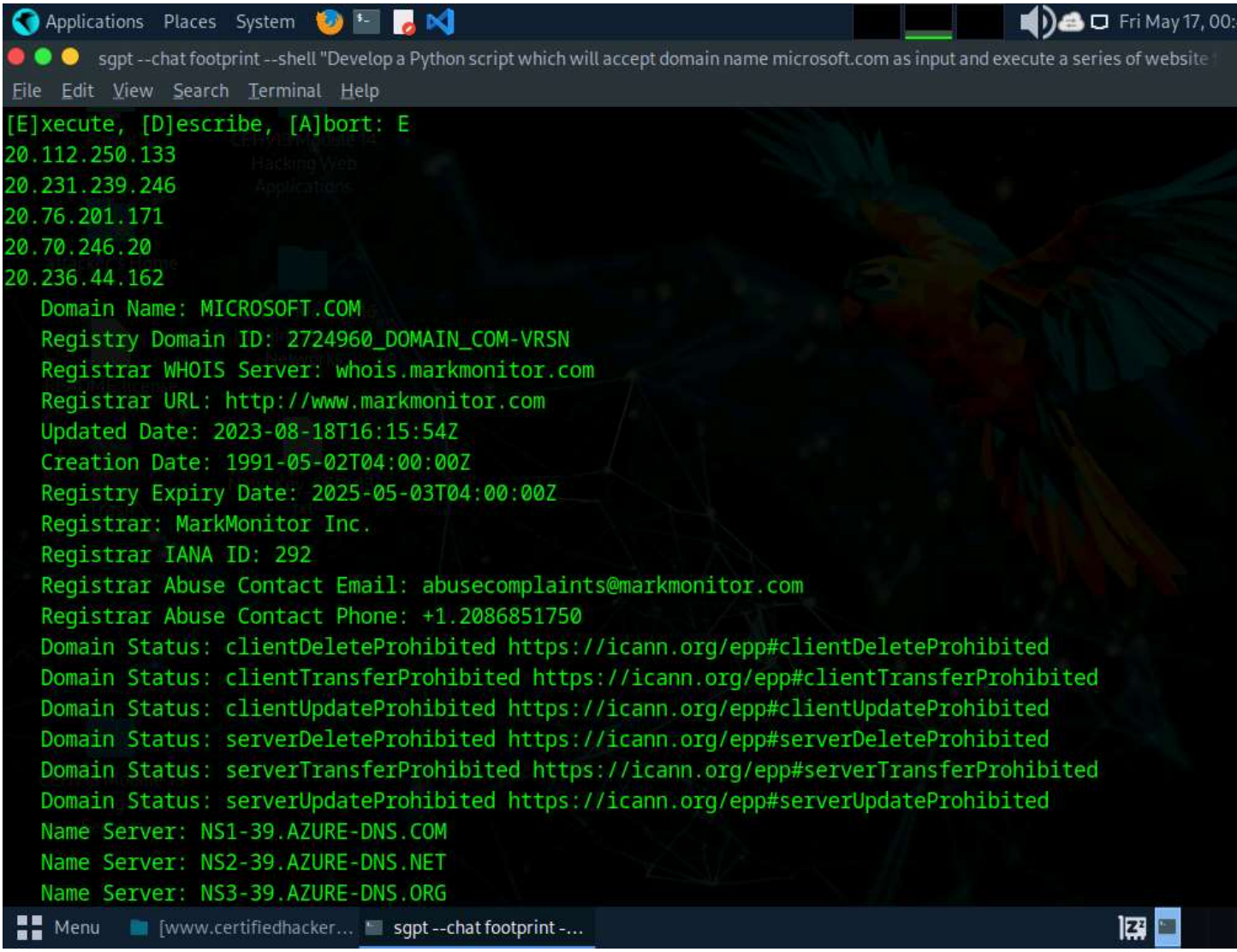
24. Now run **sgpt --chat footprint --shell "Develop a Python script which will accept domain name microsoft.com as input and execute a series of website footprinting commands, including DNS lookups, WHOIS records retrieval, email enumeration, and more to gather information about the target domain"**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

25. In the prompt type **E** and press **Enter** to execute the command.
26. It might take some time develop and run the script.

27.


Applications Places System
Fri May 17, 00:
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 rec
rds 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 -...

28.



29. 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.
30. This concludes the demonstration of performing footprinting using the ShellGPT.
31. Close all open windows and document all the acquired information.

Question 2.9.1.1

Using ShellGPT, write a prompt and execute it to perform DNS enumeration on www.certifiedhacker.com. Enter the IP address of NS ns2.bluehost.com.

Score

- Check this box to confirm completion of this module.

4

11 Minutes Remaining

Thumbnail screenshot of virtual machineLab52602828-Windows 11

Windows 11

To release mouse, press **Ctrl+Alt+Left Arrow**

Username	Admin[5]
Password	Pa$$w0rd[6]

DVD Drive

- No Media

Ctrl+Alt+Delete Open in New Window

Thumbnail screenshot of virtual machineLab52602828-Windows Server 2019

Windows Server 2019

To release mouse, press **Ctrl+Alt+Left Arrow**

Username	Administrator[7]
Password	Pa$$w0rd[8]

DVD Drive

- No Media

Ctrl+Alt+Delete Open in New Window

Thumbnail screenshot of virtual machineLab52602828-Parrot Security

Parrot Security

To release mouse, press **Ctrl+Alt+Left Arrow**

Username	Attacker[9]

Next: Lab 5: Perform DNS Footprinting
41/159 (25%) Tasks Complete
Type Text
Type Text
Type Text
Type Text
Type Text

Password toor[10]

DVD Drive

- No Media

Ctrl+Alt+Delete Open in New Window

Help

Support Information

ID	52602828
Host	EU-HV47
Datacenter	EU North (London)

FAQs

Frequently asked questions about the lab interface

Other Help Options

Submit a Support Request
Powered by Skillable•Review Us

Notifications

Settings

Text Size

100 Standard
150 Large Text
200 Extra Large Text

Color Mode

- Light
- Dark

Type Text

- High Contrast

Actions

Join Windows

Close Window
Close Window