

Module 2 Footprinting and Reconnaissance

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**.

Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 11** machine thumbnail in the **Resources** pane.

Alternatively, you can also click **Pa\$\$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane.

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

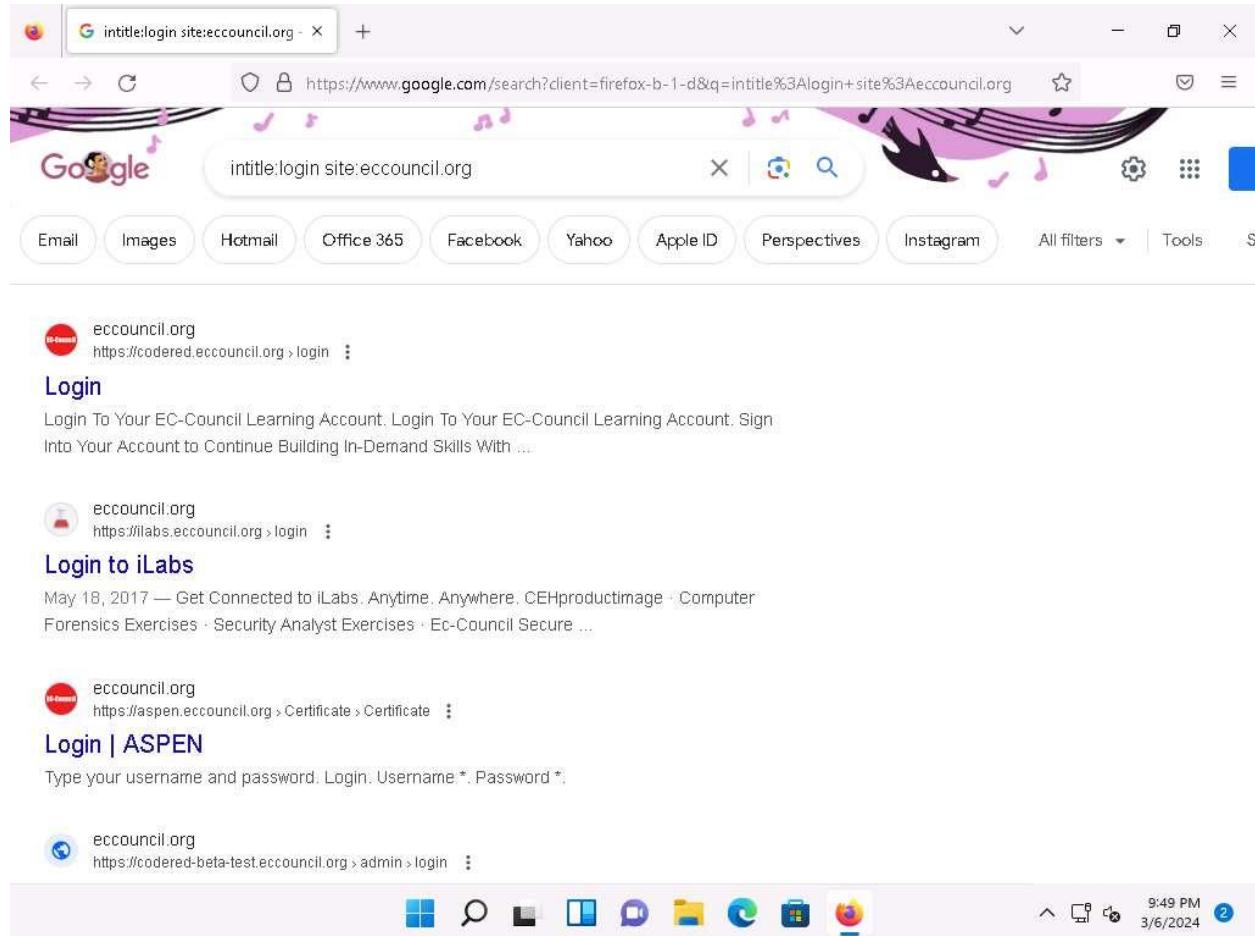
2. Launch any web browser, and go to <https://www.google.com> (here, we are using **Mozilla Firefox**).

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

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

3. 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.

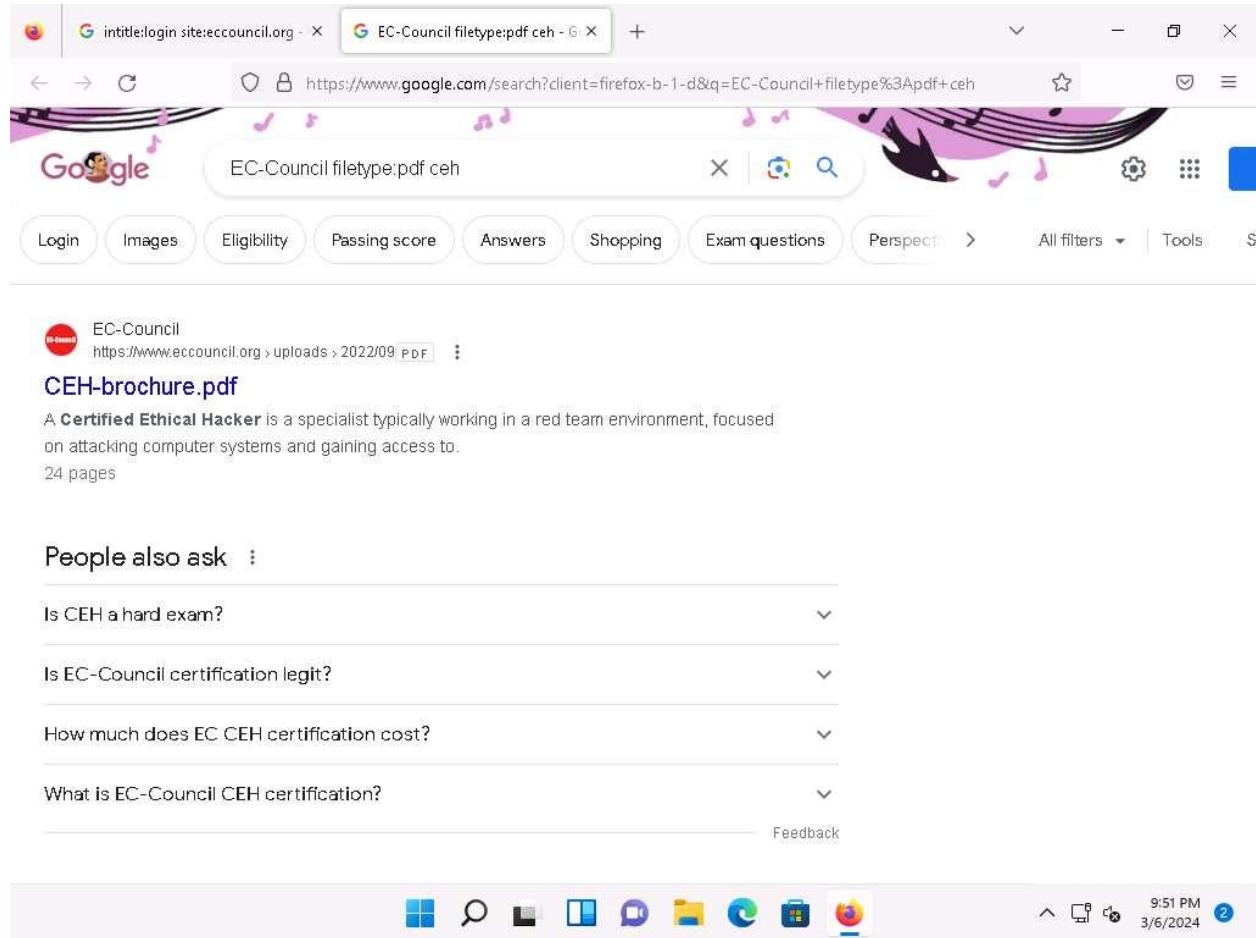
Here, this Advanced Google Search operator can help attackers and pen testers to extract login pages of the target organization's website. Attackers can subject login pages to various attacks such as credential bruteforcing, injection attacks and other web application attacks. Similarly, assessing the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



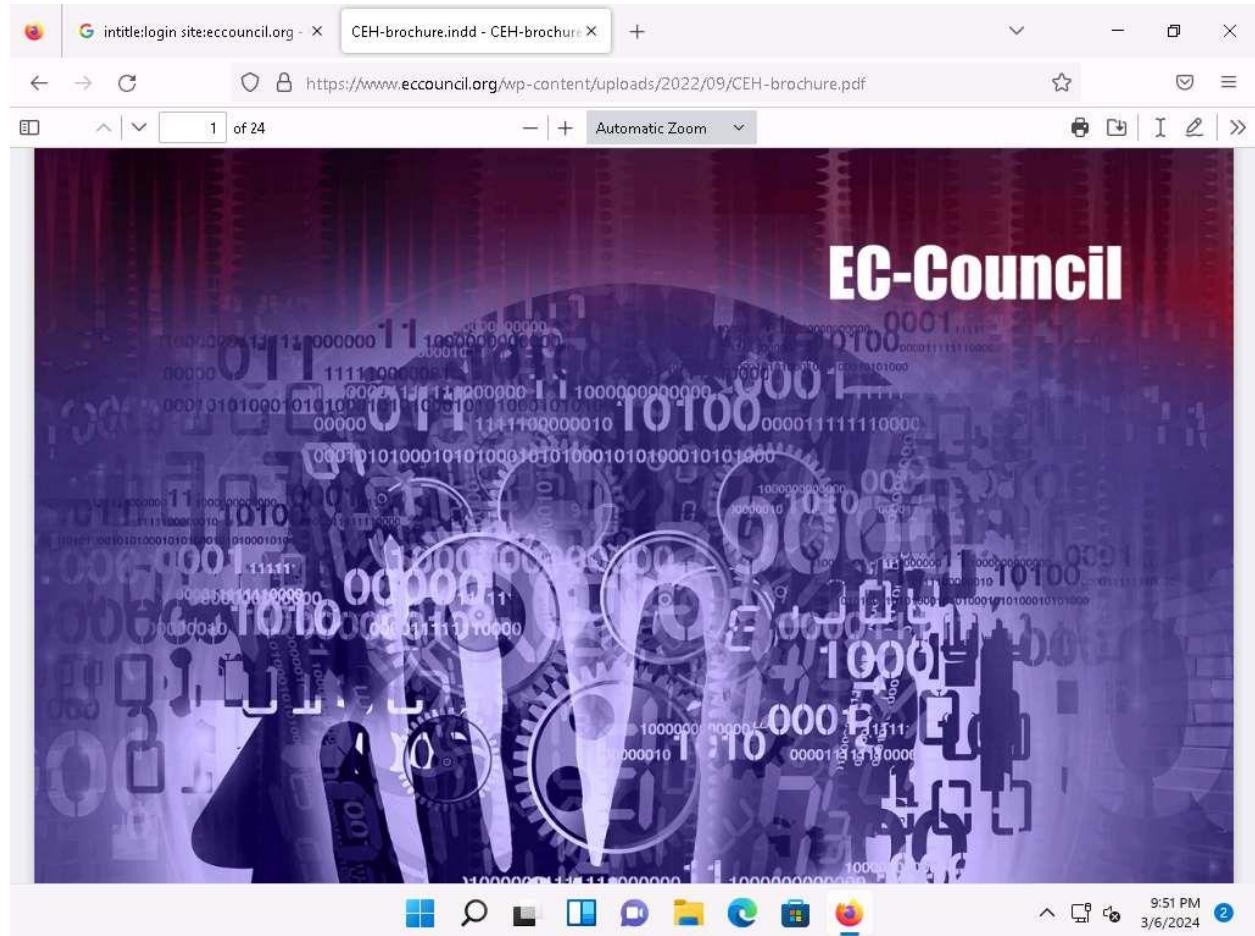
4. Similarly, type the command **EC-Council filetype:pdf ceh** in the search bar to search your results based on the file extension and the keyword (here, **ceh**). Click on any link from the results (here, **CEH-brochure.pdf**) to view the pdf file.

Here, the file type pdf is searched for the target organization EC-Council. The result might differ when you perform this task.

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.



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



6. 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
7. 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.
 8. 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).

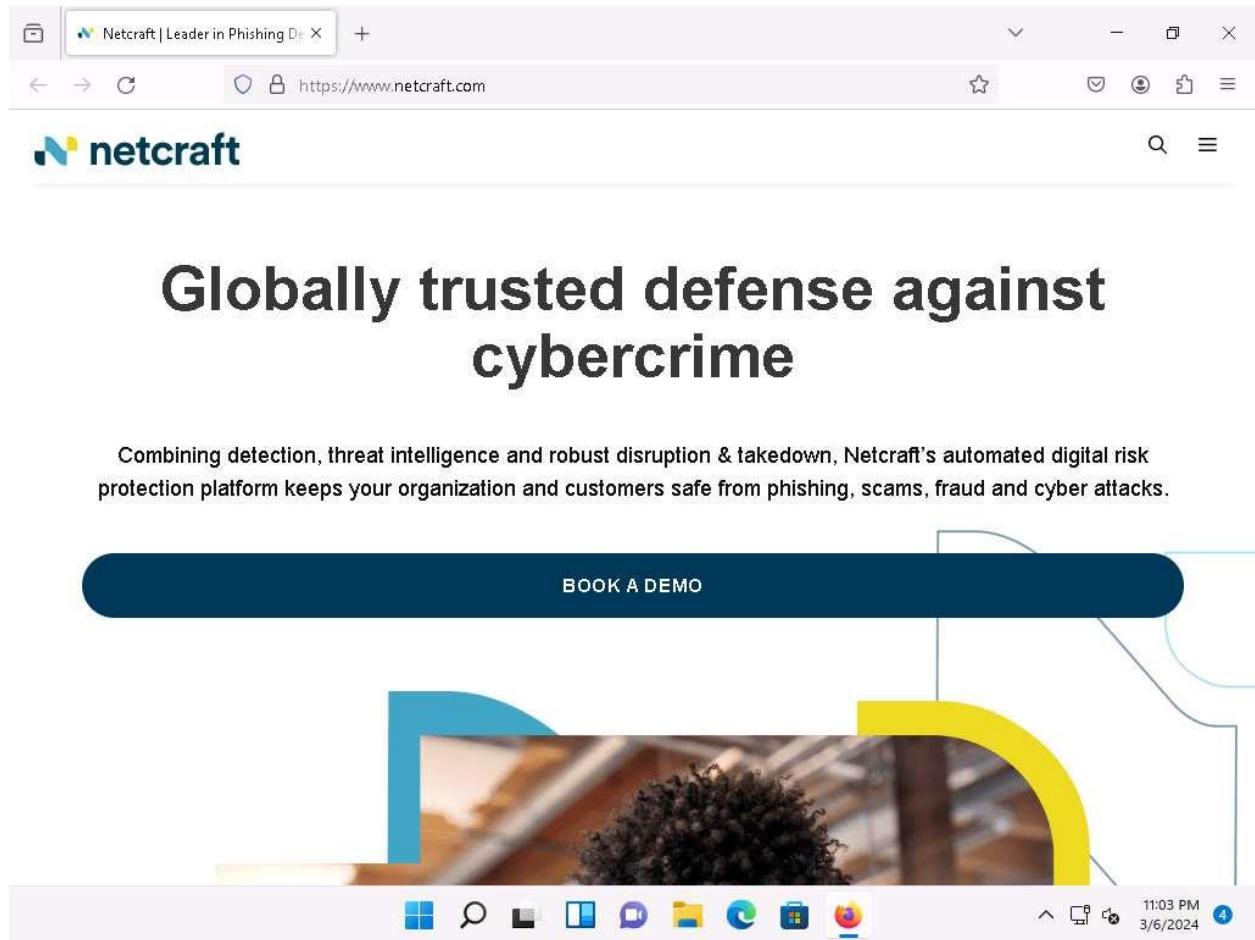
Task 1: Find the Company's Domains, Subdomains and Hosts using Netcraft and DNSdumpster

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.

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



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

Netcraft | Leader in Phishing Defense

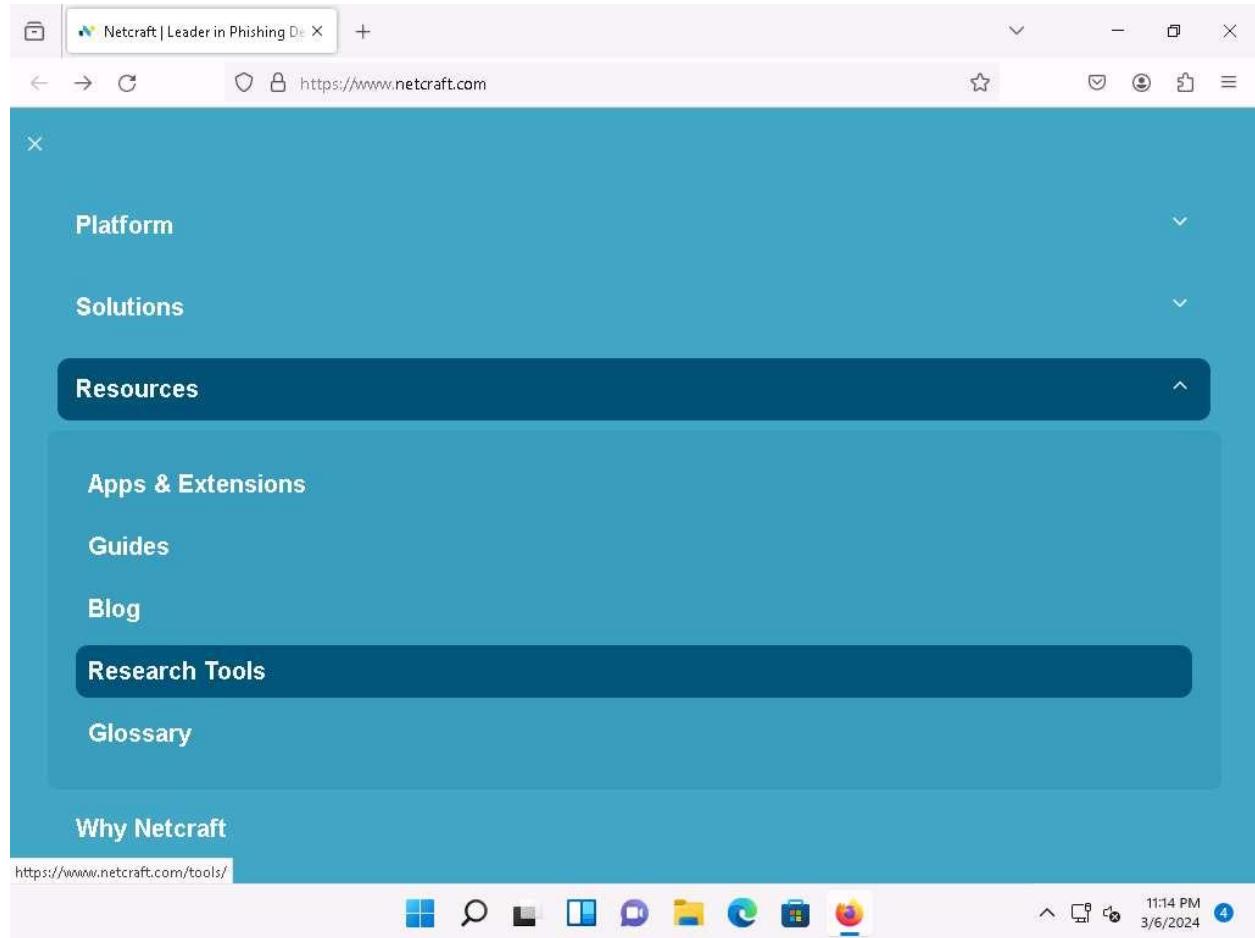
https://www.netcraft.com

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



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

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

the most popular, and how to stay safe on the internet.

Internet Research Tools



Site Report

Using results from our internet data mining, find out the



Search DNS

Explore hostnames visited by



Most Popular Sites

Find out which sites are most visited globally or for any

11:16 PM
3/6/2024

5. 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.

Tools | Netcraft

What's that site running? | Netcraft

https://sitereport.netcraft.com

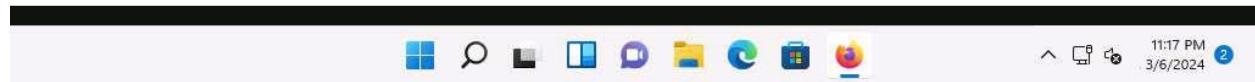
What's that site running?

Find out the infrastructure and technologies used by any site using results from our **internet data mining**

https://www.certifiedhacker.com

Example: <https://www.netcraft.com>

LOOK UP



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

The screenshot shows a Microsoft Edge browser window displaying a Netcraft site report for the URL <https://www.certifiedhacker.com>. The browser's address bar and various control buttons are visible at the top.

Background Section:

| Site title | Not Acceptable! | Date first seen |
|-------------|-----------------|------------------|
| | | January 2018 |
| Site rank | 10752 | Primary language |
| | | English |
| Description | Not Present | |

Network Section:

| Site | https://www.certifiedhacker.com | Domain | certifiedhacker.com |
|-------------------------|---------------------------------|-------------------------|---|
| Netblock Owner | | Unified Layer | Nameserver |
| Hosting company | Newfold Digital | Domain registrar | networksolutions.com |
| Hosting country | US | Nameserver organisation | whois.domain.com |
| IPv4 address | 162.241.216.11 (VirusTotal) | Organisation | 5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, 32256, US |
| IPv4 autonomous systems | AS46606 | DNS admin | dnsadmin@box5331.bluehost.com |
| IPv6 address | Not Present | Top Level Domain | Commercial entities (.com) |

The bottom of the browser window shows the Windows taskbar with icons for File Explorer, Task View, Start, and other system functions. The date and time (11:18 PM, 3/6/2024) are also visible in the bottom right corner.

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

The screenshot shows a Microsoft Edge browser window displaying a Netcraft site report for the URL <https://www.certifiedhacker.com>. The report is titled "Network".

Site: <https://www.certifiedhacker.com>

Domain: certifiedhacker.com

Netblock Owner: Unified Layer

Nameserver: ns1.bluehost.com

Hosting company: Newfold Digital

Domain registrar: networksolutions.com

Hosting country: US

Nameserver organisation: whois.domain.com

IPv4 address: 162.241.216.11 (VirusTotal)

Organisation: 5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, 32256, US

IPv4 autonomous systems: AS46606

DNS admin: dnsadmin@box5331.bluehost.com

IPv6 address: Not Present

Top Level Domain: Commercial entities (.com)

IPv6 autonomous systems: Not Present

DNS Security Extensions: Unknown

Reverse DNS: box5331.bluehost.com

IP delegation:

IPv4 address (162.241.216.11): https://searchdns.netcraft.com/?host=*.certifiedhacker.com

The browser interface includes the Netcraft logo, a navigation bar with back, forward, and search icons, and a status bar at the bottom showing the time (11:19 PM) and date (3/6/2024).

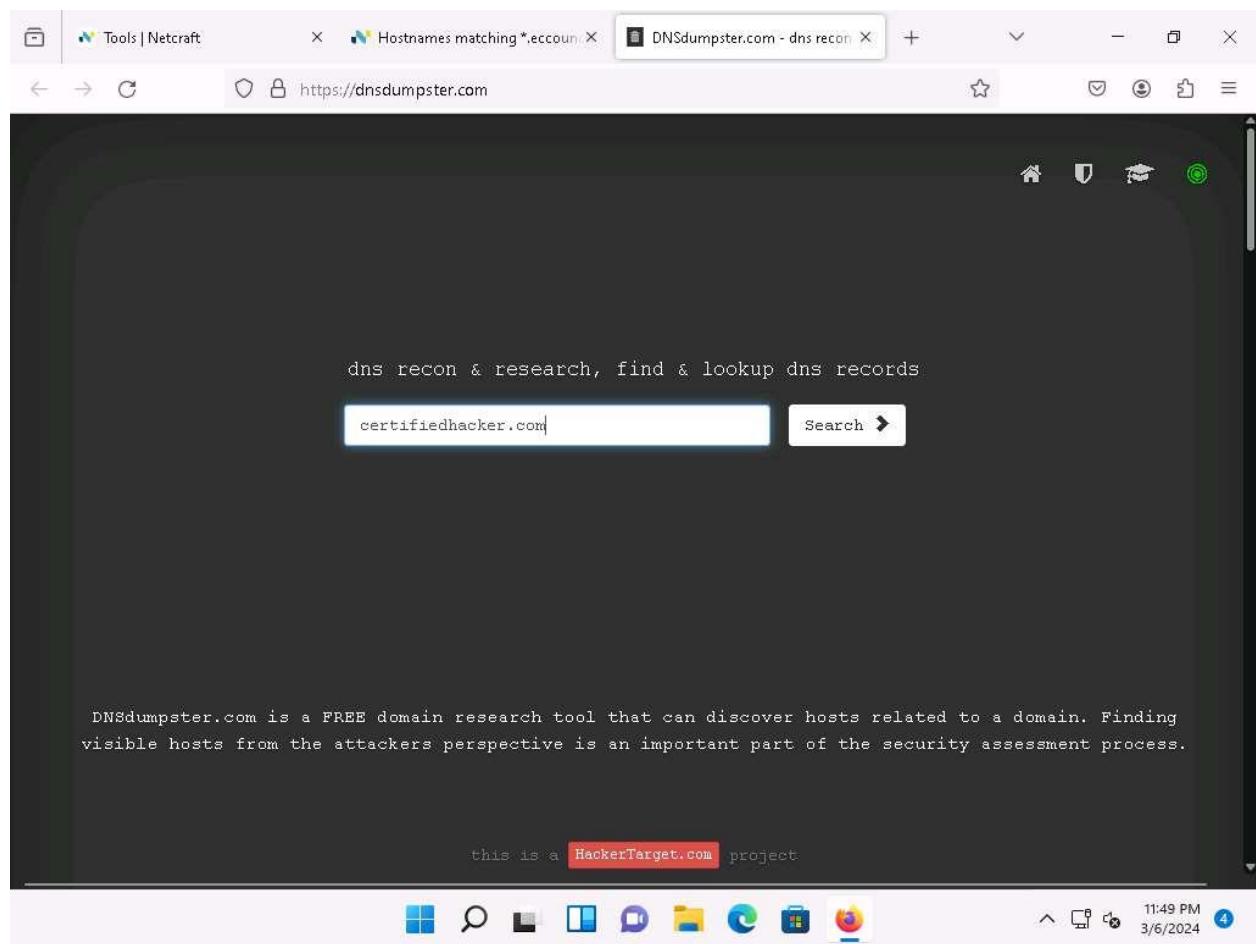
8. The result will display the subdomains of the target website along with netblock and operating system information, as shown in the screenshot.

The screenshot shows a Firefox browser window with the following details:

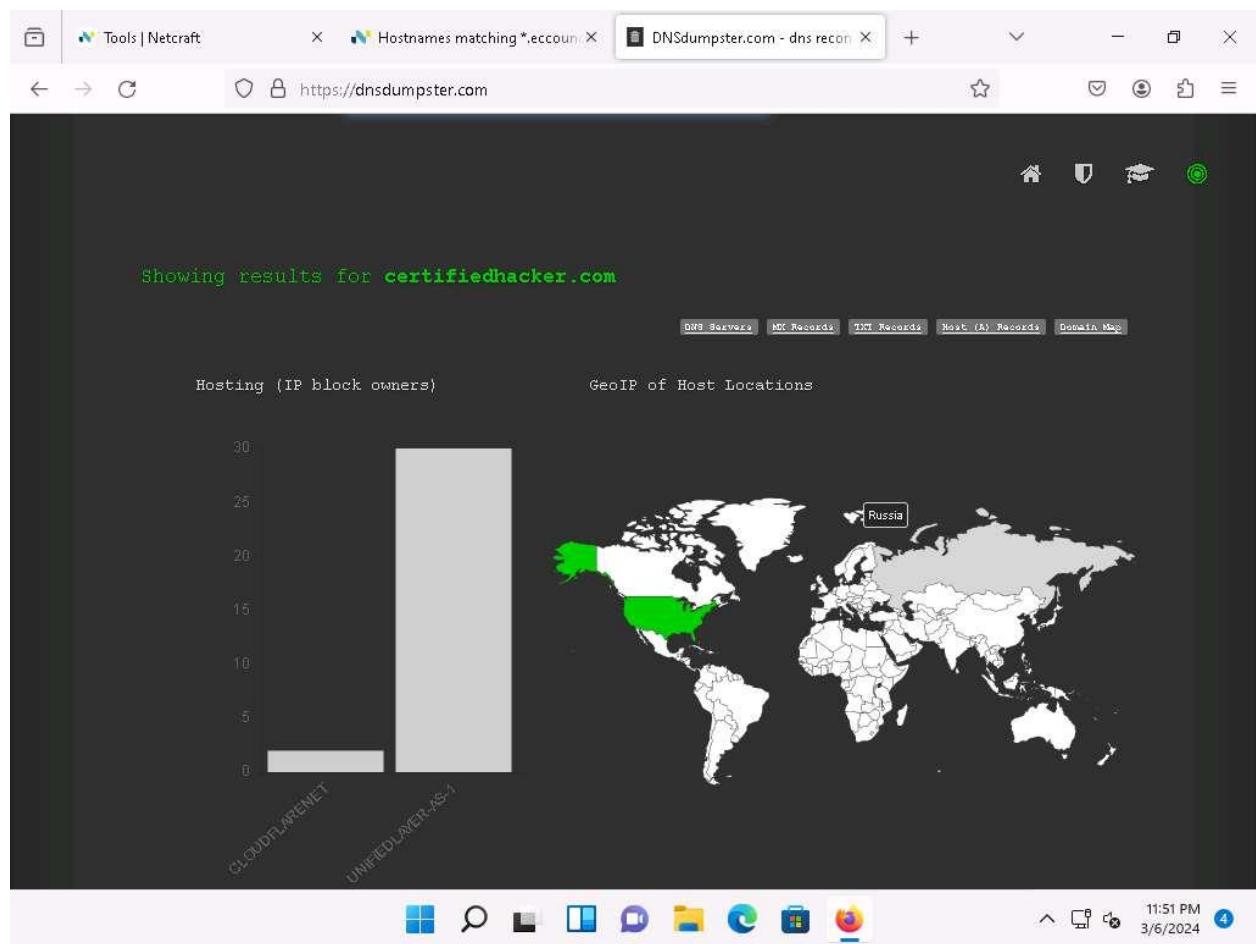
- Address Bar:** https://searchdns.netcraft.com/?host=*.certifiedhacker.com
- Title Bar:** Hostnames matching *.certifiedhacker.com
- Content Area:**
 - Netcraft Logo:** A blue and yellow logo.
 - Section Header:** Hostnames matching *.certifiedhacker.com
 - Search Bar:** ▶ Search with another pattern?
 - Results Summary:** 3 results
 - Table:** A table showing the following data:

| Rank | Site | First seen | Netblock | OS | Site Report |
|---------|--|----------------|---------------|-------|-------------|
| 10752 | www.certifiedhacker.com | December 2002 | Unified Layer | Linux | |
| 1182836 | cpanel.certifiedhacker.com | January 2017 | Unified Layer | Linux | |
| 1452256 | www.sftp.certifiedhacker.com | September 2018 | Unified Layer | Linux | |
 - Bottom Navigation:** Includes icons for Windows Start, Search, Task View, File Explorer, Mail, Edge, Task Manager, and File Explorer.

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



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



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

The screenshot shows a web browser window with the URL <https://dnsdumpster.com>. The page displays DNS information for the domain 'eccoun...'. It includes sections for DNS Servers, MX Records, TXT Records, and Host Records (A). The Host Records section lists two entries: 'soc.certifiedhacker.com' and 'www.soc.certifiedhacker.com', both pointing to IP 162.241.216.11 and located in the United States via AS-1. The browser interface includes a navigation bar with tabs for 'Tools | Netcraft', 'Hostnames matching *eccoun...', and 'DNSdumpster.com - dns recon'. The bottom right corner shows the date and time as 3/6/2024 at 11:54 PM.

DNS Servers

| Name | IP Address | Provider |
|-------------------|----------------|--------------------------|
| ns1.bluehost.com. | 162.159.24.80 | CLOUDFLARENET unknown |
| ns2.bluehost.com. | 162.159.25.175 | CLOUDFLARENET unknown |

MX Records ** This is where email for the domain goes...

| MX Record | IP Address | Provider |
|-----------------------------|----------------|------------------------------------|
| 0 mail.certifiedhacker.com. | 162.241.216.11 | UNIFIEDLAYER-AS-1 United States |

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

```
"v=spf1 a mx ptr include:bluehost.com ?all"
```

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

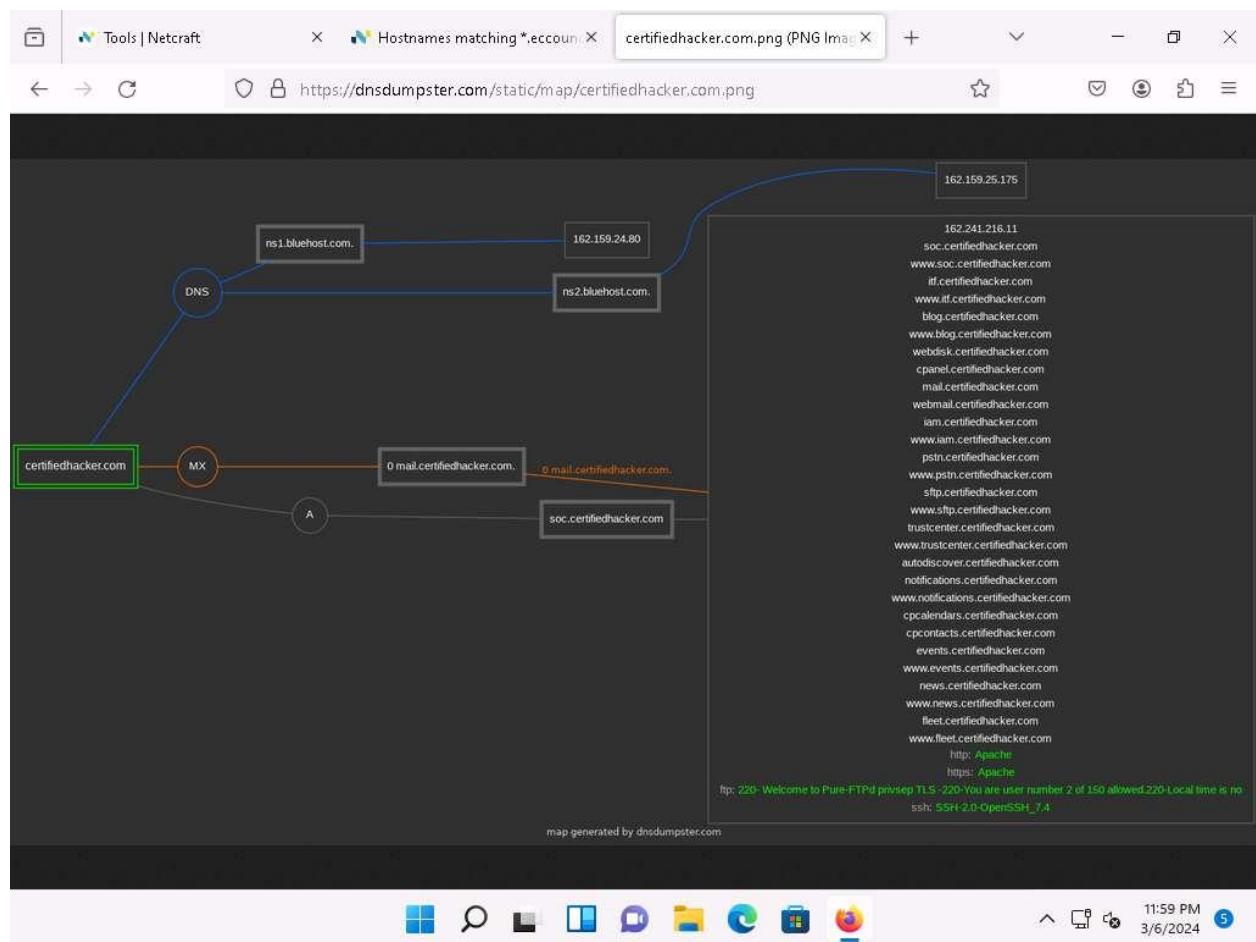
| Name | IP Address | Provider |
|-----------------------------|----------------|------------------------------------|
| soc.certifiedhacker.com | 162.241.216.11 | UNIFIEDLAYER-AS-1 United States |
| www.soc.certifiedhacker.com | 162.241.216.11 | UNIFIEDLAYER-AS-1 United States |

11:54 PM 3/6/2024 4

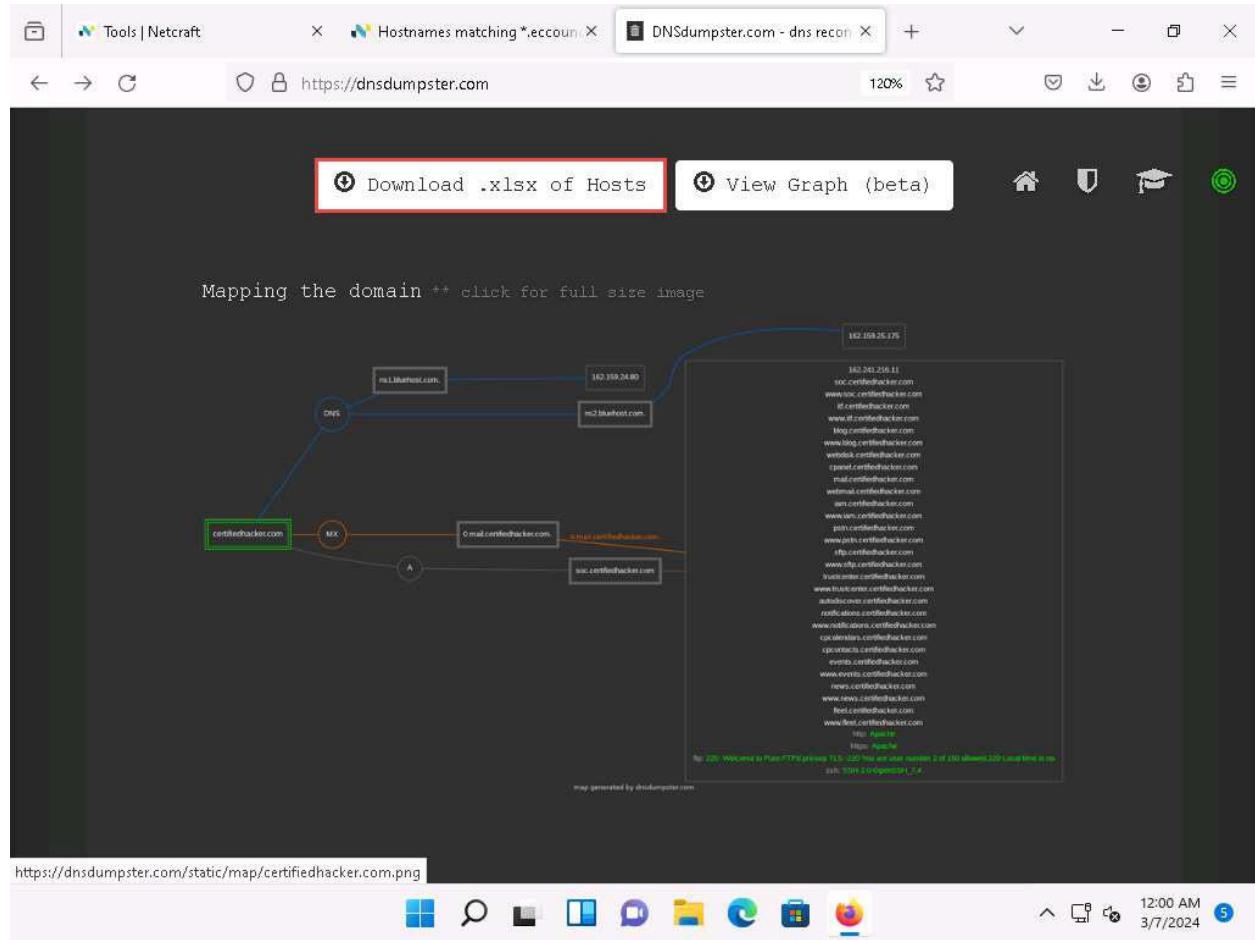
13. Further, scroll down to view the domain mapping of the website.

Click on the map to view the full-size image.

Click back to exit from full-size image.



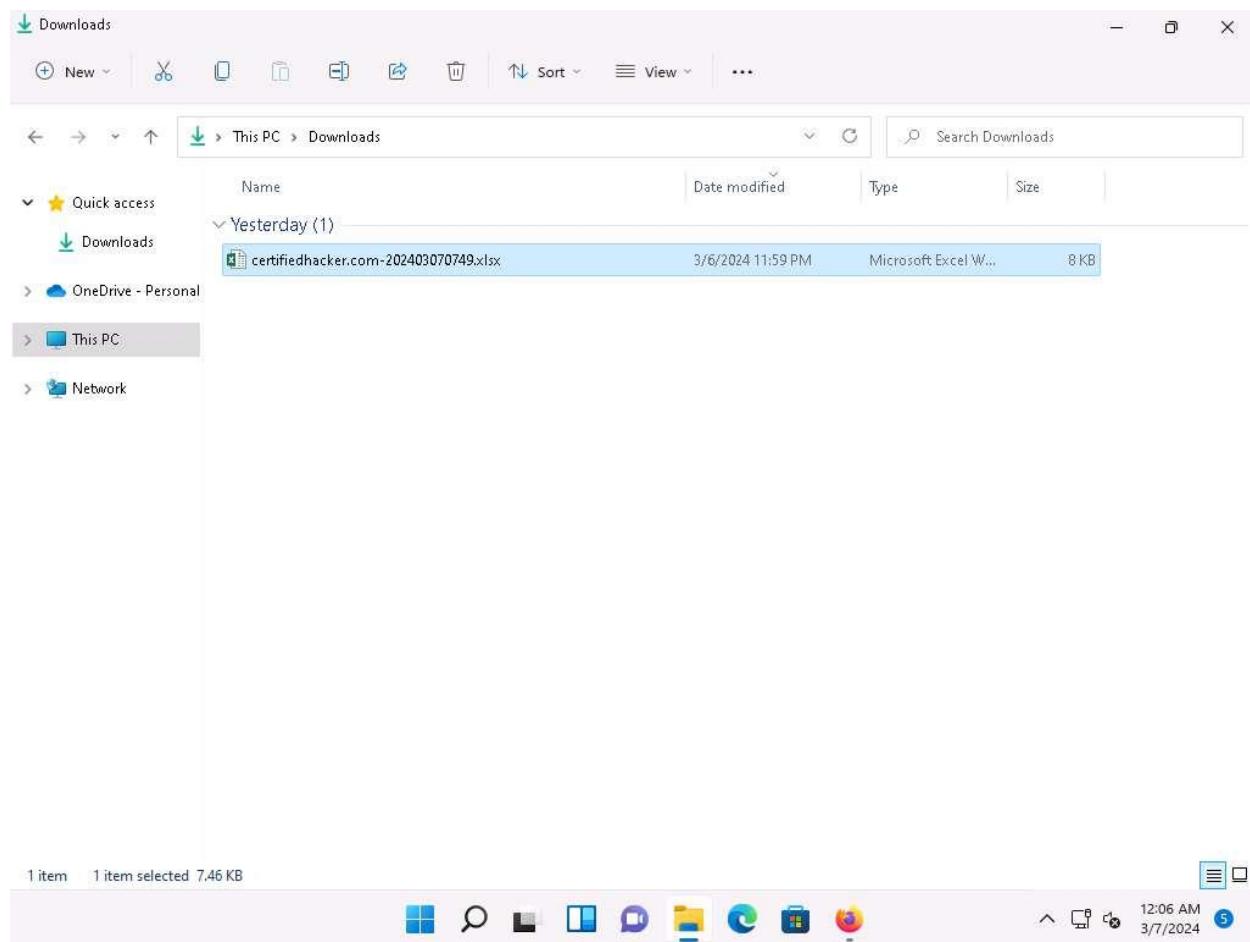
14. Click on **Download .xlsx of Hosts** button to download the list of hosts.



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

In the Microsoft Office Activation Wizard window, click on **Close**.

At the top of the Excel sheet, click on **Enable Editing**.



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

| | Hostname | IP Address | Reverse DNS | Netblock Owner | Country | Tech / Apps | HTTP / Title |
|----|------------------------------|----------------|------------------------|-------------------|---------------|-------------|-----------------------------|
| 1 | soc.certifiedhacker.com | 162.241.216.11 | A box5331.bluehost.com | UNIFIEDLAYER-AS-1 | United States | | Apache title: 404 Not Found |
| 2 | www.soc.certifiedhacker.com | 162.241.216.11 | A box5331.bluehost.com | UNIFIEDLAYER-AS-1 | United States | | Apache title: 404 Not Found |
| 3 | itf.certifiedhacker.com | 162.241.216.11 | A box5331.bluehost.com | UNIFIEDLAYER-AS-1 | United States | | Apache title: 404 Not Found |
| 4 | www.itf.certifiedhacker.com | 162.241.216.11 | A box5331.bluehost.com | UNIFIEDLAYER-AS-1 | United States | | Apache title: 404 Not Found |
| 5 | blog.certifiedhacker.com | 162.241.216.11 | A box5331.bluehost.com | UNIFIEDLAYER-AS-1 | United States | | Apache title: 404 Not Found |
| 6 | www.blog.certifiedhacker.com | 162.241.216.11 | A box5331.bluehost.com | UNIFIEDLAYER-AS-1 | United States | | Apache title: 404 Not Found |
| 7 | webdisk.certifiedhacker.com | 162.241.216.11 | A box5331.bluehost.com | UNIFIEDLAYER-AS-1 | United States | | Apache title: 404 Not Found |
| 8 | cpanel.certifiedhacker.com | 162.241.216.11 | A box5331.bluehost.com | UNIFIEDLAYER-AS-1 | United States | | Apache title: 404 Not Found |
| 9 | mail.certifiedhacker.com | 162.241.216.11 | A box5331.bluehost.com | UNIFIEDLAYER-AS-1 | United States | | Apache title: 404 Not Found |
| 10 | webmail.certifiedhacker.com | 162.241.216.11 | A box5331.bluehost.com | UNIFIEDLAYER-AS-1 | United States | | Apache title: 404 Not Found |
| 11 | iam.certifiedhacker.com | 162.241.216.11 | A box5331.bluehost.com | UNIFIEDLAYER-AS-1 | United States | | Apache title: 404 Not Found |
| 12 | | | | | | | |

17. 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.
18. 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.
19. 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.

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.

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.

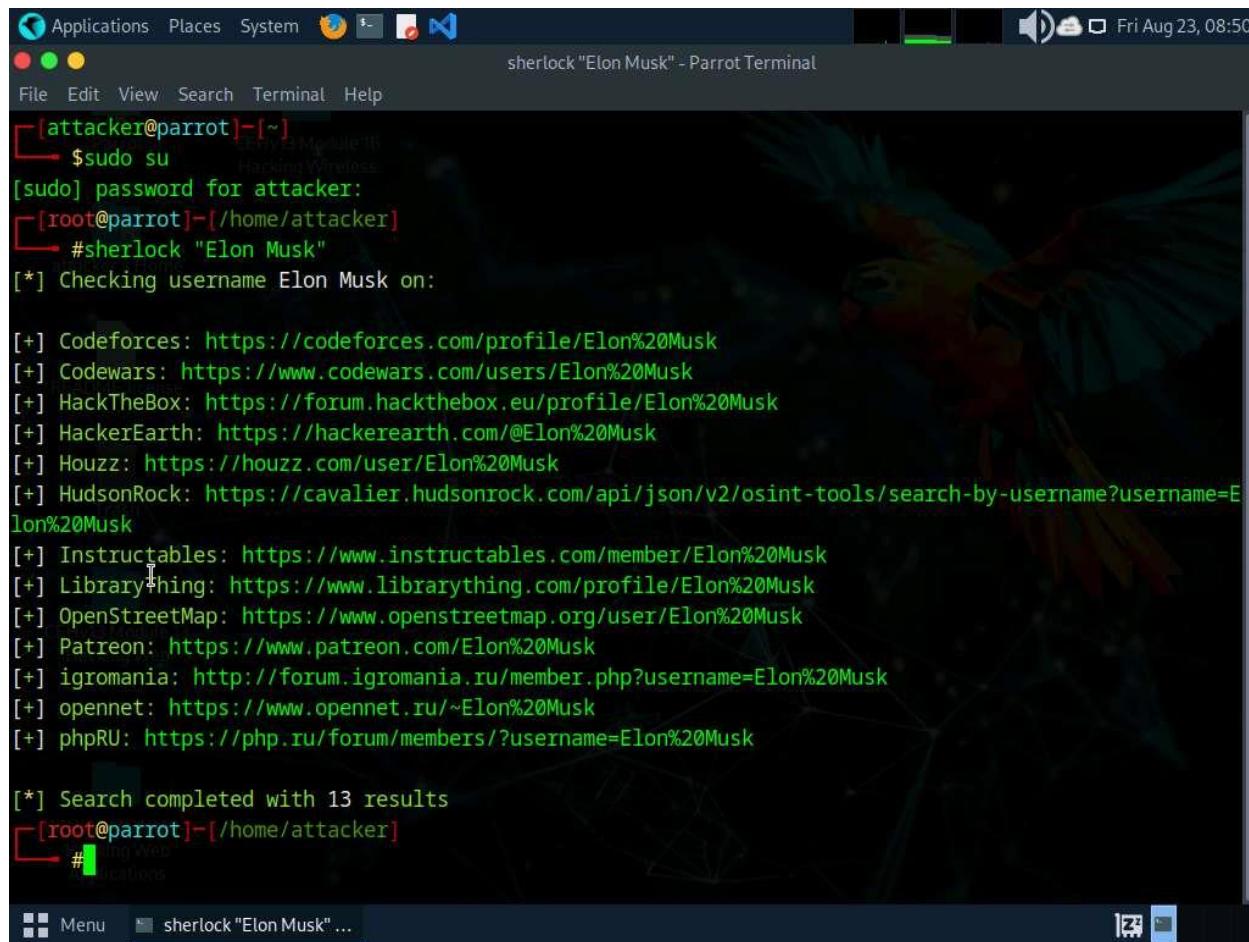
Here, we are gathering information about **Elon Musk**. However, you can select a target of your choice.

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**).

The password that you type will not be visible.

3. 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.

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



The screenshot shows a terminal window titled "sherlock "Elon Musk" - Parrot Terminal". The terminal session starts with the user switching to root using "sudo su". It then prompts for the password, which is not visible. After becoming root, the user runs the "sherlock" command with the argument "Elon Musk". The output lists 13 different websites where the target's name appears. The terminal window has a dark background with some graphical elements on the right side.

```
[attacker@parrot] -[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot] -[/home/attacker]
└─# sherlock "Elon Musk"

[*] Checking username Elon Musk on:

[+] Codeforces: https://codeforces.com/profile/Elon%20Musk
[+] Codewars: https://www.codewars.com/users/Elon%20Musk
[+] HackTheBox: https://forum.hackthebox.eu/profile/Elon%20Musk
[+] HackerEarth: https://hackerearth.com/@Elon%20Musk
[+] Houzz: https://houzz.com/user/Elon%20Musk
[+] HudsonRock: https://cavalier.hudsonrock.com/api/json/v2/osint-tools/search-by-username?username=Elon%20Musk
[+] Instructables: https://www.instructables.com/member/Elon%20Musk
[+] LibraryThing: https://www.librarything.com/profile/Elon%20Musk
[+] OpenStreetMap: https://www.openstreetmap.org/user/Elon%20Musk
[+] Patreon: https://www.patreon.com/Elon%20Musk
[+] igromania: http://forum.igromania.ru/member.php?username=Elon%20Musk
[+] opennet: https://www.opennet.ru/~Elon%20Musk
[+] phpRU: https://php.ru/forum/members/?username=Elon%20Musk

[*] Search completed with 13 results
[root@parrot] -[/home/attacker]
└─#
```

4. 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.
5. This concludes the demonstration of gathering personal information from various social networking sites using Sherlock.
 6. 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.
 7. 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.

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

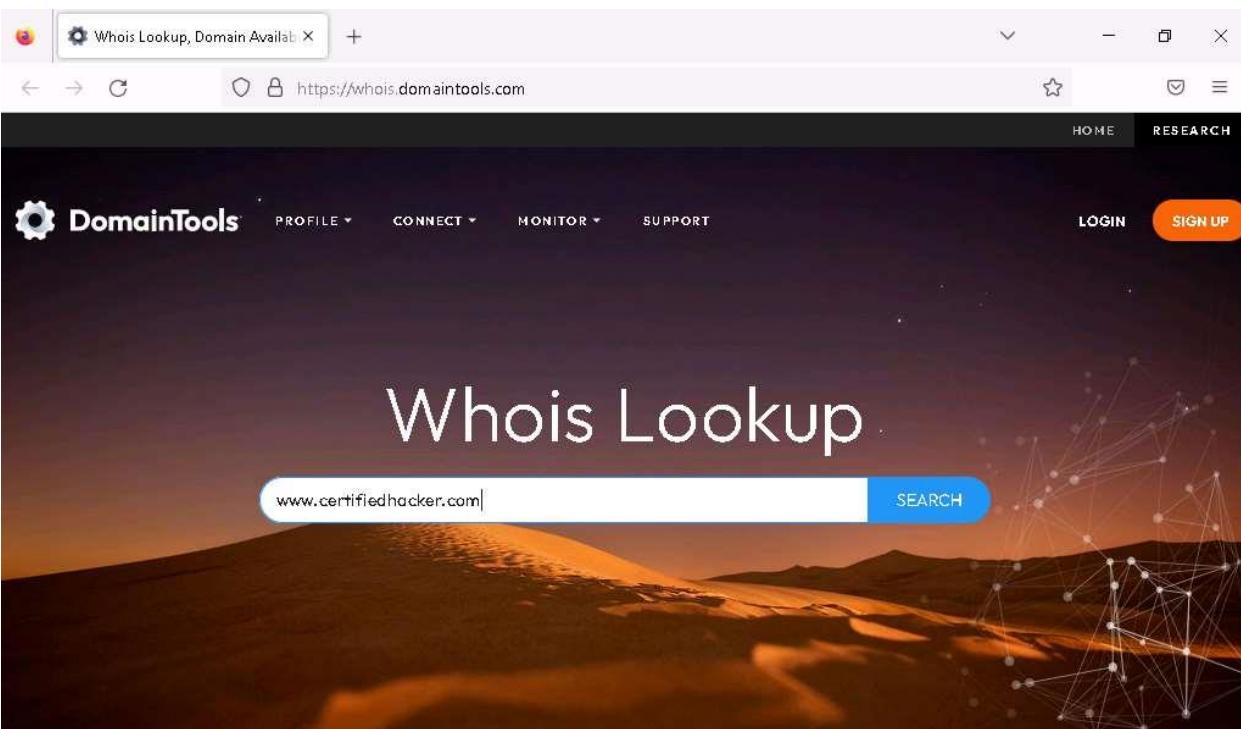
This lab focuses on how to perform a Whois lookup and analyze the results. Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource such as a domain name, an IP address block, or an autonomous system. This protocol listens 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**.



The screenshot shows a Mozilla Firefox browser window with the URL <https://whois.domaintools.com> in the address bar. The page title is "Whois Lookup". The search bar contains the URL www.certifiedhacker.com. Below the search bar, there is a "SEARCH" button. The background of the page features a desert landscape at sunset with a network graph overlay. At the bottom of the page, there is a promotional banner for upgrading membership.

Upgrade Your Membership and Elevate Your Defenses

You've got valuable starting data with Whois. Now it's time to take that information and make deeper connections to profile attackers, guide online fraud investigations,

11:13 PM
3/7/2024

3. 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.

CertifiedHacker.com WHOIS DI X +

https://whois.domaintools.com/certifiedhacker.com

HOME RESEARCH

DomainTools PROFILE CONNECT MONITOR SUPPORT WHOIS

LOG IN 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 | USA - Utah - Provo - Unified Layer |

AKA: [certifiedhacker.com](#) (Last updated: 2024-03-07)

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



The screenshot shows a web browser window with the following details:

- Address Bar:** https://whois.domaintools.com/certifiedhacker.com
- DomainTools Header:** CertifiedHacker.com WHOIS, DI X
- Navigation:** HOME | RESEARCH | PROFILE | CONNECT | MONITOR | SUPPORT | WHOIS | LOG IN | SIGN UP
- Domain Details:**
 - IP Location: USA - Utah - Provo - Unified Layer
 - ASN: AS46606 UNIFIEDLAYER-AS-1, US (registered Oct 24, 2008)
 - Domain Status: Registered And No Website
 - IP History: 13 changes on 13 unique IP addresses over 18 years
 - Registrar History: 3 registrars with 3 drops
 - Hosting History: 6 changes on 4 unique name servers over 21 years
- Whois Record (last updated on 2024-03-08):**

```

Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2023-08-22T07:58:34Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2024-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL

```
- Available TLDs:** General TLDs | Country TLDs
- Note:** The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)
 - Taken domain.
 - Available domain.
 - Deleted previously owned domain.
- Domain Options:**

| | |
|----------------------|------------|
| CertifiedHacker.com | View Whois |
| CertifiedHacker.net | View Whois |
| CertifiedHacker.org | View Whois |
| CertifiedHacker.info | Buy Domain |
| CertifiedHacker.biz | Buy Domain |
| CertifiedHacker.us | Buy Domain |
- System Information:** 11:15 PM | 3/7/2024 | 5

4. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
5. 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.
6. 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.
7. 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.

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.

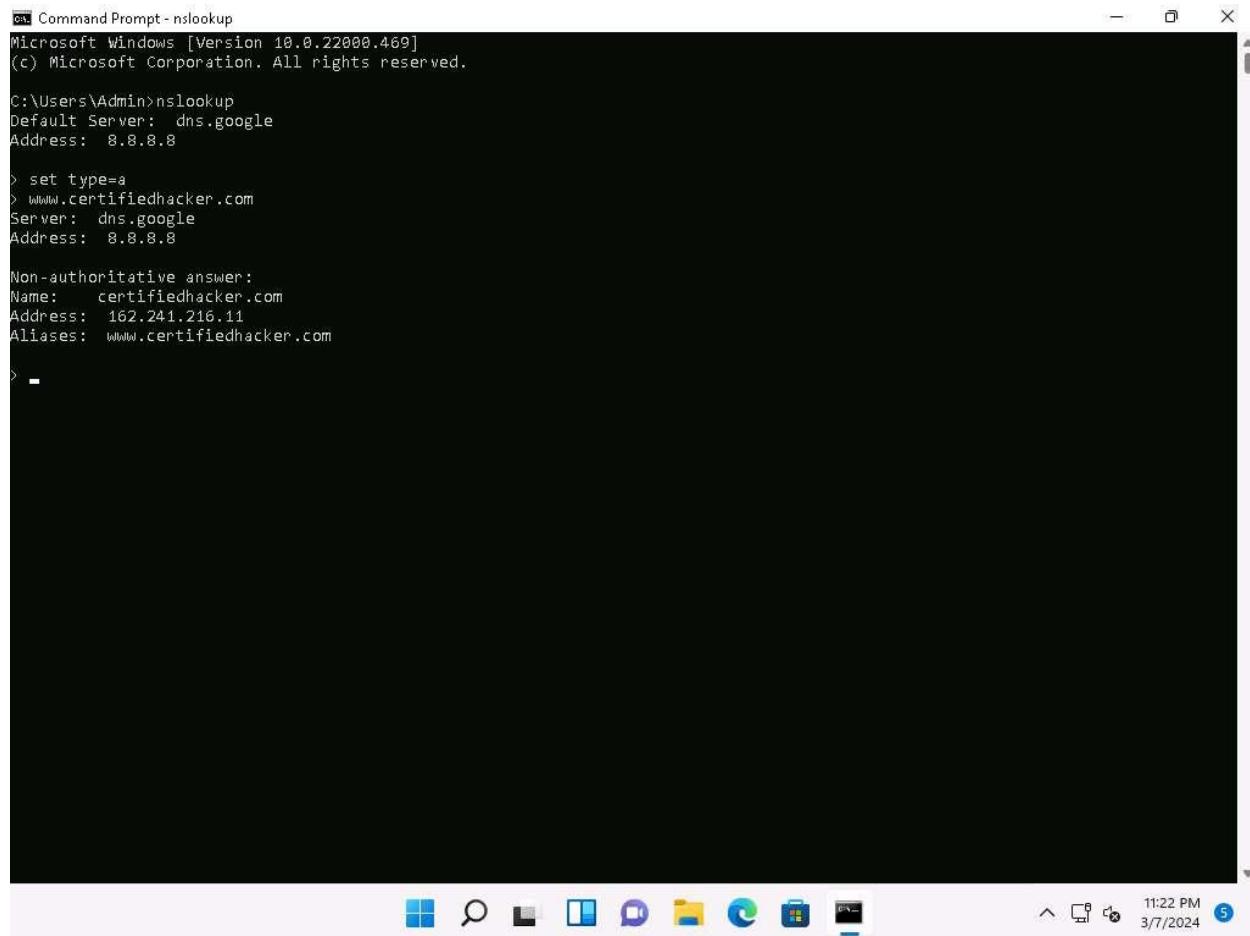
Task 1: Gather DNS Information using nslookup Command Line Utility and Online Tool

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.



```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

> set type=a
> www.certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: certifiedhacker.com
Address: 162.241.216.11
Aliases: www.certifiedhacker.com

>
```

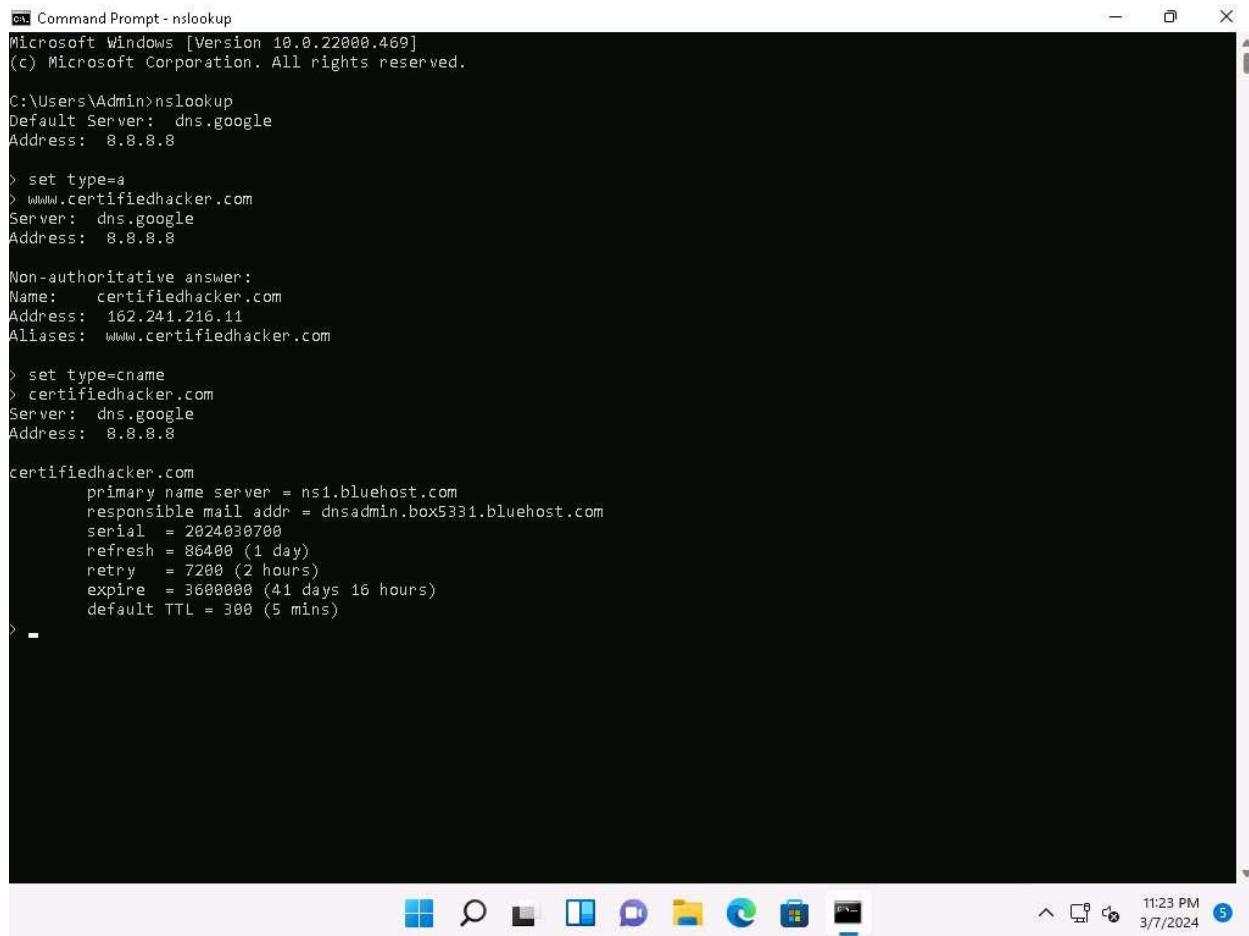
4. The first two lines in the result are:

Server: **dns.google** and Address: **8.8.8.8**

This specifies that the result was directed to the default server hosted on the local machine (**Windows 11**) that resolves your requested domain.

5. 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**.
6. Since the result returned is non-authoritative, you need to obtain the domain's authoritative name server.

7. 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.
8. Type **certifiedhacker.com** and press **Enter**.
9. 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.



```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

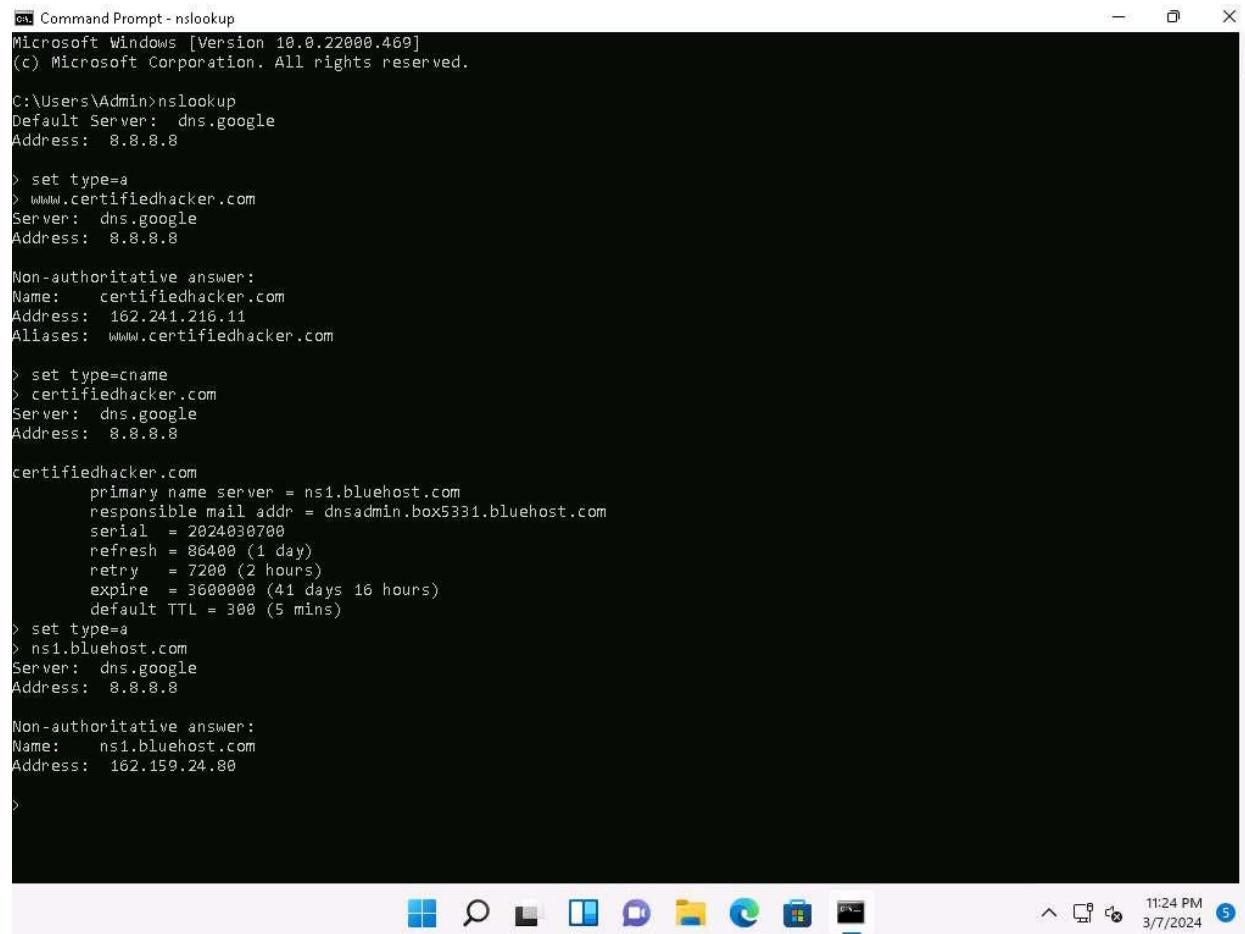
> set type=a
> www.certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: certifiedhacker.com
Address: 162.241.216.11
Aliases: www.certifiedhacker.com

> set type cname
> certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2024030700
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
>
```

10. Since you have obtained the authoritative name server, you will need to determine the IP address of the name server.
11. Issue the command **set type=a** and press **Enter**.
12. 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.



```
C:\ Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.409]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server: dns.google
Address: 8.8.8.8

> set type=a
> www.certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: certifiedhacker.com
Address: 162.241.216.11
Aliases: www.certifiedhacker.com

> set type=cname
> certifiedhacker.com
Server: dns.google
Address: 8.8.8.8

certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2024030700
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)

> set type=a
> ns1.bluehost.com
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: ns1.bluehost.com
Address: 162.159.24.80

>
```

13. 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.
14. 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.
15. Now, we will use an online tool NSLOOKUP to gather DNS information about the target domain.
16. Open any web browser and go to <http://www.kloth.net/services/nslookup.php> (here, we are using Mozilla Firefox).
17. NSLOOKUP website appears, as shown in the screenshot.

18. 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.

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: ... the name of the machine to look up.

Server: ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query:

... 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 11 of max 100]

19. In the **Query:** field, click the drop-down arrow and check the different options that are available, as shown in the screenshot.

20. 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.

KLOTH.NET - NSLOOKUP - DNS X +

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 (UBEUCE 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: ... the name of the machine to look up.

Server: ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query:

... 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

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/JUCE 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: ... the name of the machine to look up.

Server: ... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better).

Query:

... here is the nslookup result for **www.certifiedhacker.com** from server localhost, querytype=AAAA:

```
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.

Authoritative answers can be found from:
certifiedhacker.com
    origin = ns1.bluehost.com
    mail addr = dnsadmin.box5331.bluehost.com
    serial = 2024030700
    refresh = 86400
    retry = 7200
    expire = 3600000
    minimum = 300

[Query 16 of max 100]
```

NSLOOKUP is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035, RFC1033]). The NSLOOKUP utility is a unix tool. If you want to learn more, here is the nslookup

11:41 PM
3/7/2024

21. This concludes the demonstration of DNS information gathering using the nslookup command-line utility and NSLOOKUP online tool.
22. You can also use DNS lookup tools such as **DNSdumpster** (<https://dnsdumpster.com>) to extract additional target DNS information.
23. 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.

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.

The results might differ when you perform the lab.

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window displays the output of the "tracert" command. The command was run from the path "C:\Users\Admin>". The output shows the tracing route to the website "www.certifiedhacker.com" over a maximum of 30 hops. The route passes through various IP addresses and domain names, including 10.10.1.2, 172.18.0.1, 192.168.0.1, 103.186.82.26, 103.186.82.3, g10-1-1-15.rcr21.iad01.atlas.cogentco.com [38.104.207.233], be2956.ccr41.iad02.atlas.cogentco.com [154.54.30.193], telia.iad02.atlas.cogentco.com [154.54.12.62], ash-bb2-link.ip.twelve99.net [62.115.123.124], nyk-bb2-link.ip.twelve99.net [62.115.136.200], palo-b24-link.ip.twelve99.net [62.115.122.36], salt-b2-link.ip.twelve99.net [62.115.140.53], newfolddigital-ic-380138.ip.twelve99-cust.net [80.239.167.103], 69-195-64-103.unifiedlayer.com [69.195.64.103], po97.prv-leaf1a.net.unifiedlayer.com [162.144.240.123], and box5331.bluehost.com [162.241.216.11]. The trace is complete after 16 hops.

```
C:\ Command Prompt  
Microsoft Windows [Version 10.0.22000.409]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\Admin>tracert www.certifiedhacker.com  
  
Tracing route to certifiedhacker.com [162.241.216.11]  
over a maximum of 30 hops:  
  
 1    1 ms    <1 ms    <1 ms  10.10.1.2  
 2    2 ms    2 ms    3 ms  172.18.0.1  
 3    4 ms    1 ms    4 ms  192.168.0.1  
 4    1 ms    3 ms    1 ms  103.186.82.26  
 5    2 ms    5 ms    3 ms  103.186.82.3  
 6    4 ms    2 ms    3 ms  g10-1-1-15.rcr21.iad01.atlas.cogentco.com [38.104.207.233]  
 7    4 ms    1 ms    7 ms  be2956.ccr41.iad02.atlas.cogentco.com [154.54.30.193]  
 8    2 ms    *       *       telia.iad02.atlas.cogentco.com [154.54.12.62]  
 9    4 ms    4 ms    2 ms  ash-bb2-link.ip.twelve99.net [62.115.123.124]  
10   9 ms    9 ms    8 ms  nyk-bb2-link.ip.twelve99.net [62.115.136.200]  
11  79 ms   78 ms   78 ms  palo-b24-link.ip.twelve99.net [62.115.122.36]  
12  92 ms   91 ms   91 ms  salt-b2-link.ip.twelve99.net [62.115.140.53]  
13  101 ms   92 ms  100 ms  newfolddigital-ic-380138.ip.twelve99-cust.net [80.239.167.103]  
14  92 ms   94 ms   94 ms  69-195-64-103.unifiedlayer.com [69.195.64.103]  
15  92 ms   92 ms   93 ms  po97.prv-leaf1a.net.unifiedlayer.com [162.144.240.123]  
16  92 ms   92 ms   94 ms  box5331.bluehost.com [162.241.216.11]  
  
Trace complete.  
C:\Users\Admin>
```

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

```
Command Prompt
Microsoft Windows [Version 10.0.22000.409]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>tracert www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

 1   1 ms    <1 ms    <1 ms  10.10.1.2
 2   2 ms    2 ms    3 ms  172.18.0.1
 3   4 ms    1 ms    4 ms  192.168.0.1
 4   1 ms    3 ms    1 ms  103.186.82.26
 5   2 ms    5 ms    3 ms  103.186.82.3
 6   4 ms    2 ms    3 ms  g10-1-1-15.rcr21.lad01.atlas.cogentco.com [38.104.207.233]
 7   4 ms    1 ms    7 ms  be2956.ccr41.iad02.atlas.cogentco.com [154.54.30.193]
 8   2 ms    *       *       telia.iad02.atlas.cogentco.com [154.54.12.62]
 9   4 ms    4 ms    2 ms  ash-bb2-link.ip.twelve99.net [62.115.123.124]
10   9 ms    9 ms    8 ms  nyk-bb2-link.ip.twelve99.net [62.115.136.200]
11   79 ms   78 ms   78 ms  palo-b24-link.ip.twelve99.net [62.115.122.36]
12   92 ms   91 ms   91 ms  salt-b2-link.ip.twelve99.net [62.115.140.53]
13   101 ms   92 ms   100 ms newfoldigital-ic-380138.ip.twelve99-cust.net [80.239.167.103]
14   92 ms   94 ms   94 ms  69-195-64-103.unifiedlayer.com [69.195.64.103]
15   92 ms   92 ms   93 ms  po97.prv-leaf1a.net.unifiedlayer.com [162.144.240.123]
16   92 ms   92 ms   94 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d           Do not resolve addresses to hostnames.
  -h maximum_hops Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list (IPv4-only).
  -w timeout    Wait timeout milliseconds for each reply.
  -R           Trace round-trip path (IPv6-only).
  -S srcaddr    Source address to use (IPv6-only).
  -4           Force using IPv4.
  -6           Force using IPv6.

C:\Users\Admin>
```

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

-h: Number of maximum hops.

```

Select Command Prompt
6   4 ms    2 ms    3 ms  gi0-1-1-15.rcr21.iad01.atlas.cogentco.com [38.104.207.233]
7   4 ms    1 ms    7 ms  be2956.ccr41.iad02.atlas.cogentco.com [154.54.30.193]
8   2 ms    *        *      telia.iad02.atlas.cogentco.com [154.54.12.62]
9   4 ms    4 ms    2 ms  ash-bb2-link.ip.twelve99.net [62.115.123.124]
10  9 ms    9 ms    8 ms  nyk-bb2-link.ip.twelve99.net [62.115.136.200]
11  79 ms   78 ms   78 ms  palo-b24-link.ip.twelve99.net [62.115.122.36]
12  92 ms   91 ms   91 ms  salt-b2-link.ip.twelve99.net [62.115.140.53]
13  181 ms   92 ms   100 ms newfoldigital-ic-380138.ip.twelve99-cust.net [80.239.167.103]
14  92 ms   94 ms   94 ms  69-195-64-103.unifiedlayer.com [69.195.64.103]
15  92 ms   92 ms   93 ms  po97.prv-leaf1a.net.unifiedlayer.com [162.144.240.123]
16  92 ms   92 ms   94 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d          Do not resolve addresses to hostnames.
  -h maximum_hops Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list (IPv4-only).
  -w timeout   Wait timeout milliseconds for each reply.
  -R          Trace round-trip path (IPv6-only).
  -S srcaddr   Source address to use (IPv6-only).
  -4          Force using IPv4.
  -6          Force using IPv6.

C:\Users\Admin>tracert -h 5 www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 5 hops:

  1  2 ms    1 ms    2 ms  10.10.1.2
  2  2 ms    1 ms    1 ms  172.18.0.1
  3  3 ms    1 ms    1 ms  192.168.0.1
  4  3 ms    1 ms    1 ms  103.186.82.26
  5  2 ms    1 ms    1 ms  103.186.82.3

Trace complete.

C:\Users\Admin>

```

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

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.

The screenshot shows a terminal window titled "traceroute www.certifiedhacker.com - Parrot Terminal". The terminal displays the results of a traceroute command. The output shows the path from the attacker's machine to the target website, www.certifiedhacker.com, through 16 different routers. Each router entry includes its IP address, name, and the time taken for the packet to reach that point. The routers listed include various ISP and network nodes, such as 10.10.1.2, 172.18.0.1, 192.168.0.1, 103.186.82.26, 103.186.82.3, gi0-1-1-15.rcr21.iad01.atlas.cogentco.com, be2956.ccr41.iad02.atlas.cogentco.com, telia.iad02.atlas.cogentco.com, rest-bb1-link.ip.twelve99.net, nyk-bb1-link.ip.twelve99.net, nyk-bb2-link.ip.twelve99.net, palo-b24-link.ip.twelve99.net, salt-b2-link.ip.twelve99.net, newfoldigital-ic-380138.ip.twelve99-cust.net, 69-195-64-105.unifiedlayer.com, po99.prv-leaf1a.net.unifiedlayer.com, po97.prv-leaf1b.net.unifiedlayer.com, and box5331.bluehost.com.

```
traceroute to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1  10.10.1.2 (10.10.1.2)  0.770 ms  1.198 ms  0.595 ms
 2  172.18.0.1 (172.18.0.1)  1.071 ms  1.496 ms  0.964 ms
 3  192.168.0.1 (192.168.0.1)  1.602 ms  1.549 ms  1.497 ms
 4  103.186.82.26 (103.186.82.26)  2.924 ms  2.858 ms  1.340 ms
 5  103.186.82.3 (103.186.82.3)  1.715 ms  1.663 ms  1.611 ms
 6  gi0-1-1-15.rcr21.iad01.atlas.cogentco.com (38.104.207.233)  2.818 ms  2.204 ms  2.118 ms
 7  be2956.ccr41.iad02.atlas.cogentco.com (154.54.30.193)  3.210 ms  2.744 ms  2.690 ms
 8  telia.iad02.atlas.cogentco.com (154.54.12.62)  2.452 ms  2.399 ms  2.533 ms
 9  rest-bb1-link.ip.twelve99.net (62.115.123.122)  2.881 ms  ash-bb2-link.ip.twelve99.net (62.115.123.124)  2.244 ms
10  rest-bb1-link.ip.twelve99.net (62.115.141.245)  8.720 ms  nyk-bb2-link.ip.twelve99.net (62.115.136.200)  8.889 ms  8.821 ms
11  nyk-bb1-link.ip.twelve99.net (62.115.138.191)  2.449 ms
12  palo-b24-link.ip.twelve99.net (62.115.138.117)  77.193 ms  77.141 ms  palo-b24-link.ip.twelve99.net (62.115.138.111)  76.999 ms
13  salt-b2-link.ip.twelve99.net (62.115.140.53)  90.856 ms  90.602 ms  91.834 ms
14  newfoldigital-ic-380138.ip.twelve99-cust.net (80.239.167.103)  106.769 ms  106.653 ms  106.602 ms
15  69-195-64-105.unifiedlayer.com (69.195.64.105)  92.872 ms  69-195-64-103.unifiedlayer.com (69.195.64.103)  91.532 ms
16  69-195-64-105.unifiedlayer.com (69.195.64.105)  93.167 ms
17  po99.prv-leaf1a.net.unifiedlayer.com (162.144.240.127)  92.946 ms  po97.prv-leaf1b.net.unifiedlayer.com (162.144.240.135)  93.126 ms
18  box5331.bluehost.com (162.241.216.11)  93.016 ms  92.995 ms  92.402 ms
```

7. This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.
8. 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.
9. 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.

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:

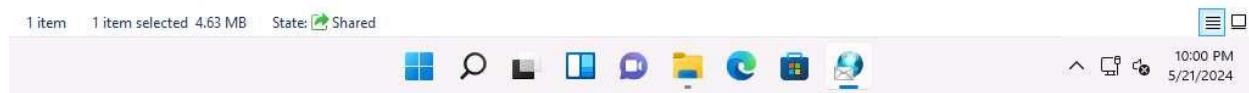
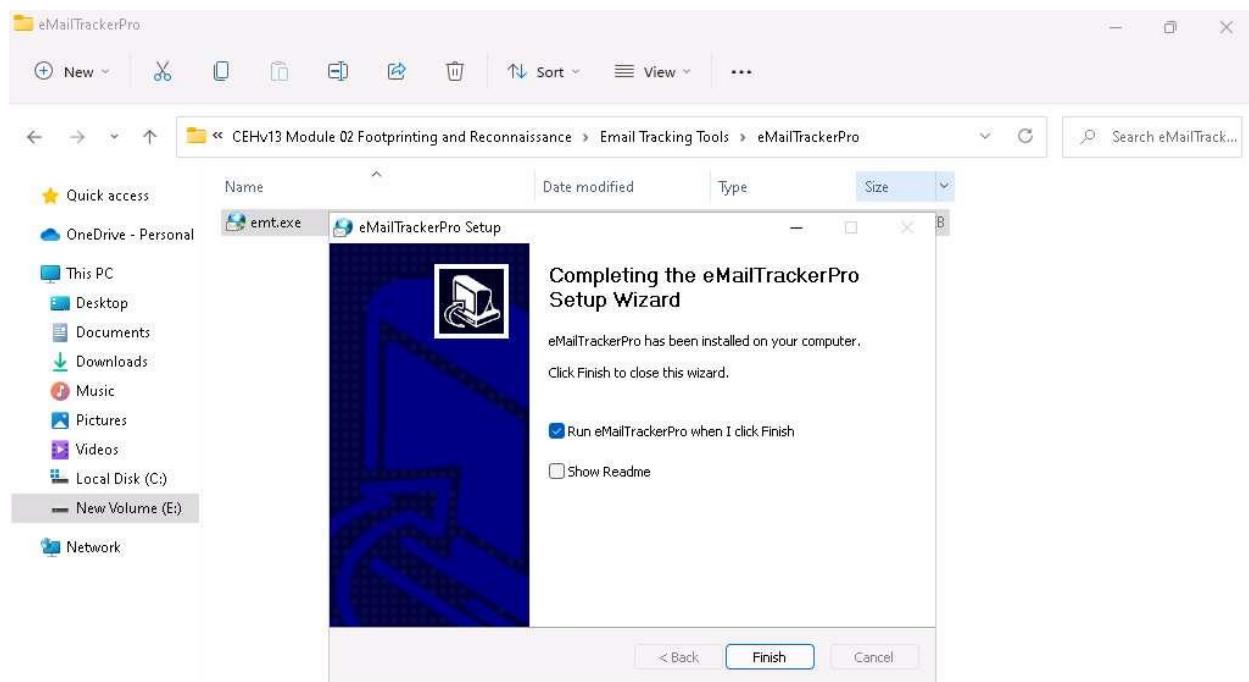
- Recipient's system IP address
- The GPS coordinates and map location of the recipient
- When an email message was received and read
- Type of server used by the recipient
- Operating system and browser information
- If a destructive email was sent
- The time spent reading the email
- Whether or not 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

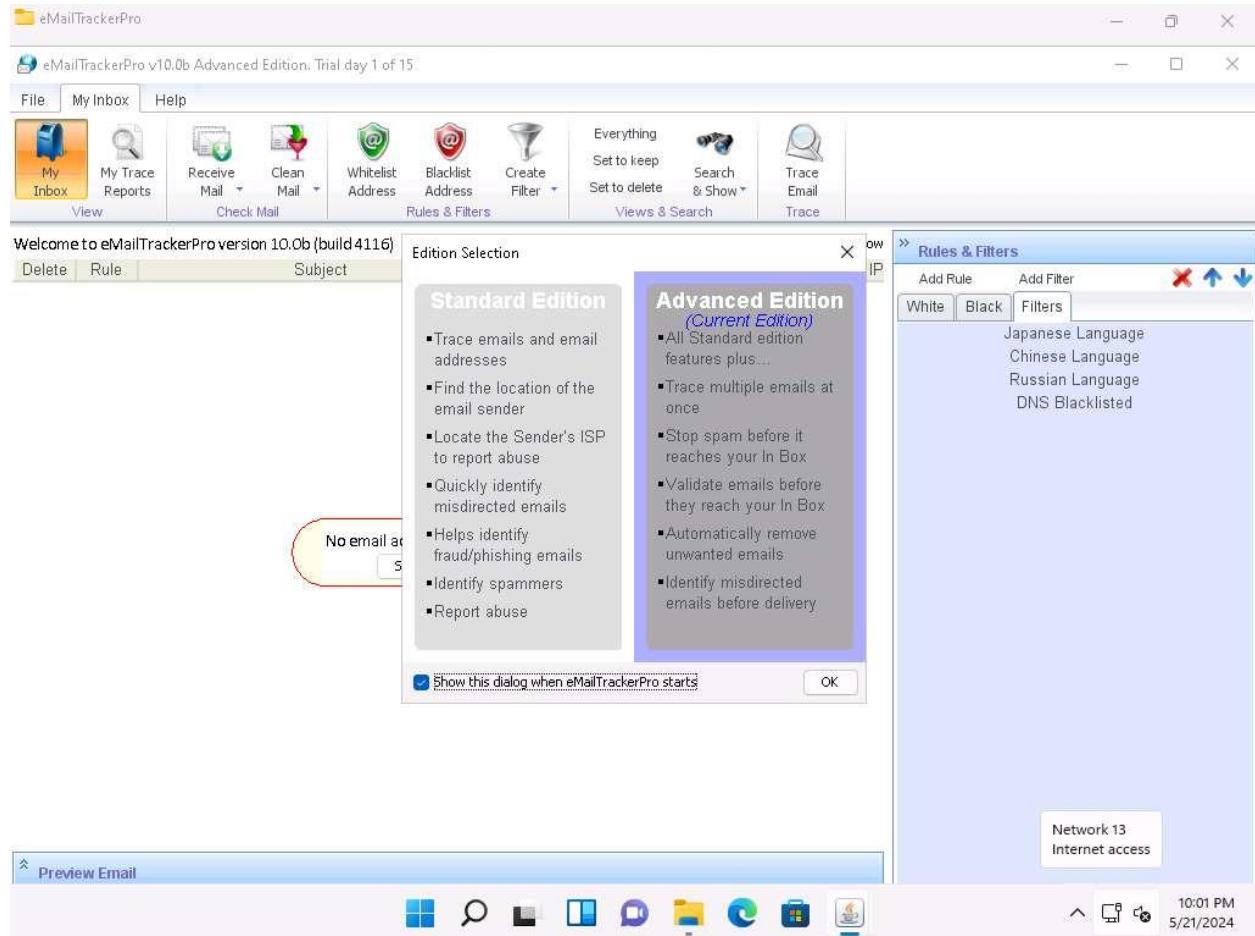
The email header is a crucial part of any email and it is considered a great source of information for any ethical hacker launching attacks against a target. An email header contains the details of the sender, routing information, addressing scheme, date, subject, recipient, etc. Additionally, the email 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.

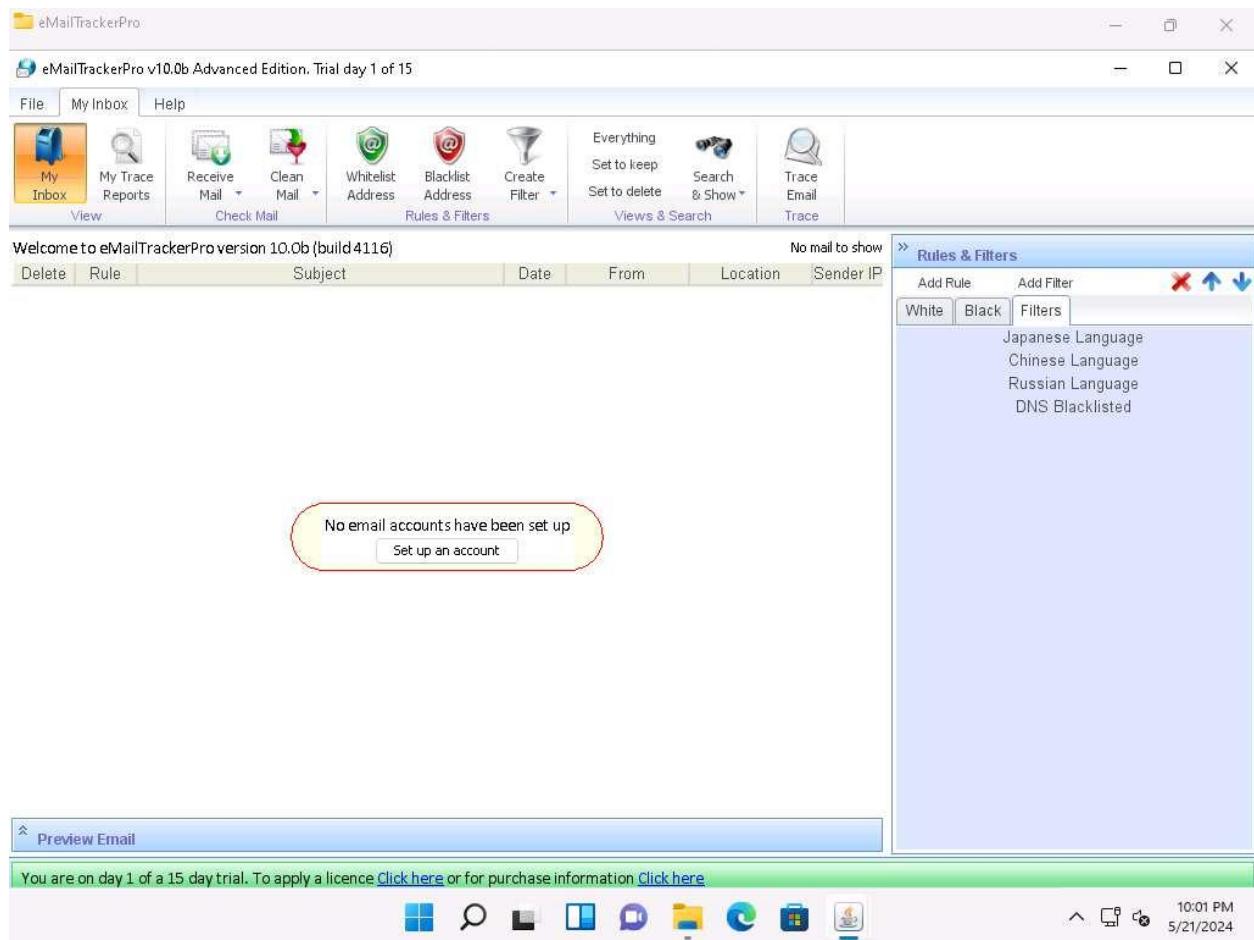
1. Click **Windows 11** to switch to the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv13 Module 02 Footprinting and Reconnaissance>Email Tracking Tools\EmailTrackerPro** and double-click **emt.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.
3. The **eMailTrackerPro 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.



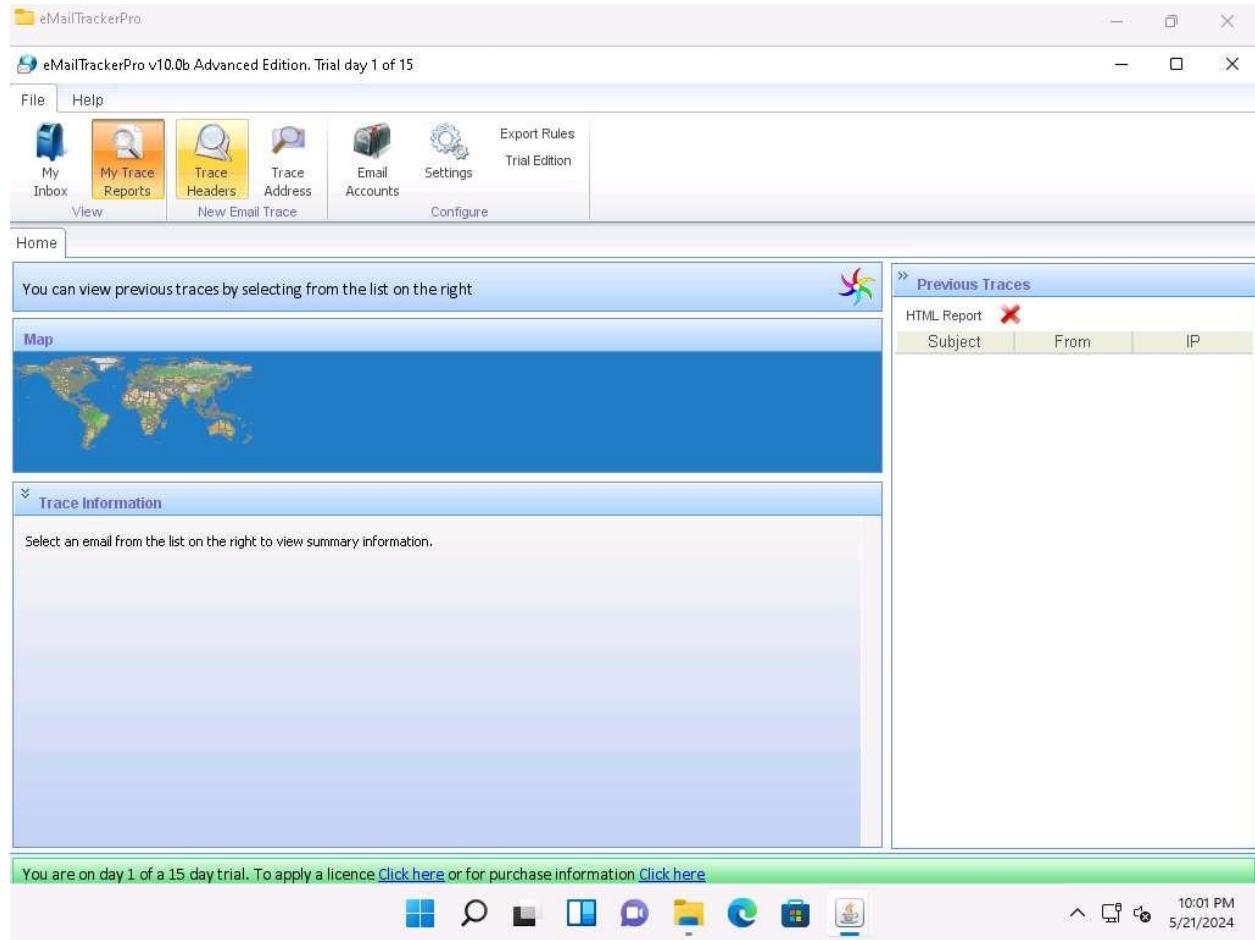
5. The main window of **eMailTrackerPro** appears along with the **Edition Selection** pop-up; click **OK**.



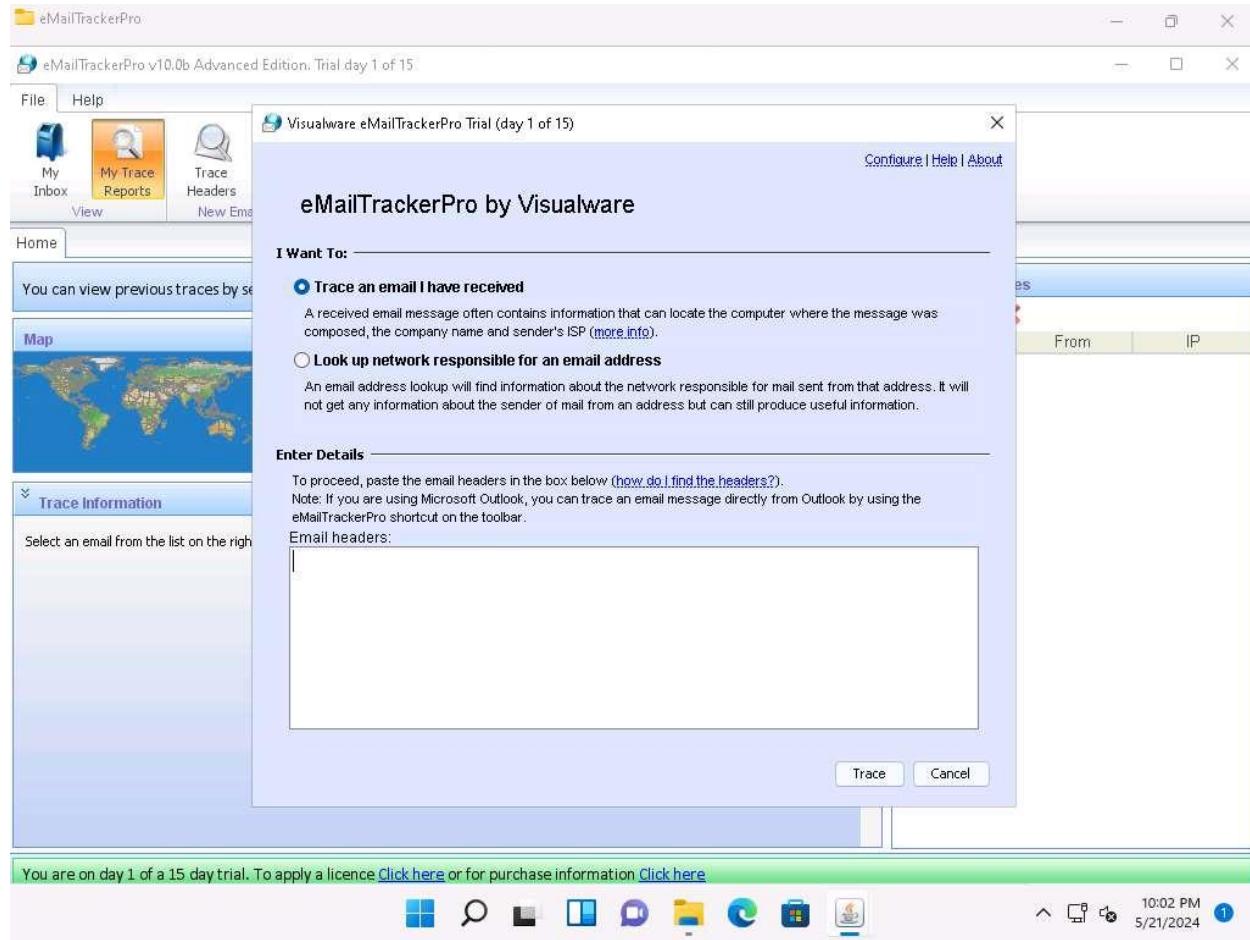
6. The **eMailTrackerPro** main window appears, as shown in the screenshot.



7. 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).
8. Click the **Trace Headers** icon from the **New Email Trace** section to start the trace.



9. 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.



10. 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.

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

The screenshot shows an email message in an Outlook client. The title bar says "Original message". The message header is shown in a table:

| | |
|-------------|---|
| Message ID | [REDACTED] le.com> |
| Created on: | 6 May 2024 at 21:54 (Delivered after 2 seconds) |
| From: | [REDACTED] @accounts.google.com> |
| To: | [REDACTED] @gmail.com |
| Subject: | Security alert |
| SPF: | PASS with IP 209.85.220.73 Learn more |
| DKIM: | 'PASS' with domain accounts.google.com Learn more |
| DMARC: | 'PASS' Learn more |

Below the table are two buttons: "Download original" and "Copy to clipboard".

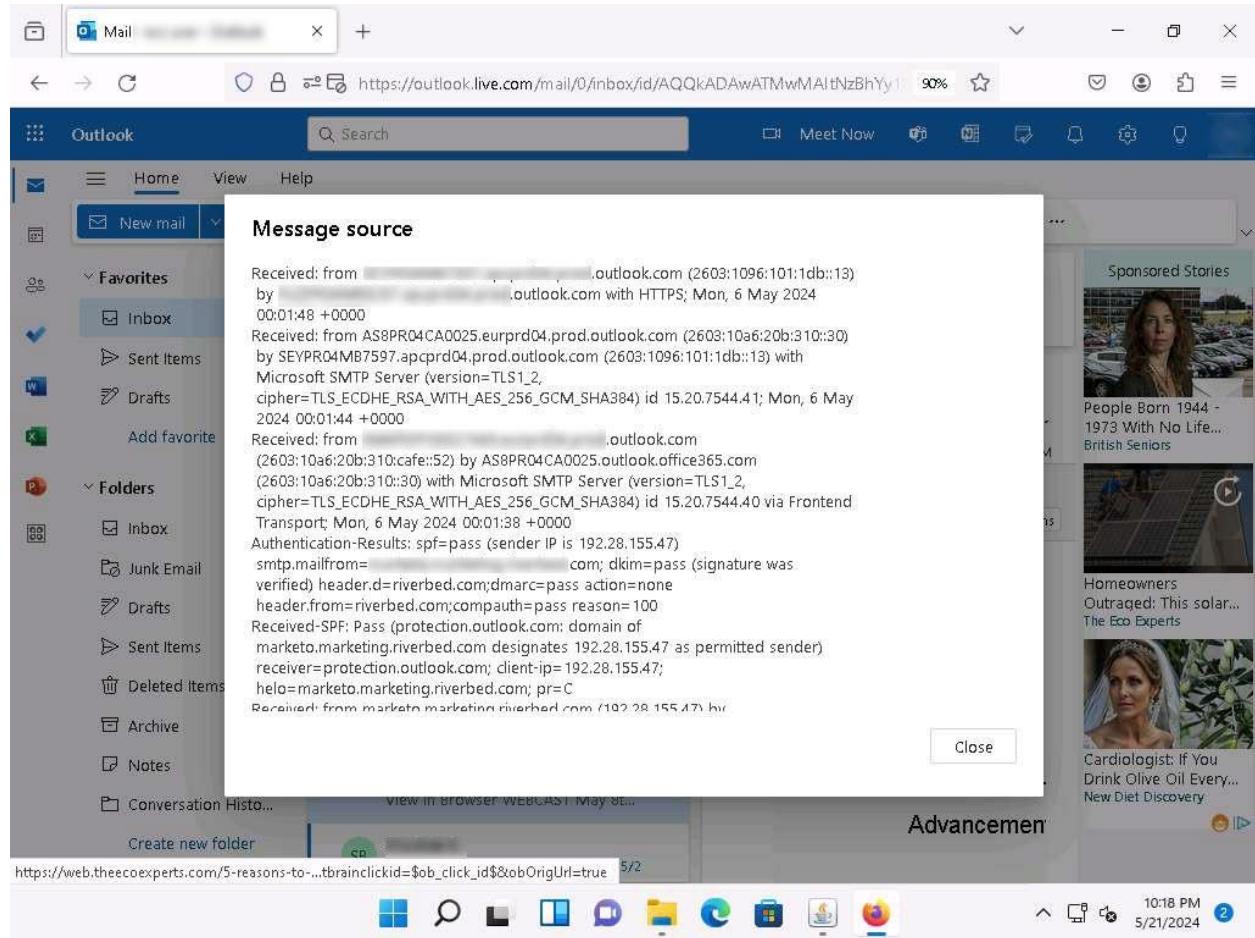
A red box highlights the "View message source" window, which contains the following text:

```
Delivered-To: [REDACTED].com
Received: by 2002:a17:522:8809:b0:57f:e019:7b93 with SMTP id cg9csp1708318pbv;
Mon, 6 May 2024 21:54:07 -0700 (PDT)
X-Received: by 2002:a05:6102:818:b0:47b:d3a9:e6ee with SMTP id g24-2002a056102081800b0047bd3a9e6eemr12195506vsb.
21.1715057647027;
Mon, 06 May 2024 21:54:07 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1715057647; cv=none;
d=google.com; s=arc-20160816;
b=H0zc59sx8UmB+i408qH491Zrt/Vmtm8kR/61Z0yGTUv+x445b+p4RFmgc5LqhKT1w
HiUHszyP7zwXNx819k39WjNTGFi99DEb3A3VYDxK/j1R3xPMGhb5qh1rqpPKmsuS1RYU
```

The status bar at the bottom right shows "10:11 PM 5/21/2024" and a notification icon.

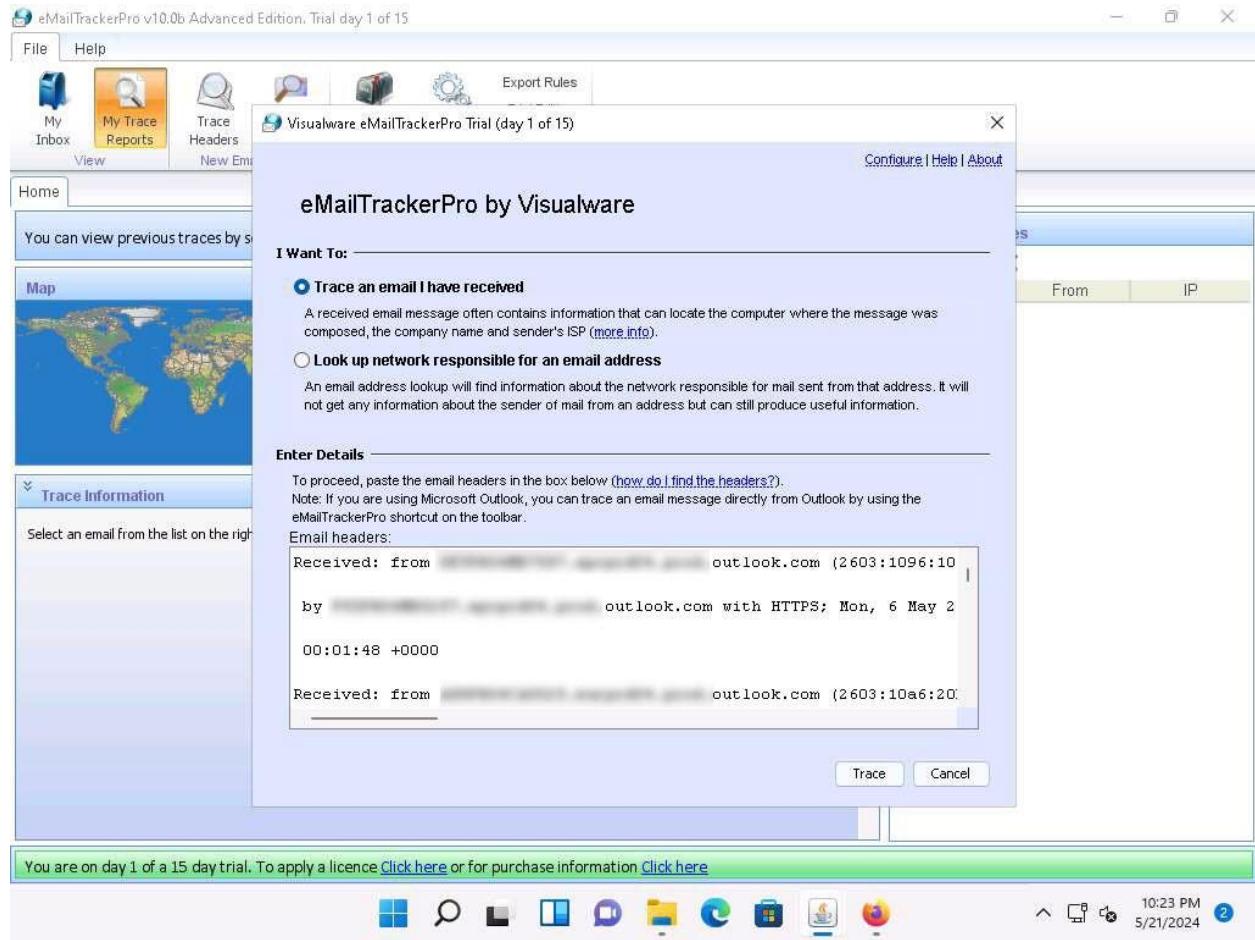
In **Outlook**, find the email header by following the steps:

- 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



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

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



12. The **My Trace Reports** window opens.
13. 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.

eMailTrackerPro v10.0b Advanced Edition. Trial day 1 of 15

File Help

My Inbox My Trace Reports Trace Headers Trace Address Email Accounts Settings Export Rules Trial Edition

View

Home Subject: Last Chance! ... X

The trace is complete, the information found is displayed on the right New Trace View Report

Map

Email Summary

From: [REDACTED]
To: [REDACTED]
Date: Sun, 5 May 2024 19:01:35 -0500 (CDT)
Subject: Last Chance! Register for Riverbed Launch Webcast
Location: [America]

Misdirected: No
Abuse Address: mktabuse@adobe.com
Abuse Reporting: To automatically generate an email abuse
From IP: 192.28.155.47

System Information:

- The system is running a mail server (***** port 25. This means that this system can be used to send emails)
- There is no HTTP server running on this system (the port 80 is free)
- There is no HTTPS server running on this system (the port 443 is free)
- There is no FTP server running on this system (the port 21 is free)

Network Whois

Domain Whois

Email Header

You are on day 1 of a 15 day trial. To apply a licence [Click here](#) or for purchase information [Click here](#)

Windows Start Taskbar 10:27 PM 5/21/2024

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

| # | Hop IP | Hop Name | Location |
| --- | --- | --- | --- |
| 1 | 10.1 | | |
| 2 | 172. | | |
| 3 | 192. | | |
| 4 | 185. | | (Australia) |
| 6 | 5.57 | lonap-gw-no-dns-yet.zayo.com | (Australia) |
| 10 | 64.1 | ae15.er4.iad10.us.zip.zayo.com | (America) |
| 11 | 128. | 128.177.77.186.IPYX-260031-911 | (America) |
| 12 | 208. | rt-bt-1-be-1.va5.ne.adobe.net | (America) |
| 13 | 208. | sr-cdbs-1-po-6.va5.omniture.com | (America) |

 A green banner at the bottom says 'You are on day 1 of a 15 day trial. To apply a licence Click here or for purchase information Click here'. The system tray shows standard icons like Task View, File Explorer, and Task Manager. The system clock shows 10:37 PM on 5/21/2024."/>

15. This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.
16. 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.
17. 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.

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.

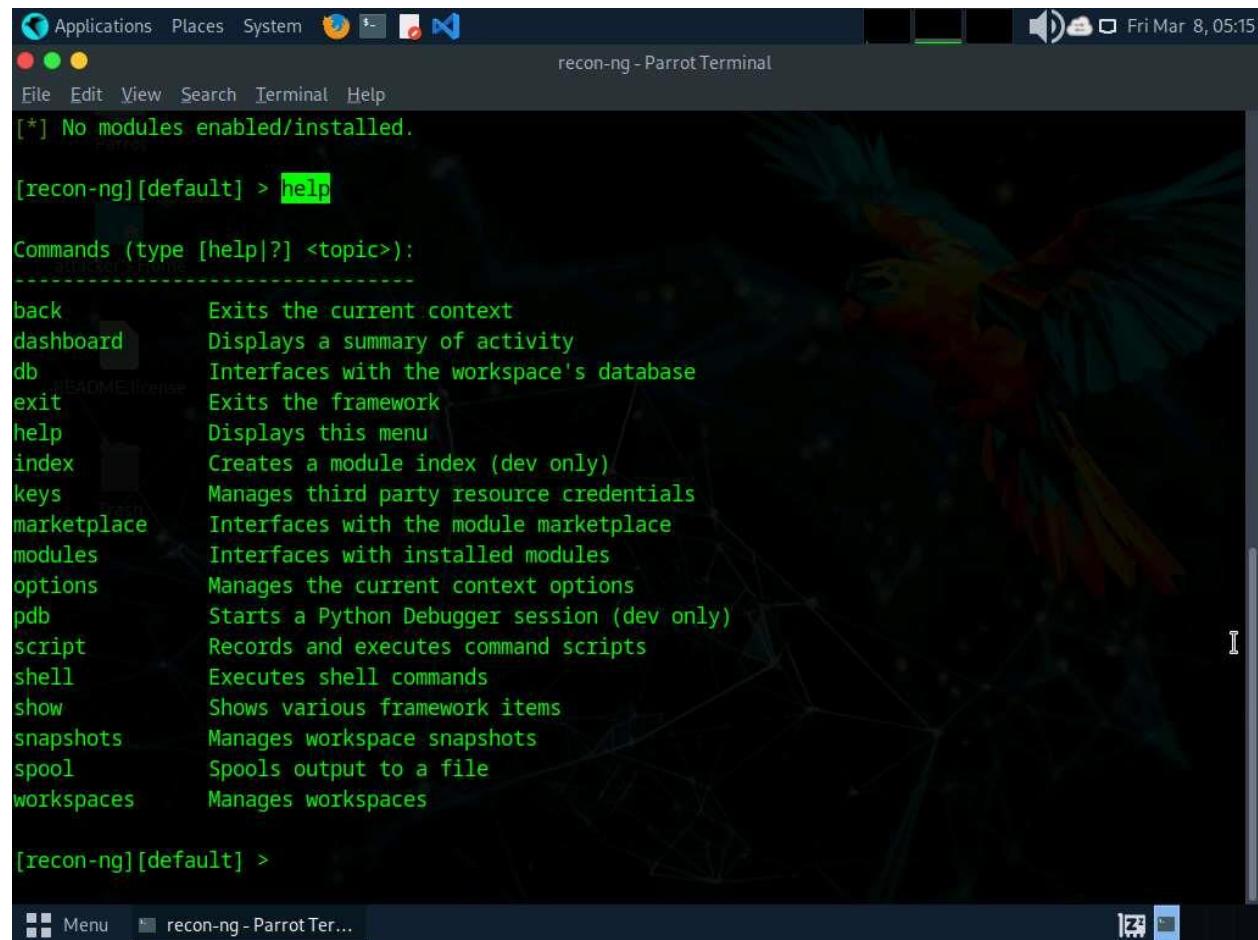
1. In the **Parrot Security** machine, open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
The password that you type will not be visible.
2. Now, run **cd** command to jump to the root directory and run **recon-ng** command to launch the application.

The screenshot shows a Parrot OS desktop environment. A terminal window titled "cd - Parrot Terminal" is open, displaying the following command sequence:

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] /home/attacker
# cd
[root@parrot] ~
# recon-ng
```

The desktop background features a colorful parrot. The taskbar at the bottom includes icons for the menu, workspace switching (Workspace 1), and system status.

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



The screenshot shows a Parrot OS desktop environment. A terminal window titled "recon-ng - Parrot Terminal" is open, displaying the help menu for the recon-ng framework. The terminal output is as follows:

```
[*] No modules enabled/installed.

[recon-ng][default] > help

Commands (type [help|?] <topic>):
-----
back           Exits the current context
dashboard      Displays a summary of activity
db              Interfaces with the workspace's database
exit           Exits the framework
help            Displays this menu
index          Creates a module index (dev only)
keys            Manages third party resource credentials
marketplace    Interfaces with the module marketplace
modules        Interfaces with installed modules
options        Manages the current context options
pdb             Starts a Python Debugger session (dev only)
script         Records and executes command scripts
shell          Executes shell commands
show           Shows various framework items
snapshots      Manages workspace snapshots
spool          Spools output to a file
workspaces     Manages workspaces

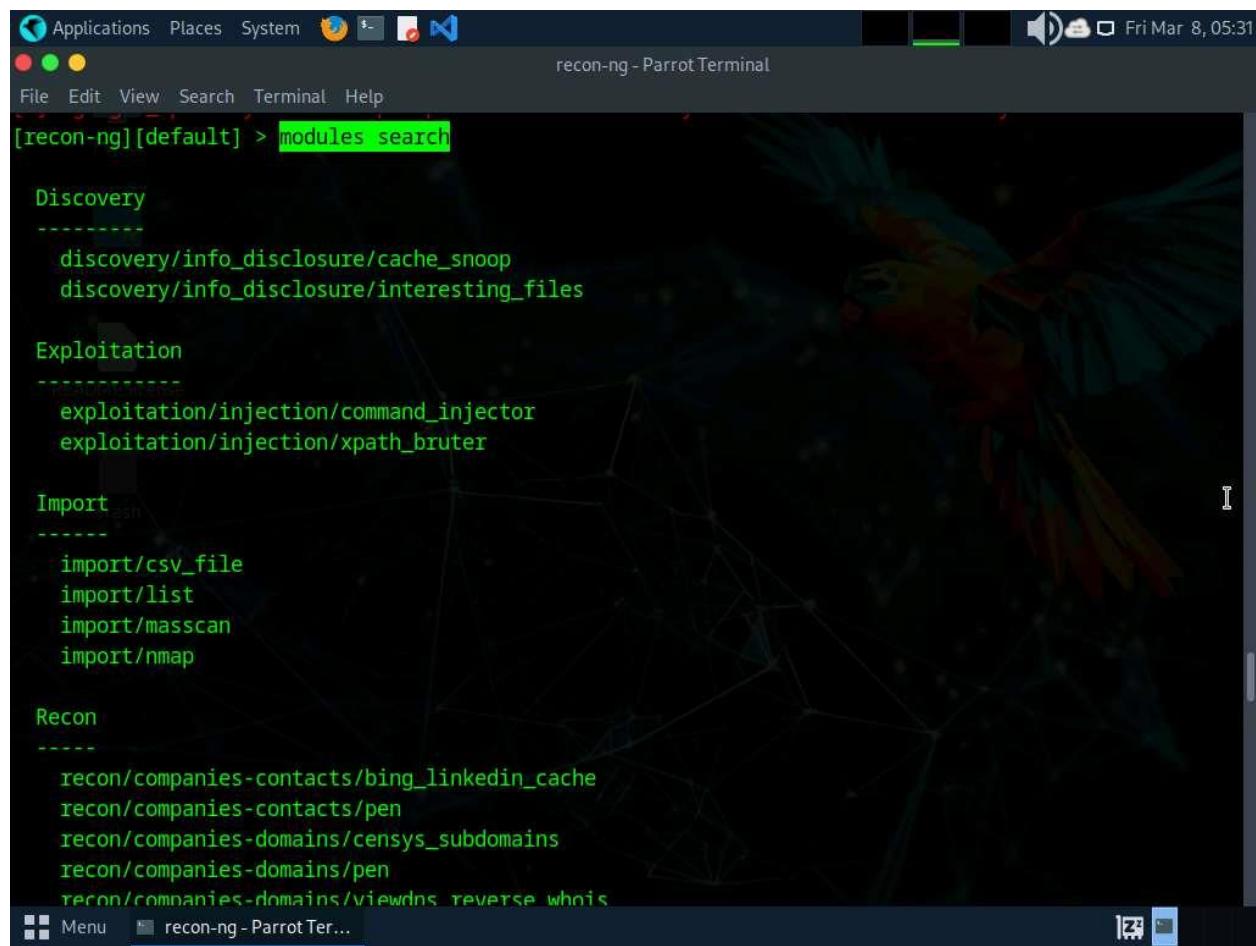
[recon-ng][default] >
```

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

Ignore the errors while running the command.

```
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-hosts/censys_org
[*] Module installed: recon/companies-hosts/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
[*] Module installed: recon/companies-multi/whois_miner
[*] Module installed: recon/contacts-contacts/abc
[*] Module installed: recon/contacts-contacts/mailtester
[*] Module installed: recon/contacts-contacts/mangle
[*] Module installed: recon/contacts-contacts/unmangle
```

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



```
[recon-ng] [default] > modules search

Discovery
-----
discovery/info_disclosure/cache_snoop
discovery/info_disclosure/interesting_files

Exploitation
-----
exploitation/injection/command_injector
exploitation/injection/xpath_bruter

Import
-----
import/csv_file
import/list
import/masscan
import/nmap

Recon
-----
recon/companies-contacts/bing_linkedin_cache
recon/companies-contacts/pen
recon/companies-domains/censys_subdomains
recon/companies-domains/pen
recon/companies-domains/viewdns_reverse_whois
```

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

```
Applications Places System Firefox S- P recon-ng - Parrot Terminal
File Edit View Search Terminal Help
recon/profiles-profiles/profiler
recon/profiles-profiles/twitter_mentioned
recon/profiles-profiles/twitter_mentions
recon/profiles-repositories/github_repos
recon/repositories-profiles/github_commits
recon/repositories-vulnerabilities/gists_search
recon/repositories-vulnerabilities/github_dorks

Reporting
-----
reporting/csv
reporting/html
reporting/json
reporting/list
reporting/proxifier
reporting/pushpin
reporting/xlsx
reporting/xml

[recon-ng] [default] > workspaces
Manages workspaces

Usage: workspaces <create|list|load|remove> [...]

[recon-ng] [default] >
```

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

The screenshot shows a terminal window titled "recon-ng - Parrot Terminal". The terminal is displaying the output of the command "[recon-ng] [default] > workspaces create CEH". The output consists of numerous warning messages in red text, indicating that various API keys are not set and their respective modules will likely fail at runtime. These warnings are grouped by module name, such as "bing_api", "recon/companies-contacts/censys_email_address", "censysio_id", etc. The terminal window has a standard Linux desktop interface with icons for Applications, Places, System, and various system status indicators like battery level and signal strength.

```
[recon-ng] [default] > workspaces create CEH
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-contacts/censys_email_address' disabled. Dependency required: 'me 'CensysIPv4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
[!] 'censysio_id' key not set. censys_subdomains module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_subdomains module will likely fail at runtime. See 'keys add'.
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-hosts/censys_org' disabled. Dependency required: 'me 'CensysIPv4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
[!] Module 'recon/companies-hosts/censys_tls_subjects' disabled. Dependency required: 'me 'CensysIPv4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_org module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_breach module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_paste module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_api' key not set. fullcontact module will likely fail at runtime. See 'keys add'.
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-companies/censys_companies' disabled. Dependency required: 'me 'CensysIPv4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/__init__.py)'.
[!] 'whoxy_api' key not set. whoxy_whois module will likely fail at runtime. See 'keys add'.
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: "'PyPDF3'".
[!] Module 'recon/domains-credentials/pwnedlist/account_creds' disabled. Dependency required: "'pyaes'".
```

10. 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.

The screenshot shows a terminal window titled "recon-ng - Parrot Terminal" running on a Parrot OS desktop environment. The terminal displays the output of the command "[recon-ng] [CEH] > workspaces list". The output shows a table of workspaces:

| Workspaces | Modified |
|------------|---------------------|
| CEH | 2024-03-08 05:32:47 |
| default | 2024-03-08 05:14:49 |

11. Add a domain in which you want to perform network reconnaissance.
12. Issue the command **db insert domains**.
13. 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.
14. You can view the added domain by issuing the **show domains** command, as shown in the screenshot.

The screenshot shows a terminal window titled "recon-ng - Parrot Terminal" running on a Parrot OS desktop environment. The terminal displays the following commands and their outputs:

```
[!] 'github_api' key not set. github_dorks module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[recon-ng][CEH] > workspaces list

+-----+
| Workspaces |      Modified   |
+-----+
| CEH        | 2024-03-08 05:32:47 |
| default    | 2024-03-08 05:14:49 |
+-----+

[recon-ng][CEH] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][CEH] > show domains

+-----+
| rowid |      domain     | notes |      module   |
+-----+
| 1     | certifiedhacker.com |       | user_defined |
+-----+

[*] 1 rows returned
[recon-ng][CEH] >
```

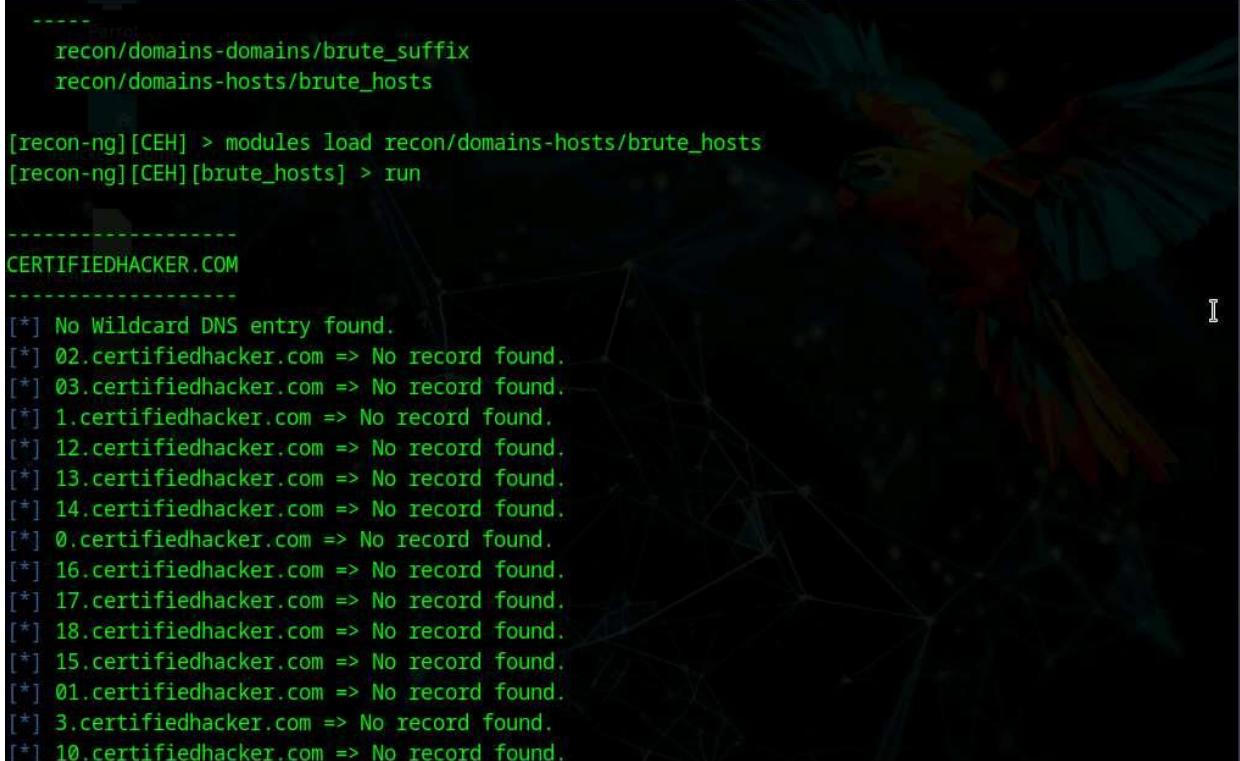
15. Harvest the hosts-related information associated with **certifiedhacker.com** by loading network reconnaissance modules such as `brute_hosts`, `Netcraft`, and `Bing`.
16. Issue **modules load brute** command to view all the modules related to brute forcing. In this task, we will be using the **recon/domains-hosts/brute_hosts**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

The screenshot shows a terminal window titled "recon-ng - Parrot Terminal" running on a Parrot OS desktop environment. The terminal displays the following session:

```
domain (TEXT): certifiedhacker.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][CEH] > show domains
+-----+
| rowid | domain | notes | module |
+-----+
| 1 | certifiedhacker.com | | user_defined |
+-----+
[*] 1 rows returned
[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.
Exploitation
-----
exploitation/injection/xpath_bruter
Recon
-----
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts

[recon-ng][CEH] >
```

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



Applications Places System recon-ng - Parrot Terminal

```
File Edit View Search Terminal Help

-----  
recon/domains-domains/brute_suffix  
recon/domains-hosts/brute_hosts

[recon-ng][CEH] > modules load recon/domains-hosts/brute_hosts
[recon-ng][CEH][brute_hosts] > run

-----
CERTIFIEDHACKER.COM
-----
[*] No Wildcard DNS entry found.
[*] 02.certifiedhacker.com => No record found.
[*] 03.certifiedhacker.com => No record found.
[*] 1.certifiedhacker.com => No record found.
[*] 12.certifiedhacker.com => No record found.
[*] 13.certifiedhacker.com => No record found.
[*] 14.certifiedhacker.com => No record found.
[*] 0.certifiedhacker.com => No record found.
[*] 16.certifiedhacker.com => No record found.
[*] 17.certifiedhacker.com => No record found.
[*] 18.certifiedhacker.com => No record found.
[*] 15.certifiedhacker.com => No record found.
[*] 01.certifiedhacker.com => No record found.
[*] 3.certifiedhacker.com => No record found.
[*] 10.certifiedhacker.com => No record found.
[*] 11.certifiedhacker.com => No record found.
```

Menu recon-ng - Parrot Ter...

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

```
[*] young.certifiedhacker.com => No record found.
[*] yt.certifiedhacker.com => No record found.
[*] yellow.certifiedhacker.com => No record found.
[*] yu.certifiedhacker.com => No record found.
[*] x.certifiedhacker.com => No record found.
[*] z-log.certifiedhacker.com => No record found.
[*] za.certifiedhacker.com => No record found.
[*] zera.certifiedhacker.com => No record found.
[*] yankee.certifiedhacker.com => No record found.
[*] zeus.certifiedhacker.com => No record found.
[*] wusage.certifiedhacker.com => No record found.
[*] y.certifiedhacker.com => No record found.
[*] zulu.certifiedhacker.com => No record found.
[*] z.certifiedhacker.com => No record found.
[*] ye.certifiedhacker.com => No record found.
[*] zw.certifiedhacker.com => No record found.
[*] zebra.certifiedhacker.com => No record found.
[*] zlog.certifiedhacker.com => No record found.
[*] zm.certifiedhacker.com => No record found.

-----
SUMMARY
-----
[*] 23 total (20 new) hosts found.
[recon-ng][CEH][brute_hosts] >
```

20. 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.

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

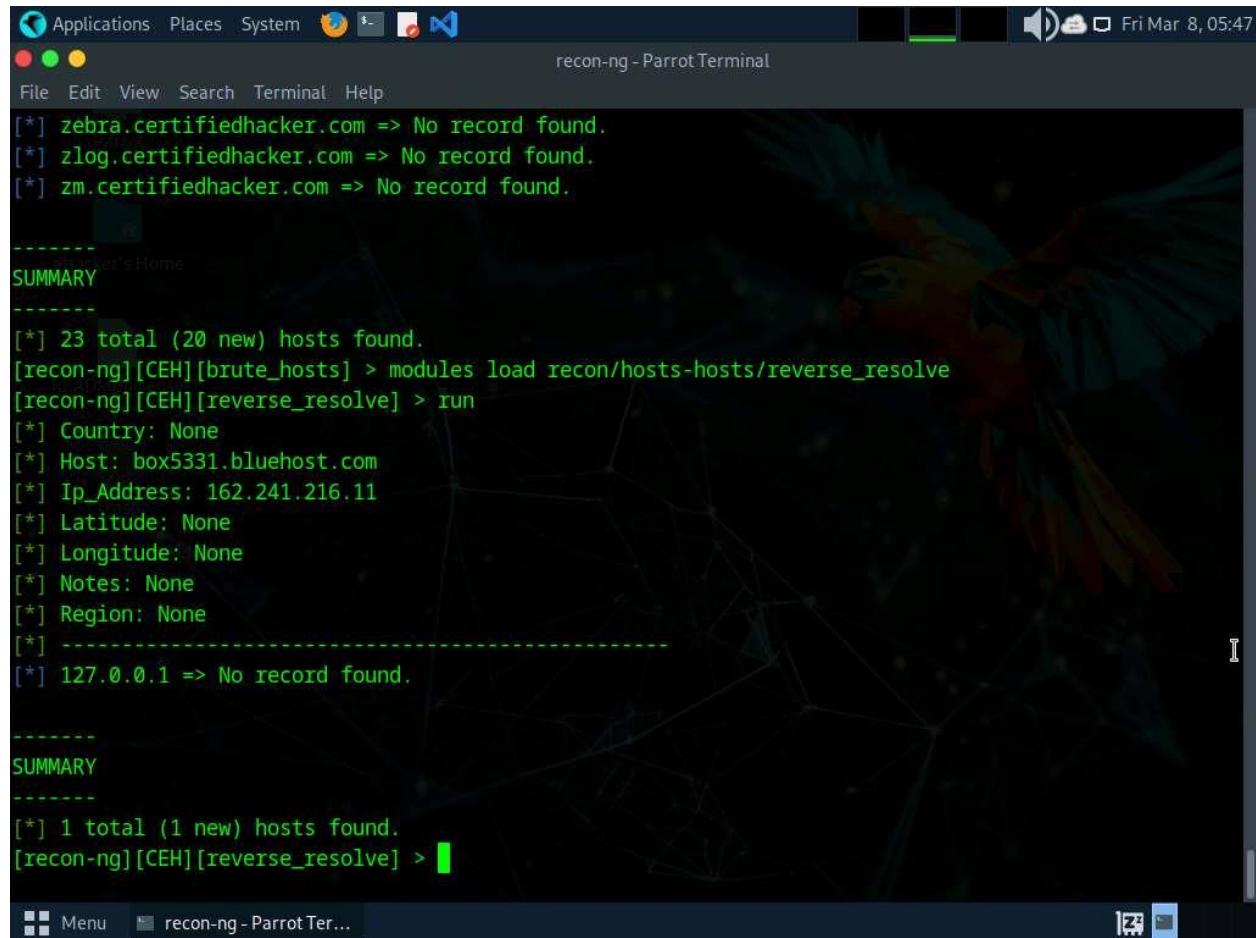
To resolve hosts using the Bing module, use the following commands:

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

21. Now, perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames.
22. 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.

23. Run the **modules load recon/hosts-hosts/reverse_resolve** command to load the module.

24. Issue the **run** command to begin the reverse lookup.



The screenshot shows a terminal window titled "recon-ng - Parrot Terminal". The terminal displays the following command-line session:

```
[*] zebra.certifiedhacker.com => No record found.  
[*] zlog.certifiedhacker.com => No record found.  
[*] zm.certifiedhacker.com => No record found.  
  
-----  
[*] 23 total (20 new) hosts found.  
[recon-ng][CEH][brute_hosts] > modules load recon/hosts-hosts/reverse_resolve  
[recon-ng][CEH][reverse_resolve] > run  
[*] Country: None  
[*] Host: box5331.bluehost.com  
[*] Ip_Address: 162.241.216.11  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] -----  
[*] 127.0.0.1 => No record found.  
  
-----  
[*] 1 total (1 new) hosts found.  
[recon-ng][CEH][reverse_resolve] >
```

25. 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.

```
[*] 1 total (1 new) hosts found.
[recon-ng][CEH][reverse_resolve] > show hosts

+-----+
| rowid |          host      |   ip_address | region | country | latitude | longitude |
|       | module      |               |           |          |          |          |
+-----+
| 1    | autodiscover.certifiedhacker.com | 162.241.216.11 |       |       |       |       |
|     | brute_hosts |               |           |          |          |          |
| 2    | blog.certifiedhacker.com        | 162.241.216.11 |       |       |       |       |
|     | brute_hosts |               |           |          |          |          |
| 3    | demo.certifiedhacker.com       | 162.241.216.11 |       |       |       |       |
|     | brute_hosts |               |           |          |          |          |
| 4    | events.certifiedhacker.com    | 162.241.216.11 |       |       |       |       |
|     | brute_hosts |               |           |          |          |          |
| 5    | certifiedhacker.com           |               |       |       |       |       |
|     | brute_hosts |               |           |          |          |          |
| 6    | ftp.certifiedhacker.com       |               |       |       |       |       |
|     | brute_hosts |               |           |          |          |          |
| 7    | ftp.certifiedhacker.com       | 162.241.216.11 |       |       |       |       |
|     | brute_hosts |               |           |          |          |          |
| 8    | mail.certifiedhacker.com     |               |       |       |       |       |
|     | brute_hosts |               |           |          |          |          |
+-----+
```

26. Now, use the **back** command to go back to the CEH attributes terminal.
27. Now, that you have harvested several hosts, we will prepare a report containing all the hosts.
28. 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**.
29. Run the **modules load reporting/html** command.
30. 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**).

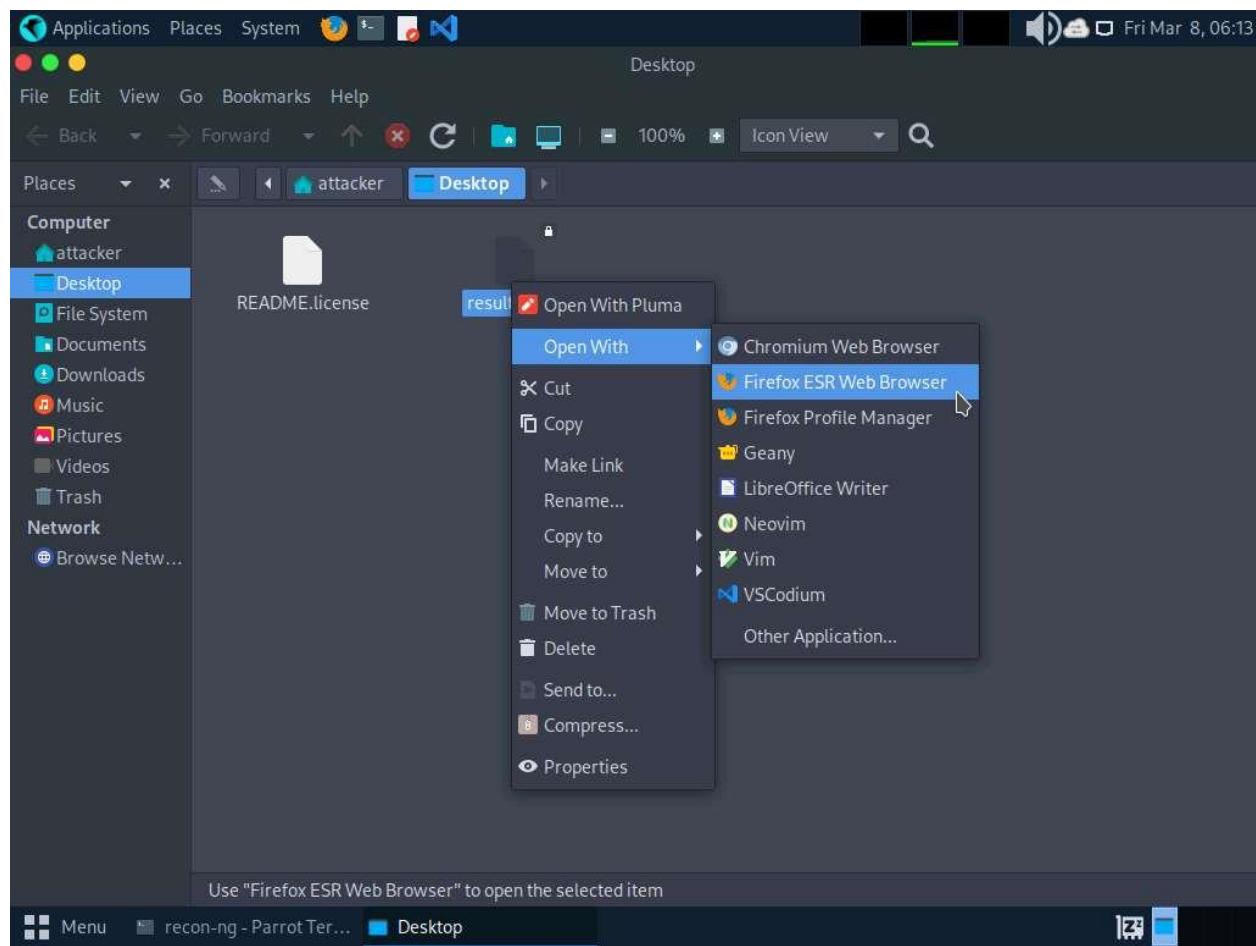
- **options set CUSTOMER Certifiedhacker Networks** (since you have performed network reconnaissance on **certifiedhacker.com** domain).
31. Use the **run** command and press **Enter** to create a report for all the hosts that have been harvested.

```

Applications Places System Terminal Help recon-ng - Parrot Terminal
File Edit View Search Terminal Help
| 18 | webmail.certifiedhacker.com | 162.241.216.11 |
|    | brute_hosts      | |
| 19 | www.certifiedhacker.com | |
|    | brute_hosts      | |
| 20 | www.certifiedhacker.com | 162.241.216.11 |
|    | brute_hosts      | |
| 21 | box5331.bluehost.com | 162.241.216.11 |
|    | reverse_resolve | |
+-----+
[*] 21 rows returned
[recon-ng][CEH][reverse_resolve] > back
[recon-ng][CEH] > modules load reporting/html
[recon-ng][CEH][html] > options set FILENAME /home/attacker/Desktop/results.html
FILENAME => /home/attacker/Desktop/results.html
[recon-ng][CEH][html] > options set CREATOR Jason
CREATOR => Jason
[recon-ng][CEH][html] > options set CUSTOMER Certifiedhacker Networks
CUSTOMER => Certifiedhacker Networks
[recon-ng][CEH][html] > run
[*] Report generated at '/home/attacker/Desktop/results.html'.
[recon-ng][CEH][html] >

```

32. The generated report is saved to **/home/attacker/Desktop/**.
33. 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.



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

The screenshot shows a Firefox browser window with the title "Recon-ng Reconnaissance". The address bar displays "file:///home/attacker/Desktop/results.html". Below the address bar is a toolbar with various icons. The main content area is a table titled "[-] Hosts" with the following data:

| host | ip_address | region | country | latitude | longitude | notes | module |
|----------------------------------|----------------|--------|---------|----------|-----------|-------|-----------------|
| autodiscover.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |
| blog.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |
| box5331.bluehost.com | 162.241.216.11 | | | | | | reverse_resolve |
| certifiedhacker.com | | | | | | | brute_hosts |
| demo.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |
| events.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |
| ftp.certifiedhacker.com | | | | | | | brute_hosts |
| imap.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |
| imap.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |
| localhost.certifiedhacker.com | 127.0.0.1 | | | | | | brute_hosts |
| mail.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |
| mail.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |
| news.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |
| pop.certifiedhacker.com | | | | | | | brute_hosts |
| pop.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |
| smtp.certifiedhacker.com | | | | | | | brute_hosts |
| smtp.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |
| webmail.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |
| www.certifiedhacker.com | | | | | | | brute_hosts |
| www.certifiedhacker.com | 162.241.216.11 | | | | | | brute_hosts |

Created by: Jason
Fri, Mar 08 2024 06:06:21

At the bottom, there are navigation buttons for "Menu", "recon-ng - Parrot Ter...", "Desktop", and the title bar "Recon-ng Reconnaiss...".

36. Close all open windows.
37. Until now, we have used the Recon-**ng** tool to perform network reconnaissance on a target domain
38. Now, we will use Recon-**ng** to gather personnel information.
39. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
The password that you type will not be visible.
40. Run **cd** command to jump to the root directory and run **recon-**ng**** command.
41. Add a workspace by issuing the command **workspaces create reconnaissance** and press **Enter**. This creates a workspace named **reconnaissance**.

```
Applications Places System Firefox Terminal recon-ng - Parrot Terminal
File Edit View Search Terminal Help
attacker's Home Sponsored by...
README LICENSE
Trash results.html
[85] Recon modules
[13] Disabled modules
[8] Reporting modules
[4] Import modules
[2] Exploitation modules
[2] Discovery modules

[recon-ng] [default] > workspace create reconnaissance
```

42. Set a domain and perform footprinting on it to extract contacts available in the domain.
43. 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.
44. Run the **info command** command to view the options required to run this module.
45. Run **options set SOURCE facebook.com** command to add facebook.com as a target domain.

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

The screenshot shows a terminal window titled "recon-ng - Parrot Terminal". The terminal displays the following command-line session:

```
[recon-ng][reconnaissance] > modules load recon/domains-contacts/whois_pocs
[recon-ng][reconnaissance][whois_pocs] > info command

    Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
    Version: 1.0

Description:
    Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
    'contacts' table with the results.

Options:
    Name      Current Value  Required  Description
    -----  -----  -----  -----
    SOURCE    default        yes       source of input (see 'info' for details)

Source Options:
    default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
    <string>    string representing a single input
    <path>      path to a file containing a list of inputs
    query <sql>  database query returning one column of inputs

[recon-ng][reconnaissance][whois_pocs] > options set SOURCE facebook.com
SOURCE => facebook.com
[recon-ng][reconnaissance][whois_pocs] >
```

46. 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

Results might differ when you perform the lab.

```
[recon-ng] [reconnaissance] [whois_pocs] > run
-----
FACEBOOK.COM
-----
[*] URL: http://whois.arin.net/rest/pocs;domain=facebook.com
[*] URL: http://whois.arin.net/rest/poc/BST184-ARIN
[*] Country: United States
[*] Email: bstout@facebook.com
[*] First_Name: Brandon
[*] Last_Name: Stout
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Chicago, IL
[*] Title: Whois contact
[*] -----
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
[*] Country: United States
[*] Email: domain@facebook.com
[*] First_Name: None
[*] Last_Name: Operations
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Menlo Park, CA
```

47. Until now, we have obtained contacts related to the domains. Note down these contacts' names. Close all the open windows.
48. Now, we will use Recon-**ng** to extract a list of subdomains and IP addresses associated with the target URL.
49. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
The password that you type will not be visible.
50. Now, run **cd** command to jump to the root directory and run **recon-**ng**** command.
51. To extract a list of subdomains and IP addresses associated with the target URL, we need to load the **recon/domains-hosts/hackertarget** module.
52. Run the **modules load recon/domains-hosts/hackertarget** command and run **options set SOURCE certifiedhacker.com** command.

53. 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.

```
[recon-ng] [default] > modules load recon/domains-hosts/hackertarget
[recon-ng] [default][hackertarget] > options set SOURCE certifiedhacker.com
SOURCE => certifiedhacker.com
[recon-ng] [default][hackertarget] > run

-----
CERTIFIEDHACKER.COM
-----
[*] Country: None
[*] Host: autodiscover.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: blog.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[ Menu ] [x] recon-ng - Parrot Ter...
```

54. This concludes the demonstration of gathering host information of the target domain and gathering personnel information of a target organization.

55. 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.

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.

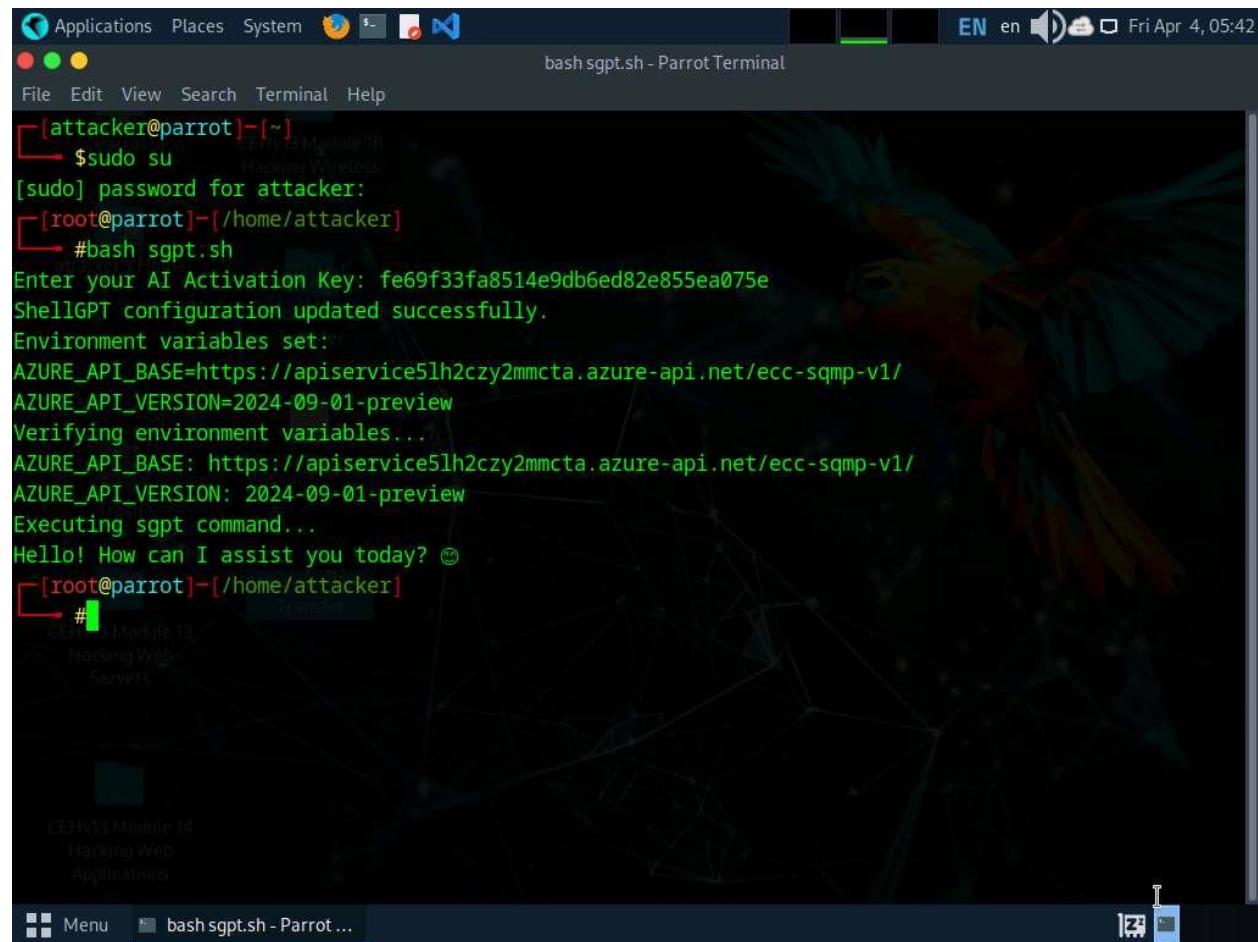
The commands generated by ShellGPT may vary depending on the prompt used and the tools available on the machine. Due to these variables, the output generated by ShellGPT might differ from what is shown in the screenshots. These differences arise from the dynamic nature of the AI's processing and the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

The password that you type will not be visible.

- Run **bash sgpt.sh** command to configure ShellGPT and the AI activation key.

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 - CEHv13](#).



The screenshot shows a terminal window titled "bash sgpt.sh - Parrot Terminal". The terminal output is as follows:

```
[attacker@parrot] [~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot] [~/home/attacker]
# bash sgpt.sh
Enter your AI Activation Key: fe69f33fa8514e9db6ed82e855ea075e
ShellGPT configuration updated successfully.
Environment variables set:
AZURE_API_BASE=https://apiservice5lh2czy2mmcta.azure-api.net/ecc-sqmp-v1/
AZURE_API_VERSION=2024-09-01-preview
Verifying environment variables...
AZURE_API_BASE: https://apiservice5lh2czy2mmcta.azure-api.net/ecc-sqmp-v1/
AZURE_API_VERSION: 2024-09-01-preview
Executing sgpt command...
Hello! How can I assist you today? 😊
[root@parrot] [~/home/attacker]
#
```

The terminal window is part of a desktop environment with a dark theme. The desktop background features a colorful parrot. Icons for various modules like "CEHv13 Module 13 Hacking Wireless Networks" and "CEHv13 Module 14 Hacking Web Applications" are visible in the dock at the bottom.

- 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.

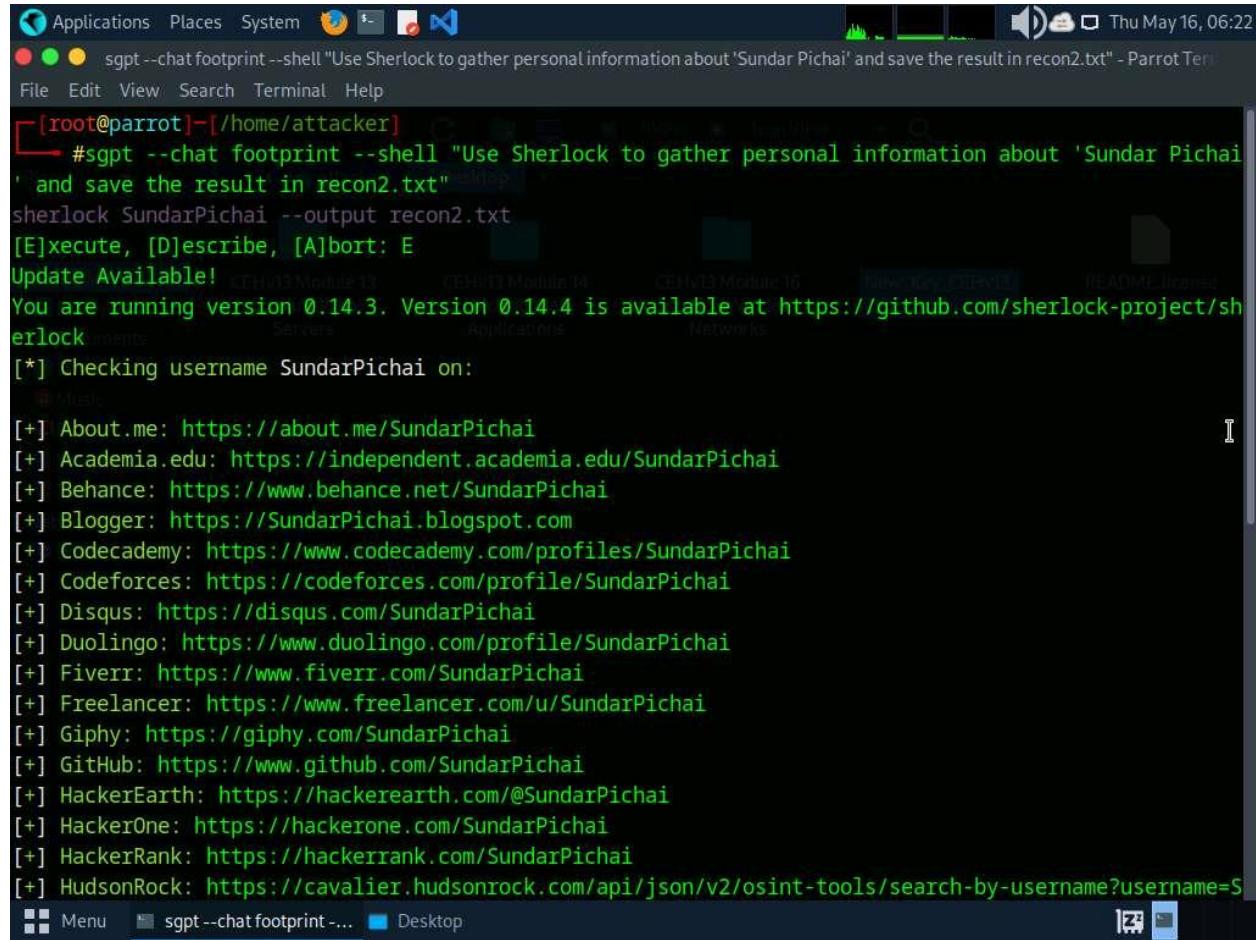
In the prompt type **E** and press **Enter** to execute the command.

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


```
[*] Target: microsoft.com
[*] Searching Baidu.
[*] No IPs found.
[*] Emails found: 3
a-yuwa@microsoft.com
contactopencode@microsoft.com
emailopencode@microsoft.com
[*] Hosts found: 22
.windowsupdate.microsoft.com
2Fdevblogs.microsoft.com
account.microsoft.com
azure.microsoft.com
clarity.microsoft.com
devblogs.microsoft.com
docs.microsoft.com
go.microsoft.com
learn.microsoft.com
learning.microsoft.com
login.microsoft.com
```

5. 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.



The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "sgpt --chat footprint --shell "Use Sherlock to gather personal information about 'Sundar Pichai' and save the result in recon2.txt" - Parrot Terminal". The terminal content displays the execution of the command and its output, which is a list of URLs for various online profiles of Sundar Pichai.

```
[root@parrot]~[/home/attacker]
#sgpt --chat footprint --shell "Use Sherlock to gather personal information about 'Sundar Pichai' and save the result in recon2.txt"
sherlock SundarPichai --output recon2.txt
[E]xecute, [D]escribe, [A]bort: E
Update Available!
You are running version 0.14.3. Version 0.14.4 is available at https://github.com/sherlock-project/sherlock
[*] Checking username SundarPichai on:
[+] About.me: https://about.me/SundarPichai
[+] Academia.edu: https://independent.academia.edu/SundarPichai
[+] Behance: https://www.behance.net/SundarPichai
[+] Blogger: https://SundarPichai.blogspot.com
[+] Codecademy: https://www.codecademy.com/profiles/SundarPichai
[+] Codeforces: https://codeforces.com/profile/SundarPichai
[+] Disqus: https://disqus.com/SundarPichai
[+] Duolingo: https://www.duolingo.com/profile/SundarPichai
[+] Fiverr: https://www.fiverr.com/SundarPichai
[+] Freelancer: https://www.freelancer.com/u/SundarPichai
[+] Giphy: https://giphy.com/SundarPichai
[+] GitHub: https://www.github.com/SundarPichai
[+] HackerEarth: https://hackerearth.com/@SundarPichai
[+] HackerOne: https://hackerone.com/SundarPichai
[+] HackerRank: https://hackerrank.com/SundarPichai
[+] HudsonRock: https://cavalier.hudsonrock.com/api/json/v2/osint-tools/search-by-username?username=SundarPichai
```

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

The screenshot shows a terminal window titled "ls --color=auto - ParrotTerminal". The command entered was "#sgpt --chat footprint --shell "Use Sherlock to gather personal information about Sundar Pichai and save the result in recon2.txt"" followed by "sherlock Sundar Pichai --print-found > recon2.txt". The terminal then displays "[E]xecute, [D]escribe, [A]bort: E". The user then types "#ls" to list the contents of the directory, which includes files like jwt_tool, lazys3-master, Maltego.v4.6.0.deb, microsoft_emails.json, microsoft_emails.xml, Music, HTML_theft, passwords.txt, PhoneExploit-Pro, Photon, Pichai.txt, Pictures, PowerTools-master, Public, PwnXSS, and several folders. The file "recon2.txt" is highlighted in green. The terminal prompt "#>" is shown at the bottom.

```
[root@parrot]~[/home/attacker]
└─#sgpt --chat footprint --shell "Use Sherlock to gather personal information about Sundar Pichai and save the result in recon2.txt"
sherlock Sundar Pichai --print-found > recon2.txt
[E]xecute, [D]escribe, [A]bort: E
[root@parrot]~[/home/attacker]
└─#ls
AndroRAT      jwt_tool
BloodHound-win32-x64.zip  lazys3-master
ClickjackPoc   Maltego.v4.6.0.deb
create_ap      microsoft_emails.json
Desktop       microsoft_emails.xml
dirsearch     Music
dnsrecon      HTML_theft
Documents     passwords.txt
Downloads    PhoneExploit-Pro
DSSS          Photon
ghauri        Pichai.txt
ghost_eye     Pictures
GRecon        PowerTools-master
Havoc          Public
holehe        PwnXSS
jdk-8u202-linux-x64.tar.gz  recon2.txt
[root@parrot]~[/home/attacker]
└─#
```

7. 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.

A screenshot of a terminal window titled "recon2.txt (/home/attacker) - Pluma (as superuser)". The window displays a list of 15 URLs, each starting with "https://about.me/SundarPichai". The URLs are numbered 1 through 15. The terminal window has a dark background with a colorful parrot logo on the right side. The bottom of the window shows the command "#pluma recon2.txt".

```
1 https://about.me/SundarPichai
2 https://independent.academia.edu/SundarPichai
3 https://www.behance.net/SundarPichai
4 https://SundarPichai.blogspot.com
5 https://www.codecademy.com/profiles/SundarPichai
6 https://codeforces.com/profile/SundarPichai
7 https://disqus.com/SundarPichai
8 https://www.duolingo.com/profile/SundarPichai
9 https://www.fiverr.com/SundarPichai
10 https://www.freelancer.com/u/SundarPichai
11 https://giphy.com/SundarPichai
12 https://www.github.com/SundarPichai
13 https://hackerearth.com/@SundarPichai
14 https://hackerone.com/SundarPichai
15 https://hackerrank.com/SundarPichai
```

ls

8. 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.

```
[root@parrot]~[/home/attacker]
[sudo] password for root:
#sgpt --chat footprint --shell "Install and use DNSRecon to perform DNS enumeration on the target domain www.certifiedhacker.com" - Parrot OS
[E]xecute, [D]escribe, [A]bort: E
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dnsrecon is already the newest version (1.1.3-2).
The following packages were automatically installed and are no longer required:
  ccze hcxdumptool hcxtools hostapd isc-dhcp-server libubcl1 lua-lpeg macchanger
  oracle-instantclient-basic policycoreutils postgresql rfkill selinux-utils tmux upx-ucld
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 179 not upgraded.
[*] std: Performing General Enumeration against: www.certifiedhacker.com...
[-] DNSSEC is not configured for www.certifiedhacker.com
[*]      SOA ns1.bluehost.com 162.159.24.80
[*]      NS ns1.bluehost.com 162.159.24.80
[*]      NS ns2.bluehost.com 162.159.25.175
[*]      Bind Version for 162.159.25.175 "2024.5.2"
[*]      MX mail.certifiedhacker.com 162.241.216.11
[*]      CNAME www.certifiedhacker.com certifiedhacker.com
[*]      A certifiedhacker.com 162.241.216.11
[*]      TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*]  Enumerating SRV Records
[+] 0 Records Found
```

9. 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.

The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar indicates the command is "sgpt --chat footprint --shell" and the target host is "www.certifiedhacker.com". The terminal content displays a traceroute to the target host, showing 13 routers along the path with their respective IP addresses, latencies, and round-trip times. The traceroute command used was "#sgpt --chat footprint --shell "Perform network tracerouting to discover the routers on the path to a target host www.certifiedhacker.com"".

```
[root@parrot]~[/home/attacker]
└─#sgpt --chat footprint --shell "Perform network tracerouting to discover the routers on the path to a target host www.certifiedhacker.com"
traceroute www.certifiedhacker.com
[E]xecute, [D]escribe, [A]bort: E
traceroute to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1  10.10.1.2 (10.10.1.2)  0.808 ms  0.754 ms  1.418 ms
 2  172.18.0.1 (172.18.0.1)  3.062 ms  3.033 ms  3.008 ms
 3  192.168.0.1 (192.168.0.1)  2.996 ms  2.970 ms  2.893 ms
 4  185.254.56.25 (185.254.56.25)  1.627 ms  1.600 ms  2.123 ms
 5  * * * port-channel4.switch2.lon3.he.net (216.66.95.117)  3.096 ms
 6  * * *
 7  port-channel8.core2.lon2.he.net (184.104.197.217)  34.378 ms  34.353 ms  16.650 ms
 8  ae-23.edge7.London1.Level3.net (4.68.127.237)  34.296 ms  34.270 ms  34.245 ms
 9  ae1.37.bar4.SaltLakeCity1.level3.net (4.69.219.58)  128.244 ms  142.395 ms  142.369 ms
10  4.53.7.174 (4.53.7.174)  159.655 ms  153.902 ms  159.438 ms
11  69-195-64-111.unifiedlayer.com (69.195.64.111)  160.043 ms  159.995 ms  147.701 ms
12  po97.prv-leaf1a.net.unifiedlayer.com (162.144.240.123)  143.202 ms po99.prv-leaf1b.net.unifiedlayer.com (162.144.240.127)  147.611 ms po97.prv-leaf1b.net.unifiedlayer.com (162.144.240.131)  147.570 ms
13  box5331.bluehost.com (162.241.216.11)  150.722 ms  149.059 ms  147.165 ms
[root@parrot]~[/home/attacker]
└─#
```

10. 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

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"

[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

```
[E]xecute, [D]escribe, [A]bort: E
20.112.250.133
20.231.239.246
20.76.201.171
20.70.246.20
20.236.44.162
Domain Name: MICROSOFT.COM
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-08-18T16:15:54Z
Creation Date: 1991-05-02T04:00:00Z
Registry Expiry Date: 2025-05-03T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1-39.AZURE-DNS.COM
Name Server: NS2-39.AZURE-DNS.NET
Name Server: NS3-39.AZURE-DNS.ORG
```

11. 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.
12. This concludes the demonstration of performing footprinting using the ShellGPT.
13. 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.