

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).

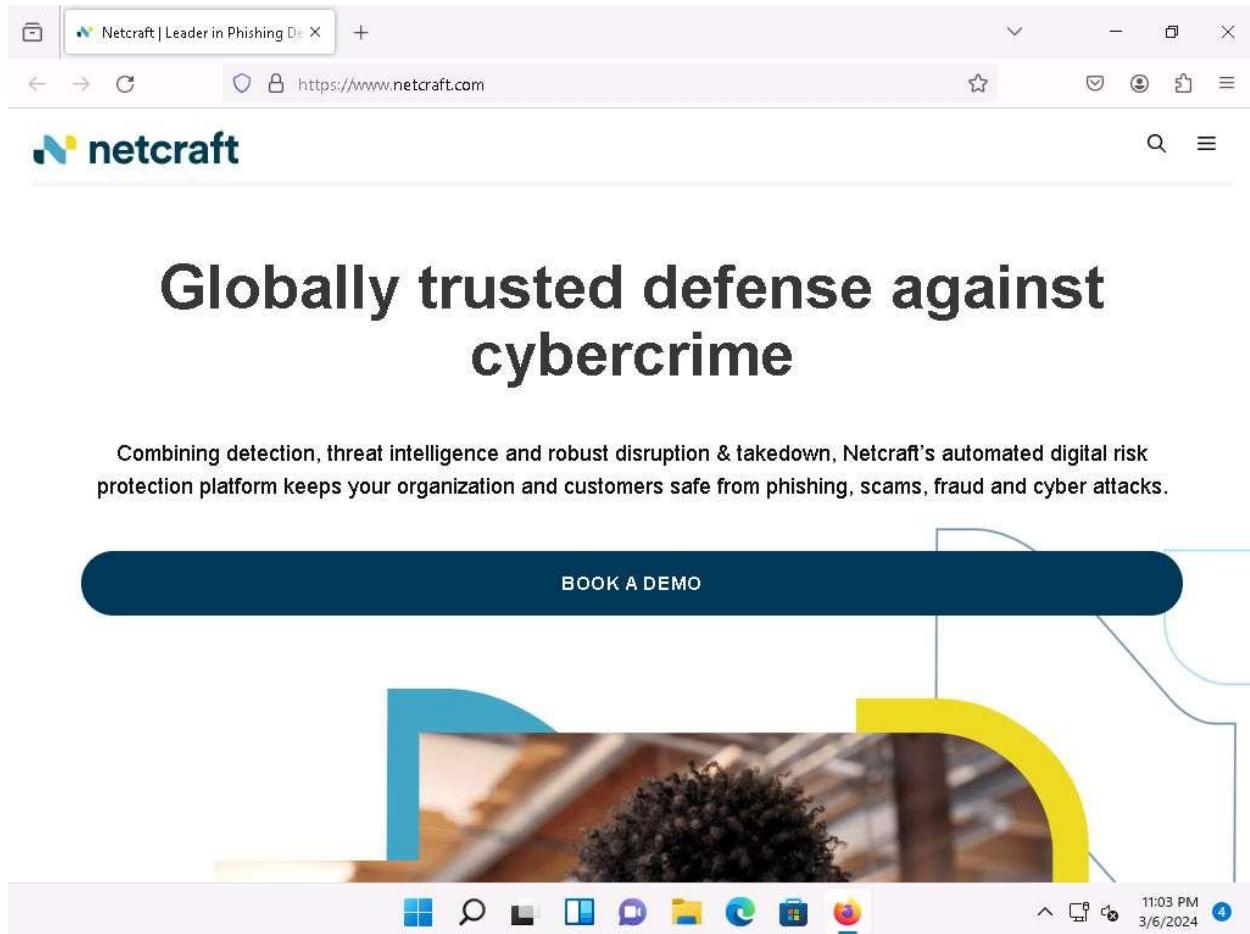
Task 1: Find the Company's Domains, Subdomains and Hosts using Netcraft and DNSdumpster

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

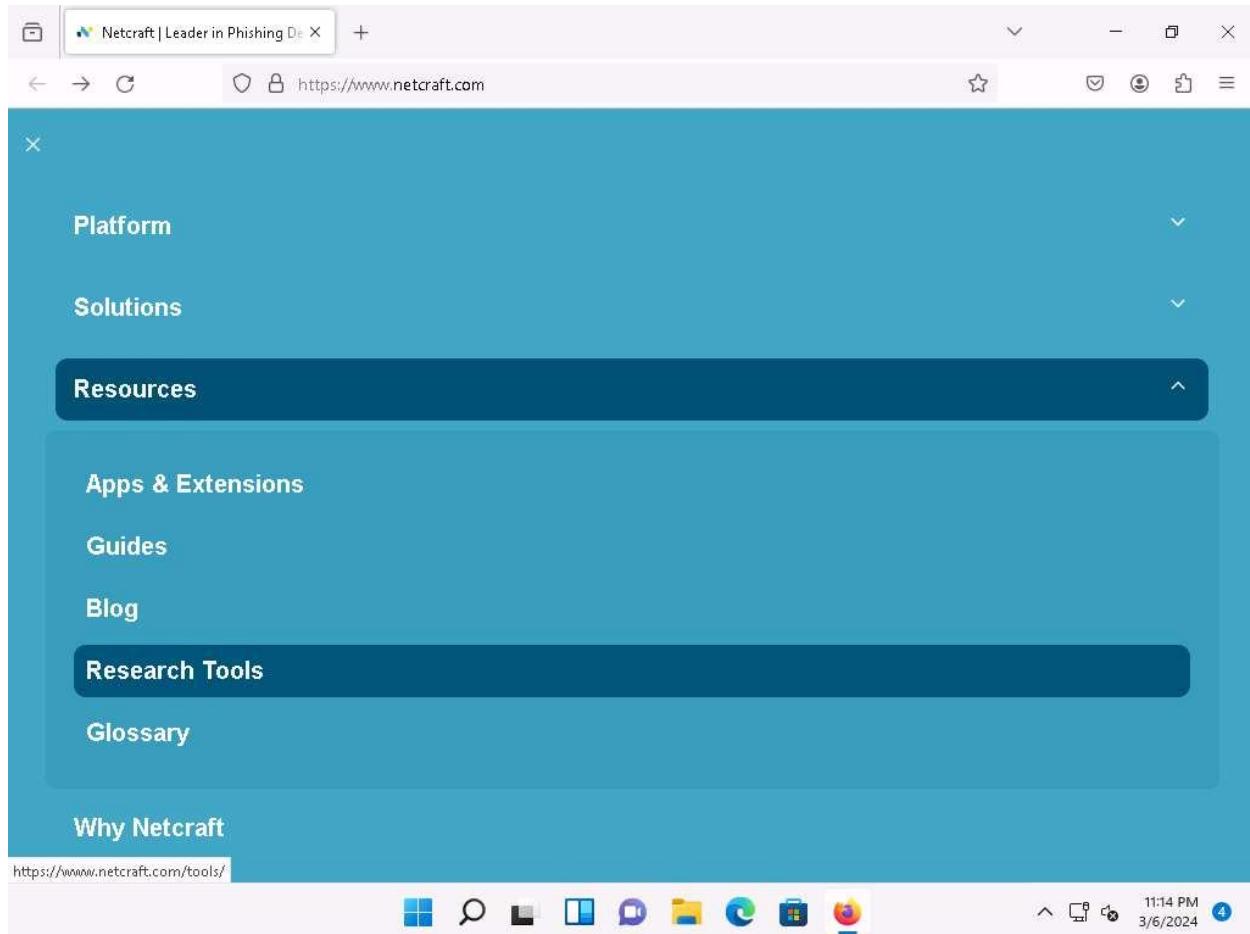
https://www.netcraft.com

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**.

A screenshot of a web browser window titled "Tools | Netcraft". The URL in the address bar is <https://www.netcraft.com/tools/>. The page content discusses various tools to find out what infrastructure and technologies any site is using, which sites are 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 users of the [Netcraft](#)



Most Popular Sites

Find out which sites are most visited globally or for any

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.



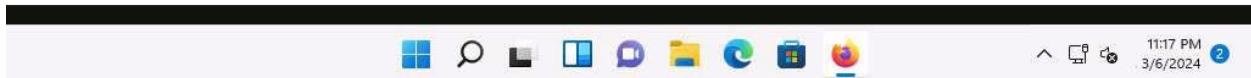
What's that site running?

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 web browser window with the following details:

- Address Bar:** https://sitereport.netcraft.com/?url=https%3A%2F%2Fwww.certifiedhacker.com
- Title Bar:** Site report for https://www.certifiedhacker.com
- Content Area:**
 - Background:** Shows basic site information:

Site title	Not Acceptable!	Date first seen	January 2018
Site rank	10752	Primary language	English
Description	Not Present		
 - Network:** Shows network infrastructure details:

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)

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

Network

Site	Domain
https://www.certifiedhacker.com	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

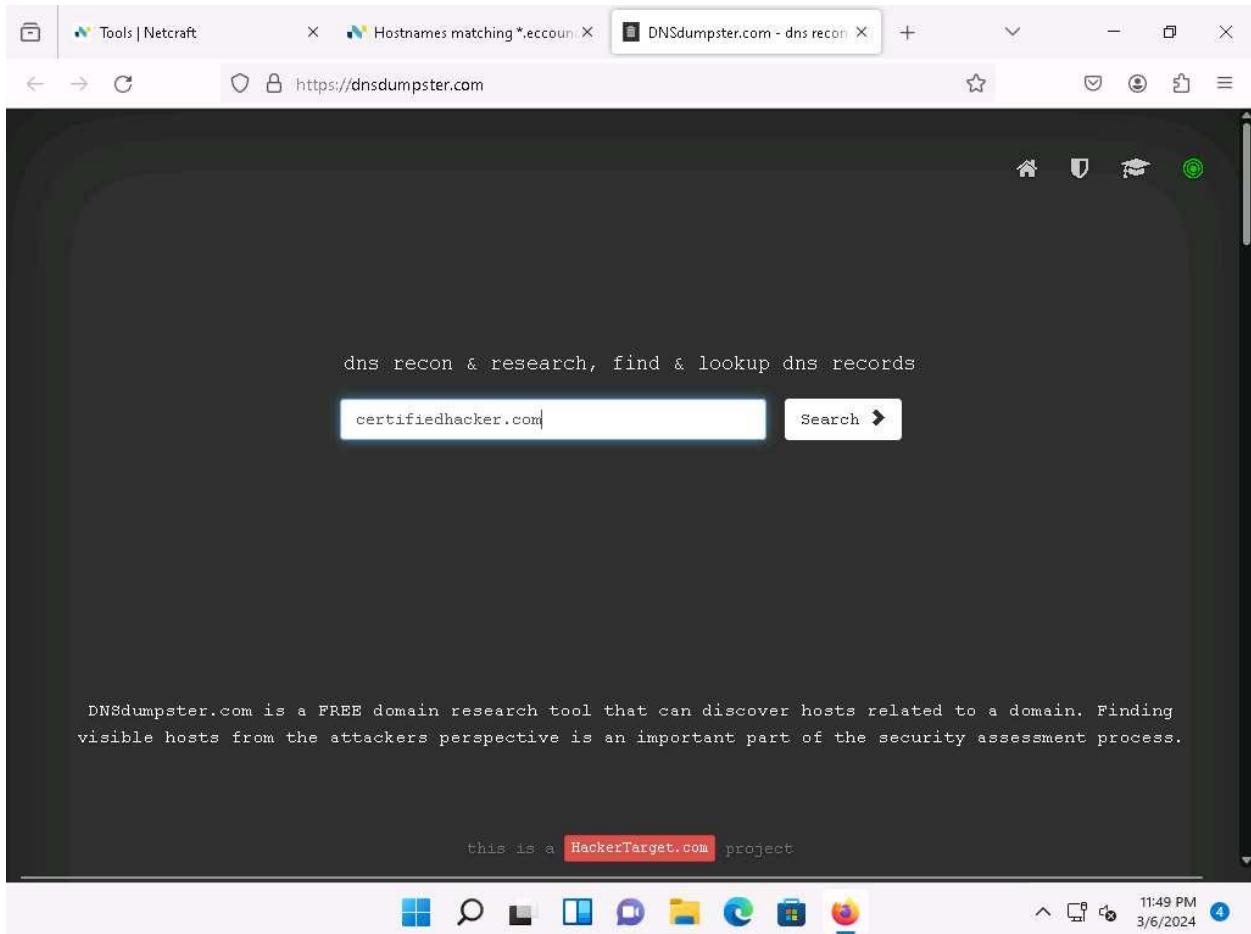
11:19 PM 3/6/2024

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

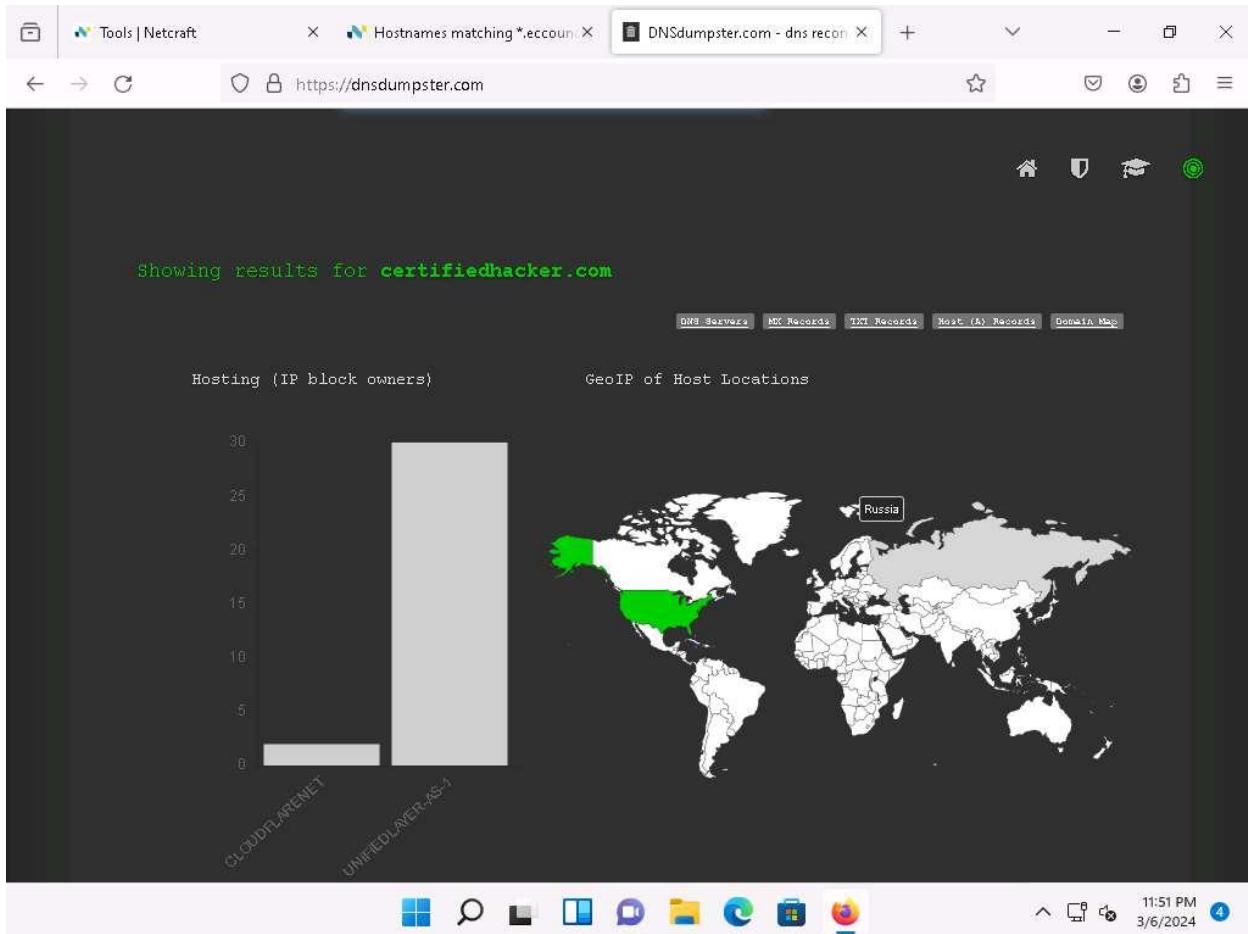
The screenshot shows a web browser window with the following details:

- Address Bar:** https://searchdns.netcraft.com/?host=*.certifiedhacker.com
- Title Bar:** Hostnames matching *.certifiedhacker.com
- Content Area:**
 - Netcraft Logo:** netcraft
 - Section Header:** Hostnames matching *.certifiedhacker.com
 - Search Bar:** ▶ Search with another pattern?
 - Results Section:** 3 results
 - Rank: 10752 Site: www.certifiedhacker.com First seen: December 2002 Netblock: Unified Layer OS: Linux
 - Rank: 1182836 Site: cpanel.certifiedhacker.com First seen: January 2017 Netblock: Unified Layer OS: Linux
 - Rank: 1452256 Site: www.sftp.certifiedhacker.com First seen: September 2018 Netblock: Unified Layer OS: Linux
- Bottom Bar:** Includes icons for Windows Start, Search, Task View, File Explorer, Chat, Edge, File, and Task Manager, along with system status (11:20 PM, 3/6/2024).

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 content is as follows:

DNS Servers

Host	IP Address	Location
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...
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)

Host	IP Address	Location
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

HTTP: Apache
FTP: 220- Welcome to Pure-FTPD privsep TLS
-220- You are user number 2 of 150 allowed.
220- Local time is no
SSH: SSH-2.0-OpenSSH_7.4

www.soc.certifiedhacker.com 162.241.216.11 UNIFIEDLAYER-AS-1 United States

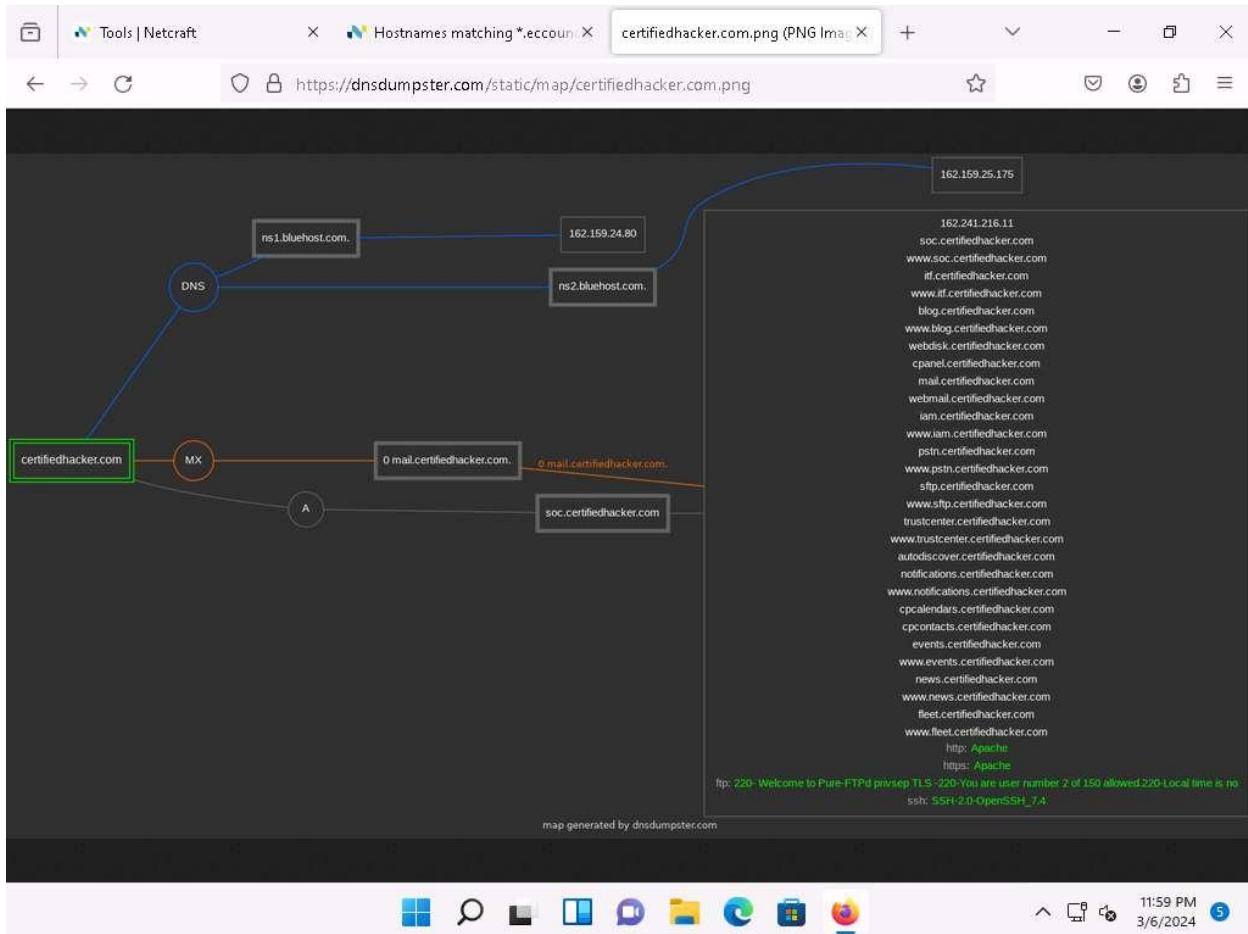
HTTP: Apache
FTP: 220- Welcome to Pure-FTPD privsep TLS
-220- You are user number 2 of 150 allowed.
220- Local time is no

11:54 PM 3/6/2024 4

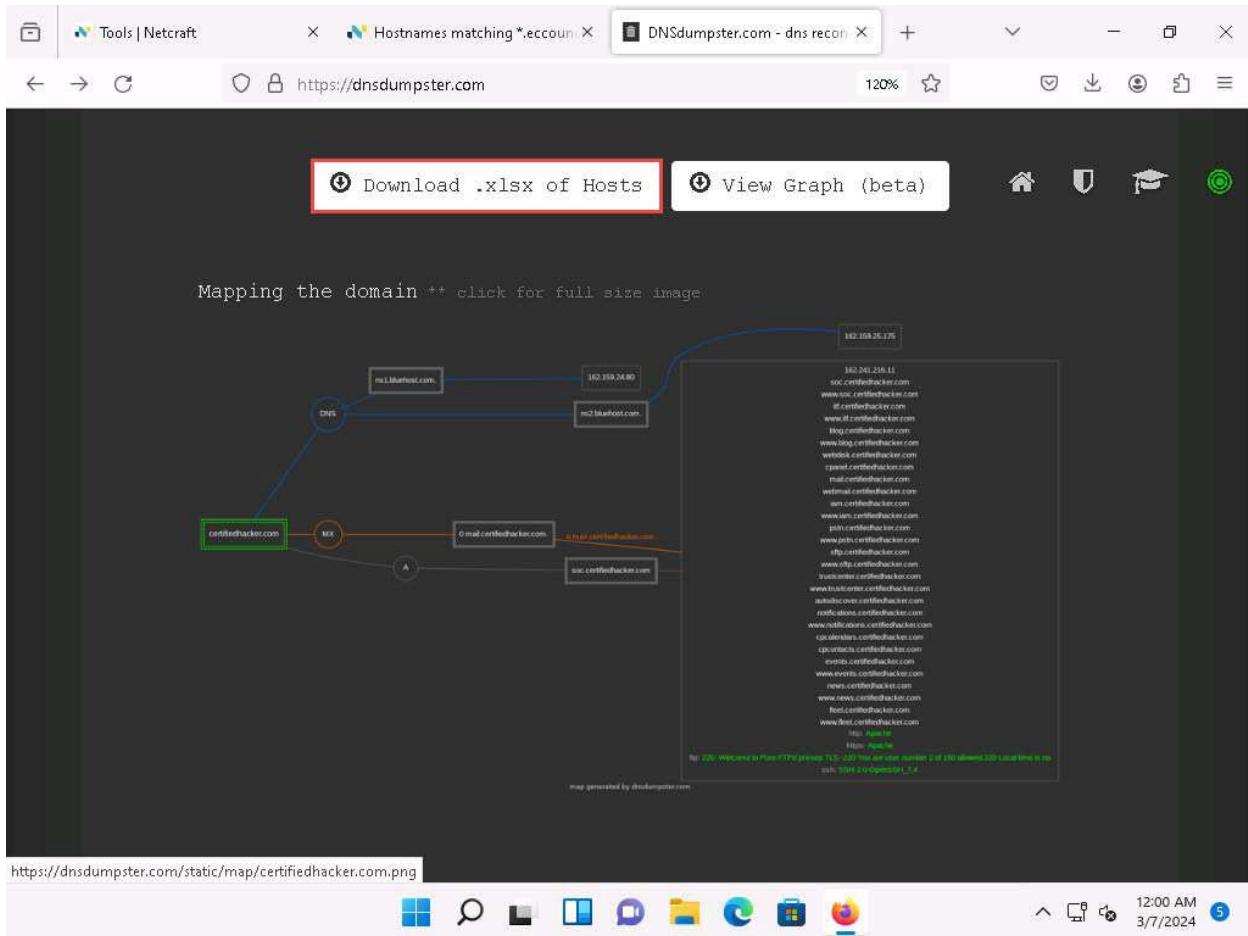
13. Further, scroll down to view the domain mapping of the website.

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

Click back to exit from full-size image.



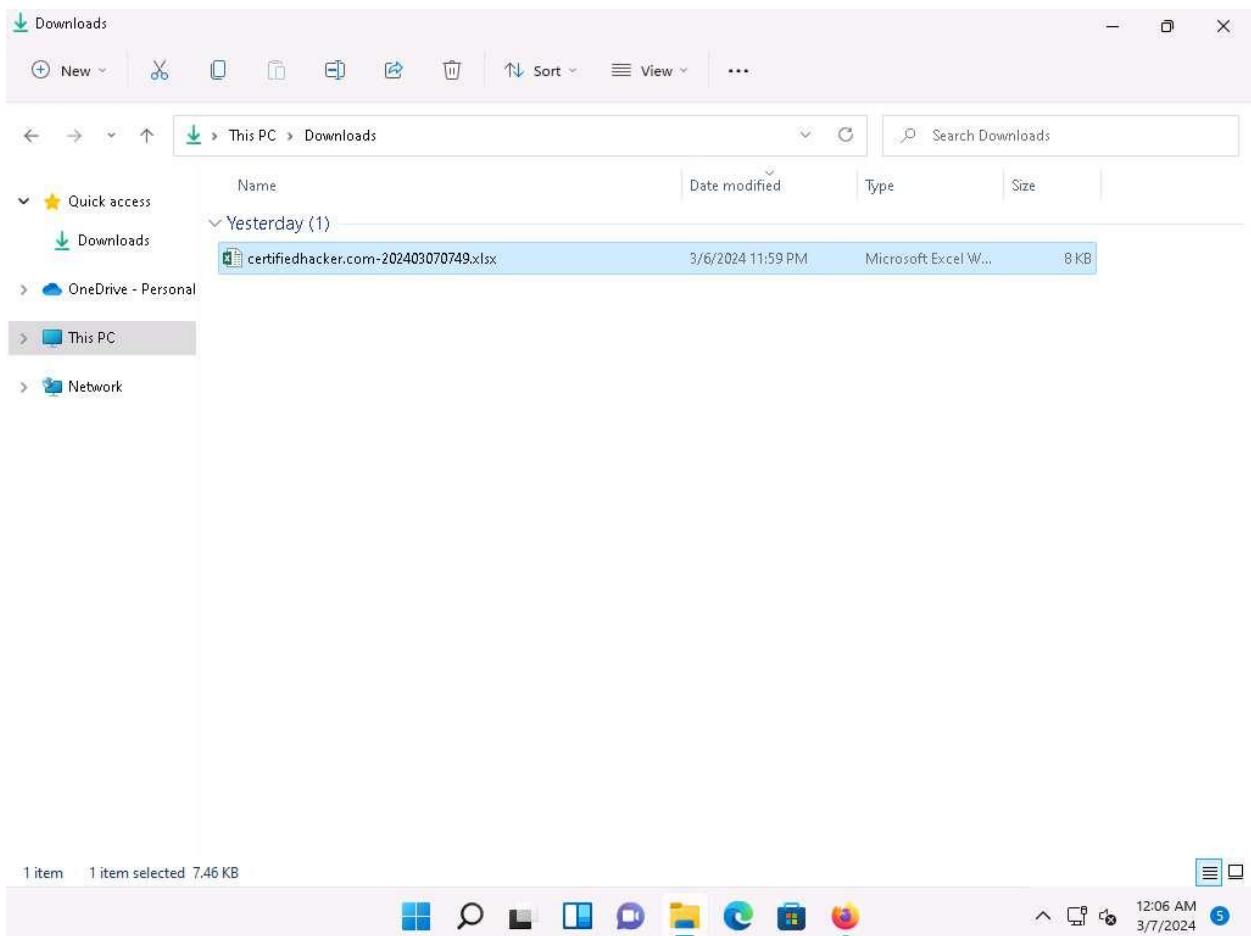
14. Click on **Download .xlsx of Hosts** button to download the list of hosts.



15. Navigate to the **Downloads** folder and double-click on **certifiedhacker.com-xxxxxxxx.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.

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

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.