

# **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).

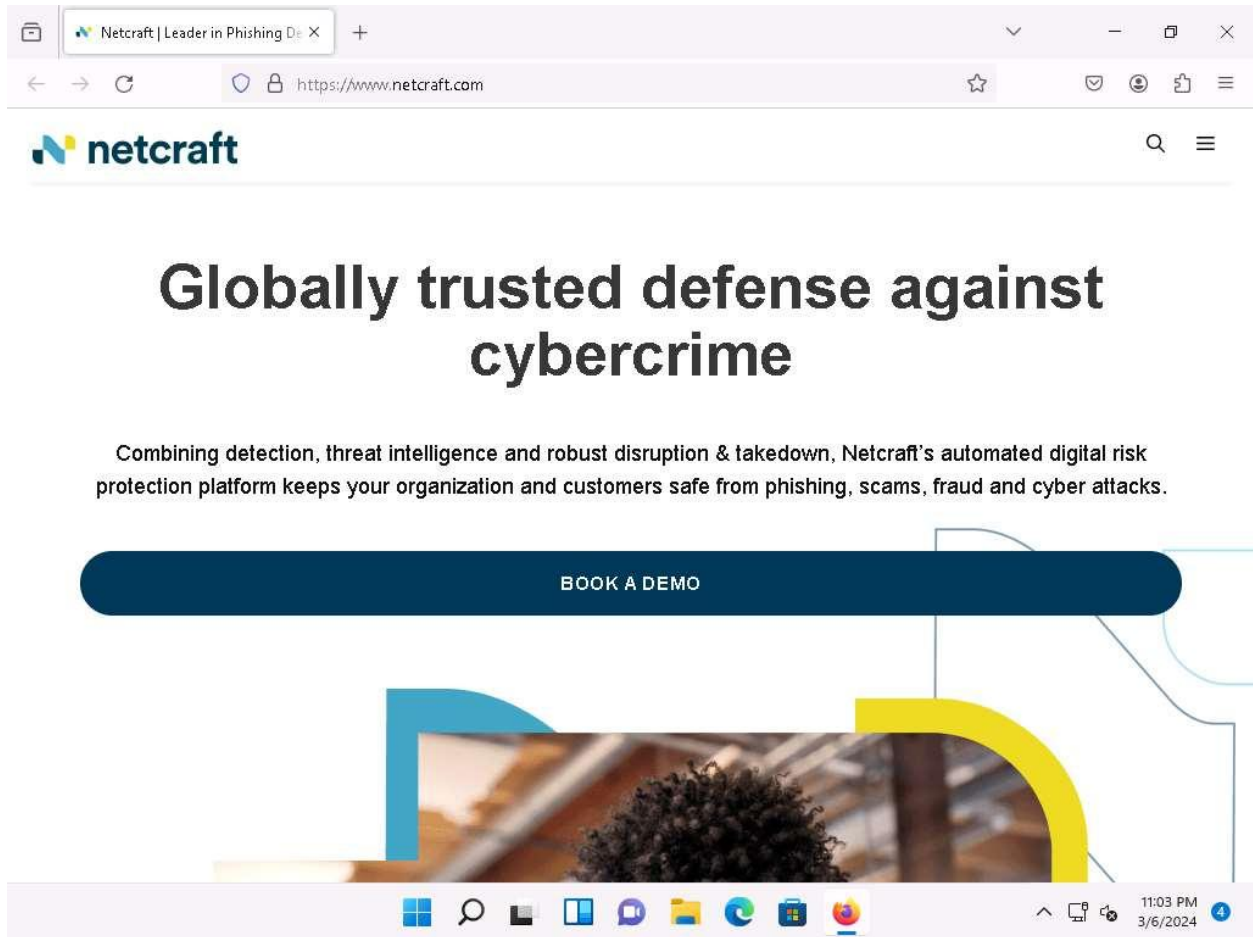
Task 1: Find the Company's Domains, Subdomains and Hosts using Netcraft and DNSdumpster

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.

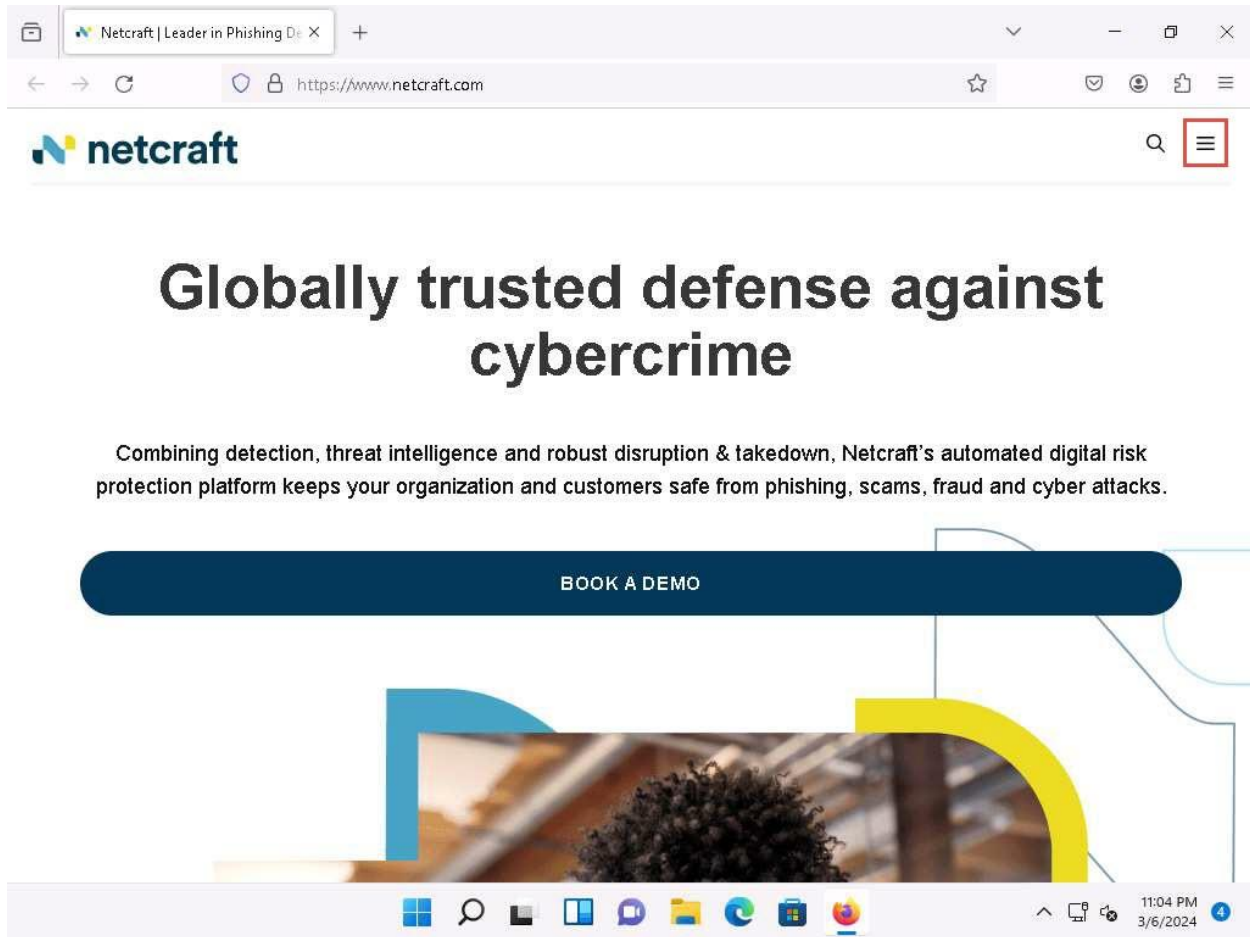
Here, we will extract the company's domains and subdomains using the Netcraft and DNSdumpster tools.

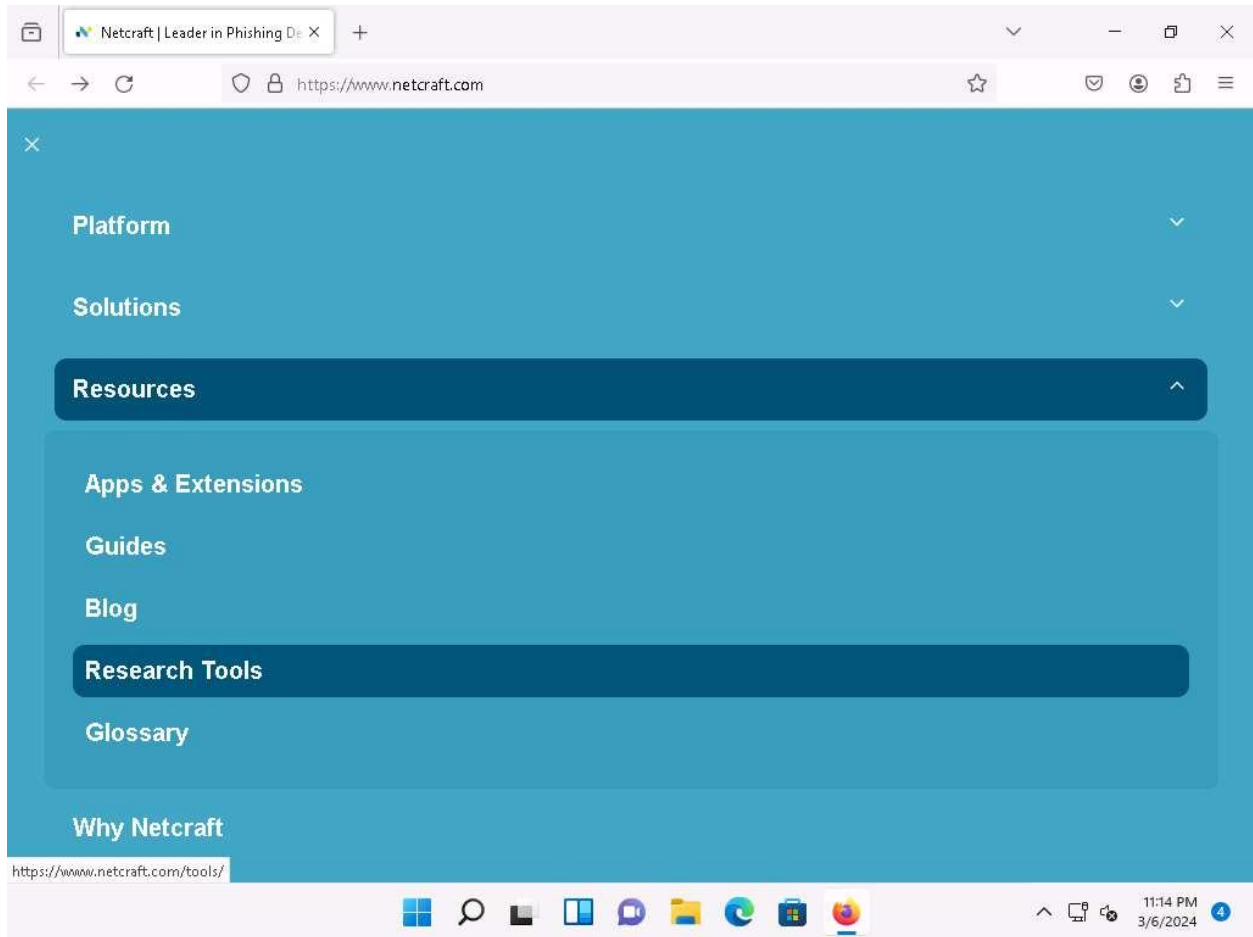
1. Launch any web browser, and go to **<https://www.netcraft.com>** (here, we are using **Mozilla Firefox**).
2. **Netcraft** page appears, as shown in the screenshot.

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



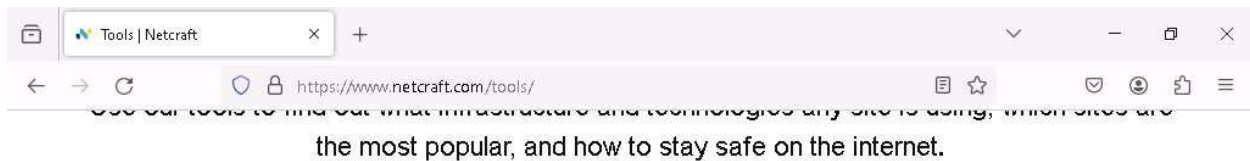
3. Click on menu icon from the top-right corner of the page and navigate to the **Resources** - > **Research Tools**.





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

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



## Internet Research Tools



### Site Report

Using results from our internet  
data mining, find out the



### Search DNS

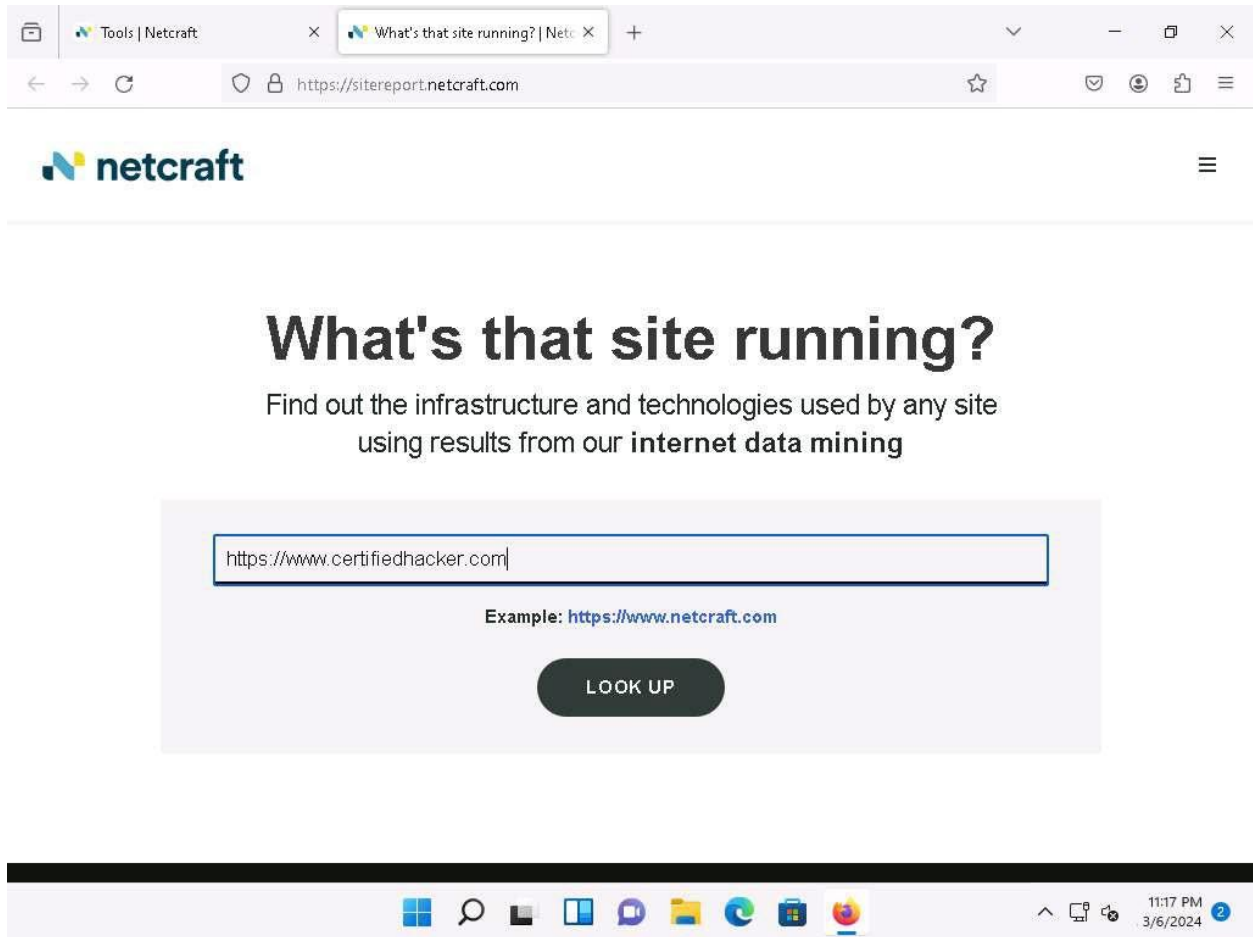
Explore hostnames visited by  
users of the [Netcraft](#)



### 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.



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.

Tools | Netcraft

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

<https://sitereport.netcraft.com/?url=https%3A%2F%2Fwww.certifiedhacker.com>

**netcraft**

### Background

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

### Network

Site	<a href="https://www.certifiedhacker.com">https://www.certifiedhacker.com</a>	Domain	<a href="https://www.certifiedhacker.com">certifiedhacker.com</a>
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)

11:18 PM 3/6/2024

- In the **Network** section, click on the website link (here, [certifiedhacker.com](https://www.certifiedhacker.com)) in the **Domain** field to view the subdomains.

Tools | Netcraft

Site report for https://www.certifiedhacker.com

https://sitereport.netcraft.com/?url=https%3A%2F%2Fwww.certifiedhacker.com

netcraft

### Network

Site	<a href="https://www.certifiedhacker.com">https://www.certifiedhacker.com</a>	Domain	<a href="https://www.certifiedhacker.com">certifiedhacker.com</a>
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		

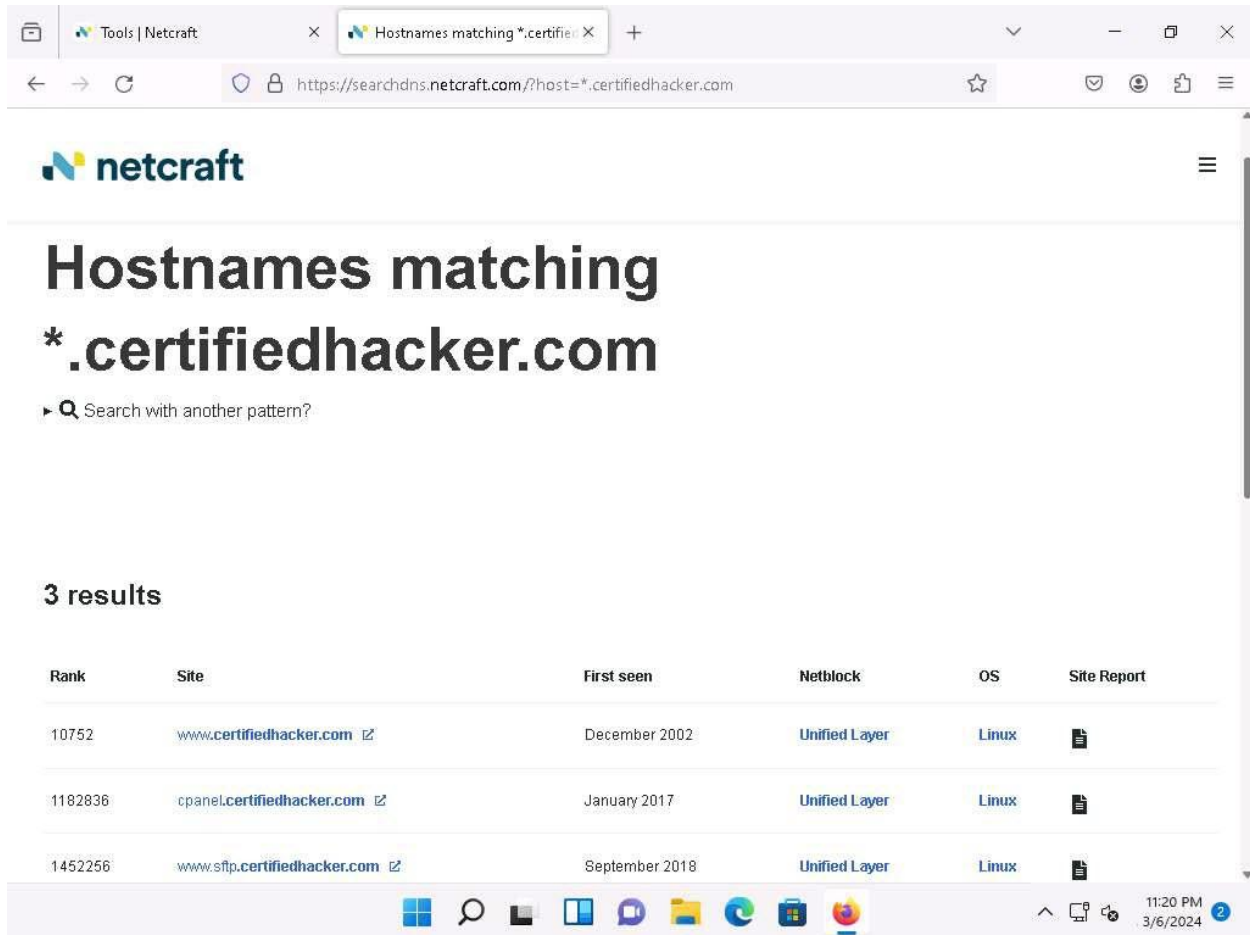
### IP delegation

IPv4 address (162.241.216.11)




[https://searchdns.netcraft.com/?host=\\*.certifiedhacker.com](https://searchdns.netcraft.com/?host=*.certifiedhacker.com)

11:19 PM 3/6/2024

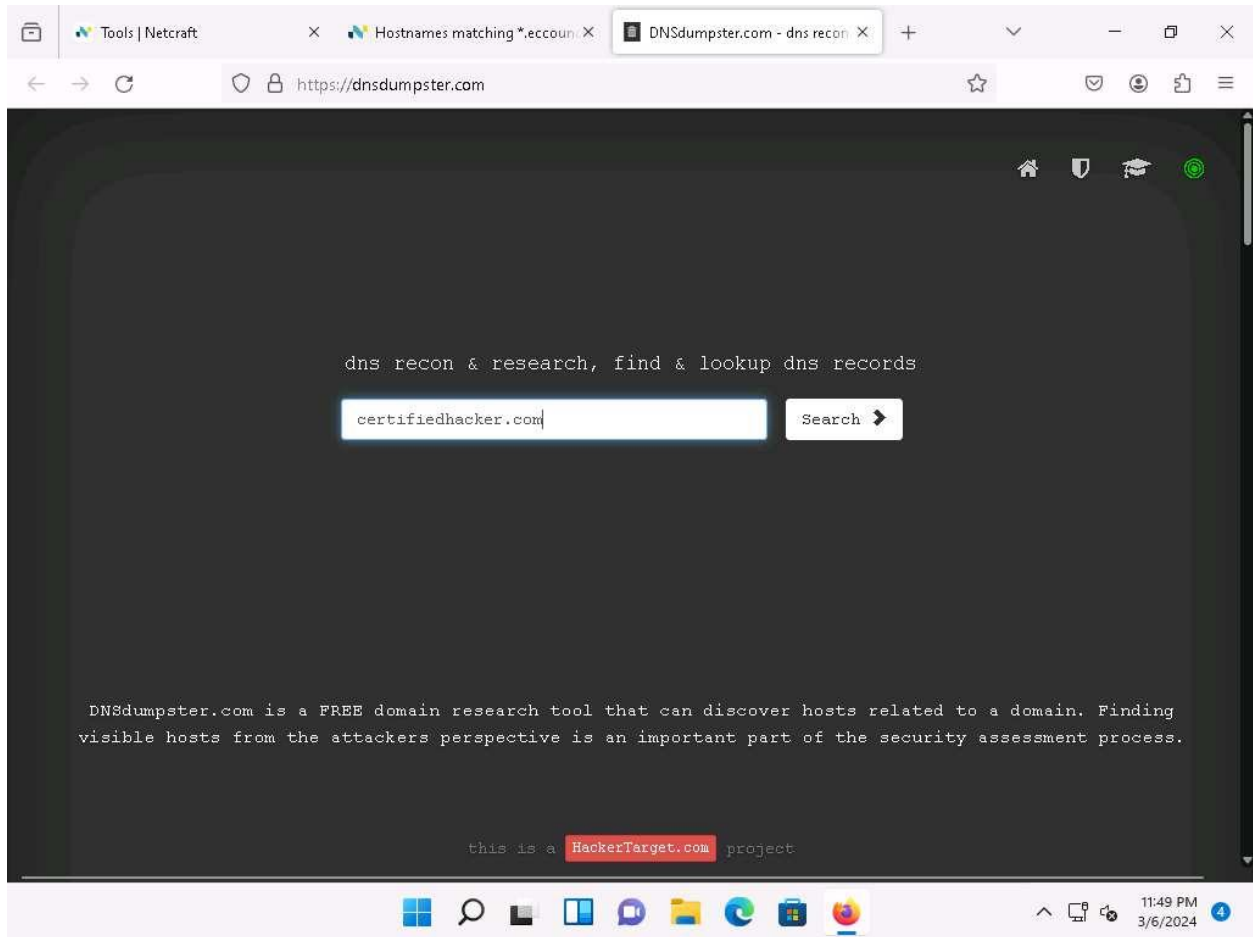
8. The result will display the subdomains of the target website along with netblock and operating system information, as shown in the screenshot.



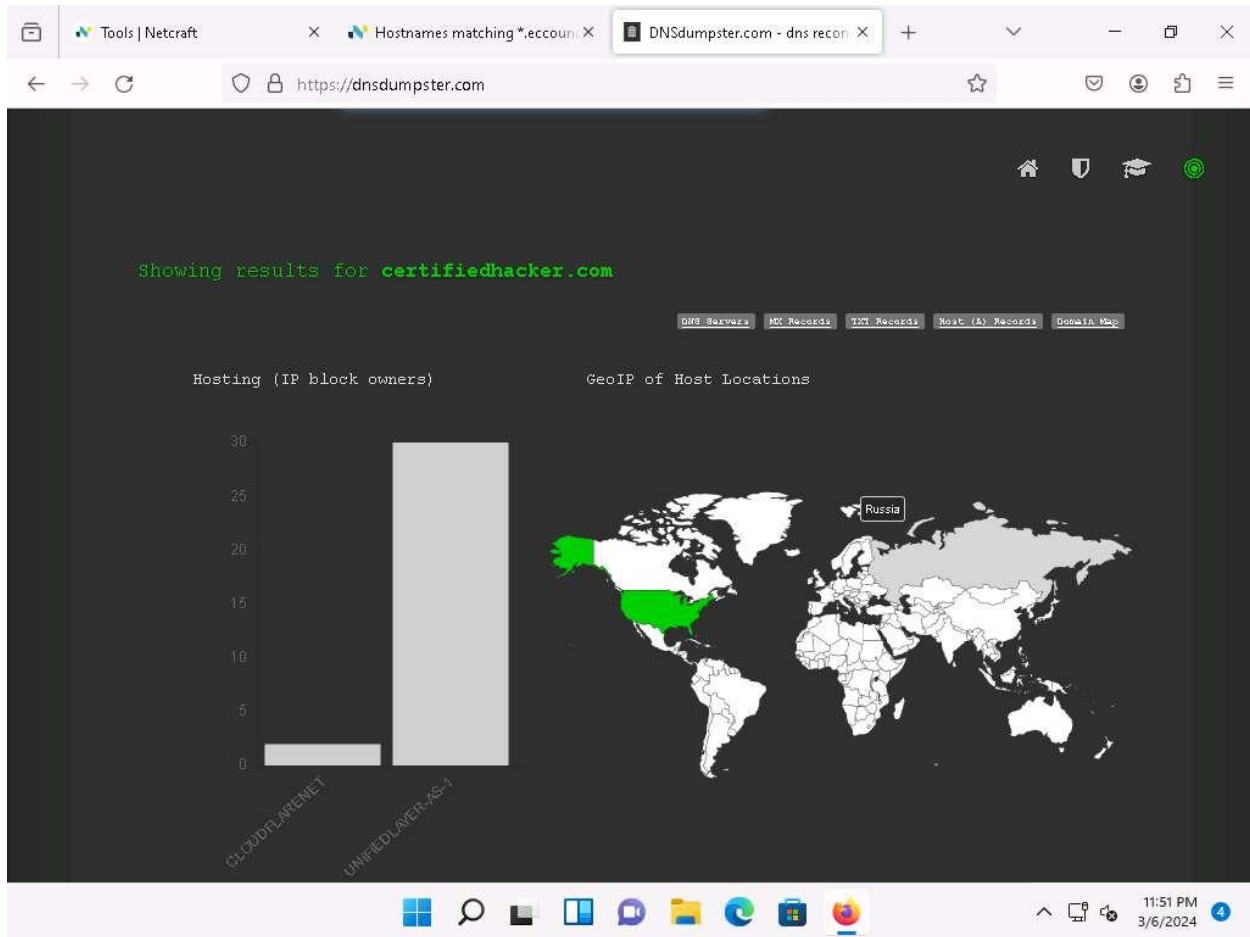
The screenshot shows a web browser window with the Netcraft search results for the pattern `*.certifiedhacker.com`. The browser's address bar shows the URL `https://searchdns.netcraft.com/?host=*.certifiedhacker.com`. The Netcraft logo is in the top left, and a search bar with the pattern `*.certifiedhacker.com` is at the top. Below the search bar, the text "Hostnames matching \*.certifiedhacker.com" is displayed. A link "Search with another pattern?" is visible. The results section shows "3 results". A table lists the results with columns: Rank, Site, First seen, Netblock, OS, and Site Report. The table contains three rows of data.

Rank	Site	First seen	Netblock	OS	Site Report
10752	<a href="http://www.certifiedhacker.com">www.certifiedhacker.com</a>	December 2002	Unified Layer	Linux	
1182836	<a href="http://cpanel.certifiedhacker.com">cpanel.certifiedhacker.com</a>	January 2017	Unified Layer	Linux	
1452256	<a href="http://www.sftp.certifiedhacker.com">www.sftp.certifiedhacker.com</a>	September 2018	Unified Layer	Linux	

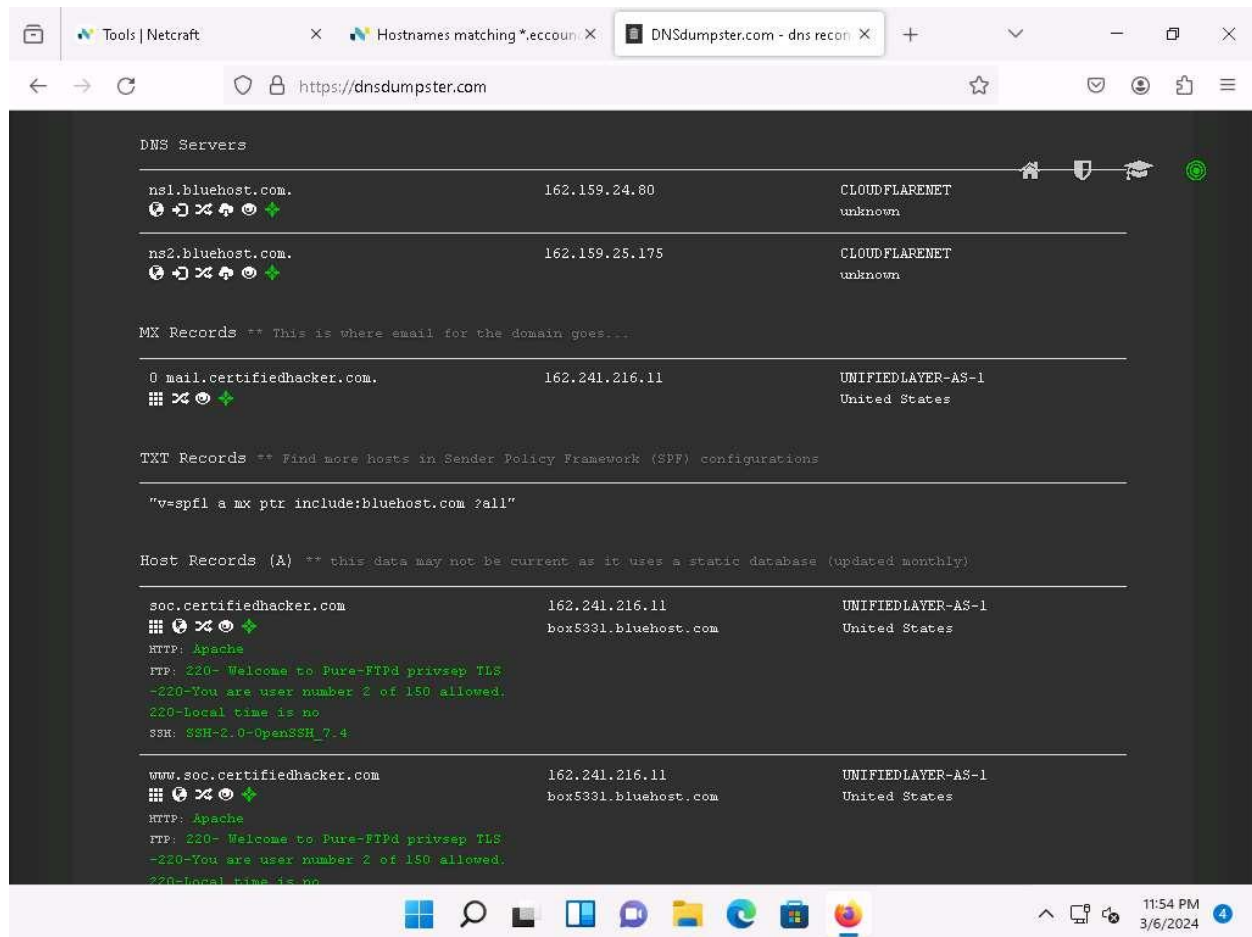
- Now, we will find company's DNS Servers along with Geo IP and domain mapping using DNSdumpster website.
- Open a new tab in **Firefox** browser and go to <https://dnsdumpster.com/>. Search for **certifiedhacker.com** in the search box.



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



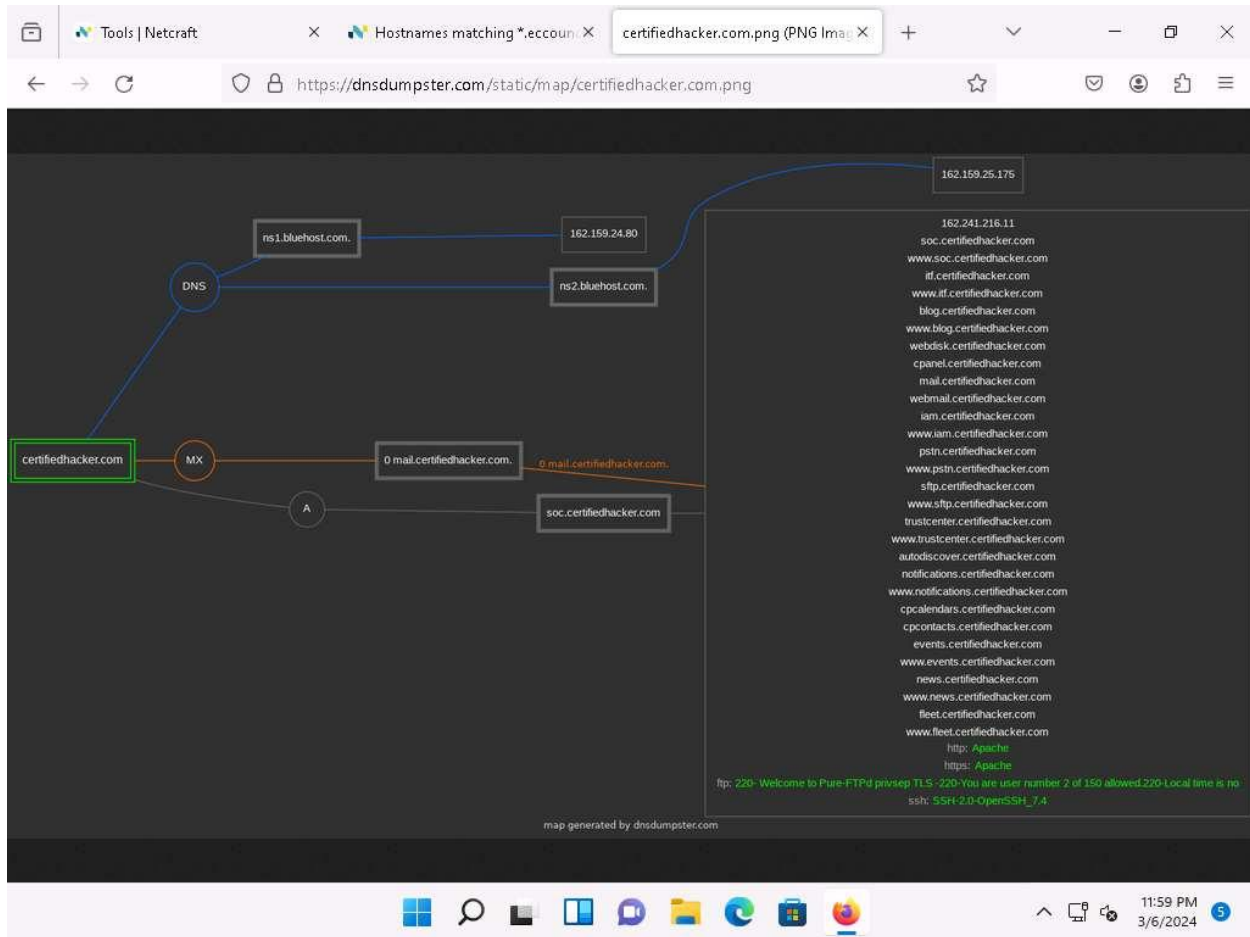
12. Scroll down to view the list of **DNS Servers**, **MX Records**, **Host Record (A)** along with their IP addresses.



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

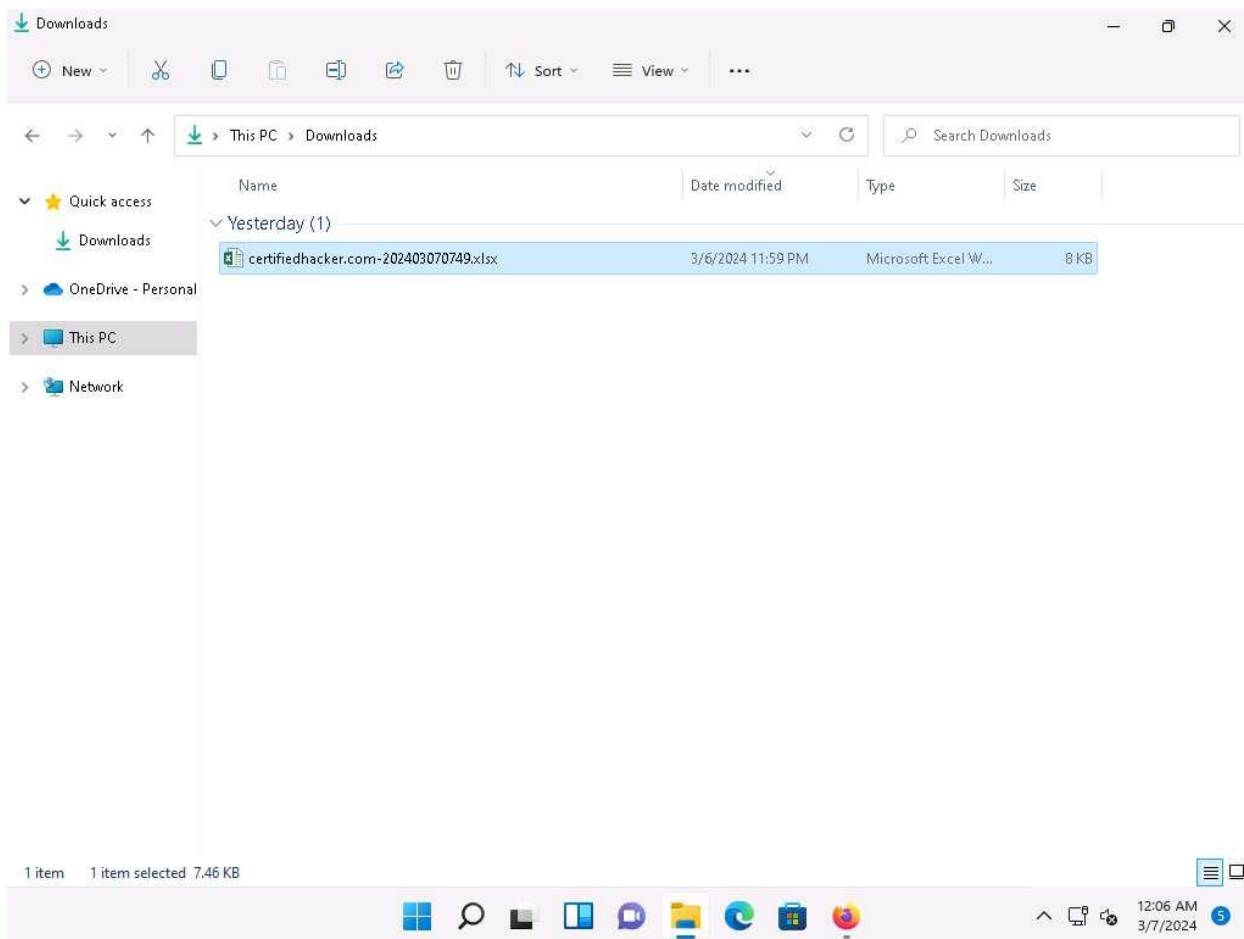
Click on the map to view the full-size image.

Click back to exit from full-size image.



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





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
	Hostname	IP Address	T	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.