Lab 2: Perform Footprinting Through Web 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 web services. By doing so, you can extract critical information such as a target organization’s domains, sub-domains, 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 Sub-domains using Netcraft
* Gather Personal Information using PeekYou Online People Search Service
* Gather an Email List using theHarvester
* Gather Information using Deep and Dark Web Searching
* Determine Target OS Through Passive Footprinting

**Overview of Web Services**

Web services such as social networking sites, 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 and Sub-domains using Netcraft

Domains and sub-domains are part of critical network infrastructure for any organization. A company's top-level domains (TLDs) and sub-domains 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.

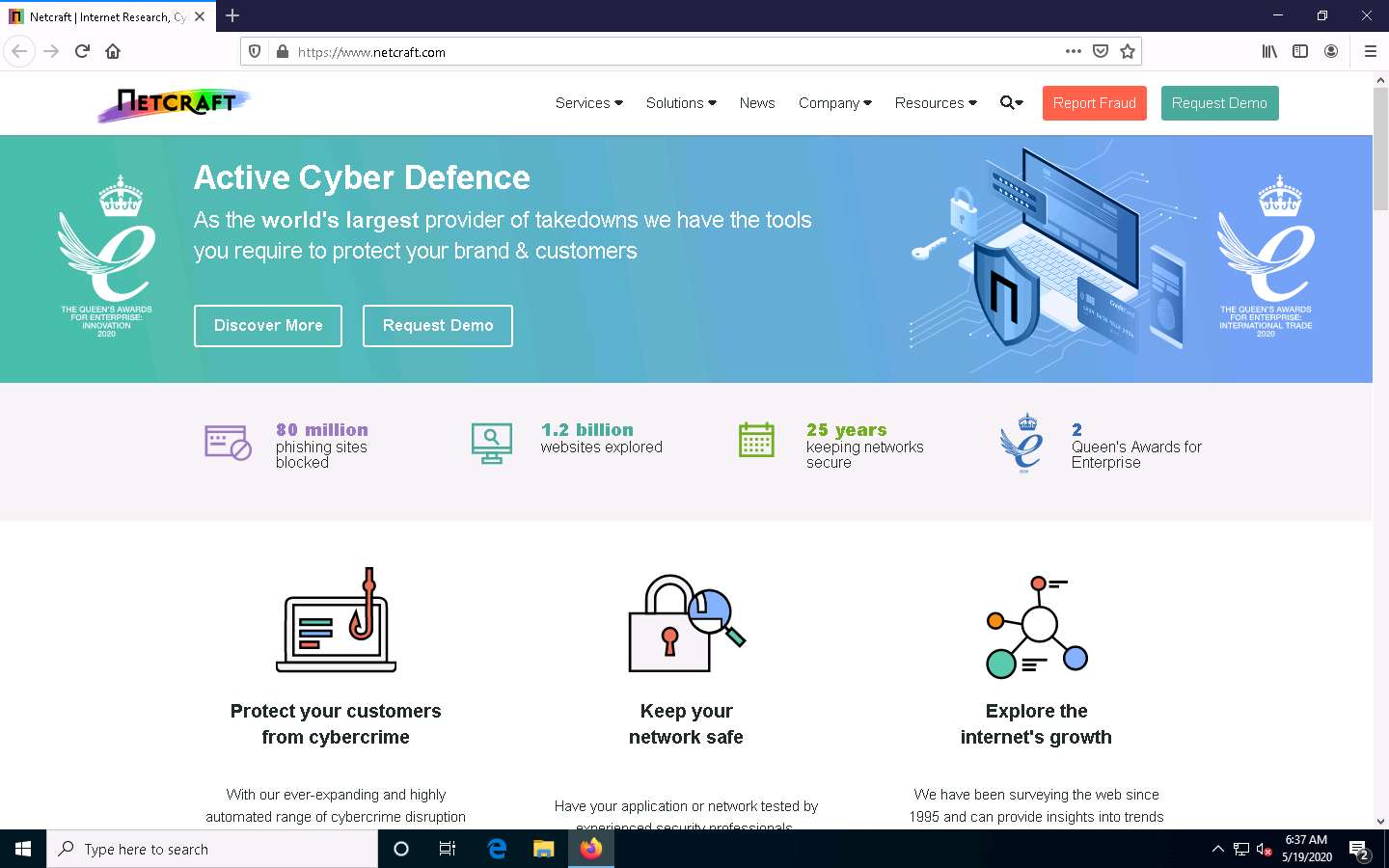
Here, we will extract the company’s domains and sub-domains using the Netcraft web service.

1. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and click https://www.netcraft.com and press **Enter**.

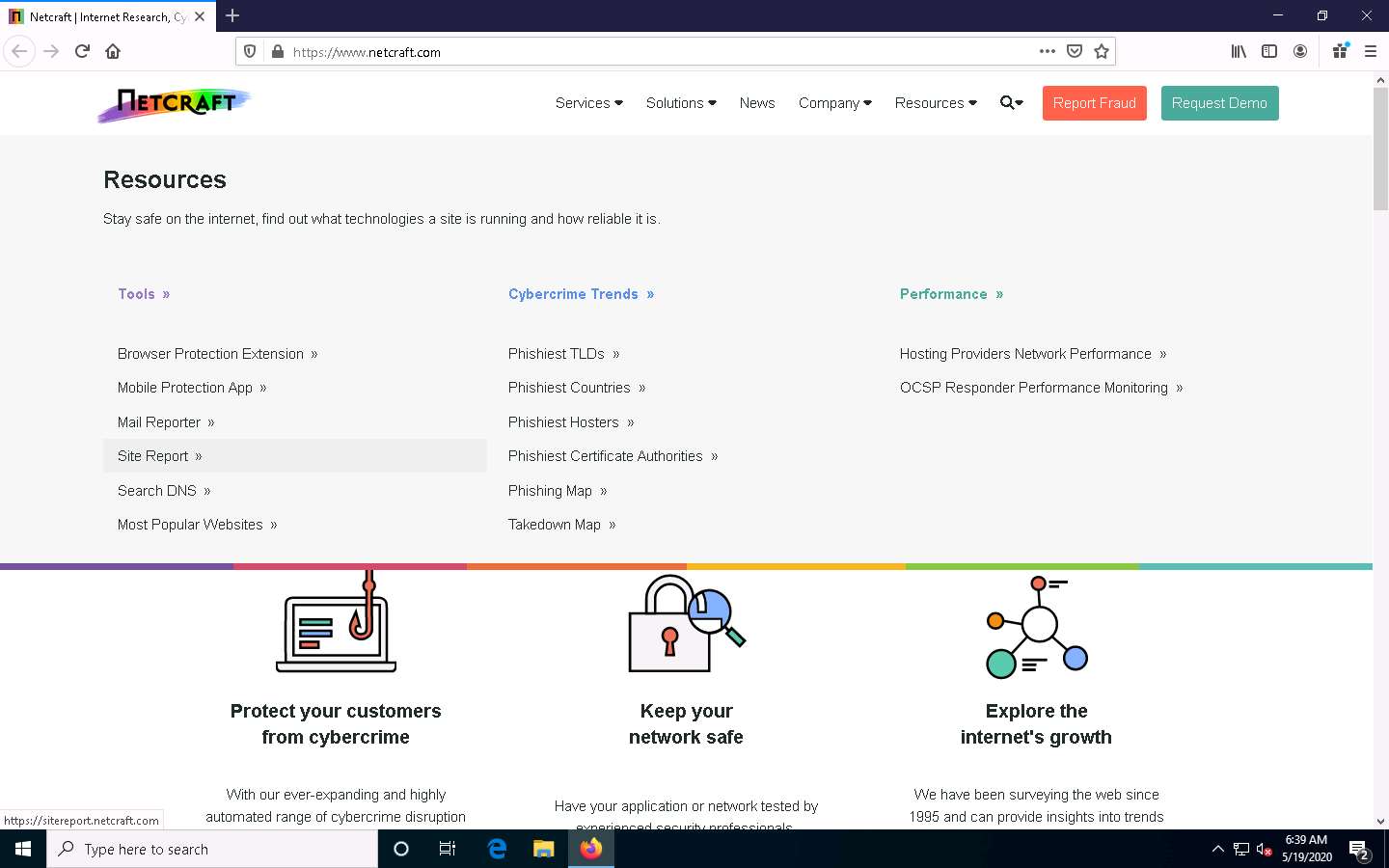
If you choose to use another web browser, the screenshots will differ.

1. **Netcraft** page appears, as shown in the screenshot.

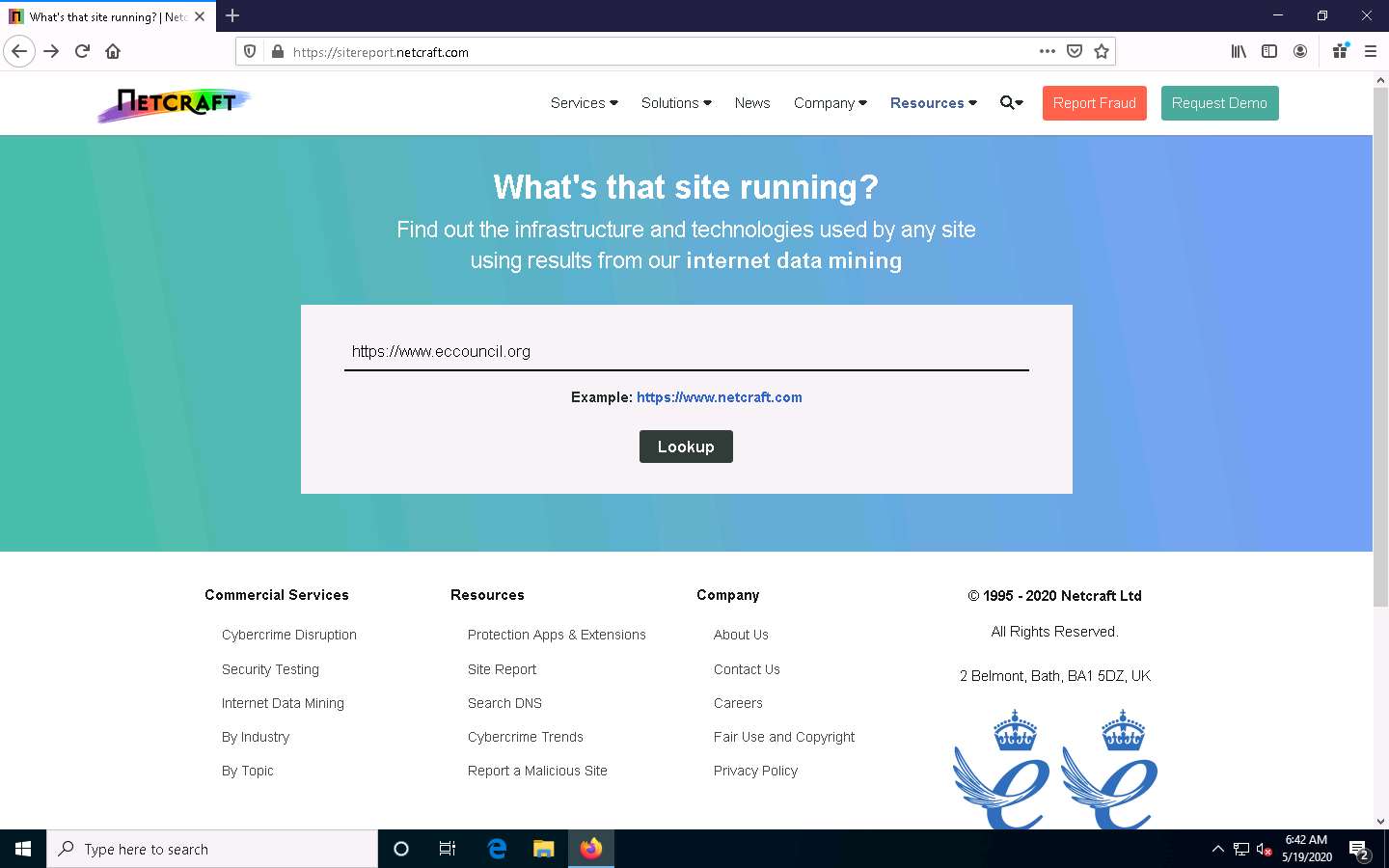
If cookie pop-up appears at the lower section of the browser, click **Accept**.



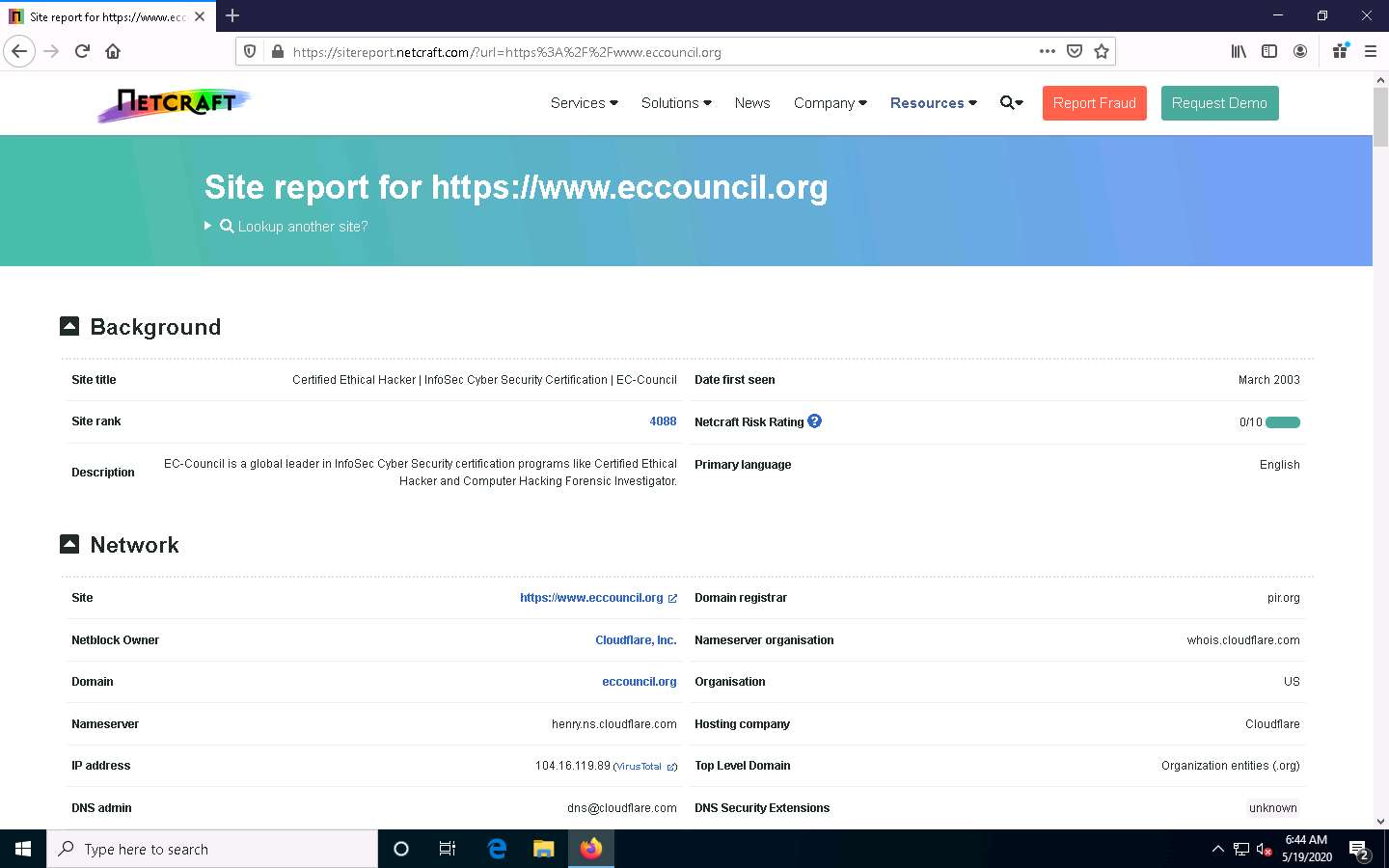
1. Click the **Resources** tab from the menu bar and click on the **Site Report** link under the Tools section.



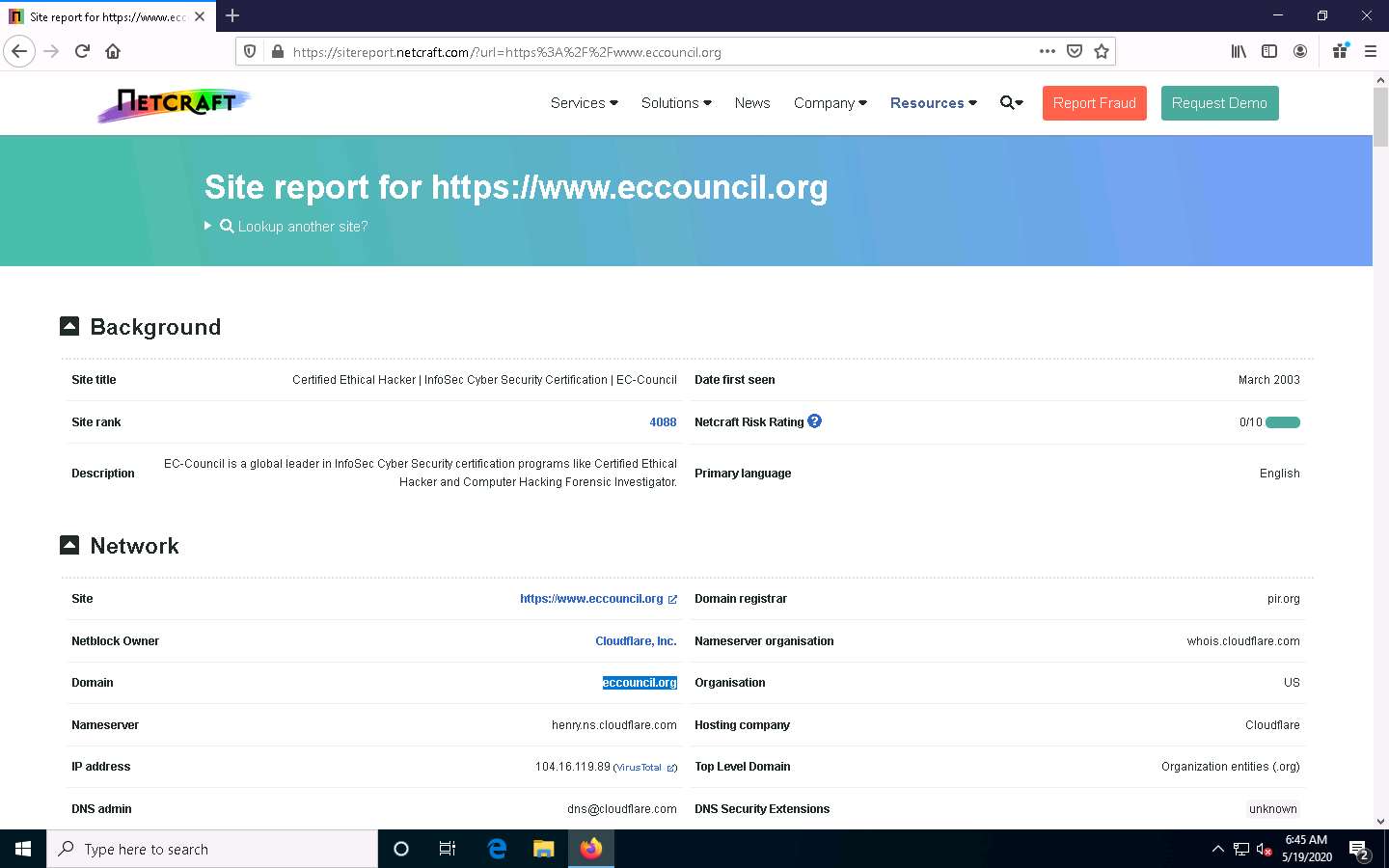
1. The **What’s that site running?** page appears. To extract information associated with the organizational website such as infrastructure, technology used, sub domains, background, network, etc., type the target website’s URL (here, **https://www.eccouncil.org**) in the text field, and then click the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



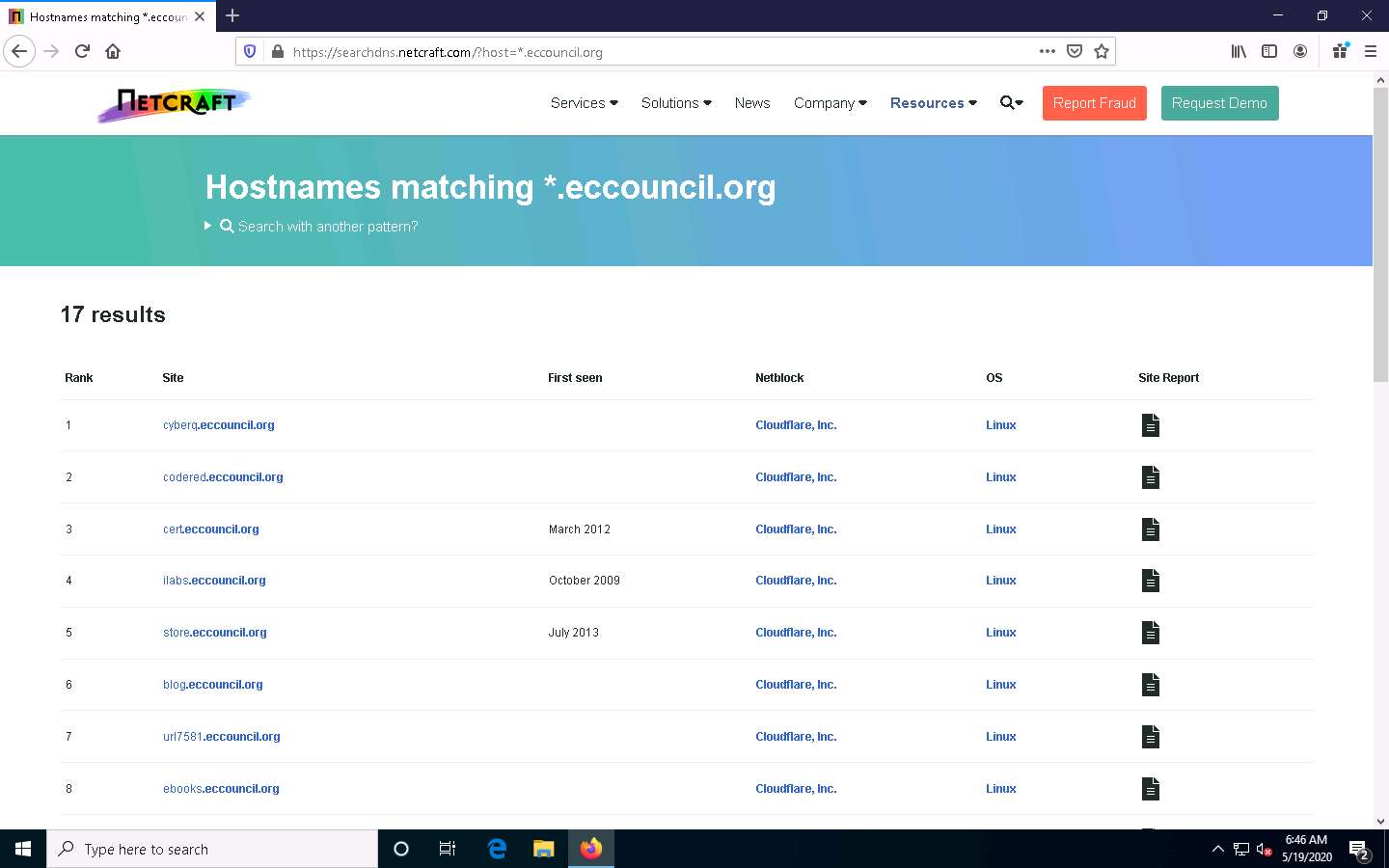
1. The **Site report for https://www.eccouncil.org** page appears, containing information related to **Background**, **Network**, **Hosting History**, etc., as shown in the screenshot.



1. In the **Network** section, click on the website link (here, **eccouncil.org**) in the **Domain** field to view the subdomains.



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



1. This concludes the demonstration of finding the company’s domains and sub-domains using the Netcraft tool.
2. You can also use tools such as **Sublist3r** (https://github.com), **Pentest-Tools Find Subdomains** (https://pentest-tools.com), etc. to identify the domains and sub-domains of any target website.
3. Close all open windows and document all the acquired information.

Task 2: Gather Personal Information using PeekYou Online People Search Service

Online people search services, also called public record websites, are used by many individuals to find personal information about others; these services provide names, addresses, contact details, date of birth, photographs, videos, profession, details about family and friends, social networking profiles, property information, and optional background on criminal checks.

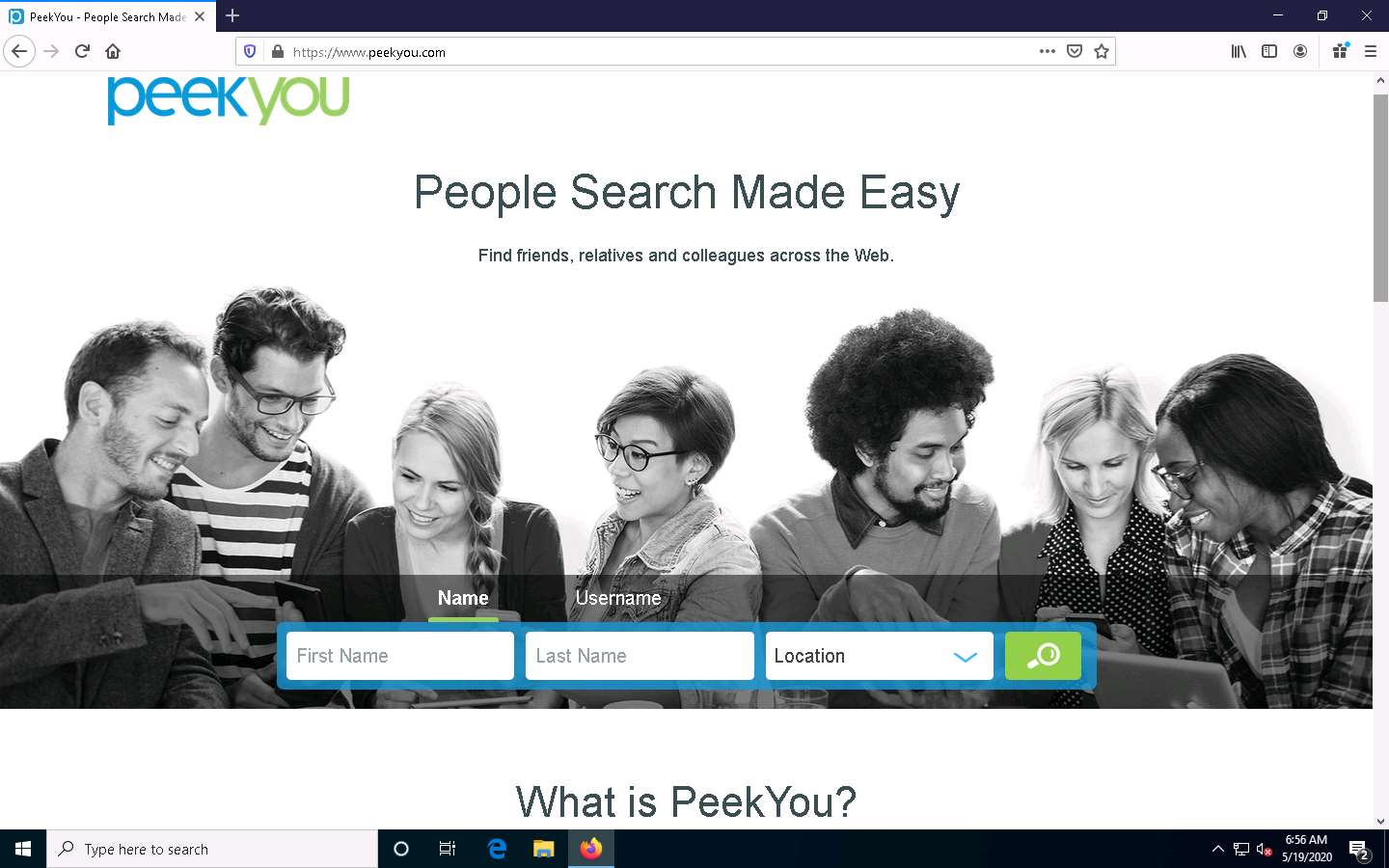
Here, we will gather information about a person from the target organization by performing people search using the PeekYou online people search service.

1. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and click https://www.peekyou.com and press **Enter**.

If you choose to use another web browser, the screenshots will differ.

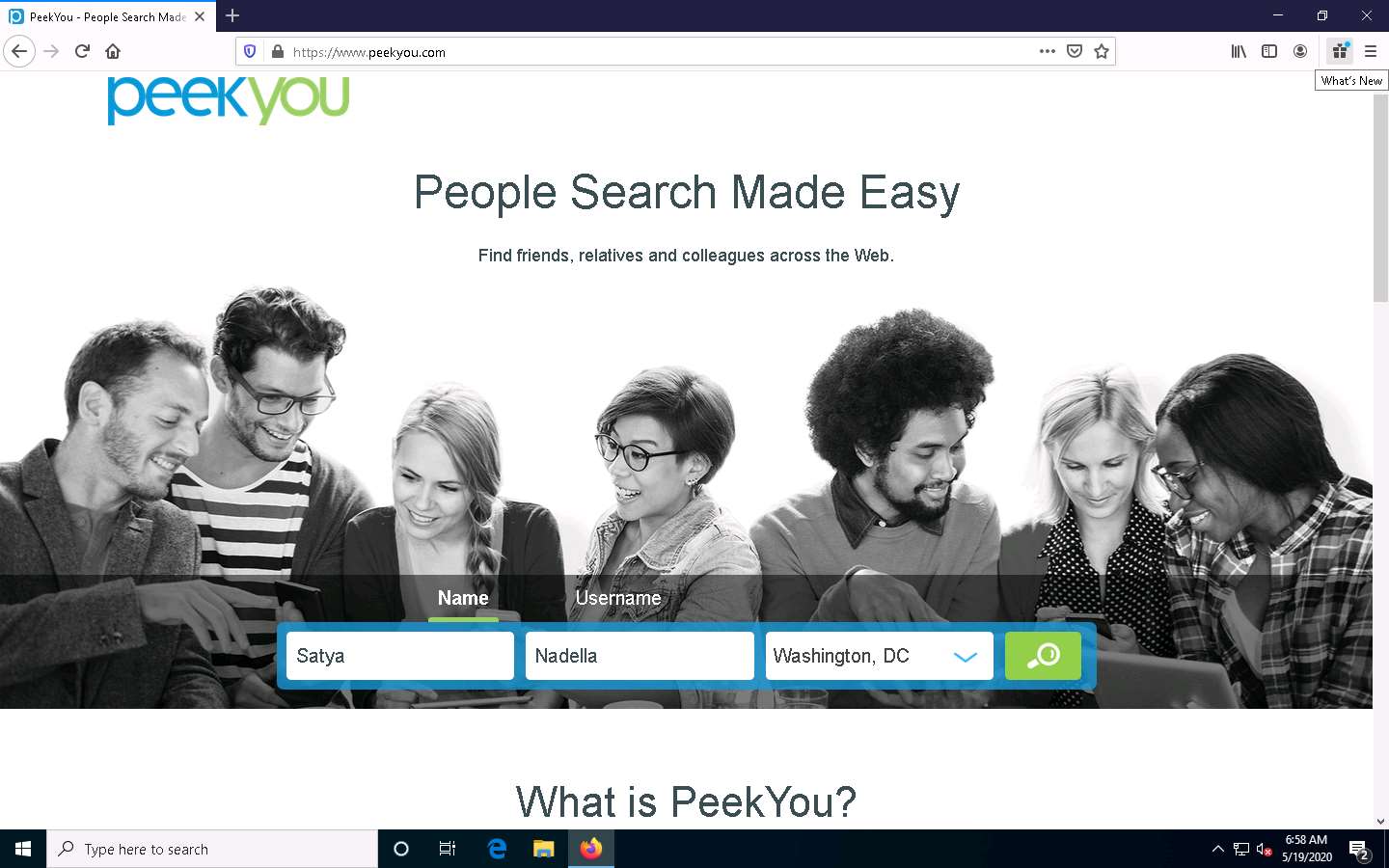
1. **PeekYou** page appears, as shown in the screenshot.

If cookie pop-up appears at the lower section of the browser, click **I agree**.

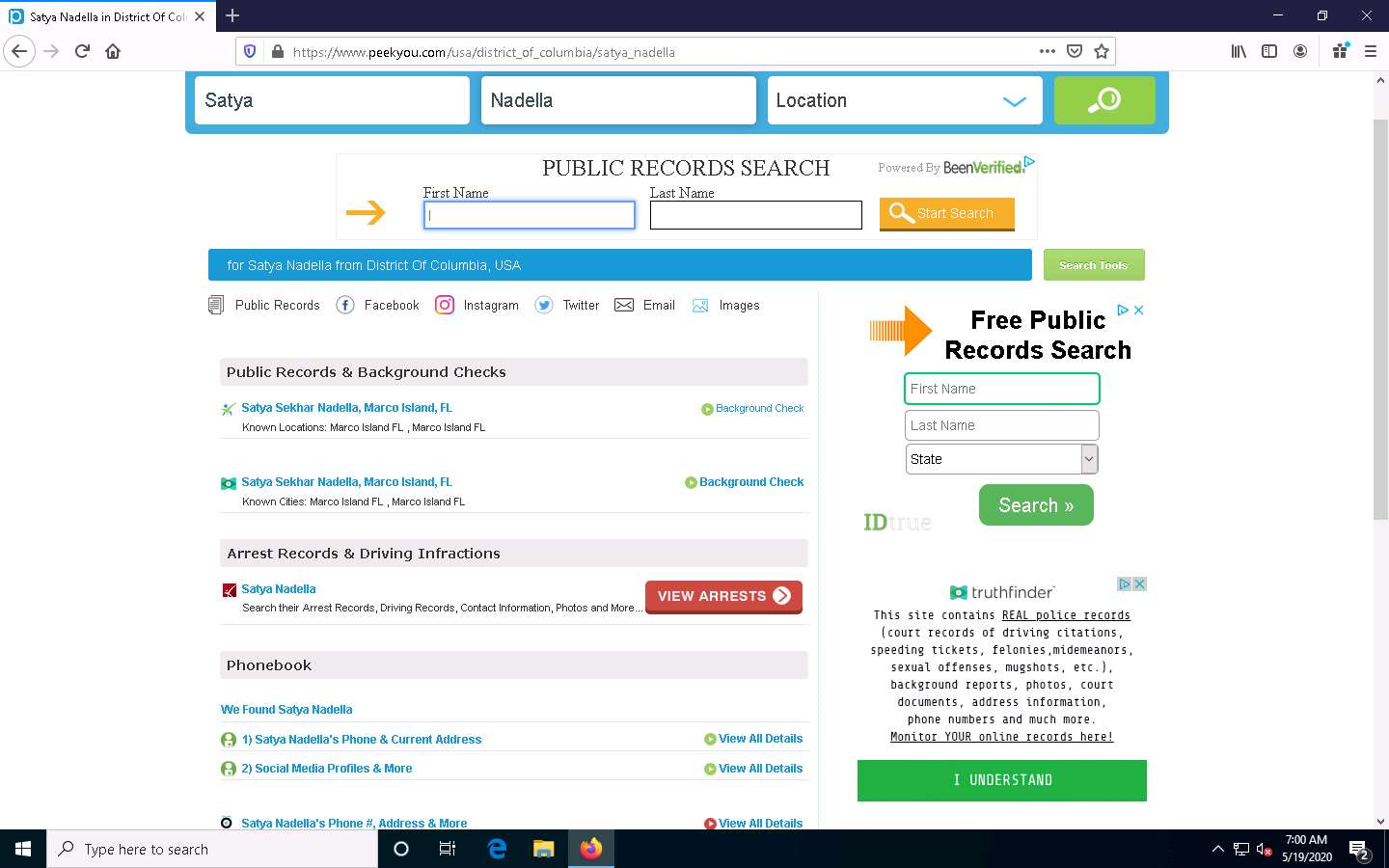


1. In the **First Name** and **Last Name** fields, type **Satya** and **Nadella**, respectively. In the **Location** drop-down box, select **Washington, DC**. Then, click the **Search** icon.

The list of location might differ in your lab environment.



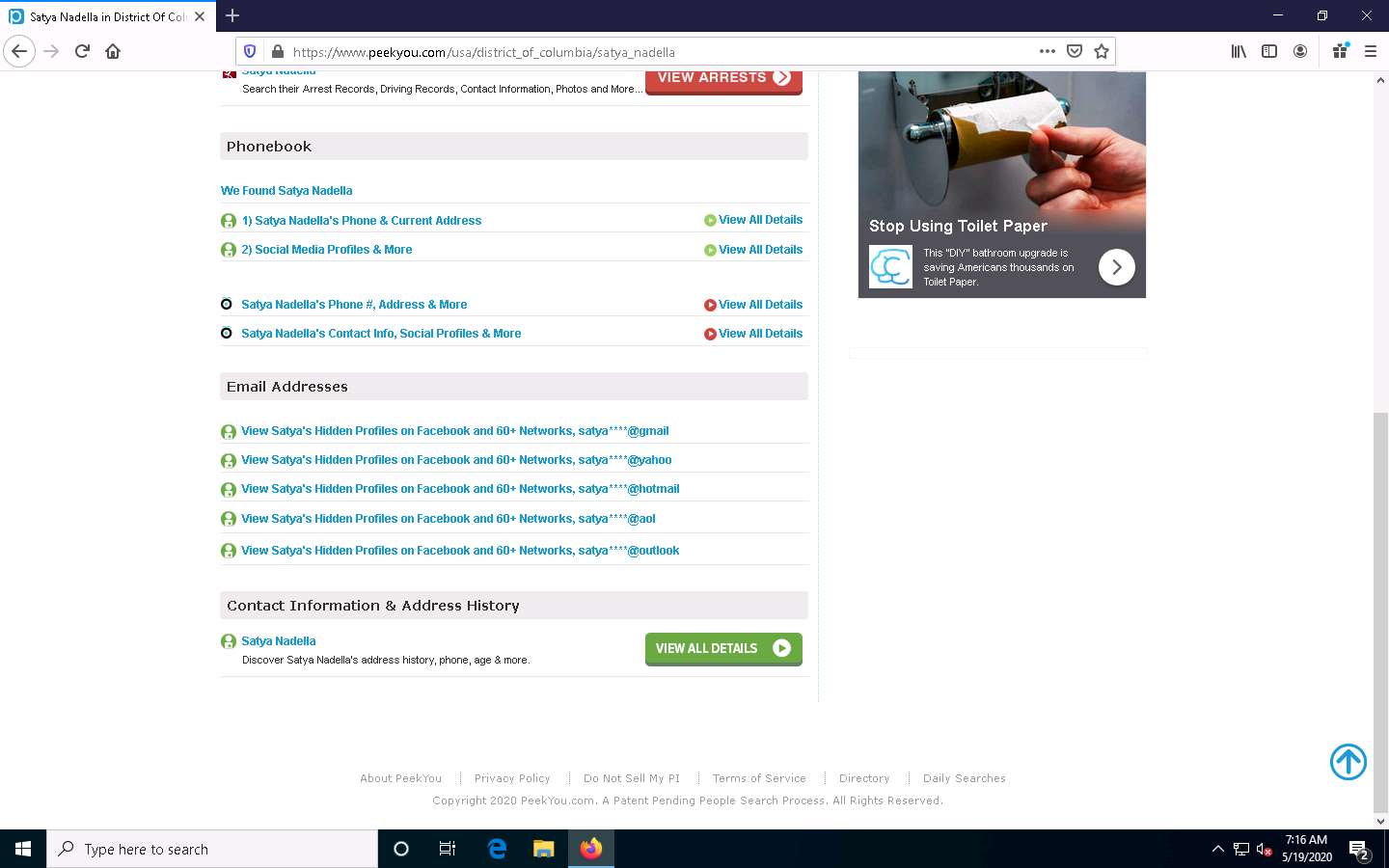
1. The people search begins, and the best matches for the provided search parameters will be displayed.



1. You can further click on the appropriate result to view the detailed information about the target person to see a detailed information about the target person.

After you click on any result, you will be redirected to a different website and it will take some time to load the information about the target.

1. Scroll down to view the entire information about the target person.



1. This concludes the demonstration of gathering personal information using the PeekYou online people search service.
2. You can also use **pipl** (https://pipl.com), **Intelius** (https://www.intelius.com), **BeenVerified** (https://www.beenverified.com), etc., which are people search services to gather personal information of key employees in the target organization.
3. Close all open windows and document all the acquired information

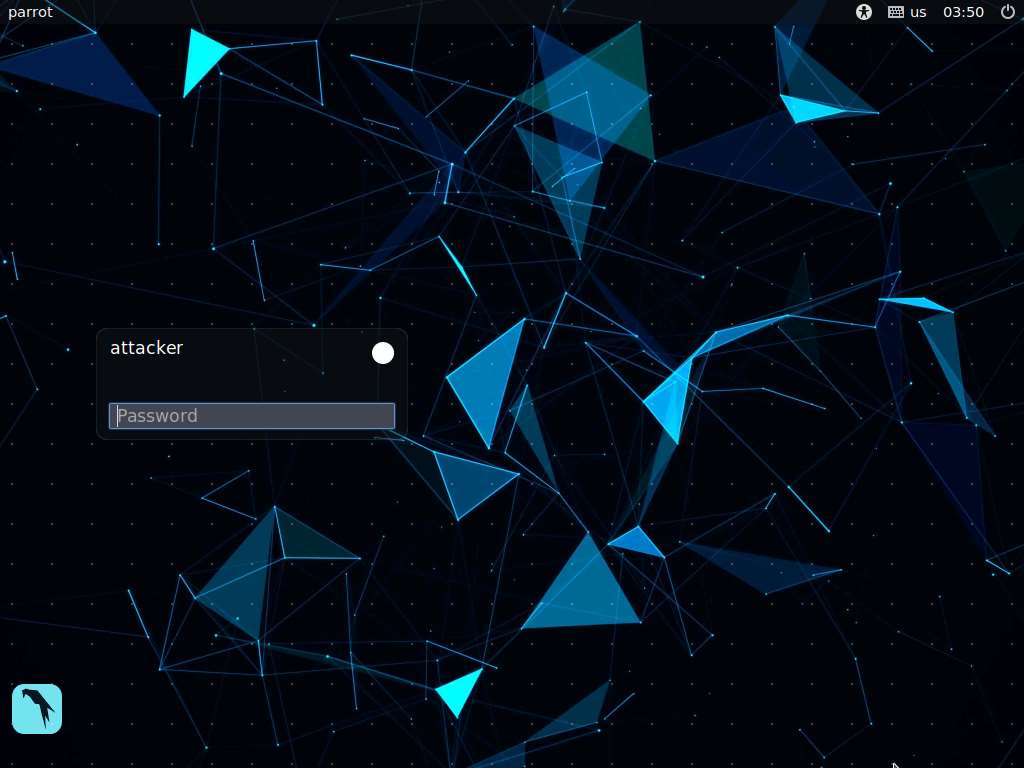
Task 3: Gather an Email List using theHarvester

Emails are messaging sources that are crucial for performing information exchange. Email ID is considered by most people as the personal identification of employees or organizations. Thus, gathering the email IDs of critical personnel is one of the key tasks of ethical hackers.

Here, we will gather the list of email IDs related to a target organization using theHarvester tool.

**theHarvester**: This tool gathers emails, subdomains, hosts, employee names, open ports, and banners from different public sources such as search engines, PGP key servers, and the SHODAN computer database as well as uses Google, Bing, SHODAN, etc. to extract valuable information from the target domain. This tool is intended to help ethical hackers and pen testers in the early stages of the security assessment to understand the organization’s footprint on the Internet. It is also useful for anyone who wants to know what organizational information is visible to an attacker.

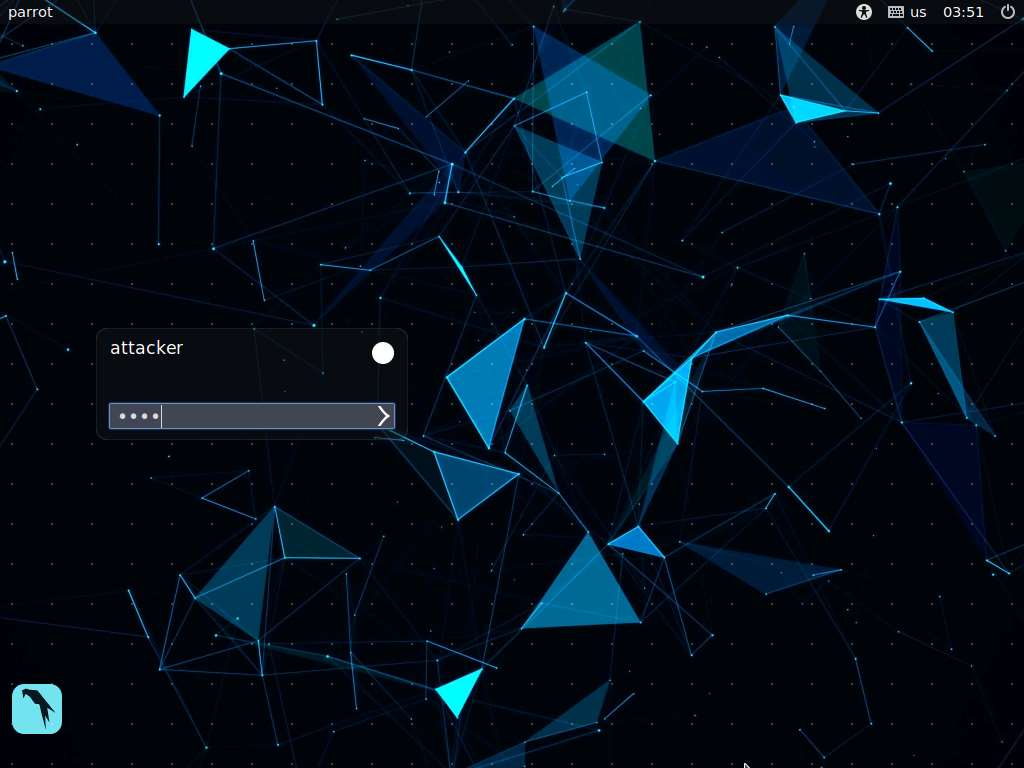
1. To launch **Parrot Security** machine, click [Parrot Security](https://labclient.labondemand.com/Instructions/b16bedc2-7151-47a3-9211-5daccdd8c426?rc=10).



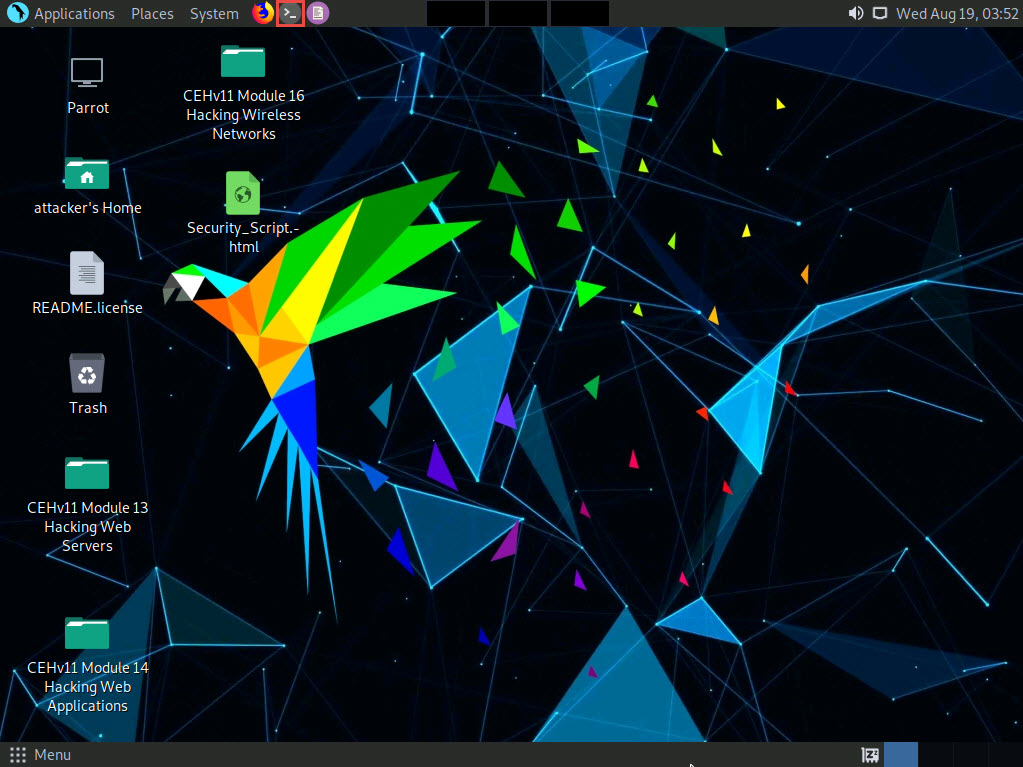
1. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



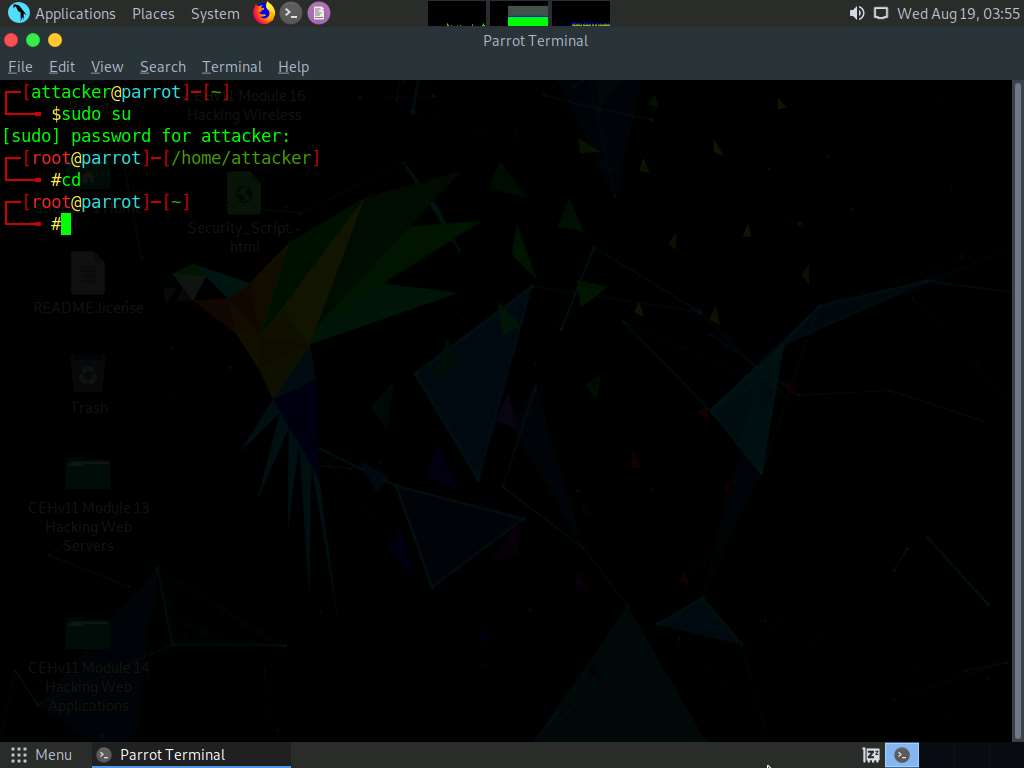
1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



1. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
2. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

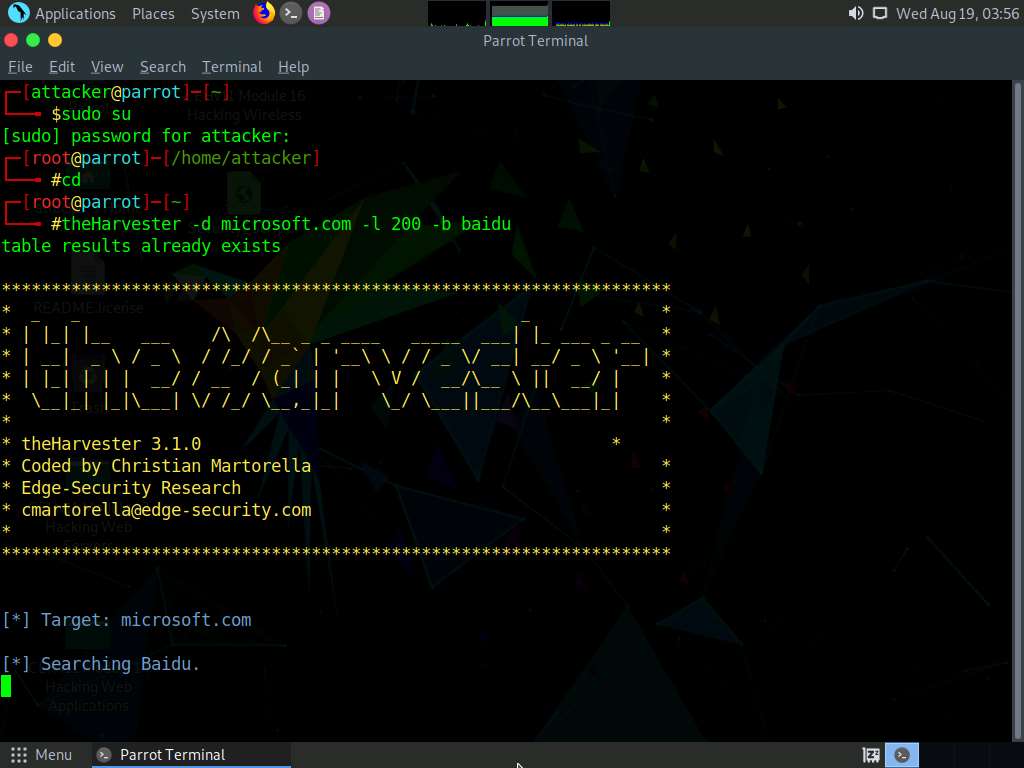
The password that you type will not be visible.

1. Now, type **cd** and press **Enter** to jump to the root directory.



1. In the terminal window, type **theHarvester -d microsoft.com -l 200 -b baidu** and press **Enter**.

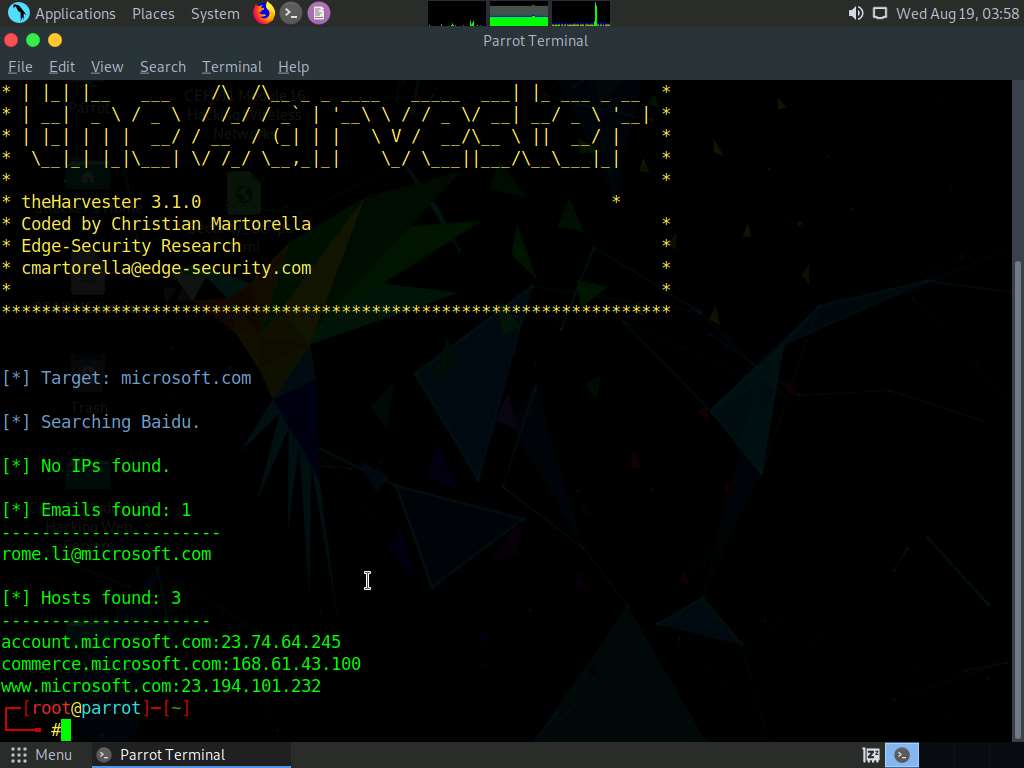
In this command, **-d** specifies the domain or company name to search, **-l** specifies the number of results to be retrieved, and **-b** specifies the data source.



1. theHarvester starts extracting the details and displays them on the screen. You can see the email IDs related to the target company and target company hosts obtained from the Baidu source, as shown in the screenshot.

The results might differ when you perform the lab.

Here, we specify Baidu search engine as a data source. You can specify different data sources (e.g., Baidu, bing, bingapi, dogpile, Google, GoogleCSE, Googleplus, Google-profiles, linkedin, pgp, twitter, vhost, virustotal, threatcrowd, crtsh, netcraft, yahoo, all) to gather information about the target.



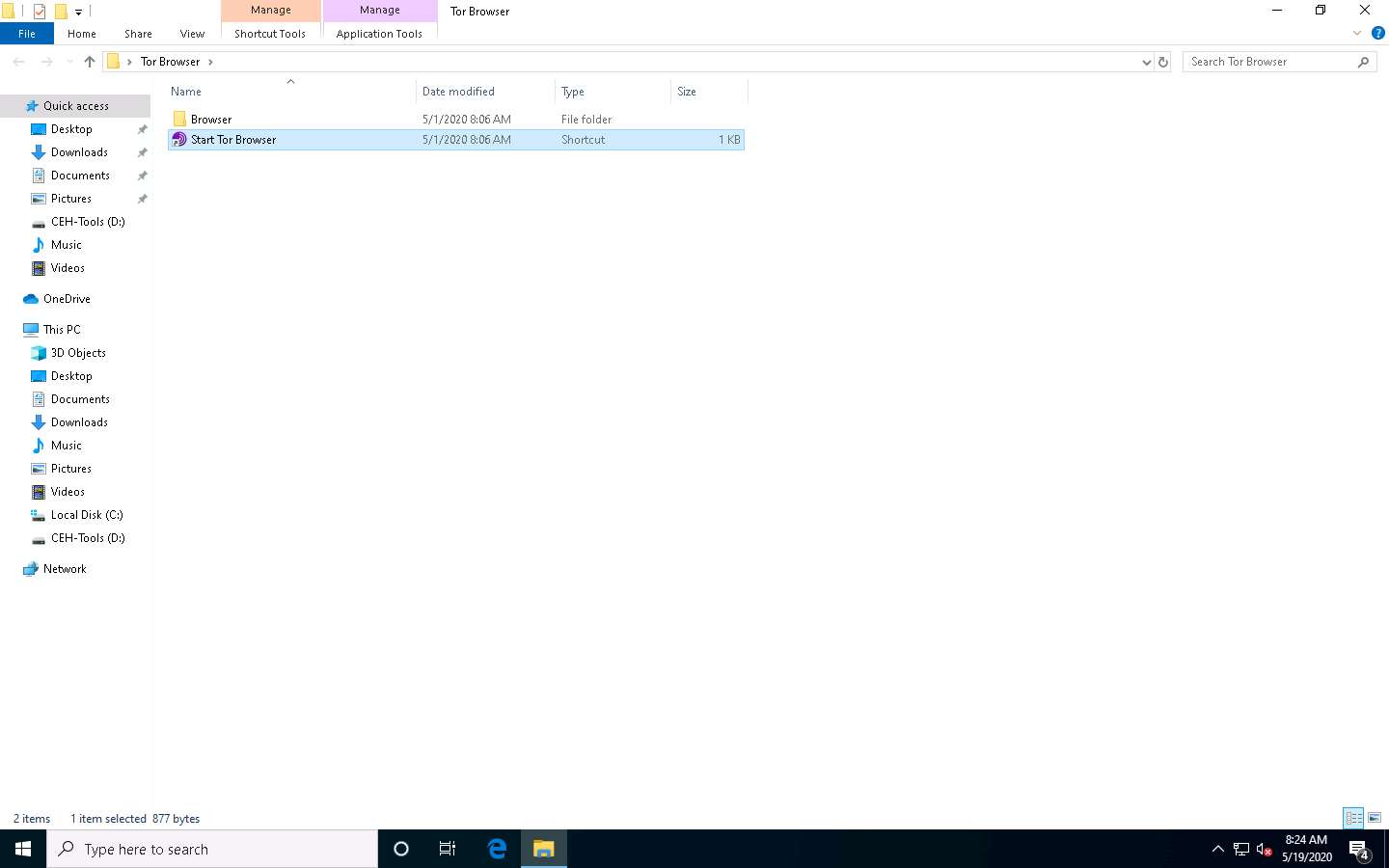
1. This concludes the demonstration of gathering an email list using theHarvester.
2. Close all open windows and document all the acquired information.

Task 4: Gather Information using Deep and Dark Web Searching

The deep web consists of web pages and content that are hidden and unindexed and cannot be located using a traditional web browser and search engines. It can be accessed by search engines such as Tor Browser and The WWW Virtual Library. The dark web or dark net is a subset of the deep web, where anyone can navigate anonymously without being traced. Deep and dark web search can provide critical information such as credit card details, passports information, identification card details, medical records, social media accounts, Social Security Numbers (SSNs), etc.

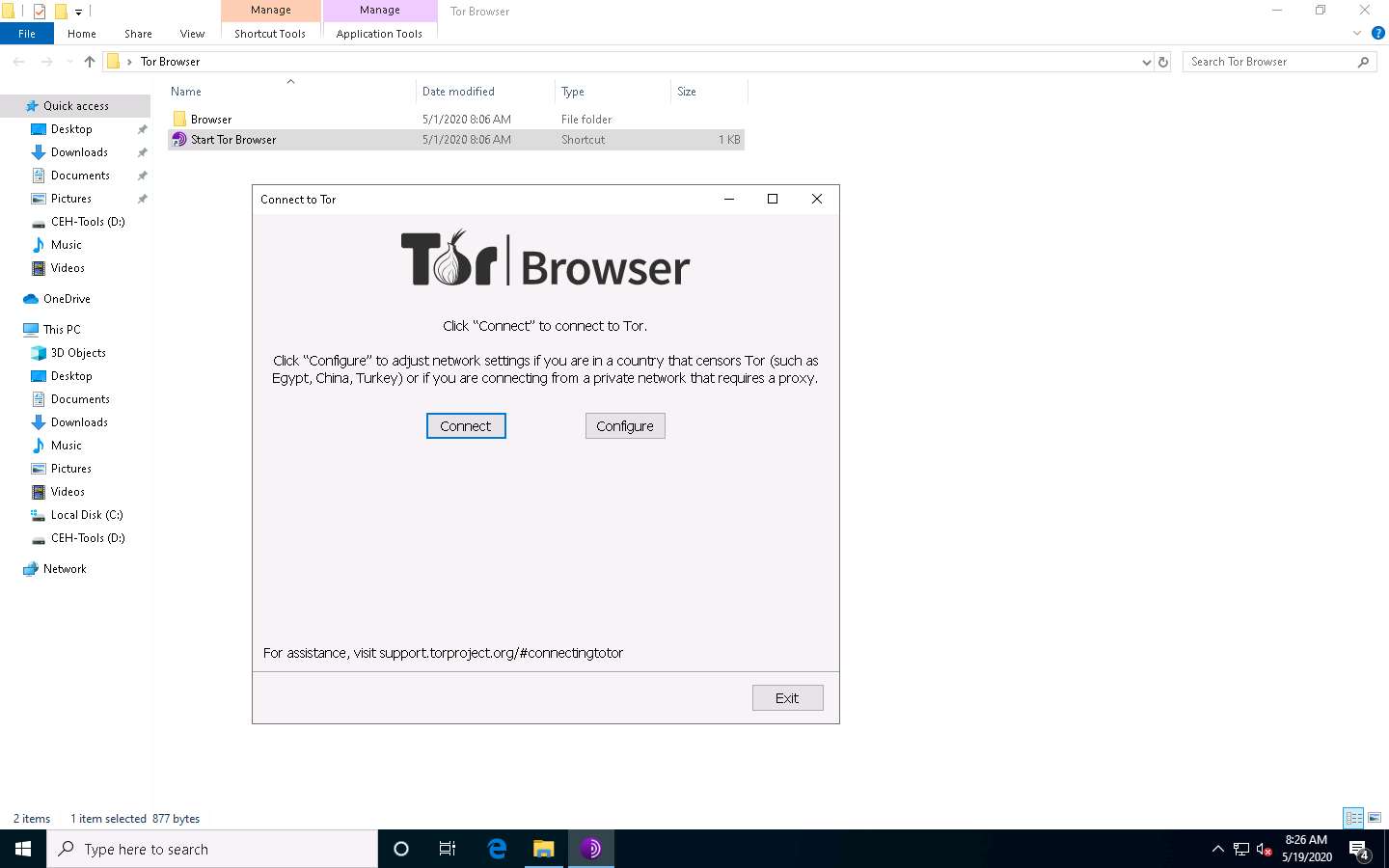
Here, we will understand the difference between surface web search and dark web search using Mozilla Firefox and Tor Browser.

1. Click [Windows 10](https://labclient.labondemand.com/Instructions/b16bedc2-7151-47a3-9211-5daccdd8c426?rc=10) to switch to the **Windows 10** machine.
2. Open a **File Explorer**, navigate to **C:\Users\Admin\Desktop\Tor Browser**, and double-click **Start Tor Browser**.

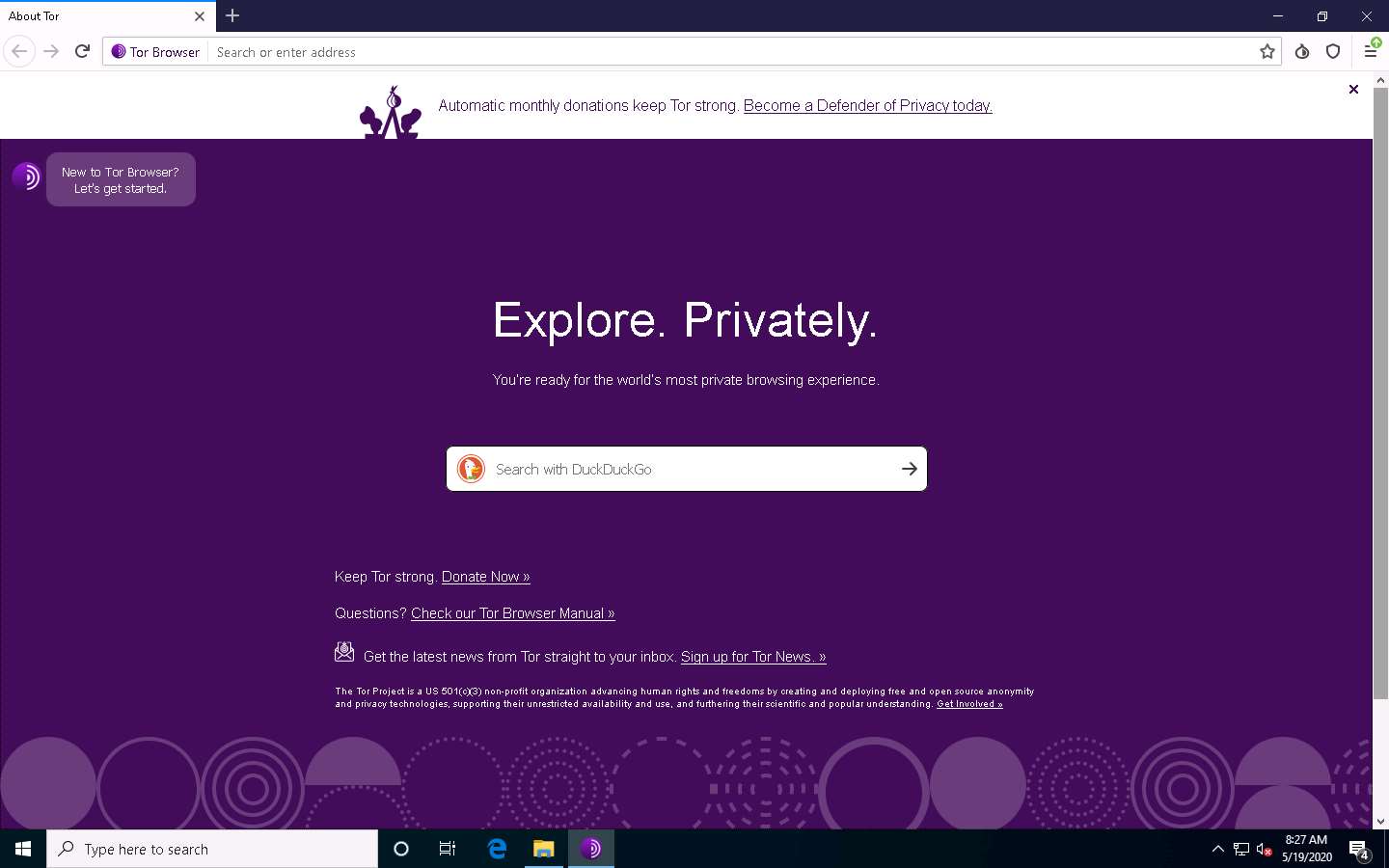


1. The **Connect to Tor** window appears. Click the **Connect** button to directly browse through Tor Browser’s default settings.

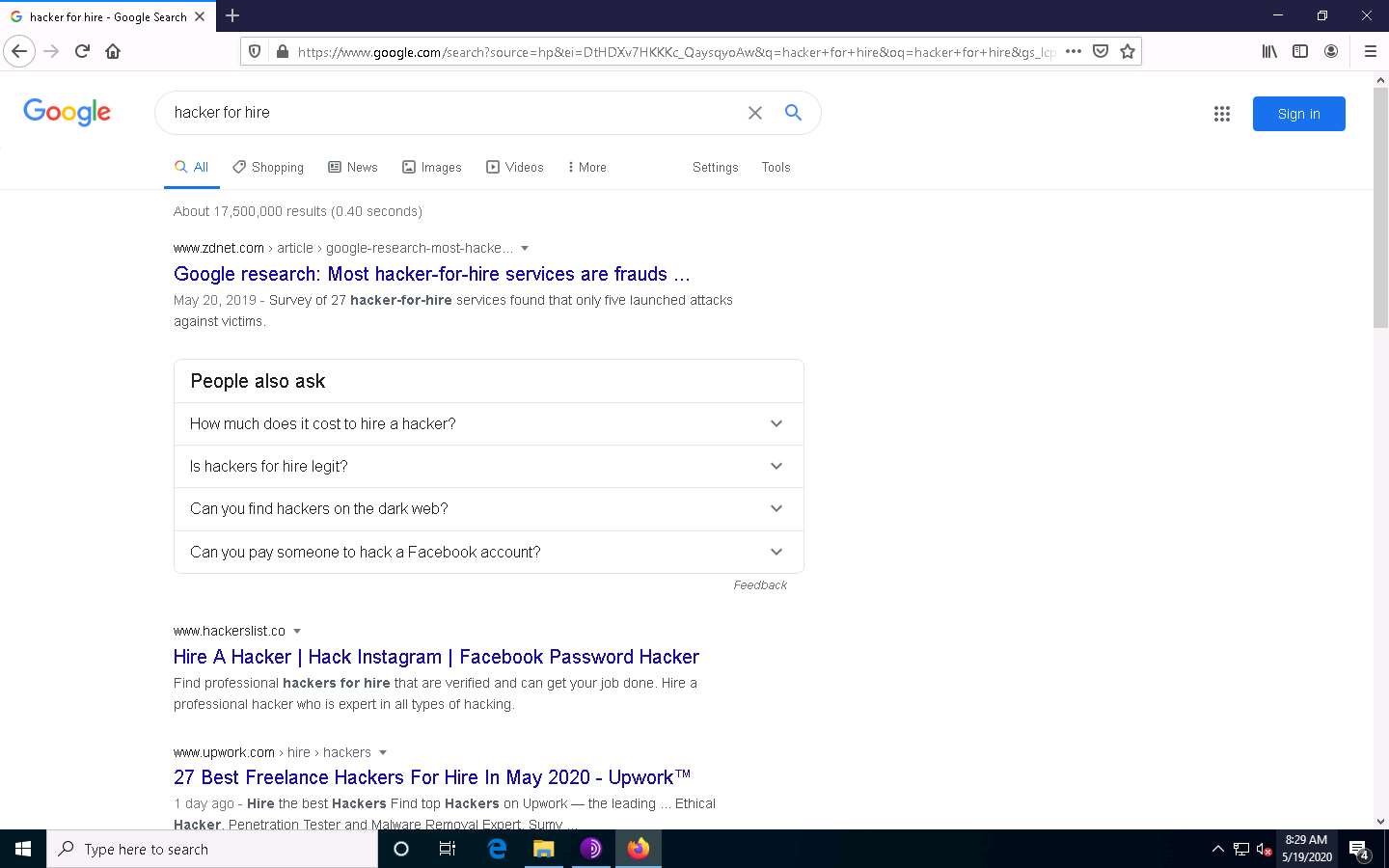
If Tor is censored in your country or if you want to connect through Proxy, click the Configure button and continue.



1. After a few seconds, the Tor Browser home page appears. The main advantage of Tor Browser is that it maintains the anonymity of the user throughout the session.



1. As an ethical hacker, you need to collect all possible information related to the target organization from the dark web. Before doing so, you must know the difference between surface web searching and dark web searching.
2. To understand surface web searching, first, minimize **Tor Browser** and open **Mozilla Firefox**. Navigate to **www.google.com**; in the Google search bar, search for information related to **hacker for hire**. You will be presented with much irrelevant data, as shown in the screenshot.



1. Now switch to **Tor Browser** and search for the same (i.e., **hacker for hire**). You will find the relevant links related to the professional hackers who operate underground through the dark web.

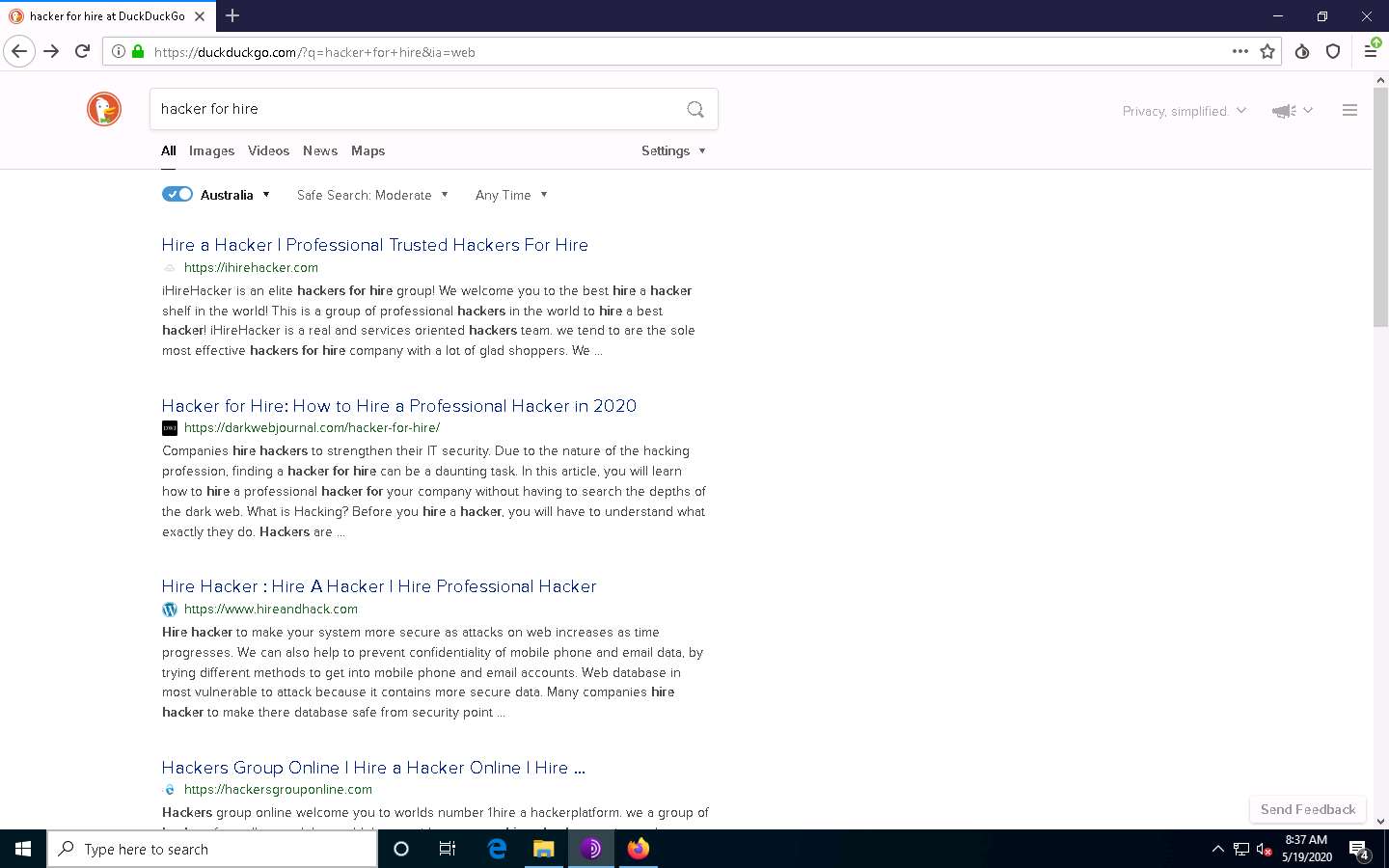
Tor uses the **DuckDuckGo** search engine to perform a dark web search. The results may vary in your environment.

1. Now, click on the toggle button that specifies the country of VPN/Proxy (here, by default, **Germany** is selected) and select a relevant country (here, **Australia**).

Here, country might differ in your lab environment.

1. Search results for **hacker for hire** will be loaded, as shown in the screenshot. Click to open any of the search results (here, **https://ihirehacker.com**).

The search results will be different in your lab environment.



1. The **https://ihirehacker.com** webpage opens up, as shown in the screenshot. You can see that the site belongs to professional hackers who operate underground.



1. ihirehacker is an example. These search results will help you in identifying professional hackers. However, as an ethical hacker, you can gather critical and sensitive information about your target organization using deep and dark web search.
2. You can also anonymously explore the following onion sites using Tor Brower to gather other relevant information about the target organization:
   * **The Hidden Wiki** is an onion site that works as a Wikipedia service of hidden websites. (http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main\_Page)
   * **FakeID** is an onion site for creating fake passports (http://fakeidskhfik46ux.onion/)
   * **The Paypal Cent** is an onion site that sells PayPal accounts with good balances (http://nare7pqnmnojs2pg.onion/)
3. You can also use tools such as **ExoneraTor** (https://metrics.torproject.org), **OnionLand Search engine** (https://onionlandsearchengine.com), etc. to perform deep and dark web browsing.
4. This concludes the demonstration of gathering information using deep and dark web searching using Tor Browser.
5. Close all open windows and document all the acquired information.

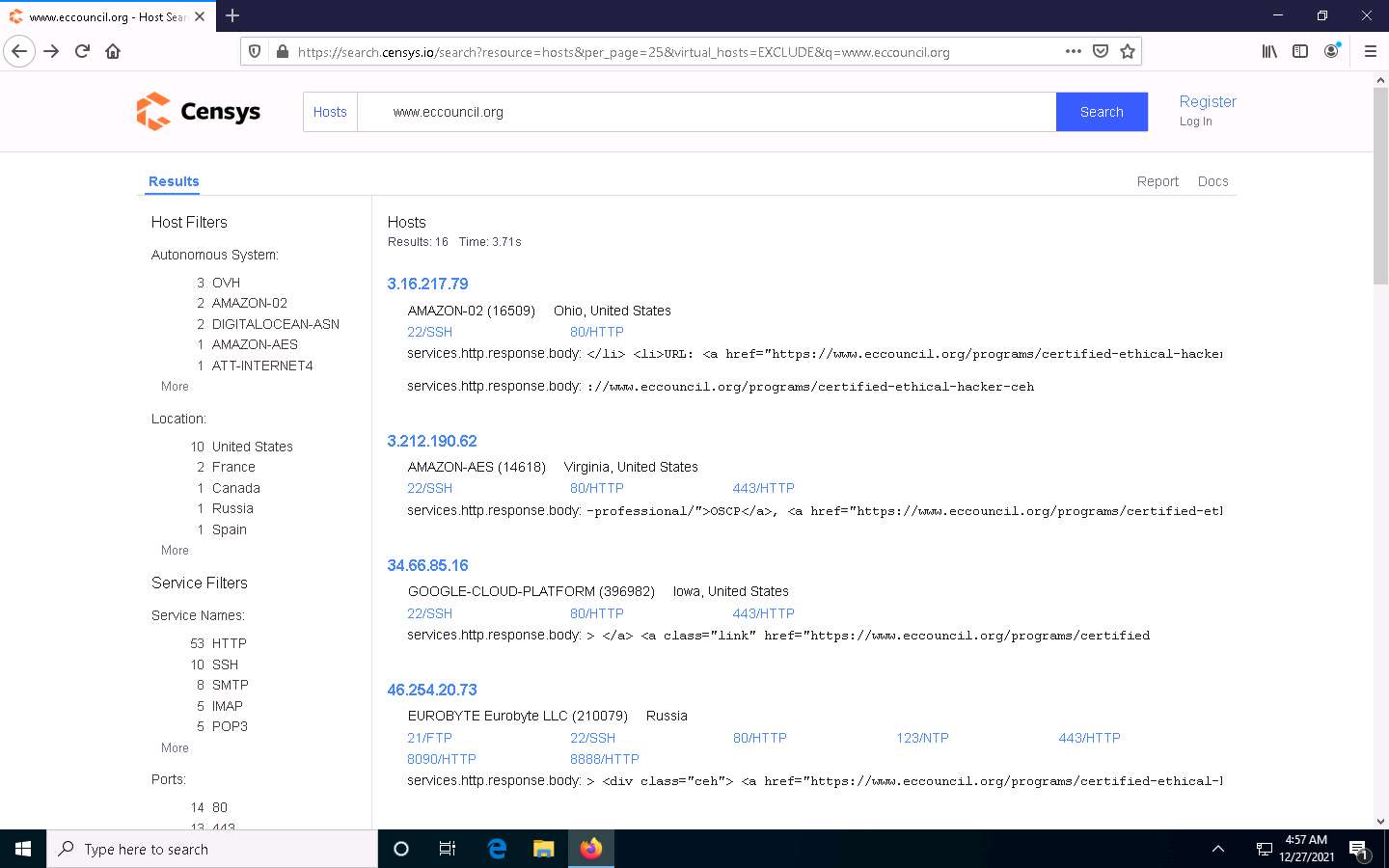
Task 5: Determine Target OS Through Passive Footprinting

Operating system information is crucial for every ethical hacker. Ethical hackers can acquire details of the operating system running on the target machine by performing various passive footprinting techniques.

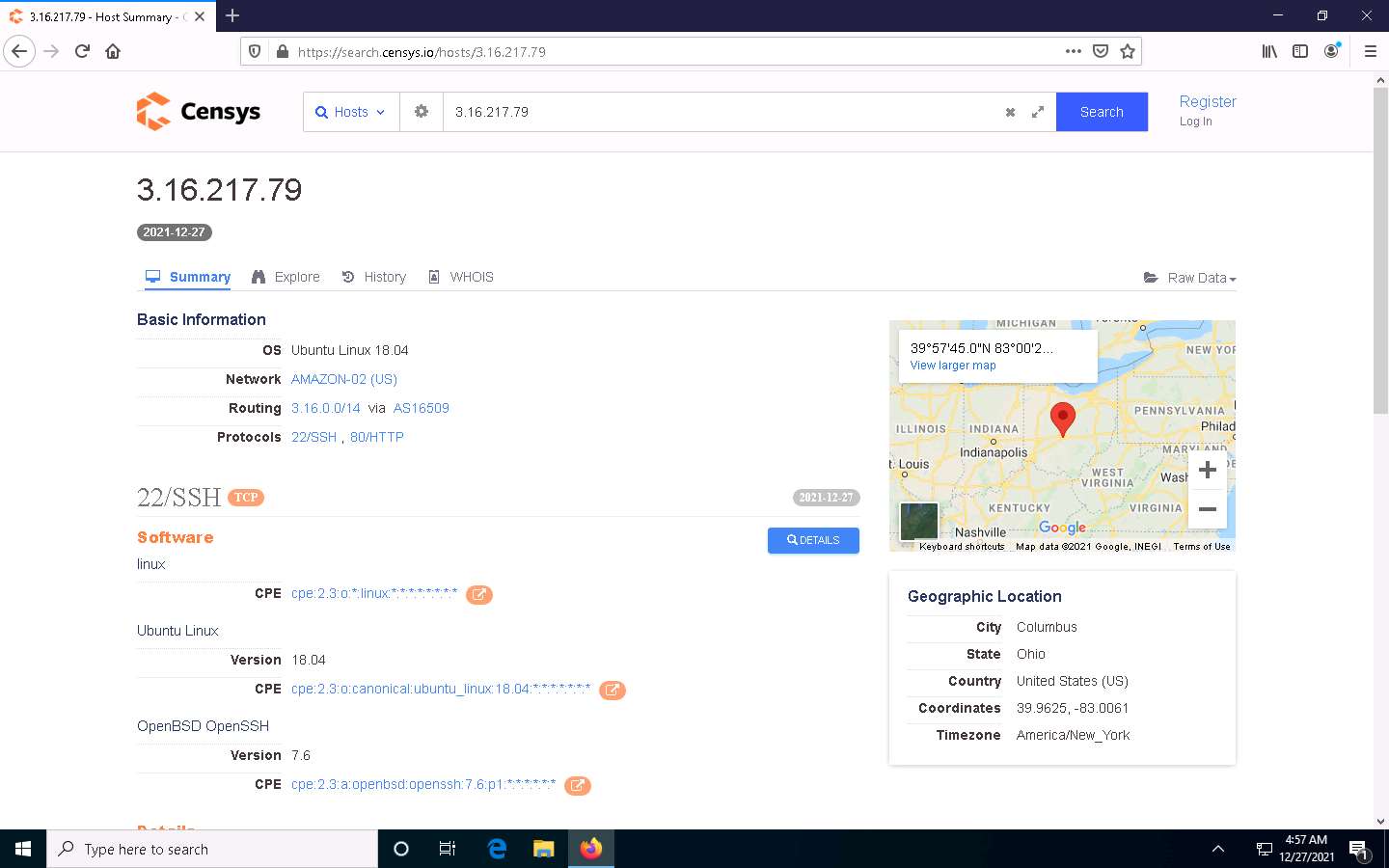
Here, we will gather target OS information through passive footprinting using the Censys web service.

1. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and click https://censys.io/domain?q= and press **Enter**.
2. In the search field, type the target website (here, **www.eccouncil.org**) and press **Enter**. From the results, click any **Hosts** IP address which you want to gather the OS details.

The result might differ, when you perform this lab task.



1. The selected host page appears, as shown in the screenshot. Under the **Basic Information** section, you can observe that the **OS** is **Ubuntu**. Apart from this, you can also observe other details such as protocols running, host keys, etc.



1. This concludes the demonstration of gathering OS information through passive footprinting using the Censys web service.
2. You can also use webservices such as **Netcraft** (https://www.netcraft.com), **Shodan** (https://www.shodan.io), etc. to gather OS information of target organization through passive footprinting.
3. Close all open windows and document all the acquired information.