CEH v12 Lesson 1 : Footprinting & Reconnaissance

Footprinting & Reconnaissance Part 1

Exercise 1 — Footprinting and Reconnaissance

Exercise 2 — Footprinting Using Search Engines

Exercise 3 — Footprinting Using Web Services

Exercise 4 — Footprinting through Social Networking Sites

Exercise 5 — Website Footprinting

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 — Footprinting and Reconnaissance
- Exercise 2 — Footprinting Using Search Engines
- Exercise 3 — Footprinting Using Web Services
- Exercise 4 — Footprinting through Social Networking Sites
- Exercise 5 — Website Footprinting

After completing this module, you will be able to:

- Footprint Using Google Advanced Search Operators
- Use Web Services for Footprinting
- Footprint using Opencorporates
- Footprint using source code
- Footprint Using Archive.org
- Create a Wordlist Using CeWL

- Perform Banner Grabbing using Nmap

After completing this module, you will have further knowledge of:

- Footprinting Concepts
- Footprinting Methodology
- Footprinting Countermeasures
- Footprinting Methodology

Lab Duration

It will take approximately **1 hour** to complete this lab.

Footprinting Concepts

You, as an ethical hacker, can collect some of the following information about a target using reconnaissance or Footprinting:

- Collect the basic information using Web searches
- Locate the live systems on the network
- Determine the network size
- Identify the open ports and running services
- Determine the operating system version

Some experts consider that reconnaissance has three parts or phases, which are:

1. **Footprinting**: It is about collecting information about an organization passively.
2. **Scanning**: It uses active reconnaissance methods, such as nmap scanning to extract information about networks and systems.
3. **Enumeration**: After the first two, Footprinting and Scanning, are complete, you can use the information to find the area that you want to attack. For example, if an attacker finds out that a specific version of Apache is being used, an attacker can narrow down the attack to exploit its vulnerabilities.

Reconnaissance or Footprinting can either be active or passive.

Active

Using the active reconnaissance method, you directly interact with the system. For example, you can execute a nmap command to collect information about open ports.

Active Reconaissance can include the following methods:

- Performing IP or Port scanning
- Perform operating system scanning
- Conduct Footprinting of existing services in a system
- Perform zone transfer on an internal DNS server
- Spider the public Webpages
- Perform fuzzing
- Conduct Social Engineering

Passive

On the other hand, passive reconnaissance is the opposite of active reconnaissance. You do not interact with the system. Rather, you use various methods, such as a Web search, to find the information about a target.

Passive reconnaissance can use the following methods:

- Search the Whois database
- Browse through a target's website
- Perform Social Network scraping
- Search Google or any search engine
- Extract DNS information
- Review blogs, public forums, and Websites
- Search breach databases and DarkWeb about a target

Objectives of Footprinting

Whether you are a hacker or an ethical hacker, Footprinting plays a vital role in gathering information. Without Footprinting, it would be difficult for a hacker to break into a system or network. Therefore, hackers spend a significant amount of time gathering information about the organization's system or network. Hackers build their hacking strategy and execute it based on the collected information. As an ethical hacker, you gain the following benefits when you perform Footprinting:

Understand Security Posture When your footprint is an organization's network, you can understand the footprint of the organization's security posture. For example, you can understand if the organization has single-layered security, such as a firewall, which contains multiple layers of security devices. You can gain information on the security devices, the level of defense, and much more information about the security implementation. Based on the information that you collect, you build your attack accordingly.**Reduce Focus Area**

A focus or attack area is a term used for a target system or network you want to exploit. When an attacker focuses on a smaller area, such as a single system, they are more agile and reduce the chances of being noticed. Generally, an attacker would reduce the focus area to a network subnet, a specific domain name, or an individual system that connects to the Internet directly.

Identifty VulnerabilitiesA detailed footprint of a target system maximizes the information an attacker can use. This information can be put into a database for analysis which will then identify the weak areas or vulnerabilities in the system. An attacker will go after those first.**Draw Network Diagrams**Using the Footprinting method, you can collect information and generate a network diagram to help you understand the network layout. For example, you can run the tracert tool to find the path from a system to a target system. A network diagram clarifies how systems are placed on a network. For example, you can find whether the Internet-facing servers are placed on the same network or a separate network, such as the demilitarized zone (DMZ).

Footprinting Tools

Various tools can be used in reconnaissance or footprinting, such as:

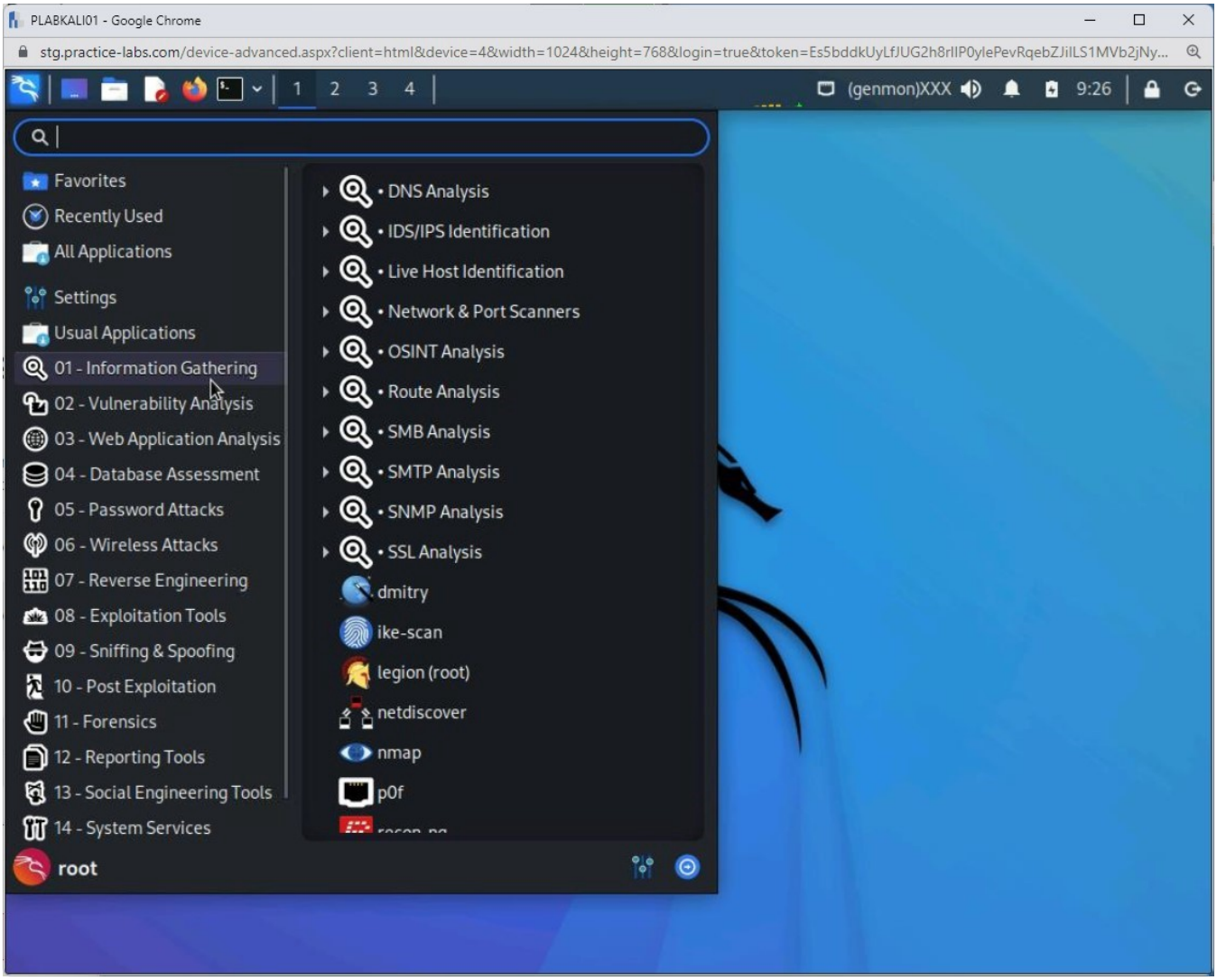
- **Whois** — Queries for domain names
- **Nslookup** — Queries DNS
- **FOCA** — Enumeration for users, files, folders, and OS information

- **theHarvester** — Information gathering for an Email address, subdomains, hostnames, banners
- **Shodan** — Information search engine using metadata
- **Maltego** — Information gathering
- **Recon-ng** — Web reconnaissance
- **Censys** — Search engine for information about devices on the Internet

Kali Linux also includes reconnaissance or Footprinting tools under different categories, which are:

- DNS Analysis
- IDS/IPS Identification
- Live Host Identification
- Network & Port Scanners
- OSINT Analysis
- Route Analysis
- SMB Analysis
- SMTP Analysis
- SNMP Analysis
- SSL Analysis

You will be using some of these tools in this module.



Footprinting Methodology

Footprinting is a method of collecting information about a target. The information can be of different types, such as:

- IP address
- Email address
- Geolocations
- Domain and subdomain names
- Contact information

To collect information, an attacker can use a variety of tools. An attacker can use various techniques as part of the Footprinting methodology to collect information. These techniques are:

- Search Engines Footprinting

- Web Services Footprinting
- Social Networking Sites Footprinting
- Website Footprinting
- Email Footprinting
- Whois Footprinting
- DNS Footprinting
- Network Footprinting
- Social Engineering Footprinting

Each of these techniques is covered in separate exercises in this module.

Exercise 2 — Footprinting Using Search Engines

Search engines can provide a wealth of information about the target organizations. You can simply type the name of the organization in the search field. The search results can provide information, such as:

- The physical location of the organization's offices
- Contact information
- Email addresses
- Employee names

An attacker can use all this information to initiate an attack. For example, an attacker can initiate a social engineering attack using contact information, telephone, or mobile numbers.

In this exercise, you will use footprint using search engines.

Learning Outcomes

After completing this exercise, you will be able to:

- Footprinting Using Google Advanced Search Operators

Your Devices

You will be using the following devices in this lab. Please power these on now.

PLABDC01Domain Controller192.168.0.1/24PLABWIN10Domain MemberWorkstation192.168.0.3/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

Task 1 — Footprint Using Google Advanced Search Operators

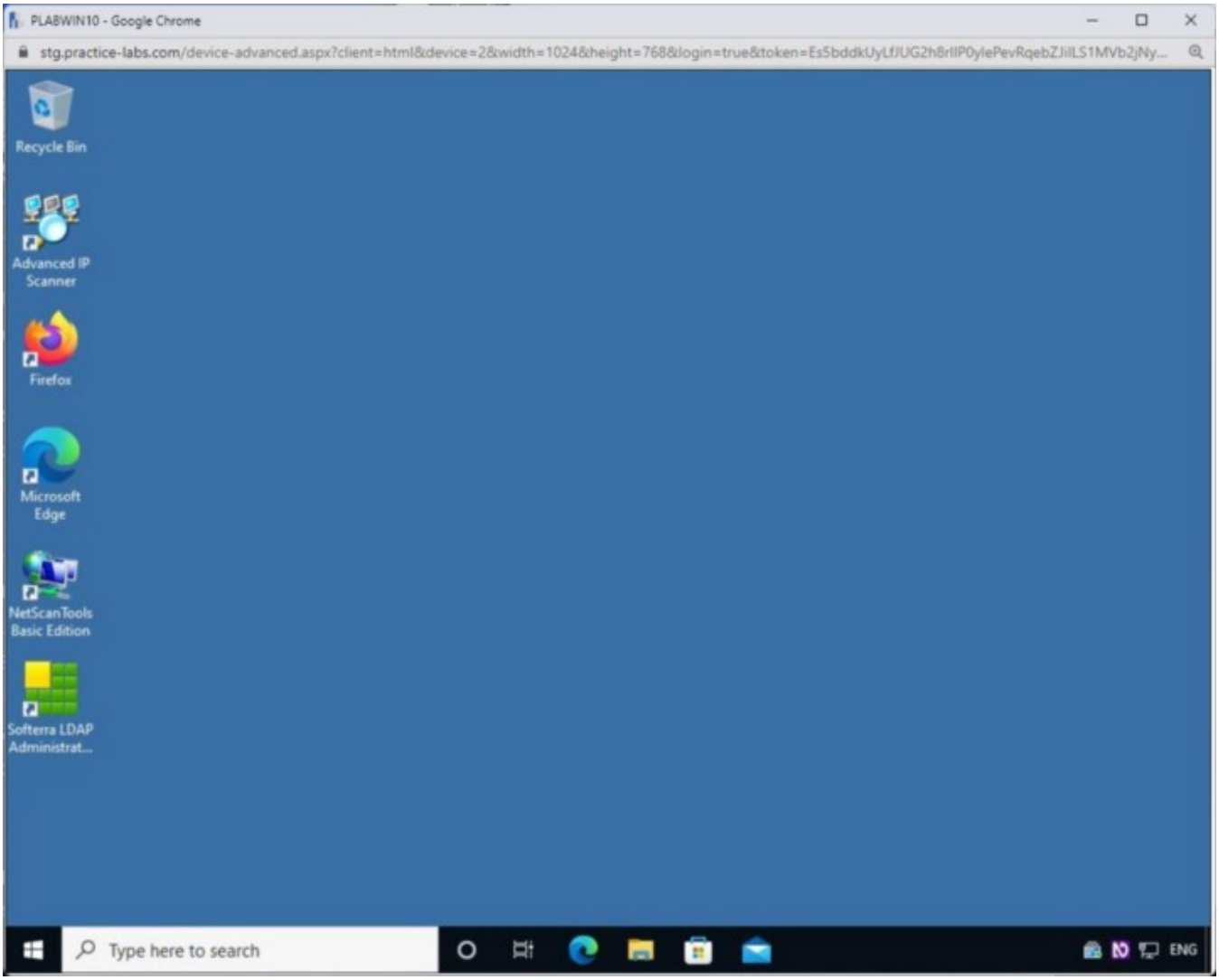
Search engines, such as Google, provide advanced search operators to retrieve information that would have been not easily retrievable from the search engine. With the help of search operators, you can narrow down your search and get the information you need.

With Google specifically, you have several advanced search operators that can locate information. Even though Google provides several keywords, you will use a few key ones in this task.

In this task, you will learn to use some of the key Google Advanced Search Operators.

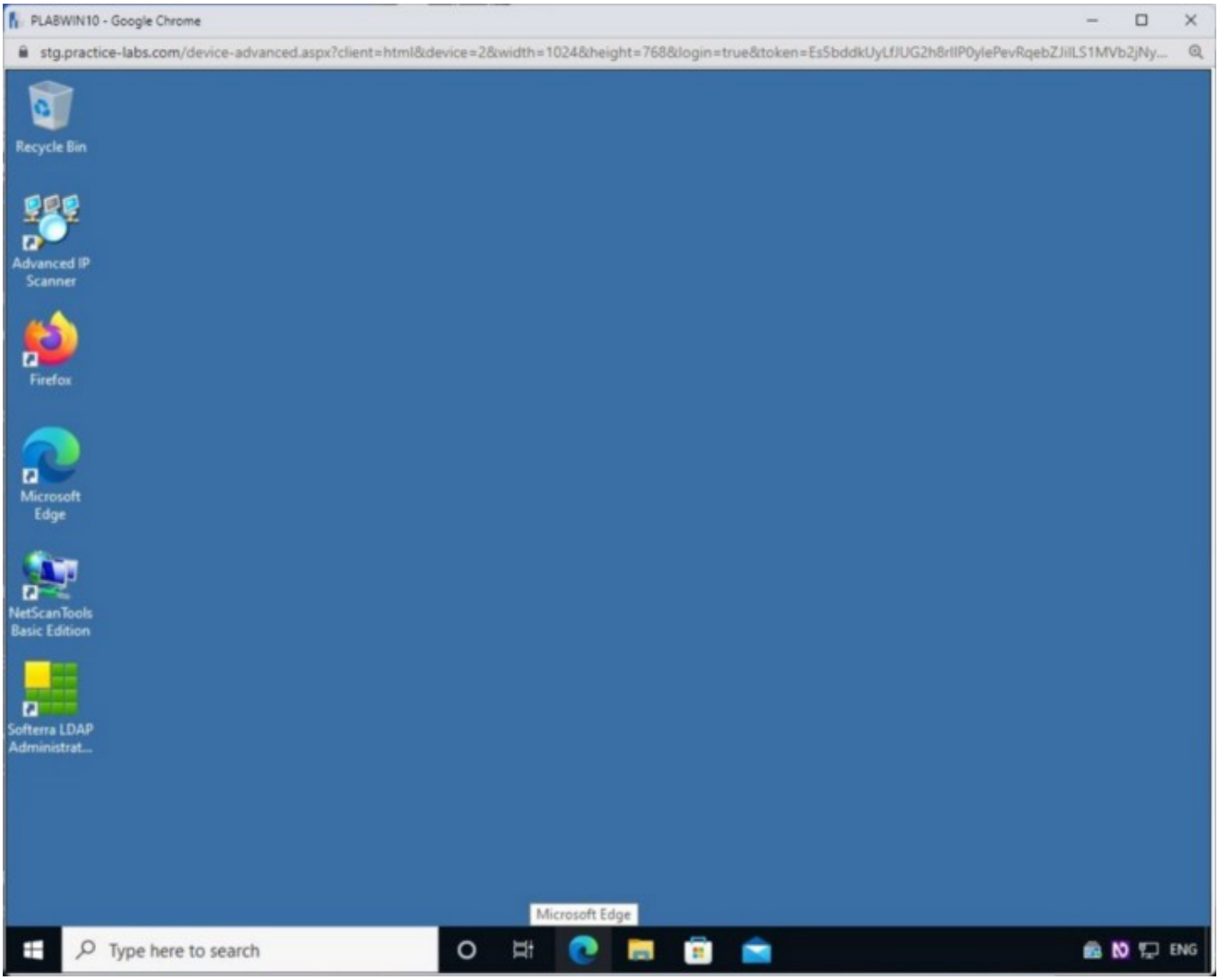
Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10**.



Step 2

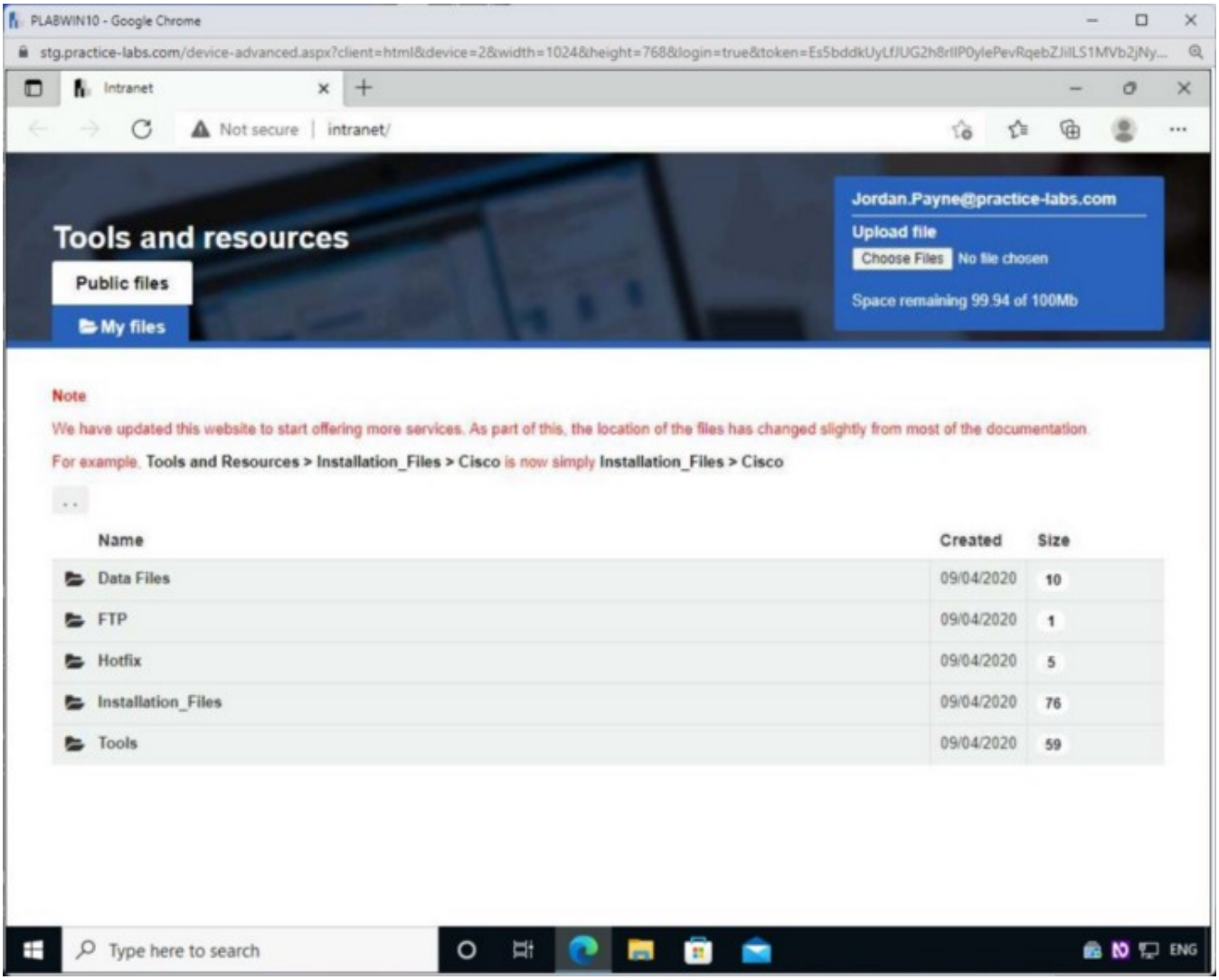
From the taskbar, click the **Microsoft Edge** icon.



Step 3

The **Microsoft Edge** window opens.

The default homepage, the **Practice Labs Intranet**, is displayed.



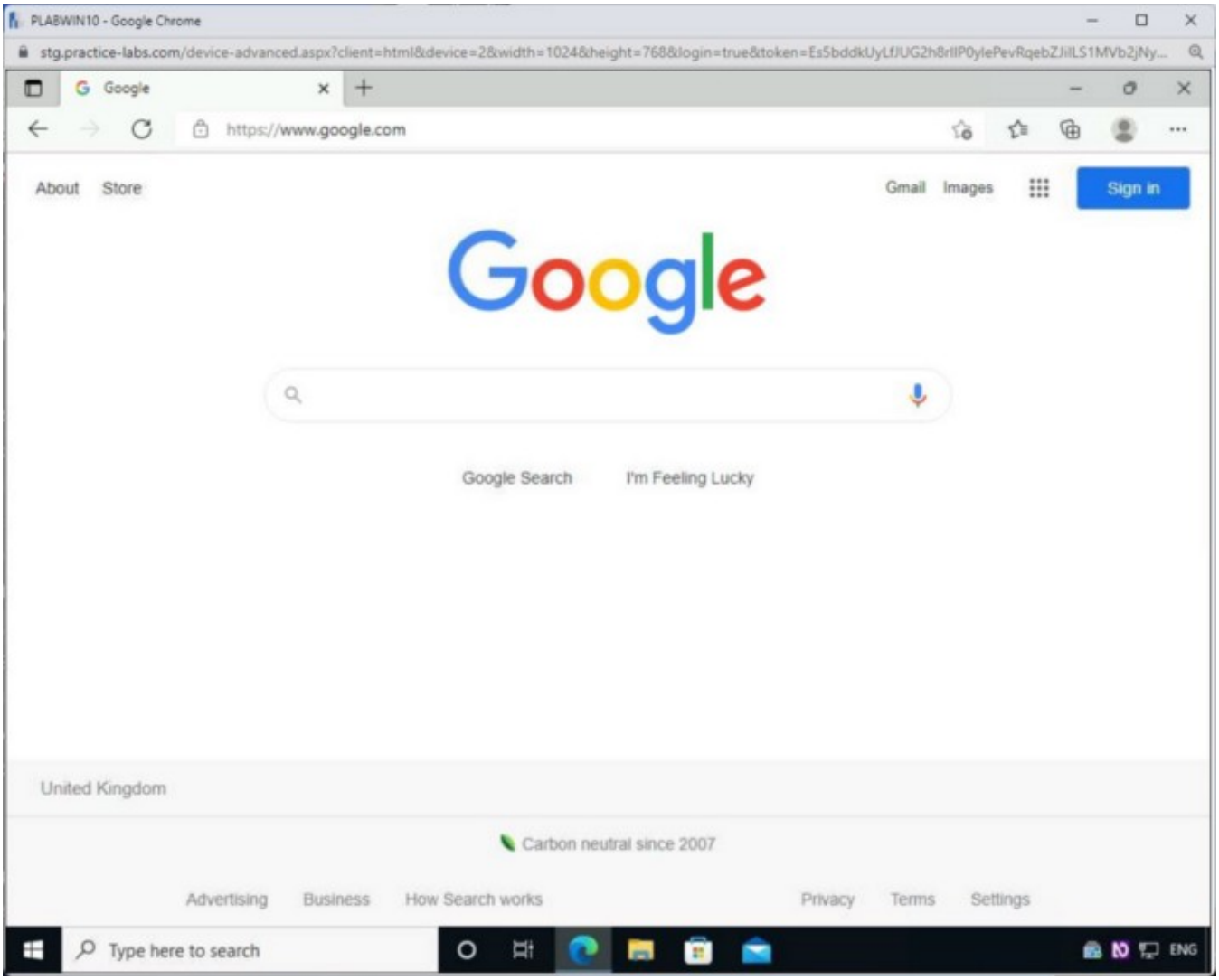
Step 4

In the address bar, navigate to the following URL:

`https://www.google.com`

Press **Enter**.

The **Google** website is displayed.

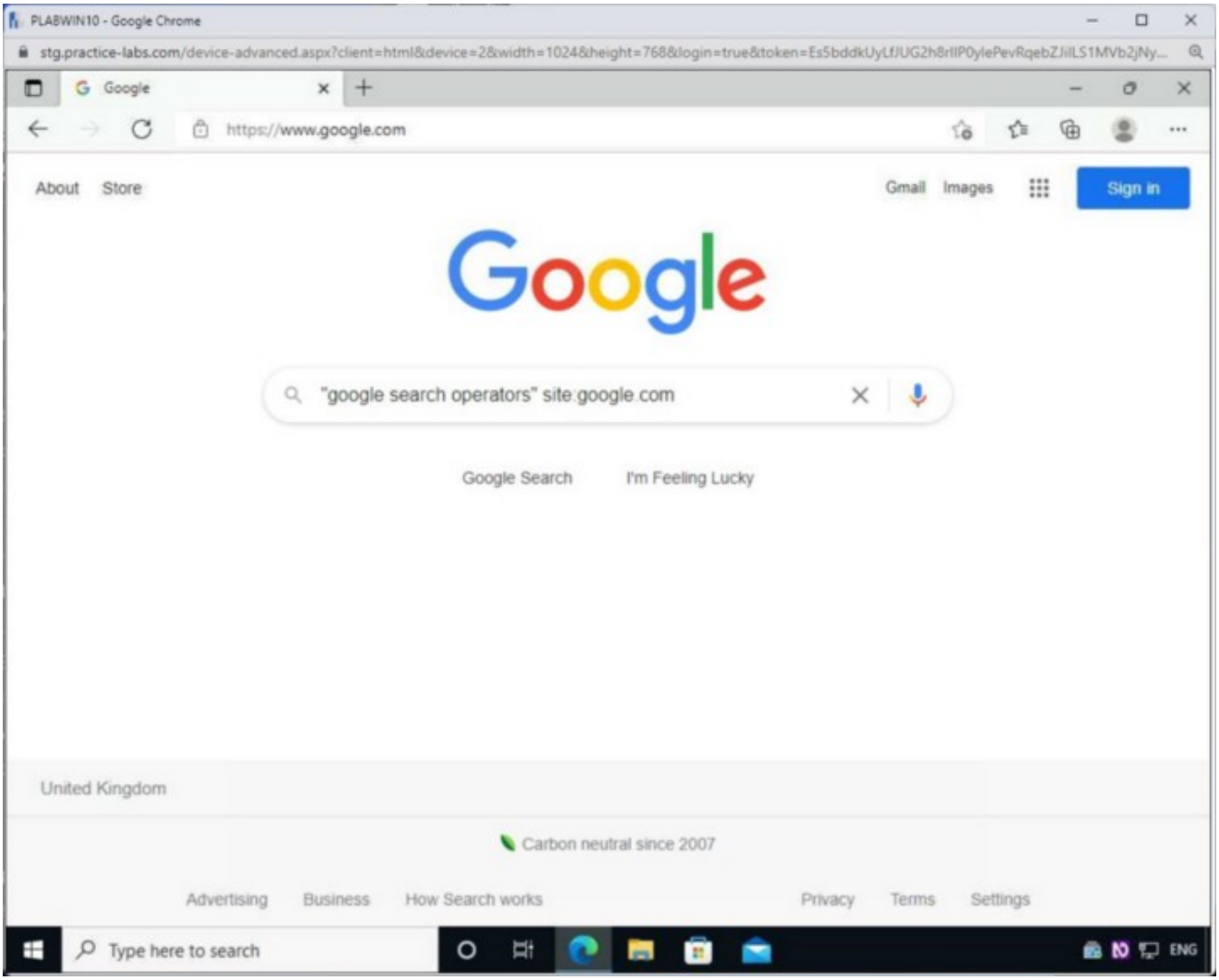


Step 5

In the search text box, type the following:

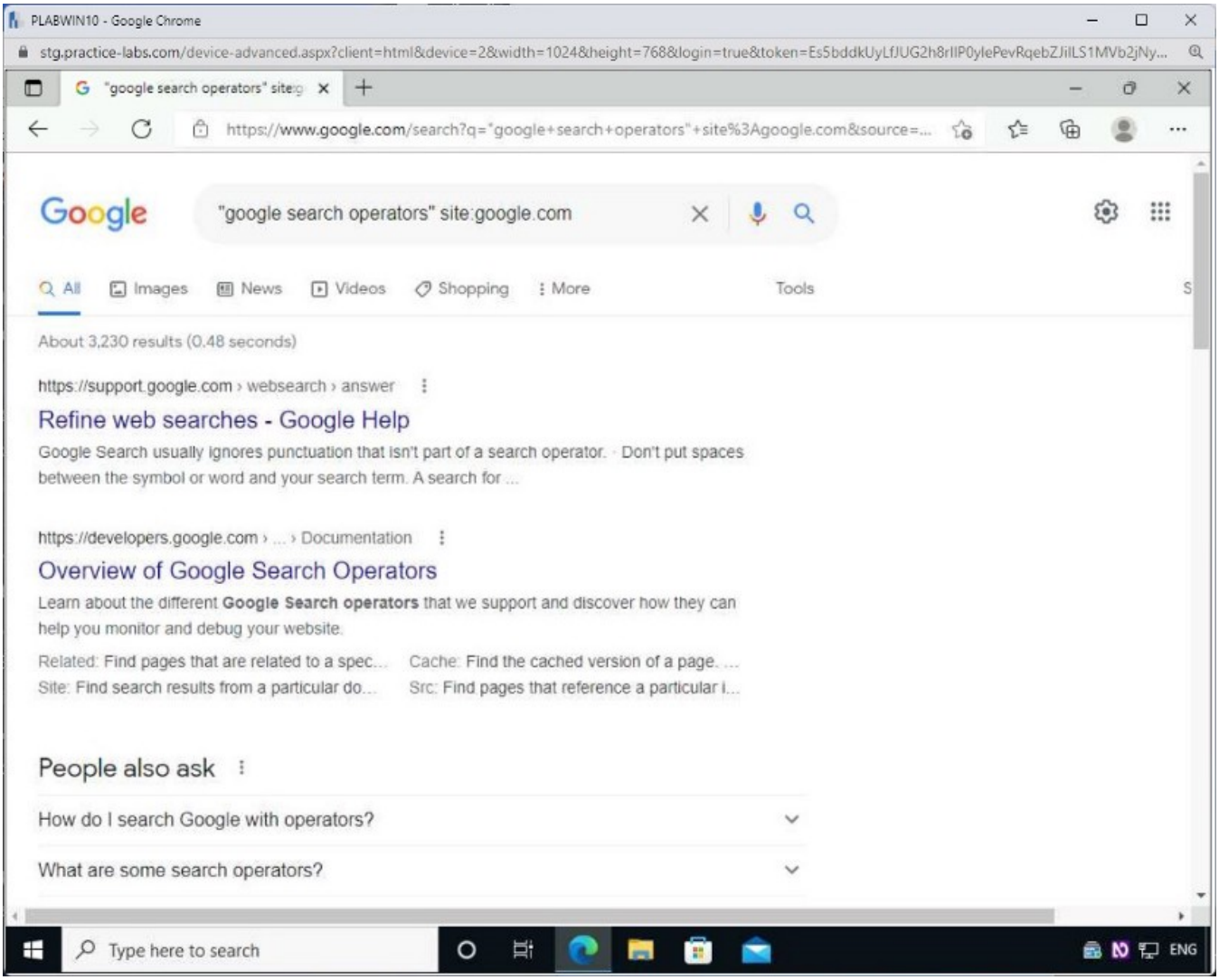
```
"google search operators" site:google.com
```

Press **Enter**. In this case, you use the **site** keyword to restrict the search to a specific website. In this case, you are restricting the searched string to **google.com**.



Step 6

Notice that all the search results are only from **google.com**.



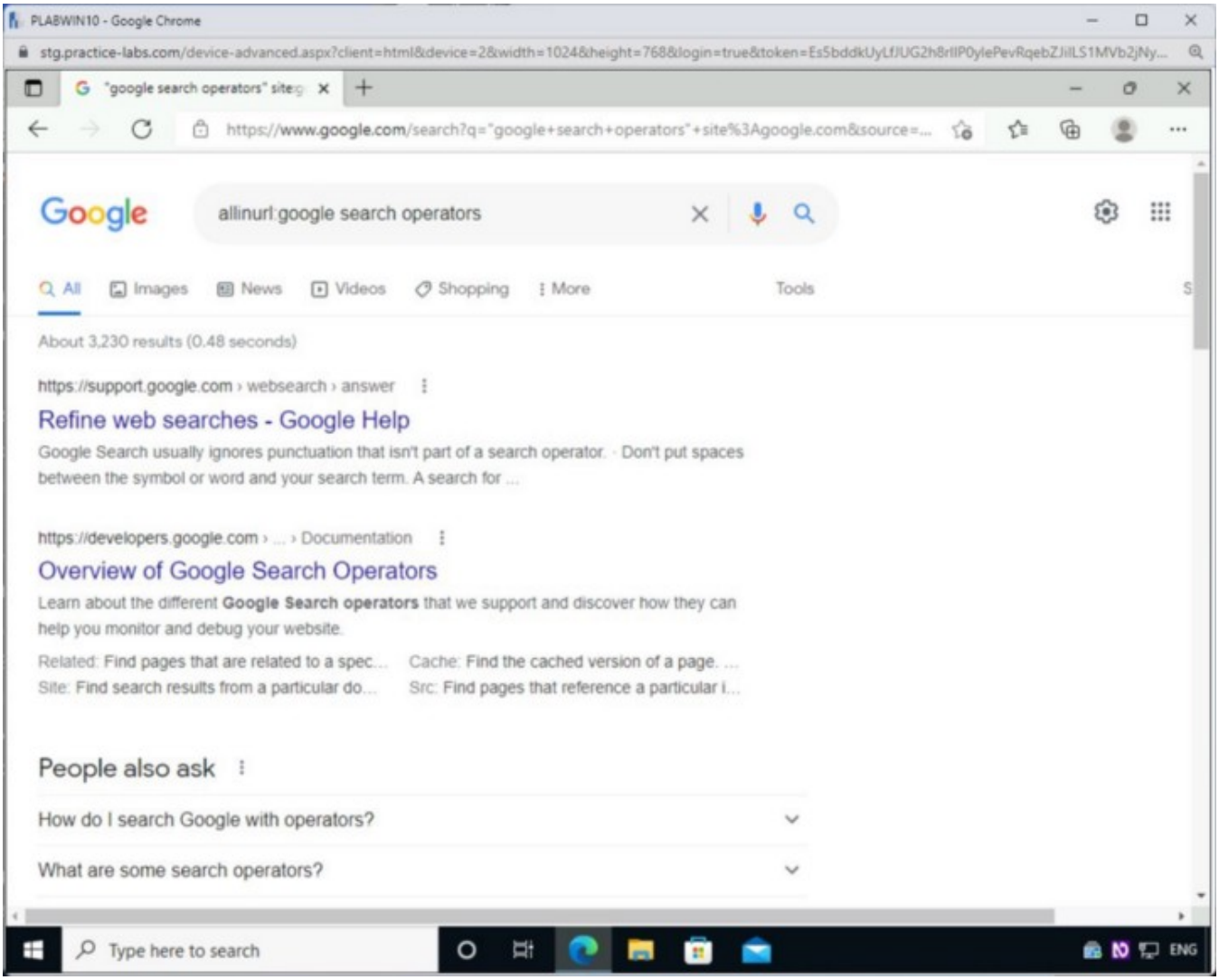
Step 7

You can also find specific words or a string of words in the URL. You need to use the allinurl keyword to do this, looking for the exact string of text you defined.

Let's say that you want to search for the "**google search operators**" string in the URL:

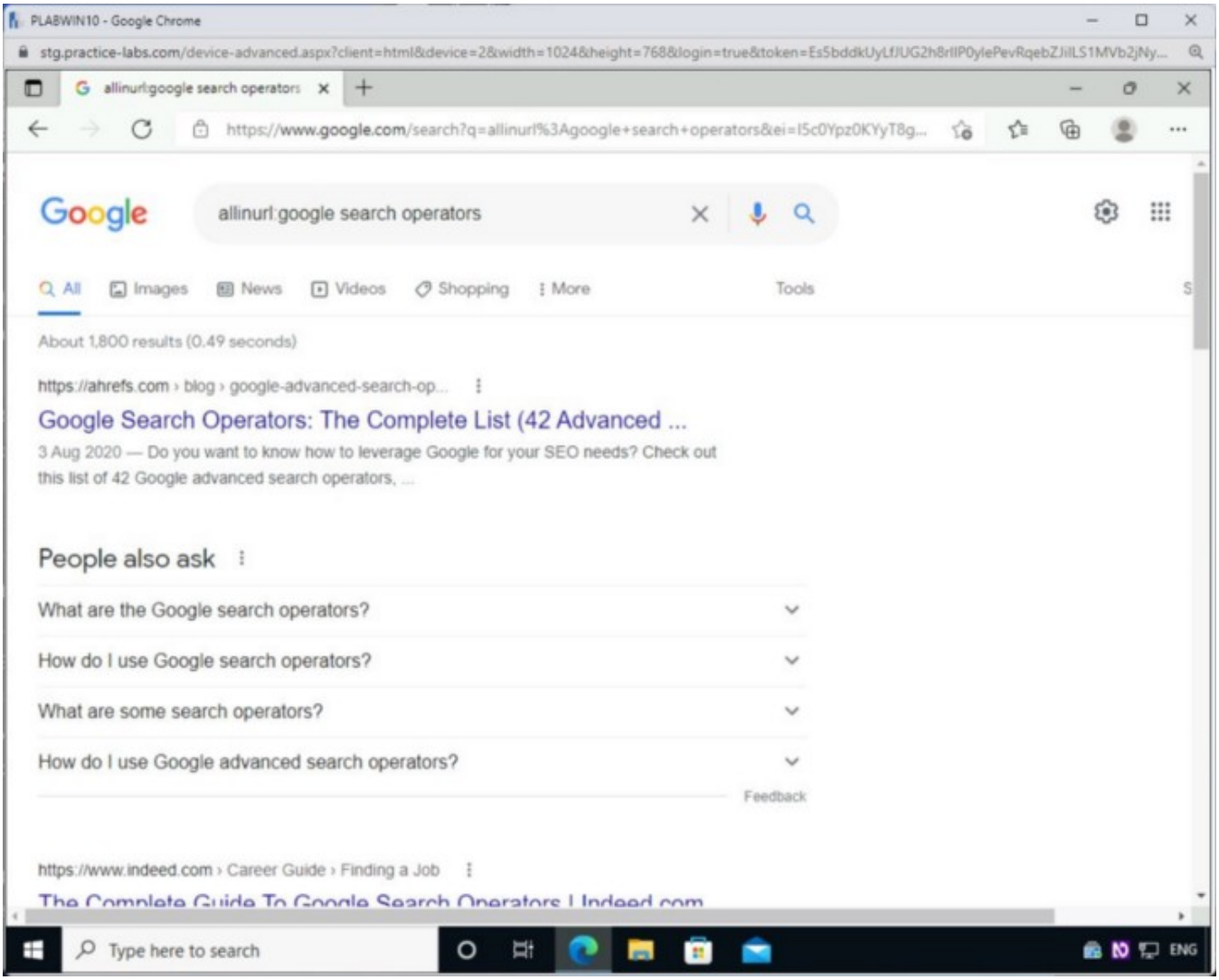
```
allinurl:google search operators
```

Press **Enter**.



Step 8

Notice that all the results have the exact text string you searched for.



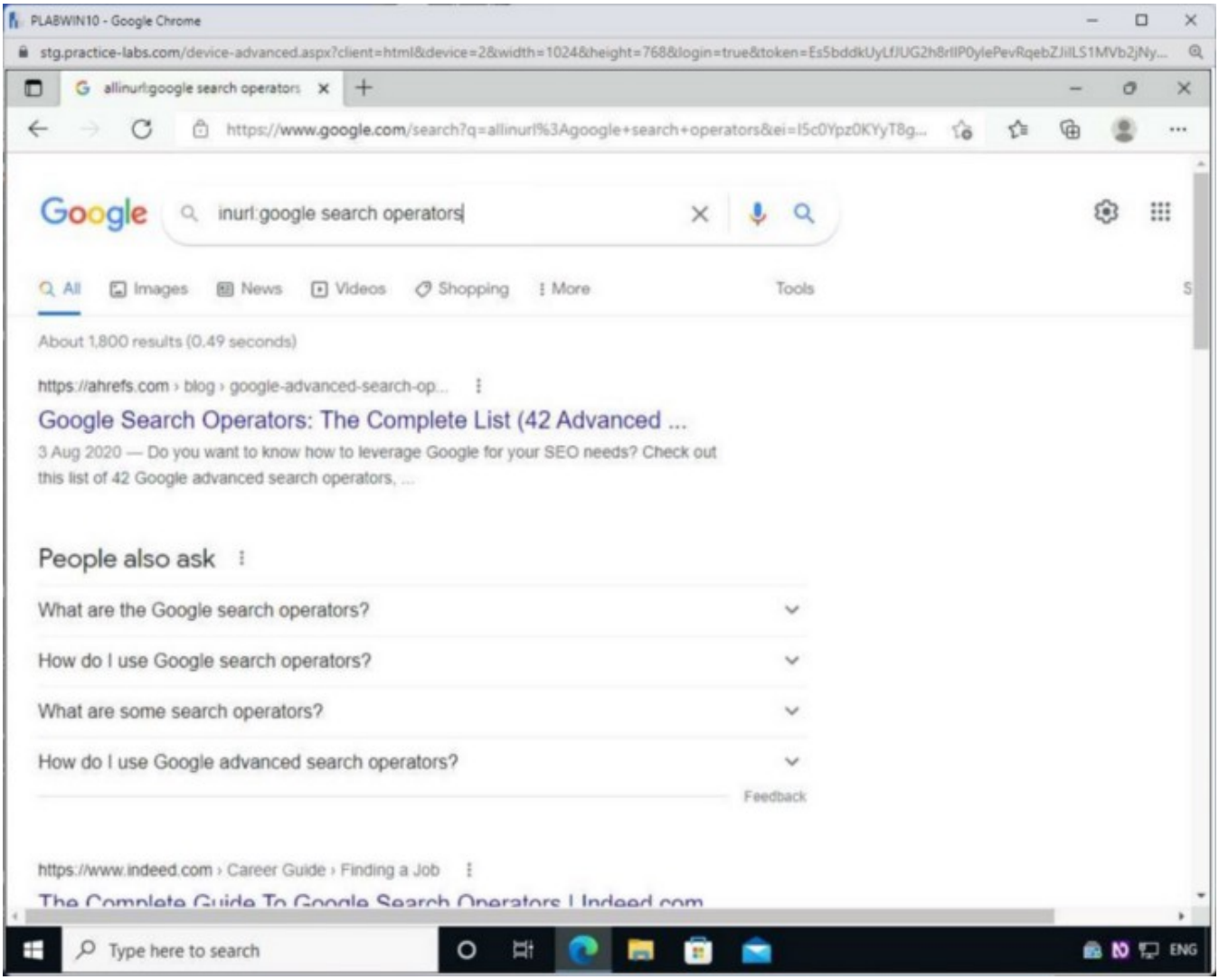
Step 9

Similar to **allinurl**, you have another keyword, **inurl**. Unlike **allinurl**, it will look for the words somewhere in the URL.

Type the following:

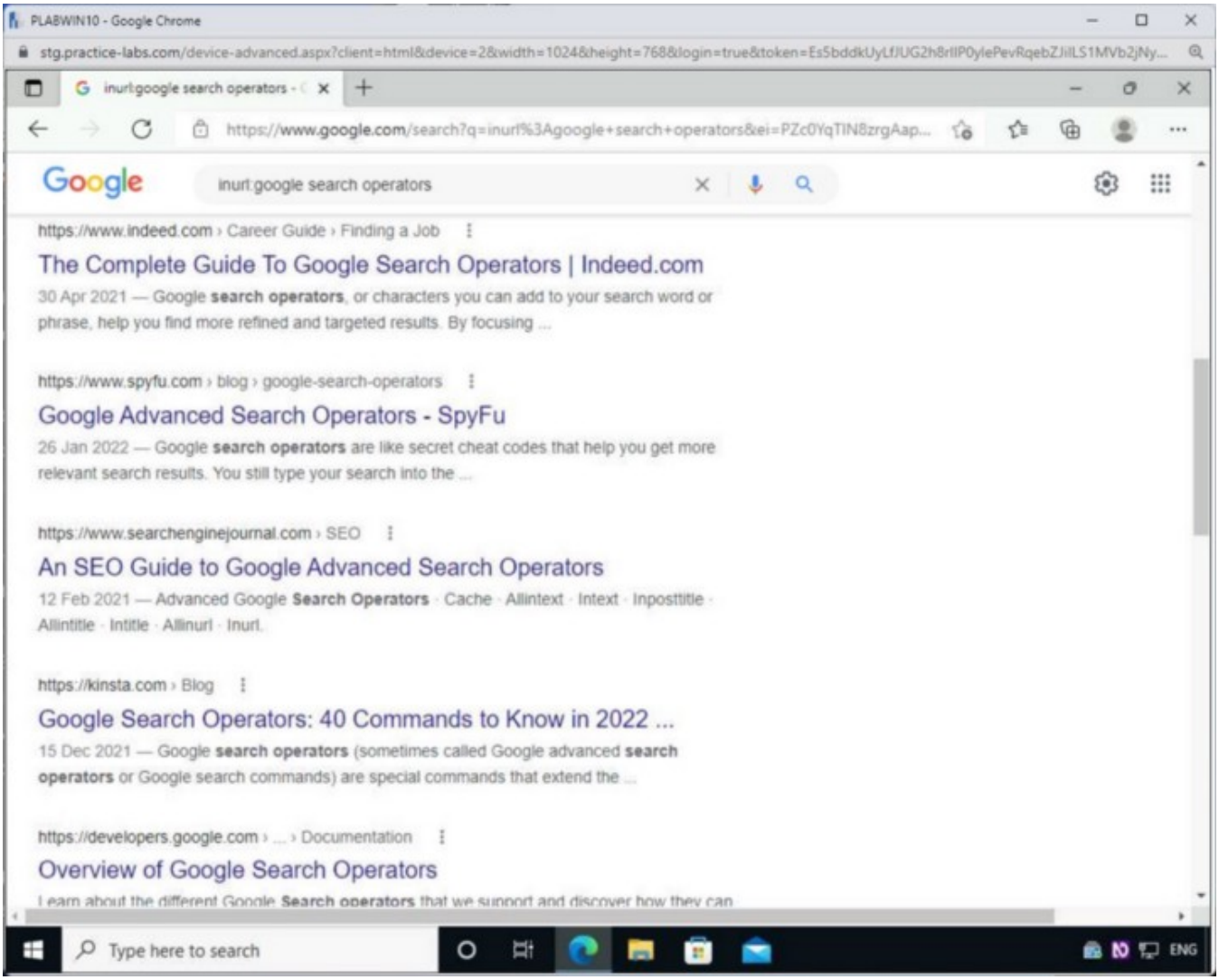
```
inurl:google search operators
```

Press **Enter**.



Step 10

The results are returned. However, when you scroll down, there are similar strings like **Advanced Google Search Operators** that are also located.

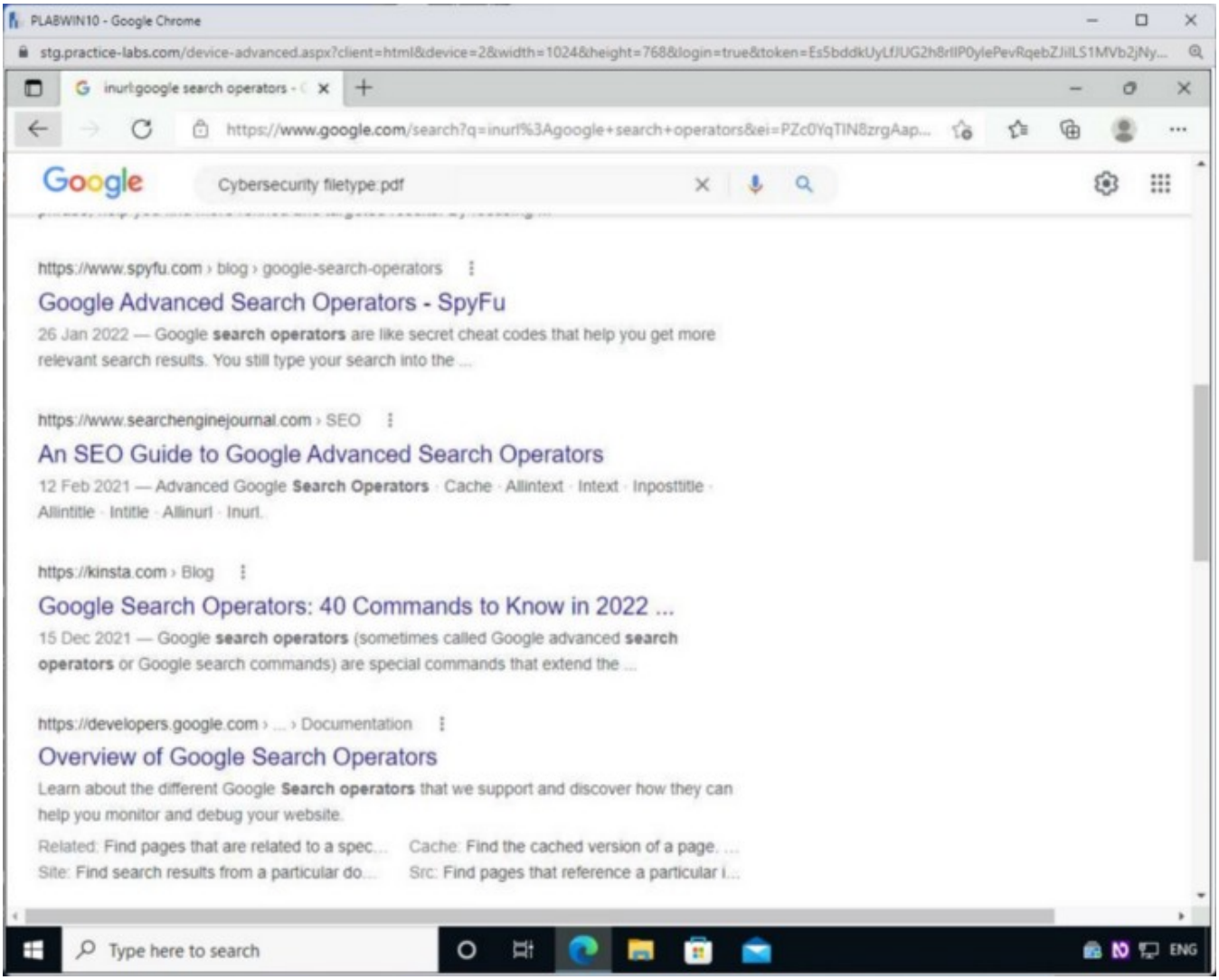


Step 11

You can also restrict the search to specific file types. For example, you can search for only **PDF** files.

```
Cybersecurity filetype:pdf
```

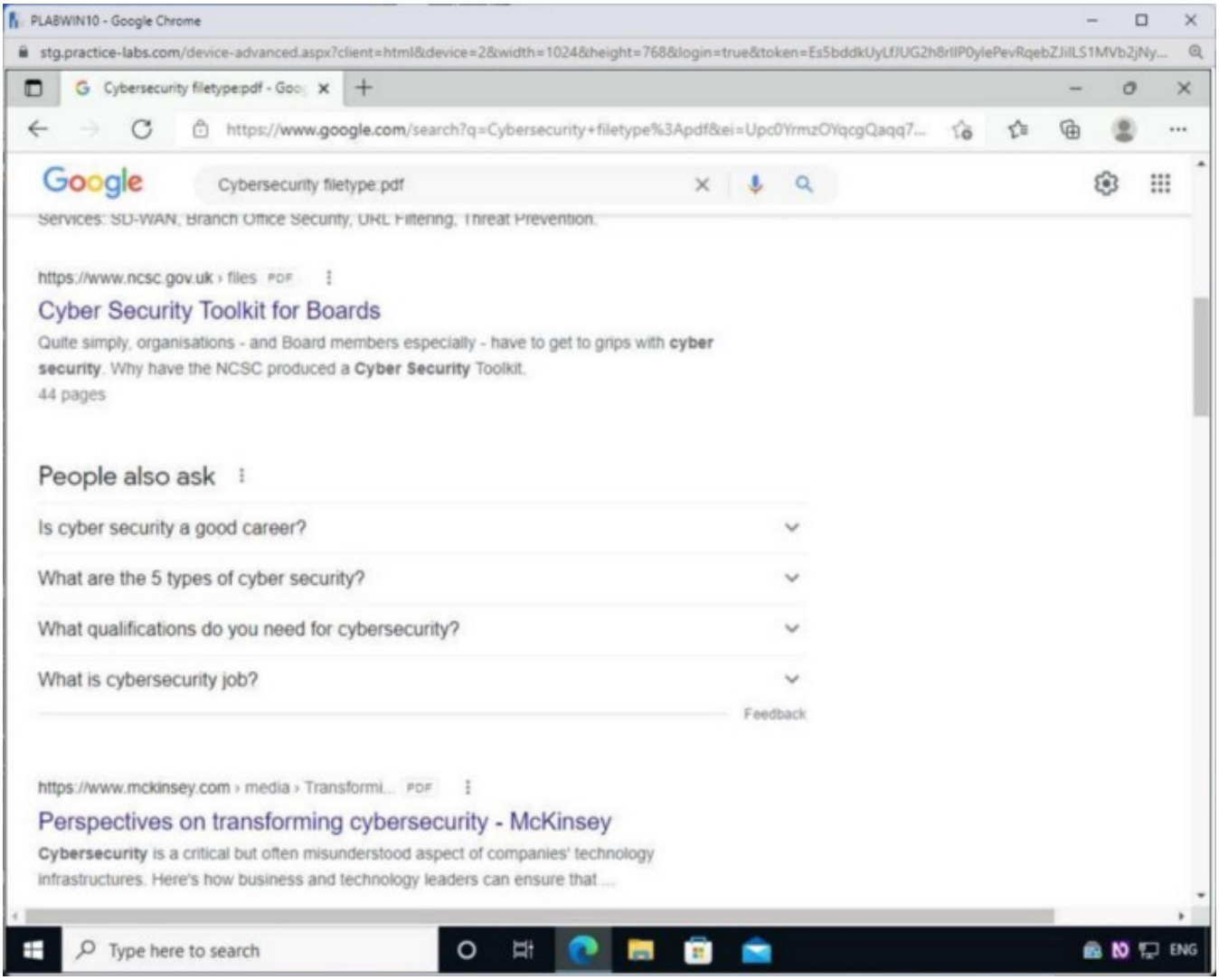
Press **Enter**.



Step 12

The search results display **PDF** files with the **Cybersecurity** word in their title.

***Note**: You may have to scroll past Google ads that appear at the top of the search.*

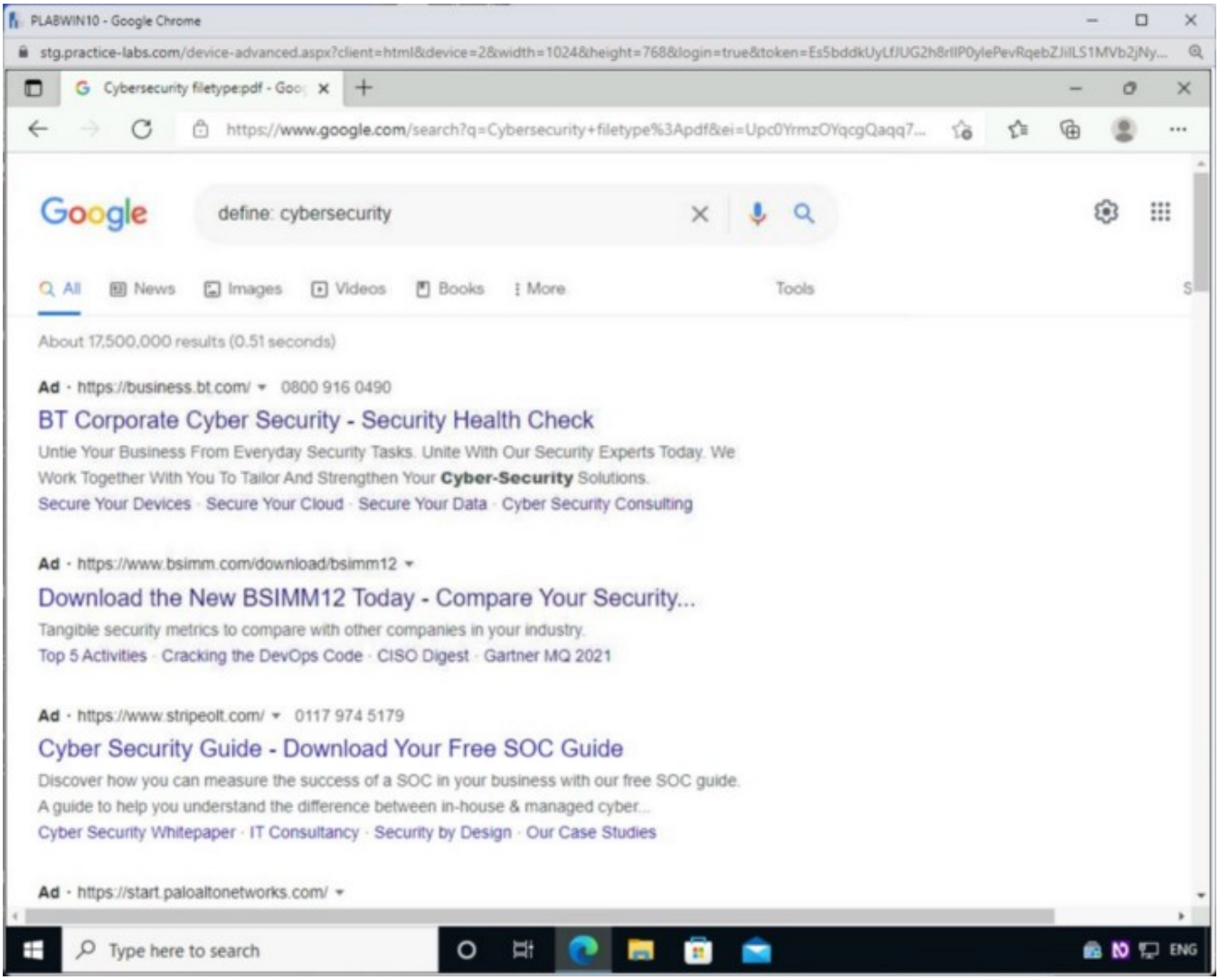


Step 13

You can also look for definitions using the define keyword. To do this, type the following command:

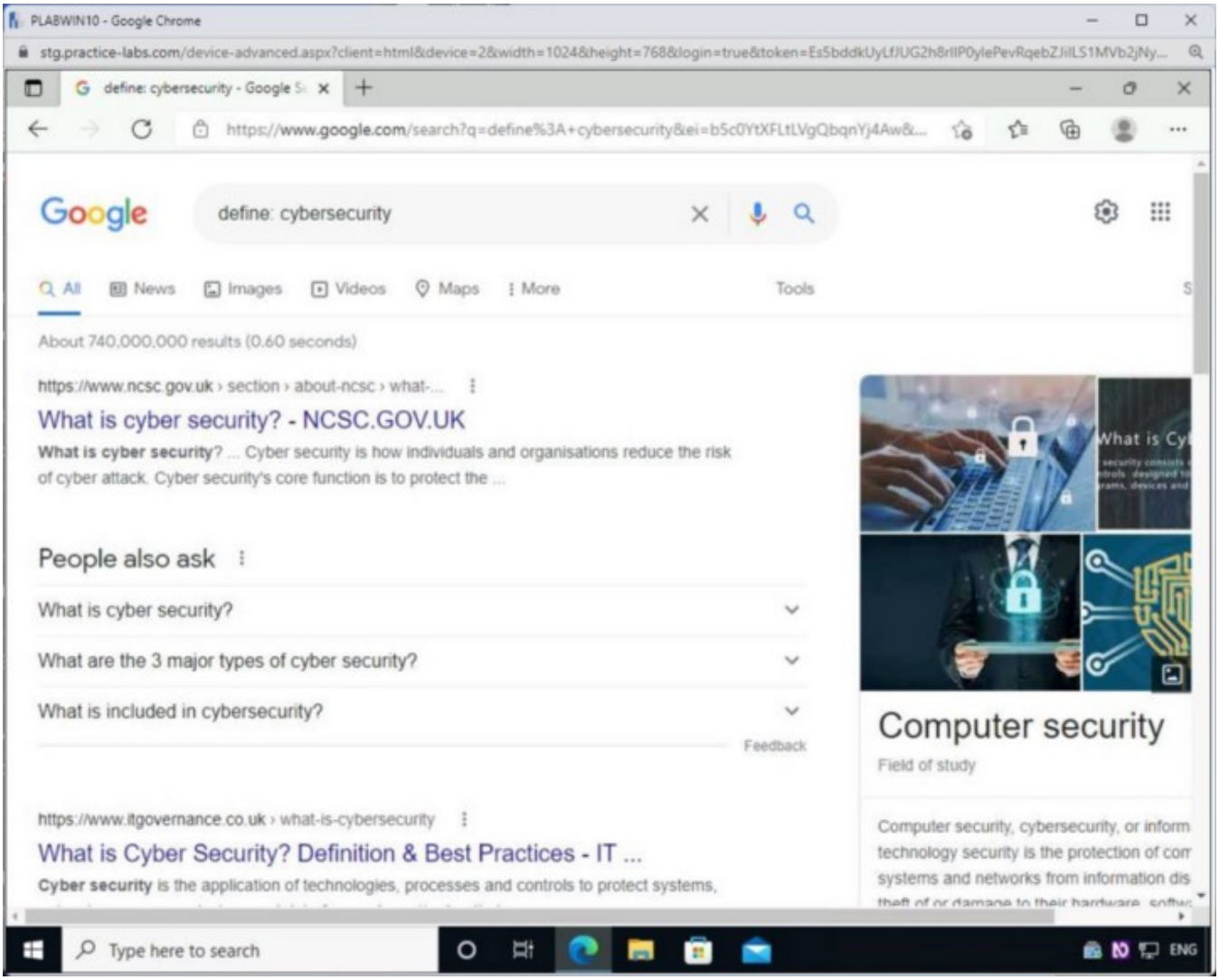
```
define:cybersecurity
```

Press **Enter**.



Step 14

The output displays the definition of **Cybersecurity**.



Exercise 3 — Footprinting Using Web Services

You can use various Web services to search for information about the target. For example, people's search services may provide many details about an individual target. Similarly, professional sites like LinkedIn can be a good resource to know about an organization. An attacker typically looks for various information, such as system and network information. Such information can be retrieved from a variety of sources, such as the company's website.

In this exercise, you will learn to footprint using Web services.

Learning Outcomes

After completing this exercise, you will be able to:

- Use Web Services for Footprinting

Your Devices

You will be using the following devices in this lab. Please power these on now.

PLABDC01Domain Controller192.168.0.1/24PLABWIN10Domain MemberWorkstation192.168.0.3/24PLABKALI01Domain MemberWorkstation192.168.0.5/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

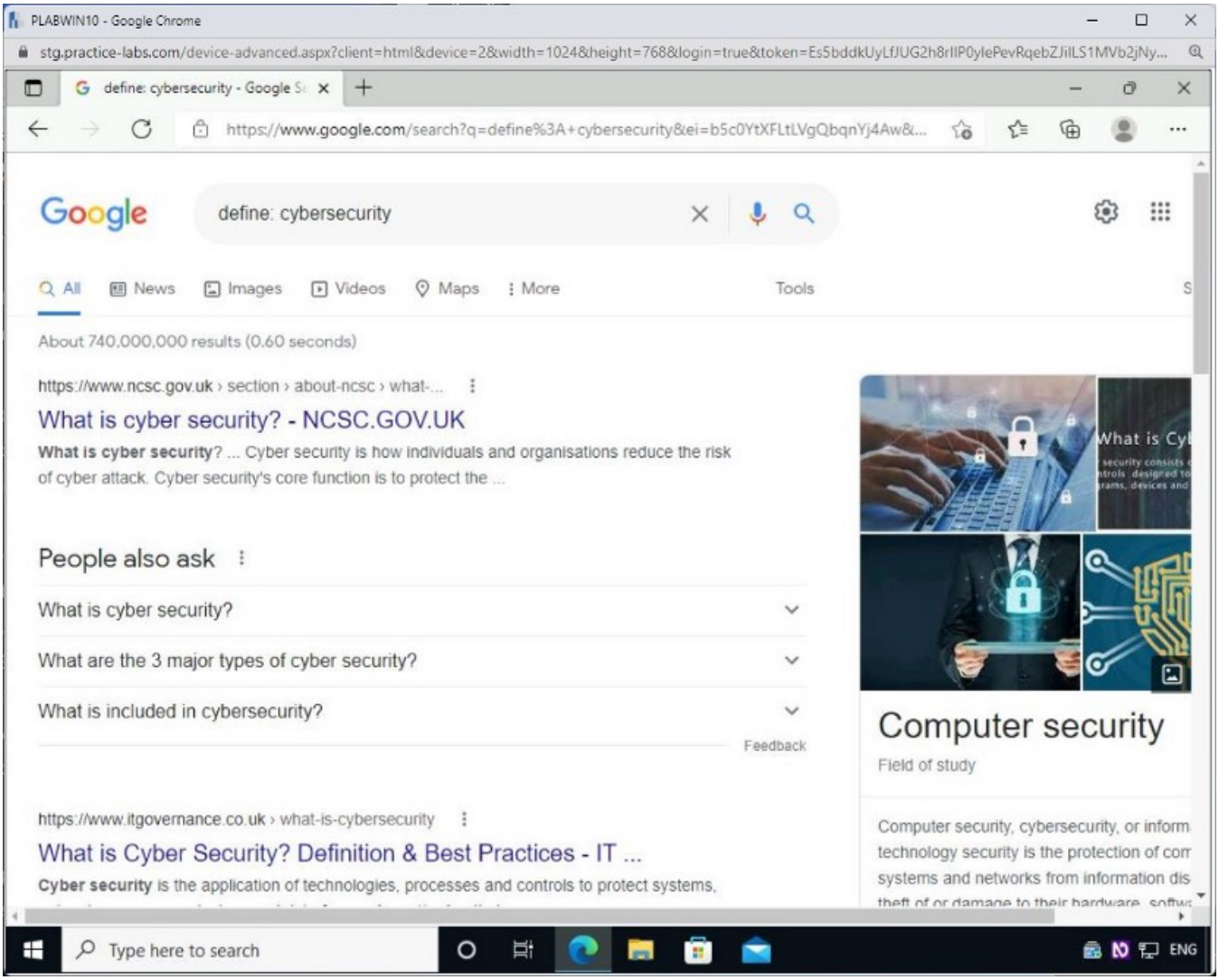
Task 1 — Use Web Services for Footprinting

Web services can be of different types. Search services are the most used web services for locating information about the targets or general by a normal user. An attacker can use various web services, such as job sites, social networking sites, or people search services to find the information required to set the base for an attack. Once an attacker captures the information, they can set the tone of the attack — the type of attack they need to conduct.

In this task, you will learn to get information about the domains and subdomains.

Step 1

Connect to **PLABWIN10**. The **Edge** web browser should be open.

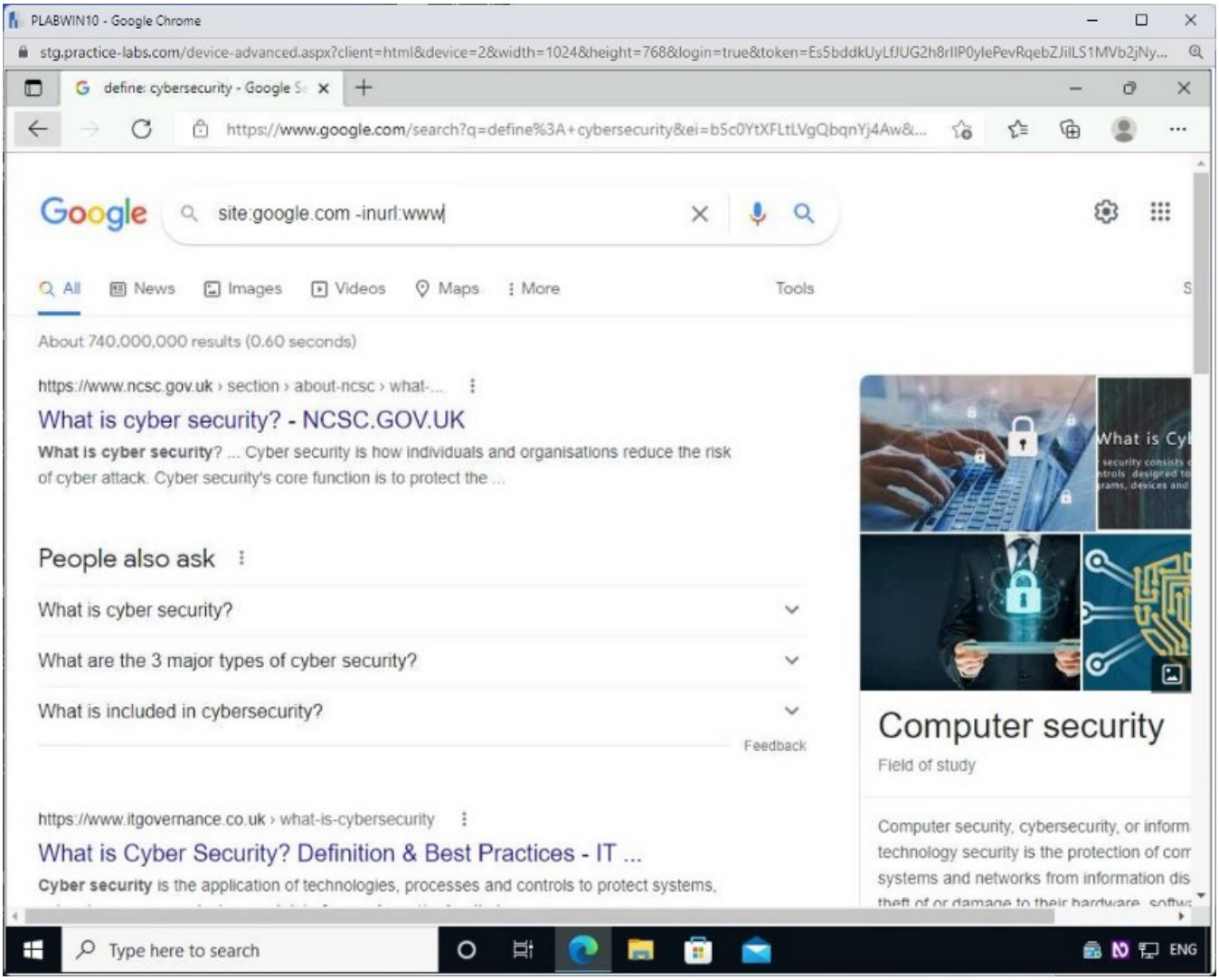


Step 2

To find the information about the domains of a company, you can use a search engine like **Google**. For example, you want to find out all the subdomains of **Google**. Then you need to use the following command:

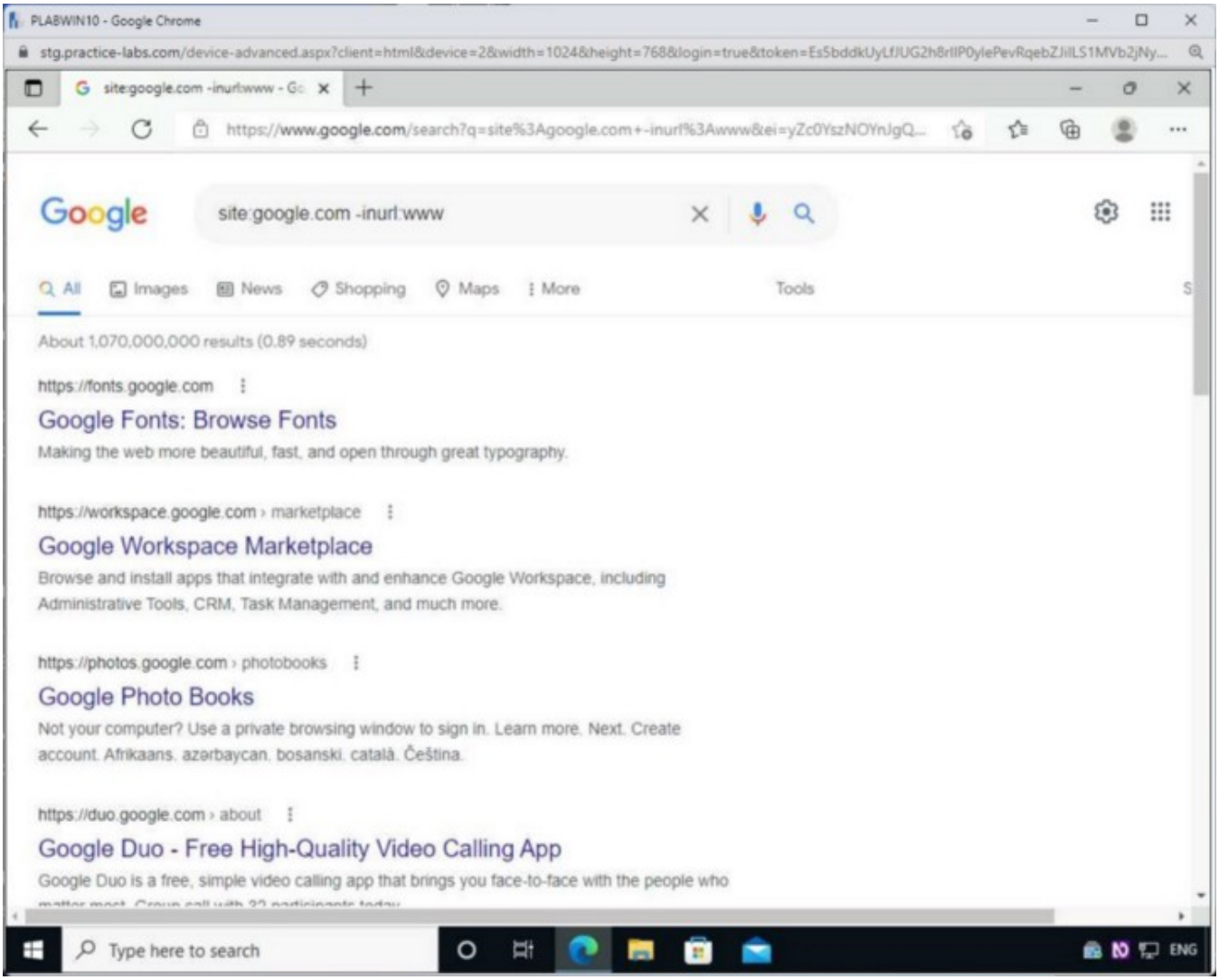
```
site:google.com -inurl:www
```

In the previous task, you learned about the inurl keyword. Here, you put a — (minus) sign before inurl, which means it will search for all words but **www** in the URL.
Press **Enter**.



Step 3

The result displays several URLs with the subdomains like **font.google.com** and **workspace.google.com**. However, because you omitted the **www** search, it does not feature the results.



Step 4

Connect to **PLABKALI01**.

Log in using the following credentials:

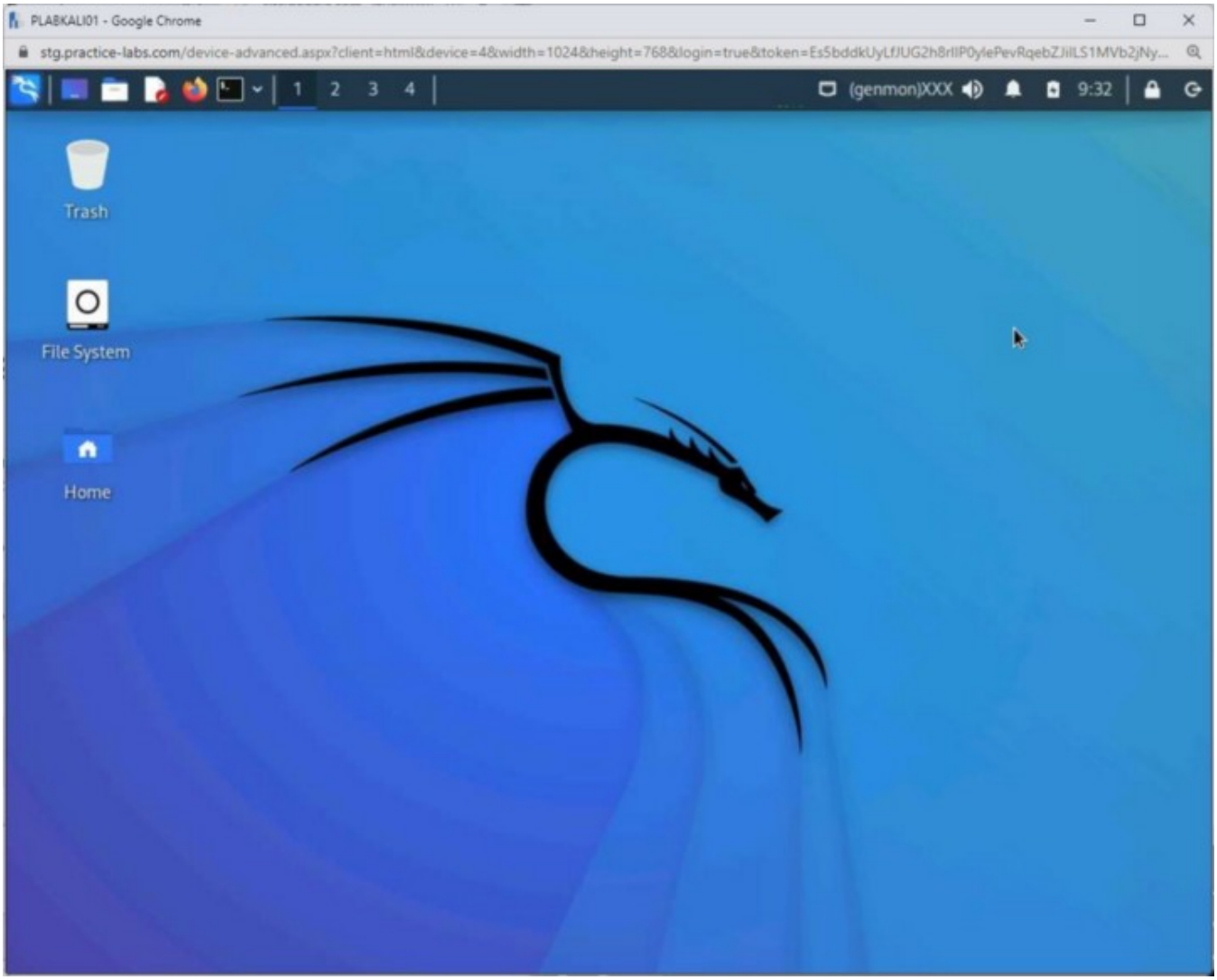
Username:

```
root
```

Password:

Password

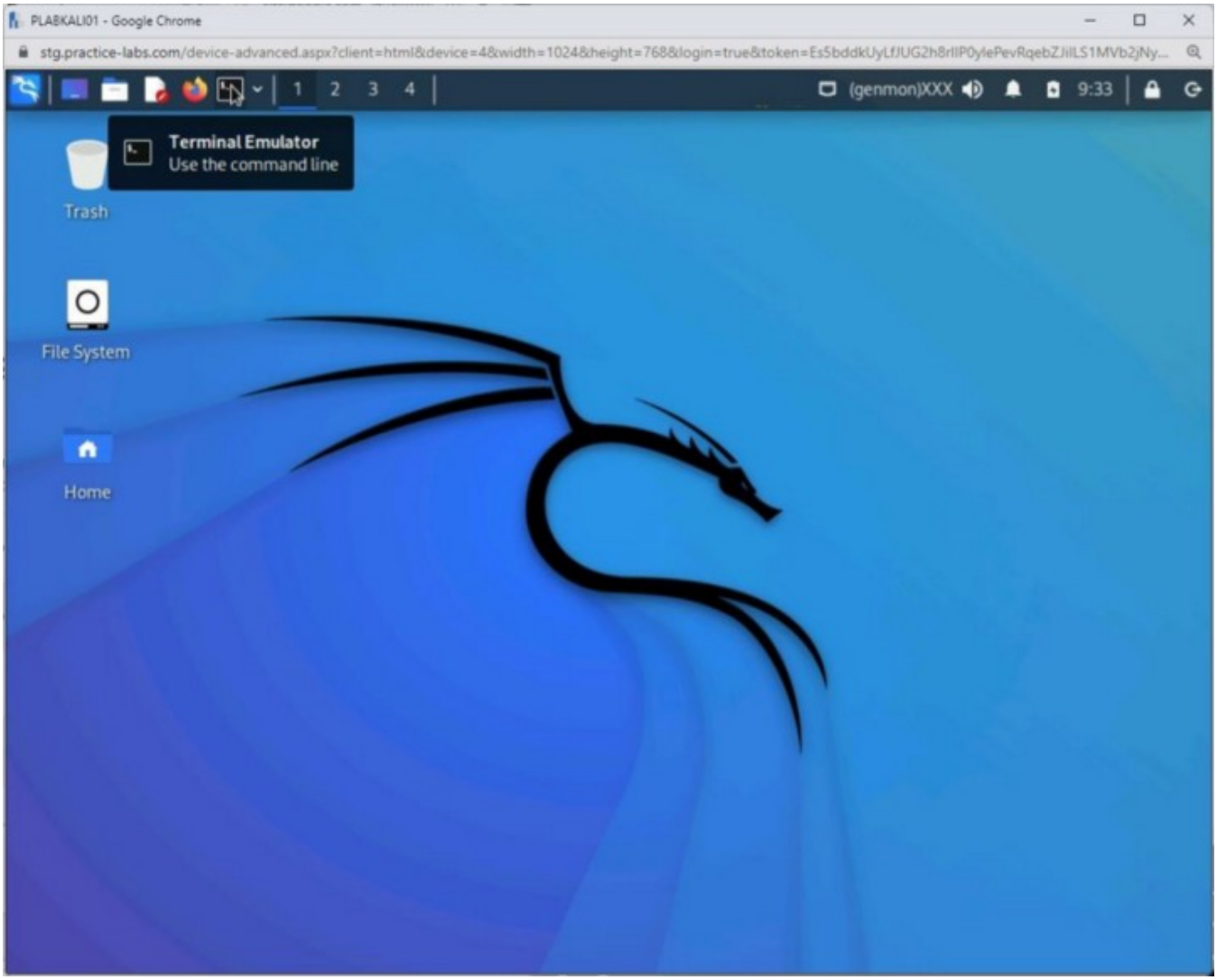
The desktop of **PLABKALI01** is displayed.



Step 5

You can use a tool named **Sublist3r** to enumerate the subdomains for google.com.

To do this, first open the terminal by clicking the **Terminal Emulator** icon on the taskbar at the top of the page.

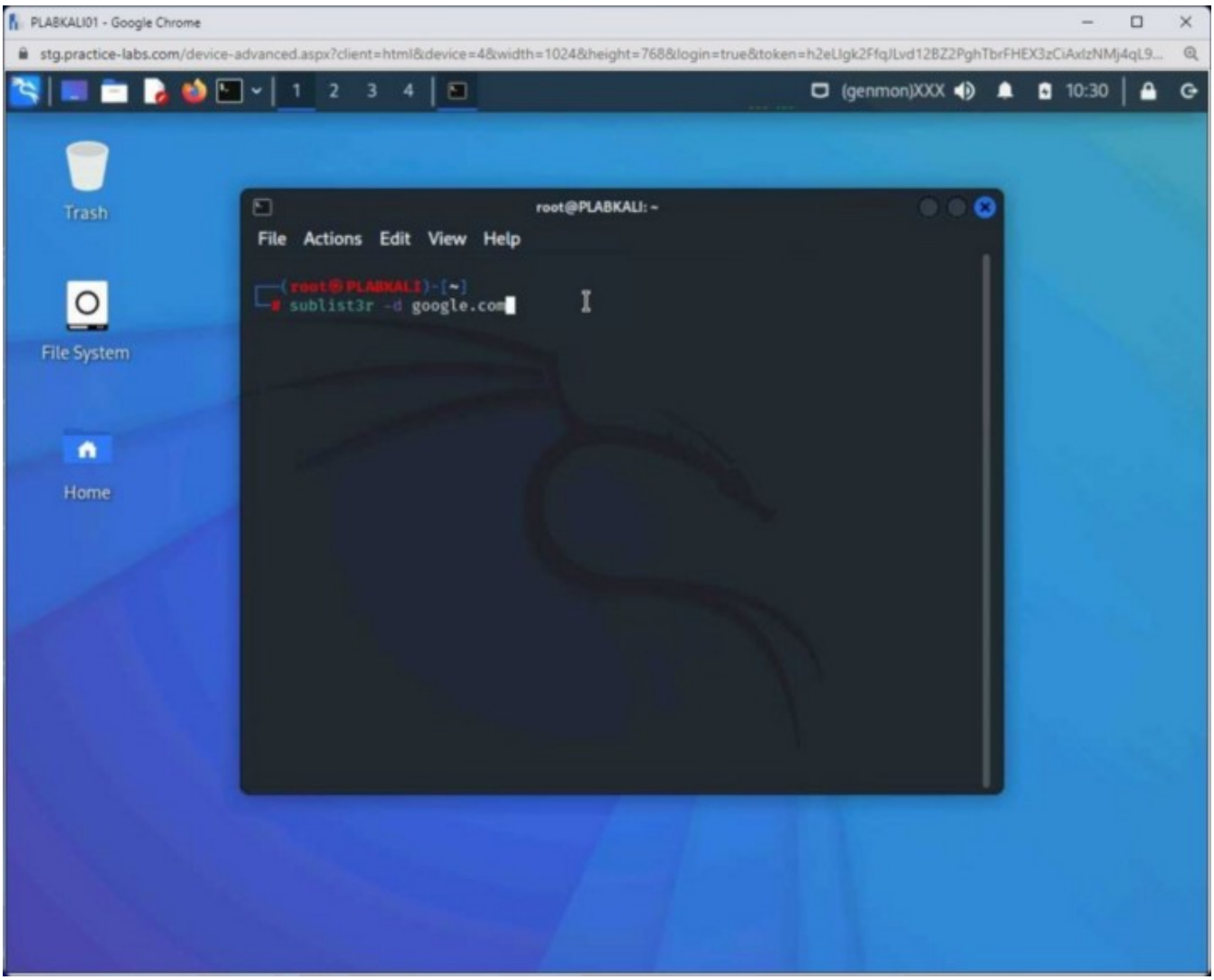


Step 6

Now, you are in the **Sublist3r** directory. Let's now enumerate the subdomains for **google.com**. To do this, type the following command:

```
sublist3r -d google.com
```

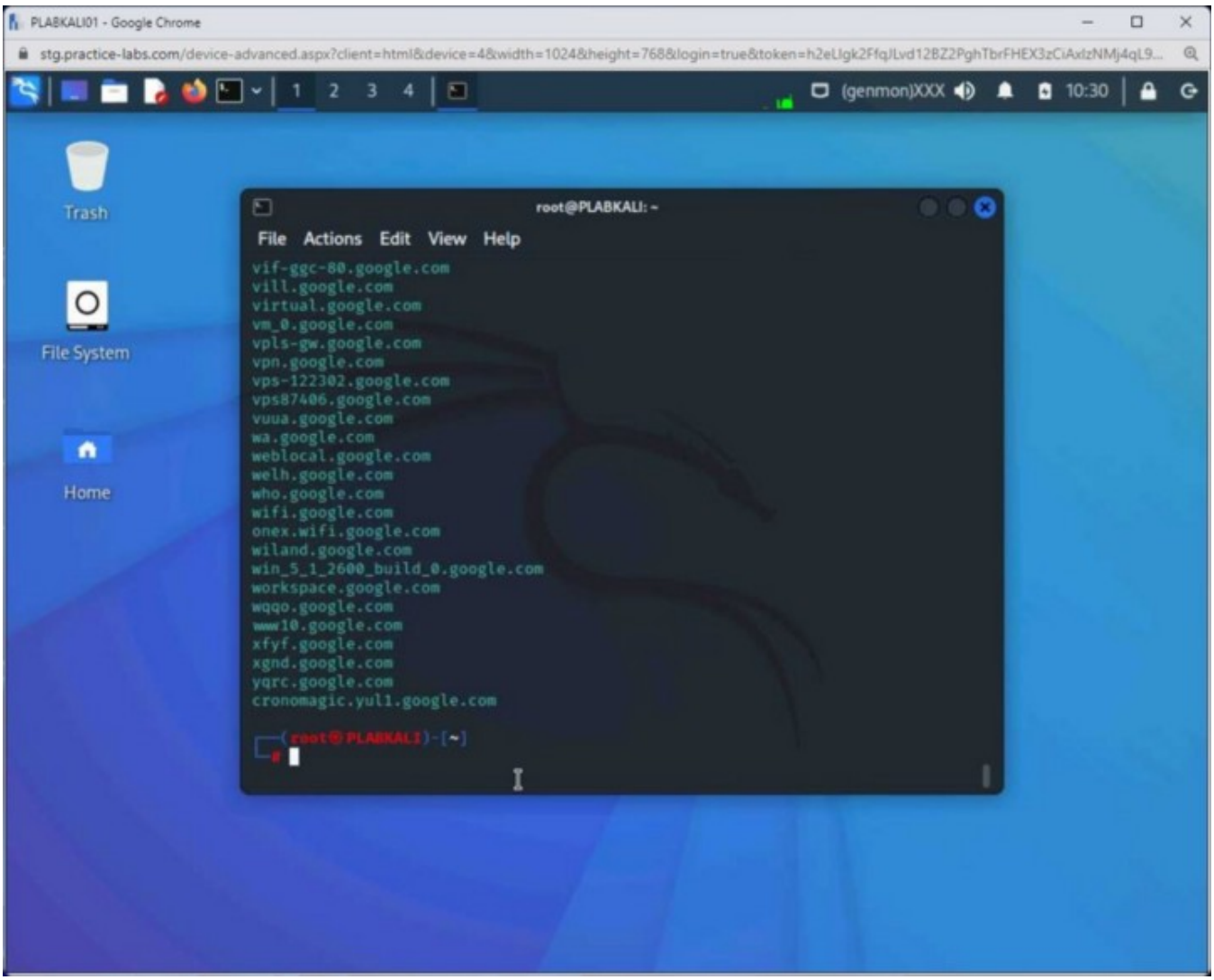
Press **Enter**. The **-d** parameter is used to define the domain name.



Step 7

The **sublist3r** tool scan through various search engines as you had not specified a specific search engine.

Post scanning, the search engines lists hundreds of enumerated subdomains for **google.com**.



Exercise 4 — Footprinting through Social Networking Sites

Social media websites hold both personal and organizational information. Organizations create their profiles to promote and market their products and services. At the same time, the employees of these organizations use social media websites for their profiles.

Organizations and people use several popular social media websites, such as:

- **Twitter:** Mostly used for promotional and information sharing by individuals and organizations.
- **Facebook:** Used for marketing, product promotions, and information sharing by individuals who can share images, videos, and advertisements.
- **LinkedIn:** LinkedIn is one of the prominent social media websites used for professional purposes, such as networking and hiring purposes. Organizations use LinkedIn for promoting their products and services.

- **Instagram:** It is used for picture sharing by individuals and organizations. While individuals can share personal pictures of their vacation, etc., the organizations can promote their brand, product, or service.

Organizations and individuals create their profiles with their information, email address, and phone numbers. Such information can be useful to an attacker.

In this exercise, you will learn to get information about targets from public sources on the Internet.

Learning Outcomes

After completing this exercise, you will be able to:

- Footprint using Opencorporates

Your Devices

You will be using the following devices in this lab. Please power these on now.

PLABDC01Domain Controller192.168.0.1/24PLABKALI01Domain MemberWorkstation192.168.0.5/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2019.2 — Linux Kali Workstation192.168.0.5/24

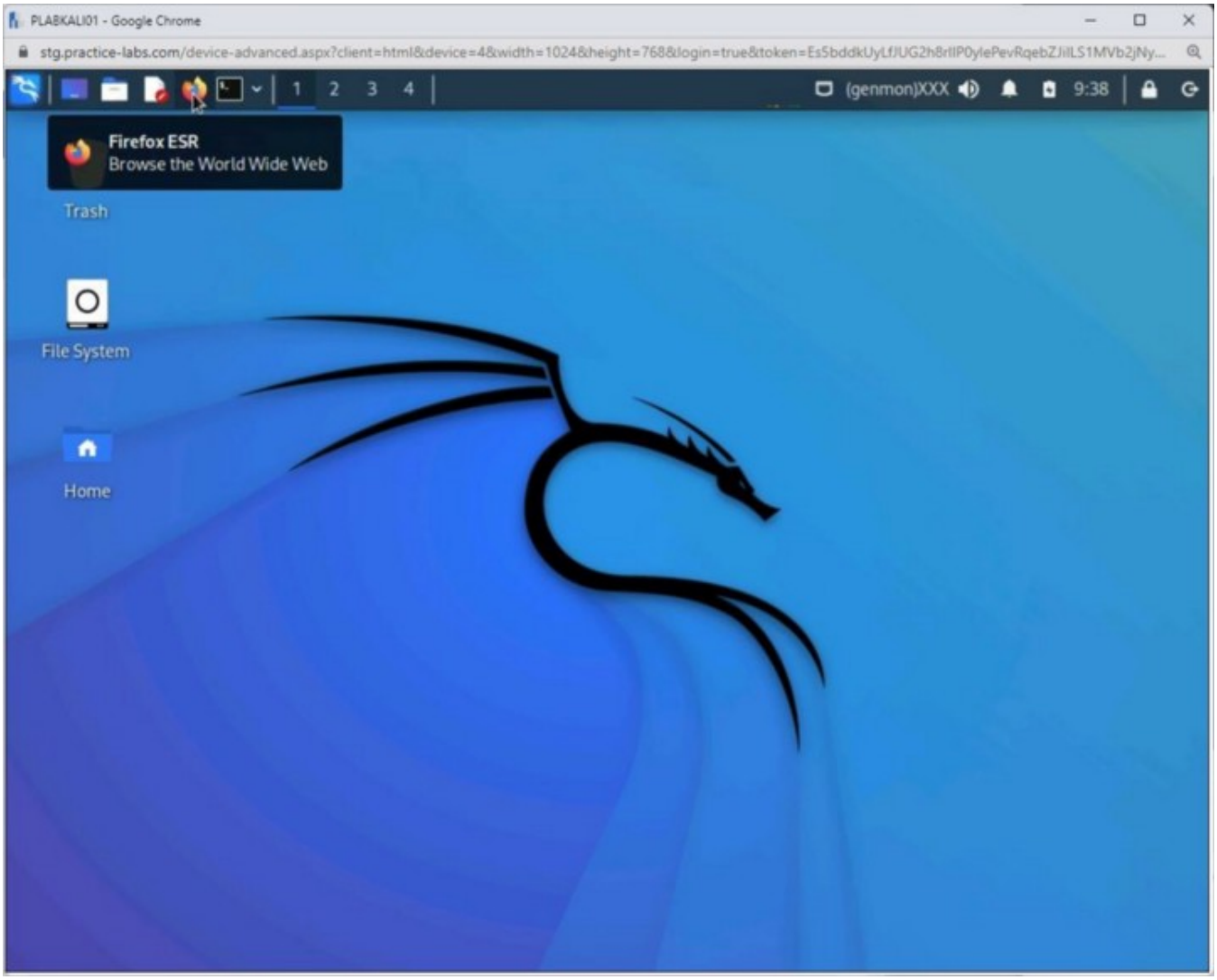
Task 1 — Footprint using Opencorporates

You can use web services such as opencorporates.com to get more information about a target company. You can get information, such as an address, contact number, service industry, and provided services.

This is only one example of several different tools you can use, such as Mention.com or Hunter.io, depending on what sort of information you are trying to footprint.

Step 1

Connect to **PLABKALI01** and open **Firefox ESR** by clicking the icon on the taskbar.

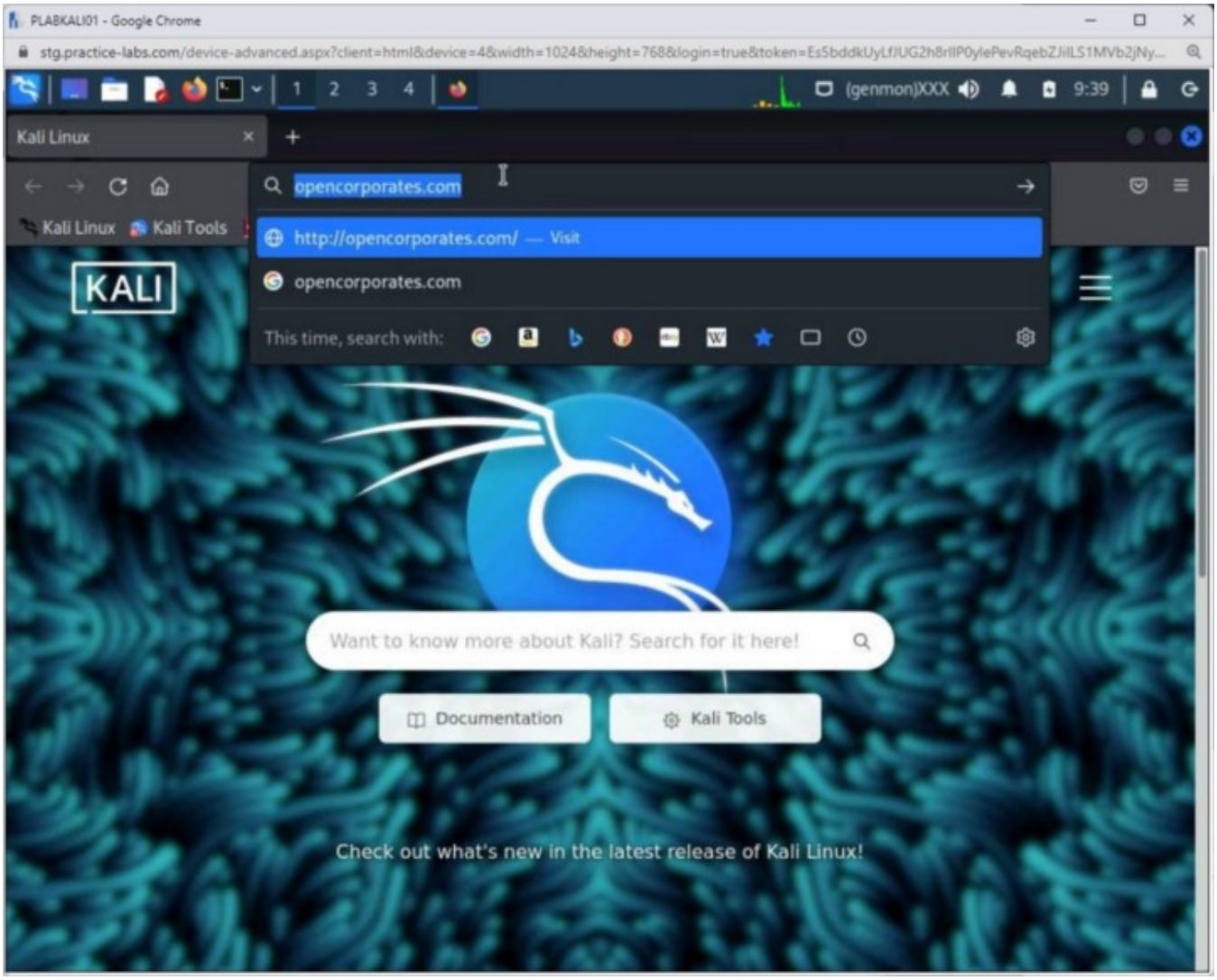


Step 2

In the Web browser window, type the following address:

```
opencorporates.com
```

Press **Enter**.

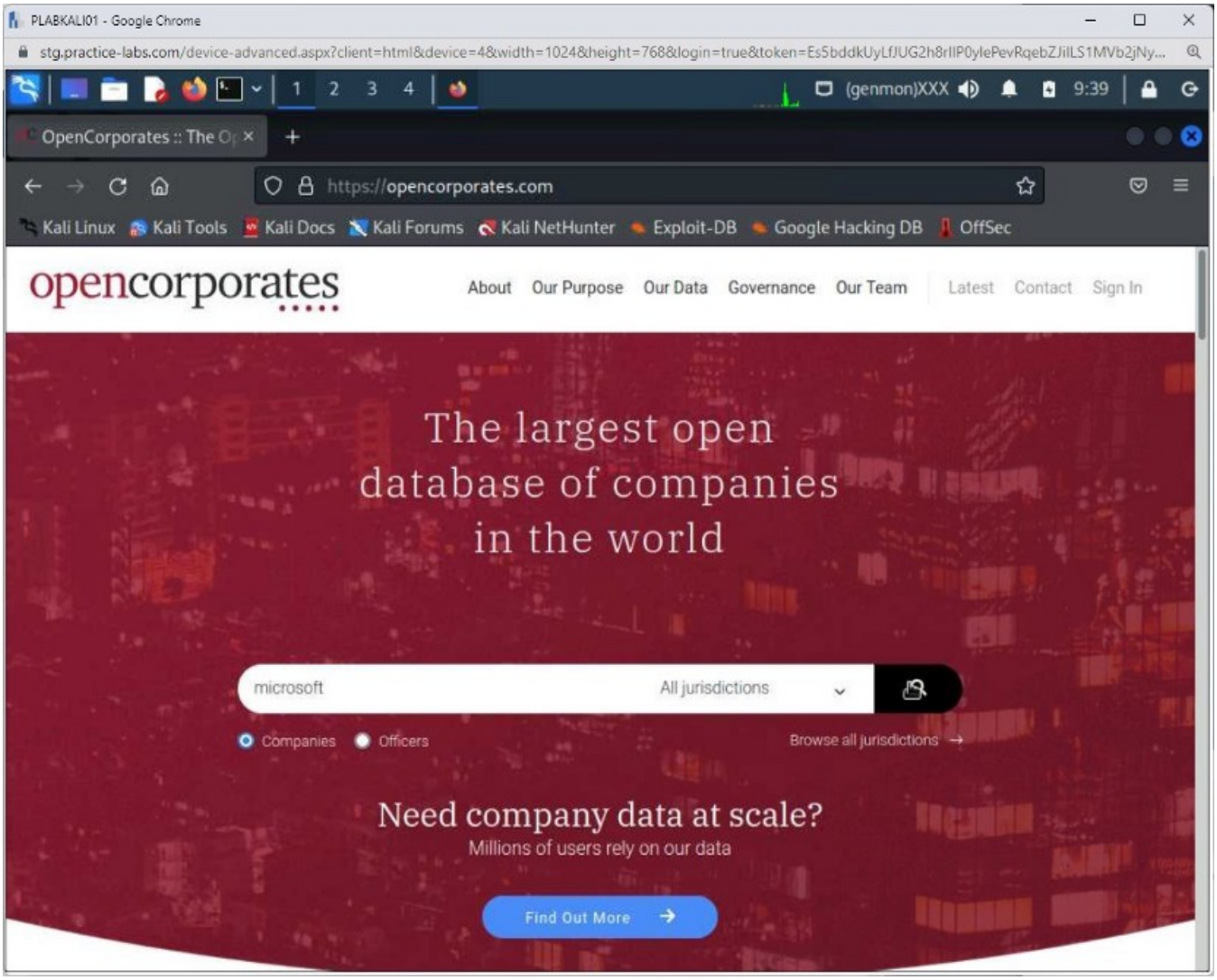


Step 3

In the search text box, type the following:

```
microsoft
```

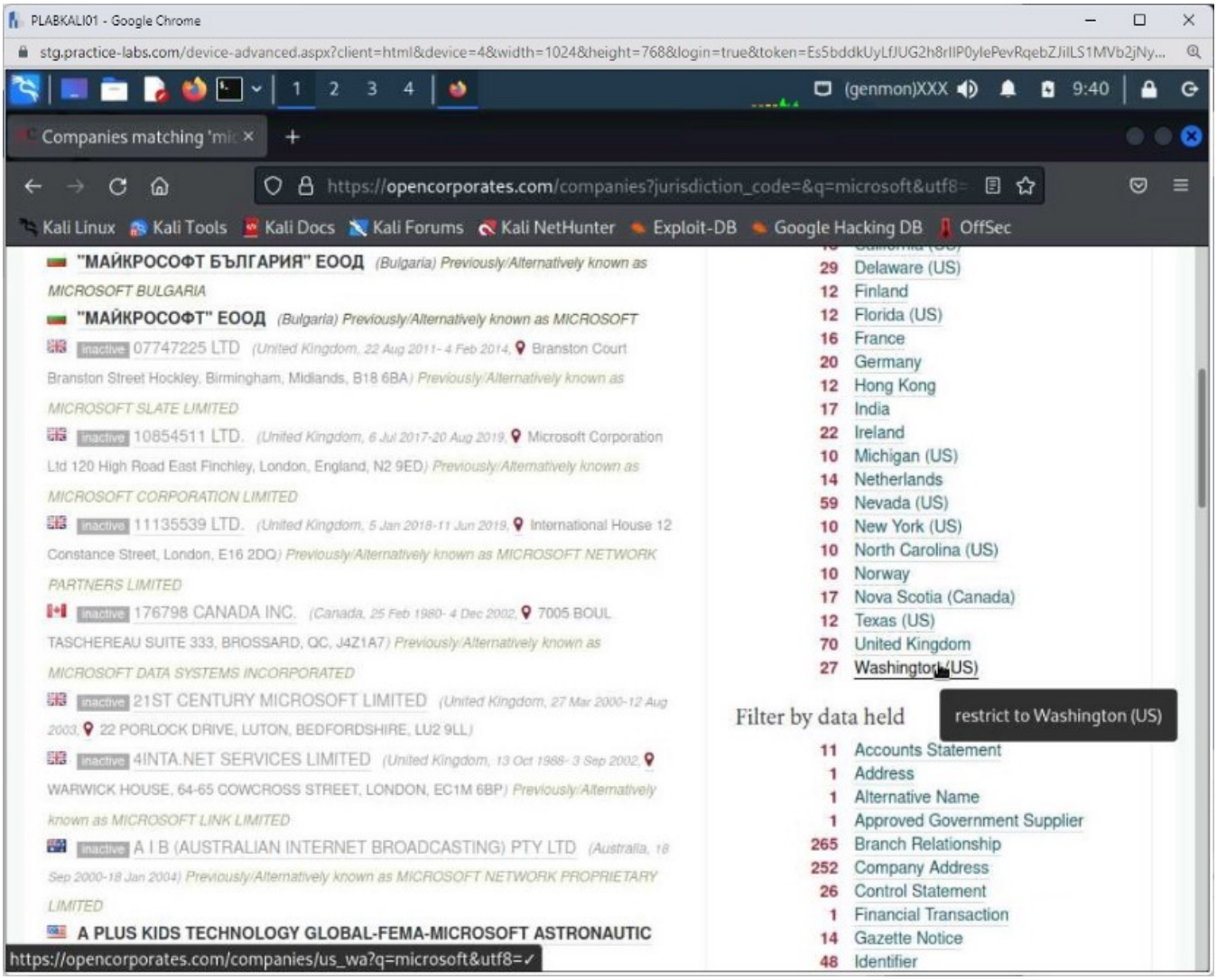
Click the **Search** icon.



Step 4

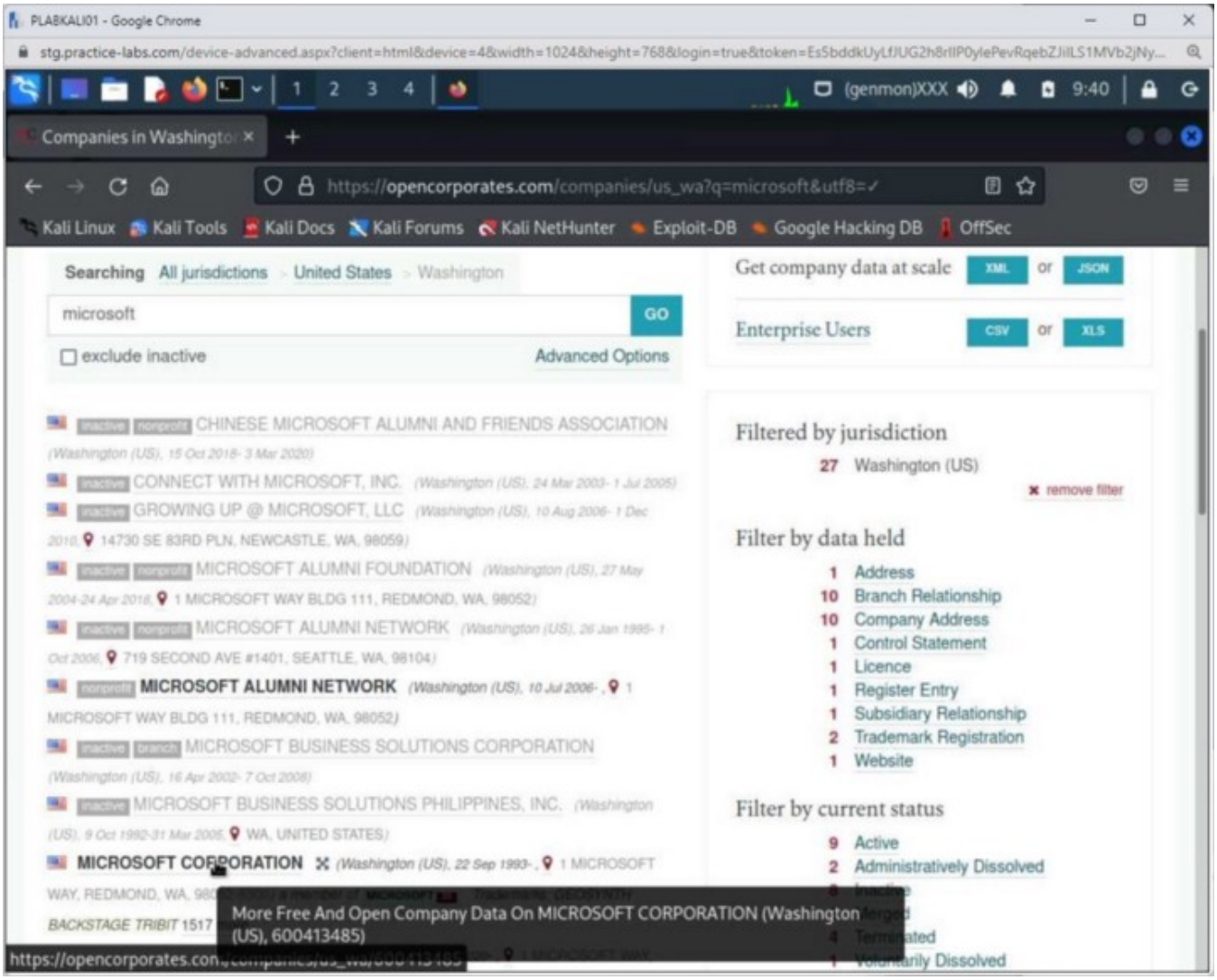
The results display the **Microsoft** companies throughout the world.

In the right pane, scroll down and select **Washington (US)**.



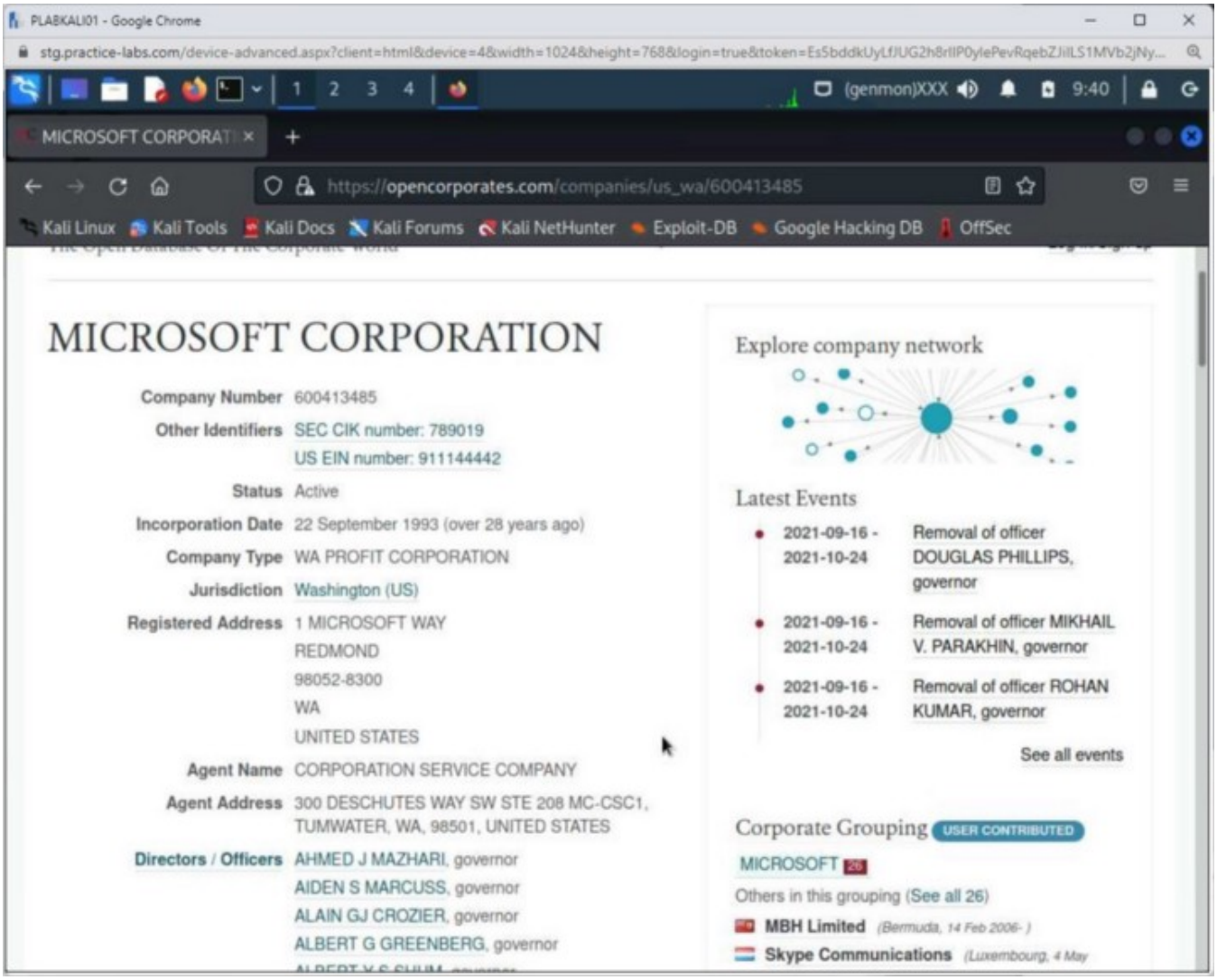
Step 5

The results are updated in the left pane. Scroll down and select **MICROSOFT CORPORATION**.



Step 6

The left pane displays the information about **Microsoft**. You can scroll down to read more information.



Exercise 5 — Website Footprinting

Organizations put a lot of information on their websites. You can find office addresses, senior management information, and contact numbers. An attacker can use various methods to footprint a website.

For example, an attacker may simply mirror a website and analyze it offline to understand the website's map and architecture.

An attacker can gather a lot of information, such as:

- Software and their versions
- Operating systems and their versions
- Webserver directory structure
- Technologies and programming or scripting languages used

This task will teach you about website Footprinting using various tools and methods.

Learning Outcomes

After completing this exercise, you will be able to:

- Footprint using source code
- Footprint Using Archive.org
- Create a Wordlist Using CeWL
- Perform Banner Grabbing using Nmap

Your Devices

You will be using the following devices in this lab. Please power these on now.

PLABDC01Domain Controller192.168.0.1/24PLABKALI01Domain MemberWorkstation192.168.0.5/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2019.2 — Linux Kali Workstation192.168.0.5/24

Task 1 — Footprint Using Source Code

A website source can help an attacker determine quite a lot of information. For example, with the source code, an attacker can determine if any directories are used in the file paths or any hidden files used. An attacker can analyze the functions in the source code to determine weaknesses.

In this task, you will learn about website Footprinting by accessing source code.

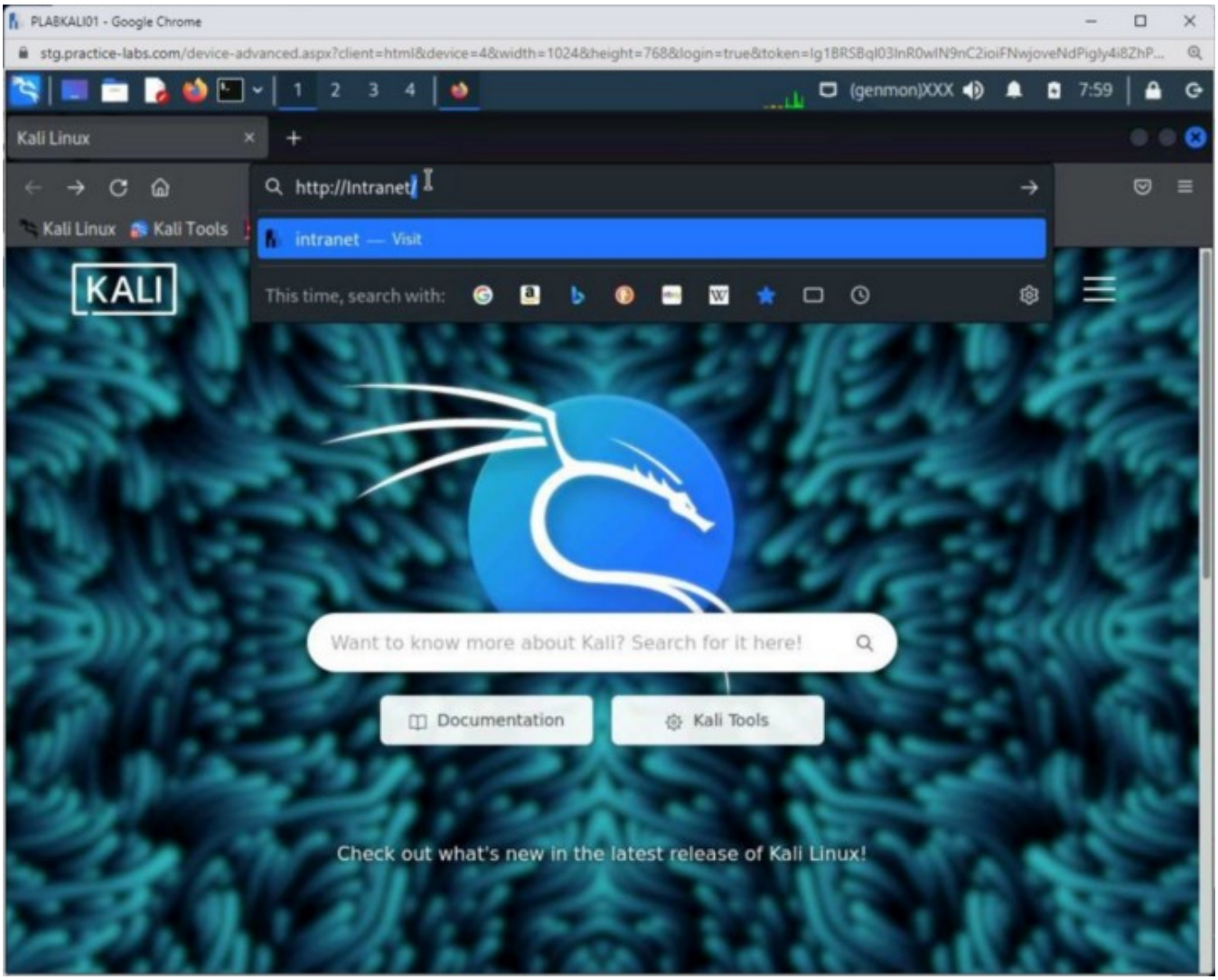
Step 1

Ensure that you are connected to **PLABKALI01** and open **Firefox ESR** by clicking on the icon on the taskbar.

The Kali homepage is displayed as the default home page. In the address bar, type the following:

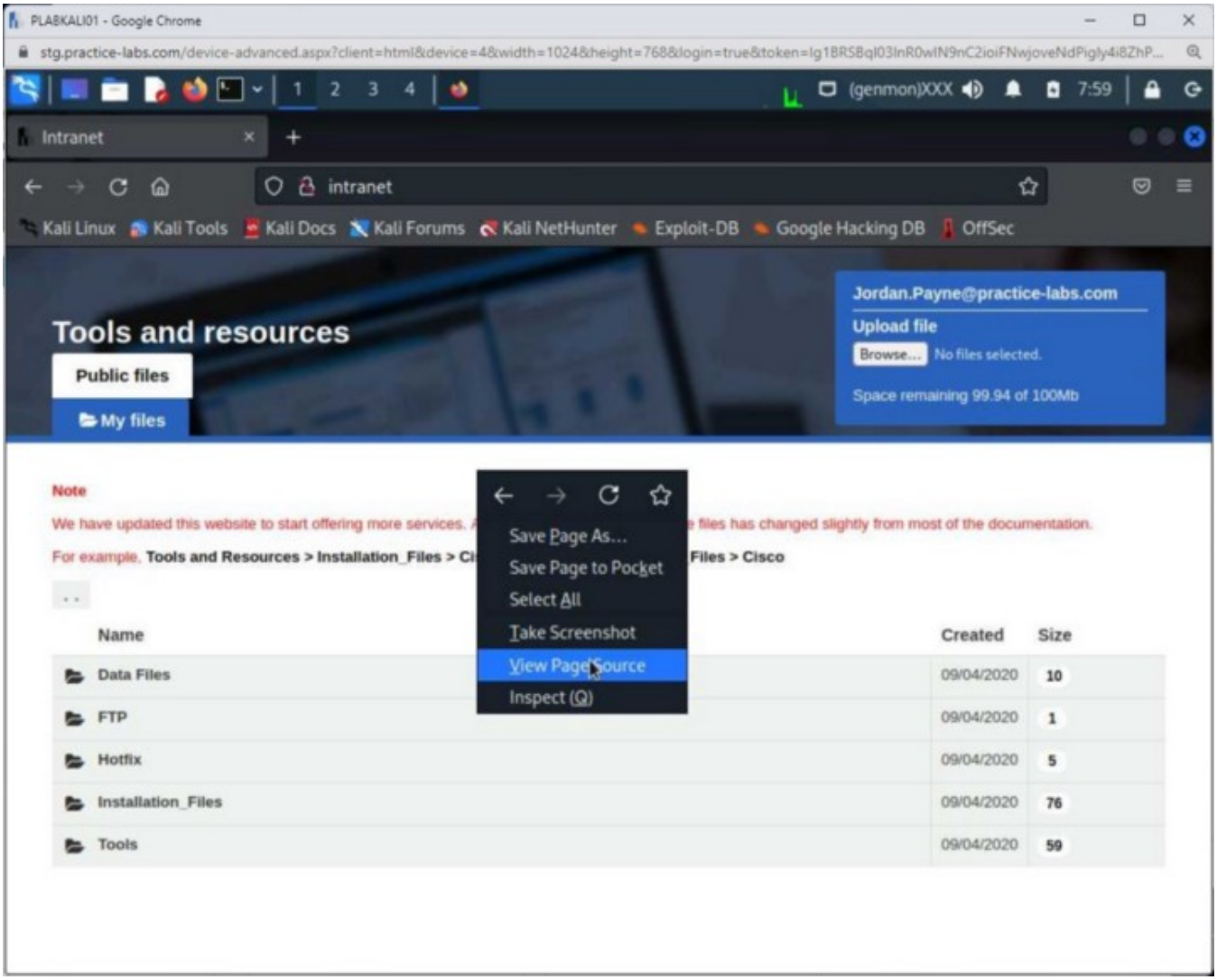
```
http://intranet
```

Press **Enter**.



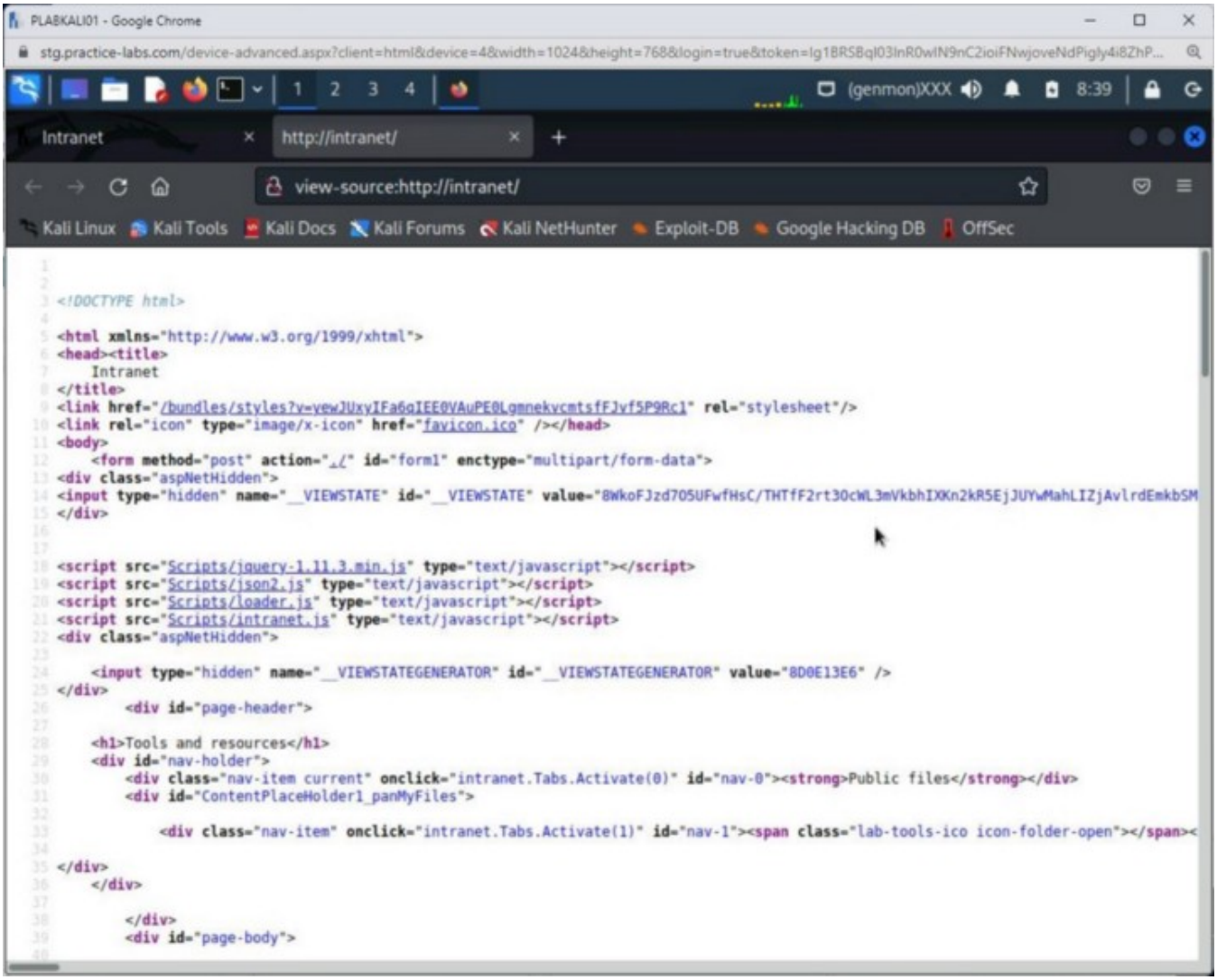
Step 2

Right-click anywhere on the webpage and select **View Page Source**.



Step 3

The webpage source is now displayed.

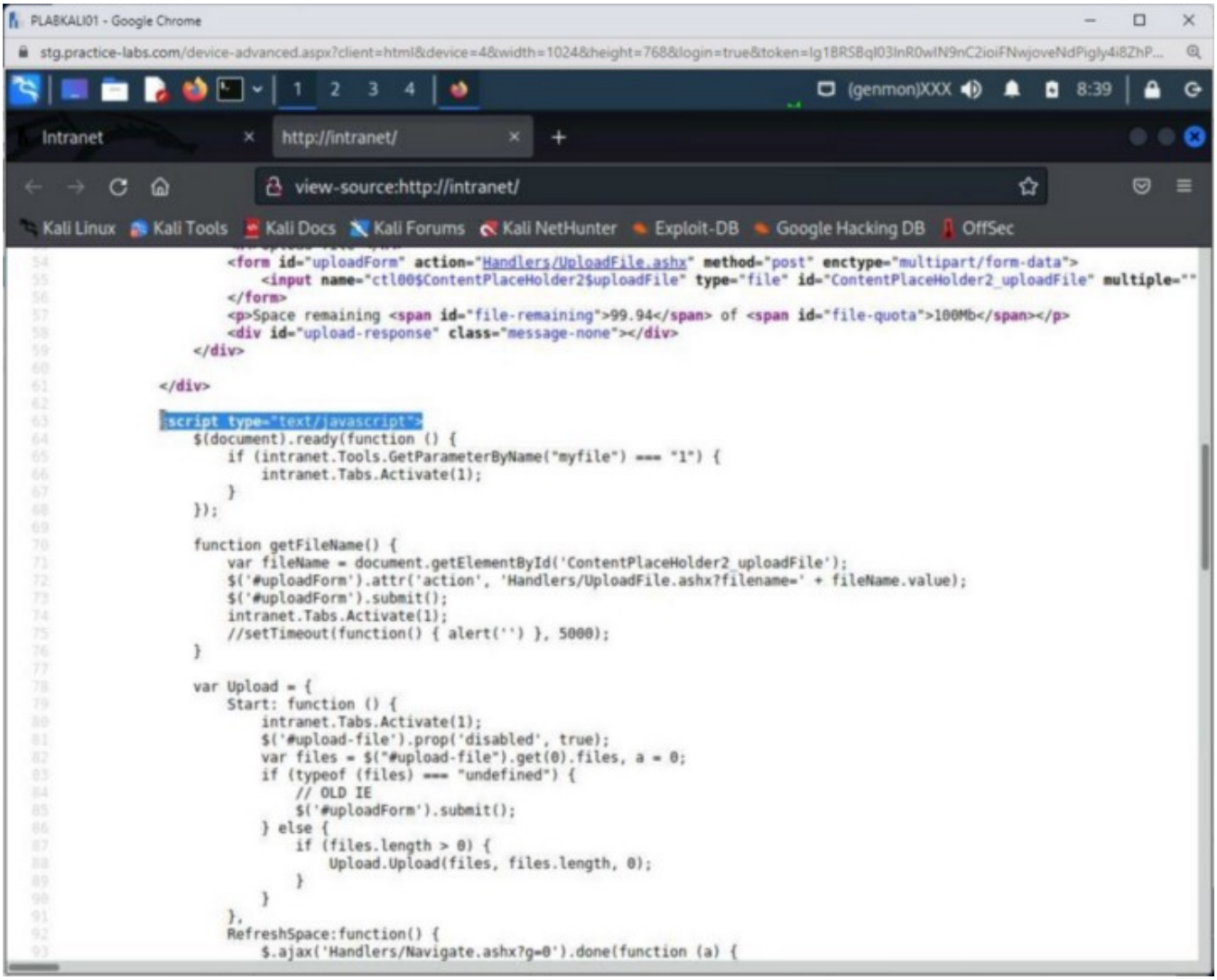


Step 4

Scroll down to line **63**, which mentions **text/javascript**.

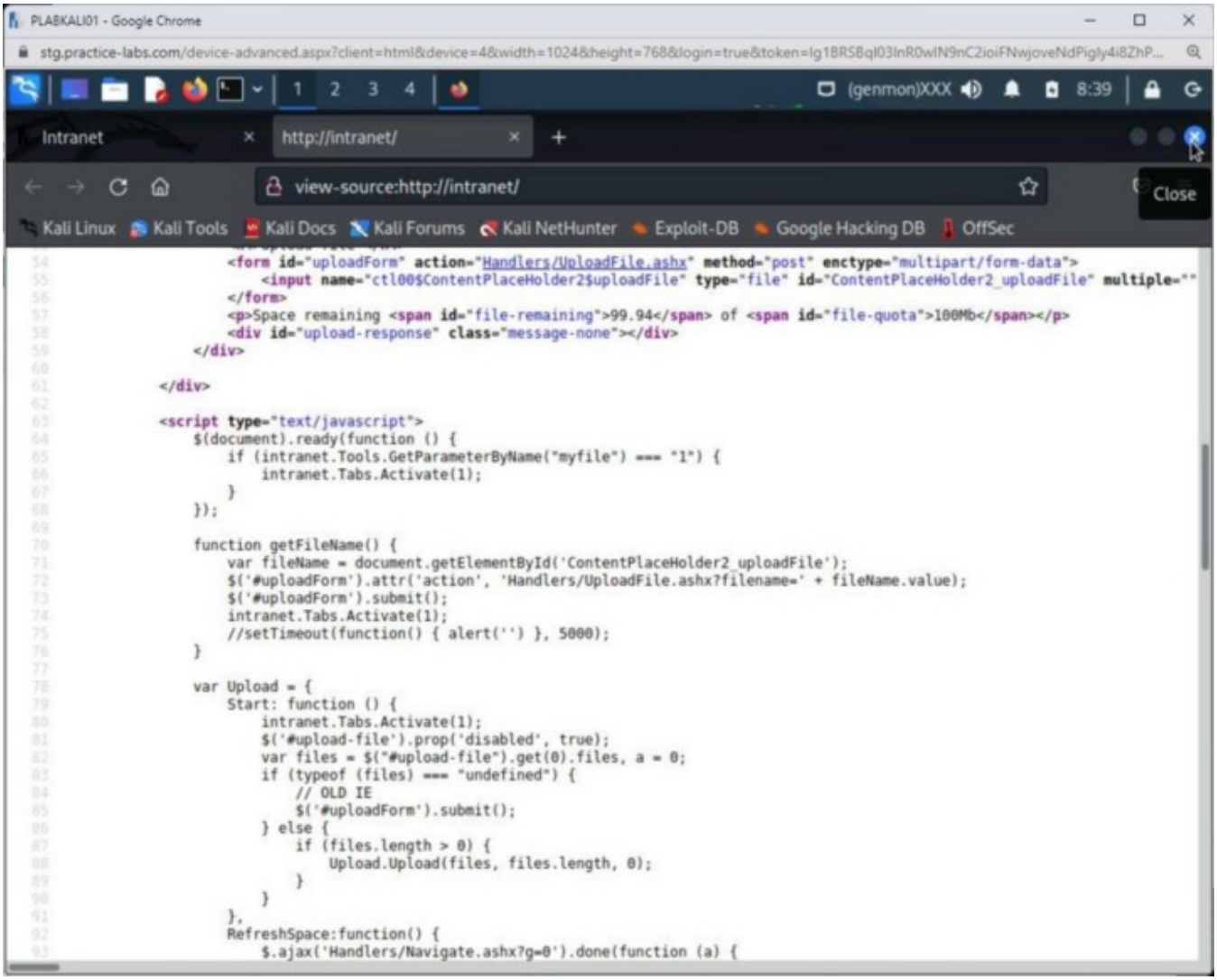
Now, you know that **JavaScript** is being used. You can also study the code to figure out any vulnerabilities.

***Note**: There are also references to the languages being used above in the code.*



Step 5

Close the **Firefox** window.



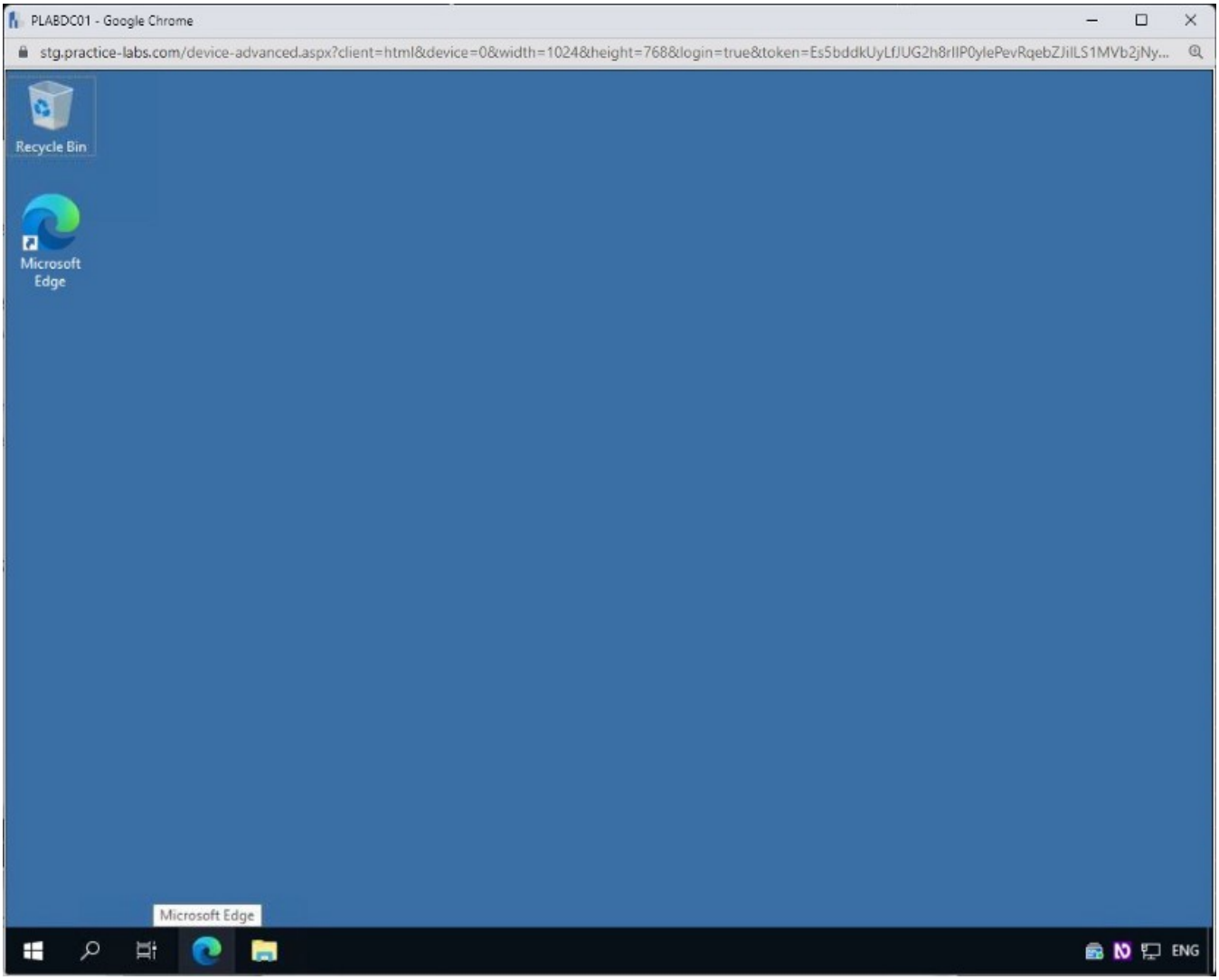
Task 2 — Footprint Using Archive.org

Organizations keep updating their websites from time to time. The archive.org website keeps track of all the updates or changes since the website was launched. An attacker can use this website to determine the changes made on the website. An attacker may use this information to conduct various attacks, such as phishing.

In this task, you will learn about Footprinting using the archive.org website.

Step 1

Connect to **PLABWIN10**. Click the **Microsoft Edge** icon on the taskbar.

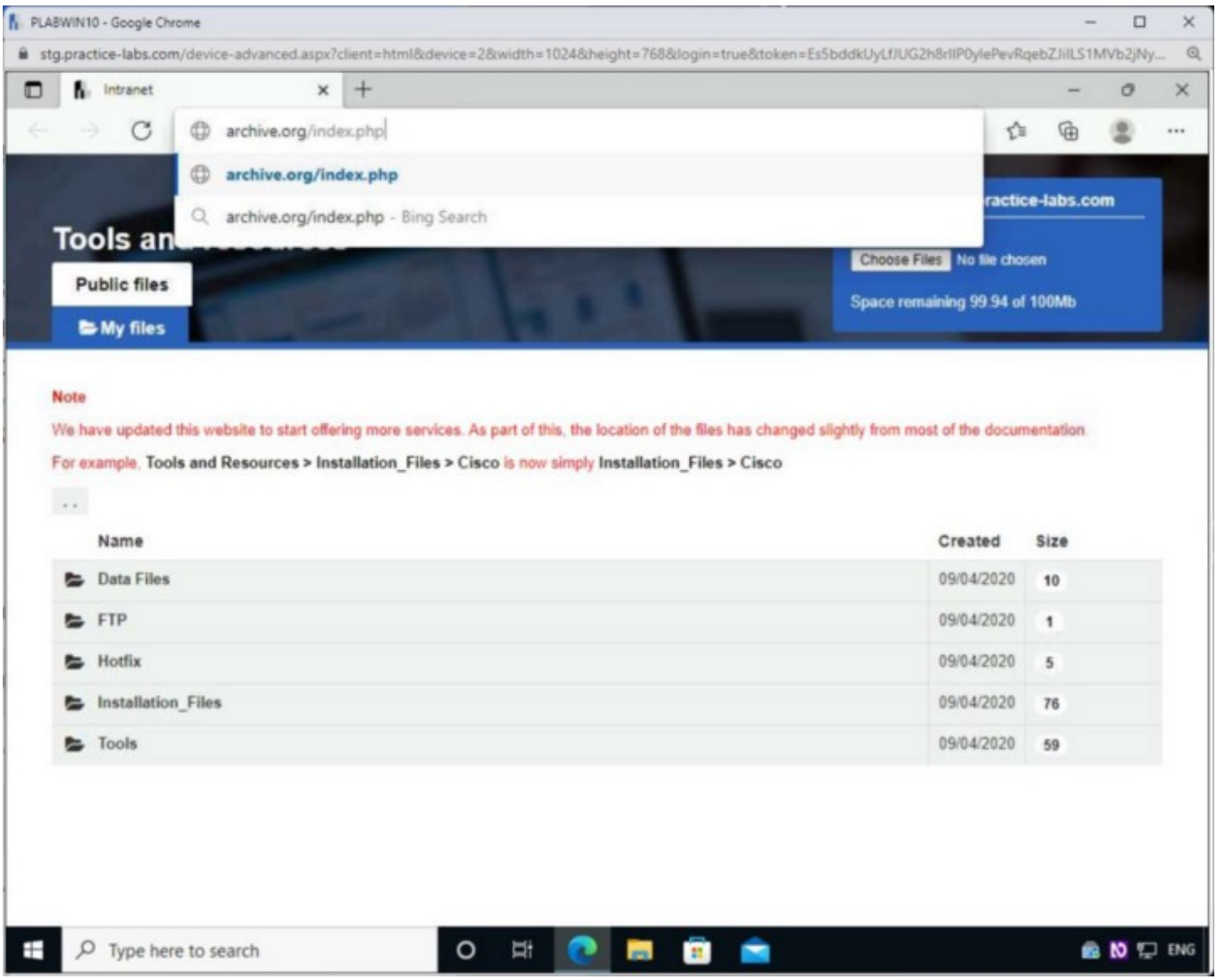


Step 2

In the address bar, type the following URL:

`https://archive.org/index.php`

Press **Enter**.



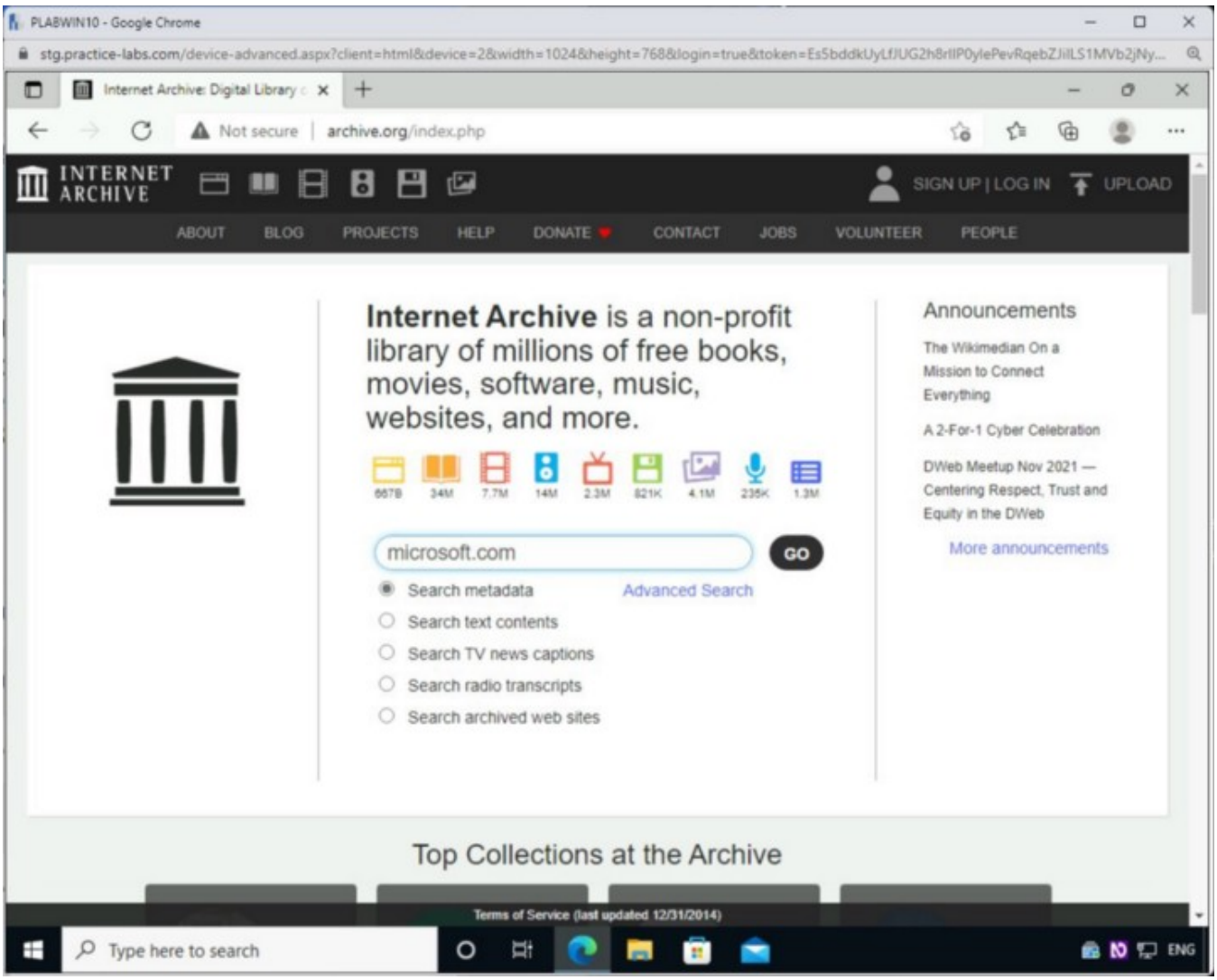
Step 3

The **archive.org** website's homepage is displayed.

In the search textbox, type the following:

```
microsoft.com
```

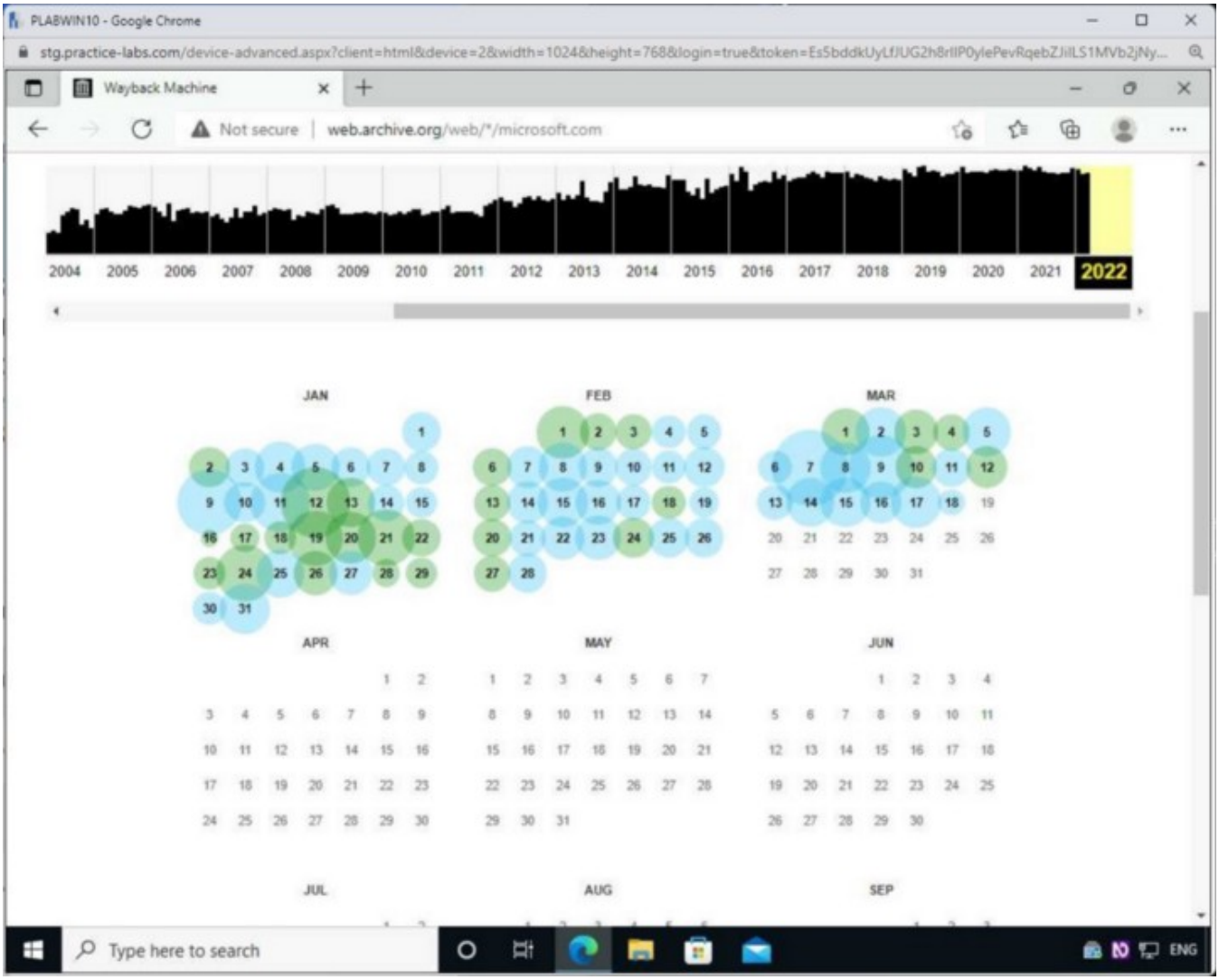
Click **Go** or press **Enter**.



Step 4

A chart of several years is displayed, and will default to the current year.

Notice that most dates are marked in circles when updates have taken place.

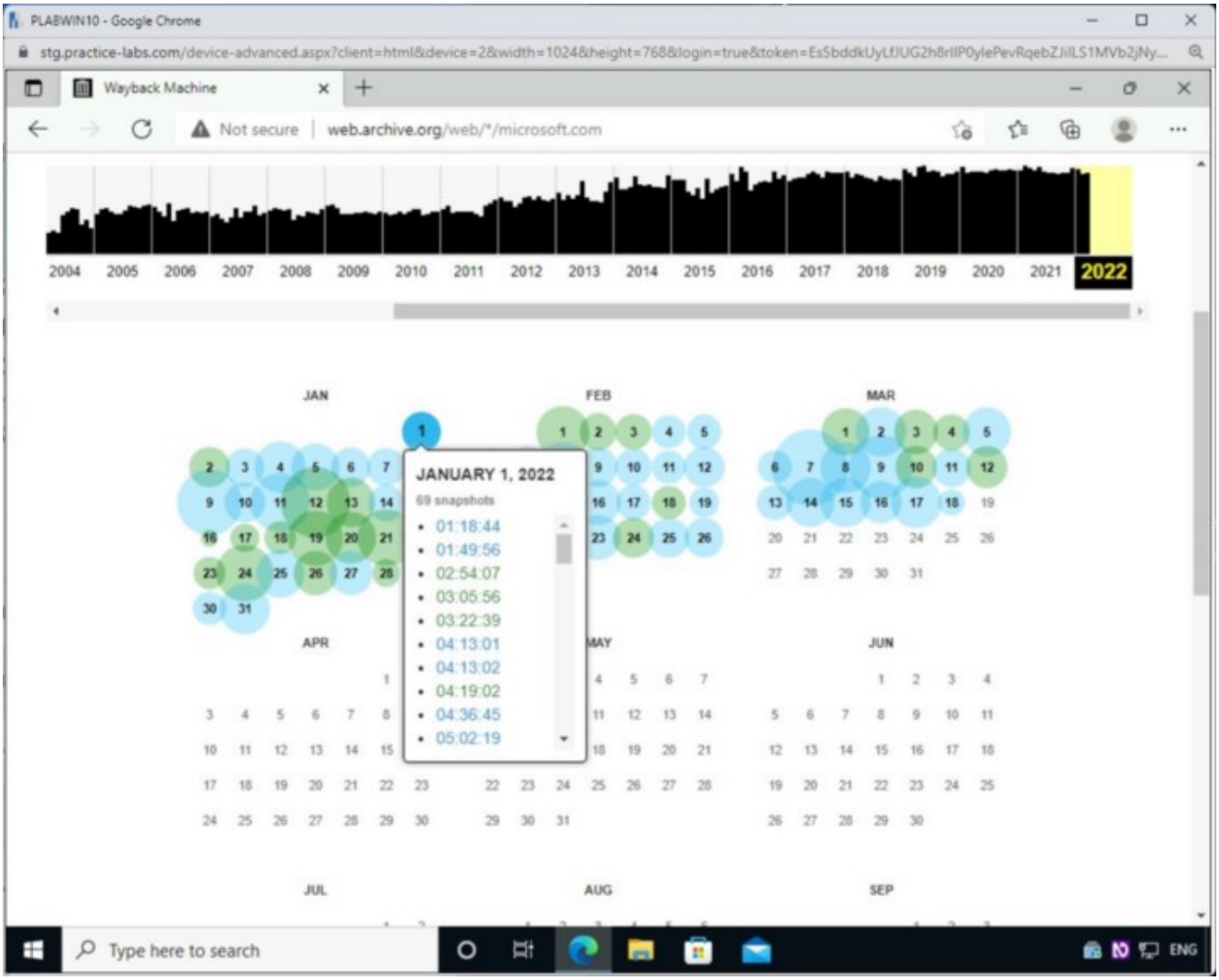


Step 5

Hover mouse over **1** in **Jan** and notice that a list is displayed.

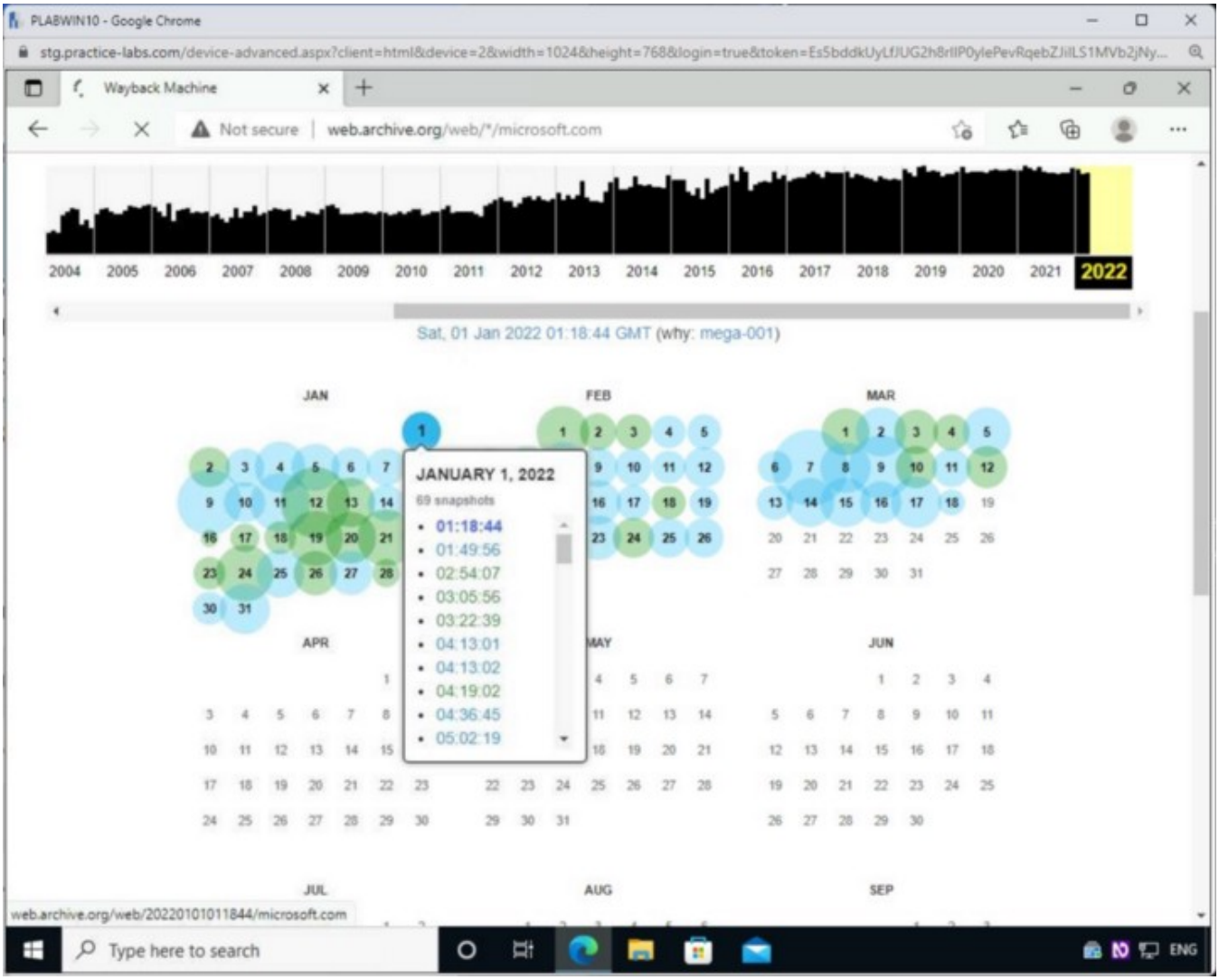
It indicates that **69** snapshots were taken on this date.

Note: *The number of snapshots will vary.*



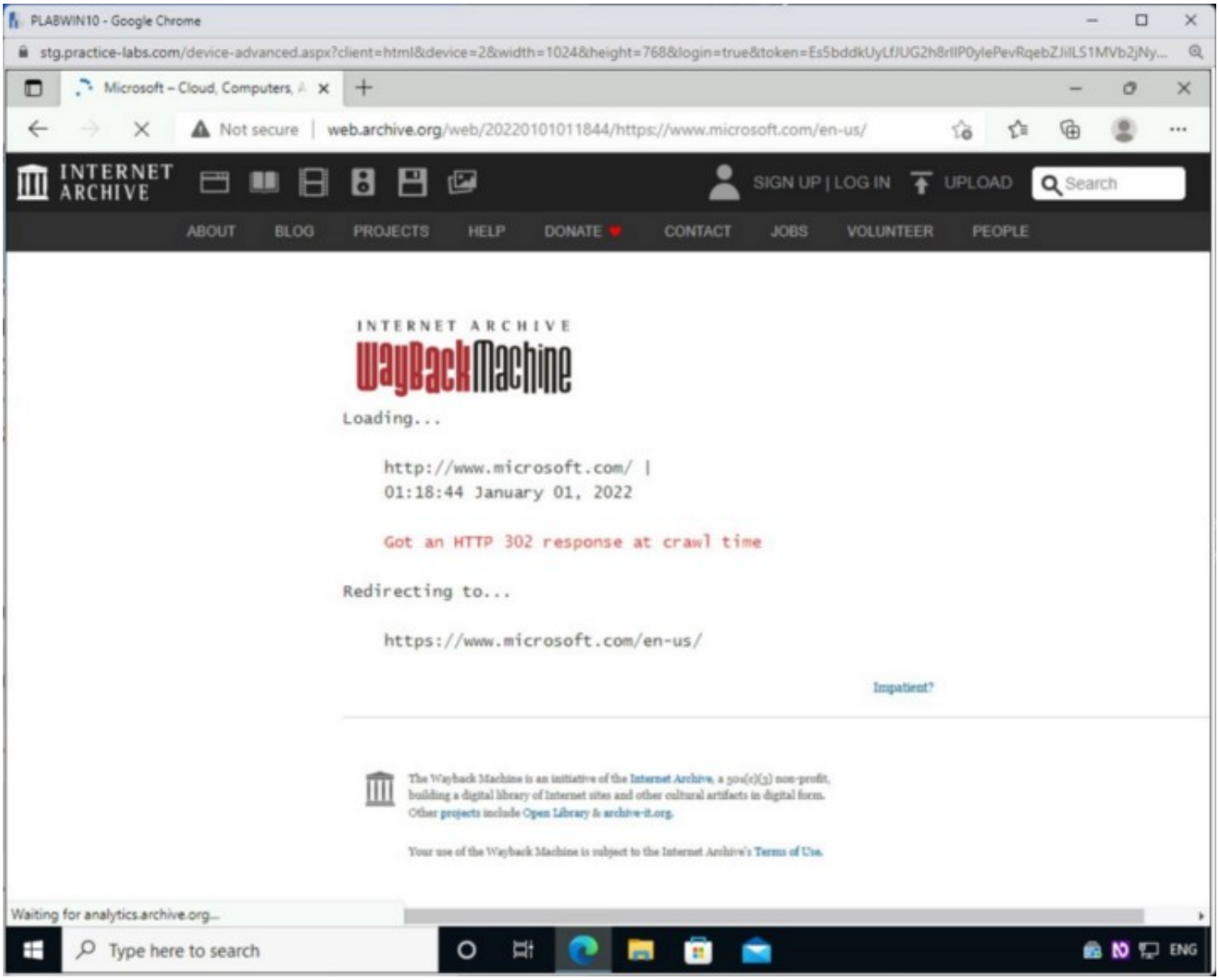
Step 6

Click on the first timestamp, **01:18:44**.



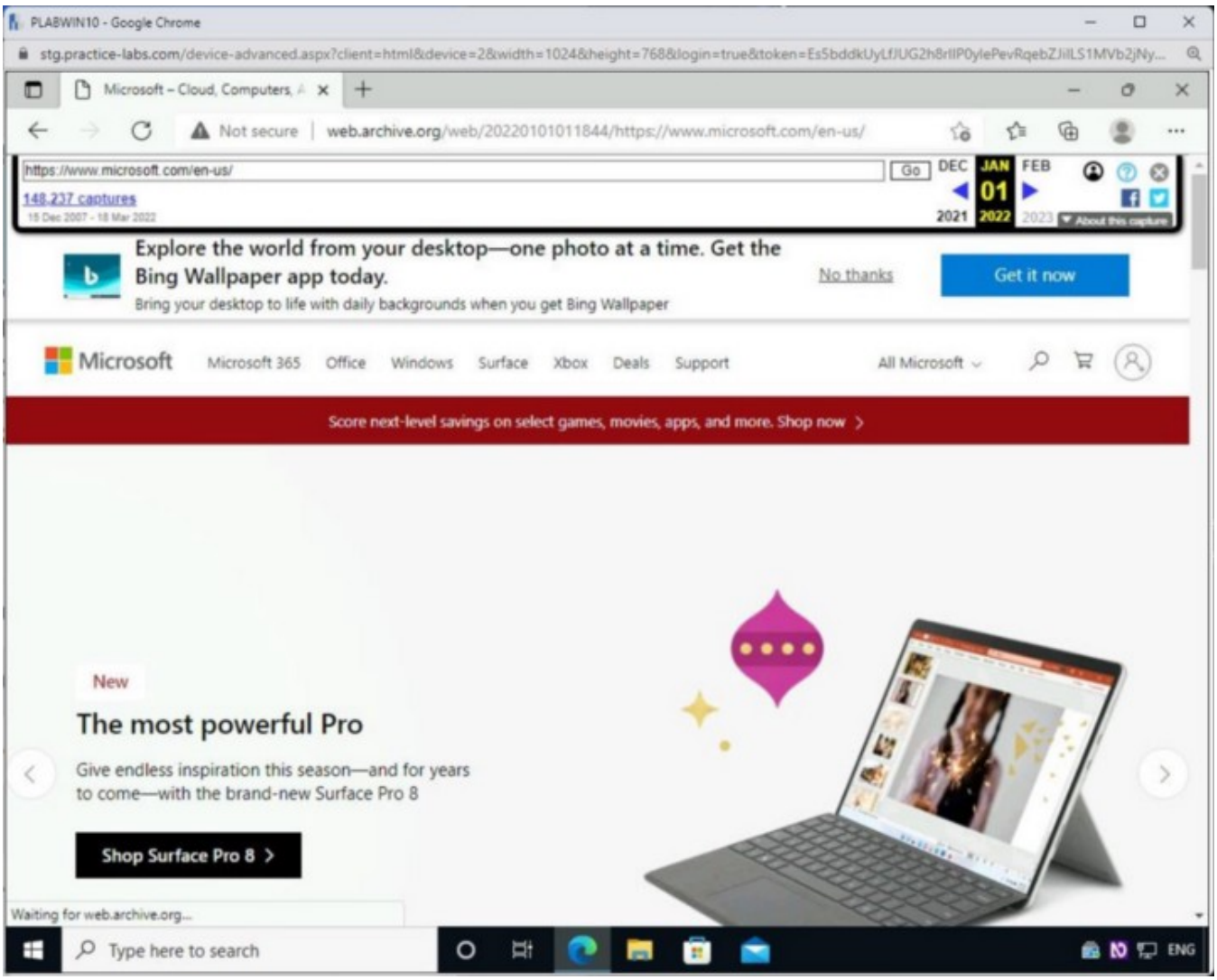
Step 7

The **archive.org** website is loading the snapshot from its archive.



Step 8

After a few seconds, archive will load the website from the specified time.



Close the **Microsoft Edge** window.

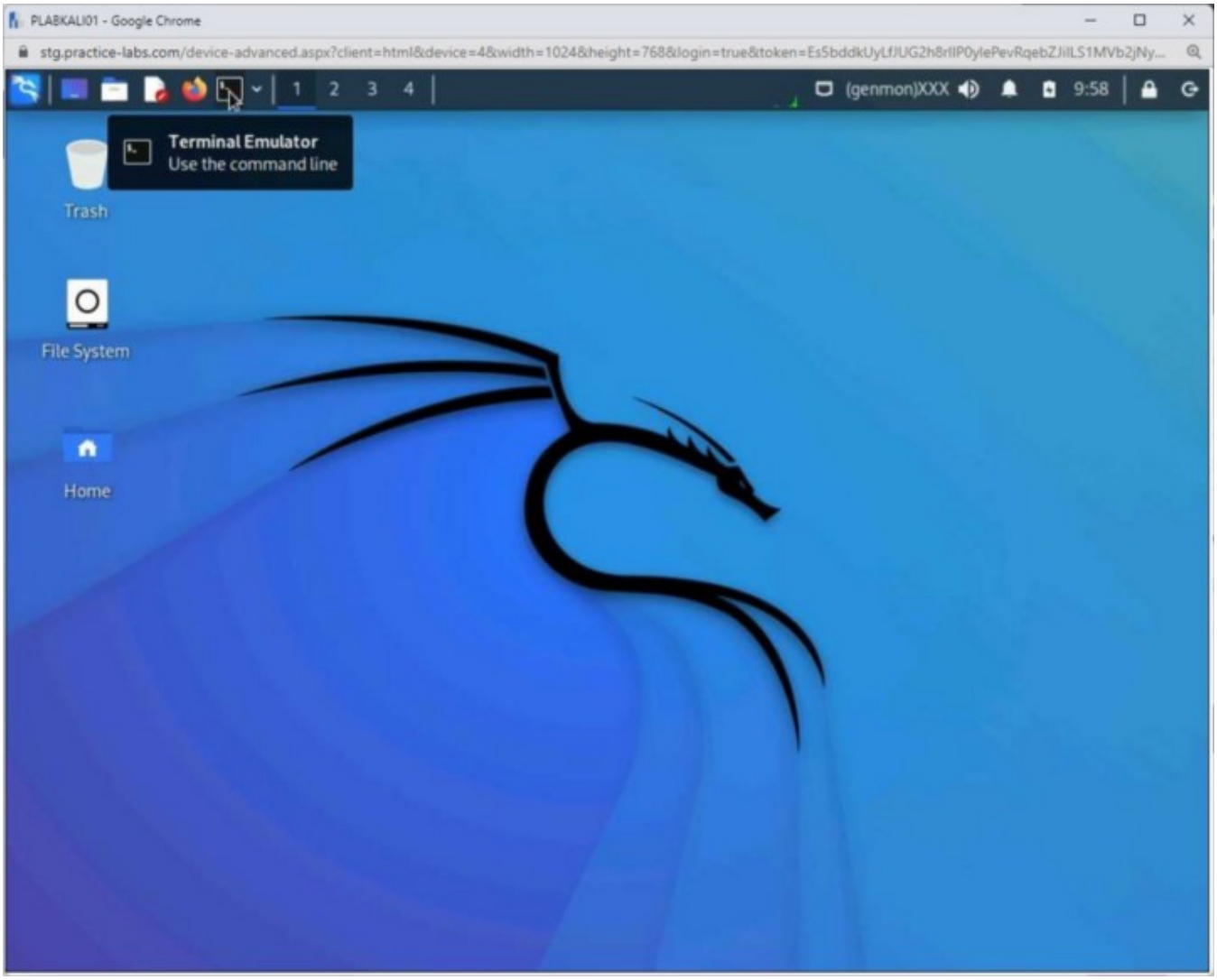
Task 3 — Create a Wordlist Using CeWL

An attacker may seek out words that are used on the website. These words are then used to create a wordlist that is further used for cracking passwords. Kali Linux contains a tool named CeWL, which generates wordlists.

In this task, you will create a wordlist using CeWL.

Step 1

Connect to **PLABKALI01** and open a new terminal window by clicking the **Terminal Emulator** icon on the taskbar.

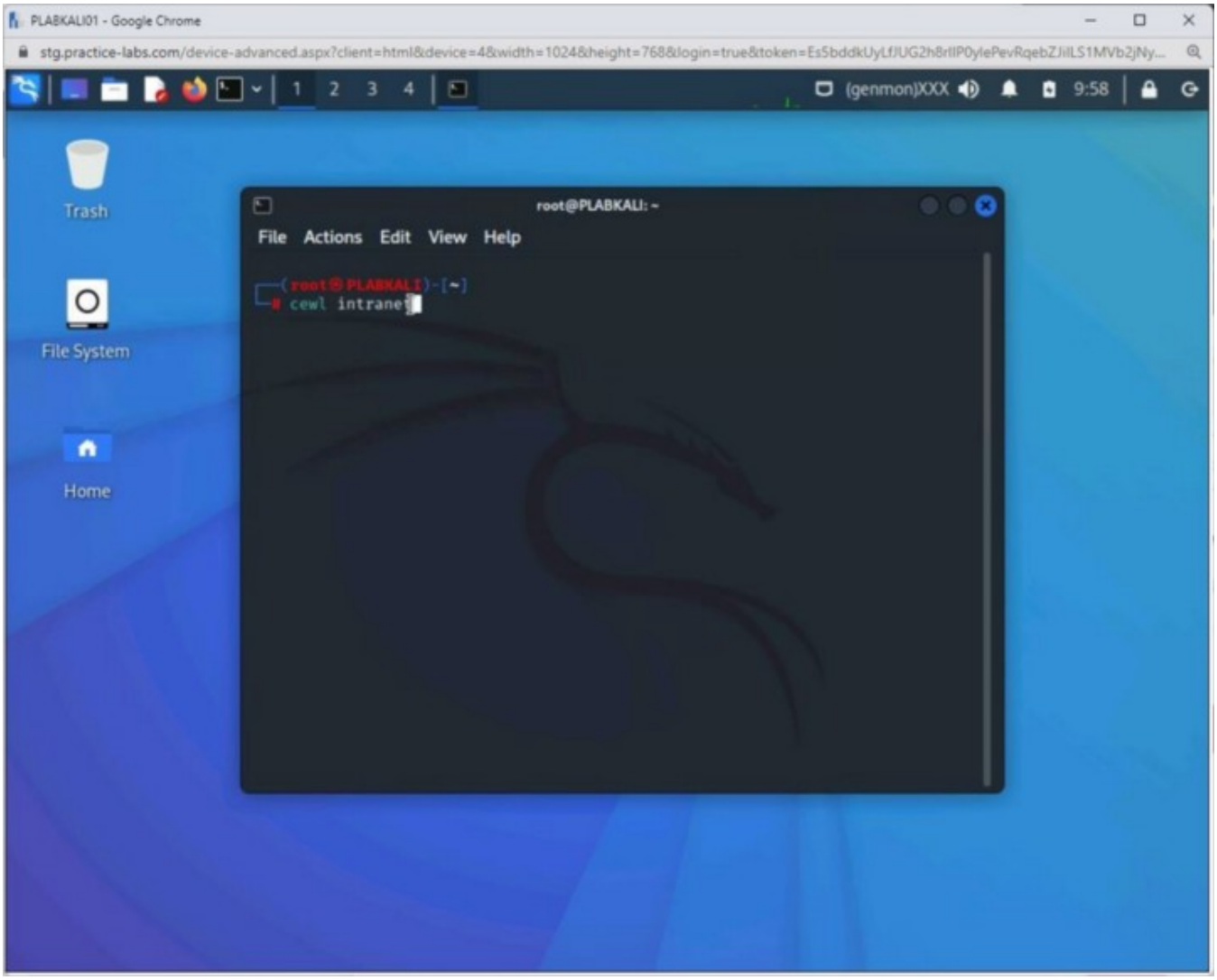


Step 2

Let's display the wordlist on the terminal. To do this, you need to execute the following command:

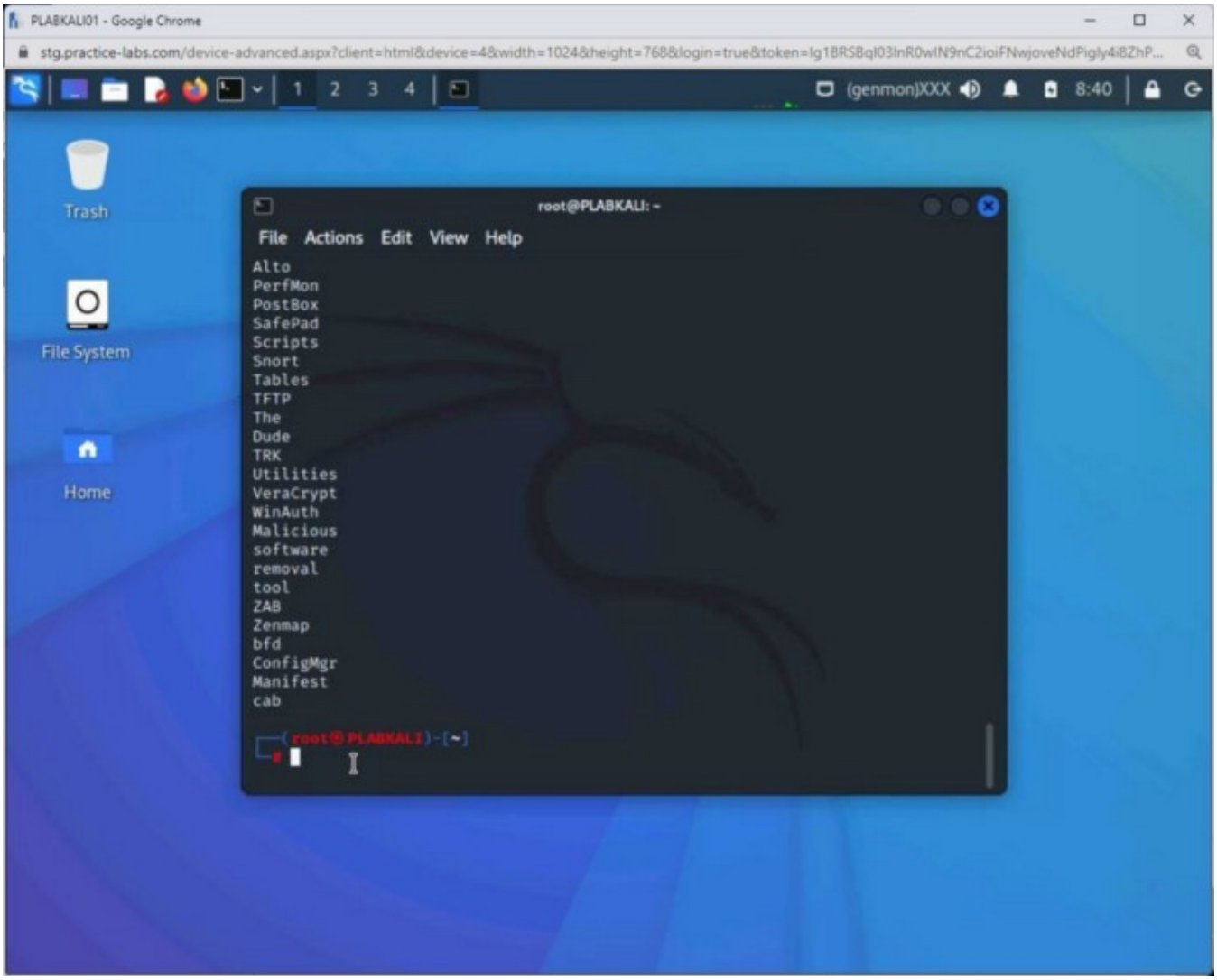
```
cewl intranet
```

Press **Enter**. The command execution starts.



Step 3

The wordlist is generated and displayed on the terminal. Notice that keywords were picked up and displayed as part of the wordlist.



Step 4

Clear the terminal with the following command:

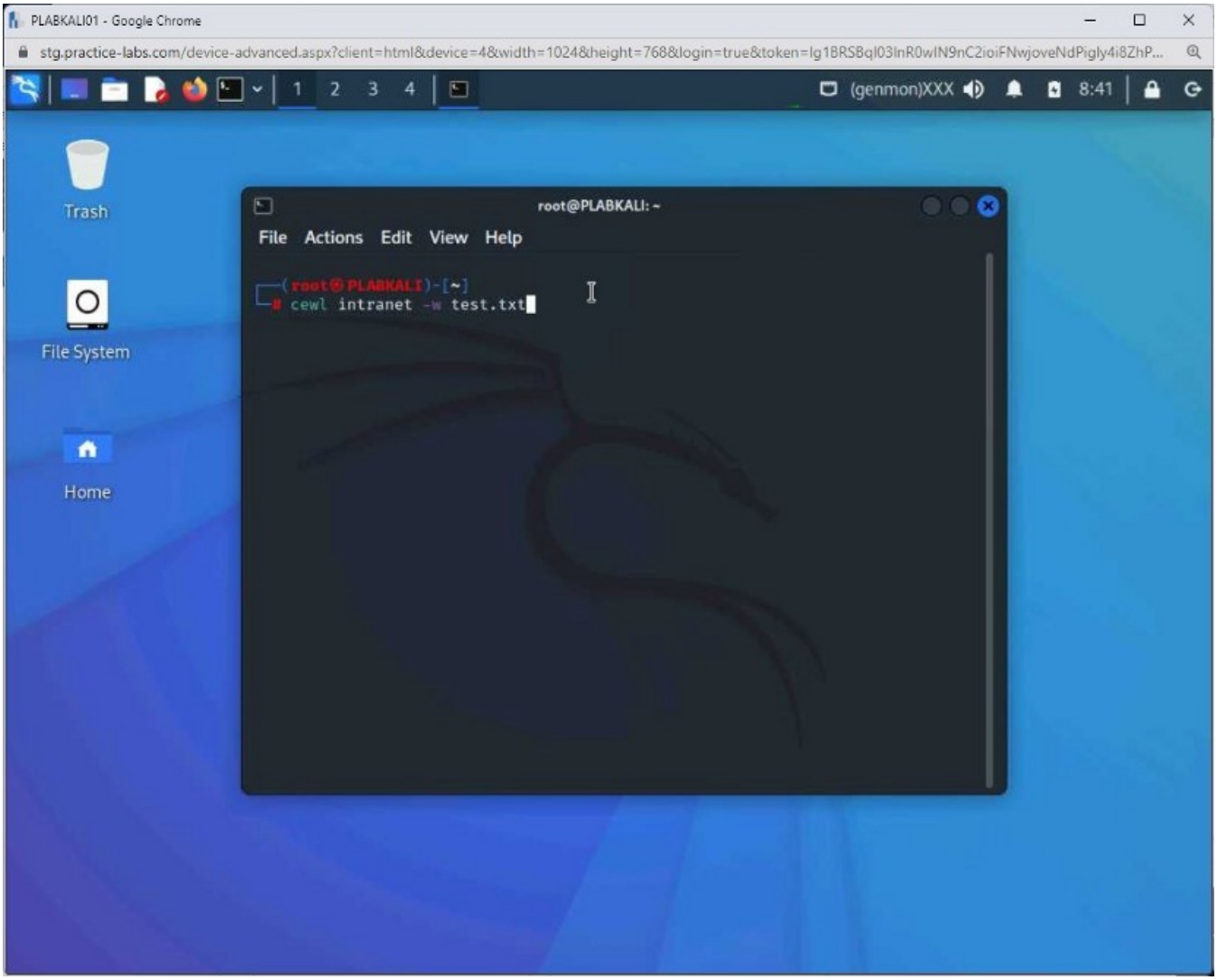
```
clear
```

Press **Enter**.

Next, you can write the output to a file without displaying it on the terminal. To do this, you need to use the **-w** parameter:

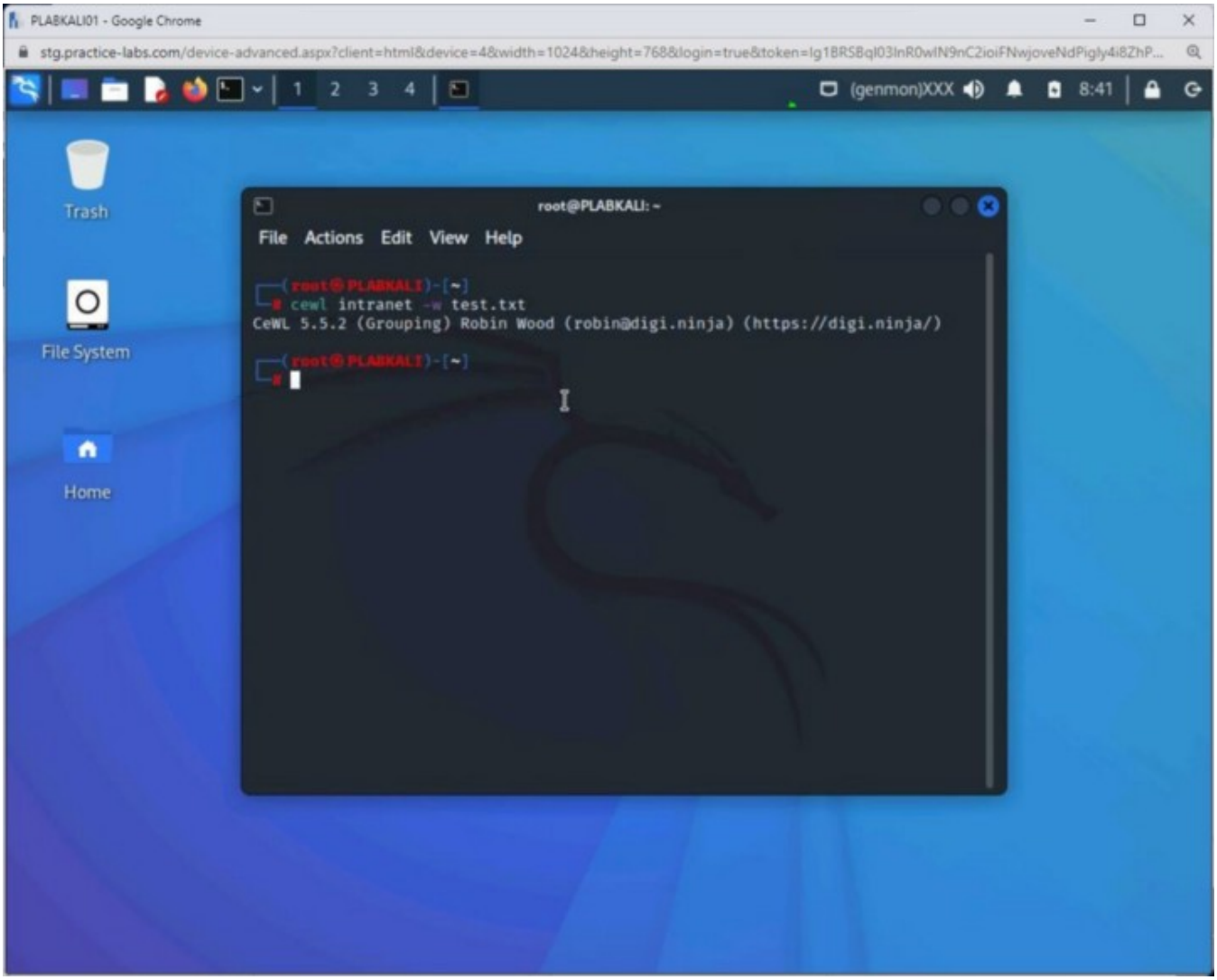
```
cewl intranet -w test.txt
```

Press **Enter**. The command execution starts.



Step 5

Notice that no output is generated on the terminal. The output is written to the **test.txt** file.

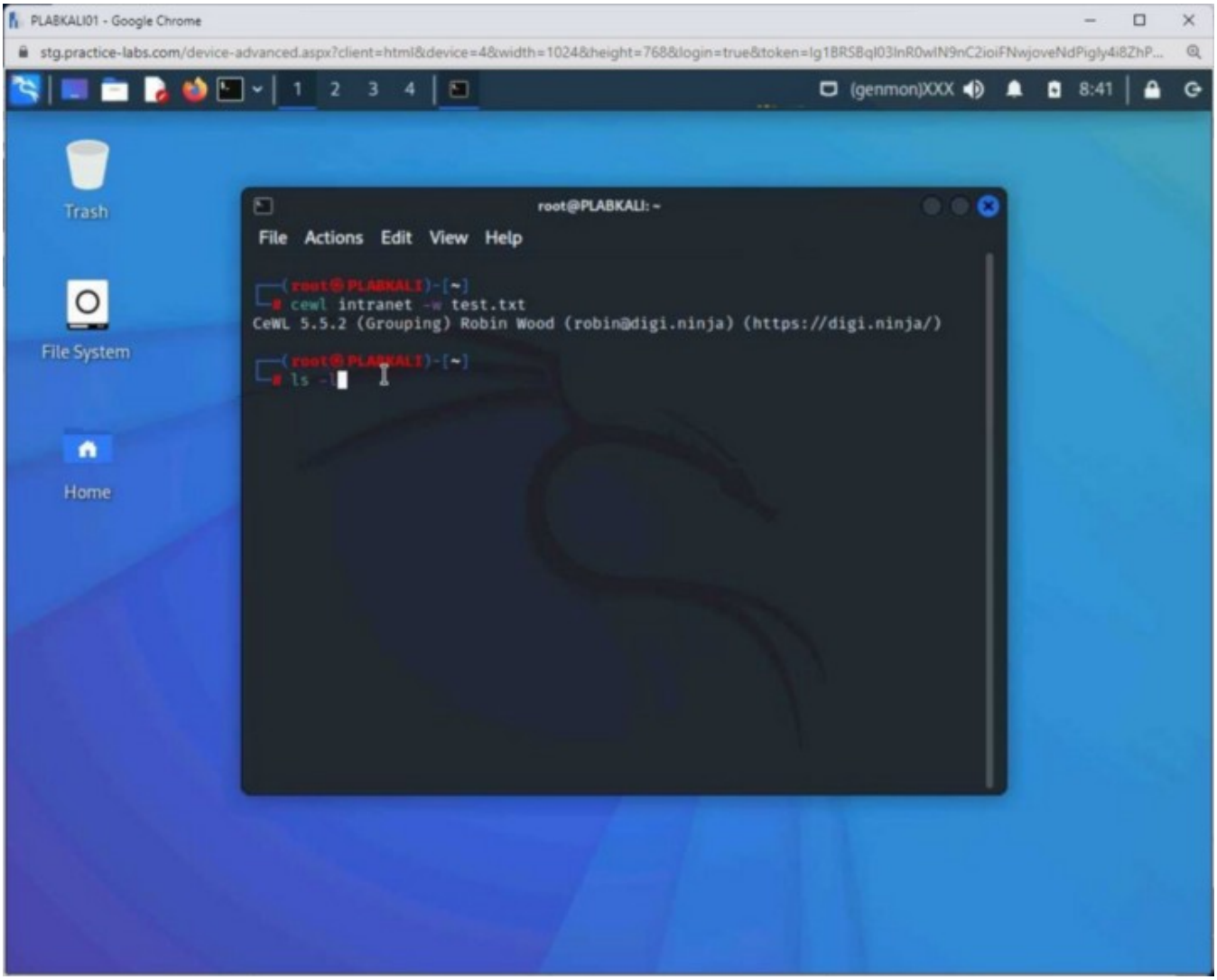


Step 6

Let's verify if the **test.txt** file has been created. Type the following command:

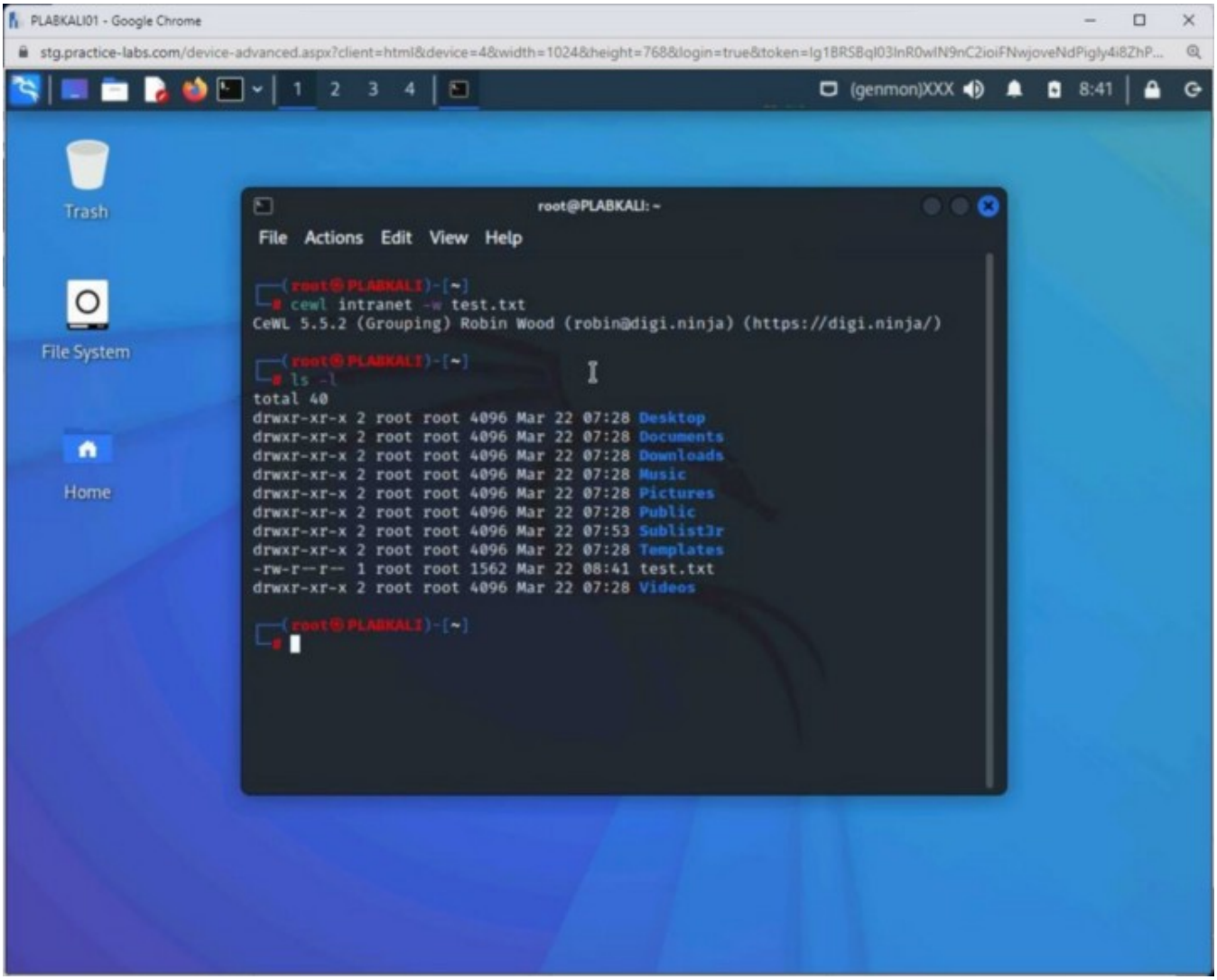
```
ls -l
```

Press **Enter**.



Step 7

Notice that the file is listed.



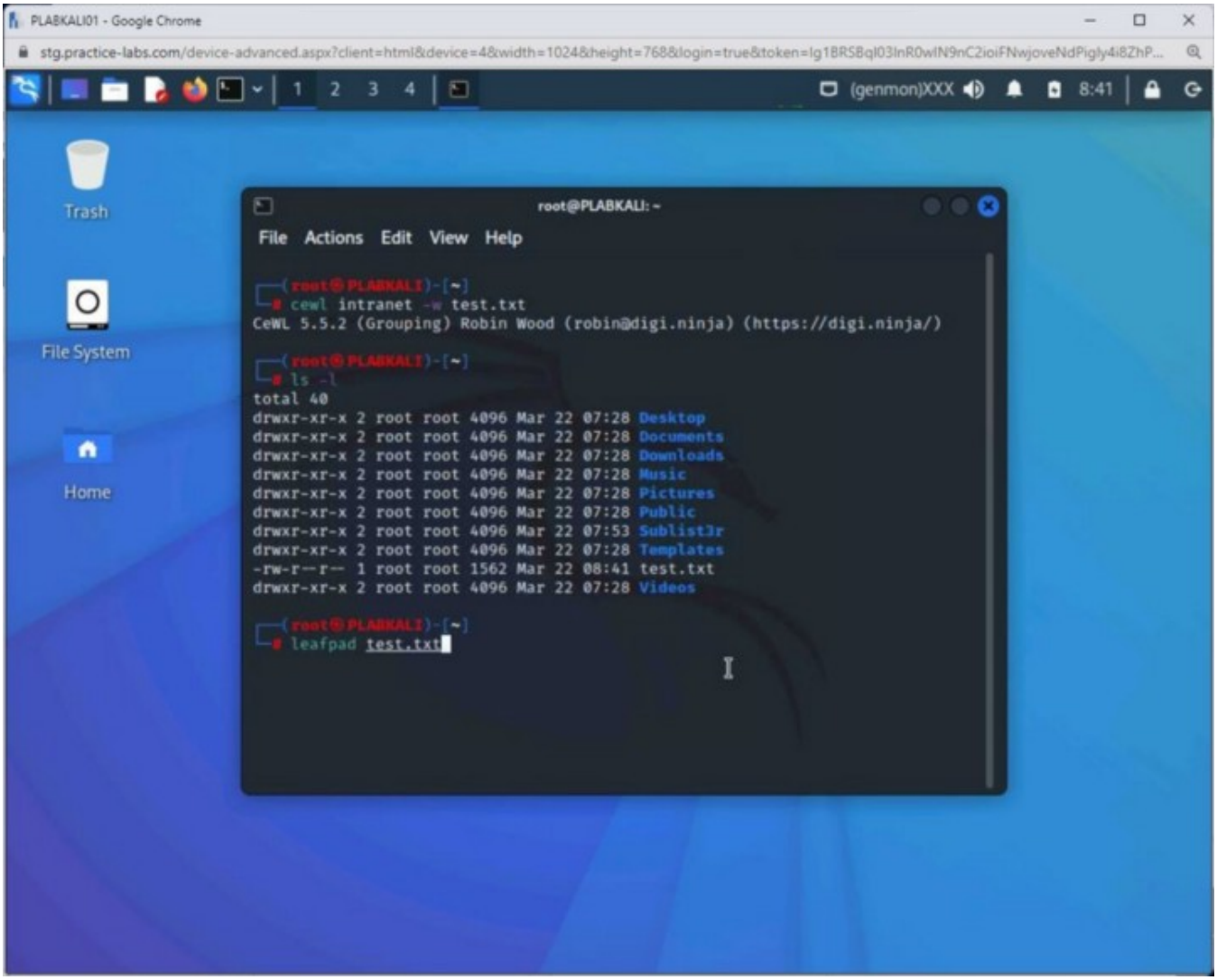
Step 8

Let's open the **test.txt** file and see the stored words in it.

Type the following command:

```
leafpad test.txt
```

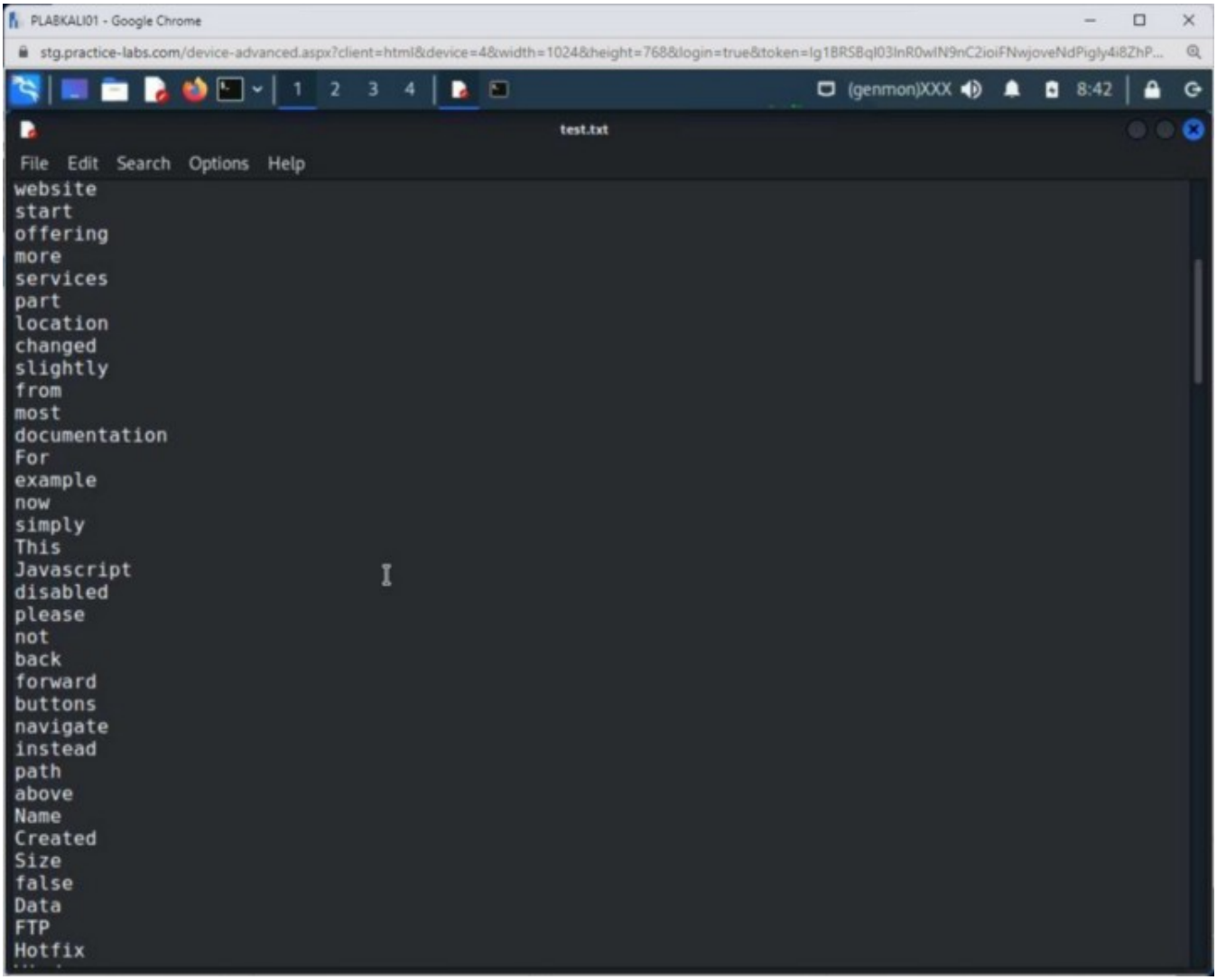
Press **Enter**.



Step 9

The **test.txt** file is now open. It has captured several words from the Intranet Website. Notice that there are words with three letters or more.

When you are ready, close this file.



Step 10

Clear the terminal with the following command:

```
clear
```

Press **Enter**.

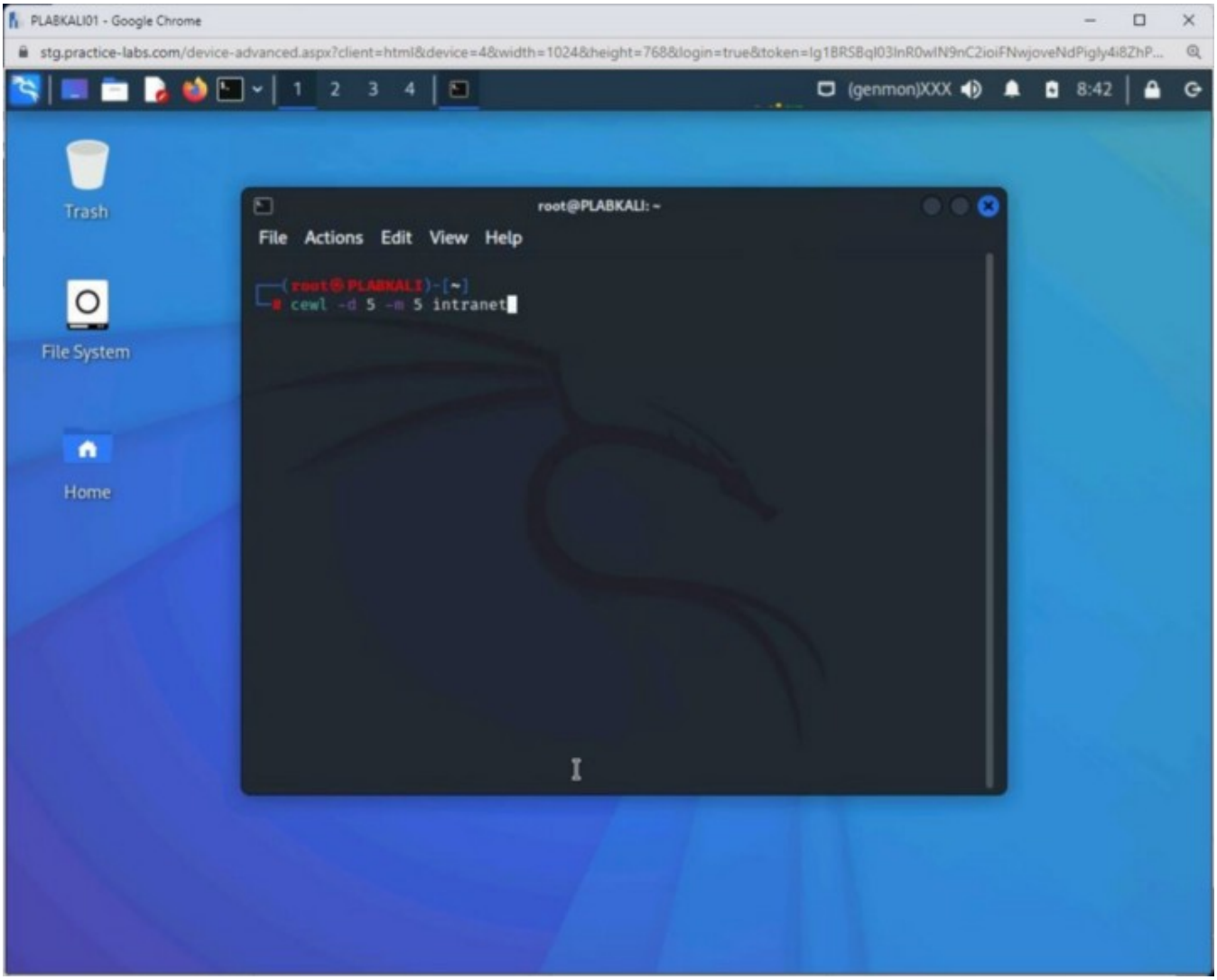
You will now display the output with two exceptions:

- You will add words of five letters or more using the -m parameter
- You will also select the depth of search using the -d parameter

Type the following command:

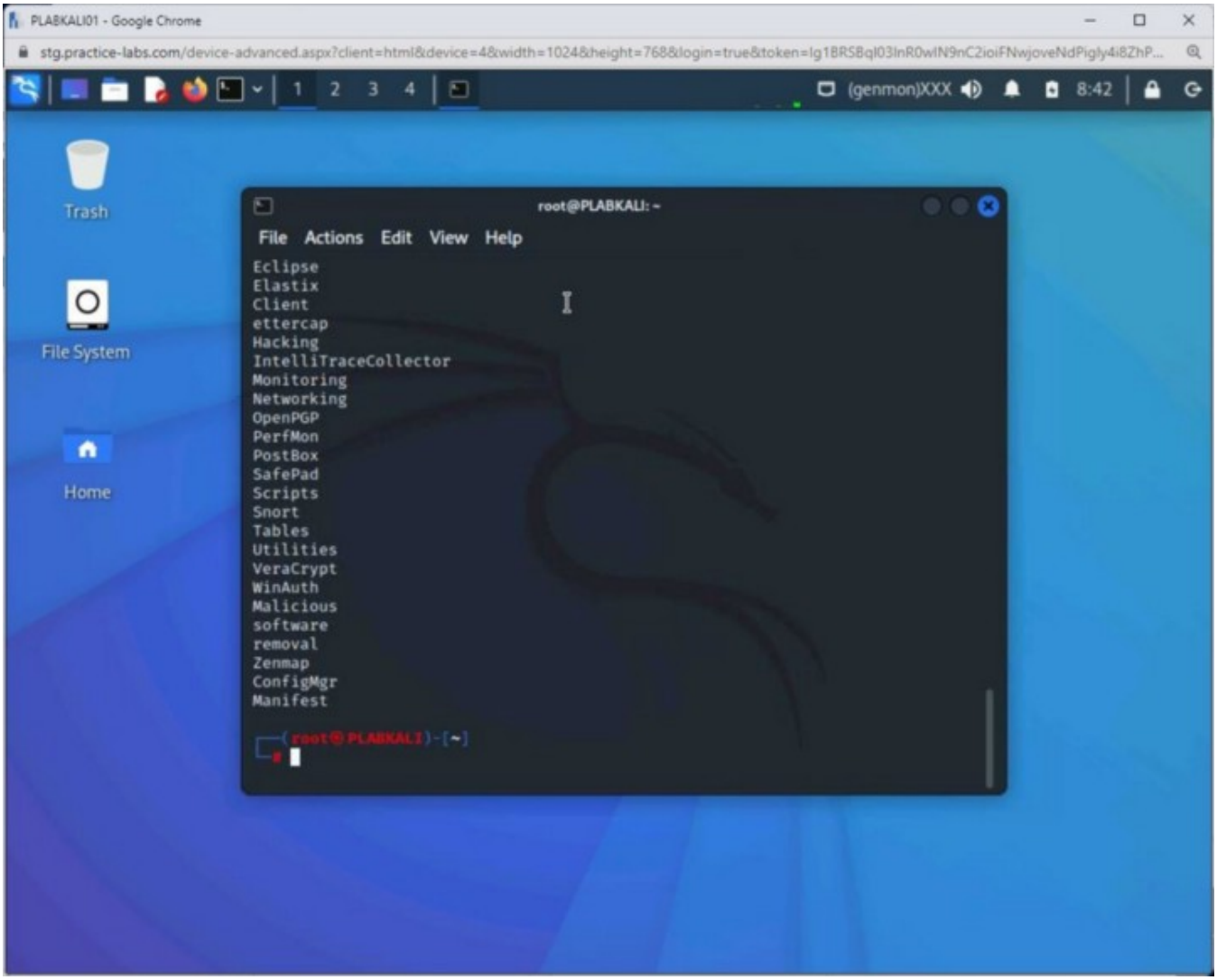
```
cewl -d 5 -m 5 intranet
```

Press **Enter**.



Step 11

The command runs successfully without any error. However, it is important to notice that there are no words with less than five letters.



Step 12

Clear the terminal with the following command:

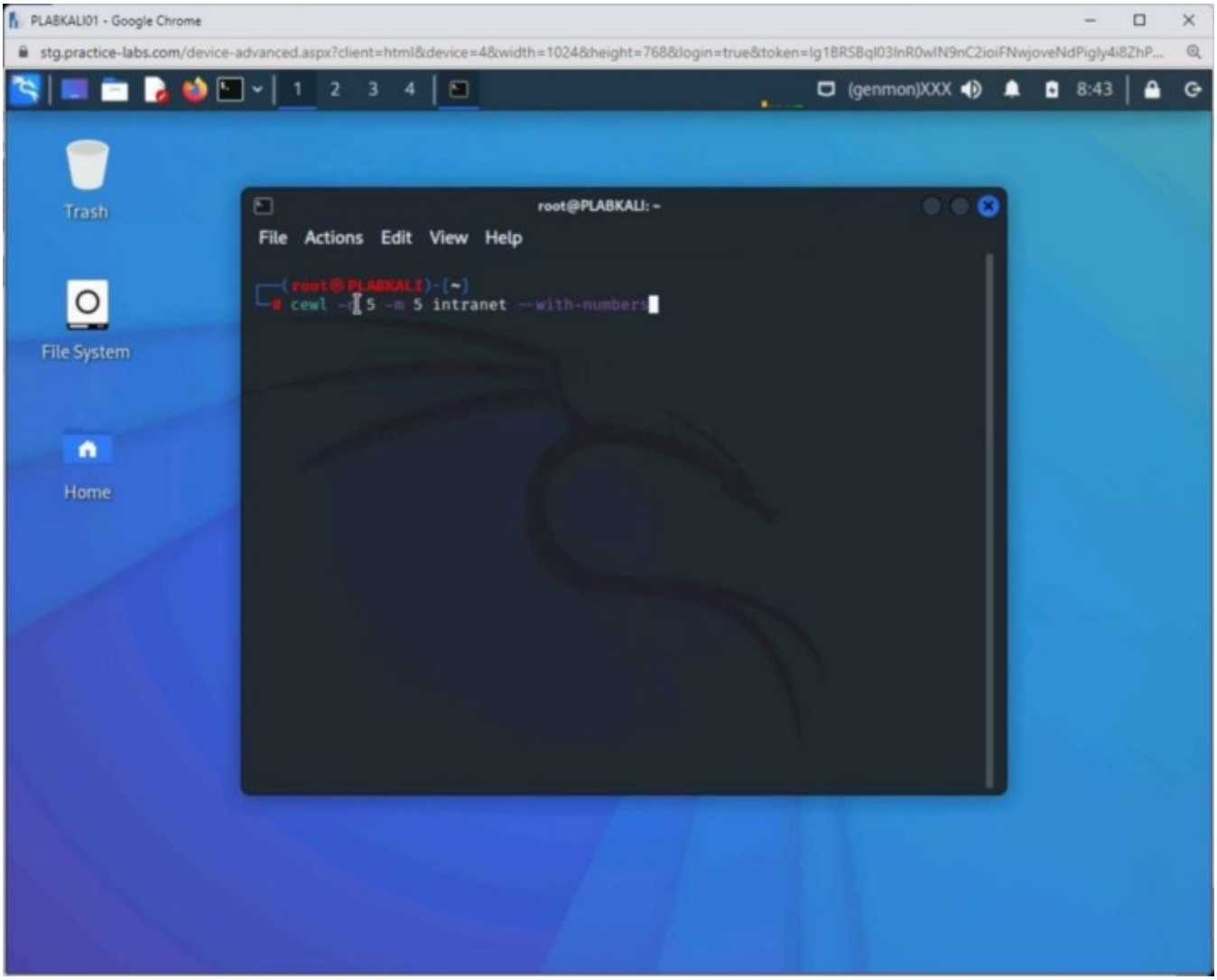
```
clear
```

Press **Enter**.

You can also generate words that are a mix of letters and numbers. To do this, you need to use the **— with-numbers** parameter. Type the following command:

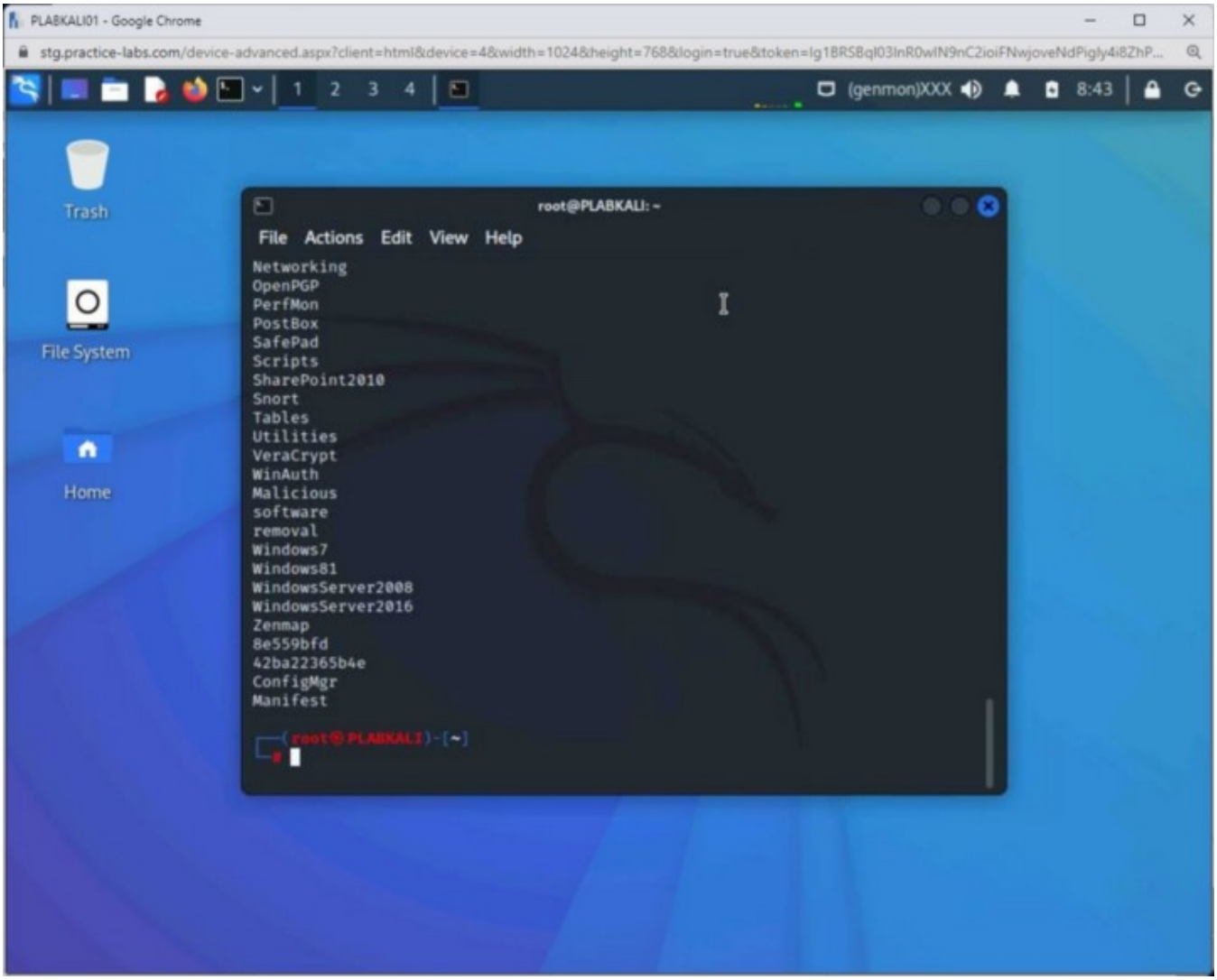
```
cewl -d 5 -m 5 intranet --with-numbers
```

Press **Enter**.



Step 13

The output displays words that are made of letters and numbers.



Keep the terminal window open.

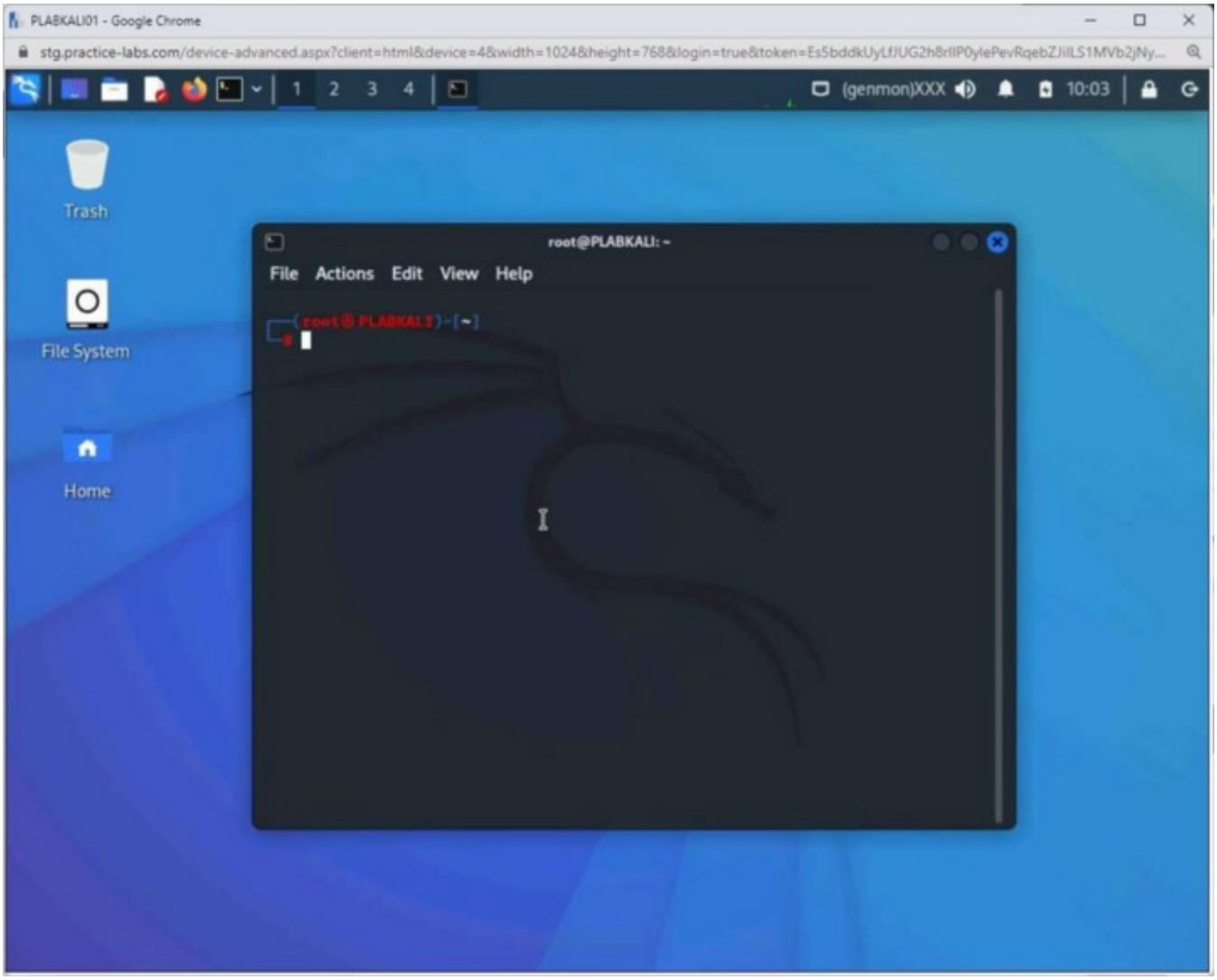
Task 4 — Perform Banner Grabbing using Nmap

Various tools can help you grab the banner of a website, but nmap is quick in doing this. For example, you can figure out the webserver name and so on.

In this task, you will grab the banner using Nmap. To do this, perform the following steps:

Step 1

Connect to **PLABKALI01** and ensure that the terminal window is open.



Step 2

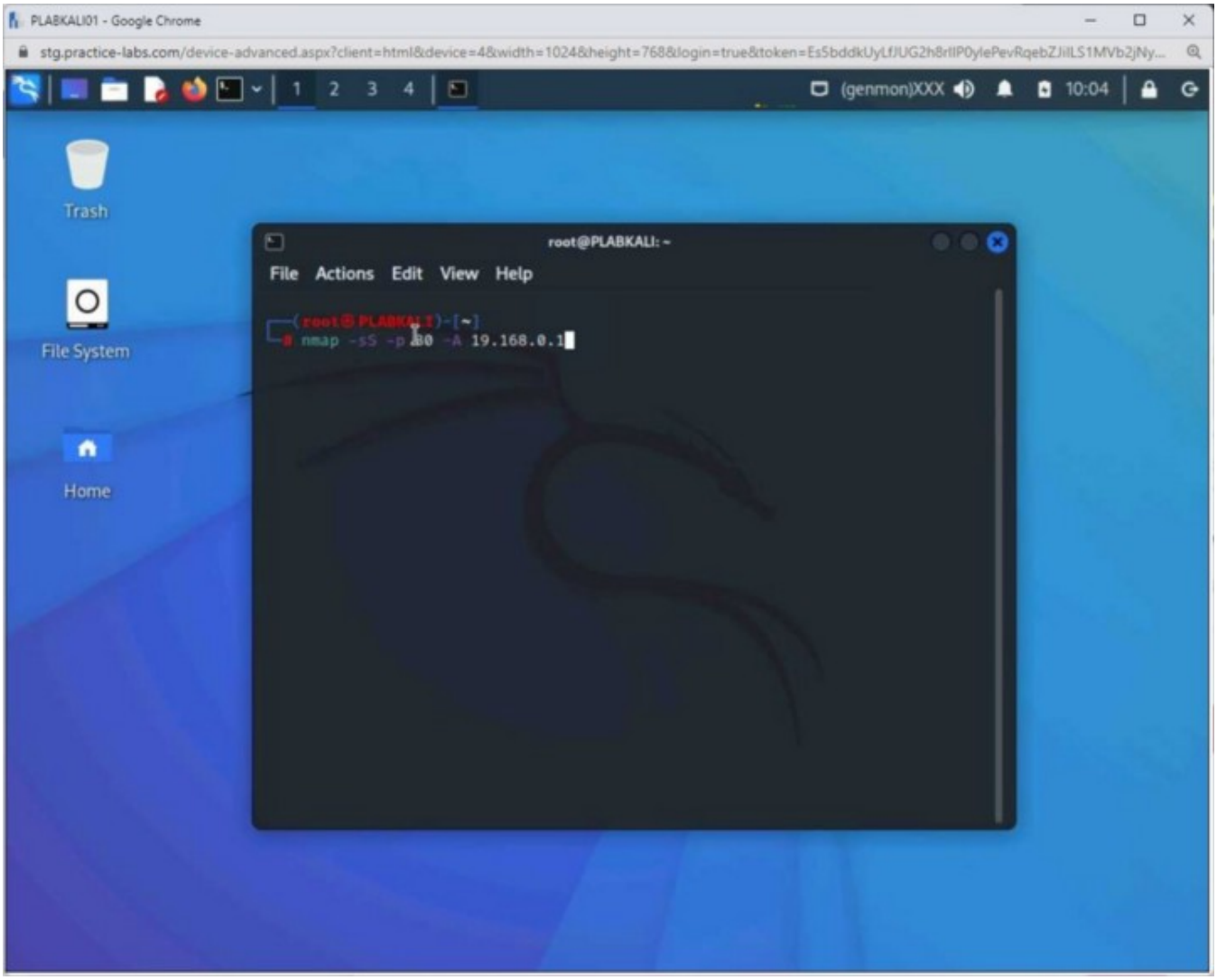
Type the following command:

```
nmap -sS -p 80 -A 192.168.0.1
```

Press **Enter**.

The given command uses the following parameters:

- **-sS** = SYN Scan
- **-p** = Port Number
- **-A** = Aggressive mode



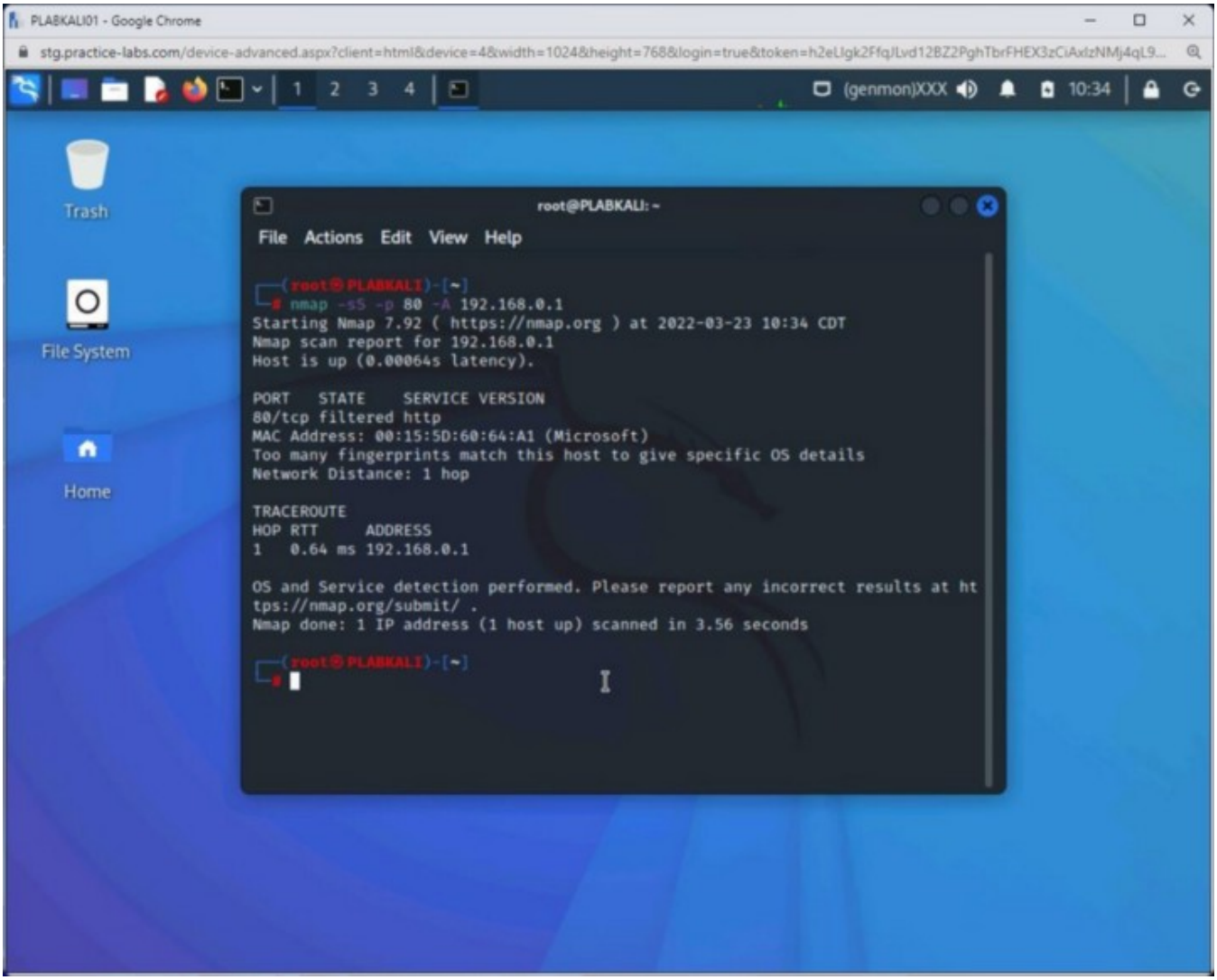
Step 3

Notice that the output displays information about the operating system of the target system and the services running on open ports.

There is quite a lot of information you can get from this scan, such as:

- Webserver name and version
- Operating system type and version
- MAC address

An attacker can use all this information. For example, an attacker may simply find the webserver name and version and look for vulnerabilities. If they are not patched on this webserver, then an attacker has a golden chance of exploiting the vulnerability.



Review

Well done, you have completed the **Footprinting & Reconnaissance — Part 1** CertMaster Lab

Footprinting & Reconnaissance Part 2

Exercise 1 — Whois Footprinting

Exercise 2 — DNS Footprinting

Exercise 3 — Network Footprinting

Exercise 4 — Footprinting through Social Engineering

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 2 — Whois Footprinting

- Exercise 3 — DNS Footprinting
- Exercise 4 — Network Footprinting
- Exercise 5 — Footprinting through Social Engineering

After completing this module, you will be able to:

- Footprint using Whois
- DNS Footprint using Nslookup
- DNS Footprint using Dnsenum
- Use Network Topology Mapper
- Use the Advanced IP Scanner

After completing this module, you will have further knowledge of:

- Social Engineering Methods
- Key Footprinting Countermeasures

Lab Duration

It will take approximately **1 hour** to complete this lab.

Exercise 1 — Whois Footprinting

The Whois Website is a website that returns information about a domain name. For example, if you enter a domain name, such as practice-labs.com, Whois will return the name and address of the domain's owner, which in this case is Practice Labs. You can also use the Whois command in Kali Linux. Using this command, you can find out information about a domain, such as:

- Registrar
- Server name
- Whois Server
- Referral URL
- IP address range

You can find out a lot of information about a particular domain. This information can be further used in attacking a particular domain or a server.

Note: *This is a live website. Therefore, search results may vary from what is shown in the screenshots.*

In this exercise, you will learn to use Whois to gather information about a domain.

Learning Outcomes

After completing this exercise, you will be able to:

- Footprint Using Whois

Your Devices

You will be using the following devices in this lab. Please power these on now.

PLABDC01Domain Controller192.168.0.1/24PLABWIN10Domain MemberWorkstation192.168.0.3/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

Task 1 — Footprint using Whois

Most people are unaware that Whois is a website and a query and response protocol that works on TCP port 43. Using Whois, you can query the domain databases and related information.

With the execution of a Whois query, you can get the following information:

- Domain name
- Domain owner’s information
- DNS servers
- Registration and expiration date

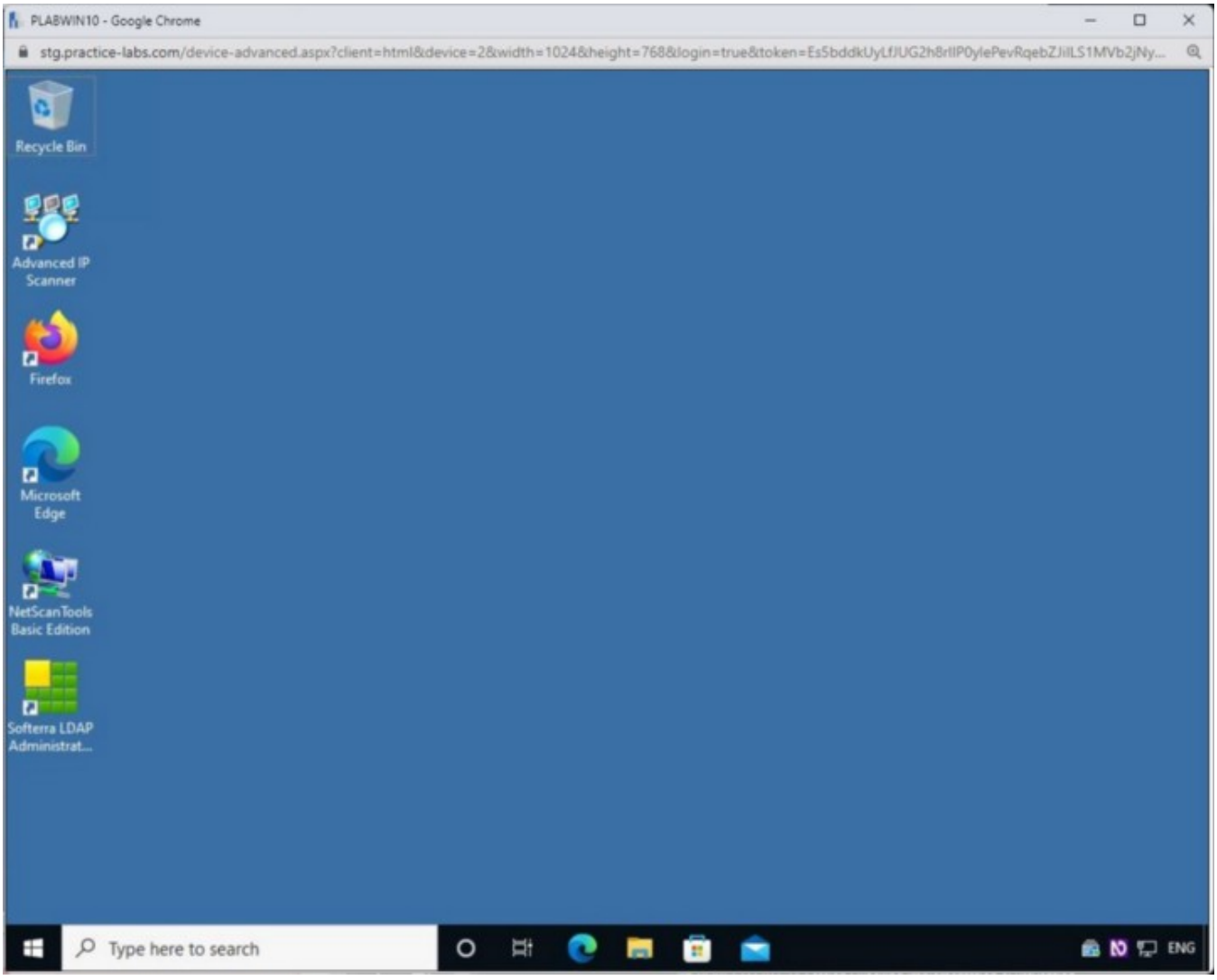
- Last update

All this information can be handy for an attacker. For example, an attacker may use this information to conduct a social engineering attack.

In this task, you will use the Whois website.

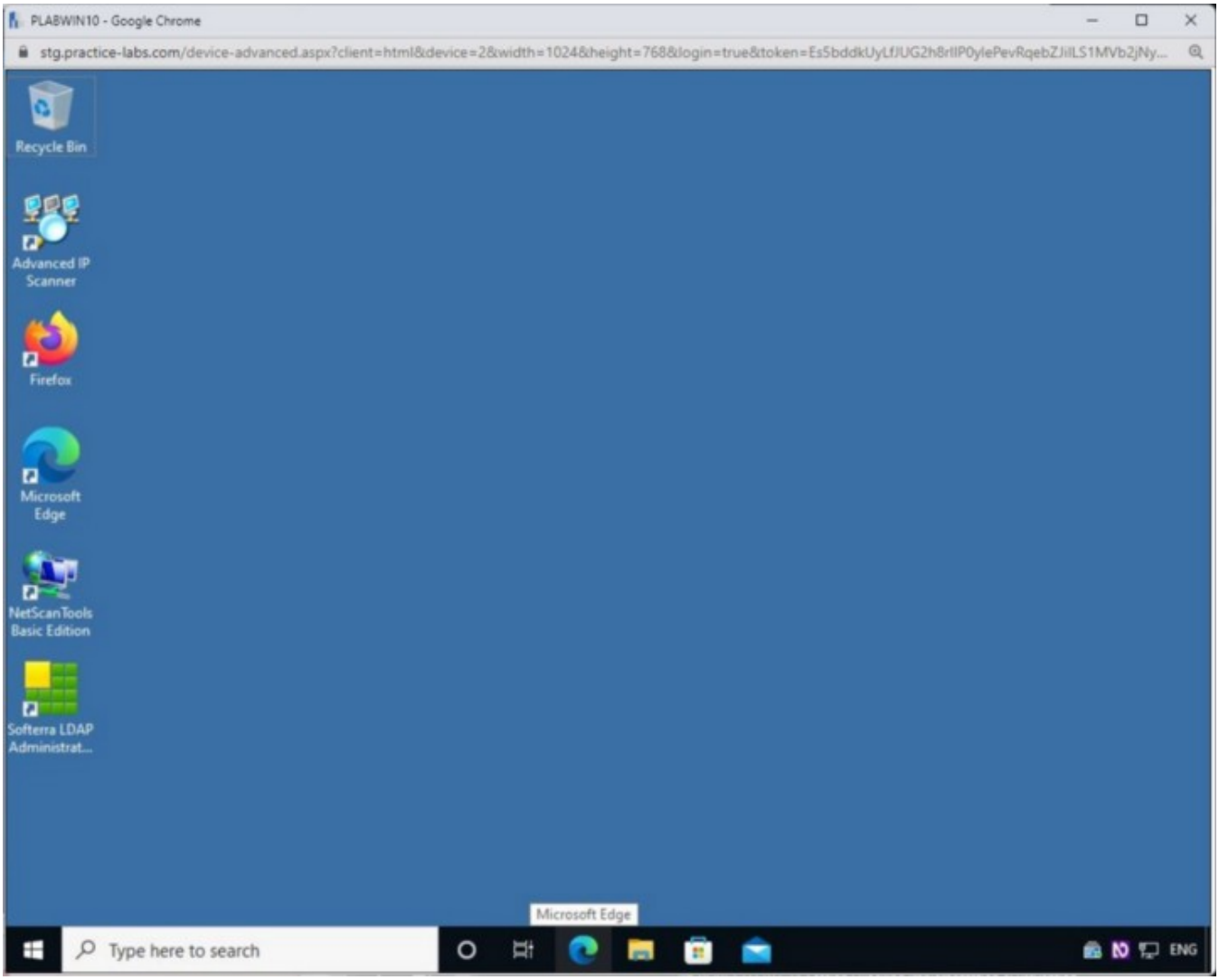
Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10**.



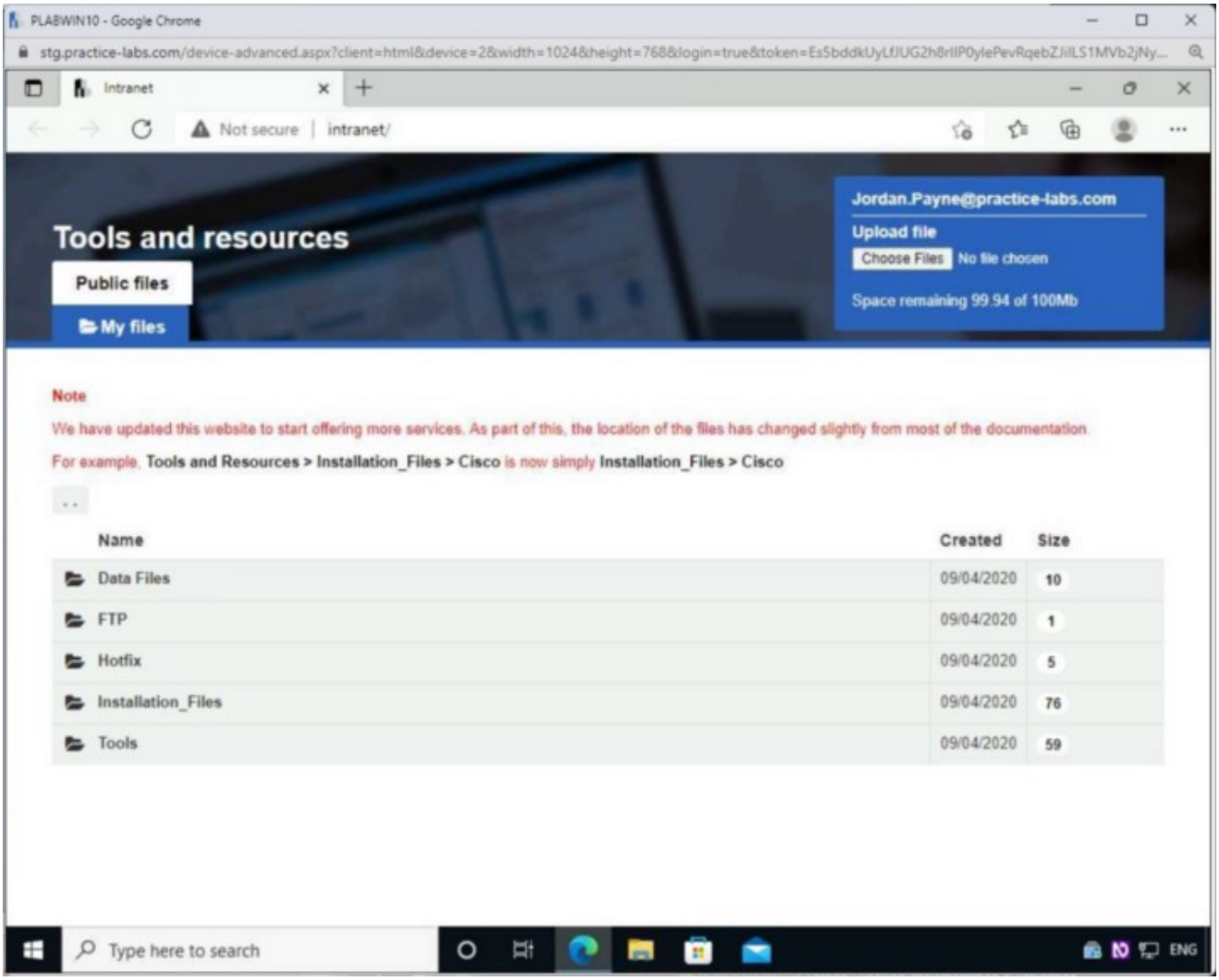
Step 2

From the taskbar, click the **Microsoft Edge** icon.



Step 3

The **Microsoft Edge** window is displayed. In the **Microsoft Edge** window, the default homepage, the **Practice Labs Intranet**, is displayed.

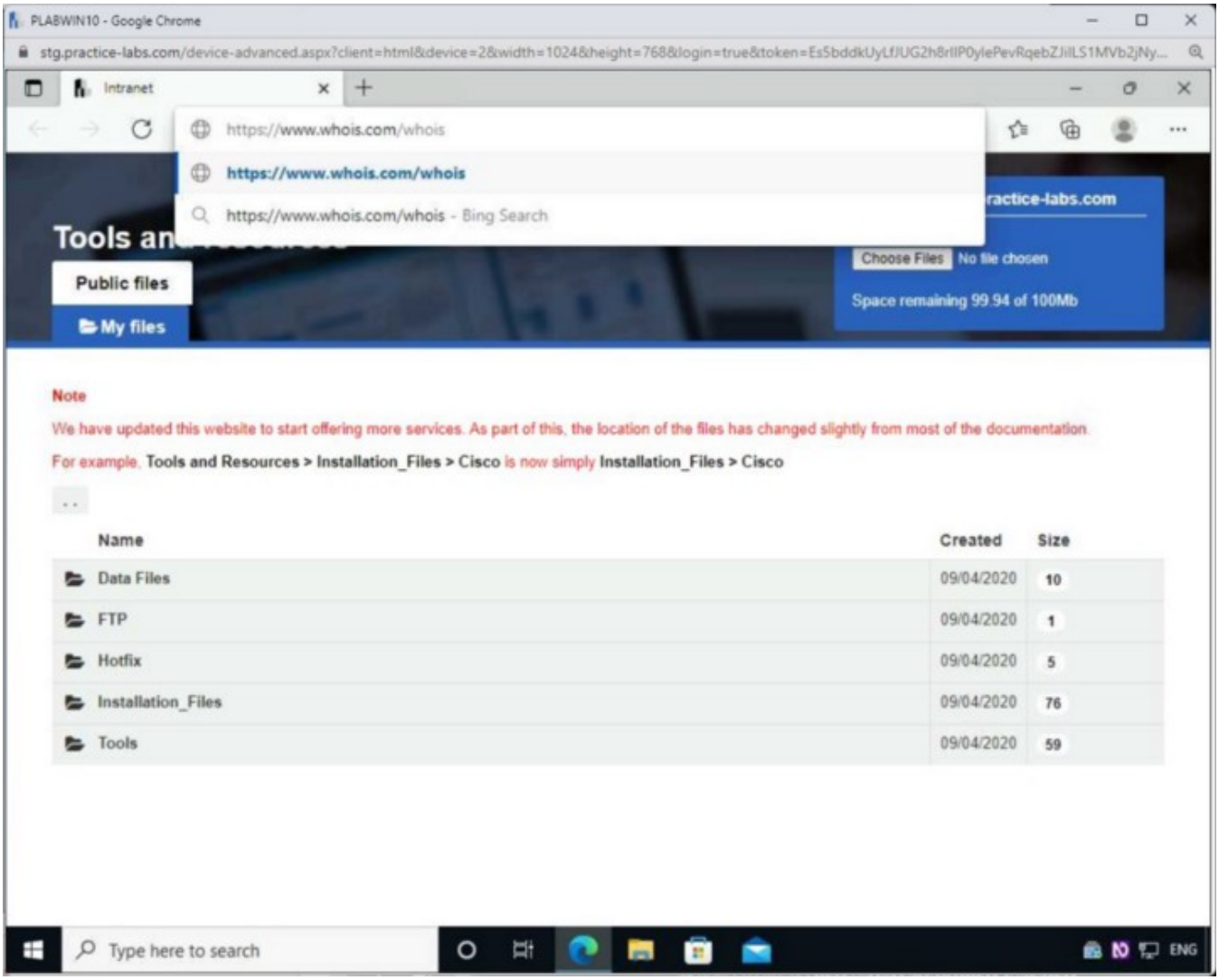


Step 4

In the browser address bar, type the following URL:

`https://www.whois.com/whois`

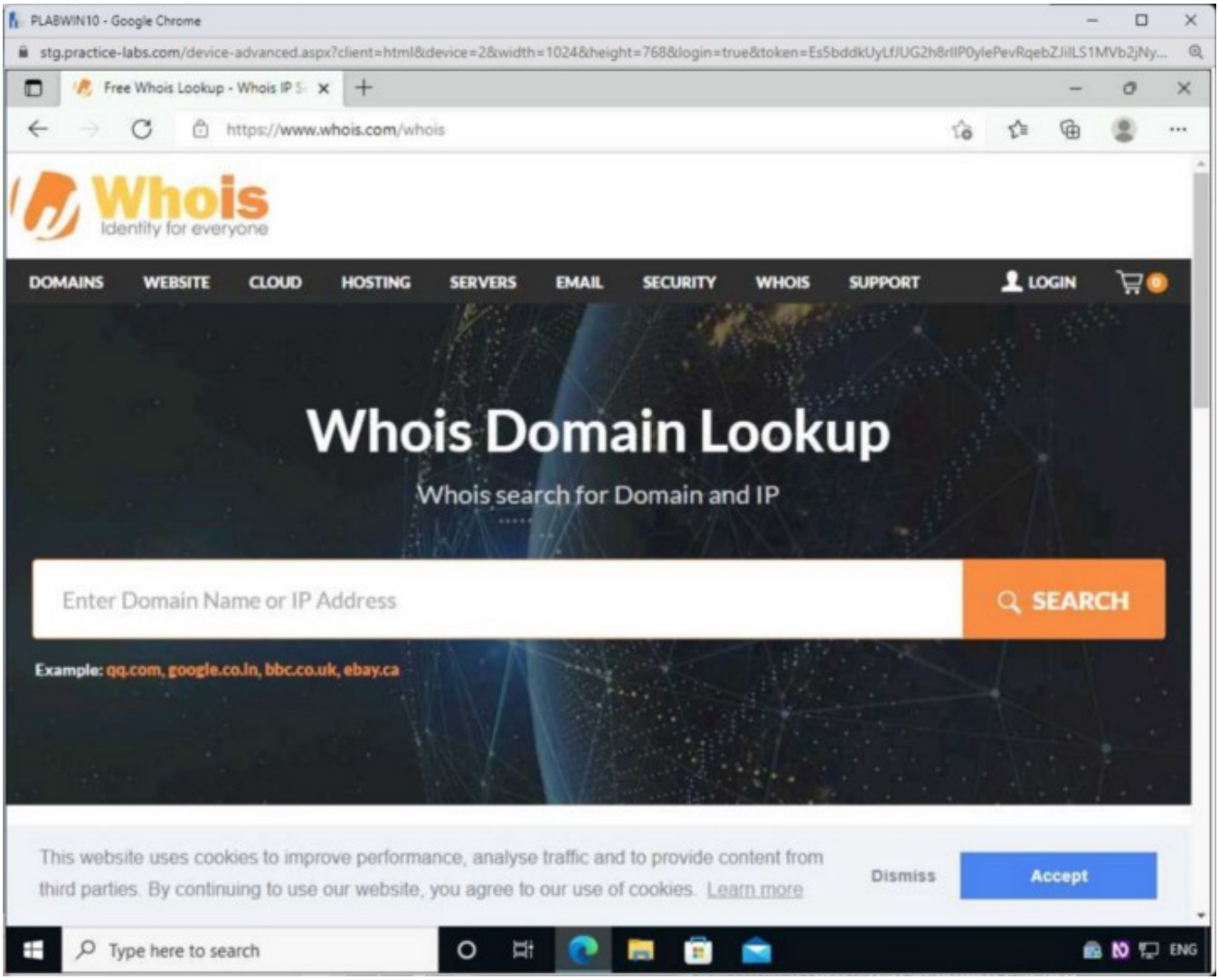
Press **Enter**.



Step 5

The **WHOis.com/whois** website is displayed.

***Note**: Even if you enter http, it will automatically convert to HTTPS. Also, you can get the domain information from the https://whois.icann.org/en website.*

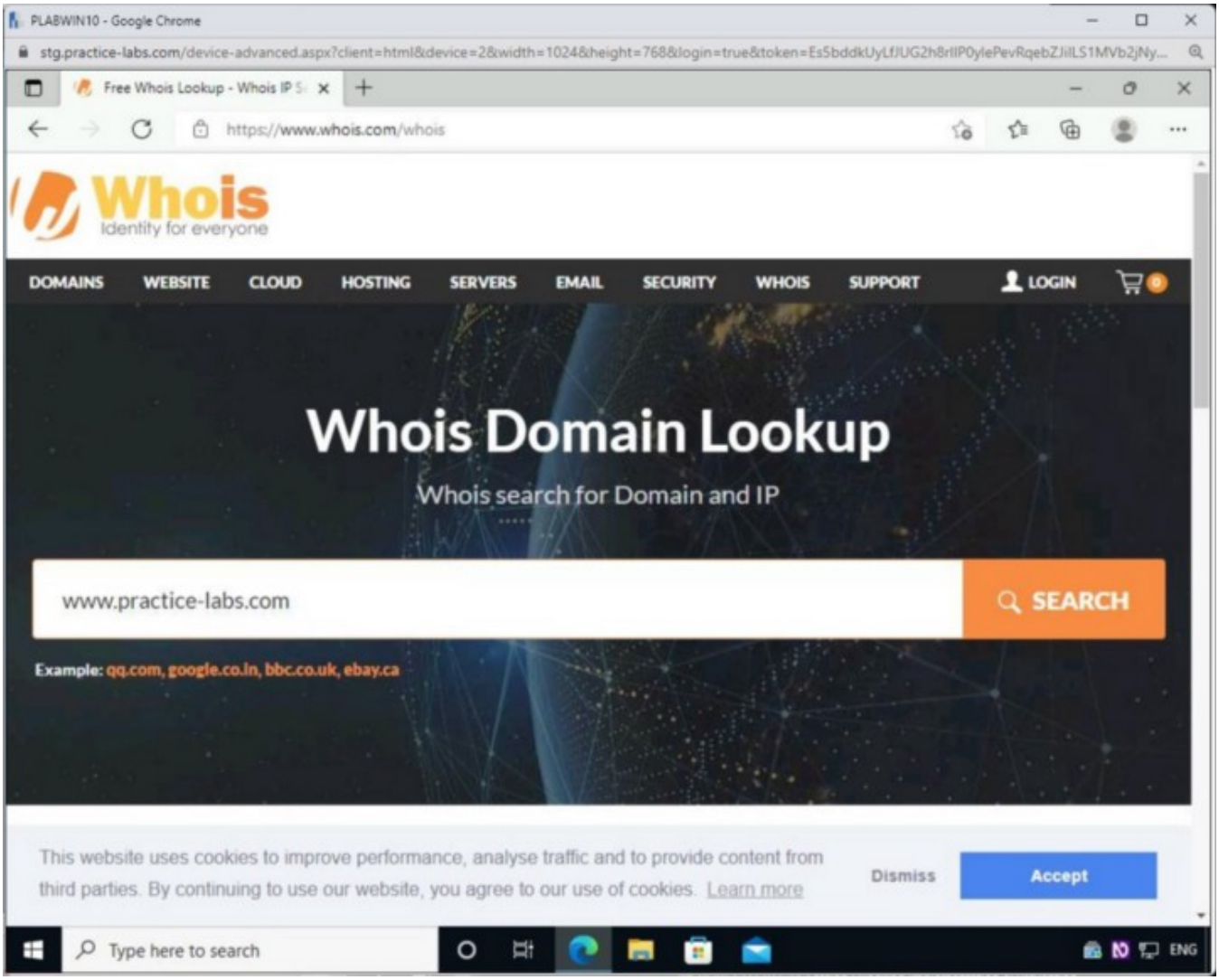


Step 6

In the **Enter Domain Name or IP Address** search textbox, type the following URL:

```
www.practice-labs.com
```

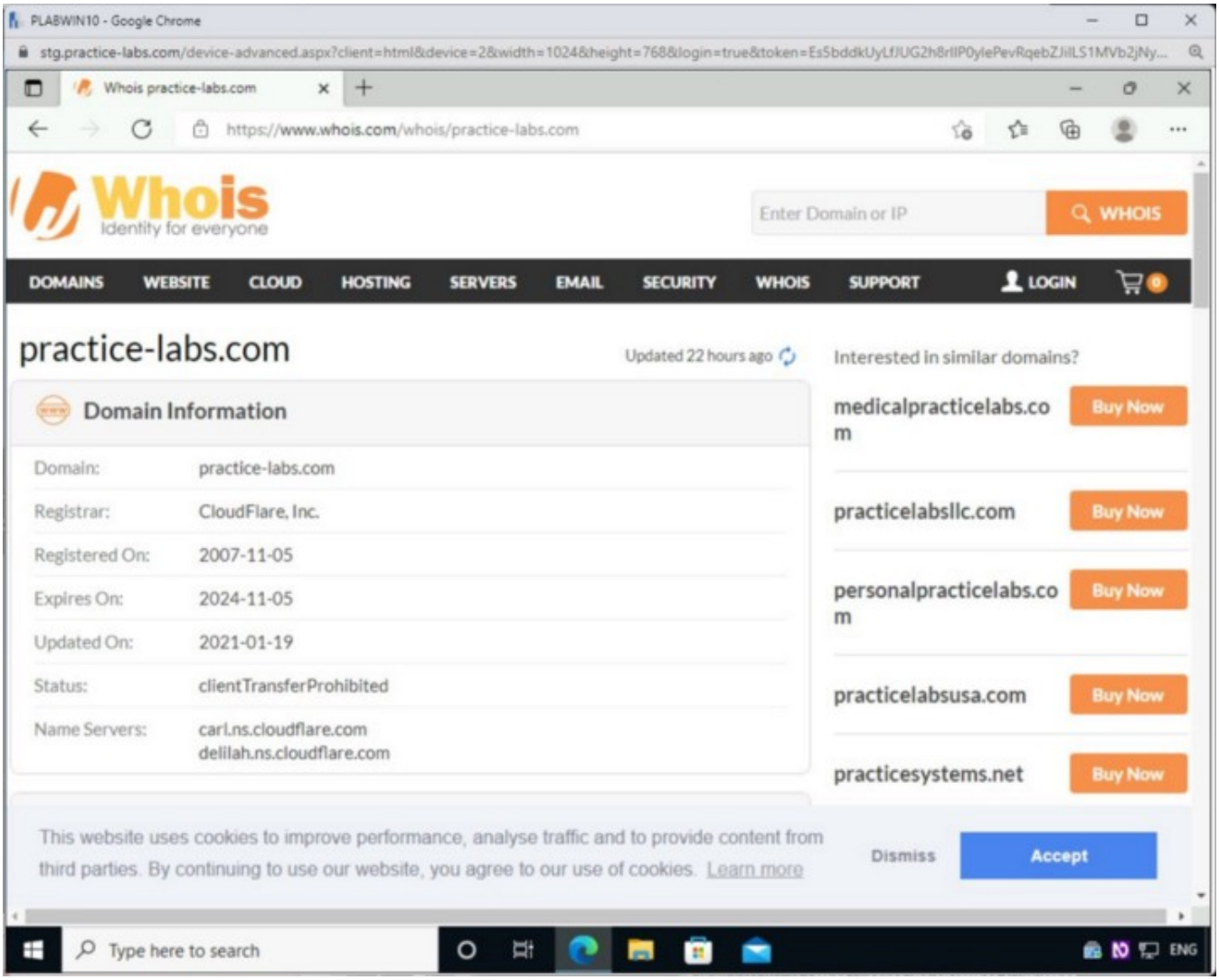
Press **Enter** or click on the **Search** button.



Step 7

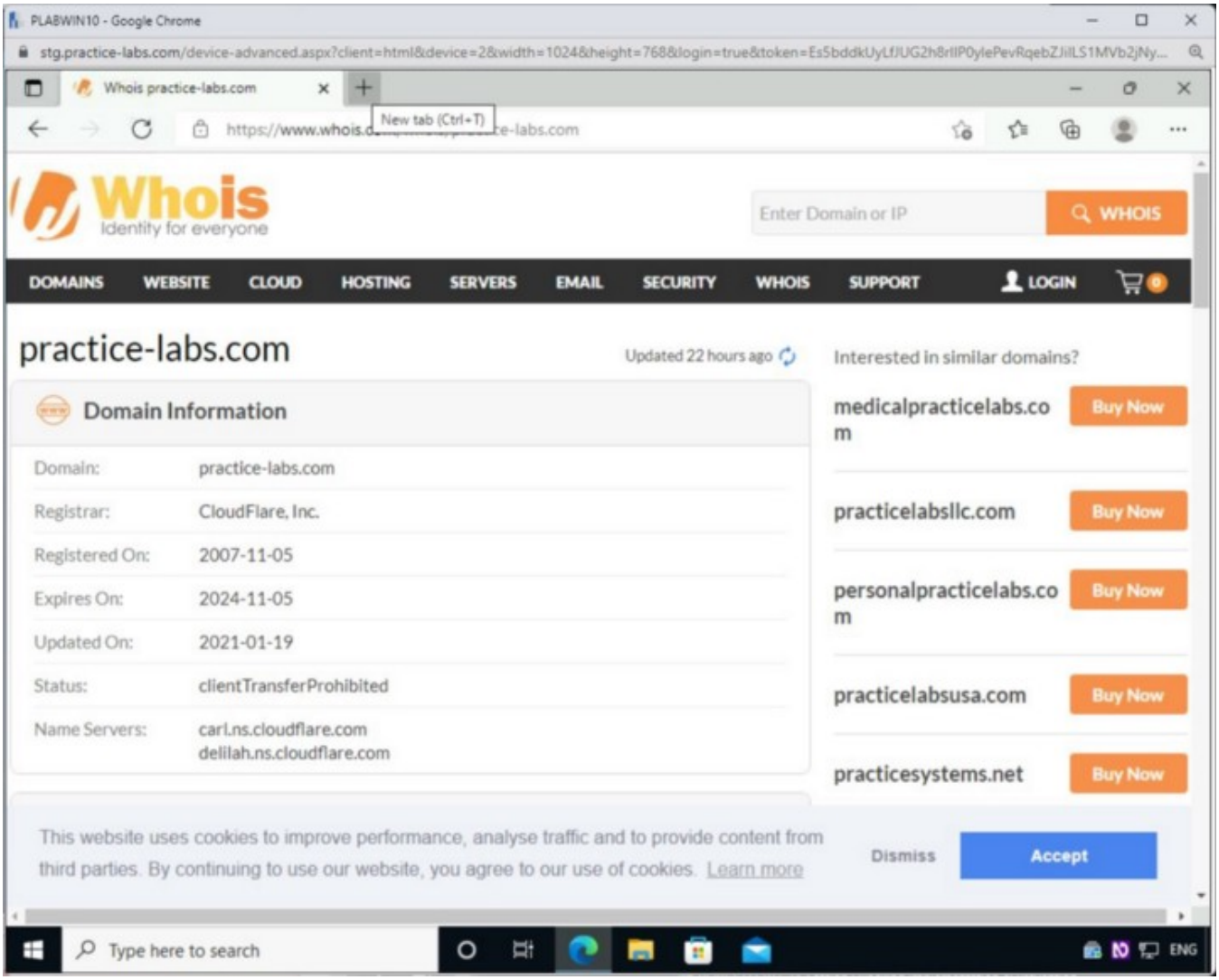
The results are displayed. Notice in the results several key points about the website are displayed. Some of the key ones are:

- Domain name
- Registrar
- Whois server
- Referral URL
- Creation, Updated, and Expiration Date



Step 8

Open another tab in **Microsoft Edge** by clicking the **New tab** (+) icon.

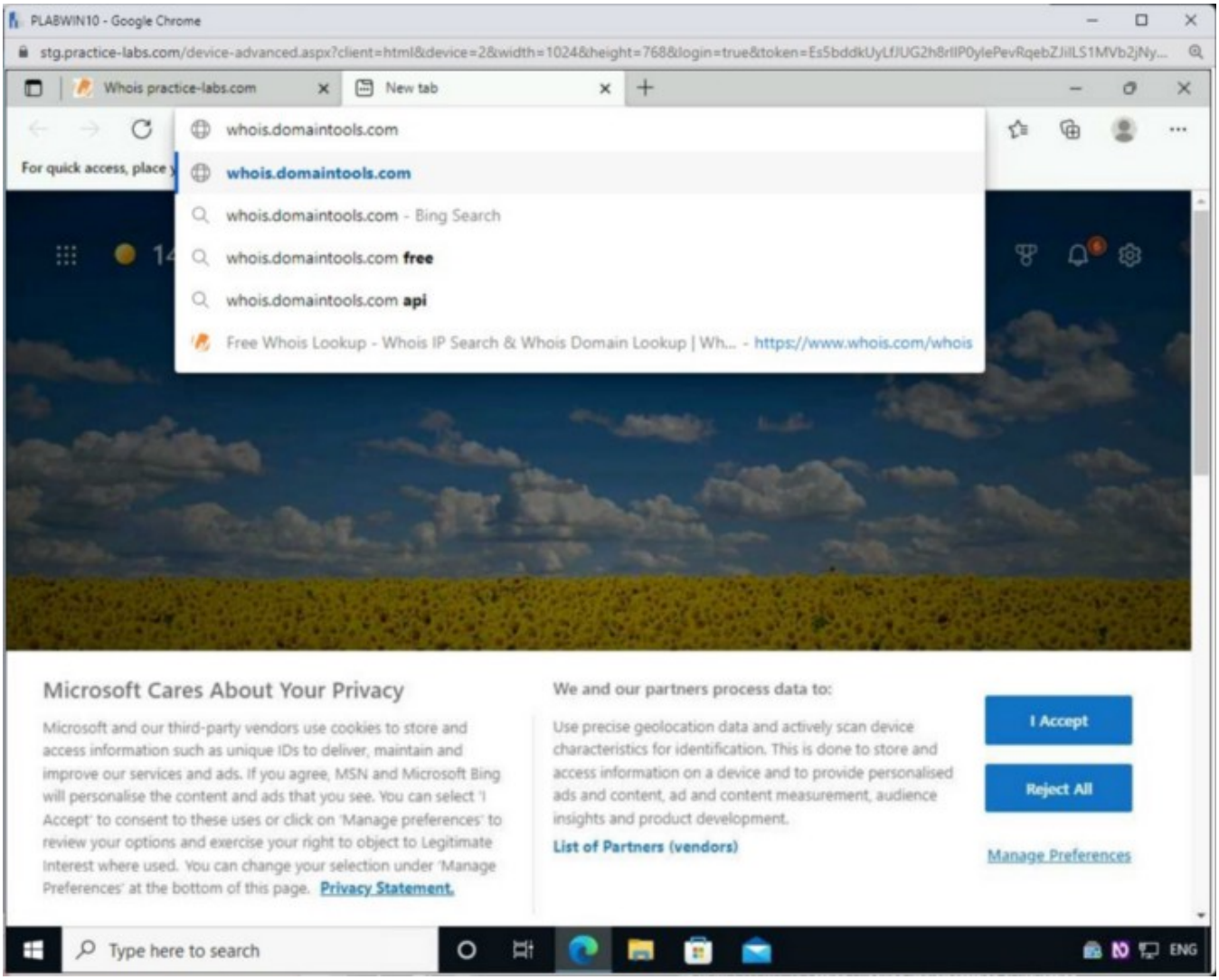


Step 9

In the new tab, type the following URL in the address bar:

```
whois.domaintools.com
```

Press **Enter**.

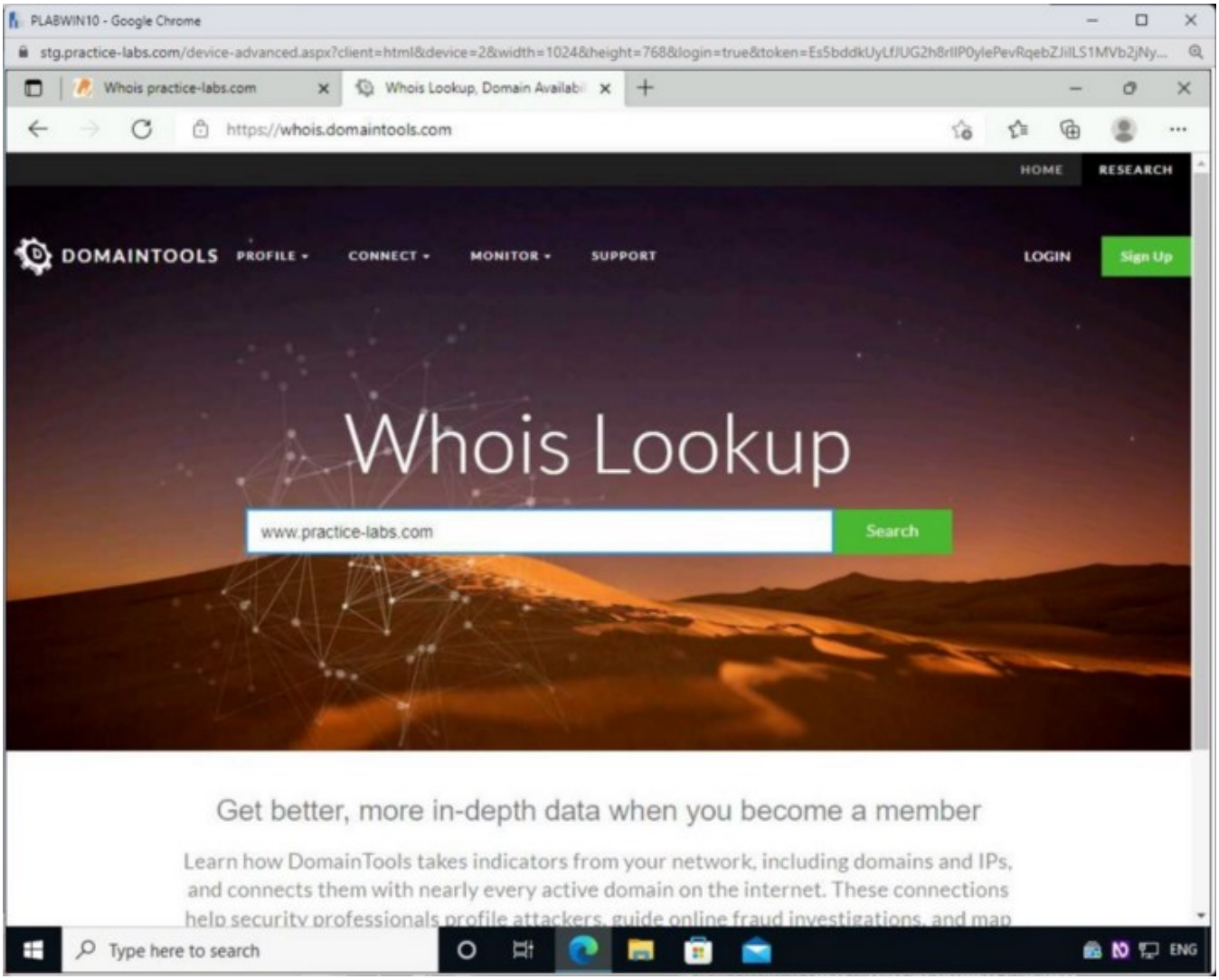


Step 10

The **Whois Lookup** webpage is loaded. In the search text box, type the following URL:

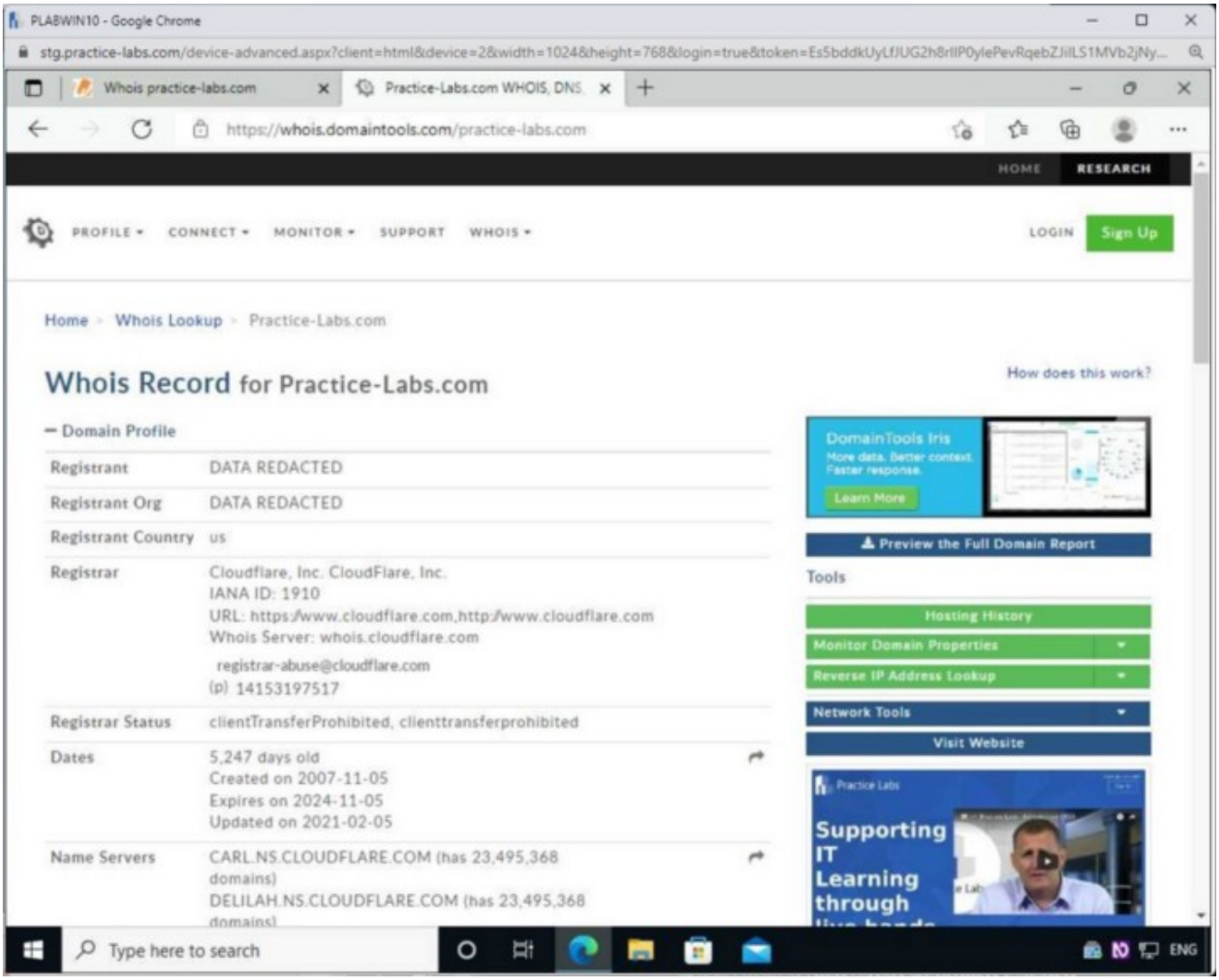
`www.practice-labs.com`

Press **Enter**. Alternatively, click **Search**.



Step 11

The **Whois Record** webpage is loaded.

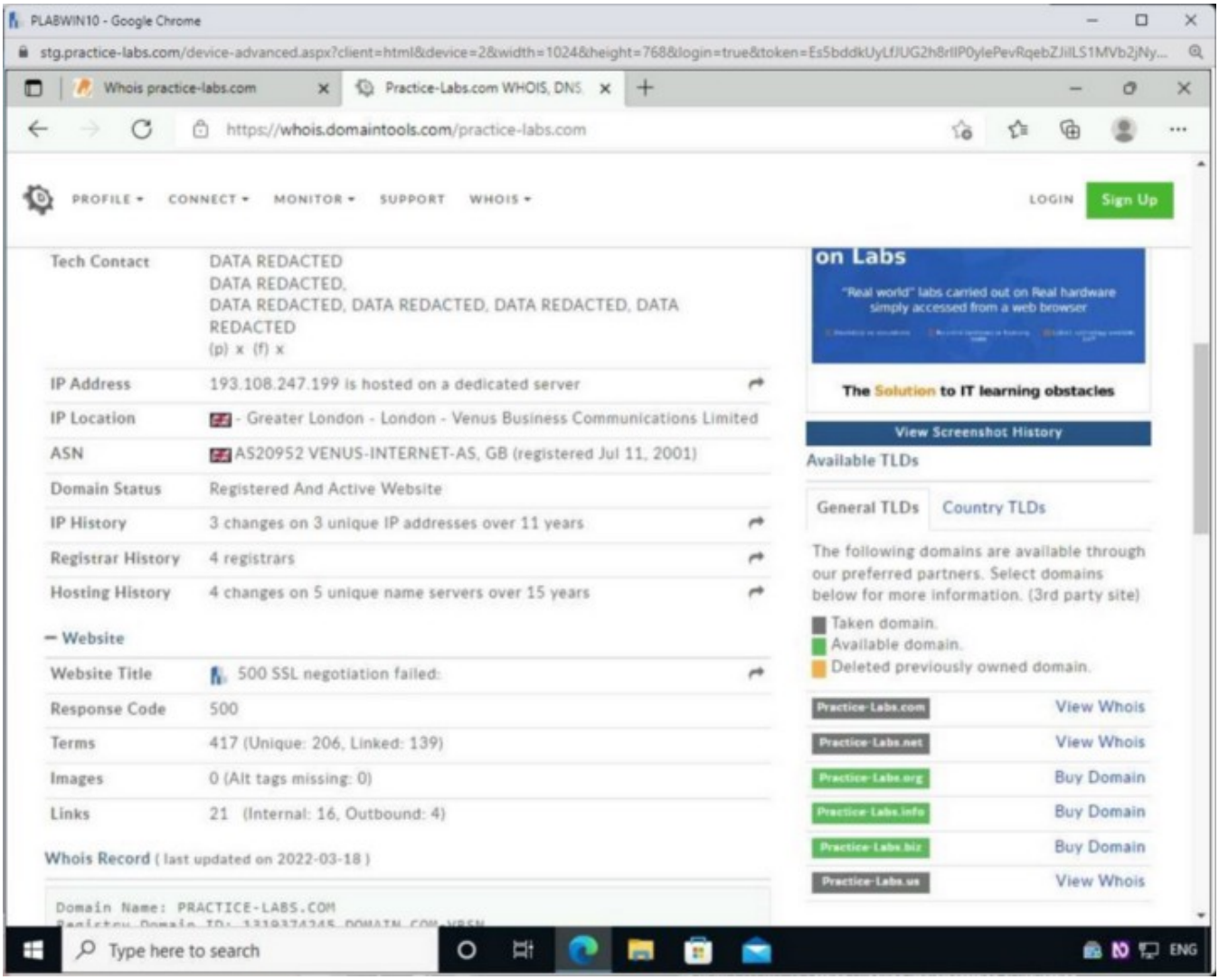


Step 12

You can scroll down to read more about the searched website. Notice that this webpage displays a lot of information compared to the **Whois** Website.

Scroll down to view some of the following information:

- IP address
- IP location
- IP history
- Registrar history
- Domain Status



Exercise 2 — DNS Footprinting

You have collected a lot of information using the Whois database. The next task that you need to perform is to perform DNS footprinting, which helps you gather the following information:

- DNS servers and different types
- DNS records

By performing DNS footprinting, an attacker can gather quite a lot of information about the hosts and systems within the organization.

In this exercise, you will learn to perform DNS footprinting.

Learning Outcomes

After completing this exercise, you will be able to:

- DNS Footprint Using Nslookup

- DNS Footprint using Dnsenum

Your Devices

You will be using the following devices in this lab. Please power these on now.

PLABDC01Domain Controller192.168.0.1/24PLABKALI01Domain MemberWorkstation192.168.0.5/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2019.2 — Linux Kali Workstation192.168.0.5/24

Task 1 — DNS Footprint using Nslookup

nslookup is a network administration command-line tool primarily used to query the Domain Name System (DNS). Using this tool, you can obtain the domain name or IP address mapping.

- **A**: provides the IP address of the specified domain
- **AAAA**: defines the hostname to an IPv6 address
- **Canonical name (CNAME)**: sets an alias name for a domain
- **Mail exchange (MX)**: used for message routing
- **Start of Authority (SOA)**: provides the administrative information that includes administrator's name, domain updation time, refresh time, and time-to-live
- **Pointer (PTR)**: is used for reverse DNS lookup, IP address to domain name lookup
- **Text (TXT)**: has two different records:
- **TXT (SPF)**: specifies a list of authorized host names or IP addresses from which a mail can trigger in a domain

- **TXT (DKIM)**: is Domain Keys Identified Mail. It provides authentication of mail sent and received by the same messaging server
- **Service (SRV)**: is a service location record specifying a port number along with an IP address
- **Name server (NS)**: defines the domain name for the DNS server

In this task, you will perform DNS footprinting using Nslookup.

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABKALI01**.

Log in using the following credentials:

Username:

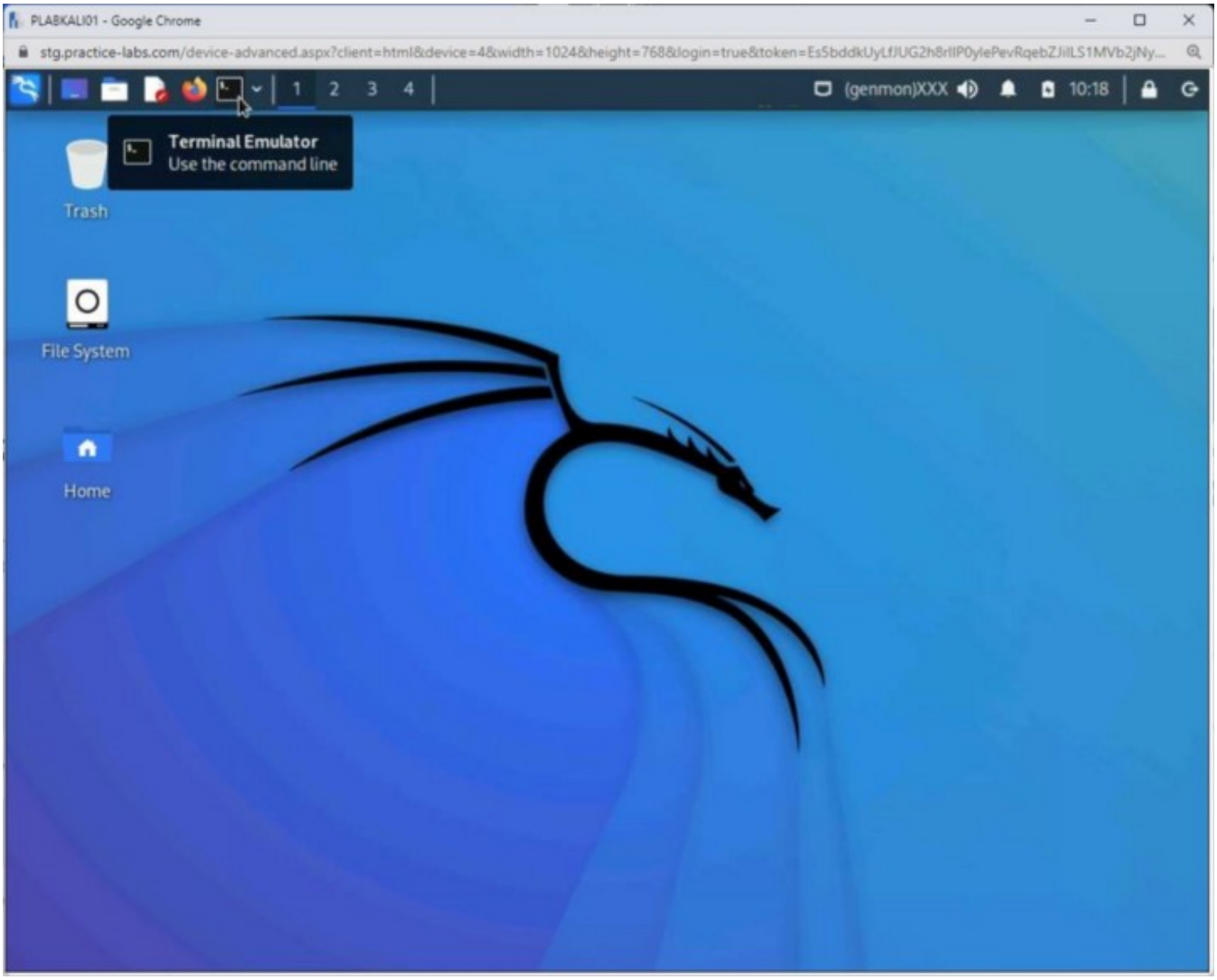
```
root
```

Password:

Password

The desktop of **PLABKALI01** is displayed.

Open a new terminal window by clicking the **Terminal Emulator** icon on the taskbar.

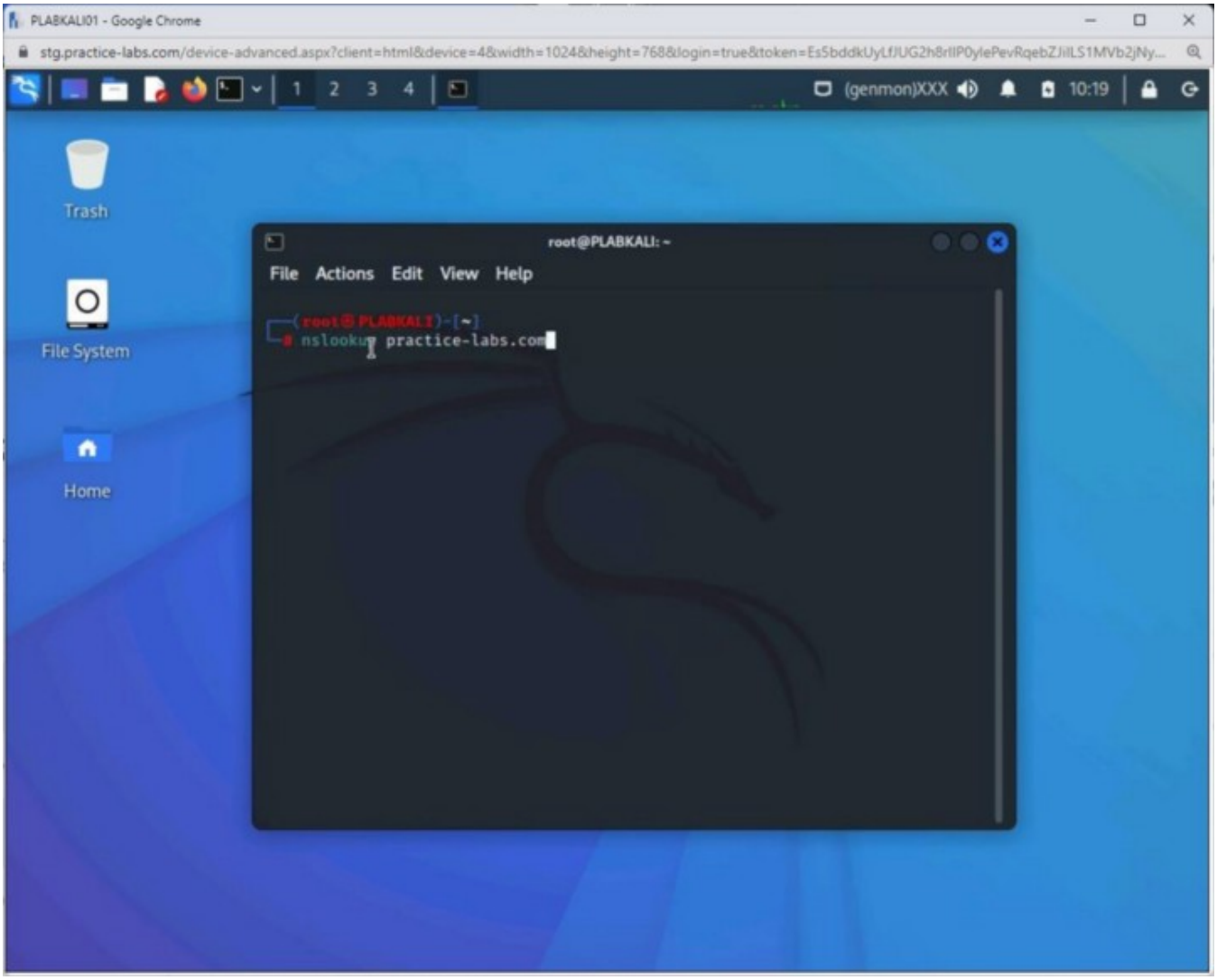


Step 2

The terminal window is displayed. Enter the following command:

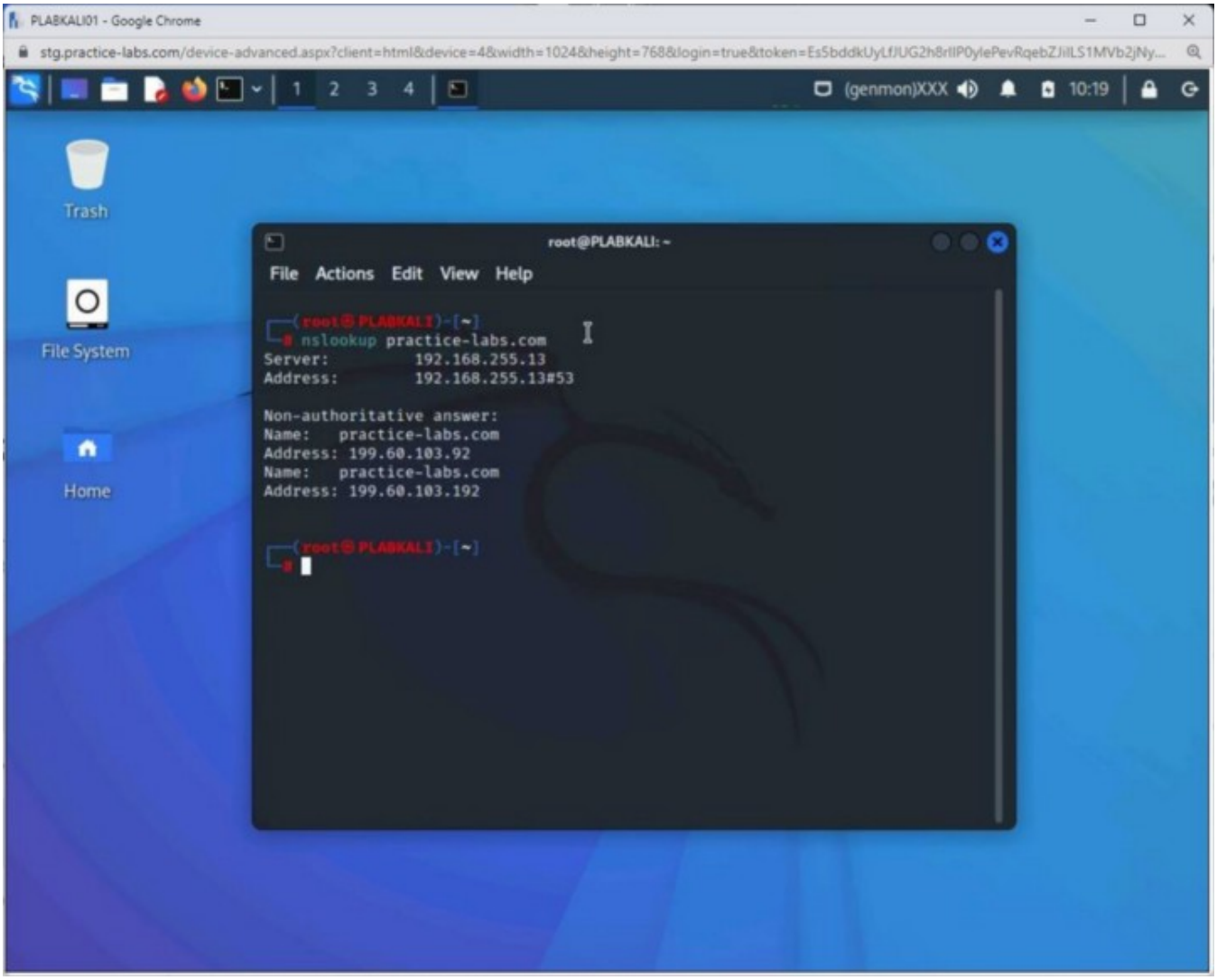
```
nslookup practice-labs.com
```

Press **Enter**.



Step 3

The first two output lines specify the server to which the request was directed. This is the default server for DNS name resolution. The second section provides the name of the record and its corresponding IP address. Note that the IP address for the domain, **practicelabs.com,** is displayed.

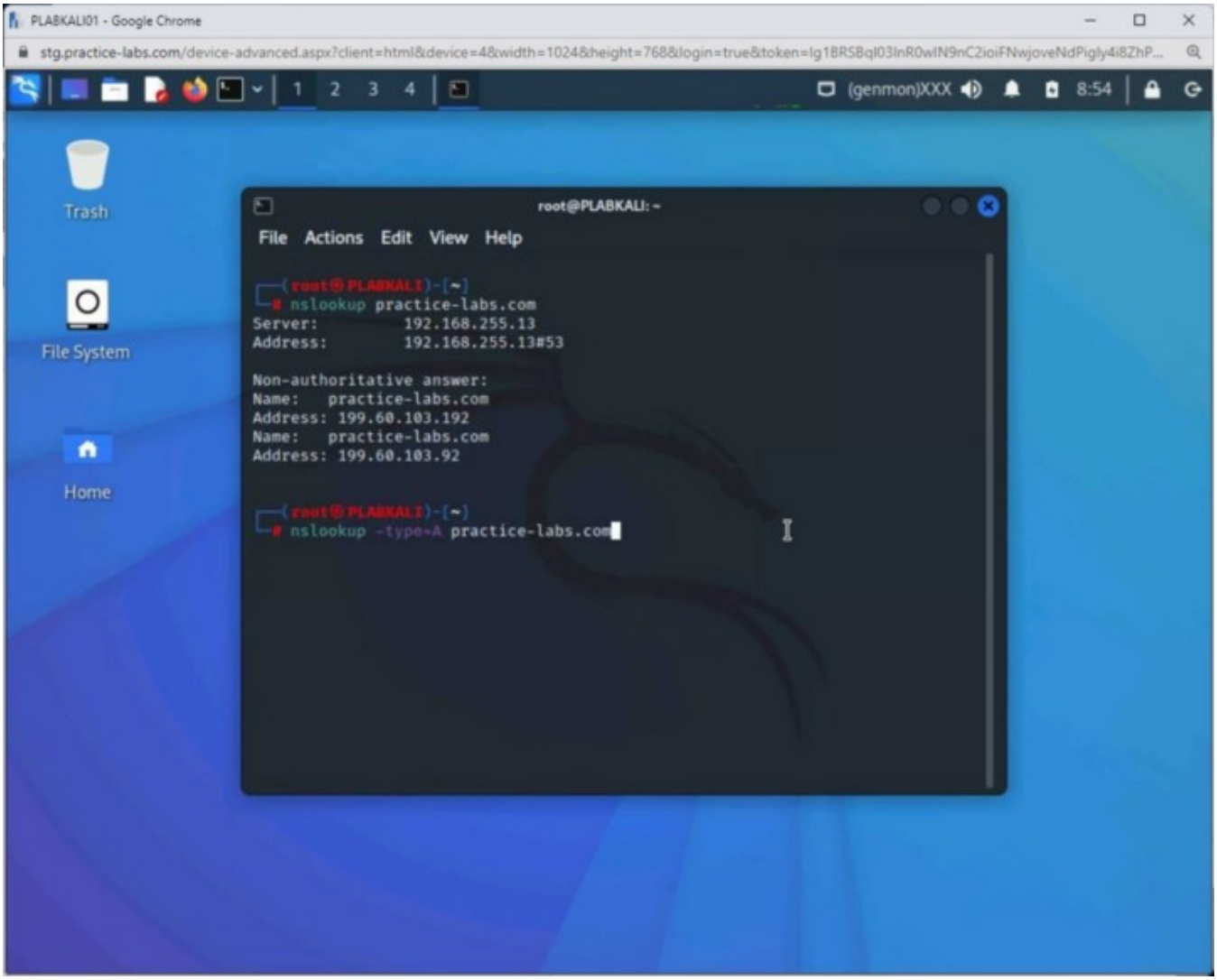


Step 4

You can also check for a specific record. For example, to check for any **A** records for **practicelabs.com**, type the following command:

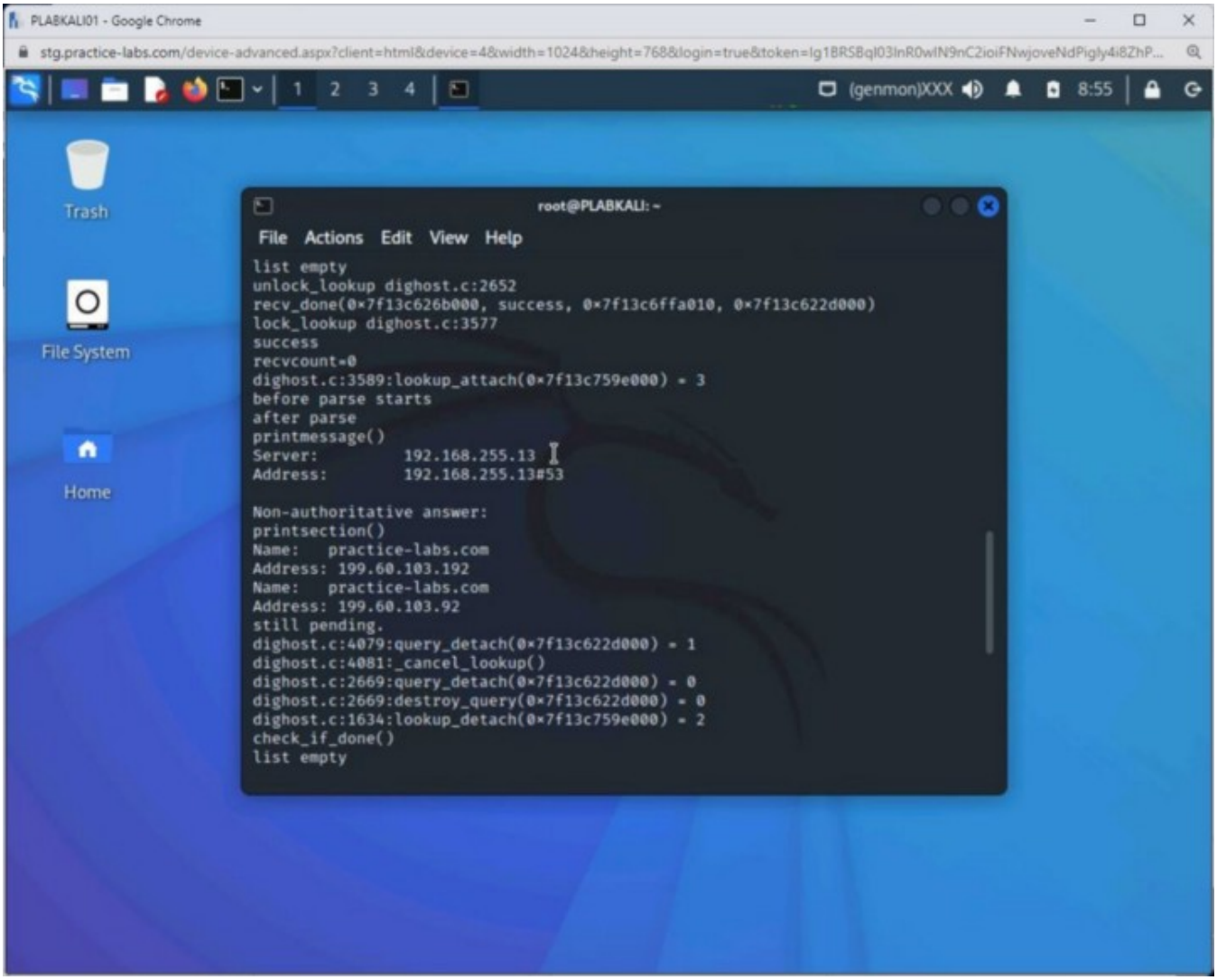
```
nslookup -type=A practice-labs.com
```

Press **Enter**.



Step 5

Note that the IP address for the domain, **practicelabs.com**, is displayed.

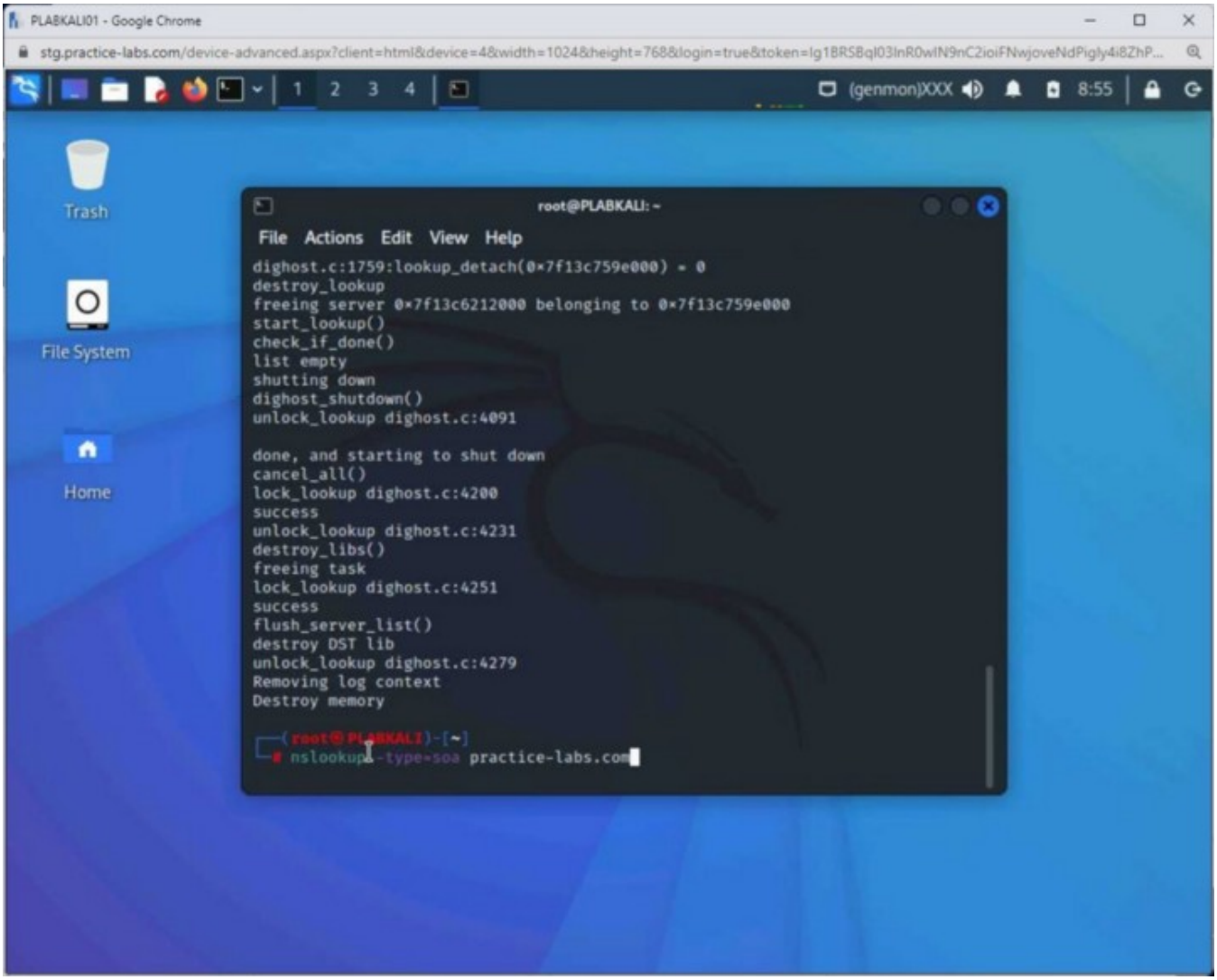


Step 6

You can use the **-type=soa** option to tell **nslookup** to display the authoritative (primary) name server. Type the following command:

```
nslookup -type=soa practice-labs.com
```

Press **Enter**.



Step 7

Clear the terminal with the following command:

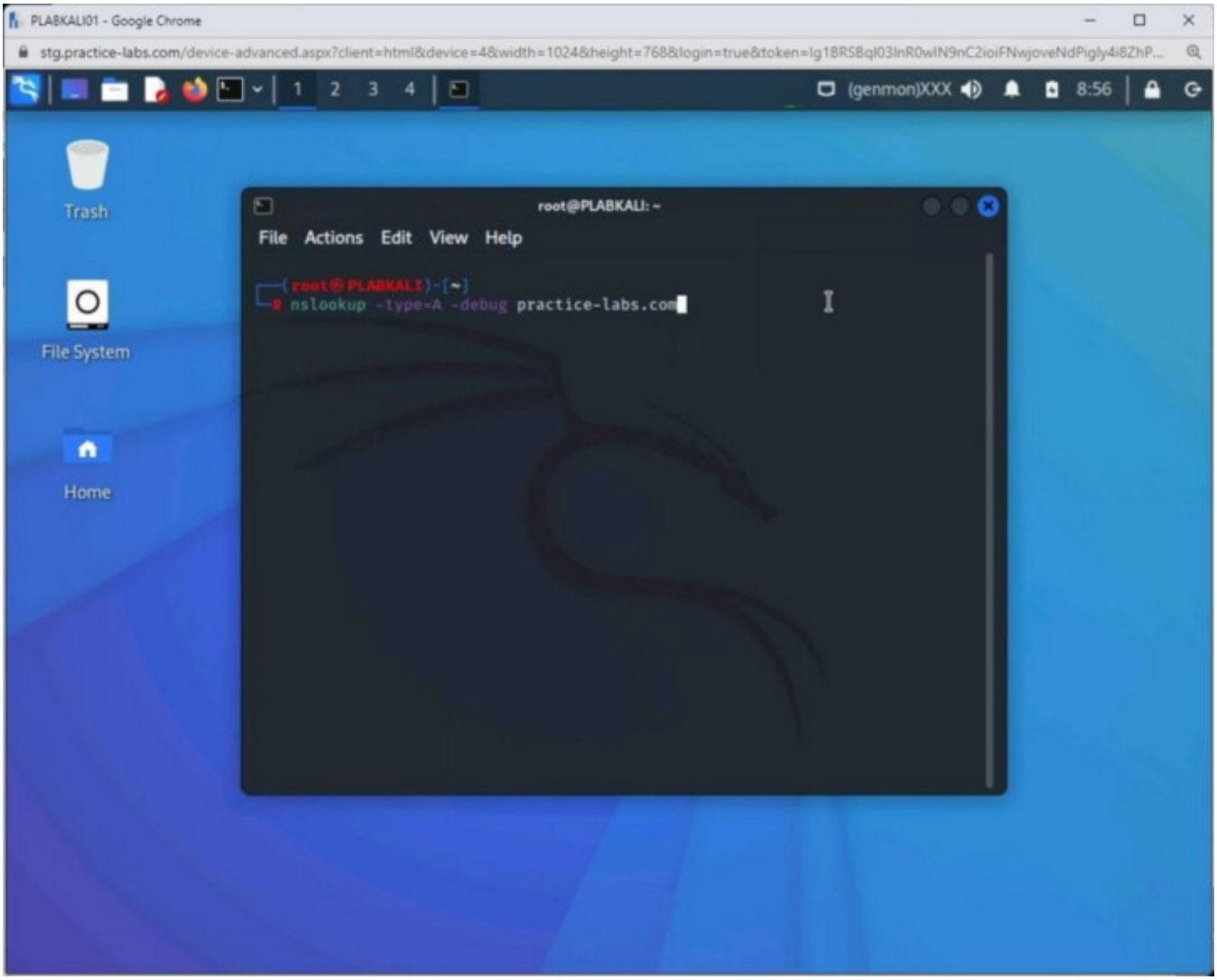
```
clear
```

Press **Enter**.

You can also verify how long a record is cached using the debug parameter. Type the following command:

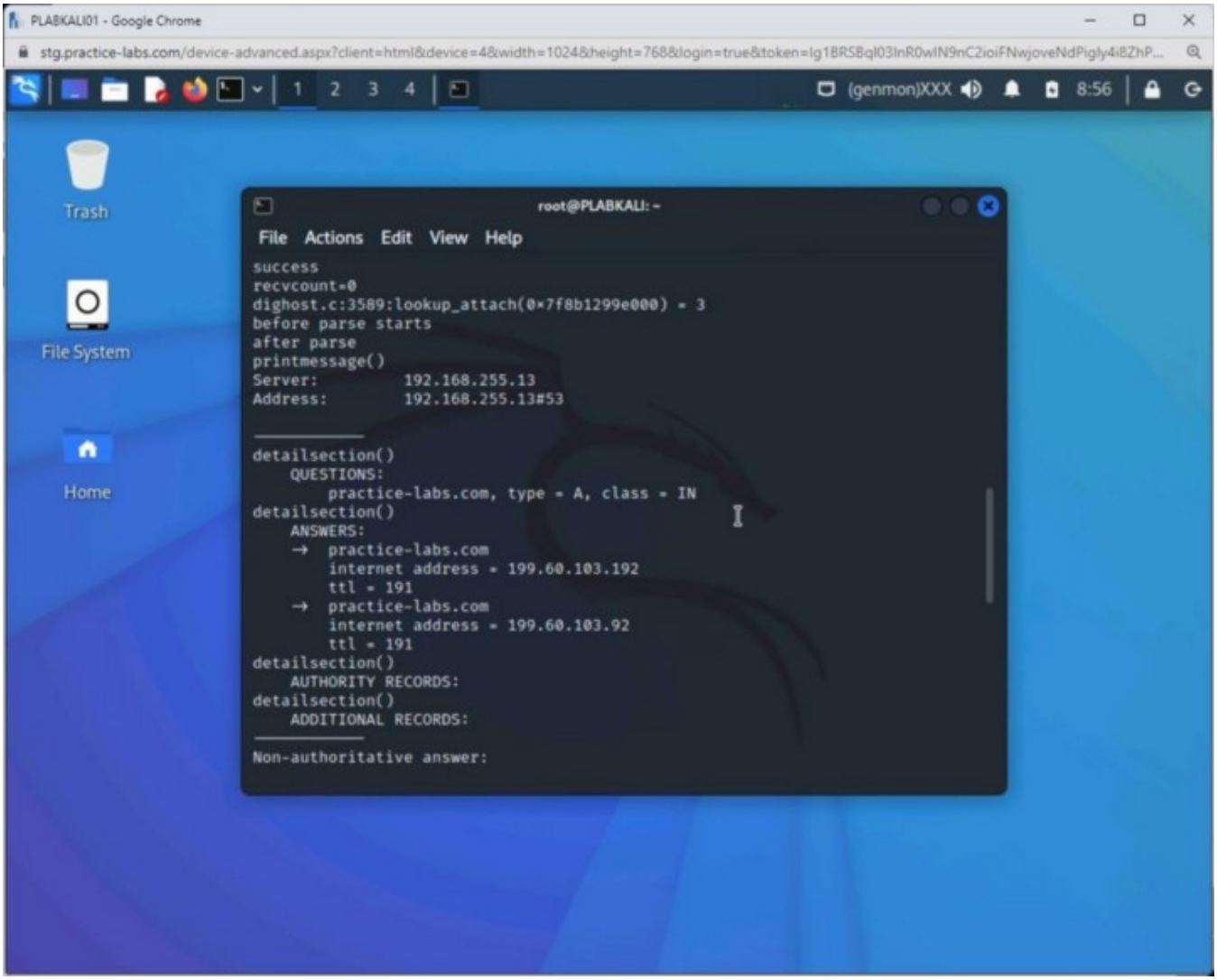
```
nslookup -type=A -debug practice-labs.com
```

Press **Enter**.



Step 8

Note that there is no indication of when the records will expire, as the internal server does not provide complete details.



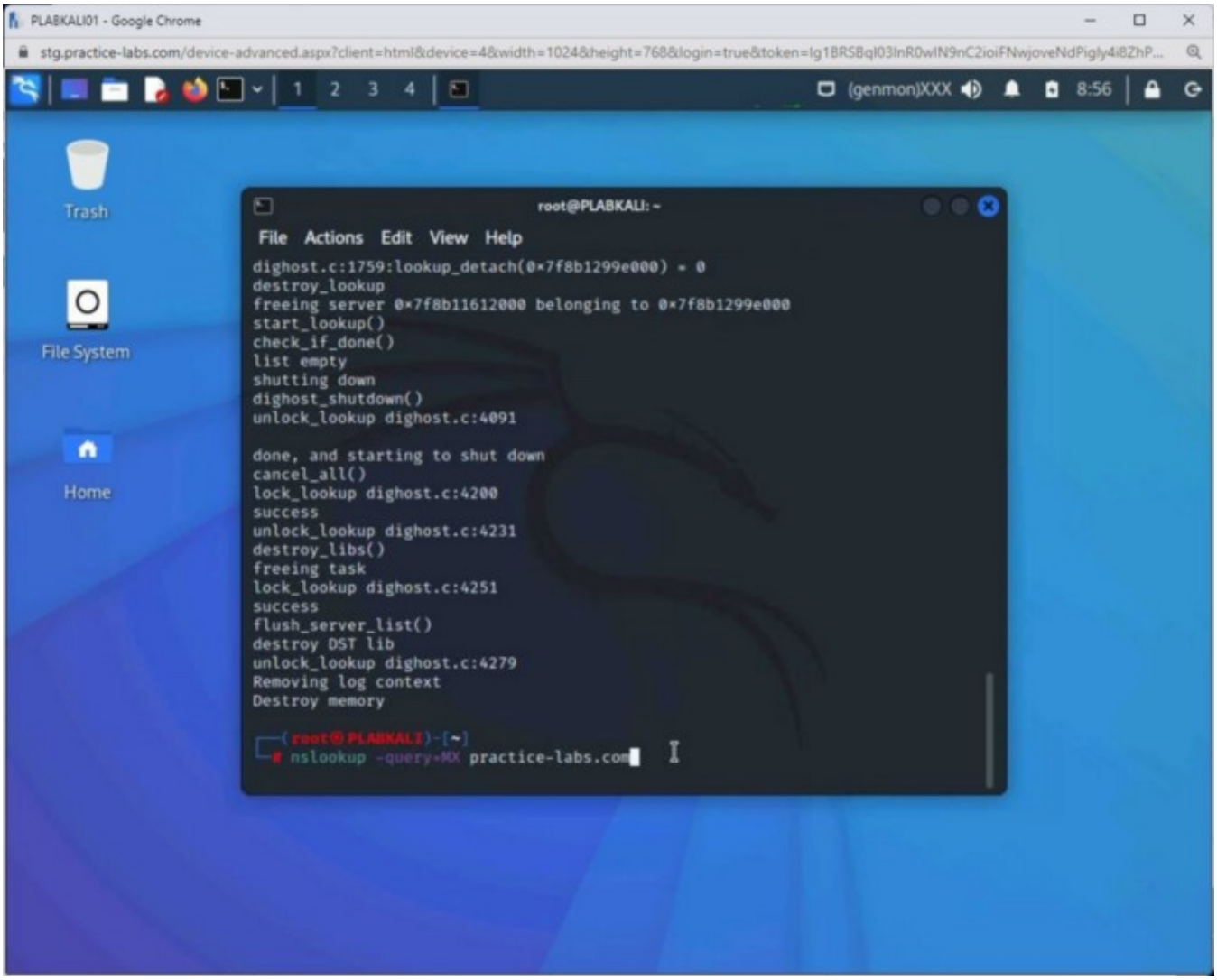
Step 9

You can also use the **MX** record to map a domain name to a list of mail exchange servers for that domain. For example, the **MX** record provides the details of the mail server to which all the E-mails are sent for the **practicelabs.com** domain. Type the following command:

```
nslookup -query=MX practicelabs.com
```

Press **Enter**.

Since there is no mail server for this domain, notice that this command is failing.



Step 10

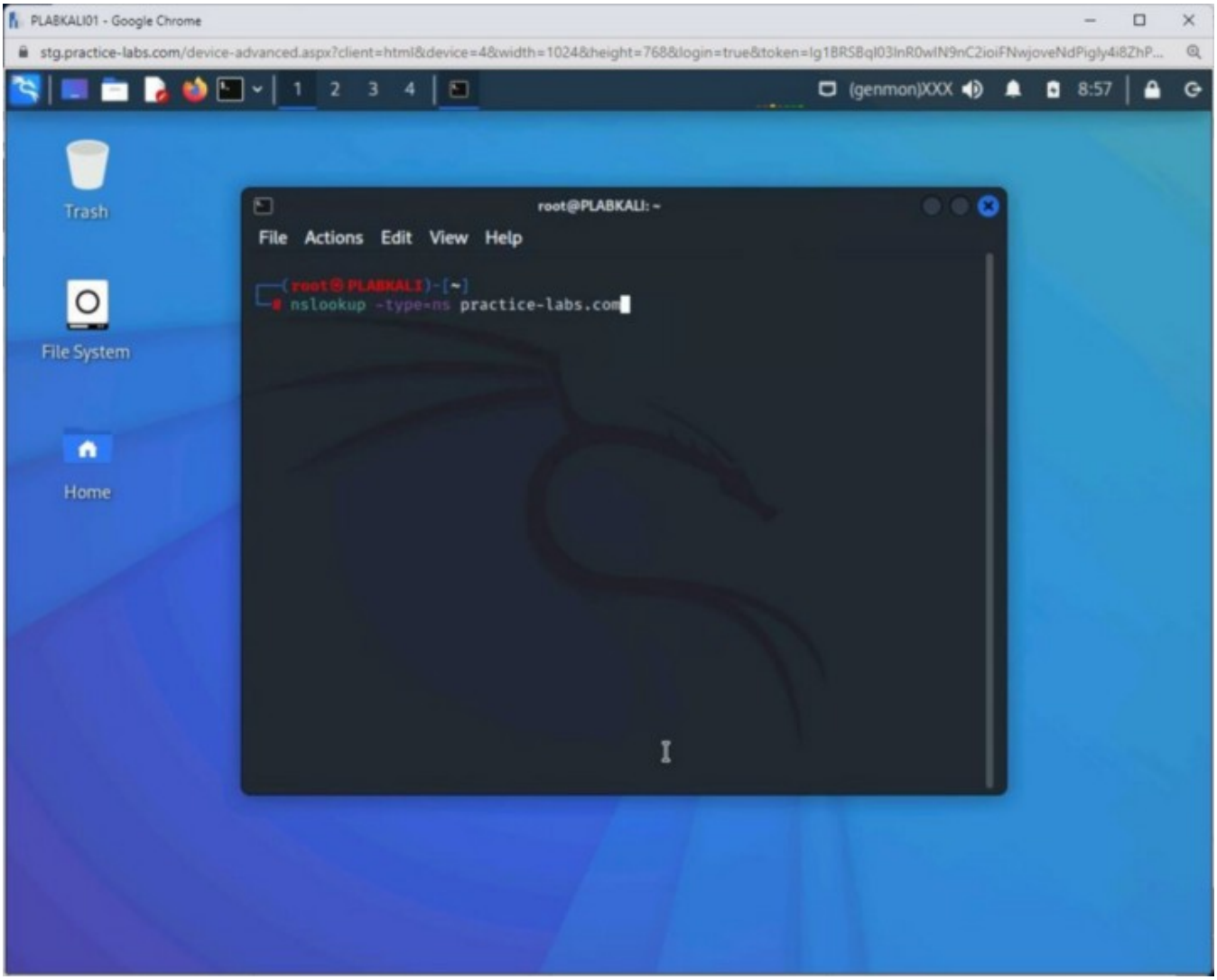
Clear the screen by entering the following command:

```
clear
```

The NS record maps a domain name to a list of the DNS servers that are authoritative for this domain. Type the following command:

```
nslookup -type=ns practice-labs.com
```

Press **Enter**. Since there is only one DNS server, it is now listed as the response to the command.

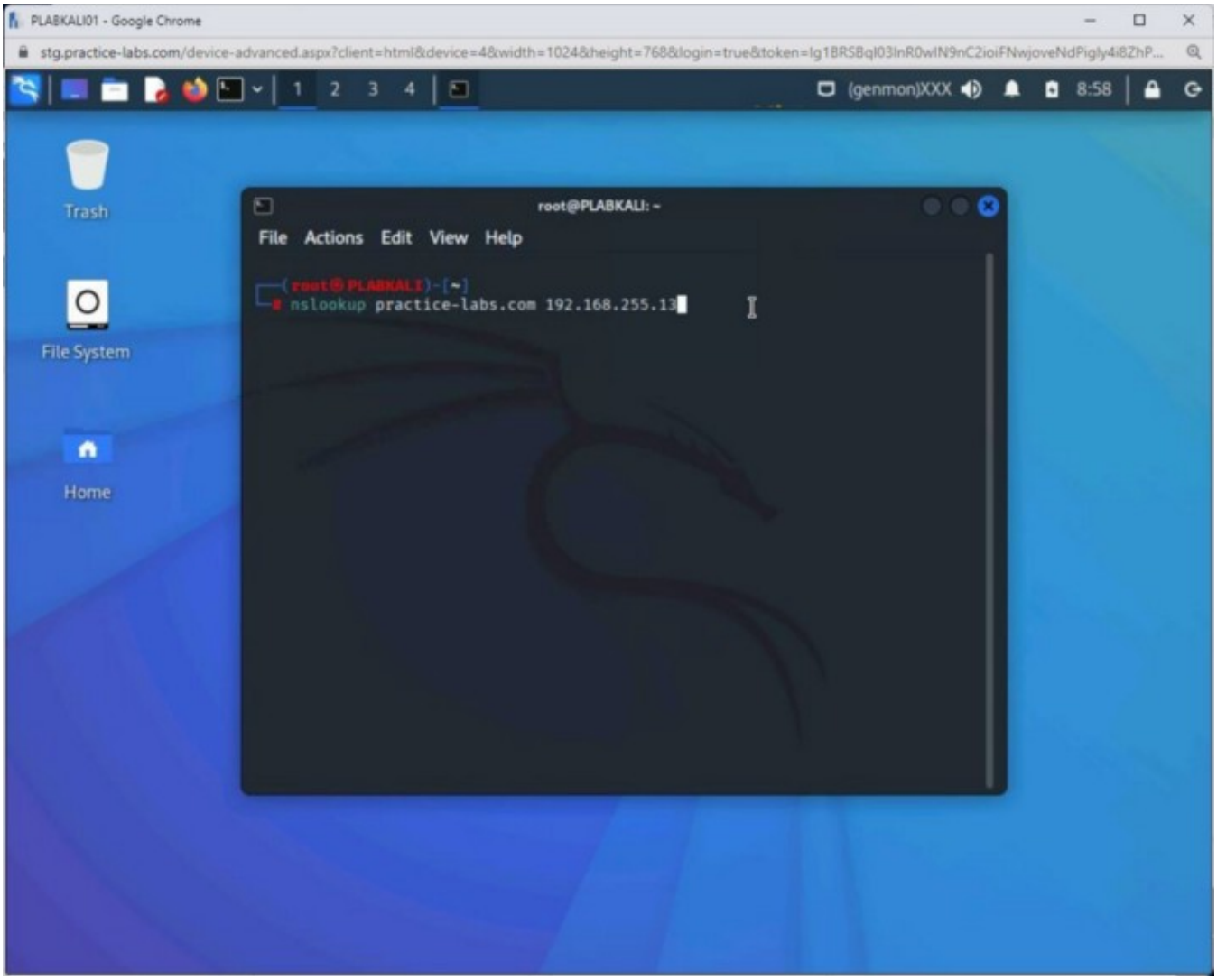


Step 11

You can perform domain name resolution using a specific DNS server. Type the following command:

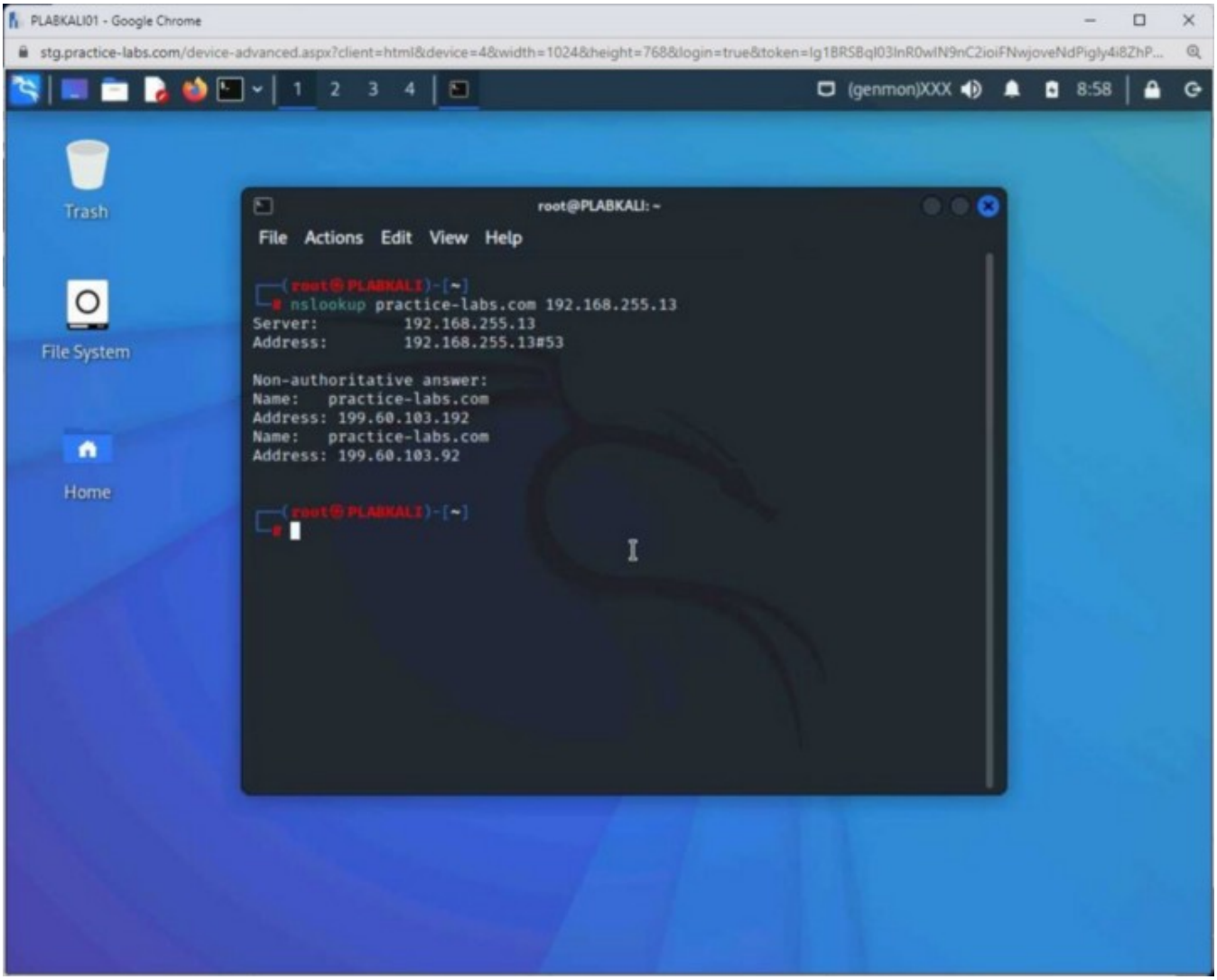
```
nslookup practicelabs.com 192.168.255.13
```

Press **Enter**.



Step 12

Notice the listed details as the output of this command.



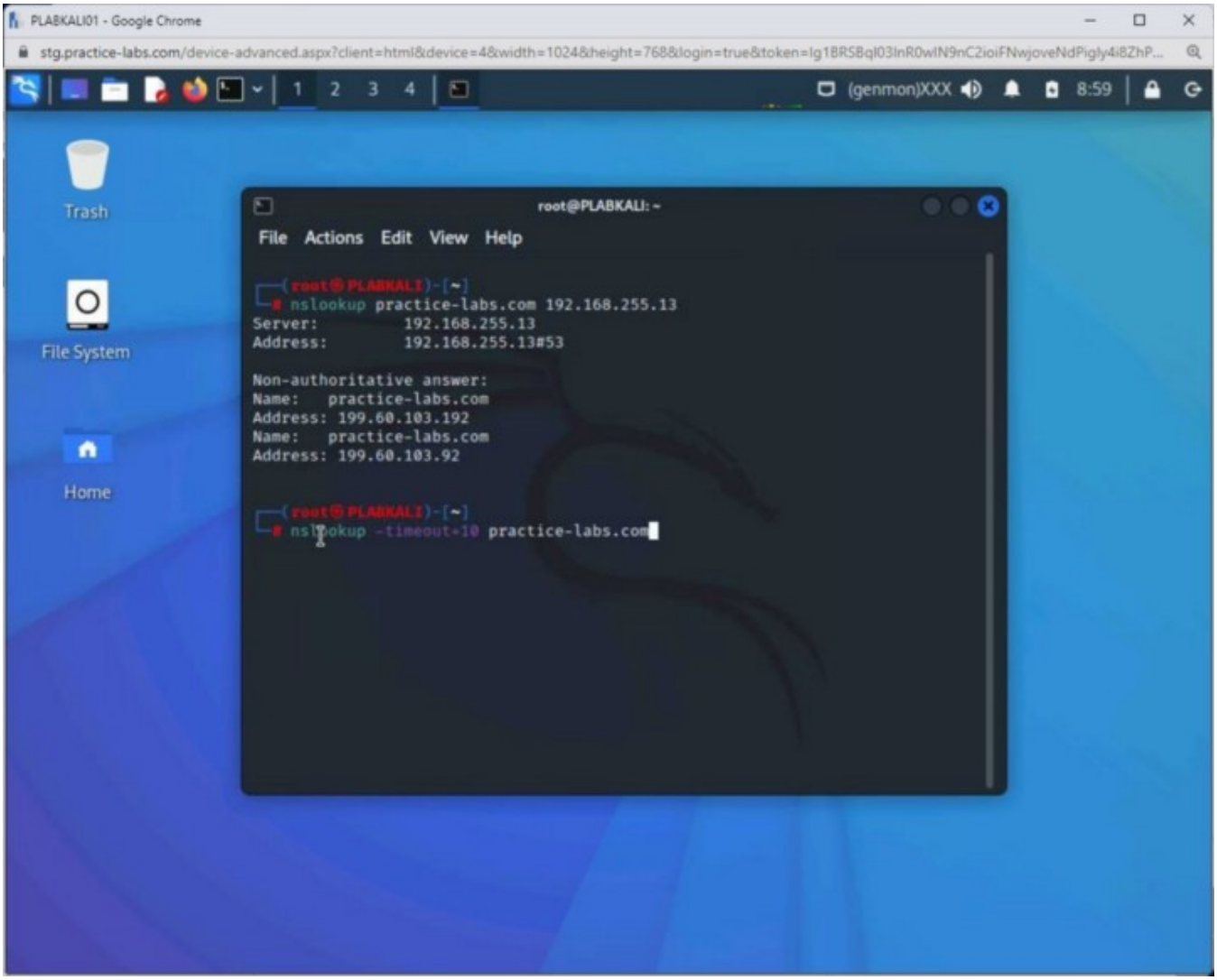
Step 13

You can also change the default timeout to wait for a reply using the **-timeout** option. Type the following command:

```
nslookup -timeout=10 practicelabs.com
```

Press **Enter**.

Observe the output of the command.



Step 14

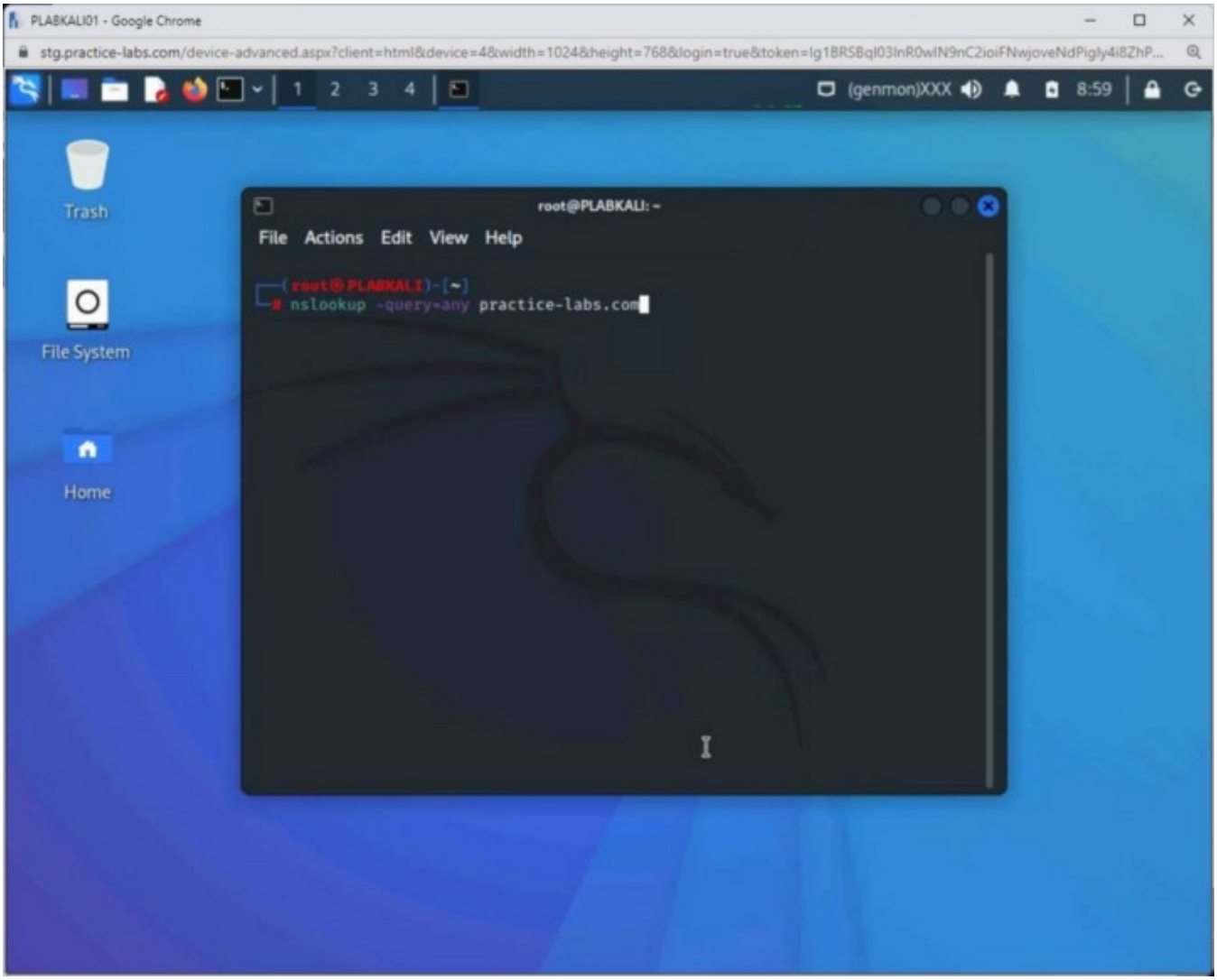
Clear the screen by entering the following command:

```
clear
```

You can view all the available DNS records using the **-query=any** option. Type the following command:

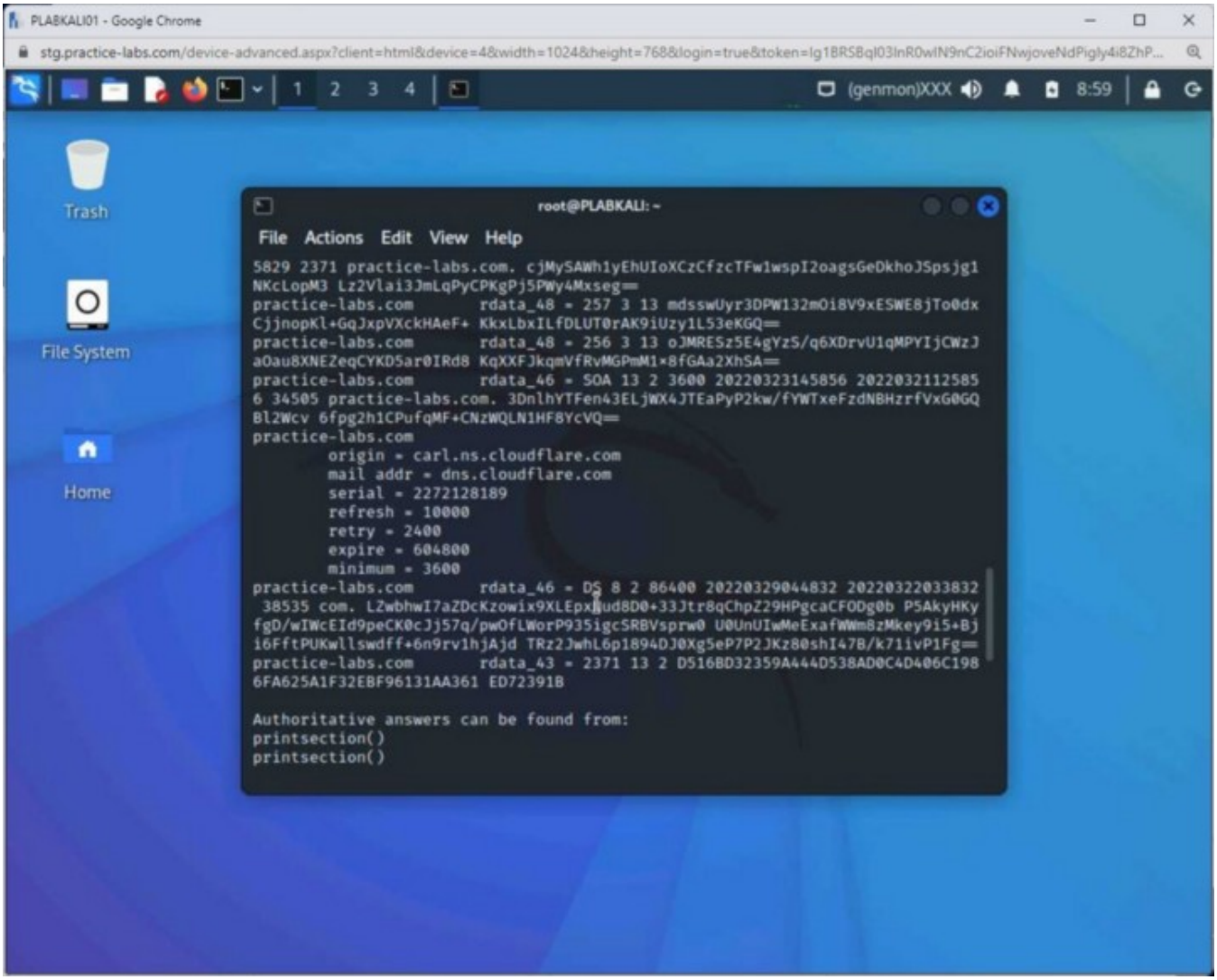
```
nslookup -query=any practice-labs.com
```

Press **Enter**.



Step 15

Notice the listed details as the output of this command.



Keep the terminal window open.

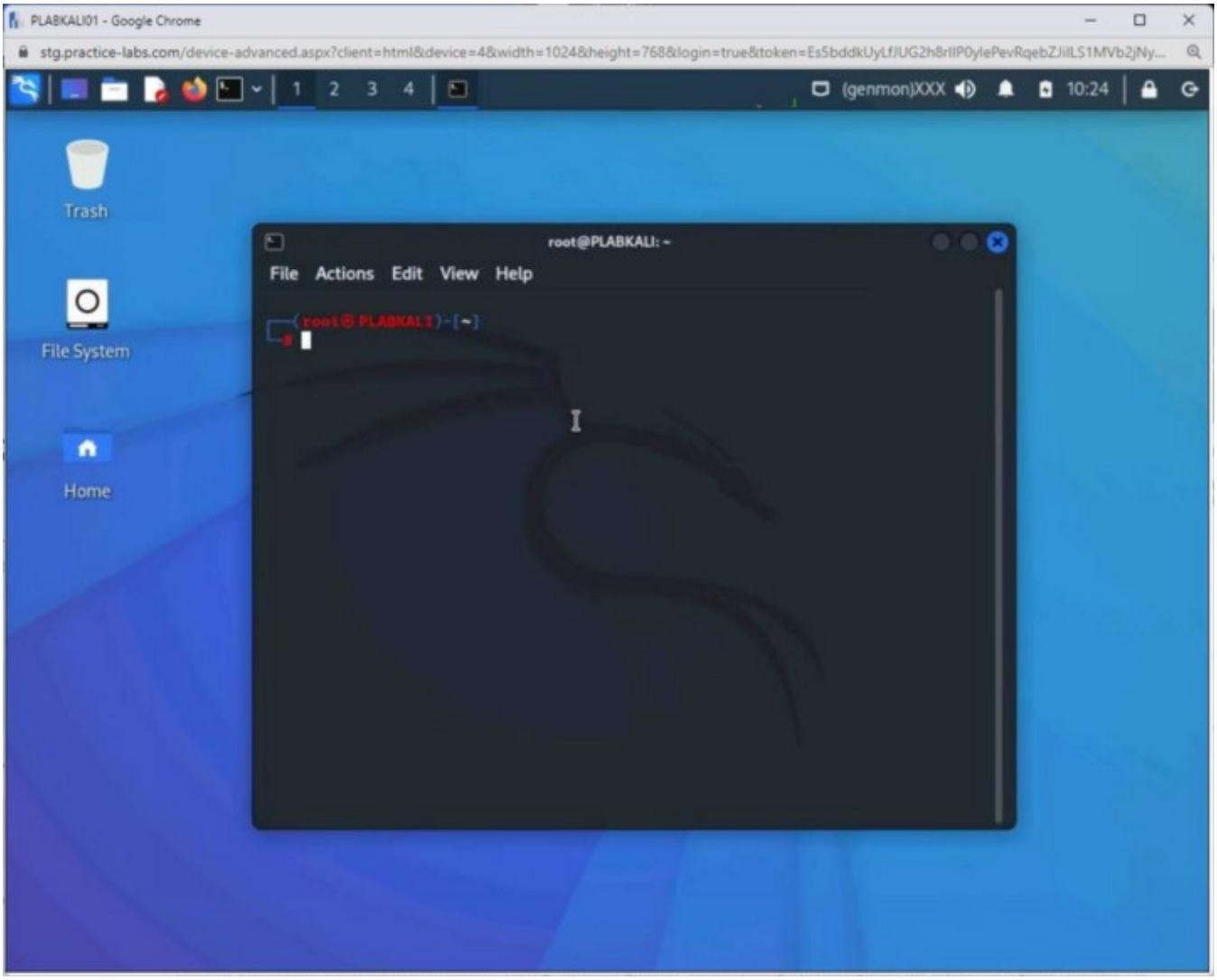
Task 2 — DNS Footprint using Dnsenum

Dnsenum is a DNS enumeration tool that is readily available in Kali Linux. Else, you can always download and install it on a different Linux variant. The core purpose of this tool is to help you determine which DNS information is publicly available.

In this task, you will learn to use the Dnsenum tool.

Step 1

Connect to **PLABKALI01** and ensure that the terminal window is open.

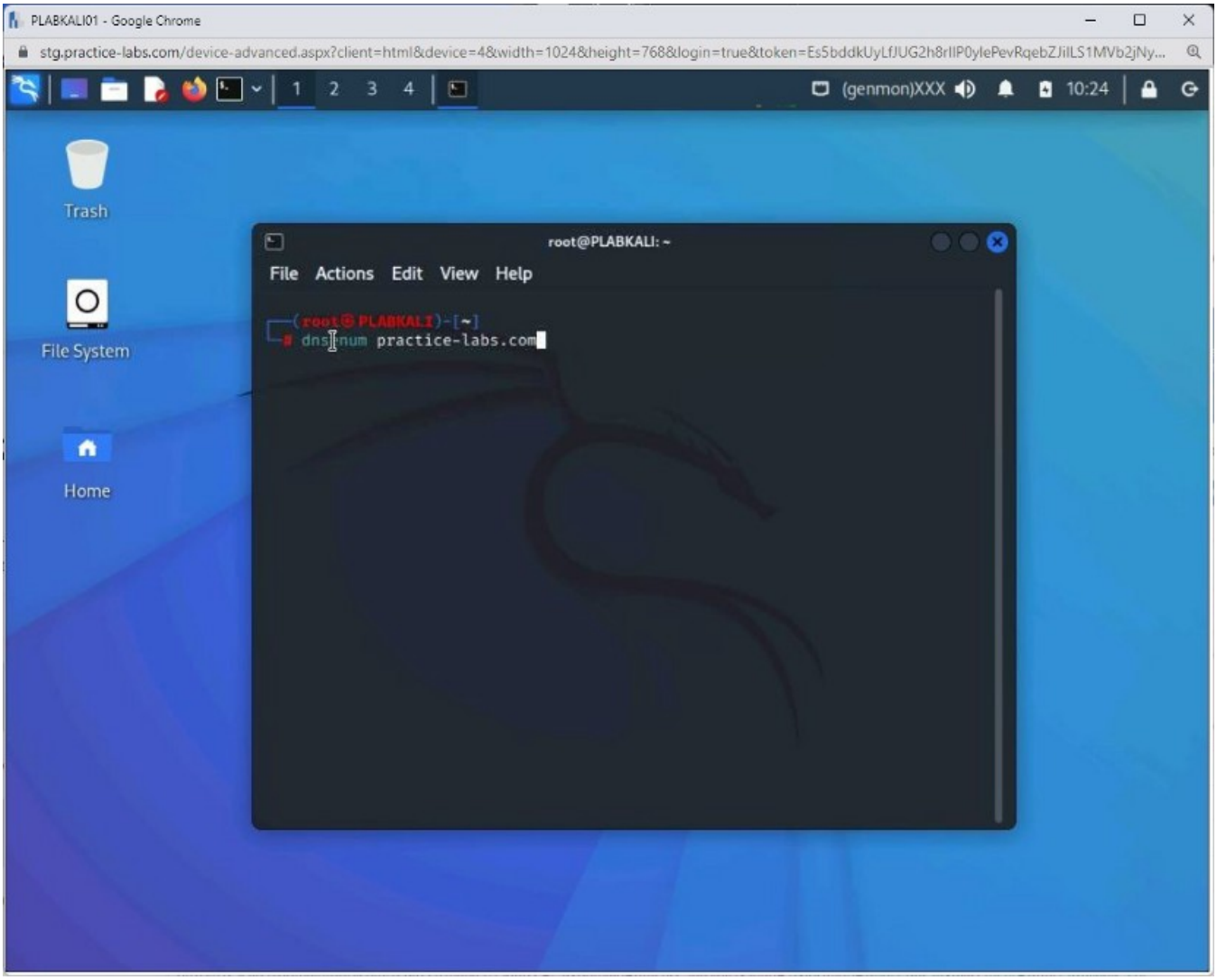


Step 2

The **dnsenum** command is simple to execute. You need to pass the name of the domain as the argument. Type the following command:

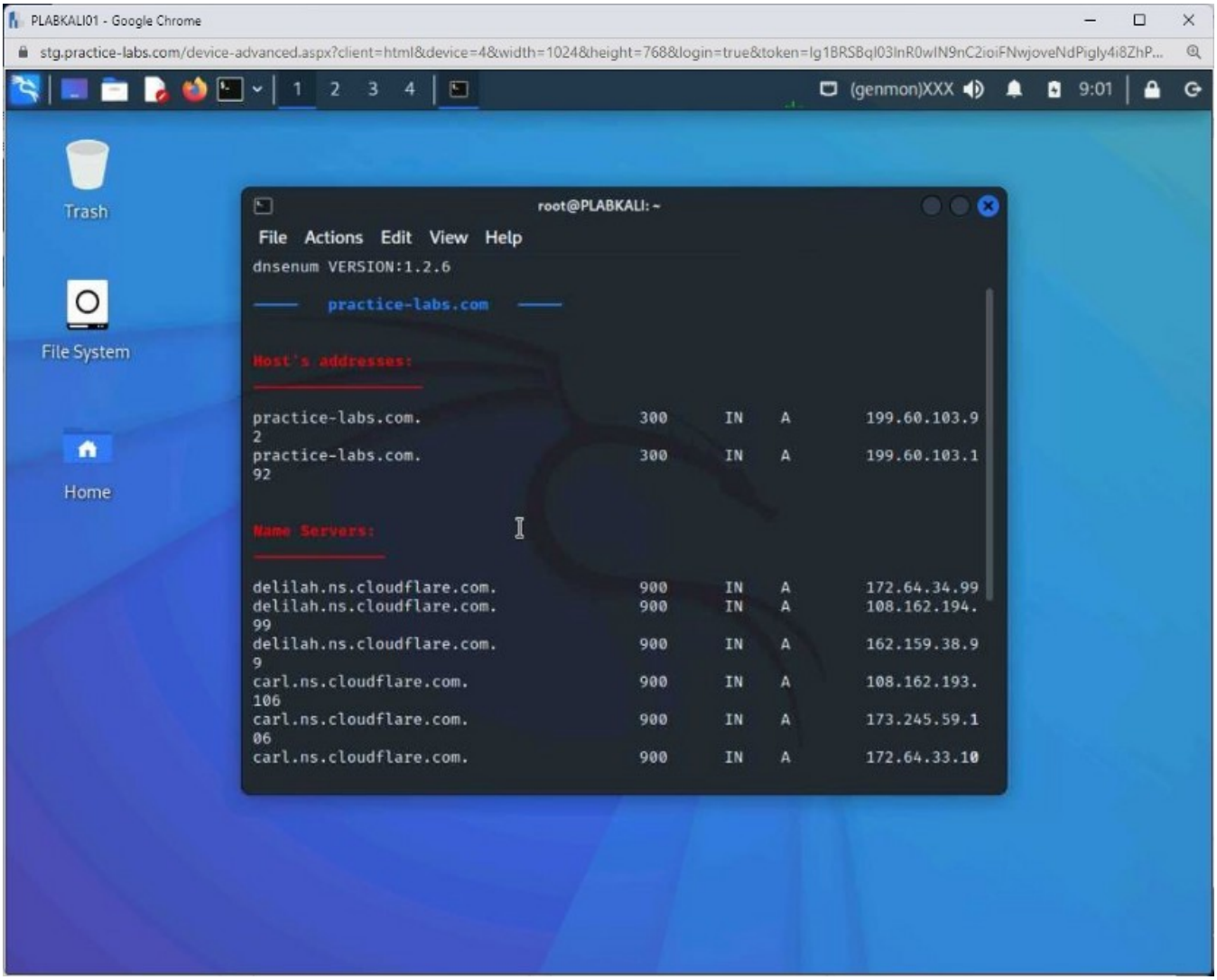
```
dnsenum practice-labs.com
```

Press **Enter**.



Step 3

The output displays mail records, DNS servers, and IP addresses.



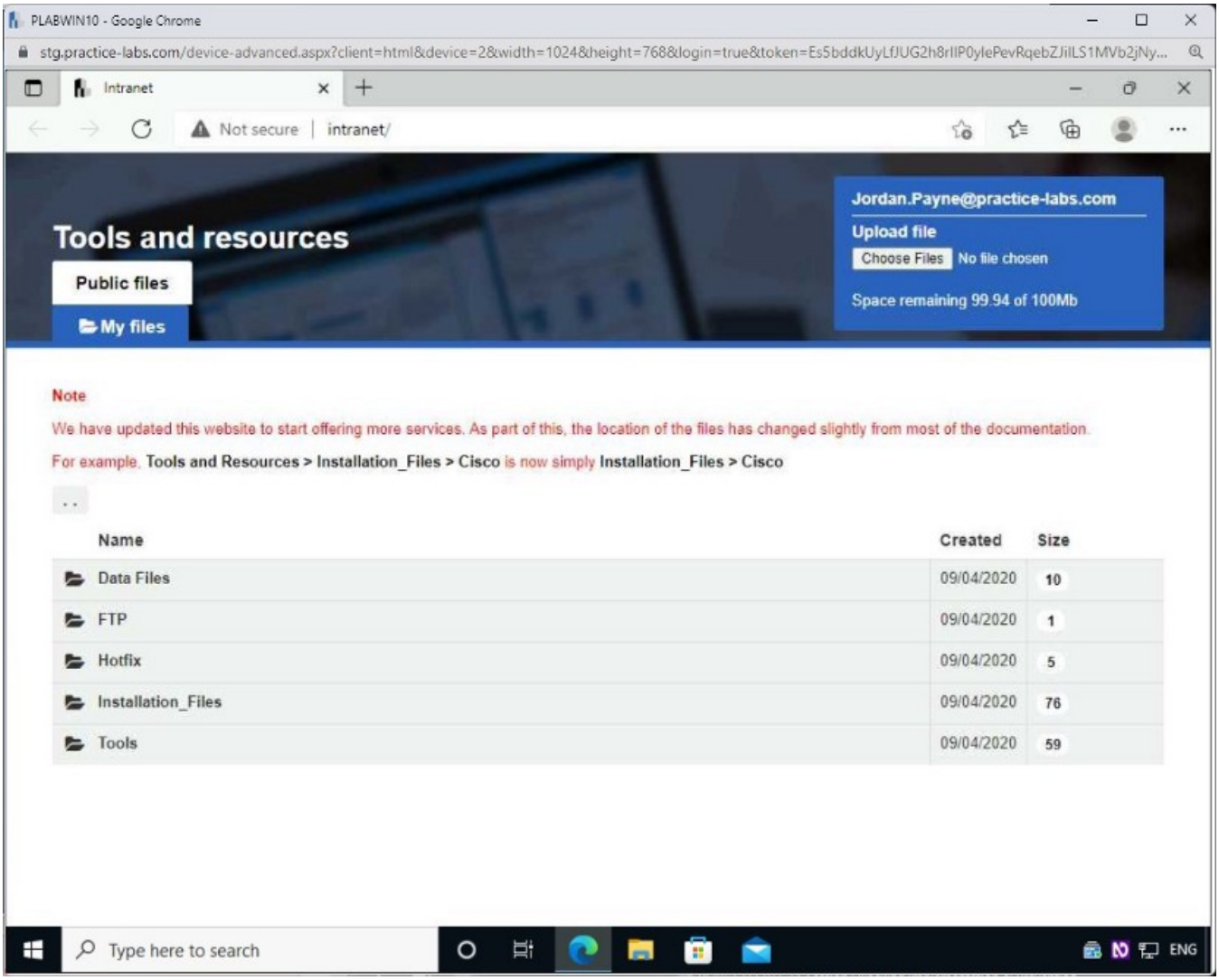
Task 3 — Footprinting using Reverse IP Domain Check

An attacker may be interested to know whether there is any other website hosted on the same server as the target website.

In this task, you will learn to use yougetsignal.com for reverse IP domain check.

Step 1

Connect to **PLABWIN10** and open **Microsoft Edge**.

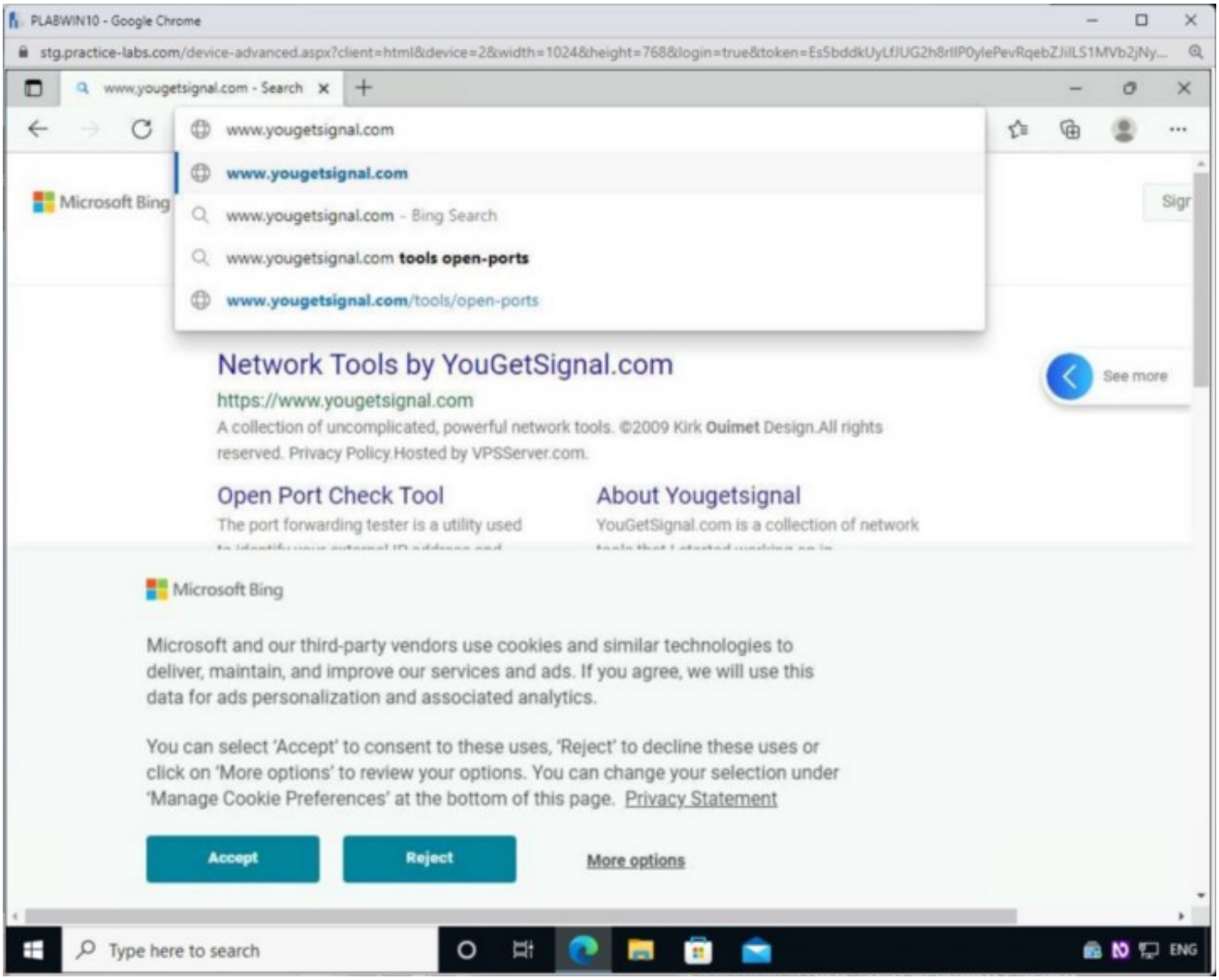


Step 2

In the address bar, type the following URL:

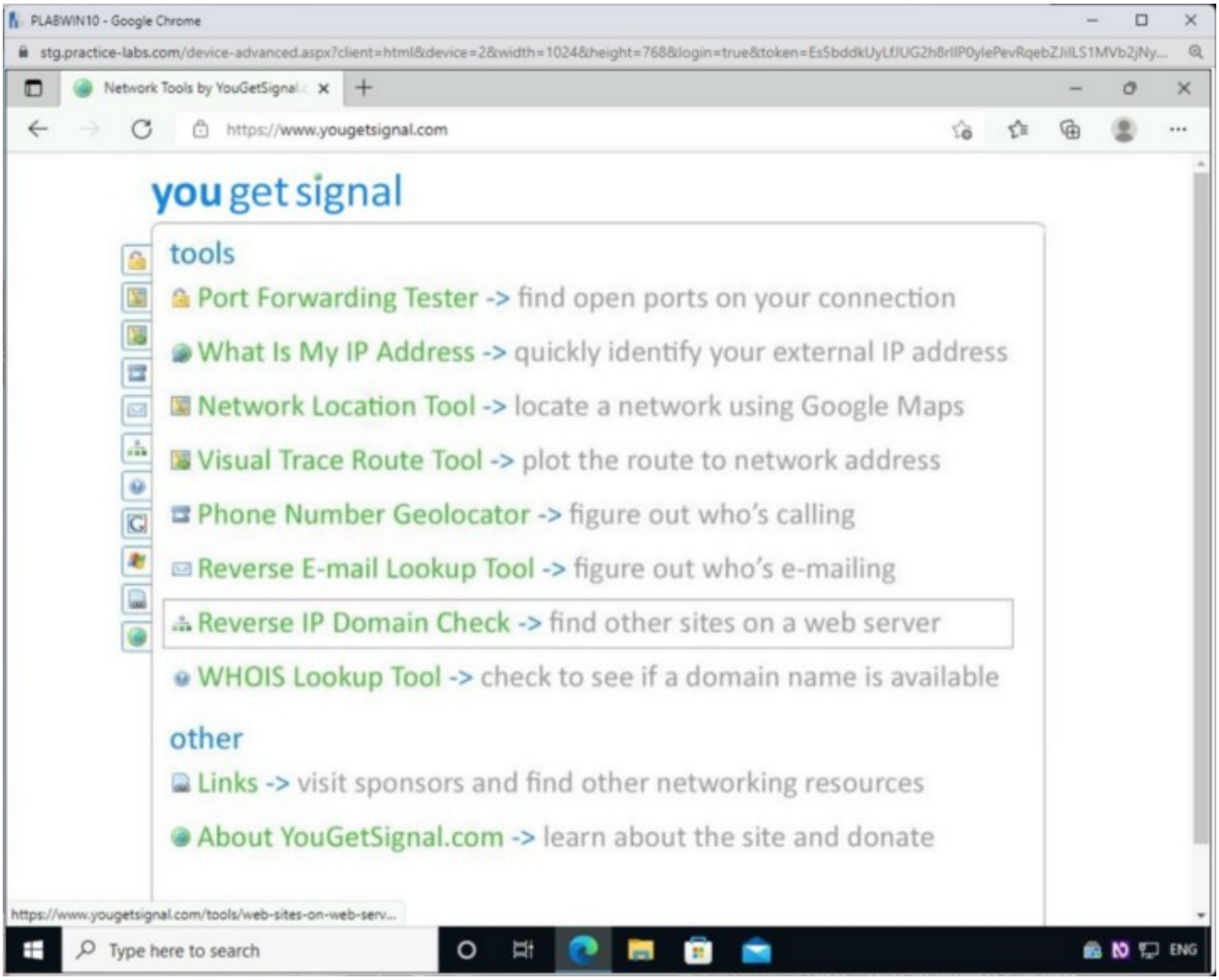
`www.yougetsignal.com`

Press **Enter**.



Step 3

The **you get signal** webpage is loaded. Click **Reverse IP Domain Check**.

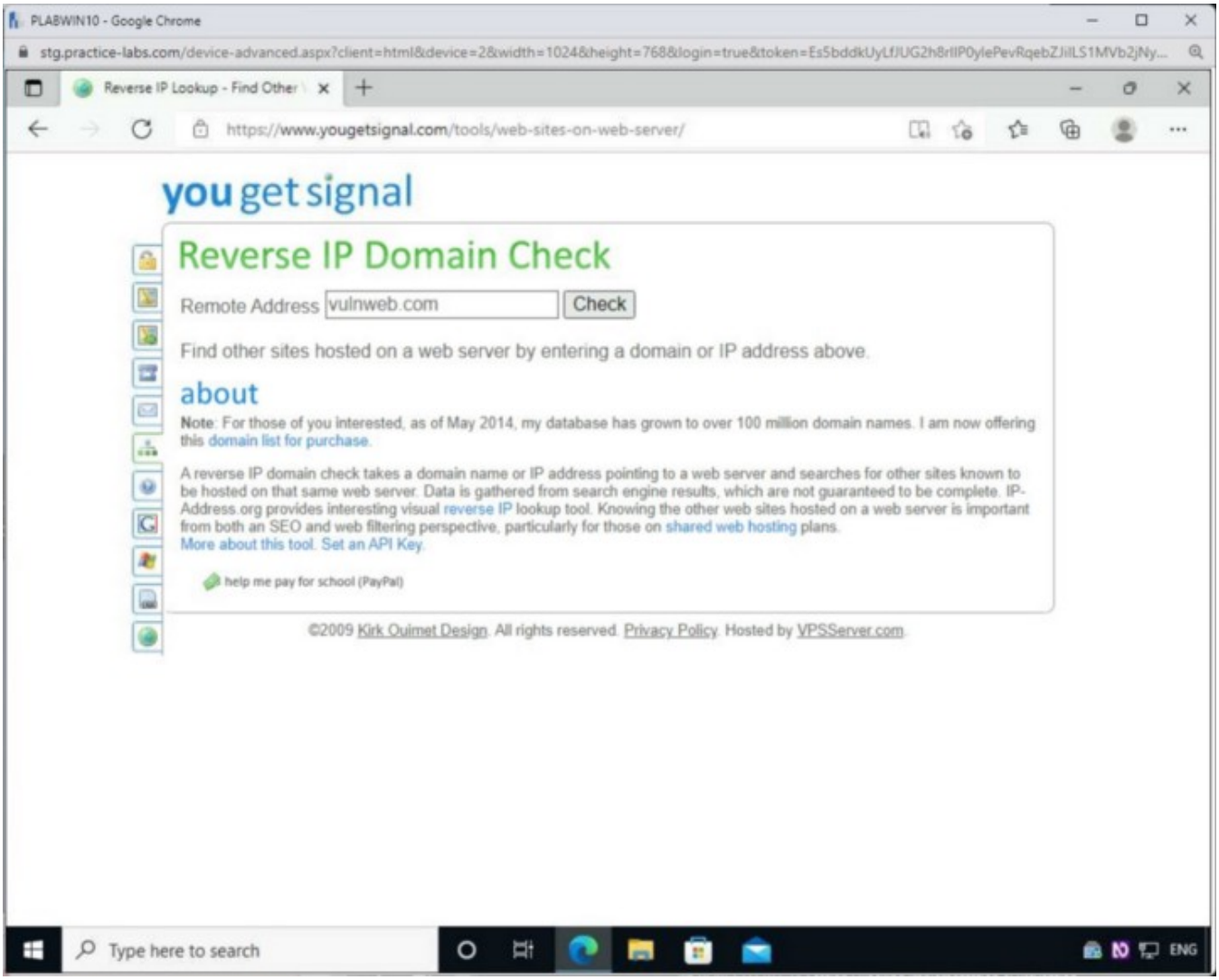


Step 4

The **Reverse IP Domain Check** webpage is displayed. In the **Remote Address** textbox, type the following domain name:

```
vulnweb.com
```

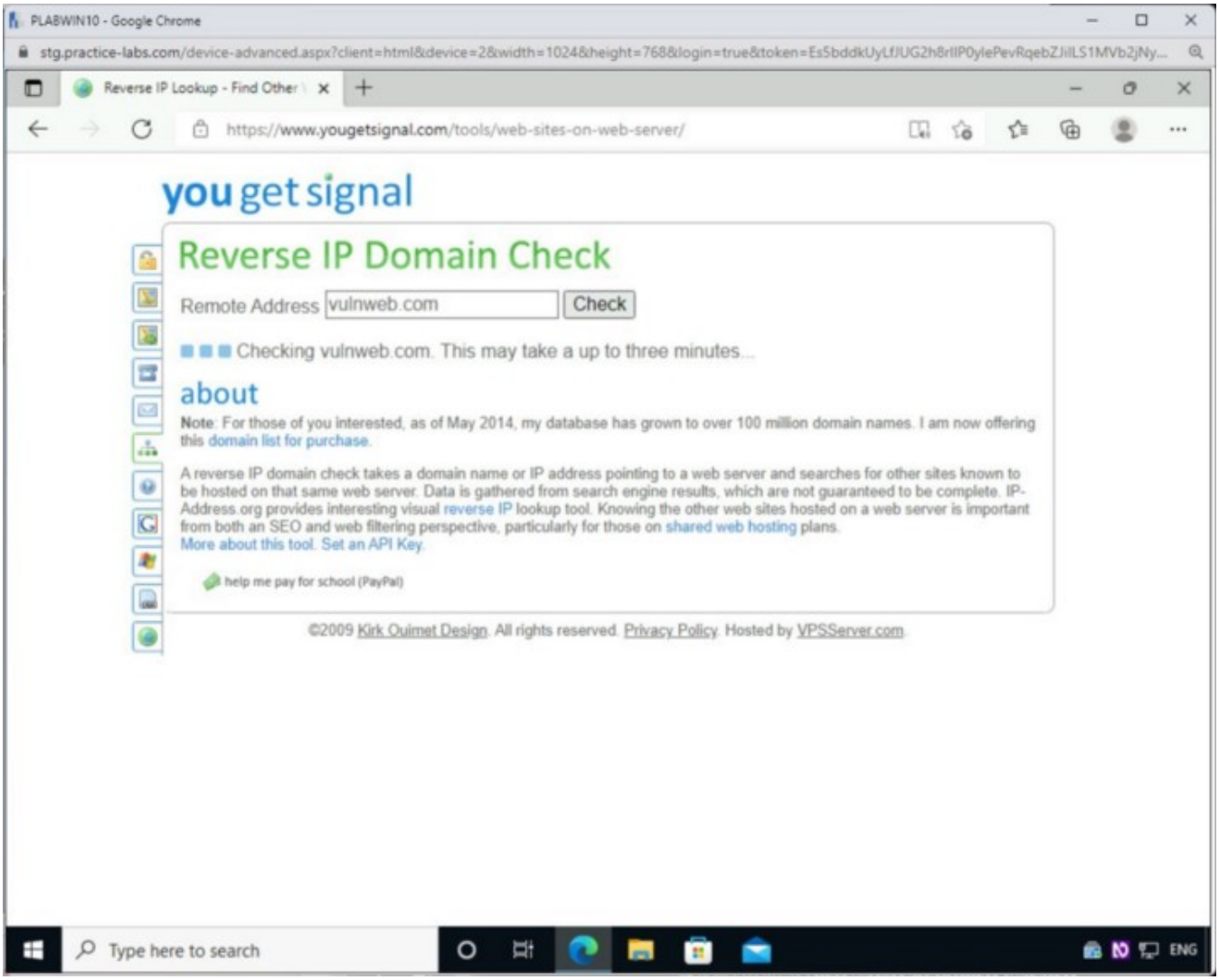
Click **Check**.



Step 5

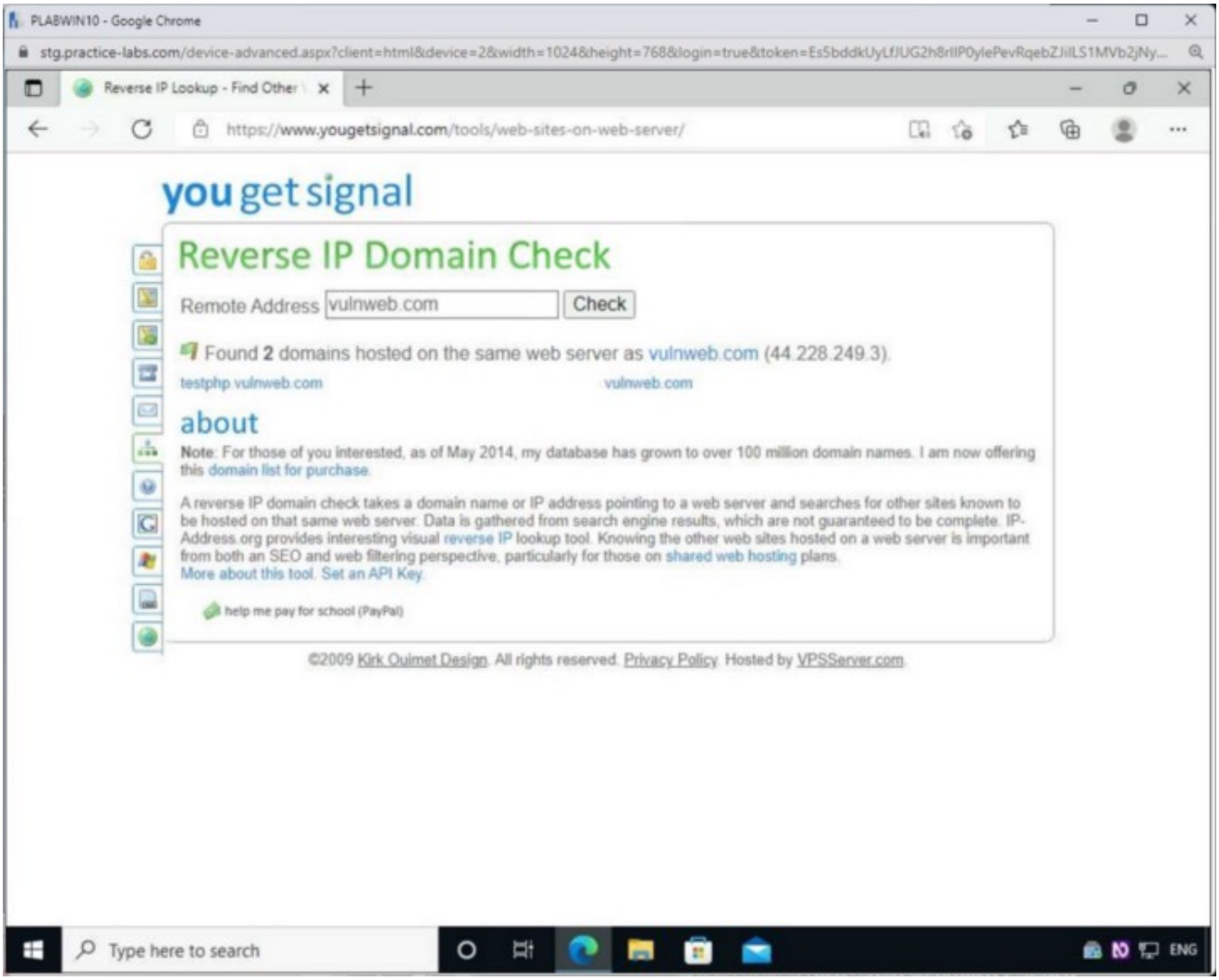
The scanning process begins.

Notice that it mentions that it might take up to three minutes.



Step 6

It has found two more domains hosted on the same server.



Exercise 3 — Network Footprinting

If you manage a small network, it is much easier to keep track of connected devices. However, as a network grows to instead include hundreds or thousands of connected devices, it becomes nearly impossible to track them manually.

You may have to track and map them, but a manual discovery can be a daunting task. You can use various tools to automatically draw a network, eliminating this issue.

In this exercise, you will learn about various email footprinting tools and methods.

Learning Outcomes

After completing this exercise, you will be able to:

- Use Network Topology Mapper
- Use the Advanced IP Scanner

Your Devices

You will be using the following devices in this lab. Please power these on now.

PLABDC01Domain Controller192.168.0.1/24PLABWIN10Domain MemberWorkstation192.168.0.3/24PLABKALI01Domain MemberWorkstation192.168.0.5/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

Task 1 — Installing SolarWinds Network Topology Mapper

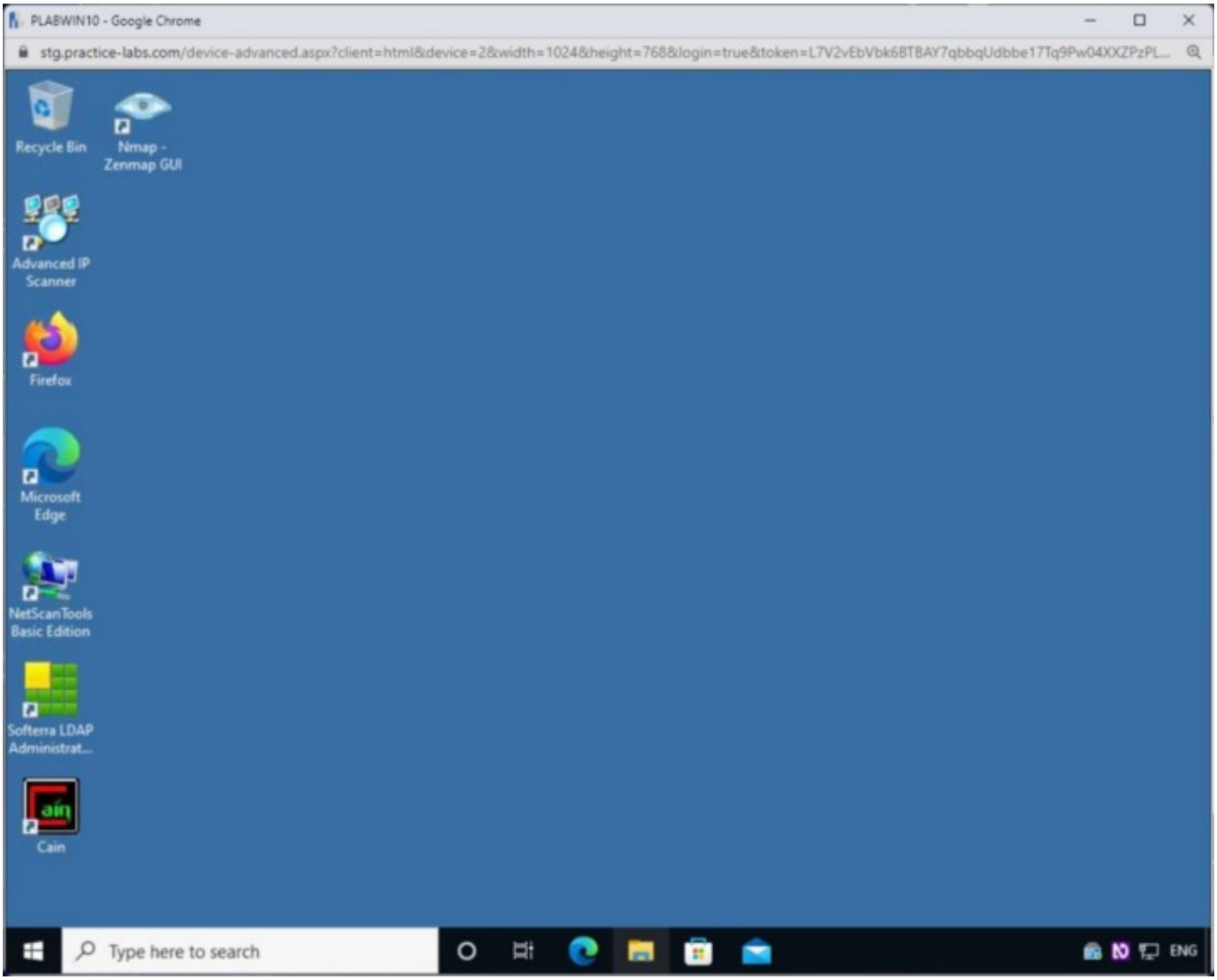
You can use SolarWinds Network Topology Mapper to create a network map, which automatically discovers and maps an associated local network.

In this task, you will install the trial version of this tool.

Step 1

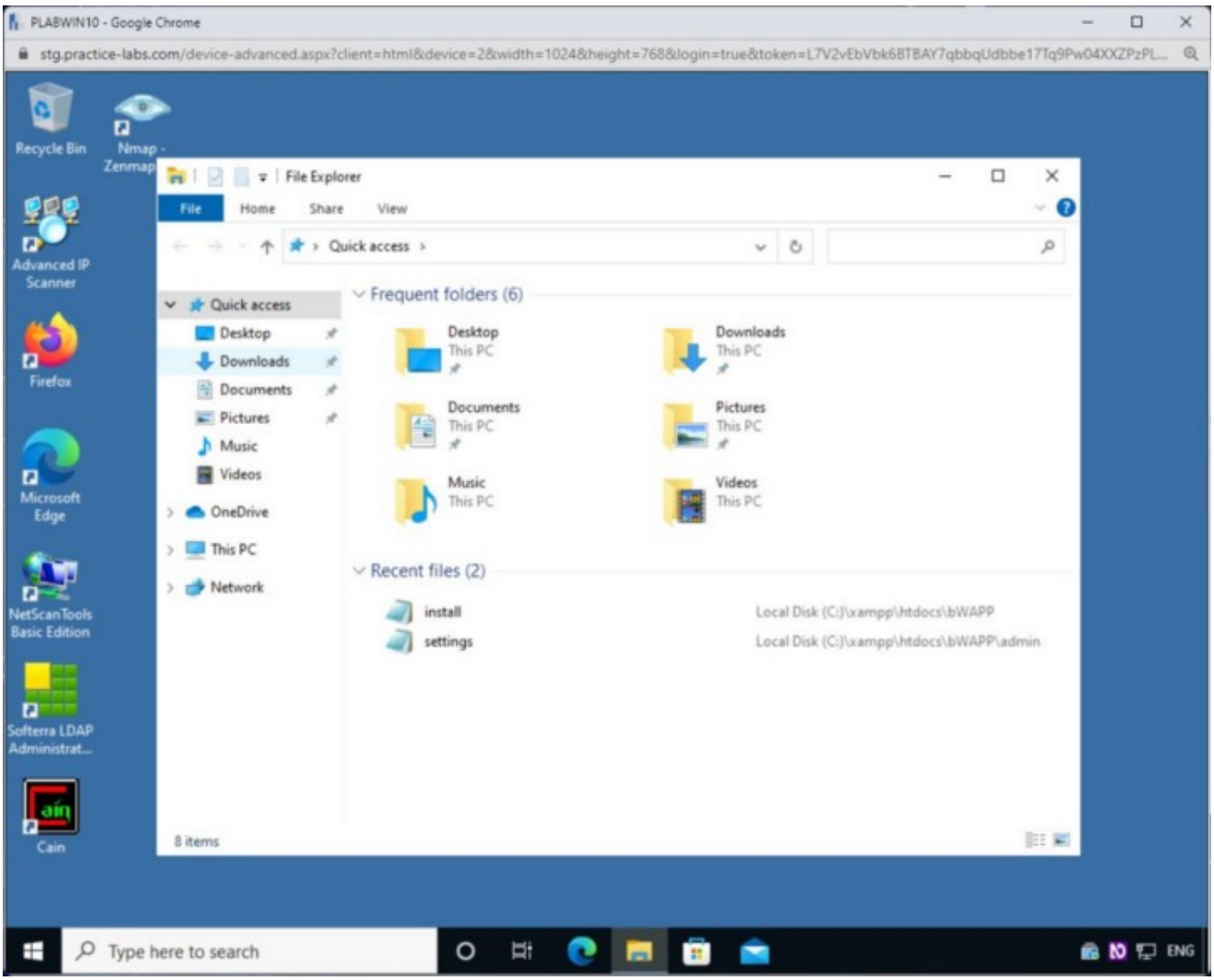
Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10.**

Open **File Explorer** from the taskbar.



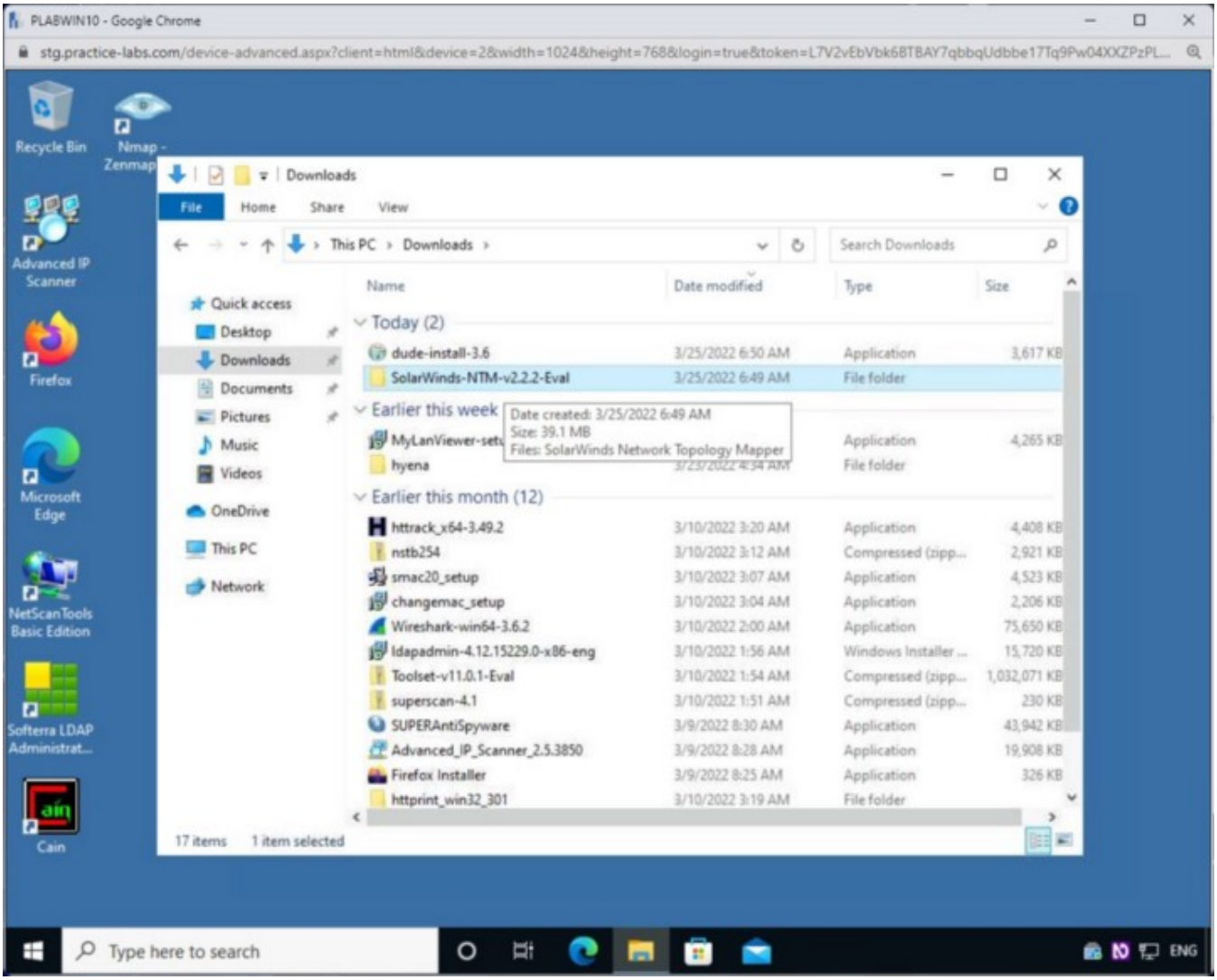
Step 2

Navigate to the **Downloads** folder.



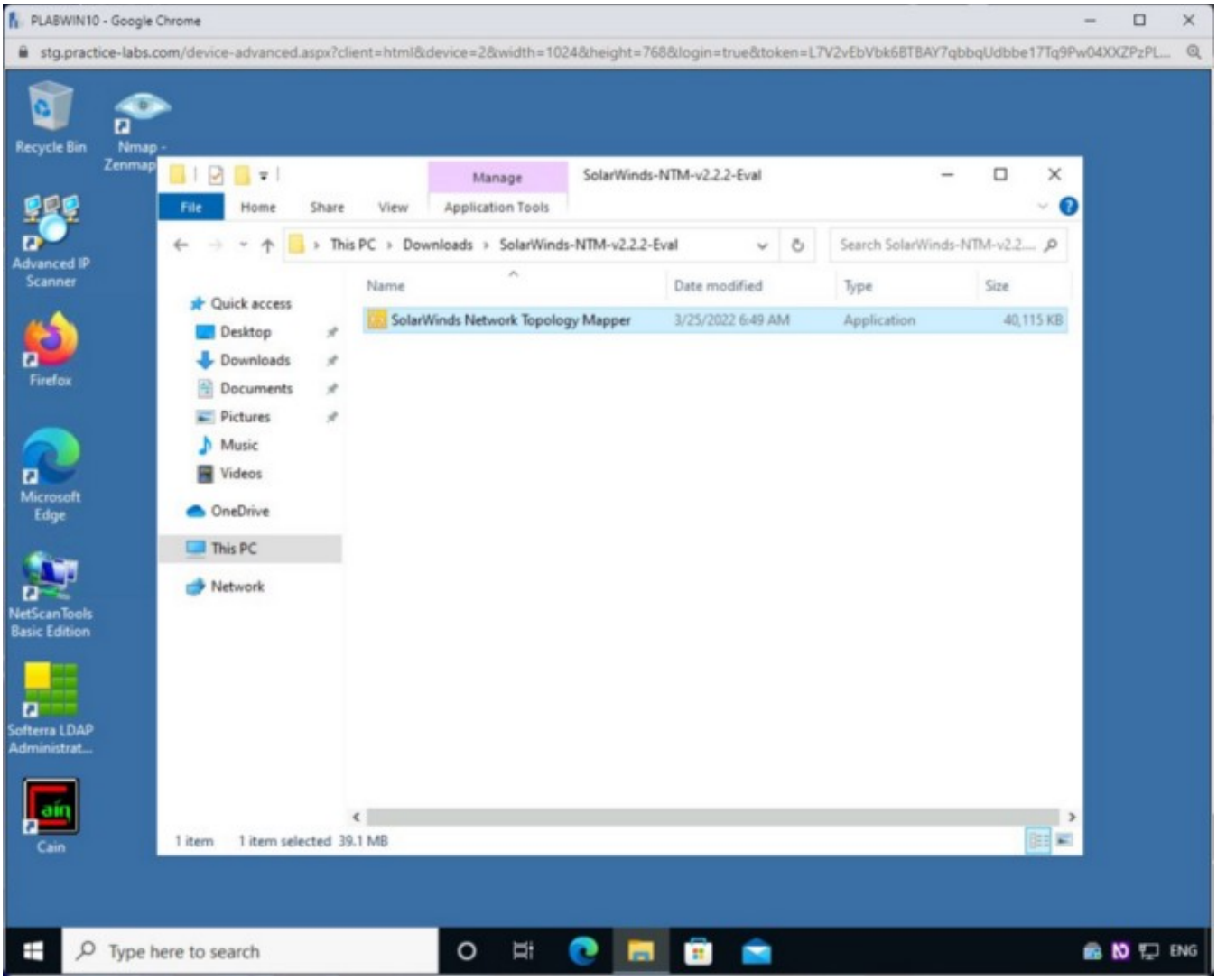
Step 3

Scroll down the list and double-click on the **SolarWinds-NTM-v2.2.2-Eval** folder.



Step 4

Double click on the **SolarWinds Network Topology Mapper** executable file.



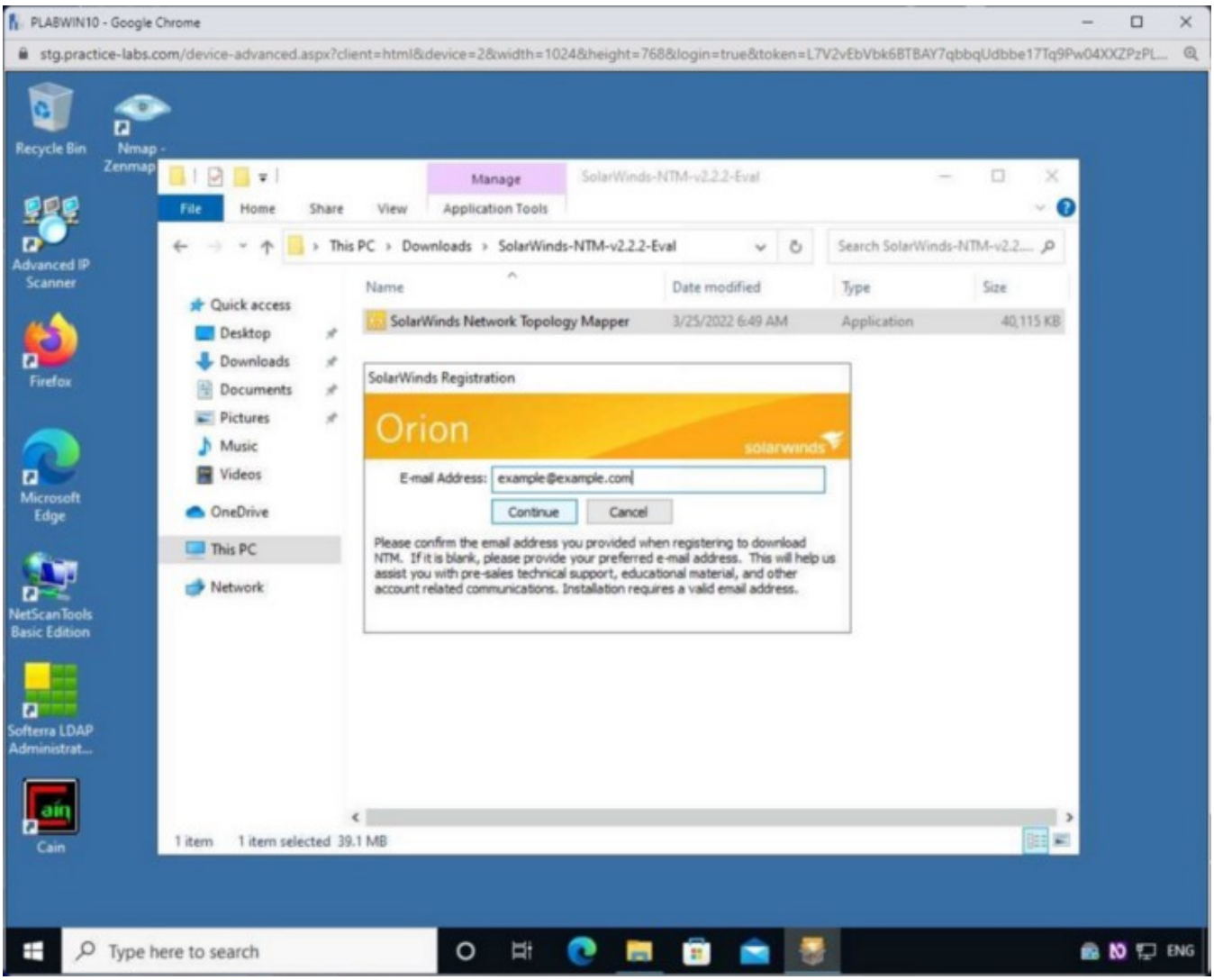
Step 5

On the **SolarWinds Registration** page, type the following into the **E-mail address** field:

```
example@example.com
```

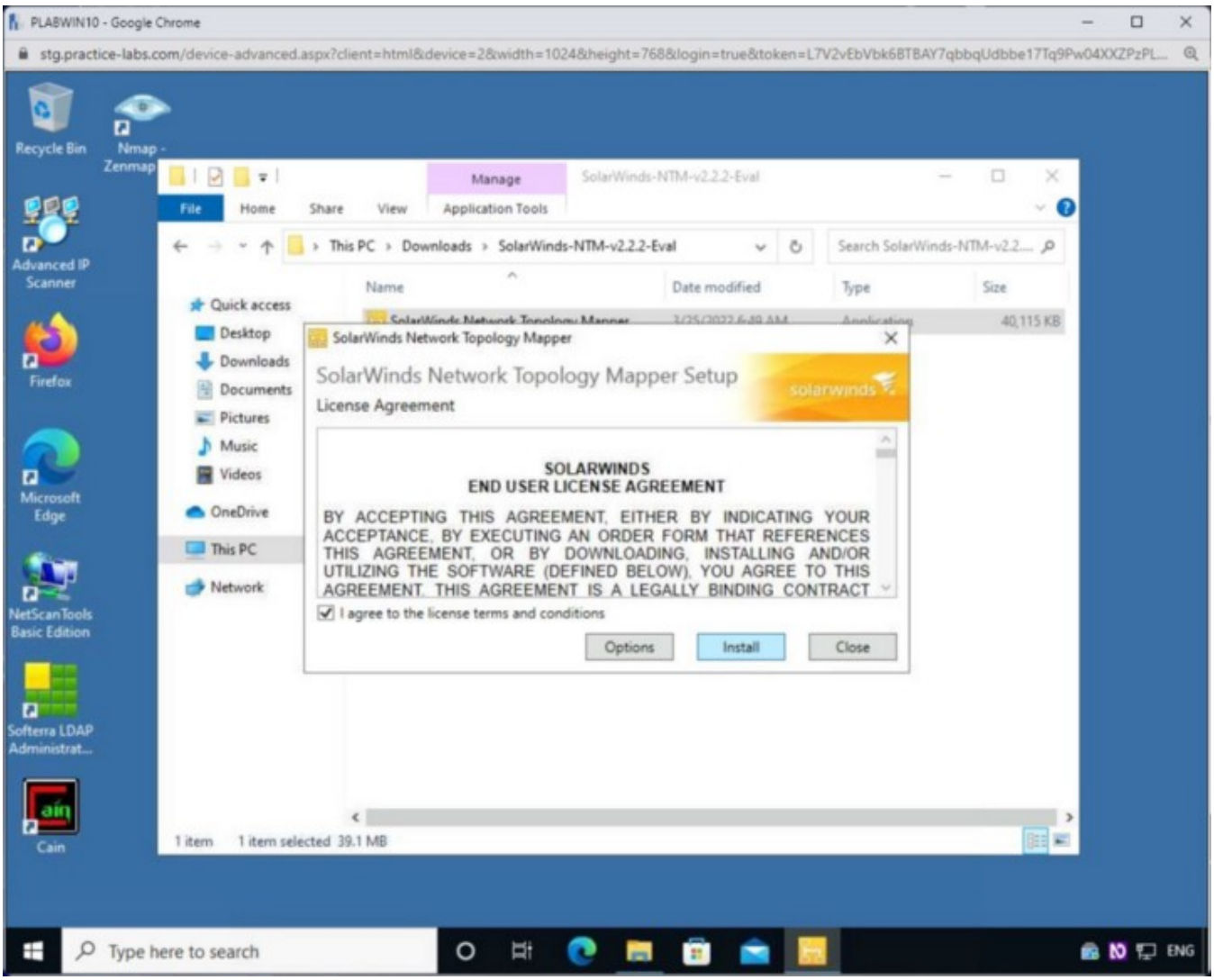
Press **Continue**.

***Note**: In a real-world example, you would instead use either your own personal or a business e-mail address.*



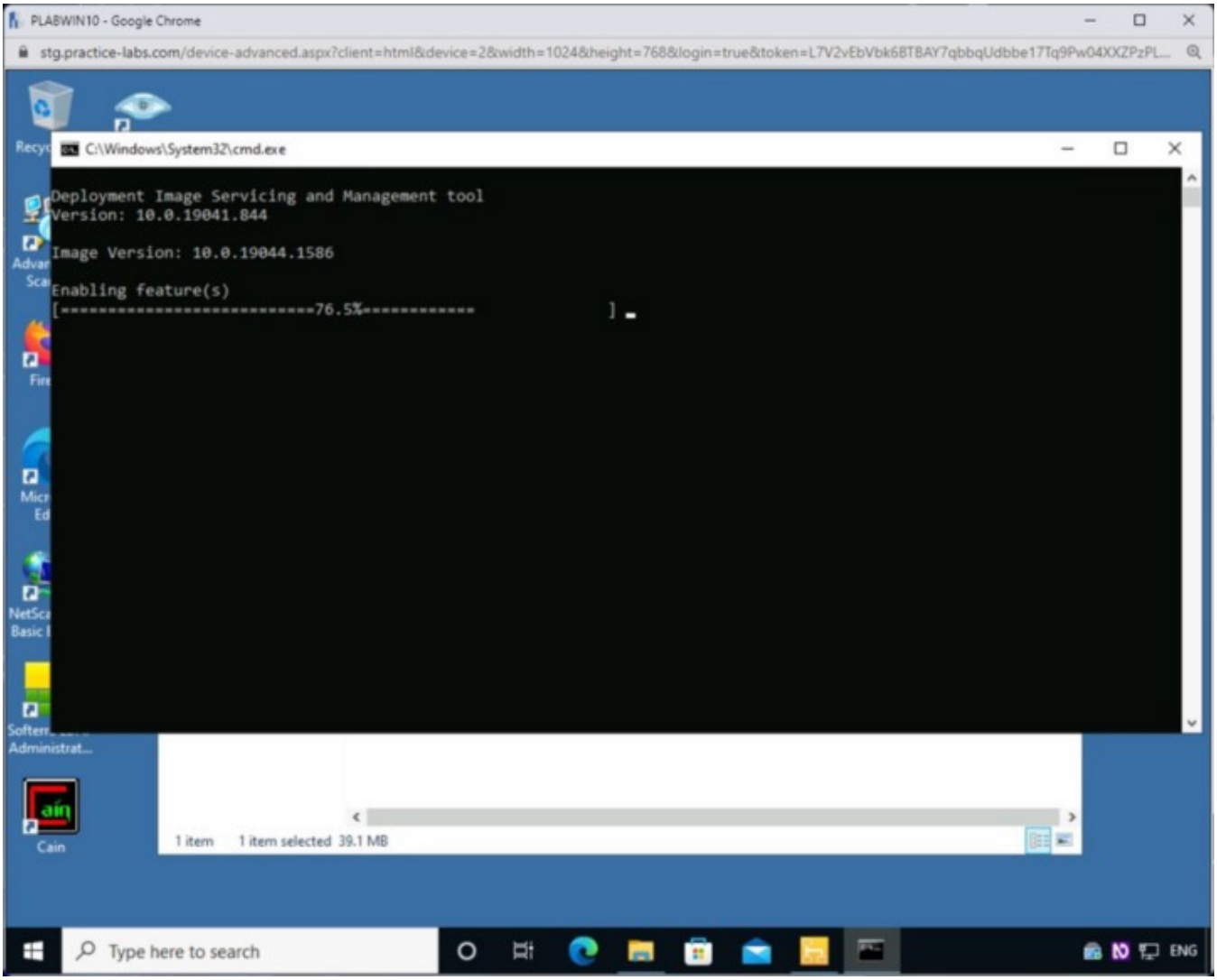
Step 6

On the **Licence Agreement** page, click **I agree to the licence terms and conditions** checkbox and click **Install**.



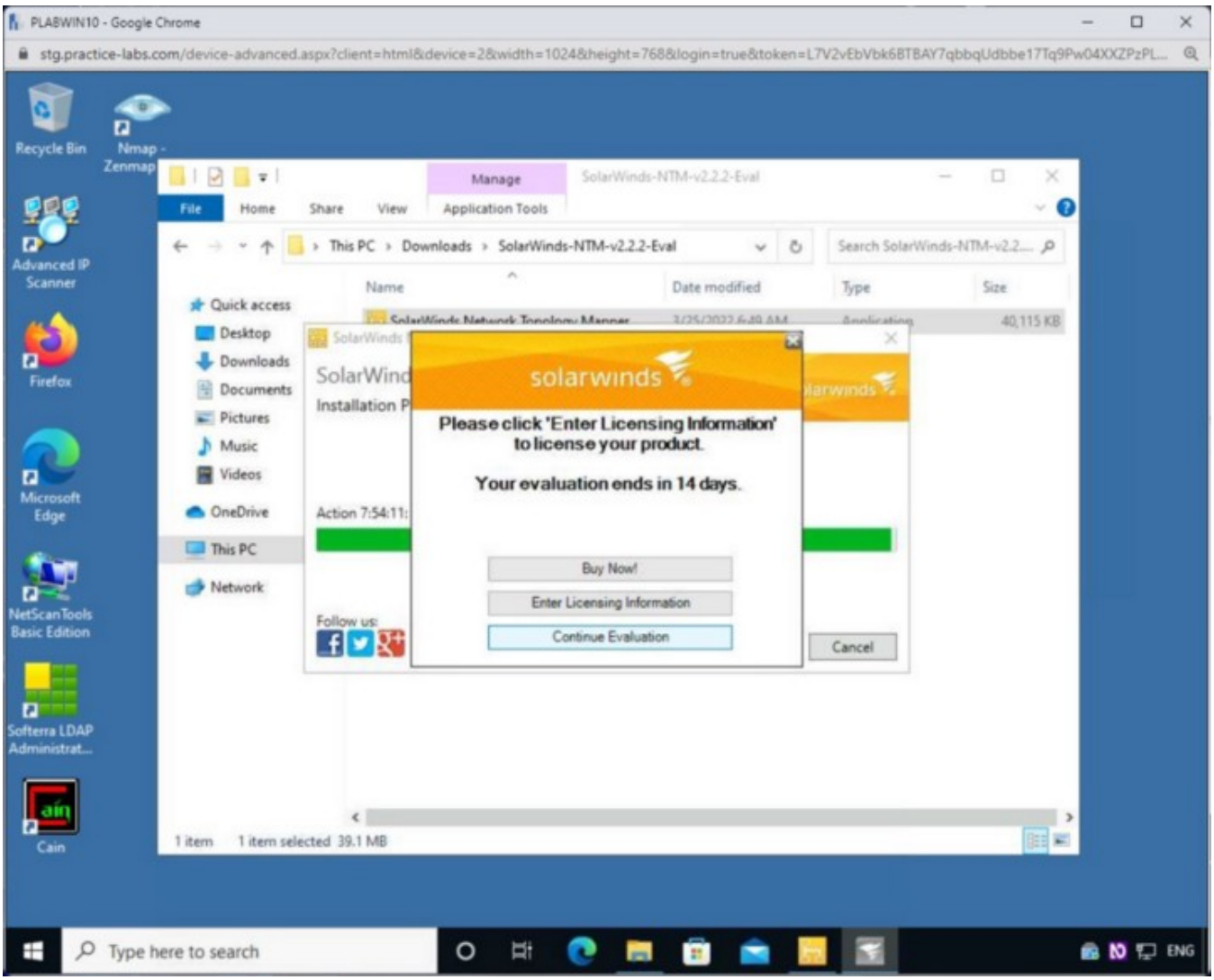
Step 7

During the installation, a **Command Prompt** window will open stating that features are being enabled. Please allow this process to complete.



Step 8

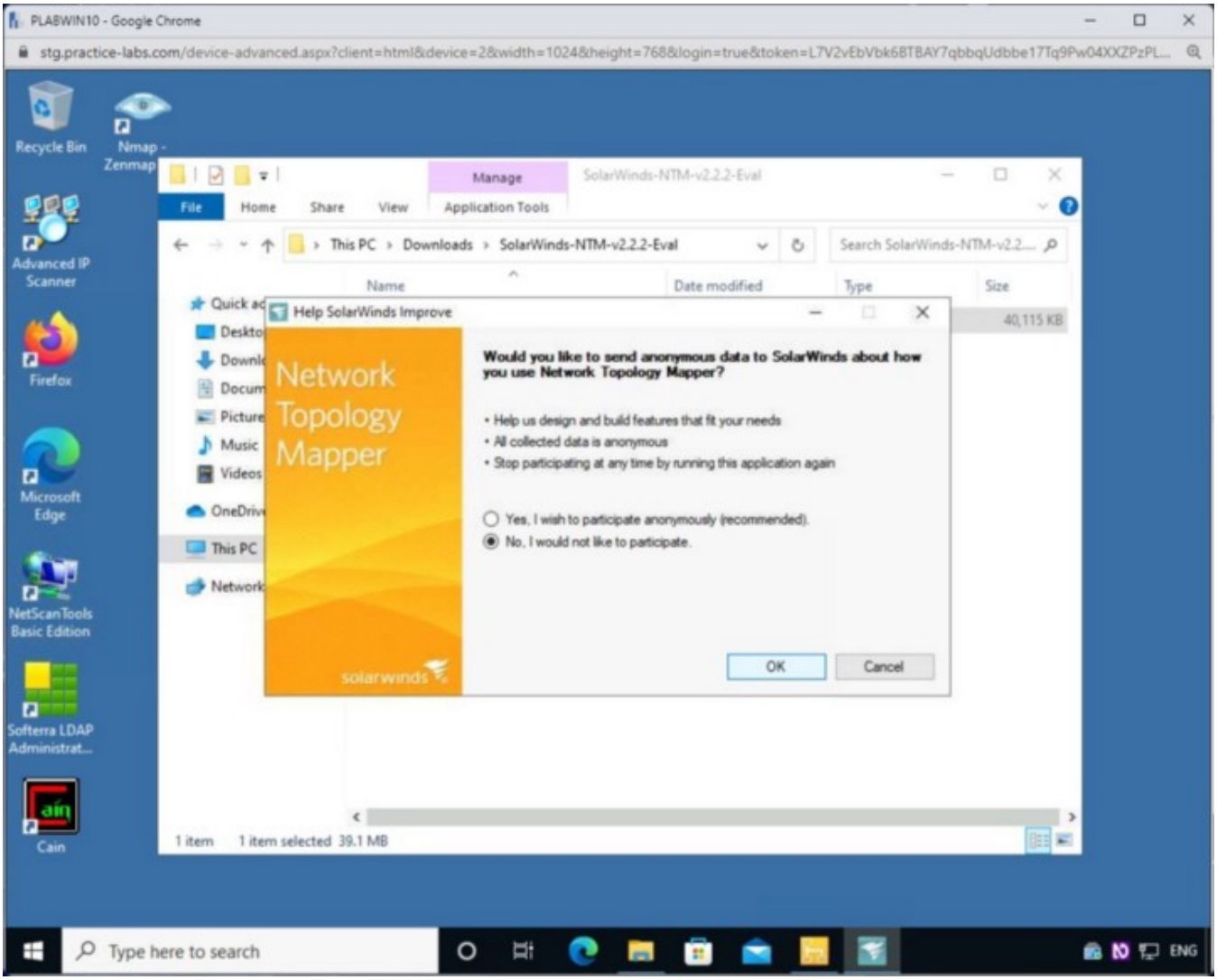
On the **Enter Licensing Information** page, click **Continue Evaluation.**



Step 9

On the **Help SolarWinds Improve** page, select the **No, I would not like to participate** checkbox and click **OK**.

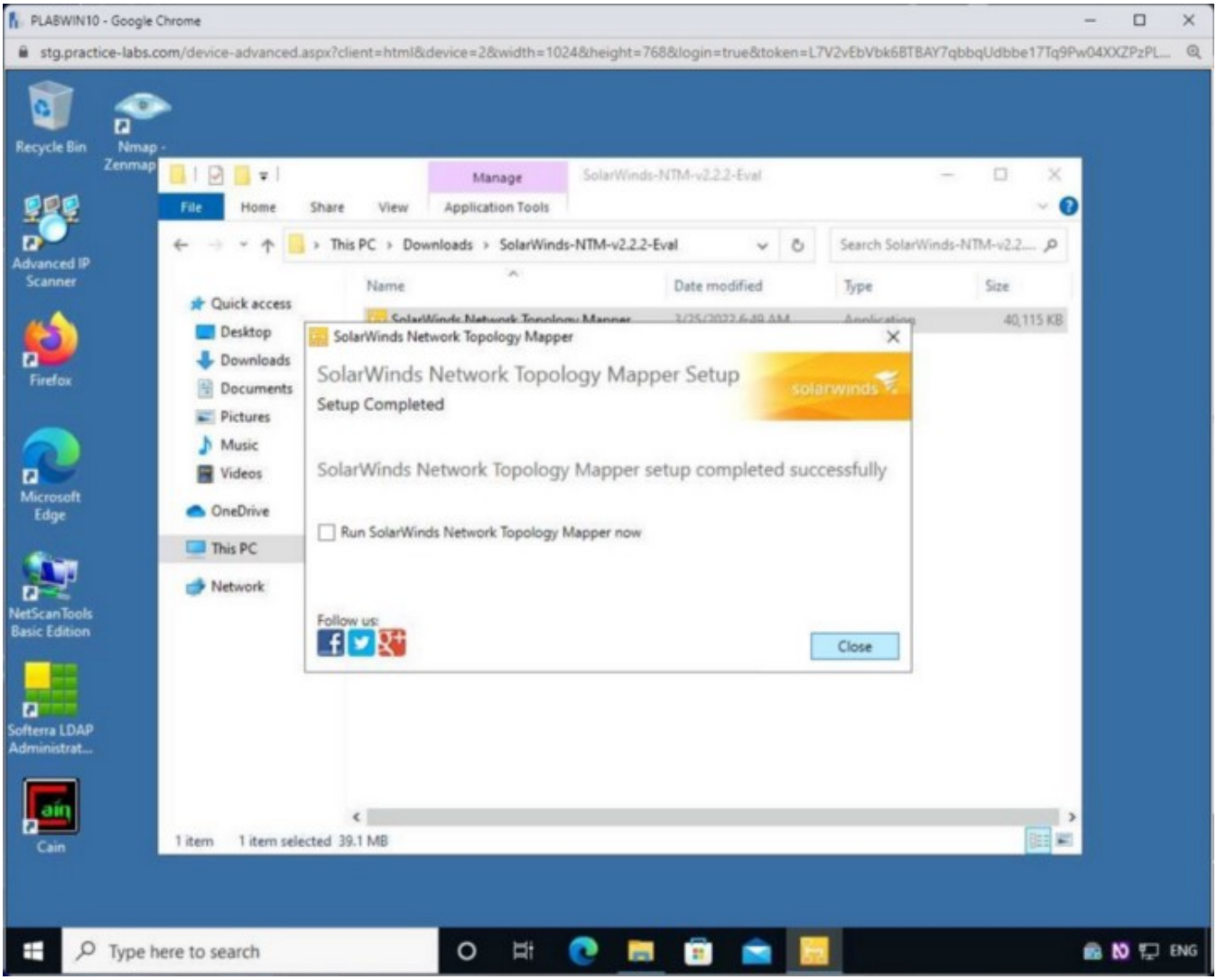
***Note**: A window may also appear to state that SolarWinds is installing some extra tools. Please allow this to complete.*



Step 10

Finally, on the **Completed SolarWinds Toolset v11.0.1 Setup Wizard** page, uncheck the **Run SolarWinds Network Topology Mapper now** checkbox.

Click **Close**.



Close all open windows.

Task 2 — Use Network Topology Mapper

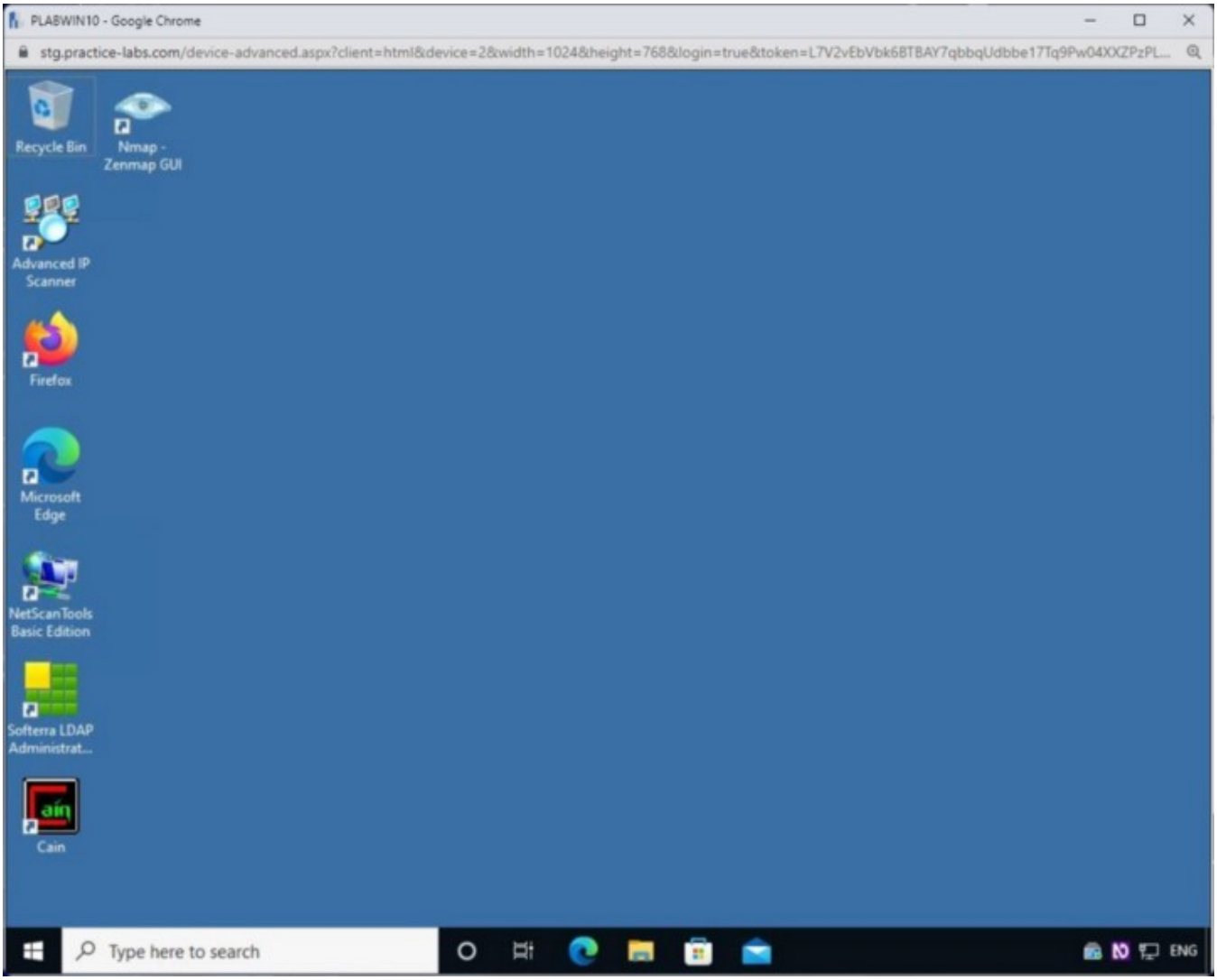
SolarWinds Network Topology Mapper can use various discovery methods, such as SNMP, CDP, ICMP, or WMI.

You can also use it to create reports compliant with the security standards, such as PCI, FIPS 140–2, and HIPAA. After creating a map, you can also export it with different applications, such as Microsoft Visio.

In this task, you will use Network Topology Mapper.

Step 1

Reconnect to **PLABWIN10**.

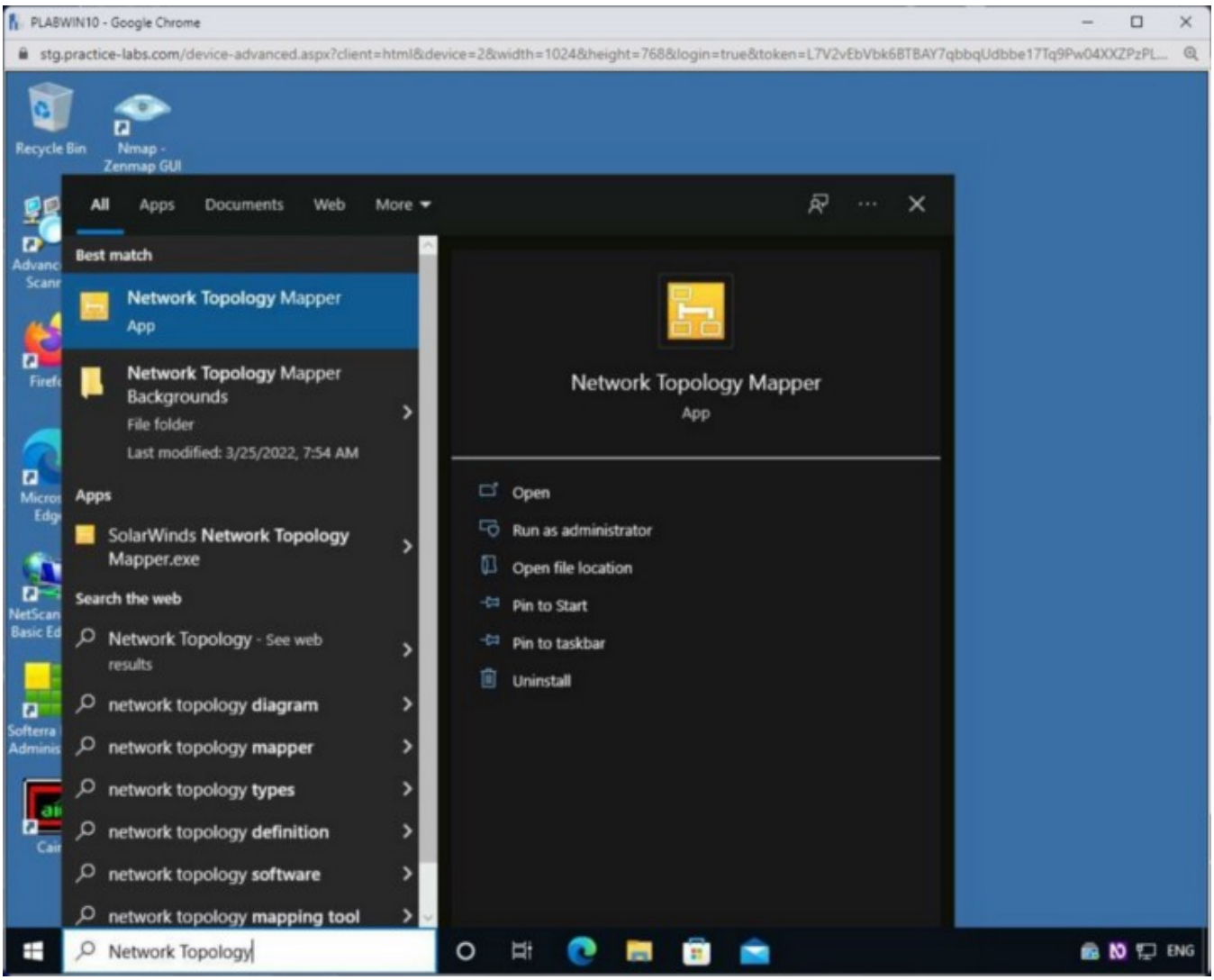


Step 2

In the **Type here to search** textbox, type the following:

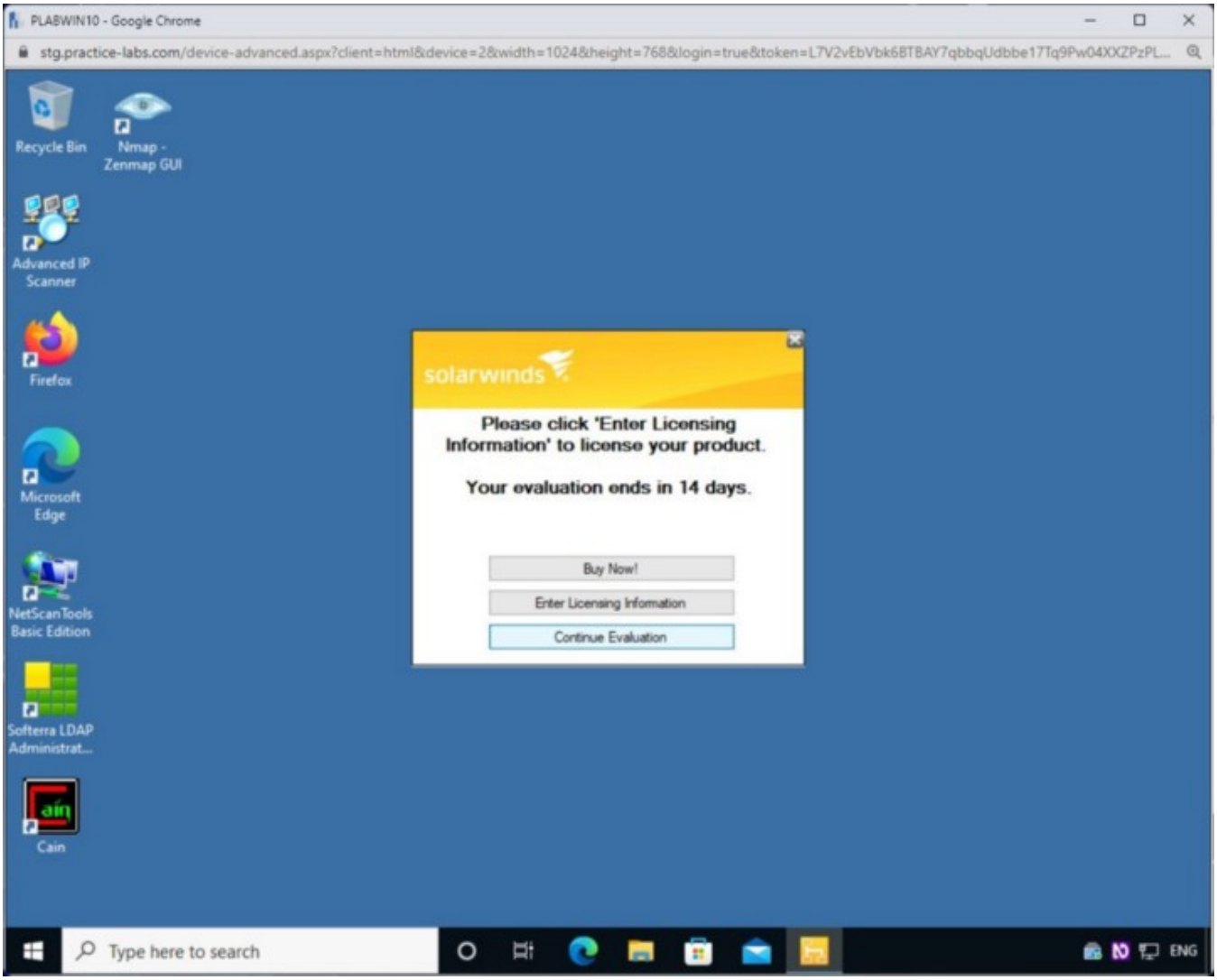
```
Network Topology
```

From the search results, select **Network Topology Mapper**.



Step 3

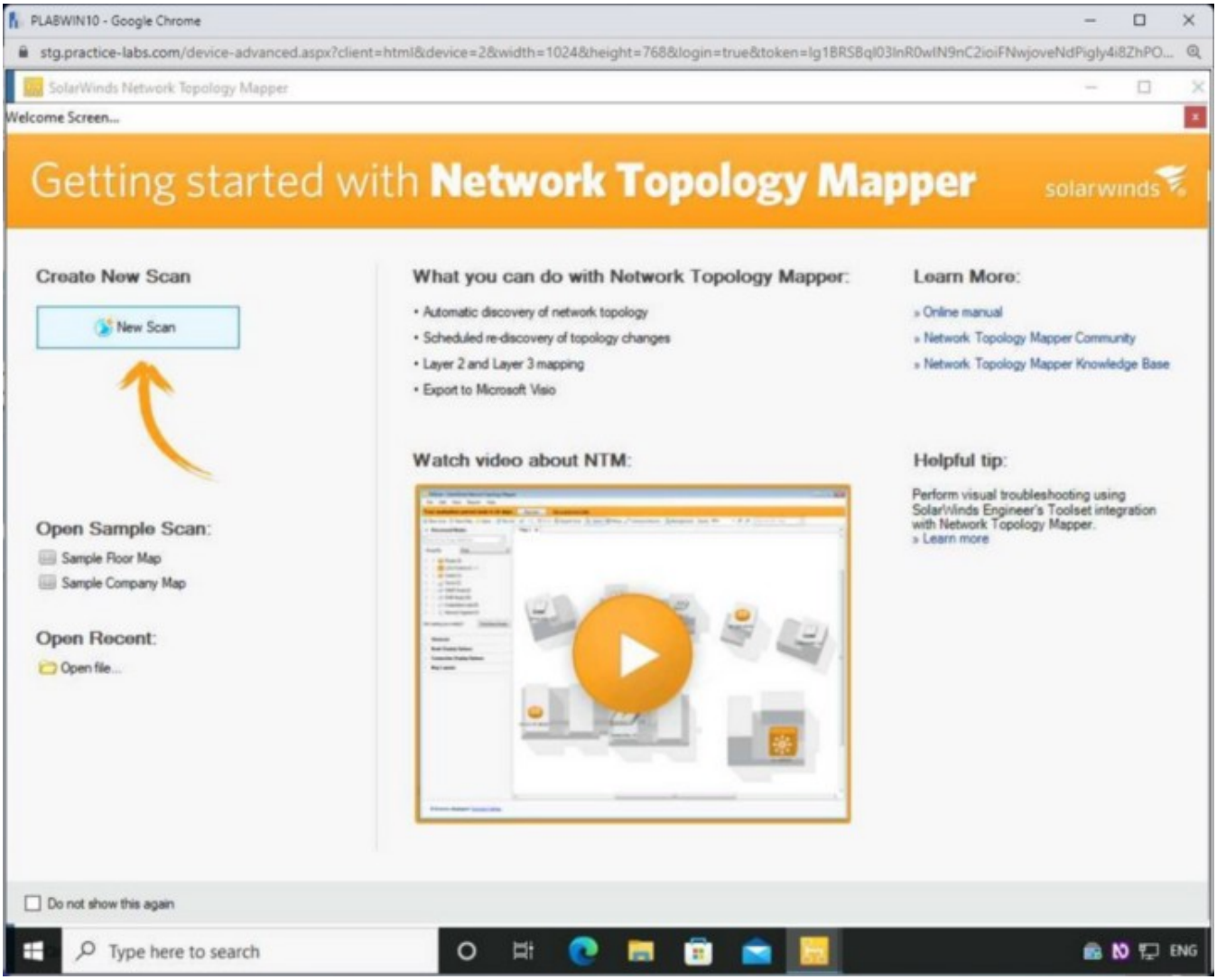
On the **Enter Licensing Information** page, click **Continue Evaluation**.



Step 4

The **Getting started with Network Topology Mapper** dialog box is displayed.

Click **New Network Scan**.



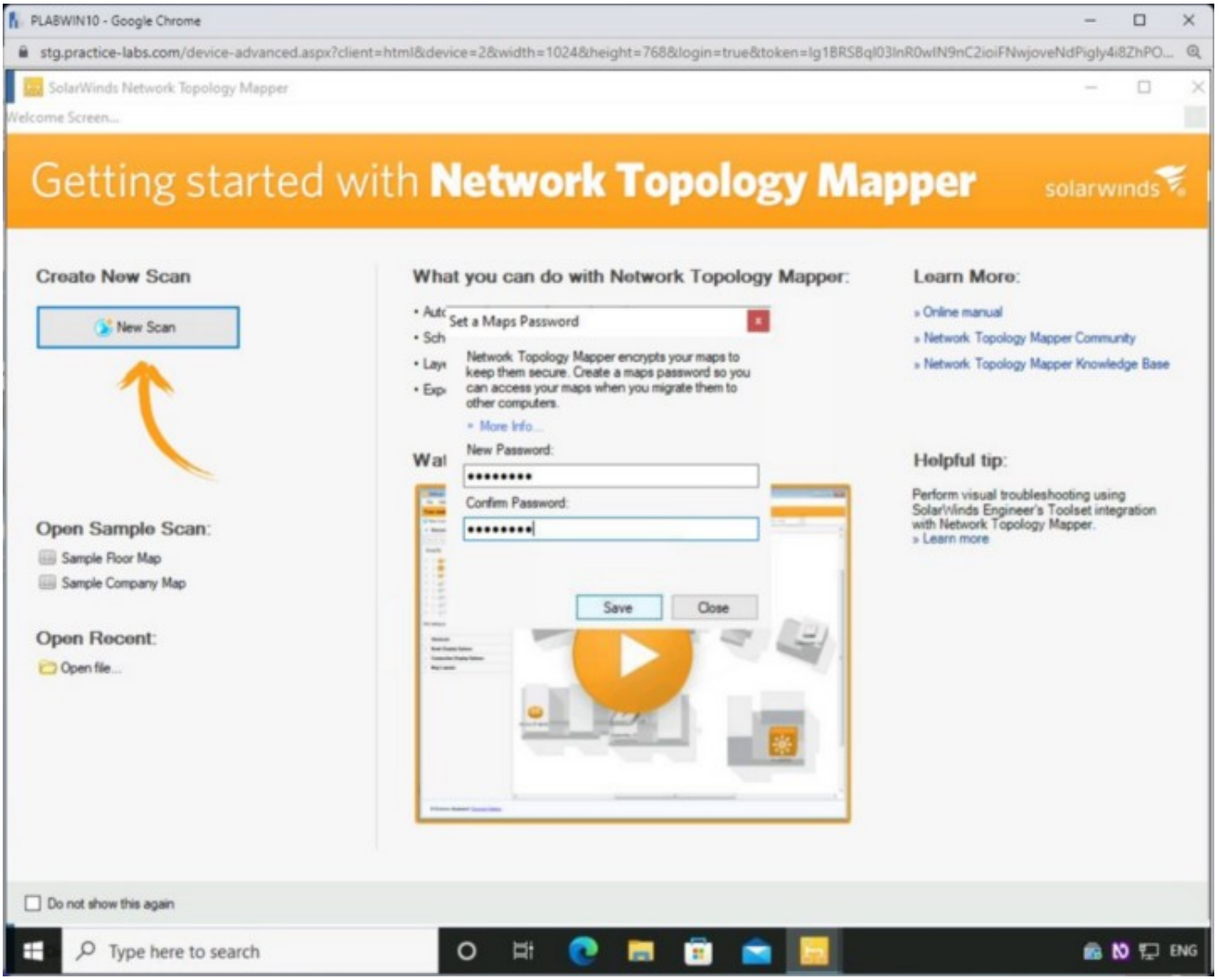
Step 5

The **Set a Maps Password** dialog box is displayed. In the **New Password** and **Confirm Password** text boxes.

Type the following password:

Password

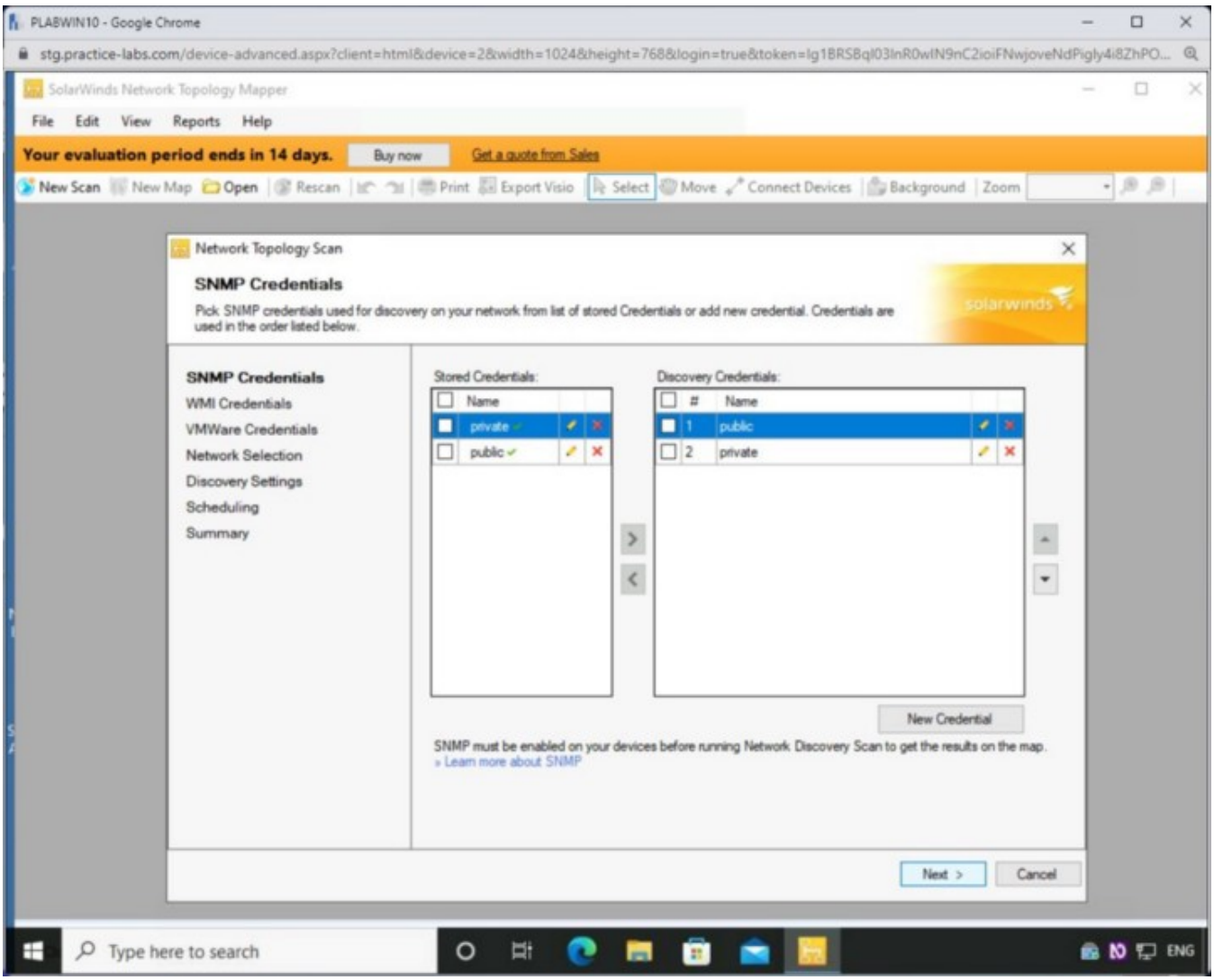
Click **Save**.



Step 6

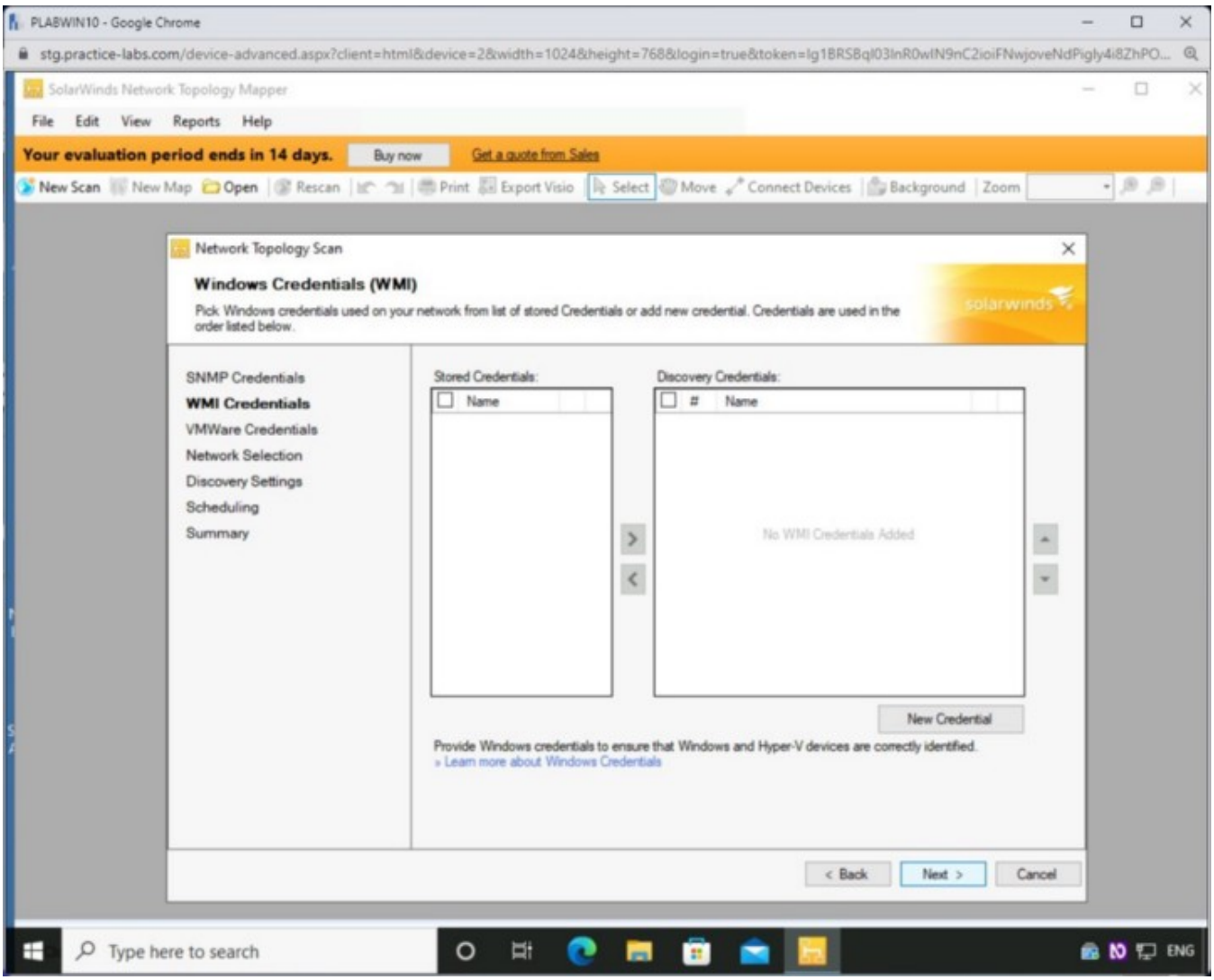
The **Network Discovery Scan** wizard is displayed.

Keep the default settings on the **SNMP Credentials** page and click **Next**.



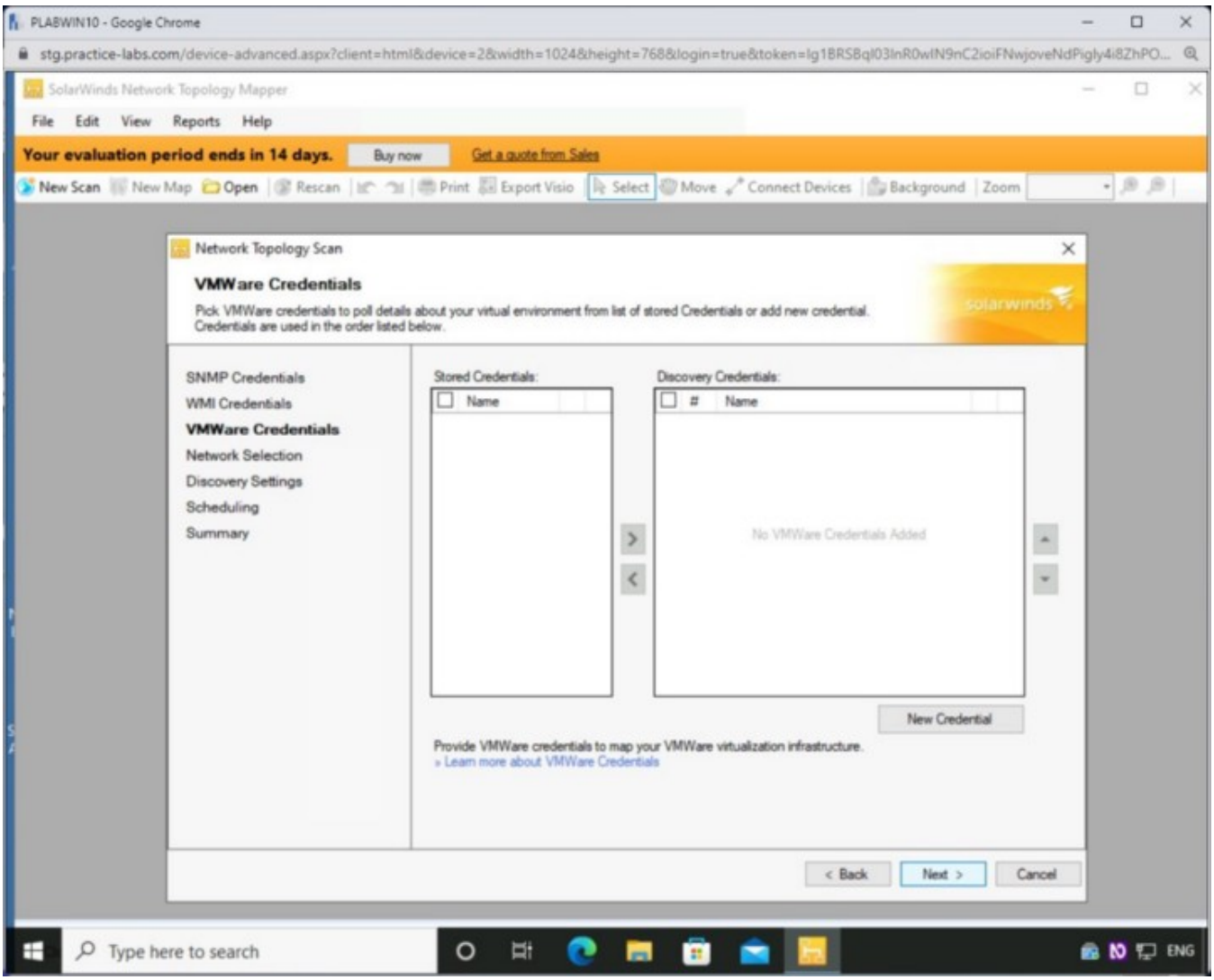
Step 7

On the **Windows Credentials** page, keep the default settings and click **Next**.



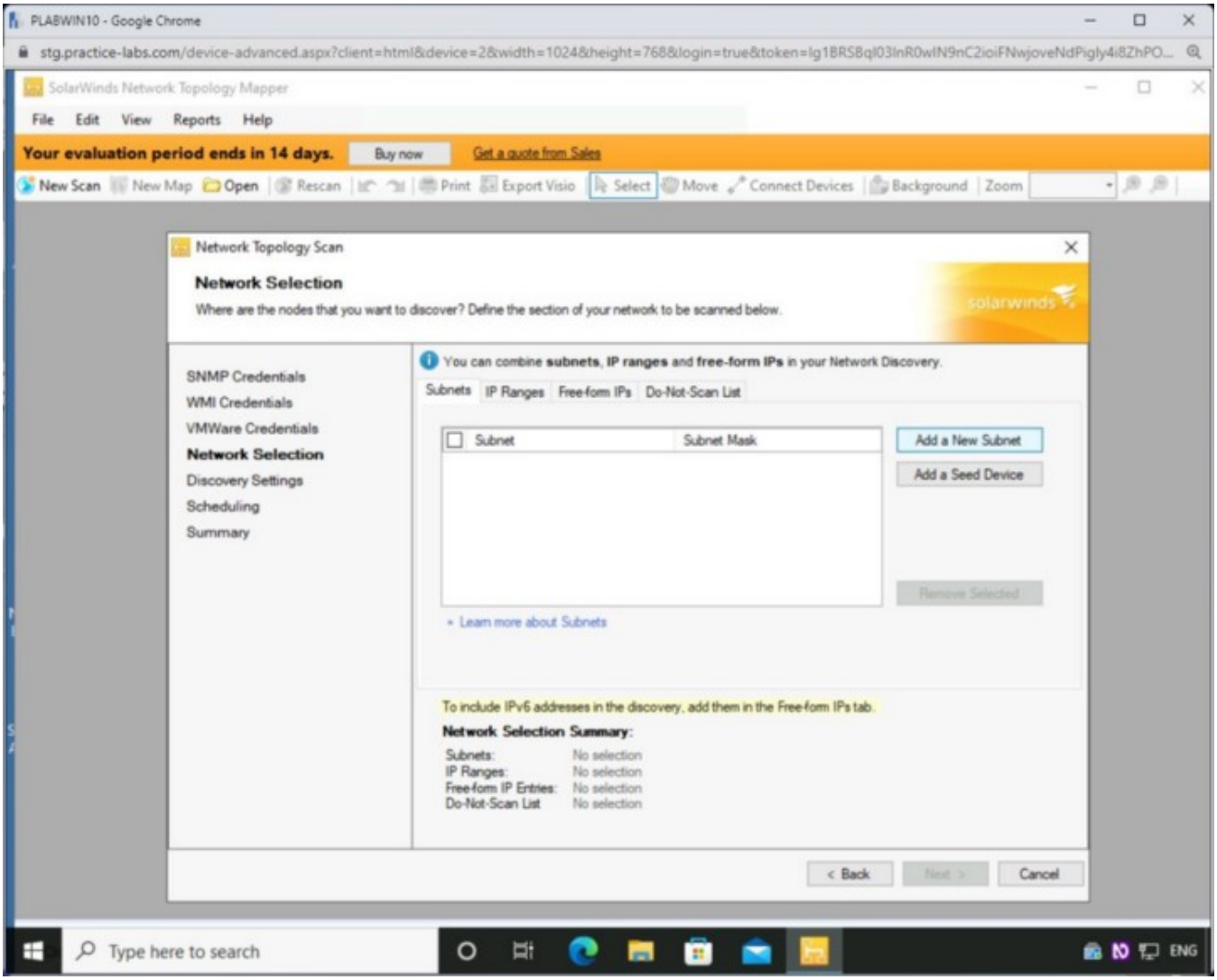
Step 8

On the **VMWare Credentials** page, keep the default settings, and click **Next**.



Step 9

On the **Network Selection** page, click **Add a New Subnet**.



Step 10

The **Add a New Subnet** dialog box is displayed.

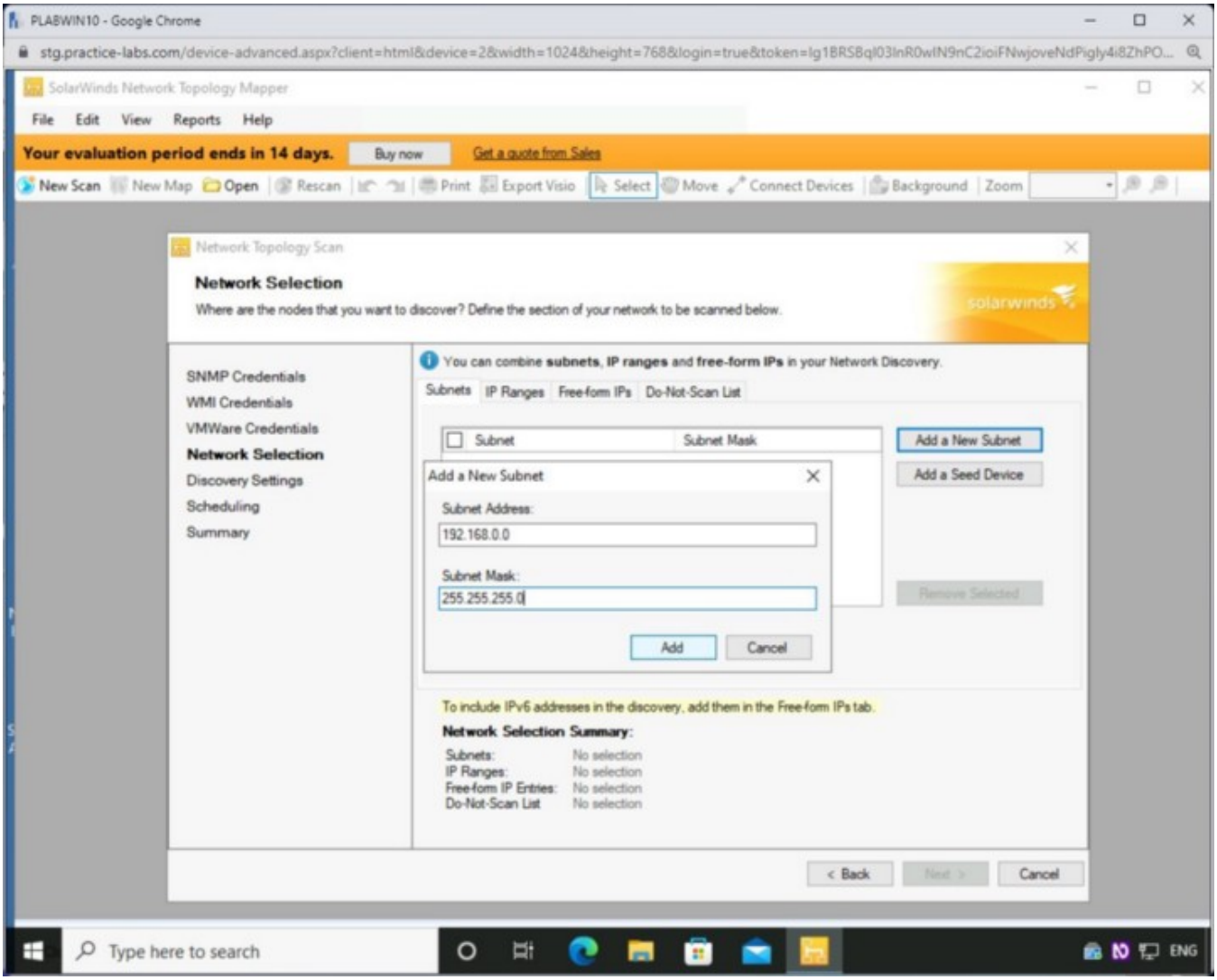
In the **Subnet Address** box, type the following:

```
192.168.0.0
```

In the **Subnet Mask** textbox, type the following:

```
255.255.255.0
```

Click **Add**.

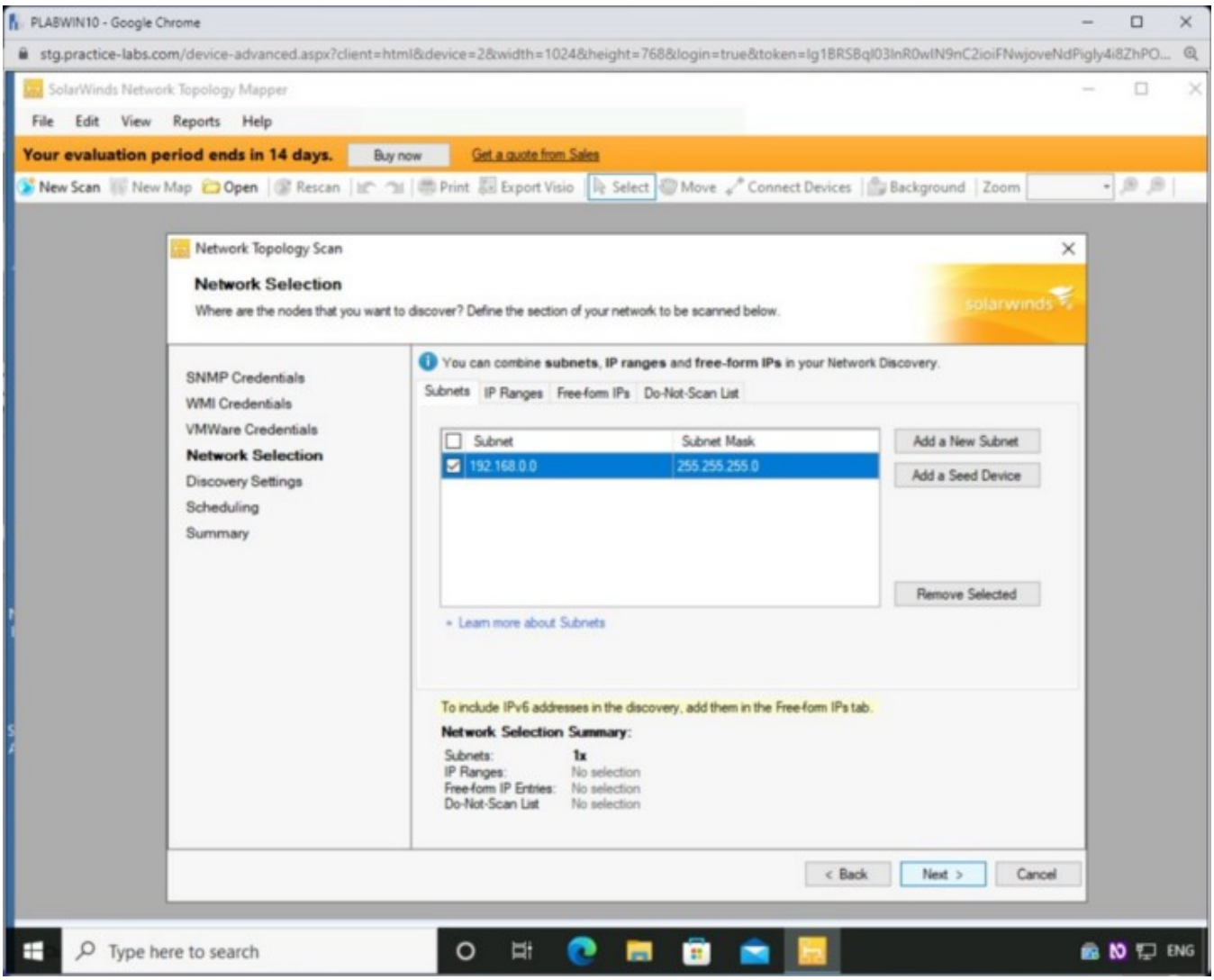


Step 11

Note that the new subnet is now added.

Select the **192.168.0.0** checkbox.

Click **Next**.



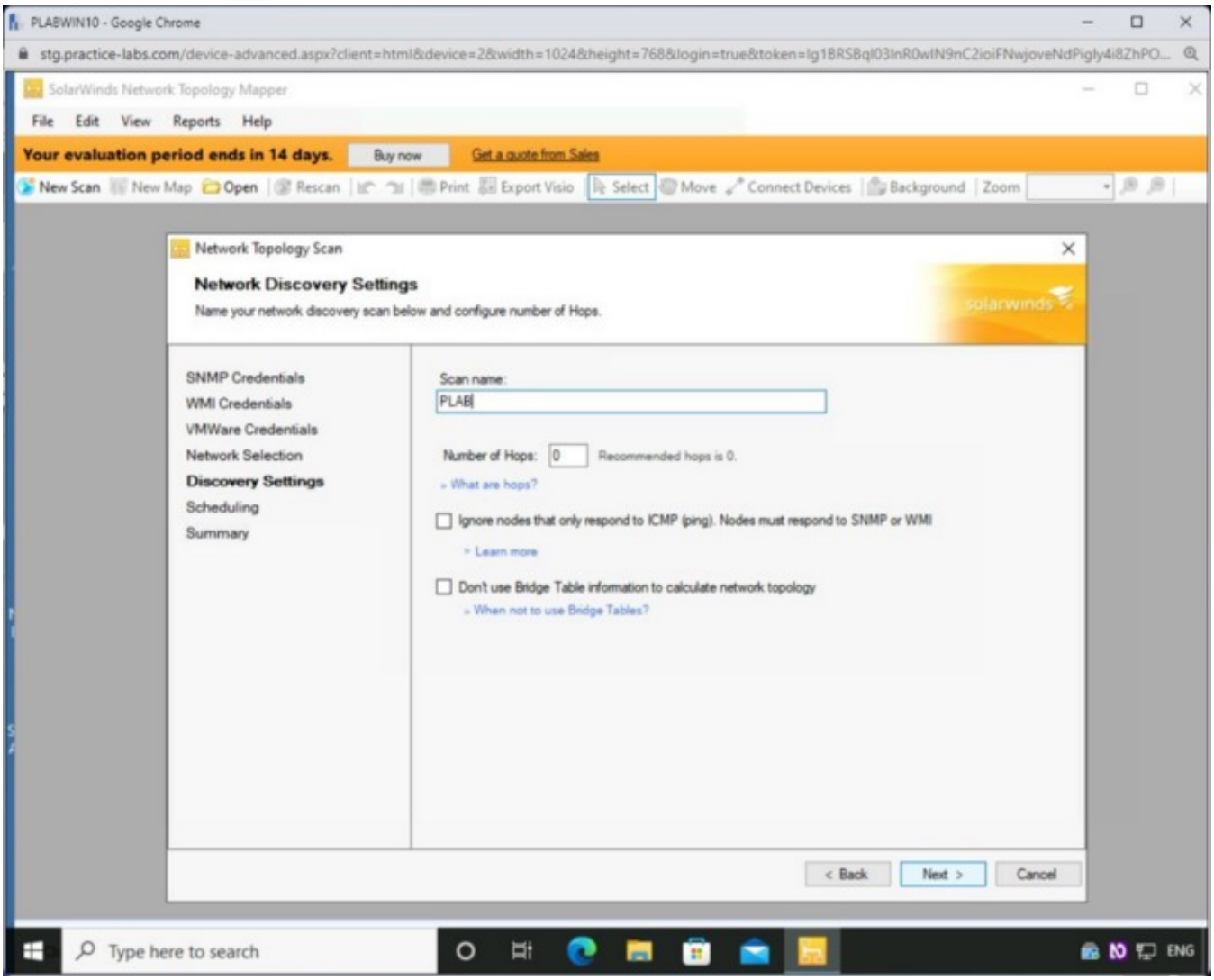
Step 12

On the **Network Discovery Settings** page, in the **Map name** textbox, type-over the given entry with the following:

```
PLAB
```

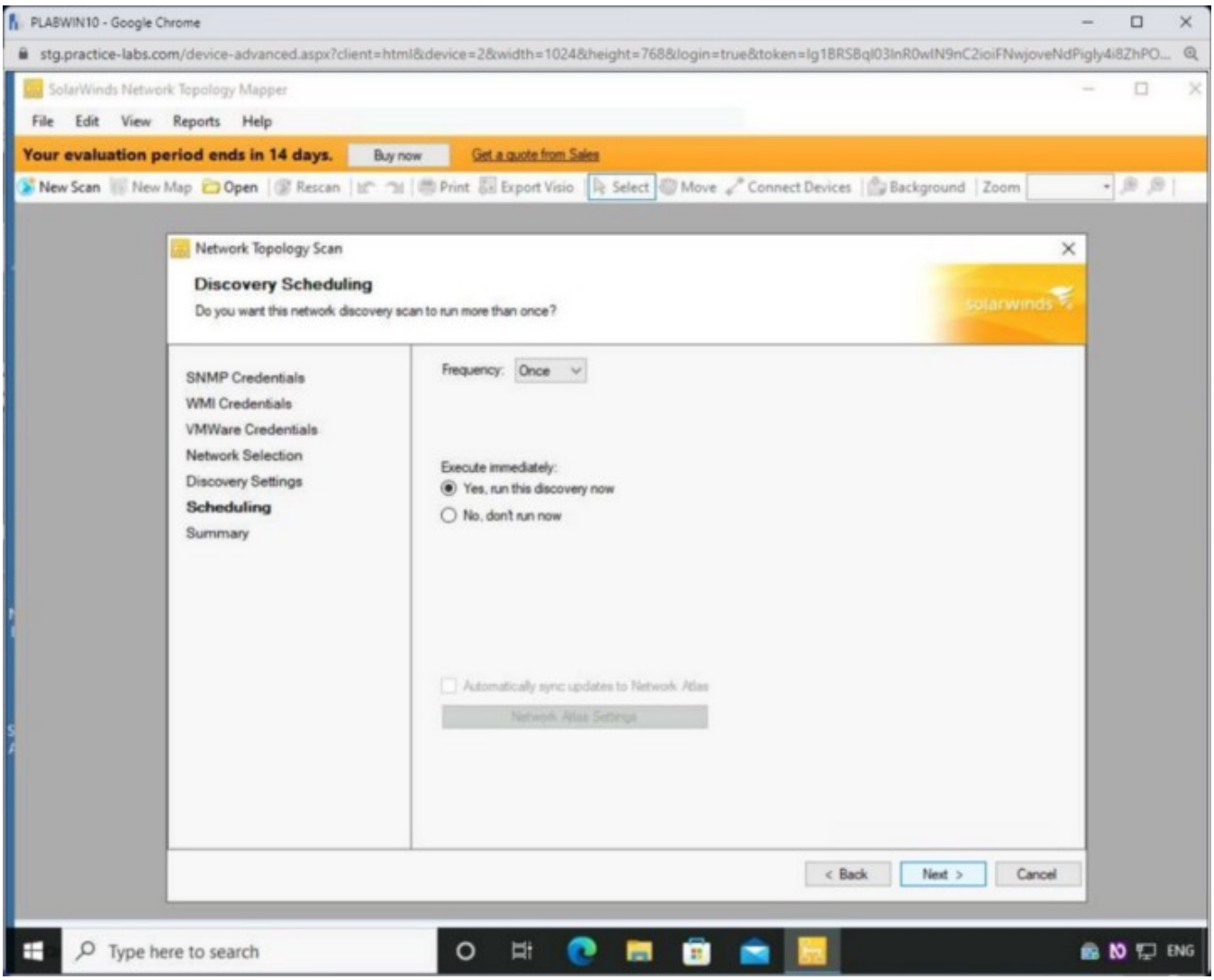
Click **Next**.

Note: *By default, the name will be added in the Map name textbox. It will use the naming convention Untitled_MM-DD-YYYY.*



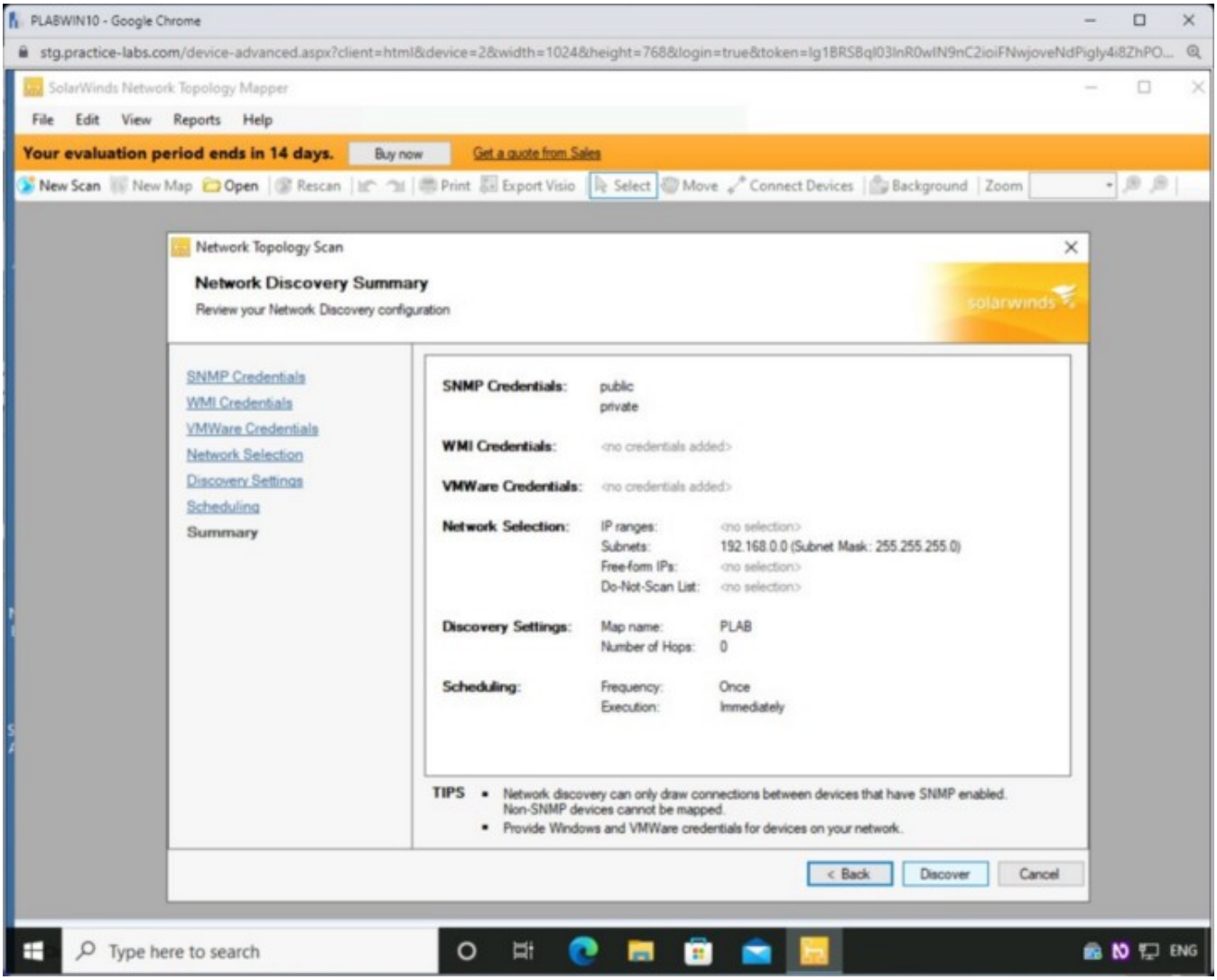
Step 13

On the **Discovery Scheduling** page, keep the default settings and click **Next**.



Step 14

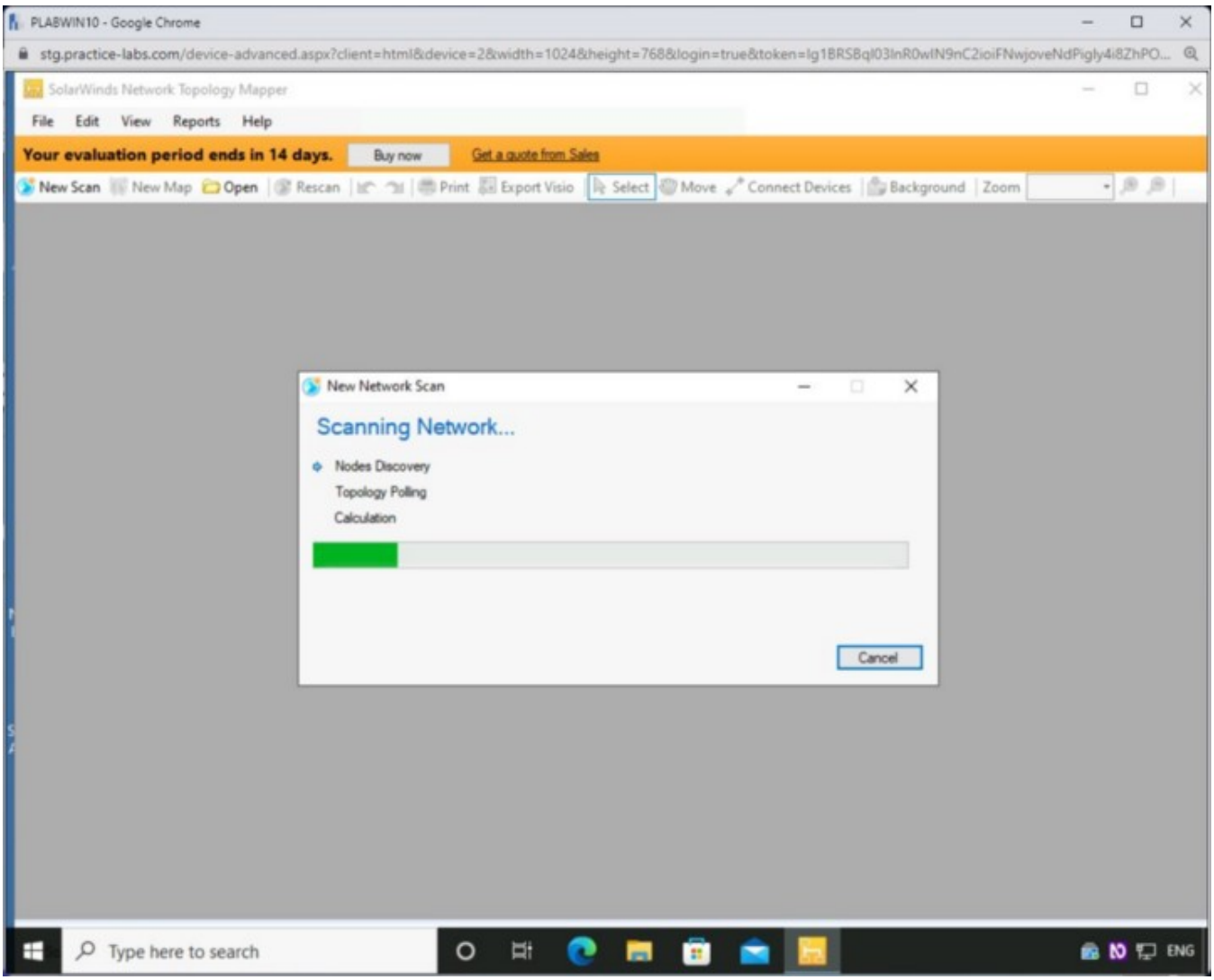
On the **Network Discovery Summary** page, review the configuration and click **Discover**.



Step 15

Network scanning is in progress.

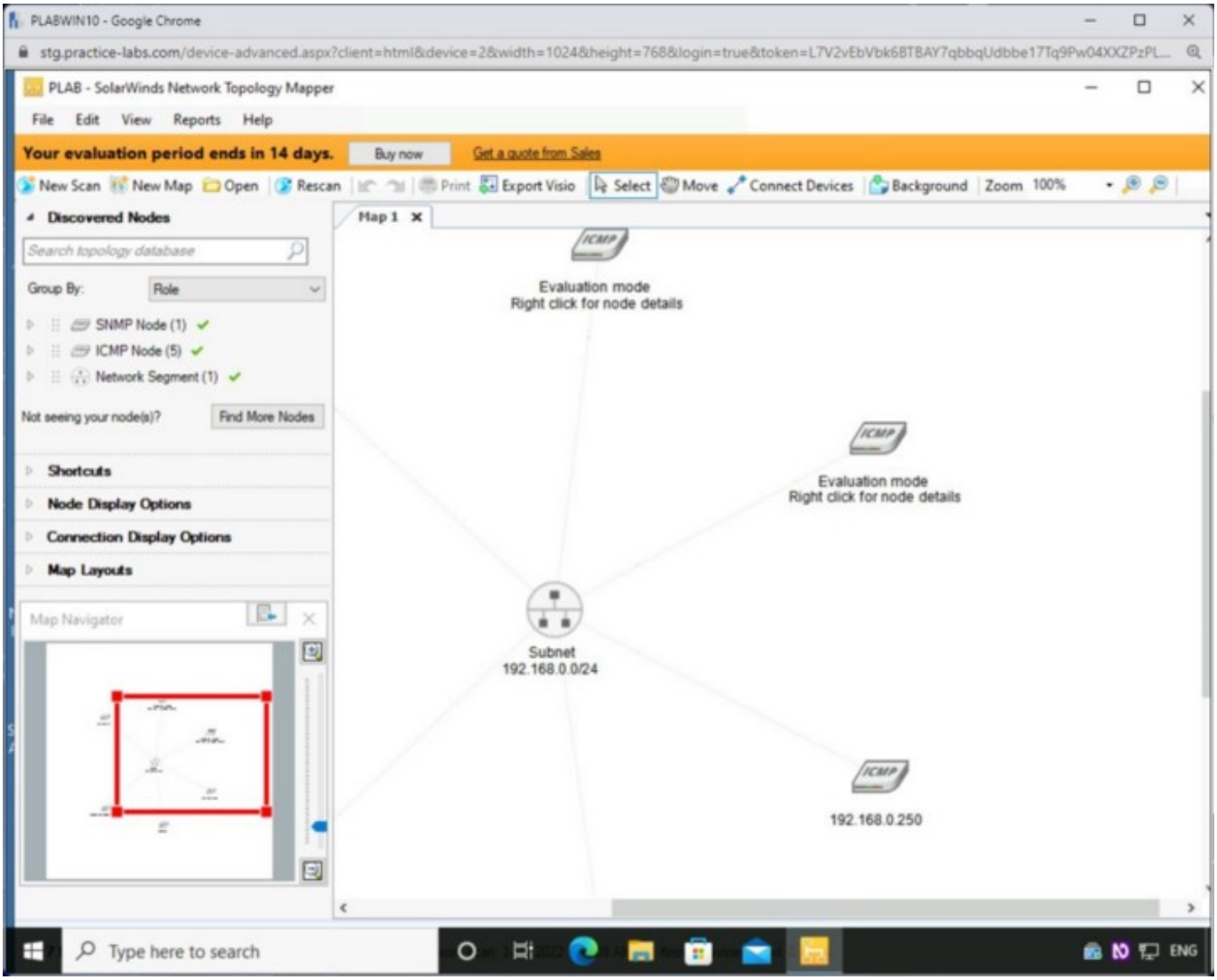
The **New Network Scan** dialog box is displayed. This will take a few moments.



Step 16

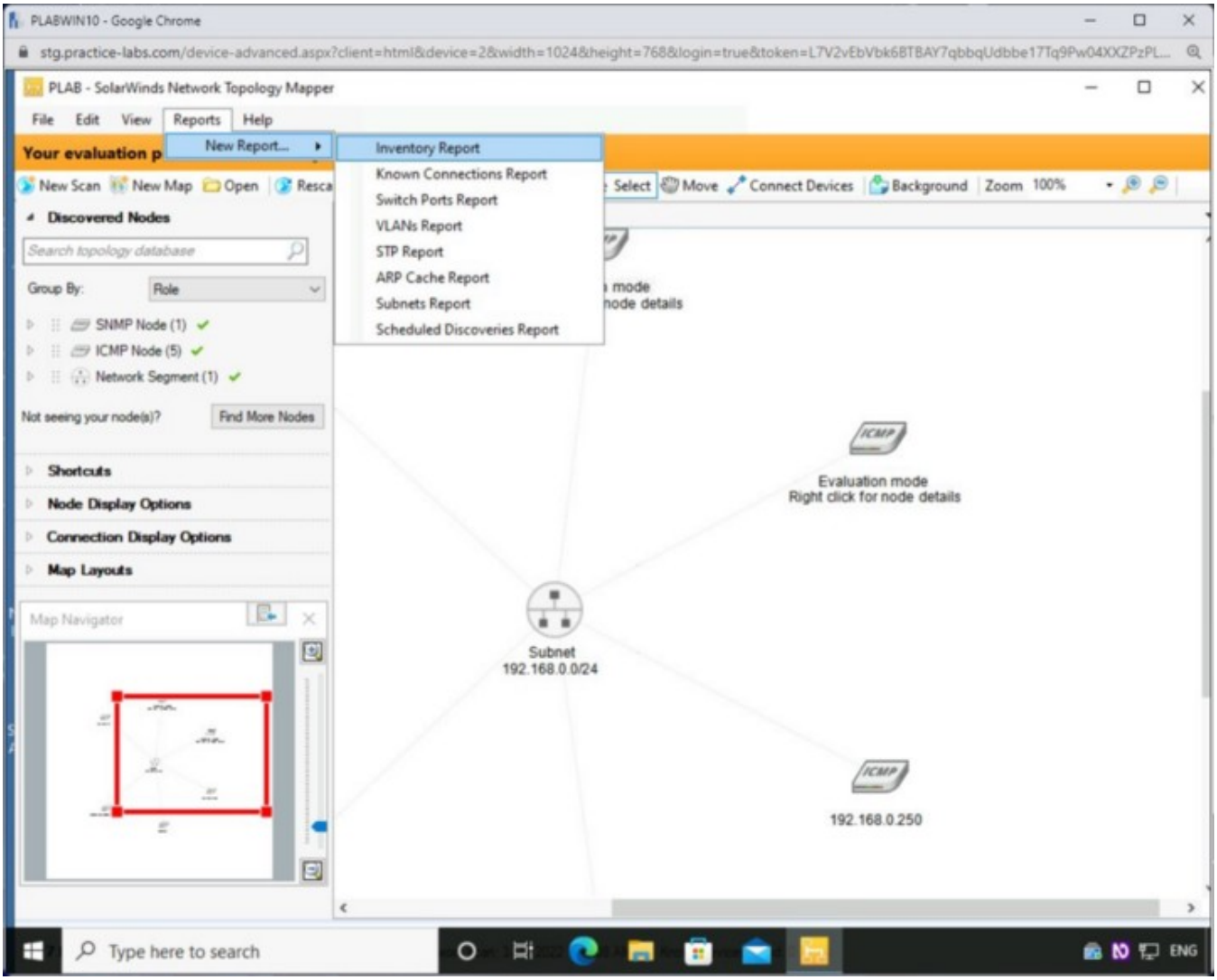
When the scan is complete, the **Map Navigator** dialog box is displayed. It allows you to control the size of the map.

With the **Map Navigator**, you will also see the **Map1** tab in the right pane. It displays the map of the devices that are found.



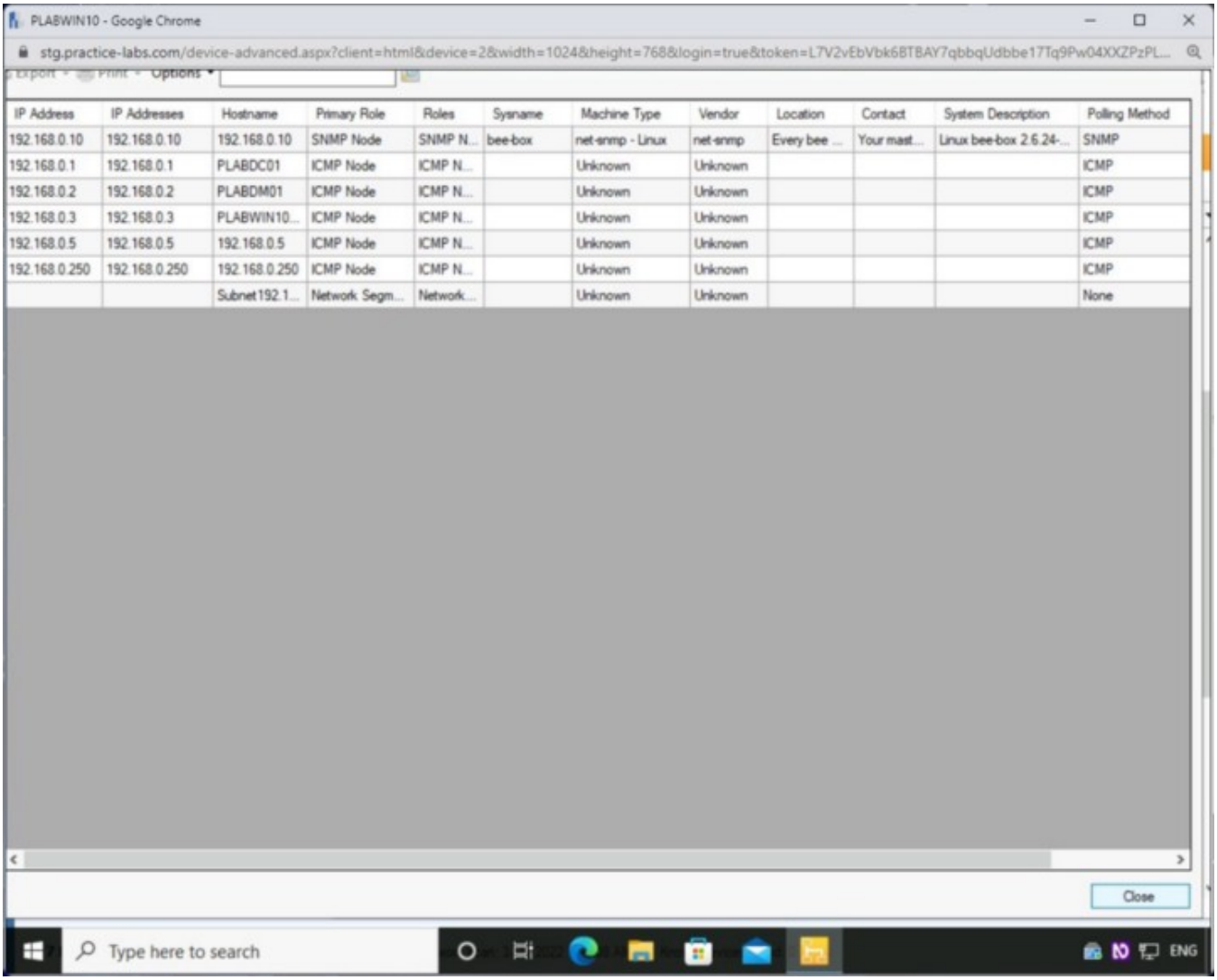
Step 17

You can also create several reports. Click **Reports**, select **New Report**, and then select **Inventory Report**.



Step 18

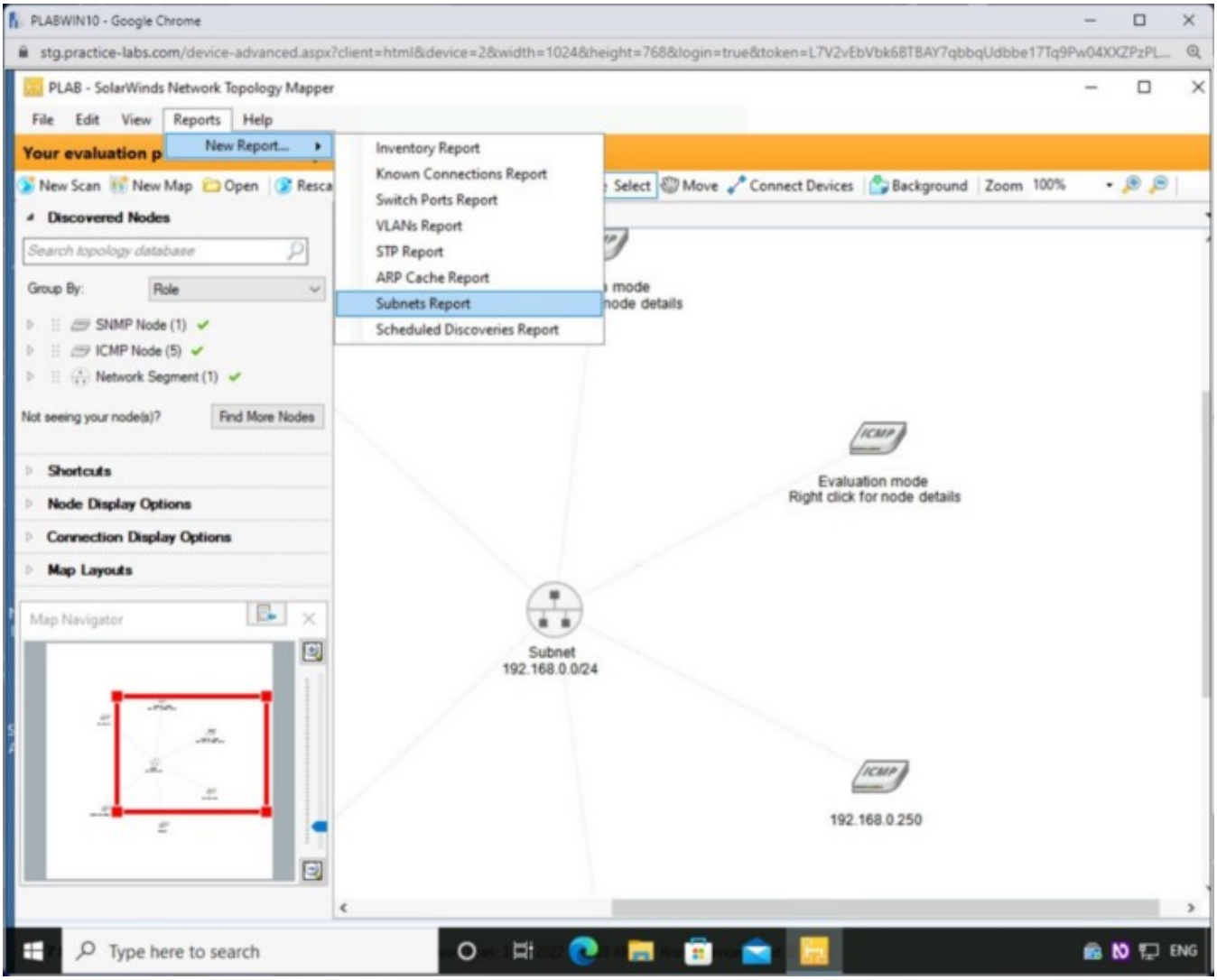
The **Inventory Report** is now displayed. Click **Close**.



Step 19

You can also view the subnet information.

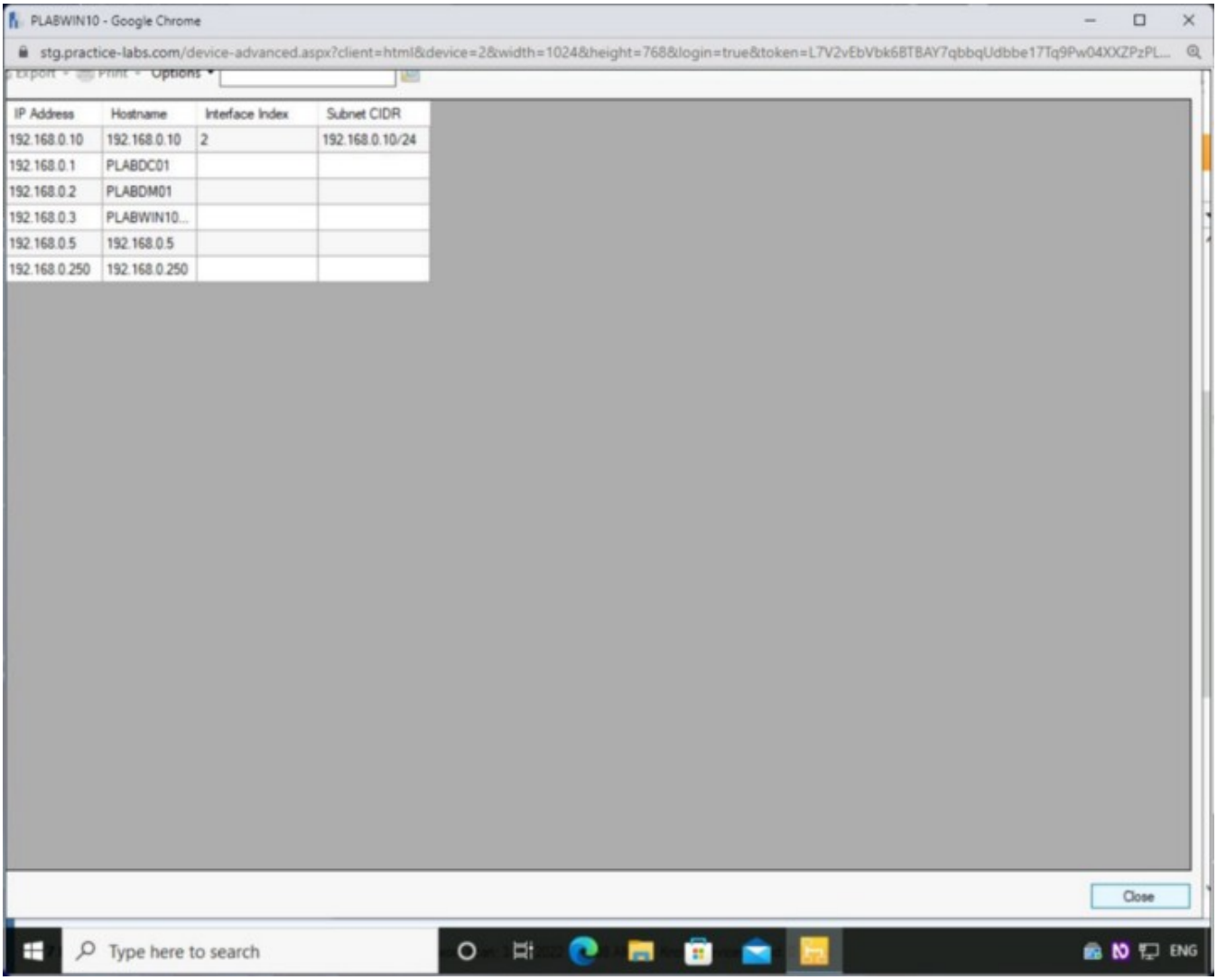
Click **Reports**, select **New Report**, and then select **Subnets Report**.



Step 20

All present devices on the network are displayed.

Click **Close**.



Close the **SolarWinds Network Topology Mapper** window.

Task 3 — Use the Advanced IP Scanner

Advanced IP Scanner allows you to scan a network to determine the machines available.

In this task, you will use the network scanner, which is Advanced IP Scanner.

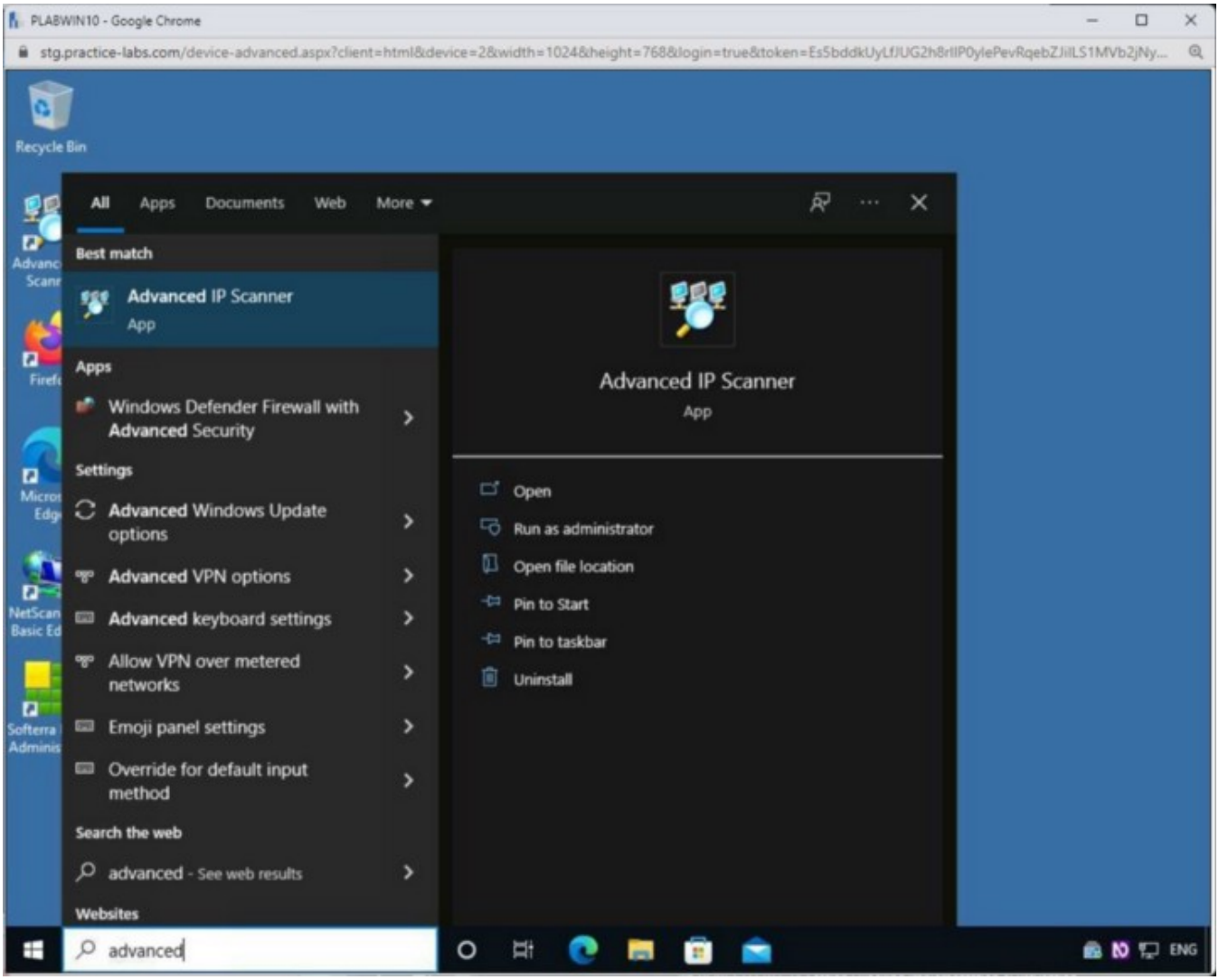
Step 1

Connect to **PLABWIN10**.

In the **Type here to search** textbox, type the following:

```
advanced
```

From the search results, select **Advanced IP Scanner**.



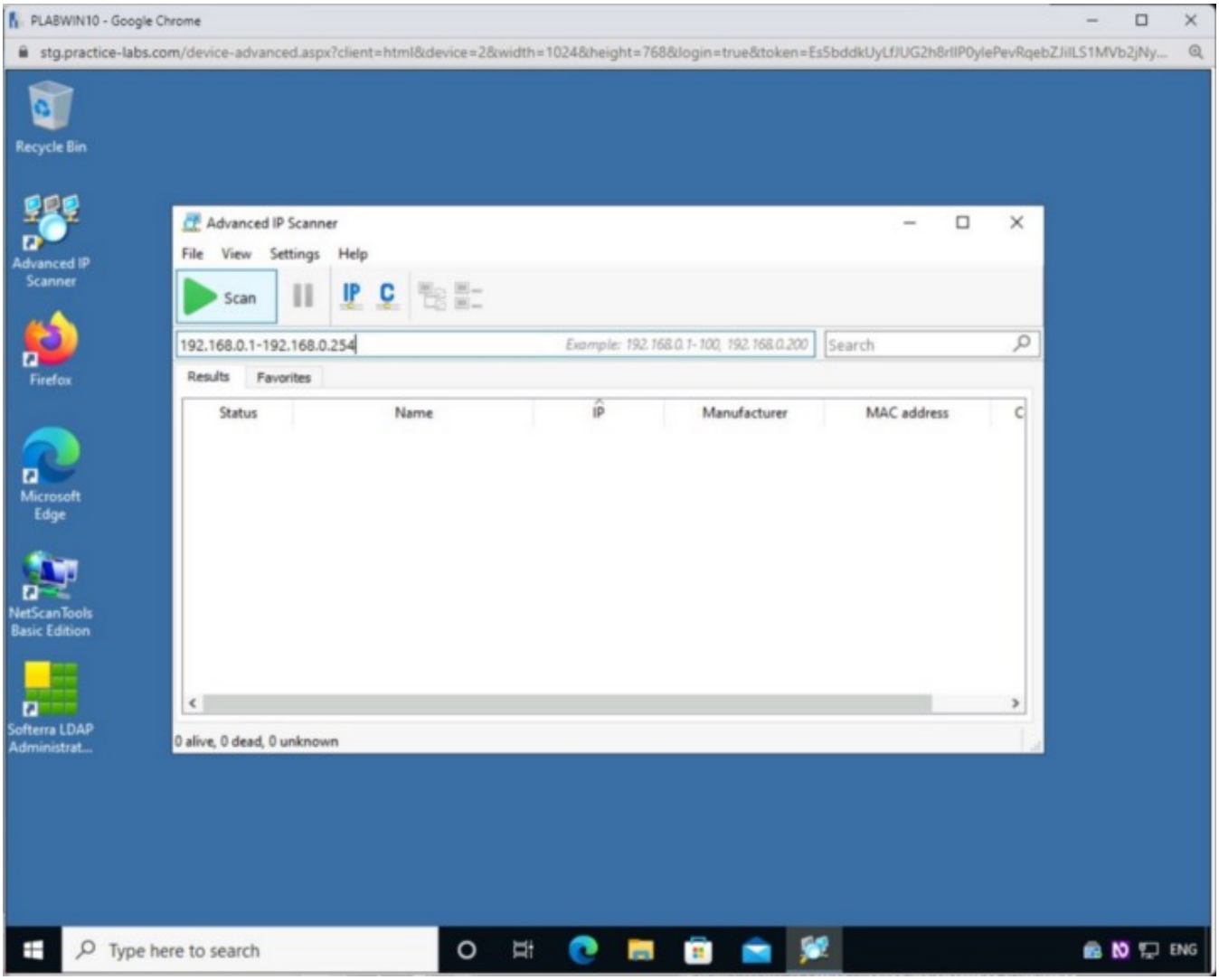
Step 2

The **Advanced IP Scanner** window is displayed. Note that a default IP address range is already defined in the drop-down. If your network uses the same range, you can simply click Scan or change the IP address range.

For this task, only the following address range must be present:

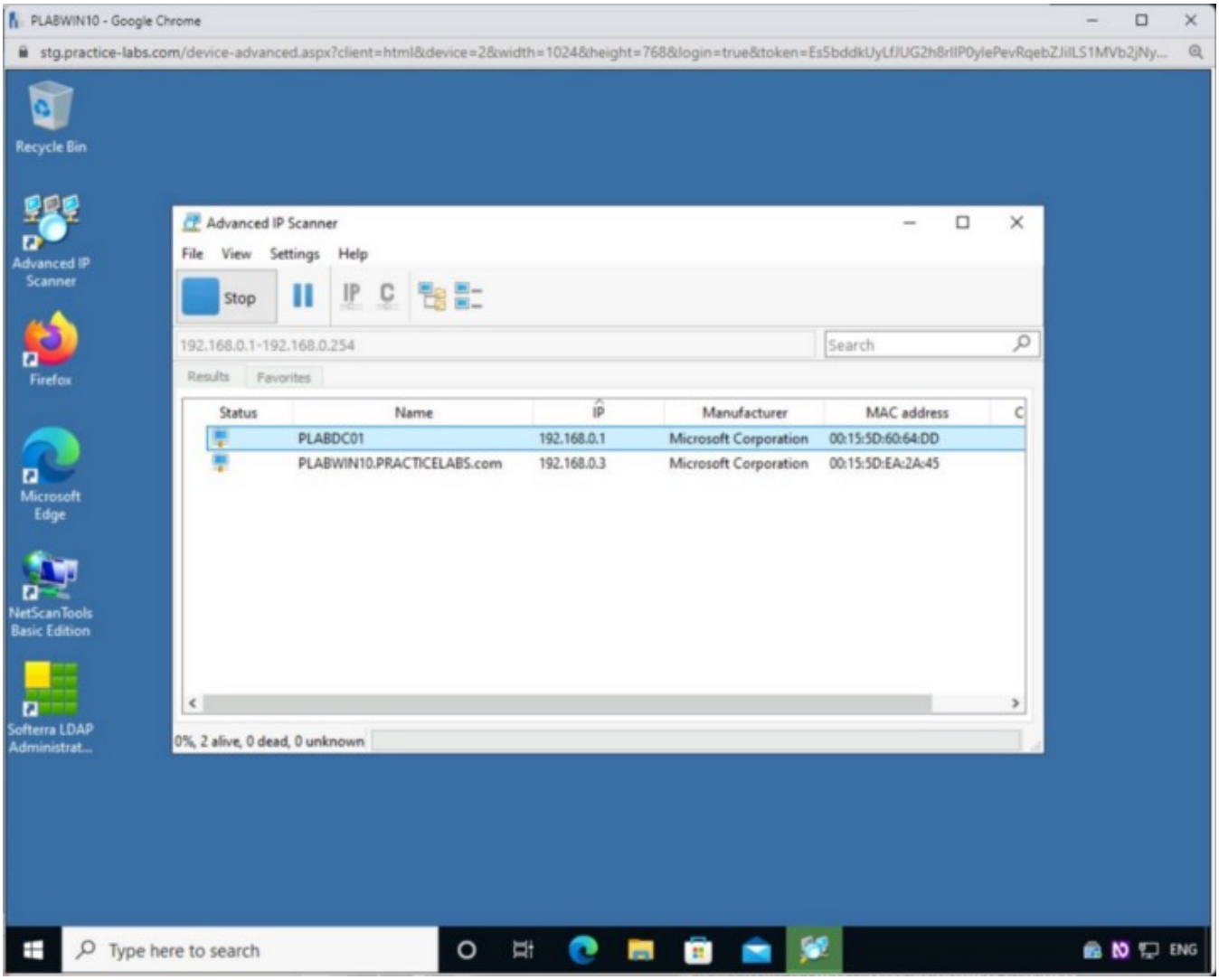
```
192.168.0.1-192.168.0.254
```

Click **Scan**.



Step 3

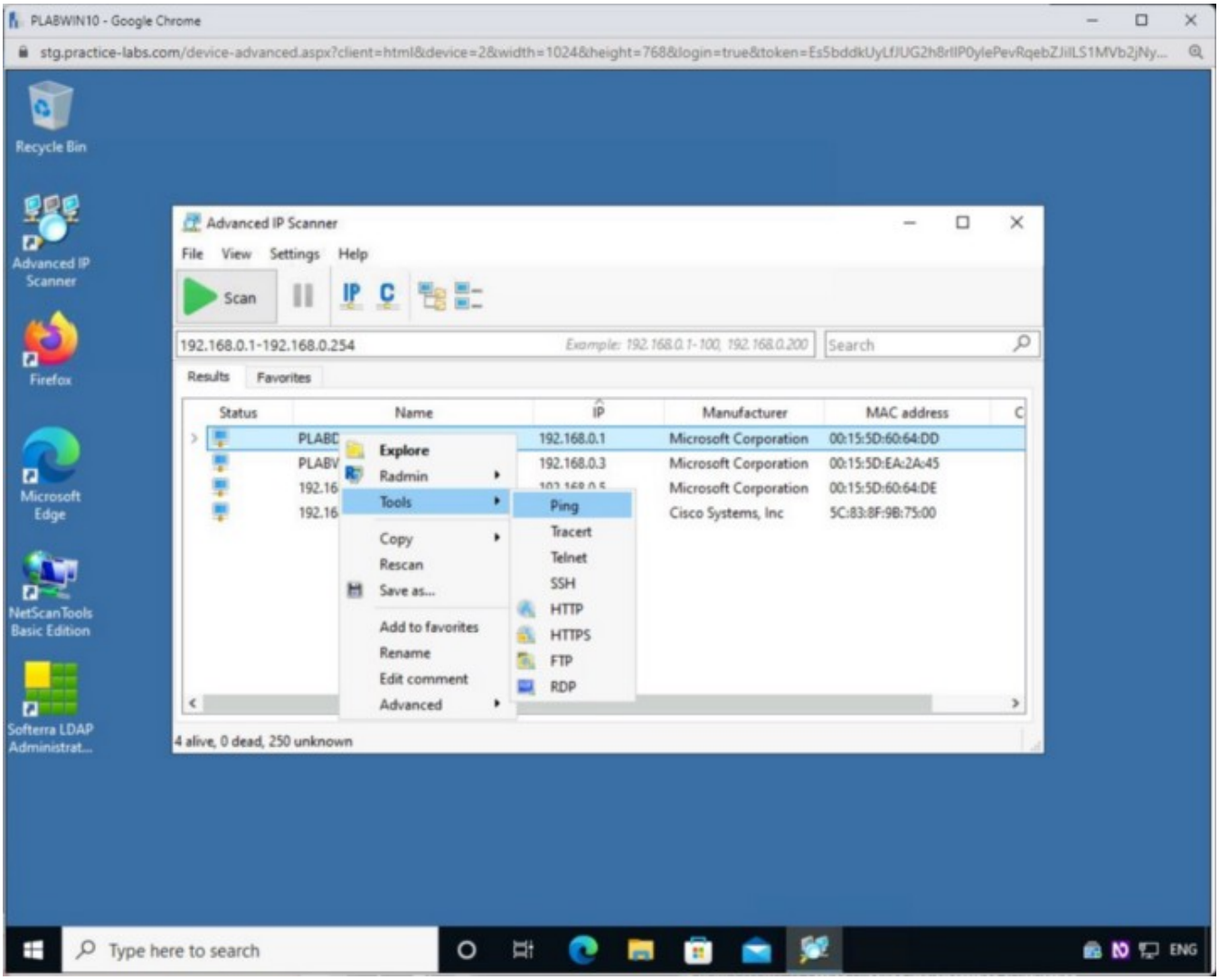
The scanning process starts.



Step 4

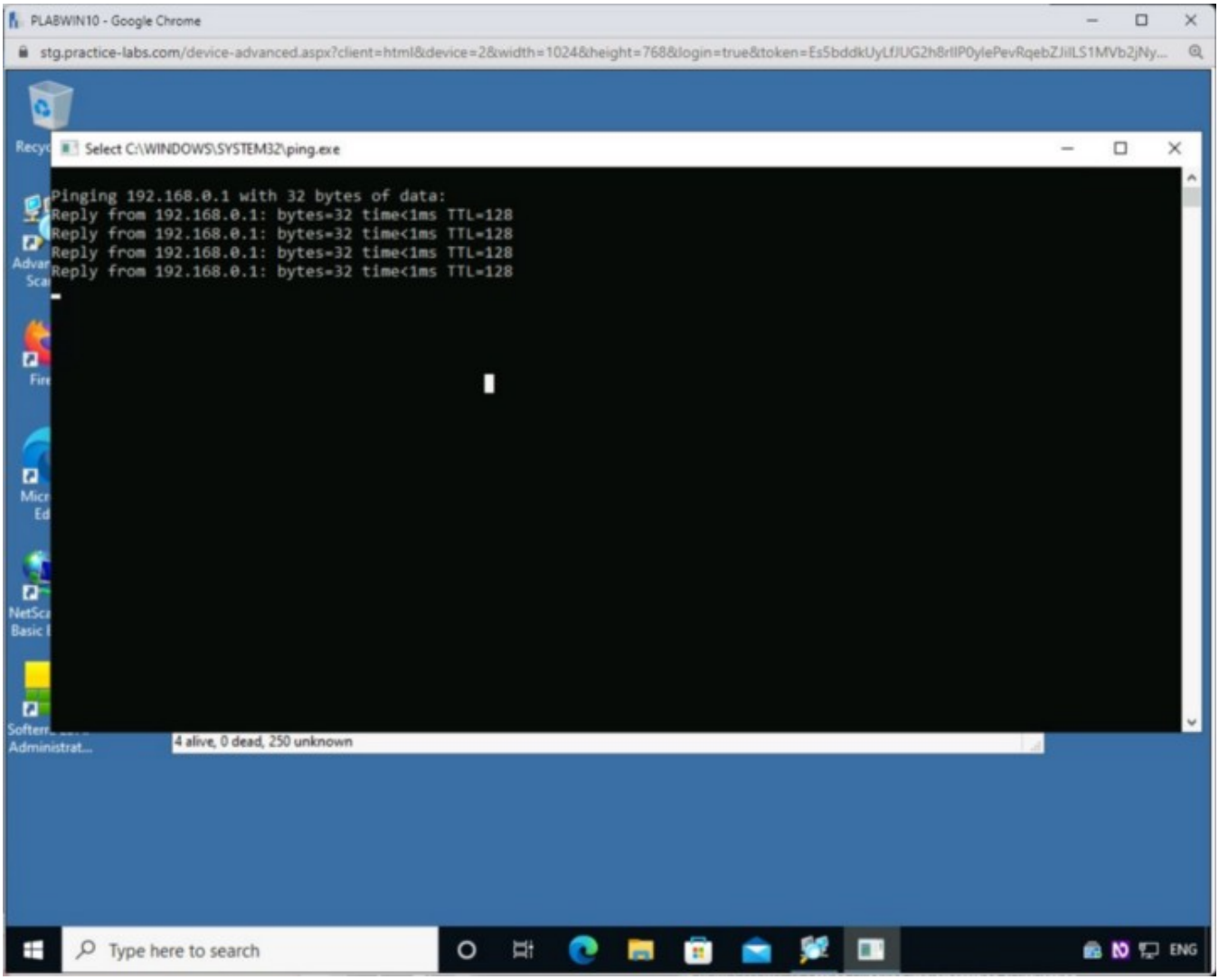
Note that several systems are detected on the subnet.

Right-click **PLABDC01**, select **Tools,** and then select **Ping**.



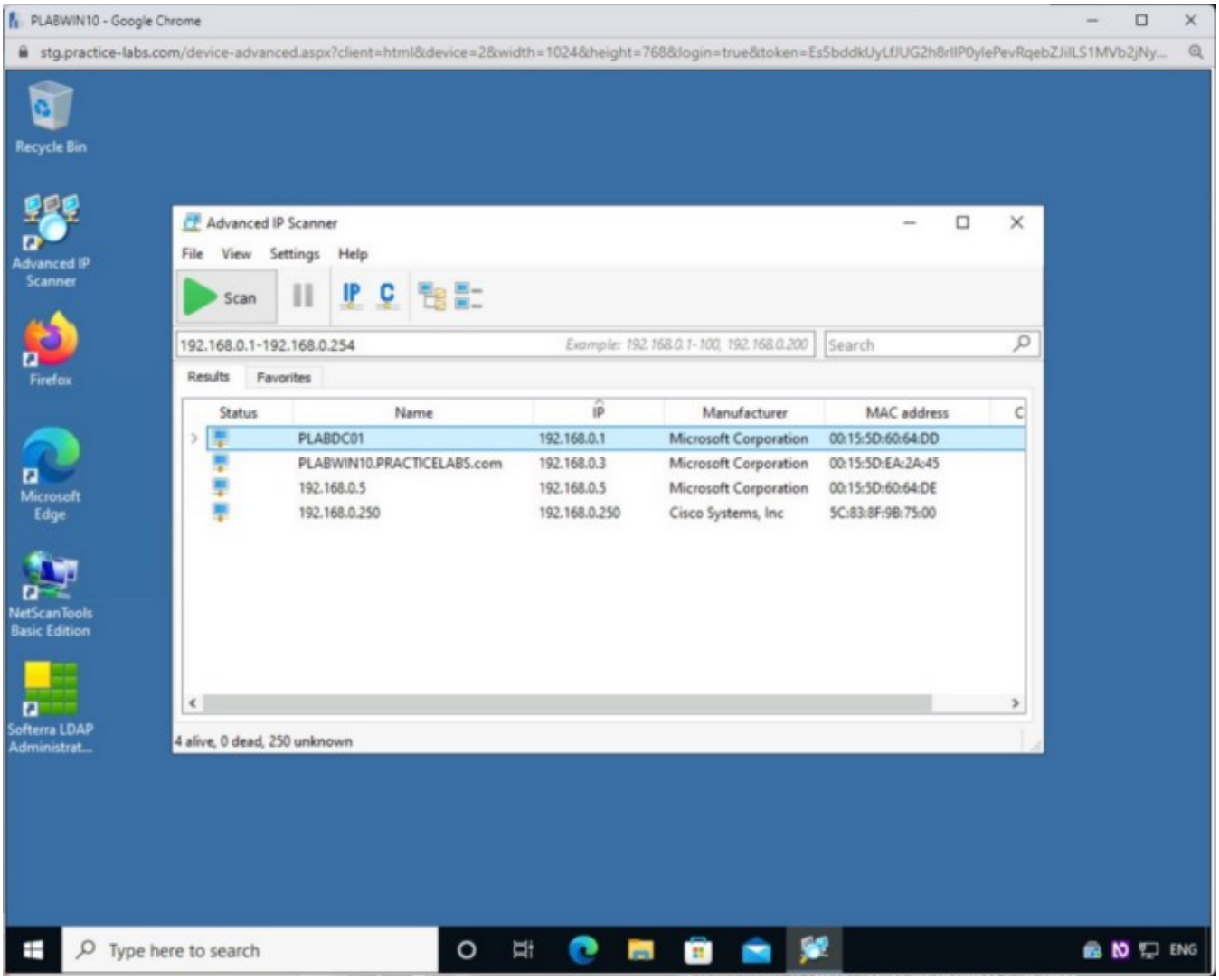
Step 5

Note that a command prompt window opens. The ping command is executed.



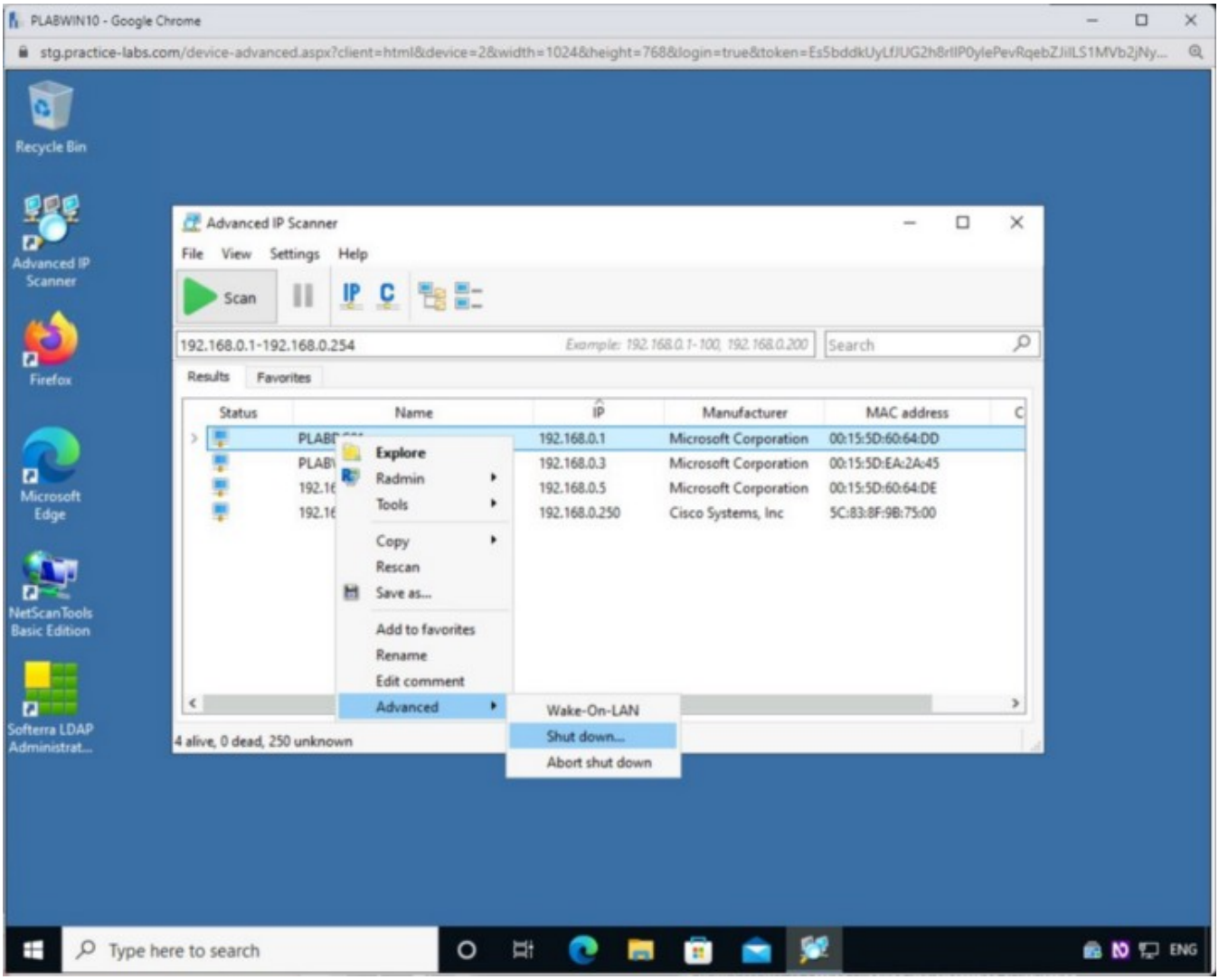
Step 6

Press **Ctrl + C** to terminate the ping command. The command prompt window closes automatically. You are back on the **Advanced IP Scanner** window.



Step 7

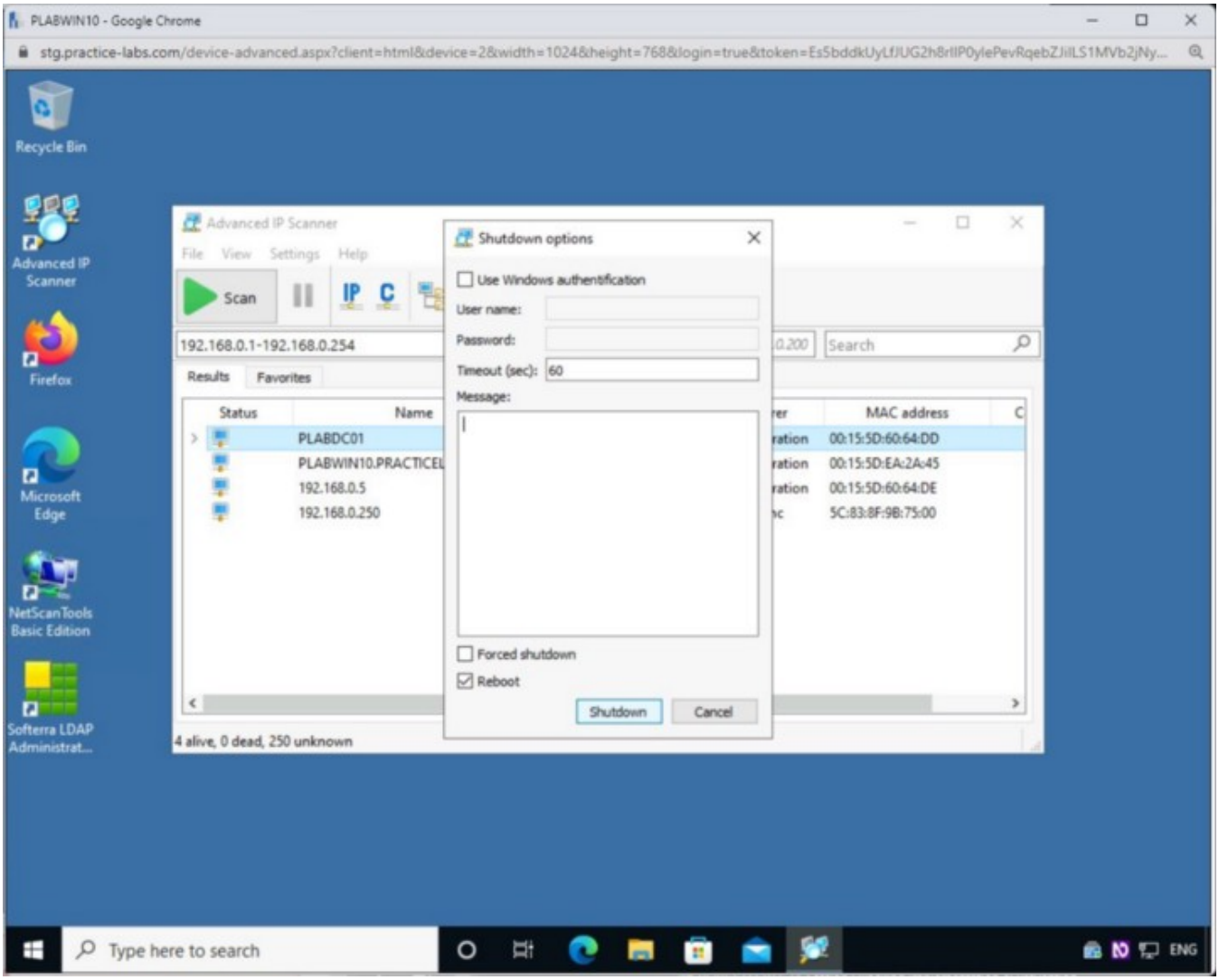
Right-click **PLABDC01**, select **Advanced** and then select **Shutdown**.



Step 8

The **Shutdown options** dialog box is displayed.

Select **Reboot** and then click **Shutdown**.



Step 9

The **Shutdown results** dialog box is displayed. It shows **Succeeded** message.

3

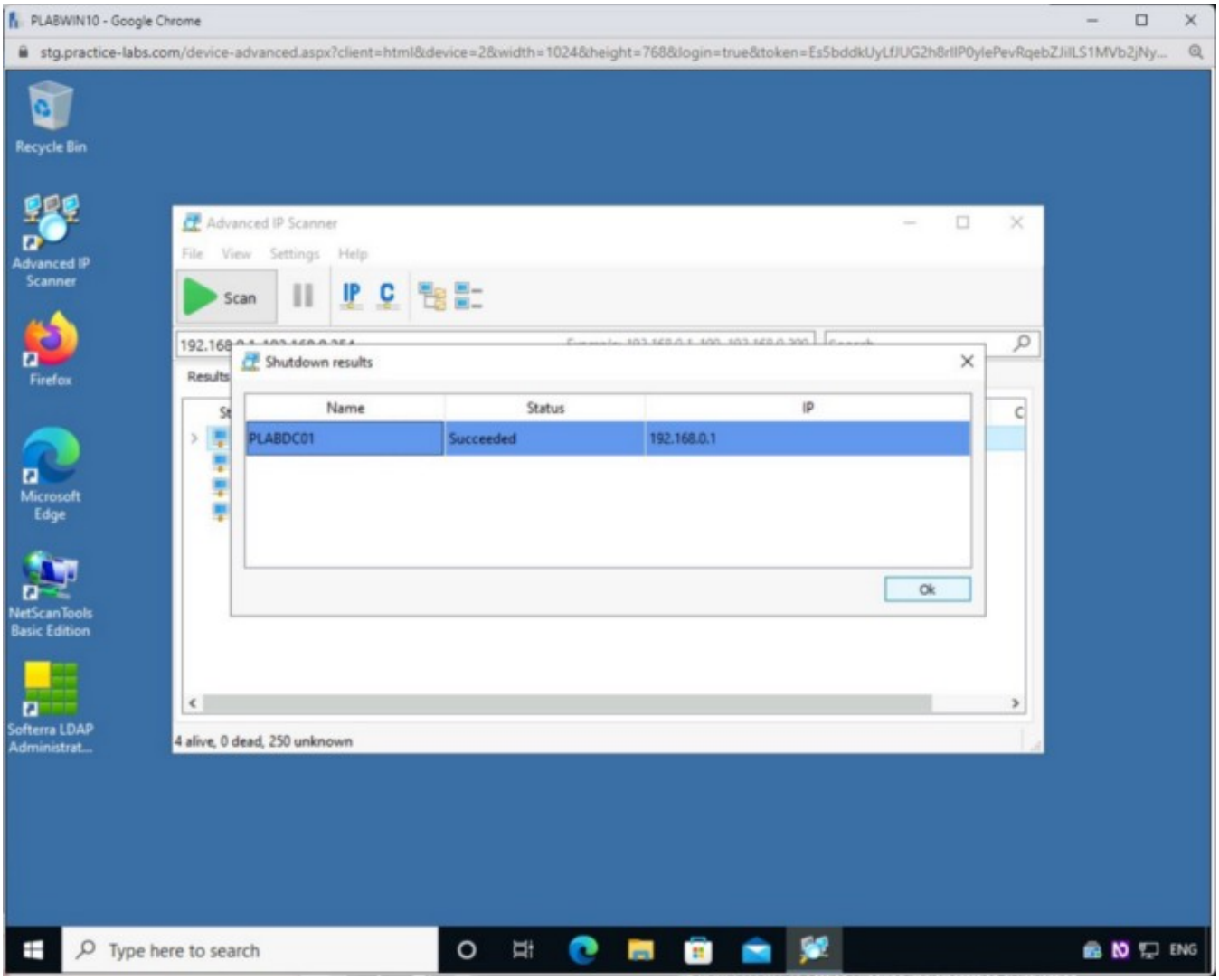
Screenshot

Click the button to take a screenshot of PLABWIN10

Take screenshot

3 of 9

Click **Ok**.



Close the **Advanced IP Scanner** application and proceed to the next exercise.

Exercise 4 — Footprinting through Social Engineering

Social engineering is a process that an attacker uses to gain confidential knowledge in an attack. An attacker first gains the victim's confidence and convinces the victim to provide the required information. When social engineering is being conducted, the victim is unaware of it and provides the required information.

The variety of information that an attacker may want is as follows:

- Personal information, such as social security number or user credentials
- Organizational information, such as email ID and phone numbers
- Technical information, such as software and operating system versions, IP addresses, and network architectures

In this exercise, you will learn about the footprinting methods using social engineering.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- The Social Engineering Methods

Your Devices

This exercise contains supporting materials for **Ethical Hacker v11**.

Social Engineering Methods

An attacker can use a variety of methods to conduct social engineering. The end goal of each method is to get the required information. Some of the common methods used in social engineering are as follows:

Shoulder Surfing

Shoulder surfing is a social engineering attack performed by looking over the victim's shoulder to retrieve a credit card number, password, or other pertinent information. An attacker directly observes the information entered by the victim by standing very close or behind the victim or using vision-enhancing aids or binoculars to observe from far. Shoulder surfing attackers also use the technique of fixing up closed-circuit cameras hidden behind the wall or ceiling to obtain sensitive information.

Dumpster Diving

Dumpster diving is another social engineering attack that uses physical access to vulnerable information. Documents sent to a company's dumpster or recycling bins may contain highly sensitive information. Attackers screen those documents carefully to get valuable information. An attacker may target the papers and electronic media, or anything that can be useful to them.

Depending on the attack, attackers can look for the following information:

- User IDs
- Passwords
- Phone numbers
- E-mail IDs
- Bank account numbers

- Critical process and procedural information

As part of penetration testing, you should look for the information mentioned above in a pile of documents that are considered junk. Users often print critical and confidential documents that are never collected and end up on a paper pile near the printer or in the dust bin.

For confidential information stored on hard drives, there are specialist shredders that can be used and trusted disposal services. Alternatively, a data wipe can be performed on the hard drives before disposal.

Impersonation

Using impersonation, an attacker can pretend to be legitimate and trick the individual into getting the information they are looking for.

An attacker can pretend to be a law enforcement officer, a technical support professional, or anyone who can fit into that situation.

Eavesdropping

Eavesdropping is the process of listening or capturing some form of communication between people without their consent. An attacker can gather this information by tapping phones, intercepting audio, video, or written communications as well as simply being in earshot of two people and hearing / recording what they are saying.

Note: *Social Engineering will be covered in more detail in a future module.*

Key Footprinting Countermeasures

Even though you can apply several countermeasures in one go, not all may be effective. While countermeasures are used for security reasons, they can also add complexities in the network environment. Therefore, you should implement only what is necessary.

Some of the key countermeasures that you can use are:

- Perform footprinting to see what is visible to an external entity, such as an attacker
- Disable unnecessary ports and services
- Configure a firewall to lockout ports that are not required
- Configure webservers to use only required ports and disable the remaining ports
- Configure an intrusion detection system (IDS) to filter traffic and look for Footprinting patterns
- Enforce security policies on systems
- Educate users about the security policies and various attacks, such as social engineering
- Disable directory listings on the Webservers
- Use separate internal and external DNS servers
- Use TCP/IP and IPsec filters
- Configure Webservers to disable banner