# CEH v12 Lesson 2 : Network Resource Discovery Methods

## Learning Outcomes Part 1

In this module, you will complete the following exercises:

- Exercise 1 — Network Scanning Concepts and Scanning Tools
- Exercise 2 — Host Discovery
- Exercise 3 — Port and Service Discovery

After completing this module, you will be able to:

- Use Hping3 for Network Scanning
- Perform a TCP Scan Using Dmitry
- Perform Stealth Scanning Using Nmap
- Use fping for Network Scanning
- Explore a Network Using Zenmap
- Use MyLanViewer to Scan a Network
- Using Msfconsole to Perform TCP Stealth on a Network
- Identify Live Hosts on a Network
- Perform Discovery Scans
- Scan for Open Ports and Services
- Perform Port Scanning
- Perform Service Probing
- Use Netcat for Port Scanning

## Lab Duration

It will take approximately **1 hour and 30 minutes** to complete this lab.

## Exercise 1 — Network Scanning Concepts and Scanning Tools

Network scanning helps you determine hosts and systems running on a network. You can determine hosts and ports, services, and even applications running on said hosts.

An attacker can decide the target and the type of attack to conduct. Based on the information an attacker gathers, the next point of action for the attack can be determined.

Several Windows-based network scanning tools are available. Some key examples are:

- ID Serve
- CurrPorts
- Nmap
- MyLanViewer
- NetView
- Amap
- Netscan Tools Pro
- LANSurveyor
- Friendly Pinger
- Global Network Inventory

It is important to understand that some tools work similarly, such as discovering live systems on a network. On the other hand, some tools, such as ID Serve, have a distinct function, such as scanning a Webserver and extracting its configuration information.

In this exercise, you will learn to use some of the key network scanning tools and also the concept of network scanning.

### Learning Outcomes

After completing this exercise, you will be able to:

- Use Hping3 for Network Scanning
- Perform a TCP Scan Using Dmitry

- Perform Stealth Scanning Using Nmap
- Use fping for Network Scanning
- Explore a Network Using Zenmap
- Use MyLanViewer to Scan a Network
- Using Msfconsole to Perform TCP Stealth on a Network

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

- Networking Tools

## 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 MemberWorkstation192.168.0.5/24PLABDM01Domain Member Server192.168.0.2/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABDM01

Windows Server 2019 — Domain Member192.168.0.2/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

## Task 1 — Using Hping3 for Network Scanning

Hping3 is a powerful tool that can be used for various types of scanning in a network, which can perform Layer 3 and Layer 4 scanning.

In this task, you will use the hping3 tool to perform various types of network scanning. To do this, perform the following steps:

#### 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**:

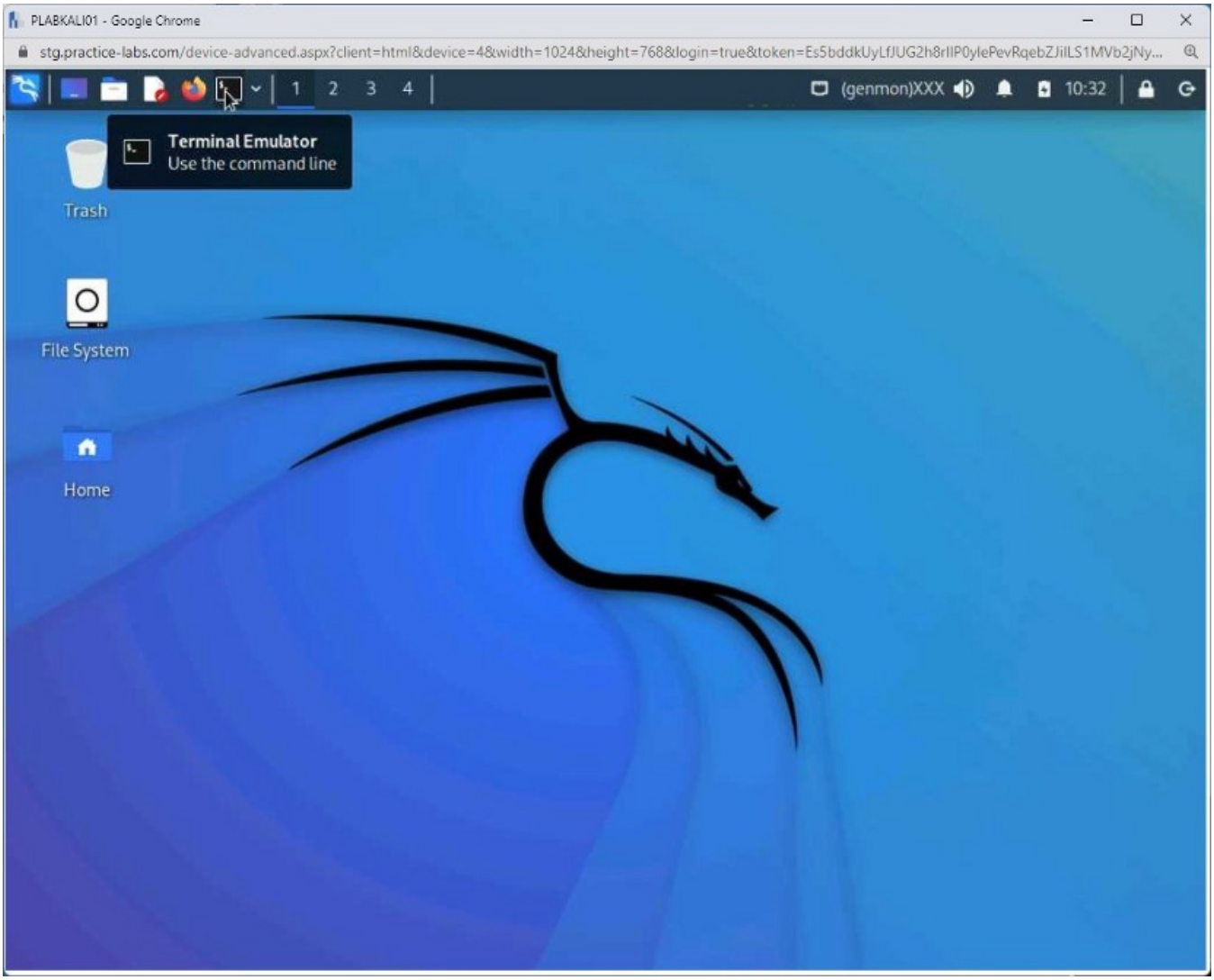
```
root
```

**Password**:

**Password**

The desktop of **PLABKALI01** is displayed.

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



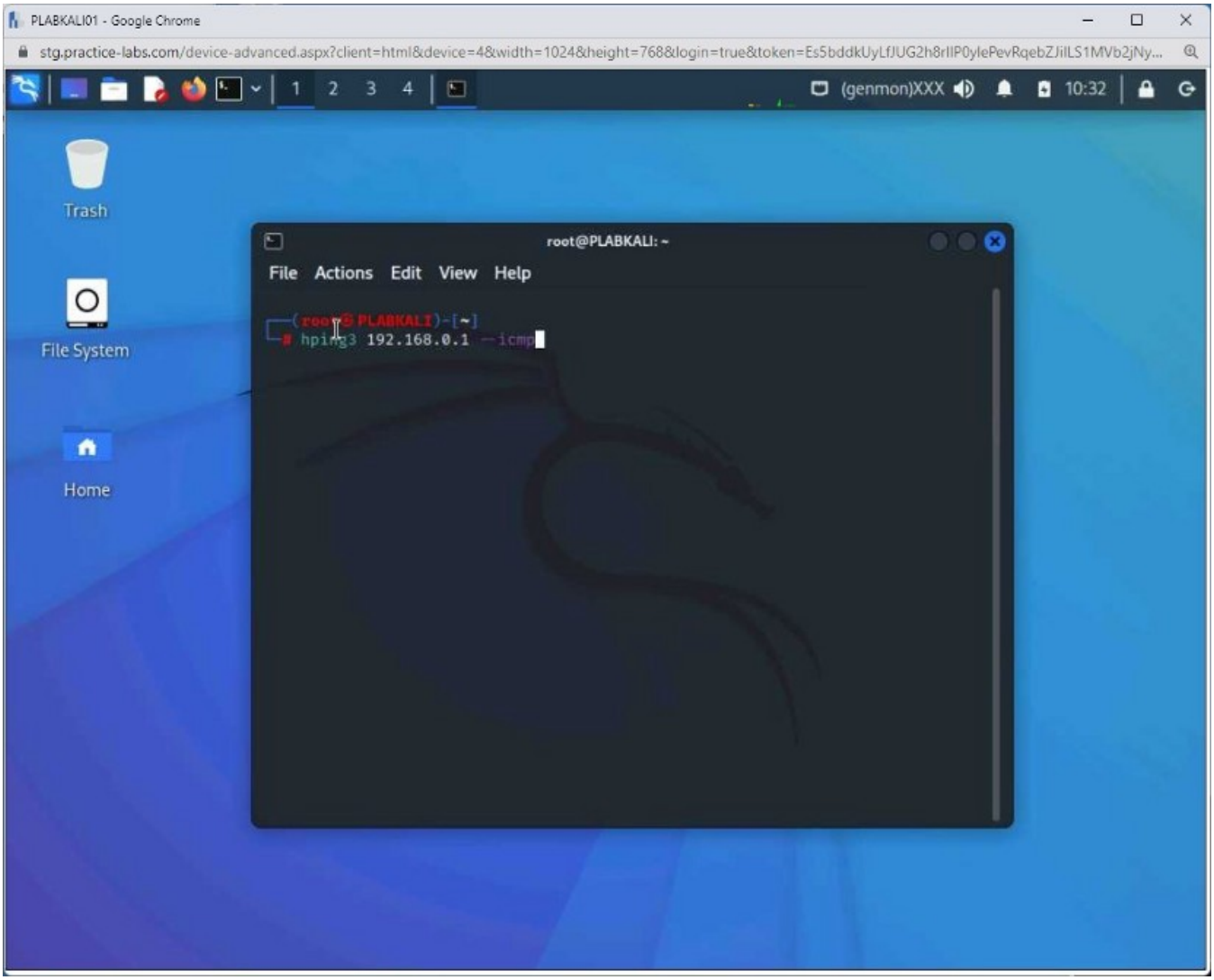

**Step 2**

The terminal window is displayed. You can perform an **ICMP** discovery of a single host using **hping3**.

Type the following command:

```
hping3 192.168.0.1 --icmp
```

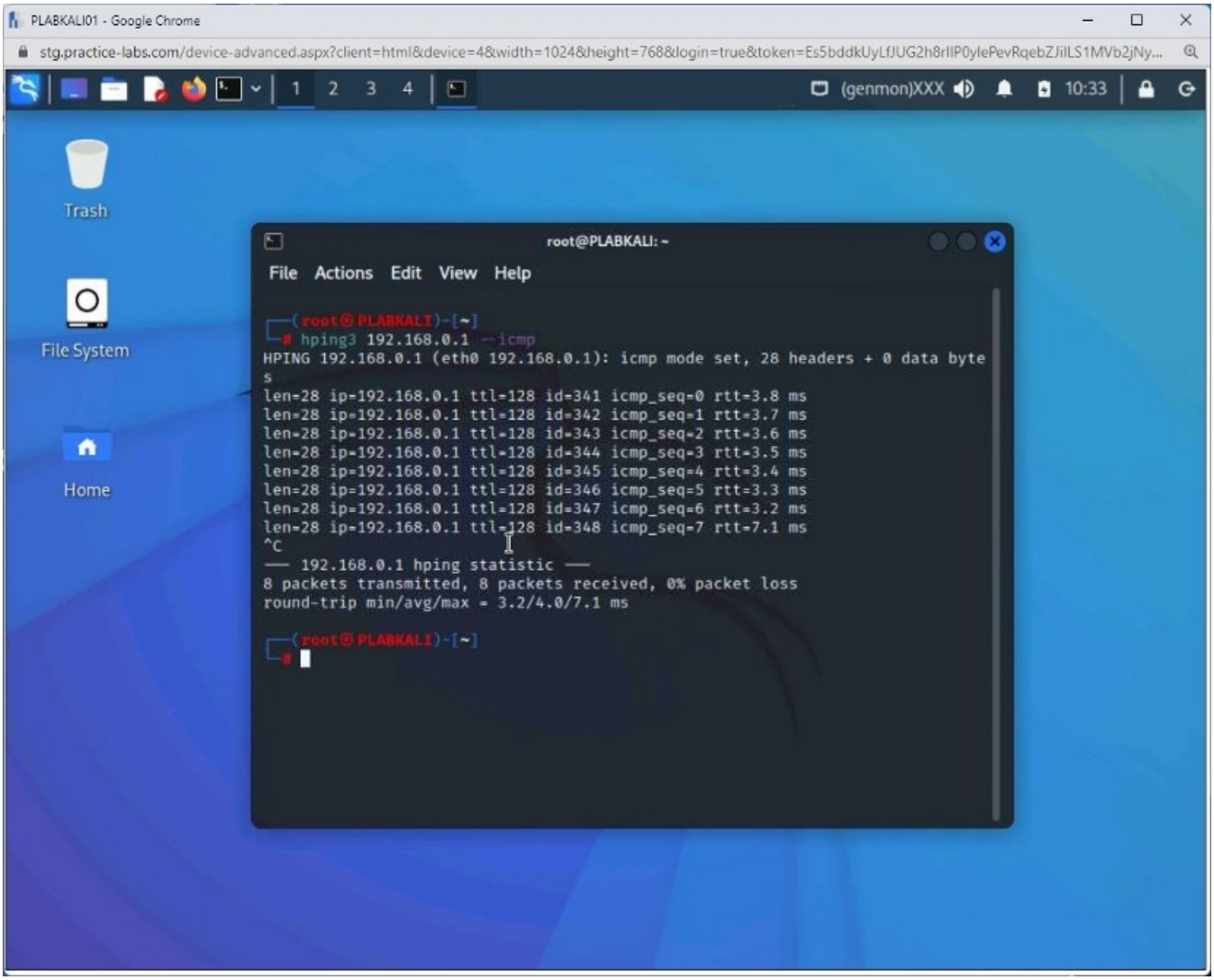
Press **Enter**.




**Step 3**

The **hping3** command will continue for an indefinite time unless you stop it. To do this, press the **Ctrl** + **C** keys.

The output of the hping3 command is displayed.




**Step 4**

Clear the screen by entering the following command:

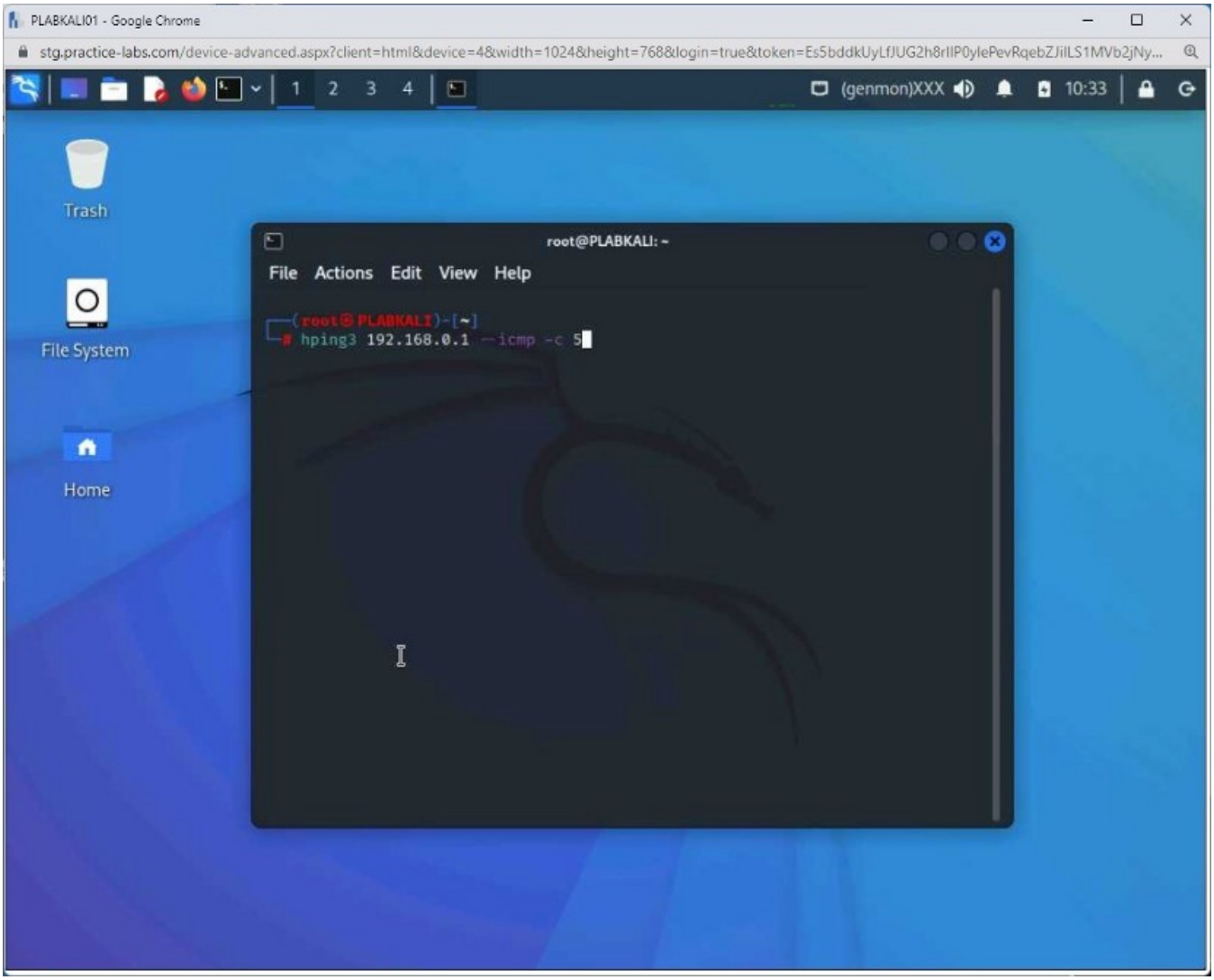
```
clear
```

You can also limit the command to perform **ICMP** discovery for a limited number. To do this, type the following command:

***Note:*** *The -S parameter sets the SYN flag.*

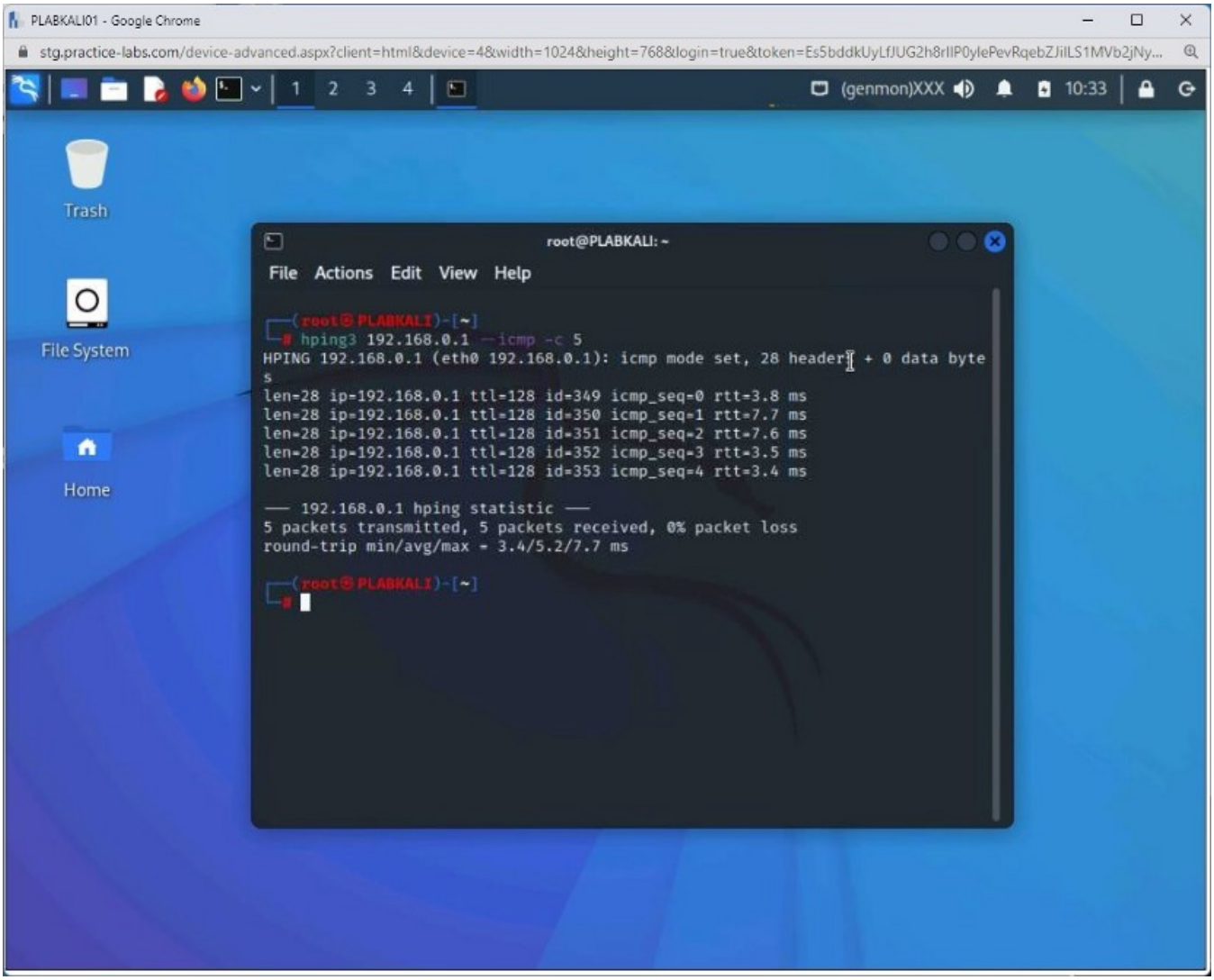
```
hping3 192.168.0.1 --icmp -c 5
```

Press **Enter**.




**Step 5**

The output of the **hping3** command will be limited to five times.




**Step 6**

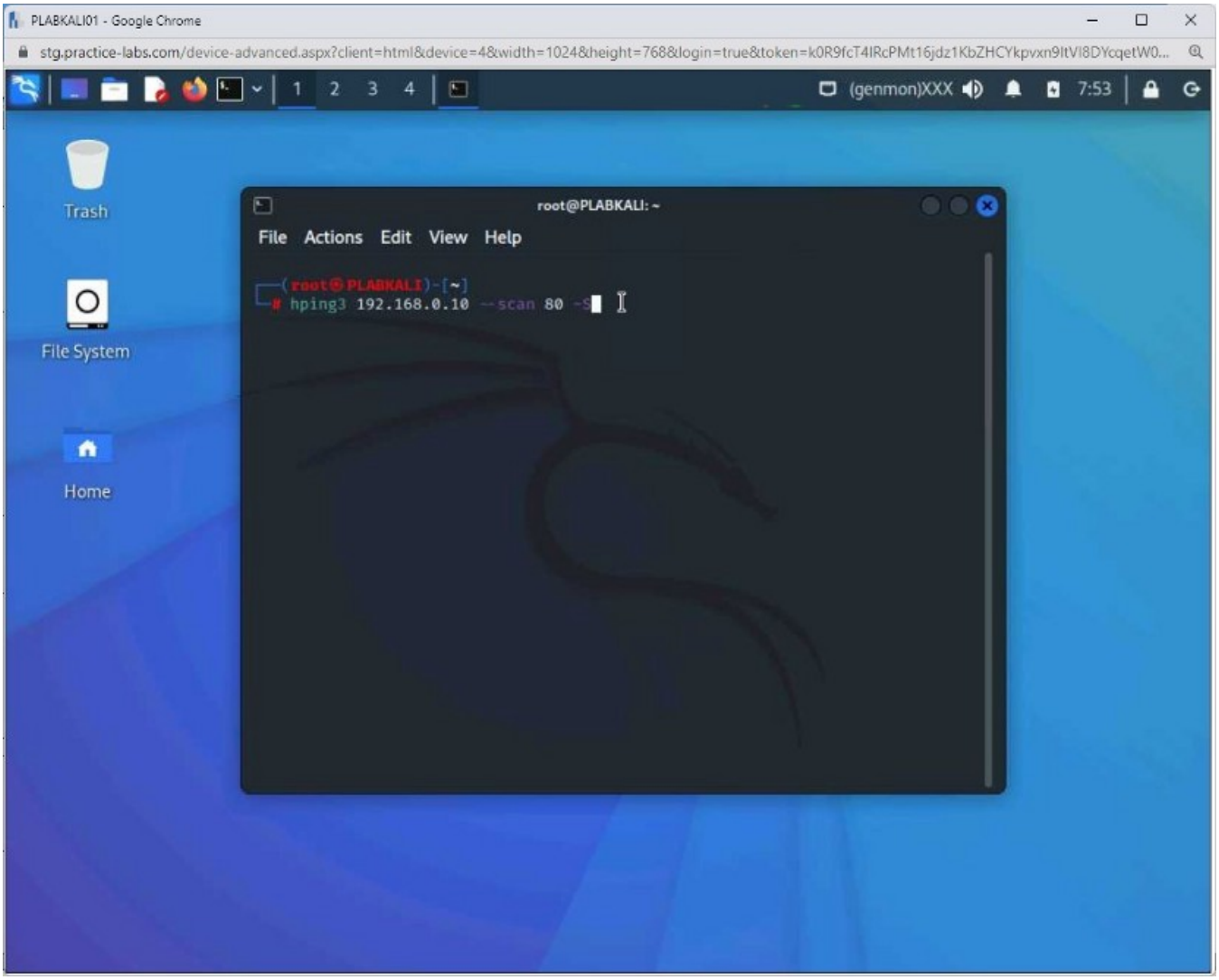
Clear the screen by entering the following command:

```
clear
```

You can also use the **hping3** command to scan for a specific TCP port. You need to specify the port number with the **— — scan** parameter. Type the following command:

```
hping3 192.168.0.10 --scan 80 -S
```

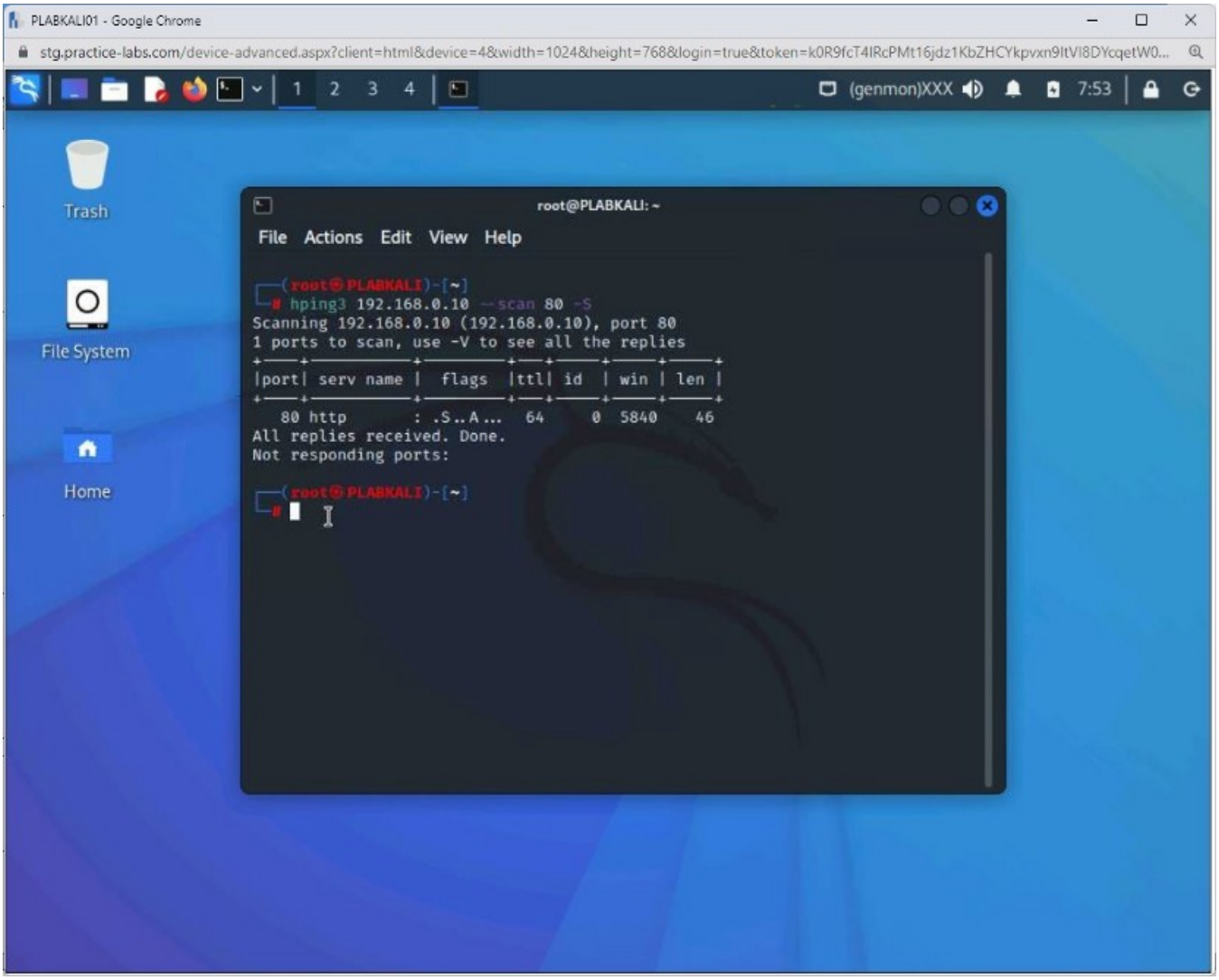
Press **Enter**.




**Step 7**

Notice that in the **flags** column, **S** and **A** are mentioned.

This means that the **SYN+ACK** response was received from the target system.




**Step 8**

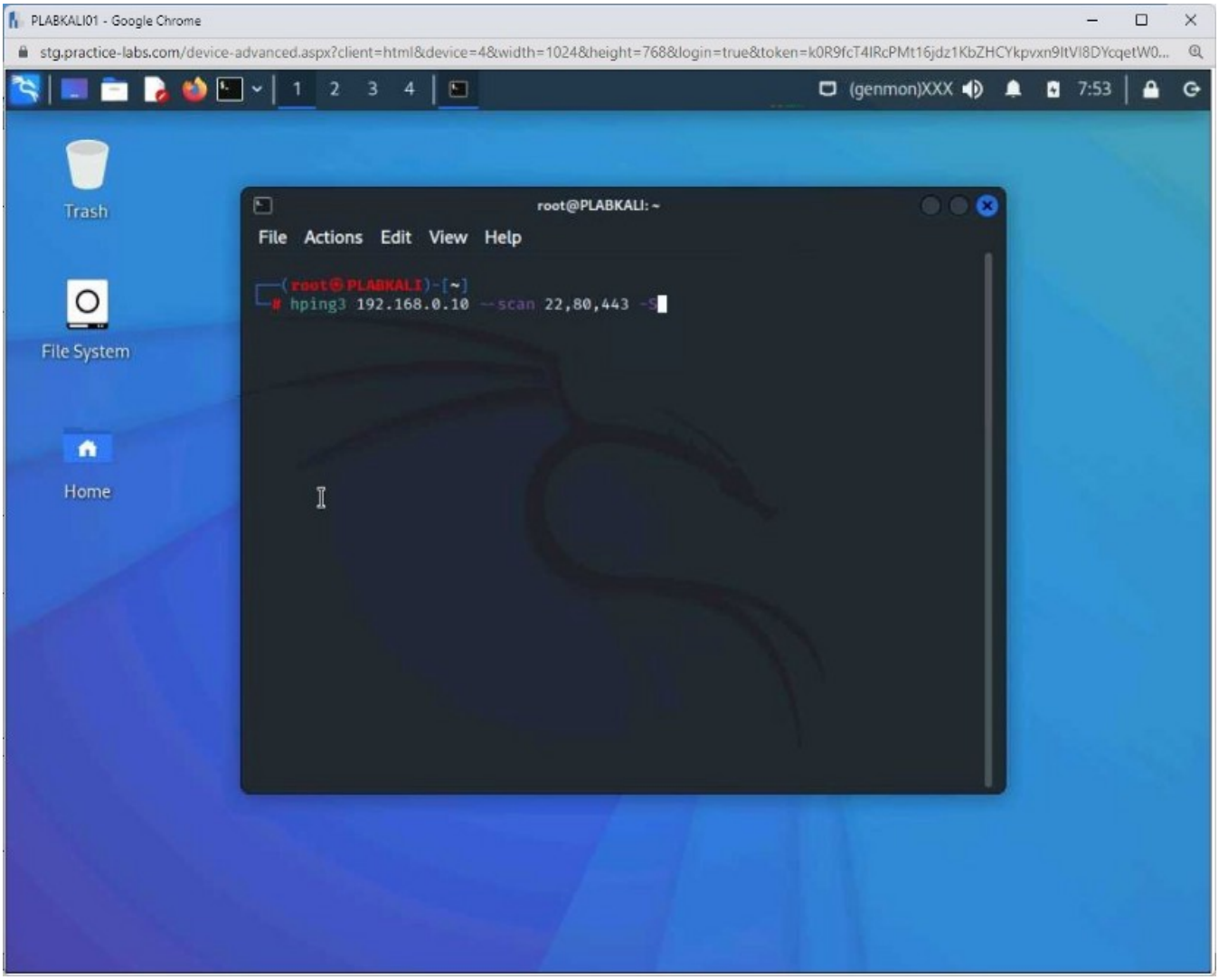
Clear the screen by entering the following command:

```
clear
```

You can also scan for multiple ports using the **hping3** command. To do this, type the following command:

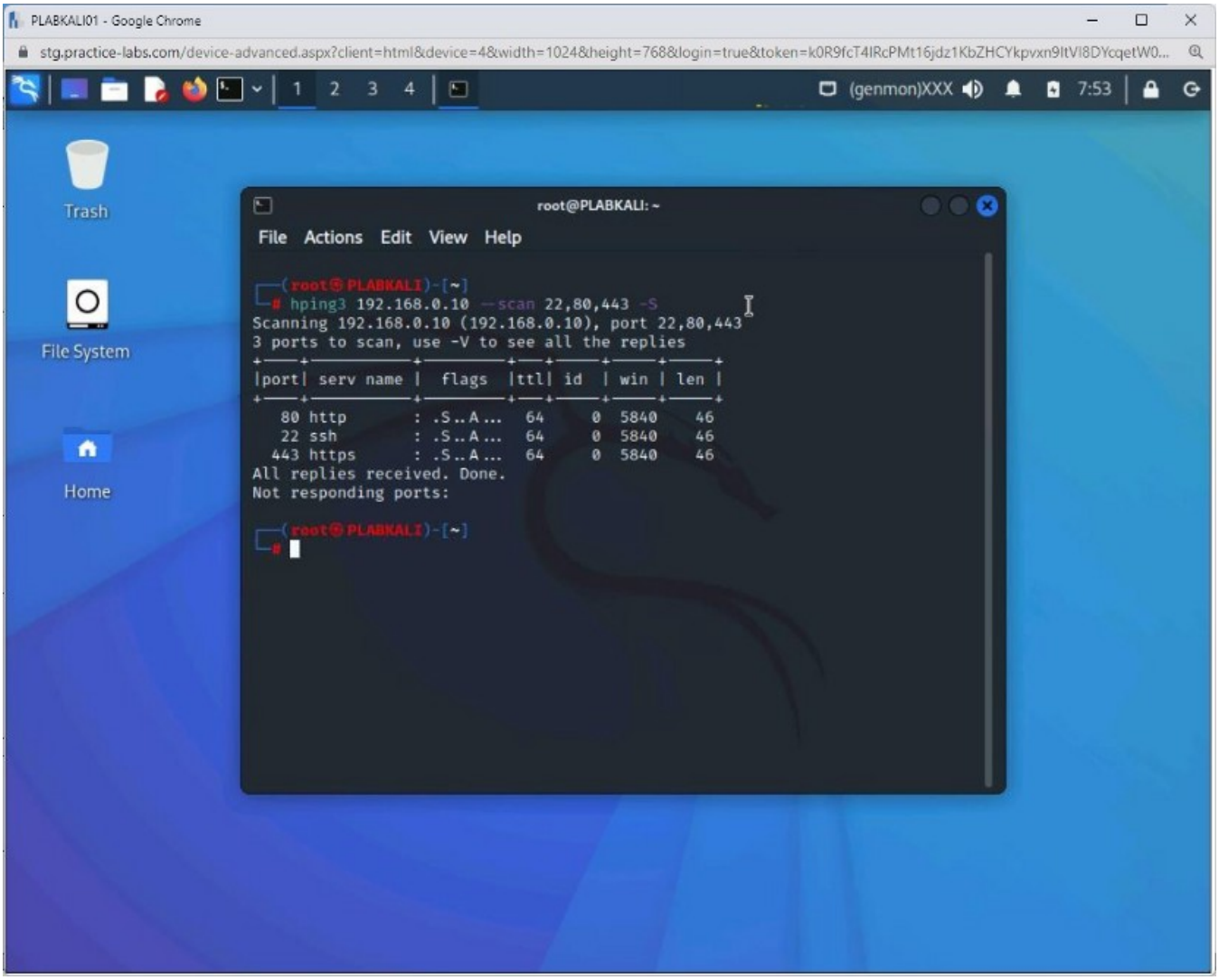
```
hping3 192.168.0.10 --scan 22,80,443 -S
```

Press **Enter**.




**Step 9**

Notice the output. All ports have responded. The output only displays the ports if the **SYN+ACK** response is received.




**Step 10**

Clear the screen by entering the following command:

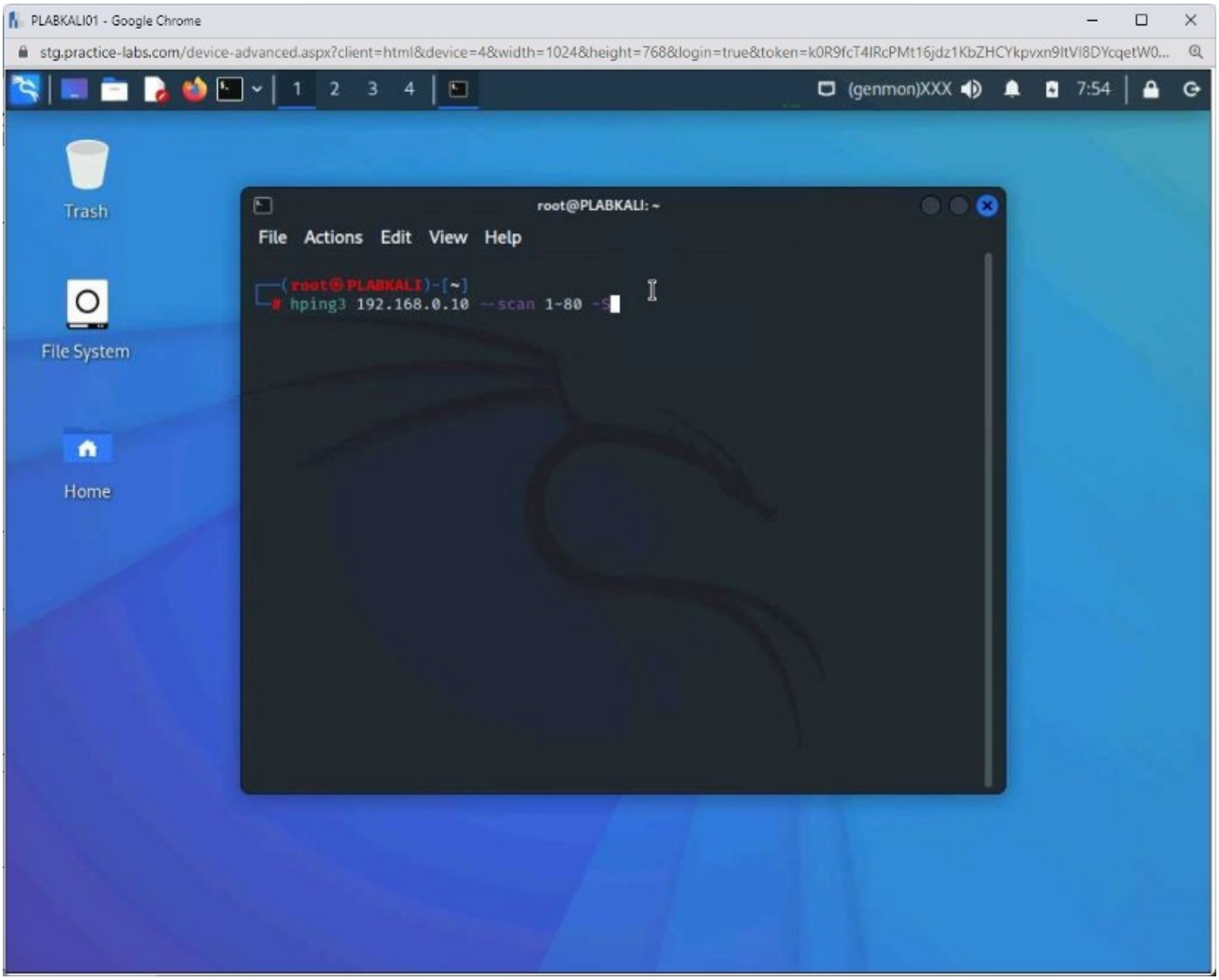
```
clear
```

You can also scan for a range of ports. You need to specify the first and the last port to do this.

Type the following command:

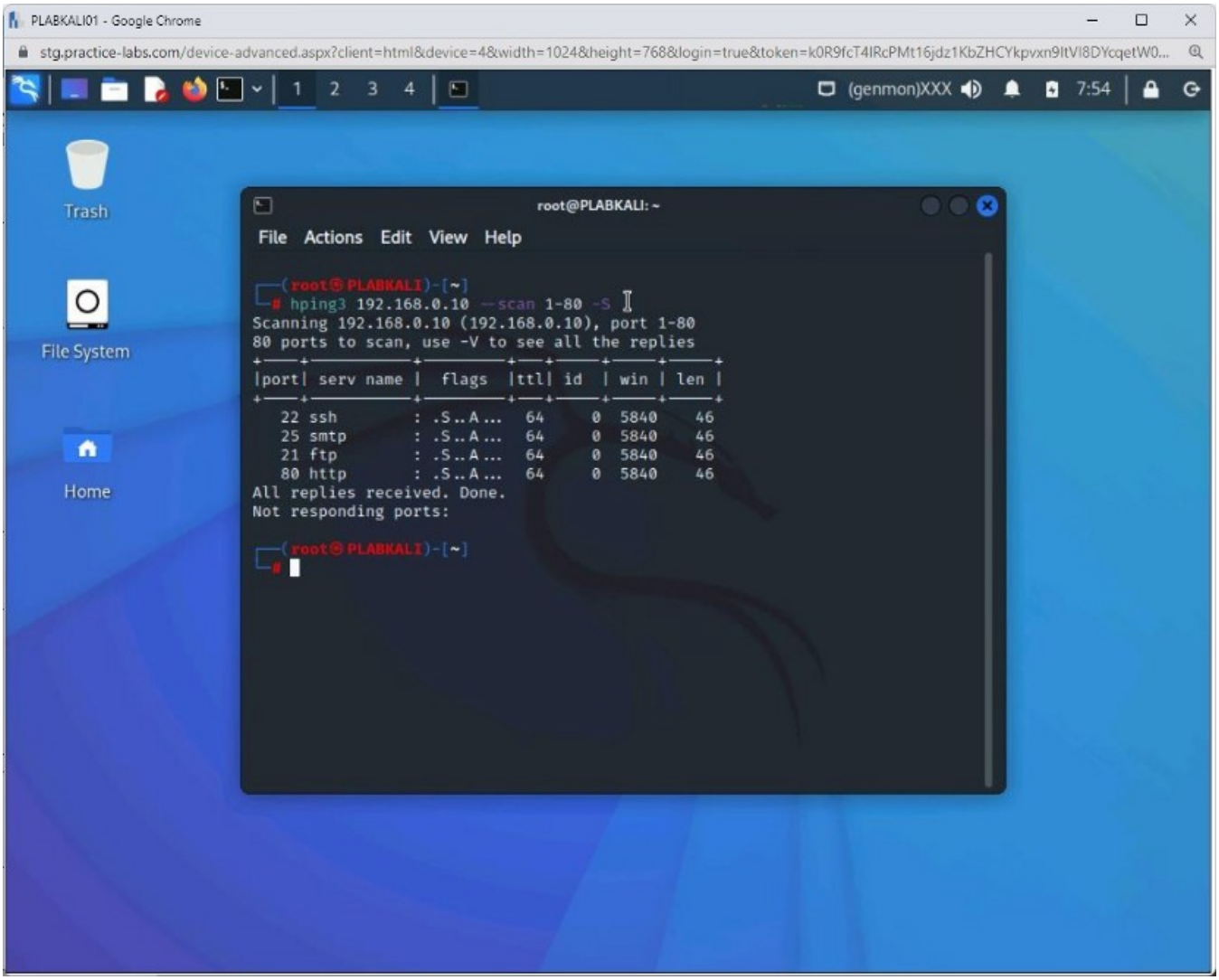
```
hping3 192.168.0.10 --scan 1-80 -S
```

Press **Enter**.




**Step 11**

Notice the output mentioning the open ports from the range of **1** to **80**.




**Step 12**

Clear the screen by entering the following command:

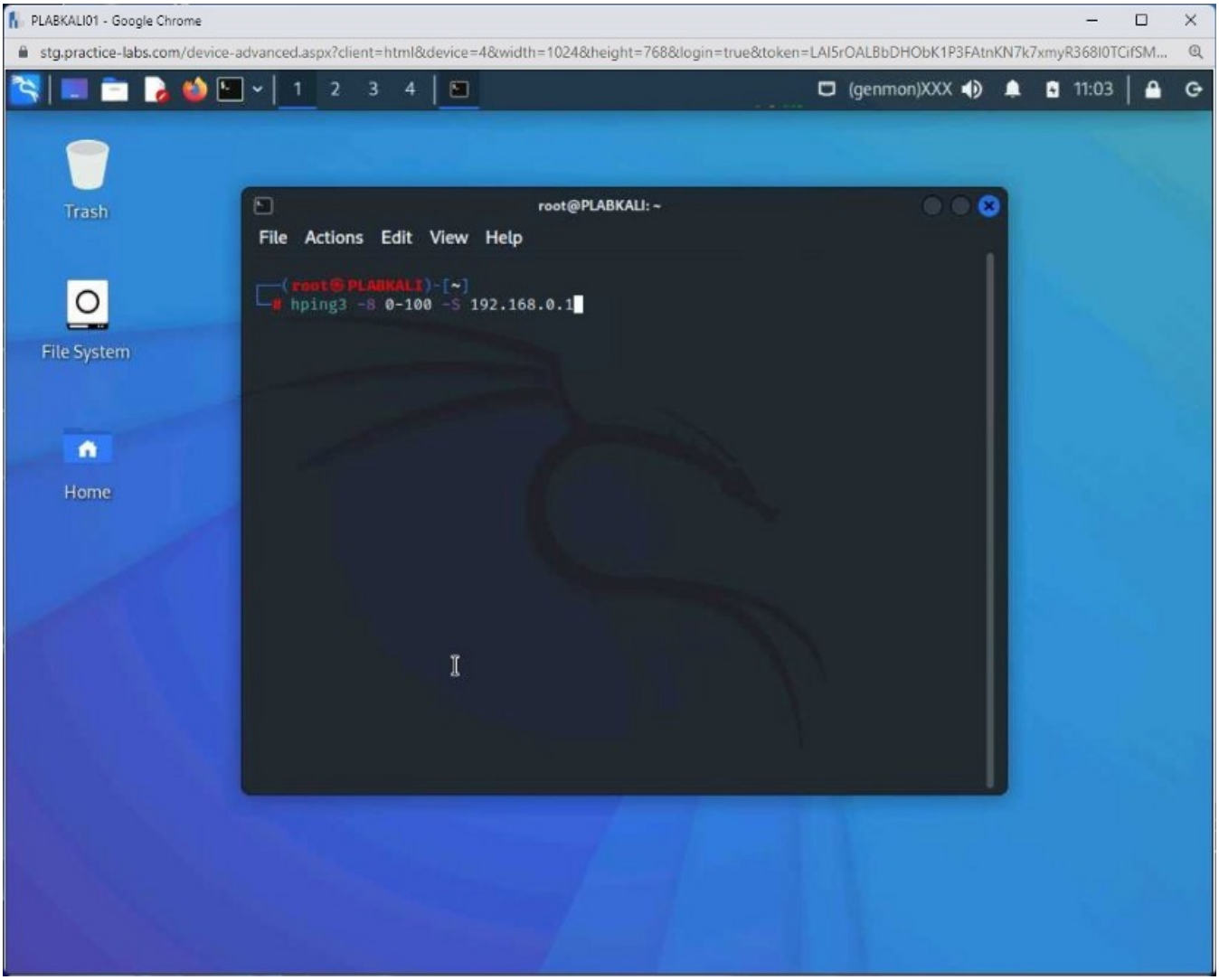
```
clear
```

You can use **hping3** to determine open ports on a target. To identify open ports on **192.168.0.1**, type the following command:

```
hping3 -8 0-100 -S 192.168.0.1
```

Press **Enter**. The given command specifies the following switches:

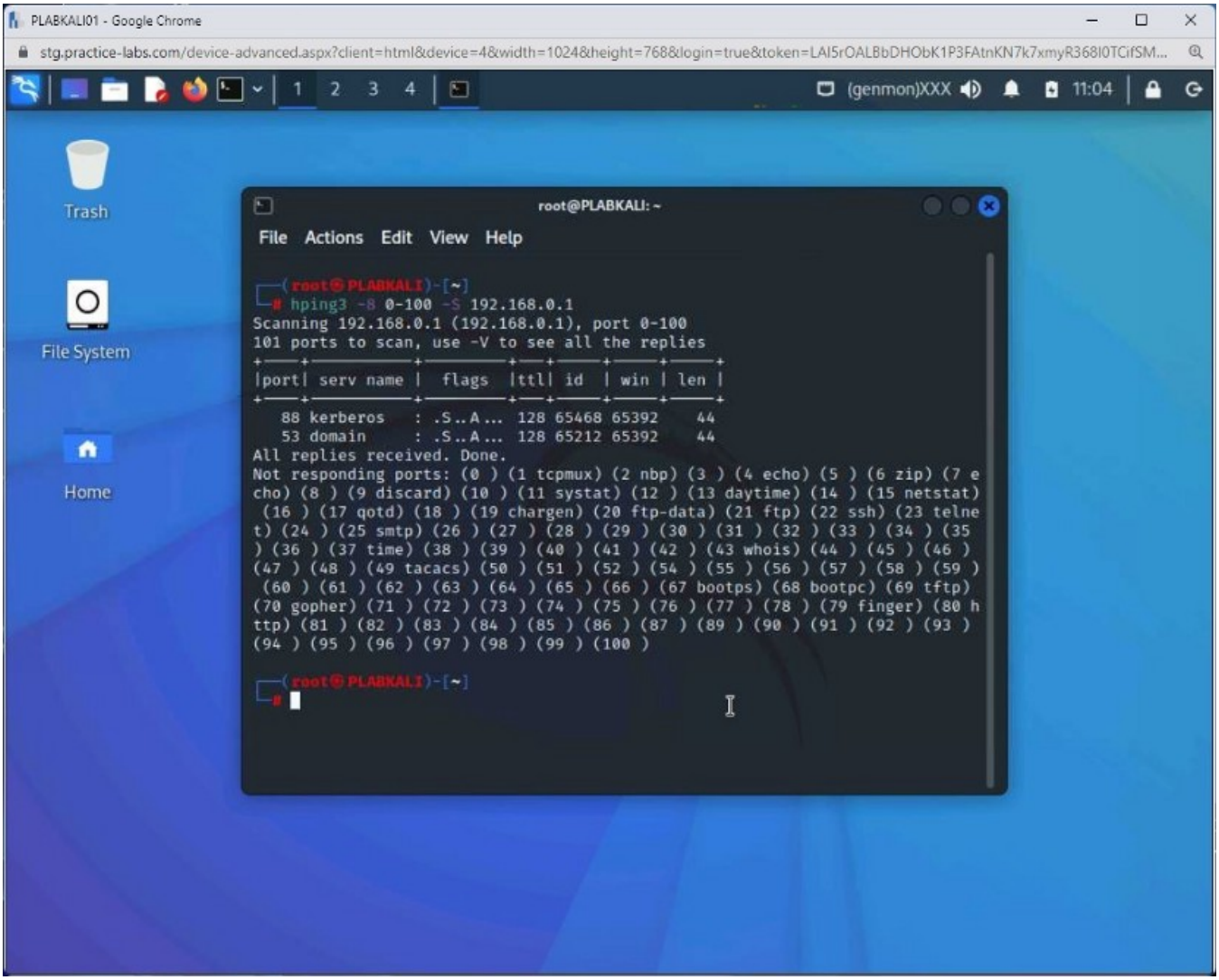
***Note:*** *-8 = Enable SCAN mode.*
*0–100 = Range of ports to scan.*
*-S = set SYN flag.*




**Step 13**

The output displays the list of open ports and their services. The output also displays the ports that do not respond to the scan.

***Note:*** *Notice that the given command sent the SYN flag and received the SYN-ACK flag from each open port on PLABDC01.*




Keep the terminal window open.

## Task 2 — Perform a TCP Scan Using Dmitry

Dmitry is an information-gathering tool. It can gather the following type of information:

- Subdomains
- E-mail addresses
- Uptime information
- TCP port scan
- WHOis lookups

In this task, you will use Dmitry for a TCP scan. To do this, perform the following steps:

### Step 1

Ensure that you are connected to **PLABKALI01** and that the terminal window is open.

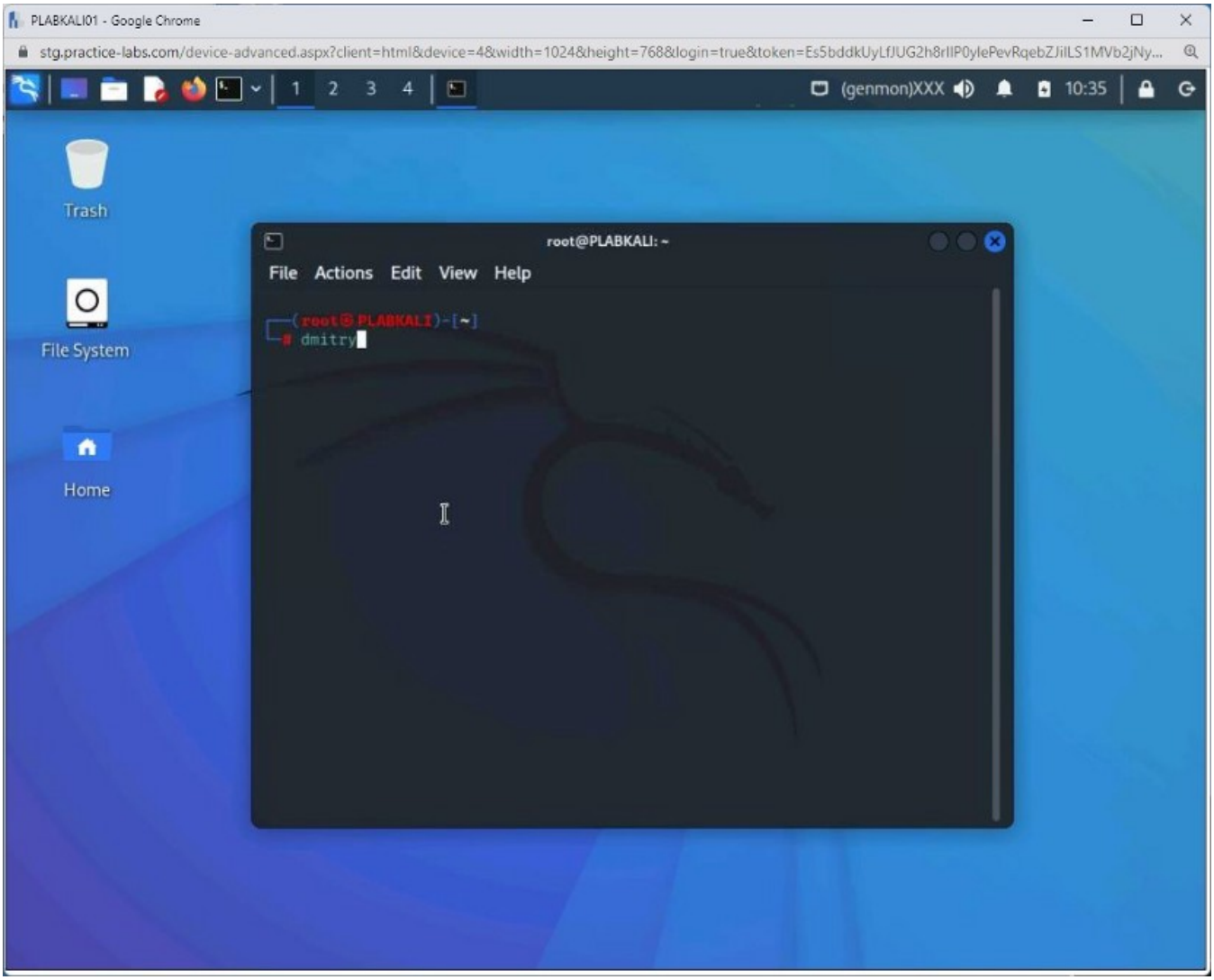
Clear the screen by entering the following command:

```
clear
```

To view the parameters of the dmitry command, type the following command:

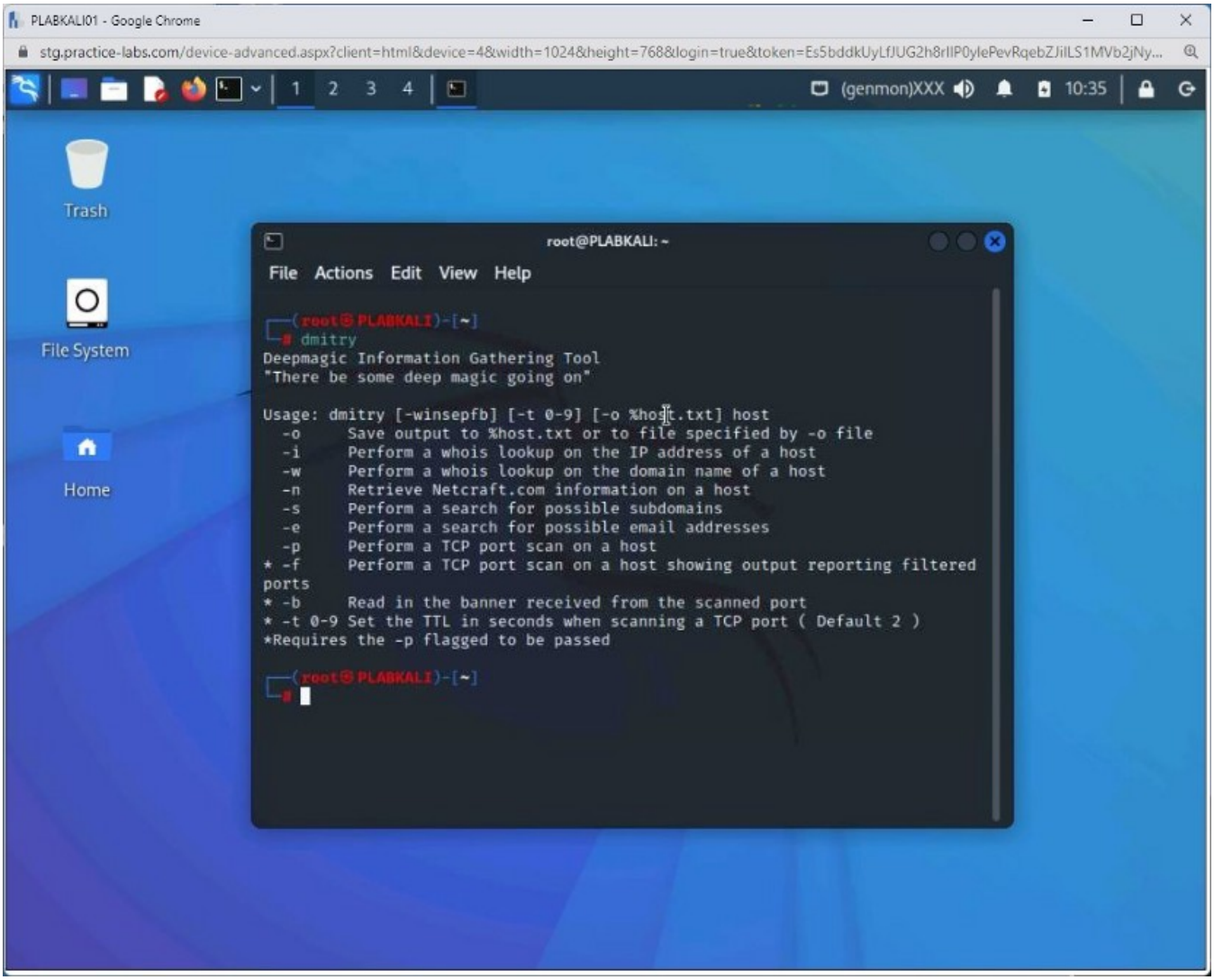
```
dmitry
```

Press **Enter**.




### Step 2

Notice that the output displays the list of parameters.




**Step 3**

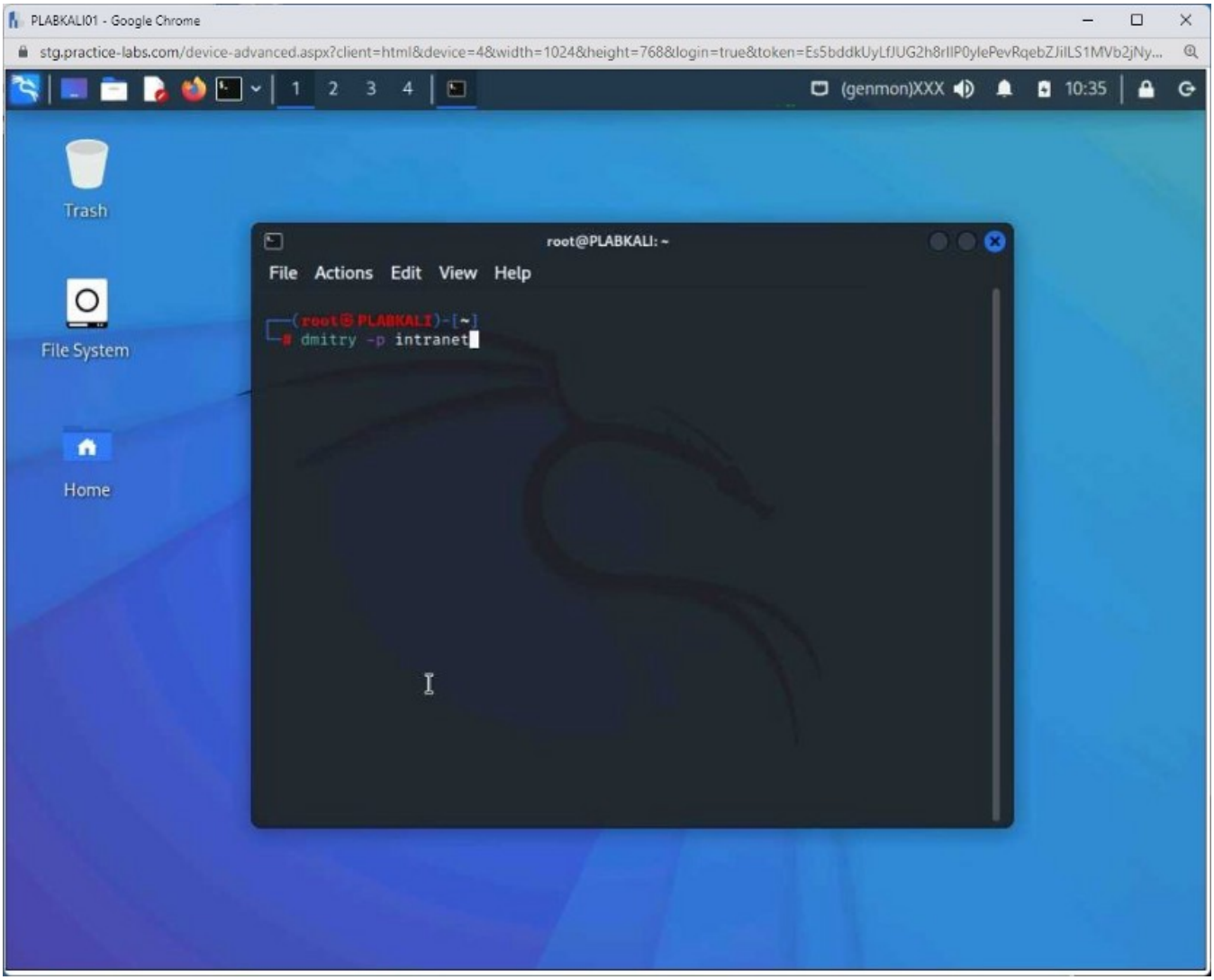
Clear the screen by entering the following command:

```
clear
```

You will now use the **-p** parameter along with the **dmitry** command to perform a **TCP scan**. Type the following command:

```
dmitry -p intranet
```

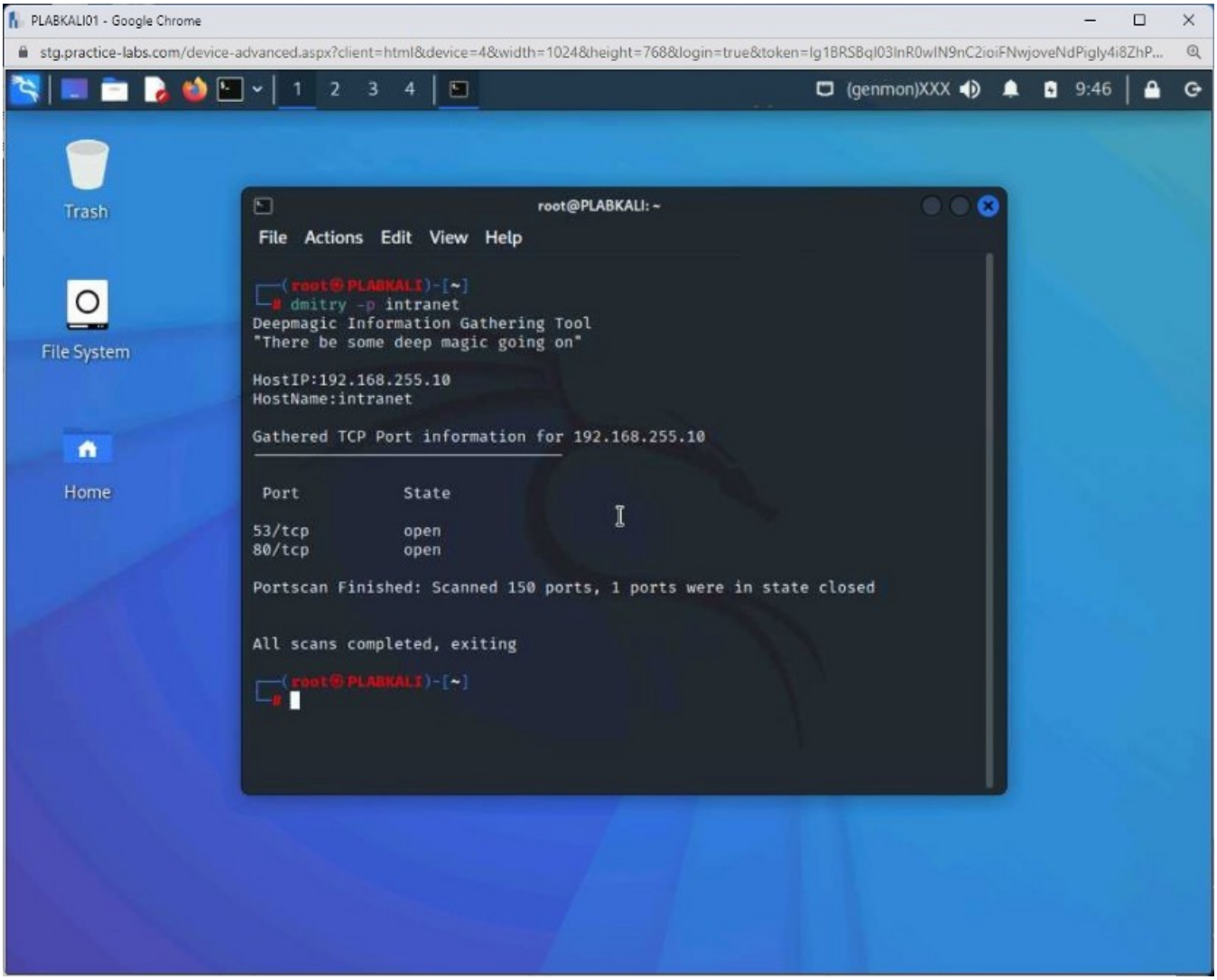
Press **Enter**.




**Step 4**

Notice that the output displays the list of open ports. The output also displays the target's IP address.

***Note**: The amount of open ports may be different to what is shown in the screenshots.*




**Step 5**

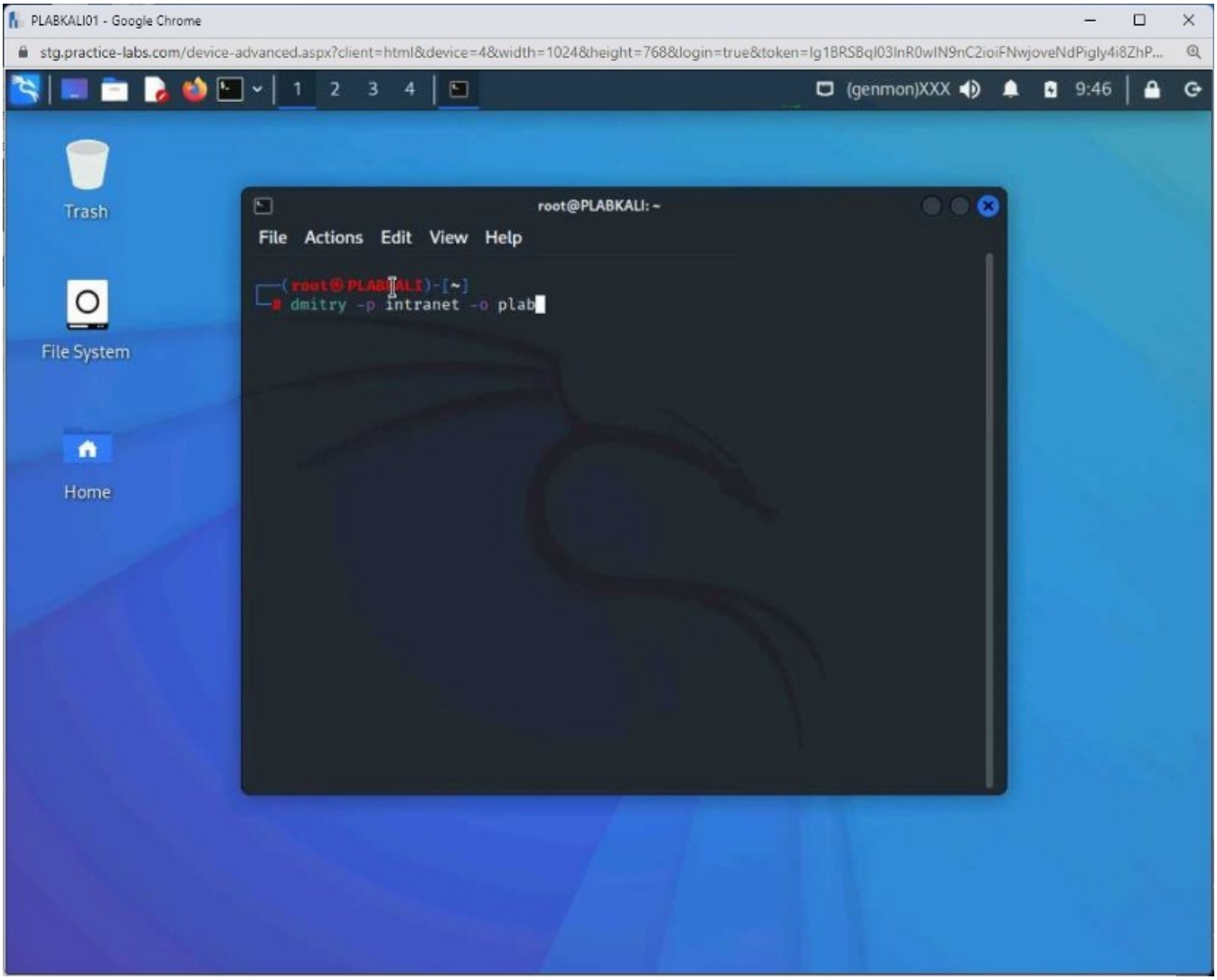
Clear the screen by entering the following command:

```
clear
```

You can also send the **dmitry** output to a text file. In this step, you will send the output to a text file named **plab**. To do this, type the following command:

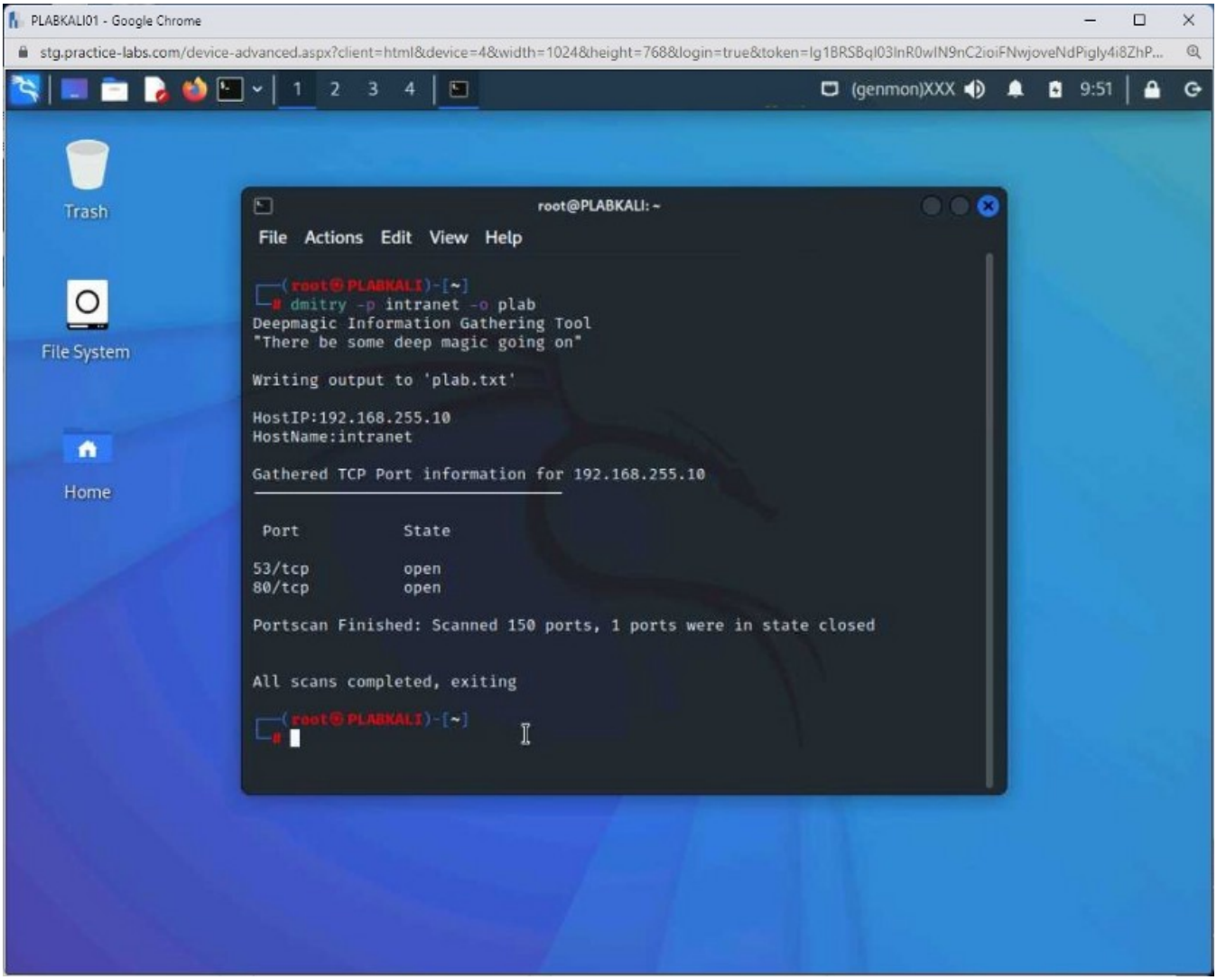
```
dmitry -p intranet -o plab
```

Press **Enter**.




**Step 6**

Notice that the output mentions writing output to **plab.txt**.




**Step 7**

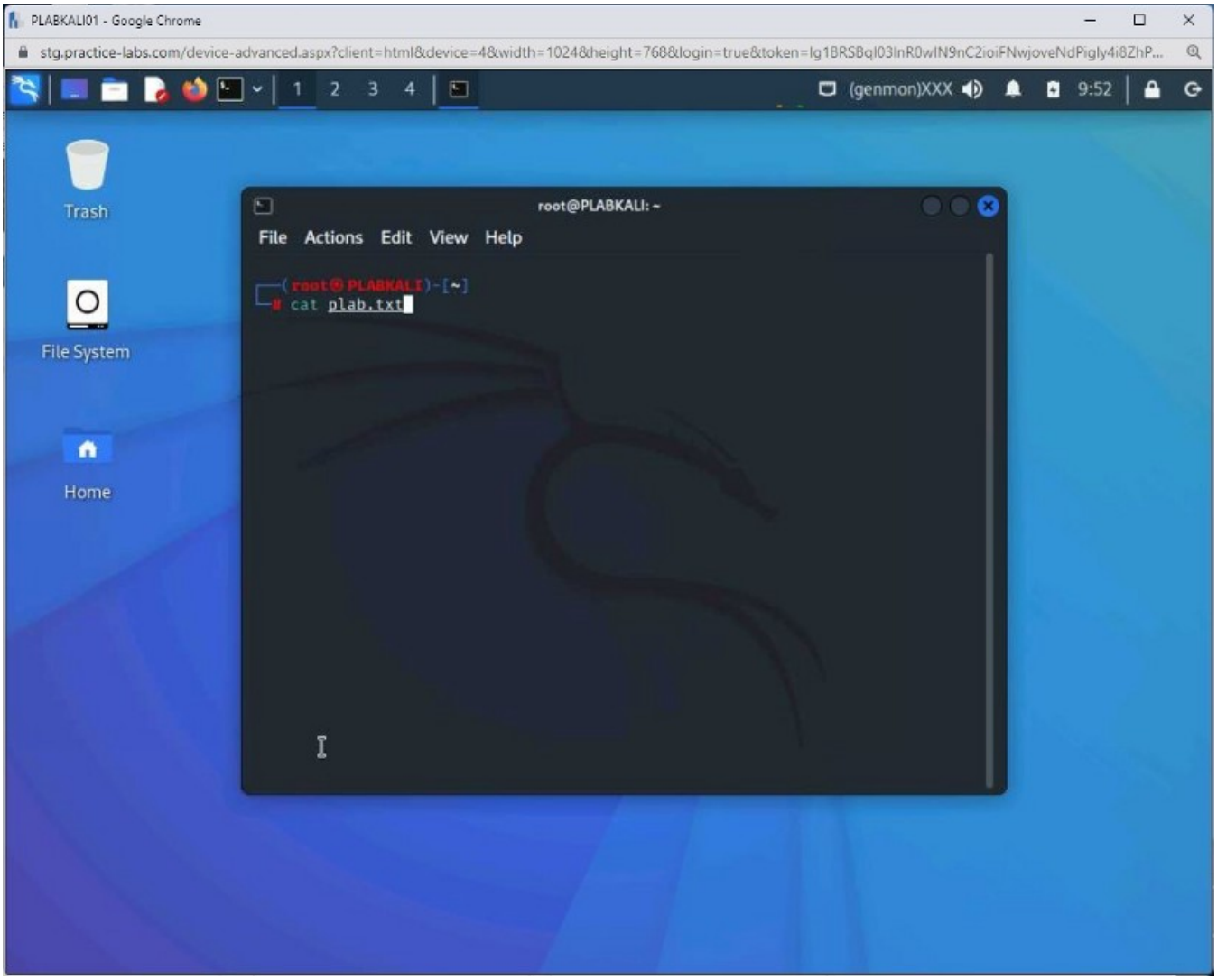
Clear the screen by entering the following command:

```
clear
```

Let's view the **plab.txt** file. Type the following command:

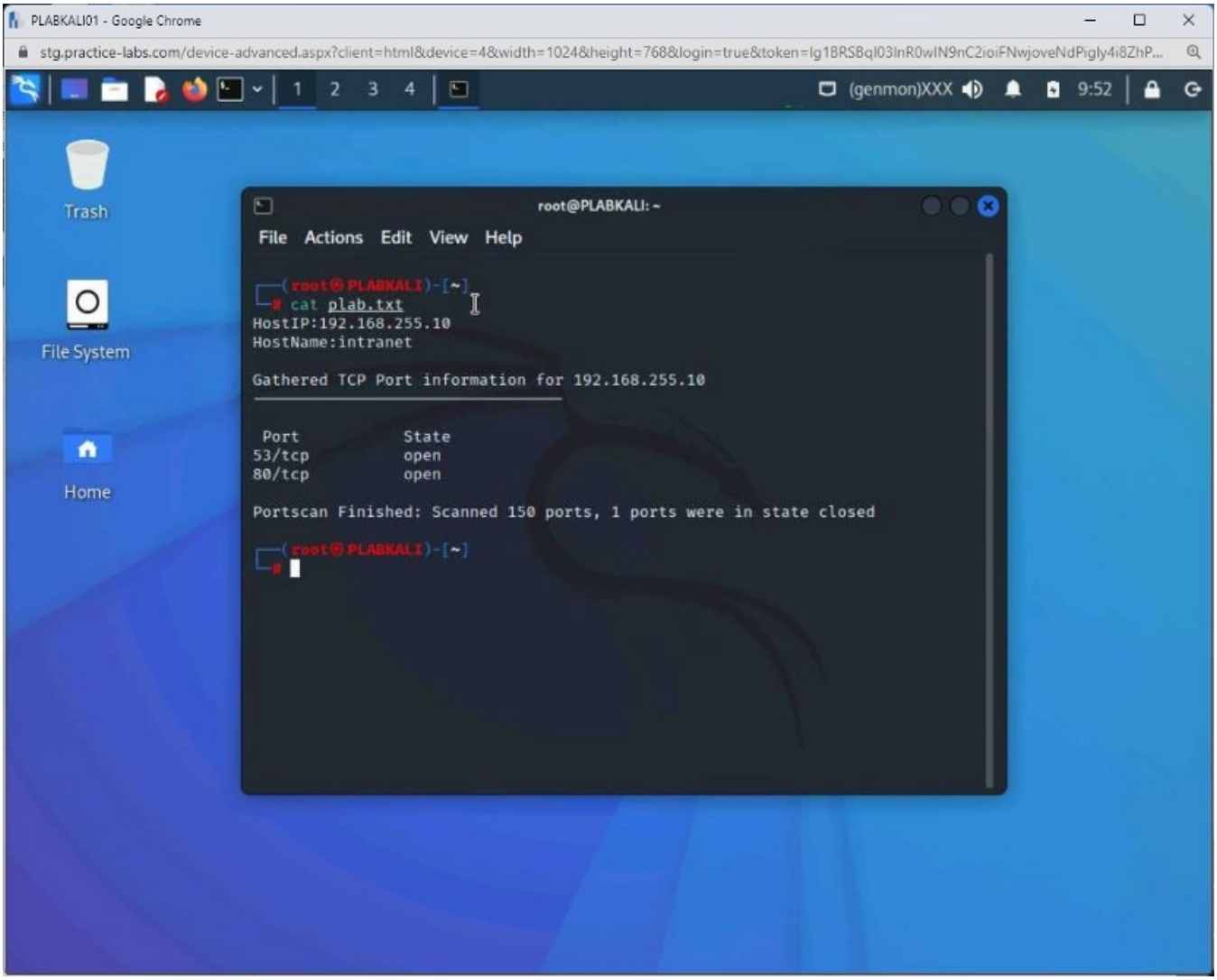
```
cat plab.txt
```

Press **Enter**.




**Step 8**

Notice that the output is the same as the output shown on the command line.




Keep the terminal window open.

## Task 3 — Perform Stealth Scanning Using Nmap

An attacker does not complete the three-way handshake with the victim's system in a stealth scan and, therefore, goes undetected. Nmap has different options for conducting stealth scans, which you will perform in this task.

To conduct stealth scanning, perform the following steps:

### Step 1

Ensure that you are connected to **PLABKALI01** and that the terminal window is open.

Clear the screen by entering the following command:

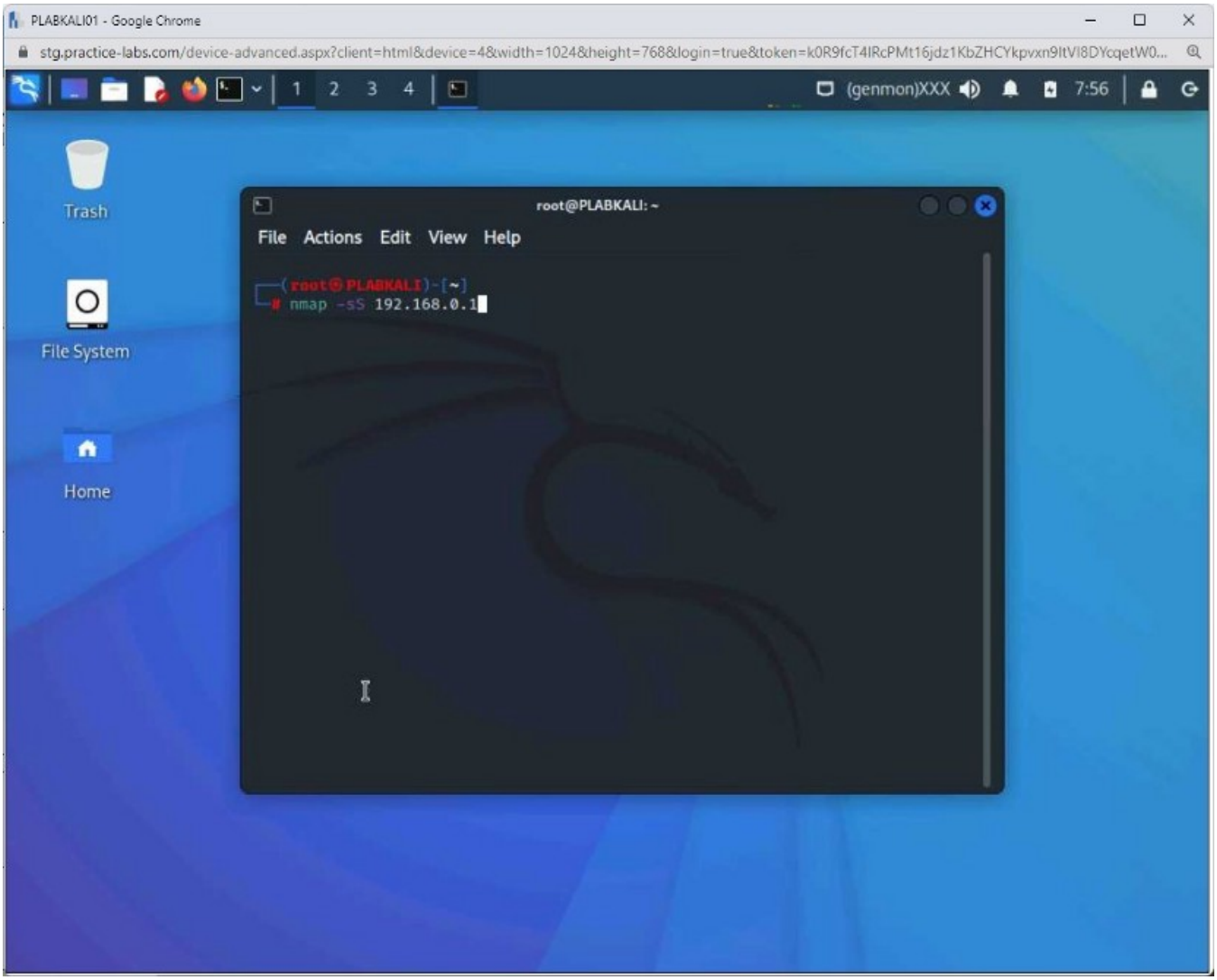
```
clear
```

You will now scan the ports using a **TCP SYN** scan, known as a stealth scan. Type the following command:

***Note:*** *If no port range is specified, the command nmap -sS <target> performs a SYN scan on well-known 1,000 TCP ports on the host <target>. Nmap scans can be specifically crafted as desired. Detailed information about all the switches supported by Nmap can be found in the help section of the tool.*

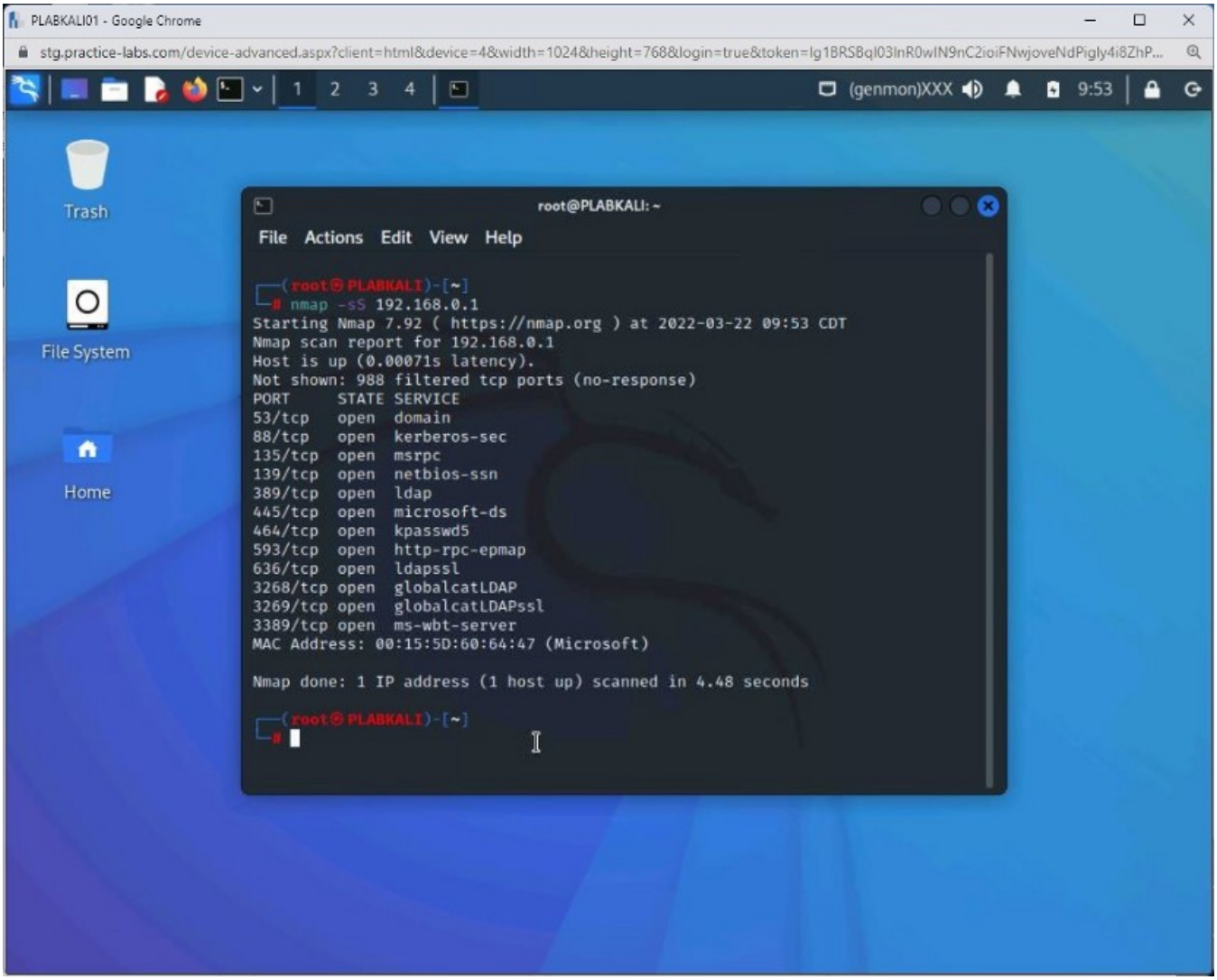
```
nmap -sS 192.168.0.1
```

Press **Enter**.




### Step 2

Notice that the output which lists the open ports on **192.168.0.1**.




**Step 3**

Clear the screen by entering the following command:

```
clear
```

The **ACK** scan cannot be used for scanning ports. This type of scan will never show ports in the “open” state, and hence it should be used in conjunction with other scan types to gain more information about firewalls or packet filters between your source machine and the target machine.

If used for port scanning, the ACK scan will provide meaningful results only if the target OS flavor is Solaris.

ACK scanning is mainly used to discover the rules of a filter and can help determine if a firewall is stateless (blocks incoming SYN packets) or stateful (tracks connections and blocks unsolicited ACK packets).

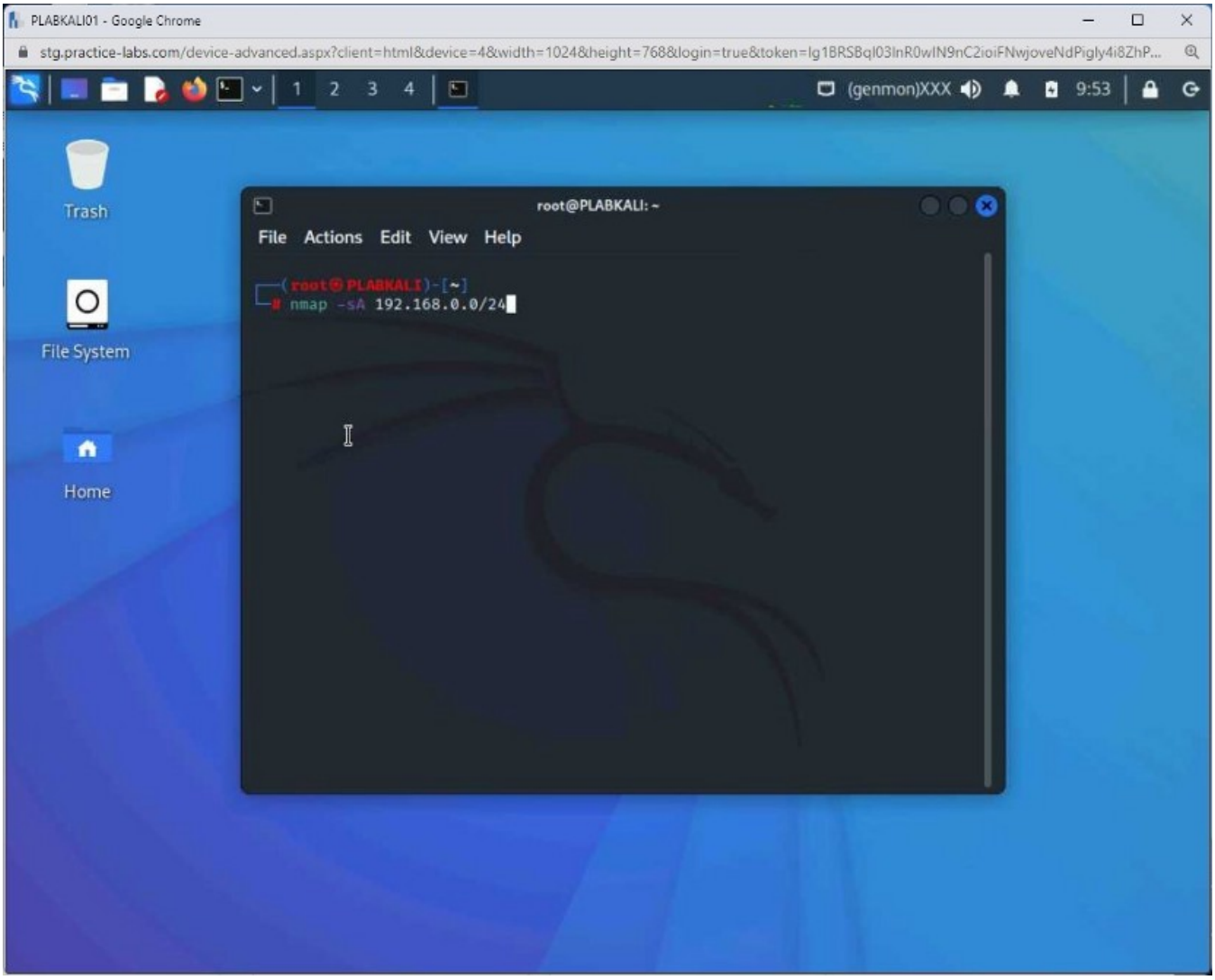
As the name indicates, the ACK scan sends ACK packets to the target host. If the target responds with an RST packet, then the port is classified as "**unfiltered**" i.e., the port can send its RST packet through the firewall in place. If no packets are received, the port is "**filtered**" i.e., the firewall prevented the RST packet sent from the port.

To perform a **TCP ACK** scan, type the following command:

```
nmap -sA 192.168.0.0/24
```

Press **Enter**.

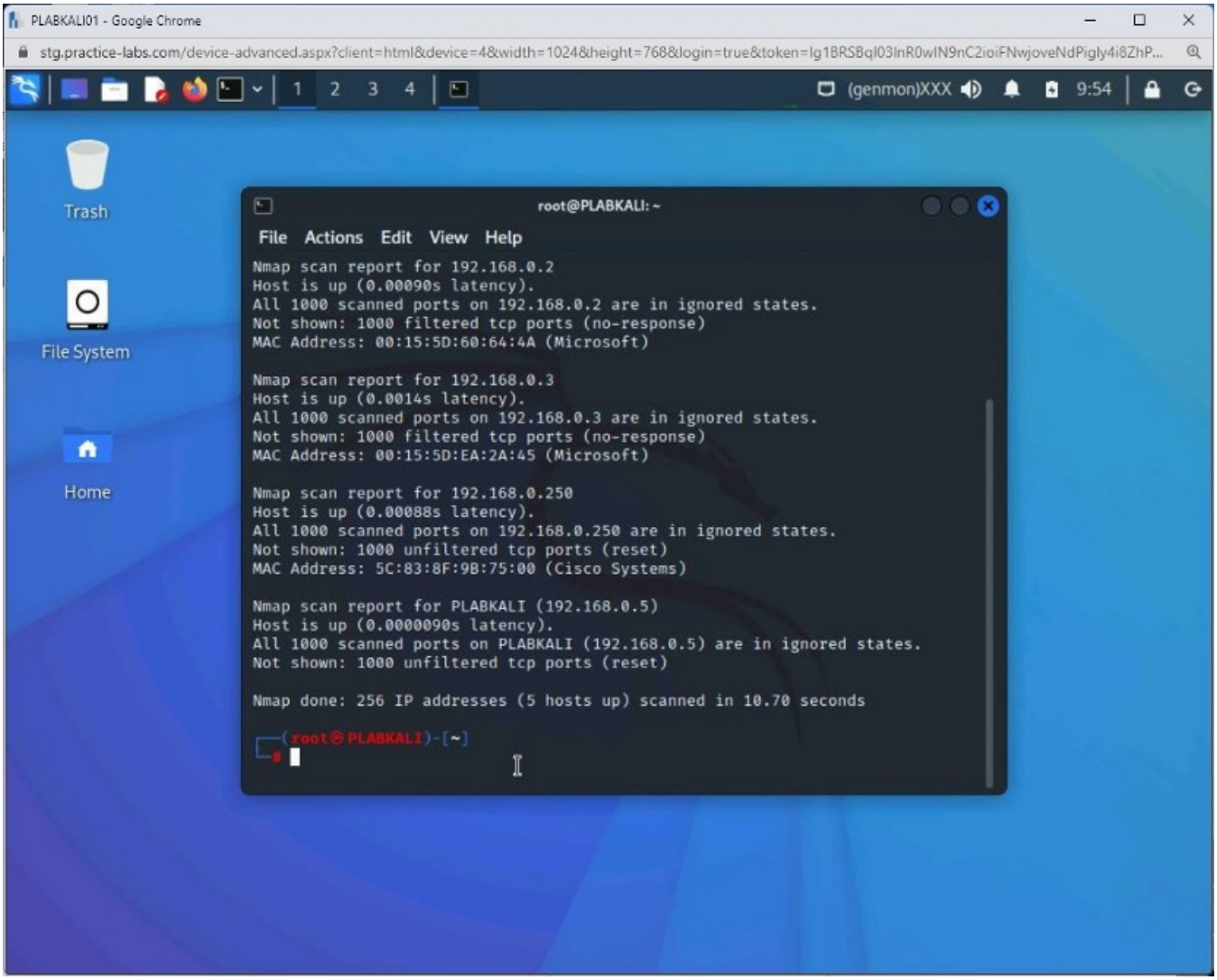
***Note:*** *The following are the switches used in the given command:*
*-sA: ACK Scan*
*-p: Specific port number to scan (port range can also be specified)*




**Step 4**

The output of this command is displayed. The output does not contain the **open** or **closed** ports but **filtered** or **unfiltered** ports.

For example, all **1000** ports on **192.168.0.2** are filtered whereas, on **192.168.0.250**, they are unfiltered.




**Step 5**

Clear the screen by entering the following command:

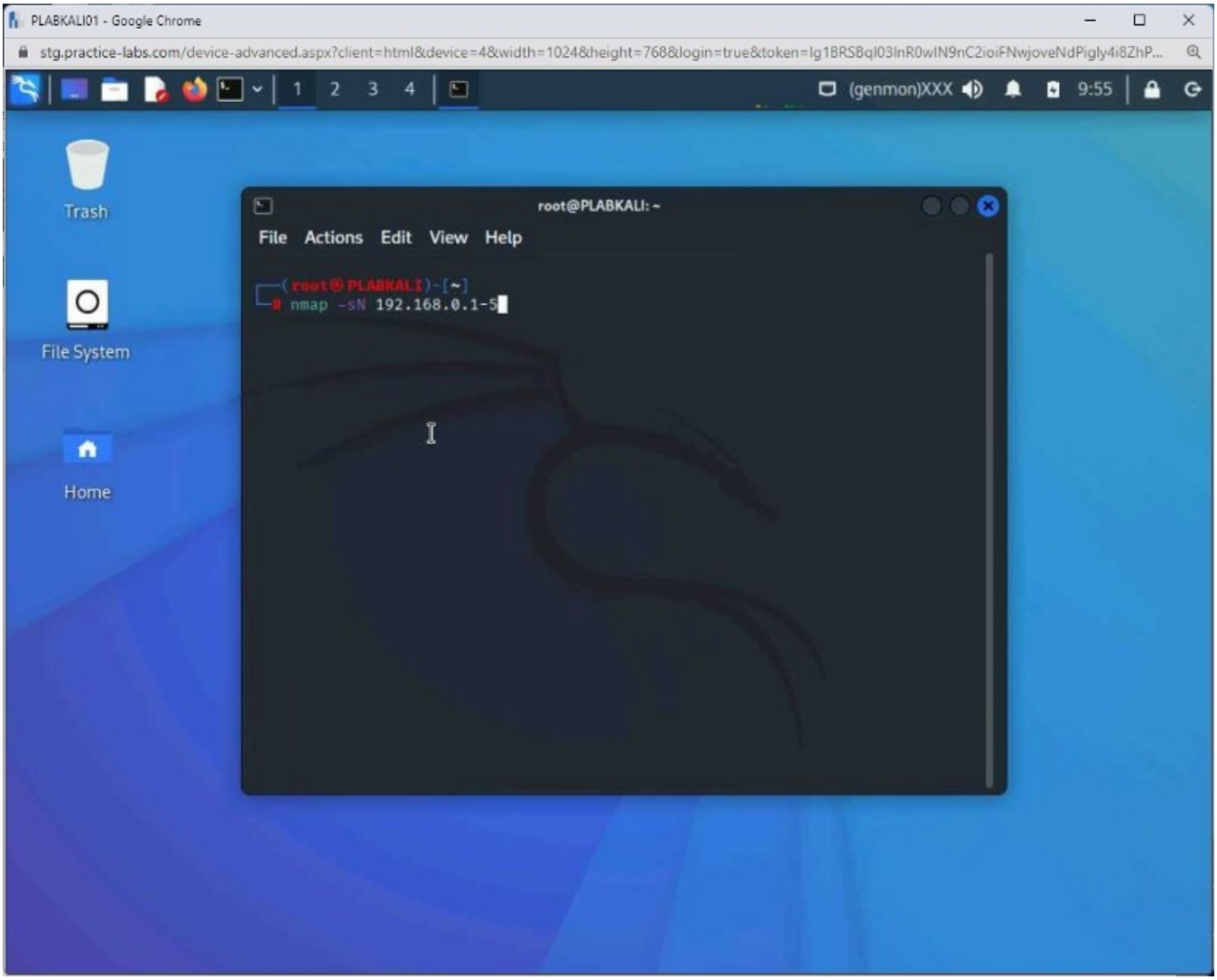
```
clear
```

You can also perform a stealth scan to avoid detecting the non-stateful firewalls. This is known as a **Null** scan. The TCP segment does not carry a flag in this type of scan. There would be at least the ACK flag raised in the usual state. To perform this type the following command:

```
nmap -sN 192.168.0.1-5
```

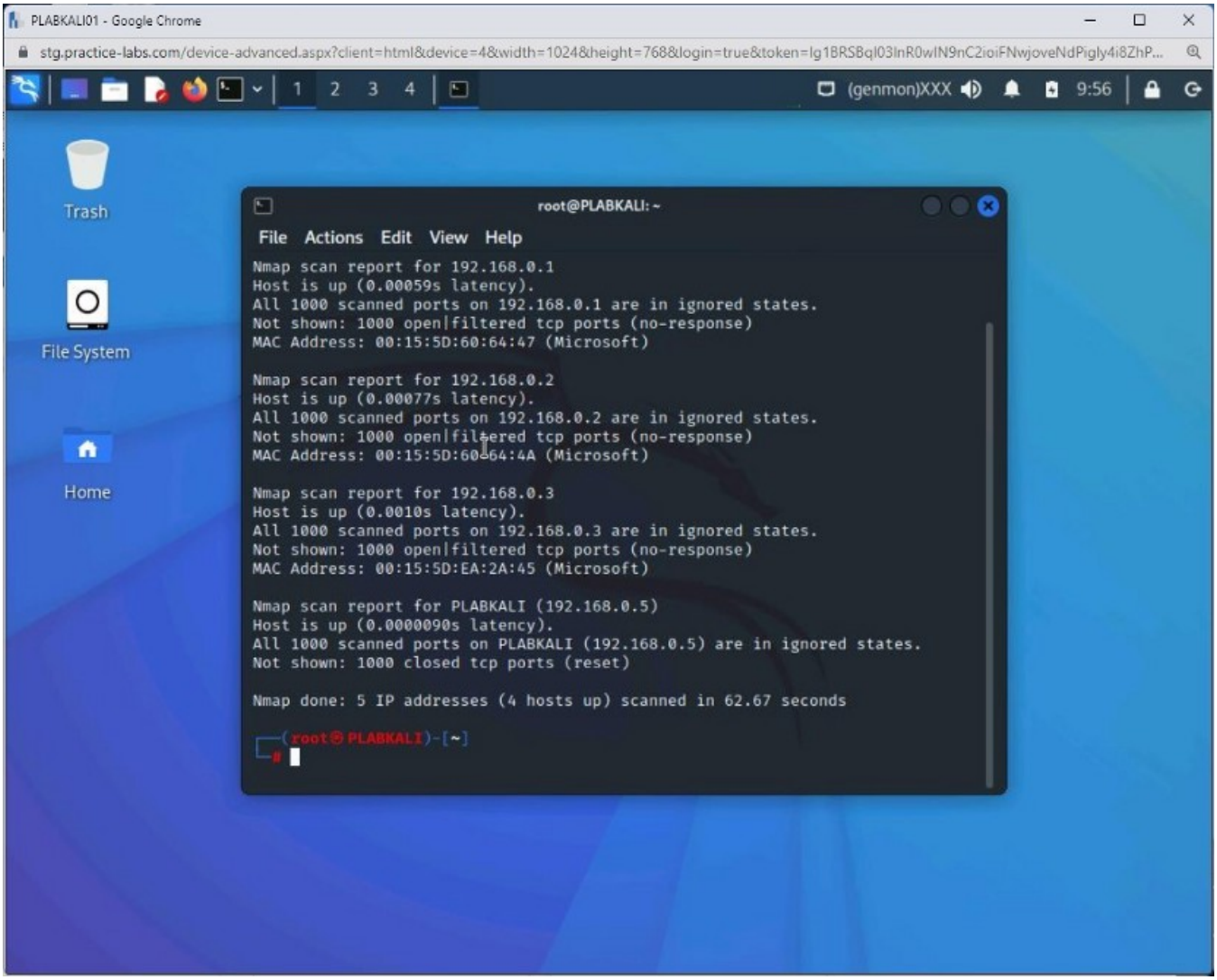
Press **Enter**.

***Note:*** *This scan takes a few minutes to provide output.*




**Step 6**

The output of this command is displayed. It lists the open and filtered ports on various target systems.




**Step 7**

Clear the screen by entering the following command:

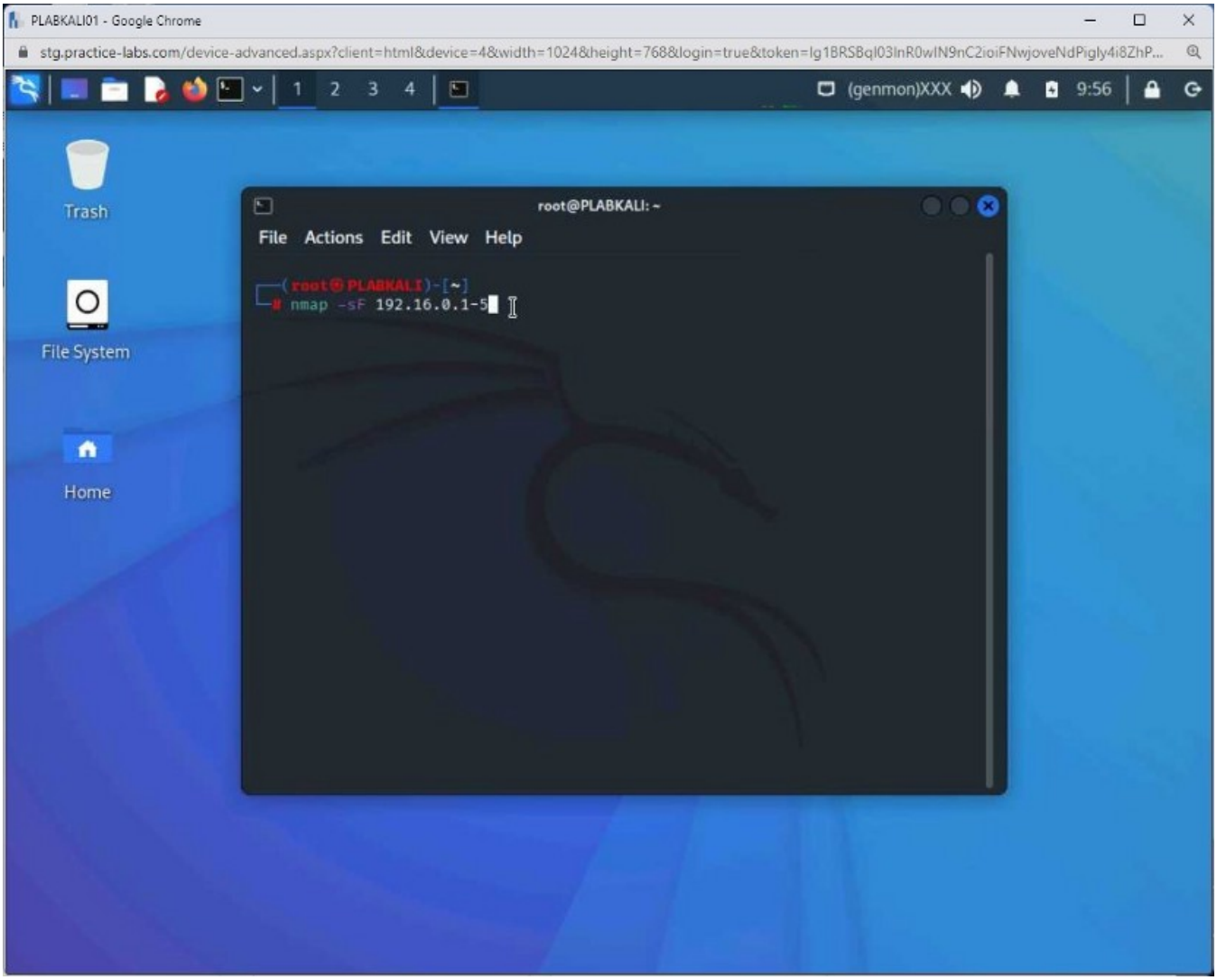
```
clear
```

Another type of stealth scan is **FIN** scan, which sends a **TCP FIN** message. To conduct a **FIN** scan, type the following command:

```
nmap -sF 192.168.0.1-5
```

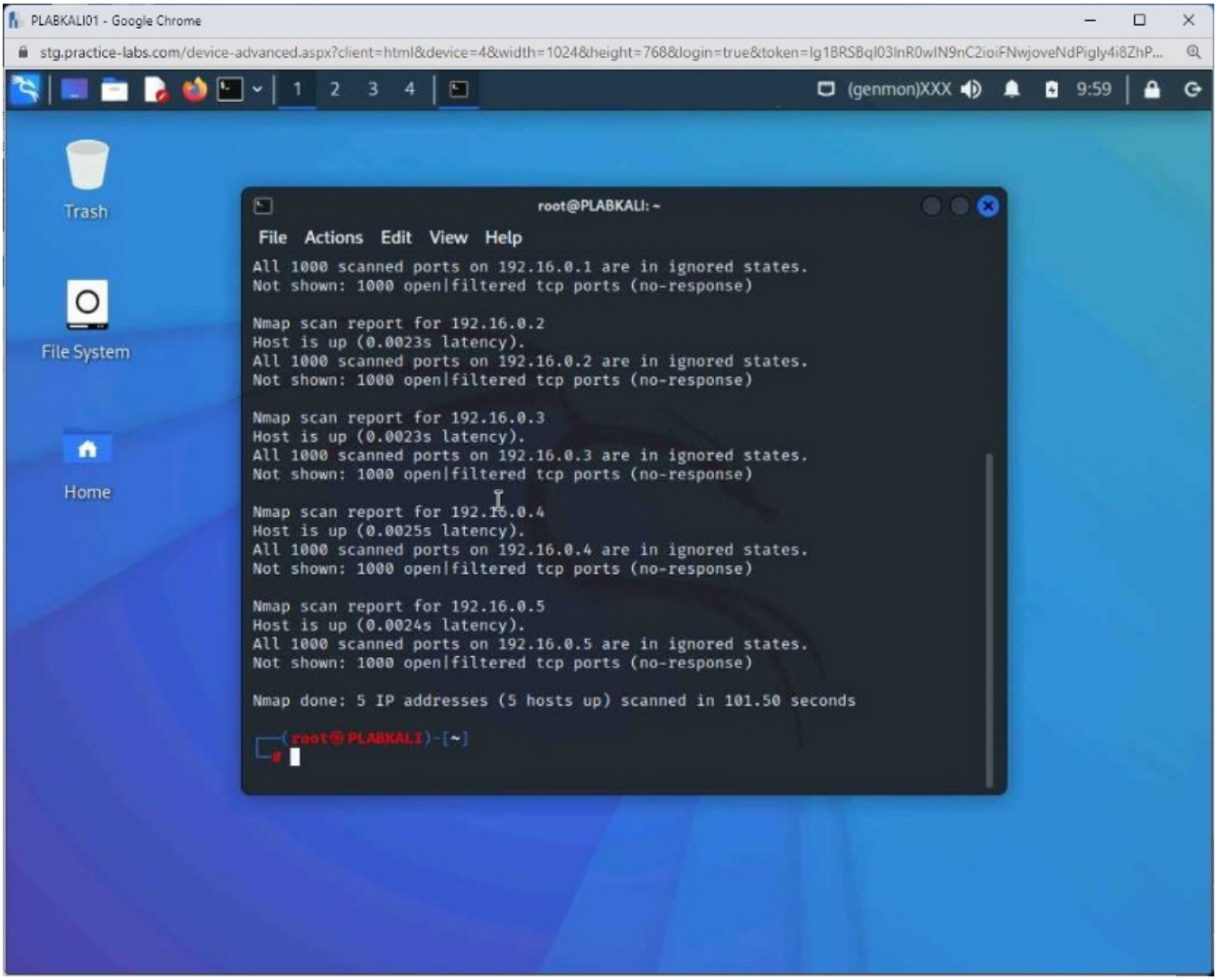
Press **Enter**.

***Note:*** *This scan takes a few minutes to provide output.*




**Step 8**

The output of this command is displayed.




**Step 9**

Clear the screen by entering the following command:

```
clear
```

The next type of stealth scan is the **Xmas** scan, which sends the **TCP** segment with **three flags** raised. These flags are **FIN**, **PSH**, and **URG**.

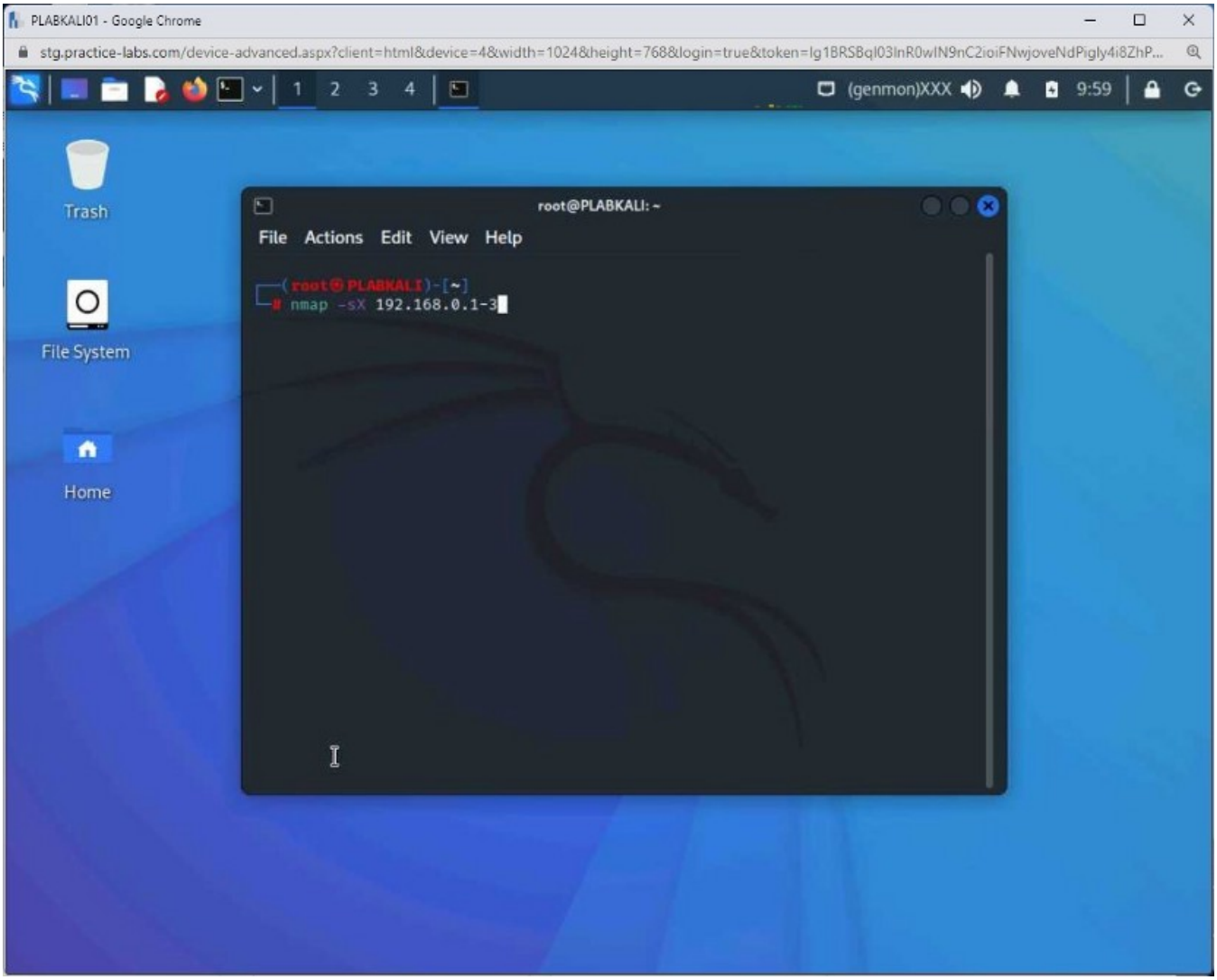
***Note:*** *The Null, FIN, and Xmas scans are used to avoid being detected by the non-stateful firewall.*

To perform an **Xmas** scan, type the following command:

```
nmap -sX 192.168.0.1-3
```

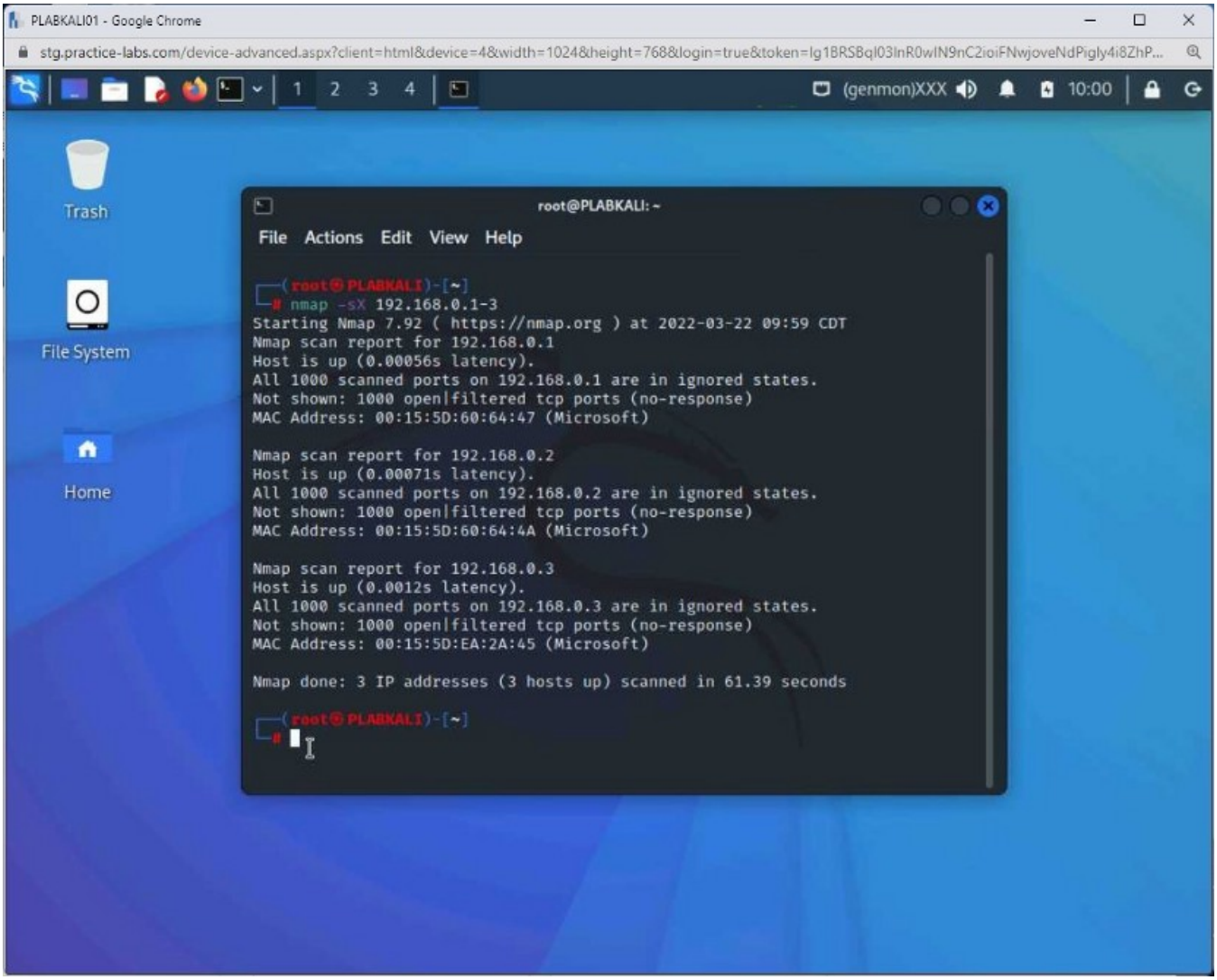
Press **Enter**.

***Note:*** *This scan takes a few minutes to provide output.*




**Step 10**

Notice the outcome of this command.




**Step 11**

Clear the screen by entering the following command:

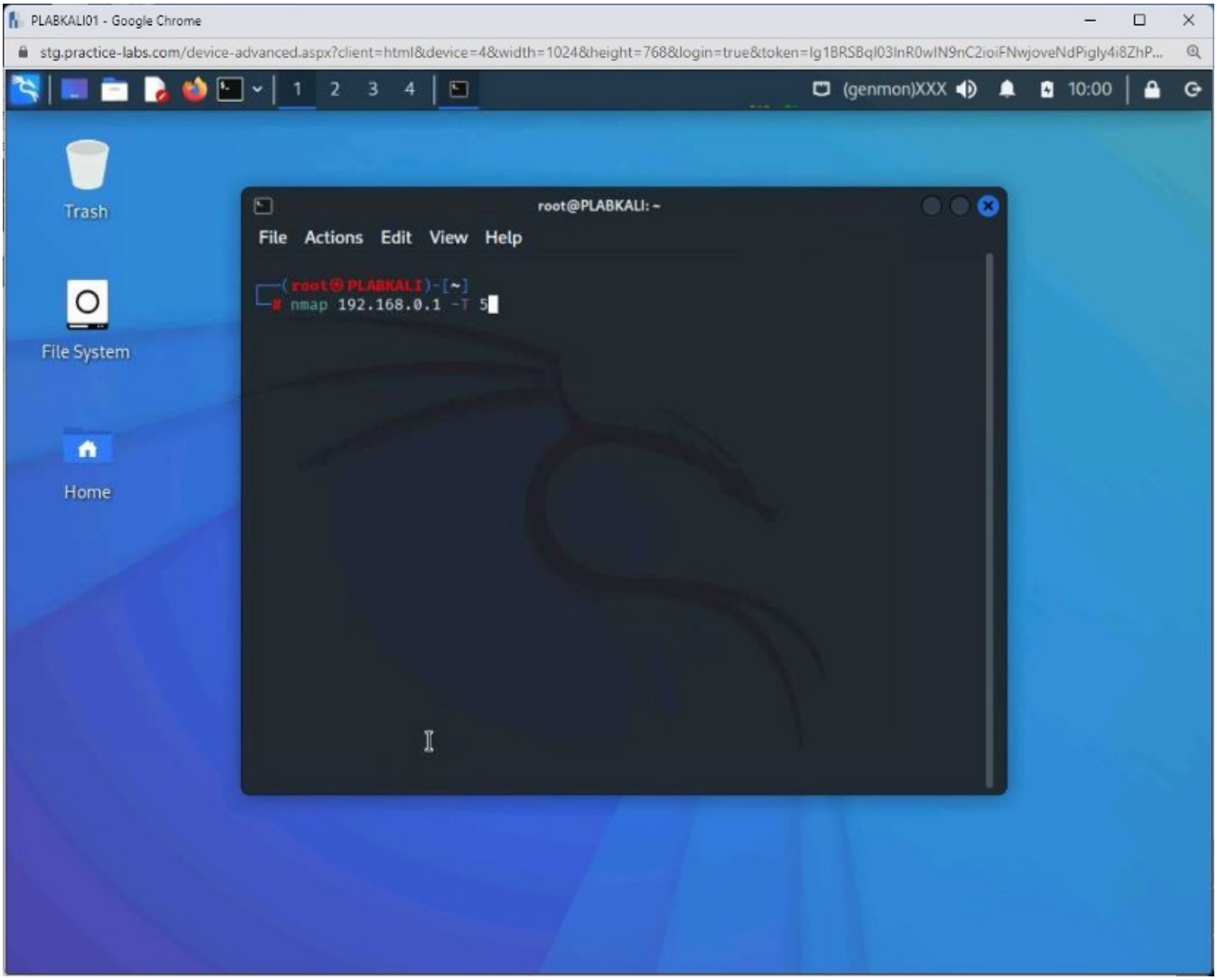
```
clear
```

You can also choose the speed of your stealth scan. For example, you choose **paranoid**, **sneaky**, **polite**, **normal**, **aggressive**, and **insane**.

These are defined as **T0** to **T5**, where **T5** is the fastest. Let's perform a **T5** scan on a system. Type the following command:

```
nmap 192.168.0.1 -T 5
```

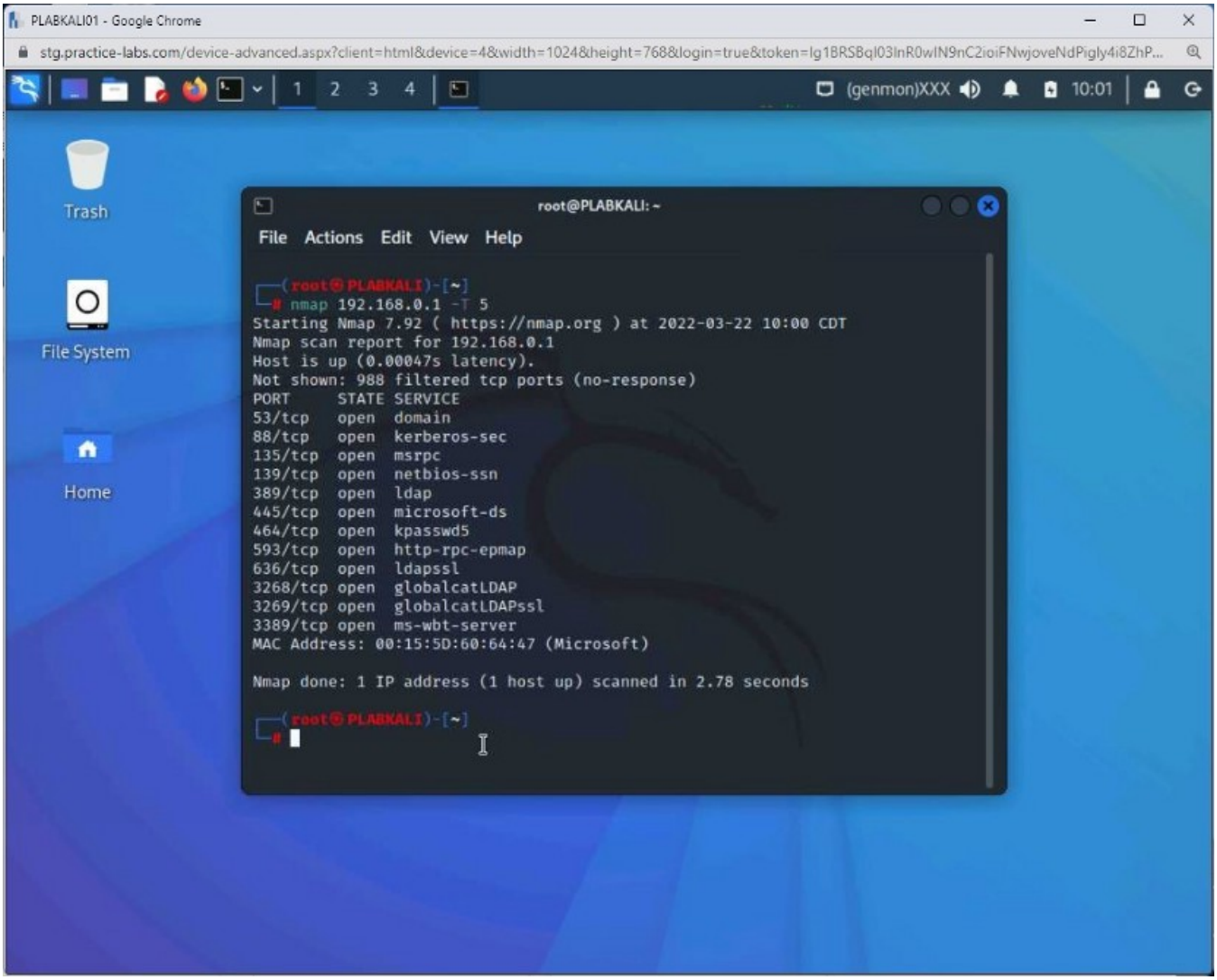
Press **Enter**.




**Step 12**

Notice the speed of the scan.

***Note:*** *You should attempt to perform a T1 or T2 scan and notice the timing difference.*




Keep the terminal window open.

## Task 4 — Use fping for Network Scanning

The fping tool is similar to the ping tool but has additional features. One of the additional features is that it can be used as a scanning tool. To use fping as a scanning tool, perform the following steps:

### Step 1

Ensure that you are connected to **PLABKALI01** and open the terminal window.

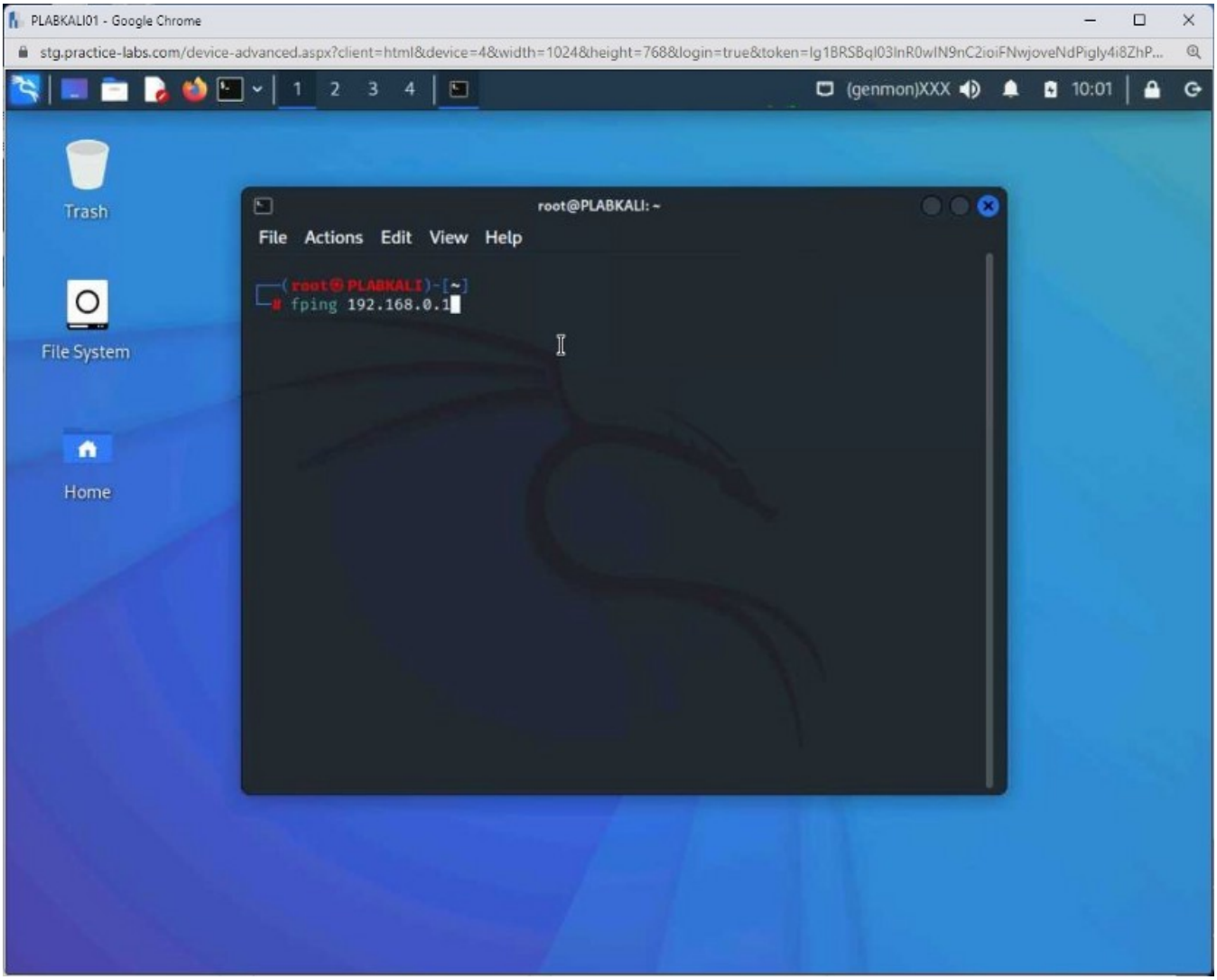
Clear the screen by entering the following command:

```
clear
```

You can simply pass the IP address to the fping command as a parameter to check if a system is alive on the network. Type the following command:

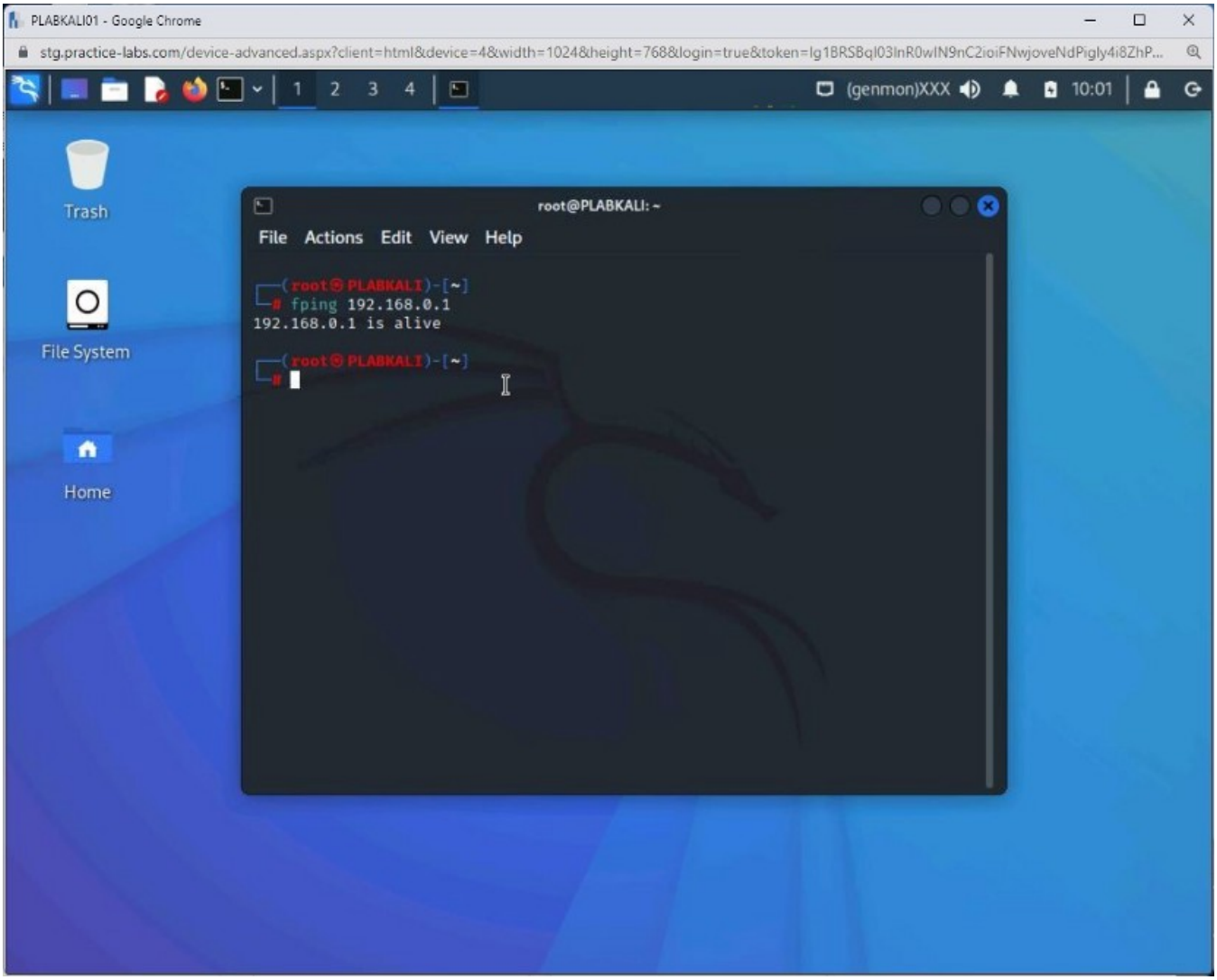
```
fping 192.168.0.1
```

Press **Enter**.




### Step 2

Notice the output, which shows that the mentioned system is live on the network.

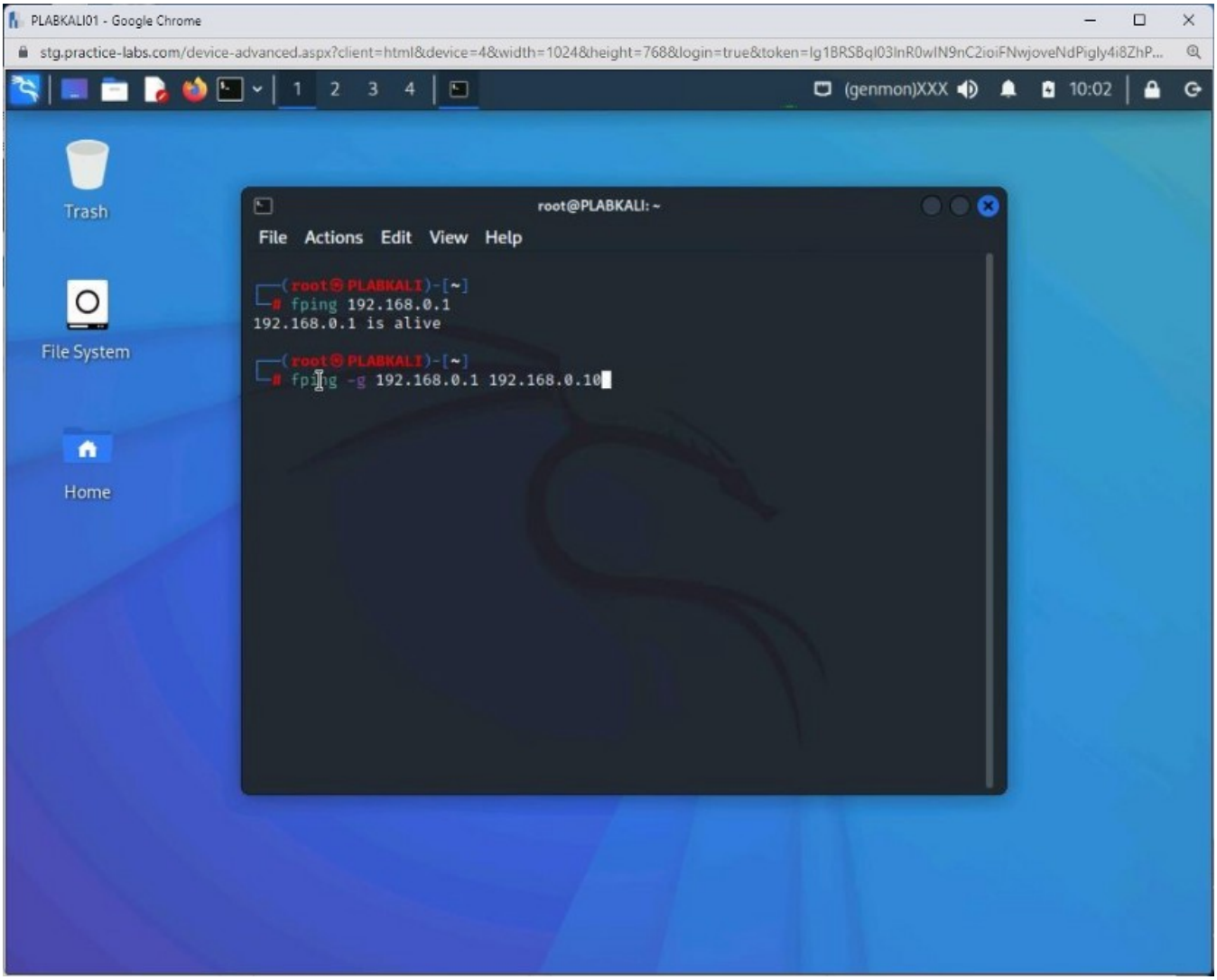



**Step 3**

Using the **-g** parameter, you can scan for more than one system on the network. To do this, type the following command:

```
fping -g 192.168.0.1 192.168.0.10
```

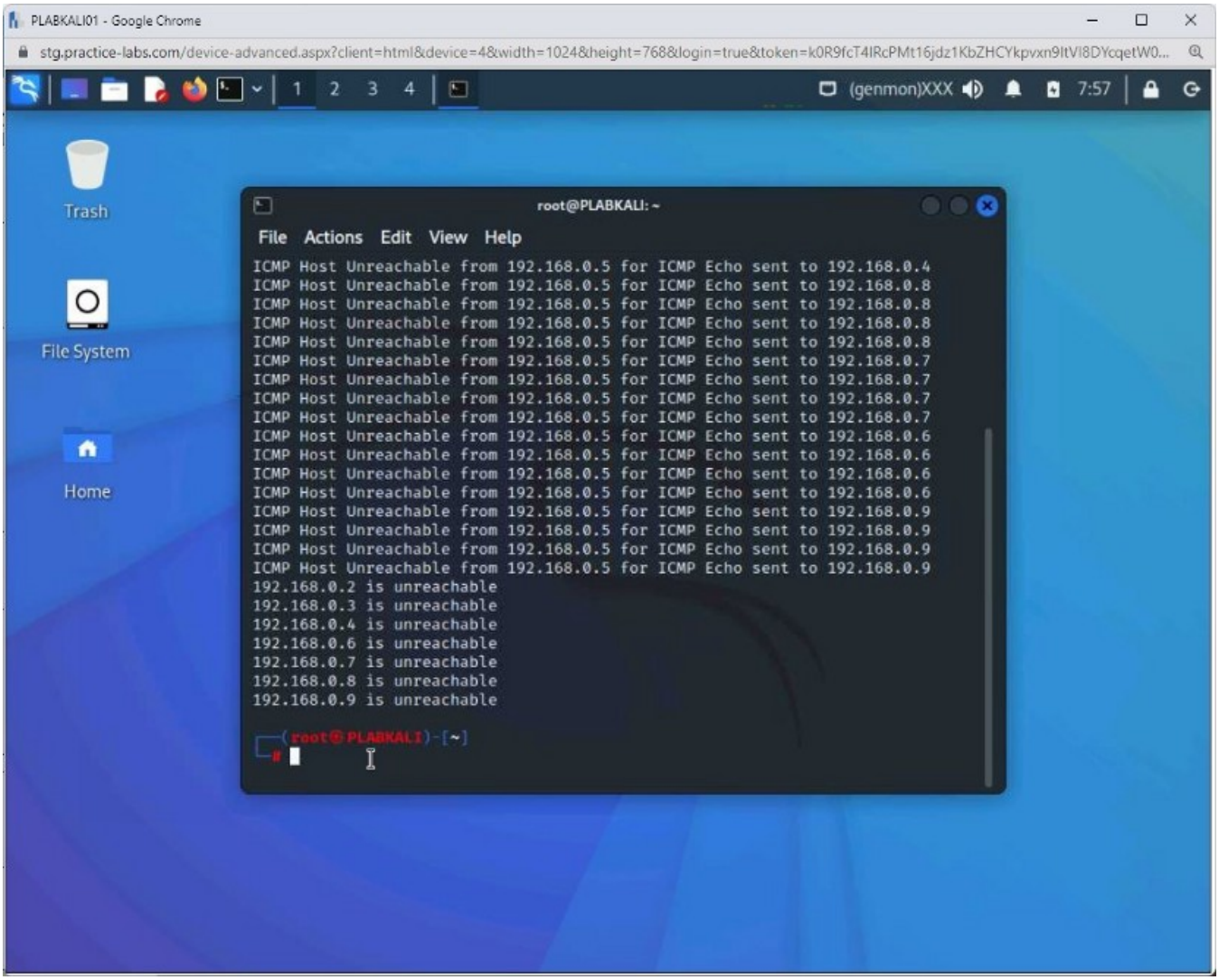
Press **Enter**. This command will scan the range from 192.168.0.1 to 192.168.0.10.




**Step 4**

Notice that output displays the status of each of the systems.'

***Note**: Which IP addresses are listed as alive will depend on which devices are currently powered on.*




#### Step 5

Clear the screen by entering the following command:

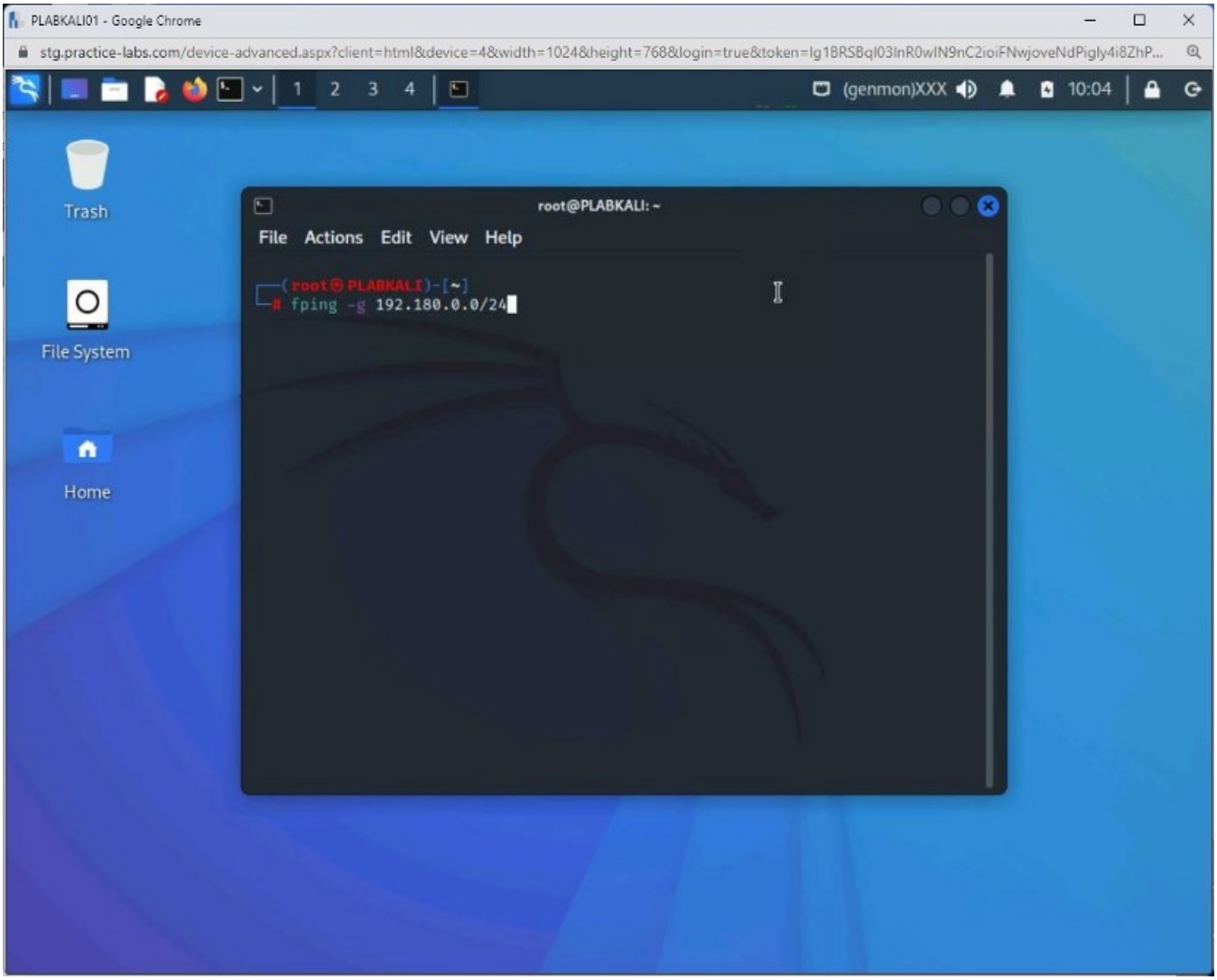
```
clear
```

Press **Enter**.

Using the **-g** parameter, you can scan an entire subnet using the **CIDR** notation. To do this, type the following command:

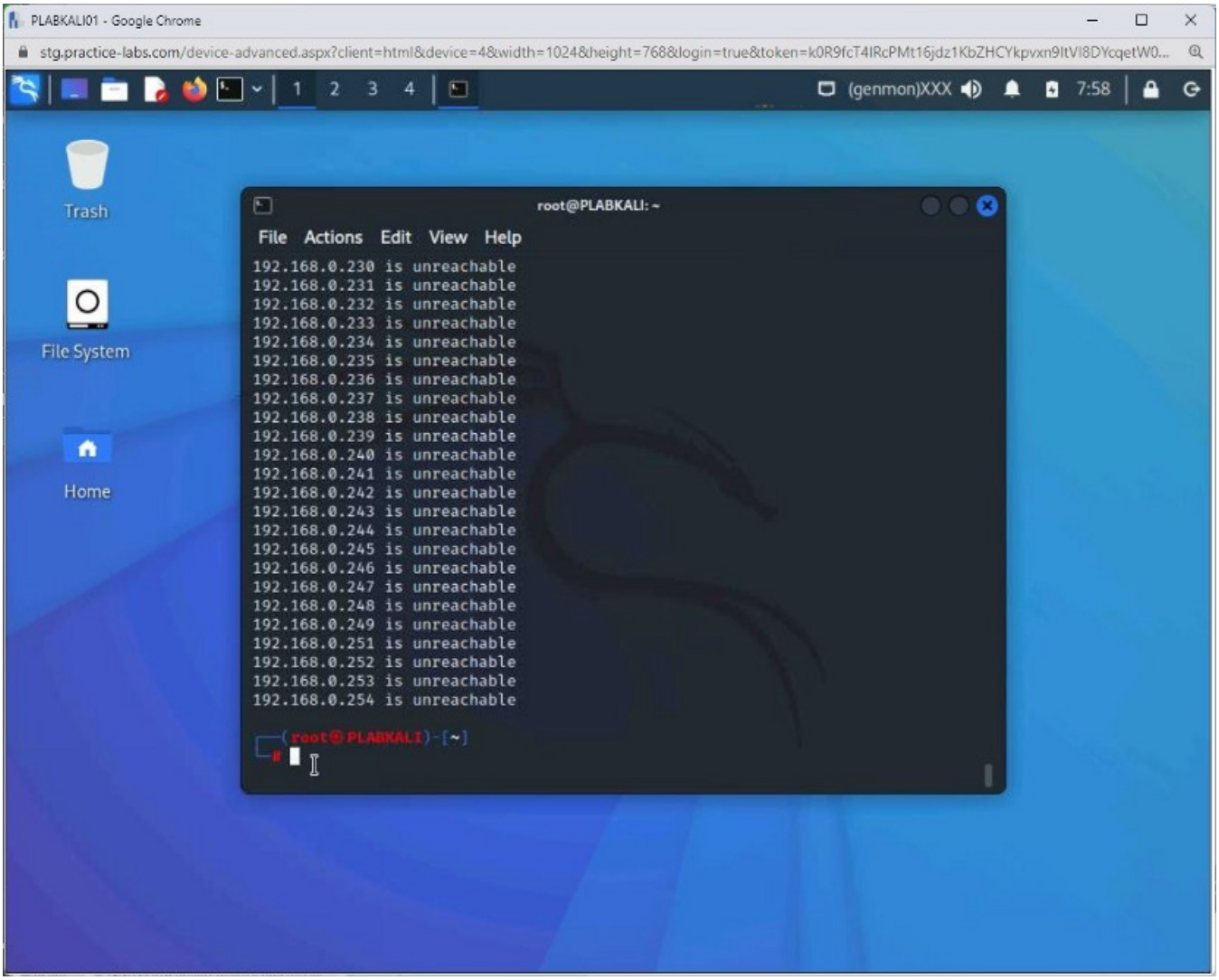
```
fping -g 192.168.0.0/24
```

Press **Enter**.




**Step 6**

Notice the output scans for the live systems on the entire subnet and list each IP address's status.




Close the terminal window.

## Task 5 — Explore a Network Using Zenmap

Nmap has a graphical user interface (GUI) named Zenmap, which has the same capabilities as Nmap. You can scan for ports, services, and so on. Instead of executing commands on the command line, you get a visual tool to execute commands instead.

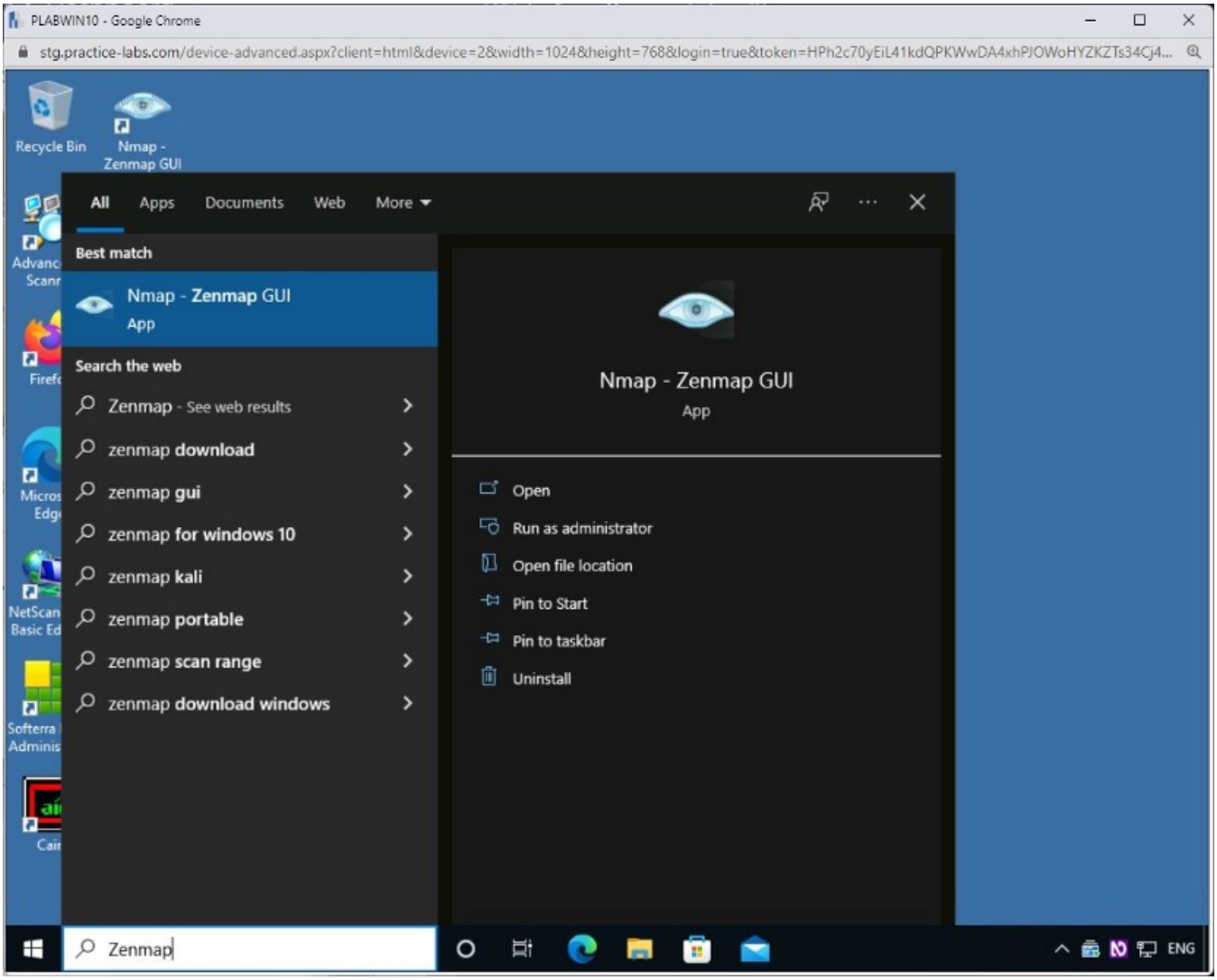
In this task, you will explore a network using Zenmap. To do this, perform the following steps:

### Step 1

Connect to **PLABWIN10**. In the **Type here to search** textbox, type the following:

```
Zenmap
```

From the search results, select **Nmap — Zenmap GUI**.




**Step 2**

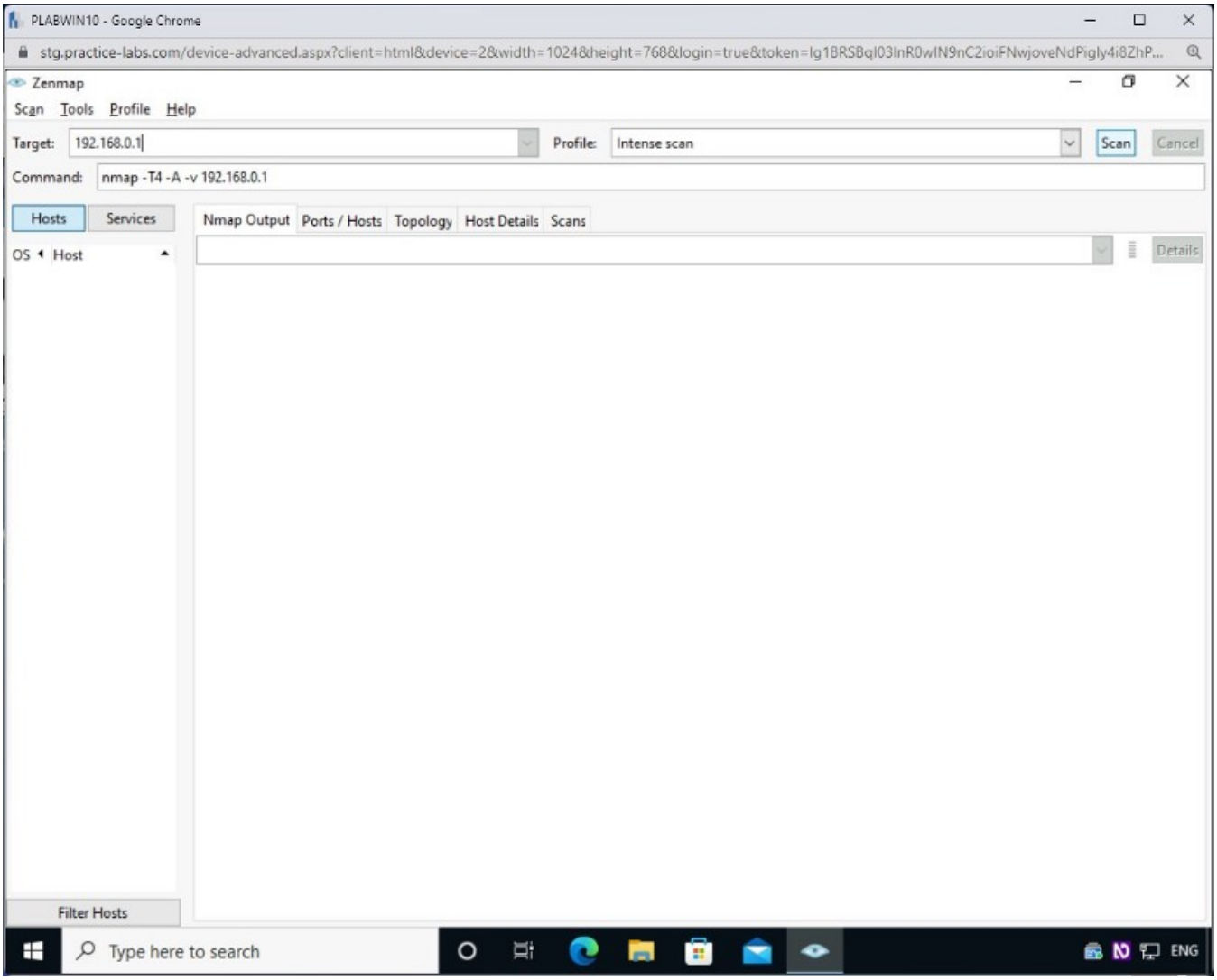
The **Zenmap** window is displayed. The top section has three key fields:

- **Target**: this is the system that you want to scan.
- **Profile**: is a pre-defined scan method. Default is an **Intense** scan.
- **Command**: this is entered based on the profile selection. You can choose to type a command manually.

In the **Target** text box, type the following IP address:

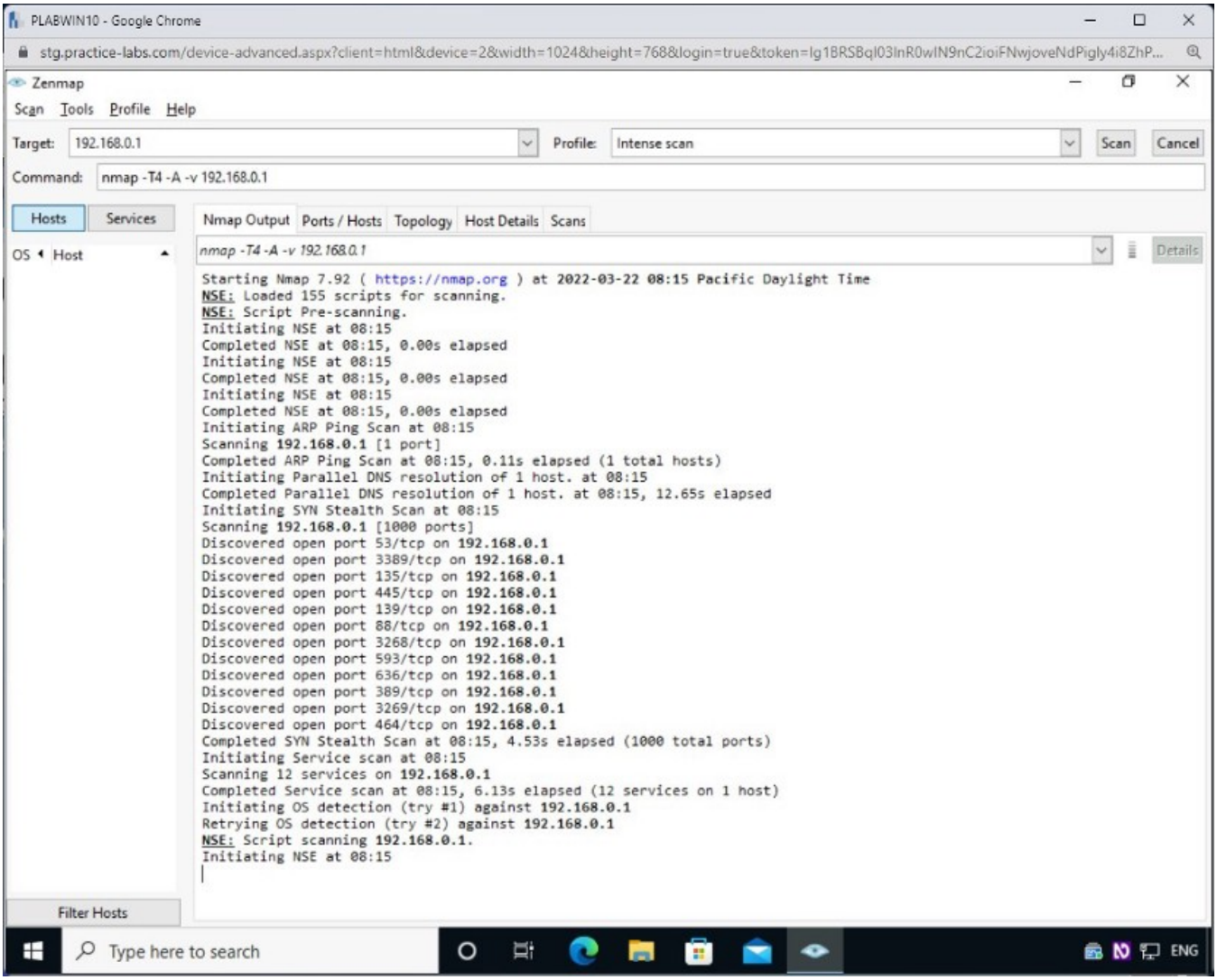
```
192.168.0.1
```

Click **Scan**. Notice that the **Command** textbox uses a pre-defined formula based on the **Profile** that you select.




### Step 3

The output is displayed on the **Nmap Output** tab in the right pane.

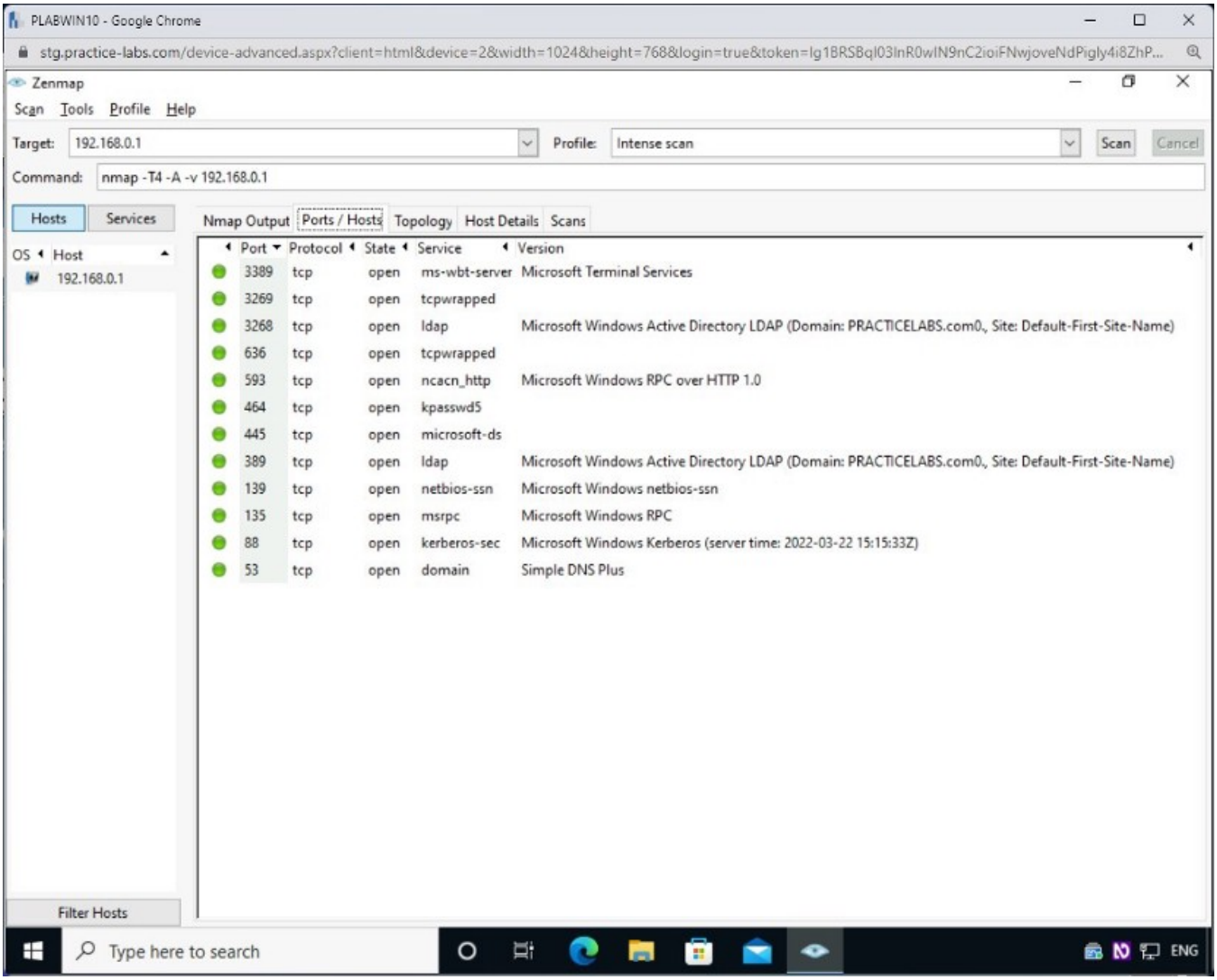



**Step 4**

To view the ports information only, click the **Ports / Hosts** tab.

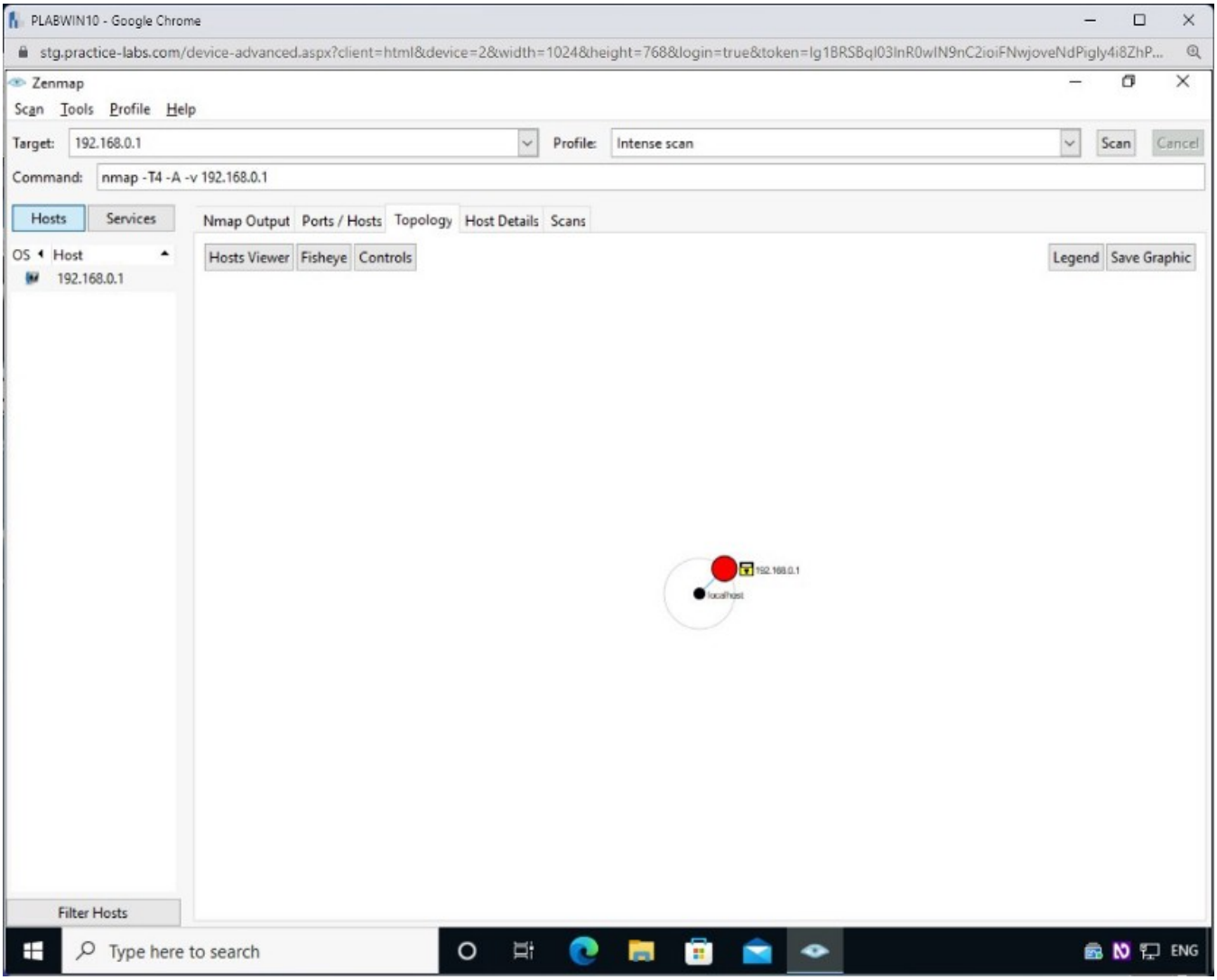
Notice that this tab only displays the open ports information. You get a list of ports, states, protocol, and version details.

***Note**: This and subsequent tabs will only populate once the command has fully executed.*



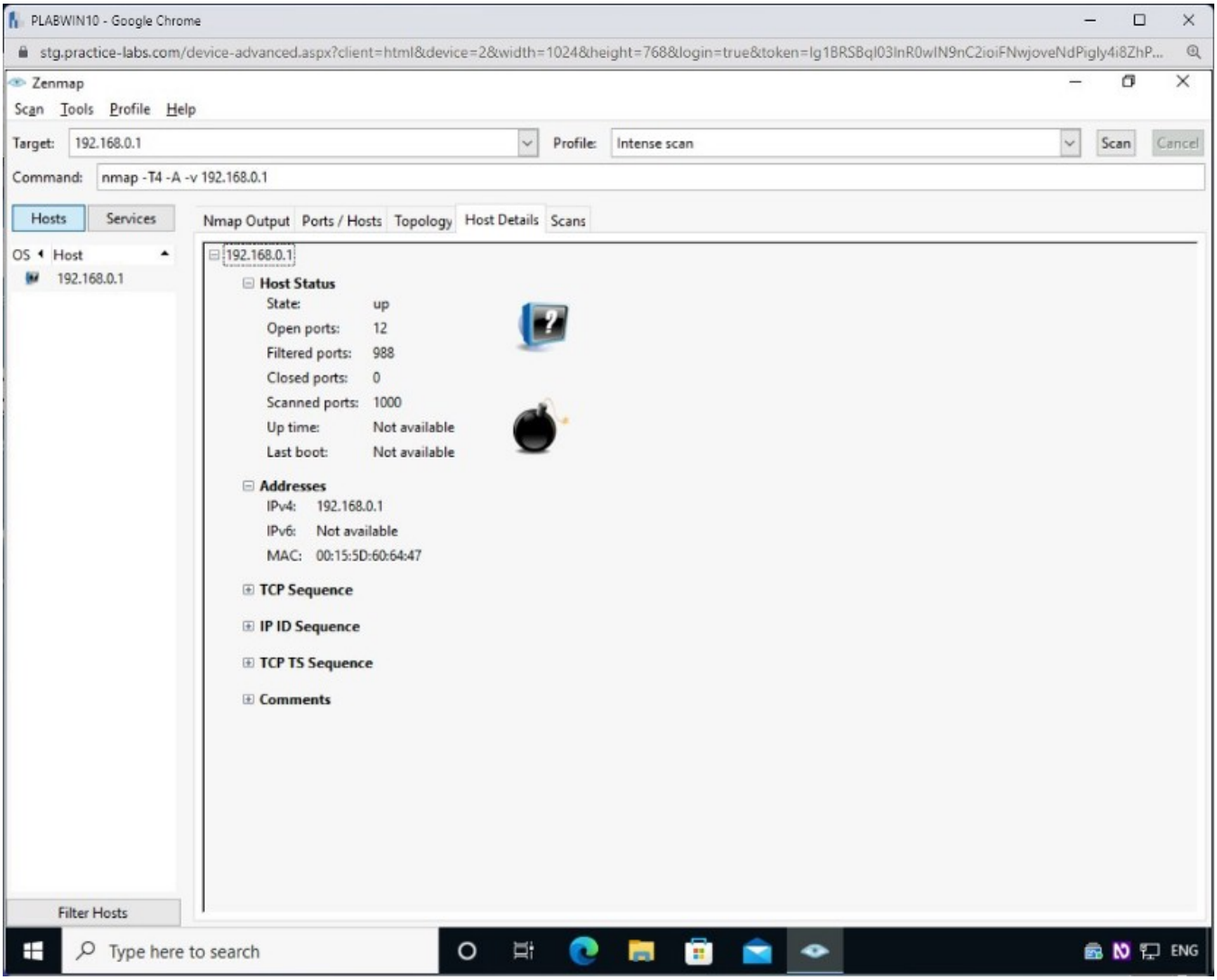

### Step 5

Click the **Topology** tab. The topology for **192.168.0.1** is displayed.




### Step 6

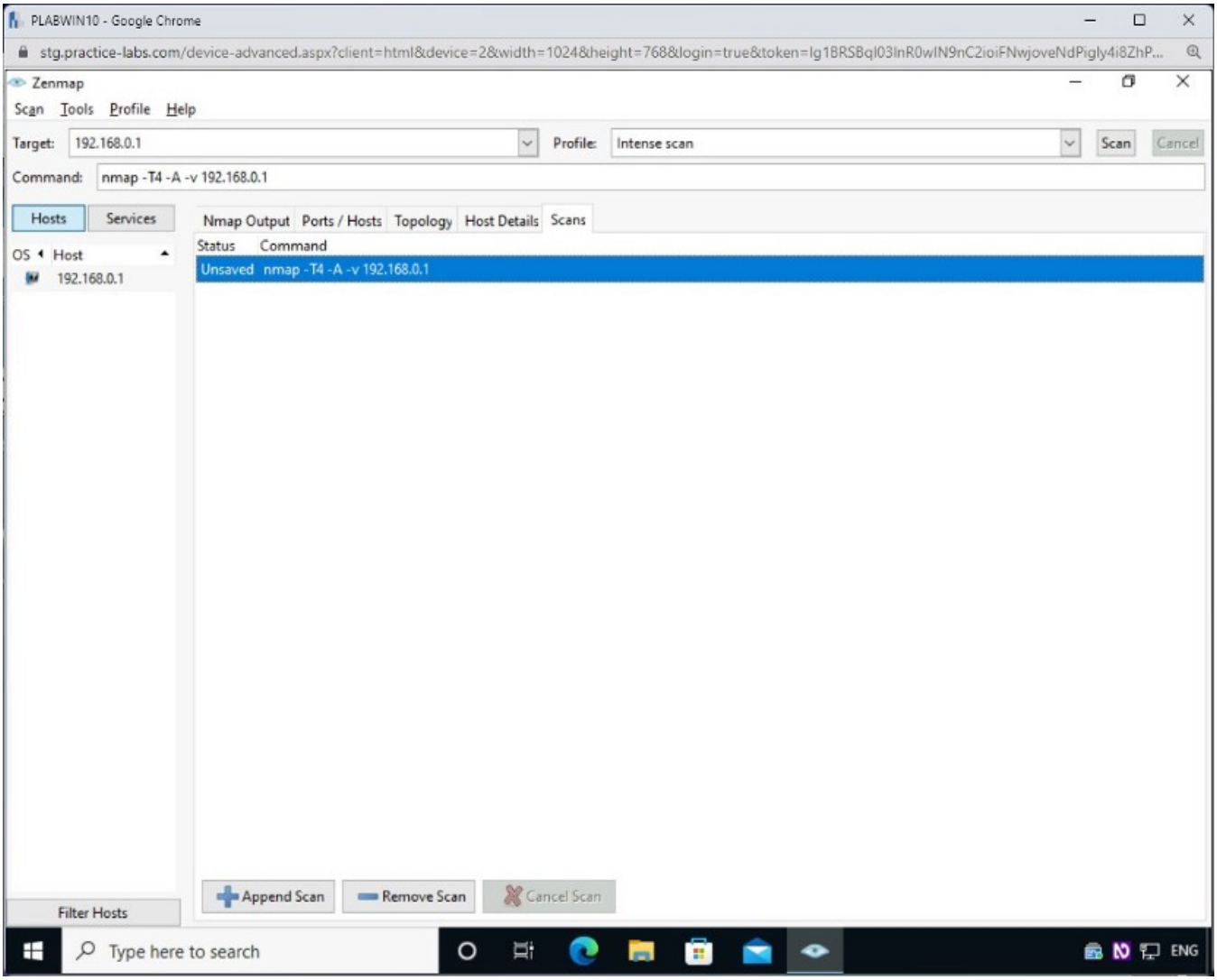
Click the **Host Details** tab. Notice that it displays quite a bit of detail. You can find its state, which is up, open ports, filtered ports, and scanned ports.




### Step 7

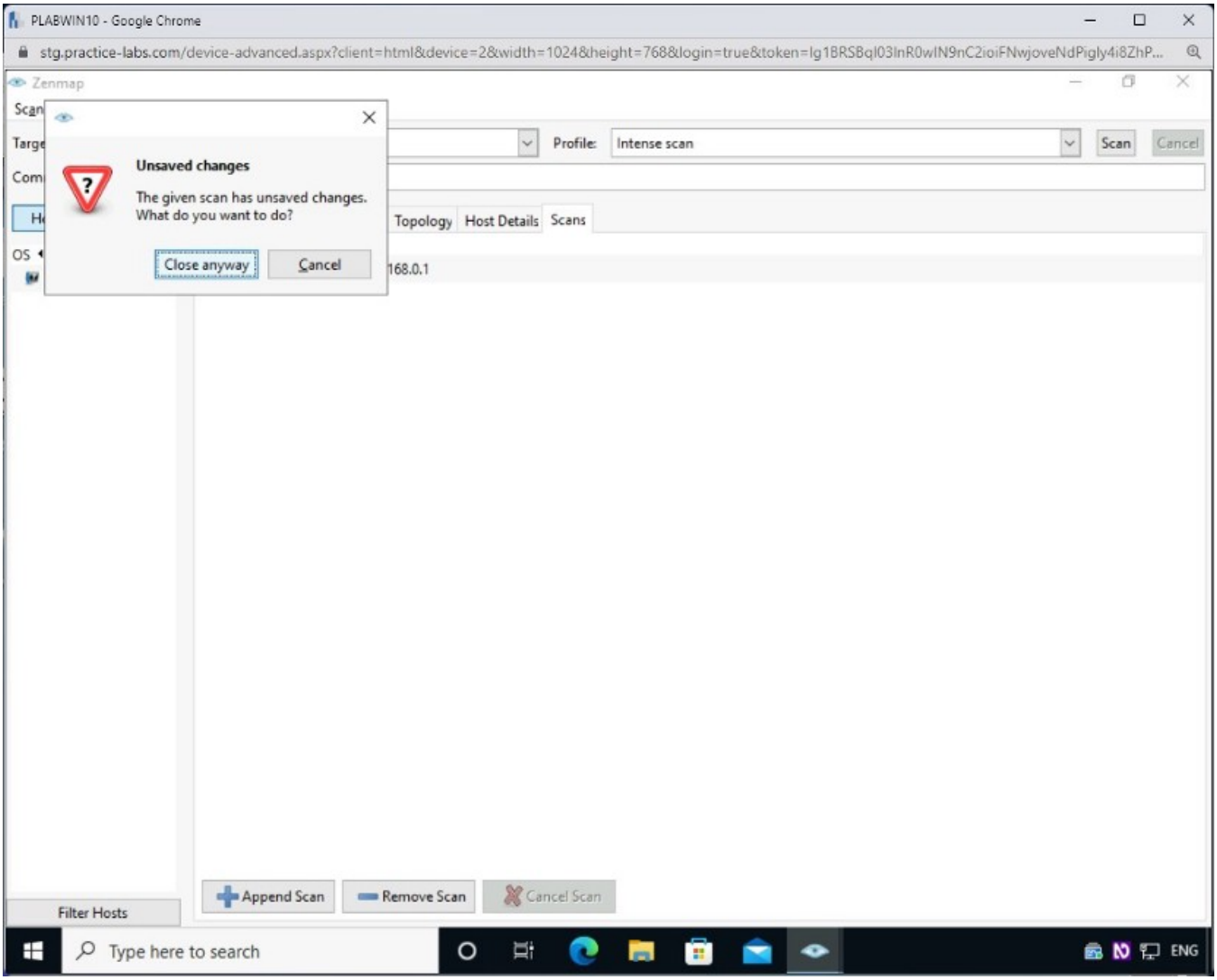
Click the **Scans** tab. Notice that it displays the command executed to get the information about the target system.

***Note:*** *The current scan is unsaved. You can use the* ***Scan*** *>* ***Save Scan*** *option to save the scan. Alternatively, you can press the* ***Ctrl*** *+* ***S*** *keys to save the scan.*




### Step 8

Close the **Zenmap** window. When prompted to save changes, click **Close anyway**.




## Task 6 — Use MyLanViewer to Scan a Network

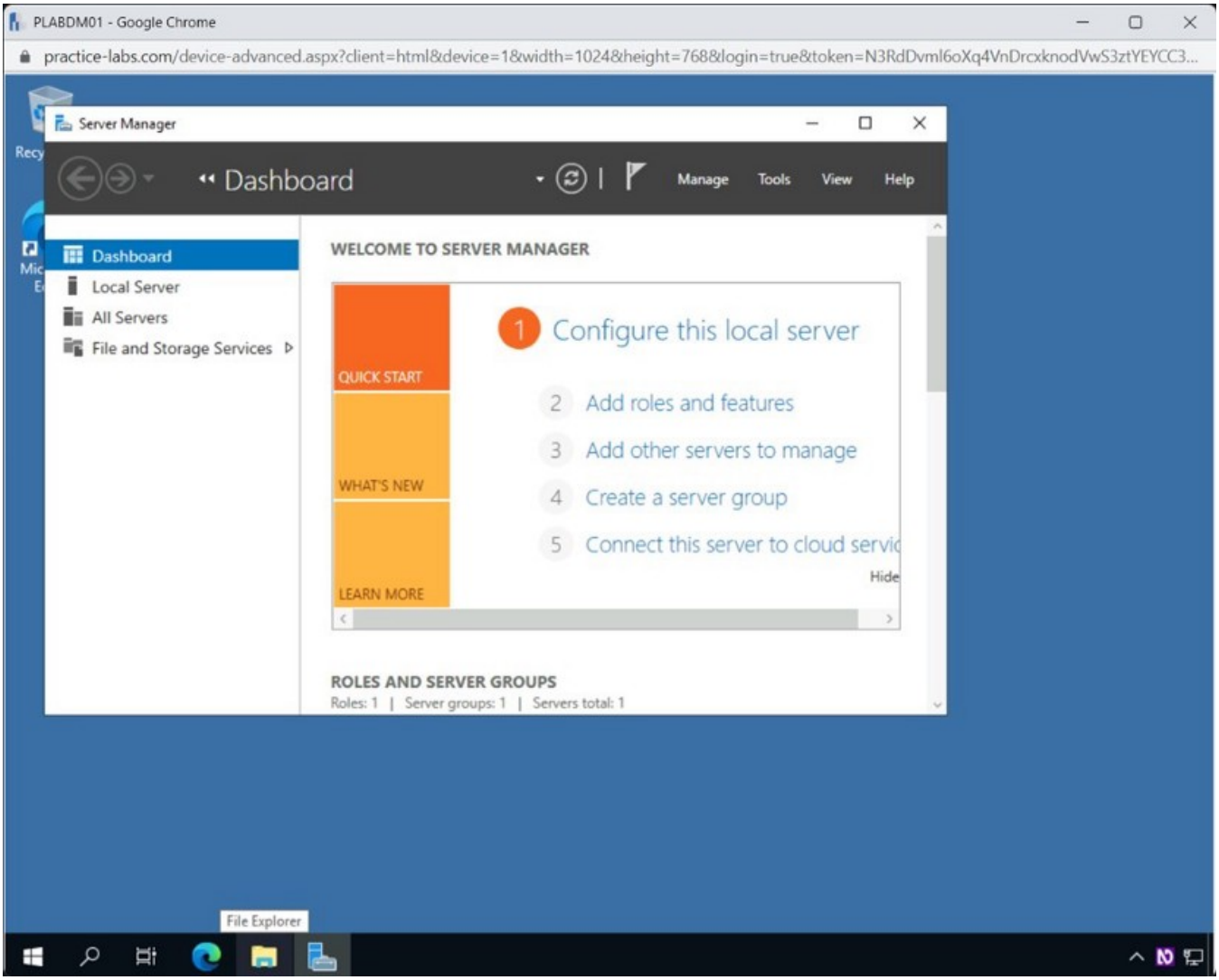
MyLanViewer is a network and IP Scanner. It is also a tool that can search the Whois database. You can use it for multiple purposes, such as:

- traceroute
- remote shutdown
- Wake On LAN (WOL) manager
- wireless network scanner and monitor.

In this task, you will use MyLanViewer to scan the network. To use MyLanViewer, perform the following steps:

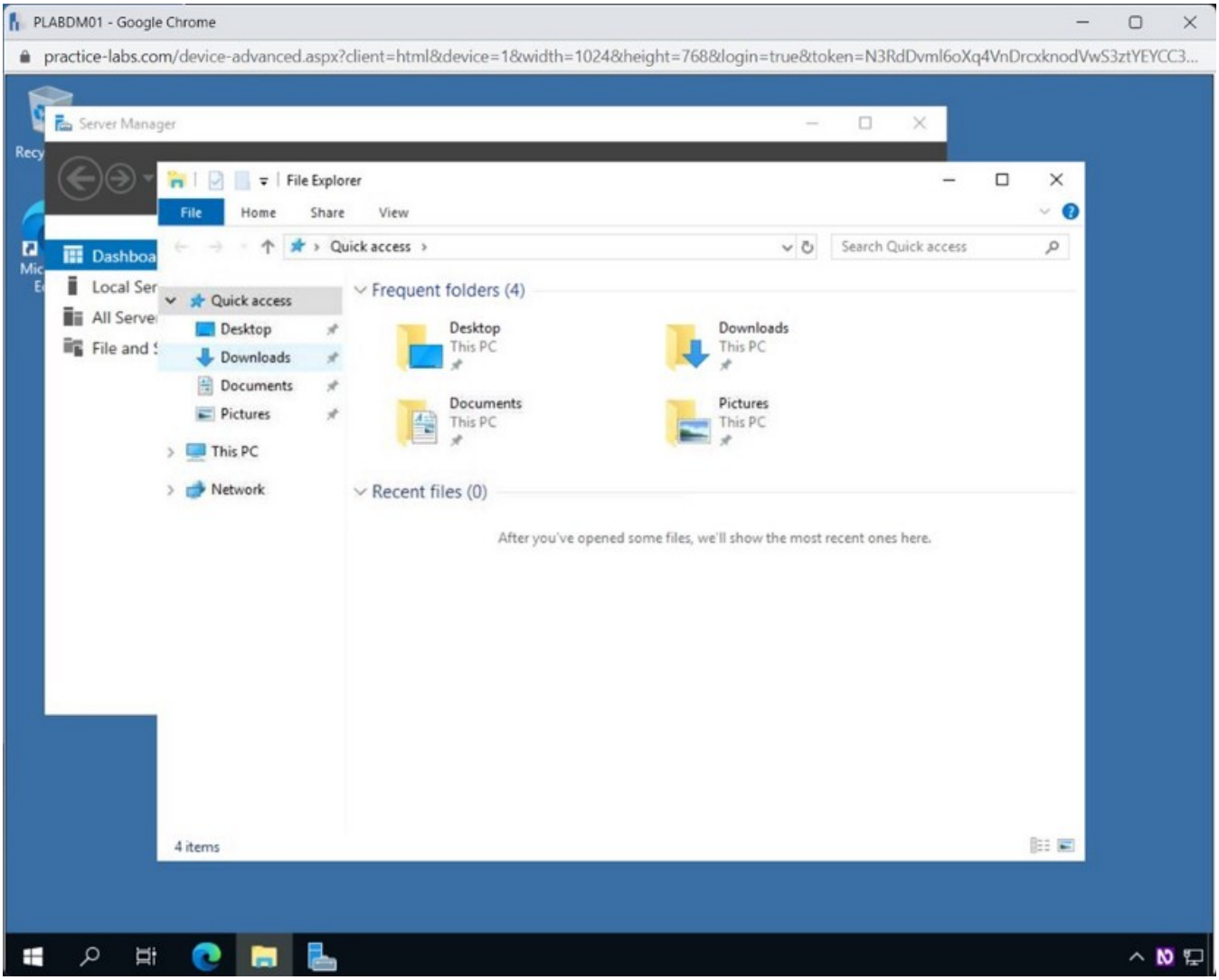
### Step 1

Connect to **PLABDM01**, from the **Taskbar** and open **File Explorer**.



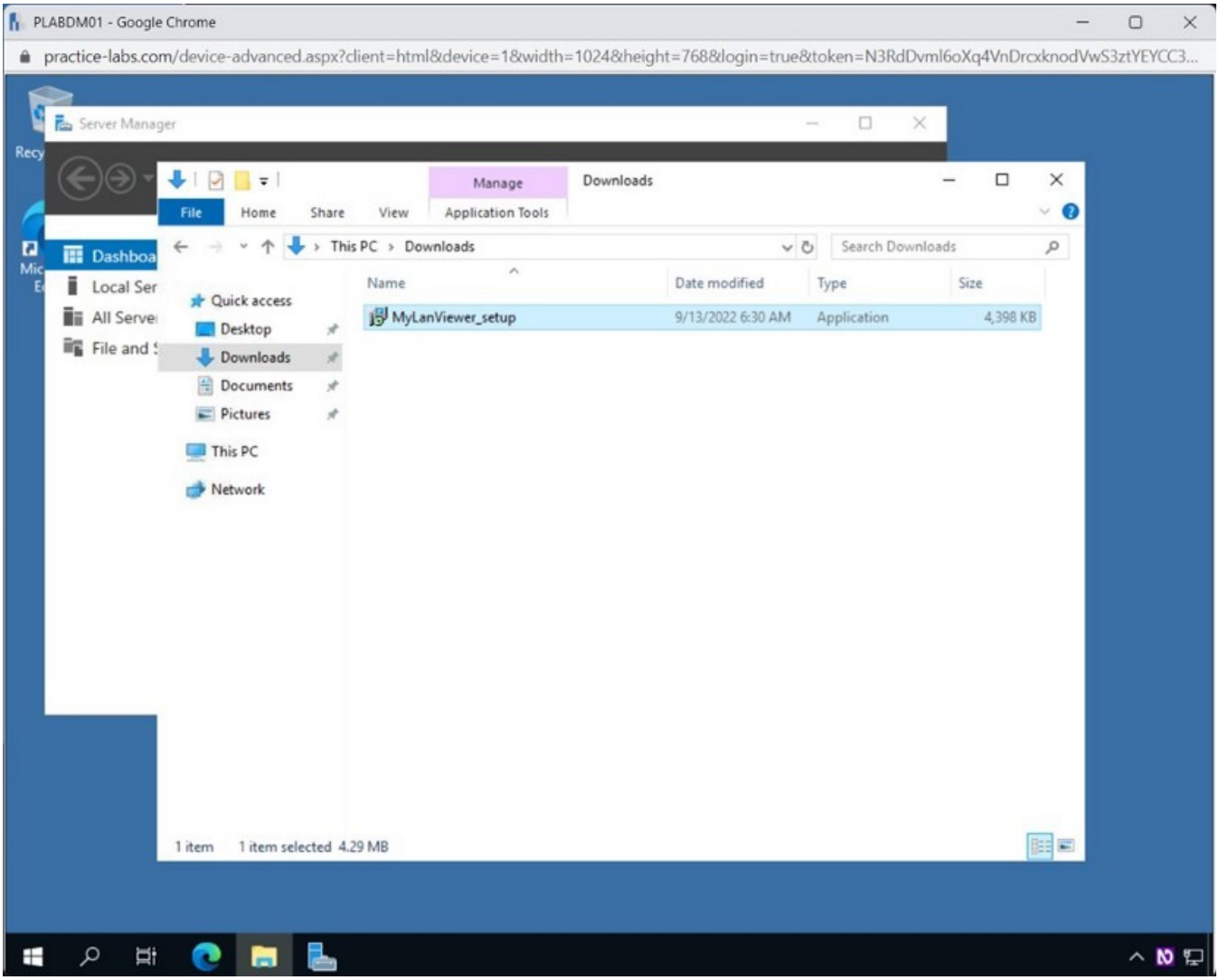

**Step 2**

In **File Explorer,** select **Downloads**.



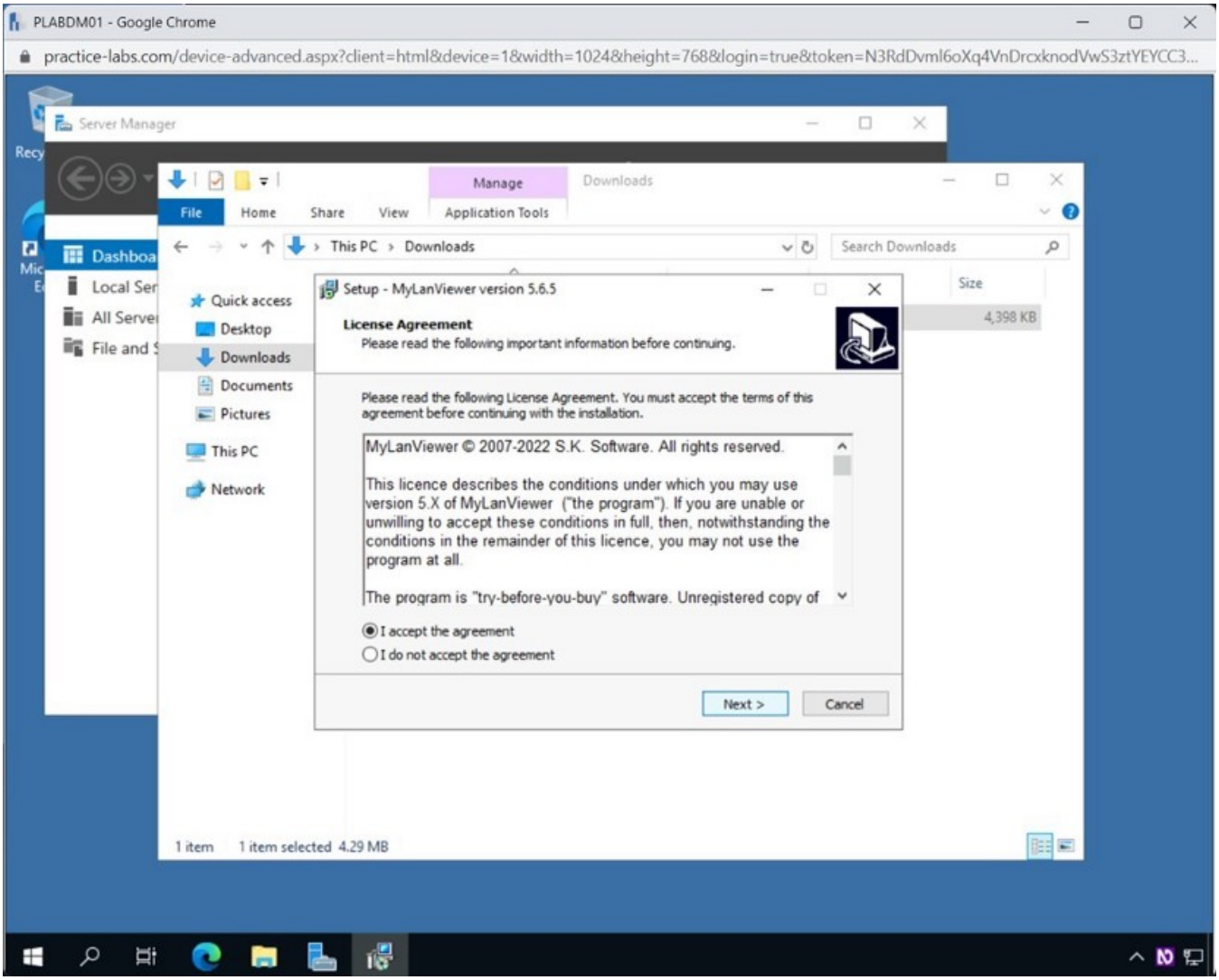

### Step 3

In the **Downloads** folder, double-click the **MyLanViewer_setup** file.



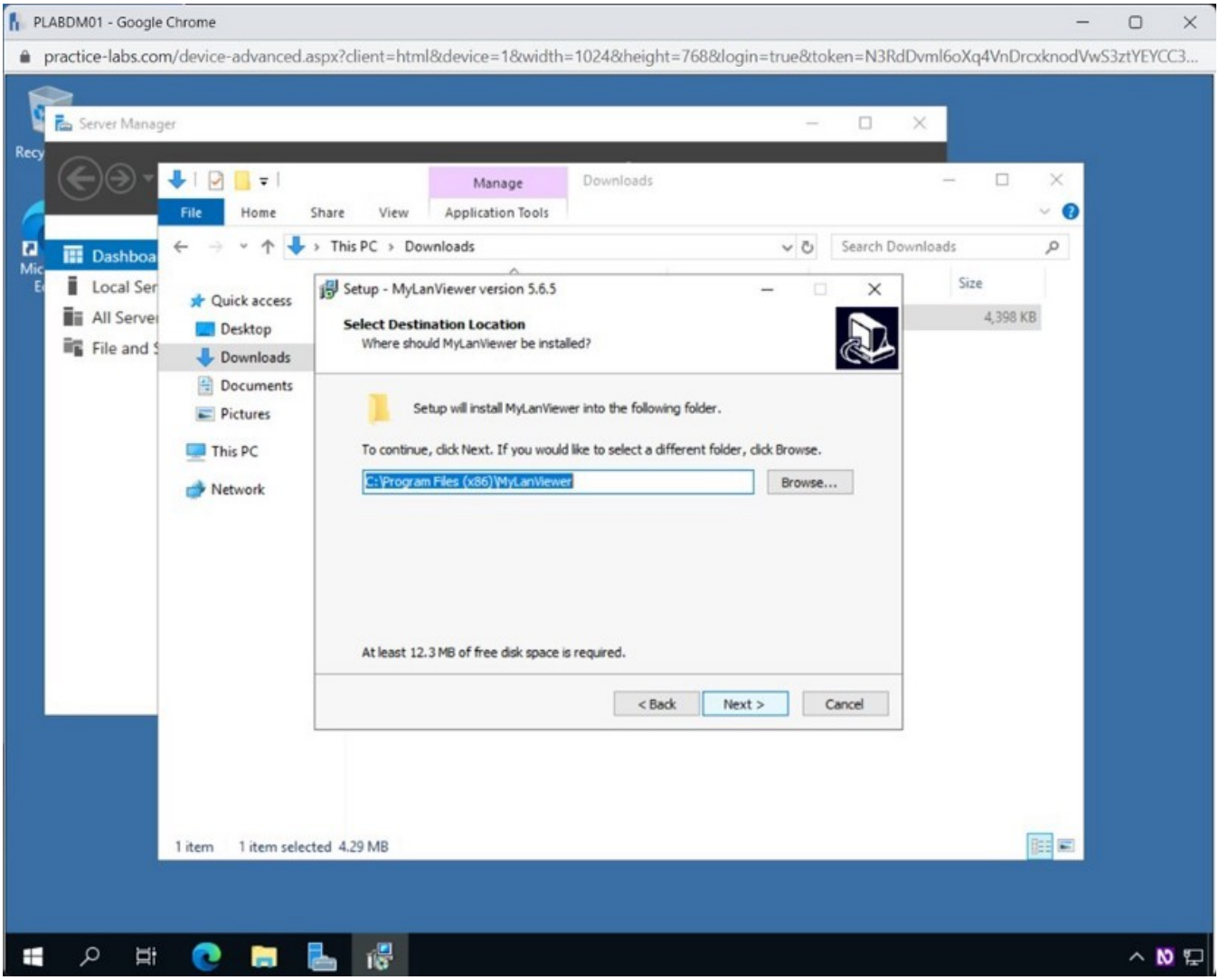

### Step 4

In the **Setup — MyLanViewr version 5.6.5** pop-up window, select the **I accept the agreement** radio button and click **Next**.



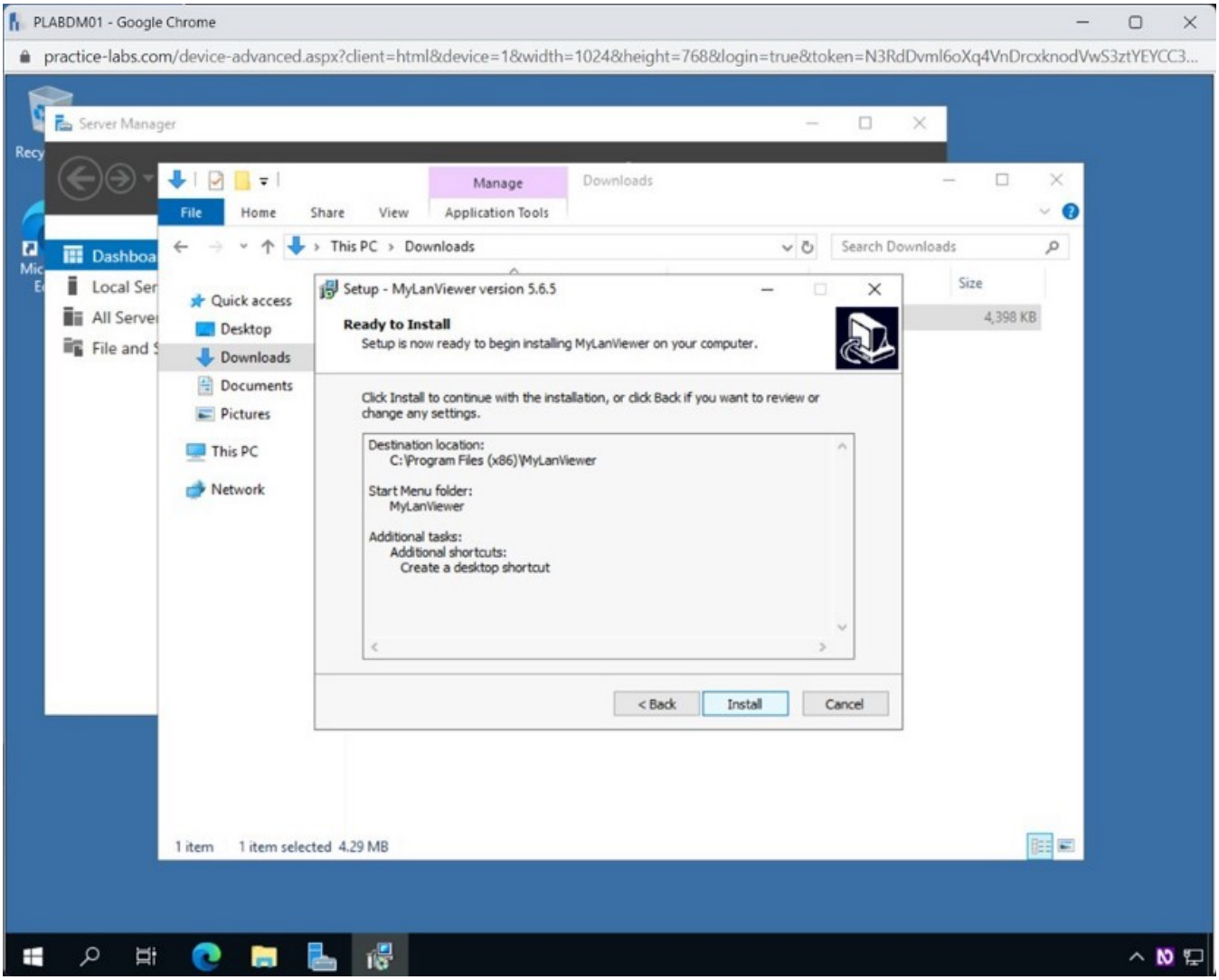

### Step 5

Click **Next,** keeping all the default selections.



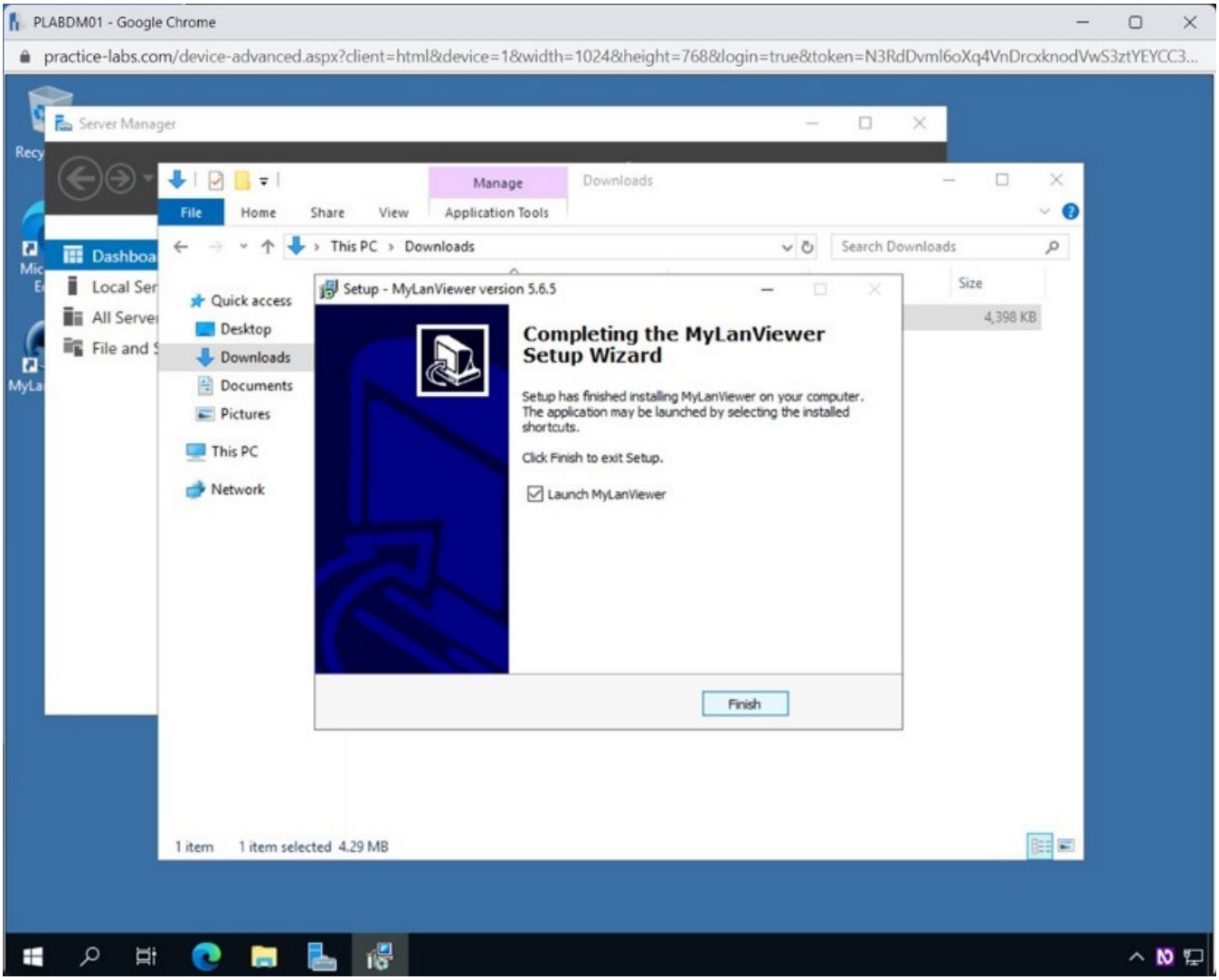

### Step 6

On the **Ready to Install** window, select **Install**.



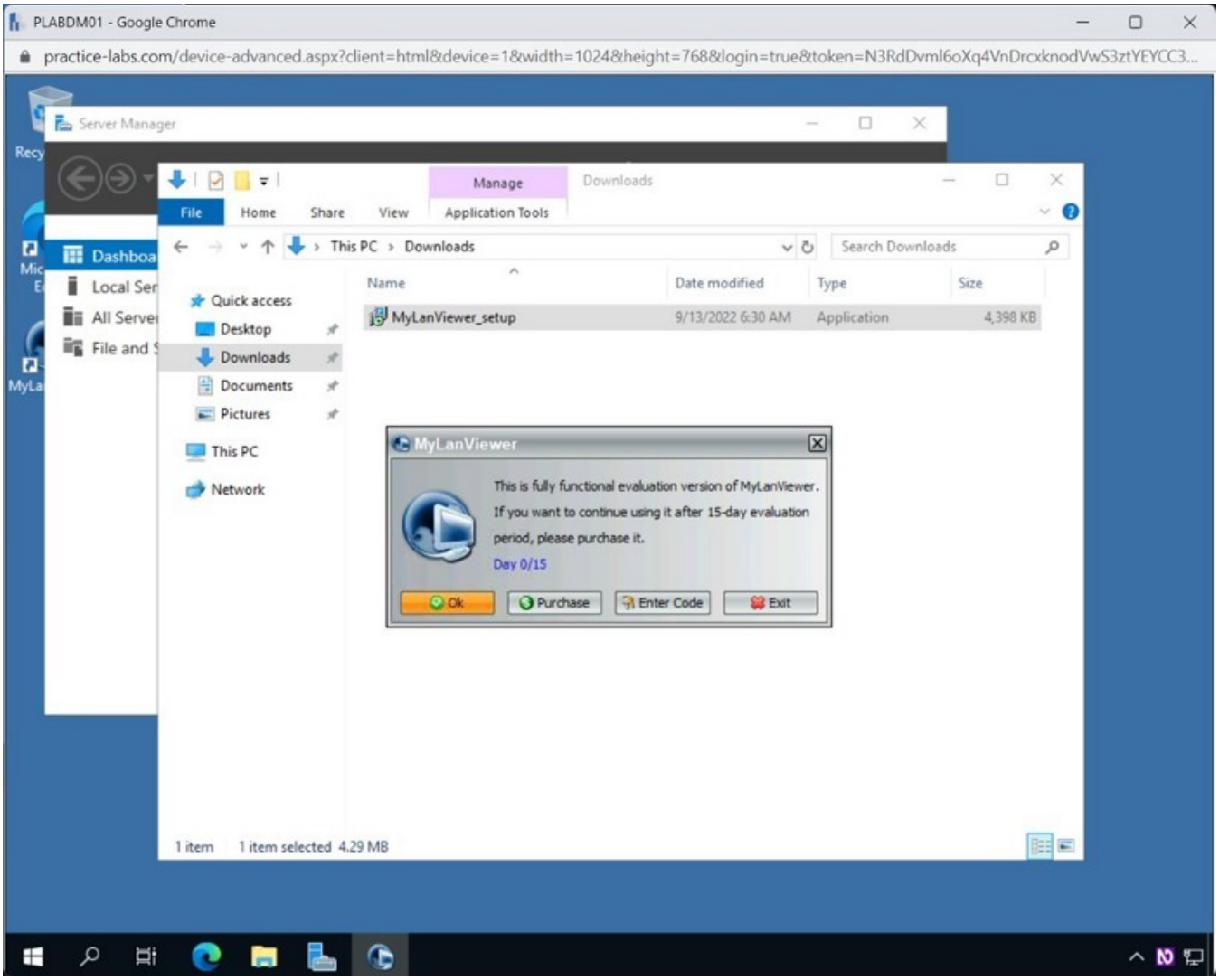

**Step 7**

Click **Finish** on the **Completing the MyLanViewr Setup Wizard** ensuring the **Launch MyLanViewr** tick-box is ticked.




**Step 8**

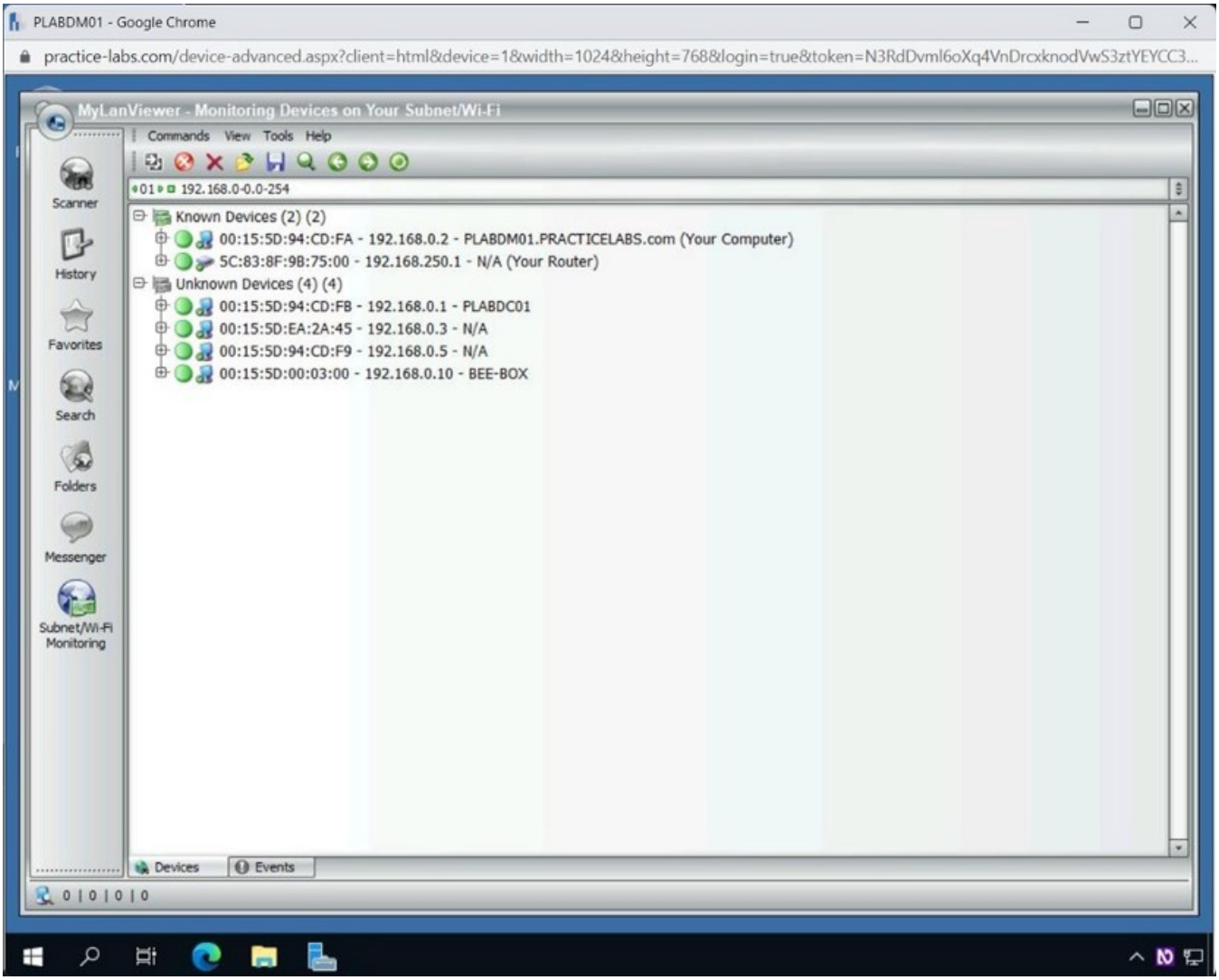
This trial version will work as a fully functional product for 15 days.
The **MyLANViewer** dialog box is displayed. Click **OK**.




**Step 9**

The **MyLANViewer — Monitoring Devices on Your Subnet/Wi-Fi** window is displayed.

**MyLANViewer** will now start to scan the subnet or Wi-Fi network, depending on your system's connectivity.

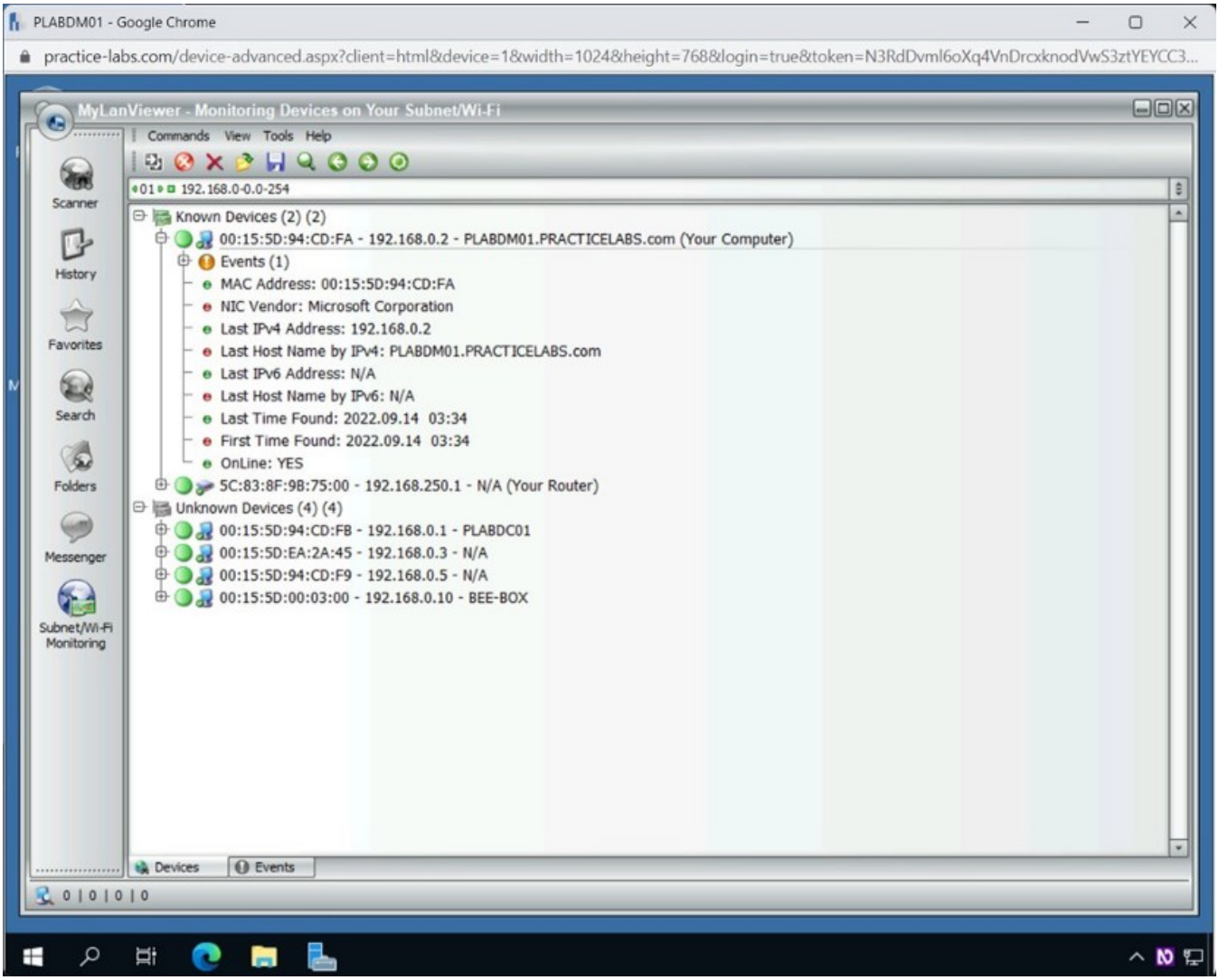



**Step 10**

After a few minutes, it can scan for the live systems on the subnet.
Expand **PLABDM01.PRACTICELABS.COM (Your Computer)**.

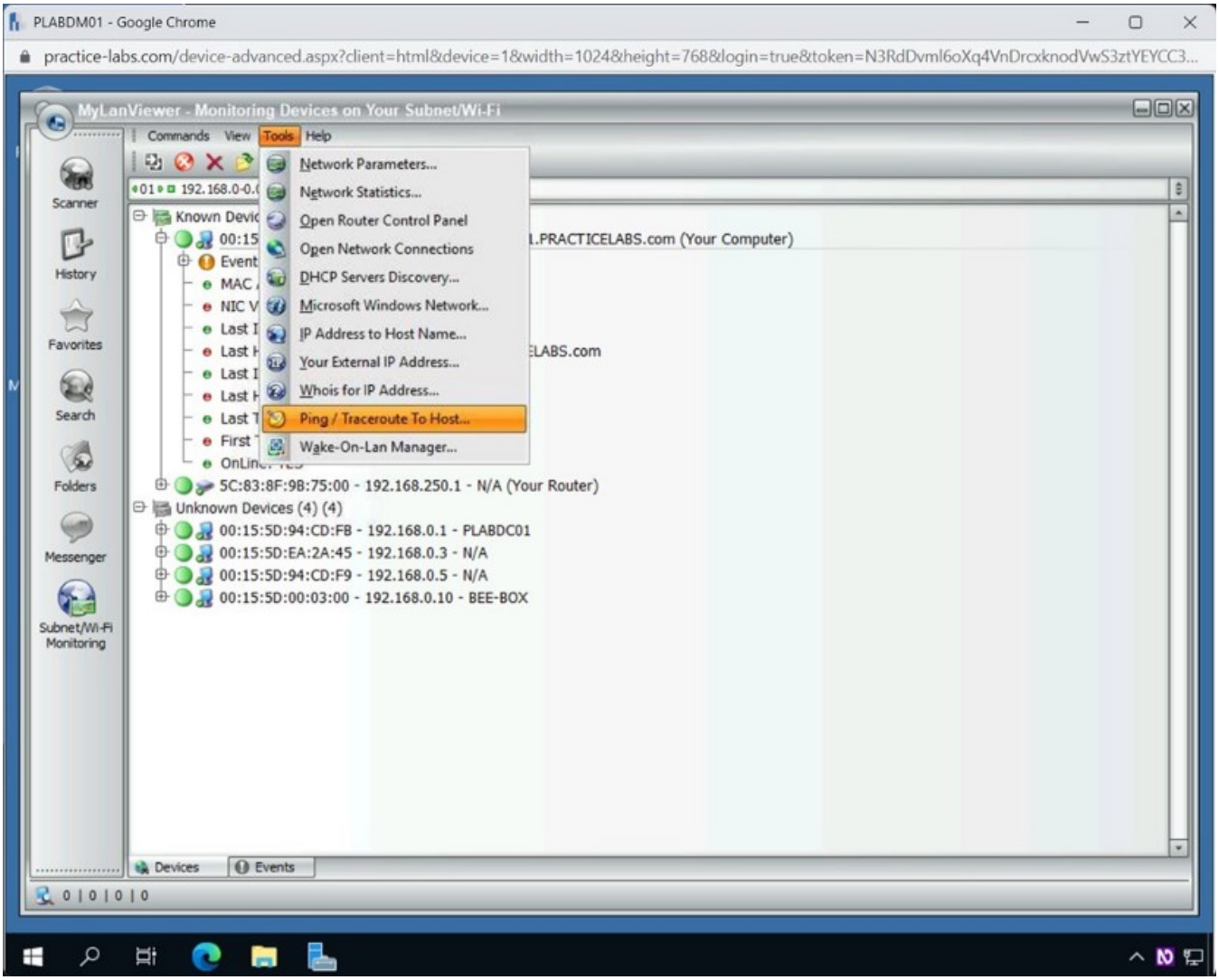
Notice that it has captured a lot of system-related information. For example, you can find its MAC address, IP address, and online status.

***Note**: The list of devices may be different to what is shown in the screenshots.*




**Step 11**

Click **Tools** and select **Ping / Traceroute To Host**.



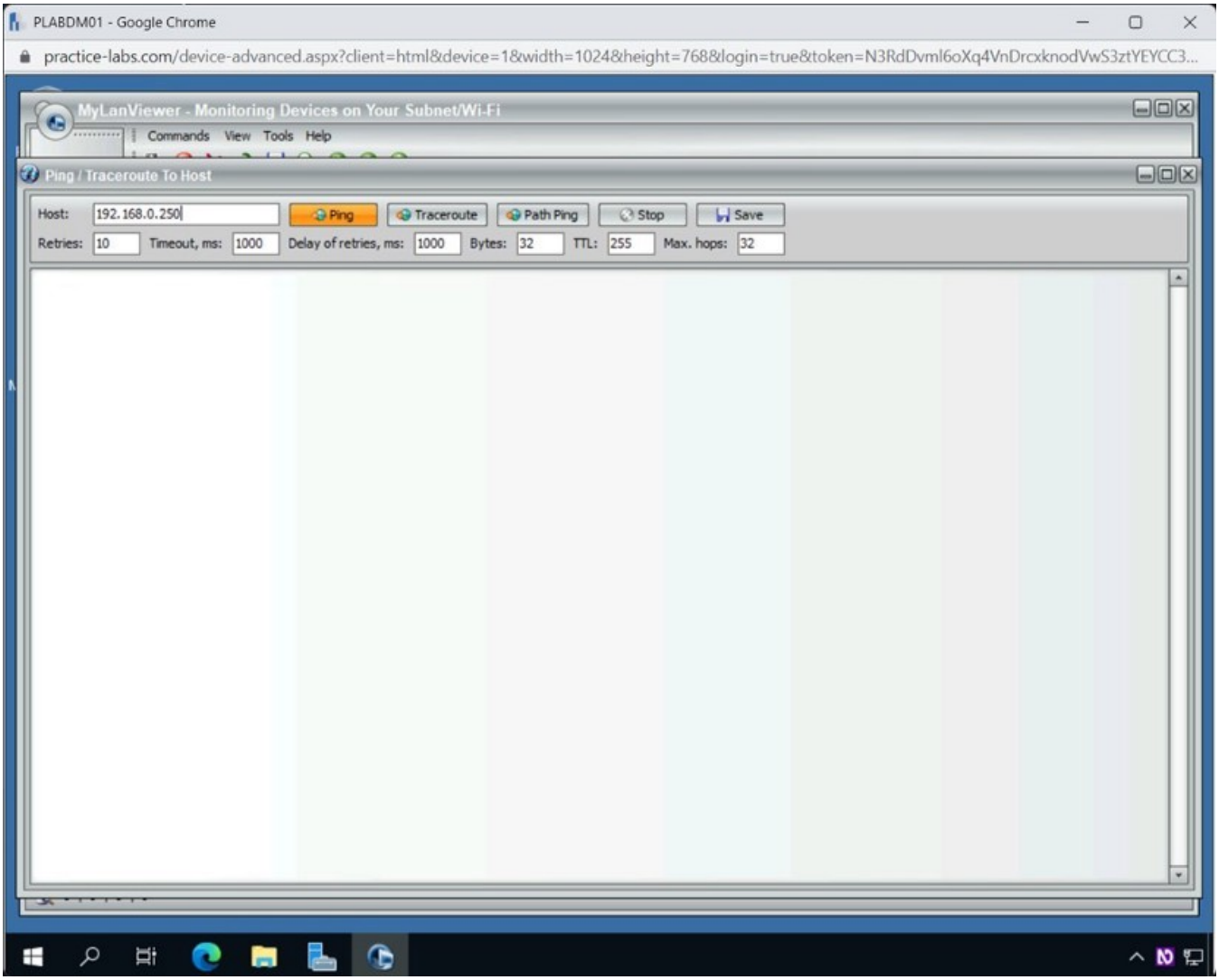

**Step 12**

The **Ping / Traceroute To Host** dialog box is displayed.

In the **Host** text box, type the following IP address:

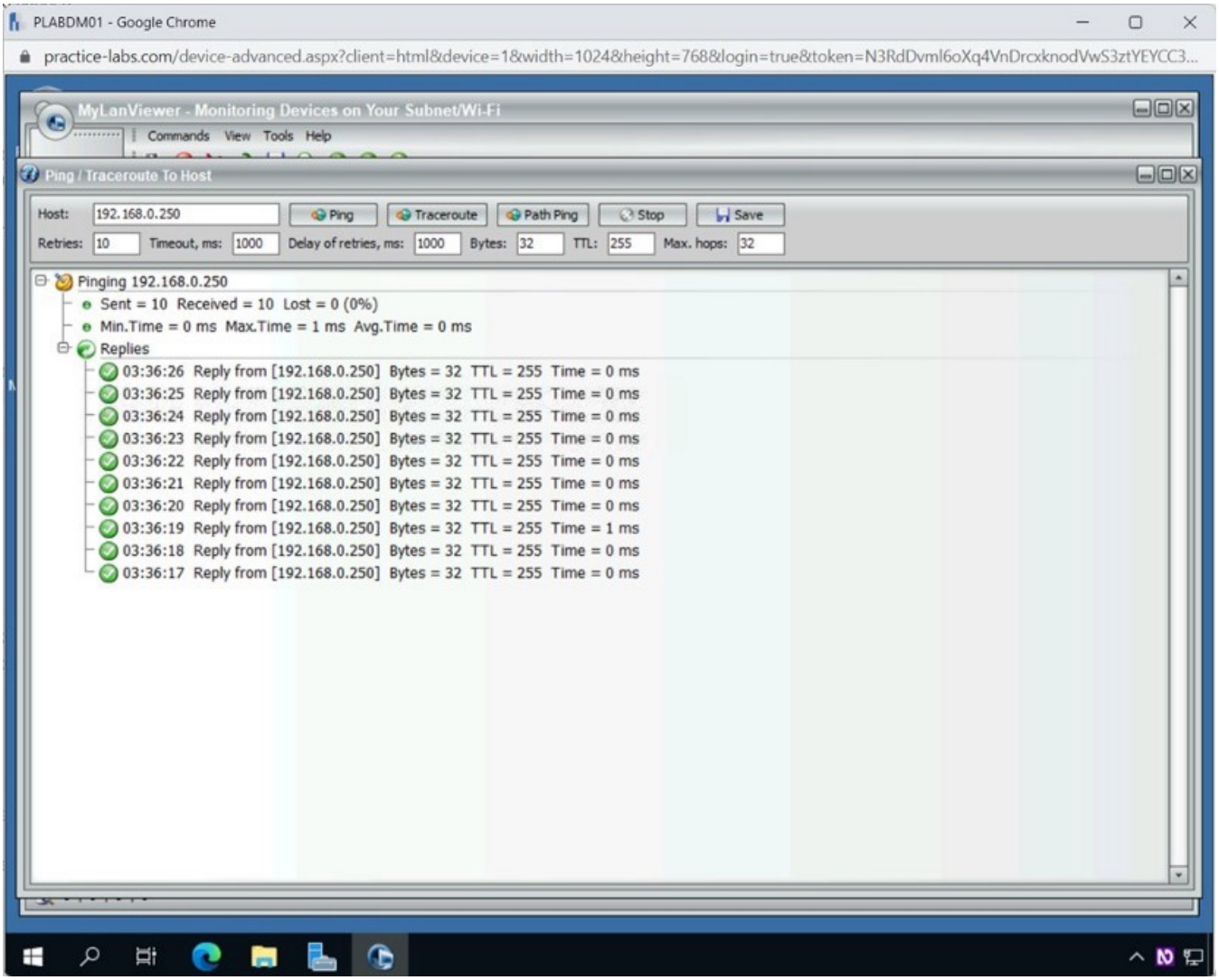
```
192.168.0.250
```

Click **Ping**.



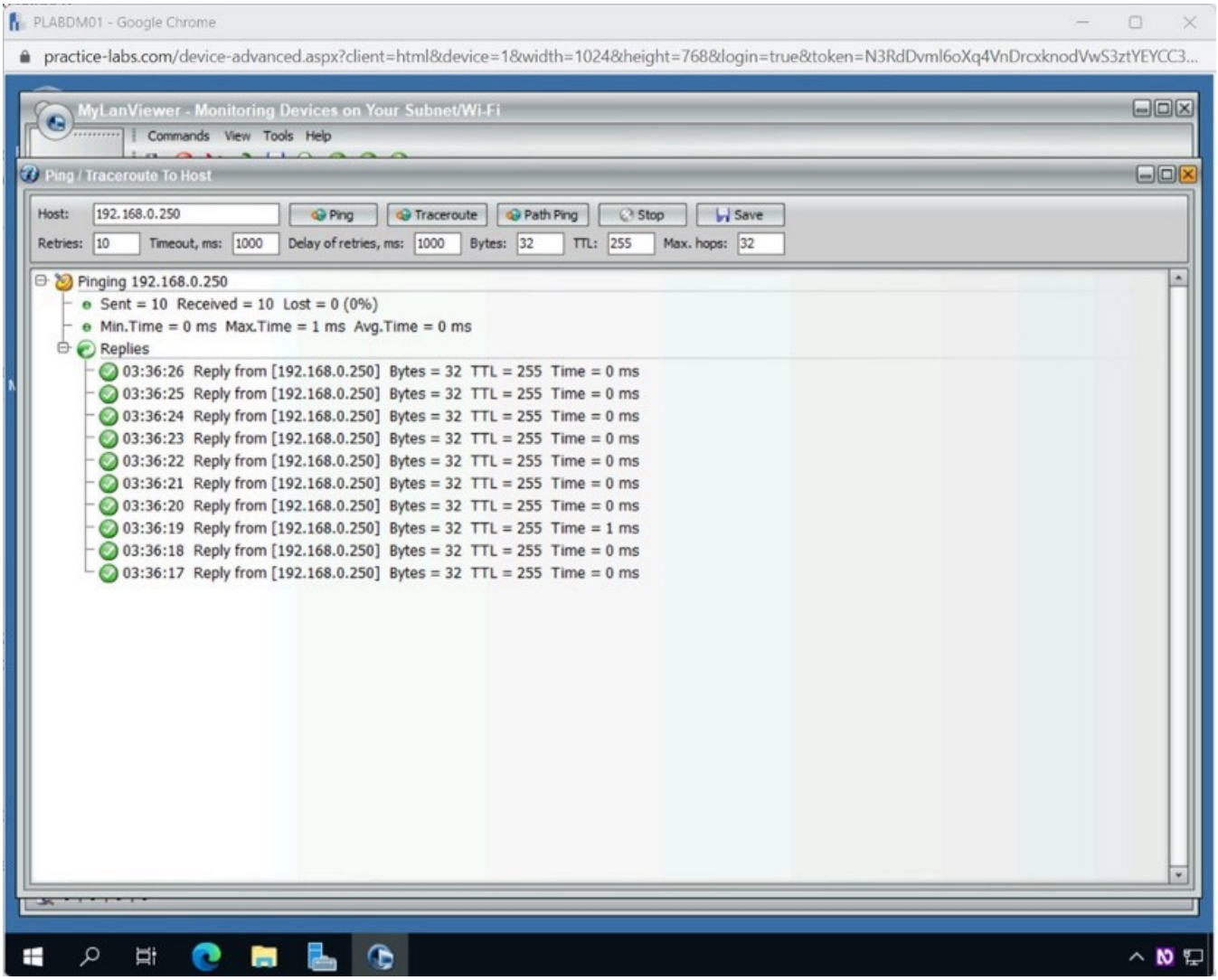

**Step 13**

Notice that the replies are received from the target, **192.168.0.250**.



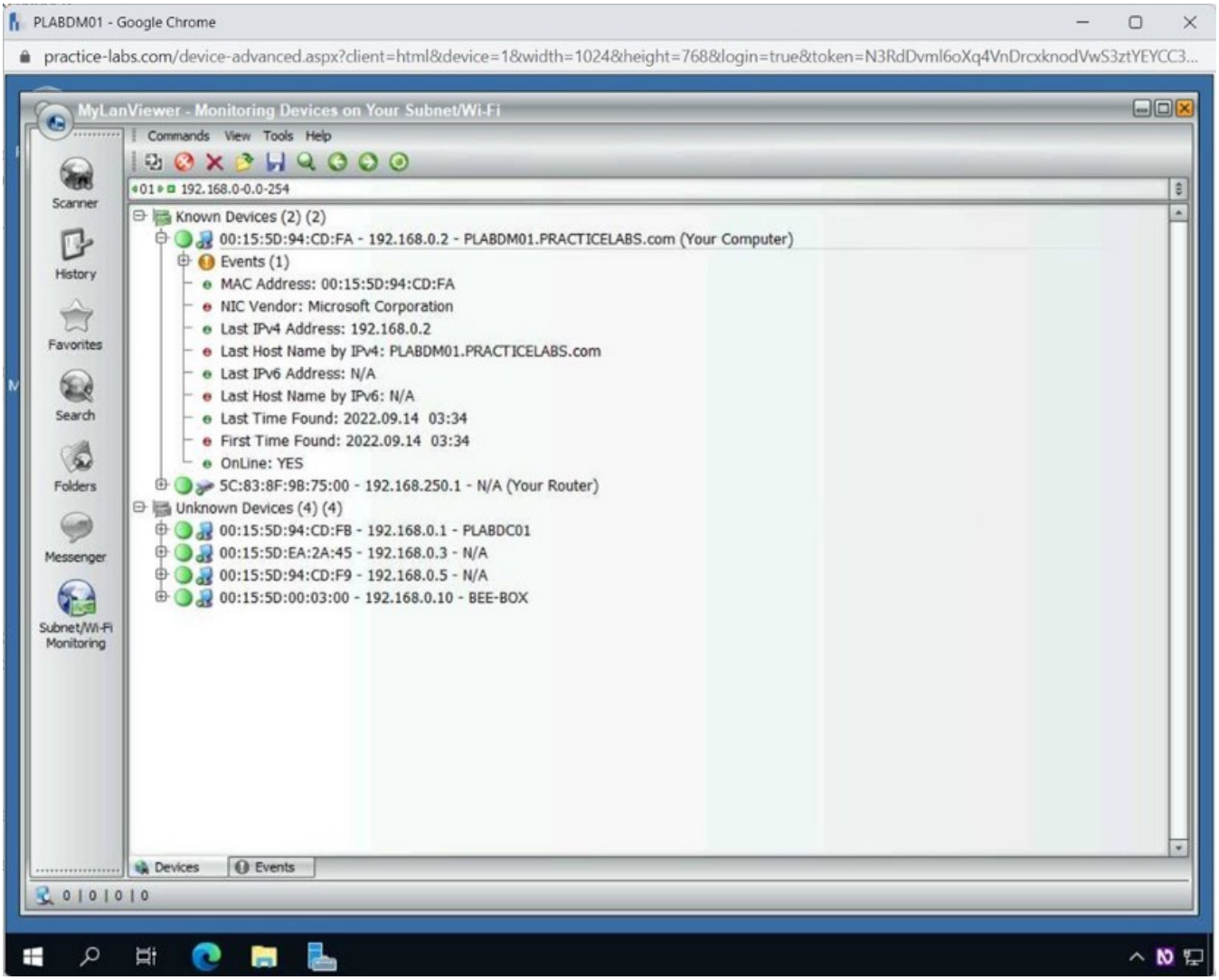

**Step 14**

Close the **Ping / Traceroute To Host** dialog box.




**Step 15**

Close the **MyLANViewer — Monitoring Devices on Your Subnet/Wi-Fi** window.




## Task 7 — Using Msfconsole to Perform TCP Stealth on a Network

Metasploit Framework is the most widely used tool in exploiting vulnerabilities. A free edition is available in Kali Linux. Metasploit has a modular and flexible architecture that helps you develop new exploits as more and more vulnerabilities are discovered. On the other hand, it is also used in penetration testing. Other than the modules for penetration testing, Metasploit Framework also contains modules that can be used for various types of scans, such as:

- UDP scan
- TCP Stealth scan
- Full connect scan

In this task, you will perform a TCP Stealth scan using Msfconsole. To do this, perform the following steps:

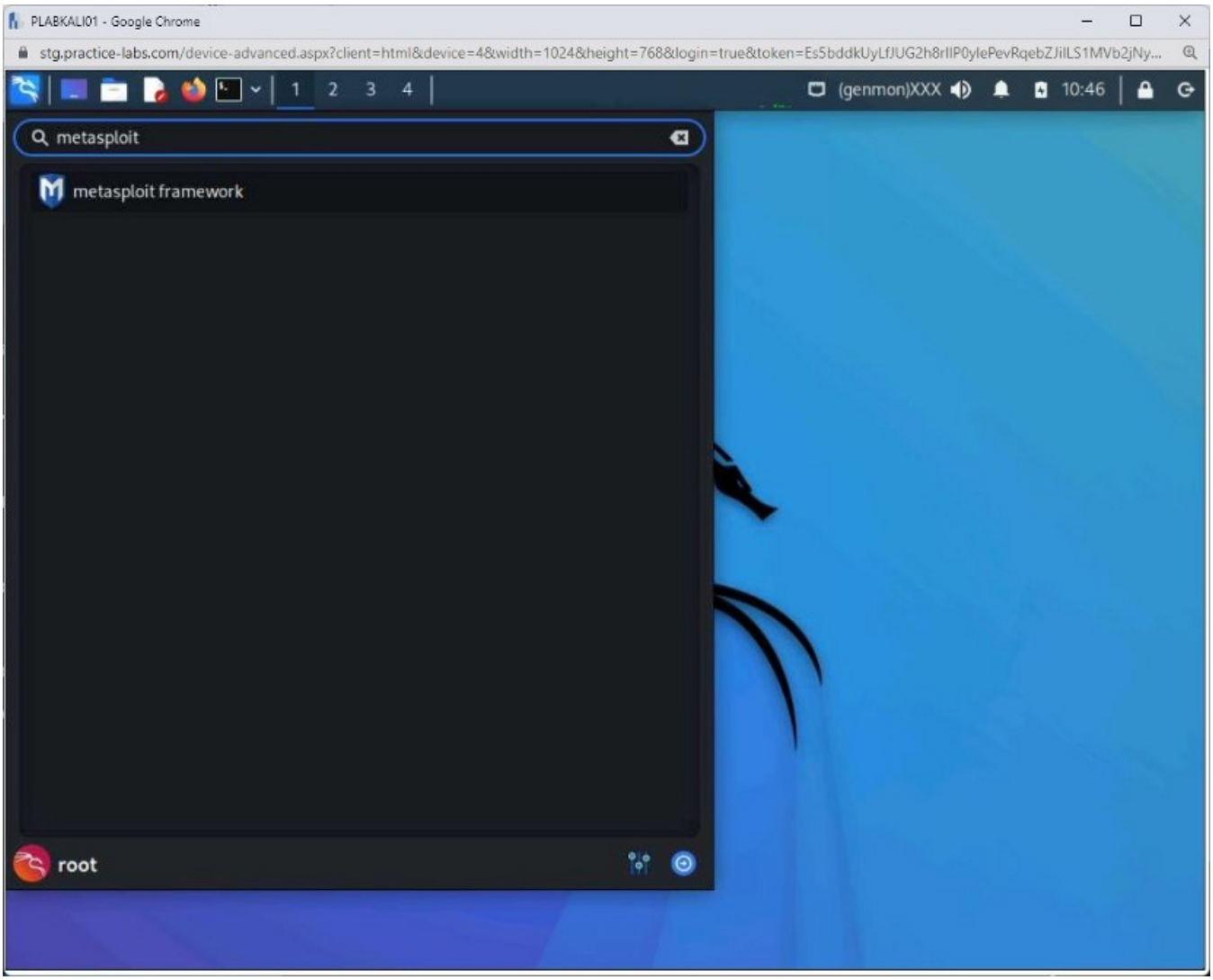
### Step 1

Connect to **PLABKALI01**.

Click the **Application** icon on the taskbar, and in the search field type the following:

```
metasploit
```

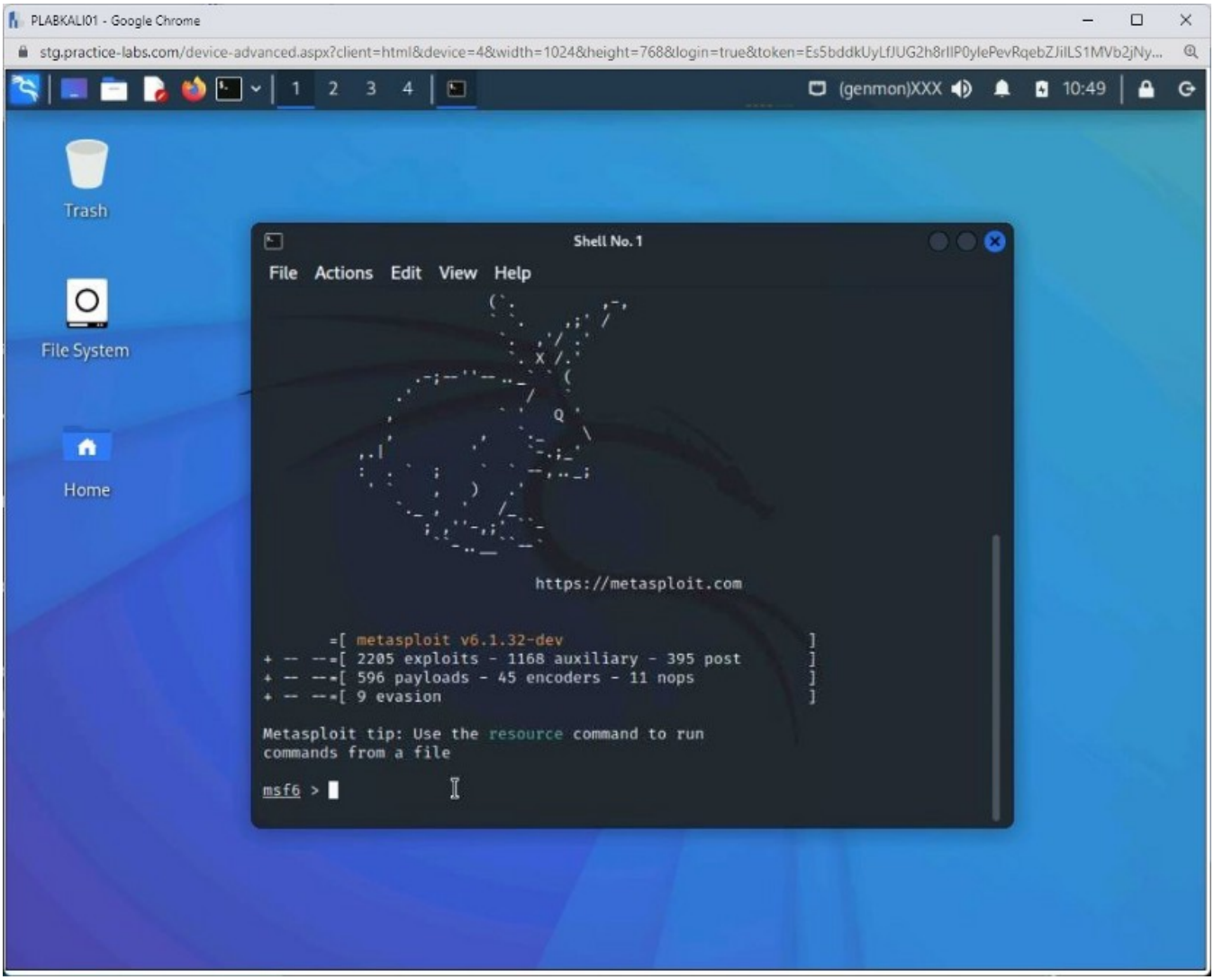
Click **Metasploit framework**.




### Step 2

After a few moments, a terminal window is displayed with a prompt once the Metasploit framework has loaded.

***Note:*** *The number of exploits and payloads will change from time to time.*

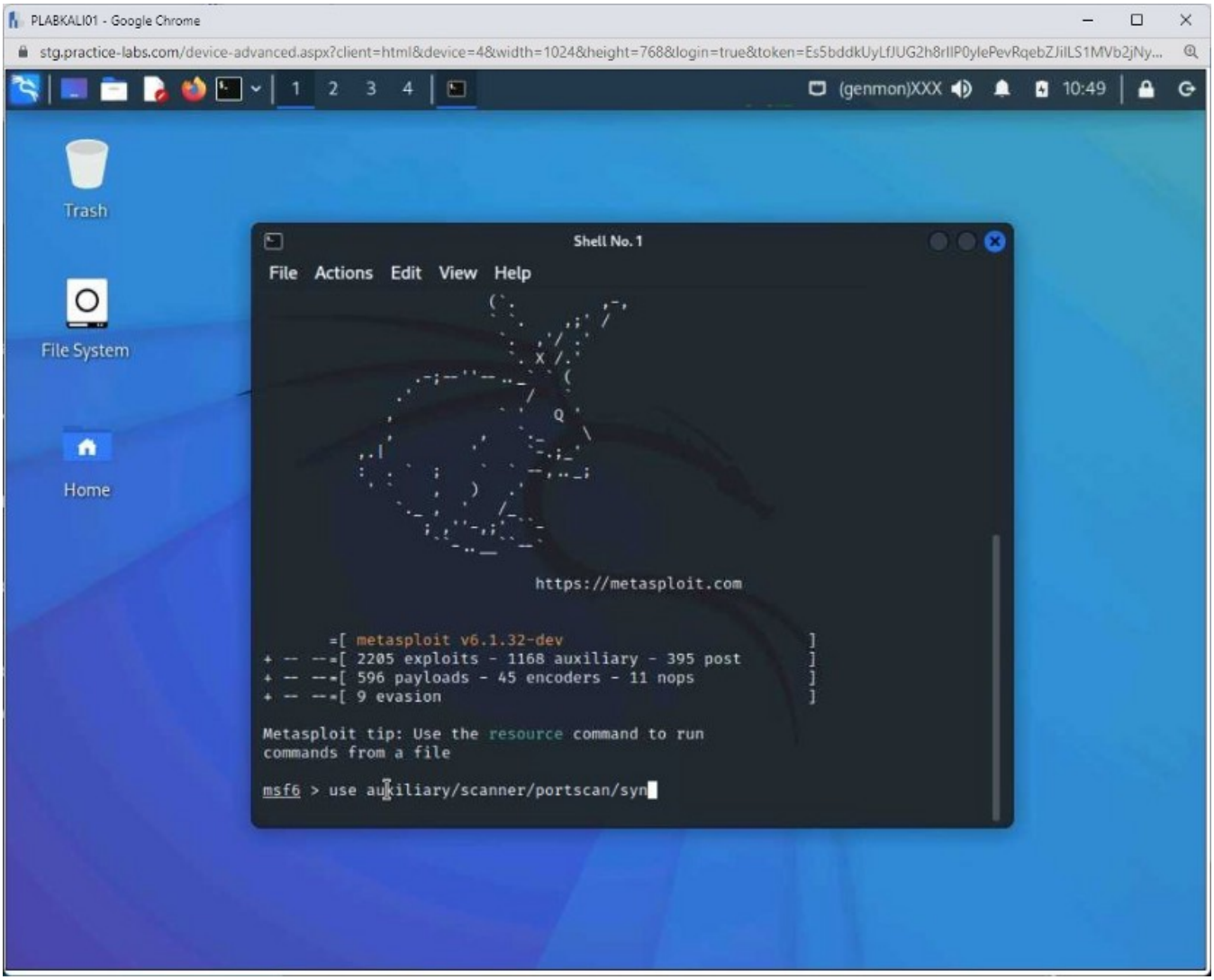



**Step 3**

Next, you will load the module with the **use** command. To do this, type the following command:

```
use auxiliary/scanner/portscan/syn
```

Press **Enter**.

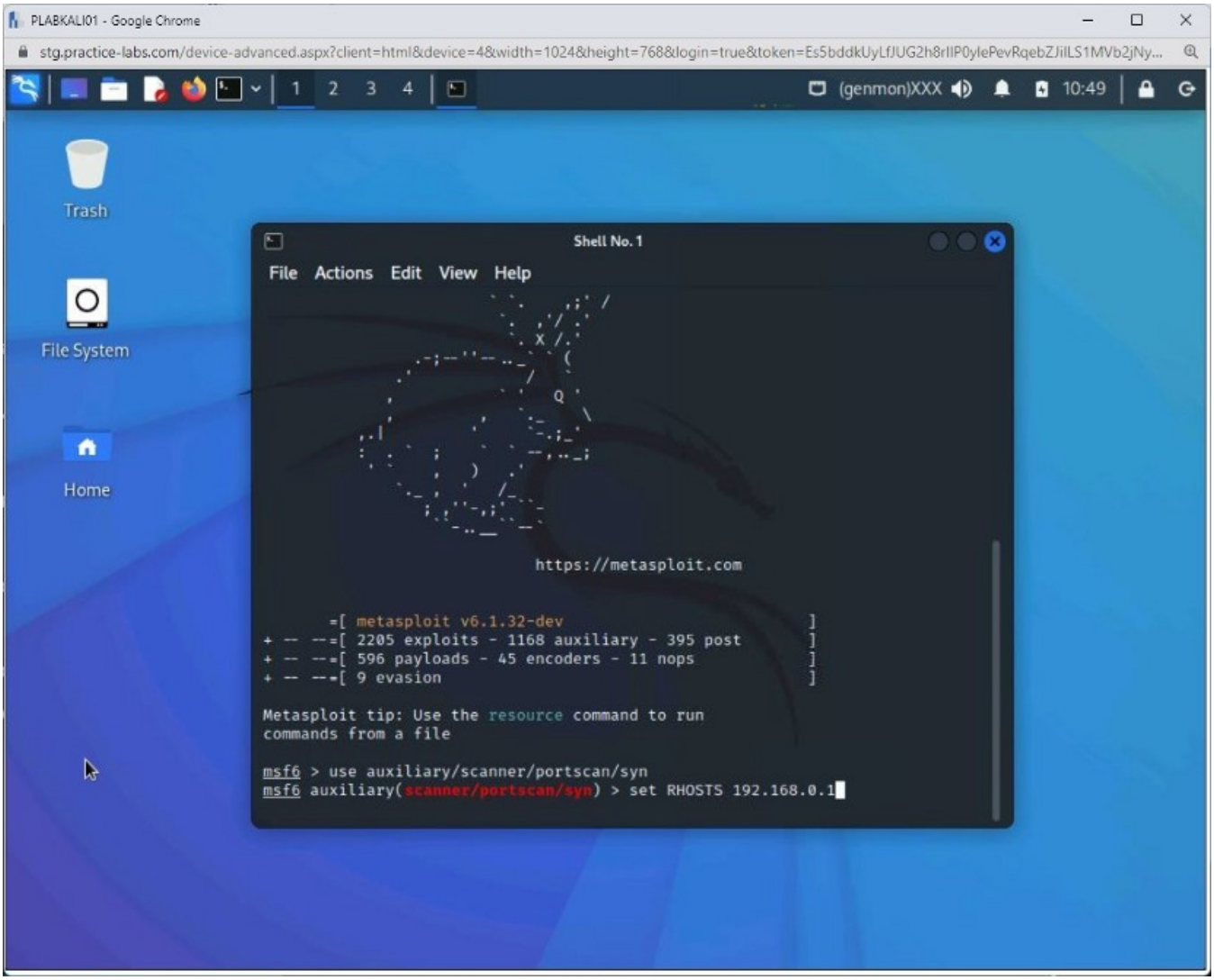



**Step 4**

You will now need to set the remote host on which you want to perform **the TCP stealth scan**. Type the following command:

```
set RHOSTS 192.168.0.1
```

Press **Enter**.

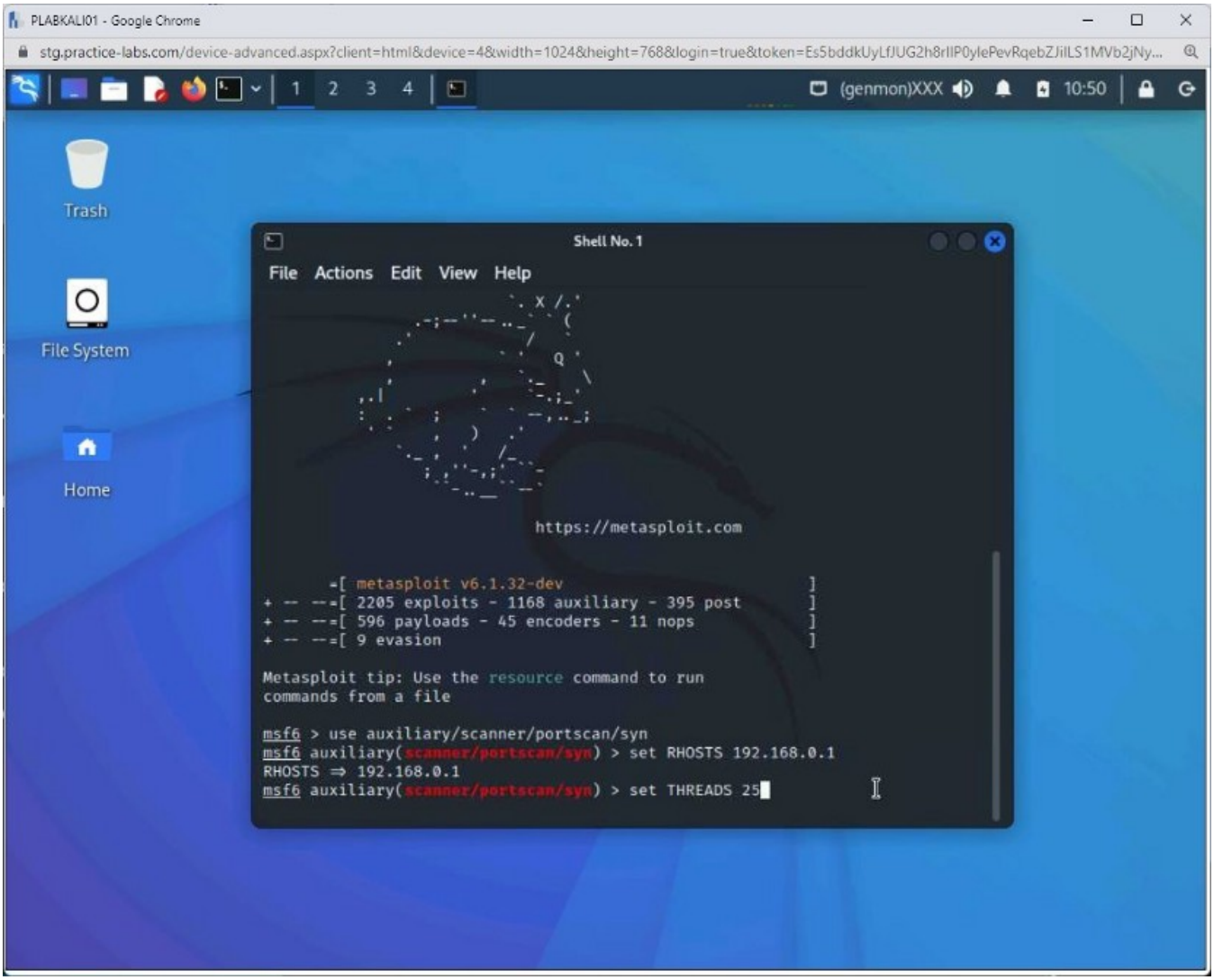



**Step 5**

Notice that the **RHOSTS** value is now set. You will now set the number of concurrent tasks to be performed in the background. This is done by setting the **THREADS** value. Type the following command:

```
set THREADS 25
```

Press **Enter**.

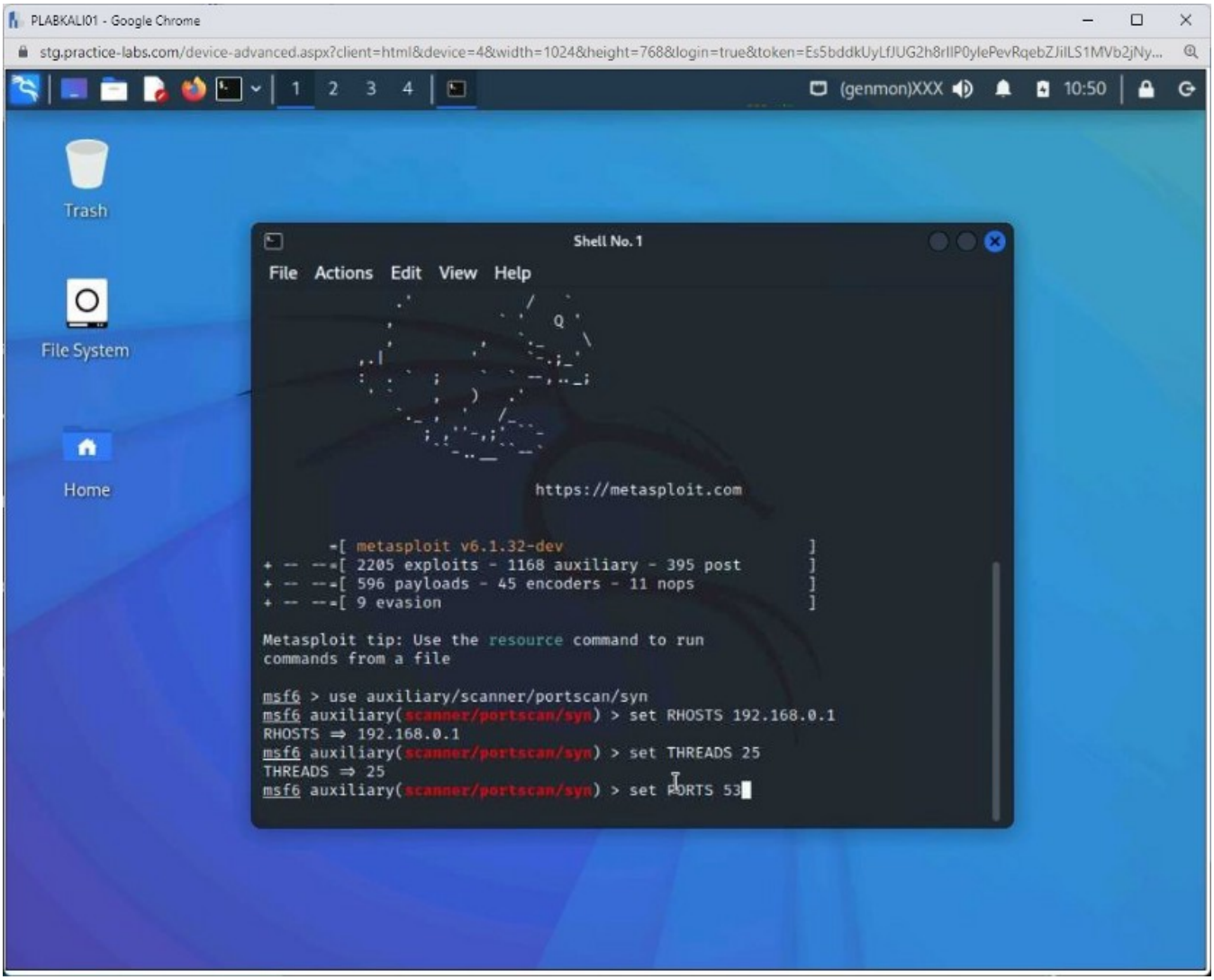



**Step 6**

Notice that the **THREADS** value is now set. You will need to set the port. This is done by setting the **PORTS** value. Type the following command:

```
set PORTS 53
```

Press **Enter**.

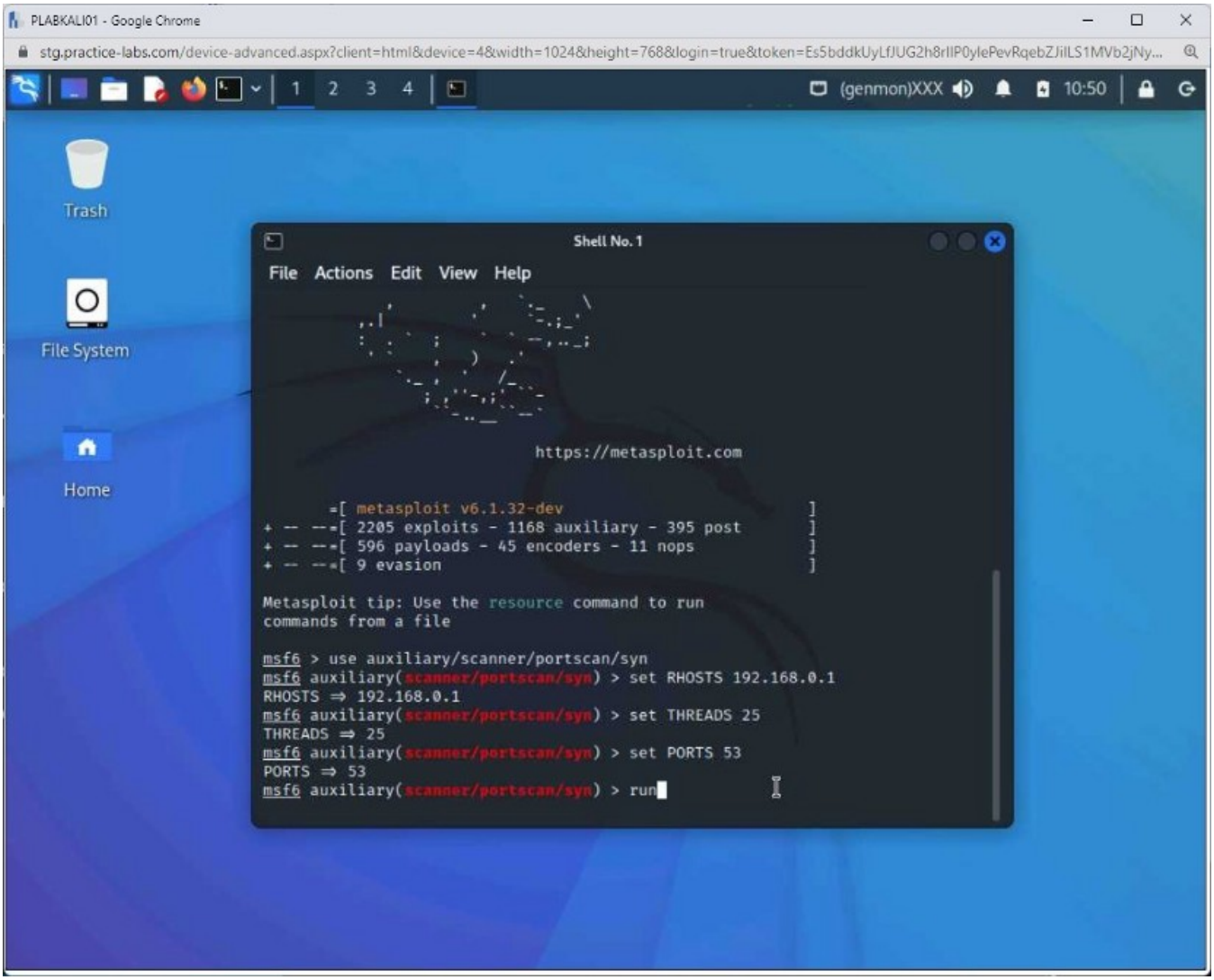



### Step 7

Notice that the **PORTS** value is now set. You can now execute the module. To do this, type the following command:

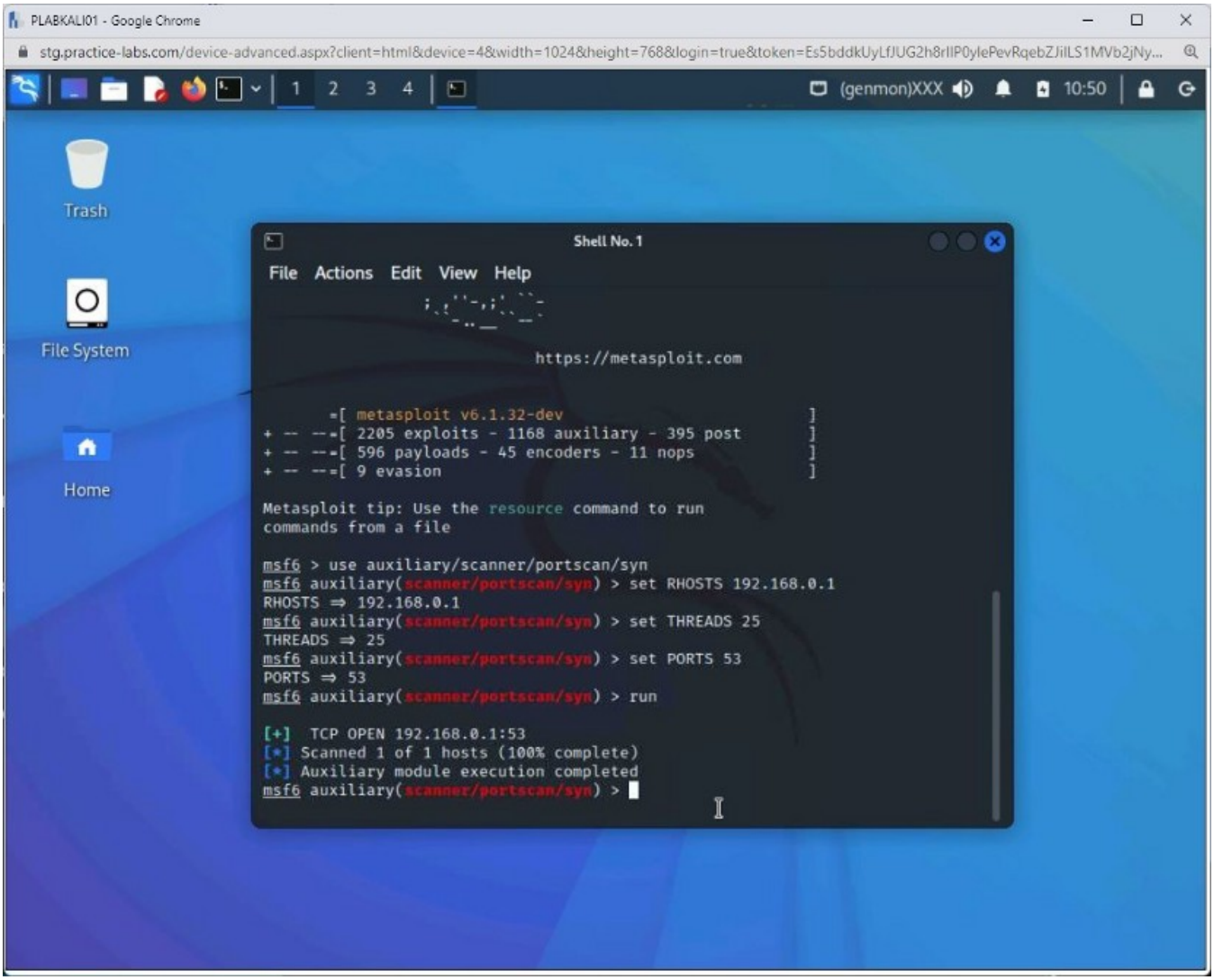
```
run
```

Press **Enter**.




### Step 8

Notice the output. It has found **port 53** to be open.



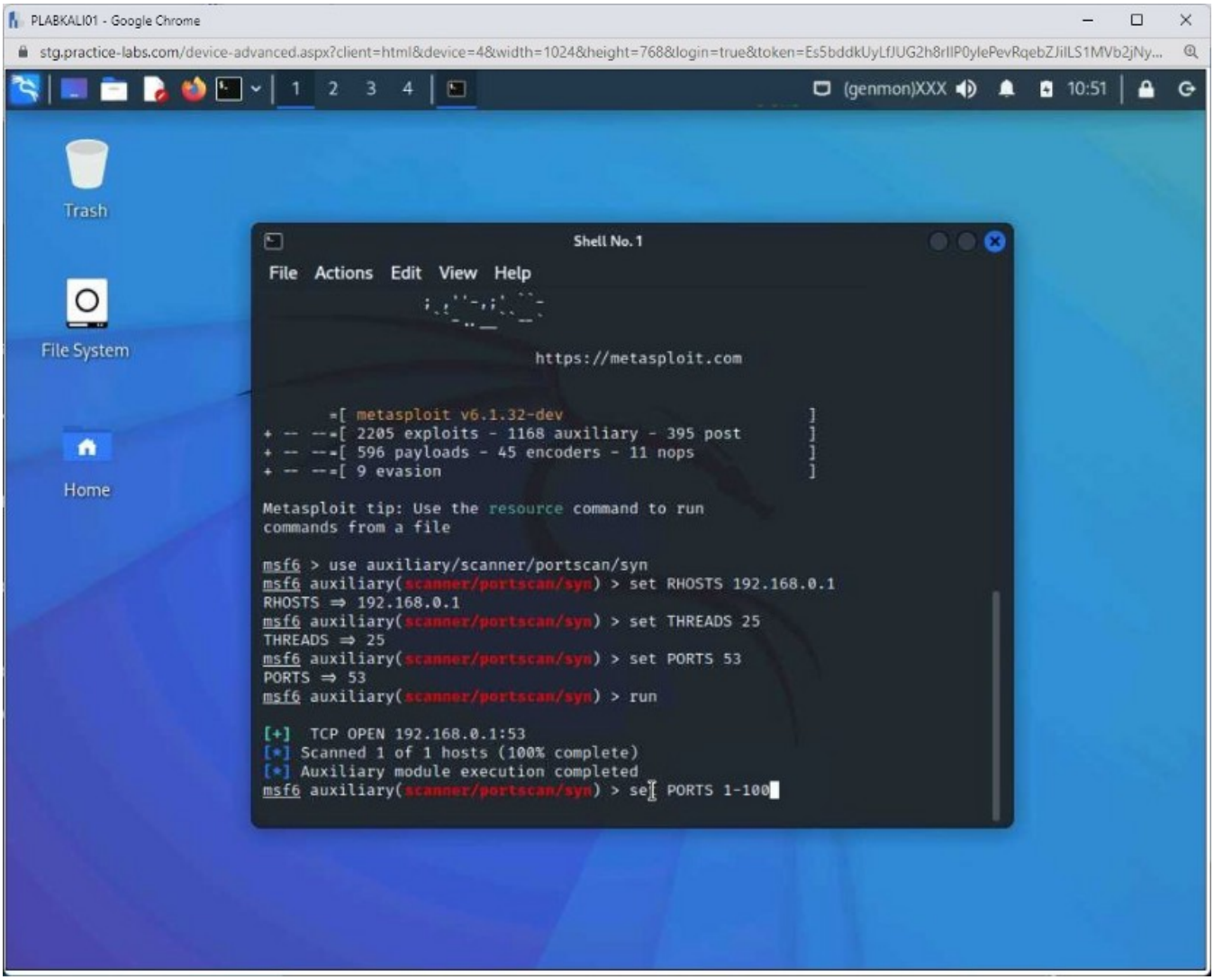

**Step 9**

Let's now scan against a range of ports. To do this, you need to reset the **PORTS** value. Type the following command:

```
set PORTS 1-100
```

Press **Enter**.

Notice that the value of **PORTS** has been reset to **1–100**. This means ports **1** to **100** will be scanned.



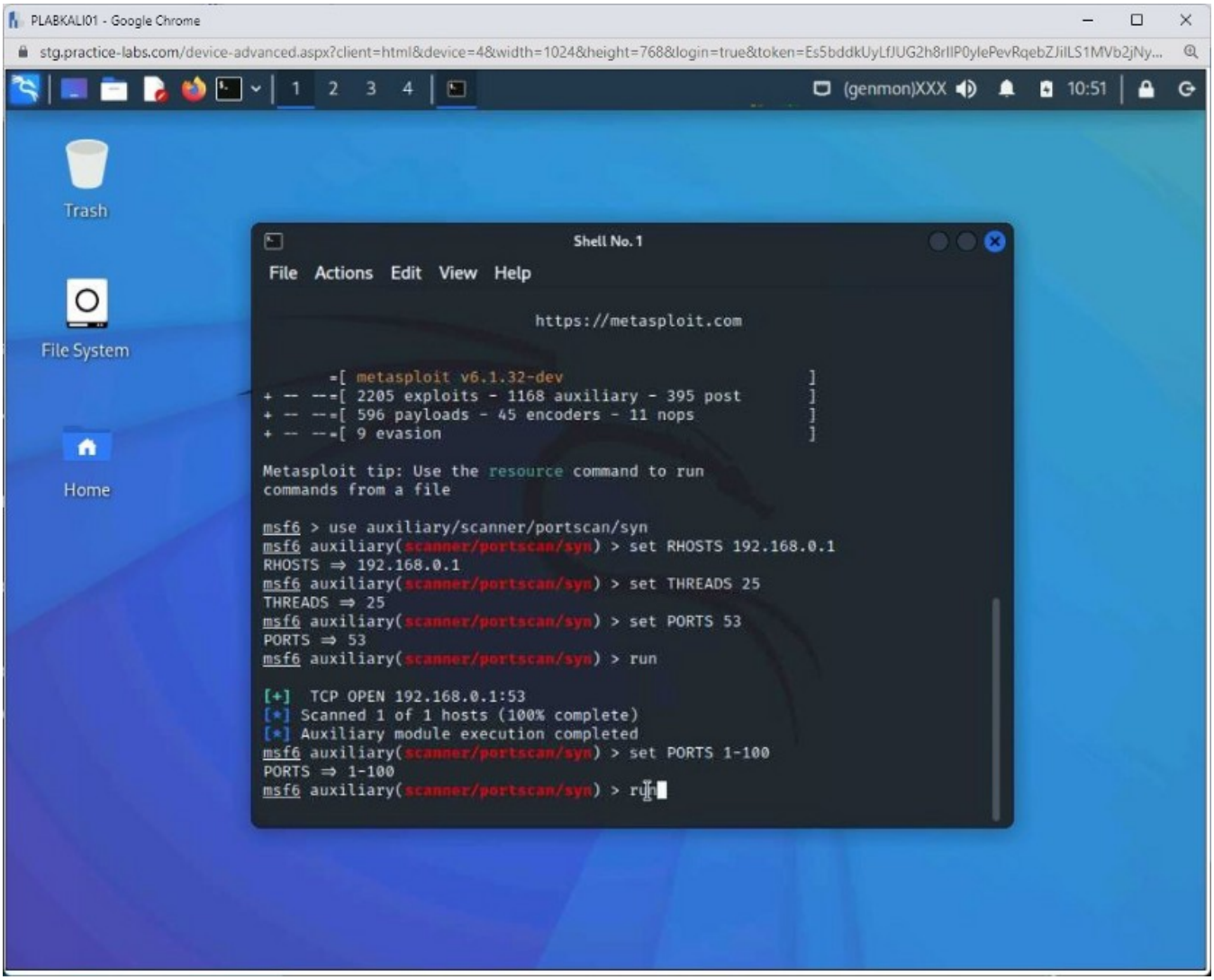

**Step 10**

You can now execute the module. To do this, type the following command:

```
run
```

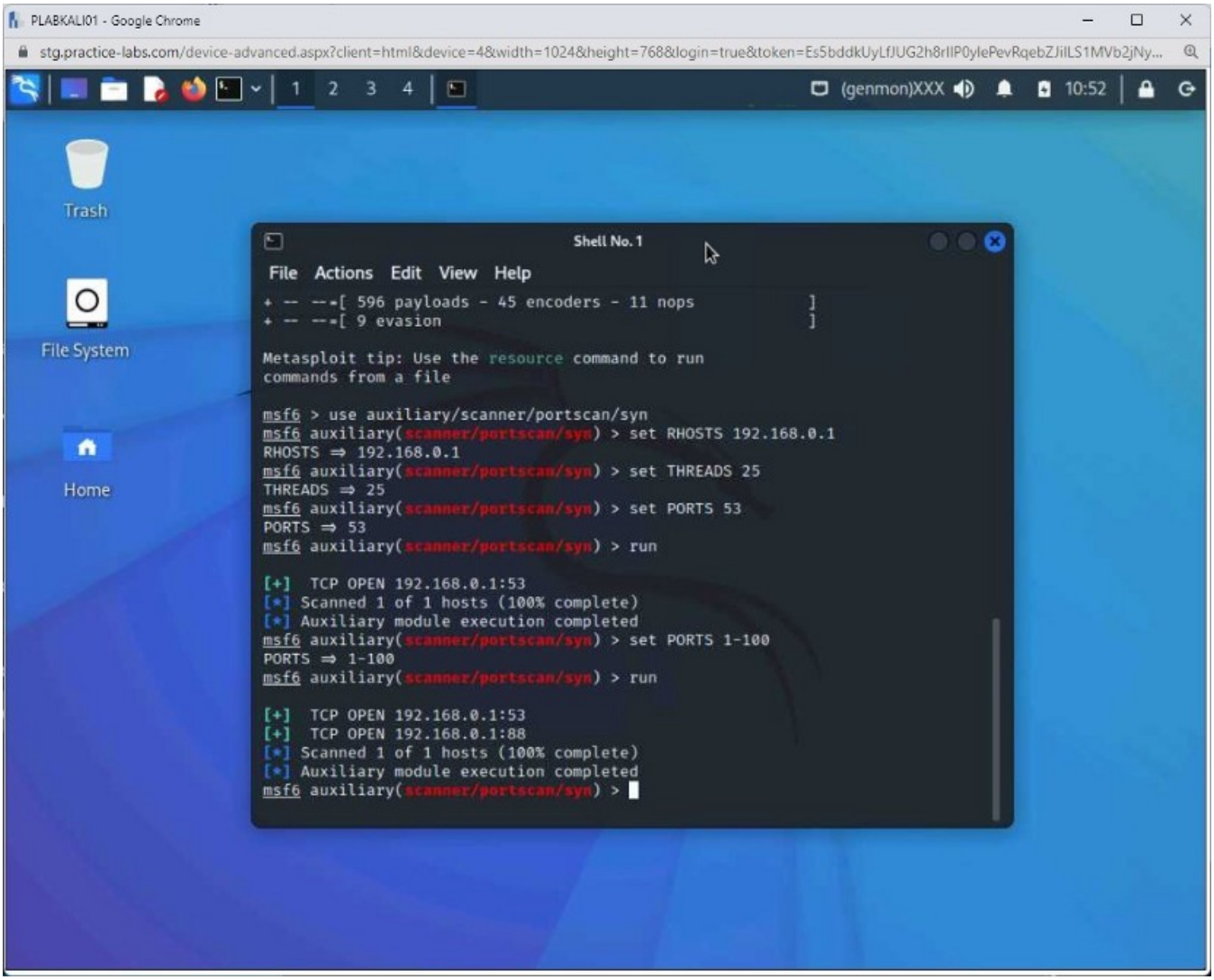
Press **Enter**.

***Note:*** *Because you are scanning for 100 ports, the scanner takes a few minutes to provide the results.*




### Step 11

Notice that in the range of **1** to **100**, two ports, **53** and **88**, are found open.

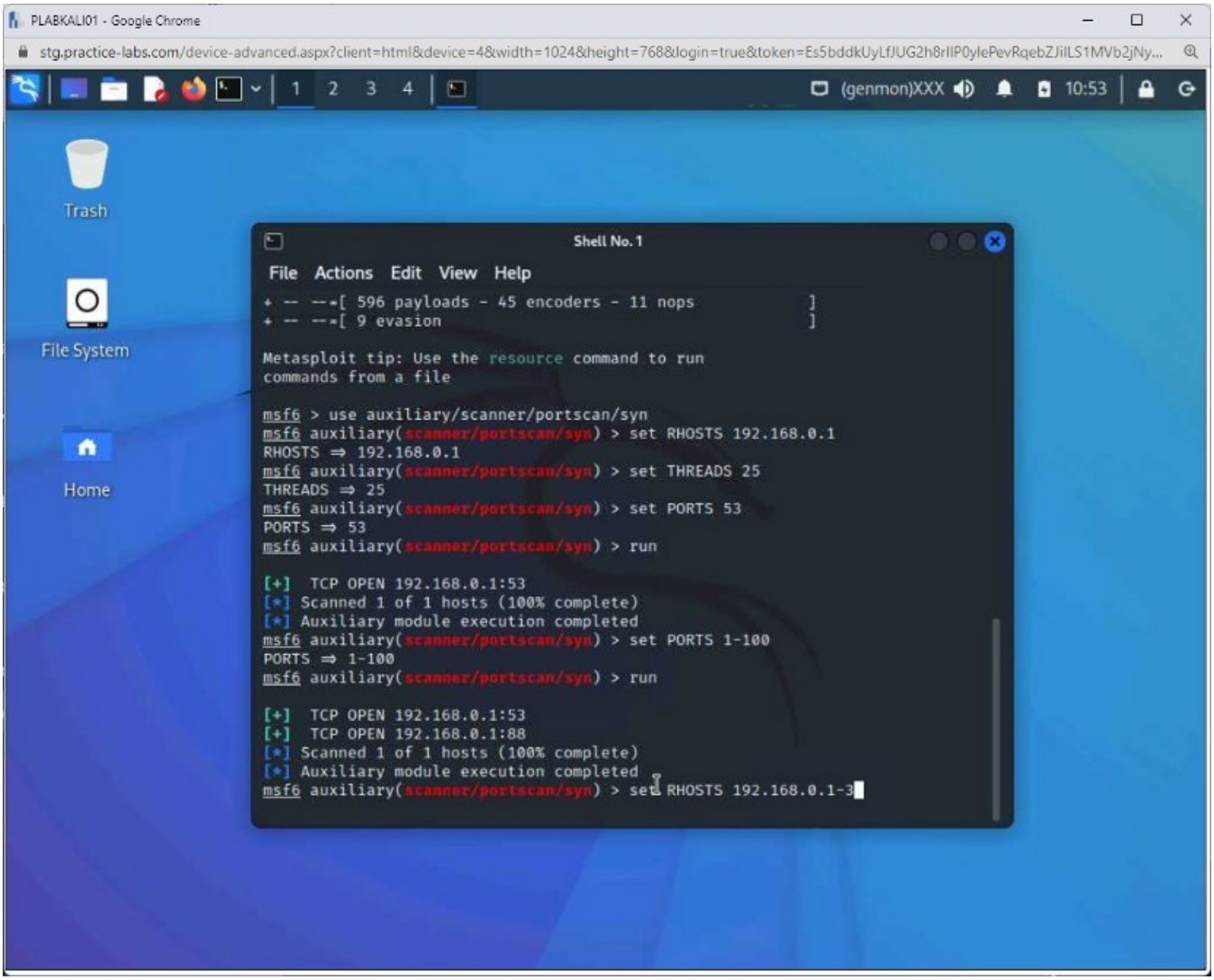



**Step 12**

You have performed a **TCP stealth scan** against a single host. You can reset the **RHOSTS** value to perform this scan against multiple hosts in one go. To do this, type the following command:

```
set RHOSTS 192.168.0.1-3
```

Press **Enter**. Notice that the value of **RHOSTS** has been reset to **192.168.0.1–3**.



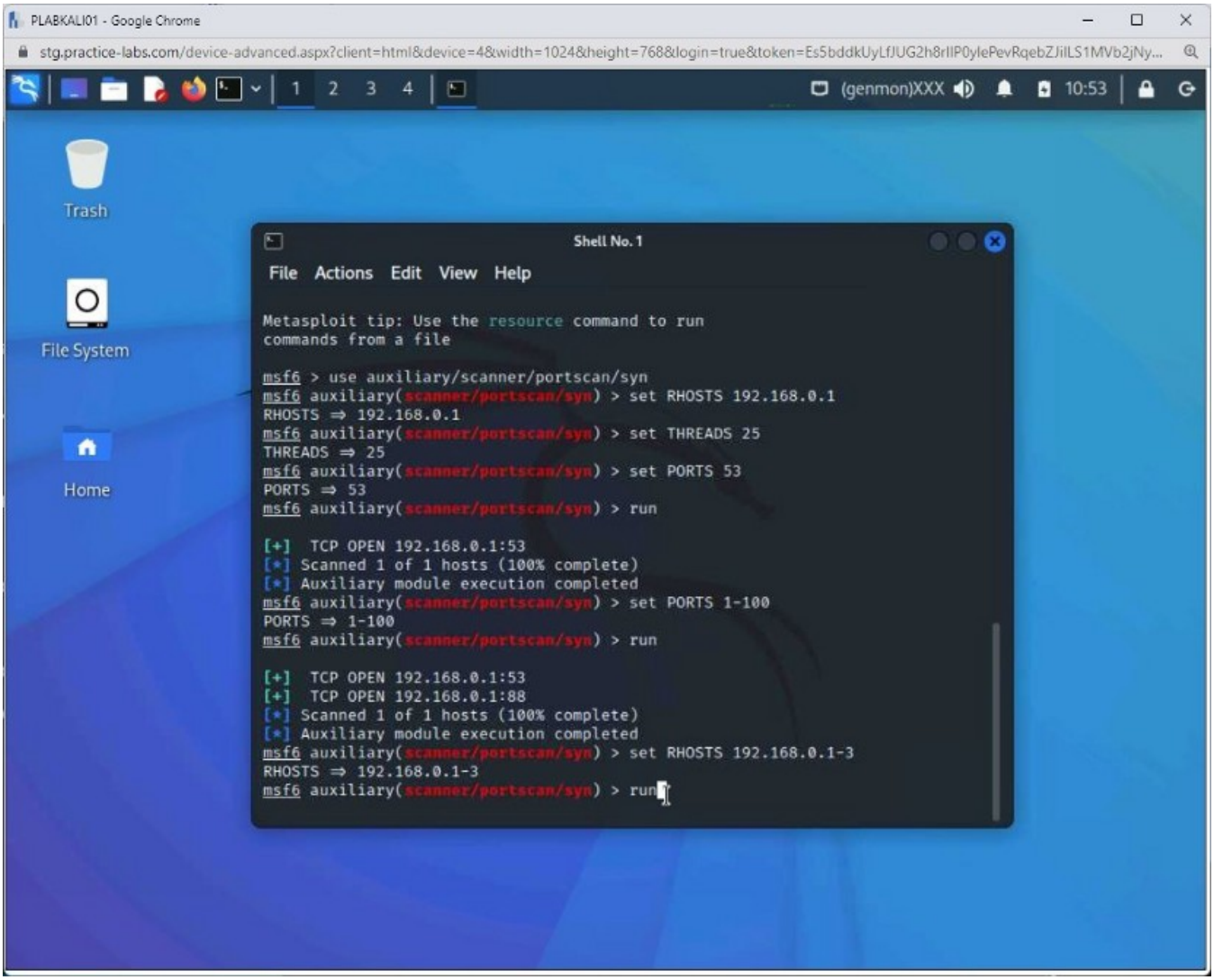

**Step 13**

You can now execute the module. To do this, type the following command:

```
run
```

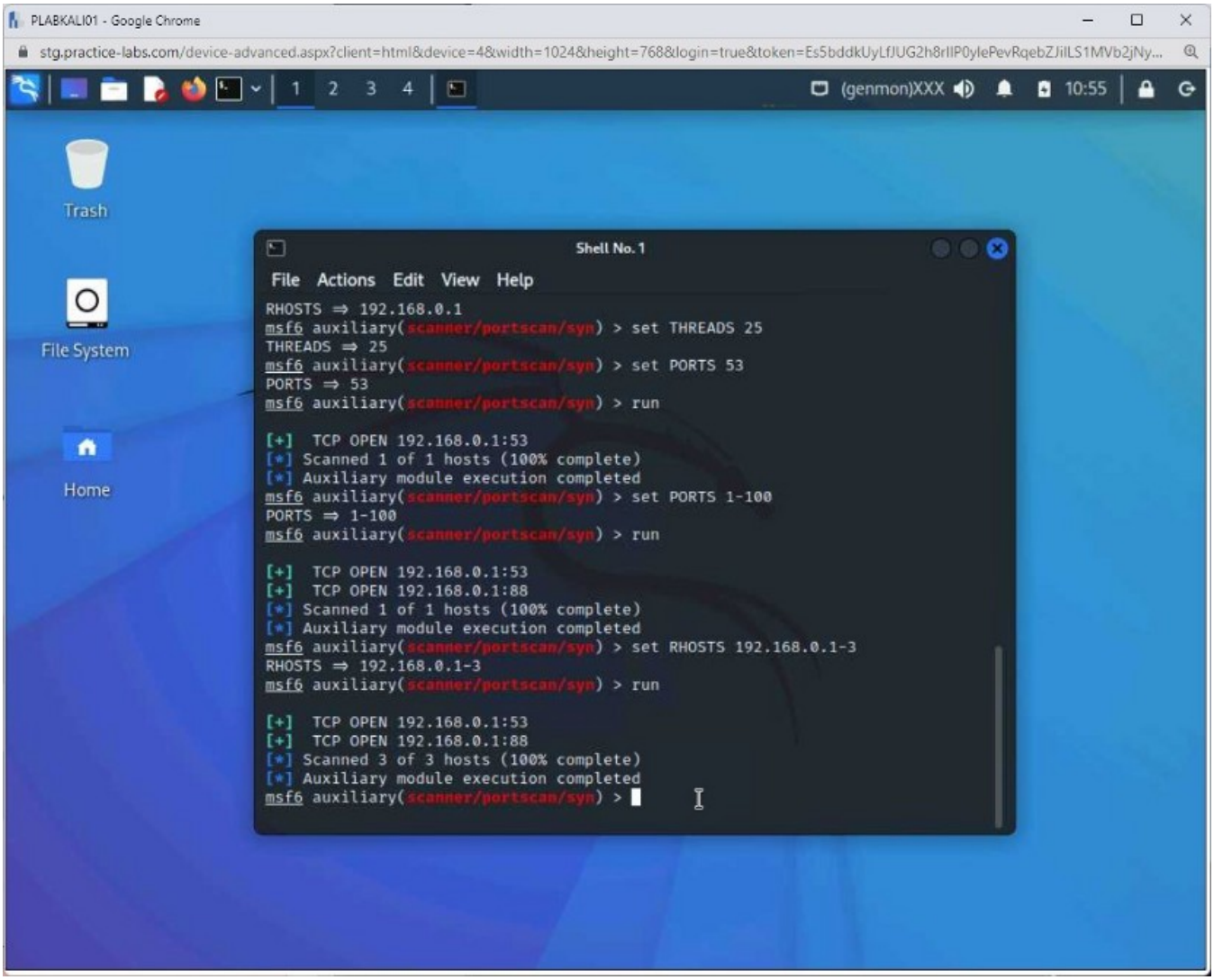
Press **Enter**.

***Note**: This command may take a few minutes to fully execute.*




### Step 14

Notice the output. Port **53** and **88** are open on **192.168.0.1**.




## Exercise 2 — Host Discovery

The amount of systems connected to a network can be vastly different, from only a few to a few thousand depending on how the network is utilized. For an attacker, it is necessary to discover live systems on a network, which can be determined via host discovery.

When an attacker performs host discovery, they can determine the correct status of connected systems.

In this exercise, you will learn to perform host discovery.

## Learning Outcomes

After completing this exercise, you will be able to:

- Identify Live Hosts on a Network
- Perform Discovery Scans

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

- Networking Tools

### 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 MemberWorkstation192.168.0.5/24PLABDM01Domain Member Server192.168.0.2/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABDM01

Windows Server 2019 — Domain Member192.168.0.2/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

### Task 1 — Identify Live Hosts on a Network

More commonly known as Nmap, Network Mapper is a network and host discovery tool. It is one of the most widely used tools for various activities, such as:

- discovering hosts, services, and ports
- fingerprinting operating system
- Enumeration
- Discovering vulnerabilities on the local and remote host
- Find the IP address of a remote system

Using Nmap, you can scan for targets in the following way:

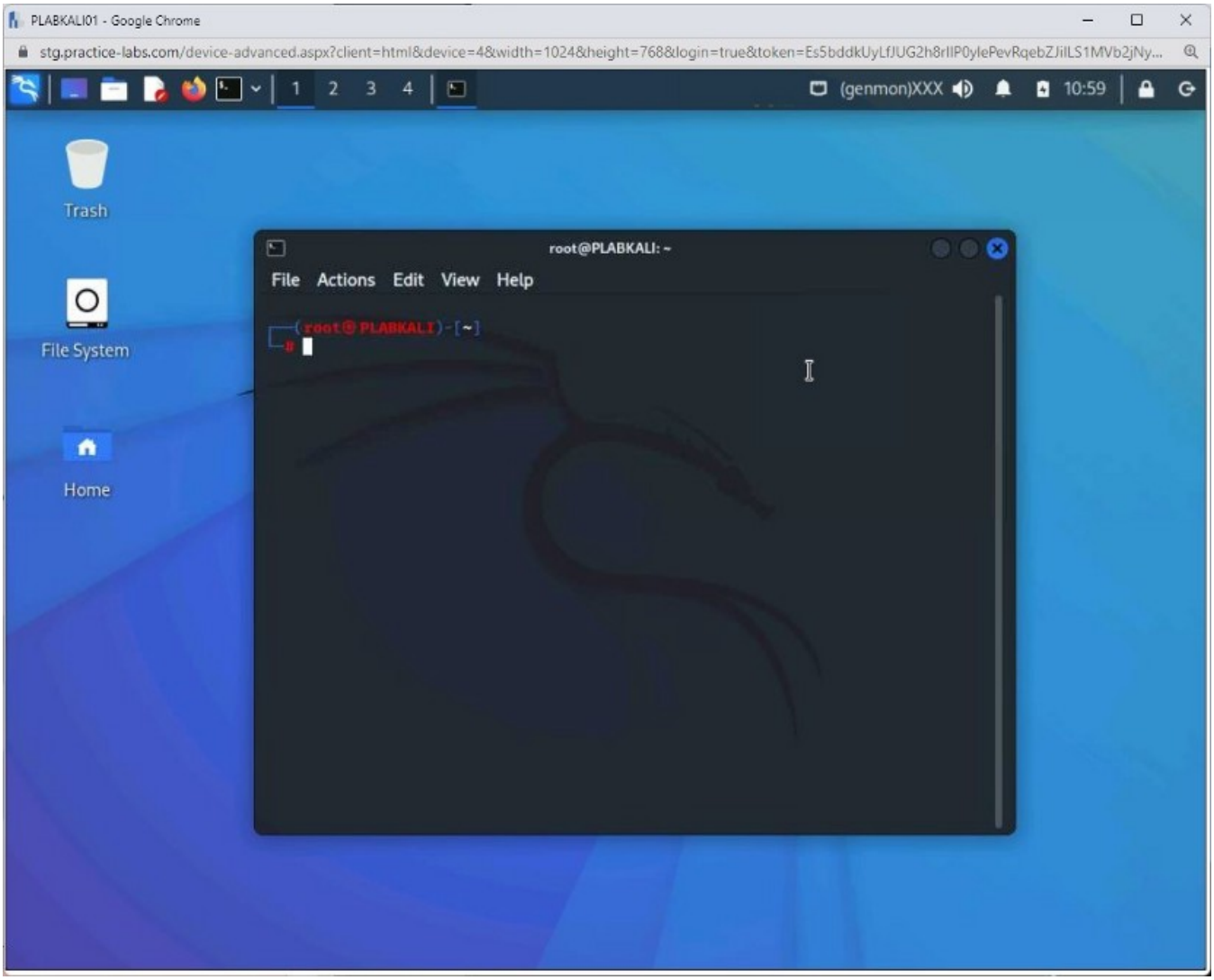
- Scan for a single IP: nmap 192.168.0.1

- Scan for a host by using its name: nmap host1.plab.com
- Scan an entire subnet: nmap plab.com/24, nmap 192.168.0.0/24, nmap 192.168.0.*
- Scan for a range of IP addresses: nmap 192.168.0.1–10
- Scan for a range and a system outside the range: nmap 192.168.0.1, 1.10

In this task, you will use Nmap to identify the live systems on a network. To do this, perform the following steps:

#### Step 1

Connect to **PLABKALI01** and open a new **Terminal** window.



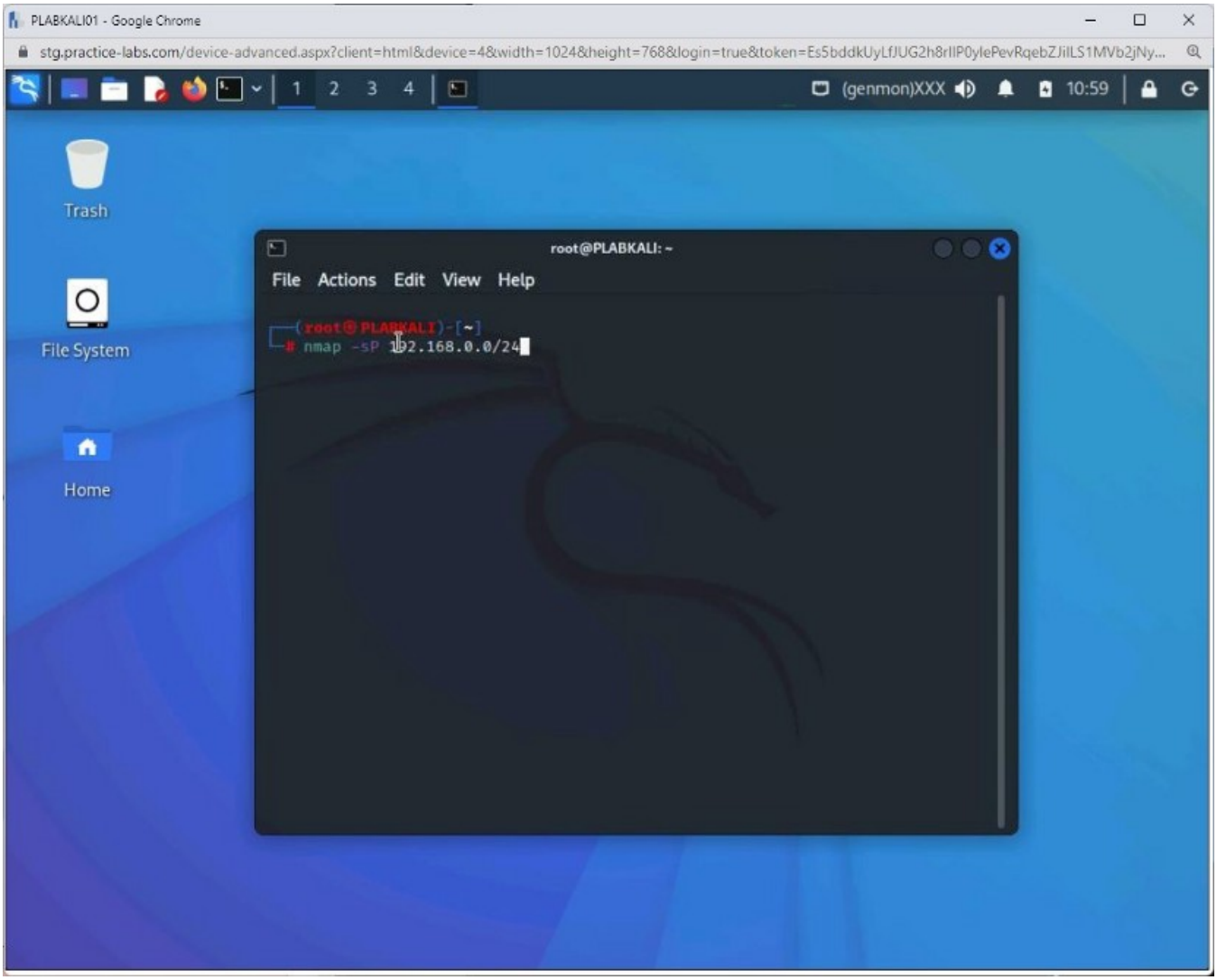

#### Step 2

You will now perform a ping scan to discover the live hosts in a network. Type the following command:

***Note:*** *the -sP parameter is used for ping scanning. When you use CIDR /24, Nmap will scan all 256 IP addresses on the network.*

```
nmap -sP 192.168.0.0/24
```

Press **Enter**.

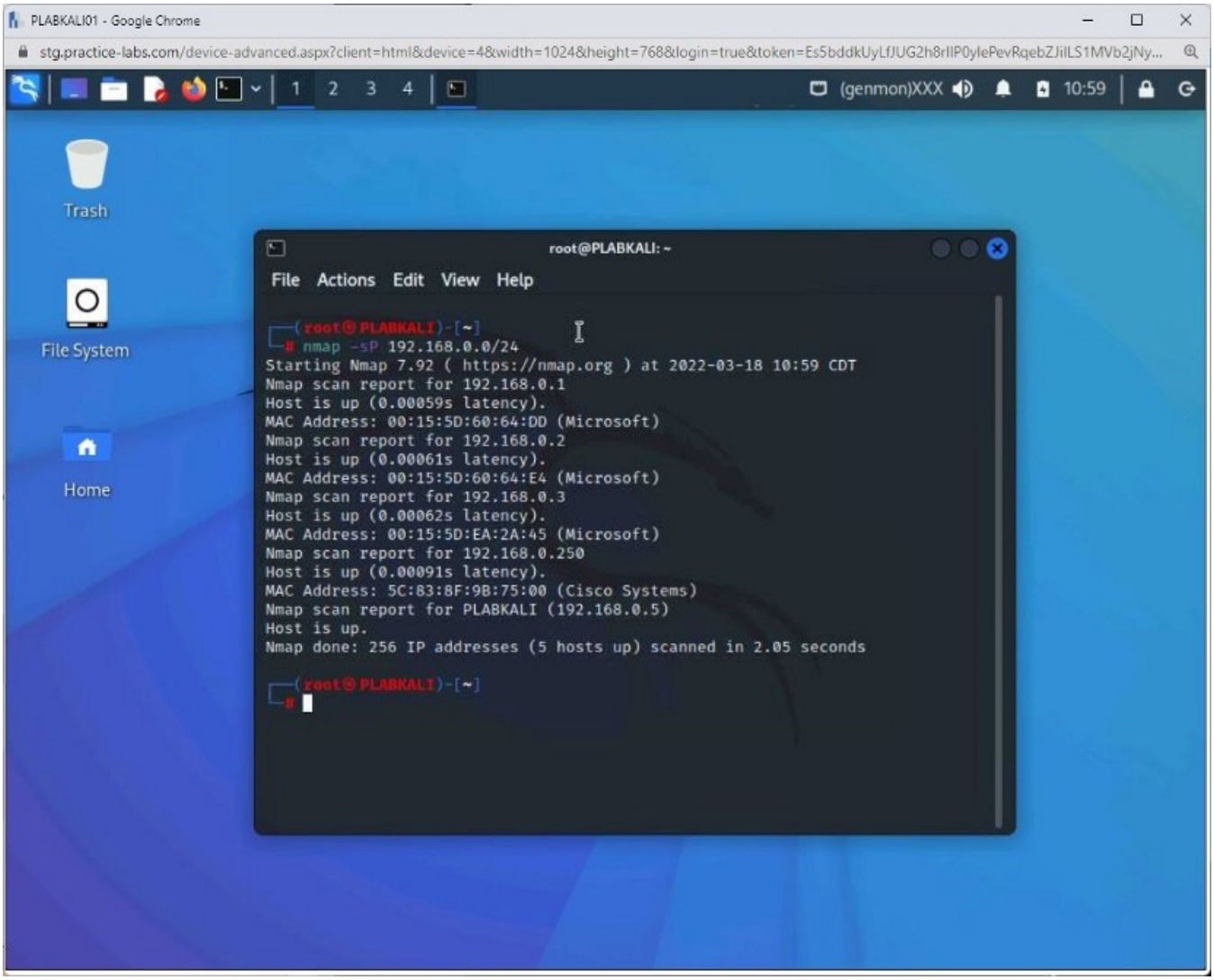



#### Step 3

The output of the following command is displayed.

Notice that **5** hosts were detected. It has found four systems in the lab environment, including Kali.

Along with this, the gateway IP, **192.168.0.250**, is also found.




**Step 4**

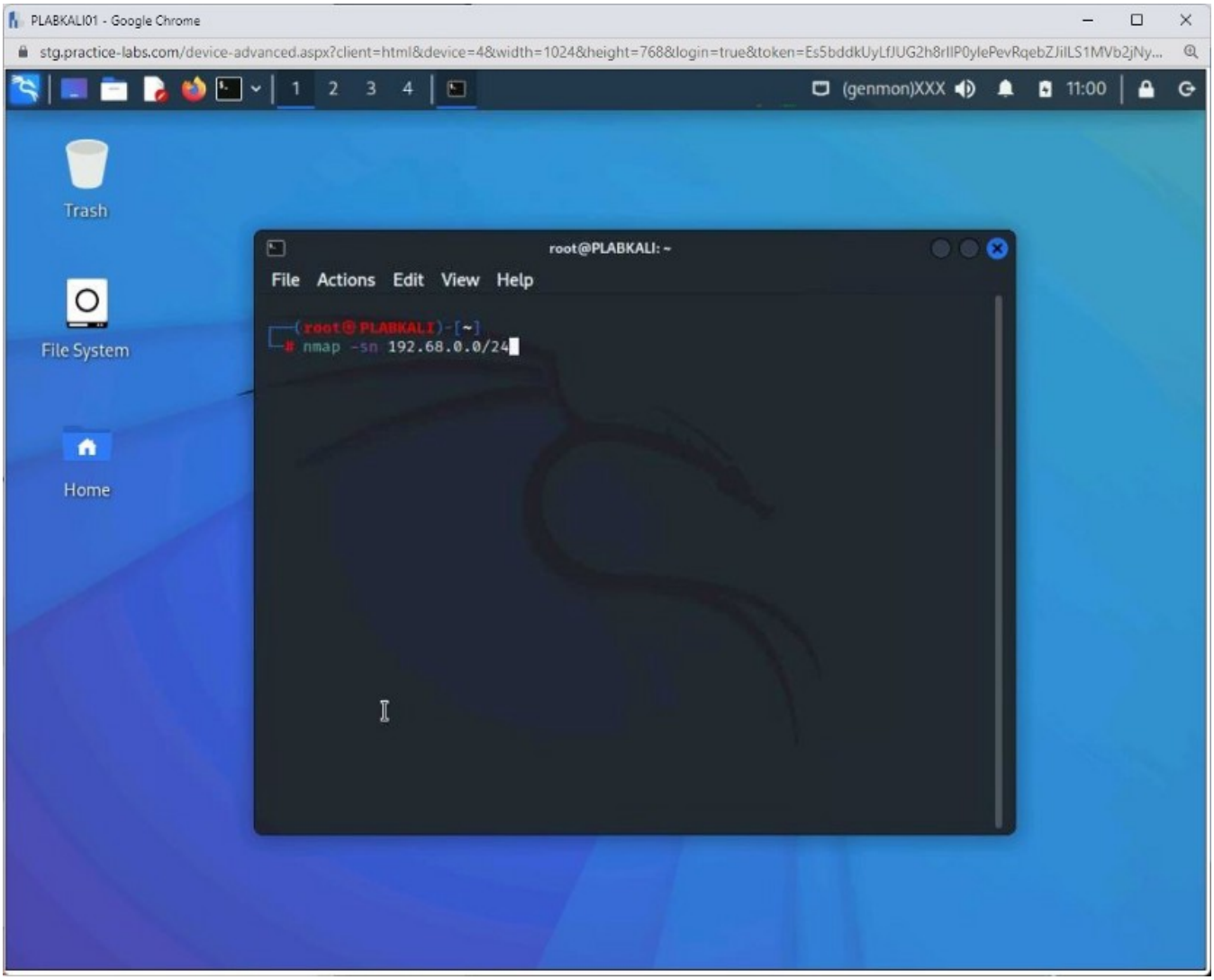
Clear the screen by entering the following command:

```
clear
```

You can also perform a scan without ping. To do this, type the following command:

```
nmap -sn 192.168.0.0/24
```

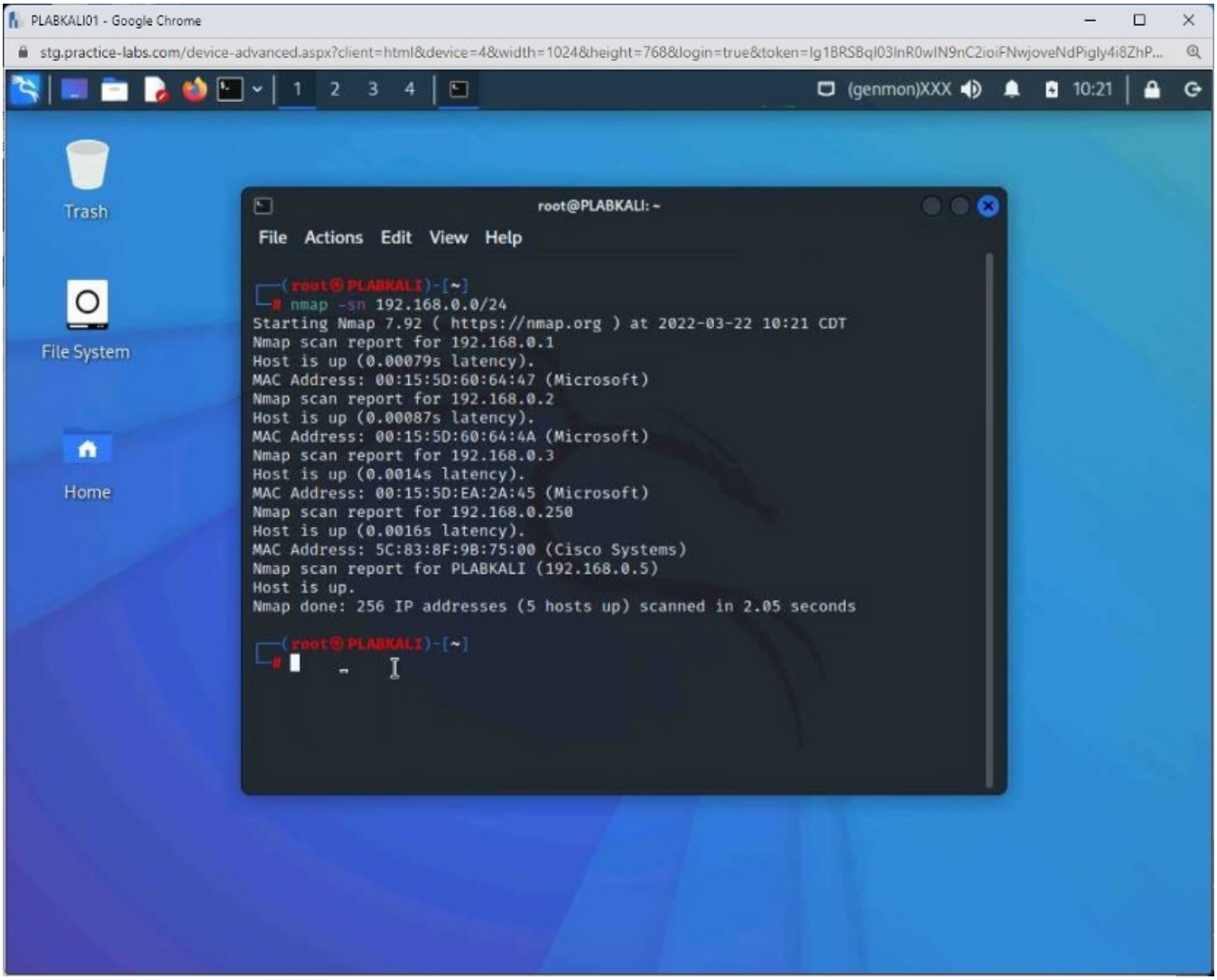
Press **Enter**.




**Step 5**

The output of the following command is displayed.

Notice that it has detected five systems on the network without the ping scan.




**Step 6**

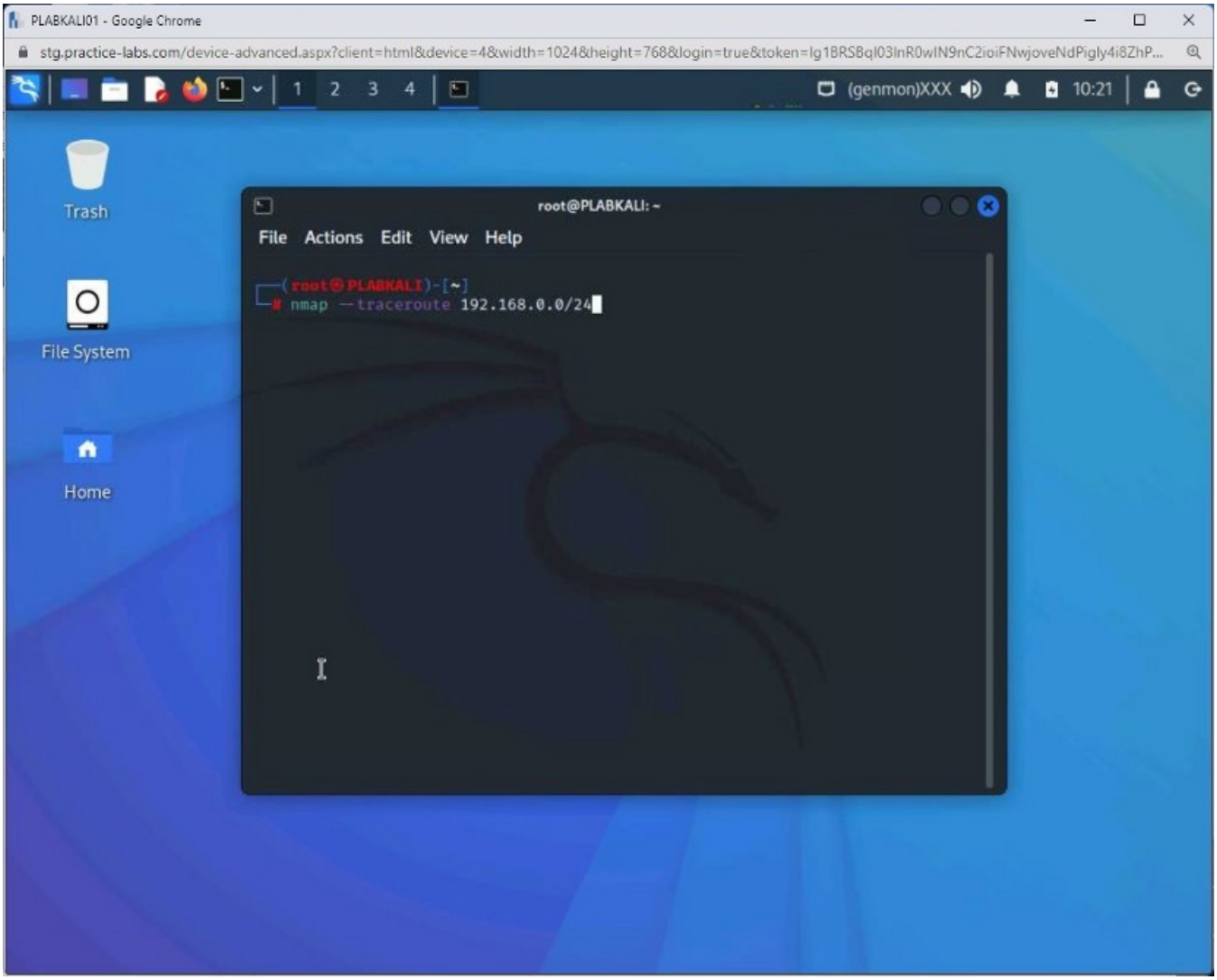
Clear the screen by entering the following command:

```
clear
```

You can also trace the path between your system and each host that is live on the network. To do this, type the following command:

```
nmap --traceroute 192.168.0.0/24
```

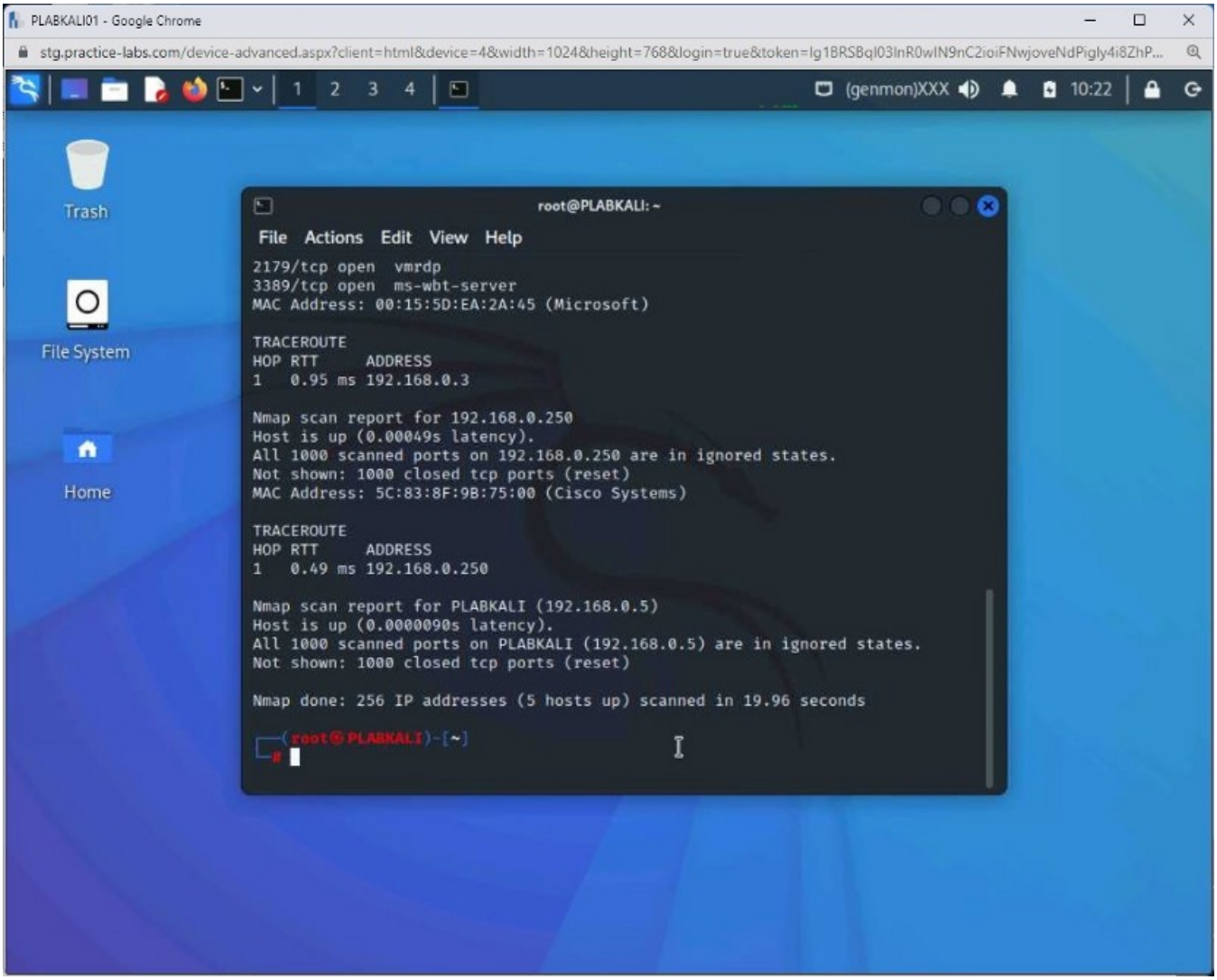
Press **Enter**.




**Step 7**

Notice the output of the command. In the output, the hops from your system to the systems on the network are displayed.

Since this is within the same IP subnet, there is a single hop. The output also displays open ports on each live system.




**Step 8**

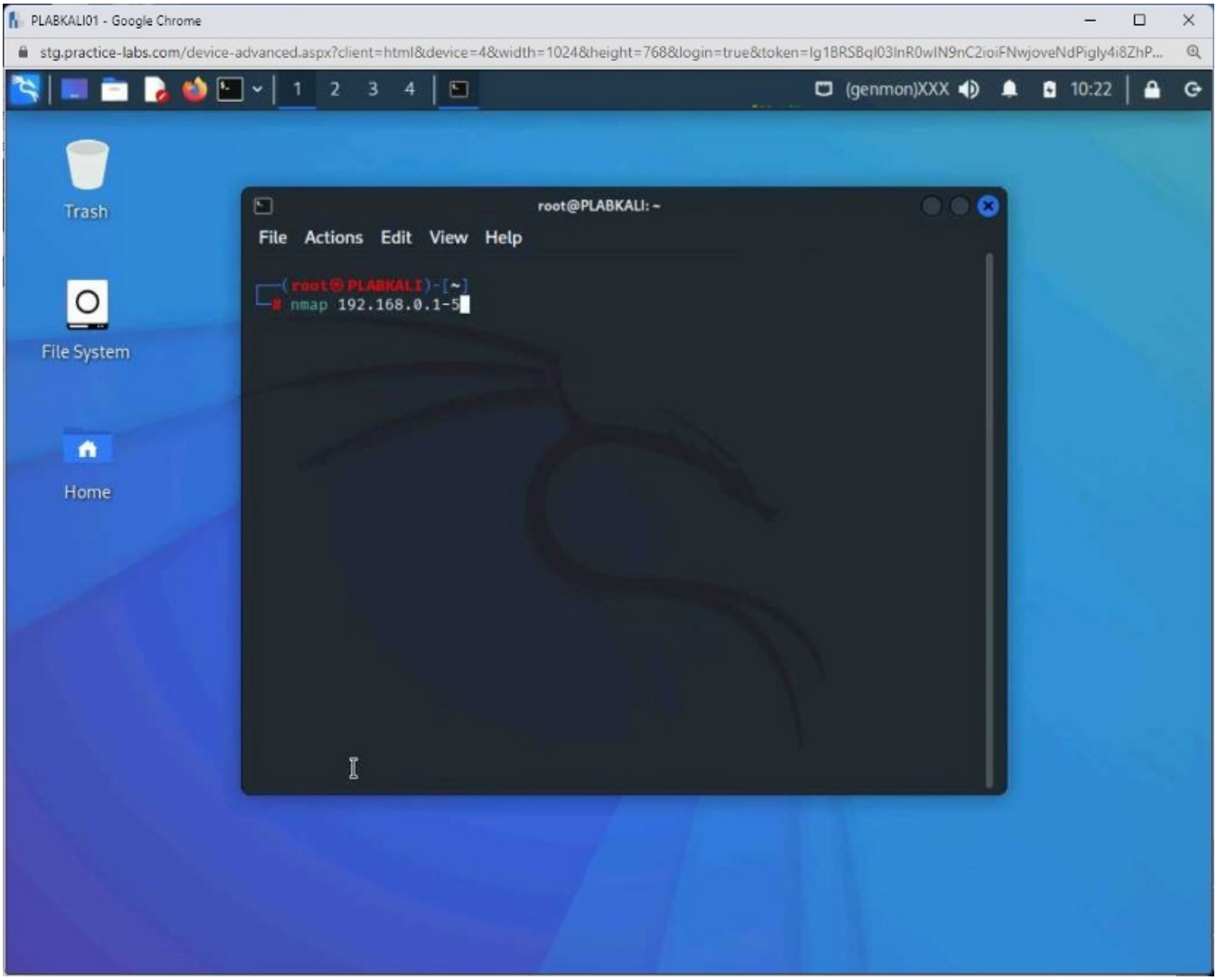
Clear the screen by entering the following command:

```
clear
```

You can also scan for live hosts on a network using an IP address range. To do this, type the following command:

```
nmap 192.168.0.1-5
```

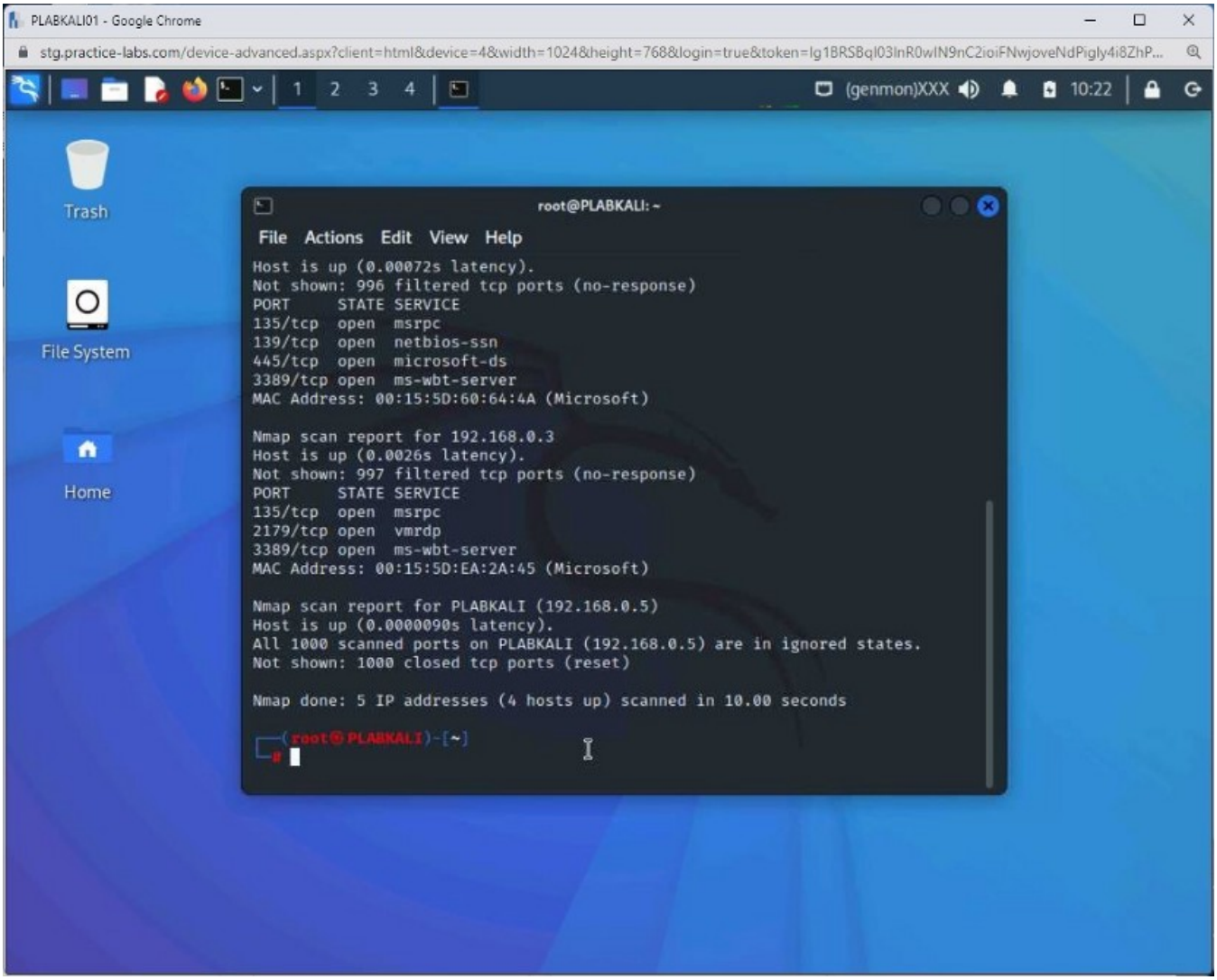
Press **Enter**.




**Step 9**

The output of the following command is displayed.

The nmap command scans the live systems and open ports without any parameters. Notice that only five hosts are listed in the scan.




**Step 10**

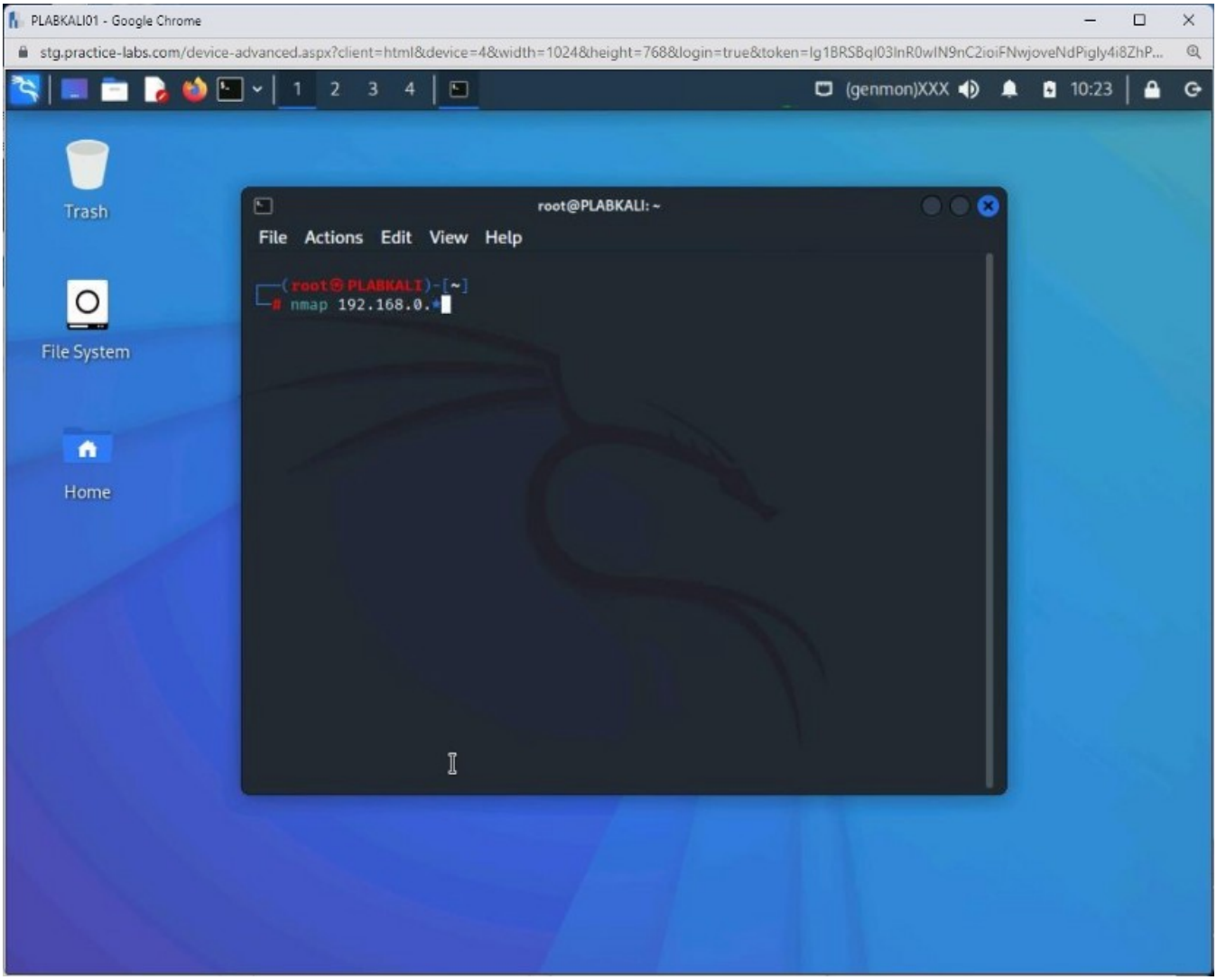
Clear the screen by entering the following command:

```
clear
```

You can also use a wildcard to scan an IP range. To do this, type the following command:

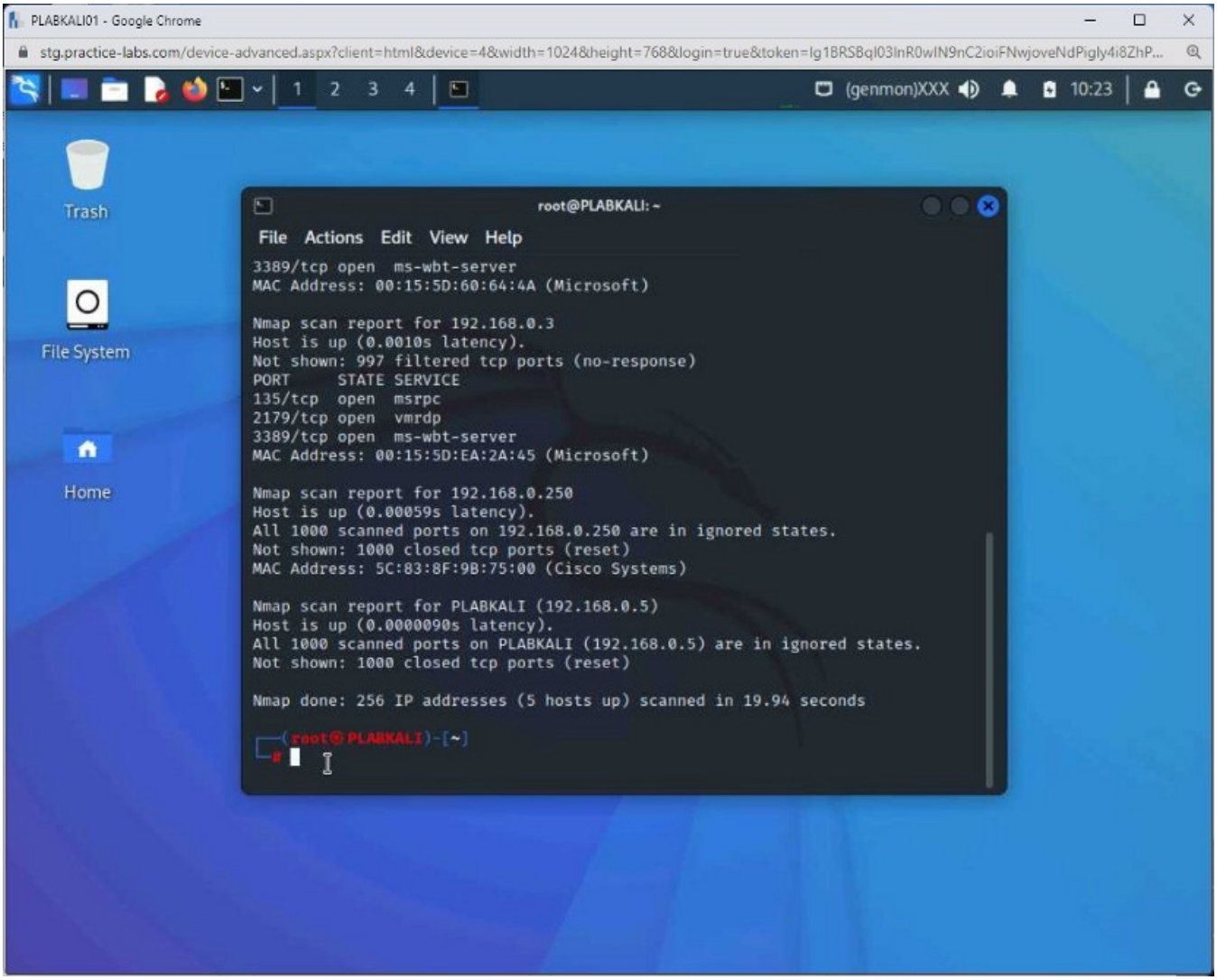
```
nmap 192.168.0.*
```

Press **Enter**.




**Step 11**

Notice the output of the nmap command with the asterisk. It has searched for all live systems in the subnet of 256 IP addresses.




Keep the terminal window open.

## Task 2 — Perform Discovery Scans

A Discovery scan is used for locating live hosts on a network. Various methods can be used in discovery scans. Some of these are:

- Using ping scan
- Using ARP scan
- Using a port scan

In this task, you will learn to perform different discovery scans. To do this, perform the following steps:

### Step 1

Ensure that you are connected to **PLABKALI01** and open the terminal window.

Clear the screen by entering the following command:

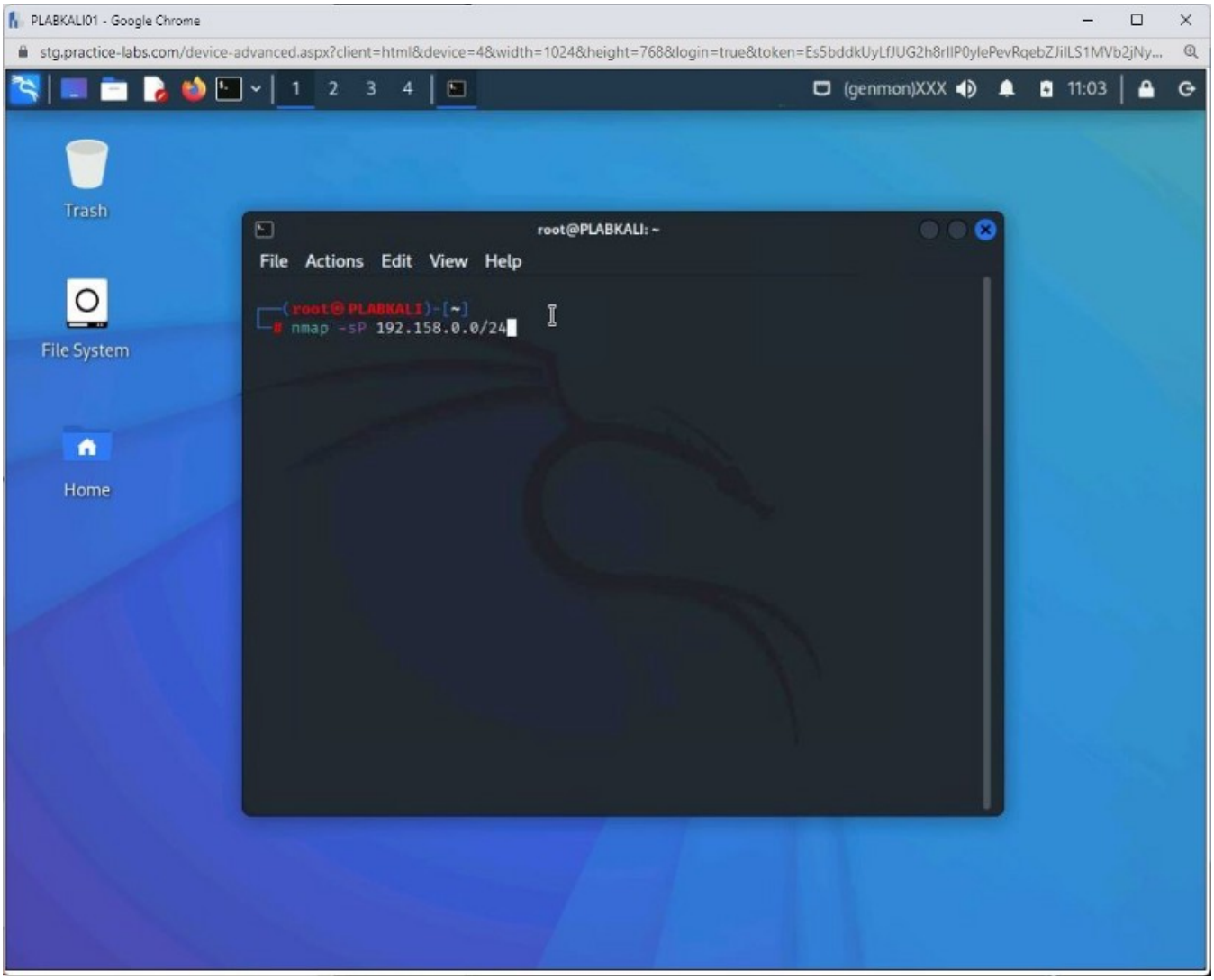
```
clear
```

Using ping for discovering a host is a common method. Type the following command:

***Note:*** *Several systems have firewalls running that block ping commands, and therefore, discovering a host using ping may not be successful.*

```
nmap -sP 192.168.0.0/24
```

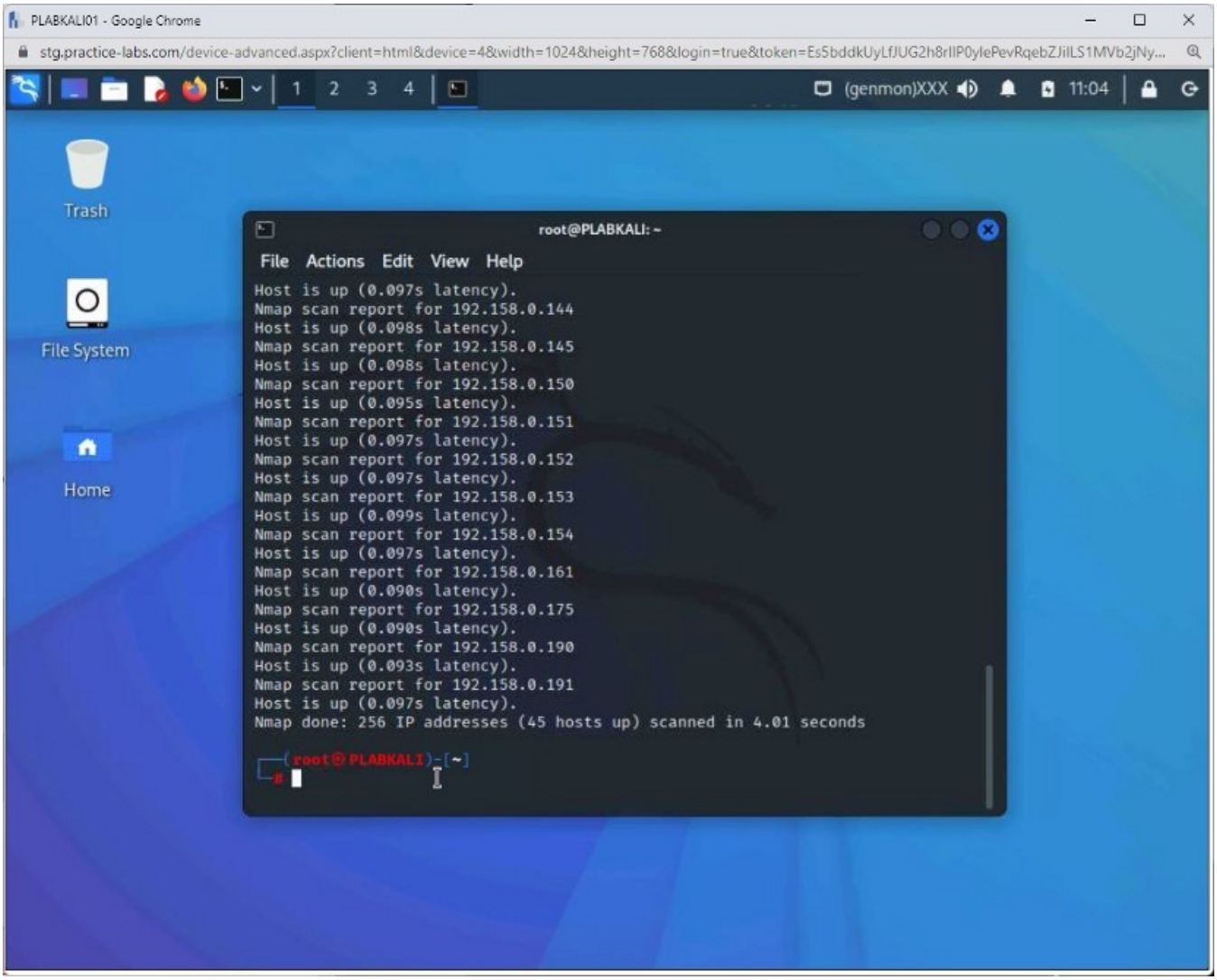
Press **Enter**.




**Step 2**

Notice the output of the command. This command sends an **ICMP REQUEST** message to every IP address when you execute it.

The hosts that respond to the message are considered alive and are listed in the output. This command does not list the hosts that do not respond.




**Step 3**

Clear the screen by entering the following command:

```
clear
```

You can also send the ARP requests to the hosts on a given subnet, and if the target system responds to the ARP requests, it is alive. Unlike the **Ping** scan method, this method is not blocked by the firewall in most cases. Therefore, you are likely to get a better outcome.

To send the ARP requests to the **192.168.0.0/24** subnet, type the following command:

```
nmap -PR 192.168.0.0/24
```

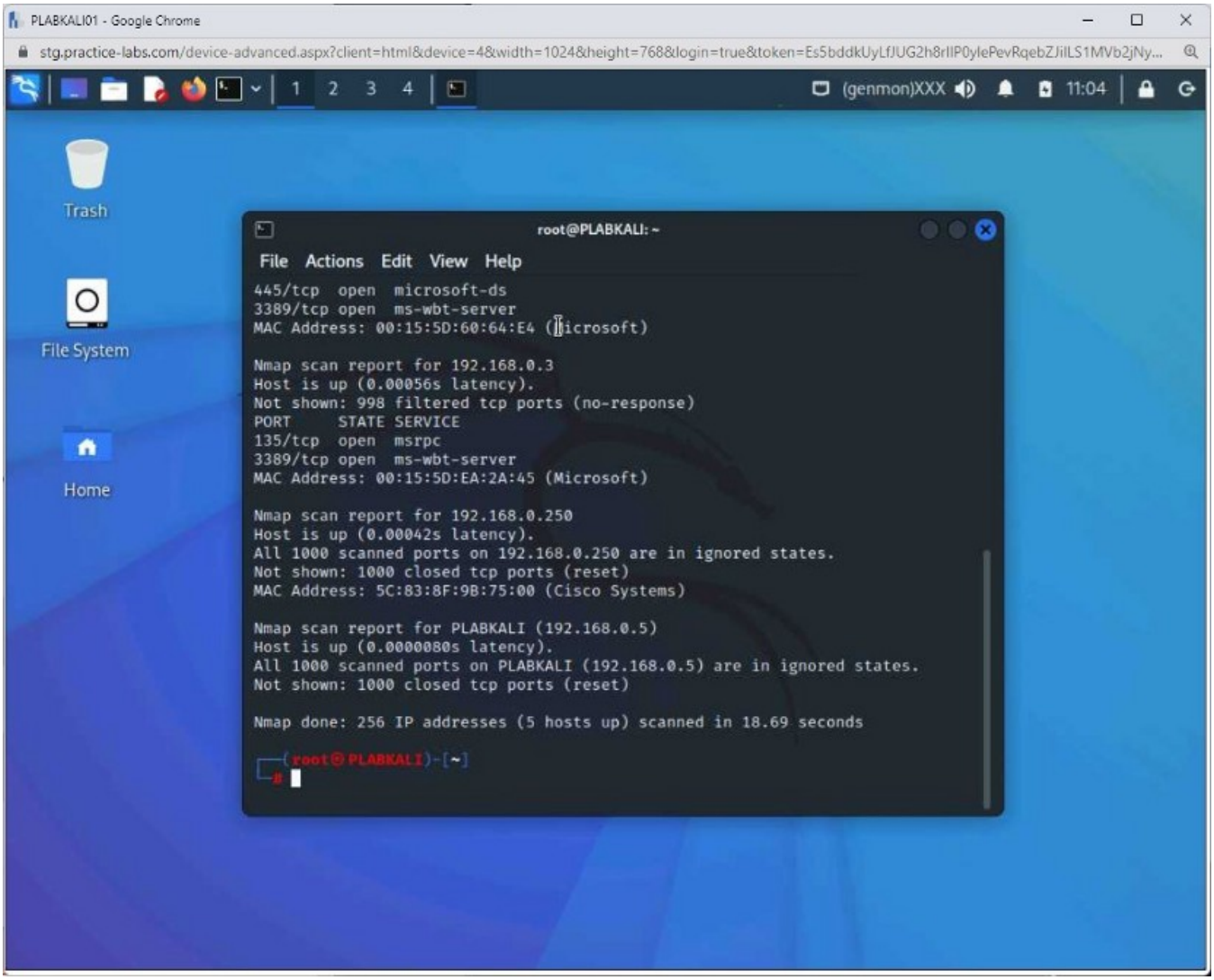
Press **Enter**.

### Step 4

Notice the outcome of this command. The nmap command has scanned **256** IP addresses with the **-PR** parameter and found seven hosts live.

Notice that open ports are also listed.

***Note:*** *You can scan for the live hosts without detecting the open ports. To do this, you can use the following command: nmap -sn 192.168.0.0/24.*




### Step 5

Clear the screen by entering the following command:

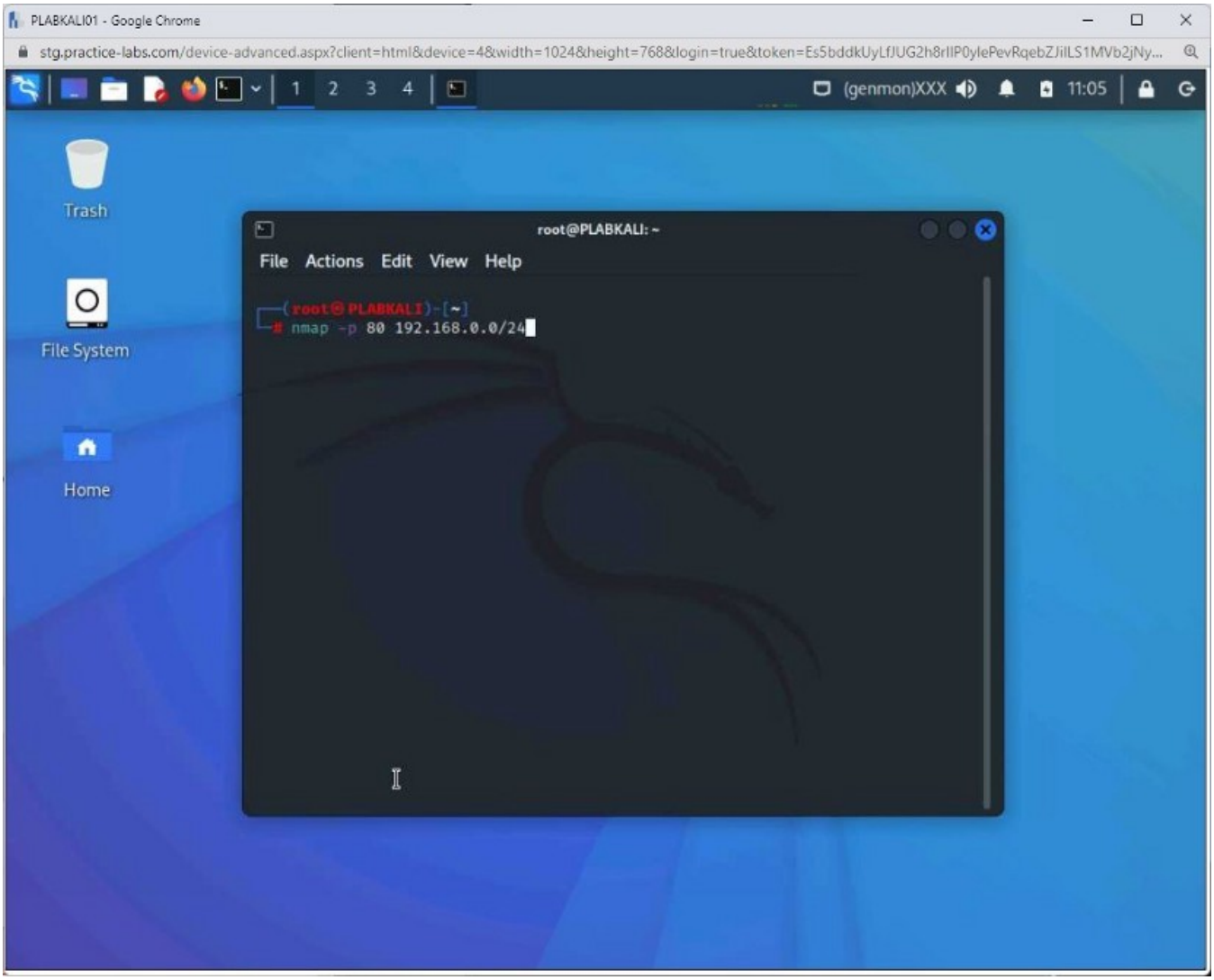
```
clear
```

You can also scan for open ports to detect the system status. This could be useful when these systems have firewalls enabled, or the systems are in another subnet or network.

When you attempt to detect the ports, the systems respond to the request. Type the following command:

```
nmap -p 80 192.168.0.0/24
```

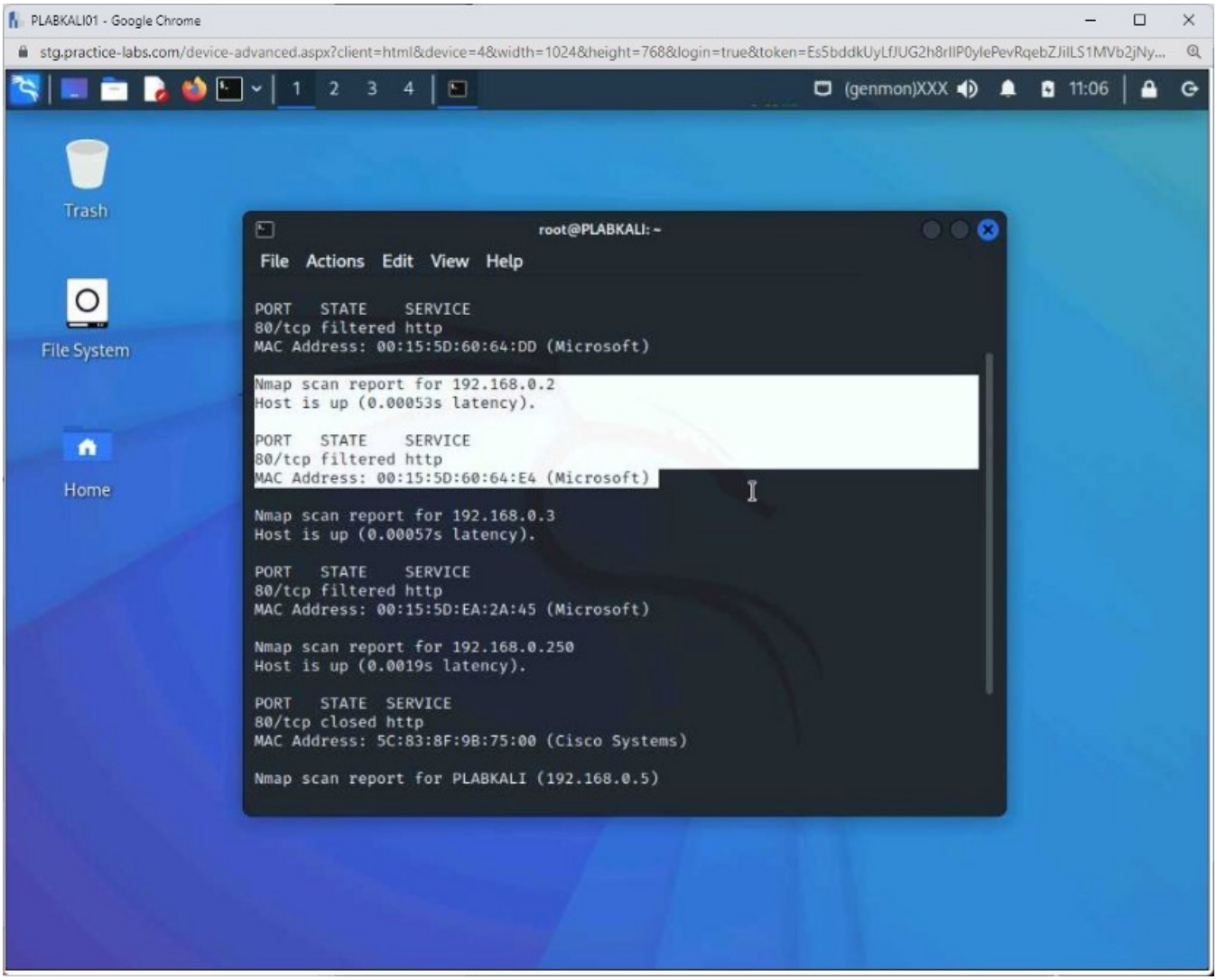
Press **Enter**.




**Step 6**

The output of this command is displayed. Notice that seven hosts are scanned, but one host, **192.168.0.2**, runs a web server.

***Note:*** *With the -p parameter, you can scan for more than one port. For example, you can use the following command: nmap -p 22, 23, 80, 139, 445, 3389 192.168.0.0/24. Each port number needs to be separated by a comma.*




#### Step 7

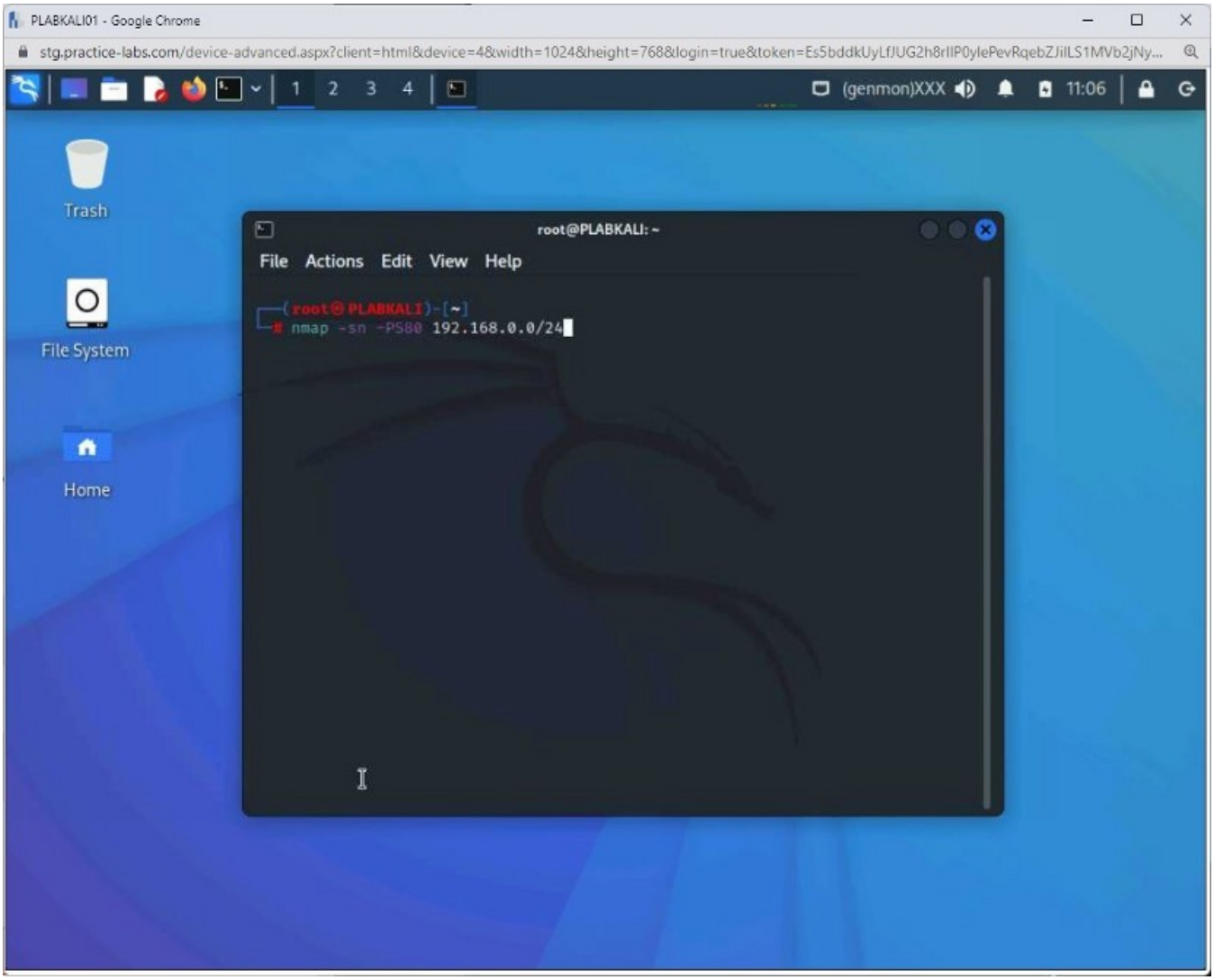
Clear the screen by entering the following command:

```
clear
```

You can also send the **SYN** message to a specific port on a subnet to detect live systems. To do this, type the following command:

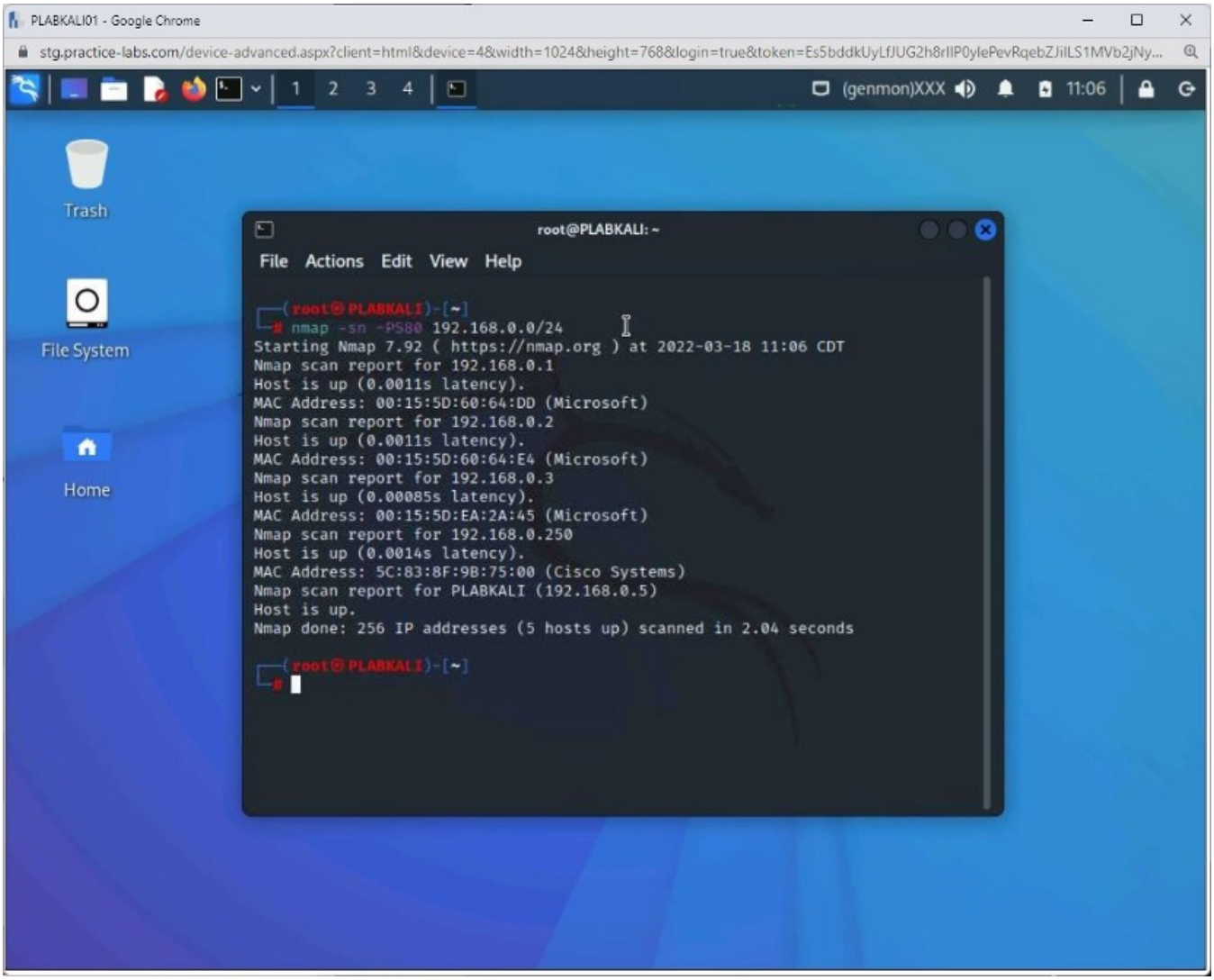
```
nmap -sn -PS80 192.168.0.0/24
```

Press **Enter**.




### Step 8

The output of this command is displayed. Notice that five hosts were found to be live in this subnet.




## Exercise 3 — Port and Service Discovery

When an attacker detects live systems on a network, the next task would be to detect open ports and services, which the users can intentionally or unintentionally leave open.

Attackers look for open ports and services and then exploit them. This is probably one of the easiest methods to launch an attack.

In this exercise, you will perform port and service discovery.

## Learning Outcomes

After completing this exercise, you will be able to:

- Scan for Open Ports and Services
- Perform Port Scanning
- Perform Service Probing

- Use Netcat for Port Scanning

## 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 MemberWorkstation192.168.0.5/24PLABDM01Domain Member Server192.168.0.2/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABDM01

Windows Server 2019 — Domain Member192.168.0.2/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

## Task 1 — Scan for Open Ports and Services

The **Nmap** and **Netstat** Linux command enable you to discover open ports on a system. Using the **Nmap** command, you can perform port scanning of a specific system or more than one system on the network. The **Netstat** command is a network information tool that can provide information about the network connection, routing tables, and much more.

In this task, you will discover open ports on a system.

### Step 1

Ensure that you are connected to **PLABKALI01** and open the terminal window.

Clear the screen by entering the following command:

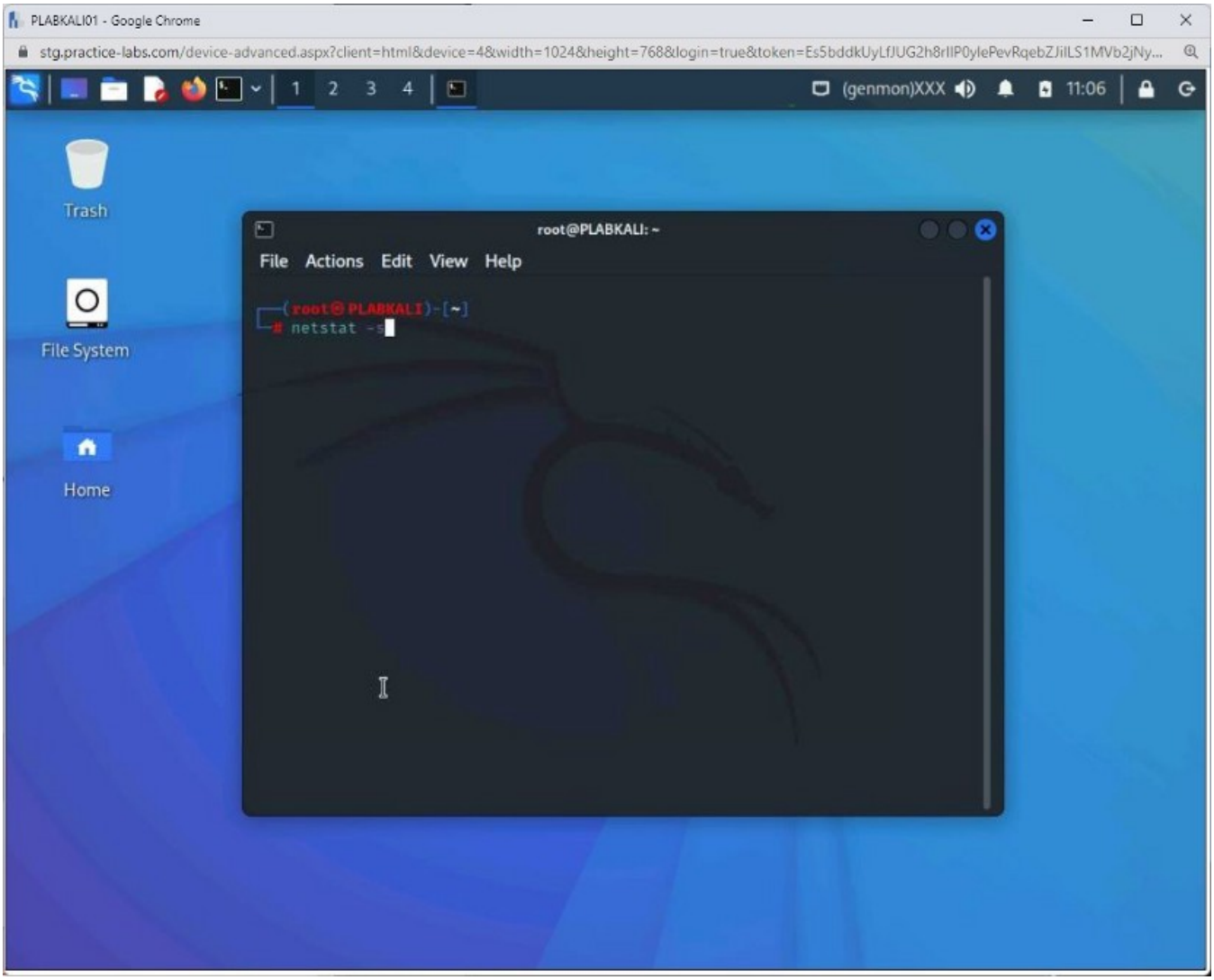
```
clear
```

To show protocol statistics, which are the protocols being used on the local system, type the following information:

```
netstat -s
```

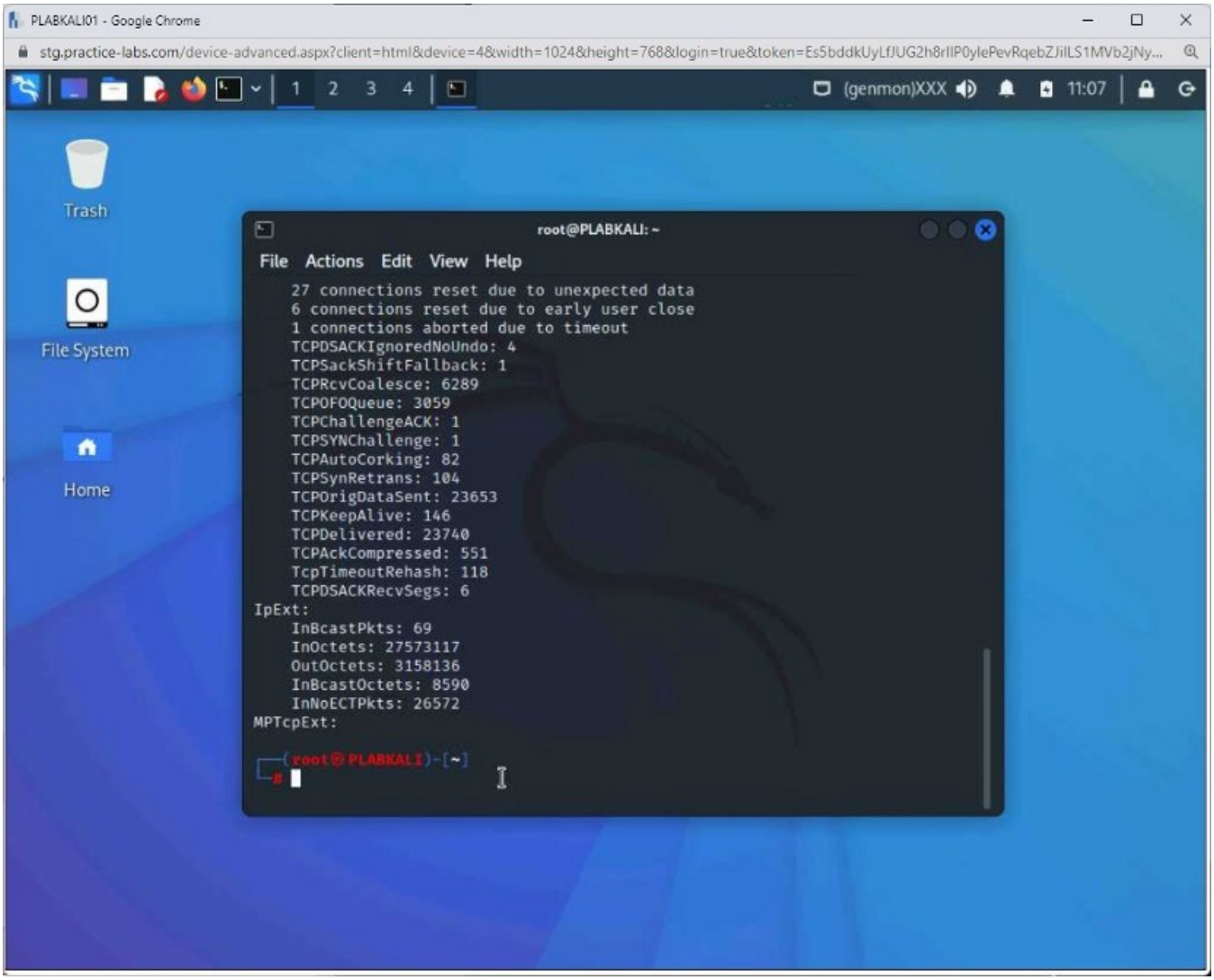
Press **Enter**.

***Note:*** *The* ***-s*** *parameter shows the per-protocol statistics. To view the complete details, scroll up in the terminal window.*




**Step 2**

The output of the **netstat -s** command is displayed.




**Step 3**

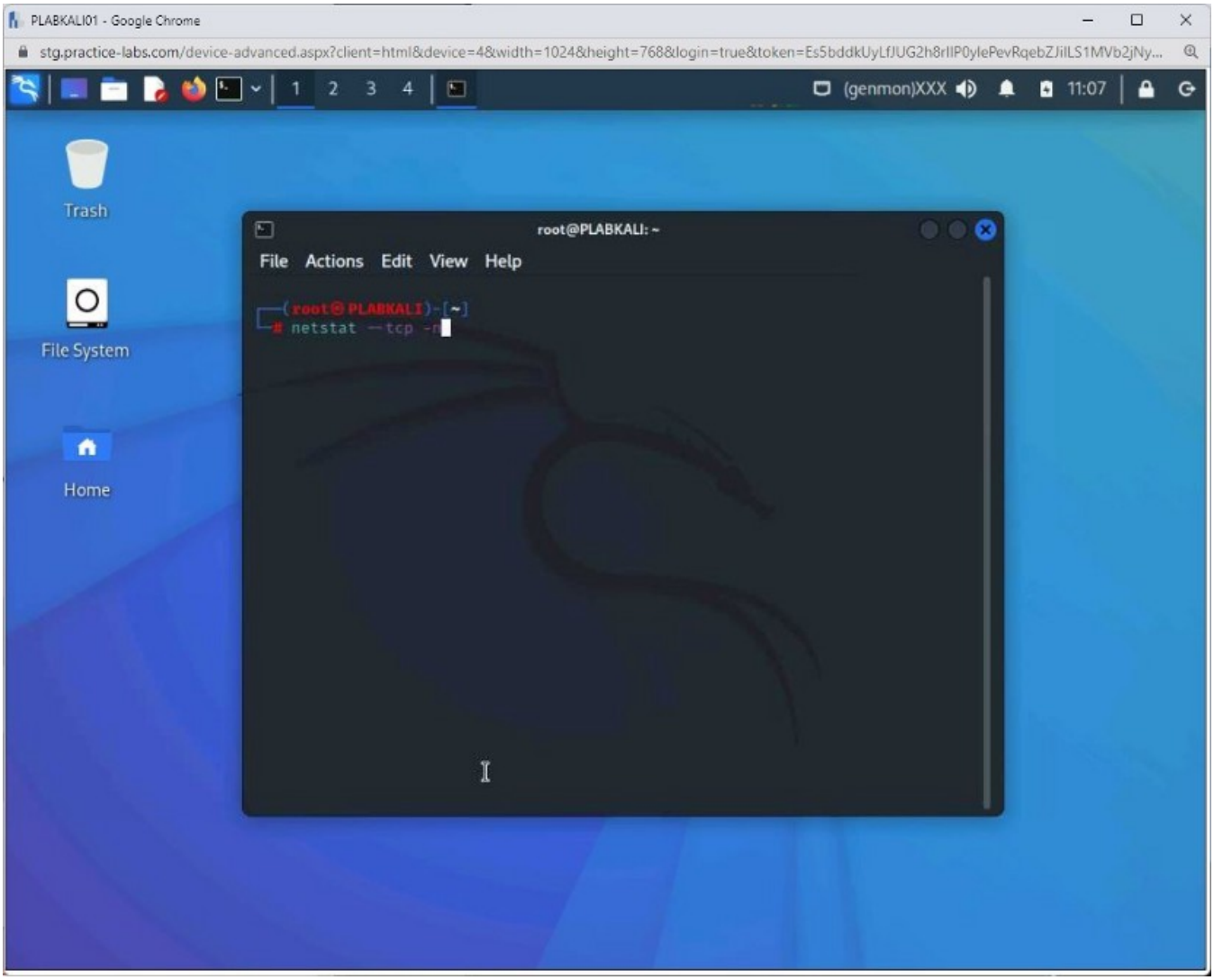
Clear the screen by entering the following command:

```
clear
```

To display the active **TCP** connections, type the following command:

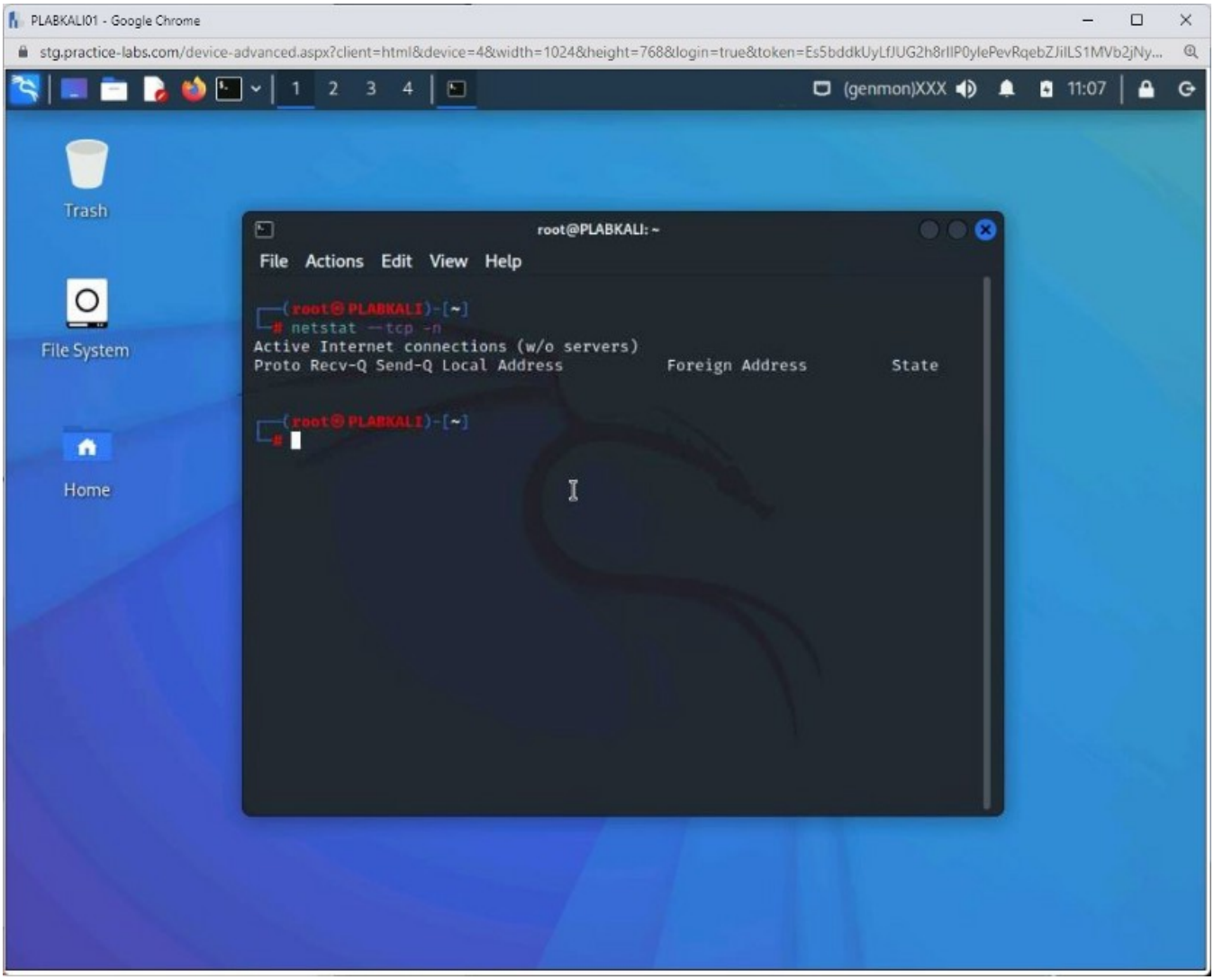
```
netstat --tcp -n
```

Press **Enter**.




**Step 4**

This command shows connections with the network addresses on the TCP protocol. Currently, there seem to be no TCP connections.




**Step 5**

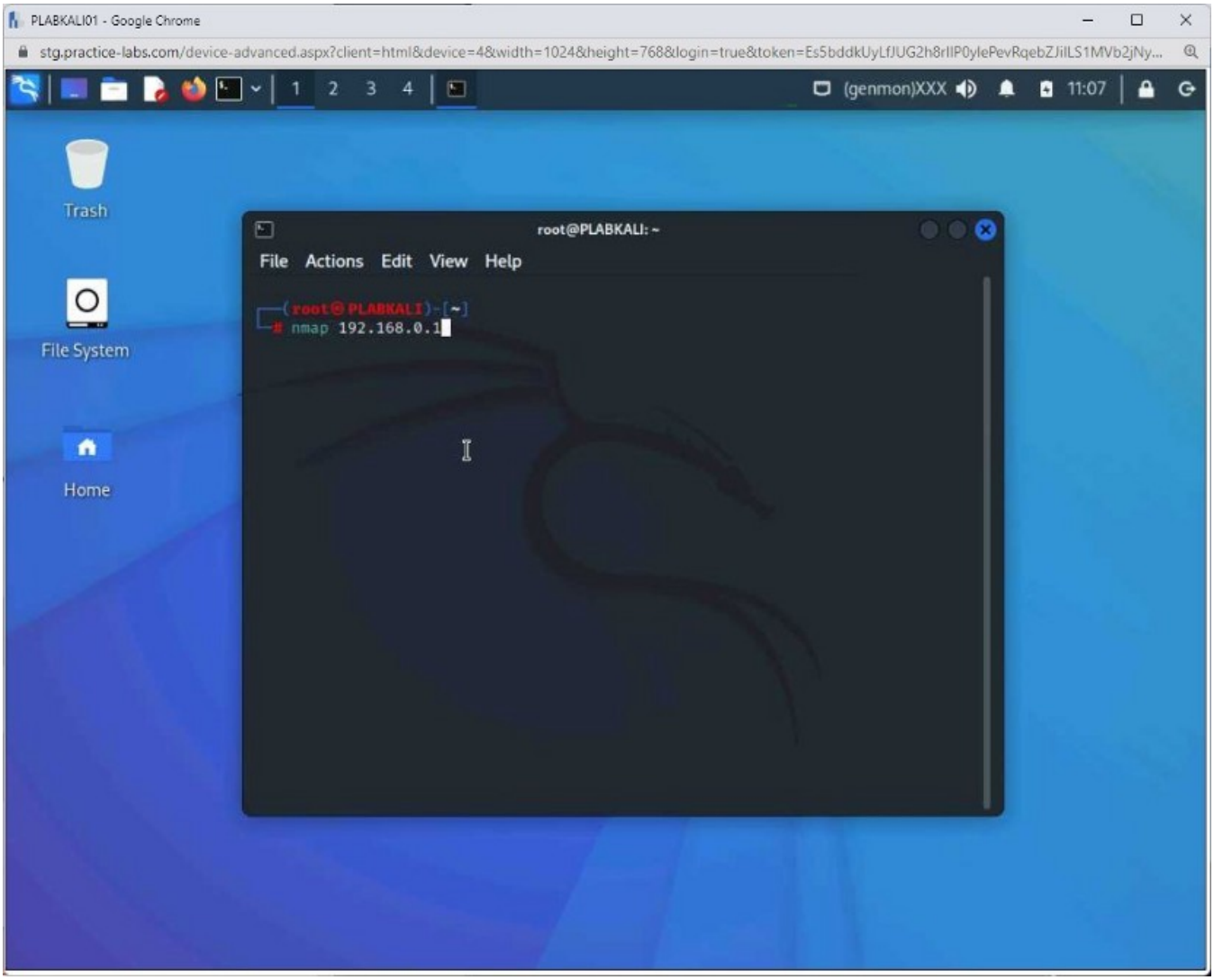
Clear the screen by entering the following command:

```
clear
```

Let's now use the nmap command. Type the following command:

```
nmap 192.168.0.1
```

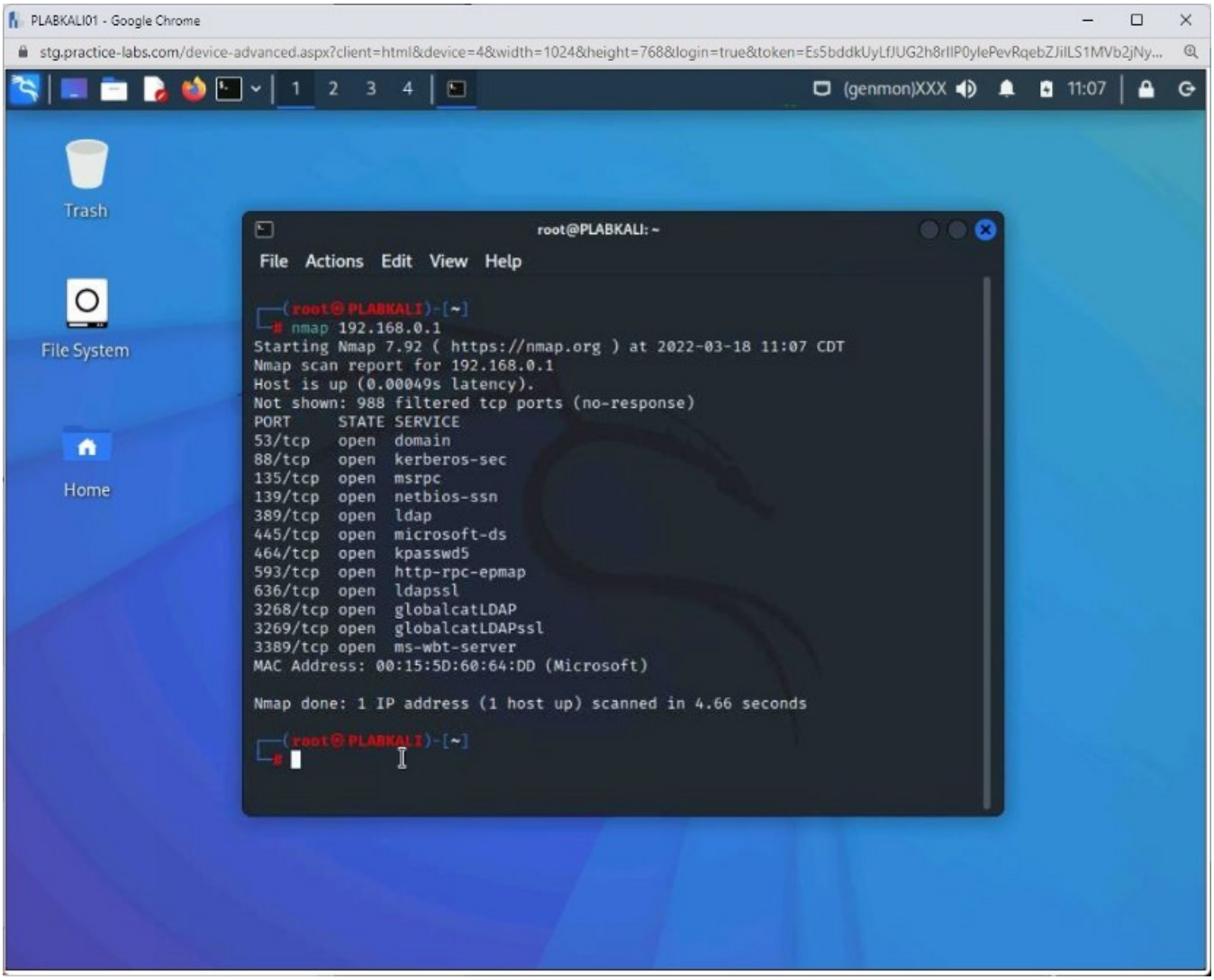
Press **Enter**.




**Step 6**

The results are displayed.

The output shows the open ports with the protocols.




**Step 7**

Clear the screen by entering the following command:

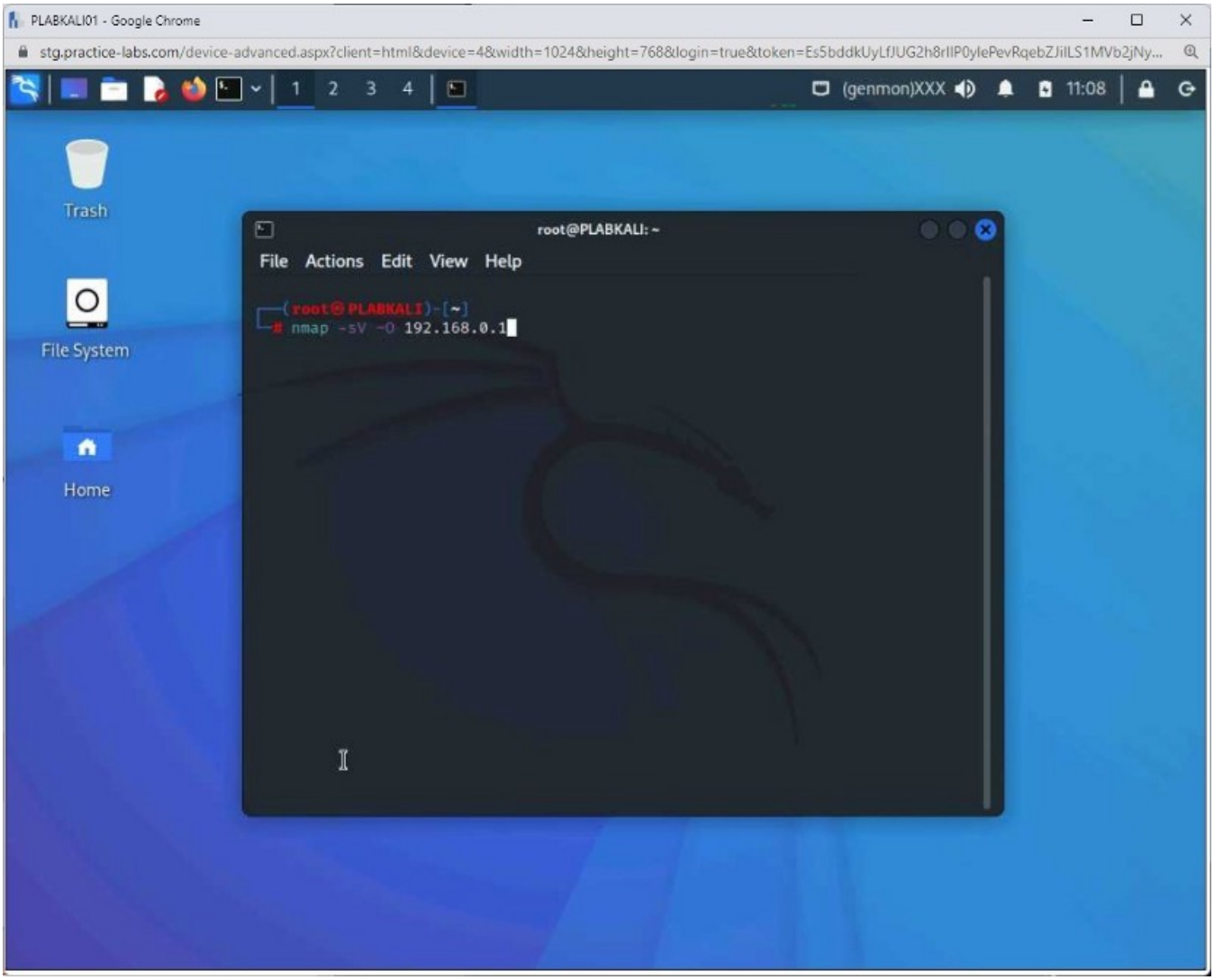
```
clear
```

You can also list the services and their versions running on a system along with its operating system.

To do this, type the following command:

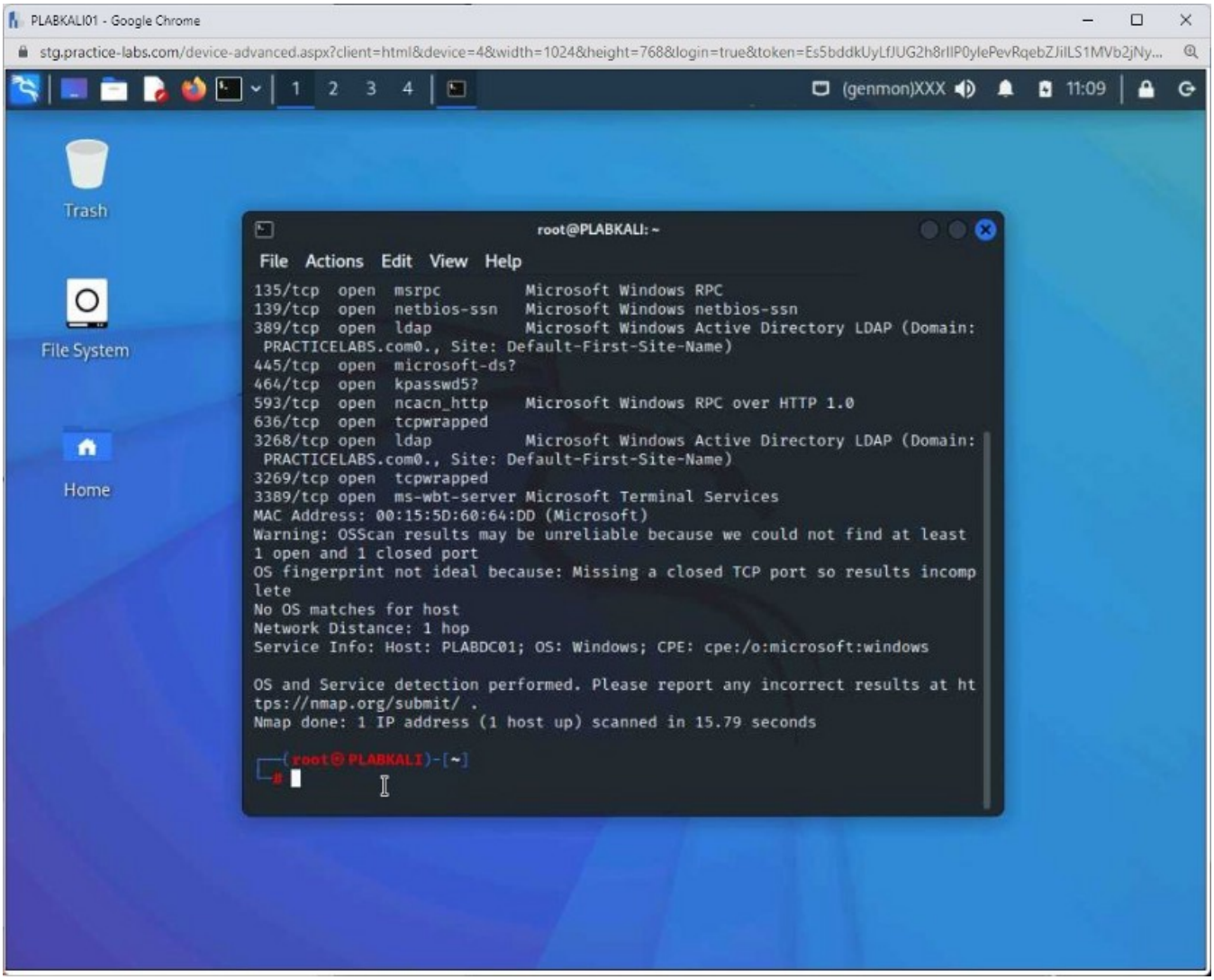
```
nmap -sV -O 192.168.0.1
```

Press **Enter**.




**Step 8**

As a result of the command, several running services and the operating system have been detected.




**Step 9**

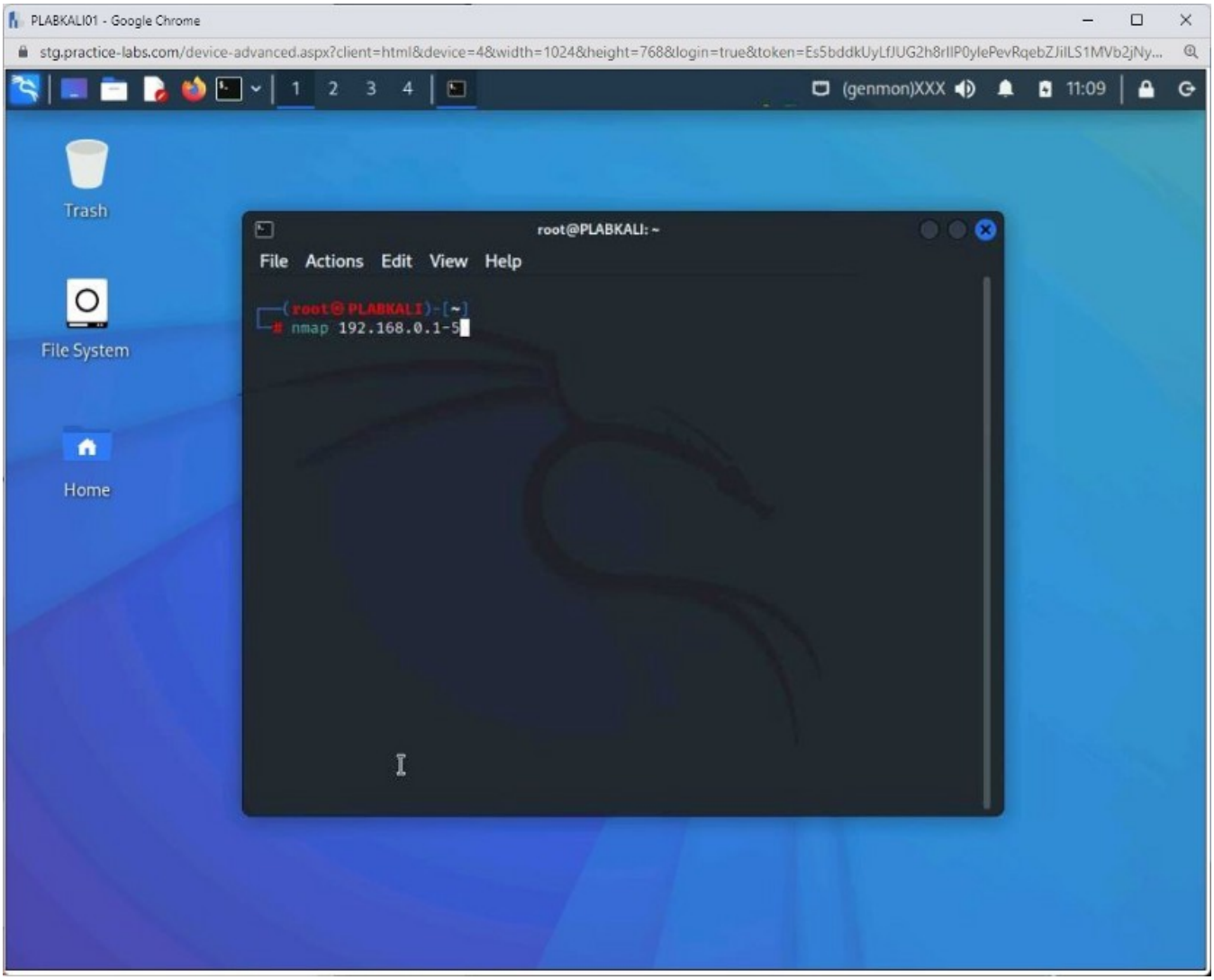
Clear the screen by entering the following command:

```
clear
```

You can also scan for open ports on several systems at once. To do this, type the following command:

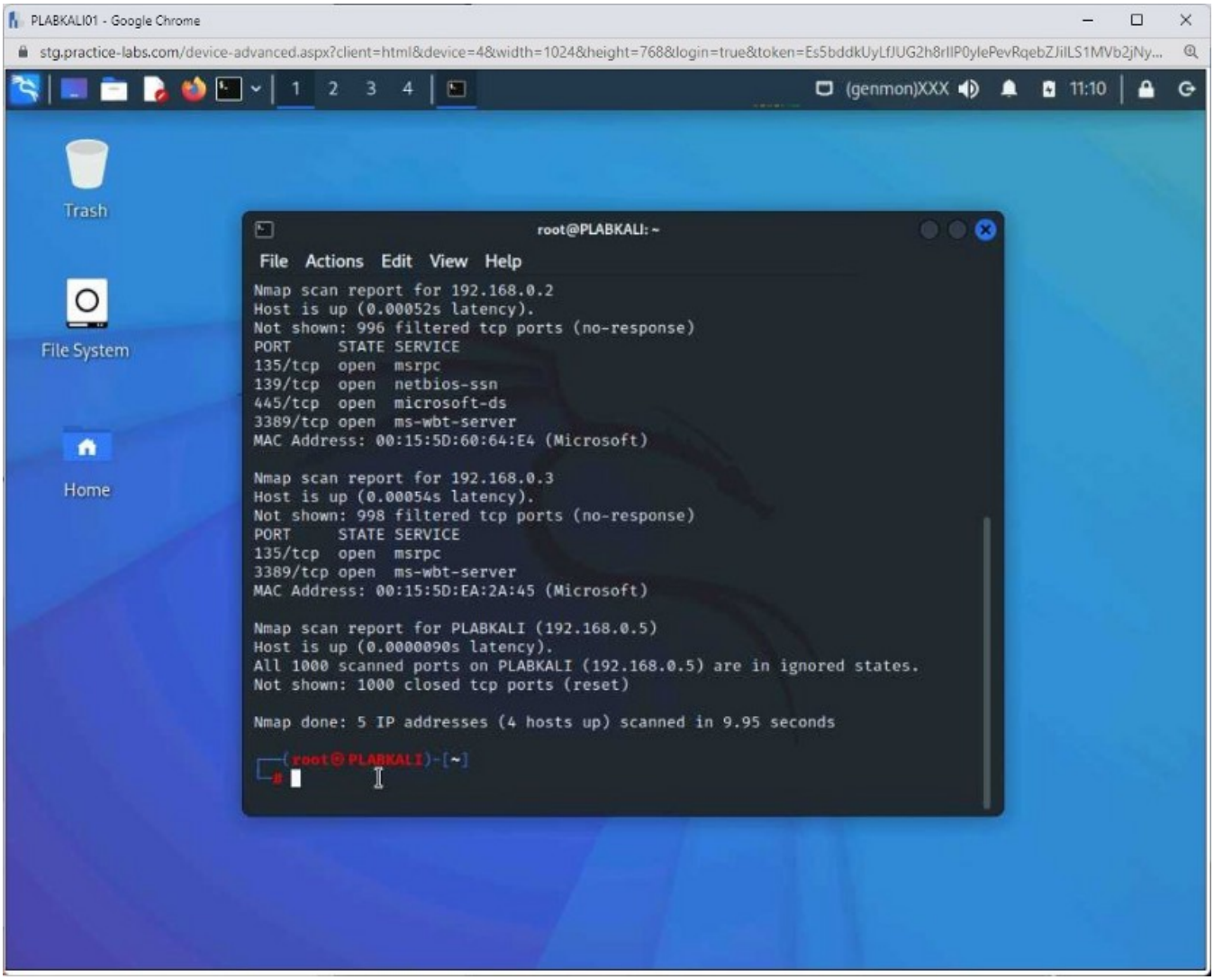
```
nmap 192.168.0.1-5
```

Press **Enter**.




**Step 10**

The command takes a few seconds to run and then displays the output.




Keep the terminal window open.

## Task 2 — Perform Port Scanning

Using the port scan method, you can determine the TCP or UDP port. You can either scan for the entire range of ports, from **1** to **65535**, or scan for specific ports.

When scanning for ports, you need to be aware that there can be different states of a port:

- **Open**: An application is listening for connections on this port.
- **Closed**: The messages were received, but no application listened on the port.
- **Filtered**: The messages were not received, and the state of the port could not be determined. This state occurs when some type of filtering is used on the port.
- **Unfiltered**: The messages are received, but still, the state of the port cannot be determined.

- **Open/Filtered**: The port was either filtered or open, but Nmap could not determine the state.
- **Closed/Filtered**: The port was either filtered or closed, but Nmap could not determine the state.

To use port scanning, perform the following steps:

#### Step 1

Ensure that you are connected to **PLABKALI01** and open the terminal window.

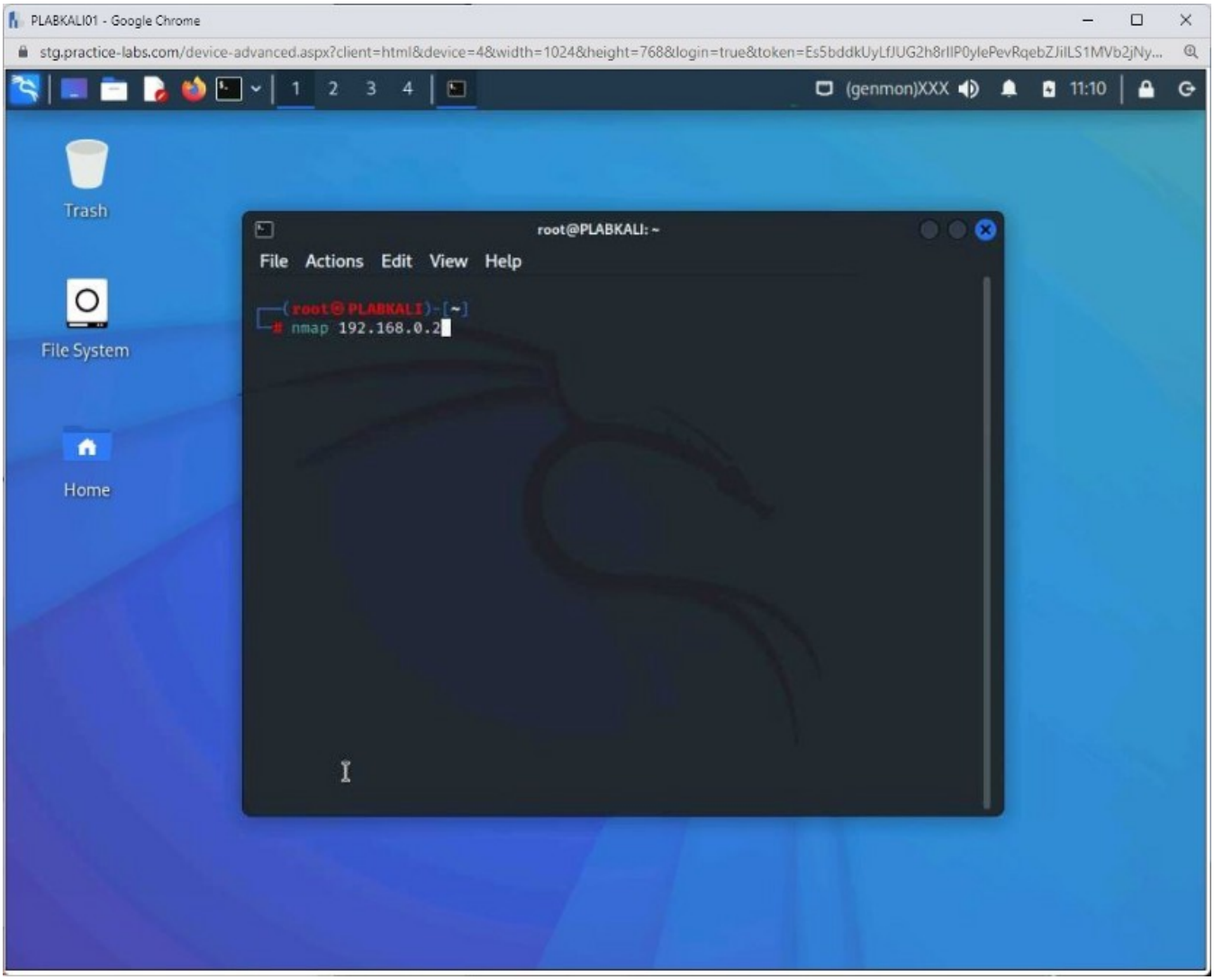
Clear the screen by entering the following command:

```
clear
```

One of the simplest methods is to target a system with the **nmap** command without using any parameters.

```
nmap 192.168.0.2
```

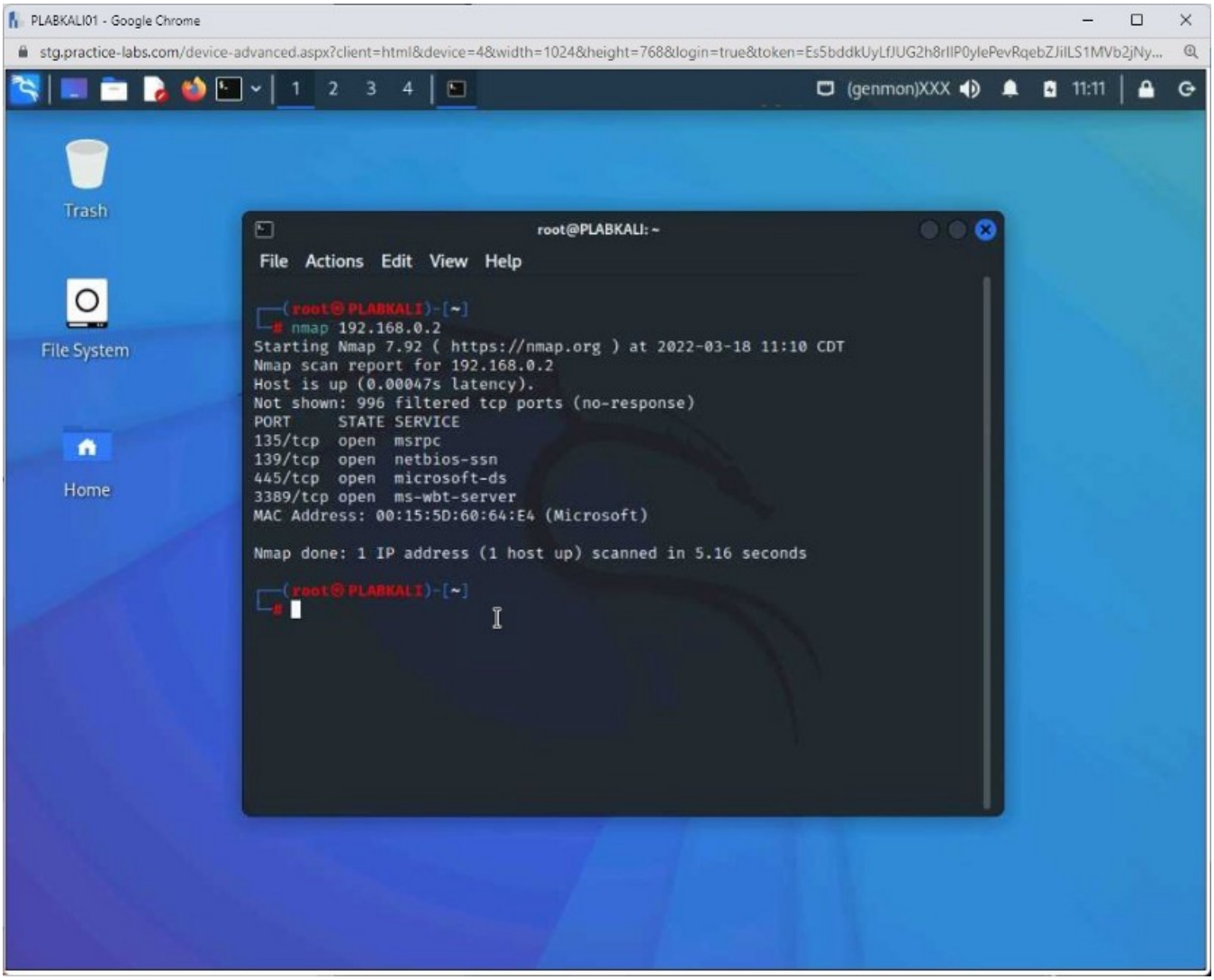
Press **Enter**.




**Step 2**

The output of this command is displayed.

Notice that **192.168.0.2** has four ports open, which are **135**, **139**, **445** and **3389**.




**Step 3**

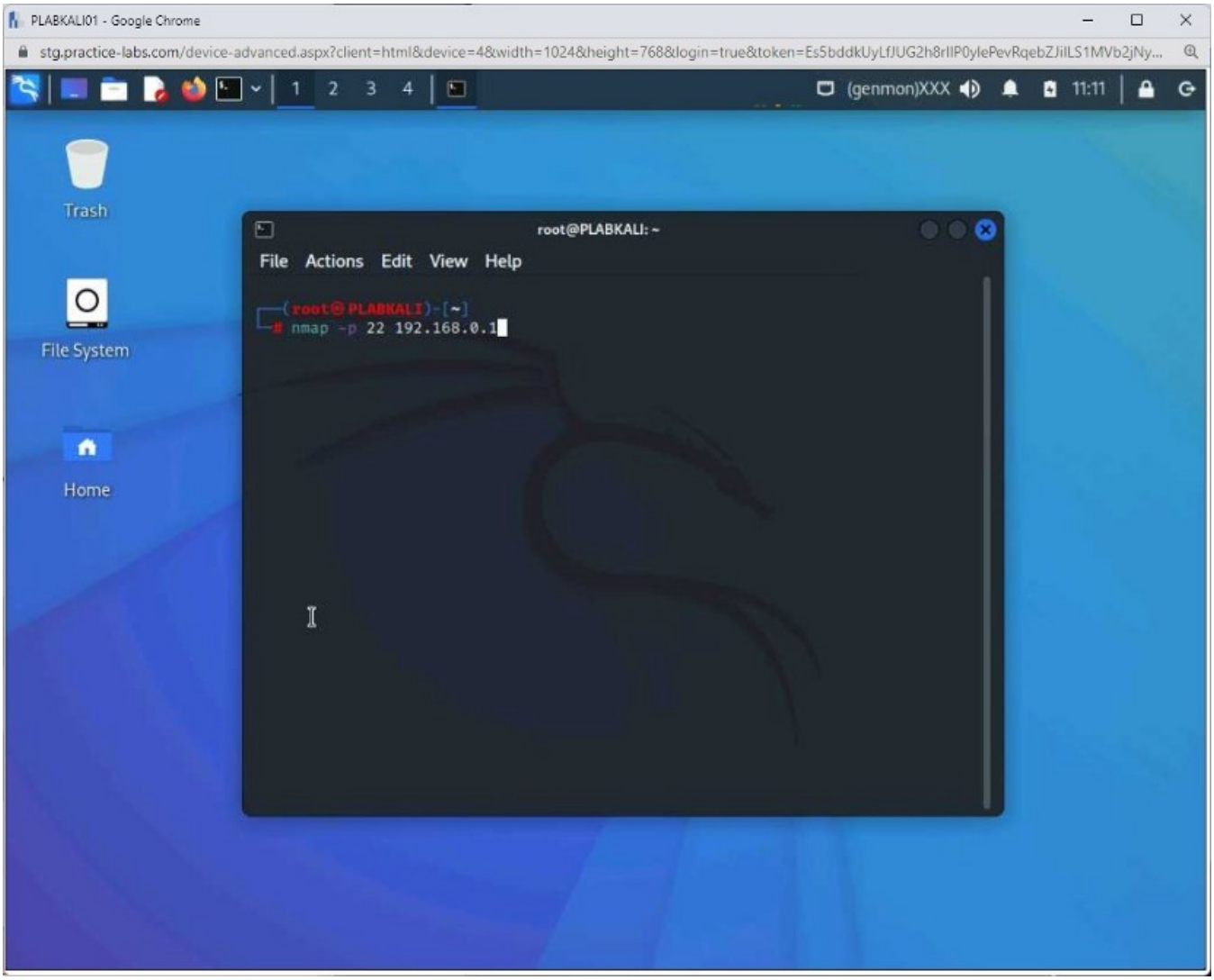
Clear the screen by entering the following command:

```
clear
```

You can scan for a single port on a host. To do this, type the following command:

```
nmap -p 22 192.168.0.1
```

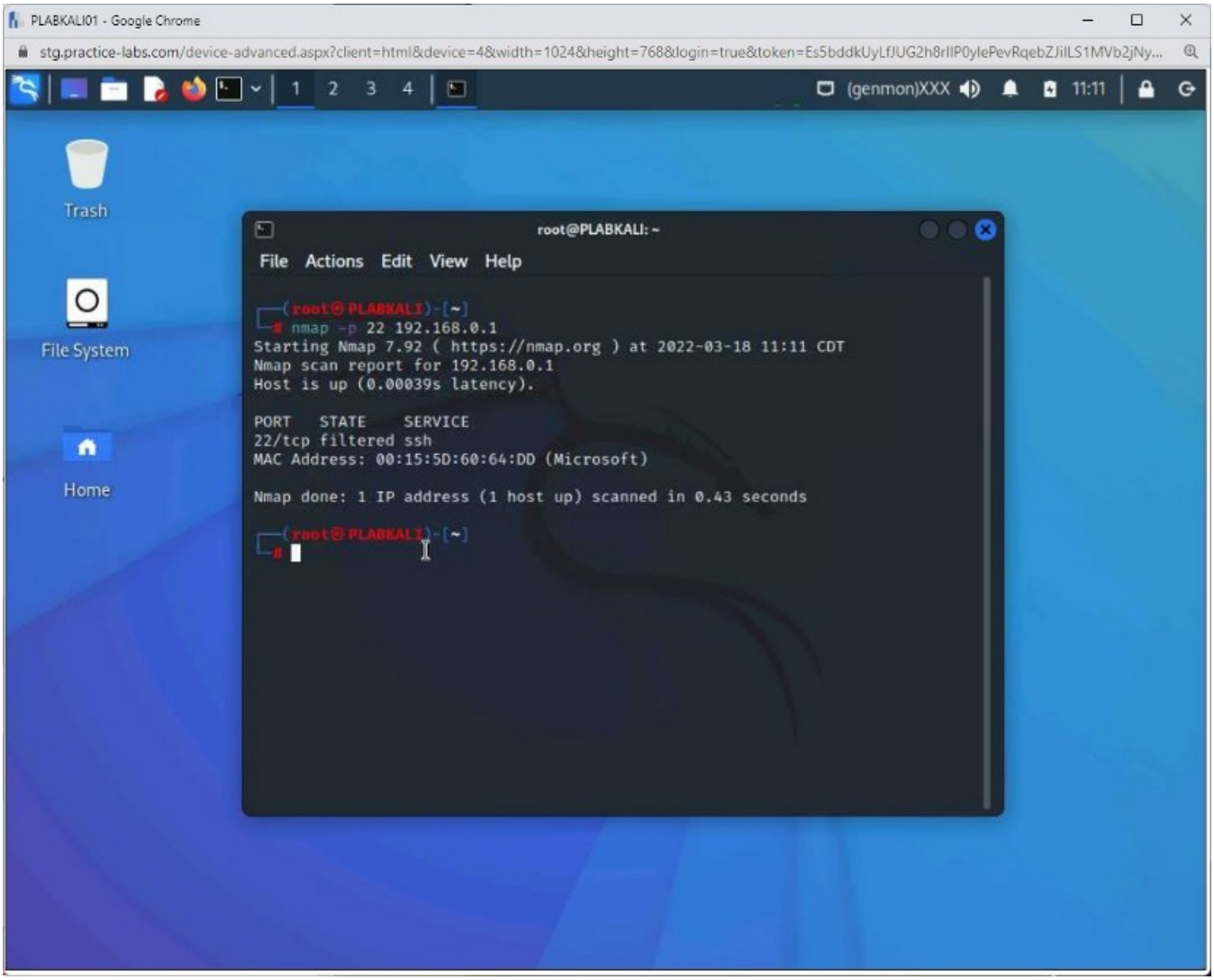
Press **Enter**.




**Step 4**

The output of this command is displayed.

Notice that the state of the port is set to **filtered**.

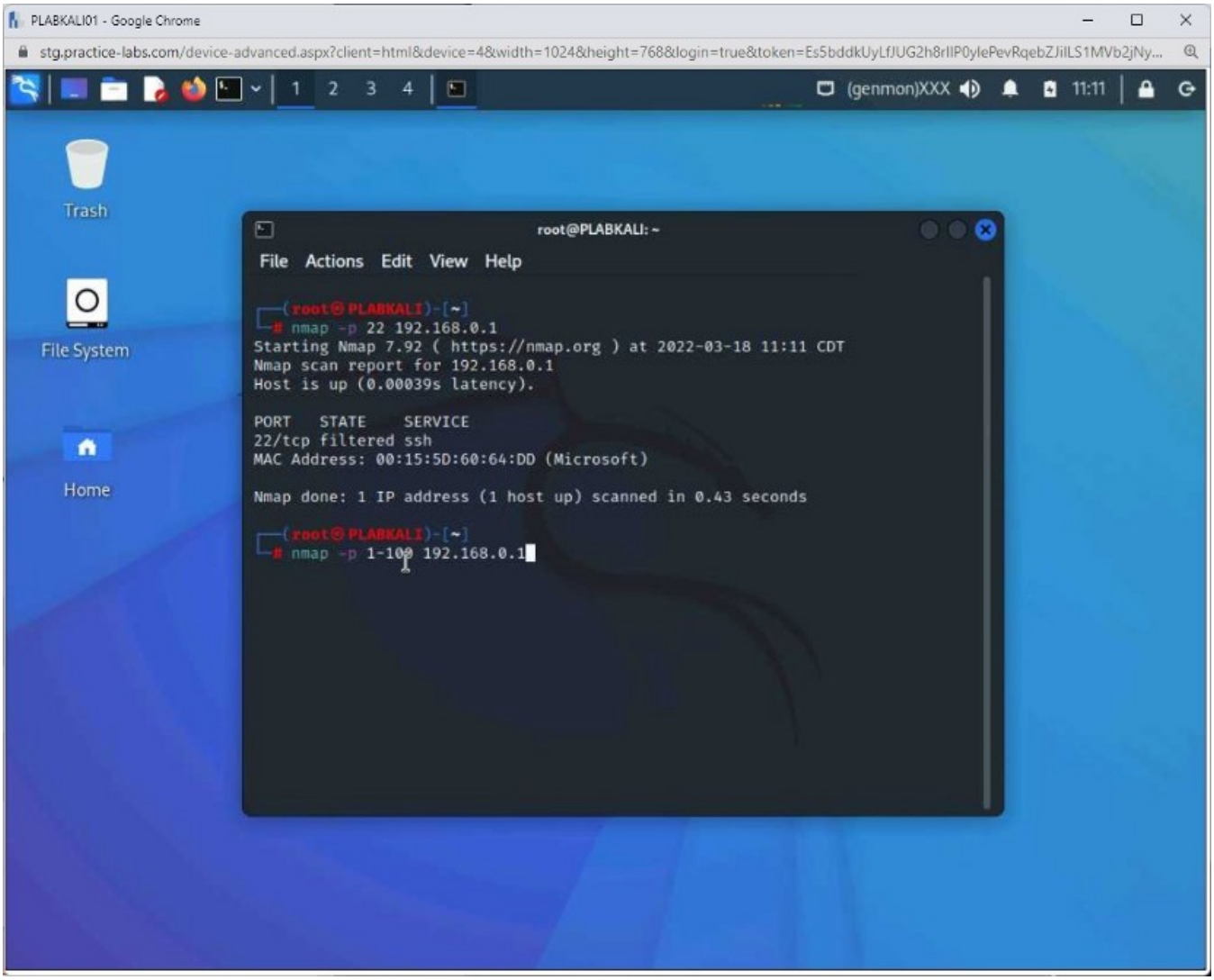



**Step 5**

Let's try to scan for the range of ports on **192.168.0.1**, which is the domain controller. To do this, type the following command:

```
nmap -p 1-100 192.168.0.1
```

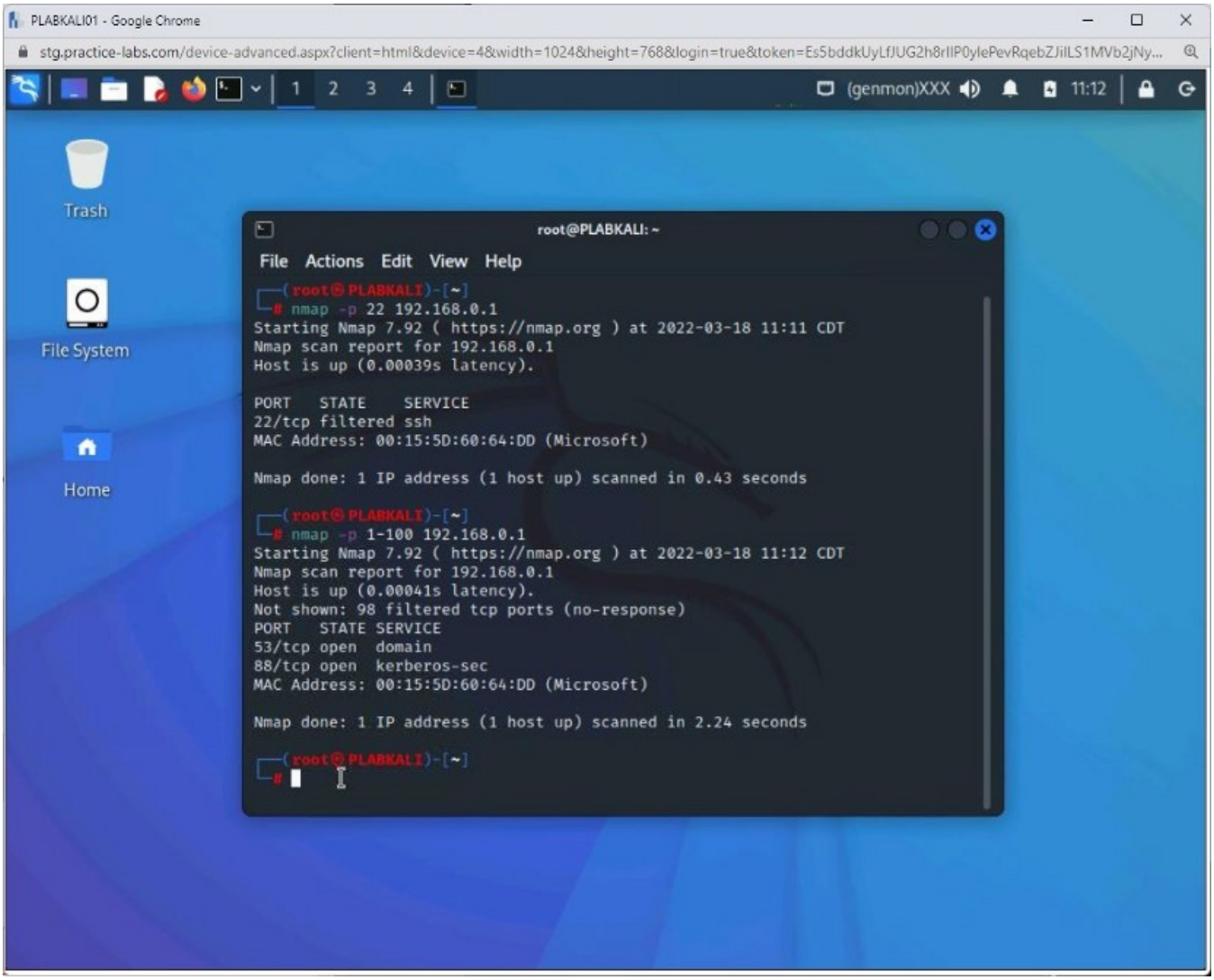
Press **Enter**.




**Step 6**

Notice that the command has been executed successfully.

The output displays **98** filtered ports and two open ports, **53** and **88**.




**Step 7**

Clear the screen by entering the following command:

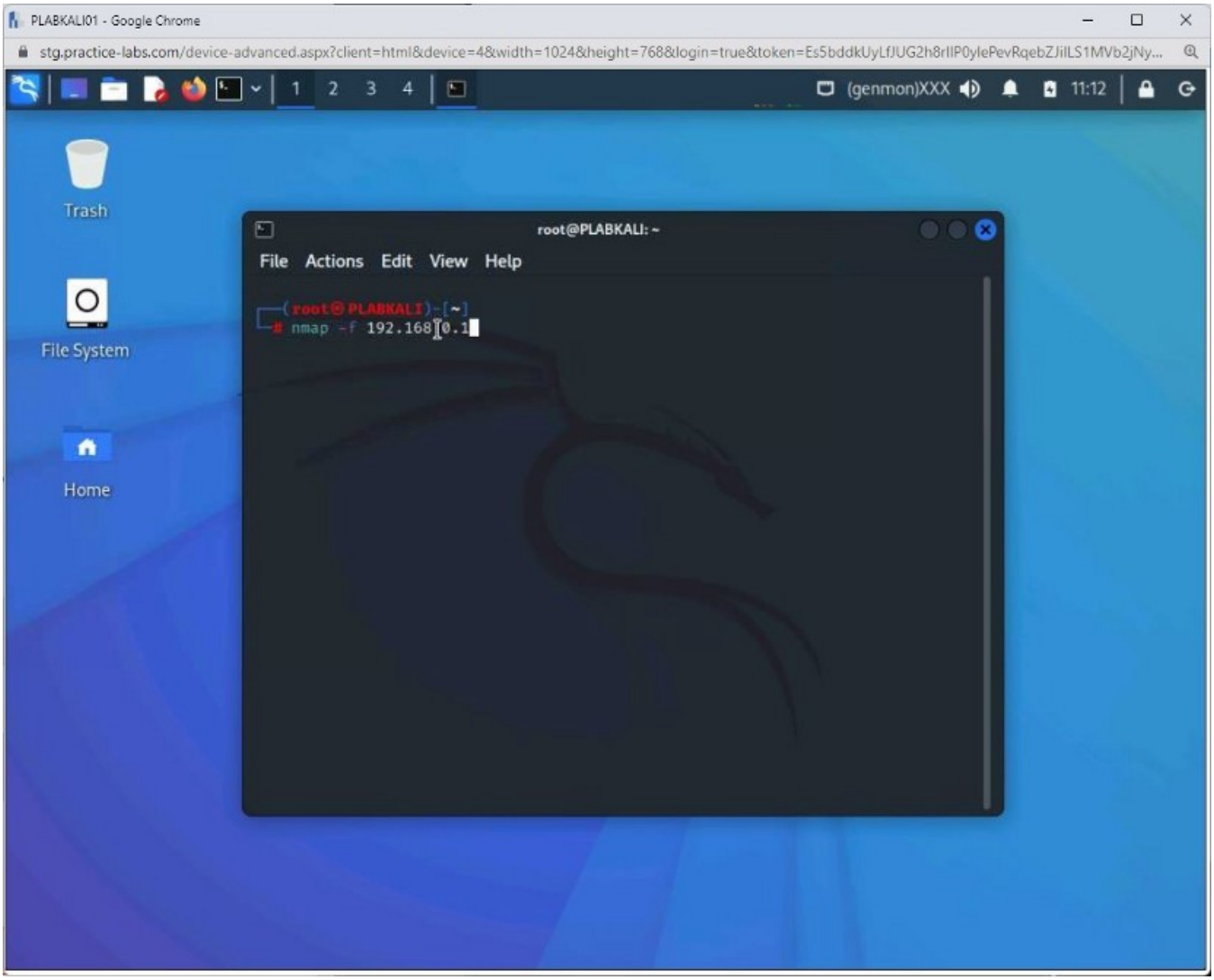
```
clear
```

Now, let's try a fast scan, which will scan for the 100 common ports on a given system.

To do this, type the following command:

```
nmap -F 192.168.0.1
```

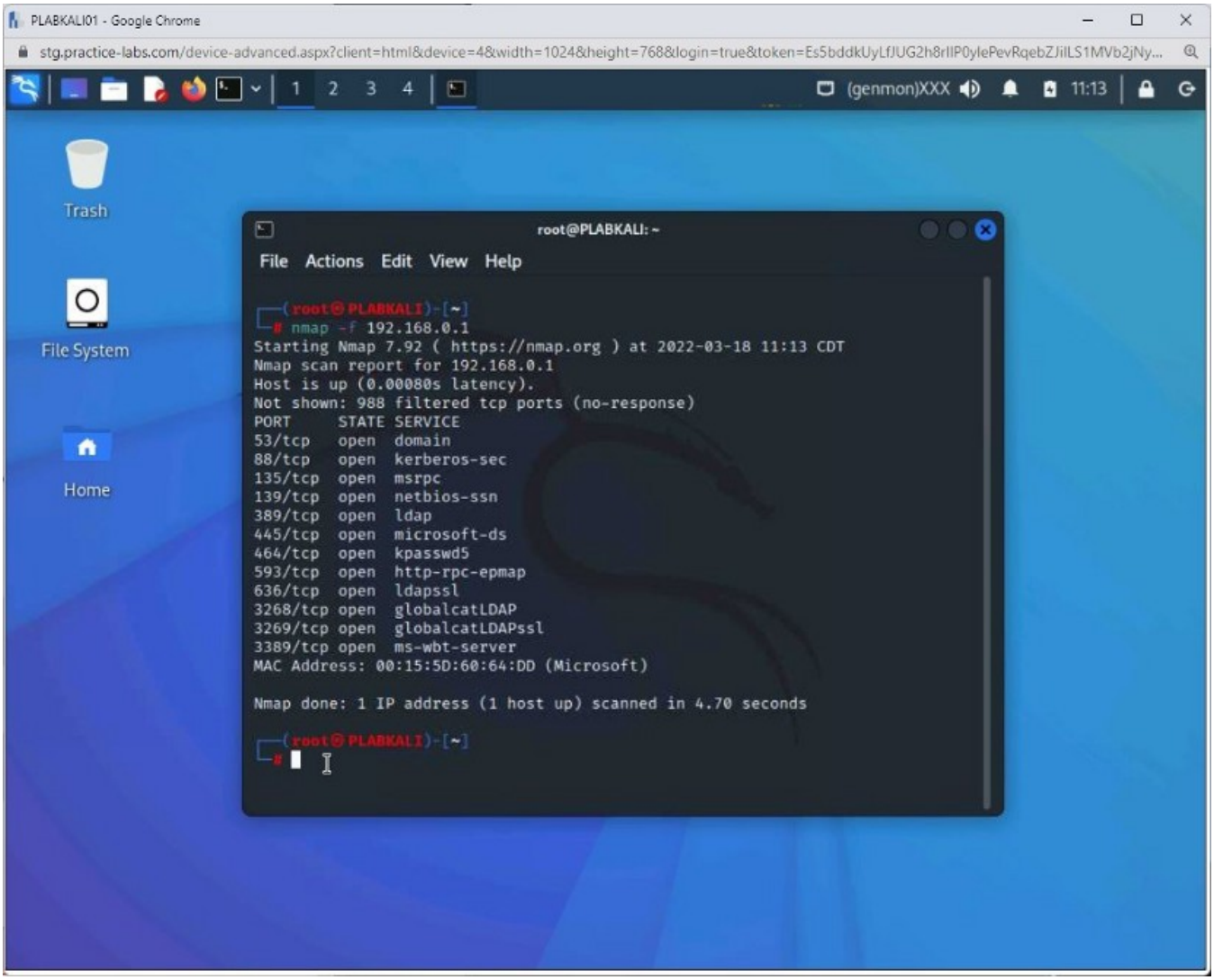
Press **Enter**.




**Step 8**

The output of this command is displayed — notice that the output of this command is different than the previous command.

It shows **92** filtered ports and **12** open ports. The output is different because the fast scan uses the **100** most common ports.




**Step 9**

Clear the screen by entering the following command:

```
clear
```

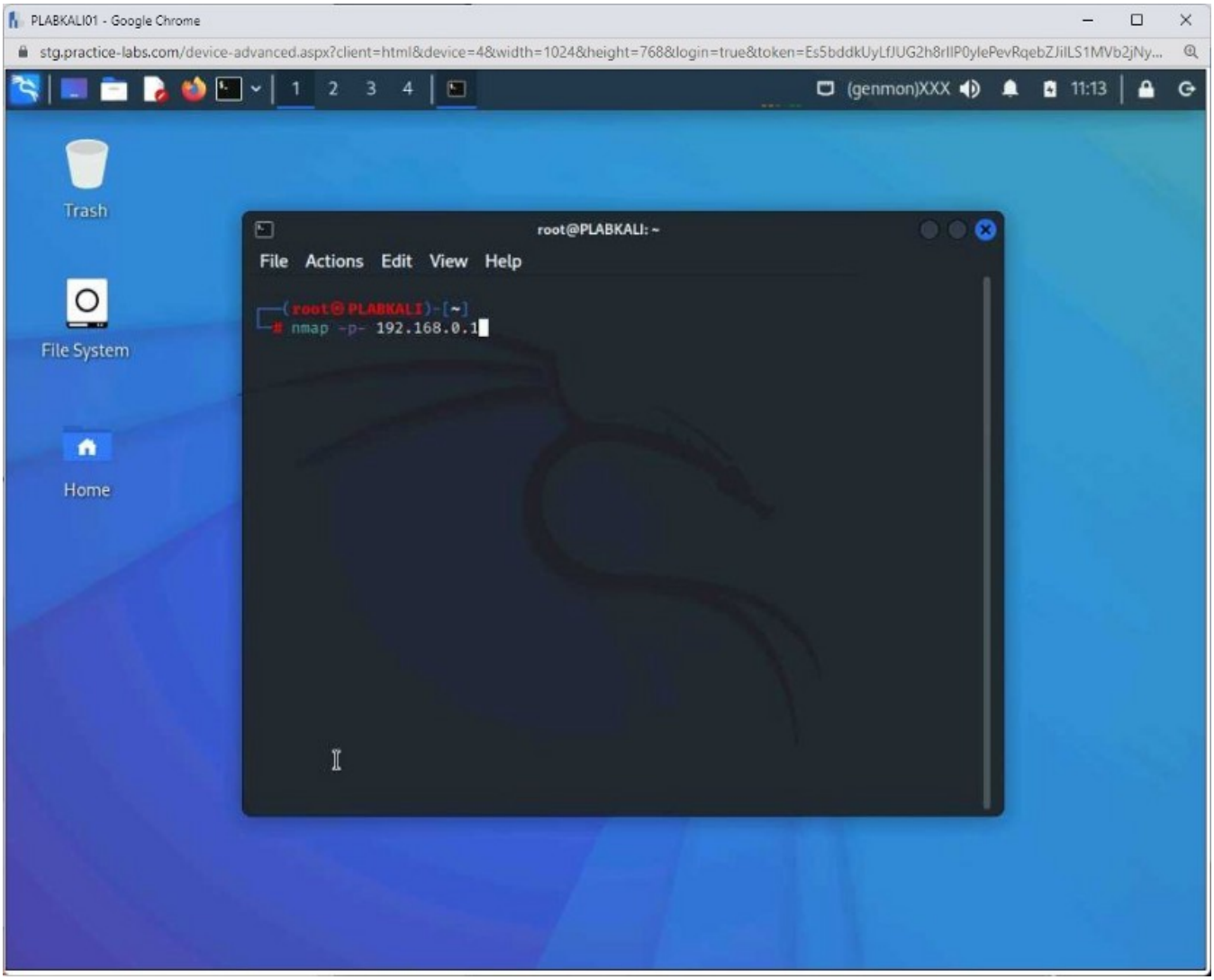
You will now scan for **65535** ports on a system.

To do this, type the following command:

```
nmap -p- 192.168.0.1
```

Press **Enter**.

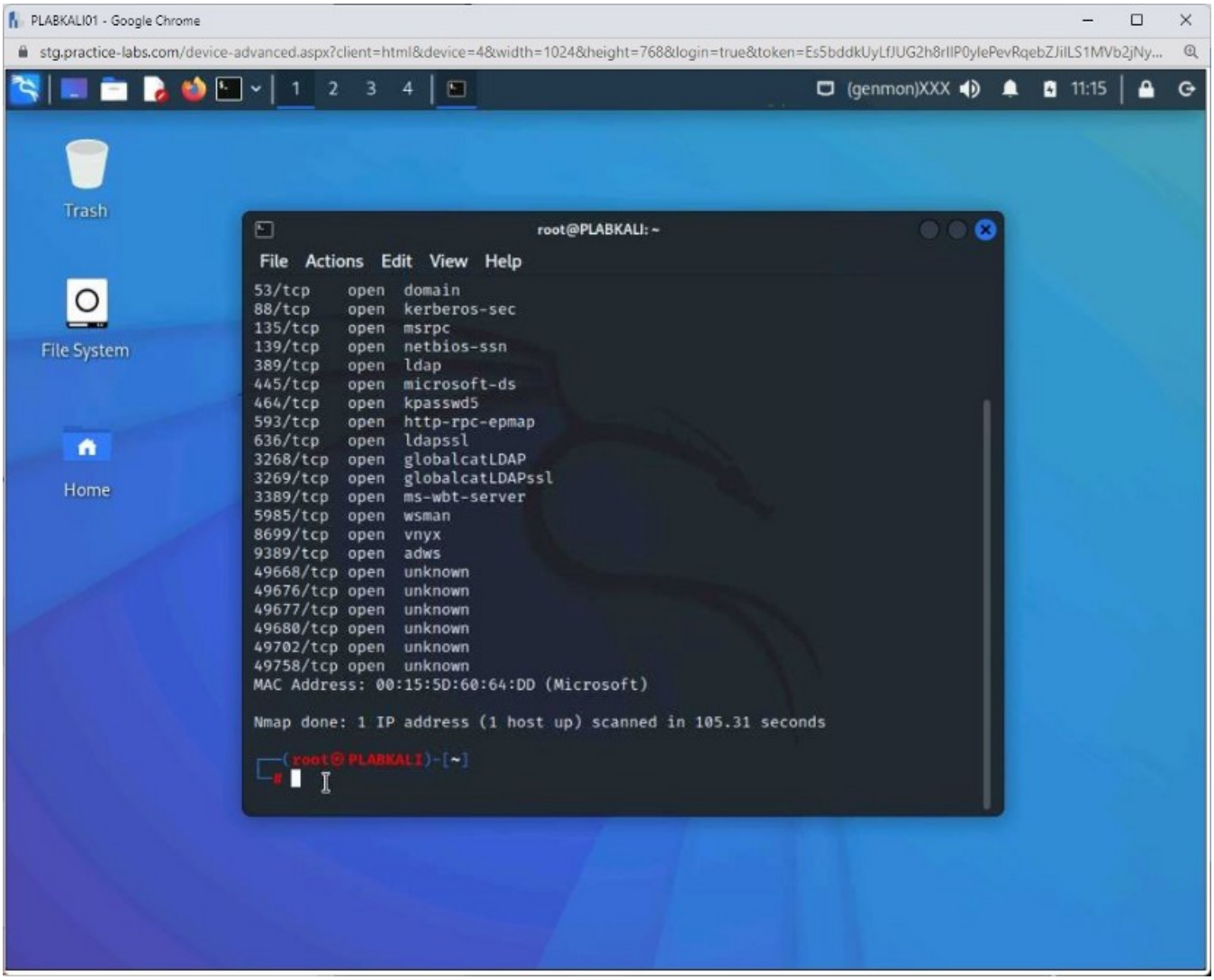
***Note:*** *This command will take a while to generate the output. Remember, it is scanning for 65535 ports on a system.*




**Step 10**

The output of this command is displayed.

Note that the output and found several ports open on the domain controller, **192.168.0.1**.




**Step 11**

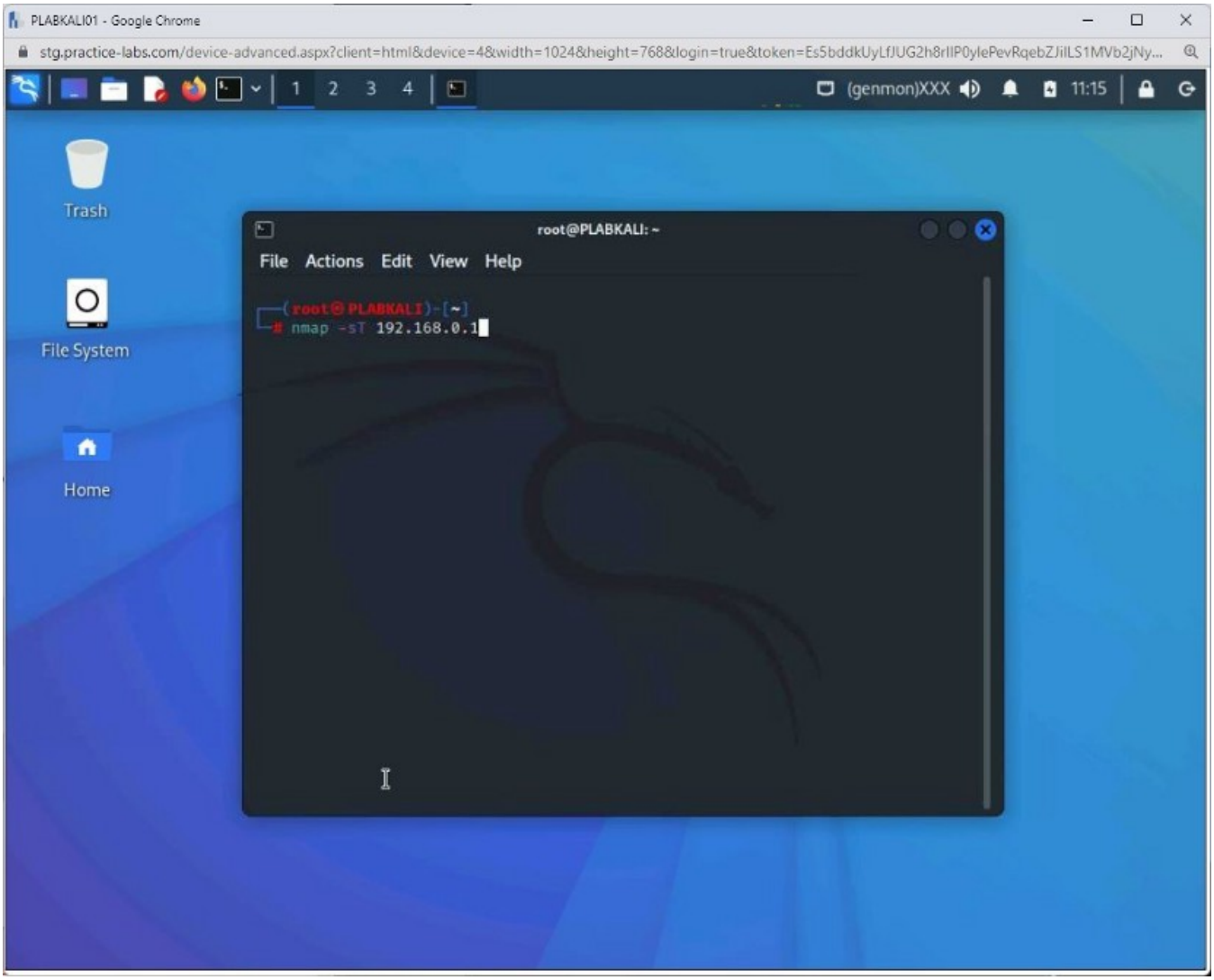
Clear the screen by entering the following command:

```
clear
```

Next, you will perform port scanning using **TCP** connect scan with the **-sT** parameter. Type the following command:

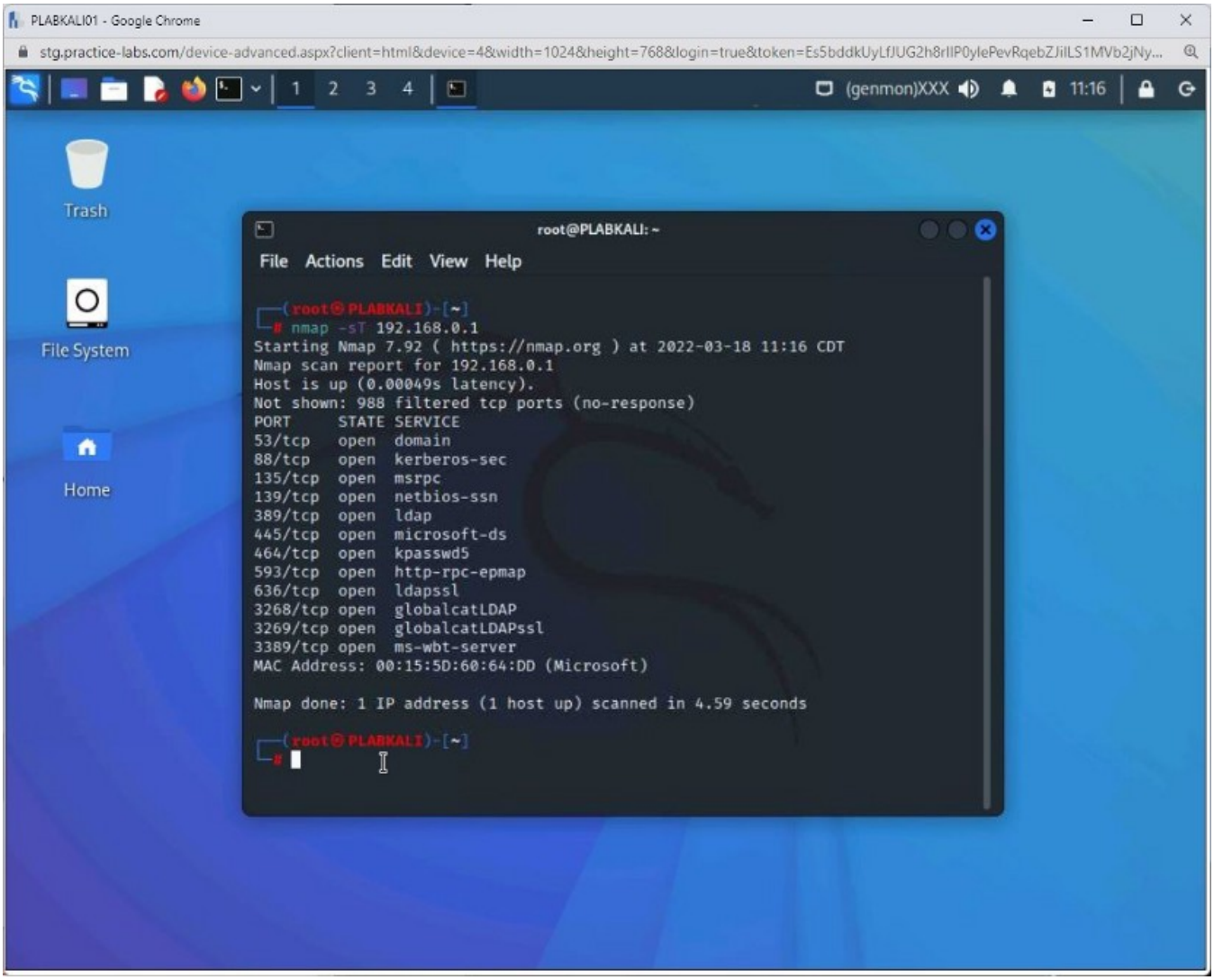
```
nmap -sT 192.168.0.1
```

Press **Enter**.




**Step 12**

Notice the output. This command has scanned **1000** ports. There are **988** filtered and **12** open ports.




**Step 13**

Clear the screen by entering the following command:

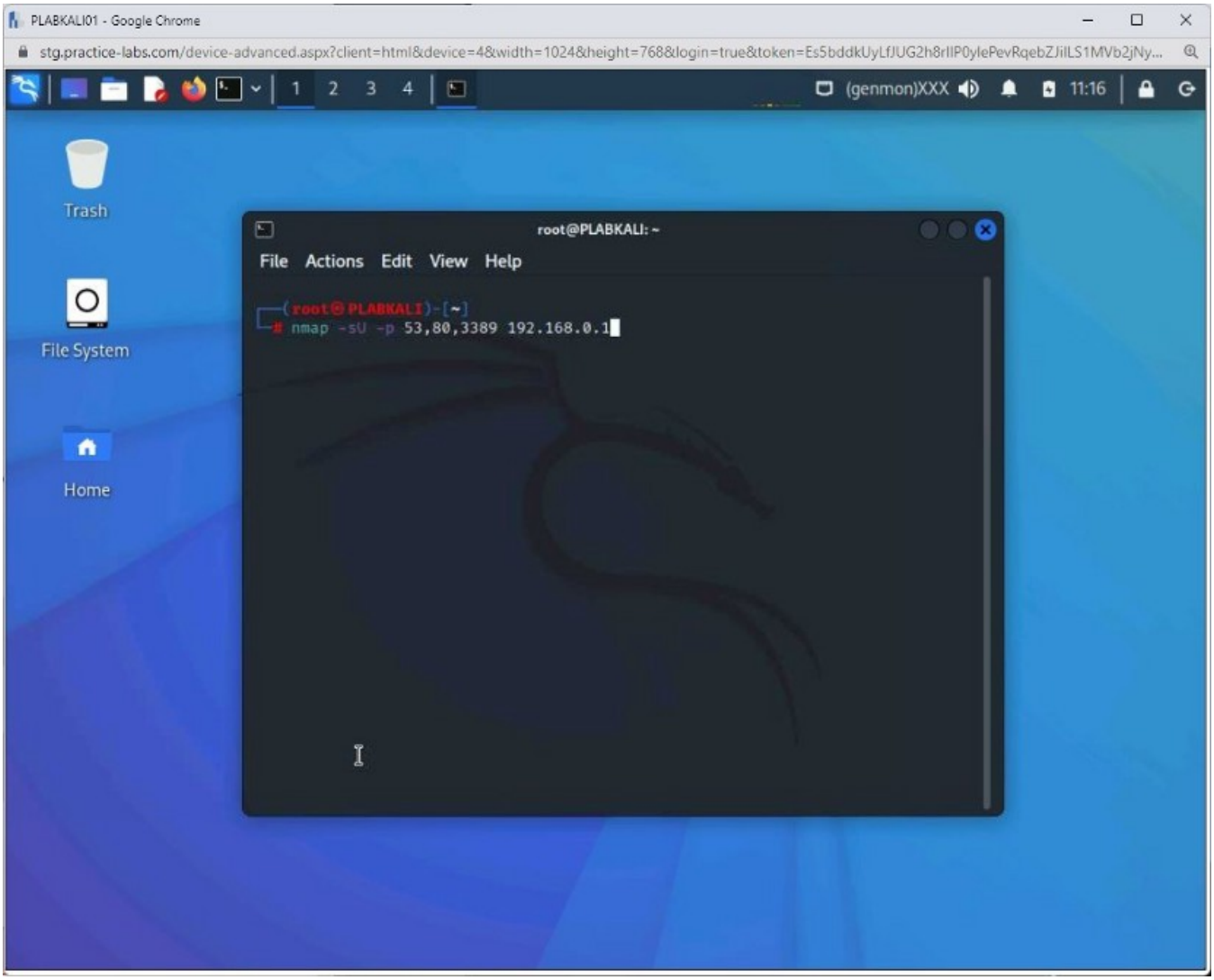
```
clear
```

Let's scan for the selective **UDP** ports only. Type the following command:

```
nmap -sU -p 53,80,3389 192.168.0.1
```

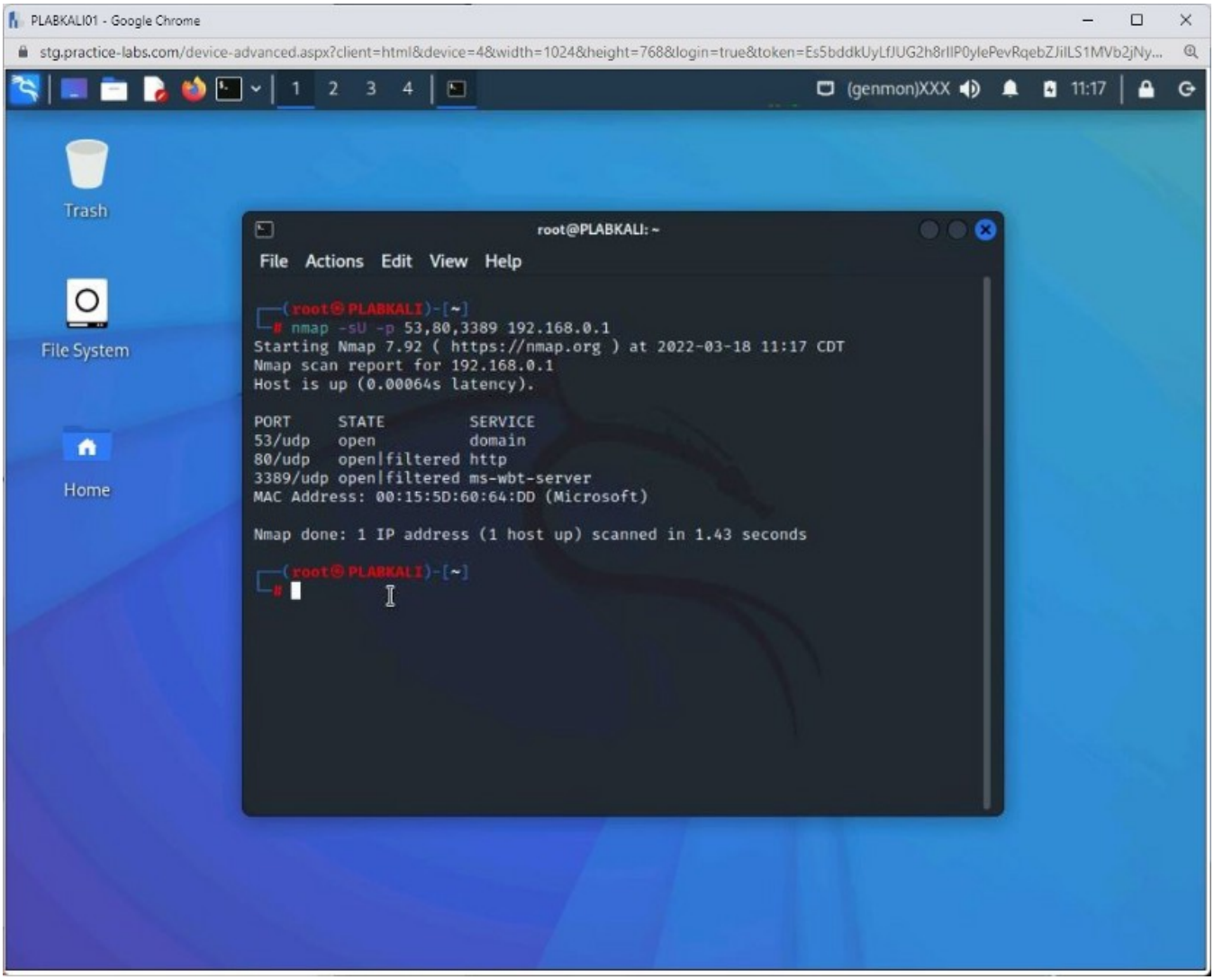
Press **Enter**.

***Note:*** *Do not type a space after the comma when listing the ports, as Nmap considers it the IP address and will attempt to find the route to the port number.*




**Step 14**

The output of this command is displayed. Notice that all three ports are open.




**Step 15**

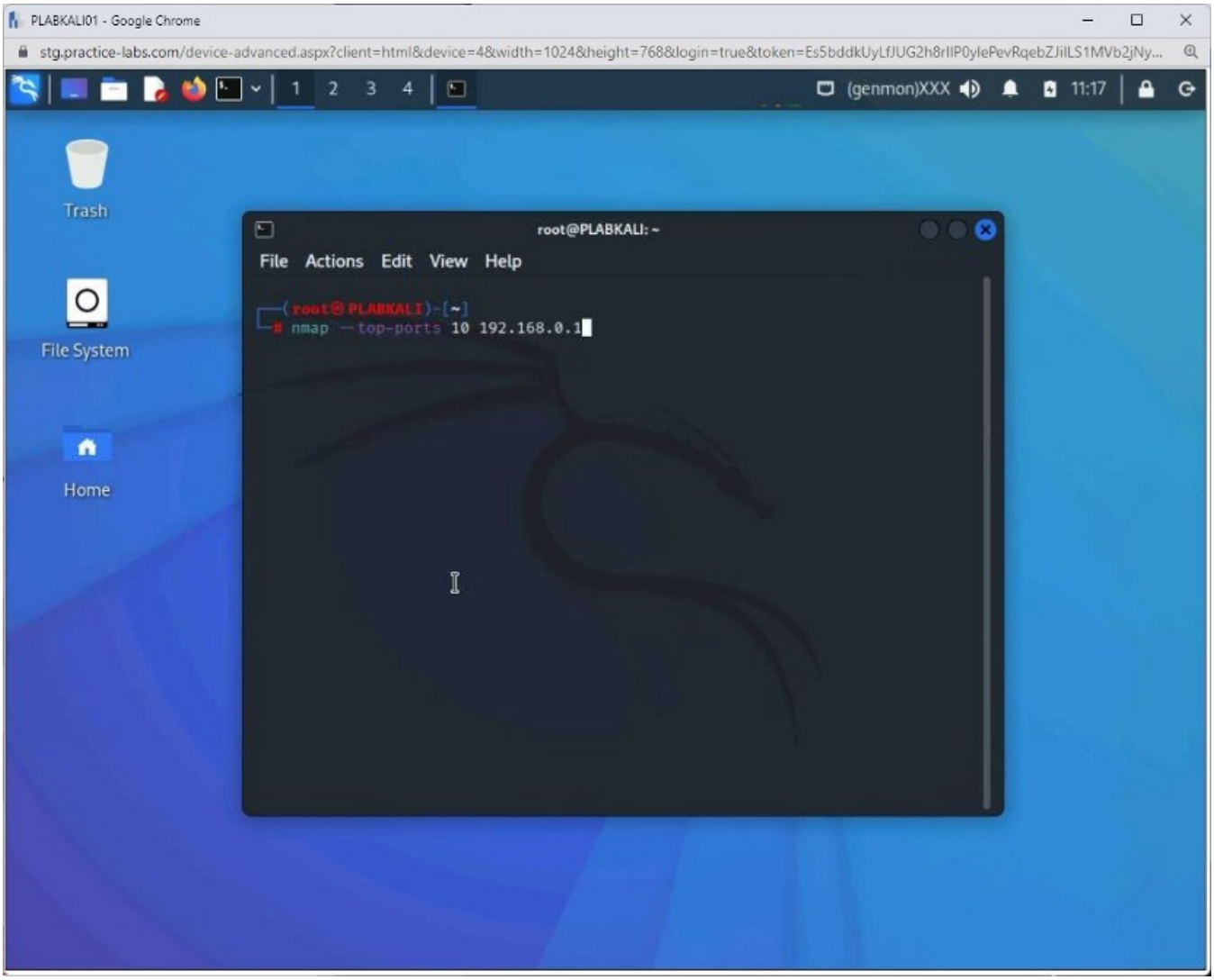
Clear the screen by entering the following command:

```
clear
```

You can also use the — — **top-ports** parameter with a specified number to find ports. To do this, type the following command:

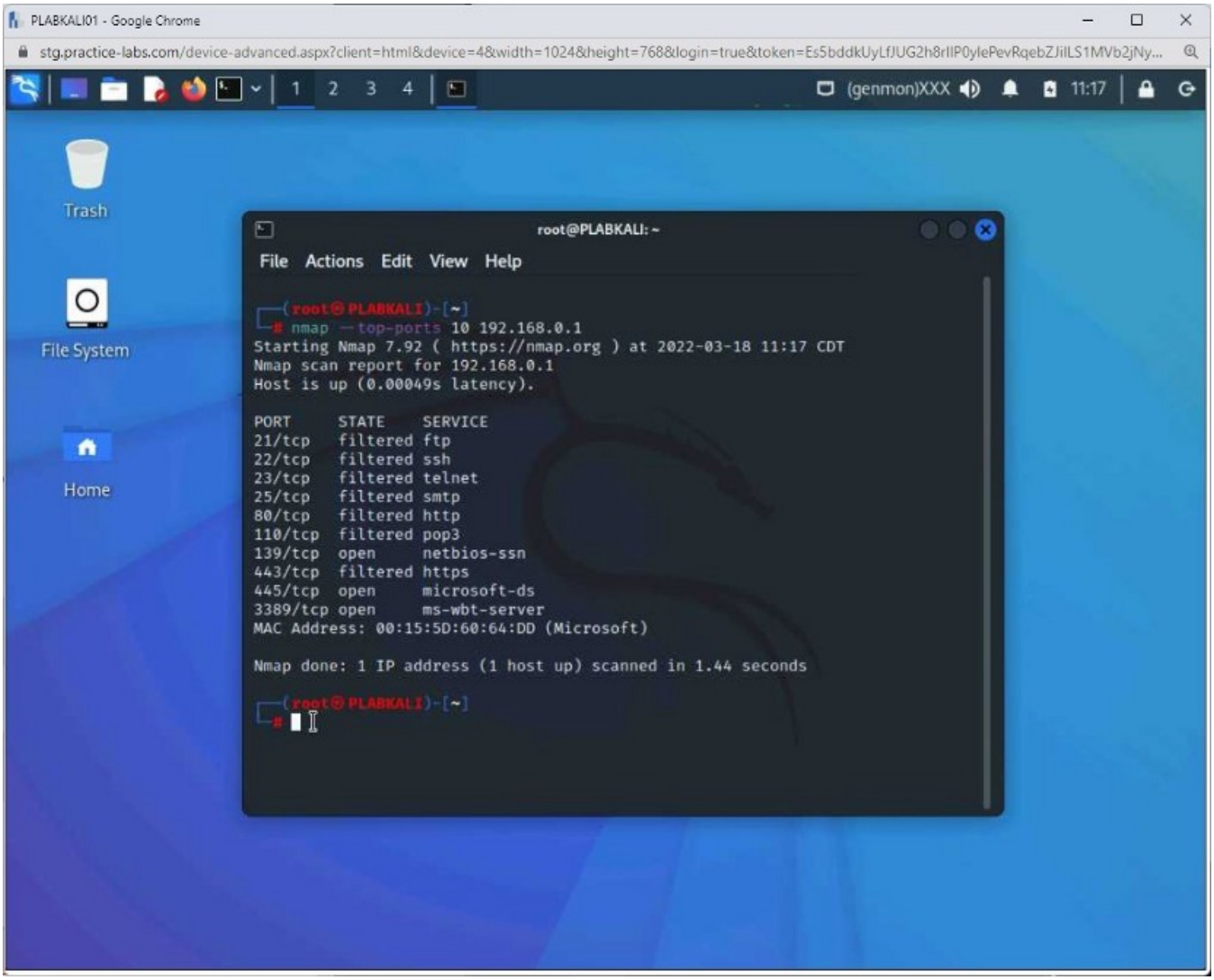
```
nmap --top-ports 10 192.168.0.1
```

Press **Enter**.




**Step 16**

Notice that the top 10 used ports are listed as the output with their current state.




Keep the terminal window open.

## Task 3 — Perform Service Probing

Using Nmap, you can find many details about the running services and their version numbers. In this task, you will learn about service probing.

To do this, perform the following steps:

### Step 1

Ensure that you are connected to **PLABKALI01** and open the terminal window.

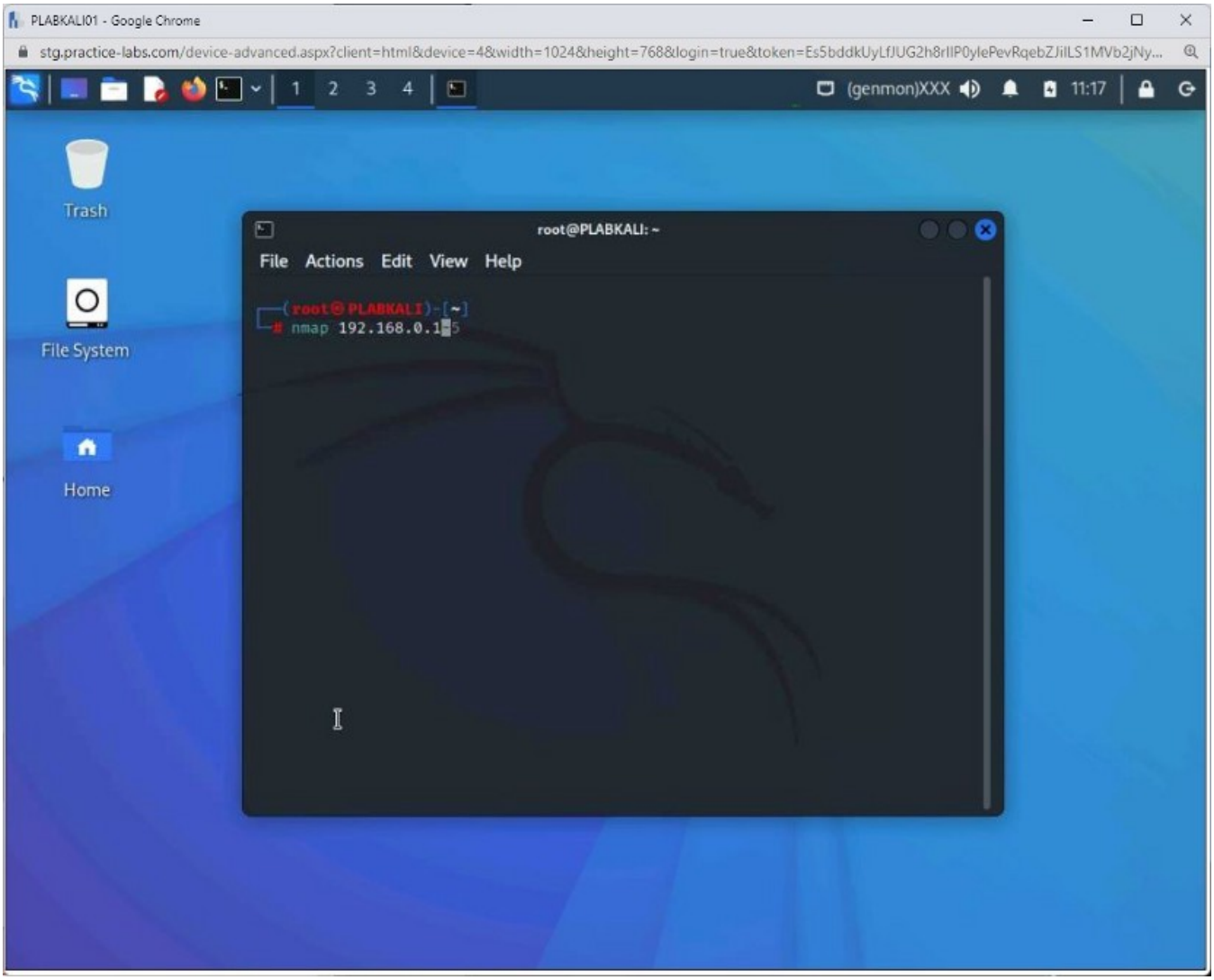
Clear the screen by entering the following command:

```
clear
```

Let’s check the ports open on a system.

```
nmap 192.168.0.1
```

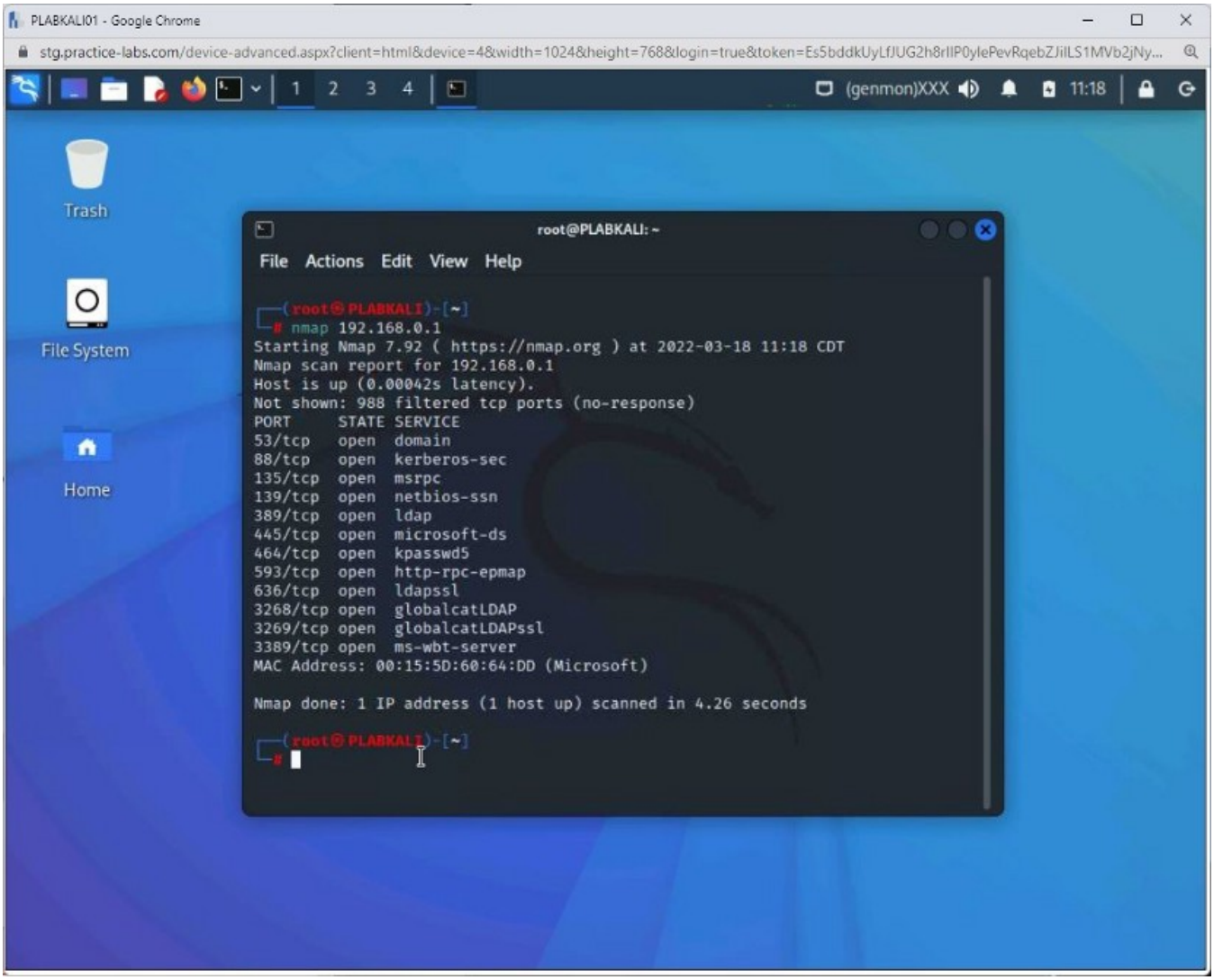
Press **Enter**.




### Step 2

Notice the output that displays several open ports on **192.168.0.1**.

Along with the ports, the services are also mentioned.




**Step 3**

Clear the screen by entering the following command:

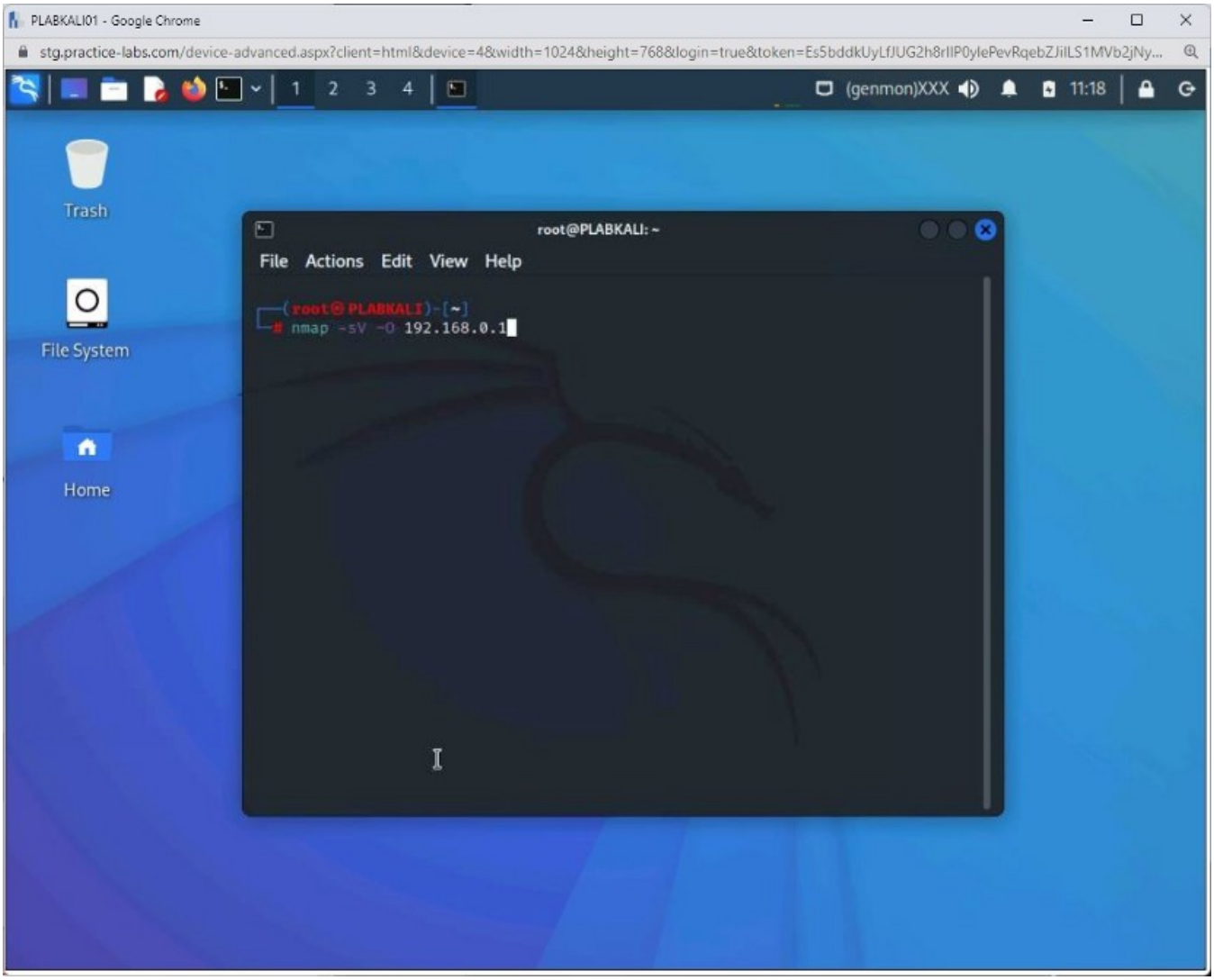
```
clear
```

Next, let's check the services version on the open ports on **192.168.0.1**.

Type the following command:

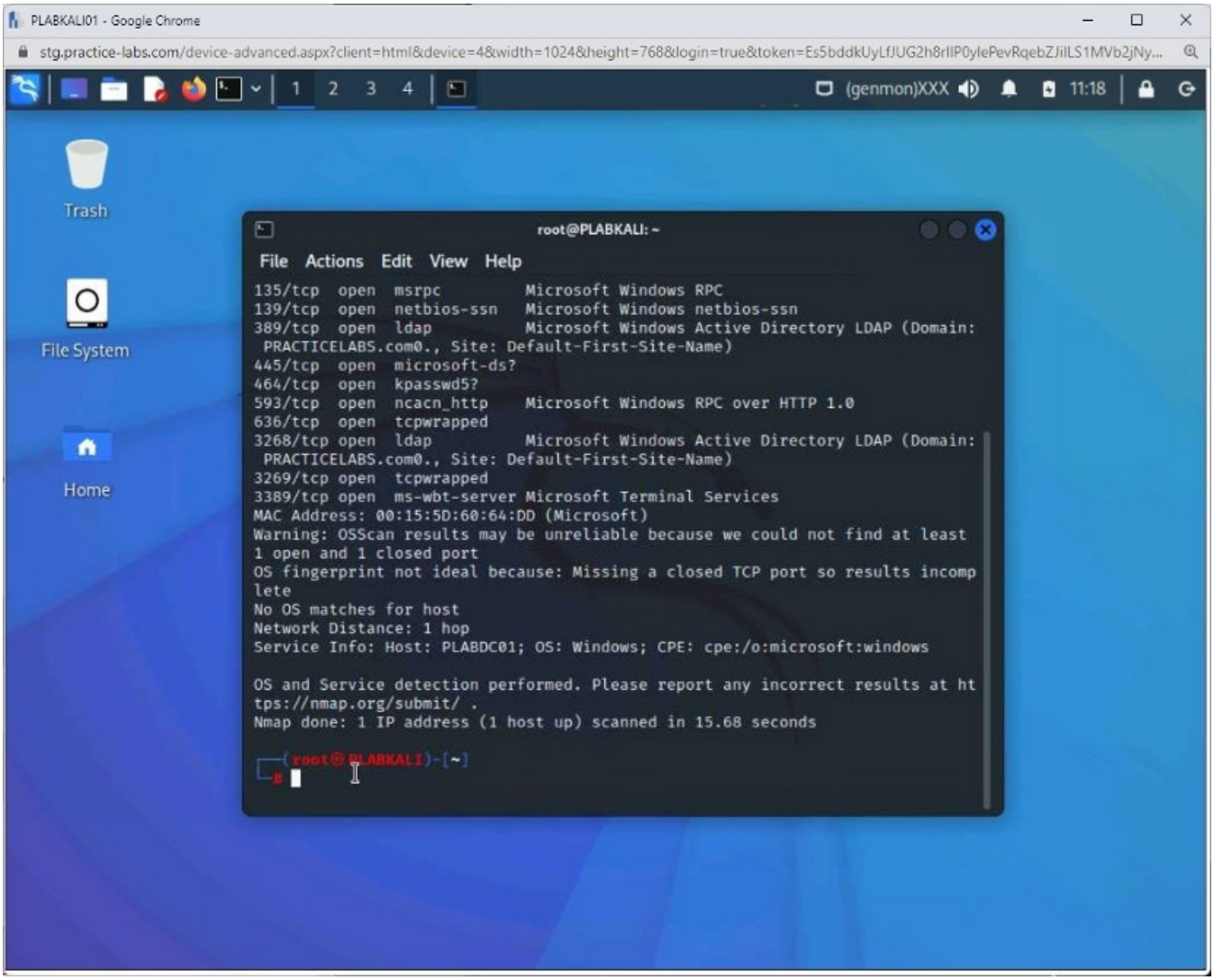
```
nmap -sV -O 192.168.0.1
```

Press **Enter**.




**Step 4**

The output displays the version number of most of the services. Close the command prompt window.




Keep the terminal window open.

## Task 4 — Use Netcat for Port Scanning

Netcat, or nc, is a tool used to monitor network connections. The command is nc, which can also be used for port scanning.

In this task, you will use nc for port scanning. To do this, perform the following steps:

### Step 1

Ensure you have powered on the required devices and connect to **PLABKALI01**.

If you continue the previous task, the terminal window should be open. If not, then open a new terminal window.

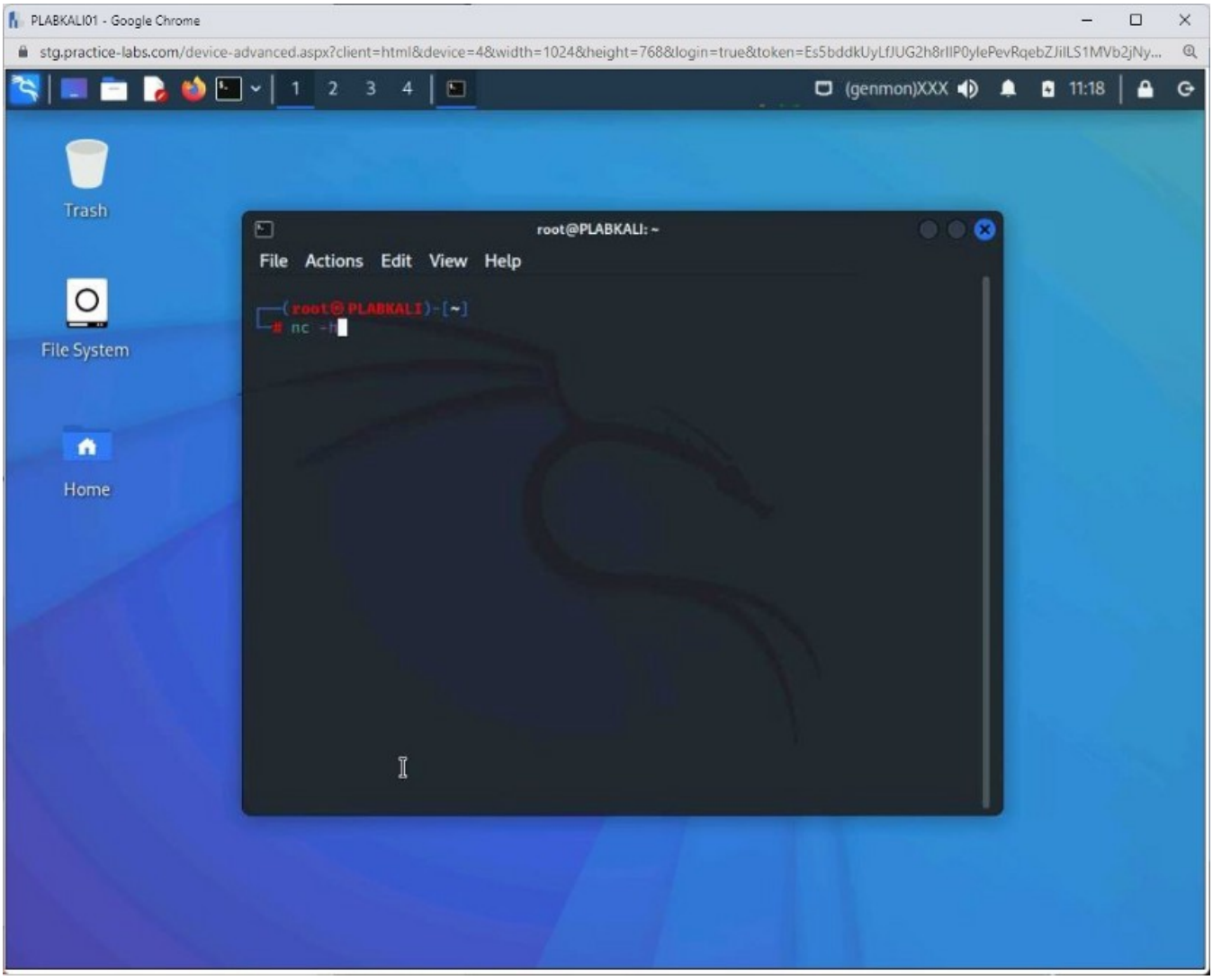
If continuing from the previous task, then clear the screen by entering the following command:

```
clear
```

To view the list of parameters of the **nc** command, type the following command:

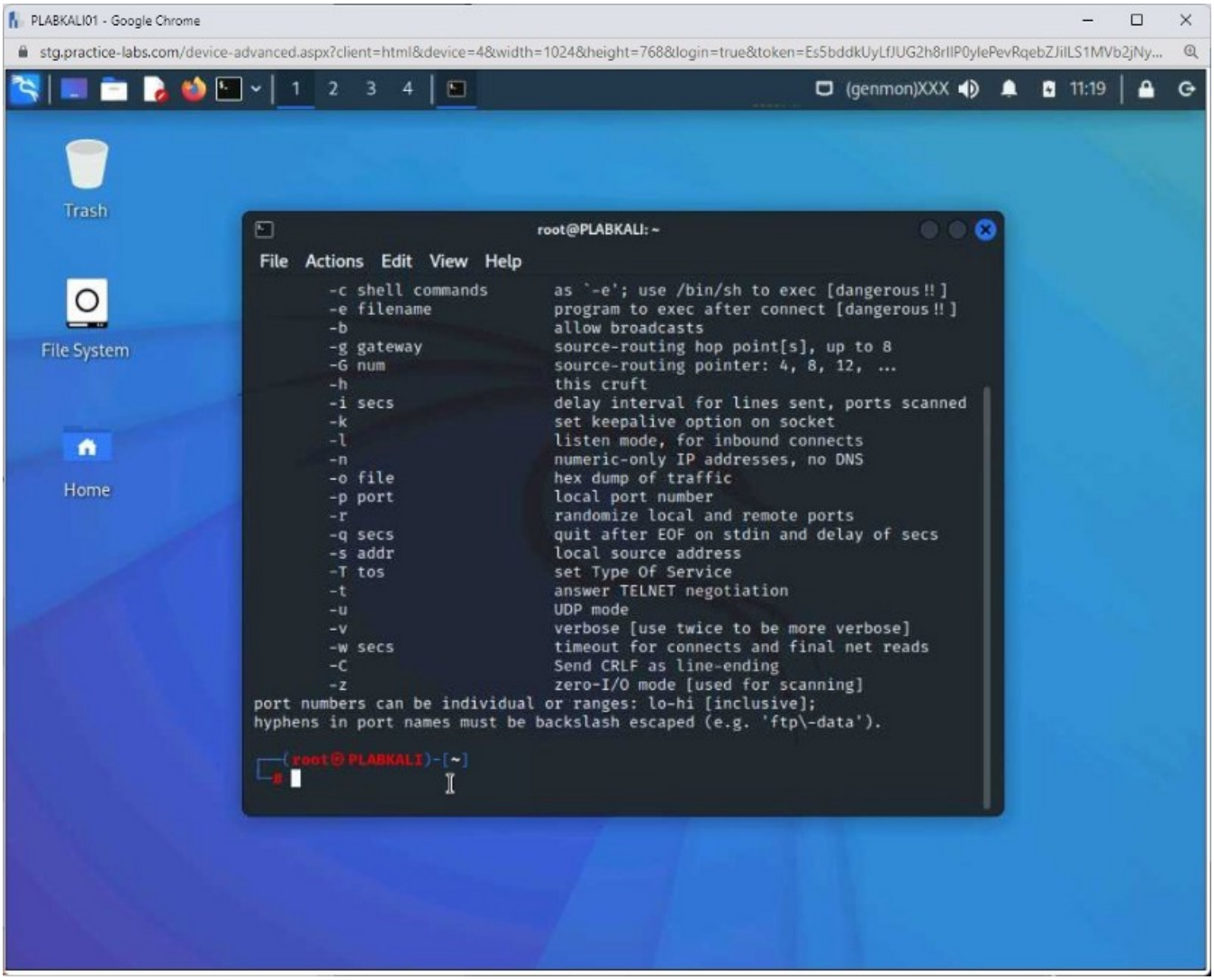
```
nc -h
```

Press **Enter**.




### Step 2

The output of the **nc -h** command is displayed.




**Step 3**

Clear the screen by entering the following command:

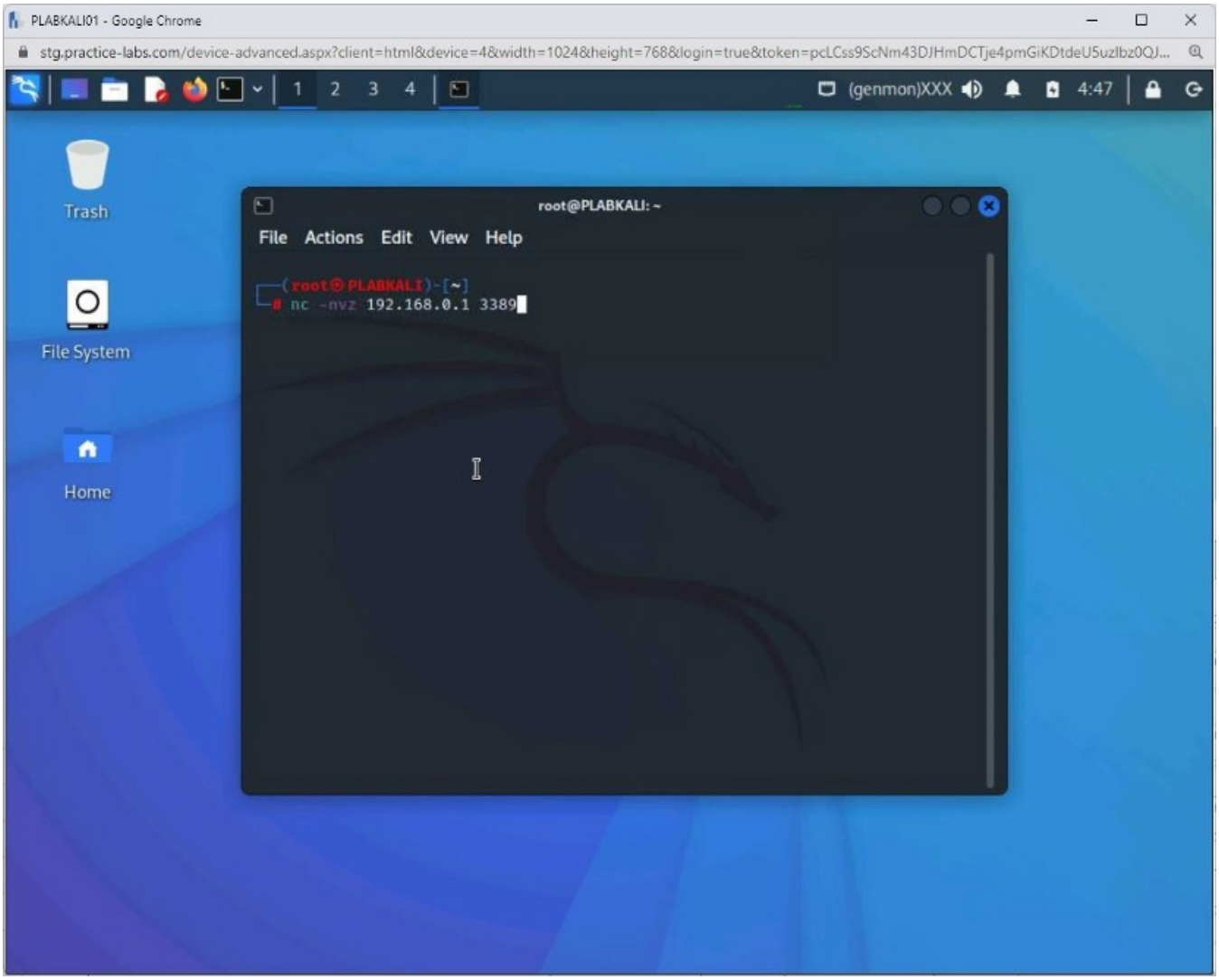
```
clear
```

To scan for a specific port, type the following command:

***Note:*** *The -n parameter states that an IP address will be used. The -z parameter is used for scanning. The -v parameter is used for verbose output.*

```
nc -nvz 192.168.0.1 3389
```

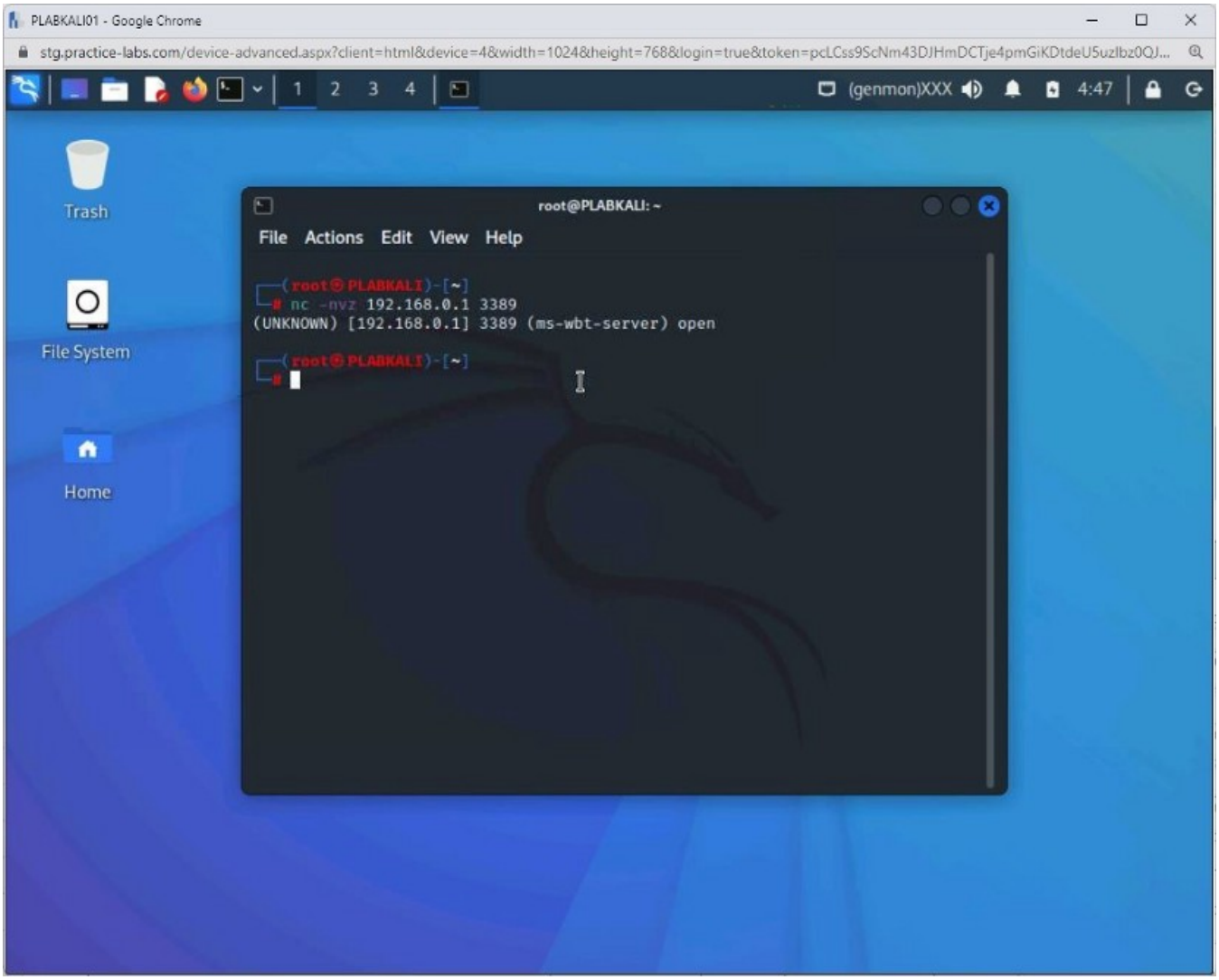
Press **Enter**.




**Step 4**

The output of the **nc** command is displayed.

It confirms that port **3389** is open.




## Review

Well done, you have completed the **Network Resource Discovery Methods — Part 1** CertMaster Lab.

## Learning Outcomes Part 2

In this module, you will complete the following exercises:

- Exercise 1 — OS Discovery (Banner Grabbing / OS Fingerprinting)
- Exercise 2 — Scanning Beyond IDS and Firewall
- Exercise 3 — Draw Network Topologies

After completing this module, you will be able to:

- Perform Banner Grabbing Using ID Serve
- Perform Active Fingerprinting an Operating System

- Perform Passive Fingerprinting an Operating System
- Perform Scan Using Packet Fragmentation
- Perform Source Port Manipulation
- Draw Network Topologies using The Dude

### Lab Duration

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

### Exercise 1 — OS Discovery (Banner Grabbing / OS Fingerprinting)

Attackers are keen to find the operating systems and their versions on servers and systems they want to exploit. Finding the operating systems and their versions is known as operating system fingerprinting. After the operating system and its version is determined, An attacker can find the vulnerabilities and exploit them.

In this exercise, you will learn about operating system discovery, including operating system banner grabbing and fingerprinting.

### Learning Outcomes

After completing this exercise, you will be able to:

- Perform Banner Grabbing Using ID Serve
- Perform Active Fingerprinting an Operating System
- Perform Passive Fingerprinting an Operating System

### 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 MemberWorkstation192.168.0.5/24PLABDM01Domain Member Server192.168.0.2/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABDM01

Windows Server 2019 — Domain Member192.168.0.2/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

## Task 1 — Perform Banner Grabbing Using ID Serve

It is important to know banner grabbing methods as an ethical hacker. ID Serve is one of the key tools used in banner grabbing. ID Serve can connect any of the server ports on any:

- Domain
- IP address

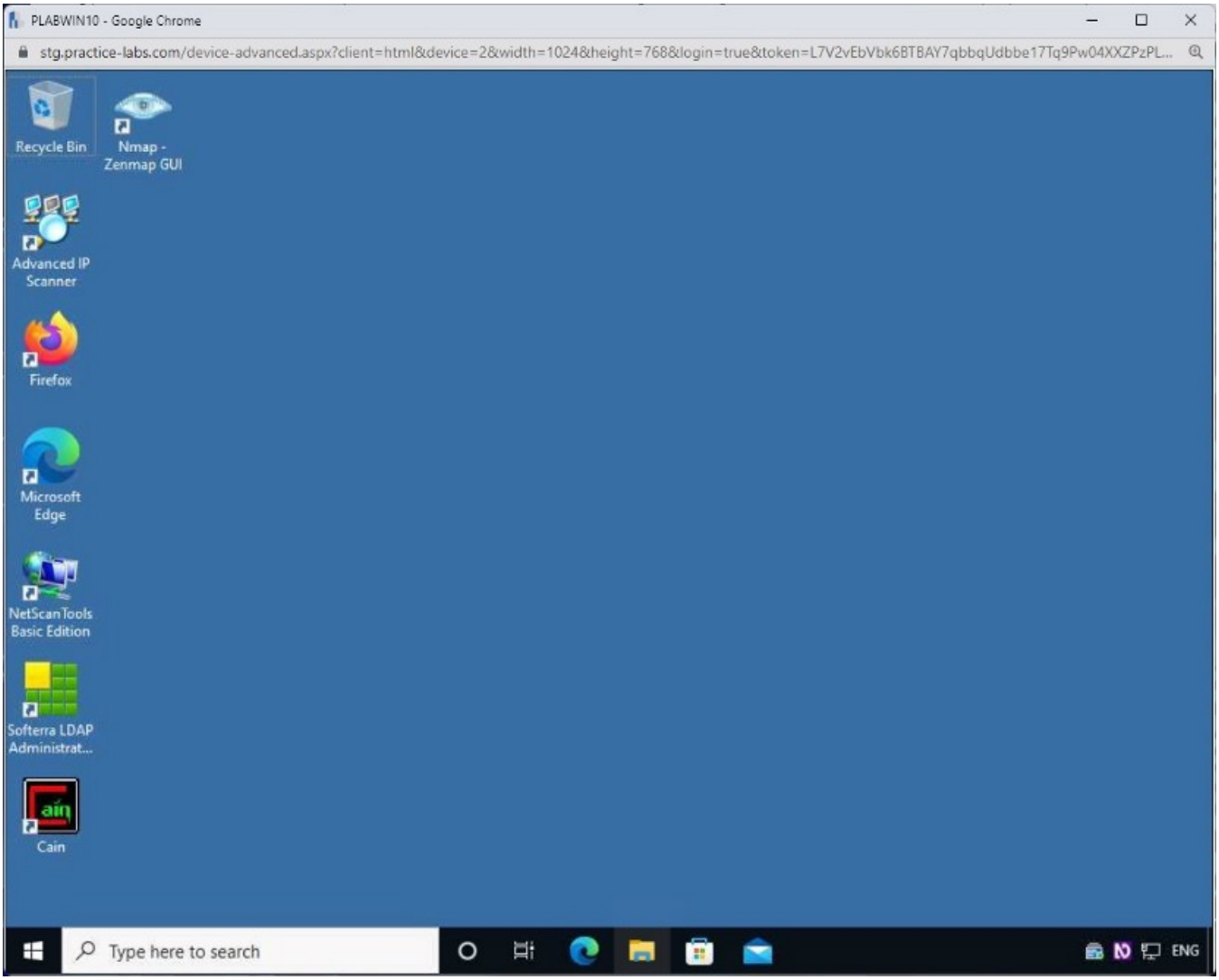
ID Serve can grab the server's greeting message, if any, along with the make and model. It can also grab the operating system information.

In this task, you will perform banner grabbing using ID Serve. To do this, perform the following steps:

#### Step 1

Ensure you have powered on the required devices and connect to **PLABWIN10**.

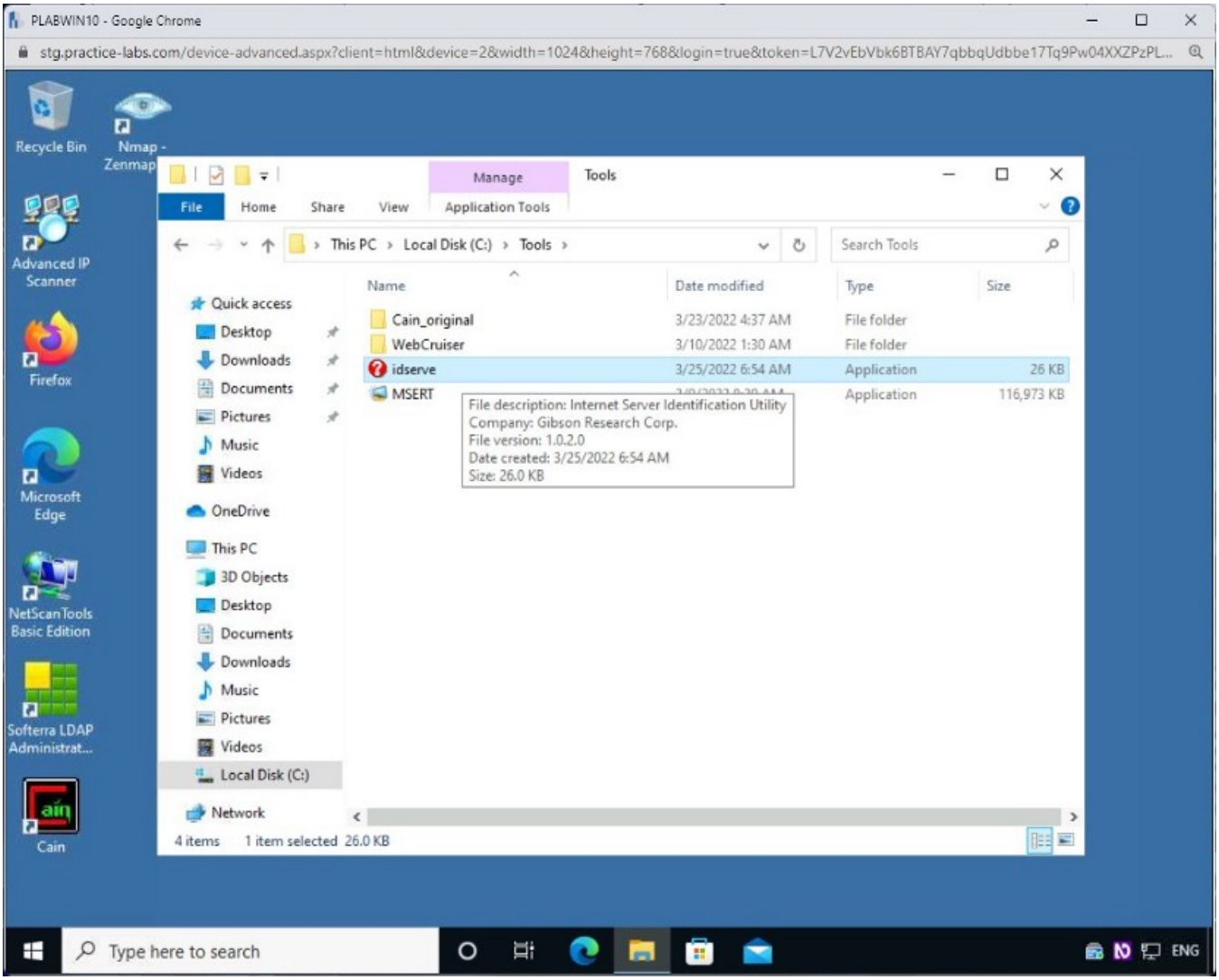
Open **File Explorer** by clicking the icon on the taskbar.




**Step 2**

In **File Explorer**, navigate to the **Local Disk** ©: > **Tools** folder.

Click on the **idserve** application.



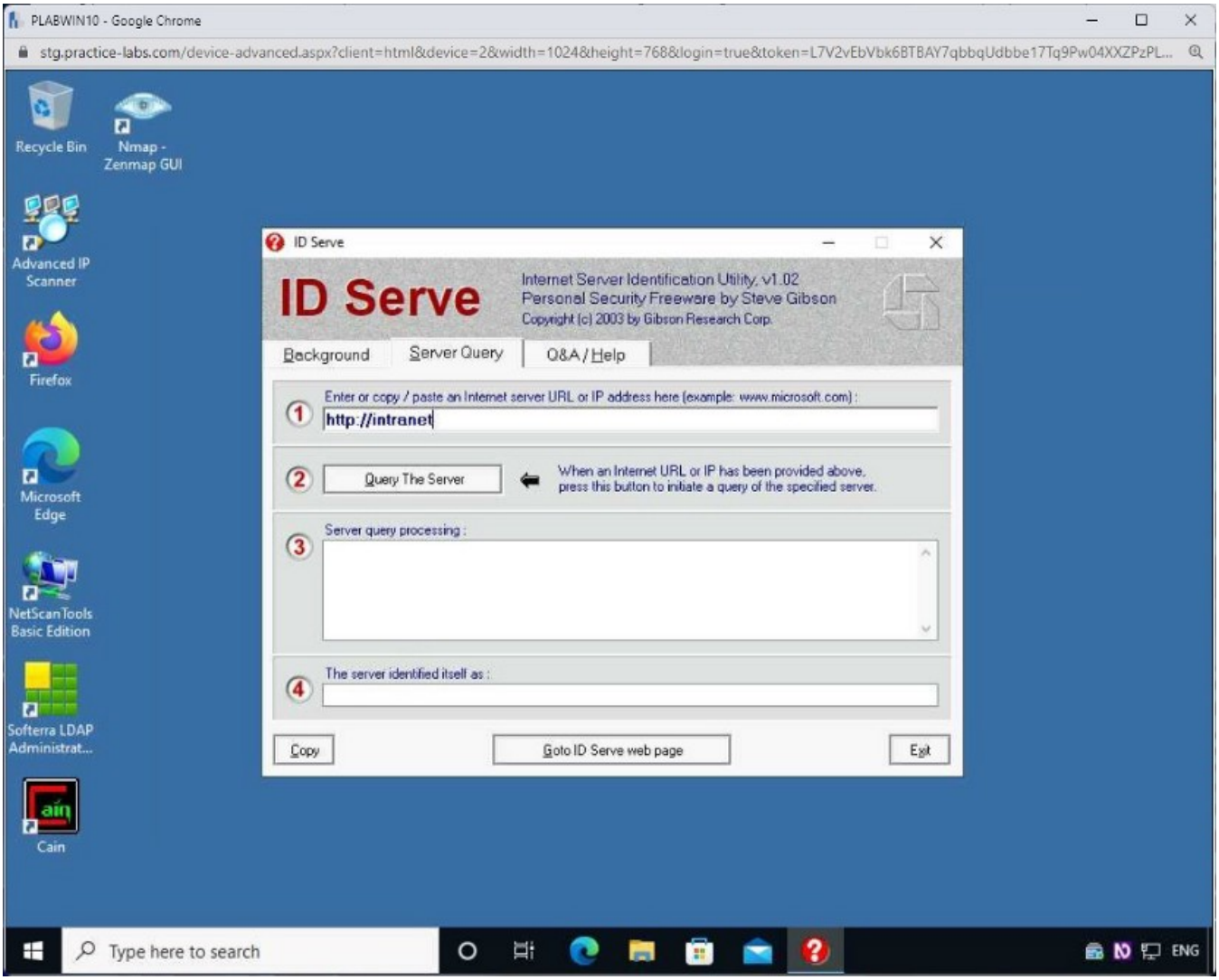

**Step 3**

Close **File Explorer**.

On the **Server Query** tab, type the following URL in the **Enter or copy/paste an Internet server URL or IP address here** text box:

```
http://intranet
```

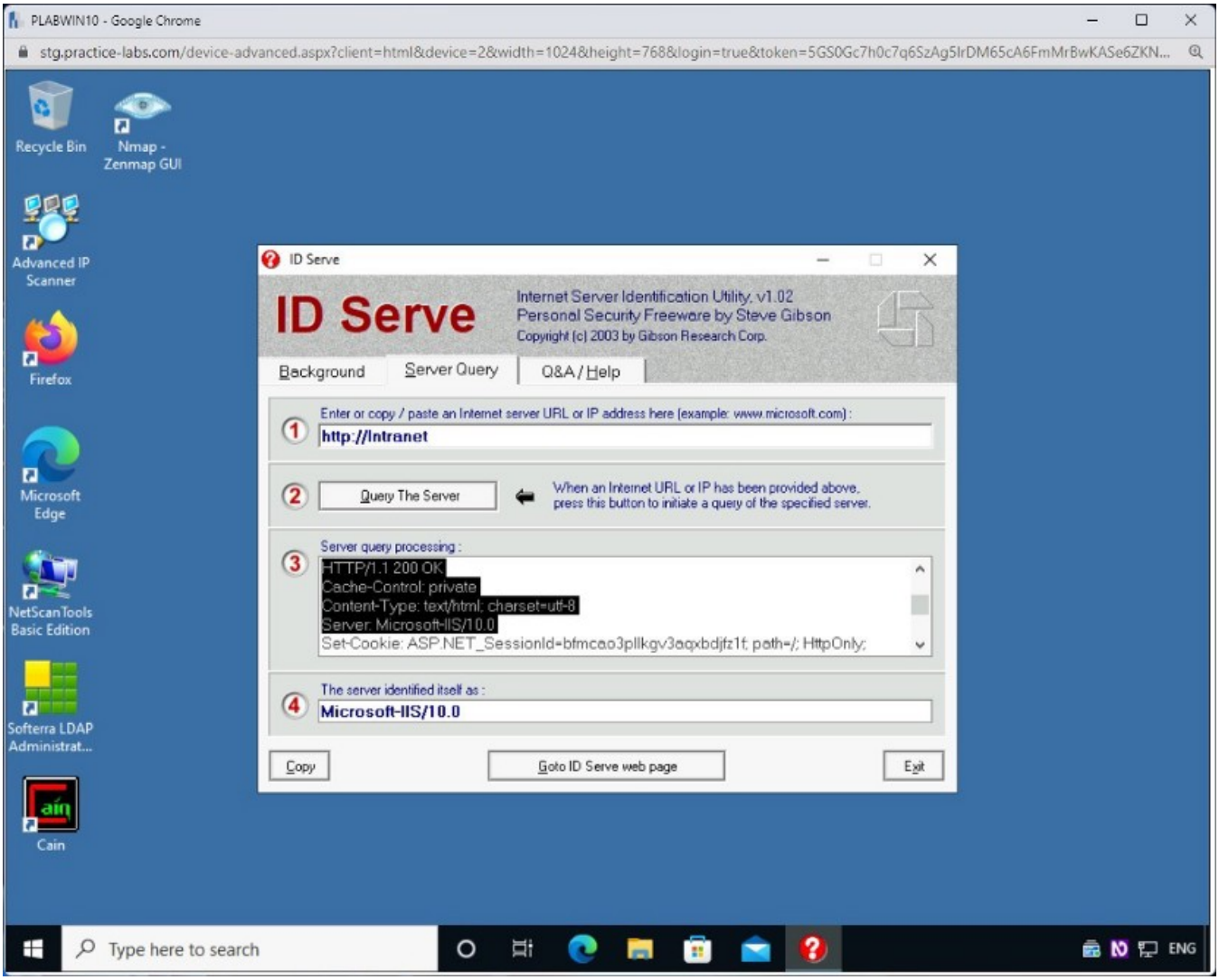
Click **Query The Server**.




**Step 4**

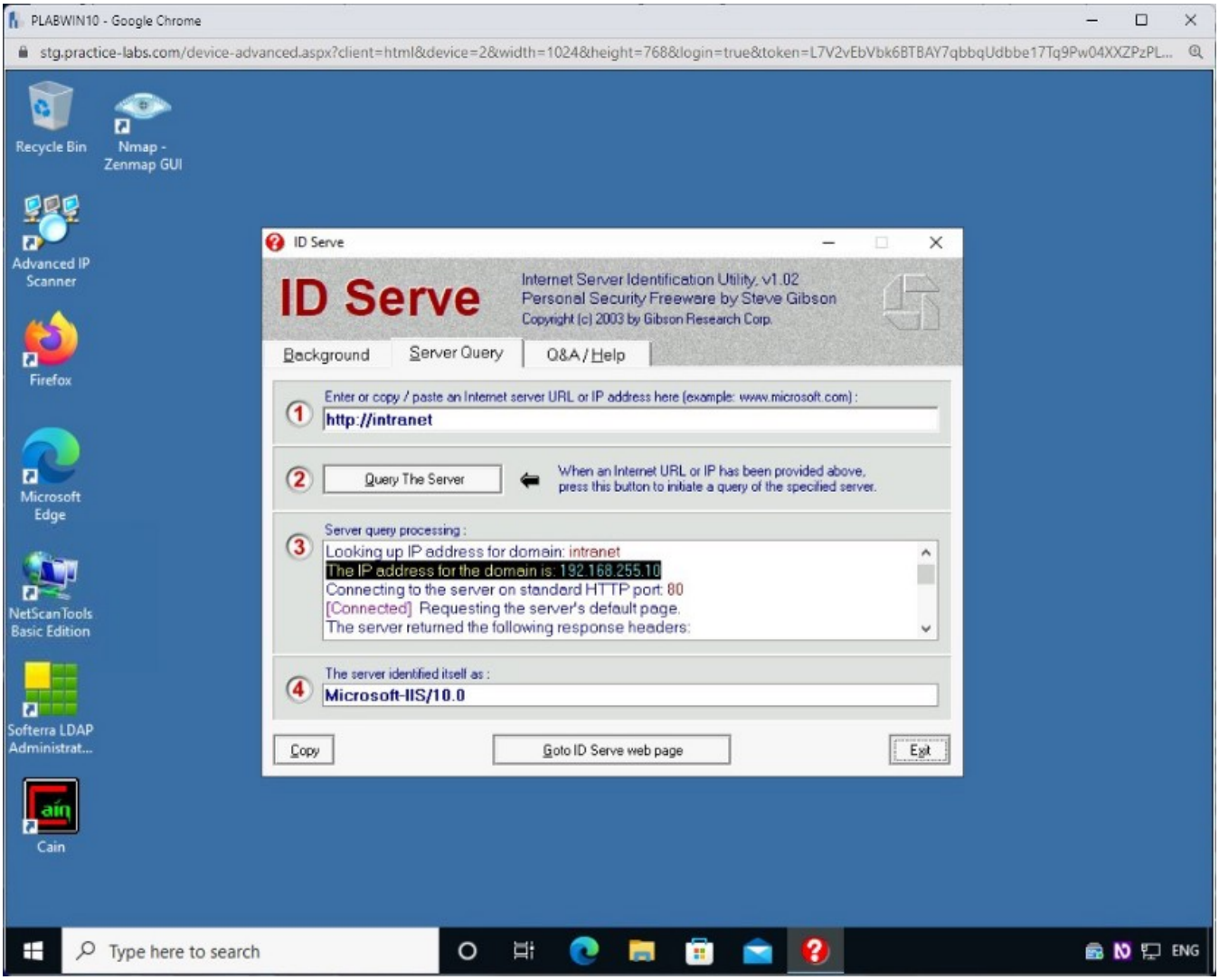
A lot of web server information is displayed.

You can scroll up and find the operating system and version of the Intranet web server.




### Step 5

Click **Exit** to close the **ID Serve** dialog box.




## Task 2 — Perform Active Fingerprinting on an Operating System

Operating system fingerprinting is also known as banner grabbing. With the help of fingerprinting, you can determine the type of operating system and its version on a remote system.

There are primarily two types of fingerprinting: Active and Passive.

You perform the Active fingerprinting using Nmap, which contains a list of the operating system. When you execute a command to determine the operating system of a remote host, packets are sent to the remote host, and the response is received, which is compared with the list of operating systems. Nmap then provides the closest match.

***Note:*** *In the next task, you will learn about passive operating system fingerprinting.*

In this task, you will learn to perform Active operating system fingerprinting.

### Step 1

Connect to **PLABKALI01**.

Log in using the following credentials:

**Username**:

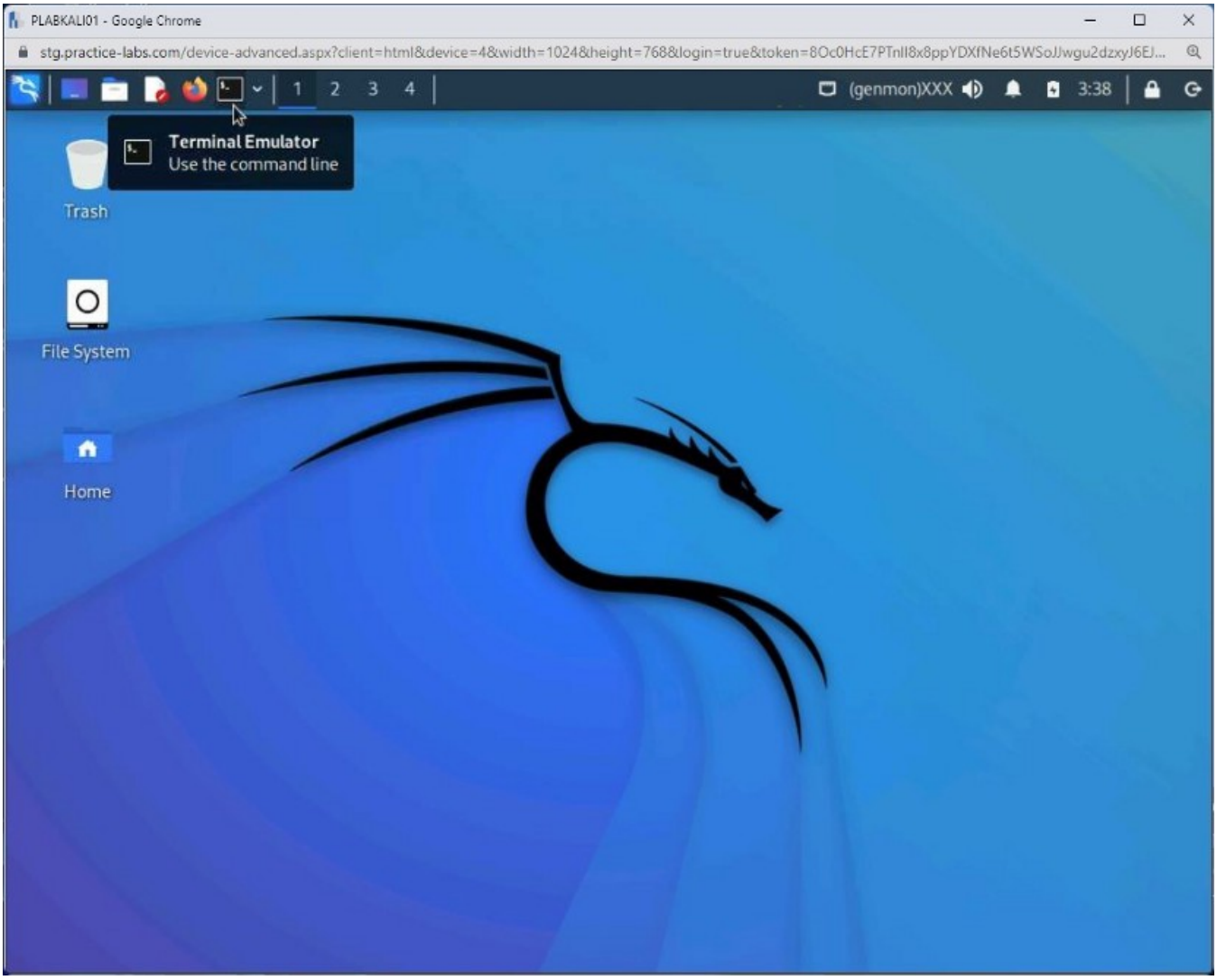
```
root
```

**Password**:

**Password**

The desktop of **PLABKALI01** is displayed.

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

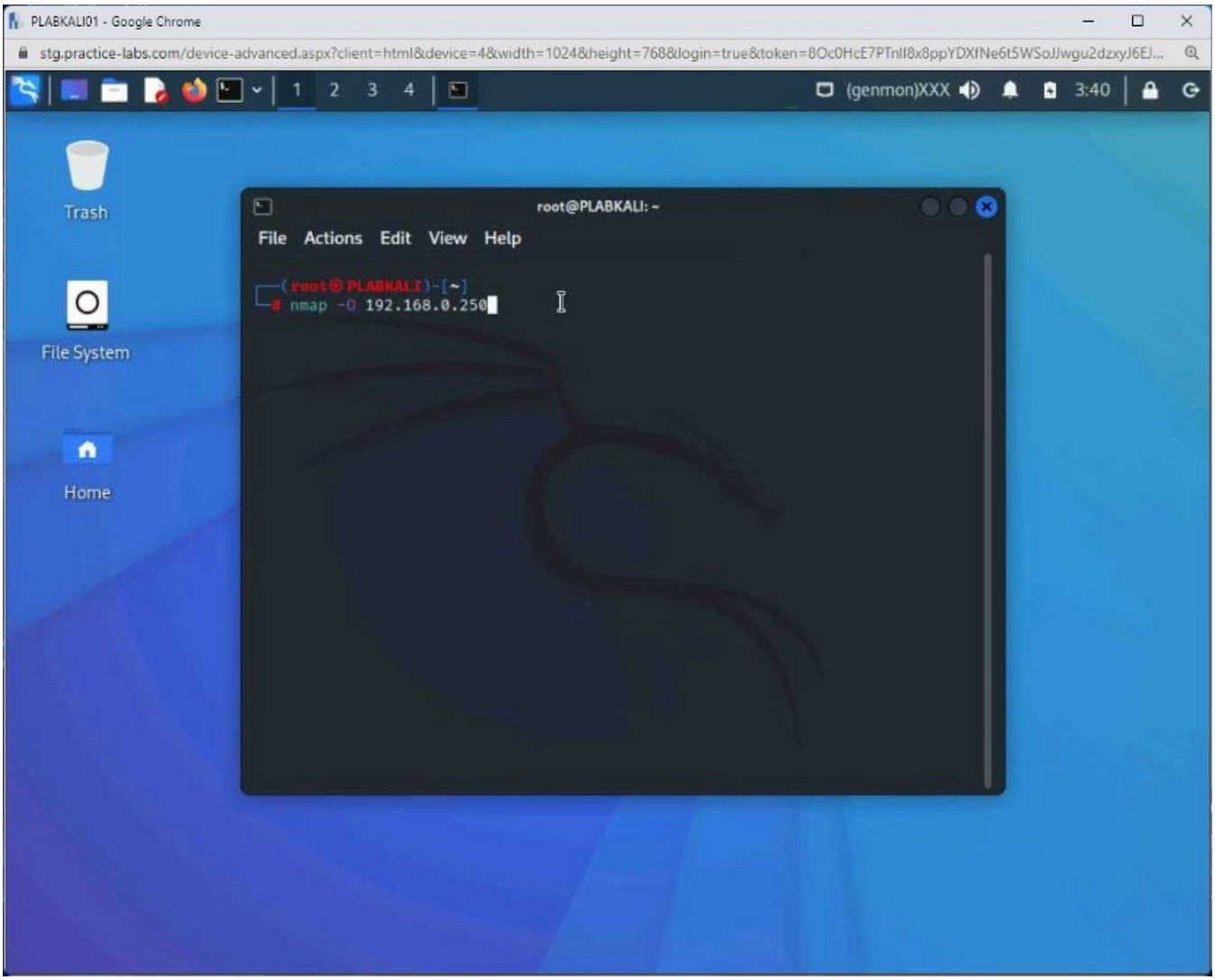



**Step 2**

To fingerprint a remote system with the **-O** parameter that performs the operating system detection. Type the following command:

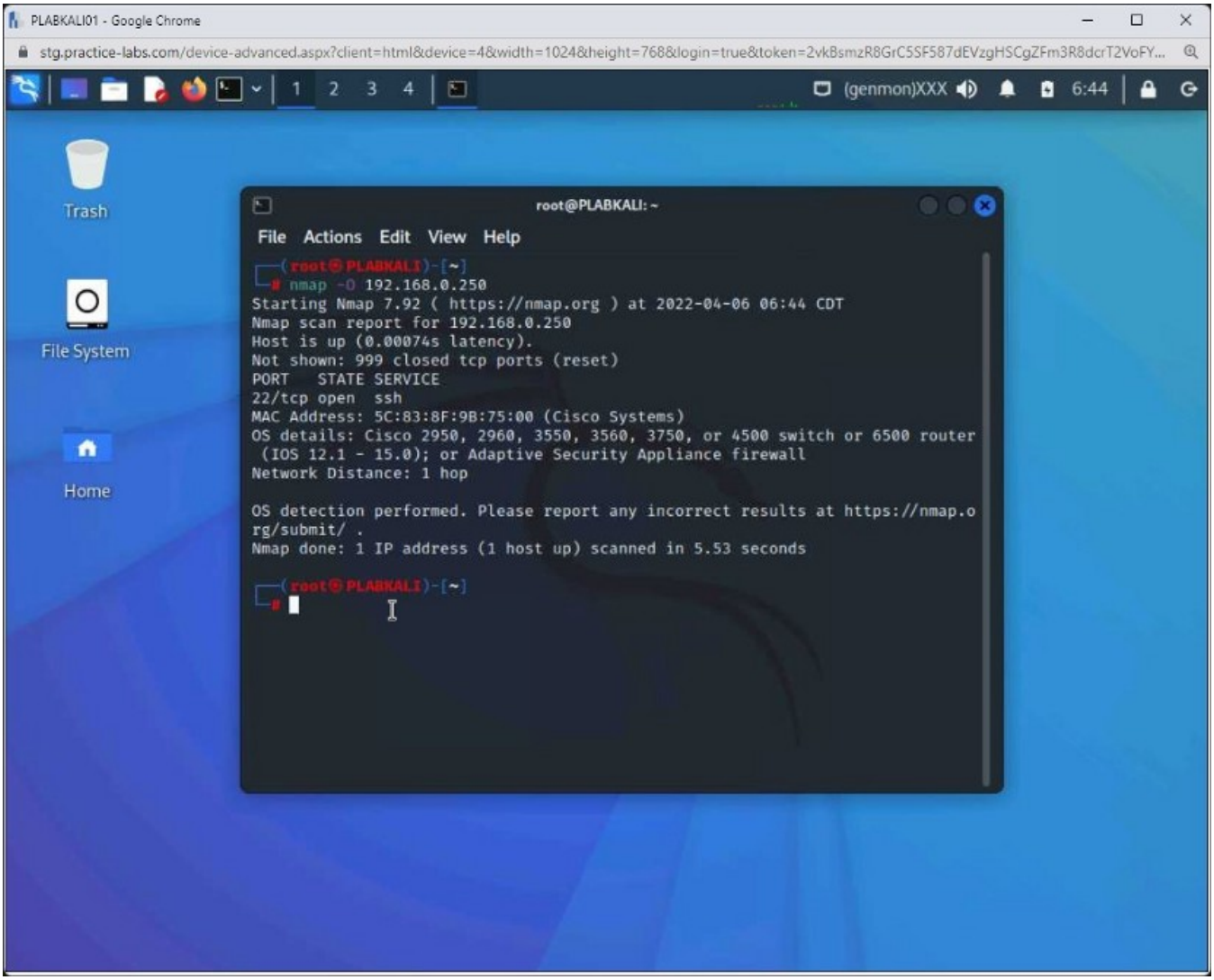
```
nmap -O 192.168.0.250
```

Press **Enter**.




### Step 3

The command ran successfully. The operating system is detected as **Cisco**, specifically **IOS 12.1–15.0**. The command also detects the type of switch or router is used.




**Step 4**

Clear the screen by entering the following command:

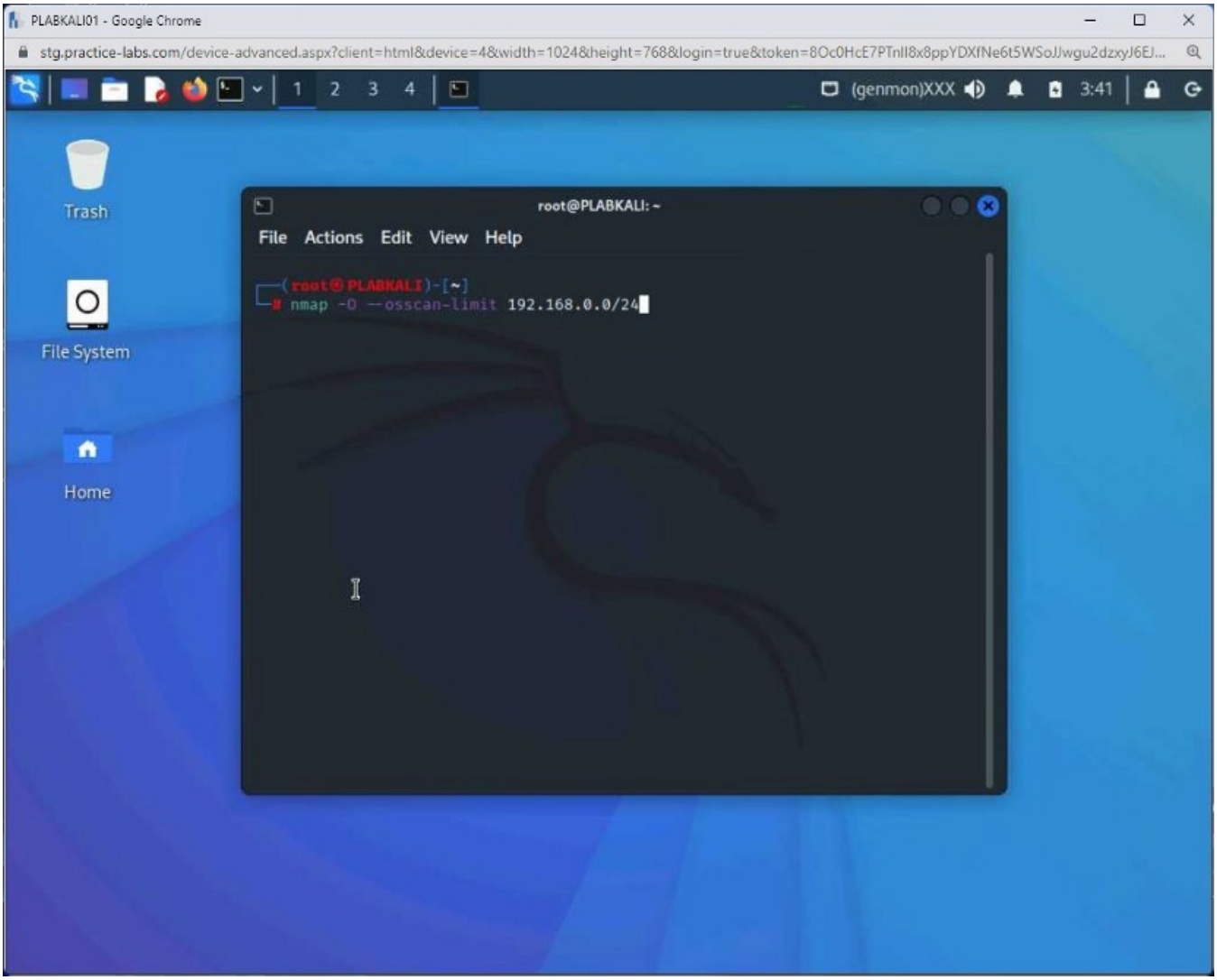
```
clear
```

You can choose to skip the hosts that are not up and running and scan for the operating system only on the live hosts. To do this, type the following command:

```
nmap -O --osscan-limit 192.168.0.0/24
```

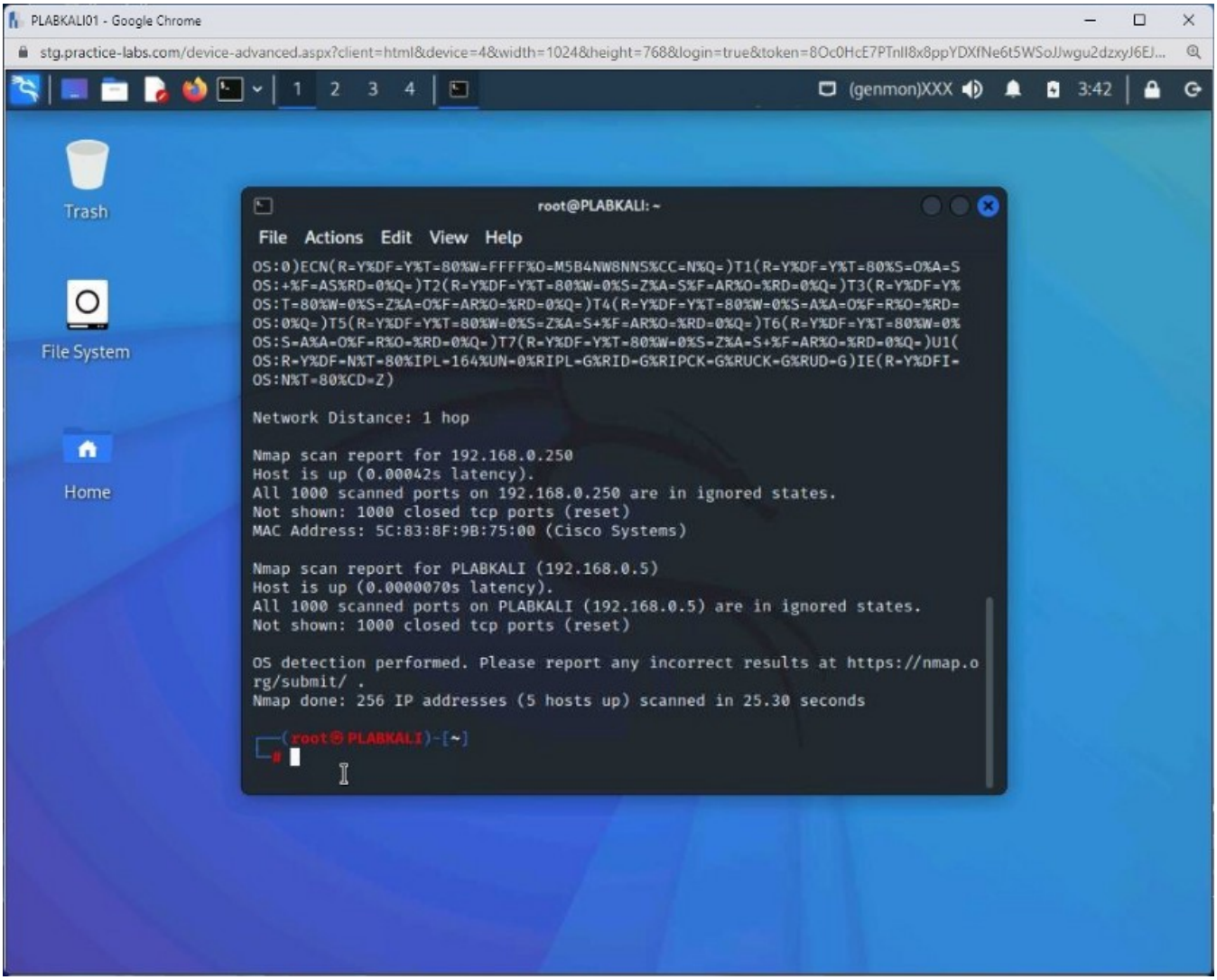
Press **Enter**. You can also use the **— osscan-guess** option with the **-O** parameter. It will attempt to detect the operating system.

If it cannot do so, it will provide the closest signature possible. It performs an aggressive detection of the operating system.




**Step 5**

The output is displayed. Scrolling up through the output, three operating systems, **Microsoft**, **Linux**, and **Cisco**, are detected.




**Step 6**

Clear the screen by entering the following command:

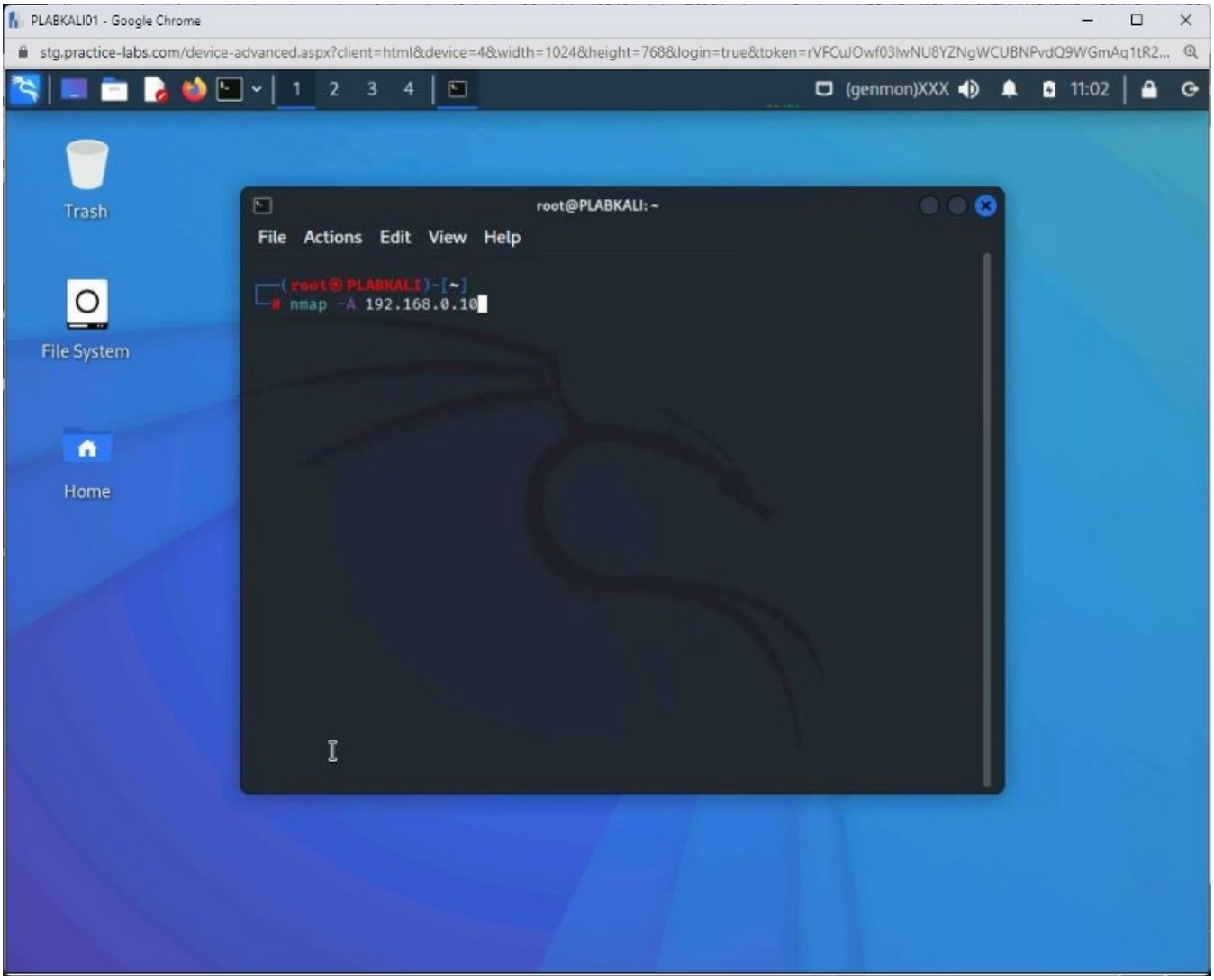
```
clear
```

You can also use the **-A** parameter with the nmap command to perform fingerprinting. To do this, type the following command:

```
nmap -A 192.168.0.10
```

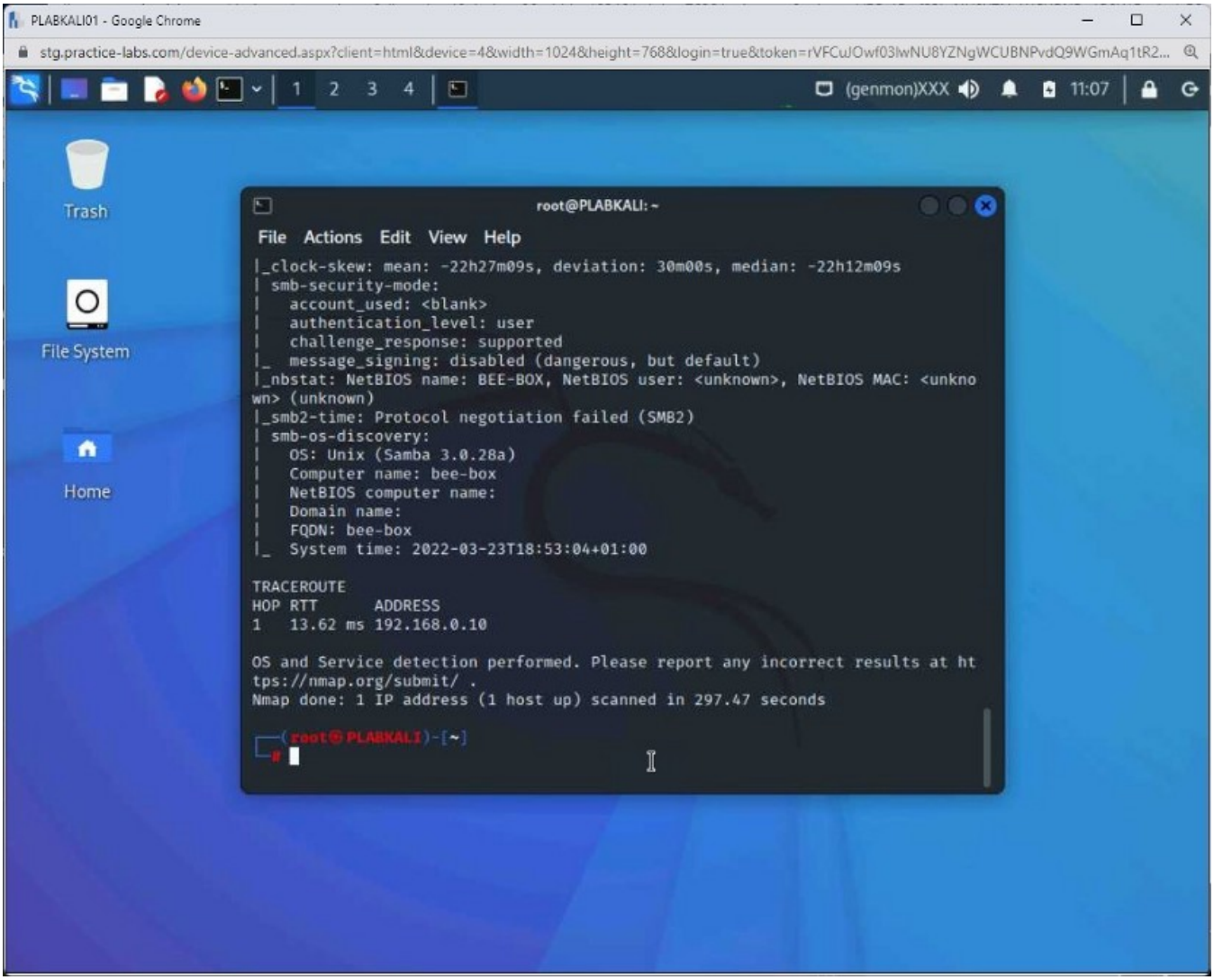
Press **Enter**.

***Note**: this command may take up to 5 minutes to complete.*




**Step 7**

Scrolling up slightly on the output, the **Linux** operating system is detected.




Keep the terminal window open.

## Task 3 — Perform Passive Fingerprinting on an Operating System

Passive fingerprinting can be done in different ways. For example, you can get many details from error messages, which can contain information, such as the type of operating system and server.

Sniffing network traffic can also help determine the operating system.

In this task, you will perform passive fingerprinting of an operating system.

### Step 1

Clear the screen by entering the following command:

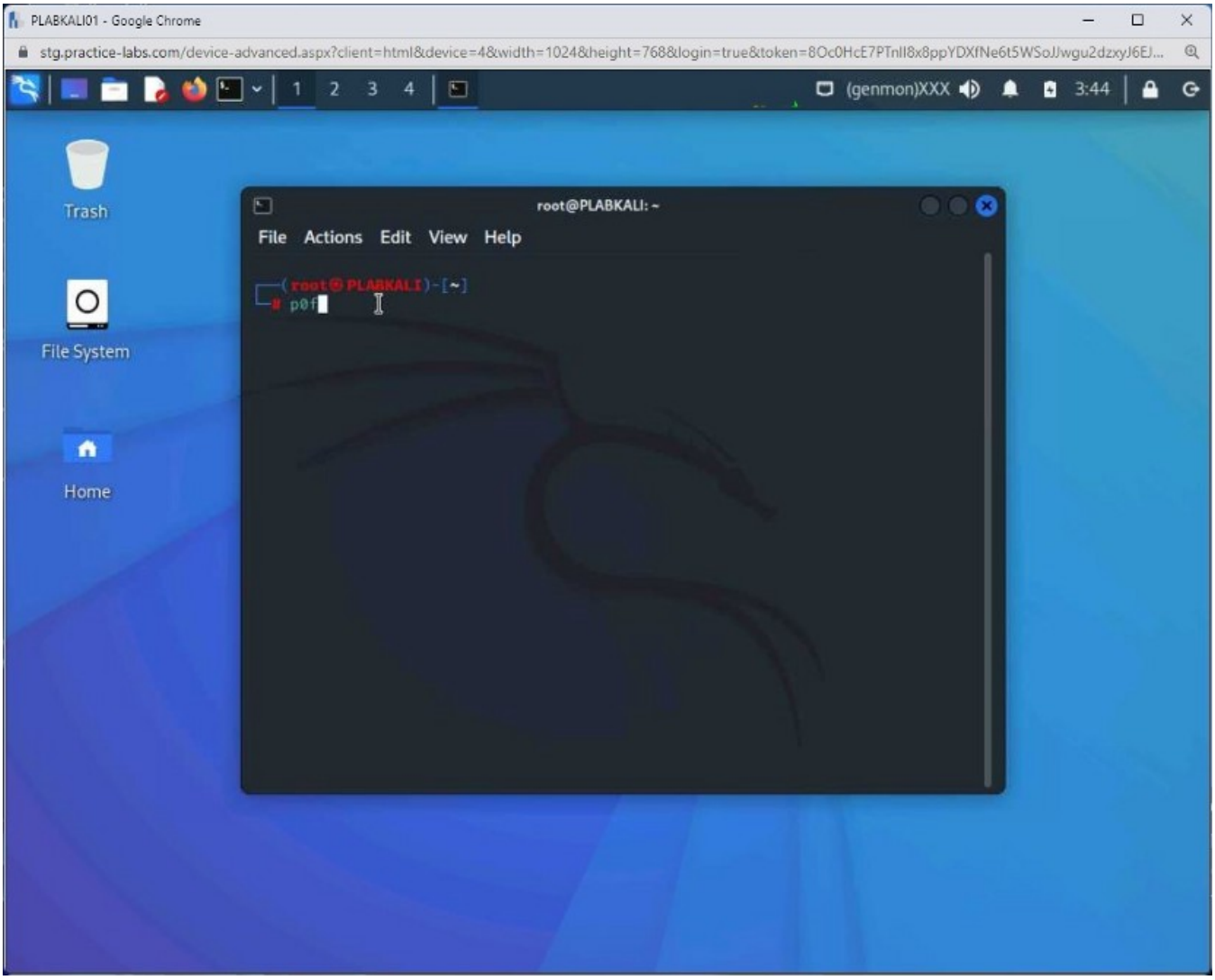
```
clear
```

Other than Nmap, you can also use another tool named **p0f** for operating system fingerprinting. It is a good tool to find out the website's operating system. To use the p0f tool, type the following command:

***Note:*** *You can use the* ***p0f*** *command with the* ***-i <interface_name>*** *to use a specific interface on your system. For example, you can use* ***eth0 -i eth0****.*

```
p0f
```

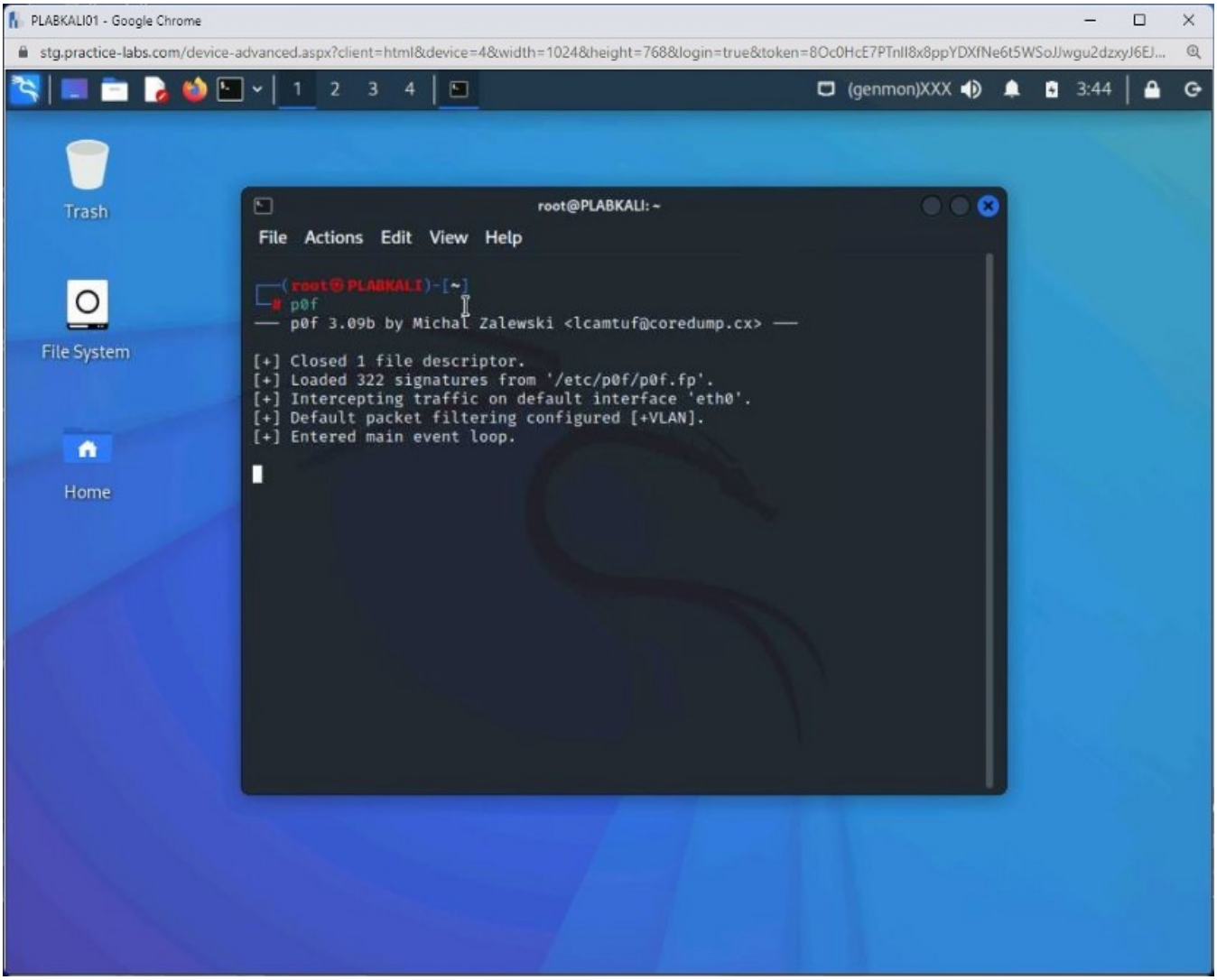
Press **Enter**.




#### Step 2

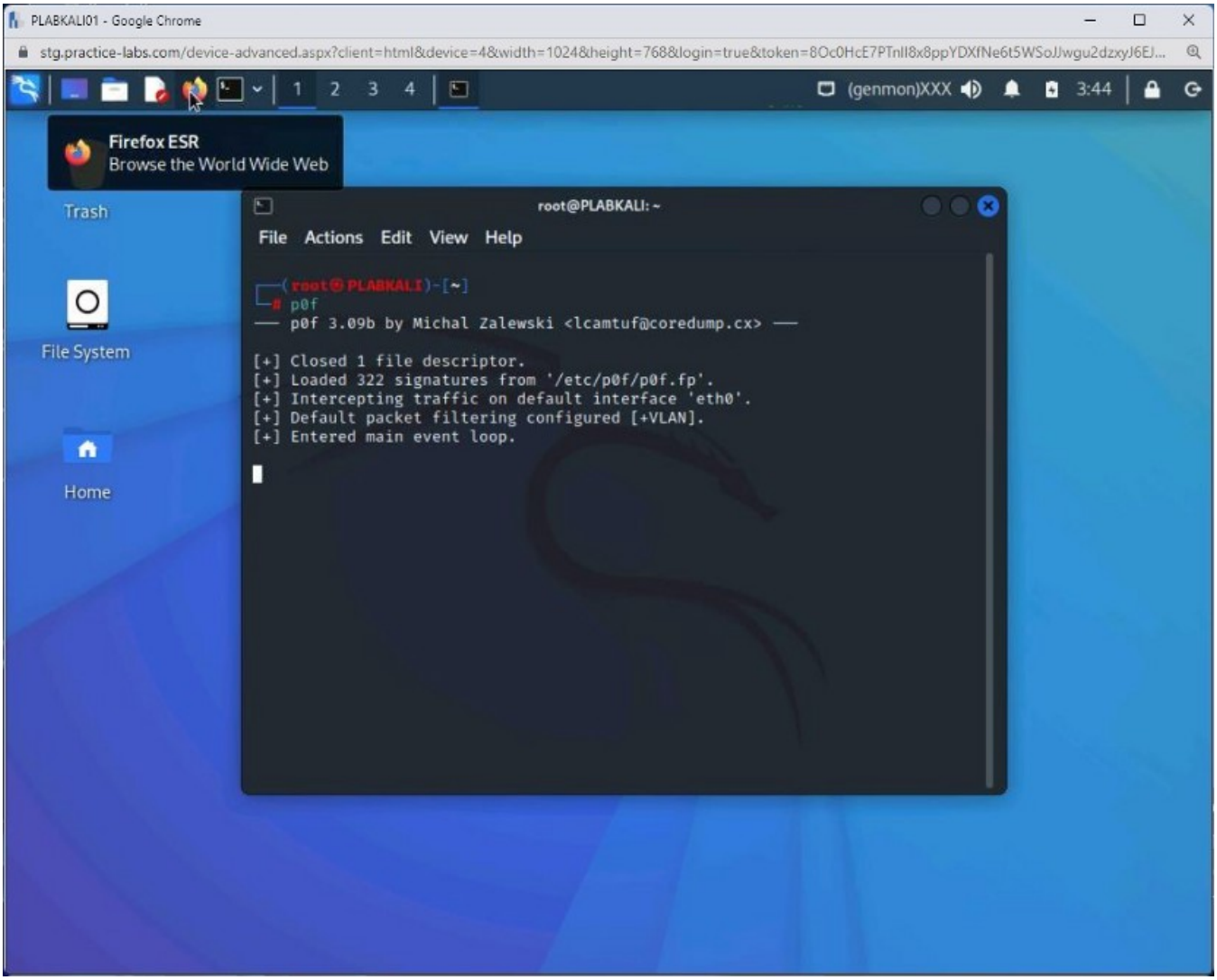
Notice that the **p0f** tool has started but is not doing anything. It has **322** signatures in the **/etc/p0f/p0f.fp** file.

It also mentions that it is using the **eth0** interface.




**Step 3**

Next, you need to open a website. Open **Firefox ESR** by clicking on the icon on the taskbar.

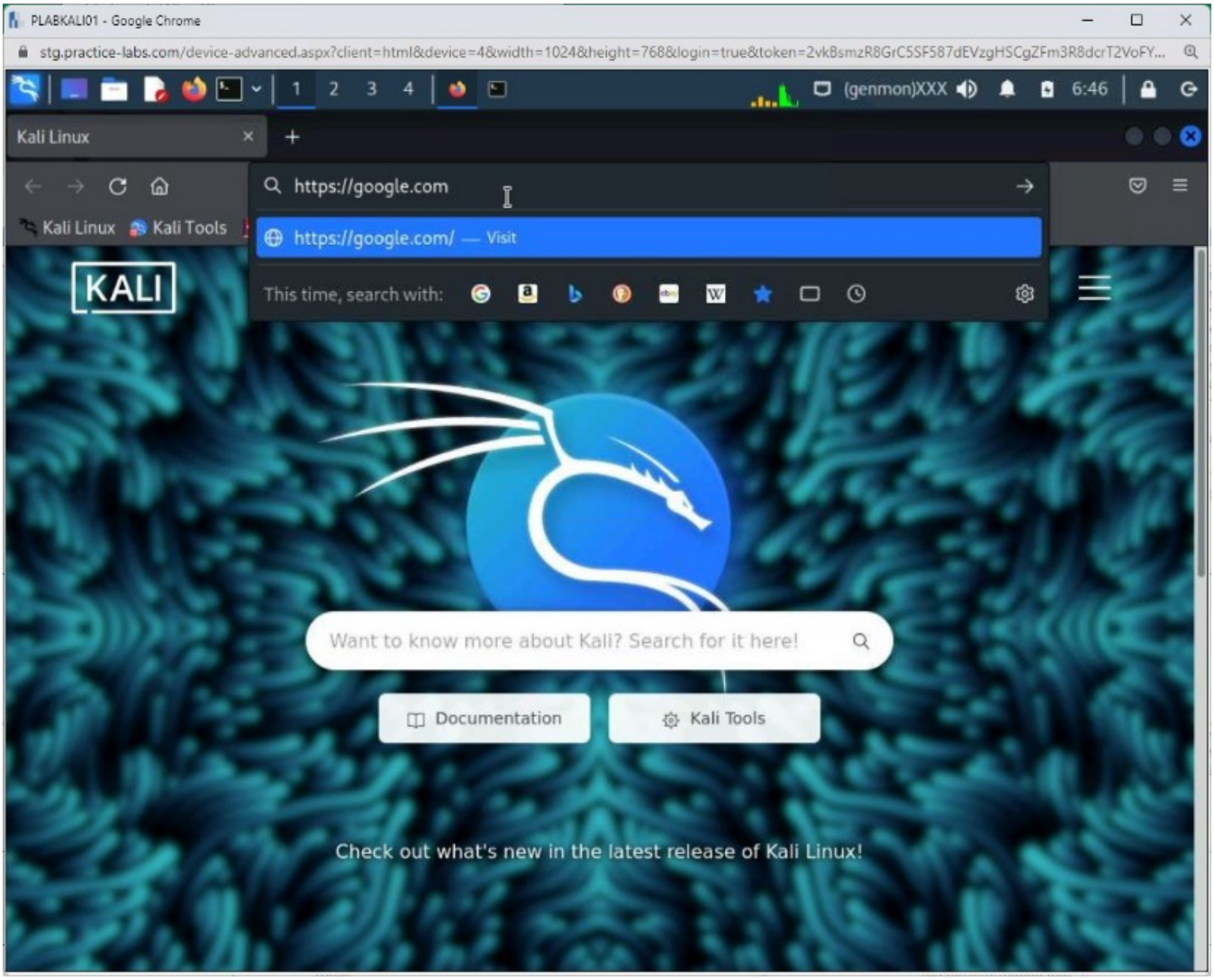



**Step 4**

The default Welcome to **Kali Linux** page is displayed. In the address bar, type the following URL:

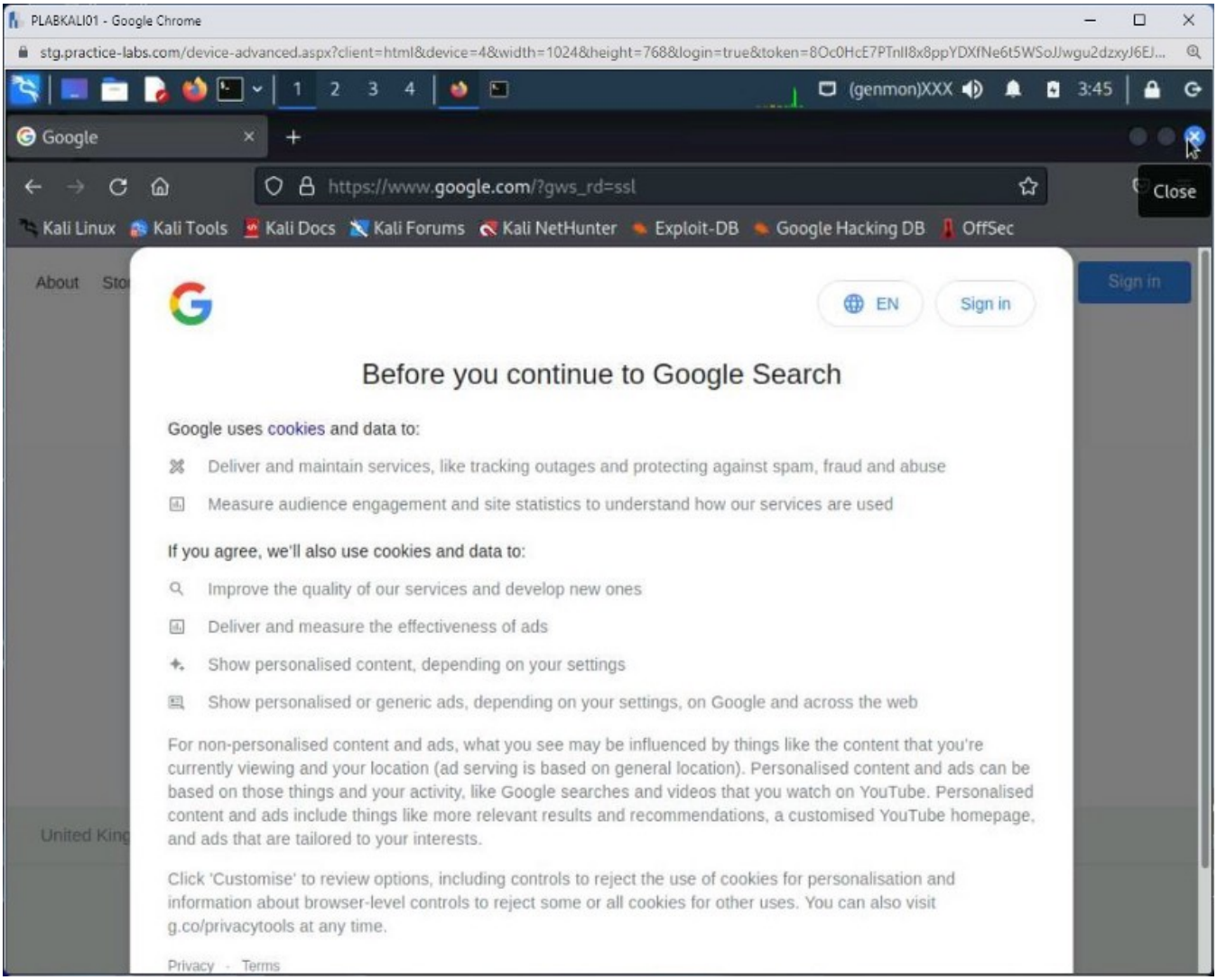
```
https://google.com
```

Press **Enter**.




**Step 5**

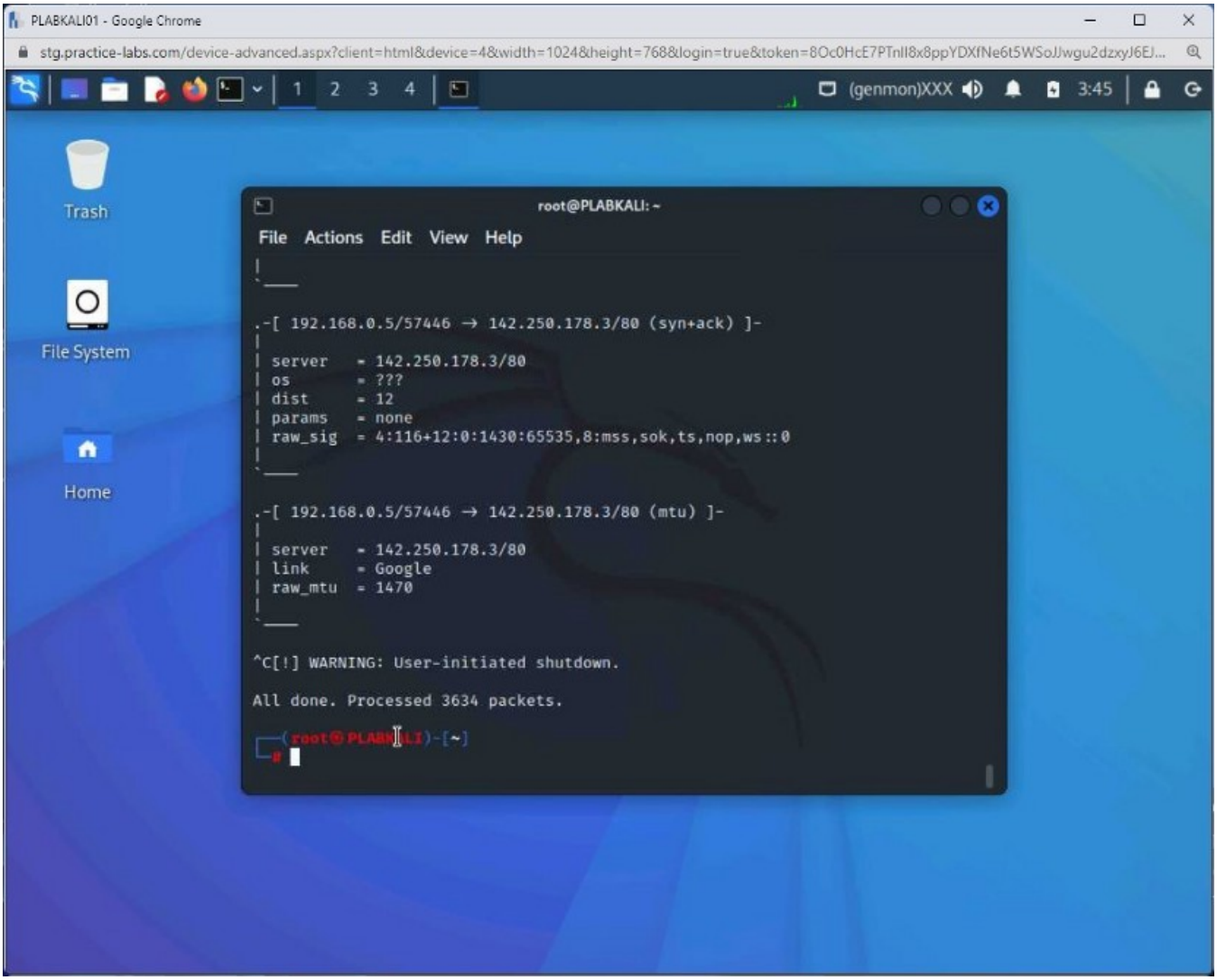
Close the **Firefox ESR** window.




**Step 6**

Notice that **pof** has started to capture a lot of data. Press **Ctrl + C** to stop the pof tool.

Scrolling up, you will notice that it has captured quite a bit of information, such as the operating system.




## Exercise 2 — Scanning Beyond Firewalls

To protect your network from an attacker, you can use various security controls like a firewall, intrusion prevention system (IPS), or intrusion detection system (IDS). Such security controls prevent malicious network traffic from intruding into the network. However, there are various methods that you can use to evade IDS /IPS and firewall detection.

In this exercise, you will learn about various methods to evade the IDS/IPS and firewall detection and perform the network scan.

## Learning Outcomes

After completing this exercise, you will be able to:

- Perform Scan Using Packet Fragmentation
- Perform Source Port Manipulation

## 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 MemberWorkstation192.168.0.5/24PLABDM01Domain Member Server192.168.0.2/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABDM01

Windows Server 2019 — Domain Member192.168.0.2/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

## Task 1 — Perform Scan Using Packet Fragmentation

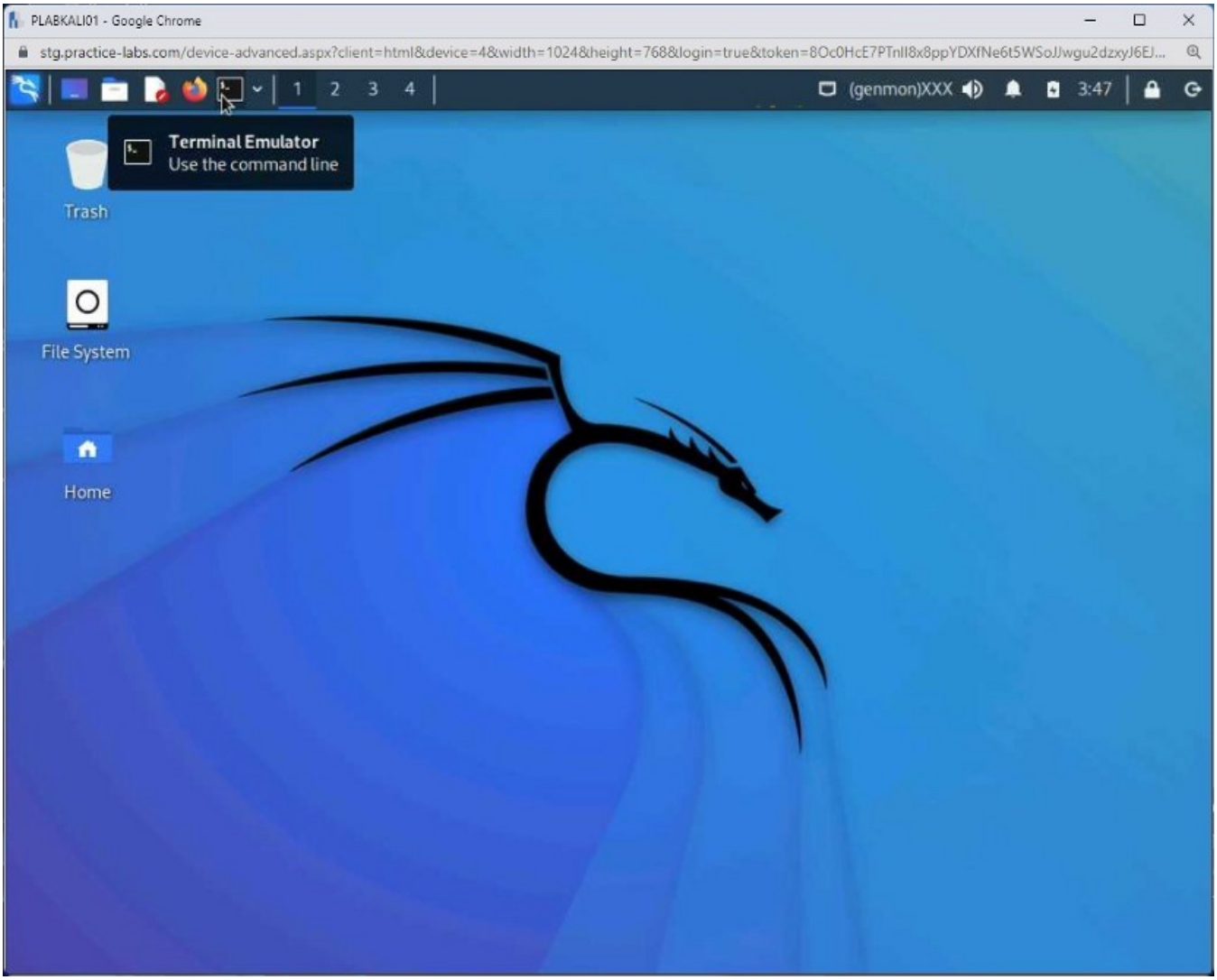
Packet fragmentation is a method of splitting a packet into smaller packets while sending it to the target systems.

Packets are split before they are sent, and then reassembled after reaching the target system(s). Because they are fragmented, IDS/IPS or a firewall cannot block them. Instead, packets are queued and processed one by one by these security controls.

In this task, you will learn to perform a packet fragmentation scan.

#### Step 1

Connect to **PLABKALI01**. Open the terminal window.



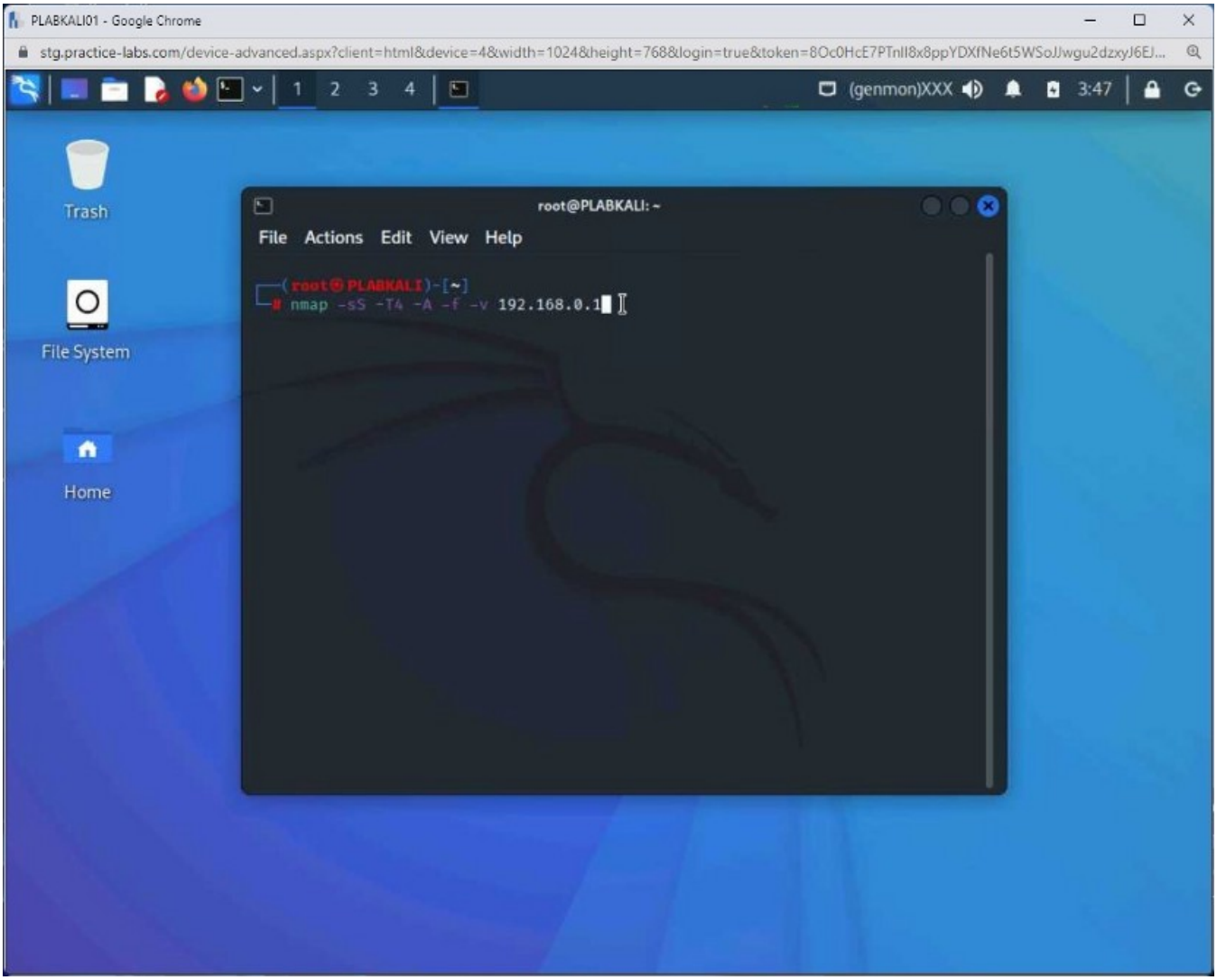

**Step 2**

You will perform the **TCP SYN** port scan but with fragmented packets. You will use the **-f** parameter to fragment the packets into smaller pieces to avoid detection. Type the following command:

```
nmap -sS -T4 -A -f -v 192.168.0.1
```

Press **Enter**.

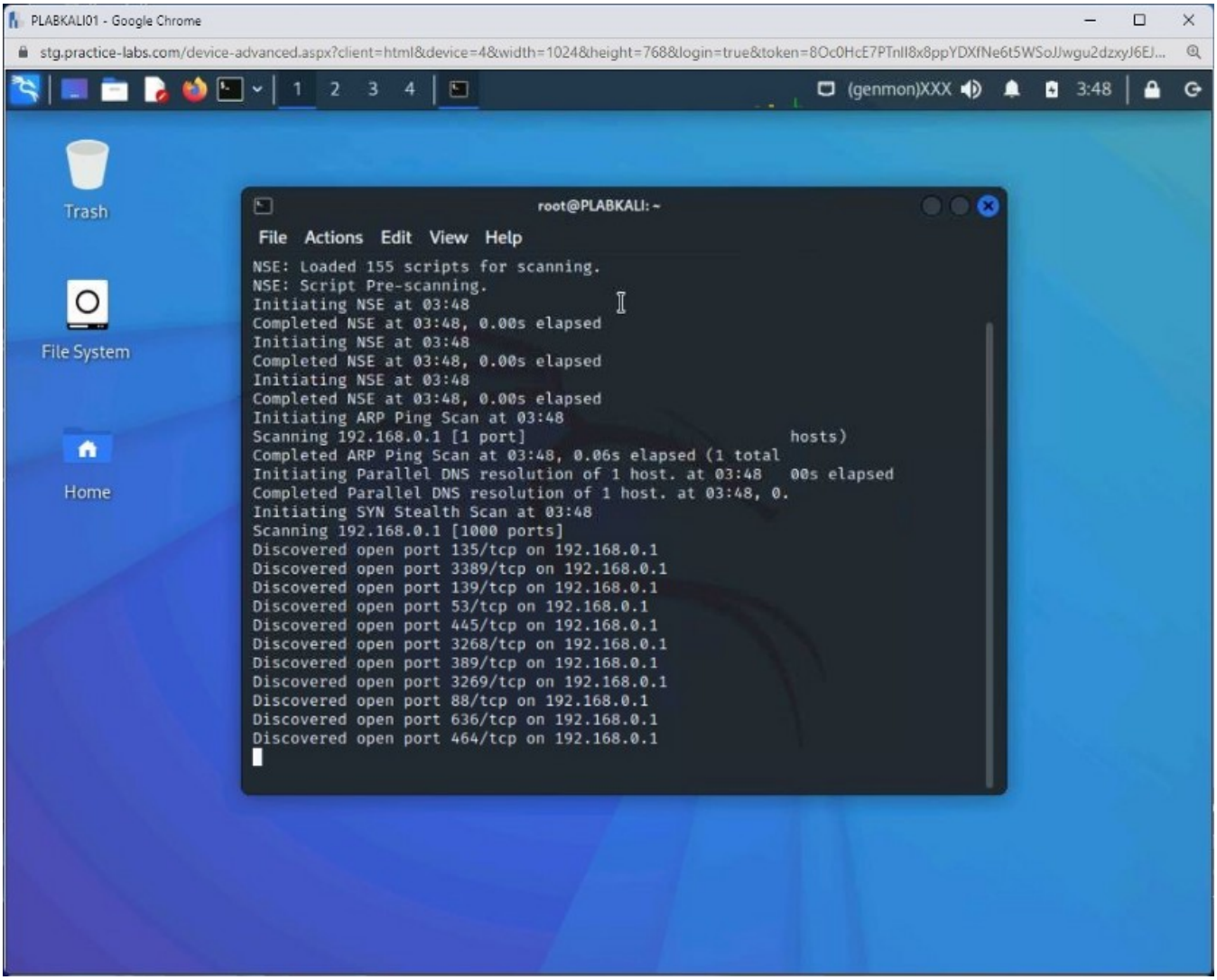
*The **-sS** parameter will perform the TCP SYN port scan.*
*The **-T4** parameter performs an aggressive scan.*
*The **-A** parameter is for operating system detection.*
*The **-f** parameter fragments the packets into smaller pieces.*
*The **-v** parameter performs a verbose scan.*




**Step 3**

The scanning process begins.

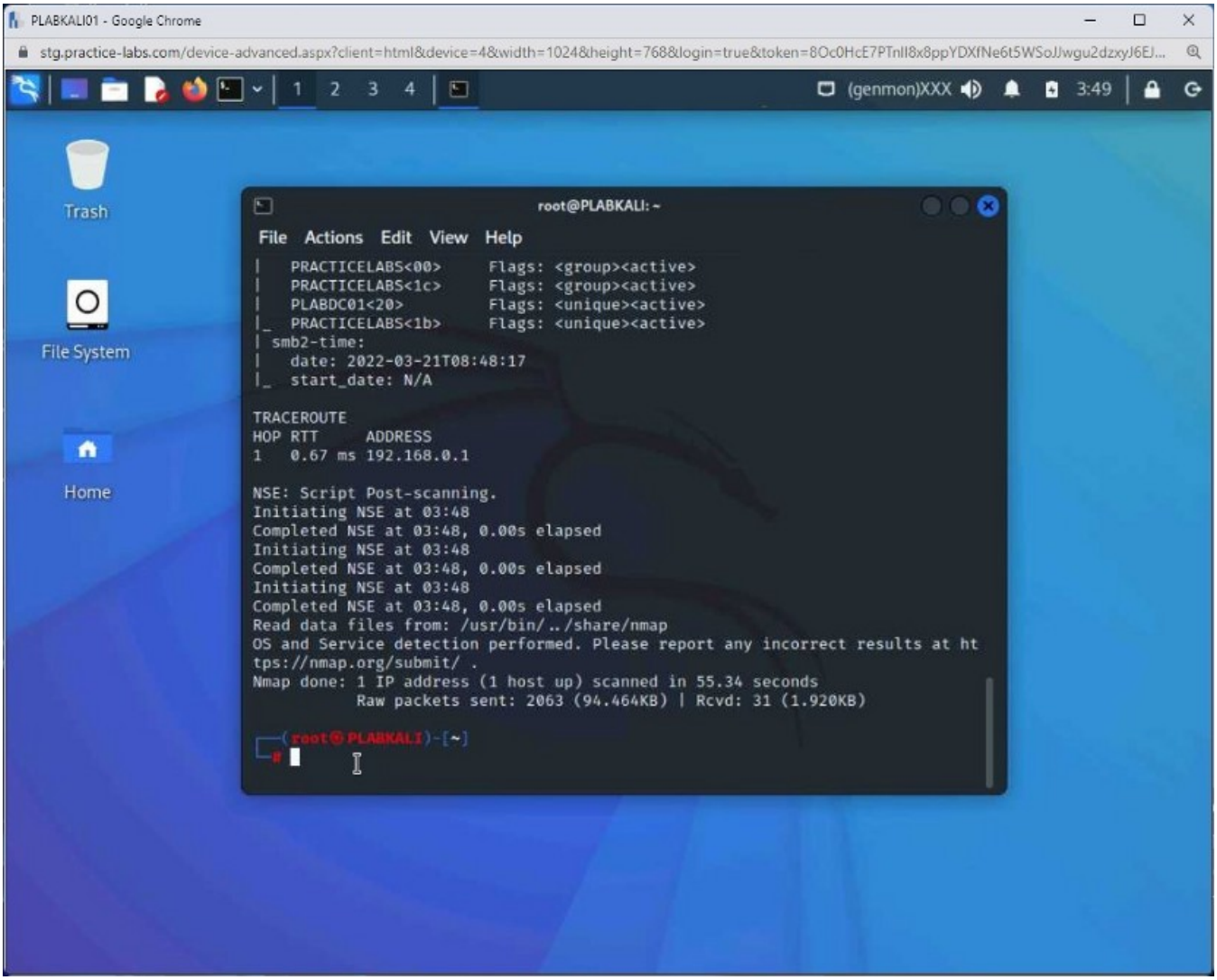
***Note**: It may takee a few minutes to complete the scan.*




**Step 4**

After a few minutes, the outcome of the command is displayed.

The scanning is successful, and the command has discovered the open ports using a stealth scan.




Keep the terminal window open.

## Task 2 — Perform Source Port Manipulation

To avoid IDS/IPS or firewall detection, attackers can use common ports like HTTP or HTTPS to avoid IDS/IPS or firewall detection. To perform the target detection, they can use the common ports so that the detection is avoided by any of the security controls like a firewall.

In this task, you will learn to perform source port manipulation.

### Step 1

Clear the screen by entering the following command:

```
clear
```

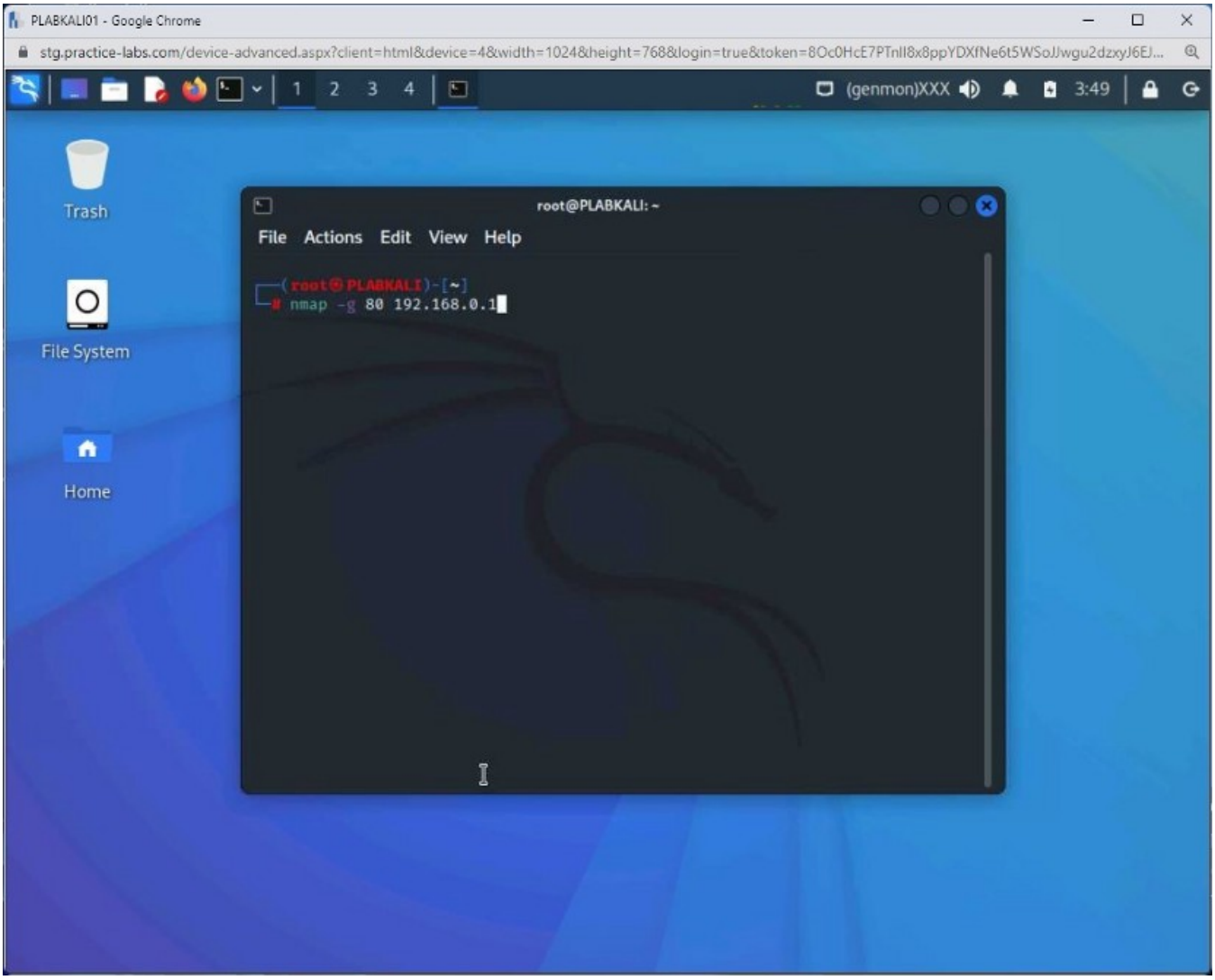
Press **Enter**.

Nmap provides two parameters for using a specific port when sending the traffic to a target system. You can either use the **-g** or **— source-port** parameter.

Let's go ahead and use the **-g** parameter and specify **port 80** for sending traffic to **192.168.0.1**. Type the following command:

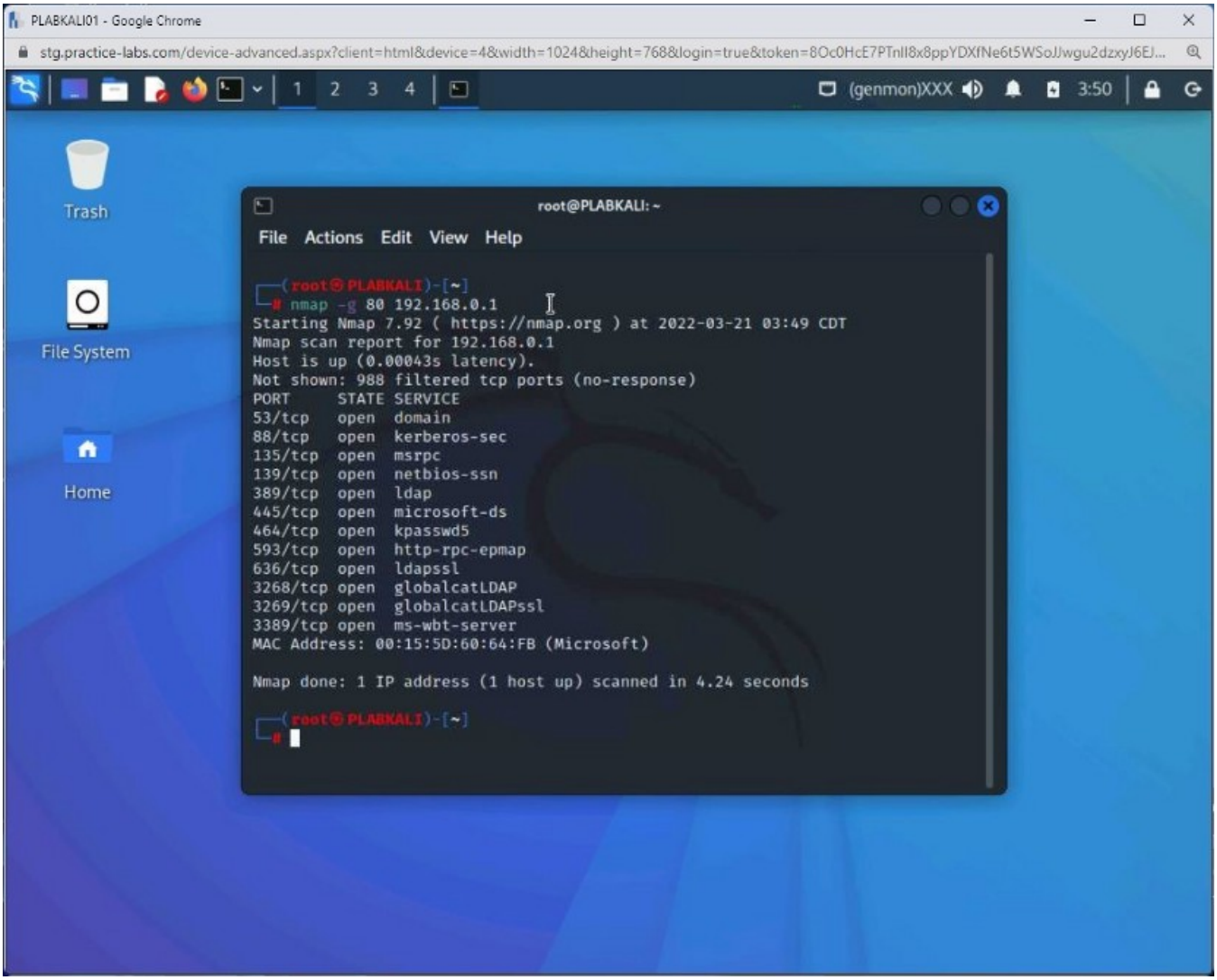
```
nmap -g 80 192.168.0.1
```

Press **Enter**.




**Step 2**

The command executes successfully.




**Step 3**

Clear the screen by entering the following command:

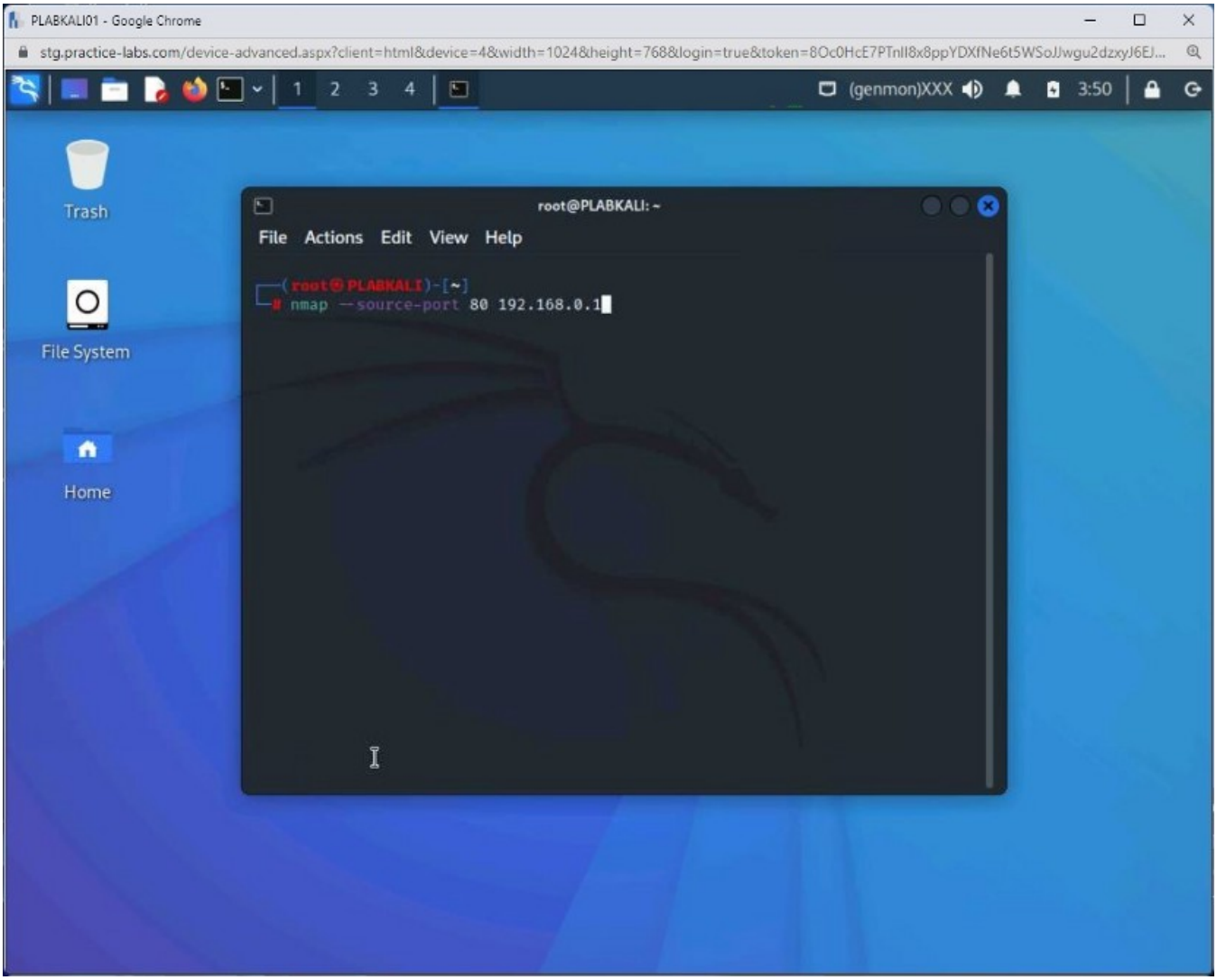
```
clear
```

Press **Enter**.

Let’s execute the same command with the — source-port parameter. Type the following command:

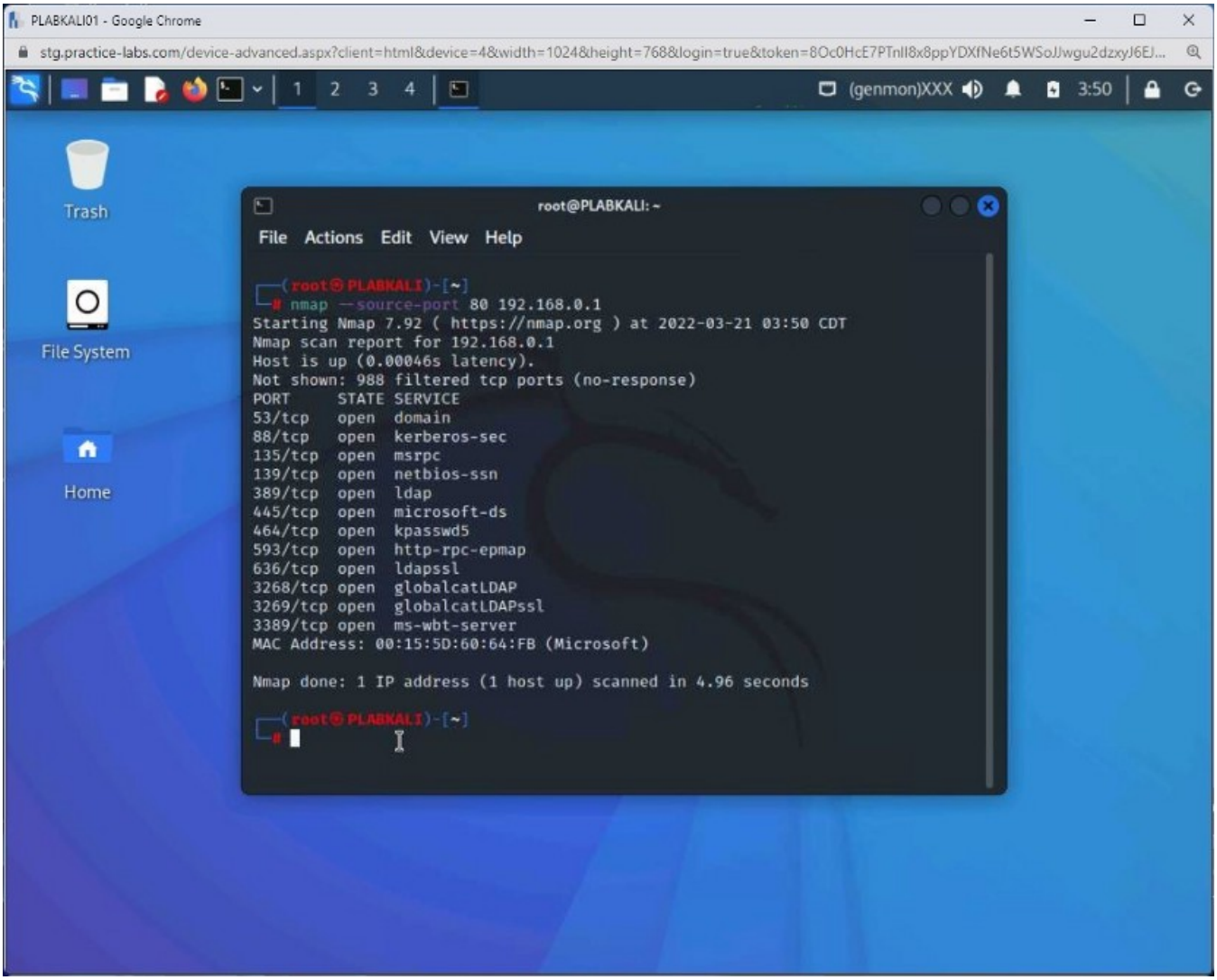
```
nmap --source-port 80 192.168.0.1
```

Press **Enter**.




**Step 4**

The same output is generated as the **-g** parameter.




## Exercise 3 — Draw Network Topologies

Network diagrams are essential for network administrators, which are used to visualize network configurations so they know the “placement” of each connected device.

If there is a network issue, administrators can use the network diagrams to narrow down the issue with a specific device quickly.

However, network diagrams also help attackers to understand the network architecture and correctly pinpoint the target host. With network diagrams, An attackers can also determine the position of the various security controls, like IDS and IPS.

## Learning Outcomes

After completing this exercise, you will be able to:

- Draw Network Topologies using The Dude

## 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 MemberWorkstation192.168.0.5/24PLABDM01Domain Member Server192.168.0.2/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABDM01

Windows Server 2019 — Domain Member192.168.0.2/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

### Task 1 — Use of Network Topologies

A network topology diagram is a visual depiction of network architecture. It uses different symbols and connections, which are represented by lines. A network diagram can help a user understand the layout of the network.

The network topology diagram should detail out how the network is designed. It should mention the following (at minimum):

- Devices that are present on the network
- Connectivity between these devices
- IP addresses and names of these devices

Assume a situation in which you have joined an organization as Network Administrator. You have been asked to troubleshoot a network problem. Without the help of a network diagram, it would take you a while to understand the network architecture. However, if the network diagram is available, you can visualize the problem quickly.

It is also important to note that network diagrams are not static. You should update the corresponding diagram as new devices are added or removed from the network. Even if an IP address of a server has changed, you should update it on the diagram.

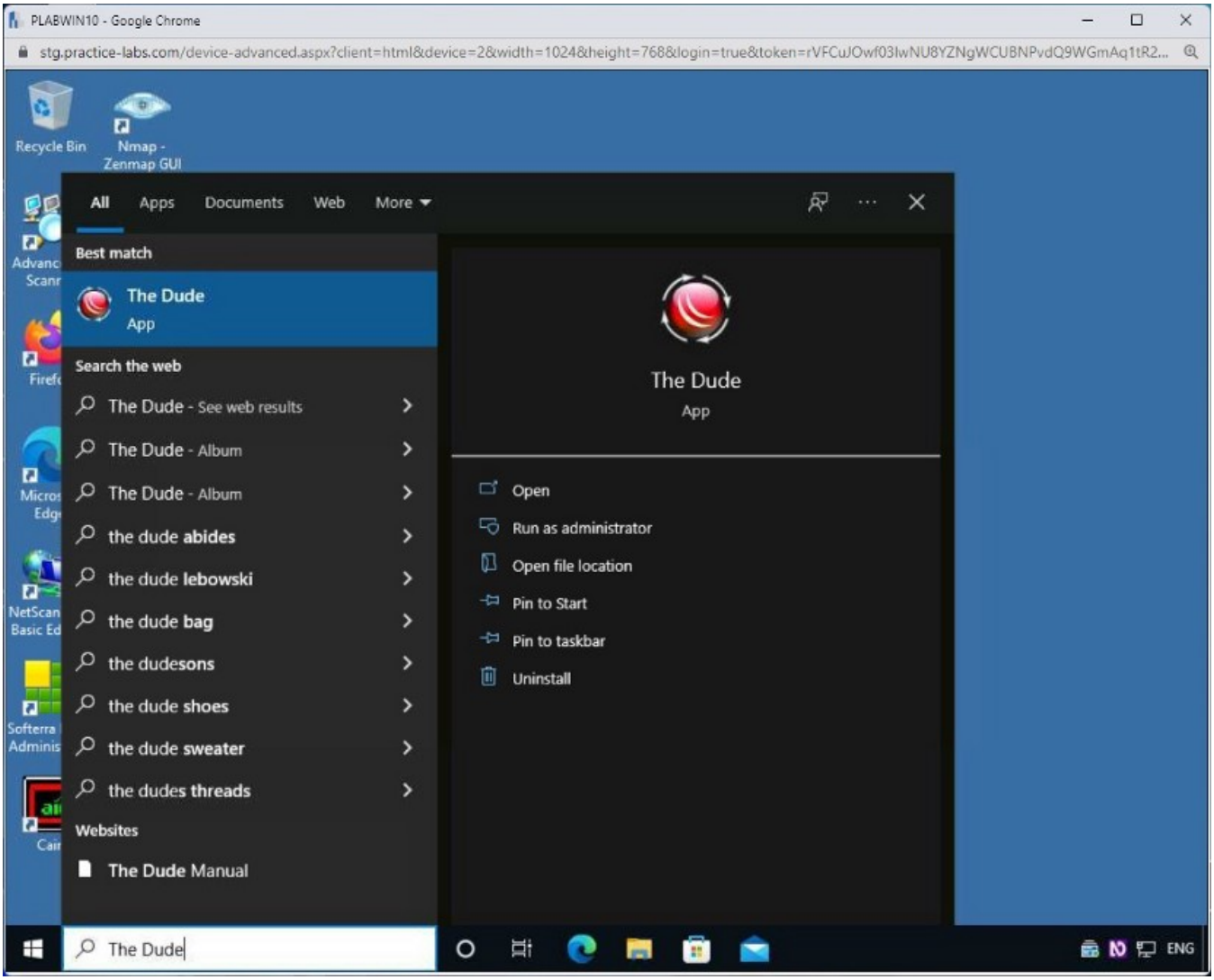
To create a network diagram, you can use various tools to discover the servers and network devices on the network and create a network map. In this task, you will use The Dude to create a network diagram.

### Step 1

Connect to **PLABWIN10**. In the Type here to search textbox, type the following:

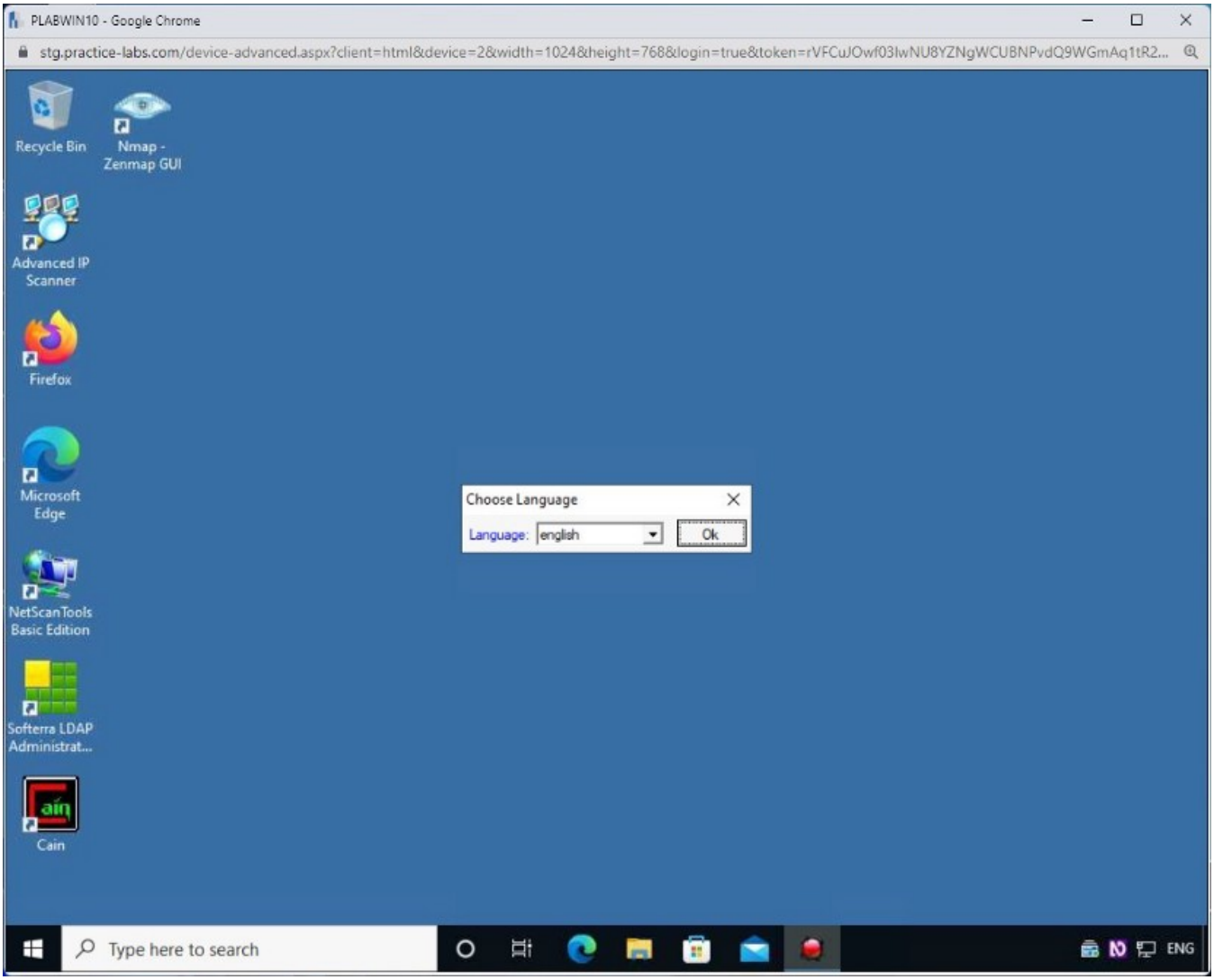
```
The Dude
```

From the search results, select **The Dude**.




### Step 2

The **Choose Language** dialog box is displayed. Select the default language and click **Ok**.

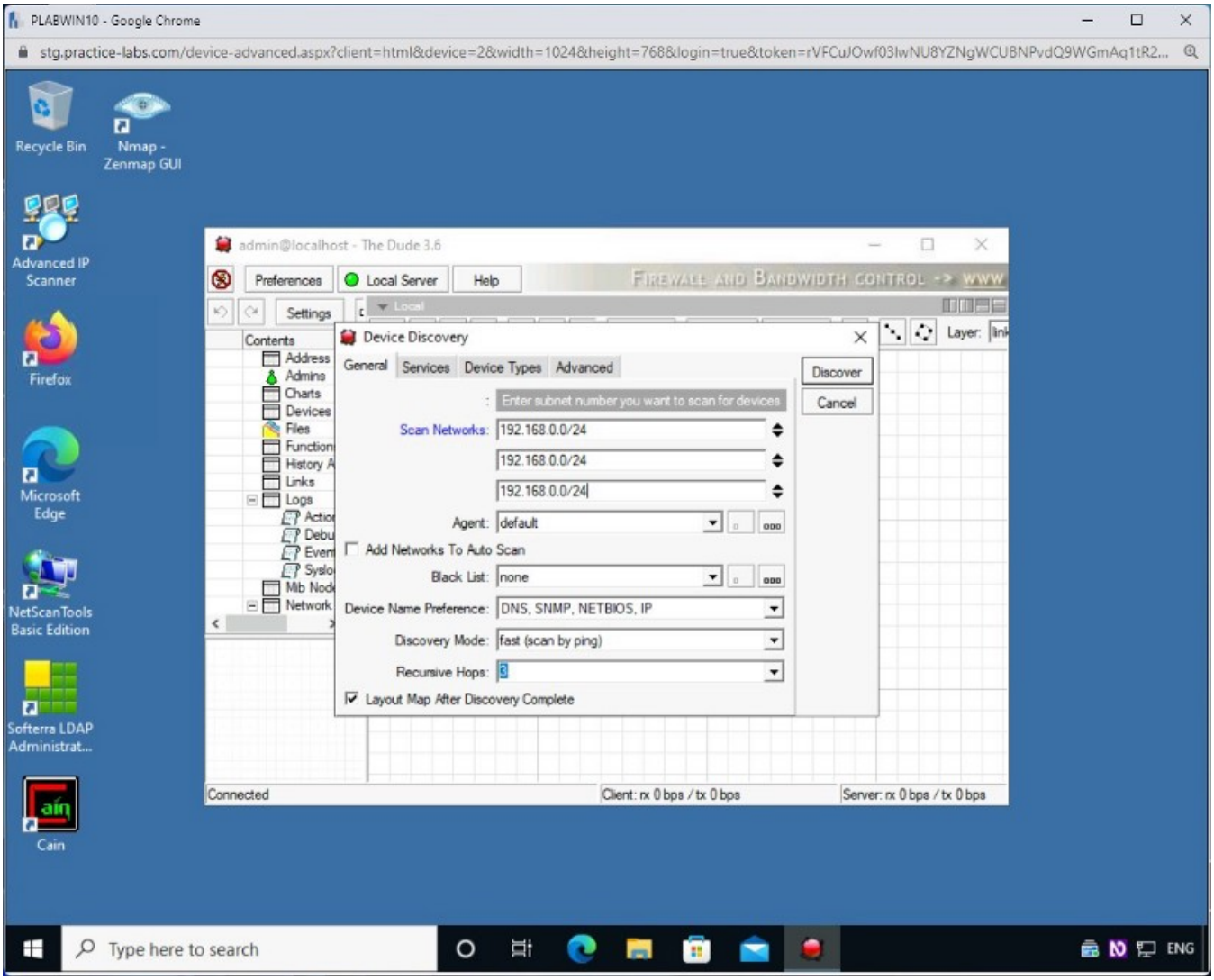



### Step 3

The **Device Discovery** dialog box is displayed. In the three **Scan Networks** textboxes, type the following CIDR range:

```
192.168.0.0/24
```

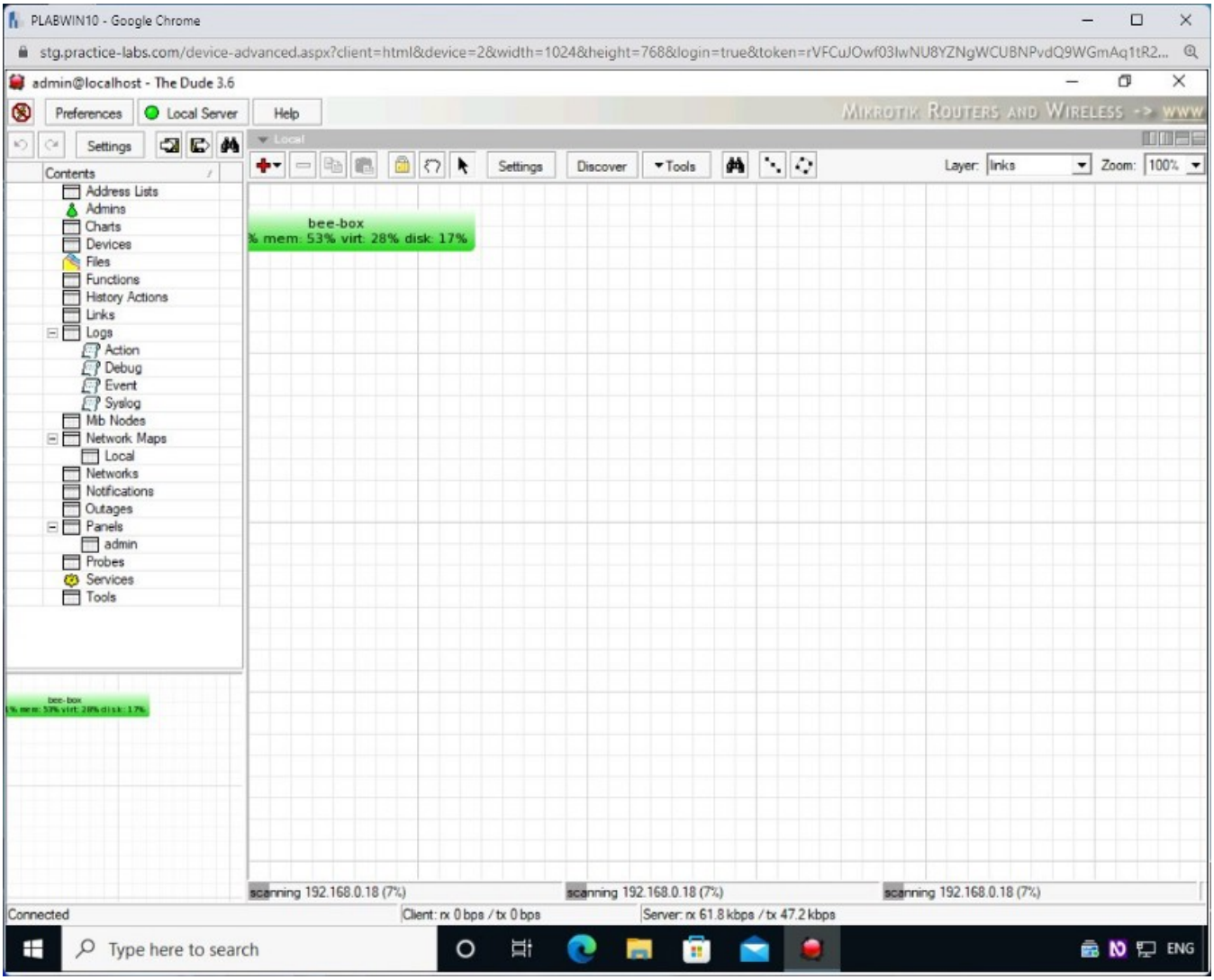
Click **Discover**.




**Step 4**

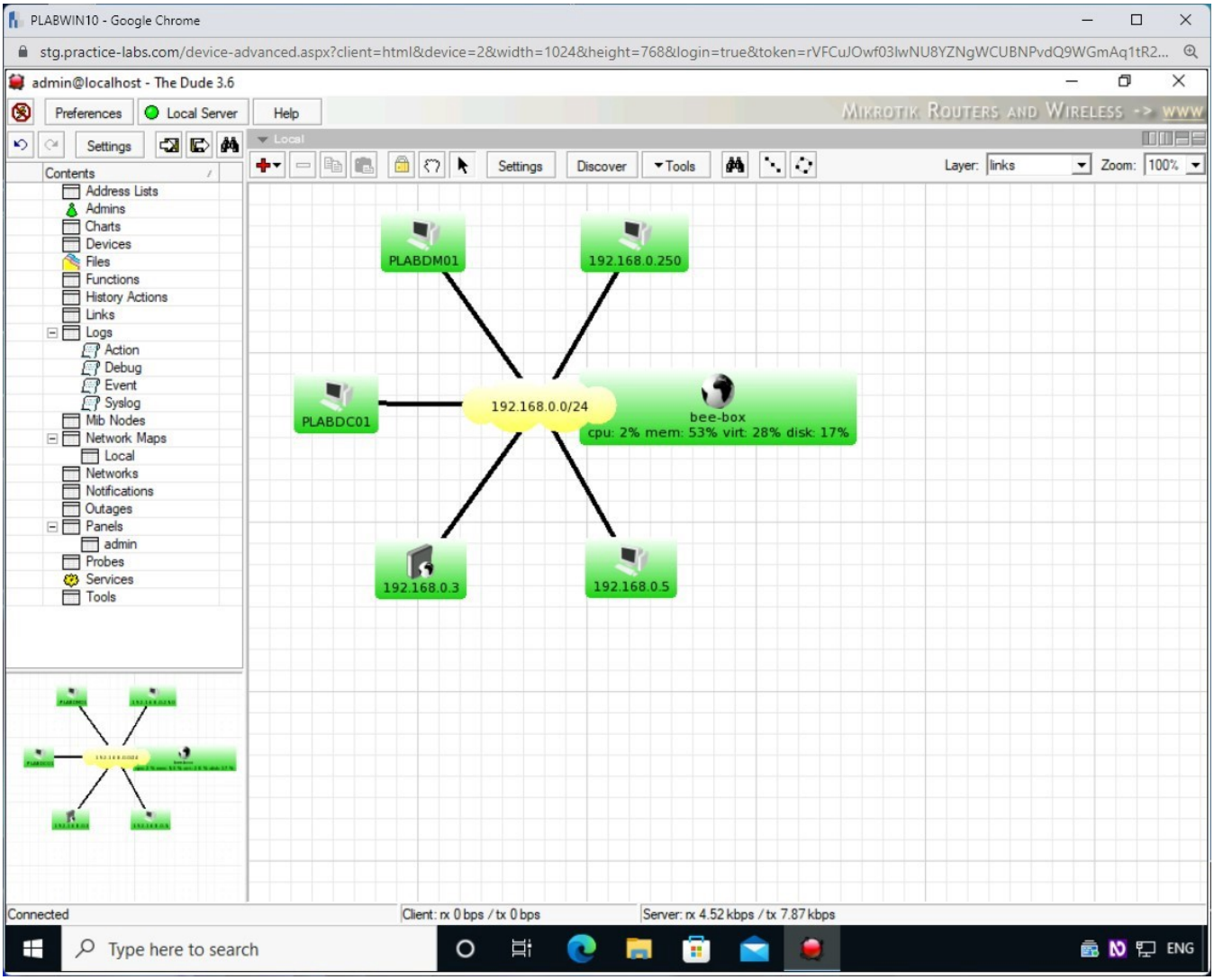
The device discovery process starts. This process takes a few minutes to complete.

***Note:*** *You can maximize the window.*




### Step 5

The network map is generated after the device discovery process.


PLABWIN10 - Google Chrome
admin@localhost - The Dude 3.6
Preferences
Local Server
Help
Settings
Discover
Tools
Layer: links
Zoom: 100%
Contents
Address Lists
Admins
Charts
Devices
Files
Functions
History Actions
Links
Logs
Action
Debug
Event
Syslog
Mib Nodes
Network Maps
Local
Networks
Notifications
Outages
Panels
admin
Probes
Services
Tools
PLABDM01
192.168.0.250
PLABDC01
192.168.0.0/24
bee-box
cpu: 2% mem: 53% virt: 28% disk: 17%
192.168.0.3
192.168.0.5
Connected
Client: rx 0 bps / tx 0 bps
Server: rx 4.52 kbps / tx 7.87 kbps
Type here to search
ENG

## Review