CEH v12 Lesson 4 : NTP, DNS & Other Network Enumeration Techniques & Countermeasures

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 — NTP Enumeration
- Exercise 2 -DNS Enumeration
- Exercise 3 — Other Enumeration Techniques
- Exercise 4 — Enumeration Countermeasures

After completing this module, you will be able to:

- Use ntpdate
- Perform NTP enumeration using Nmap
- Perform DNS Enumeration
- Perform Server Message Block (SMB) Enumeration
- Perform Windows Host Enumeration Using rpcclient
- Perform Linux Host Enumeration using Nmap
- Use Hyena for Enumeration
- Perform Website Enumeration using Nmap
- Prevent Web Applications Enumeration

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

- Methods to Prevent DNS Enumeration
- Methods to Prevent Windows Enumeration
- Methods to Prevent FTP Enumeration
- Methods to Prevent SMTP Enumeration

Lab Duration

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

Exercise 1 — NTP Enumeration

The Network Time Protocol (NTP) is used for time synchronization. It can provide information to connect users to an NTP server, system names, and operating systems. Systems internal to a network can use either an internal or external NTP server. Even though the NTP service is not a concern for many network administrators, if exploited, it can provide a wealth of information to the attacker.

Attackers can extract a list of connected hosts along with their operating systems and IP addresses, which is vital information to use as a starting point for a wider attack.

In this exercise, you will learn to perform NTP enumeration.

Learning Outcomes

After completing this exercise, you will be able to:

- Use ntpdate
- Perform NTP enumeration using Nmap

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

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

Task 1 — Use ntpdate

The ntpdate command collects the time source server information. You can use this command to test a connection with a specific NTP server that may be hosted within or outside your organization. An attacker can use this command to force DNS resolution, force the time to be slowed or stepped up, or simply collect time samples from different time sources.

You can even use it to synchronize the time of a system with a specific time server. In this task, you will learn to use ntpdate.

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:

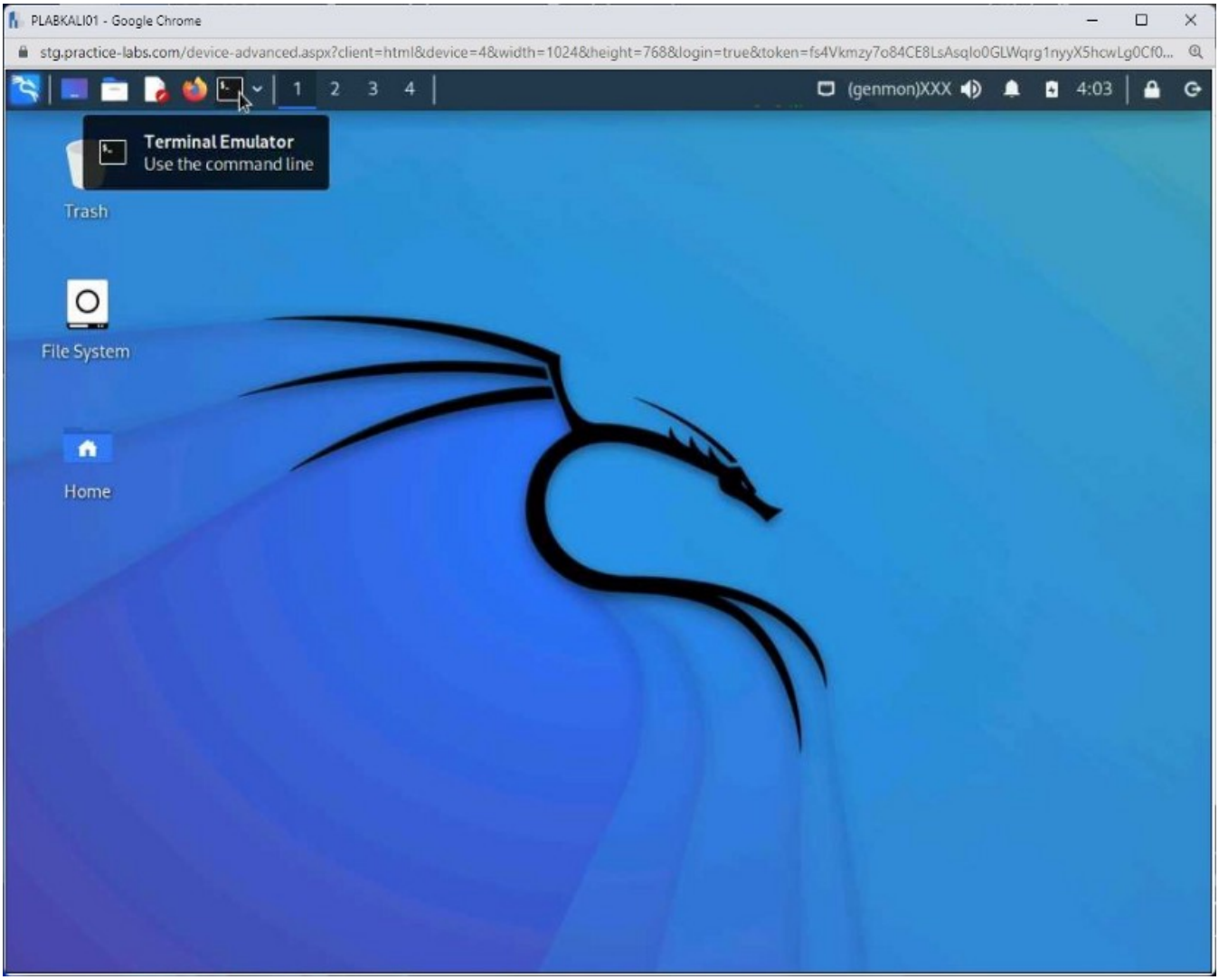
```
root
```

Password:

Password

The desktop of **PLABKALI01** is displayed.

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



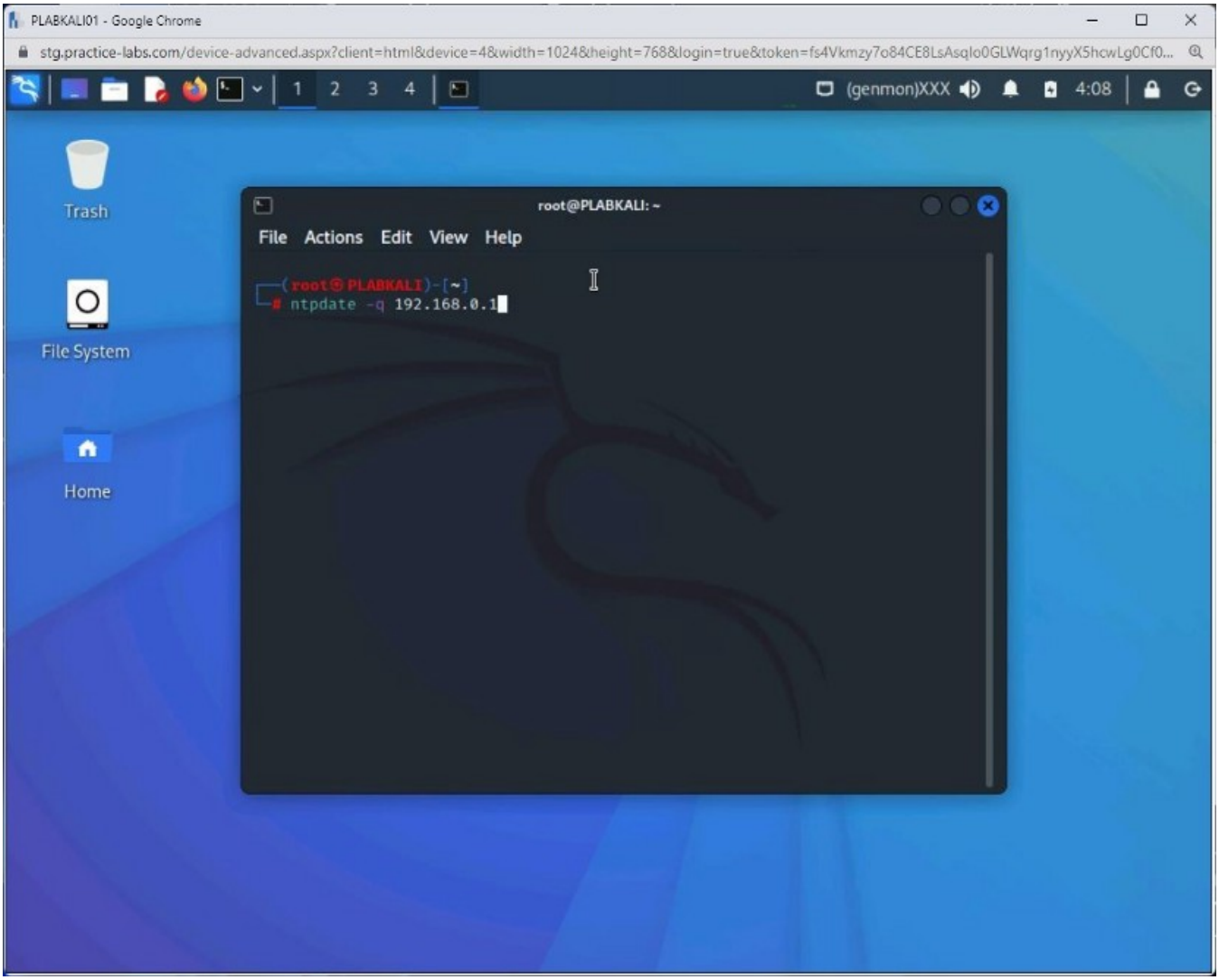
Step 2

Using the **-q** parameter, you can test connection to an NTP server.

When you use the **-q** parameter, you will only query the time server. In this scenario, you can test the connection with **192.168.0.1**, **PLABDC01**. To do this, you need to execute the following command:

```
ntpdate -q 192.168.0.1
```

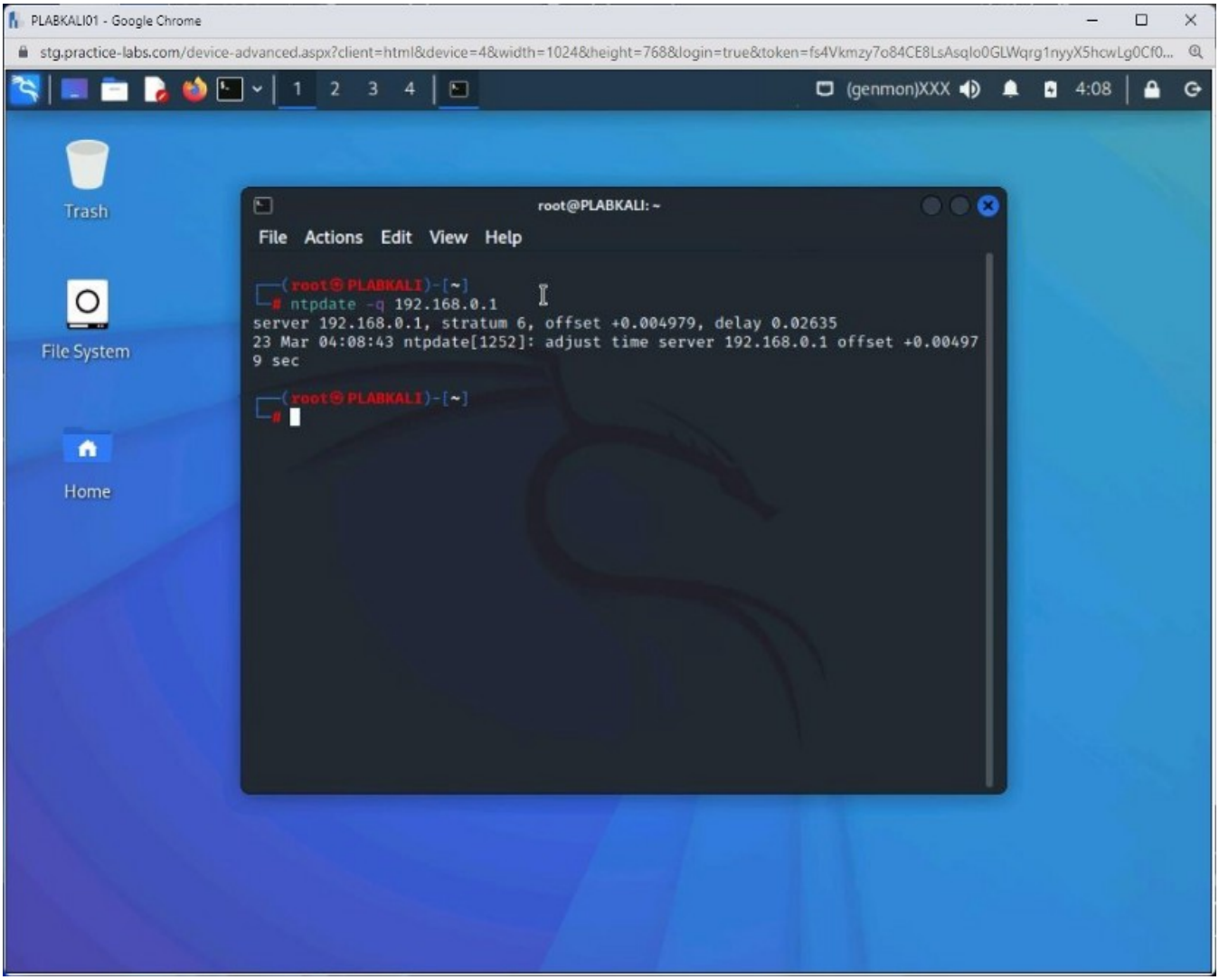
Press **Enter**.



Step 3

The output is displayed. There are various parameters displayed in the output. Let's look at each one of them.

- **Stratum**: is the 6th level time server in the hierarchy. Stratum 1 is the highest in the hierarchy.
- **Offset**: is the time difference between the time on the local system and the mentioned NTP Server.
- **Delay**: is the latency with the NTP Server.

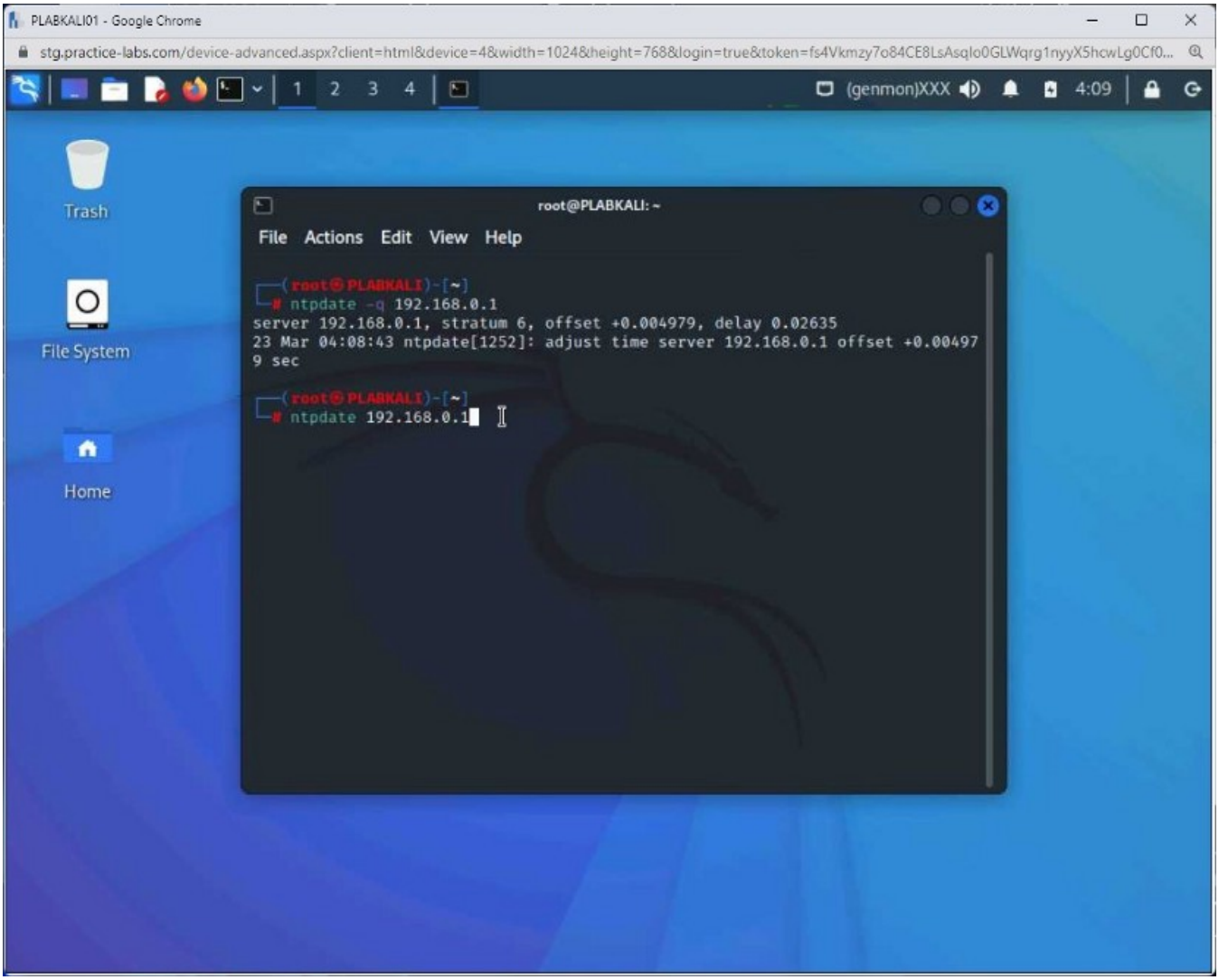


Step 4

You can also synchronize the time with a specific time server. To do this, type the following command:

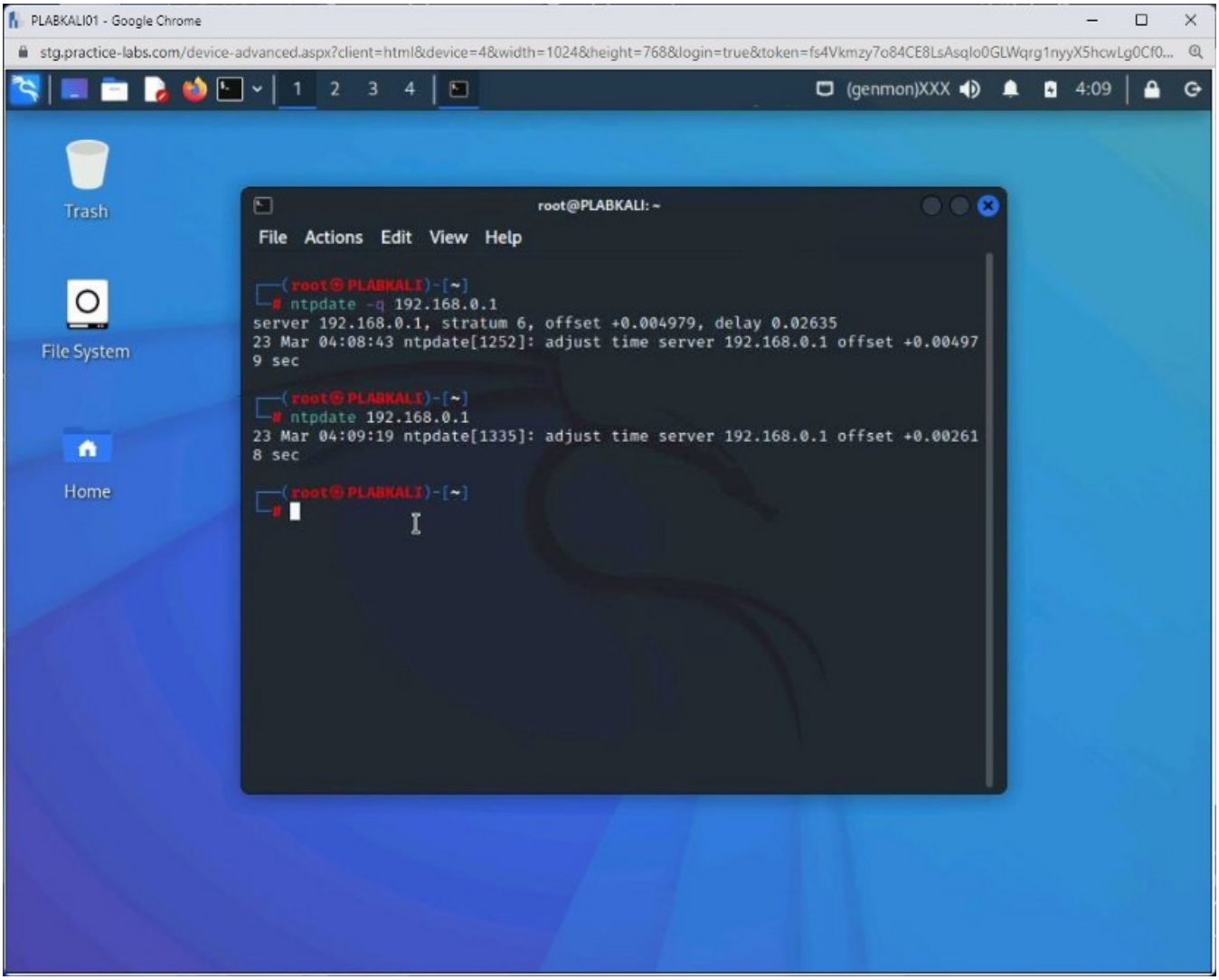
```
ntpdate 192.168.0.1
```

Press **Enter**.



Step 5

The output displays that the time server is now set.



Step 6

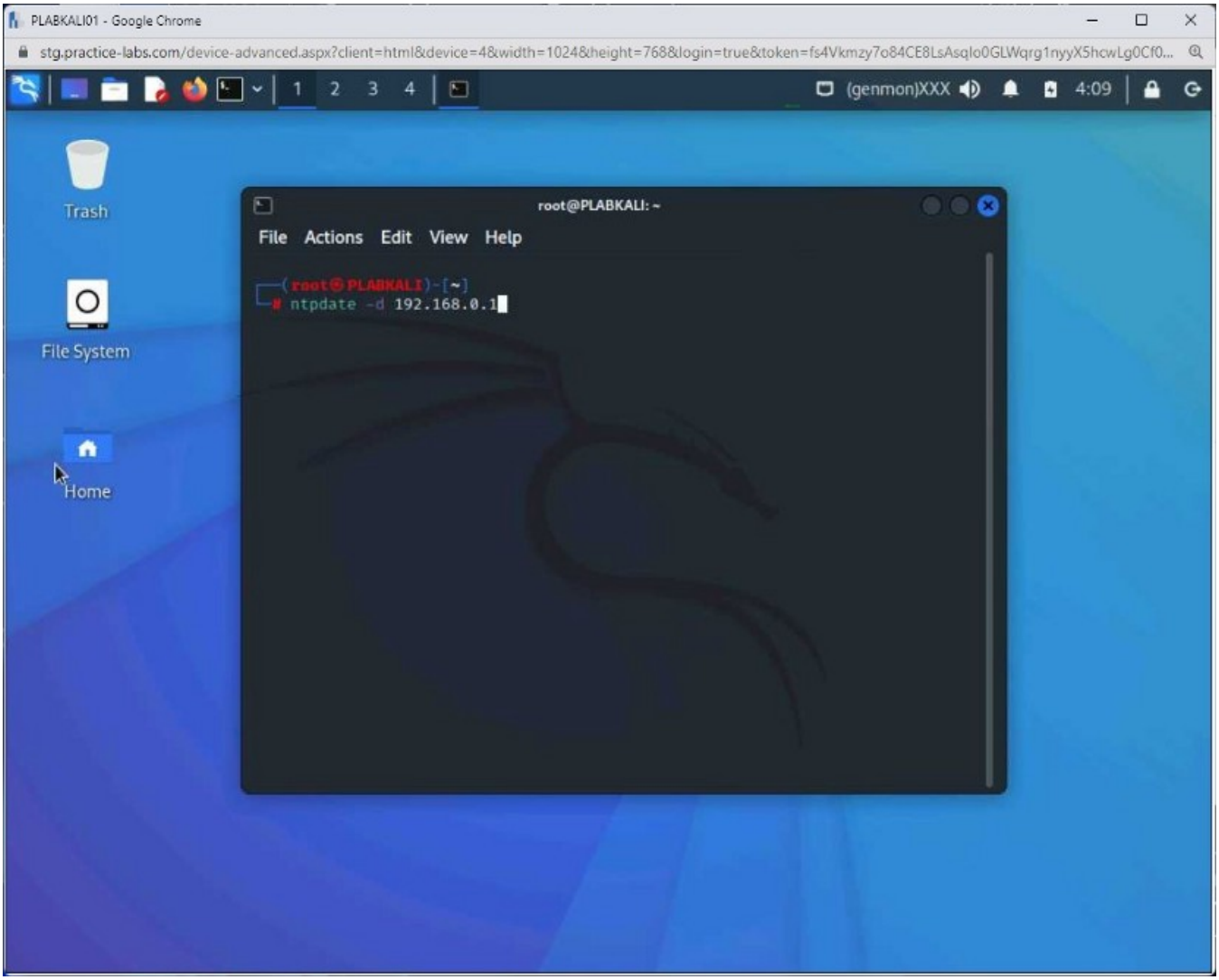
Clear the screen by entering the following command:

```
clear
```

You can also enable the debug mode with the **-d** parameter. To do this, type the following command:

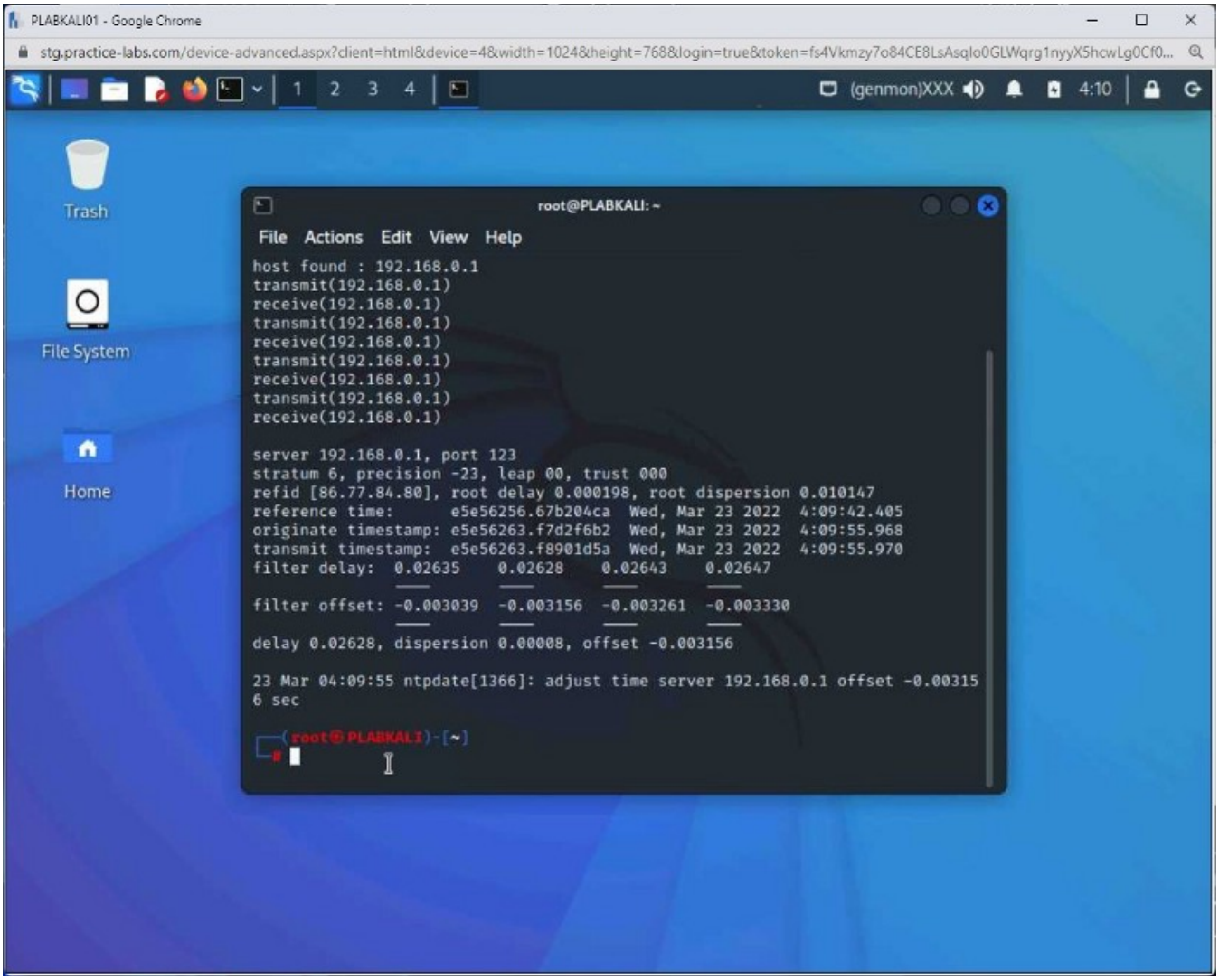
```
ntpdate -d 192.168.0.1
```

Press **Enter**.



Step 7

The output in the debug mode is displayed.



Keep the terminal window open.

Task 2 — Perform NTP enumeration using Nmap

You can use Nmap to perform NTP enumeration. Nmap contains a script named ntp-info.nse to get time and configuration information from a time server. The script returns the output that contains the port number and MAC address, which an attacker can use to further enumerate and exploit a server.

For example, an attacker can find the operating system (such as Windows), then the attacker can focus on further enumeration and find out the version of Windows Server. With a MAC address, an attacker can spoof the MAC address with their own system.

In this task, you will learn to perform NTP enumeration using Nmap.

Step 1

Connect to **PLABKALI01**. Ensure that the terminal window is open.

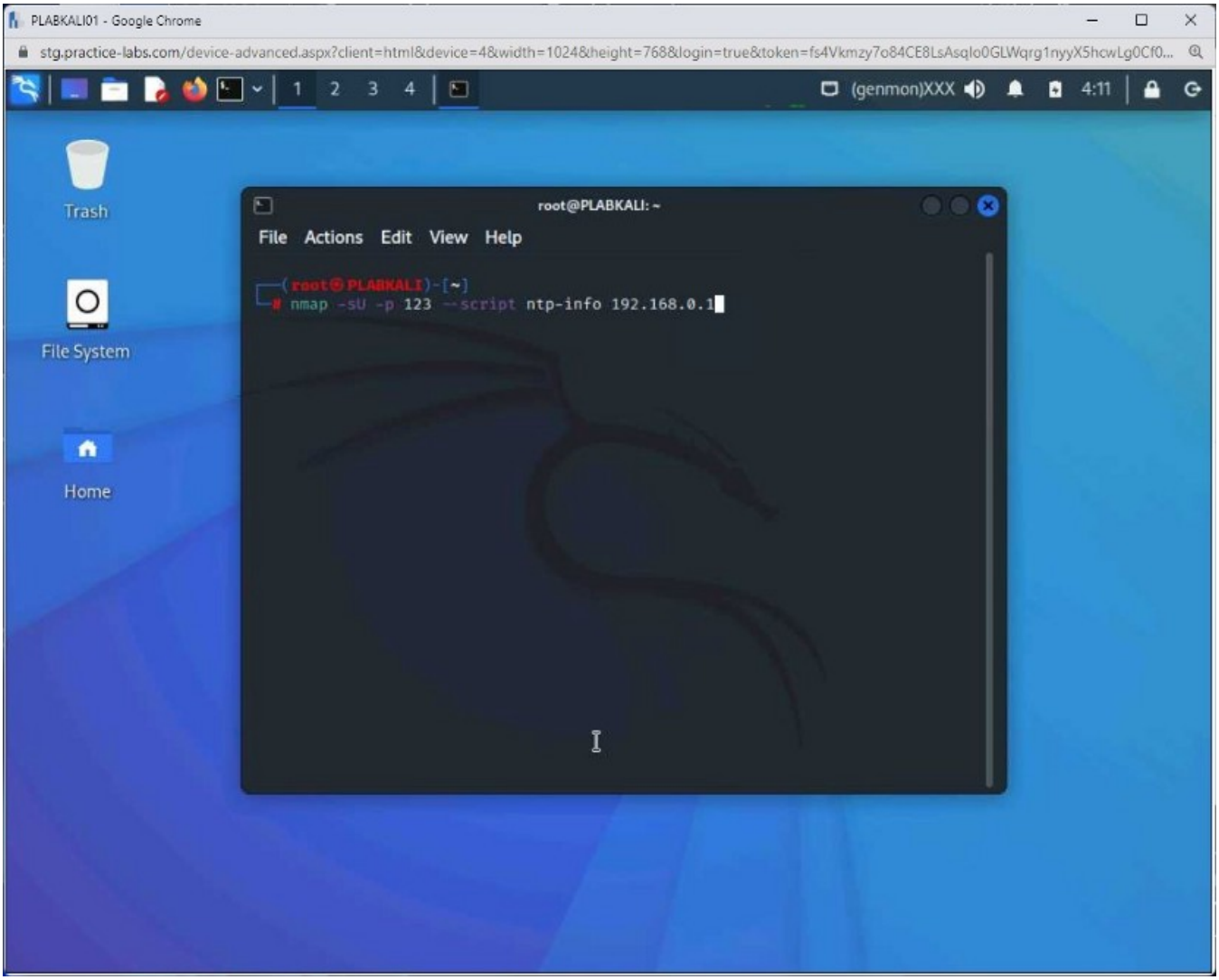
Clear the screen by entering the following command:

```
clear
```

Type the following command:

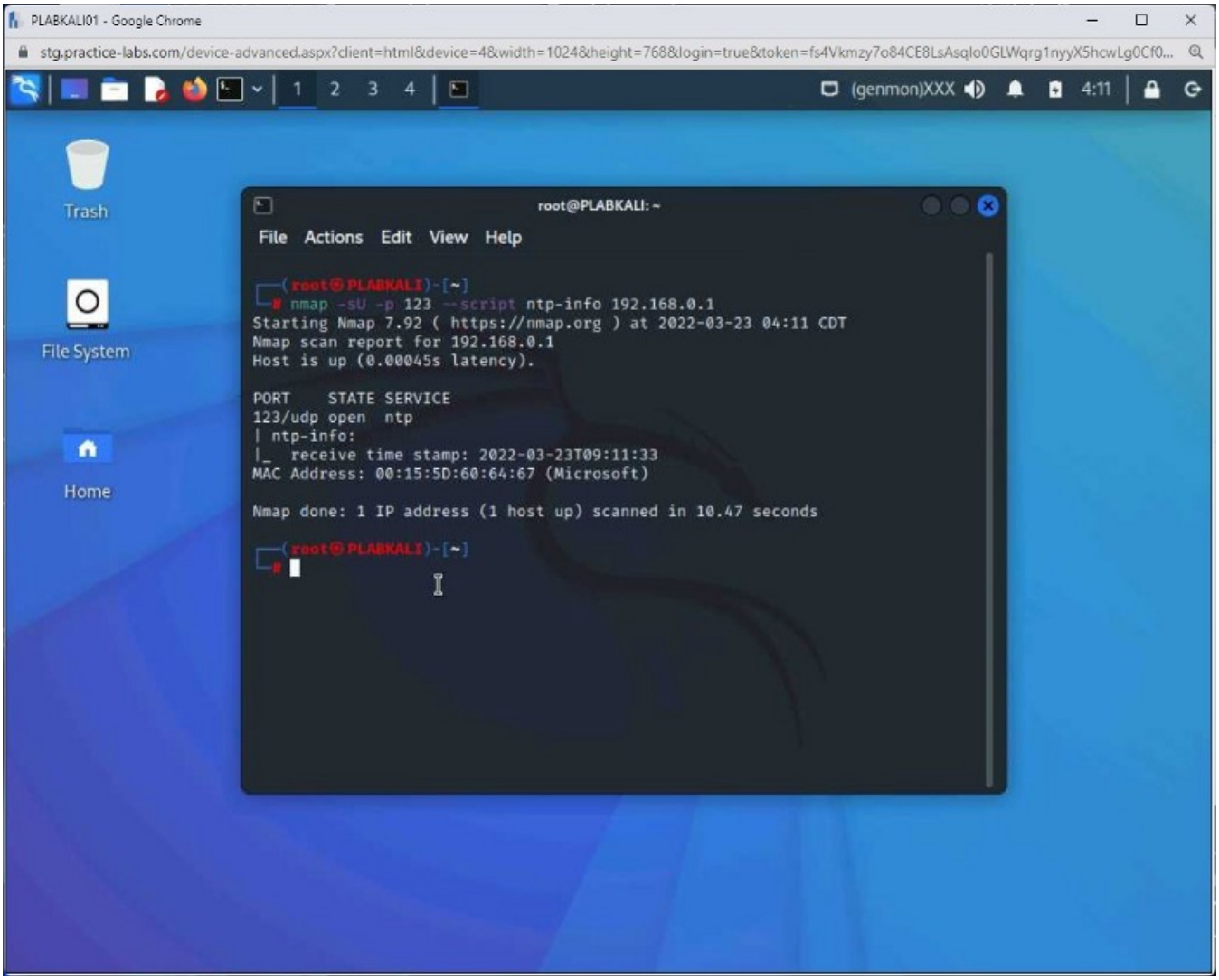
```
nmap -sU -p 123 --script ntp-info 192.168.0.1
```

Press **Enter**.



Step 2

The output of the command is displayed. The output indicates that it is a Microsoft-based time server.



Exercise 2 -DNS Enumeration

In DNS enumeration, an attacker copies the entire DNS zone file for a particular domain from the DNS server. When the attacker has the zone file, the attacker gets a lot of information, such as hostnames, IP addresses, usernames, and aliases.

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

Learning Outcomes

After completing this exercise, you will be able to:

- Perform DNS Enumeration

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

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

Task 1 — Perform DNS Enumeration

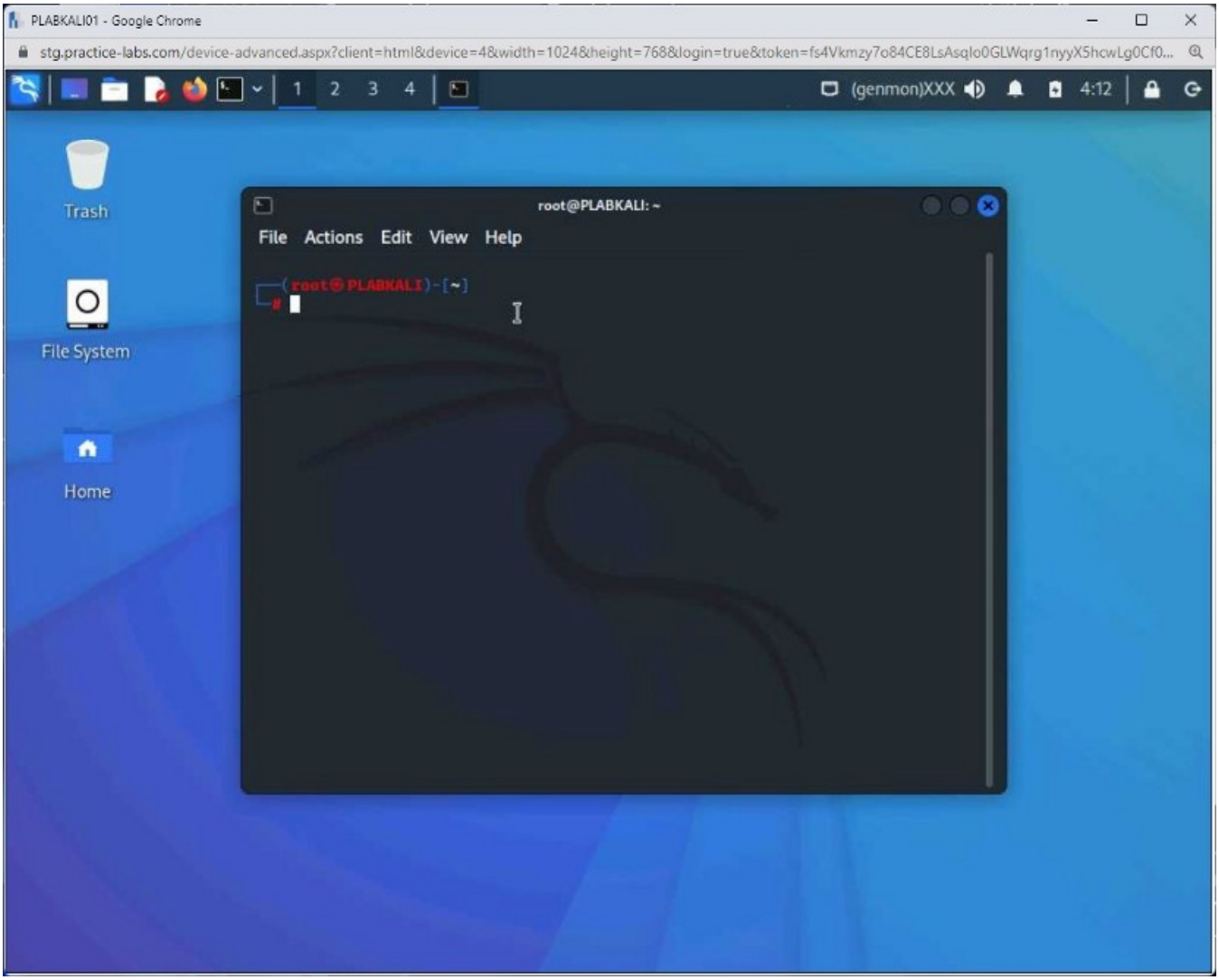
DNS plays a vital role on the Internet. It translates a domain name to an IP address. You can find information about DNS and mail servers for a specific domain by probing a DNS. In DNS enumeration, an attacker can attempt to perform a zone transfer so that a wealth of information can be retrieved. For example, if a DNS server allows zone transfers to any other DNS server, then an attacker can perform a zone transfer and get information on hostnames, IP addresses, and aliases from for a specific domain of which the zone transfer has taken place.

There are several tools that the attacker can use to perform a zone transfer. Some of the key tools are nslookup, dig, and DNSRecon. The host command can also provide a lot of information, such as SOA records of the authoritative nameservers or print the IP addresses of a specific domain.

In this task, you will perform DNS enumeration. To do this, perform the following steps:

Step 1

Reconnect to **PLABKALI01** and open a new terminal window.



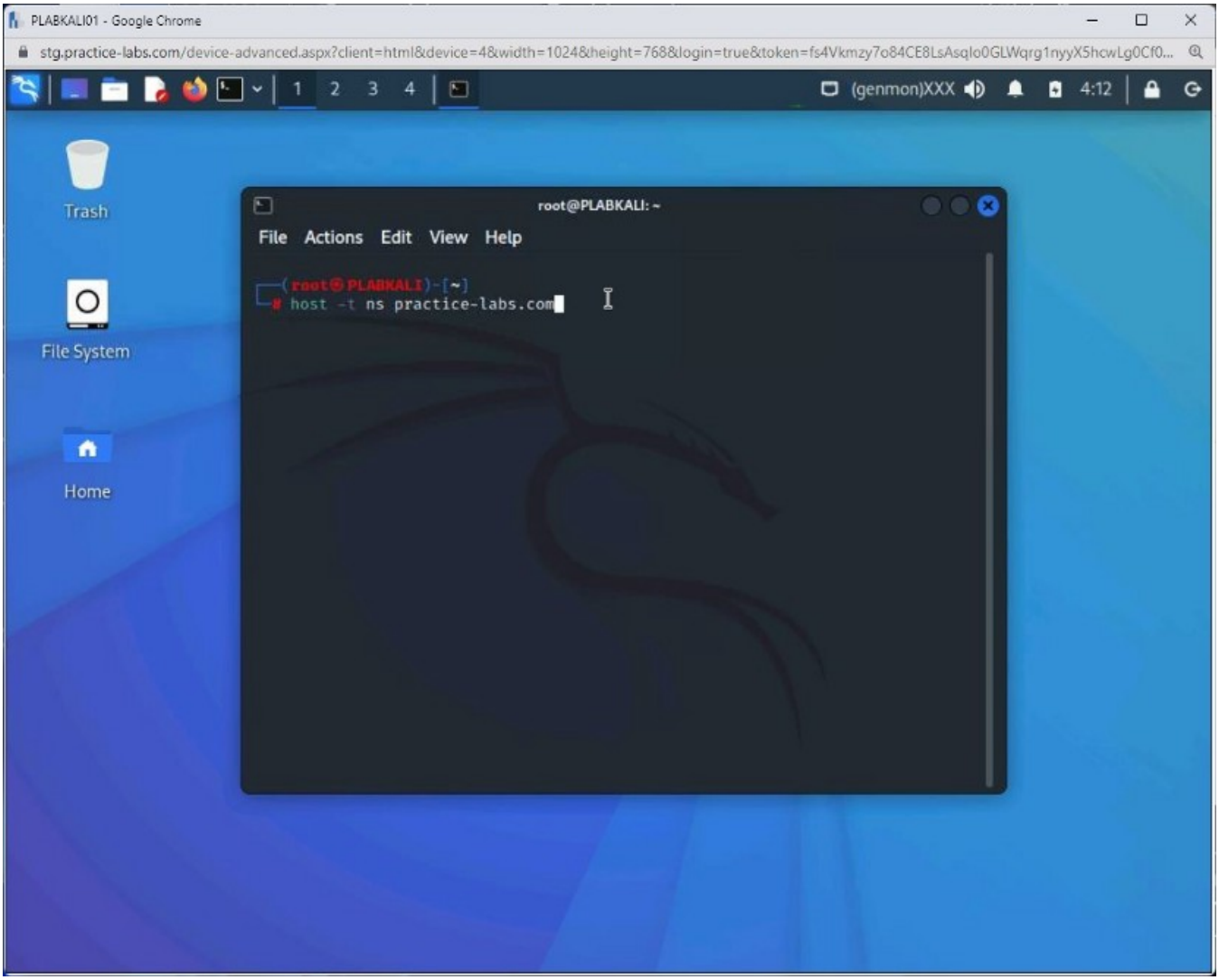
Step 2

The terminal window is displayed. Let's first find the nameserver for the **practice-labs.com** domain.

You can use the **host** command with the **-t** parameter to do the same. The **ns** parameter is for the nameserver. Type the following command:

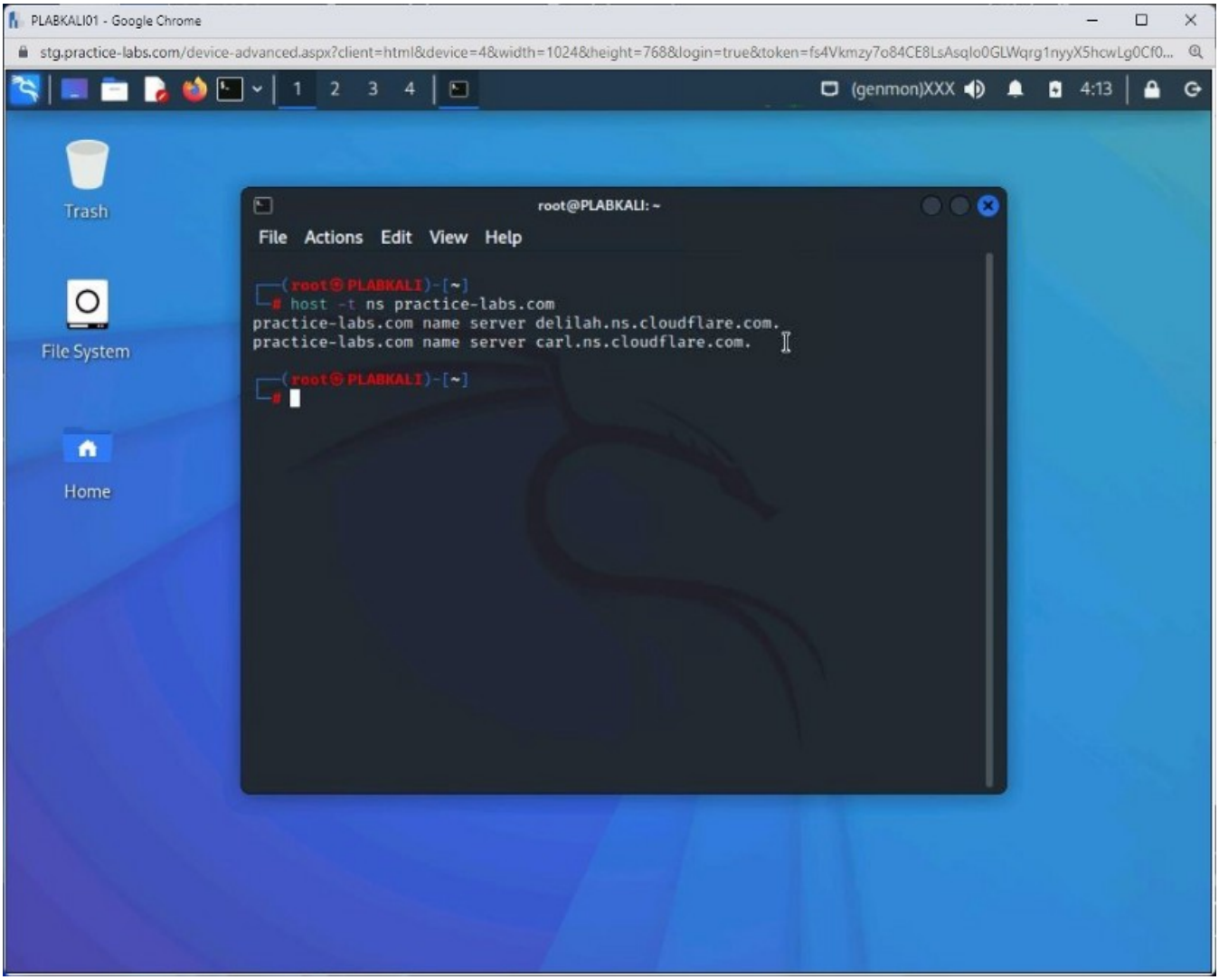
```
host -t ns practice-labs.com
```

Press **Enter**.



Step 3

Notice that the **name** server details are displayed.



Step 4

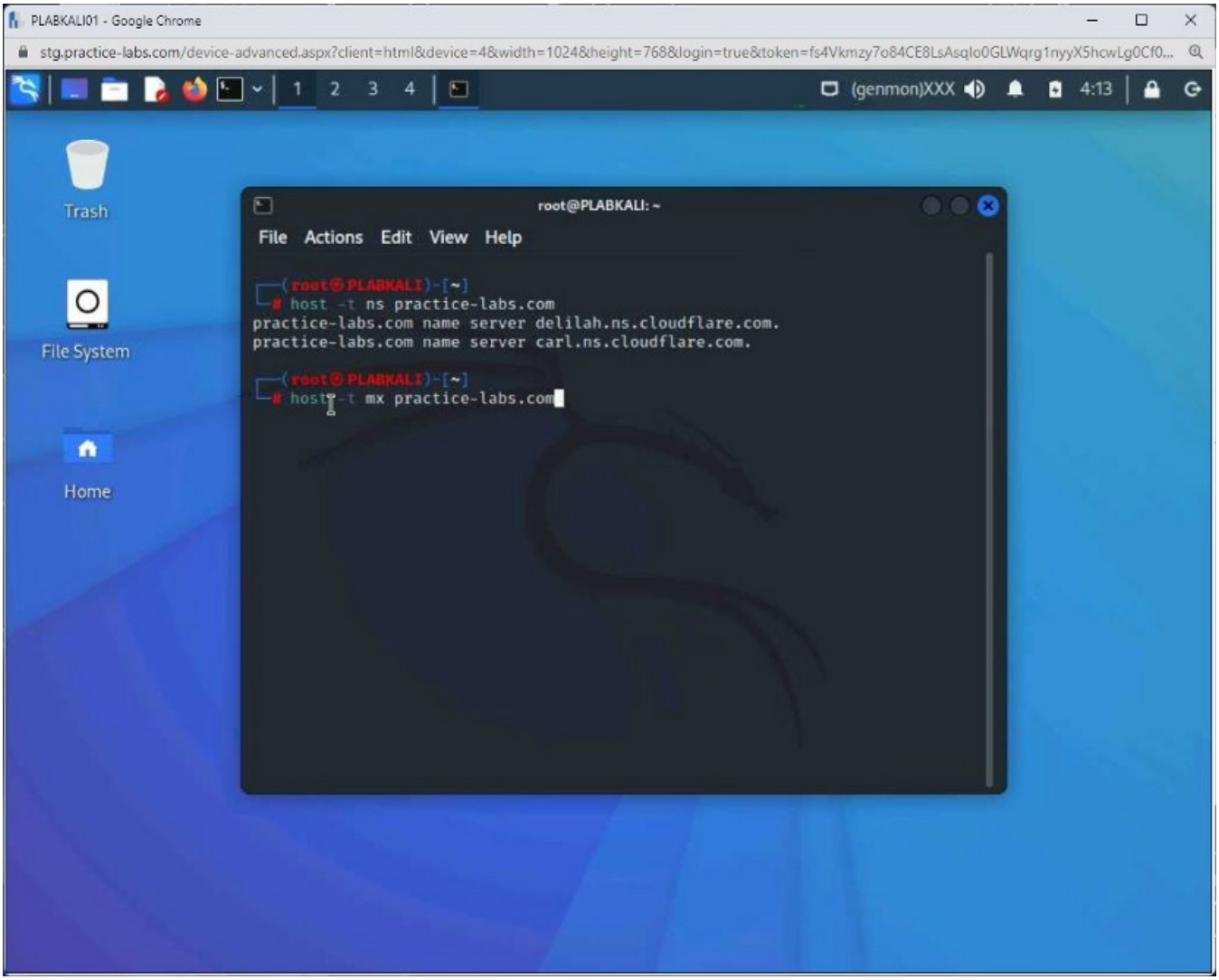
Let's now find the mail server for the **practice-labs.com** domain. You can use the host command with the **-t** parameter to do the same.

The **mx** parameter is for the mail server.

Type the following command:

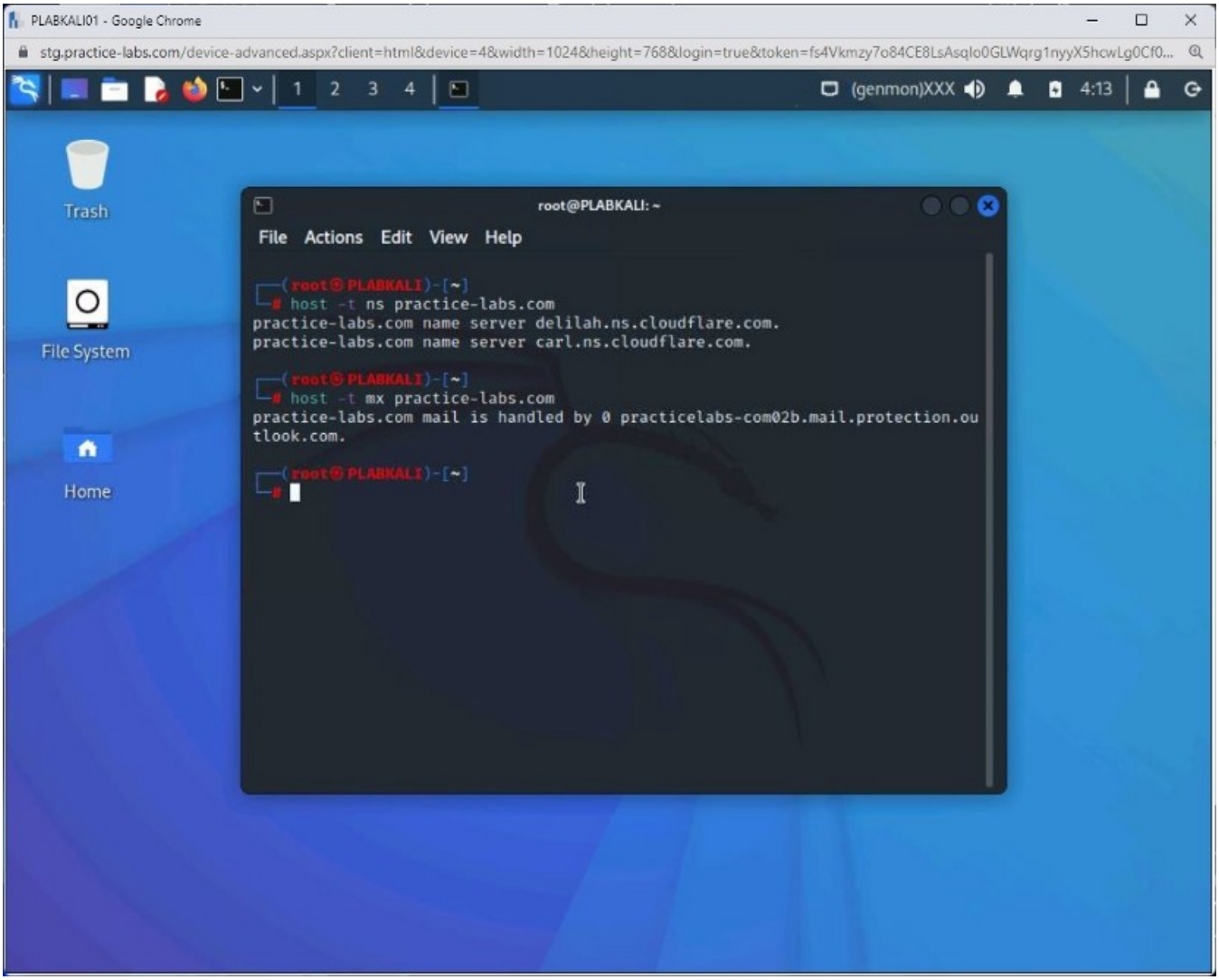
```
host -t mx practice-labs.com
```

Press **Enter**.



Step 5

Notice that in the output there is an **Outlook** server response.



Step 6

Clear the screen by entering the following command:

```
clear
```

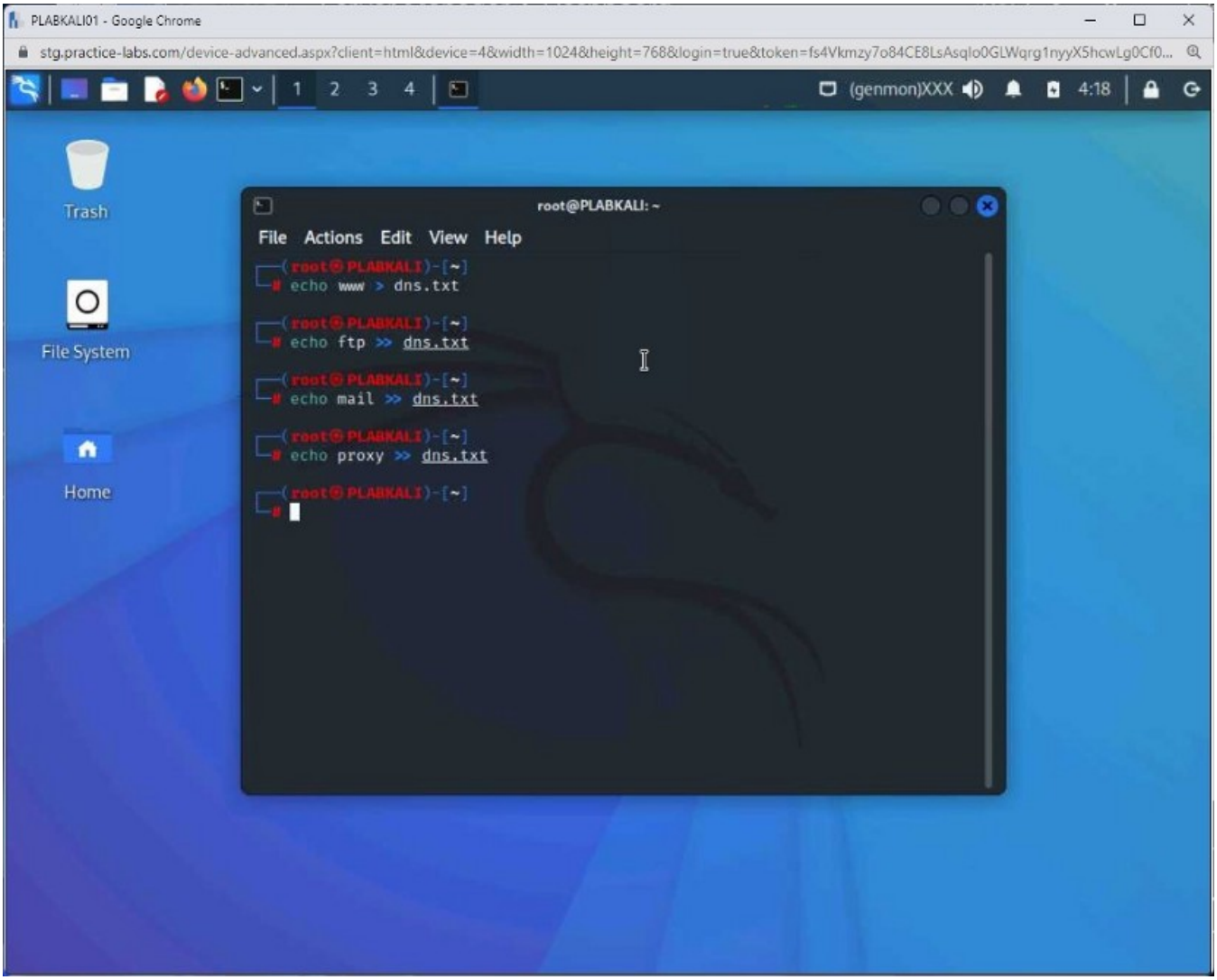
You will now gather the information about various services in a text file named **dns.txt**. Later, you will create a loop with the hostname and display the details of each service if it exists.

Note: *The first command will write the output of the echo command in a file named dns.txt using the > operator. The second to the last command will append the output to the plab.txt file using the >> operator.*

Type the following commands:

```
echo www > dns.txt
echo ftp >> dns.txt
echo mail >> dns.txt
echo proxy >> dns.txt
```

Press **Enter** after each command.



Step 7

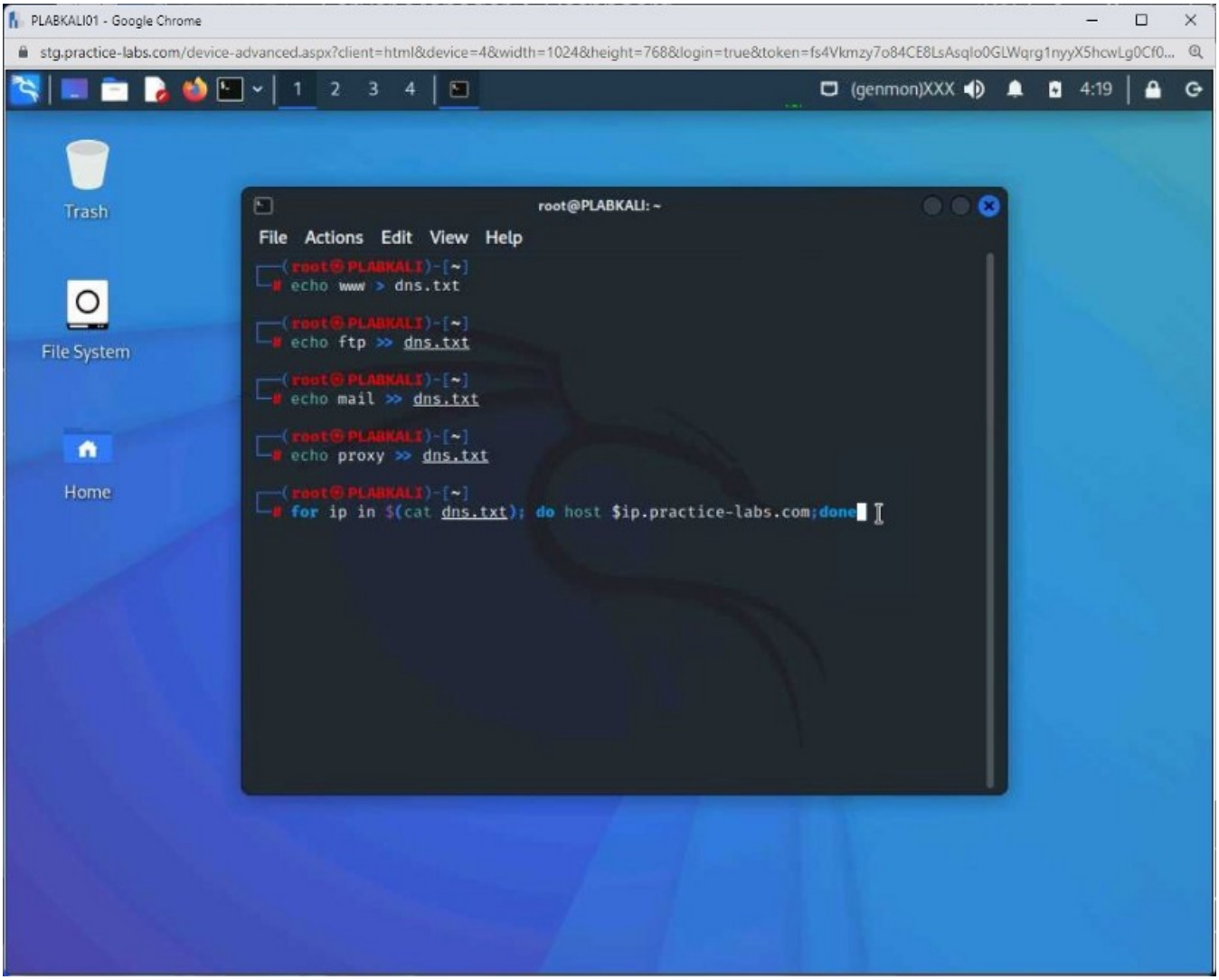
Next, you will create a for loop to generate the list of services with their IP addresses. In this command, you automate the **Forward DNS Lookup** using the host command.

You can attempt to guess valid names for the servers using this script. For example, if there is a web server configured for practice-labs.com, you will be able to find it using this script.

Type the following command:

```
for ip in $(cat dns.txt); do host $ip.practice-labs.com;done
```

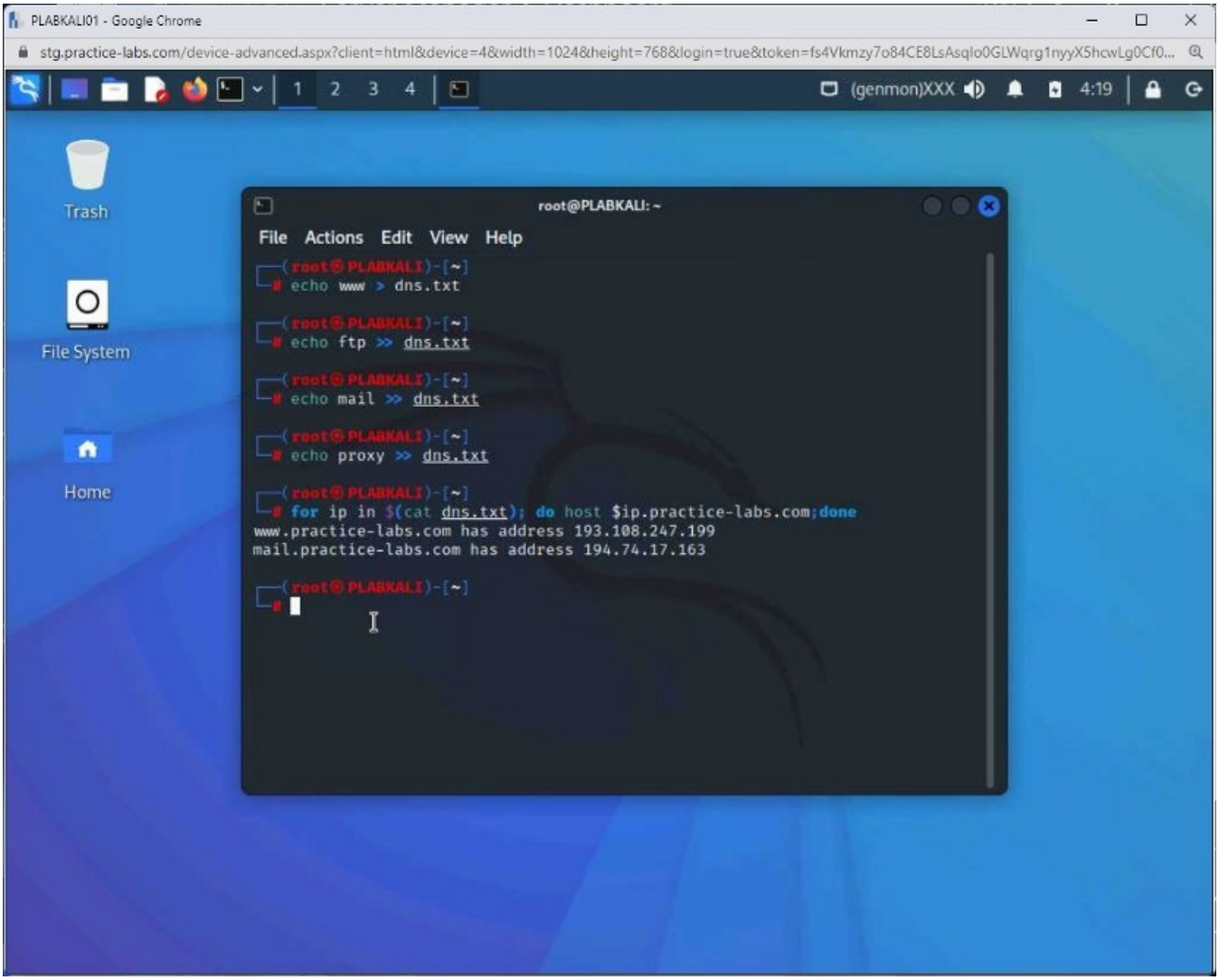
Press **Enter**.



Step 8

Notice the output of the loop.

Two services were found, the domain and the mail server.



Step 9

Clear the screen by entering the following command:

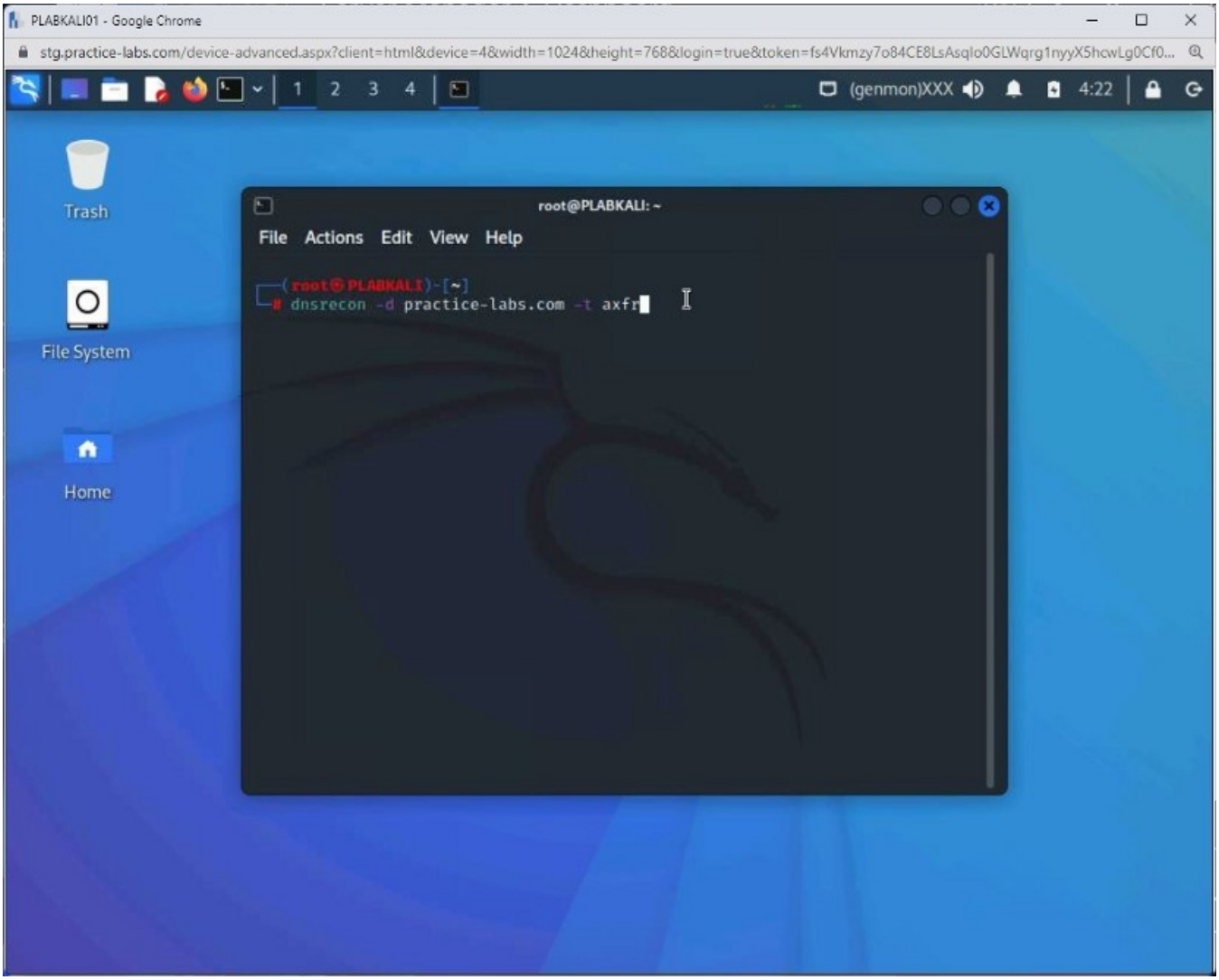
```
clear
```

Kali Linux also contains a DNS enumeration tool named **DNSRecon**. To use **DNSRecon**, type the following command:

Note: *The -d parameter defines the domain name. The -t parameter defines the type of enumeration.*

```
dnsrecon -d practice-labs.com -t axfr
```

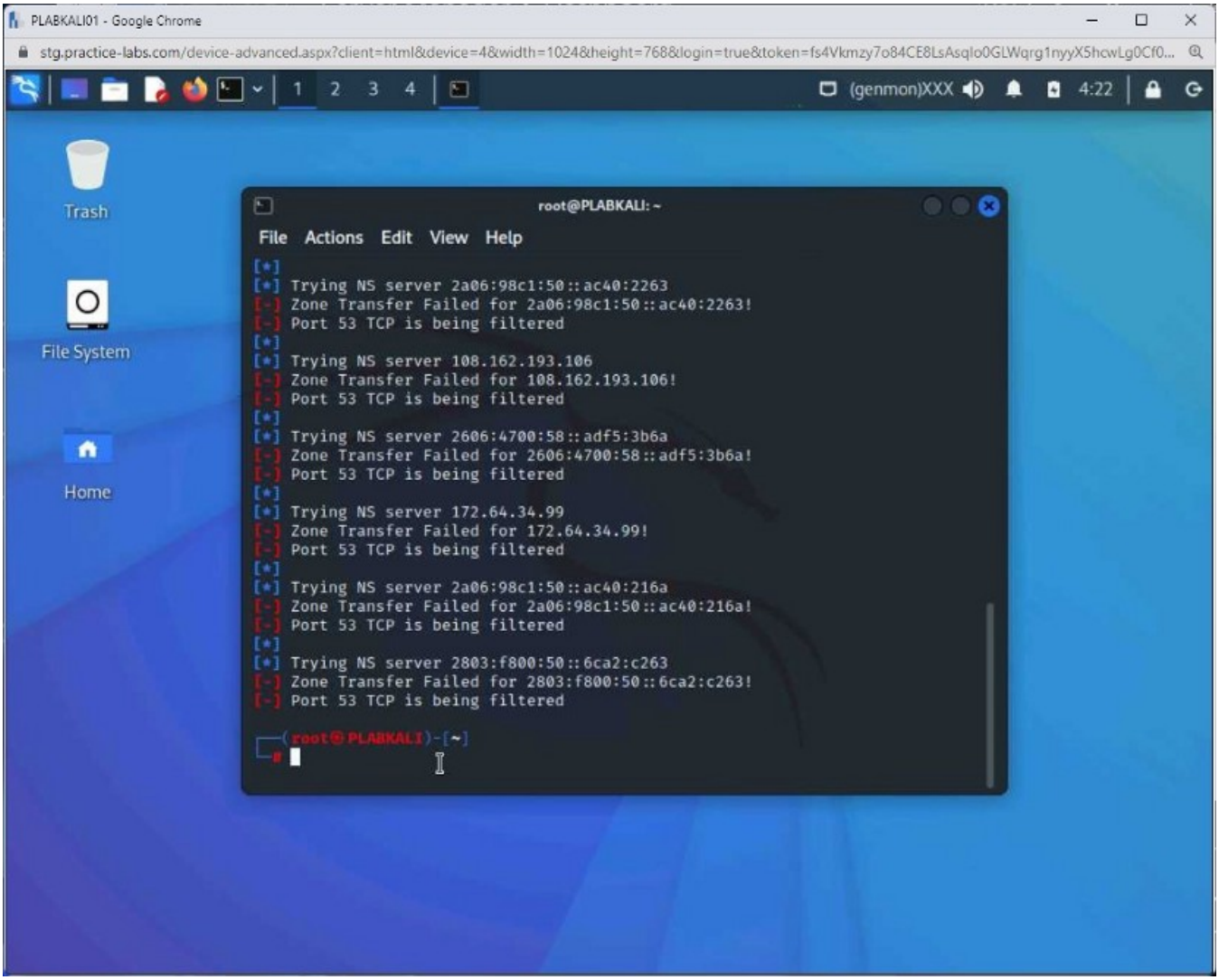
Press **Enter**.



Step 10

Notice the output of this command. It tests the zone transfer, which fails, and lists the **Name** servers.

It also provides open ports on the server.



Step 11

Clear the screen by entering the following command:

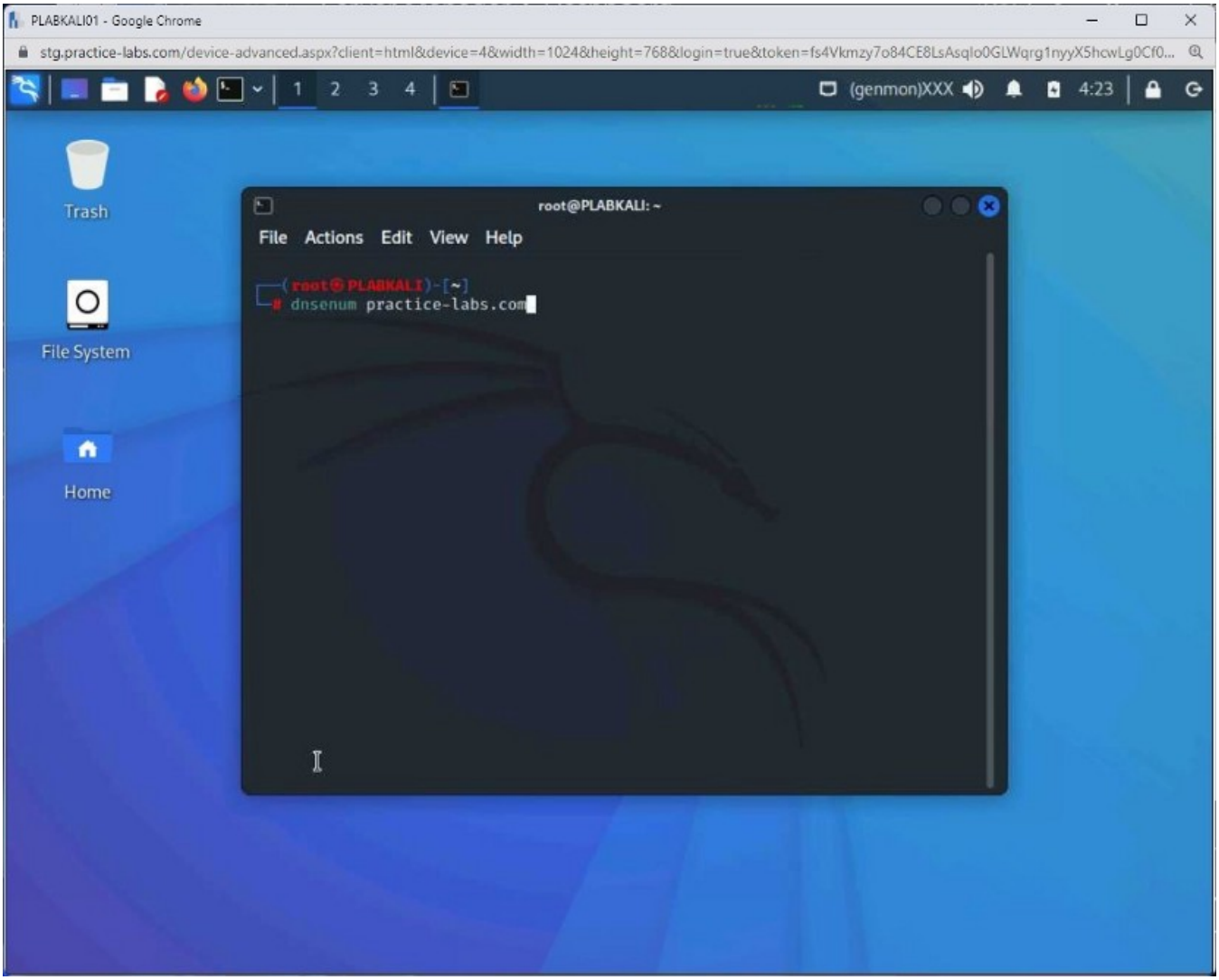
```
clear
```

Next, you can also use another tool named **DNSEnum**, which provides similar information to the **DNSRecon** tool.

Type the following command:

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

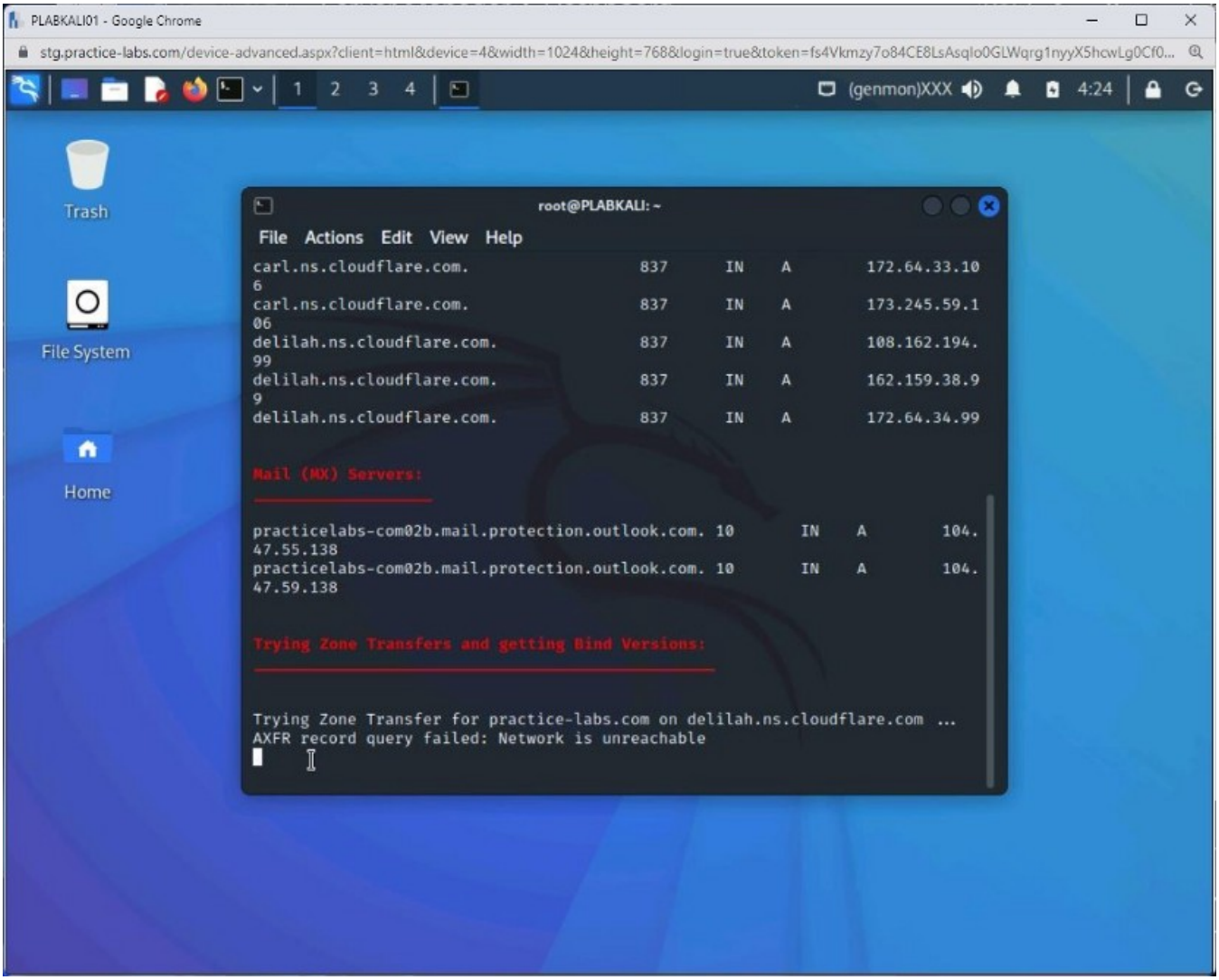
Press **Enter**.



Step 12

Notice the output nameserver name and IP address, and mail server. It also shows zone transfer results, which in this case is unreachable.

***Note**: The command may take some time to fully execute. To escape the command, press **Control** + **C**.*



Exercise 3 — Other Enumeration Techniques

An attacker can use various enumeration techniques or methods to gain information to initiate an attack. To enumerate information, an attacker can target Telnet, FTP, TFTP, SMB, and BGP protocols.

However, it all depends on the attacker's needs and objectives to use a specific type of enumeration technique. In this exercise, you will learn about various other types of enumeration techniques.

Learning Outcomes

After completing this exercise, you will be able to:

- Perform Server Message Block (SMB) Enumeration
- Perform Windows Host Enumeration Using rpcclient
- Perform Linux Host Enumeration using Nmap

- Use Hyena for Enumeration
- Perform Website Enumeration using Nmap

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

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

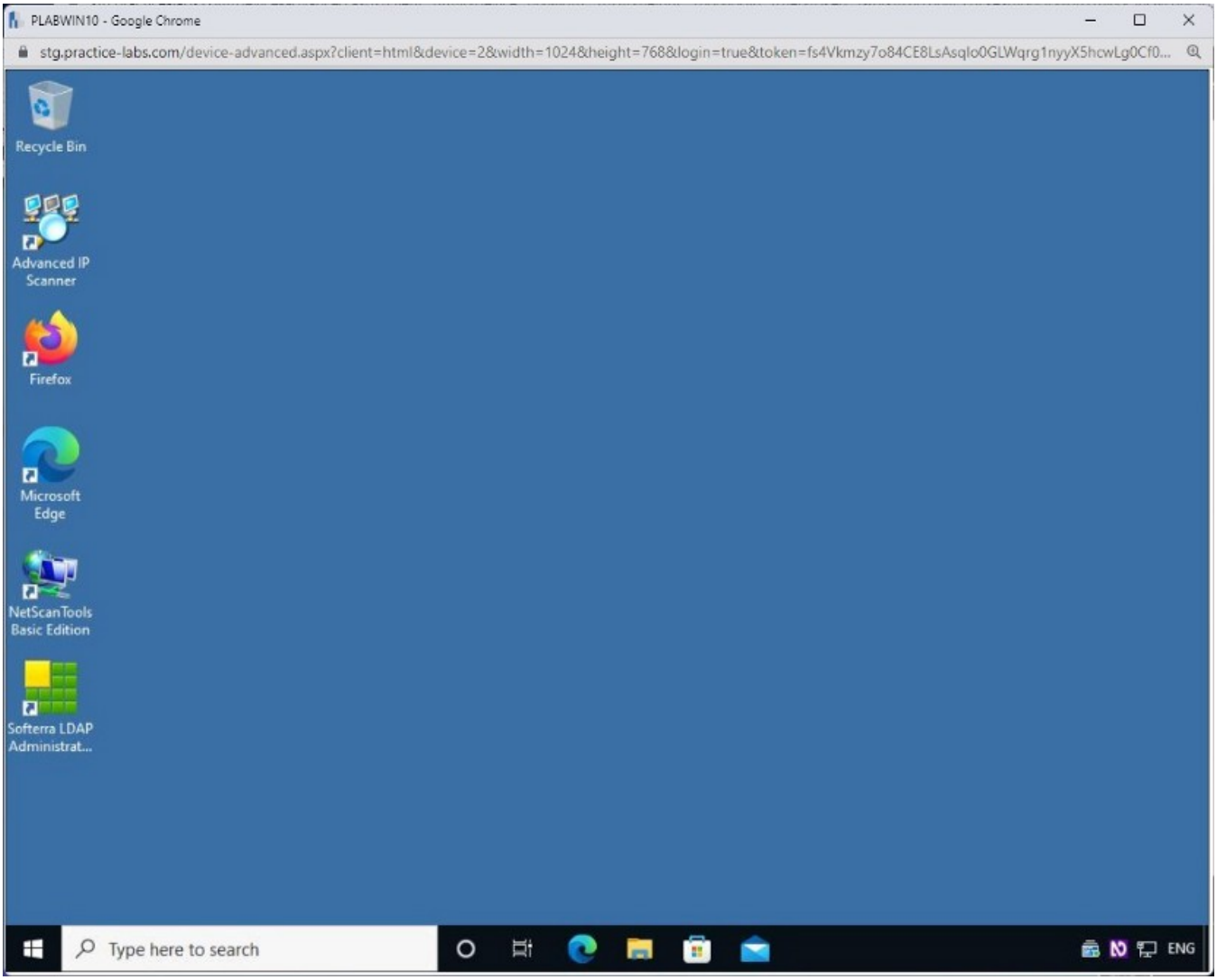
Task 1 — Disabling the Windows 10 Firewall

Before performing the following types of enumeration, you will need to switch off the **Windows Firewall** on **PLABWIN10**.

To switch off the **Windows Firewall** on **PLABWIN10**, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction, and that you have connected to **PLABWIN10**. The desktop is displayed.

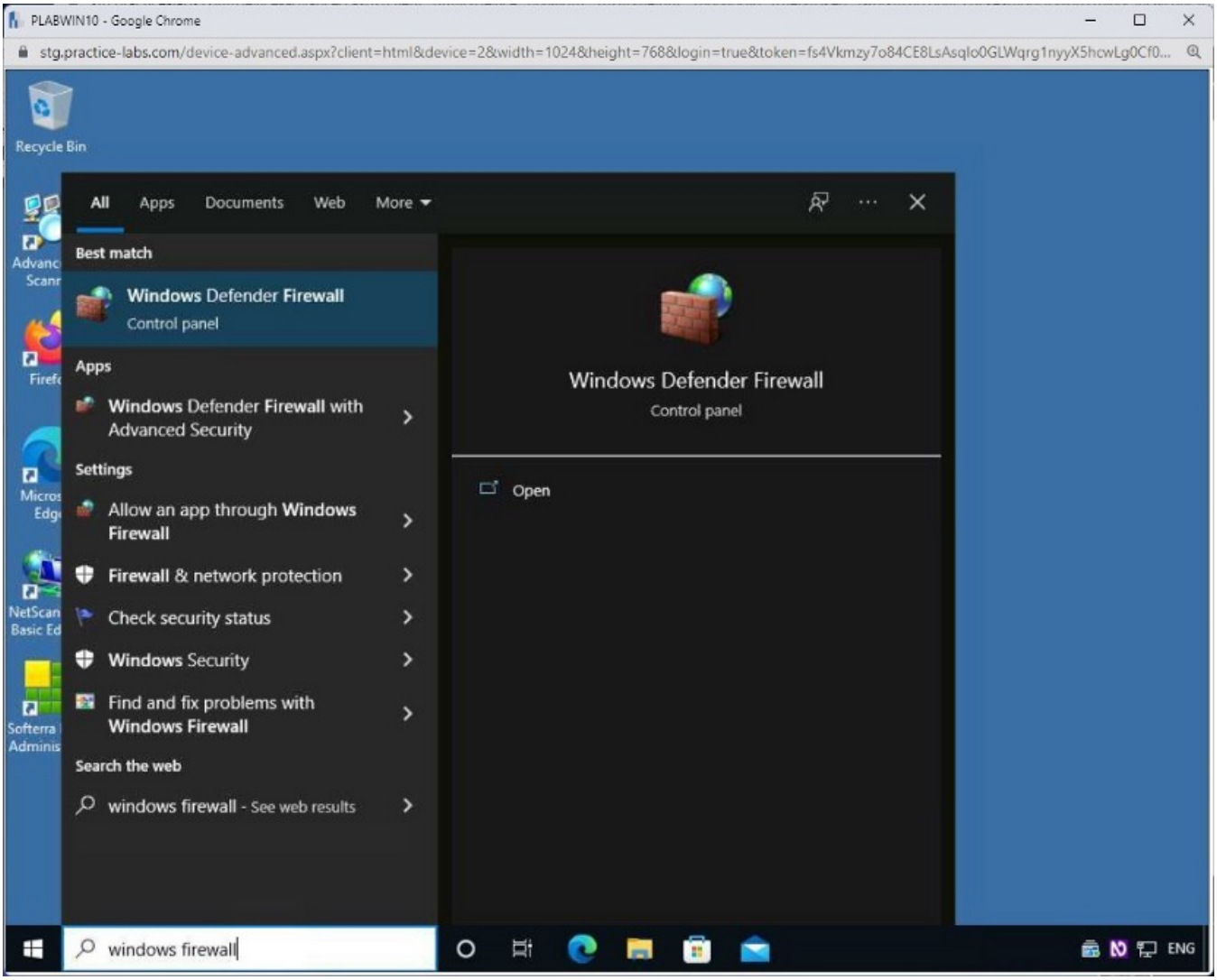


Step 2

In the **Type here to search** text box, type the following:

```
windows firewall
```

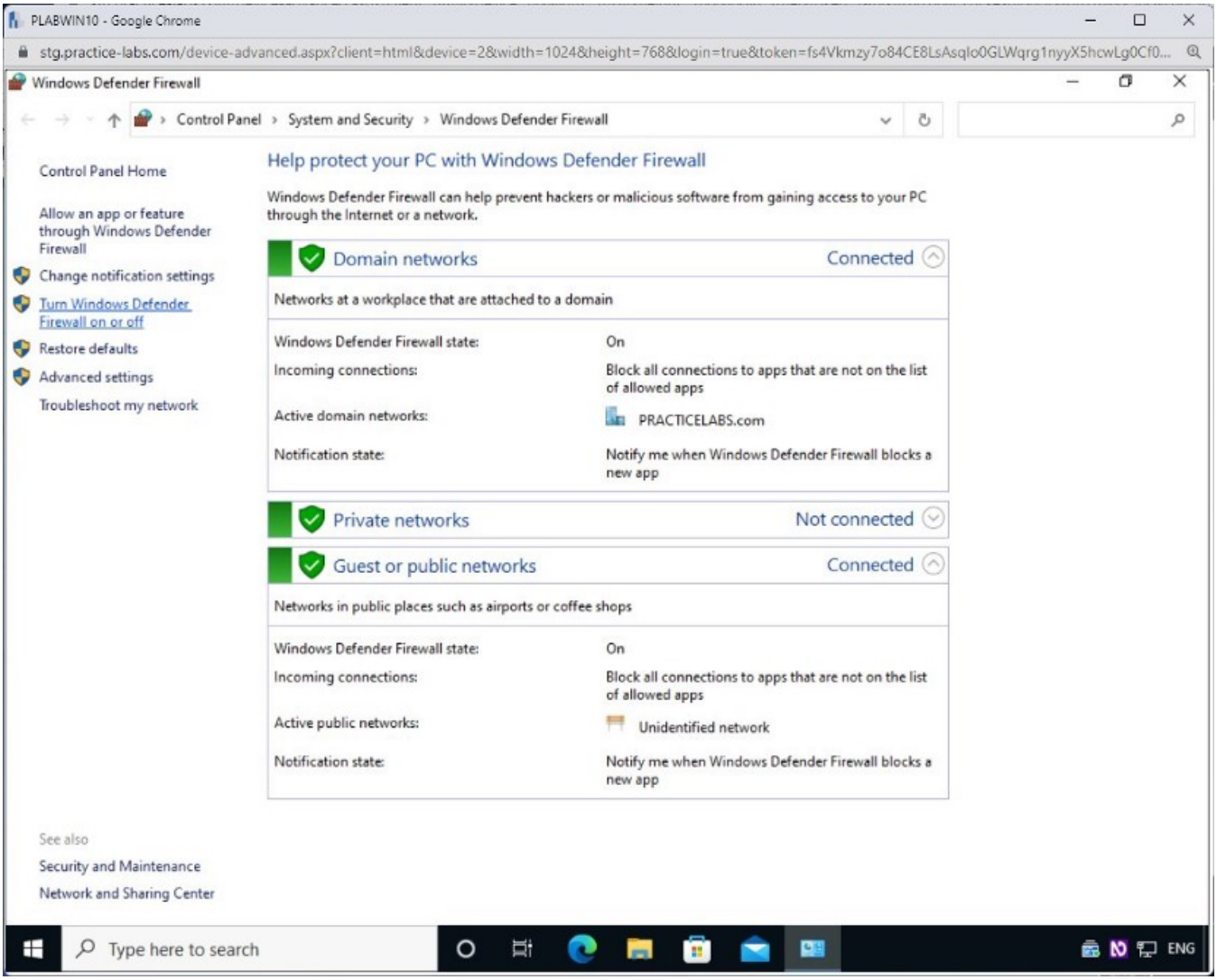
From the search results, select the **Windows Defender Firewall**.



Step 3

The **Windows Defender Firewall** window is displayed.

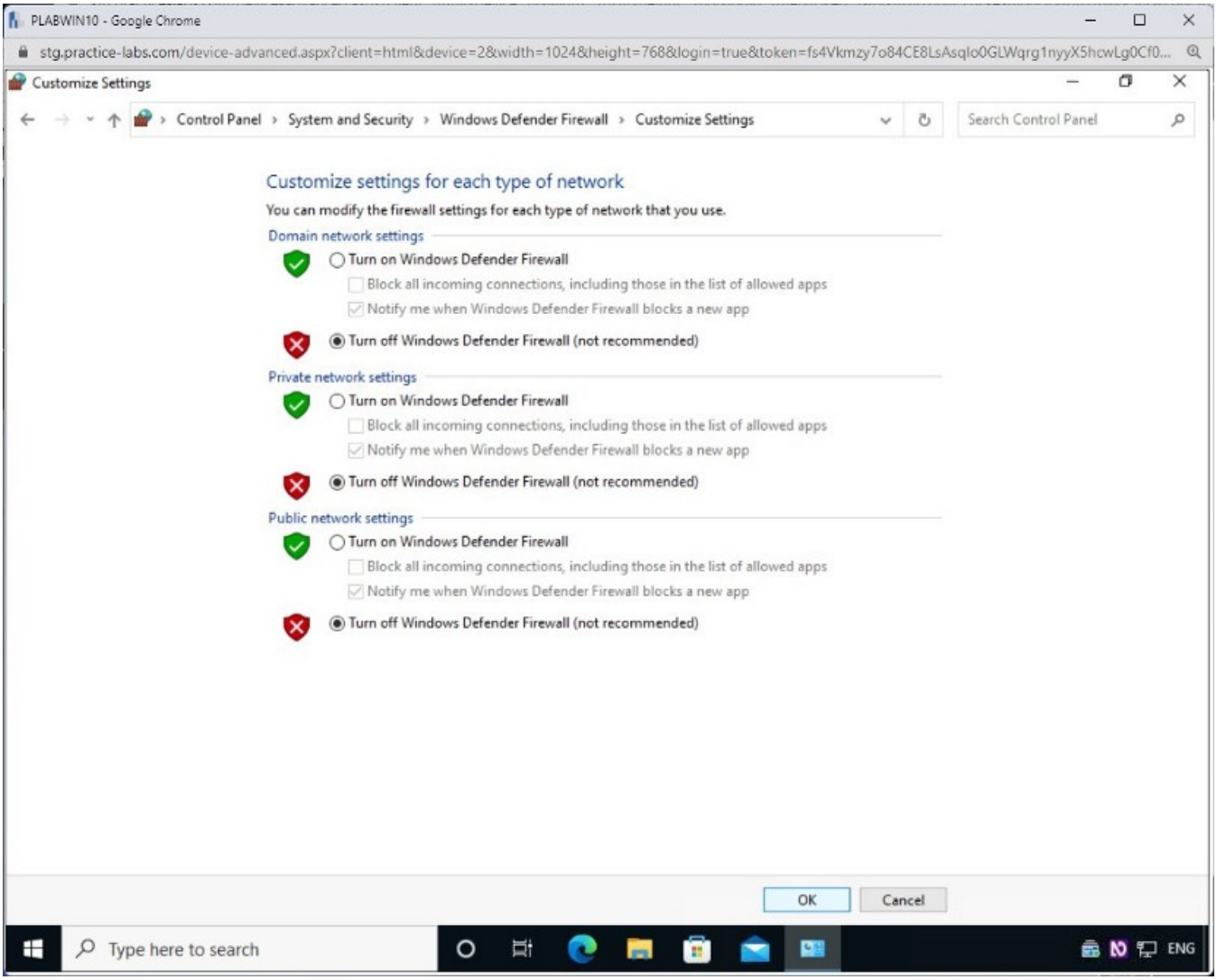
On the **Help protect your PC with Windows Defender Firewall** page, click **Turn Windows Defender Firewall on or off** in the left-hand pane.



Step 4

On the **Customize settings for each type of network** page, select **Turn off Windows Defender Firewall (not recommended)** for **Domain**, **Private**, and **Public** network.

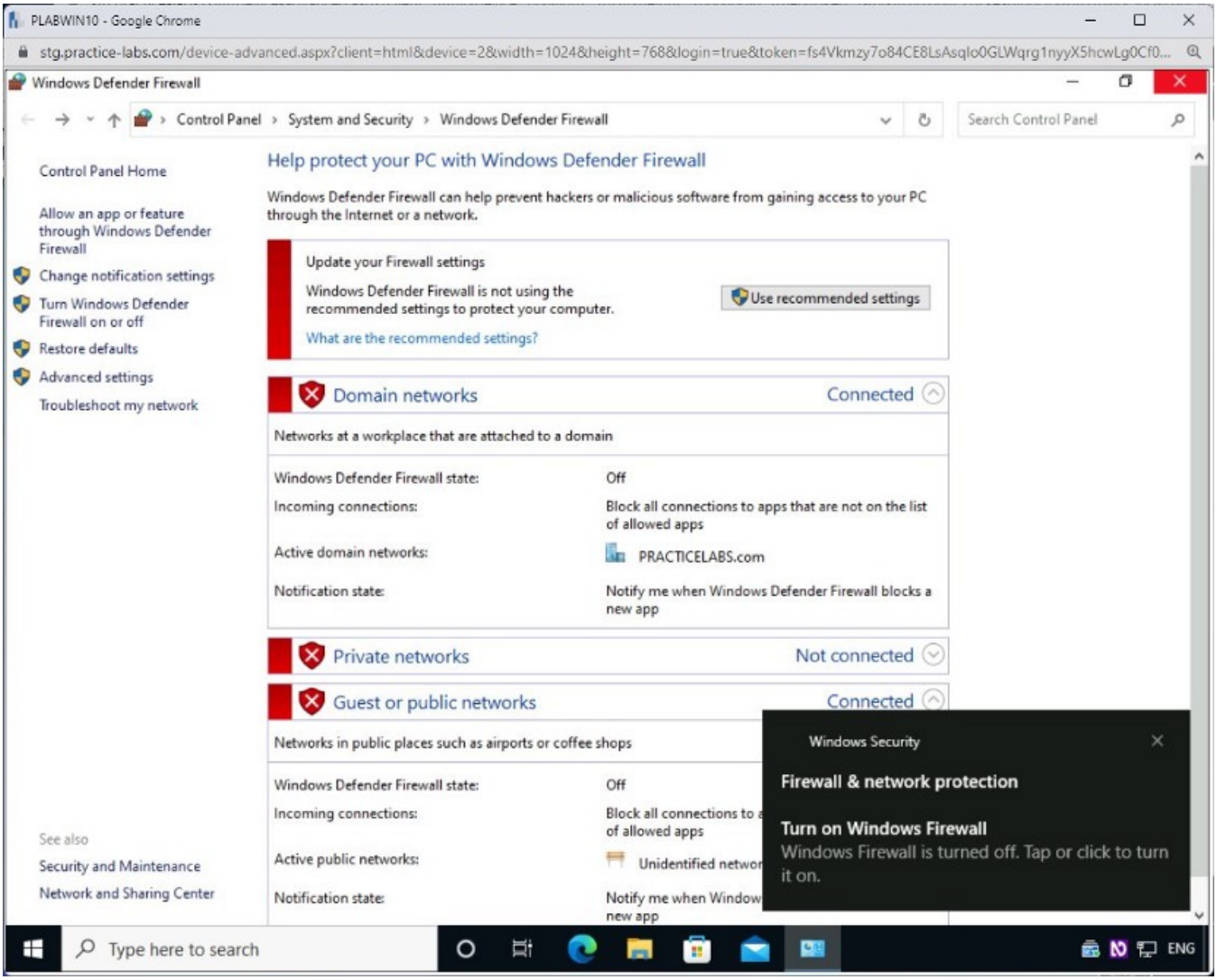
Click **OK**.



Step 5

On the **Help protect your PC with Windows Defender Firewall** page, notice that **Windows Defender Firewall** is now turned off for **Domain**, **Private**, and **Public** networks.

Close the **Control Panel** window and the **PLABWIN10** window.



Task 2 — Perform Server Message Block (SMB) Enumeration

Operating systems use the SMB protocol to share files and printers. It is known to be a weak protocol, and various versions have been included in different versions of Windows.

- **SMB1** — Windows 2000, Windows XP, and Windows Server 2003
- **SMB2** — Windows Vista SP1 and Windows Server 2008
- **SMB2.1** — Windows 7 and Windows Server 2008 R2
- **SMB3** — Windows 8 and above, Windows Server 2012 and above

When a network runs the SMB service, it can provide a great deal of information about a target network. For instance, an attacker can perform banner grabbing to get the operating system details. Based on the information collected in enumeration, the attacker can conduct various types of attacks, such as SMB relay attacks.

In this task, you will perform SMB enumeration. To do this, perform the following steps:

Step 1

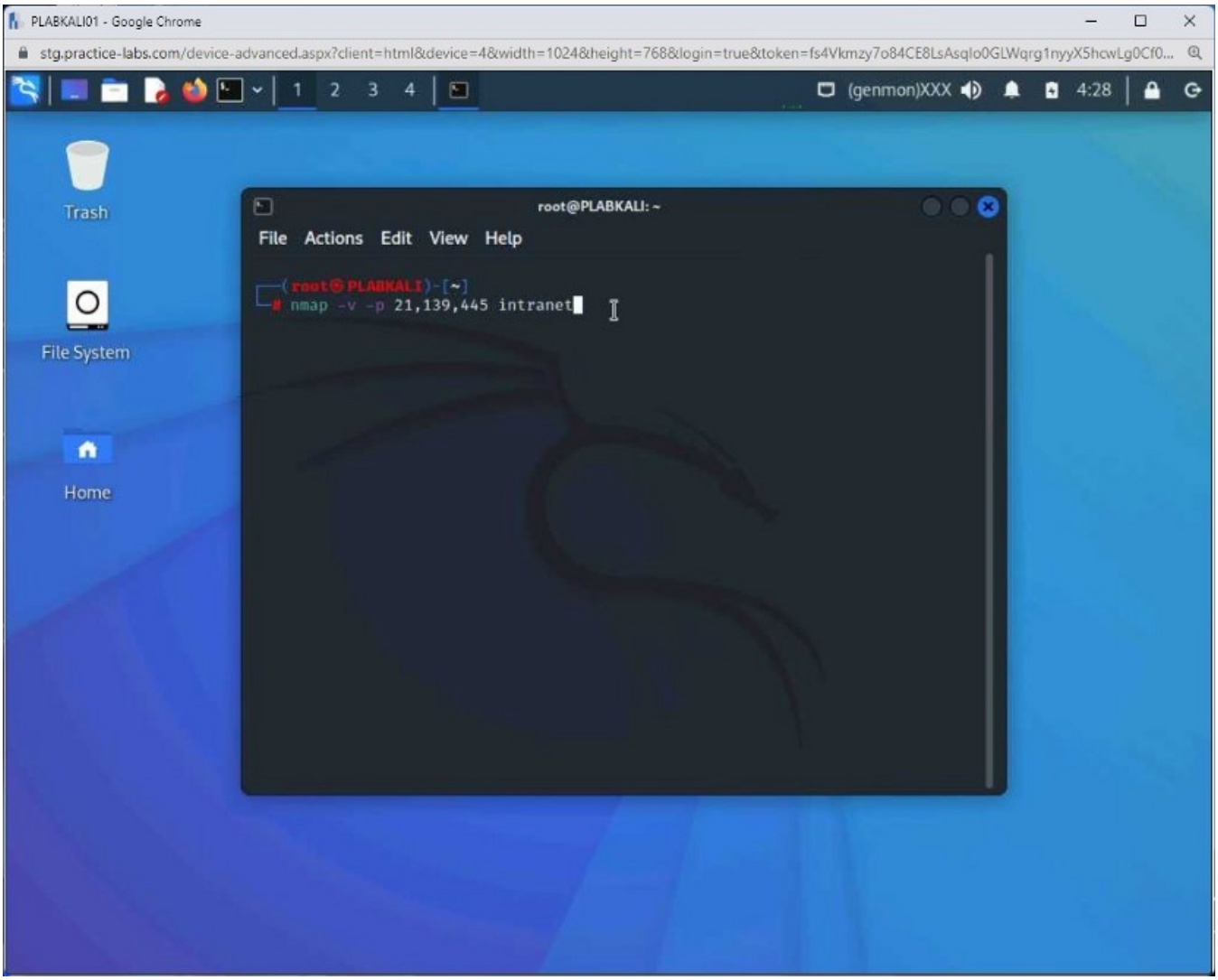
Reconnect to **PLABKALI01** and open a new terminal window.

You can use **Nmap** to perform **SMB NetBIOS** enumeration. To do this, type the following command:

Note: *SMB uses TCP ports 139 and 445. When using the nmap command, you should specify both ports.*

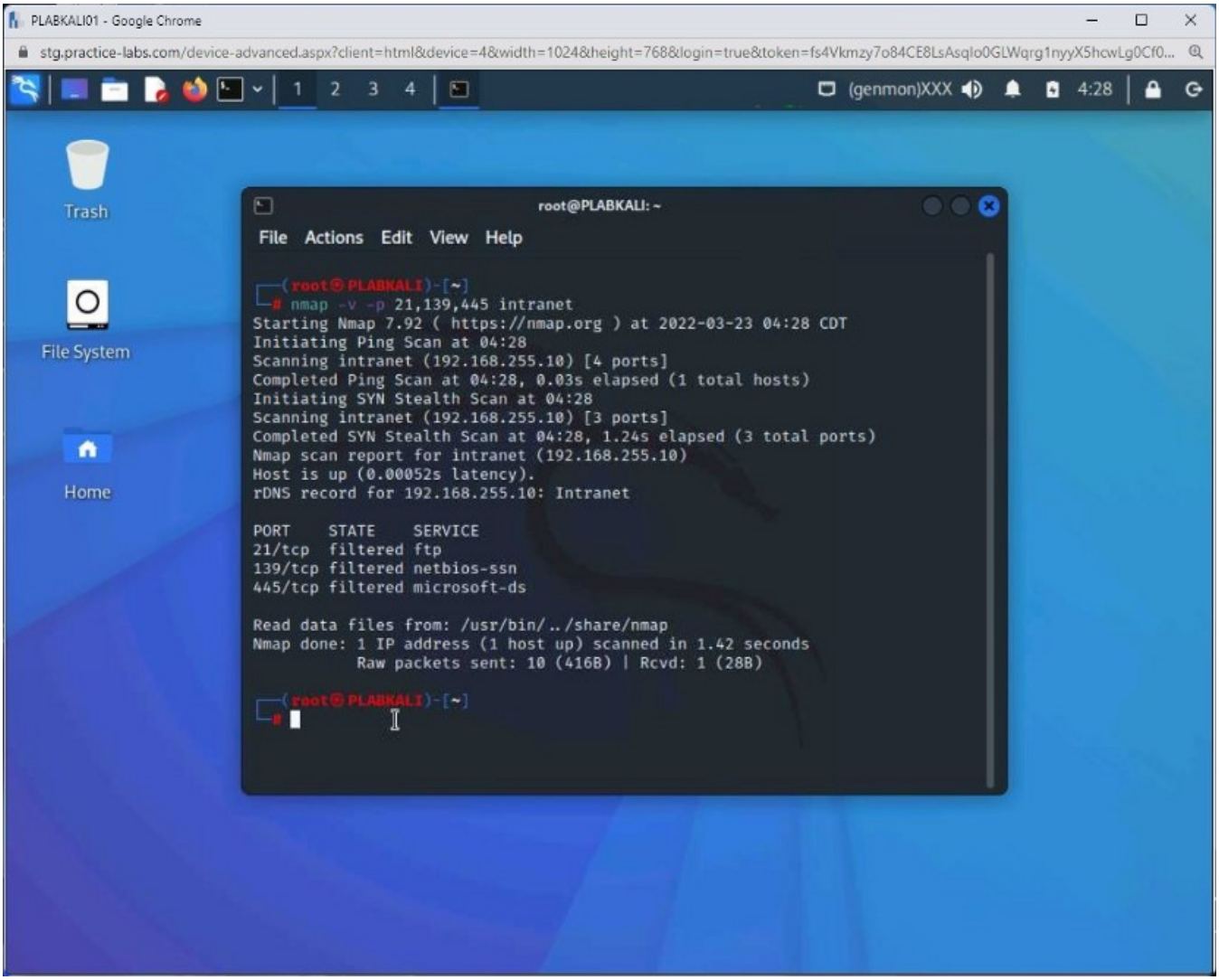
```
nmap -v -p 21,139,445 intranet
```

Press **Enter**.



Step 2

Notice the outcome of this command. All three ports were found as filtered.



Step 3

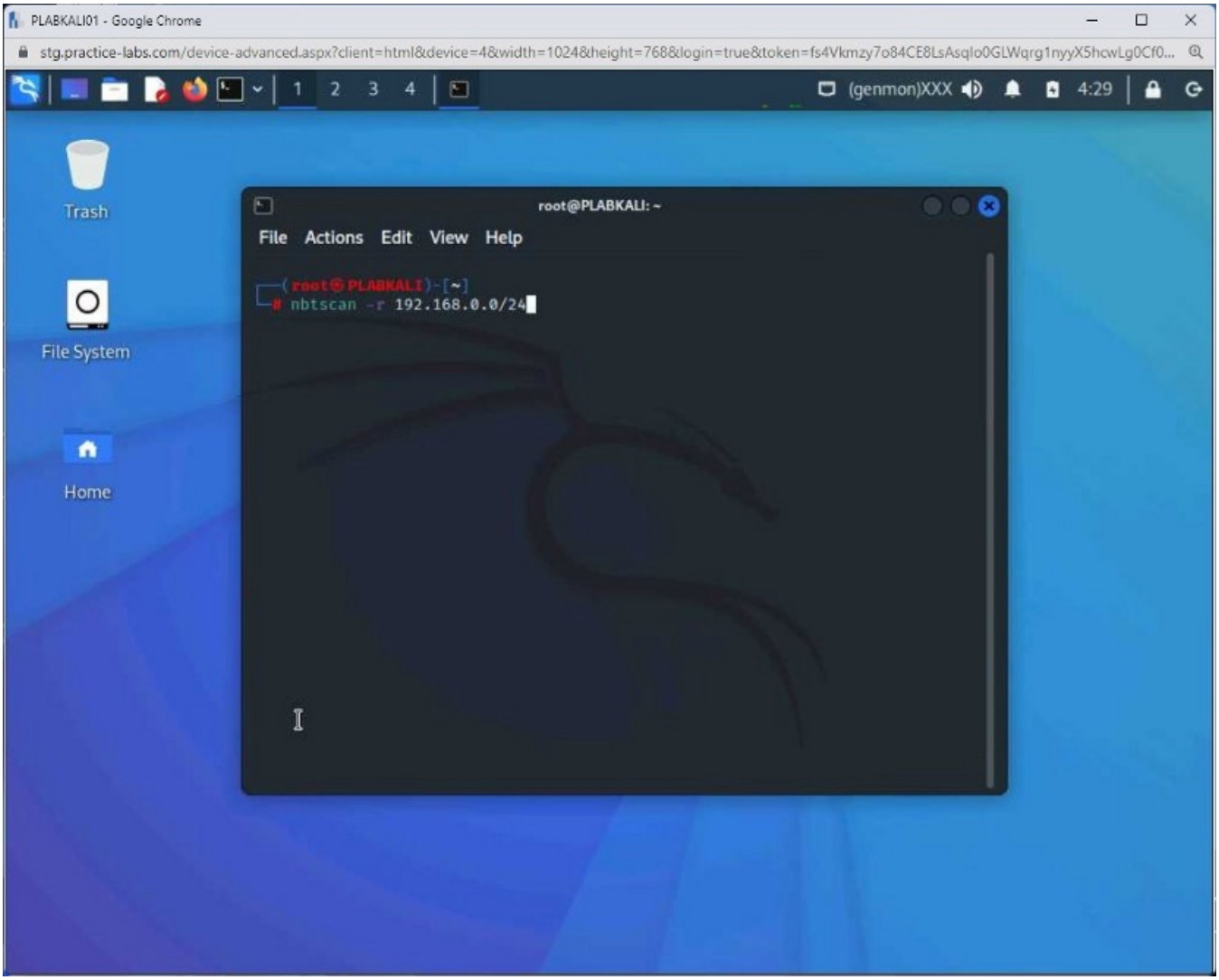
Clear the screen by entering the following command:

```
clear
```

To identify the **NetBIOS** information, you can use the **nbtscan** command. Type the following command:

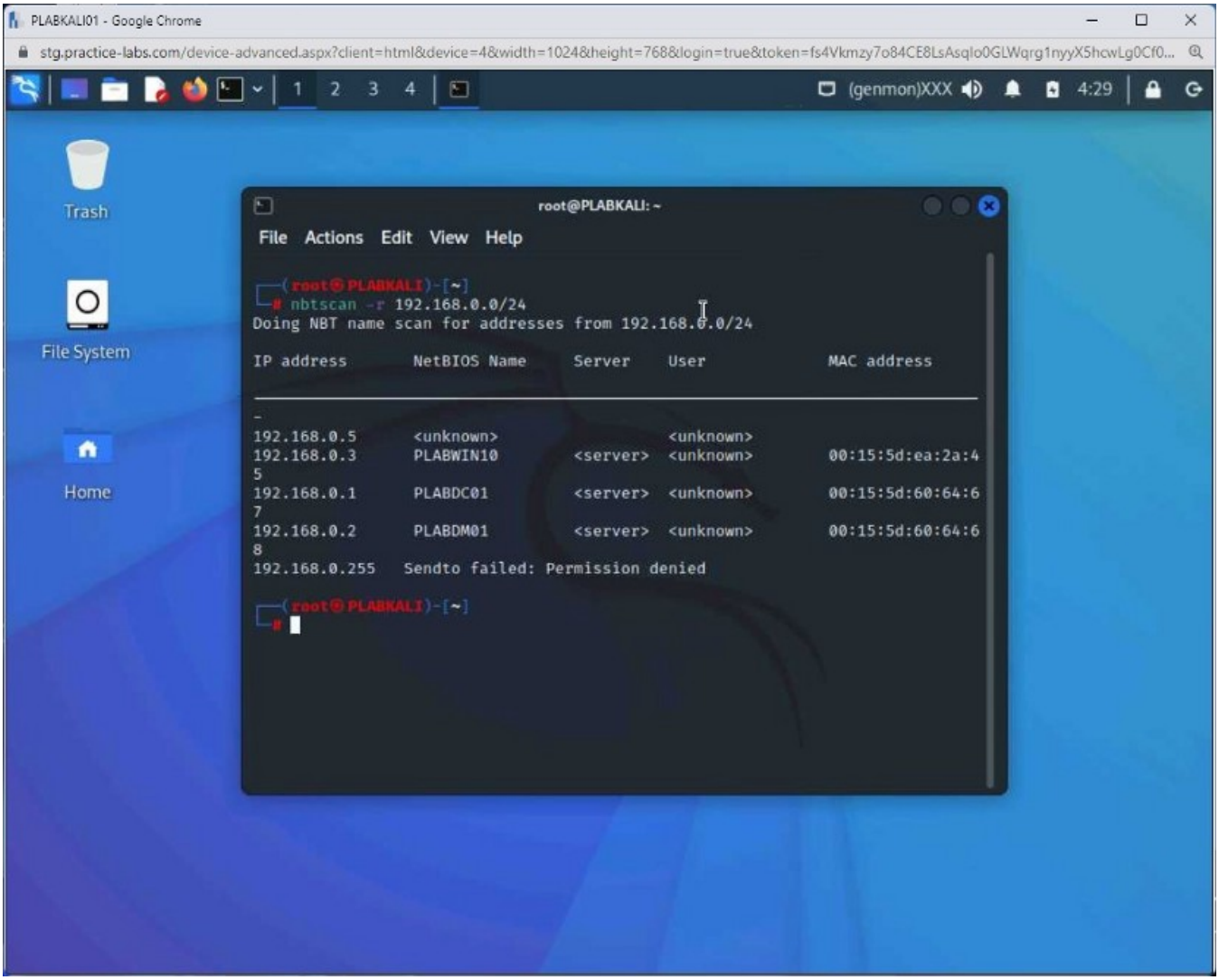
```
nbtscan -r 192.168.0.0/24
```

Press **Enter**.



Step 4

The output reveals the **NetBIOS** information.



Step 5

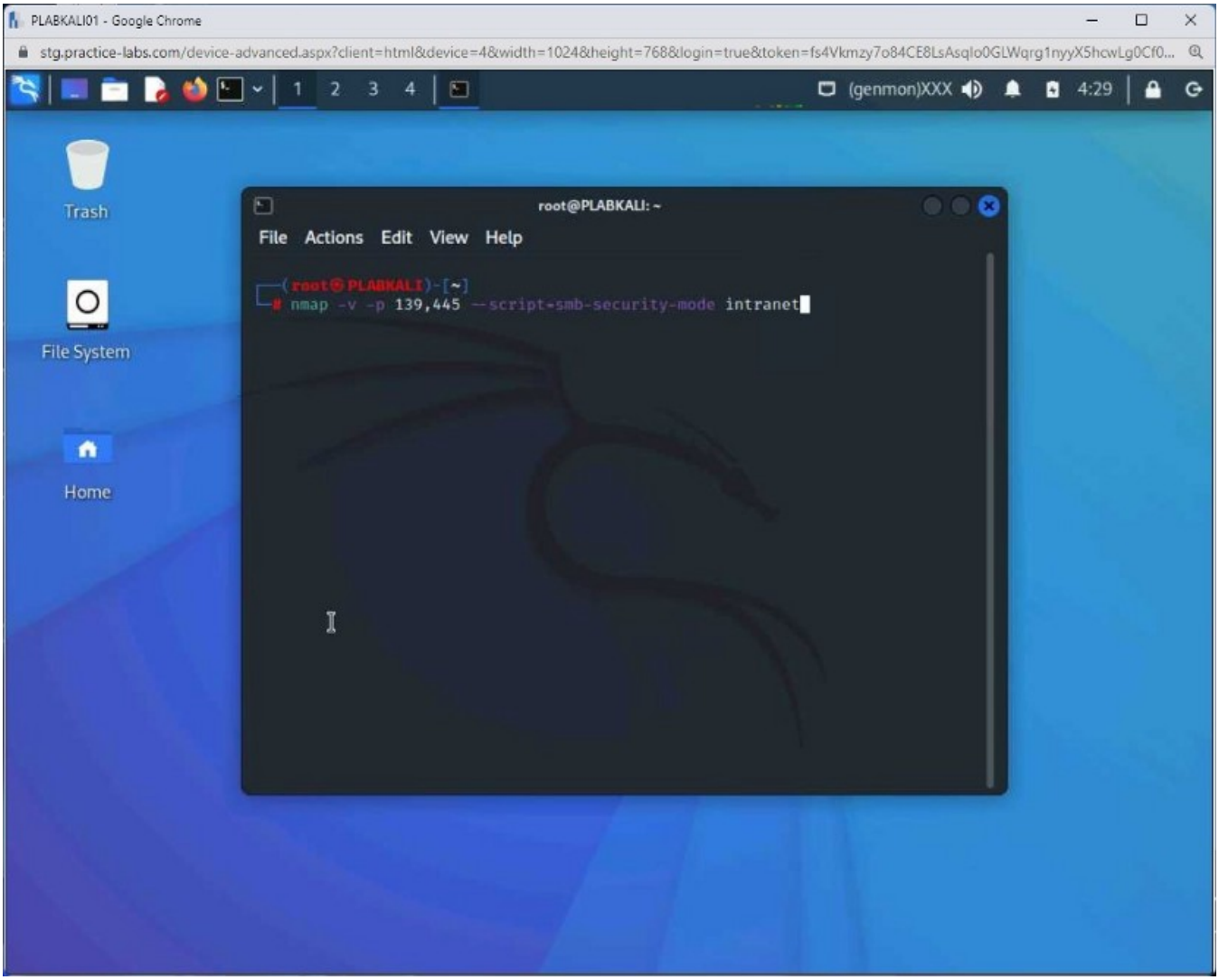
Clear the screen by entering the following command:

```
clear
```

You can check the security level of the SMB server using the **Nmap** script. To do this, type the following command:

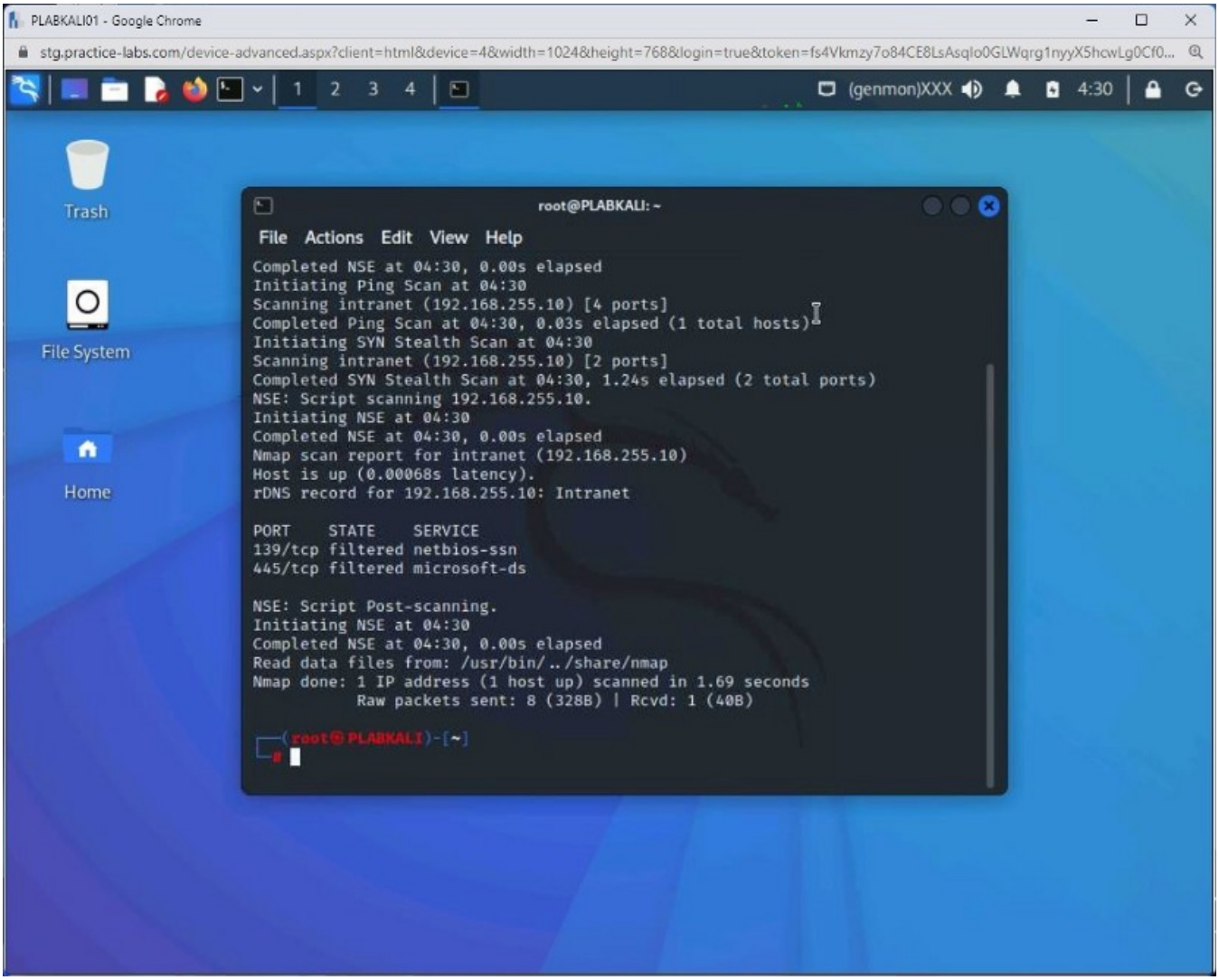
```
nmap -v -p 139,445 --script=smb-security-mode intranet
```

Press **Enter**.



Step 6

Notice the output as it details the **SMB** security details.



Keep the terminal window open.

Task 3 — Perform Windows Host Enumeration Using rpcclient

There are different ways to enumerate a Windows host. Using enumeration, you can discover information, such as:

- OS version
- Users
- Services
- Groups
- Privileges
- Shares
- Configuration Settings

A Windows host can be enumerated using different methods. For example, you can enumerate a Windows host using:

- Built-in commands
- Nmap
- Rpcclient
- Metasploit Framework

Note: *This module will focus on built-in commands of Windows and Rpcclient.*

Besides the commands, Nmap also contains ready-made scripts that can be used for various reasons, such as enumerating a Windows host. For example, consider the following command:

```
nmap 192.168.0.1 --script smb-os-discovery.nse
```

Some of the built-in commands in Windows that are commonly used include :

- dir
- ipconfig
- arp
- route
- net share
- net user

Other than the Windows command, Windows PowerShell also offers several built-in cmdlets that can be used. Some key cmdlets include:

- Get-Website
- Get-LocalUser
- Get-LocalGroup

- Get-LocalGroup
- Get-Command

***Note**: This list is non exhaustive.*

In this task, you will learn to perform Windows host enumeration. To do this, perform the following steps:

Step 1

Reconnect to **PLABKALI01**.

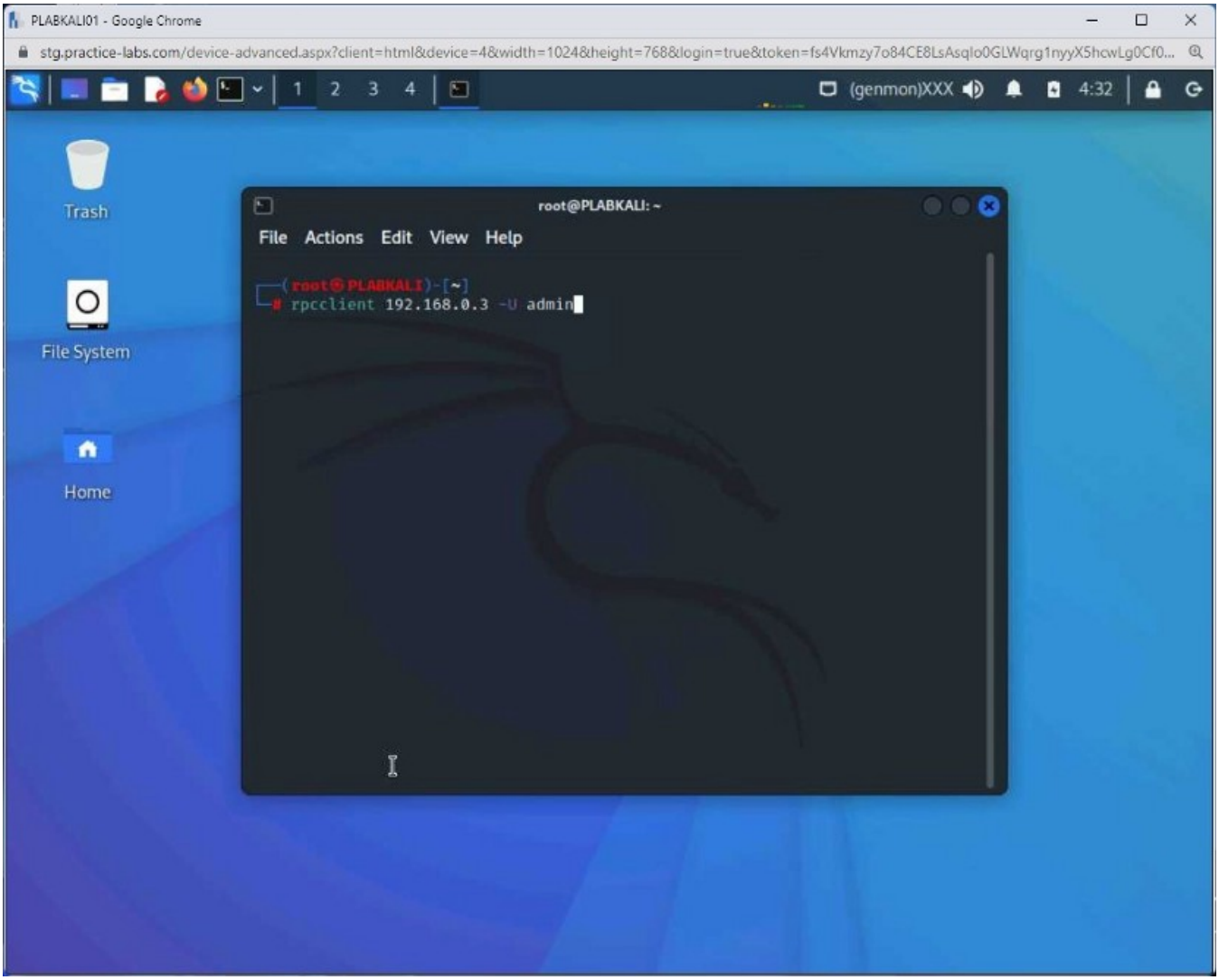
Clear the terminal window by entering the following command:

```
clear
```

First, you will work with **Rpcclient**. Type the following command to connect to **PLABWIN10**:

```
rpcclient 192.168.0.3 -U admin
```

Press **Enter**.



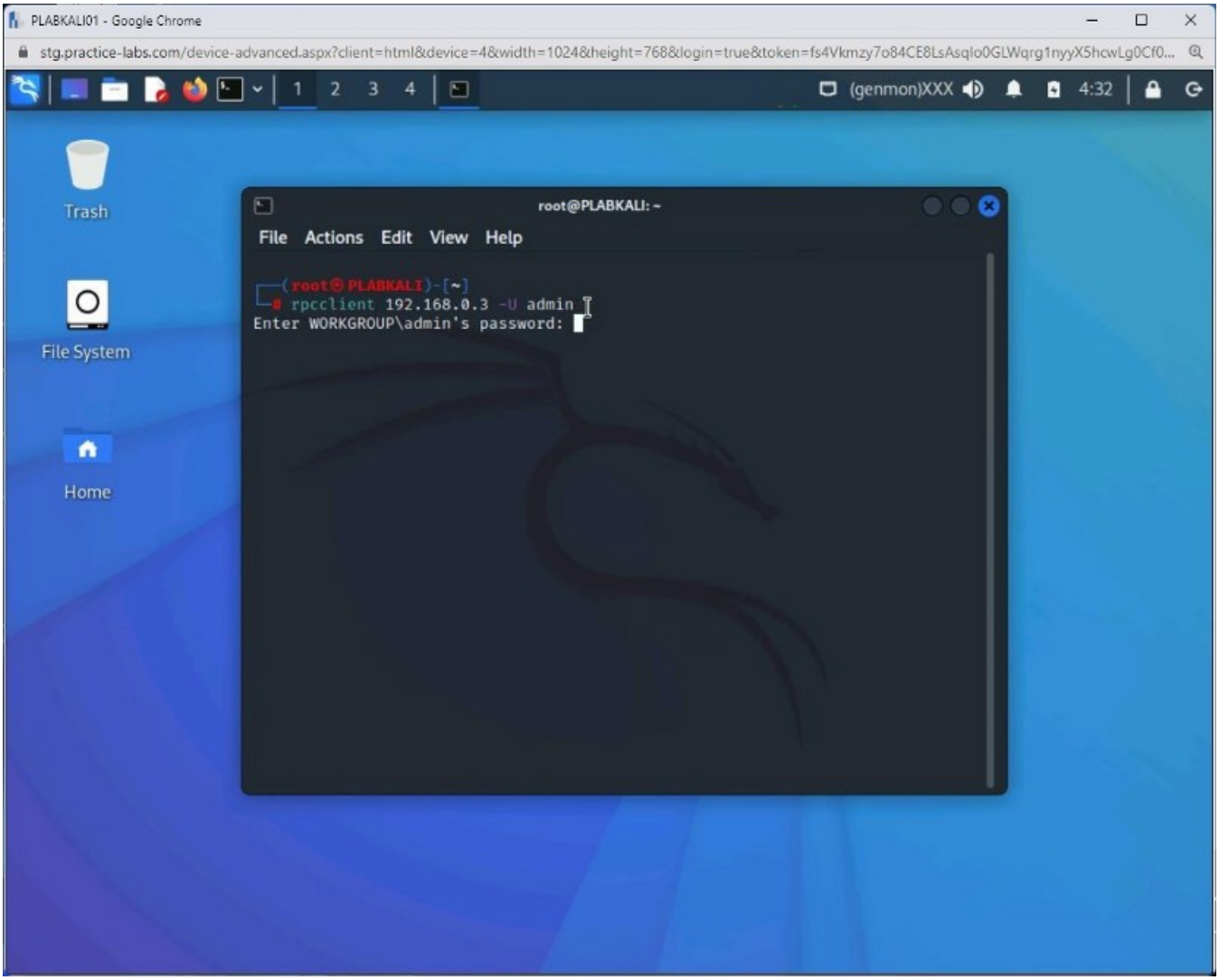
Step 2

You are now prompted for the admin password. Type the following:

Password

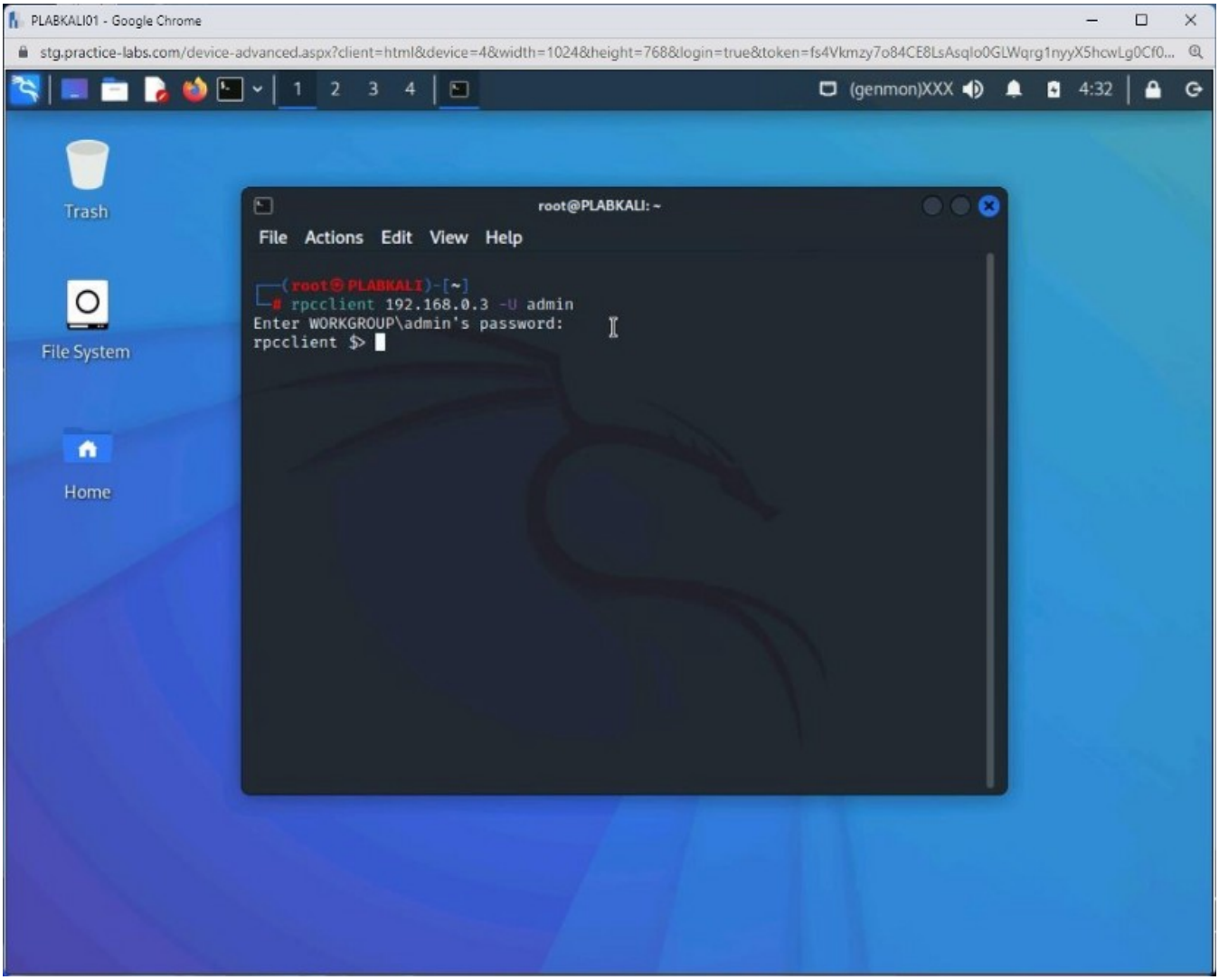
Press **Enter**.

Note: *The password will not be visible when entered.*



Step 3

Notice that the **rpcclient** prompt appears. This indicates that you have connected to **PLABWIN10** successfully.

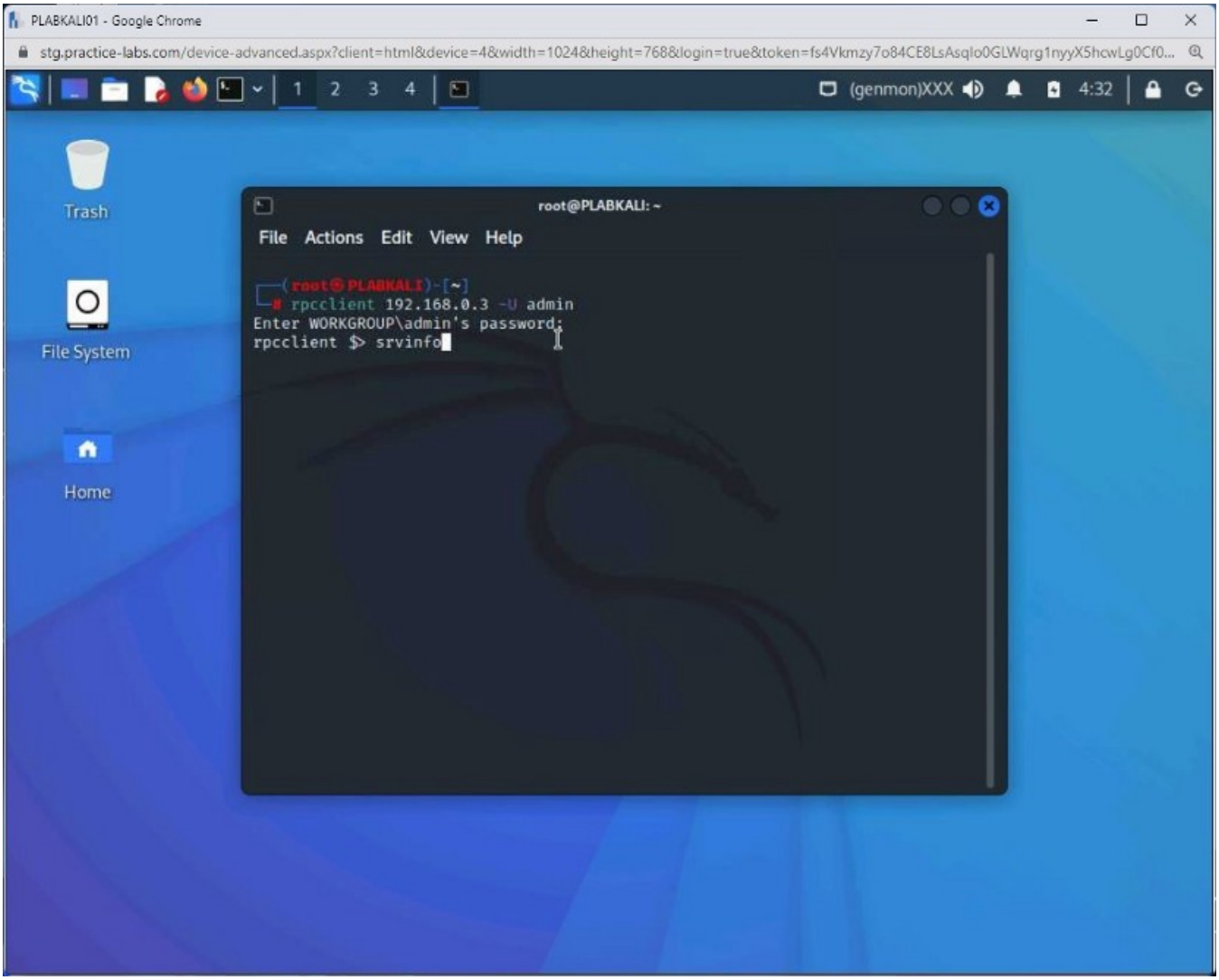


Step 4

To display **PLABWIN10** details, type the following command:

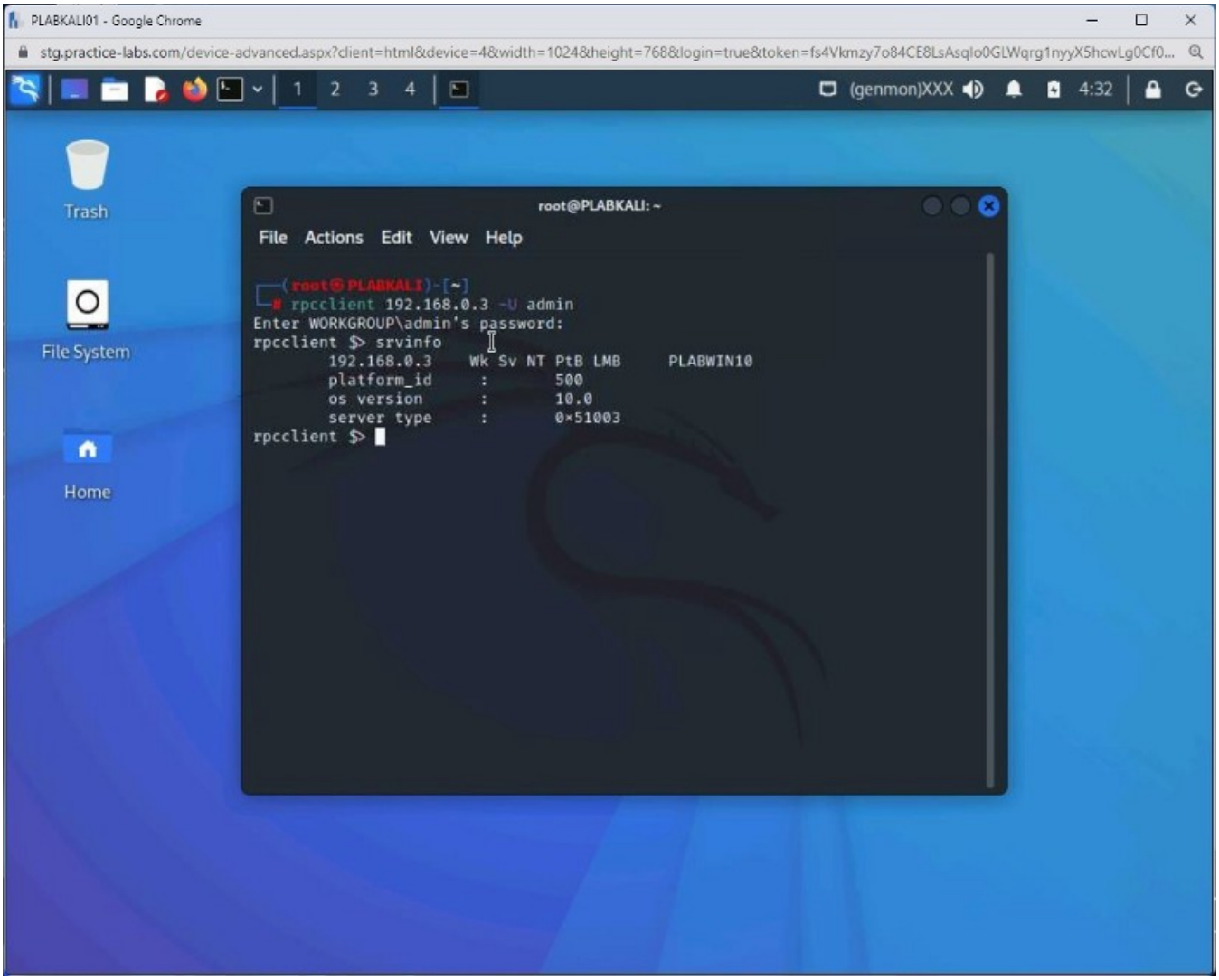
```
srvinfo
```

Press **Enter**.



Step 5

Notice the output of the **srvinfo** command. It displays the IP address, type of operating system, its version, etc.

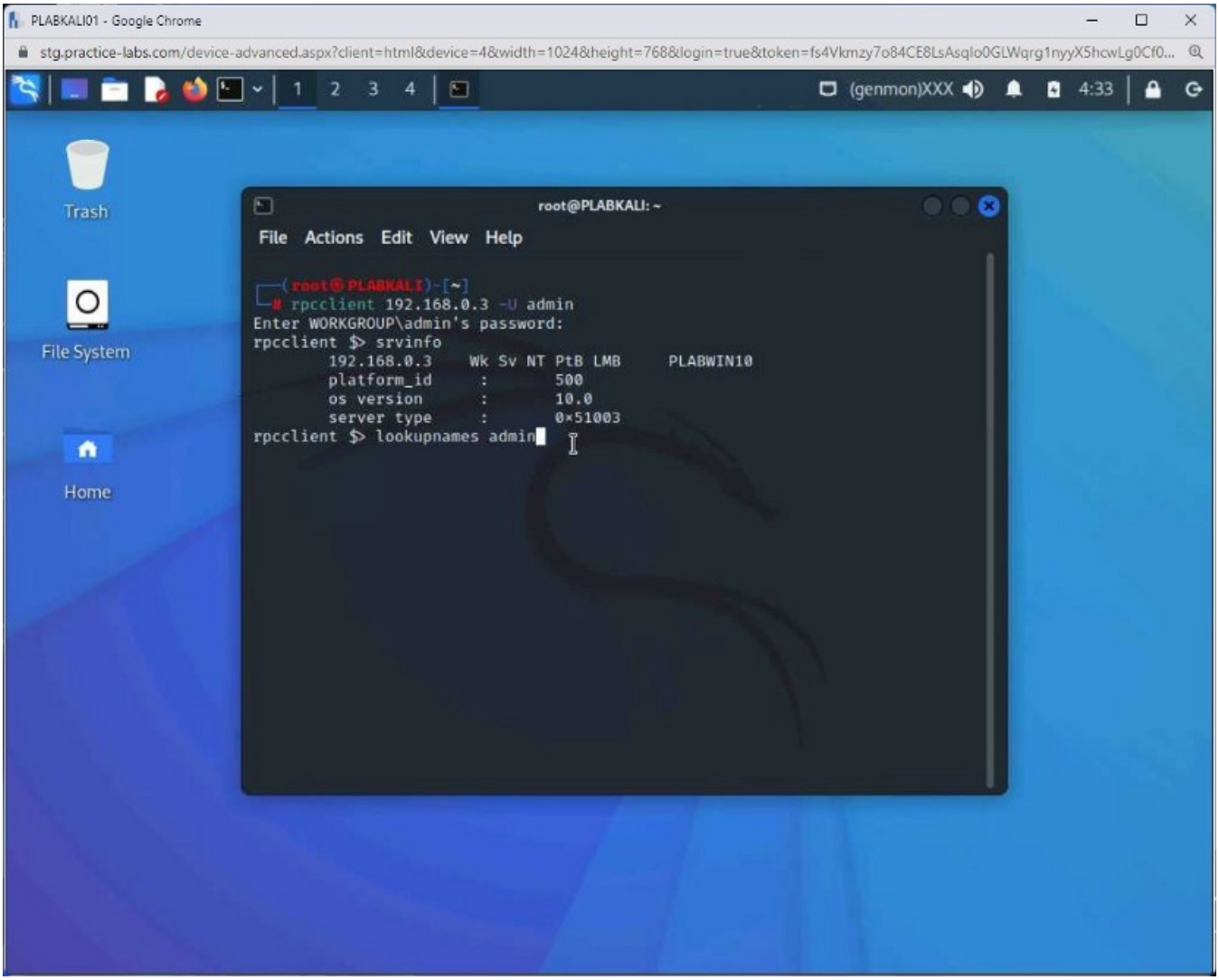


Step 6

Let's find out the **admin** account's **security ID (SID)**. Type the following command:

```
lookupnames admin
```

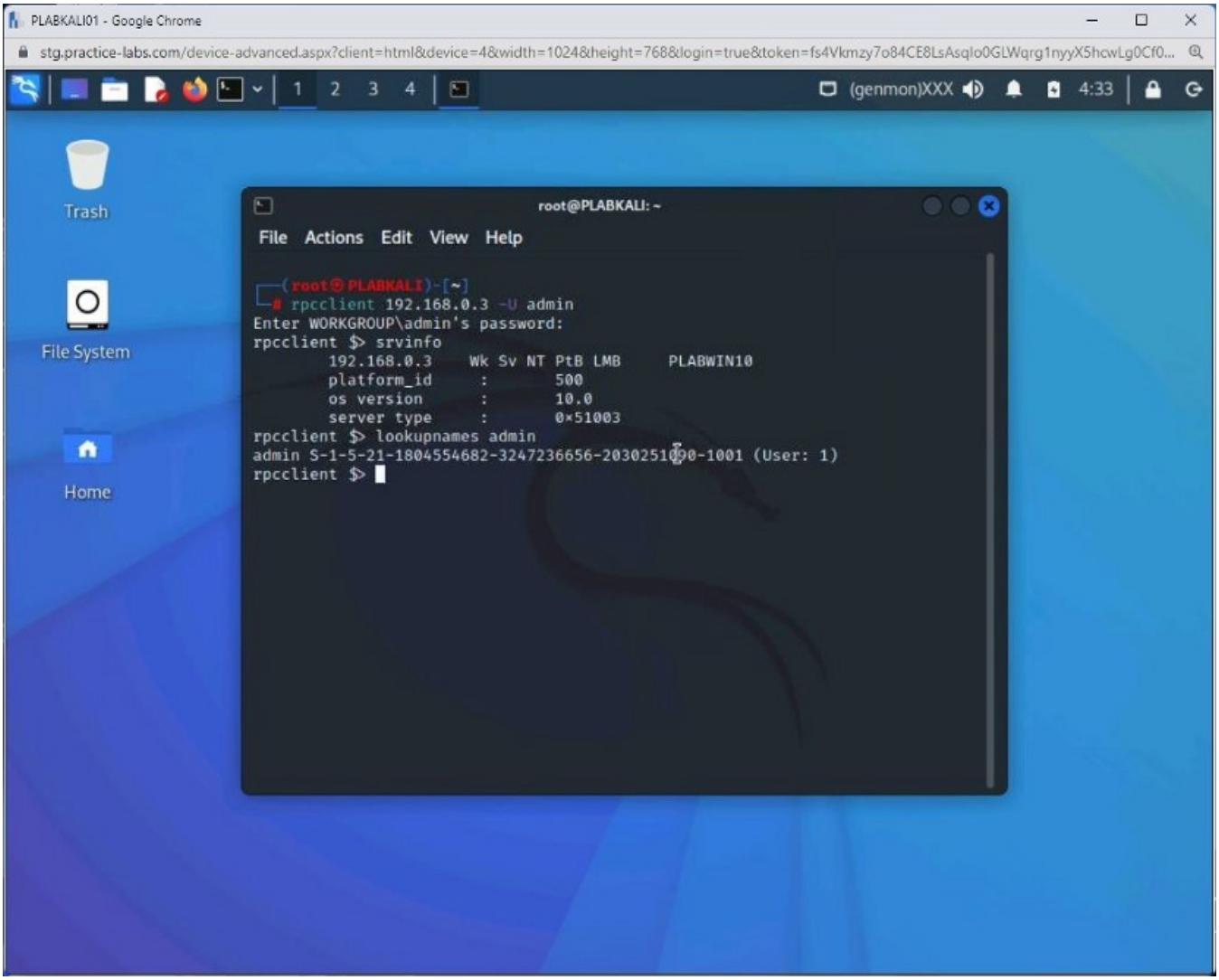
Press **Enter**.



Step 7

Notice that the **SID** for the admin account is now displayed. **SID** for the **admin** account ends with **1001**.

Note: *If this was the built-in administrator account, its* ***SID*** *will always end with 500.* ***SID*** *will never change even if you rename the administrator account.*

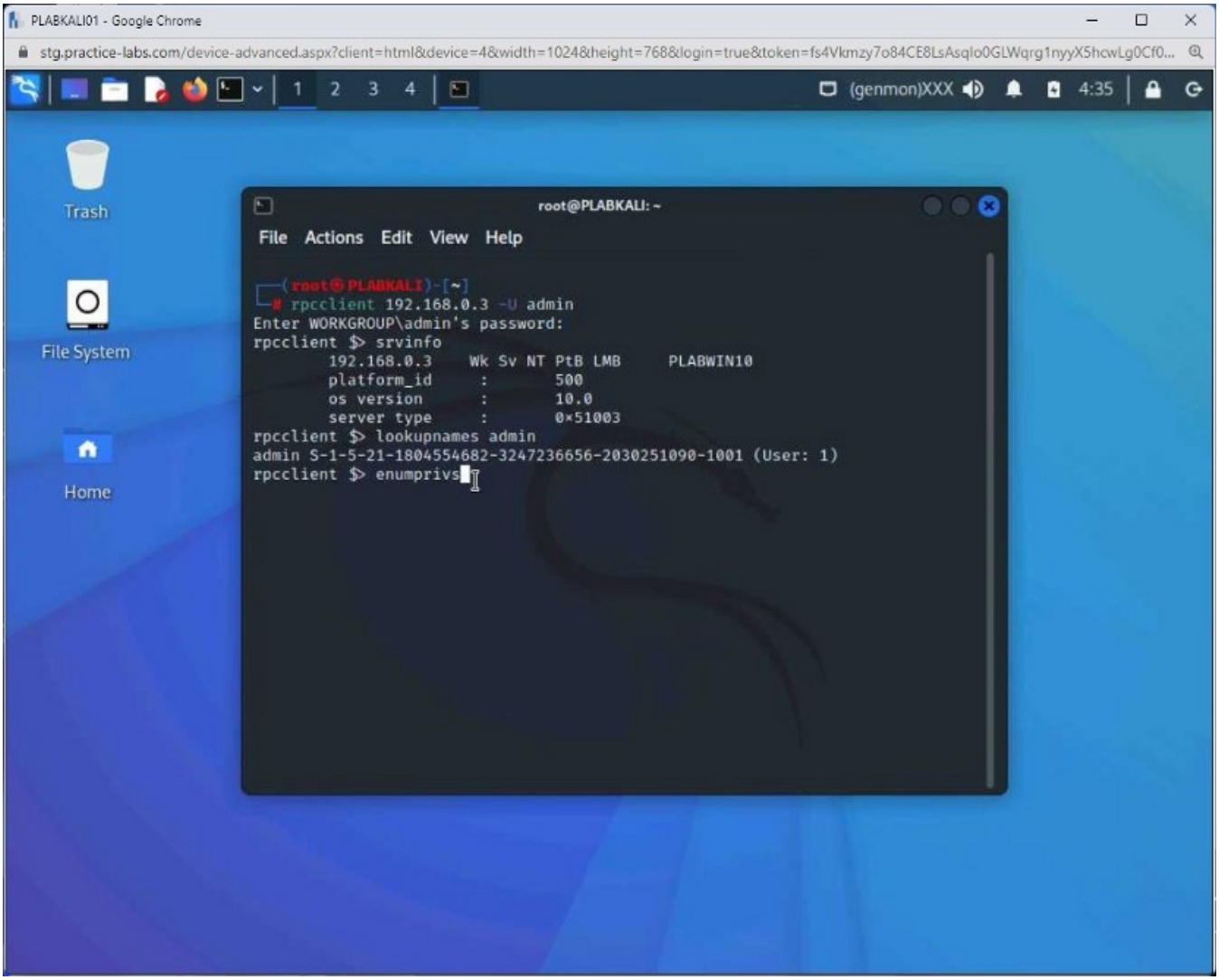


Step 8

You can also list the privileges that are known in this domain. Type the following command:

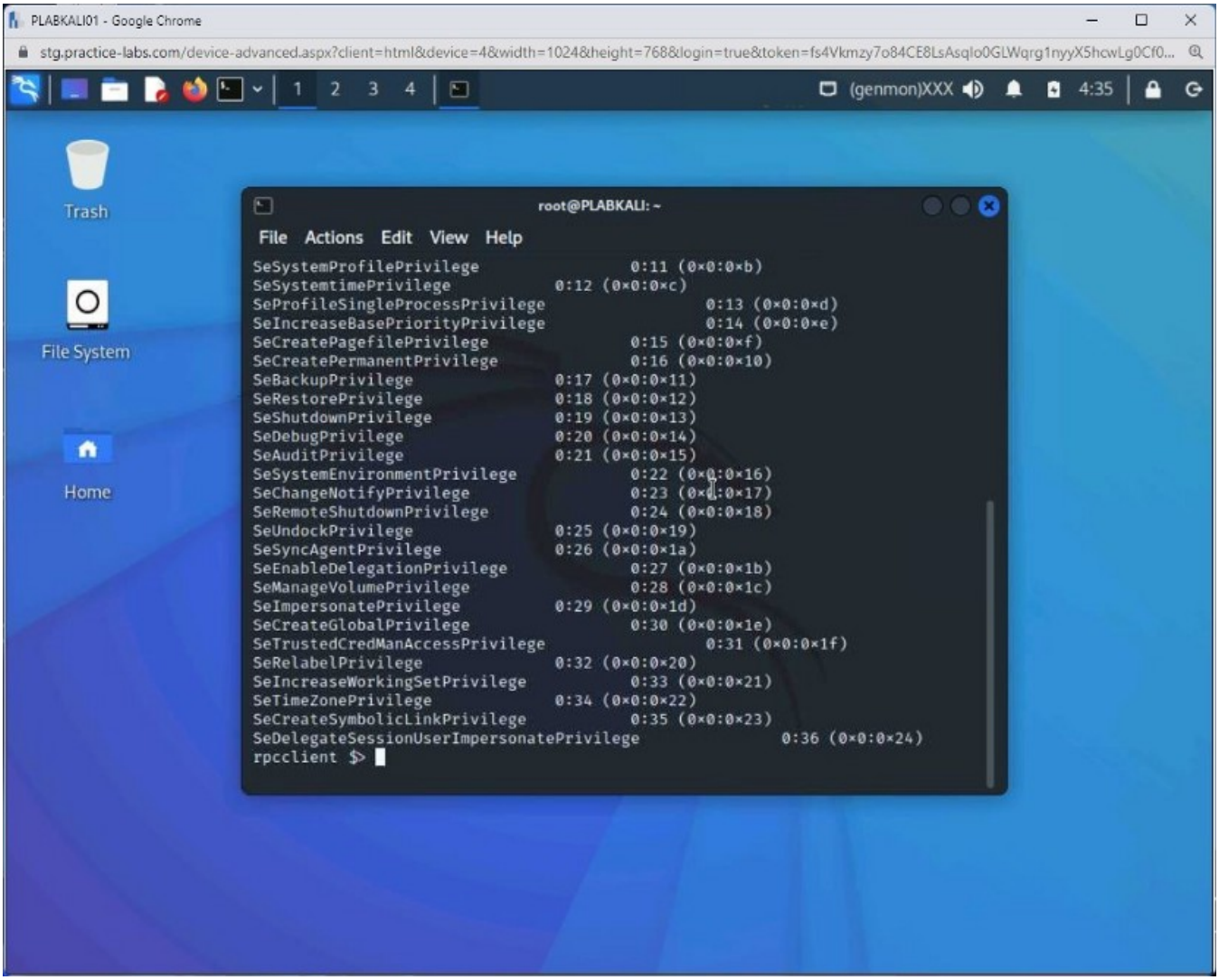
```
enumprivs
```

Press **Enter**.



Step 9

The output for the **enumprivs** command is displayed.

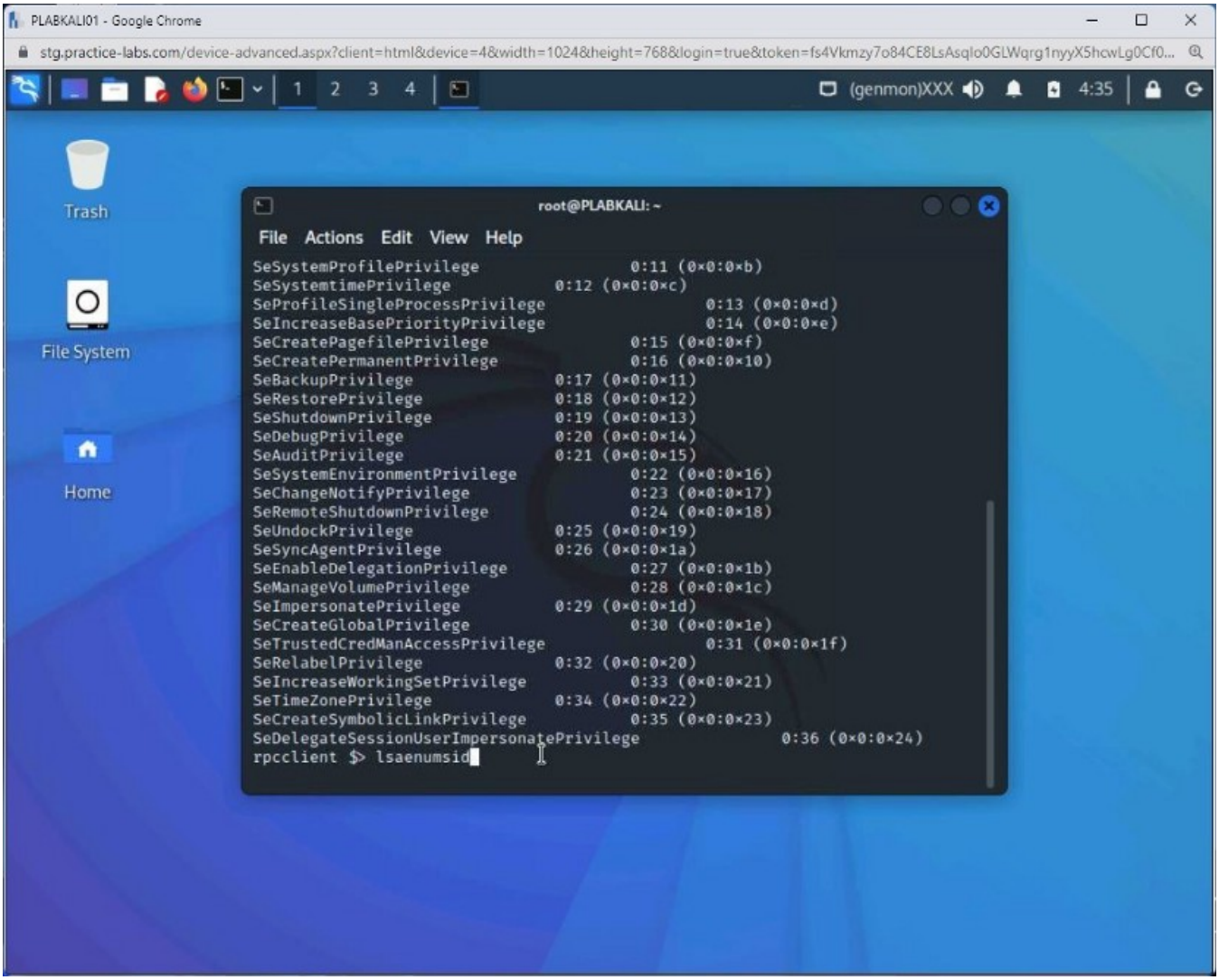


Step 10

You can also list the **SIDs** for the **local LSA**. Type the following command:

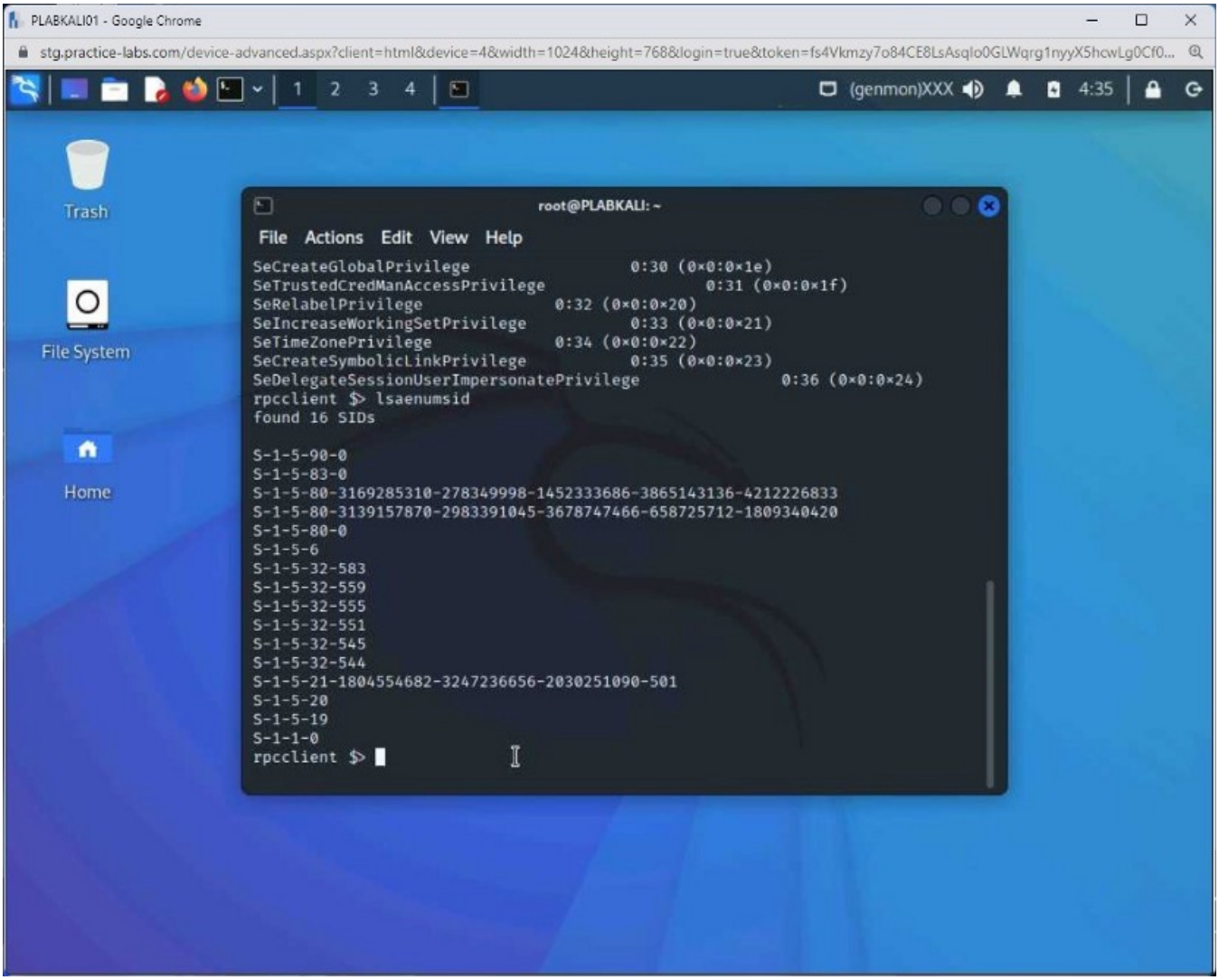
```
lsaenumsid
```

Press **Enter**.



Step 11

Notice that the **SIDs** for the **local LSA** are now listed.

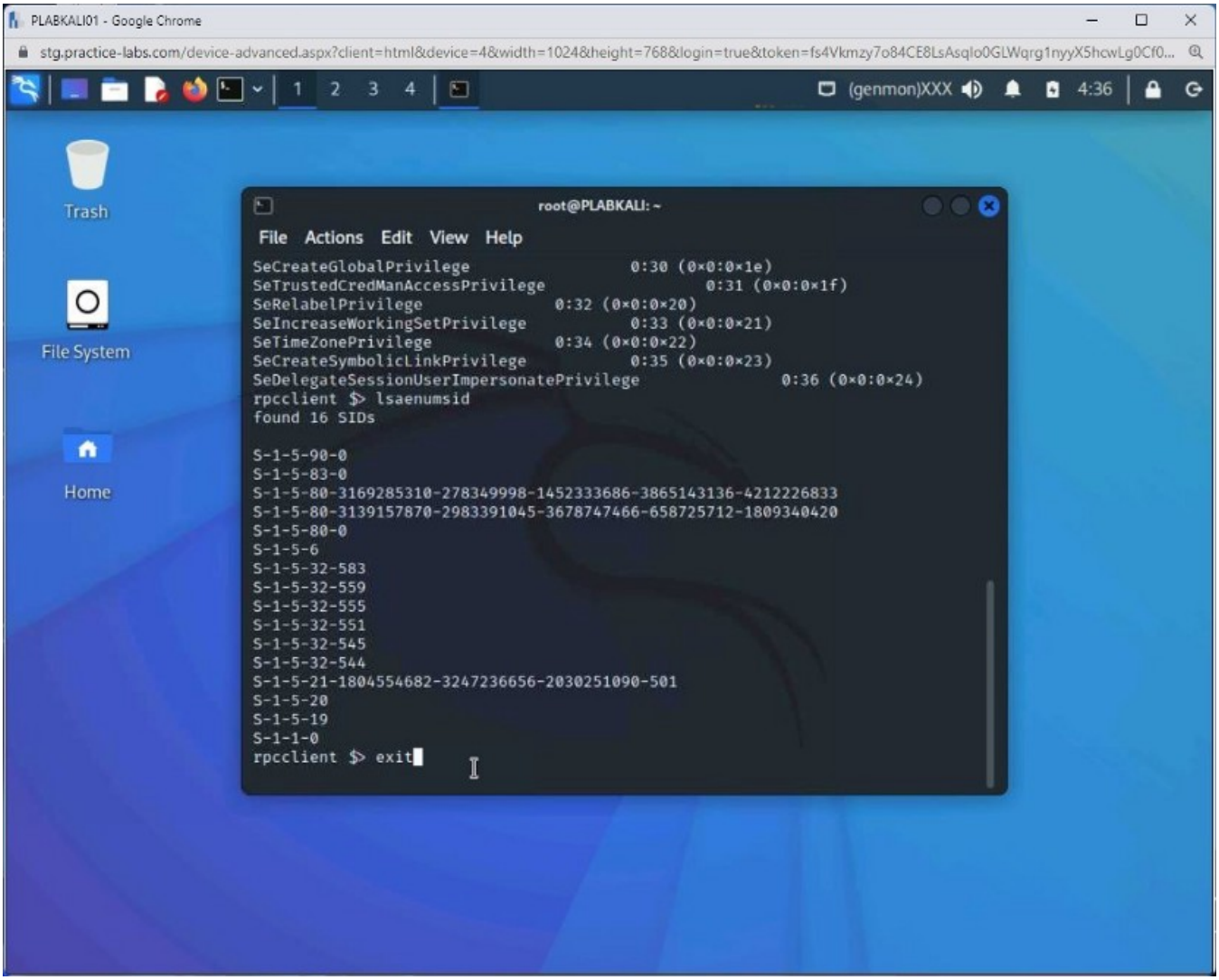


Step 12

To exit from the **rpcclient**, type the following command:

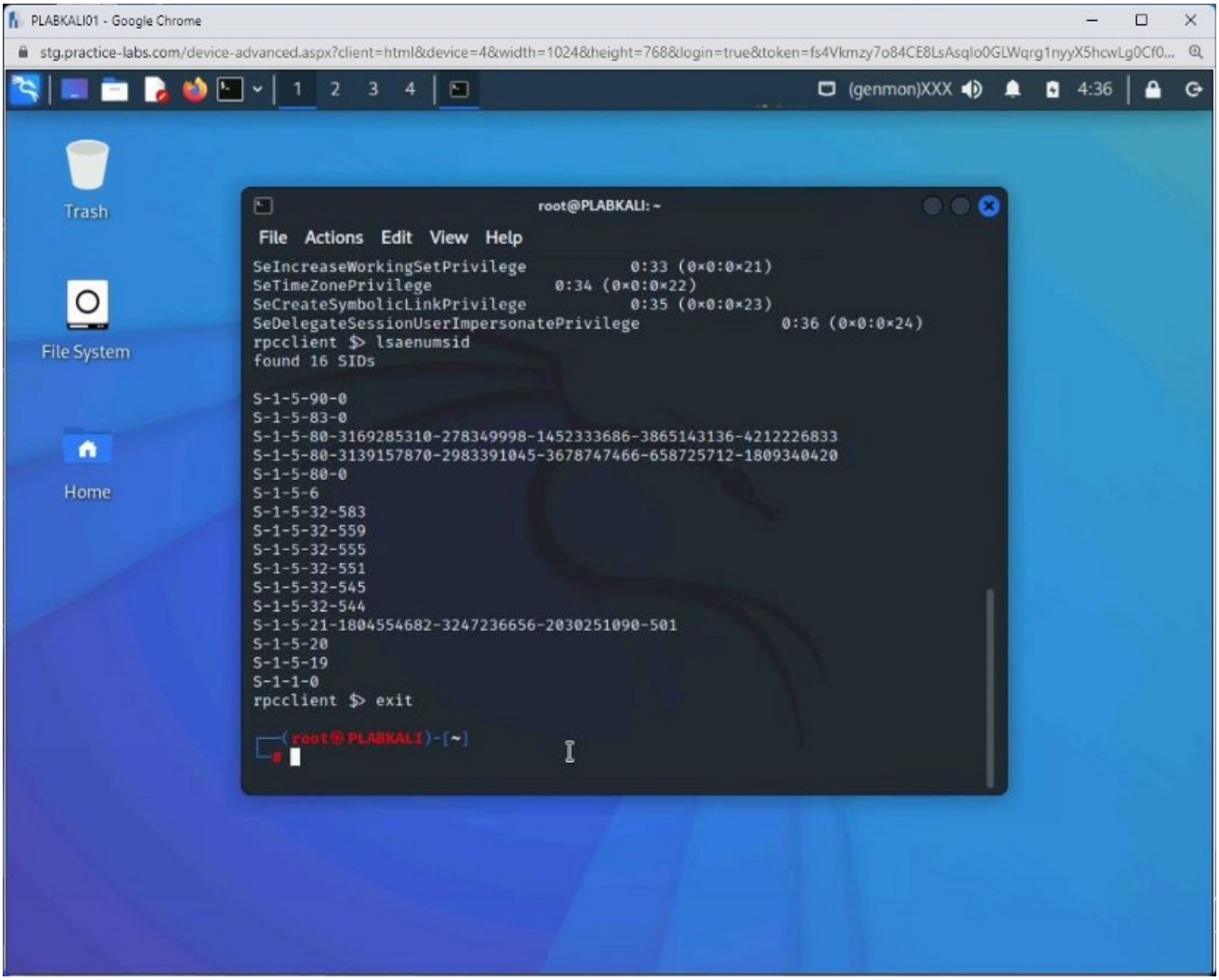
```
exit
```

Press **Enter**.



Step 13

You are now back on the terminal prompt.



Keep the terminal window open.

Task 4 — Perform Linux Host Enumeration using Nmap

Just like Windows, you can also perform Linux host enumeration. Linux also offers several built-in commands that can be useful in enumeration. Some of the key commands are:

- uname -a
- hostname
- route
- arp
- ifconfig
- mount

- whoami

If you want to find information about the installed packages, you can run the **dpkg** command.

In this task, you will use nmap to enumerate a host on the network, which contains various parameters that can be used to collect information about a target. For example, with the -O parameter, you can get the details about the operating system.

Step 1

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

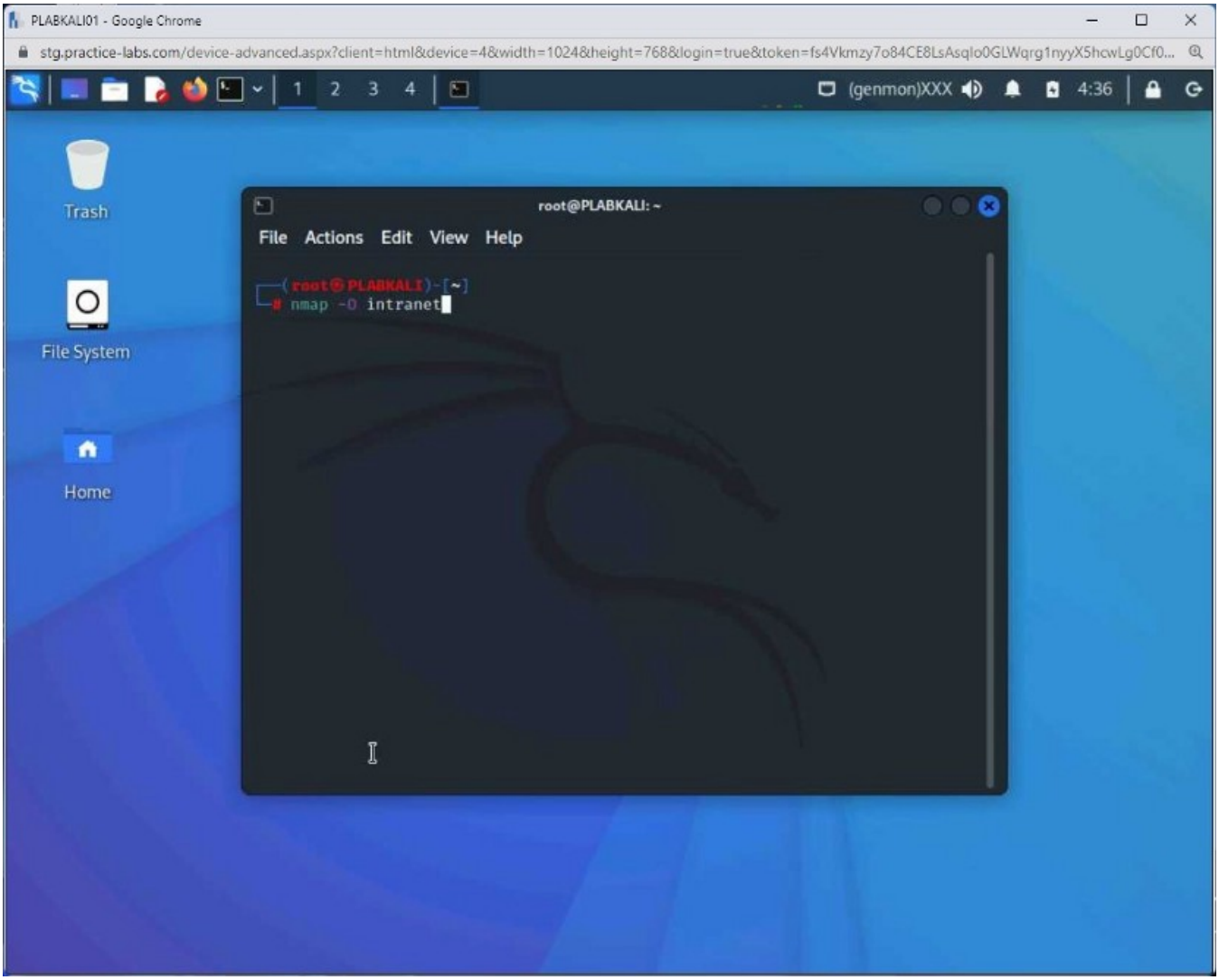
Clear the screen by entering the following command:

```
clear
```

You will first perform operating system detection. Type the following command:

```
nmap -O intranet
```

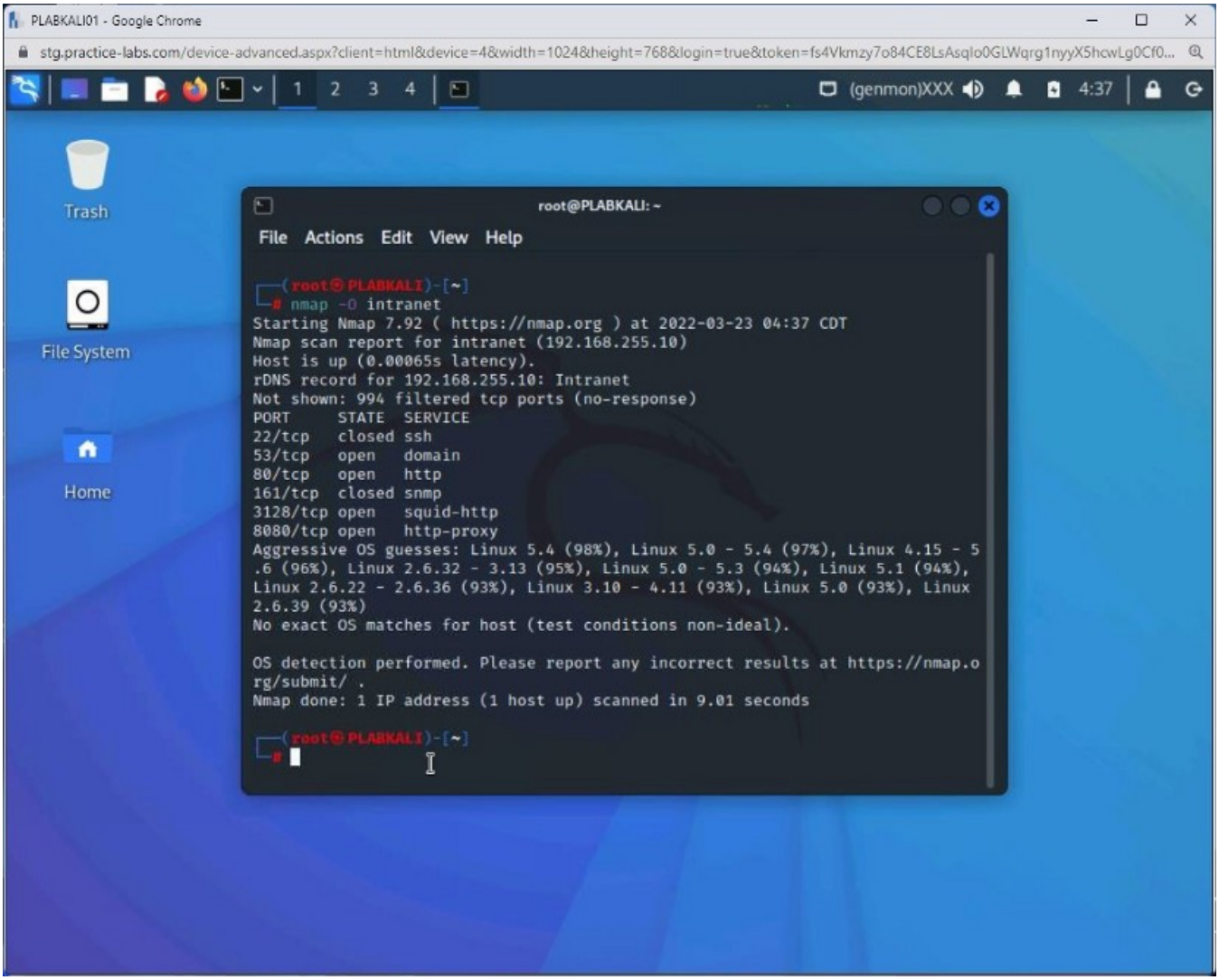
Press **Enter**.



Step 2

Notice that the output provides several pointers.

It lists the open ports along with the TCP/IP fingerprint.



Step 3

Clear the screen by entering the following command:

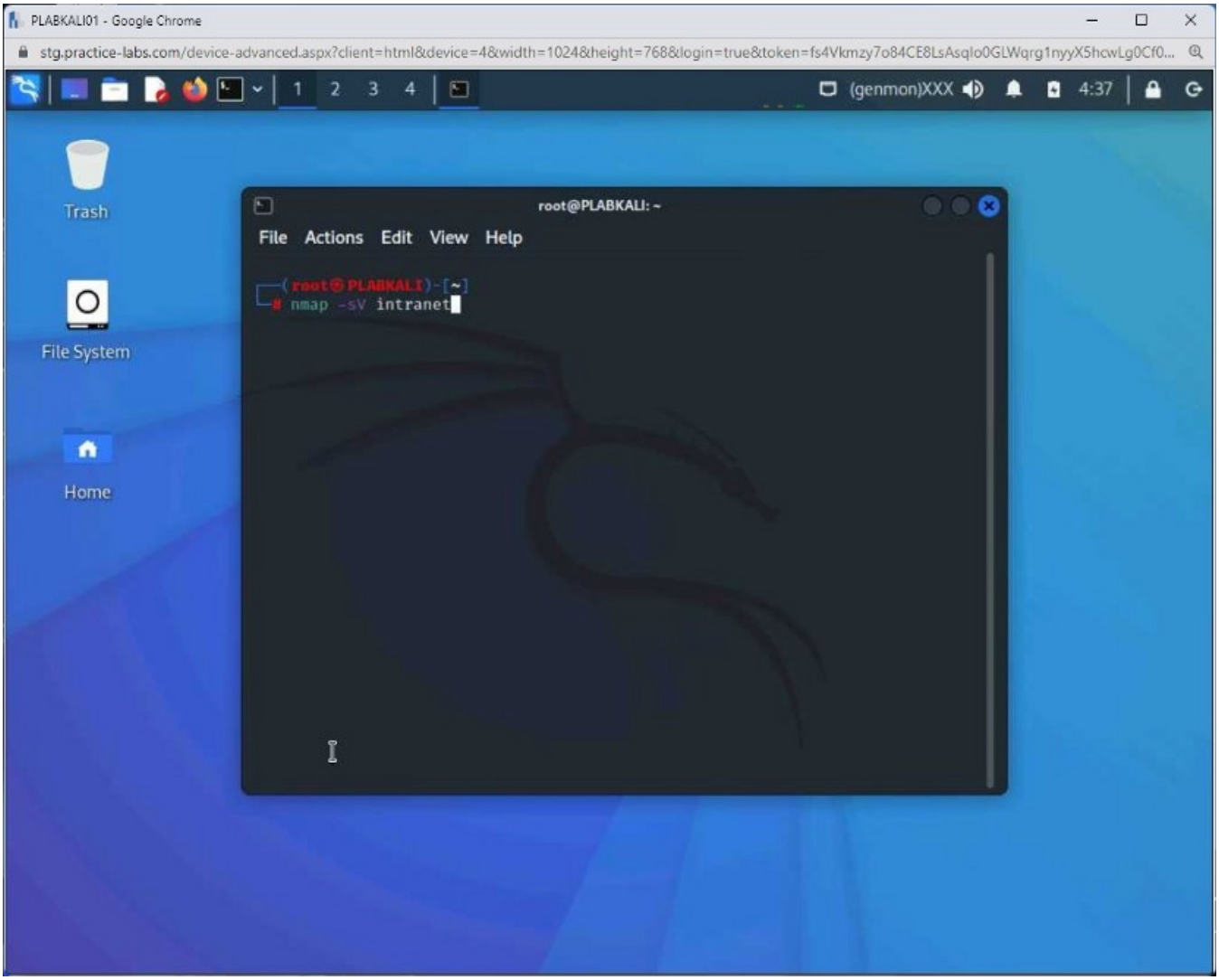
```
clear
```

You can perform detailed enumeration on a Linux host, such as list the running services.

Type the following command:

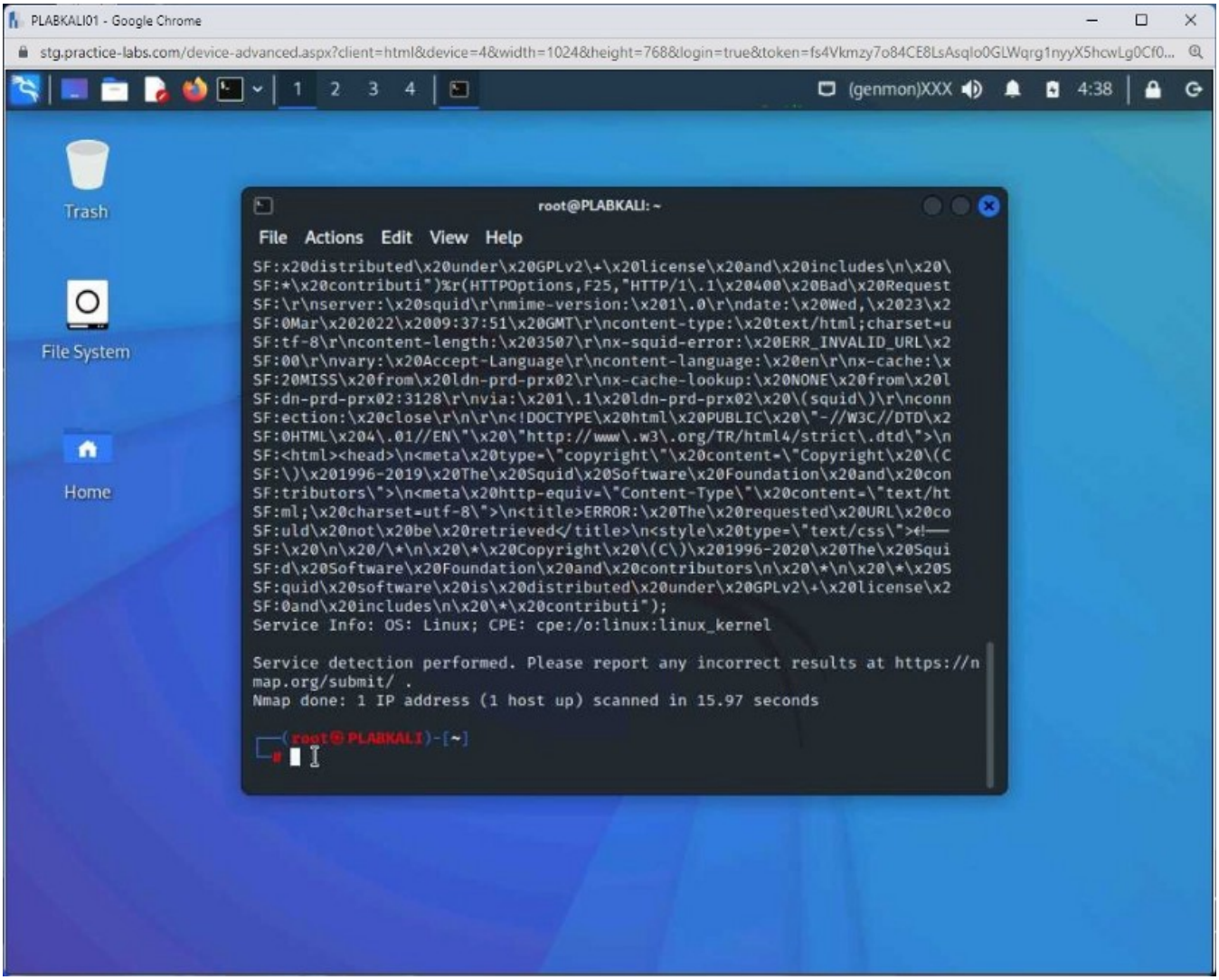
```
nmap -sV intranet
```

Press **Enter**.



Step 4

Notice that the output lists the open ports, running services, and versions.



Step 5

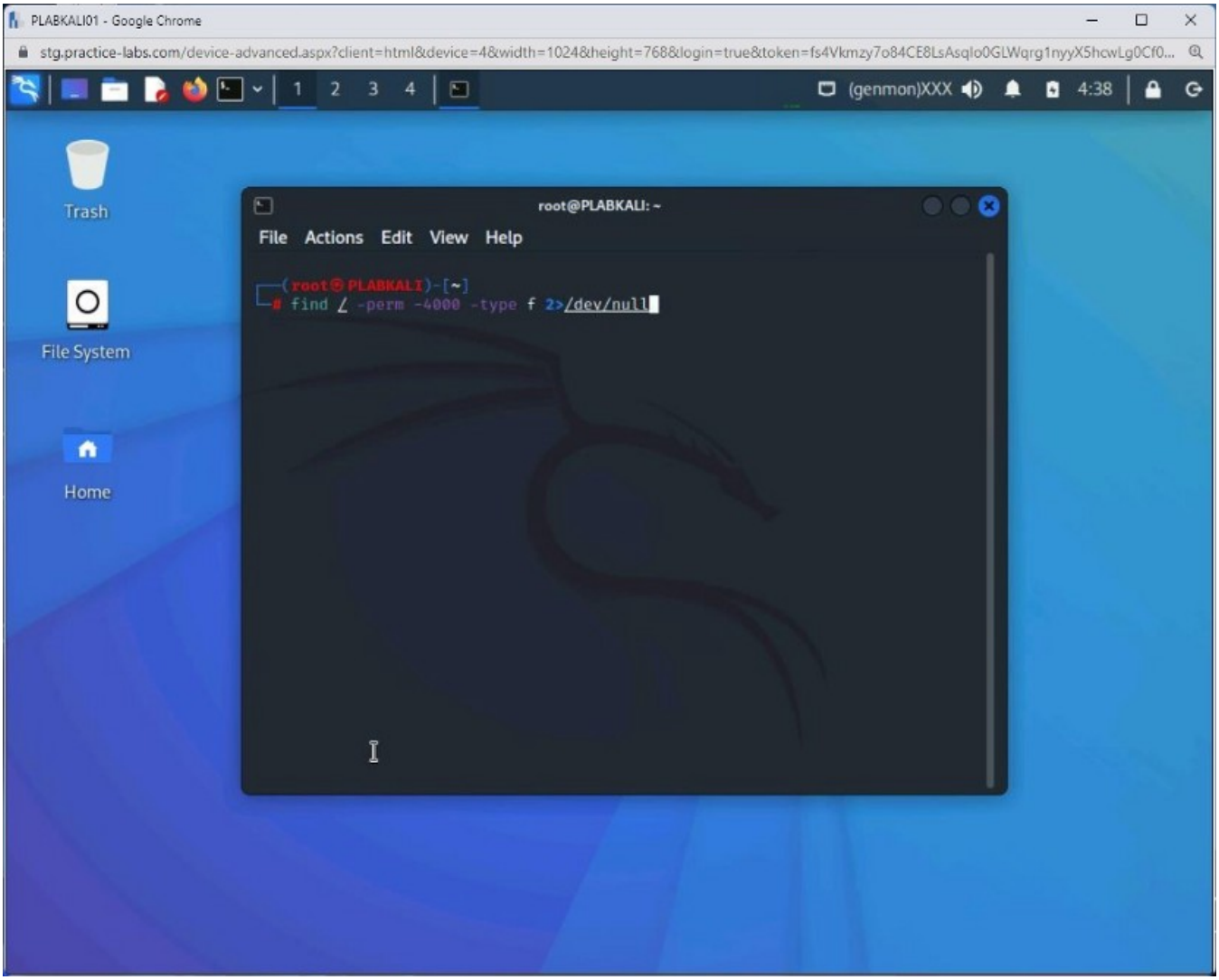
Clear the screen by entering the following command:

```
clear
```

You can also use several built-in commands to extract information useful in ethical hacking. For example, you can find all SUID files. To do this, type the following command:

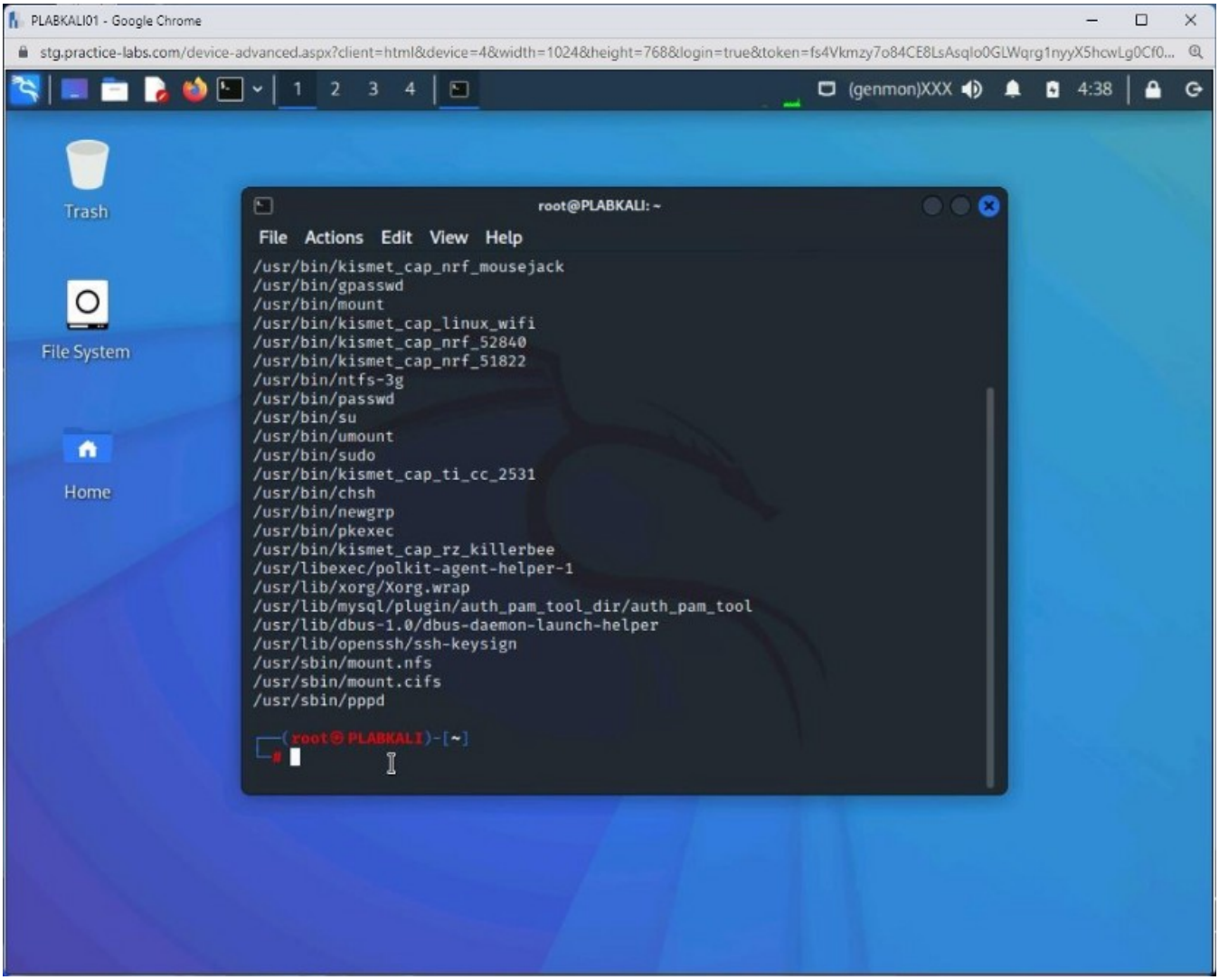
```
find / -perm -4000 -type f 2>/dev/null
```

Press **Enter**.



Step 6

The output lists several files.



Step 7

Clear the screen by entering the following command:

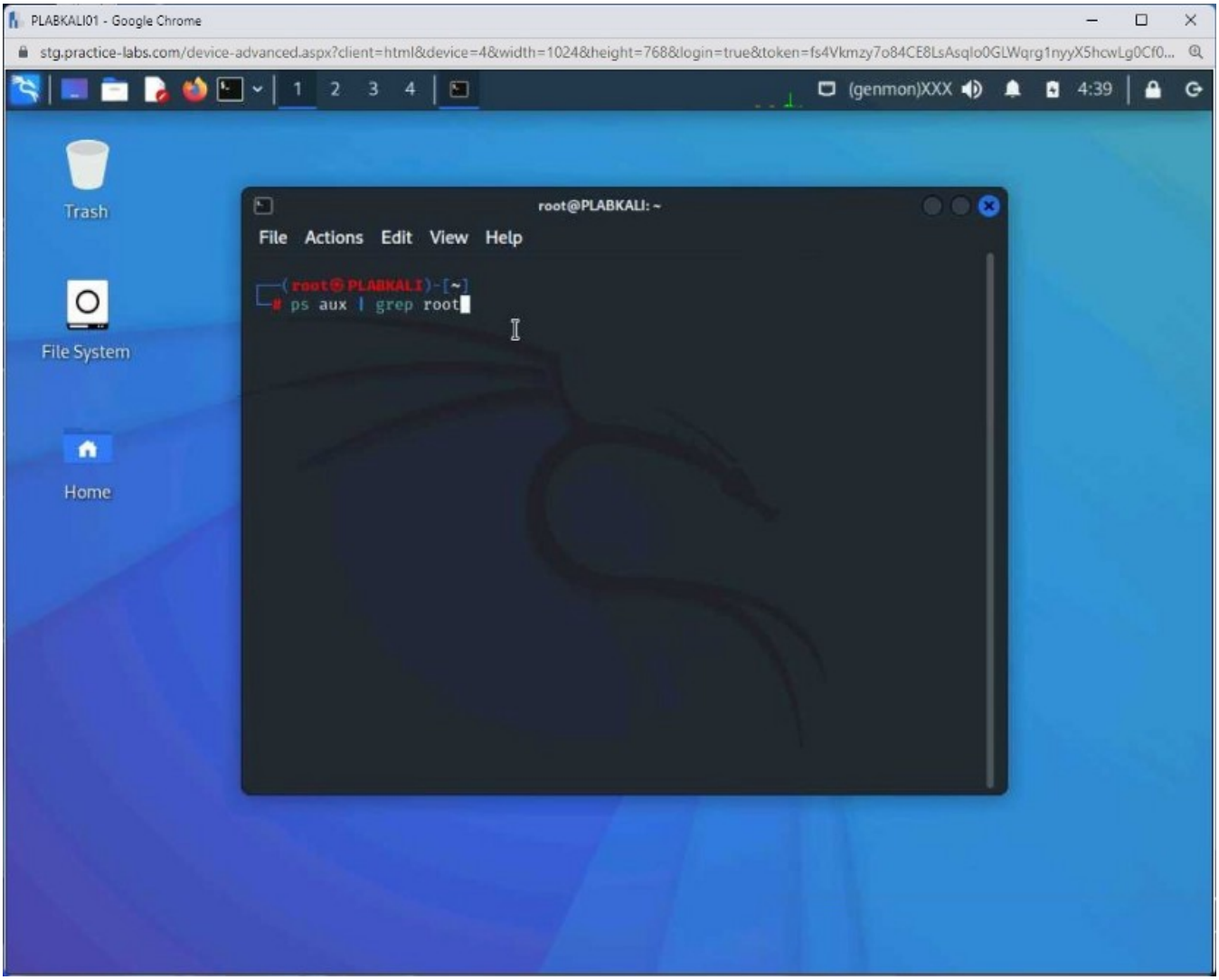
```
clear
```

You might also want to list services that are running as **root**.

Type the following command:

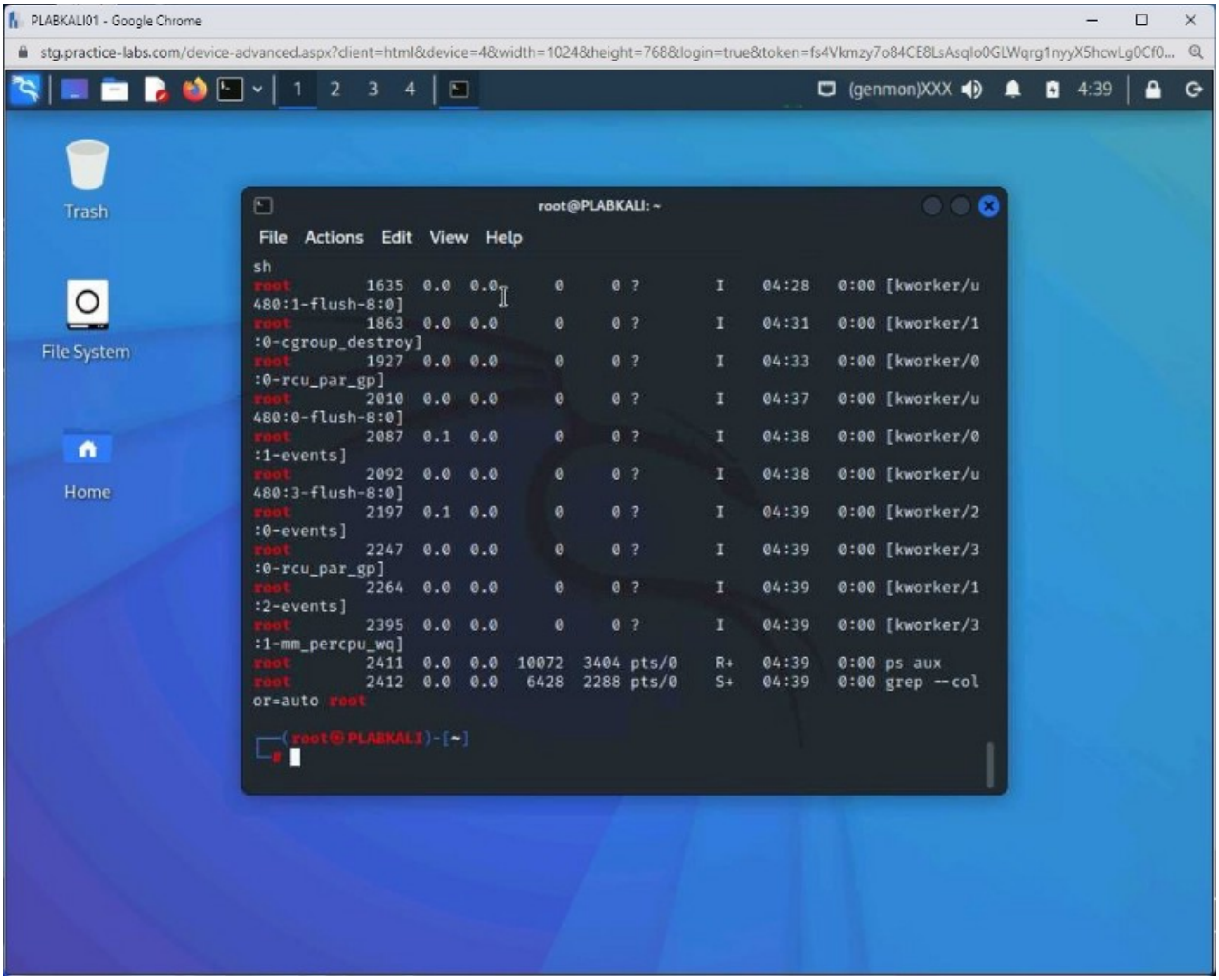
```
ps aux | grep root
```

Press **Enter**.



Step 8

A set of services is listed as the output.



Keep the terminal window open.

Task 5 — Use Hyena for Enumeration

Hyena is one of the most renowned tools for system management for network administrators. It can help you enumerate information, such as users, shares, and services. Instead of using a command-line tool such as Nmap, you can also use Hyena for enumerating target systems.

A benefit of using Hyena is that It also provides the capabilities of enumerating directory services, if you have administrative privileges for a target.

In this task, you will learn to use Hyena for enumeration. To use Hyena, perform the following steps:

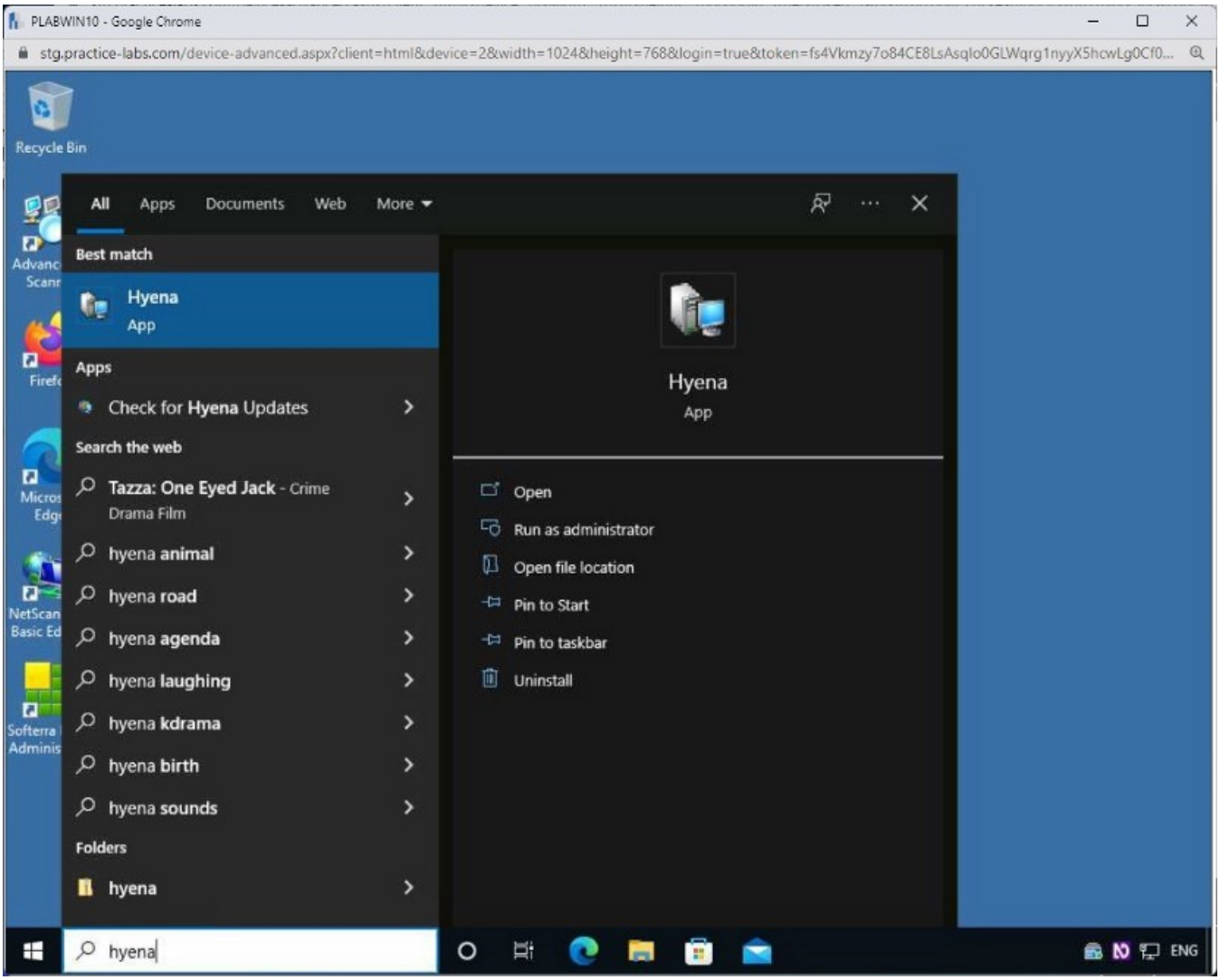
Step 1

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

In the **Type here to search** text box, type the following:

```
hyena
```

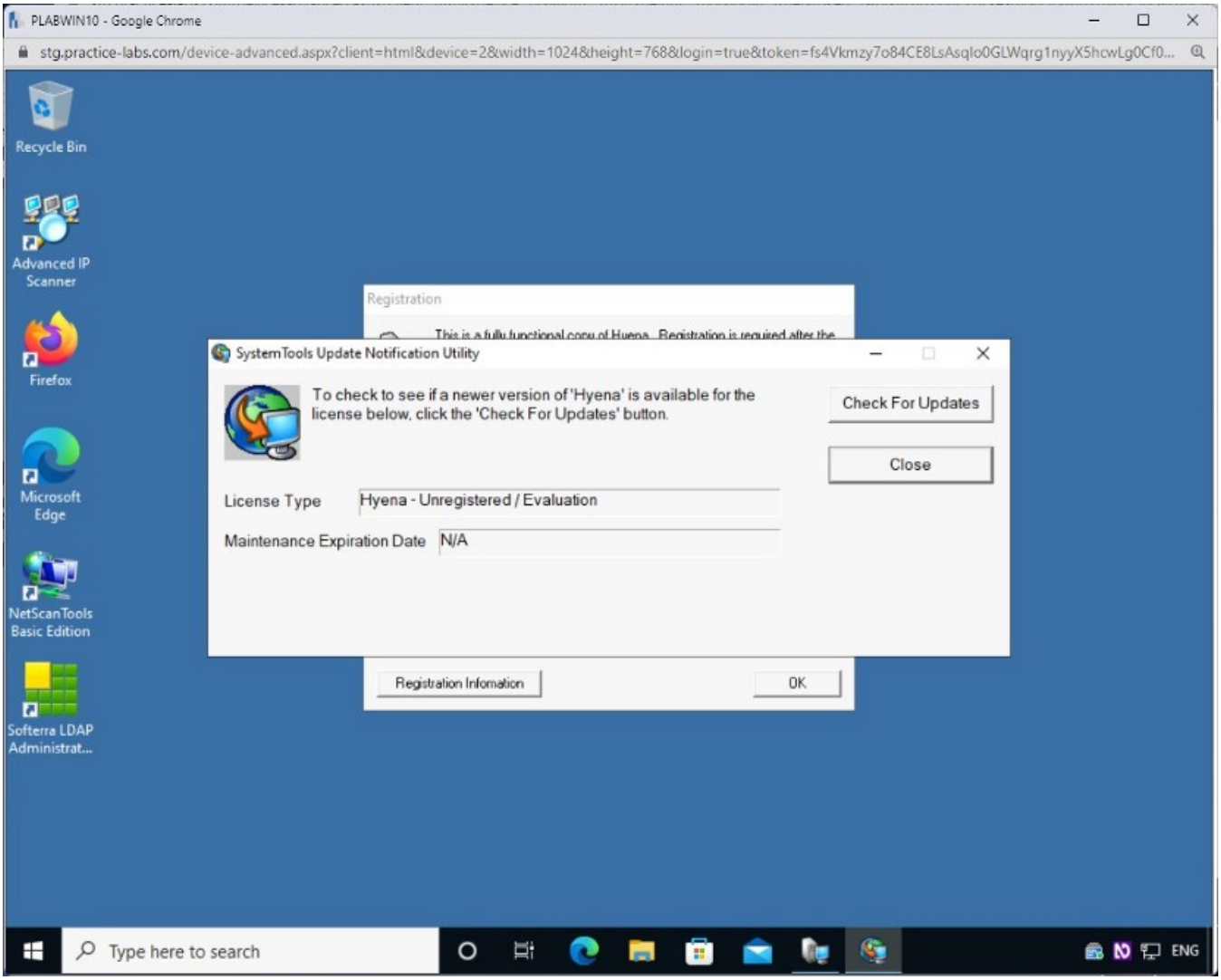
From the search results, select **Hyena**.



Step 2

The **SystemTools Update Notification Utility** dialog box is displayed.

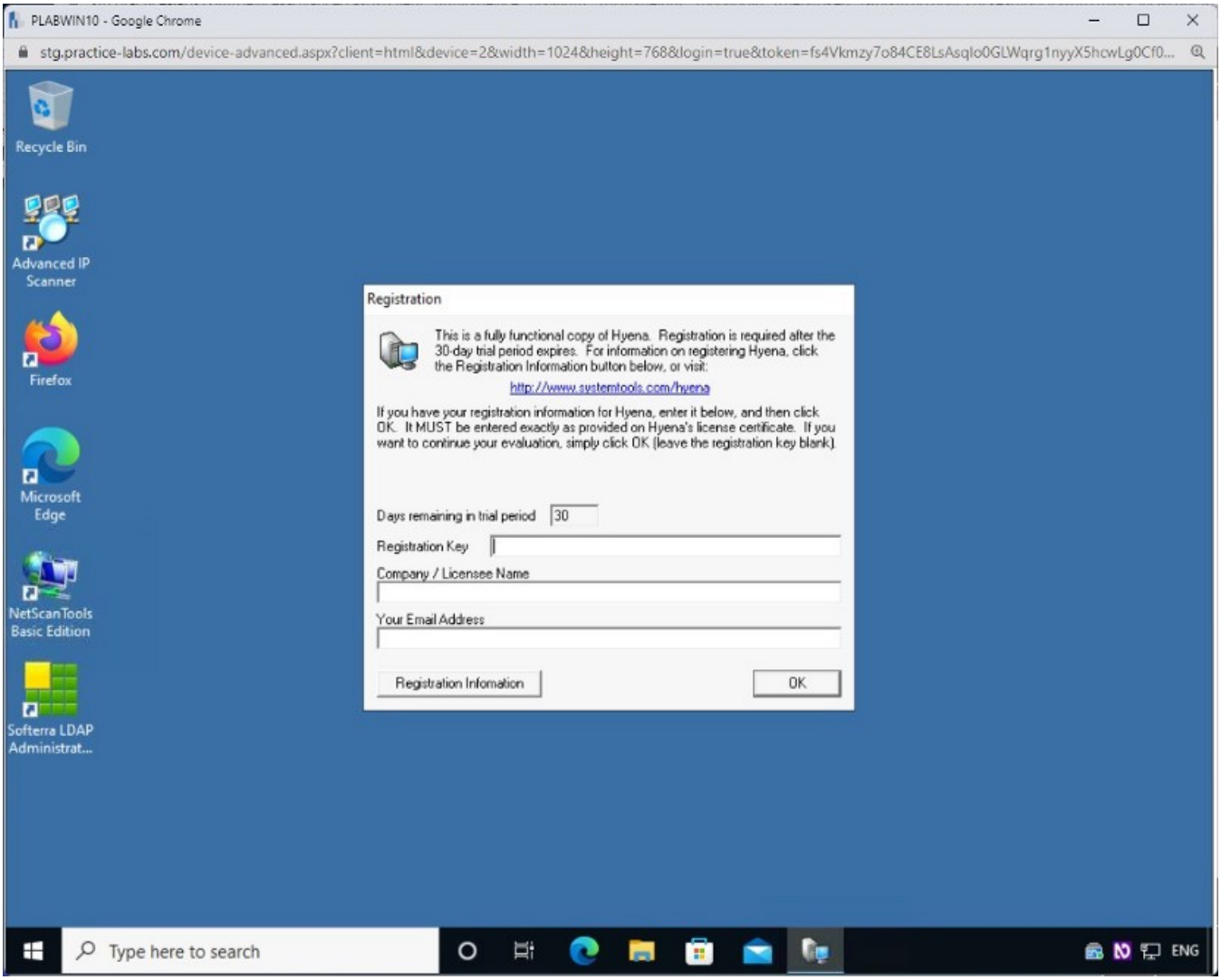
Click **Close**.



Step 3

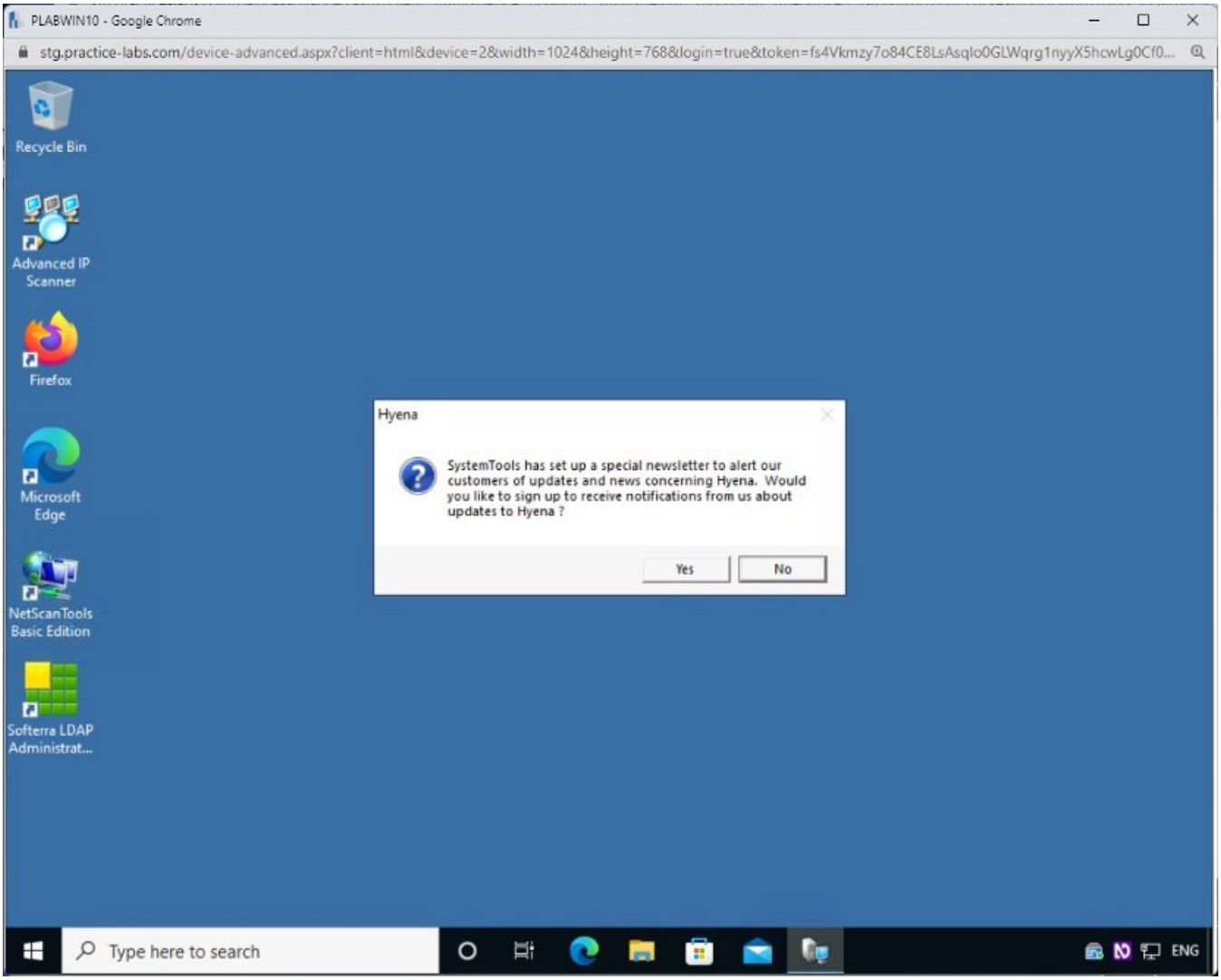
On the **Registration** dialog box, click **OK**.

You can skip the registration process.



Step 4

On the **Hyena** dialog box, click **No**.

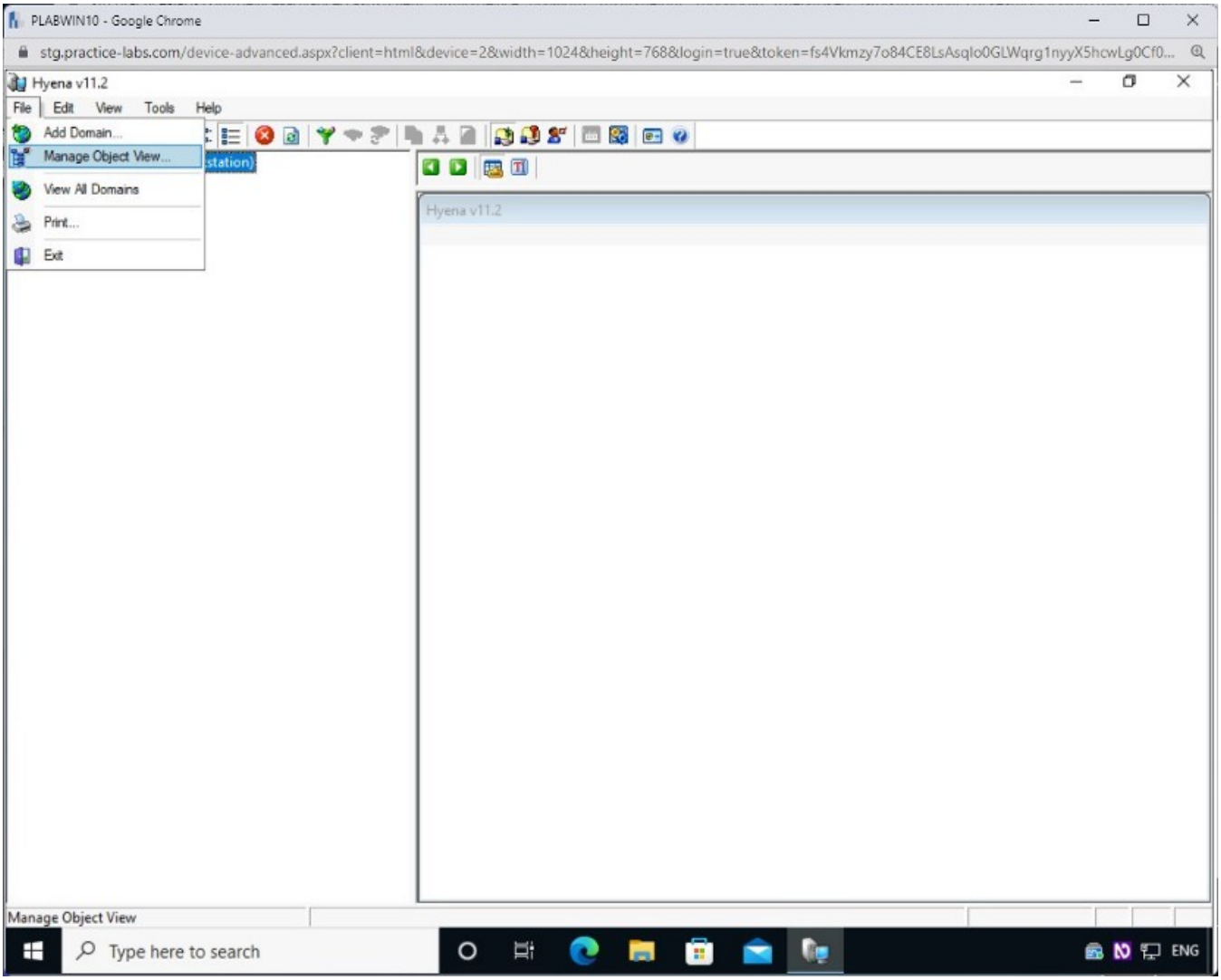


Step 5

The **Hyena v11.2** window is displayed. It is divided into the left and right panes.

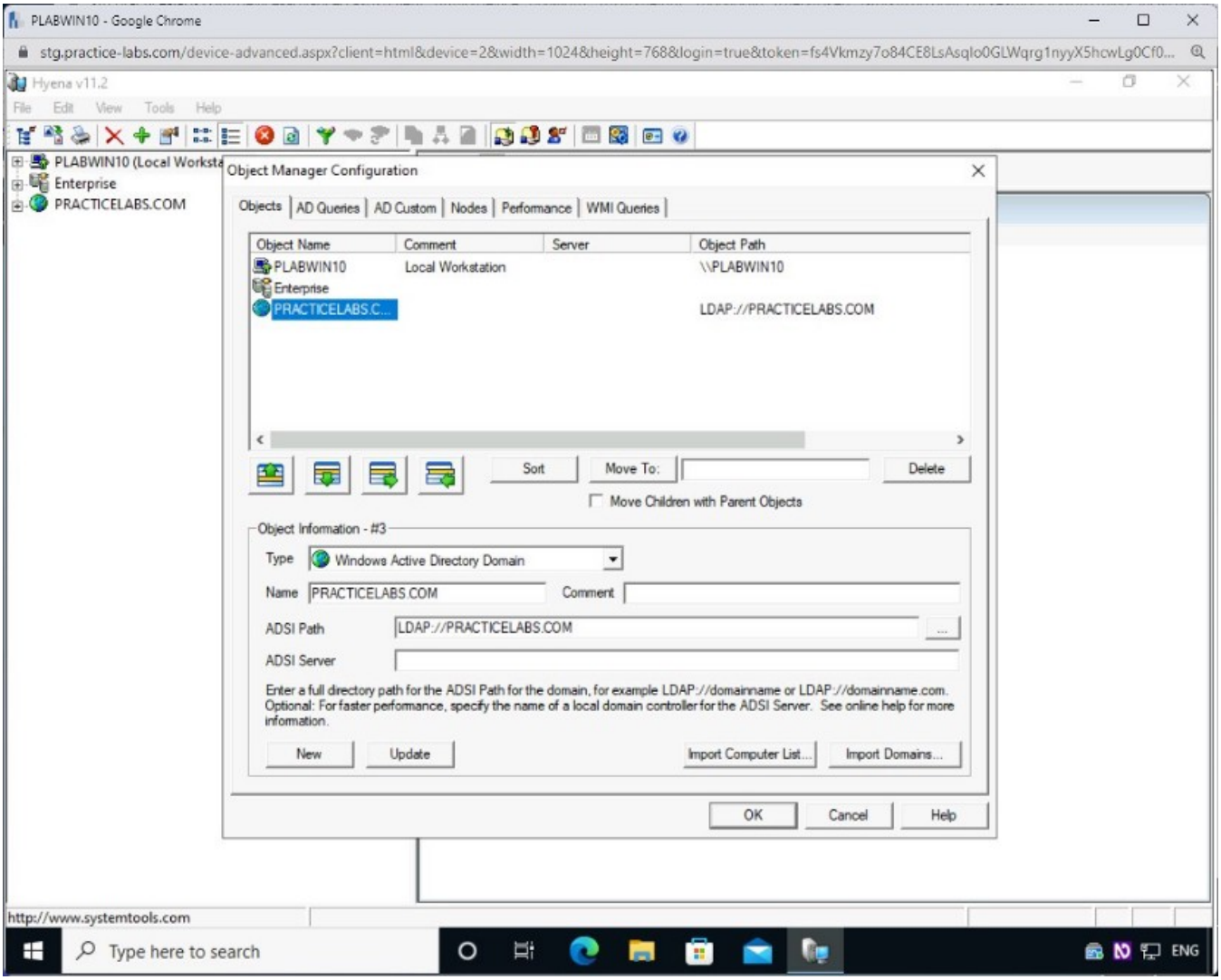
In the left-hand pane, the **PRACTICELABS.COM** domain has already been added automatically.

To remove a domain, click **File** and then select **Manage object View.**



Step 6

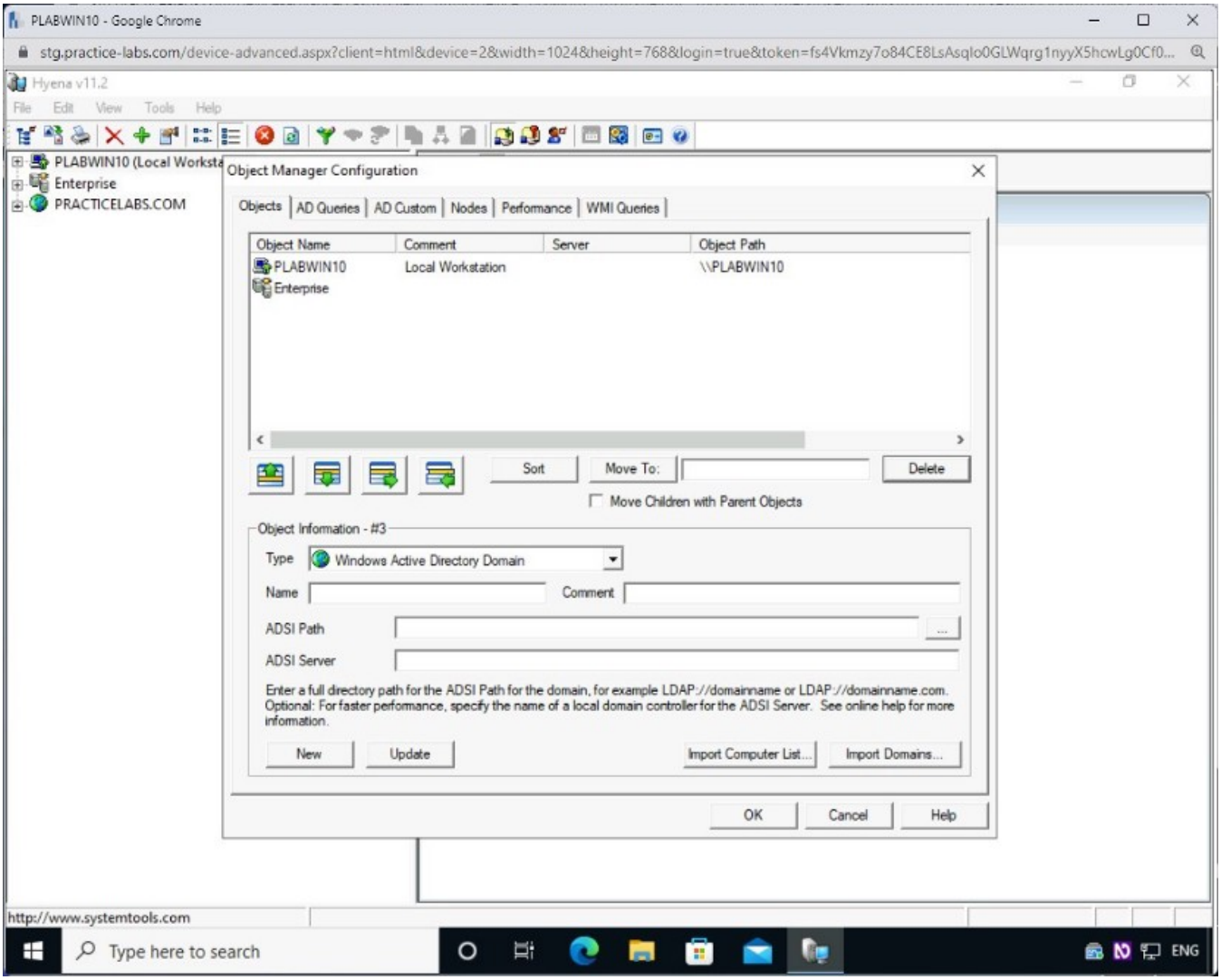
In the **Object Manager Configuration** dialog box, select the **PRACTICELABS.COM** domain under the **Object Name** column and click **Delete**.



Step 7

The **PRACTICELABS.COM** domain is removed now.

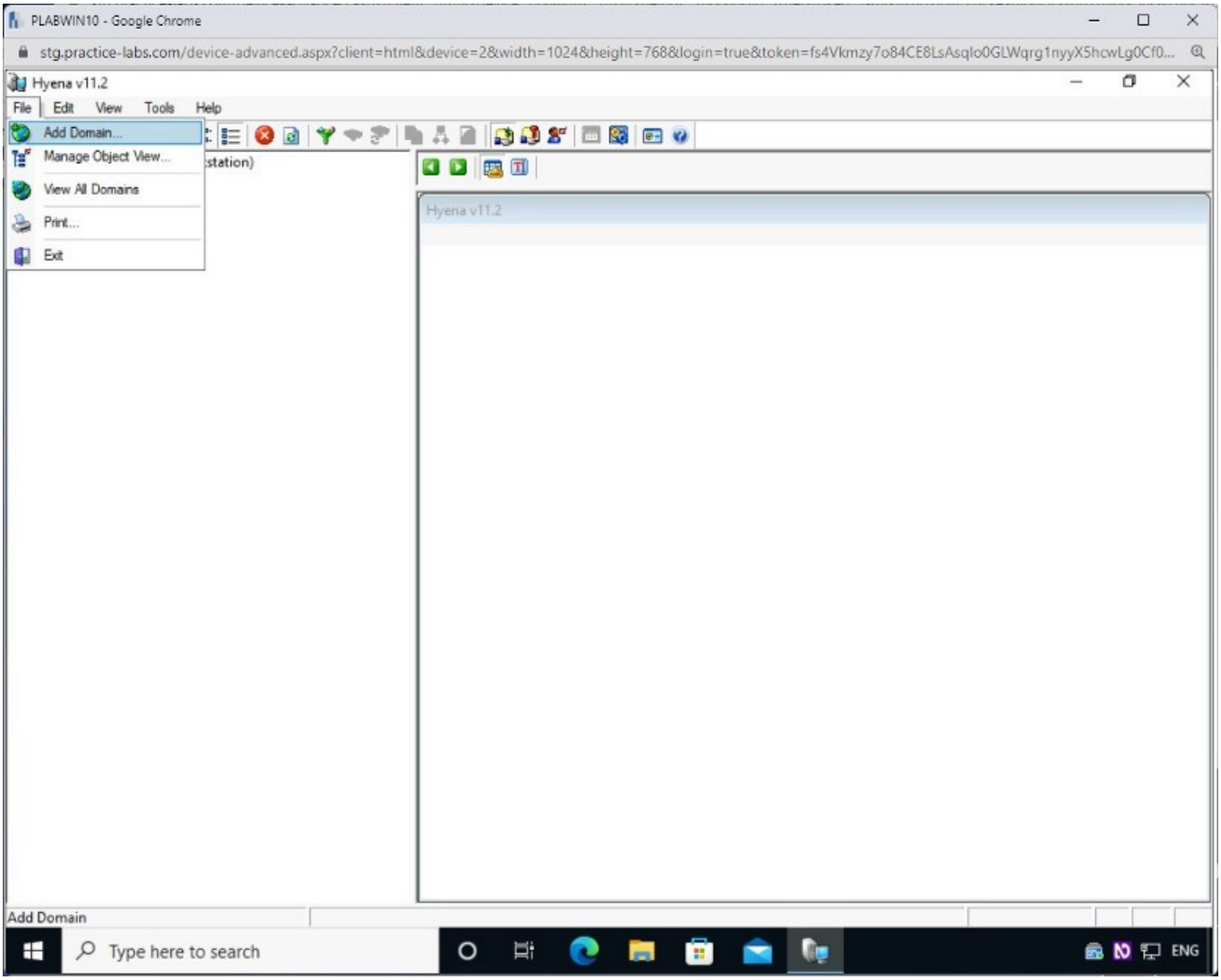
Click **OK** to close the **Object Manager Configuration** dialog box.



Step 8

You are back on the **Hyena v11.2** window. Notice that the **PRACTICE-LABS.COM** domain is no longer listed in the left pane.

To add a domain, click **File** and **Add Domain**.



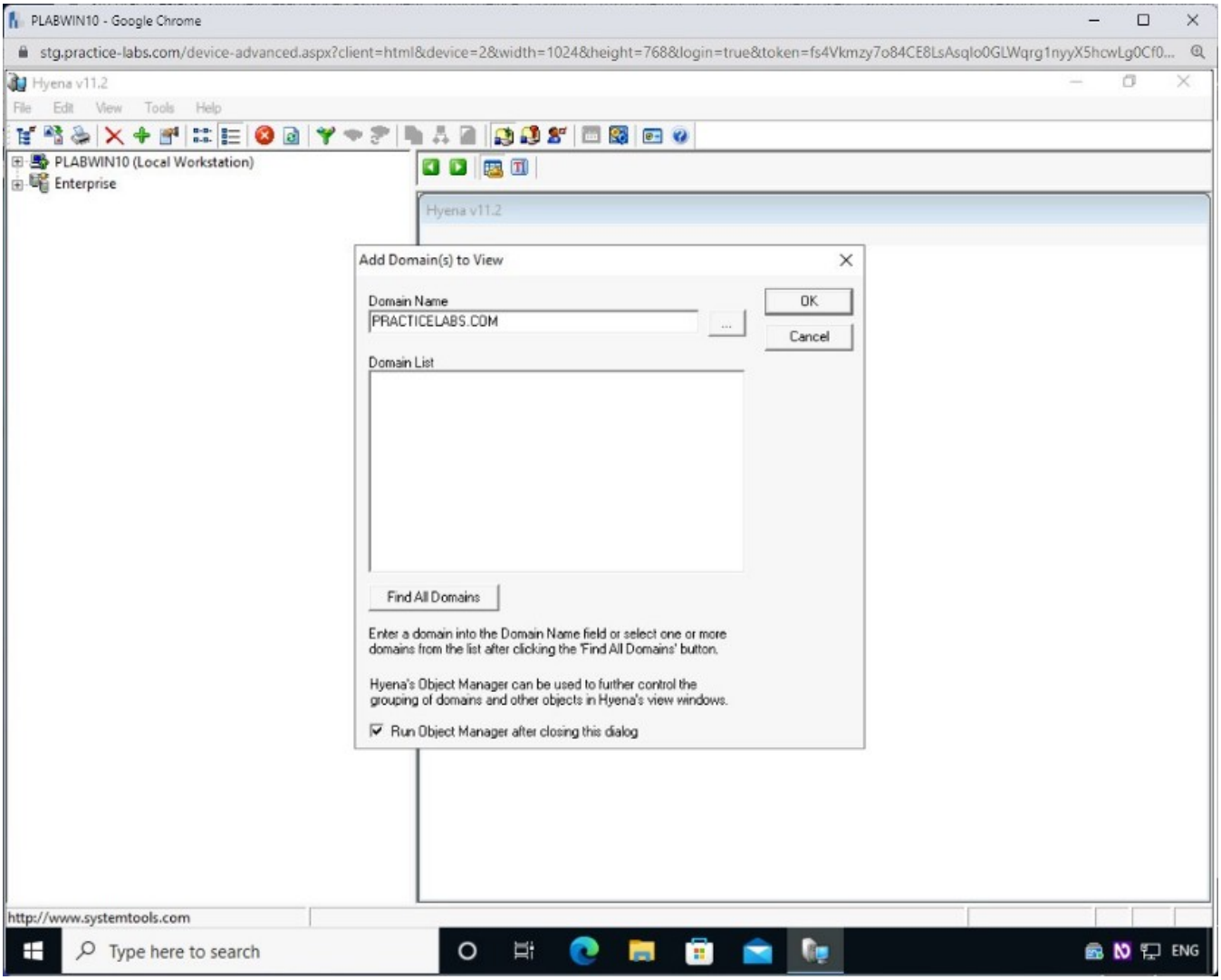
Step 9

The **Add Domain(s) to View** dialog box is displayed.

In the **Domain Name** text box, type the following domain name:

```
PRACTICELABS.COM
```

Click **OK**.

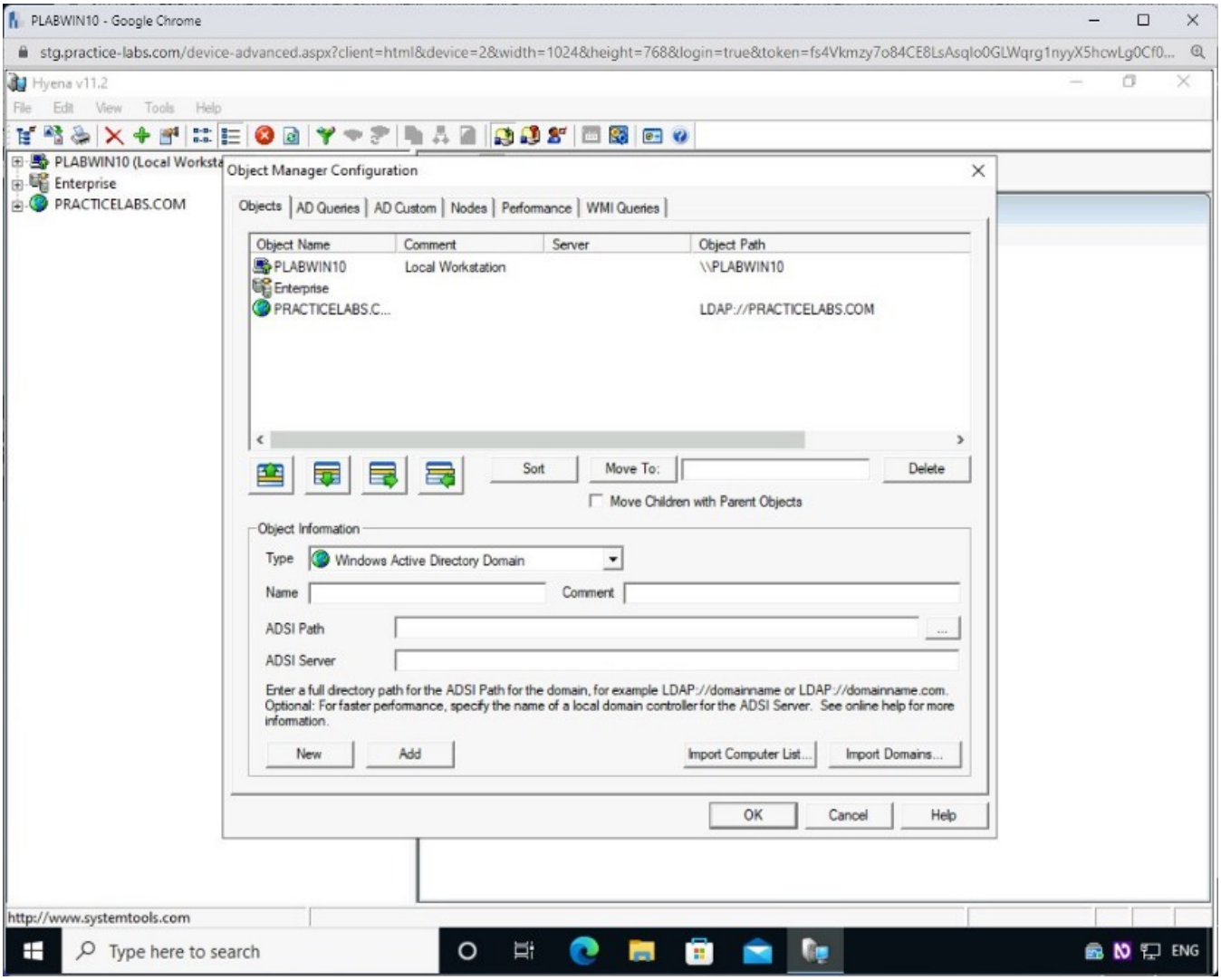


Step 10

The **PRACTICELABS.COM** domain reappears in the left pane.

Along with this, the **Object manager Configuration** opens automatically.

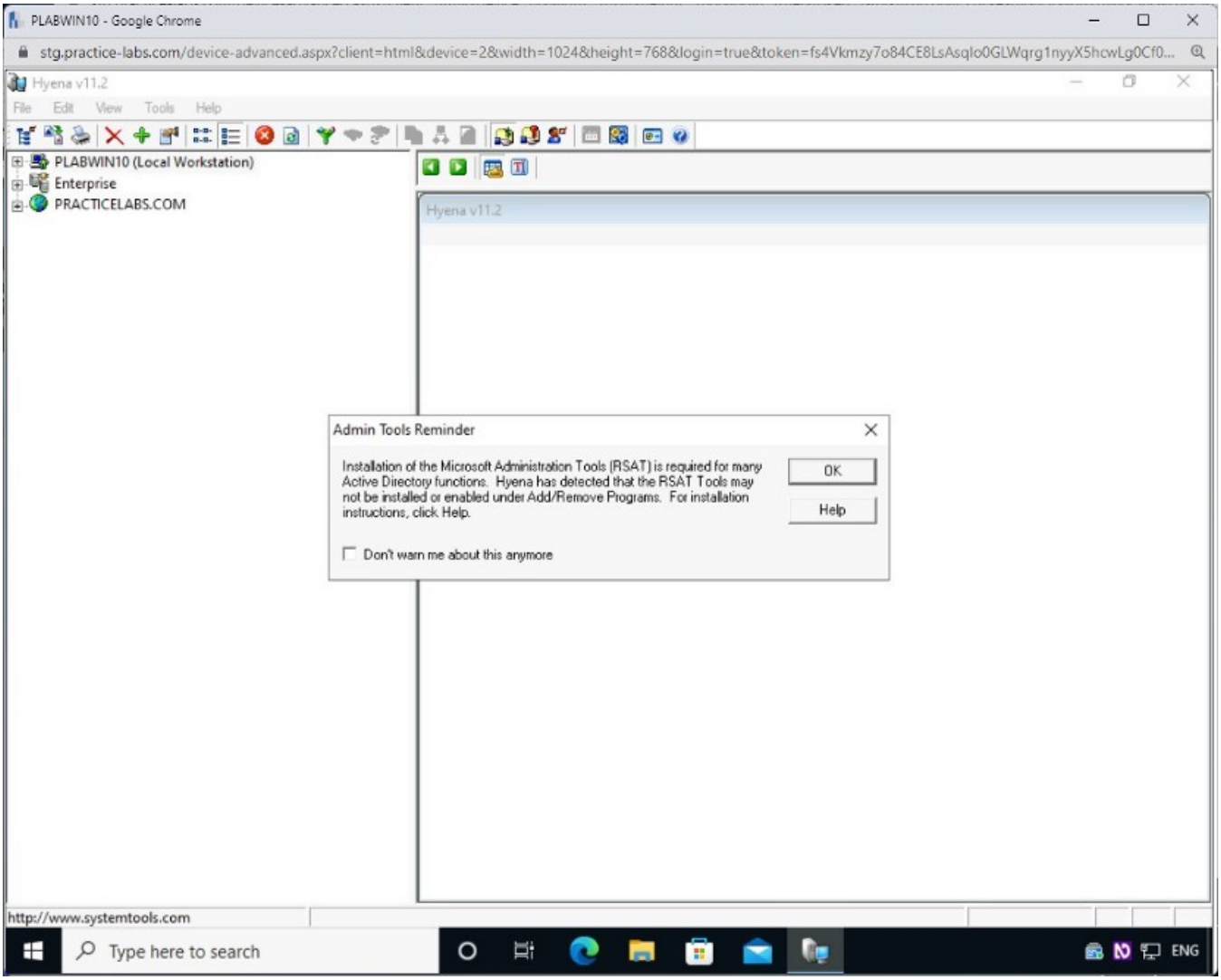
Click **OK** to close it.



Step 11

In the left-hand pane, expand **PRACTICELABS.COM**.

The **Admin Tools Reminder** dialog box is displayed. Click **OK**.



Step 12

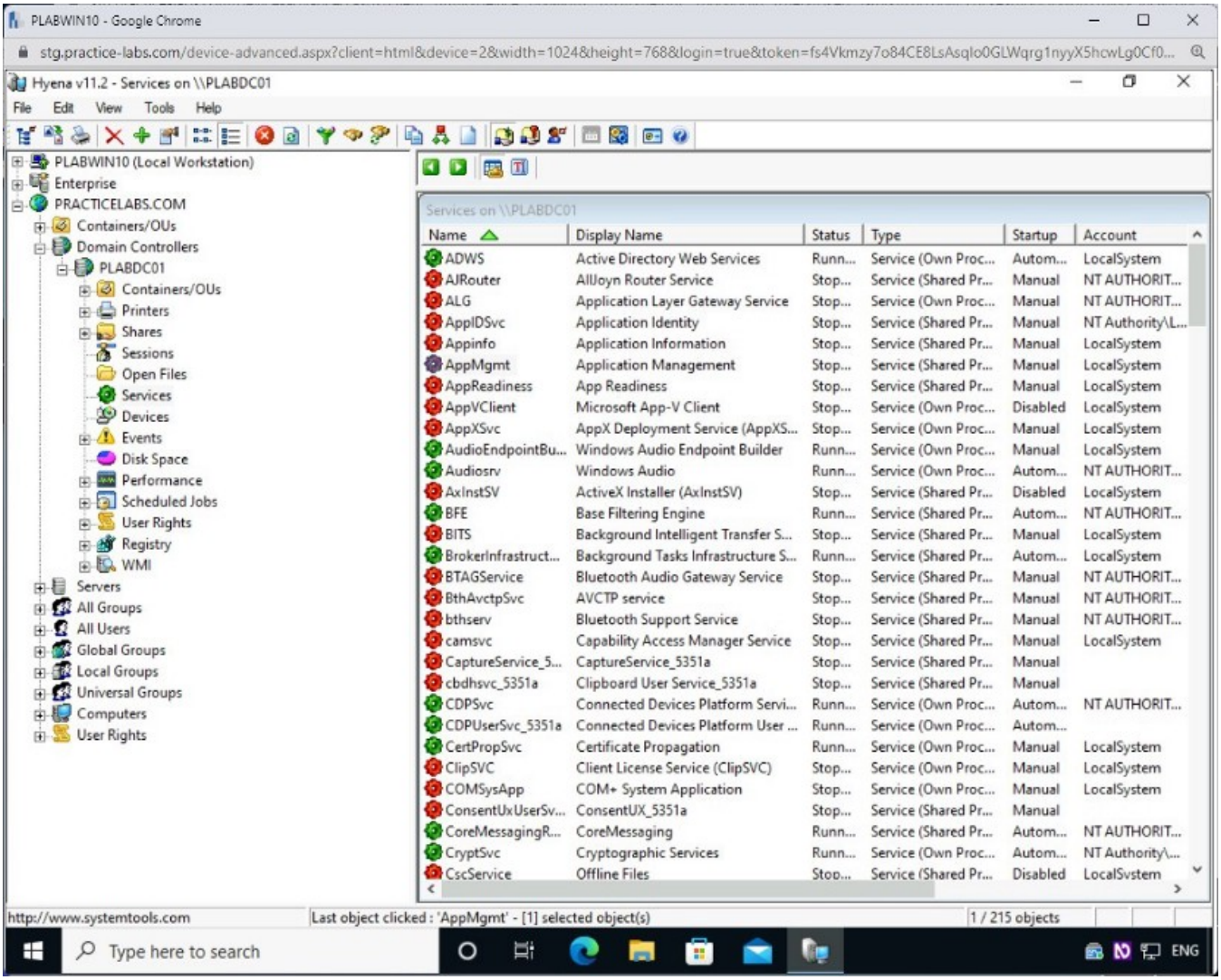
You should now notice several nodes that are now visible below **PRACTICELABS.COM**.

Expand **Domain Controllers** >**PLABDC01**, and then double-click **Services**.

***Note**: You can click on various nodes and view information. It may take a few moments for the services to populate.*

Notice that a list of services running (alongside their statuses) on **PLABDC01** is displayed. This information is useful to an attacker for discovering vulnerabilities for exploitation.

As an example, you will note that the **Application Layer Gateway Service** (**ALG**) has been stopped in the lab environment — which could indicate an attack vector.

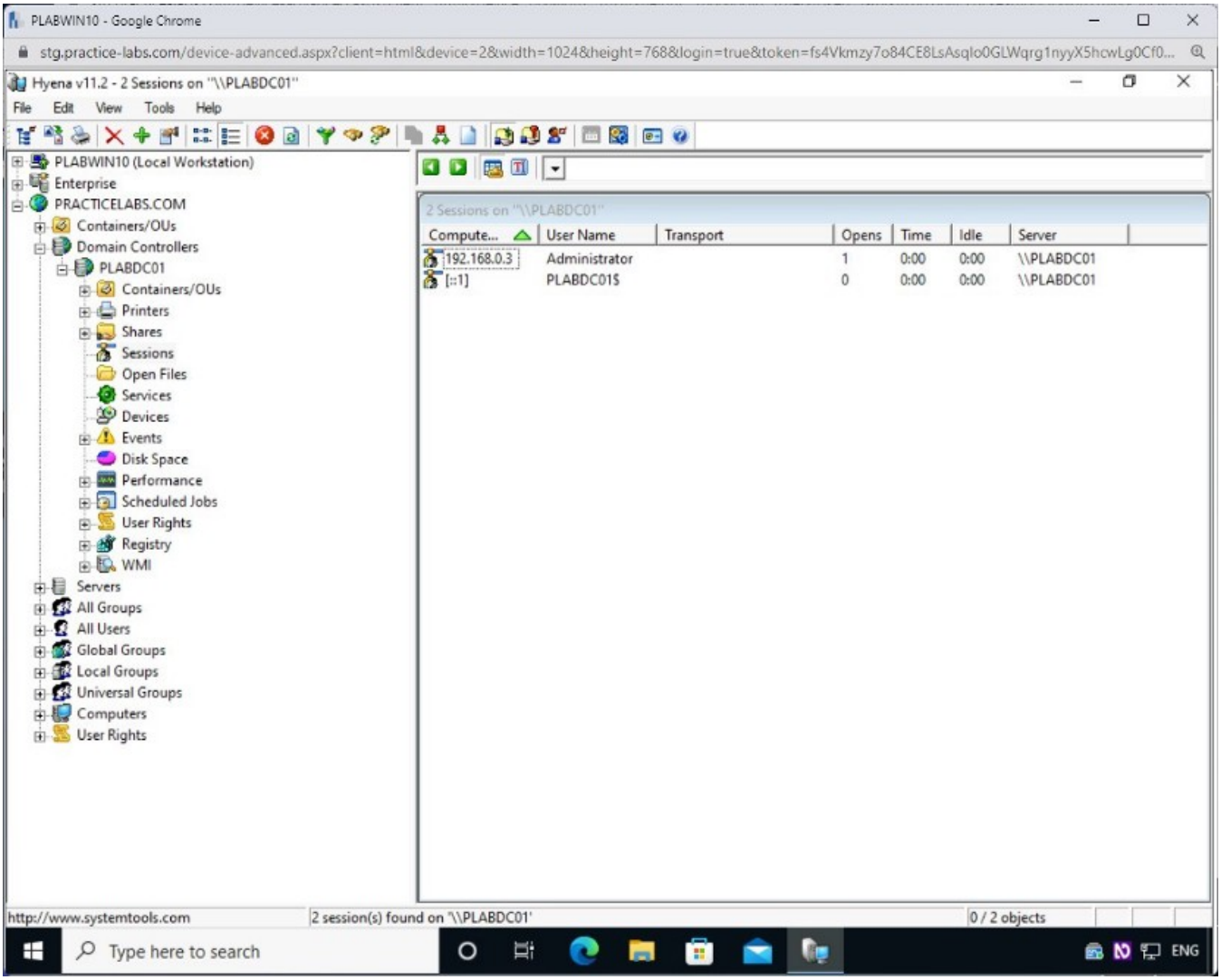


Step 13

Double-click **Sessions**.

The right-hand pane displays the number of established sessions, information useful to perform Session Hijacking attacks.

***Note**: The current number of users may vary from the screenshot below.*

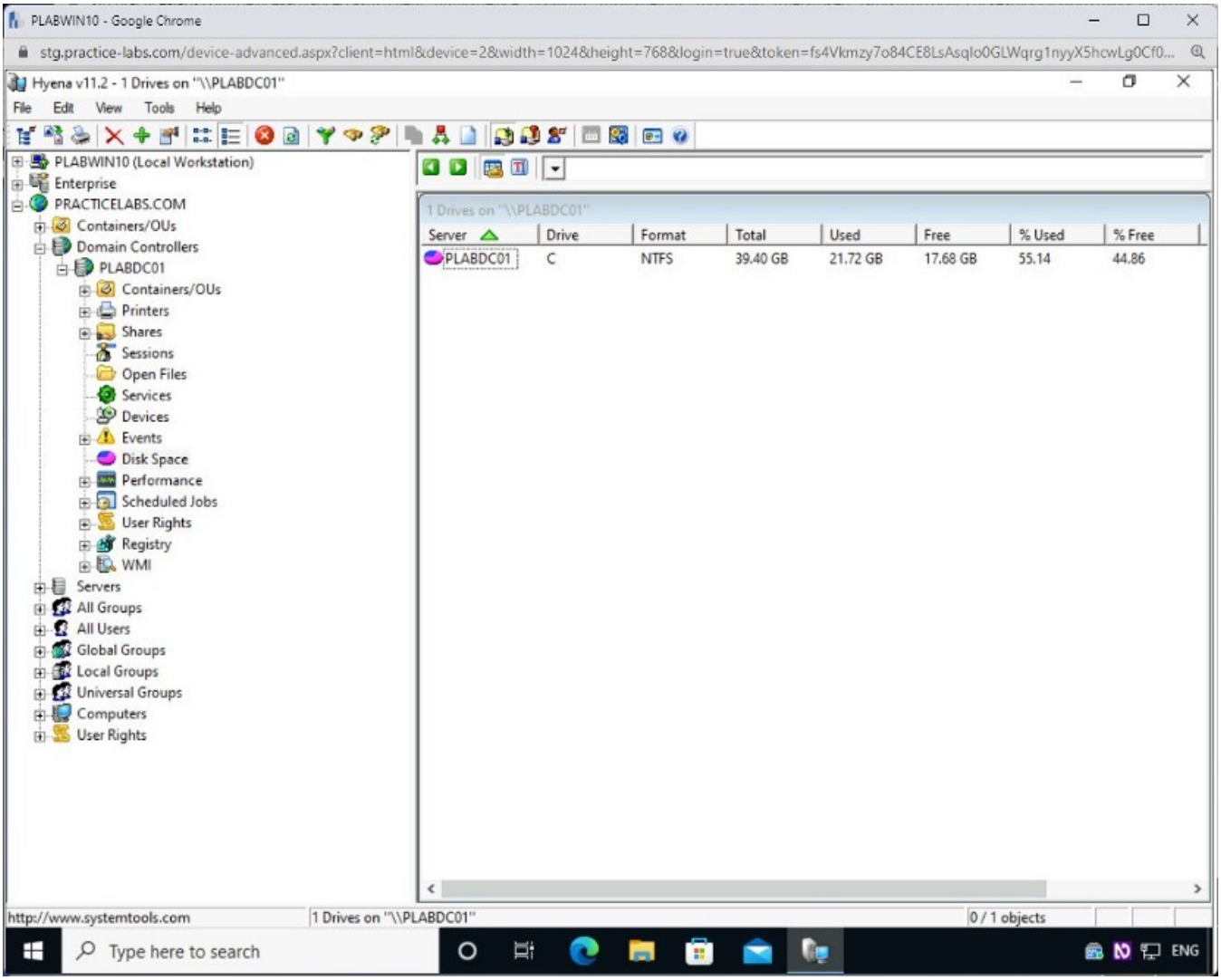


Step 14

Double-click **Disk Space**.

The right-hand pane displays the available drives and information on space such as total, free, and used space.

Again, useful information for an attacker looking to perform disk-based Denial of Service (DoS) attacks, among others.



Close all open windows.

Task 6 — Perform Website Enumeration using Nmap

There are different methods to enumerate a Website. For example, you can use a manual method using a web browser. You can try:

```
http://www.plab.com/admin
```

After the URL, you can add a directory name, such as admin. You are likely to get one of the following responses:

- **200** — OK
- **401** — Unauthorized
- **402** — Payment Required

- **403** — Forbidden
- **404** — Not Found

If the admin does not return a **404** error but something else, such as **403**, it indicates clearly that this directory exists.

You can also enumerate a website using Nmap, which provides several scripts to enumerate different websites, such as WordPress or Drupal.

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

Step 1

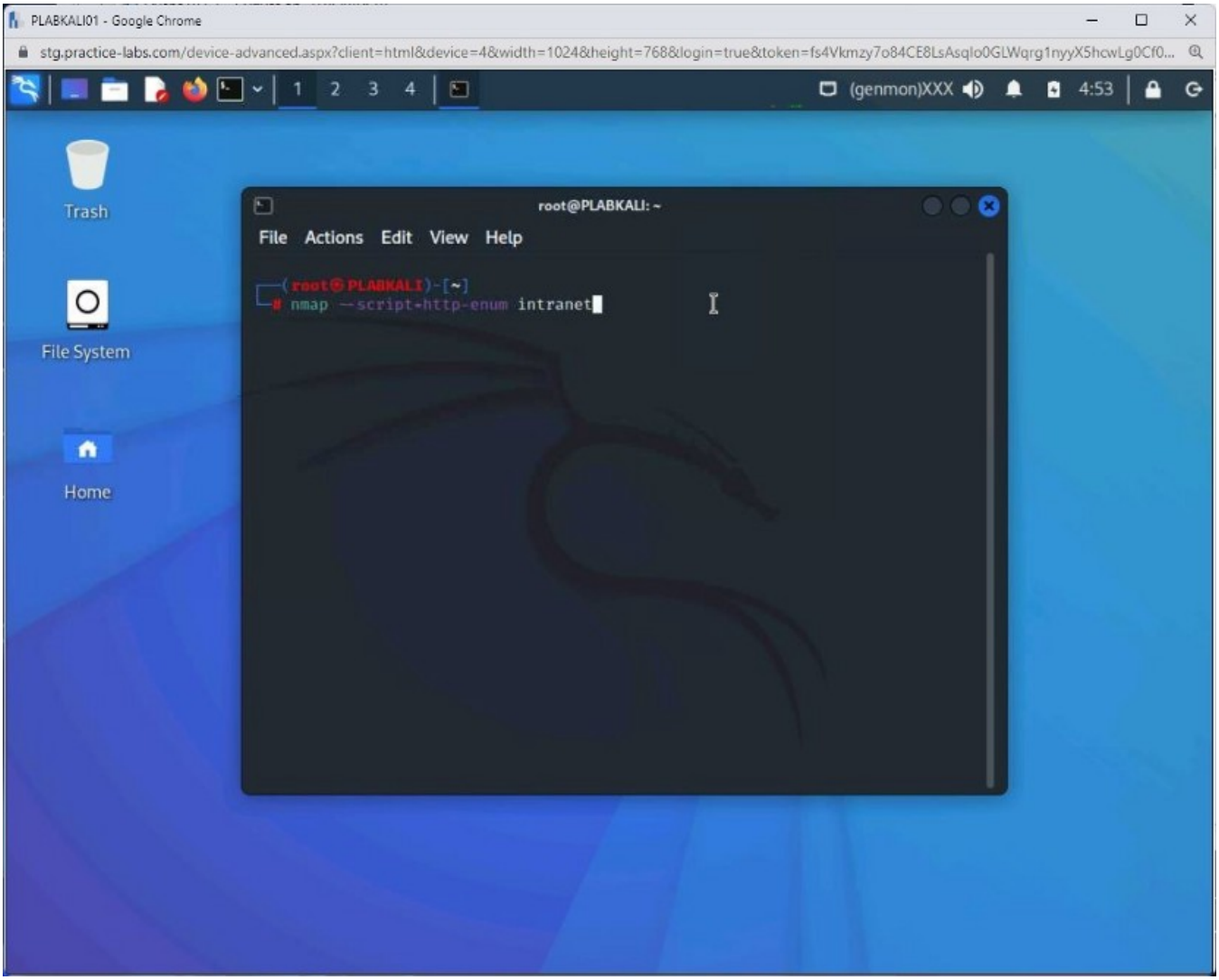
Reconnect to **PLABKALI01** and open a new terminal window.

To perform a website enumeration, type the following command:

```
nmap --script=http-enum intranet
```

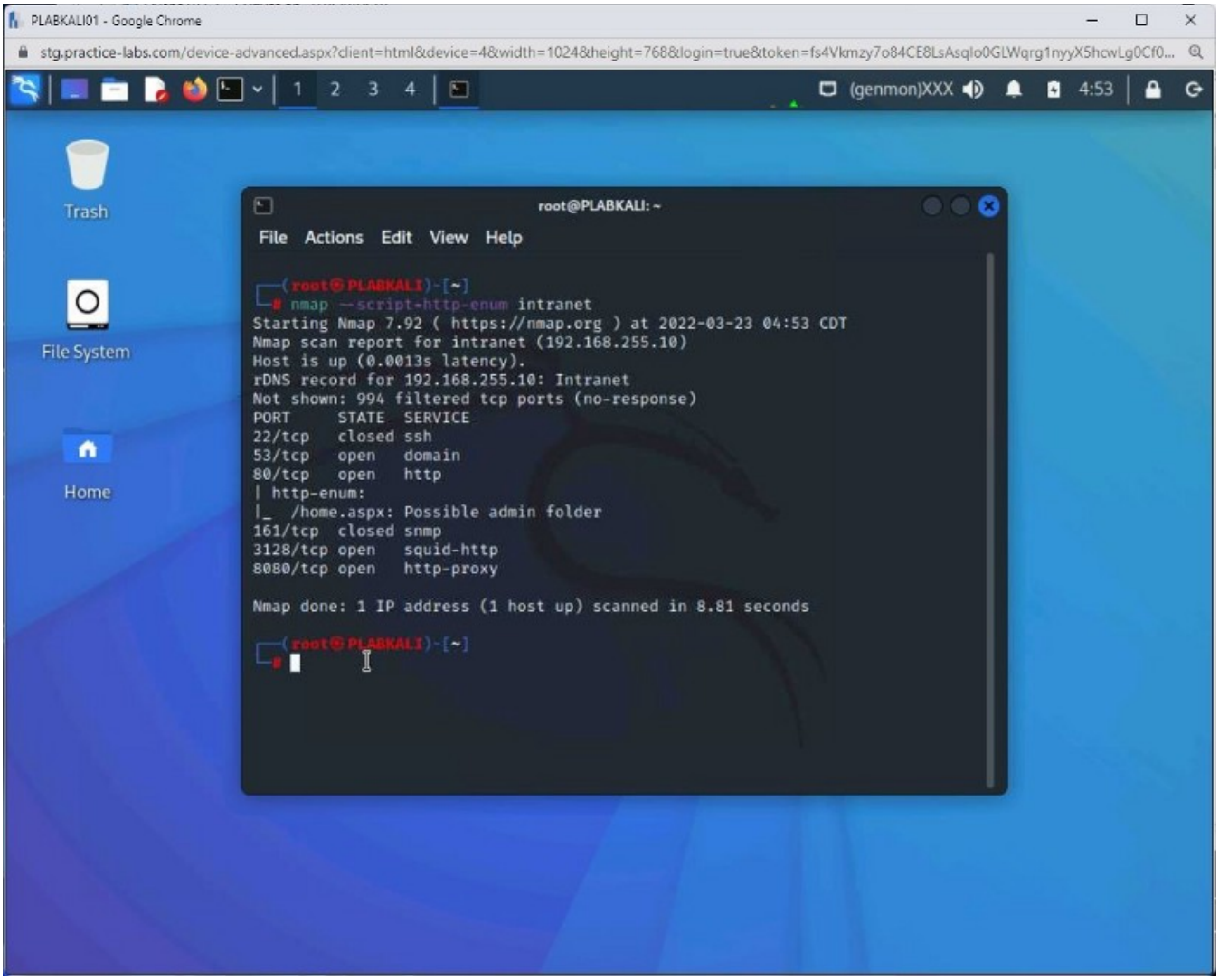
Press **Enter**.

Note: *This command may take a few minutes to provide output.*



Step 2

Notice the output. It has been able to list the open ports and a possible admin folder.



Exercise 4 — Enumeration Countermeasures

As there are different types of enumerations, such as SNMP and DNS, you need to use different prevention methods. For example, a web application enumeration can be prevented using a Web Application Firewall (WAF).

In this exercise, you will learn about enumeration prevention techniques using Kali Linux tools.

Learning Outcomes

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

- Preventing Web Applications Enumeration
- Preventing SNMP Enumeration
- Preventing LDAP Enumeration
- Preventing DNS Enumeration

- Preventing Windows Enumeration

Your Devices

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

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

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2019.2 — Linux Kali Workstation192.168.0.5/24

Task 1 — Prevent Web Applications Enumeration

Web application enumeration can be prevented using a Web Application Firewall (WAF). The wafw00f tool helps determine whether the Web application is behind a WAF.

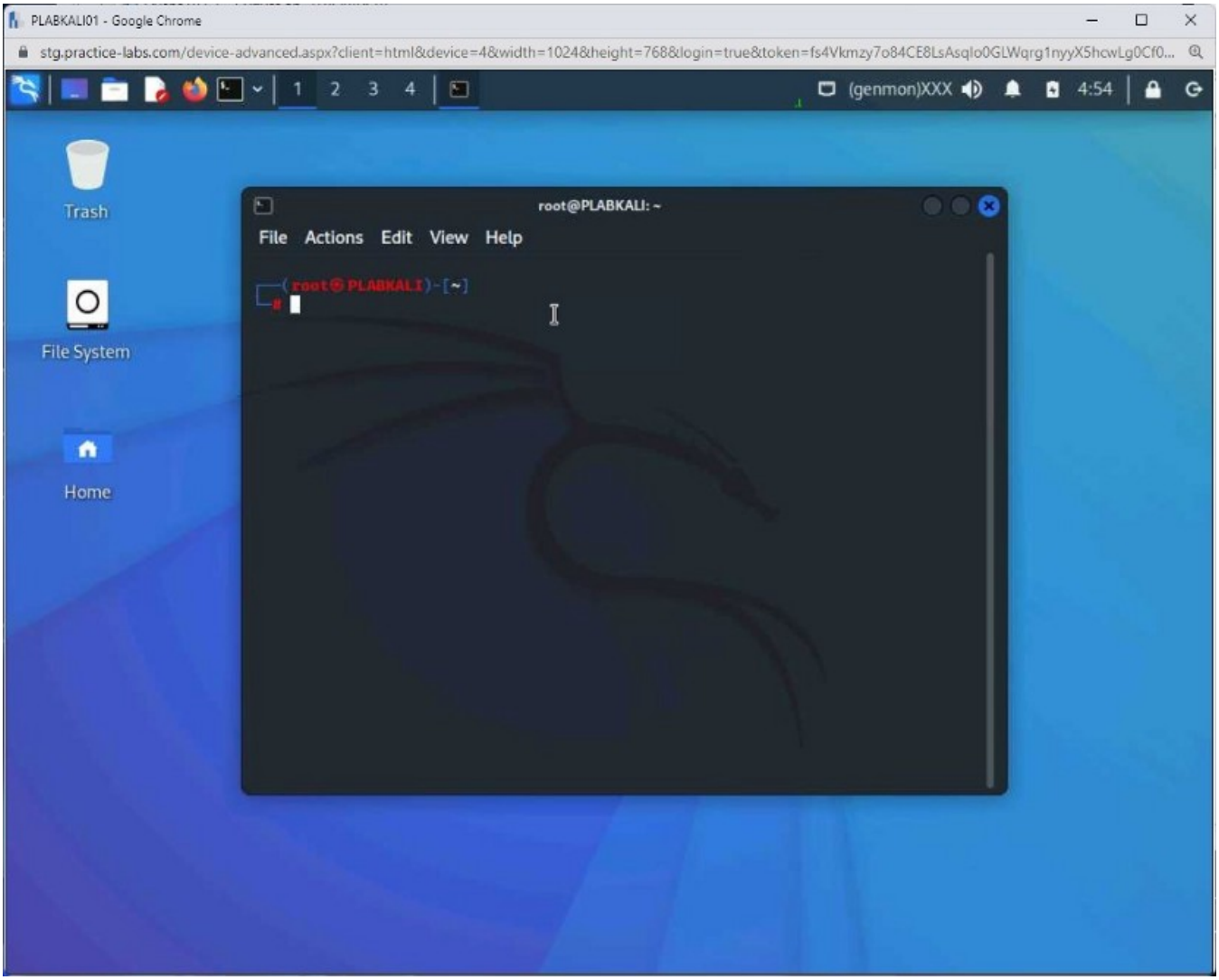
A hacker may want to analyze the application before launching an attack. wafw00f is a useful tool to determine whether the application is behind a firewall. Accordingly, the attacker may decide the next course of action.

***Note**: Using Wafw00f to detect a WAF has also been covered in a previous module.*

In this task, you will learn to use wafw00f. To do this, perform the following steps:

Step 1

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



Step 2

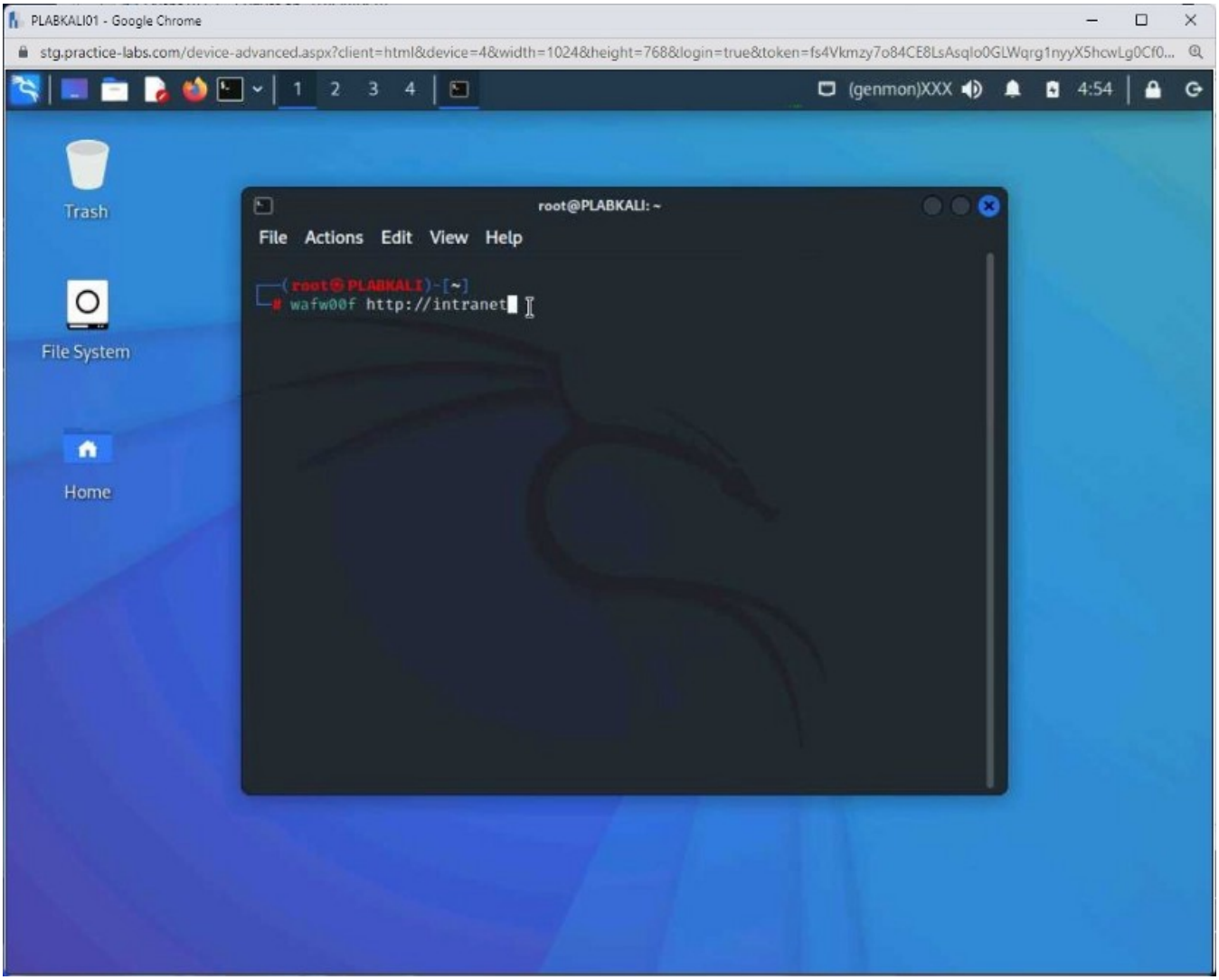
You will determine whether a web application is behind the **Web Application Firewall (WAF)**.

You will use a tool named **wafwoof** for this purpose.

Type the following command:

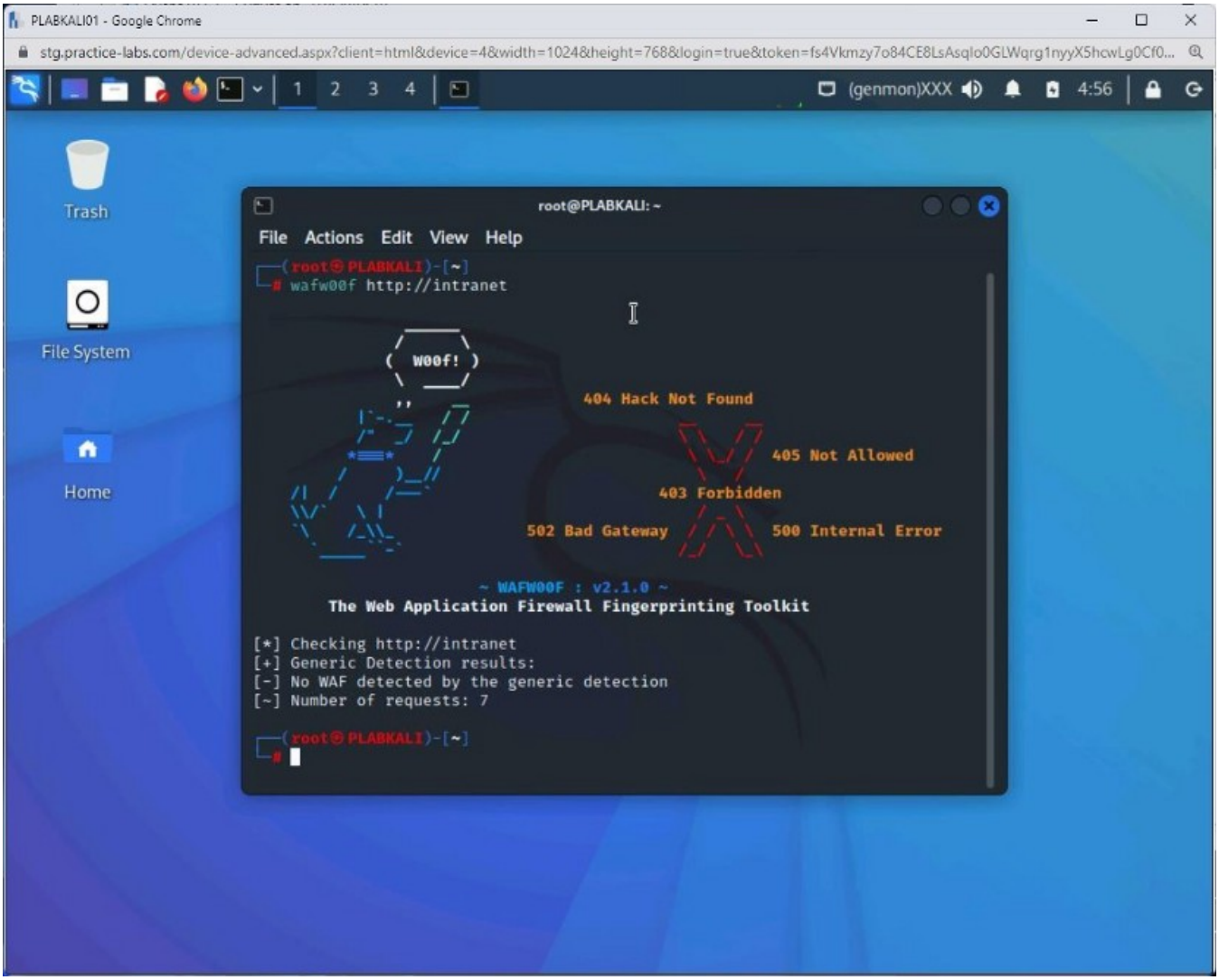
```
wafw00f http://intranet
```

Press **Enter**.



Step 3

Notice that the output has detected not detected a **WAF**.



Methods of Prevention

In the above exercises, you learned that you could perform Enumeration using different methods. Let's investigate how to prevent these methods from being performed.

Prevent DNS Enumeration

DNS enumeration can be prevented using the following methods:

- DNS zone transfers to done with the authenticated and known hosts
- DNS zone transfers must not include the HINFO information
- Keep the private and public DNS server separate. Private zone information should not be published to public DNS servers

Along with above, you should ensure that DNS zone files include only the necessary information. These files should not be able to reveal extra information.

Prevent Windows Enumeration

Windows enumeration can be prevented with the following methods:

- Stop unnecessary services from running
- Close open ports that are not in use
- Configure a firewall on the Windows host

Prevent FTP Enumeration

FTP enumeration can be prevented with the following methods:

- Replace FTP with SFTP or FTPS
- Implement either complex password policy or use certificate-based authentication
- Disable the default anonymous authentication to the FTP server
- Limit the access to the FTP server by IP or domain name
- Enable access control lists or ACLs on the FTP server

Prevent SMTP Enumeration

SMTP enumeration can be prevented with the following methods:

- Disable the open relay feature on the messaging server
- Install and configure SPAM filter
- Disable the EXPN, RCPT TO, and VRFY commands
- Hide sensitive information in the mail messages