CEH v12 Lesson 8 : Network Sniffing Techniques & Attacks

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 — Sniffing Concepts
- Exercise 2 — Sniffing Tools
- Exercise 3 — Sniffing Technique: MAC Attacks
- Exercise 4 — Sniffing Technique: DHCP Attacks
- Exercise 5 — Sniffing Technique: DNS Poisoning
- Exercise 6 — Sniffing Countermeasures and Detection Methods

After completing this module, you will be able to:

- Use Wireshark
- Perform Media Access Control (MAC) Flooding with Macof
- Perform MAC Flooding using Yersinia
- Use macof to Flood Switches with MAC Addresses
- Launch the DHCP Starvation Attack
- Use DNSChef
- Use XArp Utility

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

- Sniffing Concepts
- Types of Sniffing
- Steps in Sniffing
- Vulnerable Protocols

- Methods to Defend Against Sniffing
- Methods to Detect Sniffing

Lab Duration

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

Lab Topology

During your session, you will have access to the following lab configuration.

Depending on the exercises, you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.

- 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

- PLABDROID

Android Device192.168.0.4/24

- PLABKALI01

Kali 2022.1 — Linux Kali Workstation192.168.0.5/24

Exercise 1 — Sniffing Concepts

Sniffing is a process in which data packets traveling over a network are captured by a tool such as Wireshark. A network adapter configured to promiscuous mode can capture packets in transit.

In this exercise, you will learn about the various concepts related to sniffing and its tools.

Learning Outcomes

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

- Sniffing Concepts
- Types of Sniffing
- Steps in Sniffing
- Vulnerable Protocols

Sniffing Concepts

Imagine someone planting a microphone and listening to the conversation between you and your friends. The concept of sniffing works in the same manner, and someone can capture and monitor whatever network traffic is sent over a network. If the traffic is not encrypted, it is an added advantage for the attacker who would retrieve information, such as passwords, from captured traffic. Any information transmitted in cleartext is available to the attacker to read through.

This can be the starting point of a breach or attack. For example, an attacker can gain user credentials, which are then used to break into a system.

Types of Sniffing

Sniffing can either be passive or active. During passive sniffing, the sniffing system does not send out packets, rather it simply captures packets sent to it. The network interface card of the sniffing computer is set to promiscuous mode which means it will read all packets, regardless of the MAC address. Passive sniffing is done by connecting the sniffing system to a hub.

Alternatively, for active sniffing, the sniffing system is connected to a switch. Since the switch sends traffic through a switchport to the MAC address specified in the CAM table, If the MAC address is not in the CAM table, the switch will send it out through all switchports. Active sniffing tries to either change the CAM table settings or overflow it through various methods such as MAC flooding, spoofing attack, and ARP poisoning to confuse the switch into send the sniffing system packets being sent to a particular MAC address or any MAC address.

Steps in Sniffing

To perform sniffing, an attacker follows the following steps:

1. They connect to a network by connecting the system to a port
2. They perform network discovery using various tools
3. They find a target on the network
4. They send spoofed ARP messages to the target system
5. Using spoofed ARP messages, they divert traffic to their system
6. They become the recipient of traffic intended for another system

Vulnerable Protocols

Networks run various applications that use various protocols. For example, a messaging server can use the Post Office Protocol (POP) or the File Transfer Protocol (FTP). These protocols are vulnerable as they send information in clear text, including user credentials. Network administrators should avoid using the following vulnerable protocols:

- Telnet
- Rlogin
- HyperText Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- Network News Transfer Protocol (NNTP)
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP)

Each of these protocols are prone to sniffing attacks because they send the information and user credentials in cleartext.

Exercise 2 — Sniffing Tools

If a tool provides an advantage to a network administrator, it can also benefit an attacker. For example, in the context of sniffing, if a tool allows a network administrator to capture the network traffic for review to ensure everything is going fine, it can also be an advantage for the attacker to find a lot of valuable information.

In this exercise, you will learn about the various sniffing tools.

Learning Outcomes

After completing this exercise, you will be able to:

- Use Wireshark

Your Devices

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

PLABDC01 - Domain Controller 192.168.0.1/24

PLABWIN10Domain Member

Workstation192.168.0.3/24

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

Task 1 — Using Wireshark

Wireshark is the most sought-after packet capturing and sniffing tool. It helps you capture the live network traffic from various networks. You can use it to monitor the network or even get sensitive information like passwords transmitted in cleartext. You can also filter the traffic to find the information you are looking for.

In this task, you will learn to use Wireshark.

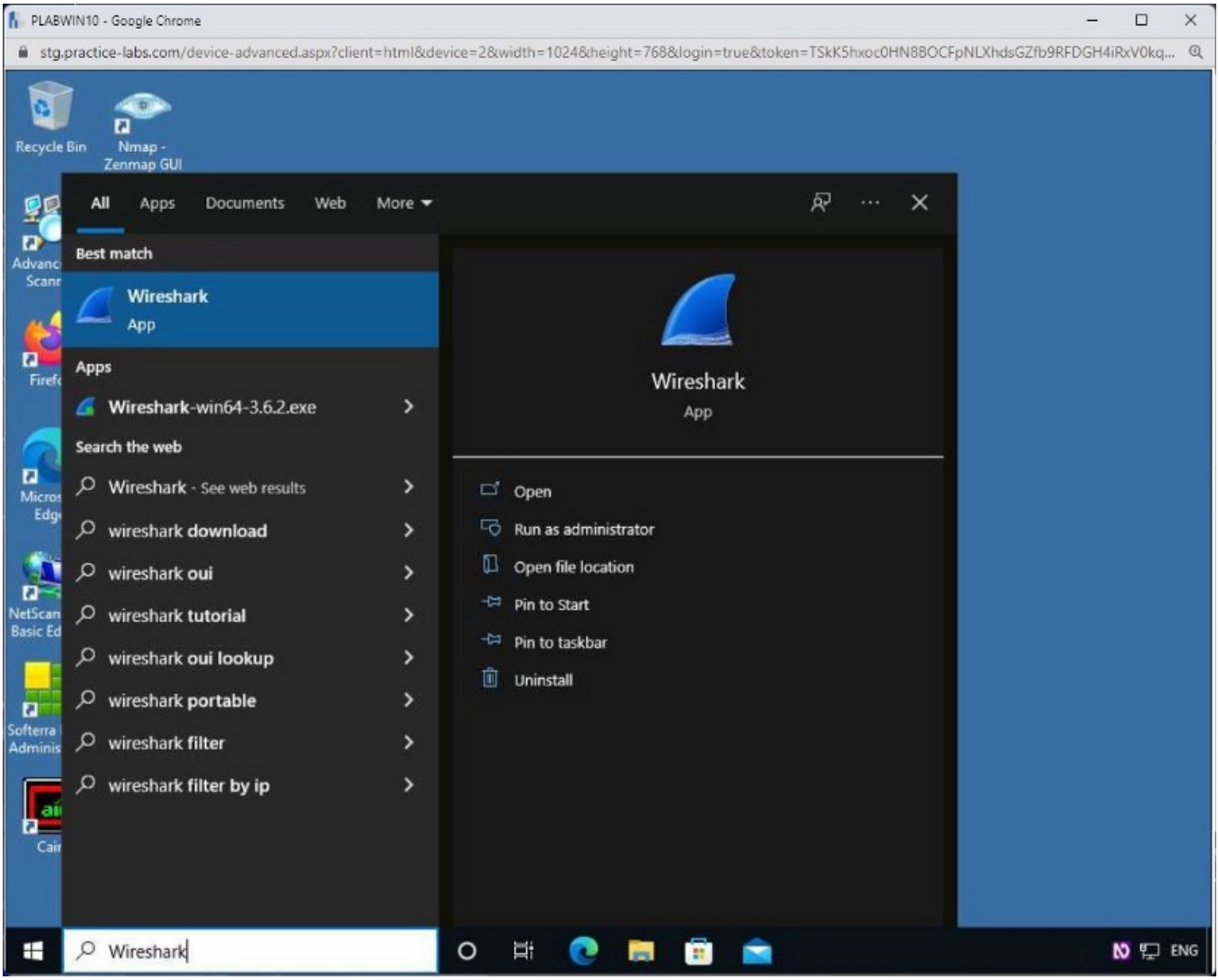
Step 1

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

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

```
Wireshark
```

From the search results, click **Wireshark**.

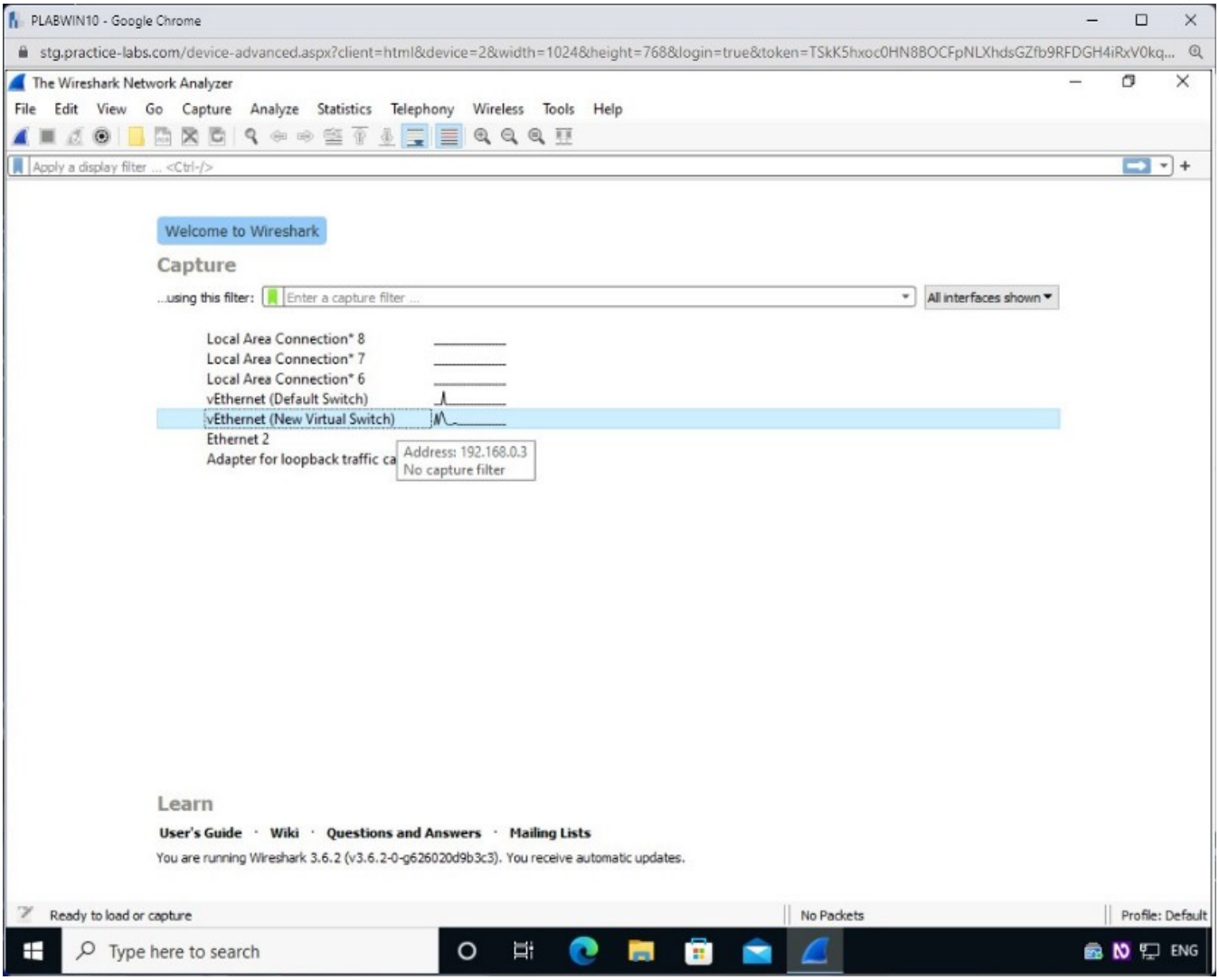


Step 2

The Wireshark Network Analyzer window is displayed.

Double-click **vEthernet (New Virtual Switch)**.

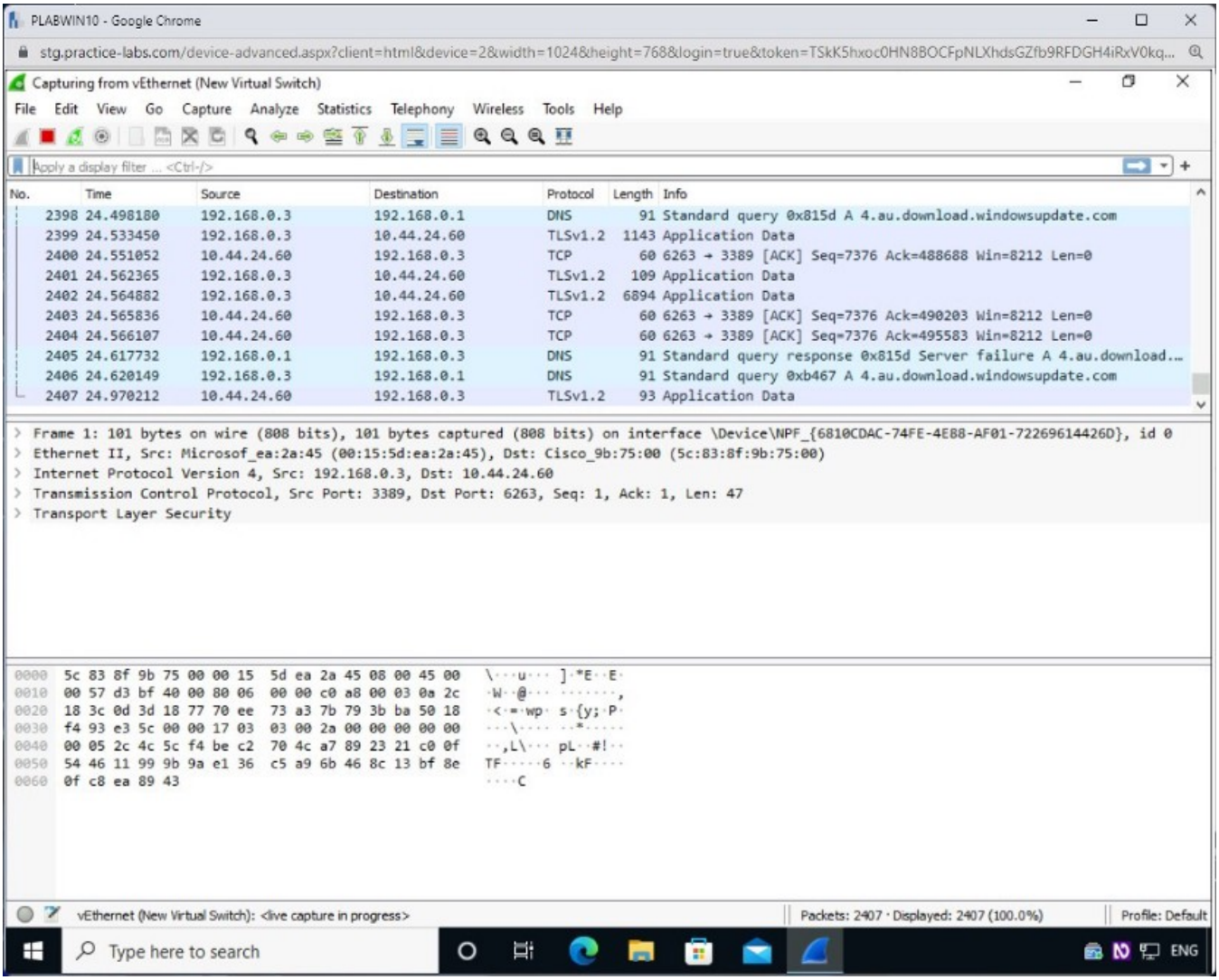
***Note**: Wireshark may prompt you to update. Please close this window if it appears.*



Step 3

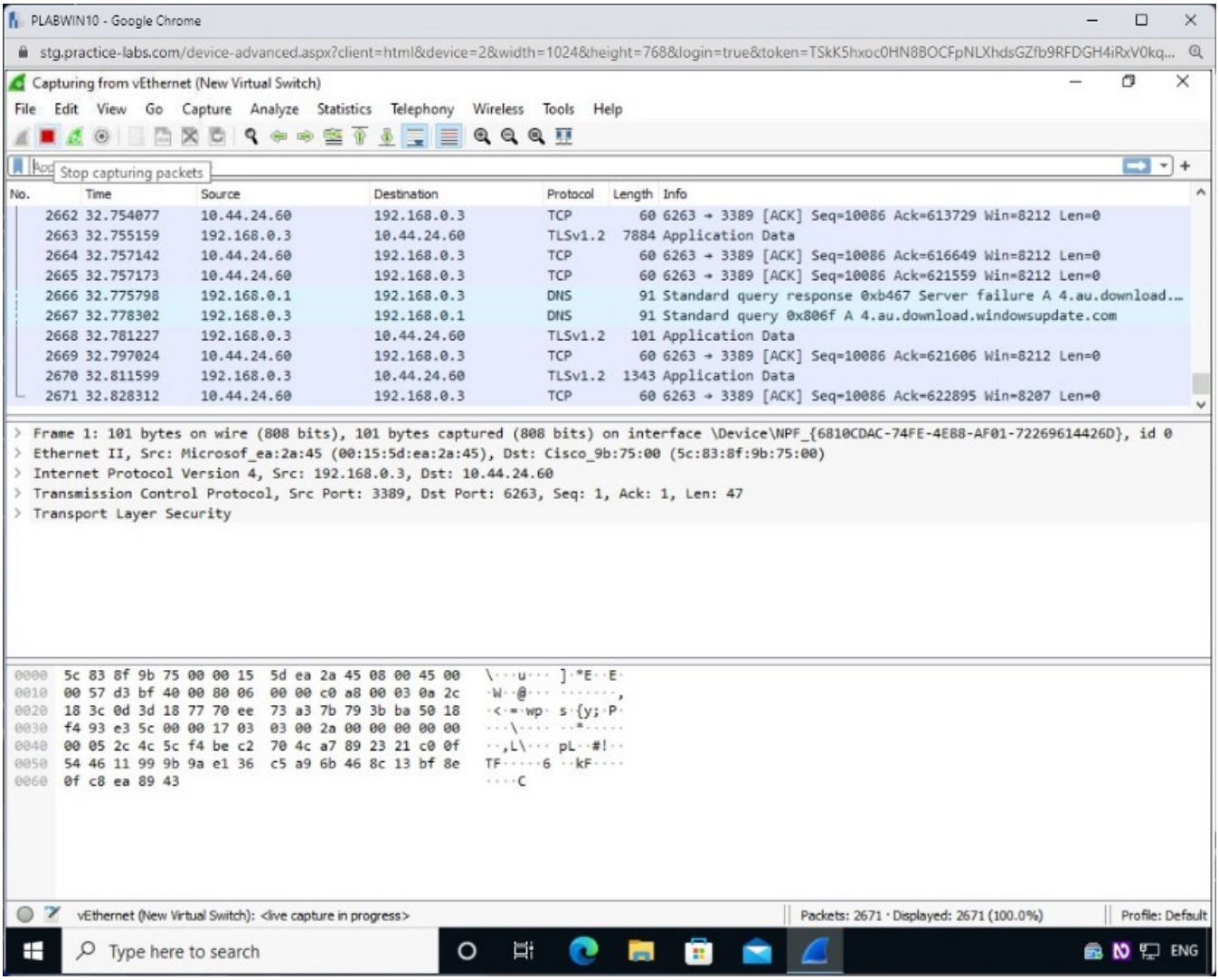
The **Capturing from Ethernet** window is displayed.

Note that there are several packets being captured.



Step 4

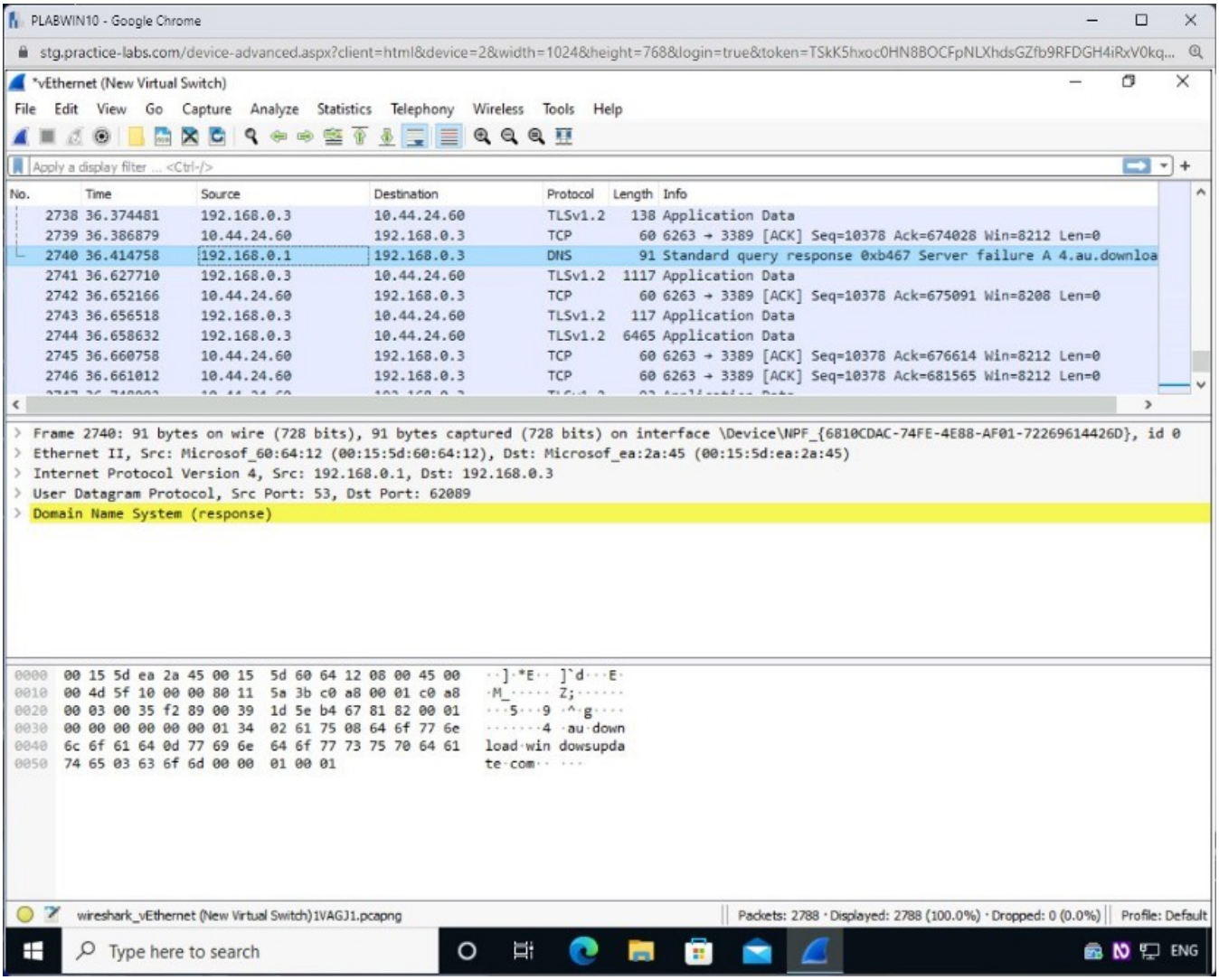
Click **Stop**.



Step 5

Packet capturing has stopped.

PLABWIN10 is in promiscuous mode, due to which its NIC was able to capture packets from all systems on the network.



Exercise 3 — Sniffing Technique: MAC Attacks

Switches rely on the MAC addresses to forward traffic to the appropriate port. An attacker can conduct a MAC attack to make a switch work as a hub. When the CAM table is filled with the spoofed MAC address, it cannot save any new MAC address and behaves like a hub.

In this exercise, you will learn to perform MAC attacks.

Learning Outcomes

After completing this exercise, you will be able to:

- Perform Media Access Control (MAC) Flooding with Macof
- Perform MAC Flooding using Yersinia
- Use macof to Flood Switches with MAC Addresses

Cert Master Lab devices

- PLABDC01

Windows Server 2019 — Domain Server192.168.0.1/24

- PLABWIN10

Windows 10 — Workstation192.168.0.3/24

- PLABKALI01

Kali 2019.2 — Linux Kali Workstation192.168.0.5/2

Task 1 — Perform Media Access Control (MAC) Flooding with Macof

The macof tool can flood a switch with a fake MAC address. When this tool sends a list of MAC addresses to a switch, it fills its CAM table. Post this, the switch cannot save any new MAC address and starts sending information to all the ports. In this task, you will learn to use macof to perform MAC flooding.

Step 1

Connect to **PLABKALI01**.

Log in using the following credentials:

Username:

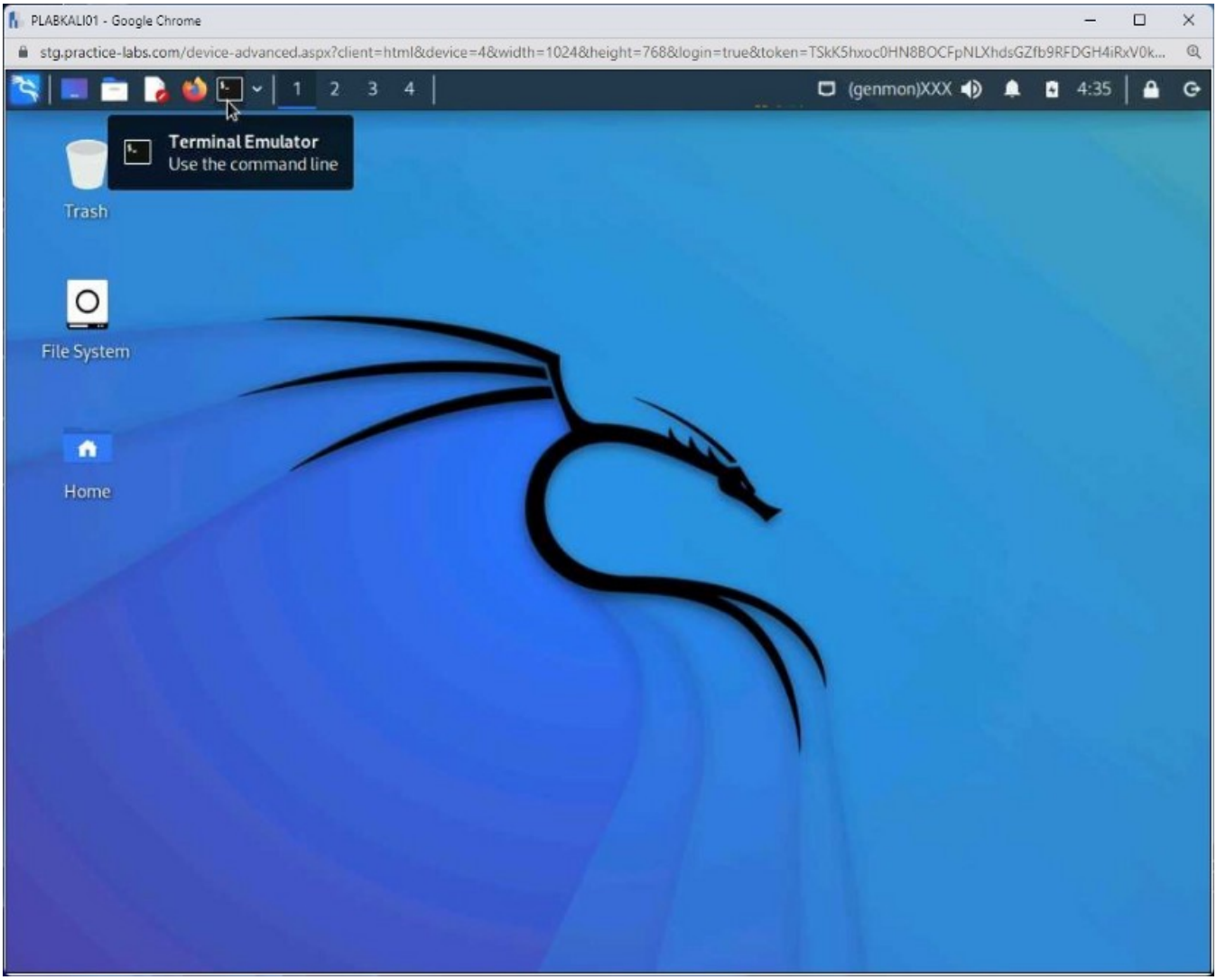
```
root
```

Password:

Password

The desktop of **PLABKALI01** is displayed.

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

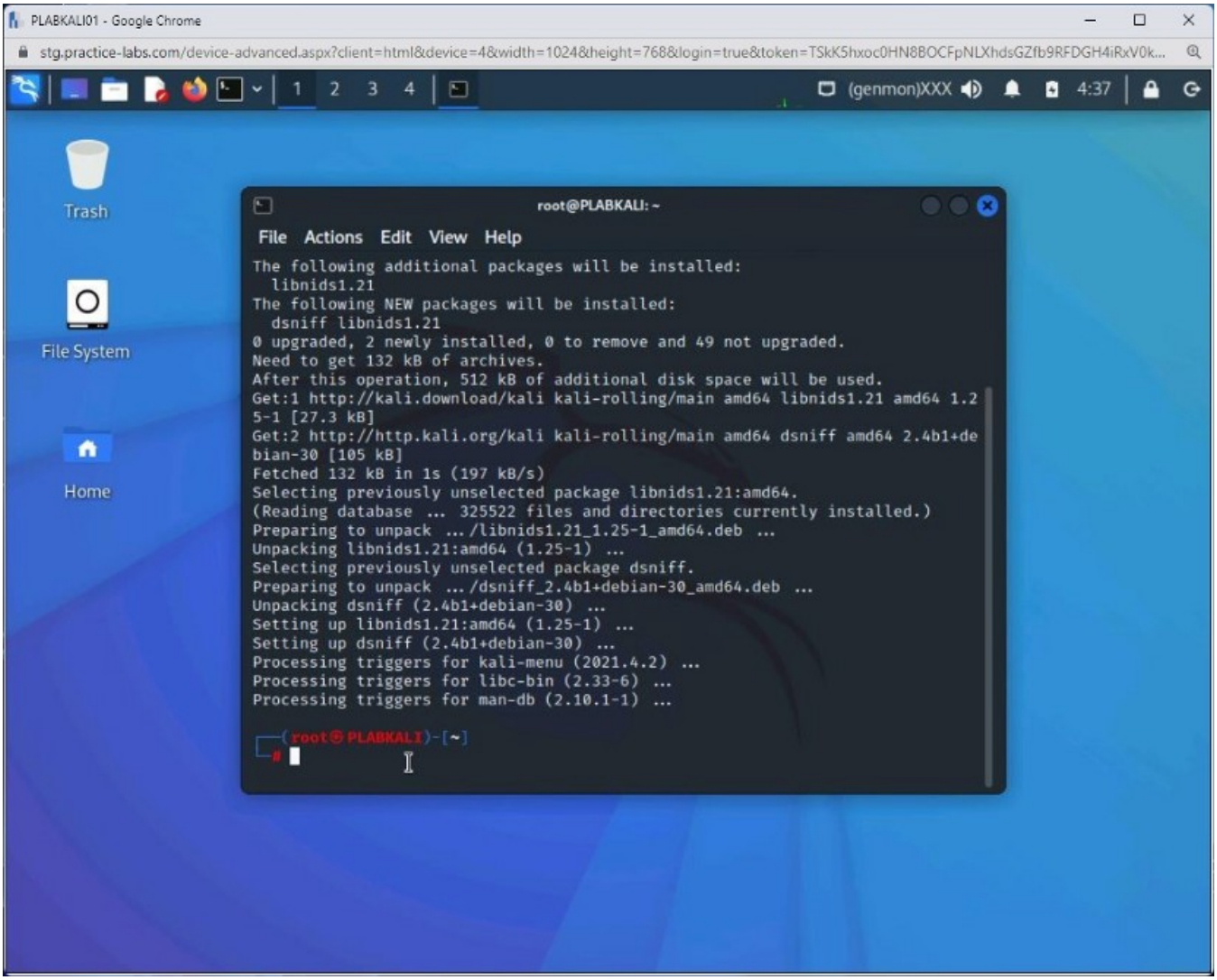


Step 2

In the older versions of Kali, macof was pre-installed. However, you need to install the dsniff package, which contains various tools, including macof. To begin the installation of dsniff, type the following command:

```
apt-get install dsniff -y
```

Press **Enter**.



Step 3

The installation of **dsniff** does not take a long time. After the installation is

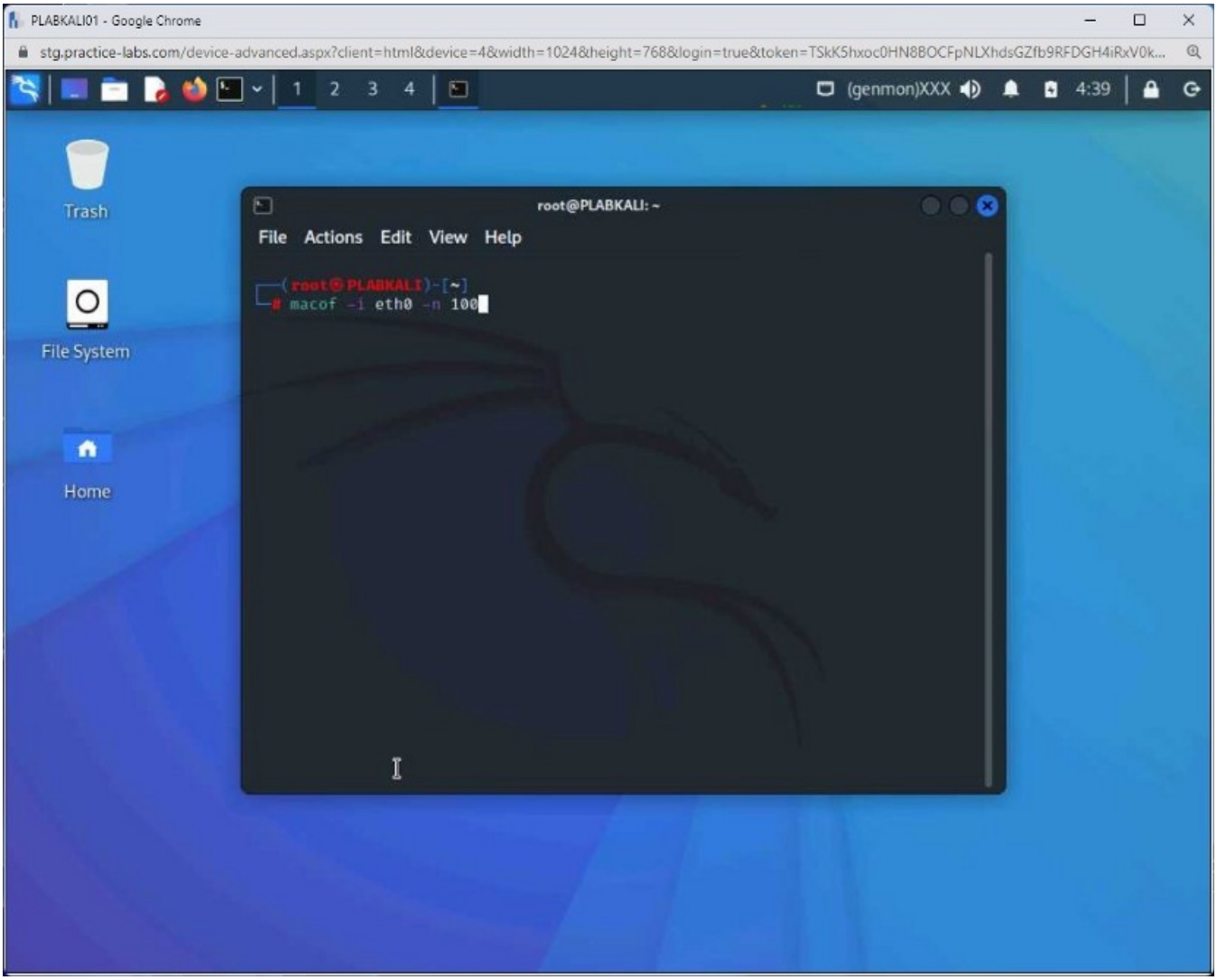
Clear the screen by entering the following command:

```
clear
```

Type the following command to initiate MAC flooding:

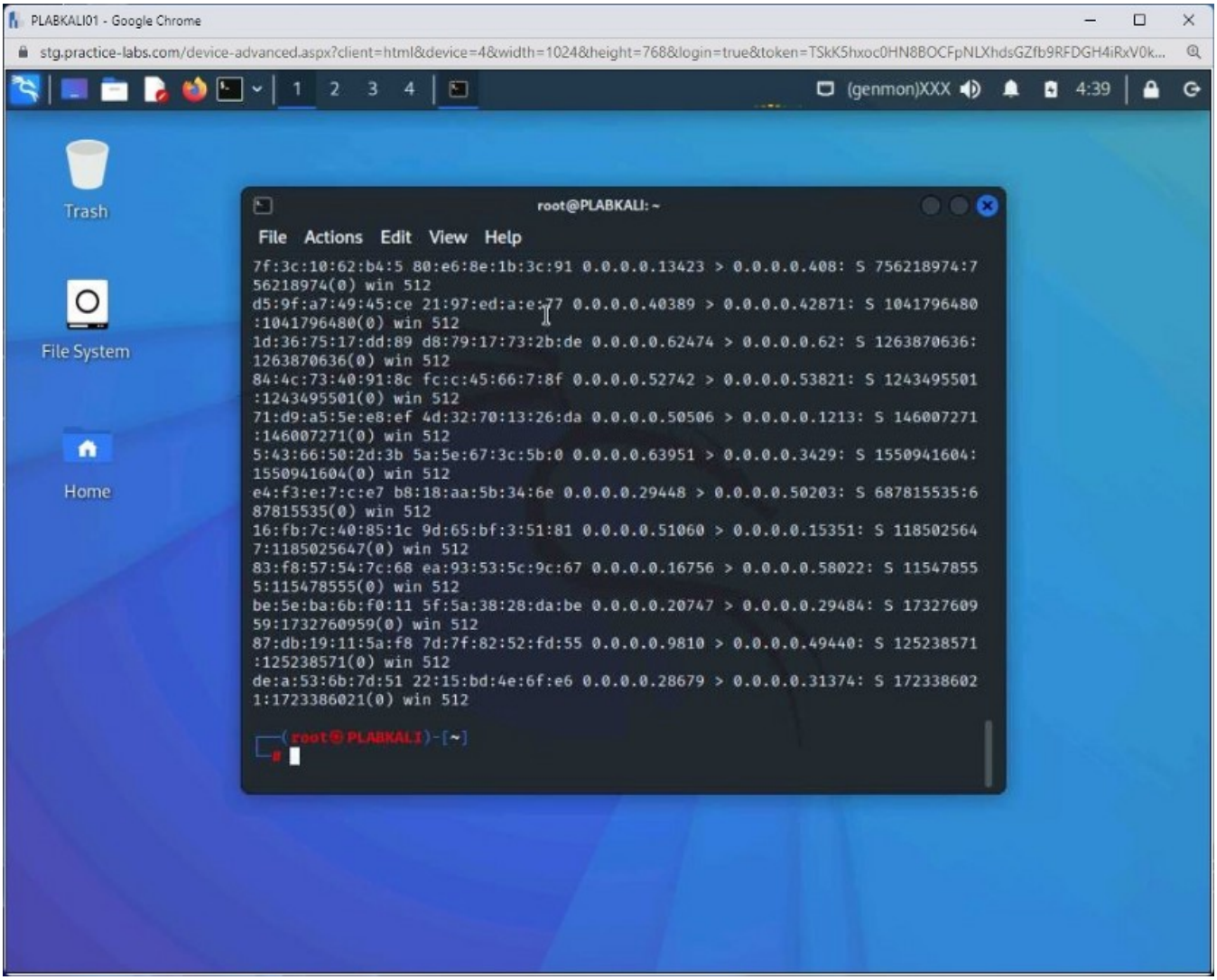
```
macof -i eth0 -n 100
```

In this command, **etho** is the interface for sending out packets, and **-n** is used to send several MAC addresses.



Step 4

The packets are sent out using different MAC addresses.



Close the terminal window.

Task 2 — Perform MAC Flooding using Yersinia

Like the **macof** tool, you can use **Yersinia** to perform MAC flooding.

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

Step 1

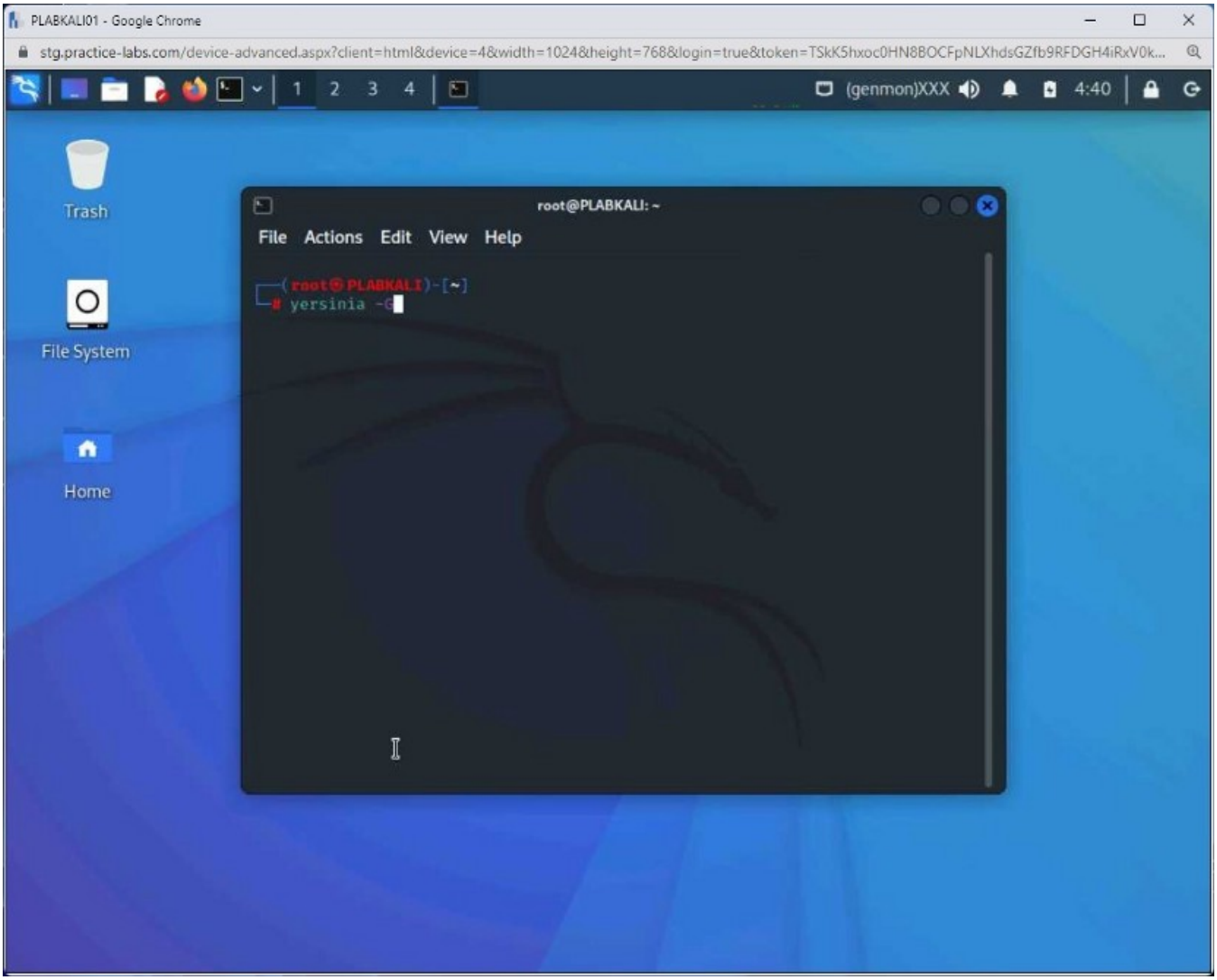
Connect to **PLABKALI01**. Ensure that you are on the command prompt.

Type the following command:

```
yersinia -G
```

Press **Enter**.

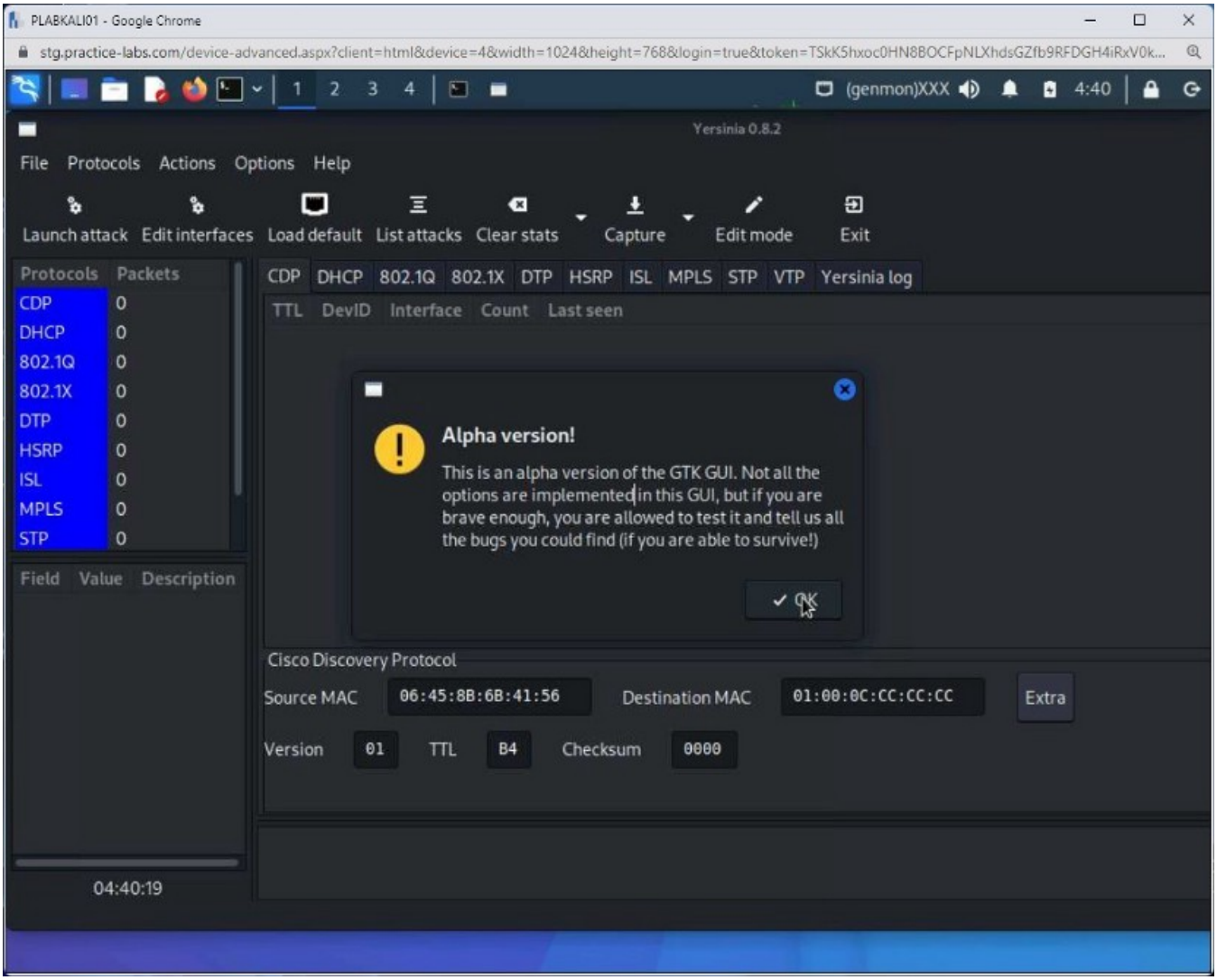
***Note**: The -G parameter is to display the graphical interface.*



Step 2

The **Yersinia** window is displayed. Note that you are prompted to warn that it is an alpha version.

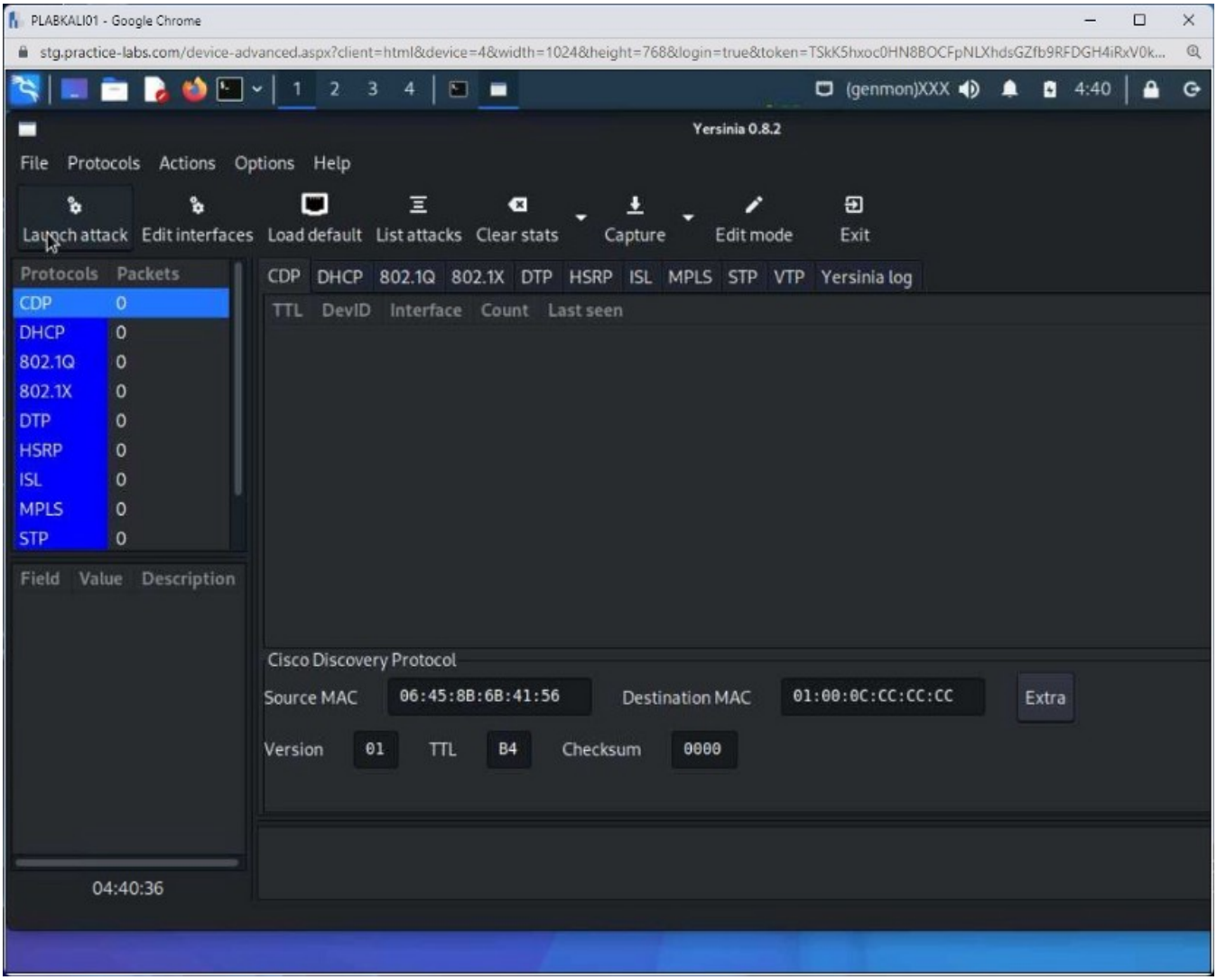
Click **OK**.



Step 3

The **Yersinia** window is now fully visible. Ensure that you are on the **CDP** tab in the right pane.

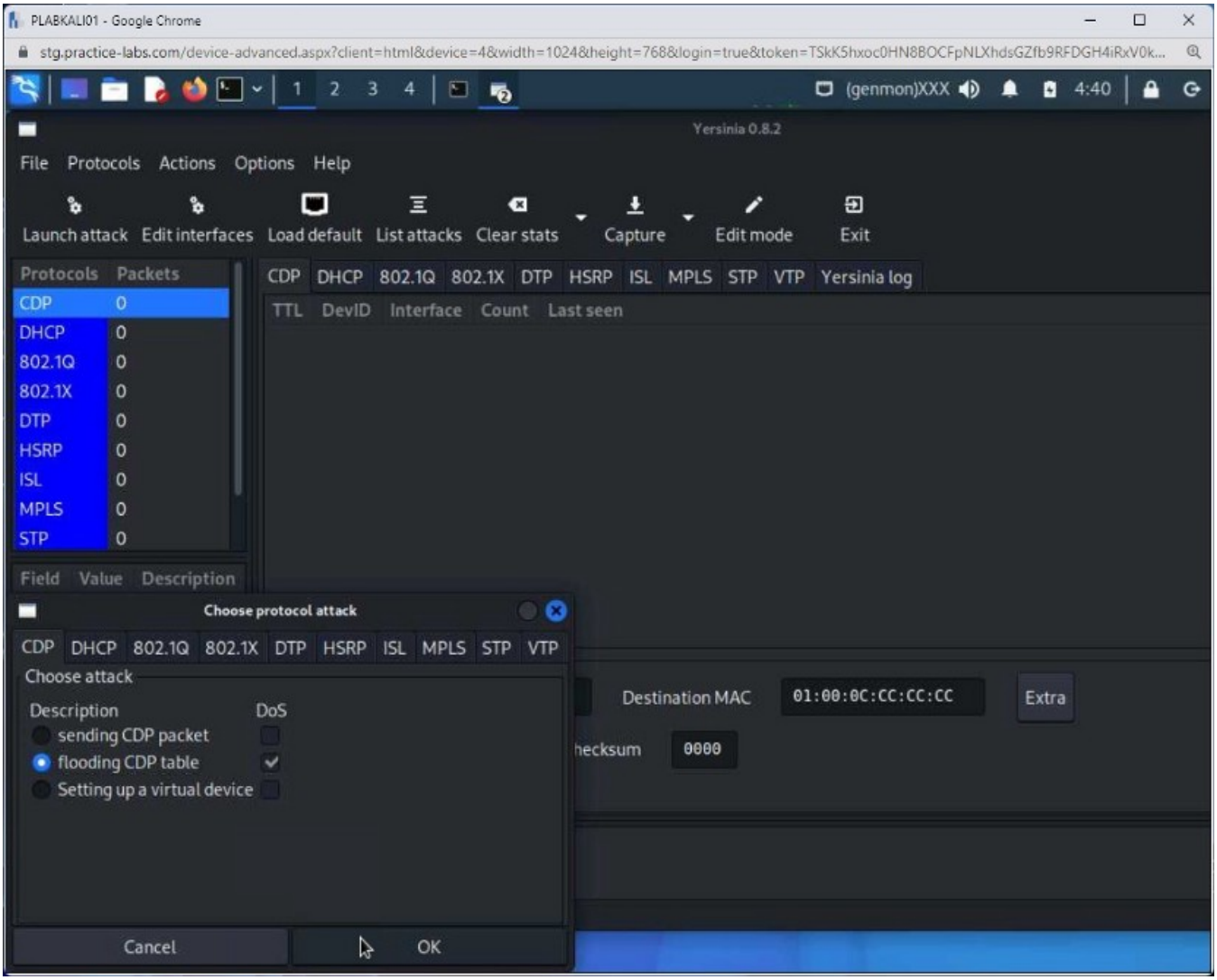
Click **Launch attack**.



Step 4

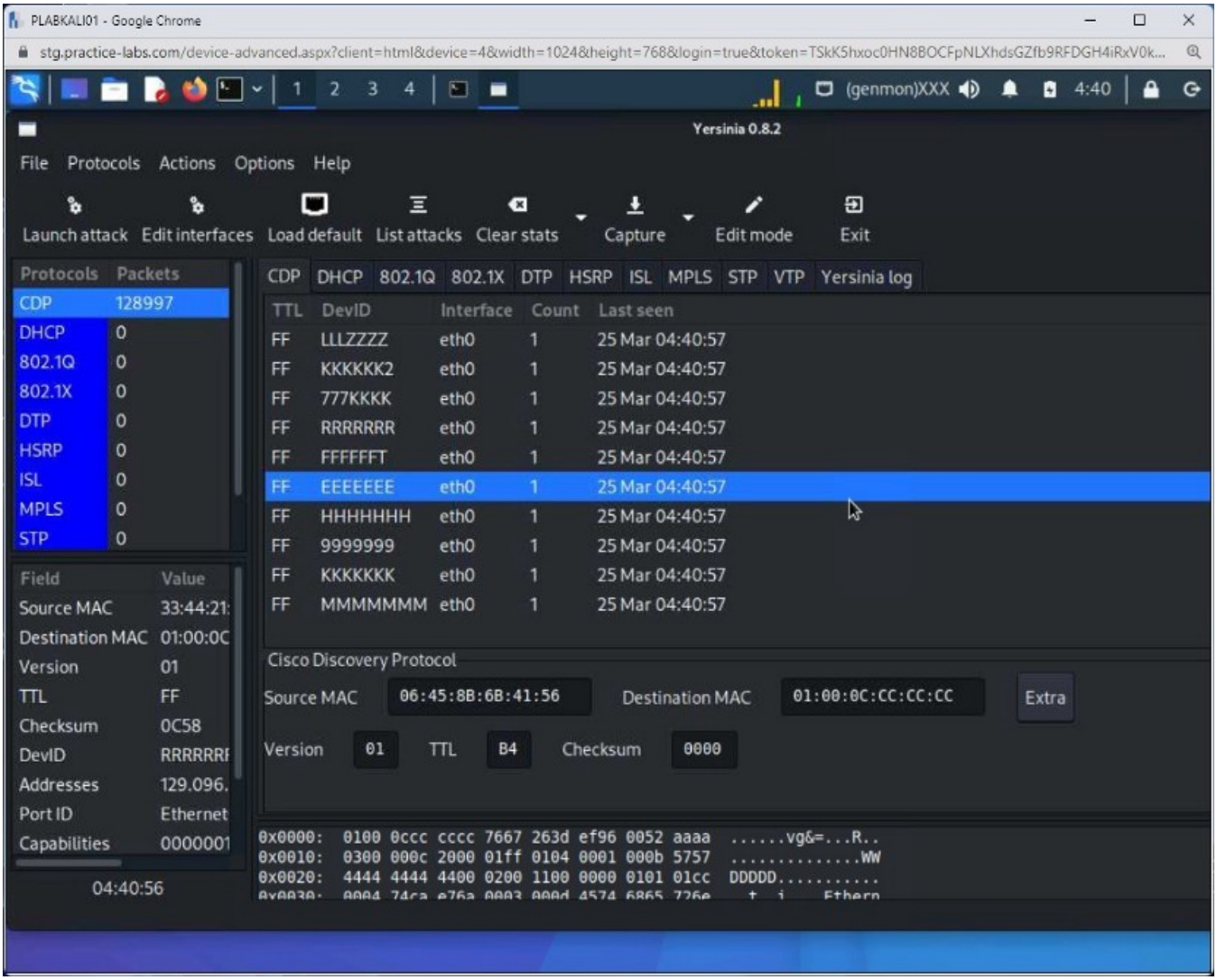
The **Choose attack** dialog box is displayed. The sending CDP packet option is selected by default.

Select **flooding CDP table** and click **OK**.



Step 5

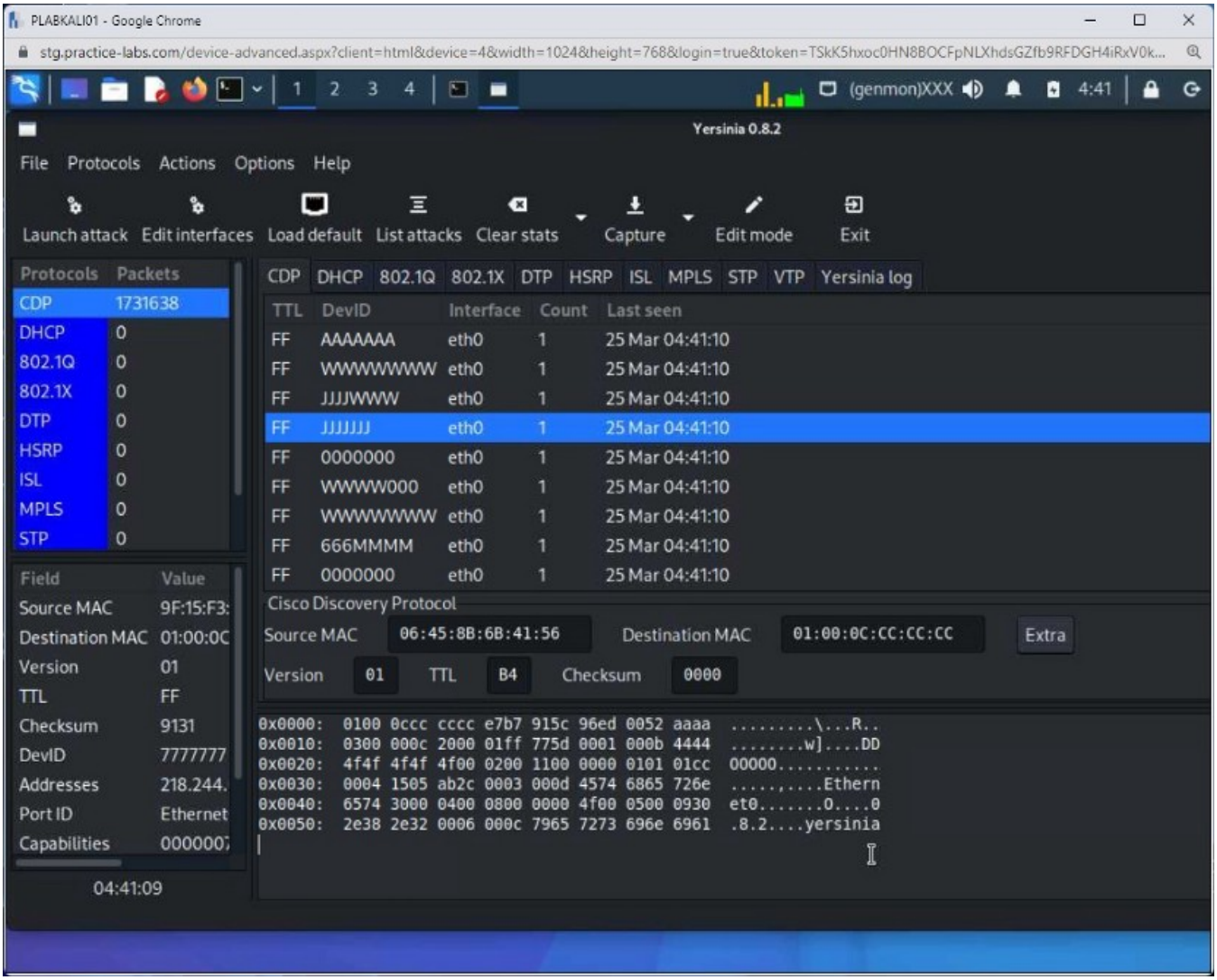
Note that flooding is initiated instantly.



Step 6

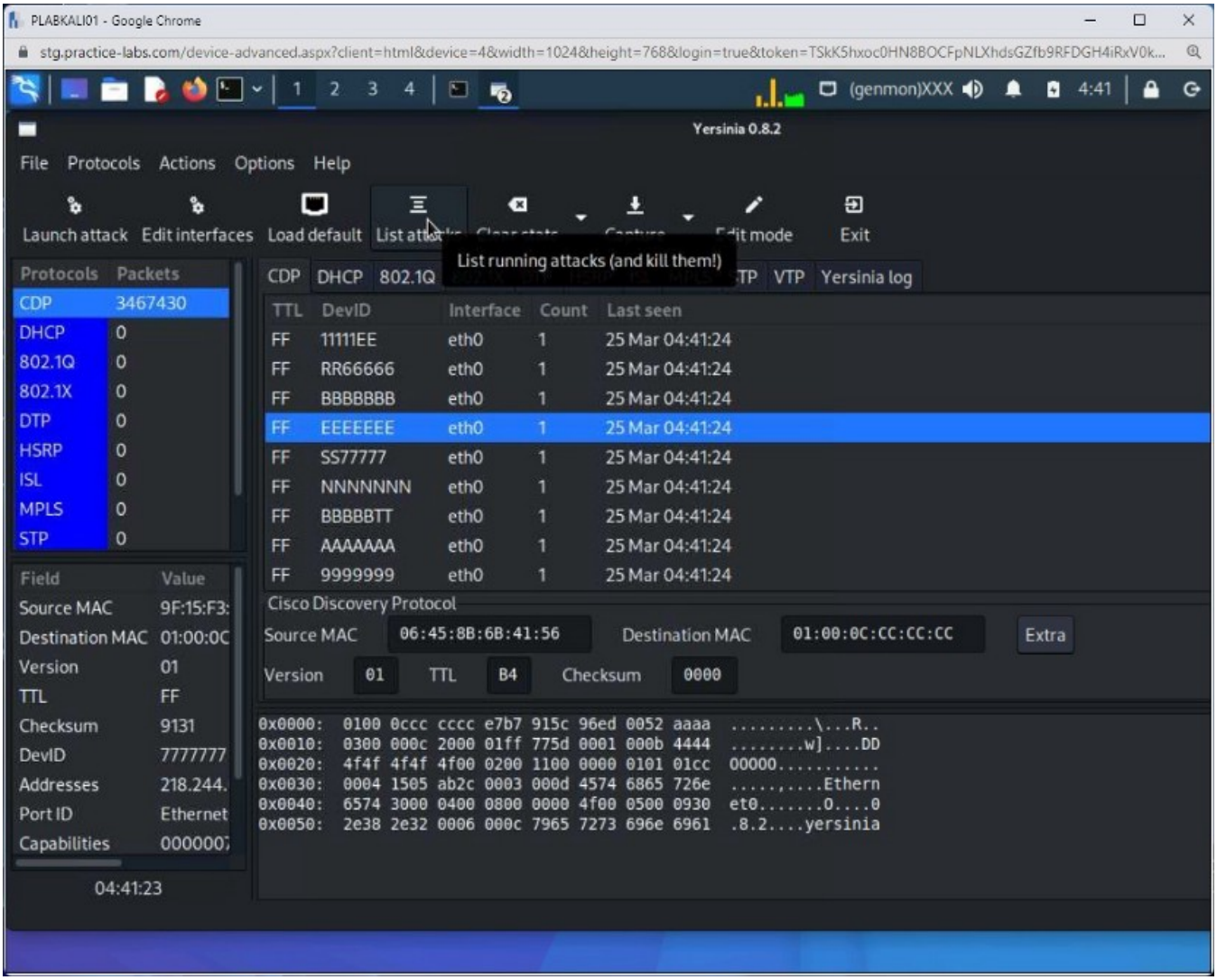
Select a value in the upper right pane. Note that the bottom left pane displays the source MAC address. Select a number of them and note that each has a different MAC address.

***Note**: During this attack, the device may become unresponsive.*



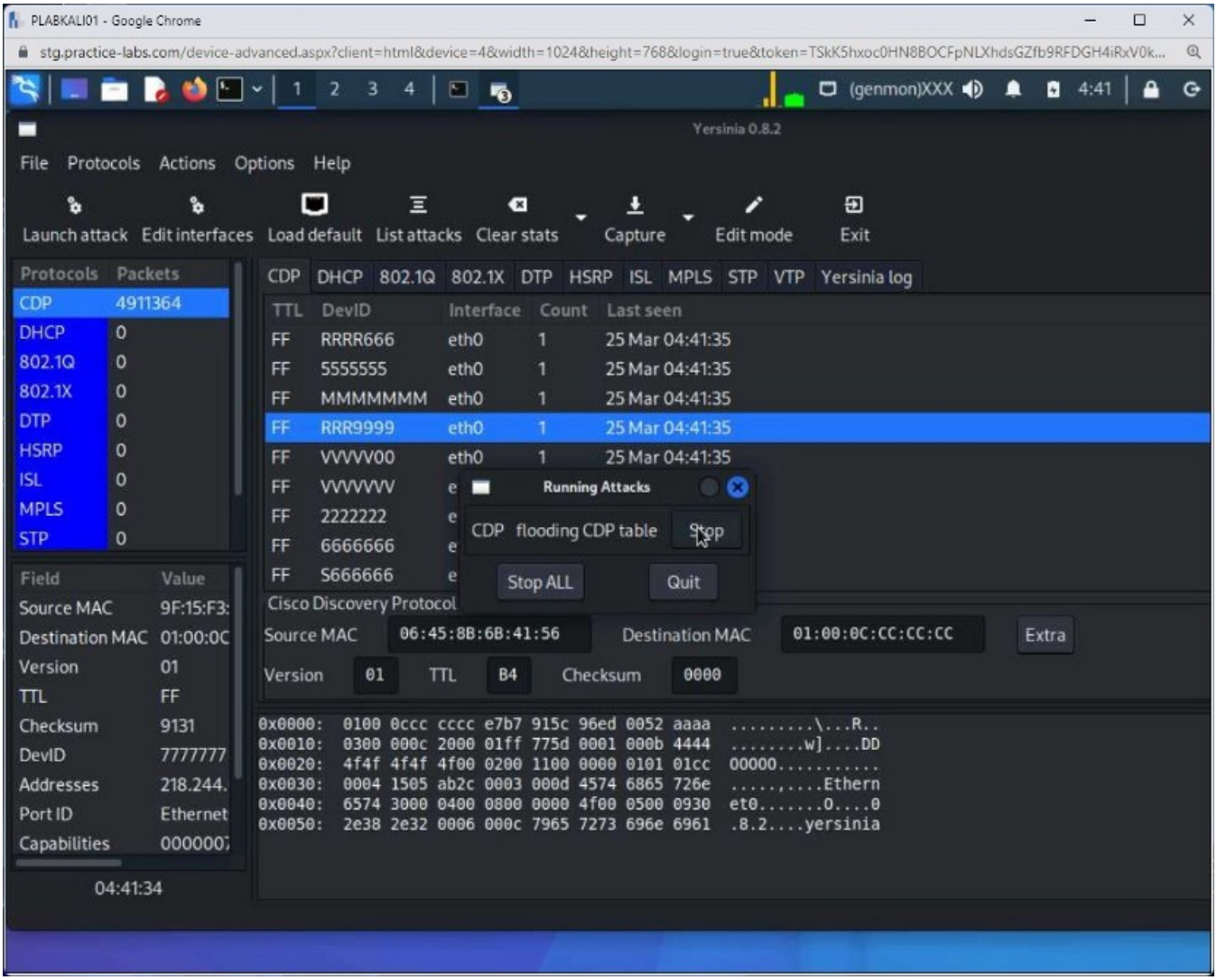
Step 7

Click **List attacks**.



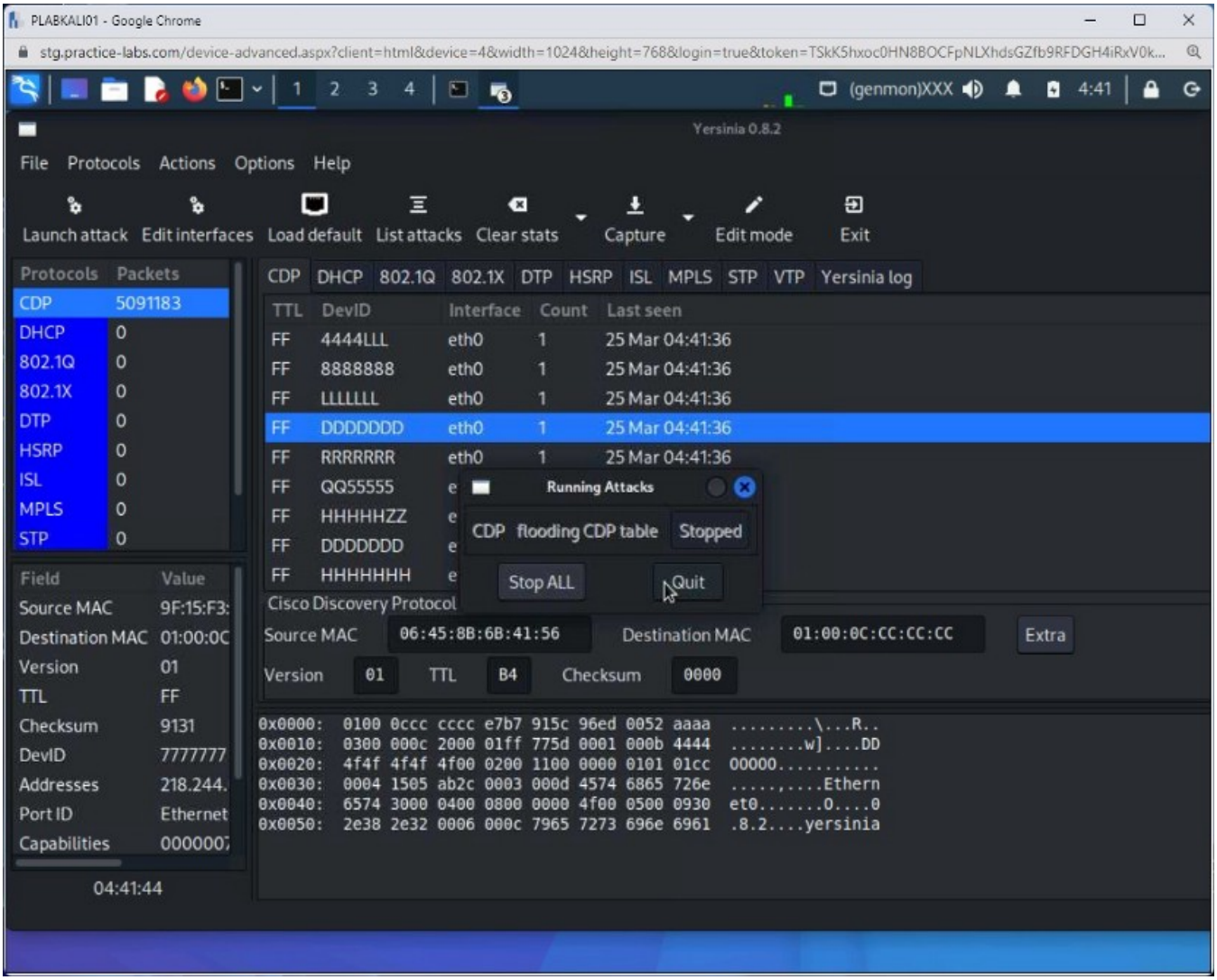
Step 8

The **Running Attacks** dialog box is displayed. Click **Stop**.



Step 9

Note that the attack is now stopped. Click **Quit** on the **Running Attacks** dialog box.



Close the Yersinia 0.8.2 window.

Task 3 — Use macof to Flood Switches with MAC Addresses

In a switched network, it can be difficult to sniff traffic. However, with a tool like macof, you can flood a network with spoofed MAC addresses, which eventually causes a switch to fail and work as a hub. Once the switch acts like a hub that starts broadcasting packets to all connected systems. It makes it easier for the attacker to sniff traffic.

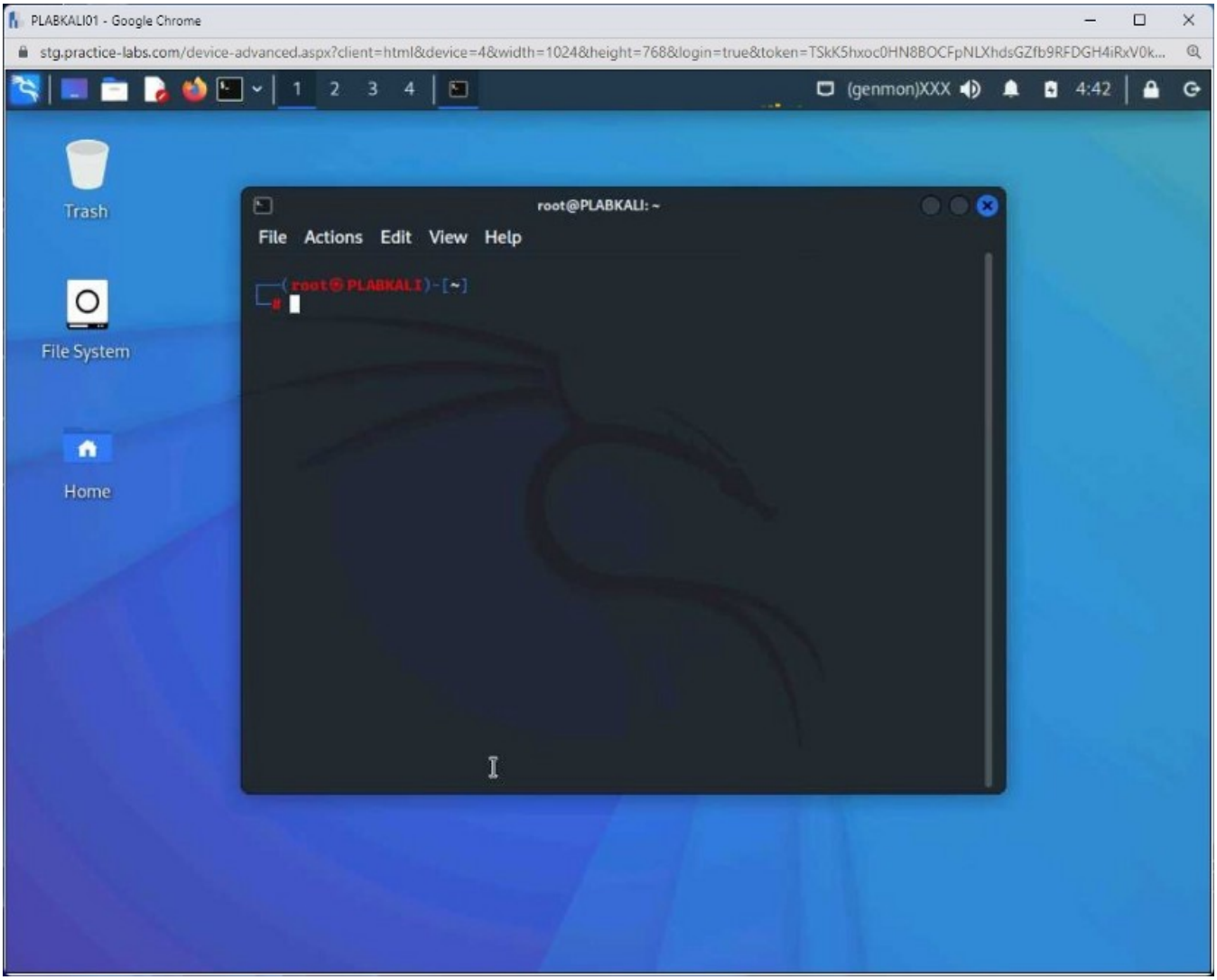
In this task, you will learn to use the macof tool.

Step 1

Connect to **PLABKALI01**. The terminal window should be displayed.

Clear the screen by entering the following command:

```
clear
```

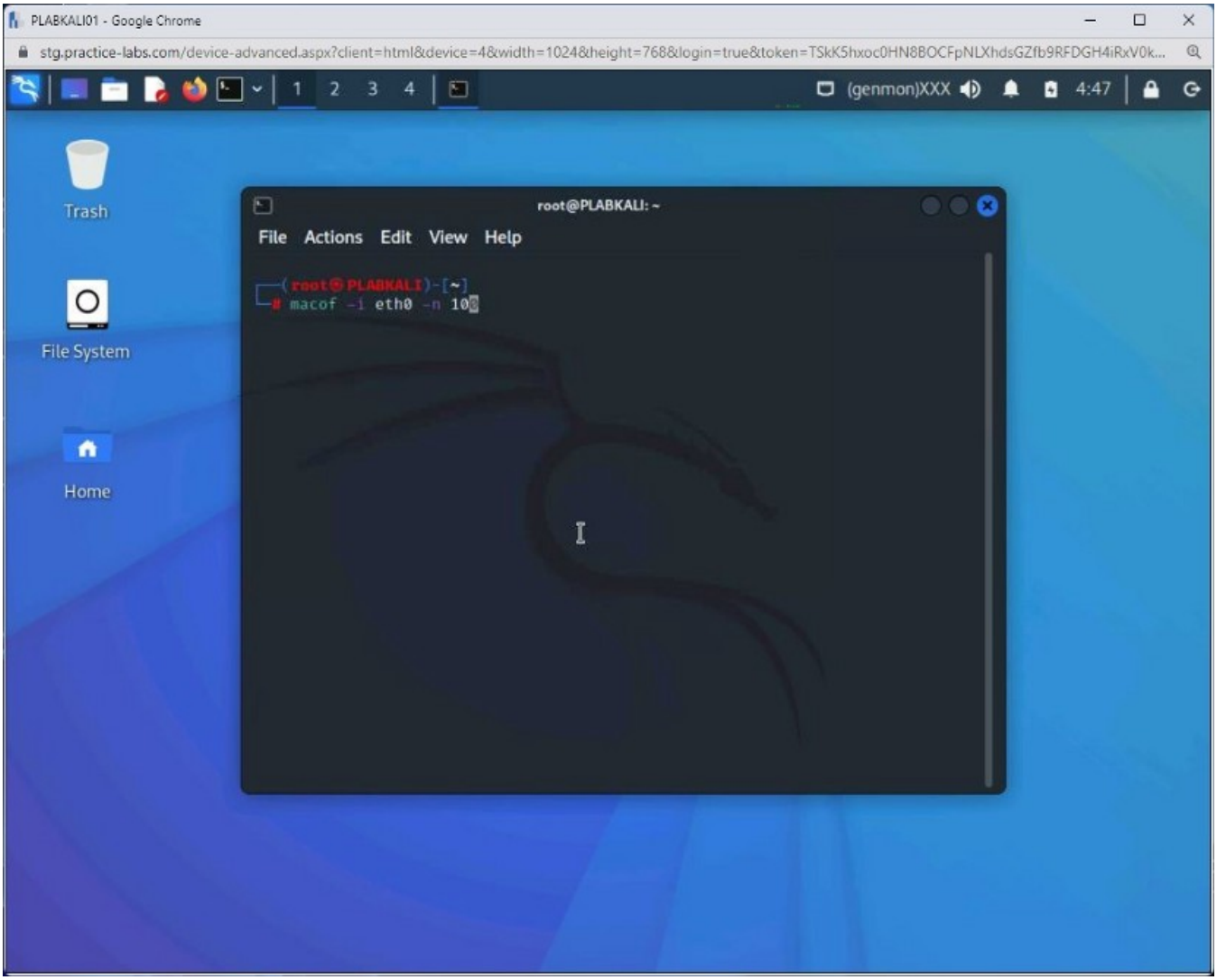


Step 2

You need to now flood a switch with the spoofed MAC addresses. To do this, type the following command:

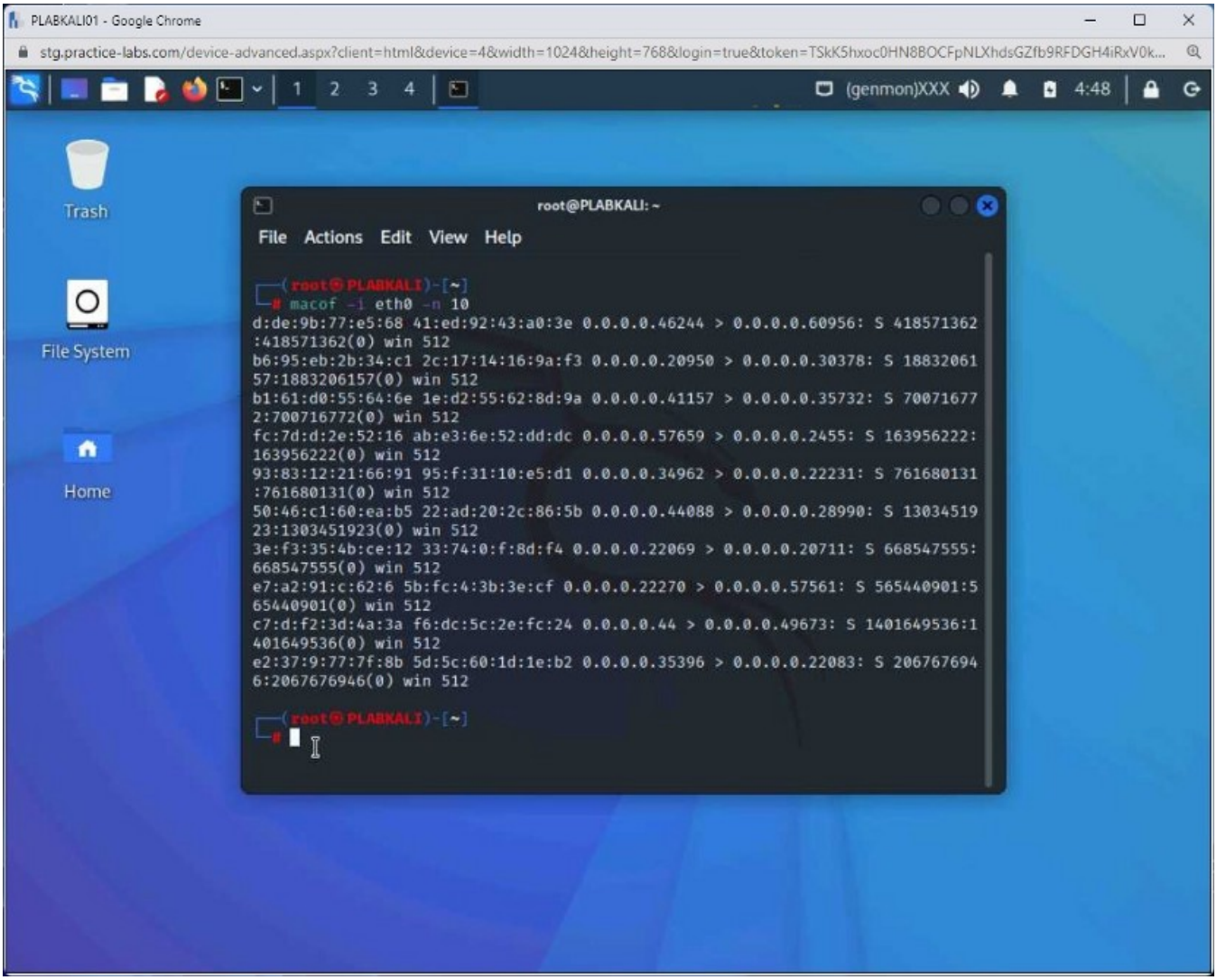
```
macof -i eth0 -n 10
```

Press **Enter**. The **-i** parameter is used to define the network interface used for sending out packets.



Step 3

The MAC flooding process starts. It will send **5000** packets per second and loop the process **10** times.



Step 4

You can also target a specific switch. Let's assume that the switch has the IP address of **192.168.0.1**.

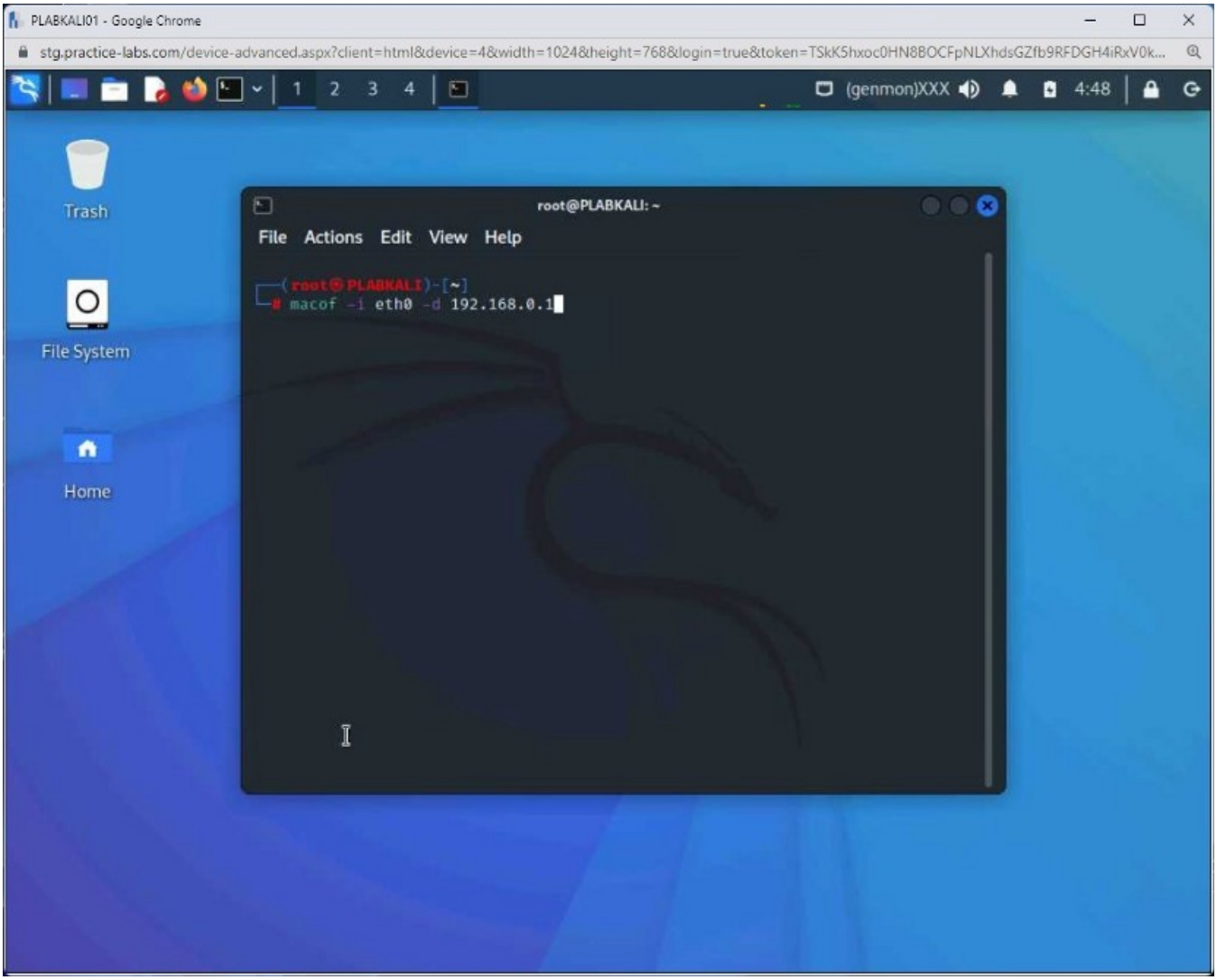
Clear the screen by entering the following command:

```
clear
```

You can target it and send the spoofed MAC addresses directly to it with the following command:

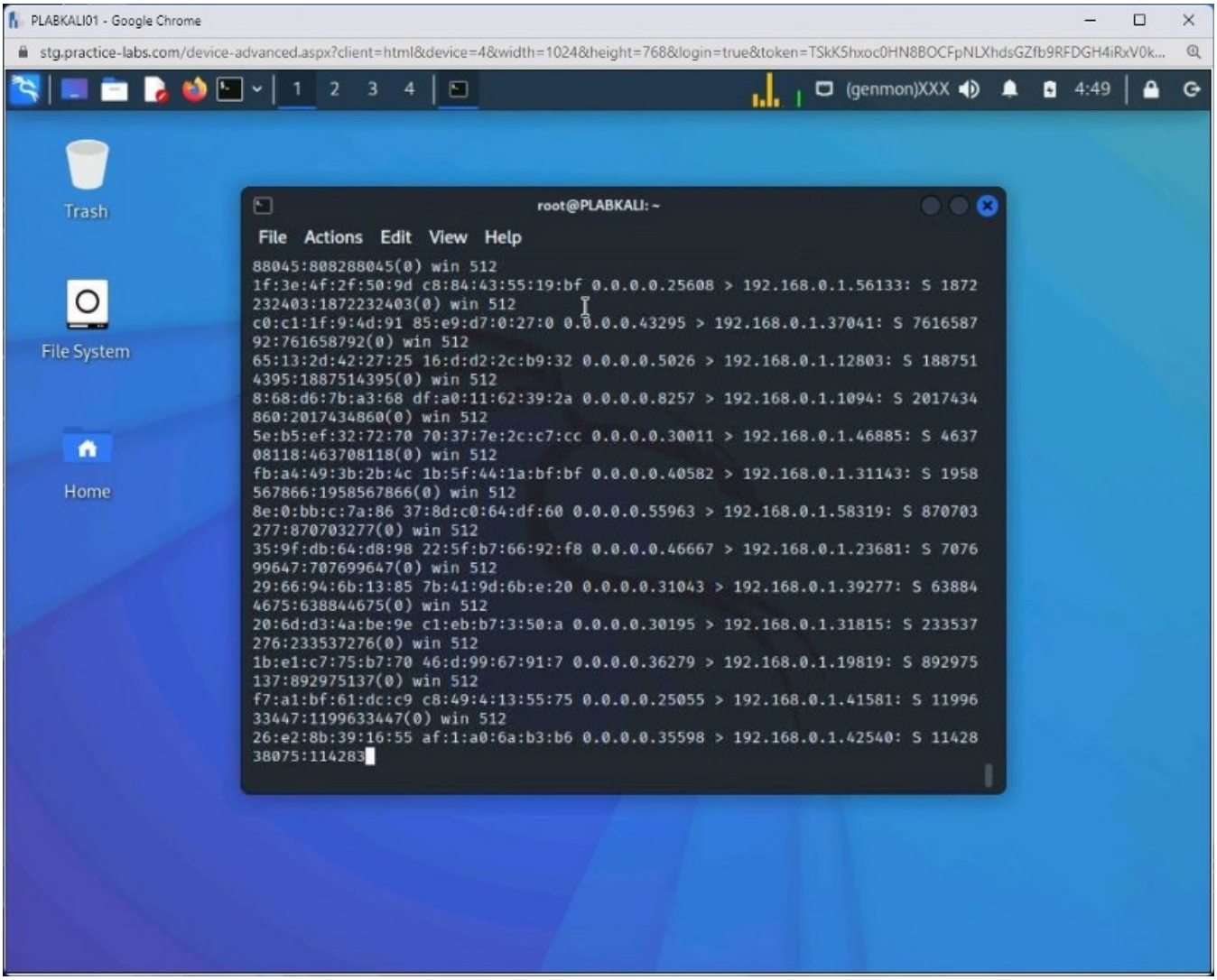
```
macof -i eth0 -d 192.168.0.1
```

Press **Enter**. The **-d** parameter is used for defining the device.



Step 5

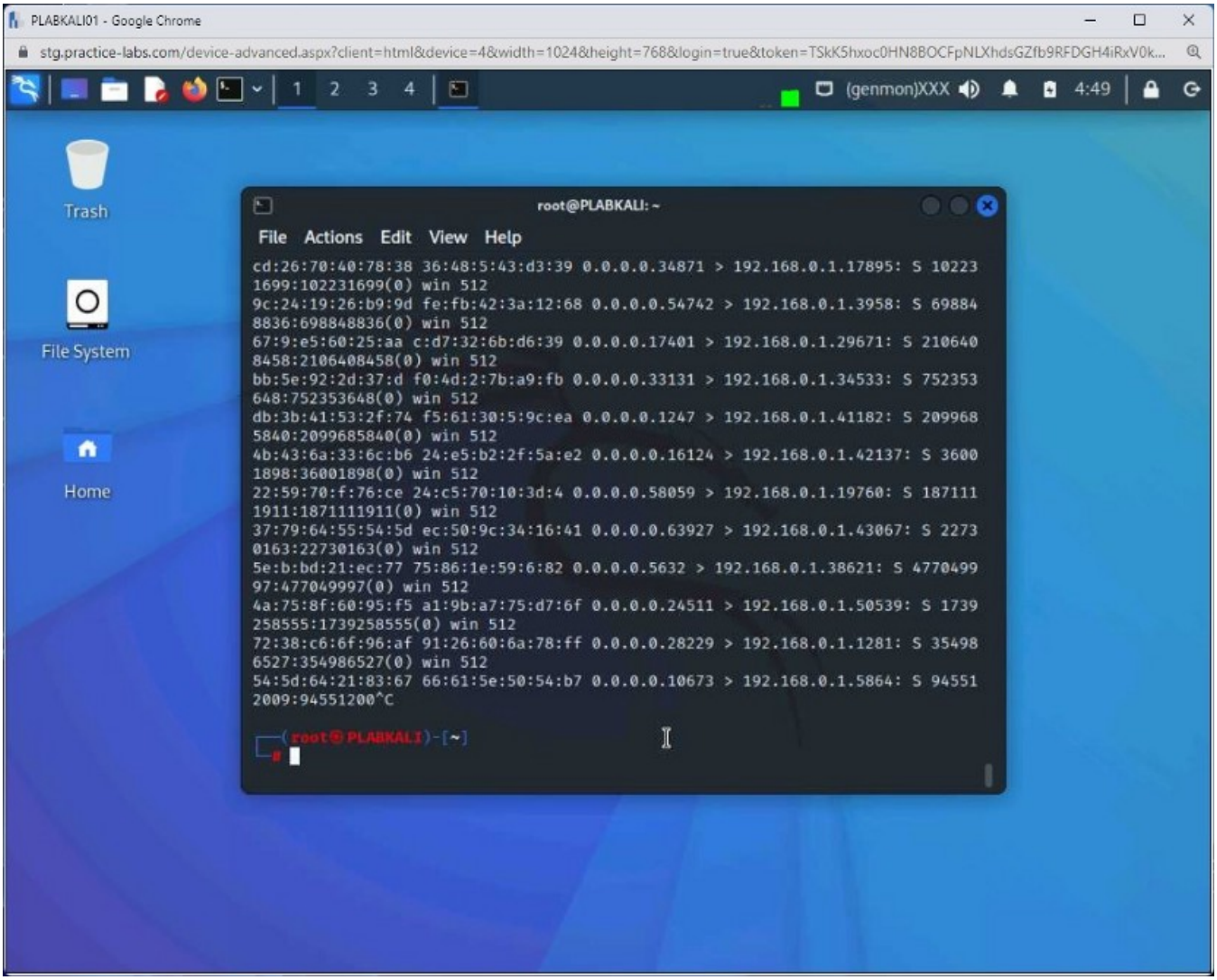
The MAC flooding process starts. However, this process may take a little longer than the previous flooding process.



Step 6

You can terminate the process by pressing **Ctrl** + **C**.

An error might be generated, which can be ignored. A switch would have been overwhelmed with so many requests.



Exercise 4 — Sniffing Technique: DHCP Attacks

A DHCP server is configured to lease IP addresses to clients on a network. An attacker can target DHCP with the DHCP starvation attack. Using this attack, an attacker sends many DHCP requests to a DHCP server, which eventually forces the server to lease all IP addresses.

In this scenario, you will learn to launch the DHCP attacks.

Learning Outcomes

After completing this exercise, you will be able to:

- Launch the DHCP Starvation Attack

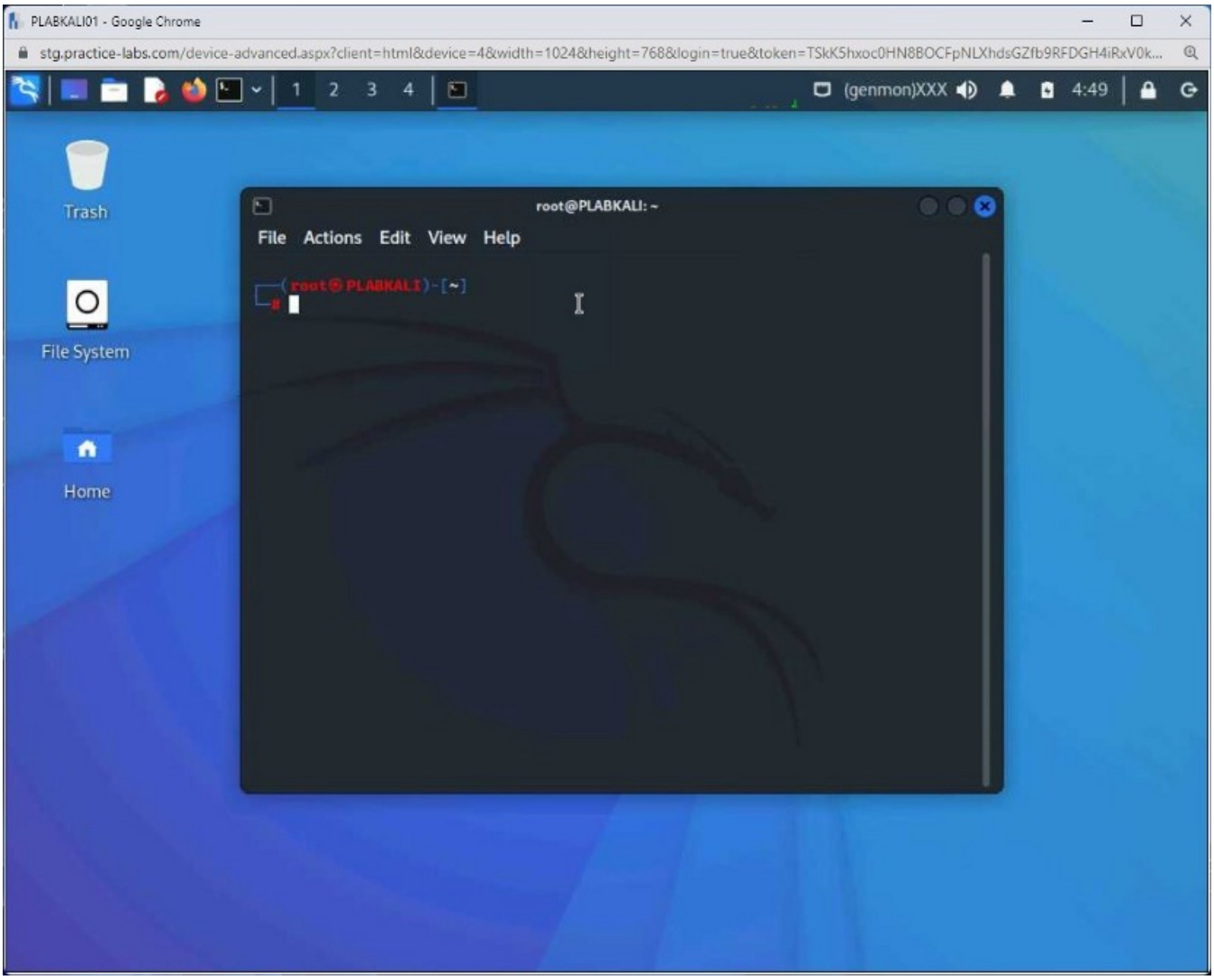
Task 1 — Launch the DHCP Starvation Attack

A DHCP has a limited set of IP addresses (254) that it can lease to legitimate clients. During a Starvation attack, the server will run out of available IP addresses to lease.

In this task, you will learn to launch the DHCP starvation attack using Yersinia.

Step 1

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

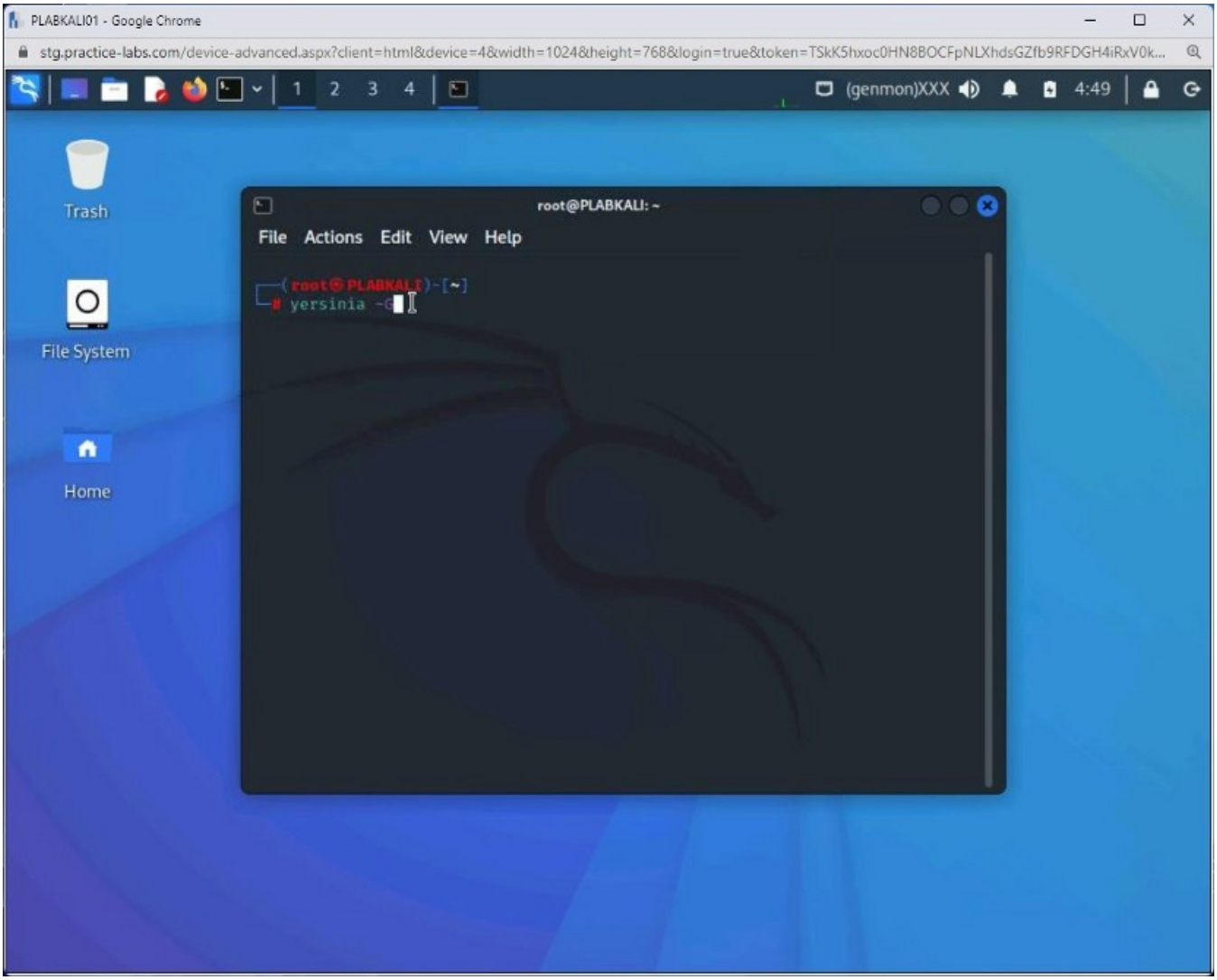


Step 2

You need to launch the graphical GTK version of **Yersinia**. To do this, type the following command:

```
yersinia -G
```

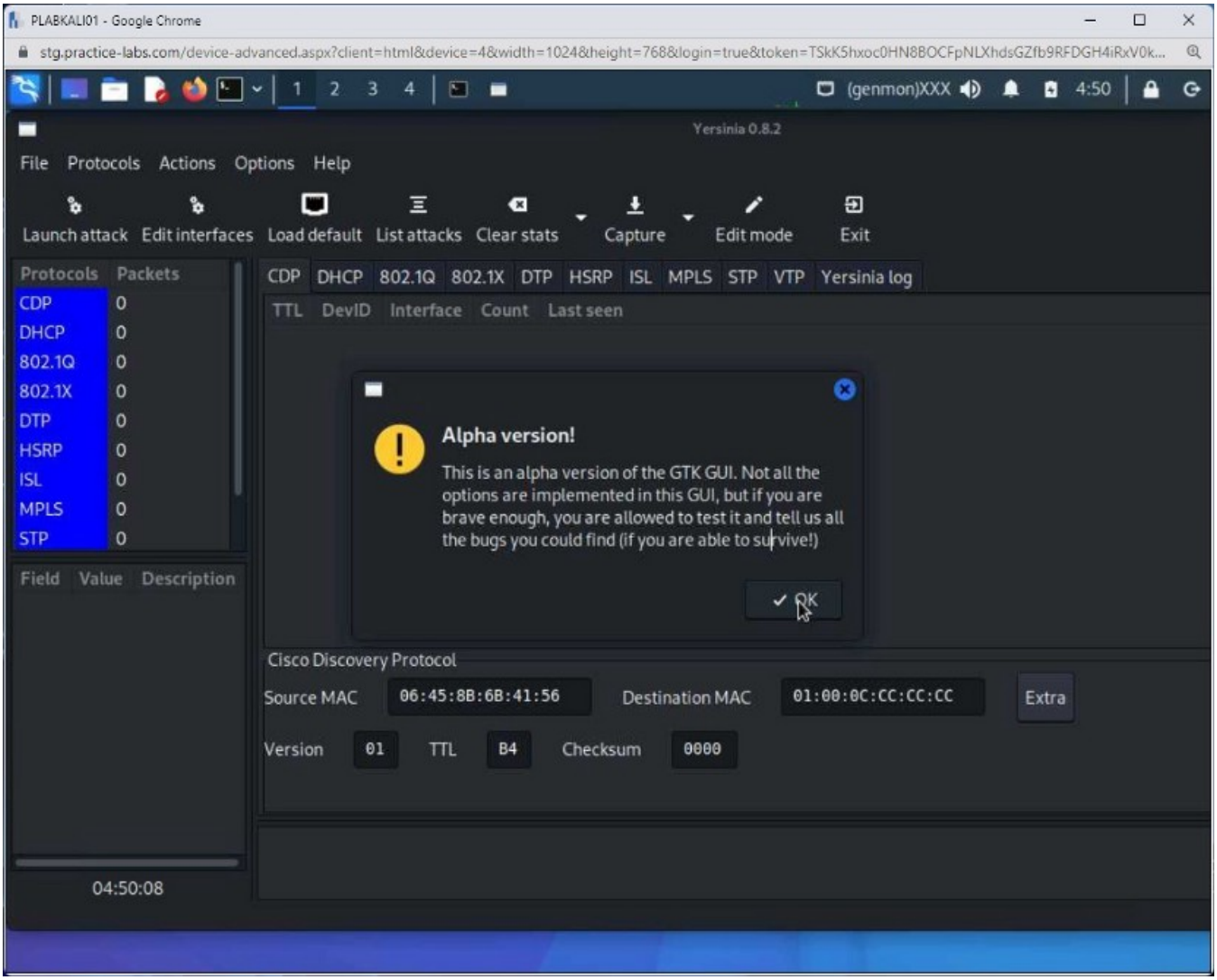
Press **Enter**.



Step 3

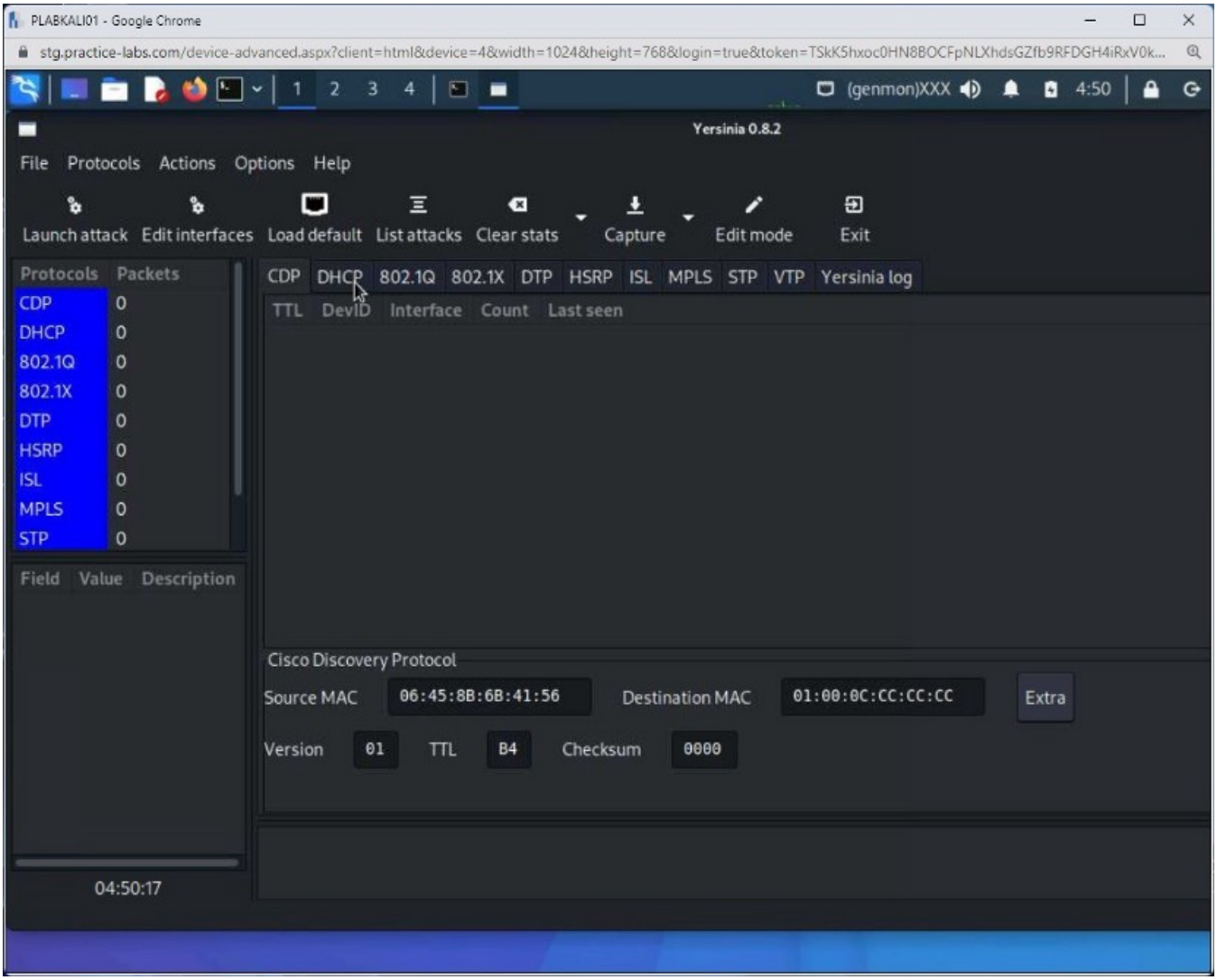
The graphical version of **Yersinia** starts.

Click **OK** on the **Alpha version!** dialog box.



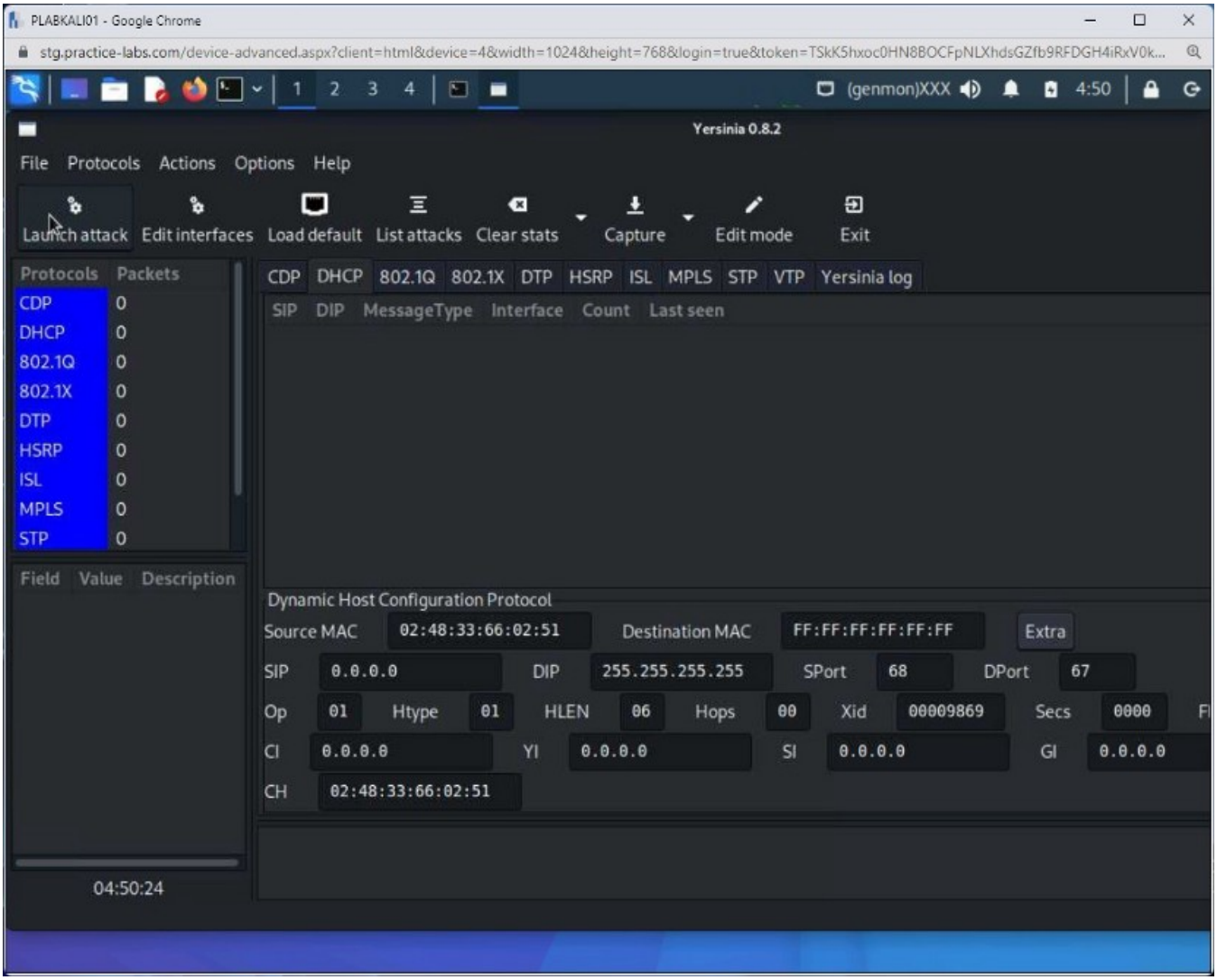
Step 4

Click the **DHCP** tab in the right-hand pane.



Step 5

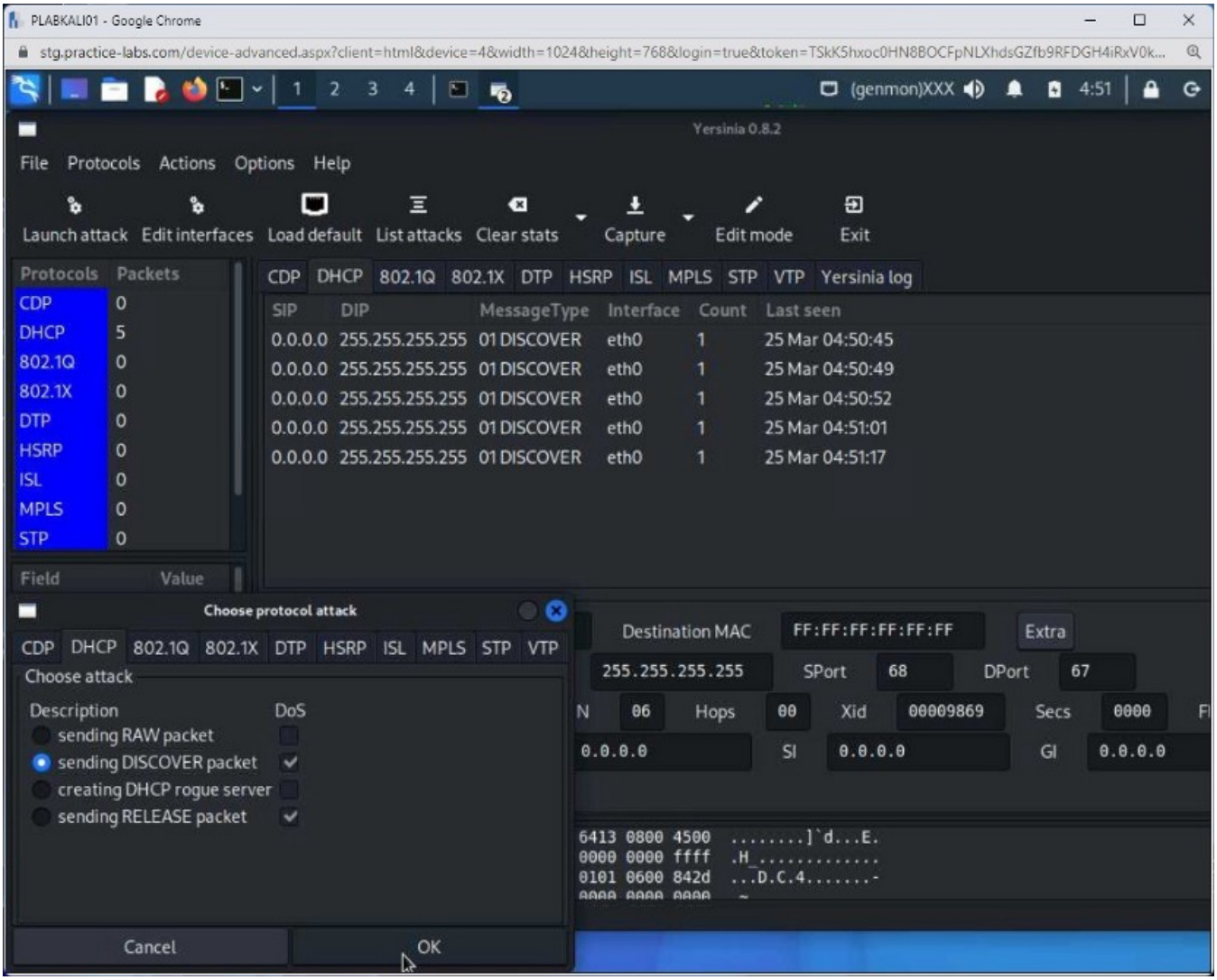
Click **Launch attack**.



Step 6

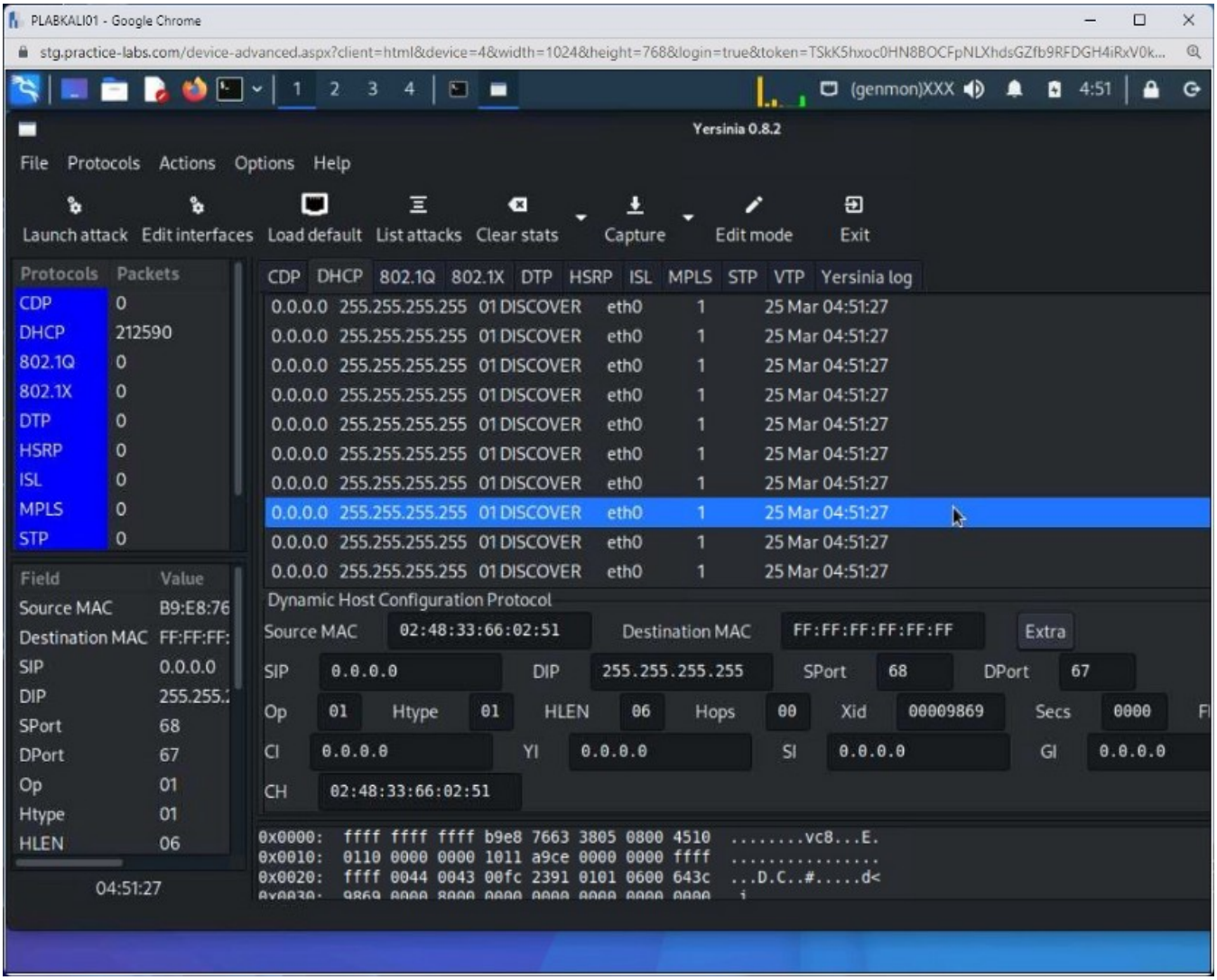
The **Choose protocol attack** dialog box is displayed.

Select **sending DISCOVER packet** and click **OK**.



Step 7

The starvation attack starts.



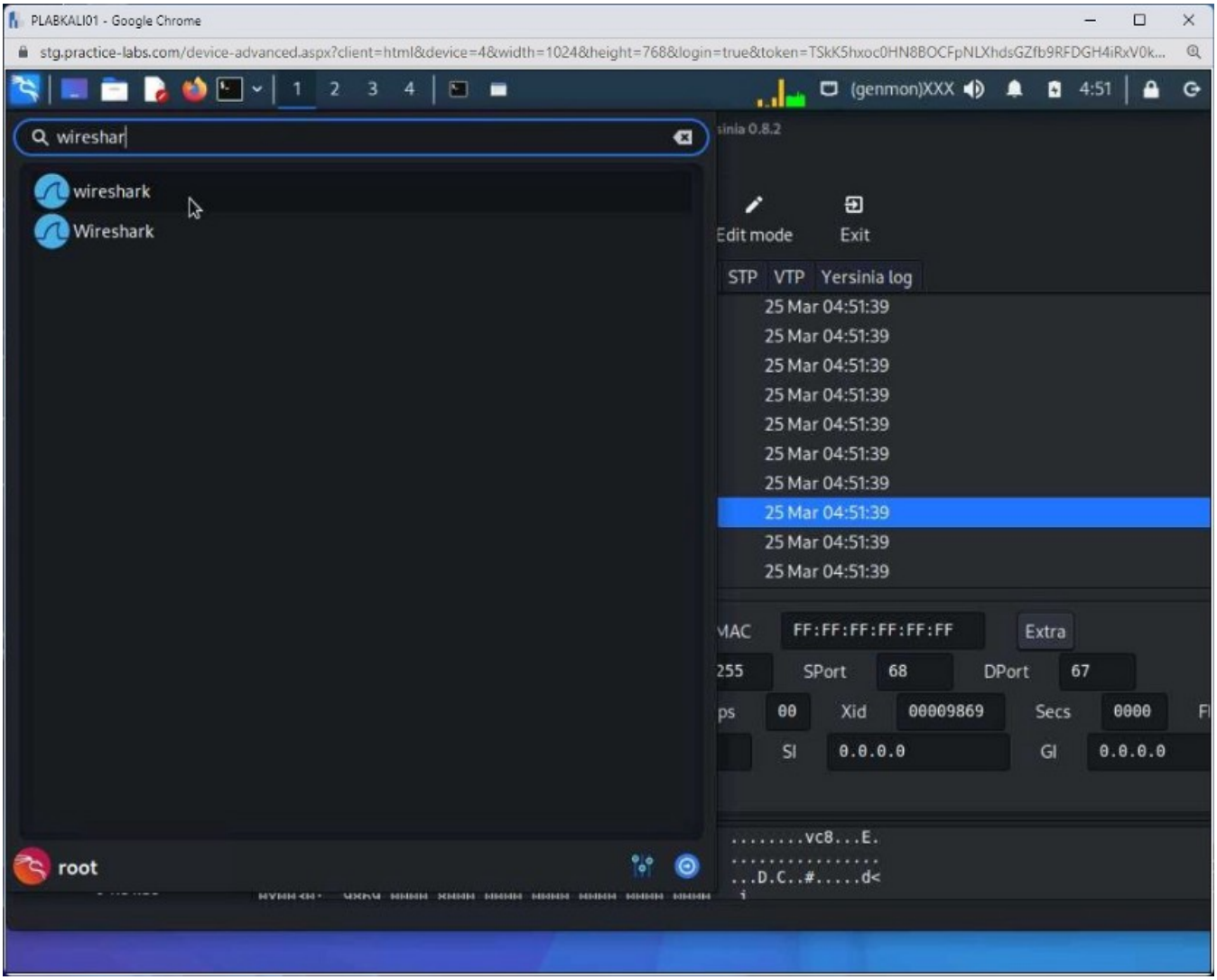
Step 8

Let's now start **Wireshark**.

To do this, open the **Applications** menu, and in the search field type the following:

```
Wireshark
```

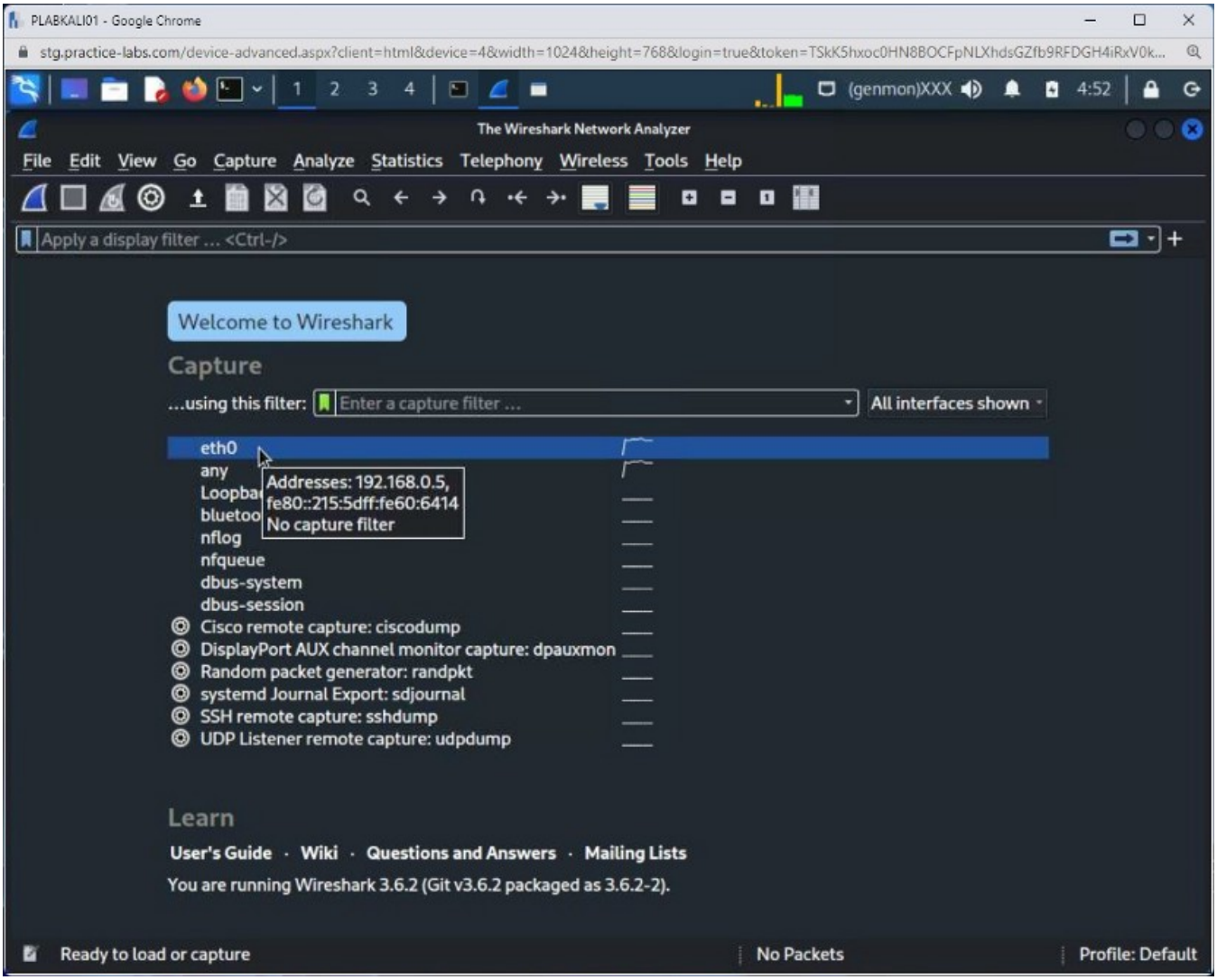
Click the top listing for **Wireshark**.



Step 9

The **Wireshark Network Analyzer** window is displayed.

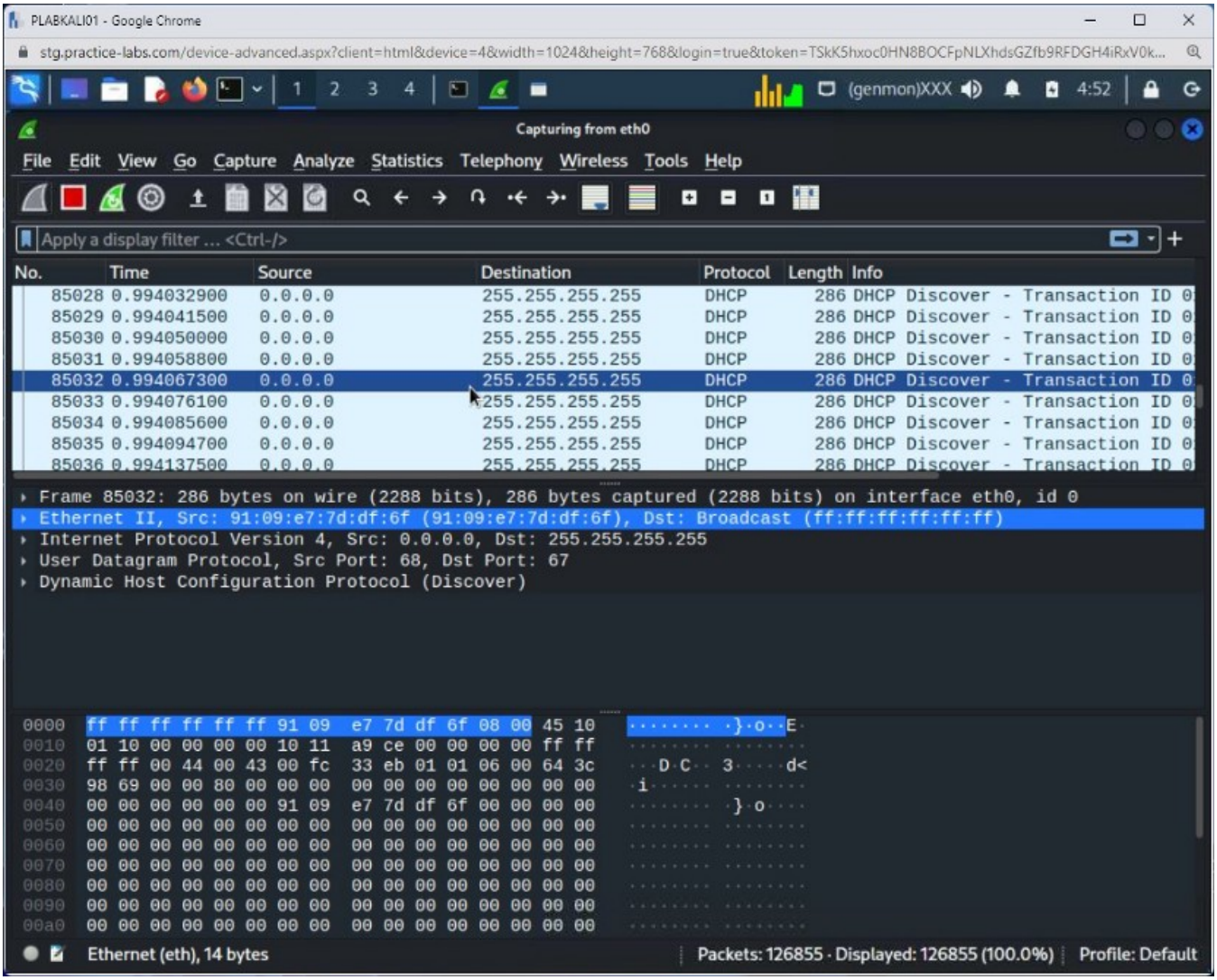
Double-click **etho**.



Step 10

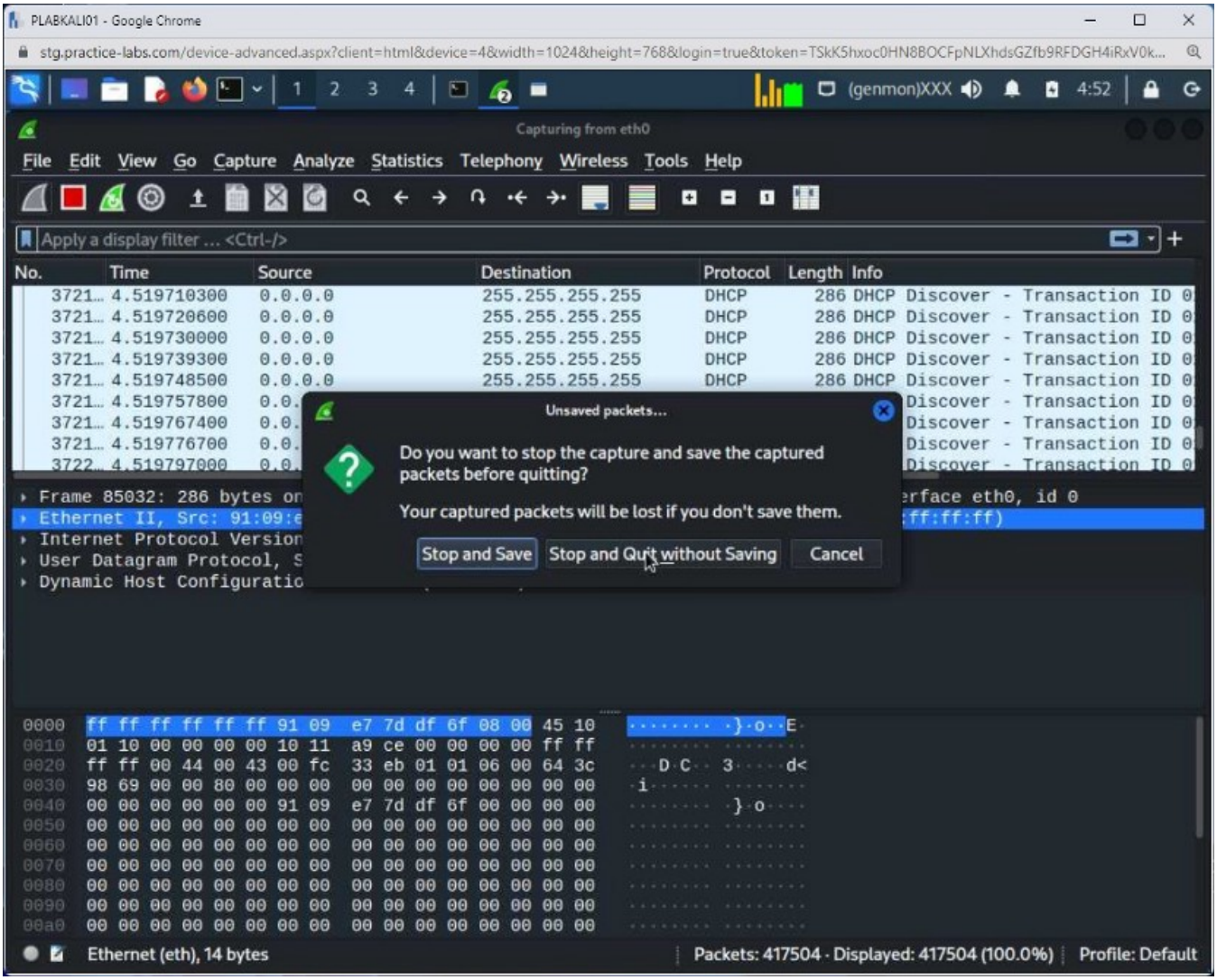
Notice that there are **DISCOVER** packets is being sent over the network.

Close the **Capturing from etho** window.



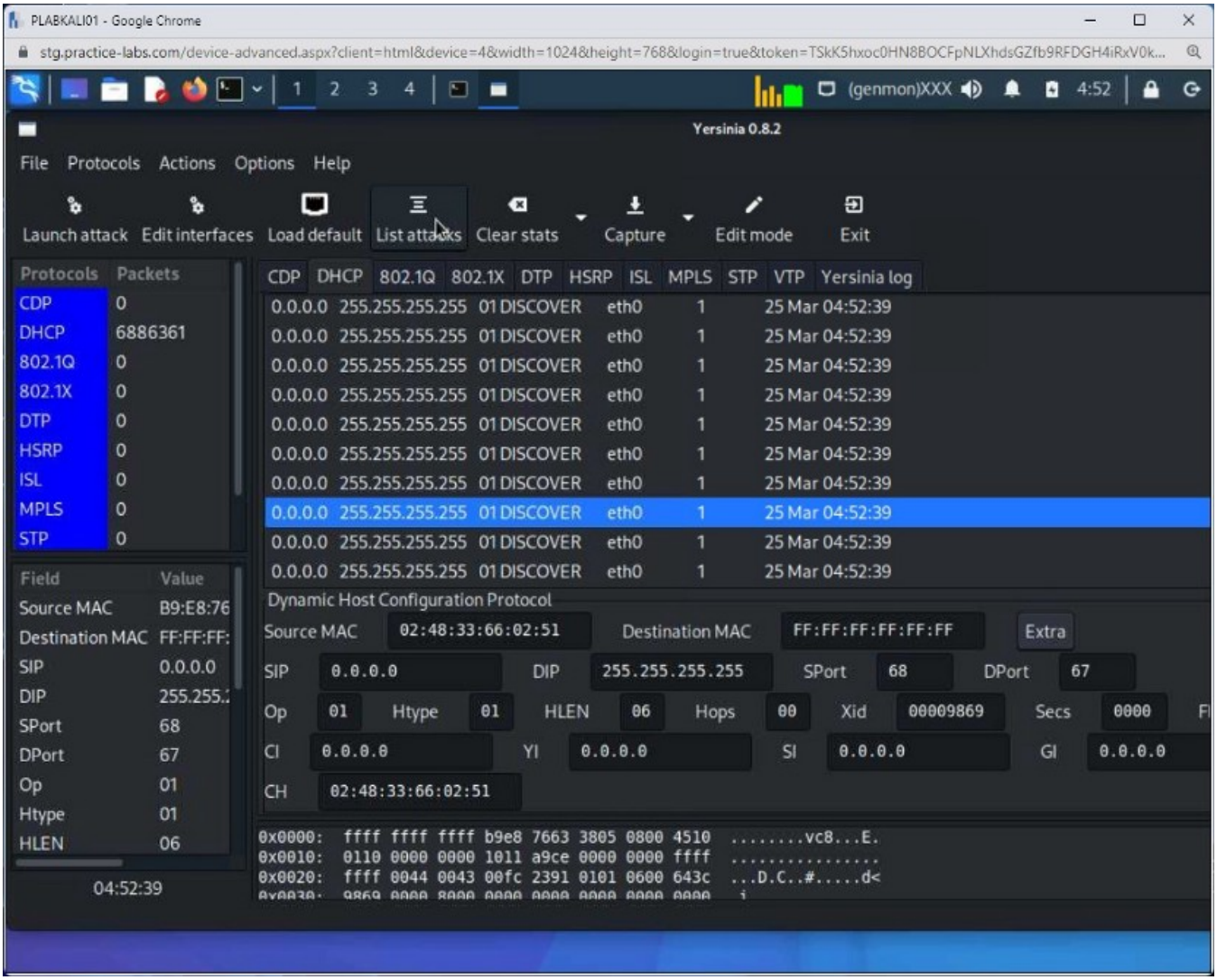
Step 11

On the **Unsaved packets** dialog box, click **Stop and Quick without Saving**.



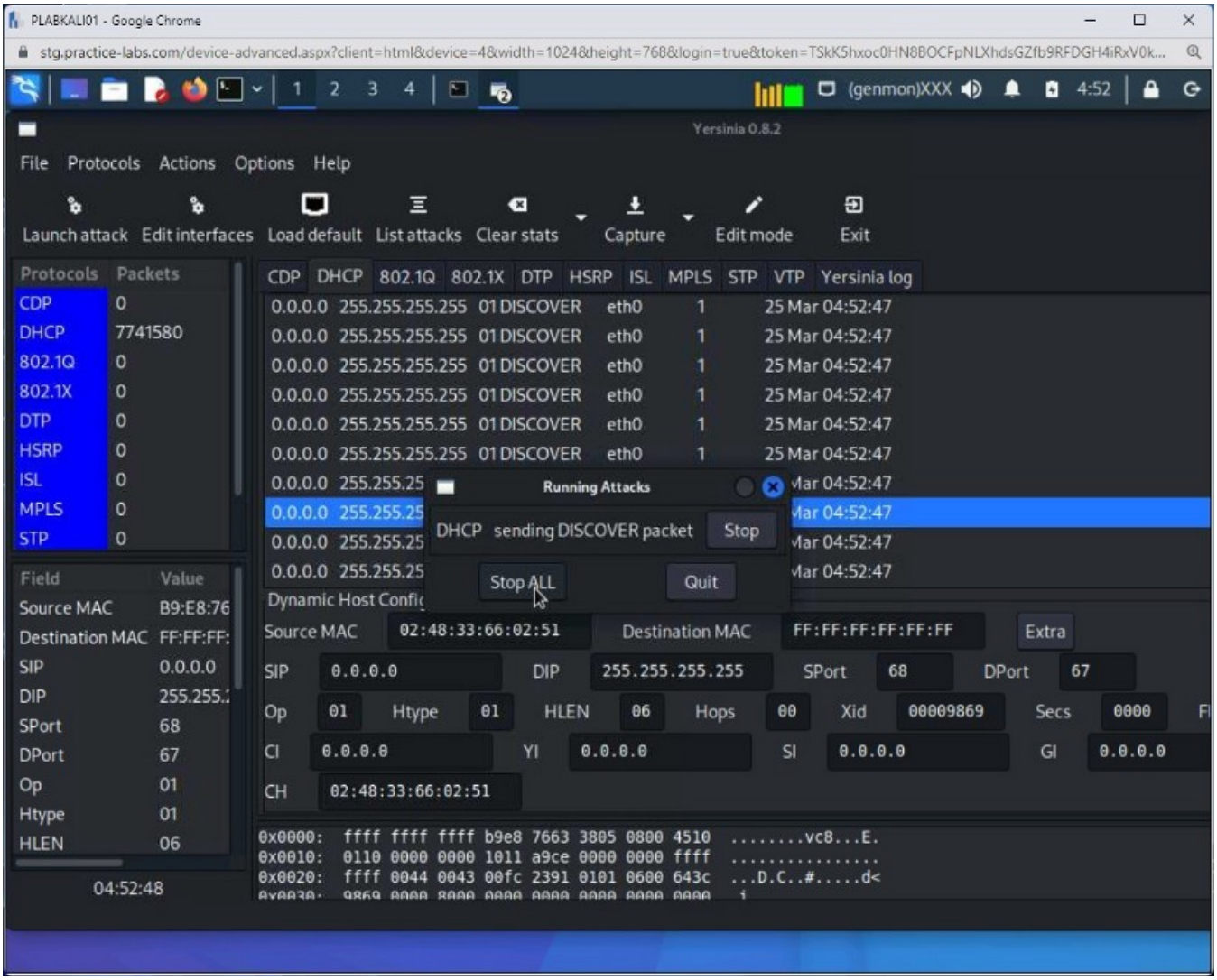
Step 12

Back on the **Yersinia 0.8.2** window, click **List attacks**.



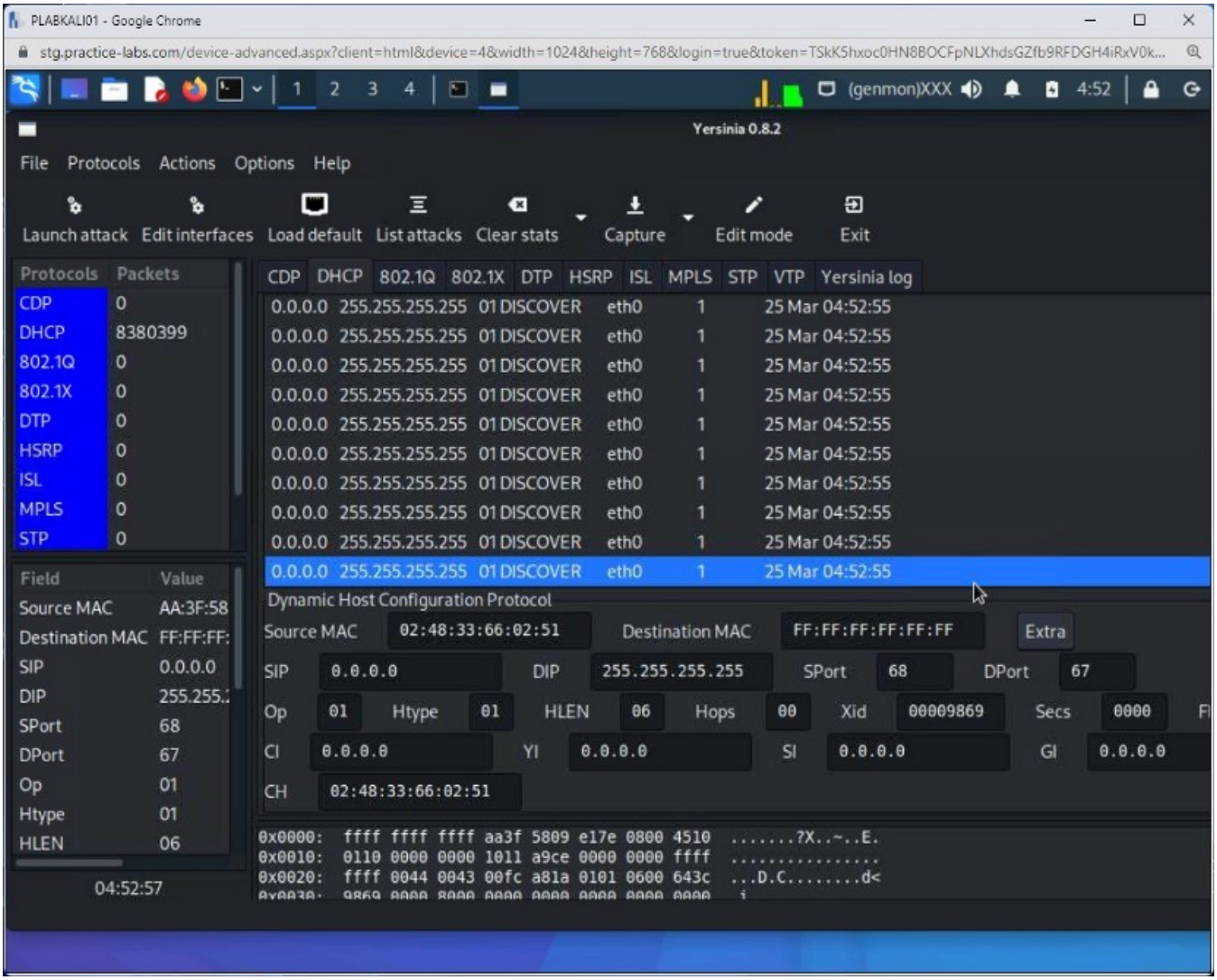
Step 13

The **Running Attacks** dialog box is displayed. Click **Stop ALL**.



Step 14

The starvation attack has now stopped.



Exercise 5 — Sniffing Technique: DNS Poisoning

DNS poisoning intends to forge the DNS records so that the victim can be redirected to the malicious sites. The attacker adds the fake or forged records into the DNS resolver cache, which the DNS uses to respond to the DNS queries received from the clients.

In this task, you will learn to perform DNS poisoning.

Learning Outcomes

After completing this exercise, you will be able to:

- Use DNSChef

ask 1 — Use DNSChef

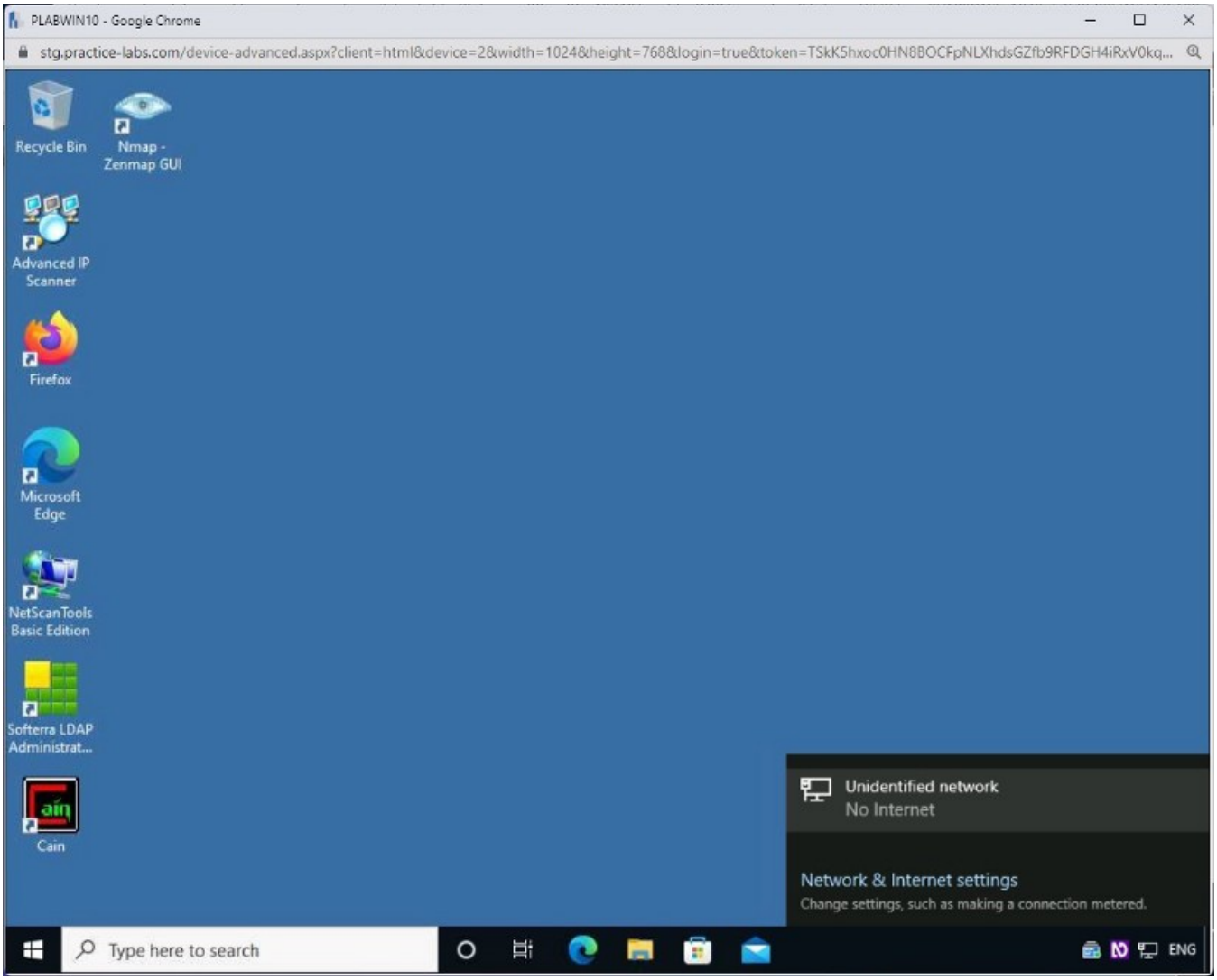
DNSChef is a DNS proxy that allows you to redirect all DNS queries to a single IP address. You can use this application to forward connections to the destination of your choice. For example, when you send a query for Microsoft.com, it redirects the query to

the DNS server you specified. You will use PLABWIN10 to use 192.168.0.4 as the DNS server and verify the name resolution using nslookup.

In this task, you will learn to use DNSChef.

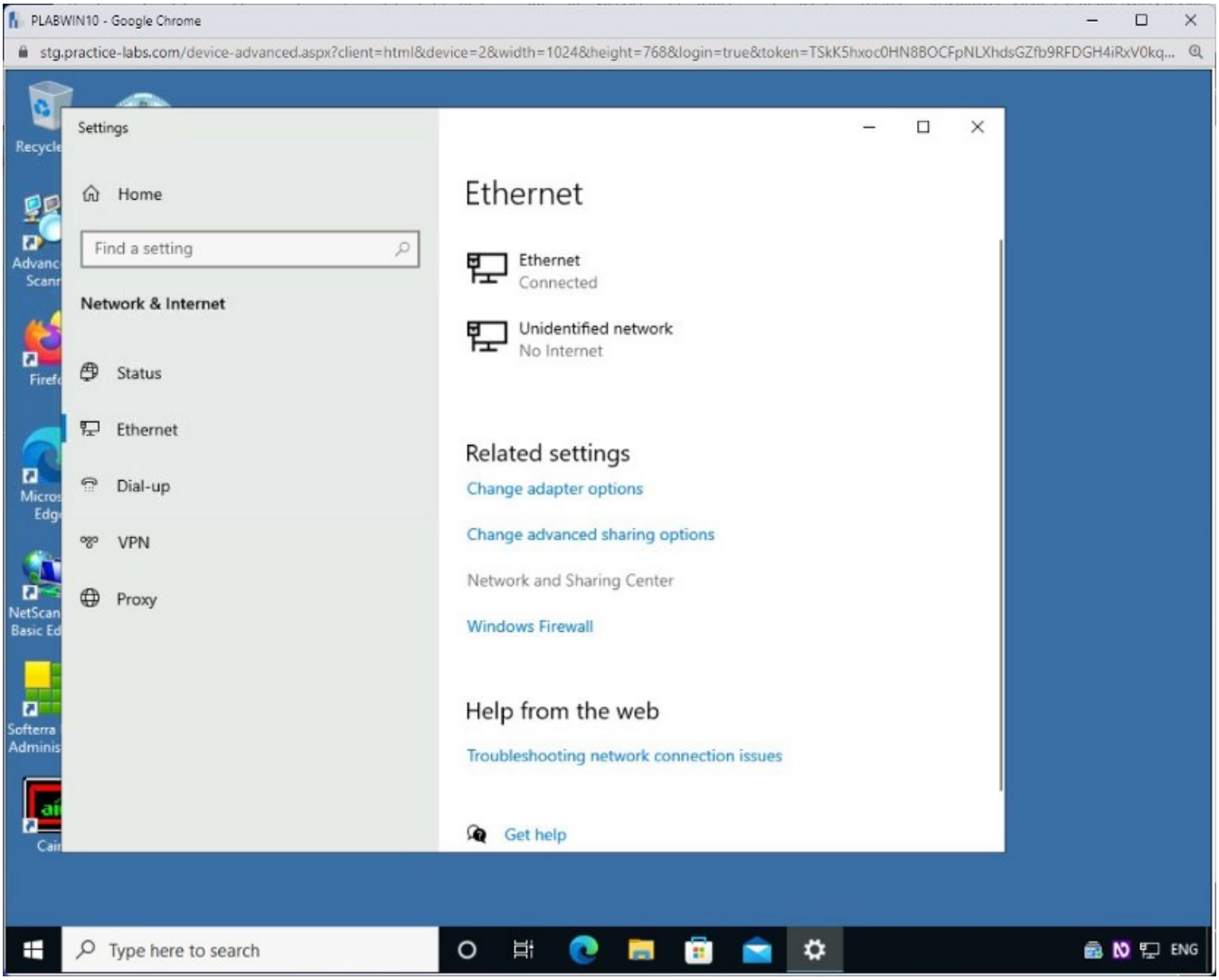
Step 1

Connect to **PLABWIN10**. In the system tray, click the computer icon and then select **Unidentified network**.



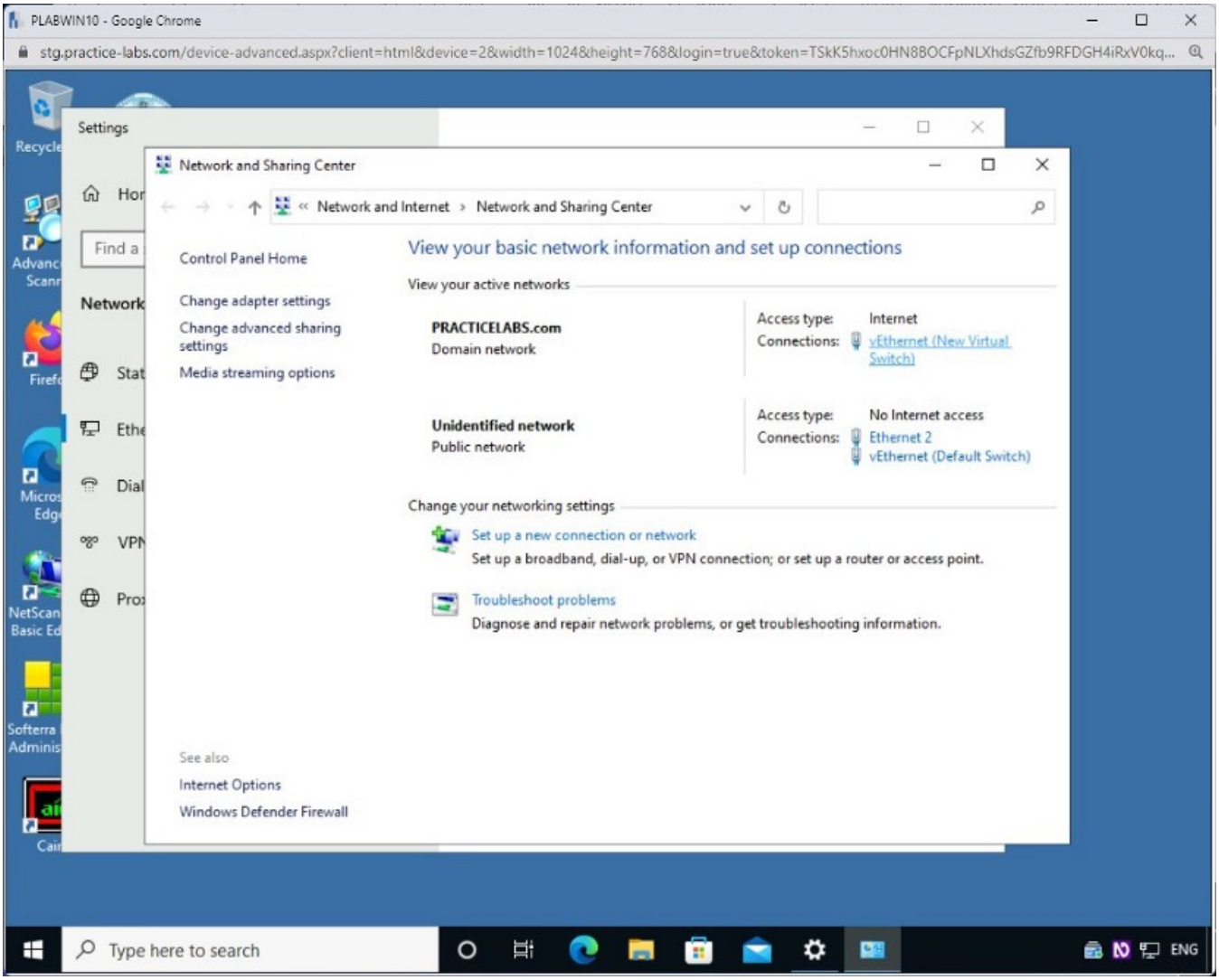
Step 2

On the **Ethernet** page, click **Network and Sharing Center**.



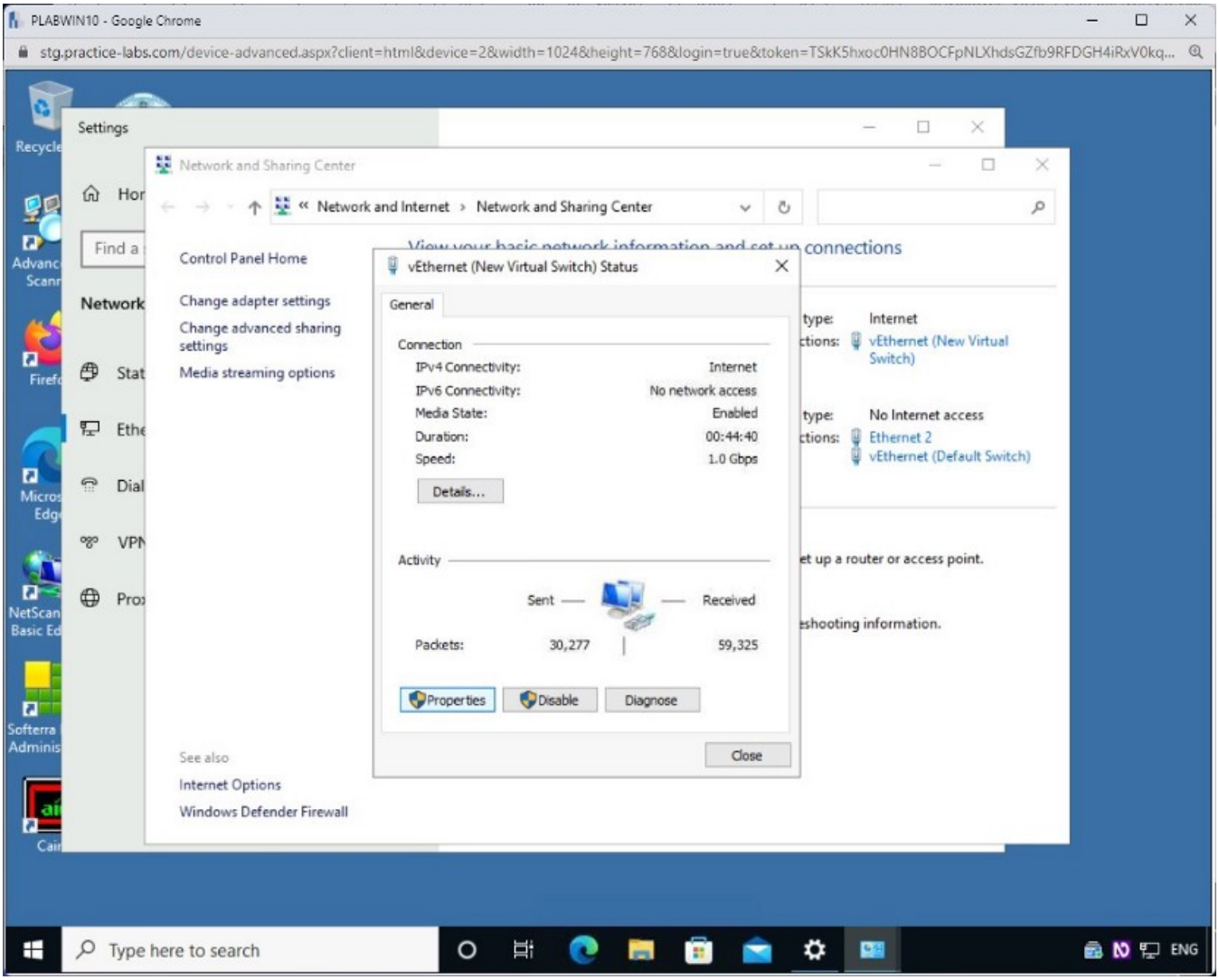
Step 3

A page with the network connections is displayed. Click **vEthernet (New Virtual Switch)** for **PRACTICELABS.COM**.



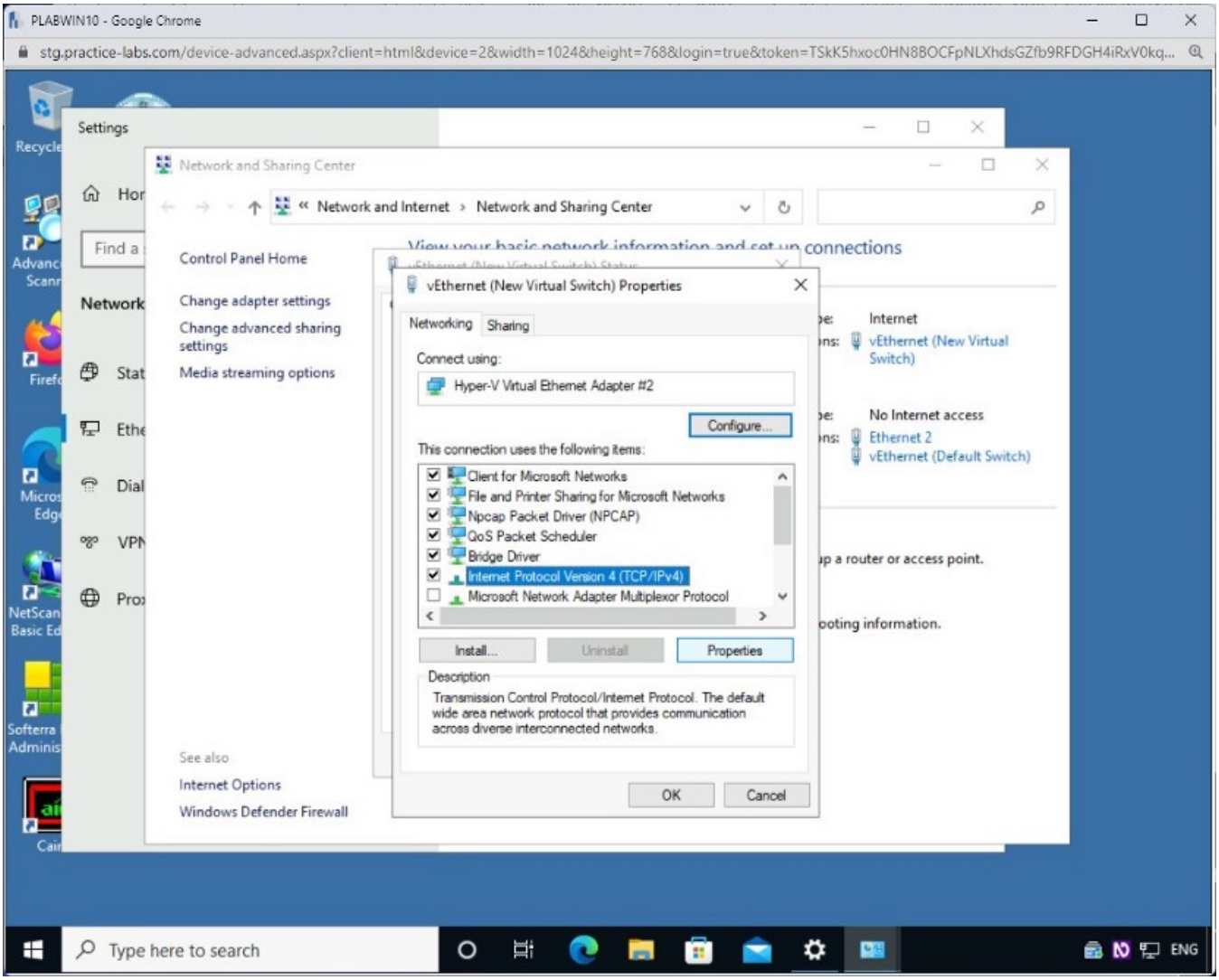
Step 4

Click **Properties** on the **vEthernet (New Virtual Switch) Status** dialog box.



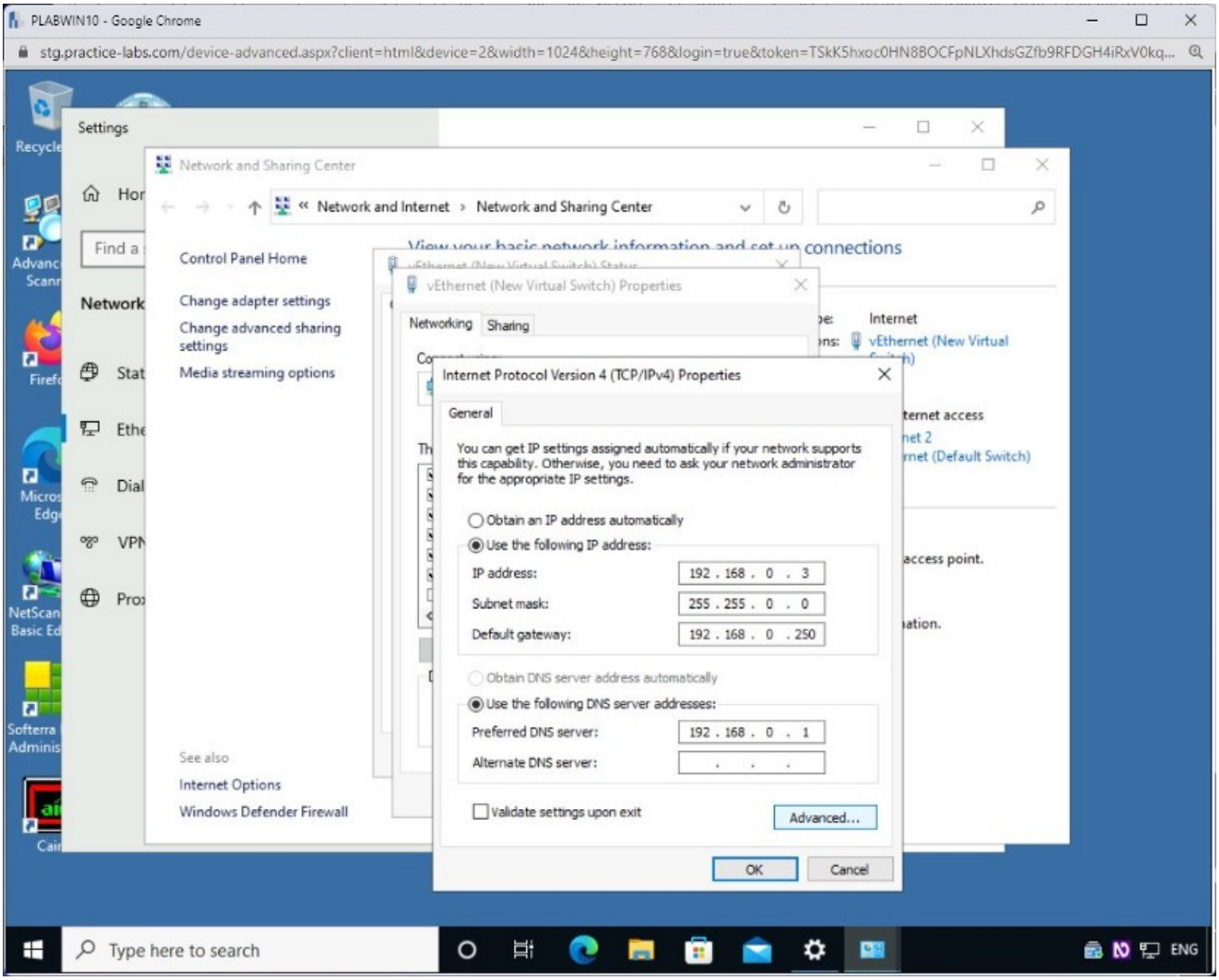
Step 5

On the **vEthernet (New Virtual Switch) Properties** dialog box, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



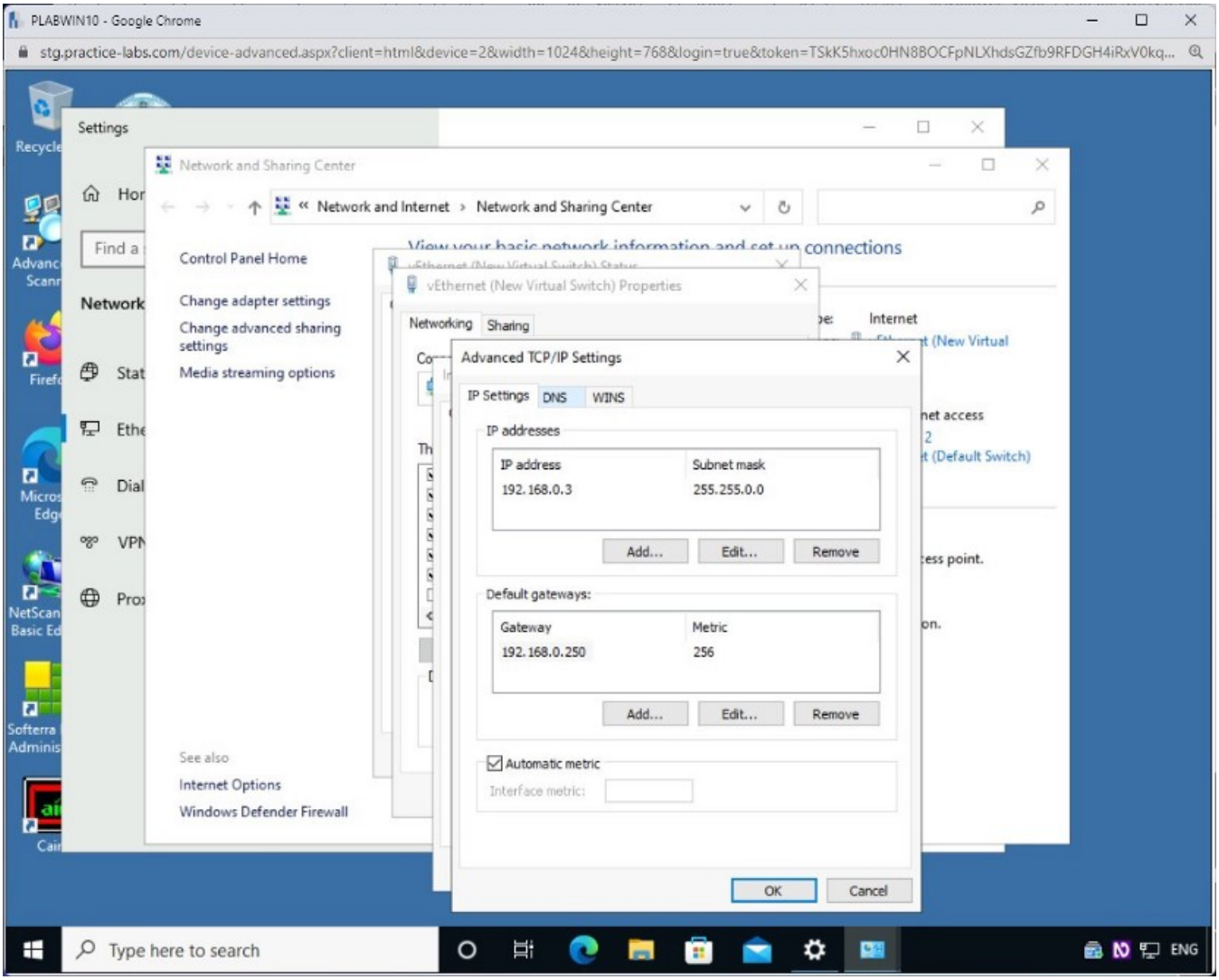
Step 6

Click **Advanced** on the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box.



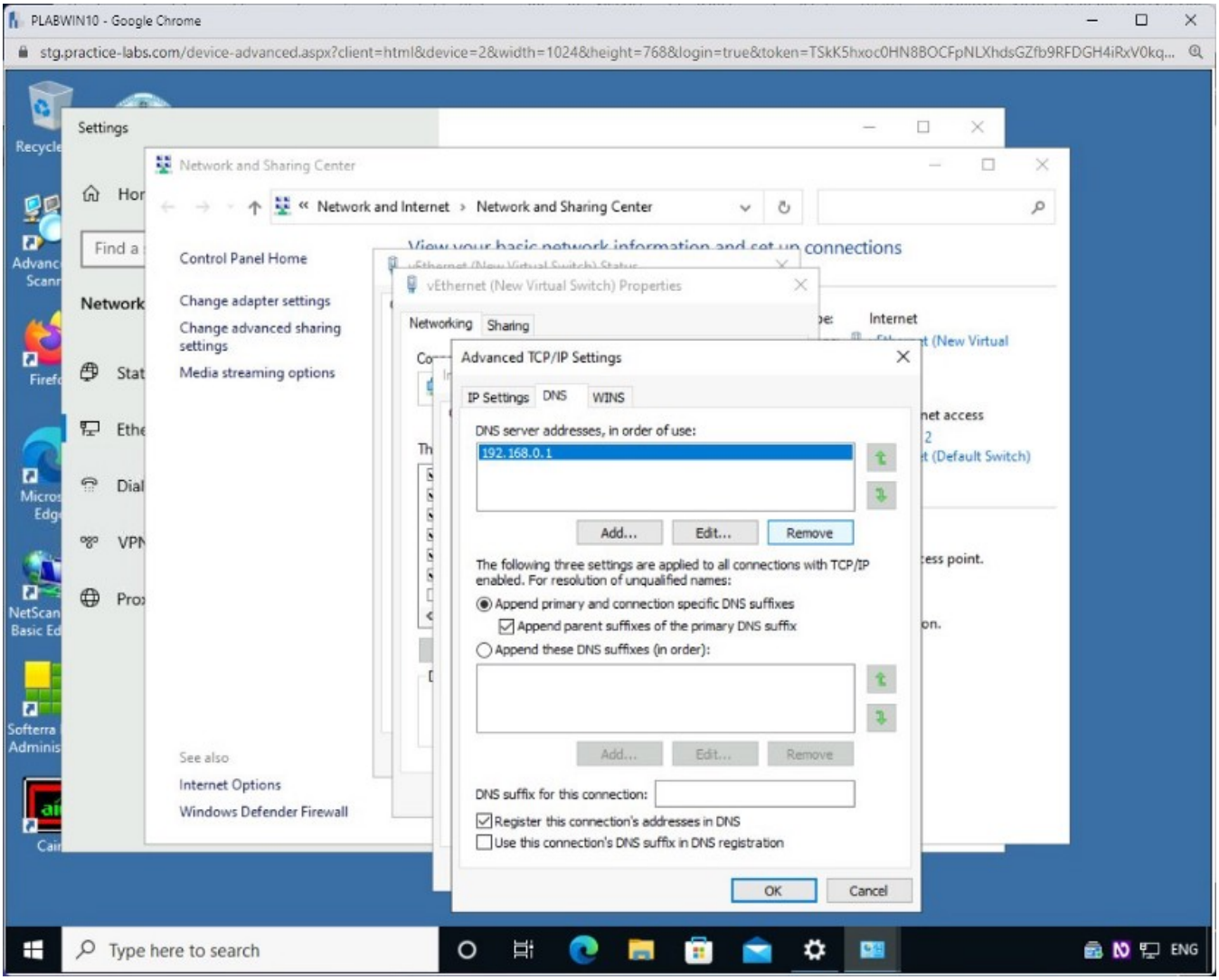
Step 7

Click the **DNS** tab on the **Advanced TCP/IP Settings** dialog box.



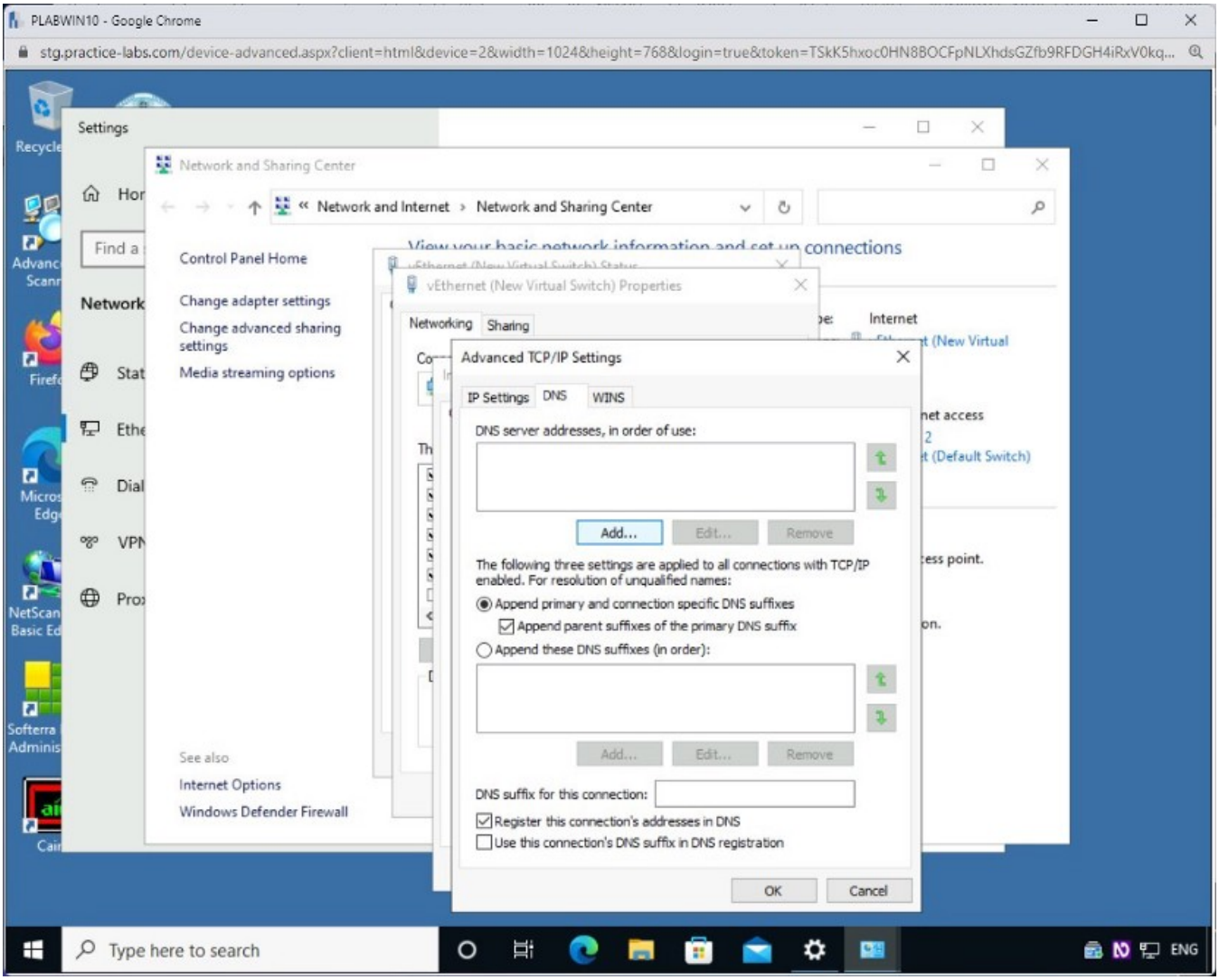
Step 8

On the **DNS** tab, ensure **192.168.0.1** is selected. Click **Remove**.



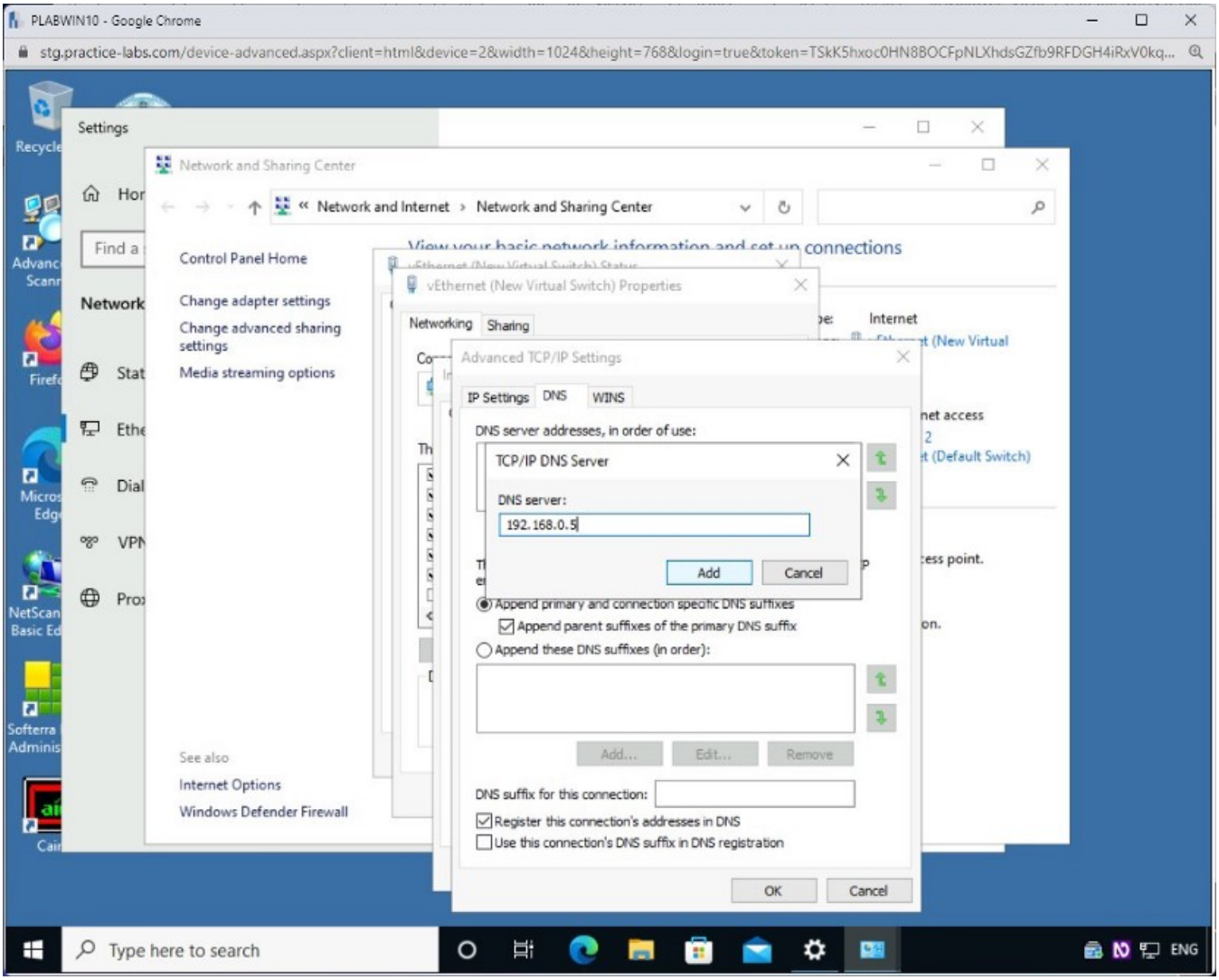
Step 9

Click **Add**.



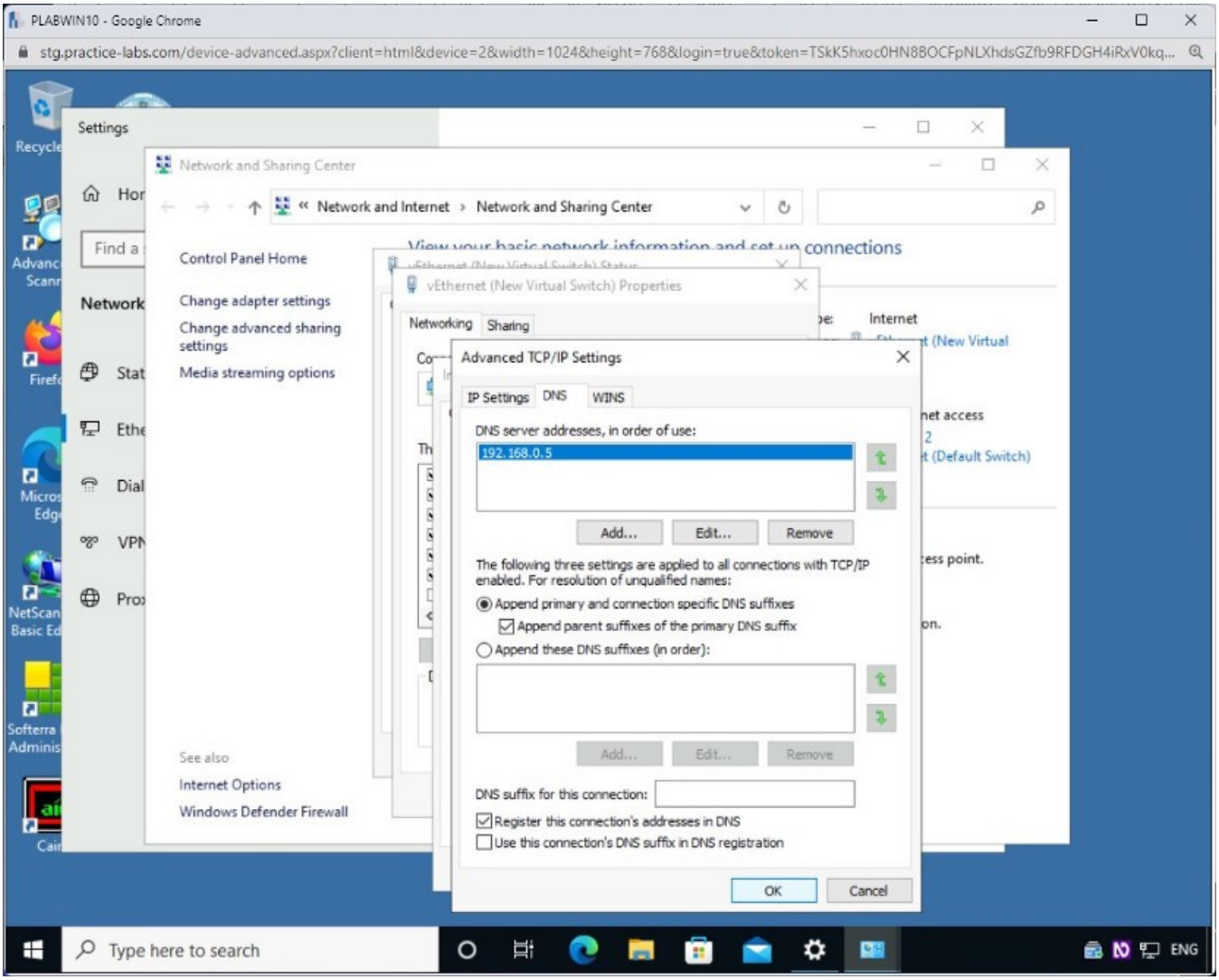
Step 10

In the **TCP/IP DNS Server** dialog box, **192.168.0.1** appears automatically. Change it to **192.168.0.5** and click **Add**.



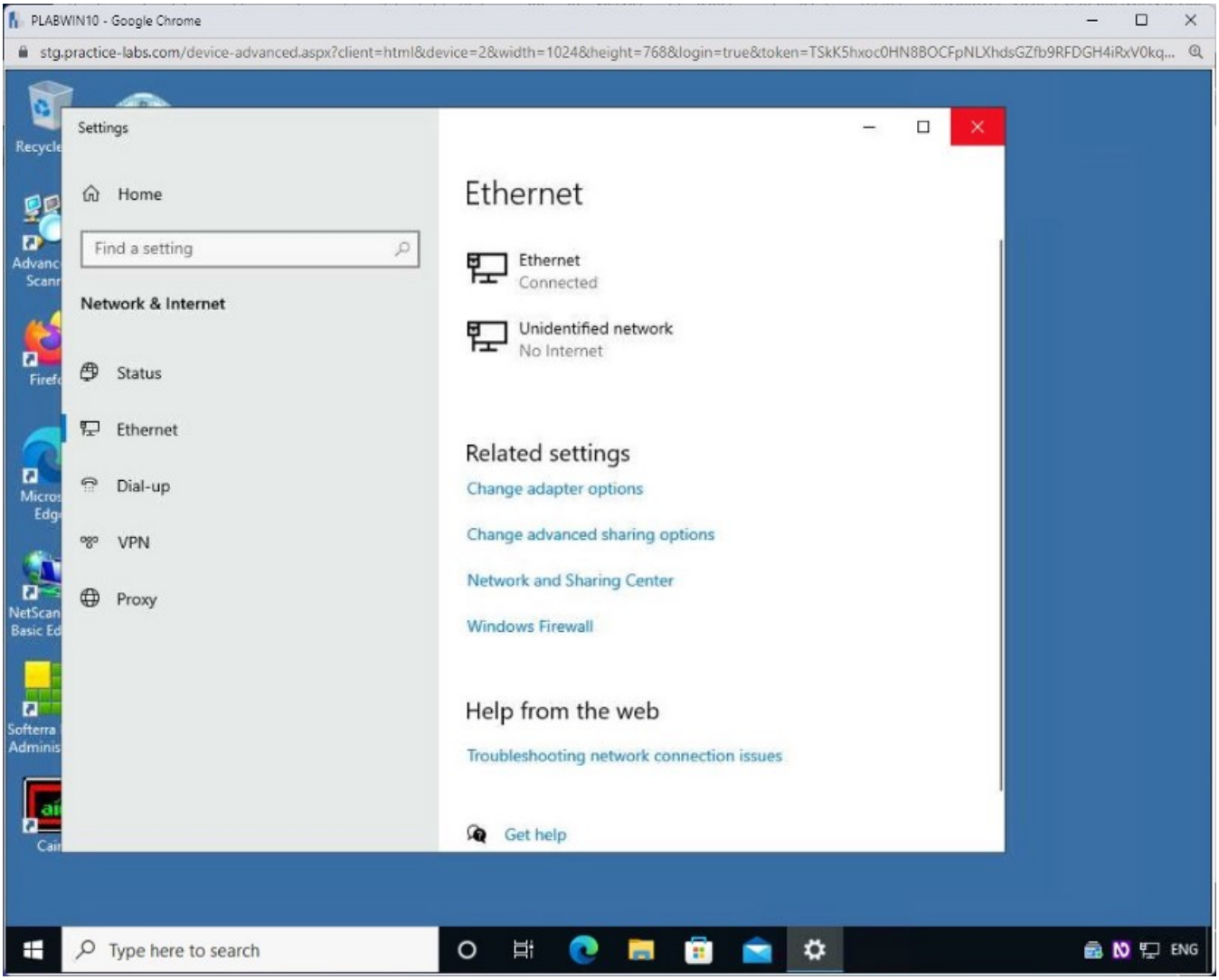
Step 11

Notice that **192.168.0.5** is now added as the **DNS** server. Click **OK** to close the dialog box.



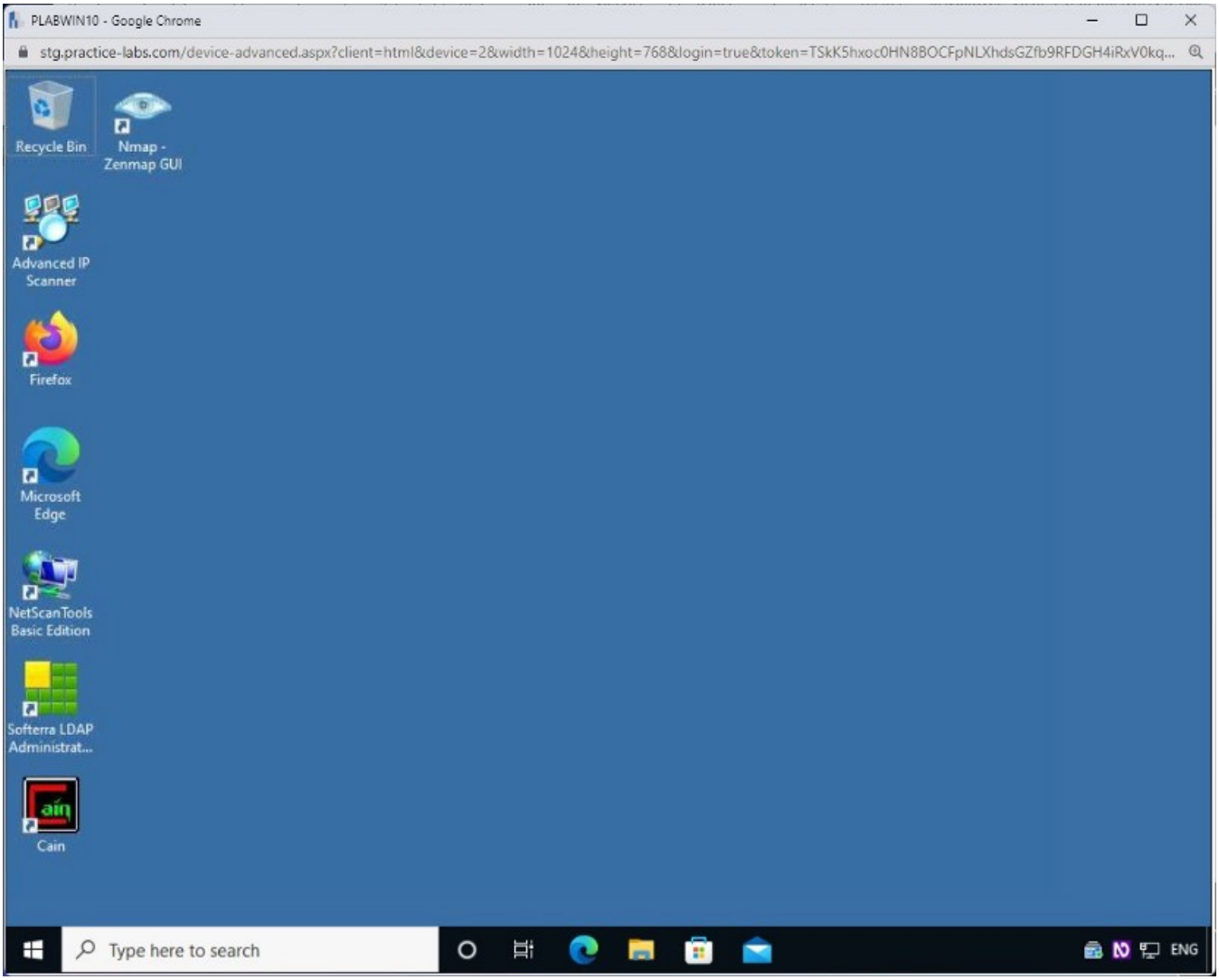
Step 12

Close the remaining dialog boxes and close all open windows.



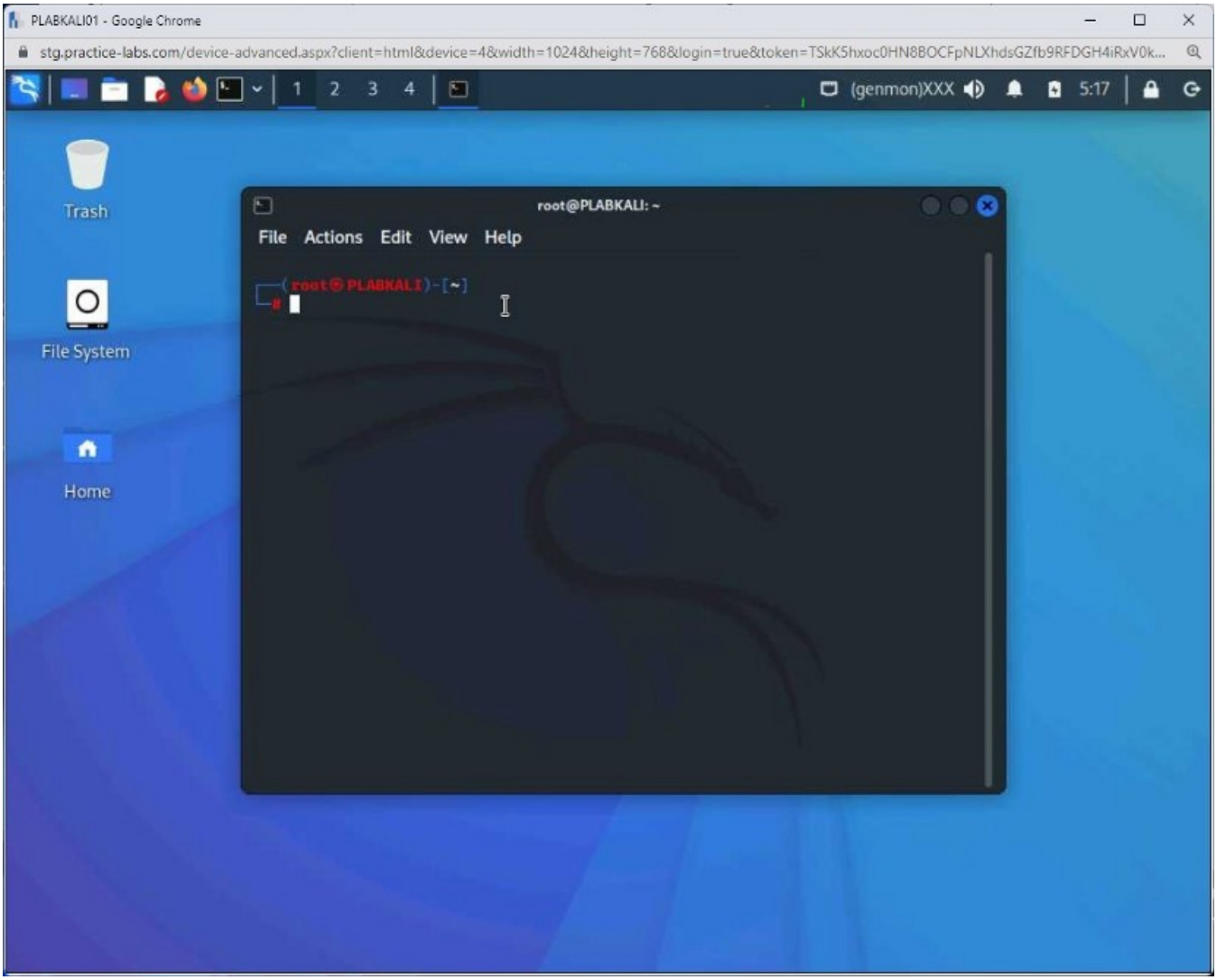
Step 13

You should now be on your desktop.



Step 14

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

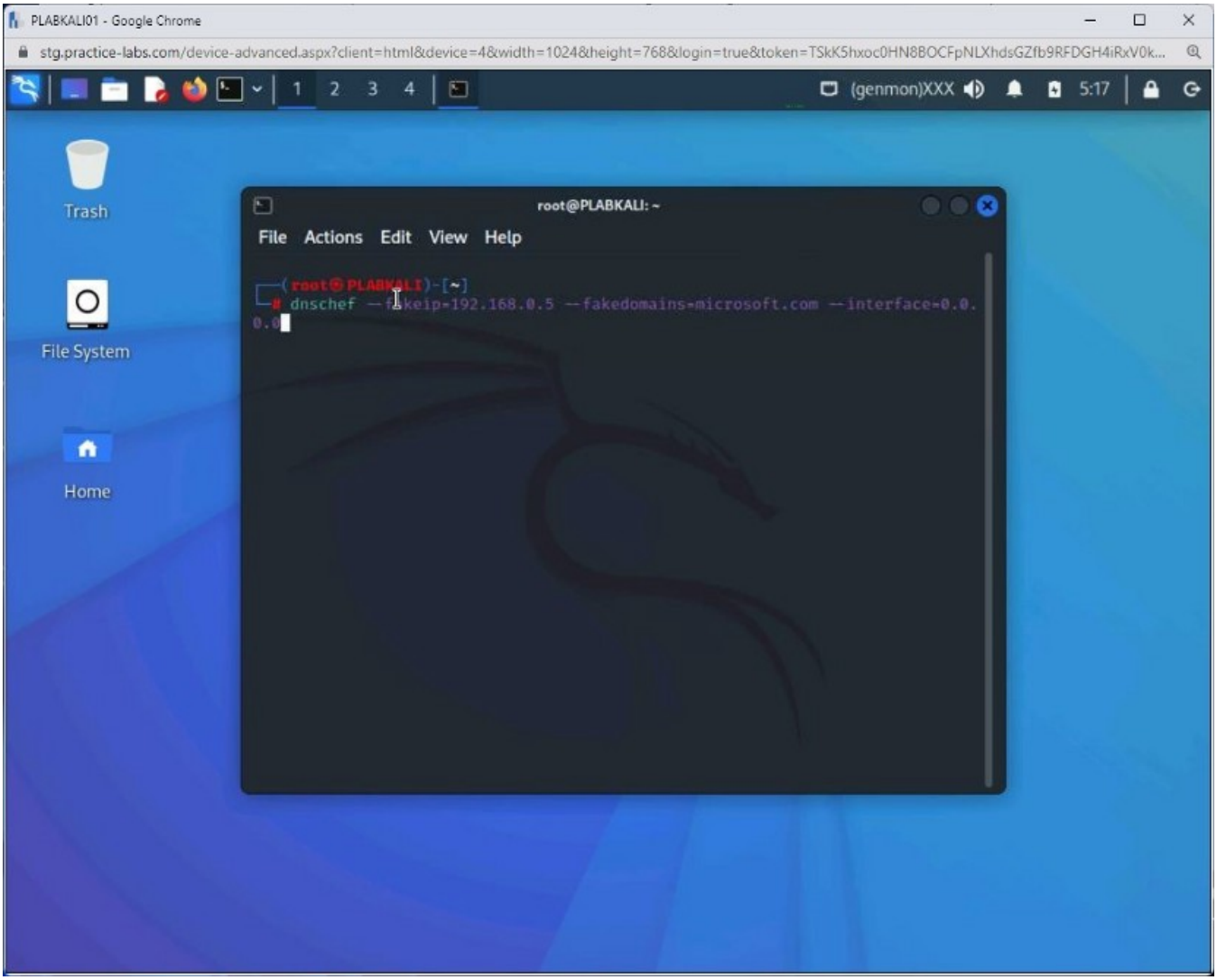


Step 15

You will now use DNSChef to resolve the domain names to fake IP addresses. To do this, type the following command:

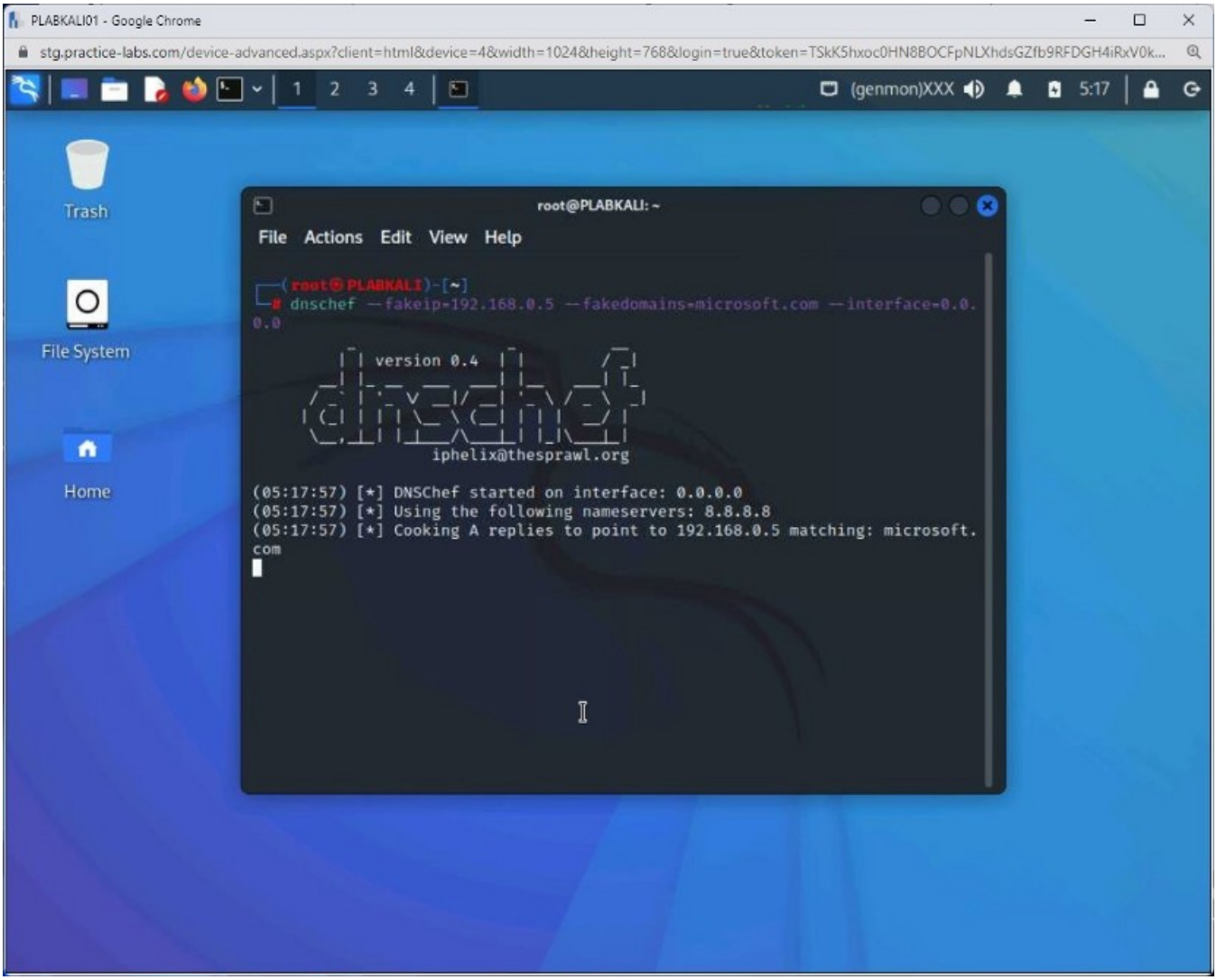
```
dnschef --fakeip=192.168.0.4 --fakedomains=microsoft.com --
interface=0.0.0.0
```

Press **Enter**.



Step 16

The DNS proxy starts. Keep the terminal window open and DNSChef running.

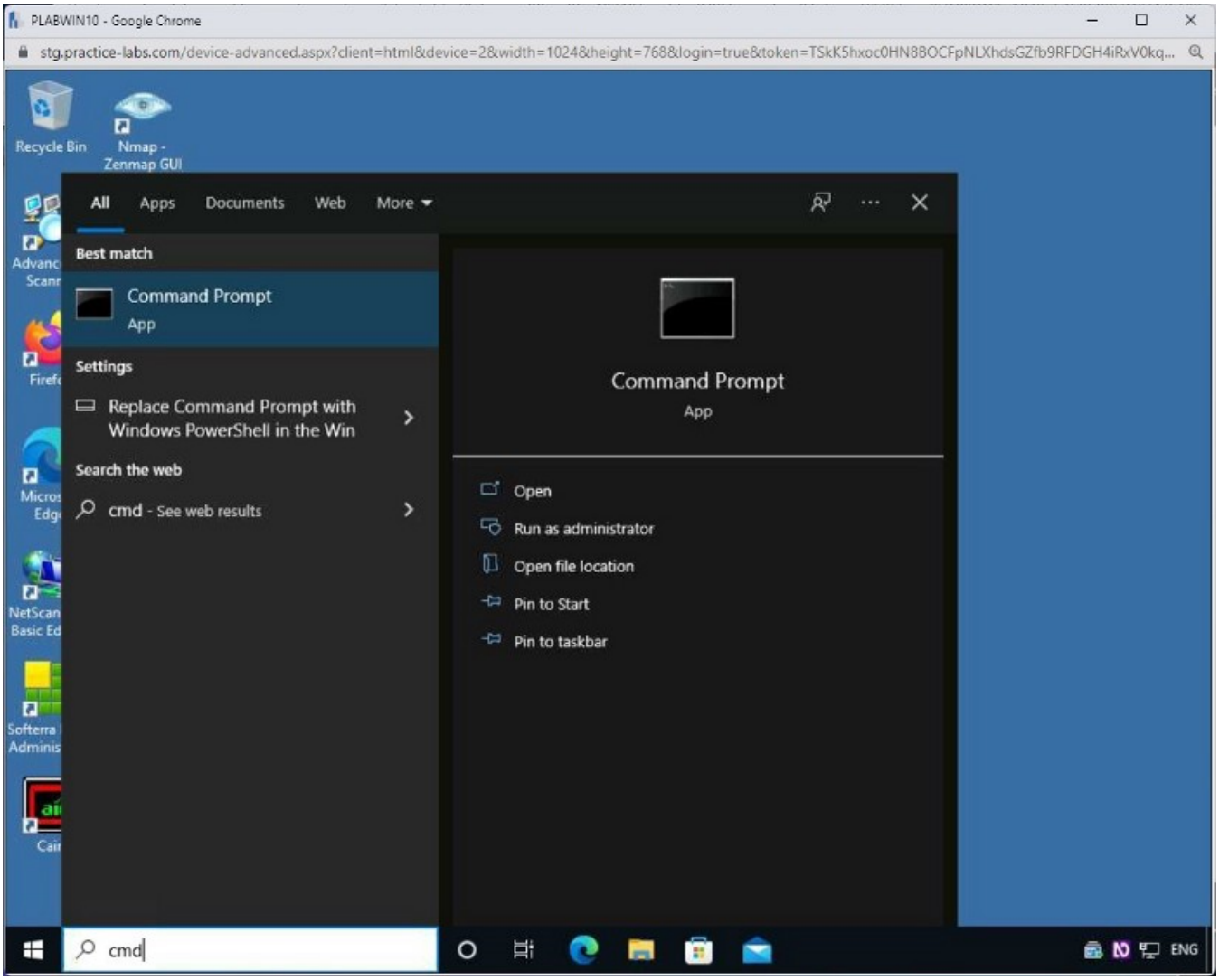


Step 17

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

```
cmd
```

From the given search results, select **Command Prompt**.

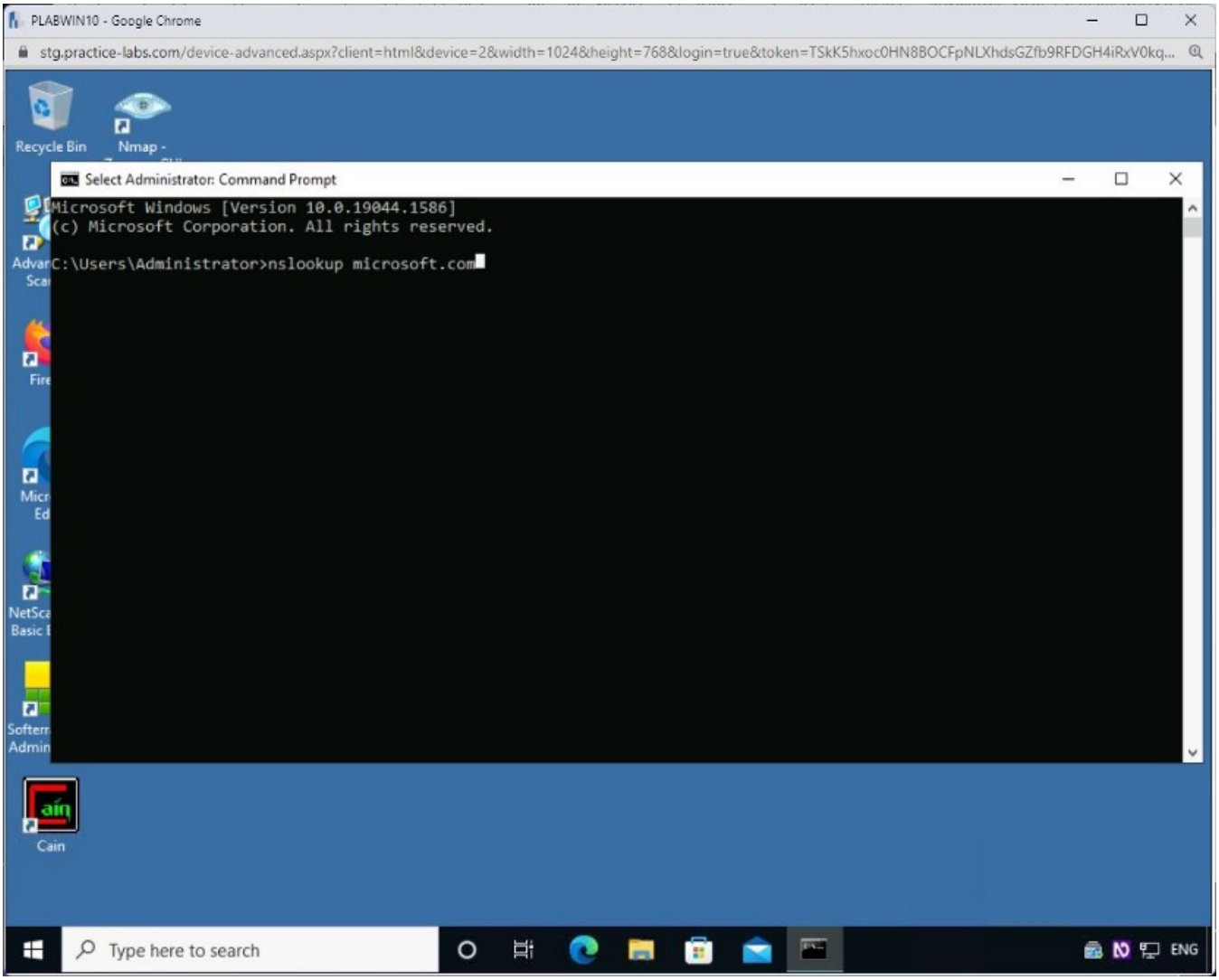


Step 18

In the command prompt window, type the following command:

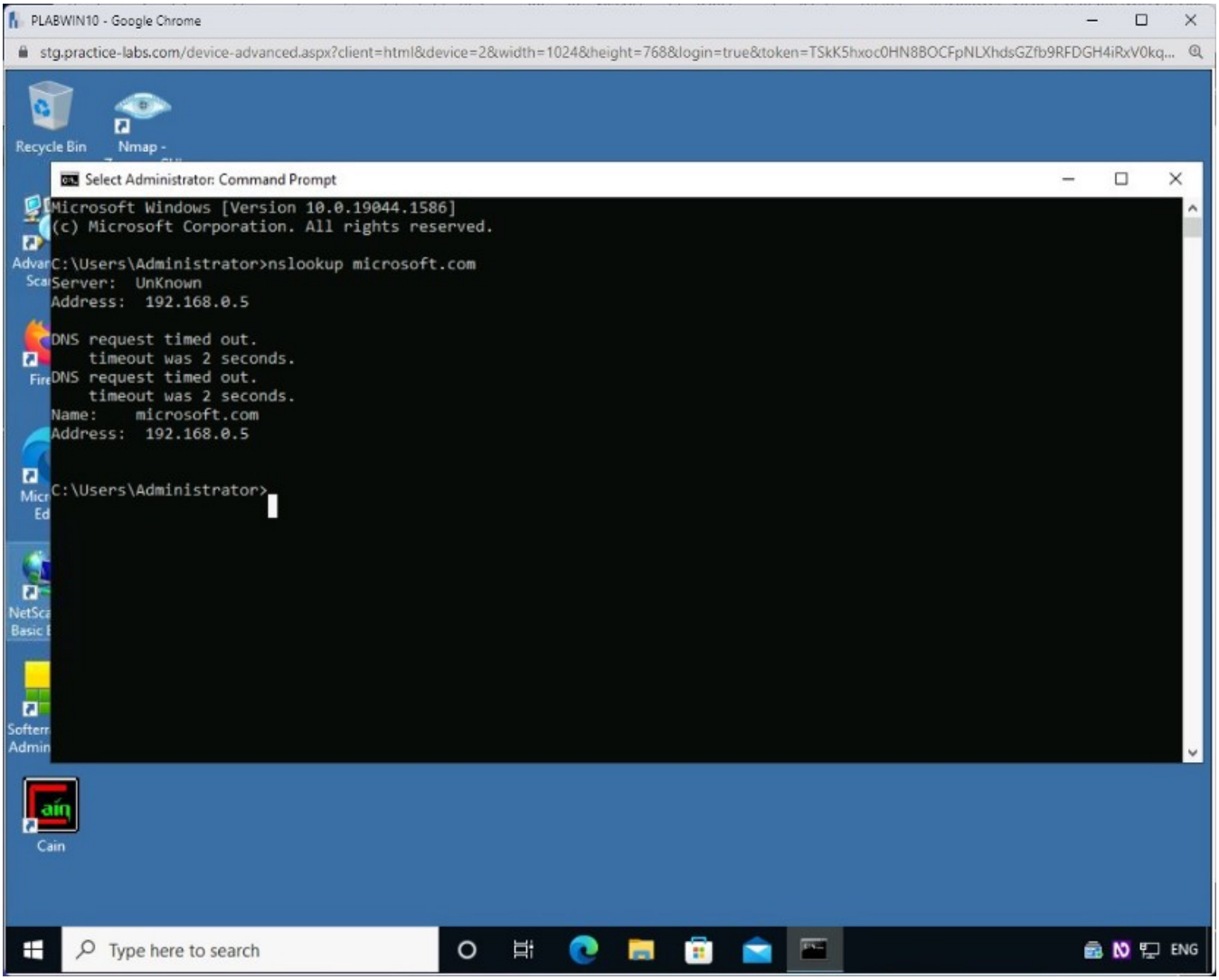
```
nslookup microsoft.com
```

Press **Enter**.



Step 19

In the output, notice that **microsoft.com** is resolved to **192.168.0.5**.



Exercise 6 — Sniffing Countermeasures and Detection Methods

Various methods can be used against sniffing, which usually takes place using weak protocols, such as HTTP and FTP. As a basic precaution, you would avoid using weak protocols. It is always advisable to use protocols that encrypt traffic. Encryption also prevents the attacker from reading data in transmission.

In this exercise, you will learn to prevent sniffing attacks.

Learning Outcomes

After completing this exercise, you will be able to:

- Use XArp utility

After completing this module, you have further knowledge of:

- Defend Against Sniffing
- Detect Sniffing

Defend Against Sniffing

You can follow a few simple rules to avoid sniffing:

- Avoid using secure protocols, such as:
- HTTPS instead of HTTP
- SCP or SFTP instead of FTP
- SSH instead of Telnet
- POP3 instead of POP
- SNMPv3 instead of SNMPv1 or v2
- Avoid retrieving MAC addresses from the operating system. Rather, retrieve it from the Network Interface Card (NIC) directly
- Use Access Control Lists (ACL)
- Avoid using a hub and use a switch instead
- Configure DHCP Snooping
- Configure Dynamic ARP inspection
- Configure Source guard
- Use a tool such as XArp to detect ARP-based attacks
- Use a sniffing detection tool to detect a network adapter working in promiscuous mode
- Use appropriate encryption
- Restrict access to physical media to prevent someone from installing a physical packet sniffer
- Ensure that the gateway's MAC address is added to the ARP cache
- Implement network monitoring and scanning tools, such as an Intrusion Detection System IDS and Nmap to detect sniffers and malicious traffic

Detect Sniffing

Detecting sniffers on a network is not easy. This is because sniffers do not transmit any data back to target systems. They sit quietly on a network and capture traffic in passive mode. Various methods can be used for detecting sniffers.

One method you can use is finding systems with their Network Interface Cards (NICs) configured in promiscuous mode. This can be done with the tools such as Nmap and methods like reverse DNS lookup.

Another method that can be used is sending a ping request to a suspected system with a sniffer installed. If the system is not running a sniffer, it finds the MAC address to be incorrect and rejects the ping request. On the other hand, a system with a sniffer does not reject as it accepts all traffic even if it is with an incorrect MAC address. Because of this, you can get a clue by sending the ping request with an incorrect MAC address.

Sniffers that perform reverse DNS lookup tend to increase the network traffic. If you suspect a system is performing a reverse DNS lookup, attempt to capture its traffic. A high volume of traffic could be indicative of a sniffer.

Task 1 — Use XArp Utility

XArp helps you detect ARP-based attacks.

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

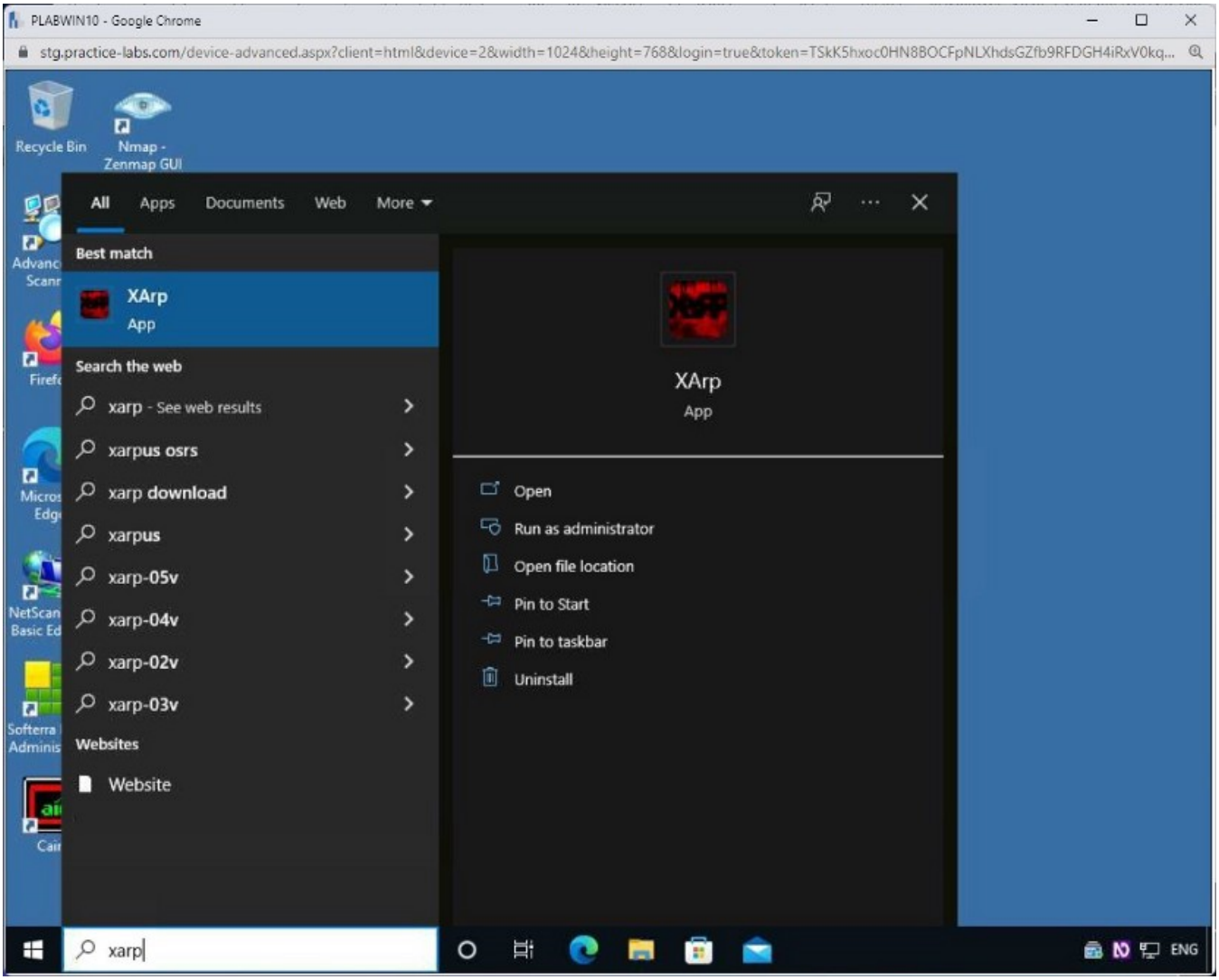
Step 1

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

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

```
Xarp
```

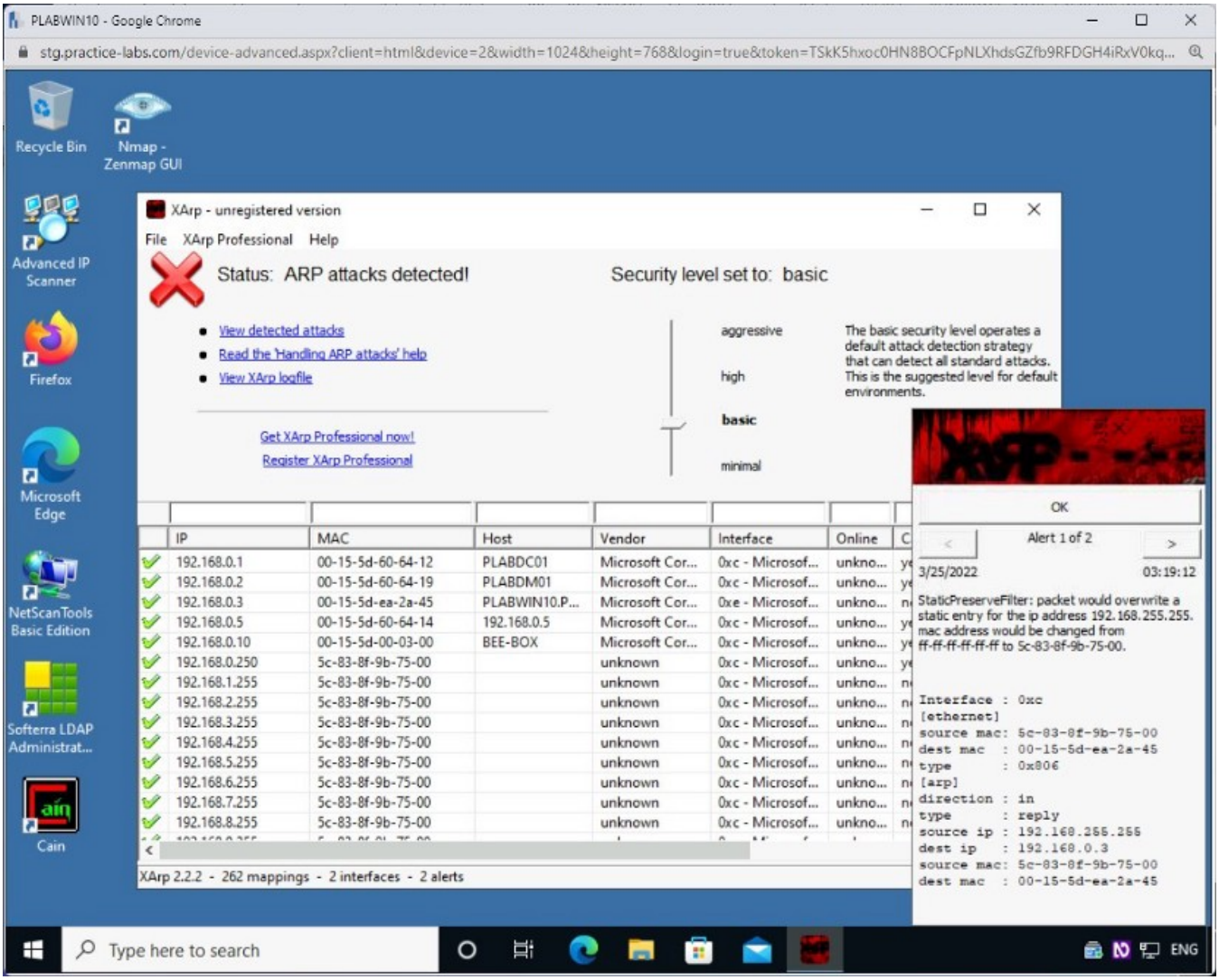
From the search results, click **XArp**.



Step 2

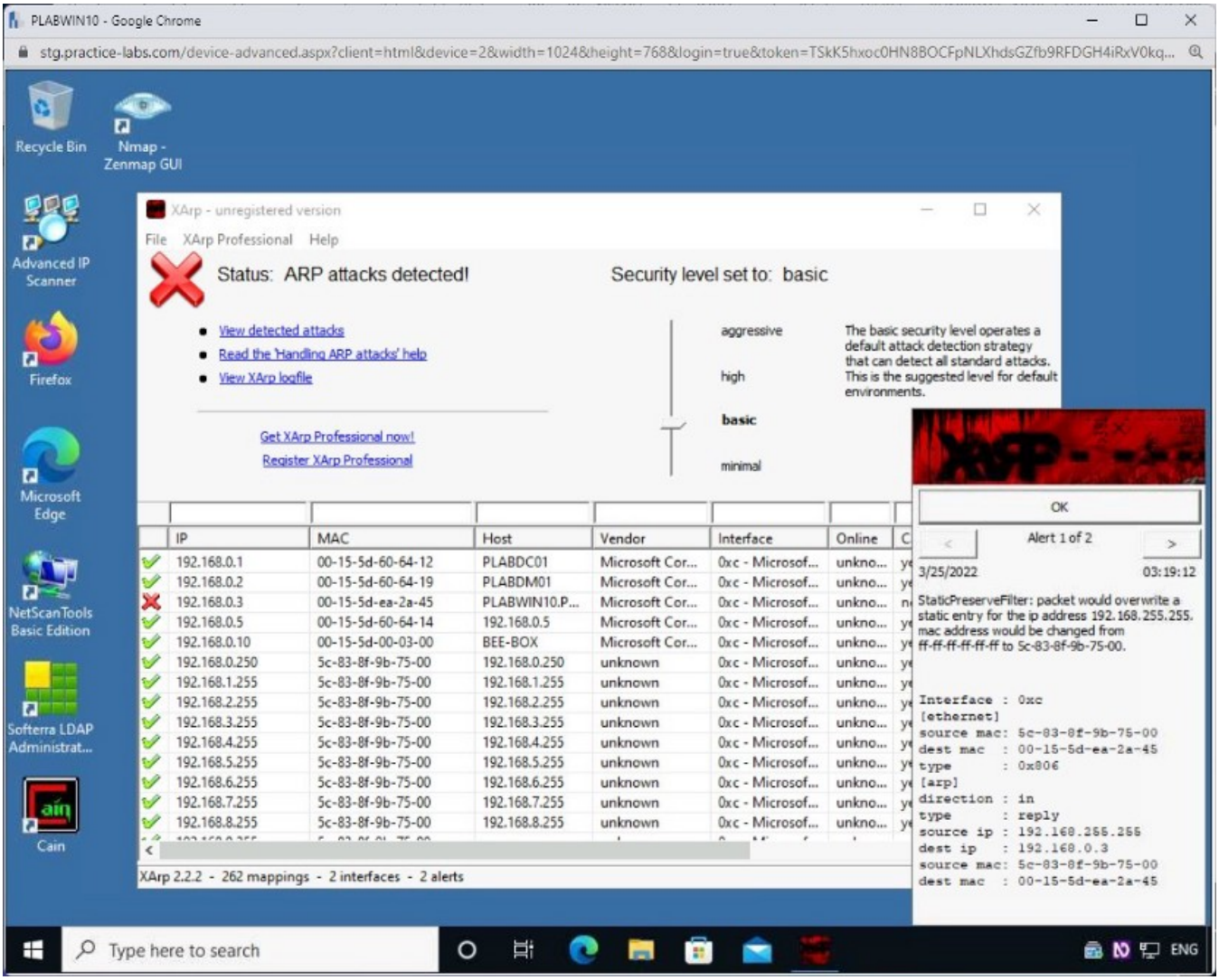
The **XArp — unregistered version** window is displayed.

Note that the default security level is set to **basic**, but it is still detecting an active ARP attack.



Step 3

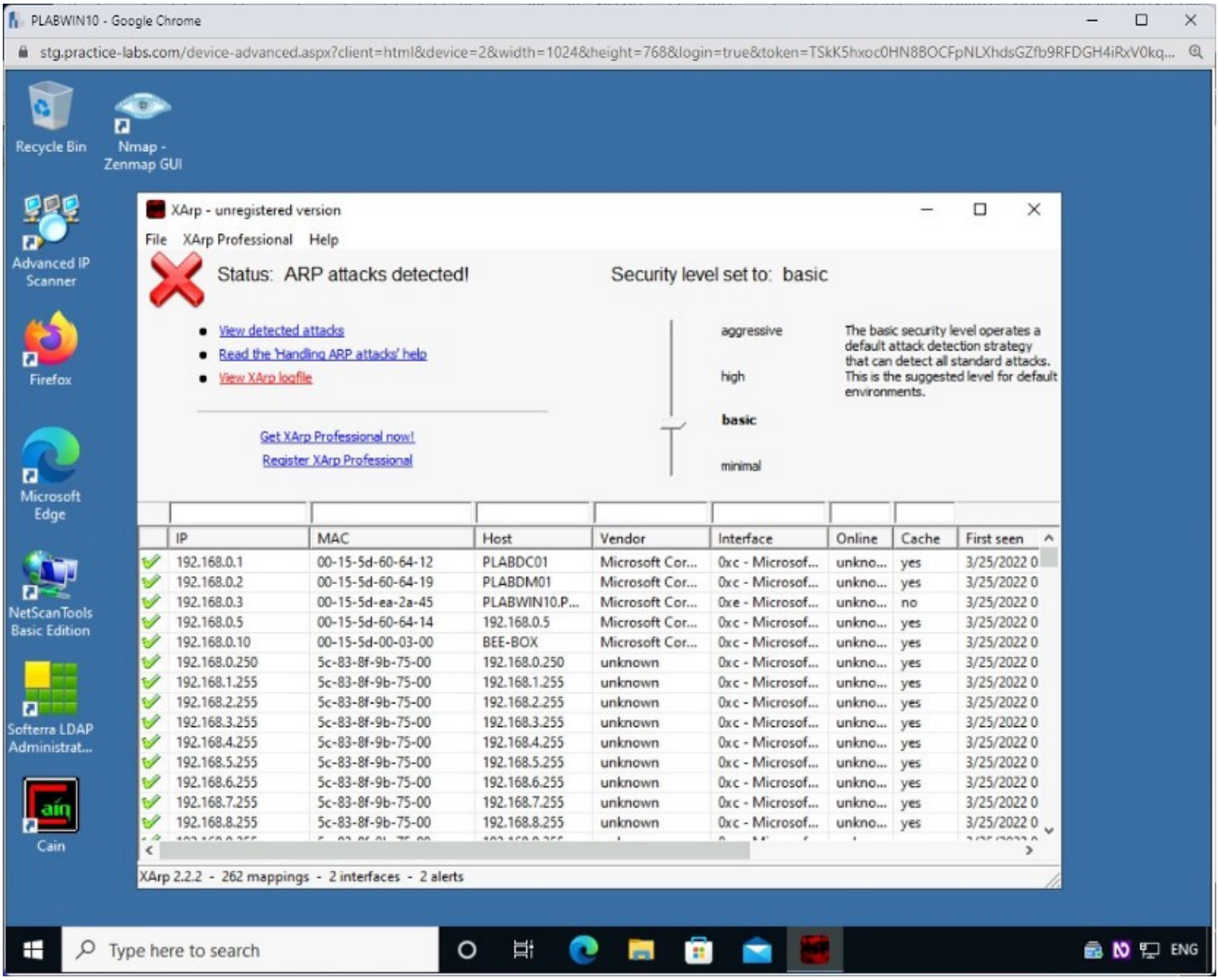
Click OK on the **Alert 1 of 2** window.



Step 4

You can also view the detailed log.

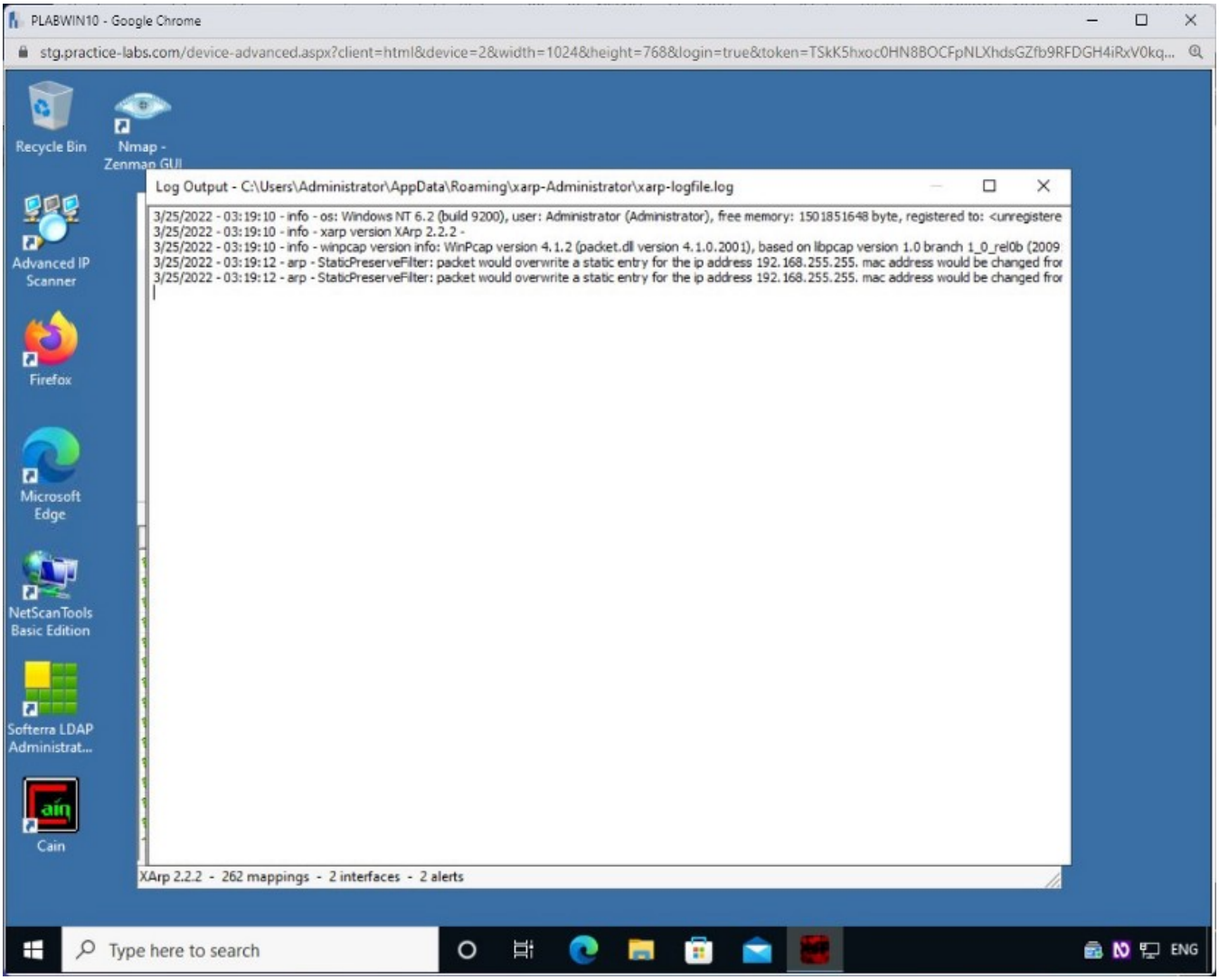
Click **View XArp logfile**.



Step 5

The **Log Output** file is displayed.

A detailed list of events is entered into this log file.



Close the XArp window.

Task 2 — Use Nmap to Detect Sniffers

You can use Nmap to detect a sniffer on a suspected system. Nmap contains a script named sniffer-detect that can detect a sniffer.

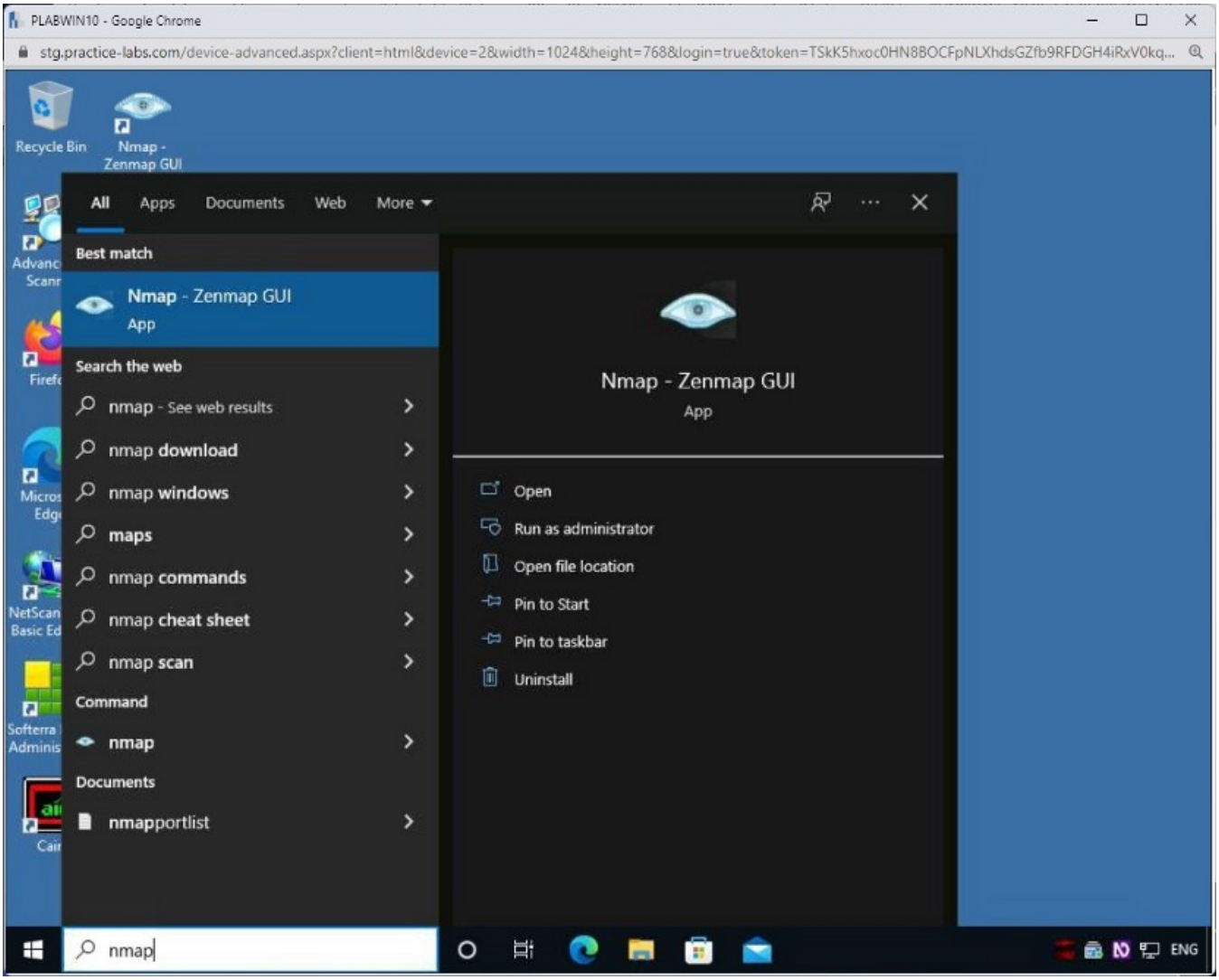
To detect a sniffer, you need to perform the following steps:

Step 1

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

```
nmap
```

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



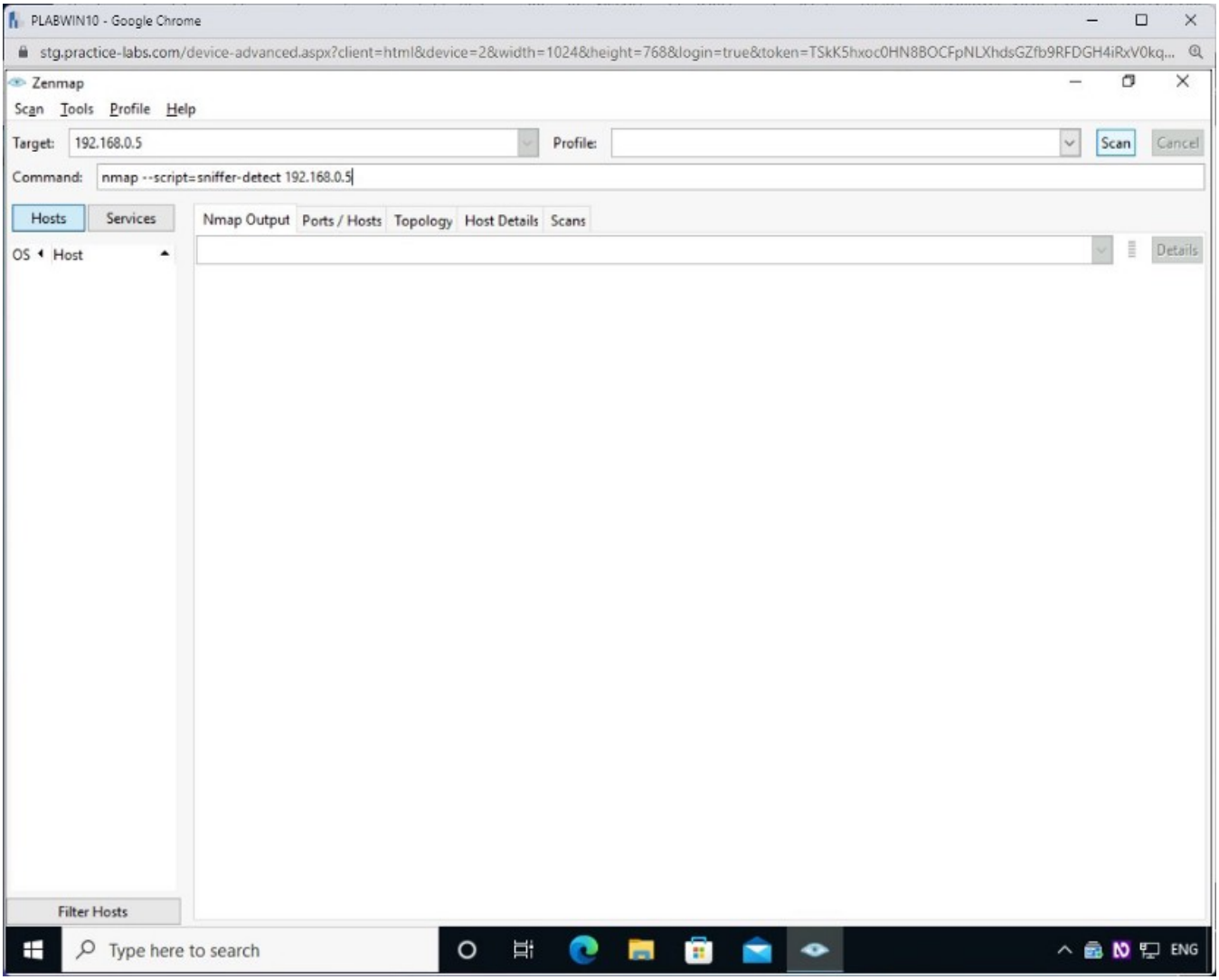
Step 2

The Zenmap window is displayed. Type the following command in the **Command** textbox:

```
nmap --script=sniffer-detect 192.168.0.5
```

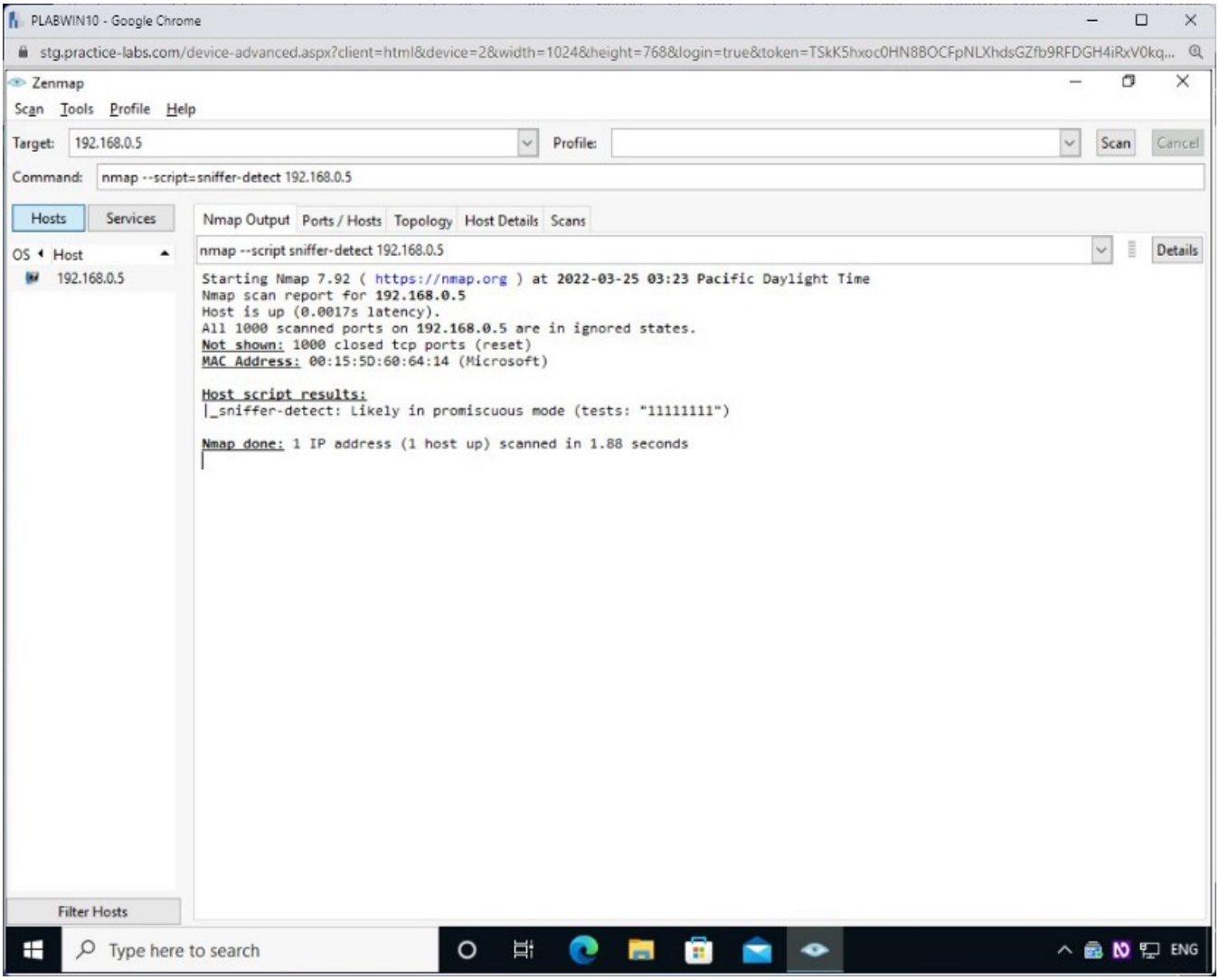
Click **Scan**.

*In this command, you execute a script named **sniffer-detect** with the —**script** parameter.*
*Then, you have defined the target system as **192.168.0.5**.*



Step 3

The scan process runs for a few seconds and can determine a sniffer in the target system. Notice that it mentions it in the **Host script results** section.


PLABWIN10 - Google Chrome
stg.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=TSkK5hxoc0HN8BOCFpNLXhdsGZfb9RFDGH4iRxV0kq...
Zenmap
Scan Tools Profile Help
Target: 192.168.0.5
Profile:
Scan
Cancel
Command: nmap --script=sniffer-detect 192.168.0.5
Hosts
Services
OS Host
192.168.0.5
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap --script sniffer-detect 192.168.0.5
Details
Starting Nmap 7.92 (https://nmap.org) at 2022-03-25 03:23 Pacific Daylight Time
Nmap scan report for 192.168.0.5
Host is up (0.0017s latency).
All 1000 scanned ports on 192.168.0.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:15:5D:60:64:14 (Microsoft)
Host script results:
|_sniffer-detect: Likely in promiscuous mode (tests: "11111111")
Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
Type here to search
ENG