Module 08: Sniffing

Lab 1: Perform Active Sniffing

Lab Scenario

As a professional ethical hacker or pen tester, the first step is to perform active sniffing on the target network using various active sniffing techniques such as MAC flooding, DHCP starvation, ARP poisoning, or MITM. In active sniffing, the switched Ethernet does not transmit information to all systems connected through the LAN as it does in a hub-based network.

In active sniffing, ARP traffic is actively injected into a LAN to sniff around a switched network and capture its traffic. A packet sniffer can obtain all the information visible on the network and records it for future review. A pen tester can see all the information in the packet, including data that should remain hidden.

An ethical hacker or pen tester needs to ensure that the organization's network is secure from various active sniffing attacks by analyzing incoming and outgoing packets for any attacks.

Lab Objectives

- Perform MAC flooding using macof
- Perform a DHCP starvation attack using Yersinia

Overview of Active Sniffing

Active sniffing involves sending out multiple network probes to identify access points. The following is the list of different active sniffing techniques:

- **MAC Flooding**: Involves flooding the CAM table with fake MAC address and IP pairs until it is full
- **DNS Poisoning**: Involves tricking a DNS server into believing that it has received authentic information when, in reality, it has not
- **ARP Poisoning**: Involves constructing a large number of forged ARP request and reply packets to overload a switch
- **DHCP Attacks**: Involves performing a DHCP starvation attack and a rogue DHCP server attack
- **Switch port stealing**: Involves flooding the switch with forged gratuitous ARP packets with the target MAC address as the source
- **Spoofing Attack**: Involves performing MAC spoofing, VLAN hopping, and STP attacks to steal sensitive information

Task 1: Perform MAC Flooding using macof

MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods the switch's CAM tables (131,000 per minute) by sending forged MAC entries. When the MAC table fills up, the switch converts to a hub-like operation where an attacker can monitor the data being broadcast.

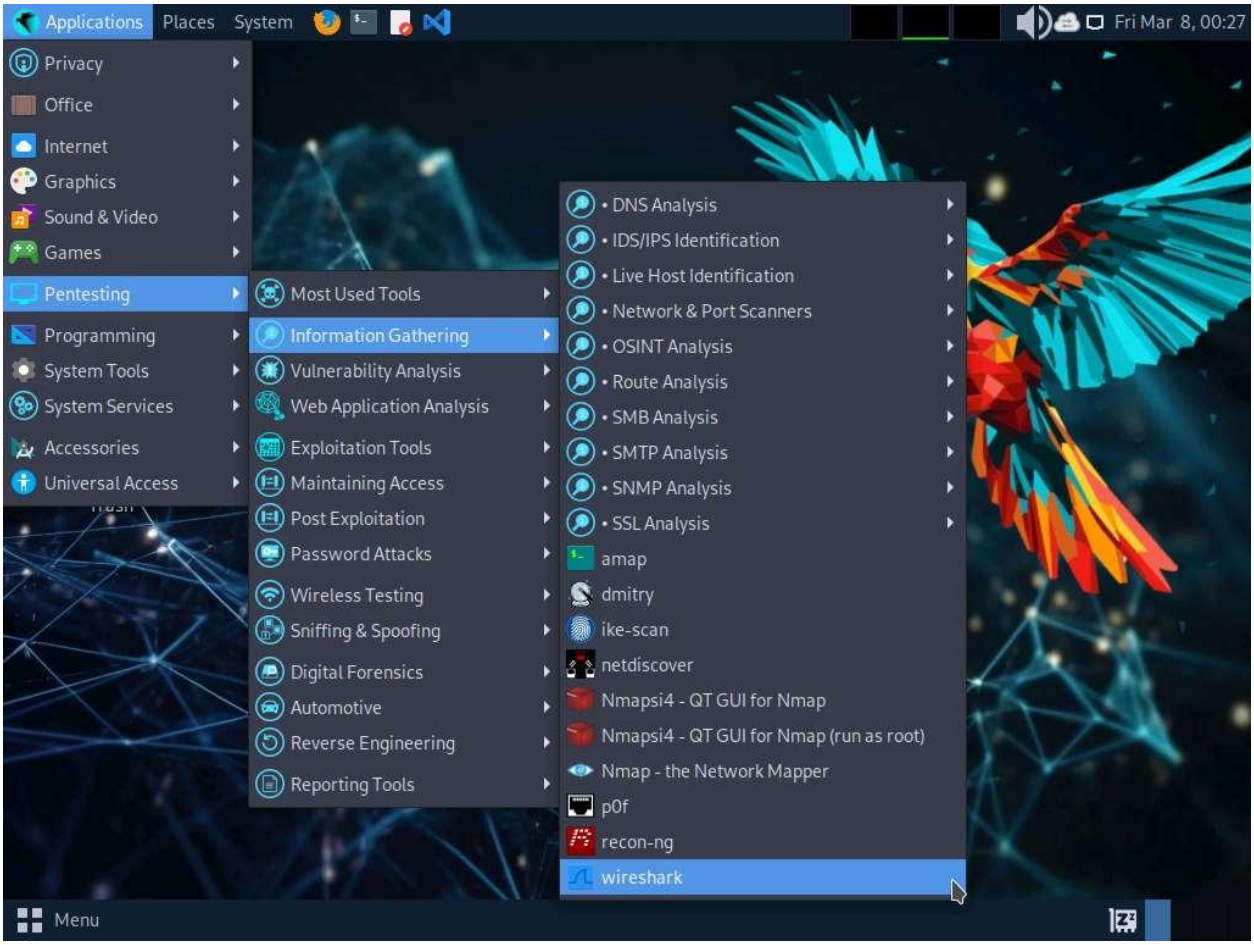
Here, we will use the macof tool to perform MAC flooding.

1. By default Windows 11 machine selected, to launch **Parrot Security** machine, click Parrot Security and login with **attacker/toor**.

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

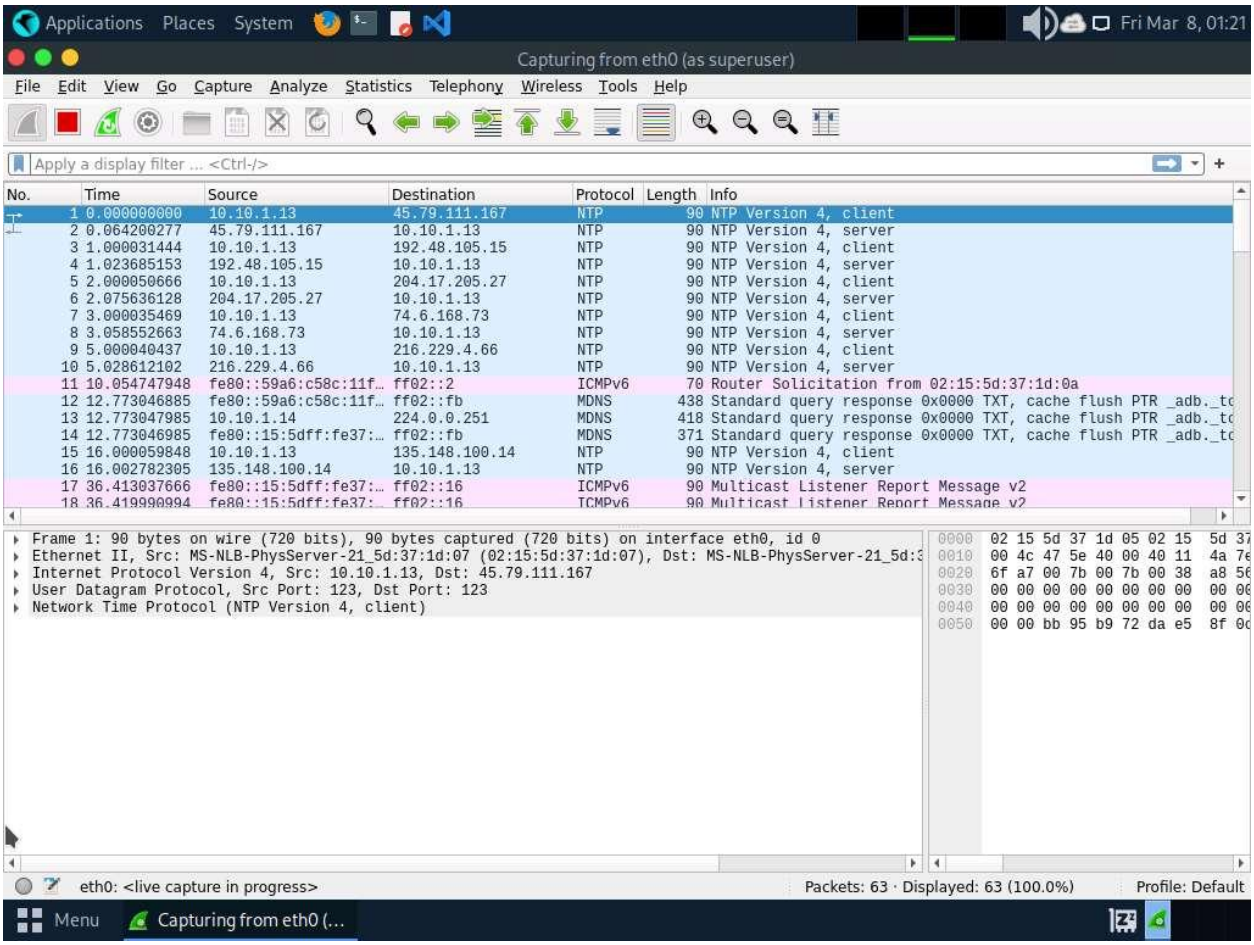
If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

2. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



3. A security pop-up appears, authenticate by providing **toor** as a password.

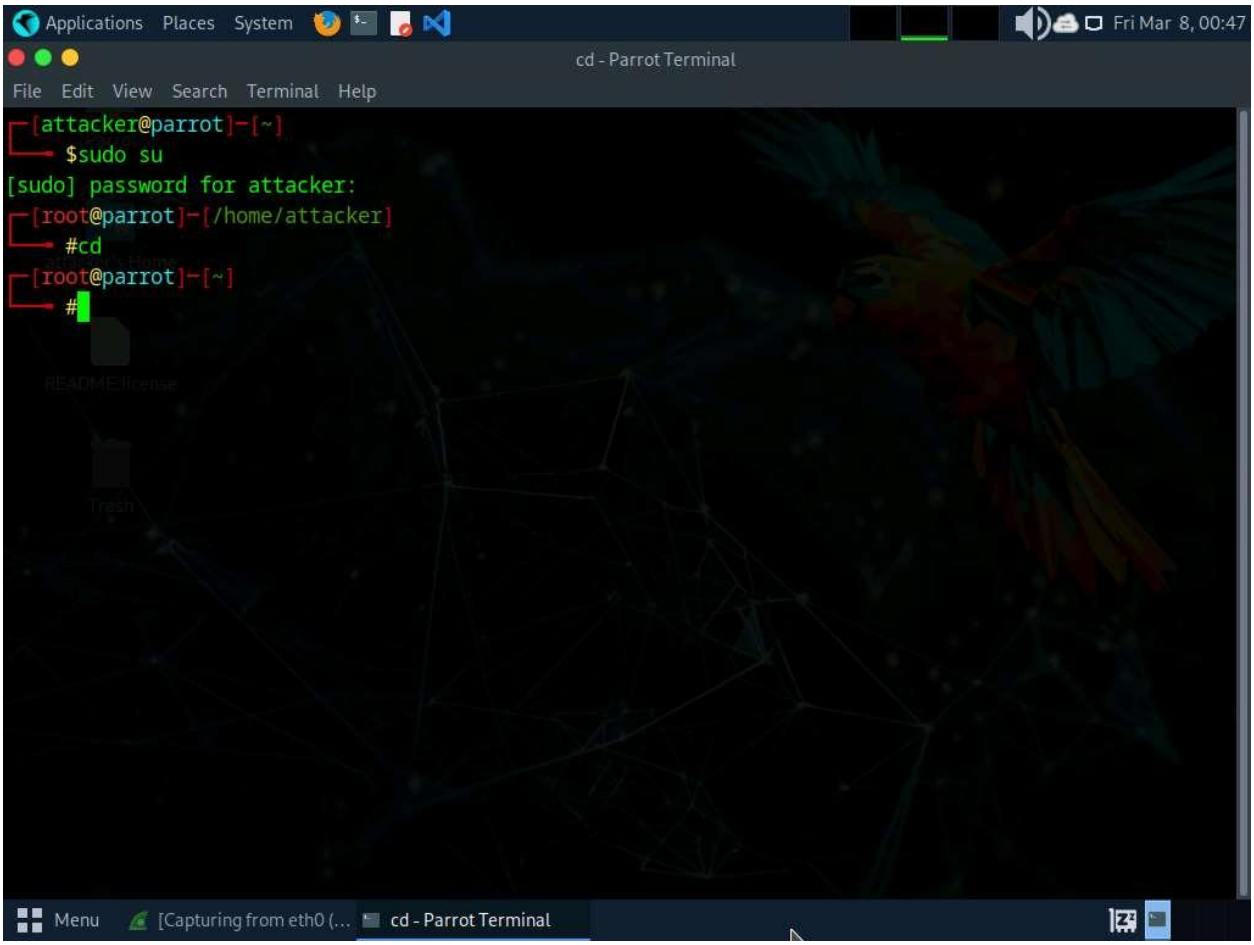
4. **Wireshark Network Analyzer** window appears, start capturing the network traffic on the primary network interface (here, **eth0**).



5. Leave the **Wireshark** application running.
6. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

7. Now, run **cd** command to jump to the root directory.

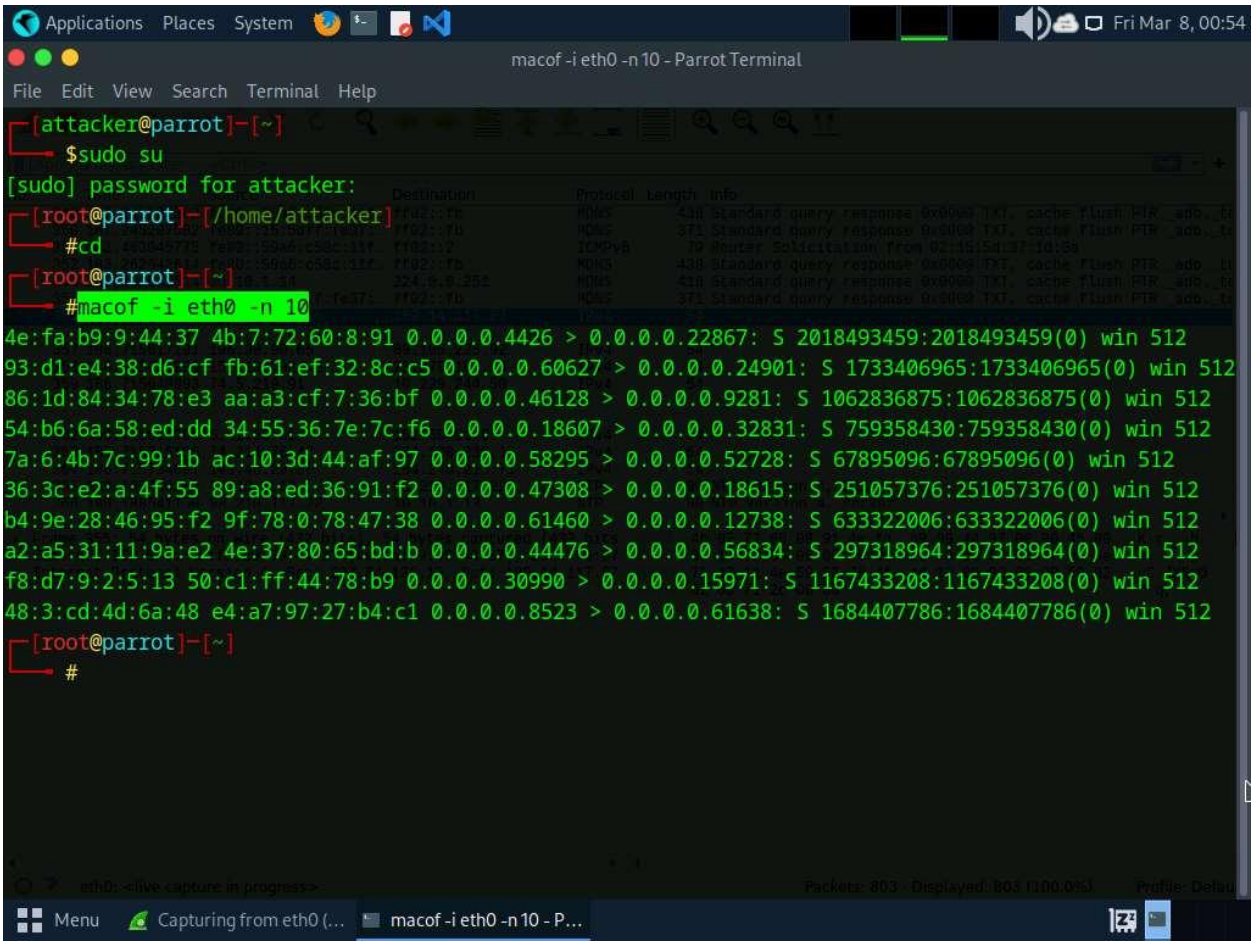


8. Execute **macof -i eth0 -n 10** in the root directory.

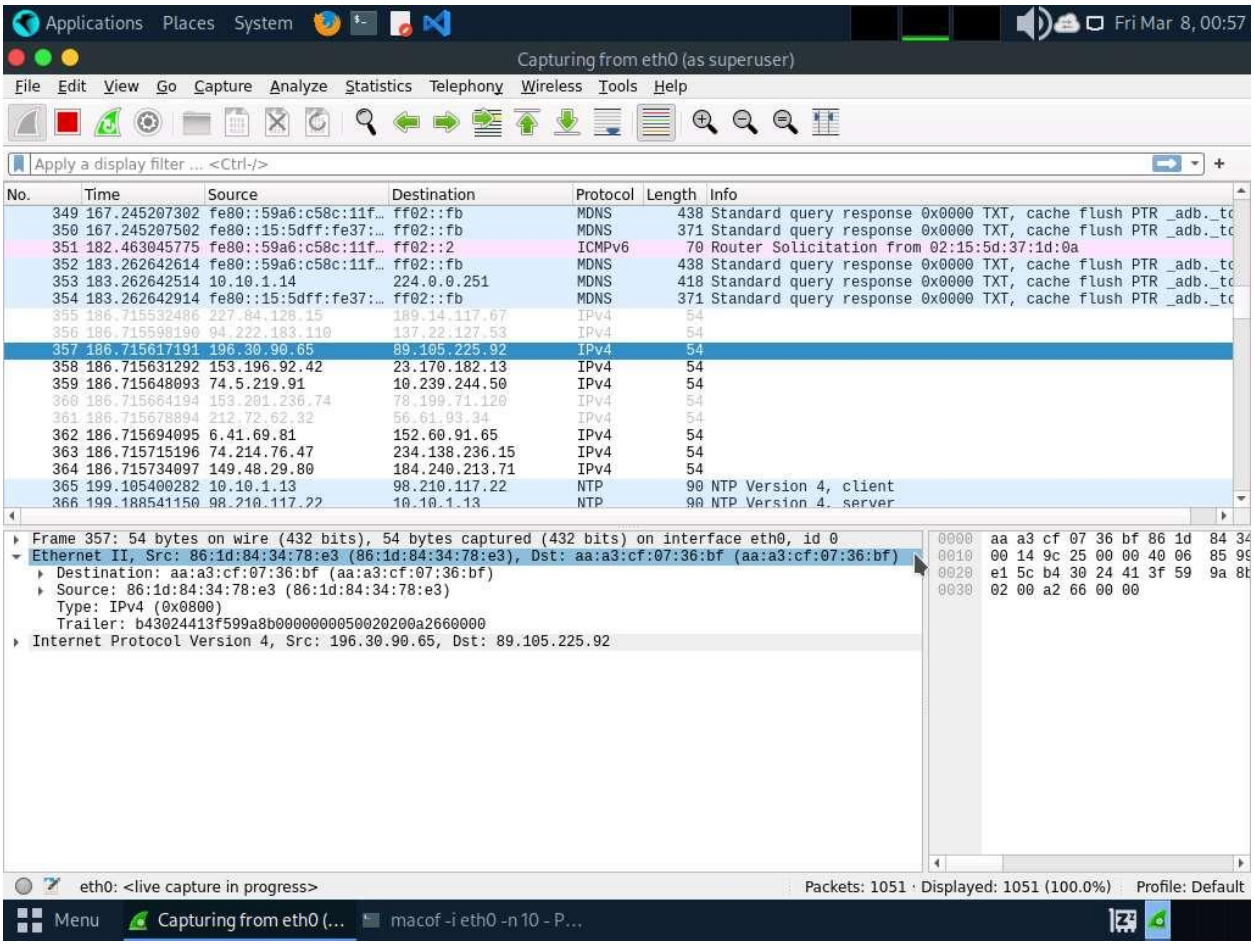
-i: specifies the interface and **-n**: specifies the number of packets to be sent (here, **10**).

You can also target a single system by issuing the command **macof -i eth0 -d [Target IP Address]** (**-d**: Specifies the destination IP address).

9. This command will start flooding the CAM table with random MAC addresses, as shown in the screenshot.



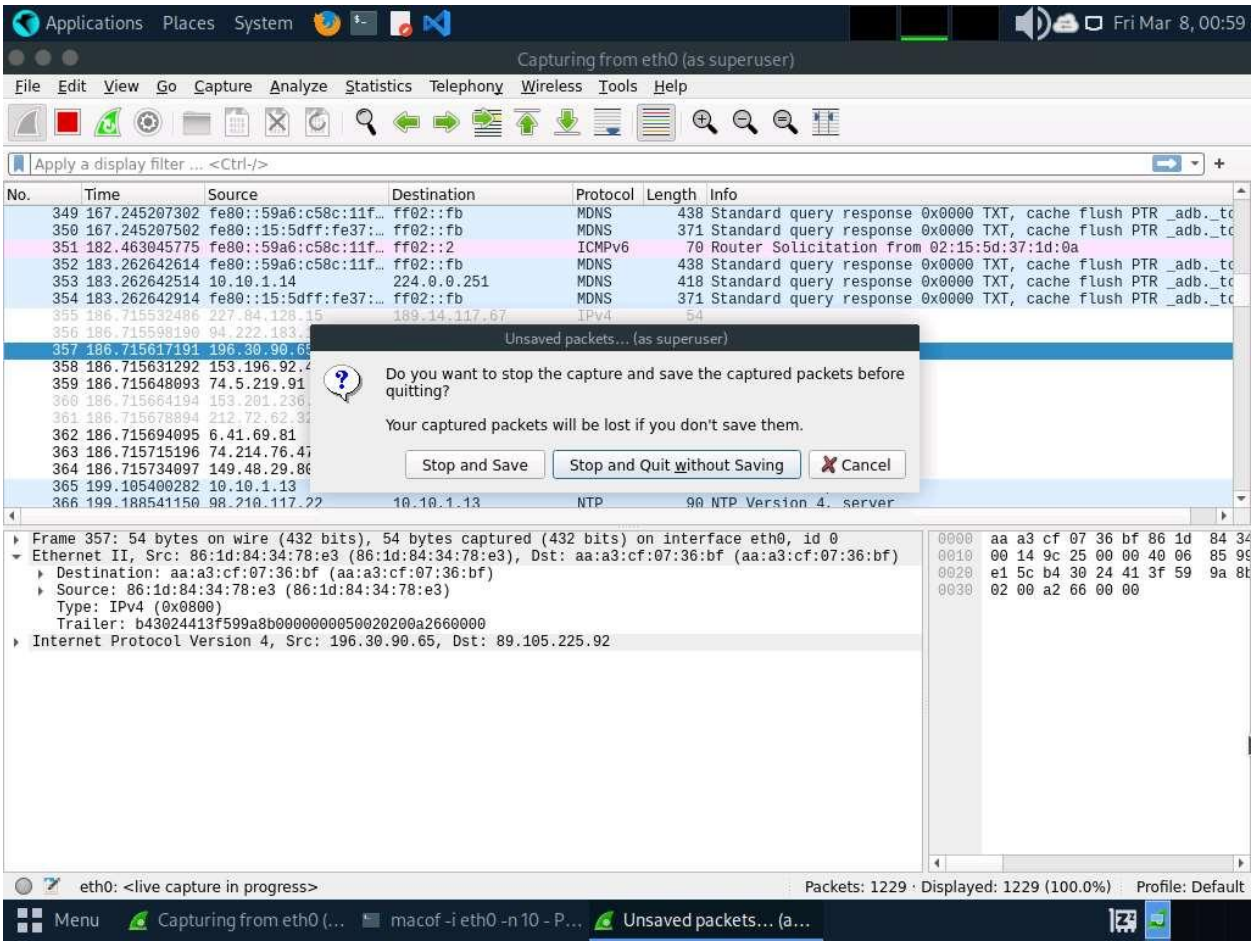
10. Switch to the **Wireshark** window and observe the **IPv4** packets from random IP addresses.
11. Click on any captured **IPv4** packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.



12. Similarly, you can switch to a different machine to see the same packets that were captured by Wireshark in the **Parrot Security** machine.

13. Macof sends the packets with random MAC and IP addresses to all active machines in the local network. If you are using multiple targets, you will observe the same packets on all target machines.

14. Close the **Wireshark** window. If an **Unsaved packets**… pop-up appears, click **Stop and Quit without Saving** to close the Wireshark application.



15. This concludes the demonstration of how to perform MAC flooding using macof.
16. Close all open windows and document all the acquired information.

Question 8.1.1.1

Use macof on the Parrot Security machine to perform MAC flooding on the Windows 11 target machine. What is the default size of the IP packets that macof uses to flood the CAM table with random MAC addresses?

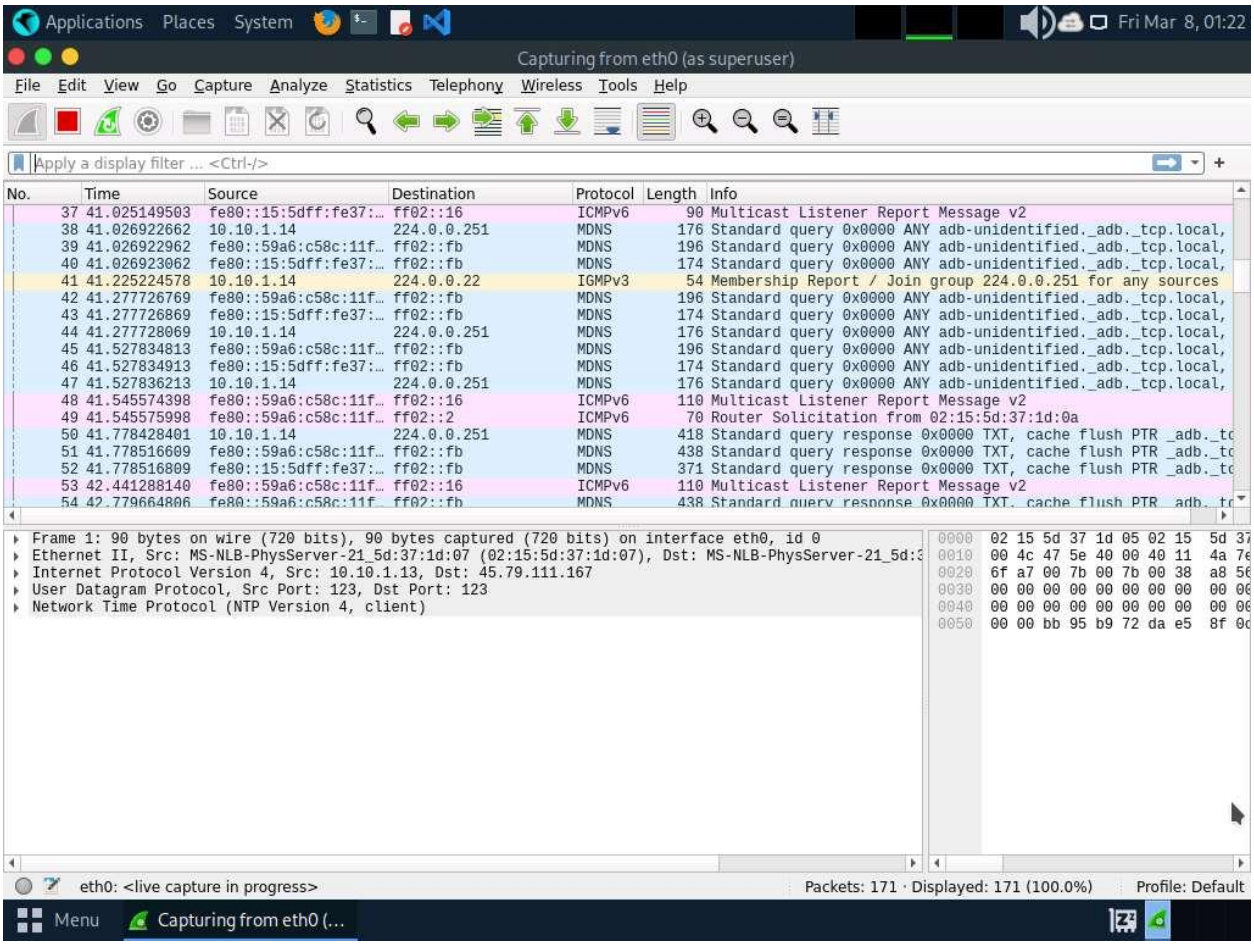
Task 2: Perform a DHCP Starvation Attack using Yersinia

In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a Denial-of-Service (DoS) attack. Because of this issue, valid users cannot obtain or renew their IP addresses, and thus fail to access their network. This attack can be performed by using various tools such as Yersinia and Hyenae.

Yersinia is a network tool designed to take advantage of weaknesses in different network protocols such as DHCP. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

Here, we will use the Yersinia tool to perform a DHCP starvation attack on the target system.

1. In **Parrot Security** machine, launch **Wireshark** and start packet capturing on available ethernet or interface (here,**eth0**).



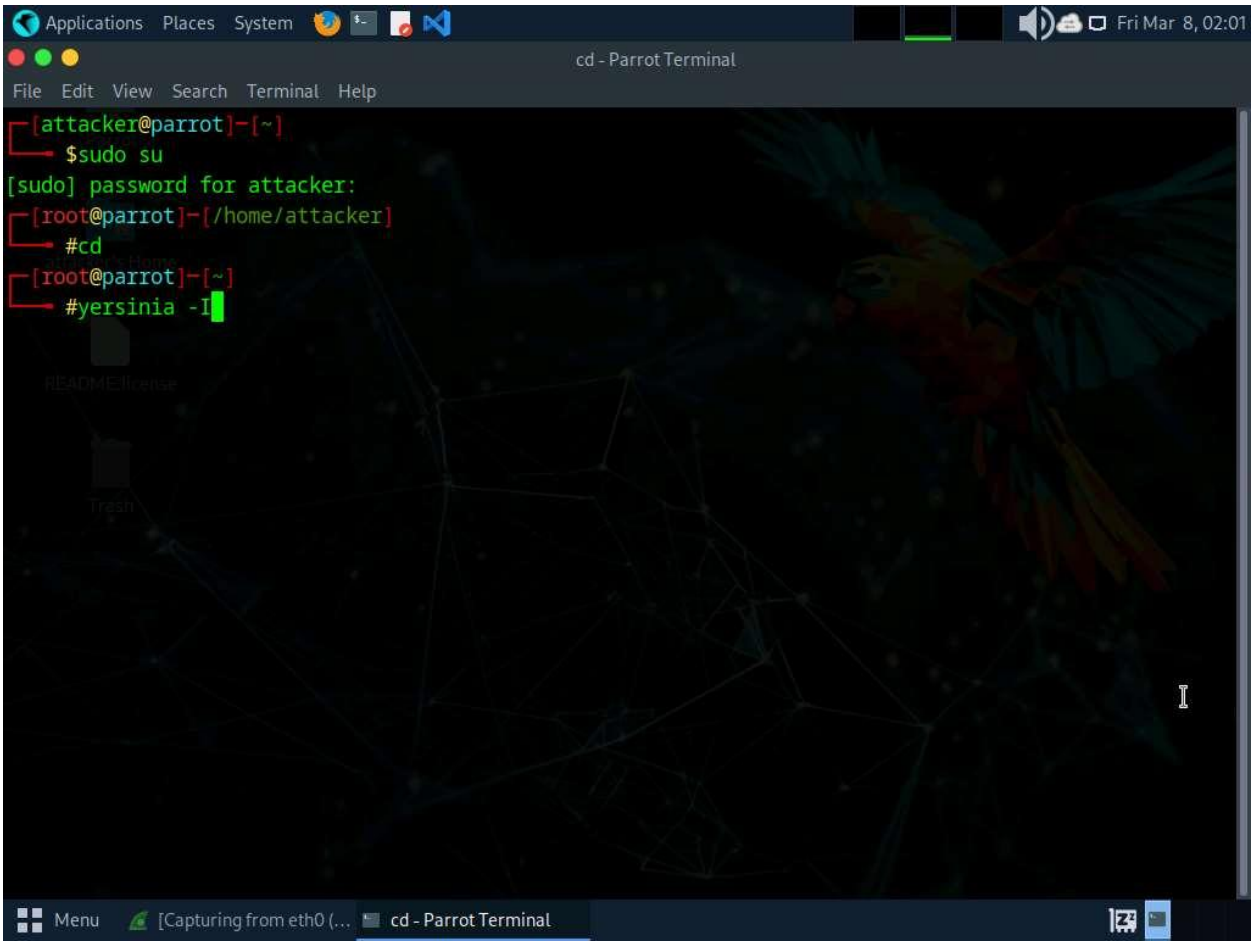
2. Leave the **Wireshark** application running.
3. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**). Run **cd** to navigate to the root directory.

Click the **Maximize Window** icon to maximize the terminal window.

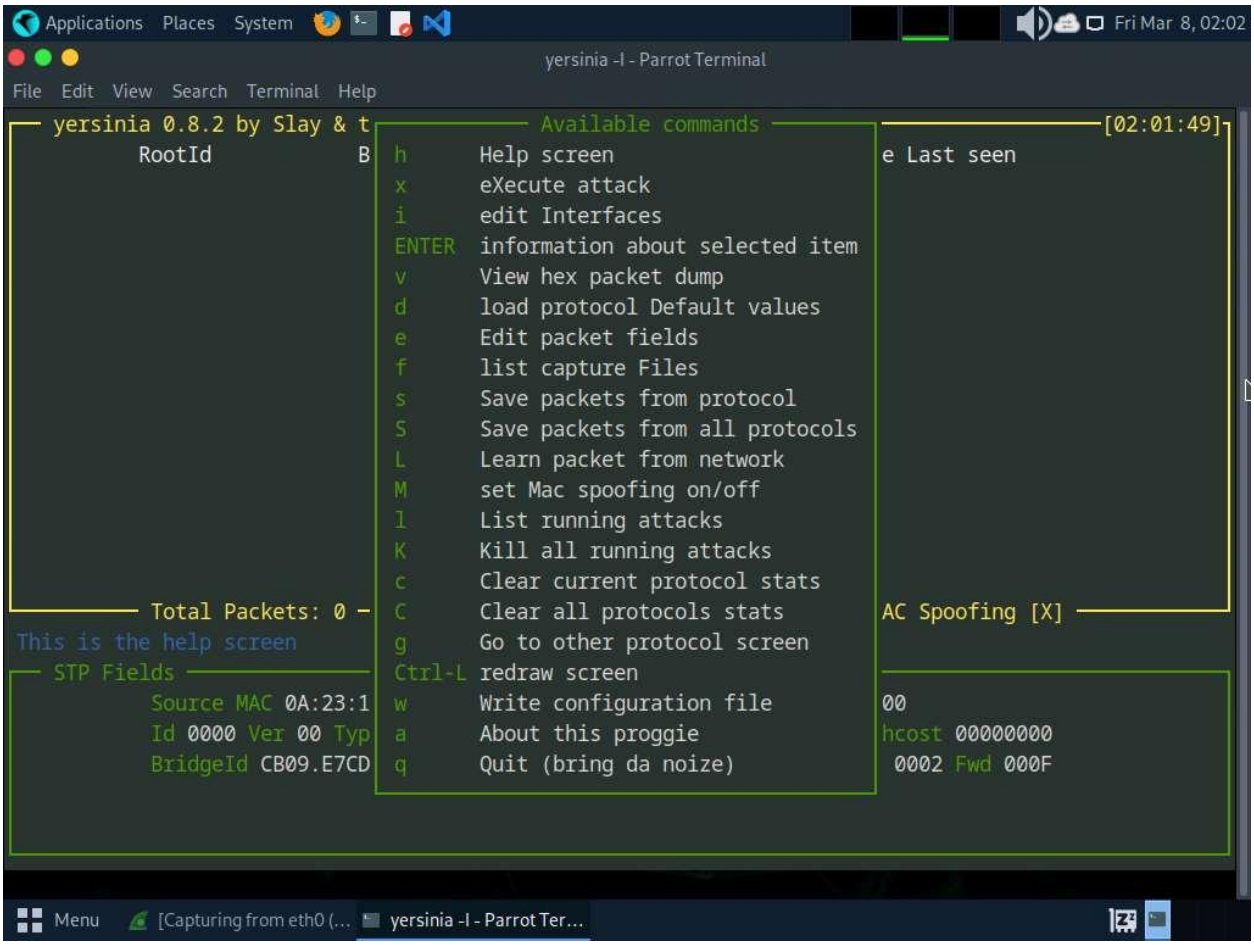
The interactive mode of the Yersinia application only works in a maximized terminal window.

4. Run **yersinia -I** to open Yersinia in interactive mode.

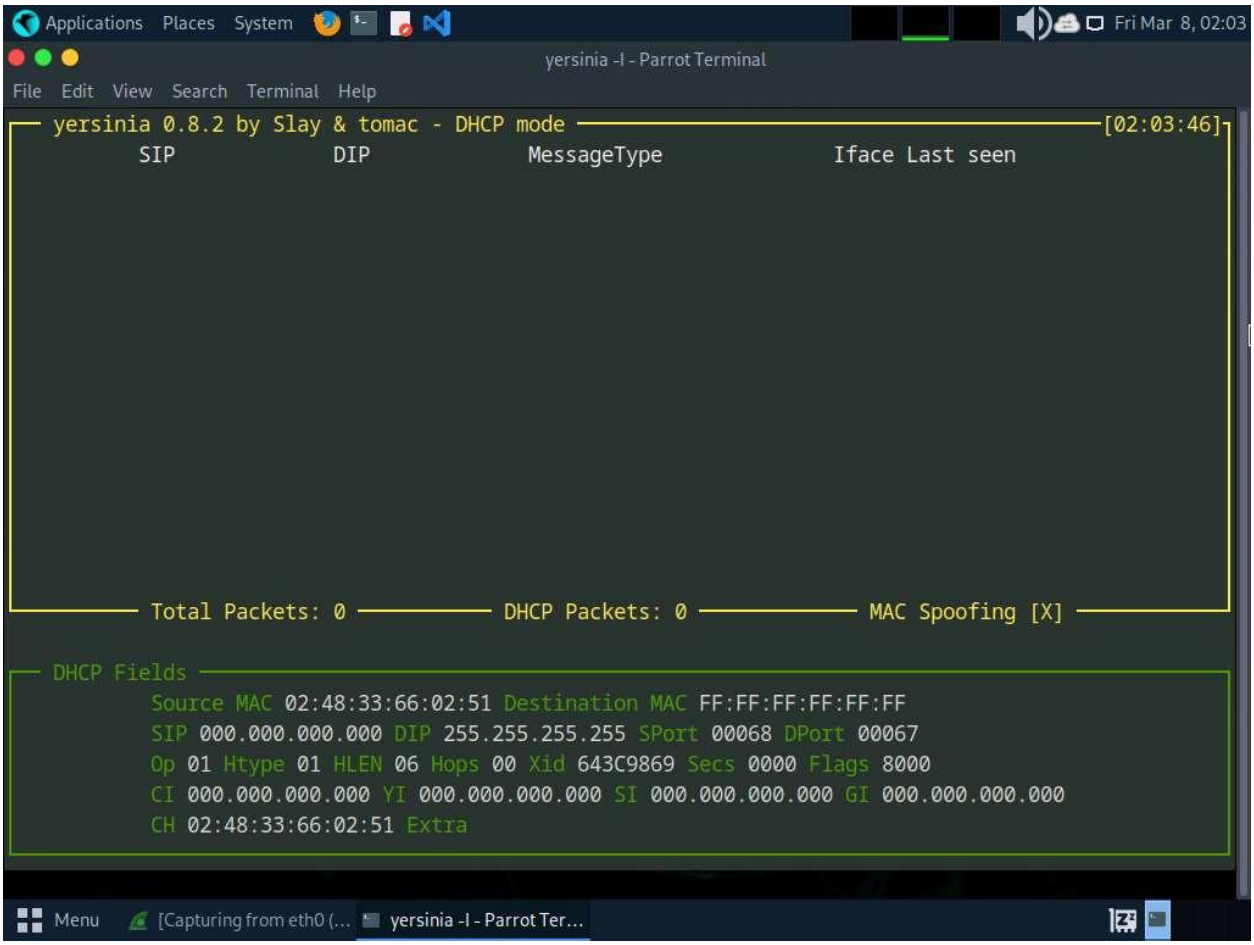
-I: Starts an interactive session.



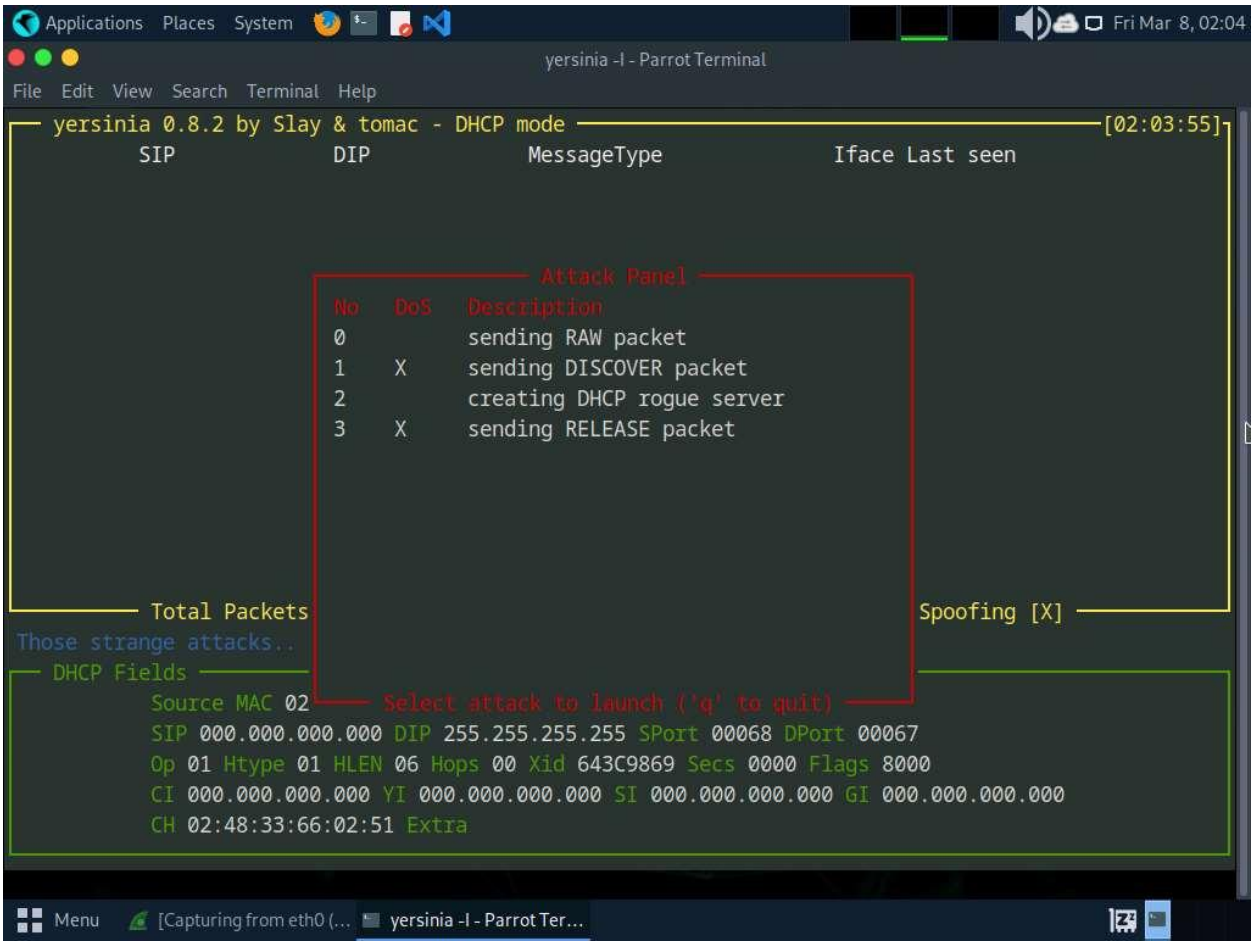
5. Yersinia interactive mode appears in the terminal window.
6. To remove the **Notification window**, press any key, and then press **h** for help.
7. The **Available commands** option appears, as shown in the screenshot.



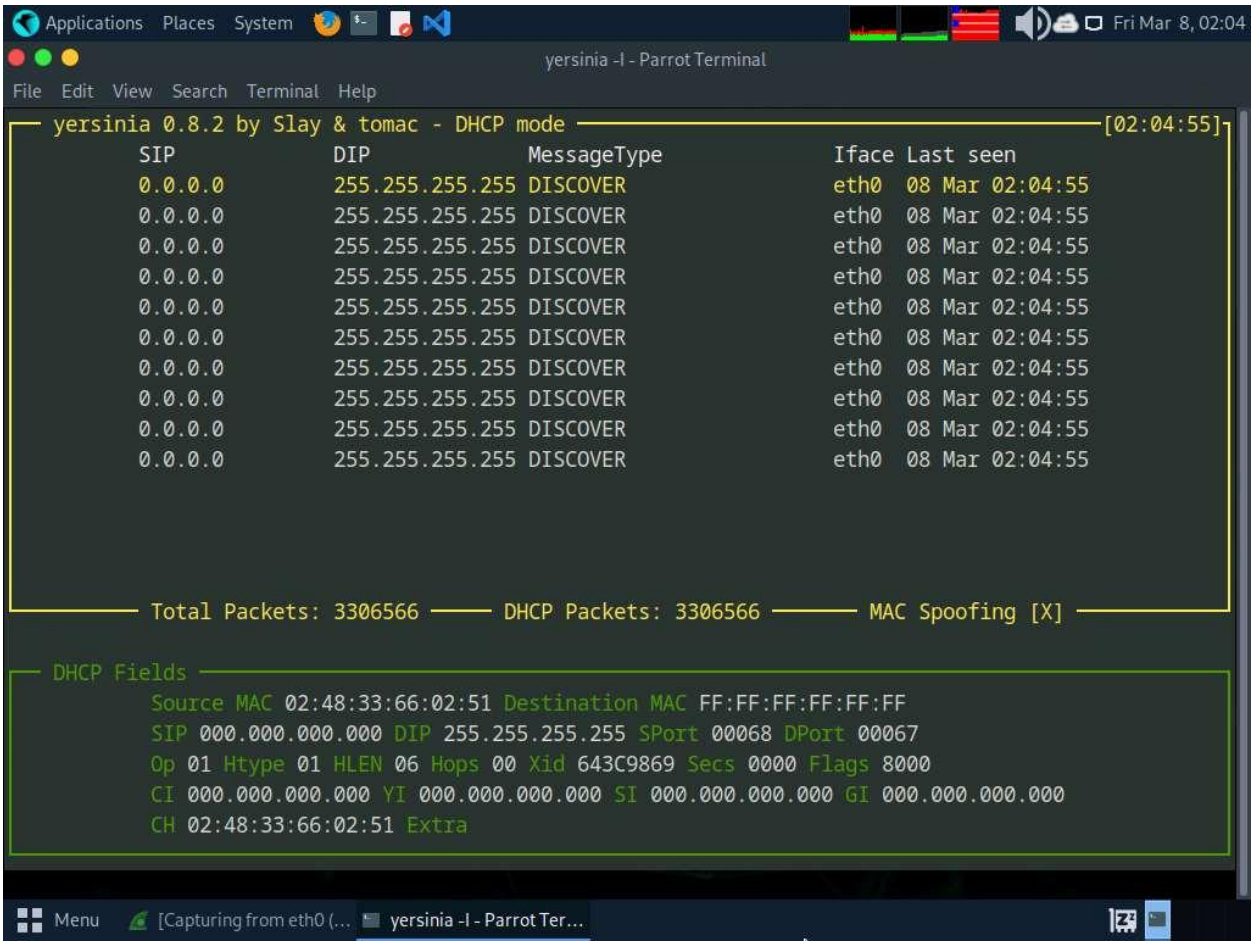
8. Press **q** to exit the help options.
9. Press **F2** to select DHCP mode. In DHCP mode, **STP Fields** in the lower section of the window change to **DHCP Fields**, as shown in the screenshot.



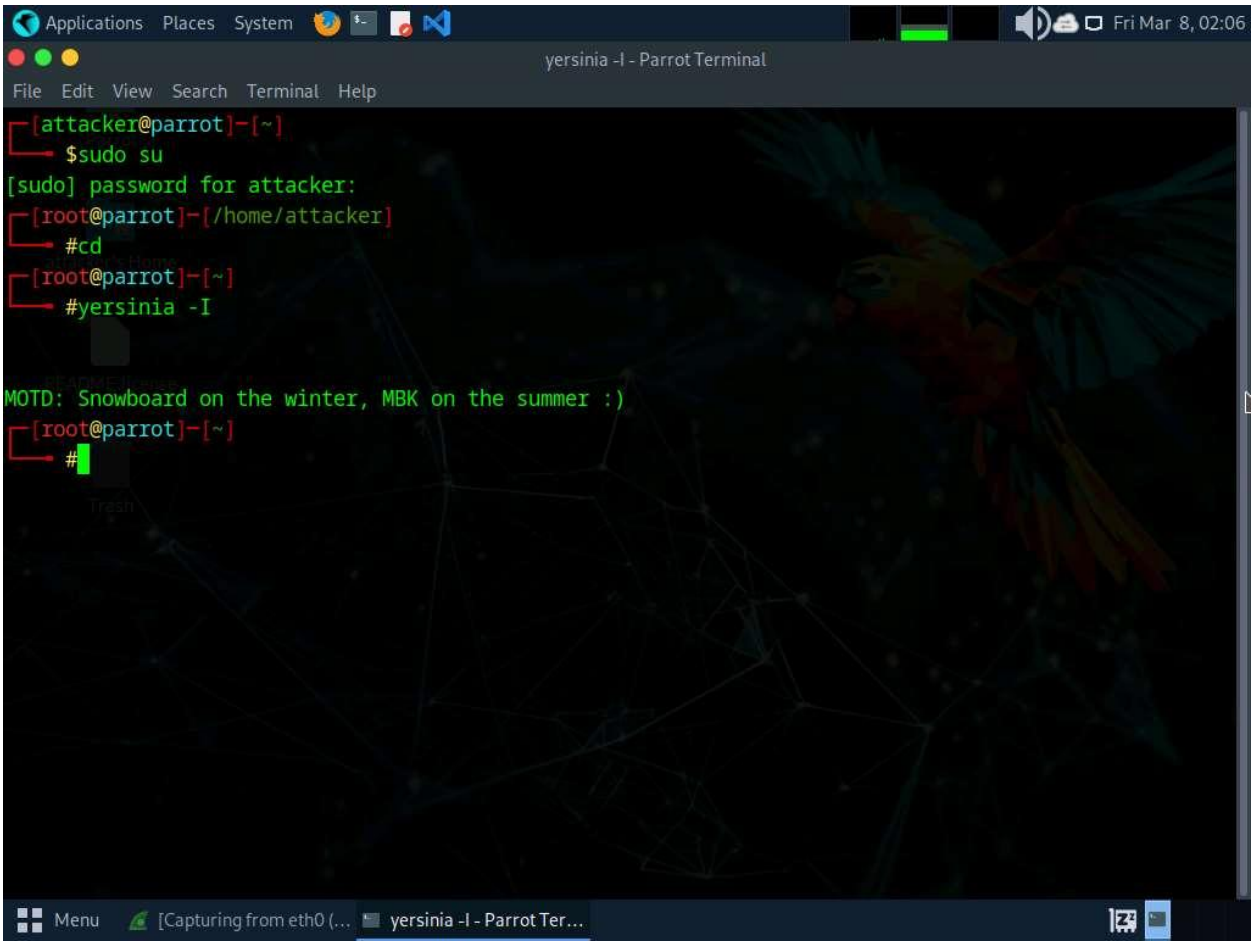
10. Press **x** to list available attack options.
11. The **Attack Panel** window appears; press **1** to start a DHCP starvation attack.



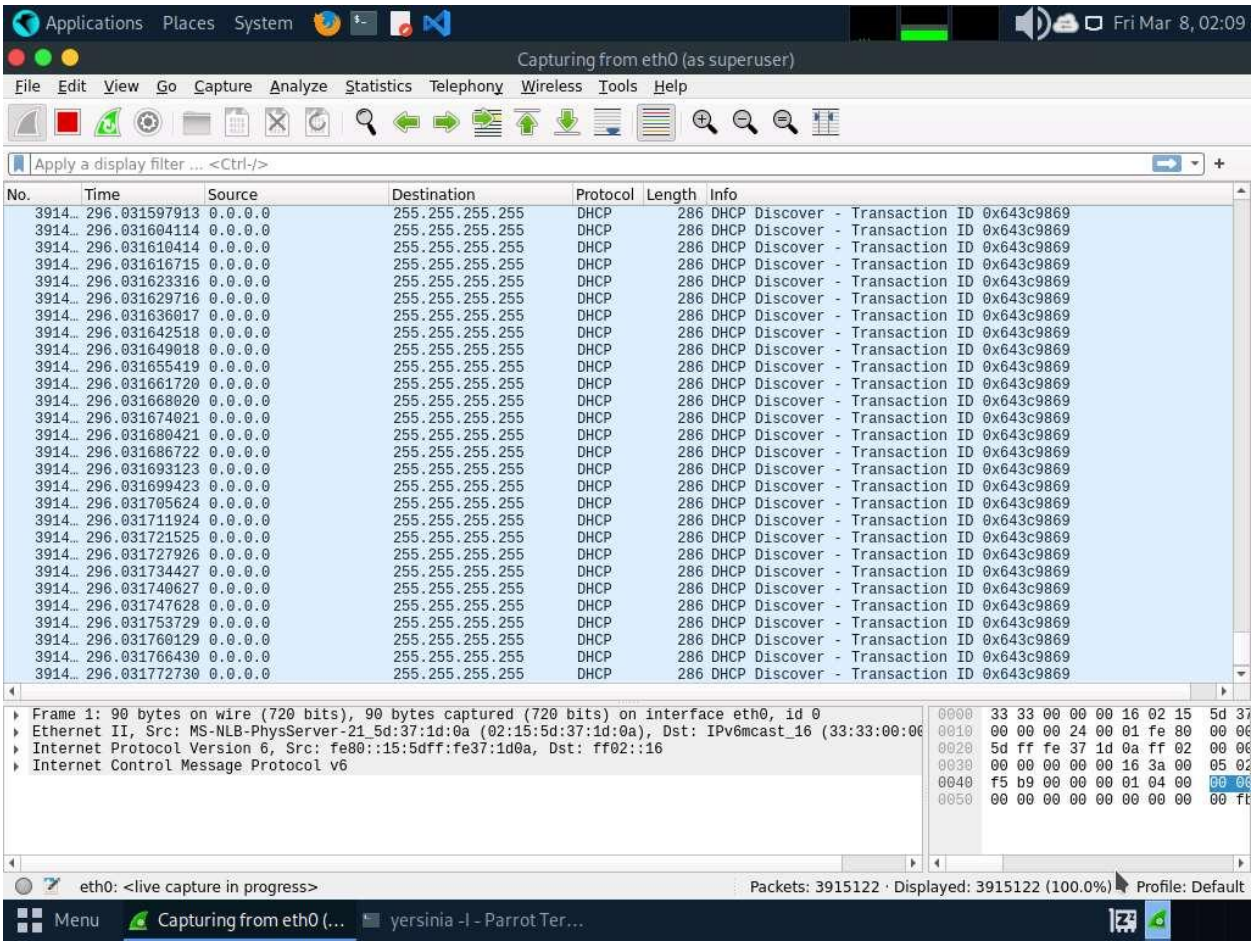
12. **Yersinia** starts sending DHCP packets to the network interface as shown in the screenshot.



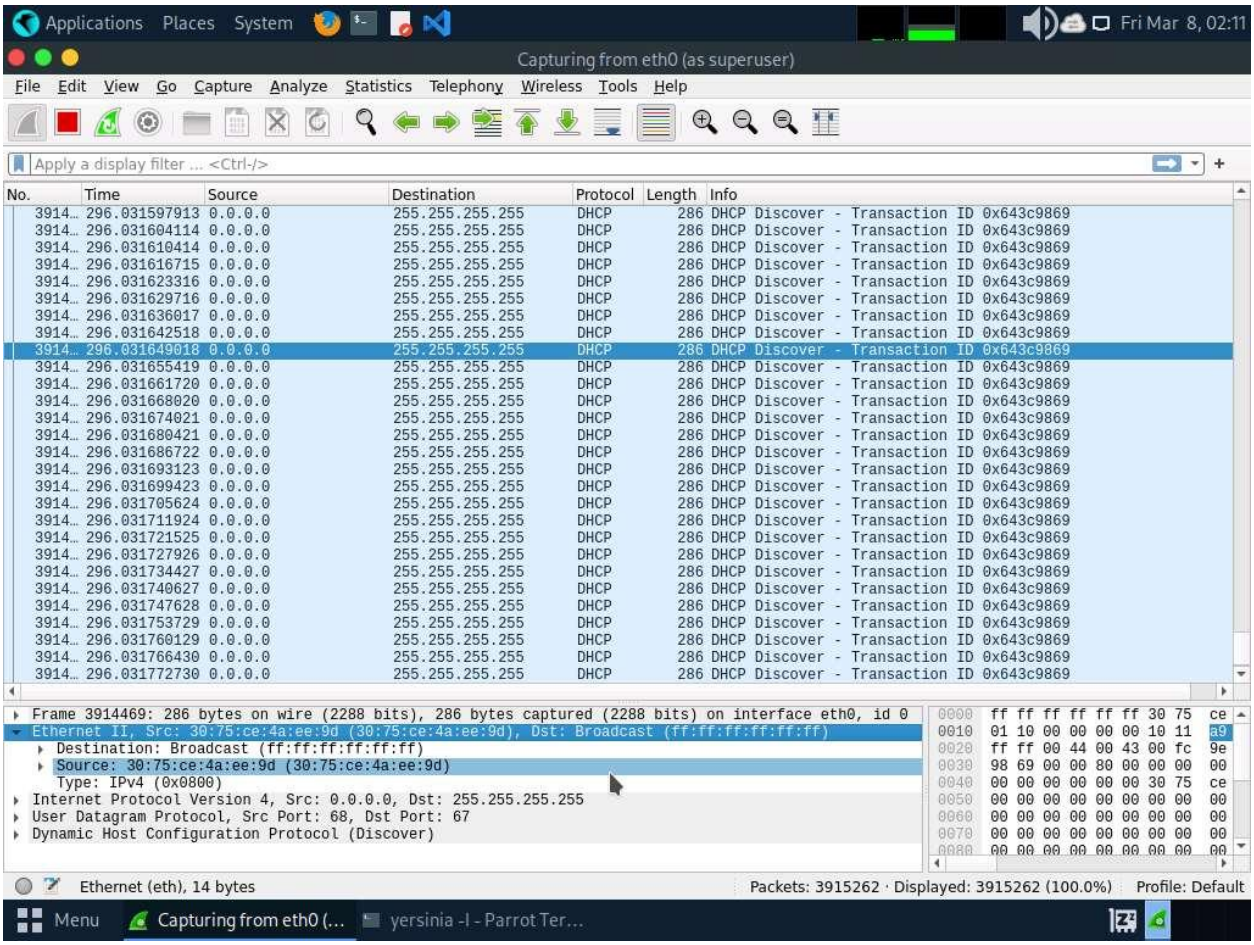
13. After a few seconds, press **q** to stop the attack and terminate Yersinia, as shown in the screenshot.



14. Now, switch to the **Wireshark** window and observe the huge number of captured **DHCP** packets, as shown in the screenshot.



15. Click on any DHCP packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.



16. Close the **Wireshark** window. If an **Unsaved packets…** pop-up appears, click **Stop and Quit without Saving**.
17. This concludes the demonstration of how to perform a DHCP starvation attack using Yersinia.
18. Close all open windows and document all the acquired information.

Question 8.1.2.1

Use Yersinia on the Parrot Security machine to perform a DHCP starvation attack. What is the default source port used by Yersinia in the DHCP mode?