

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.

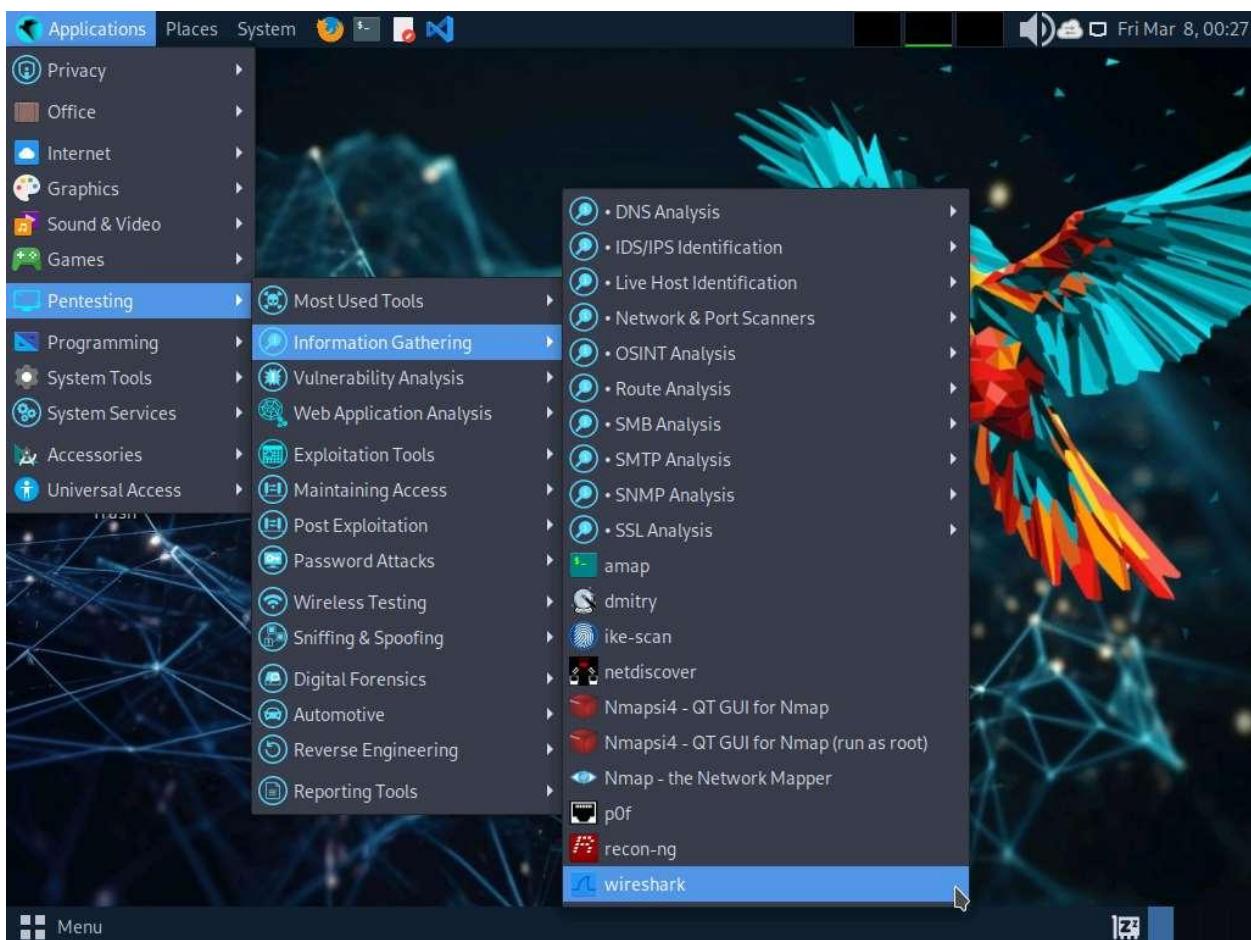
Here, we will use the macof tool to perform MAC flooding.

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

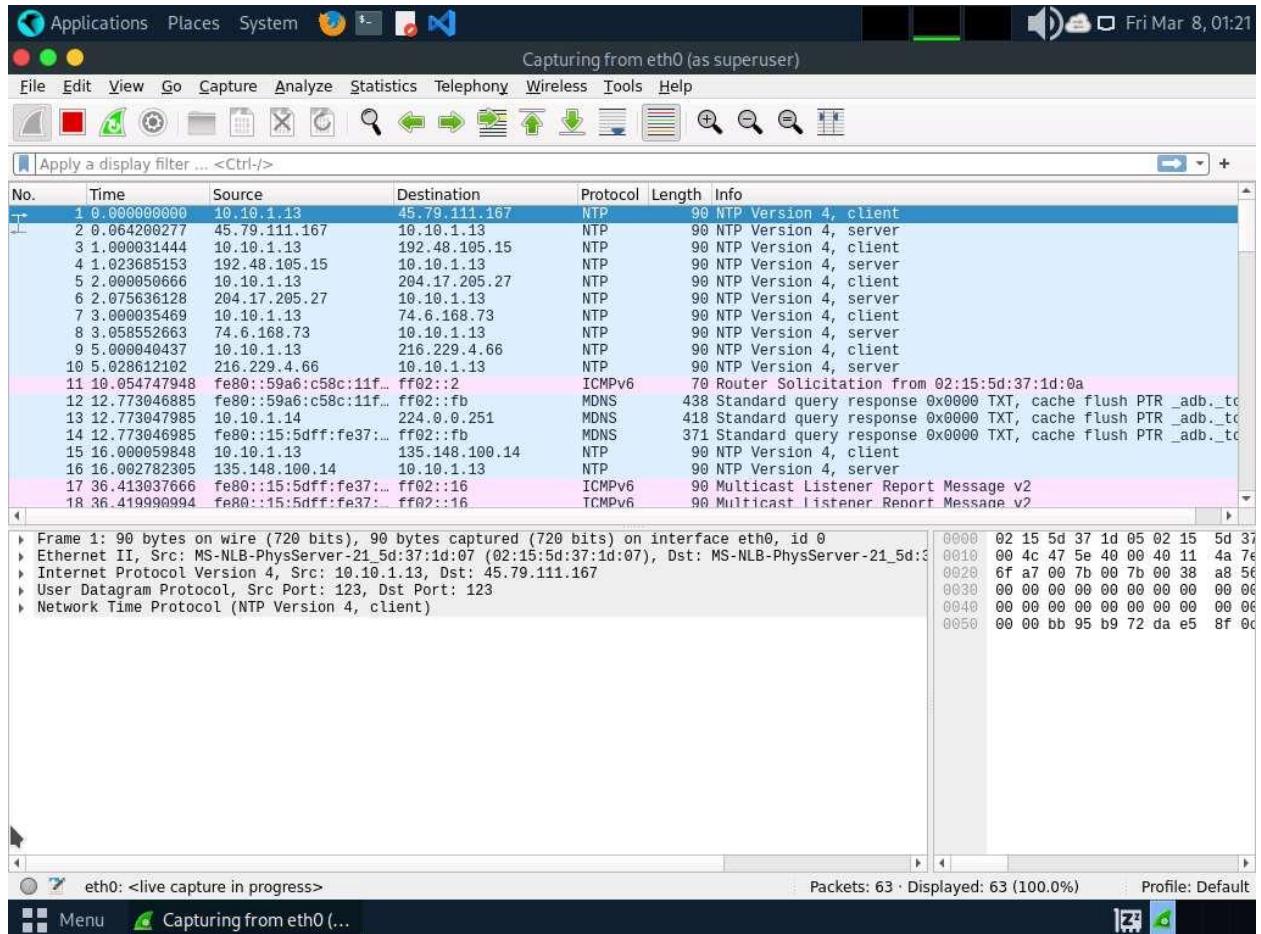
If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

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.

The screenshot shows a Parrot OS desktop environment. In the foreground, a terminal window titled "cd - Parrot Terminal" is open, displaying the following command sequence:

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
#cd
[root@parrot] ~
#
```

The desktop background features a dark, abstract network graph. The taskbar at the bottom shows the "cd - Parrot Terminal" window is active. Other icons include "Menu", "[Capturing from eth0 ...]", and a system status icon.

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**).

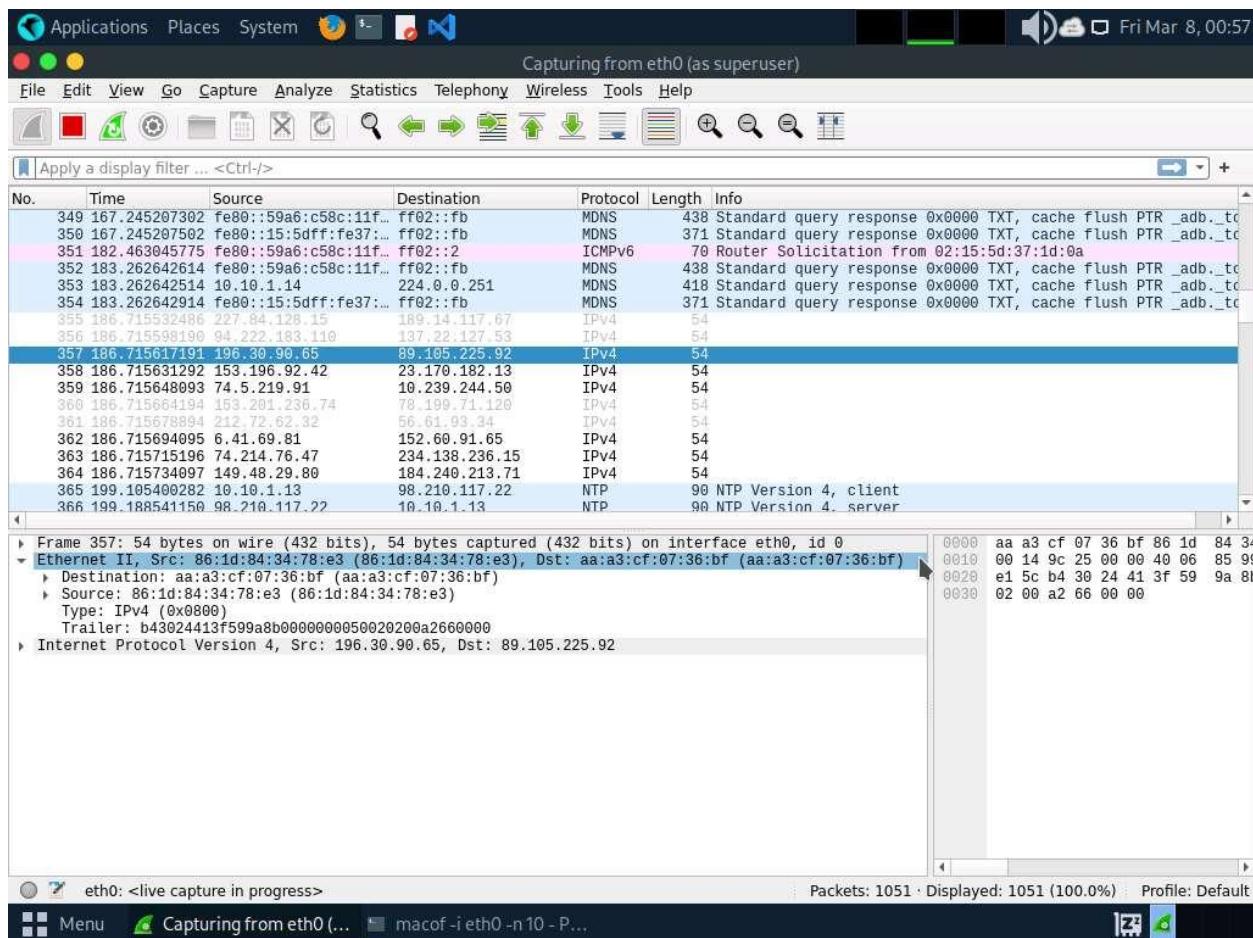
You can also target a single system by issuing the command **macof -i eth0 -d [Target IP Address]** (**-d:** Specifies the destination IP address).

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

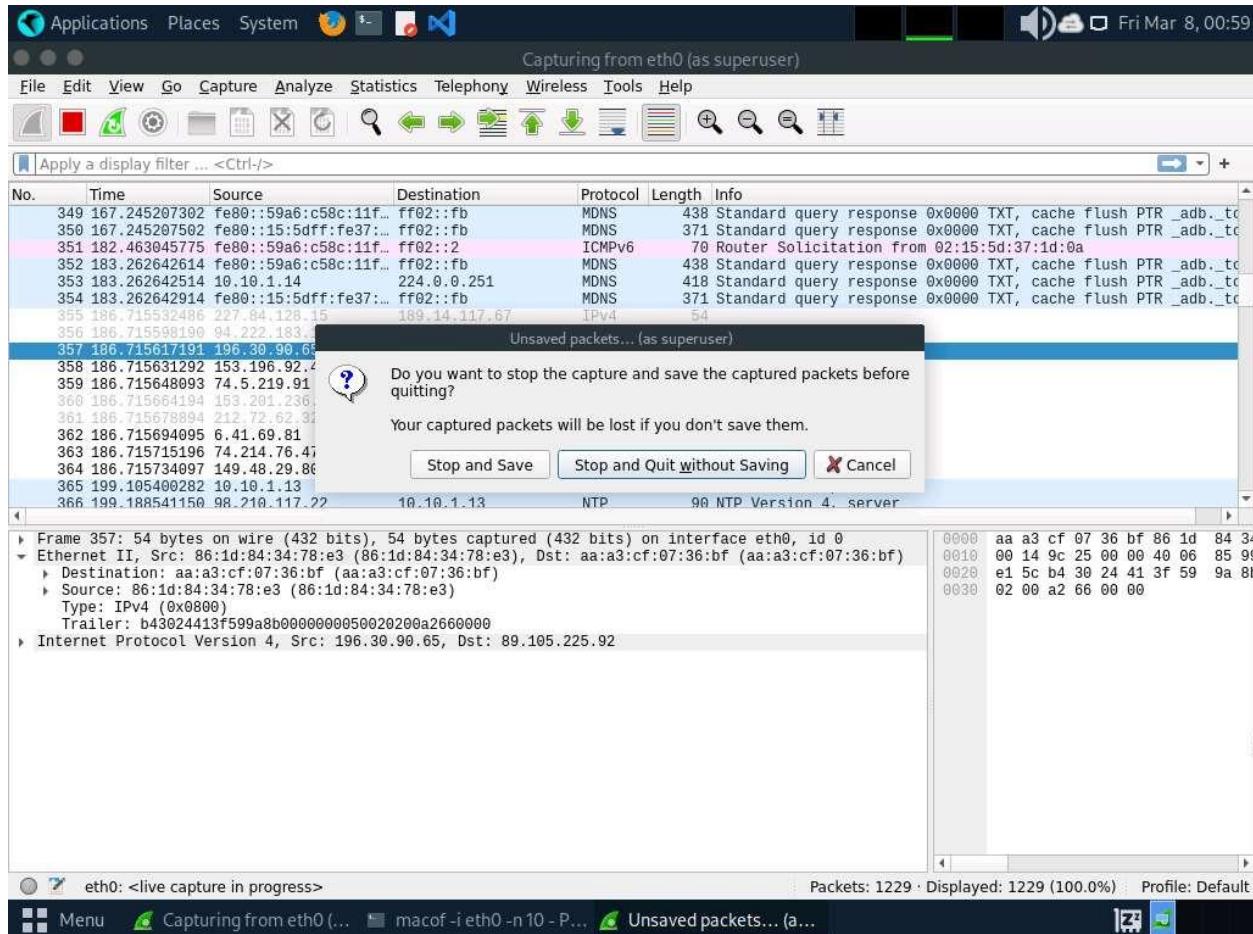
```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]$ cd
[root@parrot]~$ ./macof -i eth0 -n 10
4e:fa:b9:9:44:37 4b:7:72:60:8:91 0.0.0.0.4426 > 0.0.0.0.22867: S 2018493459:2018493459(0) win 512
93:d1:e4:38:d6:cf fb:61:ef:32:8c:c5 0.0.0.0.60627 > 0.0.0.0.24901: S 1733406965:1733406965(0) win 512
86:1d:84:34:78:e3 aa:a3:cf:7:36:bf 0.0.0.0.46128 > 0.0.0.0.9281: S 1062836875:1062836875(0) win 512
54:b6:6a:58:ed:dd 34:55:36:7e:7c:f6 0.0.0.0.18607 > 0.0.0.0.32831: S 759358430:759358430(0) win 512
7a:6:4b:7c:99:1b ac:10:3d:44:af:97 0.0.0.0.58295 > 0.0.0.0.52728: S 67895096:67895096(0) win 512
36:3c:e2:a:4f:55 89:a8:ed:36:91:f2 0.0.0.0.47308 > 0.0.0.0.18615: S 251057376:251057376(0) win 512
b4:9e:28:46:95:f2 9f:78:0:78:47:38 0.0.0.0.61460 > 0.0.0.0.12738: S 633322006:633322006(0) win 512
a2:a5:31:11:9a:e2 4e:37:80:65:bd:b 0.0.0.0.44476 > 0.0.0.0.56834: S 297318964:297318964(0) win 512
f8:d7:9:2:5:13 50:c1:ff:44:78:b9 0.0.0.0.30990 > 0.0.0.0.15971: S 1167433208:1167433208(0) win 512
48:3:cd:4d:6a:48 e4:a7:97:27:b4:c1 0.0.0.0.8523 > 0.0.0.0.61638: S 1684407786:1684407786(0) win 512
[root@parrot]~#
```

eth0: <live capture in progress> Packets: 803 Displayed: 803 (100.0%) Profile: Default
Menu Capturing from eth0 ... macof -i eth0 -n10 - P...

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?

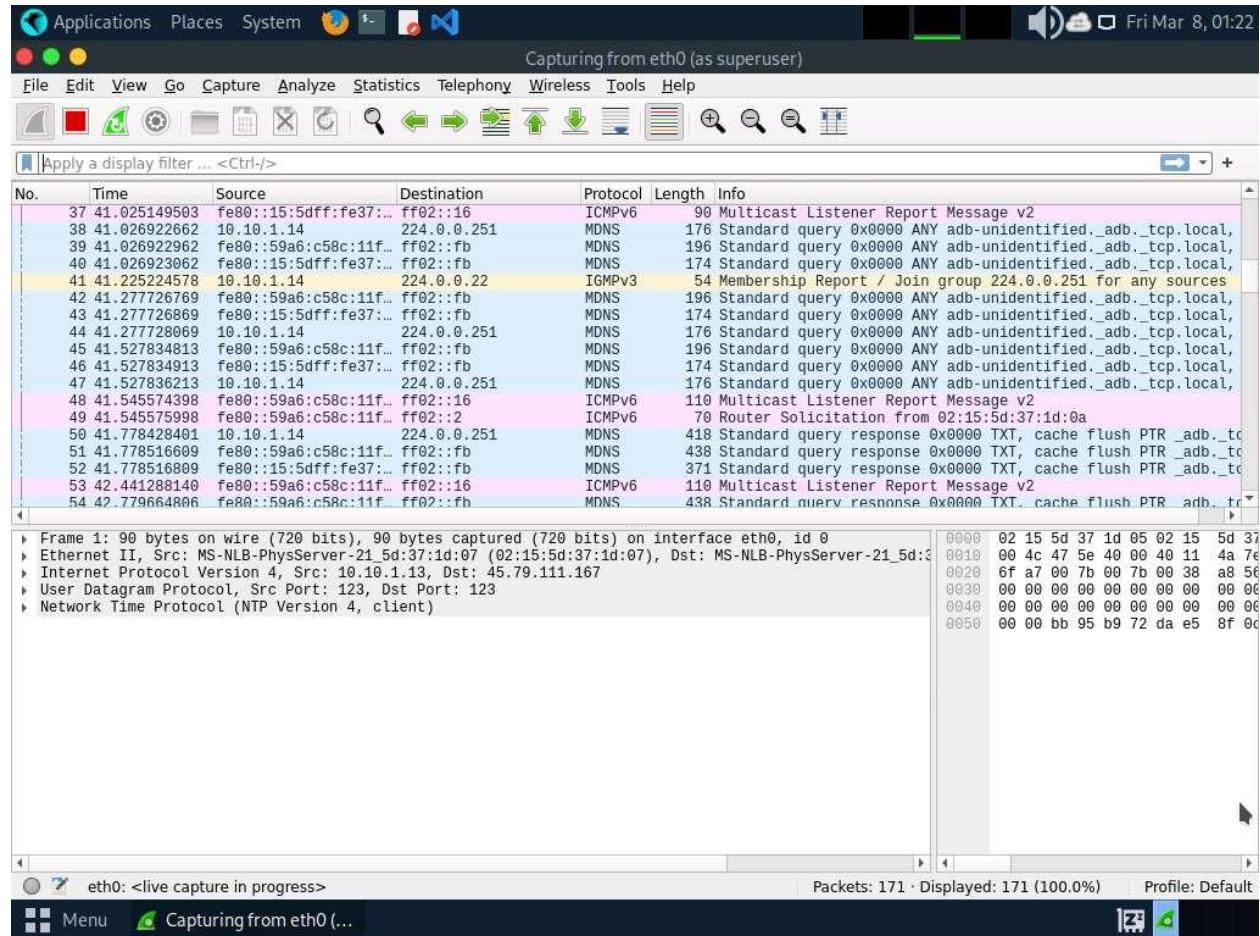
Task 2: Perform a DHCP Starvation Attack using Yersinia

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 Hyena.

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**).



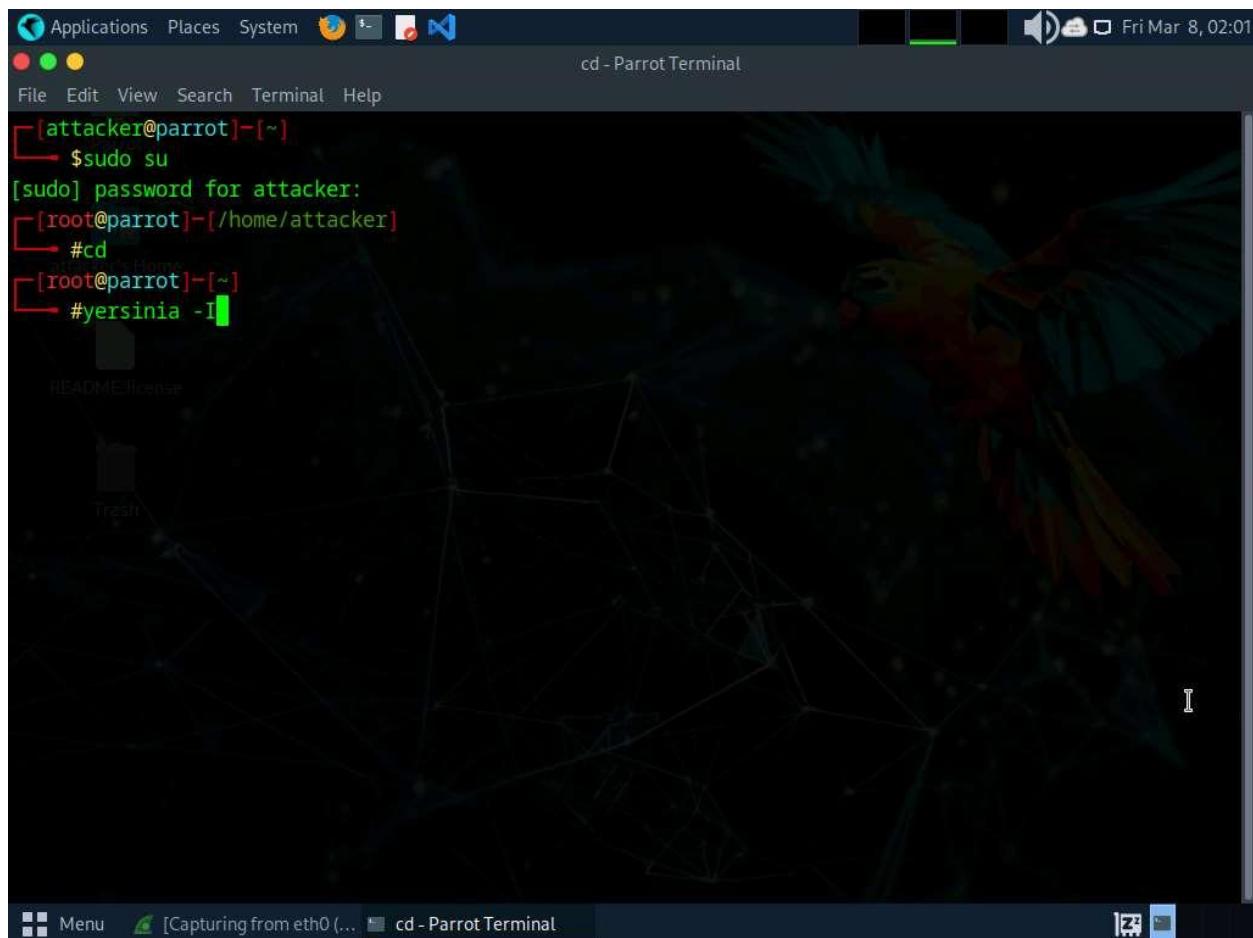
2. Leave the **Wireshark** application running.
3. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**). Run **cd** to navigate to the root directory.

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.

The screenshot shows a terminal window titled "yersinia -l - Parrot Terminal". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The main area displays the yersinia 0.8.2 help screen. At the top left, it says "yersinia 0.8.2 by Slay & t" and "RootId". A large box on the right lists "Available commands" with various options like "Help screen", "eXecute attack", and "Quit (bring da noize)". On the left, there's a section for "STP Fields" showing "Source MAC 0A:23:1", "Id 0000 Ver 00 Typ", and "BridgeId CB09.E7CD". The bottom right shows "AC Spoofing [X]" and some configuration values: "00", "hcost 00000000", and "0002 Fwd 000F". The status bar at the bottom shows "Menu", "[Capturing from eth0 (...]", "yersinia -l - Parrot Ter...", and icons for signal strength and battery.

```
yersinia 0.8.2 by Slay & t
RootId
Available commands
[02:01:49]
e Last seen

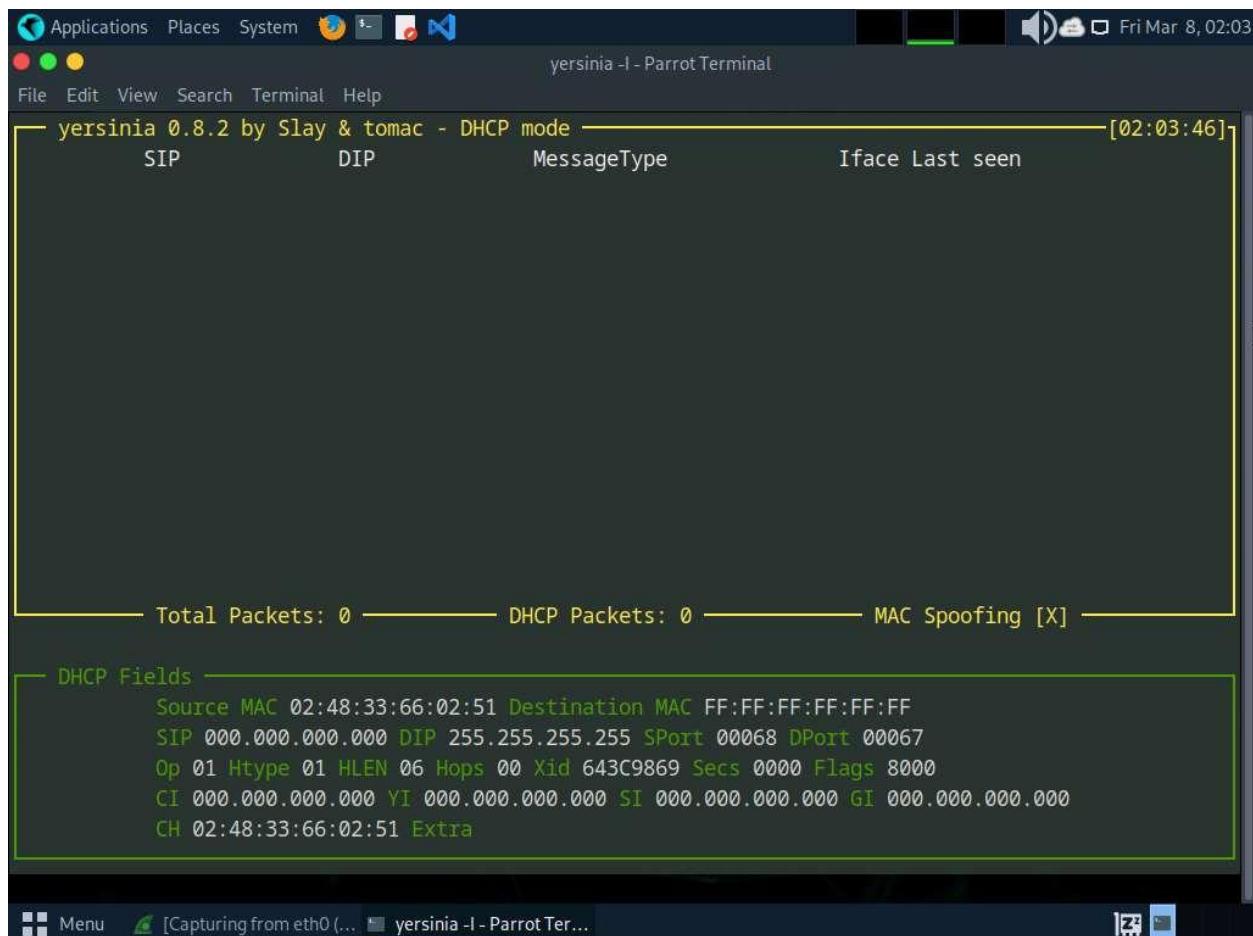
h Help screen
x eXecute attack
i edit Interfaces
ENTER information about selected item
v View hex packet dump
d load protocol Default values
e Edit packet fields
f list capture Files
s Save packets from protocol
S Save packets from all protocols
L Learn packet from network
M set Mac spoofing on/off
l List running attacks
K Kill all running attacks
c Clear current protocol stats
C Clear all protocols stats
g Go to other protocol screen
Ctrl-L redraw screen
w Write configuration file
a About this proggie
q Quit (bring da noize)

Total Packets: 0 -
This is the help screen
STP Fields
Source MAC 0A:23:1
Id 0000 Ver 00 Typ
BridgeId CB09.E7CD

AC Spoofing [X]

00
hcost 00000000
0002 Fwd 000F
```

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.

The screenshot shows a terminal window titled "yersinia -l - Parrot Terminal" running on a Linux system. The window displays the Yersinia 0.8.2 tool in DHCP mode. At the top, there's a header with "File Edit View Search Terminal Help". Below it, a table lists SIP, DIP, MessageType, Iface, and Last seen columns. A red box highlights the "Attack Panel" section which lists four attack types:

No	DoS	Description
0		sending RAW packet
1	X	sending DISCOVER packet
2		creating DHCP rogue server
3	X	sending RELEASE packet

Below the attack panel, a green box highlights the "DHCP Fields" section, which shows the configuration for the selected attack (Op 01). The fields include Source MAC (02), SIP (000.000.000.000), DIP (255.255.255.255), SPort (00068), DPort (00067), Op (01), Htype (01), HLEN (06), Hops (00), Xid (643C9869), Secs (0000), Flags (8000), CI (000.000.000.000), YI (000.000.000.000), SI (000.000.000.000), GI (000.000.000.000), and CH (02:48:33:66:02:51). A red box also highlights the "Total Packets" and "Spoofing [X]" sections.

At the bottom, the terminal shows "Capturing from eth0 (...)" and the title bar includes "Menu" and "yersinia -l - Parrot Ter...".

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.

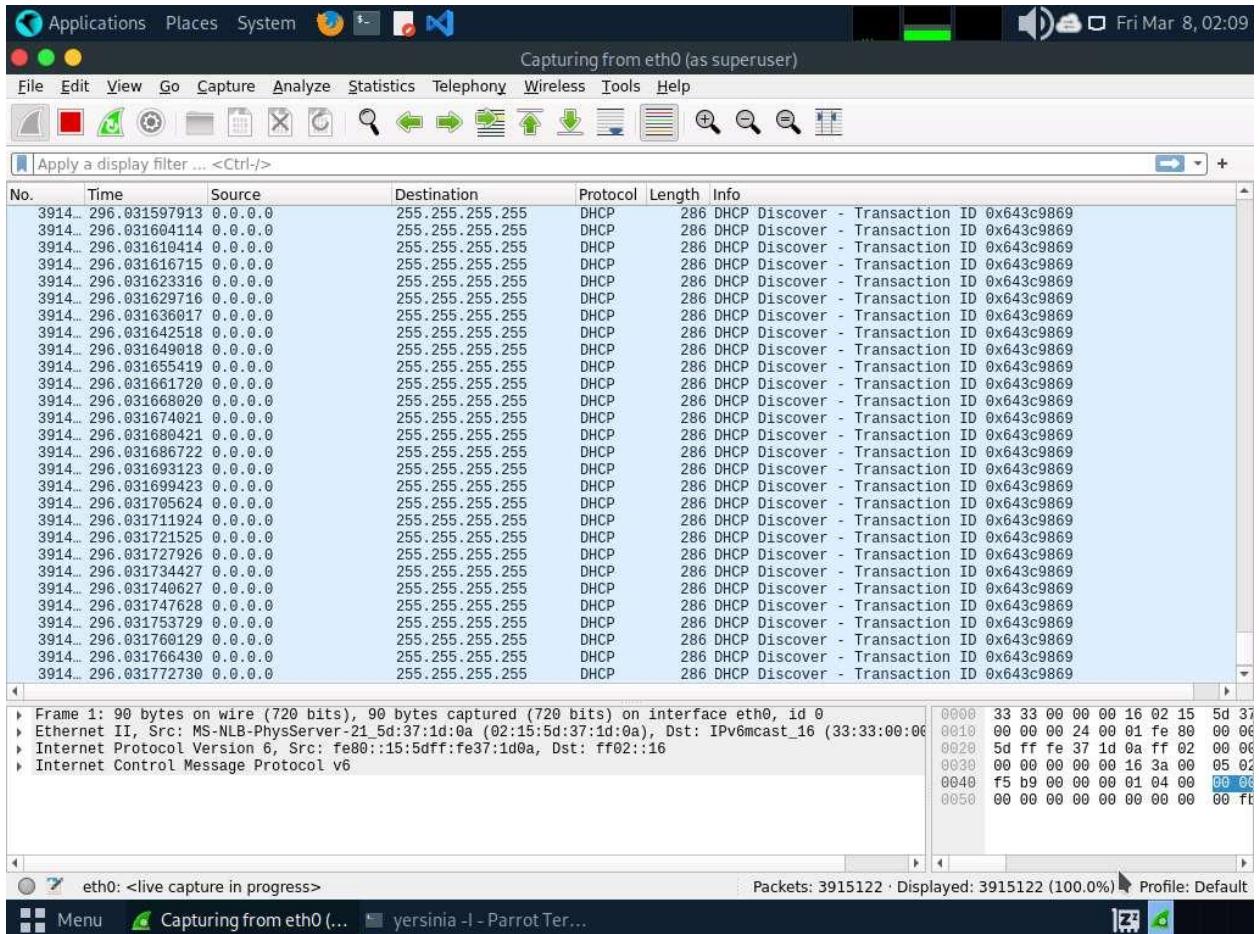
The screenshot shows a terminal window titled "yersinia -l - Parrot Terminal". The terminal session is as follows:

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
#cd
[root@parrot] ~
#yersinia -I

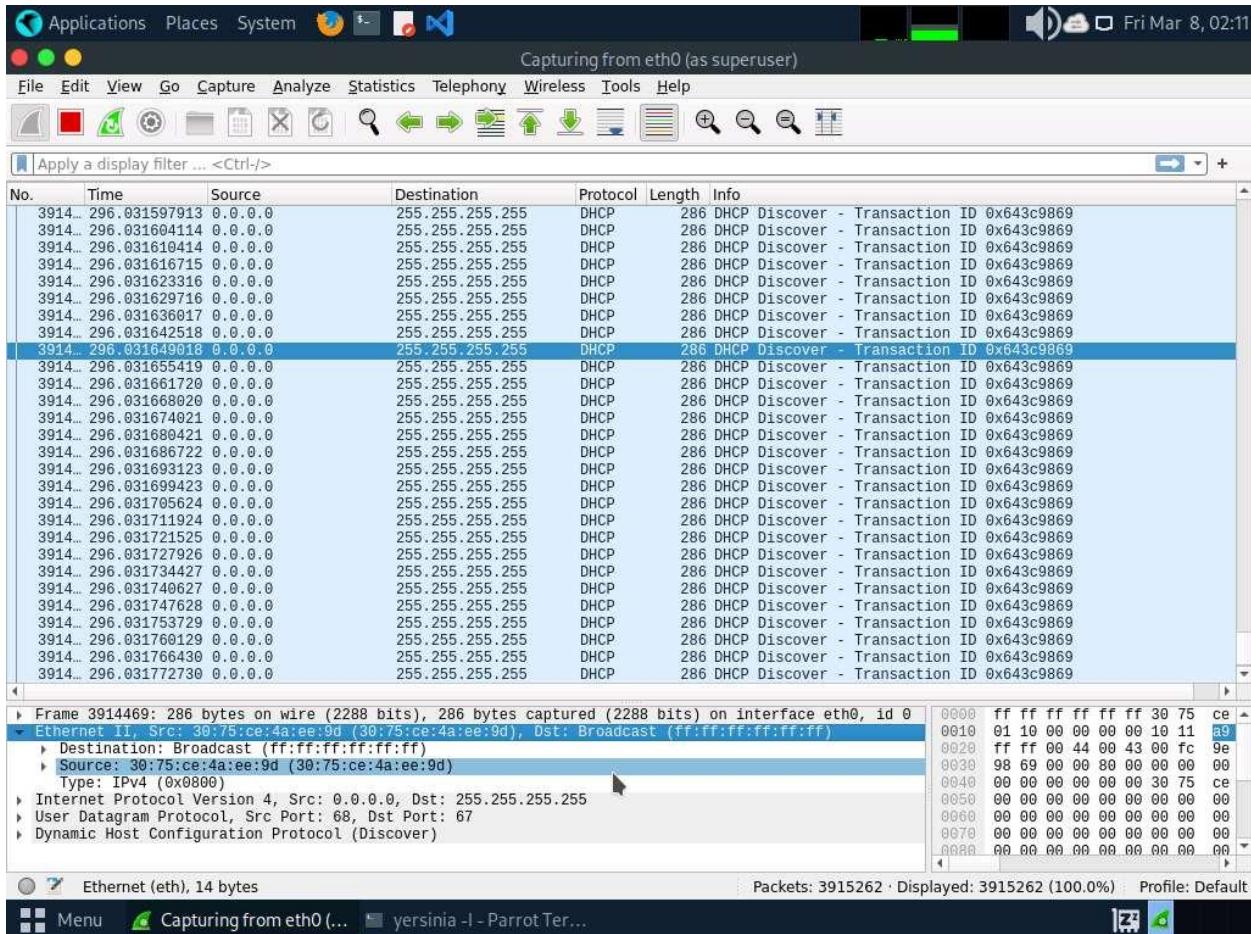
MOTD: Snowboard on the winter, MBK on the summer :)
[root@parrot] ~
#
```

The terminal is running on a Parrot OS desktop environment, indicated by the desktop icons in the background and the desktop menu bar at the bottom.

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?