SIMULATING ATTACKS AND DEFENDING AGAINST THEM.

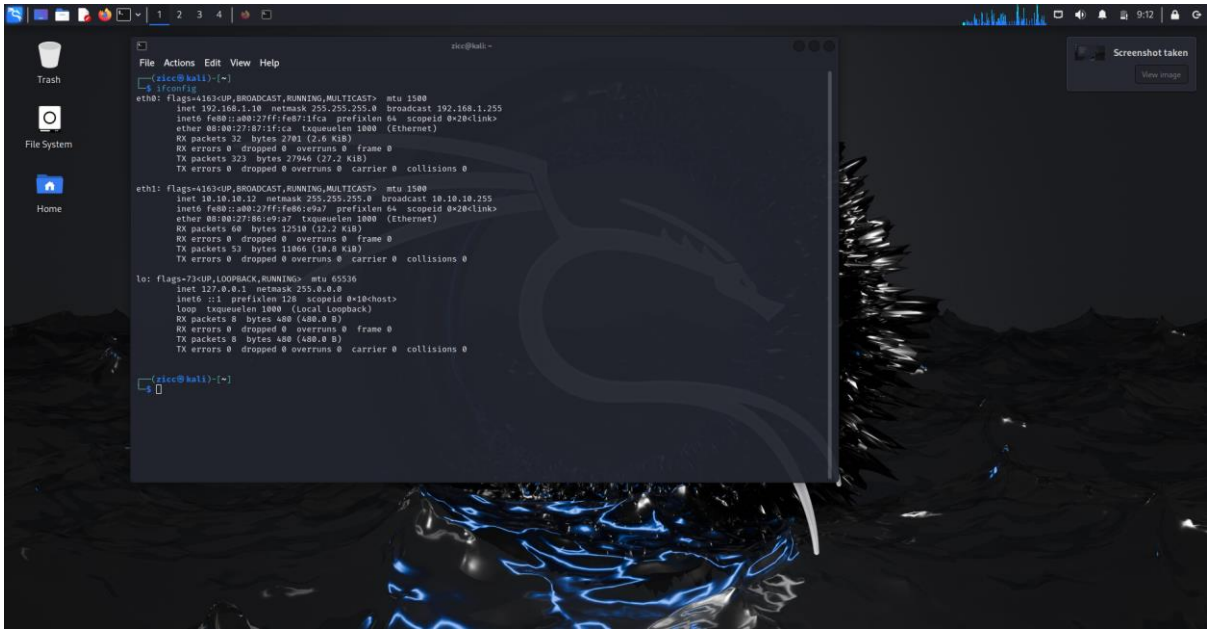
Objective: Simulating network attacks using arpspoof or ping floods in a virtual environment to analyze detection and mitigation techniques.

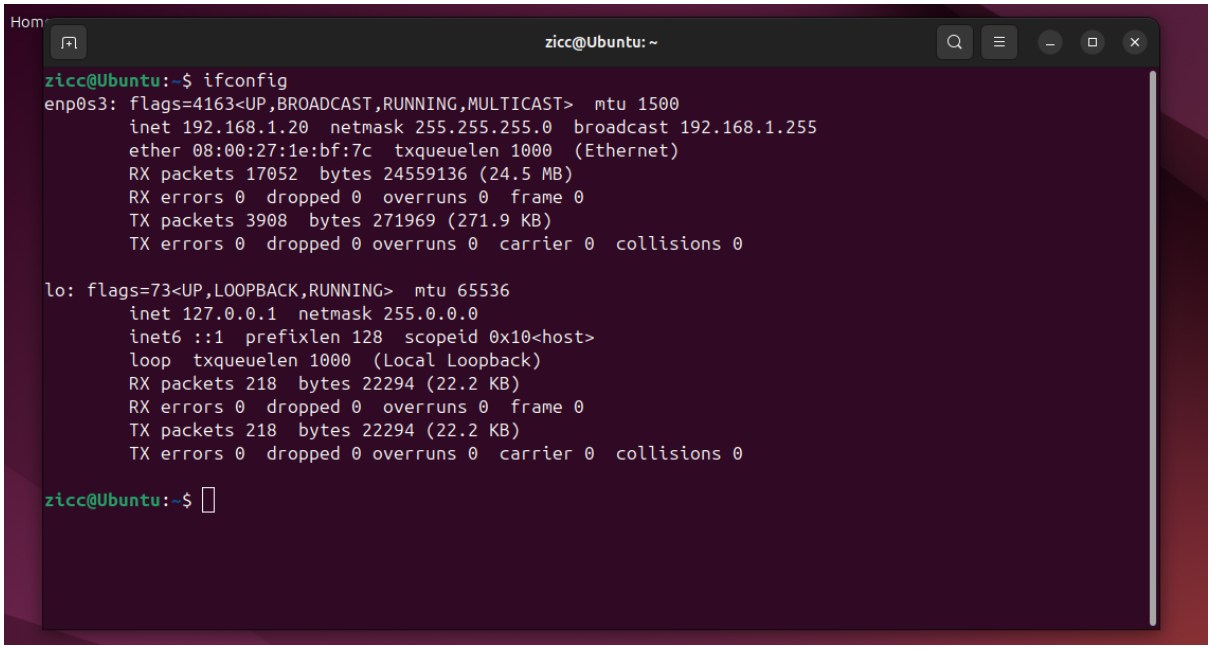
Tools used:

- Virtualbox or Vmware (Download from www.virtualbox.com or www.vmware.com)
- Kali linux. (Download from www.kali.org).
- Ubuntu (Download from www.ubuntu.com)
- Installing dsniff to your kali linux.
- Installing Wireshark on Ubuntu.

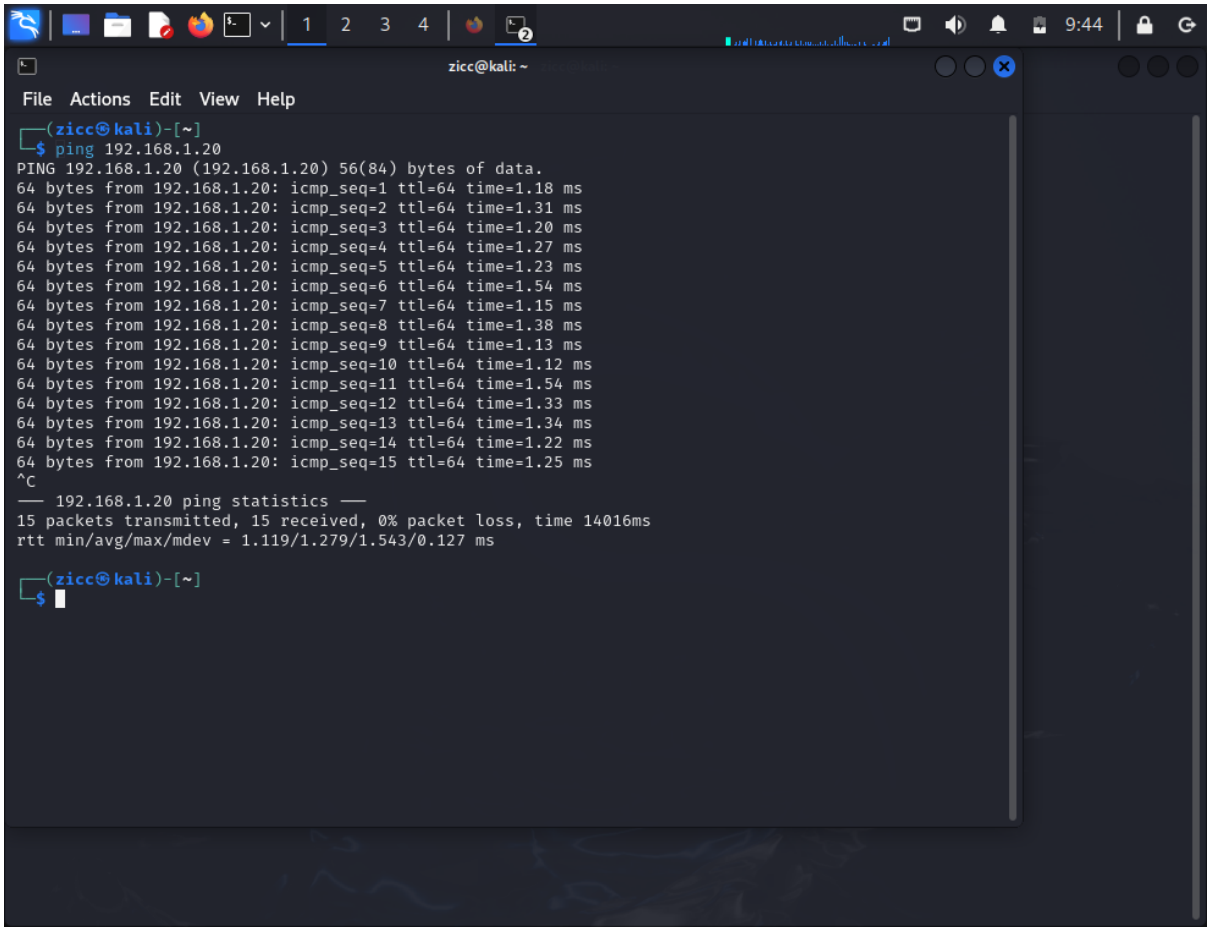
Steps:

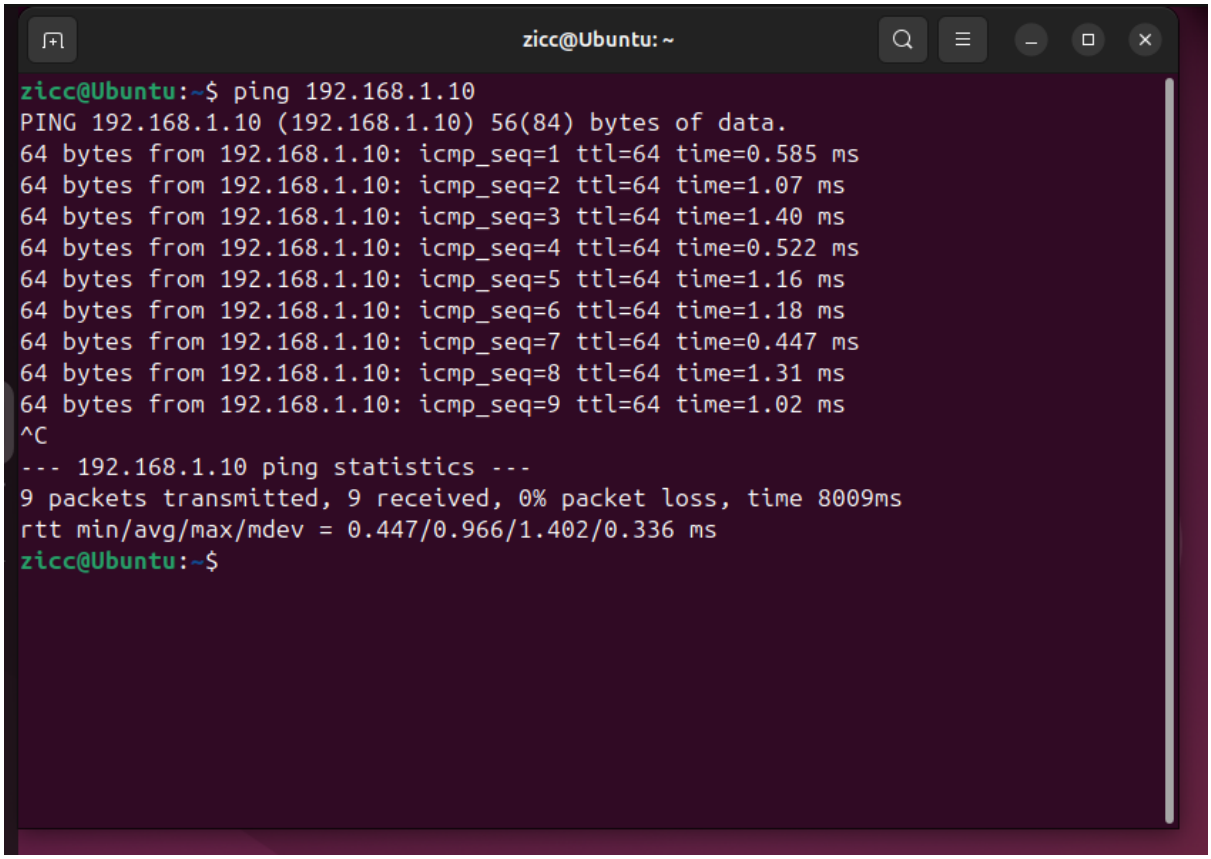
- Your downloaded kali linux and Ubuntu will be installed on your Virtualbox. The Kali linux for the purpose of this project will be the attacker and the Ubuntu will be the defender.
- Ensure both servers are configured to be on the same network so that they will be able to communicate with each other. (if you will be using **NAT** for both servers, ensure they are set to the same network or if you will be using **Host-Only**, ensure they are both set to **Host-Only**). You do this by going to the settings of each servers, click network and configure it. You can also create your own network under the **NAT-Network**. It all depends on you.
- Open the terminal of both servers and input **ifconfig.** As you can see, I setup two connections for my kali and Ubuntu, but I will be using the IP addresses 192.168.1.10 for the attacker(kali) and 192.168.1.20 for my defender(ubuntu).





- We will then ping the attacker and victim system to ensure they can communicate with each other. **Using ping 192.168.1.20**(pinging the victim) and **ping 192.168.1.10** (pinging the attacker)



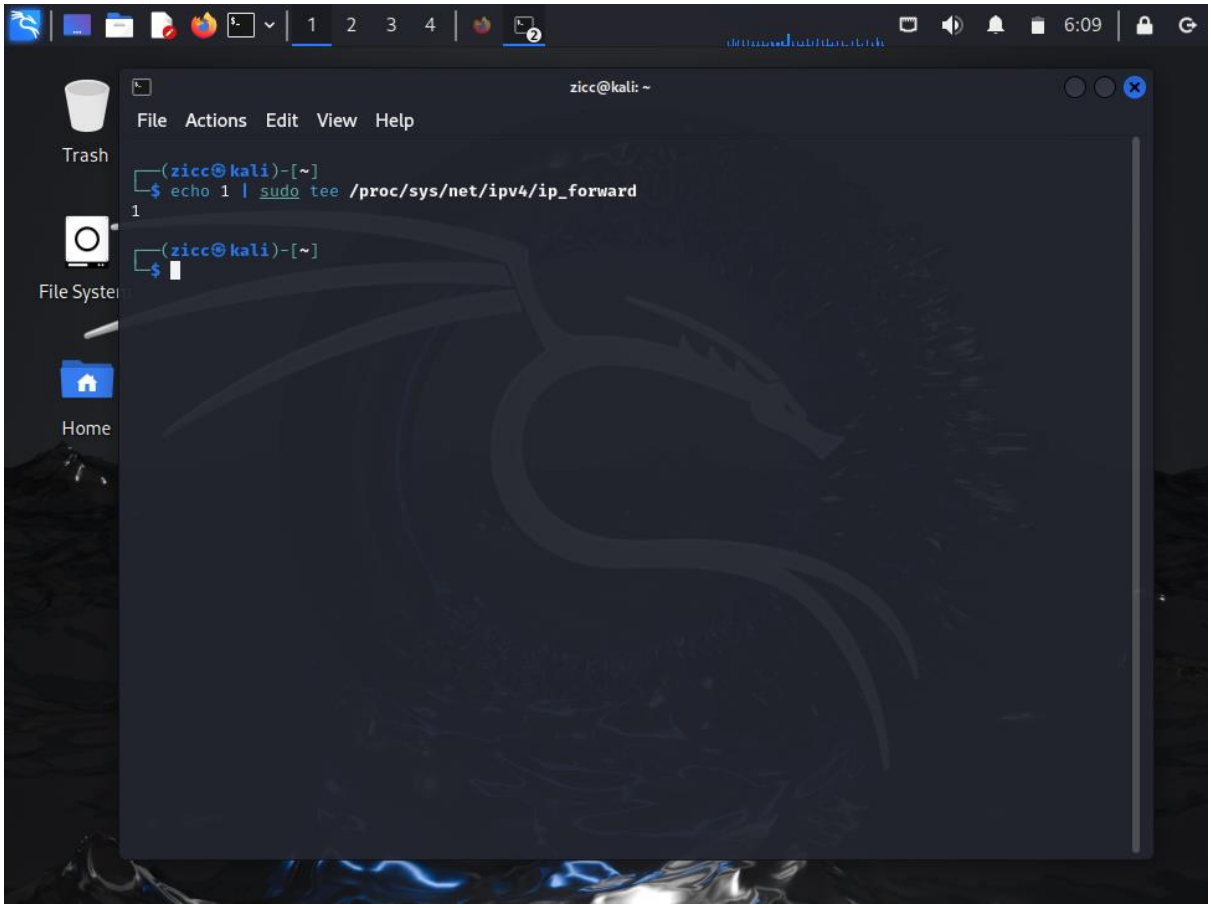


This shows that the attacker and the victim system can communicate with each other and their pings are successful.

I need to enable IP forwarding because I will be spoofing from the attacker system.

I used **echo 1 | Sudo tee /proc/sys/net/ipv4/ip_forward**

From the screenshot, the output is **1** which means it is successful.



- Next step is to install and update dnsiff using the following commands:

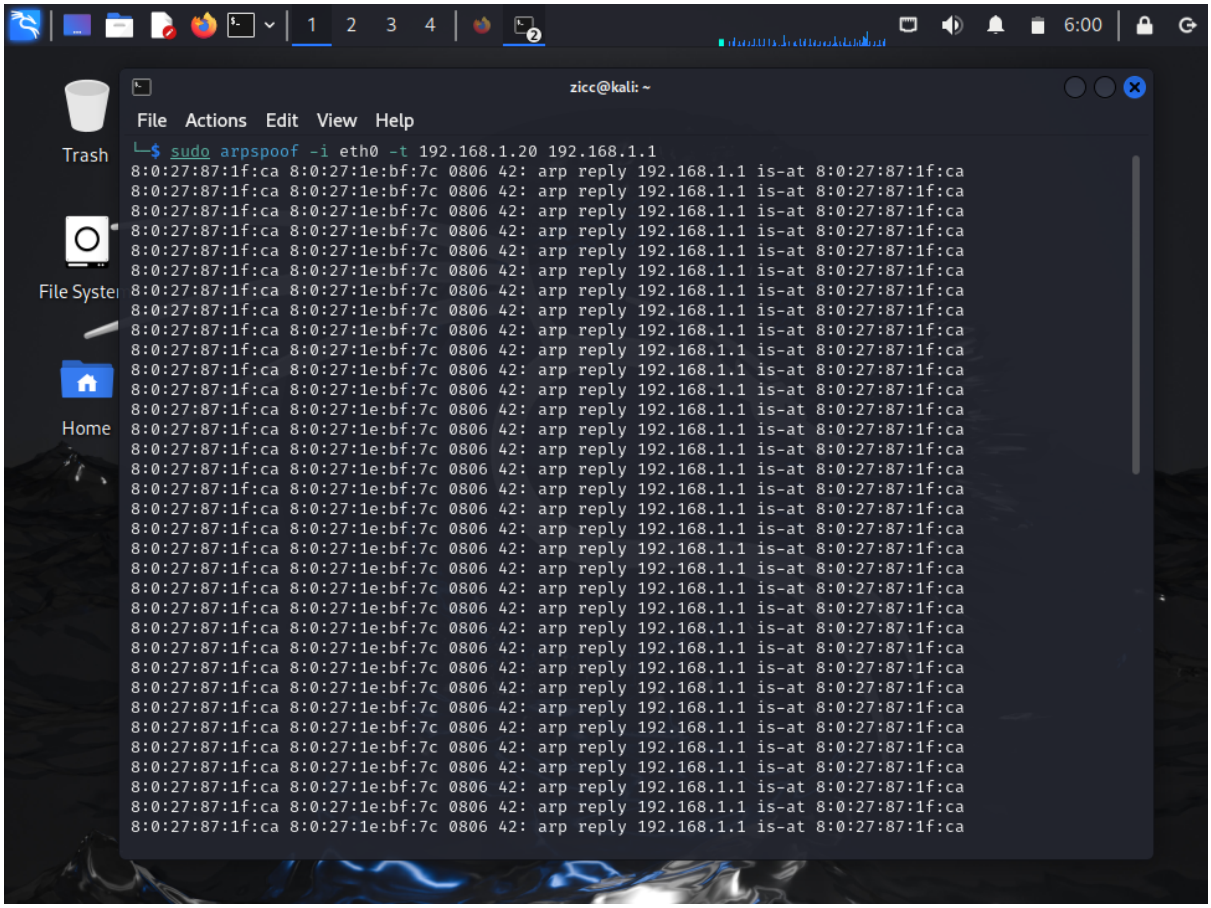
  Sudo apt update

  Sudo apt install Dsniff.

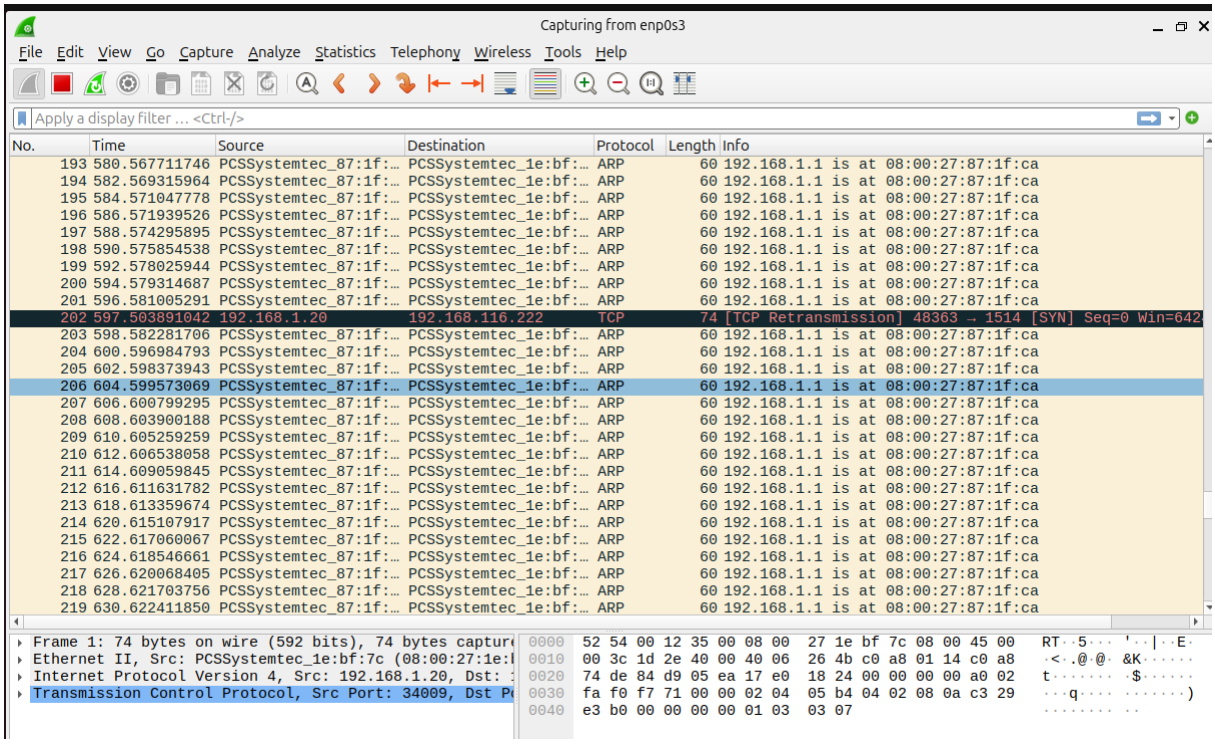
  After installation of dsniff, you use the arpspoof to spoof your victim.

We use **Sudo arpspoof –i eth0 –t 192.168.1.20 192.168.1.1.**

This is to trick the victim system into internet traffic meant for the gateway we are acting as, but it goes to the attacker instead.

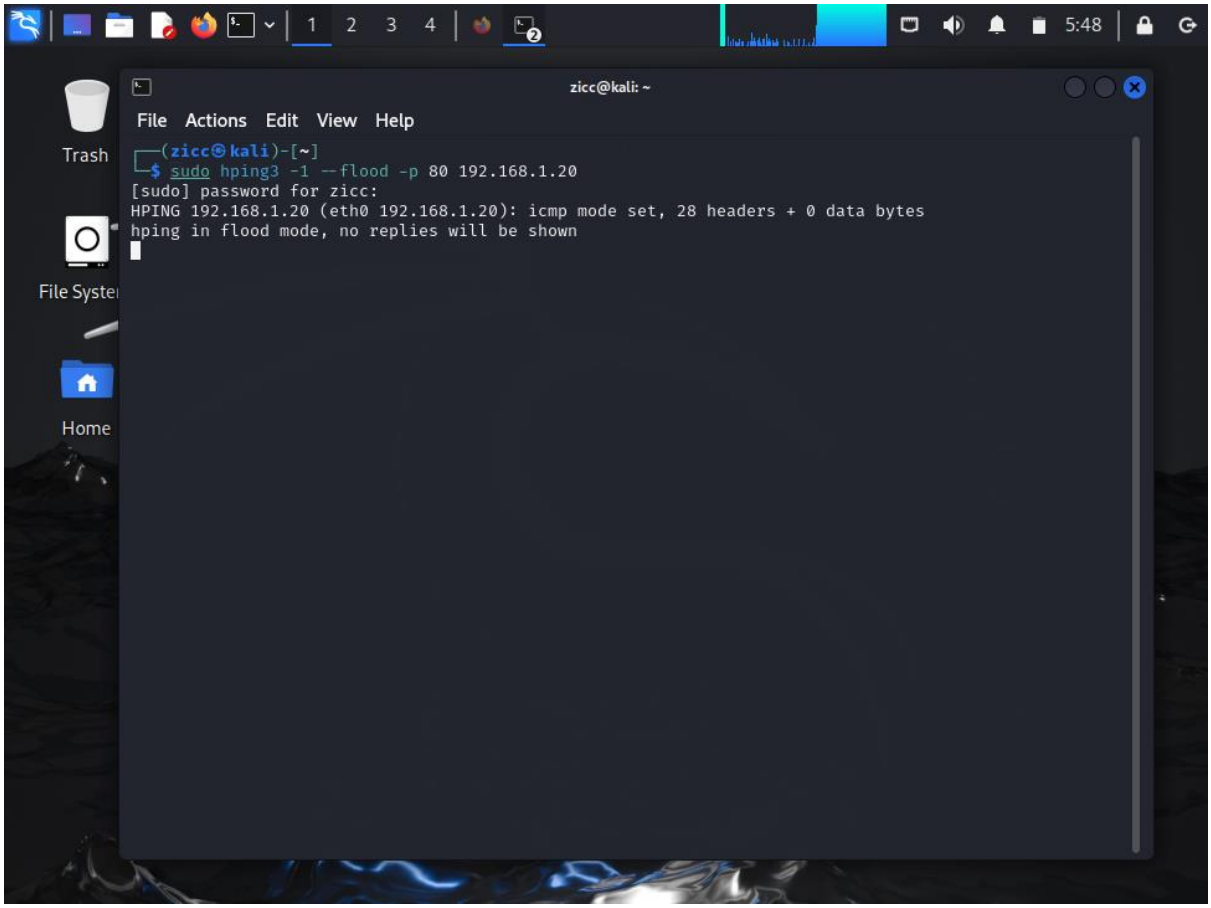


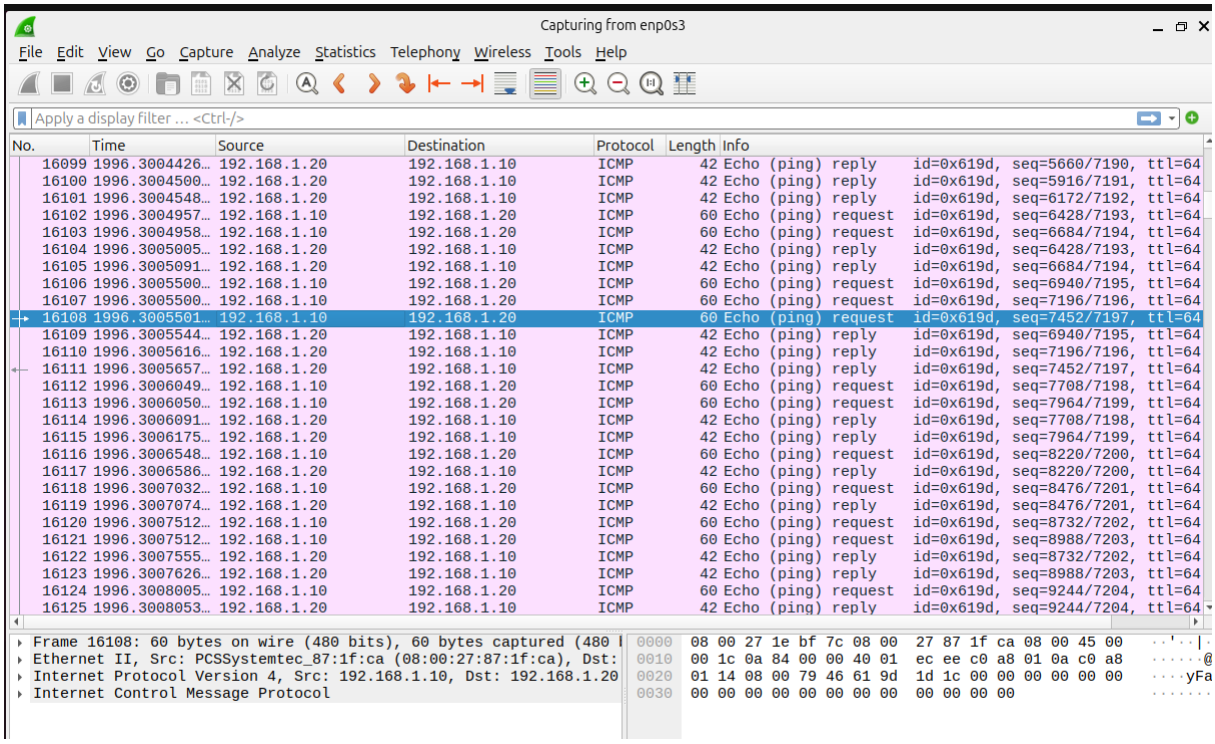
As you can see, it is feeding the gateway IP 192.168.1.1 its internet traffic but it is actually feeding the attacker.



Next is to install hping3 using **sudo apt install hping3.** This is used for aggressive flooding to the victim machine.

Sudo hping3 -1 –flood –p 80 192.168.1.20





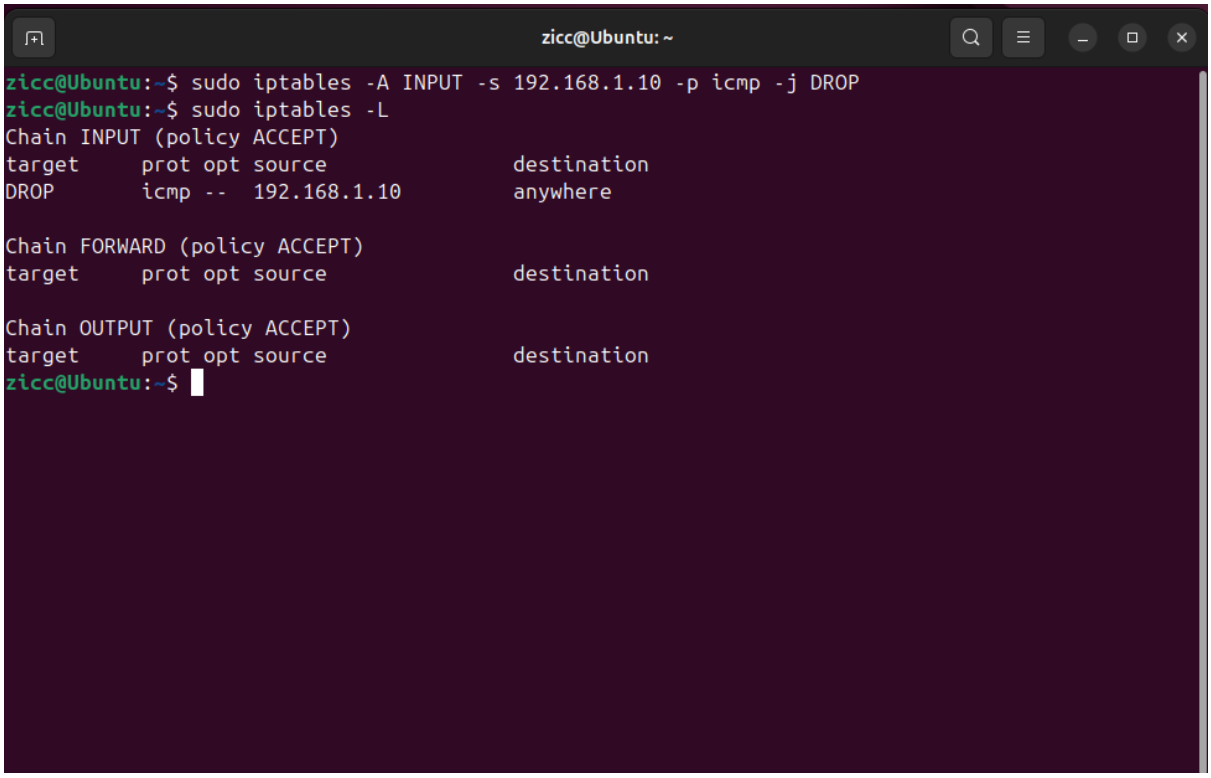
DEFENDING AGAINST THE ATTACK.

To defend against the attack, we use iptables on Ubuntu system.

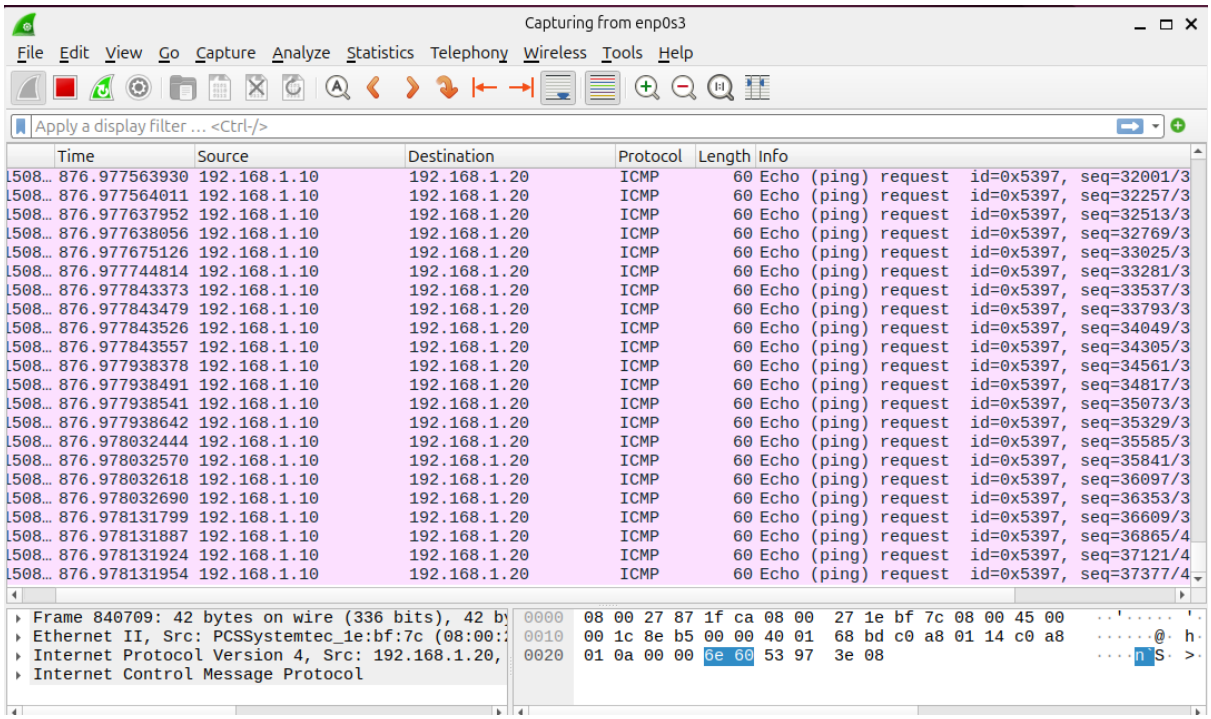
Sudo iptables –A INPUT –s 192.168.1.10 -p icmp –j DROP

This prevents all incoming ICMP Packets from the attacker's IP.

To ensure the rule was applied, **Sudo iptables -L**



This ensures that the victim system stopped responding to the ICMP packets. The attacker's system kept sending echo request but got no echo reply from the victim.



CONCLUSION.

This is a Man-in-the-Middle Attack (MITM) and it is used to intercept network traffic.

To prevent such attack:

- Always use encrypted HTTP (HTTPS)
- Always use vpn when connecting to public wifi.