LAN BASED ATTACKS

Requirements:

Host – kali linux (192.168.196.130)

Target device – Ubuntu (192.168.196.131)

ARP POISONING

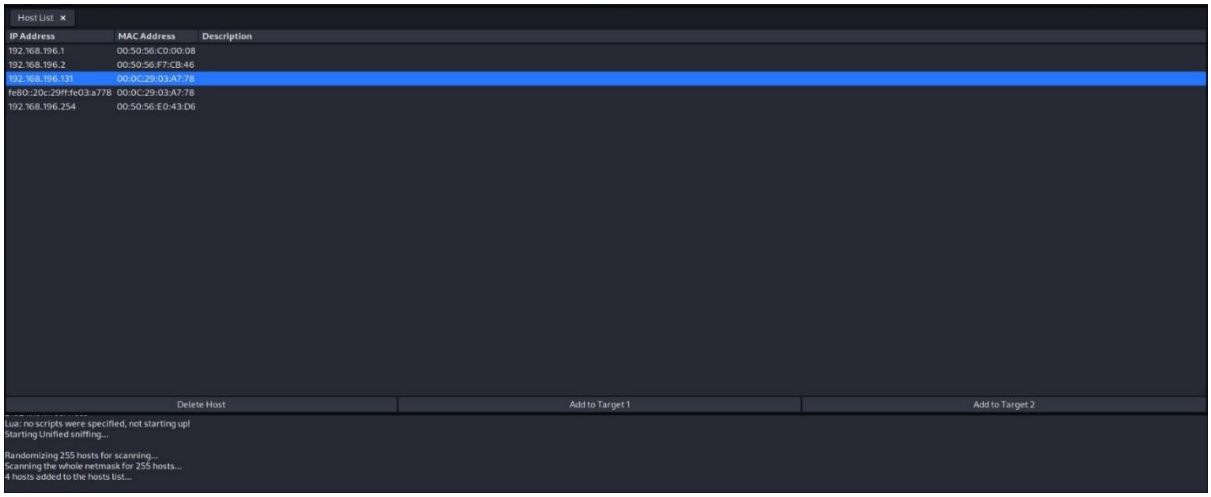
- Cyber attack carried out over a LAN, that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP address to MAC address table.
- Attacker sends an ARP reply to the gateway, informing that its MAC address is associated with the target's IP address.
- When gateway receives this message, it broadcast changes to all other devices on the network.
- ARP Poisoning can cause DoS condition by intercepting or dropping the target's packets.

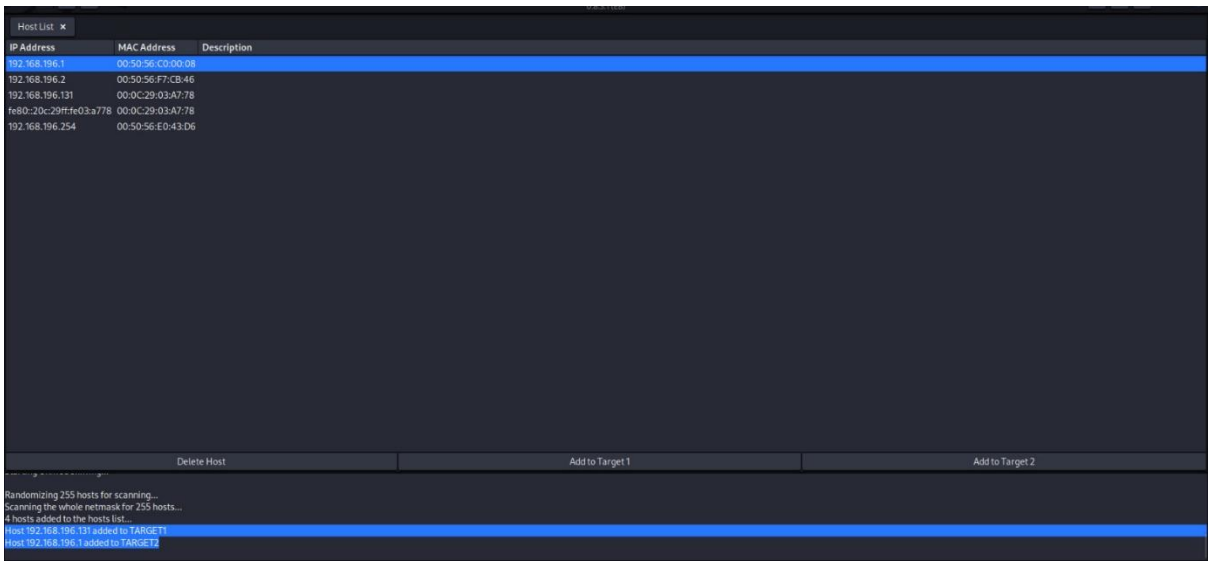
Implementation –

1. Start ettercap in host and set up the tool.

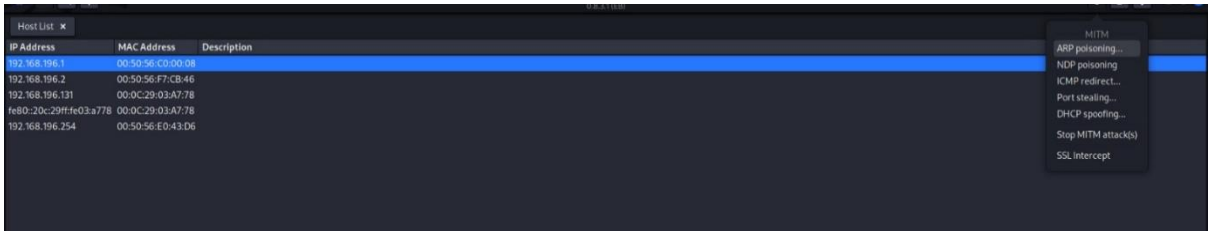
2. Scan for the hosts.

3. We can see a number of devices available. Identify the IP address of ubuntu and add it as target 1 and gateway as target 2.

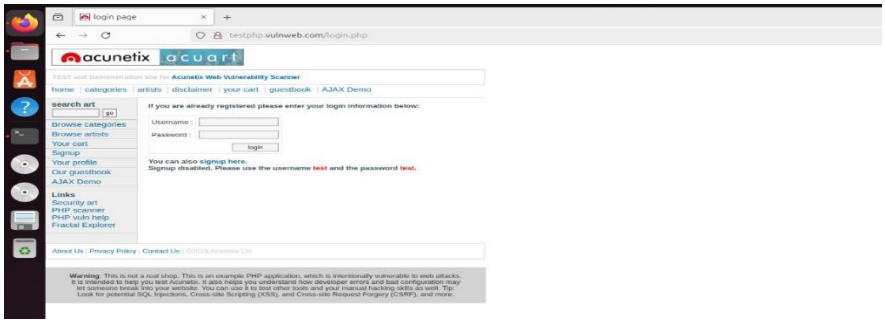




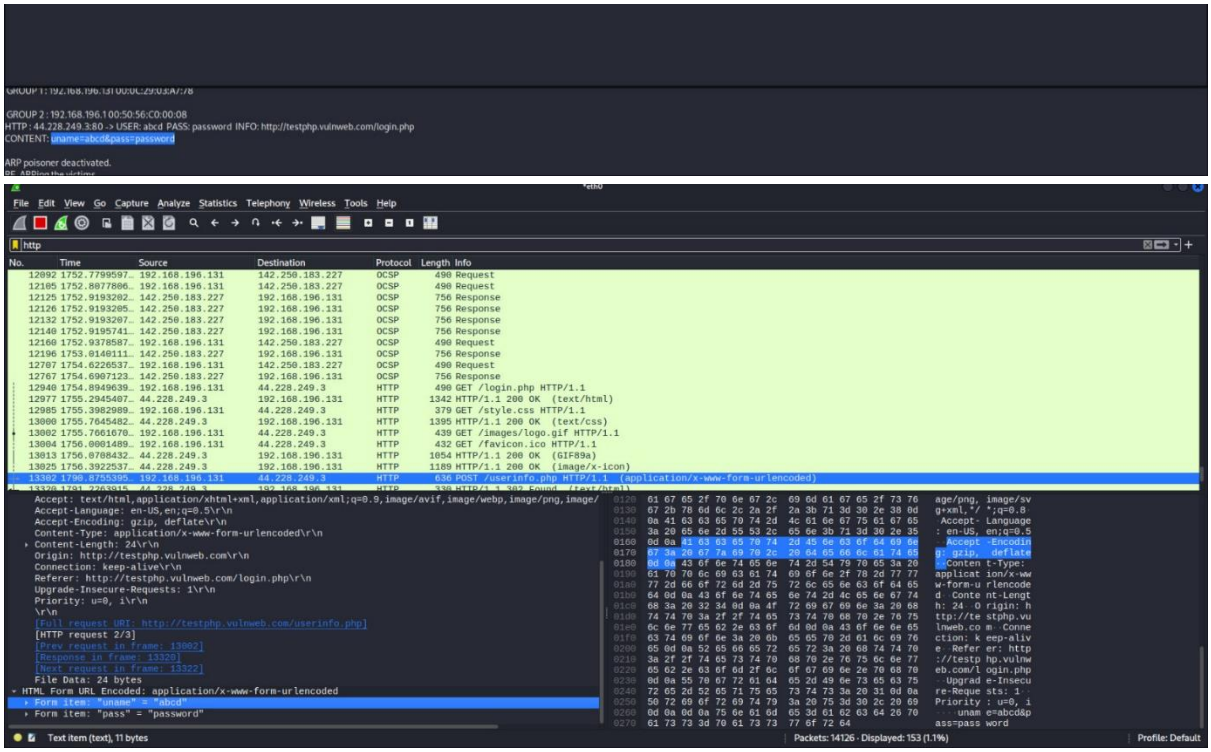
4. Start wireshark in kali and start packet capturing.
5. In Ettercap select MITM -> ARP poisoning.



6. Login to any website from target device (Username: abcd & password: password)



7. Now this username and password will be visible to the attacker.

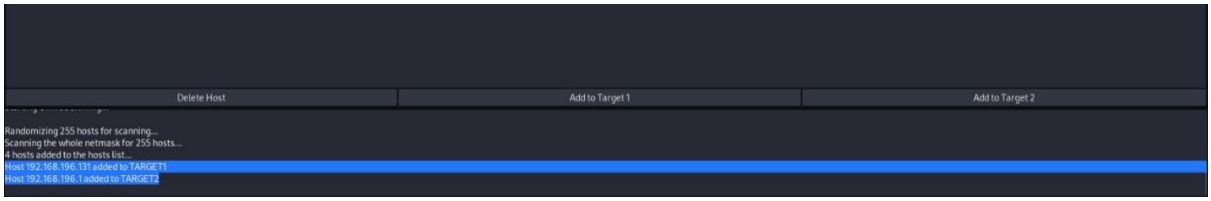


Denial of services (DoS)

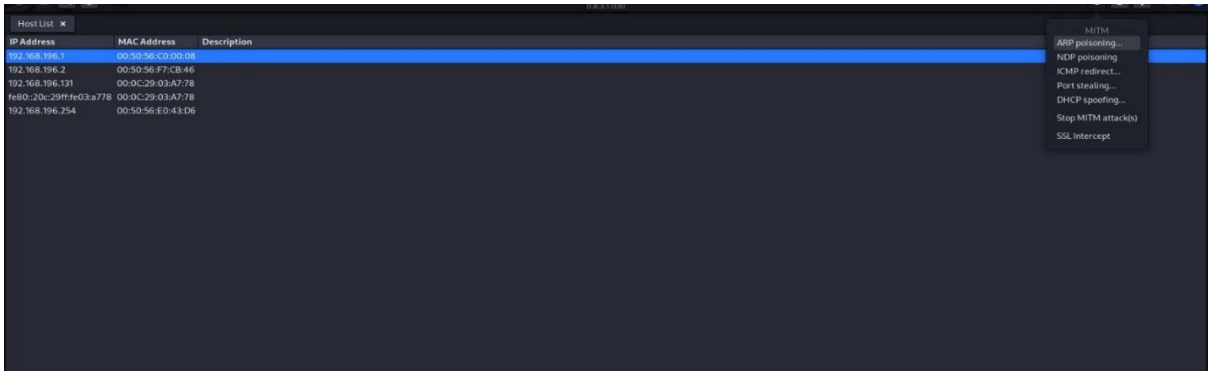
- DoS is cyber attack in which attacker makes a system unavailable to the intended user by interrupting its normal functioning.
- It overwhelms a network or server with excess traffic, causing service disruption.

Implementation**:**

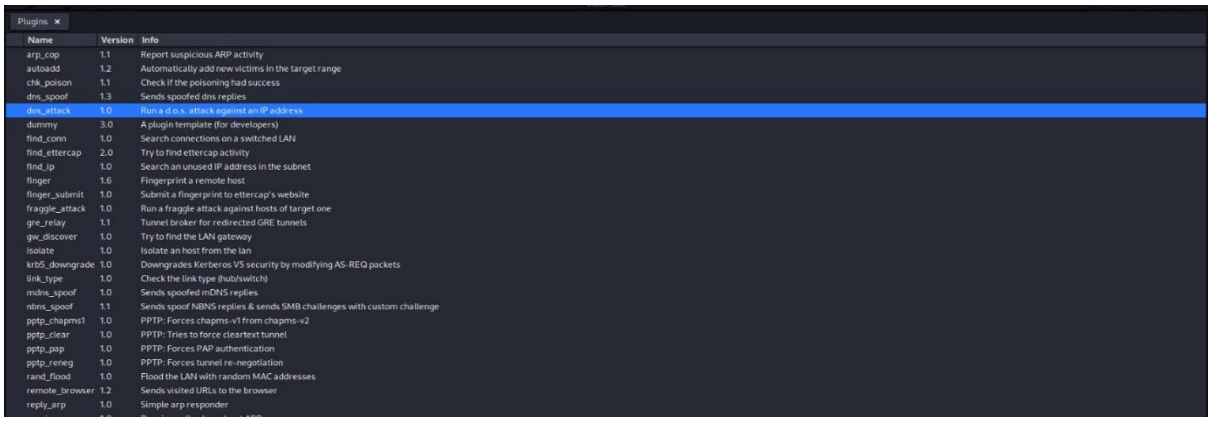
1. Start ettercap in host (kali linux) and set up the tool.
2. Scan for the hosts.
3. We can see the number of devices available. Identify the IP address of ubuntu and add it as target 1 then add gateway as target 2.



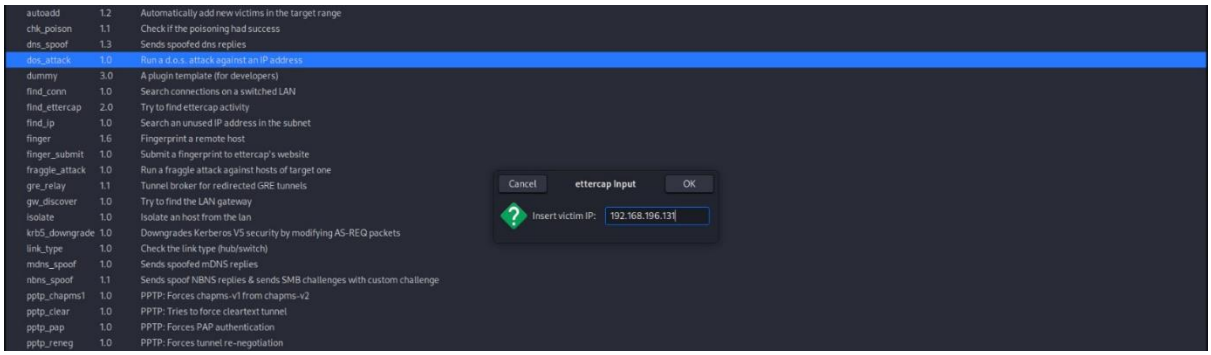
4. Start wireshark in kali and start packet capturing.
5. In Ettercap select MITM -> ARP poisoning.

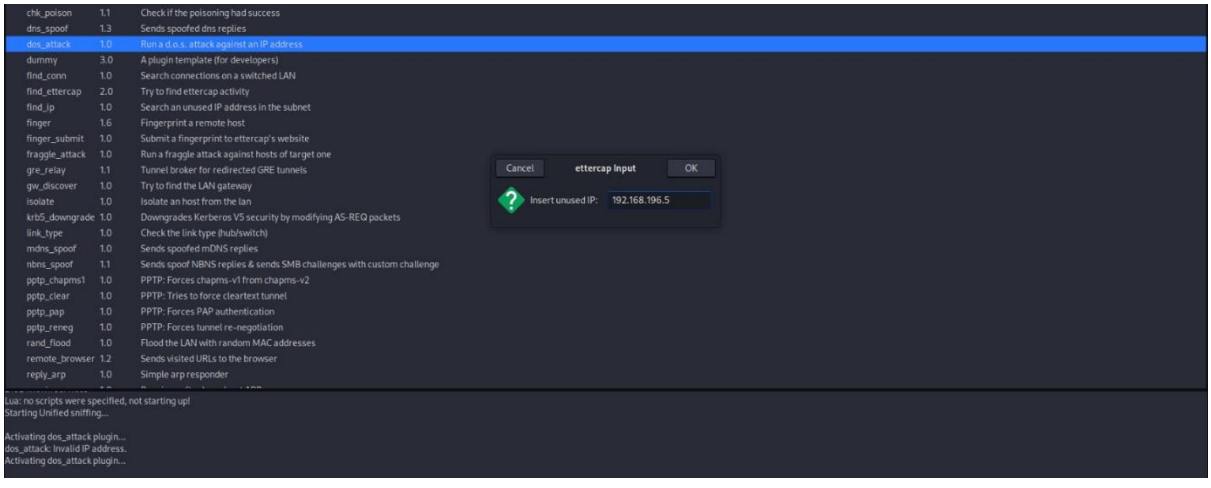


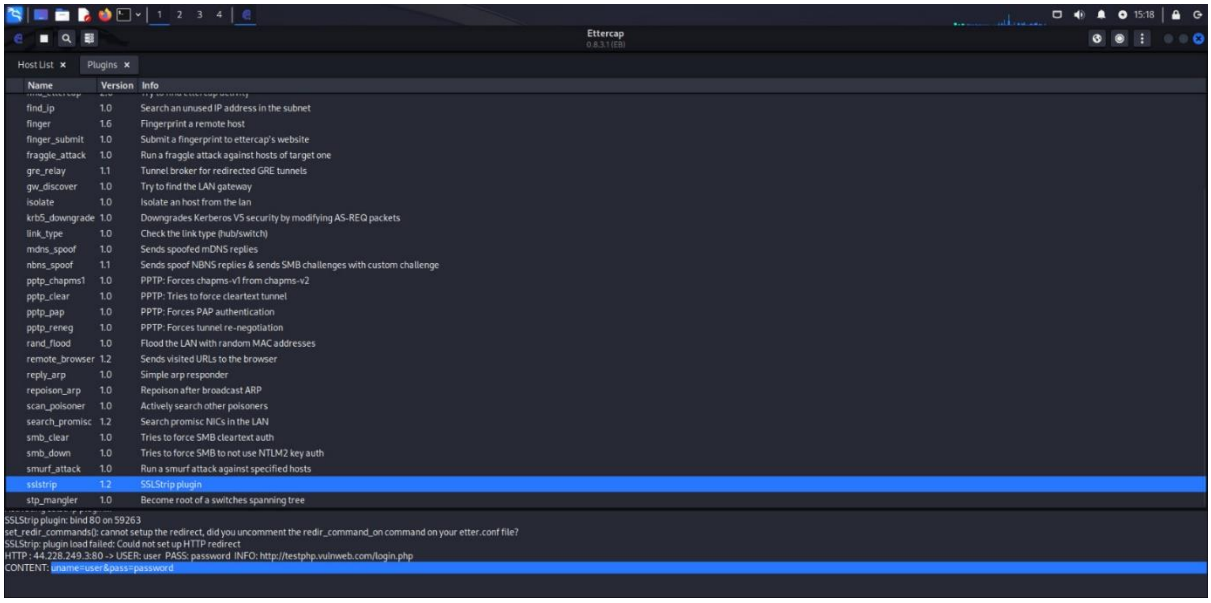
6. Select DoS plugins from plugins list.

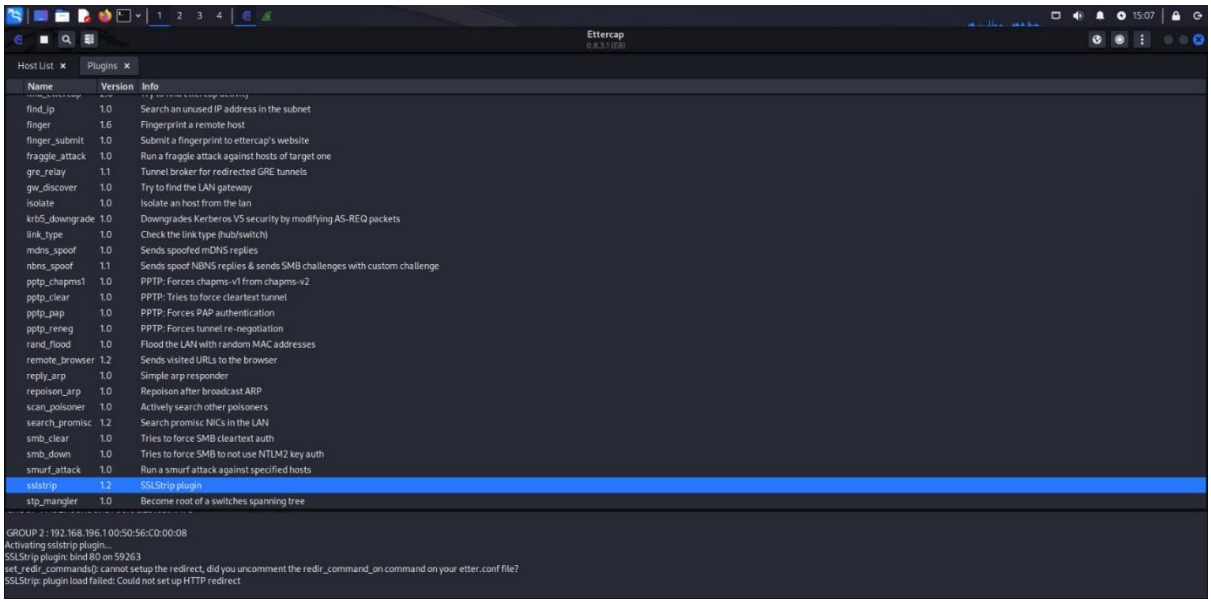


7. Add target ip address as ubuntu's IP address and any unused IP address.

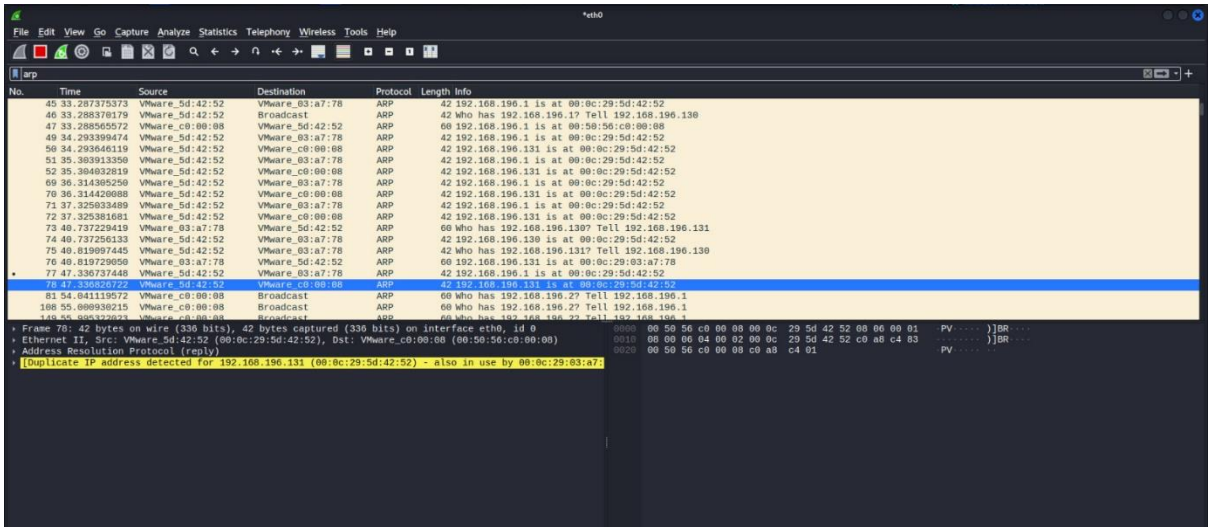




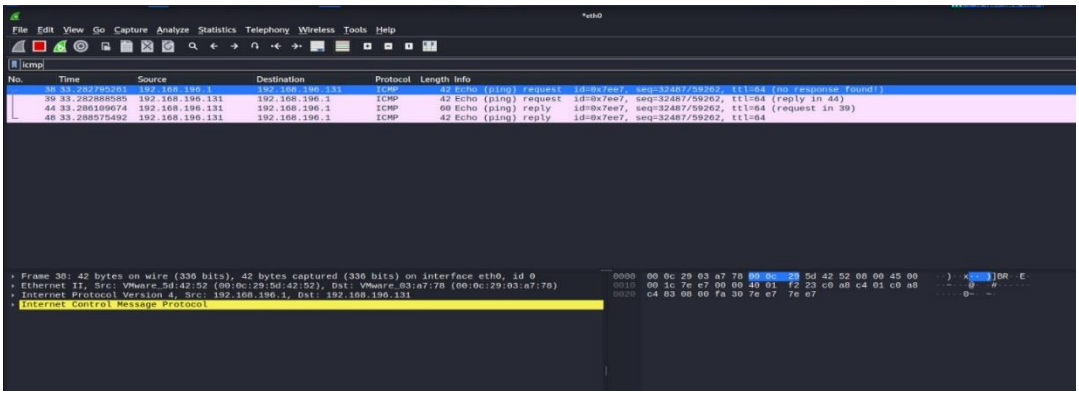




8. In wireshark, open the captured packets and apply filter as arp or icmp.



Here, ubuntu's IP address has multiple associated MAC addresses. This creates a conflict where multiple devices claim to own the same IP address.



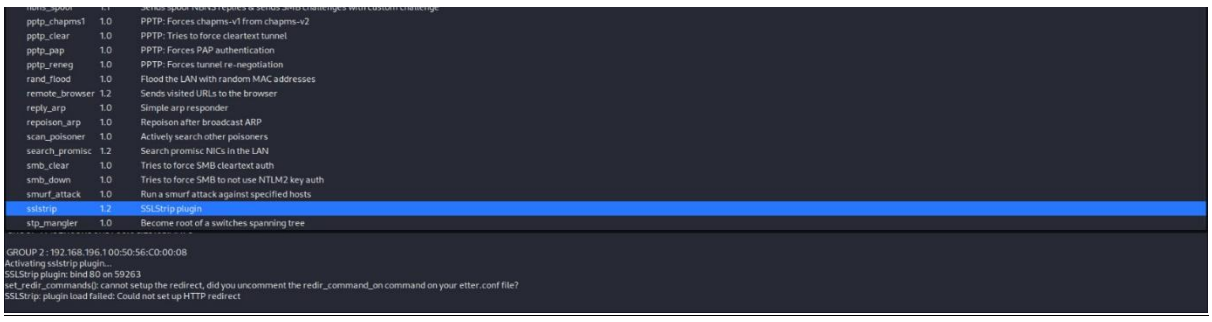
Here, target failed to produce the packet. It might be overwhelmed or intentionally dropping packets to protect itself.

SSL STRIPPING:

- Attack in which attacker intercepts the transition from HTTP to HTTPS.
- They do this by capturing a user's request to the server during the protocol redirection.
- The attacker then sets up a secure HTTPS connection with the server on one end and an unsecured HTTP connection with the user on the other, effectively positioning themselves as a "bridge" between the two.

Implementation –

1. Scan for hosts in Ettercap and add ubuntu as target 1 then gateway as target 2.
2. Go to MITM -> ARP Poisoning then enable sniff poisoning.
3. Go to plugins and select ssltrip.



4. In target system, try to visit any https site (username = user & password= password).
5. As a result of SSL stripping, https connection will downgrade to http.
6. Attacker will get these login credentials.