ARP SPOOFING PROJECT

Submitted by:
Priya Vart Kumar Priyanshu
ERP: 6606467
B.Tech CSE – 3Rd Semester

TOOL USED

- Oracle VirtualBox
- Kali Linux (Attacker System)
- Ubuntu Linux (Victim System)
- dsniff / arpspoof Tool
- Terminal (Command Line Interface)

IP CONFIGUATION(VICTIM)

- The victim machine is configured with Ubuntu Linux.
- The system receives a dynamic IP address from the network.
- The IP address and network interface are verified using the 'ip a' command.
- This confirms that the victim system is connected to the same network as the attacker.

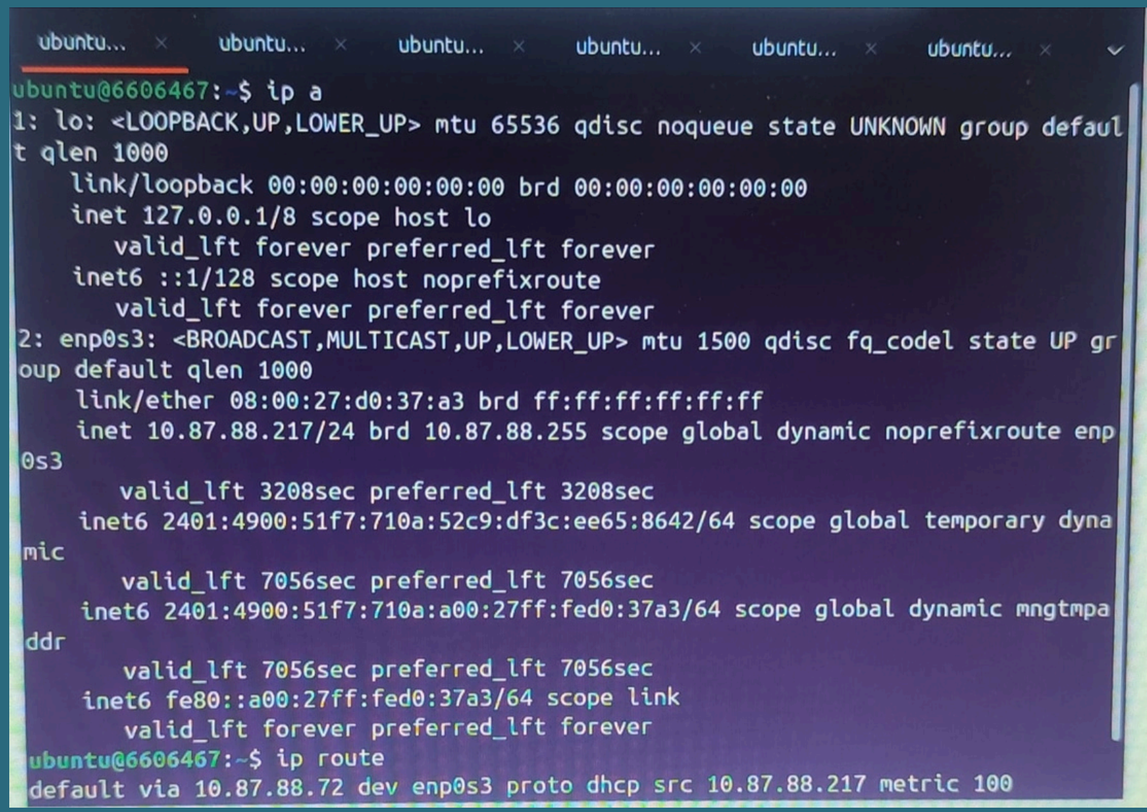

Figure 1: IP address details of Ubuntu victim system

IP CONFIGURATION(ATTACKER SYSTEM-KALI LINUX)

- Kali Linux is used as the attacker system.
- The attacker machine is connected to the same network as the victim.
- IP address and network interface details are verified using the 'ip a' command.
- This confirms that the attacker can communicate with the victim system.

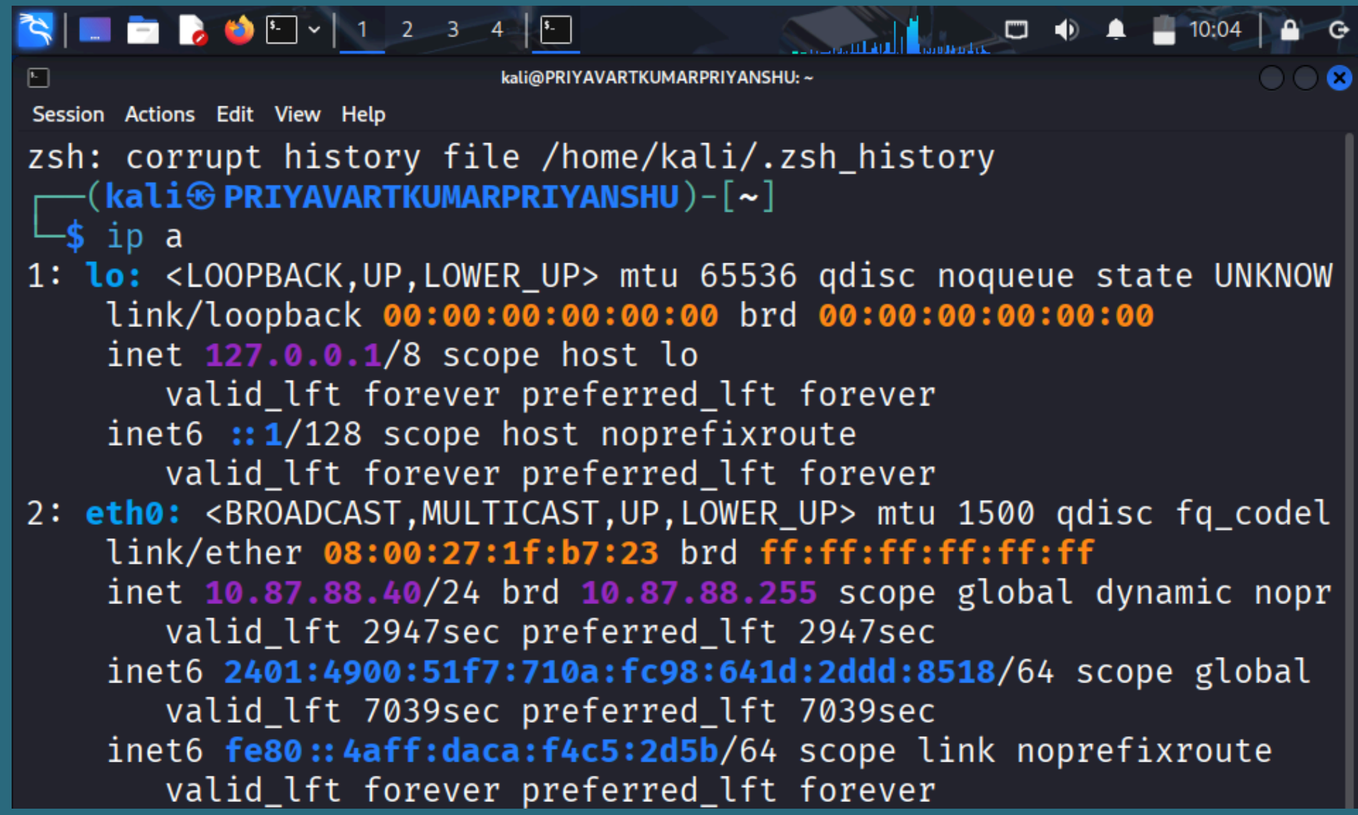

Figure 2: IP address details of Kali Linux attacker system

Network Connectivity Verification

- Before performing the ARP spoofing attack, network connectivity is verified.
- ICMP ping is used to test communication between attacker and victim systems.
- Successful ping responses confirm that both systems are on the same network.
- This step ensures that the attack can be executed properly.

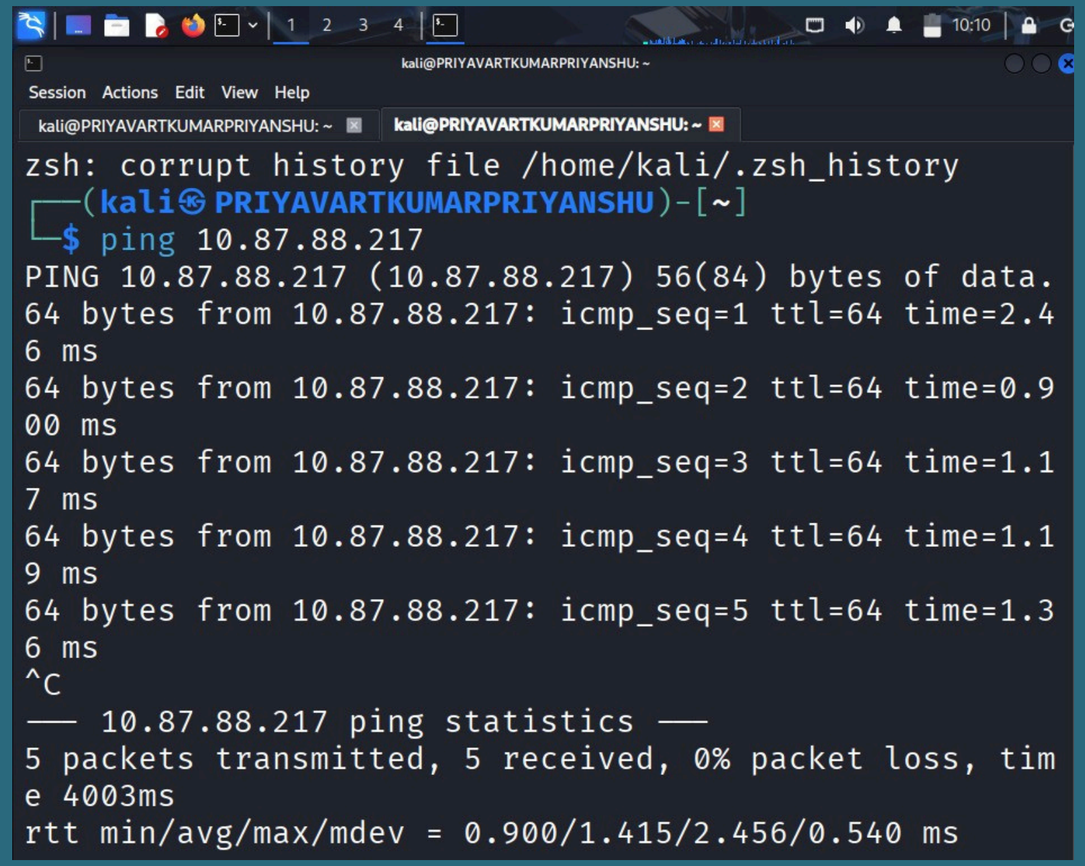

Figure 3: Successful ping response between attacker and victim systems

ARP Table Before Attack

- The ARP table stores mappings between IP addresses and MAC addresses.
- Before the attack, each IP address is mapped to a unique MAC address.
- The ARP table is checked using the 'arp -a' command on the victim system.
- This represents the normal and secure state of the network.

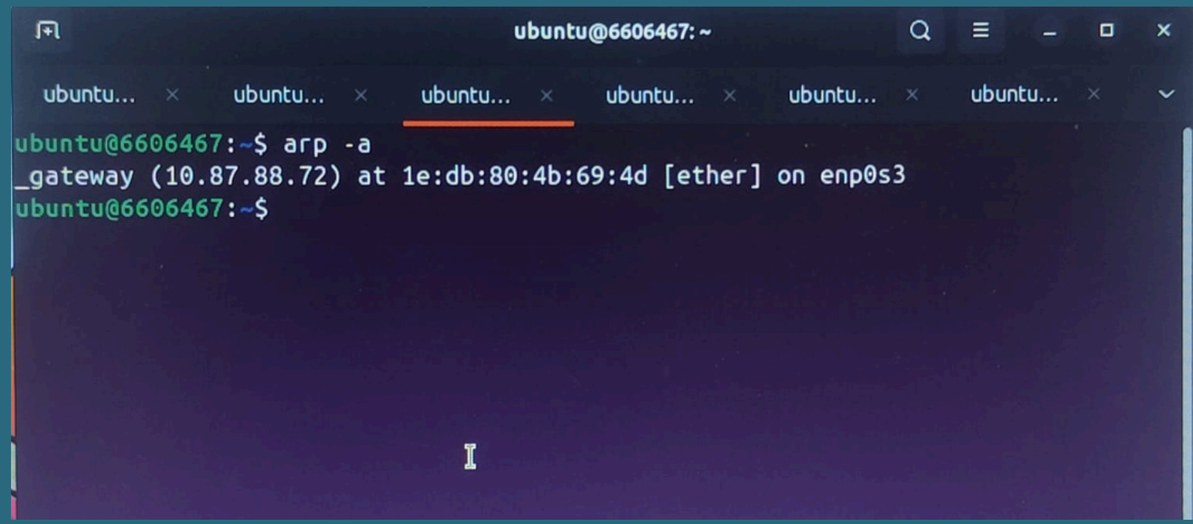

Figure 4: ARP table of victim system before ARP spoofing attack

ARP Spoofing Attack Execution

- After verifying network connectivity, the ARP spoofing attack is initiated.
- The attacker sends forged ARP replies to the victim system.
- These fake replies associate the attacker's MAC address with a trusted IP address.
- The attack is performed using the arpspoof tool available in Kali Linux.

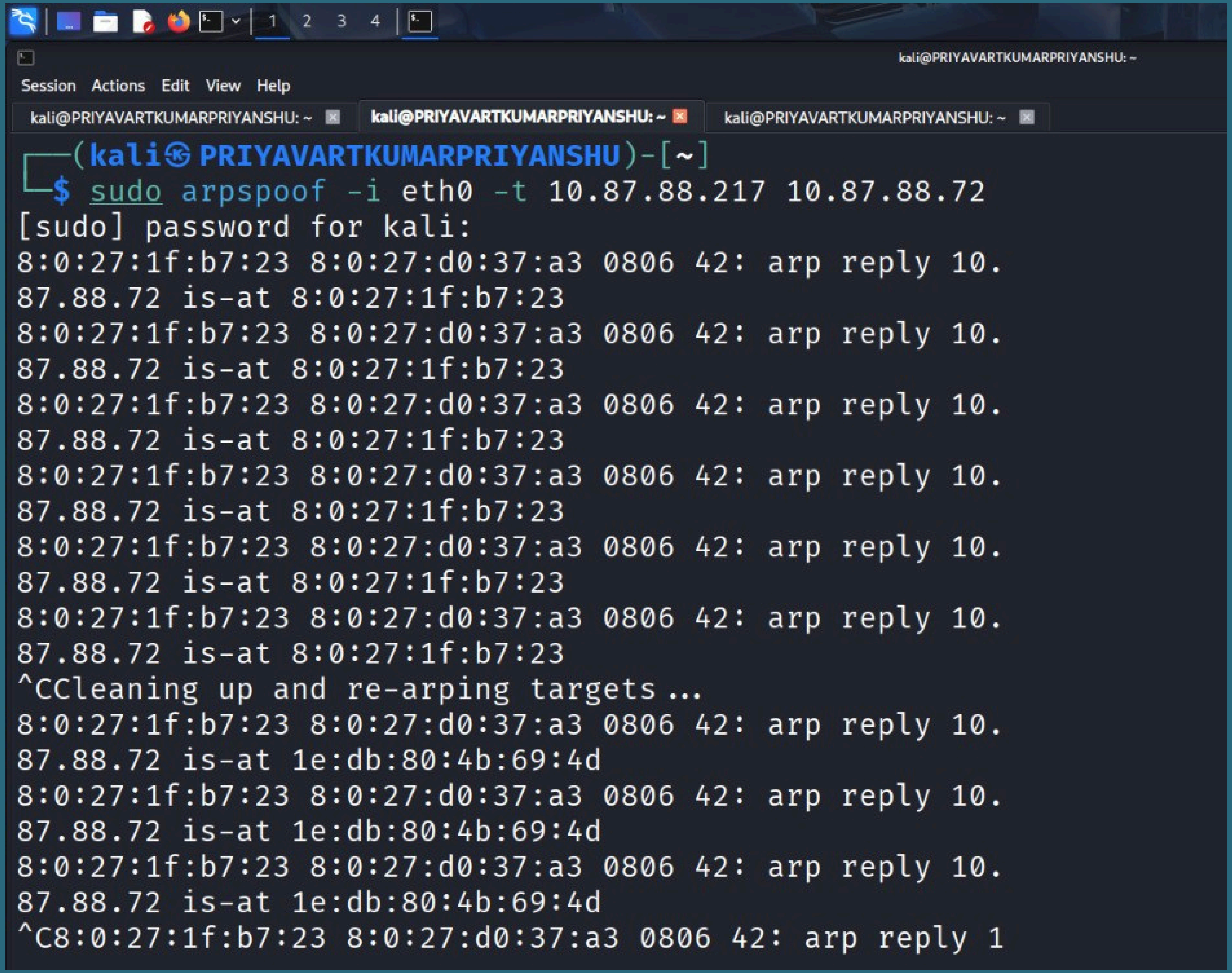

Figure 5: Execution of ARP spoofing attack from Kali Linux attacker system

ARP TABLE AFTER ATTACK

- After executing the ARP spoofing attack, the ARP table of the victim system is checked again.
- The ARP cache is found to be poisoned due to forged ARP replies.
- Multiple IP addresses are mapped to the same MAC address.
- This confirms a successful ARP spoofing and Man-in-the-Middle attack.

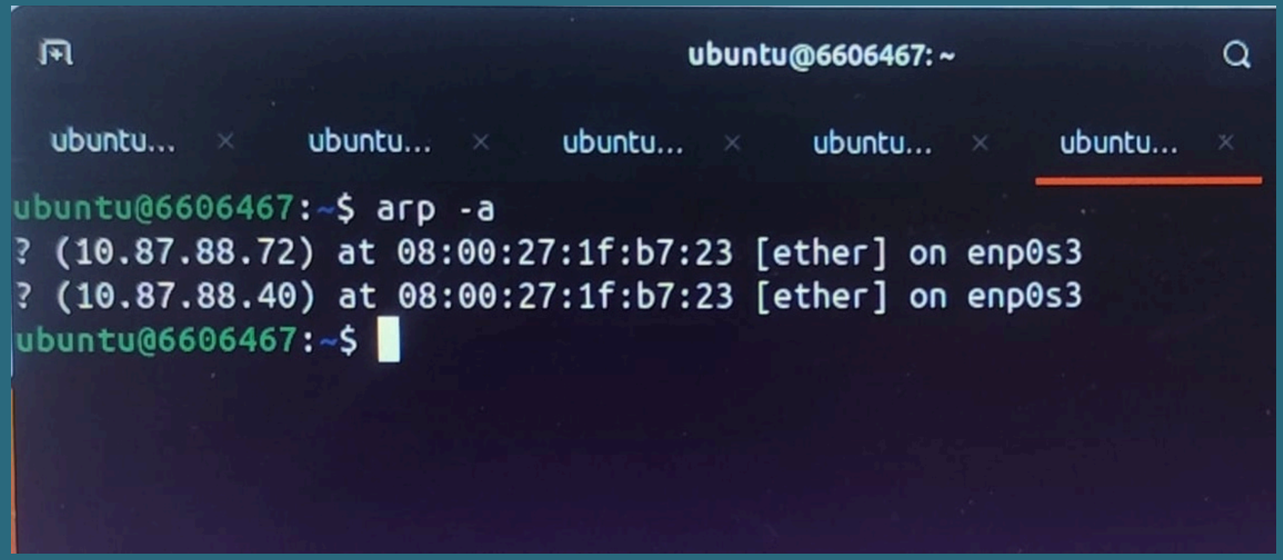

Figure 6: ARP table of victim system after ARP spoofing showing duplicate MAC addresses

Result and Observation

- The ARP spoofing attack was successfully executed in a virtual environment.
- The victim system accepted forged ARP replies from the attacker.
- As a result, multiple IP addresses were mapped to a single MAC address.
- This placed the attacker in a Man-in-the-Middle position between the victim and the gateway.