

Name: Vaishnavi Verma

Branch: Cse cybersecurity

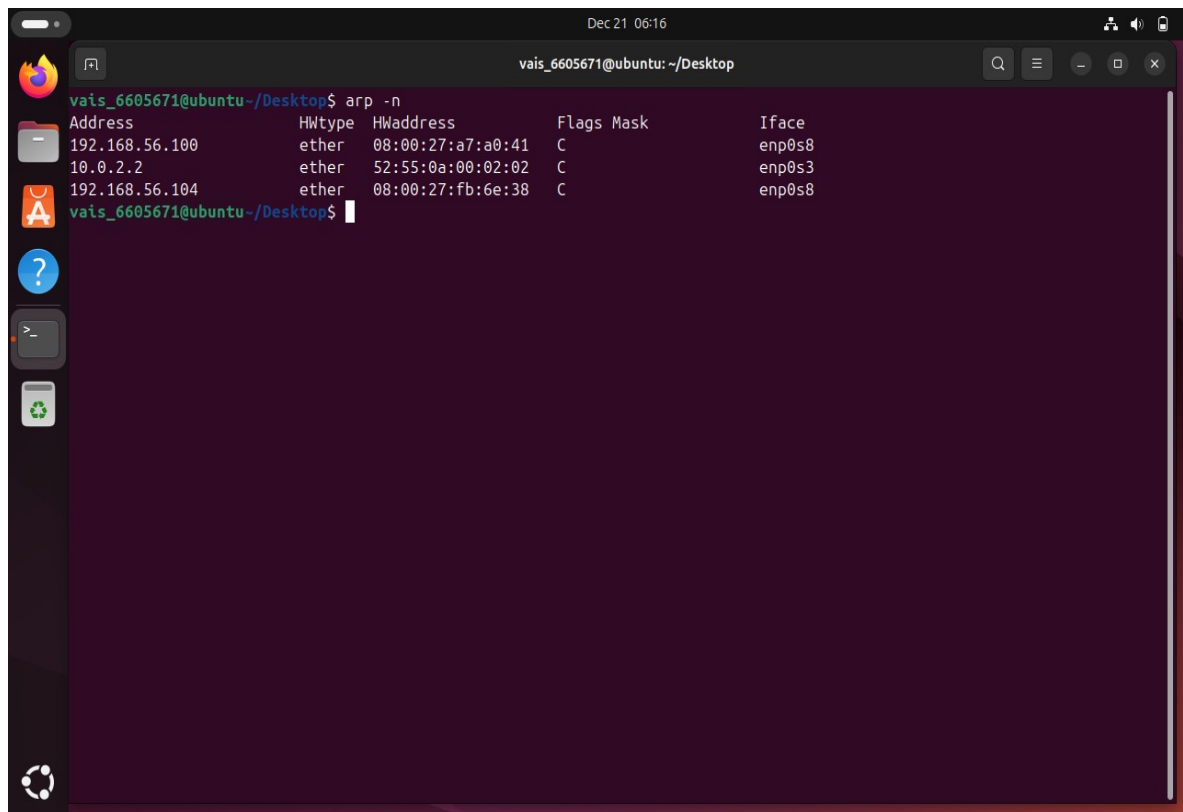
Group: G4 3rd Sem

PROJECT TITLE: ARP Spoofing Attack Demonstration

Project description: This project demonstrates an ARP Spoofing (ARP Poisoning) attack in a controlled virtual lab to highlight security weaknesses in the Address Resolution Protocol (ARP). Since ARP does not authenticate responses, it can be exploited to perform Man-in-the-Middle (MITM) attacks.

1. ARP table before communication

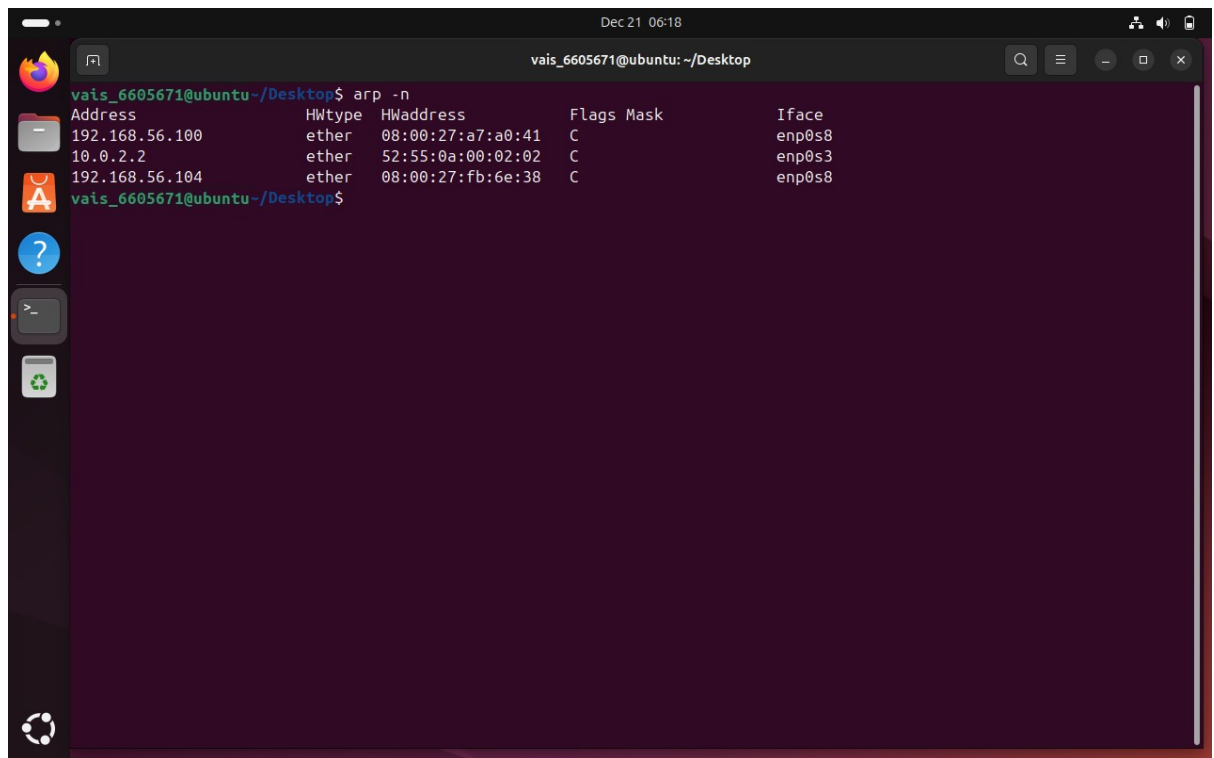
This section shows the ARP table before any active communication with the gateway. Only previously known IP-MAC address mappings are present. This represents a normal and stable ARP state.

A terminal window titled 'vais_6605671@ubuntu: ~/Desktop' showing the output of the 'arp -n' command. The output is a table with five columns: Address, HWtype, HWaddress, Flags Mask, and Iface. The table contains three entries. The terminal window has a dark purple background and a sidebar on the left with various icons.

Address	HWtype	HWaddress	Flags Mask	Iface
192.168.56.100	ether	08:00:27:a7:a0:41	C	enp0s8
10.0.2.2	ether	52:55:0a:00:02:02	C	enp0s3
192.168.56.104	ether	08:00:27:fb:6e:38	C	enp0s8

2. ARP table after normal ping

After the communication attempt, the ARP table updates automatically. New entries appear as the system resolves MAC addresses for recently contacted IPs. This reflects dynamic ARP behavior in real-time network communication.

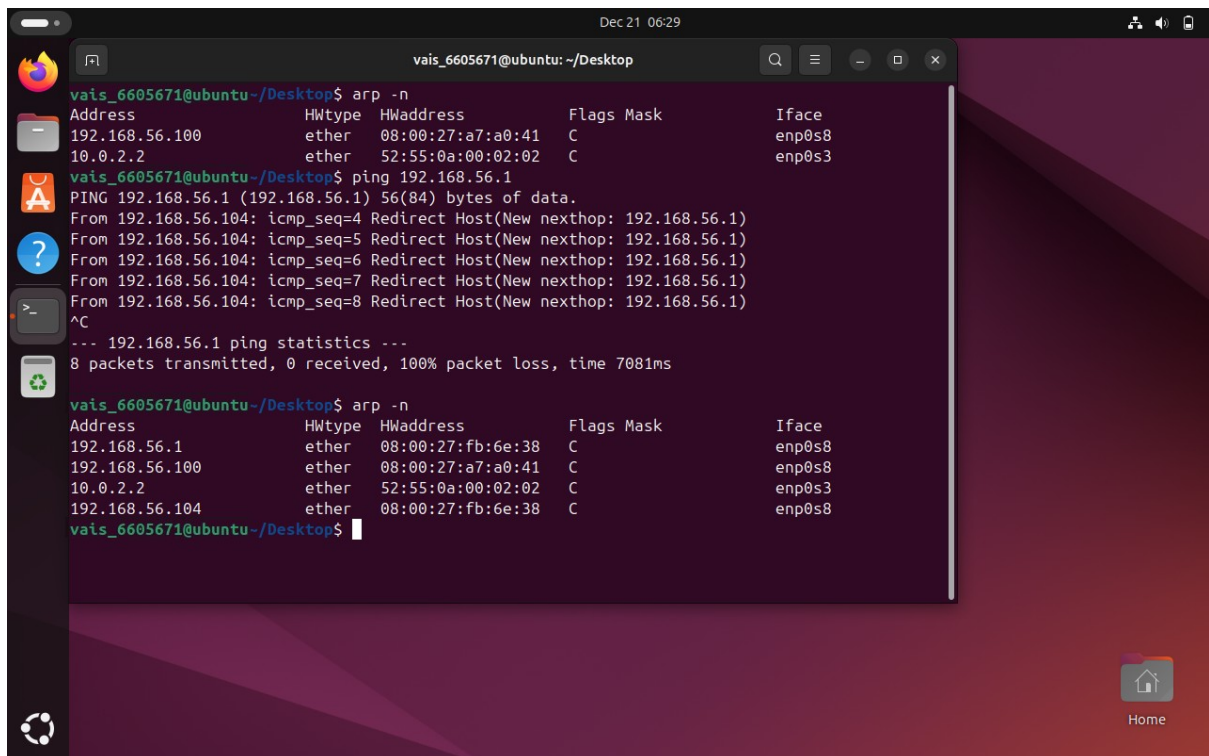


The image shows a terminal window on an Ubuntu desktop. The terminal title is 'vais_6605671@ubuntu: ~/Desktop'. The user has executed the command 'arp -n'. The output is a table with five columns: Address, HWtype, HWaddress, Flags Mask, and Iface. The table contains three entries for the IP addresses 192.168.56.100, 10.0.2.2, and 192.168.56.104, all using the 'ether' hardware type and the 'enp0s8' interface.

```
vais_6605671@ubuntu~/Desktop$ arp -n
Address          HWtype  HWaddress    Flags Mask    Iface
192.168.56.100   ether   08:00:27:a7:a0:41  C             enp0s8
10.0.2.2         ether   52:55:0a:00:02:02  C             enp0s3
192.168.56.104   ether   08:00:27:fb:6e:38  C             enp0s8
vais_6605671@ubuntu~/Desktop$
```

3.Successful ARP Spoofing Evidence

In this stage, abnormal network behavior is observed. When a ping request is sent to the gateway (192.168.56.1), ICMP Redirect Host messages appear. This indicates routing confusion or possible ARP spoofing activity, where traffic is being redirected incorrectly.



The screenshot shows a terminal window titled "vais_6605671@ubuntu: ~/Desktop" with a search bar and window controls. The terminal output is as follows:

```
vais_6605671@ubuntu~/Desktop$ arp -n
Address          HWtype  HWaddress      Flags Mask    Iface
192.168.56.100    ether    08:00:27:a7:a0:41  C             enp0s8
10.0.2.2          ether    52:55:0a:00:02:02  C             enp0s3

vais_6605671@ubuntu~/Desktop$ ping 192.168.56.1
PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.
From 192.168.56.104: icmp_seq=4 Redirect Host(New nexthop: 192.168.56.1)
From 192.168.56.104: icmp_seq=5 Redirect Host(New nexthop: 192.168.56.1)
From 192.168.56.104: icmp_seq=6 Redirect Host(New nexthop: 192.168.56.1)
From 192.168.56.104: icmp_seq=7 Redirect Host(New nexthop: 192.168.56.1)
From 192.168.56.104: icmp_seq=8 Redirect Host(New nexthop: 192.168.56.1)
^C
--- 192.168.56.1 ping statistics ---
 8 packets transmitted, 0 received, 100% packet loss, time 7081ms

vais_6605671@ubuntu~/Desktop$ arp -n
Address          HWtype  HWaddress      Flags Mask    Iface
192.168.56.1      ether    08:00:27:fb:6e:38  C             enp0s8
192.168.56.100    ether    08:00:27:a7:a0:41  C             enp0s8
10.0.2.2          ether    52:55:0a:00:02:02  C             enp0s3
192.168.56.104    ether    08:00:27:fb:6e:38  C             enp0s8
vais_6605671@ubuntu~/Desktop$
```

4.CONCLUSION

- **ARP dynamically maps IP addresses to MAC addresses.**
- **Network communication triggers ARP table updates.**
- **ICMP Redirect messages suggest abnormal routing behavior.**
- **Monitoring ARP tables is important for detecting network issues and security threats.**