Name - HARSHIL AMIT BUCH
Class - TY CSF-1
Roll Number - 14

Experiment No. 4

Detecting ARP Spoofing & Understanding MITM Attacks

Aim:

Understand ARP, detect ARP spoofing, and simulate defensive steps against Man-in-the-Middle (MITM) attacks in a safe, controlled environment.

Requirements:

1. Kali Linux (Virtual Machine or physical machine)
2. Tools: Wireshark, tcpdump, arpwatch, nmap
3. Isolated lab network (VirtualBox/VMware internal network)
4. Two or more virtual machines (attacker, victim, gateway simulation)

Procedure:

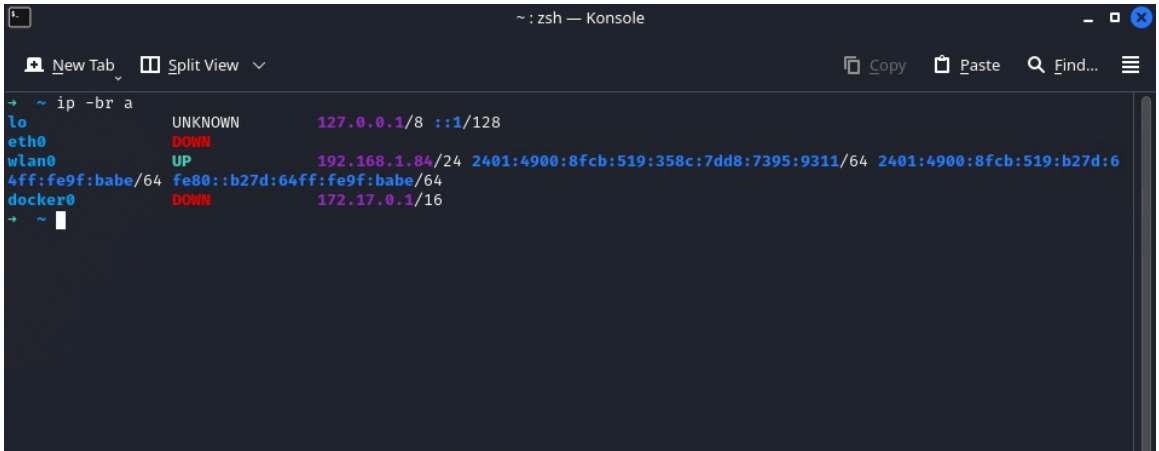
Step 1: Install Required Tools

Update system and install tools:

sudo apt update
sudo apt install -y wireshark tcpdump arpwatch arping nmap iproute2 net-tools

Step 2: Check Network Interface

Find your active interface:



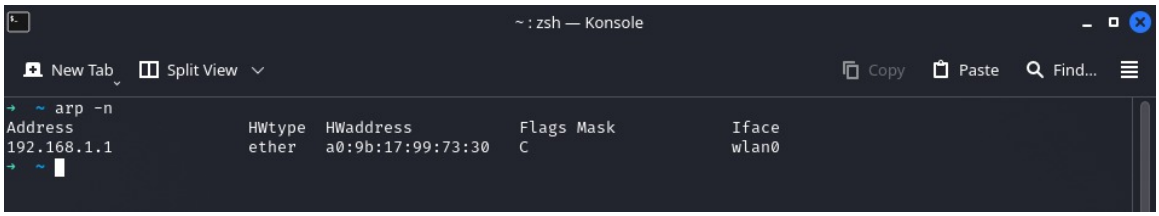
ip -br a
(Example: eth0, ens33, wlan0)

Step 3: View ARP Table

Display ARP cache:

ip neigh show

arp -n



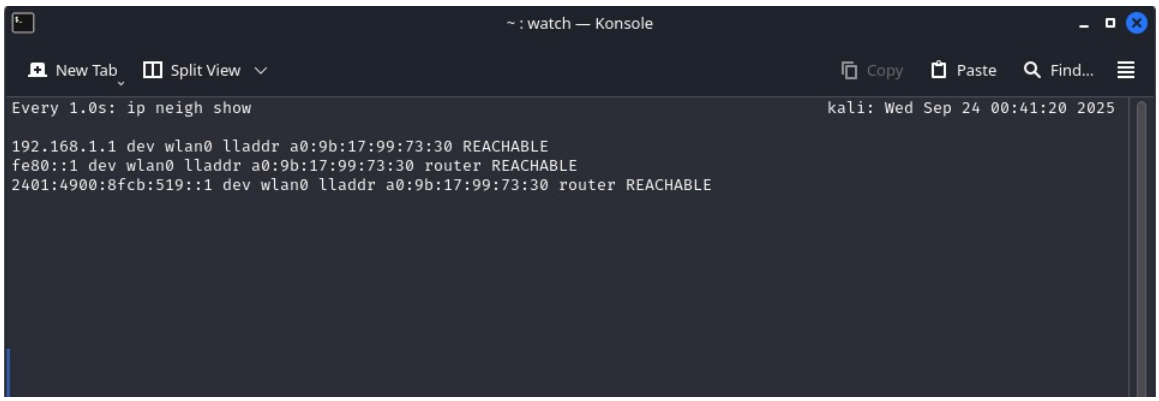
Observe IP and MAC mappings.

Step 4: Monitor ARP Table in Real Time

Run:

watch -n 1 "ip neigh show”

Check for changes in MAC addresses for same IP.

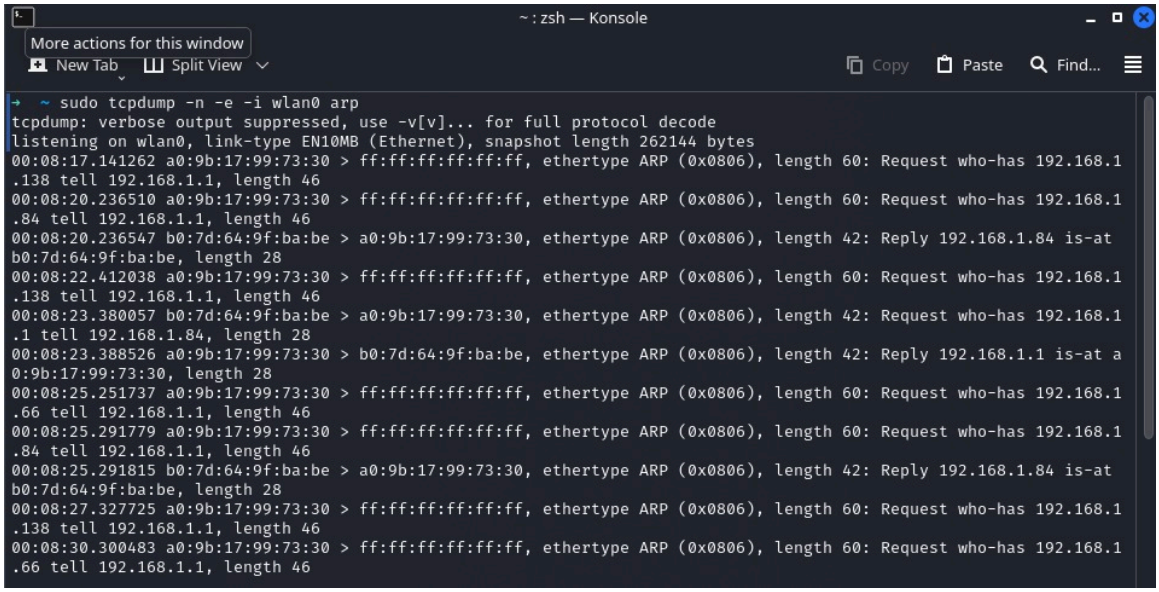


Step 5: Capture ARP Packets

Use tcpdump:

sudo tcpdump -n -e -i <interface> arp

Indicators of ARP spoofing:
- Multiple ARP replies without requests
- Gateway IP mapping to unusual MAC addresses

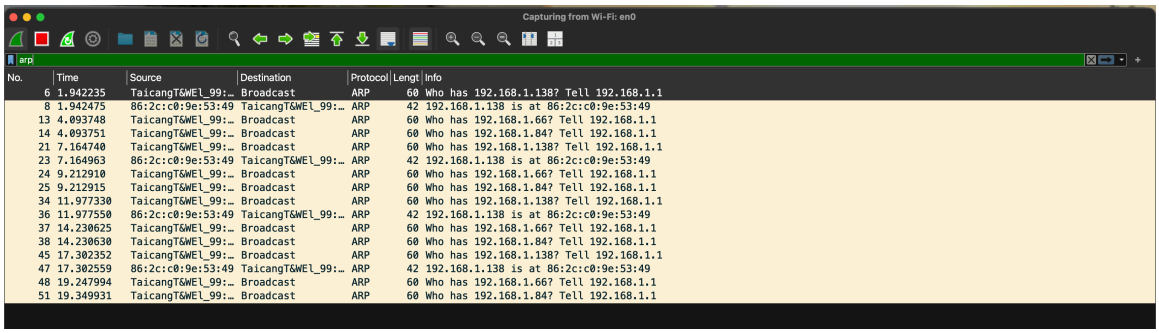


Step 6: Wireshark Analysis

Start Wireshark and apply filter:

arp

Look for duplicate IP and unsolicited ARP replies.

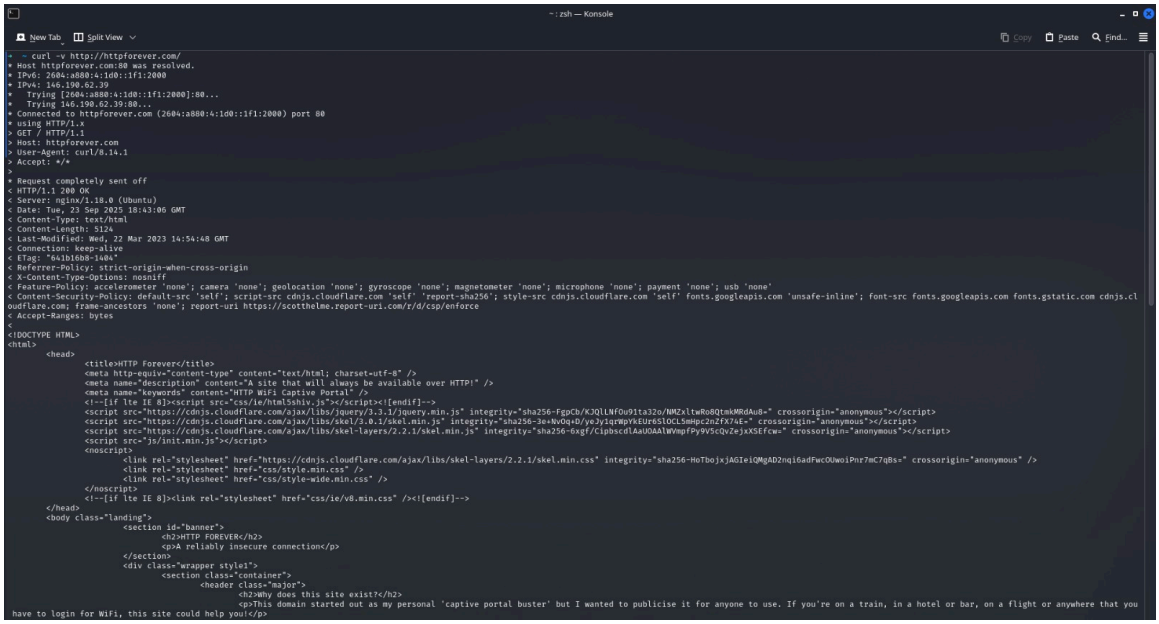


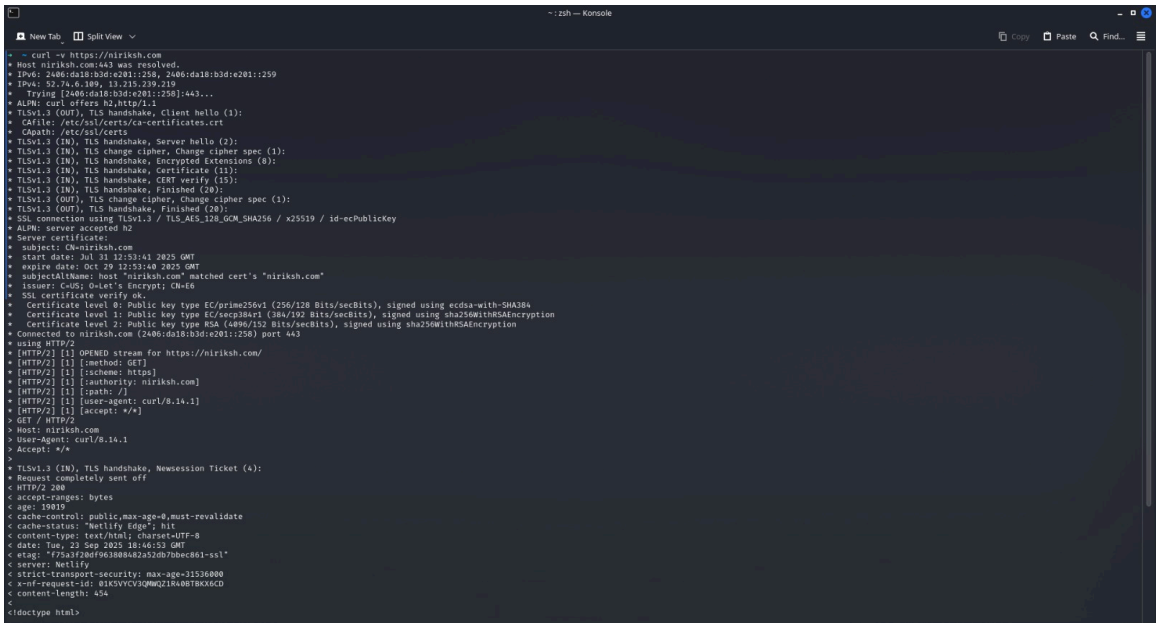
Step 7: Test HTTP vs HTTPS Security

Compare unencrypted and encrypted traffic:

curl -v http://example.com
curl -v https://example.com

Discuss how HTTPS prevents MITM attacks.

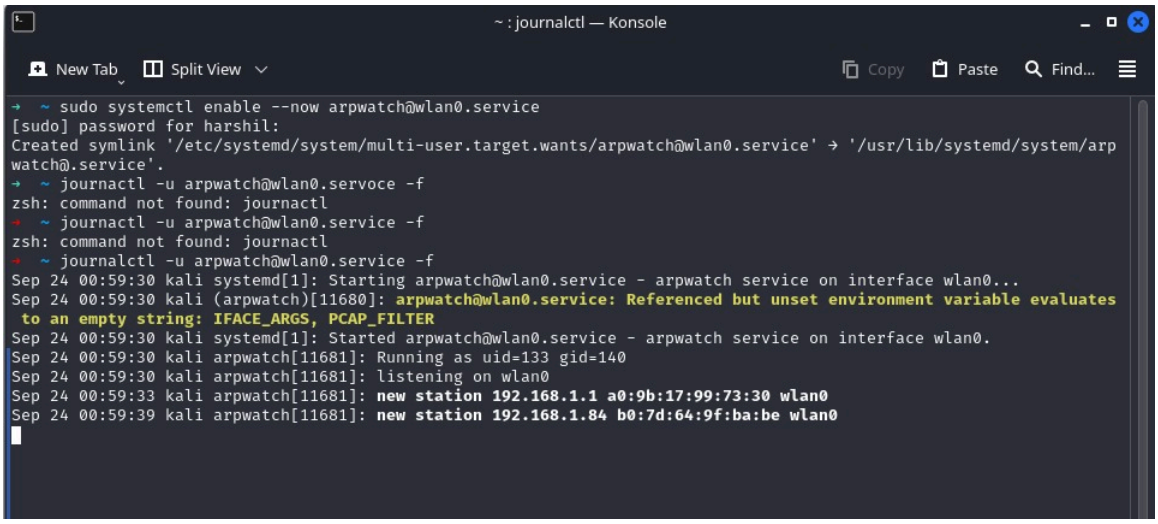




Step 8: Continuous Monitoring with arpwatch

Enable arpwatch service:

sudo systemctl enable --now arpwatch@<interface>.service
journalctl -u arpwatch@<interface>.service -f



Observe new MAC and IP changes.

Step 9: Network Scanning

Run a ping sweep:

nmap -sn 192.168.0.0/24

Compare results with your expected network map.

Step 10: Static ARP Entry (Defense)
Get gateway IP and MAC:

ip route | grep default
ip neigh show | grep <gateway_ip>

Set static entry:
sudo ip neigh replace <gateway_ip> lladdr <gateway_mac> nud permanent dev <interface>

Remove static entry:
sudo ip neigh del <gateway_ip> dev <interface>

Expected Outcomes:
1. Students will learn how to check ARP tables and monitor changes.
2. Detect unusual ARP behavior using tcpdump and Wireshark.
3. Understand the difference between HTTP and HTTPS security.
4. Use arpwatch for ARP spoof detection.
5. Apply static ARP entries for security.

Viva/Review Questions:
1. What is ARP and why is it vulnerable?
2. How does ARP spoofing enable MITM attacks?
3. Why does HTTPS reduce MITM risk?
4. What is the purpose of static ARP entries?
5. Which network configurations prevent ARP spoofing?