Module 6: ARP Poisoning and Detection

# Objective:

The objective of this practical exercise is to perform an ARP poisoning attack using Ettercap and to monitor and detect ARP traffic using Wireshark.

# Setup Environment:

Network with at least three devices:

* - Attacker machine (with Ettercap installed).
* - Victim machine.
* - Mobile Hotspot.

Installed Wireshark and Ettercap on the attacker machine.

# Perform ARP Poisoning:

1. Open Ettercap on the attacker machine and run it in root mode.
2. Scan for hosts in the network: Click on 'Hosts' → 'Scan for Hosts'.
3. List detected hosts: Click on 'Hosts' → 'Hosts List'.
4. Select the victim's IP as target 1.
5. Select the gateway's IP as target 2.
6. Begin ARP poisoning: Click on 'Mitm' → 'Arp Poisoning' → Select 'Sniff Remote Connections'.
7. Start the attack by clicking 'Start'.

# Monitor ARP Packets in Wireshark:

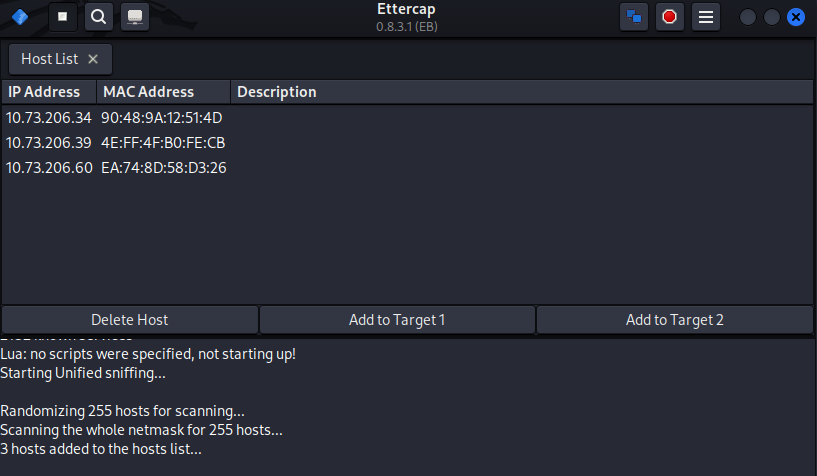
Open Wireshark on the attacker or victim machine. Start capturing packets on the interface connected to the network.

# Screenshot Evidence:

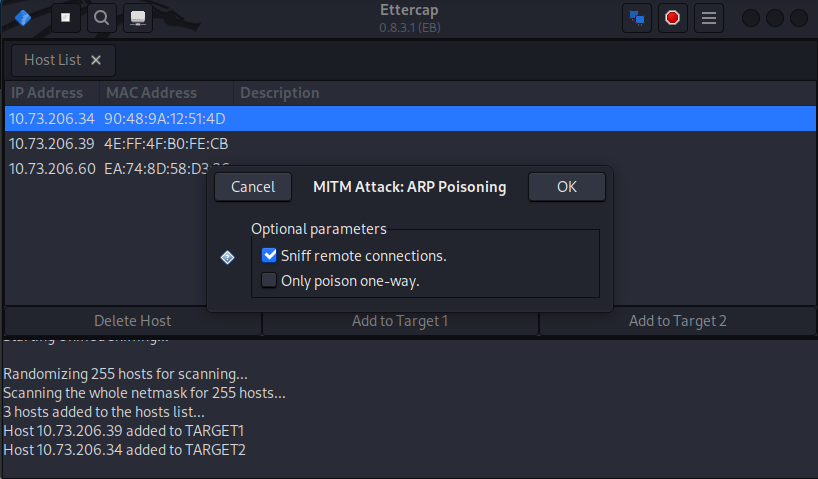
Ettercap Setup Interface.



Ettercap Host List Showing Detected Devices.



ARP Poisoning Configuration with Victim and Gateway Selected.



Wireshark Showing ARP Packets with Altered MAC Addresses.

