Name: Kunal Demla Roll No: 102003088 Subgroup: 3COE4

ARP Poisoning

ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses. Because the ARP protocol was designed purely for efficiency and not for security, ARP Poisoning attacks are extremely easy to carry out as long as the attacker has control of a machine within the target LAN or is directly connected to it.

In this experiment, we will simulate ARP poisoning by creating a virtual LAN network which will consist of an attacker machine, a victim machine and a default gateway.

	Machine A(Attacker)	Machine B(Victim)	Default Gateway
IP Address	172.16.55.165	172.16.58.88	172.16.48.1
MAC Address	18:26:49:4c:f5:31	c8:b2:9b:b1:7d:7b	04:d5:90:6e:91:19

Our goal is to map gateway's IP address with attacker machine's MAC address, such that all packets sent from victim to gateway are routed to attacker's machine.

For doing the poisoning, we need to install some tools.

1. Wireshark: Wireshark is a packet sniffer and analysis tool. It captures network traffic from ethernet, Bluetooth, wireless (IEEE. 802.11), token ring, and frame relay connections, among others, and stores that data for offline analysis.
2. Hexedit: To manipulate the packet.
3. File2cable: To send manipulated packets to the victim.

   Now we will send an ARP reply packet from attacker machine to victim machine which will contain the MAC address of attacker machine but IP address of the gateway.

   ARP poisoning is done.

Name: Kunal Demla Roll No: 102003088 Subgroup: 3COE4