ARP Poisoning/Spoofing (aka Man in the middle attack)

ARP → Address Resolution Protocol is responsible for finding the MAC (hardware) address related to a specific IP address. It works by broadcasting an ARP query, "Who has this IP address? Tell me". And the response is of the form, "The IP address is at this MAC address"

So, ARP is a technology responsible for allowing devices to identify themselves on a network.

ARP Poisoning/Spoofing or MITM attack is a type of attack that involves network jamming/manipulating by sending malicious ARP packet to the default gateway.

ARP analysis in a nutshell:

- Works on the local network
- Enables the communication between MAC addresses
- Not a secure protocol
- Not a routable protocol
- It doesn't have an authentication function
- Common patterns are request and response, announcement and gratuitous packets.

Wireshark: Global search
↳ arp

In ARP packets, the opcode tells the ARP type:

- arp.opcode==1 → ARP Request (Who has IPX? Tell Y)
- arp.opcode == 2 → ARP Reply/Response (IP X is at MAC ...)

ARP Scanning is when something sends many ARP requests to discover which IPs are alive on the local subnet

So, by using arp.opcode==1, we can take a look at what IP address is sending request for many ~~sub~~ sequential IPs
And, we can see the high rate of requests in a short time.

ARP poisoning (ARP spoofing) is when ~~the~~ an attacker sends fake ARP replies so victim map:

Gateway IP → attacker MAC
Victim IP → attacker MAC

What we watch for:

- Lots of ARP replies (arp.opcode==2) that are unsolicited (replies when nobody asked)
- Same IP being 'at' different MAC addresses over time
- Duplicate - address warning

ARP flooding is when ARP packets are spammed at high volume (cause CPU or network noise and disruptions)

- We will use:
  - Very high ARP packet rate
  - Often many requests + Broadcast Behavior

Overall

`arp.opcode == 1` → requests
`arp.opcode == 2` → Reply
`arp.dst.hw_mac == xx:xx:...` → Destination MAC

`arp.duplicate-address-detected` or `arp.duplicate-address-frame`

- Wireshark flags possible duplicate IP address usage on LAN
- This triggers when Wireshask sees:
  - Two different MACs claiming the same IP
  - ARP probes/announcements that indicate a conflict

- This happens from:
  - Legit misconfig
  - VM cloning mistake
  - ARP spoofing

`((arp) && (arp.opcode==1)) && (arp.src.hw_mac == target-mac-address)`

This shows ARP requests coming from specifically from one MAC address

- So we can see if the device is scanning, flooding, etc

Exercise

1) What is the numbes of ARP requests crafted by the attacker?

- Selected the marked packet from wireshask which having multiple IPs
- And got the sender's MAC address from the packet
- And used this filter:

((arp)&&(arp-~~code~~ opcode==1)&&(arp.src.hw_mac==00:0c:29:e2:18:b4)

request

attacker MAC

2) what is the numbes of HTTP packet received by the attacker

eth.dst==(Attacker mac) && http

3) what is the numbes of sniffed username and password entries?

looked at the POST /userinfo.php and counted the entries, ~~z~~especially those followed by 302 Found

4) what is the password of the 'Client986'?

Packet no: 1668

5) what is the comment provided by the 'Client354'?

Packet no: 2320