Arp Poisoning Using Ettercap

An Arp Poisoning attack is a Man-in-the-Middle attack where an Attacker tricks both a target and a gateway into routing traffic through the Attacker. The Attacker "poisons" the arp cache on both machines in order to receive traffic and then passes it along.

Party	IP	MAC
Victim	192.168.0.112	F3:2D:5D:19:6C:B1
Attacker	192.168.0.22	34:23:54:FF:CB:DA
Gateway	192.168.0.1	21:27:44:B3:A3:D9

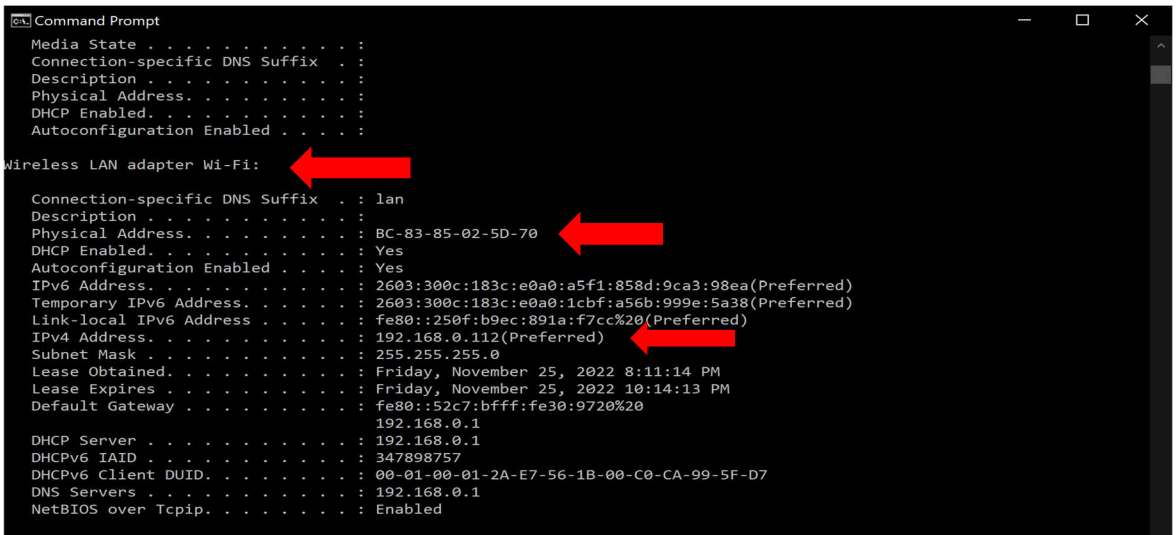
The attacker will broadcast to the target "192.168.0.1 (Gateway IP) is at 34:23:54:FF:CB:DA (Attacker MAC). This will cause the Victim to associate 192.168.0.1 with the Attacker's machine. The attacker will then broadcast to the gateway that IP 192.168.0.112 (Target IP) belongs to MAC address 34:23:54:FF:CB:DA (Attacker MAC address) In doing so, the attacker will now stand in the middle of the Victim and Gateway. They can then view traffic sent between the two.

Resources Needed:

- VMware
- Kali Linux VM
- A target OS (Windows is used in this example)
    - Has Wireshark installed

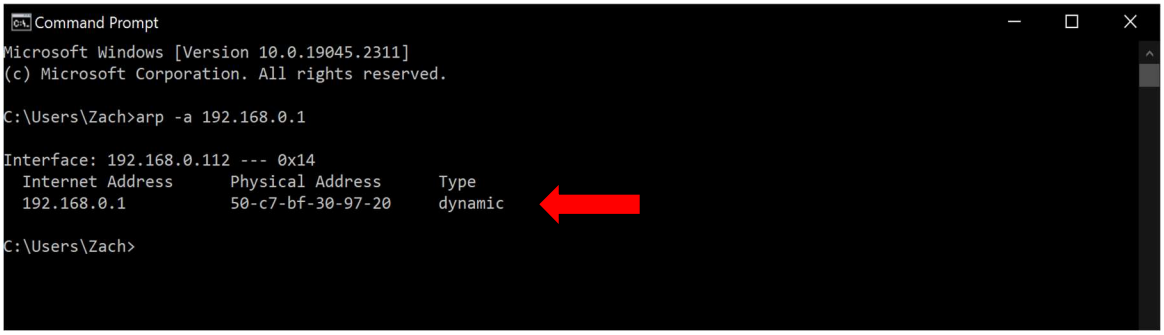
I. Setting up the Target machine

1) Boot up the Target machine (Windows)
2) Open Command Prompt and find your IP address.
    a. >ipconfig /all
        i. -Look for the wireless interface you are using.
            1. Record your IP address, MAC address (Physical address), and your default gateway IP



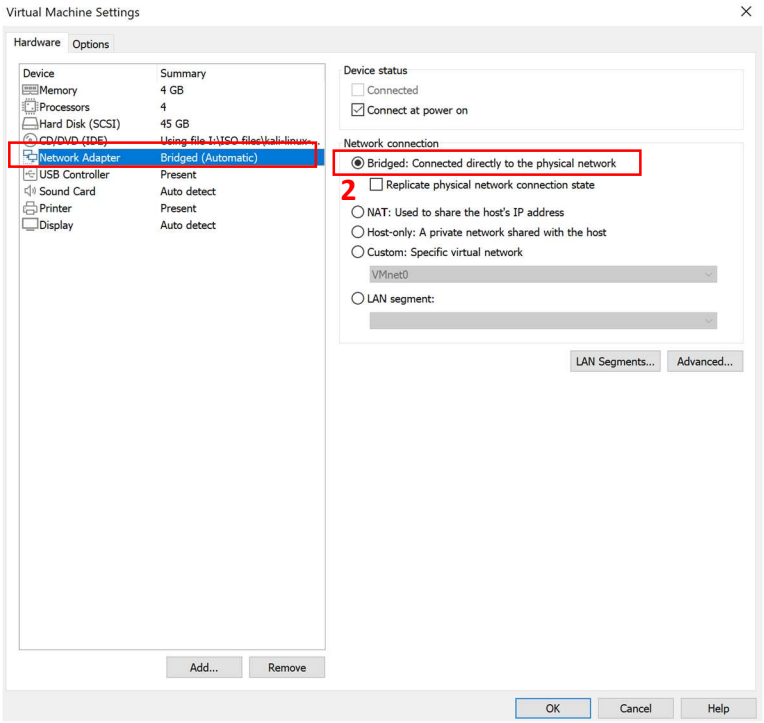
b. >arp -a <gateway IP address>

i. -Record the MAC address associated with the gateway IP address



II. Setting up the Attack machine

1) In VMware, change the network adapter to “Bridged mode” in the machine settings



2) Boot up the Attack machine
3) Open a terminal and type

a. >ifconfig

i. -Record the IP address and MAC address associated with the interface you are using

- For myself, I will be using “wlan0” but it may be “eth0” for you

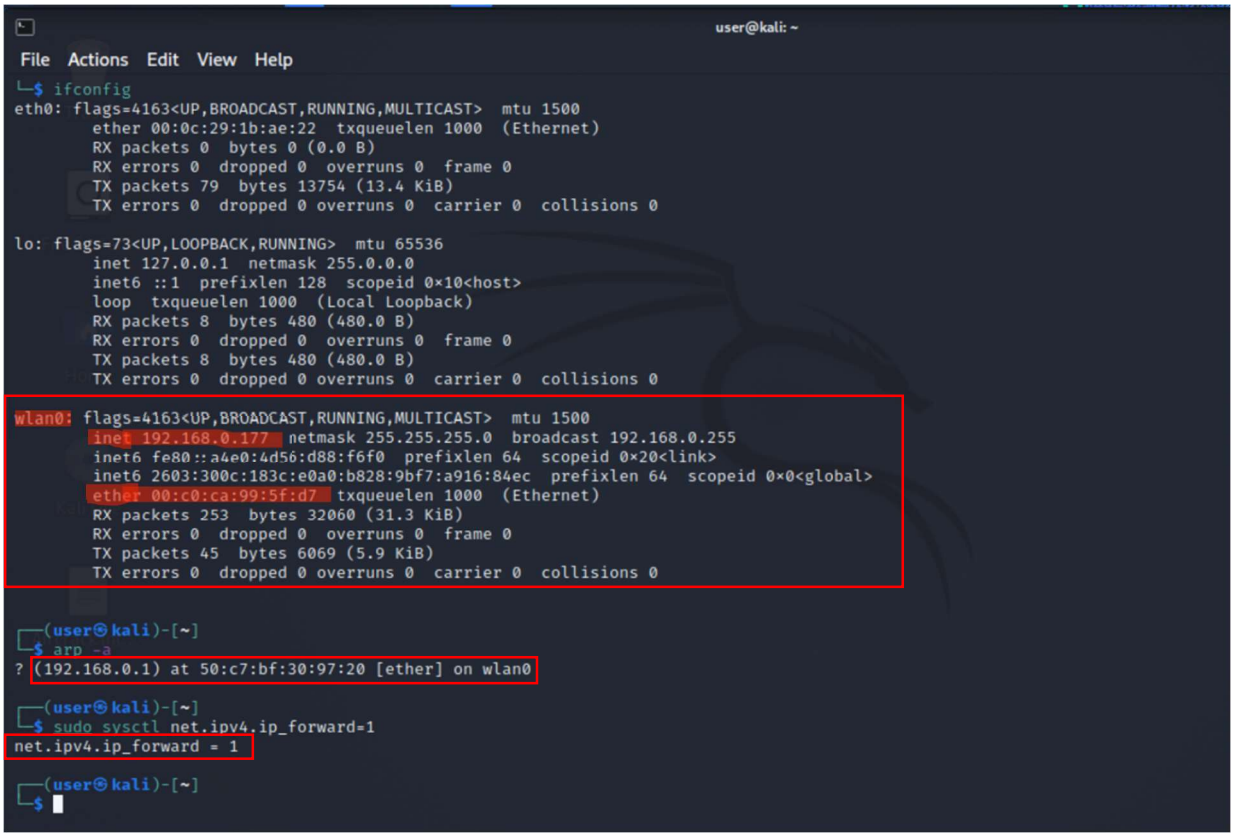
1. -The MAC address may be referred to as “ether XX:XX:XX:XX:XX:XX”

b. >arp -a

i. – Like earlier, recognize that the default gateway IP address and MAC address should be the same as earlier.

c. >sudo sysctl net.ipv4.ip_forward=1

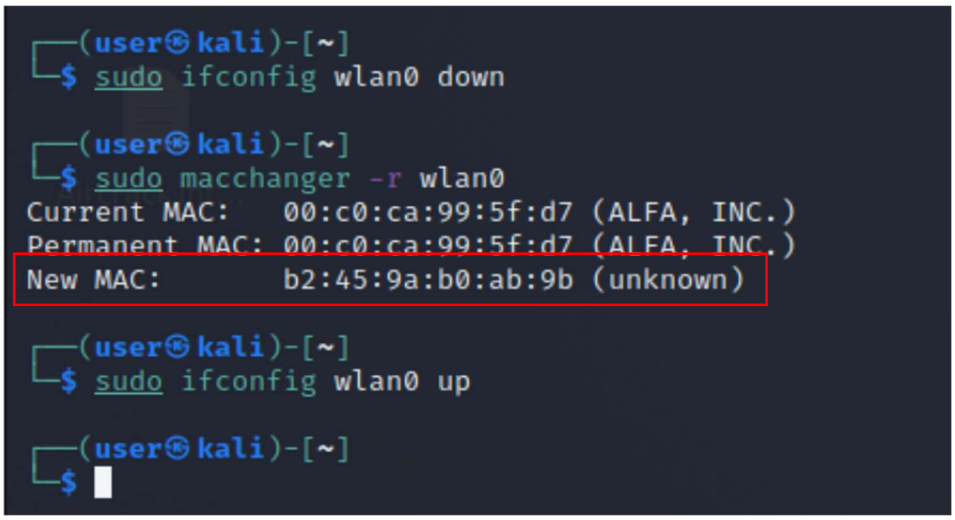
i. -This command allows us toward on traffic to either party. Without doing so, traffic will be sent to the Attack but not forwarded.



III. Spoof your MAC address

1) In the terminal type:
   a. >sudo ifconfig <interface> down
   b. >sudo macchanger -r <interface>
   c. >sudo ifconfig <interface> up

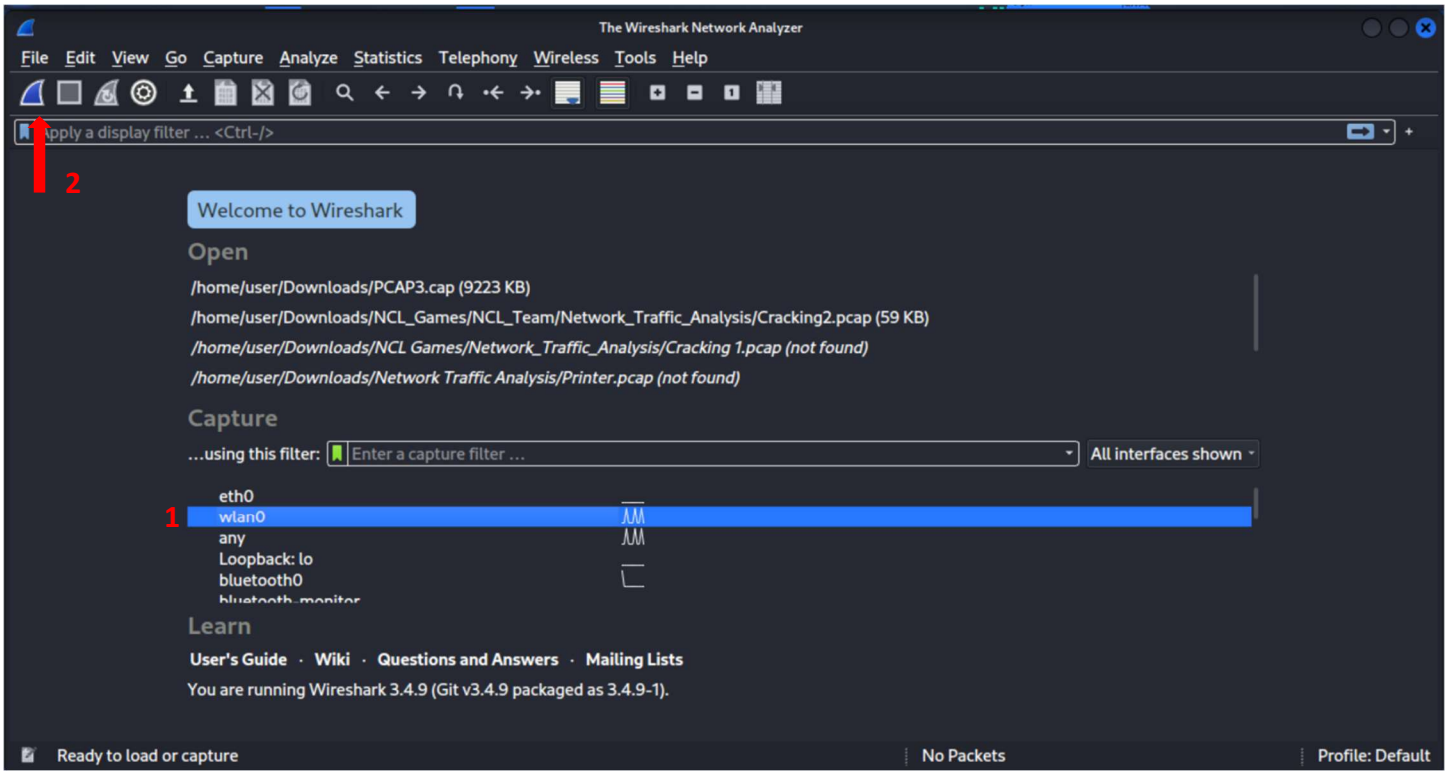
-Now your MAC address should change for your interface



IV. Open Wireshark

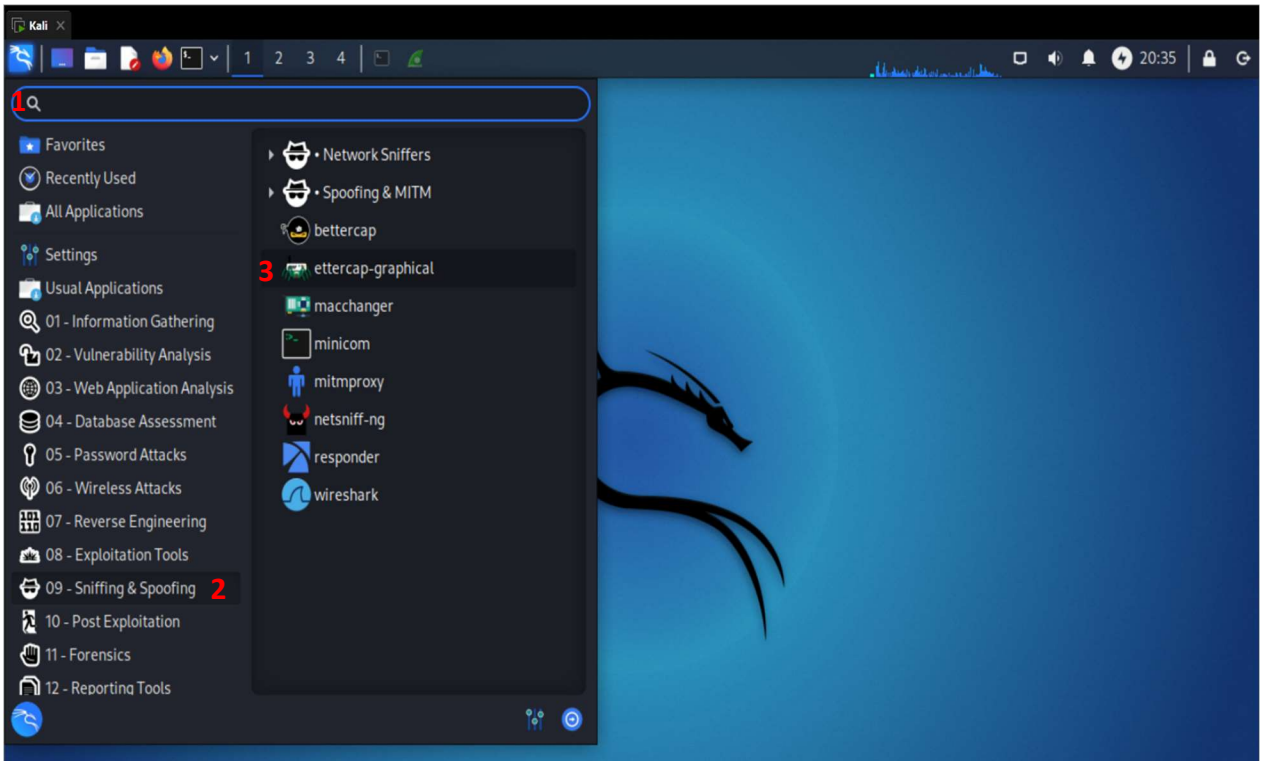
1) Click on the Kali logo on the Desktop
   a. Type “wireshark” in the search field
      i. Click on “wireshark”

2) On the Wireshark window, select the interface from earlier then start capturing packets



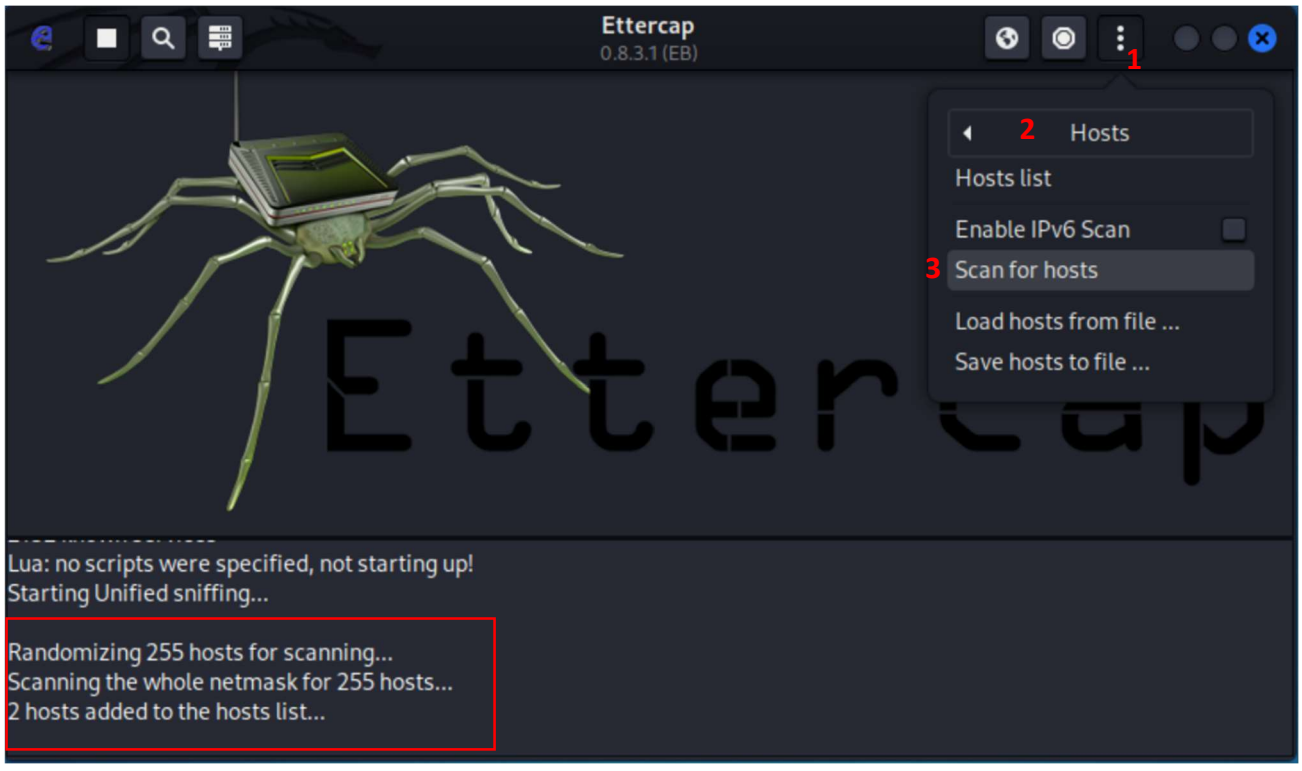
V. Using Ettercap to perform a MITM Arp Poisoning attack

1) Open Ettercap (graphical)
    a. Click on the Kali logo on the top right of the Desktop and expand the “09 - Sniffing & Spoofing“ directory
        i. You should see “ettercap-graphical”
            1. Click to open
                a. Type password

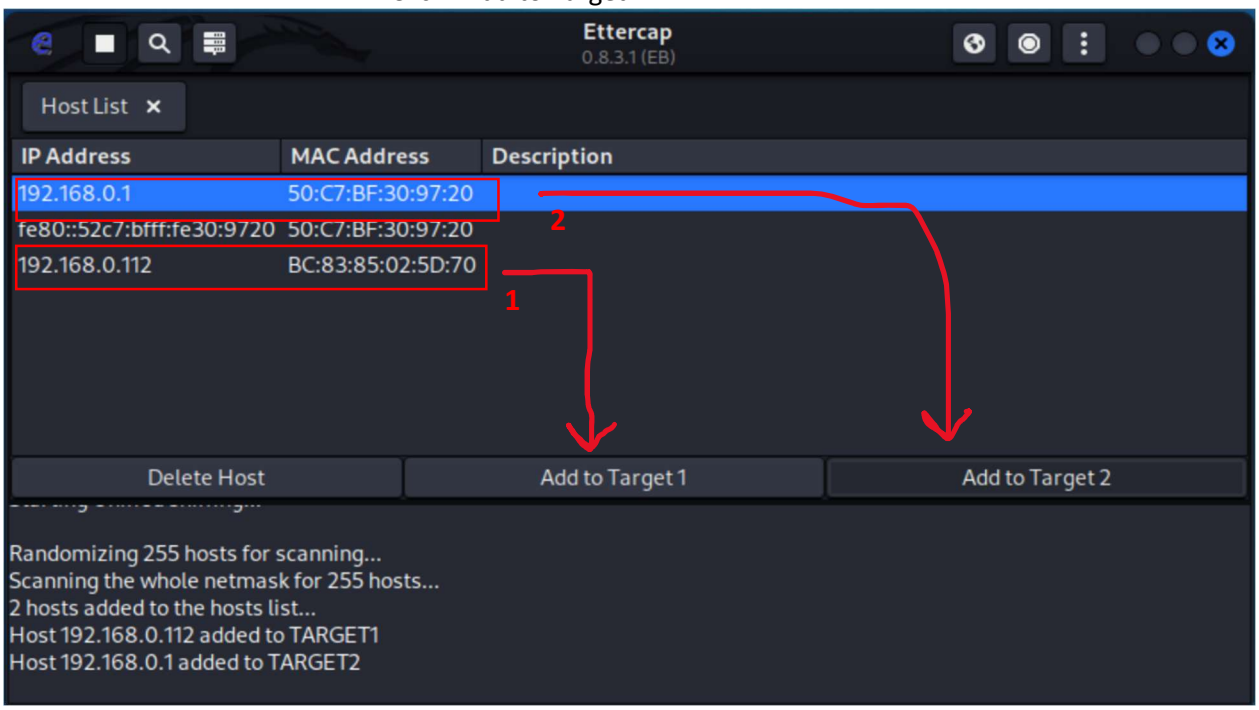


2) When Ettercap opens;
    a. Select the interface under the drop-down menu of “Primary Interface”
    b. Hit the check mark

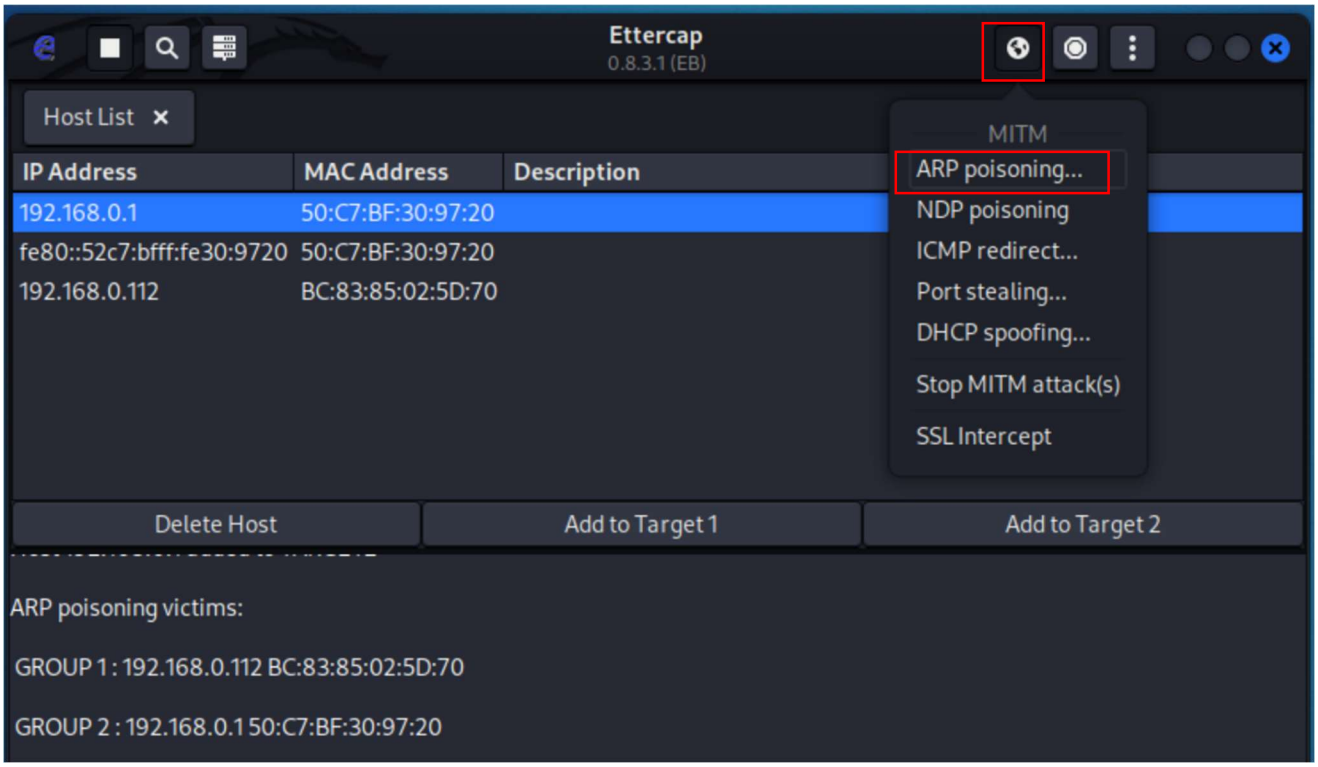
3) Scan for hosts
    a. Click on the 3 vertical dots> Hosts>Scan for hosts
        i. This will scan the network for hosts and add them to a list

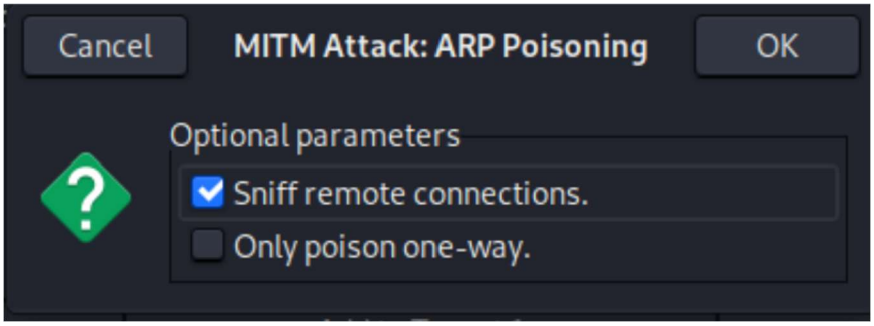


4) Select targets to poison
    a. Click on the 3 vertical dots> Hosts>Hosts list
        i. Now select from the list the IP address of the client you want to poison
            1. Click “Add to Target 1”
        ii. Select the gateway IP address you want to poison
            1. Click “Add to Target 2”



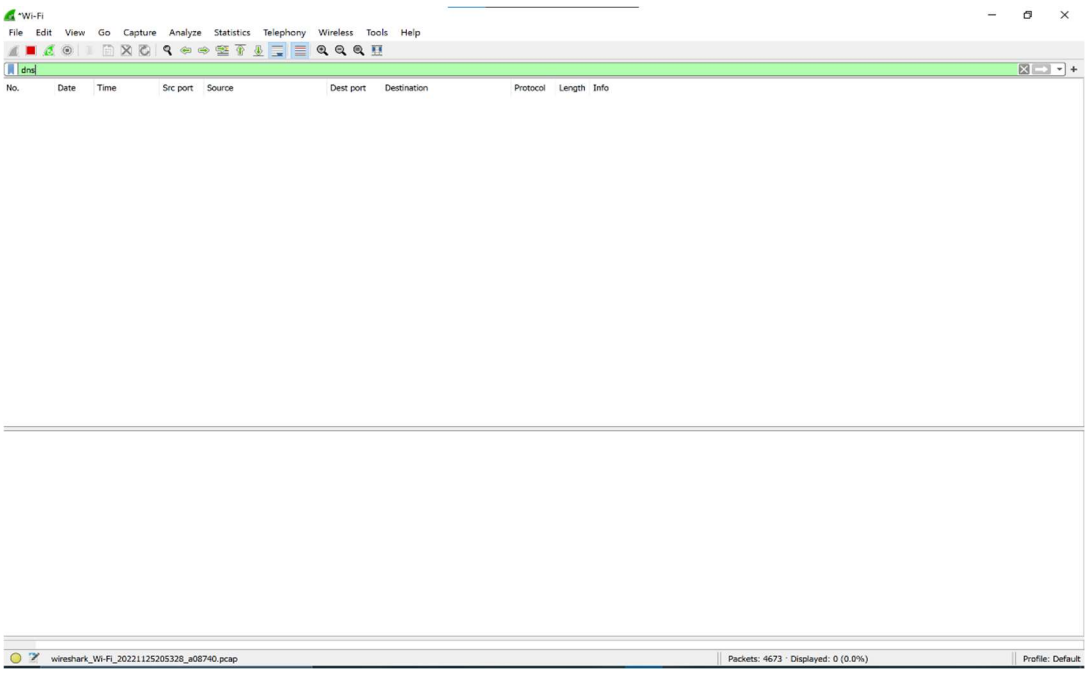
5) Begin the arp poison attack
    a. Click on the MitM icon that looks like a “world” 2 icons left of the 3 dots we clicked on earlier
        i. Select “ARP poisoning….”
            1. For optional parameters, check mark “Sniff remote connections.”
                a. Hit “OK” to begin





VI. View Wireshark on Attack machine

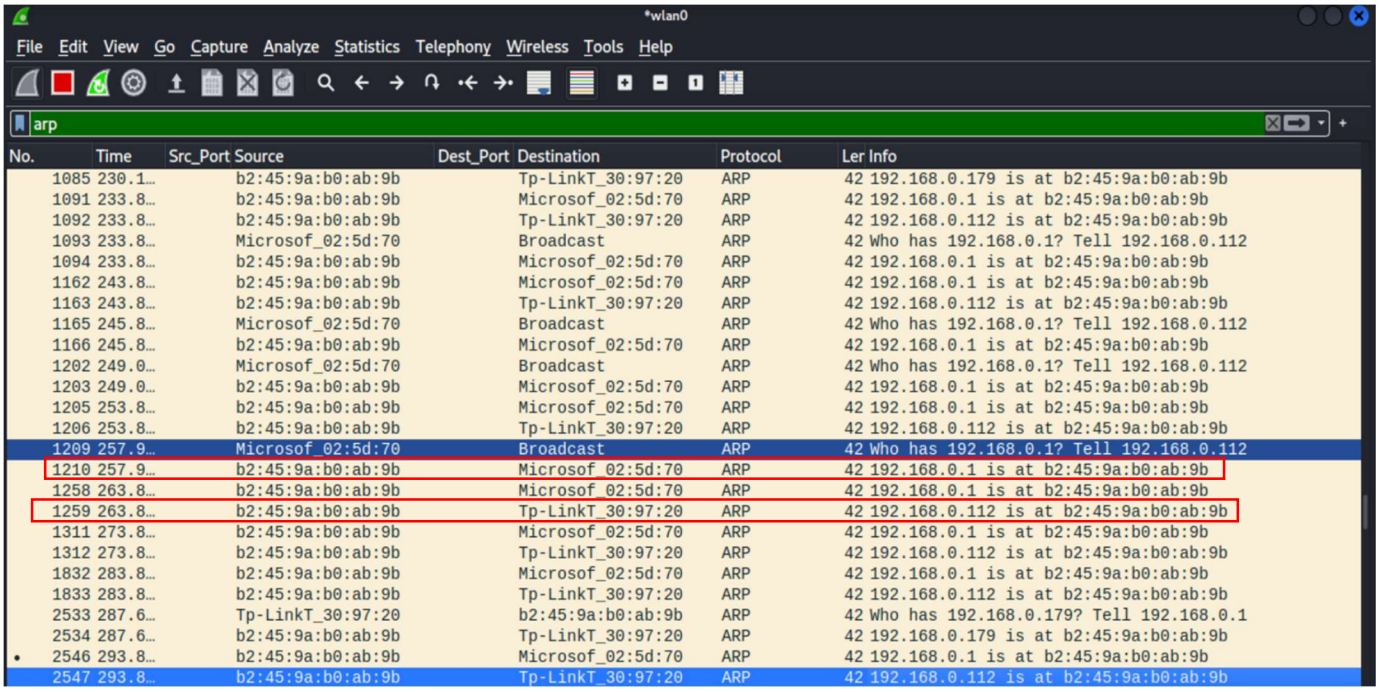
1) In the display filter, put a “dns” filter on the attack machine



2) On the Target machine open a website:
   - **a.** HTTPS
   - **b.** HTTP
3) Go back to Wireshark
   a. HTTPS encrypts traffic, but you can see websites that are being browsed
   b. HTTP traffic is NOT encrypted. If someone logs into a website the credentials will be in plain view

   **If the target is using VPN, traffic will be encrypted and we will not be able to see what websites they go to.

4) Put the display filter “arp” on the attack machine
   a. We can see that the Attack machine is saying that both the gateway IP and the Target IP belong to the Attacker’s MAC address



V. Stop the ARP Poisoning

1) Click on the icon next to the MitM icon from earlier to stop the attack

END