

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)
 - o 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

```
Command Prompt
Media State . . . . . :
Connection-specific DNS Suffix . :
Description . . . . . :
Physical Address. . . . . :
DHCP Enabled. . . . . :
Autoconfiguration Enabled . . . . :
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : lan
Description . . . . . :
Physical Address. . . . . : BC-83-85-02-5D-70
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2603:300c:183c:e0a0:a5f1:858d:9ca3:98ea(Preferred)
Temporary IPv6 Address. . . . . : 2603:300c:183c:e0a0:1cbf:a56b:999e:5a38(Preferred)
Link-local IPv6 Address . . . . . : fe80::250f:b9ec:891a:f7cc%20(Preferred)
IPv4 Address. . . . . : 192.168.0.112(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, November 25, 2022 8:11:14 PM
Lease Expires . . . . . : Friday, November 25, 2022 10:14:13 PM
Default Gateway . . . . . : fe80::52c7:bfff:fe30:9720%20
192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 347898757
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-E7-56-1B-00-C0-CA-99-5F-D7
DNS Servers . . . . . : 192.168.0.1
NetBIOS over Tcpip. . . . . : Enabled
```

b. `>arp -a <gateway IP address>`

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

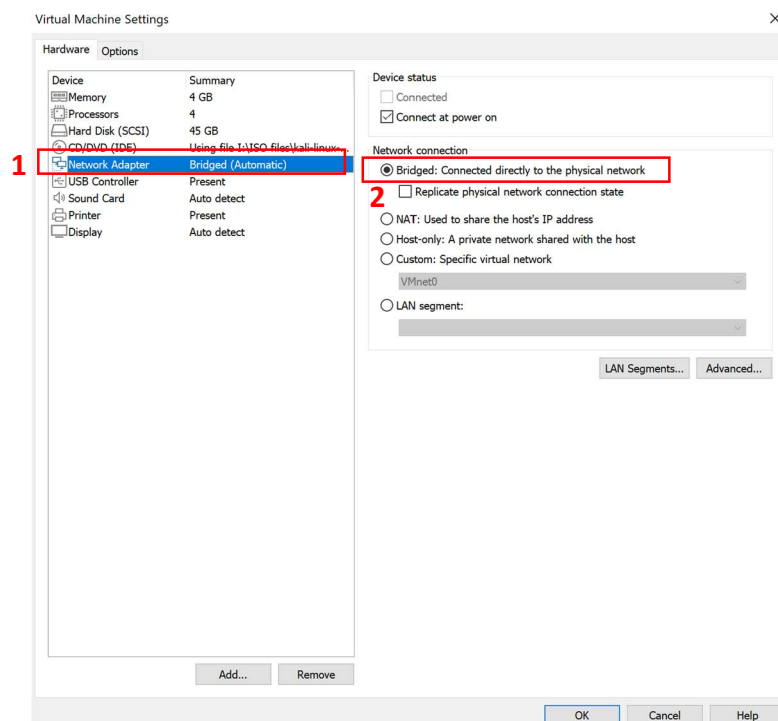
```
Command Prompt
Microsoft Windows [Version 10.0.19045.2311]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Zach>arp -a 192.168.0.1

Interface: 192.168.0.112 --- 0x14
    Internet Address      Physical Address      Type
    192.168.0.1           50-c7-bf-30-97-20    dynamic
```

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.

```
user@kali: ~  
File Actions Edit View Help  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    ether 00:0c:29:1b:ae:22 txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 79 bytes 13754 (13.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.0.177 netmask 255.255.255.0 broadcast 192.168.0.255  
    inet6 fe80::a4e0:4d56:d88:f6f0 prefixlen 64 scopeid 0<link>  
    inet6 2603:300c:183c:e0a0:b828:9bf7:a916:84ec prefixlen 64 scopeid 0<global>  
    ether 00:c0:ca:99:5f:d7 txqueuelen 1000 (Ethernet)  
    RX packets 253 bytes 32060 (31.3 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 45 bytes 6069 (5.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(user@kali)-[~]  
$ arp -a  
? (192.168.0.1) at 50:c7:bf:30:97:20 [ether] on wlan0  
  
(user@kali)-[~]  
$ sudo sysctl net.ipv4.ip_forward=1  
net.ipv4.ip_forward = 1  
  
(user@kali)-[~]  
$
```

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`

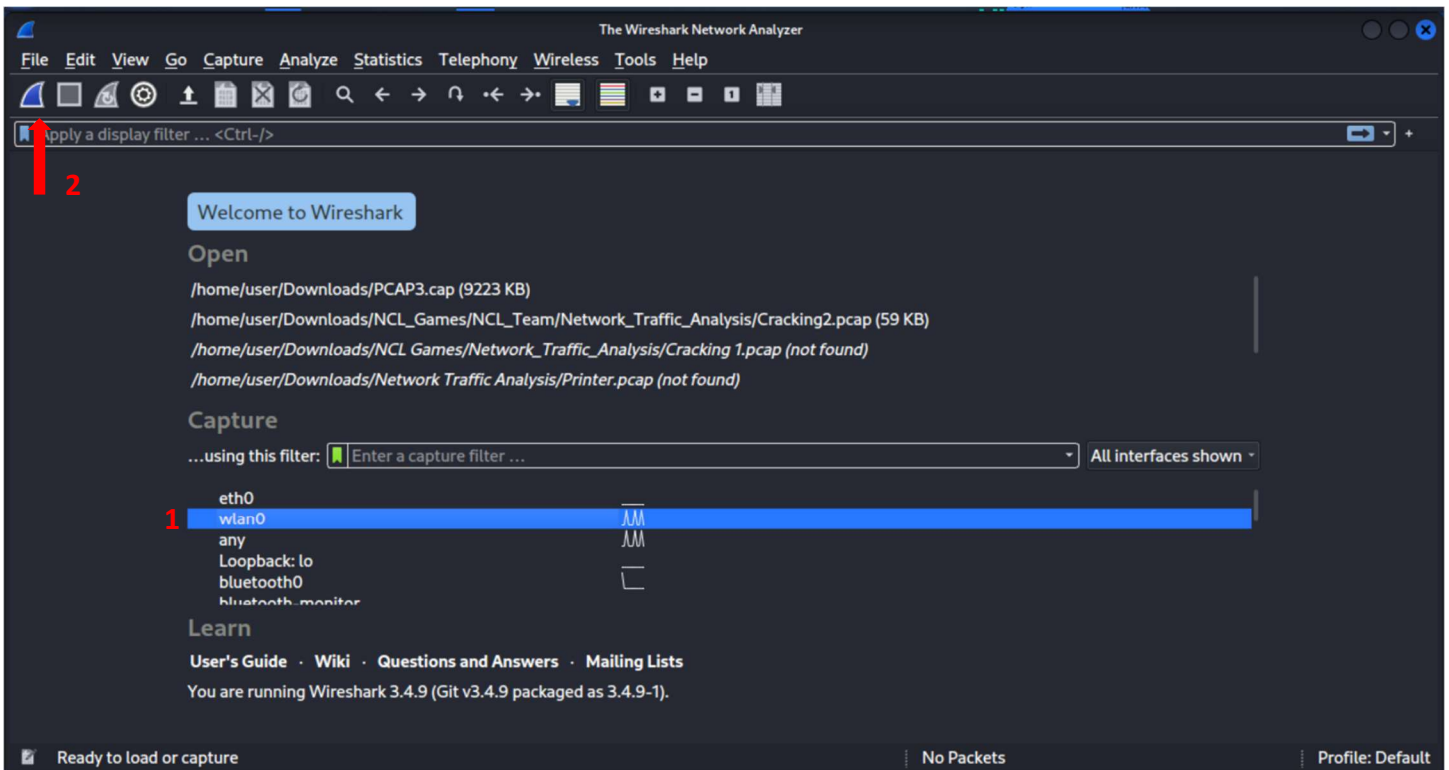
-Now your MAC address should change for your interface

```
(user@kali)-[~]  
$ sudo ifconfig wlan0 down  
  
(user@kali)-[~]  
$ sudo macchanger -r wlan0  
Current MAC: 00:c0:ca:99:5f:d7 (ALFA, INC.)  
Permanent MAC: 00:c0:ca:99:5f:d7 (ALFA, INC.)  
New MAC: b2:45:9a:b0:ab:9b (unknown)  
  
(user@kali)-[~]  
$ sudo ifconfig wlan0 up  
  
(user@kali)-[~]  
$
```

IV. Open Wireshark

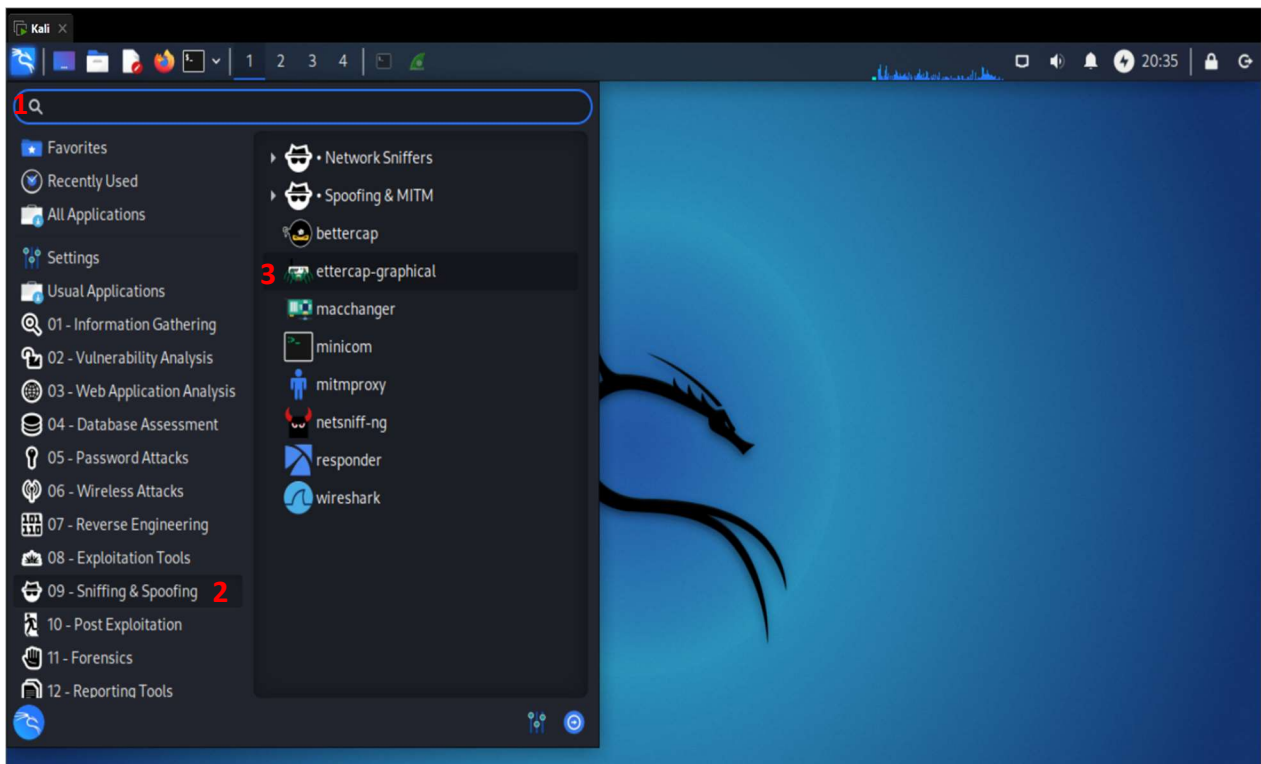
- 1) Click on the Kali logo on the Desktop
 - a. Type "wireshark" in the search field
 - i. Click on "wireshark"

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



V. Using Ettercap to perform a MITM Arp Poisoning attack

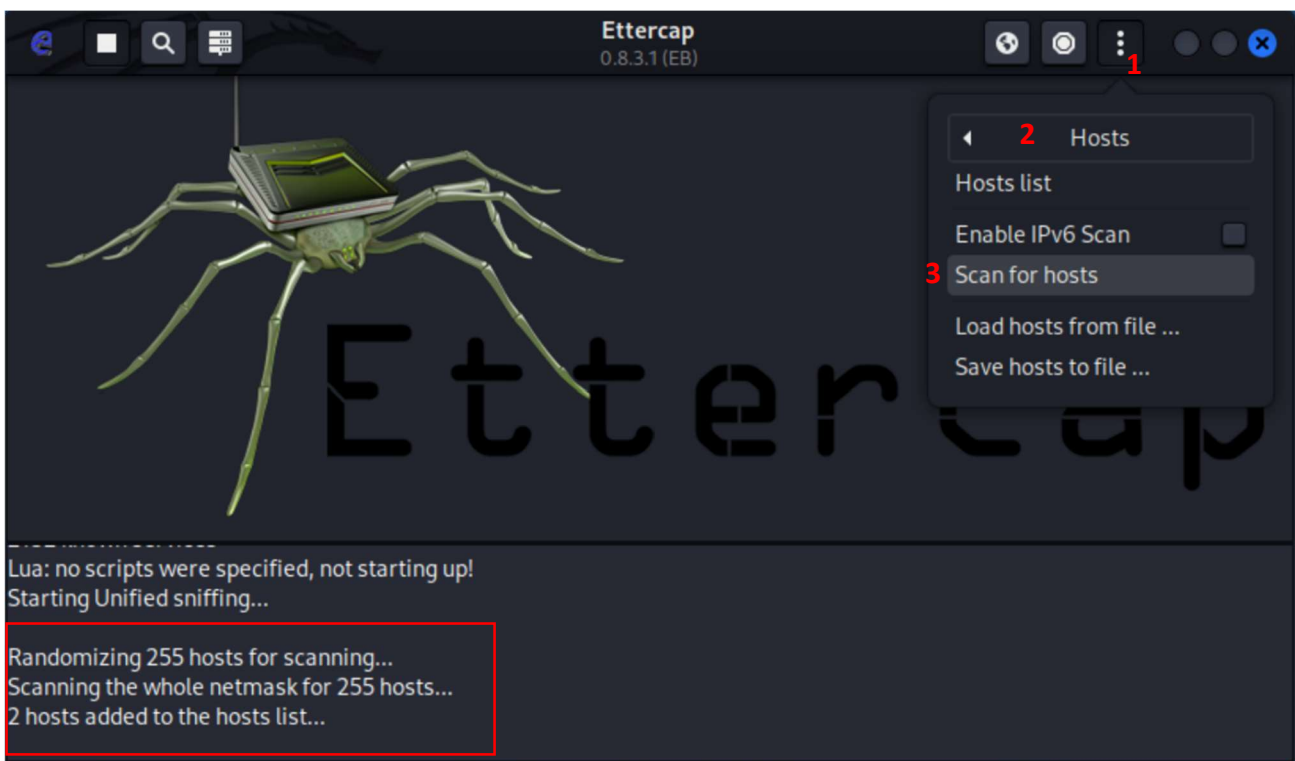
- 1) Open Ettercap (graphical)
 - a. Click on the Kali logo on the top right of the Desktop and expand the “09 - Sniffing & Spoofing” directory
 - i. You should see “ettercap-graphical”
 1. Click to open
 - a. Type password



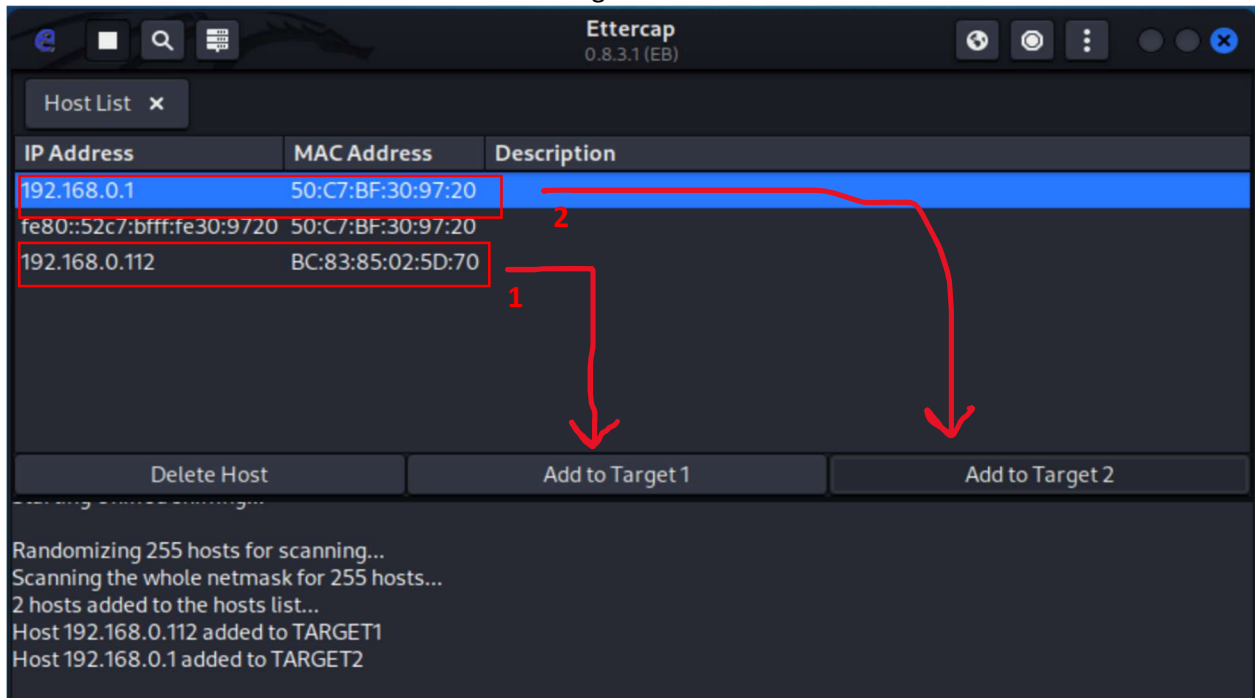
- 2) When Ettercap opens;
 - a. Select the interface under the drop-down menu of “Primary Interface”
 - b. Hit the check mark



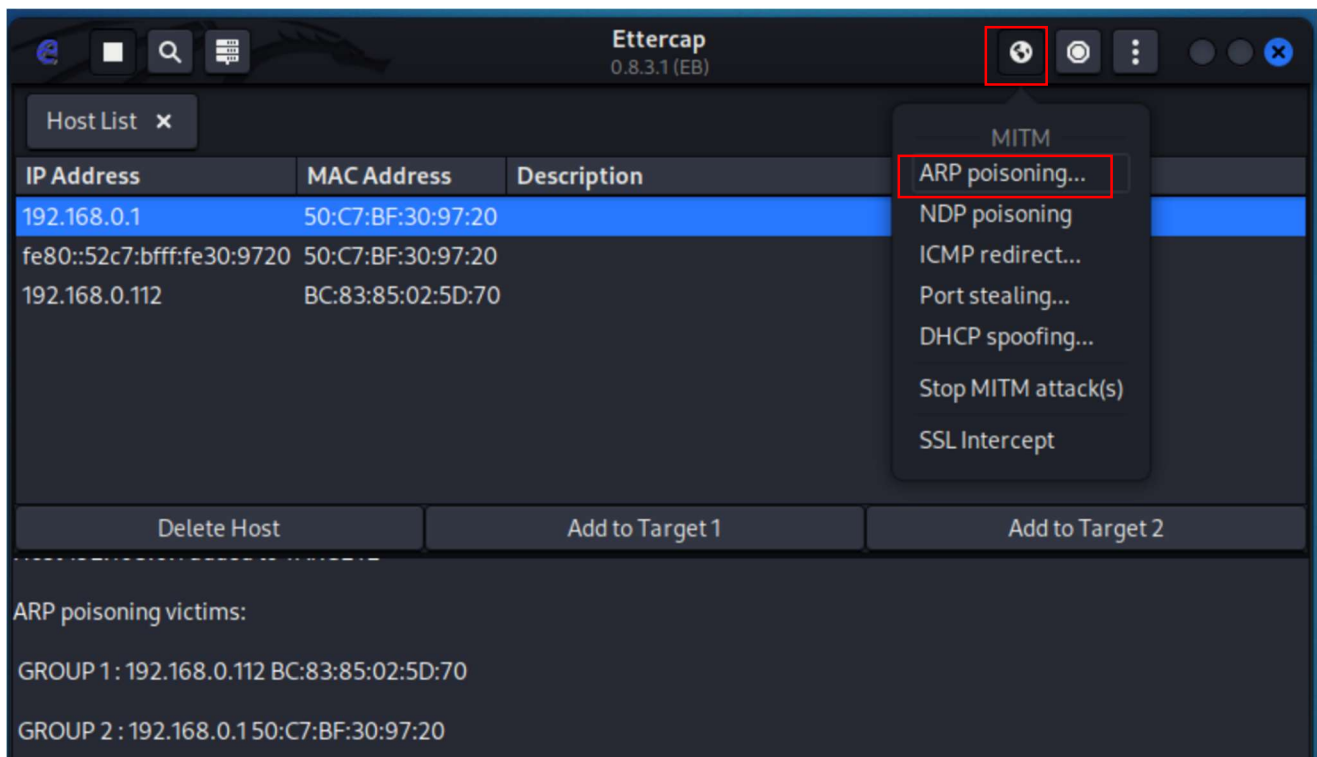
- 3) Scan for hosts
 - a. Click on the 3 vertical dots> Hosts>Scan for hosts
 - i. This will scan the network for hosts and add them to a list

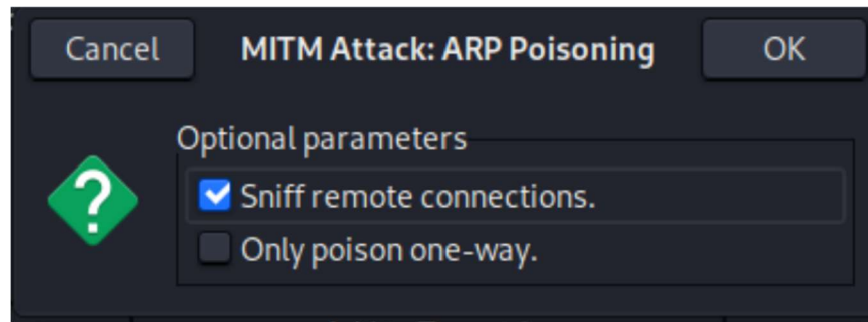


- 4) Select targets to poison
 - a. Click on the 3 vertical dots> Hosts>Hosts list
 - i. Now select from the list the IP address of the client you want to poison
 1. Click “Add to Target 1”
 - ii. Select the gateway IP address you want to poison
 1. Click “Add to Target 2”



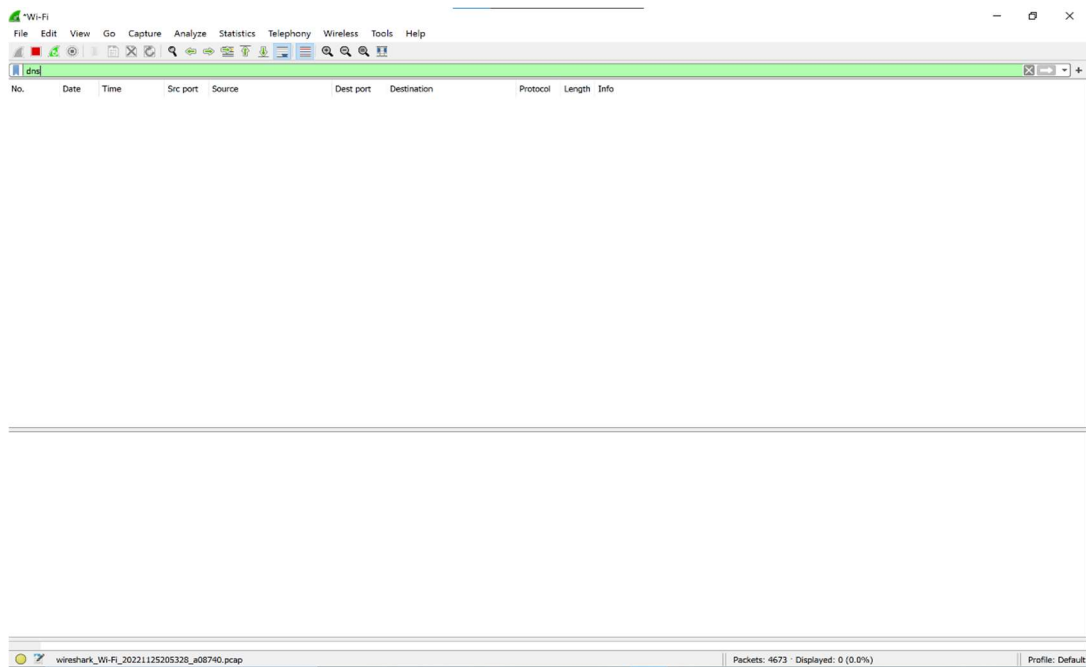
- 5) Begin the arp poison attack
 - a. Click on the MitM icon that looks like a “world” 2 icons left of the 3 dots we clicked on earlier
 - i. Select “ARP poisoning....”
 1. For optional parameters, check mark “Sniff remote connections.”
 - a. Hit “OK” to begin





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

*wlan0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
arp						
No.	Time	Src_Port	Source	Dest_Port	Destination	Protocol
1085	230.1...		b2:45:9a:b0:ab:9b		Tp-LinkT_30:97:20	ARP
1091	233.8...		b2:45:9a:b0:ab:9b		Microsof_02:5d:70	ARP
1092	233.8...		b2:45:9a:b0:ab:9b		Tp-LinkT_30:97:20	ARP
1093	233.8...		Microsof_02:5d:70		Broadcast	ARP
1094	233.8...		b2:45:9a:b0:ab:9b		Microsof_02:5d:70	ARP
1162	243.8...		b2:45:9a:b0:ab:9b		Microsof_02:5d:70	ARP
1163	243.8...		b2:45:9a:b0:ab:9b		Tp-LinkT_30:97:20	ARP
1165	245.8...		Microsof_02:5d:70		Broadcast	ARP
1166	245.8...		b2:45:9a:b0:ab:9b		Microsof_02:5d:70	ARP
1202	249.0...		Microsof_02:5d:70		Broadcast	ARP
1203	249.0...		b2:45:9a:b0:ab:9b		Microsof_02:5d:70	ARP
1205	253.8...		b2:45:9a:b0:ab:9b		Microsof_02:5d:70	ARP
1206	253.8...		b2:45:9a:b0:ab:9b		Tp-LinkT_30:97:20	ARP
1209	257.9...		Microsof_02:5d:70		Broadcast	ARP
1210	257.9...		b2:45:9a:b0:ab:9b		Microsof_02:5d:70	ARP
1258	263.8...		b2:45:9a:b0:ab:9b		Microsof_02:5d:70	ARP
1259	263.8...		b2:45:9a:b0:ab:9b		Tp-LinkT_30:97:20	ARP
1311	273.8...		b2:45:9a:b0:ab:9b		Microsof_02:5d:70	ARP
1312	273.8...		b2:45:9a:b0:ab:9b		Tp-LinkT_30:97:20	ARP
1832	283.8...		b2:45:9a:b0:ab:9b		Microsof_02:5d:70	ARP
1833	283.8...		b2:45:9a:b0:ab:9b		Tp-LinkT_30:97:20	ARP
2533	287.6...		Tp-LinkT_30:97:20		b2:45:9a:b0:ab:9b	ARP
2534	287.6...		b2:45:9a:b0:ab:9b		Tp-LinkT_30:97:20	ARP
2546	293.8...		b2:45:9a:b0:ab:9b		Microsof_02:5d:70	ARP
2547	293.8...		b2:45:9a:b0:ab:9b		Tp-LinkT_30:97:20	ARP

V. Stop the ARP Poisoning

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

END