

Primero he utilizado arp-scan para ver todas las IPs de mi red local.

```
(root㉿kali)-[~]
# arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:36:33:40, IPv4: 192.168.1.22
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1      60:8d:26:ef:d3:09      Arcadyan Corporation
192.168.1.12     54:ec:b0:5b:b8:8c      (Unknown)
192.168.1.10     84:01:12:3a:2b:98      Kaonmedia CO., LTD.
192.168.1.17     bc:f4:d4:0d:ab:3f      CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.
192.168.1.13      1c:53:f9:ac:93:3a      Google, Inc.
192.168.1.21      f8:b5:4d:ff:d6:47      Intel Corporate
192.168.1.28      aa:47:1e:20:3d:c4      (Unknown: locally administered)
192.168.1.255    1c:53:f9:ac:93:3a      Google, Inc.
192.168.1.26      04:70:56:6d:d2:bc      Arcadyan Corporation

9 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.042 seconds (125.37 hosts/sec). 9 responded
```

Para averiguar la IP de mi router, primero he usado el comando “ip route | grep default”

```
(root㉿kali)-[~]
# ip route | grep default
default via 192.168.1.1 dev eth0 proto dhcp src 192.168.1.22 metric 100
```

Ahí he obtenido que la IP de mi router que es 192.168.1.1 y la MAC pertenece a Arcadyan, fabricante habitual de routers/ONT de operadores.

Ahora para ver la IP de Kali ejecuto el comando ifconfig y me sale:

```
(root㉿kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.1.22  netmask 255.255.255.0  broadcast 192.168.1.255
      inet6 fe80::a00:27ff:fe36:3340  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:36:33:40  txqueuelen 1000  (Ethernet)
          RX packets 11785  bytes 888316 (867.4 KiB)
          RX errors 57  dropped 90  overruns 0  frame 57
          TX packets 8682  bytes 655198 (639.8 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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
          RX packets 365  bytes 31272 (30.5 KiB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 365  bytes 31272 (30.5 KiB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

La IP es 192.168.1.22 de Kali

Para obtener la IP de mi ordenador he abierto el CMD y he puesto el comando ipconfig y me ha dado la IP que es 192.168.1.17.

Adaptador de LAN inalámbrica Wi-Fi:

```
Sufijo DNS específico para la conexión. . . : home
Vínculo: dirección IPv6 local. . . : fe80::6aed:f421:6ab3:1174%7
Dirección IPv4. . . . . : 192.168.1.17
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : 192.168.1.1
```

Por último, para obtener la IP de mi teléfono he ejecutado el comando nmap -sV con cada una de las IP hasta que he dado con que la IP 192.168.1.28 es la de mi teléfono.

```
[root@kali) [~]
# nmap -sV 192.168.1.28 -T 5 -o
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-13 12:52 CEST
Nmap scan report for 192.168.1.28
Host is up (0.0080s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
49152/tcp open  tcpwrapped
62078/tcp open  tcpwrapped
MAC Address: AA:47:1E:20:3D:C4 (Unknown)
Device type: phone
Running: Apple iOS 15.X
OS CPE: cpe:/o:apple:iphone_os:15
OS details: Apple iOS 15.0 - 15.6 (Darwin 21.1.0 - 21.6.0)
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.48 seconds
```

He utilizado nmap con la IP de mi router para ver que puertos tenía abiertos para atacar al puerto http (el 80).

```
[root@kali) [~]
# nmap 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-13 18:59 CEST
Nmap scan report for Livebox (192.168.1.1)
Host is up (0.019s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE
23/tcp    closed telnet
53/tcp    open  domain
80/tcp    open  http
139/tcp   closed netbios-ssn
443/tcp   open  https
445/tcp   closed microsoft-ds
2006/tcp  closed invokator
2007/tcp  closed dectalk
2323/tcp  closed 3d-nfsd
6969/tcp  open  acmsoda
8000/tcp  open  http-alt
8200/tcp  closed trivnet1
8443/tcp  open  https-alt
MAC Address: 60:8D:26:EF:D3:09 (Arcadyan)

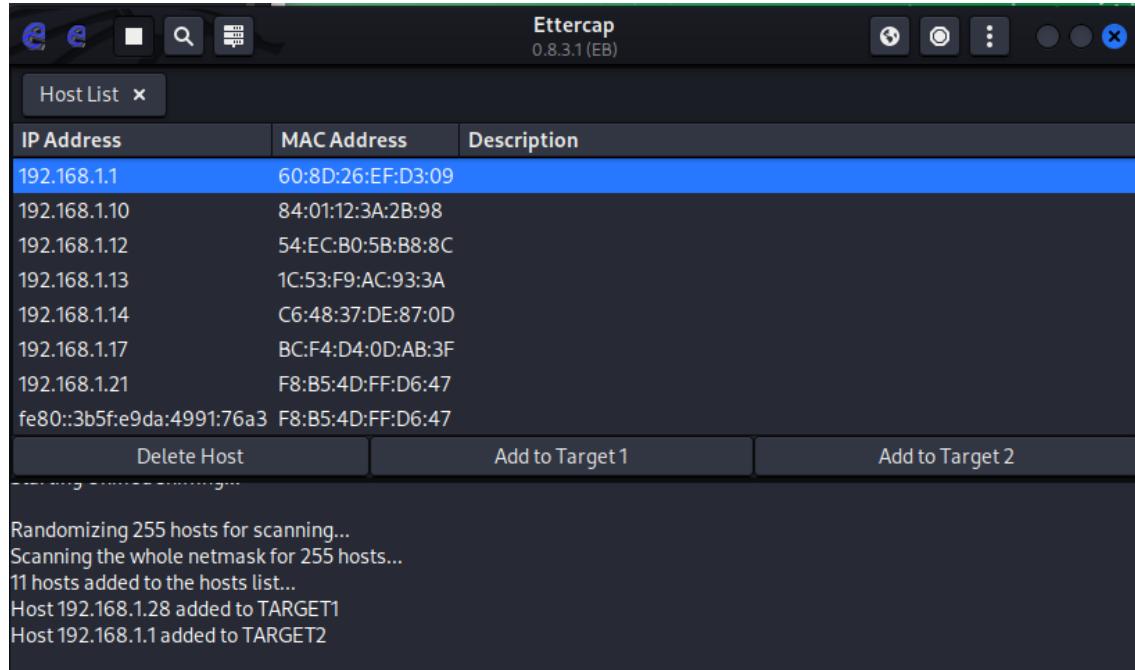
Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds
```

Luego he iniciado Etternet con el comando:

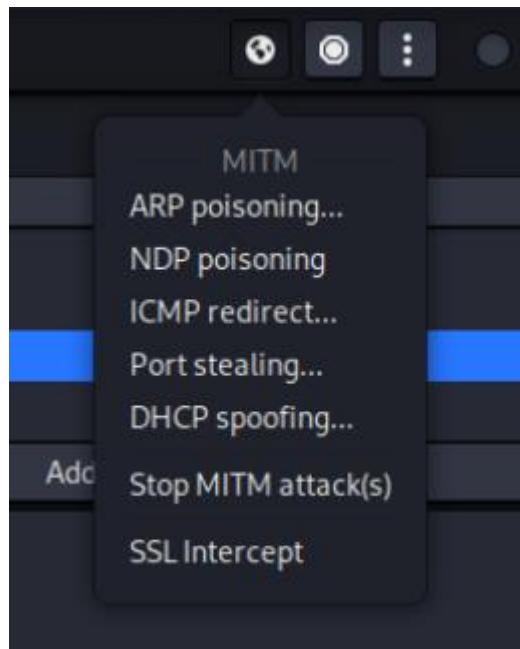
```
(root㉿kali)-[~]
# ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

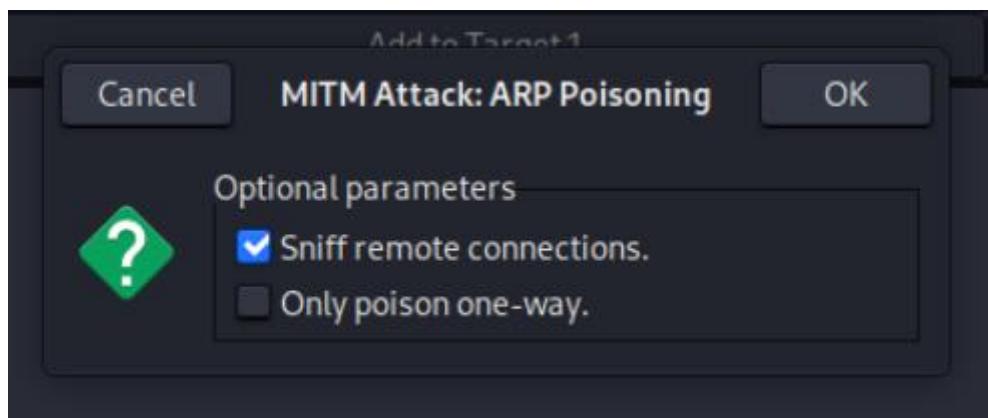
Una vez dentro hay que darle a la lupa luego a su derecha al icono que aparece como un dialogo y he puesto como target 1 mi móvil y como target 2 el router como ves en la captura.



Ahora vamos arriba a la derecha y clickamos en el icono con forma de bola de mundo (“MITM”), seleccionamos “ARP poisoning” y luego “Sniff remote connections

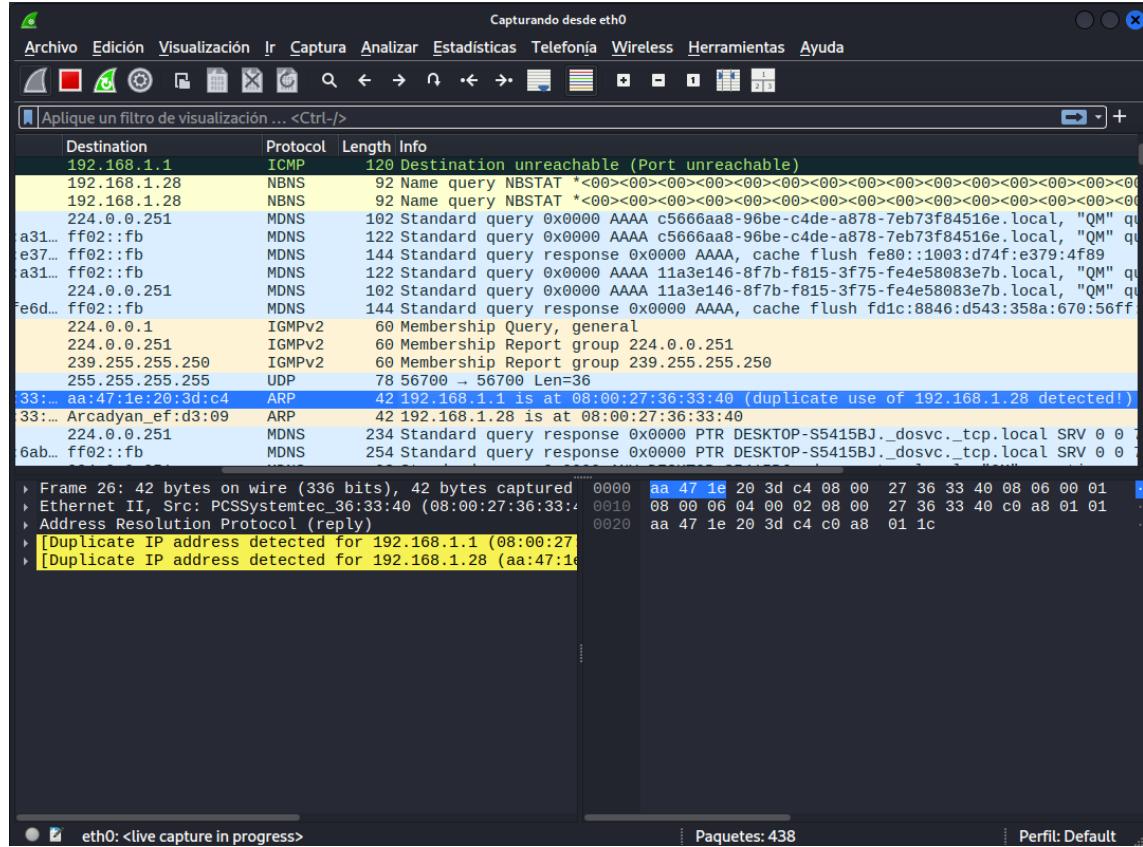


Ahora al seleccionarlo le das a Sniff remote connections (que suele aparecer por defecto).



Abrimos en Kali wireshark:

Ahora se podrá apreciar como se ha duplicado correctamente la MAC.



Añadimos el filtro ip.dst == 10 and http and http.request.method == "POST" Ahora al poner el filtro se ve el inicio de sesión que hemos realizado a través del teléfono.

