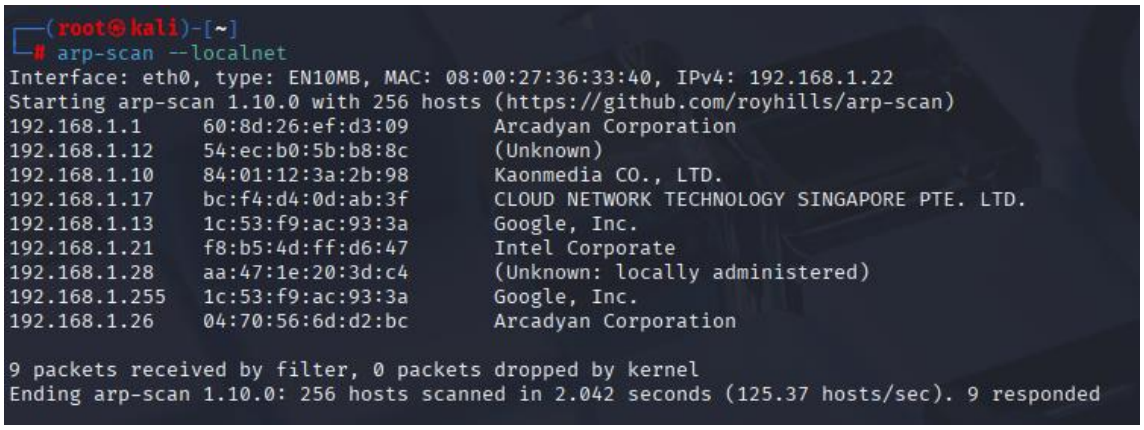
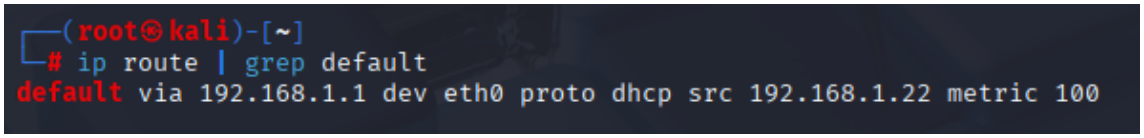
Primero he utilizado arp-scan para ver todas las IPS de mi red local.

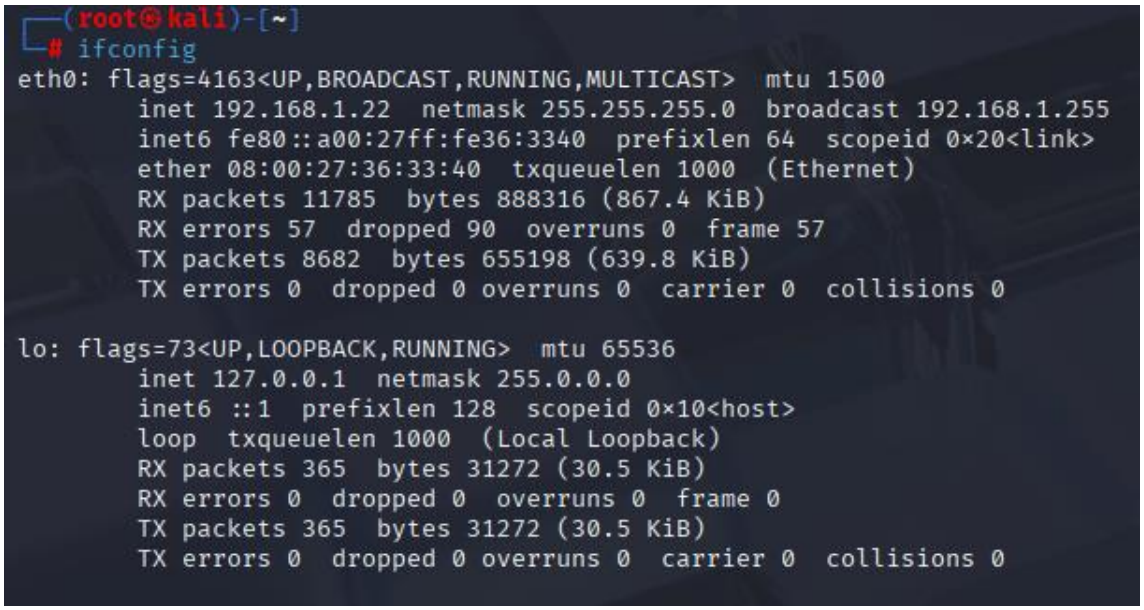


Para averiguar la IP de mi router, primero he usado el comando “ip route | grep default”



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:



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
```

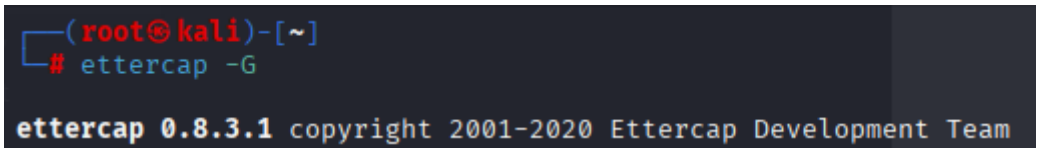
Por último, para obtener la IP de mi teléfono he ejecutado el comando nmap -sV con cada una de las IP hasta que he dado con que la IP 192.168.1.28 es la de mi teléfono.

```
┌──(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
```

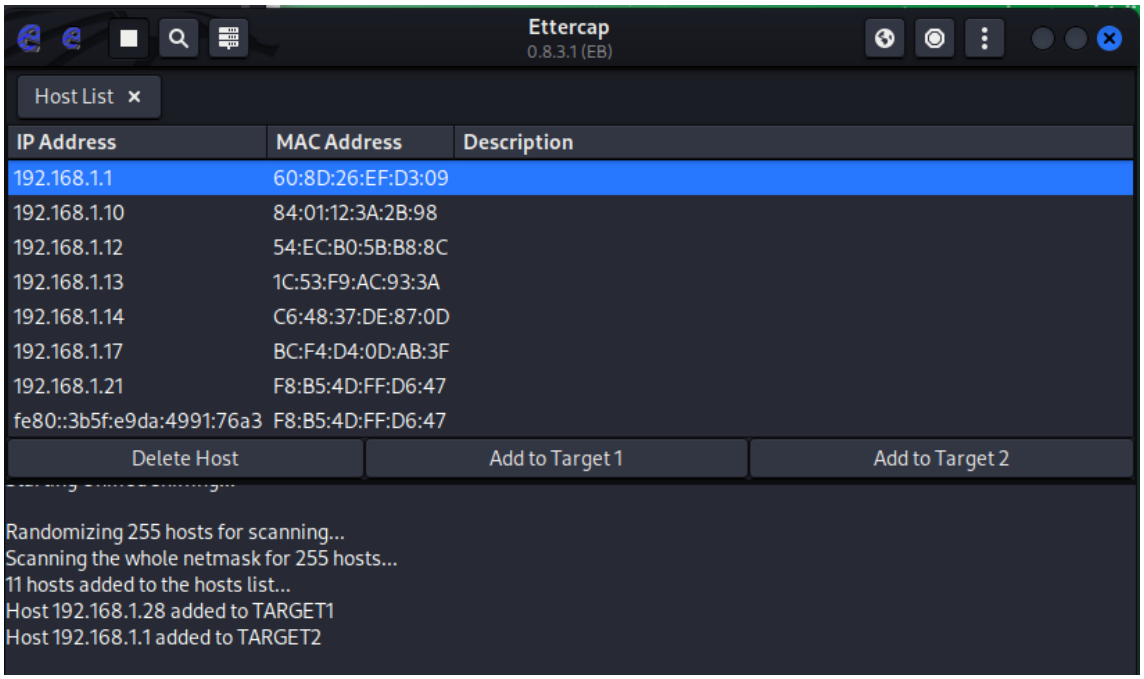
He utilizado nmap con la IP de mi router para ver que puertos tenia abiertos para atacar al puerto http (el 80).

```
┌──(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
```

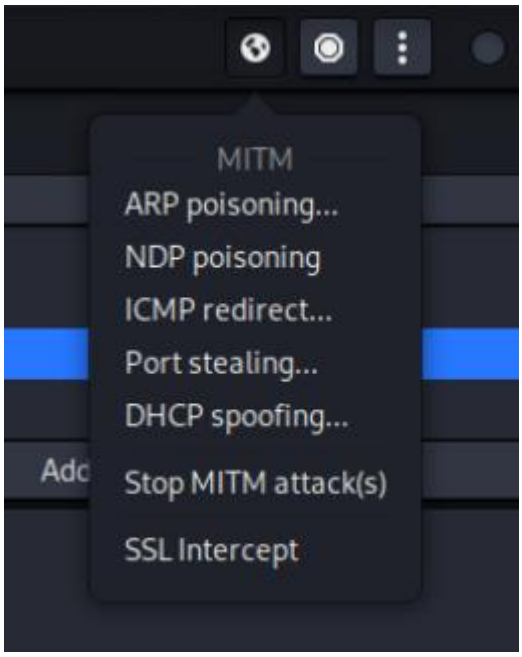
Luego he iniciado Etternet con el comando:



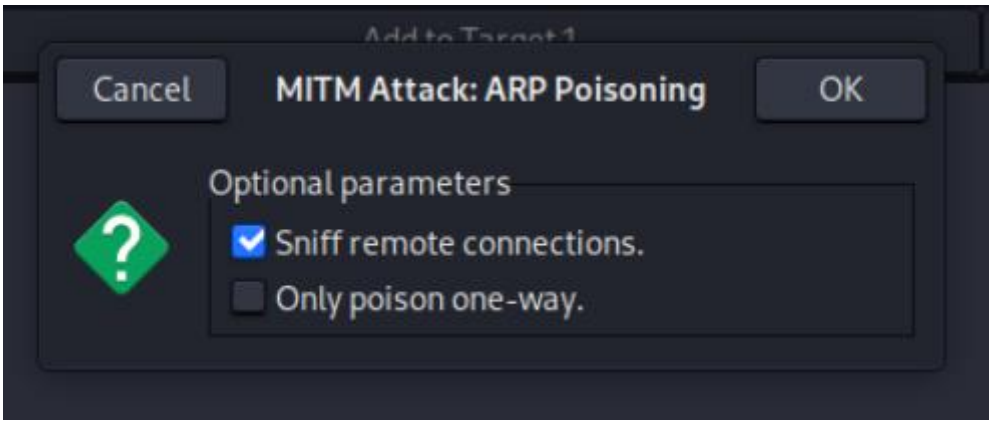
Una vez dentro hay que darle a la lupa luego a su derecha al icono que aparece como un dialogo y he puesto como target 1 mi móvil y como target 2 el router como ves en la captura.



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

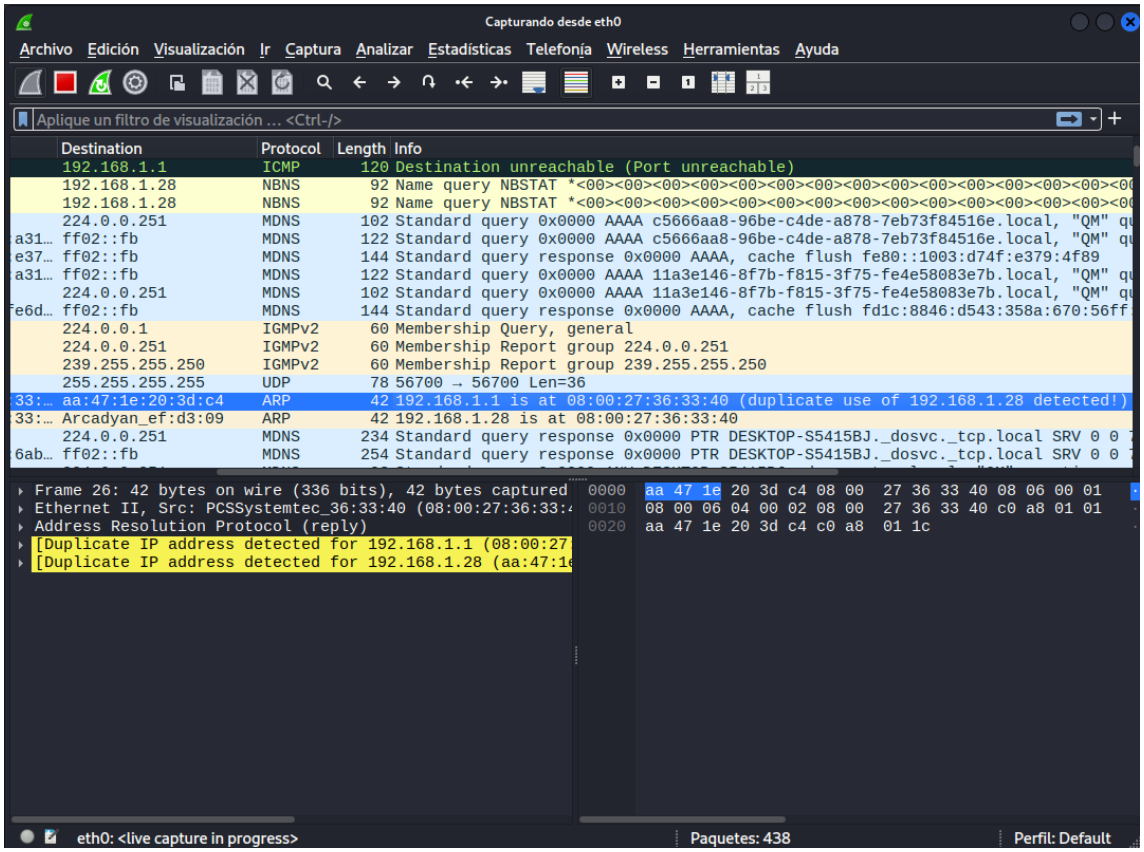


Ahora al seleccionarlo le das a Sniff remote connections (que suele aparecer por defecto).



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.