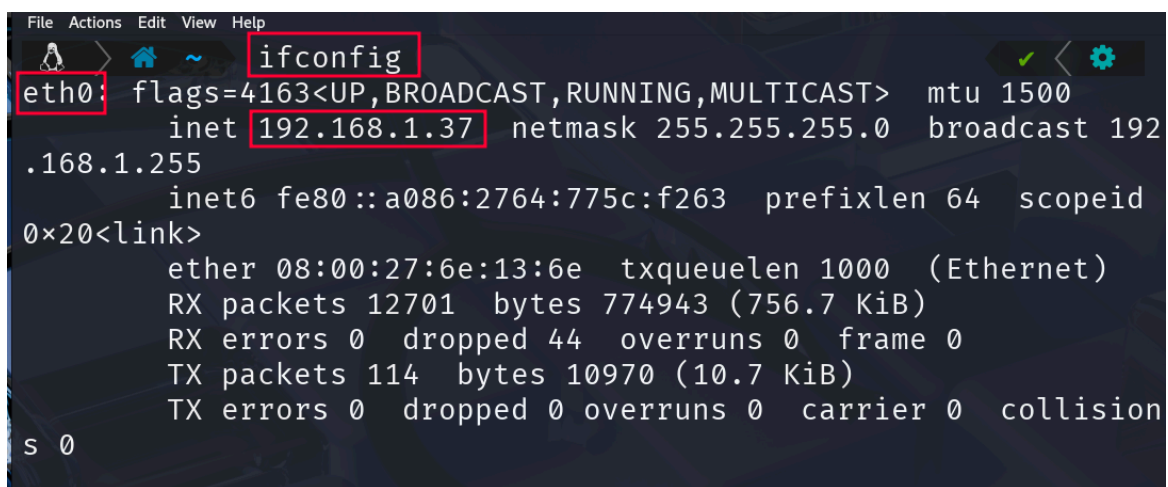


Reconocimiento de la red con ARP-SCAN o NETDISCOVER

Vamos a ver como poder encontrar equipos que estén dentro de mi red privada.

Para utilizar estas herramientas tendremos que tener en cuenta algunos datos que obtendremos utilizando el comando **ifconfig** en nuestra consola de Kali.



```
File Actions Edit View Help
~ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.37 netmask 255.255.255.0 broadcast 192
      .168.1.255
      inet6 fe80::a086:2764:775c:f263 prefixlen 64 scopeid
      0x20<link>
      ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)
      RX packets 12701 bytes 774943 (756.7 KiB)
      RX errors 0 dropped 44 overruns 0 frame 0
      TX packets 114 bytes 10970 (10.7 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collision
s 0
```

- **eth0** : Sera **nuestra interfaz** de red en la que nos encontramos.
- **192.168.1.37** : Es **nuestra dirección IP** que además nos señala nuestro segmento de red **192.169.1.0/24**
- **Herramienta ARP-SCAN:**

```
sudo arp-scan -I eth0 --localnet
```

El comando , `sudo arp-scan -I eth0 --localnet`, se utiliza para realizar un escaneo de red local y detectar los dispositivos conectados. Vamos a desglosarlo:

Propósito del comando

Este comando escanea la red local para identificar las direcciones IP y direcciones MAC de los dispositivos conectados en esa red.

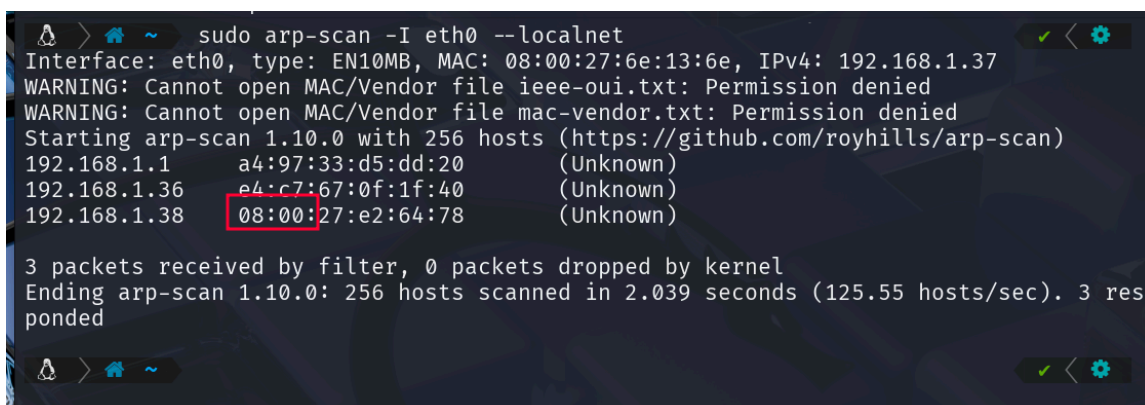
Explicación de los parámetros

sudo: Otorga **permisos administrativos** necesarios para realizar el escaneo, ya que interactuar con la red requiere privilegios elevados.

arp-scan: Es la **herramienta** que realiza el escaneo utilizando el protocolo ARP (Address Resolution Protocol). Esta herramienta envía paquetes ARP a la red para descubrir dispositivos.

-I eth0: Especifica **la interfaz de red a usar** para el escaneo. En este caso, eth0 indica una interfaz Ethernet. Si necesitas escanear en otra interfaz (como Wi-Fi), tendrías que cambiarla por el nombre correspondiente (por ejemplo, wlan0).

--localnet: Indica que se **debe escanear la red local completa**, basándose en la dirección y máscara de subred configuradas en la interfaz seleccionada.



```
> ~ sudo arp-scan -I eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:6e:13:6e, IPv4: 192.168.1.37
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1      a4:97:33:d5:dd:20      (Unknown)
192.168.1.36    e4:c7:67:0f:1f:40      (Unknown)
192.168.1.38    08:00:27:e2:64:78      (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.039 seconds (125.55 hosts/sec). 3 res
ponded
```

NOTA: Como truco que una **MAC** comience como **08:00:** identifica a una maquina virtual.

NOTA2: Podemos saber si una maquina es Windows o Linux mediante el comando Ping.

El comando ping se utiliza para verificar la conectividad entre tu dispositivo y otro en la red local o remota.

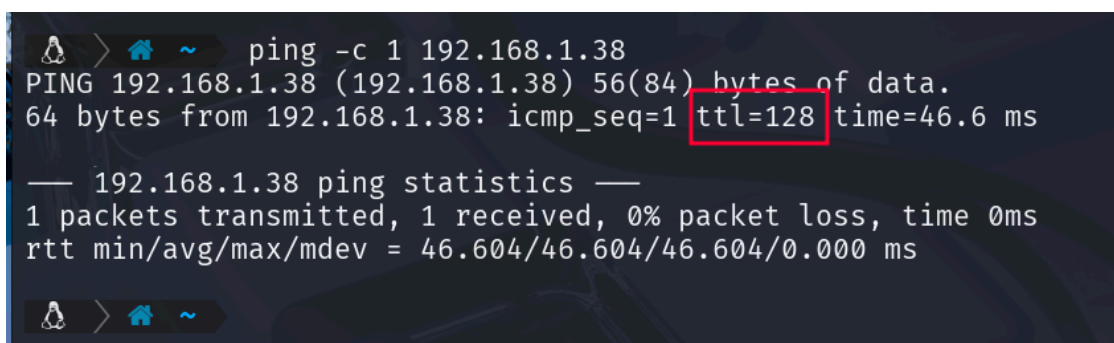
```
ping -c 1 192.168.1.38
```

Parámetros explicados

ping: Es la **herramienta** que realiza la prueba de conectividad mediante paquetes ICMP.

-c 1: Este parámetro especifica **la cantidad de paquetes que se enviarán**. En este caso, el valor 1 indica que solo se enviará un paquete.

192.168.1.38: Es la **dirección IP** del destino al que se envía el paquete.



```
ping -c 1 192.168.1.38
PING 192.168.1.38 (192.168.1.38) 56(84) bytes of data.
64 bytes from 192.168.1.38: icmp_seq=1 ttl=128 time=46.6 ms

— 192.168.1.38 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 46.604/46.604/46.604/0.000 ms
```

- Como vemos el **ttl** devuelto es **128**. Este valor suele ser respondido por máquinas **Windows**.

Si el valor fuera **127** indica que el paquete **pasó por al menos un router** antes de llegar.

- Un valor de **64** indica que probablemente el origen del paquete es un dispositivo basado en **Linux**.

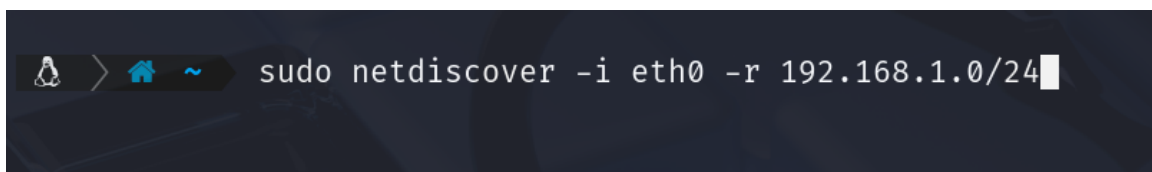
Si el valor fuera **63** indica que el paquete **pasó por al menos un router** antes de llegar.

- **255**: Utilizado en ciertos **dispositivos de red** (routers) o configuraciones especiales.

Por tanto permite estimar el tipo de dispositivo que originó el paquete y cuántos routers o saltos hay entre el origen y destino.

- **Herramienta NETDISCOVER**

```
sudo netdiscover -i eth0 -r 192.168.1.0/24
```



```
Currently scanning: Finished! | Screen View: Unique Hosts
345 Captured ARP Req/Rep packets, from 3 hosts. Total size: 20700
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	a4:97:33:d5:dd:20	343	20580	ASKEY COMPUTER CORP
192.168.1.36	e4:c7:67:0f:1f:40	1	60	Unknown vendor
192.168.1.38	08:00:27:e2:64:78	1	60	PCS Systemtechnik GmbH

Propósito

Netdiscover escanea la red en el rango especificado y muestra una lista de dispositivos activos. Este comando es especialmente útil para redes locales donde no se utiliza un servidor DHCP.

Explicación de los parámetros

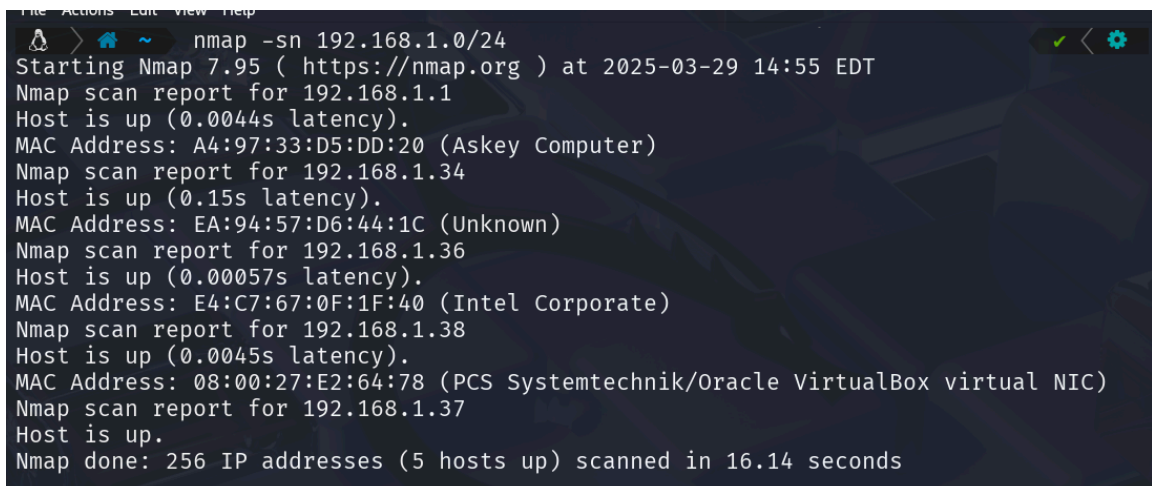
netdiscover: Es la **herramienta** que realiza el escaneo de ARP en la red.

-i eth0: Especifica **la interfaz de red a usar**, en este caso eth0 (Ethernet). Si estás usando Wi-Fi, puedes cambiarlo por el nombre de la interfaz correspondiente (como wlan0).

-r 192.168.1.0/24: Define el **rango de IP a escanear**. Aquí, 192.168.1.0/24 indica que se escaneará toda la subred (de 192.168.1.1 a 192.168.1.254), común en redes privadas.

- **Herramienta NMAP**

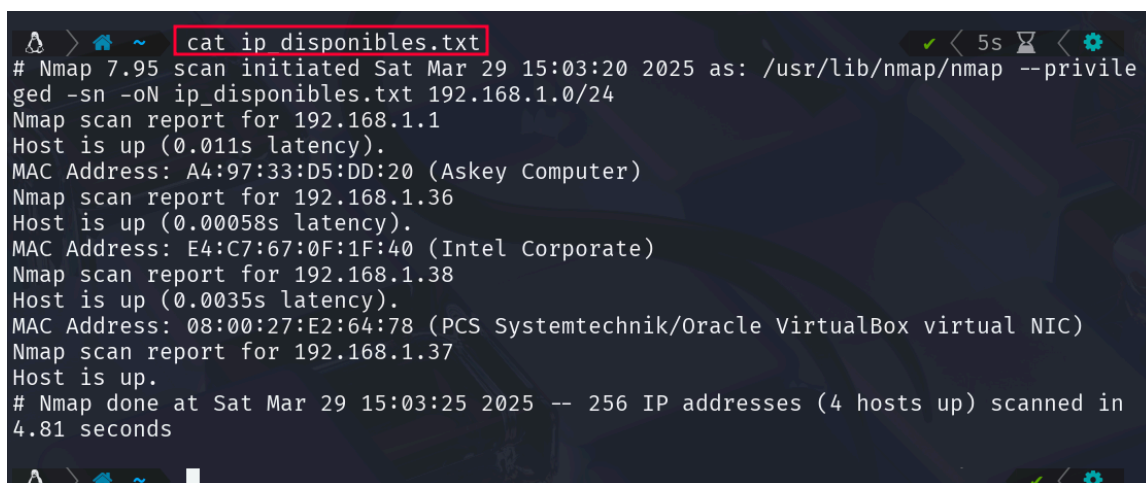
`nmap -sn 192.168.1.0/24`



```
File Actions Edit View Help
nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-29 14:55 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0044s latency).
MAC Address: A4:97:33:D5:DD:20 (Askey Computer)
Nmap scan report for 192.168.1.34
Host is up (0.15s latency).
MAC Address: EA:94:57:D6:44:1C (Unknown)
Nmap scan report for 192.168.1.36
Host is up (0.00057s latency).
MAC Address: E4:C7:67:0F:1F:40 (Intel Corporate)
Nmap scan report for 192.168.1.38
Host is up (0.0045s latency).
MAC Address: 08:00:27:E2:64:78 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.37
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 16.14 seconds
```

Si queremos guardar el resultado del escaneo de red en un archivo lo escribiríamos así:

`nmap -sn 192.168.1.0/24 -oN ip_disponibles.txt`



```
# Nmap 7.95 scan initiated Sat Mar 29 15:03:20 2025 as: /usr/lib/nmap/nmap --privile
ged -sn -oN ip_disponibles.txt 192.168.1.0/24
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
MAC Address: A4:97:33:D5:DD:20 (Askey Computer)
Nmap scan report for 192.168.1.36
Host is up (0.00058s latency).
MAC Address: E4:C7:67:0F:1F:40 (Intel Corporate)
Nmap scan report for 192.168.1.38
Host is up (0.0035s latency).
MAC Address: 08:00:27:E2:64:78 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.37
Host is up.
# Nmap done at Sat Mar 29 15:03:25 2025 -- 256 IP addresses (4 hosts up) scanned in
4.81 seconds
```

Explicación de los parámetros



-sn: Este parámetro indica que Nmap **realizará un escaneo de ping ("ping scan") únicamente**. Esto significa que **no se realizarán escaneos de puertos** en los hosts, sino que simplemente verificará qué dispositivos están activos en la red especificada.

192.168.1.0/24: Esta es la **dirección de red** que deseas escanear.

El formato

/24 indica una **máscara de subred**, que en este caso cubre todas las direcciones IP desde 192.168.1.0 hasta 192.168.1.255. Es decir, estás escaneando un rango completo de IPs en esa subred.

-oN ip_disponibles.txt: Este parámetro **guarda los resultados del escaneo en un archivo llamado ip_disponibles.txt** en un formato normal (legible). Esto te permite analizar más tarde qué hosts están activos.