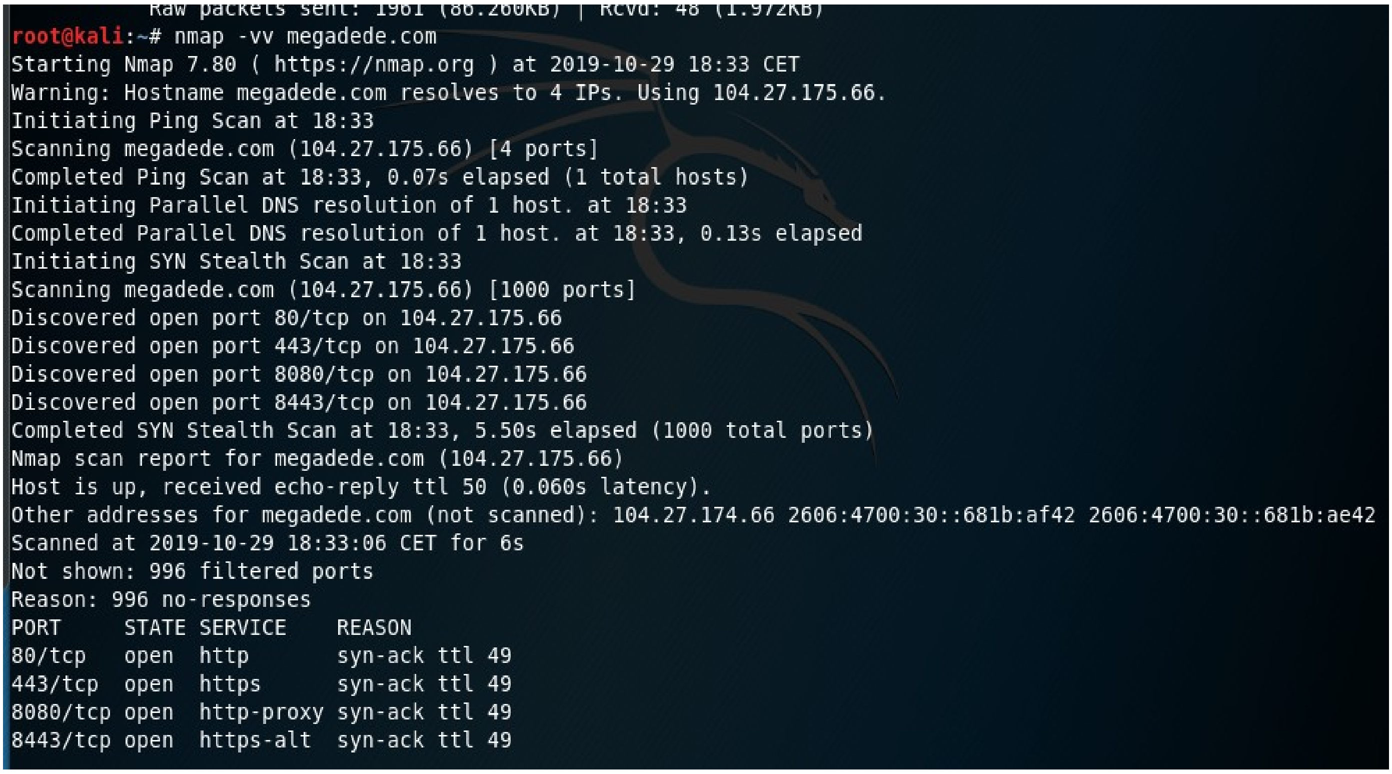
NMAP

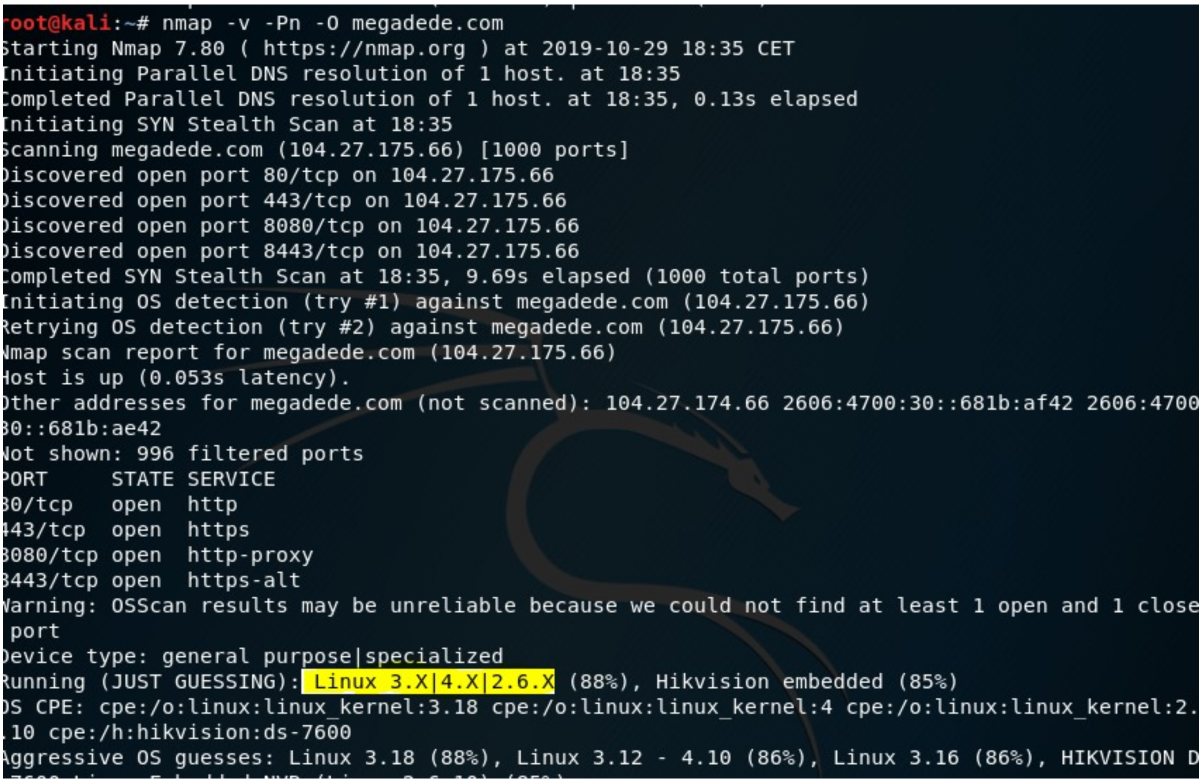
Network Mapped (Nmap) es una herramienta de escaneo de red y detección de host. Se usa para recopilar información sobre cualquier red. Si deseas buscar un servicio (HTTP, FTP, SSH, etc.) ejecutándose en una computadora, el sistema operativo de cualquier dispositivo, etc., entonces puedes usar nmap.

Escanear puertos con NMAP



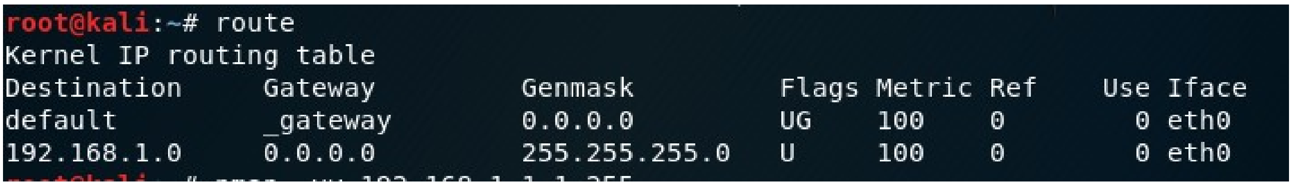
```
          Raw packets sent: 1961 (86.260KB) | Rcvd: 48 (1.972KB)
root@kali:~# nmap -vv megadede.com
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-29 18:33 CET
Warning: Hostname megadede.com resolves to 4 IPs. Using 104.27.175.66.
Initiating Ping Scan at 18:33
Scanning megadede.com (104.27.175.66) [4 ports]
Completed Ping Scan at 18:33, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:33
Completed Parallel DNS resolution of 1 host. at 18:33, 0.13s elapsed
Initiating SYN Stealth Scan at 18:33
Scanning megadede.com (104.27.175.66) [1000 ports]
Discovered open port 80/tcp on 104.27.175.66
Discovered open port 443/tcp on 104.27.175.66
Discovered open port 8080/tcp on 104.27.175.66
Discovered open port 8443/tcp on 104.27.175.66
Completed SYN Stealth Scan at 18:33, 5.50s elapsed (1000 total ports)
Nmap scan report for megadede.com (104.27.175.66)
Host is up, received echo-reply ttl 50 (0.060s latency).
Other addresses for megadede.com (not scanned): 104.27.174.66 2606:4700:30::681b:af42 2606:4700:30::681b:ae42
Scanned at 2019-10-29 18:33:06 CET for 6s
Not shown: 996 filtered ports
Reason: 996 no-responses
PORT     STATE SERVICE    REASON
80/tcp   open  http       syn-ack ttl 49
443/tcp  open  https      syn-ack ttl 49
8080/tcp open  http-proxy syn-ack ttl 49
8443/tcp open  https-alt  syn-ack ttl 49
```

Detectar el sistema operativo



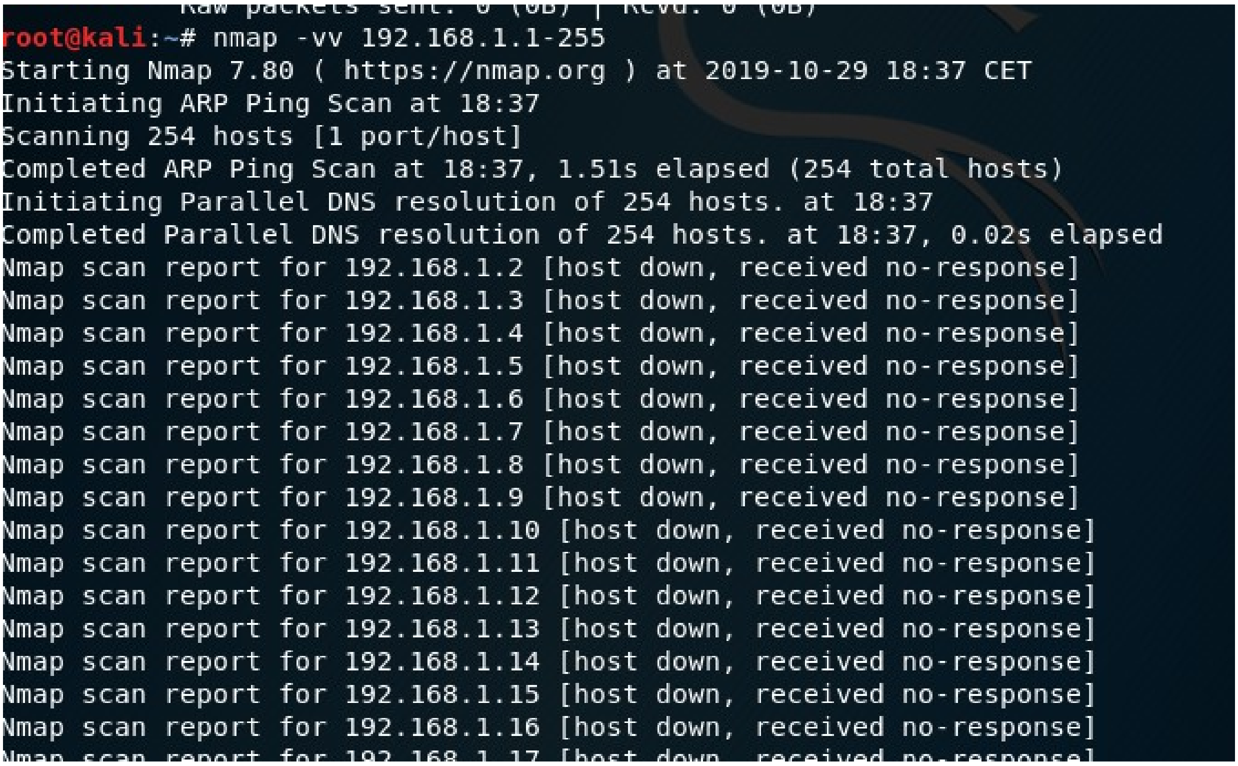
```
oot@kali:~# nmap -v -Pn -O megadede.com
tarting Nmap 7.80 ( https://nmap.org ) at 2019-10-29 18:35 CET
nitiating Parallel DNS resolution of 1 host. at 18:35
ompleted Parallel DNS resolution of 1 host. at 18:35, 0.13s elapsed
nitiating SYN Stealth Scan at 18:35
canning megadede.com (104.27.175.66) [1000 ports]
iscovered open port 80/tcp on 104.27.175.66
iscovered open port 443/tcp on 104.27.175.66
iscovered open port 8080/tcp on 104.27.175.66
iscovered open port 8443/tcp on 104.27.175.66
ompleted SYN Stealth Scan at 18:35, 9.69s elapsed (1000 total ports)
nitiating OS detection (try #1) against megadede.com (104.27.175.66)
etrying OS detection (try #2) against megadede.com (104.27.175.66)
map scan report for megadede.com (104.27.175.66)
ost is up (0.053s latency).
ther addresses for megadede.com (not scanned): 104.27.174.66 2606:4700:30::681b:af42 2606:4700
0::681b:ae42
ot shown: 996 filtered ports
ORT      STATE SERVICE
0/tcp    open  http
43/tcp   open  https
080/tcp open  http-proxy
443/tcp open  https-alt
arning: OSScan results may be unreliable because we could not find at least 1 open and 1 close
 port
evice type: general purpose|specialized
unning (JUST GUESSING): Linux 3.X|4.X|2.6.X (88%), Hikvision embedded (85%)
S CPE: cpe:/o:linux:linux_kernel:3.18 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.
.10 cpe:/h:hikvision:ds-7600
ggressive OS guesses: Linux 3.18 (88%), Linux 3.12 - 4.10 (86%), Linux 3.16 (86%), HIKVISION D
```

Escanear rangos de direcciones IP

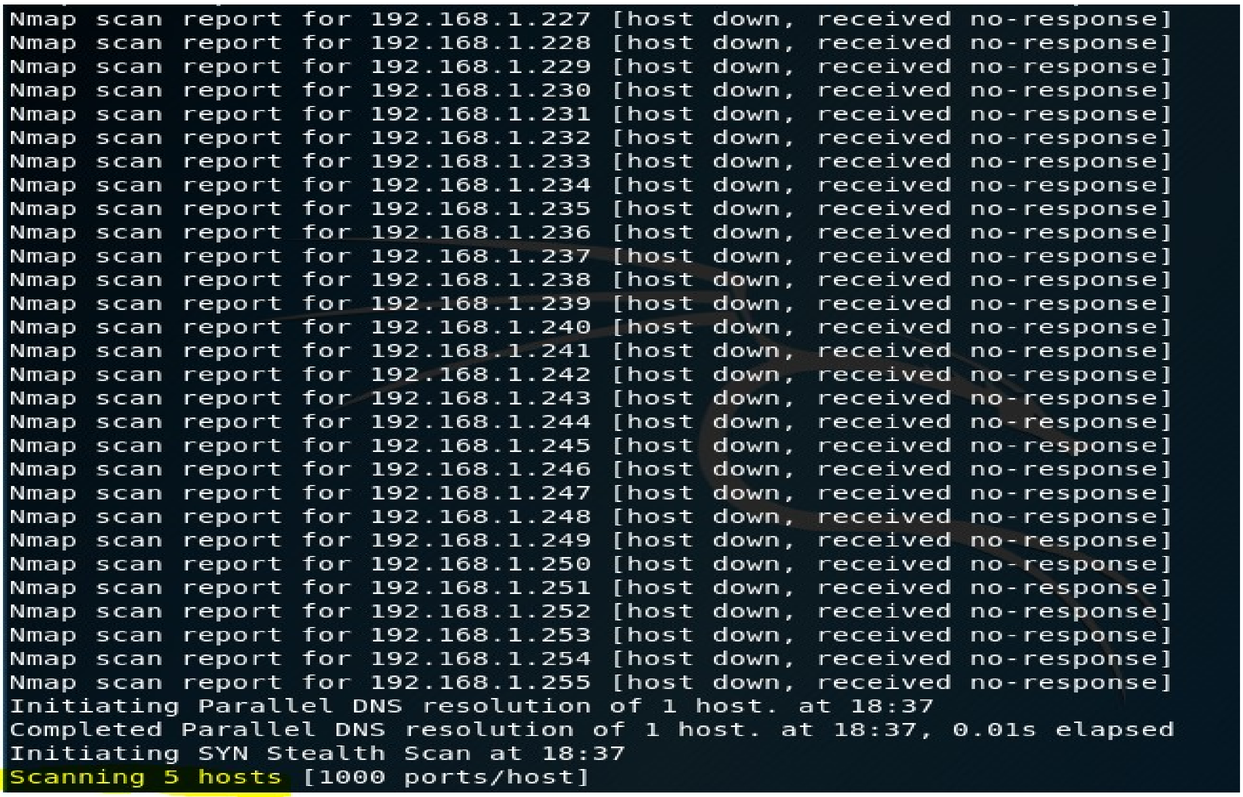


```
root@kali:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

Escanear 192.168.1.1/255

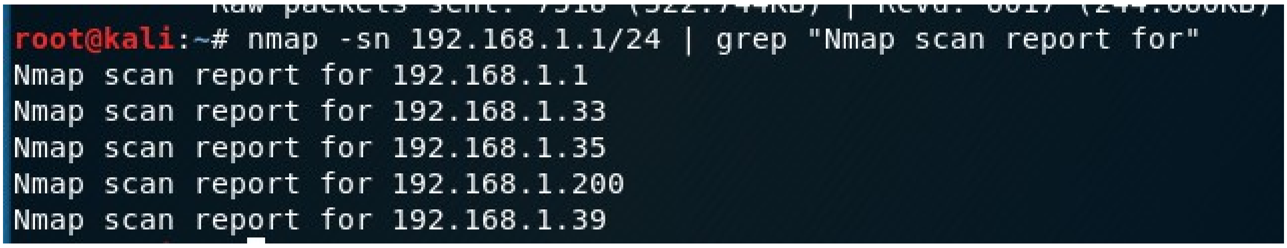


```
          Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
root@kali:~# nmap -vv 192.168.1.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-29 18:37 CET
Initiating ARP Ping Scan at 18:37
Scanning 254 hosts [1 port/host]
Completed ARP Ping Scan at 18:37, 1.51s elapsed (254 total hosts)
Initiating Parallel DNS resolution of 254 hosts. at 18:37
Completed Parallel DNS resolution of 254 hosts. at 18:37, 0.02s elapsed
Nmap scan report for 192.168.1.2 [host down, received no-response]
Nmap scan report for 192.168.1.3 [host down, received no-response]
Nmap scan report for 192.168.1.4 [host down, received no-response]
Nmap scan report for 192.168.1.5 [host down, received no-response]
Nmap scan report for 192.168.1.6 [host down, received no-response]
Nmap scan report for 192.168.1.7 [host down, received no-response]
Nmap scan report for 192.168.1.8 [host down, received no-response]
Nmap scan report for 192.168.1.9 [host down, received no-response]
Nmap scan report for 192.168.1.10 [host down, received no-response]
Nmap scan report for 192.168.1.11 [host down, received no-response]
Nmap scan report for 192.168.1.12 [host down, received no-response]
Nmap scan report for 192.168.1.13 [host down, received no-response]
Nmap scan report for 192.168.1.14 [host down, received no-response]
Nmap scan report for 192.168.1.15 [host down, received no-response]
Nmap scan report for 192.168.1.16 [host down, received no-response]
Nmap scan report for 192.168.1.17 [host down, received no-response]
```



```
Nmap scan report for 192.168.1.227 [host down, received no-response]
Nmap scan report for 192.168.1.228 [host down, received no-response]
Nmap scan report for 192.168.1.229 [host down, received no-response]
Nmap scan report for 192.168.1.230 [host down, received no-response]
Nmap scan report for 192.168.1.231 [host down, received no-response]
Nmap scan report for 192.168.1.232 [host down, received no-response]
Nmap scan report for 192.168.1.233 [host down, received no-response]
Nmap scan report for 192.168.1.234 [host down, received no-response]
Nmap scan report for 192.168.1.235 [host down, received no-response]
Nmap scan report for 192.168.1.236 [host down, received no-response]
Nmap scan report for 192.168.1.237 [host down, received no-response]
Nmap scan report for 192.168.1.238 [host down, received no-response]
Nmap scan report for 192.168.1.239 [host down, received no-response]
Nmap scan report for 192.168.1.240 [host down, received no-response]
Nmap scan report for 192.168.1.241 [host down, received no-response]
Nmap scan report for 192.168.1.242 [host down, received no-response]
Nmap scan report for 192.168.1.243 [host down, received no-response]
Nmap scan report for 192.168.1.244 [host down, received no-response]
Nmap scan report for 192.168.1.245 [host down, received no-response]
Nmap scan report for 192.168.1.246 [host down, received no-response]
Nmap scan report for 192.168.1.247 [host down, received no-response]
Nmap scan report for 192.168.1.248 [host down, received no-response]
Nmap scan report for 192.168.1.249 [host down, received no-response]
Nmap scan report for 192.168.1.250 [host down, received no-response]
Nmap scan report for 192.168.1.251 [host down, received no-response]
Nmap scan report for 192.168.1.252 [host down, received no-response]
Nmap scan report for 192.168.1.253 [host down, received no-response]
Nmap scan report for 192.168.1.254 [host down, received no-response]
Nmap scan report for 192.168.1.255 [host down, received no-response]
Initiating Parallel DNS resolution of 1 host. at 18:37
Completed Parallel DNS resolution of 1 host. at 18:37, 0.01s elapsed
Initiating SYN Stealth Scan at 18:37
Scanning 5 hosts [1000 ports/host]
```

Encontrar dispositivos conectados a la red



```
           Raw packets sent: 7518 (322.744KB) | Rcvd: 6017 (244.080KB)
root@kali:~# nmap -sn 192.168.1.1/24 | grep "Nmap scan report for"
Nmap scan report for 192.168.1.1
Nmap scan report for 192.168.1.33
Nmap scan report for 192.168.1.35
Nmap scan report for 192.168.1.200
Nmap scan report for 192.168.1.39
```