

SPOOFING DE RED EN MANJARO

Primero co

```
nmap --version

Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.3.2 libssh2-1.11.0 libz-1.3.1 libpcap-1.10.5 nmap-
libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

NMAP a un host

```
nmap example.com
nmap 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-28 11:31 CET
Nmap scan report for example.com (93.184.215.14)
Host is up (0.10s latency).
Other addresses for example.com (not scanned): 2606:2800:21f:cb07:6820:80d
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
1119/tcp  closed bnetgame
1935/tcp  closed rtmp

Nmap done: 1 IP address (1 host up) scanned in 8.21 seconds
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-28 11:31 CET
Nmap scan report for Livebox (192.168.1.1)
Host is up (0.016s latency).
Not shown: 989 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
8000/tcp  open  http-alt
8200/tcp  closed trivnet1

Nmap done: 1 IP address (1 host up) scanned in 4.48 seconds
```

NMAP Puertos

SPOOFING DE RED EN MANJARO

```
nmap -p 20-80 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-28 11:38 CET
Nmap scan report for Livebox (192.168.1.1)
Host is up (0.0076s latency).
Not shown: 58 filtered tcp ports (no-response)
PORT      STATE SERVICE
23/tcp    closed telnet
53/tcp    open  domain
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```

Servicios en los puertos abiertos

```
nmap -sV 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-28 11:39 CET
Nmap scan report for Livebox (192.168.1.1)
Host is up (0.0054s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
23/tcp    closed telnet
53/tcp    open  domain         Cloudflare public DNS
80/tcp    open  http           Arcadyan httpd 1.0
139/tcp   closed netbios-ssn
443/tcp   open  ssl/https      Arcadyan httpd 1.0
445/tcp   closed microsoft-ds
2006/tcp  closed invokator
2007/tcp  closed dectalk
2323/tcp  closed 3d-nfsd
6969/tcp  open  tcpwrapped
8000/tcp  open  http-alt
8200/tcp  closed trivnet1
8443/tcp  open  ssl/https-alt

3 services unrecognized despite returning data. If you know the service/version
owing fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port80-TCP:V=7.95%I=7%D=11/28%Time=6748487B%P=x86_64-pc-linux-gnu%r(Get
SF:Request,109,"HTTP/1.1x20302x20Found\r\nServer:x20Arcadyanx20httpd\
SF:x201.0\r\nPragma:x20no-cache\r\nCache-Control:x20no-cache,x20must-r
SF:validate\r\nContent-length:x200\r\nLocation:x20/login\.htm\r\nX-Cont
SF:ent-Type-Options:x20nosniff\r\nX-XSS-Protection:x201;x20mode=block\r
SF:\nX-Frame-Options:x20SAMEORIGIN\r\nConnection:x20close\r\n\r\n")%r(HT
SF:TPOptions,109,"HTTP/1.1x20302x20Found\r\nServer:x20Arcadyanx20http
SF:d\r\nPragma:x20no-cache\r\nCache-Control:x20no-cache,x20must
SF:-revalidate\r\nContent-length:x200\r\nLocation:x20/login\.htm\r\nX-Co
SF:ntent-Type-Options:x20nosniff\r\nX-XSS-Protection:x201;x20mode=block
SF:\r\nX-Frame-Options:x20SAMEORIGIN\r\nConnection:x20close\r\n\r\n")%r(
SF:Four0hFourRequest,109,"HTTP/1.1x20302x20Found\r\nServer:x20Arcadyan
```

Nmap redes enteras

SPOOFING DE RED EN MANJARO

```
nmap 192.168.1.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-28 12:03 CET
Nmap scan report for Livebox (192.168.1.1)
Host is up (0.0080s 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

Nmap scan report for 192.168.1.12
Host is up (0.011s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync

Nmap scan report for 192.168.1.14
Host is up (0.0084s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
8008/tcp  open  http
8009/tcp  open  ajp13
```