Laboratorio #3: NMAP

Fernando Cutire (8-972-906)
Díaz, Gabriel (20-53-5198)
Gamero, Jonathan (8-982-2008)

Nota: El servidor server1.cyberciti.biz, no funcionaba a la hora de realizar este laboratorio, por lo que se usó fernandocutire.com

Tiempo estimado de duración: 1.5 hora (90 minutos)

Nota importante: Atienda las instrucciones del profesor para el desarrollo del laboratorio, luego realice las actividades de acuerdo a sus instrucciones.

Instrucciones del laboratorio #1: Ud. es un administrador de red que desea conocer el uso de "nmap" para la de búsqueda de los componentes de la red interna y los cuales pueden ser posibles objetivos para los APT's.

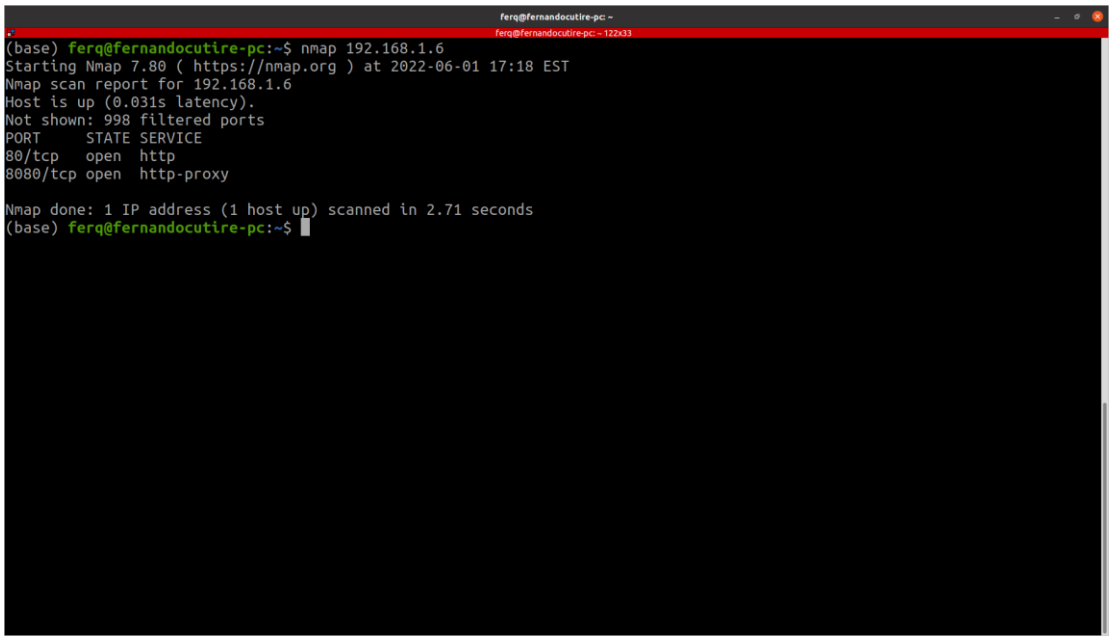
Recursos necesarios: Uso de la máquina virtual Kali Linux 2016.

nmap [Tipo(s) de Análisis] [Opciones] {especificación de objetivos}

Ejercicio 1: Realice un escaneo a un único host y a una dirección IP (IPv4)

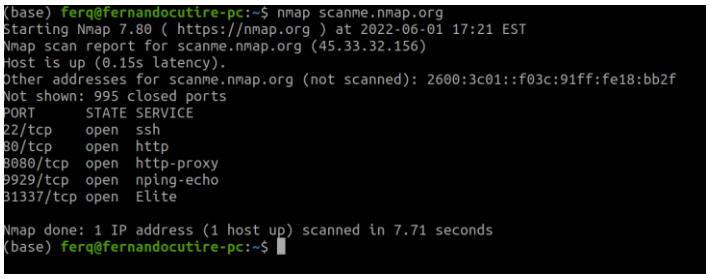
Instrucción: Escanear una única dirección IP

```
nmap 192.168.1.6
```



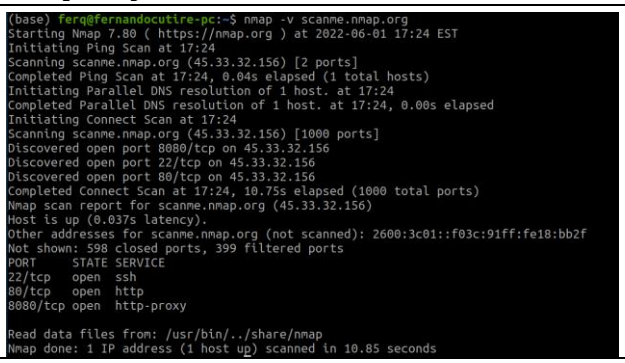
Instrucción: Escanear un nombre de host

```
nmap scanme.nmap.org
```



Instrucción: Escanear un nombre de host con más información

```
nmap -v scanme.nmap.org
```

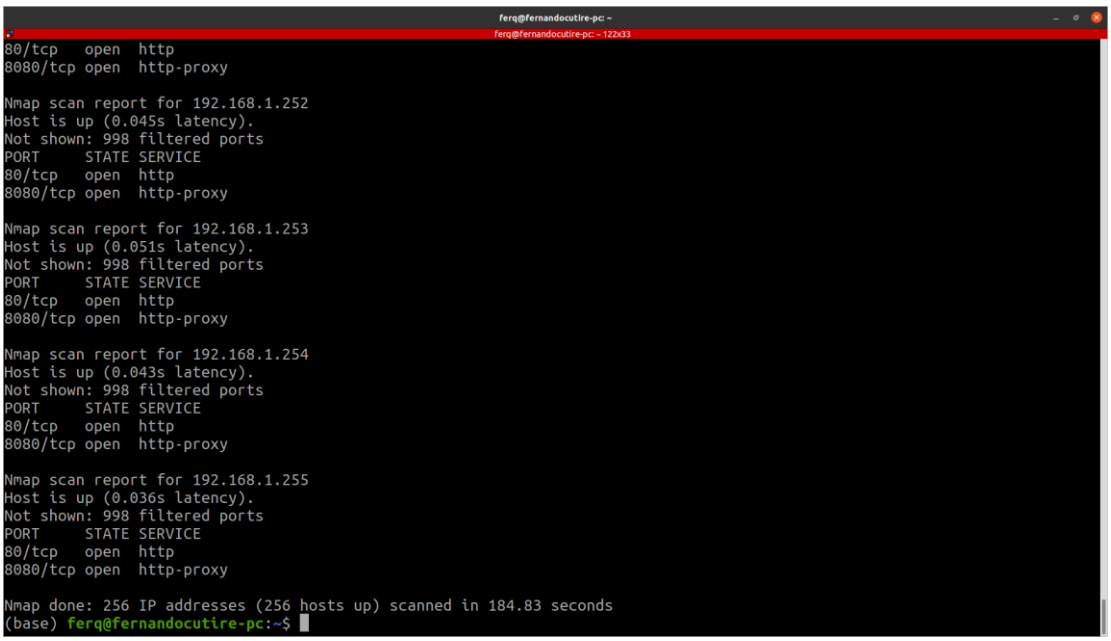


Ejercicio 2: Escanear varias direcciones IP o subred (IPv4)

Instrucción: Escanear la red utilizando la secuencia de tipo: IP1,IP2,IP3 y con comas
`nmap 192.168.1.1,2,3`

```
(base) ferq@fernandocutire-pc:~$ nmap 192.168.1.1,2,3
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-01 17:25 EST
Nmap scan report for 192.168.1.1
Host is up (0.035s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap scan report for 192.168.1.2
Host is up (0.041s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap scan report for 192.168.1.3
Host is up (0.050s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 3 IP addresses (3 hosts up) scanned in 3.86 seconds
```

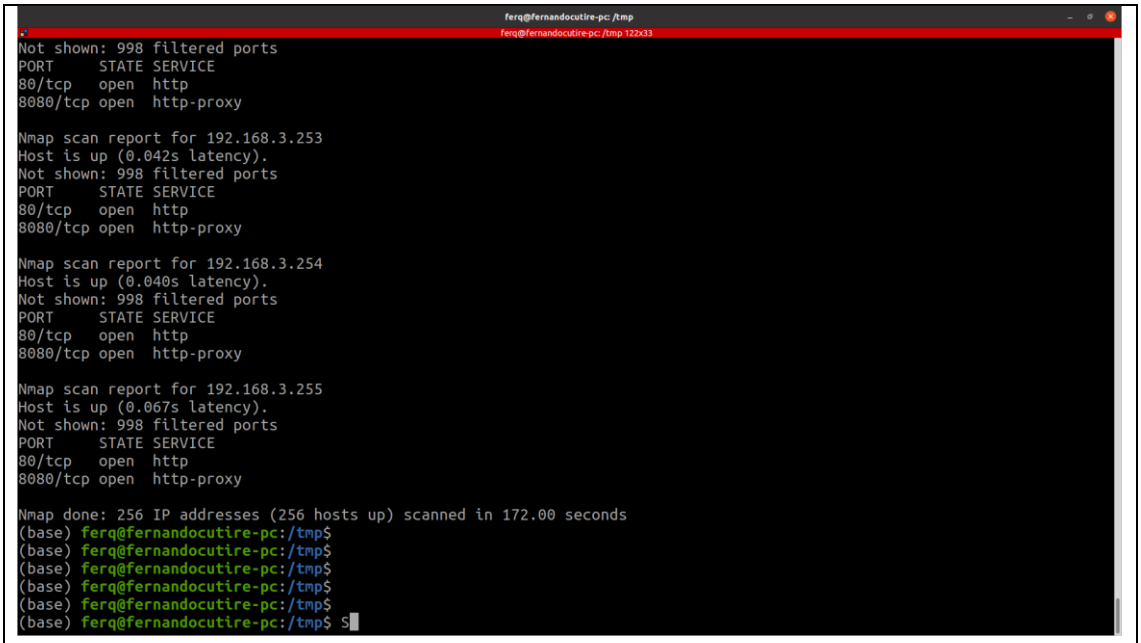
Instrucción: Escanear un rango de direcciones
`nmap 192.168.1.1-20, nmap 192.168.1.*, nmap 192.168.1.0/24`



Ejercicio 3: Lea la lista de hosts / redes desde un archivo (IPv4)

Instrucción: Crear un archivo de texto con el nombre y extensión “su_apellido.txt” (ruta: cat > /tmp/apellido.txt) para analizar el rango de direcciones (192.168.1.0/24, 192.168.1.1/24, 192.168.2.1/24, 192.168.3.1/24), ejecute el comando siguiente:

```
nmap -iL /root/Desktop/su_apellido.txt
```



Ejercicio 4: Exclusión de hosts / redes (IPv4)

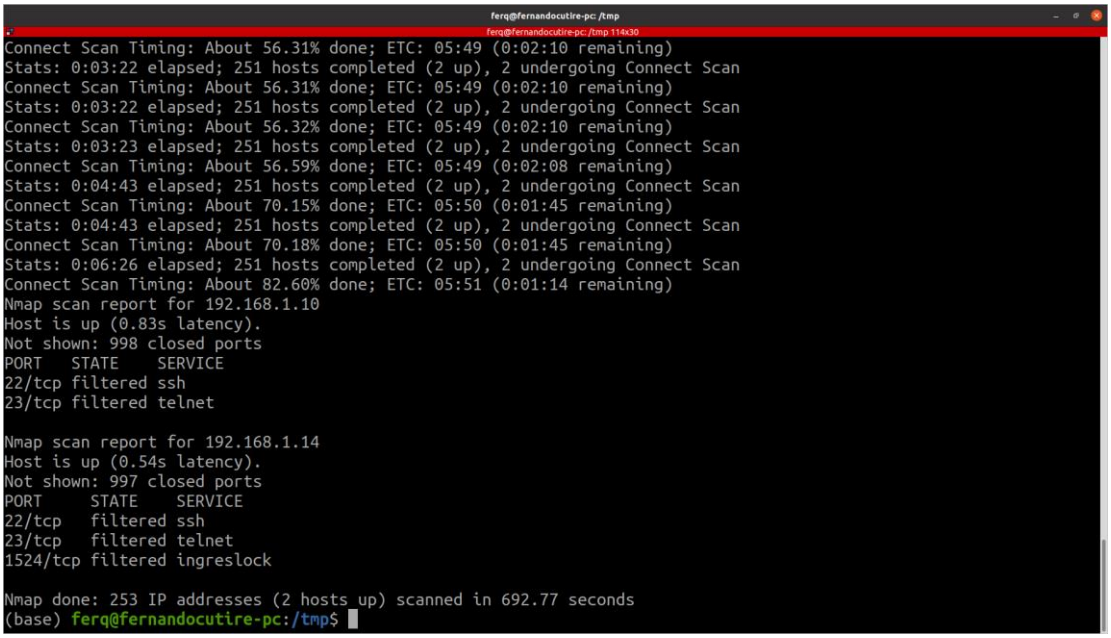
Instrucción: Escanear un gran número de hosts / redes se pueden excluir los hosts de una exploración, ejecutar lo siguiente:

```
nmap 192.168.1.0/24 --exclude 192.168.1.1
nmap 192.168.1.0/24 --exclude 192.168.1.1,192.168.1.254
nmap 192.168.1.* --exclude 192.168.1.3
```

O excluir lista desde un archivo llamado “exclude.txt” en la ruta: /tmp/exclude.txt

Ejecutar:

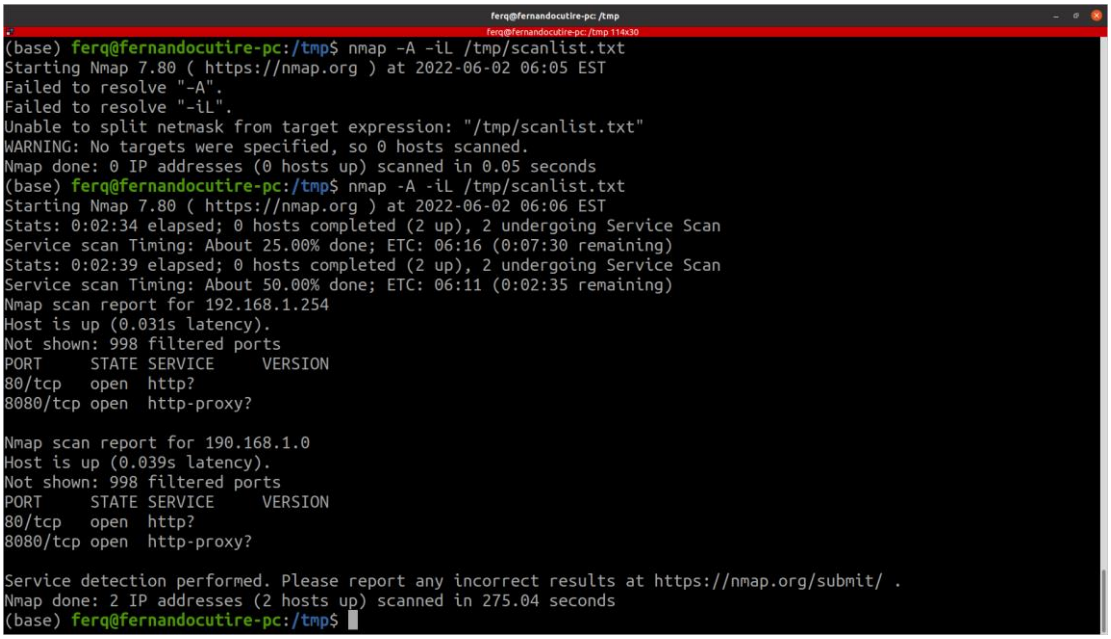
```
nmap -iL/tmp/scanlist.txt --excludefile /tmp/exclude.txt
```



Ejercicio 5: Utilice un script para detectar el sistema operativo (IPv4)

Instrucción: Se puede detectar que sistema operativo y versión se está ejecutando en el host remoto. Para habilitar la detección de sistema operativo y versión, la exploración de la escritura y la Ruta de seguimiento, podemos usar la opción "-A".

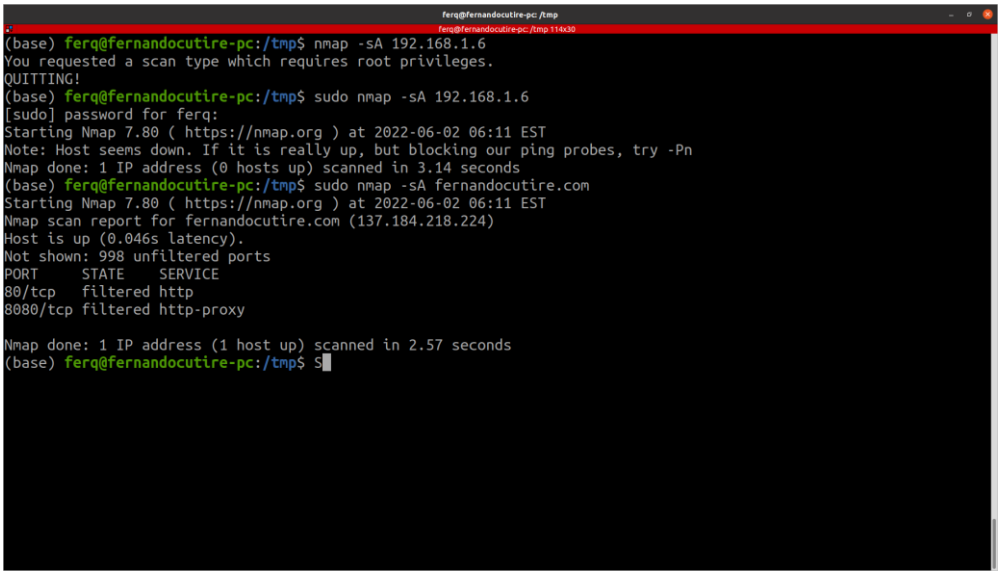
```
nmap -A 192.168.1.254
nmap -v -A 192.168.1.1
nmap -A -iL /tmp/scanlist.txt
```



Ejercicio 6: Para saber si un host / red están protegidos por un firewall

Instrucción: Ejecutar las sentencias descritas e indique los resultados

```
nmap -sA 192.168.1.6
nmap -sA server1.cyberciti.biz
```



Ejercicio 7: Escanear un host si está protegido por el firewall

Instrucción: Para escanear un host si está protegido por ningún software de filtrado de paquetes o cortafuegos. Realizar la siguiente consulta

```
nmap -PN 192.168.1.6
nmap -PN server1.cyberciti.biz
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -PN 192.168.1.6
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:16 EST
Nmap scan report for 192.168.1.6
Host is up (0.035s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -PN server1.cyberciti.biz
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:16 EST
Failed to resolve "server1.cyberciti.biz".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.22 seconds
(base) ferq@fernandocutire-pc:/tmp$ nmap -PN fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:16 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.032s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
```

Ejercicio 8: Escanear una red y averiguar qué servidores y dispositivos están en marcha

Instrucción: Con la ayuda de la opción "-sP" podemos comprobar que hosts están vivos y en red, con esta opción se salta nmap la detección de puertos y otras acciones.

```
nmap -sP 192.168.1.0/24
```

```
Host is up (0.051s latency).
Nmap scan report for 192.168.1.245
Host is up (0.045s latency).
Nmap scan report for 192.168.1.246
Host is up (0.051s latency).
Nmap scan report for 192.168.1.247
Host is up (0.051s latency).
Nmap scan report for 192.168.1.248
Host is up (0.047s latency).
Nmap scan report for 192.168.1.249
Host is up (0.047s latency).
Nmap scan report for 192.168.1.250
Host is up (0.052s latency).
Nmap scan report for 192.168.1.251
Host is up (0.051s latency).
Nmap scan report for 192.168.1.252
Host is up (0.051s latency).
Nmap scan report for 192.168.1.253
Host is up (0.051s latency).
Nmap scan report for 192.168.1.254
Host is up (0.036s latency).
Nmap scan report for 192.168.1.255
Host is up (0.048s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 0.72 seconds
```

Ejercicio 9: Realizar un análisis rápido

Instrucción: Se puede realizar un análisis rápido con la opción "-F" para las exploraciones para los puertos que figuran en los archivos de nmap-services y deja todos los demás puertos.

```
nmap -F 192.168.1.1
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -F 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:18 EST
Nmap scan report for 192.168.1.1
Host is up (0.034s latency).
Not shown: 98 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy
```

Ejercicio 10: Mostrar la razón (reason), un puerto está en un estado particular

Instrucción: Realizar la siguiente instrucción:

```
nmap –reason 192.168.1.6
nmap –reason server1.cyberciti.biz
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -reason 192.168.1.6
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:19 EST
Nmap scan report for 192.168.1.6
Host is up, received syn-ack (0.034s latency).
Not shown: 998 filtered ports
Reason: 597 host-unreaches and 401 no-responses
PORT     STATE SERVICE    REASON
80/tcp   open  http       syn-ack
8080/tcp open  http-proxy syn-ack
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -reason fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:19 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up, received syn-ack (0.029s latency).
Not shown: 996 filtered ports
Reason: 956 host-unreaches and 40 no-responses
PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack
80/tcp   open  http       syn-ack
443/tcp  open  https      syn-ack
8080/tcp open  http-proxy syn-ack
```

Ejercicio 11: Mostrar únicamente los puertos abiertos (o posiblemente abiertos)

Instrucción: Ejecutar las siguientes instrucciones para mostrar los puertos abiertos de las direcciones

```
nmap --open 192.168.1.1
nmap --open server1.cyberciti.biz
```

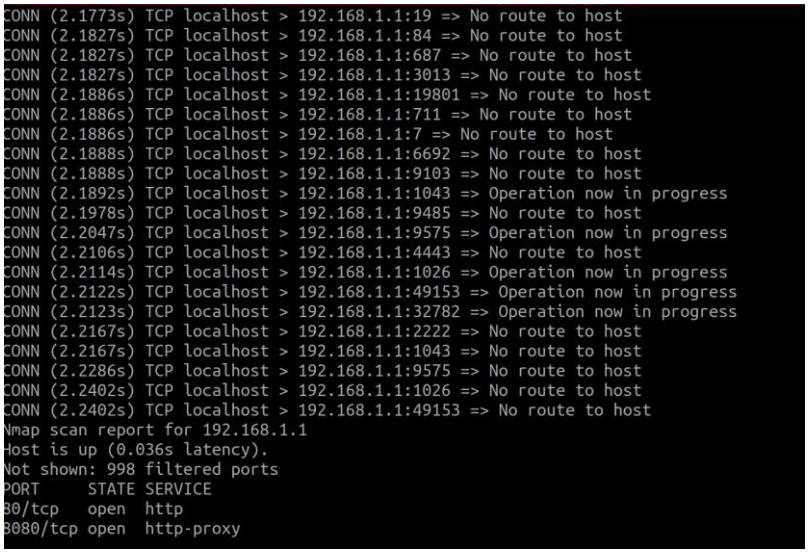
```
(base) ferq@fernandocutire-pc:/tmp$ nmap --open 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:22 EST
Nmap scan report for 192.168.1.1
Host is up (0.033s latency).
Not shown: 998 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy
```

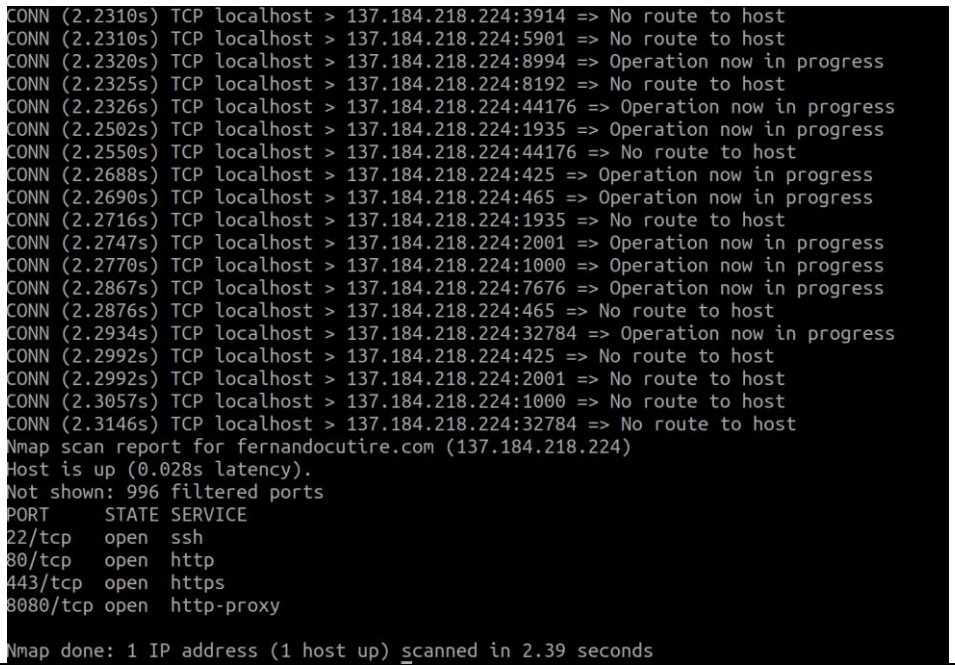
```
(base) ferq@fernandocutire-pc:/tmp$ nmap --open fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:22 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.035s latency).
Not shown: 996 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
```

Ejercicio 12: Muestra todos los paquetes enviados y recibidos

Instrucción: Ejecutar las siguientes instrucciones:

```
nmap --packet-trace 192.168.1.1
nmap --packet-trace server1.cyberciti.biz
```





Ejercicio 13: show interfaces de host y rutas

Instrucción: Ejecutar las siguientes instrucciones:

```
nmap --iflist
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap --iflist
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:26 EST
**********************INTERFACES**********************
DEV             (SHORT)           IP/MASK                     TYPE     UP MTU   MAC
lo              (lo)              127.0.0.1/8                 loopback up 65536
lo              (lo)              ::1/128                     loopback up 65536
wlp2s0          (wlp2s0)          192.168.65.24/24            ethernet up 1500  C0:B6:F9:B0:B0:49
wlp2s0          (wlp2s0)          fe80::a9dd:c5d:e30c:b75c/64 ethernet up 1500  C0:B6:F9:B0:B0:49
br-02d2ef232dd8 (br-02d2ef232dd8) 172.18.0.1/16               ethernet up 1500  02:42:FD:3D:2B:69
docker0         (docker0)         172.17.0.1/16               ethernet up 1500  02:42:6E:F8:80:CC
br-4c85140e0d28 (br-4c85140e0d28) 172.19.0.1/16               ethernet up 1500  02:42:A6:1E:DD:AB

************************ROUTES************************
DST/MASK                    DEV             METRIC GATEWAY
192.168.65.0/24             wlp2s0          600
172.17.0.0/16               docker0         0
172.18.0.0/16               br-02d2ef232dd8 0
172.19.0.0/16               br-4c85140e0d28 0
169.254.0.0/16              br-02d2ef232dd8 1000
0.0.0.0/0                   wlp2s0          600    192.168.65.20
::1/128                     lo              0
fe80::a9dd:c5d:e30c:b75c/128 wlp2s0         0
::1/128                     lo              256
fe80::/64                   wlp2s0          600
ff00::/8                    wlp2s0          256
```

Ejercicio 14: Escanear puertos específicos

Instrucción: Ejecutar las siguientes instrucciones (**nmap-p [puerto] hostName**).
Escanear el puerto 21, 23, 80 y 443.

```
nmap -p [puerto] 192.168.1.1
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -p 21,23,80,443 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:48 EST
Nmap scan report for 192.168.1.1
Host is up (0.051s latency).

PORT    STATE    SERVICE
21/tcp  filtered ftp
23/tcp  filtered telnet
80/tcp  open     http
443/tcp filtered https
```

Instrucción: Escanear el puerto **TCP** 443 (especificando el puerto)

```
nmap -p T:443 192.168.1.2
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -p T:443 192.168.1.2
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:49 EST
Nmap scan report for 192.168.1.2
Host is up (0.048s latency).

PORT    STATE    SERVICE
443/tcp filtered https
```

Instrucción: Escanear el puerto UDP 53 (especificando el puerto).

```
nmap -sU -p 53,3478 192.168.1.6
```

```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -sU -p 53,3478 fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:50 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.16s latency).

PORT     STATE         SERVICE
53/udp   open|filtered domain
3478/udp open|filtered stun
```

Instrucción: Escanear dos puertos – múltiples puertos 80, 443

```
nmap -p 80,443 192.168.1.3
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -p 80,443 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:51 EST
Nmap scan report for 192.168.1.3
Host is up (0.047s latency).

PORT    STATE    SERVICE
80/tcp  open     http
443/tcp filtered https
```

Instrucción: Escanea rangos de puertos siguiente:

```
nmap -p 80-200 192.168.1.2
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -p 80-200 192.168.1.2
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 06:52 EST
Nmap scan report for 192.168.1.2
Host is up (0.028s latency).
Not shown: 120 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.95 seconds
```

Instrucción: Combinar todas las opciones

```
nmap -p U:53,111,137,T:21-25,80,139,8080 192.168.1.6
nmap -p U:53,111,137,T:21-25,80,139,8080 server1.cyberciti.biz
nmap -v -sU -sT -p U:53,111,137,T:21-25,80,139,8080 192.168.1.6
```

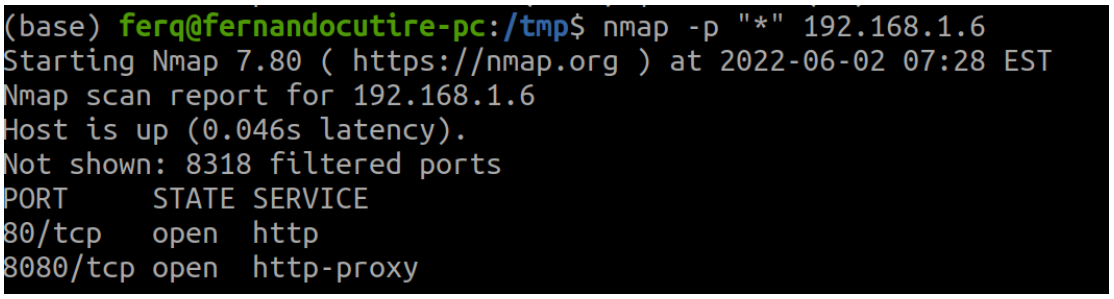
```
(base) ferq@fernandocutire-pc:/tmp$ nmap -p U:53,111,137,T:21-25,80,139,8080 192.168.1.6
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 07:25 EST
Nmap scan report for 192.168.1.6
Host is up (0.045s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
24/tcp   filtered priv-mail
25/tcp   filtered smtp
80/tcp   open     http
139/tcp  filtered netbios-ssn
8080/tcp open     http-proxy
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -p U:53,111,137,T:21-25,80,139,8080 fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 07:27 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.055s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
23/tcp   filtered telnet
24/tcp   filtered priv-mail
25/tcp   filtered smtp
80/tcp   open     http
139/tcp  filtered netbios-ssn
8080/tcp open     http-proxy
```

```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -v -sU -sT -p U:53,111,137,T:21-25,80,139,8080 192.168.1.6
[sudo] password for ferq:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 07:27 EST
Initiating Ping Scan at 07:27
Scanning 192.168.1.6 [4 ports]
Completed Ping Scan at 07:27, 3.04s elapsed (1 total hosts)
Nmap scan report for 192.168.1.6 [host down]
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.17 seconds
           Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
```

Instrucción: Analizar todos los puertos con comodín " * "

```
nmap -p "*" 192.168.1.6
```



Instrucción: Escanear puertos principales, es decir $ escanear puertos numéricos más comunes

```
nmap --top-ports 5 192.168.1.1
nmap --top-ports 10 192.168.1.1
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap --top-ports 5 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 07:29 EST
Nmap scan report for 192.168.1.1
Host is up (0.040s latency).

PORT    STATE    SERVICE
21/tcp  filtered ftp
22/tcp  filtered ssh
23/tcp  filtered telnet
80/tcp  open     http
443/tcp filtered https
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap --top-ports 10 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 07:29 EST
Nmap scan report for 192.168.1.1
Host is up (0.038s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   open     http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server
```

Ejercicio 15: La forma más rápida para escanear todos los dispositivos / equipos para puertos abiertos a la vez

Instrucción: Ejecutar la siguiente instrucción:

```
nmap -T5 192.168.1.0/24
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -T5 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 07:30 EST
Nmap scan report for 192.168.1.0
Host is up (0.042s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap scan report for 192.168.1.1
Host is up (0.063s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap scan report for 192.168.1.2
Host is up (0.065s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap scan report for 192.168.1.3
Host is up (0.048s latency).
Not shown: 998 filtered ports
```

```
Nmap scan report for 192.168.1.252
Host is up (0.052s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap scan report for 192.168.1.253
Host is up (0.051s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap scan report for 192.168.1.254
Host is up (0.047s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap scan report for 192.168.1.255
Host is up (0.050s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 256 IP addresses (240 hosts up) scanned in 133.35 seconds
```

Ejercicio 16: Detectar el sistema operativo remoto

Instrucción: Utilice la opción "-O" y "-osscan-guess" también ayuda a descubrir la información del sistema operativo.

```
nmap -O 192.168.1.6
nmap -O --osscan-guess 192.168.1.6
nmap -v -O --osscan-guess 192.168.1.6
```

El servidor `192.168.1.6 presentó problemas de conexión al momento de realizar este laboratorio.`

```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -O fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 07:33 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.045s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.46 seconds
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -O morenojose.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 07:34 EST
Nmap scan report for morenojose.com (69.163.216.148)
Host is up (0.031s latency).
rDNS record for 69.163.216.148: apache2-dap.cooston.dreamhost.com
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3690/tcp open  svn
5222/tcp open  xmpp-client
5269/tcp open  xmpp-server
8080/tcp open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
```

```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -O --osscan-guess morenojose.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 07:40 EST
Nmap scan report for morenojose.com (69.163.216.148)
Host is up (0.11s latency).
rDNS record for 69.163.216.148: apache2-dap.cooston.dreamhost.com
Not shown: 991 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
587/tcp  open  submission
3690/tcp open  svn
5222/tcp open  xmpp-client
5269/tcp open  xmpp-server
8080/tcp open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|media device|load balancer|storage-misc|WAP
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (87%), Google embedded (86%), Kemp embedded (86%), Western Digital em
bedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:kemp:loadm
aster_2400 cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:3.0 cpe:/o:linux:linux_kernel:3.10
Aggressive OS guesses: Linux 3.12 - 4.10 (87%), Linux 3.16 (87%), Google Chromecast (86%), Linux 2.6.32 (86%), Lin
ux 2.6.32 - 3.10 (86%), Linux 2.6.32 - 3.3 (86%), Linux 3.10 - 4.1 (86%), Linux 3.2.0 (86%), Kemp LoadMaster LM-24
00 Firmware 7.1 (86%), Dahua or Amcrest network video recorder (Linux) (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.75 seconds
```

```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -v -O --osscan-guess fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 07:42 EST
Initiating Ping Scan at 07:42
Scanning fernandocutire.com (137.184.218.224) [4 ports]
Completed Ping Scan at 07:42, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:42
Completed Parallel DNS resolution of 1 host. at 07:42, 0.01s elapsed
Initiating SYN Stealth Scan at 07:42
Scanning fernandocutire.com (137.184.218.224) [1000 ports]
Discovered open port 443/tcp on 137.184.218.224
Discovered open port 22/tcp on 137.184.218.224
Discovered open port 80/tcp on 137.184.218.224
Discovered open port 8080/tcp on 137.184.218.224
Completed SYN Stealth Scan at 07:42, 11.75s elapsed (1000 total ports)
Initiating OS detection (try #1) against fernandocutire.com (137.184.218.224)
Retrying OS detection (try #2) against fernandocutire.com (137.184.218.224)
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.085s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): DEC Digital UNIX 5.X (85%), iPXE 1.X (85%)
OS CPE: cpe:/o:dec:digital_unix:5.x cpe:/o:ipxe:ipxe:1.0.0%2b
Aggressive OS guesses: DEC Digital UNIX 5.X (85%), iPXE 1.0.0+ (85%)
No exact OS matches for host (test conditions non-ideal).
```

Ejercicio 17: Detectar servicios remotos (servidor / daemon) números de versión

Instrucción: Ejecutar la siguiente instrucción:
`nmap -sV 192.168.1.1`

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -sV 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:28 EST
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:01:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:02:03 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.1.1
Host is up (0.032s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE     VERSION
80/tcp   open  http?
8080/tcp open  http-proxy?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 210.75 seconds
```

Ejercicio 18: Escanear un host que utiliza TCP ACK (PA) y TCP Syn (PS) de ping

Instrucción: A veces, los cortafuegos de filtrado de paquetes bloquea las solicitudes de ping ICMP estándar, en ese caso, podemos utilizar métodos TCP ACK y TCP Syn para escanear hosts remotos. Ejecutar la siguiente instrucción:
`nmap -PS 192.168.1.6`

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -PS 192.168.1.6
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:32 EST
Nmap scan report for 192.168.1.6
Host is up (0.043s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.19 seconds
```

Ejercicio 18a - Analizar Host remoto para puertos específicos con TCP Syn

Instrucción: Realizar las siguientes instrucción:

```
nmap -PS 80,21,443 192.168.1.1
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -PS 80 fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:33 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.033s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 2 IP addresses (1 host up) scanned in 4.21 seconds
(base) ferq@fernandocutire-pc:/tmp$ nmap -PS 21 fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:34 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.031s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 2 IP addresses (1 host up) scanned in 2.92 seconds
(base) ferq@fernandocutire-pc:/tmp$ nmap -PS 443 fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:34 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.031s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 2 IP addresses (1 host up) scanned in 2.84 seconds
```

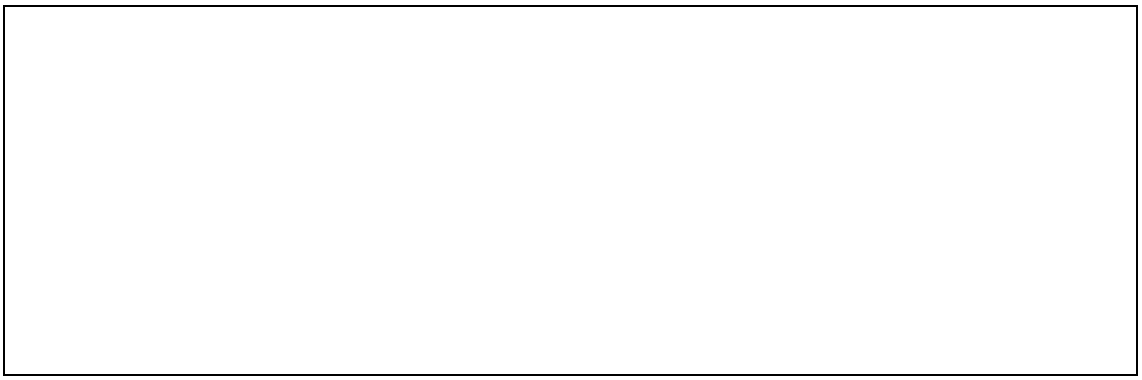
Ejercicio 18b - Analizar Host remoto para puertos específicos con TCP ACK

Instrucción: Realizar las siguientes instrucciones:

```
nmap -PA -p 22,80 192.168.1.3
nmap -PA 192.168.1.1
nmap -PA 80,21,200-512 192.168.1.1
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -PA -p 22,80 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:35 EST
Nmap scan report for 192.168.1.3
Host is up (0.050s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh
80/tcp open     http

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

```
Nmap done: 2 IP addresses (1 host up) scanned in 2.84 seconds
(base) ferq@fernandocutire-pc:/tmp$ ^C
(base) ferq@fernandocutire-pc:/tmp$
(base) ferq@fernandocutire-pc:/tmp$ nmap -PA -p 22,80 192.168.1.3
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:35 EST
Nmap scan report for 192.168.1.3
Host is up (0.050s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh
80/tcp open     http

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
(base) ferq@fernandocutire-pc:/tmp$ nmap -PA 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:36 EST
Nmap scan report for 192.168.1.1
Host is up (0.042s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 3.58 seconds
(base) ferq@fernandocutire-pc:/tmp$ nmap -PA 80,21,200-512 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:36 EST
Failed to resolve "80,21,200-512".
Nmap scan report for 192.168.1.1
Host is up (0.033s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy
```



Ejercicio 19: Escanear un host utilizando el protocolo IP

Instrucción: Ejecutar la siguiente instrucción:

```
nmap -PO 192.168.1.1
```

```
(base) ferq@fernandocutire-pc:/tmp$ nmap -PO 192.168.1.1
Sorry, IPProto Ping (-PO) only works if you are root (because we need to read raw responses off the wire)
QUITTING!
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -PO 192.168.1.1
[sudo] password for ferq:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:38 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -PO fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:38 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.084s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
```

Ejercicio 20: Escanear un host con el protocolo UDP

Instrucción: Este análisis no pasa por firewalls y filtros de pantalla que sólo TCP:

```
nmap -PU 192.168.1.1
nmap -PU 2000.2001 192.168.1.1
```

```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -PU -Pn fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:39 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.048s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
```

```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -PU 2000 -Pn fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:43 EST
Nmap scan report for 2000 (0.0.7.208)
Host is up.
All 1000 scanned ports on 2000 (0.0.7.208) are filtered

Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.13s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
```

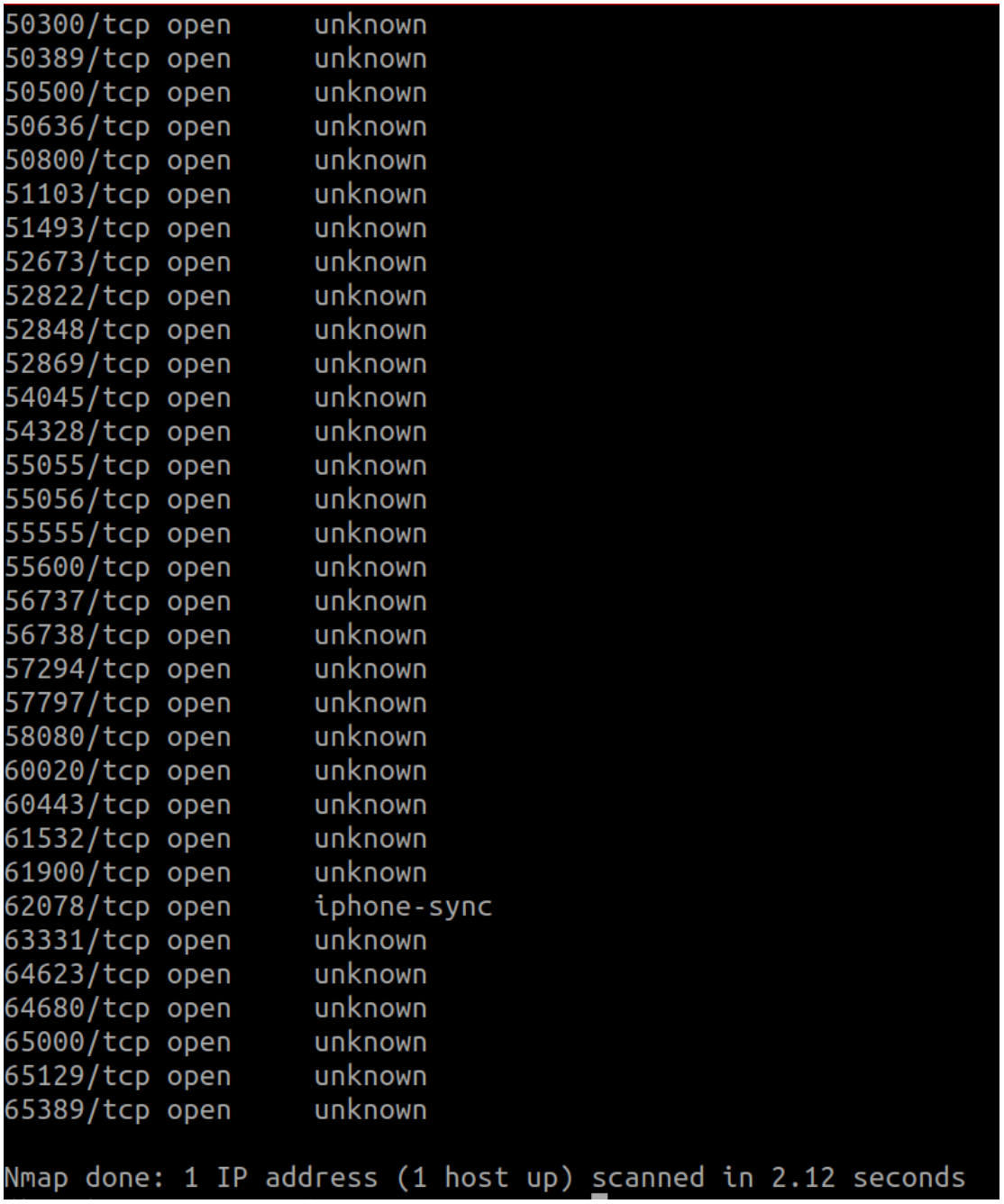
Ejercicio 21: Descubre los más utilizados los puertos TCP que utilizan TCP SYN Scan

Instrucción: Para realizar un escaneo sigiloso realizar:
`nmap -sS 192.168.1.6`

- Conoce las más comunes que utilizan los puertos TCP usando “TCP connect scan” (aviso: no hay exploración sigilosa)
- Conocer el sistema operativo - Compruebe más puertos utilizando TCP Syn # # #
  `nmap -sT 192.168.1.6`
- Conoce las más comunes que utilizan los puertos TCP usando TCP ACK scan
  `nmap -sA 192.168.1.6`
- Conoce las más comunes que utilizan los puertos TCP usando TCP Window scan
  `nmap -sW 192.168.1.6`
- Conoce las más comunes que utilizan los puertos TCP usando TCP Maimon scan
  `nmap -sM 192.168.1.6`

```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -sS fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:46 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.14s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 14.91 seconds
(base) ferq@fernandocutire-pc:/tmp$ nmap -sT 192.168.1.6
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:47 EST
Nmap scan report for 192.168.1.6
Host is up (0.036s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy
```

```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -sA fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:48 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.055s latency).
Not shown: 998 unfiltered ports
PORT     STATE    SERVICE
80/tcp   filtered http
8080/tcp filtered http-proxy
```



```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -sM fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 10:50 EST
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Maimon Scan
Maimon Scan Timing: About 69.50% done; ETC: 10:53 (0:00:52 remaining)
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Maimon Scan
Maimon Scan Timing: About 69.55% done; ETC: 10:53 (0:00:53 remaining)
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Maimon Scan
Maimon Scan Timing: About 69.60% done; ETC: 10:53 (0:00:52 remaining)
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Maimon Scan
Maimon Scan Timing: About 70.00% done; ETC: 10:53 (0:00:51 remaining)
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.17s latency).
All 1000 scanned ports on fernandocutire.com (137.184.218.224) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 172.27 seconds
```

Ejercicio 22: Escanear un host para servicios UDP (UDP scan)

Instrucción: La mayoría de los servicios populares de internet se extienden sobre el protocolo TCP. No obstante, DNS, SNMP y DHCP; estos son tres de los servicios UDP más comunes. Utilice la sintaxis siguiente para averiguar los servicios UDP:

```
nmap -sU nas03
nmap -sU 192.168.1.6
```

```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -sU fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 15:53 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.090s latency).
All 1000 scanned ports on fernandocutire.com (137.184.218.224) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 10.39 seconds
```

Ejercicio 23: Analizar en busca de protocolo IP

Instrucción: Este tipo de análisis permite determinar qué protocolos IP (TCP, ICMP, IGMP, etc) son compatibles con los equipos de destino. Ejecutar la siguiente instrucción:

```
nmap -sO 192.168.1.6
```

```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -sO fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 15:56 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.086s latency).
All 256 scanned ports on fernandocutire.com (137.184.218.224) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 28.88 seconds
```

Ejercicio 24: Escanear debilidades de seguridad en un firewall

Instrucción: Los siguientes tipos de exploración explotar una escapatoria sutil en el TCP y bueno para probar la seguridad de los ataques más comunes:

- TCP Null Scan para engañar a un servidor de seguridad para generar una respuesta
- No establece ningún bit (encabezado TCP bandera es 0).

```
nmap -sN 192.168.1.6
```

- TCP Fin scan para comprobar el firewall
- Establece sólo el bit TCP FIN

```
nmap -sF 192.168.1.6
```

- TCP Xmas escaneado para comprobar firewall
- Establece el FIN, PSH, URG y banderas, encendiendo el paquete como un árbol de Navidad

```
nmap -sX 192.168.1.6
```

```
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -sN fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 15:58 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.085s latency).
All 1000 scanned ports on fernandocutire.com (137.184.218.224) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 86.96 seconds
(base) ferq@fernandocutire-pc:/tmp$ nmap -sF fernandocutire.com
You requested a scan type which requires root privileges.
QUITTING!
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -sF fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 16:00 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.13s latency).
All 1000 scanned ports on fernandocutire.com (137.184.218.224) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 16.15 seconds
(base) ferq@fernandocutire-pc:/tmp$ nmap -sX 192.168.1.6
You requested a scan type which requires root privileges.
QUITTING!
(base) ferq@fernandocutire-pc:/tmp$ sudo nmap -sX fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 16:01 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up (0.11s latency).
All 1000 scanned ports on fernandocutire.com (137.184.218.224) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 11.18 seconds
```

Ejercicio 25: Digitalizar un servidor de seguridad de los fragmentos de paquetes

Instrucción: La opción-f hace que la exploración solicitada (incluyendo las exploraciones ping) a utilizar pequeños paquetes IP fragmentados. La idea es dividir la cabecera TCP a través de varios paquetes para que sea más difícil para los filtros de paquetes, sistemas de detección de intrusos y otras molestias para detectar lo que está haciendo.

```
nmap -f 192.168.1.1
nmap -f fw2.nixcraft.net.in
nmap -f 15 fw2.nixcraft.net.in
```

- Establece el tamaño de su propia compensación con la opción --mtu

```
nmap --mtu 32 192.168.1.1
```

```
(base) ferq@fernandocutire-pc:~$ sudo nmap -f -Pn 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 16:26 EST
Nmap scan report for 192.168.1.1
Host is up.
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.40 seconds
```

```
(base) ferq@fernandocutire-pc:~$ sudo nmap -f -Pn fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 16:31 EST
Nmap scan report for fernandocutire.com (137.184.218.224)
Host is up.
All 1000 scanned ports on fernandocutire.com (137.184.218.224) are filtered
```

```
(base) ferq@fernandocutire-pc:~$ sudo nmap -f 15 -Pn fernandocutire.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 16:36 EST
Failed to resolve "fernandocutire.com".
Failed to resolve "fernandocutire.com".
Nmap scan report for 15 (0.0.0.15)
Host is up.
All 1000 scanned ports on 15 (0.0.0.15) are filtered

Failed to resolve "fernandocutire.com".
Nmap done: 1 IP address (1 host up) scanned in 231.41 seconds
```

```
(base) ferq@fernandocutire-pc:~$ sudo nmap --mtu 32 -Pn 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 16:41 EST
Nmap scan report for 192.168.1.1
Host is up.
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap done: 1 IP address (1 host up) scanned in 206.51 seconds
```

Ejercicio 26: Capa de un análisis con señuelos

Instrucción: La opción-D que aparece al host remoto que el host (s) se especifica como señuelos a escanear la red de destino también. Así, sus IDS puede informar escaneos de puertos 5-10 de direcciones IP únicas, pero no sabrán qué IP se escanearlos y que eran señuelos inocentes:

```
nmap -n -Ddecoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4
remote-host-ip
nmap -n -D192.168.1.5,10.5.1.2,172.1.2.4,3.4.2.1 192.168.1.5
```

```
(base) ferq@fernandocutire-pc:~$ sudo nmap -n -Pn -D192.168.1.5,10.5.1.2,172.1.2.4,3.4.2.1 192.168.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 16:46 EST
Nmap scan report for 192.168.1.5
Host is up.
All 1000 scanned ports on 192.168.1.5 are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.39 seconds
```

Ejercicio 27: Digitalizar un firewall para la falsificación de direcciones MAC

Instrucción: Realice un “Spoof” (disfrazar) de su dirección MAC

```
nmap --spoof-mac MAC-ADDRESS-HERE 192.168.1.6
```

Añadir otra opción

```
nmap -v -sT -PN --spoof-mac MAC-ADDRESS-HERE 192.168.1.6
```

Usar una dirección MAC aleatoria:
El número 0, significa nmap elige una dirección MAC al azar

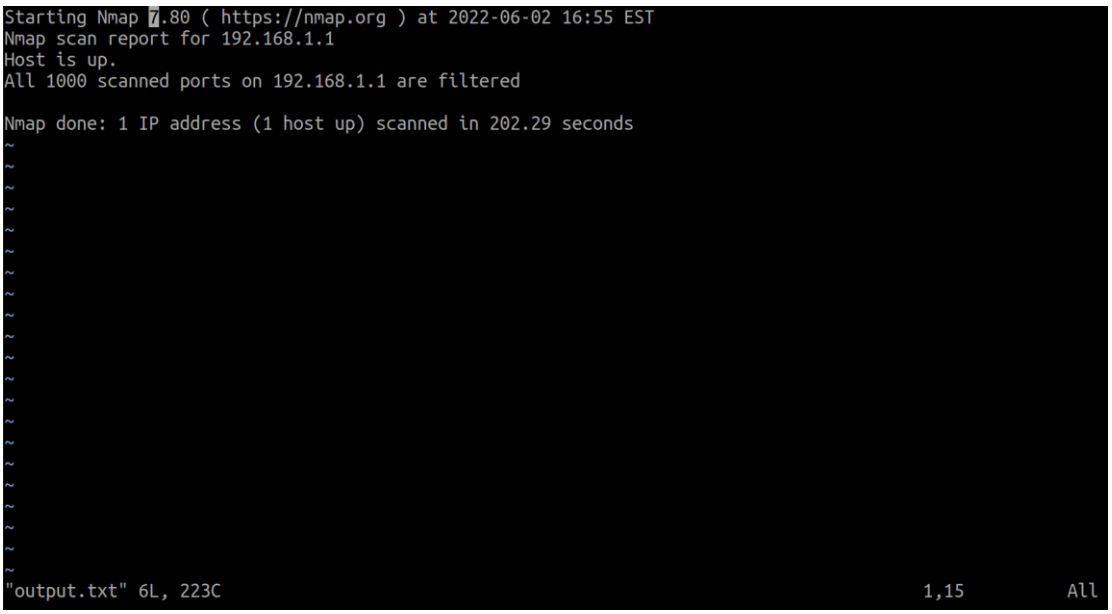
```
nmap -v -sT -PN --spoof-mac 0 192.168.1.1
```

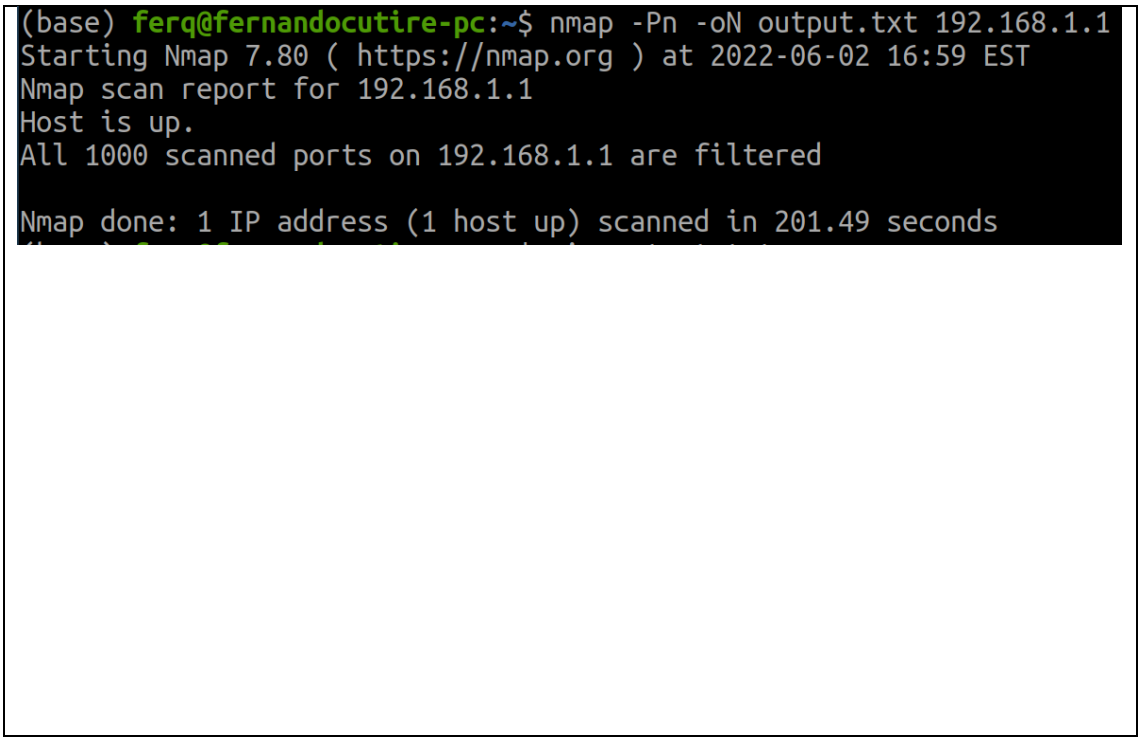
```
(base) ferq@fernandocutire-pc:~$ nmap -v -sT -Pn --spoof-mac 0 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 16:50 EST
Spoofing MAC address 17:61:44:13:A6:4F (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored without the necessary privileges.
Initiating Parallel DNS resolution of 1 host. at 16:50
Completed Parallel DNS resolution of 1 host. at 16:50, 0.05s elapsed
Initiating Connect Scan at 16:50
Scanning 192.168.1.1 [1000 ports]
Connect Scan Timing: About 15.50% done; ETC: 16:53 (0:02:49 remaining)
Connect Scan Timing: About 30.50% done; ETC: 16:53 (0:02:19 remaining)
Connect Scan Timing: About 45.50% done; ETC: 16:53 (0:01:49 remaining)
Connect Scan Timing: About 60.50% done; ETC: 16:53 (0:01:19 remaining)
Connect Scan Timing: About 75.50% done; ETC: 16:53 (0:00:49 remaining)
Completed Connect Scan at 16:53, 201.38s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up.
All 1000 scanned ports on 192.168.1.1 are filtered

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 201.48 seconds
```

Ejercicio 28: Guardar la salida en un archivo de texto

Instrucción: Ejecute la siguientes instrucciones para guardar en un archivo de texto.

```
nmap 192.168.1.1 > output.txt
nmap -oN /path/to/filename 192.168.1.1
nmap -oN output.txt 192.168.1.1
```





Ejercicio 29: Versión de NMAP instalado

Instrucción: Ejecutar la siguiente instrucción para conocer la versión de nmap instalado.

```
nmap -V
```

```
(base) ferq@fernandocutire-pc:~$ nmap -Pn -oN output.txt 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 16:59 EST
Nmap scan report for 192.168.1.1
Host is up.
All 1000 scanned ports on 192.168.1.1 are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.49 seconds
```

Ejercicio 30: Escaneo de puertos de forma consecutiva

Instrucción: Ejecutar la siguiente instrucción:

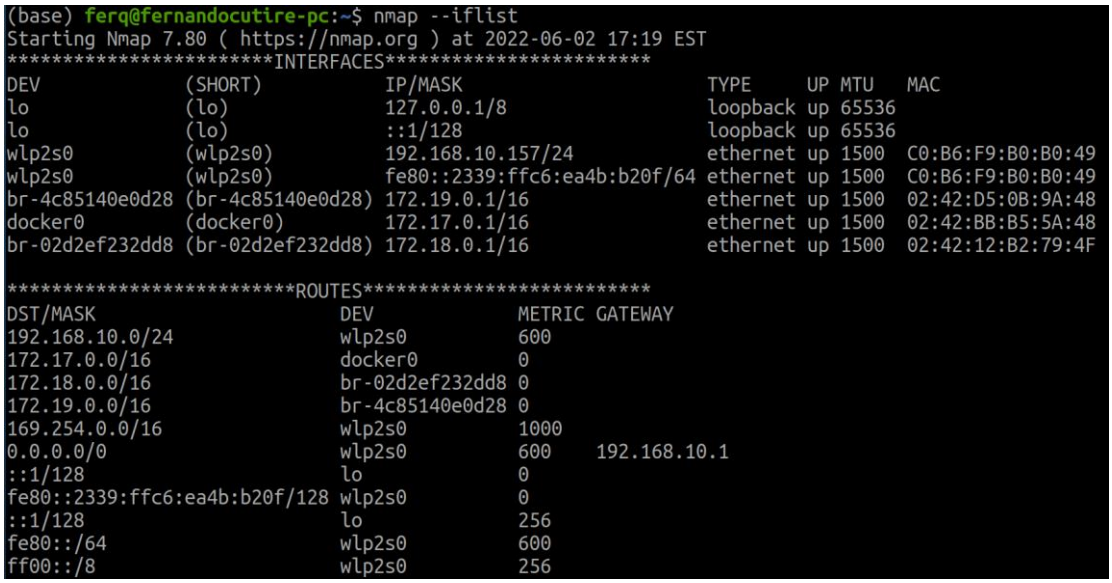
```
nmap -r 192.168.0.101
```

```
(base) ferq@fernandocutire-pc:~$ nmap -r -Pn 192.168.0.101
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 17:14 EST
Nmap scan report for 192.168.0.101
Host is up.
All 1000 scanned ports on 192.168.0.101 are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.44 seconds
```

Ejercicio 31: Interfaces de impresión de Host y rutas

Instrucción: Usted puede encontrar la interfaz y ruta de información de host con nmap con la opción "-iflist". Ejecutar lo siguiente:

```
nmap --iflist
```



Laboratorio 1: Uso de Zenmap

Explicación: Esta opción sondea todos los puertos TCP reservados en el servidor scanme.nmap.org. La opción -v activa el modo detallado (también llamado verboso). `nmap -v scanme.nmap.org`

Indique los resultados:

```
(base) ferq@fernandocutire-pc:~$ nmap -v scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 17:20 EST
Initiating Ping Scan at 17:20
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 17:20, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:20
Completed Parallel DNS resolution of 1 host. at 17:20, 0.19s elapsed
Initiating Connect Scan at 17:20
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
```

```
Completed Ping Scan at 17:20, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:20
Completed Parallel DNS resolution of 1 host. at 17:20, 0.19s elapsed
Initiating Connect Scan at 17:20
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 75 out of 249 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 5 to 10 due to max_successful_tryno increase to 4
Discovered open port 31337/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 10 to 20 due to max_successful_tryno increase to 5
Increasing send delay for 45.33.32.156 from 20 to 40 due to max_successful_tryno increase to 6
Discovered open port 9929/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 40 to 80 due to max_successful_tryno increase to 7
Completed Connect Scan at 17:21, 54.59s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.15s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 55.16 seconds
```

Explicación: Lanza un sondeo de tipo SYN sigiloso contra cada una de las 255 máquinas en la “clase C” de la red donde está el sistema "analizame". También intenta determinar cuál es el sistema operativo que se ejecuta en cada máquina que esté encendida. Esto requiere permisos de root por la opción de sondeo SYN y por la de detección de sistema operativo.

```
nmap -sS -O scanme.nmap.org/24
```

Indique los resultados:

```
Network Distance: 11 hops

Nmap scan report for li982-82.members.linode.com (45.33.32.82)
Host is up (0.17s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https
Aggressive OS guesses: Linux 2.6.32 - 3.13 (96%), Linux 2.6.22 - 2.6.36 (94%), Linux 3.10 - 4.11 (94%), Lin
ux 2.6.32 (94%), Linux 3.2 - 4.9 (94%), Linux 2.6.32 - 3.10 (93%), HP P2000 G3 NAS device (93%), Linux 2.6.
18 (93%), Linux 3.10 (93%), Linux 2.6.26 - 2.6.35 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for li982-83.members.linode.com (45.33.32.83)
Host is up (0.17s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (94%), Linux 2.6.32 - 3.10 (93%), Linux 2.6.32 (92%), Linux 3.10 - 4
.11 (92%), Synology DiskStation Manager 5.2-5644 (92%), Linux 2.6.32 - 3.13 (92%), Linux 2.6.22 - 2.6.36 (9
1%), Linux 3.4 - 3.10 (91%), Linux 2.6.39 (91%), Linux 3.10 (90%)
No exact OS matches for host (test conditions non-ideal).
```

Explicación: Lanza una enumeración de equipos y un sondeo TCP a cada uno de la primera mitad de las 255 posibles subredes de 8 bit en la red de clase B 198.116. Esto probará si los sistemas están ejecutando sshd, DNS, pop3d, imapd o tienen un servidor en el puerto 4564. Para cualquier puerto que se encuentre abierto, se realizará una detección de versión para determinar qué aplicación se está ejecutando.

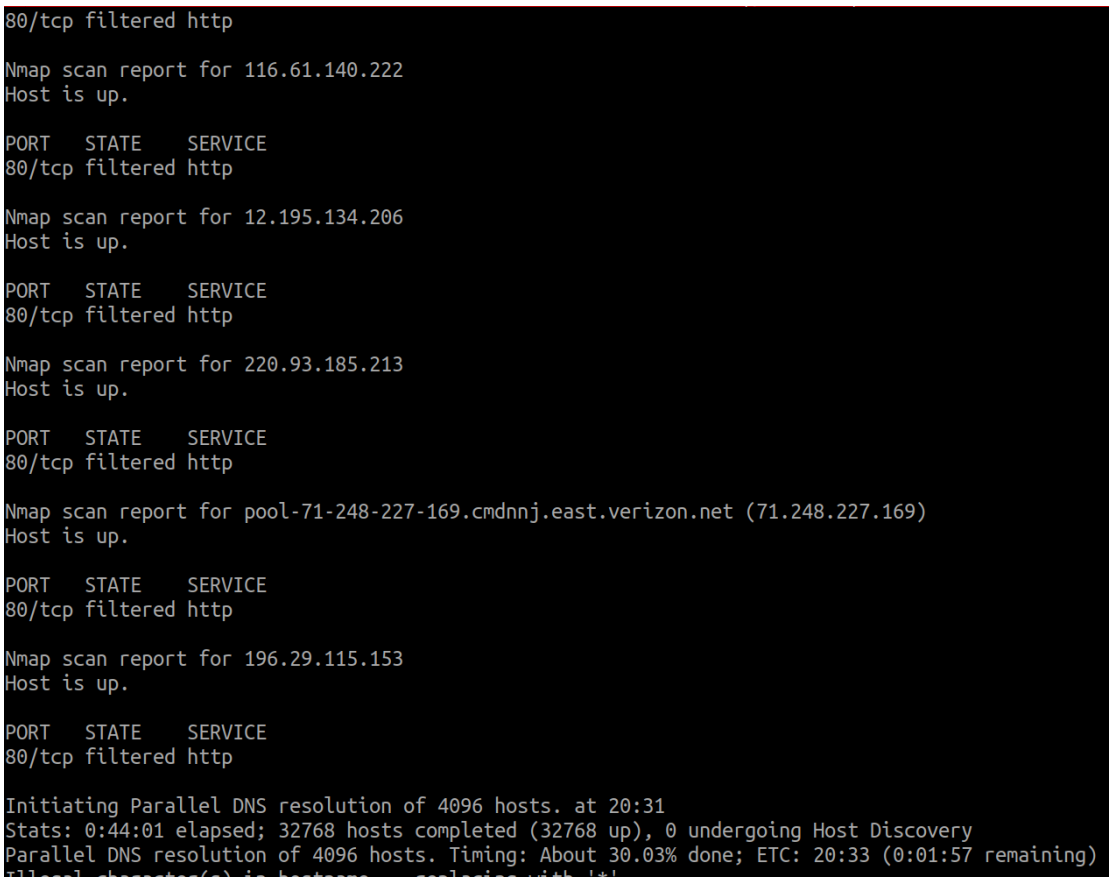
Ejecutar: `nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127`

Indique los resultados:

```
(base) ferq@fernandocutire-pc:~$ nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-02 18:43 EST
Stats: 0:10:20 elapsed; 20450 hosts completed (30 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 81.81% done; ETC: 18:54 (0:01:10 remaining)
Stats: 0:10:21 elapsed; 20450 hosts completed (30 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 81.92% done; ETC: 18:54 (0:01:09 remaining)
Stats: 0:10:21 elapsed; 20450 hosts completed (30 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 81.99% done; ETC: 18:54 (0:01:09 remaining)
Stats: 0:10:21 elapsed; 20450 hosts completed (30 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 82.06% done; ETC: 18:54 (0:01:09 remaining)
Stats: 0:10:22 elapsed; 20450 hosts completed (30 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 82.17% done; ETC: 18:54 (0:01:08 remaining)
Nmap scan report for biz2.arc.nasa.gov (198.116.3.33)
Host is up (0.20s latency).

PORT     STATE    SERVICE VERSION
22/tcp   filtered ssh
53/tcp   filtered domain
110/tcp  filtered pop3
143/tcp  filtered imap
4564/tcp filtered unknown

Nmap scan report for narwhal.arc.nasa.gov (198.116.3.72)
Host is up (0.17s latency).

PORT     STATE    SERVICE VERSION
22/tcp   filtered ssh
53/tcp   filtered domain
110/tcp  filtered pop3
143/tcp  filtered imap
4564/tcp filtered unknown
```

```
4564/tcp closed unknown

Nmap scan report for gsfcvpn.nasa.gov (198.116.203.2)
Host is up (0.14s latency).

PORT     STATE    SERVICE VERSION
22/tcp   filtered ssh
53/tcp   filtered domain
110/tcp  filtered pop3
143/tcp  filtered imap
4564/tcp filtered unknown

Nmap scan report for jscwebvpn.nasa.gov (198.116.209.1)
Host is up (0.13s latency).

PORT     STATE  SERVICE VERSION
22/tcp   closed ssh
53/tcp   closed domain
110/tcp  closed pop3
143/tcp  closed imap
4564/tcp closed unknown

Nmap scan report for jscvpn.nasa.gov (198.116.209.2)
Host is up (0.14s latency).

PORT     STATE    SERVICE VERSION
22/tcp   filtered ssh
53/tcp   filtered domain
110/tcp  filtered pop3
143/tcp  filtered imap
4564/tcp filtered unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32512 IP addresses (41 hosts up) scanned in 1164.18 seconds
```


Ejecutar: `nmap -v -iR 100000 -P0 -p 80` Explicación: Solicita a Nmap que elija 100.000 sistemas aleatoriamente y los sondee buscando servidores web (puerto 80). La enumeración de sistemas se deshabilita con -P0 ya que es un desperdicio enviar un par de pruebas para determinar si el sistema debe ser analizado cuando de todas maneras sólo se va a analizar un puerto.
Indique los resultados:



Explicación: Esto sondea 4096 IP's para buscar cualquier servidor web (sin enviar sondas ICMP) y guarda la salida en formato para grep y en XML.

```
nmap -P0 -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20
```

Indique los resultados:

```
80/tcp filtered http

Nmap scan report for 116.61.140.222
Host is up.

PORT   STATE    SERVICE
80/tcp filtered http

Nmap scan report for 12.195.134.206
Host is up.

PORT   STATE    SERVICE
80/tcp filtered http

Nmap scan report for 220.93.185.213
Host is up.

PORT   STATE    SERVICE
80/tcp filtered http

Nmap scan report for pool-71-248-227-169.cmdnnj.east.verizon.net (71.248.227.169)
Host is up.

PORT   STATE    SERVICE
80/tcp filtered http

Nmap scan report for 196.29.115.153
Host is up.

PORT   STATE    SERVICE
80/tcp filtered http

Initiating Parallel DNS resolution of 4096 hosts. at 20:31
Stats: 0:44:01 elapsed; 32768 hosts completed (32768 up), 0 undergoing Host Discovery
Parallel DNS resolution of 4096 hosts. Timing: About 30.03% done; ETC: 20:33 (0:01:57 remaining)
```

Fuente: https://nmap.org/man/es/man-examples.html