Seguridad en Redes
Practica 3.1

David Antuña Rodríguez
Javier Carrión García

No tenemos la maquina Ubuntu porque no nos permitia descargarla.

1 Sniffing con Wireshark

Como no tenemos la maquina ubuntu solo hemos realizado los ping a metasploit.
Aparecen dos paquetes ICMP, uno de echo request y otro de echo reply.

Trama ICMP (request)
IP origen 192.168.2.2
IP destino 192.168.1.1
MAC origen 08:00:27:66:bf:ba
MAC destino 08:00:27:43:e6:46

Trama ICMP (reply)
IP origen 192.168.1.1
IP destino 192.168.2.2
MAC origen 08:00:27:43:e6:46
MAC destino 08:00:27:66:bf:ba

La IP 192.168.2.2 y la MAC 08:00:27:66:bf:ba pertenecen a la maquina Host(atacante).
La IP 192.168.1.1 y la MAC 08:00:27:43:e6:46 pertenecen a la maquina metasploitable.

2 Network scanning con nmap

2.1 Descubrimieto de IPs

Utiliza una ARP request para cada una de las posibles direcciones de la red.
Ambos escaneos detectan los mismos host pero el segundo tambien determina la MAC del router.

```
usuario@debian:~$ nmap -sn 192.168.2.0/24

Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:12 CET
Nmap scan report for 192.168.2.2
Host is up (0.00035s latency).
Nmap scan report for 192.168.2.3
Host is up (0.00037s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.01 seconds
```

Figure 2.1.1 : Sondeo red 2 sin sudo.

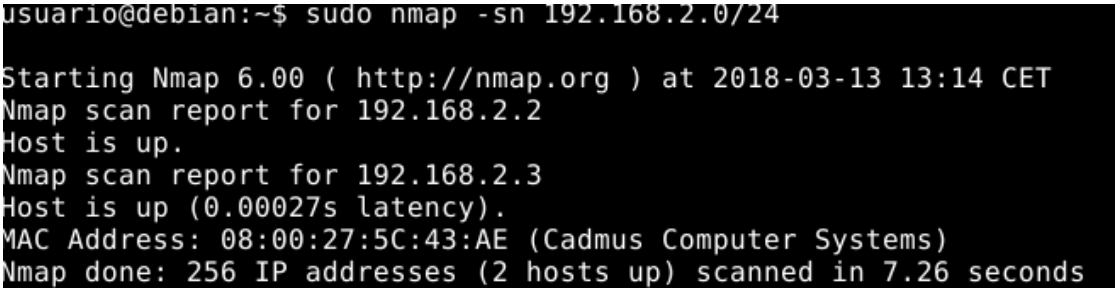

Figure 2.1.2 : Sondeo red 2 con sudo.

No hay diferencia en sus resultados pero el segundo escaneo ha tardado más en completarse.
Ahora no es capaz de devolver la MAC del router porque no forma parte de la red que está escaneando.

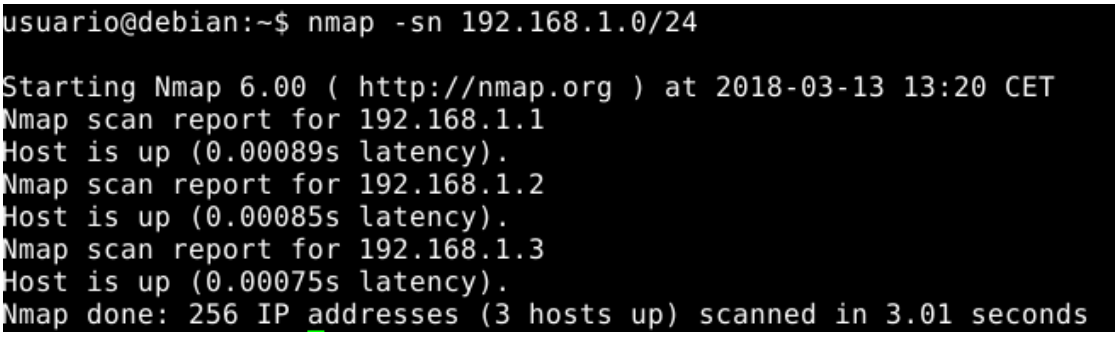

Figure 2.1.3 : Sondeo red 1 sin sudo.

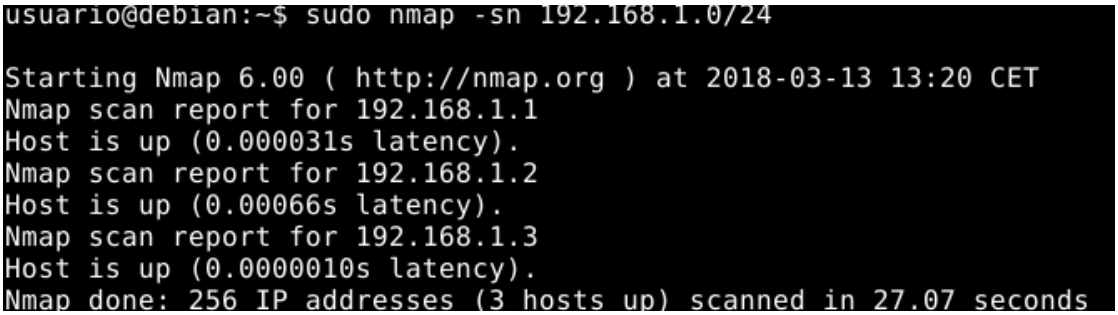

Figure 2.1.4 : Sondeo red 1 con sudo.

2.2 Escaneo de puertos

Cuando el puerto está abierto se contesta con un mensaje TCP que tiene las flags RST y ACK activas, no puede detectar puertos UDP porque el escaneo es por TCP.

```
usuario@debian:~$ sudo nmap -sS 192.168.2.3 --reason

Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:30 CET
Nmap scan report for 192.168.2.3
Host is up, received arp-response (0.00012s latency).
Not shown: 998 closed ports
Reason: 998 resets
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
23/tcp open  telnet  syn-ack
MAC Address: 08:00:27:43:E6:46 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 16.56 seconds
```

Figure 2.2.1 : sudo nmap −sS 192.168.2.3 −−reason

```
Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:36 CET
Nmap scan report for 192.168.1.1
Host is up (0.00064s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 16.58 seconds
```

Figure 2.2.2 : sudo nmap −sS 192.168.1.1

```
usuario@debian:~$ sudo nmap -sS 192.168.1.2

Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:35 CET
Nmap scan report for 192.168.1.2
Host is up (0.0011s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 22.09 seconds
```

Figure 2.2.3 : sudo nmap −sS 192.168.1.2

Repetimos los escaneos para el puerto 80 despues de añadir la nueva regla.

```
usuario@debian:~$ sudo nmap -sS 192.168.2.3 -p 80 --reason

Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:41 CET
Nmap scan report for 192.168.2.3
Host is up, received arp-response (0.00022s latency).
PORT   STATE  SERVICE REASON
80/tcp closed http    reset
MAC Address: 08:00:27:43:E6:46 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 16.53 seconds
usuario@debian:~$
usuario@debian:~$
usuario@debian:~$ sudo nmap -sF 192.168.2.3 -p 80 --reason

Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:41 CET
Nmap scan report for 192.168.2.3
Host is up, received arp-response (0.00025s latency).
PORT   STATE  SERVICE REASON
80/tcp closed http    reset
MAC Address: 08:00:27:43:E6:46 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 16.53 seconds
```

Figure 2.2.4 : sudo nmap −sS 192.168.2.3 −p 80 −−reason.

```
usuario@debian:~$ sudo nmap -sS 192.168.1.2 -p 80

Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:42 CET
Nmap scan report for 192.168.1.2
Host is up (0.00045s latency).
PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 16.53 seconds
usuario@debian:~$
usuario@debian:~$
usuario@debian:~$
usuario@debian:~$ sudo nmap -sF 192.168.1.2 -p 80

Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:43 CET
Nmap scan report for 192.168.1.2
Host is up (0.00053s latency).
PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 16.53 seconds
```

Figure 2.2.5 : sudo nmap −sS 192.168.1.2 −p 80

```
usuario@debian:~$ sudo nmap -sS 192.168.1.1 -p 80

Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:43 CET
Nmap scan report for 192.168.1.1
Host is up (0.0020s latency).
PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds
usuario@debian:~$
usuario@debian:~$
usuario@debian:~$
usuario@debian:~$ sudo nmap -sF 192.168.1.1 -p 80

Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:44 CET
Nmap scan report for 192.168.1.1
Host is up (0.00033s latency).
PORT   STATE         SERVICE
80/tcp open|filtered http

Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds
```

Figure 2.2.6 : sudo nmap −sS 192.168.1.1 −p 80

Exploracion de los puertos TCP en metasploitable.

```
usuario@debian:~$ sudo nmap -sA 192.168.1.1

Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:48 CET
Nmap scan report for 192.168.1.1
Host is up (0.00016s latency).
All 1000 scanned ports on 192.168.1.1 are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 16.56 seconds
```

Figure 2.2.7 : Sondeo TCP ACK.

```
Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:47 CET
Nmap scan report for 192.168.1.1
Host is up (0.00033s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 17.83 seconds
```

Figure 2.2.8 : Sondeo TCP FIN.

2.3 Detectar servicios y versiones

```
usuario@debian:~$ sudo nmap -sV 192.168.1.1

Starting Nmap 6.00 ( http://nmap.org ) at 2018-03-13 13:50 CET
Nmap scan report for 192.168.1.1
Host is up (0.00037s latency).
Not shown: 977 closed ports
PORT     STATE    SERVICE              VERSION
21/tcp   open     ftp                  vsftpd 2.3.4
22/tcp   open     ssh                  OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet               Linux telnetd
25/tcp   open     smtp                 Postfix smtpd
53/tcp   open     domain               ISC BIND 9.4.2
80/tcp   filtered http
111/tcp  open     rpcbind (rpcbind V2) 2 (rpc #100000)
139/tcp  open     netbios-ssn          Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn          Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open     exec                 netkit-rsh rexecd
513/tcp  open     login?
514/tcp  open     shell?
1099/tcp open     rmiregistry          GNU Classpath grmiregistry
1524/tcp open     ingreslock?
2049/tcp open     nfs (nfs V2-4)       2-4 (rpc #100003)
2121/tcp open     ftp                  ProFTPD 1.3.1
3306/tcp open     mysql                MySQL 5.0.51a-3ubuntu5
5432/tcp open     postgresql           PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc                  VNC (protocol 3.3)
6000/tcp open     X11                  (access denied)
6667/tcp open     irc                  Unreal ircd
8009/tcp open     ajp13                Apache Jserv (Protocol v1.3)
8180/tcp open     http                 Apache Tomcat/Coyote JSP engine 1.1
2 services unrecognized despite returning data. If you know the service/version, pl
ttp://www.insecure.org/cgi-bin/servicefp-submit.cgi :
```

Figure 2.3.1 : Deteccion de servicios en metasploit.

```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port514-TCP:V=6.00%I=7%D=3/13%Time=5AA7C925%P=x86_64-unknown-linux-gnu%
SF:r(NULL,33,"\x01getnameinfo:\x20Temporary\x20failure\x20in\x20name\x20re
SF:solution\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1524-TCP:V=6.00%I=7%D=3/13%Time=5AA7C92B%P=x86_64-unknown-linux-gnu
SF:%r(NULL,17,"root@metasploitable:/#\x20")%r(GenericLines,73,"root@metasp
SF:loitable:/#\x20root@metasploitable:/#\x20root@metasploitable:/#\x20root
SF:@metasploitable:/#\x20root@metasploitable:/#\x20")%r(GetRequest,428,"ro
SF:ot@metasploitable:/#\x20<HTML>\n<HEAD>\n<TITLE>Directory\x20/</TITLE>\n
SF:<BASE\x20HREF=\"file:/\">\n</HEAD>\n<BODY>\n<H1>Directory\x20listing\x2
SF:0of\x20/</H1>\n<UL>\n<LI><A\x20HREF=\"\./\">\./</A>\n<LI><A\x20HREF=\"\
SF:.\./\">\.\./</A>\n<LI><A\x20HREF=\"bin/\">bin/</A>\n<LI><A\x20HREF=\"bo
SF:ot/\">boot/</A>\n<LI><A\x20HREF=\"cdrom/\">cdrom/</A>\n<LI><A\x20HREF=\
SF:"dev/\">dev/</A>\n<LI><A\x20HREF=\"etc/\">etc/</A>\n<LI><A\x20HREF=\"ho
SF:me/\">home/</A>\n<LI><A\x20HREF=\"initrd/\">initrd/</A>\n<LI><A\x20HREF
SF:=\"initrd\.img\">initrd\.img</A>\n<LI><A\x20HREF=\"lib/\">lib/</A>\n<LI
SF:><A\x20HREF=\"lost%2Bfound/\">lost\+found/</A>\n<LI><A\x20HREF=\"media/
SF:\">media/</A>\n<LI><A\x20HREF=\"mnt/\">mnt/</A>\n<LI><A\x20HREF=\"nohup
SF:\.out\">nohup\.out</A>\n<LI><A\x20HREF=\"opt/\">opt/</A>\n<LI><A\x20HRE
SF:F=\"proc/\">proc/</A>\n<LI><A\x20HREF=\"root/\">root/</A>\n<LI><A\x20HR
SF:EF=\"sbin/\">sbin/</A>\n<LI><A\x20HREF=\"srv/\">srv/</A>\n<LI><A\x20HRE
SF:F=\"sys/\">sys/</A>\n<LI><A\x20HREF=\"tmp/\">tmp/</A>\n<LI><A\x20HREF=\
SF:"usr/\">usr/</A>\n<LI><A\x20HREF=\"var/\">var/</A>\n<LI><A\x20HREF=\"vm
SF:linuz\">vmlinuz</A>\n<")%r(HTTPOptions,94,"root@metasploitable:/#\x20ba
SF:sh:\x20OPTIONS:\x20command\x20not\x20found\nroot@metasploitable:/#\x20r
SF:oot@metasploitable:/#\x20root@metasploitable:/#\x20root@metasploitable:
SF:/#\x20")%r(RTSPRequest,94,"root@metasploitable:/#\x20bash:\x20OPTIONS:\
SF:x20command\x20not\x20found\nroot@metasploitable:/#\x20root@metasploitab
SF:le:/#\x20root@metasploitable:/#\x20root@metasploitable:/#\x20")%r(RPCCh
SF:eck,17,"root@metasploitable:/#\x20")%r(DNSVersionBindReq,17,"root@metas
SF:ploitable:/#\x20")%r(DNSStatusRequest,17,"root@metasploitable:/#\x20")%
```

Figure 2.3.2 : Deteccion de servicios en metasploit (2).

2.4 Detectar sistema operativo

La maquina de Windows se cayó y no pudimos ejecutar este apartado en ella.

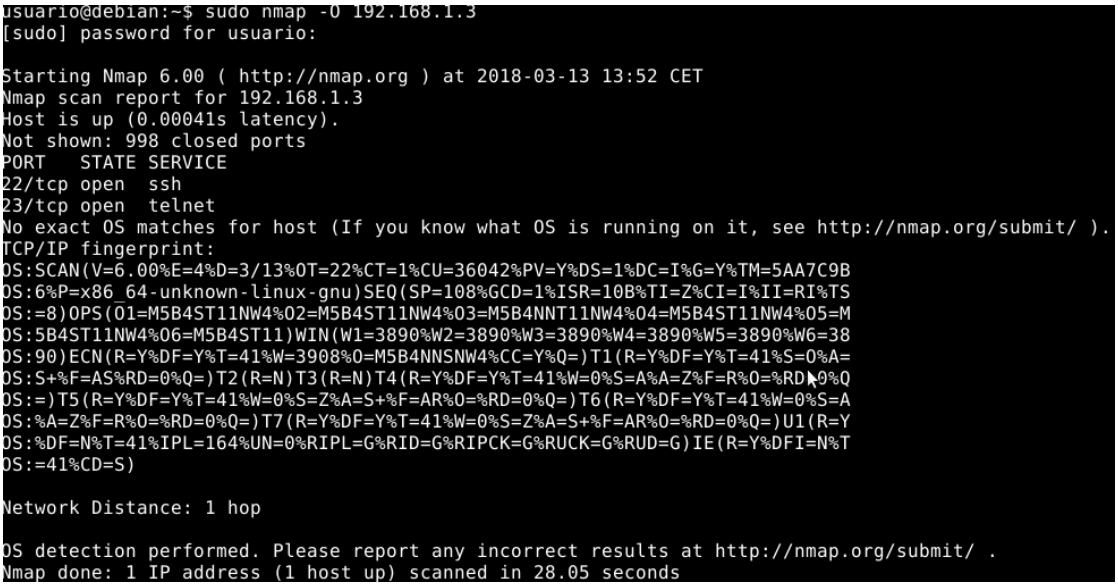

Figure 2.4.1 : Sondeo SO router.

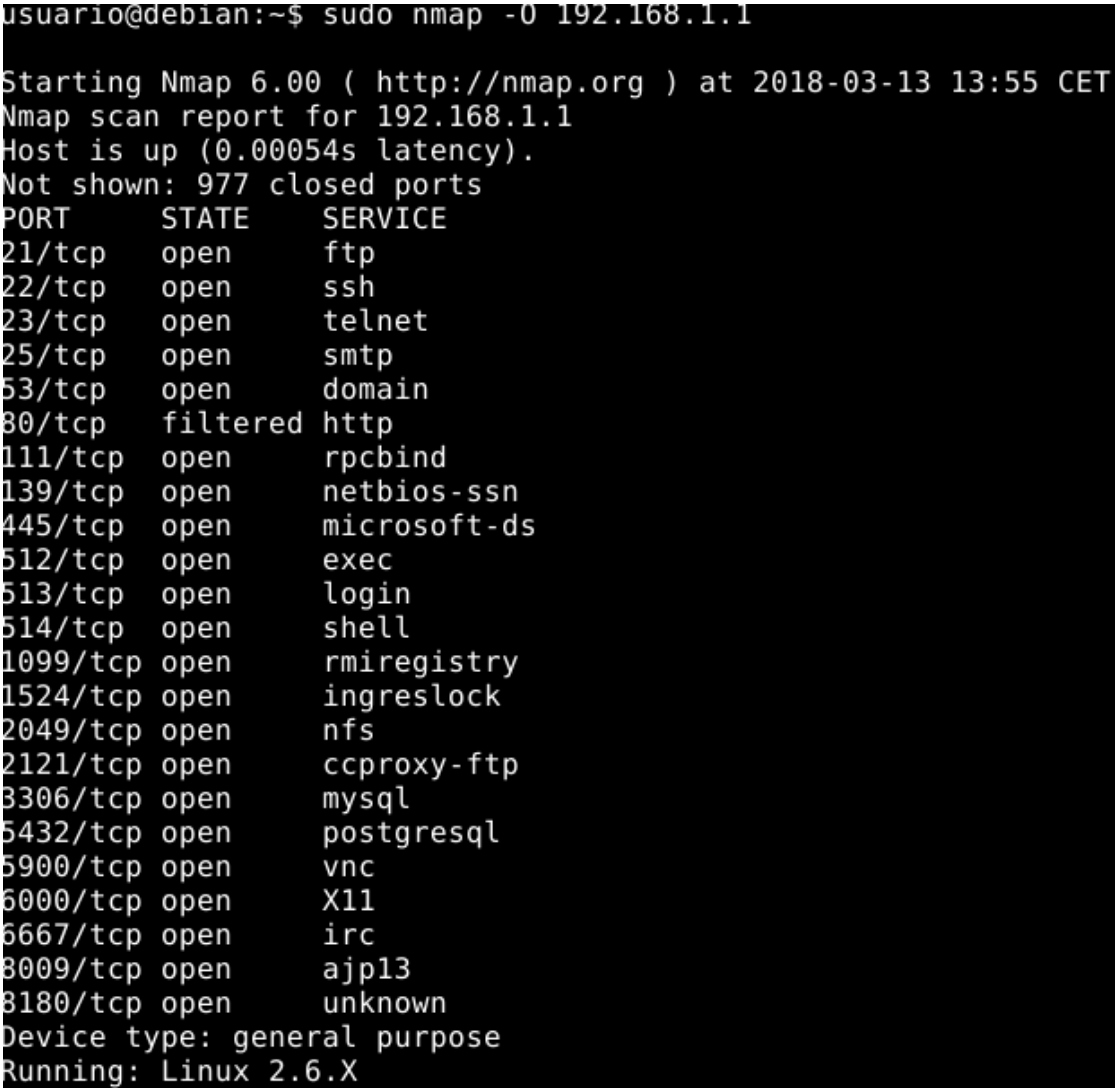

Figure 2.4.2 : Sondeo SO metasploitable.