

# Práctica 4

ANÁLISIS DE TRÁFICO Y ESCANEEO DE PUERTOS

JACOBO MARTINEZ GÓMEZ

## Ejercicio 1

Después del escaneo de eth0 el equipo observador captura los paquetes de la conexión telnet entre interno1 y interno2:

OBSERVADOR\_jmgomez2 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

\*enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
7	13.558047744	192.168.100.11	192.168.100.22	TelNET	93	Telnet Data ...
9	14.098423391	192.168.100.22	192.168.100.11	TelNET	87	Telnet Data ...
11	14.098504260	192.168.100.22	192.168.100.11	TelNET	88	Telnet Data ...
13	14.098842591	192.168.100.11	192.168.100.22	TelNET	141	Telnet Data ...
15	14.098977013	192.168.100.22	192.168.100.11	TelNET	90	Telnet Data ...
16	14.099178813	192.168.100.11	192.168.100.22	TelNET	155	Telnet Data ...
17	14.109380841	192.168.100.22	192.168.100.11	TelNET	69	Telnet Data ...
18	14.109508996	192.168.100.11	192.168.100.22	TelNET	69	Telnet Data ...
19	14.109771405	192.168.100.22	192.168.100.11	TelNET	88	Telnet Data ...
20	14.110021350	192.168.100.11	192.168.100.22	TelNET	82	Telnet Data ...
21	14.110153101	192.168.100.22	192.168.100.11	TelNET	133	Telnet Data ...
23	14.340510764	192.168.100.22	192.168.100.11	TelNET	91	Telnet Data ...
25	33.373263416	192.168.100.11	192.168.100.22	TelNET	74	Telnet Data ...
26	33.373821371	192.168.100.22	192.168.100.11	TelNET	75	Telnet Data ...
28	33.492075806	192.168.100.22	192.168.100.11	TelNET	79	Telnet Data ...
30	37.807505275	192.168.100.11	192.168.100.22	TelNET	74	Telnet Data ...
31	37.811489045	192.168.100.22	192.168.100.11	TelNET	68	Telnet Data ...
33	38.038773864	192.168.100.22	192.168.100.11	TelNET	156	Telnet Data ...
35	38.058898769	192.168.100.22	192.168.100.11	TelNET	359	Telnet Data ...
37	38.859427592	192.168.100.22	192.168.100.11	TelNET	110	Telnet Data ...
39	55.038290992	192.168.100.11	192.168.100.22	TelNET	72	Telnet Data ...
40	55.038478979	192.168.100.22	192.168.100.11	TelNET	71	Telnet Data ...
42	55.038779734	192.168.100.22	192.168.100.11	TelNET	68	Telnet Data ...
44	55.192118338	192.168.100.22	192.168.100.11	TelNET	73	Telnet Data ...
46	55.192354923	192.168.100.22	192.168.100.11	TelNET	68	Telnet Data ...
48	55.19284144	192.168.100.22	192.168.100.11	TelNET	110	Telnet Data ...

Si usamos la opción de follow->TCP Stream obtenemos la lista de comandos que se realizaron.

OBSERVADOR\_jmgomez2 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

\*enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

No.	Time	Source
4	13.557604676	192.168.100.11
5	13.557606295	192.168.100.22
6	13.557714891	192.168.100.11
7	13.558047744	192.168.100.11
8	13.558049544	192.168.100.22
9	14.098423391	192.168.100.22
10	14.098501452	192.168.100.11
11	14.098504260	192.168.100.22
12	14.098640201	192.168.100.11
13	14.098842591	192.168.100.11
14	14.098844800	192.168.100.22
15	14.098977013	192.168.100.22
16	14.099178813	192.168.100.11
17	14.109380841	192.168.100.22

```
.....*.....#..%..&.....#..%..$.....#..%..$.....P.....".....b.....b.....B.
.....#.....38400,38400....#..interno1.ssh.net:0.0.....#..DISPLAY:interno1.ssh.net:
0.0.....xterm.....
Linux 4.9.0-11-amd64 (interno2.ssh.net) (pts/0)

interno2.ssh.net nombre: usuario
usuario
Contrase~a: usuario

Linux interno2.ssh.net 4.9.0-11-amd64 #1 SMP Debian 4.9.189-3+deb9u1 (2019-09-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
.j0:usuario@interno2: ~.usuario@interno2:~$ ls -l
ls -l
total 0
.j0:usuario@interno2: ~.usuario@interno2:~$
```

## Tarea 1

Ahora vamos a hacer el mismo paso pero con una conexión SSH entre interno1 y interno2.

OBSERVADOR\_jmgomez2 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

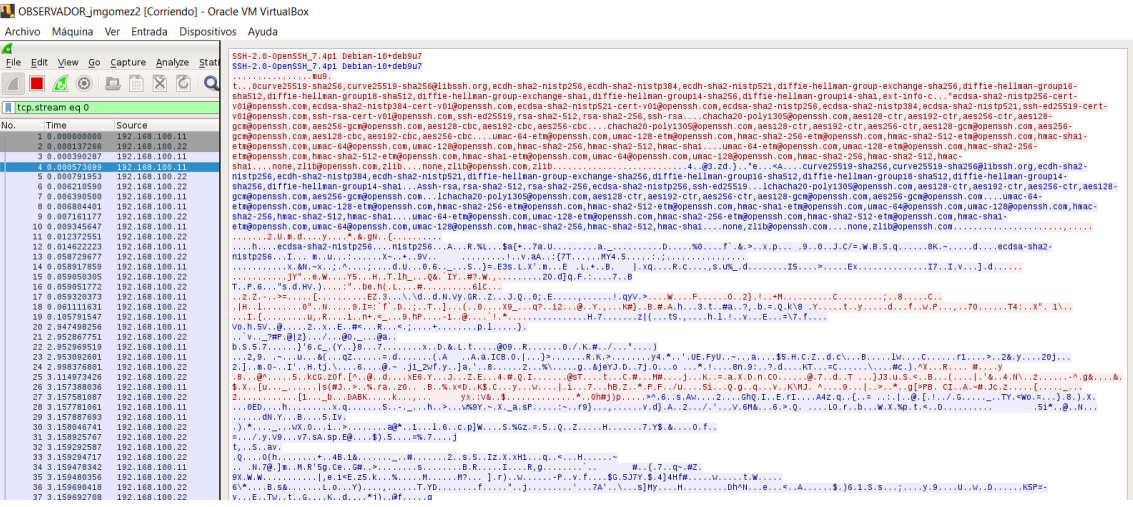
\*enp0s3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssh

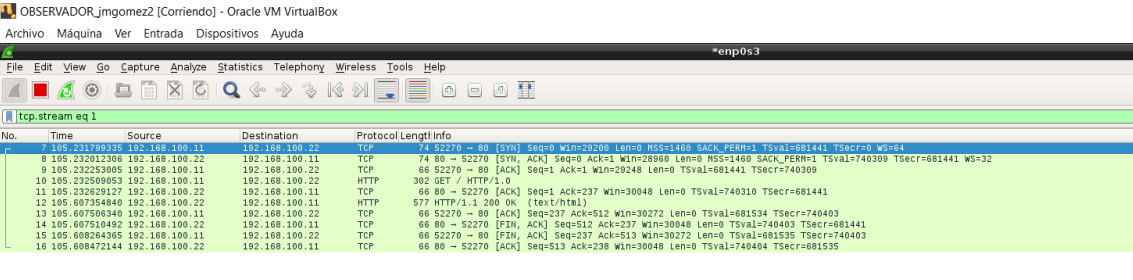
No.	Time	Source	Destination	Protocol	Length	Info
4	0.000573699	192.168.100.11	192.168.100.22	SSHv2	106	Client: Protocol (SSH-2.0-openssh_7.4p1 Debian-10+deb9u7)
6	0.006210590	192.168.100.22	192.168.100.11	SSHv2	105	Server: Protocol (SSH-2.0-openssh_7.4p1 Debian-10+deb9u7)
8	0.006804401	192.168.100.11	192.168.100.22	SSHv2	1498	Client: Key Exchange Init
9	0.007161177	192.168.100.22	192.168.100.11	SSHv2	1146	Server: Key Exchange Init
10	0.009345647	192.168.100.11	192.168.100.22	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
11	0.012372551	192.168.100.22	192.168.100.11	SSHv2	486	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=140)
12	0.014622223	192.168.100.11	192.168.100.22	SSHv2	82	Client: New Keys
14	0.058917859	192.168.100.11	192.168.100.22	SSHv2	110	Client: Encrypted packet (len=44)
16	0.059051772	192.168.100.22	192.168.100.11	SSHv2	110	Server: Encrypted packet (len=44)
17	0.059320373	192.168.100.11	192.168.100.22	SSHv2	134	Client: Encrypted packet (len=68)
18	0.061111831	192.168.100.22	192.168.100.11	SSHv2	118	Server: Encrypted packet (len=52)
20	2.947498256	192.168.100.11	192.168.100.22	SSHv2	214	Client: Encrypted packet (len=148)
21	2.952867751	192.168.100.22	192.168.100.11	SSHv2	94	Server: Encrypted packet (len=28)
23	2.953092601	192.168.100.11	192.168.100.22	SSHv2	178	Client: Encrypted packet (len=112)
25	3.114973426	192.168.100.22	192.168.100.11	SSHv2	566	Server: Encrypted packet (len=500)
27	3.157581087	192.168.100.22	192.168.100.11	SSHv2	110	Server: Encrypted packet (len=44)
29	3.157887883	192.168.100.11	192.168.100.22	SSHv2	518	Client: Encrypted packet (len=444)

Ahora se comprueba que no se pueden ver los datos intercambiados entre interno1 y interno 2 dado que el protocolo SSH cifra las comunicaciones.

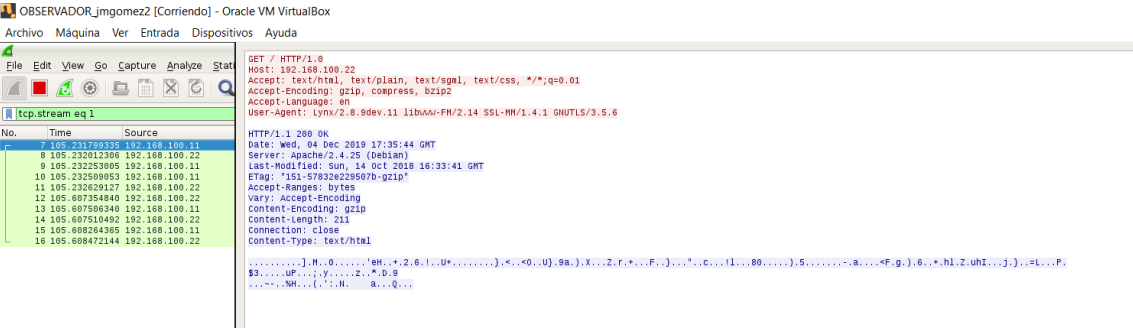


## Tarea 2

### Conexión web hacia el servidor apache de interno2



Como se comprueba parte del contenido no se ve correctamente porque viene comprimido en gzip tal y como informa en la cabecera del mensaje.



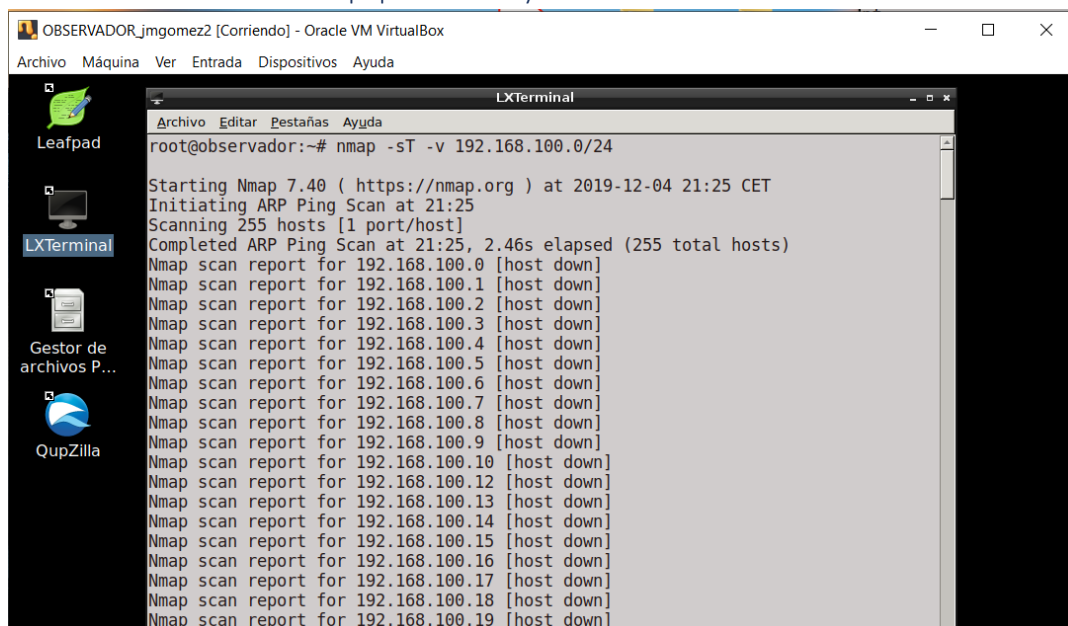
## Tarea 3

En este caso después de usar el protocolo SSL realiza varios intentos fallidos hasta que se acepta el certificado al realizar la conexión al sitio web.



## Ejercicio 2

Enumerar el número de equipos en red y sus servicios:



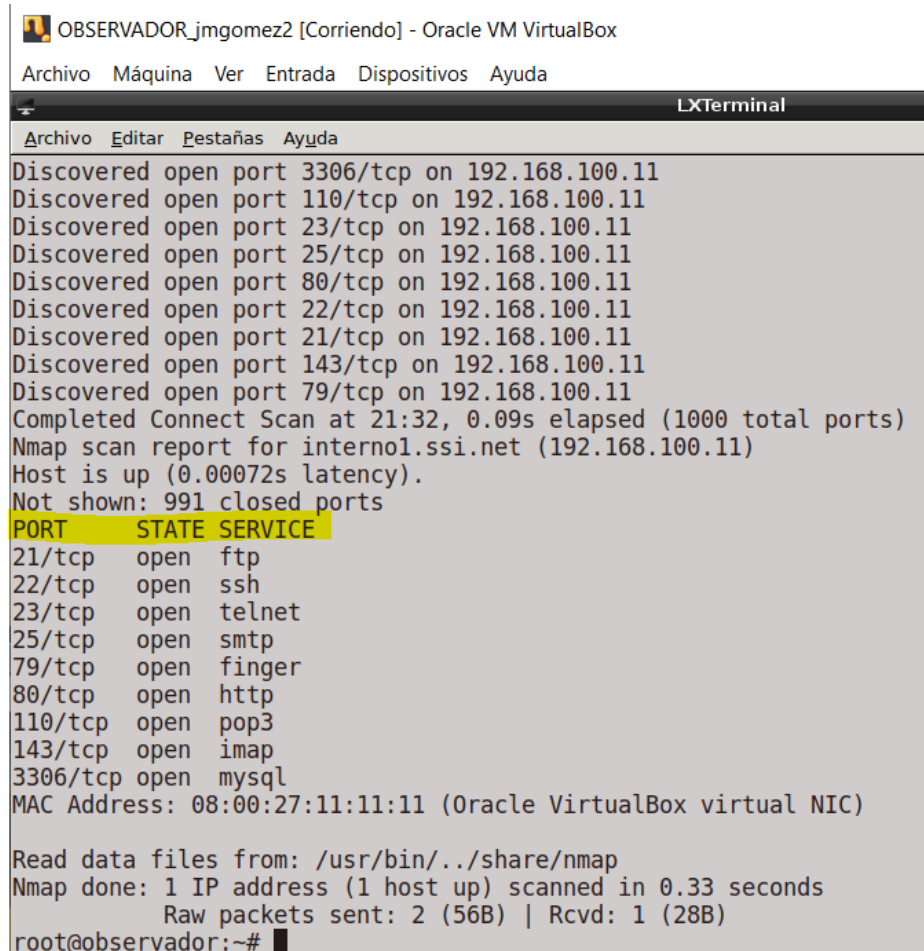
```
OBSERVADOR_jmgomez2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

LXTerminal
Archivo Editar Pestañas Ayuda
root@observador:~# nmap -sT -v 192.168.100.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2019-12-04 21:25 CET
Initiating ARP Ping Scan at 21:25
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 21:25, 2.46s elapsed (255 total hosts)
Nmap scan report for 192.168.100.0 [host down]
Nmap scan report for 192.168.100.1 [host down]
Nmap scan report for 192.168.100.2 [host down]
Nmap scan report for 192.168.100.3 [host down]
Nmap scan report for 192.168.100.4 [host down]
Nmap scan report for 192.168.100.5 [host down]
Nmap scan report for 192.168.100.6 [host down]
Nmap scan report for 192.168.100.7 [host down]
Nmap scan report for 192.168.100.8 [host down]
Nmap scan report for 192.168.100.9 [host down]
Nmap scan report for 192.168.100.10 [host down]
Nmap scan report for 192.168.100.11 [host down]
Nmap scan report for 192.168.100.12 [host down]
Nmap scan report for 192.168.100.13 [host down]
Nmap scan report for 192.168.100.14 [host down]
Nmap scan report for 192.168.100.15 [host down]
Nmap scan report for 192.168.100.16 [host down]
Nmap scan report for 192.168.100.17 [host down]
Nmap scan report for 192.168.100.18 [host down]
Nmap scan report for 192.168.100.19 [host down]
```

Comprobar los puertos abiertos de interno1 y interno2:

-Interno 1:



```
OBSERVADOR_jmgomez2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

LXTerminal
Archivo Editar Pestañas Ayuda
root@observador:~# nmap -sT -v 192.168.100.11

Starting Nmap 7.40 ( https://nmap.org ) at 2019-12-04 21:32 CET
Initiating ARP Ping Scan at 21:32
Scanning 1 hosts [1 port/host]
Completed ARP Ping Scan at 21:32, 0.09s elapsed (1 total hosts)
Nmap scan report for 192.168.100.11
Discovered open port 3306/tcp on 192.168.100.11
Discovered open port 110/tcp on 192.168.100.11
Discovered open port 23/tcp on 192.168.100.11
Discovered open port 25/tcp on 192.168.100.11
Discovered open port 80/tcp on 192.168.100.11
Discovered open port 22/tcp on 192.168.100.11
Discovered open port 21/tcp on 192.168.100.11
Discovered open port 143/tcp on 192.168.100.11
Discovered open port 79/tcp on 192.168.100.11
Completed Connect Scan at 21:32, 0.09s elapsed (1000 total ports)
Nmap scan report for interno1.ssi.net (192.168.100.11)
Host is up (0.00072s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
3306/tcp  open  mysql
MAC Address: 08:00:27:11:11:11 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
Raw packets sent: 2 (56B) | Rcvd: 1 (28B)
root@observador:~#
```

-Interno 2:

```
OBSERVADOR_jimgomez2 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

LXTerminal
Archivo Editar Pestañas Ayuda
Discovered open port 23/tcp on 192.168.100.22
Discovered open port 22/tcp on 192.168.100.22
Discovered open port 25/tcp on 192.168.100.22
Discovered open port 3306/tcp on 192.168.100.22
Discovered open port 443/tcp on 192.168.100.22
Discovered open port 143/tcp on 192.168.100.22
Discovered open port 80/tcp on 192.168.100.22
Discovered open port 79/tcp on 192.168.100.22
Completed Connect Scan at 21:34, 0.09s elapsed (1000 total ports)
Nmap scan report for interno2.ssi.net (192.168.100.22)
Host is up (0.00068s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
3306/tcp  open  mysql
MAC Address: 08:00:27:22:22:22 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
Raw packets sent: 2 (56B) | Rcvd: 1 (28B)
root@observador:~#
```

## Comprobar servicios y sistema operativo en interno 1:

```
OBSERVER@jmgomez2[Corriendo] - Oracle VM VirtualBox
```

Archivo Máquina Ver Entrada Dispositivos Ayuda

LXTerminal

Archivo Editar Pestañas Ayuda

```
root@observador:~# nmap -sT -O -sV 192.168.100.11
```

Starting Nmap 7.40 (<https://nmap.org>) at 2019-12-04 21:36 CET  
Nmap scan report for [internal.ssi.net \(192.168.100.11\)](#)  
Host is up (0.00048s latency).  
Not shown: 991 closed ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp	open	ssh	OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
23/tcp	open	telnet	
25/tcp	open	smtp	Postfix smtpd
79/tcp	open	finger	Debian fingerd
80/tcp	open	http	Apache httpd 2.4.25 ((Debian))
110/tcp	open	pop3	Dovecot pop3d
143/tcp	open	imap	Dovecot imapd
3306/tcp	open	mysql	MariaDB (unauthorized)

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service>:  
SF:Port23-TCP:V=7.40%I=7%D=12/4%Time=5DE818E7P=x86\_64-pc-linux-gnu%(NULL  
SF:,15,"\\xfbf\\xfb%\\xff\\xfd\\x18\\xff\\xfd\\x20\\xff\\xfd%\\xff\\xfd'\\xff\\x  
SF:f\\fd\$")%(GenericLines,15,"\\xff\\xfb%\\xff\\xfb%\\xff\\xfd\\x18\\xff\\xfd\\x20\\xf  
SF:f\\xfd%\\xff\\xfd'\\xff\\xfd\$")%(tn3270,15,"\\xff\\xfb%\\xff\\xfb%\\xff\\xfd\\x18  
SF:\\xff\\xfd\\x20\\xff\\xfd%\\xff\\xfd'\\xff\\xfd\$")%(GetRequest,15,"\\xff\\xfb%\\x  
SF:f\\xfb%\\xff\\xfd\\x18\\xff\\xfd\\x20\\xff\\xfd%\\xff\\xfd'\\xff\\xfd\$")%(RPCChec  
SF:k,15,"\\xff\\xfb%\\xff\\xfb%\\xff\\xfd\\x18\\xff\\xfd\\x20\\xff\\xfd%\\xff\\xfd'\\xff\\  
SF:x\\fd\$")%(Help,15,"\\xff\\xfb%\\xff\\xfb%\\xff\\xfd\\x18\\xff\\xfd\\x20\\xff\\xfd%\\  
SF:x\\ffd'\\xff\\xfd\$")%(SIPOptions,15,"\\xff\\xfb%\\xff\\xfb%\\xff\\xfd\\x18\\xf  
SF:f\\xfd\\x20\\xff\\xfd%\\xff\\xfd'\\xff\\xfd\$")%(NCP,15,"\\xff\\xfb%\\xff\\xfb%\\xf  
SF:f\\xfd\\x18\\xff\\xfd\\x20\\xff\\xfd%\\xff\\xfd'\\xff\\xfd\$");  
MAC Address: 08:00:27:11:11:11 (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
**Running: Linux 3.X|4.X**  
OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4  
**OS details: Linux 3.2 - 4.6**  
Network Distance: 1 hop  
Service Info: Host: base.home; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.  
Nmap done: 1 IP address (1 host up) scanned in 49.14 seconds  
root@observador:~# █

\*enp0s3 LXTerminal 21:39

Syslog de interno1:

```
Dec  4 21:32:02 internal postfix/smtpd[2033]: connect from Observador.ssi.net[192.168.100.33]
Dec  4 21:32:02 internal postfix/smtpd[2033]: lost connection after CONNECT from observador.ssi.net[192.168.100.33]
Dec  4 21:32:02 internal postfix/smtpd[2033]: disconnect from observador.ssi.net[192.168.100.33] commands=0/0
Dec  4 21:32:02 internal ftpd[2051]: getpeername (in.ftpd): Transport endpoint is not connected
Dec  4 21:35:22 internal postfix/anvil[2039]: statistics: max connection rate 1/60s for (smtp:unknown) at Dec  4 21:31:13
Dec  4 21:35:22 internal postfix/anvil[2039]: statistics: max connection count 1 for (smtp:unknown) at Dec  4 21:31:13
Dec  4 21:35:22 internal postfix/anvil[2039]: statistics: max cache size 2 at Dec  4 21:32:02
Dec  4 21:36:48 internal inetd[312]: could not getpeername
Dec  4 21:36:48 internal in.ftpd[2053]: warning: can't get client address: Connection reset by peer
Dec  4 21:36:48 internal in.ftpd[2053]: connect from unknown (unknown)
Dec  4 21:36:48 internal ftpd[2053]: getpeername (in.ftpd): Transport endpoint is not connected
Dec  4 21:36:48 internal dovecot: imap-login: Disconnected (disconnected before auth was ready, waited 0 secs): user=<>,
rip=192.168.100.33, lip=192.168.100.11, session=<Bi
2fxeaYzsDAqGQh>
Dec  4 21:36:49 internal postfix/smtpd[2057]: connect from unknown[unknown]
```

```
Dec  4 21:36:49 internal in.fingerd[2061]: warning: can't get client address: Connection reset by peer
Dec  4 21:36:49 internal in.fingerd[2061]: connect from unknown (unknown)
Dec  4 21:36:49 internal postfix/smtpd[2057]: last connection after CONNECT from unknown[unknown]
Dec  4 21:36:49 internal postfix/smtpd[2057]: disconnect from unknown[unknown] commands=0/0
Dec  4 21:36:49 internal dovecot: pop3-login: Disconnected (no auth attempts in 1 secs): user=<>, rip=192.168.100.33,
lip=192.168.100.11, session=<83SfxeaYVpDAqGQh>
Dec  4 21:36:49 internal postfix/smtpd[2057]: connect from observador.ssi.net[192.168.100.33]
Dec  4 21:36:49 internal postfix/smtpd[2057]: last connection after CONNECT from observador.ssi.net[192.168.100.33]
Dec  4 21:36:49 internal postfix/smtpd[2057]: disconnect from observador.ssi.net[192.168.100.33] commands=0/0
Dec  4 21:36:49 internal telnetd[2064]: connect from 192.168.100.33 (192.168.100.33)
Dec  4 21:36:49 internal in.ftpd[2063]: connect from 192.168.100.33 (192.168.100.33)
```

En este log de interno1 se aprecian las conexiones de la maquina observador que le proporcionan información a nmap.

#### Escaneos Silenciosos:

Escribimos la regla de netfilter para loguear los paquetes SYN con intentos de conexión TCP:

```
iptables -A INPUT -i enp0s3 -p tcp --tcp-flags SYN SYN -m state --state NEW -j LOG --log-prefix
"Inicio conex:"
```



## TCP connect scanning

OBSERVADOR\_jimgomez2 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
LXTerminal
Archivo Editar Pestañas Ayuda
root@observador:~# npam -sT 192.168.100.11
bash: npam: no se encontró la orden
root@observador:~# nmap -sT 192.168.100.11

Starting Nmap 7.40 ( https://nmap.org ) at 2019-12-04 21:56 CET
Nmap scan report for interno1.ssi.net (192.168.100.11)
Host is up (0.00067s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
3306/tcp  open  mysql
MAC Address: 08:00:27:11:11:11 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
root@observador:~#
```

En estos 33 segundos se genera bastante información en el log.

## SYN scanning

OBSERVADOR\_jimgomez2 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda


```
LXTerminal
Archivo Editar Pestañas Ayuda
root@observador:~# nmap -sS 192.168.100.11

Starting Nmap 7.40 ( https://nmap.org ) at 2019-12-04 21:58 CET
Nmap scan report for interno1.ssi.net (192.168.100.11)
Host is up (0.00019s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
3306/tcp  open  mysql
MAC Address: 08:00:27:11:11:11 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.10 seconds
root@observador:~#
```

Este es el escaneo que mas entradas en el log genera.

## NULL scanning

 OBSERVADOR\_jmgomez2 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
LXTerminal
Archivo Editar Pestañas Ayuda
root@observador:~# nmap -sN 192.168.100.11

Starting Nmap 7.40 ( https://nmap.org ) at 2019-12-04 21:59 CET
Nmap scan report for interno1.ssi.net (192.168.100.11)
Host is up (0.00042s latency).
Not shown: 991 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
79/tcp    open|filtered finger
80/tcp    open|filtered http
110/tcp   open|filtered pop3
143/tcp   open|filtered imap
3306/tcp  open|filtered mysql
MAC Address: 08:00:27:11:11:11 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 98.77 seconds
root@observador:~#
```

Por otro lado este es el escaneo que mas tarda pero el que no genera apenas información en el log.

### Conclusiones Ejercicio 2

Para concluir en estas pruebas que hemos hecho de NMAP se puede apreciar como a pesar de conseguir la misma información cada prueba lleva su tiempo y genera sus entradas en el log.

La opción de nmap mas rápida es -sT pero deja algún rastro en el equipo escaneado, sin embargo la opción -sN es mas lenta pero no deja ningún rastro en el equipo.

La última opción -sS es la opción que mas rastro genera en el log.