Práctica 4

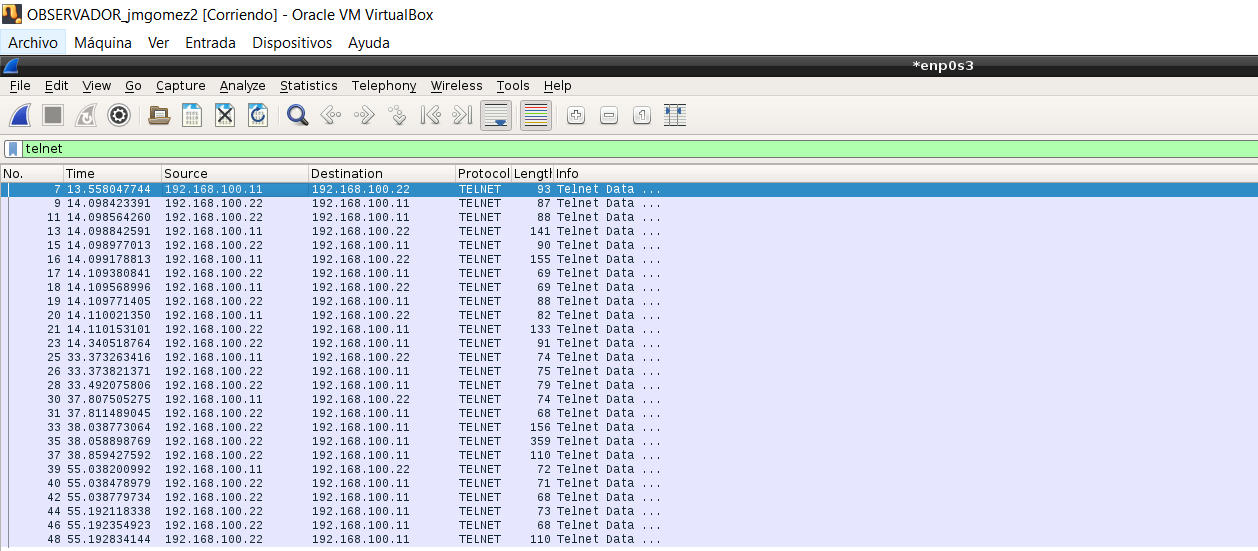
Análisis de tráfico y escaneo de puertos

Jacobo Martinez Gómez

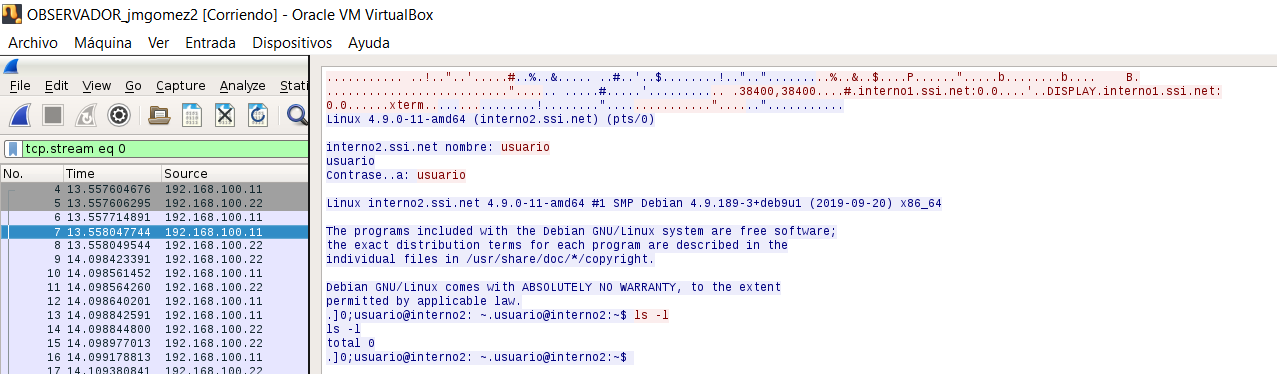
19/20

## Ejercicio 1

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

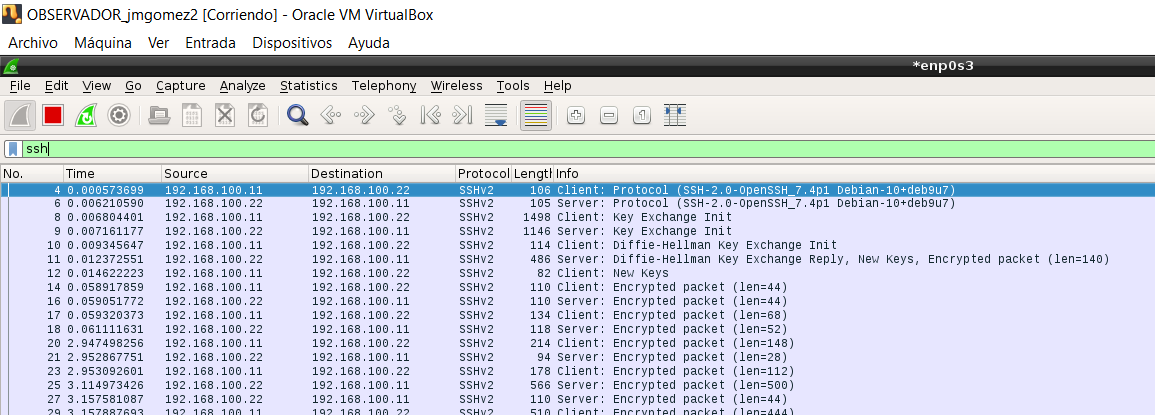


Si usamos la opción de follow->TCP Stream obtenemos la lista de comandos que se realizaron.

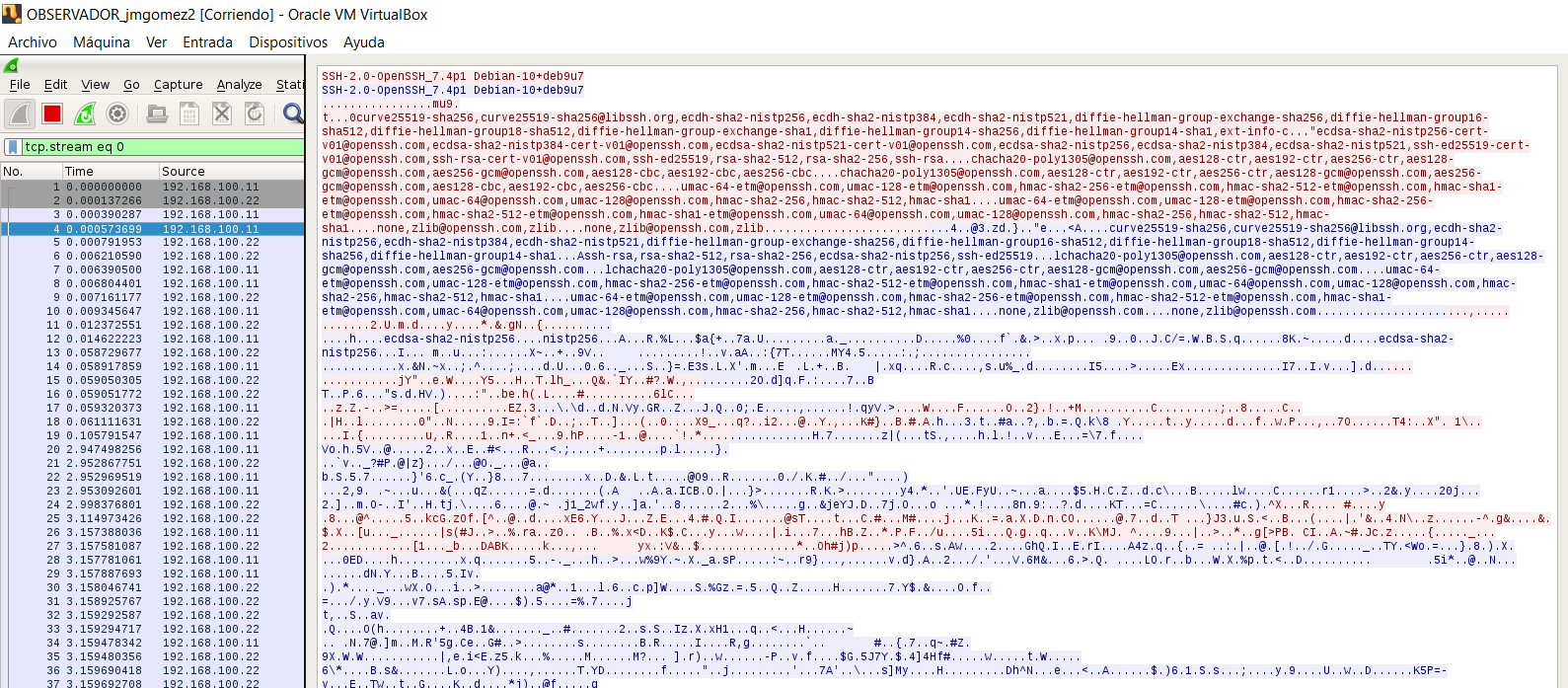


## Tarea 1

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

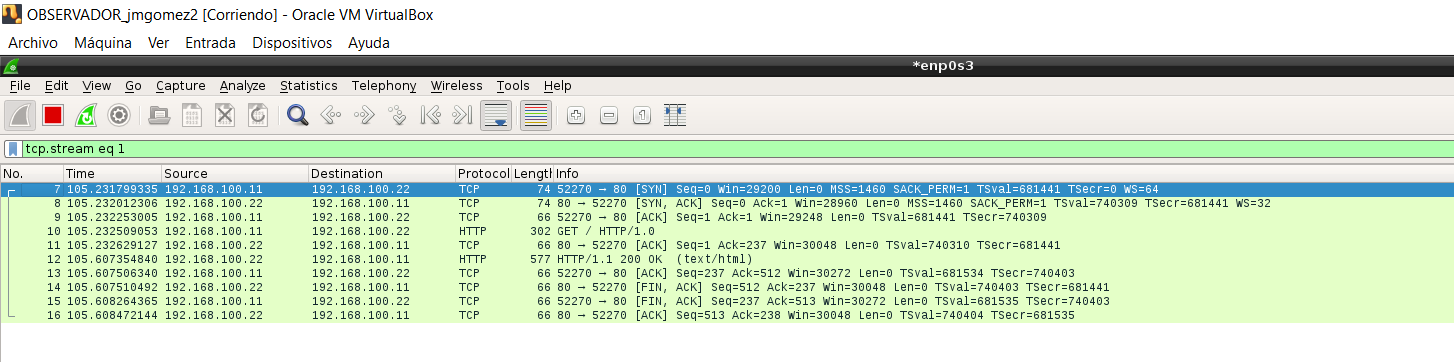


Ahora se comprueba que no se pueden ver los datos intercambiados entre interno1 y interno 2 dado que el protocolo SSH cifra las comunicaciones.



## Tarea 2

Conexión web hacia el servidor apache de interno2

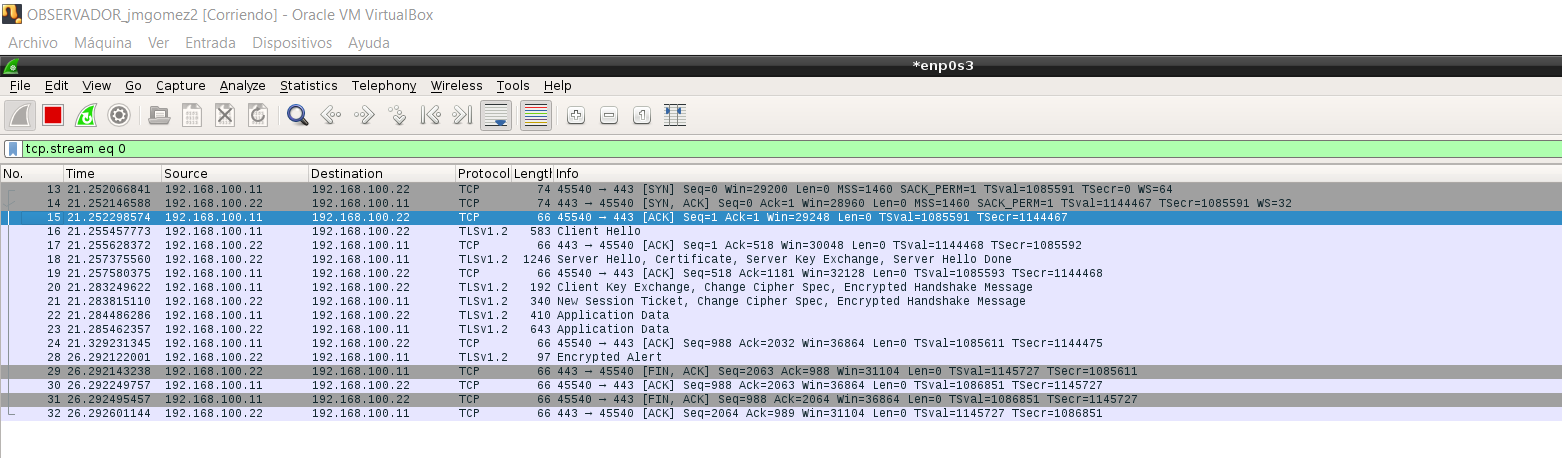


Como se comprueba parte del contenido no se ve correctamente porque viene comprimido en gzip tal y como informa en la cabecera del mensaje.



## 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.



Una vez observamos los paquetes comprobamos que todo viene cifrado:



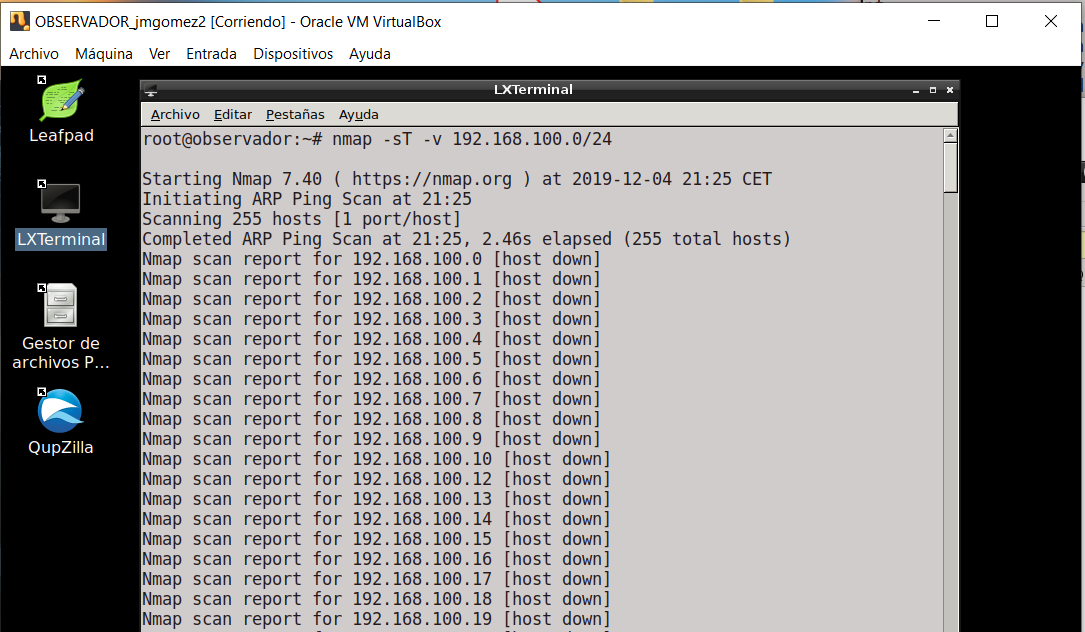
## Conclusiones Ejercicio 1

En este ejercicio podemos ver la importancia de cifrar todas las comunicaciones para así evitar que otras personas se hagan con la información que transmitimos.

El uso de los protocolos SSH y SSL nos aportan la seguridad y confidencialidad que se necesita en el intercambio de información que no sea pública.

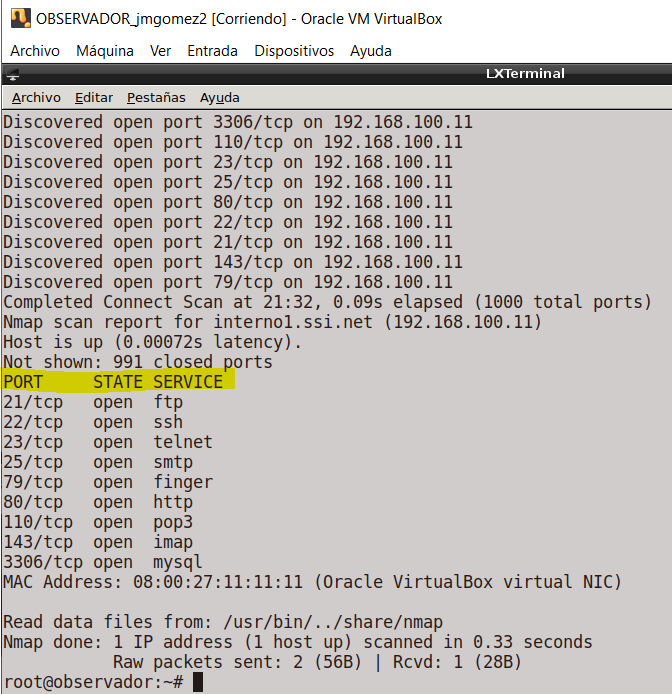
## Ejercicio 2

### Enumerar el número de equipos en red y sus servicios:

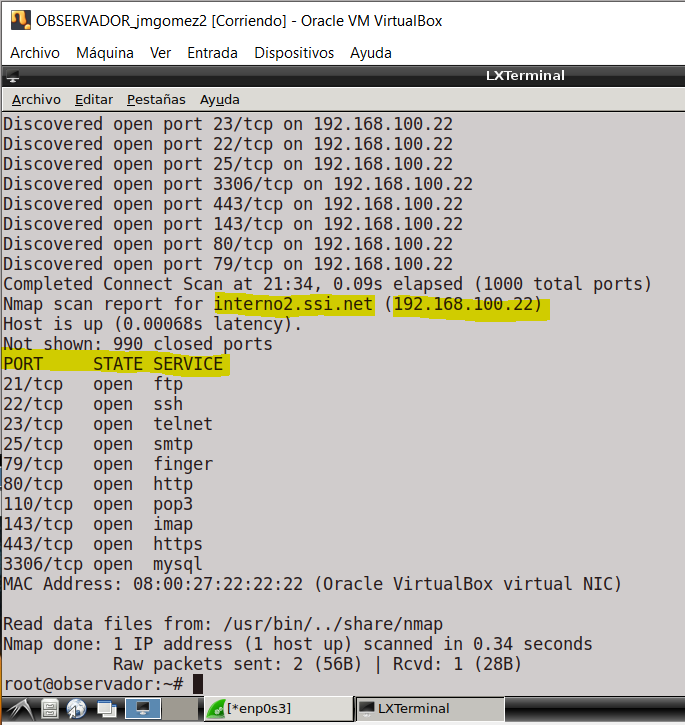


### Comprobar los puertos abiertos de interno1 y interno2:

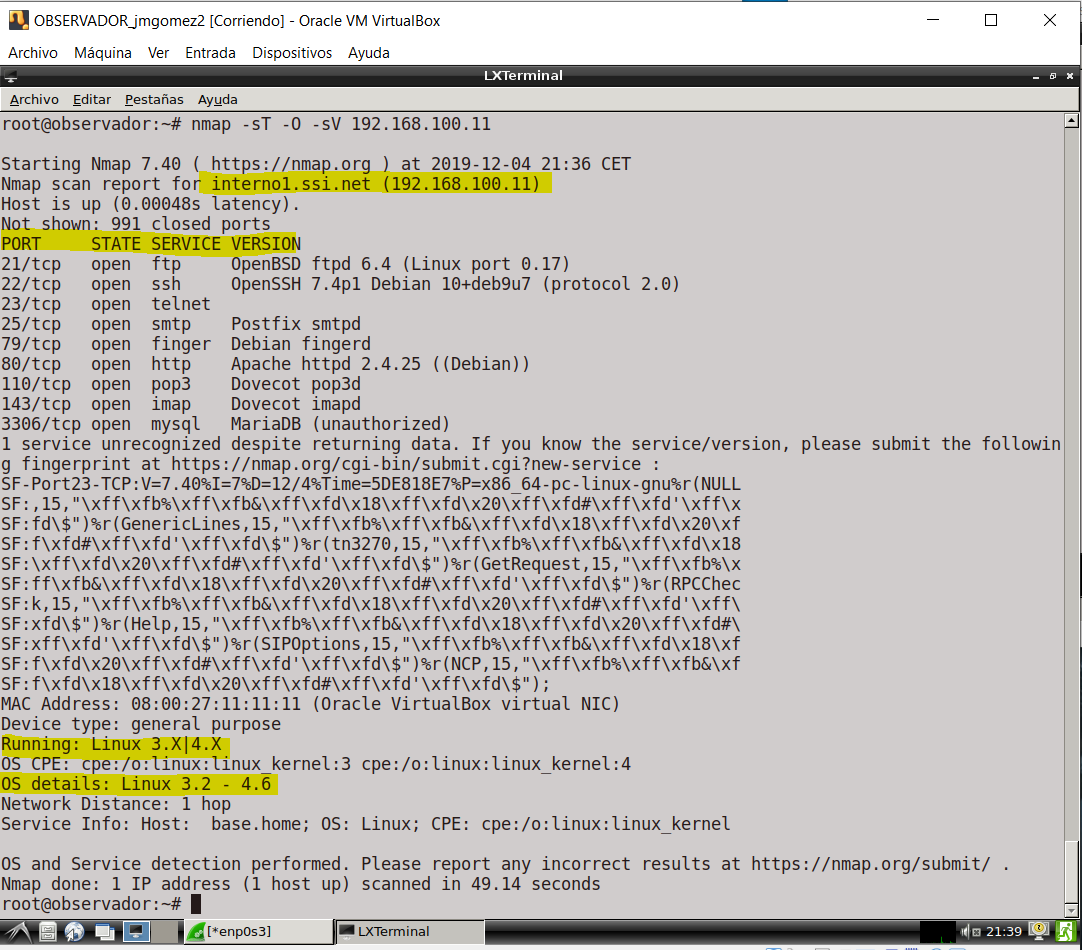
#### -Interno 1:



#### -Interno 2:



### Comprobar servicios y sistema operativo en interno 1:



### Syslog de interno1:

Dec 4 21:32:02 interno1 postfix/smtpd[2033]: connect from Observador.ssi.net[192.168.100.33]

Dec 4 21:32:02 interno1 postfix/smtpd[2033]: lost connection after CONNECT from observador.ssi.net[192.168.100.33]

Dec 4 21:32:02 interno1 postfix/smtpd[2033]: disconnect from observador.ssi.net[192.168.100.33] commands=0/0

Dec 4 21:32:02 interno1 ftpd[2051]: getpeername (in.ftpd): Transport endpoint is not connected

Dec 4 21:35:22 interno1 postfix/anvil[2039]: statistics: max connection rate 1/60s for (smtp:unknown) at Dec 4 21:31:13

Dec 4 21:35:22 interno1 postfix/anvil[2039]: statistics: max connection count 1 for (smtp:unknown) at Dec 4 21:31:13

Dec 4 21:35:22 interno1 postfix/anvil[2039]: statistics: max cache size 2 at Dec 4 21:32:02

Dec 4 21:36:48 interno1 inetd[312]: could not getpeername

Dec 4 21:36:48 interno1 in.ftpd[2053]: warning: can't get client address: Connection reset by peer

Dec 4 21:36:48 interno1 in.ftpd[2053]: connect from unknown (unknown)

Dec 4 21:36:48 interno1 ftpd[2053]: getpeername (in.ftpd): Transport endpoint is not connected

Dec 4 21:36:48 interno1 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 interno1 postfix/smtpd[2057]: connect from unknown[unknown]

Dec 4 21:36:49 interno1 in.fingerd[2061]: warning: can't get client address: Connection reset by peer

Dec 4 21:36:49 interno1 in.fingerd[2061]: connect from unknown (unknown)

Dec 4 21:36:49 interno1 postfix/smtpd[2057]: lost connection after CONNECT from unknown[unknown]

Dec 4 21:36:49 interno1 postfix/smtpd[2057]: disconnect from unknown[unknown] commands=0/0

Dec 4 21:36:49 interno1 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 interno1 postfix/smtpd[2057]: connect from observador.ssi.net[192.168.100.33]

Dec 4 21:36:49 interno1 postfix/smtpd[2057]: lost connection after CONNECT from observador.ssi.net[192.168.100.33]

Dec 4 21:36:49 interno1 postfix/smtpd[2057]: disconnect from observador.ssi.net[192.168.100.33] commands=0/0

Dec 4 21:36:49 interno1 telnetd[2064]: connect from 192.168.100.33 (192.168.100.33)

Dec 4 21:36:49 interno1 in.ftpd[2063]: connect from 192.168.100.33 (192.168.100.33)

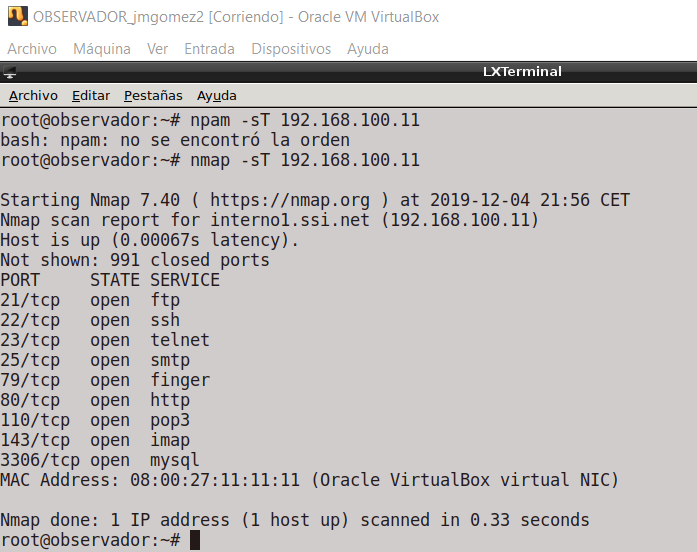
En este log de interno1 se aprecian las conexiones de la maquina observador que le proporcionan información a nmap.

### Escaneos Silenciosos:

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

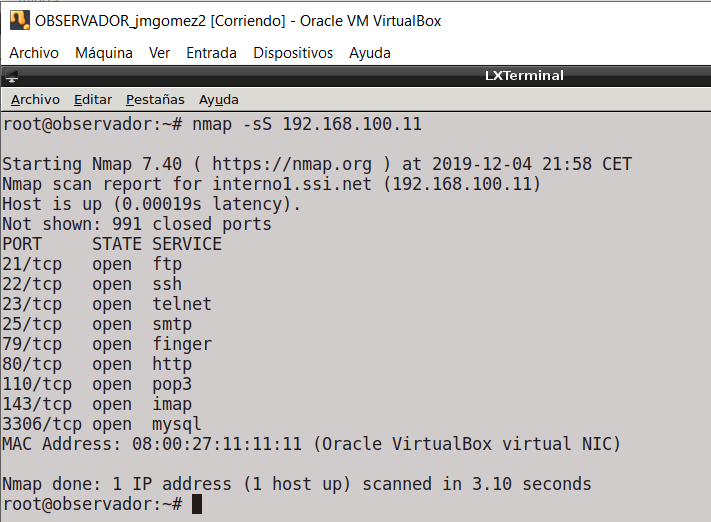
iptables -A INPUT -i enp0s3 -p tcp --tcp-flags SYN SYN -m state --state NEW -j LOG --log-prefix "Inicio conex:"

**TCP connect scanning**



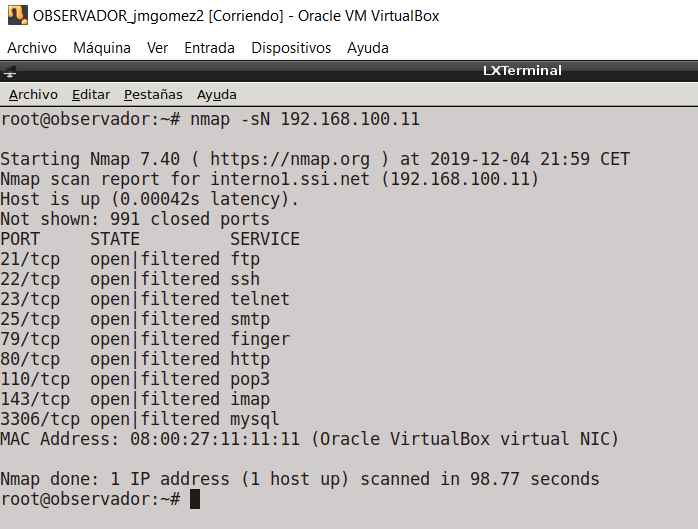
En estos 33 segundos se genera bastante información en el log.

**SYN scanning**



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

**NULL scanning**



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.