

Ejercicios de Seguridad en Redes Escucha y análisis de tráfico + Escaneo de puertos

Luis Miguel Raña Cortizo

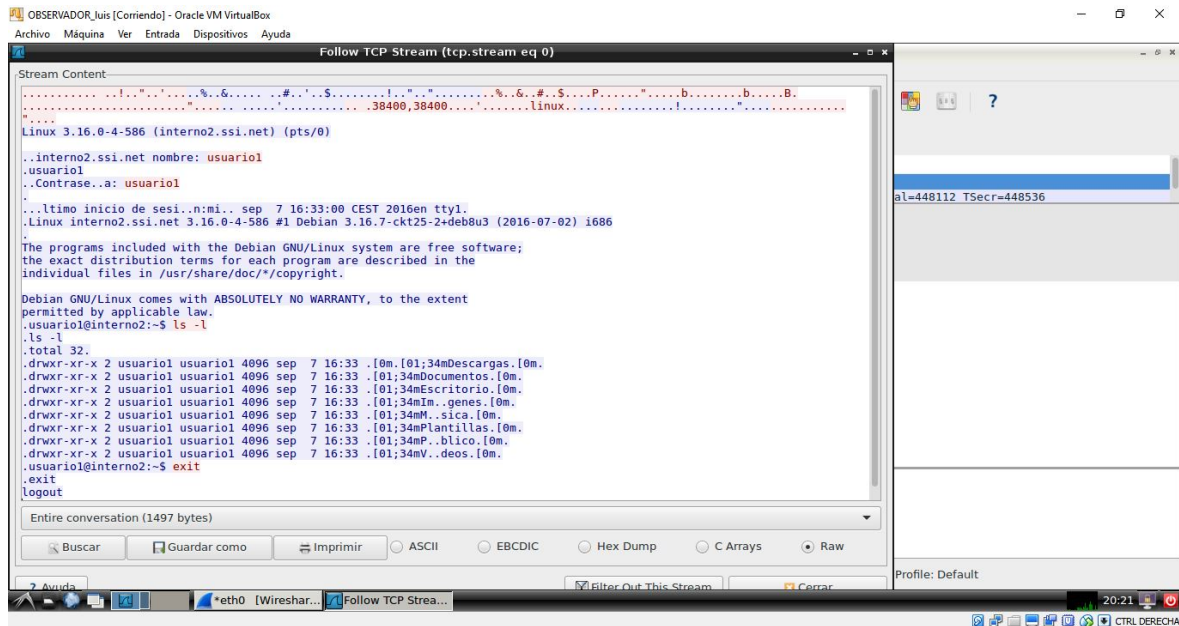
Ejercicio 1

Se trata de usar la herramienta Wireshark desde el equipo *observador* para interceptar el tráfico TELNET, HTTP y SSH entre los equipos *interno1* e *interno2*.

Iniciamos Wireshark en el *observador* (192.168.100.33) escuchando en la interfaz *eth0*.

Luego iniciamos una conexión TELNET en *interno1* (192.168.100.11): con *interno2* (192.168.100.22), y una vez dentro realizamos un `ls -l` y salimos.

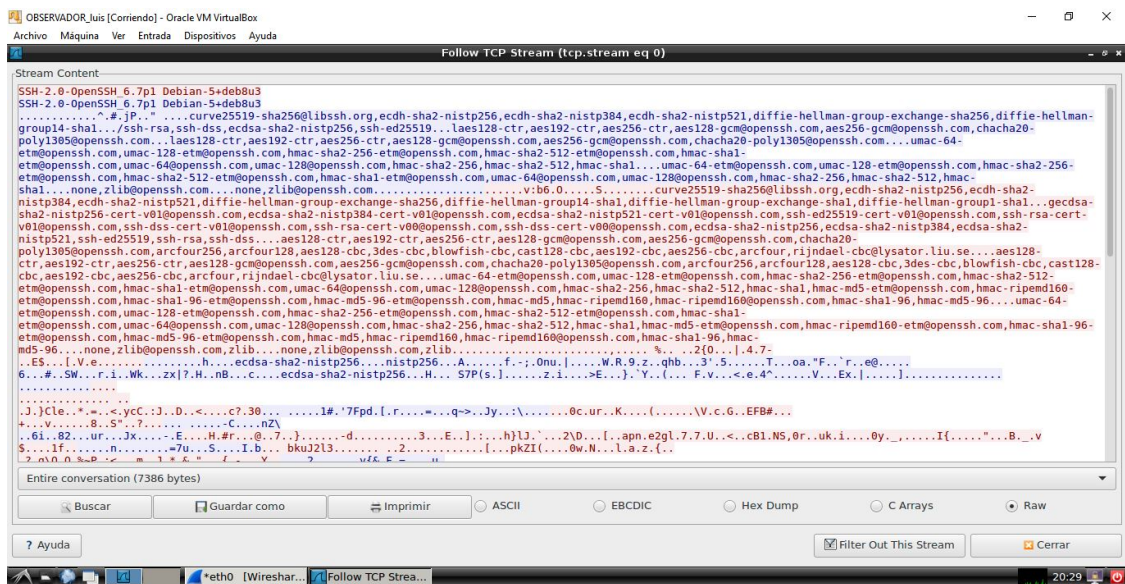
En *observador* (192.168.100.33) detenemos la escucha y filtramos el tráfico TELNET capturado:



Vemos que se han capturado las acciones que realizamos desde *interno1*.

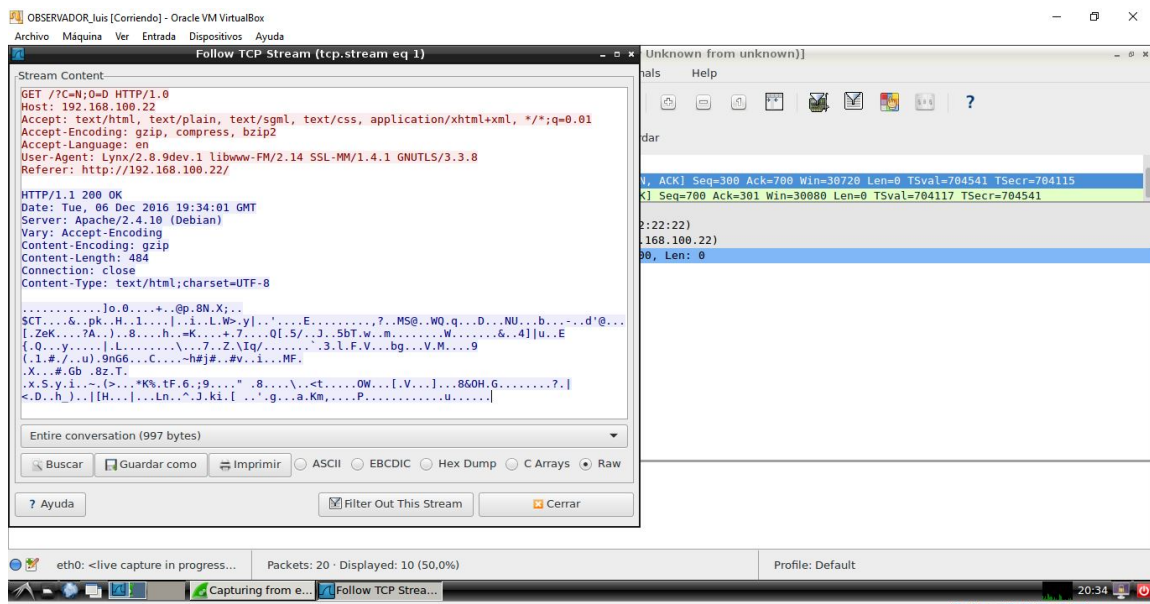
Tarea 1

Repetimos el proceso pero esta vez con una conexión SSH desde *interno1* (192.168.100.11) a *interno2* (192.168.100.22) y estos son los resultados de la captura:



Tarea 2

Mismo proceso usando una conexión WEB desde *interno1* (192.168.100.11) a *interno2* (192.168.100.22). Resultados:



Tarea 3

Habilitamos el soporte SSL en el servidor Apache2 de *interno2* (192.168.100.22) para comprobar que sucede cuando se "escucha" una conexión SSL/TLS.

Creamos un certificado autofirmado para el servidor web, luego editamos la configuración SSL por defecto para indicar el certificado del servidor y su respectiva clave privada, y por último habilitamos el soporte SSL en Apache2 y la configuración SSL por defecto.

Una vez configurado, procedemos a hacer la escucha en observador de la conexión SSL/TLS de *interno1* (192.168.100.11) a *interno2* (192.168.100.22), y vemos que la diferencia esta vez es que se trata de una conexión que va cifrada.

Ejercicio 2

Se usará la herramienta de escaneo de puertos NMAP para obtener información de los equipos y servicios de la red.

Primero se lanza desde *observador* un *Ping Sweeping* para identificar las máquinas que componen la red. Sobre cada uno de los equipos que aparezcan como activos realizar un escaneo de tipo *TCP connect scanning* para determinar que puertos están abiertos. Identificamos el Sistema Operativo y la versión concreta de los servicios que tiene activados *interno1*.

Comprobamos el ratro que han dejado los escaneos:

```
INTERNO1_luis [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@interno1:~# tail /var/log/syslog
Dec 6 20:44:00 interno1 telnetd[2228]: connect from 192.168.100.33 (192.168.100.33)
Dec 6 20:44:02 interno1 fingerd[2227]: Finger program not found
Dec 6 20:44:02 interno1 in.fingerd[2229]: connect from 192.168.100.33 (192.168.100.33)
Dec 6 20:44:05 interno1 telnetd[2228]: ttloop: peer died: Success
Dec 6 20:44:05 interno1 telnetd[2231]: connect from 192.168.100.33 (192.168.100.33)
Dec 6 20:44:07 interno1 fingerd[2229]: Finger program not found
Dec 6 20:44:07 interno1 in.fingerd[2233]: connect from 192.168.100.33 (192.168.100.33)
Dec 6 20:44:10 interno1 telnetd[2231]: ttloop: peer died: Success
Dec 6 20:44:10 interno1 telnetd[2234]: connect from 192.168.100.33 (192.168.100.33)
Dec 6 20:44:12 interno1 fingerd[2233]: Finger program not found
root@interno1:~# _
```

Evaluaremos el comportamiento de los distintos tipos de escaneo sobre la máquina ***interno1(192.168.100.11)***.

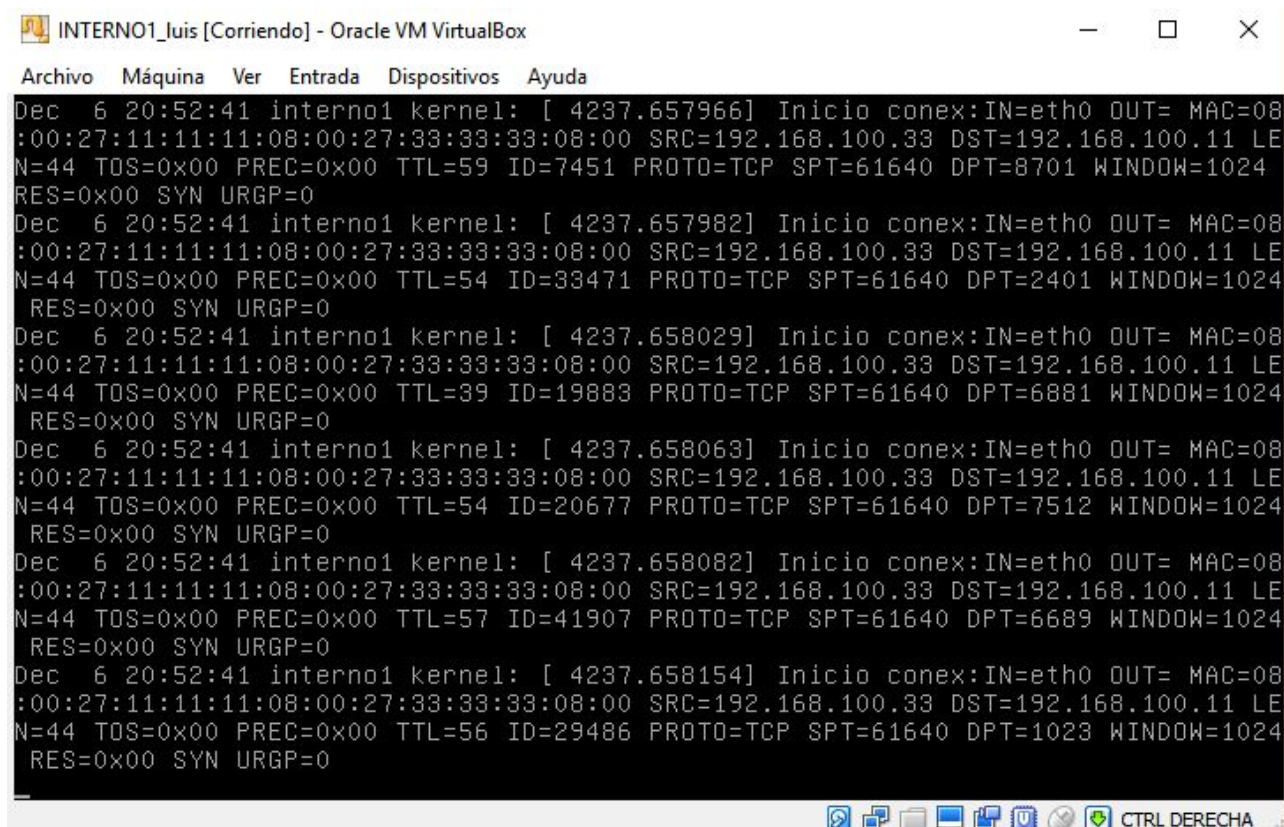
En interno1 se habilitará una regla del firewall *netfilter* para hacer log de los paquetes SYN con intentos de conexión TCP. Monorotizamos el fichero /var/log/syslog.

Desde ***observador*** lanzamos tres tripos de escaneo y miramos como evoluciona el log:

TCP connect scanning

```
INTERNO1_luis [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
9200 RES=0x00 SYN URG=0
Dec 6 20:55:45 interno1 kernel: [ 4422.517758] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11:11:11:08:00:27:33:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=12216 DF PROTO=TCP SPT=36900 DPT=65129 WINDOW=29200 RES=0x00 SYN URG=0
Dec 6 20:55:45 interno1 kernel: [ 4422.517896] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11:11:11:08:00:27:33:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=64512 DF PROTO=TCP SPT=50104 DPT=2869 WINDOW=29200 RES=0x00 SYN URG=0
Dec 6 20:55:46 interno1 inetd[522]: could not getpeername
Dec 6 20:55:46 interno1 inetd[522]: could not getpeername
Dec 6 20:55:46 interno1 dovecot: imap-login: Disconnected (no auth attempts in 0 secs): user=<>, rip=192.168.100.33, lip=192.168.100.11, session=<Gz9DygJdpQDAcGQh>
Dec 6 20:55:46 interno1 in.fingerd[2315]: warning: can't get client address: Connection reset by peer
Dec 6 20:55:46 interno1 in.fingerd[2315]: connect from unknown[unknown]
Dec 6 20:55:46 interno1 dovecot: pop3-login: Disconnected (no auth attempts in 0 secs): user=<>, rip=192.168.100.33, lip=192.168.100.11, session=<52BDygJDrADAcGQh>
Dec 6 20:55:46 interno1 postfix/smtpd[2312]: connect from unknown[unknown]
Dec 6 20:55:46 interno1 postfix/smtpd[2312]: lost connection after CONNECT from unknown[unknown]
Dec 6 20:55:46 interno1 postfix/smtpd[2312]: disconnect from unknown[unknown]
```

SYN scanning



```
Dec 6 20:52:41 interno1 kernel: [ 4237.657966] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PREC=0x00 TTL=59 ID=7451 PROTO=TCP SPT=61640 DPT=8701 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 6 20:52:41 interno1 kernel: [ 4237.657982] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PREC=0x00 TTL=54 ID=33471 PROTO=TCP SPT=61640 DPT=2401 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 6 20:52:41 interno1 kernel: [ 4237.658029] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PREC=0x00 TTL=39 ID=19883 PROTO=TCP SPT=61640 DPT=6881 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 6 20:52:41 interno1 kernel: [ 4237.658063] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PREC=0x00 TTL=54 ID=20677 PROTO=TCP SPT=61640 DPT=7512 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 6 20:52:41 interno1 kernel: [ 4237.658082] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PREC=0x00 TTL=57 ID=41907 PROTO=TCP SPT=61640 DPT=6689 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 6 20:52:41 interno1 kernel: [ 4237.658154] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PREC=0x00 TTL=56 ID=29486 PROTO=TCP SPT=61640 DPT=1023 WINDOW=1024 RES=0x00 SYN URGP=0
```

NULL scanning

No genera logs porque los flags están todos a 0. En atacante vemos que no se asegura que ningún puerto esté abierto.