SSO Práctica 1 Sesión 2

Andrés Merlo Trujillo

Índice

Ejercicio 1

Apartado A

Mediante la orden `lsof -i` ejecutada como root, podemos obtener la informacion de los servicios y procesos que tienen alguna conexion abierta o archivo abierto.

La orden ofrece 9 columnas con los siguientes signifiacdos:

- **COMMAND:** Nombre del comando asociado al proceso/archivo.
- **PID:** Process IDentificator (identificador de proceso).
- **USER:** UID del usuario al que pertenece el proceso/archivo.
- **FD:** Descriptor de fichero.
- **TYPE:** Tipo de archivo asociado al mismo (GDIR, GREG, ...) o indica el tipo de conexion (en cpaa de red) (IPv4, IPv6, X.25, etc.).
- **DEVICE:** Numero de dispotivio.
- **SIZE/OFF:** Tamaño del archivo.
- **NODE:** Numero de nodo/inodo de un fichero o el procotolo en capa de transporte (TCP, UDP, ...).
- **NAME:** Punto de montaje y sistema de archivos que usa el archivo abierto. Tambien puede significar la direccion local o remota de internet o de un socket.

A continuación explicaré dos procesos de la salida del comando anterior:

sshd

- **COMMAND:** sshd
- **PID:** 1319
- **USER:** root
- **FD:** 3u/4u (FDs 3 y 4. La letra “u” indica acceso de lectura y escritua)
- **TYPE:** IPv4/IPv6 (está a la espera de recibir algo en las dos versiones del protocolo IP.)
- **DEVICE:** 22997/23008
- **SIZE/OFF:** 0t0 (Offset, el segundo “0” indica que no hay offset)
- **NODE:** TCP (usan este protocolo de transporte porque asegura que se reciben los paquetes mediante ACKs).
- **NAME:** *:ssh (LISTEN) (El asterisco indica que espera de cualquier IP, en el puerto ssh (configurable, por defecto el 22)).

avahi-daemon

- **COMMAND:** avahi-dae (avahi-daemon)
- **PID:** 1144
- **USER:** avahi
- **FD:** 14u (FD 14. La letra “u” indica acceso de lectura y escritua)
- **TYPE:** IPv6
- **DEVICE:** 22668
- **SIZE/OFF:** 0t0 (Offset, el segundo “0” indica que no hay offset)
- **NODE:** UDP
- **NAME:** *:53167 (Cualquier IP en el puerto 53167).

Apartado B

Leyendo el manual, hace falta usar el switch "-i", como en el apartado anterior, y añadiendo que busque las conexiones con el servicio "ssh". Por tanto, el comando quedaria asi: `lsof -i :ssh`.

Ahora mismo no hay nadie conectado, solo estan los "daemons" a la escucha de peticiones de conexion. Si ahora me conecto desde el otra maquina virtual a la de Ubuntu, la salida es la siguiente:

Aparecen dos lineas nuevas y en el apartado `NAME` se ve que la conexion es entre el usuario "andres-kvm" (Ubuntu) usando el servicio "ssh" (en mi caso es el puerto 22) y el usuario "archlinux" en el puerto 57686, que es un puerto que se asigna aleatoriamente para enviar informacion (escuchar) a "archlinux".

Con la orden `lsof -c sshd` se puede ver los archivos que tiene abiertos SSH:

Como se puede ver, aparece el usuario conectado y con el mismo PID aparecen todos los archivos abiertos por `sshd`

Apartado C

Para mostrar los archivos que usa un proceso concreto, es necesario referenciarlo con su PID. Para ello es necesario usar el siguiente comando: `lsof -p PID`.

Y ahora para ver los archivos que esta usando un usuario concreto, se debe usar el switch "-u": `lsof -u usuario`

Por ultimo, para obtener los archivos que tiene abiertos un proceso **Y** un usuario, es necesario usar el switch adicional "-a". Esto es debido a que por defecto solo busca, en caso de haber varios switches, utilizando un criterio **OR**. Comando: `lsof -u usuario -p PID -a`