

SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática - Complementos de Ing. del Software

Curso 2018-19

Práctica 1. Administración de la seguridad en Linux

Sesión 2. Herramientas básicas de seguridad

Autor¹: Víctor García Carrera

Ejercicio 1.

En este apartado trabajamos con el comando *lsof*, que nos permite listar los ficheros abiertos en nuestro sistema. Como establece la propia entrada en el manual de este comando (*man lsof*), los ficheros o archivos abiertos pueden ir desde un fichero regular a una librería o hasta un fichero de red (sockets), por lo que nos permite incluso ver si hay procesos o servicios de nuestro sistema que están accediendo a la red, algo especialmente útil para valorar si hay tráfico sospechoso. En concreto, el comando *lsof -i* nos permite listar todos los archivos de red de Internet y x.25 (HP-UX). Si añadimos como parámetro -i4 or -i6 sin ninguna dirección específica, solo aquellos archivos de la versión IP indicada, IPv4 or IPv6, se muestran.

Al utilizar el comando *lsof* vemos que aparecen multitud de entradas y de ficheros, donde cada entrada consta de la siguiente información:

COMMAND	PID	TID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE NAME
---------	-----	-----	------	----	------	--------	----------	-----------

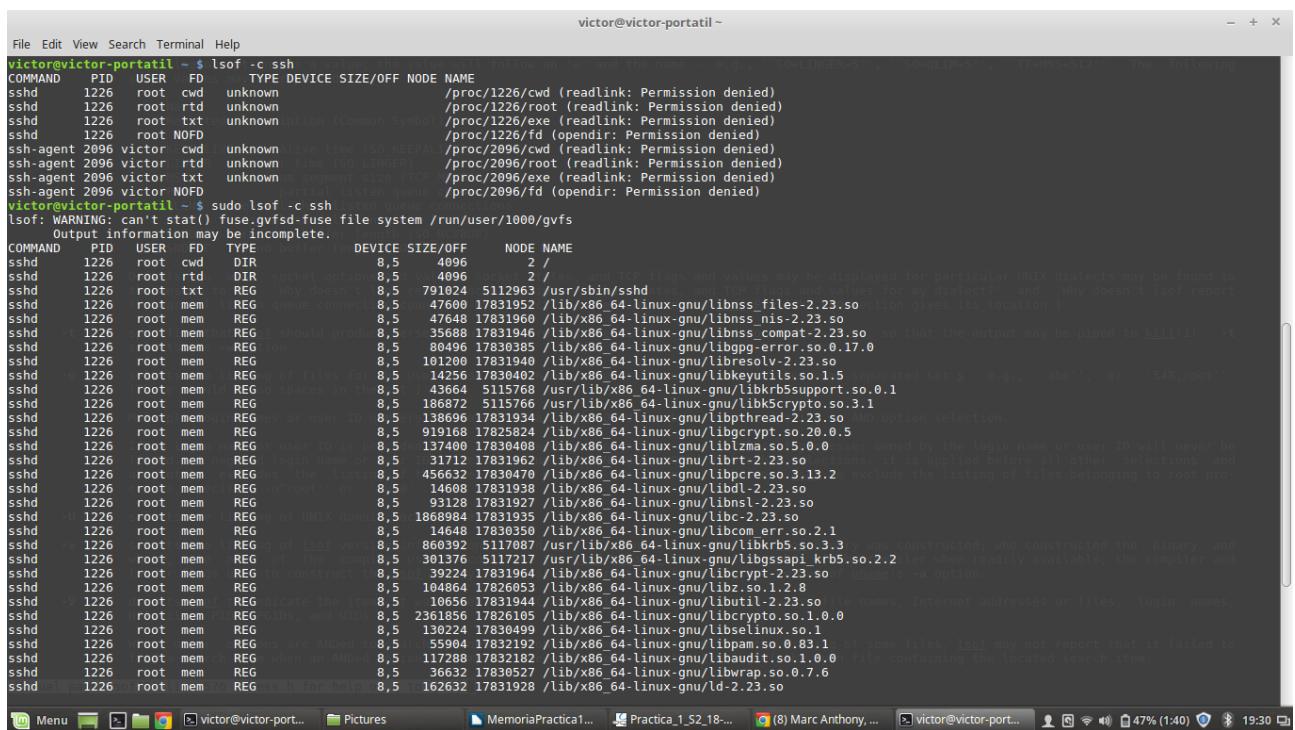
Utilizamos el comando *lsof -i* para ver sólo aquellos archivos relacionados con conexiones abiertas en nuestro sistema, que devuelve la siguiente salida:

```
victor@victor-portatil ~ $ lsof -i
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
chrome 3518 victor 10gu IPv4 34528 0t0 TCP 192.168.0.163:58278->wa-in-f188.1e100.net:5228 (ESTABLISHED)
chrome 3518 victor 134u IPv4 93267 0t0 UDP 192.168.0.163:41592->mad08s04-in-f3.1e100.net:https
chrome 3518 victor 145u IPv4 60052 0t0 UDP 192.168.0.163:58138->mad06s09-in-f14.1e100.net:https
chrome 3518 victor 150u IPv4 36234 0t0 UDP *:mdns
chrome 3518 victor 151u IPv6 36235 0t0 UDP *:mdns
chrome 3518 victor 155u IPv4 58126 0t0 UDP 192.168.0.163:37454->62.42.250.145.static.user.ono.com:https
chrome 3518 victor 163u IPv4 34617 0t0 UDP *:mdns
victor@victor-portatil ~ $ lsof -i
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
gvfsd-smb 7011 victor 1lu IPv4 93153 0t0 TCP 192.168.0.163:41066->192.168.0.154:netbios-ssn (ESTABLISHED)
victor@victor-portatil ~ $ lsof -i
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
gvfsd-smb 7011 victor 1lu IPv4 93153 0t0 TCP 192.168.0.163:41066->192.168.0.154:netbios-ssn (ESTABLISHED)
victor@victor-portatil ~ $ lsof -i
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
gvfsd-smb 7011 victor 1lu IPv4 93153 0t0 TCP 192.168.0.163:41066->192.168.0.154:netbios-ssn (ESTABLISHED)
chrome 7117 victor 8lu IPv4 96465 0t0 UDP *:mdns
chrome 7117 victor 86u IPv4 95490 0t0 UDP 192.168.0.163:59229
chrome 7117 victor 114u IPv4 93697 0t0 TCP 192.168.0.163:58320->wa-in-f188.1e100.net:5228 (ESTABLISHED)
chrome 7117 victor 120u IPv4 95522 0t0 TCP 192.168.0.163:50258->mad08s05-in-f3.1e100.net:https (ESTABLISHED)
chrome 7117 victor 138u IPv4 95521 0t0 UDP 192.168.0.163:54499->arn02s06-in-f163.1e100.net:https
chrome 7117 victor 145u IPv6 96466 0t0 UDP *:mdns
chrome 7117 victor 146u IPv4 93778 0t0 UDP 192.168.0.163:55628->mad07s10-in-f10.1e100.net:https
chrome 7117 victor 156u IPv4 95537 0t0 TCP 192.168.0.163:40756->mad07s10-in-f10.1e100.net:https (ESTABLISHED)
chrome 7117 victor 191u IPv4 95052 0t0 UDP 192.168.0.163:46881->mad08s06-in-f1.1e100.net:https
chrome 7117 victor 193u IPv4 93830 0t0 TCP 192.168.0.163:41912->mad08s06-in-f13.1e100.net:https (ESTABLISHED)
chrome 7117 victor 202u IPv4 95046 0t0 UDP 192.168.0.163:36906->mad08s06-in-f13.1e100.net:https
chrome 7117 victor 224u IPv4 96568 0t0 UDP 192.168.0.163:50613->par03s12-in-f142.1e100.net:https
chrome 7117 victor 227u IPv4 96571 0t0 UDP 192.168.0.163:37794->muc03s14-in-f33.1e100.net:https
chrome 7117 victor 234u IPv4 95059 0t0 TCP 192.168.0.163:43310->par03s12-in-f142.1e100.net:https (ESTABLISHED)
chrome 7117 victor 241u IPv4 96596 0t0 UDP 192.168.0.163:44905->arn02s06-in-f174.1e100.net:https
chrome 7117 victor 245u IPv4 95641 0t0 TCP 192.168.0.163:36498->arn02s06-in-f174.1e100.net:https (ESTABLISHED)
chrome 7117 victor 253u IPv4 96632 0t0 TCP 192.168.0.163:33246->muc03s14-in-f10.1e100.net:https (ESTABLISHED)
victor@victor-portatil ~ $
```

¹ Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la “Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada” esto “conllevará la calificación numérica de cero ... independientemente del resto de calificaciones que el estudiante hubiera obtenido ...”

En la primera llamada estaba reproduciendo en google chrome un video de youtube. Vemos como hay un proceso TCP que parece que se utiliza para establecer la conexión con el servidor, y otros procesos que utilizan UDP que seguramente se traten de aquellos destinados al tráfico del video en si. En la segunda y tercera llamada había cerrado el buscador, y sólo aparece una entrada asociada a un proceso que monta SAMBA, utilizado para compartir archivos a través de la red (gvfsd-smb). En las últimas llamadas de nuevo he abierto el buscador y reproducido un video de youtube, apareciendo entradas similares a las primeras. La herramienta, como he descrito previamente, proporciona información como el PID del proceso asociado (podemos ver los PID de los procesos del sistema con el comando `ps`), el usuario del mismo, la versión IP...

Cabe destacar que estos comandos proporcionan una información más completa cuando se ejecutan en modo superusuario (sudo). Si queremos conocer por ejemplo si hay tráfico ssh, podemos utilizar el comando `lsof -c ssh` para así listar los archivos abiertos por procesos activos que utilizan el comando ssh. De esta manera, podemos ver no sólo la ruta de estos archivos, sino además el usuario del proceso que está ejecutando ese comando (generando el tráfico ssh).



```
victor@victor-portatil ~ $ lsof -c ssh
File Edit View Search Terminal Help
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
sshd 1226 root cwd unknown /proc/1226/cwd (readlink: Permission denied)
sshd 1226 root rtd unknown /proc/1226/root (readlink: Permission denied)
sshd 1226 root txt unknown /proc/1226/exe (readlink: Permission denied)
sshd 1226 root NOFD /proc/1226/fd (opendir: Permission denied)
sshd-agent 2894 victor cwd unknown /proc/2894/cwd (readlink: Permission denied)
sshd-agent 2894 victor rtd unknown /proc/2894/root (readlink: Permission denied)
sshd-agent 2894 victor txt unknown /proc/2894/exe (readlink: Permission denied)
sshd-agent 2894 victor NOFD /proc/2894/fd (opendir: Permission denied)
victor@victor-portatil ~ $ sudo lsof -c ssh
lsof: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
sshd 1226 root cwd DIR 0,5 4096 2 /
sshd 1226 root rtd DIR 0,5 4096 2 / (warning: some flags and values may be displayed for particular UNIX dialects; see the man page for my dialect!) and "Why doesn't lsof report
sshd 1226 root txt REG 0,5 791024 5112963 /usr/sbin/sshd (warning: some flags and values may be displayed for particular UNIX dialects; see the man page for my dialect!) and "Why doesn't lsof report
sshd 1226 root mem REG 0,5 47600 17831952 /lib/x86_64-linux-gnu/libnss_files-2.23.so
sshd 1226 root mem REG 0,5 47648 17831960 /lib/x86_64-linux-gnu/libnsc_nis-2.23.so
sshd 1226 root mem REG 0,5 35688 17831946 /lib/x86_64-linux-gnu/libnss_compat-2.23.so so that the output may be piped to kill(1). -t
sshd 1226 root mem REG 0,5 80496 17830385 /lib/x86_64-linux-gnu/libcrypt-error.so.0.17.0
sshd 1226 root mem REG 0,5 101200 17831948 /lib/x86_64-linux-gnu/libresolv-2.23.so
sshd 1226 root mem REG 0,5 14256 17830402 /lib/x86_64-linux-gnu/libcrypt-0.1.5
sshd 1226 root mem REG 0,5 43664 5115768 /usr/lib/x86_64-linux-gnu/libkrb5support.so.0.1
sshd 1226 root mem REG 0,5 186872 5115766 /usr/lib/x86_64-linux-gnu/libk5crypto.so.3.1
sshd 1226 root mem REG 0,5 138606 17831934 /lib/x86_64-linux-gnu/libpthread-2.23.so
sshd 1226 root mem REG 0,5 910168 17828824 /lib/x86_64-linux-gnu/libcrypt.so.0.20.5
sshd 1226 root mem REG 0,5 137408 17830408 /lib/x86_64-linux-gnu/libzma.so.5.0.0
sshd 1226 root mem REG 0,5 31712 17831962 /lib/x86_64-linux-gnu/librt-2.23.so
sshd 1226 root mem REG 0,5 456632 17830470 /lib/x86_64-linux-gnu/libpcrypt.so.3.13.2
sshd 1226 root mem REG 0,5 14608 17831938 /lib/x86_64-linux-gnu/libdl-2.23.so
sshd 1226 root mem REG 0,5 93128 17831929 /lib/x86_64-linux-gnu/libnss-2.23.so
sshd 1226 root mem REG 0,5 1809984 17831935 /lib/x86_64-linux-gnu/libc-2.23.so
sshd 1226 root mem REG 0,5 14648 17830350 /lib/x86_64-linux-gnu/libcom_err.so.2.1
sshd 1226 root mem REG 0,5 860392 51179097 /usr/lib/x86_64-linux-gnu/libkrb5.so.3.3
sshd 1226 root mem REG 0,5 301376 5117217 /usr/lib/x86_64-linux-gnu/libgsapi_krb5.so.2.2
sshd 1226 root mem REG 0,5 39224 17831964 /lib/x86_64-linux-gnu/libcrypt-2.23.so
sshd 1226 root mem REG 0,5 104864 17826053 /lib/x86_64-linux-gnu/libz.so.1.2.8
sshd 1226 root mem REG 0,5 10656 17831944 /lib/x86_64-linux-gnu/libutil-2.23.so
sshd 1226 root mem REG 0,5 2361856 17826105 /lib/x86_64-linux-gnu/libcrypto.so.1.0.0
sshd 1226 root mem REG 0,5 130224 17830499 /lib/x86_64-linux-gnu/libselinux.so.1
sshd 1226 root mem REG 0,5 55904 17832192 /lib/x86_64-linux-gnu/libpam.so.0.83.1
sshd 1226 root mem REG 0,5 117288 17832182 /lib/x86_64-linux-gnu/libaudit.so.1.0.0
sshd 1226 root mem REG 0,5 36632 17830527 /lib/x86_64-linux-gnu/libwrap.so.0.7.6
sshd 1226 root mem REG 0,5 162632 17831928 /lib/x86_64-linux-gnu/ld-2.23.so
victor@victor-portatil ~ $
```

Finalmente, si queremos conocer los archivos a los que está accediendo un proceso con PID x en concreto, utilizamos el comando `lsof -p "x"`. Si queremos conocer los archivos en uso por un usuario con nombre y, utilizamos el comando `lsof -u "y"`.

A continuación se encuentran 2 imágenes donde se ejemplifica esto, mostrando los archivos del proceso con PID 8941 y los archivos del usuario "victor" (que son bastantes al ser el usuario principal del sistema):

```
victor@victor-portatil ~
File Edit View Search Terminal Help
8941 pts/0 S+ 0:00 man lsof
8950 pts/0 S+ 0:00 man lsof
8951 pts/0 S+ 0:00 pager
8979 ? S 0:00 [kworker/u16:2]
9056 pts/1 Ss 0:00 bash
9071 ? S 0:03 [kworker/0:1]
9481 ? S 0:00 [kworker/1:1]
9509 ? S 0:00 [kworker/3:0]
9760 ? Sl 0:01 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671,131072 --service-pipe-token=983854353
9779 ? Sl 0:02 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671,131072 --service-pipe-token=175008022
9795 ? S 0:00 [kworker/2:0]
9871 ? S 0:00 [kworker/u16:0]
10026 ? S 0:00 [kworker/1:2]
10059 ? S 0:01 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671,131072 --service-pipe-token=127120573
10092 ? Sl 0:00 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671,131072 --service-pipe-token=843091464
10106 ? Sl 0:00 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671,131072 --service-pipe-token=663695750
10117 ? S 0:00 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671,131072 --service-pipe-token=551537625
10151 ? S 0:00 [kworker/3:1]
10659 ? S 0:00 [kworker/2:0]
10666 ? S 0:00 [kworker/0:2]
10789 ? S 0:00 [kworker/1:0]
10816 ? S 0:00 [kworker/3:2]
10828 ? Sl 0:00 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671,131072 --service-pipe-token=511984071
10951 ? S 0:00 [kworker/2:1]
10953 ? S 0:00 [kworker/0:0]
11049 pts/1 R+ 0:00 ps -ax
victor@victor-portatil ~ $ lsof -p "8941"
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
man 8941 victor cwd DIR 8,5 4096 5767212 /usr/share/man
man 8941 victor rtd DIR 8,5 4096 2 /
man 8941 victor txt REG 8,5 167008 5112714 /usr/bin/man
man 8941 victor mem REG 8,5 4228608 5113961 /usr/lib/locale/locale-archive
man 8941 victor mem REG 8,5 104864 17826653 /lib/x86_64-linux-gnu/libz.so.1.2.8 command names, file names, Internet addresses or files, login names,
man 8941 victor mem REG 8,5 22600 5121799 /usr/lib/x86_64-linux-gnu/libgdbm.so.3.0.0
man 8941 victor mem REG 8,5 1868984 17831935 /lib/x86_64-linux-gnu/libc-2.23.so
man 8941 victor mem REG 8,5 55136 5122775 /usr/lib/x86_64-linux-gnu/libpipeline.so.1.4.1 listing of some files, lsof may not report that it failed to
man 8941 victor mem REG 8,5 136192 5119976 /usr/lib/man-db/libman-2.7.5.so
man 8941 victor mem REG 8,5 23268 5119972 /usr/lib/man-db/libmandb-2.7.5.so
man 8941 victor mem REG 8,5 162632 17831928 /lib/x86_64-linux-gnu/ld-2.23.so
man 8941 victor mem REG 8,5 26258 5507572 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache XSECURITY are defined at compile time and they prevent
man 8941 victor ou CHR 136,0 0t0 3 /dev/pts/0
man 8941 victor lu CHR 136,0 0t0 3 /dev/pts/0
man 8941 victor zu CHR 136,0 0t0 3 /dev/pts/0
man 8941 victor 3r DIR 8,5 4096 18743298 /home/victor
victor@victor-portatil ~ $
```

Iconos de la barra de tareas: Menu, Home, Minimizar, Maximizar, Cerrar, victor@victor-port..., Pictures, MemoriaPractica1..., Practica_1_S2_18..., (8) lofi hip hop radi..., victor@victor-port..., 41% (1:22), 19:39

```
victor@victor-portatil ~
File Edit View Search Terminal Help
chrome 11650 victor 27r FIFO 0,10 0t0 134815 pipe
chrome 11650 victor 28w FIFO 0,10 0t0 134815 pipe
chrome 11650 victor 29u unix 0x0000000000000000 0t0 132879 type=STREAM
chrome 11650 victor 30u REG 0,21 2897152 53 /dev/shm/.com.google.Chrome.coKfv (deleted)
chrome 11650 victor 32r REG 0,21 101220 12 /dev/shm/.com.google.Chrome.SwRQEd (deleted)
chrome 11650 victor 33r REG /nologin 8,5 105640 16661727 /home/victor/.config/google-chrome/Subresource Filter/Index Rules/20/9.0/Ruleset Data
chrome 11650 victor 34r REG /nologin 8,5 446642 18748915 /home/victor/.config/google-chrome/Dictionaries/en-US-0.bdic
lsof 12400 victor cwd DIR /login 8,5 4096 1874298 /home/victor
lsof 12400 victor rtd DIR /login 8,5 4096 2 /
lsof 12400 victor txt REG /nologin 8,5 163224 5112682 /usr/bin/lsof
lsof 12400 victor mem REG /sbin/nologin 8,5 47600 17831952 /lib/x86_64-linux-gnu/libnss_files-2.23.so
lsof 12400 victor mem REG /nologin 8,5 47648 17831960 /lib/x86_64-linux-gnu/libnss_nis-2.23.so
lsof 12400 victor mem REG /sbin/nologin 8,5 93128 17831927 /lib/x86_64-linux-gnu/libnsl-2.23.so
lsof 12400 victor mem REG /nologin 8,5 35688 17831946 /lib/x86_64-linux-gnu/libnss_compat-2.23.so
lsof 12400 victor mem REG /nologin 8,5 4228608 5113961 /usr/lib/locale/locale-archive
lsof 12400 victor mem REG /nologin 8,5 138696 17831934 /lib/x86_64-linux-gnu/libpthread-2.23.so
lsof 12400 victor mem REG /nologin 8,5 14608 17831938 /lib/x86_64-linux-gnu/libdl-2.23.so
lsof 12400 victor mem REG /nologin 8,5 456632 17830470 /lib/x86_64-linux-gnu/libpcre.so.3.13.2
lsof 12400 victor mem REG /nologin 8,5 1868984 17831935 /lib/x86_64-linux-gnu/libc-2.23.so
lsof 12400 victor mem REG /nologin 8,5 130224 17830499 /lib/x86_64-linux-gnu/libselinux.so.1
lsof 12400 victor mem REG /nologin 8,5 162632 17831928 /lib/x86_64-linux-gnu/ld-2.23.so
lsof 12400 victor ou CHR /Proxy 136,0 0t0 3 /dev/pts/0
lsof 12400 victor lu CHR 136,0 0t0 3 /dev/pts/0
lsof 12400 victor zu CHR 136,0 0t0 3 /dev/pts/0
lsof 12400 victor 3r DIR /false 0,4 0 1 /proc
lsof 12400 victor 4r DIR 0,4 0 139984 /proc/12400/fd
lsof 12400 victor 5w FIFO 0,10 0t0 139989 pipe
lsof 12400 victor 6r FIFO 0,10 0t0 139990 pipe
lsof 12401 victor cwd DIR 8,5 4096 18743298 /home/victor
lsof 12401 victor rtd DIR 8,5 4096 2 /
lsof 12401 victor txt REG 8,5 163224 5112682 /usr/bin/lsof
lsof 12401 victor mem REG 8,5 47600 17831952 /lib/x86_64-linux-gnu/libnss_files-2.23.so
lsof 12401 victor mem REG 8,5 47648 17831960 /lib/x86_64-linux-gnu/libnss_nis-2.23.so
lsof 12401 victor mem REG 8,5 93128 17831927 /lib/x86_64-linux-gnu/libnsl-2.23.so
lsof 12401 victor mem REG 8,5 35688 17831946 /lib/x86_64-linux-gnu/libnss_compat-2.23.so
lsof 12401 victor mem REG 8,5 4228608 5113961 /usr/lib/locale/locale-archive
lsof 12401 victor mem REG 8,5 138696 17831934 /lib/x86_64-linux-gnu/libpthread-2.23.so
lsof 12401 victor mem REG 8,5 14608 17831938 /lib/x86_64-linux-gnu/libdl-2.23.so
lsof 12401 victor mem REG 8,5 456632 17830470 /lib/x86_64-linux-gnu/libpcre.so.3.13.2
lsof 12401 victor mem REG 8,5 1868984 17831935 /lib/x86_64-linux-gnu/libc-2.23.so
lsof 12401 victor mem REG 8,5 130224 17830499 /lib/x86_64-linux-gnu/libselinux.so.1
lsof 12401 victor mem REG 8,5 162632 17831928 /lib/x86_64-linux-gnu/ld-2.23.so
lsof 12401 victor 4r FIFO 0,10 0t0 139989 pipe
lsof 12401 victor 7w FIFO 0,10 0t0 139990 pipe
victor@victor-portatil ~ $
```

Iconos de la barra de tareas: Menu, Home, Minimizar, Maximizar, Cerrar, victor@victor-port..., Pictures, MemoriaPractica1..., Practica_1_S2_18..., (8) lofi hip hop radi..., root@victor-port..., 32% (1:29), 19:59

Ejercicio 2.

En el siguiente apartado trabajamos con el comando `ps`, que permite listar los procesos activos en el sistema. Tomamos capturas de la salida de este comando en diversos momentos, con diversas opciones para visualizar unos procesos u otros (`ps -aux` para ver todos los procesos activos, `ps -eau` para ver el momento de inicio de los mismos), y comprobamos con el comando `diff` que las diferencias básicamente radican en los nuevos procesos creados (y la finalización de otros) a raíz de un uso normal del

sistema, como puede ser ver una entrada de un comando en el manual (*man diff*), ejecutar en otra terminal la herramienta Lynis para explorar vulnerabilidades del sistema...

```
victor@victor-portatil ~ $ ps
  PID TTY      TIME CMD
 3496 pts/0    00:00:00 bash
12652 pts/0    00:00:00 ps
victor@victor-portatil ~ $ ps -eau
USER   PID %CPU %MEM   VSZ   RSS TTY      STAT START  TIME COMMAND
root   1516  0.0  0.0 17156 1876 ttyl    S+ 17:11  0:00 /sbin/agetty --noclear ttyl linux
root   1643  1.3  0.6 419292 103784 ttys8  S+ 17:11  2:23 /usr/lib/xorg/Xorg :0 -audit 0 -auth /var/lib/xdm/:0.Xauth -nolisten tcp vt8
victor 3496  0.0  0.0 24016 5636 pts/0   Ss 17:37  0:00 bash XDG_CONFIG_DIRS=/etc/xdg/xdg-cinnamon:/etc/xdg LC_TELEPHONE=es_ES.UTF-8 LANG=en_US.UTF-8 DISPLAY=:
victor 9056  0.0  0.0 24008 5584 pts/1   Ss 19:14  0:00 bash XDG_CONFIG_DIRS=/etc/xdg/xdg-cinnamon:/etc/xdg LC_TELEPHONE=es_ES.UTF-8 LANG=en_US.UTF-8 DISPLAY=:
root  11402  0.0  0.0 97036 5100 pts/1   S 19:41  0:00 sudo su
root  11403  0.0  0.0 96608 5000 pts/1   S 19:41  0:00 su
root  11412  0.0  0.0 23868 5568 pts/1   S+ 19:41  0:00 bash
victor 12658  0.0  0.0 38584 3400 pts/0   R+ 20:04  0:00 ps -eau LC_PAPER=es_ES.UTF-8 XDG_VTNR=8 LC_ADDRESS=es_ES.UTF-8 SSH_AGENT_PID=2096 XDG_SESSION_ID=c1 LC_
victor@victor-portatil ~ $
```

```
victor@victor-portatil ~ $ ps -eau
  PID TTY      TIME CMD
 3496 pts/0    00:00:00 bash
13069 pts/0    00:00:00 ps
victor@victor-portatil ~ $ ps
  PID TTY      TIME CMD
 3496 pts/0    00:00:00 bash
13298 pts/0    00:00:00 ps
victor@victor-portatil ~ $ ps -eau
USER   PID %CPU %MEM   VSZ   RSS TTY      STAT START  TIME COMMAND
root   1516  0.0  0.0 17156 1876 ttyl    S+ 17:11  0:00 /sbin/agetty --noclear ttyl linux
root   1643  1.4  0.6 428916 108196 ttys8  S+ 17:11  2:29 /usr/lib/xorg/Xorg :0 -audit 0 -auth /var/lib/xdm/:0.Xauth -nolisten tcp vt8
victor 3496  0.0  0.0 24016 5636 pts/0   Ss 17:37  0:00 bash XDG_CONFIG_DIRS=/etc/xdg/xdg-cinnamon:/etc/xdg LC_TELEPHONE=es_ES.UTF-8 LANG=en_US.UTF-8 DISPLAY=:
victor 9056  0.0  0.0 24008 5584 pts/1   Ss 19:14  0:00 bash XDG_CONFIG_DIRS=/etc/xdg/xdg-cinnamon:/etc/xdg LC_TELEPHONE=es_ES.UTF-8 LANG=en_US.UTF-8 DISPLAY=:
root  11402  0.0  0.0 97036 5100 pts/1   S 19:41  0:00 sudo su
root  11403  0.0  0.0 96608 5000 pts/1   S 19:41  0:00 su
root  11412  0.0  0.0 23868 5568 pts/1   S+ 19:41  0:00 bash
victor 12711  0.0  0.0 23932 5296 pts/2   S+ 20:05  0:00 bash XDG_CONFIG_DIRS=/etc/xdg/xdg-cinnamon:/etc/xdg LC_TELEPHONE=es_ES.UTF-8 LANG=en_US.UTF-8 DISPLAY=:
victor 13920  0.0  0.0 38584 3452 pts/0   R+ 20:08  0:00 ps -eau LC_PAPER=es_ES.UTF-8 XDG_VTNR=8 LC_ADDRESS=es_ES.UTF-8 SSH_AGENT_PID=2096 XDG_SESSION_ID=c1 LC_
victor@victor-portatil ~ $ ps
  PID TTY      TIME CMD
 3496 pts/0    00:00:00 bash
13298 pts/0    00:00:00 ps
victor@victor-portatil ~ $ ps -eau
USER   PID %CPU %MEM   VSZ   RSS TTY      STAT START  TIME COMMAND
root   1516  0.0  0.0 17156 1876 ttyl    S+ 17:11  0:00 /sbin/agetty --noclear ttyl linux
root   1643  1.3  0.6 423620 103540 ttys8  S+ 17:11  2:30 /usr/lib/xorg/Xorg :0 -audit 0 -auth /var/lib/xdm/:0.Xauth -nolisten tcp vt8
victor 3496  0.0  0.0 24016 5636 pts/0   Ss 17:37  0:00 bash XDG_CONFIG_DIRS=/etc/xdg/xdg-cinnamon:/etc/xdg LC_TELEPHONE=es_ES.UTF-8 LANG=en_US.UTF-8 DISPLAY=:
victor 9056  0.0  0.0 24008 5584 pts/1   Ss 19:14  0:00 bash XDG_CONFIG_DIRS=/etc/xdg/xdg-cinnamon:/etc/xdg LC_TELEPHONE=es_ES.UTF-8 LANG=en_US.UTF-8 DISPLAY=:
root  11402  0.0  0.0 97036 5100 pts/1   S 19:41  0:00 sudo su
root  11403  0.0  0.0 96608 5000 pts/1   S 19:41  0:00 su
root  11412  0.0  0.0 23868 5568 pts/1   S+ 19:41  0:00 bash
victor 12711  0.0  0.0 23932 5296 pts/2   S+ 20:05  0:00 bash XDG_CONFIG_DIRS=/etc/xdg/xdg-cinnamon:/etc/xdg LC_TELEPHONE=es_ES.UTF-8 LANG=en_US.UTF-8 DISPLAY=:
victor 13897  0.0  0.0 19568 3004 pts/2   S+ 20:08  0:00 man diff LC_PAPER=es_ES.UTF-8 XDG_VTNR=8 LC_ADDRESS=es_ES.UTF-8 SSH_AGENT_PID=2096 XDG_SESSION_ID=c1 LC_
victor 13109  0.0  0.0 18876  884 pts/2   S+ 20:08  0:00 pager LC_PAPER=es_ES.UTF-8 XDG_VTNR=8 LC_ADDRESS=es_ES.UTF-8 SSH_AGENT_PID=2096 XDG_SESSION_ID=c1 LC_
victor 13305  0.0  0.0 38584 3412 pts/0   R+ 20:12  0:00 ps -eau LC_PAPER=es_ES.UTF-8 XDG_VTNR=8 LC_ADDRESS=es_ES.UTF-8 SSH_AGENT_PID=2096 XDG_SESSION_ID=c1 LC_
victor@victor-portatil ~ $
```

```
victor@victor-portatil ~ $ ps -eau
  PID TTY      TIME CMD
 3496 pts/0    00:00:00 bash
13069 pts/0    00:00:00 ps
victor@victor-portatil ~ $ ps
  PID TTY      TIME CMD
 3496 pts/0    00:00:00 bash
13298 pts/0    00:00:00 ps
victor@victor-portatil ~ $ ps -eau
USER   PID %CPU %MEM   VSZ   RSS TTY      STAT START  TIME COMMAND
root   1516  0.0  0.0 17156 1876 ttyl    S+ 17:11  0:00 /sbin/agetty --noclear ttyl linux
root   1643  1.5  0.6 438216 108848 ttys8  S+ 17:11  3:30 /usr/lib/xorg/Xorg :0 -audit 0 -auth /var/lib/xdm/:0.Xauth -nolisten tcp vt8
victor 3496  0.0  0.0 24076 5700 pts/0   Ss 17:37  0:00 bash XDG_CONFIG_DIRS=/etc/xdg/xdg-cinnamon:/etc/xdg LC_TELEPHONE=es_ES.UTF-8 LANG=en_US.UTF-8 DISPLAY=:
victor 9212  0.0  0.0 38584 3432 pts/2   R+ 20:51  0:00 ps -eau LC_PAPER=es_ES.UTF-8 XDG_VTNR=8 LC_ADDRESS=es_ES.UTF-8 SSH_AGENT_PID=2096 XDG_SESSION_ID=c1 LC_
victor 12711  0.0  0.0 23932 5296 pts/2   Ss 20:05  0:00 bash XDG_CONFIG_DIRS=/etc/xdg/xdg-cinnamon:/etc/xdg LC_TELEPHONE=es_ES.UTF-8 LANG=en_US.UTF-8 DISPLAY=:
root  30379  0.0  0.0 97320 5316 pts/0   S+ 20:50  0:00 sudo lynis audit system
root  30383  3.3  0.0 5000  2256 pts/0   S+ 20:50  0:01 /bin/sh /usr/sbin/lynis audit system
victor@victor-portatil ~ $
```

```
root 10789  0.0  0.0     0   0 ?      S 19:32  0:00 [kworker/1:0]
root 10951  0.0  0.0     0   0 ?      S 19:34  0:00 [kworker/2:1]
root 11298  0.0  0.0     0   0 ?      S 19:39  0:01 [kworker/u16:3]
root 11402  0.0  0.0 97036 5100 pts/1   S 19:41  0:00 sudo su
root 11403  0.0  0.0 96608 5000 pts/1   S 19:41  0:00 su
root 11412  0.0  0.0 23868 5568 pts/1   S+ 19:41  0:00 bash
root 11665  0.0  0.0     0   0 ?      S 19:43  0:00 [kworker/3:3]
victor 11614  0.0  0.7 751304 117264 ?    Sl 19:43  0:01 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
root 12867  0.0  0.0     0   0 ?      S 19:52  0:00 [kworker/u16:1]
root 12315  0.0  0.0     0   0 ?      S 19:58  0:00 [kworker/1:2]
root 12362  0.0  0.0     0   0 ?      S 19:58  0:00 [kworker/3:0]
root 12446  0.0  0.0     0   0 ?      S 20:00  0:00 [kworker/2:2]
root 12448  0.0  0.0     0   0 ?      S 20:00  0:00 [kworker/0:2]
root 12618  0.0  0.0     0   0 ?      S 20:03  0:00 [kworker/1:1]
root 12632  0.0  0.0     0   0 ?      S 20:03  0:00 [kworker/3:1]
root 12661  0.0  0.0     0   0 ?      S 20:04  0:00 [kworker/u16:0]
victor 12711  0.0  0.0 23932 5296 pts/2   S+ 20:05  0:00 bash
root 12750  0.0  0.0     0   0 ?      S 20:05  0:00 [kworker/2:0]
root 12752  0.0  0.0     0   0 ?      S 20:05  0:00 [kworker/0:0]
root 12783  0.0  0.0     0   0 ?      S 20:06  0:00 [kworker/u16:2]
victor 12827 11.6  1.2 908776 212324 ?    Sl 20:06  0:08 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
victor 12856  0.0  0.3 669544 64544 ?    Sl 20:06  0:08 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
victor 12903  1.0  0.6 722712 106932 ?    Sl 20:06  0:08 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
victor 12938  0.0  0.2 656092 48508 ?    Sl 20:06  0:08 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
victor 12984  0.0  0.0 38584 3428 pts/0   R+ 20:07  0:00 ps -aux
victor@victor-portatil ~ $
```

Social Entradas

2018 (112) v. Ocubre (10)

Monitorear la actividad de Name.com Gramea-HMmx09+colleci... Charcar medidas de colectad... con Gramea De acuerdo

```

root 10951 0.0 0.0 0 0 ? S 19:34 0:00 [kworker/2:1]
root 11298 0.0 0.0 0 0 ? S 19:39 0:01 [kworker/u16:3]
root 11402 0.0 0.0 97036 5100 pts/1 S 19:41 0:00 sudo su
root 11403 0.0 0.0 96608 5000 pts/1 S 19:41 0:00 su
root 11412 0.0 0.0 23868 5568 pts/1 S+ 19:41 0:00 bash
root 11605 0.0 0.0 0 0 ? S 19:43 0:00 [kworker/3:3]
victor 11614 0.0 0.7 751304 118180 ? Sl 19:43 0:01 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
root 12315 0.0 0.0 0 0 ? S 19:58 0:00 [kworker/1:2]
root 12448 0.0 0.0 0 0 ? S 20:00 0:00 [kworker/0:2]
root 12618 0.0 0.0 0 0 ? S 20:03 0:00 [kworker/1:1]
root 12632 0.0 0.0 0 0 ? S 20:03 0:00 [kworker/3:1]
root 12661 0.0 0.0 0 0 ? S 20:04 0:00 [kworker/u16:0]
victor 12711 0.0 0.0 23932 5296 pts/2 Ss 20:05 0:00 bash
root 12750 0.0 0.0 0 0 ? S 20:05 0:00 [kworker/2:0]
root 12752 0.0 0.0 0 0 ? S 20:05 0:00 [kworker/0:0]
root 12783 0.0 0.0 0 0 ? S 20:06 0:00 [kworker/u16:2]
victor 12827 6.0 1.3 938040 226072 ? Sl 20:06 0:23 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
victor 12903 0.1 0.6 721284 106428 ? Sl 20:06 0:00 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
victor 12938 0.0 0.2 656092 48508 ? Sl 20:06 0:00 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
root 13079 0.0 0.0 0 0 ? S 20:08 0:00 [kworker/1:0]
root 13086 0.1 0.0 0 0 ? S 20:08 0:00 [kworker/0:3]
victor 13097 0.0 0.0 19568 3004 pts/2 S+ 20:08 0:00 man diff
victor 13109 0.0 0.0 10876 884 pts/2 S+ 20:08 0:00 pager
root 13165 0.0 0.0 0 0 ? S 20:09 0:00 [kworker/3:0]
root 13226 0.0 0.0 0 0 ? S 20:10 0:00 [kworker/2:2]
root 13294 0.0 0.0 0 0 ? S 20:12 0:00 [kworker/u16:1]
root 13325 0.0 0.0 15672 1144 ? Ss 20:12 0:00 /lib/systemd/systemd-hostnamed
victor 13339 0.0 0.0 38584 3432 pts/0 R+ 20:13 0:00 ps -aux
victor@victor-portatil ~ $ █ press h for help or q to quit
```

Terminal window showing the output of the 'ps aux' command.

```

Victor 10117 0.0 0.6 732716 108680 ? Sl 19:27 0:00 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
Victor 11614 0.0 0.7 751304 118699 ? Sl 19:43 0:01 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
Victor 12711 0.0 0.0 23932 5296 pts/2 Ss 20:05 0:00 bash
Victor 12903 0.0 0.6 732936 103696 ? Sl 20:06 0:00 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
root 13089 0.0 0.0 0 0 ? S 20:14 0:00 [kworker/3:1]
victor 14941 0.0 0.6 726148 100388 ? Sl 20:17 0:01 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
victor 27801 13.4 1.6 997740 274232 ? Sl 20:28 2:56 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
root 28043 0.0 0.0 0 0 ? S 20:30 0:00 [kworker/2:2]
root 28120 0.4 0.0 0 0 ? S 20:32 0:04 [kworker/0:0]
victor 28637 0.0 0.6 740488 110468 ? Sl 20:37 0:00 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
root 28664 0.0 0.0 0 0 ? S 20:37 0:00 [kworker/u16:3]
victor 28716 0.0 0.2 378844 41596 ? S 20:37 0:00 /usr/bin/kuiserver
root 29178 0.0 0.0 0 0 ? S 20:39 0:00 [kworker/1:0]
root 29541 0.0 0.0 0 0 ? S 20:41 0:00 [kworker/2:0]
root 29612 0.0 0.0 0 0 ? S 20:42 0:00 [kworker/u16:1]
root 29613 0.0 0.0 0 0 ? S 20:42 0:00 [kworker/0:2]
root 29851 0.0 0.0 0 0 ? S 20:44 0:00 [kworker/1:2]
root 29883 0.0 0.0 0 0 ? S 20:44 0:00 [kworker/3:2]
root 30009 0.0 0.0 0 0 ? S 20:46 0:00 [kworker/2:1]
root 30103 0.0 0.0 0 0 ? S 20:47 0:00 [kworker/u16:0]
root 30108 0.0 0.0 0 0 ? S 20:47 0:00 [kworker/0:1]
victor 30113 0.0 0.3 677868 64012 ? Sl 20:47 0:00 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
victor 30124 0.0 0.3 664288 49468 ? Sl 20:47 0:00 /opt/google/chrome/chrome --type=renderer --field-trial-handle=6174303405770928592,14387189769227263671
root 30336 0.0 0.0 0 0 ? S 20:49 0:00 [kworker/3:0]
root 30364 0.0 0.0 0 0 ? S 20:50 0:00 [kworker/1:1]
root 30379 0.0 0.0 97320 5316 pts/0 S+ 20:50 0:00 sudo lynis audit system
root 30383 6.4 0.0 5000 2256 pts/0 S+ 20:50 0:01 /bin/sh /usr/sbin/lynis audit system
victor@victor-portatil ~ $ █
```

Terminal window showing the output of the 'ps aux' command.

Ejercicio 3.

En este ejercicio trabajamos con la herramienta Lynis. Comenzamos utilizando el comando `sudo lynis audit system` para realizar una auditoría del sistema, evaluar los fallos del mismo y obtener recomendaciones para solucionarlos.

```

victor@victor-portatil ~
File Edit View Search Terminal Help
victor@victor-portatil ~ $ sudo lynis audit system
[ Lynis 2.1.1 ]
#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

Copyright 2007-2015 - CISOfy, https://cisofy.com
Enterprise support and plugins available via CISOfy
#####

[+] Initializing program
- Detecting OS... [ DONE ]

Program version: 2.1.1
Operating system: Linux
Operating system name: Debian
Operating system version: stretch/sid
Kernel version: 4.4.0
Hardware platform: x86_64
Hostname: victor-portatil
Auditor: [Unknown]
Profile: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins

- Checking profile file (/etc/lynis/default.prf)... [ WARNING ]
- Program update status... [ WARNING ]

Lynis update available En este ejercicio trabajamos con la herramienta Lynis
Current version : 211 Latest version : 266
Please update to the latest version for new features, bug fixes, tests
and baselines.
```

Este es un ejemplo de uno de los tests y comprobaciones que realiza:

The screenshot shows the Lynis tool interface running in a terminal window titled "victor@victor-portatil ~". The main pane displays a detailed report of system checks. Under the "System Tools" section, it lists various system components and their status: "binaries" (FOUND), "PAM modules" (Not Installed), and "File System Checks" (NOT ENCRYPTED). The "Software" section shows several packages as Not Installed. A note at the top states: "Note: plugins have more extensive tests, which may take a few minutes to complete". The bottom of the window has a message: "En este ejercicio trabaja en la ejecución de la herramienta Lynis". The status bar at the bottom shows the terminal command "ps aux" and the date/time "20:26".

```
victor@victor-portatil ~
File Edit View Search Terminal Help
[+] System Tools
- Scanning available tools...
- Checking system binaries...
[+] Plugins (phase 1) Ejercicio 2.
Note: plugins have more extensive tests, which may take a few minutes to complete
- Plugin: debian
[
[+] Debian Tests
- Checking for system binaries that are required by Debian Tests... [ FOUND ]
- Checking /bin... [ FOUND ]
- Checking /sbin... [ FOUND ]
- Checking /usr/bin... [ FOUND ]
- Checking /usr/sbin... [ FOUND ]
- Checking /usr/local/bin... [ FOUND ]
- Checking /usr/local/sbin... [ FOUND ]
- Authentication:
  - PAM (Pluggable Authentication Modules):
    - libpam-tmpdir [ Not Installed ]
    - libpam-usb [ Not Installed ]
- File System Checks:
  - DM-Crypt, Cryptsetup & Cryptmount:
    - Checking / on /dev/sda5 [ NOT ENCRYPTED ]
    - Checking /boot/efi on /dev/sdal [ NOT ENCRYPTED ]
    - Checking /media/victor/SE03-FEFD on /dev/mmcblk0p1 [ NOT ENCRYPTED ]
  - Encryptfs
    - Home for victor [ INSTALLED ]
    - Home for victor [ NO ]
    - Home for pruebauser [ NO ]
- Software:
  - apt-listbugs [ Not Installed ]
  - apt-listchanges [ Not Installed ]
  - checkrestart [ Not Installed ]
  - debsecan [ Not Installed ]
  - debsums [ Not Installed ]
  - fail2ban [ Not Installed ]
[ Press [ENTER] to continue, or [CTRL]+C to stop ]
]
Page 4 of 4 544 words, 3,376 characters Default Style Spanish (Spain)
Menu Pictures victor@victor... MemoriaPract... Practica_1_S2... Lynis Installati... victor@victor... "ps aux" explic... 28% (5:41) 20:26
```

A continuación se muestra el reporte final de la herramienta:

The screenshot shows the final report from the Lynis tool. It includes a "Warnings" section with a link to update the tool, and a "Suggestions" section with a list of actions to improve the system's security. The suggestions include installing specific packages like libpam-tmpdir and libpam-usb, configuring Encryptfs, and updating the system with the latest patches. The status bar at the bottom shows the terminal command "ps aux" and the date/time "20:27".

```
victor@victor-portatil ~
File Edit View Search Terminal Help
[ Lynis 2.1.1 Results ]-
Warning:
- Version of Lynis is very old and should be updated [test:NONE]
  https://ciscofy.com/controls/test:NONE/
- Found one or more vulnerable packages. [PKG5-7392]
  https://ciscofy.com/controls/PKG5-7392/
- Couldn't find 2 responsive nameservers [NETW-2705]
  https://ciscofy.com/controls/NETW-2705/
Suggestions:
- Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]
  https://your-domain.example.org/controls/CUST-0280/
- Install libpam_usb to enable multi-factor authentication for PAM sessions [CUST-0285]
  https://your-domain.example.org/controls/CUST-0285/
- As root run 'cryptsetup-migrate-home --user victor' to configure Encryptfs for user's home directory [CUST-0520]
  https://your-domain.example.org/controls/CUST-0520/
- As root run 'cryptsetup-migrate-home --user pruebauser' to configure Encryptfs for user's home directory [CUST-0520]
  https://your-domain.example.org/controls/CUST-0520/
- Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-0810]
  https://your-domain.example.org/controls/CUST-0810/
- Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CUST-0811]
  https://your-domain.example.org/controls/CUST-0811/
- Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of libraries and need restarting. [CUST-0830]
  https://your-domain.example.org/controls/CUST-0830/
- Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-0870]
  https://your-domain.example.org/controls/CUST-0870/
- Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]
  https://your-domain.example.org/controls/CUST-0875/
- Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
  https://ciscofy.com/controls/DEB-0880/
- Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
  https://ciscofy.com/controls/BOOT-5122/
- Determine runlevel and services at startup [BOOT-5180]
  https://ciscofy.com/controls/BOOT-5180/
- Configure password aging limits to enforce password changing on a regular base [AUTH-9286]
  https://ciscofy.com/controls/AUTH-9286/
- Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
  https://ciscofy.com/controls/AUTH-9328/
[ Press [ENTER] to continue, or [CTRL]+C to stop ]
]
Page 4 of 4 544 words, 3,376 characters Default Style Spanish (Spain)
Menu Pictures victor@victor... MemoriaPract... Practica_1_S2... Lynis Installati... victor@victor... "ps aux" explic... 29% (5:31) 20:27
```

```

victor@victor-portatil ~
File Edit View Search Terminal Help
- Harden compilers like restricting access to root user only [HRDN-7222]
  https://ciscofy.com/controls/HRDN-7222/
Follow-up:
-----
- Check the logfile for more details (less /var/log/lynis.log)
- Read security controls texts (https://ciscofy.com)
- Use --upload to upload data (Lynis Enterprise users)

Lynis security scan details:
Hardening index : 59 [#####
Tests performed : 197
Plugins enabled : 1

Quick overview:
- Firewall [X] - Malware scanner [V]
Lynis Modules:
- Heuristics Check [NA] - Security Audit [V]
- Compliance Tests [X] - Vulnerability Scan [V]
Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

Notice: Lynis update available
Current version : 211 Latest version : 266

Tip: Disable all tests which are not relevant or are too strict for the purpose of this particular machine. This will remove unwanted suggestions and also boost the hardening index. Each test should be properly analyzed to see if the related risks can be accepted, before disabling the test.

Lynis 2.1.1
Auditing, hardening and compliance for BSD, Linux, Mac OS and Unix
Copyright 2007-2015 - CISOfy, https://ciscofy.com
Enterprise support and plugins available via CISOfy
victor@victor-portatil ~ $ 
```

En la primera imagen se muestran algunos warnings y sugerencias acerca de los problemas que ha encontrado y recomendaciones de cómo solventarlos. Estos mismos podemos encontrarlos en el log localizado en la ruta `/var/log/lynis.log`. A lo largo de los tests utiliza colores (verde, amarillo, rojo) para indicar el grado de severidad de los mismos. En la última imagen podemos además observar en qué grado de fortalecimiento se encuentra nuestro sistema, un 59% en este caso.

Podemos comprobar si la herramienta detecta una vulnerabilidad en concreto en la ruta `/usr/share/lynis/include/tests_shells`. Con ayuda del comando `grep`, buscamos si la herramienta comprueba la vulnerabilidad *Shellshock*. La siguiente salida muestra cómo efectivamente realiza un test para comprobar esta vulnerabilidad.

```

victor@victor-portatil / $ cd /usr/share/lynis/include
victor@victor-portatil /usr/share/lynis/include $ ls
binaries      profiles      tests_insecure_services  tests_memory_processes  tests_snmp      tests_virtualization
consts       thumbnails     tests_databases        tests_kernel            tests_nameservices  tests_solaris    tests_webservers
data_upload   tests_accounting  tests_file_integrity  tests_kernel_hardening  tests_networking  tests_squid
functions    tests_authentication  tests_file_permissions  tests_ldap           tests_php          tests_ssh
helper_audit_dockerfile  tests_banners      tests_filesystems      tests_logging        tests_ports_packages  tests_storage
helper_update  tests_boot_services  tests_firewalls      tests_mac_frameworks  tests_printers_spools  tests_storage_nfs
osdetection   tests_containers    tests_hardening      tests_mail.messaging  tests_scheduling   tests_time
parameters   tests_crypto       tests_homedirs      tests_malware         tests_shells       tests_tooling
victor@victor-portatil /usr/share/lynis/include $ sudo cat tests_shells | grep shellshock
SHELLSHOCK TMP= mktemp /tmp/lynis-shellshock-test.XXXXXXXXXX' || exit 1
logtext "Result: Vulnerable to original shellshock (CVE-2014-6271)" "¿Qué pasos debemos dar para eliminarlas.
Display --indent 2 --text ". Shellshock: CVE-2014-6271 (original shellshock)" --result "WARNING" --color RED
logtext "Result: Not vulnerable to original shellshock (CVE-2014-6271)" "#Display --indent 4 --text ". CVE-2014-6271 (original shellshock)" --result "OK" --color GREEN
echo "#shellshock='() { echo vulnerable; }' bash -c shellshock 2>/dev/null | grep 'vulnerable'" > ${SHELLSHOCK TMP}
logtext "Test: Check for bug Exploit #3 - shellshock.net (no CVE)" "#Exploit# on shellshock.net (no CVE)" --color GREEN
logtext "Result: Vulnerable to CVE-2014-6271 (exploit #3 on shellshock.net)" "#Exploit# on shellshock.net (no CVE)" --color GREEN
Display --indent 2 --text ". Shellshock: Exploit #3 on shellshock.net (no CVE)" --result "WARNING" --color RED
logtext "Result: Not vulnerable to exploit #3 on shellshock.net (no CVE)" "#Exploit# on shellshock.net (no CVE)" --result "OK" --color GREEN
#Display --indent 4 --text ". Exploit#3 on shellshock.net (no CVE)" --result "OK" --color GREEN
victor@victor-portatil /usr/share/lynis/include $ 
```

En el archivo `tests_malware` de este mismo directorio podemos ver qué comprobaciones hace acerca del antivirus instalado en el sistema. La herramienta checkea la presencia o no de un antivirus por defecto. Si queremos cambiar esto para que detecte otro diferente, hay que modificar la configuración de uno de los perfiles de Lynis, que por defecto está el archivo `etc/lynis/default.prf`, creando un nuevo archivo de configuración `custom.prf` donde establecemos este cambio en la comprobación del antivirus.

Ejercicio 4.

Por último trabajamos con la herramienta rkhunter para comprobar rootkits y backdoors o puertas traseras. Tras instalarlo y actualizarlo utilizamos el comando `sudo rkhunter --check [--skip-keypress]` con esta última opción para ejecutar el diagnóstico, resultando en la siguiente salida:

```
victor@victor-portatil ~
File Edit View Search Terminal Help
Checking system startup files for malware
Performing group and account checks
  Checking for passwd file [ Found ]
  Checking for root equivalent (UID 0) accounts [ None found ]
  Checking for passwordless accounts [ None found ]
  Checking for passwd file changes [ None found ]
  Checking for group file changes [ None found ]
  Checking for root account shell history files [ None found ]
Performing system configuration file checks
  Checking for an SSH configuration file [ Found ]
  Checking if SSH root access is allowed [ Warning ] Indicar que rkhunter se ha ejecutado solamente para generar avisos e informar de problemas potenciales.
  Checking if SSH protocol v1 is allowed [ Not allowed ]
  Checking for a running system logging daemon [ Found ]
  Checking for a system logging configuration file [ Found ]
  Checking if syslog remote logging is allowed [ Not allowed ] Cuando ejecutamos la herramienta por primera vez en un sistema nuevo podemos ver muchos avisos, por esto es importante ejecutarla recién instalado el sistema. Si recibimos un correo con un aviso durante la operación normal del sistema [Warning] nos acercaremos a él y ver qué está pasando. Algunos avisos son benignos y se deben a actualizaciones [Found] de archivos, pero no debemos ignorarlos.
Performing filesystem checks
  Checking /dev for suspicious file types [ Warning ] En concreto, podemos encontrar avisos cuando la herramienta comprueba los archivos/directorios ocultos que se encuentran en /proc pero que son habituales en algunas distribuciones. Por ejemplo, en Debian tenemos
  Checking for hidden files and directories [ Warning ]
System checks summary
=====
File properties checks...
  Files checked: 144
  Suspect files: 1
Rootkit checks...
  Rootkits checked : 380
  Possible rootkits: 0
Applications checks...
  All checks skipped
The system checks took: 49 seconds
All results have been written to the log file: /var/log/rkhunter.log
One or more warnings have been found while checking the system. Please check the log file (/var/log/rkhunter.log)
victor@victor-portatil ~ $
```

Podemos ver de forma más detenida el resultado del análisis en el log localizado en la ruta `/var/log/rkhunter.log`. En la siguiente imagen de ese log podemos visualizar los avisos indicados:

```
victor@victor-portatil ~$ sudo cat rkhunter.log | grep Warning
[21:45:57] /usr/bin/lwp-request [Warning]
[21:45:57] Warning: The command '/usr/bin/lwp-request' has been replaced by a script: /usr/bin/lwp-request; a /usr/bin/perl -w script, ASCII text executable.
[21:46:33] Checking if SSH root access is allowed [Warning]
[21:46:33] Warning: The SSH and rkhunter configuration options should be the same.
[21:46:35] Checking /dev for suspicious file types [Warning]
[21:46:35] Warning: Suspicious file types found in /dev:[29]:/bin/netstat [Warning]
[21:46:35] Checking for hidden files and directories [Warning] The file properties have changed.
[21:46:35] Warning: Hidden directory found: /etc/.java [Warning]
[21:46:36] Warning: Hidden file found: /etc/.login.defs.swp: Vim swap file, version 7.4
victor@victor-portatil ~$
```

Estos son falsos positivos que podemos corregir modificando el archivo de configuración `etc/rkhunter.conf`.

Para solucionar el primero de *command ... has been replaced by a script*, primero comprobamos que el programa está bien, y a continuación para que no salte de nuevo el aviso en futuros diagnósticos, descomentamos la linea

`SCRIPTWHITELIST=/usr/bin/lwp-request`.

Además, para solucionar el aviso de directorios ocultos en archivos que sí son del sistema, descomentamos las siguientes líneas:

`ALLOWHIDDENDIR=/dev/.udev`

`ALLOWHIDDENDIR=/dev/.static`

`ALLOWHIDDENDIR=/dev/.initramfs`

```

victor@victor-portatil /etc
File Edit View Search Terminal Help
GNU nano 2.5.3          File: rkhunter.conf
SCRIPTWHITELIST=/bin/which
SCRIPTWHITELIST=/usr/bin/ldd
SCRIPTWHITELIST=/usr/bin/lwp-request
SCRIPTWHITELIST=/usr/sbin/adduser
#SCRIPTWHITELIST=/usr/sbin/prelink
#SCRIPTWHITELIST=/usr/sbin/unhide.rb
SCRIPTWHITELIST=/usr/bin/lwp-request.

#
# Allow the specified file to have the immutable attribute set.
# Además, para solucionar el aviso de directorios ocultos en archivos que sí son del sistema, descomentá las siguientes líneas:
#
# This option may be specified more than once, and may use wildcard characters.
#
# The default value is the null string ALLOWHIDDENDIR=/dev/udev
# ALLOWHIDDENDIR=/sbin/ifdown
#IMMUTWHITELIST=/sbin/ifdown          ALLOWHIDDENDIR=/dev/static
#
# If this option is set to '1', then the immutable-bit test is reversed. That
# is, the files are expected to have the bit set. A value of '0' means that the
# immutable-bit should not be set.
#
# The default value is '0'.
#IMMUTABLE_SET=0

#
# Allow the specified hidden directory to be whitelisted.
#
# This option may be specified more than once, and may use wildcard characters.
#
# The default value is the null string.
# ALLOWHIDDENDIR=/etc/.java
ALLOWHIDDENDIR=/etc/.git
ALLOWHIDDENDIR=/dev/.lxc

#
# Allow the specified hidden file to be whitelisted.
#
# This option may be specified more than once, and may use wildcard characters.

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   ^Y Prev Page   ^V First Line   M-W WhereIs Next   ^M Mark Text
^X Exit      ^R Read File   ^U Replace    ^U Uncut Text  ^T To Spell   ^G Go To Line   ^V Next Page   ^L Last Line   M-L To Bracket   M-C Copy Text

```

Icons at the bottom include: Menu, Pictures, MemoriaPractica1..., Practica_1_S2_18-1..., editar archivos po..., victor@victor-portatil..., 100%, 22:29.

Finalmente volvemos a ejecutar el diagnóstico de rkhunter y comprobamos que hemos solventado esos falsos positivos:

```

System checks summary
-----
File properties checks...
  Files checked: 144
  Suspect files: 0

Rootkit checks...
  Rootkits checked : 380
  Possible rootkits: 0

Applications checks...
  All checks skipped

The system checks took: 43 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

victor@victor-portatil /etc $ 

```

Icons at the bottom include: Menu, Pictures, MemoriaPractica1..., Practica_1_S2_18-1..., editar archivos po..., victor@victor-portatil..., 100%, 22:28.

El único aviso que aparece en el log es el de *The SSH and rkhunter configuration options should be the same*. Hemos eliminado los falsos positivos.