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.**

Autor[1]: **Matilde Cabrera González**

Ejercicio 1.

Resuelve las siguientes cuestiones:

(a) Utiliza esta herramienta para conocer que procesos/servicios[1] de nuestro sistema están accediendo a la red o tiene archivos abiertos. Indicar algunos de los servicios que tenéis activos, es decir, la actividad de la red, indicando que información da la herramienta.

```
mati@mati-VirtualBox:~$ sudo lsof -i
[sudo] contraseña para mati:
COMMAND     PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r   404 systemd-resolve   12u  IPv4  15753      0t0  UDP localhost:domain
systemd-r   404 systemd-resolve   13u  IPv4  15754      0t0  TCP localhost:domain (LISTEN)
avahi-dae   543           avahi   12u  IPv4  17793      0t0  UDP *:mdns
avahi-dae   543           avahi   13u  IPv6  17794      0t0  UDP *:mdns
avahi-dae   543           avahi   14u  IPv4  17795      0t0  UDP *:45418
avahi-dae   543           avahi   15u  IPv6  17796      0t0  UDP *:52532
sshd        685            root    3u  IPv4  21655      0t0  TCP *:ssh (LISTEN)
sshd        685            root    4u  IPv6  21657      0t0  TCP *:ssh (LISTEN)
dhclient   6392            root    6u  IPv4  54079      0t0  UDP *:bootpc
cupsd      6652            root    6u  IPv6  55752      0t0  TCP ip6-localhost:ipp (LISTEN)
cupsd      6652            root    7u  IPv4  55753      0t0  TCP localhost:ipp (LISTEN)
cups-brow  6654            root    7u  IPv4  55761      0t0  UDP *:ipp
```

Ahora establezco una conexión con www.google.es para ver la diferencia:

```
mati@mati-VirtualBox:~$ sudo lsof -i
COMMAND     PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r   404 systemd-resolve   12u  IPv4  15753      0t0  UDP localhost:domain
systemd-r   404 systemd-resolve   13u  IPv4  15754      0t0  TCP localhost:domain (LISTEN)
avahi-dae   543           avahi   12u  IPv4  17793      0t0  UDP *:mdns
avahi-dae   543           avahi   13u  IPv6  17794      0t0  UDP *:mdns
avahi-dae   543           avahi   14u  IPv4  17795      0t0  UDP *:45418
avahi-dae   543           avahi   15u  IPv6  17796      0t0  UDP *:52532
sshd        685            root    3u  IPv4  21655      0t0  TCP *:ssh (LISTEN)
sshd        685            root    4u  IPv6  21657      0t0  TCP *:ssh (LISTEN)
dhclient   6392            root    6u  IPv4  54079      0t0  UDP *:bootpc
cupsd      6652            root    6u  IPv6  55752      0t0  TCP ip6-localhost:ipp (LISTEN)
cupsd      6652            root    7u  IPv4  55753      0t0  TCP localhost:ipp (LISTEN)
cups-brow  6654            root    7u  IPv4  55761      0t0  UDP *:ipp
firefox    6762            mati   63u  IPv4  57540      0t0  TCP mati-VirtualBox:48158->192.219.106.212.static.jazztel.es:http (ESTABLISHED)
firefox    6762            mati   69u  IPv4  58981      0t0  TCP mati-VirtualBox:48188->ec2-52-42-79-121.us-west-2.compute.amazonaws.com:https (ESTABLISHED)
firefox    6762            mati   70u  IPv4  57988      0t0  TCP mati-VirtualBox:38516->ec2-34-208-68-174.us-west-2.compute.amazonaws.com:https (ESTABLISHED)
firefox    6762            mati   71u  IPv4  58982      0t0  TCP mati-VirtualBox:48190->ec2-52-42-79-121.us-west-2.compute.amazonaws.com:https (ESTABLISHED)
firefox    6762            mati   73u  IPv4  58986      0t0  TCP mati-VirtualBox:56956->93.184.220.29:http (ESTABLISHED)
firefox    6762            mati   75u  IPv4  58022      0t0  TCP mati-VirtualBox:56920->93.184.220.29:http (ESTABLISHED)
firefox    6762            mati   78u  IPv4  58355      0t0  TCP mati-VirtualBox:56870->mad08s06-in-f10.1e100.net:https (ESTABLISHED)
firefox    6762            mati  102u  IPv4  58972      0t0  TCP mati-VirtualBox:60406->mad08s04-in-f2.1e100.net:https (ESTABLISHED)
firefox    6762            mati  113u  IPv4  58362      0t0  TCP mati-VirtualBox:46030->arn02s06-in-f174.1e100.net:http (ESTABLISHED)
firefox    6762            mati  125u  IPv4  58368      0t0  TCP mati-VirtualBox:42788->arn02s06-in-f164.1e100.net:https (ESTABLISHED)
firefox    6762            mati  127u  IPv4  58376      0t0  TCP mati-VirtualBox:46036->arn02s06-in-f174.1e100.net:http (ESTABLISHED)
firefox    6762            mati  128u  IPv4  58377      0t0  TCP mati-VirtualBox:46038->arn02s06-in-f174.1e100.net:http (ESTABLISHED)
firefox    6762            mati  130u  IPv4  58775      0t0  TCP mati-VirtualBox:50886->mad08s06-in-f3.1e100.net:https (ESTABLISHED)
firefox    6762            mati  131u  IPv4  58381      0t0  TCP mati-VirtualBox:46044->arn02s06-in-f174.1e100.net:http (ESTABLISHED)
firefox    6762            mati  132u  IPv4  58420      0t0  TCP mati-VirtualBox:50034->arn02s06-in-f174.1e100.net:https (ESTABLISHED)
```

---

[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 ..."

(b) Qué órdenes y opciones darías para conocer que cuenta podría estar generando tráfico saliente malicioso de ssh y dónde se encuentra el archivo.

Hemos estudiado la herramienta lsof. Los principales usos que son de nuestro interés son:

- # lsof -p PID // lista los ficheros abiertos de un determinado pid
- # lsof /partición //lista los ficheros abiertos en un dispositivo o partición.
- # lsof -u alex // Listar ficheros abiertos de un determinado usuario.
- # lsof -i -nP // comprobar los servicios o puertos que están escuchando
- # lsof -u mati -a +D /tmp //lista archivos dentro del directorio tmp del usuario mati
- # lsof +D /etc //muestra los archivos abiertos y por quien en la ruta especificada etc.
- # lsof -c sshd // archivos y conexiones del proceso sshd
- # lsof -Ri :22 //actividad en tiempo real mostrando el pid.
- # lsof -i //actividad de la red en tiempo real

```
mati@mati-VirtualBox:~$ lsof -i :22
mati@mati-VirtualBox:~$ lsof -RPni :22
mati@mati-VirtualBox:~$ sudo lsof -RPni :22
[sudo] contraseña para mati:
COMMAND  PID PPID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd     685    1 root    3u  IPv4  21655      0t0  TCP *:22 (LISTEN)
sshd     685    1 root    4u  IPv6  21657      0t0  TCP *:22 (LISTEN)
mati@mati-VirtualBox:~$ sudo lsof -i :22
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd     685 root    3u  IPv4  21655      0t0  TCP *:ssh (LISTEN)
sshd     685 root    4u  IPv6  21657      0t0  TCP *:ssh (LISTEN)
mati@mati-VirtualBox:~$
```

Vamos a hacer una conexión ssh desde la máquina anfitrión a la máquina virtual donde hacemos nuestro trabajo, para ver la diferencia.

```
mati@mati-VirtualBox:~$ sudo lsof -Ri :22
COMMAND   PID PPID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd      737    1 root    3u  IPv4  21259      0t0  TCP *:ssh (LISTEN)
sshd      737    1 root    4u  IPv6  21261      0t0  TCP *:ssh (LISTEN)
sshd     1832  737 root    3u  IPv4  27763      0t0  TCP mati-VirtualBox:ssh->192.168.56.1:52723
 (ESTABLISHED)
sshd     1933 1832 mati    3u  IPv4  27763      0t0  TCP mati-VirtualBox:ssh->192.168.56.1:52723
 (ESTABLISHED)
mati@mati-VirtualBox:~$
```

(c) Muestra los archivos a los que está accediendo un proceso concreto y los que están en uso por un usuario.

Archivos por el proceso sshd

```
mati@mati-VirtualBox:~$ sudo lsof -c sshd
lsof: WARNING: 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    697 root  cwd    DIR                8,1     4096      2 /
sshd    697 root  rtd    DIR                8,1     4096      2 /
sshd    697 root  txt    REG                8,1   786856  14125 /usr/sbin/sshd
sshd    697 root  mem    REG                8,1    47568 400138 /lib/x86_64-linux-gnu/libnss_files-2.27.so
sshd    697 root  mem    REG                8,1    47576 400149 /lib/x86_64-linux-gnu/libnss_nis-2.27.so
sshd    697 root  mem    REG                8,1    39744 400134 /lib/x86_64-linux-gnu/libnss_compat-2.27.so
sshd    697 root  mem    REG                8,1    84032 400089 /lib/x86_64-linux-gnu/libgpg-error.so.0.22.0
sshd    697 root  mem    REG                8,1   101168 400187 /lib/x86_64-linux-gnu/libresolv-2.27.so
sshd    697 root  mem    REG                8,1    14256 400102 /lib/x86_64-linux-gnu/libkeyutils.so.1.5
sshd    697 root  mem    REG                8,1    43616   4690 /usr/lib/x86_64-linux-gnu/libkrb5support.so.0.1
sshd    697 root  mem    REG                8,1   199104   4682 /usr/lib/x86_64-linux-gnu/libk5crypto.so.3.1
sshd    697 root  mem    REG                8,1   144976 400181 /lib/x86_64-linux-gnu/libpthread-2.27.so
sshd    697 root  mem    REG                8,1  1155768 400087 /lib/x86_64-linux-gnu/libgcrypt.so.20.2.1
sshd    697 root  mem    REG                8,1   112672   4721 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1
sshd    697 root  mem    REG                8,1   153984 400108 /lib/x86_64-linux-gnu/liblzma.so.5.2.2
sshd    697 root  mem    REG                8,1    31680 400189 /lib/x86_64-linux-gnu/librt-2.27.so
sshd    697 root  mem    REG                8,1   464824 400170 /lib/x86_64-linux-gnu/libpcre.so.3.13.3
sshd    697 root  mem    REG                8,1    14560 400071 /lib/x86_64-linux-gnu/libdl-2.27.so
sshd    697 root  mem    REG                8,1    18712 400051 /lib/x86_64-linux-gnu/libcap-ng.so.0.0.0
sshd    697 root  mem    REG                8,1    97176 400132 /lib/x86_64-linux-gnu/libnsl-2.27.so
sshd    697 root  mem    REG                8,1  2030544 400048 /lib/x86_64-linux-gnu/libc-2.27.so
sshd    697 root  mem    REG                8,1    14248 400057 /lib/x86_64-linux-gnu/libcom_err.so.2.1
sshd    697 root  mem    REG                8,1   877056   4688 /usr/lib/x86_64-linux-gnu/libkrb5.so.3.3
sshd    697 root  mem    REG                8,1   305456   4517 /usr/lib/x86_64-linux-gnu/libgssapi_krb5.so.2.2
sshd    697 root  mem    REG                8,1    39208 400058 /lib/x86_64-linux-gnu/libcrypt-2.27.so
sshd    697 root  mem    REG                8,1   116960 400220 /lib/x86_64-linux-gnu/libz.so.1.2.11
sshd    697 root  mem    REG                8,1    10592 400213 /lib/x86_64-linux-gnu/libutil-2.27.so
sshd    697 root  mem    REG                8,1  2357760   4235 /usr/lib/x86_64-linux-gnu/libcrypto.so.1.0.0
sshd    697 root  mem    REG                8,1   536648 400202 /lib/x86_64-linux-gnu/libsystemd.so.0.21.0
sshd    697 root  mem    REG                8,1   154832 400193 /lib/x86_64-linux-gnu/libselinux.so.1
sshd    697 root  mem    REG                8,1    55848 400157 /lib/x86_64-linux-gnu/libpam.so.0.83.1
sshd    697 root  mem    REG                8,1   124848 400038 /lib/x86_64-linux-gnu/libaudit.so.1.0.0
sshd    697 root  mem    REG                8,1    39784 400218 /lib/x86_64-linux-gnu/libwrap.so.0.7.6
sshd    697 root  mem    REG                8,1   170960 400020 /lib/x86_64-linux-gnu/ld-2.27.so
sshd    697 root    0r   CHR                1,3      0t0      6 /dev/null
sshd    697 root    1u  unix 0xffff9ba5c570cc00      0t0  19894 type=STREAM
sshd    697 root    2u  unix 0xffff9ba5c570cc00      0t0  19894 type=STREAM
sshd    697 root    3u  IPv4              21627      0t0    TCP *:ssh (LISTEN)
sshd    697 root    4u  IPv6              21629      0t0    TCP *:ssh (LISTEN)
mati@mati-VirtualBox:~$
```

Los archivos correspondientes al usuario mati, nos sorprende su extensión.

```
mati@mati-VirtualBox:~$ sudo lsof -u mati
lsof: WARNING: 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
systemd    777 mati  cwd       DIR                8,1     4096          2 /
systemd    777 mati  rtd       DIR                8,1     4096          2 /
systemd    777 mati  txt       REG                8,1  1595792     399558 /lib/systemd/systemd
systemd    777 mati  mem       REG                8,1  1700792     400111 /lib/x86_64-linux-gnu/libm-2.27.so
systemd    777 mati  mem       REG                8,1   121016     400208 /lib/x86_64-linux-gnu/libudev.so.1.6.9
systemd    777 mati  mem       REG                8,1    84032     400089 /lib/x86_64-linux-gnu/libgpg-error.so.0.22.0
systemd    777 mati  mem       REG                8,1    43304     400100 /lib/x86_64-linux-gnu/libjson-c.so.3.0.1
systemd    777 mati  mem       REG                8,1    34872       4096 /usr/lib/x86_64-linux-gnu/libargon2.so.0
systemd    777 mati  mem       REG                8,1   432640     400070 /lib/x86_64-linux-gnu/libdevmapper.so.1.02.1
systemd    777 mati  mem       REG                8,1    18680     400036 /lib/x86_64-linux-gnu/libattr.so.1.1.0
systemd    777 mati  mem       REG                8,1    18712     400051 /lib/x86_64-linux-gnu/libcap-ng.so.0.0.0
systemd    777 mati  mem       REG                8,1    27112     400216 /lib/x86_64-linux-gnu/libuuid.so.1.3.0
systemd    777 mati  mem       REG                8,1    14560     400071 /lib/x86_64-linux-gnu/libdl-2.27.so
systemd    777 mati  mem       REG                8,1   464824     400170 /lib/x86_64-linux-gnu/libpcre.so.3.13.3
systemd    777 mati  mem       REG                8,1   144976     400181 /lib/x86_64-linux-gnu/libpthread-2.27.so
systemd    777 mati  mem       REG                8,1   112672       4721 /usr/lib/x86_64-linux-gnu/liblz4.so.1.7.1
systemd    777 mati  mem       REG                8,1   153984     400108 /lib/x86_64-linux-gnu/liblzma.so.5.2.2
systemd    777 mati  mem       REG                8,1   206872     400095 /lib/x86_64-linux-gnu/libidn.so.11.6.16
systemd    777 mati  mem       REG                8,1    27088       4647 /usr/lib/x86_64-linux-gnu/libip4tc.so.0.1.0
systemd    777 mati  mem       REG                8,1  1155768     400087 /lib/x86_64-linux-gnu/libgcrypt.so.20.2.1
systemd    777 mati  mem       REG                8,1    22768     400053 /lib/x86_64-linux-gnu/libcap.so.2.25
systemd    777 mati  mem       REG                8,1   310040     401984 /lib/x86_64-linux-gnu/libcryptsetup.so.12.2.0
systemd    777 mati  mem       REG                8,1    31232     400026 /lib/x86_64-linux-gnu/libacl.so.1.1.0
systemd    777 mati  mem       REG                8,1    64144     395212 /lib/x86_64-linux-gnu/libapparmor.so.1.4.2
systemd    777 mati  mem       REG                8,1    92208     400104 /lib/x86_64-linux-gnu/libkmod.so.2.3.2
systemd    777 mati  mem       REG                8,1   124848     400038 /lib/x86_64-linux-gnu/libaudit.so.1.0.0
systemd    777 mati  mem       REG                8,1    55848     400157 /lib/x86_64-linux-gnu/libpam.so.0.83.1
systemd    777 mati  mem       REG                8,1   311720     400040 /lib/x86_64-linux-gnu/libblkid.so.1.1.0
systemd    777 mati  mem       REG                8,1   340232     400117 /lib/x86_64-linux-gnu/libmount.so.1.1.0
systemd    777 mati  mem       REG                8,1   154832     400193 /lib/x86_64-linux-gnu/libselinux.so.1
systemd    777 mati  mem       REG                8,1   280776     400192 /lib/x86_64-linux-gnu/libseccomp.so.2.3.1
systemd    777 mati  mem       REG                8,1    31680     400189 /lib/x86_64-linux-gnu/librt-2.27.so
systemd    777 mati  mem       REG                8,1  2355440     399555 /lib/systemd/libsystemd-shared-237.so
systemd    777 mati  mem       REG                8,1  2030544     400048 /lib/x86_64-linux-gnu/libc-2.27.so
```

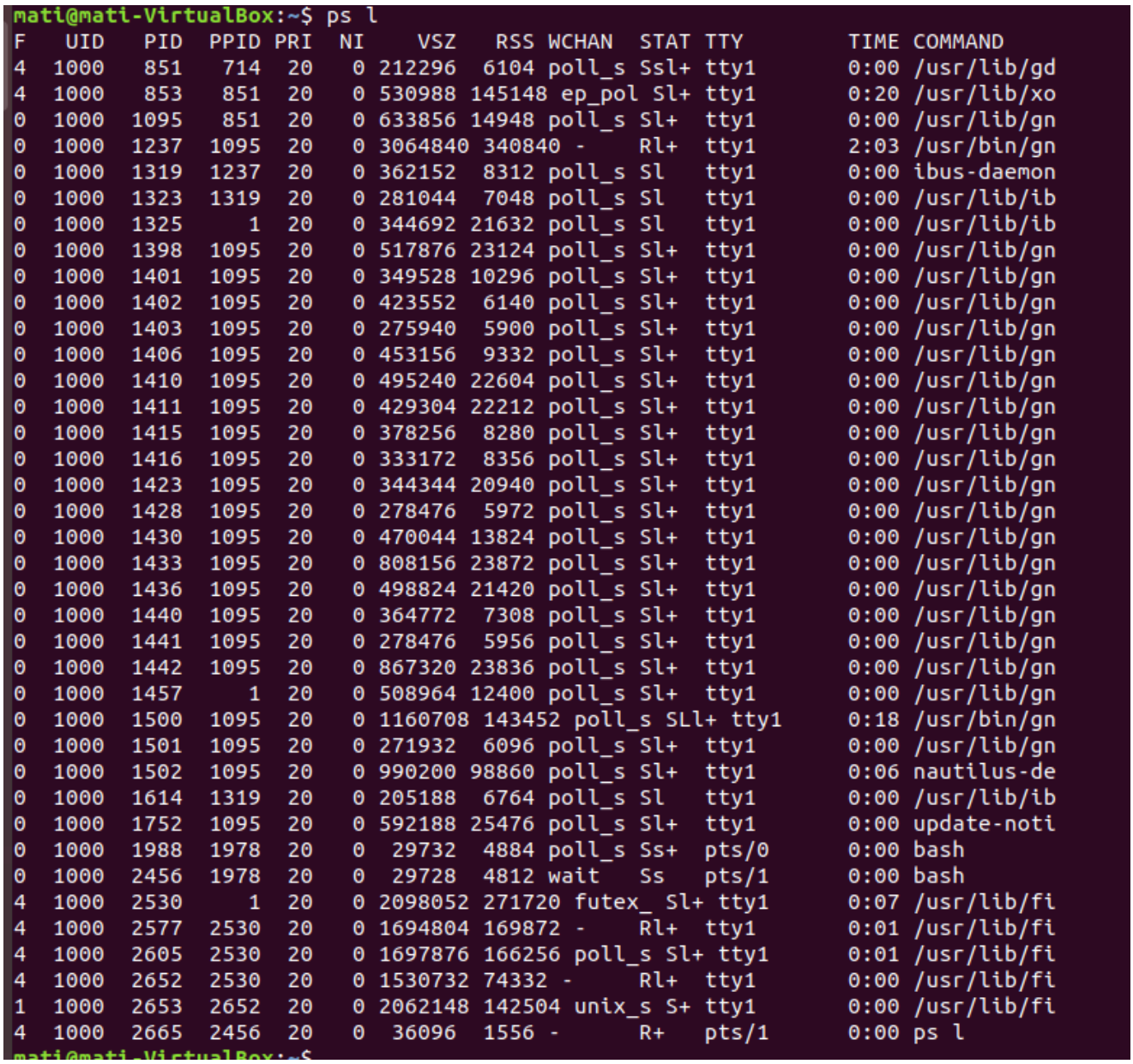
Ambas ordenes se pueden combinar de la siguiente forma “sudo lsof -c shhd -u mati”, nos daría los

archivos del proceso ssh correspondientes al usuario mati.

Ejercicio 2.

Ejecuta la orden `ps` para conocer los procesos de sistema habituales que vamos a encontrar en nuestro sistema y que por tanto no deberán considerarse sospechosos en nuestras labores de seguridad. Toma tres instantáneas de tu sistema en tres momentos diferentes y compáralas. ¿hay diferencias (utiliza `diff`)? ¿Cuál es la causa de las mismas? (indicarlo en términos de procesos en ejecución).

```
mati@mati-VirtualBox:~$ ps l
F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY        TIME COMMAND
4  1000   851   714  20   0 212296  6104 poll_s Ssl+ tty1       0:00 /usr/lib/gd
4  1000   853   851  20   0 428428 78568 ep_pol Sl+  tty1       0:07 /usr/lib/xo
0  1000  1095   851  20   0 633856 14928 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1237  1095  20   0 3013308 294880 poll_s Sl+ tty1      0:45 /usr/bin/gn
0  1000  1319  1237  20   0 361752  8048 poll_s Sl   tty1       0:00 ibus-daemon
0  1000  1323  1319  20   0 281044  7048 poll_s Sl   tty1       0:00 /usr/lib/ib
0  1000  1325     1  20   0 344692 21632 poll_s Sl   tty1       0:00 /usr/lib/ib
0  1000  1398  1095  20   0 517876 22880 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1401  1095  20   0 349528 10296 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1402  1095  20   0 423552  6140 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1403  1095  20   0 275940  5900 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1406  1095  20   0 453156  9332 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1410  1095  20   0 495240 22604 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1411  1095  20   0 429304 22212 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1415  1095  20   0 378256  8280 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1416  1095  20   0 333172  8356 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1423  1095  20   0 344344 20940 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1428  1095  20   0 278476  5972 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1430  1095  20   0 470044 13824 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1433  1095  20   0 808156 23604 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1436  1095  20   0 498824 21420 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1440  1095  20   0 364772  7308 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1441  1095  20   0 278476  5956 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1442  1095  20   0 793588 23440 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1457     1  20   0 508964 12400 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1500  1095  20   0 1133196 132724 poll_s SLl+ tty1     0:07 /usr/bin/gn
0  1000  1501  1095  20   0 271932  6096 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1502  1095  20   0 982812 84604 poll_s Sl+  tty1       0:04 nautilus-de
0  1000  1614  1319  20   0 205188  6764 poll_s Sl   tty1       0:00 /usr/lib/ib
0  1000  1752  1095  20   0 592188 25472 poll_s Sl+  tty1       0:00 update-noti
0  1000  1988  1978  20   0  29732  4884 wait   Ss   pts/0      0:00 bash
0  1000  2294  1988  20   0  36096  1456 -      R+   pts/0      0:00 ps l
mati@mati-VirtualBox:~$ ps l
F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY        TIME COMMAND
4  1000   851   714  20   0 212296  6104 poll_s Ssl+ tty1       0:00 /usr/lib/gd
4  1000   853   851  20   0 460308 112672 ep_pol Sl+ tty1       0:09 /usr/lib/xo
0  1000  1095   851  20   0 633856 14948 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1237  1095  20   0 3062700 338468 -     Rl+  tty1       1:00 /usr/bin/gn
0  1000  1319  1237  20   0 361752  8056 poll_s Sl   tty1       0:00 ibus-daemon
0  1000  1323  1319  20   0 281044  7048 poll_s Sl   tty1       0:00 /usr/lib/ib
0  1000  1325     1  20   0 344692 21632 poll_s Sl   tty1       0:00 /usr/lib/ib
0  1000  1398  1095  20   0 517876 23136 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1401  1095  20   0 349528 10296 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1402  1095  20   0 423552  6140 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1403  1095  20   0 275940  5900 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1406  1095  20   0 453156  9332 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1410  1095  20   0 495240 22604 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1411  1095  20   0 429304 22212 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1415  1095  20   0 378256  8280 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1416  1095  20   0 333172  8356 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1423  1095  20   0 344344 20940 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1428  1095  20   0 278476  5972 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1430  1095  20   0 470044 13824 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1433  1095  20   0 808156 23868 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1436  1095  20   0 498824 21420 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1440  1095  20   0 364772  7308 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1441  1095  20   0 278476  5956 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1442  1095  20   0 793588 23440 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1457     1  20   0 508964 12400 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1500  1095  20   0 1133196 132724 poll_s SLl+ tty1     0:07 /usr/bin/gn
0  1000  1501  1095  20   0 271932  6096 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1502  1095  20   0 990200 98860 poll_s Sl+  tty1       0:06 nautilus-de
0  1000  1614  1319  20   0 205188  6764 poll_s Sl   tty1       0:00 /usr/lib/ib
0  1000  1752  1095  20   0 592188 25472 poll_s Sl+  tty1       0:00 update-noti
0  1000  1988  1978  20   0  29732  4884 wait   Ss   pts/0      0:00 bash
4  1000  2296     1  20   0 2381244 248536 poll_s Sl+ tty1      0:12 /usr/lib/fi
4  1000  2334  2296  20   0 1927884 347840 -     Rl+  tty1       0:25 /usr/lib/fi
4  1000  2384  2296  20   0 1585276 84316 poll_s Sl+ tty1       0:00 /usr/lib/fi
4  1000  2436  1988  20   0  36096  1460 -      R+   pts/0      0:00 ps l
mati@mati-VirtualBox:~$
```



```
mati@mati-VirtualBox:~$ ps l
F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY        TIME COMMAND
4  1000   851   714  20   0 212296  6104 poll_s Ssl+ tty1       0:00 /usr/lib/gd
4  1000   853   851  20   0 530988 145148 ep_pol Sl+ tty1       0:20 /usr/lib/xo
0  1000  1095   851  20   0 633856 14948 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1237  1095  20   0 3064840 340840 -     Rl+  tty1       2:03 /usr/bin/gn
0  1000  1319  1237  20   0 362152  8312 poll_s Sl   tty1       0:00 ibus-daemon
0  1000  1323  1319  20   0 281044  7048 poll_s Sl   tty1       0:00 /usr/lib/ib
0  1000  1325     1  20   0 344692 21632 poll_s Sl   tty1       0:00 /usr/lib/ib
0  1000  1398  1095  20   0 517876 23124 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1401  1095  20   0 349528 10296 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1402  1095  20   0 423552  6140 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1403  1095  20   0 275940  5900 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1406  1095  20   0 453156  9332 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1410  1095  20   0 495240 22604 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1411  1095  20   0 429304 22212 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1415  1095  20   0 378256  8280 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1416  1095  20   0 333172  8356 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1423  1095  20   0 344344 20940 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1428  1095  20   0 278476  5972 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1430  1095  20   0 470044 13824 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1433  1095  20   0 808156 23872 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1436  1095  20   0 498824 21420 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1440  1095  20   0 364772  7308 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1441  1095  20   0 278476  5956 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1442  1095  20   0 867320 23836 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1457     1  20   0 508964 12400 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1500  1095  20   0 1160708 143452 poll_s SLl+ tty1     0:18 /usr/bin/gn
0  1000  1501  1095  20   0 271932  6096 poll_s Sl+  tty1       0:00 /usr/lib/gn
0  1000  1502  1095  20   0 990200 98860 poll_s Sl+  tty1       0:06 nautilus-de
0  1000  1614  1319  20   0 205188  6764 poll_s Sl   tty1       0:00 /usr/lib/ib
0  1000  1752  1095  20   0 592188 25476 poll_s Sl+  tty1       0:00 update-noti
0  1000  1988  1978  20   0  29732  4884 poll_s Ss+  pts/0      0:00 bash
0  1000  2456  1978  20   0  29728  4812 wait   Ss   pts/1      0:00 bash
4  1000  2530     1  20   0 2098052 271720 futex_ Sl+ tty1      0:07 /usr/lib/fi
4  1000  2577  2530  20   0 1694804 169872 -     Rl+  tty1       0:01 /usr/lib/fi
4  1000  2605  2530  20   0 1697876 166256 poll_s Sl+ tty1      0:01 /usr/lib/fi
4  1000  2652  2530  20   0 1530732 74332 -      Rl+  tty1       0:00 /usr/lib/fi
1  1000  2653  2652  20   0 2062148 142504 unix_s S+ tty1       0:00 /usr/lib/fi
4  1000  2665  2456  20   0  36096  1556 -      R+   pts/1      0:00 ps l
mati@mati-VirtualBox:~$
```

La primera vez que ejecutamos ps tenemos la máquina virtual recién levantada.
La segunda vez hemos entrado en internet y ponemos un video a reproducir.
La tercera vez hemos abierto varios archivos simultáneos.

Hemos elegido la orden ps l porque creemos que es la que más información nos aporta para nuestro ejercicio.

Hemos volcado los datos de los archivos en ficheros con la orden “ps l > archivo”

Para ver la diferencia entre archivos usamos la orden diff como se pide en el ejercicio, de la siguiente manera “diff -yi archivo1 archivo2”, de esta forma nos indica las diferencias en dos columnas, ignorando las diferencias entre mayúsculas y minúsculas. Lo hacemos así porque resaltan mas a la vista las diferencias, las cuales tienen un diferenciador “|”.
Diferencias entre archivo1 y archivo2

```
mati@mati-VirtualBox:~$ diff -yi archivo1 archivo2
F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY        F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY
4  1000   851   714  20   0 212296  6104 poll_s Ssl+ tty1       4  1000   851   714  20   0 212296  6104 poll_s Ssl+ tty1
4  1000   853   851  20   0 475128 113780 ep_pol Sl+ tty1     | 4  1000   853   851  20   0 478520 117204 ep_pol Sl+ tty1
0  1000  1095   851  20   0 642440 15272 poll_s Sl+  tty1     | 0  1000  1095   851  20   0 642312 15236 poll_s Sl+  tty1
0  1000  1237  1095  20   0 3072024 346040 poll_s Sl+ tty1    | 0  1000  1237  1095  20   0 3062808 339984 poll_s Sl+ tty1
0  1000  1319  1237  20   0 362152  8464 poll_s Sl   tty1       0  1000  1319  1237  20   0 362152  8464 poll_s Sl   tty1
0  1000  1323  1319  20   0 281044  7048 poll_s Sl   tty1       0  1000  1323  1319  20   0 281044  7048 poll_s Sl   tty1
0  1000  1325     1  20   0 344692 21632 poll_s Sl   tty1       0  1000  1325     1  20   0 344692 21632 poll_s Sl   tty1
0  1000  1398  1095  20   0 517876 23132 poll_s Sl+  tty1       0  1000  1398  1095  20   0 517876 23132 poll_s Sl+  tty1
0  1000  1401  1095  20   0 349528 10296 poll_s Sl+  tty1       0  1000  1401  1095  20   0 349528 10296 poll_s Sl+  tty1
0  1000  1402  1095  20   0 423552  6140 poll_s Sl+  tty1       0  1000  1402  1095  20   0 423552  6140 poll_s Sl+  tty1
0  1000  1403  1095  20   0 275940  5900 poll_s Sl+  tty1       0  1000  1403  1095  20   0 275940  5900 poll_s Sl+  tty1
0  1000  1406  1095  20   0 453156  9332 poll_s Sl+  tty1       0  1000  1406  1095  20   0 453156  9332 poll_s Sl+  tty1
0  1000  1410  1095  20   0 495240 22608 poll_s Sl+  tty1       0  1000  1410  1095  20   0 495240 22608 poll_s Sl+  tty1
0  1000  1411  1095  20   0 429304 22476 poll_s Sl+  tty1       0  1000  1411  1095  20   0 429304 22476 poll_s Sl+  tty1
0  1000  1415  1095  20   0 378256  8280 poll_s Sl+  tty1       0  1000  1415  1095  20   0 378256  8280 poll_s Sl+  tty1
0  1000  1416  1095  20   0 333172  8356 poll_s Sl+  tty1       0  1000  1416  1095  20   0 333172  8356 poll_s Sl+  tty1
0  1000  1423  1095  20   0 344344 20940 poll_s Sl+  tty1       0  1000  1423  1095  20   0 344344 20940 poll_s Sl+  tty1
0  1000  1428  1095  20   0 278476  5972 poll_s Sl+  tty1       0  1000  1428  1095  20   0 278476  5972 poll_s Sl+  tty1
0  1000  1430  1095  20   0 470044 13824 poll_s Sl+  tty1       0  1000  1430  1095  20   0 470044 13824 poll_s Sl+  tty1
0  1000  1433  1095  20   0 808156 23880 poll_s Sl+  tty1       0  1000  1433  1095  20   0 808156 23880 poll_s Sl+  tty1
0  1000  1436  1095  20   0 498824 21420 poll_s Sl+  tty1       0  1000  1436  1095  20   0 498824 21420 poll_s Sl+  tty1
0  1000  1440  1095  20   0 364772  7308 poll_s Sl+  tty1       0  1000  1440  1095  20   0 364772  7308 poll_s Sl+  tty1
0  1000  1441  1095  20   0 278476  5956 poll_s Sl+  tty1       0  1000  1441  1095  20   0 278476  5956 poll_s Sl+  tty1
0  1000  1442  1095  20   0 867320 23980 poll_s Sl+  tty1     | 0  1000  1442  1095  20   0 867320 23836 poll_s Sl+  tty1
0  1000  1457     1  20   0 508964 12400 poll_s Sl+  tty1       0  1000  1457     1  20   0 508964 12400 poll_s Sl+  tty1
0  1000  1500  1095  20   0 1160708 143452 poll_s SLl+ tty1      0  1000  1500  1095  20   0 1160708 143452 poll_s SLl+ tty1
0  1000  1501  1095  20   0 271932  6096 poll_s Sl+  tty1       0  1000  1501  1095  20   0 271932  6096 poll_s Sl+  tty1
0  1000  1502  1095  20   0 1064336 100596 poll_s Sl+ tty1    | 0  1000  1502  1095  20   0 1064336 100508 poll_s Sl+ tty1
0  1000  1614  1319  20   0 205188  6764 poll_s Sl   tty1       0  1000  1614  1319  20   0 205188  6764 poll_s Sl   tty1
0  1000  1752  1095  20   0 595776 27636 poll_s Sl+  tty1     | 0  1000  1752  1095  20   0 592188 25476 poll_s Sl+  tty1
0  1000  2456  1978  20   0  29728  4812 wait   Ss   pts/1      0  1000  2456  1978  20   0  29728  4812 wait   Ss   pts/1
0  1000  3321  2456  20   0  36096  1488 -      R+   pts/1    | 4  1000  3160     1  20   0 2052524 204408 poll_s Sl+ tty1
                                                             > 4  1000  3198  3160  20   0 1678376 141636 poll_s Sl+ tty1
                                                             > 4  1000  3255  3160  20   0 1585288 82368 poll_s Sl+ tty1
                                                             > 4  1000  3279  2456  20   0  36096  1508 -      R+   pts/1
mati@mati-VirtualBox:~$
```

Diferencias entre el archivo2 y archivo3:

```
mati@mati-VirtualBox:~$ diff -yi archivo2 archivo3
                                                             > mati@mati-VirtualBox:~$ ps l
F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY        F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY
4  1000   851   714  20   0 212296  6104 poll_s Ssl+ tty1     | 4  1000   851   714  20   0 212296  6104 poll_s Ssl+ tty1
4  1000   853   851  20   0 478520 117204 ep_pol Sl+ tty1     | 4  1000   853   851  20   0 530988 145148 ep_pol Sl+ tty1
0  1000  1095   851  20   0 642312 15236 poll_s Sl+  tty1     | 0  1000  1095   851  20   0 633856 14948 poll_s Sl+  tty1
0  1000  1237  1095  20   0 3062808 339984 poll_s Sl+ tty1    | 0  1000  1237  1095  20   0 3064840 340840 -    Rl+  tty1
0  1000  1319  1237  20   0 362152  8464 poll_s Sl   tty1     | 0  1000  1319  1237  20   0 362152  8312 poll_s Sl   tty1
0  1000  1323  1319  20   0 281044  7048 poll_s Sl   tty1     | 0  1000  1323  1319  20   0 281044  7048 poll_s Sl   tty1
0  1000  1325     1  20   0 344692 21632 poll_s Sl   tty1     | 0  1000  1325     1  20   0 344692 21632 poll_s Sl   tty1
0  1000  1398  1095  20   0 517876 23132 poll_s Sl+  tty1     | 0  1000  1398  1095  20   0 517876 23124 poll_s Sl+  tty1
0  1000  1401  1095  20   0 349528 10296 poll_s Sl+  tty1     | 0  1000  1401  1095  20   0 349528 10296 poll_s Sl+  tty1
0  1000  1402  1095  20   0 423552  6140 poll_s Sl+  tty1     | 0  1000  1402  1095  20   0 423552  6140 poll_s Sl+  tty1
0  1000  1403  1095  20   0 275940  5900 poll_s Sl+  tty1     | 0  1000  1403  1095  20   0 275940  5900 poll_s Sl+  tty1
0  1000  1406  1095  20   0 453156  9332 poll_s Sl+  tty1     | 0  1000  1406  1095  20   0 453156  9332 poll_s Sl+  tty1
0  1000  1410  1095  20   0 495240 22608 poll_s Sl+  tty1     | 0  1000  1410  1095  20   0 495240 22604 poll_s Sl+  tty1
0  1000  1411  1095  20   0 429304 22476 poll_s Sl+  tty1     | 0  1000  1411  1095  20   0 429304 22212 poll_s Sl+  tty1
0  1000  1415  1095  20   0 378256  8280 poll_s Sl+  tty1     | 0  1000  1415  1095  20   0 378256  8280 poll_s Sl+  tty1
0  1000  1416  1095  20   0 333172  8356 poll_s Sl+  tty1     | 0  1000  1416  1095  20   0 333172  8356 poll_s Sl+  tty1
0  1000  1423  1095  20   0 344344 20940 poll_s Sl+  tty1     | 0  1000  1423  1095  20   0 344344 20940 poll_s Sl+  tty1
0  1000  1428  1095  20   0 278476  5972 poll_s Sl+  tty1     | 0  1000  1428  1095  20   0 278476  5972 poll_s Sl+  tty1
0  1000  1430  1095  20   0 470044 13824 poll_s Sl+  tty1     | 0  1000  1430  1095  20   0 470044 13824 poll_s Sl+  tty1
0  1000  1433  1095  20   0 808156 23880 poll_s Sl+  tty1     | 0  1000  1433  1095  20   0 808156 23872 poll_s Sl+  tty1
0  1000  1436  1095  20   0 498824 21420 poll_s Sl+  tty1     | 0  1000  1436  1095  20   0 498824 21420 poll_s Sl+  tty1
0  1000  1440  1095  20   0 364772  7308 poll_s Sl+  tty1     | 0  1000  1440  1095  20   0 364772  7308 poll_s Sl+  tty1
0  1000  1441  1095  20   0 278476  5956 poll_s Sl+  tty1     | 0  1000  1441  1095  20   0 278476  5956 poll_s Sl+  tty1
0  1000  1442  1095  20   0 867320 23836 poll_s Sl+  tty1     | 0  1000  1442  1095  20   0 867320 23836 poll_s Sl+  tty1
0  1000  1457     1  20   0 508964 12400 poll_s Sl+  tty1     | 0  1000  1457     1  20   0 508964 12400 poll_s Sl+  tty1
0  1000  1500  1095  20   0 1160708 143452 poll_s SLl+ tty1   | 0  1000  1500  1095  20   0 1160708 143452 poll_s SLl+ tty1
0  1000  1501  1095  20   0 271932  6096 poll_s Sl+  tty1     | 0  1000  1501  1095  20   0 271932  6096 poll_s Sl+  tty1
0  1000  1502  1095  20   0 1064336 100508 poll_s Sl+ tty1    | 0  1000  1502  1095  20   0 990200 98860 poll_s Sl+  tty1
0  1000  1614  1319  20   0 205188  6764 poll_s Sl   tty1     | 0  1000  1614  1319  20   0 205188  6764 poll_s Sl   tty1
0  1000  1752  1095  20   0 592188 25476 poll_s Sl+  tty1     | 0  1000  1752  1095  20   0 592188 25476 poll_s Sl+  tty1
                                                             > 0  1000  1988  1978  20   0  29732  4884 poll_s Ss+  pts/0
0  1000  2456  1978  20   0  29728  4812 wait   Ss   pts/1      0  1000  2456  1978  20   0  29728  4812 wait   Ss   pts/1
4  1000  3160     1  20   0 2052524 204408 poll_s Sl+ tty1    | 4  1000  2530     1  20   0 2098052 271720 futex_ Sl+ tty1
4  1000  3198  3160  20   0 1678376 141636 poll_s Sl+ tty1    | 4  1000  2577  2530  20   0 1694804 169872 -    Rl+  tty1
4  1000  3255  3160  20   0 1585288 82368 poll_s Sl+ tty1     | 4  1000  2605  2530  20   0 1697876 166256 poll_s Sl+ tty1
4  1000  3279  2456  20   0  36096  1508 -      R+   pts/1    | 4  1000  2652  2530  20   0 1530732 74332 -     Rl+  tty1
                                                             > 1  1000  2653  2652  20   0 2062148 142504 unix_s S+ tty1
                                                             > 4  1000  2665  2456  20   0  36096  1556 -      R+   pts/1
                                                             >
```

Diferencias entre archivo1 y archivo3:

```
mati@mati-VirtualBox:~$ diff -yi archivo1 archivo3
                                                              > mati@mati-VirtualBox:~$ ps l
F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY        F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY
4  1000   851   714  20   0 212296  6104 poll_s Ssl+ tty1     | 4  1000   851   714  20   0 212296  6104 poll_s Ssl+ tty1
4  1000   853   851  20   0 475128 113780 ep_pol Sl+ tty1     | 4  1000   853   851  20   0 530988 145148 ep_pol Sl+ tty1
0  1000  1095   851  20   0 642440 15272 poll_s Sl+  tty1     | 0  1000  1095   851  20   0 633856 14948 poll_s Sl+  tty1
0  1000  1237  1095  20   0 3072024 346040 poll_s Sl+ tty1    | 0  1000  1237  1095  20   0 3064840 340840 -    Rl+  tty1
0  1000  1319  1237  20   0 362152  8464 poll_s Sl   tty1     | 0  1000  1319  1237  20   0 362152  8312 poll_s Sl   tty1
0  1000  1323  1319  20   0 281044  7048 poll_s Sl   tty1     | 0  1000  1323  1319  20   0 281044  7048 poll_s Sl   tty1
0  1000  1325     1  20   0 344692 21632 poll_s Sl   tty1     | 0  1000  1325     1  20   0 344692 21632 poll_s Sl   tty1
0  1000  1398  1095  20   0 517876 23132 poll_s Sl+  tty1     | 0  1000  1398  1095  20   0 517876 23124 poll_s Sl+  tty1
0  1000  1401  1095  20   0 349528 10296 poll_s Sl+  tty1     | 0  1000  1401  1095  20   0 349528 10296 poll_s Sl+  tty1
0  1000  1402  1095  20   0 423552  6140 poll_s Sl+  tty1     | 0  1000  1402  1095  20   0 423552  6140 poll_s Sl+  tty1
0  1000  1403  1095  20   0 275940  5900 poll_s Sl+  tty1     | 0  1000  1403  1095  20   0 275940  5900 poll_s Sl+  tty1
0  1000  1406  1095  20   0 453156  9332 poll_s Sl+  tty1     | 0  1000  1406  1095  20   0 453156  9332 poll_s Sl+  tty1
0  1000  1410  1095  20   0 495240 22608 poll_s Sl+  tty1     | 0  1000  1410  1095  20   0 495240 22604 poll_s Sl+  tty1
0  1000  1411  1095  20   0 429304 22476 poll_s Sl+  tty1     | 0  1000  1411  1095  20   0 429304 22212 poll_s Sl+  tty1
0  1000  1415  1095  20   0 378256  8280 poll_s Sl+  tty1     | 0  1000  1415  1095  20   0 378256  8280 poll_s Sl+  tty1
0  1000  1416  1095  20   0 333172  8356 poll_s Sl+  tty1     | 0  1000  1416  1095  20   0 333172  8356 poll_s Sl+  tty1
0  1000  1423  1095  20   0 344344 20940 poll_s Sl+  tty1     | 0  1000  1423  1095  20   0 344344 20940 poll_s Sl+  tty1
0  1000  1428  1095  20   0 278476  5972 poll_s Sl+  tty1     | 0  1000  1428  1095  20   0 278476  5972 poll_s Sl+  tty1
0  1000  1430  1095  20   0 470044 13824 poll_s Sl+  tty1     | 0  1000  1430  1095  20   0 470044 13824 poll_s Sl+  tty1
0  1000  1433  1095  20   0 808156 23880 poll_s Sl+  tty1     | 0  1000  1433  1095  20   0 808156 23872 poll_s Sl+  tty1
0  1000  1436  1095  20   0 498824 21420 poll_s Sl+  tty1     | 0  1000  1436  1095  20   0 498824 21420 poll_s Sl+  tty1
0  1000  1440  1095  20   0 364772  7308 poll_s Sl+  tty1     | 0  1000  1440  1095  20   0 364772  7308 poll_s Sl+  tty1
0  1000  1441  1095  20   0 278476  5956 poll_s Sl+  tty1     | 0  1000  1441  1095  20   0 278476  5956 poll_s Sl+  tty1
0  1000  1442  1095  20   0 867320 23980 poll_s Sl+  tty1     | 0  1000  1442  1095  20   0 867320 23836 poll_s Sl+  tty1
0  1000  1457     1  20   0 508964 12400 poll_s Sl+  tty1     | 0  1000  1457     1  20   0 508964 12400 poll_s Sl+  tty1
0  1000  1500  1095  20   0 1160708 143452 poll_s SLl+ tty1   | 0  1000  1500  1095  20   0 1160708 143452 poll_s SLl+ tty1
0  1000  1501  1095  20   0 271932  6096 poll_s Sl+  tty1     | 0  1000  1501  1095  20   0 271932  6096 poll_s Sl+  tty1
0  1000  1502  1095  20   0 1064336 100596 poll_s Sl+ tty1    | 0  1000  1502  1095  20   0 990200 98860 poll_s Sl+  tty1
0  1000  1614  1319  20   0 205188  6764 poll_s Sl   tty1     | 0  1000  1614  1319  20   0 205188  6764 poll_s Sl   tty1
0  1000  1752  1095  20   0 595776 27636 poll_s Sl+  tty1     | 0  1000  1752  1095  20   0 592188 25476 poll_s Sl+  tty1
                                                              > 0  1000  1988  1978  20   0  29732  4884 poll_s Ss+  pts/0
0  1000  2456  1978  20   0  29728  4812 wait   Ss   pts/1      0  1000  2456  1978  20   0  29728  4812 wait   Ss   pts/1
0  1000  3321  2456  20   0  36096  1488 -      R+   pts/1     | 4  1000  2530     1  20   0 2098052 271720 futex_ Sl+ tty1
                                                              > 4  1000  2577  2530  20   0 1694804 169872 -    Rl+  tty1
                                                              > 4  1000  2605  2530  20   0 1697876 166256 poll_s Sl+ tty1
                                                              > 4  1000  2652  2530  20   0 1530732 74332 -     Rl+  tty1
                                                              > 1  1000  2653  2652  20   0 2062148 142504 unix_s S+ tty1
                                                              > 4  1000  2665  2456  20   0  36096  1556 -      R+   pts/1
                                                              >
```

Estas diferencias son debido al RSS, esto es la memoria física del proceso en Kb. También hay diferencias por procesos que antes no había.

Ejercicio 3.

Instalar y ejecutar la citada herramienta en vuestro sistema de cara a:

```
mati@mati-VirtualBox:~$ sudo apt-get install lynis
[sudo] contraseña para mati:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  menu
Paquetes sugeridos:
  apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n gksu | kde-runtime
  | ktsuss
Se instalarán los siguientes paquetes NUEVOS:
  lynis menu
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 17 no actualizados.
Se necesita descargar 532 kB de archivos.
Se utilizarán 2.858 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu bionic/universe amd64 lynis all 2.6.2-1 [183 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 menu amd64 2.1.47ubuntu2.1 [349 kB]
Descargados 532 kB en 1s (662 kB/s)
Seleccionando el paquete lynis previamente no seleccionado.
(Leyendo la base de datos ... 159012 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../archives/lynis_2.6.2-1_all.deb ...
Desempaquetando lynis (2.6.2-1) ...
Seleccionando el paquete menu previamente no seleccionado.
Preparando para desempaquetar .../menu_2.1.47ubuntu2.1_amd64.deb ...
Desempaquetando menu (2.1.47ubuntu2.1) ...
Configurando lynis (2.6.2-1) ...
Procesando disparadores para mime-support (3.60ubuntu1) ...
Procesando disparadores para desktop-file-utils (0.23-1ubuntu3.18.04.1) ...
Procesando disparadores para install-info (6.5.0.dfsg.1-2) ...
Configurando menu (2.1.47ubuntu2.1) ...
Procesando disparadores para man-db (2.8.3-2) ...
Procesando disparadores para gnome-menus (3.13.3-11ubuntu1.1) ...
Procesando disparadores para menu (2.1.47ubuntu2.1) ...
mati@mati-VirtualBox:~$
```

a) Mostrar que vulnerabilidades hay en vuestro sistema, asignarle un grado de severidad (en una escala: alta, media, o baja) e indicar qué pasos debemos dar para eliminarlas.

Ejecutamos

```
mati@mati-VirtualBox:~$ sudo lynis audit system --auditor mati

[ Lynis 2.6.2 ]

################################################################################
  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.

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
```

Conforme se ejecuta la auditoria te dice si algo va mal en el sistema y lo casifica por nombre y colores, en rojo lo critico, en amarillo las sugerencias y en verde lo que está bien.

Miramos los archivos “/var/log/lynis-report.dat” y “/var/log/lynis.log”, son demasiado extensos y es un imposible encontrar algo. Buscamos las vulnerabilidades con grep.

```
mati@mati-VirtualBox:~$ sudo cat /var/log/lynis-report.dat | grep suggest
suggestion[]=LYNIS|Version of Lynis outdated, consider upgrading to the latest version|-|-|
suggestion[]=CUST-0280|Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions|-|-|
suggestion[]=CUST-0285|Install libpam-usb to enable multi-factor authentication for PAM sessions|-|-|
suggestion[]=CUST-0810|Install apt-listbugs to display a list of critical bugs prior to each APT installation.|-|-|
suggestion[]=CUST-0811|Install apt-listchanges to display any significant changes prior to any upgrade via APT.|-|-|
suggestion[]=CUST-0830|Install debian-goodies so that you can run checkrestart after upgrades to determine which services
are using old versions of libraries and need restarting.|-|-|
suggestion[]=CUST-0831|Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrade
s to determine which daemons are using old versions of libraries and need restarting.|-|-|
suggestion[]=CUST-0870|Install debsecan to generate lists of vulnerabilities which affect this installation.|-|-|
suggestion[]=CUST-0875|Install debsums for the verification of installed package files against MD5 checksums.|-|-|
suggestion[]=DEB-0880|Install fail2ban to automatically ban hosts that commit multiple authentication errors.|-|-|
suggestion[]=BOOT-5122|Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user
mode without password)|-|-|
suggestion[]=AUTH-9262|Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc|-|-|
```

En la imagen anterior nos aconseja que instalemos algunas herramientas, suponemos que mejoramos la seguridad de nuestro so si las instalamos. Le damos a estas vulnerabilidades un grado bajo.

```
suggestion[]=AUTH-9286|Configure minimum password age in /etc/login.defs|-|-|
suggestion[]=AUTH-9286|Configure maximum password age in /etc/login.defs|-|-|
suggestion[]=AUTH-9308|Set password for single user mode to minimize physical access attack surface|-|-|
suggestion[]=AUTH-9328|Default umask in /etc/login.defs could be more strict like 027|-|-|
suggestion[]=FILE-6310|To decrease the impact of a full /home file system, place /home on a separated partition|-|-|
suggestion[]=FILE-6310|To decrease the impact of a full /tmp file system, place /tmp on a separated partition|-|-|
suggestion[]=FILE-6310|To decrease the impact of a full /var file system, place /var on a separated partition|-|-|
suggestion[]=STRG-1840|Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft|-|-|
suggestion[]=NAME-4028|Check DNS configuration for the dns domain name|-|-|
suggestion[]=PKGS-7346|Purge old/removed packages (3 found) with aptitude purge or dpkg --purge command. This will cleanup
 old configuration files, cron jobs and startup scripts.|-|-|
suggestion[]=PKGS-7370|Install debsums utility for the verification of packages with known good database.|-|-|
suggestion[]=PKGS-7394|Install package apt-show-versions for patch management purposes|-|-|
suggestion[]=NETW-2705|Check your resolv.conf file and fill in a backup nameserver if possible|-|-|
suggestion[]=NETW-3032|Consider running ARP monitoring software (arpwatch,arpon)|-|-|
suggestion[]=PRNT-2307|Access to CUPS configuration could be more strict.|-|-|
```

En la imagen anterior nos aconseja que separemos por particiones el home, tmp y var, denotaríamos esta vulnerabilidad como media, es algo importante pero no esencial.

```
suggestion[]=SSH-7408|Consider hardening SSH configuration|AllowTcpForwarding (YES --> NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|ClientAliveCountMax (3 --> 2)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|Compression (YES --> (DELAYED|NO))|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|LogLevel (INFO --> VERBOSE)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|MaxAuthTries (6 --> 2)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|MaxSessions (10 --> 2)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|PermitRootLogin (WITHOUT-PASSWORD --> NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|Port (22 --> )|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|TCPKeepAlive (YES --> NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|X11Forwarding (YES --> NO)|-|
suggestion[]=SSH-7408|Consider hardening SSH configuration|AllowAgentForwarding (YES --> NO)|-|
```

Nos aconseja que configuremos ssh, por defecto cualquier usuario se puede conectar por ssh sabiendo tu contraseña, ademas no tenemos password por defecto, nos dice que le pongamos un máximo de sesiones por ssh, en definitiva protejamos lo mejor posible las conexiones ssh. Es una vulnerabilidad alta, las repercusiones pueden ser desastrosas si alguien se conecta por ssh con malas intenciones.

```
suggestion[]=LOGG-2190|Check what deleted files are still in use and why.|-|-|
suggestion[]=BANN-7126|Add a legal banner to /etc/issue, to warn unauthorized users|-|-|
suggestion[]=BANN-7130|Add legal banner to /etc/issue.net, to warn unauthorized users|-|-|
suggestion[]=ACCT-9622|Enable process accounting|-|-|
suggestion[]=ACCT-9626|Enable sysstat to collect accounting (no results)|-|-|
suggestion[]=ACCT-9628|Enable auditd to collect audit information|-|-|
suggestion[]=FINT-4350|Install a file integrity tool to monitor changes to critical and sensitive files|-|-|
suggestion[]=TOOL-5002|Determine if automation tools are present for system management|-|-|
suggestion[]=KRNL-6000|One or more sysctl values differ from the scan profile and could be tweaked||Change sysctl value or
 disable test (skip-test=KRNL-6000:<sysctl-key>)|
suggestion[]=HRDN-7222|Harden compilers like restricting access to root user only|-|-|
suggestion[]=HRDN-7230|Harden the system by installing at least one malware scanner, to perform periodic file system scans
|-|Install a tool like rkhunter, chkrootkit, OSSEC|
```

b) En clase de teoría, vimos la vulnerabilidad *Shellshock* (CVE-2014-6271), indicar si la herramienta citada comprueba dicha vulnerabilidad y explicar cómo lo hace (esto nos servirá para conocer cómo podríamos desarrollar nuestro propio test). Consejo, revisar el contenido del archivo de la herramienta *include/tests_shells*.

```
mati@mati-VirtualBox:~$ sudo cat /var/log/lynis.log | grep SHLL
2018-10-09 19:53:29 Skipped test SHLL-6202 (Check console TTYs)
2018-10-09 19:53:29 Performing test ID SHLL-6211 (Checking available and valid shells)
2018-10-09 19:53:30 Performing test ID SHLL-6220 (Checking available and valid shells)
2018-10-09 19:53:30 Performing test ID SHLL-6230 (Perform umask check for shell configurations)
mati@mati-VirtualBox:~$
```

“sudo cat /var/log/lynis.log”

```
2018-10-09 19:53:29 Skipped test SHLL-6202 (Check console TTYs)
2018-10-09 19:53:29 Reason to skip: Incorrect guest OS (FreeBSD only)
2018-10-09 19:53:29 ===-------------------------------------------------------------===
2018-10-09 19:53:29 Performing test ID SHLL-6211 (Checking available and valid shells)
2018-10-09 19:53:29 Test: Searching for /etc/shells
2018-10-09 19:53:29 Result: Found /etc/shells file
2018-10-09 19:53:29 Test: Reading available shells from /etc/shells
2018-10-09 19:53:29 Found installed shell: /bin/sh
2018-10-09 19:53:29 Found installed shell: /bin/bash
2018-10-09 19:53:29 Found installed shell: /bin/rbash
2018-10-09 19:53:29 Found installed shell: /bin/dash
2018-10-09 19:53:29 ===-------------------------------------------------------------===
2018-10-09 19:53:30 Performing test ID SHLL-6220 (Checking available and valid shells)
2018-10-09 19:53:30 Test: Search for session timeout tools or settings in shell
2018-10-09 19:53:30 IsRunning: process 'timeoutd' not found
2018-10-09 19:53:30 IsRunning: process 'autolog' not found
2018-10-09 19:53:30 Result: could not find TMOUT setting in /etc/profile
2018-10-09 19:53:30 Result: could not find export, readonly or typeset -r in /etc/profile
2018-10-09 19:53:30 Result: could not find TMOUT setting in /etc/profile.d/*.sh
2018-10-09 19:53:30 Result: could not find export, readonly or typeset -r in /etc/profile
2018-10-09 19:53:30 Hardening: assigned partial number of hardening points (1 of 3). Currently having 28
points (out of 65)
2018-10-09 19:53:30 ===-------------------------------------------------------------===
2018-10-09 19:53:30 Performing test ID SHLL-6230 (Perform umask check for shell configurations)
2018-10-09 19:53:30 Result: file /etc/bashrc not found
2018-10-09 19:53:30 Result: file /etc/bash.bashrc exists
2018-10-09 19:53:30 Result: did not find umask configured in /etc/bash.bashrc
2018-10-09 19:53:30 Result: file /etc/csh.cshrc not found
2018-10-09 19:53:30 Result: file /etc/profile exists
2018-10-09 19:53:30 Result: did not find umask configured in /etc/profile
2018-10-09 19:53:30 Checking permissions of /usr/share/lynis/include/tests_filesystems
2018-10-09 19:53:30 File permissions are OK
2018-10-09 19:53:30 ===-------------------------------------------------------------===
mati@mati-VirtualBox:~$ sudo cat /usr/share/lynis/include/tests_s
tests_scheduling        tests_snmp              tests_ssh               tests_storage_nfs
tests_shells            tests_squid             tests_storage           tests_system_integrity
mati@mati-VirtualBox:~$ sudo cat /usr/share/lynis/include/tests_shells
#!/bin/sh

#################################################################################
#
#   Lynis
# -----------------
#
# Copyright 2007-2013, Michael Boelen
# Copyright 2007-2018, CISOfy
#
# Website  : https://cisofy.com
# Blog     : http://linux-audit.com
# GitHub   : https://github.com/CISOfy/lynis
#
# 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 LICENSE file for usage of this software.
#
#################################################################################
#
# Shells
#
#################################################################################
#
    IDLE_TIMEOUT=0
    InsertSection "Shells"
#
#################################################################################
#
    # bash
    # Files (interactive login shells):     /etc/profile $HOME/.bash_profile
    #                                       $HOME/.bash_login $HOME/.profile
    # Files (interactive non-login shells): $HOME/.bash_rc

    # csh/tcsh
    # Files: /etc/csh.cshrc /etc/csh.login
    # zsh
    # Files: /etc/zshenv /etc/zsh/zshenv $HOME/.zshenv /etc/zprofile
    #        /etc/zsh/zprofile $HOME/.zprofile /etc/zshrc /etc/zsh/zshrc
    #        $ZDOTDIR/.zshrc /etc/zlogin /etc/zsh/zlogin

    SHELL_LOGIN_FILES="${ROOTDIR}etc/csh.cshrc ${ROOTDIR}etc/csh.login ${ROOTDIR}etc/zshenv ${ROOTDIR}etc/zsh/zshenv
```

c) Suponiendo que nuestro sistema tiene un antivirus, Avx, no contemplado por la herramienta.

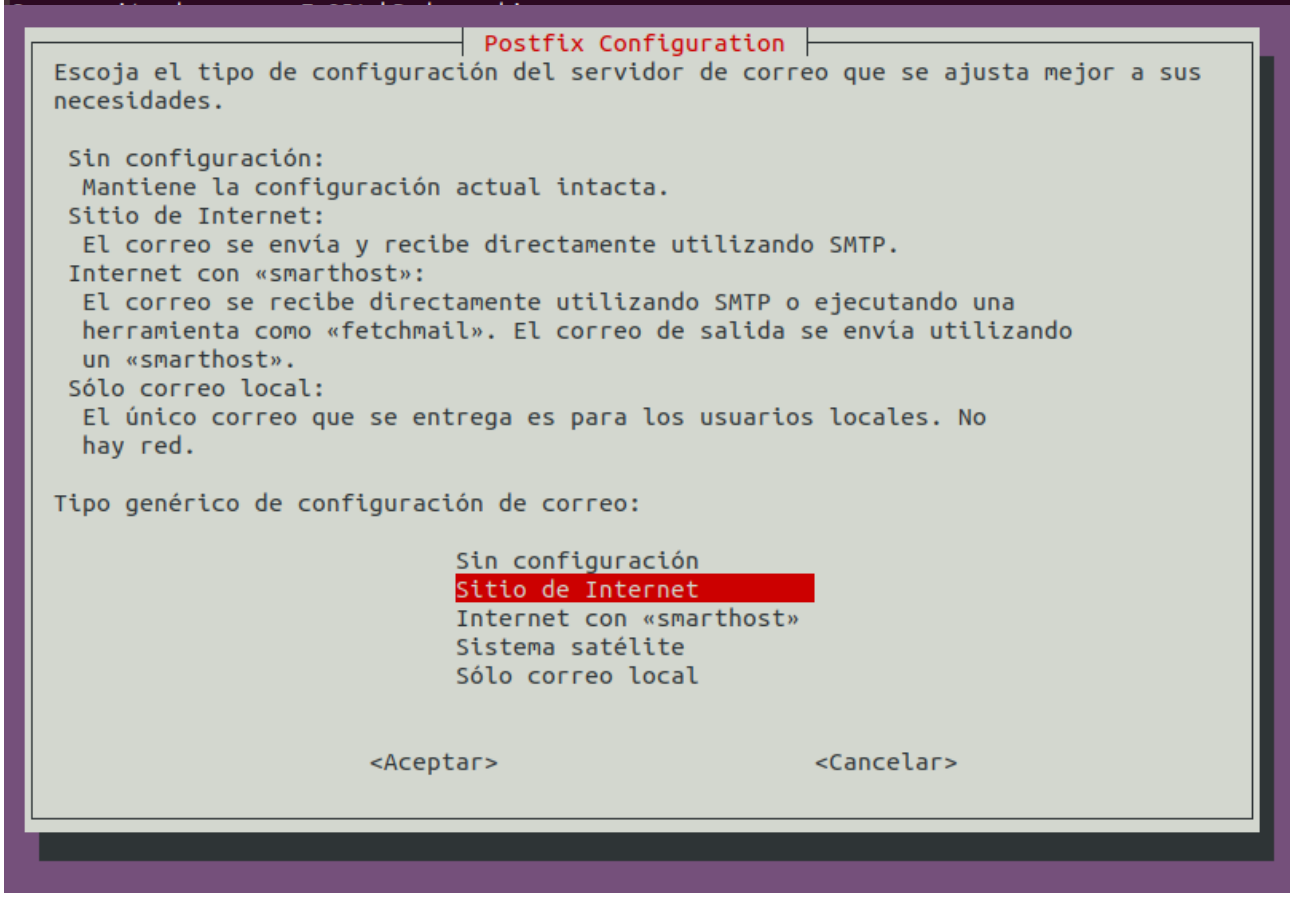
Indicar qué debemos hacer para que la herramienta lo detecte y no muestre en el informe final que no tenemos solución antivirus).

```
mati@mati-VirtualBox:~$ sudo cat /var/log/lynis.log | grep anti
2018-10-09 21:14:19 Performing test ID MALW-3280 (Check if anti-virus tool is installed)
2018-10-09 21:14:19 Test: checking process TmccMac to test for Trend Micro anti-virus (macOS)
2018-10-09 21:14:19 Result: no commercial anti-virus tools found
mati@mati-VirtualBox:~$
```

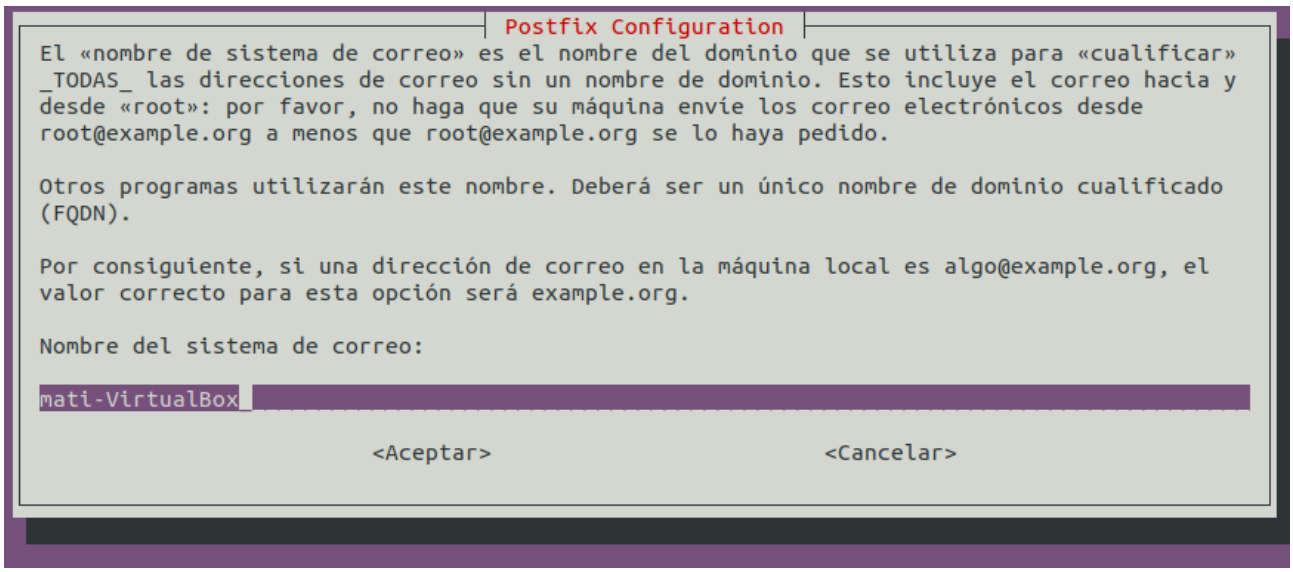
Ejercicio 4.

Instalar y ejecutar la citada herramienta en vuestro sistema de cara a:

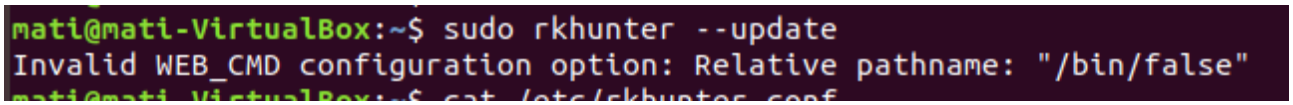
```
mati@mati-VirtualBox:~$ sudo apt-get install rkhunter
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  bsd-mailx fonts-lato javascript-common libjs-jquery liblockfile-bin liblockfile1 libruby2.5
  net-tools postfix rake ruby ruby-did-you-mean ruby-minitest ruby-net-telnet ruby-power-assert
  ruby-test-unit ruby2.5 rubygems-integration unhide unhide.rb
Paquetes sugeridos:
  apache2 | lighttpd | httpd procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre
  postfix-lmdb postfix-sqlite sasl2-bin dovecot-common resolvconf postfix-cdb postfix-doc ri
  ruby-dev bundler
Se instalarán los siguientes paquetes NUEVOS:
  bsd-mailx fonts-lato javascript-common libjs-jquery liblockfile-bin liblockfile1 libruby2.5
  net-tools postfix rake rkhunter ruby ruby-did-you-mean ruby-minitest ruby-net-telnet
  ruby-power-assert ruby-test-unit ruby2.5 rubygems-integration unhide unhide.rb
0 actualizados, 21 nuevos se instalarán, 0 para eliminar y 17 no actualizados.
```



Escogemos sin configuración.



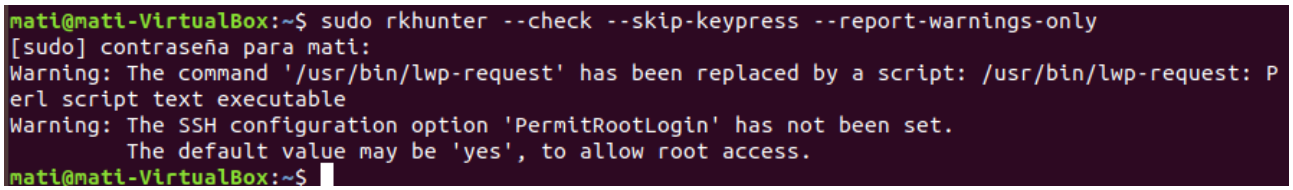
Las ordenes de las transparencias para preparar la herramienta antes de chequear el sistema me daban el siguiente error:



Hemos cambiado esa línea en el archivo de configuración “/etc/rkhunter.conf”.

a) Realizar un análisis del sistema para ver si está o no comprometido.

Me salen dos avisos:



b) De los avisos, soluciona los que sean falsos positivos, bien eliminando los tests bien ajustándolos adecuadamente.

Creemos que el primer aviso del punto anterior es un falso positivo, vamos a inspeccionar el programa para asegurarnos de ello.

```
mati@mati-VirtualBox:~$ cat /usr/bin/lwp-request
#!/usr/bin/perl

# Simple user agent using LWP library.

=head1 NAME

lwp-request, GET, POST, HEAD - Simple command line user agent

=head1 SYNOPSIS

B<lwp-request> [B<-afPuUsSedvhx>] [B<-m> I<method>] [B<-b> I<base URL>] [B<-t> I<timeout>]
            [B<-i> I<if-modified-since>] [B<-c> I<content-type>]
            [B<-C> I<credentials>] [B<-p> I<proxy-url>] [B<-o> I<format>] I<url>...

=head1 DESCRIPTION

This program can be used to send requests to WWW servers and your
local file system. The request content for POST and PUT
methods is read from stdin.  The content of the response is printed on
stdout.  Error messages are printed on stderr.  The program returns a
status value indicating the number of URLs that failed.

The options are:
```

Vamos buscar y a cambiar el archivo “/etc/rkhunter.conf” para añadir el camino de la orden anterior y que no de más un falso positivo, si alguien manipula los archivos, se mostrará un nuevo resultado que ya sabremos es positivo.

```
# The default value is the null string.
#
SCRIPTWHITELIST=/bin/egrep
SCRIPTWHITELIST=/bin/fgrep
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

#
```

Solo hemos tenido que descomentar “/usr/bin/lwp-request”