

SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software
Curso 2019-20

Práctica [1]. Administración de la seguridad en Linux.

Sesión [2]. Herramientas básicas de seguridad.

Autor¹: Nazaret Román Guerrero

Ejercicio 1.

Resuelve las siguientes cuestiones:

- a) Utiliza esta herramienta para conocer que procesos/servicios de nuestro sistema están accediendo a la red o tienen archivos abiertos. Indicar algunos de los servicios que tenéis activos , es decir, la actividad de la red, indicando qué información da la herramienta.
- b) Qué órdenes y opciones darías para conocer qué cuenta podría estar generando tráfico saliente malicioso de ssh y dónde se encuentra el archivo.
- c) Muestra los archivos a los que está accediendo un proceso concreto y los que están en uso por un usuario.
- a) Para poder ver los archivos que está usando el sistema y que están relacionados con la red se utiliza la opción `-i` de `lsof`; nos da información sobre qué agente está usando el archivo, el PID, el usuario y el tipo, el nombre del archivo y el tipo de protocolo de transporte, entre otros.

Es importante estar navegando por Internet para que haya algún archivo abierto que esté siendo usado por un agente. Si se ejecuta la orden sin que haya ningún navegador o aplicación que requiera de Internet la orden no da salida alguna, ya que no hay ningún archivo que pueda mostrar relacionado con la red.

Adicionalmente se podría usar la opción `-P`, que muestra los puertos, y la opción `-n`, que resuelve las IP y coloca el nombre de dominio en su lugar.

La salida es la que se muestra a continuación, en la imagen que hay en la siguiente página:

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 ...”

```
Archivo Editar Ver Buscar Terminal Ayuda
nazaretroque@nazaretroque:~$ lsof -i
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
firefox 20762 nazaretroque 96u IPv4 294590 0t0 TCP nazaretroque:55350->a92-123-180-89.deploy.static.akamaitechnologies.com:http (ESTABLISHED)
firefox 20762 nazaretroque 102u IPv4 294878 0t0 TCP nazaretroque:55352->a92-123-180-89.deploy.static.akamaitechnologies.com:http (ESTABLISHED)
firefox 20762 nazaretroque 121u IPv4 299020 0t0 TCP nazaretroque:52384->212.230.193.14:https (ESTABLISHED)
firefox 20762 nazaretroque 125u IPv4 299021 0t0 TCP nazaretroque:52386->212.230.193.14:https (ESTABLISHED)
firefox 20762 nazaretroque 129u IPv4 295360 0t0 TCP nazaretroque:35264->ec2-54-149-112-77.us-west-2.compute.amazonaws.com:https (ESTABLISHED)
firefox 20762 nazaretroque 137u IPv4 295396 0t0 TCP nazaretroque:54150->server-13-224-106-111.mad50.r.cloudfront.net:https (ESTABLISHED)
firefox 20762 nazaretroque 142u IPv4 295445 0t0 TCP nazaretroque:47208->93.184.220.29:http (ESTABLISHED)
firefox 20762 nazaretroque 145u IPv4 295447 0t0 TCP nazaretroque:43300->server-13-224-119-228.mad50.r.cloudfront.net:https (ESTABLISHED)
firefox 20762 nazaretroque 146u IPv4 295433 0t0 TCP nazaretroque:40530->ec2-52-33-184-165.us-west-2.compute.amazonaws.com:https (ESTABLISHED)
firefox 20762 nazaretroque 151u IPv4 295573 0t0 TCP nazaretroque:39424->ec2-52-42-239-171.us-west-2.compute.amazonaws.com:https (ESTABLISHED)
firefox 20762 nazaretroque 152u IPv4 296317 0t0 TCP nazaretroque:60742->muc03s14-in-f3.1e100.net:http (ESTABLISHED)
firefox 20762 nazaretroque 154u IPv4 295794 0t0 TCP nazaretroque:47494->a2-21-85-72.deploy.static.akamaitechnologies.com:http (ESTABLISHED)
firefox 20762 nazaretroque 177u IPv4 296243 0t0 TCP nazaretroque:45798->151.101.133.137:https (ESTABLISHED)
firefox 20762 nazaretroque 178u IPv4 296250 0t0 TCP nazaretroque:36650->assets.ubuntu.com:https (ESTABLISHED)
firefox 20762 nazaretroque 179u IPv4 296251 0t0 TCP nazaretroque:36652->assets.ubuntu.com:https (ESTABLISHED)
firefox 20762 nazaretroque 181u IPv4 296259 0t0 TCP nazaretroque:42152->mad07s09-in-f4.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 182u IPv4 296252 0t0 TCP nazaretroque:36654->assets.ubuntu.com:https (ESTABLISHED)
firefox 20762 nazaretroque 186u IPv4 296314 0t0 TCP nazaretroque:36664->assets.ubuntu.com:https (ESTABLISHED)
firefox 20762 nazaretroque 187u IPv4 296315 0t0 TCP nazaretroque:36666->assets.ubuntu.com:https (ESTABLISHED)
firefox 20762 nazaretroque 188u IPv4 296324 0t0 TCP nazaretroque:49132->arn02s06-in-f168.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 189u IPv4 296322 0t0 TCP nazaretroque:36670->assets.ubuntu.com:https (ESTABLISHED)
firefox 20762 nazaretroque 190u IPv4 296358 0t0 TCP nazaretroque:42188->mad07s10-in-f3.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 191u IPv4 296359 0t0 TCP nazaretroque:56096->mad08s05-in-f14.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 192u IPv4 296445 0t0 TCP nazaretroque:42202->mad07s10-in-f3.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 193u IPv4 296440 0t0 TCP nazaretroque:58768->muc03s14-in-f54.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 194u IPv4 296361 0t0 TCP nazaretroque:60754->muc03s14-in-f3.1e100.net:http (ESTABLISHED)
firefox 20762 nazaretroque 195u IPv4 296462 0t0 TCP nazaretroque:53338->mad07s10-in-f10.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 196u IPv4 296369 0t0 TCP nazaretroque:60758->muc03s14-in-f3.1e100.net:http (ESTABLISHED)
firefox 20762 nazaretroque 197u IPv4 296465 0t0 TCP nazaretroque:51770->arn02s06-in-f161.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 198u IPv4 296495 0t0 TCP nazaretroque:46040->muc03s14-in-f13.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 199u IPv4 296510 0t0 TCP nazaretroque:59868->mad06s25-in-f14.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 201u IPv4 296510 0t0 TCP nazaretroque:50320->mad07s09-in-f2.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 204u IPv4 296470 0t0 TCP nazaretroque:60778->muc03s14-in-f3.1e100.net:http (ESTABLISHED)
firefox 20762 nazaretroque 205u IPv4 296480 0t0 TCP nazaretroque:60780->muc03s14-in-f3.1e100.net:http (ESTABLISHED)
firefox 20762 nazaretroque 207u IPv4 296488 0t0 TCP nazaretroque:48256->mad08s04-in-f3.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 209u IPv4 296527 0t0 TCP nazaretroque:42214->mad07s09-in-f4.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 211u IPv4 298688 0t0 TCP nazaretroque:50350->mad07s09-in-f2.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 214u IPv4 296697 0t0 TCP nazaretroque:60798->muc03s14-in-f3.1e100.net:http (ESTABLISHED)
firefox 20762 nazaretroque 220u IPv4 298446 0t0 TCP nazaretroque:54370->mad08s06-in-f6.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 228u IPv4 298506 0t0 TCP nazaretroque:34100->muc03s14-in-f3.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 232u IPv4 298258 0t0 TCP nazaretroque:42230->mad07s09-in-f4.1e100.net:https (ESTABLISHED)
firefox 20762 nazaretroque 236u IPv4 298562 0t0 TCP nazaretroque:44386->mad07s10-in-f2.1e100.net:https (ESTABLISHED)
nazaretroque@nazaretroque:~$
```

- b) En este caso, se pueden utilizar distintas medidas para saber si hay alguien utilizando el servicio de ssh en nuestro sistema sin que nosotros lo sepamos.

Una opción es utilizar el comando `lsof` con la opción `-i`, añadiendo parámetros adicionales a esta opción, como el servicio o el puerto. El comando completo quedaría como:

```
lsof -i:ssh,22 [-P -n]
```

donde `ssh` es el servicio y `22` el puerto que éste usa; las opciones `-P` y `-n` no son necesarias como tal, pero son útiles para lo comentado en el apartado anterior.

La salida del comando con estas opciones se muestra más abajo. Como se puede comprobar, no hay ningún servicio que esté utilizando el puerto 22, por lo que no hay tráfico malicioso.

```
Archivo Editar Ver Buscar Terminal Ayuda
nazaretroque@nazaretroque:~$ lsof -i:ssh,22
nazaretroque@nazaretroque:~$
```

También podemos utilizar el comando como

```
lsof | grep ssh
```

que muestra además los procesos que no tienen ningún archivo en ejecución para el servicio de `ssh` (es decir, que realmente no lo están usando) pero cuentan con algún tipo de archivo abierto que contiene en el nombre la palabra `ssh`:

```
root@nazaretroque: /home/nazaretroque
Archivo Editar Ver Buscar Terminal Ayuda
root@nazaretroque: /home/nazaretroque# lsof | grep ssh
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
systemd    828      gdm      23u      unix 0xffff8dba3570f800      0t0      21437 /run/user/121/gnupg/S.gpg-agent.ssh type=STREAM
systemd    957      nazaretroque 25u      unix 0xffff8dba38445c00      0t0      89223 /run/user/1000/gnupg/S.gpg-agent.ssh type=STREAM
gnome-key  974      nazaretroque 14u      unix 0xffff8dba351e4400      0t0      90495 /run/user/1000/keyring/ssh type=STREAM
gnain      974      975      nazaretroque 14u      unix 0xffff8dba351e4400      0t0      90495 /run/user/1000/keyring/ssh type=STREAM
gdbus      974      976      nazaretroque 14u      unix 0xffff8dba351e4400      0t0      90495 /run/user/1000/keyring/ssh type=STREAM
timer      974      1181     nazaretroque 14u      unix 0xffff8dba351e4400      0t0      90495 /run/user/1000/keyring/ssh type=STREAM
ssh-agent  1137     nazaretroque cwd      DIR      8,1      4096      2 /
ssh-agent  1137     nazaretroque rtd      DIR      8,1      4096      2 /
ssh-agent  1137     nazaretroque txt      REG      8,1      362640    132331 /usr/bin/ssh-agent (deleted)
ssh-agent  1137     nazaretroque mem      REG      8,1      14560     399385 /lib/x86_64-linux-gnu/libdl-2.27.so
ssh-agent  1137     nazaretroque mem      REG      8,1      2030544   399362 /lib/x86_64-linux-gnu/libc-2.27.so
ssh-agent  1137     nazaretroque DEL      REG      8,1      142237    142237 /usr/lib/x86_64-linux-gnu/libcrypto.so.1.0.0
ssh-agent  1137     nazaretroque mem      REG      8,1      170960    399334 /lib/x86_64-linux-gnu/ld-2.27.so
ssh-agent  1137     nazaretroque 0u      CHR      1,3      0t0       6 /dev/null
ssh-agent  1137     nazaretroque 1u      CHR      1,3      0t0       6 /dev/null
ssh-agent  1137     nazaretroque 2u      CHR      1,3      0t0       6 /dev/null
ssh-agent  1137     nazaretroque 3u      unix 0xffff8dba350afc00      0t0      90096 /tmp/ssh-wNxlN0PUSaXU/agent.1006 type=STREAM
systemd    7564     root     28u      unix 0xffff8dba3662bc00      0t0      362200 /run/user/0/gnupg/S.gpg-agent.ssh type=STREAM
root@nazaretroque: /home/nazaretroque#
```

Como se puede ver, se muestra el usuario, la ruta del archivo, el tipo o el PID del proceso que lo está usando.

- c) Para mostrar todos los archivos abiertos por un proceso se utiliza la opción `-p <PID>` (en este caso en minúscula, ya que la mayúscula es usada para los puertos de los servicios). Al utilizar la opción `-p` hay que añadir el PID del proceso del que queremos conocer los archivos abiertos. En el ejemplo de la imagen, se ha utilizado el PID del bash que se estaba usando:

```
nazaretroque@nazaretroque: ~
Archivo Editar Ver Buscar Terminal Ayuda
nazaretroque@nazaretroque:~$ ps
  PID TTY          TIME CMD
 7145 pts/0    00:00:00 bash
 7544 pts/0    00:00:00 ps
nazaretroque@nazaretroque:~$ lsof -p 7145
COMMAND  PID  USER      FD  TYPE  DEVICE  SIZE/OFF  NODE NAME
bash     7145 nazaretroque cwd   DIR    8,1      4096    278889 /home/nazaretroque
bash     7145 nazaretroque rtd   DIR    8,1      4096      2 /
bash     7145 nazaretroque txt   REG    8,1    1113504 262890 /bin/bash
bash     7145 nazaretroque mem   REG    8,1    47568    399452 /lib/x86_64-linux-gnu/libnss_files-2.27.so
bash     7145 nazaretroque mem   REG    8,1    97176    399446 /lib/x86_64-linux-gnu/libnsl-2.27.so
bash     7145 nazaretroque mem   REG    8,1    47576    399463 /lib/x86_64-linux-gnu/libnss_nis-2.27.so
bash     7145 nazaretroque mem   REG    8,1    39744    399448 /lib/x86_64-linux-gnu/libnss_compat-2.27.so
bash     7145 nazaretroque mem   REG    8,1   10281936 137979 /usr/lib/locale/locale-archive
bash     7145 nazaretroque mem   REG    8,1    2030544 399362 /lib/x86_64-linux-gnu/libc-2.27.so
bash     7145 nazaretroque mem   REG    8,1    14560    399385 /lib/x86_64-linux-gnu/libdl-2.27.so
bash     7145 nazaretroque mem   REG    8,1    170784    399520 /lib/x86_64-linux-gnu/libtinfo.so.5.9
bash     7145 nazaretroque mem   REG    8,1    170960    399334 /lib/x86_64-linux-gnu/ld-2.27.so
bash     7145 nazaretroque mem   REG    8,1   179664    533748 /usr/share/locale-langpack/es/LC_MESSAGES/bash.mo
bash     7145 nazaretroque mem   REG    8,1    26376    267170 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
bash     7145 nazaretroque 0u    CHR   136,0      0t0      3 /dev/pts/0
bash     7145 nazaretroque 1u    CHR   136,0      0t0      3 /dev/pts/0
bash     7145 nazaretroque 2u    CHR   136,0      0t0      3 /dev/pts/0
bash     7145 nazaretroque 255u  CHR   136,0      0t0      3 /dev/pts/0
nazaretroque@nazaretroque:~$
```

Para mostrar los archivos abiertos por un usuario en concreto, se usa la opción `-u <user>`, donde user es el usuario que buscamos. En este caso, se muestra un fragmento de los archivos abiertos por root:

```
root@nazaretroque: /home/nazaretroque
Archivo Editar Ver Buscar Terminal Ayuda
root@nazaretroque: /home/nazaretroque# lsof -u root
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   1  root      cwd   DIR    8,1      4096      2 /
systemd   1  root      rtd   DIR    8,1      4096      2 /
systemd   1  root      txt   REG    8,1    1595792 393756 /lib/systemd/systemd
systemd   1  root      mem   REG    8,1    1700792 399425 /lib/x86_64-linux-gnu/libm-2.27.so
systemd   1  root      mem   REG    8,1    121016    395174 /lib/x86_64-linux-gnu/libudev.so.1.6.9
systemd   1  root      mem   REG    8,1     84032    399403 /lib/x86_64-linux-gnu/libgpg-error.so.0.22.0
systemd   1  root      mem   REG    8,1    43304    399414 /lib/x86_64-linux-gnu/libjson-c.so.3.0.1
systemd   1  root      mem   REG    8,1     34872    142090 /usr/lib/x86_64-linux-gnu/libargon2.so.0
systemd   1  root      DEL   REG    8,1      399384 /lib/x86_64-linux-gnu/libdevmapper.so.1.02.1
systemd   1  root      mem   REG    8,1     18680    399350 /lib/x86_64-linux-gnu/libattr.so.1.1.0
systemd   1  root      mem   REG    8,1     18712    399365 /lib/x86_64-linux-gnu/libcap-ng.so.0.0.0
systemd   1  root      DEL   REG    8,1      399530 /lib/x86_64-linux-gnu/libuuid.so.1.3.0
systemd   1  root      mem   REG    8,1     14560    399385 /lib/x86_64-linux-gnu/libdl-2.27.so
```

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).

Para mostrar todos los procesos activos en el sistema, se utiliza la opción `-A` o la opción `-e` (ambas muestran exactamente la misma información). Para poder ver si hay diferencia entre las distintas ejecuciones del comando y saber si hay nuevos procesos funcionando o si se ha cerrado alguno, volcamos la salida en archivos para poder hacer después `diff`.

El primer volcado se lleva a cabo con la máquina recién encendida. El segundo después de abrir el navegador de la máquina, y la última, después de cerrar dicho navegador (matando el proceso).

```
nazaretroque@nazaretroque:~$ ps -A > toma1.txt
nazaretroque@nazaretroque:~$ firefox &
[1] 8662
nazaretroque@nazaretroque:~$ ps -A > toma2.txt
nazaretroque@nazaretroque:~$ kill -9 8662
nazaretroque@nazaretroque:~$ [GFX1-]: Receive IPC close with reason=AbnormalShutdown
[Child 8787, Chrome_ChildThread] WARNING: pipe error (3): Conexión reiniciada por la máquina remota: file /build/firefox-y_KX3V/firefox-69.0.1+build1/ipc/chromium/src/chrome/common/ipc_channel_posix.cc, line 358
Exiting due to channel error.
[GFX1-]: Receive IPC close with reason=AbnormalShutdown
[Child 8748, Chrome_ChildThread] WARNING: pipe error (3): Conexión reiniciada por la máquina remota: file /build/firefox-y_KX3V/firefox-69.0.1+build1/ipc/chromium/src/chrome/common/ipc_channel_posix.cc, line 358
Exiting due to channel error.
[GFX1-]: Receive IPC close with reason=AbnormalShutdown
[Child 8707, Chrome_ChildThread] WARNING: pipe error (3): Conexión reiniciada por la máquina remota: file /build/firefox-y_KX3V/firefox-69.0.1+build1/ipc/chromium/src/chrome/common/ipc_channel_posix.cc, line 358
Exiting due to channel error.
[1]+ Terminado (killed) firefox
nazaretroque@nazaretroque:~$ ps -A > toma3.txt
nazaretroque@nazaretroque:~$
```

Una vez sacadas las tomas, buscamos las diferencias entre los archivos.

Como se puede comprobar, existen diferencias en los tres archivos. Eso se debe a los procesos que se crean y mueren en el sistema (tanto los voluntarios, es decir, los que lleva a cabo el usuario de forma consciente, como los involuntarios, en los que el usuario no tiene conocimiento de que se han iniciado o matado procesos, ya que se encarga el sistema de manera autónoma).

```
nazaretroque@nazaretroque:~$ diff toma1.txt toma2.txt
96c96
< 1182 tty2      00:02:43 gnome-shell
---
> 1182 tty2      00:02:44 gnome-shell
184c184,188
< 8659 pts/0    00:00:00 ps
---
> 8662 pts/0     00:00:01 firefox
> 8707 pts/0     00:00:00 Web Content
> 8748 pts/0     00:00:00 WebExtensions
> 8787 pts/0     00:00:00 Web Content
> 8815 pts/0     00:00:00 ps

nazaretroque@nazaretroque:~$ diff toma1.txt toma3.txt
96c96
< 1182 tty2      00:02:43 gnome-shell
---
> 1182 tty2      00:02:45 gnome-shell
163c163
< 1579 tty2      00:00:01 ibus-engine-sim
---
> 1579 tty2      00:00:02 ibus-engine-sim
184c184
< 8659 pts/0     00:00:00 ps
---
> 8817 pts/0     00:00:00 ps

nazaretroque@nazaretroque:~$ diff toma2.txt toma3.txt
96c96
< 1182 tty2      00:02:44 gnome-shell
---
> 1182 tty2      00:02:45 gnome-shell
163c163
< 1579 tty2      00:00:01 ibus-engine-sim
---
> 1579 tty2      00:00:02 ibus-engine-sim
184,188c184
< 8662 pts/0     00:00:01 firefox
< 8707 pts/0     00:00:00 Web Content
< 8748 pts/0     00:00:00 WebExtensions
< 8787 pts/0     00:00:00 Web Content
< 8815 pts/0     00:00:00 ps
---
> 8817 pts/0     00:00:00 ps
```

Ejercicio 3.

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

- Mostrar qué 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.
 - En clase de teoría vimos la vulnerabilidad Shellshock, indicar si la herramienta citada comprueba dicha vulnerabilidad y explicar cómo lo hace (esto nos servirá para conocer como podríamos desarrollar nuestro propio test). Consejo, revisar el contenido del archivo de la herramienta `include/tests_shells`.
 - 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).
- a) Para llevar a cabo un test de vulnerabilidades en `lynis` utilizamos la opción `--checkall`, cuya resultado es el siguiente:

```
-[ Lynis 2.6.2 Results ]-

Warnings (4):
-----
! Version of Lynis is very old and should be updated [LYNIS]
  https://cisofy.com/controls/LYNIS/

! No password set for single mode [AUTH-9308]
  https://cisofy.com/controls/AUTH-9308/

! Couldn't find 2 responsive nameservers [NETW-2705]
  https://cisofy.com/controls/NETW-2705/

! iptables module(s) loaded, but no rules active [FIRE-4512]
  https://cisofy.com/controls/FIRE-4512/
```

Arreglar estas vulnerabilidades es sencillo.

- La versión de `lynis` es antigua y debe ser actualizada. Es un grado de severidad alto, debido a que un sistema desactualizado supone una presa fácil. Para arreglarlo solo tenemos que actualizar `lynis`.

```
root@nazaretroque: /home/nazaretroque
Archivo Editar Ver Buscar Terminal Ayuda
root@nazaretroque:/home/nazaretroque# sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-
v-keys C80E383C3D9F082E01391A0366C67DE91CA5D5F
Executing: /tmp/apt-key-gpghome.00w13ah2C/gpg.1.sh --keyserver keyserver.ubuntu.com --recv-k
eys C80E383C3D9F082E01391A0366C67DE91CA5D5F
gpg: key 366C67DE91CA5D5F: 2 firmas no comprobadas por falta de claves
gpg: clave 366C67DE91CA5D5F: clave pública "CISOFy Software (signed software packages) <softw
are@cisofy.com>" importada
gpg: Cantidad total procesada: 1
gpg:      importadas: 1
root@nazaretroque:/home/nazaretroque# sudo apt install apt-transport-https
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
liblvm7
Utilice «sudo apt autoremove» para eliminarlo.
Se instalarán los siguientes paquetes NUEVOS:
  apt-transport-https
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 1.692 B de archivos.
Se utilizarán 153 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 apt-transport-https a
ll 1.6.12 [1.692 B]
Descargados 1.692 B en 1s (3.114 B/s)
Seleccionando el paquete apt-transport-https previamente no seleccionado.
(Leyendo la base de datos ... 164746 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../apt-transport-https_1.6.12_all.deb ...
Desempaquetando apt-transport-https (1.6.12) ...
Configurando apt-transport-https (1.6.12) ...
root@nazaretroque:/home/nazaretroque# echo 'Acquire::Languages "none";' | sudo tee /etc/apt/a
pt.conf.d/99disable-translations
Acquire::Languages "none";
root@nazaretroque:/home/nazaretroque#
```


- El segundo warning nos indica que el grub no tiene contraseña (de hecho, ni siquiera está configurado), lo que puede suponer una amenaza. No obstante, en este caso la amenaza es de severidad media-baja, puesto que al no estar configurado no se puede acceder desde el grub a la BIOS, directamente entra al sistema operativo de la máquina. No obstante, el arreglo es sencillo, solo hay que configurar el grub.

Para ello, primero generamos una clave pública.

```
root@nazaretroque: /home/nazaretroque
Archivo Editar Ver Buscar Terminal Ayuda
root@nazaretroque:/home/nazaretroque# grub-mkpasswd-pbkdf2
Introduzca la contraseña:
Reintroduzca la contraseña:
El hash PBKDF2 de su contraseña es grub.pbkdf2.sha512.10000.B37869A54C8F2D7E1CF1
```

Tras esto, la incluimos en el fichero /etc/grub.d/00_header y como se ve en la imagen y actualizamos el grub.

```
cat << EOF
set superusers="admin"
password_pbkdf2 admin
grub.pbkdf2.sha512.10000
EOF|
```

```
root@nazaretroque: /home/nazaretroque
Archivo Editar Ver Buscar Terminal Ayuda
root@nazaretroque:/home/nazaretroque# gedit /etc/grub.d/00_header
root@nazaretroque:/home/nazaretroque# update-grub2
Sourcing file '/etc/default/grub'
Generando un fichero de configuración de grub...
Encontrada imagen de linux: /boot/vmlinuz-5.0.0-31-generic
Encontrada imagen de memoria inicial: /boot/initrd.img-5.0.0-31-generic
Encontrada imagen de linux: /boot/vmlinuz-5.0.0-29-generic
Encontrada imagen de memoria inicial: /boot/initrd.img-5.0.0-29-generic
Found memtest86+ image: /boot/memtest86+.elf
Found memtest86+ image: /boot/memtest86+.bin
hecho
root@nazaretroque:/home/nazaretroque#
```

- El tercer warning se arregla automáticamente al actualizar la versión de lynis. Al tener una versión antigua, no leía correctamente el fichero donde se encuentran las IPs de los servidores DNS; una vez actualizada, ese fallo desaparece. Esta vulnerabilidad es de severidad baja puesto que con que un solo DNS funcione, todo irá bien.
- El último warning nos advierte que no tenemos ninguna regla en el cortafuegos. Su severidad alta puesto que nuestro sistema está expuesto. De hecho el cortafuegos ni siquiera está activado, por lo que el primer paso es habilitarlo. Tras esto, se añade una regla que acepta todo el tráfico cuyo protocolo sea TCP y proveniente del puerto 80.

Una vez añadida, se recarga el cortafuegos para que se active la nueva configuración.

```
root@nazaretroque: /home/nazaretroque
Archivo Editar Ver Buscar Terminal Ayuda
root@nazaretroque:/home/nazaretroque# ufw enable
El cortafuegos está activo y habilitado en el arranque del sistema
root@nazaretroque:/home/nazaretroque# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@nazaretroque:/home/nazaretroque# ufw reload
El cortafuegos se ha recargado
root@nazaretroque:/home/nazaretroque#
```

Una vez tratadas todos los warnings (y ejecutando el test después de eliminar cada una para comprobar que lo que se está haciendo va por buen camino), volvemos a ejecutar el test, obteniendo la siguiente salida:

```
-[ Lynis 2.7.5 Results ]-  
  
Great, no warnings
```

Por lo que nuestro sistema ahora no tiene vulnerabilidades.

- b) En el archivo de lynis tests_shells, se llevan a cabo tests para vulnerabilidades (concretamente para la 6211, la 6220 y la 6230) pero no para shellshock, cuyo identificador es el 6271. También se puede observar al ejecutar un test (como el del apartado anterior), cuya salida es:

```
[+] Shells  
-----  
- Checking shells from /etc/shells  
  Result: found 4 shells (valid shells: 4).  
- Session timeout settings/tools [ NONE ]  
- Checking default umask values  
  - Checking default umask in /etc/bash.bashrc [ NONE ]  
  - Checking default umask in /etc/profile [ NONE ]
```

Por lo que podemos ver que no está el test para shellshock y que, por tanto, no lo comprueba.

- c) Para evitar que la herramienta detecte que no hay antivirus cuando éste es desconocido, hay que modificar el archivo include/tests_malware.

Con este archivo se detectan ciertos antivirus, pero si tenemos uno que no está contemplado, al ejecutar los tests nos avisará de que no hay antivirus en nuestra máquina cuando en realidad sí lo hay. Para evitar esto, una de las variables globales que está iniciada a 0 (a false) se cambiaría a 1 (true) por lo que se habría establecido ya que el antivirus está instalado (aunque no se está comprobando realmente en los tests por lo que no es la mejor opción).

Una segunda opción, más exhaustiva, es crear a mano un test y añadirlo al fichero mencionado, de manera que se ejecute también cuando se lance la herramienta de lynis.

Ejercicio 4.

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

- Realizar un análisis del sistema para ver si está o no comprometido.
- De los avisos, soluciona los que sean falsos positivos, bien eliminando los tests, bien ajustándolos adecuadamente.

- a) Para comprobar si el sistema está comprometido se analiza con la opción -c (o --check) y da como resultado el siguiente resumen:

```
System checks summary
=====

File properties checks...
  Files checked: 149
  Suspect files: 1

Rootkit checks...
  Rootkits checked : 479
  Possible rootkits: 0

Applications checks...
  All checks skipped

The system checks took: 1 minute and 41 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)
```

Como podemos observar, no hay rootkits en el sistema.

El único warning registrado es sobre /usr/bin/lwp-request. El archivo de log /var/log/rkhunter.log explica con más detalle el warning: el comando /usr/bin/lwp-request ha sido sustituido por un script ejecutable escrito en Perl.

```
/usr/bin/nmmtc [ OK ]
/usr/bin/mawk [ OK ]
/usr/bin/lwp-request [ Warning ]
/usr/bin/bsd-mailx [ OK ]
/usr/bin/lwp-64-linux-gnu-size [ OK ]
```

```
[15:24:52] /usr/bin/mawk [ OK ]
[15:24:52] /usr/bin/lwp-request [ Warning ]
[15:24:52] Warning: The command '/usr/bin/lwp-request' has been replaced by a script: /usr/bin/lwp-request: Perl script text executable
[15:24:52] /usr/bin/bsd-mailx [ OK ]
[15:24:52] /usr/bin/lwp-64-linux-gnu-size [ OK ]
```

- b) Para solucionar esto, hay que modificar el archivo /etc/rkhunter.conf y añadir el script en la parte SCRIPTWHITELIST. Como se puede observar, el script ya estaba añadido y solo es necesario descomentar la línea.

```
#
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
```

Una vez hecho esto, volvemos a ejecutar rkhunter -c para comprobar que la medida ha sido efectiva.

El resumen del nuevo chequeo no contiene ningún archivo sospechoso ni tampoco se indica que haya ningún warning en el archivo de log (última línea), como se puede ver en la

siguiente imagen:

```
System checks summary
=====

File properties checks...
  Files checked: 149
  Suspect files: 0

Rootkit checks...
  Rootkits checked : 479
  Possible rootkits: 0

Applications checks...
  All checks skipped

The system checks took: 1 minute and 3 seconds

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

No warnings were found while checking the system.
```

Además, mientras se ejecuta el test podemos comprobar que, en efecto, el comando `/usr/bin/lwp-request` no da warning alguno:

```
/usr/bin/mawk [ OK ]
/usr/bin/lwp-request [ OK ]
/usr/bin/bsd-mailx [ OK ]
```

Por lo que está arreglado y nuestro sistema ahora es seguro.