INFORME DE INCIDENTE DE SEGURIDAD

Nicolás Oriol Sengáriz

4Geeks

Índice

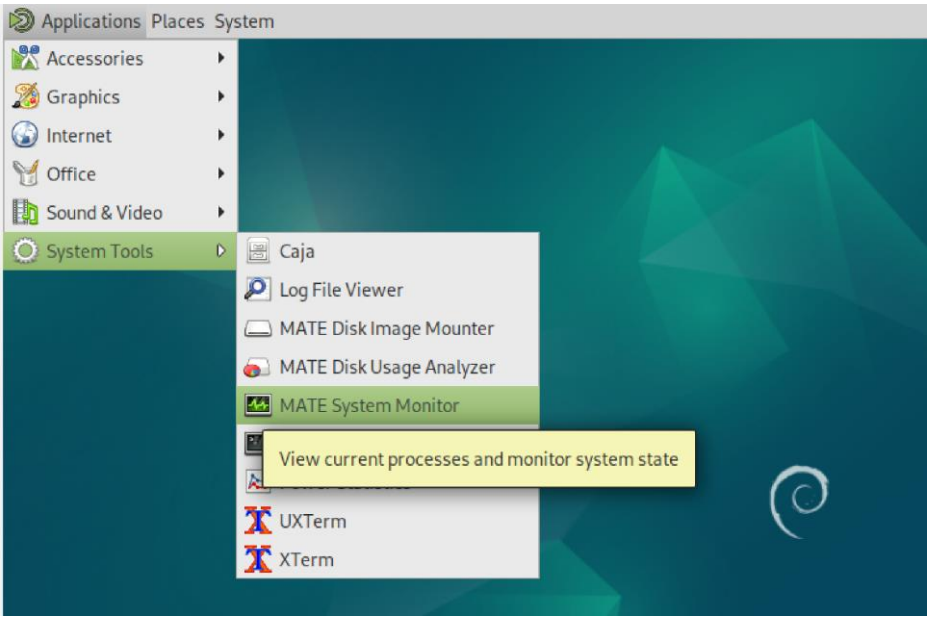
Introducción

El objetivo de este informe es llevar a cabo un análisis sobre un incidente de seguridad que ha habido en un servidor crítico de 4Geeks Academy.

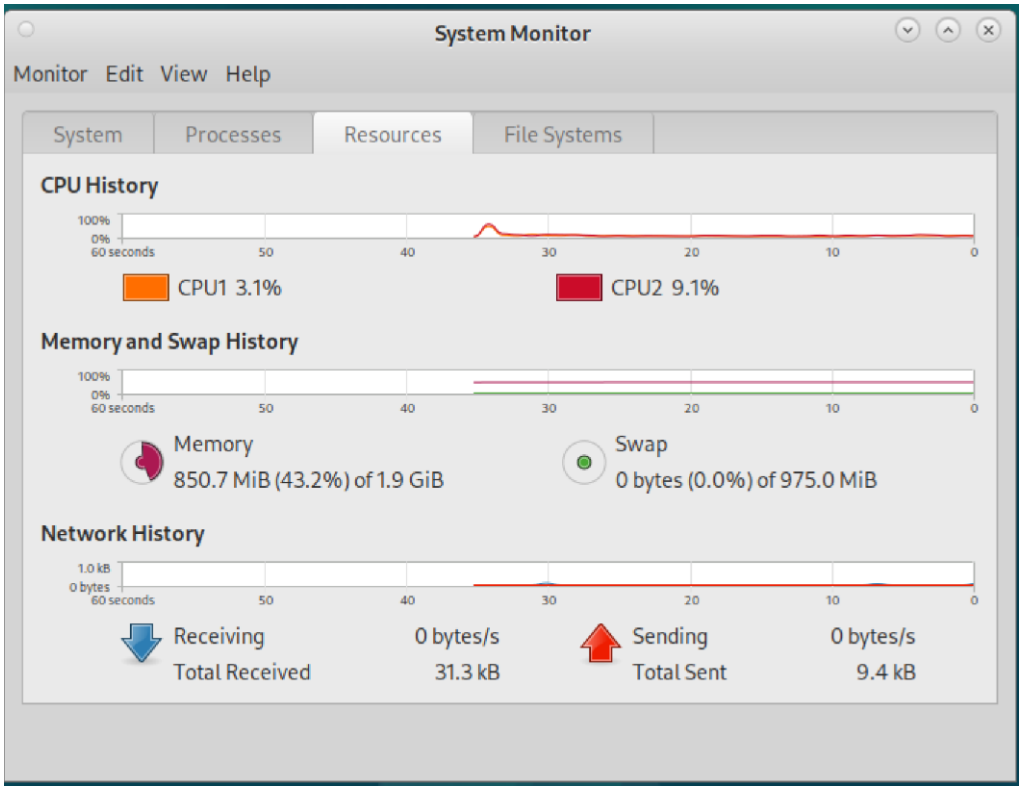
Procesos en ejecución

Se realiza una investigación de los procesos en ejecución para ver si hay algún proceso sospechoso.

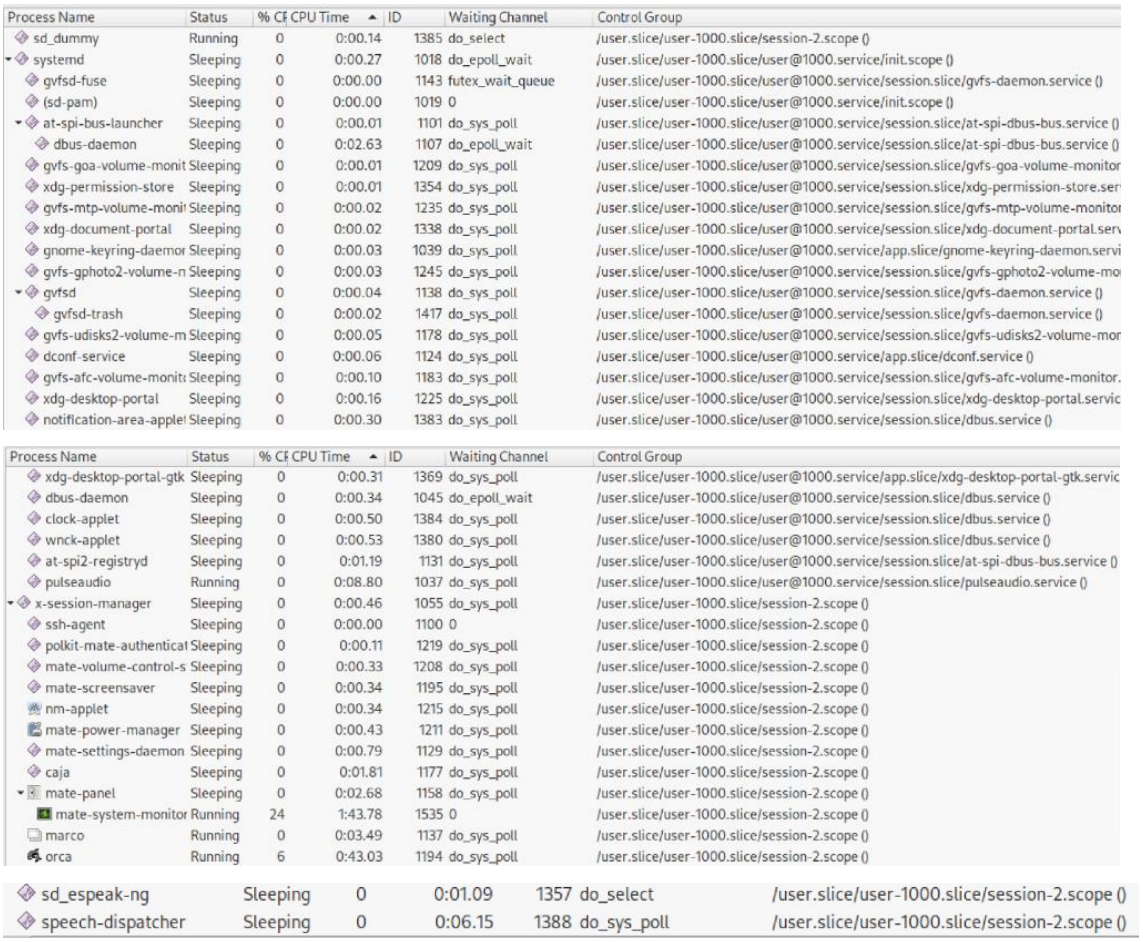
Al ser una máquina debian eso se puede hacer desde System Tools – MATE System Monitor.



Esta ventana permite ver los procesos en ejecución y monitorear el estado del sistema, como el uso del CPU, RAM y la red de internet.



En el apartado de “Processes” aparecen los procesos en ejecución que son los de las imágenes de abajo.



Process Name	Status	% CF	CPU Time	ID	Waiting Channel	Control Group
sd_dummy	Running	0	0:00.14	1385	do_select	/user.slice/user-1000.slice/session-2.scope ()
systemd	Sleeping	0	0:00.27	1018	do_epoll_wait	/user.slice/user-1000.slice/user@1000.service/init.scope ()
gvfsd-fuse	Sleeping	0	0:00.00	1143	futex_wait_queue	/user.slice/user-1000.slice/user@1000.service/session.slice/gvfs-daemon.service ()
(sd-pam)	Sleeping	0	0:00.00	1019	0	/user.slice/user-1000.slice/user@1000.service/init.scope ()
at-spi-bus-launcher	Sleeping	0	0:00.01	1101	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/at-spi-dbus-bus.service ()
dbus-daemon	Sleeping	0	0:02.63	1107	do_epoll_wait	/user.slice/user-1000.slice/user@1000.service/session.slice/at-spi-dbus-bus.service ()
gvfs-goa-volume-monit	Sleeping	0	0:00.01	1209	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/gvfs-goa-volume-monitor
xdg-permission-store	Sleeping	0	0:00.01	1354	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/xdg-permission-store.ser
gvfs-mtp-volume-monit	Sleeping	0	0:00.02	1235	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/gvfs-mtp-volume-monitor
xdg-document-portal	Sleeping	0	0:00.02	1338	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/xdg-document-portal.serv
gnome-keyring-daemor	Sleeping	0	0:00.03	1039	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/app.slice/gnome-keyring-daemon.servi
gvfs-gphoto2-volume-n	Sleeping	0	0:00.03	1245	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/gvfs-gphoto2-volume-mo
gvfsd	Sleeping	0	0:00.04	1138	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/gvfs-daemon.service ()
gvfsd-trash	Sleeping	0	0:00.02	1417	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/gvfs-daemon.service ()
gvfs-udisks2-volume-m	Sleeping	0	0:00.05	1178	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/gvfs-udisks2-volume-mor
dconf-service	Sleeping	0	0:00.06	1124	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/app.slice/dconf.service ()
gvfs-afc-volume-monit	Sleeping	0	0:00.10	1183	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/gvfs-afc-volume-monitor.
xdg-desktop-portal	Sleeping	0	0:00.16	1225	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/xdg-desktop-portal.servic
notification-area-apple	Sleeping	0	0:00.30	1383	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/dbus.service ()

Process Name	Status	% CF	CPU Time	ID	Waiting Channel	Control Group
xdg-desktop-portal-gtk	Sleeping	0	0:00.31	1369	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/app.slice/xdg-desktop-portal-gtk.servic
dbus-daemon	Sleeping	0	0:00.34	1045	do_epoll_wait	/user.slice/user-1000.slice/user@1000.service/session.slice/dbus.service ()
clock-applet	Sleeping	0	0:00.50	1384	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/dbus.service ()
wnck-applet	Sleeping	0	0:00.53	1380	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/dbus.service ()
at-spi2-registryd	Sleeping	0	0:01.19	1131	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/at-spi-dbus-bus.service ()
pulseaudio	Running	0	0:08.80	1037	do_sys_poll	/user.slice/user-1000.slice/user@1000.service/session.slice/pulseaudio.service ()
x-session-manager	Sleeping	0	0:00.46	1055	do_sys_poll	/user.slice/user-1000.slice/session-2.scope ()
ssh-agent	Sleeping	0	0:00.00	1100	0	/user.slice/user-1000.slice/session-2.scope ()
polkit-mate-authenticat	Sleeping	0	0:00.11	1219	do_sys_poll	/user.slice/user-1000.slice/session-2.scope ()
mate-volume-control-s	Sleeping	0	0:00.33	1208	do_sys_poll	/user.slice/user-1000.slice/session-2.scope ()
mate-screensaver	Sleeping	0	0:00.34	1195	do_sys_poll	/user.slice/user-1000.slice/session-2.scope ()
nm-applet	Sleeping	0	0:00.34	1215	do_sys_poll	/user.slice/user-1000.slice/session-2.scope ()
mate-power-manager	Sleeping	0	0:00.43	1211	do_sys_poll	/user.slice/user-1000.slice/session-2.scope ()
mate-settings-daemon	Sleeping	0	0:00.79	1129	do_sys_poll	/user.slice/user-1000.slice/session-2.scope ()
caja	Sleeping	0	0:01.81	1177	do_sys_poll	/user.slice/user-1000.slice/session-2.scope ()
mate-panel	Sleeping	0	0:02.68	1158	do_sys_poll	/user.slice/user-1000.slice/session-2.scope ()
mate-system-monitor	Running	24	1:43.78	1535	0	/user.slice/user-1000.slice/session-2.scope ()
marco	Running	0	0:03.49	1137	do_sys_poll	/user.slice/user-1000.slice/session-2.scope ()
orca	Running	6	0:43.03	1194	do_sys_poll	/user.slice/user-1000.slice/session-2.scope ()

sd_espeak-ng	Sleeping	0	0:01.09	1357	do_select	/user.slice/user-1000.slice/session-2.scope ()
speech-dispatcher	Sleeping	0	0:06.15	1388	do_sys_poll	/user.slice/user-1000.slice/session-2.scope ()

Después de realizar una investigación sobre los procesos en ejecución no se detecta ningún proceso malicioso o fuera de lo común.

Todos los procesos pertenecen al usuario debian, con ID 1000.

Escaneo de rootkit

Para realizar un escaneo para buscar rootkits se usará la herramienta Rkhunter.

Para usarlo hay que instalar la herramienta con el comando sudo apt install rkhunter.

```
debian@debian:~$ sudo apt install rkhunter
```

Antes de escanear interesa actualizar la base de datos, especialmente si hace tiempo que tienes instalada la herramienta Rkhunter.

Se actualiza con los siguientes comandos:

sudo rkhunter –update

```
debian@debian:~$ sudo rkhunter --update
[ Rootkit Hunter version 1.4.6 ]
```

sudo rkhunter –propupd

```
debian@debian:~$ sudo rkhunter --propupd
[ Rootkit Hunter version 1.4.6 ]
```

Una vez ya está actualizada la base de datos, se procede a realizar el escaneo de rootkits usando el comando sudo rkhunter –check.

```
debian@debian:~$ sudo rkhunter --check
[ Rootkit Hunter version 1.4.6 ]
```

```
Checking for rootkits...

  Performing check of known rootkit files and directories
    55808 Trojan - Variant A                                 [ Not found ]
    ADM Worm                                                 [ Not found ]
    AjaKit Rootkit                                           [ Not found ]
    Adore Rootkit                                            [ Not found ]
    aPa Kit                                                  [ Not found ]
    Apache Worm                                              [ Not found ]
    Ambient (ark) Rootkit                                    [ Not found ]
    Balaur Rootkit                                           [ Not found ]
    BeastKit Rootkit                                         [ Not found ]
    beX2 Rootkit                                             [ Not found ]
    BOBKit Rootkit                                           [ Not found ]
    cb Rootkit                                               [ Not found ]
    CiNIK Worm (Slapper.B variant)                           [ Not found ]
    Danny-Boy's Abuse Kit                                    [ Not found ]
    Devil RootKit                                            [ Not found ]
    Diamorphine LKM                                          [ Not found ]
    Dica-Kit Rootkit                                         [ Not found ]
    Dreams Rootkit                                           [ Not found ]
    Duarawkz Rootkit                                         [ Not found ]
    Ebury backdoor                                           [ Not found ]
    Enye LKM                                                 [ Not found ]
    Flea Linux Rootkit                                       [ Not found ]
    Fu Rootkit                                               [ Not found ]
```

```
Fuck`it Rootkit                                 [ Not found ]
GasKit Rootkit                                  [ Not found ]
Heroin LKM                                      [ Not found ]
HjC Kit                                         [ Not found ]
ignoKit Rootkit                                 [ Not found ]
IntoXonia-NG Rootkit                            [ Not found ]
Irix Rootkit                                    [ Not found ]
Jynx Rootkit                                    [ Not found ]
Jynx2 Rootkit                                   [ Not found ]
KBeast Rootkit                                  [ Not found ]
Kitko Rootkit                                   [ Not found ]
Knark Rootkit                                   [ Not found ]
ld-linuxv.so Rootkit                            [ Not found ]
Li0n Worm                                       [ Not found ]
Lockit / LJK2 Rootkit                           [ Not found ]
Mokes backdoor                                  [ Not found ]
Mood-NT Rootkit                                 [ Not found ]
MRK Rootkit                                     [ Not found ]
Ni0 Rootkit                                     [ Not found ]
Ohhara Rootkit                                  [ Not found ]
Optic Kit (Tux) Worm                            [ Not found ]
Oz Rootkit                                      [ Not found ]
Phalanx Rootkit                                 [ Not found ]
Phalanx2 Rootkit                                [ Not found ]
Phalanx2 Rootkit (extended tests)               [ Not found ]
Portacelo Rootkit                               [ Not found ]
R3dstorm Toolkit                                [ Not found ]
RH-Sharpe's Rootkit                             [ Not found ]
RSHA's Rootkit                                  [ Not found ]
Scalper Worm                                    [ Not found ]
Sebek LKM                                       [ Not found ]
Shutdown Rootkit                                [ Not found ]
SHV4 Rootkit                                    [ Not found ]
SHV5 Rootkit                                    [ Not found ]
Sin Rootkit                                     [ Not found ]
Slapper Worm                                    [ Not found ]
Sneakin Rootkit                                 [ Not found ]
'Spanish' Rootkit                               [ Not found ]
Suckit Rootkit                                  [ Not found ]
Superkit Rootkit                                [ Not found ]
TBD (Telnet BackDoor)                           [ Not found ]
TeLeKiT Rootkit                                 [ Not found ]
T0rn Rootkit                                    [ Not found ]
trNkit Rootkit                                  [ Not found ]
Trojanit Kit                                    [ Not found ]
Tuxtendo Rootkit                                [ Not found ]
URK Rootkit                                     [ Not found ]
Vampire Rootkit                                 [ Not found ]
VcKit Rootkit                                   [ Not found ]
Volc Rootkit                                    [ Not found ]
Xzibit Rootkit                                  [ Not found ]
zaRwT.KiT Rootkit                               [ Not found ]
ZK Rootkit                                      [ Not found ]
```

En las imágenes anteriores se puede apreciar que la herramienta Rkhunter no ha encontrado ningún rootkit habiendo escaneado 75 rootkits.

```
Performing additional rootkit checks
  Suckit Rootkit additional checks                          [ OK ]
  Checking for possible rootkit files and directories       [ None found ]
  Checking for possible rootkit strings                     [ None found ]

Performing malware checks
  Checking running processes for suspicious files           [ None found ]
  Checking for login backdoors                              [ None found ]
  Checking for sniffer log files                            [ None found ]
  Checking for suspicious directories                       [ None found ]
  Checking for suspicious (large) shared memory segments    [ Warning ]
  Checking for Apache backdoor                              [ Not found ]

Performing Linux specific checks
  Checking loaded kernel modules                            [ OK ]
  Checking kernel module names                              [ OK ]
```

Lo que ha encontrado han sido segmentos grandes de memoria compartida que son los tres procesos de la foto de abajo, así que no es peligroso.

```
Warning: The following suspicious (large) shared memory segments have been found:
         Process: /usr/bin/mate-panel    PID: 1158    Owner: debian    Size: 4.0MB (configured size allowed: 1.0MB)
         Process: /usr/bin/caja    PID: 1177    Owner: debian    Size: 32MB (configured size allowed: 1.0MB)
         Process: /usr/bin/mate-terminal    PID: 1910    Owner: debian    Size: 4.0MB (configured size allowed: 1.0
```

Rkhunter tiene una configuración interna antigua que hace que considere cualquier segmento de memoria compartida mayor a 1 MB sospechoso, porque antiguamente los rootkits usaban estos espacios para esconderse.

Sin embargo, las aplicaciones gráficas modernas necesitan más de 1 MB para funcionar correctamente.

```
Rootkit checks...
    Rootkits checked : 497
    Possible rootkits: 3

Applications checks...
    All checks skipped

The system checks took: 7 minutes and 48 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)
```

Los tres posibles rootkits que ha detectado son los tres procesos que consumen más memoria de la que deberían según los antiguos parámetros Rkhunter que todavía usa.

Así que no se ha detectado ningún rootkit.

Identificación de cambios

Se busca si hay nuevos usuarios creados por el atacante.

Para saber todos los usuarios creados en este sistema se usa el comando `cat /etc/passwd` que nos lista todos los usuarios del sistema.

```
debian@debian:/etc$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:110:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:103:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:104:112:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:105:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:106:114:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:107:117::/var/lib/saned:/usr/sbin/nologin
lightdm:x:108:118:Light Display Manager:/var/lib/lightdm:/bin/false
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:109:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:110:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
debian:x:1000:1000:4geeks,,,:/home/debian:/bin/bash
mysql:x:111:121:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
ftp:x:113:122:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
Debian-exim:x:114:123::/var/spool/exim4:/usr/sbin/nologin
```

Se revisan todos los nombres de usuario y no se detecta ningún usuario fuera de lo normal, todos son legítimos.

Hay dos tipos de usuarios:

- Los usuarios que tienen permiso para acceder como personas, solo hay dos usuarios que son root y debian que tienen este permiso, esto se sabe porque acaban en **/bin/bash**.
- Los usuarios que **no** tienen permiso para acceder como personas, que son la mayoría de usuarios, esto se sabe porque acaban en **/bin/false** o **/sbin/nologin**. A estos usuarios no los pueden suplantar los ciberdelincuentes.

Se buscan backdoors creadas por el ciberatacante de la siguiente manera:

- No se detectan conexiones SSH a través del usuario debian o root.
- Se usa el comando `crontab -l` para buscar tareas programadas y no se encuentra ninguna para el usuario debian y usuario root.

```
debian@debian:/$ crontab -l
no crontab for debian
debian@debian:/$ sudo su
root@debian:/# crontab -l
no crontab for root
```

Por lo tanto, no se detectan backdoors.

La herramienta Rkhunter ha detectado que está permitido el acceso root vía SSH

```
Performing system configuration file checks
  Checking for an SSH configuration file                  [ Found ]
  Checking if SSH root access is allowed                  [ Warning ]
  Checking if SSH protocol v1 is allowed                  [ Not set ]
  Checking for other suspicious configuration settings    [ None found ]
  Checking for a running system logging daemon            [ Found ]
  Checking for a system logging configuration file        [ Found ]
```

Al estar el puerto abierto de SSH no hace falta crear una backdoor ya que tienes una forma de acceso conocida, se podría considerar el acceso root vía SSH como la backdoor ya que hace esa función sin haber sido creada maliciosamente para esa función.

Actualización de la seguridad

Se usan los comandos:

Sudo apt update

```
debian@debian:~$ sudo apt update
```

Sudo apt upgrade

```
debian@debian:~$ sudo apt upgrade
```

Y así nos aseguramos que los programas están actualizados y el sistema, en este caso Debian, esté al día con las últimas correcciones de seguridad y funcionalidades, manteniendo el sistema estable y seguro.

Se debe cerrar el puerto innecesario 21.

En el puerto 21 se usa el servicio **FTP** para la transferencia de archivos.

- Este protocolo es antiguo y poco seguro ya que envía las contraseñas en texto plano, sin cifrar.
- Tiene una versión más segura que es el **SFTP.**
- Por el puerto 22 también se puede realizar un intercambio de archivos, en este caso sería de forma segura mediante **SFTP**.

El puerto se cierra con el comando en el firewall UFW `sudo ufw deny 21/tcp` y en el firewall iptables sería el comando `sudo iptables -A INPUT -p tcp --dport 21 -j DROP`.

En el puerto 22 hay que realizar unos ajustes para securizarlo.

En el puerto 22 se usa **SSH** para el acceso remoto seguro.

Se debe quitar el acceso root vía SSH

Quitar el acceso root vía SSH se realiza de la siguiente manera:

Se usa el comando `sudo nano /etc/ssh/sshd_config`.

```
debian@debian:~$ sudo nano /etc/ssh/sshd_config
```

Dentro del archivo sshd_config hay que buscar la línea PermitRootLogin, como está permitido el acceso root pondrá **yes**, hay que cambiar el **yes** por un **no**, de esta manera no se permite el acceso root vía SSH.

Se guarda los cambios en el archivo con Ctrl + O e Intro y se sale del archivo con Ctrl+X.

Se debe reiniciar el servicio de SSH con el siguiente comando: sudo systemctl restart ssh

```
debian@debian:~$ sudo systemctl restart ssh
```