

# SSO Práctica 1

Andrés Merlo Trujillo

## Índice

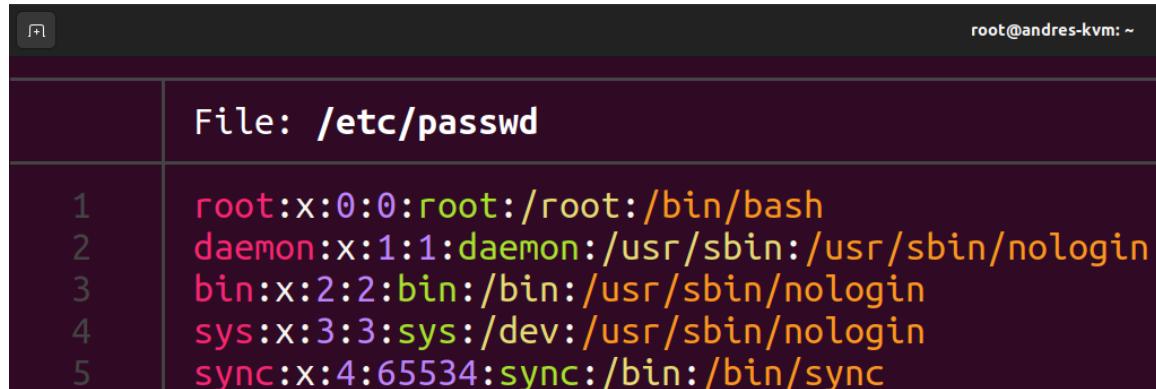
<b>Ejercicio 1</b>	<b>2</b>
/etc/passwd . . . . .	2
/etc/group . . . . .	3
/etc/shadow . . . . .	4
/etc/gshadow . . . . .	5
<b>Ejercicio 2</b>	<b>5</b>
<b>Ejercicio 3</b>	<b>8</b>
<b>Ejercicio 4</b>	<b>8</b>
/etc/pam.d/chfn . . . . .	9
/etc/pam.d/chsh . . . . .	10
<b>Ejercicio 5</b>	<b>11</b>
Apartado A . . . . .	11
Apartado B . . . . .	12
<b>Ejercicio 6</b>	<b>12</b>
<b>Ejercicio 7</b>	<b>14</b>
<b>Ejercicio 8</b>	<b>14</b>
/var/log/lastlog . . . . .	15
/var/log/wtmp . . . . .	15
/var/log/utmp . . . . .	17
/var/log/btmp . . . . .	17
/var/log/sudo . . . . .	18
/var/log/messages . . . . .	18
<b>Ejercicio 9</b>	<b>19</b>
PC de mi casa . . . . .	19
PC de prácticas (máquina virtual) . . . . .	22

## Ejercicio 1

A continuación, voy a explicar el formato y el significado de cada uno de los campos. Para ello, voy a dividir cada archivo en subsecciones:

### /etc/passwd

**Formato:** nombre\_login:contra\_encriptada:UID:GID:comentario:shell



The screenshot shows a terminal window with the title 'File: /etc/passwd'. The window contains the following text:

	File: /etc/passwd
1	root:x:0:0:root:/root:/bin/bash
2	daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3	bin:x:2:2:bin:/bin:/usr/sbin/nologin
4	sys:x:3:3:sys:/dev:/usr/sbin/nologin
5	sync:x:4:65534:sync:/bin:/bin sync

Figura 1: Ejemplo de entradas en el archivo.

Este fichero está formado por líneas de 7 campos separados por “:”. Los campos y sus significados son los siguientes:

1. **Nombre de login:** Nombre de usuario.
2. **Contraseña encriptada opcional:** Contraseña encriptada del usuario. Si este campo tiene la letra “x” minúscula, significa que la contraseña se almacena en `/etc/shadow`.  
Si se encuentra vacío, significa que no hace falta contraseña para autenticar.  
Si comienza en exclamación, significa que la contraseña ha sido bloqueada.  
Además, si contiene una exclamación o un asterisco (\*), significa que el usuario no podrá usar la contraseña para iniciar sesión (pero puede usar otro medio).
3. **User ID numérico:** ID del usuario.
4. **Group ID numérico:** ID del grupo al que pertenece.
5. **Nombre de usuario o campo de comentario:** Este campo sirve para poder poner un comentario sobre el usuario (por ejemplo: acción que realiza, para evitar confusión con dos usuarios similares, etc.).
6. **Directorio home del usuario:** Directorio que será el home privado del usuario. Además sirve para poner la variable de entorno \$HOME
7. **Interprete opcional de comando de usuario:** Shell que usará el usuario por defecto (bash, sh, zsh, fish, etc.). Además, pondrá la variable de entorno \$SHELL a este valor.

## /etc/group

Formato: nombre\_grupo:contra:GID:usuario1,usuario2,...

File: /etc/group	
1	root:x:0:
2	daemon:x:1:
3	bin:x:2:
4	sys:x:3:
5	adm:x:4:syslog, andres

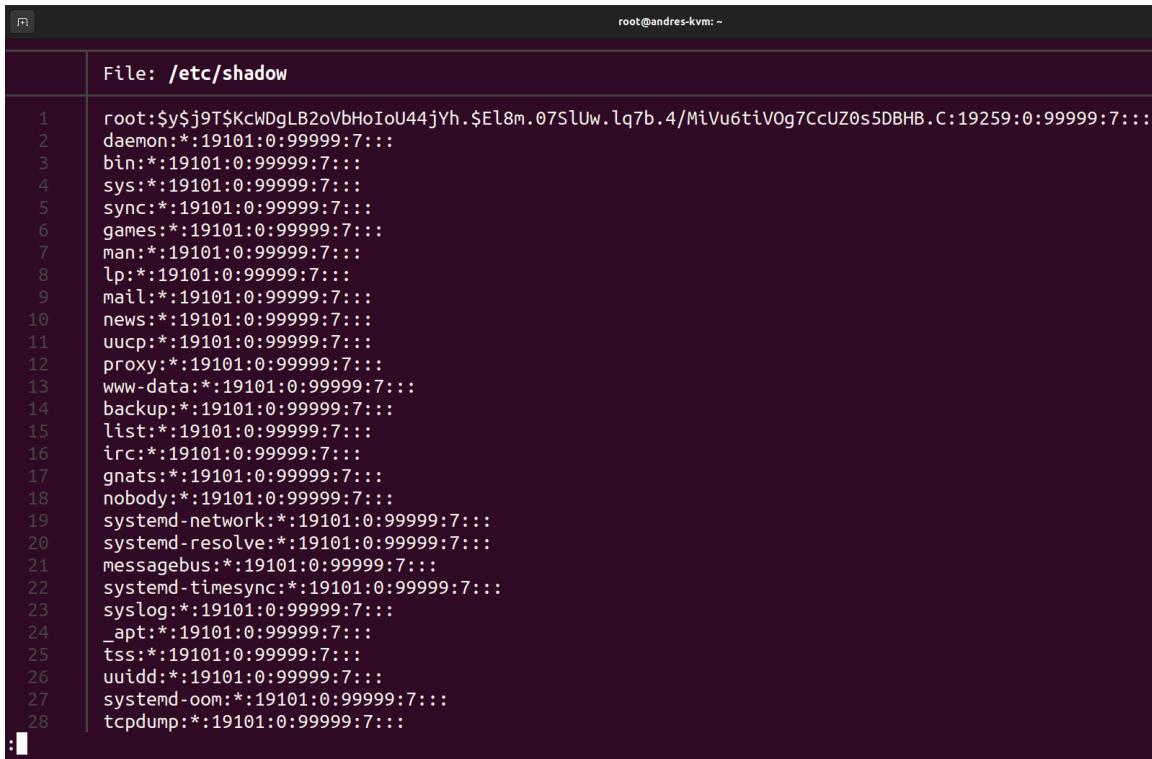
Figura 2: Ejemplo de entradas en el archivo.

Este fichero está formado por 4 campos separados por “.”. EL significado de cada campo es el siguiente:

1. **Nombre del grupo:** Nombre del grupo. Este nombre debe ser único en el sistema.
2. **Contraseña:** Contraseña del grupo. Si es una letra “x” minúscula significa que la contraseña encriptada se encuentra en /etc/gpasswd.
3. **Group ID:** Indica el ID del grupo. Este valor debe ser único en el sistema.
4. **Usuarios:** Lista de usuarios separados por coma (“,”) los cuales son miembros del grupo.

## /etc/shadow

Formato: login:pass:last\_change:min\_age:max\_age:pass\_warn:pass\_inact:acc\_exp:reserved



The screenshot shows a terminal window with the title 'File: /etc/shadow'. The terminal prompt is 'root@andres-kvm: ~'. The content of the /etc/shadow file is displayed, showing 28 entries, each consisting of nine fields separated by colons. The first few entries are:

```
1 root:$y$j9T$KcWDgLB2oVbHoIoU44jYh.$El8m.07Sluw.lq7b.4/MiVu6tiV0g7CcUZ0s5DBHB.C:19259:0:99999:7:::
2 daemon:*:19101:0:99999:7:::
3 bin:*:19101:0:99999:7:::
4 sys:*:19101:0:99999:7:::
5 sync:*:19101:0:99999:7:::
6 games:*:19101:0:99999:7:::
7 man:*:19101:0:99999:7:::
8 lp:*:19101:0:99999:7:::
9 mail:*:19101:0:99999:7:::
10 news:*:19101:0:99999:7:::
11 uucp:*:19101:0:99999:7:::
12 proxy:*:19101:0:99999:7:::
13 www-data:*:19101:0:99999:7:::
14 backup:*:19101:0:99999:7:::
15 list:*:19101:0:99999:7:::
16 irc:*:19101:0:99999:7:::
17 gnats:*:19101:0:99999:7:::
18 nobody:*:19101:0:99999:7:::
19 systemd-network:*:19101:0:99999:7:::
20 systemd-resolve:*:19101:0:99999:7:::
21 messagebus:*:19101:0:99999:7:::
22 systemd-timesync:*:19101:0:99999:7:::
23 syslog:*:19101:0:99999:7:::
24 _apt:*:19101:0:99999:7:::
25 tss:*:19101:0:99999:7:::
26 uidd:*:19101:0:99999:7:::
27 systemd-oom:*:19101:0:99999:7:::
28 tcpdump:*:19101:0:99999:7:::
```

Figura 3: Ejemplo de entradas en el archivo.

Este fichero está formado por líneas de 9 campos separados por “:”. Los campos y sus significados son los siguientes:

1. **login name (nombre de login):** Nombre de la cuenta del usuario. Debe existir en el sistema.
2. **encrypted password (contraseña encriptada):** Contraseña encriptada del usuario especificado en “login name”. Si este campo está vacío, significa que ese usuario no requiere contraseña para iniciar sesión.  
Además, en caso de que la contraseña comience con una exclamación (“!”), significa que la contraseña ha sido bloqueada.  
Por último, si la contraseña contiene el carácter de exclamación mencionado anteriormente o asterisco (“\*”), significa que no puede iniciar sesión (si es exclamación también se cumple lo de arriba).
3. **date of last password change (fecha del último cambio de contraseña):** El último cambio de contraseña, expresado como el número de días desde el epoch (1 de enero de 1970). Además, si el valor es 0 significa que el usuario debe cambiar la contraseña en el próximo login. En cambio, si el campo está vacío significa que las contraseñas no tienen edad (y por tanto no se cumplen estas restricciones).
4. **minimum password age (edad mínima de la contraseña):** Número de días que el usuario tiene que esperar antes de poder cambiar la contraseña de nuevo. Un valor 0 ó vacío indica que no hay un mínimo de días.
5. **maximum password age (edad máxima de la contraseña):** Número máximo de días en los cuales la contraseña “caduca” (tiene que cambiarla). Al pasar este número de días, el sistema pedirá al usuario que cambie la contraseña.  
Si el valor máximo es mayor que el del campo anterior, el usuario no podrá cambiar su contraseña.

Por último, si el campo está vacío, se deshabilitara este servicio junto con “password warning period” y “password inactivity period”.

6. **password warning period (periodo de advertencia de la contraseña):** El número de días antes de que la contraseña “caduque” durante los cuales se le advierte al usuario.  
Un valor 0 o cadena vacía indica que no habrá advertencias.
7. **password inactivity period (periodo de inactividad de la contraseña):** Número de días después de que la contraseña haya “caducado” en el cual debería ser aceptada. Al pasar este periodo, el usuario no podrá iniciar sesión.  
Un campo vacío indica que no se cumple esta regla.
8. **account expiration date (fecha de caducidad de la cuenta):** La fecha en la que la cuenta expira. Esta fecha se expresa como el número de días desde el epoch.  
La diferencia con la caducidad de una contraseña es que, si la cuenta expira, no podrá iniciar sesión de ninguna forma, mientras que si la contraseña expira, tendrá otros medios para iniciar sesión.  
El campo vacío indica que la cuenta no expira. Además, no se debe usar el valor 0, ya que se puede interpretar como que la cuenta expira en el epoch o que no expira.
9. **reserved field (campo reservado):** Este campo está reservado para usos futuros.

## /etc/gshadow

**Formato:** group\_name:encrypted\_pass:admin1,admin2,...:member1,member2,...

File: /etc/gshadow	
1	root:*::
2	daemon:*::
3	bin:*::
4	sys:*::
5	adm:*::syslog, andres

Figura 4: Ejemplo de entradas en el archivo.

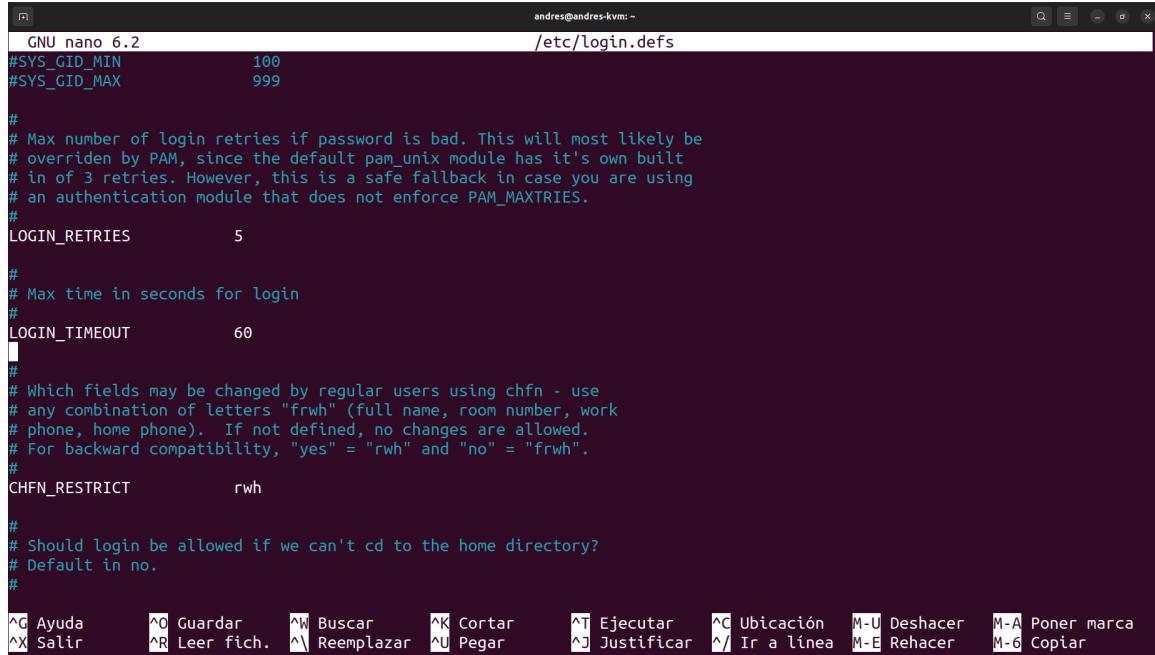
Este fichero está también formado por 4 campos separados por el símbolo “:”. El significado de cada campo es el siguiente:

1. **Nombre del grupo:** Nombre del grupo. Debe existir en el sistema.
2. **Contraseña encriptada:** Contraseña encriptada que sirve para que un usuario que no es miembro del grupo obtenga los permisos.  
Si el campo está vacío, entonces cualquier usuario puede obtener los privilegios del grupo.  
Si la contraseña comienza por una exclamación, significa que esta está bloqueada.  
Si contiene una exclamación o asterisco, los usuarios no podrán acceder al grupo si no están en él.
3. **Administradores:** Lista de usuarios separados por coma que puede realizar operaciones como cambiar la contraseña del grupo o administrar los usuarios del mismo.
4. **Miembros:** Lista de usuarios separados por coma. Los miembros del grupo pueden acceder al mismo sin necesitar la contraseña.

## Ejercicio 2

En este ejercicio se pide modificar el valor de la variable LOGIN\_TIMEOUT y comprobar sus efectos con un usuario nuevo que se haya creado manualmente.

Para ello, modiflico la variable, que estaba por defecto a **60 segundos**:



```
GNU nano 6.2                               andres@andres-kvm: ~
/etc/login.defs
#SYS_GID_MIN          100
#SYS_GID_MAX          999

#
# Max number of login retries if password is bad. This will most likely be
# overriden by PAM, since the default pam_unix module has it's own built
# in of 3 retries. However, this is a safe fallback in case you are using
# an authentication module that does not enforce PAM_MAXTRIES.
#
LOGIN_RETRIES          5

#
# Max time in seconds for login
#
LOGIN_TIMEOUT          60

#
# Which fields may be changed by regular users using chfn - use
# any combination of letters "frwh" (full name, room number, work
# phone, home phone). If not defined, no changes are allowed.
# For backward compatibility, "yes" = "rwh" and "no" = "frwh".
#
CHFN_RESTRICT          rwh

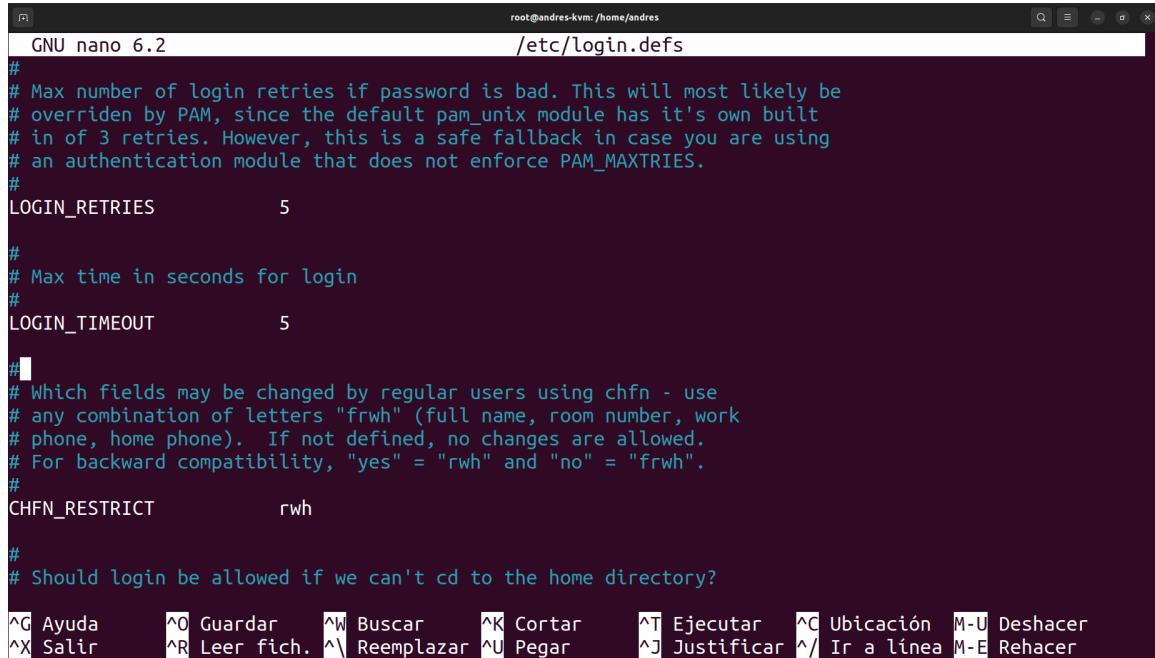
#
# Should login be allowed if we can't cd to the home directory?
# Default is no.
#



^G Ayuda      ^O Guardar     ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación  M-U Deshacer  M-A Poner marca
^X Salir      ^R Leer fich.  ^\ Reemplazar  ^U Pegar      ^J Justificar ^/ Ir a línea M-E Rehacer   M-6 Copiar
```

Figura 5: Valor por defecto.

Y lo cambio a otro valor, por ejemplo, **5 segundos**:



```
root@andres-kvm: /home/andres
GNU nano 6.2                               root@andres-kvm: /home/andres
/etc/login.defs
# Max number of login retries if password is bad. This will most likely be
# overriden by PAM, since the default pam_unix module has it's own built
# in of 3 retries. However, this is a safe fallback in case you are using
# an authentication module that does not enforce PAM_MAXTRIES.
#
LOGIN_RETRIES          5

#
# Max time in seconds for login
#
LOGIN_TIMEOUT          5

#
# Which fields may be changed by regular users using chfn - use
# any combination of letters "frwh" (full name, room number, work
# phone, home phone). If not defined, no changes are allowed.
# For backward compatibility, "yes" = "rwh" and "no" = "frwh".
#
CHFN_RESTRICT          rwh

#
# Should login be allowed if we can't cd to the home directory?



^G Ayuda      ^O Guardar     ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación  M-U Deshacer  M-A Poner marca
^X Salir      ^R Leer fich.  ^\ Reemplazar  ^U Pegar      ^J Justificar ^/ Ir a línea M-E Rehacer   M-6 Copiar
```

Figura 6: Valor cambiado a 5 segundos.

A continuación, creo el usuario llamado “prueba”, le cambio la contraseña y hago login con él desde la terminal. Cuando se encuentre en la parte de pedir la contraseña de este usuario nuevo, se espera un tiempo hasta que la terminal devuelva un mensaje:

```
root@andres-kvm:~# useradd prueba
root@andres-kvm:~# passwd prueba
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
root@andres-kvm:~# login prueba
Contraseña:
El acceso caducó después de 5 segundos.
root@andres-kvm:~#
```

Como se puede ver, pone que han pasado 5 segundos y el acceso ha caducado.

Ahora, pruebo con otro valor, por ejemplo **12 segundos**:

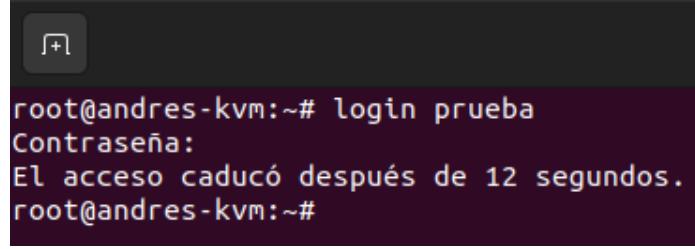
```
GNU nano 6.2
UID_MAX          60000
# System accounts
#SYS_UID_MIN      100
#SYS_UID_MAX      999

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN          1000
GID_MAX          60000
# System accounts
#SYS_GID_MIN      100
#SYS_GID_MAX      999

#
# Max number of login retries if password is bad. This will most likely be
# overridden by PAM, since the default pam_unix module has its own built
# in of 3 retries. However, this is a safe fallback in case you are using
# an authentication module that does not enforce PAM_MAXTRIES.
#
LOGIN_RETRIES      5

#
# Max time in seconds for login
#
LOGIN_TIMEOUT     12
```

E intento iniciar sesión de nuevo con el usuario “prueba” y espero en la parte de la contraseña.



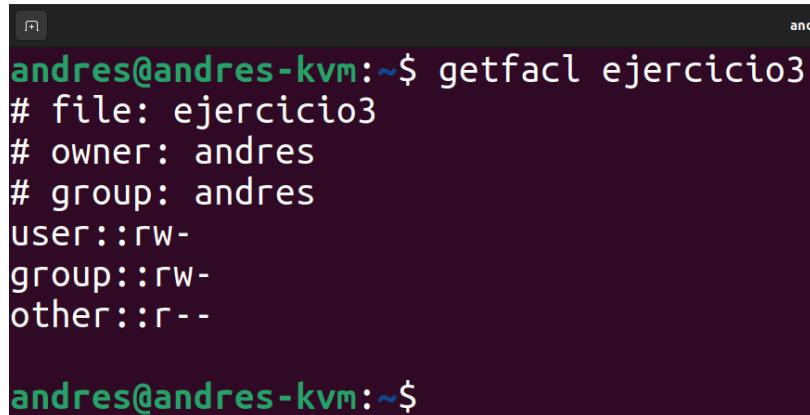
```
root@andres-kvm:~# login prueba
Contraseña:
El acceso caducó después de 12 segundos.
root@andres-kvm:~#
```

Como se puede ver, el timeout ahora es distinto.

### Ejercicio 3

En este ejercicio se pide crear un archivo y darle, mediante un ACL, permisos de lectura y escritura al usuario creado (en mi caso sigue siendo “prueba”). Para ello, mediante la orden `touch` creo el archivo denominado `ejercicio3`.

Ahora bien, al menos en Ubuntu 22.04 no están las órdenes `getacl/setacl`, sino que se llaman `getfacl/setfacl`. El resultado no varía y tienen las mismas sintaxis.

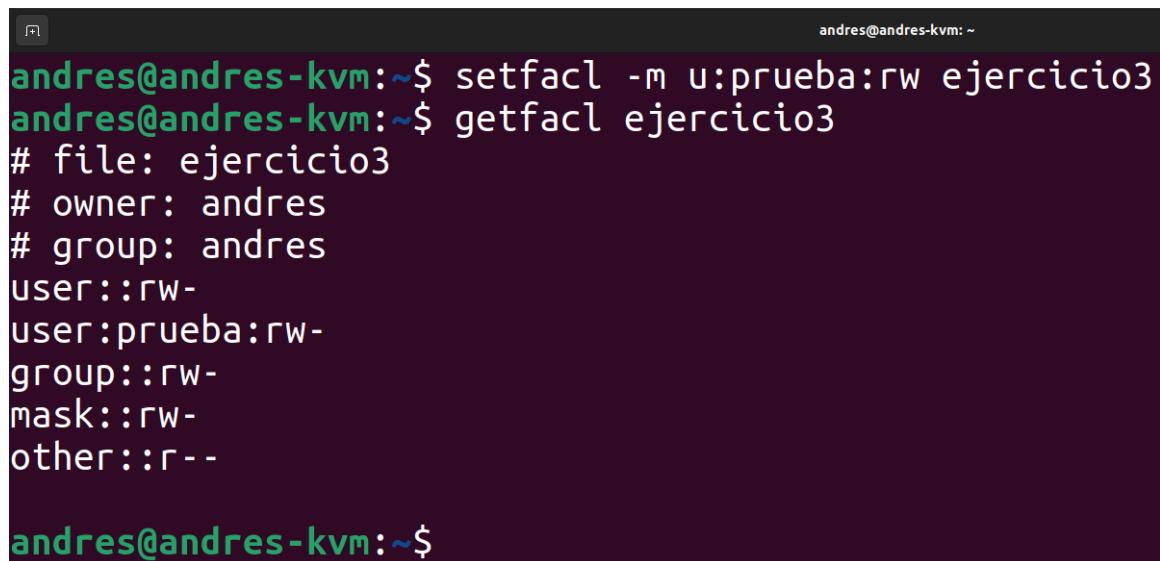


```
andres@andres-kvm:~$ getfacl ejercicio3
# file: ejercicio3
# owner: andres
# group: andres
user::rw-
group::rw-
other::r--
```

andres@andres-kvm:~\$

Figura 7: Se puede ver que solo el usuario “andres” tiene los permisos

Ahora, con la orden `setfacl -m u:prueba:rw ejercicio3` se le dará al usuario “prueba” permisos “rw”. Y de nuevo mostramos con `getfacl` el archivo anterior:



```
andres@andres-kvm:~$ setfacl -m u:prueba:rw ejercicio3
andres@andres-kvm:~$ getfacl ejercicio3
# file: ejercicio3
# owner: andres
# group: andres
user::rw-
user:prueba:rw-
group::rw-
mask::rw-
other::r--
```

andres@andres-kvm:~\$

Como se puede observar, ahora aparece una línea que indica que el usuario “prueba” tiene permisos “rw”.

## Ejercicio 4

Con el comando `ls` muestro los archivos que se encuentran en el directorio `/etc/pam.d`:



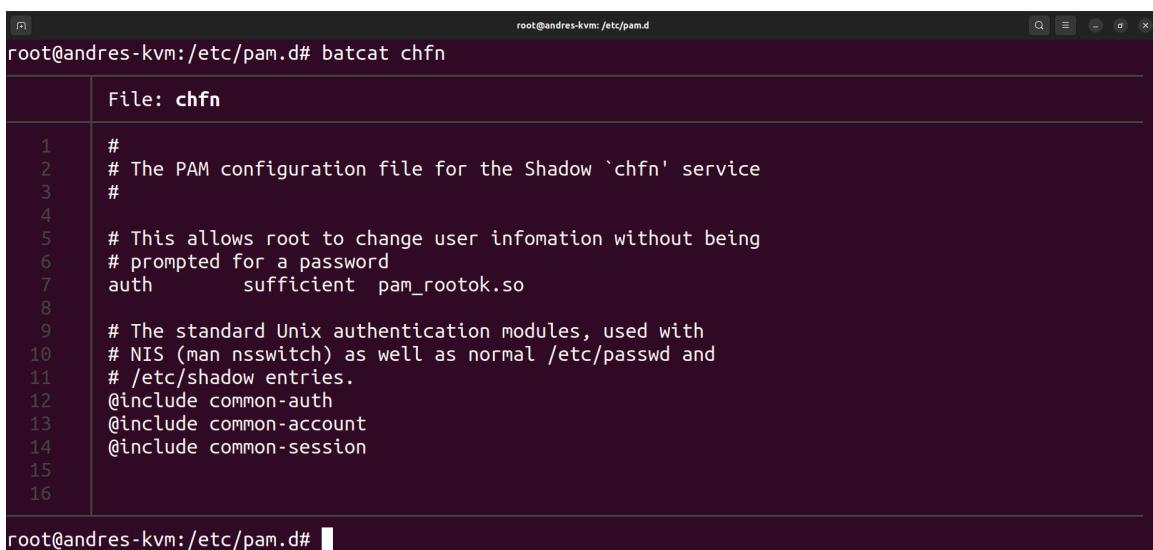
```
andres@andres-kvm:~$ ls /etc/pam.d
chfn      common-session-noninteractive  gdm-smartcard      passwd    sudo
chpasswd   cron                  gdm-smartcard-pkcs11-exclusive  polkit-1  sudo-i
chsh      cups                  gdm-smartcard-sssd      ppp       su-l
common-account  gdm-autologin      gdm-smartcard-sssd-or-password  runuser   runuser-l
common-auth    gdm-fingerprint    login                 runuser-l
common-password gdm-launch-environment newusers  sshd
common-session  gdm-password     other
andres@andres-kvm:~$
```

A continuación explicaré dos archivos:

### `/etc/pam.d/chfn`

Permite cambiar la información personal de un usuario tales como: el nombre, el número de teléfono, de habitación, etc. Estos datos luego pueden ser leídos por comandos como `finger`.

El contenido del archivo es:



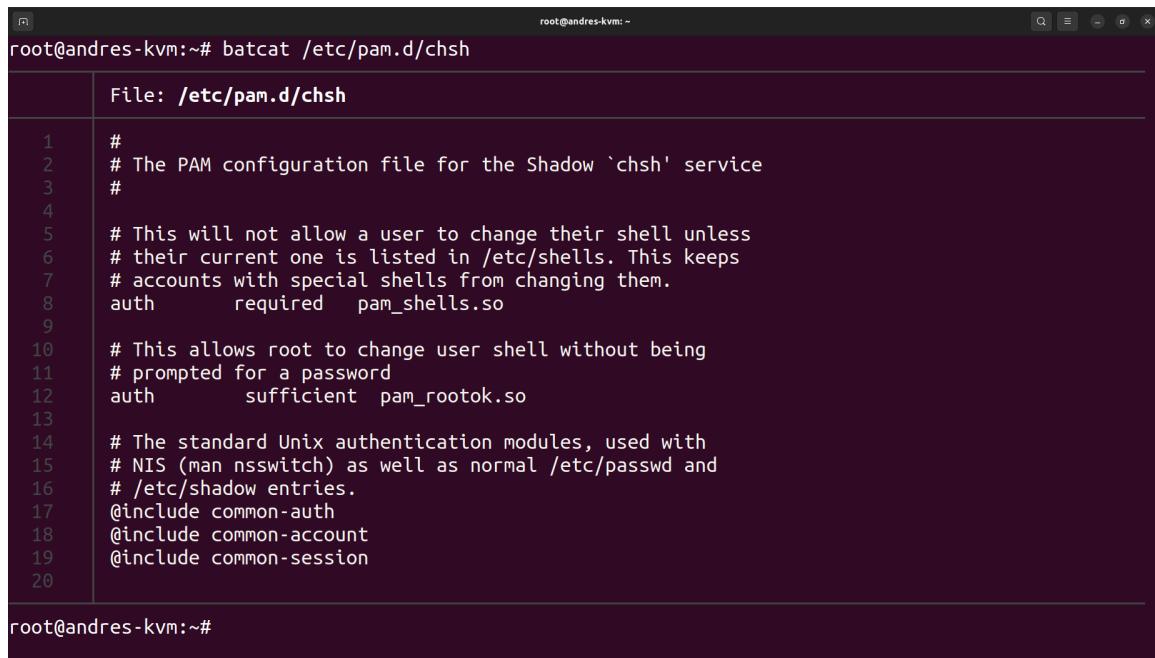
```
root@andres-kvm:/etc/pam.d# batcat chfn
File: chfn
1 #
2 # The PAM configuration file for the Shadow 'chfn' service
3 #
4
5 # This allows root to change user infomation without being
6 # prompted for a password
7 auth      sufficient pam_rootok.so
8
9 # The standard Unix authentication modules, used with
10 # NIS (man nsswitch) as well as normal /etc/passwd and
11 # /etc/shadow entries.
12 @include common-auth
13 @include common-account
14 @include common-session
15
16
root@andres-kvm:/etc/pam.d#
```

La función de la línea 7 es para no pedir la contraseña al usuario root cuando esté usando este comando. Para ello, hace uso del campo de control `sufficient`, que hace que si tiene éxito retorne sin ejecutar más módulos. Además, hace uso del módulo `pam_rootok.so` que hace que solo tenga éxito si el usuario tiene el UID a 0 (es el usuario root).

## /etc/pam.d/chsh

El comando `chsh` permite cambiar la shell por defecto del usuario que lo invoca. Si no se le pasa ningún parámetro se activa el modo interactivo para realizar el cambio de shell.

El contenido del archivo es el siguiente:



The screenshot shows a terminal window with the title bar "root@andres-kvm: ~". The command "batcat /etc/pam.d/chsh" is run, displaying the file's content. The file contains PAM configuration code for the 'chsh' service. Lines 1 through 20 show the configuration, with line 8 specifically mentioning the requirement for the shell to be listed in /etc/shells. Line 12 shows the use of pam\_rootok.so for root users. The file concludes with three @include directives pointing to common-auth, common-account, and common-session modules.

```
File: /etc/pam.d/chsh
1 #
2 # The PAM configuration file for the Shadow `chsh` service
3 #
4 #
5 # This will not allow a user to change their shell unless
6 # their current one is listed in /etc/shells. This keeps
7 # accounts with special shells from changing them.
8 auth      required  pam_shells.so
9 #
10 # This allows root to change user shell without being
11 # prompted for a password
12 auth      sufficient pam_rootok.so
13 #
14 # The standard Unix authentication modules, used with
15 # NIS (man nsswitch) as well as normal /etc/passwd and
16 # /etc/shadow entries.
17 @include common-auth
18 @include common-account
19 @include common-session
```

Como se puede ver en la línea 8, esta llamada lo que hace es prohibir el cambio de shell a no ser que se encuentre listada en `/etc/shells`. Esto se consigue mediante el campo de control `required`, que provocará un fallo de autenticación en el sistema (ejecutará la línea siguiente, pero al ser irrelevante, no pasa nada) si el módulo falla. También se consigue mediante la llamada al módulo `pam_shells.so`, que hace que si la shell pasada como parámetro no se encuentra en `/etc/shells` dé un fallo.

La función de la línea 12 es de permitir al superusuario cambiar la shell sin ser necesario introducir la contraseña. Esto se realiza mediante el campo de control `sufficient` y el módulo `pam_rootok.so`. Con `sufficient`, cuando la orden tiene éxito retorna sin ejecutar los demás módulos. Además, con el módulo `pam_rootok.so` autoriza solo al usuario con el UID 0 (root).

## Ejercicio 5

### Apartado A

Es necesario modificar el archivo PAM `common-password` y en Ubuntu 22.04 ya como primera línea aparece el uso del módulo `pam_pwquality`.

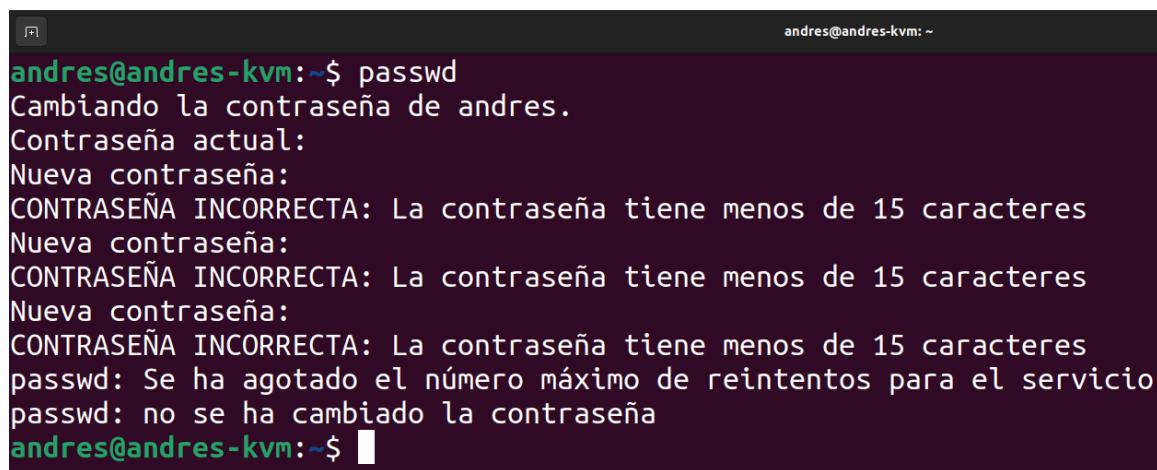
Ahora bien si leemos el manual de este módulo con `man 8 pam_pwquality` se puede ver que hay un argumento denominado `minlen` y que valor por defecto es **8**. No obstante, no se puede bajar del valor **4**, ya que es un límite que tiene `Cracklib` y mostrará que la contraseña es muy corta. Por eso, voy a poner el límite a **15 caracteres**.



```
GNU nano 6.2          /etc/pam.d/common-password
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password      requisite          pam_pwquality.so retry=3 minlen=15
```

Y ahora al usar el comando `passwd` y poner una contraseña con menos de 15 palabras, muestra un error:



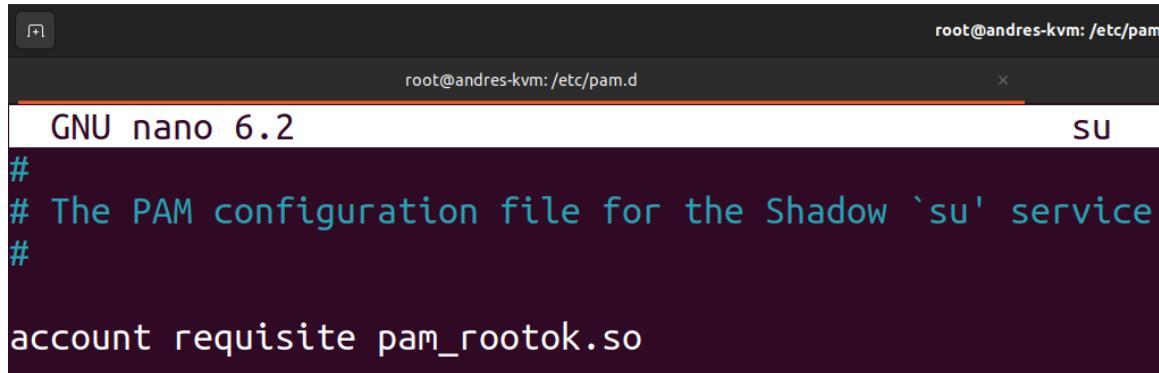
```
andres@andres-kvm:~$ passwd
Cambiando la contraseña de andres.
Contraseña actual:
Nueva contraseña:
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 15 caracteres
Nueva contraseña:
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 15 caracteres
Nueva contraseña:
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 15 caracteres
passwd: Se ha agotado el número máximo de reintentos para el servicio
passwd: no se ha cambiado la contraseña
andres@andres-kvm:~$
```

Y al agotarse los intentos (que son 3) se sale del programa.

## Apartado B

En esta parte he restringido el acceso al comando `su` para así evitar que un usuario que ponga el comando sin `sudo` pueda entrar. En cambio, si ponen `sudo su` sí van a poder entrar, pero esto es así porque son usuarios administradores (y es una decisión de diseño, ya que en otro caso no podría usar nadie `sudo`), en ese caso lo recomendable es deshabilitar el acceso al grupo `sudo` (en el caso de Ubuntu) para que no lo pueda usar (editando el archivo `sudoers` mediante el comando `visudo`).

Para conseguir esto, es necesario modificar el archivo `/etc/pam.d/su` y añadir la siguiente línea al principio:

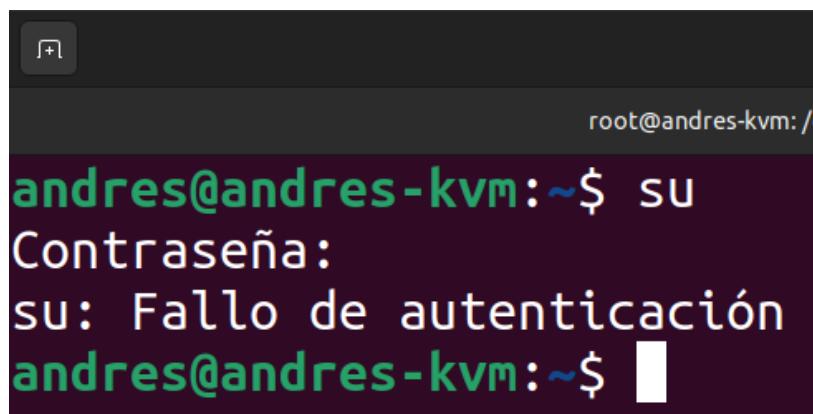


```
root@andres-kvm: /etc/pam
GNU nano 6.2
#
# The PAM configuration file for the Shadow `su' service
#
account requisite pam_rootok.so
```

Figura 8: Línea necesaria para que se deniegue el acceso al usuario “root”.

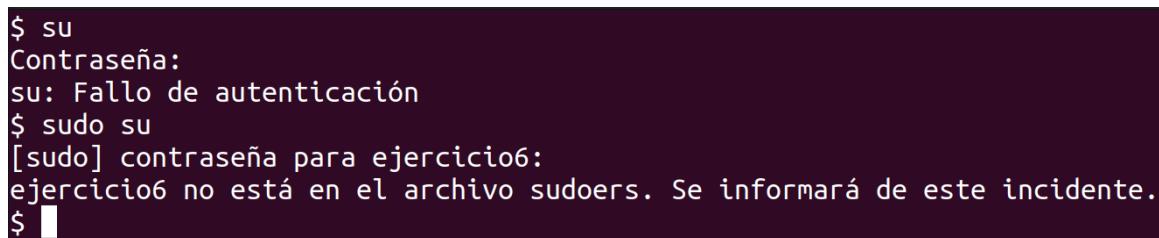
La línea que he añadido lo que hace es comprobar que la cuenta sea root (UID=0) y en caso de no serlo, no sigue ejecutando el archivo provocando un error de autenticación.

Ahora, al ejecutar el comando `su` con un usuario normal aparece lo siguiente:



```
root@andres-kvm: /
andres@andres-kvm:~$ su
Contraseña:
su: Fallo de autenticación
andres@andres-kvm:~$
```

En cambio, si el usuario puede usar `sudo`, si puede acceder.



```
$ su
Contraseña:
su: Fallo de autenticación
$ sudo su
[sudo] contraseña para ejercicio6:
ejercicio6 no está en el archivo sudoers. Se informará de este incidente.
$
```

Figura 9: El usuario que se ha creado en esta práctica no tiene permisos para usar “sudo” y por tanto no puede entrar de ninguna manera.

## Ejercicio 6

En Ubuntu 22.04 los cambios de contraseña no se almacenan en `/var/log/messages`, sino en `/var/log/auth.log`. [Enlace](#) a la guía.

Voy a crear el usuario “ejercicio6” y le voy a cambiar la contraseña:

```
root@andres-kvm:~# useradd ejercicio6
root@andres-kvm:~# passwd ejercicio6
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
root@andres-kvm:~# su ejercicio6
$ passwd
Cambiando la contraseña de ejercicio6.
Contraseña actual:
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
$ 
```

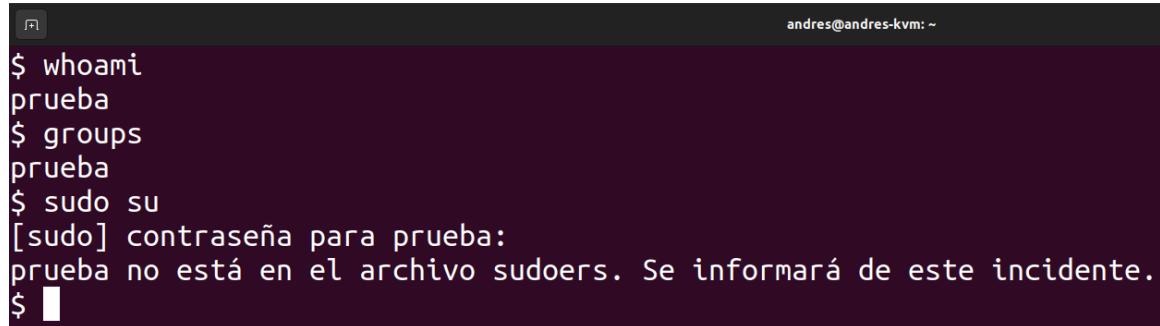
Y ahora, al mostrar el archivo `/var/log/auth.log` aparecen las siguientes líneas:

```
41 Sep 21 20:05:12 andres-kvm useradd[2779]: new group: name=ejercicio6, GID=1002
42 Sep 21 20:05:12 andres-kvm useradd[2779]: new user: name=ejercicio6, UID=1002, GID=1002, home=/home/ejercicio6, s
hell=/bin/sh, from=/dev/pts/1
43 Sep 21 20:05:30 andres-kvm passwd[2788]: pam_unix(passwd:chauthok): password changed for ejercicio6
44 Sep 21 20:05:30 andres-kvm passwd[2788]: gkr-pam: couldn't update the login keyring password: no old password was
entered
45 Sep 21 20:05:34 andres-kvm su: (to ejercicio6) root on pts/1
46 Sep 21 20:05:34 andres-kvm su: pam_unix(su:session): session opened for user ejercicio6(uid=1002) by andres(uid=0
)
47 Sep 21 20:05:46 andres-kvm passwd[2792]: pam_unix(passwd:chauthok): password changed for ejercicio6
48 Sep 21 20:05:46 andres-kvm passwd[2792]: gkr-pam: unable to locate daemon control file
49 Sep 21 20:06:39 andres-kvm su: pam_unix(su:session): session closed for user ejercicio6
```

## Ejercicio 7

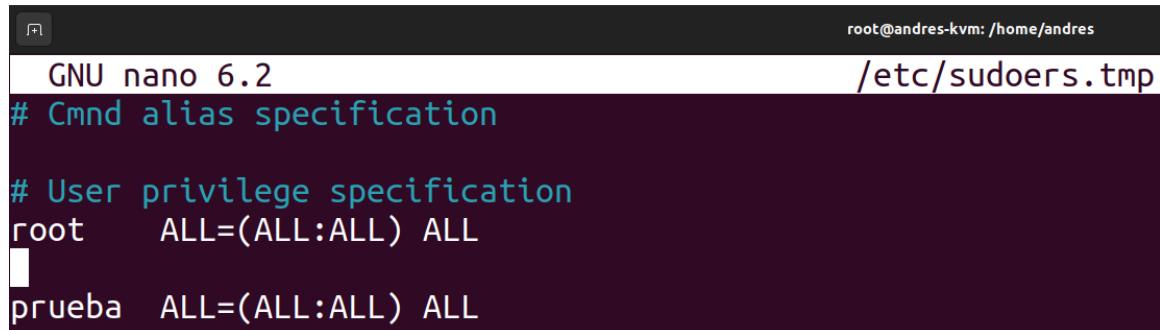
Para empezar, el propio archivo `sudoers` recomienda usar la orden `visudo`. Por tanto, es necesario usar `visudo` para que no haya problemas después. Además, por defecto usa el editor `vi`, esto se puede cambiar usando el comando siguiente: `EDITOR=nano visudo`

Ahora, voy a asignarle permisos para usar sudo al usuario “prueba” que no se encuentra en el grupo “sudo”, que es el que usa Ubuntu para dar permisos.



```
$ whoami
prueba
$ groups
prueba
$ sudo su
[sudo] contraseña para prueba:
prueba no está en el archivo sudoers. Se informará de este incidente.
$ 
```

Si añadimos la siguiente línea en el archivo `sudoers` tendremos acceso con `sudo`:

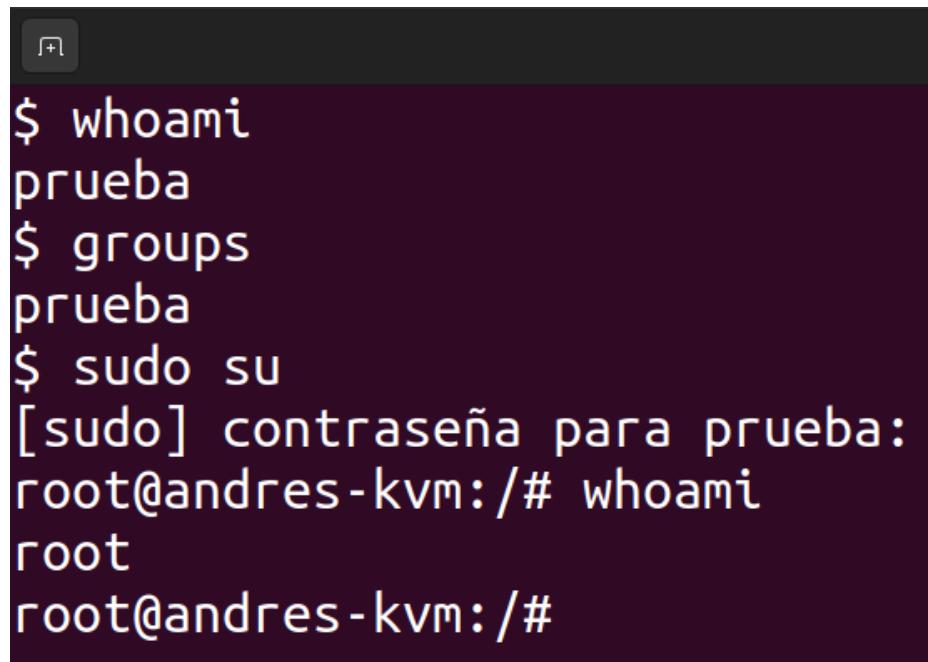


```
GNU nano 6.2                                     /etc/sudoers.tmp
# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
prueba  ALL=(ALL:ALL) ALL

```

Y ahora al hacer una prueba se puede ver que ya funciona:



```
$ whoami
prueba
$ groups
prueba
$ sudo su
[sudo] contraseña para prueba:
root@andres-kvm:/# whoami
root
root@andres-kvm:/# 
```

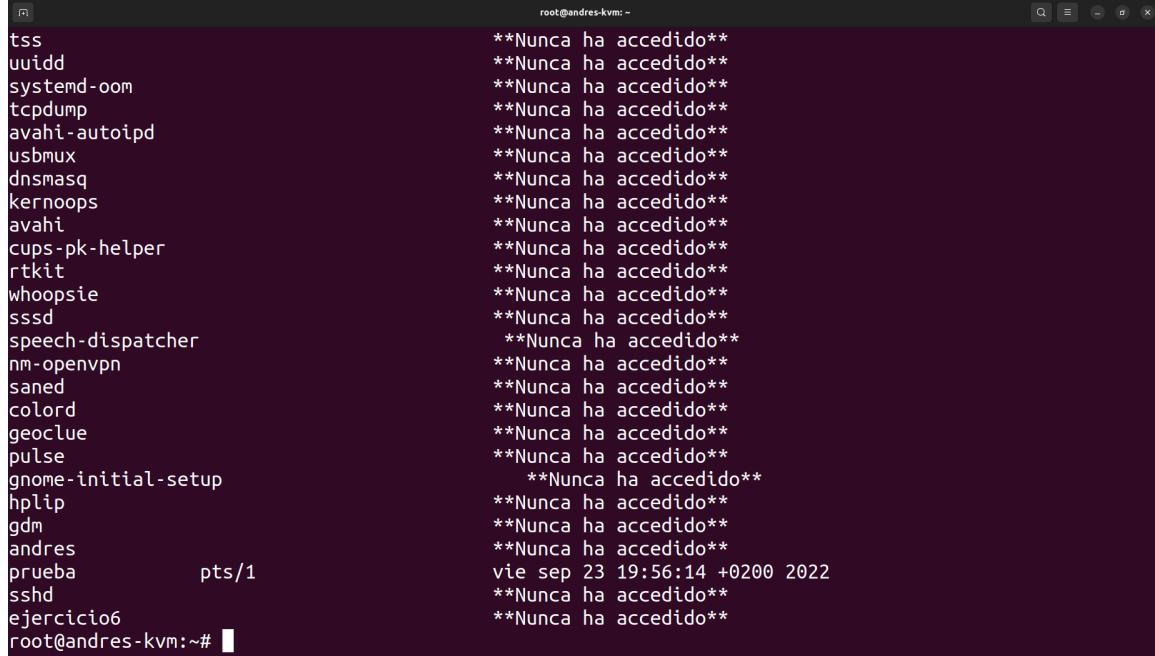
Figura 10: Puede usar el comando “sudo” sin estar en el grupo con el mismo nombre.

## Ejercicio 8

Voy a examinar cada uno de los archivos y comprobar que se registran eventos que realizaré. Para ello, voy a dividir la explicación en subsecciones para cada uno de los archivos.

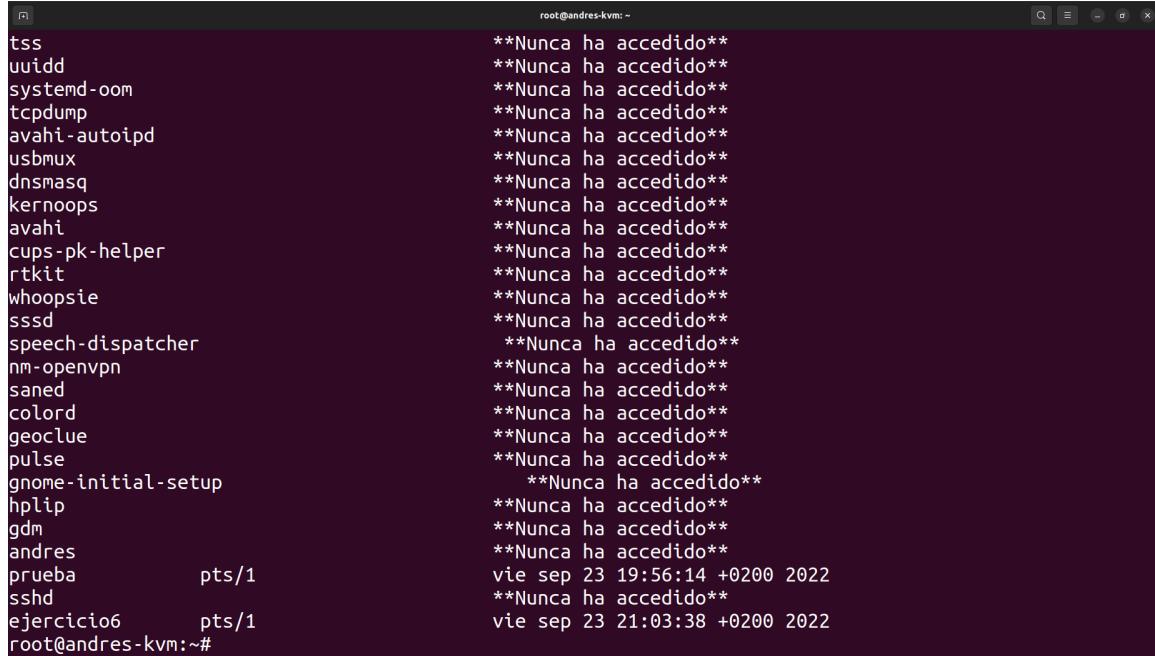
### /var/log/lastlog

Este archivo almacena información sobre el último inicio de sesión de los usuarios. Para acceder a la información es necesario utilizar el comando `lastlog`:



```
root@andres-kvm: ~
tss                                **Nunca ha accedido**
uuidd                               **Nunca ha accedido**
systemd-oom                          **Nunca ha accedido**
tcpdump                             **Nunca ha accedido**
avahi-autoipd                        **Nunca ha accedido**
usbmux                               **Nunca ha accedido**
dnsmasq                             **Nunca ha accedido**
kernooops                           **Nunca ha accedido**
avahi                               **Nunca ha accedido**
cups-pk-helper                       **Nunca ha accedido**
rtkit                                **Nunca ha accedido**
whoopsie                            **Nunca ha accedido**
sssd                                 **Nunca ha accedido**
speech-dispatcher                   **Nunca ha accedido**
nm-openvpn                           **Nunca ha accedido**
saned                                **Nunca ha accedido**
colord                               **Nunca ha accedido**
geoclue                              **Nunca ha accedido**
pulse                                **Nunca ha accedido**
gnome-initial-setup                 **Nunca ha accedido**
hplip                                **Nunca ha accedido**
gdm                                   **Nunca ha accedido**
andres                               **Nunca ha accedido**
prueba      pts/1                     vie sep 23 19:56:14 +0200 2022
sshd                                **Nunca ha accedido**
ejercicio6                           **Nunca ha accedido**
root@andres-kvm:~#
```

Como se puede ver, el usuario “ejercicio6” nunca ha iniciado sesión en el sistema. Ahora si inicio sesión y vuelvo a usar la orden `lastlog` aparece lo siguiente:



```
root@andres-kvm: ~
tss                                **Nunca ha accedido**
uuidd                               **Nunca ha accedido**
systemd-oom                          **Nunca ha accedido**
tcpdump                             **Nunca ha accedido**
avahi-autoipd                        **Nunca ha accedido**
usbmux                               **Nunca ha accedido**
dnsmasq                             **Nunca ha accedido**
kernooops                           **Nunca ha accedido**
avahi                               **Nunca ha accedido**
cups-pk-helper                       **Nunca ha accedido**
rtkit                                **Nunca ha accedido**
whoopsie                            **Nunca ha accedido**
sssd                                 **Nunca ha accedido**
speech-dispatcher                   **Nunca ha accedido**
nm-openvpn                           **Nunca ha accedido**
saned                                **Nunca ha accedido**
colord                               **Nunca ha accedido**
geoclue                              **Nunca ha accedido**
pulse                                **Nunca ha accedido**
gnome-initial-setup                 **Nunca ha accedido**
hplip                                **Nunca ha accedido**
gdm                                   **Nunca ha accedido**
andres                               **Nunca ha accedido**
prueba      pts/1                     vie sep 23 19:56:14 +0200 2022
sshd                                **Nunca ha accedido**
ejercicio6      pts/1                vie sep 23 21:03:38 +0200 2022
root@andres-kvm:~#
```

Figura 11: Ahora aparece la fecha del último inicio de sesión del usuario “ejercicio6”.

## /var/log/wtmp

Almacena los *login* y *logout* de los distintos usuarios del sistema. Se accede con el comando `last`.

```
root@andres-kvm: ~
andres  tty2      tty2      Wed Sep 21 17:08 - down  (00:56)
reboot system boot 5.15.0-48-generi Wed Sep 21 17:07 - 18:04  (00:57)
andres  tty2      tty2      Tue Sep 20 19:38 - down  (00:01)
reboot system boot 5.15.0-48-generi Tue Sep 20 19:38 - 19:40  (00:01)
andres  tty2      tty2      Tue Sep 20 18:06 - down  (01:24)
reboot system boot 5.15.0-48-generi Tue Sep 20 18:06 - 19:31  (01:24)
andres  tty2      tty2      Tue Sep 20 17:17 - down  (00:48)
reboot system boot 5.15.0-47-generi Tue Sep 20 17:17 - 18:06  (00:48)
andres  tty2      tty2      Tue Sep 20 16:28 - down  (00:00)
reboot system boot 5.15.0-47-generi Tue Sep 20 16:28 - 16:29  (00:00)
andres  tty2      tty2      Tue Sep 20 15:33 - down  (00:01)
reboot system boot 5.15.0-47-generi Tue Sep 20 15:32 - 15:34  (00:02)
andres  tty2      Mon Sep 19 22:21 - down  (00:03)
reboot system boot 5.15.0-47-generi Mon Sep 19 22:21 - 22:24  (00:03)
prueba  pts/0      Mon Sep 19 19:17 - 19:18  (00:01)
andres  tty2      Mon Sep 19 19:08 - crash  (03:13)
reboot system boot 5.15.0-47-generi Mon Sep 19 19:08 - 22:24  (03:16)
prueba  pts/1      Mon Sep 19 19:04 - 19:04  (00:00)
andres  tty2      Mon Sep 19 19:03 - down  (00:04)
reboot system boot 5.15.0-47-generi Mon Sep 19 19:03 - 19:08  (00:04)
andres  tty2      Mon Sep 19 18:30 - down  (00:03)
reboot system boot 5.15.0-47-generi Mon Sep 19 18:30 - 18:33  (00:03)
andres  tty2      Mon Sep 19 18:28 - down  (00:01)
reboot system boot 5.15.0-47-generi Mon Sep 19 18:27 - 18:29  (00:01)

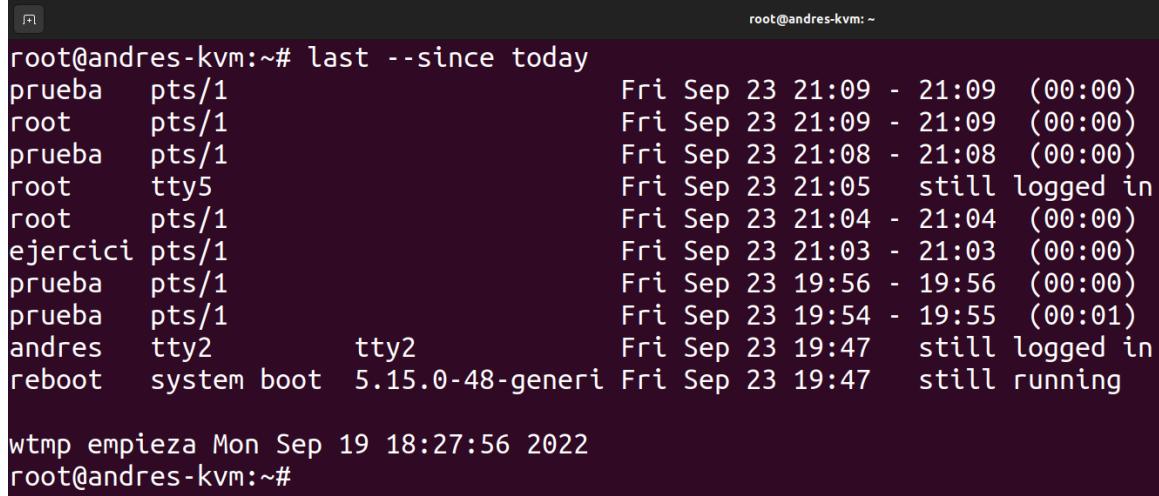
wtmp empieza Mon Sep 19 18:27:56 2022
root@andres-kvm:~#
```

Ahora con el comando `last --since today` muestra solo la información de hoy.

```
root@andres-kvm: ~# last --since today
root    pts/1          Fri Sep 23 21:09  still logged in
prueba  pts/1          Fri Sep 23 21:08 - 21:08  (00:00)
root    tty5          Fri Sep 23 21:05  still logged in
root    pts/1          Fri Sep 23 21:04 - 21:04  (00:00)
ejercici pts/1         Fri Sep 23 21:03 - 21:03  (00:00)
prueba  pts/1          Fri Sep 23 19:56 - 19:56  (00:00)
prueba  pts/1          Fri Sep 23 19:54 - 19:55  (00:01)
andres  tty2      tty2      Fri Sep 23 19:47  still logged in
reboot system boot 5.15.0-48-generi Fri Sep 23 19:47  still running

wtmp empieza Mon Sep 19 18:27:56 2022
root@andres-kvm:~#
```

A continuación, voy a iniciar sesión con el usuario “prueba” y a hacer logout para ver como se almacena la información:



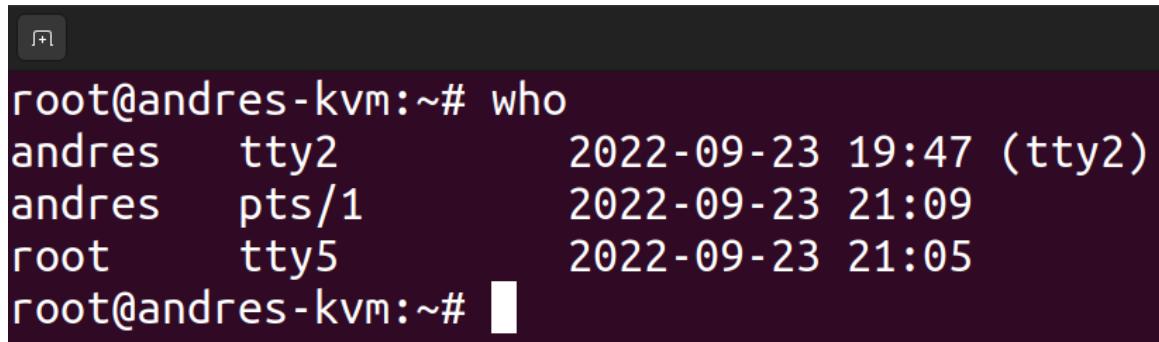
```
root@andres-kvm:~# last --since today
prueba    pts/1                      Fri Sep 23 21:09 - 21:09  (00:00)
root      pts/1                      Fri Sep 23 21:09 - 21:09  (00:00)
prueba    pts/1                      Fri Sep 23 21:08 - 21:08  (00:00)
root      tty5                       Fri Sep 23 21:05   still logged in
root      pts/1                      Fri Sep 23 21:04 - 21:04  (00:00)
ejercici pts/1                      Fri Sep 23 21:03 - 21:03  (00:00)
prueba    pts/1                      Fri Sep 23 19:56 - 19:56  (00:00)
prueba    pts/1                      Fri Sep 23 19:54 - 19:55  (00:01)
andres   tty2           tty2          Fri Sep 23 19:47   still logged in
reboot   system boot  5.15.0-48-generi Fri Sep 23 19:47   still running

wtmp empieza Mon Sep 19 18:27:56 2022
root@andres-kvm:~#
```

Figura 12: Se puede observar como el usuario “prueba” aparece en la primera línea.

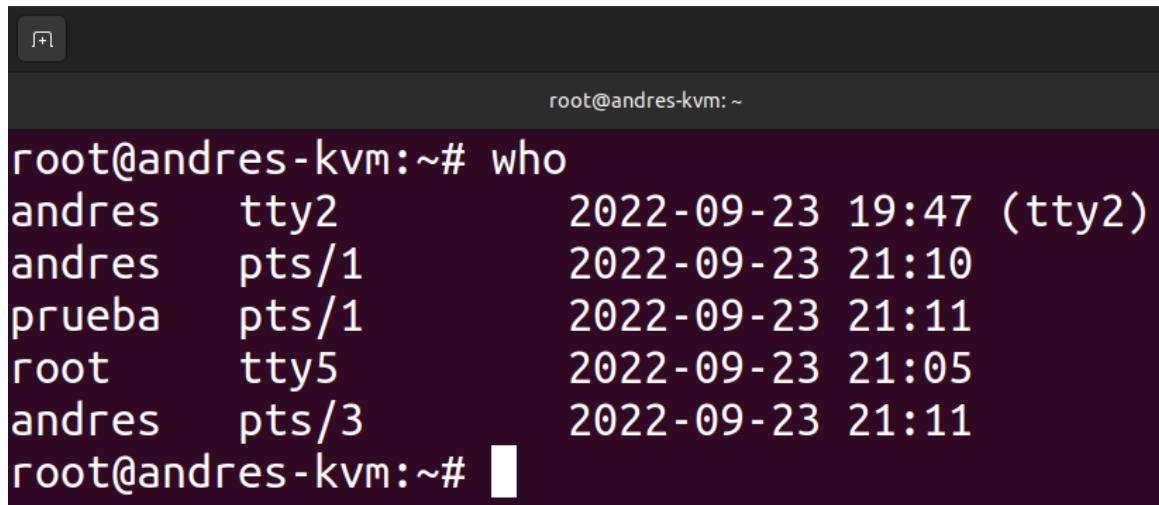
### /var/log/utmp

Muestra los usuarios que están *loggeados* en el sistema. Se puede obtener esta información mediante la orden `who`.



```
root@andres-kvm:~# who
andres   tty2                      2022-09-23 19:47 (tty2)
andres   pts/1                      2022-09-23 21:09
root     tty5                      2022-09-23 21:05
root@andres-kvm:~#
```

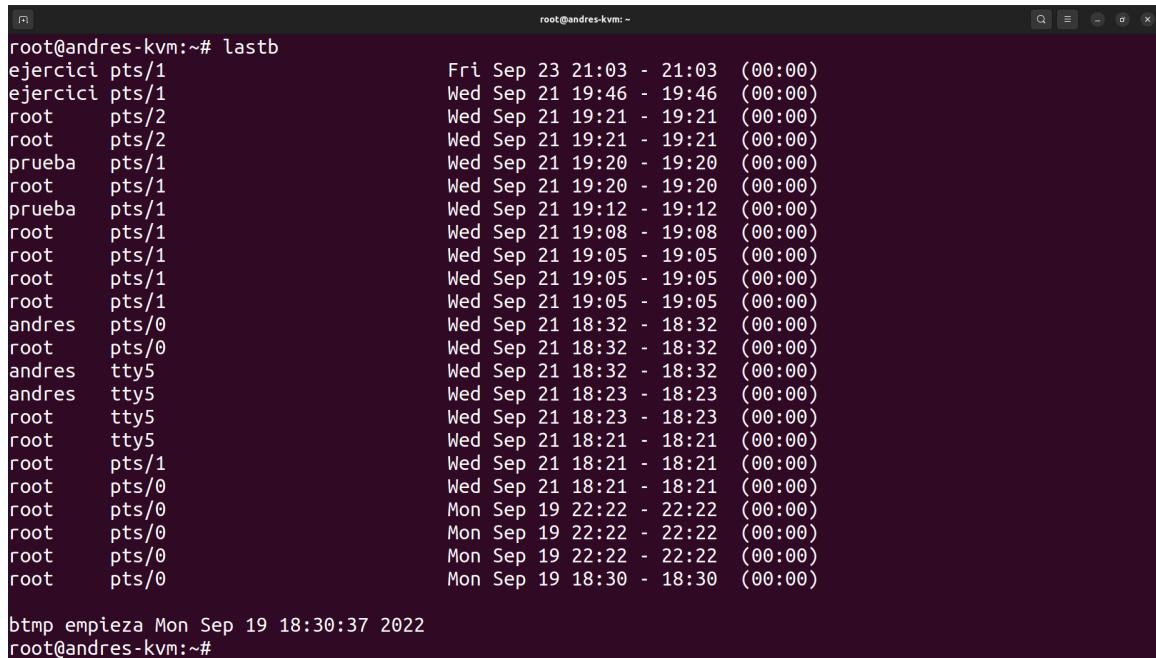
Ahora si inicio sesión con el usuario “prueba”, debería aparecer usando de nuevo la misma orden:



```
root@andres-kvm:~# who
andres   tty2                      2022-09-23 19:47 (tty2)
andres   pts/1                      2022-09-23 21:10
prueba   pts/1                      2022-09-23 21:11
root     tty5                      2022-09-23 21:05
andres   pts/3                      2022-09-23 21:11
root@andres-kvm:~#
```

## /var/log/btmp

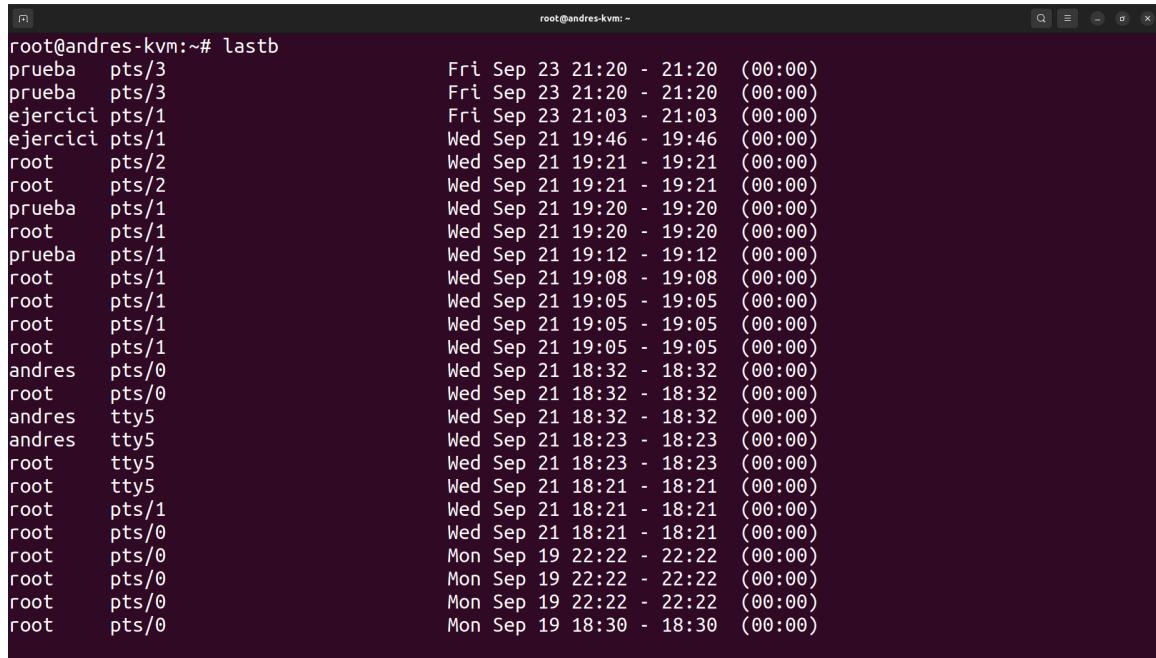
Muestra los intentos fallidos de inicio de sesión en el sistema. Se puede obtener con la orden `lastb`.



```
root@andres-kvm:~# lastb
ejercici pts/1          Fri Sep 23 21:03 - 21:03 (00:00)
ejercici pts/1          Wed Sep 21 19:46 - 19:46 (00:00)
root     pts/2          Wed Sep 21 19:21 - 19:21 (00:00)
root     pts/2          Wed Sep 21 19:21 - 19:21 (00:00)
prueba   pts/1          Wed Sep 21 19:20 - 19:20 (00:00)
root     pts/1          Wed Sep 21 19:20 - 19:20 (00:00)
prueba   pts/1          Wed Sep 21 19:12 - 19:12 (00:00)
root     pts/1          Wed Sep 21 19:08 - 19:08 (00:00)
root     pts/1          Wed Sep 21 19:05 - 19:05 (00:00)
root     pts/1          Wed Sep 21 19:05 - 19:05 (00:00)
root     pts/1          Wed Sep 21 19:05 - 19:05 (00:00)
andres   pts/0          Wed Sep 21 18:32 - 18:32 (00:00)
root     pts/0          Wed Sep 21 18:32 - 18:32 (00:00)
andres   tty5          Wed Sep 21 18:32 - 18:32 (00:00)
andres   tty5          Wed Sep 21 18:23 - 18:23 (00:00)
root     tty5          Wed Sep 21 18:23 - 18:23 (00:00)
root     tty5          Wed Sep 21 18:21 - 18:21 (00:00)
root     pts/1          Wed Sep 21 18:21 - 18:21 (00:00)
root     pts/0          Wed Sep 21 18:21 - 18:21 (00:00)
root     pts/0          Mon Sep 19 22:22 - 22:22 (00:00)
root     pts/0          Mon Sep 19 22:22 - 22:22 (00:00)
root     pts/0          Mon Sep 19 22:22 - 22:22 (00:00)
root     pts/0          Mon Sep 19 18:30 - 18:30 (00:00)

btmp empieza Mon Sep 19 18:30:37 2022
root@andres-kvm:~#
```

Ahora, si hago que falle el inicio de sesión del usuario “prueba” debería de salir:



```
root@andres-kvm:~# lastb
prueba  pts/3          Fri Sep 23 21:20 - 21:20 (00:00)
prueba  pts/3          Fri Sep 23 21:20 - 21:20 (00:00)
ejercici pts/1          Fri Sep 23 21:03 - 21:03 (00:00)
ejercici pts/1          Wed Sep 21 19:46 - 19:46 (00:00)
root     pts/2          Wed Sep 21 19:21 - 19:21 (00:00)
root     pts/2          Wed Sep 21 19:21 - 19:21 (00:00)
prueba   pts/1          Wed Sep 21 19:20 - 19:20 (00:00)
root     pts/1          Wed Sep 21 19:20 - 19:20 (00:00)
prueba   pts/1          Wed Sep 21 19:12 - 19:12 (00:00)
root     pts/1          Wed Sep 21 19:08 - 19:08 (00:00)
root     pts/1          Wed Sep 21 19:05 - 19:05 (00:00)
root     pts/1          Wed Sep 21 19:05 - 19:05 (00:00)
root     pts/1          Wed Sep 21 19:05 - 19:05 (00:00)
root     pts/1          Wed Sep 21 19:05 - 19:05 (00:00)
root     pts/1          Wed Sep 21 19:05 - 19:05 (00:00)
root     pts/1          Wed Sep 21 19:05 - 19:05 (00:00)
root     pts/1          Wed Sep 21 19:05 - 19:05 (00:00)
root     pts/1          Wed Sep 21 19:05 - 19:05 (00:00)
root     pts/1          Wed Sep 21 19:05 - 19:05 (00:00)
andres   pts/0          Wed Sep 21 18:32 - 18:32 (00:00)
root     pts/0          Wed Sep 21 18:32 - 18:32 (00:00)
andres   tty5          Wed Sep 21 18:32 - 18:32 (00:00)
andres   tty5          Wed Sep 21 18:23 - 18:23 (00:00)
root     tty5          Wed Sep 21 18:23 - 18:23 (00:00)
root     tty5          Wed Sep 21 18:21 - 18:21 (00:00)
root     pts/1          Wed Sep 21 18:21 - 18:21 (00:00)
root     pts/0          Wed Sep 21 18:21 - 18:21 (00:00)
root     pts/0          Mon Sep 19 22:22 - 22:22 (00:00)
root     pts/0          Mon Sep 19 22:22 - 22:22 (00:00)
root     pts/0          Mon Sep 19 22:22 - 22:22 (00:00)
root     pts/0          Mon Sep 19 18:30 - 18:30 (00:00)
```

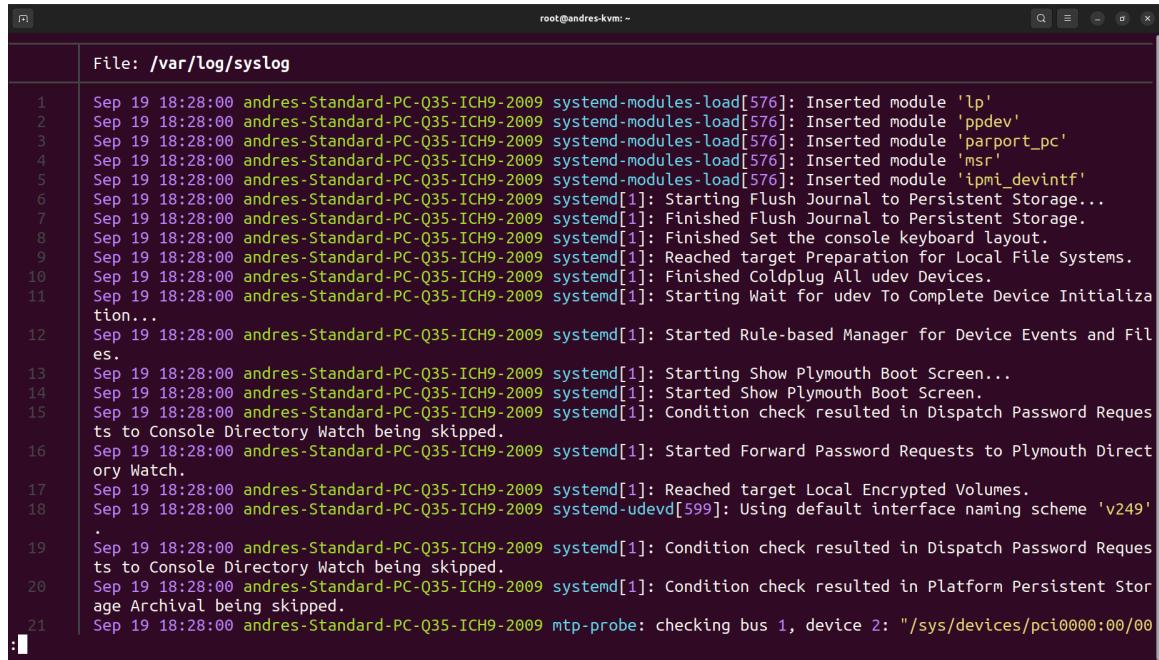
Figura 13: Se puede ver que las dos primeras líneas pertenecen a intentos de login con el usuario “prueba”.

## /var/log/sudo

Este archivo, al menos en Ubuntu, no existe, por tanto no puedo mostrar información al respecto sobre la actividad del uso de `sudo`.

## /var/log/messages

En Ubuntu (no sé si en otras distribuciones también) ya no existe este archivo porque duplicaba información con /var/log/syslog. Por tanto, voy a mostrar este último archivo:



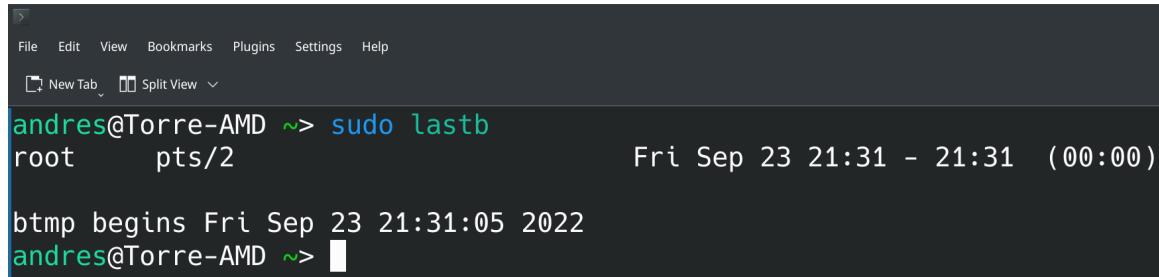
The screenshot shows a terminal window titled "root@andres-kvm: ~". The file being viewed is "/var/log/syslog". The log entries are as follows:

```
1 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd-modules-load[576]: Inserted module 'lp'
2 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd-modules-load[576]: Inserted module 'ppdev'
3 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd-modules-load[576]: Inserted module 'parport_pc'
4 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd-modules-load[576]: Inserted module 'msr'
5 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd-modules-load[576]: Inserted module 'ipmi_devintf'
6 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Starting Flush Journal to Persistent Storage...
7 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Finished Flush Journal to Persistent Storage.
8 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Reached Set the console keyboard layout.
9 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Reached target Preparation for Local File Systems.
10 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Finished Coldplug All udev Devices.
11 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Starting Wait for udev To Complete Device Initialization...
12 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Started Rule-based Manager for Device Events and Files.
13 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Starting Show Plymouth Boot Screen...
14 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Started Show Plymouth Boot Screen.
15 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Condition check resulted in Dispatch Password Requests to Console Directory Watch being skipped.
16 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Started Forward Password Requests to Plymouth Directory Watch.
17 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Reached target Local Encrypted Volumes.
18 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd-udevd[599]: Using default interface naming scheme 'v249' .
19 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Condition check resulted in Dispatch Password Requests to Console Directory Watch being skipped.
20 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 systemd[1]: Condition check resulted in Platform Persistent Storage Archival being skipped.
21 Sep 19 18:28:00 andres-Standard-PC-Q35-ICH9-2009 mtp-probe: checking bus 1, device 2: "/sys/devices/pci0000:00/00
```

## Ejercicio 9

### PC de mi casa

Para comprobar los intentos de inicio de sesión fallidos en el ordenador de mi casa, voy a usar la orden `lastb`:



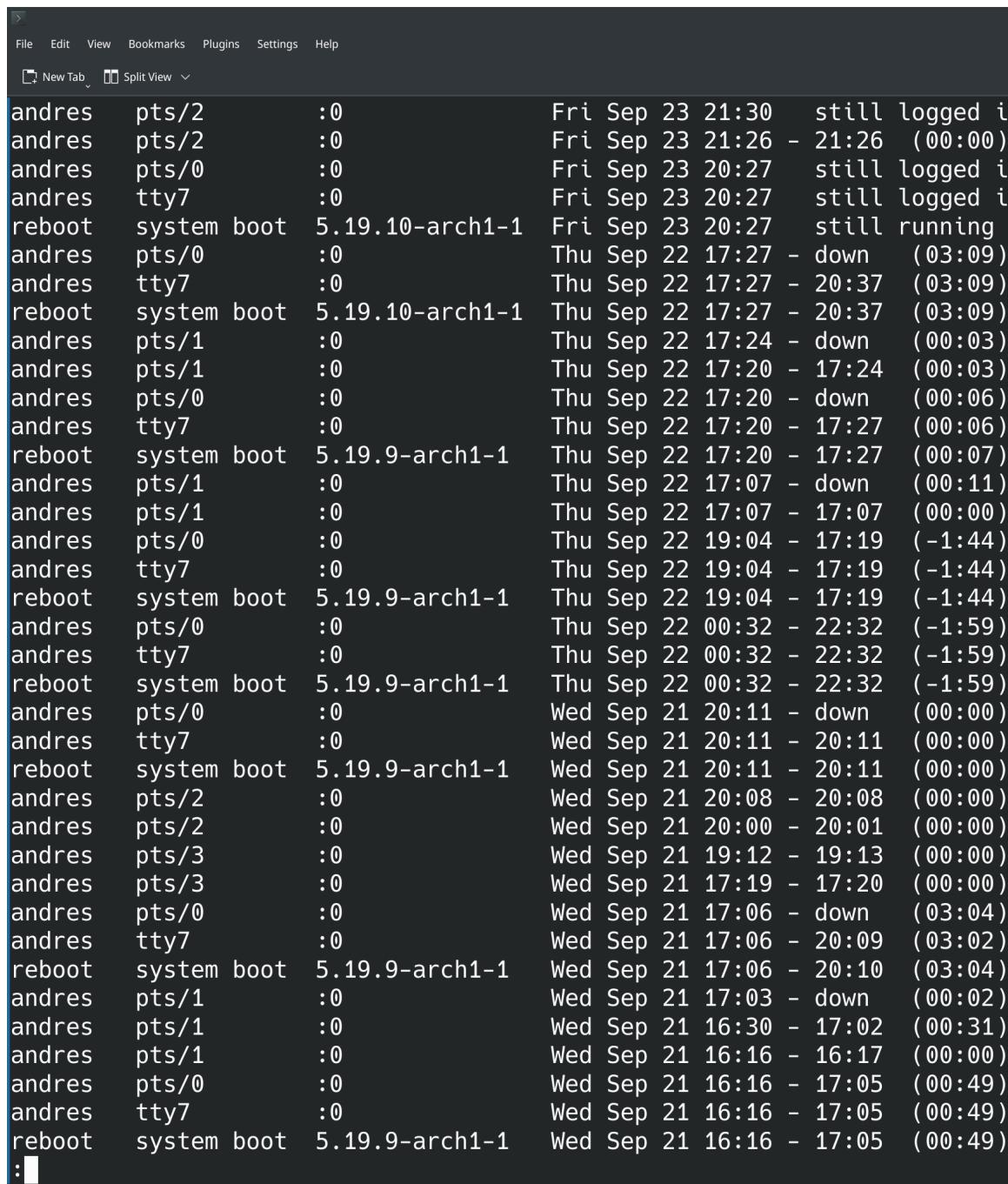
The screenshot shows a terminal window with a menu bar at the top. The command entered is `sudo lastb`. The output shows a single failed login attempt:

```
andres@Torre-AMD ~> sudo lastb
root      pts/2          Fri Sep 23 21:31 - 21:31  (00:00)

btmp begins Fri Sep 23 21:31:05 2022
andres@Torre-AMD ~>
```

El único intento fallido de inicio de sesión que he tenido ha sido provocado por mí en el momento de hacer esta parte del ejercicio.

Ahora, muestro con el comando `last` los login y logout del sistema:



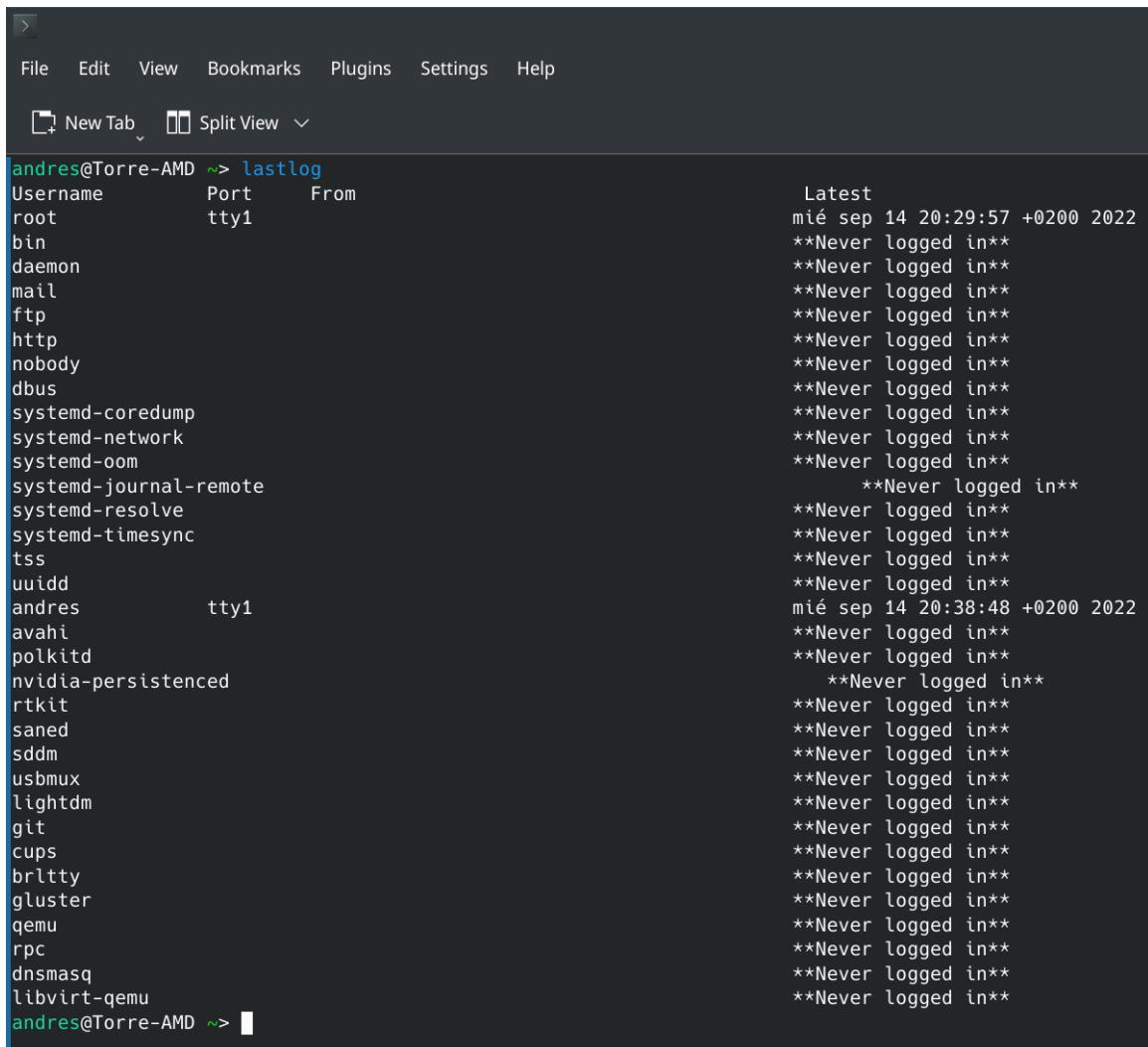
The screenshot shows a terminal window with a dark background and light-colored text. At the top, there's a menu bar with options: File, Edit, View, Bookmarks, Plugins, Settings, and Help. Below the menu, there are buttons for New Tab and Split View. The main area of the terminal displays the output of the 'last' command, which lists system events. The columns from left to right are: user, device, port, timestamp, and status. The output shows multiple logins and reboots for a user named 'andres'. The first few entries are as follows:

user	device	port	timestamp	status
andres	pts/2	:0	Fri Sep 23 21:30	still logged in
andres	pts/2	:0	Fri Sep 23 21:26	- 21:26 (00:00)
andres	pts/0	:0	Fri Sep 23 20:27	still logged in
andres	tty7	:0	Fri Sep 23 20:27	still logged in
reboot	system boot	5.19.10-arch1-1	Fri Sep 23 20:27	still running

This pattern repeats several times, indicating a continuous loop of logins and reboots. The last entry in the list is a colon followed by a blank line.

Por lo que puedo ver, no ha habido ningún inicio en el sistema por SSH (se mostraría en la tercera columna la dirección IP del que lo ha intentado).

Por último, con la orden `lastlog` muestro los inicios de sesión producidos en el sistema.



```
andres@Torre-AMD ~> lastlog
Username      Port     From          Latest
root          tty1
bin
daemon
mail
ftp
http
nobody
dbus
systemd-coredump
systemd-network
systemd-oom
systemd-journal-remote
systemd-resolve
systemd-timesync
tss
uuid
andres        tty1
avahi
polkitd
nvidia-persistenced
rtkit
saned
sddm
usbmux
lightdm
git
cups
brltty
gluster
qemu
rpc
dnsmasq
libvirt-qemu
andres@Torre-AMD ~>
```

Como se puede ver, no hay ninguno en el que aparezca SSH y los inicios de sesión me concuerdan, lo cual me puede indicar que el sistema no ha sido (a simple vista) comprometido.

## PC de prácticas (máquina virtual)

Voy a usar los mismos comandos para la máquina virtual y comprobar su seguridad. Para suponer que el sistema ha sido comprometido, he usado SSH desde el ordenador de mi casa (host) hacia la máquina virtual.

```
andres@andres-kvm: ~
andres  ssh:notty  192.168.122.1   Fri Sep 23 21:39 - 21:39  (00:00)
prueba  pts/3      Fri Sep 23 21:20 - 21:20  (00:00)
prueba  pts/3      Fri Sep 23 21:20 - 21:20  (00:00)
ejercici pts/1     Fri Sep 23 21:03 - 21:03  (00:00)
ejercici pts/1     Wed Sep 21 19:46 - 19:46  (00:00)
root    pts/2      Wed Sep 21 19:21 - 19:21  (00:00)
root    pts/2      Wed Sep 21 19:21 - 19:21  (00:00)
prueba  pts/1      Wed Sep 21 19:20 - 19:20  (00:00)
root    pts/1      Wed Sep 21 19:20 - 19:20  (00:00)
prueba  pts/1      Wed Sep 21 19:12 - 19:12  (00:00)
root    pts/1      Wed Sep 21 19:08 - 19:08  (00:00)
root    pts/1      Wed Sep 21 19:05 - 19:05  (00:00)
root    pts/1      Wed Sep 21 19:05 - 19:05  (00:00)
root    pts/1      Wed Sep 21 19:05 - 19:05  (00:00)
andres  pts/0      Wed Sep 21 18:32 - 18:32  (00:00)
root    pts/0      Wed Sep 21 18:32 - 18:32  (00:00)
andres  tty5      Wed Sep 21 18:32 - 18:32  (00:00)
andres  tty5      Wed Sep 21 18:23 - 18:23  (00:00)
root    tty5      Wed Sep 21 18:23 - 18:23  (00:00)
root    tty5      Wed Sep 21 18:21 - 18:21  (00:00)
root    pts/1      Wed Sep 21 18:21 - 18:21  (00:00)
root    pts/0      Wed Sep 21 18:21 - 18:21  (00:00)
root    pts/0      Mon Sep 19 22:22 - 22:22  (00:00)
root    pts/0      Mon Sep 19 22:22 - 22:22  (00:00)
root    pts/0      Mon Sep 19 22:22 - 22:22  (00:00)
root    pts/0      Mon Sep 19 18:30 - 18:30  (00:00)
:
:
```

Como se puede ver, la dirección IP “192.168.122.1” ha intentado conectarse a la máquina con el usuario “andres” por SSH.

```
andres@andres-kvm: ~
andres  pts/0      192.168.122.1   Fri Sep 23 21:35 - 21:35  (00:00)
prueba  pts/1      Fri Sep 23 21:11 - 21:18  (00:07)
prueba  pts/1      Fri Sep 23 21:09 - 21:09  (00:00)
root    pts/1      Fri Sep 23 21:09 - 21:09  (00:00)
prueba  pts/1      Fri Sep 23 21:08 - 21:08  (00:00)
root    tty5      Fri Sep 23 21:05 still logged in
root    pts/1      Fri Sep 23 21:04 - 21:04  (00:00)
ejercici pts/1     Fri Sep 23 21:03 - 21:03  (00:00)
prueba  pts/1      Fri Sep 23 19:56 - 19:56  (00:00)
prueba  pts/1      Fri Sep 23 19:54 - 19:55  (00:01)
andres  tty2      Fri Sep 23 19:47 still logged in
reboot  system boot 5.15.0-48-generi Fri Sep 23 19:47 still running
andres  tty2      Wed Sep 21 20:03 - down  (00:04)
reboot  system boot 5.15.0-48-generi Wed Sep 21 20:03 - 20:08  (00:05)
andres  tty2      Wed Sep 21 20:03 - down  (00:00)
reboot  system boot 5.15.0-48-generi Wed Sep 21 20:03 - 20:03  (00:00)
andres  tty2      Wed Sep 21 20:02 - down  (00:01)
reboot  system boot 5.15.0-48-generi Wed Sep 21 20:01 - 20:03  (00:01)
ejercici pts/1     Wed Sep 21 20:00 - 20:00  (00:00)
ejercici pts/1     Wed Sep 21 19:59 - 19:59  (00:00)
andres  tty2      Wed Sep 21 19:43 - down  (00:18)
reboot  system boot 5.15.0-48-generi Wed Sep 21 19:43 - 20:01  (00:18)
root    pts/2      Wed Sep 21 19:11 - 19:11  (00:00)
root    tty5      Wed Sep 21 18:21 - down  (01:21)
andres  tty2      tty2      Wed Sep 21 18:06 - down  (01:36)
reboot  system boot 5.15.0-48-generi Wed Sep 21 18:06 - 19:43  (01:36)
:
:
```

También se ve que alguien ha entrado al sistema con SSH usando el usuario “andres”.

```
andres@andres-kvm: ~
tss                                **Nunca ha accedido**
uuidd                               **Nunca ha accedido**
systemd-oom                          **Nunca ha accedido**
tcpdump                             **Nunca ha accedido**
avahi-autoipd                        **Nunca ha accedido**
usbmux                               **Nunca ha accedido**
dnsmasq                              **Nunca ha accedido**
kernoops                            **Nunca ha accedido**
avahi                               **Nunca ha accedido**
cups-pk-helper                       **Nunca ha accedido**
rtkit                                **Nunca ha accedido**
whoopsie                             **Nunca ha accedido**
sssd                                 **Nunca ha accedido**
speech-dispatcher                   **Nunca ha accedido**
nm-openvpn                           **Nunca ha accedido**
saned                                **Nunca ha accedido**
colord                               **Nunca ha accedido**
geoclue                             **Nunca ha accedido**
pulse                                **Nunca ha accedido**
gnome-initial-setup                 **Nunca ha accedido**
hplip                                **Nunca ha accedido**
gdm                                  **Nunca ha accedido**
andres      pts/0    192.168.122.1  vie sep 23 21:35:05 +0200 2022
prueba     pts/1    192.168.122.1  vie sep 23 21:11:34 +0200 2022
sshd                                **Nunca ha accedido**
ejercicio6   pts/1    192.168.122.1  vie sep 23 21:03:38 +0200 2022
(END)
```

Aquí también se puede observar que alguien ha accedido con la misma dirección IP anterior mediante SSH y ha conseguido iniciar sesión en el sistema.

Según estos datos, suponiendo que no hubiera sido yo, se podría decir que alguien ha intentado acceder al sistema y ha conseguido iniciar sesión como el usuario “andres”. Una vez sacada esta conclusión, lo recomendable es detectar los cambios que ha realizado en el sistema y el tráfico de red para ver que posibles datos se ha podido llevar o el posible daño que puede haber hecho al sistema.