

# SSO Práctica 1

Andrés Merlo Trujillo

## Índice

<b>1. Primer ejercicio</b>	<b>1</b>
1.1. /etc/passwd . . . . .	1
1.2. /etc/group . . . . .	2
1.3. /etc/shadow . . . . .	3
1.4. /etc/gshadow . . . . .	5
<b>2. Segundo ejercicio</b>	<b>6</b>
<b>3. Tercer ejercicio</b>	<b>8</b>
<b>4. Ejercicio 4</b>	<b>9</b>
4.1. /etc/pam.d/chfn . . . . .	10
4.2. /etc/pam.d/chsh . . . . .	10
<b>5. Quinto ejercicio</b>	<b>11</b>
5.1. Apartado a . . . . .	11
5.2. Apartado b . . . . .	11
<b>6. Sexto ejercicio</b>	<b>13</b>
<b>7. Séptimo ejercicio</b>	<b>13</b>
<b>8. Octavo ejercicio</b>	<b>14</b>
8.1. /var/log/lastlog . . . . .	15
8.2. /var/log/wtmp . . . . .	15
8.3. /var/log/utmp . . . . .	17
8.4. /var/log/btmp . . . . .	17
8.5. /var/log/sudo . . . . .	18
8.6. /var/log/messages . . . . .	18
8.7. Noveno ejercicio . . . . .	19
8.8. PC de mi casa . . . . .	19
8.9. PC de prácticas (máquina virtual) . . . . .	21

## 1. Primer ejercicio

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:

### 1.1. /etc/passwd

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

```

root@andres-kvm: ~
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

```

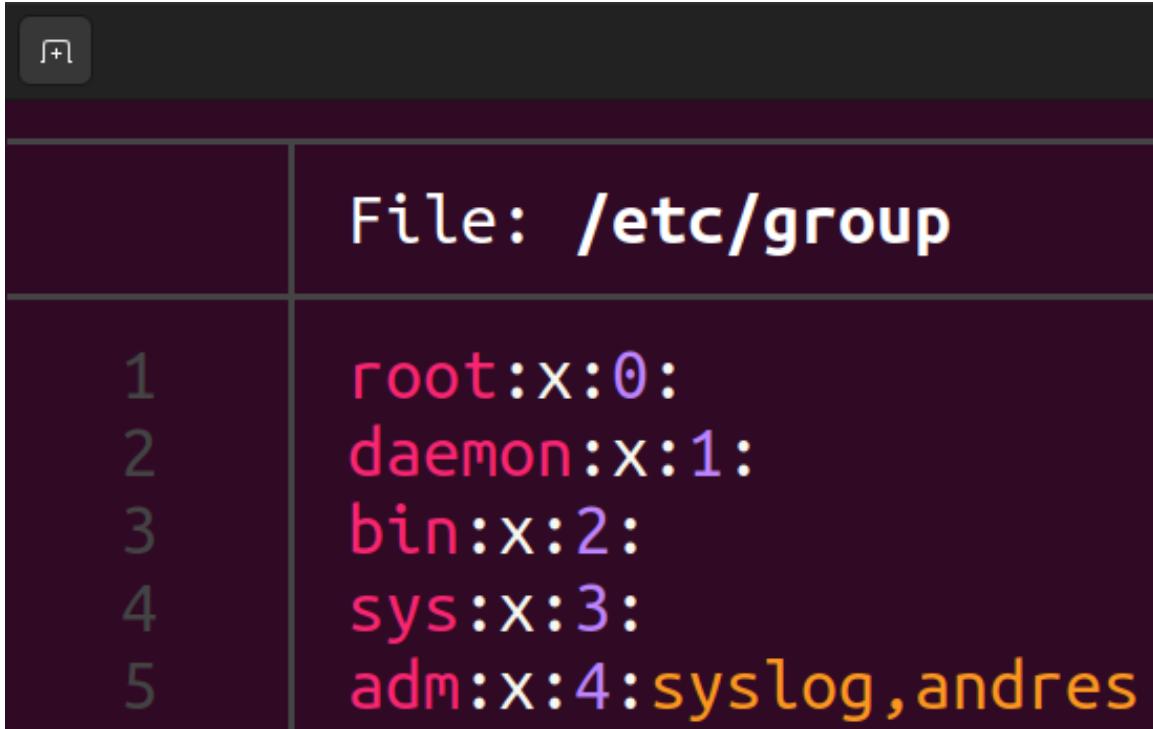
Figura 1: Ejemplo de entradas en el archivo.

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” minuscula, significa que la contraseña se almacena en “/etc/shadow”.  
Si se encuentra vacio, significa que no hace falta contraseña para autenticar.  
Si comienza en exclamacion, significa que la contraseña ha sido bloqueada.  
Ademas, si contiene una exclamacion o un asterisco, significa que el usuario no podra usar la contraseña para iniciar sesion (pero puede usar otro medio).
3. **User ID numerico:** ID del usuario.
4. **Group ID numerico:** 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: accion que realiza, para evitar confusion 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). Ademas, pondra la variable de entorno “\$SHELL” a este valor.

## 1.2. /etc/group

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



The screenshot shows a terminal window with a dark background. At the top, there is a small icon in a rounded square. Below the title bar, the text "File: /etc/group" is displayed in white. The main area of the terminal contains five lines of text, each starting with a number from 1 to 5 followed by a colon and then the group information:

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

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” minuscula 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.

### 1.3. /etc/shadow

**Formato:** `login:pass:last_change:min_age:max_age:pass_warn:pass_inact:acc_exp:reserved`

```

File: /etc/shadow

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 uuidd:*: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 encryptada):** 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 exclamacion (“!”), significa que la contraseña ha sido bloqueada.

Por último, si la contraseña contiene el carácter de exclamacion 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 ultimo cambio de contraseña):** El último cambio de contraseña, expresado como el numero de dias desde el epoch (1 de enero de 1970).

Además, si el valor es 0 significa que el usuario debe cambiar la contraseña en el proximo login.

En cambio, si el campo está vacio significa que las contraseñas no tienen edad (y por tanto no se cumplen estas restricciones).

- 4. minimum password age (edad minima de la contraseña):** Numero de dias que el usuario tiene que esperar antes de poder cambiar la contraseña de nuevo. Un valor 0 ó vacio indica que no hay un minimo de dias.

- 5. maximum password age (edad maxima de la contraseña):** Numero maximo de dias en los cuales la contraseña “caduca” (tiene que cambiarla). Al pasar este numero de dias, el sistema pedira al usuario que cambie la contraseña.

Si el valor maximo es mayor que el del campo anterior, el usuario no podra cambiar su contraseña.

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

6. **password warning period (periodo de advertencia de la contraseña):** El numero de dias antes de que la contraseña “caduque” durante los cuales se le advierte al usuario.  
Un valor 0 o cadena vacia indica que no habra advertencias.
7. **password inactivity period (periodo de inactividad de la contraseña):** Numero de dias despues de que la contraseña haya “caducado” en el cual deberia ser aceptada. Al pasar este periodo, el usuario no podra iniciar sesion.  
Un campo vacio indica que no se cumple esta regla.
8. **account expiration date (fecha de expiracion de la cuenta):** La fecha en la que la cuenta expira. Esta fecha se expresa como el numero de dias desde el epoch.  
La diferencia con la expiracion de una contraseña es que, si la cuenta expira, no podra iniciar sesion de ninguna forma, mientras que si la contraseña expira, tendra otros medios para iniciar sesion.  
El campo vacio indica que la cuenta no expira. Ademas, 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 està reservado para usos futuros.

#### 1.4. /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 està tambien 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 està vacio, entonces cualquier usuario puede obtener los privilegios del grupo.  
Si la contraseña comienza por una exclamacion, significa que esta està bloqueada.

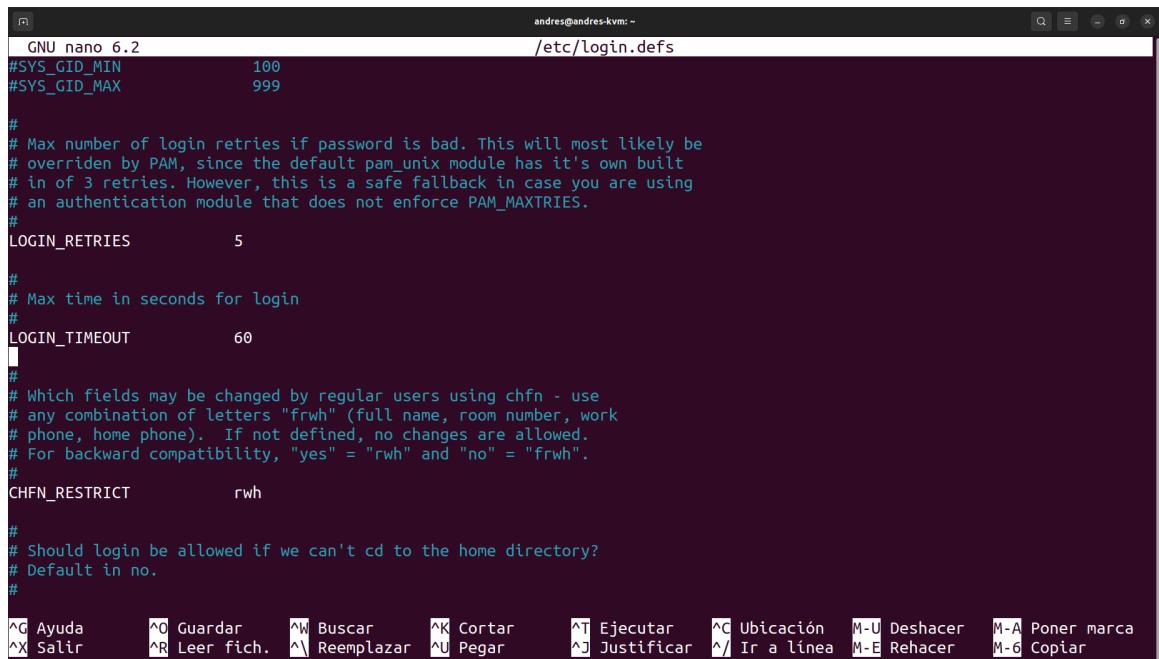
Si contiene una exclamacion o asterisco, los usuarios no podran acceder al grupo si no estan en el.

3. **Administradores:** Lista de usuarios separados por coma que puede realizar operaciones como cambiar la contrasñea del grupo o administrar los usuarios del mismo.
4. **Miembros:** Lista de usaurios separados por coma. Los miembros del grupo pueden acceder al mismo sin necesitar la contraseña.

## 2. Segundo ejercicio

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
# 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          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.  ^Y Reemplazar  ^U Pegar       ^J Justificar   ^I Ir a línea    M-B Rehacer      M-G Copiar
```

Figura 5: Valor por defecto.

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

```

GNU nano 6.2                               /etc/login.defs
#
# Max number of login retries if password is bad. This will most likely be
# overridden 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?

```

**Keyboard Shortcuts:**

- ^G Ayuda
- ^O Guardar
- ^W Buscar
- ^K Cortar
- ^T Ejecutar
- ^C Ubicación
- M-U Deshacer
- ^X Salir
- ^R Leer fich.
- ^V Reemplazar
- ^U Pegar
- ^J Justificar
- ^Y Ir a línea
- M-E Rehacer

Figura 6: Valor cambiado a 5 segundos.

A continuacion, 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 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    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.

### 3. Tercer ejercicio

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 ordenes “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:~\$**

Figura 8: se puede ver que solo el usuario “andres” tiene los permisos

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

## 4. Ejercicio 4

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

File	Description	File	Description	File	Description
chfn	common-session-noninteractive	gdm-smartcard		passwd	sudo
chpasswd	cron	gdm-smartcard-pkcs11-exclusive		polkit-1	sudo-i
chsh	cups	gdm-smartcard-sssd-exclusive		ppp	su-l
common-account	gdm-autologin	gdm-smartcard-sssd-or-password		runuser	
common-auth	gdm-fingerprint	login		runuser-l	
common-password	gdm-launch-environment	newusers		sshd	
common-session	gdm-password	other		su	

**andres@andres-kvm:~\$**

A continuacion explicare dos archivos:

#### 4.1. /etc/pam.d/chfn

Permite cambiar la informacion personal de un usuario tales como: el nombre, el numero de telefono, de habitacion, etc. Estos datos luego pueden ser leidos 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 funcion de la linea 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 mas modulos. Ademas, hace uso del modulo “pam\_rootok.so” que hace que solo tenga exito si el usuario tiene el UID a 0 (es el usuario root).

#### 4.2. /etc/pam.d/chsh

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

El contenido del archivo es el siguiente:

```
root@andres-kvm:~# batcat /etc/pam.d/chsh
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
20
root@andres-kvm:~#
```

Como se puede ver en la linea 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. **COMPROBAR AFIRMACIÓN: (Como es el último puede retornar sin problema).** Además, con el módulo “pam\_rootok.so” autoriza al usuario con el UID 0 (root).

## 5. Quinto ejercicio

### 5.1. 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”.

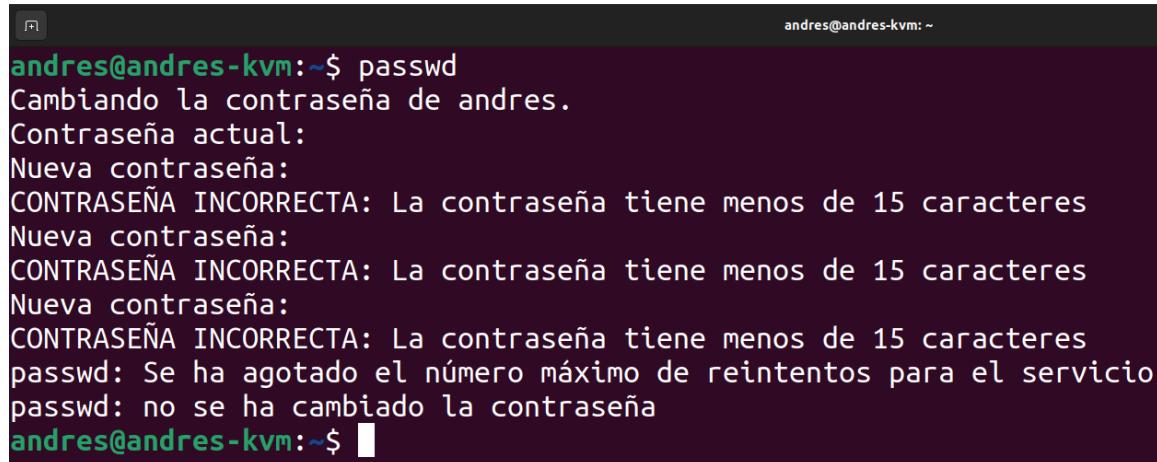
Ahora bien si leemos el manual de este módulo con “man 8 pam\_pwquality” se puede ver que hay un argumento denominado “minlen” y que valor por defecto es 8. No obstante, no se puede bajar del valor 4, ya que es un límite que tiene “Cracklib” y mostrará que la contraseña es muy corta. Por eso, voy a poner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

### 5.2. 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. Si ponen “sudo su” sí van a poder entrar, pero esto es así ya que 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:

The screenshot shows a terminal window with the title "root@andres-kvm: /etc/pam.d". The command "nano 6.2" is at the top. The file content is:

```
GNU nano 6.2
#
# The PAM configuration file for the Shadow `su' service
#
account requisite pam_rootok.so
```

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

The screenshot shows a terminal window with the title "root@andres-kvm: /". The command "andres@andres-kvm:~\$ su" is entered. The response is:

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

En cambio, si el usuario puede usar “sudo”, si puede acceder.

The screenshot shows a terminal window with the title "root@andres-kvm: /". The command "\$ su" is entered, followed by "Contraseña:", then "su: Fallo de autenticación", and finally a prompt "\$".

```
$ su
Contraseña:
su: Fallo de autenticación
$
```

Figura 9: el usuario que se ha creado en esta practica no tiene permisos de sudo y por tanto no puede entrar de ninguna manera

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

## 6. Sexto ejercicio

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 lineas:

```
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, shell=/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
(END)
```

## 7. Séptimo ejercicio

Para empezar, el propio archivon de 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.

```
andres@andres-kvm: ~
$ 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 linea en el archivo “sudoers” tendremos acceso con sudo:

```
root@andres-kvm: /home/andres
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:

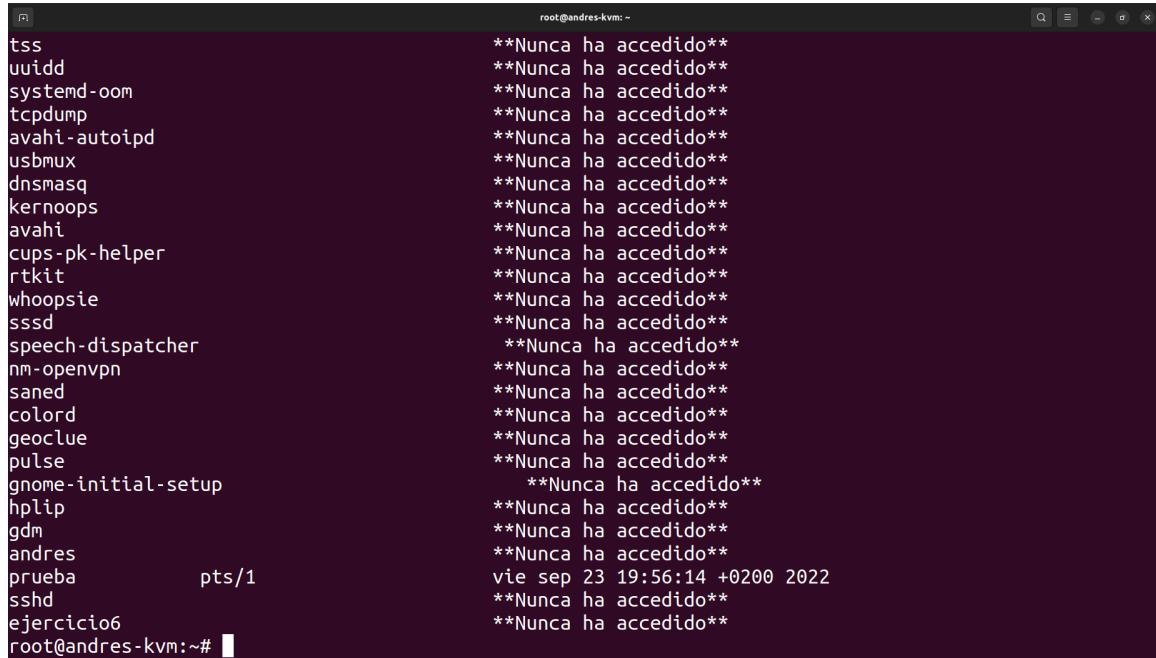
```
andres@andres-kvm: ~
$ whoami
prueba
$ groups
prueba
$ sudo su
[sudo] contraseña para prueba:
root@andres-kvm: # whoami
root
root@andres-kvm: #
```

## 8. Octavo ejercicio

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

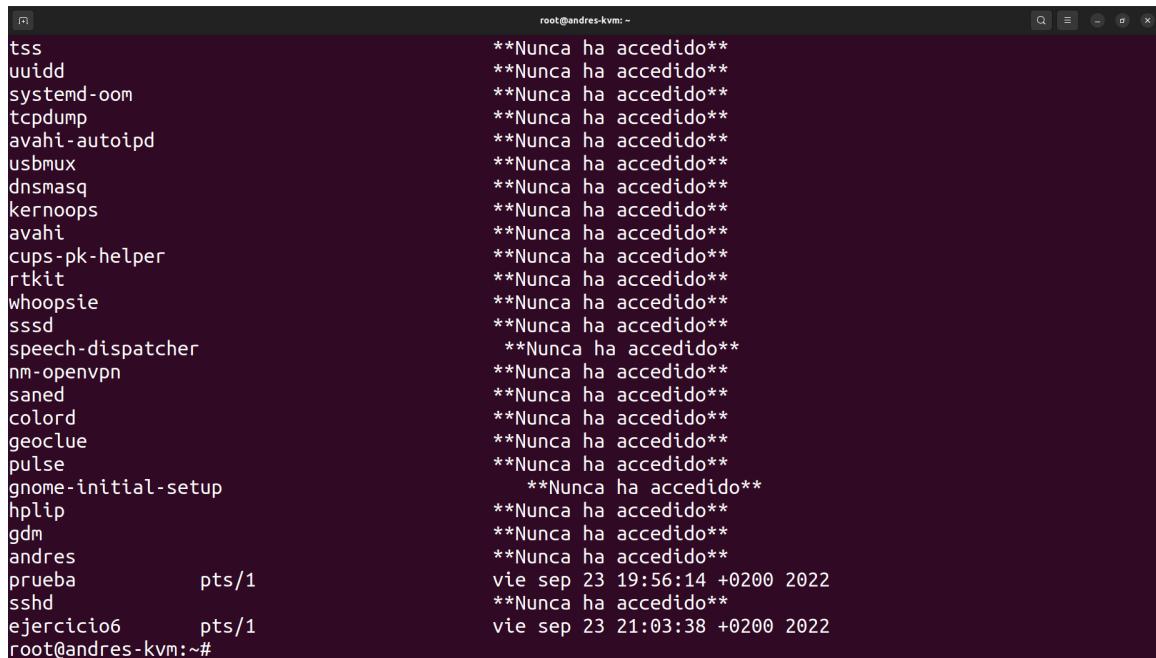
## 8.1. /var/log/lastlog

Este archivo almacena informacion sobre le ultimo inicio de sesion de los usuarios. Para acceder a la informacion 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**
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                             **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 sesion en el sistema. Ahora si inicio sesion 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**
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                             **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:~#
```

Ahora como se puede ver aparece la fecha del ultimo inicio de sesion del usuario “ejercicio6”.

## 8.2. /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      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      pts/0      Mon Sep 19 19:17 - 19:18 (00:01)
andres  tty2      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      pts/1      Mon Sep 19 19:04 - 19:04 (00:00)
andres  tty2      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      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      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 informacion 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:~# █

```

Y ahora voy a iniciar sesion con el usuario “prueba” y lo hago para ver como se almacena la informacion:

```

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:~#

```

### 8.3. /var/log/utmp

Muestra los usuarios que estan *loggeados* en el sistema. Se puede obtener esta información con 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 sesion con el usuario “prueba” deberia aparecer con el comando anterior:

```
root@andres-kvm:~#
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:~#
```

### 8.4. /var/log/btmp

Muestra los intentos fallidos de inicio de sesion 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 fallo el inicio de sesion del usuario “prueba” deberia 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)
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 10: Se puede ver que las dos primeras lineas pertenecen a intentos de login con le usuario “prueba”.

## 8.5. /var/log/sudo

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

## 8.6. /var/log/messages

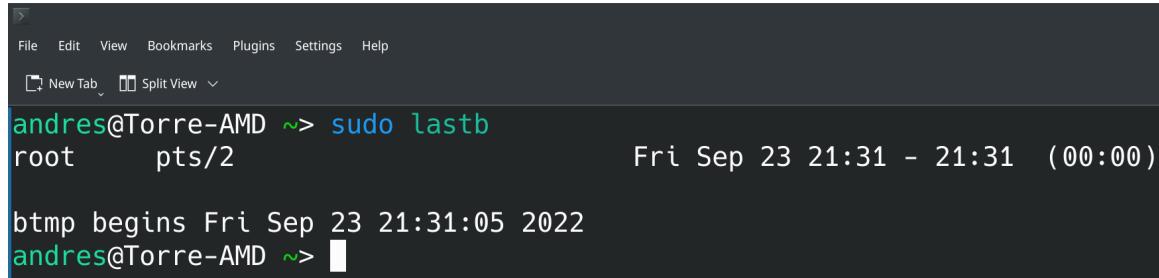
En Ubuntu (no sé si en otras distribuciones también) ya no existe este archivo porque duplicaba informacion con “/var/log/syslog”. Por tanto, voy a mostrar este archivo:

```
File: /var/log/syslog
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]: Finished 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
```

## 8.7. Noveno ejercicio

## 8.8. PC de mi casa

Para comprobar los intentos de inicio de sesion fallidos en el ordenador de mi casa, voy a usar “lastb”:



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 following text:

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

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

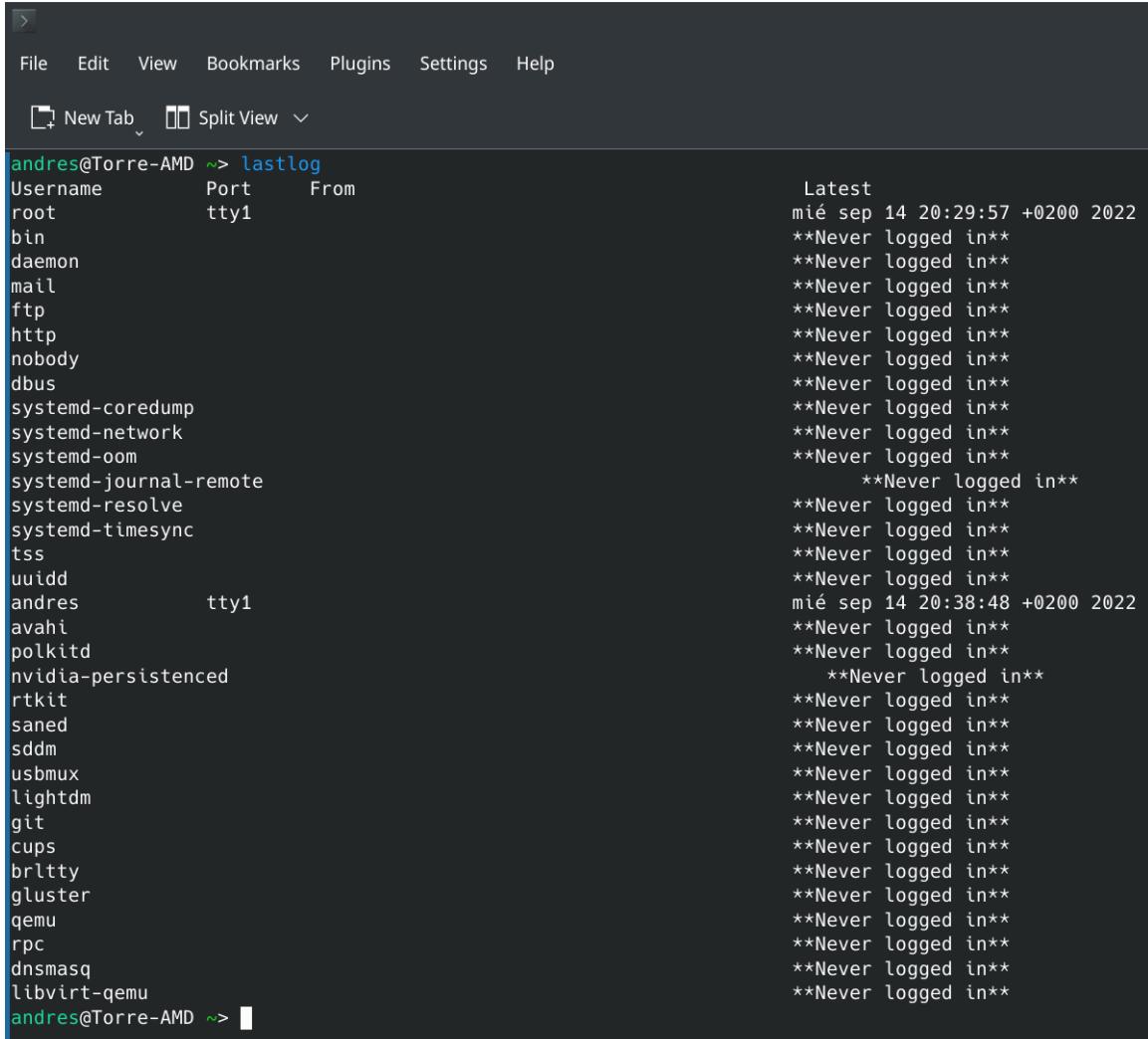
Como se puede observar, el unico intento fallido de inicio de sesion que he tenido ha sido provocado por mi en el momento de hacer esta parte del ejercicio.

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

andres	pts/2	:	0		Fri	Sep	23	21:30	still	logged	i
andres	pts/2	:	0		Fri	Sep	23	21:26	-	21:26	(00:00)
andres	pts/0	:	0		Fri	Sep	23	20:27	still	logged	i
andres	tty7	:	0		Fri	Sep	23	20:27	still	logged	i
reboot	system boot	5.19.10-arch1-1			Fri	Sep	23	20:27	still	running	
andres	pts/0	:	0		Thu	Sep	22	17:27	-	down	(03:09)
andres	tty7	:	0		Thu	Sep	22	17:27	-	20:37	(03:09)
reboot	system boot	5.19.10-arch1-1			Thu	Sep	22	17:27	-	20:37	(03:09)
andres	pts/1	:	0		Thu	Sep	22	17:24	-	down	(00:03)
andres	pts/1	:	0		Thu	Sep	22	17:20	-	17:24	(00:03)
andres	pts/0	:	0		Thu	Sep	22	17:20	-	down	(00:06)
andres	tty7	:	0		Thu	Sep	22	17:20	-	17:27	(00:06)
reboot	system boot	5.19.9-arch1-1			Thu	Sep	22	17:20	-	17:27	(00:07)
andres	pts/1	:	0		Thu	Sep	22	17:07	-	down	(00:11)
andres	pts/1	:	0		Thu	Sep	22	17:07	-	17:07	(00:00)
andres	pts/0	:	0		Thu	Sep	22	19:04	-	17:19	(-1:44)
andres	tty7	:	0		Thu	Sep	22	19:04	-	17:19	(-1:44)
reboot	system boot	5.19.9-arch1-1			Thu	Sep	22	19:04	-	17:19	(-1:44)
andres	pts/0	:	0		Thu	Sep	22	00:32	-	22:32	(-1:59)
andres	tty7	:	0		Thu	Sep	22	00:32	-	22:32	(-1:59)
reboot	system boot	5.19.9-arch1-1			Thu	Sep	22	00:32	-	22:32	(-1:59)
andres	pts/0	:	0		Wed	Sep	21	20:11	-	down	(00:00)
andres	tty7	:	0		Wed	Sep	21	20:11	-	20:11	(00:00)
reboot	system boot	5.19.9-arch1-1			Wed	Sep	21	20:11	-	20:11	(00:00)
andres	pts/2	:	0		Wed	Sep	21	20:08	-	20:08	(00:00)
andres	pts/2	:	0		Wed	Sep	21	20:00	-	20:01	(00:00)
andres	pts/3	:	0		Wed	Sep	21	19:12	-	19:13	(00:00)
andres	pts/3	:	0		Wed	Sep	21	17:19	-	17:20	(00:00)
andres	pts/0	:	0		Wed	Sep	21	17:06	-	down	(03:04)
andres	tty7	:	0		Wed	Sep	21	17:06	-	20:09	(03:02)
reboot	system boot	5.19.9-arch1-1			Wed	Sep	21	17:06	-	20:10	(03:04)
andres	pts/1	:	0		Wed	Sep	21	17:03	-	down	(00:02)
andres	pts/1	:	0		Wed	Sep	21	16:30	-	17:02	(00:31)
andres	pts/1	:	0		Wed	Sep	21	16:16	-	16:17	(00:00)
andres	pts/0	:	0		Wed	Sep	21	16:16	-	17:05	(00:49)
andres	tty7	:	0		Wed	Sep	21	16:16	-	17:05	(00:49)
reboot	system boot	5.19.9-arch1-1			Wed	Sep	21	16:16	-	17:05	(00:49)
:■											

Por lo que puedo ver, no ha habido ningun inicio en el sistema por ssh (se mostraria en la tercera columna la direccion IP del que lo ha intentado).

Por ultimo, con la orden "lastlog" muestro los inicios de sesion 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 sesion me concuerdan, lo cual me puede indicar que el sistema no ha sido (a simple vista) comprometido.

### 8.9. PC de prácticas (máquina virtual)

Voy a usar los mismo comandoos para la maquina 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 maquina 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-generic Fri Sep 23 19:47 still running
andres tty2   Wed Sep 21 20:03 - down (00:04)
reboot system boot 5.15.0-48-generic 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-generic 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-generic 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-generic 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   Wed Sep 21 18:06 - down (01:36)
reboot system boot 5.15.0-48-generic Wed Sep 21 18:06 - 19:43 (01:36)
:
```

Se puede observar 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                                **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)
```

Aqui tambien se puede observar que alguien ha accedido con la misma direccion IP anterior mediante SSH y ha conseguido iniciar sesion en el sistema.

Segun estos datos, suponiendo que no hubiera sido yo, se podria decir que alguien ha intentado acceder al sistema y ha conseguido iniciar sesion como el usuario “andres”. Una vez sacada esta conclusion, lo recomendable es detectar los cambios que ha realizado en el sistema y el tradico de red para ver que posibles datos se ha podido llevar.