# SEGURIDAD EN SISTEMAS OPERATIVOS
## 4º Grado en Informática – Complementos de Ing. del Software
## Curso 2020-21

Práctica [1]. .....

Sesión [1]. .....

Autor[1]: ...Jose Armando Albarado Mamani..

## Ejercicio 1.

**Indicar los formatos de los archivos /etc/passwd, /etc/group, /etc/shadow, /etc/gshadow**

El archivo de configuración **/etc/passwd** tiene le formato siguiente:

**pepe:x:500:500:Cuenta de pepe:/home/pepe:/bin/bash**

Ordenados de izquierda a derecha están formados por:

- **Usuario:** Es el primer campo e indica el nombre de usuario.
- **Contraseña:** El segundo campo indica la contraseña del usuario, aparece una **x** ya que la contraseña está encriptada.
- **Identificador de usuario (UID):** El tercer campo indica el número que identifica al usuario.
- **Identificador de Grupo (GID):** El cuarto campo indica el número que identifica al grupo del usuario.
- **Descripción:** El quinto campo indica la descripción del usuario.
- **Directorio home:** El sexto campo indica donde se encuentra el directorio home del usuario.
- **Shell:** El último campo indica el interprete de comandos que tendrá asociado el usuario.

Para poder acceder a ver este archivo de configuración se debe introducir por comando:

```
jose@jose-CX61-2PC:~$ sudo cat /etc/passwd
```

Se obtiene algo similar a:

```
jose:x:1000:1000:Jose,,,:/home/jose:/bin/bash
```

El archivo de configuración **/etc/group** tiene el formato siguiente:

**grupo1:x:5:pepe,maria,manolo**

Ordenados de izquierda a derecha están formados por:

- **Nombre del grupo:** Es el primer campo e indica el nombre de grupo.

---

1 Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la "Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada" esto "conllevará la calificación numérica de cero … independientemente del resto de calificaciones que el estudiante hubiera obtenido ..."

- **Contraseña:** El segundo campo indica la contraseña del grupo, aparece una **x** ya que la contraseña está encriptada.
- **Identificador de Grupo (GID):** El tercer campo indica el número que identifica al grupo.
- **Participantes:** El cuarto campo indica los participantes que conforman el grupo

Para poder acceder a ver este archivo de configuración se debe introducir por comando:

```
jose@jose-CX61-2PC:~$ sudo cat /etc/group
```

Se obtiene algo similar a:

```
sambashare:x:126:jose
```

El archivo de configuración **/etc/shadow** tiene el formato siguiente:

**<nombre de usuario>:<contraseña cifrada>:<1>:<2>:<3>:<4>:<5>:<6>: Reservado**

En el primer campo se encuentre el nombre de usuario, en el segundo campo se almacena la clave del usuario cifrada, y en los campos restantes:

- **1:** Los días que han transcurrido desde el 1 de enero de 1970 hasta la actualidad donde la contraseña fue cambiado por última vez.
- **2:** El número mínimo de días que deben pasar para poder cambiar de nuevo la contraseña.
- **3:** El número de días que deben pasar para que la contraseña caduque y deba ser cambiada.
- **4:** El número de días de antelación para avisar al usuario de que su contraseña ha caducado.
- **5:** Días que transcurrirán hasta deshabilitar una cuenta cuya contraseña haya caducado.
- **6:** Número de días desde el 1 de enero de 1970 hasta el día en que la cuenta ha sido deshabilitada.
- **Reservado:** Es un campo reservado.

Para poder acceder a ver este archivo de configuración se debe introducir por comando:

```
jose@jose-CX61-2PC:~$ sudo cat /etc/shadow
```

Se obtiene algo similar a:

```
jose:$6$NmFG/rFz$CLG3cpJKXIlZlK0euJbR2lMPThDLncUZTWbKOHJkrpQc5HXiV.TDxdoAZ45ff5H
iB50EVRw1PyVPSohUMo95u/:18160:0:99999:7:::
```

El archivo de configuración **/etc/gshadow** tiene el formato siguiente:

**grupo1:<contraseña cifrada del grupo>:pepe:maria,pepe,david**

Ordenados de izquierda están formados por:

- **Nombre del grupo:** El primer campo indica el nombre del grupo.
- **Contraseña cifrada:** En el segundo campo se indica la contraseña de grupo cifrada.
- **Administrador:** En el tercer campo se indica que usuario es el administrador del

grupo

- **Participantes:** En el último campo se indican que usuario conforman el grupo.

Para poder acceder a ver este archivo de configuración se debe introducir por comando:

```
jose@jose-CX61-2PC:~$ sudo cat /etc/gshadow
```

Se obtiene algo similar a:

```
sambashare:!::jose
```

## Ejercicio 2.

**Modificar el archivo /etc/login.defs para que los usuarios creados a partir de ese momento tenga un valor asignado para las directiva LOGIN_TIMEOUT. Crear un usuario y comprobar que tiene efecto la citada directiva.**

1.- Para editar el archivo se debe introducir en terminal:

```
jose@jose-CX61-2PC:~$ sudo gedit /etc/login.defs
```

2.- Dentro del archivo se busca la directiva **LOGIN_TIMEOUT:**

```
#
# Max time in seconds for login
#
LOGIN_TIMEOUT           60
```

Tiene asignado por defecto 60 segundos.

3.- Voy a asignar 5 segundos de **timeout** en el login, para ello:

```
#
# Max time in seconds for login
#
LOGIN_TIMEOUT           5
```

Una vez modificado el archivo se guarda y salimos.

4.- Ahora voy a crear una cuenta nueva, para poder así comprobar que los cambios se han realizado correctamente.

```
jose@jose-CX61-2PC:~$ sudo su
root@jose-CX61-2PC:/home/jose# useradd -m pepito
root@jose-CX61-2PC:/home/jose# passwd pepito
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@jose-CX61-2PC:/home/jose#
```

5.- Una vez creado el nuevo usuario **Pepito,** procedo a realizar el login:

```
root@jose-CX61-2PC:/home/jose# login pepito
Contraseña:
El acceso caducó después de 5 segundos.
root@jose-CX61-2PC:/home/jose#
```

Como se puede ver en la imagen, se dispone sólo de 5 segundos para realizar el login en otra cuenta.

## Ejercicio 3.

**Crear un ACL para un archivo de vuestro sistema de forma que el usuario creado en el Ejercicio 2 tenga acceso de lectura y escritura.**

```
jose@jose-CX61-2PC:~$ touch archivoEjercicio2
jose@jose-CX61-2PC:~$ sudo setfacl -m u:pepito:rw archivoEjercicio2
jose@jose-CX61-2PC:~$ getfacl archivoEjercicio2
# file: archivoEjercicio2
# owner: jose
# group: jose
user::rw-
user:pepito:rw-
group::r--
mask::rw-
other::r--

jose@jose-CX61-2PC:~$
```

Lo primero que he realizado es crear el archivo **archivoEjercicio2**, a continuación he procedido a crear la ACL de forma que pepito pueda leer y escribir en el **archivoEjercicio2,** ya por último, para comprobar que se ha realizado correctamente compruebo que se ha realizado correctamente con **getfacl.**

## Ejercicio 4.

**En el sistema que tenemos en uso, indicar los archivos de configuración existentes y comentar la misión de un par de ellos y cómo lo hacen.**

Para ver que archivos de configuración tiene PAM debemos ejecutar el siguiente comando:

```
jose@jose-CX61-2PC:~$ ls /etc/pam.d/
chfn                common-session-noninteractive  login     runuser-l
chpasswd            cron                           newusers  sshd
chsh                cups                           other     su
common-account      gdm-autologin                  passwd    sudo
common-auth         gdm-fingerprint                polkit-1  systemd-user
common-password     gdm-launch-environment         ppp
common-session      gdm-password                   runuser
jose@jose-CX61-2PC:~$
```

Realizando el **ls /etc/pam.d/** se ven todos los archivos de configuración de PAM, voy a analizar un par de ellos.

- **common-auth**
- **common-password**
- **newusers**

*Para la realización de este ejercicio he tenido que consultar los manuales de **pam_unix.**

Como he mencionado el primer archivo de configuración que voy a describir es **common-auth,** para ello lo que debemos de hacer es mostrar el contenido del archivo de configuración:


Como se puede apreciar en la imagen las distintas lineas que componen el archivo de configuración son:

| | | |
|---|---|---|
| **[1] auth** | **[success=1 default=ignore]** | **pam_unix.so nullok_secure** |
| **[2] auth** | **requisite** | **pam_deny.so** |
| **[3] auth** | **required** | **pam_permit.so** |
| **[4] auth** | **optional** | **pam_cap.so** |

Como se puede ver está formado por 5 líneas:

- La primera linea[1]: indica que el tipo de servicio es de autenticación (**auth**), que el tipo de control es **[success=1 default=ignore]** esto indica que en caso de que el módulo termine con éxito entonces se ignora la siguiente linea, en cualquier caso contrario al caso de éxito entonces se ignora esta línea y se pasa a la siguiente. Además se indican que los módulos a ejecutar son **pam_unix.so,** este módulo se encarga de extraer información de la cuenta, así como la autenticación para poder ejecutar la orden del proceso involucrado. Además como parámetro se introduce **nullok_secure,** para saber para que sirve este parámetro he tenido que buscar en el manual de **pam_unix,** el manual indica que este parámetro permite acceder a aquellos usuarios que tengan una contraseña vacía, es decir, en blanco.
- La segunda línea [2]: Indica también que es un servicio de autenticación (**auth**), el tipo de control es **requisite,** esto indica que en caso de que el módulo comunique un fallo inmediatamente se provoca un fallo de autenticación sin llegar a ejecutar los demás módulos. El módulo a ejecutar es **pam_deny.so** el cual se encarga de denegar el acceso. Esta línea de ejecutará sí y solo sí la primera linea falla.
- La tercera línea [3]: Indica también que es un servicio de autenticación (**auth**), el tipo de control en este caso es **required** lo que indica que en caso de que el módulo comunique un fallo se comunica de dicho fallo pero en este caso a

diferencia de **requisite** este tipo de control si invoca el resto de módulos. El módulo a ejecutar es **pam_permit.so** que según los manuales es un módulo que se encarga de permitir el acceso.

- La cuarta línea [4]: Indica que también es un servicio de autenticación (**auth**), en este caso el tipo de control es **optional** lo que indica que si esta línea tiene éxito o falla no es relevante. El módulo a ejecutar es **pam_cap.so** que según los manuales es un módulo que se encarga de establecer las capacidades heredables del proceso actual.

En este caso voy a describir el archivo de configuración de **common-password,** para ello lo que debemos hacer es mostrar el contenido del archivo del configuración:

```
jose@jose-CX61-2PC:~$ cat /etc/pam.d/common-password
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords.  Without this option,
# the default is Unix crypt.  Prior releases used the option "md5".
#
# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# 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        [success=1 default=ignore]      pam_unix.so obscure sha512
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
jose@jose-CX61-2PC:~$
```

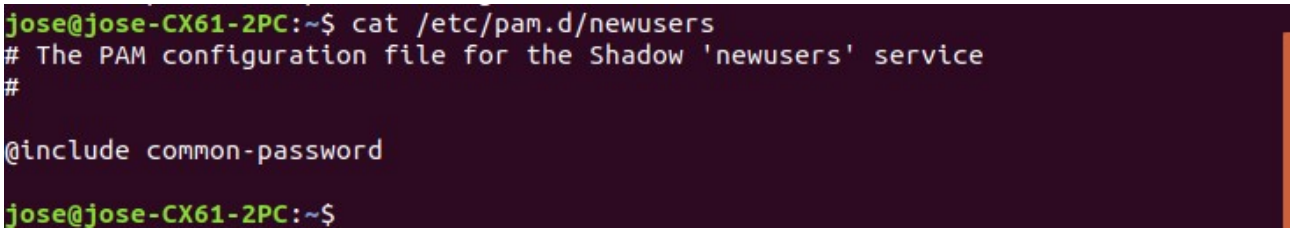
Como se puede ver en la imagen está compuesto por las siguientes líneas:

| | | |
|---|---|---|
| **[1] password** | **[success=1 default=ignore]** | **pam_unix.so obscure sha512** |
| **[2] password** | **requisite** | **pam_deny.so** |
| **[3] password** | **required** | **pam_permit.so** |
| **[4] password** | **optional** | **pam_gnome_kering.so** |

Ahora voy a explicar cada una de las líneas:

- La primera línea [1]: El tipo de servicio es de contraseña (**password**), el tipo de control es **[success=1 default=ignore]** esto quiere decir si los módulo a ejecutar resultan en éxito entonces la siguiente linea se ignore, en caso de que el módulo a ejecutar de un resultado distinto a éxito entonces se ignora esta línea y se pasa a la siguiente línea. El módulo a ejecutar es **pam_unix.so,** que como ya he mencionado anteriormente este módulo se encarga de extraer información de la cuenta, así como la autenticación para poder ejecutar la orden del proceso involucrado. Además se introducen dos parámetros **obscure** y **sha512,** como se puede intuir **sha512** indica el tipo de encriptado que se va a llevar a cabo, mientras que **obscure** según los manuales se encarga de activar algunas comprobaciones adicionales en la seguridad de la contraseña.
- La segunda línea [2]: El tipo de servicio es también de contraseña (**password**), el tipo de control es **requisite** lo que indica que si el módulo a ejecutar falla entonces se comunica el fallo de forma inmediata sin llegar a invocar los módulos restantes. El módulo a ejecutar es **pam_deny.so** el cual se encarga de denegar el acceso.
- La tercera línea [3]: El tipo de servicio también es de contraseña (**password**), el tipo de control en este caso de **required** que en caso de recibir fallo por los módulo a ejecutar comunicará el fallo pero en este caso sí se invocan a los módulos restantes. El módulo a ejecutar es **pam_permit.so** que se encarga de permitir el acceso.
- La última línea [4]: El tipo de servicio es también de contraseña (**password**), en este caso el tipo de control es opcional, es decir si la ejecución de los módulo resulta éxito o fallo será irrelevante. El módulo a ejecutar es **pam_gnome_kering.so** que según los manuales se encarga de la autenticación, la sesión y la contraseña.

Por último queda el archivo de configuración **newusers,** para poder ver el contenido del archivo de configuración se debe:




Como se puede ver en la imagen es básicamente un include de **common-password** el cual ya se ha explicado anteriormente, luego no voy a volver a explicarlo.

## Ejercicio 5.

**(a) Modificar la configuración para que se la autenticación exija que la clave de un usuario tenga una longitud mínima. Debemos utilizar el módulo pam_cracklib !Cuidado! Pues modificaciones inadecuadas puden dejar sin acceso a usuario que existen en el sistema.**

El archivo de configuración relacionado con la autenticación es el que ya he explicado en el ejercicio anterior, **common-password** el cual se encuentra en **/etc/pam.d/commom-password,** buscando en el manual de **pam_cracklib** he encontrado que existe un

parámetro **minlen=N** que indica el tamaño mínimo aceptable para la nueva contraseña, el valor por defecto para este parámetro es 9. En mi caso como estoy trabajando en mi ordenador persona y actualmente tengo una contraseña de 7 caracteres voy a establecer que el tamaño mínimo sea de 10 para evitar tener problemas con mi cuenta principal. Pues bien para ello:

Antes del cambio:

```
jose@jose-CX61-2PC:~$ cat /etc/pam.d/common-password
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords.  Without this option,
# the default is Unix crypt.  Prior releases used the option "md5".
#
# The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# 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        [success=1 default=ignore]      pam_unix.so obscure sha512
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
jose@jose-CX61-2PC:~$
```

Como se aprecia en la imagen la línea:

**password [success=1 default=ignore] pam_unix.so obscure sha512**

Voy a añadir un nuevo parámetro para indicar el tamaño mínimo como ya he menciona anteriormente utilizando **minlen=N,** de forma que el resultado debe ser:

**password [success=1 default=ignore] pam_unix.so obscure sha512 minlen=5**

Esto debe quedar en el archivo de la forma:

```
# here are the per-package modules (the "Primary" block)
password        [success=1 default=ignore]      pam_unix.so obscure sha512 minle
n=10
```

Debemos ser root para poder cambiar dicho archivo. Para comprobar que todo se ha realizado correctamente voy a intentar cambiar la contraseña de los usuarios que he creado en los anteriores ejercicios(Pepita lo he creado en el siguiente ejercicio pero es que

este ejercicio lo hice después ya que tenía dudas y no sabía como hacerlo así que cuando estaba bloqueado decidí continuar con los siguientes), por ejemplo el usuario de Pepita cuya contraseña actual es pepita123, voy a intentar cambiarla por pepita:

```
pepita@jose-CX61-2PC:~$ passwd
Cambiando la contraseña de pepita.
(actual) contraseña de UNIX:
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
Debe elegir una contraseña más larga
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
Debe elegir una contraseña más larga
Introduzca la nueva contraseña de UNIX:
```

Efectivamente, los cambios se han realizado correctamente.

**(b) Piensa otra modificación de tu preferencia e implementala. Por ejemplo, deshabilitar el acceso a root directo por consola, evitar que un usuario que no es el root tire el sistema, etc.**

Voy a realizar modificaciones en el archivo de configuración de **su,** de forma que solo el root pueda acceder a esta opción, para ello, lo primero recordar cuales son los archivos de configuración disponibles:

```
jose@jose-CX61-2PC:~$ ls /etc/pam.d/
chfn             common-session-noninteractive  login     runuser-l
chpasswd         cron                           newusers  sshd
chsh             cups                           other     su
common-account   gdm-autologin                  passwd    sudo
common-auth      gdm-fingerprint                polkit-1  systemd-user
common-password  gdm-launch-environment         ppp
common-session   gdm-password                   runuser
jose@jose-CX61-2PC:~$
```

Como se puede ver en la imagen existe el archivo de configuración **su,** para ver su contenido:

```
jose@jose-CX61-2PC:~$ cat /etc/pam.d/su
#
# The PAM configuration file for the Shadow `su' service
#

# This allows root to su without passwords (normal operation)
auth       sufficient pam_rootok.so

# Uncomment this to force users to be a member of group root
# before they can use `su'. You can also add "group=foo"
# to the end of this line if you want to use a group other
# than the default "root" (but this may have side effect of
# denying "root" user, unless she's a member of "foo" or explicitly
# permitted earlier by e.g. "sufficient pam_rootok.so").
# (Replaces the `SU_WHEEL_ONLY' option from login.defs)
# auth       required   pam_wheel.so
```

vemos que la única línea relacionada con el tipo de servicio de autenticación es

**auth sufficient pam_rootok.so**

Lo que indica que como ya he mencionado anteriormente se trata de un servicio de autenticación, el tipo de control es suficiente, es decir, si el módulo a ejecutar resulta exitoso entonces no se ejecutan los siguientes módulos y se comunica el éxito. El módulo a ejecutar es **pam_rootok.so** Para que sólo el root pueda acceder se debe añadir otra línea de tal forma que el resultado sea:

**auth requisite pam_denny.so**

Con esto se indica que el tipo de servicio es de autenticación (**auth**), el tipo de control es **requisite,** es decir, que en caso de que el módulo a ejecutar no resulte exitoso entonces se comunicará del fallo de forma inmediata sin llegar a ejecutar los módulos restantes. El módulo a ejecutar es **pam_denny.so** que se encarga de denegar el acceso. Con esto se cumple el objetivo que deseamos, solo el root podrá ejecutar **su**.

El resultado debe ser:

```
jose@jose-CX61-2PC:~$ cat /etc/pam.d/su
#
# The PAM configuration file for the Shadow `su' service
#

# This allows root to su without passwords (normal operation)
auth       sufficient pam_rootok.so
auth       requisite  pam_denny.so

# Uncomment this to force users to be a member of group root
# before they can use `su'. You can also add "group=foo"
# to the end of this line if you want to use a group other
# than the default "root" (but this may have side effect of
# denying "root" user, unless she's a member of "foo" or explicitly
# permitted earlier by e.g. "sufficient pam_rootok.so").
# (Replaces the `SU_WHEEL_ONLY' option from login.defs)
# auth       required   pam_wheel.so
```

## Ejercicio 6.

**Crear en el sistema un usuario con las características que deseéis, entrando como ese usuario cambiar la contraseña y analizar los archivos log para ver el mensaje correspondiente.**

1.- Lo primero que se debe realizar es crear un nuevo usuario, para ello:

```
jose@jose-CX61-2PC:~$ sudo su
root@jose-CX61-2PC:/home/jose# adduser pepita
Añadiendo el usuario `pepita' ...
Añadiendo el nuevo grupo `pepita' (1002) ...
Añadiendo el nuevo usuario `pepita' (1002) con grupo `pepita' ...
Creando el directorio personal `/home/pepita' ...
Copiando los ficheros desde `/etc/skel' ...
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para pepita
Introduzca el nuevo valor, o presione INTRO para el predeterminado
        Nombre completo []: pepita
        Número de habitación []: a
        Teléfono del trabajo []: b
        Teléfono de casa []: c
        Otro []: d
¿Es correcta la información? [S/n]
root@jose-CX61-2PC:/home/jose#
```

He creado a un nuevo usuario, el nuevo usuario es Pepita, con contraseña Pepita.

2.- Ahora procedo a cambiar la contraseña del nuevo usuario.

```
root@jose-CX61-2PC:/home/jose# passwd pepita
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@jose-CX61-2PC:/home/jose#
```

Ahora la nueva contraseña es pepita123.

3.- Procedo a comprobar los mensajes que se han generado en el log:

```
root@jose-CX61-2PC:/home/jose# cat /var/log/auth.log
```

En esta dirección se almacenan todos los logs relacionados con la gestión de cuentas:

```
Oct  1 21:00:47 jose-CX61-2PC systemd-logind[1078]: New session 3 of user root.
Oct  1 21:00:47 jose-CX61-2PC systemd: pam_unix(systemd-user:session): session opened for user root by (uid=0)
Oct  1 21:00:51 jose-CX61-2PC groupadd[23163]: group added to /etc/group: name=pepita, GID=1002
Oct  1 21:00:51 jose-CX61-2PC groupadd[23163]: group added to /etc/gshadow: name=pepita
Oct  1 21:00:51 jose-CX61-2PC groupadd[23163]: new group: name=pepita, GID=1002
Oct  1 21:00:51 jose-CX61-2PC useradd[23167]: new user: name=pepita, UID=1002, GID=1002, home=/home/pepita, shell=/bin/bash
Oct  1 21:00:57 jose-CX61-2PC passwd[23175]: pam_unix(passwd:chauthtok): password changed for pepita
Oct  1 21:00:57 jose-CX61-2PC passwd[23175]: gkr-pam: couldn't update the login keyring password: no old password was entered
Oct  1 21:01:04 jose-CX61-2PC chfn[23176]: changed user 'pepita' information
Oct  1 21:09:01 jose-CX61-2PC CRON[24004]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct  1 21:09:01 jose-CX61-2PC CRON[24004]: pam_unix(cron:session): session closed for user root
Oct  1 21:17:01 jose-CX61-2PC CRON[24737]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct  1 21:17:01 jose-CX61-2PC CRON[24737]: pam_unix(cron:session): session closed for user root
Oct  1 21:19:34 jose-CX61-2PC passwd[24747]: pam_unix(passwd:chauthtok): password changed for pepita
Oct  1 21:19:34 jose-CX61-2PC passwd[24747]: gkr-pam: couldn't update the login keyring password: no old password was entered
```

En los mensajes se puede comprobar cada una de las acciones que se han realizado, la creación de la nueva cuenta, el grupo en que se ha añadido, su directorio principal, el directorio shell, etc. Por último, también se especifica que la contraseña de pepita ha sido cambiada.

## Ejercicio 7.

**Modificar el archivo sudoers para que un usuario determinado tenga acceso a todas las órdenes del root.**

1.- Para poder añadir a un usuario con poder de sudoers se debe modificar el archivo **/etc/sudoers:**

```
jose@jose-CX61-2PC:~$ sudo su
root@jose-CX61-2PC:/home/jose# gedit /etc/sudoers
```

2.- Dentro del archivo se añade al usuario en cuestión de la forma:

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
pepita  ALL=(ALL:ALL) ALL
```

De esta forma pepita tendrá todo los permisos de root.

3.- Para comprobarlo voy a acceder a un archivo que solo los usuario con permisos de root pueden acceder:

```
pepita@jose-CX61-2PC:~$ sudo su
[sudo] contraseña para pepita:
Lo sentimos, vuelva a intentarlo.
[sudo] contraseña para pepita:
root@jose-CX61-2PC:/home/pepita# cat /etc/shadow
root:!:18160:0:99999:7:::
daemon:*:18113:0:99999:7:::
bin:*:18113:0:99999:7:::
sys:*:18113:0:99999:7:::
sync:*:18113:0:99999:7:::
games:*:18113:0:99999:7:::
man:*:18113:0:99999:7:::
```

Si intento acceder a dicho archivo con una cuenta que no tiene permisos de root, ocurre lo siguiente:

```
root@jose-CX61-2PC:/home/jose# login pepito
Contraseña:
Último inicio de sesión: sáb oct  3 11:16:46 CEST 2020 en pts/1
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Pueden actualizarse 3 paquetes.
0 actualizaciones son de seguridad.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2023.
$ cat /etc/shadow
cat: /etc/shadow: Permiso denegado
$
```

No tiene los permisos necesarios para ello.

## Ejercicio 8.

**Analiza el contenido de estos archivos de registro del sistema de prácticas y comprueba que efectivamente se registran los eventos indicados.**

1.- Para ver los accesos fallidos al sistema:

```
jose@jose-CX61-2PC:~$ sudo su
root@jose-CX61-2PC:/home/jose# utmpdump /var/log/btmp
Volcado utmp de /var/log/btmp
[7] [11929] [/1  ] [pepito  ] [pts/1      ] [                    ] [0.0.0.0        ] [2020-10-03T09:16:34,615601+0000]
[7] [19689] [/0  ] [pepita  ] [pts/0      ] [                    ] [0.0.0.0        ] [2020-10-03T10:13:12,409964+0000]
[7] [19691] [/0  ] [pepito  ] [pts/0      ] [                    ] [0.0.0.0        ] [2020-10-03T10:13:25,540201+0000]
root@jose-CX61-2PC:/home/jose#
```

De esta forma se pueden ver todos los accesos fallidos a las cuentas de pepito y pepita.

2.- Para ver los inicios de sesión llevados a cabo en los últimos 10 días:

```
root@jose-CX61-2PC:/home/jose# lastlog --time 10
Nombre           Puerto   De               Último
pepito           pts/1                     sáb oct  3 11:33:21 +0200 2020
pepita           pts/1                     sáb oct  3 11:15:19 +0200 2020
root@jose-CX61-2PC:/home/jose#
```

Si se desea ver todo el historial completa de las últimas sesiones:

```
root@jose-CX61-2PC:/home/jose# lastlog
Nombre           Puerto   De               Último
root                                       **Nunca ha accedido**
daemon                                     **Nunca ha accedido**
bin                                        **Nunca ha accedido**
sys                                        **Nunca ha accedido**
sync                                       **Nunca ha accedido**
games                                      **Nunca ha accedido**
man                                        **Nunca ha accedido**
lp                                         **Nunca ha accedido**
mail                                       **Nunca ha accedido**
news                                       **Nunca ha accedido**
uucp                                       **Nunca ha accedido**
proxy                                      **Nunca ha accedido**
www-data                                   **Nunca ha accedido**
backup                                     **Nunca ha accedido**
list                                       **Nunca ha accedido**
irc                                        **Nunca ha accedido**
gnats                                      **Nunca ha accedido**
nobody                                     **Nunca ha accedido**
systemd-network                            **Nunca ha accedido**
systemd-resolve                            **Nunca ha accedido**
syslog                                     **Nunca ha accedido**
messagebus                                 **Nunca ha accedido**
_apt                                       **Nunca ha accedido**
uuidd                                      **Nunca ha accedido**
avahi-autoipd                              **Nunca ha accedido**
usbmux                                     **Nunca ha accedido**
dnsmasq                                    **Nunca ha accedido**
rtkit                                      **Nunca ha accedido**
cups-pk-helper                             **Nunca ha accedido**
speech-dispatcher                           **Nunca ha accedido**
whoopsie                                   **Nunca ha accedido**
kernoops                                   **Nunca ha accedido**
saned                                      **Nunca ha accedido**
pulse                                      **Nunca ha accedido**
avahi                                      **Nunca ha accedido**
colord                                     **Nunca ha accedido**
hplip                                      **Nunca ha accedido**
geoclue                                    **Nunca ha accedido**
gnome-initial-setup                           **Nunca ha accedido**
gdm                                        **Nunca ha accedido**
jose                                       **Nunca ha accedido**
mysql                                      **Nunca ha accedido**
sshd                                       **Nunca ha accedido**
mongodb                                    **Nunca ha accedido**
pepito           pts/1                     sáb oct  3 11:33:21 +0200 2020
pepita           pts/1                     sáb oct  3 11:15:19 +0200 2020
root@jose-CX61-2PC:/home/jose#
```

3.- Para ver los registros de los usuarios que todavía están conectados al sistema:

```
root@jose-CX61-2PC:/home/jose# utmpdump /var/run/utmp
Volcado utmp de /var/run/utmp
[2] [00000] [~~  ] [reboot  ] [~          ] [5.4.0-48-generic    ] [0.0.0.0        ] [2020-10-02T08:16:55,023242+0000]
[1] [00053] [~~  ] [runlevel] [~          ] [5.4.0-48-generic    ] [0.0.0.0        ] [2020-10-02T08:17:04,716909+0000]
[7] [03739] [    ] [jose    ] [:0         ] [:0                  ] [0.0.0.0        ] [2020-10-03T08:50:47,576798+0000]
[7] [11679] [/0  ] [pepita  ] [pts/0      ] [                    ] [0.0.0.0        ] [2020-10-03T09:12:49,499074+0000]
[7] [15087] [/1  ] [pepito  ] [pts/1      ] [                    ] [0.0.0.0        ] [2020-10-03T09:33:21,456783+0000]
root@jose-CX61-2PC:/home/jose#
```

4.- Para ver el registros de todos los usuarios que han hecho login y logout desde que se creó el archivo:

```
root@jose-CX61-2PC:/home/jose# utmpdump /var/log/wtmp
Volcado utmp de /var/log/wtmp
[8] [03734] [    ] [        ] [:0         ] [:0               ] [0.0.0.0       ] [2020-10-01T08:48:58,968938+0000]
[1] [00000] [~~  ] [shutdown] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T08:49:01,439828+0000]
[2] [00000] [~~  ] [reboot  ] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T08:49:13,024861+0000]
[1] [00053] [~~  ] [runlevel] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T08:49:22,311120+0000]
[7] [02660] [    ] [jose    ] [:0        ] [:0               ] [0.0.0.0       ] [2020-10-01T08:49:25,177586+0000]
[1] [00000] [~~  ] [shutdown] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T10:23:41,792475+0000]
[2] [00000] [~~  ] [reboot  ] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T10:36:41,018216+0000]
[1] [00053] [~~  ] [runlevel] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T10:36:50,941817+0000]
[7] [02534] [    ] [jose    ] [:0        ] [:0               ] [0.0.0.0       ] [2020-10-01T10:36:54,709527+0000]
[1] [00000] [~~  ] [shutdown] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T10:41:38,105179+0000]
[2] [00000] [~~  ] [reboot  ] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T15:49:14,021800+0000]
[1] [00053] [~~  ] [runlevel] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T15:49:23,755283+0000]
[7] [02461] [    ] [jose    ] [:0        ] [:0               ] [0.0.0.0       ] [2020-10-01T15:49:25,114692+0000]
[8] [02461] [    ] [        ] [:0        ] [:0               ] [0.0.0.0       ] [2020-10-01T16:00:42,324395+0000]
[1] [00000] [~~  ] [shutdown] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T16:00:45,117843+0000]
[2] [00000] [~~  ] [reboot  ] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T17:23:22,018419+0000]
[1] [00053] [~~  ] [runlevel] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T17:23:31,677959+0000]
[7] [02650] [    ] [jose    ] [:0        ] [:0               ] [0.0.0.0       ] [2020-10-01T17:23:40,121785+0000]
[8] [02650] [    ] [        ] [:0        ] [:0               ] [0.0.0.0       ] [2020-10-01T19:30:06,564445+0000]
[1] [00000] [~~  ] [shutdown] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T19:31:36,887133+0000]
[2] [00000] [~~  ] [reboot  ] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T19:31:54,019361+0000]
[1] [00053] [~~  ] [runlevel] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T19:32:04,151612+0000]
[7] [02454] [    ] [jose    ] [:0        ] [:0               ] [0.0.0.0       ] [2020-10-01T19:32:15,053121+0000]
[1] [00000] [~~  ] [shutdown] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-01T19:32:41,152876+0000]
[2] [00000] [~~  ] [reboot  ] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-02T08:16:55,023242+0000]
[1] [00053] [~~  ] [runlevel] [~         ] [5.4.0-48-generic ] [0.0.0.0       ] [2020-10-02T08:17:04,716909+0000]
[7] [03739] [    ] [jose    ] [:0        ] [:0               ] [0.0.0.0       ] [2020-10-03T08:50:47,576798+0000]
[7] [11590] [    ] [pepita  ] [pts/0     ] [                 ] [0.0.0.0       ] [2020-10-03T09:12:49,158322+0000]
[7] [11758] [    ] [pepita  ] [pts/1     ] [                 ] [0.0.0.0       ] [2020-10-03T09:15:19,741801+0000]
[7] [11852] [    ] [pepito  ] [pts/1     ] [                 ] [0.0.0.0       ] [2020-10-03T09:16:09,955315+0000]
[8] [11852] [    ] [        ] [pts/1     ] [                 ] [0.0.0.0       ] [2020-10-03T09:16:16,795831+0000]
[7] [11933] [    ] [pepito  ] [pts/1     ] [                 ] [0.0.0.0       ] [2020-10-03T09:16:46,224462+0000]
[8] [11933] [    ] [        ] [pts/1     ] [                 ] [0.0.0.0       ] [2020-10-03T09:17:05,764285+0000]
[8] [11758] [    ] [        ] [pts/1     ] [                 ] [0.0.0.0       ] [2020-10-03T09:17:10,572601+0000]
[7] [15026] [    ] [pepito  ] [pts/1     ] [                 ] [0.0.0.0       ] [2020-10-03T09:33:21,265387+0000]
[8] [15026] [    ] [        ] [pts/1     ] [                 ] [0.0.0.0       ] [2020-10-03T09:39:45,392036+0000]
[8] [11590] [    ] [        ] [pts/0     ] [                 ] [0.0.0.0       ] [2020-10-03T09:40:21,423013+0000]
root@jose-CX61-2PC:/home/jose#
```

5.- Para ver toda la actividad que se ha realizado con la orden sudo:

```
root@jose-CX61-2PC:/home/jose# cat /var/log/auth.log
Sep 30 10:09:01 jose-CX61-2PC CRON[8657]: pam_unix(cron:session): session opened
 for user root by (uid=0)
Sep 30 10:09:01 jose-CX61-2PC CRON[8657]: pam_unix(cron:session): session closed
 for user root
Sep 30 10:17:01 jose-CX61-2PC CRON[8925]: pam_unix(cron:session): session opened
 for user root by (uid=0)
Sep 30 10:17:01 jose-CX61-2PC CRON[8925]: pam_unix(cron:session): session closed
 for user root
Sep 30 10:35:37 jose-CX61-2PC systemd-logind[1063]: Watching system buttons on /
dev/input/event16 (1C:91:9D:F4:A1:68)
Sep 30 10:39:01 jose-CX61-2PC CRON[10565]: pam_unix(cron:session): session opene
d for user root by (uid=0)
Sep 30 10:39:01 jose-CX61-2PC CRON[10565]: pam_unix(cron:session): session close
d for user root
Sep 30 11:09:01 jose-CX61-2PC CRON[12492]: pam_unix(cron:session): session opene
d for user root by (uid=0)
Sep 30 11:09:01 jose-CX61-2PC CRON[12492]: pam_unix(cron:session): session close
d for user root
Sep 30 11:17:01 jose-CX61-2PC CRON[12722]: pam_unix(cron:session): session opene
d for user root by (uid=0)
Sep 30 11:17:01 jose-CX61-2PC CRON[12722]: pam_unix(cron:session): session close
d for user root
Sep 30 11:34:05 jose-CX61-2PC dbus-daemon[1096]: [system] Rejected send message,
```

6.- Ya por último para poder ver los mensajes del sistema, se pueden ver en:

```
root@jose-CX61-2PC:/home/jose# cat /var/log/syslog
Oct  3 10:55:43 jose-CX61-2PC anacron[3512]: Job `cron.daily' terminated
Oct  3 10:55:43 jose-CX61-2PC anacron[3512]: Normal exit (1 job run)
Oct  3 11:03:17 jose-CX61-2PC systemd[1]: Started Run anacron jobs.
Oct  3 11:03:17 jose-CX61-2PC anacron[7331]: Anacron 2.3 started on 2020-10-03
Oct  3 11:03:17 jose-CX61-2PC anacron[7331]: Normal exit (0 jobs run)
Oct  3 11:08:00 jose-CX61-2PC dbus-daemon[3760]: [session uid=1000 pid=3760] Act
ivating via systemd: service name='org.gnome.Terminal' unit='gnome-terminal-serv
er.service' requested by ':1.79' (uid=1000 pid=8491 comm="/usr/bin/gnome-termina
l.real " label="unconfined")
Oct  3 11:08:00 jose-CX61-2PC systemd[3711]: Starting GNOME Terminal Server...
Oct  3 11:08:00 jose-CX61-2PC dbus-daemon[3760]: [session uid=1000 pid=3760] Suc
cessfully activated service 'org.gnome.Terminal'
Oct  3 11:08:00 jose-CX61-2PC systemd[3711]: Started GNOME Terminal Server.
Oct  3 11:08:08 jose-CX61-2PC systemd[1]: Created slice User Slice of root.
Oct  3 11:08:08 jose-CX61-2PC systemd[1]: Starting User Manager for UID 0...
Oct  3 11:08:08 jose-CX61-2PC systemd[1]: Started Session 7 of user root.
Oct  3 11:08:08 jose-CX61-2PC systemd[8514]: Starting D-Bus User Message Bus Soc
ket.
Oct  3 11:08:08 jose-CX61-2PC systemd[8514]: Listening on GnuPG cryptographic ag
ent and passphrase cache (restricted).
Oct  3 11:08:08 jose-CX61-2PC systemd[8514]: Listening on GnuPG cryptographic ag
ent (ssh-agent emulation).
Oct  3 11:08:08 jose-CX61-2PC systemd[8514]: Listening on GnuPG cryptographic ag
ent and passphrase cache.
```

## Ejercicio 9.

**Analizar las conexiones al sistema de prácticas y al de casa. ¿Hay o ha habido alguna conexión ajena al equipo?**

Como estos ejercicios los hago en casa solo puedo mostrar los resultados de casa. Para poder ver si se ha realizado alguna conexión externa a mi pc en los últimos 30 días, voy a comprobarlo con la orden **lastlog:**

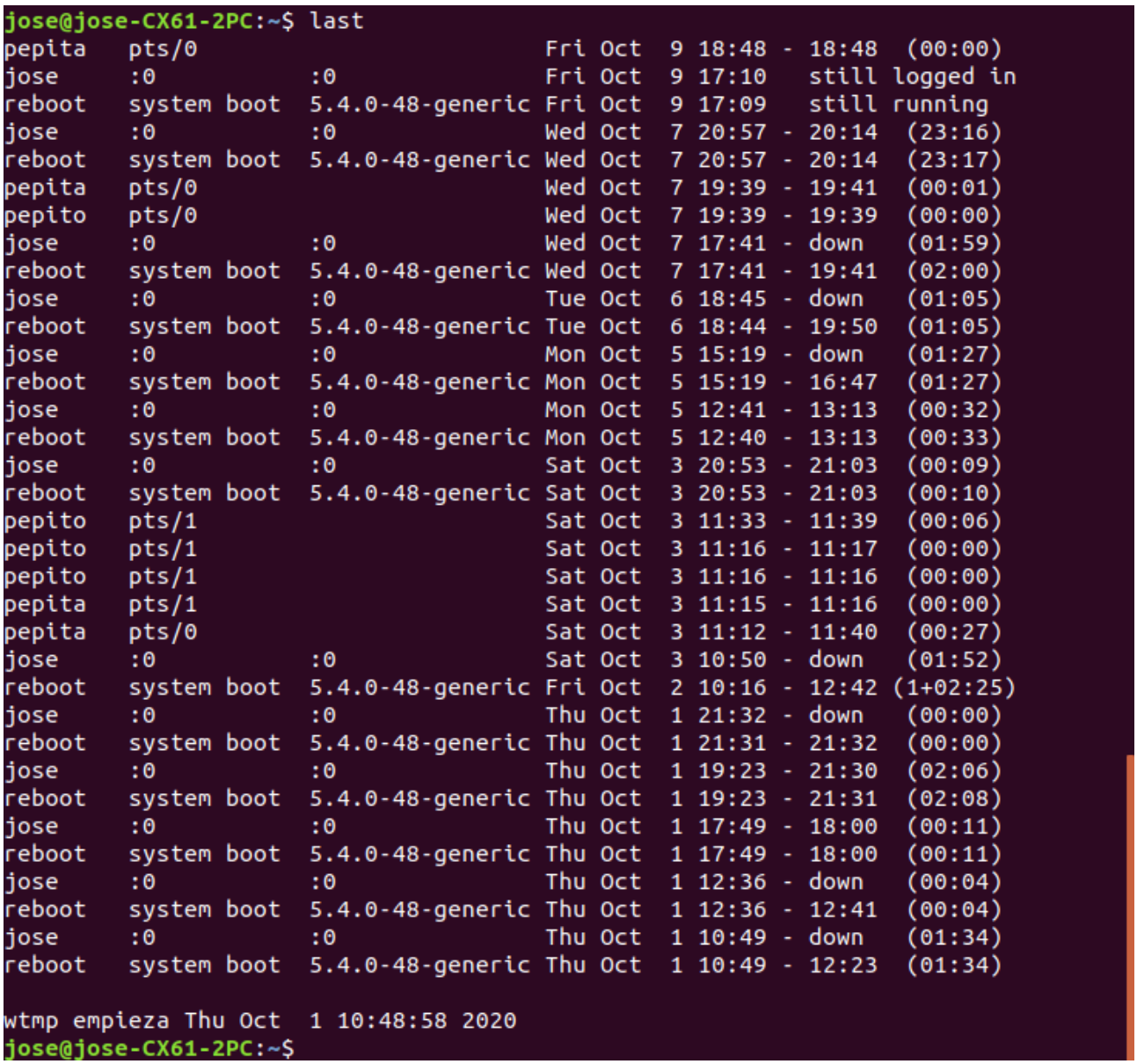
```
root@jose-CX61-2PC:/home/jose# lastlog --time 30
Nombre           Puerto   De               Último
pepito           pts/1                     sáb oct  3 11:33:21 +0200 2020
pepita           pts/1                     sáb oct  3 11:15:19 +0200 2020
root@jose-CX61-2PC:/home/jose#
```

Además intentos fallidos:

```
root@jose-CX61-2PC:/home/jose# lastb
pepito   pts/0                        Sat Oct  3 12:13 - 12:13  (00:00)
pepita   pts/0                        Sat Oct  3 12:13 - 12:13  (00:00)
pepito   pts/1                        Sat Oct  3 11:16 - 11:16  (00:00)

btmp empieza Sat Oct  3 11:16:34 2020
root@jose-CX61-2PC:/home/jose#
```

Ahora voy a comprobar que resultados me ofrece **last:**




Como se puede ver en las imágenes anteriores todos los accesos son de cuentas locales, no he encontrado ningún intento de login extraño.