

ADSO
Training 4
Gestió d'usuaris

Índex

1. Introducció.....	3
1.1. Objectius.....	3
2. Profile i entorn d'usuari.....	3
La variable d'entorn que defineix el prompt en la majoria dels shells de Unix com Bash és PS1. Aquesta és la variable primària que s'utilitza per definir l'aparença del prompt de la línia d'ordres quan s'utilitza un shell interactiu.....	
3. Creació manual d'usuaris.....	4
4. Creació automàtica d'usuaris.....	10
Trieu i justifiqueu el lloc més adequat per als home de tots els usuaris.....	
5. Connexió remota d'usuaris.....	14
6. Eliminació i des-activació d'usuaris.....	17
7. Usuari especial asosh.....	25
8. Sudo i control d'execució d'aplicacions.....	27

1. Introducció

Al sistema cada usuari té un compte associat. Un compte són tots els fitxers, recursos i informació que pertanyen a cada usuari. Els comptes d'usuari permeten al sistema diferenciar les dades i processos de cada usuari i permeten als usuaris protegir la seva informació.

Per al kernel els usuaris s'identifiquen amb un nombre enter conegut com l'identificador d'usuari (*user identifier* o *UID*). A més hi ha una base de dades que associa el UID amb un nom textual: el *username*. Aquest *username* és l'utilitzat per l'usuari per fer *login*. La base de dades d'usuaris inclou altra informació relativa a l'usuari com la ruta del directori *home*, el nom complet de l'usuari i l'interpret de comandes (shell).

La creació de un nou usuari inclou l'assignació d'un UID i la modificació de la base de dades d'usuaris per assignar els paràmetres propis de l'usuari. A més és necessari associar almenys un grup a l'usuari i finalment copiar els fitxers de configuració i personalització al directori *home* de cada usuari.

Opcionalment es pot assignar l'usuari a més d'un grup, la qual cosa permet a l'administrador del sistema dividir els usuaris en grups amb diferents permisos i privilegis. D'aquesta manera podem mantenir un millor control sobre què poden fer els usuaris.

1.1. Objectius

Gestionar els usuaris del sistema: realitzar l'alta i baixa d'usuaris i modificar les propietats dels comptes d'usuari.

2. Profile i entorn d'usuari

Quant s'inicia un *login* interactiu, el *shell* automàticament executa un o més fitxers predefinits. Cada *shell* executa fitxers diferents. El shell **bash** executa el fitxer */etc/profile* i a més a més executa el fitxer *.profile*, *.bash_profile* o *.bashrc* del *home* de cada usuari. El fitxer */etc/profile* permet a l'administrador del sistema definir un entorn comú per a tots els usuaris, especialment definint la variable **PATH**. Per altra banda *.bash_profile* o *.bashrc* permet a cada usuari definir el seu propi entorn adequant el *PATH*, el *prompt*, etc.

Quan es crea el directori *home* d'un usuari s'han de copiar els fitxers del directori */etc/skel*. L'administrador del sistema pot posar fitxers a */etc/skel* que donin un entorn inicial pels usuaris. Per exemple, com administradors creeu un fitxer */etc/skel/.bashrc* (si no està ja creat) amb unes definicions bàsiques que després l'usuari podria canviar.

Comproveu que al PATH de tots els usuaris hi sigui el directori */usr/local/bin* i, si cal, feu que el *.bashrc* modifiqui el PATH per incloure un directori bin situat en el directori *home* de cada usuari (**\$HOME/bin**).

Executem la comanda:

```
echo PATH
```

Si */usr/local/bin* no apareix editem */etc/profile* i afegim:

```
export PATH="/usr/local/bin:$PATH"
```

Volem que el *prompt* sigui el *username* seguit de la data actual i finalment "> " (per exemple, el de l'usuari xavim seria "xavim (Tue April 10) >")

```
root@AusiasP (Wed Nov 13):~# export PS1="\u (\d) > "
root (Wed Nov 13) >
```

Quina variable d'entorn té la definició del prompt?

La variable d'entorn que defineix el prompt en la majoria dels shells de Unix com Bash és PS1. Aquesta és la variable primària que s'utilitza per definir l'aparença del prompt de la línia d'ordres quan s'utilitza un shell interactiu.

Per verificar la configuració actual del prompt, s'utilitza el comandament `echo $PS1` en el terminal.

3. Creació manual d'usuaris

Ara volem donar d'alta un compte d'usuari per a dos usuaris. Abans de començar trieu els paràmetres de cada usuari. Els usuaris han de formar part del grup *admin*.

Omple la següent taula:

Editeu la base de dades d'usuaris per afegir els nous usuaris. Utilitzeu la comanda *vipw* per editar aquest fitxer.

Assignació UID:

- Ha de ser major o igual a 1000, ja que els que són menors s'utilitzen per als usuaris del sistema.
- No podem assignar un UID si ja està assignat a un altre usuari prèviament:
 - Ho comprovem amb la comanda `grep "UID" /etc/passwd`

A Usuari 1 li donarem el UID 1001, comprovem que no hi ha un usuari amb

aquest UID assignat:

```
root@ehsanR (Wed Nov 20) >:~# grep 1001 /etc/passwd
root@ehsanR (Wed Nov 20) >:~#
```

A Usuari 2 li assignem el UID 1002, fem la mateixa comprovació:

```
root@ehsanR (Wed Nov 20) >:~# grep 1002 /etc/passwd
root@ehsanR (Wed Nov 20) >:~#
```

paràmetres /Usuari	Usuari 1	Usuari 2
UID	1001	1002
<i>Username</i>	user1	user2
Directori home	/home/user1	/home/user2
<i>Shell</i>	/bin/bash	/bin/bash
Grups	admin	admin

Entrem a usuari root i escrivim la comanda vipw i escollim la primera opció:

```
root@ehsanR (Wed Nov 20) >:~# vipw
Select an editor. To change later, run 'select-editor'.
 1. /bin/nano      <---- easiest
 2. /usr/bin/vim.basic
 3. /usr/bin/vim.tiny
Choose 1-3 [1]: █
```

Afegim les següents línies al final per als nous usuaris:

```
user1:x:1001:1001::/home/user1:/bin/bash
```

```
user2:x:1002:1002::/home/user2:/bin/bash
```

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
admin:x:0:0:root:/root:/bin/bash
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110:/nonexistent:/usr/sbin/nologin
aso:x:1000:1000,,:/home/aso:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
avahi:x:105:112:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
pulse:x:106:113:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin
saned:x:107:116:/var/lib/saned:/usr/sbin/nologin
lightdm:x:108:117:Light Display Manager:/var/lib/lightdm:/bin/false
polkitd:x:998:998:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:109:118:RealtimeKit,,:/proc:/usr/sbin/nologin
colord:x:110:119:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
user1:x:1001:1001:/home/user1:/bin/bash
user2:x:1002:1002:/home/user2:/bin/bash

```

Desem amb Ctrl + o i sortim amb Ctrl + x.

Quina és la diferencia en usar vipw o editar directament el fitxer de passwd amb vi?(pista: obriu dos vipw en sessions diferents)

Si fem servir vipw, ens assegurem que es bloquegi l'accés al fitxer /etc/passwd mentre s'està editant. El seu ús ens permet evitar que altres processos o usuaris facin canvis al fitxer de forma simultània, el que podria causar inconsistències.

D'altra banda, si ho editem directament amb vi, això no passaria, de manera que un altre usuari o procés podria modificar el fitxer al mateix temps.

De la mateixa manera, utilitzeu la comanda vigr per crear un grup per a cada usuari i definir els altres grups que siguin necessaris.

Per afegir un grup per a cada usuari amb un GID únic:

- Comprovem que en el fitxer /etc/group no hi hagi un grup amb el mateix GID

Fem servir la comanda grep "UID" /etc/group. Farem servir el GID 1003 per admin

```

root@ehsanR (Wed Nov 20) >:~# grep admin /etc/group
root@ehsanR (Wed Nov 20) >:~# grep 1003 /etc/group
root@ehsanR (Wed Nov 20) >:~#

```

- Escrivim la comanda vigr i afegim la següent línia:

admin:x:1003:

```
lightdm:x:117:
polkitd:x:998:
rtkit:x:118:
colord:x:119:
admin:x:1003:
```

- Per últim afegim els usuaris al grup admin escrivint les comandes:

```
usermod -aG admin user1
```

```
usermod -aG admin user2
```

```
root@ehsanR (Wed Nov 20) >:~# usermod -aG admin user1
root@ehsanR (Wed Nov 20) >:~# usermod -aG admin user2
```

Això és el que hauria de sortir si fem la comanda `id nomUsuari`:

```
root@ehsanR (Wed Nov 20) >:~# id user1
uid=1001(user1) gid=1001 groups=1001,1003(admin)
root@ehsanR (Wed Nov 20) >:~# id user2
uid=1002(user2) gid=1002 groups=1002,1003(admin)
```

Com es pot desactivar un compte de forma que l'usuari no pugui fer *login*?

Es pot de dues maneres:

- Bloquejant el compte amb `usermod -L nomUsuari`
 - Això afegeix el símbol `!` davant de la contrasenya xifrada al fitxer `/etc/shadow`, per tant, l'usuari no podrà iniciar sessió perquè la contrasenya queda inhabilitada, però el compte segueix existent.
- Canviant el shell de l'usuari a `/usr/sbin/nologin`: `sudo usermod -s /usr/sbin/nologin nomUsuari`
 - Canvia la shell de l'usuari a una shell especial que mostra un missatge indicant que el compte està desactivat.

Desactiveu els comptes nous fins que no hagi finalitzat de donar d'alta els usuaris.

Escrivim la comanda `usermod -L nomUsuari`:

```
root@ehsanR (Wed Nov 20) >:~# usermod -L user1
root@ehsanR (Wed Nov 20) >:~# usermod -L user2
```

Creeu el directori *home* de cada usuari, copieu els fitxers que estiguin a `/etc/skel` i assigneu el propietari i permisos adequats per al directori *home* i per a tots els fitxers que estiguin dintre del directori.

Creem els directoris amb les comandes:

```
mkdir /home/user1
```

```
mkdir /home/user2
```

```
root@ehsanR (Wed Nov 20) >:~# mkdir /home/user1
root@ehsanR (Wed Nov 20) >:~# mkdir /home/user2
```

Seguidament escrivim les comandes per copiar els fitxers del directori /etc/skel a /home/nomUsuari:

```
cp -r /etc/skel/. /home/user1/
```

```
cp -r /etc/skel/. /home/user2/
```

```
root@ehsanR (Wed Nov 20) >:~# cp -r /etc/skel/. /home/user1
root@ehsanR (Wed Nov 20) >:~# cp -r /etc/skel/. /home/user2
```

I assignem els propietaris escrivint:

```
chown -R user1:admin /home/user1
```

```
chown -R user2:admin /home/user2
```

```
root@ehsanR (Wed Nov 20) >:~# chown -R user1:admin /home/user1
root@ehsanR (Wed Nov 20) >:~# chown -R user2:admin /home/user2
```

Assignem permisos de lectura, escriptura i d'execució al propietari, als altres usuaris i a la resta només de lectura i execució.

```
chmod 755 /home/user1
```

```
chmod 755 /home/user2
```

```
root@ehsanR (Wed Nov 20) >:~# chmod 755 /home/user1
root@ehsanR (Wed Nov 20) >:~# chmod 755 /home/user2
```

Ara assigneu una clau (password) per a cada usuari nou.

Per raons de seguretat la clau no es posa directament al fitxer /etc/passwd. Per això hi ha un altre fitxer anomenat /etc/shadow que només té permisos de lectura per al superusuari. En aquest fitxer es posa la clau xifrada i altres paràmetres associats a la vigència de la clau.

Amb quina comanda es pot editar de manera segura el fitxer de *shadow*?

Utilitzem la comanda passwd per establir una contrasenya per a cada usuari:

```
passwd user1
```

```
root@ehsanR (Wed Nov 20) >:~# passwd user1
New password:
Retype new password:
passwd: password updated successfully
```


Quin es el significat dels altres paràmetres que es poden definir al fitxer de shadow?

```
user1:$y$j9T$FQDuAJ4dmcnMesKl36XoP0$6B4ZuH/6,kPtED6lJb4ithCYieu0XRhr6FcXz5HHiCB:20047:::~
```

1:2:3:4:5:6:7:8

- ### Amb quina comanda es poden modificar aquests paràmetres?

- chage -M X nomUsuari (establir nombre màxim de dies abans de forçar un canvi de contrasenya)
- chage -m X nomUsuari (establir el nombre mínim de dies entre canvis de contrasenya)
- chage -W X nomUsuari (definir dies d'inactivitat abans de bloquejar el compte)

Per consultar la configuració actual, escrivim `chage -l nomUsuari`:

```

root@ehsanR (Wed Nov 20) >:~# chage -l user1
Last password change                : Nov 20, 2024
Password expires                    : never
Password inactive                   : never
Account expires                     : never
Minimum number of days between password change : -1
Maximum number of days between password change : -1
Number of days of warning before password expires : -1

```

Per editar altres paràmetres del compte d'usuari es poden utilitzar les comandes: chfn i chsh. Utilitzeu aquestes comandes per assignar valors adequats als comptes creats.

Si executem chfn nomUsuari (que modifica camps com el nom complet, número de telèfon, etc., que es troben al fitxer /etc/passwd), ens apareix això:

```

root@ehsanR (Wed Nov 20) >:~# chfn user1
Changing the user information for user1
Enter the new value, or press ENTER for the default
Full Name []: █

```

Afegim la nostra informació:

```

root@ehsanR (Wed Nov 20) >:~# chfn user1
Changing the user information for user1
Enter the new value, or press ENTER for the default
Full Name []: Floyd Mayweather
Room Number []: 13
Work Phone []: 112
Home Phone []: 911
Other []:
root@ehsanR (Wed Nov 20) >:~# █

```

Si fem cat /etc/passwd podrem observar la nostra informació:

```

user1:x:1001:1001:Floyd Mayweather,13,112,911:/home/user1:/bin/bash

```

D'altra banda, chsh permet modificar el shell predeterminat d'un usuari. Aquesta configuració es troba al camp final de cada entrada al fitxer /etc/passwd.

Si escrivim la comanda chsh -s /bin/sh user1, canvia el shell predeterminat:

```

root@ehsanR (Wed Nov 20) >:~# chsh -s /bin/sh user1

```

Podem veure-ho si fem cat /etc/passwd:

```

user1:x:1001:1001:Floyd Mayweather,13,112,911:/home/user1:/bin/sh

```

4. Creació automàtica d'usuaris

La majoria de les distribucions de Linux inclouen programes per automatitzar les tasques de creació i modificació de dades d'usuaris. Unes d'aquestes aplicacions son useradd i adduser, que permeten crear usuaris i assignar els diferents

paràmetres necessaris per donar d'alta cada compte.

Utilitzeu aquestes comandes per donar d'alta els usuaris següents:

Product Owners: PO1, PO2, PO3

Scrum Master: SM1, SM2

Equip de Desenvolupament (ED): El nom d'usuari del compte serà: nomX, on nom és el vostre nom i X la primera lletra del vostre cognom en minúscules.

Trieu i justifiqueu el lloc més adequat per als home de tots els usuaris.

El lloc més adequat es /home/ ja que és la ubicació estàndard per norma. Una de les raons es que els permisos del directori /home garanteixen la privadesa de cada usuari i permeten un control segur de l'accés als seus fitxers. L'estructura també separa clarament els fitxers del sistema dels fitxers dels usuaris, evitant problemes quan s'actualitza o modifica el sistema.

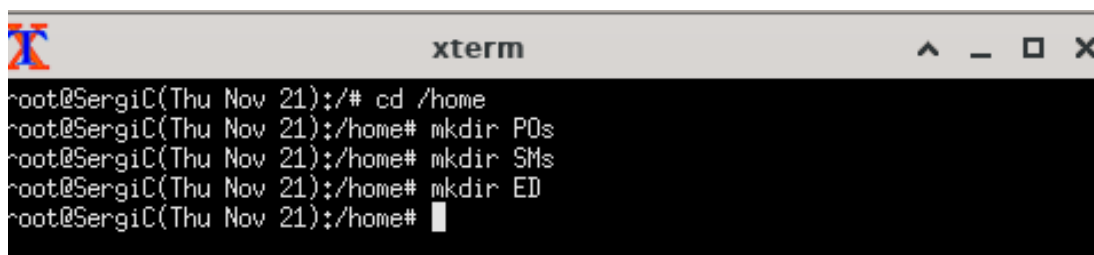
Els permisos de cadascun d'aquests grups d'usuaris (POs, SMs i ED) venen definits de la següent forma:

- ☐ Els POs tindran control d'accés a nivell de grup a tots els fitxers de tots els usuaris definits. És a dir: l'accés dels POs a fitxers i directoris dels altres usuaris vindrà determinat pels permisos de grup d'aquests fitxers i directoris. No tindrà accés als altres PO
- ☐ Els SMs tindran control d'accés, a nivell de grup, a tots els fitxers de tots els usuaris, exceptuant els dels usuaris POs i els altres SM.
- ☐ Els membres del ED NO tindran accés, a nivell de grup, als fitxers dels POs, ni dels SMs, ni dels altres membres del ED.

Tingueu en compte que les condicions anteriors estan especificant els nivells d'accés. El nivell d'accés només indica a quin nivell es miren els privilegis sobre un fitxer o directori determinat (user, group, other).

Mostra tot el procés de creació indicant pas a pas que s'ha fet

Creem directoris a home per tenir ordenats els usuaris



```
root@SergiC(Thu Nov 21):/# cd /home
root@SergiC(Thu Nov 21):/home# mkdir POs
root@SergiC(Thu Nov 21):/home# mkdir SMs
root@SergiC(Thu Nov 21):/home# mkdir ED
root@SergiC(Thu Nov 21):/home#
```

Ara creem els grups on després crearem els usuaris, ho fem amb groupadd nom

```

root@SergiC(Wed Nov 27):/home/P0s# groupadd P0
root@SergiC(Wed Nov 27):/home/P0s# groupadd SM
root@SergiC(Wed Nov 27):/home/P0s# groupadd ED

```

En cas que ens hàgim equivocat o vulguem esborrar-ho, hem de fer: `groupdel nomgrup`
 comprovem que tot hagi sortit correctament fent `nano /etc/group`

```

root@SergiC(Thu Nov 21):~# nano /etc/group

```

```

messagebus:x:110:
aso:x:1000:
systemd-coredump:x:999:
sgx:x:111:
avahi:x:112:
pulse:x:113:
pulse-access:x:114:
scanner:x:115:saned
saned:x:116:
lightdm:x:117:
polkitd:x:998:
rtkit:x:118:
colord:x:119:
admin:x:1003:user1,user2
P0:x:1004:
SM:x:1005:
ED:x:1006:

```

[^]G Help [^]O Write Out [^]W Where Is [^]K Cut [^]T Execute [^]C Location
[^]X Exit [^]R Read File [^] Replace [^]U Paste [^]J Justify [^]/ Go To Line

Creem els usuaris dins del grup pertinent, ho podem fer amb
`useradd -m -d /home/directori/nomusuari -s /bin/bash -G nomgrup nomusuari`
 on directori és el que hem creat abans

```

root@SergiC(Wed Nov 27):~# useradd -m -d /home/P0s/P01 -G P0 P01
root@SergiC(Wed Nov 27):~# useradd -m -d /home/P0s/P02 -G P0 P02
root@SergiC(Wed Nov 27):~# useradd -m -d /home/P0s/P03 -G P0 P03
root@SergiC(Wed Nov 27):~# useradd -m -d /home/SMs/SM1 -G SM SM1
root@SergiC(Wed Nov 27):~# useradd -m -d /home/SMs/SM2 -G SM SM2
root@SergiC(Wed Nov 27):~# useradd -m -d /home/ED/SergiC -G ED SergiC

```

Creem les contrasenyes per a cada usuari amb `passwd nomusuari`

```

root@SergiC(Thu Nov 21):~# passwd P03
New password:
Retype new password:
passwd: password updated successfully
root@SergiC(Thu Nov 21):~# passwd P01
New password:
Retype new password:
passwd: password updated successfully
root@SergiC(Thu Nov 21):~# passwd P02
New password:
Retype new password:
passwd: password updated successfully

```

```

root@SergiC(Thu Nov 21):~# passwd SM1
New password:
Retype new password:
passwd: password updated successfully
root@SergiC(Thu Nov 21):~# passwd SM2
New password:
Retype new password:
passwd: password updated successfully

```

```

root@SergiC(Thu Nov 21):~# passwd SergiC
New password:
Retype new password:
passwd: password updated successfully

```

Si volem que el usuari canvi la contrasenya al entrar fem: `chage -d 0 nomusuari` llistem els usuaris del sistema per comprovar que tot ha sortit correctament

```

root@SergiC(Thu Nov 21):~# cut -d: -f1 /etc/passwd

```

```

avahi
pulse
saned
lightdm
polkitd
rtkit
colord
user1
user2
P01
P02
P03
SM1
SM2
SergiC
root@SergiC(Tue Nov 26):~#

```

```

root@SergiC(Thu Nov 21):~# groups P01
P01 : P01 P0
root@SergiC(Thu Nov 21):~# groups P02
P02 : P02 P0
root@SergiC(Thu Nov 21):~# groups P03
P03 : P03 P0
root@SergiC(Thu Nov 21):~#

```

I donem els permisos necessaris:

700 restringim l'accés només al propietari del directori

770 el propietari i el grup tenen accés complet al directori

```

root@SergiC(Tue Nov 26):~# chmod 700 /home/P0s/P01
root@SergiC(Tue Nov 26):~# chmod 700 /home/P0s/P02
root@SergiC(Tue Nov 26):~# chmod 700 /home/P0s/P03

```

```

root@SergiC(Tue Nov 26):~# chmod 770 /home/SMs/SM1
root@SergiC(Tue Nov 26):~# chmod 770 /home/SMs/SM2
root@SergiC(Tue Nov 26):~# chmod 770 /home/ED/SergiC

```

I posem els propietaris pertinents amb la comanda `chown`

```

chown: cannot access /home/P01: No such file or directory
root@SergiC(Tue Nov 26):/home/ED# chown P01:P0 /home/P0s/P01
root@SergiC(Tue Nov 26):/home/ED# chown P02:P0 /home/P0s/P02
root@SergiC(Tue Nov 26):/home/ED# chown P03:P0 /home/P0s/P03
root@SergiC(Tue Nov 26):/home/ED# chown :P0 /home/SMs/SM1
root@SergiC(Tue Nov 26):/home/ED# chown :P0 /home/SMs/SM2

```

```

root@SergiC(Tue Nov 26):/home/ED# chown :PO /home/ED/SergiC
root@SergiC(Tue Nov 26):/home/ED# chown SM1:SM /home/SMs/SM1
root@SergiC(Tue Nov 26):/home/ED# chown SM2:SM /home/SMs/SM2
root@SergiC(Tue Nov 26):/home/ED# chown :SM /home/ED/SergiC
root@SergiC(Tue Nov 26):/home/ED# chown SergiC:ED /home/ED/SergiC
root@SergiC(Tue Nov 26):/home/ED#

```

I comprovem que tot hagi sortit correctament

```

root@SergiC(Thu Nov 21):/home# ls
ED POs SMs aso lost+found
root@SergiC(Thu Nov 21):/home# cd POs
root@SergiC(Thu Nov 21):/home/POs# ls
PO1 PO2 PO3
root@SergiC(Thu Nov 21):/home/POs# cd ..

```

```

root@SergiC(Thu Nov 21):/home# cd SMs
root@SergiC(Thu Nov 21):/home/SMs# ls
SM1 SM2
root@SergiC(Thu Nov 21):/home/SMs# cd ..
root@SergiC(Thu Nov 21):/home# cd ED
root@SergiC(Thu Nov 21):/home/ED# ls
SergiC
root@SergiC(Thu Nov 21):/home/ED#

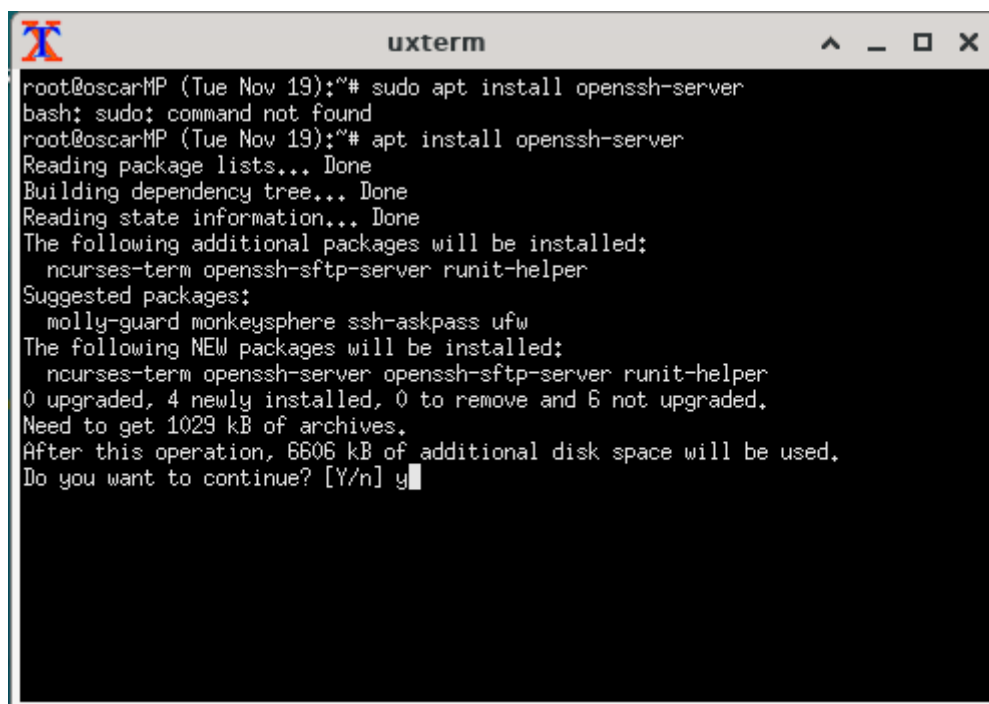
```

5. Connexió remota d'usuaris

Els usuaris de la nostra màquina han de tenir l'opció de poder connectar-se en remot de una forma segura.

instal·leu el paquet *openssh-server* i *openssh-client* (si cal)

Amb la comanda *sudo apt install openssh-server* instal·lem el paquet per poder exercir de servidor, i amb *sudo apt install openssh-client*, el paquet per exercir de client



```

root@oscarMP (Tue Nov 19):~# sudo apt install openssh-server
bash: sudo: command not found
root@oscarMP (Tue Nov 19):~# apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server runit-helper
Suggested packages:
  molly-guard monkeysphere ssh-askpass ufw
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server runit-helper
0 upgraded, 4 newly installed, 0 to remove and 6 not upgraded.
Need to get 1029 kB of archives.
After this operation, 6606 kB of additional disk space will be used.
Do you want to continue? [Y/n] y

```

```
uxterm
root@oscarMP (Tue Nov 19):~# apt install openssh-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-client is already the newest version (1:9.2p1-2+deb12u3).
openssh-client set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
root@oscarMP (Tue Nov 19):~#
```

Ara fem us de la comanda **sudo systemctl enable ssh**, per activar la opció d'ssh sempre que la maquina estigui activa. Després **sudo systemctl start ssh**, i per acabar, **sudo systemctl status ssh**, per comprovar que funciona correctament.

```
root (Wed Nov 27) > systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Wed 2024-11-27 09:36:27 UTC; 39s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 1915 (sshd)
     Tasks: 1 (limit: 2294)
    Memory: 1.4M
       CPU: 39ms
    CGroup: /system.slice/ssh.service
            └─1915 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Nov 27 09:36:27 aso-client systemd[1]: Starting ssh.service - OpenBSD Secure Sh
Nov 27 09:36:27 aso-client sshd[1915]: Server listening on 0.0.0.0 port 22.
Nov 27 09:36:27 aso-client sshd[1915]: Server listening on :: port 22.
Nov 27 09:36:27 aso-client systemd[1]: Started ssh.service - OpenBSD Secure She
```

Comproveu que us podeu connectar remotament a un altra màquina.

Per comprovar que funciona fem la següent comanda: **ssh usuari_local@ip_local**.

```
root@oscarMP (Tue Nov 19):~# ssh oscarmpu@10.192.238.200
The authenticity of host '10.192.238.200 (10.192.238.200)' can't be established.
ED25519 key fingerprint is SHA256:LRHVJeqwzE3JacI2G+CJUc2EfQ4fdWc5R83mxxP0XwI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.192.238.200' (ED25519) to the list of known hosts
+
oscarmpu@10.192.238.200's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-48-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 35 actualizaciones de forma inmediata.
15 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable
```

En cas que ens deixi accedir remotament, significarà que funciona correctament com a client.

Ara per poder connectar amb ssh a la maquina virtual, hem d'apagar la maquina, i anar a la configuració de la MV. Un cop allà, anem a l'apartat Red, i

cliquem a la opció "reenvío de puertos". Afegim una nova regla, i la posem de la següent manera:

Reglas de reenvío de puertos					
Nombre	Protocolo	IP anfitrión	Puerto anfitrión	IP invitado	Puerto invitado
ssh	TCP		3022		22

Comprovem el correcte funcionament desde el PC local: (Abans de fer la comanda ens hem d'assegurar que ssh es trobi instal·lat en el nostre ordinador local)

```
oscarmarpu@oscarmarpu-VLT-WX0:~$ ssh aso@localhost -p 3022
The authenticity of host '[localhost]:3022 ([127.0.0.1]:3022)' can't be established.
ED25519 key fingerprint is SHA256:Nk7KLlbmdfXX1EpcKXs+Pit6qyZvfbCGDAMJTt3bIiw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:3022' (ED25519) to the list of known hosts.
aso@localhost's password:
Linux aso-client 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

Prova des d'un altre ordinador:


```

oscar-marquez@oscar-marquez:~$ ssh -p 3022 aso@192.168.1.134
The authenticity of host '[192.168.1.134]:3022 ([192.168.1.134]:3022)' can't be
established.
ED25519 key fingerprint is SHA256:51x9vm+Yk4diAwgtjaD7JvE8Kf74nPABJhX8aF6ntzg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.1.134]:3022' (ED25519) to the list of known
hosts.
aso@192.168.1.134's password:
Linux aso-client 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08
-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Nov  2 08:31:52 2024

```

6. Eliminació i des-activació d'usuaris

Per donar de baixa un usuari és necessari eliminar tots els seus fitxers, les bústies de correu, treballs d'impressió, treballs cron i at i totes les referències a l'usuari. Després d'això es poden esborrar les línies associades a l'usuari al fitxer de passwd i de grups. Com un usuari pot tenir fitxers fora del seu directori home es necessari buscar per tot l'arbre de directoris el fitxers que pertanyen l'usuari i esborrar-los.

Crea un usuari de prova (o escolleix un existent) i afegeix fitxers al seu home.

Creem l'usuari de prova:

```

root@Victor (Wed Nov 27) >:"#useradd -m -s /bin/bash prova
root@Victor (Wed Nov 27) >:"#passwd prova
New password:
Retype new password:
passwd: password updated successfully
root@Victor (Wed Nov 27) >:"#

```

I afegim fitxers qualsevols al seu home

```

root@Victor (Mon Nov 25) >:"#echo "Fitxer1" > /home/prova/fitxer1.txt
root@Victor (Mon Nov 25) >:"#echo "Fitxer2" > /home/prova/fitxer2.txt
root@Victor (Mon Nov 25) >:"#chown prova:prova /home/prova/fitxer1.txt
root@Victor (Mon Nov 25) >:"#chown prova:prova /home/prova/fitxer2.txt
root@Victor (Mon Nov 25) >:"#

```

És una bona practica de seguretat primer desactivar el compte del usuari abans de començar el procés de donar-lo de baixa.

Una manera de desactivar un compte, a banda d'invalidar el password,

consisteix en canviar el *shell* de l'usuari per un un programa senzill que només escriu a la pantalla un missatge i dona informació a l'usuari de les raons per les quals el seu compte d'usuari ha estat desactivat. Per això es pot crear un 'tail script'. Per exemple:

```
#!/usr/bin/tail -n 2
```

```
This account has been closed due to a security problem. Please contact the system administrator.
```

Aquest script es pot posar com shell de l'usuari usant la comanda `chsh` i es pot guardar en un directori separat, per exemple `/usr/local/lib/no-login`.

Utilitzeu la comanda `chsh` per posar un *tail script* per desactivar el compte de l'usuari creat .

Creem el script al directori `/usr/local/lib`:

```
root@Victor (Mon Nov 25) >~#nano /usr/local/lib/no-login.sh
root@Victor (Mon Nov 25) >~#
```

Y el modifiquem. Hem de posar un `sleep` per a que la terminal no es tanqui i l'usuari pugui llegir el missatge que hem configurat. El `sleep 10` farà que el terminal es mostri 10 segons i després es tanqui.

```
#!/bin/bash
echo "This account has been closed due to a security problem. Please contact the system administrator"
sleep 10
exit 0
```

I utilitzem la comanda `chsh` per desactivar el usuari prova

```
root@Victor (Mon Nov 25) >~#chmod +x /usr/local/lib/no-login.sh
root@Victor (Mon Nov 25) >~#chsh -s /usr/local/lib/no-login.sh prova
root@Victor (Mon Nov 25) >~#
```

Com es pot comprovar que el compte ha quedat desactivat?

Es pot comprovar de diferents formes, primer podem comprovar al fitxer `passwd` com s'ha posat al directori `no-login`.

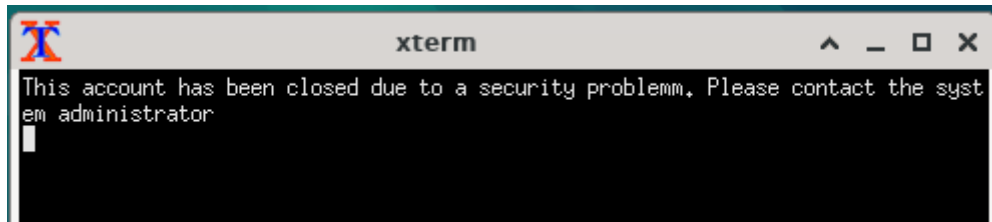
```
root@Victor (Mon Nov 25) >~#grep "prova" /etc/passwd
prova:x:1009:1013::/home/prova:/usr/local/lib/no-login.sh
root@Victor (Mon Nov 25) >~#
```

I a més, podem intentar iniciar sessió amb l'usuari prova:

```
root@Victor (Mon Nov 25) >~#su - prova
This account has been closed due to a security problem. Please contact the system administrator
root@Victor (Mon Nov 25) >~#
```

I podem veure com ens surt el missatge que hem configurat al script

També podem entrar directament amb l'usuari nou i veure la terminal:



Fes un backup amb tots els fitxers de l'usuari (tingueu en compte que potser una llista molt llarga de fitxers. Pista: feu servir xargs)

Utilitzem la comanda `find / -user prova` per trobar tots els fitxers de l'usuari prova, i la comanda `xargs tar -czvf /home/backup_prova.tar.gz` per comprimir tots aquests fitxers en un backup.

```
root@Victor (Fri Nov 22):~#find / -user prova | xargs tar -czvf /home/backup_prova.tar.gz
find: '/proc/1135/task/1135/fd/6': No such file or directory
find: '/proc/1135/task/1135/fdinfo/6': No such file or directory
find: '/proc/1135/fd/5': No such file or directory
find: '/proc/1135/fdinfo/5': No such file or directory
tar: Removing leading '/' from member names
/home/prova/
/home/prova/.face
tar: Removing leading '/' from hard link targets
/home/prova/.bash_history
/home/prova/.bash_logout
/home/prova/fitxer1.txt
/home/prova/.face.icon
/home/prova/fitxer2.txt
/home/prova/.profile
/home/prova/.bashrc
/home/prova/.face
/home/prova/.bash_history
/home/prova/.bash_logout
/home/prova/fitxer1.txt
/home/prova/.face.icon
/home/prova/fitxer2.txt
/home/prova/.profile
/home/prova/.bashrc
root@Victor (Fri Nov 22):~#
```

Els errors que ens surten del directori proc són perquè aquest directori té arxius dinàmics que poden canviar amb el temps, encara això aquest error no afecta a la comanda i es poden ometre.

Comprovem que al backup estiguin tots els fitxers

```

root@Victor (Fri Nov 22):/home#ls
ED  P0s  SMs  backup_prova.tar.gz  homeA  homeB  prova  user1  user2
root@Victor (Fri Nov 22):/home#tar -tf backup_prova.tar.gz
home/prova/
home/prova/.face
home/prova/.bash_history
home/prova/.bash_logout
home/prova/fitxer1.txt
home/prova/.face.icon
home/prova/fitxer2.txt
home/prova/.profile
home/prova/.bashrc
home/prova/.face
home/prova/.bash_history
home/prova/.bash_logout
home/prova/fitxer1.txt
home/prova/.face.icon
home/prova/fitxer2.txt
home/prova/.profile
home/prova/.bashrc
root@Victor (Fri Nov 22):/home#

```

Quin problema hi ha amb els fitxers que tinguin espais al seu nom? Com es pot resoldre això? (veure les opcions de la comanda xargs o la opció -exec de find)

Si hi han fitxers que tinguin espais al nom poden haver problemes al ser processats per la comanda xargs, ja que l'espai es interpretat com un separador d'arguments i pot partir el fixter en dos, per exemple el el fixter "Fitxer 1.txt" la comanda xargs només llegirà fins Fitxer, i la resta ho llegirà com un altre document.

Per solucionar-ho hem d'executar la comanda find amb el parametre "-print0", i la comanda xargs amb el parametre "-0".

```

root@Victor (Fri Nov 22):/home#find / -user prova -print0 | xargs -0 tar -czvf /home/backup_prova.tar.gz
find: '/proc/1165/task/1165/fd/6': No such file or directory
find: '/proc/1165/task/1165/fdinfo/6': No such file or directory
find: '/proc/1165/fd/5': No such file or directory
find: '/proc/1165/fdinfo/5': No such file or directory
tar: Removing leading '/' from member names
/home/prova/
/home/prova/.face
tar: Removing leading '/' from hard link targets
/home/prova/.bash_history
/home/prova/.bash_logout
/home/prova/fitxer1.txt
/home/prova/.face.icon
/home/prova/fitxer2.txt
/home/prova/.profile
/home/prova/.bashrc
/home/prova/.face
/home/prova/.bash_history
/home/prova/.bash_logout
/home/prova/fitxer1.txt
/home/prova/.face.icon
/home/prova/fitxer2.txt
/home/prova/.profile
/home/prova/.bashrc
root@Victor (Fri Nov 22):/home#

```

Busca tots els fitxers de l'usuari i esborrar-los.

Utilitzem la comanda `find / -user prova` per trobar tots els fitxers de l'usuari prova i per a cada fitxer fem `-exec rm -rf '{}' +` per eliminar els arxius

```
find: missing argument to -exec
root@Victor (Fri Nov 22):/home#find / -user prova -exec rm -rf '{}' +
find: '/proc/1171/task/1171/fd/6': No such file or directory
find: '/proc/1171/task/1171/fdinfo/6': No such file or directory
find: '/proc/1171/fd/5': No such file or directory
find: '/proc/1171/fdinfo/5': No such file or directory
```

I comprovem que no estiguin els fitxers.

```
root@Victor (Fri Nov 22):/home#find / -user prova
find: '/proc/1173/task/1173/fd/6': No such file or directory
find: '/proc/1173/task/1173/fdinfo/6': No such file or directory
find: '/proc/1173/fd/5': No such file or directory
find: '/proc/1173/fdinfo/5': No such file or directory
root@Victor (Fri Nov 22):/home#
```

Ara crea un script que donat el nom d'usuari, faci un backup del seu directori home, esborri tots els fitxers que l'usuari tingui al sistema i canviï el shell per un *tail script* que avisi a l'usuari que el seu compte ha estat esborrat.

C/C++

```
#!/bin/bash

# Comprovar que s'ha proporcionat un usuari
if [ -z "$1" ]; then
    echo "Ús: $0 nom_usuari"
    exit 1
fi

# Variables
USUARI=$1
BACKUP_DIR="/root/backups"
BACKUP_FILE="${BACKUP_DIR}/${USUARI}_home_backup.tar.gz"
TAIL_SCRIPT="/usr/local/lib/no-login.sh"

# 1. Comprovar si l'usuari existeix
if ! id "$USUARI" &>/dev/null; then
    echo "Error: L'usuari '$USUARI' no existeix."
    exit 2
fi
```

```

# 2. Crear el directori de backups si no existeix
if [ ! -d "$BACKUP_DIR" ]; then
    mkdir -p "$BACKUP_DIR"
    echo "Directori de backups creat a $BACKUP_DIR."
fi

# 3. Fer un backup del directori home de l'usuari
echo "Fent backup del directori home de l'usuari..."
tar -czvf "$BACKUP_FILE" "/home/$USUARI" 2>/dev/null
if [ $? -eq 0 ]; then
    echo "Backup completat: $BACKUP_FILE"
else
    echo "Error en fer el backup del directori home."
    exit 3
fi

# 4. Eliminar tots els fitxers de l'usuari al sistema
echo "Eliminant tots els fitxers de l'usuari..."
find / -user "$USUARI" -exec rm -rf '{}' + 2>/dev/null
if [ $? -eq 0 ]; then
    echo "Tots els fitxers de l'usuari han estat eliminats."
fi

# 5. Crear un script de no-login
echo "Creant el tail script per desactivar l'usuari..."
cat <<EOT > "$TAIL_SCRIPT"
#!/usr/bin/tail -n 2

Aquest compte ha estat tancat per l'administrador del sistema.
Si us plau, contacteu amb l'administrador.
EOT

# Fer executable el script
chmod +x "$TAIL_SCRIPT"
if [ $? -eq 0 ]; then
    echo "Tail script creat a $TAIL_SCRIPT."
else
    echo "Error en crear el tail script."

```

```

        exit 5
    fi

    # 6. Canviar el shell de l'usuari pel tail script
    echo "Canviant el shell de l'usuari..."
    chsh -s "$TAIL_SCRIPT" "$USUARI"
    if [ $? -eq 0 ]; then
        echo "Shell canviat correctament per a l'usuari '$USUARI'."
    else
        echo "Error en canviar el shell de l'usuari."
        exit 6
    fi

    # 7. Finalització
    echo "Procés completat. L'usuari '$USUARI' ha estat desactivat i el seu backup
    es troba a $BACKUP_FILE."

    exit 0

```

Comprova que s'ha fet correctament

Primer creem una altra vegada l'usuari prova amb els passos anteriors, i executem el script.

```

root@Victor (Fri Nov 22):~/Downloads# ./gestio_usuaris.sh prova
Fent backup del directori home de l'usuari...
/home/prova/
/home/prova/.face
/home/prova/.bash_logout
/home/prova/.fitxer1.txt
/home/prova/.face.icon
/home/prova/.fitxer2.txt
/home/prova/.profile
/home/prova/.bashrc
Backup completat: /root/backups/prova_home_backup.tar.gz
Eliminant tots els fitxers de l'usuari...
Creant el tail script per desactivar l'usuari...
Tail script creat a /usr/local/lib/no-login.sh.
Canviant el shell de l'usuari...
Shell canviat correctament per a l'usuari 'prova'.
Procés completat. L'usuari 'prova' ha estat desactivat i el seu backup es troba
a /root/backups/prova_home_backup.tar.gz.
root@Victor (Fri Nov 22):~/Downloads#

```

Comprovem:

1. Els fitxers estan borrats

```

root@Victor (Fri Nov 22):~/Downloads#find / -user prova
find: '/proc/2542/task/2542/fd/6': No such file or directory
find: '/proc/2542/task/2542/fdinfo/6': No such file or directory
find: '/proc/2542/fd/5': No such file or directory
find: '/proc/2542/fdinfo/5': No such file or directory
root@Victor (Fri Nov 22):~/Downloads#

```

2. El backup conté tots els fitxers

```

root@Victor (Fri Nov 22):~/Downloads#tar -tf /root/backups/prova_home_backup.tar.gz
home/prova/
home/prova/.face
home/prova/.bash_logout
home/prova/fitxer1.txt
home/prova/.face.icon
home/prova/fitxer2.txt
home/prova/.profile
home/prova/.bashrc
root@Victor (Fri Nov 22):~/Downloads#

```

3. L'usuari prova no pot iniciar sessió:

```

root@Victor (Fri Nov 22):~#su - prova
This account has been closed due to a security problem,
Please contact the system administrator
root@Victor (Fri Nov 22):~#

```

7. Usuari especial asosh

A Unix hi ha comandes com el shutdown per apagar la màquina que només pot executar l'usuari root. En moltes ocasions pot ser interessant que algun altre usuari pugui apagar també la màquina però sense que tingui accés als privilegis de root.

Per aconseguir-ho es demana que creeu un compte especial que serveixi per executar un shell simplificat que permetrà fer shutdown i altres tasques especials amb permisos de superusuari. L'username corresponent serà asosh, i el password que decidiu. Quan algú faci un login en aquest compte s'executarà l'script asosh que hauríeu de tenir instal·lat de la pràctica anterior d'aplicacions. Per raons de seguretat cal que us assegureu que quan s'entra amb aquest compte no s'executa cap shell script. Quins permisos posaríeu a aquesta aplicació perquè no pugui ser executat per cap usuari directament?

useradd -m asosh: Crear l'usuari asosh amb un directori /home propi.

passwd asosh: Assignar una contrasenya a l'usuari asosh.

nano /home/asosh/asosh.sh: Crear un script (asosh.sh) per executar com a shell de l'usuari asosh.

Unset

```
#!/bin/bash

# Mostrar un menú simple al usuario
echo "1. reboot"
echo "2. shutdown"
echo "e. exit"
read -p "Insereix un nombre: " command

# Evaluar la opción ingresada
if [ "$command" -eq 1 ]; then
    echo "Reiniciant el sistema..."
    # Ejecutar el reinicio con permisos adecuados
    exec sudo /usr/sbin/shutdown -r now
elif [ "$command" -eq 2 ]; then
    echo "Apagant el sistema..."
    # Ejecutar el apagado con permisos adecuados
    exec sudo /usr/sbin/shutdown now
elif [ "$command" == "e" ]; then
    echo "Sortint de l'usuari ASOSH..."
    exit 0
else
    echo "Nombre no valid"
    exit 1
fi
```

chown asosh:asosh /home/asosh/asosh.sh: Assignar la propietat del script asosh.sh a l'usuari asosh.ch

chmod u+s /home/asosh/asosh.sh: Establir el bit SetUID perquè el script s'executi amb permisos del propietari (no és necessari en aquest cas, pots ometre-ho).

chmod 700 /home/asosh/asosh.sh: Donar permisos per llegir, escriure i executar només a l'usuari asosh.

visudo (en cas que no es trobi instal·lat fem **apt install sudo**): Afegir la línia asosh

ALL=(ALL) NOPASSWD: /usr/sbin/shutdown per permetre a asosh executar el comando shutdown sense contrasenya.

```
GNU nano 7.2 /etc/sudoers.tmp

# Host alias specification

# User alias specification

# Cmnd alias specification

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

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

asosh ALL=(ALL) NOPASSWD: /usr/sbin/shutdown
# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
```

nano /etc/passwd: Modificar la línia de l'usuari asosh per utilitzar el script asosh.sh com a shell:

asosh:x:1001:1001::/home/asosh:/home/asosh/asosh.sh

```
asosh:x:1001:1001::/home/asosh:/home/asosh/asosh.sh
```

Finalment executem **su - asosh** per entrar a l'usuari i comprovem que entra correctament a l'usuari

```
root@oscarMP (Wed Nov 27):~# su - asosh
1. reboot
2. shutdown
e. exit
Insereix un nombre: █
```

Com queda finalment l'entrada de la base de dades d'usuaris per a l'usuari **asosh**?

Executem nano /etc/passwd i veiem l'usuari asosh d'aquesta manera:

```
asosh:x:1001:1001::/home/asosh:/home/asosh/asosh.sh
```

8. Sudo i control d'execució d'aplicacions

Com el shutdown hi ha altres comandes d'administració que només poden ser executades per el superusuari. És una mala pràctica de seguretat utilitzar el compte del superusuari per executar aquestes comandes. Per resoldre això es pot utilitzar la comanda **sudo**. Sudo permet executar una comanda a un usuari autoritzat com superusuari o un altre usuari. L'especificació de quines aplicacions pot executar un determinat usuari es defineix al fitxer /etc/sudoers.

Aquest fitxer es pot editar de forma segura fent servir la comanda visudo.

Feu els canvis necessaris perquè els membres del grup admin puguin executar qualsevol comanda amb privilegis de superusuari.

Primer instal·lem sudo fent:

```
apt update
```

```
apt install sudo
```

Obrir /etc/sudoers usant:

```
visudo /etc/sudoers
```

I afegim:

```
%admin ALL=(ALL:ALL) ALL
```

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

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

asnsdh  ALL=(ALL:ALL) NOPASSWD: /usr/sbin/shutdown

%admin  ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "@include" directives:

@include /etc/sudoers.d
```

Feu els canvis necessaris perquè els usuaris PO puguin executar l'script per esborrar els usuaris que heu creat abans i tots els binaris que siguin al directori /usr/local/PO/bin.

Creem la carpeta /usr/local/PO/bin fent:

```
mkdir -p /usr/local/PO/bin
```

```
root@IvanP (mié nov 27) aso-client:/# mkdir -p /usr/local/PO/bin
```

Per a que el grup PO sigui propietari de la carpeta fem:

```
chown root:PO /usr/local/PO/bin
```

```
root@IvanP (mié nov 27) aso-client:/usr/local/PO/bin# chown root:PO /usr/local/PO/bin/gestio_usuaris.sh
```

I donem permisos per executar binaris amb la comanda:

```
chmod 750 /usr/local/PO/bin/gestio_usuaris.sh
```

```
root@IvanP (mié nov 27) aso-client:/usr/local/PO/bin# chmod 750 /usr/local/PO/bin/gestio_usuaris.sh
```

Copiem l'script a la carpeta /usr/local/PO/bin amb la comanda:

cp <ruta al directori on hem guardat l'script> /usr/local/PO/bin

```
root@IvanP (mié nov 27) aso-client:/# cp /root/Documentos/Scripts/gestio_usuaris.sh /usr/local/PO/bin
```

Obrim /etc/sudoers usant:

visudo /etc/sudoers

I afegim:

%PO ALL=(ALL) NOPASSWD: /usr/local/PO/bin/gestio_usuaris.sh

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

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

asosh    ALL=(ALL:ALL) NOPASSWD: /usr/sbin/shutdown

%admin   ALL=(ALL:ALL) ALL

%PO      ALL=(ALL) NOPASSWD: /usr/local/PO/bin/gestio_usuaris.sh
# See sudoers(5) for more information on "@include" directives:

@include /etc/sudoers.d
```

Comproveu que això funciona executant la comanda **vipw**.

Executem vipw i comprovem que l'usuari està actiu:

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
admin:x:0:0:root:/root:/bin/bash
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
aso:x:1000:1000,,:/home/aso:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
avahi:x:105:112:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
pulse:x:106:113:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin
saned:x:107:116::/var/lib/saned:/usr/sbin/nologin
lightdm:x:108:117:Light Display Manager:/var/lib/lightdm:/bin/false
polkitd:x:998:998:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:109:118:RealtimeKit,,:/proc:/usr/sbin/nologin
colord:x:110:119:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
vboxadd:x:997:1::/var/run/vboxadd:/bin/false
user1:x:1001:1001:Fernando Alonso,14,633333333,614141414,El lechero asturiano:/home/user1:/bin/bash
user2:x:1002:1002:Ilia Topuria,16,616161616,616161616,El matador:/home/user2:/bin/bash
PO1:x:1003:1007::/home/POs/PO1:/bin/sh
PO2:x:1004:1008::/home/POs/PO2:/bin/sh
PO3:x:1005:1009::/home/POs/PO3:/bin/sh
SM1:x:1006:1010::/home/SMs/SM1:/bin/sh
SM2:x:1007:1011::/home/SMs/SM2:/bin/sh
IvanP:x:1008:1012::/home/ED/IvanP:/bin/sh
sshd:x:111:65534::/run/ssh:/usr/sbin/nologin
asosh:x:1009:1013::/home/asosh:/home/asosh/asosh.sh
prueba:x:1010:1014::/home/prueba:/bin/sh

```

Entrem a l'usuari PO1 i executem l'script:

```

root@IvanP (mié nov 27) aso-client:/usr/local/PO/bin# login
aso-client nombre: PO1
Contraseña:
Linux aso-client 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64
Si tens cap problema i vols contactar amb l'administrador,
pots contactar amb:
    ivan.pena.carreno@estudiantat.upc.edu
$ sudo /usr/local/PO/bin/gestio_usuaris.sh prueba
Directorio de backups creat a /root/backups.
Fent backup del directori home de l'usuari...
/home/prueba/
/home/prueba/.bashrc
/home/prueba/.face.icon
/home/prueba/.face
/home/prueba/.profile
/home/prueba/.bash_logout
Backup completat: /root/backups/prueba_home_backup.tar.gz
Eliminant tots els fitxers de l'usuari...
Creant el tail script per desactivar l'usuari...
Tail script creat a /usr/local/lib/no-login.sh.
Canviant el shell de l'usuari...
Shell canviat correctament per a l'usuari 'prueba'.
Procés completat. L'usuari 'prueba' ha estat desactivat i el seu backup es troba a /root/backups/prueba_home_backup.tar.gz.
$ █

```

I comprovem amb vipw el resultat:

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
admin:x:0:0:root:/root:/bin/bash
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
aso:x:1000:1000,,:/home/aso:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
avahi:x:105:112:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
pulse:x:106:113:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin
saned:x:107:116:/var/lib/saned:/usr/sbin/nologin
lightdm:x:108:117:Light Display Manager:/var/lib/lightdm:/bin/false
polkitd:x:998:998:polkit:/nonexistent:/usr/sbin/nologin
rtkit:x:109:118:RealtimeKit,,:/proc:/usr/sbin/nologin
colord:x:110:119:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
vboxadd:x:997:1:/var/run/vboxadd:/bin/false
user1:x:1001:1001:Fernando Alonso,14,633333333,614141414,El lechero asturiano:/home/user1:/bin/bash
user2:x:1002:1002:Ilia Topuria,16,616161616,616161616,El matador:/home/user2:/bin/bash
PO1:x:1003:1007:/home/POs/PO1:/bin/sh
PO2:x:1004:1008:/home/POs/PO2:/bin/sh
PO3:x:1005:1009:/home/POs/PO3:/bin/sh
SM1:x:1006:1010:/home/SMs/SM1:/bin/sh
SM2:x:1007:1011:/home/SMs/SM2:/bin/sh
IvanP:x:1008:1012:/home/ED/IvanP:/bin/sh
sshd:x:111:65534:/run/sshd:/usr/sbin/nologin
asosh:x:1009:1013:/home/asosh:/home/asosh/asosh.sh
prueba:x:1010:1014:/home/prueba:/usr/local/lib/no-login.sh

```

Quins canvis heu fet al fitxer /etc/sudoers per activar els controls anteriors?

```

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

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

asosh ALL=(ALL:ALL) NOPASSWD: /usr/sbin/shutdown

%admin ALL=(ALL:ALL) ALL

%PO ALL=(ALL:ALL) NOPASSWD: /usr/local/PO/bin/gestio_usuaris.sh
# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d

```

Hem afegit les línies asosh, %admin i %PO.

Finalment desactiveu el compte del root de tal forma no es pugui fer *login* com superusuari. Les comandes d'administració es podran fer només des dels comptes del grup admin o fent ús de l'usuari asosh. Assegureu-vos que podeu fer comandes des d'un usuari administrador abans de desactivar-ho.

Abans de fer res amb l'usuari root, hem de comprovar que els usuaris del grup admin puguin executar comandes amb sudo.

Per fer això primer hem d'activar aquests usuaris en cas que no els haguem activat abans amb la comanda `usermod -U user1`

I comprovem que funcioni el sudo.

```
user1@aso-client:~$ sudo mkdir prova
[sudo] password for user1:
user1@aso-client:~$ ls
Desktop  Downloads  Pictures  Templates  prova
Documents Music      Public    Videos
user1@aso-client:~$
```

Fem la següent comanda:

```
usermod -s /sbin/nologin root
```

```
root@IvanP (mié nov 27) aso-client:/usr/local/P0/bin# usermod -s /sbin/nologin root
```

Després desactivem ssh obrint `/etc/ssh/sshd_config` i descomentant la línia:

```
PermitRootLogin prohibit-password
```

```
#LoginGraceTime 2m
PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Un cop desats els canvis, reiniciem el servei ssh amb `sudo systemctl restart sshd`.

```
root@IvanP (mié nov 27) aso-client:/usr/local/P0/bin# systemctl restart sshd
```

Finalment verifiquem que podem entrar a root fent `su`.

```
$ su
Contraseña:
This account is currently not available.
$
```