Objectiu 4: Gestió d'usuaris

1 Objectius

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

2 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 é*s 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 el usuaris.

3 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.

3.1 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*).*

Abrimos el fichero etc/profile con nuestro editor de texto y al principio del fichero nos encontraremos con las siguientes líneas:

```
if [ "`id -u`" -eq 0 ]; then
  PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
else
  PATH="/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games"
fi
export PATH
```

En el if tenemos el PATH del usuario con ID 0, es decir, es el PATH del usuario root. En el else está definido el PATH para los demás usuarios.

Ahora vamos a añadir el $HOME/bin al path de todos los usuarios del sistema, para ello añadimos «PATH=$PATH:$HOME/bin» antes de exportar la variable PATH:

```
if [ "`id -u`" -eq 0 ]; then
  PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
else
  PATH="/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games"
fi

PATH=$PATH:$HOME/bin
```

Para aplicar los cambios tenemos dos opciones:

1.- Cerrar sesión.

2.- Ejecutar el fichero /etc/profile con el comando «source /etc/profile» si el único usuario conectado somos nosotros.

Por últimos vamos a comprobar que el PATH es correcto, para ello mostraremos la variable PATH de los usuarios «aso» y «root»

```
aso@aso-client:~$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/home/aso/bin
aso@aso-client:~$ su root
Password:
root@aso-client:/home/aso# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
root@aso-client:/home/aso#
```

3.2 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) >”)

Tenemos que ir a ~/.bashrc y comentar este fragmento del script:

```
# set a fancy prompt (non-color, unless we know we "want" color)
#case "$TERM" in
#xterm-color)
#    PS1='${debian_chroot:+($debian_chroot)}\[\033[01;32m\]\u@\h\[\033[00m\]:\[\033[01;34m\]\w\[\033[00m$
#    ;;
#*)
#    PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
#    ;;
#esac
```

de esta forma el PATH de todos los usuarios existentes estará definido en la variable PS1 del fichero /etc/bash.bashrc:

```
# set a fancy prompt (non-color, overwrite the one in /etc/profile)
PS1='${debian_chroot:+($debian_chroot)}\u (\d) > '
```

donde:

- \u → username del usuario actual.

- \d → muestra la fecha actual con el siguiente formato «Tue April 10»

Ahora el prompt de los usuarios que tenemos en el sistema es el siguiente:

```
aso (Fri Nov 24) >
```

Por último tenemos que comentar las siguientes líneas en «/etc/skel/.bashrc» ya que sinó los nuevos usuarios mantendrán el prompt antiguo:

```
#if [ "$color_prompt" = yes ]; then
#    PS1='${debian_chroot:+($debian_chroot)}\[\033[01;32m\]\u@\h\[\033[00m\]:\[\033[01;34m\]\w\[\033[00m$
#else
#    PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
#fi
```

3.3 Quina variable d'entorn té la definició del prompt?

En la variable PS1

```
aso (Fri Nov 24) > echo $PS1
${debian_chroot:+($debian_chroot)}\u (\d) >
```

4 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*.

4.1 Omple la següent taula:

paràmetres /Usuari	Usuari 1	Usuari 2
UID	1001	1002
Username	adso1	adso2
Directori home	/home/adso1	/home/adso2
Shell	/bin/bash	/bin/bash
Grups	adso (116)	adso (116)

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

Ejecutamos el comando vipw, la primera vez que lo hagamos nos preguntará que editor de textos queremos utilizar:

```
root (Sat Nov 18) >$ 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]: 1
```

Una vez seleccionado el editor de textos se abrirá el fichero etc/passwd, vamos al final del fichero y añadimos estas 2 líneas:

```
adso1:x:1001:116::/home/adso1:/bin/false
adso2:x:1002:116::/home/adso2:/bin/false
```

Cada línea representa un usuario y el caracter «:» se utiliza para separar los campos del usuario, los campos del /etc/passwd son los siguientes:

1.- Nombre de usuario

2.- Clave del usuario. En este campo pondremos siempre «x», la clave del usuario está en el fichero /etc/shadow y codificada.

3.- El UID del usuario.

4.- El GID del usuario.

5.- Una descripción del usuario.

6.- Ruta del directorio home.

7.- Ruta del shell del usuario.

Una vez añadidos los dos usuarios al fichero /etc/passwd guardamos los cambios y salimos del fichero. Por último tenemos que modificar el fichero /etc/shadow, para ello utilizaremos el comando «vipw -s»:

```
You have modified /etc/passwd.
You may need to modify /etc/shadow for consistency.
Please use the command 'vipw -s' to do so.
root (Sat Nov 18) >$
```

Al igual que con el fichero passwd cada usuario está representado en una línea:

```
adso1:*:116::::::
adso2:*:116::::::
```

Con esto ya tenemos los usuarios creados, falta asignar las claves de acceso a cada usuario, crear el grupo, directorios home y asignar los permisos adecuados. El grupos lo podemos crear con el comando vigr:

```
adso:x:116:
```

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

Si sólo utilizamos vipw nos aseguramos de que nadie más esté modificando los ficheros de «/etc/passwd» y «/etc/shadow», si editamos los ficheros directamente no.

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

4.4 Mostra quins grups heu creat i quins usuaris pertanyen a aquests grups

```
aso (lun nov 27) > cat /etc/group | grep "adso"
adso:x:116:
aso (lun nov 27) > cat /etc/passwd | grep "adso"
adso1:x:1001:116::/home/adso1:/bin/bash
adso2:x:1002:116::/home/adso2:/bin/bash
aso (lun nov 27) >
```

Per raons de seguretat és millor desactivar el compte de l'usuari fins que tot el procés d'alta no hagi finalitzat.

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

Buscamos la línia del usuario en el fichero /etc/passwd y en el último campo lo cambiamos por /bin/false o /bin/nologin

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

A definir los usuarios ya les hemos asignado la shell /bin/false

4.7 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 el fitxers que estiguin dintre del directori.

En este apartado vamos a utilizar los siguientes comandos:

cp -r dir_original dir_destino, el -r → Copiamos el directorio.

chown -R propietario ruta_directorio → Asigna el propietario a un directorio.

chgrp -R grupo ruta_directorio → Asigna el grupo a un directorio.

chmod permisos ruta_directorio → Asigna permisos a un directorio

```
root (Sat Nov 18) >$ cp -r /etc/skel/ /home/adso1
root (Sat Nov 18) >$ cp -r /etc/skel/ /home/adso2
root (Sat Nov 18) >$ chown -R adso1 /home/adso1
root (Sat Nov 18) >$ chown -R adso2 /home/adso2
root (Sat Nov 18) >$ chgrp -R adso /home/adso1
root (Sat Nov 18) >$ chgrp -R adso /home/adso2
root (Sat Nov 18) >$ chmod 700 /home/adso1
root (Sat Nov 18) >$ chmod 700 /home/adso2
root (Sat Nov 18) >$
```

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

Asignamos la clave de usuario con el comando passwd nombre_usuario

```
root (Sat Nov 18) >$ passwd adso1
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root (Sat Nov 18) >$ passwd adso2
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root (Sat Nov 18) >$
```

Ahora tenemos los usuarios adso1 y adso2 dados de alta.

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 el posa la clau xifrada i altres paràmetres associats a la vigència de la clau.

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

vipw -s

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

1.- Nombre del usuario.

2.- Clave.

3.- Número de días (desde 1 Enero de 1970) desde que el último cambio de clave.

4.- Minimo de días entre el cambio de claves.

5.- Cada cuantos días hay que cambiar la clave de usuario.

6.- Número de dias de antelación que tardará en avisar al usuario que debe cambiar de clave

7.- Los días que vamos a esperar para que el usuario cambie la clave antes de deshabilitar el usuario una vez superado el máximo de días entre el cambio de claves.

8.- Número de días desde el 1 de Enero que lleva esta cuenta deshabiitada.

9.- Campo reservado para un nuevo uso.

4.11 Amb quina comanda es poden modificar aquests paràmetres?

Per editar altres paràmetres del compte d'usuari es poden utilitzar les comandes: **chfn** i **chsh.**

4.12 Utilitzeu aquestes comandes per assignar valors adequats als comptes creats.

Utilizaremos chsh para cambiar la shell de «adso1» y «adso2»

Por último entramos con «adso1» y «adso2» para comprobar que todo ha salido bien:

```
adso1 (Sat Nov 18) >$ su adso2
Password:
adso2 (Sat Nov 18) >$
```

5 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.

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

En el «/home», en un principio puede parecer buena idea guardar los usuarios en carpetas separadas en el directorio home ya que nos puede ahorrar tiempo a la hora de asignar los permisos de los home de usuarios sm y ed, sin embargo vamos a tener que cambiar el home manualmente ya que el adduser deja los home por defecto en /home. Al final se ha dejado los home en el /home por comodidad y por convenio.

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 acces 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 l'altre .

• 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).

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

Creación de usuarios:

adduser po1

adduser po2

adduser po3

adduser sm1

adduser sm2

adduser noelc

Al crear cada uno de los usuarios con el comando «adduser» nos aparecerá esto en la terminal (solución de los warnings en el apartado 7):

```
root (Thu Nov 23) >$ adduser noelc
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
        LANGUAGE = (unset),
        LC_ALL = (unset),
        LANG = "es_ES.UTF-8"
    are supported and installed on your system.
perl: warning: Falling back to the standard locale ("C").
Adding user `noelc' ...
Adding new group `noelc' (1003) ...
Adding new user `noelc' (1005) with group `noelc' ...
Creating home directory `/home/noelc' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for noelc
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
root (Thu Nov 23) >$
```

Creación de grupos:

groupadd po

groupadd sm

groupadd ed

```
root (Thu Nov 23) >$ groupadd po
root (Thu Nov 23) >$ groupadd sm
root (Thu Nov 23) >$ groupadd ed
root (Thu Nov 23) >$
```

Asignación de grupos:

Asignamos el grupo po y sm a po1, po2 y po3.

```
aso (Fri Nov 24) > sudo usermod -g sm po1
aso (Fri Nov 24) > sudo usermod -g sm po2
aso (Fri Nov 24) > sudo usermod -g sm po3
```

```
aso (Fri Nov 24) > sudo usermod -G po po3
aso (Fri Nov 24) > sudo usermod -G po po2
aso (Fri Nov 24) > sudo usermod -G po po1
```

Podemos ver información sobre el usuario con el comando id <usuario>, de esta forma podemos ver en que grupos está <usuario>

```
aso (Fri Nov 24) > id po1
uid=1006(po1) gid=1010(sm) grupos=1010(sm),1009(po)
```

Asignamos el grupo sm a sm1 y sm2

```
root (Thu Nov 23) >$ usermod -G sm sm1
root (Thu Nov 23) >$ usermod -G sm sm2
```

Asignamos el grupo ed a noelc

```
root (Thu Nov 23) >$ usermod -G ed noelc
```

Asignación de grupos a los directorios:

po1, po2 y po3 los dejamos igual (grupo po1, po2 y po3).

Al home y al contenido de sm1 y sm2 le asignamos el grupo po

```
root (Thu Nov 23) >$ chgrp -R po /home/sm1
root (Thu Nov 23) >$ chgrp -R po /home/sm2
```

Al home y al contenido de noelc le asignamos el grupo sm

```
root (Fri Nov 24) >$ chgrp -R sm /home/noelc
```

Permisos sobre los directorios home:

Damos permisos 770, es decir, sólo el usuario y el grupo tienen acceso total a los home, los demás usuarios no tendrán ningún tipo de acceso:

```
root (Thu Nov 23) >$ chmod -R 770 /home/po2
root (Thu Nov 23) >$ chmod -R 770 /home/po3
root (Thu Nov 23) >$ chmod -R 770 /home/po1
root (Thu Nov 23) >$ chmod -R 770 /home/sm1
root (Thu Nov 23) >$ chmod -R 770 /home/sm2
root (Thu Nov 23) >$ chmod -R 770 /home/noelc
```

Por último vamos a probar que todo funciona correctamente:

Con el usuario po1 podemos acceder a todos los home a excepción de los home de otros po:

```
aso (Fri Nov 24) > su po1
Password:
po1 (Fri Nov 24) > cd /home/po1/
po1 (Fri Nov 24) > cd /home/po2/
bash: cd: /home/po2/: Permission denied
po1 (Fri Nov 24) > cd /home/po3/
bash: cd: /home/po3/: Permission denied
po1 (Fri Nov 24) > cd /home/sm1
po1 (Fri Nov 24) > cd /home/sm2
po1 (Fri Nov 24) > cd /home/noelc
po1 (Fri Nov 24) >
```

Con el usuario sm1 sólo podemos acceder a los usuarios ed (noelc)

```
aso (Fri Nov 24) > su sm1
Password:
sm1 (Fri Nov 24) > cd /home/sm2
bash: cd: /home/sm2: Permission denied
sm1 (Fri Nov 24) > cd /home/sm1
sm1 (Fri Nov 24) > cd /home/po1
bash: cd: /home/po1: Permission denied
sm1 (Fri Nov 24) > cd /home/po2
bash: cd: /home/po2: Permission denied
sm1 (Fri Nov 24) > cd /home/po3
bash: cd: /home/po3: Permission denied
sm1 (Fri Nov 24) > cd /home/noelc
sm1 (Fri Nov 24) >
```

Con el usuario noelc (grupo ed) sólo podemos acceder a nuestro home

```
noelc (Fri Nov 24) > cd /home/po1
bash: cd: /home/po1: Permission denied
noelc (Fri Nov 24) > cd /home/po2
bash: cd: /home/po2: Permission denied
noelc (Fri Nov 24) > cd /home/po3
bash: cd: /home/po3: Permission denied
noelc (Fri Nov 24) > cd /home/sm1
bash: cd: /home/sm1: Permission denied
noelc (Fri Nov 24) > cd /home/sm2
bash: cd: /home/sm2: Permission denied
noelc (Fri Nov 24) > cd /home/noelc/
noelc (Fri Nov 24) >
```

6 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.

6.1 Instal·leu el paquet openssh-server i openssh-client (si cal)

```
root@aso-client:~# apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server
Suggested packages:
  molly-guard monkeysphere rssh ssh-askpass ufw
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server
0 upgraded, 3 newly installed, 0 to remove and 2 not upgraded.
Need to get 888 kB of archives.
After this operation, 5310 kB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

6.2 Comproveu que us podeu connectar remotament a un altra màquina.

Si hacemos la redirección de puertos en la configuración de virtualbox podemos conectarnos remotamente a nuestra máquina virtual vía SSH.

«ssh -p 3022 aso@localhost»

```
noel@noel-Inspiron-7720:~$ ssh -p 3022 aso@localhost
aso@localhost's password:
Linux aso-client 3.2.0-4-686-pae #1 SMP Debian 3.2.57-3 i686

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 18 11:01:56 2017 from 10.0.2.2
aso@aso-client:~$
```

Si no se puede ejecutar el comando ssh necesitaremos instalar el paquete «openssh-client», en ubuntu este paquete viene instalado por defecto.

7 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.

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

Al crear usuarios nuevos en el apartado 5 salen warnings de los locales, este error lo podemos solucionar descomentando la línia «es_ES.UTF-8» en el fichero «/etc/locale.gen», ejecutamos locale-gen «es_ES.UTF-8» y luego un dpkg-reconfigure seleccionando de nuevo «es_ES.UTF-8»

```
aso (Fri Nov 24) > sudo nano /etc/locale.gen
aso (Fri Nov 24) > sudo locale-gen "es_ES.UTF-8"
Generating locales (this might take a while)...
  es_ES.UTF-8... done
Generation complete.
aso (Fri Nov 24) >
```

```
[ ] es_DO ISO-8859-1
[ ] es_DO.UTF-8 UTF-8
[ ] es_EC ISO-8859-1
[ ] es_EC.UTF-8 UTF-8
```

```
aso (Fri Nov 24) > sudo adduser prueba
Añadiendo el usuario `prueba' ...
Añadiendo el nuevo grupo `prueba' (1001) ...
Añadiendo el nuevo usuario `prueba' (1004) con grupo `prueba' ...
Creando el directorio personal `/home/prueba' ...
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 prueba
Introduzca el nuevo valor, o pulse INTRO para usar el valor predeterminado
        Nombre completo []:
        Número de habitación []:
        Teléfono del trabajo []:
        Teléfono de casa []:
        Otro []:
¿Es correcta la información? [S/n] S
aso (Fri Nov 24) >
```

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 dóna 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.*

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

```
root (Sat Nov 18) >$ chsh prueba
Changing the login shell for prueba
Enter the new value, or press ENTER for the default
        Login Shell [/bin/bash]: /usr/local/lib/no-login
root (Sat Nov 18) >$
```

7.3 Com es pot comprovar que el compte ha quedat desactivat?

Intentamos acceder con el usuario «prueba», pero antes vamos a darle al fichero no-login permisos 755, de esta forma el propietario puede tiene acceso total al fichero y los miembros del grupo del fichero y otros usuarios podrán leer y ejecutar el fichero.

```
root (Sat Nov 18) >$ chmod 755 /usr/local/lib/no-login
root (Sat Nov 18) >$ su prueba

This account has been closed due to a security problem. Please contact the system administrator.
root (Sat Nov 18) >$
```

7.4 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)

```
tar -zcvf . /home/prueba
```

7.5 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)

Al hacer un .tar.gz no tenemos ningún problema con los espacios.

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

```
find / -user prueba -exec rm -r «{}» \; 2> /dev/null
```

```
root (Sun Nov 19) >$ find / -user prueba -exec rm -r "{}" \; 2> /dev/null
root (Sun Nov 19) >$
```

7.7 Ara crea un script que donat el nom d'usuari, faci un backup del seu directori home, esborri tots el 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.

El código está en el fichero deluserbkp.sh

7.8 Comprova que s'ha fet correctament

- El login del usuario está deshabilitado:

```
root (Sun Nov 19) >$ cat /etc/passwd | grep "prueba"
prueba:x:1004:1001:,,,:/home/prueba:/usr/local/lib/no-login
root (Sun Nov 19) >$ su prueba

This account has been closed due to a security problem. Please contact the system administrator.
root (Sun Nov 19) >$
```

- Hay un .tar.gz en el directorio de backups.

```
root (Sun Nov 19) >$ ls /root/backups/prueba_19-11-2017.tar.gz
/root/backups/prueba_19-11-2017.tar.gz
root (Sun Nov 19) >$
```

- El directorio home del usuario no existe.

```
root (Sun Nov 19) >$ ls /home/prueba
ls: cannot access '/home/prueba': No such file or directory
root (Sun Nov 19) >$
```

- No hay ficheros del usuario en el sistema.

8 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.

8.1 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?

La ruta de la shell es /usr/local/bin/asosh. Para que el script no pueda ser ejecutado por otro usuario le asignaremos como propietario a «asosh» y le pondremos permisos 700 para que sólo el propietario tenga control total sobre el ejecutable:

```
root (Sat Nov 18) >$ chown asosh /usr/local/bin/asosh
root (Sat Nov 18) >$ chmod 700 /usr/local/bin/asosh
```

```
adso1 (Sat Nov 18) >$ /usr/local/bin/asosh
-bash: /usr/local/bin/asosh: Permission denied
adso1 (Sat Nov 18) >$
```

Evitaremos que se ejecuten otros script asignando «/usr/local/bin/asosh» como shell para el usuario «asosh» mediante el comando chsh:

```
root (Sat Nov 18) >$ chsh asosh
Changing the login shell for asosh
Enter the new value, or press ENTER for the default
        Login Shell [/usr/local/bin/asosh]:
root (Sat Nov 18) >$
```

Ahora al identificarse como asosh se ejecutará la shell «asosh», aún haciendo «control+C» el SO no nos dejará ejecutar comandos bash.

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

```
root (Sat Nov 18) >$ cat /etc/passwd | tail -1
asosh:x:1003:1000:,,,:/home/asosh:/usr/local/bin/asosh
root (Sat Nov 18) >$ cat /etc/shadow | tail -1
asosh:$6$pwIKOdWb$YcTxmEo85jzA5yINBQy8xoQXq6cG0ZHBKFIMztWbhleaTQc9PdvpFNEUmBmXCvHHr8pSK9.7mOH3p7KWp8MUS1:
17488:0:99999:7:::
root (Sat Nov 18) >$
```

9 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.**

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

Creamos el grupo «admin»

```
root (Sun Nov 19) >$ groupadd admin
```

Ejecutamos el comando visudo para modificar el fichero «/etc/sudoers» y añadimos el grupo admin.

```
root (Sun Nov 19) >$ visudo
```

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

9.2 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.

Creamos y movemos el script de borrar usuarios a la ruta «usr/local/PO/bin»

```
root (Fri Nov 24) >$ mkdir -p /usr/local/PO/bin
root (Fri Nov 24) >$ mv deluserbkp.sh /usr/local/PO/bin/deluserbkp.sh
```

Asignamos permisos 750 al directorio que hemos creado y al script, dejamos a root como propietario y asignamos el grupo «po»

```
root (Fri Nov 24) >$ chmod -R 750 /usr/local/PO
root (Fri Nov 24) >$ chgrp -R po /usr/local/PO
```

Añadimos el directorio «/usr/local/PO/bin» al path modificando la variable PATH del fichero «/etc/profile»

```
aso (vie nov 24) > deluserbkp.sh
-bash: deluserbkp.sh: no se encontró la orden
```

```
po1 (vie nov 24) > deluserbkp.sh
Usage: deluserbkp.sh <user>
```

9.3 Comproveu que això funciona executant la comanda vipw.

```
aso (Fri Nov 24) >$ sudo vipw
sudo: unable to resolve host aso-client: Connection timed out
You have modified /etc/passwd.
You may need to modify /etc/shadow for consistency.
Please use the command 'vipw -s' to do so.
aso (Fri Nov 24) >$
```

El error «unable to resolve host aso-client: Connection timed out» lo podemos solucionar añadiendo las siguientes líneas al «/etc/hosts»

```
127.0.0.1    localhost.localdomain localhost
127.0.1.1    aso-client
```

Si volvemos a ejecutar el comando «sudo vipw» veremos que el error no aparece:

```
aso (Fri Nov 24) >$ sudo vipw
vipw: /etc/passwd is unchanged
aso (Fri Nov 24) >$
```

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

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

9.5 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.

9.6 Com es pot desactivar l'accés de login per a l'usuari root?

Passwd -l root

```
aso (Fri Nov 24) >$ sudo passwd -l root
passwd: password expiry information changed.
aso (Fri Nov 24) >$ su root
Password:
su: Authentication failure
aso (Fri Nov 24) >$
```