Lab 4: User Management

1. **In which files are defined users, passwords, and group databases?**

Users: /etc/passwd (UID, GID, personal directory and shell

Passwords: /etc/shadow (crypted passwords)

Group: /etc/group (group, name group, GID and members group)

2. **How UID (user identifiers) can be mapped for new users?**

Per defecte els nous usuaris s'emmagatzema començant pel 1000 i incrementant per cada nou usuari, aquest comportament es configura al /etc/login.def on es defineix el rang dels UIDs dels usuaris normal.

Si volem un UID específic hem de fer: **useradd -u UID nom_usuari**

3. **Which commands can be used to change the owners and permissions of a file? And of all the files in a directory?**

Per canviar el propietari fem: **chown nou_propietari fitxer**

Per canviar el propietari i el grup fem: **chown nou_prop:nou_grup fitxer**

Per canviar els propietari (i grup) d'un directori fem: **chown -R nou_prop:nou_grup directori/**

Per canviar els permisos fem: chmod 755 fitxer o d'un directori sencer: **chmod -R 755 directori/**

Per canviar el grup: **chgrp nou_grup fitxer**

4. **Analyse the above command and explain here how it works**

El comandament **export PATH=$PATH:/usr/local/bin** afegeix el directori **/usr/local/bin** al final de la variable **PATH**, que és una llista de directoris on el sistema busca executables. La comanda **export** assegura que la variable modificada estigui disponible per al shell actual i els seus processos fills.

5. **What are the changes you applied to the PATH variable?**

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

6. **In which environment variable the prompt is defined?**

El prompt del sistema es defineix a la variable d'entorn **PS1**.

7. **What are the changes that you applied to the prompt variable?**

Hem configurat PS1 per mostrar: **export PS1="aso:\w - \$(date +'%d/%m %H:%M') \$ "**

- El nom de l'usuari (aso).
- El directori de treball actual (\w).
- La data en format dia/mes hora:minut ($(date +'%d/%m %H:%M')).
- El símbol del prompt (\$).

8. **What is the difference between using the vipw command and edit directly the database with a text editor like vi?**

vipw per editar de forma segura el /etc/passwd, bloqueja el fitxer /etc/passwd per evitar que altres procesos el modifiquin simultanàment
vi no bloqueja els altres procesos, llavors el poden modificar, si es modificar malament el sistema pot quedar en un estat inconsistent, impedint que els usuaris fagin login, amb vi no es valida la sintaxis.

9. **What groups you have created?**

Hem creat el grup **admin.**

10. **Which users are part of that groups?**

Hem posat a **xavi** i a **xavi2** dintre.

11. **How you can deactivate an user account, in such a way that the user can not make login?**

Tenim diverses opcions:

- sudo passwd -l usuari (activar de nou, sudo passwd -u usuari)
- sudo usermod -s /usr/sbin/nologin usuari (sudo usermod -s /bin/bash usuari)
- sudo usermod -L usuari (sudo usermod -U usuari)
- editar /etc/shadow i posar * davant de la contrasenya

12. **What commands and parameters you have used to change the owner of the home directory?**

sudo chown usuari1 /home/usuari1 -R

13. **What commands you have used to change the file permissions?**

sudo chmod 700 /home/usuari1

14. **What are the security risks associated by putting the password in the user database?**

El fitxer /etc/passw es pot llegir per qualsevol usuari del sistema, ja que necessita ser accessible per algunes aplicacions, a més si un hash es descodifica, un atacant podria obtenir accés a comptes protegits.

15. **Which command can be used to edit safely the shadow file?**

sudo vipw -s

16. **What is the meaning of the password parameters defined in the /etc/shadow file?**

Cada línia del fitxer /etc/shadow representa un usuari i els seus paràmetres de contrasenya.

Exemple d'una línia:

usuari1:6hashcomplex:19353:0:99999:7:::

Significat dels camps (separats per :):

- usuari1: Nom de l'usuari.
- 6hashcomplex: Hash de la contrasenya (exemple: $6 indica que s'ha utilitzat SHA-512 per generar el hash).
- 19353: Data de l'últim canvi de contrasenya (en dies des de l'1 de gener de 1970).
- 0: Dies mínims abans que l'usuari pugui canviar la contrasenya.
- 99999: Dies màxims que la contrasenya pot estar activa abans que caduqui.
- 7: Període d'avís abans de caducar la contrasenya.
- :::: Camps reservats per al bloqueig del compte i altres funcions.

17. What command can be used to modify those password parameters?

Canviar els dies mínims i màxims:

sudo chage -m 1 -M 90 usuari1

- **-m 1**: L'usuari ha d'esperar 1 dia abans de canviar la contrasenya.
- **-M 90**: La contrasenya caducarà després de 90 dies.

Configurar un avís de caducitat:

sudo chage -W 7 usuari1

- **-W 7**: Avisa l'usuari 7 dies abans que caduqui la contrasenya.

Mostrar els paràmetres actuals:

sudo chage -l usuari1

18. How can you configure the directory permissions to inherit to the created files within the directory automatically?

sudo chmod g+s /path/to/directory

umask 027

source ~/.bashrc

19. Which command(s) you can use to make the backup of all the files of a user?

Per fer un **backup** de tots els fitxers d'un usuari, pots utilitzar la comanda **find** combinada amb **tar** o **cp**.

Còpia amb tar (empaquetar els fitxers):

sudo find / -user usuari1 -print0 | sudo tar --null -cvzf backup_usuari1.tar.gz --files-from=-

- **find / -user usuari1**: Cerca tots els fitxers propietat de l'usuari usuari1.
- **-print0**: Gestiona fitxers amb espais al nom.
- **tar --null**: Empaqueta els fitxers gestionant espais al nom.

Còpia amb cp (copiar directament a un directori):

sudo find / -user usuari1 -exec cp --parents {} /backup/usuari1/ \;

- **--parents**: Manté l'estructura de directoris original.

20. What's wrong with the files that have spaces in their name? How you can resolve this? (Hint: see options of xargs command or the -exec option of find)

Els fitxers amb espais poden provocar errors perquè la majoria de comandes interpreten els espais com a separadors. Això pot causar:

- Divisió incorrecta dels noms de fitxer.
- Errors quan es passen arguments a altres comandes.

Solució:

- Utilitza **-print0** amb **find** i **--null** amb comandes com **xargs** o **tar**:

sudo find / -user usuari1 -print0 | xargs -0 tar -cvzf backup.tar.gz

- Alternativament, utilitza **-exec** amb **find**:

sudo find / -user usuari1 -exec cp --parents {} /backup/usuari1/ \;

21. Which command you can use for searching all files of a user and delete them?

Per cercar i eliminar tots els fitxers propietat d'un usuari:

Cercar i llistar fitxers:

sudo find / -user usuari1

Eliminar els fitxers trobats:

sudo find / -user usuari1 -exec rm -rf {} +

22. How can you check that the account has been deactivated?

Iniciant sessió del usuari desactivat.

23. What is the content of this script?

```
#!/bin/bash


# Verifica que s'ha especificat un nom d'usuari
if [ -z "$1" ]; then
  echo "Ús: $0 <nom_usuari>"
  exit 1
fi


USER=$1
BACKUP_DIR="/backup/$USER"
```

```
SHELL_SCRIPT="/usr/local/bin/failed-login.sh"

# Comprova si l'usuari existeix
if ! id "$USER" &>/dev/null; then
  echo "L'usuari $USER no existeix."
  exit 2
fi

# 1. Crear còpia de seguretat de tots els fitxers de l'usuari
echo "Creant còpia de seguretat per a l'usuari $USER..."
sudo mkdir -p "$BACKUP_DIR"
sudo find / -user "$USER" -print0 | sudo tar --null -cvzf
"$BACKUP_DIR/backup_$USER.tar.gz"  --files-from=-

# 2. Eliminar tots els fitxers de l'usuari
echo "Eliminant tots els fitxers de l'usuari $USER..."
sudo find / -user "$USER" -exec rm -rf {} +

# 3. Canviar la shell de l'usuari pel script de desactivació
echo "Desactivant el compte de l'usuari $USER..."
if ! grep -q "^$SHELL_SCRIPT$" /etc/shells; then
  echo "Afegint $SHELL_SCRIPT a /etc/shells..."
  echo "$SHELL_SCRIPT" | sudo tee -a /etc/shells
fi

sudo chsh -s "$SHELL_SCRIPT" "$USER"

echo "Operació completada. L'usuari $USER ha estat desactivat."
```

24. What are the required set of permissions for this application in order to avoid a direct execution by any user?

sudo chown root:asosh /usr/local/bin/asosh

sudo chmod 750 /usr/local/bin/asosh

25. What is the appropriate values for the entry in the user database for asosh?

L'entrada a **/etc/passwd** per a l'usuari **asosh** ha de tenir els següents valors:

asosh:x:1003:1003::/home/asosh:/usr/local/bin/asosh

- **Descripció dels camps:**
    1. **asosh**: Nom de l'usuari.
    2. **x**: Indica que la contrasenya es troba a **/etc/shadow**.
    3. **1003:1003**: UID i GID únics per a l'usuari **asosh**.
    4. **/home/asosh**: Directori personal de l'usuari.
    5. **/usr/local/bin/asosh**: Shell assignada, en aquest cas l'aplicació restringida **asosh**.

26. What changes are required in the /etc/sudoers file to enable the configuration described above?

Obrir el fitxer amb visudo:

sudo visudo

Permetre que els membres del grup admin executin totes les comandes com a superusuari:

Afegeix la següent línia:

%admin ALL=(ALL) ALL

- **%admin**: Fa referència al grup admin.
- **ALL=(ALL) ALL**: Permet als membres del grup executar qualsevol comanda com a qualsevol usuari, incloent root.

Permetre que els membres del grup teachers executin l'script i binaris específics: Afegeix les línies següents:

%teachers ALL=(ALL) NOPASSWD: /path/to/delete-users-script

%teachers ALL=(ALL) NOPASSWD: /usr/local/teachers/bin/

- **%teachers**: Fa referència al grup teachers.
- **NOPASSWD**: Permet executar aquestes comandes sense demanar la contrasenya de l'usuari.
- **/path/to/delete-users-script**: Substitueix-ho pel camí complet de l'script per eliminar usuaris.

- **/usr/local/teachers/bin/**: Permet executar tots els binaris dins d'aquest directori.

27. What are the steps required to disable the root account?

Desactivar el compte root implica fer que no es pugui iniciar sessió directament com a **root**, mantenint la possibilitat de realitzar tasques administratives a través de **sudo**.