Nilda BALDA ***SIO 1***	Bloc 1	TP 3 **UTILISATEURS ET DROITS** 2023 - 2024 Semestre 2

Compte-rendu

SOMMAIRE

Introduction :

- **Utilisateurs :** Utilisateurs réguliers, ce sont les utilisateurs standard qui ont un accès limité au système. Ils peuvent exécuter des programmes et accéder à leurs propres fichiers, mais ils ne peuvent pas effectuer des opérations système qui nécessitent des privilèges spéciaux.

- **Droits** : Les fichiers sous Linux ont des autorisations qui déterminent qui peut les lire, les écrire et les exécuter. Les répertoires ont également des autorisations, qui contrôlent qui peut accéder à leur contenu.Certains utilisateurs peuvent avoir accès à certaines commandes système, tandis que d'autres peuvent être restreints.

Q1 - Est-ce que les utilisateurs daemon et btssio existent ? Si oui, donnez leurs UID, GID et groupes respectifs ? Qu'est-ce qu'un UID, un GID ?

```
root@Debian-12-Bookworm:/home/administrateur# id daemon
uid=1(daemon) gid=1(daemon) groupes=1(daemon)
root@Debian-12-Bookworm:/home/administrateur# id btssio
uid=1001(btssio) gid=1001(btssio) groupes=1001(btssio),100(users)
```

Un **UID** est un identifiant utilisateur, un numéro attribué par Linux à chaque utilisateur du système. Ce numéro permet au système d'identifier l'utilisateur. Les UID sont stockés dans le fichier.

GID (identifiant groupe de l'utilisateur) Un utilisateur sous Linux possède également des groupes, identifiable via leurs **GID**. Les groupes sont stockés dans le fichier.

Q2 – Créez les groupes jedi et rebelles.

```
root@Debian-12-Bookworm:/home/administrateur# sudo addgroup jedi
Ajout du groupe « jedi » (GID 1002)...
Fait.
root@Debian-12-Bookworm:/home/administrateur# sudo addgroup rebelles
Ajout du groupe « rebelles » (GID 1003)...
Fait.
```

Q3 – Créez les comptes luke, vador et solo.

```
root@Debian-12-Bookworm:/home/administrateur# sudo adduser luke jedi
Ajout de l'utilisateur « luke » au groupe « jedi » ...
Fait.
root@Debian-12-Bookworm:/home/administrateur# sudo adduser luke rebelles
Ajout de l'utilisateur « luke » au groupe « rebelles » ...
Fait.
root@Debian-12-Bookworm:/home/administrateur# sudo adduser vador jedi
Ajout de l'utilisateur « vador » au groupe « jedi » ...
Fait.
root@Debian-12-Bookworm:/home/administrateur# sudo adduser solo rebelles
Ajout de l'utilisateur « solo » au groupe « rebelles » ...
Fait.
```

Q4 – mettez le mot « password » comme mot de passe à l'utilisateur luke.

```
root@Debian-12-Bookworm:/home/administrateur# sudo passwd luke
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
```

Q5 – Essayez de vous connecter sous l'identité luke. Vérifiez.
Q6 – Créez l'arborescence de fichiers suivante :

```
root@Debian-12-Bookworm:/home/luke# mkdir /home/etoilenoire
root@Debian-12-Bookworm:/home/luke# cd /home/etoilenoire/
```

```
root@Debian-12-Bookworm:/home/etoilenoire# echo "voici les plans" > plans
root@Debian-12-Bookworm:/home/etoilenoire# echo "c'est ouvert" > entree_secrets
root@Debian-12-Bookworm:/home/etoilenoire#
```

Q7 - On change les caractéristiques du répertoire etoilenoire : son propriétaire sera luke, son groupe jedi. Il sera accessible en rwx pour son propriétaire. Il sera accessible en lecture et parcours (accès au contenu du répertoire) au groupe mais pas aux autres.

Q8 - On change les caractéristiques des fichiers : ils seront accessibles en lecture seule pour le groupe et n'auront aucun droit pour les autres. On affilie le fichier plans au groupe jedi et le fichier entree_secrete au groupe rebelles.

```
root@Debian-12-Bookworm:/home/etoilenoire# ls -l
total 12
-rw-r--r-- 1 root root   13 12 mars  11:17 entree_secrets
drwxr-x--- 2 luke jedi 4096 12 mars  11:38 etoilenoire
-rw-r--r-- 1 root root   16 12 mars  11:16 plans
```

Q9 – On teste les accès :
Après avoir tester les accès, tout est accessible.

Q10 – Supprimez temporairement le droit d'exécution de la commande uptime.
Q11 – Affichez les caractéristiques de l'utilisateur luke et du groupe rebelles.

```
root@Debian-12-Bookworm:/home/solo# sudo chmod u-x /usr/bin/uptime
root@Debian-12-Bookworm:/home/solo# id luke
uid=1004(luke) gid=1004(luke) groupes=1004(luke),100(users),1002(jedi),1003(rebe
lles)
```

Q12 – Affichez les annuaires utilisés pour gérer les comptes et les mots de passe.

```
root@Debian-12-Bookworm:/home/solo# cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         files systemd
group:          files systemd
shadow:         files systemd
gshadow:        files systemd

hosts:          files mdns4_minimal [NOTFOUND=return] dns myhostname
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Q13 - On crée l'utilisateur lola. Quel est son groupe principal ?

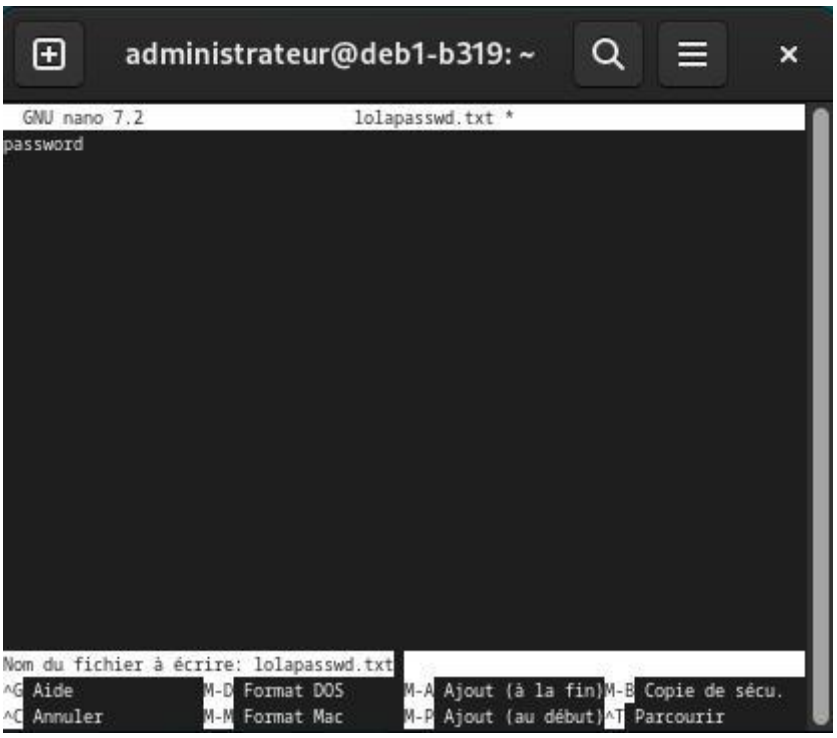
```
root@Debian-12-Bookworm:/home/solo# id lola
uid=1007(lola) gid=1007(lola) groupes=1007(lola),100(users)
```

Q14 – Gestion des groupes secondaires :

```
root@Debian-12-Bookworm:/home/solo# sudo usermod -aG rebelles lola
root@Debian-12-Bookworm:/home/solo# sudo usermod -aG jedi lola
root@Debian-12-Bookworm:/home/solo# sudo usermod -aG jedi,rebelles lola
root@Debian-12-Bookworm:/home/solo# sudo usermod -G "" lola
```

Q15 – Attribuer un mot de passe de manière scriptable à lola.

```
root@deb1-b319:/home/administrateur# touch lolapasswd.txt
root@deb1-b319:/home/administrateur# nano lolapasswd.txt
```



Q16 – Rechercher les fichiers de l'utilisateur lola.

```
/home/lola/.config/ibus/bus/70bf90ee49204e3582f7e8a25a153f7f-unix-wayland-0
/home/lola/.config/ibus/bus/70bf90ee49204e3582f7e8a25a153f7f-unix-0
/home/lola/.config/dconf
/home/lola/.config/dconf/user
/home/lola/.config/goa-1.0
/home/lola/.config/evolution
/home/lola/.config/evolution/sources
/home/lola/.config/evolution/sources/system-proxy.source
/home/lola/.config/gtk-3.0
/home/lola/.config/gtk-3.0/bookmarks
/home/lola/.config/xdg-terminals.list
/home/lola/.config/.gsd-keyboard.settings-ported
/home/lola/.config/user-dirs.locale
/home/lola/.config/GNOME-xdg-terminals.list
/home/lola/Images
/home/lola/.face
/home/lola/.bash_logout
/home/lola/Bureau
/home/lola/.vboxclient-seamless-tty2-control.pid
/home/lola/Modèles
/home/lola/.vboxclient-vmsvga-session-tty2-control.pid
```

Après avoir passé la commande : “find /home/lola”. Tous les fichiers qui se trouvent dans le l’utilisateur lola s’affiche.

Q17 – Supprimer les comptes et les fichiers des répertoires personnels de lola.

```
root@Debian-12-Bookworm:/home/lola# sudo rm -r /home/lola
root@Debian-12-Bookworm:/home/lola# find /home/lola
find: '/home/lola': Aucun fichier ou dossier de ce type
```

Une fois la commande de suppression passée, on peut voir qu'aucun fichier du répertoires personnels de lola s'affiche.

Q18 - On ajoute les droits spéciaux SGID et Sticky-bit au répertoire etoilenoire.

Q19 - pour vérifier l'impact des droits SGID et Sticky-bit, on crée des fichiers dans le répertoire etoilenoire.

Sous le compte root, on crée le fichier F1.

```
root@Debian-12-Bookworm:/home/administrateur# su root
root@Debian-12-Bookworm:/home/administrateur# mkdir F1
root@Debian-12-Bookworm:/home/administrateur# cd F1
```

Sous le compte luke, on crée le fichier F2.

```
root@Debian-12-Bookworm:/home/luke# mkdir F2
root@Debian-12-Bookworm:/home/luke# cd F2
root@Debian-12-Bookworm:/home/luke/F2#
```

Q20 – Vador va essayer de détruire le fichier de luke.

```
vador@debian:/home/nilda/F1/F2$ nano etoilenoire
vador@debian:/home/nilda/F1/F2$ rm etoilenoire/F1
rm: impossible de supprimer 'etoilenoire/F1': Aucun fichier ou dossier de ce typ
e
vador@debian:/home/nilda/F1/F2$ chmod -t etoilenoire
chmod: impossible d'accéder à 'etoilenoire': Aucun fichier ou dossier de ce type
vador@debian:/home/nilda/F1/F2$ nano etoilenoire
vador@debian:/home/nilda/F1/F2$ ls etoilenoire
ls: impossible d'accéder à 'etoilenoire': Aucun fichier ou dossier de ce type
```

Q21 – Qui peut formater la partition /dev/sda1 ?

Les utilisateurs qui peuvent formater la partition /dev/sda1, doivent avoir les droits appropriés. L'utilisateur root a un accès complet à tous les fichiers et

périphériques du système, y compris la partition /dev/sda1.

Q22 – L'administrateur copie les fichiers du répertoire etoilenoire dans /tmp en conservant leurs attributs.

```
root@debian:/home/nilda/F1/F2# cp -a etoilenoire/* /tmp
```

Q23 – L'administrateur donne le fichier entree_secrete à luke.

```
root@debian:/home/nilda/F1/F2# chown luke entree_secrete
```

Q24 – On visualise les droits des fichiers shadow et passwd.

```
root@debian:/home/nilda/F1/F2# ls -l /etc/shadow /etc/passwd
-rw-r--r-- 1 root root   2085 16 avril 14:14 /etc/passwd
-rw-r----- 1 root shadow 1166 16 avril 14:14 /etc/shadow
```

Conclusion :

En conclusion, la gestion des utilisateurs et des droits est une composante essentielle de la sécurité et de la gestion des systèmes Linux.

Utilisateurs et Groupes : Linux permet la création et la gestion de multiples utilisateurs et groupes. Chaque utilisateur est identifié par un nom d'utilisateur unique, et chaque utilisateur peut appartenir à un ou plusieurs groupes.

Droits d'accès : Chaque fichier et répertoire sur un système Linux possède des autorisations qui définissent qui peut lire, écrire et exécuter ces fichiers. Les autorisations sont généralement définies pour trois catégories d'utilisateurs : propriétaire, groupe et autres.