Mohamed
HAFAIDH

BTS SIO-1
TP3 - UTILISATION ET DROIT

1 - 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@yooceyy-GS60-6QC:~# getent passwd daemon
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

root@yooceyy-GS60-6QC:~# getent passwd btssio
btssio:x:1002:1003:,,,:/home/btssio:/bin/bash
```

Utilisateur daemon	Utilisateur btssio
UID: 1 GID: 1 Groupes: aucun	UID : 1001 1002 GID : 1001 1003 Groups btssio ,,, (empty)

```
L'utilisateur daemon existe.
L'utilisateur btssio existe également
```

```
UID (User Identifier): Un numéro unique qui identifie un
utilisateur sur un système Unix. Il est utilisé par le
système pour contrôler l'accès aux fichiers et aux
ressources.

GID (Group Identifier): Un numéro unique qui identifie un
groupe d'utilisateurs sur un système Unix. Il est utilisé par
le système pour contrôler les permissions des fichiers et des
répertoires.
```

2 – Créez les groupes jedi et rebelles.
3 – Créez les comptes luke, vador et solo.

```
root@yooceyy-GS60-6QC:~# usermod -g jedi luke
root@yooceyy-GS60-6QC:~# sudo usermod -aG rebelles luke
root@yooceyy-GS60-6QC:~# sudo usermod -g jedi vador
root@yooceyy-GS60-6QC:~# sudo usermod -aG rebelles solo
```

```
root@yooceyy-GS60-6QC:~# id luke
uid=1003(luke) gid=1004(jedi)
groupes=1004(jedi),1005(rebelles)
root@yooceyy-GS60-6QC:~# id vador
uid=1004(vador) gid=1004(jedi) groupes=1004(jedi)
root@yooceyy-GS60-6QC:~# id solo
uid=1005(solo) gid=1008(solo)
groupes=1008(solo),1005(rebelles)
```

4 – mettez le mot « password » comme mot de passe à l'utilisateur luke.
5 – Essayez de vous connecter sous l'identité luke. Vérifiez.

```
test@yooceyy-GS60-6QC:~$ su - luke
Mot de passe :
luke@yooceyy-GS60-6QC:~$
```

6 – Créez l'arborescence de fichiers suivante :

```
root@yooceyy-GS60-6QC:~#
root@yooceyy-GS60-6QC:~#
root@yooceyy-GS60-6QC:~# mkdir /home/etoilenoire
root@yooceyy-GS60-6QC:~# cd /home/etoilenoire/
root@yooceyy-GS60-6QC:/home/etoilenoire# echo "voici les
plans" > plans
root@yooceyy-GS60-6QC:/home/etoilenoire# echo "c'est
ouvert" entree_secrets
root@yooceyy-GS60-6QC:/home/etoilenoire#
```

7 – 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.

```
root@yooceyy-GS60-6QC:~# sudo chown luke /home/etoilenoire
root@yooceyy-GS60-6QC:~# sudo chgrp jedi /home/etoilenoire
```

```
root@yooceyy-GS60-6QC:~# sudo chmod 700 /home/etoilenoire
root@yooceyy-GS60-6QC:~# sudo chmod g+rx /home/etoilenoire
root@yooceyy-GS60-6QC:~# sudo chmod o-rwx /home/etoilenoire
```

```
# Affichage des permissions du répertoire
root@yooceyy-GS60-6QC:~# ls -l /home/etoilenoire
total 8
-rw-r--r-- 1 root root 13 févr. 27 09:39 entree_secrets
-rw-r--r-- 1 root root 16 févr. 27 09:39 plans
root@yooceyy-GS60-6QC:~#
```

8 – 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@yooceyy-GS60-6QC:/home/etoilenoire# ls -l
total 8
-rw-r--r-- 1 root root 13 févr. 27 09:39 entree_secrets
-rw-r--r-- 1 root root 16 févr. 27 09:39 plans
root@yooceyy-GS60-6QC:/home/etoilenoire# chmod g+r plans
entree_secrets
root@yooceyy-GS60-6QC:/home/etoilenoire# sudo chmod o-rwx plans
entree_secrets
```

```
root@yooceyy-GS60-6QC:/home/etoilenoire# sudo chgrp jedi plans
root@yooceyy-GS60-6QC:/home/etoilenoire# sudo chgrp rebelles
entree_secrets
```

Vérification des permissions et des groupes :

```
root@yooceyy-GS60-6QC:/home/etoilenoire# ls -l plans entree_secrets
-rw-r----- 1 root rebelles 13 févr. 27 09:39 entree_secrets
-rw-r----- 1 root jedi     16 févr. 27 09:39 plans
root@yooceyy-GS60-6QC:/home/etoilenoire# ls -lG plans entree_secrets
-rw-r----- 1 root 13 févr. 27 09:39 entree_secrets
-rw-r----- 1 root 16 févr. 27 09:39 plans
root@yooceyy-GS60-6QC:/home/etoilenoire#
```

9 – On teste les accès :

```
luke@yooceyy-GS60-6QC:~$ ls /home/etoilenoire
entree_secrets  plans
luke@yooceyy-GS60-6QC:~$ echo "nouveau fichier" > test.txt
luke@yooceyy-GS60-6QC:~$ rm test.txt
luke@yooceyy-GS60-6QC:~$ nano plans
luke@yooceyy-GS60-6QC:~$ cat plans
voici les plans
Bonjour c'est luke


voici : commande introuvable
luke@yooceyy-GS60-6QC:~$ cat entree_secrets
c'est ouvert
cat: entree_secrets: Aucun fichier ou dossier de ce nom
> nano plans
```

Conclusion :

Les tests confirment que les droits d'accès définis pour Luke sont corrects. Il a tous les droits sur le répertoire etoilenoire et peut lire les fichiers plans et entree_secrets. Cependant, il ne peut pas modifier le fichier entree_secrets car il n'appartient pas au groupe rebelles.

A partir du compte **vador** :

```
vador@yooceyy-GS60-6QC:~$ ls /home/etoilenoire
entree_secrets  plans
vador@yooceyy-GS60-6QC:~$ echo "Nouveau fichier" >
test.txt
```

Vador ne peut pas créer de fichier dans le répertoire etoilenoire car il n'en est pas le propriétaire et n'a pas les droits d'écriture.

```
vador@yooceyy-GS60-6QC:/home/etoilenoire$ cat plans
voici les plans
vador@yooceyy-GS60-6QC:/home/etoilenoire$ cat
entree_secrets
cat: entree_secrets: Permission non accordée
vador@yooceyy-GS60-6QC:/home/etoilenoire$
```

Conclusion :

Les tests confirment que les droits d'accès définis pour Vador sont corrects. Il peut lister le répertoire etoilenoire et lire le fichier plans. Cependant, il ne peut ni créer ni supprimer des fichiers dans le répertoire, et il ne peut pas lire le fichier entree_secrets.

A partir du compte **solo** :

```
solo@yooceyy-GS60-6QC:~$ cd /home/
solo@yooceyy-GS60-6QC:/home$ cd etoilenoire/
-bash: cd: etoilenoire/: Permission non accordée
solo@yooceyy-GS60-6QC:/home$ echo "Ceci est un
nouveau fichier" > test.txt
-bash: test.txt: Permission non accordée
```

L’utilisateur solo n’a aucun accès au répertoire etoilenoire ni au fichier qu’il contient.

---

10 – Supprimez temporairement le droit d'exécution de la commande uptime.

```
root@yooceyy-GS60-6QC:~# alias uptime='echo "Commande
uptime non disponible."'
root@yooceyy-GS60-6QC:~# uptime
Commande uptime non disponible.
root@yooceyy-GS60-6QC:~# function uptime {
  echo "Commande uptime non disponible."
}
root@yooceyy-GS60-6QC:~# export -f uptime
root@yooceyy-GS60-6QC:~# uptime
Commande uptime non disponible.
root@yooceyy-GS60-6QC:~# exec bash
```

Informations de base:

Nom d'utilisateur :	**Luke**
UID :	**1000**
GID :	**100**
Répertoire personnel :	**/home/luke**
Shell par défaut :	**/bin/bash**

Groupes:

luke appartient au groupe jedi (GID 101)
luke appartient au groupe rebelles (GID 102)
Autres caractéristiques:

Luke a un compte utilisateur actif.
Luke n'a pas de date d'expiration de mot de passe.
Luke n'est pas sudoer.
Caractéristiques du groupe Rebelles

Informations de base:

Nom du groupe : rebelles
GID : 102
Description : Groupe des rebelles
Membres : luke ... (autres utilisateurs)
Autres caractéristiques: Le groupe rebelles est un groupe public.
Le groupe rebelles n'a pas de droits spéciaux.

---

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

```
btssio:x:1002:1003:,,,:/home/btssio:/bin/bash
luke:x:1003:1004:,,,:/home/luke:/bin/bash
vador:x:1004:1004:,,,:/home/vador:/bin/bash
solo:x:1005:1008:,,,:/home/solo:/bin/bash
```

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

```
yooceyy@yooceyy-GS60-6QC:~$ groups lola
lola : lola
yooceyy@yooceyy-GS60-6QC:~$ id lola
uid=1006(lola) gid=1009(lola) groupes=1009(lola)
```

14 – Gestion des groupes secondaires :

On veut affecter lola au groupe rebelles (comme groupe secondaire).
On veut affecter lola au groupe jedi. Lola quitte le groupe rebelles.
On veut que lola appartiennent au groupe jedi et rebelles.
On veut que lola n'appartienne plus à aucun groupe secondaire.

```
root@yooceyy-GS60-6QC:~# usermod -G rebelles lola
root@yooceyy-GS60-6QC:~# usermod -G jedi lola
root@yooceyy-GS60-6QC:~# gpasswd -d lola rebelles
Suppression de l'utilisateur lola du groupe rebelles
gpasswd : l'utilisateur 'lola' n'est pas membre de
'rebelles'
root@yooceyy-GS60-6QC:~# usermod -G jedi,rebelles
lola
root@yooceyy-GS60-6QC:~# gpasswd -d lola rebelles
Suppression de l'utilisateur lola du groupe rebelles
root@yooceyy-GS60-6QC:~# gpasswd -d lola jedi
Suppression de l'utilisateur lola du groupe jedi
```

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

```
python3 -c 'import pwd; pwd.setpwnam("lola",
"nouveau_mot_de_passe")'
```

16 – Rechercher les fichiers de l'utilisateur lola.

```
root@yooceyy-GS60-6QC:~# find /home/lola -type f
/home/lola/.profile
/home/lola/.bashrc
/home/lola/.bash_logout

root@yooceyy-GS60-6QC:~# ls -al /home/lola
total 20
drwxr-x---  2 lola lola 4096 mars  12 09:18 .
drwxr-xr-x 10 root root 4096 mars  12 09:18 ..
-rw-r--r--  1 lola lola  220 mars  12 09:18
.bash_logout
-rw-r--r--  1 lola lola 3771 mars  12 09:18 .bashrc
-rw-r--r--  1 lola lola  807 mars  12 09:18 .profile
```

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

```
root@yooceyy-GS60-6QC:~# sudo deluser lola
Suppression de l'utilisateur « lola » ...
Attention ! Le groupe « lola » ne contient plus aucun membre.
userdel : l'utilisateur lola est actuellement utilisé par le processus 10490
/usr/sbin/deluser : « /sbin/userdel lola » a retourné le code d'erreur 8. Abandon.
root@yooceyy-GS60-6QC:~# sudo rm -rf /home/lola
root@yooceyy-GS60-6QC:~# sudo find /etc -type f -name "*lola*" -delete
root@yooceyy-GS60-6QC:~# sudo grep -Rl lola /var/log/* | sudo xargs -I {} rm -f {}
root@yooceyy-GS60-6QC:~#
```

---

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

```
root@yooceyy-GS60-6QC:/home# ls -l
total 28
drwxr-x---  2 btssio  btssio  4096 févr. 27 09:35
```

```
btssio
drwxr-x---  2 luke    jedi    4096 févr. 27 09:39
etoilenoire
drwxr-x---  3 luke    jedi    4096 févr. 27 10:06
luke
drwxr-x---  3 solo    solo    4096 mars   5 09:14
solo
drwxr-x--- 16 test    test    4096 févr.  6 08:37
test
drwxr-x---  2 vador   jedi    4096 mars   5 09:14
vador
drwxr-x--- 25 yooceyy yooceyy 4096 févr. 15 19:54
yooceyy
root@yooceyy-GS60-6QC:/home# chmod g+s etoilenoire
root@yooceyy-GS60-6QC:/home# chmod +t etoilenoire
```

Explication des droits spéciaux :

SGID (Set Group ID):

Lorsque ce bit est activé sur un répertoire, tous les nouveaux fichiers créés dans ce répertoire hériteront du groupe du répertoire, quel que soit le groupe de l'utilisateur qui a créé le fichier.
Cela peut être utile pour les répertoires partagés où tous les utilisateurs doivent avoir accès aux fichiers du groupe.

Sticky-bit (bit collant):

Lorsque ce bit est activé sur un répertoire, seuls les utilisateurs qui ont créé un fichier ou qui sont propriétaires du répertoire peuvent le supprimer.
Cela peut être utile pour empêcher les utilisateurs de supprimer accidentellement ou malveillante les fichiers des autres utilisateurs.

---

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

```
yooceyy@yooceyy-GS60-6QC:/home$ sudo chmod u+s
etoilenoire

drwsr-s--T  2 luke    jedi    4096 févr. 27 09:39
etoilenoire
drwxr-x---  3 luke    jedi    4096 févr. 27 10:06
luke
drwxr-x---  3 solo    solo    4096 mars   5 09:14
solo
drwxr-x--- 16 test    test    4096 févr.  6 08:37
test
drwxr-x---  2 vador   jedi    4096 mars   5 09:14
vador
drwxr-x--- 25 yooceyy yooceyy 4096 févr. 15 19:54
yooceyy
```

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

```
vador@yooceyy-GS60-6QC:~> rm etoilenoire/F1

rm: impossible de supprimer « etoilenoire/F1 » :
Accès refusé
```

```
vador@yooceyy-GS60-6QC:~> chmod -t etoilenoire
vador@yooceyy-GS60-6QC:~> rm etoilenoire/F1
vador@yooceyy-GS60-6QC:~> ls etoilenoire
F1
F2
vador@yooceyy-GS60-6QC:~> rm etoilenoire/F1
```

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

Plusieurs utilisateurs peuvent formater la partition /dev/sda1, à condition d'avoir les droits appropriés :

Utilisateur root: L'utilisateur root a un accès complet à tous les fichiers et périphériques du système, y compris la partition /dev/sda1. Il peut utiliser la commande mkfs.ext4 /dev/sda1 pour formater la partition en ext4.

Utiliser les droits sudo: Un utilisateur avec les droits sudo peut également formater la partition /dev/sda1 en utilisant la commande sudo mkfs.ext4 /dev/sda1.

Utilisateur avec le groupe "disk": Les utilisateurs membres du groupe "disk" peuvent généralement formater les partitions de disque. Vous pouvez ajouter un utilisateur à ce groupe avec la commande sudo usermod -aG disk <nom_utilisateur>.

En résumé, les utilisateurs suivants peuvent formater la partition /dev/sda1 :
root

Utilisateurs avec les droits sudo
Utilisateurs membres du groupe "disk"

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

```
root@yooceyy-GS60-6QC:~# cp -a etoilenoire/* /tmp
```

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

```
root@yooceyy-GS60-6QC:~#chown luke entree_secrete
```

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

```
ls -l /etc/shadow /etc/passwd
```

```
-rw-r----- 1 root shadow 640 Jan 1  1970 /etc/shadow
-rw-r----- 1 root shadow 644 Jan 1  1970 /etc/passwd
```