Compte-Rendu TP10 : Les utilisateurs et les droits

1. La gestion des utilisateurs

- Afin de savoir si les comptes utilisateurs daemon et luke existent, on utilise respectivement les commandes **id daemon** et **id luke**. On aperçoit que le compte daemon existe, il a pour uid, gid et groupe : daemon. Cependant, le compte utilisateur luke n'existe pas.

```
root@DS1: ~#id daemon
uid=1(daemon) gid=1(daemon) groupes=1(daemon)
root@DS1: ~#id luke
id: « luke » : utilisateur inexistant
root@DS1: ~#_
```

- On créer les groupes jedi et rebelles avec la commande **groupadd**.

```
root@DS1: ~#groupadd jedi
root@DS1: ~#groupadd rebelles
root@DS1: ~#_
```

- On créer les comptes utilisateurs luke, vador et solo grâce à la commande **useradd**. On va les assigner directement à leurs groupes, luke appartiendra au groupe jedi en tant que groupe principal, grâce à la commande **–g jedi**, ainsi qu'au groupe secondaire rebelles avec la commande **–G rebelles**. On assigne également vador au groupe principal jedi par la même opération. Quant à solo on lui assigne rebelles en tant que groupe principal. On obtient donc 3 commandes :

1. **useradd –g jedi –G rebelles –m luke**
2. **useradd –g jedi –m vador**
3. **useradd –g rebelles –m solo**

On vérifie ensuite que les comptes ont bien été créés et assignés aux bons groupes en utilisant les commandes **id luke**, **id vador** et **id solo**.

```
root@DS1: ~#useradd -g jedi -G rebelles -m luke
root@DS1: ~#useradd -g jedi -m vador
root@DS1: ~#useradd -g rebelles -m solo
root@DS1: ~#id luke
uid=1002(luke) gid=1002(jedi) groupes=1002(jedi),1003(rebelles)
root@DS1: ~#id vador
uid=1003(vador) gid=1002(jedi) groupes=1002(jedi)
root@DS1: ~#id solo
uid=1004(solo) gid=1003(rebelles) groupes=1003(rebelles)
root@DS1: ~#_
```

- On affiche les dernières lignes des fichiers /etc/passwd et /etc/group en utilisant la commande **tail**. Ici, on affiche les 3 dernières lignes du fichier /etc/passwd avec **tail –3 /etc/passwd** et les 2 dernières lignes du fichier /etc/group en saisissant la commande **tail -2 /etc/group**.

```
root@DS1: ~#tail -3 /etc/passwd
luke:x:1002:1002::/home/luke:/bin/sh
vador:x:1003:1002::/home/vador:/bin/sh
solo:x:1004:1003::/home/solo:/bin/sh
root@DS1: ~#tail -2 /etc/group
jedi:x:1002:
rebelles:x:1003:luke
root@DS1: ~#_
```

- On saisit la commande **passwd luke**, afin de créer un mot de passe à l'utilisateur luke, qui sera password.

```
root@DS1: ~#passwd luke
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
root@DS1: ~#
```

- On ouvre une seconde console avec la commande **CTRL+ALT+F2**, et on se connecte sur le compte utilisateur luke. Le prompt qui s'affiche est "$".

- On se déconnecte du compte luke, et sur la première console, connectée en tant que root. On modifie le compte luke afin de remplacer le shell sh par bash. On entre alors la commande **usermod –s /bin/bash luke**.

```
root@DS1: ~#usermod -s /bin/bash luke
root@DS1: ~#_
```

- On se reconnecte sous le compte luke sur la seconde console. Le prompt a changé. De plus, on entre la commande **id**, sans préciser le compte à identifier, car celle-ci va automatiquement identifier l'utilisateur courant. On se déconnecte ensuite du compte, avec la commande **exit**.

```
luke@DS1:~$ id
uid=1002(luke) gid=1002(jedi) groupes=1002(jedi),1003(rebelles)
luke@DS1:~$ exit
```

- De retour sur root, on créer maintenant l'utilisateur leia, avec la commande **useradd**. On saisit la commande **id leia**, pour voir son groupe. Le compte leia, appartient au groupe principal du même nom, leia.

```
root@DS1: ~#useradd leia
root@DS1: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia)
root@DS1: ~#
```

- On fait un **ls –l /home** pour observer si le répertoire personnel de l'utilisateur leia a été créé. Ce n'est pas le cas.

```
root@DS1: ~#ls -l /home
total 36
drwxr-xr-x 7 guest guest     4096 déc.  16 15:42 guest
drwx------ 2 root  root     16384 déc.   1 15:10 lost+found
drwxr-xr-x 3 luke  jedi      4096 janv. 10 16:49 luke
drwxr-xr-x 3 sio   sio       4096 déc.   1 15:38 sio
drwxr-xr-x 2 solo  rebelles  4096 janv. 10 16:44 solo
drwxr-xr-x 2 vador jedi      4096 janv. 10 16:44 vador
root@DS1: ~#
```

- On affecte le compte utilisateur leia au groupe secondaire rebelles en saisissant la commande **usermod –G rebelles leia**.

```
root@DS1: ~#usermod -G rebelles leia
root@DS1: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1003(rebelles)
root@DS1: ~#
```

- On affecte le compte utilisateur leia au groupe secondaire jedi en saisissant la commande **usermod –G jedi leia**. De ce fait, il quitte le groupe rebelles.

```
root@DS1: ~#usermod -G jedi leia
root@DS1: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi)
root@DS1: ~#_
```

- On affecte ensuite leia aux groupes secondaires jedi et rebelles en utilisant la commande **usermod –G jedi,rebelles leia**.

```
root@DS1: ~#usermod -G jedi,rebelles leia
root@DS1: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi),1003(rebelles)
root@DS1: ~#
```

- On va maintenant désaffecter leia des groupes secondaires, en entrant la commande **usermod –G "" leia**.

```
root@DS1: ~#usermod -G "" leia
root@DS1: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia)
root@DS1: ~#
```

- On affecte ensuite leia au groupe secondaire jedi en utilisant la commande **usermod –G jedi leia**. Puis, sans désaffecter leia du groupe jedi, on va lui rajouter le groupe secondaire rebelles grâce à la commande **usermod –aG rebelles leia**.

```
root@DS1: ~#usermod -G jedi leia
root@DS1: ~#usermod -aG rebelles leia
root@DS1: ~#id leia
uid=1005(leia) gid=1005(leia) groupes=1005(leia),1002(jedi),1003(rebelles)
root@DS1: ~#_
```

- On supprime le compte utilisateur leia, en saisissant la commande **userdel leia**.

```
root@DS1: ~#userdel leia
root@DS1: ~#_
```

- On recréer le compte leia avec un répertoire de connexion. On va donc saisir la commande **useradd –m leia**. On se déplace ensuite, dans le répertoire qui vient d'être créé, avec la commande **cd /home/leia**. A partir de ce répertoire on utilise la commande **su – leia**, afin de se connecter sur le compte leia. Puis on va créer un fichier, d'abord on créer un répertoire avec la commande **mkdir rep1**, ensuite, on se déplace dans ce répertoire grâce à **cd rep1**, puis on créer le fichier en saisissant **touch fichier1**, puis on liste les fichiers avec **ls –l**. Le fichier précédemment créer apparaît bien. On se déconnecte ensuite du compte utilisateur leia grâce à **exit**, puis on quitte le répertoire /home/leia, avec la commande **cd**.

```
root@DS1: ~#useradd -m leia
root@DS1: ~#cd /home/leia
```

```
root@DS1: /home/leia#su - leia
$ mkdir rep1
$ cd rep1
$ touch fichier1
$ ls -l
total 0
-rw-r--r-- 1 leia leia 0 janv. 10 16:55 fichier1
$ exit
root@DS1: /home/leia#cd
root@DS1: ~#
```

- On supprime le compte utilisateur leia et les fichiers répertoriés dans son répertoire de connexion, en utilisant la commande **userdel –r leia**. On vérifie que tout a bien été supprimé.

```
root@DS1: ~#userdel -r leia
```

```
root@DS1: ~#ls -l /home/leia
ls: impossible d'accéder à '/home/leia': Aucun fichier ou dossier de ce type
root@DS1: ~#id leia
id: « leia » : utilisateur inexistant
root@DS1: ~#_
```

- On souhaite recréer le compte leia à l'identique, pour cela on utilise la commande **groupadd –g 1007 leia**, ainsi que la commande **useradd -u 1007 –g leia –m –s /bin/bash leia**. On vérifie ensuite qu'il a bien été créé, puis on lui assigne un mot de passe, le même que pour luke, password.

```
root@DS1: ~#groupadd -g 1007 leia
root@DS1: ~#useradd -u 1007 -g leia -m -s /bin/bash leia
root@DS1: ~#id leia
uid=1007(leia) gid=1007(leia) groupes=1007(leia)
root@DS1: ~#passwd leia
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
root@DS1: ~#
```

- On créer le compte toor afin qu'il ait les mêmes droits que root, on utilise donc la commande **useradd –u 0 –o –d /root -s /bin/bash toor**. On vérifie sa création avec **id toor**, puis on lui assigne un mot de passe avec **passwd toor**.

```
root@DS1: ~#useradd -u 0 -o -d /root -s /bin/bash toor
root@DS1: ~#id toor
uid=0(root) gid=0(root) groupes=0(root)
root@DS1: ~#passwd toor
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
root@DS1: ~#_
```

- On ouvre une seconde console et on se connecte sur le compte toor, on voit que le prompt s'affiche comme si on était sur le compte root.

```
Debian GNU/Linux 10 DS1 tty2

Hint: Num Lock on

DS1 login: toor
Password:
Last login: Sun Jan 10 16:49:37 CET 2021 on tty2
Linux DS1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) 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.
root@DS1: ~#_
```

- On créer maintenant un autre compte utilisateur nommé palpatine qui respectera la charte Debian, en utilisant la commande **adduser palpatine**.

```
root@DS1: ~#adduser palpatine
Ajout de l'utilisateur « palpatine » ...
Ajout du nouveau groupe « palpatine » (1004) ...
Ajout du nouvel utilisateur « palpatine » (1005) avec le groupe « palpatine » ...
Création du répertoire personnel « /home/palpatine »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
Changing the user information for palpatine
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Cette information est-elle correcte ? [O/n]y
root@DS1: ~#id palpatine
uid=1005(palpatine) gid=1004(palpatine) groupes=1004(palpatine)
root@DS1: ~#
```

- On affiche maintenant les caractéristiques de l'utilisateur local luke et du groupe local rebelles. Pour cela, on saisit la commande **grep luke /etc/passwd**, puis la commande **grep rebelles /etc/group**.

```
root@DS1: ~#grep luke /etc/passwd
luke:x:1002:1002::/home/luke:/bin/bash
root@DS1: ~#grep rebelles /etc/group
rebelles:x:1003:luke
root@DS1: ~#_
```

- On affiche les caractéristiques de l'utilisateur luke avec la commande **getent passwd luke**, puis du groupe jedi en utilisant **getent group jedi**.

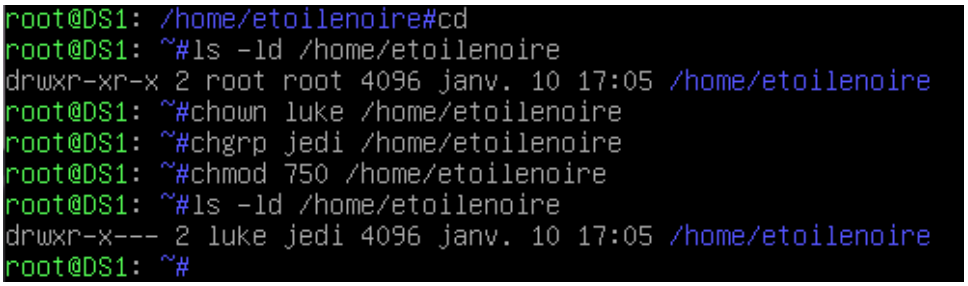
```
root@DS1: ~#getent passwd luke
luke:x:1002:1002::/home/luke:/bin/bash
root@DS1: ~#getent group jedi
jedi:x:1002:
root@DS1: ~#_
```

2. La gestion des droits

- On va créer une arborescence de fichiers, pour cela on créer dans un premier temps le répertoire /home/etoilenoire avec la commande **mkdir /home/etoilenoire**. Ensuite, on se déplace à l'intérieur de ce fichier, avec la commande **cd /home/etoilenoire**. On va désormais inscrire les messages "voici les plans" dans le fichier plans, et "c'est ouvert" dans le fichier entree_secrete, en saisissant respectivement les commandes **echo "voici les plans" > plans** et **echo "c'est ouvert" > entree_secrete**.

```
root@DS1: ~#mkdir /home/etoilenoire
root@DS1: ~#cd /home/etoilenoire
root@DS1: /home/etoilenoire#echo "voici les plans" > plans
root@DS1: /home/etoilenoire#echo "c'est ouvert" > entree_secrete
root@DS1: /home/etoilenoire#_
```

- On quitte le répertoire /home/etoilenoire en utilisant la commande **cd**. Ensuite, on liste les caractéristiques de ce répertoire avec la commande **ls –ld /home/etoilenoire**. On va maintenant, changer le propriétaire du répertoire qui sera luke, en saisissant la commande **chown luke /home/etoilenoire**, puis le groupe du répertoire qui sera jedi avec la commande **chgrp jedi /home/etoilenoire**. Enfin de modifier les permissions du fichier qui sera désormais accessible en lecture, écriture et accès au propriétaire, ainsi qu'accessible en lecture et accès au groupe mais pas aux autres, en se servant de la commande **chmod 750 /home/etoilenoire**. On vérifie ensuite les modifications.



- On change les caractéristiques des fichiers, ils seront accessibles en lecture seule pour le groupe et n'auront aucun droit pour les autres, pour cela on utilise la commande **chmod g=r,o= /home/etoilenoire***. Ensuite, on affilie le fichier plans au groupe jedi avec la commande **chgrp jedi /home/etoilenoire/plans**, et le fichier entree_secrete au groupe rebelles avec la commande **chgrp rebelles /home/etoilenoire/entree_secrete**. On vérifie les modifications en faisant un **ls –l /home/etoilenoire/**.

- On se déplace dans le compte utilisateur luke, avec **su – luke**. On liste dans un premier temps les fichiers du répertoire /home/etoilenoire, avec la commande **ls /home/etoilenoire/**. Ensuite, on affiche le contenu du fichier /home/etoilenoire/plans, en utilisant la commande **cat /home/etoilenoire/plans**. On affiche également le contenu du fichier /home/etoilenoire/entree_secrete, avec la commande **cat /home/etoilenoire/entree_secrete**. On saisit la commande **cal > /home/etoilenoire/fichier**, ce qui va créer dans un premier temps un fichier qui se nommera fichier dans le répertoire, et son contenu sera un calendrier. On liste les fichiers du répertoire, et on constate que le fichier nommé fichier est apparu. Ensuite, on supprime ce dernier avec la commande **rm /home/etoilenoire/fichier**. On liste encore une fois les fichiers du répertoire, fichier n'est plus là. Puis, on saisit la commande **echo "====" >> /home/etoilenoire/plans**, cependant luke ne possède pas les droits pour effectuer cette manipulation. On se déconnecte du compte.

```
root@DS1: ~#su - luke
luke@DS1:~$ ls /home/etoilenoire/
entree_secrete  plans
luke@DS1:~$ cat /home/etoilenoire/plans
voici les plans
luke@DS1:~$ cat /home/etoilenoire/entree_secrete
c'est ouvert
luke@DS1:~$ cal > /home/etoilenoire/fichier
luke@DS1:~$ ls /home/etoilenoire/
entree_secrete  fichier  plans
luke@DS1:~$ rm /home/etoilenoire/fichier
luke@DS1:~$ ls /home/etoilenoire/
entree_secrete  plans
luke@DS1:~$ echo "====" >> /home/etoilenoire/plans
-bash: /home/etoilenoire/plans: Permission non accordée
luke@DS1:~$ exit_
```

- On se connecte sur le compte utilisateur vador, avec **su – vador**. On liste les fichiers du répertoire /home/etoilenoire, il possède donc les fichiers entree_secrete et plans. On entre la commande **rm /home/etoilenoire/plans**, afin de supprimer le fichier plans du répertoire, mais vador ne possède pas les droits pour le faire. On saisit ensuite la commande **cal > /home/etoilenoire/fichier**, afin de créer le fichier nommé fichier est de lui mettre un calendrier en tant que contenu, mais encore une fois, le compte utilisateur n'a pas les droits. On affiche ensuite le contenu des fichiers plans et entree_secrete, avec les commandes respectives **cat /home/etoilenoire/plans** et **cat /home/etoilenoire/entree_secrete**. Cependant, le compte n'a pas les droits pour afficher le contenu du fichier entree_secrete. On saisit la commande **echo "====" >> /home/etoilenoire/plans**, mais le compte n'a également pas les drois pour l'effectuer. On se déconnecte ensuite avec **exit**.

```
root@DS1: ~#su - vador
$ ls /home/etoilenoire
entree_secrete  plans
$ rm /home/etoilenoire/plans
rm : supprimer '/home/etoilenoire/plans' qui est protégé en écriture et est du type « fichier » ? y
rm: impossible de supprimer '/home/etoilenoire/plans': Permission non accordée
$ cal > /home/etoilenoire/fichier
-sh: 3: cannot create /home/etoilenoire/fichier: Permission denied
$ cat /home/etoilenoire/plans
voici les plans
$ cat /home/etoilenoire/entree_secrete
cat: /home/etoilenoire/entree_secrete: Permission non accordée
$ echo "====" >> /home/etoilenoire/plans
-sh: 6: cannot create /home/etoilenoire/plans: Permission denied
$ exit
```

- On se connecte sur le compte utilisateur solo, avec **su – solo**. On liste les fichiers du répertoire /home/etoilenoire, mais le compte ne possède pas les droits pour effectuer cette action. On créer le fichier nommé fichier pour lui insérer un calendrier avec la commande **cal > /home/etoilenoire/fichier** mais le compte ne possède pas les droits. On supprime le fichier entree_secrete avec la commande **rm –f /home/etoilenoire/entree_secrete**, mais le compte ne possède pas les droits. On essaie d'afficher le contenu de entree_secrete grâce à la commande **cat /home/etoilenoire/entree_secrete**, mais solo ne possède toujours pas les droits. Le compte solo, ne possède donc aucuns droits. On se déconnecte avec **exit**.

```
root@DS1: ~#su - solo
$ ls /home/etoilenoire
ls: impossible d'ouvrir le répertoire '/home/etoilenoire': Permission non accordée
$ cal > /home/etoilenoire/fichier
-sh: 2: cannot create /home/etoilenoire/fichier: Permission denied
$ rm -f /home/etoilenoire/entree_secrete
rm: impossible de supprimer '/home/etoilenoire/entree_secrete': Permission non accordée
$ cat /home/etoilenoire/entree_secrete
cat: /home/etoilenoire/entree_secrete: Permission non accordée
$ exit
```

- On supprime temporairement le droit d'exécution à la commande uptime avec la commande **chmod o-x /usr/bin/uptime**. Sur root, on n'aperçoit aucun changement, cependant lorsque l'on se connecte sur le compte luke avec la commande **su – luke**, et que l'on saisit la commande **uptime**, celle-ci ne s'exécute pas, car le compte ne possède plus les droits. On se déconnecte avec **exit**.

```
root@DS1: ~#whereis uptime
uptime: /usr/bin/uptime /usr/share/man/man1/uptime.1.gz
root@DS1: ~#whatis uptime
uptime (1)           - Tell how long the system has been running.
root@DS1: ~#uptime
 17:15:30 up 33 min,  2 users,  load average: 0,00, 0,00, 0,00
root@DS1: ~#ls -l /usr/bin/uptime
-rwxr-xr-- 1 root root 10312 mai   31  2018 /usr/bin/uptime
root@DS1: ~#chmod o-x /usr/bin/uptime
root@DS1: ~#ls -l /usr/bin/uptime
-rwxr-xr-- 1 root root 10312 mai   31  2018 /usr/bin/uptime
root@DS1: ~#su - luke
luke@DS1:~$ uptime
-bash: /usr/bin/uptime: Permission non accordée
luke@DS1:~$ exit_
```

- Ensuite, on réactive le droit d'exécution à la commande uptime avec la commande **chmod o+x /usr/bin/uptime**, et lorsque l'on retourne sur le compte luke, et que l'on saisit la commande **uptime**, celle-ci est exécutée normalement.

```
root@DS1: ~#chmod o+x /usr/bin/uptime
root@DS1: ~#ls -l /usr/bin/uptime
-rwxr-xr-x 1 root root 10312 mai   31  2018 /usr/bin/uptime
root@DS1: ~#su - luke
luke@DS1:~$ uptime
 17:16:52 up 35 min,  2 users,  load average: 0,00, 0,00, 0,00
luke@DS1:~$ exit_
```

3. La gestion des droits, compléments

- On ajoute des droits spéciaux au répertoire etoilenoire, le SGID et le sticky-bit, avec la commande **chmod 3770 /home/etoilenoire/**. On liste les caractéristiques du répertoire /home/etoilenoire, en saisissant la commande **ls –ld /home/etoilenoire/**. On créer le fichier f1 et on lui applique le message "fichier un" comme contenu dans le répertoire /home/etoilenoire, avec la commande **echo "fichier un" > /home/etoilenoire/f1**. On se connecte sur le compte utilisateur luke, en entrant **su – luke**, et on créer un fichier f2 qui aura pour contenu le message "bonjour" en saisissant la commande **echo "bonjour" > /home/etoilenoire/f2**. On se déconnecte du compte luke avec **exit**.

```
root@DS1: ~#chmod 3770 /home/etoilenoire/
root@DS1: ~#ls -ld /home/etoilenoire/
drwxrws--T 2 luke jedi 4096 janv. 10 17:09 /home/etoilenoire/
root@DS1: ~#echo "fichier un" > /home/etoilenoire/f1
root@DS1: ~#su - luke
luke@DS1:~$ echo "bonjour" > /home/etoilenoire/f2
luke@DS1:~$ exit
```

- On se connecte sur le compte utilisateur vador avec **su – vador**, et on créer le fichier f3 qui aura pour contenu le message “bonjour” avec la commande **echo “bonjour” > /home/etoilenoire/f3**. On se déconnecte du compte vador avec **exit**. On liste ensuite, tous les fichiers du répertoire /home/etoilenoire, qui ont pour nom f, puis suivi d’un seul caractère (ex : f1, f2, f3) en entrant la commande **ls –l /home/etoilenoire/f?**.

```
root@DS1: ~#su - vador
$ echo "bonjour" > /home/etoilenoire/f3
$ exit
root@DS1: ~#ls -l /home/etoilenoire/f?
-rw-r--r-- 1 root  jedi 11 janv. 10 17:18 /home/etoilenoire/f1
-rw-r--r-- 1 luke  jedi  8 janv. 10 17:18 /home/etoilenoire/f2
-rw-r--r-- 1 vador jedi  8 janv. 10 17:19 /home/etoilenoire/f3
root@DS1: ~#_
```

- On se connecte sur le compte utilisateur vador avec **su – vador**, ensuite on essaie de supprimer le fichier f2 en entrant la commande **rm /home/etoilenoire/f2**, mais le compte vador ne possède pas les doits nécesssaires. On se déconnecte avec **exit**.

```
root@DS1: ~#su - vador
$ rm /home/etoilenoire/f2
rm : supprimer '/home/etoilenoire/f2' qui est protégé en écriture et est du type « fichier » ? y
rm: impossible de supprimer '/home/etoilenoire/f2': Opération non permise
$ exit
root@DS1: ~#_
```

- On supprime le droit sticky-bit, en saisissant la commande **chmod –t /home/etoilenoire/**. On liste ensuite les caractéristiques du fichier avec **ls –ld /home/etoilenoire/**. On se connecte sur le compte utilisateur avec **su – vador**, et on supprimer le fichier f2 avec la commande **rm /home/etoilenoire/f2**. Ensuite, on liste tous les fichiers de f2 en utilisant la commande **ls –l /home/etoilenoire/f2**, il ne trouve aucun résultat, ce qui montre que le fichier a bien été supprimé. On se déconnecte avec **exit**.

```
root@DS1: ~#chmod -t /home/etoilenoire/
root@DS1: ~#ls -ld /home/etoilenoire/
drwxrws--- 2 luke jedi 4096 janv. 10 17:19 /home/etoilenoire/
root@DS1: ~#su - vador
$ rm /home/etoilenoire/f2
rm : supprimer '/home/etoilenoire/f2' qui est protégé en écriture et est du type « fichier » ? y
$ ls -l /home/etoilenoire/f2
ls: impossible d'accéder à '/home/etoilenoire/f2': Aucun fichier ou dossier de ce type
$ exit
root@DS1: ~#_
```

- On fait un **ls –l /dev/sda1**, pour voir qui peut formater la partition /dev/sda1. Seul root et les membres du groupe disk peuvent.

```
root@DS1: ~#ls -l /dev/sda1
brw-rw---- 1 root disk 8, 1 janv. 10 16:41 /dev/sda1
root@DS1: ~#
```

- On copie tous les fichiers du répertoire /home/etoilenoire dans /tmp en conservant leurs attributs, en utilisant la commande **cp –p /home/etoilenoire/* /tmp**. Ensuite on fait un **ls –l /tmp/plans /tmp/entree_secrete**. On voit bien que les fichiers du répertoire etoilenoire ont été copiés dans tmp.

```
root@DS1: ~#cp -p /home/etoilenoire/* /tmp
root@DS1: ~#ls -l /tmp/plans /tmp/entree_secrete
-rw-r----- 1 root rebelles 13 janv. 10 17:05 /tmp/entree_secrete
-rw-r----- 1 root jedi     16 janv. 10 17:05 /tmp/plans
root@DS1: ~#
```

- On change le propriétaire du fichier entree_secrete, en saisissant la commande **chown luke /tmp/entree_secrete**. Le propriétaire devient alors luke. On fait un **ls –l /tmp/entree_secrete**, la modification du propriétaire est effective.

```
root@DS1: ~#chown luke /tmp/entree_secrete
root@DS1: ~#ls -l /tmp/entree_secrete
-rw-r----- 1 luke rebelles 13 janv. 10 17:05 /tmp/entree_secrete
root@DS1: ~#
```

- On se connecte sur le compte utilisateur luke avec **su – luke**. On affiche le contenu de /tmp/entree_secrete avec la commande **cat /tmp/entree_secrete**. On saisit la commande **echo “======” >> /tmp/entree_secrete**, pour rajouter le contenu des guillemets dans le fichier entree_secrete. On l’affiche encore une fois avec la commande **cat /tmp/entree_secrete**. La modification est effective. On entre la commande **/tmp/entree_secrete**, mais le compte luke n’a pas la permission pour l’exécutée. On se déconnecte avec **exit**.

```
root@DS1: ~#su - luke
luke@DS1:~$ cat /tmp/entree_secrete
c'est ouvert
luke@DS1:~$ echo "======" >> /tmp/entree_secrete
luke@DS1:~$ cat /tmp/entree_secrete
c'est ouvert
======
luke@DS1:~$ /tmp/entree_secrete
-bash: /tmp/entree_secrete: Permission non accordée
luke@DS1:~$ exit
```

- On se connecte sur le compte utilisateur solo avec **su – solo**. On affiche le contenu de /tmp/entree_secrete avec la commande **cat /tmp/entree_secrete**. On saisit la commande **echo “++++++” >> /tmp/entree_secrete**, pour rajouter le contenu des guillemets dans le fichier entree_secrete. Le compte solo n’a pas les droits pour effectuer cette action. On se déconnecte avec **exit**.

```
root@DS1: ~#su - solo
$ cat /tmp/entree_secrete
c'est ouvert
======
$ echo "++++++" >> /tmp/entree_secrete
-sh: 2: cannot create /tmp/entree_secrete: Permission denied
$ exit_
```

- A partir du compte root, on saisit la commande cat /tmp/entree_secrete pour afficher son contenu. On saisit la commande **echo "+=+=+=+=+=" >> /tmp/entree_secrete**, pour rajouter le contenu des guillemets dans le fichier entree_secrete. On affiche à nouveau le contenu du fichier, la modification est effective. On entre la commande **/tmp/entree_secrete**, mais le compte root n'a pas les droits pour l'effectuer.

- On affiche les droits du fichier shadow, en utilisant la commande **ls –l /etc/shadow**, il possède les droits de lecture et d'écriture pour l'utilisateur root, et le droit de lecture pour le groupe, les autres n'ont aucun droit. On affiche également les droits du fichier passwd, en saisissant la commande **ls -l /usr/bin/passwd**, l'utilisateur root à tous les droits, le groupe et les autres auront le droit de lecture et d'exécution.