UMBB, Faculté des Sciences — ING ***,1er année,Semestre 1***

Département d'informatique — Matière :Introduction aux Systèmes d'exploitation

COMPTE RENDU N°3
TP SYSTEME EXPLOITATION N° 04 :

PRÉSENTÉ PAR :

Prénom : Amar

Nom : Houmel

Groupe : 07

INTRODUCTION SUR LE SUJET DE TP :

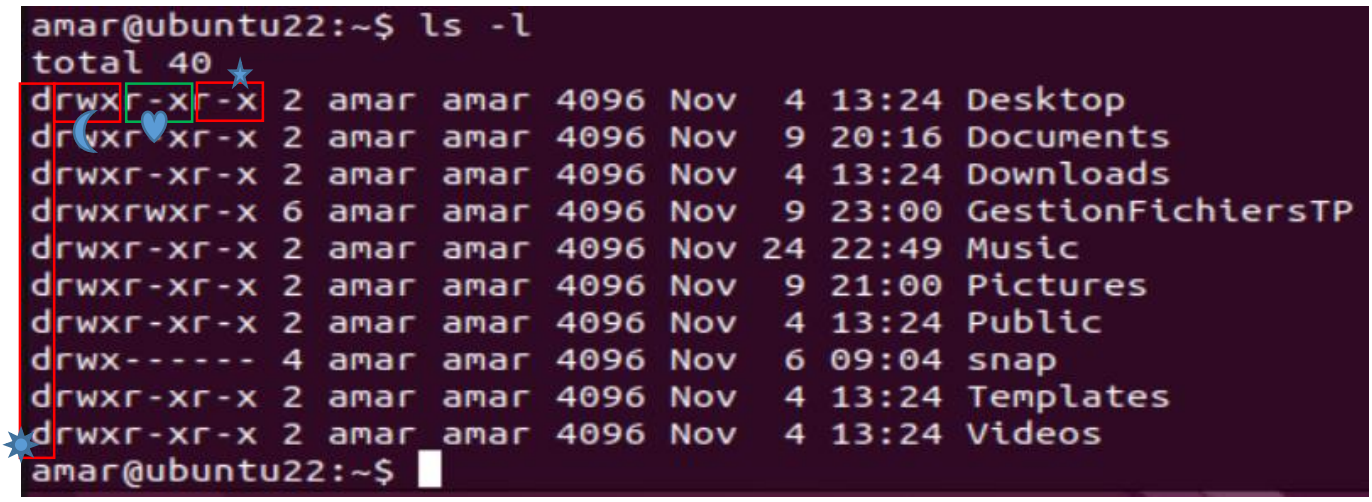
Alors cette seance pratique vous rendre plus a l'aise avec les autorisations d'acces aux fichiers et répertoires linux,cela inclut des notions avancé telle que les bits GUID SUID et le bit STICKY. Donc on va explorer en profondeur ces droits telle que comment ces permissions fonctionnent,comment les attribuer a des fichiers et répertoires.

PRÉSENTATION DES COMMANDES :

- Créé un répertoire : mkdir le_chemin/mon_dossier
- Créé un fichier : touch chemin/mon_fichier
- Enter dans un repertoires : cd chemin/nom_repertoires
- Afficher les droits des fichiers et répertoires : ls –l chemin /nom_réper
- Modifier les droit d'accés : chmod u=rwx,g=x,o=rw chemin/nom_fichier ou dossier (utilisateur peut lire ecrire , exucuter / groupe peut exuter / other peut lire et ecrire seulment)
- Pour definir le bit SUID : chmod u+s chemin/monfichier
- Créé un nouvel utilisateur : su (pour acceder aus mode root) enter
  sudo adduser utilisateur2
- Changez le propriétaire fichier pour qu'il soit dans utilisateur2 : (on est dans le mode root)
  sudo chown utilisateur2 chemin/monfichier
- Changer le groupe de fichier : sudo chown :utilisateur2 monfichier.txt
- Pour definir le bit GUID : chmod g+s chemin /nomdossier
- Pour definir le bit sticky : chmod o+t chemin/nomdossier

SOLUTION DE TP°03 :

2.1 Tâche 1 : Exploration des droits d'accès .

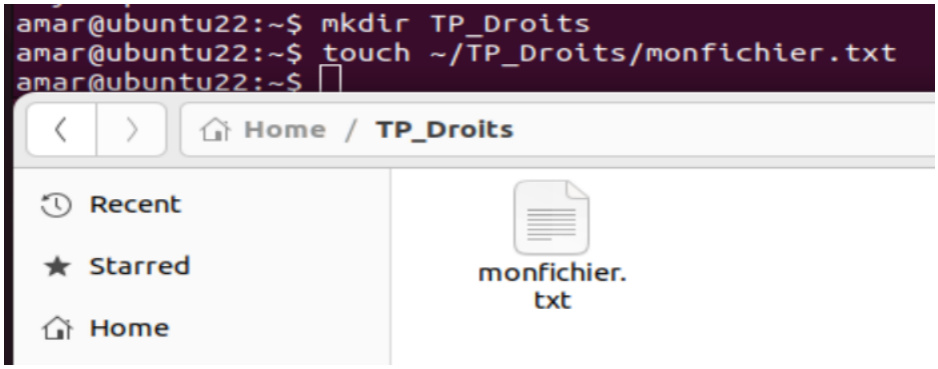


- Les propretairs de utilisateur
- Les propretairs de groupe
- Les propretairs des autres utilisateur
- Si il'ya d alors dossier et si – donc fichier

- r veut dir lire
- w veut dir ecrire
- x veut dir excuter
- veut dir rien de proprieté

2.2 Tâche 2 : Création de fichiers et de répertoires.

1. Créez un répertoire nommé "TP_Droits" dans votre répertoire personnel :et Créez un fichier vide nommé "monfichier.txt" à l'intérieur de "TP_Droits".



3. Affichez les droits d'accès du répertoire "TP_Droits" et du fichier "monfichier.txt" en utilisant ls -l.

```
amar@ubuntu22:~$ ls -l ~/TP_Droits
total 0
-rw-rw-r-- 1 amar amar 0 Dec  1 18:13 monfichier.txt
amar@ubuntu22:~$
```

2.3 Tâche 3 : Modification des droits d'accès.

```
amar@ubuntu22:~$ chmod u=rwx,g=w,o= ~/TP_Droits/monfichier.txt
amar@ubuntu22:~$ ls -l ~/TP_Droits
total 0
-rwx-w---- 1 amar amar 0 Dec  1 18:13 monfichier.txt
amar@ubuntu22:~$
```

2.4 Tâche 4 : Utilisation de chmod.

1. Utilisez la commande chmod pour donner au propriétaire du fichier "mon-fichier.txt" uniquement les dro de lecture et d'écriture. Vérifiez les droits d'accès modifiés.

```
amar@ubuntu22:~$ chmod u=rw,g=rw,o=rw ~/TP_Droits/monfichier.txt
amar@ubuntu22:~$ ls -l ~/TP_Droits
total 0
-rw-rw-rw- 1 amar amar 0 Dec  1 18:13 monfichier.txt
amar@ubuntu22:~$
```

2. Ensuite, utilisez chmod pour définir le bit SUID sur "monfichier.txt".

```
amar@ubuntu22:~$ chmod u+s ~/TP_Droits/monfichier.txt
amar@ubuntu22:~$
```

3. Expliquez ce que fait le bit SUID et comment il affecte le fichier.

Alors c'est une permission spécial sur les fichiers , il permet a un utilisateur d'éxcuter ce fichier avec les permission du propriétaire du fichier plutôt que les siennes propres lorsqu'il lance le fichier

2.5 Tâche 5 : Changement de propriétaire et de groupe.

1. Créez un nouvel utilisateur "utilisateur2" en utilisant la commande adduser.

```
amar@ubuntu22:~$ su
Password:
root@ubuntu22:/home/amar# sudo adduser utilisateur2
Adding user `utilisateur2' ...
Adding new group `utilisateur2' (1001) ...
Adding new user `utilisateur2' (1001) with group `utilisateur2' ...
Creating home directory `/home/utilisateur2' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for utilisateur2
Enter the new value, or press ENTER for the default
        Full Name []: amimar
        Room Number []: houmel
        Work Phone []: 000000000
        Home Phone []: 0000000
        Other []: 000000
Is the information correct? [Y/n]
root@ubuntu22:/home/amar#
```

2. Changez le propriétaire du fichier "monfichier.txt" pour qu'il soit "utilisateur2".

```
root@ubuntu22:/home/amar/TP_Droits# sudo chown Utilisateur2 monfichier.txt
chown: invalid user: 'Utilisateur2'
root@ubuntu22:/home/amar/TP_Droits# ls -ld monfichier.txt
-rw-rw-rw- 1 utilisateur2 amar 0 Dec  1 18:13 monfichier.txt
root@ubuntu22:/home/amar/TP_Droits# ls -l monfichier.txt
-rw-rw-rw- 1 utilisateur2 amar 0 Dec  1 18:13 monfichier.txt
root@ubuntu22:/home/amar/TP_Droits#
```

3. Changez le groupe du fichier en "utilisateur2" également.

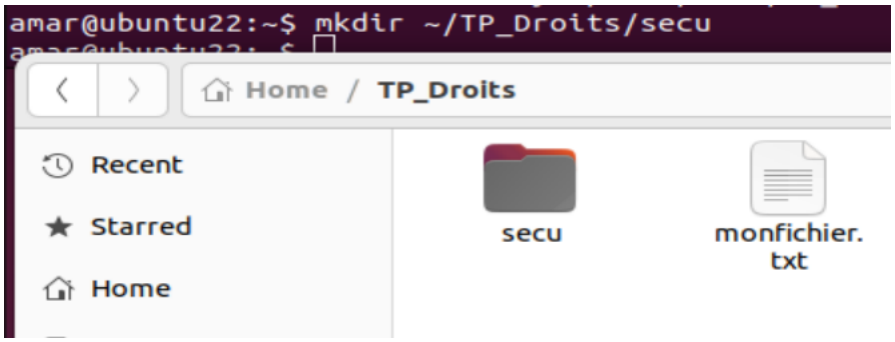
```
amar@ubuntu22:~/TP_Droits$ su
Password:
root@ubuntu22:/home/amar/TP_Droits# sudo chown Utilisateur2:audio monfichier.txt
chown: invalid user: 'Utilisateur2:audio'
root@ubuntu22:/home/amar/TP_Droits#
```

4. Affichez les propriétaires et groupes actuels du fichier.

```
amar@ubuntu22:~/TP_Droits$ ls -l
total 4
-rw-rw-rw- 1 utilisateur2 amar    0 Dec  1 18:13 monfichier.txt
drwxr-xr-x 2 root         root 4096 Dec  1 22:51 secu
```

2.6 Tâche 6 : Permissions avancées.

1. Créez un répertoire nommé "secu" à l'intérieur de "TP_Droits".



2. Modifiez les droits d'accès de "secu" de manière à ce que le propriétaire puisse tout faire, le groupe puisse lire et exécuter, et les autres utilisateurs ne puissent rien faire.

```
amar@ubuntu22:~$ chmod u=rwx,g=rx ~/TP_Droits/secu
```

3. Ensuite, utilisez chmod pour définir le bit GUID sur "secu".

```
amar@ubuntu22:~/TP_Droits$ chmod g+s secu
```

4. Expliquez ce que fait le bit GUID et comment il affecte le répertoire.

Le bit GUID est un bit d'autorisation avancé dans linux qui permet l'orsque il est activé a un utilisateur d'éxcuter un répertoire avec les autorisation du groupe propriétaire du répertoire .

2.7 Tâche 7 : Exploration des répertoires.

1. Utilisez la commande cd pour naviguer dans le répertoire "TP_Droits".

```
amar@ubuntu22:~$ cd ~/TP_Droits
amar@ubuntu22:~/TP_Droits$
```

2. Essayez de lister le contenu du répertoire "secu".

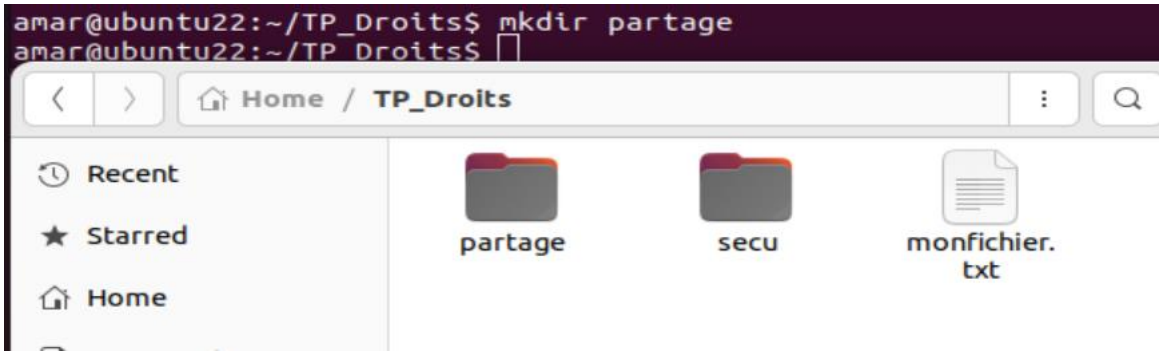
```
amar@ubuntu22:~/TP_Droits$ ls -l secu
total 0
amar@ubuntu22:~/TP_Droits$
```

3. Expliquez pourquoi vous avez ou n'avez pas pu accéder au répertoire.

J'ai pas les permission nécessaire pour accéder au répertoire , et pour les ajouter on utilisans la command chmod

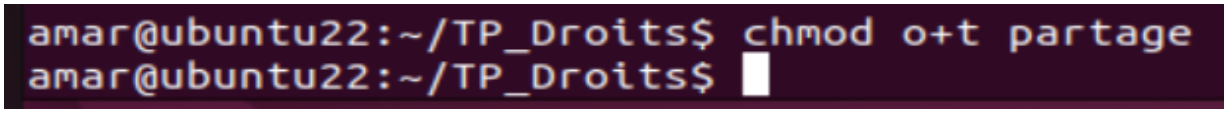
2.8 Tâche 8 : Bits Sticky.

1. Créez un répertoire nommé "partage" à l'intérieur de "TP_Droits".



2. Modifiez les droits d'accès de "partage" de manière à ce que le propriétaire puisse tout faire, le groupe puisse tout faire, et les autres utilisateurs ne puissent rien faire.

3. Ensuite, utilisez chmod pour définir le bit sticky sur "partage".



4. Expliquez ce que fait le bit sticky et comment il affecte le répertoire.

Le bits sticky lorsque il est activé a un répertoire a un effet spécial , il permet de controler la suppresion

Des fichiers par les utilisateurs. Lorsque il est activé sur un répertoire, seuls le proprietaire de fichier ,le proprietaire de répertoires et le superutilisateur peuvent supprimer ou renommer des fichiers a l'intérie de ce répertoires .

CONCLUSION :

Alors les droits d'accés sont un pilier fondamental de la sécurité et la gestion des données dans les système linux . ils offrent un contrôle granulaire sur l'accées aux fichiers et répertoires,permettant de definier qui peut lire,ecrire et exécuter des donnes.En maitrisant ces droits d'accés ,les utilisateurs peuvent controler efficacement l'accés aux ressources et garantir un environnement informatique sécurisé et bien géré.