

- 1) **Id (cette commande renvoie l' UID, GID et les groupes dont l'utilisateur est membre)**
more /etc/passwd chaque ligne du fichier contient les infos suivantes concernant un utilisateur qu'il soit humain ou logiciel
(user : mot de passe : uid : gid : description : répertoire de connexion : shell de connexion)
Rq : le root à l'uid et gid '0'
- 2) **mkdir ESI**
ls -l ESI
cd ESI
cat > STP1
ls -l STP1 (décrire les droits d'accès rwx pour les fichiers ET pour les répertoires)
la lecture, l'écriture et l'exécution n'ont pas le même sens pour les fichiers et les répertoires.
les droit sont résumés par le schémas donné en début de la fiche des questions
- 3) **cat STP1**
chmod -r STP1
cat STP1 (on constate l'interdiction d'accès, puis on réaffiche les droits d'accès du fichier et on constate encore que la commande retire les droits pour tous les utilisateurs)
- 4) **cat >> STP1**
chmod +r STP1 (le + permet de rétablir les droits et on constate que la modification du fichier resta autorisée malgré l'impossibilité de lecture)
- 5) **chmod +r-w ou chmod =rx**
cat >> STP1 (le plus pour l'ajout et le moins pour le retrait du droit, le = permet de fixer tous les droits en même temps ainsi le droit d'écriture a été retiré en n'étant pas mentionné en utilisant le =)
- 6) **rm STP1**
touch STP2
cat > STP3
ls -l
cd .. (on prépare les étapes suivantes)
- 7) **chmod -w ESI**
rm ESI/STP2 (on remarque que l'absence du droit de lecture interdit la suppression du fichier)
chmod +w ESI
chmod -w ESI/STP2
rm ESI/STP2 (on peut supprimer le fichier malgré l'avertissement car c'est le contenu du fichier que l'on ne peut supprimer et non pas le fichier lui-même)
il est possible d'ajouter l'option -f à la commande rm pour empêcher l'affichage du message d'avertissement
- 8) **chmod -r ESI**
ls ESI

cat ESI/STP3 (on peut lire le fichier qui n'est pas protégé en lecture même si le répertoire qui le contient l'est, cela impose de connaître le fichier bien sûr)

9) **chmod u=rw ESI 600**
chmod g=rw ESI 060
chmod ug=rw ESI 660
chmod o= ESI 000
chmod o-rw ESI -006
chmod g+r ESI +040
chmod g-w ESI -020
chmod g+r-w ESI +040-020
chmod g+r-w,o=rwx ESI +040-020+007
chmod a=rw ESI 666
chmod =rw ESI 666

il est possible de changer les droits d'accès individuellement avec les commandes données en exemple, le u pour l'utilisateur propriétaire, le g pour le groupe et le o pour les autres, en rouge vous avez la notation octale équivalente).

rm -r ESI
mkdir ESI2
ls -l

umask (on remarque les quatre chiffres en notation octale, ils correspondent aux droits étendus (3bits additionnels), la commande umask contrairement à chmod affiche les restrictions et non les droits autorisés par défaut lors de la création de nouveau fichiers ou répertoires)

10) **umask 007** (la commande n'exige pas de donner 4 caractères on peut aussi écrire « **umask 7** » dans cet exemple)

rm -r ESI2
mkdir ESI3

ls -l (comparer avec le dernier **ls -l** et constater que les droits autorisés par défaut à la création d'un nouveau répertoire ont changé)

11) **touch ESI3/STP4**

ls -l ESI3 (les droits par défaut changent également pour les fichiers, sauf que contrairement aux répertoires, si le droit d'exécution n'est pas restreint par le masque, le droit d'exécution ne sera pas attribué aux nouveaux fichiers, on notera aussi que le changement de droits par défaut reste valable pour toute la session)
chown user01 STP4 (on peut également utiliser l'uid (par exemple 1001). Pour l'utilisation avec ubuntu version desktop, on peut faire l'essai avec l'utilisateur « root », cela doit nécessiter d'utilisation de « sudo » avant la commande. L'utilisation de « sudo » étant restreinte aux administrateurs, cette commande ne peut être testée en salle que par votre enseignant, il est recommandé à l'étudiant de réessayer les deux dernières commandes de cette fiche sur vos PC personnels)

12) **chgrp 0 STP4**

ls -l (même chose pour le groupe **ls -l** nous montre que le groupe propriétaire a changé, il faut noter que seul le propriétaire du fichier et root ont le droit de changer les droits d'accès d'un fichier)