

# TP LINUX SA ODC P6

## EXERCICE 1 - Définition des utilisateurs (à traiter comme utilisateur)

- 1- Combien d'utilisateurs UNIX sont définis localement sur votre système?
- 2- Quel est le shell de l'utilisateur root? Et celui de l'utilisateur halt? A quoi sert ce dernier?
- 3- Que fait la commande /sbin/nologin? Quels comptes l'utilisent-elle, pourquoi?

## EXERCICE 2 - Création d'utilisateurs et de groupes (à traiter comme administrateur (root))

- 1- Lire la documentation de la commande useradd, puis créer 2 utilisateurs (Toto et Tata). Immédiatement après création, quel est le mot de passe de l'utilisateur? Pourquoi?
- 2- Dans quels groupes sont vos utilisateurs?
- 3- Créer un groupe etudiant réunissant vos deux utilisateurs créé précédemment.
- 4- Créer un utilisateur qui a les mêmes privilèges que root,
- 5- Créer un utilisateur Patato sans utiliser la commande useradd

## EXERCICE 3 - Droits (commandes chown, chgrp, chmod)

- 1- Changer (en tant qu'étudiant) les droits sur le compte "etudiant" afin que les autres utilisateurs ne puissent pas y accéder.
- 2- Créer un répertoire dans /tmp qui ne soit accessible (rx) que par les membres du groupe etudiant, puis y créer (toujours en tant qu'étudiant) un fichier maman.txt qui soit lisible et modifiable par les utilisateurs du groupe etudiant, mais pas par les autres.

Tester (ajouter un autre utilisateur au groupe etudiant).

Les utilisateurs du groupe etudiant peuvent-ils supprimer le fichier maman.txt ? Pourquoi ?

## EXERCICE 4 - Droits d'accès

**Exercice à traiter comme utilisateur (etudiant), non root!**

1- Essayer (dans un shell etudiant) de supprimer ou de modifier le fichier /var/log/messages.

Que se passe-t-il? Expliquer la situation à l'aide de la commande ls -l

2- A l'aide de la commande id, vérifier votre identité et le(s) groupe(s) auquel vous appartenez.

3- Créer un petit fichier texte mes\_notes.txt (de contenu quelconque), qui soit lisible par tout le monde, mais pas modifiable (même pas par vous).

4- Créer un répertoire nommé secret, dont le contenu soit visible uniquement par vous même. Les fichiers placés dans ce répertoire sont-ils lisibles par d'autres membres de votre groupe?

5- Créer un répertoire nommé connaisseurs tel que les autres utilisateurs ne puissent pas lister son contenu mais puissent lire les fichiers qui y sont placés. On obtiendra :

\$ ls connaisseurs

ls : connaisseurs: Permission denied

\$ cat connaisseurs/toto

<...le contenu du fichier toto (s'il existe)...>

{sidebar id=6}{sidebar id=1}

## EXERCICE 5

Il s'agit de créer un répertoire partagé par tous les membres du groupe etudiant

Créez dans /home un répertoire appelé rep-etudiant. Rappelez pourquoi cette tâche relève des prérogatives de root

Faites-le appartenir au groupe etudiant

Modifier les permissions sur le rep-etudiant, pour que tous les membres du groupe etudiant puissent y écrire et s'y déplacer.

3. En tant que etudiantx, vous créez un fichier math.txt, et vous le déposez dans /home/rep-etudiant.

Vérifier le bon accès en lecture seulement pour les membres du groupe.

Votre collègue etudianty (y#x), tente de supprimer ce fichier ou de le renommer

Y parvient-il ? Essayez !

Pourtant, vérifiez que ce fichier appartient au groupe etudiant

N'est-ce pas inquiétant ? Expliquez comment cela est possible.

Demandez à root de positionner le "sticky bit" sur le répertoire partagé.

Vérifiez bien que le problème est réglé et protège le propriétaire des tentatives de suppression ou de changement de nom de ses fichiers.

## EXERCICE 6

Travaillez en tant qu'utilisateur de base.

Copiez le fichier /etc/hosts.allow. Quels sont l'UID et le GID du fichier maintenant chez vous ?

Au moyen des commandes « chown » et « chgrp », pouvez-vous passer au nom de l'utilisateur « user » et du group « student » la copie chez vous du fichier ? Refaites en tant qu'utilisateur de base la copie du fichier précédent mais en le copiant dans « /tmp ». Réessayez après les commandes « chown » et « chgrp » en tant que root sur la copie dans « /tmp ». Est-ce OK ?

## EXERCICE 7

Sur votre machine de TP, créez dans « /tmp » un fichier. Faites ensuite les commandes suivantes en étant root :

```
# chown 3333 /tmp/foo
```

```
# chgrp 4444 /tmp/foo
```

Utilisez en fait un UID et un GID qui ne sont pas en service. Pour en être sûr, reportez-vous au fichier « /etc/passwd » et à la base de données NIS (obtenue par « ypcat passwd »).

Que vous renvoie un « ls -l /tmp/foo » ?

Recherchez avec la commande « find » dans « /tmp » les fichiers qui appartiennent à un UID pour lesquels il n'y a pas d'utilisateur associé. Pour cela, reportez vous à la documentation de « find » et cherchez-y l'option qui convient.

Faites le ménage dans « /tmp » une fois cet exercice terminé.

## EXERCICE 8

Travaillez en tant que root sur votre machine

Pouvez-vous prendre l'identité d'un autre utilisateur ? Quelle commande utiliseriez-vous pour faire cela ?

Comprenez-vous maintenant pourquoi la compromission du compte root est un tel objectif pour les pirates ?

### EXERCICE 9

Travaillez en tant qu'utilisateur de base. Passez sous l'identité de root en faisant « su ».

Réussissez-vous à lancer la commande « ifconfig -a » ?

Travaillez en tant qu'utilisateur de base. Passez sous l'identité de root en faisant « su - ».

Réussissez-vous à lancer la commande « ifconfig -a » ?

Expliquez ce qui se passe dans les deux cas. Quelle moralité en extraire ?

### EXERCICE 10

Que font les commandes « groups », « id », « whoami », « who am i » ?

### EXERCICE 11:

Définir le lot de commandes à exécuter pour créer 4 utilisateurs en suivant les règles suivantes:

- Création de 2 groupes.
  - Les premier et deuxième utilisateurs sont membres du premier groupe.
  - Les troisième et quatrième utilisateurs sont membres du second groupe.
  - Le deuxième utilisateur est aussi membre du second groupe.
  - Le quatrième utilisateur est aussi membre du premier groupe.
  - Outre leur répertoire de travail, les utilisateurs ont accès à un répertoire commun /home/groupe1 et/ou /home/groupe2 suivant leur groupe. Dans ce répertoire, ils peuvent écrire, créer des fichiers mais ne peuvent pas effacer les fichiers.
1. Détaillez les étapes de création des groupes, des utilisateurs et des répertoires en indiquant quels fichiers vous utilisez et quelles commandes vous utilisez sur ces fichiers.

2. Modifiez les profils des utilisateurs pour qu'au login, le répertoire d'accueil sur lequel il souhaite travailler lui soit demandé (s'il entre U, il sera sous son répertoire, s'il entre G, il sera sous le répertoire de son groupe).
3. Parmi ces 3 valeurs: 066, 067, 077, quel umask positionnez- vous? Expliquez pour chaque valeur quelles sont les conséquences de ce choix.