UTILISATEURS ET DROITS

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 ?

2 – Créez les groupes **jedi** et **rebelles**.

3 – Créez les comptes **luke**, **vador** et **solo**.

Le compte **luke** appartient au groupe **jedi** (comme groupe principal) et au groupe **rebelles** (comme groupe secondaire). Le compte **vador** appartient au groupe **jedi**. Le compte **solo** fait partie du groupe **rebelles**.

Visualisez ensuite les comptes créés.

4 – mettez le mot « **password** » comme mot de passe à l'utilisateur **luke**.

5 – Essayez de vous connecter sous l'identité **luke**. Vérifiez.

6 – Créez l'arborescence de fichiers suivante :

```
root@ubuntu:~# mkdir /home/etoilenoire
root@ubuntu:~# cd /home/etoilenoire/
root@ubuntu:/home/etoilenoire# echo "voici les plans" > plans
root@ubuntu:/home/etoilenoire# echo "c'est ouvert" > entree_secrets
root@ubuntu:/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 accès au groupe mais pas aux autres.

Vérification.

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**.

Vérification.

9 – On teste les accès :

A partir du compte **luke** :

l'utilisateur **luke**, en tant que propriétaire, a tous les droits sur le répertoire **etoilenoire**. Il peut le lister, créer ou supprimer des fichiers dedans et il a accès aux fichiers qu'il contient.

En tant que membre du groupe **jedi**, il peut lire le fichier , et en tant que membre du groupe **rebelles**, il peut lire le fichier **entree_secrete**. Par contre, il ne peut pas modifier le fichier **plans**. Seul root peut le faire.

A partir du compte **vador** :

l'utilisateur **vador**, en tant que membre du groupe **jedi**, peut lister le répertoire **etoilenoire**. Il a accès également aux fichiers qu'il contient. Par contre il ne peut ni créer ni supprimer des fichiers contenus dedans.

En tant que membre du groupe **jedi**, il peut lire le fichier **plans** mais pas le fichier **entree_secrete**.

Il ne peut pas modifier le fichier **plans**. Seul root peut le faire.

A partir du compte **solo** :

L'utilisateur **solo** n'a aucun droit sur le répertoire **etoilenoire**.

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

11 – Affichez les caractéristiques de l'utilisateur **luke** et du groupe **rebelles**.

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

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

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** appartienne au groupe **jedi** et **rebelles**.

- On veut que **lola** n'appartiennent plus à aucun groupe **secondaire**.

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

16 – Rechercher les fichiers de l'utilisateur **lola**.

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

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

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

- Sous le compte **root**, on crée le fichier F1.
- Sous le compte **luke**, on crée le fichier F2.

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

- cas 1 : on conserve le sticky-bit
- cas 2 : on supprime le sticky-bit.

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

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

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

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

From:
/ - **Les cours du BTS SIO**

Permanent link:
/doku.php/si5/droitstp3

Last update: **2013/12/25 18:06**