LES UTILISATEURS ET LES DROITS SOUS LINUX

La gestion des comptes utilisateurs est une prérogative du compte **root**.

GESTION DES UTILISATEURS

LES FICHIERS DE CONF

/etc/passwd

```
hannibal@box:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail...
…
hplip:x:113:7:HPLIP system user,,,:/var/run/hplip:/bin/false
saned:x:114:123::/home/saned:/bin/false
hannibal:x:1000:1000:lecter,,,:/home/hannibal:/bin/bash
dhcpd:x:115:125::/var/run:/bin/false
sshd:x:116:65534::/var/run/sshd:/usr/sbin/nologin
hannibal@box:~$
```

La base de données utilisateurs d'un système UNIX est le fichier texte **/etc/passwd** (appelé le fichier password), qui énumère tous les usernames valides avec les informations qui leur sont associées. Ce fichier possède une ligne par username, divisée en sept champs délimités par le caractère `:' :

- Username.
    - Mot de passe, encrypté.
      * user id numérique.
      * group id numérique.
      * Nom complet ou autre description du compte.
      * Répertoire d'accueil.
      * Shell de login (programme lancé au login).

etc/group

```
hannibal@box:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:hannibal
tty:x:5:
…
saned:x:123:
hannibal:x:1000:
sambashare:x:124:hannibal
dhcpd:x:125:
hannibal@box:~$
```

Ce fichier référence l'ensemble des groupes du système. Une ligne concerne un groupe et elle est structurée en quatre champs :

groupname:password:gid:member, ...

- groupname : le nom du groupe.
- password : en général, on n'utilise pas de mot de passe de groupe.
- gid : identifiant du groupe. Entier codé sur deux octets. Les valeurs inférieures à 10 sont réservées aux groupes systèmes .

- member, ... : liste des membres du groupe.

/etc/shadow

```
hannibal@box:~$ cat /etc/shadow
cat: /etc/shadow: Permission non accordée
hannibal@box:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 1098 déc.  17 11:05 /etc/shadow
hannibal@box:~$ sudo -s
[sudo] password for hannibal:
root@box:~# cat /etc/shadow
root:!:15673:0:99999:7:::
daemon:*:15455:0:99999:7:::
…
saned:*:15455:0:99999:7:::
hannibal:$6$y17A79w7$z/hJkVUGL1qLNiSNGgHWfA3NhdwL.Y0NYFNdAEXgqwPTsaZJPoLBXpBu76V4U0.5hzawr.vQO7iw.JgVLWX
EJ/:15673:0:99999:7:::
dhcpd:*:15690:0:99999:7:::
sshd:*:15691:0:99999:7:::
root@box:~#
```

Les différentes entrées de ce fichier, séparées par des « : » ont les significations suivantes :

- nom de l'utilisateur pour la connexion ;
- mot de passe chiffré (le « 1 » du début indique l'utilisation d'un chiffrement MD5. Le signe « * » indique que le compte ne peut pas se connecter) ;
- nombre de jours, à partir du 1er janvier 1970, depuis que ce mot de passe a été modifié pour la dernière fois ;
- nombre de jours restants avant que l'on ne doive modifier le mot de passe ;
- nombre de jours après lequel on doit modifier le mot de passe ;
- nombre de jours pendant lesquels l'utilisateur est averti que son mot de passe arrive en fin de validité.

LES COMMANDES

- **useradd** (variante interactive Debian : **adduser**)
  - **groupadd** (variante interactive Debian : **addgroup**)
  - **usermod** et **groupmod**
  - **userdel** et **groupdel**
  - **passwd**
  - **chpasswd**
  - **id**
  - **chsh**

    ```
        et **chfn**
    ```

    * **geten**t

  - **pwck**

    ```
        et **grpck**
    ```

LES DROITS

CATEGORIES D'UTILISATEURS

- le propriétaire du fichier,
- le groupe auquel appartient le propriétaire,
- les autres !

LES DROITS ORDINAIRES

- r (read)
- w (write)
- x (execute) droit d'exécuter le fichier ou de parcourir le répertoire.

LES DROITS SPECIAUX

LE STICKY BIT (valeur octale 1000)

Lorsque ce droit est positionné sur un répertoire, il interdit la suppression d'un fichier qu'il contient à tout utilisateur autre que le propriétaire du fichier. Néanmoins, il est toujours possible pour un utilisateur possédant les droits d'écriture sur ce fichier de le modifier (par exemple de le transformer en un fichier vide). La création de nouveaux fichiers est toujours possible pour tous les utilisateurs possédant le droit d'écriture sur ce répertoire.

C'est le cas du répertoire /tmp par exemple :

```
hannibal@ubuntu:/$ cd /
hannibal@ubuntu:/$ ls -l | grep tmp
drwxrwxrwt  17 root root 266240 nov.  10 10:30 tmp
```

DROITS D'ENDOSSEMENT

La philosophie des droits d'endossement est d'augmenter les privilèges des utilisateurs. Par exemple, le droit Set-UID (SUID) sur un binaire exécutable permet à l'utilisateur de l'application correspondante d'avoir les mêmes droits d'accès que le propriétaire du binaire. Le droit Set-GID (SGID) permet, lui, d'endosser les droits du groupe auquel est affilié le binaire.

Exemple : Le fichier /etc/shadow n'est en théorie accessible qu'à root. Or, tout utilisateur à accès en écriture à ce fichier lorsqu'il change son mot de passe grâce à la commande /usr/bin/passwd. L'explication réside dans le fait que cette commande, possédée par root possède le droit SUID et donne de fait à tous les utilisateurs les mêmes droits que root.

```
hannibal@ubuntu:/$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 42824 sept. 13 00:29 /usr/bin/passwd
hannibal@ubuntu:/$
```

LES DROITS EN OCTAL

- 4000 Le droit SUID (u+s).
  - 2000 Le droit SGID (g+s).
  - 1000 Le sticky-bit (+t).
  - 0400 Le droit de lecture pour le propriétaire (u+r).
  - 0200 Le droit d'écriture pour le propriétaire (u+w).
  - 0100 Le droit d'exécution pour le propriétaire (u+x).
  - 0040 Le droit de lecture pour le groupe (g+r).
  - 0020 Le droit d'écriture pour le groupe (g+w).
  - 0010 Le droit d'exécution pour le groupe (g+x).
  - 0004 Le droit de lecture pour les autres (o+r).
  - 0002 Le droit d'écriture pour les autres (o+w).
  - 0001 Le droit d'exécution pour les autres (o+x).

MODIFICATION DES DROITS

La commande **chmod** permet de faire ça !chmod

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

Permanent link:
/doku.php/si5/droitslinux

Last update: **2013/12/25 13:43**