R101 TD5

Initiation aux comptes et aux droits sous linux

L'objectif de ce TD est de découvrir la gestion des comptes sous linux, d'appréhender la gestion des droits et de se familiariser avec leur manipulation.

1. Comptes d'utilisateurs et groupes

Les informations concernant les comptes des utilisateurs locaux d'une machine sont stockés dans le fichier : `/etc/passwd`. Voici un exemple partiel de son contenu.

```
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
…
test:x:1000:1000:test,,,:/home/test:/bin/bash
fred:x:1001:1001:,,,:/home/fred:/bin/bash
```

Normalement le contenu est de la forme :

`Nom de connexion : Mot de passe crypté : UID : GID : commentaire : répertoire de connexion : commande gérant la session`

1. Que pouvez vous dire sur le mot de passe des différents utilisateurs ?
2. Quel est le répertoire de l'utilisateur fred ?
3. Quel est son UID, GID ?
4. Est il possible d'avoir 2 UID identique pour 2 nom différents ?

Les groupes quant à eux sont stockés dans le fichier `/etc/goup` dont la structure est la suivante :

`nom du groupe : mot de passe : GID : liste des membres`

```
root:x:0:
daemon:x:1:
bin:x:2:
cdrom:x:24:test
floppy:x:25:test
audio:x:29:test
video:x:44:test
netdev:x:109:test
bluetooth:x:110:test
scanner:x:116:saned,test
test:x:1000:
fred:x:1001:
wireshark:x:120:test
```

1. Quel est l'intérêt d'ajouter test au groupe cdrom, floppy, audio, wireshark ?
2. L'utilisateur fred pourra-t-il utiliser correctement wireshark ?

Les valeurs utilisées par défaut lors de la création d'un utilisateur sont enregistrées dans le fichier /etc/login.defs. En voici un exemple.

```
# /etc/login.defs - Configuration control definitions for the login package.
# Enable logging and display of /var/log/faillog login failure info.
# This option conflicts with the pam_tally PAM module.
FAILLOG_ENAB            yes
# Enable display of unknown usernames when login failures are recorded.
LOG_UNKFAIL_ENAB        no
# Enable logging of successful logins
LOG_OK_LOGINS           no
```

```
# Login configuration initializations:
#       ERASECHAR       Terminal ERASE character ('\010' = backspace).
#       KILLCHAR    Terminal KILL character ('\025' = CTRL/U).
#       UMASK           Default "umask" value.
# The ERASECHAR and KILLCHAR are used only on System V machines.
# UMASK is the default umask value for pam_umask and is used by
# useradd and newusers to set the mode of the new home directories.
# Prefix these values with "0" to get octal, "0x" to get hexadecimal.
ERASECHAR       0177
KILLCHAR    025
UMASK           022
# Password aging controls:
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
# Min/max values for automatic uid selection in useradd
UID_MIN                 1000
UID_MAX                 60000
# Min/max values for automatic gid selection in groupadd
GID_MIN                 1000
GID_MAX                 60000
# Max number of login retries if password is bad. This will most likely be
# overriden by PAM, since the default pam_unix module has it's own built
# in of 3 retries. However, this is a safe fallback in case you are using
# an authentication module that does not enforce PAM_MAXTRIES.
LOGIN_RETRIES           5
# Max time in seconds for login
LOGIN_TIMEOUT           60
# Should login be allowed if we can't cd to the home directory?
# Default in no.
DEFAULT_HOME    yes
```

1. Quel est l'intérêt de loger les tentatives infructueuses de login ?
2. Pourquoi n'enregistre-t-on pas les logs des tentatives fructueuses ?
3. Expliquer l'intérêt de changer les mot de passe et les valeurs données par défaut.
4. Quel sera l'UID du premier utilisateur créé sur la machine ? Peut on le savoir ?

Les mots de passe sont maintenant stockés dans le fichier `/etc/shadow`. Voici un exemple de ce fichier :

```
root:$6$kO/ww.sS$17zdtzuCQu3iAygz/sRpuWlpcK62pnuDkX/6eoNBcAd4AycNtDm.IMnKaiHmrbEKjGTlwcuqae5SsOPZ5m9Ha.:15647:0:99999:7:::
daemon:*:15647:0:99999:7:::
bin:*:15647:0:99999:7:::
…
test:$6$bY9xE1F6$EUF8y6EHaSPEHE/UvSXsPu..dFRTLf7PlzunS2.kv8DtYD95ca1/7UY6WFXrNVvUYVnSeBkhzOnRwaoKyQz0W0:15647:0:99999:7:
::
fred:$6$sOtqmwHz$jza4KyCXowk0JB8xV00a2ABMBD8.2ZSaw8sdWV5Wt/Oxa.uoBSYc6/Le.pdMOlp9Ihdw6K8adyXeWSfO1kK1K0:15918:0:99999:7:
::
```

Le format de chaque ligne contient 9 champs séparés par des « : » et est le suivant :
Nom de connexion : mot de passe chiffré:date du dernier changement de mot de passe : age minimum du mot de passe : age maximum du mot de passe : période d'avertissement pour le changement de mot de passe : période d'inactivité du mot de passe : date de fin de validité du compte : champs réservé (pas utilisé)

1. Quel est environ le jour de dernier changement du mot de passe de « test » sachant que le nombre est exprimé en jour depuis le 1/1/1970 (on oubliera les années bissextiles).
2. Qui à votre avis a le droit de consulter le fichier /etc/shadow ?
3. Pourquoi les champs age minimum et maximum sont identiques pour tous les utilisateurs créés ?

Nous reviendrons dans la partie des droits sur la valeur de la variable UCHAR …

2. Commandes de gestion des utilisateurs

Les commandes de base pour gérer les utilisateurs sont :

- useradd pour ajouter un utilisateur
- userdel pour le supprimer
- passwd pour changer le mot de passe

La syntaxe de la commande useradd est la suivante :

```
useradd [-b base_dir] [-c comment] [-d home_dir] [-e expire_date] [-f inactive_time] [-g initial_group (must exist)] [-G group[,...]] -m (create home dir) [-u UID] -U (create a group based on login) [-s Shell] -r (compte system)... login
```

1. Créer un compte pour l'utilisateur toto avec une description étudiant RT1, un répertoire à son nom, une date d'expiration au 2014-01-01, avec l'uid 1010, appartenant à un groupe toto ainsi qu'aux groupes wireshark, audio et cd_rom.

On donne le contenu du répertoire /etc/group suivant : root, test, fred (plus d'autres lié au système) et le contenu du répertoire /home (là où sont les dossiers utilisateurs) : fred, test. L'admin utilise la commande suivante :

useradd -b /home/azerty -d /home/azerty -g azerty -u 2001 azerty

2. A la création le message d'erreur apparaît : *useradd : le groupe azerty n'existe pas*. Que faut il faire pour corriger cela ?
3. Le fait que le répertoire de base n'existe pas ne bloque pas la création, est-ce normal ?
4. Que se passera-t-il quand azerty va se logger ? Dans quel répertoire va-t-il se retrouver à votre avis ?

3. Droits sur les fichiers

Lorsque l'on souhaite visualiser les caractéristiques d'un fichier on utilise la commande ls avec les options suivantes :

- -l pour avoir les droits sur les fichiers
- -a pour voir les fichiers commençant par .

Le format d'affichage est le suivant :

```
root@DebianFred_serv:/home/test# ls -al ou-personnes.ldif
-rw-r--r-- 1 root root 184  4 nov.   2012 ou-personnes.ldif
```

- Le premier – correspond au format du fichier (- pour fichier ordinaire, d pour un répertoire, s pour une socket, …)
- Ensuite viennent 9 lettres pour les droits
- Le nom de l'utilisateur
- Le nom du groupe du fichier
- La taille du fichier en octets
- La date de dernière modification
- le nom du fichier

1. Quel est le groupe auquel appartient le fichier ou-personnes.ldif ?
2. Quels sont les droit associés à l'utilisateur root ?
3. Peut il exécuter le fichier ?
4. Un membre du groupe root peut-il modifier ce fichier ?
5. Un non-membre du groupe root peut-il le modifier ?

6. On représente souvent en octale les permissions sur les fichiers Linux pourquoi ?
7. Combien de bit comprend un nombre noté en base 8 ? Donner les droits en base 8 du fichier précédent.
8. La valeur UMASK 022 (vue précédemment) permet de définir les droits par défaut lors de la création de fichiers/dossiers. Pour les fichiers les droits sont le résultat d'une soustraction entre 666 en octal et le UMASK et pour les dossiers c'est entre 777 et le UMASK. Quels sont les droits par défaut pour les fichiers et les dossiers avec un UMASK à 022 ?
9. A quoi correspondent les droits en lecture et en exécution sur un dossier ?
10. A quoi correspondent les droits 777 et 755 ? Pourquoi ne faut-il pas tout mettre en 777 ?
11. Pourquoi un utilisateur ne doit-il pas placer les droits en 555 pour un de ses fichiers ?

4. Problèmes de droits (Philippe Pujas)

1. Rappel

- L'utilisateur `toto` du groupe `rt2` ne peut **lire** un fichier que si :
  - le fichier appartient à `toto` et est en mode lecture pour le propriétaire ;
  - ou, le fichier appartient au groupe `rt2` et le fichier est en lecture pour le groupe ;
  - ou, le fichier est en lecture pour les autres.
- L'utilisateur `toto` du groupe `rt2` ne peut **créer** un fichier dans un répertoire que si :
  - le répertoire appartient à `toto` et est en mode écriture pour le propriétaire ;
  - ou, le répertoire appartient au groupe `rt2` et est en mode écriture pour le groupe ;
  - ou, le répertoire est en mode écriture pour les autres.

2. Configuration d'un serveur Web

Soit la configuration suivante. L'administrateur du site est l'utilisateur `webmaster`, son groupe est `wwwqui` ne comporte qu'un seul membre : `webmaster`. L'arborescence du site appartient à `webmaster` et au groupe `www`. Elle est en rw pour `webmaster` et en r pour `www`. Les scripts CGI sont exécutables par `webmaster` et par le groupe `www`.

1. Montrer que les documents locaux du site ne peuvent pas être accédés par les utilisateurs du serveur (sauf webmaster).
2. Pourquoi le serveur `httpd` ne doit-il pas avoir les droits suivants : propriétaire `root`, groupe `root` ?
3. Pourquoi le serveur ne peut-il pas avoir les droits : propriétaire : `webmaster`, groupe `apache`?
4. Pourquoi le serveur ne peut-il pas avoir les droits : propriétaire : `apache`, groupe `apache` ?
5. Que se passe-t-il si le serveur a été configuré avec les droits : propriétaire : `apache`, groupe `www` ?
6. Dans ce dernier cas, quels doivent être les droits des pages personnelles des utilisateurs ? Problème ?
7. Comment configurer les répertoires recevant, par exemple, les fichiers de session ?
8. Comment configurer le système pour que le site comporte plusieurs parties administrées par différents webmasters.