Gestion des utilisateurs

1 Préalables

Lisez la partie gestion des utilisateurs du cours.

2 Création d'un utilisateur à la main

Pour créer un utilisateur manuellement (afin de bien comprendre le processus) suivez les étapes ci-dessous :

1. choisissez un UID libre,
2. créer une nouvelle ligne dans `/etc/passwd` (mot de passe vide) pour un utilisateur `essai`,
3. testez l'existence de ce compte (commande `id essai`),
4. essayez de vous connecter avec ce compte cela doit marcher (**en mode texte uniquement**),
5. créez une nouvelle ligne dans `/etc/shadow`,
6. en tant que root, modifiez le mot de passe de cet utilisateur (commande `passwd essai`),
7. essayez de vous connecter à nouveau (toujours en mode texte),
8. créez un répertoire d'accueil pour cet utilisateur :

```
cp -rv /etc/skel /home/essai    # créer
chown -R essai /home/essai      # donner
```

9. essayez de vous connecter une dernière fois.

En tant qu'**administrateur**, Vous pouvez modifier les attributs de ce compte :

- verrouillage/déverrouillage (commande `passwd -l`),
- changement de la politique de sécurité (commande `chage`),

En tant que **propriétaire** du compte, vous pouvez modifier les attributs de ce compte :

- changement du shell (commande `chsh`),
- changement des informations GECOS (commande `chfn`),

3 Configurer la session utilisateur

- Commencez par prévoir un nouveau point d'installation en créant les répertoires

```
mkdir -p /opt/{bin,man/man1,doc}
```

- Puis déposez un logiciel fictif `mycom` à l'intérieur :

```
# création d'un executable simple /opt/bin/mycom
echo echo Voila un essai > /opt/bin/mycom
chmod a+rx /opt/bin/mycom

# création de la page de manuel /opt/man/man1/mycom.1
echo "Comment␣utiliser␣mycom" > /opt/man/man1/mycom.1

# création de la documentation /opt/doc/mycom.txt
echo "Ceci␣est␣une␣documentation" > /opt/doc/mycom.txt
```

- Normalement, vous ne devriez pas avoir accès à ce logiciel (commande et page de manuel).
- Nous allons enrichir la session de l'utilisateur pour offrir cet accès :
  - ▷ créez un script `/etc/profile.d/opt.sh` exécutable,

```
touch /etc/profile.d/opt.sh        # création
chmod a+rx /etc/profile.d/opt.sh   # droits
```

  - ▷ placez à l'intérieur les instructions de modification des variables d'environement `PATH` et `MANPATH` :

```
PATH=$PATH:/opt/bin
MANPATH=$MANPATH:/opt/man
```

  - ▷ Déconnectez-vous et reconnectez-vous. Vous devriez avoir accès au logiciel `mycom` :

```
type mycom
man mycom
echo $PATH
echo $MANPATH
```

Note : Les script placés dans `/etc/profile.d` sont exécutés à chaque connexion d'un utilisateur (étudiez le script `/etc/profile`). C'est un moyen simple pour configurer les sessions des utilisateurs.

4 Le mode d'authentification

Dans la RedHat (donc la CentOS) la configuration de l'authentification passe par la sélection d'un profil par ceux déjà prévus. Cette configuration est basée sur l'utilitaire `authselect`. Voici quelques exemples :

- **Important** : Prenez un instantané pour pouvoir revenir en arrière.
- Ouvrez (avec `nedit` par exemple) le fichier de configuration des modules PAM de l'authentification :

```
nedit-client /etc/pam.d/system-auth
```

- Questionnez le profil courant (ce doit être `sssd` un service d'authentification sécurisé) :

```
authselect current
```

  Vous remarquerez (dans `/etc/pam.d/system-auth`) la présence du module `pam_sss.so` à toutes les étapes de l'authentification (`auth`, `password`, `account` et `session`).

- Questionnez la liste des profils disponibles :

```
authselect list
```

- Choisissez le profil minimal (**opération dangereuse**) :

```
authselect select minimal
```

Vous observerez une simplification importante du fichier `/etc/pam.d/system-auth`.

- Chaque profil comporte des fonctionnalités. Listez celles du profil `minimal` :

```
authselect list-features minimal
```

- **Important** : Annulez les modifications et revenez à l'instantané précédent.

5 Imposer des limites aux utilisateurs

- Essayez de modifier les limites de votre session (commande `ulimit` en **mode utilisateur**) pour stopper les processus de plus de 1 seconde. **Attention** : sur nos machines virtuelles, le décompte du temps est très approximatif.

```
ulimit -t 1
time bash -c 'while␣true;␣do␣true;␣done'
```

- Faites la même chose avec le fichier `/etc/security/limits.conf` (aidez vous du manuel avec `man limits.conf`). Vérifiez (dans `/etc/pam.d/system-auth`) que le module `pam_limits.so` est utilisé.

6 Limiter l'accès

Faites en sorte d'interdire l'accès de votre machine pour certains utilisateurs (par exemple `root`) et à partir de certaines machines (fichier `/etc/security/access.conf`). **Attention** : il faut sûrement modifier la configuration PAM du service d'authentification (fichier `/etc/pam.d/system-auth`) pour utiliser le module `pam_access`

```
authselect enable-feature with-pamaccess
```

Vérifiez le blocage après un accès infructueux dans le journal avec `journalctl -n`.