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 :

⏩ **Travail à faire :**

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.

⚠ **Que les choses soient claires :** Cet exercice est destiné à vous faire comprendre le mécanisme de création des utilisateurs. Dans la pratique, si vous avez des utilisateurs à créer, vous devriez utiliser `useradd`.

⏩ **Travail à faire :** 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` à installer avec `dnf -y install util-linux-user`),

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

- changement du shell (commande `chsh` en choisissant `/bin/sh`),
- changement des informations GECOS (commande `chfn` mais après avoir modifié les droits dans le fichier `/etc/login.defs` ligne `CHFN_RESTRICT`),

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

Prenez quelques minutes pour relire le transparent sur PAM. 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 :

- 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 (il ne devrait pas être configuré) avec la commande ci-dessous.

```
authselect current
```

- Questionnez la liste des profils disponibles :

```
authselect list
```

- Choisissez le profil minimal (**opération dangereuse**) avec la commande ci-dessous. Vous observerez une simplification du fichier `/etc/pam.d/system-auth`.

```
authselect select minimal
```

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

```
authselect list-features minimal
```

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 de temps CPU. **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

Nous allons interdire l'accès à votre machine pour certains utilisateurs (par exemple `essai`) à partir de certaines machines.

- Commencez par activer `pamaccess` qui est configuré par le fichier `/etc/security/access.conf` :

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

- Vérifiez qu'une ligne `pamaccess` a bien été ajoutée au fichier de configuration de l'authentification (`/etc/pam.d/system-auth`).
- Modifiez `/etc/security/access.conf` afin de bloquer les connexions de l'utilisateur `essai` depuis `10.0.2.15`.
- Vérifiez le blocage après un accès infructueux dans le journal avec `journalctl -g pam_access`.

7 Création automatique de répertoire d'accueil

Nous allons (rapidement) ajouter un nouveau module PAM qui permet de créer les répertoires d'accueil à la volée lors de l'authentification des utilisateurs. Suivez les étapes ci-dessous :

Activer

```
# installer les logiciels nécessaires
dnf -y install oddjob-mkhomedir

# activer et démarrer le service
systemctl enable --now oddjobd.service

# activer le module PAM de création des répertoires d'accueil
authselect enable-feature with-mkhomedir
```

Tester

```
# supprimer le répertoire de l'utilisateur essai (pour tester)
mv /home/essai/ /home/essai.old

# tester
ssh essai@localhost
```

8 Bilan

Nous avons maintenant un système d'authentification enrichi de deux modules PAM :

```
authselect current
```