Gestion des utilisateurs

I - Gestion des utilisateurs

Créer un utilisateur

```
useradd [option] <NomUtilisateur>
```

Options :

- m : crée un répertoire personnel éponyme pour l'utilisateur dans /home
- d : spécifie l'emplacement pour le répertoire personnel
- s /bin/bash : permet de forcer l'utilisation de bash à la place de shell à l'utilisateur
- p : permet de définir le mot de passe (non chiffré)

Modifier le mot de passe

```
passwd <NomUtilisateur>
```

Suppression d'un utilisateur

```
userdel -r <NomUtilisateur>
```

L'option -r permet de supprimer le répertoire personnel de l'utilisateur de manière récursive, son dossier courriel ainsi que son groupe éponyme

Créer un groupe

```
groupadd <NomGroupe>
```

Ajouter un utilisateur à un groupe

```
adduser <NomUtilisateur> <NomGroupe>
```

Retirer un utilisateur d'un groupe

```
deluser <NomUtilisateur> <NomGroupe>
```

Suppression d'un groupe

```
groupdel <NomGroup>
```

Liste des utilisateurs : **/etc/passwd**
Liste des groupes : **/etc/group**
Mot de passe des utilisateurs : **/etc/shadow**

II - Désactivation de root

Pour sécuriser l'accès à un serveur / machine, il faut désactiver la cible principale des hacker : l'utilisateur "root"

Installer sudo

```
apt install sudo
```

Ajout de l'utilisateur au groupe sudo

```
adduser <user> sudo
```

L'utilisateur est maintenant capable d'exécuter des commandes superutilisateur (apt install...)

Maintenant il faut désactiver root

```
$sudo passwd -l root
```

Cette option désactive le mot de passe root et donc empêche la connexion (lock)

Pour réactiver le compte :

```
$sudo passwd -u root
```

unlock