**La gestion des utilisateurs et des groupes**

**Les différents types de comptes**

Les comptes utilisateur ne sont pas tous égaux sur Linux. On distingue trois types:

**Superutilisateur**

L'utilisateur **root** est le plus important du système d'exploitation Linux.

Avec "Ubuntu", l'utilisateur **root** n'est pas activé.

Le compte utilisateur qui est créé lors de l'installation de "Ubuntu" est membre du groupe **sudo**. Nous discuterons du groupe **sudo** dans un autre document.

L'utilisateur **root** n’est pas concerné par les droits d’accès aux fichiers.

Ce super-utilisateur aura donc à sa charge les tâches d’administration du système.

**Le UID de l'utilisateur root est égal à 0 (zéro).**

**Comptes systèmes (bin, daemon, sync, apache…)**

Plusieurs comptes ne sont pas affectés à des utilisateurs, ils servent à faciliter la gestion des droits d’accès de certaines applications et démons.

Par exemple, le serveur Web utilise l’identité du compte "apache".

Pour des raisons de sécurité, on fera en sorte que personne ne puisse se connecter à l'ordinateur à partir de l’un de ces comptes.

**Les UID compris entre 1 et 499 sont utilisés pour les comptes systèmes.**

**Comptes ordinaires**

Tous les autres comptes utilisateur sont associés à des personnes; leur vocation est de permettre à des utilisateurs de type standard de se connecter.

**Le UID d’un utilisateur sera un nombre égal ou supérieur à 1000.**

**Les commandes pour gérer les utilisateurs**

useradd, usermod et userdel sont dans le dossier /usr/sbin/

La commande **adduser** permet d’ajouter un nouvel utilisateur.

**note: cette commande est interactive et n'est pas présente dans toutes les distributions linux**

**Dans le cours C32, nous utiliserons la commande "useradd".**

**Création d'un compte utilisateur avec "useradd"**

La commande **useradd** permet d’ajouter un nouvel utilisateur.

**création d'un utilisateur sans spécifier son UID**

**sudo useradd u1**

1. ajoute une ligne à la fin du fichier **/etc/passwd**
2. un UID est assigné à l'utilisateur u1
3. par défaut le groupe principal de l'utilisateur porte le nom de l'utilisateur

Les options par défaut pour la création des utilisateurs sont spécifiées dans le fichier "**/etc/login.defs**"**.**

Les valeurs par défaut de la commande useradd se trouvent dans le fichier "**/etc/default/useradd**".

**Modification d'un compte utilisateur avec "usermod"**

La commande **usermod** permet de modifier les paramètres d'un compte utilisateur.

Pour verrouiller le compte d'un utilisateur

**sudo usermod -L u1**

Pour déverrouiller le compte d'un utilisateur

**sudo usermod -U u1**

**Destruction d'un compte utilisateur "userdel"**

La commande **userdel** permet d'effacer un compte utilisateur.

Pour supprimer l'utilisateur u1

**sudo userdel u1**

Pour supprimer l'utilisateur u1 et son dossier personnel

**sudo userdel -r u1**

**Les différents types de groupes**

Il existe différents types de groupes permettant de donner des droits communs à un ensemble d’utilisateurs.

**Groupe root**

C’est le groupe principal de l’administrateur (**root**).et son GID est 0.

**Le GID du groupe root est égal à 0 (zéro).**

**Groupes systèmes (bin, daemon, sync, apache**…)

Ces groupes jouent le même rôle que les comptes du même nom et permettent de donner les mêmes droits d’accès à un ensemble d’applications.

**Les groupes système auront un GID compris entre 1 et 499.**

**Groupes ordinaires**

Ces groupes représentent un ensemble de personnes réelles devant accéder aux mêmes fichiers.

**Les groupes ordinaires auront un GID égal ou supérieur à 1000.**

**Groupe principal**

Un utilisateur est obligatoirement membre d'un groupe d'utilisateurs sur un système LINUX, son groupe principal sera utilisé lors de la création des fichiers.

**Groupe secondaire**

Un utilisateur peut éventuellement appartenir à plusieurs autres groupes, ses groupes secondaires détermineront ses droits d'accès aux fichiers créés par d'autres membres de ces groupes.

**Les commandes pour gérer les groupes**

groupadd, groupmod et groupdel sont dans le dossier /usr/sbin/

**Création d'un groupe avec "groupadd"**

La commande **groupadd** permet d'ajouter un groupe.

**sudo groupadd g33**

La commande ajoute une ligne à la fin du fichier /etc/group

**Modification d'un groupe avec "groupmod"**

La commande **groupmod** permet de modifier les paramètres d'un groupe.

**Destruction d'un groupe avec "groupdel"**

La commande **groupdel** permet d'effacer un groupe.

**La commande "groups"**

La commande **groups** affiche l'appartenance des groupes d'un utilisateur

Affiche les groupes dont l'utilisateur actif est membre

**groups**

Affiche les groupes dont l'utilisateur u1 est membre

**sudo groups u1**

**La commande id**

La commande **id** affiche des informations sur le compte d'un utilisateur.

**id**

**id -g**

**id -gn**

**id -G**

**id -Gn**

**id u1**

**id u1 -g**

**id u1 -gn**

**id u1 -G**

**id u1 -Gn**

### id -g: Affiche le GID (Group ID) principal de l'utilisateur courant.

### id -gn: Affiche le nom du groupe principal de l'utilisateur courant.

### id -G: Affiche tous les GID (Group IDs) auxquels l'utilisateur courant appartient, séparés par des virgules.

### id -Gn: Affiche les noms de tous les groupes auxquels l'utilisateur courant appartient, séparés par des virgules.

### id u1 -g: Affiche le GID principal de l'utilisateur spécifié "u1".

### id u1 -gn: Affiche le nom du groupe principal de l'utilisateur spécifié "u1".

### id u1 -G: Affiche tous les GID auxquels l'utilisateur spécifié "u1" appartient, séparés par des virgules.

### id u1 -Gn: Affiche les noms de tous les groupes auxquels l'utilisateur spécifié "u1" appartient, séparés par des virgules.

**La commande "newgrp"**

La commande **newgrp** permet de changer de groupe principal pour la session.

Supposons que vous appartenez initialement au groupe **group1** et vous souhaitez basculer vers le groupe **group2**. Vous pouvez utiliser **newgrp** de la manière suivante :

newgrp group2

**Les fichiers importants pour la gestion des usagers et des groupes sont:**

* /etc/passwd contient la liste des comptes utilisateur
* /etc/group contient la liste des groupes
* /etc/shadow contient la liste des mots de passe cryptés

Commande pour obtenir des informations sur la structure du fichier /etc/passwd

**man 5 passwd**

Commande pour obtenir des informations sur la structure du fichier /etc/shadow

**man 5 shadow**

Commande pour obtenir des informations sur la structure du fichier /etc/group

**man 5 group**

**Le deuxième champ du fichier /etc/shadow contient le "mot de passe" crypté**

**:$y$j9T$dS** 🡺 le premier caractère est $ donc le champ contient un mot de passe

**:!$y$j9T$dS** 🡺 le compte est verrouillé

**:!:** 🡺 le mot de passe n'a pas encore été défini

**:\*:** 🡺 impossible de se connecter sur la station avec ce compte

**::** 🡺 aucun mot de passe ne sera demandé lors du login

**note 1: si le mot de passe débute par $y$ l’algorithme de hachage du mot de passe est yescrypt**

**L'algorithme yescrypt es utilisé par défaut avec Ubuntu depuis la version 22.04.**

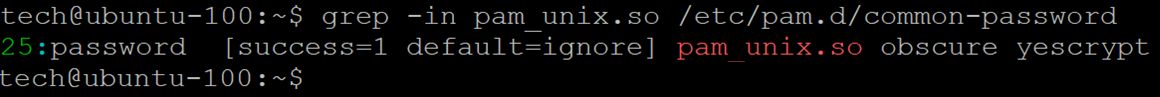
**L'algorithme yescrypt est conçu pour ralentir considérablement les attaques par force brute.**

**note 2: si le mot de passe débute par $6$ l’algorithme de hachage du mot de passe est SHA512**

**note 3: si le mot de passe débute par $5$ l’algorithme de hachage du mot de passe est SHA256**

**note 4: si le mot de passe débute par $1$ l’algorithme de hachage du mot de passe est MD5**

L'algorithme de hachage est spécifié dans le fichier **/etc/pam.d/common-password**



La ligne 25 du fichier montre que l'algorithme de hachage par défaut est yescrypt.

**24 # here are the per-package modules (the "Primary" block)**

**25 password [success=1 default=ignore] pam\_unix.so obscure yescrypt**

Pour changer l'algorithme de hachage, il faut modifier le contenu du fichier "**/etc/pam.d/common-password**".

Il est préférable de mettre la ligne 25 en commentaire et d'ajouter une nouvelle ligne pour spécifier le nouvel algorithme de hachage.

La ligne 25 est en commentaire.

La ligne 26 spécifie l'algorithme de hachage sha512.

**24 # here are the per-package modules (the "Primary" block)**

**25 # password [success=1 default=ignore] pam\_unix.so obscure yescrypt**

**26 password [success=1 default=ignore] pam\_unix.so obscure sha512**

La ligne 25 est en commentaire.

La ligne 26 est en commentaire.

La ligne 27 spécifie l'algorithme de hachage sha256.

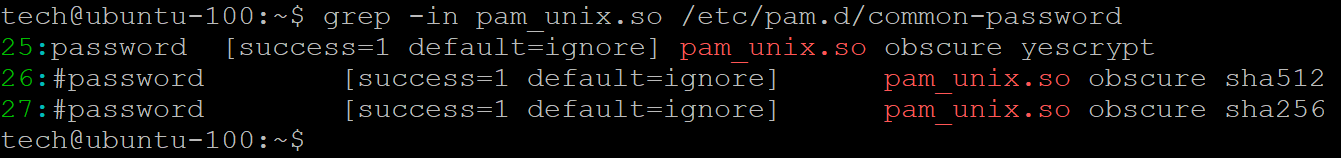
**24 # here are the per-package modules (the "Primary" block)**

**25 # password [success=1 default=ignore] pam\_unix.so obscure yescrypt**

**26 # password [success=1 default=ignore] pam\_unix.so obscure sha512**

**27 password [success=1 default=ignore] pam\_unix.so obscure sha256**

L'algorithme de hachage est yescrypt.



**La commande "sudo"**

La commande "**sudo**" permet d'exécuter une commande en tant qu'un autre utilisateur.

permet d'exécuter une commande en tant que "**root**"

**sudo passwd u1**

**sudo cat /etc/shadow**

permet d'ouvrir une session "**root**"

**sudo -i**

**La commande "passwd"**

Pour changer le mot de passe de l'utilisateur u1

**passwd u1**

Pour supprimer le mot de passe de l'utilisateur u1

**passwd -d u1**

Pour attribuer automatiquement un mot de passe à un utilisateur

**echo "nouveau\_mot\_de\_passe" | sudo passwd --stdin u1**

Pour verrouiller le compte d'un utilisateur

**passwd -l u1**

Pour déverrouiller le compte d'un utilisateur

**passwd -u u1**

**La commande "chage"**

Cette commande modifie les informations de validité d’un mot de passe.

Permet de forcer l'utilisateur u1 à changer son mot de passe au prochain login.

**chage -d 0 u1**

Affiche les informations sur les âges du compte u1.

**chage -l u1**

**La commande "newusers"**

En premier on crée la liste des usagers dans un fichier "**liste.usagers**".

**usager1:Secret1:1525:1525::/home/usager1:/bin/bash**

**usager2:Secret1:1526:1526::/home/usager2:/bin/bash**

**...**

Si le champ pour UID est vide, il est attribué automatiquement par le système.

Si le champ pour GID est vide, il est attribué automatiquement par le système.

note: la commande newusers va créer les utilisateurs et crypter le mot de passe

**sudo "newusers liste.usagers"**

**La commande "chpasswd"**

Voici la syntaxe générale pour modifier le mot de passe d'un utilisateur

**echo 'username:password' | sudo chpasswd**

La commande pour modifier le mot de passe de l'utilisateur u1

**echo 'u1:Secret1' | sudo chpasswd**

Si on veut modifier le mot de passe de plusieurs utilisateurs.

En premier on crée la liste des mots de passe dans un fichier "**liste.motdepasse**"**.**

Le fichier "**liste.motdepasse**" doit contenir le nom de l'utilisateur et son mot de passe en respectant la syntaxe suivante "**username:password**", une paire par ligne.

**usager1:MotDePasse1**

**usager2:MotDePasse2**

**...**

**cat liste.motdepasse | sudo chpasswd"**