**453---SYSTEME D'EXPLOITATION - e-learning - Séquence 18**

**Utilisateurs, groupes et droits – 1**

**Légende :**

Explications sur fond blanc

Exercice à accomplir sur fond rouge clair

Une ou plusieurs solutions possibles pour accomplir l’exercice sur fond vert clair

Héritier de UNIX, le système Linux a été édifié d’origine selon une approche de sécurité multi-utilisateur : Linux a donc toujours été un système de type « professionnel » et non de type « home ».

Linux intègre une base de données de comptes utilisateurs et de comptes groupes d’utilisateurs. Chaque compte est inscrit dans la base de données locale ou dans un annuaire réseau.

Chaque fichier (au sens large : fichier ordinaire, répertoire, etc.) est assorti de droits précisant les utilisateurs et les groupes d’utilisateurs qui sont habilités à y accéder, et de quelle façon.

Les services (applications système) sont associés à des comptes.

Le login d’un utilisateur détermine les droits de son shell, et par héritage, les droits des applications qu’il exécutera. Le root, lui, a tous les droits sur le système.

Chaque compte utilisateur est identifié par un nom (login) et un UID (User IDentification) numérique. La valeur 0 pour root. De 1 à un maximum (999) pour les services. Les valeurs supérieures au maximum pour les utilisateurs ordinaires. Chaque compte groupe est identifié par un nom et un GID (Group IDentification) numérique.

Un système Linux est absolument sensible à la casse ; par exemple, la commande : « ls » DOIT être tapée « ls », et NON « LS » ou « Ls » ! Il en est de même pour tout nom d’utilisateur, de groupe, de fichier, de répertoire, etc.

**Quelques commandes :**

SU(1)

NOM

su - Changer d'identifiant d'utilisateur ou devenir superutilisateur

SYNOPSIS

su [options] [nom\_utilisateur]

DESCRIPTION

La commande su permet de devenir un autre utilisateur pour la durée d'une session.

Invoqué sans nom d'utilisateur, le comportement par défaut de su est de devenir

superutilisateur. Le paramètre optionnel - permet d'obtenir un environnement

similaire à celui que l'utilisateur aurait obtenu lors d'une connexion directe.

ID(1)

NOM

id - Afficher les identifiants d'utilisateur et de groupe effectifs et réels

SYNOPSIS

id [OPTION]... [UTILISATEUR]

DESCRIPTION

Afficher les informations sur l'utilisateur et le groupe pour UTILISATEUR,

ou (si UTILISATEUR est omis) pour l'utilisateur courant.

GETENT(1)

NOM

getent - Récupérer des entrées depuis les bibliothèques NSS

SYNOPSIS

getent base\_de\_données [clé ...]

DESCRIPTION

La commande getent affiche les entrées des bases de données prises en charge par

les bibliothèques du Name Service Switch (NSS), qui sont configurées

dans /etc/nsswitch.conf. Si un ou plusieurs arguments clé sont fournis, alors seules

les entrées correspondantes aux clés fournies seront affichées. Sinon, si aucune clé

n'est fournie, toutes les entrées seront affichées (sauf si la base de données

ne permet pas l'énumération).

PWCK(8)

NOM

pwck - Vérifier l'intégrité des fichiers de mots de passe

SYNOPSIS

pwck [options] [passwd [ shadow ]]

DESCRIPTION

La commande pwck vérifie l'intégrité des informations du système concernant

les utilisateurs et leur mots de passe. Toutes les entrées des fichiers /etc/passwd

et /etc/shadow sont vérifiées afin de s'assurer qu'elles ont le bon format et

qu'elles contiennent des données valables dans chaque champ. Une confirmation

de l'utilisateur sera demandée pour détruire les entrées mal formatées

ou ayant d'autres erreurs non récupérables.

GRPCK(8)

NOM

grpck - Vérifier l'intégrité des fichiers d'administration des groupes

SYNOPSIS

grpck [options] [groupe [ shadow ]]

DESCRIPTION

La commande grpck vérifie l'intégrité des informations sur les groupes du

système. Toutes les entrées de /etc/group et /etc/gshadow sont vérifiées afin de

s'assurer qu'elles ont le bon format et qu'elles contiennent des données valables

dans chaque champ. Une confirmation de l'utilisateur sera demandée pour détruire

les entrées mal formatées ou ayant d'autres erreurs non récupérables.

GROUPADD(8)

NOM

groupadd - Créer un nouveau groupe

SYNOPSIS

groupadd [options] groupe

DESCRIPTION

La commande groupadd crée un nouveau compte de groupe en utilisant les

valeurs spécifiées sur la ligne de commande et les valeurs par défaut du système.

Le nouveau groupe sera inséré dans les fichiers du système selon les besoins.

GROUPMOD(8)

NOM

groupmod - Modifier la définition d'un groupe du système

SYNOPSIS

groupmod [options] groupe

DESCRIPTION

La commande groupmod modifie la définition du groupe spécifié en modifiant

l'entrée correspondante de la base de données des groupes.

GROUPDEL(8)

NOM

groupdel - Supprimer un groupe

SYNOPSIS

groupdel [options] groupe

DESCRIPTION

La commande groupdel modifie les fichiers d'administration des comptes du système,

en supprimant les entrées qui se réfèrent à groupe. Le groupe indiqué doit exister.

USERADD(8)

NOM

useradd - Créer un nouvel utilisateur ou modifier les informations par défaut

appliquées aux nouveaux utilisateurs

SYNOPSIS

useradd [options] LOGIN

useradd -D

useradd -D [options]

DESCRIPTION

useradd is a low level utility for adding users. On Debian, administrators should

usually use adduser(8) instead.

USERMOD(8)

NOM

usermod - Modifier un compte utilisateur

SYNOPSIS

usermod [options] LOGIN

DESCRIPTION

La commande usermod modifie les fichiers d'administration des comptes du

système selon les modifications qui ont été indiquées sur la ligne de commande.

USERDEL(8)

NOM

userdel - Supprimer un compte utilisateur et les fichiers associés

SYNOPSIS

userdel [options] LOGIN

DESCRIPTION

La commande userdel modifie les fichiers d'administration des comptes du système,

en supprimant les entrées qui se réfèrent à LOGIN. L'utilisateur nommé doit exister.

userdel is a low level utility for removing users. On Debian, administrators

should usually use deluser(8) instead.

PASSWD(1)

NOM

passwd - Modifier le mot de passe d'un utilisateur

SYNOPSIS

passwd [options] [LOGIN]

DESCRIPTION

La commande passwd modifie les mots de passe des comptes d'utilisateurs.

Un utilisateur normal ne peut changer que son propre mot de passe, alors que

le superutilisateur peut changer le mot de passe associé à n'importe quel compte.

passwd modifie également les dates de fin de validité du compte

ou du mot de passe associé.

CHPASSWD(8)

NOM

chpasswd - Mettre à jour des mots de passe par lot

SYNOPSIS

chpasswd [options]

DESCRIPTION

La commande chpasswd lit une liste de paires de noms d'utilisateurs et de mots

de passe depuis l'entrée standard et met en conséquence à jour les utilisateurs

existants. Chaque ligne est au format suivant : nom\_utilisateur:mot\_de\_passe

Par défaut, les mots de passe doivent être fournis en clair, et sont chiffrés par

chpasswd. L'âge du mot de passe est également mis à jour, s'il est présent.

**Quelques fichiers :**

PASSWD(5)

NOM

passwd - Fichier des mots de passe (en fait : d’informations sur les comptes utilisateurs)

DESCRIPTION

/etc/passwd contient différentes informations sur les comptes utilisateurs.

Ces informations consistent en sept champs séparés par des deux-points (« : ») :

· nom de connexion de l'utilisateur (« login »)

· un mot de passe chiffré optionnel

· l'identifiant numérique de l'utilisateur (UID)

· l'identifiant numérique du groupe de l'utilisateur (GID)

· le nom complet de l'utilisateur ou un champ de commentaires

· le répertoire personnel de l'utilisateur

· l'interpréteur de commandes de l'utilisateur (optionnel)

Le champ du mot de passe chiffré peut être vide. Dans ce cas,

aucun mot de passe n'est nécessaire pour s'authentifier avec le compte donné.

Cependant, certaines applications qui lisent le fichier /etc/passwd peuvent décider

de ne donner aucun accès si le mot de passe est vide. Si le mot de passe est un « x »

minuscule, alors le mot de passe chiffré se trouve dans le fichier shadow(5) ;

il doit y avoir une ligne correspondante dans le fichier shadow,

sinon le compte de l'utilisateur n'est pas valide.

SHADOW(5)

NOM

shadow - Fichier des mots de passe cachés

DESCRIPTION

shadow est un fichier qui contient les informations cachées concernant les mots de

passe des utilisateurs et leurs dates de validité. Il contient 9 champs :

nom de connexion de l'utilisateur (« login »)

mot de passe chiffré (ce champ peut être vide ; "!" indique que le mot de passe n'a

pas encore été configuré et "\*" que le compte a été désactivé)

date (nombre de jours depuis le 1er janvier 1970) du dernier changement de mot de passe

nombre de jours que l'utilisateur devra attendre avant de pouvoir changer de mot de passe

nombre de jours après lequel l'utilisateur devra changer de mot de passe

nombre de jours pendant lesquels l'utilisateur sera averti avant expiration du mot de passe

nombre de jours d'inactivité du mot de passe

date (nombre de jours depuis le 1er janvier 1970) de fin de validité du compte

champ réservé pour une utilisation future

GROUP(5)

NOM

group - Fichier des groupes d'utilisateurs

DESCRIPTION

Le fichier /etc/group est un fichier texte qui définit les groupes du système. Il y a une

entrée par ligne, au format suivant : nom\_du\_groupe:mot\_de\_passe:GID:liste\_utilisateurs

Les champs sont les suivants :

nom\_du\_groupe (nom du groupe)

mot\_de\_passe (mot de passe chiffré du groupe ; ce champ peut être vide)

GID (identifiant numérique du groupe)

liste\_utilisateurs (liste de nom d'utilisateurs membres du groupe, séparés par des virgules)

GSHADOW(5)

NOM

gshadow - informations cachées sur les groupes

DESCRIPTION

/etc/gshadow contient les informations cachées sur les groupes.

Ce fichier ne doit pas être accessible en lecture par les utilisateurs normaux afin de

maintenir la sécurité des mots de passe, en particulier pour prévenir les attaques

par dictionnaires. Il contient les champs suivants :

nom du groupe

mot de passe chiffré (ou « ! » ou « \* » ; ce champ peut être vide)

administrateurs (liste d'utilisateurs, séparés par des virgules)

membres (liste d'utilisateurs, séparés par des virgules ; la même que dans /etc/group)

NSSWITCH.CONF(5)

NOM

nsswitch.conf - Fichier de configuration du service de noms (« Name Service Switch »)

DESCRIPTION

Le fichier de configuration du service de noms (« Name Service Switch » ou NSS),

/etc/nsswitch.conf, est utilisé par la bibliothèque C de GNU pour déterminer les

sources desquelles obtenir les renseignements de service de noms en fonction

des catégories, et dans quel ordre. Chaque catégorie de renseignements est identifiée

par un nom de base de données.

**LABORATOIRE – Utilisateurs, groupes et droits – 1**

**Les exercices des séquences 18 à 21 s’enchaînent.**

**Il faut donc les accomplir dans l’ordre prévu.**

**Dans la distribution Debian GNU/Linux :**

Connectez-vous dans un terminal

Affichez le manuel de la commande su

man su

Dans le même terminal, connectez-vous sous le compte « root », c’est-à-dire le superutilisateur (Password du root)

su -

Vous avez maintenant tous les droits d’administration. Vous avez la responsabilité d’en faire usage avec prudence !

Affichez le manuel de la commande id

man id

Avec id, vérifiez si les comptes utilisateurs bin, daemon, UserX, UserY et UserZ existent, et, pour chacun, si c’est le cas, quel est son uid, son gid et ses groupes ?

id bin

id daemon

id UserX

id UserY

id UserZ

Avec less, affichez les comptes utilisateurs

less /etc/passwd

Avec less, affichez les comptes groupes

less /etc/group

Avec less, affichez les mots de passe locaux cryptés et leur durée de vie

less /etc/shadow

Avec less, affichez les informations sécurisées sur les groupes

less /etc/gshadow

Avec less, affichez les annuaires locaux ou réseaux où sont recherchés les comptes

less /etc/nsswitch.conf

Affichez le manuel des commandes getent, pwck et grpck

man getent

man pwck

man grpck

Avec getent, affichez les données des annuaires passwd, group et shadow

getent passwd

getent group

getent shadow

Affichez le manuel des commandes groupadd, groupmod et groupdel

man groupadd

man groupmod

man groupdel

Créez les groupes GroupA, GroupB et GroupC

groupadd GroupA

groupadd GroupB

groupadd GroupC

Visualisez les nouveaux comptes groupes

getent group

Affichez le manuel des commandes useradd, usermod et userdel

man useradd

man usermod

man userdel

Créez le compte utilisateur Ernest, ainsi que son répertoire de connexion

useradd -m Ernest

Visualisez le compte Ernest parmi tous les comptes utilisateurs

getent passwd

Affichez le manuel de la commande find

man find

Recherchez le répertoire de connexion de l’utilisateur Ernest

find / -name "Ernest" -print

Supprimez le compte utilisateur Ernest, ainsi que son répertoire de connexion

userdel -r Ernest

Créez le compte utilisateur UserX, uid = 1011, appartenant au groupe GroupA (comme groupe principal) et aux groupes GroupB et GroupC (comme groupes secondaires), commentaire = « Utilisateur X », ainsi que son répertoire de connexion

useradd -u 1011 -g GroupA -G GroupB,GroupC -c 'Utilisateur X' -m UserX

Créez le compte utilisateur UserY, uid = 1012, appartenant au groupe GroupA (comme groupe principal) et au groupe GroupC (comme groupe secondaire), commentaire = « Utilisateur Y », ainsi que son répertoire de connexion

useradd -u 1012 -g GroupA -G GroupC -c 'Utilisateur Y' -m UserY

Créez le compte utilisateur UserZ, uid = 1013, appartenant au groupe GroupB, commentaire = « Utilisateur Z », ainsi que son répertoire de connexion

useradd -u 1013 -g GroupB -c 'Utilisateur Z' -m UserZ

Affichez l’identification et les groupes des comptes UserX, UserY et UserZ

id UserX

id UserY

id UserZ

Visualisez les nouveaux comptes utilisateurs

getent passwd

Visualisez à présent les membres des groupes GroupA, GroupB et GroupC

getent group

Affichez le manuel des commandes passwd et chpasswd

man passwd

man chpasswd

Mettez les mots : « userx » comme mot de passe à l’utilisateur UserX, « usery » comme mot de passe à l’utilisateur UserY et « userz » comme mot de passe à l’utilisateur UserZ

passwd UserX

userx

userx

passwd UserY

usery

usery

passwd UserZ

userz

userz

Déconnectez-vous du compte root

exit

Déconnectez-vous du terminal

exit