**Exercice  
Gestion des utilisateurs et des groupes**

**Objectif**

Dans cet exercice, vous vous familiariserez avec la gestion des utilisateurs et les groupes sur un système Linux.

**Rappel** …  
On peut toujours obtenir de l’aide sur une commande à l’aide des modules d’aide.  
Comme exemple, pour obtenir de l’aide sur la commande **uname** …   
**>> uname --help**

**Remarque** …  
Pour les exercices suivants, l’utilisateur ayant ouvert une session est **tux**.  
L’utilisateur **tux** est également membre du groupe **sudo**.

**Étape 01**Le fichier **/etc/passwd** contient les informations des comptes d'utilisateurs, à l'exception des informations relatives au mot de passe.

Affichez le contenu de ce fichier …  
**>> head /etc/passwd**

**Étape 02**Affichez les informations du compte avec lequel vous avez ouvert un interpréteur de commande (*shell*) …  
**>> whoami  
>> grep $USER /etc/passwd**

**Étape 03**Rappelez-vous que le cinquième champ contient les "Commentaires" sur l'utilisateur.   
Modifiez ce champ en exécutant la commande chfn …  
**>> chfn  
Mot de passe :  
Modification des informations relatives à l'utilisateur tux  
Entrez la nouvelle valeur ou « Entrée » pour conserver la valeur proposée  
 Nom complet :   
 N° de bureau []:   
 Téléphone professionnel []:   
 Téléphone personnel []:**

**Étape 04**Vérifiez ces modifications en affichant les informations pour votre compte …  
**>> grep $USER /etc/passwd**

**Étape 05**Le fichier **/etc/shadow** contient des informations relatives aux mots de passe et aux politiques de sécurité des mots de passe.

**Remarque** …  
Les utilisateurs réguliers ne peuvent pas afficher le contenu de ce fichier.

Pour vérifier que le fichier n'est pas visible par un compte non privilégié …  
**>> cat /etc/shadow**

**Étape 06**Pour afficher le contenu du fichier **/etc/shadow**, précédez la commande précédente de **sudo** pour l'exécuter avec les privilèges de **root**.   
Lorsque vous y êtes invité, indiquez le mot de passe de votre compte utilisateur …  
**>> sudo cat /etc/shadow**

**Étape 07**Affichez les informations propres à votre compte …  
**>> sudo grep $USER /etc/shadow  
tux:$y$j9T$m7fx0vKc07LghNdLEWqx1.$ZVkO3JMQq4QlvR6WTdMbM7.dvlQ2PjGlMXvIZm2URX/:19415:0:99999:7:::**

**Étape 08**Créez un compte utilisateur nommé squiddly …  
**>> sudo useradd --shell /bin/bash --create-home squiddly**ou  
**>> sudo useradd -s /bin/bash -m squiddly**

Notez que la commande useradd nécessite elle aussi une élévation de privilèges en tant que **root** puisqu'elle modifie les fichiers **/etc/passwd** et **/etc/shadow**.   
Utilisez le commutateur **--shell** (forme courte **-s**) pour définir l’interpréteur de commande (de connexion)   
et **--create-home** (forme courte **-m**) pour que la commande useradd crée automatiquement le répertoire personnel de l'utilisateur.

**Étape 09**Constatez que la création du compte squiddly se traduit par l'ajout d'une ligne à la fin du fichier **/etc/passwd** …  
**>> sudo grep squiddly /etc/passwd**

**Étape 10**On remarque la présence d'un nouveau répertoire au nom de squiddly dans le répertoire /home …  
**>> ls /home/**

**Étape 11**Pour obtenir des informations sur l'utilisateur **squiddly** on peut lancer la commande **id squiddly** qui nous retourne son UID, son GID (groupe primaire) ainsi que la liste des groupes dans lequel l'utilisateur squiddly est membre …  
**>> id squiddly**

**Étape 12**Notez qu'au départ, le compte de squiddly n'a pas de mot de passe …  
**>> sudo grep squiddly /etc/shadow**

Le caractère **!** dans le deuxième champ indique que le compte n'a pas de mot de passe   
(à ne pas confondre avec un mot de passe vide).   
En conséquence, l'utilisateur ne peut pas se connecter à son compte.

**Étape 13**Pour attribuer un mot de passe pour l’utilisateur squiddly …  
**>> sudo passwd squiddly**

**Étape 14**Pour constater qu'un nouveau mot de passe a été assigné à l'utilisateur …  
**>> sudo grep squiddly /etc/shadow  
squiddly:$y$j9T$pUAXdLvYywTukqhFcAN2B1$0T1JS.lYxJiWOsEVjysPoZZCp6ANS8lWD4/SOz7fl68:19442:0:99999:7:::**

Notez que le deuxième champ ne contient pas le mot de passe en texte clair, mais plutôt une version hachée avec l’algorithme yesscript (**$y**) ou SHA512 (**$6**) – selon votre distribution de ce mot de passe.

**Étape 15**À la suite du changement de mot de passe, il est possible d'ouvrir un interpréteur de commande en tant que squiddly. Pour ce faire, lancez la commande su - squiddly et saisissez le mot de passe demandé …  
**>> su – squiddly  
Mot de passe :**

**>> whoami  
>> exit**

**Étape 16**Le fichier **/etc/group** contient des informations sur les groupes du système.   
Pour afficher les premières lignes du fichier **/etc/group** …  
**>> tail /etc/group**

**Étape 18**Pour voir de quel groupe l'utilisateur actuel est membre …  
**>> groups**

Le premier groupe affiché est le groupe primaire (ou principal) de l'utilisateur.

**Étape 19**Pour créer un nouveau groupe nommé informatique …  
**>> sudo groupadd informatique**

Pour constater que le groupe a bien été créé …  
**>> grep informatique /etc/group**

**Étape 20**Le groupe informatique ne contient à l'heure actuelle aucun utilisateur.   
Pour ajouter votre utilisateur actuel et squiddly au groupe nommé informatique …  
**>> sudo usermod -aG informatique$USER**  
**>> sudo usermod -aG informatique squiddly**

**Étape 21**Affichez maintenant la ligne du groupe informatique dans le fichier /etc/groups.   
Constatez la présence des utilisateurs tux et squiddly …  
**>> grep informatique /etc/group**

**Étape 22**Utilisez la commande **su - squiddly** pour ouvrir un interpréteur de commande en tant que **squiddly**.  
Pour constater l'appartenance de l'utilisateur squiddly aux groupes squiddly et informatique …  
**>> groups**

**Étape 23**Toujours dans un shell ouvert en tant que squiddly, lancez la commande **sudo --list** (forme courte **-l**).   
Cette commande permet d'afficher les commandes pour lesquelles **squiddly** est autorisé à exécuter en tant que **root** …  
**>> sudo --list**

L'utilisateur squiddly ne peut pas utiliser sudo. suiddly n'est pas autorisé à utiliser sudo.

**Étape 24**Pour que **squiddly** puisse lancer des commandes en tant que **super-utilisateur**, en tant que **root**, ajoutez son compte utilisateur au   
groupe **sudo** …  
**>> sudo usermod squiddly --append --groups sudo**ou  
**>> sudo usermod squiddly -aG sudo**

Pour que le changement aux groupes soit effectif pour l'utilisateur, il faut que ce dernier ferme sa session actuelle et ouvre une nouvelle session.

**Étape 25**Fermez la session de squiddly et ouvrez un nouvel interpréteur de commande.   
Lancez la commande groups et constatez que squiddly fait maintenant partie du groupe sudo …  
**>> groups**

**Étape 26**Essayer de lancer une commande en tant que root en la précédant de sudo.   
Lorsque demandé, fournissez le mot de passe de l'utilisateur squiddly  
**>> sudo apt update**

squidly peut maintenant lancer des commandes en tant que root.

**Étape 27**Nous allons maintenant verrouiller le compte de squiddly pour l'empêcher de se connecter au système.   
Pour ce faire, lancez la commande **sudo passwd --lock** **squiddly** (forme courte **-l**) …  
**>> sudo passwd --lock squiddly**  
ou **>> sudo passwd -l squiddly  
passwd : expiration du mot de passe modifiée.  
*passwd: password expiry information changed.***

**Étape 28**Affichez la ligne correspondante à l'utilisateur squiddly dans le fichier **/etc/shadow**.   
On constate la présence du caractère **!** au début de la deuxième colonne qui signifie que le compte est verrouillé …  
**>> sudo grep squiddly /etc/shadow  
squiddly:!$y$j9T$pUAXdLvYywTukqhFcAN2B1$0T1JS.lYxJiWOsEVjysPoZZCp6ANS8lWD4/SOz7fl68:19442:0:99999:7:::**

**Étape 29**Tentez d'ouvrir un interpréteur de commande en tant que squiddly …  
**>> su - squiddly  
Mot de passe :  
su: Échec de l’authentification**

On remarque que le compte est inaccessible, même en saisissant le bon mot de passe.

**Étape 30**Pour réactiver le compte, lancez la commande **sudo passwd --unlock squiddly** (forme courte **-u**).   
L'ancien mot de passe est de nouveau fonctionnel.   
Affichez ensuite la ligne correspondante à l'utilisateur squiddly dans le fichier **/etc/shadow** et constatez que le   
caractère **!** a été supprimé de la deuxième colonne …  
**>> sudo passwd --unlock squiddly**  
ou **>> sudo passwd -u squiddly  
passwd : expiration du mot de passe modifiée.  
*passwd: password expiry information changed.***

**>> sudo grep squiddly /etc/shadow  
squiddly:$y$j9T$pUAXdLvYywTukqhFcAN2B1$0T1JS.lYxJiWOsEVjysPoZZCp6ANS8lWD4/SOz7fl68:19442:0:99999:7:::**

L'utilisateur squiddly peut se connecter à nouveau au système d'exploitation.

**Questions de révision et d'expérimentation**

**Question 01**Ouvrez un interpréteur de commande (*shell*).

* Quel est le nom d'utilisateur avec lequel vous avez ouvert un interpréteur de commande sur le système ?  
  **--------------**
* Quel est son UID ?  
   **--------------**
* Quel est son groupe principal (GID) ?  
  **--------------**
* Quels sont les groupes secondaires auxquels appartient votre utilisateur ?  
  **--------------**

**Question 02**

* Quel est l'UID et le GID du compte root ?  
  **--------------**
* Le compte root a-t-il un mot passe ?   
  Comment le savez-vous ?  
  **-------------- --------------**

**Question 03**

Créez un nouveau compte nommé **wally**.   
Utilisez les options appropriées de la commande **useradd** pour lui assigner l’interpréteur de commande de connexion (*shell*) **/bin/bash** et créer automatiquement son répertoire personnel.

* Quelle commande avez-vous saisie ?  
  **--------------**
* Quel est le **UID** et le **GID** de l'utilisateur **wally** ?  
  **--------------**
* Affectez le mot de passe **linux** à l'utilisateur **wally**.   
  Quelle commande avez-vous lancée ?  
  **--------------**
* Ouvrez un interpréteur de commande en tant que **wally** dans votre terminal.   
  Quelle commande avez-vous lancée ?  
  **--------------**

**Question 04**

* Dans un terminal ouvert en tant que **wally**, tentez de lancer une commande avec **sudo**.   
  Que se passe-t-il ?  
  **--------------**
* Quel message a été ajouté au journal **/var/log/auth.log** concernant cet événement?   
  Utilisez la commande grep pour vous aider à le trouver.  
  **-------------- --------------**

**Question 05**La commande **usermod** offre une option pour modifier l’interpréteur de commande de connexion d'un utilisateur.  
Modifiez l’interpréteur de commande de connexion de **wally** pour **/usr/sbin/nologin**.

* Quelle commande avez-vous saisie ?  
  **--------------**
* Quel changement a été apporté au fichier **/etc/passwd** ?  
  **--------------**
* Que se passe-t-il si vous tentez d'ouvrir un interpréteur de commande en tant que **wally**.   
  Testez-le avec la commande **su - wally**.  
  **--------------**
* Supprimez l'utilisateur wally.  
  **--------------**