EC2LT
ECOLE CENTRALE DES LOGICIELS LIBRES
ET DE TELECOMMUNICATIONS

Première ACTIVITE

Gestion des utilisateurs et Groupes

Consignes :

Lisez attentivement la première partie avant d'attaquer les exercices.

Chacun doit rendre un rapport qui est composé d'une introduction qui décrit le rôle d'administrateur système. Le corps du rapport sera les captures des résultats des commandes, de vos remarques et vos constats. Vous terminerez le rapport avec une conclusion.

Aly TIRERA, ingénieur Télécoms et Réseaux, Certifié Linux LPIC-1 & LPIC-2

1. Objectif de l'activité

Un administrateur systèmes et réseaux doit être capable de créer des utilisateurs, de les organiser sous forme de groupe selon l'organisation de l'entreprise et de gérer la mise à jour des mots de passe.

A l'issue de cette activité l'apprenant sera capable de :

- Savoir les différents fichiers impactés lors de la création, de la suppression et de la mise à jour d'un mot de passe ;
- Créer des utilisateurs et des groupes utilisateurs ;
- Gérer les mots de passe des utilisateurs :
  - Verrouiller ou de déverrouiller un compte utilisateur ;
  - Bloquer ou débloquer un compte utilisateur ;
  - Donner une date d'expiration du mot de passe d'un compte utilisateur ;
  - Définir un nombre de jours minimum avant que l'utilisateur puisse modifier son mot de passe ;

2. Les fichiers impactés

Les commandes suivantes **adduser, useradd, userdel, groupadd, groupdel, passwd, gpasswd,** sont utilisées pour la gestion des utilisateurs. Lorsque ces commandes sont exécutées, elles ajoutent ou suppriment des informations concernant un compte utilisateur parmi les fichiers suivants :

- **/etc/passwd** : contient la liste des utilisateurs
- **/etc/group** : contient la liste des groupes et les utilisateurs membres d'un groupe donnée
- **/etc/shadow** : contient les informations concernant le mot de passe des utilisateurs

Commande	Options	Description
adduser		Ajoute un nouvel utilisateur de façon interactive
useradd	**-u**	Spécifier manuellement le UID du compte
	-g	Spécifier le groupe par défaut
	-G	Spécifier les groupes secondaires
	-c	Spécifier un commentaire
	-e	Spécifier une date d'expiration de ce compte
	-s	Indiquer le shell de connexion de l'utilisateur
	-d	Spécifier le répertoire personnel
	-m	Crée le dossier personnel s'il n'est pas créé
	-k	Spécifier le répertoire squelette, qui contient les fichiers et répertoires qui seront copiés dans le répertoire personnel de l'utilisateur, quand le répertoire personnel est créé par la commande useradd.

userdel		Supprime l'utilisateur sans supprimer son répertoire personnel

	--remove-home	Supprime l'utilisateur ainsi que son répertoire personnel
passwd	**-d**	Supprime le mot de passe (le rend vide) d'un utilisateur.
	-e	Annule immédiatement la validité du mot de passe d'un compte. Ceci force un utilisateur à changer son mot de passe lors de sa prochaine connexion.
	-i	Permet de désactiver un compte un certain nombre de jours après que son mot de passe soit arrivé en fin de validité
	-l	Verrouille le compte spécifié. Un utilisateur avec un mot de passe verrouillé n'est pas autorisé à changer son mot de passe.
	-n	Définit le nombre minimum de jours entre chaque changement de mot de passe à MIN_JOURS. Une valeur égale à zéro dans ce champ indique que l'utilisateur peut changer son mot de passe lorsqu'il le souhaite.
	-u	Déverrouille le mot de passe du compte indiqué.
	-w	Fixe le nombre de jours avant que le changement de mot de passe ne soit obligatoire. DUREE_AVERTISSEMENT est le nombre de jours précédant la fin de validité du mot de passe, et durant lesquels l'utilisateur sera averti que son mot de passe est sur le point d'arriver en fin de validité.
	-x	Fixe le nombre maximum de jours pendant lesquels un mot de passe reste valable. Après MAX_JOURS, le mot de passe devra être obligatoirement modifié.
addgroup *ou* ***groupadd***	Ajout un nouveau groupe utilisateur donné comme argument à l'une des commandes	
groupdel *ou* ***delgroup***	Supprime un groupe utilisateur donné comme argument à l'une des commandes	
gpasswd	Permet d'administrer les groupes créés par **addgroup** ou **groupadd** en intégrant, retirant des utilisateurs aux groupes ou en nommant certains comme administrateur du groupe.	
	-a	Ajoute un utilisateur d'un groupe
	-d	Retire un utilisateur d'un groupe
	-A	Nomme utilisateur comme administrateur d'un groupe
	-M	Nomme utilisateur comme membre d'un groupe

Exercice 1 : Gestion des utilisateurs et groupes utilisateurs

Vous êtes recrutés en tant qu'administrateur d'une d'entreprise qui dispose 3 départements qui sont **cisco**, **linux** et **windows.** Votre mission consiste a organisé et administré les comptes utilisateurs des trois départements. Les utilisateurs d'un même département forment un groupe utilisateurs.

Pour se faire on procède comme suit :

1. Créer un répertoire nommé **/home/entreprise**1
2. Créer pour chaque département un répertoire portant le nom du département comme suit **:**
   a. **mkdir /home/entreprise1/cisco**
   b. **mkdir /home/entreprise1/linux**
   c. **mkdir /home/entreprise1/windows**
3. Créer les groupes principaux suivants **cisco**, **linux** et **windows** en exécutant les commandes suivantes :
   sudo addgroup sidi rama salif
   sudo addgroup ansou aminata tatarose
   sudo addgroup abdou modou simon
4. Créer les comptes utilisateurs suivants :
   - Pour le département cisco on a **sidi, rama, salif,** utilisez la commande suivante pour leur créer des comptes :
     sudo useradd –u 2010 -g sidi -s /bin/bash -m -d /home/entreprise1/cisco/sidi sidi
     sudo userad d –u 2011 -g rama -s /bin/bash -m -d /home/entreprise1/cisco/rama rama
     sudo useradd –u 2012 -g salif -s /bin/bash -m -d /home/entreprise1/cisco/salif salif

   - Pour le département linux on a ansou, aminata, tatarose utilisez la commande suivante pour leur créer des comptes :

     sudo useradd –u 2013 -g ansou -s /bin/bash -m -d /home/entreprise1/linux/ansou ansou
     sudo useradd –u 2014 -g aminata **-s /bin/bash -m -d /home/entreprise1/linux/**aminata aminata
     sudo useradd –u 2015 -g tatarose **-s /bin/bash -m -d /home/entreprise1/linux/**tatarose tatarose

   - Pour le département windows on a abdou, modou, simon utilisez la commande suivante pour leur créer des comptes :
     sudo useradd –u 2016 -g abdou **-s /bin/bash -m -d /home/entreprise1/windows/**abdou abdou
     sudo useradd –u 2017 -g modou **-s /bin/bash -m -d /home/entreprise1/windows/**modou modou
     sudo useradd –u 2018 -g simon **-s /bin/bash -m -d /home/entreprise1/windows/**simon simon
5. Utilisez la commande **passwd** pour donner un mot de passe à tous les utilisateurs des différents départements avec la commande suivante : **passwd nom_utilisateur**
6. Créer les groupes secondaires suivants cisco, linux, windows avec la commande suivante :
   sudo addgroup cisco linux windows
7. Utilisez la commande **gpasswd** pour intégrer les utilisateurs de chaque département dans leur groupe respectif avec l'une des commandes suivantes :
   sudo gpasswd -a nom_utilisateur nom_groupe
   ou
   sudo gpasswd -M nom_utilisateur nom_groupe

8. Nommez les utilisateurs suivants sidi, ansou et abdou administrateurs de leur groupe respectif avec la commande suivante : **gpasswd -A nom_utilisateur nom_groupe**
9. Le département cisco recrute un stagiaire on vous de lui créer un compte nommé stagiaire en exécutant la commande suivante :

   sudo addgroup stagiaire

   sudo useradd –u 2020 -g stagiaire **-s /bin/bash -m -d /home/entreprise1/windows/**stagiaire stagiaire

10. Donnez un mot de passe au compte stagiaire avec la commande **passwd**
11. L'utilisateur rama est membre du groupe cisco exécutez la commande suivante pour vérifier **sudo id rama**
12. Connectez vous avec le compte de rama avec la commande suivante :
    su - rama
13. Une fois que vous êtes connectés essayer d'ajouter le compte **stagiaire** au groupe cisco avec la commande suivante :
    gpasswd -a stagiaire cisco
14. Déconnectez du compte de rama avec la suivante **: exit**
15. Connectez vous avec le compte de sidi avec la commande suivante **: su – sidi**
16. Tentez d'ajouter le compte **stagiaire** au groupe cisco avec la commande suivante :
    gpasswd -a stagiaire cisco

    Pourquoi avec rama n'a pas pu intégrer le compte stagiaire au groupe cisco (étape 13) ?

17. Retirez le compte modou du groupe windows avec la commande suivante :
    sudo gpasswd -d modou windows
18. Supprimez le compte **stagiaire** ainsi que son répertoire personnel avec la commande suivante :
    sudo userdel -r stagiaire
19. Supprimez le compte **salif** ainsi que son répertoire personnel avec la commande suivante :
    sudo deluser --remove-home salif

Exercice 2 : Gestion de mot de passe des comptes utilisateurs

Le fichier **/etc/shadow** accompagne le fichier **/etc/passwd**. C'est là qu'est stocké, entre autres, le mot de passe crypté des utilisateurs. Pour être plus précis il contient toutes les informations sur le mot de passe et sa validité dans le temps. Chaque ligne est composée de 9 champs séparés par des **: :** comme le montre la capture ci-dessous :

```
tirera:$6$.GsBELKR$DKNKJLpRaK9JBZYTQAhIw/5MmT2GHyo2WABklTgd9i:18277:0:99999:7:::
```

Description des différents champs :

1. Champ 1 : correspond au login de l'utilisateur.
2. Champ 2 : correspond au mot de passé crypté.
3. Champ 3 : correspond au nombre de jours depuis le 1er janvier 1970 du dernier changement de mot de passe.
4. Champ 4 : correspond au nombre de jours avant lesquels le mot de passe ne peut pas être changé 0 : il peut être changé n'importe quand).
5. Champ 5 : correspond au nombre de jours après lesquels le mot de passe doit être changé.
6. Champ 6 : correspond au nombre de jours avant l'expiration du mot de passe durant lesquels l'utilisateur doit être prévenu.
7. Champ 7 : correspond au nombre de jours après l'expiration du mot de passe après lesquels le compte est désactivé.
8. Champs 8 : correspond au nombre de jours depuis le 1er janvier 1970 à partir du moment où le compte a été désactivé.
9. Champ 9 : réservé.

NB :

Le fichier /etc/shadow appartient à root et c'est lui seul qui modifie le contenu de ce fichier comme le montre la figure ci-après :

```
root@tirera-PC:~# ls -l /etc/shadow
-rw-r----- 1 root shadow 1924 awr  4 22:15 /etc/shadow
root@tirera-PC:~#
```

1. On avait un stagiaire au niveau du département cisco, le stage est terminé on demande de désactiver ou de verrouiller le compte stagiaire.

a. Avant de verrouiller le compte faisons un tour dans le fichier /etc/shadow pour voir les informations du mot de passe avec la commande suivante :

sudo grep stagiaire /etc/shadow

b. Verrouillez le compte stagiaire avec la commande suivante :

sudo passwd -l stagiaire

c. Reprenez la commande **sudo grep stagiaire /etc/shadow** et comparez-le avec le résultat de la question **a.**

d. Quel constat avez-vous faites après avoir comparé ces deux résultats (questions a et c) ?

e. Selon votre constat est-il possible de verrouiller un compte sans utiliser la commande passwd ?

2. Essayez d'ouvrir une session avec le compte stagiaire commande suivante : **su - stagiaire** et donnez votre remarque
3. Déverrouillez le compte stagiaire en utilisant la commande suivante : **sudo passwd -u stagiaire**
4. Supprimer le mot de passe du compte stagiaire avec la commande suivante :

sudo passwd -d stagiaire

5. Regarder la ligne stagiaire du fichier **/etc/shadow** avec la commande ci-dessous et donner votre constat : **sudo grep stagiaire /etc/shadow**
6. Pour de mesure de sécurité il est recommandé de changer de mot de passe très souvent donc on va définir une date par exemple on va obliger stagiaire de changer son mot de passe dans 20 jours avec la commande suivante : **sudo passwd -x 20 stagiaire**
7. Regarder la ligne stagiaire du fichier **/etc/shadow** avec la commande ci-dessous et donner votre constat : **sudo grep stagiaire /etc/shadow**
8. On vient de spécifie que le mot de passwd du compte stagiaire doit être changé dans **20 jours** il est nécessaire de lui faire un rappel d'une semaine avant l'expiration du mot de passe avec la commande suivante : **sudo passwd -w 7 stagiaire**
9. Regarder la ligne stagiaire du fichier **/etc/shadow** avec la commande ci-dessous et donner votre constat : **sudo grep stagiaire /etc/shadow**
10. Certe il est très important de changer son mot de passe très souvent mais il ne faut pas trop abuser de ça pour changer son mot de passe tous les jours. On peut définir le nombre de jours à attendre pour pouvoir à nouveau changer de mot de passe. Par exemple si vous changez votre

mot de passe aujourd'hui vous devez attendre 30 jours pour être autorisé à modifier de mot de passe avec la commande suivante : **sudo passwd -n 30 stagiaire**

11. Regarder la ligne stagiaire du fichier **/etc/shadow** avec la commande ci-dessous et donner votre constat : **sudo grep stagiaire /etc/shadow**
12. Connectez vous avec le compte de stagiaire avec la commande suivante : **su – stagiaire**
13. Essayez de changer le mot de passe du compte stagiaire avec la commande suivante : **passwd**
14. Avez-vous pu changer le mot de passe ?
15. Quel est le message d'erreur ?