Evaluation Born2beRoot

Vérifiez que le service UFW et SSH est démarré

```
sudo systemctl status ssh ufw
```

Vérifiez que le système d'exploitation choisi est Debian ou CentOS

```
uname -v
```

`uname` est une commande qui affiche les information sur le système. L'option `-v` affiche la version du noyau

Vérifiez que l'user appartient aux groupes 'sudo' et 'user42'.

Vérifier tous les groups auxquels appartient votre user ou un user donné:

```
id
id [user-name]
```

ou

```
groups
groups [user-name]
```

Vérifier si votre user appartient à un groupe spécifique (p.ex. groupe `user42`, `sudo`):

```
getent group [nom-group]
```

Créer un nouveau user et configurer de suite le mot de passe:

```
sudo adduser [nom-user]
```

ou

```
sudo useradd [user-name]
sudo passwd [user-name]
```

L'élève évalué doit maintenant vous expliquer comment il a pu mettre en place les règles demandées dans le sujet sur sa machine virtuelle. Normalement il doit y avoir un ou deux fichiers modifiés.

Réponse:

Le premier fichier modifié est `/etc/pam.d/common-password`

Tout d'abord le paquet `libpam-pwquality` a été installé.

C'est un paquet contient des outils qui permettent de paramétrer le refus des mots de passe trop faibles pour les sessions root et utilisateurs. Ils permettent aussi de les évaluer en fonction de leur caractère et de les comparer à un dictionnaire des mots de passe trop courants.

Le paquet crée le module `pam_quality.so` dans le fichier de configuration PAM `/etc/pam.d/common-password`

Pour visualiser les options ajoutées au fichier `/etc/pam.d/common-password` en mode lecture (sans droits de modifications)

```
nano /etc/pam.d/common-password
```

ou

```
cd /etc/pam.d/
grep 'pwquality' *
```

Deuxième fichier modifié: `/etc/login.defs`.

C'est le fichier qui contient des configuration pour des commandes liés aux utilisateurs comme useradd, usermod, userdel, groupadd et autres. Ce fichier permet aussi de configurer le contrôle d'expiration des mot de passe (password aging controls)

Pour ouvrir le fichier en mode lecture:

```
nano /etc/login.defs
```

Par défaut les configurations sont:

```
PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
PASS_MIN_LEN  5
PASS_WARN_AGE 7
```

Donc par défaut les configurations sont:

- un mot de passe estvalide pendant 99'999 jours

- il n'y a pas de délai d'attente pour changer le mot de passe
- l'utilisateur recevra un message d'avertissement 7 jours avant l'expiration de osn mot de passe.

`PASS_MAX_DAYS` : Nombre maximum de jours de validité d'un mot de passe.
`PASS_MIN_DAYS` : Nombre minimum de jours autorisé avant la modification d'un mot de passe.
`PASS_WARN_AGE` : Nombre de jours durant lesquels l'utilisateur recevra un avertissement avant que son mot de passe n'arrive en fin de validité.

Les nouvelles configurations sont comme suit:

```
PASS_MAX_DAYS   30
PASS_MIN_DAYS   2
PASS_WARN_AGE   7
```

- Le mot de passe sera valide 30 jours
- il y a un délai d'attente de deux jours avant un nouveau changement du mot de passe
- l'utilisateur recevra un message d'avertissement 7 jours avant l'expiration de son mot de passe.

Vérifier la configuration d'expiration du mot de passe (valable uniquement pour de nouveaux users):

```
chage -l [user-name]
```

Créer un nouveau groupe "evaluateur"

```
sudo addgroup [group-name]
```

Ajouter un user à un groupe:

```
sudo addgroup [user-name] [group-name]
```

ou

```
sudo adduser [user-name] [group-name]
```

ou

```
sudo usermod -aG [group-name] [user-name]
```

La commande `usermod` permet de modifier la configuration d'un utilisateur (changer son nom, l'attribuer à un groupe, changer son UID, désactiver le compte et pleins d'autres configurations

Vérifiez que cet utilisateur appartient au groupe "évaluateur":

```
getent group [nom-group]
```

ou

```
id [user-name]
```

ou

```
groups [user-name]
```

Modifiez le nom d'hôte en remplacez le login par le vôtre, puis redémarrez la machine.

```
sudo hostnamectl set-hostname [new-name]
sudo reboot
```

Comment afficher les partitions pour cette machine virtuelle?

```
lsblk
```

Vérifiez que le programme "sudo" est correctement installé sur la machine virtuelle

```
sudo policy sudo
```

Afficher l'affectation de votre nouvel utilisateur au ' sudo' group

```
sudo addgroup [user-name] [group-name]
id [user-name]
```

Supprimer un user d'un groupe donné:

```
sudo deluser [user-name] [group-name]
```

Supprimer un user du système:

```
sudo deluser [user-name]
```

Supprimer un groupe

sudo groupedel [group-name]

Passer d'un user à autre

```
su - [user-name]
```

Le sujet impose des règles strictes pour sudo. L'étudiant évalué doit d'abord expliquer l'intérêt et le fonctionnement de sudo à l'aide d'exemples de son choix.

`sudo` permet à un administrateur système de donner à un utilisateur (ou un groupe d'utilisateurs) la possibilité d'exécuter une ou plusieurs commandes en tant que super utilisateur, tout **en gardant une trace des commandes** tapées et en demandant **un mot de passe à l'utilisateur avant d'exécuter sa commande**.

Ainsi, `sudo` peut **empêcher l'exécution libre de commandes critiques** (généralement des commandes d'administration) pouvant gravement affecter le système.

Vérifier que le `/var/log/sudo/` existe et contient au moins un fichier.

```
cd /var/log/sudo/
ls -a
```

Vérifiez le contenu des fichiers dans ce dossier (en mode lecture)

```
sudo cat sudo.log
```

Vérifiez que le programme 'UFW' est correctement installé sur la machine virtuelle

```
apt-cache policy ufw
```

Vérifiez qu'il fonctionne correctement:

```
sudo ufw status
```

Énumérez les règles actives dans UFW. Une règle doit exister pour le port 4242:

```
sudo ufw status numbered
```

Ajoutez une nouvelle règle pour ouvrir le port 8080. Vérifiez que celle-ci a bien été ajoutée en listant les règles actives.

```
sudo ufw allow 8080
sudo ufw status numbered
```

Supprimez cette nouvelle règle:

```
sudo ufw delete allow 8080
```

ou

```
sudo ufw delete [numéro-règle]
```

(dans le deuxième cas il faut supprimer deux règles)

Vérifiez que le service SSH est correctement installé sur la machine virtuelle:

```
apt-cache policy openssh-server
```

Vérifiez qu'il fonctionne correctement:

```
sudo systectl status ssh
```

Qu'est-ce qu'un SSH et quel est l'intérêt de l'utiliser:

Ssh (Secure Shell) est un programme qui permet de se connecter à une machine distante et d'y exécuter des commandes. Il fournit des communications sécurisées et chiffrées entre deux hôtes non fiables à travers un réseau non sécurisé. Les connexions X11 ainsi que tout port TCP/IP peuvent également être redirigés dans ce canal sécurisé. Il peut être utilisé pour fournir des canaux de communication sécurisés à des applications.

Se connecter à votre machine virtuelle depuis un terminal de votre machine hôte:

```
ssh username@127.0.0.1 -p 4242
```

Comment fonctionne son script en vous montrant le code:

```
cd /usr/local/bin/
./monitoring.sh
```

Shell script e un fichier texte qui contient une séquence de commandes pour les systèmes d'exploitation basée sur UNIX. Un Shell script est généralement créé pour des séquences de commandes qui doivent être utilisées d'une manière répétitive afin d'économiser du temps.

Le script pour s'exécute toutes les 10 minutes à partir du démarrage du serveur.

```
su -
crontab -l
```

Le script s'exécute toutes les minutes:

```
su -
crontab -e
```

et écrire:

```
* * * * * /usr/local/bin/monitoring.sh
```

Vous pouvez exécuter ce que vous voulez:

```
cd /usr/local/bin/
sudo nano monitoring.sh
```

Et écire ce que vous voulez:

```
$ wall "The system will be restarted in 10 minutes."
```

Arrêter l'exécution du script au démarrage du serveur, mais sans modifier le script lui-même (depuis utilisateur root):

```
systemctl disable cron
sudo reboot
```

Pour réactiver cron (**depuis utilisateur root**):

```
systemctl enable cron
```

Autres commandes utiles:

Afficher la liste de tous les utilisateurs:

```
cut -d: -f1 /etc/passwd
```

ou

```
cat /etc/passwd | awk -F: '{print $ 1}'
```

Afficher la liste de tous les groupes

```
cut -d: -f1 /etc/group
```

ou

```
cat /etc/group | awk -F: '{print $ 1}'
```