Titre du TP : Sécurité Unix et Gestion des Utilisateurs

Introduction :

Ce TP vise à explorer les principes de sécurité Unix et les bonnes pratiques de gestion des utilisateurs. Les exercices couvriront la séparation des privilèges, l'utilisation de comptes utilisateur, les mises à jour et correctifs, ainsi que la configuration d'un pare-feu pour assurer la sécurité réseau.

Exercice 1 : Séparation des Privilèges

Identifiez les fichiers système critiques sur votre système.

Vérifiez les permissions associées à ces fichiers.

Comparez les permissions des fichiers système avec ceux des fichiers utilisateurs.

Correction:

Fichiers critiques: Ce sont les fichiers essentiels pour le démarrage, la configuration, et la gestion du système et des utilisateurs :

Le répertoire /etc/ qui contient plusieurs fichiers qui contiennent des informations sur les utilisateurs, groupes etc.. **/etc/passwd /etc/hosts /etc/sudoers /etc/groups**

Le répertoire **/boot** contient les fichiers nécessaires au démarrage du système, y compris le noyau Linux

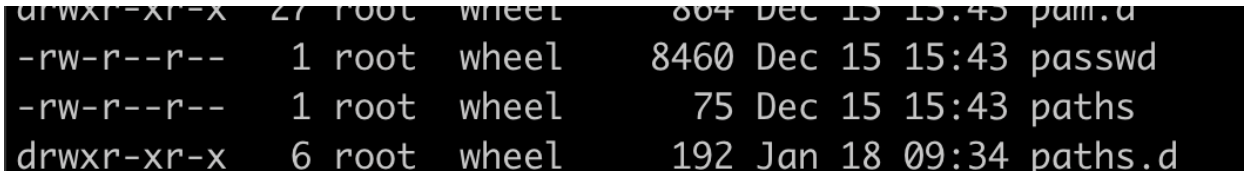
Le répertoire **/bin** qui contient des exécutables

Le répertoire **/var/log** qui contient des logs

Les droits des fichiers créés par utilisateurs , rwxr - le propriétaire peut lire écrire exécuter, le groupe associé peut lire exécuter, et toutes les utilisateurs peuvent lire , executer.

```
drwxr-xr-x@    7 vladislavyaromiy  staff      224 Oct 15 16:02 supplyChain-monorepo
drwxr-xr-x@    9 vladislavyaromiy  staff      288 Feb 14 08:51 sysDauphine
drwxr-xr-x    27 vladislavyaromiy  staff      864 Feb  7  2023 theme-1
drwxr-xr-x    11 vladislavyaromiy  staff      352 Mar  3  2023 theme-2-g-5-y-23
drwxr-xr-x     8 vladislavyaromiy  staff      256 Mar 14  2023 theme3
drwxr-xr-x    11 vladislavyaromiy  staff      352 May 22  2023 tp-js-s4-22-23
drwxr-xr-x     5 vladislavyaromiy  staff      160 May 18  2023 tp2_tp3_yaromiy_mattot
drwxr-xr-x    52 vladislavyaromiy  staff     1664 May  3  2023 tp_erreurs_yaromiy_mattot
drwxr-xr-x@    7 vladislavyaromiy  staff      224 Jan  8  2023 uni
drwxr-xr-x    15 vladislavyaromiy  staff      480 Jul  8  2023 upselling
drwxr-xr-x@    4 vladislavyaromiy  staff      128 Nov 26 16:44 wordlists
```

Maintenant on va comparer avec les fichiers critiques du système:



Le propriétaire peut lire et modifier le fichier mais ne peut pas l'exécuter. Les membres du groupe et les autres utilisateurs peuvent uniquement lire le fichier et ne peuvent ni le modifier ni l'exécuter.

On remarque aussi que le fichier passwd est en mode read pour tous les utilisateurs par défaut et en tant qu'administrateur on pourra le modifier .

Ce définit les règles permettant à certains utilisateurs ou groupes d'exécuter des commandes en tant que superutilisateur (root) ou un autre utilisateur en utilisant sudo , on remarque que le propriétaire du fichier a le droit de le lire uniquement. Les membres du groupe ont le droit de lire le fichier uniquement. Les autres utilisateurs (ni le propriétaire, ni les membres du groupe) n'ont aucun droit sur le fichier.

Exercice 2 : Gestion des Comptes Utilisateurs

Créez un nouvel utilisateur avec des privilèges limités.

Configurez le groupe sudo pour autoriser cet utilisateur à exécuter des commandes avec des privilèges élevés.

Limitez l'utilisation du compte root aux tâches d'administration critiques.

Correction:

Creation d’un user : **sudo useradd -m newuser**

-m : Cette option crée le répertoire personnel de l'utilisateur dans /home.

Création de mdp pour nouveau user: **sudo passwd newuser**

Par défaut, cet utilisateur ne disposera pas de droits d'administration. Pour donner des privilèges plus élevés on devra modifier le groupe sudo:

sudo usermod -aG sudo newuser

Pour limiter le root aux tâches d'administration critiques on peut utiliser les ACL:

setfacl -m u:newuser:r-x fichier_administratif

Cette commande donne à newuser des droits de lecture et exécution mais pas d'ecriture sur fichier_administratif.

Exercice 3 : Mises à Jour et Correctifs

Vérifiez la liste des mises à jour disponibles sur votre système.

Effectuez les mises à jour nécessaires en utilisant le gestionnaire de paquets approprié.

Vérifiez que les correctifs de sécurité sont bien appliqués.

Correction:

Cette commande met à jour la liste des paquets et versions disponibles en utilisant APT (Advanced Packaging Tool)

sudo apt update

Pour vérifier la liste des updates disponibles sans installation:

apt list --upgradable

Pour installer les mises a jours

sudo apt upgrade

Exercice 4 : Configuration d'un Pare-feu

Utilisez iptables pour configurer une règle permettant le trafic entrant sur le port SSH.

Vérifiez que la règle est correctement appliquée en testant la connexion SSH depuis un autre ordinateur.

Correction:

Pour permettre le trafic entrant sur le port 22 utilisé par SSH

iptables -A INPUT -p tcp -i eth0 --dport ssh -j ACCEPT

Pour vérifier que le règle a été bien appliqué :

```
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
```

Il faut nécessairement sauvegarder les règles car la configuration est perdue lors de redémarrage

sudo iptables-save > /etc/iptables/rules.v4

Pour se connecter depuis l'autre ordinateur:

ssh utilisateur@adresse_ip_serveur