TP : Sécurisation d'un serveur Debian via SSH avec authentification par clé

Sommaire

- 1. Introduction
- 2. Installation du service SSH
- 3. Connexion SSH par mot de passe
- 4. Création d'un nouvel utilisateur
- 5. Mise en place de l'authentification par clé SSH
- 6. Désactivation de l'authentification par mot de passe
- 7. Sécurisation supplémentaire du service SSH
- 8. Conclusion

1. Introduction

Ce TP a pour but d'installer et de sécuriser un serveur SSH sur Debian, avec mise en place d'une authentification par clé et d'une gestion des utilisateurs pour permettre l'accès sécurisé a distance au serveur.

2. Installation du service SSH

Mettre à jour le système :

```
sudo apt update && sudo apt upgrade -y
```

Installer OpenSSH :

```
sudo apt install openssh-server -y
```

Vérifier que le service est actif :

```
sudo systemctl status ssh
```

3. Connexion SSH par mot de passe

Sur la machine cliente :

```
ssh utilisateur@IP_du_serveur
```

On utilisera le mot de passe de l'utilisateur pour se connecter.

4. Création d'un nouvel utilisateur

Créer un nouvel utilisateur pour la connexion SSH :

```
sudo adduser nom_utilisateur
```

Donner les droits administrateur si besoin :

```
sudo usermod -aG sudo nom_utilisateur
```

5. Mise en place de l'authentification par clé SSH

Sur la machine cliente, générer une paire de clés :

```
ssh-keygen -t rsa -b 4096
```

Copier la clé publique sur le serveur :

```
ssh-copy-id nom_utilisateur@IP_du_serveur
```

En cas d'absence de `ssh-copy-id`, copier manuellement :

```
scp ~/.ssh/id_rsa.pub nom_utilisateur@IP_du_serveur:~/.ssh/authorized_keys
```

6. Désactivation de l'authentification par mot de passe

Modifier le fichier de configuration SSH :

```
sudo nano /etc/ssh/sshd_config
```

Changer ou ajouter les lignes suivantes :

- `PasswordAuthentication no`
- `ChallengeResponseAuthentication no`

Redémarrer le service SSH :

```
sudo systemctl reload ssh
```

7. Sécurisation supplémentaire du service SSH

- Changer le port par défaut (optionnel) :

```
Port 2222
```

- Limiter les utilisateurs autorisés :

```
AllowUsers nom_utilisateur
```

- Activer le pare-feu :

```
sudo ufw allow 2222/tcp
sudo ufw enable
```

(Adapter le port selon votre choix).

8. Conclusion

Le serveur est désormais accessible par SSH uniquement via clé pour les utilisateurs autorisés, avec un service sécurisé.