Hostin Loïc

1. Introduction

Le protocole SSH (Secure Shell) permet d'établir une connexion sécurisée à distance entre un client et un serveur. Il remplace les protocoles non sécurisés comme Telnet et FTP pour l'administration et le transfert de fichiers.

2. Prérequis

- Un serveur sous Linux (Debian, Ubuntu, CentOS, etc.)
- Un accès utilisateur avec les droits administrateurs
- Une connexion réseau fonctionnelle

3. Installation du serveur SSH

Sur Debian et Ubuntu, utilisez la commande suivante :

sudo apt update && sudo apt install openssh-server -y

Vérification du statut du service SSH :

sudo systemctl status ssh

Pour CentOS/RHEL :

sudo yum install -y openssh-server
sudo systemctl enable --now sshd

4. Configuration du serveur SSH

Le fichier de configuration principal est situé dans :

/etc/ssh/sshd_config

Quelques paramètres recommandés :

- Modifier le port par défaut (évite certains scans malveillants) :

Port 2222

- Désactiver l'accès root direct :

PermitRootLogin no

- Autoriser uniquement des utilisateurs spécifiques :

AllowUsers utilisateur1 utilisateur2

Après modification, redémarrez le service :

sudo systemctl restart ssh

5. Configuration du client SSH

Pour se connecter à un serveur SSH :

ssh utilisateur@adresse_ip -p 2222

6. Sécurisation avancée

6.1 Utilisation de clés SSH

Génération d'une clé SSH sur le client :

ssh-keygen -t rsa -b 4096

Copie de la clé publique sur le serveur :

ssh-copy-id -i ~/.ssh/id_rsa.pub utilisateur@adresse_ip

Désactivation de l'authentification par mot de passe dans **/etc/ssh/sshd_config** :

PasswordAuthentication no

Redémarrage du service :

sudo systemctl restart ssh

7. Journalisation et surveillance

Vérification des connexions SSH :

```
tail -f /var/log/auth.log  # Debian/Ubuntu
tail -f /var/log/secure     # CentOS/RHEL
```

8. Conclusion

L'implémentation de SSH sécurise l'accès distant à un serveur. L'usage de clés SSH et des restrictions d'accès renforcent cette sécurité. Il est recommandé de surveiller régulièrement les logs pour détecter toute tentative d'intrusion.