**Guide Pratique : Activation et Configuration d'un Serveur SSH**

**1. Introduction**

SSH (Secure Shell) est un protocole réseau qui permet d'établir une connexion sécurisée entre un client et un serveur.

Pour garantir la sécurité de SSH, il est recommandé de :

* - Mettre régulièrement à jour le serveur SSH.
* - Utiliser des mots de passe complexes.
* - Surveiller les connexions suspectes dans le fichier `/var/log/auth.log`.

**2. Le Système de Clés**

SSH repose sur la cryptographie asymétrique, où chaque utilisateur dispose d'une clé publique et d'une clé privée. La clé publique peut être partagée librement, tandis que la clé privée doit être gardée secrète. Ce système est combiné avec la cryptographie symétrique pour sécuriser les échanges.

**Étapes de l'échange de clés dans SSH :**

1. 1. Le serveur envoie sa clé publique au client.
2. 2. Le client génère une clé secrète et la crypte avec la clé publique du serveur avant de l'envoyer. Le serveur déchiffre cette clé pour prouver son identité.
3. 3. Le serveur crypte un message standard avec cette clé secrète et l'envoie au client. Si le client peut déchiffrer ce message, il s'agit bien du bon serveur.
4. 4. Une fois l'authentification terminée, un canal sécurisé est établi.

**3. Installation et Configuration**

pour installer le service SSH on utilise la commande:

sudo apt install openssh-server

Pour configurer un serveur SSH, modifiez le fichier de configuration `/etc/ssh/sshd\_config`. Voici quelques options importantes :

* - Port : Par défaut, SSH utilise le port 22. Vous pouvez le modifier pour renforcer la sécurité.
* - PermitRootLogin : Il est déconseillé d'autoriser les connexions en tant qu'utilisateur root.
* - X11Forwarding : Permet la transmission graphique, mais peut poser des risques de sécurité.

**4. Connexion et Transfert de Fichiers**

Pour se connecter à un serveur distant, utilisez la commande suivante :

*ssh utilisateur@adresse\_ip*

Pour transférer un fichier vers le serveur :

*scp fichier\_local utilisateur@adresse\_ip:/chemin/destination*

Pour télécharger un fichier depuis le serveur :

*scp utilisateur@adresse\_ip:/chemin/fichier\_local chemin\_destination*

**5. Connexion sans Mot de Passe**

Pour se connecter sans mot de passe, utilisez un couple de clés publique/privée. Ajoutez votre clé publique au fichier `~/.ssh/authorized\_keys` sur le serveur.

Commandes utiles :

1. 1. Générer une paire de clés : ssh-keygen -t rsa
2. 2. Ajouter la clé au serveur : ssh-copy-id utilisateur@adresse\_ip

**6. Tunnel SSH**

Un tunnel SSH permet de chiffrer n'importe quelle communication TCP entre deux machines. Par exemple, pour sécuriser une connexion HTTP :

*ssh -L 8080:serveur:80 utilisateur@adresse\_ip*

**Illustration : Génération de Clés SSH**

Exemple d'exécution de la commande `ssh-keygen -t rsa` :

**Illustration : Ajout de la Clé Publique au Serveur**

Exemple d'exécution de la commande `ssh-copy-id user@hostname` :