Comprendre SSH (Secure Shell)

Riyad Derguini

22 janvier 2025

1 Introduction

SSH (pour **Secure SHell**) est un protocole qui permet d'exécuter un shell sur un système distant de manière sécurisée. C'est un outil fondamental en administration système, car il permet d'administrer des systèmes distants sans avoir à se déplacer physiquement. Pour en savoir plus, consultez cette page *Wikipedia*.

2 Fonctionnement de SSH

SSH repose sur une architecture client-serveur :

— Le **système distant** exécute un **serveur SSH**, un programme qui écoute en permanence sur le port 22 (par défaut).

— Le **système local** exécute un **client SSH**, qui se connecte au serveur SSH distant.

2.1 Étapes de la connexion SSH

1. Le client SSH ouvre un port aléatoire sur le système local et se connecte au port 22 du système distant.
2. Le serveur SSH vérifie :
   — L'**identification** de l'utilisateur (votre login).
   — L'authentification (votre mot de passe ou une clé SSH).
   — Les **autorisations** (si vous avez le droit de vous connecter).
3. Une fois la connexion établie, le serveur SSH permet d'exécuter un shell sur le système distant.

3 Pourquoi SSH est-il sécurisé ?

SSH utilise des techniques de chiffrement pour protéger les données échangées entre le client et le serveur. Cela garantit que :

— Les informations ne peuvent pas être interceptées (confidentialité).
— Les données ne peuvent pas être modifiées (intégrité).
— L'identité du serveur est vérifiée (authentification).

4 Schéma de fonctionnement de SSH

Voici un schéma pour mieux comprendre le fonctionnement de SSH :

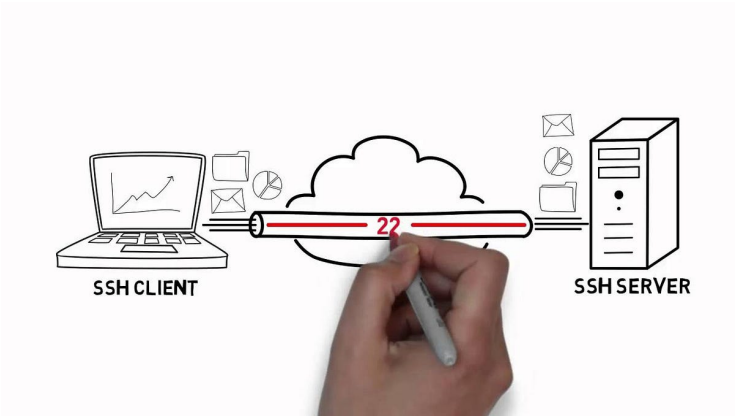

FIGURE 1 – Schéma de fonctionnement de SSH

4.1 Explication du premier schéma

— Le **client SSH** sur le système local se connecte au **serveur SSH** sur le système distant.
— Une fois la connexion établie, l'utilisateur peut exécuter des commandes sur le système distant via un shell sécurisé.

5 Authentification par clé SSH

Pour renforcer la sécurité, SSH permet d'utiliser une authentification par clé publique/privée au lieu d'un mot de passe. Voici comment cela fonctionne :

5.1 Explication du deuxième schéma

— Une **clé publique** est stockée sur le serveur SSH.
— Une **clé privée** est conservée sur le système local.
— Le serveur SSH vérifie que la clé privée correspond à la clé publique avant d'autoriser la connexion.
— Cette méthode est plus sécurisée qu'un mot de passe et évite les attaques par brute force.

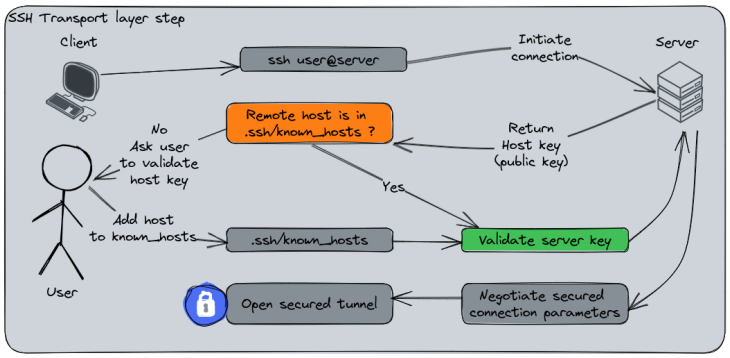

FIGURE 2 – Authentification par clé SSH

6 Conclusion

SSH est un outil indispensable pour administrer des systèmes distants de manière sécurisée. Grâce à son chiffrement et son architecture client-serveur, il garantit la confidentialité, l'intégrité et l'authentification des échanges. Utilisez-le pour gérer vos serveurs à distance en toute confiance !