TP SSH

Table des matières

Introduction

SSH :Secure Shell

Connexion sécurisé entre un client et un serveur

Version libre : OpenSSH

SSH doit être sécurisé :

- Mises à jour
- Mots de passe complexes
- Surveiller régulièrement les connexions dans /var/log/auth.log

Test de mots de passe avec John

Sudo apt install john

John /etc/shadow

```
root@gaara:/etc# sudo john shadow
No password hashes loaded (see FAQ)
root@gaara:/etc#
```

Le système de clés

- Cryptographie asymétrique :
  Chaque personne dispose d'un couple de clés : publique et privé
  La connaissance de la clé publique ne permet pas d'en déduire la clé privée

Alice — Chiffre son message → Bob perme de décrypter avec sa clés privé

Avec la clé publique de Bob

- Cryptographie symétrique :
  Bob et Alice ont tous les deux la même clé secrète.
  Cette méthode est beaucoup moins gourmande en ressources mais le problème est l'échange de la clé.

  Dans SSH, les 2 méthodes sont utilisées : d'abord la cryptographie asymétrique pour échanger la clé secrète, puis la cryptographie symétrique pour le reste de la conversation.

  Un couple de clé RSA, généré à l'installation du serveur, est stocké dans le dossier /etc/ssh
  - Clé privée : ssh_host_rsa_key 600
  - Clé publique : ssh_host_rsa_key.pub 644

  Etape :

  1 : Le serveur envoie sa clé publique au client

  2 : Le client génère une clé secrète et l'envoie au serveur en la cryptant avec la clé publique (asymétrique). Le serveur déchiffre cette clé avec sa clé privée (ce qui prouve qu'il est le bon serveur).

  3 : Le serveur crypte un message standard avec la clé secrète, il a la preuve que c'est le bon serveur.

  4 : Le canal est établi entre le client et le serveur (asymétrique).

5 : Echange du login et du mot de passe utilisateur.

Installation et configuration

Sudo apt install openssh-server

Fichier de configuration : /etc/ssh/ssh_config

Port: 22 par default

Permit Root Login : Permission root déconseillée

X11Forwarding : Transmission graphique

Démarrage du serveur : systemctl start sshd

Connexion

Commande de connexion : ssh user@machine

Où sont stockée la clé publique du serveur : ~/.ssh/know_hots

Sur windows : C:\Users\teted\.ssh\know_hosts

```
192.168.0.119 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB+BM1vZ+v4gjAj6psZbrypFpnQtxgWyH3X71qell9s2
192.168.0.119 ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDUgnArsdRnbiJPvrhkjp5DmBEh/r/5nKyYI1w8hl36bDX7to5pkBQkWMVlnv/slHpoheifgF+BLcbP9xLPhr+CNBFxiGKXZ5uwFTuEwGWhw29L
UtikNCQTx/zyyUc9btP7WR0A3Ri4Y0SmfOx+u0gv5hXzUAiL1Cr/NLHKwB7tQo/Oi71cKeOPQy0YpJLIvSBUyKjRktX/FYQOWGq0L5f4JYAf3ltx+
0zsiCJgKP5kck9ehU4pqNdTkB1kZ6id8cg5frbMd3QYTeYIXLuKuX8Vq6p+
77kOpK5BwnmL/OY5FvcIagihCaM1UeZzpf9Y7sbJng4vqcZ3z72tAnglI0f5BJbS2HzK+XkhGy7i5qKDPhhzjPd7CVZKxLxJjSfKj8cgvqz4pUwzCdPGKLoi3QqYxwWuHoqi4hl+CHD9
msLcXCNoFsI+KYeoxjT4IideTujK9Ne0hYJhdci1O7AwwaUDojt61Y5gM9/qsxzh9bVKOYwi72+bjD1A3hQF5PsXF4c=
192.168.0.119 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJMUkK/ovPxf5yZDmfnRIf2HDnJ+hHTUgD7v9
+JmX7nhGypaR5OMAY8NhJfqEUU2wUsq9c3L/bUWcWRviO4o7MQ=
```

- Authentification par clé au lieu de login/password :

  Ssh-keygen -t dsa

  ➔ ~/.ssh/id_dsa 600

  ➔ ~/ .shh/id_dsa.pub 644

- Autirisers vos clés : copier notre clé publique dans

  ➔ ~/.ssh/authorized_keys

Transfert de fichiers

Commande scp

Pour transférer test1.txt :

Scp test1.txt toto@ip:

Pour télécharger test2.txt:

Scp toto@ip:test2.txt.

Se connecter sans mots de passe

On utilise le couple de clés publique/privée mais on ne peut pas taper la passphrase chaque fois. On utilise le ssh-agent pour la garder en mémoire.

Eval $(ssh-agent)

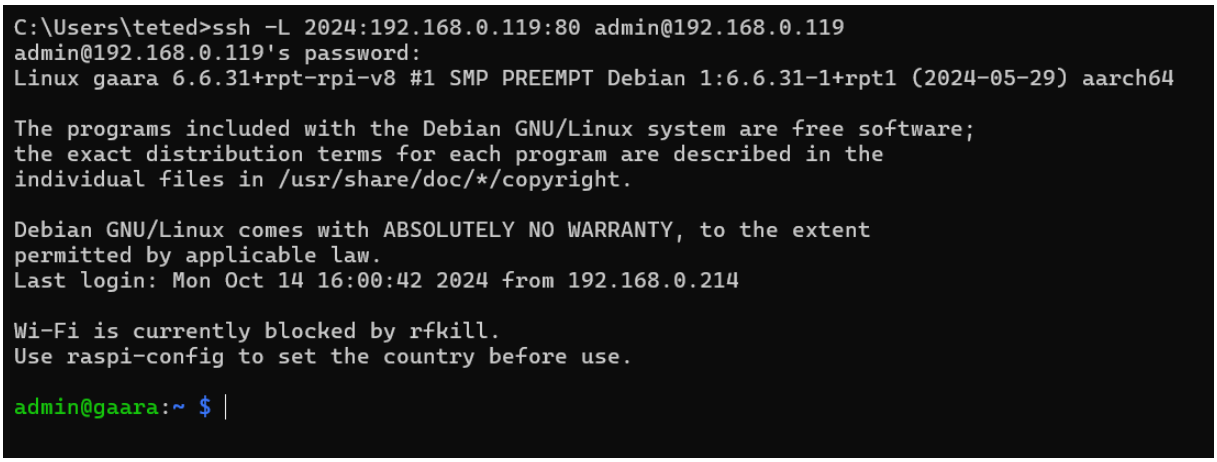
Ssh-add

Tunel SSH

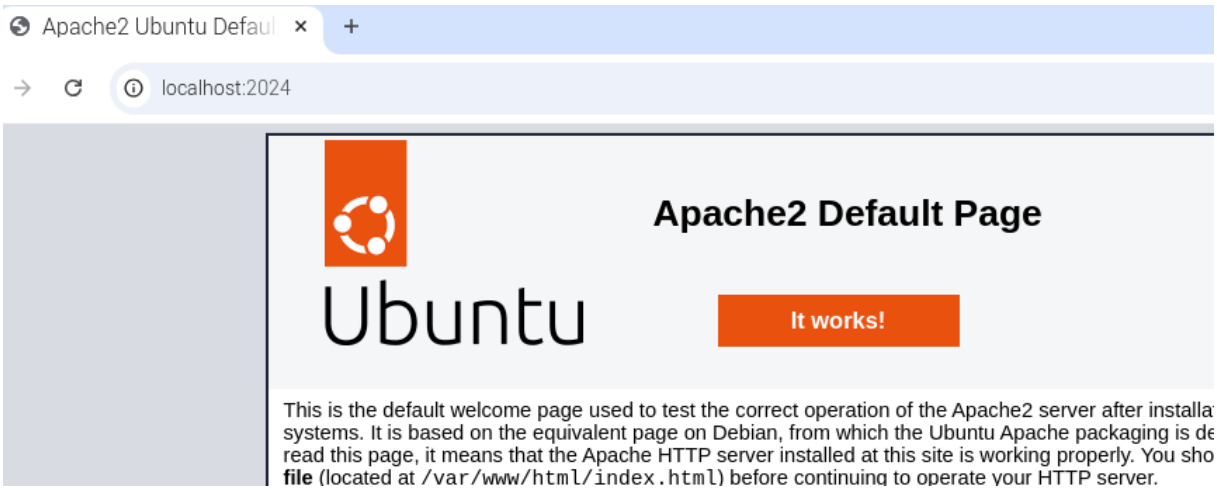
Pour chiffrer n'importe quelle communication TCP entre 2 machines.

Exemple pour une connexion http :

- Création du tunel
  - Ssh -L 2024 :ip_server :80 user@ip_serveur



- Vérification dans un navigateur : http://ip_serveur:2024


Apache2 Ubuntu Defaul
localhost:2024
Apache2 Default Page
Ubuntu
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installa
systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is de
read this page, it means that the Apache HTTP server installed at this site is working properly. You sho
file (located at /var/www/html/index.html) before continuing to operate your HTTP server.