TP SSH

1) Intro :

SSH : Secure shell

Connexion entre un client et un serveur

Version libre : openssh

Ssh doit être sécurisée :

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

Test de mdp avec john

2) Le système de clés
- Cryptographie asymétrique :

Chaque personne dispose d'un couple de clés publique et privée, la connaissance de la clé publique se permet pas d'en déduire la clé privée

- Cryptohraphie symétrique :

Bob et alice ont les deux la même secrète

Cette méthode est beacoup moins gourmande en ressources mais le problème est l'échange de la clé

Dans SSH, les 2 méthode sont utilisé : 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, et stocker dans le dossier /etc/ssh :

- Shh_host_rsa_key 600
- Ssh_host_rsa_hey.pub 644

Étapes 1 : serveur envoie sa clé publique au client.

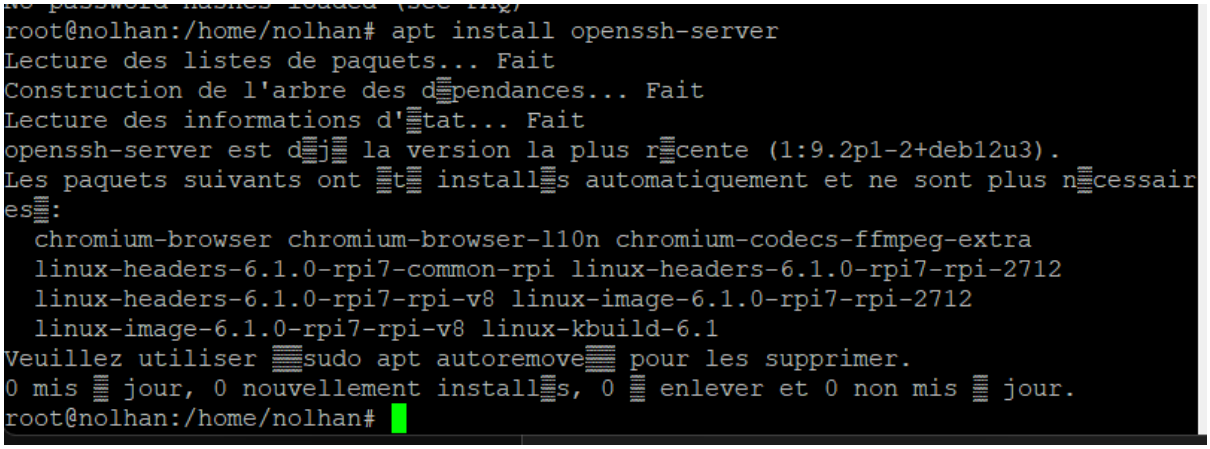
Étape 2 Le client génère une clé secrète et l'envoie au serveur en la cryptant avec la clé publique (asymétrique). Le serveur déchiffre cette clé avec sa clé ce qui prouve qu'il est le bon serveur

Étape 3 : le serveur crypte un message standard avec sa clé secrète et l'envoie au client. Si le client déchiffre le message standard avec sa clé secrète, il a la preuve qu'ik s'agit du bon serveur

Étape 4 : le canal est établie entre le client et le serveur (asymétrique)

Étape 5 : echange du login et du mdp utilisateur

3) Installation et configuration



Port 22

PermitRootLogin permission root déconseiller

X11forwording tranmission graphique

Demarrage du serveur : oui

4) Connexion

Commande de connexion : ssh user@machine

Authentification par clé au lieu de login/password

- Généré un couple de clés DSA :

Ssh –keygen –t dsa

- Autoriser vos clés : copier votre clé publique dans

5) Transfère de fichier

Commande scp

Pour transfèré un fichier test1.test

Scp test1.test toto@ip

Pour télécharger test2.test

Scp toto@ip:test2.test

6) Connecter sans mot de passe

On Utilise le couple de clé publique / privé mais on ne veut pas utiliser la passphrase chaque fois , on utilise le ssh-agent pour le garder en mémoire

En mémoire

Eval $ (ssh-agent)

7) Tunnel ssh

Pour chiffrer n'importe qu'elle communication tcp entre 2 machines

Exemple pour une connexion http :

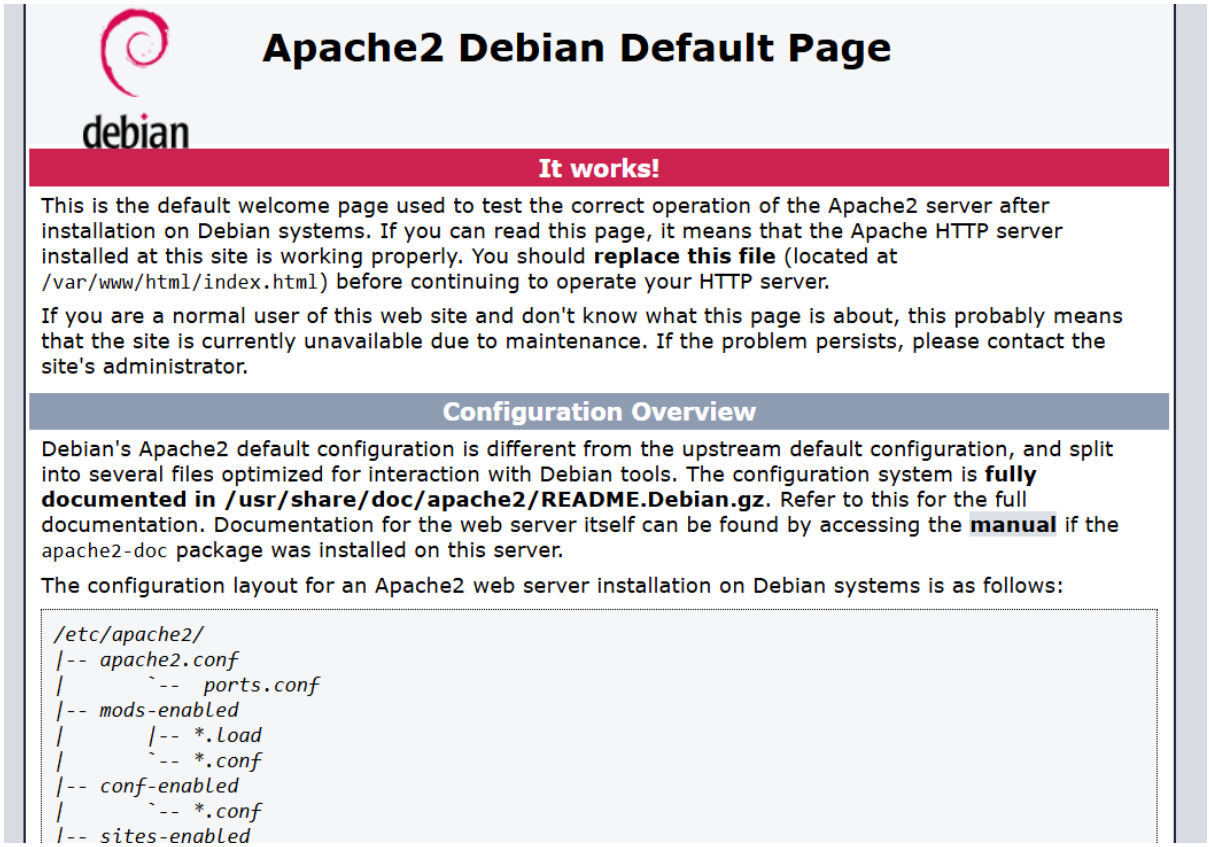
- Création du tunnel

Ssh –L 2024:ip-serveur:80 user@ip_serveur

```
nolhan@nolhan:~ $ ssh -L 2024:192.168.0.86:80 nolhan@192.168.0.86
The authenticity of host '192.168.0.86 (192.168.0.86)' can't be established.
ED25519 key fingerprint is SHA256:YZN5rlqS/GrmQQJ6khuFXGlvPPpcvHZ1za5izWqnq+I.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.86' (ED25519) to the list of known hosts.
nolhan@192.168.0.86's password:
Linux nolhan 6.6.51+rpt-rpi-v8 #1 SMP PREEMPT Debian 1:6.6.51-1+rpt1 (2024-09-26
) aarch64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Oct 14 15:58:33 2024 from 192.168.0.223
nolhan@nolhan:~ $
```



Fait de windows a raspberry