***sudObjectif :***

Comprendre le fonctionnement des clés asymétriques.

Savoir comment utiliser le protocole et la connexion SSH de manière plus sécurisée en utilisant les méthodes de chiffrement.

***Matériel nécessaire :***

Une machine Linux et une machine cliente Windows (ça peut être votre machine physique).

Avant de commencer ce TP, vérifier que vos 2 machines peuvent communiquer entre elles et que la machine linux a accès à internet.

Travail à effectuer :

Précédemment, vous avez installé le protocole SSH sur une machine Linux, et donc fait de votre machine un serveur SSH.

Vous vous êtes connecté en direct sur la machine en utilisant le nom d’un utilisateur et un mot de passe depuis votre client Windows.

# Rappel : Faites Attention !

Ne confondez pas SSH, ssh et sshd !

SSH est le protocole de communication.

ssh est le programme client permettant de se connecter au serveur

sshd est le daemon ssh du serveur ssh qui communique par défaut sur le port 22.

Pourquoi faire la distinction entre tout ça ?

Principalement pour les fichiers de configuration.

Le fichier /etc/ssh/ssh\_config est le fichier de configuration du client ssh. On a rarement besoin d’y toucher.

Tandis que le fichier /etc/ssh/sshd\_config est le fichier de configuration du serveur ssh. Et vous allez le modifier dès à présent.

# Changement du numéro de port du serveur ssh

Manipulations sur la machine Linux « principale ».

sudo nano /etc/ssh/sshd\_config.

La ligne ‘Port 22’, signifie que votre serveur SSH écoute sur le port 22. Il s’agit du port par défaut. Changez-le. Mettez le port 22320.

Vous avez changé le fichier de configuration, vous devez le relancer le service ssh pour que les modifications soient prises en compte.

systemctl restart sshd

Pour vérifier que le changement à bien été pris en compte, faites un status de la commande, et lisez les logs à le fin du status. Vous avez une ligne qui vous indique que le service est en écoute sur le port mentionné.

systemctl status sshd

De manière simple, tenter de vous connecter d’une machine cliente (Windows ou Linux) sur la machine Linux principale, en ssh. Pour que la machine cliente sache sur quel port elle doit communiquer avec le serveur, il faut lui préciser :

Depuis Putty ou Moba, spécifiez le port dans l’options appropriée.

Depuis l’invite de commande :

ssh [login]@[ip] -p 22320