

SSH Keys

Vous pouvez si vous le souhaitez désactiver la connection par mot de passe et utiliser une clé SSH à la place, pour cela rien de plus simple.

Commençons par générer une paire de clés pour cela tapez sur le terminal de votre ordinateur local (MobaXTerm dans mon cas).

```
ssh-keygen -t ed25519

# Au premier prompt mettez le nom de fichier que vous voulez #pour votre clé.
# A la seconde question pour la passphrase vous pouvez ne rien mettre si vous ne souhaitez pas
utiliser de mot de passe à chaque fois que vous vous connectez sur votre serveur.
```

Deux fichiers seront générés dont un contenant l'extension .pub, ce fichier contiendra votre clé publique. Le second contiendra votre clé privé.

Sur votre serveur allez ensuite dans le répertoire ~/.ssh/ de l'utilisateur auquel vous souhaitez vous connecter en utilisant cette clé.

Créez un fichier `authorized_keys` s'il n'existe pas déjà:

```
nano authorized_keys

# Puis copiez votre clé publique à l'intérieur directement vous pouvez en ajoutez plusieurs à
la suite
```

Soyez sûr de bien sauvegarder votre clé privée et publique dans un endroit sûr. Continuons en désactivant l'authentification par mot de passe dans le fichier de configuration SSH.

```
nano /etc/ssh/sshd_config
```

Une fois dans le fichier de configuration cherchez les valeurs suivantes et modifiez les comme ci-dessous :

```
PubkeyAuthentication yes
# Retirez le .ssh/authorized_keys2 qui peut servir à certaines attaques
AuthorizedKeysFile      .ssh/authorized_keys
PasswordAuthentication no
```

UsePAM no

Il nous suffit ensuite de redémarrer le service ssh en utilisant la commande `sudo systemctl restart sshd`

Vous pouvez désormais vous connecter en utilisant votre clé assurez cependant de bien importer votre clé privée dans l'utilitaire que vous utilisez. Sous MobaXterm déposez les dans:

`C:\Users\VOTRE_USER\Documents\MobaXterm\home\.ssh`

Revision #5

Created 2021-10-22 16:16:13 UTC by Faces

Updated 2022-06-11 09:07:27 UTC by Faces