SSH

Les tips, tricks, et autres joyeusetés en rapport avec SSH

Introduction

Le protocole SSH (Secure SHell) permet de se connecter à un système à distance. En général en ligne de commande.

On l'utilise beaucoup sur Linux, c'est même la méthode de connexion recommandée pour l'administration des serveurs.

Clients

Pour pouvoir se connecter à un serveur SSH, il faut un client SSH :

Linux

Sur Linux on peut installer le binaire `ssh` avec son gestionnaire de paquet si ce n'est pas déjà fait :

```
# Sur debian/ubuntu
apt install openssh-client

# Sur RedHat/Fedora
dnf install openssh-clients
```

Windows

Nous ne connaissons pas ces outils mais nous en avons entendu beaucoup de bien :

- MobaXTerm (https://mobaxterm.mobatek.net/)
- mRemoteNG (https://mremoteng.org/)

Connexion

Pour se connecter à un serveur Linux il nous faut au moins:

- le nom de l'utilisateur

- l'IP du serveur

On pourra ensuite se connecter avec la commande:

```
ssh  <USERNAME>@<IP>
```

Clé SSH

Générer une clé avec:

```
ssh-keygen -t ed25519
```

> La génération de la clé demande plusieurs informations, notamment sur le type de clé à créer. Le standard a été pendant longtemps le type RSA, mais c'est désormais c'est le type **Ed25519** qui est recommandé et qui devrait devenir la valeur par défaut progressivement.

Sortie standard:

```
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/corentin/.ssh/id_ed25519): /home/corentin/.ssh/id_ed25519_demo
Enter passphrase for "/home/corentin/.ssh/id_ed25519_demo" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/corentin/.ssh/id_ed25519_demo
Your public key has been saved in /home/corentin/.ssh/id_ed25519_demo.pub
The key fingerprint is:
SHA256:hdYwGKHqem4HpXu9x4vYKkBXcb7YJ6MKiFbPnpMnOhA corentin@thinkpad
The key's randomart image is:
+--[ED25519 256]--+
|     .+=o        |
|     o+  =       |
|    o  .o o      |
| E o. o...       |
|. ++ . =S.       |
|+o+ o . +        |
|o+oo =..         |
|..*.=*ooo        |
|.+.*=+Bo..       |
+----[SHA256]-----+
```

La clé publique finit par `.pub`. C'est la seule qui peut être copié ou transmise à un serveur:

```
ssh-copy-id <USERNAME>@<IP>
```