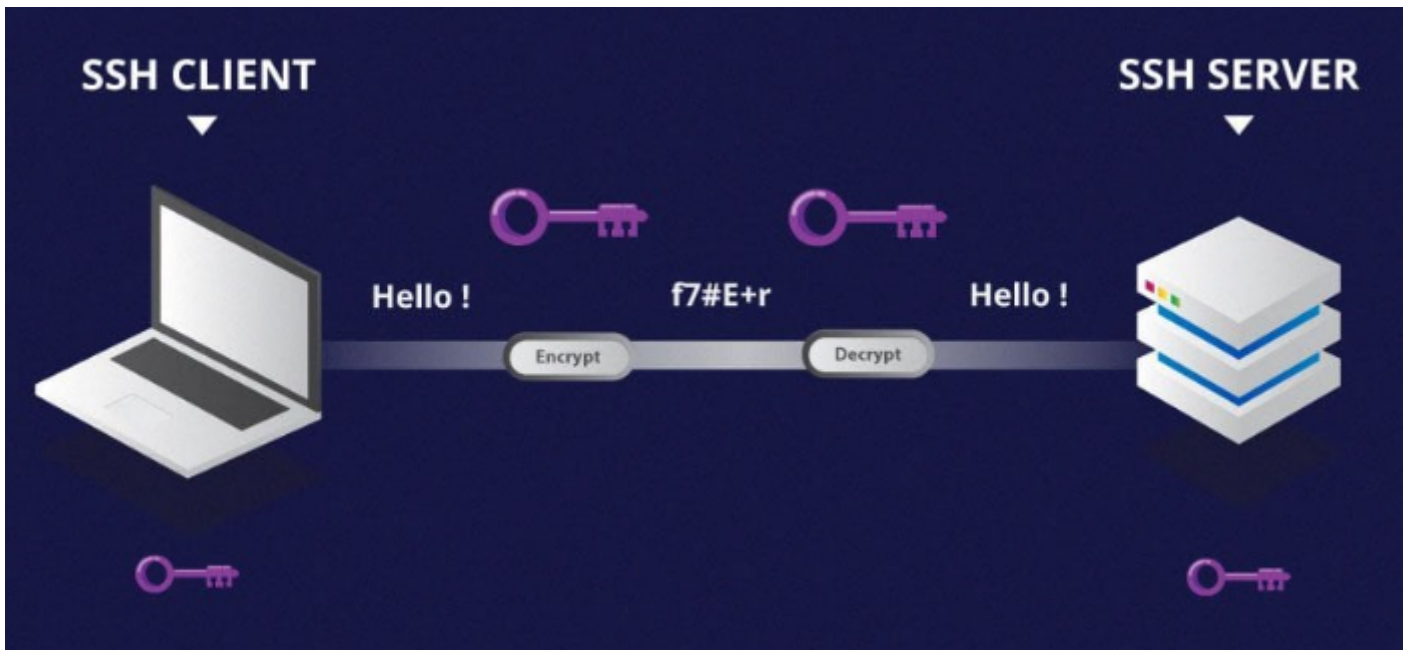


SSH

Introduction

“ C'est quoi SSH ?

Le protocole **Secure Shell (SSH)** est une méthode permettant d'envoyer en toute sécurité des commandes à un ordinateur sur un réseau non sécurisé. SSH a recours à la **cryptographie** pour authentifier et **chiffrer les connexions** entre les appareils.



Méthode d'authentification

Comment se connecter en SSH

Sur Windows, vous pouvez utiliser le client SSH intégré dans le terminal (PowerShell ou Command Prompt) à partir de la version Windows 10 1809, ou installer un programme tiers comme PuTTY, Termius...

Terminal Windows

Sur le terminal windows la connexion ssh est très simple, voici le format de la commande.

```
ssh [utilisateur]@[@IP]
```

```
PS C:\Users\LeoDe> ssh kali@192.168.118.129
The authenticity of host '192.168.118.129 (192.168.118.129)' can't be established.
ED25519 key fingerprint is SHA256:Iy8ttlW6tgcifleEXZwrtcBcZ/rynpZLNsu4ujoz0uk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.118.129' (ED25519) to the list of known hosts.
kali@192.168.118.129's password:
```

Authentification par mot de passe

Par défaut, l'authentification SSH s'effectue avec le mot de passe l'utilisateur avec lequel vous essayez de vous connecter.

La connexion ssh sur l'utilisateur **root** est par défaut désactivée, il n'est pas recommandé d'activer la connexion à l'utilisateur root pour des raisons de sécurité.

Authentification par clé

Sur de nombreux serveurs Linux, l'authentification exclusive par clé est une pratique répandue, car elle diminue les vulnérabilités associées à l'utilisation d'un mot de passe.

Création de la clé

On va procéder aux étapes pour créer une clé et s'y connecter avec sur notre serveur.

Allez dans votre Terminal en mode windows powershell et lancez la commande suivante `ssh keygen`

.

Par défaut, le nom de la clé est "id_rsa" ; vous pouvez lui donner un autre nom ; dans l'exemple ci-dessous, elle s'appellera **docs**.

Il vous sera demandé une **passphrase**, une passphrase est un mot de passe pour utiliser la clé lors de la connexion, vous pouvez le laisser vide si vous le souhaitez.

Par défaut, la clé sera sauvegardée dans le chemin suivant `%USERPROFILE%\ssh`.

```

PS C:\Users\LeoDe> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\LeoDe\.ssh\id_rsa): docs
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in docs
Your public key has been saved in docs.pub
The key fingerprint is:
SHA256:34u+IhueByZRHsRfCkEUq2kapyv9tH7cyp632fzZ2PE leode@PC-L30-F
The key's randomart image is:
+---[RSA 3072]-----+
|    +++o..    |
|    . =o..    |
|    +..       |
|    o..       |
| . = . S      |
| * . o . .    |
| o. .+.o . . . |
| .... +++=+ . * o |
| o  o+o0*o+*o= o E|
+-----[SHA256]-----+
PS C:\Users\LeoDe>

```

Maintenant que votre clé est créée il faut ajouter le contenu du fichier `%USERPROFILE%\.ssh\id_rsa.pub` dans le fichier `authorized_keys` présent dans le dossier utilisateurs dans `.ssh`.

```

root [ubuntu] $ tree -a /home/ubuntu
/home/ubuntu
├── .bash_history
├── .bash_logout
├── .bashrc
├── .cache
│   ├── motd.legal-displayed
│   ├── update-manager-core
│   └── meta-release
├── .profile
├── .ssh
│   └── authorized_keys

```

Utilisation de la clé

L'authentification avec la clé générée n'est pas compliquée, si vous l'avez l

Rédaction en cours... Just wait

Révision #4

Créé 9 février 2024 00:42:36 par Léo del Giudice

Mis à jour 15 février 2024 10:08:50 par Léo del Giudice