La sécurité SSH

OBJECTIFS

- Comprendre les mécanismes de sécurité de SSH.

- Analyser les protections contre : Les attaques par force brute et les attaques Man-in-the-Middle (MITM)

- Comprendre le rôle du fichier known_hosts.

- Résoudre les erreurs d'empreinte SSH.

Étape 1 : Installer openssh-server

Commande :

```
sudo apt install openssh-server
```

Étape 2 : Tenter une connexion SSH en root

Commande :

```
ssh root@IP_du_serveur
```

Résultat attendu :

- Connexion refusée.

Pourquoi ?

- Pour éviter les attaques par force brute.

Dans `/etc/ssh/sshd_config`, la directive suivante empêche la connexion root :

```
PermitRootLogin prohibit-password
```

Pour des raisons de sécurité :

le compte **root** est trop ciblé par les les attaques **force brute** (les hackers testent massivement la connexio `root + mot de passe`

```
Une machine malveillante teste des milliers de mots de passe par seconde :

root / 123456

root / admin

root / password

root / toto

    ...
```

SSH bloque donc l'accès root par mot de passe

Étape 3 : Désinstaller SSH

Commande :

```
sudo apt remove --purge openssh-server
```

Étape 4 : Réinstaller SSH

Commande :

```
sudo apt install openssh-server
```

Explication :

- Une nouvelle clé publique est générée automatiquement.

Étape 5 : Nouvelle connexion avec un compte utilisateur

Commande :

```
ssh utilisateur@IP_du_serveur
```

Avertissement affiché :

@@
@@@@@@

```
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:PuXN9IBczVZr3v+70ETMAGvMYh8tJawmuiTQRpDNIho.
Please contact your system administrator.
```

Explication :

- Le client compare l'empreinte de la clé publique du serveur avec celle stockée dans :

```
~/.ssh/known_hosts
```

- La clé ayant changé, SSH suspecte une attaque MITM.

-Lors d'une attaque Man-in-the-Middle :

1. L'attaquant intercepte la connexion.

2. Le serveur présente SA clé publique au client.

3. Le client voit une clé différente.

4. le client SSH déclenche l'alerte de sécurité. C'est l'une des protections majeures de SSH.

Étape 6 : Vérifier le fichier known_hosts

Commande :

```
ls  ~/.ssh/
```

Étape 7 : Supprimer l'ancienne empreinte

Méthode 1 — Supprimer uniquement l'entrée du serveur :

```
ssh-keygen -R IP_du_serveur
```

Méthode 2 — Supprimer tout le fichier known_hosts :

```
rm  ~/.ssh/known_hosts
```

Étape 8: Reconnexion

Commande :

```
ssh utilisateur@IP_du_serveur
```

```
The authenticity of host (IP_du_serveur)' can't be established.
ED25519 key fingerprint is SHA256:PuXN9IBczVZr3v+70ETMAGvMYh8tJawmuiTQRpDNIho.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

- SSH redemandera d’accepter la nouvelle empreinte.

- Le fichier known_hosts sera mis à jour.