Utiliser des certificats OpenSSH

Présentation

La connexion à distance à un serveur en SSH peut se faire avec des certificats dont le format est spécifique à OpenSSH.

Rappel : l'authentification sur le serveur en SSH consiste à renseigner votre clé publique dans le dossier .ssh/authorized_keys du compte existant sur le serveur.

Votre clé privée reste sur votre ordinateur client et ne doit pas être communiquée. Cette clé privée peut en plus être protégée par une passphrase.

Configuration du service SSH du serveur

Avec Debian, la configuration d'un serveur SSH se fait dans le fichier **/etc/ssh/sshd_config** :

- La directive **PasswordAuthentication** doit être fixée à **no** pour interdire l'authentification par mot de passe.
- dans le dossier **/etc/ssh** se trouve plusieurs types de clés privées, avec les clés publiques associées, générées automatiquement, que peut utiliser le serveur SSH : **ssh_host_ecdsa_key** (ssh_host_ecdsa_key.pub) , **ssh_host_rsa_key** (ssh_host_rsa_key.pub) et **ssh_host_ed25519_key** (ssh_host_ed25519_key.pub).

Pour **vérifier** le paramétrage du serveur SSH, lancez la commande suivante en mode debug :

```
$ sudo /usr/sbin/sshd -d
```

La commande suivante d'afficher ces différents clés publiques d'un serveur SSH (RSA, ECDSA et ED25519):

```
$ ssk_keyscan adresseIPserveurssh
```

Génération du couple de clés privée / publique par le client

Utilisation de l'utilitaire **ssh-keygen** avec les options possibles suivantes :

- option **-t** : préciser le tp de clés : dsa, rsa, ecdsa ou ed25519 (valeur par défaut) ;
  - option **-b** : préciser la longueur de la clé (2048 par défaut).
  - option **-C** : préciser un commentaire pour identifier la clé publique : courriel, nom, etc..

```
$ ssh-keygen -C "Charles Técher"
```

```
* sécuriser la clé privée
```

```
$ chmod 600 ~/.ssh/id_ed25519
```

Les clés privée et publique sont enregistrées dans le dossier **~/.ssh** : **id_ed25519** et **id_ed25519.pub**.

La passphrase de la clé privée peut être modifiée avec la commande suivante :

```
$ ssh-keygen -p -f .ssh/id_ed25519
```

La clé publique peut être affichée à partir de la clé privée :

```
$ ssh-keygen -y -f .ssh/id_ed25519
```

Paramètrage du compte du serveur avec votre clé publique

Sur le serveur distant, vous souhaitez permettre une authentification avec votre clé publique shh.

Pour cela, il suffit de **copier** le contenu de votre clé publique dans le fichier **~/.ssh/authorized_keys** du compte du serveur.

- Exemple de copie automatique de la clé publique pour un compte appelé sio créé sur le serveur distant :

```
ssh-copy-id sio@ipserveur
```

- Exemple de copie manuelle de la clé publique pour un compte appelé sio créé sur le serveur distant :

```
cat ~/.ssh/id_ed25519.pub | ssh sio@ipserveur "cat >> ~/.ssh/authorized_keys"
```

Gestion des serveurs connus

Votre client SSH va **vérifier l'identité du serveur distant** avant de se connecter. Le fichier **/etc/ssh/ssh_config** permet de configurer le client SSH pour tous les utilisateurs de votre ordinateur, et le fichier **~/.ssh/config** uniquement pour l'utilisateur qui a ouvert une session.

Lors de la **première connexion** du client sur le serveur distant, vous recevez un **message avertissement** et vous devez confirmer, à vos risques et périls, que vous acceptez de vous connecter à ce serveur. Dans ce cas, une trace du serveur (**empreinte SSHFP** - SSH FingerPrint), est enregistrée dans le fichier **~/.ssh/known_hosts**. Lors d'une prochaine connexion, si la trace d'une connexion précédente est trouvée, vous n'aurez plus le message d'avertissement.

La commande suivante permet de **prendre connaissance de l'empreinte** de la **clé publique** du serveur distant, et de la communiquer aux utilisateurs client pour **vérification** :

```
$ ssh-keygen -l -f /etc/ssh/ssh_host_ed25519_key.pub
```

Inconvénients de l'usage des clés publiques

Les clés publiques d'un serveur peuvent être changées et ne plus être celles initialement crées. C'est le cas lors d'une attaque de type Man-In-The-Middle.

De même, il n'est pas possible d garantir que la clé publique d'un client est légitime.

L'utilisation d'un certificat ajoute des informations d'identité et ce certificat est signé par une autorité de certification reconnue.

La signature du certificat est un haché des données du certificat chiffrée par la clé privée de l'autorité de certification reconnue.

En utilisant la clé publique de l'autorité de certification reconnue, il est possible de déchiffrer la signature et de comparer ensuite les hachés.

Génération d'un certificat SSH

OpenSSH permet de générer des certificat spécifiques à OpenSSH. Ce ne sont pas des certificats x509 utilisés avec SSL/TLS (https, sftp, etc.)