

Principe de l'authentification SSH par clé

Présentation

La Sécurité Informatique d'un système d'information nécessite de respecter des critères de sécurité. L'un de ces critères est l'authentification.

Définition : L'authentification permet de **vérifier** l'identité d'une entité afin de :

1. s'assurer d'abord de la **légitimité** d'une demande d'accès, faite par un opérateur humain et/ou une machine
2. Autoriser ensuite **l'accès** de l'opérateur ou la machine aux ressources demandées conformément aux règles du contrôle d'accès.

Traditionnellement, **l'authentification** se fait d'une manière **simple** en utilisant un seul élément ou **facteur** sous la forme du couple **login / mot de passe**.

- l'authentification **forte**, dite aussi authentification **multi-facteurs**, repose sur **deux facteurs ou plus** ;
- l'authentification **unique** consiste en une **seule** authentification qui est accordée à un utilisateur afin de lui permettre d'avoir accès à **plusieurs** ressources.

Activités à faire

En vous aidant des liens suivants ou de vos recherches sur Internet, vous devez réaliser un dossier documentaire sur la connexion sécurisée à distance sur un serveur avec SSH. Votre dossier doit permettre de répondre aux questions ci-dessous.

Ressources proposées

- <https://www.globalsign.fr/fr/blog/difference-entre-ssl-et-tls/>
- <http://sebsauvage.net/comprendre/ssl/>
- <https://www.it-connect.fr/chapitres/authentification-ssh-par-cles/>
- <https://www.it-connect.fr/les-cles-symetriques/>
- <https://www.it-connect.fr/les-cles-asymetriques/>
- <https://www.remipoignon.fr/authentification-ssh-par-cle-privee/>
- <https://delicious-insights.com/fr/articles/comprendre-et-maitriser-les-cles-ssh/>
- <https://openclassrooms.com/fr/courses/43538-reprenez-le-controle-a-laide-de-linux/41773-la-connexion-securisee-a-distance-avec-ssh>

Questions

- Quel est l'intérêt d'utiliser les **protocoles cryptographiques** SSL ou TLS ?
- Ces deux protocoles cryptographiques sont-ils **équivalents** ?
- Quels sont les **trois critères de sécurité** que permet les protocoles cryptographiques SSL/TLS ?
- Quelles sont les différentes méthodes de chiffrement utilisées pour les échanges avec SSH ?
- Quel est le principe du chiffrement asymétriques
- Quel type de chiffrement permet l'authentification sur un serveur ?
- Quel type de chiffrement permet le chiffrement des échanges entre le client et le serveur lors des échanges SSH ?
- Quels sont les algorithmes utilisés ?

Réalisation

En utilisant

From:

[/ - Les cours du BTS SIO](#)

Permanent link:

</doku.php/reseau/debian/coursclesh?rev=1580468916>

Last update: **2020/01/31 12:08**

