1. Principe de l'authentification SSH par clé

1.1. Présentation

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

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**.

1.2. 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.

1.2.1. 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

1.2.2. 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 ?

1.2.3. Réalisation

En utilisant

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/debian/coursclessh?rev=1580468916

Last update: **2020/01/31 11:08**