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**. Cette authentification **unique** consiste donc en une **seule** authentification qui est accordée à un utilisateur afin de lui permettre d'avoir accès à **plusieurs** ressources.

- l'authentification **forte**, repose sur plusieurs facteurs d'authentification :
  - Un élément que vous **connaissez** (facteur de **connaissance**), généralement un mot de passe.
  - Un élément que vous **avez / possédez** (facteur de **possession**), tel qu'un appareil de confiance qui n'est pas facilement dupliqué, tel un téléphone ou une clé matérielle.
  - Un élément que vous **êtes** (facteur **d'inhérence**) **identifiant** votre personne, tel qu'une empreinte digitale, un scan du visage, une reconnaissance vocale ou tout autre élément **biométrique**.

Une authentification à deux facteurs (2FA) exige que l'utilisateur présente deux facteurs d'authentification de deux catégories différentes.

Exemple :

- un facteur de connaissance (mot de passe)
- et un facteur de possession (code pin sur son smartphone)

L'authentification multifactorielle ou **multi-facteurs** MFA (Multi-factor Authentication) exige que que l'utilisateur présente trois facteurs d'authentification de trois catégories différentes.

Exemple :

- un facteur de connaissance (mot de passe)
- un facteur de possession (son smartphone)
- et un facteur **d'inhérence** (empreinte digitale sur smartphone)

- l'utilisation d'un **code PIN** et d'un **mot de passe**, tous deux étant dans la catégorie **quelque chose que vous savez** n'est pas considérée comme une authentification multifactorielle.
- l'utilisation d'un **code PIN** (appartenant à la catégorie **quelque chose que vous savez**)et d'une **reconnaissance faciale** (appartenant à la catégorie **quelque chose que vous êtes**) est considérée comme une authentification multifactorielle.
- Un mot de passe n'est pas nécessaire pour bénéficier d'une solution MFA qui peut donc être entièrement sans mot de passe.

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://openclassrooms.com/fr/courses/43538-reprenez-le-controle-a-laide-de-linux/41773-la-connexion-securisee-a-distance-avec-ssh
- 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://www.onespan.com/fr/topics/authentification-multifactorielle

Questions

- Quel est l'intérêt d'utiliser les **protocoles cryptographiques** SSL ou TLS ?
- Qu'est-ce qu'est SSH ?
- Ces deux protocoles cryptographiques sont-ils **équivalents** ?
- Quels sont les **trois critères de sécurité** qui mis en oeuvre grâce aux protocoles cryptographiques SSL/TLS ?
- Quel est le principe du **chiffrement asymétriques** ?
- Quel type de chiffrement permet **l'authentification** sur un serveur pour SSH ?
- Quel type de chiffrement permet le **chiffrement des échanges** entre le client et le serveur lors des échanges SSH ?
- Quels sont les **algorithmes** utilisés ?

Schéma à réalisation

Vous devez réaliser un schéma décrivant les étapes de la création d'un canal sécurisé avec SSH, depuis l'authentification jusqu'à la sécurisation des échanges.

Réalisez votre schéma, sous forme de diagramme de séquence, en utilisant la solution en ligne PlanUML

- Site de PlantUML : https://plantuml.com/fr/
- Le guide de PlantUML : http://plantuml.com/fr/guide
- Le site pour la création du diagramme en ligne de PlantUML : http://www.plantuml.com/plantuml/uml/

Optionnel : SSH sous linux

Indiquez les **différentes** étapes et les **commandes** associées à utiliser sur un client linux (type Debian) pour mettre en place un accès SSH avec un autre serveur Linux (Type Debian).

Vous ne devez utiliser que la **ligne de commande**.