Cybersécurité - Avancée

1. Synthèse du protocole Secure Shell (SSH)

Le **protocole Secure Shell (SSH)** est un protocole de communication **sécurisé**, conçu en 1995 par **Tatu Ylönen** pour remplacer des protocoles non chiffrés comme rlogin**,** telnet**,** rcp **et** rsh. Il repose sur un échange de clés de chiffrement en début de connexion et chiffre **tous les** segments TCP (protocole de transport fiable), empêchant ainsi toute interception des données via un analyseur de paquets.

Depuis **2006**, la version **SSH-2** est **largement utilisée** dans le monde. En **2023**, l'alternative **SSH3** propose les mêmes services en s'appuyant sur HTTP/3 **et** QUIC (protocole de transport fiable et sécurisé).

Authentification SSH et sécurité des clés

SSH utilise la cryptographie asymétrique :

- **Clé publique** → Permet la connexion sur le web
- **Clé privée** → Protégée par mot de passe et stockée sur le poste local

L'agent SSH conserve le mot de passe de la clé privée durant toute la session. Des protocoles comme SCP (transfert sécurisé de fichiers entre deux ordinateurs via SSH) et SFTP (définition des extensions SSH) exploitent également cette architecture.

Sécurité du serveur et vérification des clés

Le serveur possède aussi une **clé privée**, permettant aux clients d'identifier la **clé publique**. Lors de la **première connexion**, l'**agent SSH** stocke cette clé et s'assure de sa **stabilité dans le temps**.

Si la clé change, SSH affiche une **alerte** : ✅ **Mise à jour légitime du serveur** → La connexion peut être poursuivie. ❌ **Usurpation par un pirate** → La connexion doit être abandonnée pour éviter une fuite de données confidentielles.

2. Qu'est-ce que le Hash

L'utilisation d'une fonction de **hachage** permet de ne pas stocker les mots de passe en clair dans la base mais uniquement de stocker une empreinte de ces derniers. Il est important d'utiliser un algorithme public réputé fort afin de calculer les dites empreintes. **A ce jour, MD5 ne fait plus partie des algorithmes réputés forts**.

De même, les fonctions de hachage publiques réputées fortes étant par nature à la disposition de tous, il est techniquement possible pour tout un chacun de calculer des

empreintes. Aujourd'hui, on trouve facilement sur internet des dictionnaires immenses d'empreintes MD5 précalculées et, grâce à ces données, il est aisé de retrouver instantanément le mot de passe ayant été utilisé afin de générer ces empreintes. Afin de limiter ce risque, il est conseillé d'utiliser des fonctions spécialisées appelées « fonction de dérivation de clé », telles que scrypt ou Argon2 par exemple, qui sont conçues spécifiquement pour stocker des mots de passe.

MD5 = fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier. Il a été inventé par Ronald Rivest en 1991.

3. Différentes méthodes d'encryptage

https://www.sealpath.com/fr/blog/types-de-chiffrement-guide/