SAE11 - Lot B : Accès SSH

GODET Thomas
LEMÉE Raphael
RAVELOSON Ho Koloina
RUF Victoria
VIGNEUX Florian

Sommaire

PB : En quoi le protocole SSH est-il un outil indispensable à l'hygiène informatique et à la Cybersécurité ?

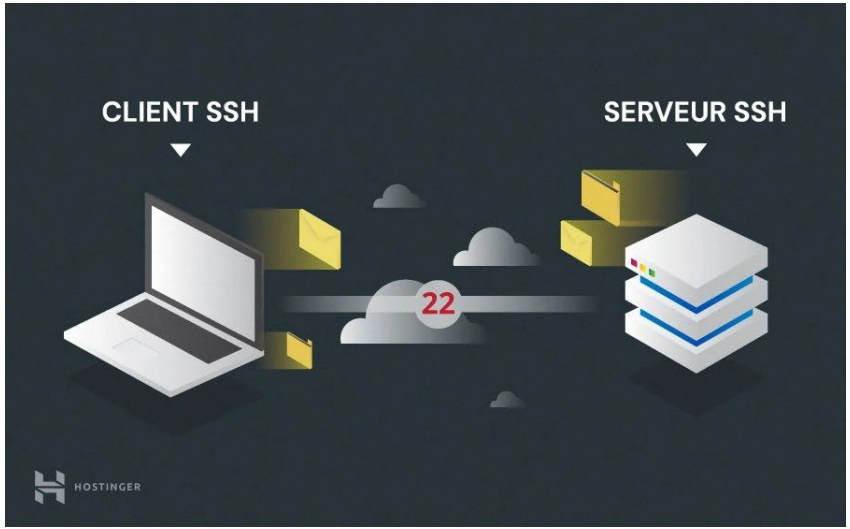
I - Présentation du protocole SSH

- SSH établi une connexion entre 2 machines
- Objectif : administrer serveur à distance
- Communication chiffrée

1 - Capacités

- Envoyer des commandes
- Transférer des fichiers à l’aide de SCP
- Mise en tunnel

2 - Principe de fonctionnement



Sous protocoles :

- SSH-USERAUTH
- SSH-TRANS
- SSH-CONNECT

II - Sécurité de connexion

1 - Méthodes d'authentification

- Avec mot de passe
- Avec clé privée / publique

Commandes utiles :

- Connexion : `ssh "UTILISATEUR_SERVEUR"@"IP_SERVEUR"`

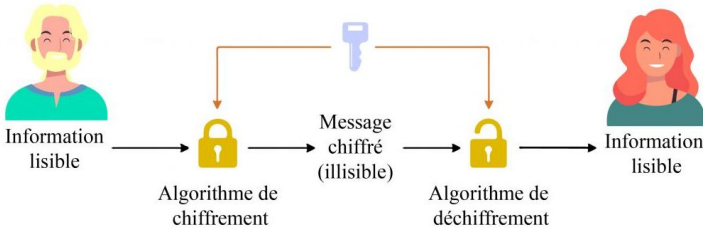
- Génération de clés : `ssh-keygen`
  - Exemple : `ssh-keygen -t ecdsa -b 256`

Phase d'authentification ➜ chiffrement asymétrique

II - Sécurité de connexion

2 - Type de chiffrement et leurs rôles

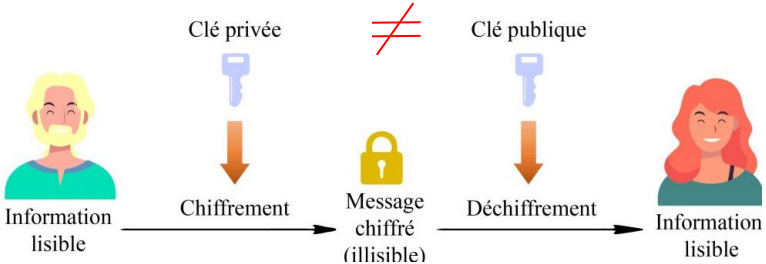
Chiffrement ***symétrique*** :



+++ chiffrer de façon rapide des volumes importants de données

- - - transmission de la clé doit être confidentielle, distribution des clés ne peut pas être utilisée à large échelle

Chiffrement ***asymétrique*** :



+++ Plus sécurisé

- - - Plus lent

III - Renforcement de la sécurité de la connexion

1 - Changement du port d'écoute

2 - Choix de l'algorithme

3 - Blocage au bout de plusieurs tentatives

- Implémentation de base
- Fail2Ban

III - Renforcement de la sécurité de la connexion

1 - Changement du port d'écoute

Objectif : Éviter une partie des menaces ➜ oblige à avoir connaissance du port défini alternativement

- Éditer fichier de configuration : `sudo nano /etc/ssh/sshd_config`
- Changer variable `Port`
- Enregistrer les modifications
- Redémarrer le service SSH : `sudo systemctl restart sshd`

III - Renforcement de la sécurité de la connexion

2 - Algorithmes

Type d'algorithme utilisé ➜ défini le niveau de sécurité de la communication SSH

Algorithmes et tailles recommandées par l'ANSSI (DSA n'est pas recommandé)

	RSA	ECDSA & EdDSA
Taille minimale recommandée (bit)	2048	256

III - Renforcement de la sécurité de la connexion

3 - Blocage au bout de plusieurs tentatives

-Implémentation de base :

Modifier la variable MaxTries dans le fichier de configuration sshd_config

-Fail2Ban (permet de bannir une IP client après plusieurs tentatives de connexion échouées) :

Commandes Fail2Ban

```
1) sudo apt install fail2ban
2) sudo apt install ssh
3) sudo systemctl start ssh
4) sudo systemctl status ssh
5) sudo systemctl start fail2ban
6) sudo systemctl status fail2ban

7) cd /etc/fail2ban
8) ls
9) sudo nano jail.local

[sshd]
Ignoreip = 192.156.10.3
Backend = systemctl
enable=tue
port=ssh
filter=ssh
logpath= /var/log/auth.log
Maxretry = 3
Bantime = 1m
```

```
10) sudo systemctl restart fail2ban
11) sudo systemctl enable fail2ban
12) sudo systemctl status fail2ban
13) ip a (sur la machine qui possède le
fail2ban)

Pour “déban” :
1) sudo fail2ban-client status
2) sudo fail2ban-client set <nom
utilisateur>unban ip <IP>
```

Conclusion :

PB : En quoi le protocole SSH est-il un outil indispensable à l'hygiène informatique et à la Cybersécurité ?

I - Présentation du protocole SSH

1 - Capacités

2 - Principes de fonctionnement

II - Sécurité de connexion

1 - Méthodes d'authentification

2 - Types de chiffrement et leurs rôles

III - Renforcement de la sécurité de la connexion

1 - Changement du port d'écoute

2 - Algorithmes

3 - Blocage au bout de plusieurs tentatives

Sources :

- Source usage sécurisé openssh Secrétariat général de la Défense et de la Sécurité nationale | Usage d'open SSH [en ligne] cyber.gouv , 23/01/2014, 23/01/2014 [consulté le 24 octobre 2024]. Disponible sur : https://cyber.gouv.fr/publications/usage-securise-dopenssh

- Source Install & param Quentin Busuttil | Installation et paramétrage Fail2Ban [en ligne] Buzut.net, 27/10/2019 [consulté le 24 octobre 2024]. Disponible sur : https://buzut.net/installer-et-parametrer-fail2ban/

- Source BAN IP Zer00CooL - Bruno | Documentation Ban IP [en ligne] Wiki unbuntu-fr, 15/03/2018, 04/10/2024 [consulté le 24 octobre 2024]. Disponible sur : https://doc.ubuntu-fr.org/fail2ban/

Images :

- Source image chiffrement symétrique Jean-Christian, Chiffrement symétrique [Schéma]. Elysiria.fr, 2015. https://www.elysiria.fr/blog/le-chiffrement-symetrique

- Source image chiffrement sauvegardes données Adrian, Chiffrement de sauvegardes de données [Schéma]. Alliance-informatique.fr, 2023. https://www.alliance-informatique.fr/revue-blog/le-chiffrement-sauvegardes-donnees/