[SSH] Serveur OpenSSH

Introduction

La bonne configuration d'un **serveur SSH** est primordiale pour sécuriser votre serveur des attaques extérieures.

C'est pourquoi je vous recommande de consulter le guide de l'ANSSI qui décrit les bonnes pratiques à avoir.

Nous verrons dans ce tutoriel, uniquement des configurations classiques et non-exhaustives.

Source

- Guide de l'ANSSI OpenSSH

Installation

Installez le paquet **openssh-server** sur votre serveur (le nom peut varier selon les distributions) :

```
sudo apt install -y openssh-server
```

Configuration

Fichier de configuration

Le fichier de configuration du serveur SSH est **/etc/ssh/sshd_config** :

```
nano /etc/ssh/sshd_config
```

> Vous pouvez activer ou désactiver des options en choisissant de les commenter ou non (caractère **#**).

Changer le port d'écoute

Option intéressante pour éviter d'être dans le viseur des bots qui brute force les serveurs SSH exposés sur Internet .

Par exemple, vous pouvez remplacer le port **22** définit par défaut par le port 2222 :

```
Port 2222
```

Changer l'interface d'écoute

Par sécurité, il peut être intéressant de définir l'interface d'écoute du serveur SSH. Par défaut, toutes les interfaces sont en écoute.

Prenons l'exemple d'un serveur appartenant à deux réseaux :

Nom du réseau	Adresse IP
LAN	192.168.1.10
DMZ	10.0.0.10

Vous pouvez donc décider d'activer l'administration par SSH **seulement via le LAN** pour protéger votre serveur grâce à l'option suivante :

```
ListenAddress 192.168.1.10
```

Connexion root

Cette option n'est pas recommandée mais elle est importante à connaître.

Elle permet d'activer ou non la connexion en root et le type d'authentification autorisé.

- Si vous souhaitez **interdire la connexion root** :

```
PermitRootLogin no
```

- Si vous souhaitez **autoriser la connexion root par mot de passe et par clé** :

```
PermitRootLogin yes
```

- Si vous souhaitez **autoriser la connexion root uniquement par clé** :

```
PermitRootLogin prohibit-password
```

Revision #1
Created 16 November 2023 09:35:31 by Elieroc
Updated 16 November 2023 09:52:19 by Elieroc