TUTOS-INFO
L'informatique par l'exemple

TUTORIEL

SECURISER DEBIAN
(règles de base)

ALERTE

SOMMAIRE

CONFIRME
DIFFICULTE

SECURISER DEBIAN 12 (règles de base)

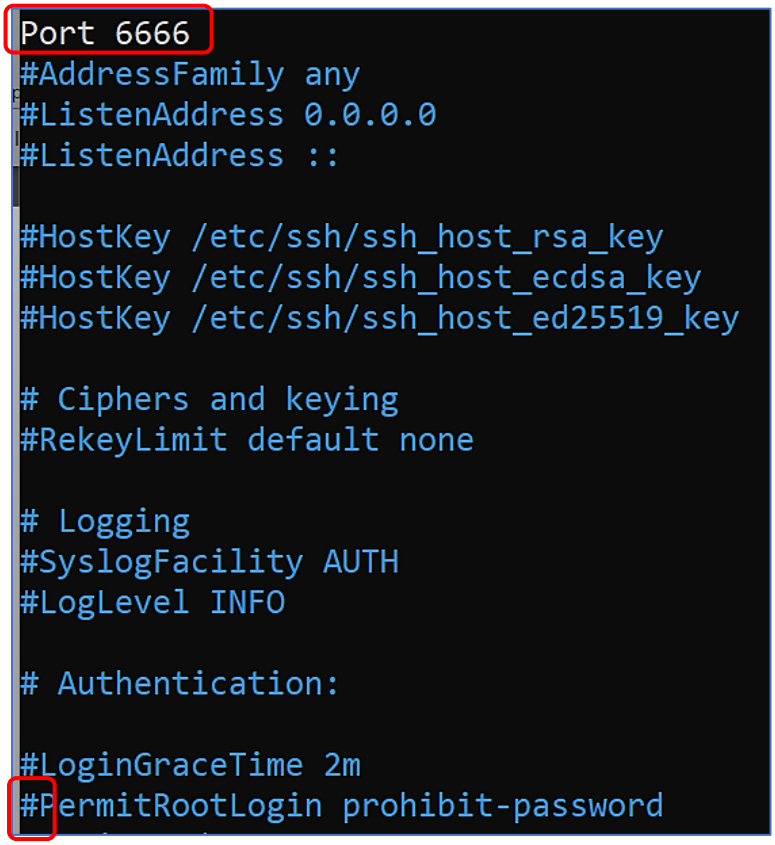
Comme pour l'hyperviseur Proxmox (voir tutoriel), il est important de sécuriser Debian 12 (règles de base).

1ère étape : désactivation de l'accès SSH pour le root et modification du port SSH par défaut

Connectez-vous en tant que « root » sur la machine Debian et éditez le fichier « sshd_config » avec la commande :

nano /etc/ssh/sshd_config

- Modifiez le port SSH par défaut (utilisez un port disponible >1024)
- Assurez-vous que le « **PermitRootLogin** » est bien commenté (#)



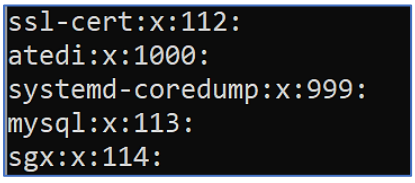
- Quittez et sauvegardez le fichier « sshd_config »
- Relancez le service SSH avec la commande :

systemctl restart ssh

2ème étape : installation de « sudo » et ajout d'un utilisateur au groupe « sudo »

Afficher les utilisateurs du système :

cat /etc/group



Afficher les groupes auxquels appartient un utilisateur :

groups nom_user

```
root@debian-atedi:~# groups atedi
atedi : atedi cdrom floppy sudo audio dip video plugdev netdev
```

Installer « sudo » :

apt install sudo -y

Affecter un utilisateur au groupe « sudo » :

usermod -aG sudo nom_user

Dorénavant, l'utilisateur « sudoer » pourra exécuter des commandes avec des privilèges « root ». Il suffira d'ajouter « sudo » devant la commande (le mot de passe de l'utilisateur sudo sera à saisir une fois).

3ème étape : installation de Fail2ban sur Debian 12

Fail2ban est un framework de prévention contre les intrusions, écrit en Python. Pour l'installer depuis le shell de la machine Debian 12, effectuez les manipulations suivantes :

1 – Installer Fail2ban sur Debian 12 (depuis la console)

apt update
apt upgrade -y
apt install fail2ban -y

2 – Copier le fichier modèle "jail.conf" en "jail.local"

cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

3 – Éditer le fichier "jail.local" et ajouter les éléments donnés ci-dessous :

nano /etc/fail2ban/jail.local

Éléments à ajouter dans le fichier "**jail.local**", puis quitter en sauvegardant les modifications :

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = journal
backend = systemd
maxretry = 2
findtime = 300
banaction = iptables-allports
bantime = 86400
ignoreip = 127.0.0.1
```

4 – Redémarrer Fail2ban et vérifier le statut

systemctl restart fail2ban
systemctl status fail2ban

COMMANDES UTILES FAIL2BAN

Bannir une IP
fail2ban-client set [nom du jail] banip [IP à bannir]

Enlever le ban d'une IP
fail2ban-client set [nom du jail] unbanip [IP concerné]

Lister les règles
fail2ban-client status

Afficher les détails d'une règle
fail2ban-client status sshd

Lister les tentatives de connexion
tail /var/log/auth.log

Lister les tentatives de connexion (en temps réel)
tail -f /var/log/auth.log

Si nécessaire créer le fichier auth.log avec droits 640 :

touch /var/log/auth.log
chmod 640 /var/log/auth.log

Si les adresses IPv6 ne sont pas gérées, la désactivation se fait au niveau du groupe [Définitions] du fichier « fail2ban.conf » :

nano /etc/fail2ban/fail2ban.conf

- Décommentez la ligne "**allowipv6**"
- Saisissez le paramètre "**no**"
- Quittez et sauvegardez le fichier

Redémarrer Fail2ban et vérifier le statut (statut « active » sans erreur)

systemctl restart fail2ban
systemctl status fail2ban

```
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-03-25 20:05:40 CET; 21h ago
       Docs: man:fail2ban(1)
   Main PID: 1194316 (fail2ban-server)
      Tasks: 7 (limit: 76819)
     Memory: 65.5M
        CPU: 1min 30.503s
     CGroup: /system.slice/fail2ban.service
             └─1194316 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
```

4ème étape : modification du mot de passe d'un compte utilisateur Debian

Pensez à sécuriser vos mots de passe (12 caractères au minimum avec des caractères alphanumériques, des symboles, des majuscules).

- Saisissez (en tant que « root » ou utilisateur « sudo ») la commande suivante :

sudo passwd nom_user

5ème étape : création de mots de passe chiffrés avec le paquet "apache2-utils"

De nos jours, les mots de passe forts sont la règle. On évitera donc les mots de passe simple et inférieurs à 12 caractères. Sur Debian, il est possible de créer des mots de passe chiffrés de la manière suivante :

- Installez le paquet "apache2-utils" avec la commande suivante :

apt install apache2-utils -y

- Créez un mot de passe chiffré de la manière suivante :

htpasswd -nb nom_user AdminDebian12!

Ici, on créé le mot de passe "AdminDebian12!" pour l'utilisateur "nom_user" (à modifier par un nom d'utilisateur de votre système Debian.

IMPORTANT – PRENEZ LE TEMPS D'AFFINER VOS REGLES DE SECURITE

Ces règles sont des bases à appliquer sur tous systèmes exposés au web. Ne négligez pas ces manipulations au risque de voir votre serveur et vos machines internes corrompues !