PENSE-BÊTE

SECURISER DEBIAN 12 AVEC FAIL2BAN ET CRÉER DES MOTS DE PASSE CHIFFRES

1ère étape : installation et configuration de Fail2ban sur Debian 12

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
```

2ème 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

3ème étape : création d'un mot de passe chiffré sur Debian 12

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.