PENSE-BÊTE

SECURISER PROXMOX 8.1 AVEC FAIL2BAN

1 – Installer Fail2ban sur l'hyperviseur (depuis le shell)

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 :

```
[proxmox]
enabled = true
port = https,http,8006
filter = proxmox
logpath = journal
backend = systemd
maxretry = 3
findtime = 2d
bantime = 1h

[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 – Configurer le filtre en éditant le fichier "proxmox.conf" et en ajoutant les éléments donnés :

nano /etc/fail2ban/filter.d/proxmox.conf

Éléments à ajouter au fichier :

```
[Definition]
failregex = pvedaemon\[.*authentication failure; rhost=<HOST> user=.* msg=.*
ignoreregex =
```

5 – 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

```
Status
|- Number of jail:      1
`- Jail list:   sshd
```

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

```
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     5
|  `- File list:       /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.21
```

Lister les tentatives de connexion
tail /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