4. Configuration de Fail2Ban

Mise en place & configuration de Fail2Ban

Installation

```
sudo apt-get install fail2ban
```

Configuration

Le fichier `/etc/fail2ban/jail.conf` contient l'ensemble des plugins que vous pouvez activer pour protéger les services de votre serveur. Pour chaque plugin les actions possibles sont commentées dans le fichier.

Mais vous ne devez pas modifier ce fichier directement. Car lors des mises à jour de votre serveur Debian, le fichier peut être remplacé à tout moment avec une version plus récente.

En fait, Fail2ban charge les configurations dans cet ordre :

- /etc/fail2ban/jail.conf
- puis /etc/fail2ban/jail.d/defaults-debian.conf
- et enfin /etc/fail2ban/jail.local **(le notre)**

On crée donc notre fichier de config perso :

```
sudo nano /etc/fail2ban/jail.local
```

Voici un exemple de configuration standard :

```
[DEFAULT]
# 1 jour de bannissement pour tous les plugins
bantime = 86400

# A host is banned if it has generated "maxretry" during the last "findtime" in seconds.
findtime  = 600
ignoreip = 127.0.0.1/8 123.456.789.123
```

```
# "maxretry" is the number of failures before a host get banned.
maxretry = 5

[sshd]
enabled = true
# 3 mots de passe erronés consécutifs et c'est le bannissement direct en SSH
maxretry = 3
```

Activation du service

```
sudo service fail2ban start
```

Pour vérifier le bon fonctionnement du service :

```
sudo service fail2ban status
```

Il est possible que sous certaine distribution fail2ban ne démarre pas avec cette configuration. Il faudra rajouter la ligne suivante dans le fichier `jail.local` dans la partie `[DEFAULT]` :

```
sshd_backend = systemd
```

puis redémarrer fail2ban.

Commandes Fail2Ban

Liste des commandes utiles pour Fail2Ban

Logs Fail2Ban

Pour savoir si fail2ban fonctionne on peut allez voir le fichier de logs :

```
sudo nano /var/log/fail2ban.log
```

Lister les prisons

```
sudo fail2ban-client status
```

Lister les bannis d'une prison

```
sudo fail2ban-client status <JAILNAME>
```

Mettre la sortie de la commande dans un fichier :

```
sudo fail2ban-client status <JAILNAME> > <FILENAME>

# Exemple
sudo fail2ban-client status sshd > ipban.txt
```

Filtrer les ip dans un fichier :

```
grep -n -w --color "<KEYWORD>" <FILENAME>

# Exemple
grep -n -w --color "192" ipban.list
```

Il est aussi possible de faire les 2 manipulations précédentes en une seule fois :

```
sudo fail2ban-client status <JAILNAME> | grep -n -w --color "<KEYWORD>"

# Exemple rechercher une chaine de caractère commençant par "192"
sudo fail2ban-client status sshd | grep -n -w --color "192"
```

Avec grep il est possible de faire des recherches avancés que ça soit dans le traitement d'une sortie de commande ou dans un fichier :

```
# Recherche REGEX avec grep
# Il est important de rajouter l'option -E pour signaler que c'est une recherche regex

# Exemple rechercher une chaine de caractère au format IPV4 -> "XX.XX.XX.XX"
grep -n -w --color -E "([0-9]{1,3}[\.]){3}[0-9]{1,3}" <FILENAME>

# Exemple rechercher une chaine de caractère au format IPV4 commençant par 192 ->
"192.XX.XX.XX"
sudo fail2ban-client status sshd | grep -n -w --color -E "192([\.][0-9]{1,3}[0-9]){3}"
```

Dé bannir une IP

```
sudo fail2ban-client set <JAILNAME> unbanip <IPBAN>
```