Fail2ban

Généralités

- Site officiel
- Fail2ban
- http://www.alsacreations.com/tuto/lire/622-Securite-firewall-iptables.html
- http://www.pablumfication.co.uk/2010/02/07/installing-configuring-fail2ban-ubuntu-9-04/

Installation

```
yum install fail2ban
apt install fail2ban
```

Configuration

Editer le fichier de configuration.

```
vi /etc/fail2ban/fail2ban.conf
```

Vérifier les valeurs suivantes.

```
#Niveau de détail des logs (défaut 3).
loglevel = INFO
#Chemin vers le fichier de log (description des actions entreprises par
fail2ban)
logtarget = /var/log/fail2ban.log
```

Les services à monitorer sont stockés dans jail.conf. Ce fichier ne doit pas être éditer. Il est expliqué dans l'entête de ne pas utiliser jail.conf mais un fichier jail.local ou un fichier dédié dans jail.d

Sous Debian, le fichier suivant est créé par défaut avec le contenu qui suit.

```
/etc/fail2ban/jail.d/defaults-debian.conf
[sshd]
enabled = true
```

Editer le fichier de configuration defaults-debian.conf. Chaque paramètre mentionné prend le pas sur le même paramètre définis globalement.

```
[DEFAULT]
destemail = your@email.here
sendername = Fail2Ban
ignoreip = 127.0.0.1
```

```
maxretry = 3
mta = ssmtp

[sshd]
enabled = true
port = <SSH_PORT>

[sshd-ddos]
enabled = true
port = <SSH_PORT>
```

Restart du service pour prise en compte

```
systemctl restart fail2ban
journalctl -u fail2ban
```

Ban persistant

- http://www.looke.ch/wp/list-based-permanent-bans-with-fail2ban

Créer un fichier qui contient une adresse IP à bannir par ligne. Le nommer `/etc/fail2ban/ip.blacklist`.

Ensuite, modifier le fichier de configuration `/etc/fail2ban/action.d/iptables.conf` en ajoutant la ligne dans `actionstart`.

```
[...]
actionstart = iptables -N fail2ban-<name>
              iptables -A fail2ban-<name> -j RETURN
              iptables -I INPUT -p <protocol> -m multiport --dports <port> -
j fail2ban-<name>
              # Persistent banning of IPs
              cat /etc/fail2ban/ip.blacklist | while read IP; do iptables -I
fail2ban-<name> 1 -s $IP -j DROP; done
[...]
actionban = iptables -I fail2ban-<name> 1 -s <ip> -j DROP
            # Persistent banning of IPs
            echo '<ip>' >> /etc/fail2ban/ip.blacklist
[...]
```

La ligne dans `actionban` permet d'ajouter de nouvelles IP dans la liste de IP à bannir tout le temps. Si elle n'est pas renseignée, les IP seront bannies le temps prévus dans la configuration (par défaut 600 secondes soit 10 minutes).