Logiciel

Fail2ban : Bannir des IP

fail2ban analyse les logs de divers services (SSH, Apache, FTP...) en cherchant des correspondances entre des motifs définis dans ses filtres et les entrées des logs.

Si une correspondance est trouvée, une ou plusieurs actions sont exécutées.

Typiquement, **fail2ban** cherche dans les fichiers journaux des tentatives répétées de connexions infructueuses et bannit l'adresse IP de la source en ajoutant une règle au pare-feu (iptables).

Si vous utilisez votre Raspberry Pi comme serveur ssh ou Web, votre pare-feu aura des `` trous '' pour laisser passer le trafic du serveur.

Pré-requis

Installation

```
pi@framboise:~ $ sudo apt install fail2ban
```

À l'installation, Fail2ban crée un dossier **/etc/fail2ban** contenant un fichier de configuration appelé **/etc/fail2ban/jail.conf** qui doit être copié en **/etc/fail2ban/jail.local** pour être activé :

```
pi@framboise:~ $ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Ce fichier de configuration contient un ensemble d'options par défaut, ainsi que des options pour vérifier des anomalies de services spécifiques.

Procédez comme suit pour examiner / modifier les règles utilisées pour ssh :éditez avec les droits d'administration le fichier **/etc/fail2ban/jail.local** pour le modifier comme ceci :

- La section [ssh] ressemble à ceci :

```
[ssh]
enabled  = true
port     = ssh
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 6
```

Cette section ssh, est activée, examine le port ssh, filtre à l'aide des paramètres /etc/fail2ban/filter.d/sshd.conf, analyse le /var/log/auth.log pour une activité malveillante, et autorise six tentatives avant que le seuil de détection ne soit atteint.

En vérifiant la section par défaut, nous pouvons voir que l'action de bannissement par défaut est:

```
# Default banning action (e.g. iptables, iptables-new,
# iptables-multiport, shorewall, etc) It is used to define
# action_* variables. Can be overridden globally or per
# section within jail.local file
banaction = iptables-multiport
```

iptables-multiport signifie que le système Fail2ban exécutera le fichier /etc/fail2ban/action.d/iptables-multiport.conf lorsque le seuil de détection est atteint.

Il existe un certain nombre de fichiers de configuration d'action différents qui peuvent être utilisés. Multiport interdit tous les accès sur tous les ports.

Si vous souhaitez interdire définitivement une adresse IP après trois tentatives infructueuses, vous pouvez modifier la valeur maxretry dans la section [ssh] et définir le bantime sur un nombre négatif:

```
[ssh]
enabled  = true
port     = ssh
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 3
bantime = -1
```

Configuration

Utilisation

Désinstallation

Voir aussi

- **(en)** https://www.digitalocean.com/community/tutorials/how-fail2ban-works-to-protect-services-on-a-linux-server

---

Basé sur « Bannir des IP avec fail2ban » par Wiki ubuntu-fr.