Fail2ban contre les attaques brutes-force

Si vous être propriétaire d'un serveur quelconque connecté à Internet, vous n'êtes pas sans savoir qu'il est exposé à de nombreuses attaques. Parmi elles, le brute-force. Cette attaque consiste à trouver votre mot de passe SSH en les essayant tous les uns à la suite des autres ou en utilisant des dictionnaires (ce sont des listes contenant les mots de passe les plus utilisés comme admin, 123456, etc...). Ces attaques sont généralement menées par des robots qui visent des dizaines de serveurs en même temps. Il se connectent sans cesse à votre serveur grâce à votre port SSH et essayent beaucoup de combinaisons de mot de passe jusqu'à trouver le bon (généralement, une tentative est menée toutes les 2 à 3 secondes).

Enfin, fois que les pirates ont accès à un serveur, ils peuvent par exemple s'en approprier pour exécuter d'autres attaques brute-force contre d'autres serveurs, ou bien utiliser votre serveur pour spammer des gens (par mail, par exemple). De plus, le responsable, si il y a une plainte car des attaques ont été menées depuis votre serveur, c'est vous (à moins que vous ne démontriez que vous avez vous-même été victime d'attaque et que vous n'avez plus le contrôle sur votre serveur, d'où l'importance de conserver vos logs).

Il existe beaucoup de solutions, celle que je vais vous présenter aujourd'hui, c'est Fail2ban (d'autres méthodes seront proposés dans de futurs articles). Fail2ban est un programme qui analyse vos logs système afin de détecter les attaques brute-force et ainsi bloquer l'adresse IP attaquante.

Vous pouvez consulter la manuel en anglais Fail2Ban Configuration

Installer Fail2ban

La commande suivante permet d'installer **fail2ban** avec les systèmes **Debian** et dérivées :

```
sudo apt install fail2ban
```

```
cedric@rpiluc001:~ $ sudo apt install fail2ban
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  python3-pyinotify python3-systemd
Paquets suggérés :
  monit python-pyinotify-doc
Les NOUVEAUX paquets suivants seront installés :
  fail2ban python3-pyinotify python3-systemd
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 446 ko dans les archives.
Après cette opération, 2 153 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://raspbian.raspberrypi.org/raspbian buster/main armhf fail2ban all 0.10.2-2.1 [385 kB]
Réception de :2 http://raspbian.raspberrypi.org/raspbian buster/main armhf python3-pyinotify all 0.9.6-1 [26,9 kB]
Réception de :3 http://raspbian.raspberrypi.org/raspbian buster/main armhf python3-systemd armhf 234-2+b1 [34,1 kB]
446 ko réceptionnés en 3s (174 ko/s)
Sélection du paquet fail2ban précédemment désélectionné.
(Lecture de la base de données... 54825 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../fail2ban_0.10.2-2.1_all.deb ...
Dépaquetage de fail2ban (0.10.2-2.1) ...
Sélection du paquet python3-pyinotify précédemment désélectionné.
Préparation du dépaquetage de .../python3-pyinotify_0.9.6-1_all.deb ...
Dépaquetage de python3-pyinotify (0.9.6-1) ...
Sélection du paquet python3-systemd précédemment désélectionné.
Préparation du dépaquetage de .../python3-systemd_234-2+b1_armhf.deb ...
Dépaquetage de python3-systemd (234-2+b1) ...
Paramétrage de fail2ban (0.10.2-2.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /lib/systemd/system/fail2ban.service.
[fail2ban-tmpfiles.conf:1] Line references path below legacy directory /var/run/, updating /var/run/fail2ban → /run/fa
il2ban; please update the tmpfiles.d/ drop-in file accordingly.
Paramétrage de python3-pyinotify (0.9.6-1) ...
Paramétrage de python3-systemd (234-2+b1) ...
Traitement des actions différées (« triggers ») pour man-db (2.8.5-2) ...
Traitement des actions différées (« triggers ») pour systemd (241-7~deb10u5+rpi1) ...
cedric@rpiluc001:~ $
```

Configurer fail2ban

Éditons le fichier `/etc/fail2ban/jail.local`

Liste des fichiers et dossier de configuration par défaut de **fail2ban** sous **Raspbian 10** :

```
action.d/             fail2ban.d/          jail.conf            paths-
arch.conf      paths-debian.conf
fail2ban.conf         filter.d/            jail.d/              paths-
common.conf    paths-opensuse.conf
```

Il y a deux fichiers principaux de configuration pour **fail2ban** : `/etc/fail2ban/fail2ban.conf` et `/etc/fail2ban/jail.conf`. D'autres fichiers complémentaires peuvent être dans `/etc/fail2ban/filter.d/*.conf` et `/etc/fail2ban/action.d/*.conf`

`/etc/fail2ban/fail2ban.conf` est le fichier de configuration pour le paramétrage du démon **fail2ban**. Il s'agit des paramètres **loglevel**, fichier **log**, **port**, **socket** et **pid**.

`/etc/fail2ban/jail.conf` est le fichier des recettes avec des **filtres** et des **actions**. Il permet de définir les règles de bannissements.

Les **filtres** qui spécifient les règles de détections d'échec d'identification sont à ajouter au dossier **filter.d**

Les **actions** qui définissent les règles de bannissement ou non des adresses IP sont à ajouter au dossier **filter.d**

Il est vivement conseillé d'apporter des modifications de configuration dans des fichiers nommés **fail2ban.local** et **jail.local**. Ou ajoutez des fichiers aux dossiers `fail2ban.d/` et `jail.d/`.

L'ordre de chargement des fichiers de configuration est le suivant :

1. jail.conf
2. jail.d/*.conf (dans l'ordre alphabétique)
3. jail.local
4. jail.d/*.
5. local (dans l'ordre alphabétique).

Modifications apportées à fail2ban

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

Pour ajouter les options suivantes :

```
[DEFAULT]
ignoreip = 127.0.0.1/8
bantime  = 600
maxretry = 2
destemail = root@localhost
action = %(action_mwl)s

[sshd]
enabled  = true
```

Avec **ignoreip**, les IPs qui seront spécifiées sur cette ligne ne seront par bloquées. Je vous conseille de laisser l'adresse actuelle (qui doit être 127.0.0.1/8), d'y ajouter un espace afin de la séparer et d'y mettre votre adresse (ainsi que celles de toutes les personnes qui sont susceptibles d'accéder à votre serveur sans pour autant l'attaquer)

bantime est le nombre de secondes qu'une adresse va être bloquée si elle attaque votre serveur. 10 minutes est très peu suffisant, un rapide calcul vous permet d'en être sûr. Admettons que vous êtes attaqué par 20 machines différentes, toutes à 1 mot de passe toutes les 2 secondes. Vous avez donc 10 tentatives par seconde. Si fail2ban bloque au bout de 6 tentatives par IP, 120 mots de passe sont essayés toutes les 10 minutes, soit 16 800 par jour. Donc, 10 minutes ne représentent pas grand chose face au nombre de machines qui vous attaquent.

maxretry est le nombre de tentatives auxquelles a le droit un utilisateur avant de se faire bloquer.

destemail est l'adresse mail à laquelle seront envoyés les mails de notification (quand une adresse sera bloquée)

action permet d'effectuer des actions.
`action = %(action_mw)s` permet de bannir et d'envoyer un mail avec le pays ou l'email d'abuse concernant l'IP qui a été bannie.

`action = %(action_mwl)s` ajoute les lignes de logs ou apparaissent l'IP correspondante

Ajouter les règles spécifiques

```
[sshd]
enabled = true
port = 1234


[postfix]
port = smtp,submission
enabled = true

[dovecot]
port = imaps
enabled = true
```

N'oubliez pas de redémarrer le service `sudo service fail2ban restart`