14/10/2015

Installation du service Fail2Ban

V1

Lecaudey Etienne

SOMMAIRE :

Table des matières

Tutoriel 1.1 : Installation du service Fail2Ban		
Lecaudey Etienne	Version 1.0	14/10/2015

Objectifs :

L'objectif de cette procédure est de procéder à l'installation du service Fail2Ban

Fail2ban lit les logs de divers services (SSH, Apache, FTP…) à la recherche d'erreurs d'authentification répétées et ajoute une règle iptables pour bannir l'adresse IP de la source.

Information sur les versions:

VM	Debian 8.1	Jessie	192.168.1.125

Installation des services :

Avant toute Installation, il faut réaliser une mise à jour des paquets :

```
apt-get update
```

Pour installer le paquet lancez la commande suivante :

```
apt-get install fail2ban_
```

Configuration de base :

Par défaut, le blocage par défaut est de (600s), un blocage de 1h est plus réaliste (3600s)

Attention, changer le bantime n'agit pas sur le findtime, l'inconvénient d'un grand 'findtime' pousse fail2ban à analyser de plus longs fichiers de logs ce qui pénalise les performances

Maintenant, il faut veiller à ajouter en liste blanche vos adresses ip, car l'erreur est humaine et on veut éviter de se bloquer nous-même l'accès au serveur. La liste 'ignoreip' est séparée d'espace, donc si votre IP est 192.168.1.125 ajoutez là à la liste ignoreip

Éditez le fichier **/etc/fail2ban/jail.conf** :

```
[DEFAULT]
ignoreip = 127.0.0.1 192.168.1.125
# ignorecommand = /path/to/command <ip>
ignorecommand =
# "bantime" is the number of seconds that a host is banned.
bantime  = 86400
# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime = 3600
maxretry = 3
```

Pour spécifier à **fail2ban** quels services il doit surveiller, éditez le fichier **/etc/fail2ban/jail.conf**

Dans la partie *jail* vous trouverez des blocs du type :

```
[ssh]

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

Relancez la configuration avec

```
root@debianetienne:/# service fail2ban reload
[ OK ] Reloading authentication failure monitor: fail2ban.
```

Vérification du fonctionnement de Fail2ban :

Côté serveur avec la commande :

```
service fail2ban status ssh
```

Qui peut vous retourner le statuts de la prison 'ssh' avec le nombre de tentative échouée et la liste des IP banni