4.7 Mise en place de fail2ban couplé à iptables

4.7.1 Objectifs pédagogiques

- ➢ *Savoir installer et configurer fail2ban*
- ➢ *Comprendre le fonctionnement de fail2ban*
- ➢ *Coupler fail2ban avec iptables*

4.7.2 Introduction

Fail2ban est un service qui surveille les logs de comportement malveillant (tentative de connexions, DDoS, etc.) et qui inscrit dynamiquement des règles de bannissement dans iptables. Fail2ban est compatible avec un grand nombre de services (apache, ftp, sshd,...).

4.7.3 Installation de Fail2ban

Comme pour chaque application sous Linux, l'installation se fait via le dépôt de paquets.

```
apt install fail2ban
```

4.7.4 Activation du service

```
systemctl enable fail2ban
```

Tous les fichiers de configuration sont situés dans fichier jail.local aura la précédence sur le fichier /etc/fail2ban jail.conf. Les valeurs par défaut sont situées dans un fichier jail.conf, dans l'ordre.

- /etc/fail2ban/jail.conf
- /etc/fail2ban/jail.d/*.conf, alphabetically
- /etc/fail2ban/jail.local
- /etc/fail2ban/jail.d/*.local, alphabetically

4.7.5 Activation des règles

Créer un fichier /etc/fail2ban/jail.local avec ce contenu :

```
[DEFAULT]
# Ban hosts for one hour:
bantime = 3600
# Override /etc/fail2ban/jail.d/00-firewalld.conf:
banaction = iptables-multiport
[sshd]
enabled = true
[recidive]
enabled = true
```

Démarrer fail2ban

```
systemctl start fail2ban
systemctl status fail2ban
```

```
fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2020-02-01 17:16:01 CET; 1min 11s ago
     Docs: man:fail2ban(1)
 Main PID: 10737 (fail2ban-server)
    Tasks: 3 (limit: 4915)
   Memory: 13.6M
   CGroup: /system.slice/fail2ban.service
           └─10737 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

févr. 01 17:16:01 Predator systemd[1]: Starting Fail2Ban Service...
févr. 01 17:16:01 Predator systemd[1]: Started Fail2Ban Service.
févr. 01 17:16:01 Predator fail2ban-server[10737]: Server ready
```

Surveiller fail2ban

```
fail2ban-client status
```

```
Status
|- Number of jail:  1
`- Jail list:sshd
```

Plus précisément :

```
fail2ban-client status sshd
```

```
Status for the jail: sshd
|- Filter
|  |- Currently failed:   0
|  |- Total failed: 0
|  `- File list:    /var/log/auth.log
`- Actions
   |- Currently banned:   0
   |- Total banned: 0
   `- Banned IP list:
```

Exemple sur un serveur en production depuis 1 an environ :

```
Status for the jail: sshd
|- Filter
|  |- Currently failed:   11
|  |- Total failed: 14238
|  `- File list:    /var/log/auth.log
`- Actions
   |- Currently banned:   7
   |- Total banned: 2227
```

```
   `- Banned IP list:     122.51.179.14 142.93.47.125 222.186.180.223 51.79.70.223
178.128.215.16 217.7.251.206 132.232.52.60
```

4.7.6 Aller plus loin avec fail2ban

- Lire le fichier /etc/fail2ban/jail.conf et s'en inspirer pour personnaliser le module ssh.
- Le dossier /etc/fail2ban/filter.d/ donne une idée des applications supportées.
- [Améliorez la sécurité de vos serveurs avec Fail2Ban]

```
roger@Predator:/etc$ ls /etc/fail2ban/filter.d/
3proxy.conf                exim-spam.conf          portsentry.conf
apache-auth.conf           freeswitch.conf         postfix.conf
apache-badbots.conf        froxlor-auth.conf       proftpd.conf
apache-botsearch.conf      groupoffice.conf        pure-ftpd.conf
apache-common.conf         gssftpd.conf            qmail.conf
apache-fakegooglebot.conf  guacamole.conf          recidive.conf
apache-modsecurity.conf    haproxy-http-auth.conf  roundcube-auth.conf
apache-nohome.conf         horde.conf              screensharingd.conf
apache-noscript.conf       ignorecommands          selinux-common.conf
apache-overflows.conf      kerio.conf              selinux-ssh.conf
apache-pass.conf           lighttpd-auth.conf      sendmail-auth.conf
apache-shellshock.conf     mongodb-auth.conf       sendmail-reject.conf
assp.conf                  monit.conf              sieve.conf
asterisk.conf              murmur.conf             slapd.conf
botsearch-common.conf      mysqld-auth.conf        sogo-auth.conf
common.conf                nagios.conf             solid-pop3d.conf
counter-strike.conf        named-refused.conf      squid.conf
courier-auth.conf          nginx-botsearch.conf    squirrelmail.conf
courier-smtp.conf          nginx-http-auth.conf    sshd.conf
cyrus-imap.conf            nginx-limit-req.conf    stunnel.conf
directadmin.conf           nsd.conf                suhosin.conf
domino-smtp.conf           openhab.conf            tine20.conf
dovecot.conf               openwebmail.conf        uwimap-auth.conf
dropbear.conf              oracleims.conf          vsftpd.conf
drupal-auth.conf           pam-generic.conf        webmin-auth.conf
ejabberd-auth.conf         perdition.conf          wuftpd.conf
exim-common.conf           phpmyadmin-syslog.conf  xinetd-fail.conf
exim.conf                  php-url-fopen.conf      zoneminder.conf
```

4.7.7 Travaux Pratiques

Afin de se familiariser un peu plus avec fail2ban, je vous propose de réaliser l'exercice suivant :

https://www.it-connect.fr/premiers-pas-avec-fail2ban/