Fail2ban pour Nextcloud sur Debian10 (Turnkey16)

Difficulté

Moyen

https://docs.nextcloud.com/server/latest/admin_manual/installation/harden_server.html#setup-fail2ban

HAProxy

- Régler pour obtenir les IPs de connexion tout en étant derrière le proxy: HAProxy

Fail2ban

source: https://linuxize.com/post/install-configure-fail2ban-on-debian-10/

- fail2ban est configuré d'origine sur ct Turnkey.

```
#systemctl status fail2ban
```

  le confirme

- installer `whois` pour des infos plus détaillées sur les IPs bloquées

```
# apt-get install whois
```

- copier le fichier de configuration d'origine qui ne doit pas être modifié

```
# cp /etc/fail2ban/jail.{conf,local}
```

- paramétrer dans cette copie

```
# nano /etc/fail2ban/jail.{conf,local}
     ...
     ignoreip = 127.0.0.1/8  IPs.reseau.lan.local/24   si besoin
     ...
     bantime  = 60m
     ...
     findtime  = 10m
     ...
     maxretry = 5
     ...
     destemail = admin@domain.tld
     ...
     action = %(action_mw)s
     ...
```

```
# systemctl restart fail2ban
```

- Activer les jails:
  Le plus simple est de faire ça dans webmin. Activer toutes les jails apache et SSL.

Pour Joomla

Malheureusement les jails de fail2ban ne suffisent pas car ce n'est pas Apache qui logge pas les tentatives d'identification mais Joomla!
Sources: https://www.joomla-security.de/server/joomla-login-mit-fail2ban-schuetzen.html et https://www.andrehotzler.de/de/blog/technology/62-joomla-login-mit-fail2ban-schuetzen.html

- créer le filtre:

```
# nano /etc/fail2ban/filter.d/joomla-login-errors.conf
     [Definition]
     failregex = ^.*INFO
<HOST>.*joomlafailure.*(Benutzername|Username|utilisateur).*
```

- créer la jail:

```
# nano /etc/fail2ban/jail.d/joomla-login-errors.conf
     [joomla-login-errors]
     enabled = true
     filter = joomla-login-errors
     port   = http,https
     logpath = /var/www/joomla/administrator/logs/error.php
```

-
```
# systemctl restart fail2ban
```

Restreindre l'accès au répertoire d'administration

- Dans la config d'Apache:

```
# nano /etc/apache2/sites-available/joomla.conf

et ajouter:
     <Directory /var/www/joomla/administrator>
         Order Deny,Allow
         Deny from all
         Allow from ip1.ou.bien.réseau1/24 ip2.ou.bien.réseau.2/24
```

```
    </Directory>
```

- `# systemctl restart apache2`