Fail2ban pour Nextcloud sur Ubuntu22

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 n'est pas installé d'origine sur un CT Ubuntu.

```
# apt-get install fail2ban
```

- 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.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: activer toutes les jails apache et SSL. `sshd`, `dropbear`, `apache-auth`, `apache-`

badbots, apache-noscript, apache-overflows, apache-nohome, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-shellshock.

```
# nano /etc/fail2ban/jail.local
----
[sshd]
...
enabled = true
----
```

Pour Nextcloud

Malheureusement les jails de fail2ban ne suffisent pas car ce n'est pas Apache qui logge pas les tentatives d'identification mais Nextcloud!

le filtre:

```
# nano /etc/fail2ban/filter.d/nextcloud.conf

     [Definition]
     _groupsre = (?:(?:,?\s*"\w+":(?:"[^"]+"|\w+))*)
     failregex =
^\{%(_groupsre)s,?\s*"remoteAddr":"<HOST>"%(_groupsre)s,?\s*"message":"Login
failed:
^\{%(_groupsre)s,?\s*"remoteAddr":"<HOST>"%(_groupsre)s,?\s*"message":"Trust
ed domain error.
     datepattern = ,?\s*"time"\s*:\s*"%%Y-%%m-%%d[T ]%%H:%%M:%%S(%%z)?"
```

la jail:

```
# nano /etc/fail2ban/jail.d/nextcloud.local
     [nextcloud]
     backend = auto
     enabled = true
     port = 80,443
     protocol = tcp
     filter = nextcloud
     logpath = /var/www/nextcloud-data/nextcloud.log
```

- `# systemctl restart fail2ban`

l'action:

```
# nano /etc/fail2ban/action.d/opnsense.conf
     # Fail2Ban configuration file
     # from triumvirat.org

     [Definition]

     actionban = /root/fail2ban-IP.sh ban <ip>
     actionunban = /root/fail2ban-IP.sh unban <ip>
```

Général

Placer la nouvelle action dans /etc/fail2ban/jail.local

```
...
banaction = opnsense
...
```

```
# systemctl restart fail2ban
# systemctl status fail2ban
```

Communiquer avec OPNSense

Il faut créer un petit script:

```
# nano fail2ban-IP.sh
```

```
#!/bin/sh
KEY="la_clé"
SECRET="le_mot_de_passe"
FWIP="ip.de.la.OPNSense"
FWPORT="n°_de_port"
ALIAS="fail2ban_CT_Joomla"
if [ $1 = "ban" ]; then
TODO="add"
elif [ $1 = "unban" ]; then
TODO="delete"
fi
curl -X POST -d '{"address":"'$2'"}' -H "Content-Type: application/json" -k
-u $KEY:$SECRET https://$FWIP:$FWPORT/api/firewall/alias_util/$TODO/$ALIAS
```

- La clé et le mot de passe sont les identifiants API de l'utilisateur créé à cet effet
- le n° de port est celui utilisé pour la connexion https à l'interface web
- l'alias est celui utilisé pour la règle de blocage du firewall

```
# chmod 600 fail2ban-IP.sh
# chmod +x fail2ban-IP.sh
```

Pour tester le script:

```
# ./fail2ban-IP.sh ban 192.168.1.1
# ./fail2ban-IP.sh unban 192.168.1.1
```

et pour finir:

```
# fail2ban-client set joomla-login-errors banip 192.168.1.1
# fail2ban-client set joomla-login-errors unbanip 192.168.1.1
```