mod_evasive - Protection basique contre DoS, DDoS, et bruteforce

Information

Testé sur debian 8.

mod_evasive est un module pour apache2, permettant de contrer des attaques DoS, et DDoS simples (peu violentes) et des tentatives de bruteforce sur les pages de login. Il analyse le nombre de connexions sur une page durant un intervale et bannit temporairement les IP associés à ces connexions.

Ceci est une protection basique et freinera des script kiddies, mais en aucun cas une attaque d'envergure.

Installation

Pour l'installer :

```
apt install fail2ban
```

Et activez le module :

```
a2enmod evasive
```

Configuration

Il faut ajouter le bloc suivant dans votre fichier de vhost apache2. On peut choisir un bloc unique pour tout les sites, ou bien configurer pour chaque site, à vous de voir comment faire dans vos vhosts et ce qui vous conviens.

```
<IfModule mod_evasive20.c>
```

```
    DOSHashTableSize    3097
    DOSPageCount        15
    DOSSiteCount        150
    DOSPageInterval        1
    DOSSiteInterval        1
    DOSBlockingPeriod    10
    DOSLogDir            "/var/lock/mod_evasive"
    #DOSEmailNotify       email@email.com
    #DOSSystemCommand    "su - someuser -c '/sbin/... %s ...'"
    #DOSWhitelist        127.0.0.1
    #DOSWhitelist        127.0.0.*
</IfModule>
```

Une fois la configuration modifiée :

```
service apach2 reload
```

Voici l'explication des paramètres :

`DOSHashTableSize` : Taille de la table de hash, plus la valeur est élevée, plus le traitement sera rapide, au détriment de la consommation de ressources.

`DOSPageCount` : Nombre d'appel d'une page par une IP avant blocage.

`DOSSiteCount` : Nombre d'appel sur un site par une IP avant blocage.

`DOSPageInterval` : Intervalle de prise en compte des appels d'une page avant blocage.

`DOSSiteInterval` : Intervalle de prise en compte des appels d'un site avant blocage.

`DOSBlockingPeriod` : Durée du ban en secondes.

Le reste des paramètres est assez explicite, attention à configurer l'envoi de mails par votre serveur si vous voulez en profiter.

`DOSSystemCommand` permet des actions lors d'un ban, comme le blocage par iptables, ou bien l'envoi d'une commande à un routeur.

Les valeurs fournies ici sont supérieurs à celles par défaut. Cela évite des problèmes avec des sites web ayant beaucoup d'appels de script, comme Wordpress ou Nextcloud. Il peut être nécessaire des les augmenter encore, par exemple avec l'application mobile Piwik, qui effectue beaucoup d'appels au serveur. Bref, pensez à tester la charge et adapter ces valeurs.

Test

Il est possible de tester la protection avec un script perl fourni par le module.

Il faut executer la commande suivante :

```
perl /usr/share/doc/libapache2-mod-evasive/examples/test.pl
```

Des connexions seront testés en masse depuis 127.0.0.1, d'abord acceptées (code http 200), puis refusées une fois les valeurs configurées dépassées (code http 403).

Sources

digitalocean.com - linode.com - wiki.debian-fr.xyz - blog.nicolargo.com - parkroad.co.za