Protéger un serveur apache d'un déni de service (DOS)

Le Déni de service (DoS) est une attaque ayant pour but de rendre indisponible un service de la machine ou un réseau pour ses utilisateurs destinés, comme d'interrompre ou de suspendre les services d'un hôte connecté à Internet temporairement ou indéfiniment.
Un déni de service distribué (DDoS) est le faite d'impliquer une multitude de source souvent des PC “zombies” dans l'attaque, donc des milliers de adresses IP unique.

On appelle « attaque par déni de service » toutes les actions ayant pour résultat la mise hors ligne d'un serveur.
Dans les faits, les attaques par déni de service sont opérées en saturant la bande passante d'un serveur défini.
wikipedia.org

Les attaques par déni de service distribuées sont plus difficiles à contrer.
Le principe même de l'attaque par déni de service distribuée est de diminuer les possibilités de stopper l'attaque.

Les attaques par déni de service non distribuées peuvent être contrées en identifiant l'adresse IP de la machine émettant les attaques et en la bannissant au niveau du pare-feu (iptables).

Comment, protéger notre serveur apache pour qu'il remonte ce genre d'attaque ?

Le “mod_evasive” est un module Apache pour contrer les attaques DOS.
Celui-ci est par exemple capable de détecter lorsqu'un utilisateur demande un trop grand nombre de pages sur un site web, sur un délai de temps très court.
Voici comment l'installer et le configurer pour une utilisation basique.

Installation du module

Sous Debian ou équivalent :

```
aptitude install libapache2-mod-evasive
```

Configuration de mod-evasive

Toute la configuration de se trouve dans le fichier Sous Debian ou équivalent :

```
 /etc/apache2/mods-available/evasive.conf
```

Voici ce que contient le fichier configuration :

```
<IfModule mod_evasive20.c>
#DOSHashTableSize    3097
#DOSPageCount        2
#DOSSiteCount        50
```

```
#DOSPageInterval     1
#DOSSiteInterval     1
#DOSBlockingPeriod   10
#DOSEmailNotify      you@yourdomain.com
#DOSSystemCommand    "su - someuser -c '/sbin/... %s ...'"
#DOSLogDir           "/var/log/mod_evasive"
</IfModule>
```

Voici, quelques directives décrites brièvement :

- **DOSHashTableSize** : Taille de la table hash, plus grande est la valeur, plus de mémoire sera nécessaire pour parcourir la table, plus la valeur sera petite, plus le parcourt de la table sera rapide.
- **DOSPageCount** : Définie le nombre de fois ou une page peut être appelée par la même adresse IP avant que celle-ci soit bloquée.
- **DOSSiteCount** : Définie le nombre de fois ou un site peut être demandé par la même adresse IP avant que celle-ci soit bloquée.
- **DOSPageInterval** : Détermine un intervalle en seconde qui autorise l'affichage de la même page avant un blocage.
- **DOSSiteInterval** : Détermine un interval en seconde qui autorise l'affichage d'un même site avant un blocage.
- **DOSBlockingPeriod** : Période en seconde pendant laquelle l'IP sera bloquée (vous recevrez un forbidden).
- **DOSEmailNotify** : Permet qu'un mail soit envoyé à chaque blocage d'adresses IP.
- **DOSSystemCommand** : Permet de définir une commande bien précise en cas d'attaque (bannissement de l'adresse IP dans IPTables par exemple).
- **DOSLogDir** : Détermine le chemin ou seront stockés les logs d'attaques.
- **DOSWhitelist** : Définie une liste blanche d'adresse IP.

Une configuration que j'utilise :

```
<IfModule mod_evasive20.c>
  DOSHashTableSize    3097
  # Pas plus de 200 pages en 100 seconde
  DOSPageCount        200
  DOSSiteCount        100
  # Pas plus de 1 requetes par seconde (images, CSS...)
  DOSPageInterval     1
  DOSSiteInterval     1
  # Periode en seconde pendant laquelle on bloque le client
  DOSBlockingPeriod   10
  #DOSEmailNotify      you@yourdomain.com
  #DOSSystemCommand    "su - someuser -c '/sbin/... %s ...'"
  # Dossier contenant les IP blaclistes
  DOSLogDir           "/var/log/mod_evasive"
</IfModule>
```

Pensez à remplacer you@yourdomain.com

Création du répertoire qui contiendra les logs :

```
mkdir /var/log/mod_evasive
chown :www-data /var/log/mod_evasive
chmod 771 /var/log/mod_evasive
```

Activation du module dans apache :

```
a2enmod evasive
```

Testez vos configuration

Maintenant que mod_evasive est configuré correctement, nous allons tester, si notre serveur à la protection anti DoS à l'aide ab (Apache Benchmark).
Installez ab si vous ne l'avez pas en tapant:

```
aptitude install apache2-utils
```

Vérification de nos stat dans /var/log/mod_evasive

```
root@test:~# ls -l /var/log/mod_evasive/
total 0
root@test:~#
```

Ensuite Nous allons maintenant envoyer des demandes en vrac sur le serveur, ce qui provoquera une attaque DOS en tapant :

```
ab -n 100 -c 10 http://test.domaine.com/
```

```
This is ApacheBench, Version 2.3 <$Revision: 1604373 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking test.domaine.com (be patient).....done


Server Software:        Apache
Server Hostname:        test.domaine.com
Server Port:            80

Document Path:          /
Document Length:        0 bytes

Concurrency Level:      10
Time taken for tests:   0.365 seconds
Complete requests:      100
Failed requests:        40
   (Connect: 0, Receive: 0, Length: 40, Exceptions: 0)
Non-2xx responses:      100
```

```
Total transferred:      26020 bytes
HTML transferred:       8360 bytes
Requests per second:    273.84 [#/sec] (mean)
Time per request:       36.518 [ms] (mean)
Time per request:       3.652 [ms] (mean, across all concurrent requests)
Transfer rate:          69.58 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:        6    8   2.1      6      14
Processing:    13   25  46.2     13     236
Waiting:       13   25  46.2     13     236
Total:         19   33  46.7     21     249

Percentage of the requests served within a certain time (ms)
  50%     21
  66%     22
  75%     23
  80%     24
  90%     38
  95%    225
  98%    236
  99%    249
 100%    249 (longest request)
```

Vérifier vos fichier log apache, mon petit doigt, me dit que le calme devrait avoir cesser 🤣

```
[Wed Jan 27 10:49:24.580491 2016] [evasive20:error] [pid 13449] [client
xxx.xxx.xxx.xxx:38389] client denied by server configuration:
[Wed Jan 27 10:49:24.587827 2016] [evasive20:error] [pid 13451] [client
xxx.xxx.xxx.xxx:38390] client denied by server configuration:
[Wed Jan 27 10:49:24.590058 2016] [evasive20:error] [pid 13452] [client
xxx.xxx.xxx.xxx:38392] client denied by server configuration:
[Wed Jan 27 10:49:24.590559 2016] [evasive20:error] [pid 13448] [client
xxx.xxx.xxx.xxx:38391] client denied by server configuration:
[Wed Jan 27 10:49:24.590587 2016] [evasive20:error] [pid 13474] [client
xxx.xxx.xxx.xxx:38393] client denied by server configuration:
[Wed Jan 27 10:49:24.601284 2016] [evasive20:error] [pid 13450] [client
xxx.xxx.xxx.xxx:38394] client denied by server configuration:
[Wed Jan 27 10:49:24.607367 2016] [evasive20:error] [pid 13451] [client
xxx.xxx.xxx.xxx:38395] client denied by server configuration:
[Wed Jan 27 10:49:24.609893 2016] [evasive20:error] [pid 13449] [client
xxx.xxx.xxx.xxx:38396] client denied by server configuration:
[Wed Jan 27 10:49:24.614346 2016] [evasive20:error] [pid 13450] [client
xxx.xxx.xxx.xxx:38398] client denied by server configuration:
[Wed Jan 27 10:49:24.614491 2016] [evasive20:error] [pid 13452] [client
xxx.xxx.xxx.xxx:38397] client denied by server configuration:
```