Muchas veces montamos un servidor, ya sea web o de aplicaciones, y no somos conscientes de que está expuesto a la red; con los problemas de seguridad que eso conlleva. No lo somos, hasta que se nos cae el servicio sin saber muy bien por qué o instalamos una herramienta como logwatch, fail2ban o mod_evasive y somos conscientes de los ataques constantes que realiza nuestro server.

Pues bien, en éste artículo, vamos a configurar el módulo de apache httpd ModEvasive para que nos ayude a reducir las consecuencias de esos ataques en nuestras máquinas.

1) Verificamos que estamos al día con nuestros paquetes

```
  # apt-get update -y
# apt-get upgrade -y
```

2) Instalaremos mod_evasive

```
 # apt-get install libapache2-mod-evasive
```

verificando que está instalado

```
 # apachectl -M | grep evasive
```

Si todo está bien, recibiremos este resultado

evasive20_module (shared)

3) Configuraremos el módulo

```
 # vi /etc/apache2/mods-enabled/evasive.conf
```

y lo rellenaremos como el ejemplo de a continuación, siempre, ajustándolo a nuestras necesidades

```
DOSHashTableSize 3097
DOSPageCount 2
```

```
DOSSiteCount 50
DOSPageInterval 1
DOSSiteInterval 1
DOSBlockingPeriod 10
DOSEmailNotify email@yourdomain.com
DOSSystemCommand "su - someuser -c '/sbin/... %s ...'"
DOSLogDir "/var/log/mod_evasive"
```

4) Unos últimos retoques

```
  # mkdir /var/log/mod_evasive
# chown -R www-data:www-data /var/log/mod_evasive
```

5) Y el toque personal de la casa, reiniciar apache sin tirar conexiones

```
  # systemctl restart apache2
```

Listo! ya habéis dado un paso mas en la securización de vuestro server ;)

***** Anotaciones:***

DOSHashTableSize: Tamaño de la tabla hash que almacenará las IPs (nodos). Por defecto el valor es de 3097. A más tamaño, más memoria consumida.

DOSPageCount / **DOSPageInterval:** Umbral máximo que se debe alcanzar para ser incluído en la lista de bloqueados de una página concreta en segundos.

DOSSiteCount / **DOSSiteInterval:** Umbral máximo que se debe alcanzar para ser incluído en la lista de bloqueados de cualquier objeto (imagenes, css...) en segundos.

DOSBlockingPeriod: Tiempo en segundos que permanecerá bloqueada la IP de la lista. Dentro de este periodo, los accesos desde dicha IP obtendrán un error HTTP 403 (prohibido). En el caso de que la IP intente acceder dentro del periodo de bloqueo, el contador vuelve a ponerse en su valor inicial y tendrá que volver a transcurrir el número de segundos desde el principio de nuevo.

DOSEmailNotify: Opcional. Dirección de email a la que serán enviadas (mediante el comando mail) notificaciones cuando se bloqueen IPs. Incorpora sistema lock para no repetir varios emails y notificar una sola vez.

DOSSystemCommand: Opcional. Comando que será ejecutado cada vez que se añada una IP a la lista. Se reemplazará %s por la IP. De este modo, una buena técnica es hacer lo siguiente: "/sbin/iptables -I INPUT -p tcp --dport 80 -s %s -j DROP" Lo que hará que se ejecute el firewall de Linux (iptables) y bloquee todas las peticiones entrantes por el puerto TCP/80 (web).

DOSLogDir: Opcional. Selecciona una carpeta como directorio temporal para los logs. Por defecto, si no es especificado, tiene el valor /tmp.

DOSWhitelist: Opcional. Incluye una lista blanca para IPs que no tendremos en cuenta para bloquear. Ideal para añadir por ejemplo, el rango de IPs de los bots de Google (rango CIDR 66.249.64.0/19): DOSWhitelist 66.249.73.*
Puedes usar varias directivas DOSWhitelist y comodin de rangos de hasta los 3 últimos octetos.