Manual de Configuración de Modevasive

VenCERT

Índice

Introducción

mod_evasive es un módulo de Apache que proporciona una acción evasiva en caso de un ataque de Denegacion de servicio Distribuida (DDoS) o ataque de fuerza bruta. También está diseñado para ser una herramienta de detección y gestión de la red, el mismo puede ser fácilmente configurado para hablar con ipchains, cortafuegos, routers, Etc. Mod_evasive actualmente reporta abusos vía e-mail e instalaciones de registro del sistema.

El presente manual contiene información sobre la instalación y configuración de el módulo de seguridad mod_evasive Este módulo permite proteger el puerto 80 de ataques de tipo fuerza bruta (brute force) o Denegaciones de servicio distribuido (DDoS).

Instalación de Mod Evasive

Para configurar mod_evasive se deben seguir los siguientes pasos:

Ingresar en su servidor con privilegios root y luego en la línea de comandos

 # aptitude install libapache2-mod-evasive

Luego de este paso debe reiniciar el servidor Apache

 # /etc/init.d/apache2 restart

Realizar una prueba y comprobar si funciona correctamente, utilizaremos el fichero test.pl incluido en el paquete descargado. Este se aloja en la siguiente ruta

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

Se recomienda verificar las opciones del firewall, ya que el script se trata de un programa en Perl, que realiza alrededor de 100 peticiones secuenciales a nivel local (muy rápido, menos de 1 segundo). Así, si el sistema está funcionando bien, al ejecutar el programa **perl test.pl** aparecería algo similar a esto:

HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 200 OK
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
[...]

Para ejecutar el script debera escribir en consola la siguiente sentencia:

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

Luego de realizar las pruebas iniciales se crea el fichero donde se colocarán las opciones de configuración del modevasive. Para ello se creará en la ruta que se indica a continuación:

 # touch /etc/apache2/mods-available/evasive.conf

Configuración de Mod Evasive

Una vez creado el fichero se procederá a establecer las lineas de configuración.

(Por favor antes de continuar revise el anexo que se encuentra al final del documento el cual especifica las función de cada regla de configuración las cuales deben ser adaptadas a las necesidades y especificaciones de la plataforma) .

Una vez verificado el contenido del anexo debera establecer las lineas de configuración en evasive.conf:

A continuación se muestra un ejemplo de archivo de configuración. Sin embargo usted deberá establecer sus reglas dependiendo de los requerimientos y comportamiento de su plataforma.

```
DOSHashTableSize 3097     # <– Número de IPs que almacena
DOSPageCount 2        # <– Número de páginas solicitadas a partir de las cuales el módulo se activa
DOSSiteCount 50           # <– Número de solicitudes máximas a partir de las cuales el filtro se activa
DOSPageInterval 1           # <– Intervalo en segundos, de tiempo entre las peticiones de páginas
DOSSiteInterval 1           # <– Intervalo en segundos, de tiempo entre las peticiones
DOSBlockingPeriod 900      # <– Tiempo en segundos que bloqueará el acceso a web al atacante.
DOSWhitelist 127.0.0.1      # <– IPs a las que permitiremos para el localhost
DOSWhitelist 192.168.1.*    # <– IPs a las que permitiremos para un rango de IP
```

,

```
DOSWhitelist 66.249.65.*    # <– IPs a las que permitiremos para los spider google
DOSWhitelist 66.249.66.*
```

Posterior a esto se debe incluir la siguiente linea al final del fichero evasive.load ubicado en la ruta: **/etc/apache2/mods-avaiable/evasive.load**

Include mod_evasive.conf

Finalmente, guardamos el fichero de configuración y reiniciamos el servidor Apache

 # /etc/init.d/apache2 restart.

Se recomienda realizar un test con el procedimiento descrito anteriormente para verificar si las configuraciones funcionan correctamente.

ANEXO

Esta es la configuración que trae por defecto **mod_evasive**. Sin embargo, se repasaran todas las directivas para una mayor personalización.

• **DOSHashTableSize:** Tamaño de la tabla hash que almacenará las IPs (nodos). Por defecto el valor es de 3097.

• **DOSPageCount / DOSPageInterval:** Máximo (umbral) que se debe alcanzar para ser incluído en la lista de bloqueados. En este caso el objetivo será una página concreta. (Entiendase como «Máximo de DOSPageCount páginas en DOSPageInterval segundos»). Por defecto el máximo está establecido a 2 páginas por segundo.

• **DOSSiteCount / DOSSiteInterval:** Máximo (umbral) que se debe alcanzar para ser incluído en la lista de bloqueados. En este caso el objetivo será cualquier objeto (imagenes, css...). (Entiendase como «Máximo de DOSSiteCount objetos en DOSSiteInterval segundos»). Por defecto el máximo está establecido a 50 objetos por segundo.

• **DOSBlockingPeriod:** Tiempo en segundos (contador) 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: DOSSystemCommand "/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):