

El Día a Día del Administrador de Sistemas: Mod_evasive

MANIOBRAS EVASIVAS

El servidor web Apache puede luchar contra los ataques DoS. Sólo necesita la pequeña ayuda de Mod_evasive. **POR CHARLY KÜHNAST**



Todo administrador conoce y odia los ataques de Denegación-de-Servicios. No importa si el causante es un simple estúpido, un mal intencionado o un enfermo. Lo realmente importante es que una oleada impresionante de peticiones dirigidas al servidor provoca que se cuelgue, haciendo subir la adrenalina del administrador hasta el límite. Los servidores Web son los más atacados. AEMM proporciona a Apache un mecanismo de autodefensa. El paquete denominado “Apache Evasive Maneuvers Module” tiene un nombre demasiado largo, por lo que la mayoría de los administradores simplemente se refieren a él como Mod_evasive [1], aunque es el nombre del módulo AEMM de Apache.

El Mod_evasive utiliza una lista negra. El módulo comprueba las peticiones entrantes contra una lista para encontrar si varias peticiones del mismo tipo han sido recibidas desde la misma IP en los últimos segundos. El valor umbral es configurable. A la vez, el Mod_evasive comprueba si el solicitante ha llamado a más de 50 objetos en los últimos segundos.

Si se cumple alguna de estas condiciones, Apache envía un 403 en vez de la respuesta esperada, lo que ahorra bastante ancho de banda. A la vez, Mod_evasive también puede escribir una entrada en Syslog o enviar un mensaje de correo. Desde el punto de vista del atacante, esto significa que cualquier petición recibida en los próximos 10 segundos desde su IP provocará un 403. Y este período se extiende si el atacante persiste.

Aplicaciones Prácticas

Ejecuto Apache 2.0 en mi máquina de pruebas, pero el léeme del paquete también trae instrucciones para Apache 1.3 e iPlanet. La mayoría de las versiones de Apache incluyen una aplicación de ayuda denominada Apxs (Apache Extension Tool) para ayudarle a añadir módulos. (Suse Linux oculta la herramienta en el paquete Apache-devel). Tecleando

```
apxs -i -a -c mod_evasive20.c
```

se compila el módulo, cópielo en el directorio *modules* de Apache y añada una entrada en el *httpd.conf* (Listado 1). No se olvide de recargar Apache.

DOSHashTableSize es el tamaño de la tabla hash con los URIs y el acceso a hosts. A pesar de los requerimientos de memoria, puede que desee incrementar este valor si su sistema es muy utilizado. *DOSPageCount* especifica cuantas veces un host puede llamar a una página en un *DOSPageInterval* sin provocar los mecanismos de protección.

El mismo destino espera a los clientes que solicitan el mismo objeto mediante el mismo listener más de *DOSSiteCount* veces por *DOSSiteInterval*. La variable *DOSBlockingPeriod* especifica el período de bloqueo para el atacante. No necesita dar un valor alto aquí, ya que el contador comienza en cero con cada nuevo ataque.

Mod_evasive tiene algunas limitaciones. Si los ataques DoS son tan intensos que consumen todo su ancho de banda a pesar de AEMM, o si el hardware del servidor no puede dar paso, el ataque tendrá éxito a pesar de todos sus esfuerzos. Pero no se desespere; puede usar la instrucción *DOSSystemCommand* para provocar una reacción y enviar señales de humo usando IPchains.

SYSADMIN

- Logrotate.....58**
Logrotate es una herramienta útil para manejar los ficheros de registros.
- Métodos Nmap.....60**
Mostraremos algunas técnicas para encontrar agujeros de seguridad en su red con Nmap.
- Trickle.....67**
Controla el tráfico en tu red

Listado 1: Mod_evasive en httpd.conf

```
01 <IfModule mod_evasive20.c>
02 DOSHashTableSize 3097
03 DOSPageCount 2
04 DOSSiteCount 50
05 DOSPageInterval 1
06 DOSSiteInterval 1
07 DOSBlockingPeriod 10
08 DOSEmailNotify
   admin@dos-victim.com
09 </IfModule>
```

RECURSOS

[1] Mod_evasive: http://www.nuclearelephant.com/projects/mod_evasive/