The Sysadmin's Daily Grind: Mod_evasive

EVASIVE MANEUVERS

The Apache web server can fight back against DoS attacks. You just need a little help from Mod_evasive. **BY CHARLY KÜHNAST**

Every admin knows and hates Denial-of-Service attacks. No matter whether the perpetrator is plain stupid, malevolent, or sick, a massive barrage of incessant requests directed at the server causes the server to freeze and pushes the admin's adrenalin levels way up. Web servers are most commonly attacked. AEMM gives Apache a self-defense mechanism. The package name "Apache Evasive Maneuvers Module" is too long for many people's liking, and most admins simply refer to it as Mod_evasive [1] – although this is actually just the name of the AEMM Apache module.

Under the hood, Mod_evasive uses a blacklist. The module checks incoming requests against the list to find out if multiple requests of the same type have been received from the same IP in the last few seconds. The threshold values are configurable. At the same time, Mod_evasive checks if the requester has called more than 50 objects in the last second.

If one of these conditions is true, Apache sends a 403 instead of the expected response, which saves a lot of bandwidth. At the same time, _evasive can also write a Syslog entry or send an email message. From the attacker's point of view, this means that any requests received in the next 10 seconds from his or her IP will provoke a 403. And this period is extended if the attacker persists.

Practical Applications

I run Apache 2.0 on my test machine, but the readme with the package also has instructions for Apache 1.3 and iPlanet. Most Apache versions include a helper application titled Apxs (Apache Extension Tool) to help you add modules. (Suse Linux hides the tool in the Apache-devel package.) Typing

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

compiles the module, copies it to the Apache *modules* directory, and adds an entry to *httpd.conf* (Listing 1). Don't forget to reload Apache.

DOSHashTableSize is the size of the hash table with the URIs and accessing hosts. Despite the memory requirement, you might like to increase this value if your system gets a lot of use. *DOSPageCount* specifies how many times a host can call a page in a *DOSPageInterval* without triggering the protective mechanisms.

The same fate awaits clients that request the same object via the same listener more than *DOSSiteCount* times per *DOSSiteInterval*. The *DOSBlockingPeriod* variable specifies the blocking period for the attacker. You do not need a particularly high value here, as the counter starts at zero with each new attack.

Mod_evasive has some limitations. If the DoS attack is so massive that it consumes all of your bandwidth despite AEMM, or if the server hardware can't keep pace, the attack will succeed despite all your efforts. But don't despair; you can use the *DOSSystemCommand* instruction to trigger a reaction and send up smoke signs using IPchains. ■

Listing 1: Mod_evasive in 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>
```

INFO

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

THE AUTHOR

Charly Kühnast is a Unix System Manager at the data-center in Moers, near Germany's famous River Rhine. His tasks include ensuring firewall security and availability and taking care of the DMZ (demilitarized zone).