APACHE SECURITY - MODEVASIVE

Back to apache, we have previously looked at an application level firewall module (see here), in this article we will be looking at *mod_evasive* (found here) which will help against DOS attacks. What it does is look for "bad" traffic from clients (in this case multiple requests of the same type from the same client) and if it finds it, it sends a 403 error page rather then the normal page. It is easy to install and easy to configure. Let take a look...

What is Needed?
You will, of course, need an *Apache* web server. The module works for both 1.3x and 2.x versions, although I will be focusing on the 2,x version installations as most people should be running this version for security and performance reasons. You will need the *apxs* command installed, and finally you will need to download *mod_evasive* (remember that the versions could well change)..

```
 #wget http://www.nuclearelephant.com/projects/mod_evasive
/mod_evasive_1.10.1.tar.gz
```

Installing
Once you have the code, you do the extraction..

```
#gzip -d mod_evasive_1.10.1.tar.gz
#tar -xvf mod_evasive_1.10.1.tar
```

After you change into the extracted directory, you can then create the module..

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

This will build the module and update your *httpd.conf* file with the following line..

```
LoadModule evasive20_module   /usr/lib/httpd/modules/mod_evasive20.so
```

So far so good. Now we need to configure the module, the recommended default setup for your *httpd.conf* is as follows..

```
<IfModule mod_evasive20.c>
    DOSHashTableSize    3097
    DOSPageCount        2
    DOSSiteCount        50
    DOSPageInterval     1
    DOSSiteInterval     1
    DOSBlockingPeriod   10
</IfModule>
```

Lets take a look at the options..

DOSHashTableSize	This sets the size of the hash table the module uses to store it's data. Increase this for busy systems
DOSPageCount	After this many requests for the same page, the client is part of the bad-person list
DOSSiteCount	After this manyobject requests on the same listner per site, the client is a bad-person
DOSPageInterval	The interval for the page count threshold
DOSSiteInterval	The interval for the site count threshold
DOSBlockingPeriod	The amount of time a client is blocked for after becoming a bad-person

DOSEmailNotify	Can be used to send out emails when an IP is blacklisted
DOSSystemCommand	Command run when IP is blacklisted. IP is denoted by %s
DOSLogDir	Specify an alternative log directory
DOSWhitelist	Allow trusted clients to bypass the module. Can be used many times.

And after all is done, then restart Apache.

Final Words
Web servers are the most targeted servers out there, becuase they are the most common. And Apache is the most common web server software used, using these type of security modules does I lot to help protect your server. It is not difficult and the return for the amount of time you spend doing it is large. So as always. have fun and learn.