Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Home > Faq > Apache

FreeBSD Install mod_security For The Apache HTTPD Server

Posted by Vivek Gite <vivek@nixcraft.com>

[1]

Q. mod_security supplies an array of request filtering and other security features to the Apache HTTP Server. How do I install mod_security under FreeBSD operating systems?

[2]

A. ModSecurity is an open source web application firewall that runs as an Apache module, and version 2.0 offers many new features and improvements.

It provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring and real-time analysis with no changes to existing infrastructure. Some of the features include:

=> Parallel text matching
=> Geo IP resolution
=> Credit card number detection
=> Support for content injection
=> Automated rule updates
=> scripting as well as many others.

FreeBSD install mod_security

Type the following command to update ports tree:

```
# portsnap fetch update
```

Under FreeBSD 7, mod_security can be installed by typing the following commands:

```
# cd /usr/ports/www/mod_security
# make install clean
```

Configure mod_security

The modsecurity 2 Core Rules have been installed in

```
/usr/local/etc/apache22/Includes/mod_security2/
```

By default it run in "DetectionOnly" mode as not to disturb operatings of working websites and Apache. First change directory to /usr/local/etc/apache22/Includes/mod_security2/:

```
# cd /usr/local/etc/apache22/Includes/mod_security2/
```

Now, open the ModSecuirty core rule set file - modsecurity_crs_10_config.conf, enter:

```
# vi modsecurity_crs_10_config.conf
```

The file is well documented so just customize it according to your requirements. Open httpd.conf file located at /usr/local/etc/apache22 and make sure following line exists:

```
LoadFile /usr/local/lib/libxml2.so
LoadModule security2_module libexec/apache22/mod_security2.so
```

Finally, restart the apache:

```
# /usr/local/etc/rc.d/apache22 restart
```

Monitoring mod_security log files

By default logs are written to following two files:

- /var/log/httpd-modsec2_audit.log
- /var/log/httpd-modsec2_debug.log
- /var/log/httpd-error.log or virtual domain error.log file

You can detect attacks by viewing these two files using grep or tail:

```
tail -f /var/log/httpd-modsec2_audit.log
grep cmd.exe /var/log/httpd-modsec2_audit.log
tail -f /home/httpd/example.com/logs/error.log
```

Once everything started to working perfectly open modsecurity_crs_10_config.conf file and set SecRuleEngine to On:

```
SecRuleEngine On
```

Restart apache:

```
# /usr/local/etc/rc.d/apache22 restart
```

Further readings:

- Apache Security Book [3] - The real strength of Apache Security lies in its wealth of interesting and practical advice, with many real-life examples and solutions in this book will save your life.
- Modsecurity [4] project

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/freebsd-install-configure-mod_security/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/category/freebsd/**
[2] Image: **http://www.cyberciti.biz/faq/category/apache/**
[3] Apache Security Book: **http://www.amazon.com/gp/redirect.html?ie=UTF8&location=http%3A%2F%2Fwww.amazon.com%2FApache-Security-Ivan-Ristic%2Fdp%2F0596007248%3Fie%3DUTF8%26s%3Dbooks%26qid%3D1221993197%26sr%3D8-1&tag=cyberciti-20&linkCode=ur2&camp=1789&creative=9325**
[4] Modsecurity: **http://www.modsecurity.org/**