FreeBSD Administration - Support #561

Install mod_security for Apache 2.4 on FreeBSD

02/13/2015 10:35 PM - Daniel Curtis

Status:	Closed	**Start date:**	02/13/2015
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Web Server	**Estimated time:**	1.00 hour
Target version:	FreeBSD 9	**Spent time:**	3.00 hours

Description

This is a simple guide for installing and configuring mod_security for Apache 2.4 on FreeBSD 9.2.

- Update the system and ports tree:

```
pkg update && pkg upgrade
portsnap fetch extract
```

- Install portmaster:

```
cd /usr/ports/ports-mgmt/portmaster
make install clean
pkg2ng
```

- Install git:

```
portmaster devel/git
```

- Install sudo:

```
portmaster security/sudo
```

Install mod_security

- Install mod_security

```
portmaster www/mod_security
```

Configure mod_security

- ModSecurity requires firewall rule definitions. Most people use the OWASP ModSecurity Core Rule Set (CRS). The easiest way to track the OWASP CRS repository right now is to use Git. Let's make a directory for all our ModSecurity related stuff, and clone the CRS repository under it

```
mkdir -p /usr/local/etc/modsecurity && cd /usr/local/etc/modsecurity
git clone https://github.com/SpiderLabs/owasp-modsecurity-crs crs
```

- Copy the default ModSecurity config file:

```
cp /usr/local/etc/modsecurity.conf-example /usr/local/etc/modsecurity.conf
```

- And fetch a necessary file which is currently not included in the port:

```
cd /usr/local/etc
fetch https://raw.github.com/SpiderLabs/ModSecurity/master/unicode.mapping
```

- Copy the default ModSecurity CRS config file:

```
cd /usr/local/etc/modsecurity
cp crs/modsecurity_crs_10_setup.conf.example modsecurity_crs_10_setup.conf
```

- Now create an Apache configuration snippet that loads the ModSecurity module and includes the configurations and CRS:

```
vi /usr/local/etc/apache24/modules.d/020_mod_security.conf
```

  - And add/modify the following

```
LoadModule security2_module libexec/apache24/mod_security2.so

<IfModule security2_module>
    # Include ModSecurity configuration
    Include /usr/local/etc/modsecurity.conf

    # Include OWASP Core Rule Set (CRS) configuration and base rules
    Include /usr/local/etc/modsecurity/modsecurity_crs_10_setup.conf
    Include /usr/local/etc/modsecurity/crs/base_rules/*.conf

    # Add custom configuration and CRS exceptions here. Example:
    # SecRuleRemoveById 960015
</IfModule>
```

- When the configuration is all set, simply restart Apache:

```
service apache24 restart
```

  - Confirm that ModSecurity is loaded by checking Apache's log file:

```
tail /var/log/httpd-error.log
```

  - *Example output*:

```
ModSecurity for Apache/2.7.7 (http://www.modsecurity.org/) configured.
ModSecurity: APR compiled version="1.4.8"; loaded version="1.4.8"
ModSecurity: PCRE compiled version="8.34 "; loaded version="8.34 2013-12-15"
ModSecurity: LIBXML compiled version="2.8.0"
```

- Also check with the apachectl command:

```
apachectl -M
```

  - _ Truncated output:_

```
Loaded Modules:
 ...
 security2_module (shared)
```

Enable blocking mode

- Blocking mode can be enabled by editing modsecurity.conf and changing the following line:

```
SecRuleEngine On
```

  - And restart apache to apply it:

```
service apache24 restart
```

Update Core Rule Set

- Keep the CRS updated from time to time:

```
cd /usr/local/etc/modsecurity/crs
git pull
```

Install WeBekci

- Download and extract WeBekci:

```
cd ~
wget http://downloads.sourceforge.net/project/webekci/webekci/OWASP-WeBekci-1.0/webekci-1.0.tar.gz
tar xzf webekci-1.0.tar.gz
```

- Move and change into the WeBekci directory:

```
mv webekci /usr/local/www/apache24/data
cd /usr/local/www/apache24/data/webekci
```

- Edit .htaccess file:

```
vi .htaccess
```

  - And modify the correct path for the .htpasswd file in the AuthUserFile line:

```
AuthUserFile /usr/local/www/apache24/data/webekci/.htpasswd
AuthType Basic
AuthName "Owasp-WeBekci Screet Area"
<LIMIT GET POST>
 require valid-user
</LIMIT>
```

- Now create a new .htpasswd file for user bob with password SuperSecretPassword:

```
htpasswd -bc /usr/local/www/apache24/data/webekci/.htpasswd bob SuperSecretPassword
```

- Now, you need define new Directory in the httpd.conf file.

```
vi /usr/local/etc/apache24/httpd.conf
```

  - And add the following:

```
Alias /webekci/ "/usr/local/www/apache24/data/webekci/"
<Directory "/usr/local/www/apache24/data/webekci/">
  Options None
  AllowOverride All
  Order Allow,Deny
  Allow from 127.0.0.1
</Directory>
```

    NOTE: If you are using mod_rewrite, then enter “AllowOverride All” so that .htaccess file can be read. Otherwise enter “AllowOverride None”.

- Make necessary modifications in config.php file.

```
vi config.php
```

  - Add the following line:

```
# For MySql
$config['sql_host'] = 'localhost';
$config['sql_user'] = 'webekci';
$config['sql_pass'] = 'SuperSecretPassword';
$config['sql_db']   = 'webekcidb';

# For User
$config['admin_email']        = 'bob@example';
$config['apache_conf_file']   = '/usr/local/etc/apache24/httpd.conf';
$config['modsecurity_conf']   = '/usr/local/etc/apache24/modules.d/020_mod_security.co
nf';

# sudoers file config for this command
$config['apache_config_test'] = '/usr/local/bin/sudo /usr/local/sbin/httpd -t';
$config['apache_restart']     = '/usr/local/bin/sudo /usr/local/sbin/httpd -k restart'
;

# Log files
$config['system_log']         = '/var/log/messages';
$config['apache_access_log']  = '/var/log/apache/access.log';
$config['apache_error_log']   = '/var/log/apache/error.log';

$config['apache_config_test'] = '/usr/local/bin/sudo /usr/local/sbin/httpd -t';
$config['apache_restart']='/usr/local/bin/sudo /usr/local/sbin/httpd -k restart';
```

- To give the www user read and write permissions:

```
chown www /usr/local/etc/apache24/modules.d/020_mod_security.conf
```

- The www user is the user that apache runs as. Make sure the following entries are in httpd.conf:

```
User www
Group www
```

- After configuring WeBekci you need to restart apache:

```
service apache restart
```

- Edit the sudoers file:

```
visudo
```

  - And add these lines to allow apache to run configtest and restart on itself:

```
www ALL=NOPASSWD:/usr/local/sbin/httpd -k restart
www ALL=NOPASSWD:/usr/local/sbin/httpd -t
```

    Now www user can do configtest and restart operations without having to enter a password.

- Edit the sudoers file:

```
visudo
```

  - And add these lines to allow apache to run configtest and restart on itself:

```
www ALL=NOPASSWD:/usr/local/sbin/httpd -k restart
www ALL=NOPASSWD:/usr/local/sbin/httpd -t
```

    Now www user can do “config test” and “restart” operations restart apache without having to enter password.

- Make sure the entered MySQL related changes are in the config.php file:

```
vi config.php
```

  - And modify the following to the database created earlier:

- Now browse your site and run the install.php file:
  http://www.example.com/webekci/install.php

- Do not forget to delete install.php when the install has finished:

```
rm /usr/local/www/apache24/data/webekci/install.php
```

Resources

- https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual
- https://www.owasp.org/index.php/Category:OWASP_WeBekci_Project

Related issues:

Related to FreeBSD Administration - Support #560: Hardening Apache 2.4 & PHP ...	**Closed**	**02/13/2015**

History

#1 - 02/14/2015 12:11 PM - Daniel Curtis

- Category set to Web Server

- Target version set to FreeBSD 9

#2 - 03/11/2015 08:16 AM - Daniel Curtis

- Subject changed from Installing mod_security for Apache 2.4 on FreeBSD to Install mod_security for Apache 2.4 on FreeBSD

- Description updated

- Status changed from New to In Progress

- % Done changed from 0 to 80

#3 - 03/11/2015 08:20 AM - Daniel Curtis

- Description updated

#4 - 03/11/2015 11:37 AM - Daniel Curtis

- Status changed from In Progress to Resolved

- % Done changed from 80 to 100

#5 - 03/24/2015 01:40 PM - Daniel Curtis

- Description updated

#6 - 03/24/2015 02:10 PM - Daniel Curtis

- Description updated

#7 - 03/25/2015 07:11 AM - Daniel Curtis

- Description updated

#8 - 04/11/2015 01:19 PM - Daniel Curtis

- Related to Support #560: Hardening Apache 2.4 & PHP 5 on FreeBSD added

#9 - 04/12/2015 08:13 AM - Daniel Curtis

- Description updated

#10 - 04/12/2015 01:45 PM - Daniel Curtis

- Description updated

#11 - 04/13/2015 05:13 PM - Daniel Curtis

- Description updated

#12 - 04/14/2015 01:18 PM - Daniel Curtis

- Status changed from Resolved to Closed