TecMint.com is a community driven Linux website. Our motto is to provide an effortless howto's to our valuable readers.

You are also welcome to join our community and can be part of our team, contributing and submitting well written article on Linux. If you have any query, please contact us by email **tecmint.com [at] gmail [dot] com** or use our contact form.

Protect Apache using Mod_Security and Mod_evasive on RHEL/Ce S & Fedora

By Ravi Saive Under: Apache, CentOS, Fedora, Linux Distros, RedHat On: June 27, 2012

This is our first series on Apache security, in this article we will guide you'll how to install and configure **Mod_Secu**
RHEL 6.2/6.1/6/5.8, **CentOS 6.2/6.1/6/5.8** and **Fedora 17,16,15,14,13,12** systems using source code.

These two great security modules protect **Apache** server from brute force attacks and DOS attacks. Before, moving
provide you a little description on these tow modules.

Install mod_security and mod_evasive

What is Mod_Security?

Mod_Security is an open source web application firewall (**WAF**) and intrusion detection and prevention system for web applications. It is used to protect and monitor real time HTTP traffic and web applications from brute fore attacks.

What is Mod_Evasive?

Mod_Evasive is an open source evasive maneuvers system for **Apache** server to provide evasive action in the even HTTP brute force, Dos or DDos attack. It was designed to use as a network traffic detection and network management tool and can be easily configured and integrated into firewalls, ipchains, routers etc. Presently, it sends abuses reports via email and syslog facilites.

Install Mod_Security and Mod_evasive on RHEL 6.2/6.1/6/5.8, CentOS 6.2/6.1/6/5. Fedora 17,16,15,14,13,12

How to Install Mod_Security on RHEL/CentOS & Fedora

You must have LAMP setup installed and configured in your system before installing mod_security.

Become A TecMint Subscriber to receive latest Howto's an Guides in Your Mailbox.

Enter Your Email Addr Signup Now!

- Popular
- Latest
- Comments
- Tags

- Install Wine 1.5.27 in RHEL, CentOS and Fedora63 Comments
- CentOS 6.3 Step by Step Installation Guide with Screenshots59 Comments
-

Step 1: Installing Dependencies for mod_security

Firstly, we required to install some dependency packages for mod_security. Run the following commands on your s OS.

```
## For RHEL/CentOS 6.2/6.1/6/5.8 ##
# yum install gcc make
# yum install libxml2 libxml2-devel httpd-devel pcre-devel curl-devel

## For Fedora 17,16,15,14,13,12 ##
# yum install gcc make
# yum install libxml2 libxml2-devel httpd-devel pcre-devel curl-devel
```

Step 2: Installing Mod_Security

As I said above that we use source code to install mod_security. Run the following commands as root.

```
## For RHEL/CentOS 6.2/6.1/6/5.8 ##
# cd /usr/src
# wget http://www.modsecurity.org/download/modsecurity-apache_2.6.6.tar.gz
# tar xzf modsecurity-apache_2.6.6.tar.gz
# cd modsecurity-apache_2.6.6
# ./configure
# make install
# cp modsecurity.conf-recommended /etc/httpd/conf.d/modsecurity.conf

## For Fedora 17,16,15,14,13,12 ##
# cd /usr/src
# wget http://www.modsecurity.org/download/modsecurity-apache_2.6.6.tar.gz
# tar xzf modsecurity-apache_2.6.6.tar.gz
# cd modsecurity-apache_2.6.6
# ./configure
# make install
# cp modsecurity.conf-recommended /etc/httpd/conf.d/modsecurity.conf
```

Step 3: Downloading OWASP Mod_Security Core Rule Set

Mod_Security requires OWASP (Open Web Application Security Project) core rules for base configuration, these ru used to protect from unknown vulnerabilities which often found on web applications. So, here we are going to download and install rule set for mod_security. Run the following commands.

```
## For RHEL/CentOS 6.2/6.1/6/5.8 ##
# cd /etc/httpd/
# wget http://downloads.sourceforge.net/project/mod-security/modsecurity-crs/0-CURRENT
# tar xzf modsecurity-crs_2.2.5.tar.gz
# mv modsecurity-crs_2.2.5 modsecurity-crs
# cd modsecurity-crs
# cp modsecurity_crs_10_setup.conf.example modsecurity_crs_10_config.conf

## For Fedora 17,16,15,14,13,12 ##
# cd /etc/httpd/
# wget http://downloads.sourceforge.net/project/mod-security/modsecurity-crs/0-CURRENT/modsecurity-crs_2.2.5.tar.gz
# tar xzf modsecurity-crs_2.2.5.tar.gz
# mv modsecurity-crs_2.2.5 modsecurity-crs
# cd modsecurity-crs
# cp modsecurity_crs_10_setup.conf.example modsecurity_crs_10_config.conf
```

Step 4: Configuring Mod_Security

Now, you need to modify your Apache configuration file to load the mod_security module.

```
# vi /etc/httpd/conf/httpd.conf
```

Search for the line **LoadModule** in your httpd.conf and add this below line at the bottom.

```
LoadModule security2_module modules/mod_security2.so
```

Now set the basic rule set in your httpd.conf file. Add the following lines of code at the end of the file.

```
<IfModule security2_module>
    Include modsecurity-crs/modsecurity_crs_10_config.conf
    Include modsecurity-crs/base_rules/*.conf
</IfModule>
```

Next, restart the Apache service to enable mod_security module and their rules.

```
# /etc/init.d/httpd restart
```

For more information on this topic visit the following links for your reference.

1. ModSecurity Home Page
2. OWASP ModSecurity Core Rule Set

The above installation is tested on CentOS 5.6 and successfully worked for me, I hope it will also work for you, now let's move further installation of mod_evasive module.

How to Install Mod_Evasive in RHEL/CentOS & Fedora

As we already installed required dependency packages above, so let's install the mod_evasive module.

Step 1: Installing Mod_Evasive

Just run the following commands to install mod_evasive.

```
## For RHEL/CentOS 6.2/6.1/6/5.8 ##
# cd /usr/src
```

Install Apache, MySQL 5.5.30 & PHP 5.4.12 on RHEL/CentOS 6.4/5.9 & Fedora 18-1244 Comments

- Install Skype 4.1 in Ubuntu 12.10, Xubuntu 12.10 an Linux Mint 14/1339 Comments

- Install Cacti (Network Monitoring) on RHEL/CentOS 6.3/5.8 and Fedora 17-1231 Comments

- Install VirtualBox 4.2.10 on RHEL/CentOS 6.4/5.9 a Fedora 18-1225 Comments

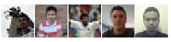
- Install Linux Malware Detect (LMD) in RHEL, Cent and Fedora17 Comments

- 30 Useful Linux Commands for System Administrato Comments

- Install WordPress 3.5 Using LAMP or LEMP on RH CentOS & Fedora17 Comments

- Install mod_pagespeed (Website Optimizer) for Apacl RHEL, CentOS and Fedora16 Comments

+1 +70



:: Top Posts ::

- A Basic Guide to Different Stages of Linux Boot Proc
- 10 Useful du (Disk Usage) Commands to Find Disk U of Files and Directories
- 13 Basic Cat Command Examples in Linux
- 10 Useful "IP" Commands to Configure Network Inte
- 8 Pratical Examples of Linux "Touch" Command
- How to Reset Forgotten Root Password in RHEL/Ce and Fedora
- 12 Tcpdump Commands – A Network Sniffer Tool
- MySQL Backup and Restore Commands for Databas Administration
- 13 Linux Network Configuration and Troubleshootin Commands
- How to Monitor User Activity with psacct or acct To
- 20 MySQL (Mysqladmin) Commands for Database Administration in Linux
- 35 Practical Examples of Linux Find Command

```
# wget http://www.zdziarski.com/blog/wp-content/uploads/2010/02/mod_evasive_1.10.1.tar.gz
# tar xzf mod_evasive_1.10.1.tar.gz
# cd mod_evasive
# apxs -cia mod_evasive20.c

## For Fedora 17,16,15,14,13,12 ##
# cd /usr/src
# wget http://www.zdziarski.com/blog/wp-content/uploads/2010/02/mod_evasive_1.10.1.tar.gz
# tar xzf mod_evasive_1.10.1.tar.gz
# cd mod_evasive
# apxs -cia mod_evasive20.c
```

Step 2: Configuring Mod_Evasive

By default installation adds the following line of mod_evasive configuration to your Apache configuration file. Please verify that it should be there like similar to below. If you can't see this below line, then add this to your httpd.conf file.

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

Now add the mod_evasive configuration parameters to your Apache configuration at the end. Replace **someone@somewhere.com** with your Email Id to get email alerts.

```
<IfModule mod_evasive20.c>
DOSHashTableSize    3097
DOSPageCount        2
DOSSiteCount        50
DOSPageInterval     1
DOSSiteInterval     1
DOSBlockingPeriod   60
DOSEmailNotify someone@somewhere.com
</IfModule>
```

Next restart the Apache service to update changes.

```
# /etc/init.d/httpd restart
```

For more additional information visit the mod_evasive Home Page.

Please drop your comments for any queries on installation, we will love to help you out and don't forget to Subscribe to our Updates.

0

Tweet

8

Like

2

+1

1

Share

12

comments

Share & Comment

- +1 2
- Tweet 0
- Like 8 Send
- Share 1

« Previous

Adobe Flash Player 11.3 Released – Install On RHEL/CentOS 6-5 and Fedora 17-12

Next »

Red Hat Enterprise Linux (RHEL) 6 Installation Guide with Screenshots

Related Post(s):

1. Install LEMP (Linux, Nginx, MySQL 5.5.29, PHP 5.4.11) on RHEL/CentOS 5-6 & Fedora 18-12
2. 35 Practical Examples of Linux Find Command
3. Basic Steps to Install Cinnamon Desktop on Fedora 18
4. Thunderbird 17 – Install on RHEL/CentOS 6.3 and Fedora 17-14
5. Install Skype 4.1 on Fedora 18 for 32-Bit OS
6. Install MongoDB 2.0.6 on on RHEL/CentOS 5-6 & Fedora 12-17

12 Responses

1. *sholeh* says:
   September 5, 2012 at 12:14 pm

   Now set the basic rule set in your httpd.conf file. Add the following lines of code at the end of the file ?

   Include modsecurity-crs/modsecurity_crs_10_config.conf
   Include modsecurity-crs/base_rules/*.conf

   my configure is error ? please give me example

   Thanks

   Reply

   -
     Ravi Saive says:
     September 5, 2012 at 12:47 pm

     Dear Sholeh,

     Use command as httpd -t and tell me the output of the error.

     Reply

2. *rohit* says:
   October 9, 2012 at 9:02 pm

   Syntax error on line 47 of /etc/httpd/modsecurity.d/activated_rules/base_rules/modsecurity_crs_21_protocol_anomalies.conf:
   ModSecurity: SkipAfter actions can only be specified by chain starter rules.

   please help me out in this.

   Reply

3.
   Ravi Saive says:
   October 10, 2012 at 5:21 pm

   @ Rohit,

   The directory activated_rules contains some rules that comes with modsecurity 2.2.5 version and are not comptaible with the modsecurity version 2.6.6. In version 2.6.6 there is no such activated_rules directory exists. see my article did i mentioned the directory above.

   This above artilce is works with modsecurity 2.6.6 only..

   Reply

4. *Miguel Mello* says:
   November 28, 2012 at 9:39 am

   Works great! Very nice and helpful tutorial. Thank you.

   Reply

5. *Séries Parlotte* says:
   December 10, 2012 at 5:18 am

   Hello,

   Can we install this on Centos 6.3 ?

   Reply

   -
     Ravi Saive says:
     December 10, 2012 at 1:02 pm

     @Series Parlotte,
     Yes! You can install it. go ahead..

     Reply

6.
   Paul Sandel says:
   December 15, 2012 at 11:35 pm

   Thanks for the info, very helpful. Can you recommend a methodology to test the efficacy of the server's security? I'm not a hacker, and do not have a strong understand of their approach

   Reply

7. *sanjeev* says:
   January 8, 2013 at 11:05 am

paul either you can use openvas or nessus(only for non-commercial) tool to check server's security

Reply

8. *Alex* says:
January 18, 2013 at 1:43 am

gracias, funciona muy bien.

Reply

9. *Tanas Alexandru Florin* says:
February 10, 2013 at 10:15 pm

Thanks but with this 2 module my ram usage uts 500 mb with out any site on my VPS.
How to uninstall this 2 module ?

Thanks

Reply

10. *Jayb* says:
March 17, 2013 at 12:19 pm

Is there any simple url script to check if mod security is enabled and working. I tried with generic samples from the web, but all of them give 'Not Found' error instead of Access Denied.

Reply

Leave a Reply

Name (Required)

Mail (will not be published) (Required)

Website

Submit Comment

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

Ubuntu / Xubuntu / Linux Mint

- Wine 1.5.27 Released – Install on Ubuntu 12.10/12.04/11.10 and Linux Mint 14/13
- KDE Plasma Media Center Released – Install on Fedora 17/18 and Ubuntu 12.10
- 25 Useful Basic Commands of APT-GET and APT-CACHE for Package Management
- How to Install Varnish Cache (Web Accelerator) in RHEL/CentOS/Fedora and Ubuntu/Debian
- How to Install Teamviewer 8 on Linux Distributions

Linux Monitoring

- 10 Command Line Tools to Monitor Linux Performance
- 13 Linux Network Configuration and Troubleshooting Commands
- Install Cacti (Network Monitoring) on RHEL/CentOS 6.3/5.8 and Fedora 17-12
- Wireshark – Network Protocol Analyzer Tool for RHEL/CentOS/Fedora
- Block SSH Server Attacks (Brute Force Attacks) Using DenyHosts

Linux Commands

- 35 Practical Examples of Linux Find Command
- 10 Useful du (Disk Usage) Commands to Find Disk Usage of Files and Directories
- 5 Basic chkconfig Command Examples in Linux
- 12 TOP Command Examples in Linux
- 25 Useful Basic Commands of APT-GET and APT-CACHE for Package Management