

[你好，游客](#) [登录](#) [注册](#) [搜索](#)[首页](#) [Linux新闻](#) [Linux教程](#) [数据库技术](#) [Linux编程](#) [服务器应用](#) [Linux安全](#) [Linux下载](#) [Linux认证](#) [Linux](#)[首页](#) → [服务器应用](#)

阅读新闻

背景：

如何在 Apache 中抵御暴力破解和 DDos 攻击

[日期：2015-06-16]

来源：Linux中国 作者：Linux

[字体：大 中 小]

对于那些需要在因特网上提供服务或托管主机的人来说，保证您的系统在面对攻击时的安全是一个重要的事情。

`mod_security`（一个开源的用于Web应用入侵检测及防护的引擎，可以无缝地集成到Web服务器）和`mod_evasive`是两个在服务器端对抗暴力破解和(D)Dos攻击的非常重要的工具。

`mod_evasive`，如它的名字一样，在受攻击时提供避实就虚的功能，它像一个雨伞一样保护Web服务器免受那些威胁。



安装`mod_security`和`mod_evasive`来保护Apache

在这篇文章中我们将讨论如何安装、配置以及在RHEL/CentOS 6、7和Fedora 21-15上将它们整合到Apache。另外，我们会模拟攻击以便验证服务器做出了正确的反应。

以上以您的系统中安装有LAMP服务器为基础，所以，如果您没有安装，请先阅读下面链接的文章再开始阅读本文。

- CentOS 7下搭建LAMP平台环境 <http://www.linuxidc.com/Linux/2015-06/118818.htm>
- CentOS 6.5系统安装配置LAMP(Apache+PHP5+MySQL)服务器环境 <http://www.linuxidc.com/Linux/2014-12/111030.htm>

(LCTT 译注：本文有修改。原文为了在RHEL/CentOS 7或Fedora 21中使用同样的工具，而删除了它们自带的 `firewalld`，使用了旧式的`iptables`。译者以为这样并不恰当，因此，译文中做了相应删节，并增加了`firewalld`的相应脚本。)

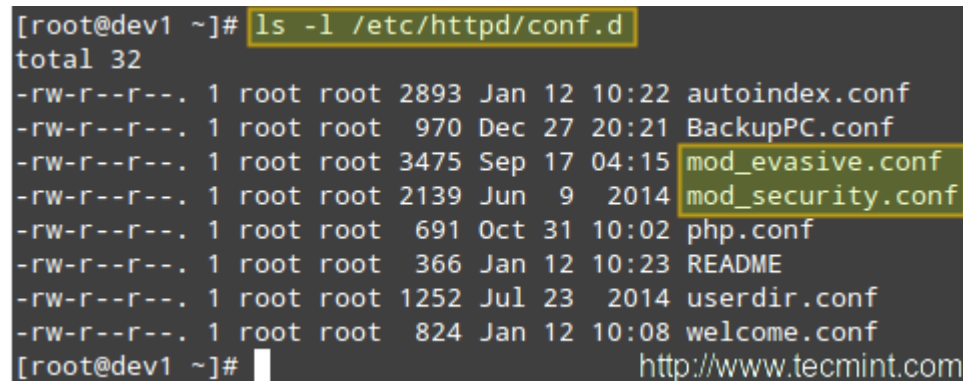
步骤 1: 安装`mod_security`和`mod_evasive`

另外，在安装LAMP后，您还需要在RHEL/CentOS 7/6中[开启EPEL仓库](#)来安装这两个包。Fedora用户不需要开启这个仓库，因为`epel`已经是Fedora项目的一部分了。

```
1. # yum update && yum install mod_security mod_evasive
```

当安装结束后，您会在`/etc/httpd/conf.d`下找到这两个工具的配置文件。

```
1. # ls -l /etc/httpd/conf.d
```



```
[root@dev1 ~]# ls -l /etc/httpd/conf.d
total 32
-rw-r--r--. 1 root root 2893 Jan 12 10:22 autoindex.conf
-rw-r--r--. 1 root root 970 Dec 27 20:21 BackupPC.conf
-rw-r--r--. 1 root root 3475 Sep 17 04:15 mod_evasive.conf
-rw-r--r--. 1 root root 2139 Jun 9 2014 mod_security.conf
-rw-r--r--. 1 root root 691 Oct 31 10:02 php.conf
-rw-r--r--. 1 root root 366 Jan 12 10:23 README
-rw-r--r--. 1 root root 1252 Jul 23 2014 userdir.conf
-rw-r--r--. 1 root root 824 Jan 12 10:08 welcome.conf
[root@dev1 ~]#
```

`mod_security` + `mod_evasive` 配置文件

现在，为了整合这两个模块到Apache，并在启动时加载它们。请确保下面几行出现在`mod_evasive.conf`和`mod_security.conf`的顶层部分，它们分别为：

1. `LoadModule evasive20_module modules/mod_evasive24.so`
2. `LoadModule security2_module modules/mod_security2.so`

请注意`modules/mod_security2.so`和`modules/mod_evasive24.so`都是从`/etc/httpd`到模块

源文件的相对路径。您可以通过列出/etc/httpd/modules的内容来验证（如果需要的话，修改它）：

1. # cd /etc/httpd/modules
2. # pwd
3. # ls -l | grep -Ei '(evasive|security)'

```
[root@dev1 modules]# pwd
/etc/httpd/modules
[root@dev1 modules]# ls -l | grep -Ei '(evasive|security)'
-rwxr-xr-x. 1 root root 19592 Sep 17 04:16 mod_evasive24.so
-rwxr-xr-x. 1 root root 396720 Jun 9 2014 mod_security2.so
[root@dev1 modules]#
```

<http://www.tecmint.com>

验证mod_security + mod_evasive模块

接下来重启Apache并且核实它已加载了mod_evasive和mod_security：

1. # service httpd restart [在RHEL/CentOS 6和Fedora 20-18上]
2. # systemctl restart httpd [在RHEL/CentOS 7和Fedora 21上]

-
1. # httpd -M | grep -Ei '(evasive|security)' [输出已加载的静态模块和动态模块列表]

```
[root@dev1 modules]# httpd -M | grep -Ei '(evasive|security)'
[Tue Feb 03 22:26:05.666807 2015] [so:warn] [pid 20818] AH01574: mo
AH00558: httpd: Could not reliably determine the server's fully qua
ess this message
security2_module (shared)
evasive20_module (shared)
[root@dev1 modules]#
```

<http://www.tecmint.com>

检查mod_security + mod_evasive模块已加载

步骤 2: 安装一个核心规则集并且配置mod_security

简单来说，一个核心规则集（即CRS）为web服务器提供特定状况下如何反应的指令。mod_security的开发者们提供了一个免费的CRS，叫做OWASP（[开放Web应用安全项目]）ModSecurity CRS，可以从下面的地址下载和安装。

下载OWASP CRS到为之创建的目录

1. # mkdir /etc/httpd/crs-tecmint
2. # cd /etc/httpd/crs-tecmint
3. # wget https://github.com/SpiderLabs/owasp-modsecurity-crs/tarball/master

```
[root@dev1 crs-tecmint]# wget https://github.com/SpiderLabs/owasp-modsecurity-crs
--2015-02-03 22:37:35-- https://github.com/SpiderLabs/owasp-modsecurity-crs/tarball/master
Resolving github.com (github.com)... 192.30.252.130
Connecting to github.com (github.com)|192.30.252.130|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/SpiderLabs/owasp-modsecurity-crs/legacy.tar.gz/master
--2015-02-03 22:37:36-- https://codeload.github.com/SpiderLabs/owasp-modsecurity-crs/legacy.tar.gz/master
Resolving codeload.github.com (codeload.github.com)... 192.30.252.146
Connecting to codeload.github.com (codeload.github.com)|192.30.252.146|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 280011 (273K) [application/x-gzip]
Saving to: 'master'

100%[=====] 280011 112 KB/s

2015-02-03 22:37:39 (112 KB/s) - 'master' saved [280011/280011]

[root@dev1 crs-tecmint]# ls
master
[root@dev1 crs-tecmint]# file master
master: gzip compressed data, from Unix
[root@dev1 crs-tecmint]#
```

Please note that this is a tarball. As such, you should use tar commands to extract it.

下载mod_security核心规则

解压CRS文件并修改文件夹名称

1. # tar xzf master
2. # mv SpiderLabs-owasp-modsecurity-crs-ebe8790 owasp-modsecurity-crs

```
[root@dev1 crs-tecmint]# tar xzf master
[root@dev1 crs-tecmint]# ls
master  SpiderLabs-owasp-modsecurity-crs-ebe8790
[root@dev1 crs-tecmint]# mv SpiderLabs-owasp-modsecurity-crs-ebe8790 owasp-modsecurity-crs
[root@dev1 crs-tecmint]# ls
master  owasp-modsecurity-crs
[root@dev1 crs-tecmint]#
```

<http://www.tecmint.com>

解压mod_security核心规则

现在，是时候配置**mod_security**了

将示例的规则文件（`owasp-modsecurity-crs/modsecuritycrs10_setup.conf.example`）拷贝为同名的配置文件。

```
1. # cp modsecurity_crs_10_setup.conf.example modsecurity_crs_10_setup.conf
```

并通过将下面的几行插入到web服务器的主配置文件/etc/httpd/conf/httpd.conf来告诉Apache将这个文件和该模块放在一起使用。如果您选择解压打包文件到另一个文件夹，那么您需要修改Include的路径：

```
1. <IfModulesecurity2_module>
2. Include crs-tecmint/owasp-modsecurity-crs/modsecurity_crs_10_setup.conf
3. Include crs-tecmint/owasp-modsecurity-crs/base_rules/*.conf
4. </IfModule>
```

最后，建议您在/etc/httpd/modsecurity.d目录下创建自己的配置文件，在那里我们可以用我们自定义的文件夹（接下来的示例中，我们会将其命名为**tecmint.conf**）而无需修改CRS文件的目录。这样做能够在CRS发布新版本时更加容易的升级。

```
1. <IfModulemod_security2.c>
2. SecRuleEngine On
3. SecRequestBodyAccess On
4. SecResponseBodyAccess On
5. SecResponseBodyMimeType text/plain text/html text/xml application/octet-stream
6. SecDataDir /tmp
7. </IfModule>
```

您可以在[SpiderLabs的ModSecurity GitHub](#)仓库中参考关于**mod_security**目录的更完整的解释。

步骤 3: 配置**mod_evasive**

mod_evasive被配置为使用/etc/httpd/conf.d/mod_evasive.conf中的指令。与**mod_security**不同，由于在包升级时没有规则来更新，因此我们不需要独立的文件来添加自定义指令。

默认的mod_evasive.conf开启了下列的目录（注意这个文件被详细的注释了，因此我们剔掉了注释以重点显示配置指令）：

1. <IfModulemod_evasive24.c>
2. DOSHashTableSize 3097
3. DOSPageCount 2
4. DOSSiteCount 50
5. DOSPageInterval 1
6. DOSSiteInterval 1
7. DOSBlockingPeriod 10
8. </IfModule>

这些指令的解释：

- **DOSHashTableSize**: 这个指令指明了哈希表的大小，它用来追踪基于IP地址的活动。增加这个数字将使得站点访问历史的查询变得更快，但如果被设置的太大则会影响整体性能。
- **DOSPageCount**: 在DOSPageInterval间隔内可由一个用户发起的针对特定的URI（例如，一个Apache 提供服务的文件）的同一个请求的数量。
- **DOSSiteCount**: 类似DOSPageCount，但涉及到整个站点总共有多少的请求可以在DOS SiteInterval间隔内被发起。
- **DOSBlockingPeriod**: 如果一个用户超过了DOSSPageCount的限制或者DOSSiteCount，他的源IP地址将会在DOSBlockingPeriod期间内被加入黑名单。在DOSBlockingPeriod期间，任何从这个IP地址发起的请求将会遭遇一个403禁止错误。

尽可能的试验这些值，以使您的web服务器有能力处理特定大小的负载。

一个小警告: 如果这些值设置的不合适，则您会蒙受阻挡合法用户的风险。

您也许还会用到以下其它有用的指令：

DOSEmailNotify

如果您运行有一个邮件服务器，您可以通过Apache发送警告消息。注意，如果SELinux已开启，您需要授权apache用户SELinux的权限来发送email。您可以通过下面的命令来授予权限：

1. # setsebool -P httpd_can_sendmail 1

接下来，将这个指令和其他指令一起加入到mod_evasive.conf文件。

1. DOSEmailNotify you@yourdomain.com

如果这个指令设置了合适的值，并且您的邮件服务器在正常的运行，则当一个IP地址被加入黑名单时，会有一封邮件被发送到相应的地址。

DOSSystemCommand

它需要一个有效的系统命令作为参数，

1. DOSSystemCommand</command>

这个指令指定当一个IP地址被加入黑名单时执行的命令。它通常结合shell脚本来使用，比如在脚本中添加一条防火墙规则来阻挡某个IP进一步的连接。

写一个shell脚本在防火墙阶段处理IP黑名单

当一个IP地址被加入黑名单，我们需要阻挡它进一步的连接。我们需要下面的shell脚本来执行这个任务。在/usr/local/bin下创建一个叫做scripts-tecmint的文件夹（或其他名字），以及一个叫做ban_ip.sh的文件。

用于iptables防火墙

```
1. #!/bin/sh
2. # 由mod_evasive检测出，将被阻挡的IP地址
3. IP=$1
4. # iptables的完整路径
5. IPTABLES="/sbin/iptables"
6. # mod_evasive锁文件夹
7. mod_evasive_LOGDIR=/var/log/mod_evasive
8. # 添加下面的防火墙规则（阻止所有从$IP流入的流量）
9. $IPTABLES -I INPUT -s $IP -j DROP
10. # 为了未来的检测，移除锁文件
11. rm -f "$mod_evasive_LOGDIR"/dos-"$IP"
```

用于firewalld防火墙

```
1. #!/bin/sh
2. # 由mod_evasive检测出，将被阻挡的IP地址
3. IP=$1
4. # firewalld-cmd的完整路径
5. FIREWALL_CMD="/usr/bin/firewall-cmd"
```



```
6. # mod_evasive锁文件夹
7. mod_evasive_LOGDIR=/var/log/mod_evasive
8. # 添加下面的防火墙规则（阻止所有从$IP流入的流量）
9. $FIREWALL_CMD --zone=drop --add-source $IP
10. # 为了未来的检测，移除锁文件
11. rm -f "$mod_evasive_LOGDIR"/dos-"$IP"
```

我们的DOSSystemCommand指令应该是这样的：

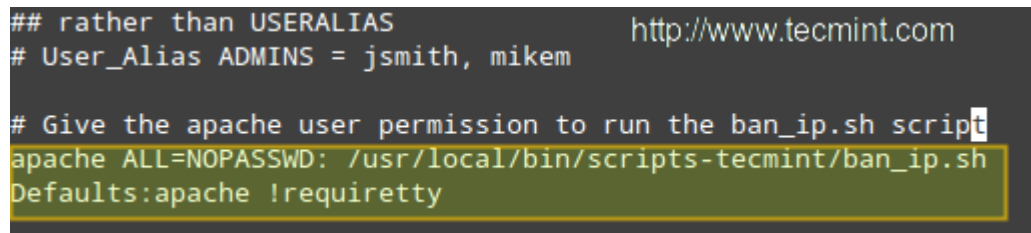
```
1. DOSSystemCommand"sudo /usr/local/bin/scripts-tecmint/ban_ip.sh %s"
```

上面一行的%s代表了由mod_evasive检测到的攻击IP地址。

将apache用户添加到sudoers文件

请注意，如果您不给予apache用户以无需终端和密码的方式运行我们脚本（关键就是这个脚本）的权限，则这一切都不起作用。通常，您只需要以root权限键入visudo来存取/etc/sudoers文件，接下来添加下面的两行即可：

```
1. apache ALL=NOPASSWD:/usr/local/bin/scripts-tecmint/ban_ip.sh
2. Defaults:apache !requiretty
```

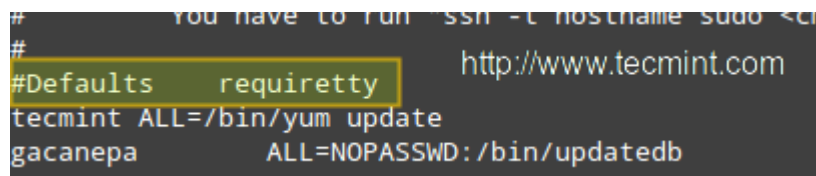


```
## rather than USERALIASES http://www.tecmint.com
# User_Alias ADMINS = jsmith, mikem
# Give the apache user permission to run the ban_ip.sh script
apache ALL=NOPASSWD: /usr/local/bin/scripts-tecmint/ban_ip.sh
Defaults:apache !requiretty
```

添加Apache用户到Sudoers

重要: 在默认的安全策略下您只能在终端中运行sudo。由于这个时候我们需要在没有tty的时候运行sudo，我们必须像下图中那样注释掉下面这一行：

```
1. #Defaults requiretty
```



```
# Defaults requiretty http://www.tecmint.com
tecmint ALL=/bin/yum update
gacanepa ALL=NOPASSWD:/bin/updatedb
```

为Sudo禁用tty

最后，重启web服务器：

1. # service httpd restart [在RHEL/CentOS 6和Fedora 20-18上]
2. # systemctl restart httpd [在RHEL/CentOS 7和Fedora 21上]

步骤4: 在Apache上模拟DDos攻击

有许多工具可以在您的服务器上模拟外部的攻击。您可以google下“tools for simulating ddos attacks”来找一找相关的工具。

注意，您（也只有您）将负责您模拟所造成的结果。请不要考虑向不在您自己网络中的服务器发起模拟攻击。

假如您想对一个由别人托管的VPS做这些事情，您需要向您的托管商发送适当的警告或就那样的流量通过他们的网络获得允许。Tecmint.com不会为您的行为负责！

另外，仅从一个主机发起一个Dos攻击的模拟无法代表真实的攻击。为了模拟真实的攻击，您需要使用许多客户端在同一时间将您的服务器作为目标。

我们的测试环境由一个CentOS 7服务器[IP 192.168.0.17]和一个Windows组成，在Windows [IP 192.168.0.103]上我们发起攻击：

```
C:\Users\Gabriel>ipconfig http://www.tecmint.com

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::d811:448f:5340:62f6
    Dirección IPv4. . . . . : 192.168.0.103
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.0.1
```

确认主机IP地址

请播放下面的视频（YT 视频，请自备梯子：https://www.youtube.com/-U_mdet06Jk），并跟从列出的步骤来模拟一个Dos攻击：

然后攻击者的IP将被防火墙阻挡：

```
[root@dev1 ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@dev1 ~]#
```

```
[root@dev1 ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  0.0.0.0:0.0.0.0:0.0.0.0:0.0.0.0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

阻挡攻击者的IP地址

结论

在开启 `mod_security` 和 `mod_evasive` 的情况下，模拟攻击会导致 CPU 和 RAM 用量在源 IP 地址被加入黑名单之前出现短暂几秒的使用峰值。如果没有这些模块，模拟攻击绝对会很快将服务器击溃，并使服务器在攻击期间无法提供服务。

我们很高兴听见您打算使用（或已经使用过）这些工具。我们期望得到您的反馈，所以，请在留言处留下您的评价和问题，谢谢！

参考链接

- <https://www.modsecurity.org/>
- http://www.zdziarski.com/blog/?page_id=442

via: http://www.tecmint.com/protect-apache-using-mod_security-and-mod_evasive-on-rhel-centos-fedora/

作者：[Gabriel Cánepa](#) 译者：[wwy-hust](#) 校对：[wxy](#)

本文由 [LCTT](#) 原创翻译，[Linux中国](#) 荣誉推出

本文永久更新链接地址：<http://www.linuxidc.com/Linux/2015-06/118916.htm>



Fabric批量远程执行操作

Keepalived构建高可用LVS集群

相关资讯

Apache

Linux+Apache+PHP+Oracle 基础环境 (今 10:40)

Apache httpd 2.4.17 发布下载 (10月14日)

Apple MacBook搭建Apache多站点 (07月08日)

聊聊 Apache 开源协议 (今 10:13)

Ubuntu 14.04下 Apache修改网站根 (07月29日)

25 个有用 Apache ‘.htaccess’ (07月01日)

0

顶一下

图片资讯



聊聊 Apache 开源协议



Apache Web Server :



Linux系统入门学习 :



Ubuntu 14.04中Apache



Apache使用详解



HTTP服务器 Apache



在Arch上使用Nginx/



2月全球Web服务器：微

本文评论

查看全部评论 (0)

表情：

姓名：

☐ 匿名

字数 0

☒ 同意评论声明

发表

评论声明

- 尊重网上道德，遵守中华人民共和国的各项有关法律法规
- 承担一切因您的行为而直接或间接导致的民事或刑事法律责任
- 本站管理人员有权保留或删除其管辖留言中的任意内容
- 本站有权在网站内转载或引用您的评论
- 参与本评论即表明您已经阅读并接受上述条款

Linux公社简介 - 广告服务 - 网站地图 - 帮助信息 - 联系我们

本站（LinuxIDC）所刊载文章不代表同意其说法或描述，仅为提供更多信息，也不作

11 of 11

12/06/2015 08:29 AM