

ModSecurity

Jesús Rodríguez Heras
Juan Pedro Rodríguez Gracia
Gabriel Fernando Sánchez Reina

31 de mayo de 2018

- 1 ModSecurity
 - Definición
 - Características
- 2 Historia
- 3 Implementación

Definición

Es un motor de detección y prevención de intrusión de código abierto (Open Source) usado como firewall en aplicaciones web que permite detectar y bloquear ataques de tipo XSS y SQLi.

Características

La característica principal de ModSecurity es su capacidad de log y filtrado que permite almacenar el detalle de cada petición en un archivo de log que incluye los “payloads” de los POST HTTP. Los pedidos ofensivos serán rechazados o registrados según se configure.

Principios

Fue creado por Ivan Ristic en el año 2002 quien abordó el desarrollo de la aplicación después de haber utilizado durante un año y medio SNORT para monitorear el tráfico web y llegar a la conclusión de que necesitaba especificar más reglas.

Desarrollo posterior

En el año 2006 Breach Security Inc adquirió ModSecurity y fue, a partir de este momento, donde el desarrollo de esta aplicación corrió por cuenta de esta empresa que le aportó mayores y mejores reglas en su implementación.

Requisitos necesarios

Para la implementación de ModSecurity necesitamos lo siguiente:

- Servidor Apache en Debian.
- Apache ModSecurity.

Instalación y configuración

Para la instalación de Apache solo tenemos que introducir el siguiente comando en la terminal:

```
sudo apt-get install apache2
```

Luego, entramos en el archivo `/etc/apache2/apache2.conf` y añadimos `"ServerName www.trabajoASRC.com"` para dotar a nuestro servidor de un nombre de dominio.

Cambiar DNS

Para poder acceder a nuestro servidor mediante el nombre de dominio previamente establecido accedemos la archivo “/etc/hosts” y agregamos “10.0.2.15 www.trabajoASRC.com”.

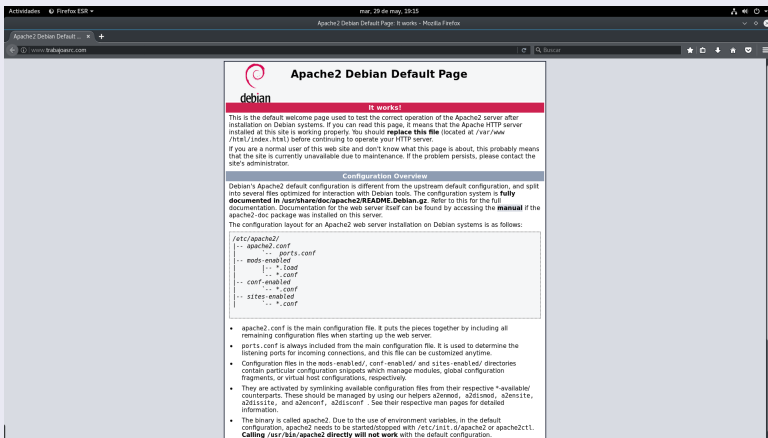
IP y nombre de dominio

La IP asociada al nombre de dominio es 10.0.2.15 debido a que estamos trabajando con una máquina virtual con Debian.

Servidor Apache en Debian

Ejecutando Apache

Al iniciar el servidor con “/etc/init.d/apache restart”, podemos ver que se ejecuta perfectamente con su correspondiente nombre de dominio.



Instalación

Para la instalación de Apache ModSecurity solo tenemos que introducir el siguiente comando en la terminal:

```
sudo apt-get install libapache2-modsecurity
```

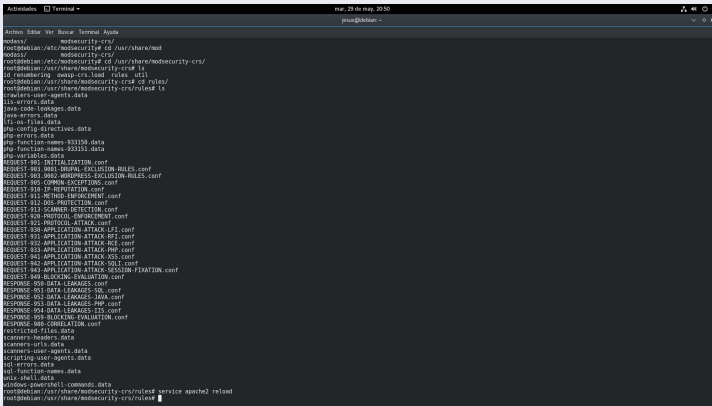
Lo que nos descargará e instalará correctamente la aplicación.

Configuración

Para la configuración, nos dirigimos a “/etc/modsecurity” y, dentro de este directorio tendremos el archivo “modsecurity.conf” que será el que tengamos que ir modificando según lo que queramos que haga ModSecurity.

Problemas configuración

Debido a que no tenemos los conocimientos necesarios sobre linux ni Apache, no hemos podido seguir, pero sí que hemos podido introducir algunas reglas en la configuración de ModSecurity:



```
Actividades Terminal - mar. 29 de may. 2018
jason@debian:~$
Activos Editar Ver Borrar Terminal Ayuda
root@debian:~# modsecurity-crs/
root@debian:~# cd /usr/share/mod
root@debian:~# modsecurity-crs/
root@debian:~# cd /usr/share/modsecurity-crs/
root@debian:~# ls
id_renaming oasp-crs.load rules.util
root@debian:~# cd /usr/share/modsecurity-crs/
root@debian:~# cd rules/
root@debian:~# ls
crawlers-user-agents.data
liss-errors.data
java-code-leakages.data
jvm-errors.data
lfi-ok-files.data
php-config-directives.data
php-errors.data
php-function-names-93150.data
php-function-names-93151.data
php-variables.data
REQUEST-901-INITIALIZATION.conf
REQUEST-903-ORIG-IP-EXCLUSION-RULES.conf
REQUEST-903-ORIG-IP-EXCLUSION-RULES.conf
REQUEST-903-ORIG-IP-EXCLUSION-RULES.conf
REQUEST-910-IP-REPUTATION.conf
REQUEST-911-METHOD-IMPROVEMENT.conf
REQUEST-912-SCN-PROTECTION.conf
REQUEST-913-SCANNER-DETECTION.conf
REQUEST-920-PROTOCOL-ENFORCEMENT.conf
REQUEST-921-PROTOCOL-ATTACK.conf
REQUEST-930-APPLICATION-ATTACK-LFI.conf
REQUEST-931-APPLICATION-ATTACK-RFI.conf
REQUEST-932-APPLICATION-ATTACK-RCE.conf
REQUEST-933-APPLICATION-ATTACK-PHP.conf
REQUEST-941-APPLICATION-ATTACK-XSS.conf
REQUEST-942-APPLICATION-ATTACK-SQL.conf
REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION.conf
REQUEST-944-BLOCKING-EVALUATION.conf
RESPONSE-950-DATA-LEAKAGES.conf
RESPONSE-951-DATA-LEAKAGES-SQL.conf
RESPONSE-952-DATA-LEAKAGES-JAVA.conf
RESPONSE-953-DATA-LEAKAGES-PHP.conf
RESPONSE-954-DATA-LEAKAGES-TLS.conf
RESPONSE-955-BLOCKING-EVALUATION.conf
RESPONSE-988-CORRELATION.conf
restricted-files.data
scanners-headers.data
scanners-urls.data
scanners-user-agents.data
scripting-user-agents.data
sql-errors.data
sql-function-names.data
unix-shell.data
windows-powershell-commands.data
root@debian:~# cd /usr/share/modsecurity-crs/rules/
root@debian:~# service apache2 reload
```