ModSecurity

Jesús Rodríguez Heras
Juan Pedro Rodríguez Gracia
Gabriel Fernando Sánchez Reina

29 de mayo de 2018

Resumen

Definición de ModSecurity como firewall de aplicaciones web Open Source.

Índice

1. ModSecurity

1.1. ¿Qué es?

Es un motor de detección y prevención de intrusión de código abierto (Open Source) para aplicaciones web.

Es un firewall de aplicaciones web que ejecuta como módulo del servidor web Apache. Provee protección contra diversos ataques web y permite monitorizar el tráfico HTTP(S), así como realizar análisis en tiempo real sin necesidad de hacer cambios en la estructura existente.

También provee un lenguaje de reglas y una API para implementar protecciones avanzadas. Esto significa que es posible filtrar tráfico HTTP(S), directamente en el servidor web, según el contenido de las peticiones de los clientes, lo cual permite detectar y bloquear ataques de tipo XSS (Cross Site Scripting)[1], SQLi (SQL injection)[2], etc.

Es un producto desarrollado por Breach Security y está disponible como Software Libre bajo la licencia GNU General Public License. A su vez, se encuentra disponbible bajo diversas licencias comerciales.

1.2. Características principales

Las características principales de ModSecurity son su capacidad de log y filtrado lo que permite almacenar el detalle de cada petición en un archivo de log, incluyendo los "payloads" de los POST HTTP. Los pedidos entrantes, a su vez, pueden ser analizados, y los pedidos ofensivos, serán rechazados (o simplemente registrados en el log, de acuerdo a cómo se configure). Esto nos permite que se ejecuten aplicaciones inseguras en nuestros servidores web ya que están siendo protegidas por ModSecurity.

2. Un poco de historia

ModSecurity fue creado por Ivan Ristic[3] en el año 2002. El señor Ristic abordó del desarrollo de esta aplicación después de haber utilizado durante un año y medio el SNORT[4] para monitorear el trafico web y llegar a la conclusión de que necesitaba una herramienta que le permmitiera especificar reglas más complejas y la capacidadd de realizar acciones relacionadas específicamente con el tráfico HTTP.

[1] Del inglés Cross-site scripting es un tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones Web, que permite a una tercera persona inyectar, en páginas web visitadas por el usuario, código JavaScript o en otro lenguaje similar (por ejemplo: VBScript), evitando medidas de control como la Política del mismo origen.

[2] Es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

[3] Especialista en seguridad web y autor de ModSecurity.

[4] Sistema de detección de intrusos en red libre y gratuito. Ofrece la capacidad de almacenamiento de bitácoras en archivos de texto y en bases de datos abiertas, como MySQL. Implementa un motor de detección de ataques y escaneo de puertos que permite registrar, aletar y responder ante cualquier anomalía previamente definida.

En septiempre de 2006 Breach Security[5] adquirió ModSecurity y fue a partir de este momento, donde el desarrollo de ModSecurity paso a llevarlo a cabo Breach Security.

3. Implementación

Para la implementación de ModSecurity, debemos contar con un servidor web Debian con Apache instalado y condigurado, en funcionamiento.

3.1. Instalación y configuración de Apache en Debian.

Con el comando "`sudo apt-get install apache2`" instalamos los archivos necesarios para que funcione nuestro servidor web.

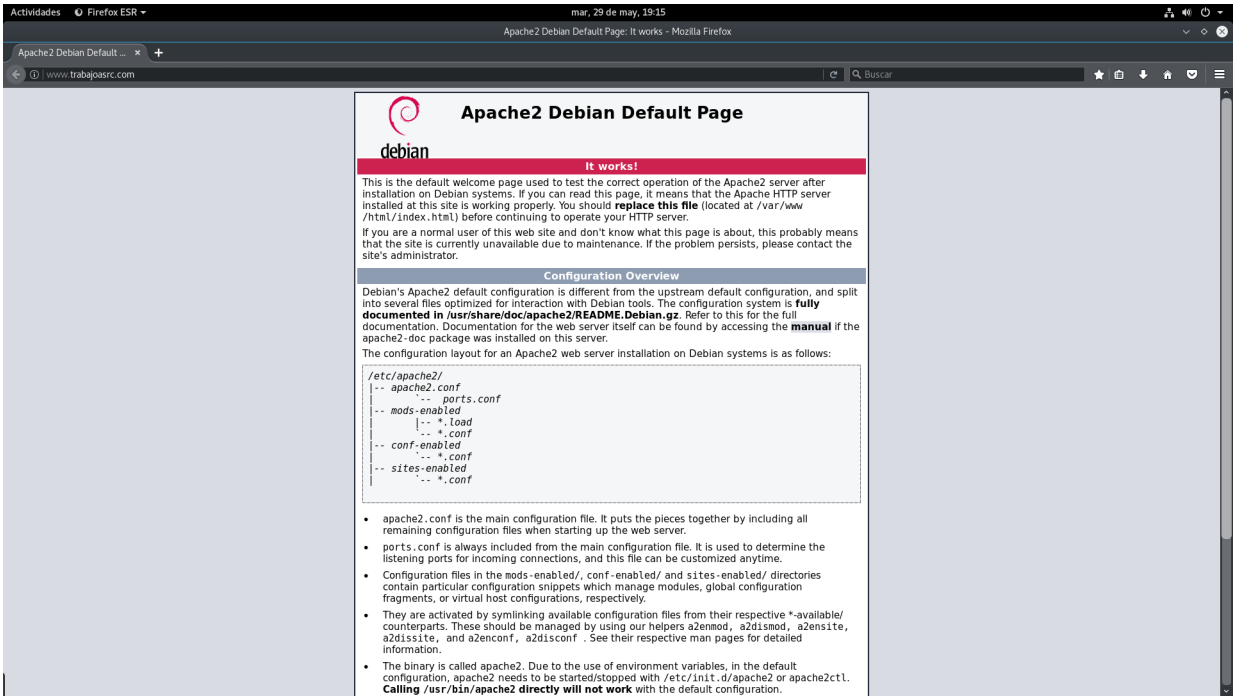
El archivo de configuración de apache2 se encuentra en la carpeta "`/etc/apache2`". En el archivo principal de condiguración, "`apache2.conf`" lo editaremos y añadiremos el siguiente parámetro: "`ServerName www.trabajoASRC.com`".

A continuación, vamos a cambiar el nombre de dominio de nuestro servidor web. Para ello, con el comando "`ifconfig`" encontramos que nuestra IP es `10.0.2.15`. Ahora, editamos el archivo "`/etc/hosts`" incluyendo nuestra IP (`10.0.2.15`) y la entrada de nuestro servidor "`www.trabajoASRC.com`".

Para arrancar el servidor, introducimos el siguiente comando: "`/etc/init.d/apache2 restart`". Si queremos pararlo, solo tenemos que introducir el comando "`/etc/init.d/apache2 stop`".

Tras ejecutar el comando de inicio del servidor, nos dirigimos al navegado, introducimos la dirección de nuestro servidor web "`www.trabajoASRC.com`" y se nos muestra la siguiente pantalla:

[5]Fundada en 2004, fue el proveedor líder de seguridad e integridad de aplicaciones web continuas en tiempo real que protege la información confidencial basada en la web.



3.2. Instalación y configuración de Apache ModSecurity

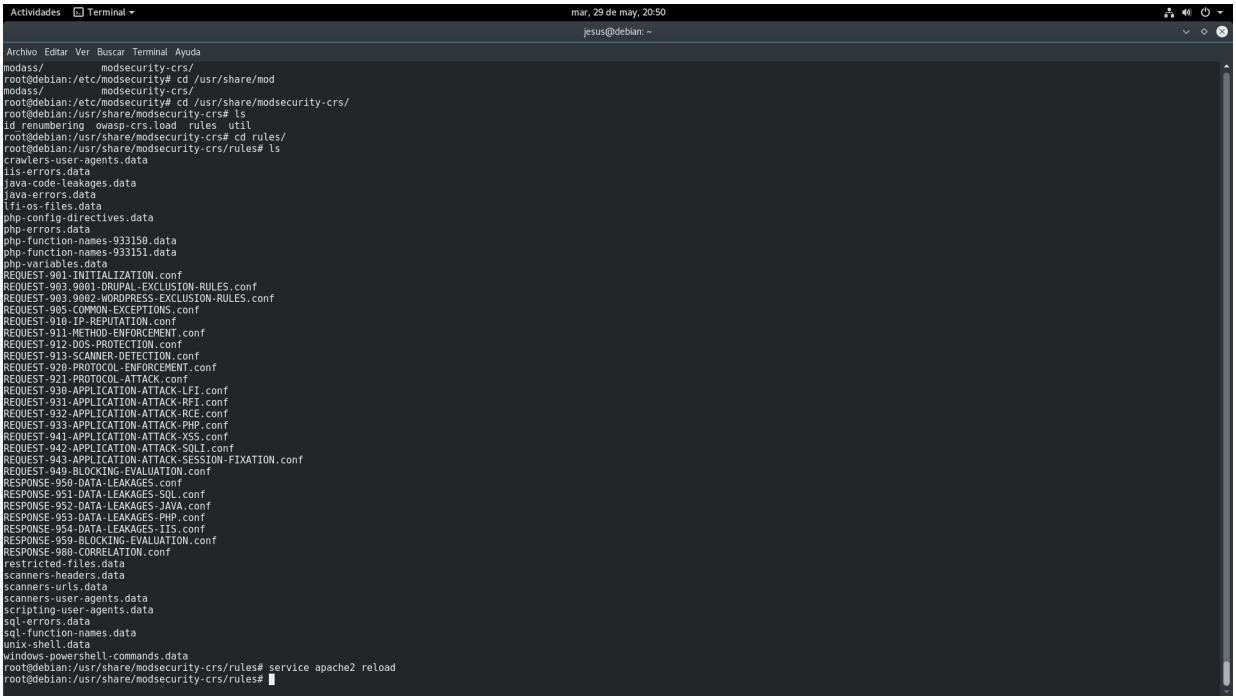
Con el comando "`apt-get install libapache2-modsecurity`" instalamos los paquetes necesarios para la correcta instalación de ModSecurity. Tal como se ha mencionado anteriormente, ModSecurity trabaja utilizando reglas para la detección y filtrado de diferentes tipos de ataques, las cuales se definen utilizando un lenguaje propio. Por defecto incluye un conjunto de reglas genéricas mantenidas por la comunidad OWASP[6], las cuales son liberadas de manera gratuita y protegen contra los ataques básicos.

A continuación, nos dirigimos a "`/etc/modsecurity`" y encontraremos el archivo "`modsecurity.conf-recommended`". Para poder trabajar con él sin perder los datos, realizamos una copia con el comando "`cp modsecurity.conf-recommended modsecurity.conf`", que nos creará el archivo de configuración de ModSecurity.

Una vez configurado ModSecurity, tal como se indica aquí: (`https://samhobbs.co.uk/2016/03/getting-started-apache-modsecurity-debian-and-ubuntu`).

A partir de aquí, tendríamos configurado nuestro servidor de Apache con ModSecurity activado pero, por falta de conocimientos y de técnica, no hemos podido seguir adelante con la implementación. Lo que sí hemos conseguido es recolectar algunas de las reglas de ModSecurity que se muestran a continuación:

[6]Acrónimo de Open Web Application Security Project, (en inglés 'Proyecto abierto de seguridad de aplicaciones web') es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo.



4. Referencias

- https://es.wikipedia.org/wiki/Mod_Security
- https://www.modsecurity.org/
- https://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL
- https://es.wikipedia.org/wiki/Cross-site_scripting
- https://blog.ivanristic.com/2006/09/modsecurity-has-been-acquired.html
- http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m3/instalacin_y_configuracin_de_apache.html
- https://www.linuxito.com/seguridad/562-como-instalar-y-configurar-modsecurity-en-apache-sobre-servidores-debian
- https://es.wikipedia.org/wiki/Open_Web_Application_Security_Project
- https://samhobbs.co.uk/2016/03/getting-started-apache-modsecurity-debian-and-ubuntu