Mod Security. Desactivación global de reglas por path

Introducción

Una vez más, con el tema de Mod Security, compruebo que el 99% de los administradores de sistemas, sigue la misma pauta de siempre, la salida hacia adelante más fácil, deshabilitando todo.

Soy cabezón, y no he basado mi seguridad en mis máquinas, en abrir la puerta menoscabando la seguridad perimetral.

Tengo cliente a los que llevo sus servicios, que son incapaces de aguantar en firme, con las normas y reglas de seguridad que trato de imponerles, pese a que eso suponga un aumento de costes en horas para limpiar problemas derivados de los **mini hackeaos**

Escenario

En el caso que me llevó a este tema, estaba implicado DirectAdmin y el webmail RoundCube en una situación algo especial.

Con las cuentas de sistema `usuario` usadas como cuenta de correo, RoundCube recibía una serie de errores al lanzarse prohibiciones vía Mod Security.

> Connection Error (Failed to reach the server)! !Error de conexión fallo al intentar alcanzar el servidor)!

> Cuando teneos problemas con RoundCube como con muchas aplicaciones web, insisto a mis clientes que observen las webmaster tools del navegador y/o al menos las cabeceras de respuesta (406) más allá de los mensajes tipo **Alert** de las aplicaciones.

Webmaster Tools - Navegador

Image not found or type unknown

Al final, localizando las reglas afectadas por RoundCube a nivel hostname, salieron a la palestra las siguiente reglas afectadas:

- 911100
- 932260
- 920340
- 932235
- 941100
- 941130
- 941160
- 941170
- 949110
- 980130

Todas ellas, con Paranoia Level 1, ModSecurity :: Concepto Paranoia Level

Uy... que cosas. EL **PR 1** es básicamente el nivel con menor número de falsos positivos, y muchas de estas rules, ofrecen una protección extraordinaria a muchos de los errores más comunes de los "programadores" de javascript.

Así que las soluciones que se presentan en, StackOverFlow, el foro de DirectAdmin, y otras muchas, no me convencían, porque se trata de atajos (workaround) que llevan a la desactivación de la regla de forma global, o en su defecto, no cumplen con la documentación de Mod Security o de DirectAdmin.

Solución

No hay que dar muchas vueltas, ni ir a templates de DirectAdmin.

Nada mas lejos.

La cuestión esta en el propio Mod Security que tiene en su instalación un fichero llamado `REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example` y en el caso de **DirectAdmin** ubicado en `/etc/modsecurity.d/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example`

Teniendo en cuenta que la instalación de Mod Security en DirectAdmin, cumple el estándar, lee todo los ficheros del directorio terminados en `.conf` `/etc/modsecurity.d/*.conf` así que se trata de leer su contenido, en el cual hay bastante ejemplos, para aprender y evitar salir por la puerta de atrás, y en su lugar cerrar bien nuestra casa.

```
SecRule REQUEST_FILENAME "@beginsWith /roundcube" \
    "id:1001,\
```

```
    phase:2,\
    pass,\
    nolog,\
    ctl:ruleRemoveById=911100,\
    ctl:ruleRemoveById=932260,\
    ctl:ruleRemoveById=920340,\
    ctl:ruleRemoveById=932235,\
    ctl:ruleRemoveById=941100,\
    ctl:ruleRemoveById=941130,\
    ctl:ruleRemoveById=941160,\
    ctl:ruleRemoveById=941170,\
    ctl:ruleRemoveById=949110,\
    ctl:ruleRemoveById=980130"
```

Este sería su contenido.

Hacemos la prueba de que no pasa nada en nuestra instalación, y como tenemos **Nginx*, es sencillo:

```
~ ❯ nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Con lo cual podemos hacer un `reload` y probar si las rules desactivadas para `/roundcube` vía `REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf` funciona como deseamos y si somos más atrevidos, pues tratamos de hacer una prueba de concepto, en una web sin usar dicho **path**.

> He visto durante mi búsqueda, aunque un poco antiguas, post, artículos y entradas, que hablan de problemas con el `/phpmyadmin/` y a ese caso sería aplicable el modelo (no las rules)

Nota para DirectAdmin

Como no es un sistema que siga los patrones de DirectAdmin, ya que no encuentro su posibilidad de uso, esto supone que cuando haga un `da build rewrite_confs` DirectAdmin machacará el fichero, ya que descarga entre otros el sistema de rules de Mod Security así que al margen de añadirlo a mis sistema de backups de ficheros a guardar, lo mejor será ya que se trata de un fichero que el no usa realmente, pero lo quiere borrar en un comando de borrado con `glob` es protegerlo contra escritura.

```
chattr +i /etc/modsecurity.d/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf
```

Así no habrá líos con esto.

```
[activating module `aclr' in /etc/httpd/conf/httpd.conf]
mod_aclr2 has been installed successfully.
Restarting apache.
rm: cannot remove '/etc/modsecurity.d/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf': Operation not permitted
Installing OWASP Core Rule Set for ModSecurity...
download_cached: using cached '/usr/local/directadmin/custombuild/cache/owasp-modsecurity-crs-4.5.0.tar.gz' file
```

Idea y apuntes

- ModSecurity Rules: Global or for Hostname?
- How do I skip certains rules for parameter in a path in ModSecurity?

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de Castris

Si necesitas soporte profesional puedes contratar con Castris soporte profesional.

Revision #3
Created 1 September 2024 17:09:35 by Abkrim
Updated 9 September 2024 17:32:51 by Abkrim