

(In)Eficacia de la correlación de logs en OSSEC para detectar XSS

Daniel Medianero (m313)
dmedianero@gmail.com
<http://www.meleagro.es.kz>

OSSEC es un detector de intrusos de Host(HIDS) que está alcanzando gran popularidad ultimamente. No es de extrañar dado que tiene múltiples e interesantes funciones: correlación de eventos, control de integridad de ficheros, multiplataforma(*nix, BSD's, Windows), soporta instalación cliente-servidor-local y personalización de reglas (en formato XML).

El propósito de este post es demostrar que, si bien la correlación de eventos puede detectar intentos de intrusiones no es la panacea ni muchísimo menos. En concreto nos centramos en la "única" regla anti XSS de OSSEC. Esta regla se encuentra en el fichero *web_rules.xml* y tiene el siguiente aspecto:

```
<rule id="31105" level="6"><if_sid>31100</if_sid><url>%3Cscript|%2Fscript|script>|script%3E|SRC=javascript|IMG%20|</url><url>%20ONLOAD=|INPUT%20|iframe%20</url><description>XSS (Cross Site Scripting) attempt.</description><group>attack,</group></rule><br/>
```

Como podemos apreciar las reglas de correlación de eventos son fácilmente entendibles debido a que están escritas en formato XML. En este caso se basan en una pequeña lista negra:

```
%3Cscript
%2Fscript
script>
script%3E
SRC=javascript
IMG%20
%20ONLOAD=
INPUT%20
iframe%20
```

Esta regla está relacionada con la que veremos a continuación:

```
<rule id="31106" level="12"> <if_sid>31103, 31104, 31105</if_sid><id>^200</id><description>A web attack returned code 200 (success).</description> <group>attack,</group></rule><br/>
```

De manera que si la regla 31105 (XSS) salta y el código de resultado que devuelve el servidor es un 200 OK salta la alerta 31106 (A web attack returned code 200).

Lo primero que hay que destacar es que la búsqueda de patrones se realiza sobre los ficheros de log del servidor web. En el caso de Apache estos tags aparecerán en el fichero *access_log* con lo cual tenemos la primera debilidad:

cualquier intento de XSS utilizando el método POST no será detectado. Tampoco serán detectados los intentos de XSS en las cabeceras http. Esto es debido a que por lo general una traza del fichero access_log tiene la siguiente pinta en el caso de un GET:

```
127.0.0.1 - - [27/Apr/2008:19:30:44 +0200] "GET /ossec/index.php?
f=VALOR_DEL_PARAMETRO HTTP/1.1" 200 259
```

En el caso de que se produzca inyección de código en el parametro *f* podrá ser correlado. Sin embargo en el caso de utilizar el método POST el valor del parametro no queda registrado en la traza por lo que no se puede correlar:

```
127.0.0.1 - - [27/Apr/2008:19:30:44 +0200] "POST /ossec/index.php HTTP/1.1" 200 259
```

De la misma manera no quedan registrados los valores de la cabecera (El servidor Apache puede ser configurado para que sí se muestren aunque en su configuración por defecto no es así y no es habitual encontrarse con servidores Apache que muestren mucha más información en sus trazas de las expuestas anteriormente).

Nos situamos en el caso de que el ataque se produzca utilizando el método GET. En este caso el correlador de logs compara con la lista negra y en caso afirmativo produce una alerta:

```
** Alert 1209321044.76264: mail - web,accesslog,attack,
2008 Apr 27 20:30:44 MI_SERVIDOR->/var/log/httpd/access_log
Rule: 31106 (level 12) -> 'A web attack returned code 200 (success).'
Src IP: 127.0.0.1
User: (none)
127.0.0.1 - - [27/Apr/2008:20:30:43 +0200] "GET /ossec/index.php?f=s%3Cscript HTTP/1.1"
200 2593
```

Vemos que en este caso el patrón **%3Cscript** ha hecho saltar las alarmas. A partir de aquí no es difícil imaginar que la correlación con la lista negra es fácilmente evitable.

Si probamos esa misma inyección de manera ofuscada en código hexadecimal comprobados la cadena en el fichero *access_log*:

```
127.0.0.1 - - [27/Apr/2008:20:41:28 +0200] "GET /ossec/index.php?f=s%3c
%73%63%72%69%70%74 HTTP/1.1" 200 2593
```

Sin embargo en el detector de intrusos no salta la alarma. Hemos conseguido realizar el ataque evadiendo el detector de intrusos.

Conclusiones.

La correlación de eventos puede prevenir algunos tipos de ataques web pero no es la panacea para la detección de los mismos. Estos detectores pueden ser evadidos sin demasiada dificultad. Las listas negras son a menudo insuficientes y tienen como riesgo añadido la falsa sensación de seguridad que aportan.