GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Seminario web: Hardening de Apache

Ejercicios

017 TU AYUDA EN CIBERSEGURIDAD
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

1. EJERCICIOS PRÁCTICOS

Este ejercicio práctico consiste en identificar, a través del log proporcionado "modsec_audit.log", diferentes ataques realizados a nuestra aplicación "dummy" en el servidor web Apache. Las peticiones que se pueden apreciar son el resultado de tener activo "ModSecurity". Vamos a identificar los tipos de ataque y advertencias que nos podemos encontrar contestando a algunas preguntas.

Abriremos el fichero "log" con cualquier editor de texto.

- **Pregunta 1:** ¿Podrías indicar qué tipo de ataque es el que se realiza en este fragmento del fichero log?

```
--a19b5a47-B--
GET /index.html?param?=../../../etc/passwd HTTP/1.1
Host: 192.168.1.5:8888
User-Agent: curl/7.65.1
Accept: */*
```

Cuadro 1 - Fragmento fichero de log

Realizando una asociación con el tipo de regla que encaja a este tipo de ataque, ModSecurity genera en el log una serie de bloques informativos.

- **Pregunta 2:** ¿Podrías identificar las líneas donde aparezcan estos bloques?

- **Pregunta 3:** En este segundo caso, ¿podrías indicar qué tipo de ataque es el que se realiza en este fragmento del fichero log?

```
--97d8ad19-B--
GET
/index.html?param=&mfMo%3D6544%20AND%201%3D1%20UNION%20ALL%20SELECT%20
1%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctab
le_name%20FROM%20information_schema.tables%20WHERE%202%3E1--
%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fp
asswd%27%29%23 HTTP/1.1
Accept-Encoding: gzip,deflate
Host: 192.168.1.5:8888
Accept: */*
User-Agent: sqlmap/1.1.12#stable (http://sqlmap.org)
Connection: close
Cache-Control: no-cache
```

Cuadro 2 - Fragmento fichero de log

Realizando una asociación con el tipo de regla que encaja a este tipo de ataque, ModSecurity genera en el log una serie de bloques informativos.

- **Pregunta 4:** ¿Podrías identificar las líneas en el log donde aparezcan estos bloques?

- **Pregunta 5**: ¿Qué tipo de REQUEST-NUM-TIPO_DE_ATAQUE_***.conf es aplicado al detectar el ataque anterior?

2. SOLUCIÓN DEL EJERCICIO:

Pregunta 1

El tipo de ataque que se ha realizado en este caso es **"Local File Inclusion" (LFI) o inclusión local de ficheros**. Se evidencia el tipo de petición que provoca el atacante queriendo leer "/etc/passwd" inyectando en el parámetro "param".

Pregunta 2

A continuación, se pueden observar las líneas que nos pide el enunciado.

```
1340
1341 --6125dd0e-H--
1342 Message: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host. [file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"
1343 Message: Warning. Pattern match "(?i)(?:\\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5(?:c(?:0%25af|1%259c)|2f|5c)|%46|f)|(?:(?:f(?:8
1344 Message: Warning. Matched phrase "../" at REQUEST_URI. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "77"]
1345 Message: Warning. Matched phrase "../" at REQUEST_URI. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "77"]
1346 Message: Warning. Matched phrase "etc/passwd" at ARGS:param?. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [lir
1347 Message: Warning. Matched phrase "etc/passwd" at ARGS:param?. [file "/usr/share/modsecurity-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [lir
```

Figura 1 - Líneas donde se aprecia la advertencia de ModSecurity.

Pregunta 3

Se está intentando producir un **ataque de inyección SQL**. Lo sabemos ya que los datos que se inyectan en `param` son cadenas características de consultas SQL, además de ver que la cabecera del navegador o "`user-agent`" es `sqlmap/1.1.12#stable.`

Pregunta 4

Algunas de las líneas que muestran la evidencia del ataque.

```
2593 Message: Warning. Matched phrase "sqlmap" at REQUEST_HEADERS:User-Agent. [file "/usr/share/modsecurity-crs/rules/REQU
2594 Message: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host. [file "/usr/share/modsecurity-crs/rules/REQUEST
2595 Message: Warning. Pattern match "(?i)(?:\\x5c|(?:%(?:c(?:0%(?:[2aq]f|5c|9v)|1%(?:[19p]c|8s|af))|2(?:5(?:c(?:0%25af|1%
2596 Message: Warning. Matched phrase "../" at REQUEST_URI. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATIC
2597 Message: Warning. Matched phrase "../" at REQUEST_URI. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATIC
```

Figura 2 - Evidencias del ataque de inyección SQL (I)

```
2603 Message: Warning. detected SQLi using libinjection with fingerprint 'n&1UE' [file "/usr/share/modsecurity-crs/rules/
2604 Message: Warning. detected SQLi using libinjection with fingerprint 'n&1UE' [file "/usr/share/modsecurity-crs/rules/
```

Figura 3 - Evidencias del ataque de inyección SQL (II)

```
2621 Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 10.0.2.2] ModSecurity: Warning. detected SQLi using libinjection with fingerprint
2622 Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 10.0.2.2] ModSecurity: Warning. Pattern match "(?i:\\\\\\\\\b(?:m(?:s(?:ysaccessob
2623 Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 10.0.2.2] ModSecurity: Warning. Pattern match "(?i:(?:\\\\\\\\s*?(?:exec|execute).
2624 Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 10.0.2.2] ModSecurity: Warning. Pattern match "(?i:(?:union(.*?)select(.*?)from))
2625 Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 10.0.2.2] ModSecurity: Access denied with code 403 (phase 2). Operator GE matched
2626 Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 10.0.2.2] ModSecurity: Warning. Operator GE matched 5 at TX:inbound anomaly score.
```

Figura 4 - Evidencias del ataque de inyección SQL (III)

Pregunta 5: Según aparece en la línea 2603, la respuesta es "REQUEST-942-APPLICATION-ATTACK-SQLI.conf".