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

Webinar: Apache hardening

Exercises

017 TU AYUDA EN CIBERSEGURIDAD
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

INDEX

FIGURE INDEX

FRAME INDEX

1. PRACTICAL EXERCISES

This practical exercise consists in identifying, through the log provided "modsec_audit.log", different attacks made to our "dummy" application in the Apache web server. The requests that can be seen are the result of having "ModSecurity" active. We will identify the types of attacks and warnings that we can find by answering some questions.

Open the log file with any text editor.

- **Question 1**: Could you indicate what type of attack is carried out on this fragment of the log file?

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

Frame 1 Log file fragment (I)

By making an association with the type of rule that fits this type of attack, ModSecurity generates a series of informative blocks in the log.

- **Question 2:** Can you identify the lines where these blocks appear?

- **Question 3:** In this next second case, could you indicate what type of attack is carried out on this fragment of the log file?

```
--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
```

Frame 2 Log file fragment (II)

By making an association with the type of rule that fits this type of attack, ModSecurity generates a series of informative blocks in the log.

- **Question 2:** Can you identify the lines where these blocks appear?

- **Question 5**: What type of REQUEST-NUM-ATTACK_TYPE_***.conf is applied when detecting the previous attack?

Exercise solution:

Question 1

The type of attack performed in this case is **"Local File Inclusion" (LFI)**. The type of request caused by the attacker wanting to read "`/etc/passwd`" is evidenced by injecting the parameter "`param`".

Question 2

Show below there are the lines required by the statement.

```
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"] [lin
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%8)?0%
1344  Message: Warning. Matched phrase "../" at REQUEST_URI. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "77"] [id "
1345  Message: Warning. Matched phrase "../" at REQUEST_URI. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "77"] [id "
1346  Message: Warning. Matched phrase "etc/passwd" at ARGS:param?. [file "/usr/share/modsecurity-crs/rules/REQUEST-930-APPLICATION-ATTACK-LFI.conf"] [line "108
1347  Message: Warning. Matched phrase "etc/passwd" at ARGS:param?. [file "/usr/share/modsecurity-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "448
```

Figure 1 Lines showing the ModSecurity warning

Question 3

An attempt is being made to produce an **SQL injection attack**. We know this because both data injected into `param` are characteristic strings of SQL queries and we see that the browser header or "`user-agent`" is `sqlmap/1.1.12#stable`.

Question 4

Some of the lines showing evidence of the attack.

```
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
```

Figure 2 Evidence of SQL injection attack (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/
```

Figure 3 Evidence of SQL injection attack (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(?:ysaccessobj
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.
```

Figure 4 Evidence of SQL injection attack (III)

Question 5: As it appears in line 2603 the answer is "REQUEST-942-APPLICATION-ATTACK-SQLI.conf"