Identifying web application attacks through logs Quiz

Creator: Igor Vieira

Description: By taking this quiz, you will be able to test your knowledge on the concepts taught in the course Identifying Web Attacks through Logs. This 21-question quiz covers knowledge-based questions across important topics that this course covered. You should take this exam once you have completed all of the lessons in the Identifying Web Attack through Logs course.

---

1) Which of the following describes the model that is web application based? (1PT)

a) Question-Answer model
b) Request-Send model
c) Client-Server model
d) Browser-Server model

2) Which of the following protocols is used to request and answer web application messages between Client and Server? (1PT)

a) DNS
b) HTTP
c) PHP
d) User agent

3) _____ are examples of web server software. (1PT)

a) Apache, Nginx and IIS

b) Ncat, telnet, Burp
c) HTTP, DNS, PHP
d) IP, TCP, UDP

4) Which of the following HTTP Response Status codes identifies a wrong user action? (1PT)

a) 200
b) 404
c) 500
d) 503

5) HTTP relies on IP to transfer messages between a Client and a Server. (1PT)

a) True
b) False

For questions 6 and 7, consider the Apache web server log below with the default logging configuration.
10.3.89.4 - - [22/Jun/2019:07:07:13 +0000] "GET /appini.html HTTP/1.1" 200 612 "http://www.example.com/login.html" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36"

6) The web server log is complete. (1PT)

a) True
b) False

7) _____ is the IP Address of the _____. The HTTP method used was _____ and the server answer code was _____ (1PT)

a) 10.3.89.4, server, GET, 612
b) 10.3.89.4, client, GET, 200
c) 10.3.89.4, client, WOW64, 537.36
d) 10.3.89.4, server, WOW, 612

8) Which of the following is **NOT** an example of key information provided by the web server log. (1PT)

a) Client IP
b) User Agent
c) System uptime
d) HTTP Method

9) Which of the following key fields from the Web Server log **cannot** be crafted by a malicious user? (1PT)

a) HTTP Status Code
b) UserID
c) Date and Time
d) User Agent

10) "An action that attempts to exploit a vulnerability or cause an impact to a web application." This is the definition of: (1PT)

a) Vulnerability
b) Risk
c) Target
d) Attack

11) _____ is a project that catalogs the most common _____. (1PT)

a) OWASP TOP 10 Project, attacks
b) OWASP TOP 10 Project, vulnerabilities
c) Open Web Foundation, attacks
d) Open Web Foundation, vulnerabilities

12) URL encoding is used only to perform attacks against web applications. (1PT)

a) True
b) False

13) Analyze the logs below and identify the type of attack. (1PT)

10.1.0.10 - - [14/Jul/2019:13:06:30 -0400] "GET /app/?username=Pablo&password=111111&Login=Login HTTP/1.1" 200 1401 "http://example.com/app/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.1.0.10 - - [14/Jul/2019:13:06:31 -0400] "GET /app/?username=Pablo&password=iloveu&Login=Login HTTP/1.1" 200 1401 "http://example.com/app/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.1.0.10 - - [14/Jul/2019:13:06:33 -0400] "GET /app/?username=Pablo&password=000000&Login=Login HTTP/1.1" 200 1401 "http://example.com/app/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.1.0.10 - - [14/Jul/2019:13:06:34 -0400] "GET /app/?username=Pablo&password=michelle&Login=Login HTTP/1.1" 200 1401 "http://example.com/app/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"

a) Brute Force
b) XSS
c) Vulnerability scan
d) File Injection

14) Which type of attack can be identified in the logs from Figure 1 below? (1PT)

```
10.1.0.10 - - [30/Jul/2019:04:29:48 -0400] "GET /shell?cat%20/etc/passwd HTTP/1.1" 404 203 "-" "Mozilla/
5.00 (Nikto/2.1.6) (Evasions:None) (Test:007084)"
10.1.0.10 - - [30/Jul/2019:04:29:48 -0400] "GET /sitecore/shell/webservice/service.asmx HTTP/1.1" 404 23
6 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:007132)"
10.1.0.10 - - [30/Jul/2019:04:29:49 -0400] "GET /shell?cat+/etc/hosts HTTP/1.1" 404 203 "-" "Mozilla/5.0
0 (Nikto/2.1.6) (Evasions:None) (Test:007235)"
10.1.0.10 - - [30/Jul/2019:05:19:21 -0400] "GET /cgi-bin/rwwwshell.pl HTTP/1.1" 404 218 "-" "Mozilla/5.0
 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
10.1.0.10 - - [30/Jul/2019:05:19:24 -0400] "GET /cgi-bin/dasp/fm_shell.asp HTTP/1.1" 404 223 "-" "Mozill
a/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
10.1.0.10 - - [30/Jul/2019:05:19:25 -0400] "GET /cgi-bin/jailshell HTTP/1.1" 404 215 "-" "Mozilla/5.0 (W
indows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
10.1.0.10 - - [30/Jul/2019:05:19:25 -0400] "GET /cgi-bin/noshell HTTP/1.1" 404 213 "-" "Mozilla/5.0 (Win
dows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
10.1.0.10 - - [30/Jul/2019:05:20:08 -0400] "GET /App_Config/sitecore/shell/sitecore.version.xml HTTP/1.1
" 404 244 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
10.1.0.10 - - [30/Jul/2019:05:20:08 -0400] "GET /sitecore/shell/WebService/Service.asmx HTTP/1.1" 404 23
6 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
10.1.0.10 - - [30/Jul/2019:05:20:11 -0400] "GET /shell?cat%20/etc/passwd HTTP/1.1" 404 203 "-" "Mozilla/
5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
10.1.0.10 - - [30/Jul/2019:05:20:11 -0400] "GET /sitecore/shell/webservice/service.asmx HTTP/1.1" 404 23
6 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
10.1.0.10 - - [30/Jul/2019:05:20:12 -0400] "GET /shell?cat+/etc/hosts HTTP/1.1" 404 203 "-" "Mozilla/5.0
 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
```

Figure 1 - Example of Logs

a) Brute Force
b) XSS
c) Vulnerability scan
d) File Injection

15) Which type of attack can be identified in the logs below? (1PT)

10.1.0.10 - - [14/Jul/2019:09:40:40 -0400] "POST /login.php HTTP/1.0" 302 - "-" "Mozilla/5.0 (Hydra Proxy)"
10.1.0.10 - - [14/Jul/2019:09:40:41 -0400] "POST /login.php HTTP/1.0" 302 - "-" "Mozilla/5.0 (Hydra Proxy)"
10.1.0.10 - - [14/Jul/2019:09:40:41 -0400] "POST /login.php HTTP/1.0" 302 - "-" "Mozilla/5.0 (Hydra Proxy)"
10.1.0.10 - - [14/Jul/2019:09:40:41 -0400] "POST /login.php HTTP/1.0" 302 - "-" "Mozilla/5.0 (Hydra Proxy)"

a) XSS
b) Brute Force
c) Vulnerability scan
d) File Injection

16) Which type of attack can be identified in the log below? (1PT)

10.1.0.10 - - [08/Sep/2019:10:45:15 -0400] "GET /login/?id=%20AND%20%28SELECT%208038%20FROM%28SELECT%20COUNT%28%2A%29%2C29%29x%20FROM%20INFORMATION_SCHEMA.PLUGINS%20GROUP%20BY%20x%29a%29 HTTP/1.1" 302 20 “-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"

a) XSS
b) CSRF
c) Vulnerability scan
d) SQL Injection

17) Which type of attack can be identified in the log below? (1PT)

10.1.0.10 - - [10/Jul/2019:17:35:13 -0400] "GET /dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert(%22%20Identify%20Web%20Attacks%20Through%20Logs%22%20)%3C/script%3E HTTP/1.1" 200 1349 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"

a) XSS
b) CSRF
c) Vulnerability scan
d) SQL Injection

18) _____ is a command that can help to identify a _____ attack. (1PT)

a) Netstat, SYN Flood
b) Netstat, HTTP Flood
c) Ping, ACK Flood
d) Ping, HTTP Flood

19) Based on the log below, complete the sentence: (1PT)

[Sat Jul 14 13:40:10 2019] [error] [client 10.1.0.10] ModSecurity: Warning. Pattern match "(?:(?<!\\\\w)(?:\\\\.(?:ht(?:access|passwd|group)|www_?acl)|global\\\\.asa|httpd\\\\.conf|boot\\\\.ini)\\\\b|\\\\/etc\\\\/)" at ARGS:page. [file "/etc/apache2/modsecurity-crs/base_rules/modsecurity_crs_40_generic_attacks.conf"] [line "205"] [id "950005"] [rev "3"] [msg "Remote File Access Attempt"] [data "Matched Data: /etc/ found within ARGS:page: ../../../../../../etc/passwd"] [severity "CRITICAL"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/WEB_ATTACK/FILE_INJECTION"] [tag "WASCTC/WASC-33"] [tag "OWASP_TOP_10/A4"] [tag "PCI/6.5.4"] [hostname "10.2.0.101"] [uri "/dvwa/vulnerabilities/fi/"] [unique_id "XfUsin8AAQEAAAgcUOwAAAAG"]

_____ IP address performed a _____ attack on _____ IP address.

a) 10.1.0.10, File Injection, 10.2.0.101
b) 10.2.0.101, WASCTC, 10.1.0.10
c) 10.2.0.101, File Injection, 10.1.0.10
d) 10.1.0.10, Remote File Access Download, 10.2.0.101

20) The only difference between IPv4 and IPv6 web server logs is the IP fields" (1PT).

a) True
b) False

21) Only web server logs can be used to identify a web application attack. (1PT)

a) True
b) False

Answer Key

1. **Answer: C**

Explanation: Web applications use the Client-Server model. In this model, the client can be a web browser, and the server is the web server. The model works with clients requesting information and servers serving the information.

2. **Answer: B**

Explanation: HTTP – Hypertext Transfer Protocol is the protocol used by clients to ask for information from the servers. GET is an example of an HTTP request.

3. **Answer: A**

Explanation: Only option A contains examples of web server software. All the other option are not examples of web server software. DNS and HTTP are protocols; Burp and telnet are user agents, and TCP and UDP are protocols.

4. **Answer: B**

Explanation: HTTP Response codes are composed of 3 numbers. Each number means something. The first number is the category of the code. The user-related category is the 4XX; therefore, the answer is B – 404.

5. **Answer: A**

Explanation: HTTP is a top layer protocol, and the IP address is one of the lower layer protocols that is used by HTTP. IP is used to connect the client and the server.

6. **Answer: A**

Explanation: The web server log contains all the key fields. Here is a list of the fields:
Source IP / Client IP, UserID, Date/Time, Method, Requested File, HTTP Status Code, HTTP Referrer, and User Agent

7. **Answer: B**

Explanation: 10.3.89.4, client, GET, 200 is the only option that can complete the sentence correctly.

8. **Answer: C**

Explanation: Web server logs do not have information about hardware or operational system. Source IP / Client IP, UserID, Date/Time, Method + Requested File, HTTP Status Code, HTTP Referrer, User Agent are examples of Key Information provided in web server logs.

9. **Answer: A**

Explanation: The HTTP Status code is generated by the web server, so it cannot be crafted by the user. All of the fields generated by the web server cannot be crafted.

10. **Answer: D**

Explanation: The sentence talks about an action to exploit a vulnerability, so the answer is "Attack." Attacks usually exploit a vulnerability.

11. **Answer: B**

Explanation: The OWASP TOP 10 Project is the project maintained by OWASP that catalogs the most common vulnerabilities and errors that are seen in web applications.

12. Answer: B

Explanation: Encoding is needed because HTTP only accepts ASCII characters. One of the uses of encoding is to represent other writing systems, like Arabic.

13. Answer: A

Explanation: A brute force attack is easy to identify because of the numerous GET requests. There are many GET requests, and the time between the requests is only 1 or 2 seconds.

14. Answer: C

Explanation: The vulnerability scan can be identified by the Nikto user agent, the number of requests, the number of 404 errors, the difference between the requests, and the requested files.

15. Answer: B

Explanation: The request uses POST, so it is hard to identify this attack. The login page, the number of accesses, and the HYDRA user agent help us to figure out that this is abrute force attack.

16. Answer: D

Explanation: There are many SQL words in the log such as SELECT, UNION, and others.

17. Answer: A

Explanation: The biggest indicator of the XSS attack is the word “script” and the encoded request with the alert “%3Cscript%3Ealert”.

18. Answer: A

Explanation: The netstat command will show the status of the TCP connections. If you see lots of SYN_RECEIVE in the netstat command output, it is a big indicator of a SYN Flood attack.

19. Answer: A

Explanation: All the fields can be found inside the log. The Client IP address is found at “[client 10.1.0.10]“, the type of attack can be found in one of the tag fields: [tag "OWASP_CRS/WEB_ATTACK/FILE_INJECTION"], and the destination is the hostname: [hostname "10.2.0.101"].

20. Answer: A

Explanation: The HTTP protocol is a top layer protocol, while the IPv4 and IPv6 are lower layer protocols. Since it changes another layer, the web server log will only change the information about this layer, the IP Layer.

21. Answer: B

Explanation: Many components can generate logs to help identify the type of attack. Examples are network bandwidth graphs, CPU usage graphs, firewall logs, and others.

Score ___/21