Chapter 5

1. Which attack intercepts communications between a web browser and the underlying computer?
2. man-in-the-middle (MITM)
3. **man-in-the-browser (MITB)**
4. replay
5. ARP poisoning
6. Olivia was asked to protect the system from a DNS poisoning attack. What are the locations she would need to protect?
7. Web server buffer and host DNS server
8. Reply referrer and domain buffer
9. Web browser and browser add-on
10. **Host table and external DNS server**
11. Newton is concerned that attackers could be exploiting vulnerability in software to gain access to resources that the user normally would be restricted from accessing. What type of attack is he worried about?
12. **Privilege escalation**
13. Session replay
14. Scaling exploit
15. Amplification
16. Which of the following adds new functionality to the web browser so that users can play music, view videos, or display special graphical images within the browser?
17. Extensions
18. Scripts
19. **Plug-ins**
20. Add-ons
21. An attacker who manipulates the maximum size of an integer type would be performing what kind of attack?
22. **integer overflow**
23. buffer overflow
24. number overflow
25. heap overflow
26. What kind of attack is performed by an attacker who takes advantage of the inadvertent and unauthorized access built through three succeeding systems that all trust one another?
27. **privilege escalation**
28. cross-site attack
29. horizontal access attack
30. transverse attack
31. Which statement is correct regarding why traditional network security devices cannot be used to block web application attacks?
32. The complex nature of TCP/IP allows for too many ping sweeps to be blocked.
33. Web application attacks use web browsers that cannot be controlled on a local computer.
34. Network security devices cannot prevent attacks from web resources.
35. **Traditional network security devices ignore the content of HTTP traffic, which is the vehicle of web application attacks**.
36. What is the difference between a DoS and a DDoS attack?
37. DoS attacks are faster than DDoS attacks
38. **DoS attacks use fewer computers than DDoS attacks**
39. DoS attacks do not use DNS servers as DDoS attacks do
40. DoS attacks user more memory than a DDoS attack
41. John was explaining about an attack that accepts user input without validating it and uses that input in a response. What type of attack was he describing?
42. SQL
43. **XSS**
44. XSRF
45. DDoS DNS
46. Which attack uses the user’s web browser settings to impersonate that user?
47. XDD
48. **XSRF**
49. Domain hijacking
50. Session hijacking
51. What is the basis of an SQL injection attack?
52. to expose SQL code so that it can be examined
53. to have the SQL server attack client web browsers
54. **to insert SQL statements through unfiltered user input**
55. to link SQL servers into a botnet
56. Which action cannot be performed through a successful SQL injection attack?
57. discover the names of different fields in a table
58. **reformat the web application server’s hard drive**
59. display a list of customer telephone numbers
60. erase a database table
61. Attackers who register domain names that are similar to legitimate domain names are performing \_\_\_\_\_.
62. Address resolution
63. HTTP manipulation
64. HTML squatting
65. **URL hijacking**
66. What type of attack involves manipulating third-party ad networks?
67. Session advertising
68. **Malvertising**
69. Clickjacking
70. Directory traversal
71. Why are extensions, plug-ins, and add-ons considered to be security risks?
72. They are written in Java, which is a weak language.
73. **They have introduced vulnerabilities in browsers**.
74. They use bitcode.
75. They cannot be uninstalled.
76. What is a session token?
77. XML code used in an XML injection attack
78. **a random string assigned by a web server**
79. another name for a third-party cookie
80. a unique identifier that includes the user’s email address
81. Which of these is not a DoS attack?
82. SYN flood
83. DNS amplification
84. smurf attack
85. **push flood**
86. What type of attack intercepts legitimate communication and forges a fictitious response to the sender?
87. SIDS
88. interceptor
89. **MITM**
90. SQL intrusion
91. A replay attack \_\_\_\_\_.
92. can be prevented by patching the web browser
93. is considered to be a type of DoS attack
94. **makes a copy of the transmission for use at a later time**
95. replays the attack over and over to flood the server
96. DNS poisoning \_\_\_\_\_.
97. floods a DNS server with requests until it can no longer respond
98. is rarely found today due to the use of host tables
99. **substitutes DNS addresses so that the computer is automatically redirected to another device**
100. is the same as ARP poisoning