Chapter 8

1. Which technology is predominately used for contactless payment systems?
2. **near field communication (NFC)**
3. wireless local area network (WLAN)
4. Bluetooth
5. Radio Frequency ID (RFID)
6. Which of these Bluetooth attacks involves accessing unauthorized information through a Bluetooth connection?
7. **Bluesnarfing**
8. Bluejacking
9. Bluecreeping
10. Bluestealing
11. What is a difference between NFC and RFID?
12. NFC is based on wireless technology while RFID is not.
13. RFID is faster than NFC.
14. **RFID is designed for paper-based tags** **while NFC is not.**
15. NFC devices cannot pair as quickly as RFID devices.
16. Which of these technologies is NOT found in a wireless router?
17. **access point**
18. router
19. dynamic host configuration protocol (DHCP) server
20. firewall
21. Why is a rogue AP a security vulnerability?
22. It uses the weaker IEEE 80211i protocol.
23. It conflicts with other network firewalls and can cause them to become disabled.
24. **It allows an attacker to bypass network security configurations.**
25. It requires the use of vulnerable wireless probes on all mobile devices.
26. Which of these is NOT a risk when a home wireless router is not securely configured?
27. **Only a small percentage of the total traffic can be encrypted.**
28. An attacker can steal data from any folder with file sharing enabled.
29. User names, passwords, credit card numbers, and other information sent over the WLAN could be captured by an attacker.
30. Malware can be injected into a computer connected to the WLAN.
31. Which of these Wi-Fi Protected Setup (WPS) methods is vulnerable?
32. Push-Button method
33. **PIN method**
34. piconet method
35. NFC method
36. Flavio visits a local coffee shop on his way to school and accesses its free Wi-Fi. When he first connects, a screen appears that requires him to first agree to an Acceptable Use Policy (AUP) before continuing. What type of AP has he encountered?
37. **captive portal**
38. web-based portal
39. rogue portal
40. authenticated portal
41. Which of the following is NOT a wireless peripheral protection option?
42. Update or replacing any vulnerable device
43. Switch to a more fully tested Bluetooth model
44. **Install a network sensor to detect an attack**
45. Substitute a wired device
46. The primary design of a(n) \_\_\_\_\_ is to capture the transmissions from legitimate users.
47. rogue access point
48. WEP
49. **evil twin**
50. Bluetooth grabber
51. Which of these is a vulnerability of MAC address filtering?
52. APs use IP addresses instead of MACs.
53. The user must enter the MAC.
54. **MAC addresses are initially exchanged unencrypted**.
55. Not all operating systems support MACs.
56. Which of these is NOT a limitation of turning off the SSID broadcast from an AP?
57. Turning off the SSID broadcast may prevent users from being able to freely roam from one AP coverage area to another.
58. Some versions of operating systems favor a network that broadcasts an SSID over one that does not.
59. **Users can more easily roam from one WLAN to another.**
60. The SSID can easily be discovered, even when it is not contained in beacon frames, because it still is transmitted in other management frames sent by the AP.
61. What is the primary weakness of wired equivalent privacy (WEP)?
62. It functions only on specific brands of APs.
63. **Its usage creates a detectable pattern**.
64. It slows down a WLAN from 104 Mbps to 16 Mbps.
65. Initialization vectors (IVs) are difficult for users to manage.
66. WPA replaces WEP with \_\_\_\_\_.
67. WPA2
68. **Temporal Key Integrity Protocol (TKIP)**
69. Cyclic Redundancy Check (CRC)
70. Message Integrity Check (MIC)
71. Adabella was asked by her supervisor to adjust the frequency spectrum settings on a new AP. She brought up the configuration page and looked through the different options. Which of the following frequency spectrum settings would she NOT be able to adjust?
72. Frequency band
73. Channel selection
74. **RFID spectrum**
75. Channel width
76. A wireless LAN controller (WLC) was recently installed, and now Kelsey needs to purchase several new APs to be managed by it. Which type of AP should he purchase?
77. **Controller AP**
78. Standalone AP
79. Fat AP
80. Any type of AP can be managed by a WLC.
81. AES-CCMP is the encryption protocol standard used in \_\_\_\_\_.
82. WPA
83. **WPA2**
84. IEEE 802.11
85. NFC
86. Elijah was asked by a student intern to explain the Extensible Authentication Protocol (EAP). What would be the best explanation of EAP?
87. It is the transport protocol used in TCP/IP for authentication
88. **It is a framework for transporting authentication protocols**
89. It is a subset of WPA2
90. It is a technology used by IEEE 802.11 for encryption
91. Minh has been asked to recommend an EAP for a system that uses both passwords and tokens with TLS. Which should she recommend?
92. EAP-TLS
93. EAP-TTLS
94. EAP-SSL
95. **EAP-FAST**
96. Which of these is NOT a type of wireless AP probe?
97. wireless device probe
98. **WNIC probe**
99. dedicated probe
100. AP probe