Chapter 9 Review Questions

1. Which of the following is NOT a reason why supply chain infections are considered especially dangerous?
2. If the malware is planted in the ROM firmware of the device this can make it difficult or sometimes even impossible to clean an infected device.
3. Users are receiving infected devices at the point of purchase and are completely unaware that a brand new device may be infected.
4. It is virtually impossible to closely monitor every step in the supply chain.
5. Supply chains take advantage of the trusted “chain of trust” concept.
6. Which type of operating system runs on a firewall, router, or switch?
7. Server OS
8. Network OS
9. Device OS
10. Resource OS
11. Which of the following is NOT designed to prevent individuals from entering sensitive areas but instead is intended to direct traffic flow?
12. Barricade
13. Fencing
14. Roller barrier
15. Type V controls
16. Which of the following is NOT a motion detection method?
17. Magnetism
18. Radio frequency
19. Moisture
20. Infrared
21. Which type of residential lock is most often used for keeping out intruders?
22. Encrypted key lock
23. Keyed entry lock
24. Privacy lock
25. Passage lock
26. A lock that extends a solid metal bar into the door frame for extra security is the \_\_\_\_\_.
27. triple bar lock
28. deadman’s lock
29. full bar lock
30. deadbolt lock
31. Which statement about a mantrap is true?
32. It is illegal in the United States.
33. It monitors and controls two interlocking doors to a room.
34. It is a special keyed lock.
35. It requires the use of a cipher lock.
36. Which of the following is NOT a typical OS security configuration?
37. Employing least functionality
38. Restricting patch management
39. Disabling default accounts/passwords
40. Disabling unnecessary ports and services
41. Which of the following can be used to secure a laptop or mobile device?
42. Mobile connector
43. Cable lock
44. Mobile chain
45. Security tab
46. Which of the following is NOT a characteristic of an alarmed carrier PDS?
47. Requires periodic visual inspections
48. Uses continuous monitoring
49. Carrier can be hidden above the ceiling
50. Eliminates the need to seal connections
51. Which of the following is NOT a memory vulnerability?
52. DLL injection
53. Pointer deference
54. Buffer overflow
55. Variable overflow
56. Which stage is a “quality assurance” test that verifies the code functions as intended?
57. Production stage
58. Testing stage
59. Staging stage
60. Development stage
61. Which model uses a sequential design process?
62. Waterfall model
63. Rigid model
64. Agile model
65. Secure model
66. What allows for a single configuration to be set and then deployed to many or all users?
67. Snap-In Replication (SIR)
68. Active Directory
69. Group Policy
70. Command Configuration
71. Which of the following is a cumulative package of all patches?
72. Rollup
73. Service pack
74. Patch
75. Hotfix
76. Which of the following is NOT an advantage to an automated patch update service?
77. Administrators can approve or decline updates for client systems, force updates to install by a specific date, and obtain reports on what updates each computer needs.
78. Downloading patches from a local server instead of using the vendor’s online update service can save bandwidth and time because each computer does not have to connect to an external server.
79. Users can disable or circumvent updates just as they can if their computer is configured to use the vendor’s online update service.
80. Specific types of updates that the organization does not test, such as hotfixes, can be automatically installed whenever they become available.
81. How can an SDIO card be made secure?
82. Using the security mechanisms on a standard Wi-Fi network.
83. Turning on patch updates to the SDIO card.
84. Requiring a username before accessing the SDIO card.
85. SDIO cards are natively secure and no security settings are needed.
86. How does heuristic detection detect a virus?
87. A virtualized environment is created and the code is executed in it.
88. A string of bytes from the virus is compared against the suspected file.
89. The bytes of a virus are placed in different “piles” and then used to create a profile.
90. The virus signature file is placed in a suspended chamber before streaming to the CPU.
91. Which of these is a list of approved email senders?
92. Blacklist
93. Whitelist
94. Bluelist
95. Yellowlist
96. Which of the following types of testing uses unexpected or invalid inputs?
97. Stress testing
98. Dynamic analysis
99. Static analysis
100. Runtime testing