Chapter 13 Review Questions

1. At what point in a vulnerability assessment would an attack tree be utilized?
2. Vulnerability appraisal
3. Risk assessment
4. Risk mitigation
5. Threat evaluation
6. Which of the following is NOT true about privacy?
7. Today, individuals can achieve any level of privacy that is desired.
8. Privacy is difficult due to the volume of data silently accumulated by technology.
9. Privacy is freedom from attention, observation, or interference based on your decision.
10. Privacy is the right to be left alone to the degree that you choose.
11. Which of the following is NOT a risk associated with the use of private data?
12. Individual inconveniences and identity theft
13. Associations with groups
14. Statistical inferences
15. Devices being infected with malware
16. Which of the following is NOT an issue raised regarding how private data is gathered and used?
17. The data is gathered and kept in secret.
18. By law, all encrypted data must contain a “backdoor” entry point.
19. Informed consent is usually missing or is misunderstood.
20. The accuracy of the data cannot be verified.
21. Which of the following is a systematic and methodical evaluation of the exposure of assets to attackers, forces of nature, and any other entity that could cause potential harm?
22. Vulnerability assessment
23. Penetration test
24. Vulnerability scan
25. Risk appraisal
26. Which of these should NOT be classified as an asset?
27. Business partners
28. Buildings
29. Employee databases
30. Accounts payable
31. Which of the following command-line tools tests a connection between two network devices?
32. Netstat
33. Ping
34. Nslookup
35. Ifconfig
36. Which statement regarding vulnerability appraisal is NOT true?
37. Vulnerability appraisal is always the easiest and quickest step.
38. Every asset must be viewed in light of each threat.
39. Each threat could reveal multiple vulnerabilities.
40. Each vulnerability should be cataloged.
41. Which of the following constructs scenarios of the types of threats that assets can face to learn who the attackers are, why they attack, and what types of attacks may occur?
42. Vulnerability prototyping
43. Risk assessment
44. Attack assessment
45. Threat modeling
46. Which of the following tools is a Linux command-line protocol analyzer?
47. Wireshark
48. Tcpdump
49. IP
50. Arp
51. Which of the following is a command-line alternative to Nmap?
52. Netcat
53. Statnet
54. Mapper
55. Netstat
56. Which of these is NOT a state of a port that can be returned by a port scanner?
57. Open
58. Busy
59. Blocked
60. Closed
61. Which of the following data sensitivity labels is the highest level of data sensitivity?
62. Ultra
63. Confidential
64. Private
65. Secret
66. Which of the following data sensitivity labels has the lowest level of data sensitivity?
67. Unrestricted
68. Public
69. Free
70. Open
71. Which of the following is NOT a function of a vulnerability scanner?
72. Detects which ports are served and which ports are browsed for each individual system
73. Alerts users when a new patch cannot be found
74. Maintains a log of all interactive network sessions
75. Detects when an application is compromised
76. Which of the following must be kept secure as mandated by HIPAA?
77. PII
78. PHI
79. PHIL
80. PLILP
81. Which statement regarding a honeypot is NOTtrue?
82. It is typically located in an area with limited security.
83. It is intentionally configured with security vulnerabilities.
84. It cannot be part of a honeynet.
85. It can direct an attacker’s attention away from legitimate servers.
86. Which of the following sends “probes” to network devices and examines the responses to evaluate whether a specific device needs remediation?
87. Active scanner
88. Probe scanner
89. Passive scanner
90. Remote scanner
91. If a tester is given the IP addresses, network diagrams, and source code of customer applications, the tester is using which technique?
92. Black box
93. White box
94. Gray box
95. Blue box
96. If a software application aborts and leaves the program open, which control structure is it using?
97. Fail-safe
98. Fail-secure
99. Fail-open
100. Fail-right