Chapter 13

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.

1. 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?
2. Vulnerability prototyping
3. Risk assessment
4. Attack assessment
5. **Threat modeling**
6. Which of the following tools is a Linux command-line protocol analyzer?
7. Wireshark
8. **Tcpdump**
9. IP
10. Arp
11. Which of the following is a command-line alternative to Nmap?
12. **Netcat**
13. Statnet
14. Mapper
15. Netstat
16. Which of these is NOT a state of a port that can be returned by a port scanner?
17. Open
18. **Busy**
19. Blocked
20. Closed
21. Which of the following data sensitivity labels is the highest level of data sensitivity?
22. Ultra
23. **Confidential**
24. Private
25. Secret
26. Which of the following data sensitivity labels has the lowest level of data sensitivity?
27. Unrestricted
28. **Public**
29. Free
30. Open
31. Which of the following is NOT a function of a vulnerability scanner?
32. Detects which ports are served and which ports are browsed for each individual system
33. **Alerts users when a new patch cannot be found**
34. Maintains a log of all interactive network sessions
35. Detects when an application is compromised
36. Which of the following must be kept secure as mandated by HIPAA?
37. PII
38. **PHI**
39. PHIL
40. PLILP
41. Which statement regarding a honeypot is NOTtrue?
42. It is typically located in an area with limited security.
43. It is intentionally configured with security vulnerabilities.
44. **It cannot be part of a honeynet**.
45. It can direct an attacker’s attention away from legitimate servers.
46. Which of the following sends “probes” to network devices and examines the responses to evaluate whether a specific device needs remediation?
47. **Active scanner**
48. Probe scanner
49. Passive scanner
50. Remote scanner
51. If a tester is given the IP addresses, network diagrams, and source code of customer applications, the tester is using which technique?
52. Black box
53. **White box**
54. Gray box
55. Blue box
56. If a software application aborts and leaves the program open, which control structure is it using?
57. Fail-safe
58. Fail-secure
59. **Fail-open**
60. Fail-right