Chapter 12

Indicate whether the statement is true or false.

1. An intranet vulnerability scan starts with the scan of the organization's default Internet search engine.
   a. True
   b. False

2. Threats cannot be removed without requiring a repair of the vulnerability.
   a. True
   b. False

3. Documentation procedures are not required for configuration and change management processes.
   a. True
   b. False

4. Policy needs to be reviewed and refreshed from time to time to ensure that it's providing a current foundation for the information security program.
   a. True
   b. False

5. Intelligence for external monitoring can come from a number of sources: Vendors, CERT organizations, public network sources and membership sites
   a. True
   b. False

6. Based on the 40% rule, when the amount of data stored on a particular hard drive averages 40% of available capacity for a prolonged period, consider an upgrade for the hard drive.
   a. True
   b. False

7. The target selection step of Internet vulnerability assessment involves using the external monitoring intelligence to configure a test engine (such as Nessus) for the tests to be performed.
   a. True
   b. False

8. An effective information security governance program requires little review once it is well established.
   a. True
   b. False

9. A maintenance model such as ISO 17799 deals with methods to manage and operate systems.
   a. True
   b. False

10. In some instances, risk is acknowledged as being part of an organization's business process.
   a. True
   b. False

Chapter 12

11. Remediation of vulnerabilities can be accomplished by accepting or transferring the risk, removing the threat, or repairing the vulnerability.

a. True

b. False

12. Documenting information system changes and assessing their potential impact on system security is an important and consequential part of digital forensics.

a. True

b. False

13. External monitoring entails collecting intelligence from various data sources and then giving that intelligence context and meaning for use by decision makers within the organization.

a. True

b. False

14. Digital forensics helps the organization understand what happened and how, after an incident.

a. True

b. False

15. Inventory characteristics for hardware and software assets that record the manufacturer and versions are related to technical functionality and should be highly accurate and updated each time there is a change.

a. True

b. False

16. US-CERT is generally viewed as the definitive authority for computer emergency response teams.

a. True

b. False

17. The vulnerability database, like the risk, threat, and attack database, both stores and tracks information.

a. True

b. False

18. If an organization deals successfully with change and has created procedures and systems that can be adjusted to the environment, the existing security improvement program will probably continue to work well.

a. True

b. False

19. Modem vulnerability assessment begins with the planning, scheduling and notification of all Internet connections, using software such as Wireshark.

a. True

b. False

20. Major planning components should be reviewed on a periodic basis to ensure that they are current, accurate, and appropriate.

a. True

b. False

Chapter 12

21. Over time, policies and procedures may become inadequate due to changes in the organization's mission and operational requirements, threats, or the environment.

a. True

b. False

22. Over time, external monitoring processes should capture information about the external environment in a format that can be referenced both across the organization as threats emerge and for historical use.

a. True

b. False

23. Rehearsal adds value by exercising the procedures, identifying shortcomings, and providing security personnel the opportunity to improve the security plan before it is needed.

a. True

b. False

24. The internal monitoring domain is the component of the maintenance model that focuses on identifying, assessing, and managing the physical security of assets in an organization.

a. True

b. False

25. All systems that are mission critical should be enrolled in platform security validation (PSV) measurement.

a. True

b. False

Indicate the answer choice that best completes the statement or answers the question.

26. When the memory usage associated with a particular CPU-based system averages _____% or more over prolonged periods, consider adding more memory.

a. 40 b. 60

c. 10 d. 100

27. A step commonly used for Internet vulnerability assessment includes _____, which is when the penetration test engine is unleashed at the scheduled time using the planned target list and test selection.

a. scanning b. subrogation

c. delegation d. targeting

28. _____ is used to respond to network change requests and network architectural design proposals.

a. Network connectivity RA b. Dialed modem RA

c. Application RA d. Vulnerability RA

29. The _____ commercial site focuses on current security tool resources.

a. Nmap-hackerz b. Packet Storm

c. Security Laser d. Snort-SIGs

Chapter 12

30. The _____ process is designed to find and document the vulnerabilities that may be present because there are misconfigured systems in use within the organization.

a. ASP b. ISP

c. SVP d. PSV

31. _____ penetration testing is usually used when a specific system or network segment is suspect and the organization wants the pen tester to focus on a particular aspect of the target.

a. White box b. Black box

c. Gray box d. Green box

32. The _____ vulnerability assessment is a process that is designed to find and document selected vulnerabilities that are likely to be present on the internal network of the organization.

a. intranet b. Internet

c. LAN d. WAN

33. A _____ is the recorded state of a particular revision of a software or hardware configuration item.

a. state b. version

c. configuration d. baseline

34. One approach that can improve the situational awareness of the information security function uses a process known as _____ to quickly identify changes to the internal environment.

a. baseline b. difference analysis

c. differential d. revision

35. A process called _____ examines the traffic that flows through a system and its associated devices to identifies the most frequently used devices..

a. difference analysis b. traffic analysis

c. schema analysis d. data flow assessment

36. The optimum approach for escalation is based on a thorough integration of the monitoring process into the _____.

a. IDE b. CERT

c. ERP d. IRP

37. Control _____ baselines are established for network traffic and also for firewall performance and IDPS performance.

a. system b. application

c. performance d. environment

38. To evaluate the performance of a security system, administrators must establish system performance _____.

a. baselines b. profiles

c. maxima d. means

39. _____, a level beyond vulnerability testing, is a set of security tests and evaluations that simulate attacks by a malicious external source (hacker).

a. Penetration testing b. Penetration simulation

c. Attack simulation d. Attack testing

Chapter 12

40. Detailed _____ on the highest risk warnings can include identifying which vendor updates apply to which vulnerabilities as well as which types of defenses have been found to work against the specific vulnerabilities reported.
a. escalation b. intelligence
c. monitoring d. elimination

41. A(n) _____ item is a hardware or software item that is to be modified and revised throughout its life cycle.
a. revision b. update
c. change d. configuration

42. The _____ is a statement of the boundaries of the RA.
a. scope b. disclaimer
c. footer d. head

43. Common vulnerability assessment processes include:
a. Internet VA b. modem VA
c. intranet VA d. all of these

44. A primary mailing list for new vulnerabilities, called simply _____, provides time-sensitive coverage of emerging vulnerabilities, documenting how they are exploited, and reporting on how to remediate them. Individuals can register for the flagship mailing list or any one of the entire family of its mailing lists.
a. Bug b. Bugfix
c. Buglist d. Bugtraq

45. The _____ list is intended to facilitate the development of the leading free network exploration tool.
a. Nmap-dev b. Packet Storm
c. Security Focus d. Snort-sigs

46. The _____ is a center of Internet security expertise and is located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.
a. US-CERT b. Bugtraq
c. CM-CERT d. CERT/CC

47. _____ allows for the major security control components to be reviewed on a periodic basis to ensure that they are current, accurate, and appropriate.
a. System review b. Project review
c. Program review d. Application review

48. The _____ vulnerability assessment process is designed to find and document any vulnerability that is present on systems that may have telephone connections to the organization's networks.
a. modem b. phone-in
c. battle-dialing d. network

49. The _____ mailing list includes announcements and discussion of an open-source IDPS.
a. Nmap-hackers b. Packet Storm
c. Security Focus d. Snort-SIGs

Chapter 12

50. _____ are a component of the security triple.
    a. Threats b. Assets
    c. Vulnerabilities d. All of the above