Domain 6 Questions

1. There are normally three stages in the product evaluation process. Which of the following is NOT true with respect to this process?

- ☐ a. Certification and accreditation take place at different times.
- ☐ b. Certification is management's formal acceptance of the risk associated with bringing the product into the organization.
- ☐ c. The order of the three activities is evaluation, certification, and accreditation
- ☐ d. TCSEC, Common Criteria, and ITSEC were all developed to assist organizations in evaluating prospective products.

2. Synthetic monitoring most typically involves having external agents run:

- ☐ a. Scripted transactions against a File Transfer Protocol (FTP) application.
- ☐ b. Batch jobs against email applications.
- ☐ c. Batch jobs against a telecommunications network (telnet) application.
- ☐ d. Scripted transactions against a web application.

3. Which of the following will cause the fewest security flaws?

- ☐ a. Design flaws in the proposed system documentation.
- ☐ b. Poor programming.
- ☐ c. Misconfiguration of security infrastructures
- ☐ d. Functional bugs in security infrastructures.

4. Good software testing techniques include:

- ☐ a. Having the developers and the testers use the same tools
- ☐ b. The idea that a successful test is one that finds an error.
- ☐ c. Having the developers and the testers work together throughout the development cycle.
- ☐ d. Running tests without pre-determining expected outcomes.

5. What would be the prime consideration for a security practitioner when considering a new software testing tool?

- ☐ a. The likelihood that the tool will expose flaws.
- ☐ b. Estimates for the potential damage to the item(s) being tested.
- ☐ c. The way in which the tool determines and manages the attack surface(s) for the items to be tested.
- ☐ d. The responsibilities of those who will manage the items to be tested.

6. Which of the following is NOT a testing structural-coverage metric?

- [ ] a. Statement coverage
- [ ] b. Dynamic coverage
- [ ] c. Path coverage
- [ ] d. Loop coverage

7. What are the two main testing strategies in software testing?

- [ ] a. Negative and Positive cases
- [ ] b. Static and Negative cases
- [ ] c. Positive and Dynamic cases
- [ ] d. Known and Unknown cases

8. In a testing environment that seeks to verify the accuracy of installed controls, which of the following is most correct?

- [ ] a. The white-hat tester is an external tester and the black-hat tester is an internal tester.
- [ ] b. A blind test is done so that insiders don't know that they are being tested by external testers.
- [ ] c. The most effective test would be a double-blind test.
- [ ] d. A black-hat blind test will produce better results that a white-hat blind test.

9. Which technique would be a black-hat tester normally use initially?

- [ ] a. Static Source Code Analysis (SAST) tools
- [ ] b. Fuzz-testing tools, or "fuzzing"
- [ ] c. No-Op/NOP sled, slides, or ramps.
- [ ] d. Reverse Engineering.

10. Which of the following describes penetration testing steps in their proper sequence?

- [ ] a. Discovery, enumeration, exploitation, Key Performance Indicators (KPIs), reporting
- [ ] b. Enumeration, discovery, vulnerability scanning, reporting
- [ ] c. Key Performance Indicators (KPIs), vulnerability scanning, exploitation, reporting
- [ ] d. Discovery, enumeration, vulnerability scanning, exploitation

11. A SOC report typically is done _____?

- [ ] a. One month after initial product installation and installed controls are tested.
- [ ] b. The quarter after initial product installation and installed controls are tested.
- [ ] c. Every year after initial product installation and installed controls are tested.
- [ ] d. Twice a year after initial product installation and installed controls are tested.

12. Which answer below is MOST accurate with respect to testing newly developed software?

- ☐ a. With a little practice, complicated new software systems can be exhaustively tested.
- ☐ b. Expected test results should be objective and according to pre-defined specifications.
- ☐ c. Examining the “Top 5 Most Often Occurring” cases is BEST PRACTICE for software testing.
- ☐ d. Best practices involve end-users in software testing as soon as the new code can be tested.

13. Which of these is MOST LIKELY to cause long-term damage?

- ☐ a. Black box, white hat tester
- ☐ b. Black box, black hat tester
- ☐ c. White box, white hat tester
- ☐ d. White box, black hat tester

14. Windows Event Manager automatically maintains several log files. Which of the following is NOT among them?

- ☐ a. System
- ☐ b. Application
- ☐ c. Host
- ☐ d. Security

15. Common Operating System log file entries contain all of the following EXCEPT?

- ☐ a. System startup and shutdown times
- ☐ b. The number of hits the Web Server took in the last day
- ☐ c. User password change attempts
- ☐ d. Failed user login attempts

16. When considering a service provider’s security controls, which is LEAST important to an auditor?

- ☐ a. Confidentiality
- ☐ b. Integrity
- ☐ c. Availability
- ☐ d. Privacy

17. Configuration Management systems track changes to several categories of products. Which of these is LEAST likely to be subject to Configuration Management tracking?

- ☐ a. Physical assets, including laptops, tablets, and cell phones
- ☐ b. Cloud assets, including public and private clouds
- ☐ c. Workplace assets, including offices, desks, and filing cabinets
- ☐ d. Virtual assets, including SAN/NAS, SDN (Storage Area Networks/Network Attached Storage, Software Defined Networks)

18. Real User Monitoring is an approach to Web monitoring that _____

- ☐ a. Aims to capture and analyze select transactions of every user of a website or application.
- ☐ b. Aims to capture and analyze every transaction of every user of a website or application.
- ☐ c. Aims to capture and analyze every transaction of only select users of a website or critical applications.
- ☐ d. Aims to capture and analyze select transactions of only select users of a website or non-critical application.

19. In what way can violation clipping levels assist in violation tracking and analysis?

- ☐ a. Set a baseline for normal user errors, and violations exceeding that line are recorded for investigation.
- ☐ b. Enable a security administrator to customize an audit trail to record only violations which are deemed security relevant.
- ☐ c. Enable a security administrator to customize an audit trail to record only actions for privileged users with access to user codes.
- ☐ d. Enable a security administrator to view all reductions in security levels which have been made to user codes that have incurred violations.

20. Synthetic performance monitoring, sometimes called proactive monitoring, involves _____.

- ☐ a. Having external agents run scripted transactions against a web application.
- ☐ b. Having internal agents run scripted transactions against a web application.
- ☐ c. Having external agents run batch jobs against a number of applications residing on a host.
- ☐ d. Having internal agents run batch jobs against a web application on a mainframe system.

21. Static Testing Techniques analyze the system

- ☐ a. Under test is executed and its behavior
- ☐ b. Without executing the system under test
- ☐ c. That is in a dormant state
- ☐ d. That is only in a secure state

22. Software code-based testing that identifies test cases based on knowledge obtained from the source code, detailed design specifications, and other development documents is also known as:

- ☐ a. grey box testing
- ☐ b. black box testing
- ☐ c. purpose box testing
- ☐ d. white box testing

23. Testing changes required for software often result from requirements creep. This is defined as requirements that have

- ☐ a. Identified vulnerabilities during the development beyond what was originally foreseen.
- ☐ b. Increased during development beyond what was originally foreseen.
- ☐ c. Decreased during development beyond what was originally foreseen.
- ☐ d. Not changed from what was originally foreseen.

24. What are the two main testing strategies in software testing? (yes this is a repeat).

- ☐ a. Positive and Dynamic
- ☐ b. Static and Dynamic
- ☐ c. Internal and External
- ☐ d. Negative and Positive

25. The maintenance and failure/error mechanisms of hardware and software differ. Software maintenance includes:

- ☐ a. Corrective, perfective, and adaptive maintenance
- ☐ b. Preventive maintenance actions
- ☐ c. Component maintenance only
- ☐ d. Corrective, perfective, and component replacement

26. The process for developing and implementing an Information Security Continuous Monitoring strategy is to:

- ☐ a. Implement, analyze, implement, establish, respond, review, and update
- ☐ b. Analyze, implement, define, establish, respond, review, and update
- ☐ c. Define, establish, implement, analyze, respond, review, and update
- ☐ d. Implement, define, establish, analyze, respond, review, and update

27. An Information Security Continuous Monitoring provides information to support risk response decisions, security status information, ongoing insight into security control effectiveness, and enables a company to move from:

- ☐ a. Compliance driven risk management to data-driven risk management
- ☐ b. Data-driven risk management to compliance driven risk management
- ☐ c. Data-driven risk management to market driven risk management
- ☐ d. Compliance driven risk management to quantitative driven risk management