Post-Class Quiz: Software Development Security Domain

1. A step-by-step implementation instruction is called …
    A. Policy
    B. Standard
    C. Procedure
    D. Guideline

2. An approved configuration of software packages that describes how and what components are assembled and implemented is called …
    A. Policy
    B. Standard
    C. Baseline
    D. Guideline

3. What is the framework that provides a common description that explains how the IT systems are aligned to the business strategy, what values are delivered, and defines measure of effectiveness.
    A. Governance framework
    B. System architecture
    C. Enterprise architecture
    D. Standard

4. The Software Engineering Institute (SEI) Software Capability Maturity Model (SW-CMM) is based on the premise that…?
    A. Good software development is a function of the number of expert programmers in the organization.
    B. The maturity of an organization's software processes cannot be measured.
    C. The quality of a software product is a direct function of the quality of its associated software development and maintenance processes.
    D. Software development is an art that cannot be measured by conventional means.

5. In configuration management, a configuration item is?
    A. The version of the operating system, which is operating on the work station, that provides information security services.

B. A component whose state is to be recorded and against which changes are to be progressed.

C. The network architecture used by the organization.

D. A series of files that contain sensitive information.

6. The Waterfall Model of software life cycle development assumes that…?

A. Iteration will be required among the steps in the process.

B. Each step can be completed and finalized without any effect from the later stages that may require rework.

C. Each phase is identical to a completed milestone.

D. Software development requires reworking and repeating some of the phases.

7. What does the Spiral Model depict?

A. A spiral that incorporates various phases of software development

B. A spiral that models the behavior of biological neurons

C. The operation of expert systems

D. Information security checklists.

8. In the software life cycle, verification…?

A. Evaluates the product in development against real world requirements

B. Evaluates the product in development against similar products

C. Evaluates the product in development against general baselines

D. Evaluates the product in development against the specification

9. In the software life cycle, validation… ?

A. Refers to the work product satisfying the real-world requirements and concepts

B. Refers to the work product satisfying derived specifications

C. Refers to the work product satisfying software maturity levels

D. Refers to the work product satisfying generally accepted principles

10. In IEEE 1220, what are the five stages within a typical system life cycle?

A. Initial, Development, Production, Support, and Disposal

B. Concept, Design, Develop, Deploy, and Operate

C. Initiation, Acquisition/Development, Implementation, Operations/Maintenance, and Disposition

D. None of the above

11. The software maintenance phase controls consist of:

A. Request control, change control, and release control

B. Request control, configuration control, and change control

C. Change control, security control, and access control

D. Request control, release control, and access control

12. In a system life cycle, information security controls should be?

A. Designed during the product implementation phase

B. Implemented prior to validation

C. Part of the feasibility phase

D. Specified after the coding phase

13. In configuration management, what is a software library?

A. A set of versions of the component configuration items

B. A controlled area accessible to only approved users who are restricted to the use of an approved procedure

C. A repository of backup tapes

D. A collection of software build lists

14. What is configuration control?

A. Identifying and documenting the functional and physical characteristics of each configuration item

B. Controlling changes to the configuration items and issuing versions of configuration items from the software library.

C. Recording the processing of changes

D. Controlling the quality of the configuration management procedures.

15. What type of security requirement is designed to measure the effectiveness of security controls?

A. Security requirement

B. Functional security requirement

C. Assurance requirement

D. Security posture

16. Which of the following statements pertaining to the security kernel is incorrect?

A. The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept.

B. The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof.

C. The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner.

D. The security kernel is an access control concept, not an actual physical component.

17. What can best be described as an abstract machine which must mediate all access to subjects to objects?

A. The reference monitor

B. A security domain

C. The security kernel

D. The security perimeter

18. What is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept?

A. Protection rings

B. A security kernel

C. A protection domain

D. The reference monitor

19. What can be described as an imaginary line that separates the trusted components of the TCB from those elements that are not trusted?

A. The reference perimeter

B. The security perimeter

C. The reference monitor

D. The security kernel

20. What are the three conditions that must be met by the reference monitor?

    A. Policy, mechanism and assurance
    B. Isolation, layering and abstraction
    C. Isolation, completeness and verifiability
    D. Confidentiality, availability and integrity

21. What are the types of un-controlled communication paths for covert chanenel?

    A. Timing and storage channels
    B. Encrypted message channels
    C. Timing channels
    D. Storage channels

22. Which of the following is a communication mechanism that enables direct conversation between two applications?

    A. ODBC
    B. DCOM
    C. DDE
    D. OLE

23. Which of the following is NOT a common database structure?

    A. Hierarchical
    B. Relational
    C. Sequential
    D. Network

24. In Software Capability Maturity Model (SW-CMM), at what CMM Level where an organization has documented software engineering and development processes and are used across the organization?

    A. CMM Level 1: Initial
    B. CMM Level 2: Repeatable
    C. CMM Level 3: Defined
    D. CMM Level 4: Managed

25. Why do buffer overflows happen?

    A. Because they are an easy weakness to exploit
    B. Because buffers can only hold so much data
    C. Because input data is not checked for appropriate length at time of input
    D. Because of insufficient system memory

26. Which of the following is used in database information security to hide information?

    A. Inheritance
    B. Delegation
    C. Polymorphism
    D. Polyinstantiation

27. What is called the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity?

    A. Aggregation
    B. Data mining
    C. Inference
    D. Polyinstantiation

28. Which of the following virus types changes some of its characteristics as it spreads?

    A. boot sector
    B. parasitic
    C. stealth
    D. polymorphic

29. Referential Integrity requires that for any foreign key attribute, the referenced relation must have a tuple with the same value for which of the following?

    A. candidate key
    B. foreign key
    C. secondary key
    D. primary key

30. The description of the database is called a schema, and the schema is defined by which of the following?

    A. Data Encapsulation Language (DEL).

    B. Data Connection Language (DCL).

    C. Data Definition Language (DDL).

    D. Data Identification Language (DIL).

31. What is used to hide data from unauthorized users by allowing a relation in a database to contain multiple tuples with the same primary keys with each instance distinguished by a security level?

    A. Noise and perturbation

    B. Cell suppression

    C. Polyinstantiation

    D. Data mining

32. A computer program in which malicious or harmful code is contained inside apparently harmless programming or data in such as way that it can get control and do damage is a:

    A. Trojan horse

    B. trap door

    C. virus

    D. worm

33. What is one disadvantage of content-dependent protection of information?

    A. It requires additional password entry.

    B. It increases processing overhead.

    C. It exposes the system to data locking.

    D. It limits the user's individual address space.

34. What type of malware is self-contained and does not need to be part of another computer program to propagate itself?

    A. Computer virus

    B. Trojan house

    C. Computer worm

D. Polymorphic virus

35. What type of malware that is capable of infect a file with an encrypted copy of itself, then modify itself when decoded to make almost impossible to detect by signature-based virus scanner?

A. Computer virus

B. Trojan house

C. Computer worm

D. Polymorphic virus