Post-Class Quiz: Access Control Domain

1. In order to perform data classification process, what must be present?
   A. A data classification policy.
   B. A data classification standard.
   C. A data classification procedure.
   D. All of the above.

2. What are the three types of access control?
   A. Administrative, physical, and technical
   B. Identification, authentication and authorization
   C. Mandatory, discretionary, and least privilege
   D. Access, management, and monitoring

3. Tokens, smart cards, and one-time password are using in what type of authentication?
   A. Something the subject knew
   B. Something the subject has
   C. Something the subject is
   D. None of the above.

4. In biometrics, the intersection of Type I Error Rate (False Rejection) and Type II Error Rate (False Acceptance) is called?
   A. Crossover Error Rate (CER)
   B. Intercept Error Rate (IER)
   C. Sensitivity and Error Ratio (SER)
   D. Complexity Ratio

5. Which of the following refers to a series of characters used to verify a user's identity?
   A. Token serial number
   B. Userid
   C. Password
   D. Security ticket

6. Company X would like to place an in-line control devices that actively monitors the network traffic for anomalies and enforces access control to prevent distributed denial of service (DDoS) attacks in real-time. What type of device is this?
   A. Intrusion Prevention System (IPS)
   B. Intrusion Detection System (IDS)
   C. Firewall
   D. Router ACL

7. What type of access control allows owners to specify who can access their files?
   A. Mandatory
   B. Discretionary
   C. Relational
   D. Administrative

8. What is the best type of authentication that prevents session hijacking?
   A. Robust
   B. Dongles
   C. Continuous
   D. Tokens

9. Which of the following access control types gives “UPDATE” privileges on Structured Query Language (SQL) database objects to specific users or groups?
   A. Supplemental
   B. Discretionary
   C. Mandatory
   D. System

10. Role-based access control _____.
   A. is unique to mandatory access control
   B. is independent of owner input
   C. is based on user’s job functions
   D. can be compromised by inheritance

11. A major disadvantage of single sign-on (SSO) is:
    A. Consistent time-out enforcement across platforms
    B. A compromised password exposes all authorized resources
    C. Use of multiple passwords to remember
    D. Password change control

12. Programmed procedures, which ensure that valid transactions are processed accurately and only once in the current timescale, are referred to as …?
    A. Data installation controls.
    B. Application controls.
    C. Operation controls.
    D. Physical controls.

13. Which of the following distinguishes misuse detection from intrusion detection?
    A. The perpetrator has no valid accounts on any of the systems in the network.
    B. It uses statistical measures to detect unusual behavior.
    C. The perpetrator has at least one valid account on one of the systems in the network.
    D. It uses a collection of known attacks to detect intrusion.

14. The three primary methods for authentication of a user to a system or network are?
    A. Passwords, tokens, and biometrics.
    B. Authorization, identification, and tokens.
    C. Passwords, encryption, and identification.
    D. Identification, encryption, and authorization.

15. Which one of the following can be identified when exceptions occur using operations security detective controls?
    A. Unauthorized people seeing printed confidential reports
    B. Unauthorized people destroying confidential reports
    C. Authorized operations people performing unauthorized functions
    D. Authorized operations people not responding to important console messages

16. Why do vendors publish MD5 hash values when they provide software patches for their customers to download from the Internet?
    A. Recipients can verify the software's integrity after downloading.
    B. Recipients can confirm the authenticity of the site from which they are downloading the patch.
    C. Recipients can request future updates to the software by using the assigned hash value.
    D. Recipients need the hash value to successfully activate the new software.

17. An access system that grants users only those rights necessary for them to perform their work is operating on which security principle?
    A. Discretionary Access
    B. Least Privilege
    C. Mandatory Access
    D. Separation of Duties

18. Three principal schemes that provide a framework for managing access control are
    A. Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC).
    B. Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Layer Based Access Protocol (LBAP).
    C. Mandatory Access Control (MAC), Layer Based Access Protocol (LBAP), and Target Based Access Protocol (TBAP).
    D. Role Based Access Control (RBAC), Layer Based Access Protocol (LBAP), and Target Based Access Protocol (TBAP).

19. In terms of access control, separation of duties means…
    A. A process is designed so that separate steps must be performed by different people.
    B. The critical task requires two people to complete.
    C. A policy that limits both the system's user and processes to access only those resources necessary to perform assigned functions.
    D. A business process that forces employees to take mandatory vacation.

20. What determines the assignment of data classifications in a mandatory access control philosophy?

A. The analysis of the users in conjunction with the audit department
B. The assessment by the information security department
C. The user's evaluation of a particular information element
D. The requirement of the organization's published security policy

21. In mandatory access control who determines the need-to-know?
A. Information owner and system
B. Information owner
C. Subject and label
D. System

22. Which one of the following can be used to increase the authentication strength of access control?
A. Multi-party
B. Two factor
C. Mandatory
D. Discretionary

23. Granularity is the level of detail to which…?
A. A trusted system can authenticate users.
B. Imperfections of a trusted system can be measured.
C. An access control system can be adjusted.
D. Packets can be filtered.

24. Which of the following does a digital signature provide?
A. It provides the ability to encrypt an individual's confidential data.
B. It ensures an individual's privacy.
C. It identifies the source and verifies the integrity of data.
D. It provides a framework for law and procedures.

25. Separation of duties should be…?
A. Enforced in all organizational areas.
B. Cost justified for the potential for loss.

C. Enforced in the program testing phase of application development.

D. Determined by the availability of trained staff.

26. What common attack can be used against a system that stores one-way encrypted passwords if a copy of the password file can be obtained?

A. Birthday attack

B. Dictionary attack

C. Plaintext attack

D. Smurf attack

27. When establishing a violation tracking and analysis process, which one of the following parameters is used to keep the quantity of data to manageable levels?

A. Quantity baseline

B. Maximum log size

C. Circular logging

D. Clipping levels

28. The accounting branch of a large organization requires an application to process expense vouchers. Each voucher must be input by one of many accounting clerks, verified by the clerk's applicable supervisor, then reconciled by an auditor before the reimbursement check is produced. Which access control technique should be built into the application to BEST serve these requirements?

A. Mandatory Access Control (MAC)

B. Password Security

C. Role-based Access Control (RBAC)

D. Terminal Access Controller Access System (TACACS)

29. What principle recommends the division of responsibilities so that one person cannot commit an undetected fraud?

A. Separation of duties

B. Mutual exclusion

C. Need to know

D. Least privilege

30. What is the best method of storing user passwords for a system?

A. Password-protected file
B. File restricted to one individual
C. One-way encrypted file
D. Two-way encrypted file

31. What role does biometrics have in logical access control?
A. Certification
B. Authorization
C. Authentication
D. Confirmation

32. What best describes two-factor authentication?
A. Something you know
B. Something you have
C. Something you are
D. A combination of two listed above

33. What are the five categories of access control?
A. Detective, preventive, corrective, recovery, and directive
B. Detective, corrective, monitoring, logging, and classification
C. Authorization, authentication, identification, confidentiality, and integrity.
D. Identification, authentication, least-privilege, need-to-know, and separation-of-duties.

34. Which of the following is not an issue for recording audit trail of system activities?
A. Control of event details to manage data volume.
B. Access control and preservation of audit logs in storage and archive.
C. Training of personnel to identify non-conformance or illegal activitess.
D. Define organizational policy for audit records.

35. An act of verifying and validating the system against a set of specified security requirements is called?
A. A security audit

B. A vulnerability assessment
C. Penetration test
D. System test.