

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 1

1. What are the three critical areas of security?
 - a) Authentication, Accreditation, and Authorization
 - b) Integrity, Confidentiality, and Availability
 - c) Confidentiality, Integrity, and Authentication
 - d) Non-repudiation, Availability, and Integrity
2. Which of the following critical areas of security represents the unauthorized modification of information?
 - a) Confidentiality
 - b) Repudiation
 - c) Authorization
 - d) Integrity
3. Which formula below accurately represents the equation for calculating the risk associated with your critical assets?
 - a) Risk = Vulnerability x Likelihood
 - b) Threat = Risk x Vulnerability
 - c) Risk = Threat x Vulnerability
 - d) Vulnerability = Threat x Risk
4. Of the four core principles of network security, which one relates to understanding which services are running on your system?
 - a) Defense-in-Depth
 - b) Principle of Least Privilege
 - c) Prevention is Ideal but Detection is a Must
 - d) Know Thy System
5. Giving Bob, the accountant, access only to the Accounting application required for his duties is an example of which core security principle?
 - a) Defense-in-Depth
 - b) Principle of Least Privilege
 - c) Know Thy User
 - d) Know Thy System
6. Which principle is represented by an accountant creating a company's books and an auditor reviewing the books for accuracy?
 - a) Separation of Duties
 - b) Principle of Least Privilege
 - c) Job Rotation
 - d) Know Thy System
7. Which access control measure method would be affected by an inaccessible system administrator?
 - a) Preventive

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 1

- b) Suggestive
 - c) Incentive
 - d) Detective
8. Which of the following concepts relates most closely to the Principle of Least Privilege?
- a) Authentication
 - b) Identity
 - c) Detection
 - d) Separation of Duties
9. If Dan, a user with level three clearance, attempts to read a document requiring a level four clearance, he is violating which of the following access control techniques?
- a) The Star Property of the Bell-LaPadula Model
 - b) The Simple Security Property of the Bell-LaPadula Model
 - c) The Simple Integrity Property of the Biba Model
 - d) The Super Simple Star Property of Biba Model
10. Which of the following access control techniques requires the user to follow a procedure to access protected data?
- a) The Clark-Wilson model
 - b) The Biba model
 - c) The Middleman model
 - d) The Bell-LaPadula model
11. Which of the following characteristics makes the BIBA model the opposite of the Bell LaPadula (BLP) model?
- a) No write down and no read up
 - b) Read up but no write down
 - c) No read down and no write up
 - d) Write down but no read up
12. In the process of employee termination, which access management activity most effectively controls access?
- a) Account administration
 - b) Account maintenance
 - c) Account monitoring
 - d) Account revocation

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 1

13. Of the four ways a user can be authenticated, which presents the use of physical human attributes in the process?
 - a) Something you are
 - b) Something you have
 - c) Something you know
 - d) Something you share

14. If you had a classified system located in the middle of the desert, which authentication method would serve best?
 - a) Something you have
 - b) Something you know and are
 - c) Something you share
 - d) Someplace you are

15. What is the MOST influential factor in determining if a biometric solution is feasible for a system?
 - a) System size
 - b) Usability
 - c) Criticality
 - d) Cost

16. Which authentication method negotiates the validity of the user through tickets?
 - a) Single Sign On (SSO)
 - b) System Generated Passwords (SGP)
 - c) Challenge Handshake Authentication Protocol (CHAP)
 - d) Kerberos

17. Which password cracking technique will eventually figure out Jim's hard-to-guess password?
 - a) Hybrid attack
 - b) Brute force attack
 - c) Dictionary attack
 - d) Long-term attack

18. Stateful inspection of packets is an example of which kind of access control?
 - a) Prevention
 - b) Detection
 - c) Suspension
 - d) Eradication

Management 414: SANS CISSP® 10 Domains +5 QUIZ - Domain 1

19. Which are the three common methods used in password cracking?
- a) Dictionary, hybrid, and brute force
 - b) Word list, brute force, and distributed
 - c) John the ripper, LOphtcrack, and hydra
 - d) SAM, passwd, and shadow
20. Which of the following are among the primary design types used for access control systems today?
- a) Mandatory, discretionary, and role-based
 - b) Interaction, fixed, and closed
 - c) Subject-based, object-based, and file-based
 - d) Mandatory, optional, and discretionary
21. Which of the following access control techniques associates a group of users and their privileges with each object?
- a) Role Based Access Control
 - b) Token Based Access Control
 - c) List Based Access Control
 - d) User Based Access Control
22. Which of the following is NOT an example of a Mandatory Access Control (MAC) technique?
- a) Secure Communications Processor (SCOMP)
 - b) SMURF
 - c) Pump
 - d) Purple Penelope
23. Which of the following access control techniques allows the user to feel empowered and able to change security attributes?
- a) Discretionary Access Control
 - b) Mandatory Access Control
 - c) Optional Access Control
 - d) User Access Control
24. Which of the following control types is used to provide alternatives to other controls?
- a) Compensating
 - b) Deterrent
 - c) Corrective
 - d) Recovery

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 1

25. Your location is one of four commonly accepted items on which authentication can be based. What are the other three?
- a) Something you say, type, or press
 - b) Something you have, do, or know
 - c) Something you do, know, type
 - d) Something you know, have, or are
26. What attribute of the Kerberos authentication process makes it so strong?
- a) Encrypting the Ticket Granting Ticket (TGT)
 - b) Mutual authentication
 - c) Using a Ticket Distribution Center (TDC) and a Key Granting Server (KGS)
 - d) User defined passwords
27. Applying which principle represents one of the best ways to thwart internal attacks using access control systems?
- a) Principle of Open Access
 - b) Principle of Least Privilege
 - c) Principle of Internal Suppression
 - d) Principle of Trust
28. There are three primary areas of threat. Of the following items, which is NOT one of those three areas?
- a) Threats to business goals
 - b) Threats based on validated data
 - c) Threats that are widely known
 - d) Threats combined with risk
29. In terms of information security, what is a vulnerability?
- a) A weakness in your systems that allows a threat to occur
 - b) A threat to your security that creates a risk condition
 - c) A combining of both a risk and a threat in the same system
 - d) A risk to your system(s) that cannot be eliminated
30. Which are the three generally accepted options for managing risk?
- a) Eliminate, quarantine, or insure
 - b) Accept, mediate, or delegate
 - c) Accept, eliminate, or transfer
 - d) Transfer, eliminate, or cogitate
31. What is the principle that ensures data has not been modified either in transit or while in storage referred to as?
- a) Non-repudiation
 - b) Assurance

Management 414: SANS CISSP® 10 Domains +S QUIZ - Domain 1

- c) Integrity
 - d) Reliability
32. What is the principle that ensures information is not disclosed to unauthorized users referred to as?
- a) Encryption
 - b) Confidentiality
 - c) Encapsulation
 - d) Security
33. The assurance of access to data when it is needed is one of the three key principles in information security. What is this principle called?
- a) Availability
 - b) Guaranteed delivery
 - c) Accessibility
 - d) Connectivity
34. Discretionary Access Control (DAC) is one of the many Access Control Models. Which of the following items is NOT part of the Discretionary Access Control (DAC) model?
- a) An administrator decides whether a user should have access to an object
 - b) Performed at the discretion of any administrator
 - c) Strictly enforced by the system and cannot be overridden
 - d) Owners can change security attributes