Domain 5 Questions

1. What is the PRIMARY use of a password?

- ☐ a. Allow access to files
- ☐ b. Identify the user
- ☐ c. Authenticate the user
- ☐ d. Segregate various users' accesses

2. A potential vulnerability of the Kerberos authentication server is:

- ☐ a. Single point of failure
- ☐ b. Asymmetric key compromise
- ☐ c. Use of dynamic passwords
- ☐ d. Limited lifetimes for authentication credentials

3. An access control matrix specifies permissions from which perspective

- ☐ a. Object
- ☐ b. View
- ☐ c. Subject
- ☐ d. Information

4. What access control methodology facilitates frequent changes to data permission for user groups?

- ☐ a. Rule-based
- ☐ b. List-based
- ☐ c. Role-based
- ☐ d. Ticket-based

5. What is the purpose of a ticket-oriented security mechanism?

- ☐ a. Permits the subject's access to objects
- ☐ b. Assigns access modes to objects
- ☐ c. Grants subject's discretionary control
- ☐ d. Assures user access accountability

6. Identity Management is:

- ☐ a. Another name for access controls
- ☐ b. A set of technologies and processes intended to offer greater efficiency in the management of a diverse user and technical environment
- ☐ c. A set of technologies and processes focused on the provisioning and decommissioning of user credentials
- ☐ d. A set of technologies and processes used to establish trust relationships with disparate systems.

7. Which of the following is NOT a part of the Kerberos authentication scheme?

- ☐ a. Authentication server
- ☐ b. Ticket granting server
- ☐ c. Users and programs
- ☐ d. Message Authentication Code

8. According to the “Orange Book’s TCSEC,” the Trusted Computing Base should enforce accountability to provide the capability to uniquely identify each individual user and to

- ☐ a. Protect that individual’s data from unauthorized modification or destruction.
- ☐ b. Create an audit record each time a user changes a password.
- ☐ c. Associate the identity with all auditable actions taken by the individual.
- ☐ d. Preclude simultaneous log on sessions by a single individual.

9. What type of attack is eavesdropping?

- ☐ a. Active
- ☐ b. Passive
- ☐ c. Aggressive
- ☐ d. Masquerading

10. Which of the following biometric devices has the highest Cross-over Error Rate (CER)?

- ☐ a. Iris scan
- ☐ b. Hand geometry
- ☐ c. Voice pattern
- ☐ d. Fingerprints

11. What physical characteristic does a retinal scan biometric device measure?

- ☐ a. The amount of light reaching the retina
- ☐ b. The colors, patterns, and rings of the retina
- ☐ c. The size, curvature, and shape of the retina
- ☐ d. The pattern of blood vessels at the back of the eye

12. While evaluating the effectiveness of several new devices, the security professional should expect that a biometric device becomes more sensitive when

- ☐ a. Both the False Acceptance Rate (FAR) and False Rejection Rate (FRR)) increase.
- ☐ b. The FAR increases while the FRR decreases.
- ☐ c. The FAR decreases while the FRR increases.
- ☐ d. Both the FAR and FRR decrease.

13. The point where the False Acceptance Rate (FAR) and False Rejection Rate (FRR) is balanced is known as:

- ☐ a. Crossover Error Rate (CER).
- ☐ b. Crossover Acceptance Rate (CAR).
- ☐ c. Equal Crossover Rate (ECR).
- ☐ d. Equal Acceptance Rate (EAR).

14. What determines the correct classification of data in a Mandatory Access Control (MAC) environment?

- ☐ 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 requirements of an organization’s published security policy

15. Which one 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

16. In order to give employees appropriate access rights, a company might choose to determine what tasks need to be accomplished, and then to define what access rights are necessary to accomplish said tasks. This form of access control is called:

- ☐ a. Rule-based access control and need-to-know
- ☐ b. Role-based access control
- ☐ c. Need-to-know and least privilege
- ☐ d. Non-discretionary access control

17. What answer lists 3 control categories?

- ☐ a. Preventative, physical, detective
- ☐ b. Physical, administrative, technical
- ☐ c. Deterrent, preventative, compensating
- ☐ d. Administrative, directive, deterrent

18. Which of the following devices has an embedded microchip which can store large amounts of data, double as an access card for doors, and an authenticator on a computer?

- ☐ a. Smart Card
- ☐ b. Proximity card, or “prox” card
- ☐ c. PIN card
- ☐ d. Magnetic-stripe card

19. Which statement BEST describes an access control?

- ☐ a. A hidden device that permits identity spoofing.
- ☐ b. A deployment of encryption to protect authorization systems.
- ☐ c. A mechanism that helps protect systems by controlling unauthorized user activities.
- ☐ d. A systems device that records all user login attempts.

20. Which of the following operations security activities requires the LEAST amount of training and experience?

- ☐ a. Maintaining operational resilience.
- ☐ b. Controlling user accounts.
- ☐ c. Protecting valuable assets.
- ☐ d. Managing security services effectively.

21. To create an effective access control system for your organizational desktops, which list or chart must be created?

- ☐ a. The company’s computer organizational placement chart.
- ☐ b. A list that shows which users need special permissions.
- ☐ c. A set of firewall rules that either permit or deny different computer systems access to specific services.
- ☐ d. A set of Kerberos rules that the Kerberos Ticket Granting Server (TGS) uses to allow users to access to certain objects.

22. Which answer below contains two of the MOST accurate biometric systems?

- ☐ a. Retinal scans and hand geometry.
- ☐ b. Iris Scans and keystroke dynamics.
- ☐ c. Fingerprint readers and facial recognition.
- ☐ d. Iris scans and vascular pattern scans.

23. In the context of the Confidentiality, Integrity, and Availability (CIA) triad, “Perfect availability” of a resource means which of the following?

- ☐ a. Availability 24 hours a day, 7 days a week (24/7)
- ☐ b. Availability whenever authorized users require access to the resource in order to do their jobs.
- ☐ c. Availability as appropriate to support the Business Continuity Plan/Disaster Recovery Plan (BCP/DRP).
- ☐ d. Full availability even to users in branch offices who have to remote in to access resources.

24. If a system’s security goal is that no subject can gain access to any object without authorization, which of the following should be implemented?

- ☐ a. The security kernel implementing the reference monitor concept.
- ☐ b. The ring protection mechanism.
- ☐ c. Virtual memory mapping and process isolation.
- ☐ d. Correct management of memory and storage.

25. Which of the following is the BEST example of two-factor authentication?

- ☐ a. Requiring a user to use both a digital fingerprint and an iris scan to get logged in.
- ☐ b. Requiring a user to provide a 14 character password and also punch in an 8 character access key to a cipher lock located at the entrance door.
- ☐ c. Requiring a token device to be inserted in a special slot at the entrance door, as well as a keyless entry device.
- ☐ d. Requiring a token device and a fingerprint.

26. Role-based access control is _____?

- ☐ a. Unique to mandatory access control systems.
- ☐ b. Often implemented by modern firewalls.
- ☐ c. A set of technologies focusing on provisioning and decommissioning user credentials.
- ☐ d. Based on the user’s job function.

27. Sarah has just successfully logged into a system using Kerberos. She wants to edit a file located on server KK, which is in the same domain that she is. Which action BEST describes how this will be done?

- ☐ a. Sarah can access the file without logging into Server KK.
- ☐ b. Sarah logs into Server KK and accesses the file.
- ☐ c. Sarah goes back to the Kerberos system, gets a special ticket for Server KK, and uses it to log into Server KK. Server KK will then decide whether Sarah can edit her requested file.
- ☐ d. Sarah goes back to the Kerberos system, gets a special ticket for Server KK, and uses it to log into Server KK. Since she is an authenticated user, she will be automatically allowed to edit the requested file.

28. When a company is considering adopting a biometric system, which is the LEAST important consideration?

- ☐ a. Technology type
- ☐ b. Reliability and accuracy
- ☐ c. User acceptance
- ☐ d. Resistance to users counterfeiting their credentials.

29. Which statement BEST describes how “role-based access control” is typically used?

- ☐ a. It only occurs in discretionary access control systems (DACs).
- ☐ b. Since it is based on the user’s job function, it can be used in many situations.
- ☐ c. It is always used in mandatory access control system (MACs).
- ☐ d. It is the accepted method for limiting users to certain tasks at certain times of the day.

30. In a SAML 2.0 system, when a user across the Internet is attempting to access a web service, which of the following happens?

- ☐ a. The web server uses a federated login system to authenticate the user.
- ☐ b. The web service provides both authentication and authorization
- ☐ c. The web service uses a direct connection to an Active Directory (AD) server to provide authentication.
- ☐ d. Web Server connects back to the user’s home login system to determine whether the user should be allowed to access the desired service.

31. The correct ordering of steps with respect to user access to an object is:

- ☐ a. Identification, authorization, auditing
- ☐ b. Identification, authentication, authorization
- ☐ c. Authorization, setup of auditing for the session, authentication
- ☐ d. Authentication, setup of auditing for the session, access

32. Which statement BEST describes the differences in the access control vulnerabilities known as skimming and spoofing?

- ☐ a. Skimming occurs when an actor is able to capture the magnetic stripe on a card (e.g., credit card or employee badge)
- ☐ b. Spoofing is using someone else's identity to get into a computer system, while skimming means that you use a radio signal detector to pick up someone's identity for later use
- ☐ c. Spoofing is easiest to do with MAC addresses on computer systems, skimming is getting a fake IP address from an unattended computer
- ☐ d. Both of these hacks are tricks to get the MAC address from someone's computer

33. What is the MOST important benefit of storing passwords as hashed values?

- ☐ a. Hashed passwords are harder to decrypt than encrypted passwords
- ☐ b. For a given word, generating a password hash is faster than encrypting it
- ☐ c. If you are able to find a word that is hashed to a stored password hash value, you have only found one password, not all of them
- ☐ d. Encryption is illegal in some countries so storing as hashes enables logins to be possible internationally

34. Often the acronym IAAA is used to describe the four phases of access control, in the order in which they are normally done. Which statement matches both the definition and sequence of the IAAA terms?

- ☐ a. Integrity, Authorization, Auditing, and Accounting
- ☐ b. Identity, Authentication, Authorization, and Auditing
- ☐ c. Integrity, Authorization, Authentication, and Auditing
- ☐ d. Identity, Accounting, Authorization, and Auditing

35. The two BEST alternative choices for key exchange available to a telecommuter using Transport Mode IPSEC are _____

- ☐ a. Certificate-based or PSK (Pre-Shared Key)
- ☐ b. Certificate-based or Diffie-Hellman Key Exchange (DH).
- ☐ c. ISAKMP (IPSec Security Association Key Management Protocol) or DH (Diffie-Hellman Key Exchange)
- ☐ d. PSK (Pre-Shared Key) or ISAKMP (IPSec Security Association Key Management Protocol)

36. In a TCP connection, which station sets the FIN bit to "on"?

- ☐ a. The client
- ☐ b. The server
- ☐ c. Whichever station initiated the connection
- ☐ d. Whichever station wants to terminate the connection

37. Modern database systems have various integrity forms. Which statement BEST describes these forms?

- ☐ a. A database system must understand the semantics of the data, else processing errors will happen
- ☐ b. The entity integrity model forces each tuple to have a unique and non-null value primary key
- ☐ c. The referential integrity model allows foreign keys to be null values
- ☐ d. To achieve data integrity, database systems hash each table, twice, one for the entire table, and then the second time for each record

38. Which of the following is the MOST likely to successfully prevent unauthorized access?

- ☐ a. An access control policy
- ☐ b. An incident response plan
- ☐ c. A visitor log
- ☐ d. An RFID-embedded badge system

39. Which of these is done by an operating system?

- ☐ a. Discretionary Access Control
- ☐ b. Database Access Control
- ☐ c. Content-Sensitive Access Control
- ☐ d. Context-Sensitive Access Control

40. “Clearance” is a concept found only in _____

- ☐ a. DAC (Discretionary Access Control)
- ☐ b. N-DAC (Non-Discretionary Access Control)
- ☐ c. MAC (Mandatory Access Control)
- ☐ d. RBAC (Role-Based Access Control)

41. Which statement about Kerberos is TRUE?

- ☐ a. It only works with Windows clients and servers
- ☐ b. It works with all or nearly all Intranet-based applications
- ☐ c. It is a single point of failure in its default configuration
- ☐ d. It requires 2-factor authentication methods

42. IDaaS (Identity as a Service) is growing in popularity. Its use is essential in which of the following?

- ☐ a. Single sign-on authentication
- ☐ b. Client-server authentication
- ☐ c. Cloud authentication
- ☐ d. Federated authentication

43. The Identity and Access Management lifecycle has three steps. Which of the following is NOT among them?

- ☐ a. Provisioning: Applying appropriate rights to users for files/folders
- ☐ b. Authentication: Examining rights before each access attempt
- ☐ c. Review: Periodic monitoring of existing rights for continued need
- ☐ d. Revocation: Removal of rights when no longer needed or warranted

44. The USA is moving to EMV (Europay, Mastercard and Visa) credit cards that have a chip. What is the MAIN security advantage of these chip-based credit cards?

- ☐ a. Losses are borne by the consumer, rather than the banks and merchants.
- ☐ b. They are less expensive to produce and replace.
- ☐ c. They have a certificate in them created by the issuing bank which cannot be forged, unlike the magnetic strip that has been used for decades.
- ☐ d. They enable payment techniques such as ApplePay and Google Wallet.