**Access Control Methods – Answers**

1. Which of the following is true of biometrics?
   1. It is used for identification in physical controls and it is not used in logical controls.
   2. It is used for authentication in physical controls and for identification in logical controls.
   3. **It is used for identification in physical controls and for authentication in logical controls.**
   4. Biometrics has not role in logical controls.
2. What security model is dependant on security labels?
   1. Discretionary access control
   2. Label-based access control
   3. **Mandatory access control**
   4. Non-discretionary access control
3. A central authority determines what subjects can have access to certain objects based on the organizational security policy is called:
   1. Mandatory Access Control
   2. Discretionary Access Control
   3. **Non-Discretionary Access Control**
   4. Rule-based Access control
4. In Discretionary Access Control the subject has authority, within certain limitations,
   1. but he is not permitted to specify what objects can be accessible and so we need to get an independent third party to specify what objects can be accessible.
   2. **to specify what objects can be accessible.**
   3. to specify on a aggregate basis without understanding what objects can be accessible.
   4. to specify in full detail what objects can be accessible.
5. Which of the following is an example of discretionary access control?
   1. **Identity-based access control**
   2. Task-based access control
   3. Role-based access control
   4. Rule-based access control
6. Which of the following is one-to-one verification using small databases used for?
   1. **Finger-scan technology**
   2. Hand-scan technology
   3. Body-scan technology
   4. Skin-scan technology
7. In biometric identification systems, false reject rate is associated with:
   1. Type 2 errors
   2. type 1 and type 2 errors
   3. type 3 errors
   4. **type 1 errors**
8. The principle of least privilege is inconsistent with which of the following?
   1. **Users may not be able to access any systems.**
   2. Users can access some systems.
   3. Users get new privileges when they change positions.
   4. Authorization creep is prevented.
9. Which of the following centralized access control mechanisms is not appropriate for mobile workers accessing the corporate network over analog lines?
   1. TACACS
   2. **Call-back**
   3. CHAP
   4. RADIUS
10. Which access control model is best suited in an environment where a high security level is required and where it is desired that only the administrator grants access control?
    1. DAC
    2. **MAC**
    3. RBAC
    4. TACACS
11. Logical or technical controls involve the restriction of access to systems and the protection of information. Which of the following statements pertaining to these types of controls is correct?
    1. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks but do not include a review of vacation history, and also do not include increased supervision.
    2. Examples of these types of controls do not include encryption, smart cards, access lists, and transmission protocols.
    3. **Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.**
    4. Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.
12. Which of the following choices describe a Challenge-response tokens generation?
    1. **A workstation or system that generates a random challenge string that the user enters into the token when prompted along with the proper PIN.**
    2. A workstation or system that generates a random login id that the user enters when prompted along with the proper PIN.
    3. A special hardware device that is used to generate ramdom text in a cryptography system.
    4. The authentication mechanism in the workstation or system does not determines if the owner should be authenticated.
13. Which of the following does not apply to system-generated passwords?
    1. Passwords are harder to remember for users.
    2. If the password-generating algorithm gets to be known, the entire system is in jeopardy.
    3. **Passwords are more vulnerable to brute force and dictionary attacks.**
    4. Passwords are harder to guess for attackers.
14. The control measures that are intended to reveal the violations of security policy using technical means are associated with:
    1. Preventive/physical
    2. **Detective/technical**
    3. Detective/physical
    4. Detective/administrative
15. In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on :
    1. sex of a person
    2. **physical attributes of a person**
    3. age of a person
    4. voice of a person
16. A timely review of system access audit records would be an example of which of the basic security functions?
    1. avoidance
    2. deterrence
    3. prevention
    4. **detection**
17. Which of the following statements pertaining to Kerberos is FALSE?
    1. Kerberos does not address availability
    2. **Kerberos does not address integrity**
    3. Kerberos is vulnerable to frequency analysis attacks
    4. Kerberos addresses confidentiality of information
18. Which of the following access control models requires security clearance for subjects?
    1. Identity-based access control
    2. Role-based access control
    3. Discretionary access control
    4. **Mandatory access control**
19. Which of the following statements relating to the Bell-LaPadula security model is FALSE?
    1. A subject is not allowed to read up.
    2. The \*- property restriction can be escaped by temporarily downgrading a high level subject.
    3. **A subject is not allowed to read down.**
    4. It is restricted to confidentiality.
20. Which of the following access control models requires defining classification for objects?
    1. Role-based access control
    2. Discretionary access control
    3. Identity-based access control
    4. **Mandatory access control**
21. The authenticator within Kerberos provides a requested service to the client after validating which of the following?
    1. **timestamp**
    2. client public key
    3. client private key
    4. server public key
22. Which of the following biometric characteristics cannot be used to uniquely authenticate an individual's identity?
    1. Retina scans
    2. Iris scans
    3. Palm scans
    4. **Skin scans**
23. Using clipping levels refers to:
    1. **setting allowable thresholds on a reported activity**
    2. limiting access to top management staff
    3. setting personnel authority limits based on need-to-know basis
    4. encryption of data so that it cannot be stolen
24. Which of the following represents the columns of the table in a relational database?
    1. **attributes**
    2. relation
    3. record retention
    4. records or tuples
25. What is considered the most important error for a biometric access control system?
    1. Type I Error
    2. **Type II Error**
    3. Combined Error Rate
    4. Crossover Error Rate
26. Controls are implemented to:
    1. eliminate risk and reduce the potential for loss
    2. mitigate risk and eliminate the potential for loss
    3. **mitigate risk and reduce the potential for loss**
    4. eliminate risk and eliminate the potential for loss
27. Which of the following pairings uses technology to enforce access control policies?
    1. Preventive/Administrative
    2. **Preventive/Technical**
    3. Preventive/Physical
    4. Detective/Administrative
28. A confidential number to verify a user's identity is called a:
    1. **PIN**
    2. userid
    3. password
    4. challenge
29. Which of the following is a preventive control?
    1. Motion detectors
    2. **Guard dogs**
    3. Audit logs
    4. Intrusion detection systems
30. Discretionary access controls:
    1. are concerned with information flow.
    2. are based upon security labels.
    3. **are widely used in commercial environments.**
    4. are less flexible than mandatory access controls.
31. What is Kerberos?
    1. A three-headed dog from Egyptian mythology
    2. **A trusted third-party authentication protocol**
    3. A security model
    4. A remote authentication dial in user server
32. Which of the following is not a complementary control when implementing logical access security?
    1. access profiles
    2. userids
    3. **employee badges**
    4. passwords
33. Mandatory Access requires that sensitivity labels be attached to all objects. Which of the following would be designated as objects on a MAC system?
    1. files, directories, processes, and sockets
    2. devices, processes and sockets
    3. users, windows, and programs
    4. **files, directories and devices**
34. There are parallels between the trust models in Kerberos and in PKI. When we compare them side by side, Kerberos tickets correspond most closely to which of the following?
    1. public keys
    2. private keys
    3. **public-key certificates**
    4. private-key certificates
35. The Terminal Access Controller Access Control System (TACACS) employs which of the following?
    1. **a user ID and static password for network access.**
    2. a user ID and dynamic password for network access.
    3. a user ID and symmetric password for network access.
    4. a user ID and asymmetric password for network access.
36. Which of the following can be defined as the task of monitoring systems for evidence of an intrusion or an inappropriate usage?
    1. **Intrusion Detection (ID) and Response**
    2. Intrusion Evaluation (IE) and Response
    3. Intrusion Protection (IP) and Response
    4. Intrusion Recognition (IR) and Response
37. What is called the percentage at which the False Rejection Rate equals the False Acceptance Rate?
    1. False Rejection Rate (FRR) or Type I Error
    2. False Acceptance Rate (FAR) or Type II Error
    3. **Crossover Error Rate (CER)**
    4. True Acceptance Rate (TAR) or Type III Error
38. In addition to the accuracy of the biometric systems, there are other factors that must also be considered:
    1. These factors include the enrolment time and the throughput rate, but not acceptability.
    2. These factors do not include the enrolment time, the throughput rate, and acceptability.
    3. **These factors include the enrolment time, the throughput rate, and acceptability.**
    4. These factors include the enrolment time, but not the throughput rate, neither the acceptability.
39. An IDS detects an attack using which of the following?
    1. an event-based ID or a statistical anomaly-based ID.
    2. a discrete anomaly-based ID or a signature-based ID.
    3. **a signature-based ID or a statistical anomaly-based ID.**
    4. a signature-based ID or an event-based ID.
40. When a biometric system is used, which error type deals with the possibility of granting access to impostors who should be rejected?
    1. Type I error
    2. **Type II error**
    3. Type III error
    4. Crossover error
41. Which of the following is a detective control?
    1. Segregation of duties
    2. Back-up procedures
    3. **Audit trails**
    4. Physical access control
42. In Kerberos, the client decrypts the message containing the session key (KC, TGS) with its secret key (KC), and will now use this session key to communicate with the:
    1. **TGS server**
    2. TGS client
    3. TGS server and TGS client
    4. TGS client and TGS server
43. In biometrics, "one-to-many" search against database of stored biometric images is done in:
    1. Authentication
    2. **Identification**
    3. Identities
    4. Identity-based access control
44. In a discretionary mode, which of the following entities is authorized to grant information access to other people?
    1. manager
    2. group leader
    3. security manager
    4. **user**
45. In an organization where there are frequent personnel changes, non-discretionary access control is useful because:
    1. people need not use discretion
    2. **the access controls are based on the individual's role or title within the organization.**
    3. the access controls are not based on the individual's role or title within the organization
    4. the access controls are often based on the individual's role or title within the organization
46. Like Kerberos, SESAME is also subject to which of the following?
    1. timeslot replay
    2. **password guessing**
    3. symmetric key resolution
    4. asymmetric key resolution
47. What physical characteristic does a retinal scan biometric device measure?
    1. The amount of light reaching the retina
    2. The amount of light reflected by the retina
    3. The pattern of light receptors at the back of the eye
    4. **The pattern of blood vessels at the back of the eye**
48. An access control policy for a bank teller is an example of the implementation of which of the following?
    1. rule-based policy
    2. identity-based policy
    3. user-based policy
    4. **role-based policy**
49. Why would anomaly detection IDSs often generate a large number of false positives?
    1. Because they can only identify correctly attacks they already know about.
    2. Because they are application-based are more subject to attacks.
    3. Because they can't identify abnormal behavior.
    4. **Because normal patterns of user and system behavior can vary wildly.**
50. Which of the following is NOT an advantage that password synchronization has over single sign-on?
    1. **higher cost**
    2. less intrusive
    3. improved security
    4. lower cost
51. The three classic ways of authenticating yourself to the computer security software are by something you know, by something you have, and by something:
    1. you need.
    2. non-trivial.
    3. **you are.**
    4. you can get.
52. Kerberos can prevent which one of the following attacks?
    1. tunneling attack
    2. **playback (replay) attack**
    3. destructive attack
    4. process attack
53. Unfortunately, Kerberos is vulnerable to replay in which of the following circumstances?
    1. When a private key is compromised within an allotted time window.
    2. When a public key is compromised within an allotted time window.
    3. **When a ticket is compromised within an allotted time window.**
    4. When the KSD is compromised within an allotted time window.
54. These, in the form of credit card-size memory cards or smart cards, or those resembling small calculators, are used to supply static and dynamic passwords are called:
    1. Tickets
    2. **Tokens**
    3. Token passing networks
    4. Coupons
55. Which of the following is true of two-factor authentication?
    1. It uses the RSA public-key signature based on integers with large prime factors.
    2. It requires two measurements of hand geometry.
    3. It does not use single sign-on technology.
    4. **It relies on two independent proofs of identity.**
56. What is the primary role of smartcards in a PKI?
    1. Transparent renewal of user keys
    2. Easy distribution of the certificates between the users
    3. Fast hardware encryption of the raw data
    4. **Tamperproof, mobile storage and application of private keys of the users**
57. Which of the following monitors network traffic in real time?
    1. **network-based IDS**
    2. host-based IDS
    3. application-based IDS
    4. firewall-based IDS
58. What IDS approach relies on a database of known attacks?
    1. **Signature-based intrusion detection**
    2. Statistical anomaly-based intrusion detection
    3. Behavior-based intrusion detection
    4. Network-based intrusion detection
59. Which access control model enables the owner of the resource to specify what subjects can access specific resources?
    1. **Discretionary Access Control**
    2. Mandatory Access Control
    3. Sensitive Access Control
    4. Role-based Access Control
60. Technical controls such as encryption and access control can be built into the operating system, be software applications, or can be supplemental hardware/software units. Such controls, also known as logical controls, represent which pairing?
    1. Preventive/Administrative Pairing
    2. **Preventive/Technical Pairing**
    3. Preventive/Physical Pairing
    4. Detective/Technical Pairing
61. How can an individual best be authenticated?
    1. UserId and password
    2. Smart card and PIN code
    3. Two-factor authentication
    4. **Biometrics**
62. Which of the following biometric devices offers the lowest CER (is the BEST)?
    1. Keystroke dynamics
    2. Voice verification
    3. **Iris scan**
    4. Fingerprint
63. What is the PRIMARY use of a password?
    1. Allow access to files.
    2. Identify the user.
    3. **Authenticate the user.**
    4. Segregate various user's accesses.
64. Which of the following is used by RADIUS for communication between clients and servers?
    1. TCP
    2. SSL
    3. **UDP**
    4. SSH
65. Single Sign-on (SSO) is characterized by which of the following advantages?
    1. convenience
    2. **convenience and centralized administration**
    3. convenience and centralized data administration
    4. convenience and centralized network administration
66. Which of the following is most likely to be useful in detecting intrusions?
    1. Access control lists
    2. Security labels
    3. **Audit trails**
    4. Information security policies
67. The act of requiring two of the three factors to be used in the authentication process refers to:
    1. **Two-Factor Authentication**
    2. One-Factor Authentication
    3. Bi-Factor Authentication
    4. Double Authentication
68. Which of the following is true about Kerberos?
    1. It utilizes public key cryptography.
    2. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
    3. **It depends upon symmetric ciphers.**
    4. It is a second party authentication system.
69. Which of the following is true in a system with Mandatory Access Control?
    1. **The system determines which users or groups may access a file.**
    2. A user can set up an access list for the file(s), and the system checks both users and groups against this list before granting access.
    3. A user can specify which groups of users can access their files, but the system determines group membership.
    4. No control is being enforced on this model.
70. Which of the following statements pertaining to access control is false?
    1. Users should only access data on a need-to-know basis.
    2. **If access is not explicitly denied, it should be implicitly allowed.**
    3. Access rights should be granted based on the level of trust a company has on a subject.
    4. Roles can be an efficient way to assign rights to a type of user who performs certain tasks.
71. Which of the following access control models is based on sensitivity labels?
    1. Discretionary access control
    2. **Mandatory access control**
    3. Rule-based access control
    4. Role-based access control
72. When dealing with access control, what is considered “bound to an object?”:
    1. **Access control list**
    2. Access control Matrix
    3. Identification controls
    4. Access terminal
73. Which of the following is an issue with signature-based intrusion detection systems?
    1. **Only previously identified attack signatures are detected.**
    2. Signature databases must be augmented with inferential elements.
    3. Previously defined attack signatures often evolve making the signatures invalid.
    4. Hackers can circumvent signature evaluations.
74. What are called user interfaces that limit the functions that can be selected by a user?
    1. **Constrained user interfaces**
    2. Limited user interfaces
    3. Mini user interfaces
    4. Unlimited user interfaces
75. Which of the following would be the best password?
    1. golf001
    2. Elizabeth
    3. **t1me4g0lf**
    4. password
76. Which of the following statements pertaining to Kerberos is false?
    1. The Key Distribution Center represents a single point of failure.
    2. Kerberos manages access permissions.
    3. **Kerberos uses a database to keep a copy of all users' public keys.**
    4. Kerberos uses symmetric key cryptography.
77. What is the most critical characteristic of a biometric identifying system?
    1. Perceived intrusiveness
    2. Storage requirements
    3. **Accuracy**
    4. Reliability
78. In the real world, access is often incorrectly granted on the basis of:
    1. Least privilege
    2. **Least effort**
    3. Separation of duties
    4. Need to know
79. In what are Access Control Lists (ACLs) and Capability Tables different?
    1. Access control lists are subject-based whereas capability tables are object-based.
    2. **Access control lists are object-based whereas capability tables are subject-based.**
    3. Capability tables are used for objects whereas access control lists are used for users.
    4. They are basically the same.
80. Which of the following is a straightforward approach that provides access rights to subjects for objects?
    1. **Access Matrix model**
    2. Take-Grant model
    3. Bell-LaPadula model
    4. Biba model
81. Controls to keep password sniffing attacks from compromising computer systems include which of the following?
    1. static and recurring passwords
    2. encryption and recurring passwords
    3. **one-time passwords and encryption**
    4. static and one-time passwords
82. Which of the following best ensures accountability of users for the actions taken within a system or domain?
    1. Identification
    2. **Authentication**
    3. Authorization
    4. Credentials
83. Administrative controls include which of the following?
    1. **policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.**
    2. policies and objectives of such policies, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.
    3. policies and procedures, security hacking training, background checks, work habit checks, a review of vacation history, and increased supervision.
    4. policies and procedures, security awareness training, background checks, work habit checks, a review of personal family history, and increased supervision.
84. Which of the following is the weakest authentication mechanism?
    1. Passphrases
    2. **Passwords**
    3. One-time passwords
    4. Token devices
85. Which of the following is a way to enforce mandatory access control?
    1. **Rule-based access control**
    2. Role-based access control
    3. User-directed access control
    4. Lattice-based access control
86. Which of the following was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support?
    1. **SESAME**
    2. RADIUS
    3. KryptoKnight
    4. TACACS+
87. The passphrase is converted:
    1. **into a virtual password by the system.**
    2. into a new passphrase by the system.
    3. by the encryption technology to produce a new passphrase
    4. into a real password by the system which can be used forever.
88. Which of following is not a service provided by AAA servers (Radius, TACACS and DIAMETER)?
    1. Authentication
    2. **Administration**
    3. Accounting
    4. Authorization
89. Which type of control is concerned with restoring controls?
    1. Compensating controls
    2. **Corrective controls**
    3. Recovery controls
    4. Preventive controls
90. Kerberos depends upon what encryption method?
    1. Public Key cryptography
    2. **Secret Key cryptography**
    3. El Gamal cryptography
    4. Blowfish cryptography
91. How are memory cards and smart cards different?
    1. Memory cards normally hold more memory than smart cards
    2. Smart cards provide a two-factor authentication whereas memory cards don't
    3. **Memory cards have no processing power**
    4. Only smart cards can be used for ATM cards
92. SESAME incorporates two certificates or tickets. Which of the following statements is correct?
    1. Both certificates provide authentication as in Kerberos.
    2. One certificate provides authentication as in Kerberos and the other certificate stops the access privileges that are assigned to a client.
    3. One certificate provides authentication and the other certificate defines the access privileges that are assigned to a client as in Kerberos.
    4. **One certificate provides authentication as in Kerberos and the other certificate defines the access privileges that are assigned to a client.**
93. Which authentication technique best protects against hijacking?
    1. Static authentication
    2. **Continuous authentication**
    3. Robust authentication
    4. Strong authentication
94. In Synchronous dynamic password tokens:
    1. **The token generates a new unique password value at fixed time intervals (this password could be the time of day encrypted with a secret key).**
    2. The token generates a new non-unique password value at fixed time intervals (this password could be the time of day encrypted with a secret key).
    3. The unique password is not entered into a system or workstation along with an owner's PIN.
    4. The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is invalid and that it was entered during the invalid time window.
95. What is called the access protection system that limits connections by calling back the number of a previously authorized location?
    1. Sendback systems
    2. Callback forward systems
    3. **Callback systems**
    4. Sendback forward systems
96. Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?
    1. Accountability of biometrics systems
    2. **Acceptability of biometrics systems**
    3. Availability of biometrics systems
    4. Adaptability of biometrics systems
97. Which of the following statements pertaining to Kerberos is false?
    1. A client can be impersonated by password-guessing.
    2. Kerberos is a third-party authentication protocol.
    3. **Kerberos uses public key cryptography.**
    4. Kerberos provides robust authentication.
98. What is called a password that is the same for each log-on session?
    1. "one-time password"
    2. "two-time password"
    3. **static password**
    4. dynamic password
99. The technical mechanisms used for protecting information and passwords from disclosure include:
    1. **Protocols, encryption, and smart cards**
    2. Protocols and smart cards
    3. Encryption and smart cards
    4. Protocols and encryption
100. Example of a clipping level is:
     1. A clipping level of two can be set for reporting failed log-on attempts at a workstation. Thus, three or fewer log-on attempts by an individual at a workstation will not be reported as a violation, thus eliminating the need for reviewing normal log-on entry errors.
     2. A clipping level of four can be set for reporting failed log-on attempts at a workstation. Thus, three or fewer log-on attempts by an individual at a workstation will not be reported as a violation, thus eliminating the need for reviewing normal log-on entry errors.
     3. A clipping level of three can be set for monitoring individual at a workstation by allowing him access according to his authority
     4. **A clipping level of three can be set for reporting failed log-on attempts at a workstation. Thus, three or fewer log-on attempts by an individual at a workstation will not be reported as a violation, thus eliminating the need for reviewing normal log-on entry errors.**