Question No: 1
A potential problem related to the physical installation of the Iris Scanner in regards to the usage of the iris pattern within a biometric system is:
A. Concern that the laser beam may cause eye damage.
B. The iris pattern changes as a person grows older.
C. There is a relatively high rate of false accepts.
D. The optical unit must be positioned so that the sun does not shine into the aperture.
Answer: D

Question No: 2
In Mandatory Access Control, sensitivity labels attached to object contain what information?
A. The item’s classification
B. The item’s classification and category set
C. The item’s category
D. The item’s need to know
Answer: B

Question No: 3
Which of the following is true about Kerberos?
A. It utilizes public key cryptography.
B. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
C. It depends upon symmetric ciphers.
D. It is a second party authentication system.
Answer: C

Question No: 4
Which of the following is needed for System Accountability?
A. Audit mechanisms.
B. Documented design as laid out in the Common Criteria.
C. Authorization.
D. Formal verification of system design.
Answer: A

Question No: 5
What is Kerberos?
A. A three-headed dog from the egyptian mythology.
B. A trusted third-party authentication protocol.
C. A security model.
D. A remote authentication dial in user server.
Answer: B
Question No: 6
Kerberos depends upon what encryption method?
A. Public Key cryptography.
B. Secret Key cryptography.
C. El Gamal cryptography.
D. Blowfish cryptography.
Answer: B

Question No: 7
A confidential number used as an authentication factor to verify a user’s identity is called a:
A. PIN
B. User ID
C. Password
D. Challenge
Answer: A

Question No: 8
Individual accountability does not include which of the following?
A. unique identifiers
B. policies & procedures
C. access rules
D. audit trails
Answer: B

Question No: 9
Which of the following exemplifies proper separation of duties?
A. Operators are not permitted to modify the system time.
B. Programmers are permitted to use the system console.
C. Console operators are permitted to mount tapes and disks.
D. Tape operators are permitted to use the system console.
Answer: A

Question No: 10
An access control policy for a bank teller is an example of the implementation of which of the following?
A. Rule-based policy
B. Identity-based policy
C. User-based policy
D. Role-based policy
Answer: D

Question No: 11
Which one of the following authentication mechanisms creates a problem for mobile users?
A. Mechanisms based on IP addresses
B. Mechanism with reusable passwords
C. One-time password mechanism.
D. Challenge response mechanism.
Answer: A

Question No: 12
Organizations should consider which of the following first before allowing external access to their LANs via the Internet?
A. Plan for implementing workstation locking mechanisms.
B. Plan for protecting the modem pool.
C. Plan for providing the user with his account usage information.
D. Plan for considering proper authentication options.
Answer: D

Question No: 13
Kerberos can prevent which one of the following attacks?
A. Tunneling attack.
B. Playback (replay) attack.
C. Destructive attack.
D. Process attack.
Answer: B

Question No: 14
In discretionary access environments, which of the following entities is authorized to grant information access to other people?
A. Manager
B. Group Leader
C. Security Manager
D. Data Owner
Answer: D

Question No: 15
What is the main concern with single sign-on?
A. Maximum unauthorized access would be possible if a password is disclosed.
B. The security administrator’s workload would increase.
C. The users’ password would be too hard to remember.
D. User access rights would be increased.
Answer: A

Question No: 16
Who developed one of the first mathematical models of a multilevel-security computer system?
A. Diffie and Hellman.
B. Clark and Wilson.
C. Bell and LaPadula.
D. Gasser and Lipner.
Question No: 17
Which of the following attacks could capture network user passwords?
A. Data diddling
B. Sniffing
C. IP Spoofing
D. Smurfing
Answer: B

Question No: 18
Which of the following would constitute the best example of a password to use for access to a system by a network administrator?
A. holiday
B. Christmas12
C. Jenny
D. GyN19Za!
Answer: D

Question No: 19
What physical characteristic does a retinal scan biometric device measure?
A. The amount of light reaching the retina
B. The amount of light reflected by the retina
C. The pattern of light receptors at the back of the eye
D. The pattern of blood vessels at the back of the eye
Answer: D

Question No: 20
The Computer Security Policy Model the Orange Book is based on is which of the following?
A. Bell-LaPadula
B. Data Encryption Standard
C. Kerberos
D. Tempest
Answer: A

Question No: 21
The end result of implementing the principle of least privilege means which of the following?
A. Users would get access to only the info for which they have a need to know
B. Users can access all systems.
C. Users get new privileges added when they change positions.
D. Authorization creep.
Answer: A

Question No: 22
Which of the following is the most reliable authentication method for remote access?
A. Variable callback system
B. Synchronous token
C. Fixed callback system
D. Combination of callback and caller ID
Answer: B

Question No: 23
Which of the following is true of two-factor authentication?
A. It uses the RSA public-key signature based on integers with large prime factors.
B. It requires two measurements of hand geometry.
C. It does not use single sign-on technology.
D. It relies on two independent proofs of identity.
Answer: D

Question No: 24
The primary service provided by Kerberos is which of the following?
A. non-repudiation
B. confidentiality
C. authentication
D. authorization
Answer: C

Question No: 25
There are parallels between the trust models in Kerberos and Public Key Infrastructure (PKI). When we compare them side by side, Kerberos tickets correspond most closely to which of the following?
A. public keys
B. private keys
C. public-key certificates
D. private-key certificates
Answer: C

Question No: 26
In which of the following security models is the subject’s clearance compared to the object’s classification such that specific rules can be applied to control how the subject-to-object interactions take place?
A. Bell-LaPadula model
B. Biba model
C. Access Matrix model
D. Take-Grant model
Answer: A

Question No: 27
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?
A. SESAME
B. RADIUS
C. KryptoKnight
D. TACACS+
Answer: A

Question No: 28
Single Sign-on (SSO) is characterized by which of the following advantages?
A. Convenience
B. Convenience and centralized administration
C. Convenience and centralized data administration
D. Convenience and centralized network administration
Answer: B

Question No: 29
What is the primary role of smartcards in a PKI?
A. Transparent renewal of user keys
B. Easy distribution of the certificates between the users
C. Fast hardware encryption of the raw data
D. Tamper resistant, mobile storage and application of private keys of the users
Answer: D

Question No: 30
What kind of certificate is used to validate a user identity?
A. Public key certificate
B. Attribute certificate
C. Root certificate
D. Code signing certificate
Answer: A

Question No: 31
The following is NOT a security characteristic we need to consider while choosing a biometric identification systems:
A. data acquisition process
B. cost
C. enrollment process
D. speed and user interface
Answer: B

Question No: 32
In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on physical attributes of a person. This raised the necessity of answering 2 questions:
A. what was the sex of a person and his age
B. what part of body to be used and how to accomplish identification that is viable
C. what was the age of a person and his income level  
D. what was the tone of the voice of a person and his habits  
Answer: B,D

Question No: 33  
In biometric identification systems, the parts of the body conveniently available for identification are:  
A. neck and mouth  
B. hands, face, and eyes  
C. feet and hair  
D. voice and neck  
Answer: B

Question No: 34  
Controlling access to information systems and associated networks is necessary for the preservation of their:  
A. Authenticity, confidentiality and availability  
B. Confidentiality, integrity, and availability.  
C. integrity and availability.  
D. authenticity, confidentiality, integrity and availability.  
Answer: B

Question No: 35  
To control access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up:  
A. Access Rules  
B. Access Matrix  
C. Identification controls  
D. Access terminal  
Answer: A

Question No: 36  
Rule-Based Access Control (RuBAC) access is determined by rules. Such rules would fit within what category of access control?  
A. Discretionary Access Control (DAC)  
B. Mandatory Access control (MAC)  
C. Non-Discretionary Access Control (NDAC)  
D. Lattice-based Access control  
Answer: C

Question No: 37  
The type of discretionary access control (DAC) that is based on an individual's identity is also called:  
A. Identity-based Access control  
B. Rule-based Access control  
C. Non-Discretionary Access Control  
D. Lattice-based Access control
Question No: 38
Which access control type has a central authority that determine to what objects the subjects have access to and it is based on role or on the organizational security policy?
A. Mandatory Access Control
B. Discretionary Access Control
C. Non-Discretionary Access Control
D. Rule-based Access control
Answer: C

Question No: 39
Which of the following control pairings include: organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks?
A. Preventive/Administrative Pairing
B. Preventive/Technical Pairing
C. Preventive/Physical Pairing
D. Detective/Administrative Pairing
Answer: A

Question No: 40
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?
A. Preventive/Administrative Pairing
B. Preventive/Technical Pairing
C. Preventive/Physical Pairing
D. Detective/Technical Pairing
Answer: B

Question No: 41
What is called the use of technologies such as fingerprint, retina, and iris scans to authenticate the individuals requesting access to resources?
A. Micrometrics
B. Macrometrics
C. Biometrics
D. MicroBiometrics
Answer: C

Question No: 42
What is called the access protection system that limits connections by calling back the number of a previously authorized location?
A. Sendback systems
B. Callback forward systems
C. Callback systems
D. Sendback forward systems
Answer: C

Question No: 43
What are called user interfaces that limit the functions that can be selected by a user?
A. Constrained user interfaces
B. Limited user interfaces
C. Mini user interfaces
D. Unlimited user interfaces
Answer: A

Question No: 44
Controls such as job rotation, the sharing of responsibilities, and reviews of audit records are associated with:
A. Preventive/physical
B. Detective/technical
C. Detective/physical
D. Detective/administrative
Answer: D

Question No: 45
The control measures that are intended to reveal the violations of security policy using software and hardware are associated with:
A. Preventive/physical
B. Detective/technical
C. Detective/physical
D. Detective/administrative
Answer: B

Question No: 46
The controls that usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists are associated with:
A. Preventive/physical
B. Detective/technical
C. Detective/physical
D. Detective/administrative
Answer: C

Question No: 47
External consistency ensures that the data stored in the database is:
A. in-consistent with the real world.
B. remains consistent when sent from one system to another.
C. consistent with the logical world.
D. consistent with the real world.
Answer: D

Question No: 48
A central authority determines what subjects can have access to certain objects based on the organizational security policy is called:
A. Mandatory Access Control
B. Discretionary Access Control
C. Non-Discretionary Access Control
D. Rule-based Access control
Answer: C

Question No: 49
What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?
A. Authentication
B. Identification
C. Authorization
D. Confidentiality
Answer: B

Question No: 50
Which one of the following factors is NOT one on which Authentication is based?
A. Type 1 Something you know, such as a PIN or password
B. Type 2 Something you have, such as an ATM card or smart card
C. Type 3 Something you are (based upon one or more intrinsic physical or behavioral traits), such as a fingerprint or retina scan
D. Type 4 Something you are, such as a system administrator or security administrator
Answer: D

Question No: 51
A central authority determines what subjects can have access to certain objects based on the organizational security policy is called:
A. Mandatory Access Control
B. Discretionary Access Control
C. Non-Discretionary Access Control
D. Rule-based Access control
Answer: C

Question No: 52
What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?
A. Authentication
B. Identification
C. Authorization
Question No: 53
What is called the verification that the user’s claimed identity is valid and is usually implemented through a user password at log-on time?
A. Authentication
B. Identification
C. Integrity
D. Confidentiality
Answer: A

Question No: 54
Which one of the following factors is NOT one on which Authentication is based?
A. Type 1 Something you know, such as a PIN or password
B. Type 2 Something you have, such as an ATM card or smart card
C. Type 3 Something you are (based upon one or more intrinsic physical or behavioral traits), such as a fingerprint or retina scan
D. Type 4 Something you are, such as a system administrator or security administrator
Answer: D

Question No: 55
The act of requiring two of the three factors to be used in the authentication process refers to:
A. Two-Factor Authentication
B. One-Factor Authentication
C. Bi-Factor Authentication
D. Double Authentication
Answer: A

Question No: 56
Which type of password provides maximum security because a new password is required for each new log-on?
A. One-time or dynamic password
B. Cognitive password
C. Static password
D. Passphrase
Answer: A

Question No: 57
What is called a password that is the same for each log-on session?
A. “one-time password”
B. “two-time password”
C. static password
D. dynamic password
Question No: 58
What is called a sequence of characters that is usually longer than the allotted number for a password?
A. passphrase
B. cognitive phrase
C. anticipated phrase
D. Real phrase
Answer: A

Question No: 59
Which best describes a tool (i.e. keyfob, calculator, memory card or smart card) used to supply dynamic passwords?
A. Tickets
B. Tokens
C. Token passing networks
D. Coupons
Answer: B

Question No: 60
Which of the following would be true about Static password tokens?
A. The owner identity is authenticated by the token
B. The owner will never be authenticated by the token.
C. The owner will authenticate himself to the system.
D. The token does not authenticates the token owner but the system.
Answer: A

Question No: 61
In Synchronous dynamic password tokens:
A. The token generates a new password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
B. The token generates a new non-unique password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
C. The unique password is not entered into a system or workstation along with an owner’s PIN.
D. 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.
Answer: B

Question No: 62
In biometrics, “one-to-many” search against database of stored biometric images is done in:
A. Authentication
B. Identification
C. Identities
D. Identity-based access control
Question No: 63
Which of the following is true of biometrics?
A. It is used for identification in physical controls and it is not used in logical controls.
B. It is used for authentication in physical controls and for identification in logical controls.
C. It is used for identification in physical controls and for authentication in logical controls.
D. Biometrics has not role in logical controls.
Answer: C

Question No: 64
What is called the percentage of valid subjects that are falsely rejected by a Biometric Authentication system?
A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. True Rejection Rate (TRR) or Type III Error
Answer: A

Question No: 65
What is called the percentage of invalid subjects that are falsely accepted by a Biometric authentication system?
A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. True Acceptance Rate (TAR) or Type III Error
Answer: B

Question No: 66
What is called the percentage at which the False Rejection Rate equals the False Acceptance Rate?
A. False Rejection Rate (FRR) or Type I Error
B. False Acceptance Rate (FAR) or Type II Error
C. Crossover Error Rate (CER)
D. Failure to enroll rate (FTE or FER)
Answer: C

Question No: 67
Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?
A. Accountability of biometrics systems
B. Acceptability of biometrics systems
C. Availability of biometrics systems
D. Adaptability of biometrics systems
Answer: B

Question No: 68
Which of the following offers advantages such as the ability to use stronger passwords, easier password administration, one set of credential, and faster resource access?
A. Smart cards
B. Single Sign-On (SSO)
C. Symmetric Ciphers
D. Public Key Infrastructure (PKI)
Answer: B

Question No: 69
Which of the following describes the major disadvantage of many Single Sign-On (SSO) implementations?
A. Once an individual obtains access to the system through the initial log-on, they have access to all resources within the environment that the account has access to.
B. The initial logon process is cumbersome to discourage potential intruders.
C. Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.
D. Once a user obtains access to the system through the initial log-on, he has to logout from all other systems
Answer: A

Question No: 70
Which of the following is implemented through scripts or smart agents that replays the users multiple log-ins against authentication servers to verify a user’s identity which permit access to system services?
A. Single Sign-On
B. Dynamic Sign-On
C. Smart cards
D. Kerberos
Answer: A

Question No: 71
Which of the following is NOT true of the Kerberos protocol?
A. Only a single login is required per session.
B. The initial authentication steps are done using public key algorithm.
C. The KDC is aware of all systems in the network and is trusted by all of them
D. It performs mutual authentication
Answer: B

Question No: 72
The authenticator within Kerberos provides a requested service to the client after validating which of the following?
A. timestamp
B. client public key
C. client private key
D. server public key
Answer: A
Question No: 73
Which of the following is addressed by Kerberos?
A. Confidentiality and Integrity
B. Authentication and Availability
C. Validation and Integrity
D. Auditability and Integrity
Answer: A

Question No: 74
Kerberos is vulnerable to replay in which of the following circumstances?
A. When a private key is compromised within an allotted time window.
B. When a public key is compromised within an allotted time window.
C. When a ticket is compromised within an allotted time window.
D. When the KSD is compromised within an allotted time window.
Answer: C

Question No: 75
Like the Kerberos protocol, SESAME is also subject to which of the following?
A. timeslot replay
B. password guessing
C. symmetric key guessing
D. asymmetric key guessing
Answer: B

Question No: 76
RADIUS incorporates which of the following services?
A. Authentication server and PIN codes.
B. Authentication of clients and static passwords generation.
C. Authentication of clients and dynamic passwords generation.
D. Authentication server as well as support for Static and Dynamic passwords.
Answer: D

Question No: 77
Which of the following protects a password from eavesdroppers and supports the encryption of communication?
A. Challenge Handshake Authentication Protocol (CHAP)
B. Challenge Handshake Identification Protocol (CHIP)
C. Challenge Handshake Encryption Protocol (CHEP)
D. Challenge Handshake Substitution Protocol (CHSP)
Answer: A

Question No: 78
Which of the following represents the columns of the table in a relational database?
A. attributes
B. relation
C. record retention
D. records or tuples
Answer: A

Question No: 79
A database view is the results of which of the following operations?
A. Join and Select.
B. Join, Insert, and Project.
C. Join, Project, and Create.
D. Join, Project, and Select.
Answer: D

Question No: 80
Which of the following is used to create and modify the structure of your tables and other objects in the database?
A. SQL Data Definition Language (DDL)
B. SQL Data Manipulation Language (DML)
C. SQL Data Relational Language (DRL)
D. SQL Data Identification Language (DIL)
Answer: A

Question No: 81
Which of the following is used to monitor network traffic or to monitor host audit logs in real time to determine violations of system security policy that have taken place?
A. Intrusion Detection System
B. Compliance Validation System
C. Intrusion Management System (IMS)
D. Compliance Monitoring System
Answer: A

Question No: 82
Which of the following monitors network traffic in real time?
A. network-based IDS
B. host-based IDS
C. application-based IDS
D. firewall-based IDS
Answer: A

Question No: 83
A host-based IDS is resident on which of the following?
A. On each of the critical hosts
B. decentralized hosts
C. central hosts
D. bastion hosts
Answer: A

Question No: 84
Which of the following usually provides reliable, real-time information without consuming network or host resources?
A. network-based IDS
B. host-based IDS
C. application-based IDS
D. firewall-based IDS
Answer: A

Question No: 85
The fact that a network-based IDS reviews packets payload and headers enable which of the following?
A. Detection of denial of service
B. Detection of all viruses
C. Detection of data corruption
D. Detection of all password guessing attacks
Answer: A

Question No: 86
Which of the following reviews system and event logs to detect attacks on the host and determine if the attack was successful?
A. host-based IDS
B. firewall-based IDS
C. bastion-based IDS
D. server-based IDS
Answer: A

Question No: 87
What would be considered the biggest drawback of Host-based Intrusion Detection systems (HIDS)?
A. It can be very invasive to the host operating system
B. Monitors all processes and activities on the host system only
C. Virtually eliminates limits associated with encryption
D. They have an increased level of visibility and control compared to NIDS
Answer: A

Question No: 88
Attributes that characterize an attack are stored for reference using which of the following Intrusion Detection System (IDS)?
A. signature-based IDS
B. statistical anomaly-based IDS
C. event-based IDS
D. inherent-based IDS
Answer: A

Question No: 89
Which of the following is an issue with signature-based intrusion detection systems?
A. Only previously identified attack signatures are detected.
B. Signature databases must be augmented with inferential elements.
C. It runs only on the Windows operating system.
D. Hackers can circumvent signature evaluations.
Answer: A

Question No: 90
Which of the following is an IDS that acquires data and defines a "normal" usage profile for the network or host?
A. Statistical Anomaly-Based ID
B. Signature-Based ID
C. Dynamical Anomaly-Based ID
D. Inferential Anomaly-Based ID
Answer: A

Question No: 91
Which of the following is most relevant to determining the maximum effective cost of access control?
A. The value of information that is protected.
B. Management's perceptions regarding data importance.
C. Budget planning related to base versus incremental spending.
D. The cost to replace lost data.
Answer: A

Question No: 92
Which of the following is NOT a factor related to Access Control?
A. Integrity
B. Authenticity
C. Confidentiality
D. Availability
Answer: B

Question No: 93
Which of the following is most appropriate to notify an external user that session monitoring is being conducted?
A. Logon Banners
B. Wall poster
C. Employee Handbook
D. Written agreement
Answer: A
Question No: 94
Which of the following pairings uses technology to enforce access control policies?
A. Preventive/Administrative  
B. Preventive/Technical  
C. Preventive/Physical  
D. Detective/Administrative  
Answer: B

Question No: 95
In the course of responding to and handling an incident, you work on determining the root cause of the incident. In which step are you in?
A. Recovery  
B. Containment  
C. Triage  
D. Analysis and tracking  
Answer: D

Question No: 96
Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It does not permit management to:
A. specify what users can do  
B. specify which resources they can access  
C. specify how to restrain hackers  
D. specify what operations they can perform on a system.  
Answer: C

Question No: 97
Access Control techniques do not include which of the following choices?
A. Relevant Access Controls  
B. Discretionary Access Control  
C. Mandatory Access Control  
D. Lattice Based Access Control  
Answer: A

Question No: 98
Which of the following statements relating to the Bell-LaPadula security model is FALSE (assuming the Strong Star property is not being used)?
A. A subject is not allowed to read up.  
B. The *- property restriction can be escaped by temporarily downgrading a high level subject.  
C. A subject is not allowed to read down.  
D. It is restricted to confidentiality.  
Answer: C

Question No: 99