

Volume: 1275 Questions

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 items'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.

ISC CISSP Exam

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 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

ISC CISSP Exam

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

ISC CISSP Exam

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

ISC CISSP Exam

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.

Answer: C

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

ISC CISSP Exam

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?

ISC CISSP Exam

- 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?

ISC CISSP Exam

- 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?

ISC CISSP Exam

- 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: