

# Systems Security Certified Practitioner

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(s): D**

---

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(s): B**

---

3. What are the components of an object's sensitivity label?

A. A Classification Set and a single Compartment.

B. A single classification and a single compartment.

C. A Classification Set and user credentials.

D. A single classification and a Compartment Set.

**Answer(s): D**

---

4. What does it mean to say that sensitivity labels are "incomparable"?

A. The number of classification in the two labels is different.

B. Neither label contains all the classifications of the other.

C. the number of categories in the two labels are different.

D. Neither label contains all the categories of the other.

**Answer(s): D**

---

5. 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(s): C**

---

6. 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(s): A**

---

7. 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(s): B**

---

8. The three classic ways of authenticating yourself to the computer security software are by something you know, by something you have, and by something:

A. you need.

B. non-trivial

C. you are.

D. you can get.

**Answer(s): C**

---

9. A timely review of system access audit records would be an example of which of the basic security functions?

A. avoidance.

B. deterrence.

C. prevention.

D. detection.

**Answer(s): D**

---

**10.** 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(s): A**

---

**11.** 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(s): A**

---

**12.** Which of the following is not a logical control when implementing logical access security?

A. access profiles.

B. userids.

C. employee badges.

D. passwords.

**Answer(s): C**

---

**13.** 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(s): A**

---

**14.** 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(s): D**

---

**15.** Which of the following would assist the most in Host Based intrusion detection?

A. audit trails.

B. access control lists.

C. security clearances.

D. host-based authentication.

**Answer(s): A**

---

**16.** Controls to keep password sniffing attacks from compromising computer systems include which of the following?

A. static and recurring passwords.

B. encryption and recurring passwords.

C. one-time passwords and encryption.

D. static and one-time passwords.

**Answer(s): C**

---

**17.** Kerberos can prevent which one of the following attacks?

A. tunneling attack.

B. playback (replay) attack.

C. destructive attack.

D. process attack.

**Answer(s): B**

---

**18.** 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(s):** D

---

**19.** 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(s):** A

---

**20.** 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(s):** C

