Chapter 2: Access Control

Chapter 2 True/False Questions

1. A deny-by-default stance is less strict than an allow-by-default stance.

2. Knowledge factor authentication is also referred to as Type I authentication factor.

3. Passwords are considered weaker than passphrases.

4. Smart cards are less expensive to implement than memory cards.

5. Retina scans have a higher accuracy than any other biometric scan.

6. Type I errors are more dangerous than Type II errors.

7. When considering FAR, FRR, and CER, smaller values are better.

8. Content-dependent access control is based on subject or object attributes or environmental characteristics.

9. A network-based IDS is the most common IDS and monitors network traffic on a local network segment.

10. Pharming and phishing are password attacks.

Chapter 2 Multiple Choice Questions

1. Which concept ensures that data is protected from unauthorized modification or data corruption?

A. Confidentiality

B. Integrity

C. Availability

D. Identification

2. Which of the following is an example of three-factor authentication?

A. Username, password, smart card

B. Password, smart card, PIN

C. Password, smart card, iris scan

D. Smart card, iris scan, keystroke dynamics

3. Of the options given, which biometric consideration is MOST important?

A. FAR

B. Enrollment time

C. Throughput rate

D. FRR

4. What defines the method for identifying and authenticating users and the level of access that is granted to users?

A. Least privilege

B. Dual controls

C. Separation of duties

D. Access control policy

5. Which accountability mechanism reviews facility and perimeter protections?

A. Physical vulnerability assessment

B. Personnel vulnerability assessment

C. Clipping level

D. Blind test

6. In which access control category do fire extinguishers fall?

A. Detective

B. Corrective

C. Preventive

D. Compensative

7. Which of the following are physical access controls?

A. Security policies

B. Baselines

C. Badges

D. Audit trails

8. In which access control model is all that is not expressly permitted is forbidden?

A. MAC

B. RBAC

C. Rule-based access control

D. DAC

9. Which type of IDS analyzes traffic and compares it to normal traffic to determine whether said traffic is a threat?

A. Anomaly-based

B. Signature-based

C. Rule-based

D. Pattern-matching

10. Which malicious software collects private user data?

A. Virus

B. Spyware

C. Worm

D. Trojan horse

Chapter 2 True/False Answers

1. False A deny-by-default stance is stricter than an allow-by-default stance.

2. True Knowledge factor authentication is also referred to as Type I authentication factor.

3. True Passwords are considered weaker than passphrases.

4. False Smart cards are more expensive to implement than memory cards.

5. False Iris scans have a higher accuracy than any other biometric scan.

6. **False** Type II errors are more dangerous than Type I errors.

7. **True** When considering FAR, FRR, and CER, smaller values are better.

8. **False** Content-dependent access control makes access decisions based on the data contained within the object. Context-dependent access control is based on subject or object attributes or environmental characteristics.

9. **True** A network-based IDS is the most common IDS and monitors network traffic on a local network segment.

10. False Pharming and phishing are social engineering attacks, not password attacks. Brute force attacks and dictionary attacks are password attacks.

Chapter 2 Multiple Choice Answers

1. B integrity

2. C Password, smart card, and iris scan - These are the only options that include something you know, something you have, and something you are.

3. A FAR

4. D Access control policy

5. A Physical vulnerability assessment

6. B Corrective

7. C Badges

8. D DAC

9. A Anomaly-based

10. B Spyware