Chapter 2: Access controls

MULTIPLE CHOICE

1. An information system that processes sensitive information is configured to require a valid userid and strong password from any user. This process of accepting and validating this information is known as:
   a. Authentication
   b. Strong authentication
   c. Two factor authentication
   d. Single sign-on

   ANS: A PTS: 1

2. The reason that two-factor authentication is preferable over ordinary authentication is:
   a. Two-factor authentication is more difficult to crack
   b. It relies upon something the user knows
   c. It relies upon something that the user has
   d. Two-factor authentication uses stronger encryption algorithms

   ANS: C PTS: 1

3. When an information system authenticates a user based on "what the user is", this refers to the use of:
   a. Authorization based upon the user's job title
   b. Role based authentication
   c. Two factor authentication
   d. Biometric authentication

   ANS: D PTS: 1

4. In an information system that authenticates users based on userid and password, the primary reason for storing a hash of the password instead of storing the encrypted password is:
   a. No one, even system administrators, can derive the password
   b. Hashing algorithms are less CPU intensive than encryption algorithms
   c. Hashed passwords require less storage space than encrypted passwords
   d. Support personnel can more easily reset a user's password when it is hashed

   ANS: A PTS: 1

5. The primary reason why users are told to use strong passwords is NOT:

a. It is more difficult to “shoulder surf” a strong password because of the additional keystrokes
b. Strong passwords are more difficult for others to guess
c. Weak passwords are susceptible to dictionary attacks
d. Passwords based on easily-discovered facts such as birthdays, spouse and pet names are easily guessed

ANS: A PTS: 1

6. One disadvantage of the use of digital certificates as a means for two-factor authentication is NOT:
a. Digital certificates may not be portable across different types of machines
b. The password used to unlock the certificate may be weak and easily guessed
c. It may be possible to steal the certificate and use it on another computer
d. A digital certificate can theoretically be copied, unlike tokens and smart cards which are not easily cloned

ANS: A PTS: 1

7. A smart card is a good form of two-factor authentication because:
a. It contains a certificate on a microchip that is resistant to cloning or cracking
b. It can double as a proximity card for building entrance key card systems
c. It does not rely on internal power like a token
d. A smart card is portable and can be loaned to others

ANS: A PTS: 1

8. Organizations that implement two-factor authentication often do not adequately plan. One result of this is:
a. Some users will lose their tokens, smart cards, or USB keys
b. Some users will store their tokens, smart cards, or USB keys with their computers, thereby defeating one of the advantages of two-factor authentication
c. Users will have trouble understanding how to use two-factor authentication
d. The cost of implementation and support can easily exceed the cost of the product itself

ANS: D PTS: 1

9. Palm scan, fingerprint scan, and iris scan are forms of:
a. Strong authentication
c. Biometric authentication

b. Two-factor authentication

d. Single sign-on

ANS: C PTS: 1

10. A biometric authentication system that incorporates the results of newer scans into a user's profile is less likely to:
    a. Have a lower False Accept Rate
    b. Reject future authentication attempts as the user's biometrics slowly change over time
    c. Correctly identify and authenticate users
    d. Reject an impostor

    ANS: B PTS: 1

11. The use of retina scanning as a biometric authentication method has not gained favor because:
    a. It is inconvenient to use retina scanning in a darkened room
    b. Many users cannot hold their eye open long enough for a scan to complete
    c. Users are uncomfortable holding their eye very near the biometric scanning device
    d. The human retina changes significantly over time

    ANS: C PTS: 1

12. Voice recognition as a biometric authentication method is difficult to measure because:
    a. Many factors including current health and respiration rate make sampling difficult
    b. Computers are not yet fast enough to adequately sample a voice print
    c. Voice recognition does not handle accents well
    d. Impatience changes voice patterns, which leads to increased False Reject Rates

    ANS: A PTS: 1

13. Which of the following statements about Crossover Error Rate (CER) is true:
    a. This is the point where the False Accept Rate falls below 50%
    b. This is the point where the False Reject Rate falls below 50%
    c. This is the point where False Reject Rate and False Accept Rate add to 100%
    d. This is the point where False Reject Rate and False Accept Rate are equal

    ANS: D PTS: 1

14. A security engineer has recently installed a biometric system, and needs to tune it. Currently the biometric system is rejecting too many valid, registered users. What adjustment does the security engineer need to make?

a. Increase the False Accept Rate
b. Reduce the False Accept Rate
c. Increase the False Reject Rate
d. Reduce the False Reject Rate

ANS: D PTS: 1

15. A security engineer is soliciting bids for a software product that will perform centralized authentication. The engineer has found two products so far: one that is based on LDAP and one that is based on TACACS. Which of the following statements is the best approach?

a. Select the LDAP based product
b. Do not consider the TACACS based product, consider the LDAP based product, and continue looking for other products
c. Select the TACACS based product
d. Consider the TACACS based product, and continue looking for other products based on TACACS

ANS: B PTS: 1

16. Which of the following is NOT an authentication protocol:

a. Lightweight Directory Authentication Protocol
b. Diameter
c. RADIUS
d. Lightweight Directory Access Protocol

ANS: A PTS: 1

17. An intruder wishes to break in to an application in order to steal information stored there. Because the application utilizes strong authentication, what is the most likely approach the intruder will take?

a. Dictionary attack
b. Malicious code attack
c. Application bypass attack
d. Password guessing attack

ANS: C PTS: 1

18. Authentication, encryption, and ACL's are examples of:

a. Defense in depth
b. Detective controls
c. Administrative controls
d. Technical controls

ANS: D PTS: 1

19. The categories of controls are:
    a. Detective, deterrent, preventive, corrective, recovery, and compensating
    b. Detective, preventive, and deterrent
    c. Technical, logical, and physical
    d. Detective, preventive, recovery, and compensating

    ANS: A PTS: 1

20. Video surveillance is an example of what type(s) of control:
    a. Detective and deterrent
    b. Detective only
    c. Deterrent only
    d. Preventive

    ANS: A PTS: 1

21. Buffer overflow, SQL injection, and stack smashing are examples of:
    a. Vulnerabilities
    b. Exploits
    c. Input attacks
    d. Injection attacks

    ANS: C PTS: 1

22. An organization is surplussing its old desktop computers. Being concerned with data remanence, what measures should the organization take first?
    a. Erase the hard drives
    b. Format the hard drives
    c. Activate its TEMPEST shielding
    d. Clear the computers' RAM

    ANS: A PTS: 1

23. What is the best defense against social engineering?
    a. Spyware filters
    b. Firewalls
    c. Data leakage protection (DLP)
    d. Security awareness training

    ANS: D PTS: 1

24. Signs, guards, guard dogs, and visible notices are examples of:
    a. Administrative controls
    b. Preventive controls
    c. Deterrent controls
    d. Detective controls

    ANS: C PTS: 1

25. The reason why preventive controls are preferred over detective controls is:

a. Preventive controls are less costly
b. Detective controls do not actually stop unwanted activity
c. Detective controls require more resources
d. Preventive controls are do not detect unwanted activity

ANS: B PTS: 1