**Chapter 10 Review Questions**

1. Each of the following is a type of authentication credential except \_\_\_\_\_\_\_.

a. what you have

b. what you are

c. what you discover – PG367

d. what you know

2. Which of the following is not a reason users create weak passwords?

a. A lengthy and complex password can be difficult to memorize.

b. A security policy requires a password to be changed regularly.

c. Having multiple passwords makes it hard to remember all of them.

d. Most sites force users to create weak passwords although they do not want to. – PG369

3. Which of the following attacks on passwords requires the attacker to have physical access to the computer to insert a USB flash drive?

a. Resetting – PG369

b. Capturing

c. Social engineering

d. Online guessing

4. What is a hybrid attack?

a. An attack that combines a dictionary attack with an online guessing attack

b. A brute force attack that uses special tables

c. An attack that slightly alters dictionary words – PG371

d. An attack that uses both automated and user input

5. Each of the following is a step in creating a strong password except \_\_\_\_\_\_.

a. use a short password so the computer can process it more quickly – PG372

b. avoid using phonetic words

c. do not use sequences

d. do not use personal information

6. A token code is valid \_\_\_\_\_\_.

a. for as long as it appears on the device – PG375

b. for up to one hour

c. only for the user who possesses the device

d. if it is longer than eight characters

7. A token system that requires the user to enter the code along with a PIN is called a \_\_\_\_\_\_\_.

a. single-factor authentication system

b. dual-prong verification system

c. multifactor authentication system – PG377

d. token-passing authentication system

8. A \_\_\_\_\_\_\_ is a U.S. Department of Defense (DoD) smart card that is used for identification for active-duty and reserve military personnel.

a. Personal Identity Verification (PIV) card

b. Government Smart Card (GSC)

c. Secure ID Card (SIDC)

d. Common Access Card (CAC) – PG378

9. Keystroke dynamics is an example of \_\_\_\_\_\_\_ biometrics.

a. resource

b. cognitive

c. adaptive

d. behavioral – PG379

10. Creating a pattern of when and from where a user accesses a remote Web account is an example of \_\_\_\_\_\_\_\_.

a. Time-Location Resource Monitoring (TLRM)

b. keystroke dynamics

c. cognitive biometrics

d. computer footprinting – PG381

11. \_\_\_\_\_\_\_ is a decentralized open source FIM that does not require specific software to be installed on the desktop.

a. SSO Login Resource (SSO-LR)

b. Windows CardSpace

c. OpenID – PG384

d. Windows Live ID

12. Which of the following human characteristics cannot be used for biometric identification?

a. face

b. weight – PG384

c. fingerprint

d. retina

13. \_\_\_\_\_\_\_\_\_ biometrics is related to the perception, thought processes, and under-

standing of the user.

a. Standard

b. Intelligent

c. Behavioral

d. Cognitive – PG381

14. Using one authentication credential to access multiple accounts or applications is known as \_\_\_\_\_\_\_.

a. credentialization

b. identification authentication

c. single sign-on – PG32

d. federal login

15. A disadvantage of biometric readers is \_\_\_\_\_\_\_

a. speed

b. size

c. cost – PG379

d. standards

16. Which single sign-on (SSO) technology depends on tokens?

a. OAuth – PG385

b. CardSpace

c. OpenID

d. All SSO technologies use tokens.

17. Why should the account lockout threshold not be set too low?

a. It could decrease calls to the help desk.

b. Because the network administrator would then have to manually reset the account.

c. So the user would not have to wait too long to have their password reset.

d. It could result in denial of service (DoS) attacks. – PG387

18. Which of the following is not a flaw in standard operating systems?

a. Operating systems by default use the principle of least privilege. – PG387

b. Operating systems are complex programs with millions of lines of code that make vulnerabilities extremely difficult to recognize.

c. Operating systems do not isolate applications from each another, so one application that is compromised can impact the entire computer.

d. Operating systems cannot create a trusted path between users and applications.

19. An operating system that is designed to be secure by controlling critical parts of it to limit access from attackers and administrators is a .

a. secure OS

b. trustworthy OS

c. managed OS

d. trusted OS – PG388

20. Which technique would prevent an attacker from China from logging into a user’s account at 4:00 AM?

a. Computer footprinting – PG381

b. OpenAuthorization

c. Cognitive biometrics

d. Internet Throttling"