Physical and Biometric security

I. Multiple choice questions

1. Which of the following is the verification of a person's identity?

A. Authorization
B. Accountability
C. Authentication
D. Password

2. Which of the following would fall into the category of "something a person Is"?

A. Passwords
B. Passphrases
C. Fingerprints
D. Smart cards

3. Which of the following are good practices for tracking user identities? (Select the two best answers.)

A. Video cameras, Key card door access systems
B. Key card door access systems, Sign-in sheets
C. Sign-in sheets, Security guards
D. Security guards, Video cameras

4. What are two examples of common single sign-on authentication configurations? (Select the two best answers.)

A. Biometrics-based, Smart card-based
B. Multifactor authentication, Biometrics-based
C. Kerberos-based, Multifactor authentication
D. Smart card-based, Kerberos-based

5. Which of the following is an example of two-factor authentication?

A. L2TP and Ipsec
B. Username and password
C. Thumbprint and key card
D. Client and server

6. What is the main purpose of a physical access log?

A. To enable authorized employee access
B. To show who exited the facility
C. To show who entered the facility
D. To prevent unauthorized employee access

7. Which of the following is not a common criteria when authenticating users?

A. Something you do
B. Something you are
C. Something you know
D. Something you like

8. Of the following, what two authentication mechanisms require something you physically possess? (Select the two best answers.)

A. Smart card, USB flash drive
B. Certificate, USB flash drive
C. USB flash drive, Username and password
D. Username and password, Smart card

9. Which of the following is the final step a user needs to take before that user can access domain resources?

A. Verification
B. Validation
C. Authorization
D. Authentication

10. To gain access to your network, users must provide a thumbprint and a username and password. What type of authentication model is this?

A. Biometrics
B. Domain logon
C. Multifactor
D. Single sign-on

11. The IT director has asked you to set up an authentication model in which users can enter their credentials one time, yet still access multiple server resources. What type of authentication model should you implement?

A. Smart card and biometrics
B. Three-factor authentication
C. SSO
D. VPN

12. Two items are needed before a user can be given access to the network. What are these two items?

A. Authentication and authorization
B. Authorization and identification
C. Identification and authentication
D. Password and authentication

13. Before gaining access to the data center, you must swipe your finger on a device. What type of authentication is this?

A. Biometrics
B. Single sign-on
C. Multifactor
D. Tokens

14. Your organization provides to its employees badges that are encoded with a private encryption key and specific personal information. The encoding is used to provide access to the organization's network. What type of authentication method is being used?

A. Token
B. Biometrics
C. Kerberos
D. Smart card

II. Discussion question

What are the advantages and disadvantages of each type of biometric security?

Sample answer

a. Advantages of Fingerprint Biometrics

Fingerprint pattern stable throughout the lifetime

Fingerprints are unique in nature

It is easily analyzed and compare

Inexpensive device

Oldest form of biometrics

b. Limitations of Fingerprint Biometrics

Wet or moist fingers, cut fingers, or dirt or grease can sometimes affect the authentication process.

It is not right tool for those persons who working in chemical labs.

III. PROJECTS/EXERCISES

1. Discussion Questions

A. Discussion Question 1

What do you think is the single greatest physical threat to information systems? Fire? Hurricanes? Sabotage? Terrorism? Discuss this question as a group. Be prepared to support your answer.

B. Discussion Question 2

Have you ever been in a building when the fire alarm sounded and most people didn't react to it at all? How do you typically react in such situations? If workers do not respond to an alarm, what does that say about the corporate culture within that workplace? What role can IT professionals play in making people make more responsible decisions about their own safety? Discuss these issues as a group.

2. **Web Projects**

A. Web Project 1

Visit the web sites of local real estate agencies and developers. Look for listings of commercial buildings that might be suitable for use as a secure data center. Compare several listings, and choose the one you think is best. Share your findings with the class.

B. Web Project 2

Search for the web site of a company that provides security dog services to businesses. Read the site's information carefully. Does the company say what it will do if a dog bites or attacks an innocent person, such as a worker who accidentally wanders into a guarded area?

C. Web Project 3

Go online and search for information about smart cards. As you learned in this chapter, several types of smart cards are available. Try to find information about each type of card and its applications. What type of card, in your view, is best suited for use as a secure-access tool? Be prepared to explain your conclusions.

D. Web Project 4

Go online and search for information on biometric security systems for individual computers. For example, small biometric devices can be added to notebook PCs, and ensure that only the computer's authorized user can access the system. Based on your research, would you purchase such a security device for your own computer? Why or why not? Summarize your findings in a brief report, to share with the class.

WEB RESOURCES

- http://www.biometricsinstitute.org/pages/types-of-biometrics.html Information about various types of biometric devices

- http://resources.infosecinstitute.com/physical-security-managing-intruder/ Article discussing various types of physical security controls

- https://www.sans.edu/cyber-research/ Article discussing physical security controls (#281)