|  |
| --- |
| **True / False** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. Voice recognition is identical to speech recognition.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2. Passwords provide strong protection.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3. Most password attacks today are an offline attack.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 4. Brute force attacks can be very slow because every character combination must be generated.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5. Hash algorithms like MD5 and SHA are considered secure for creating digests because these hashing algorithms are designed to create a digest as strong as possible.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 6. A hardware security token is typically a small device with a window display.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7. A TOTP changes after a set period.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 8. A retina scanner has become the most common type of standard biometrics.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 9. Keystroke dynamics uses two unique typing variables.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 10. Open ID Connect is an Authentication protocol that can be used in OAuth 2.0 as a standard means to obtain user identity.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |
| --- |
| **Multiple Choice** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. A secret combination of letters, numbers, and/or characters that only the user should have knowledge of, is known as a:   |  |  |  | | --- | --- | --- | |  | a. | token | |  | b. | password | |  | c. | biometric detail | |  | d. | challenge | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. What is the main weakness associated with the use of passwords?   |  |  |  | | --- | --- | --- | |  | a. | human memory | |  | b. | encryption technology | |  | c. | handshake technology | |  | d. | human reliability | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. What type of attack involves using every possible combination of letters, numbers, and characters to create candidate digests that are then matched against those in a stolen digest file?   |  |  |  | | --- | --- | --- | |  | a. | Space division | |  | b. | Brute force | |  | c. | Known ciphertext | |  | d. | Known plaintext | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. What variation of a dictionary attack involves a dictionary attack combined with a brute force attack, and will slightly alter dictionary words by adding numbers to the end of the password, spelling words backward, slightly misspelling words, or including special characters?   |  |  |  | | --- | --- | --- | |  | a. | brute force | |  | b. | hash replay | |  | c. | network replay | |  | d. | hybrid | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. The use of what item below involves the creation of a large pre-generated data set of candidate digests?   |  |  |  | | --- | --- | --- | |  | a. | rainbow tables | |  | b. | randomized character list | |  | c. | word list | |  | d. | cascade tables | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. What kind of biometrics utilizes a person's unique physical characteristics for authentication, such as fingerprints or unique characteristics of a person's face?   |  |  |  | | --- | --- | --- | |  | a. | cognitive biometrics | |  | b. | reactive biometrics | |  | c. | standard biometrics | |  | d. | physical biometrics | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. Which term below describes the time it takes for a key to be pressed and then released?   |  |  |  | | --- | --- | --- | |  | a. | dwell time | |  | b. | lead time | |  | c. | sync time | |  | d. | react time | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. Which type of biometrics is based on the perception, thought process, and understanding of the user?   |  |  |  | | --- | --- | --- | |  | a. | cognitive biometrics | |  | b. | reactive biometrics | |  | c. | standard biometrics | |  | d. | physical biometrics | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. The use of a single authentication credential that is shared across multiple networks is called:   |  |  |  | | --- | --- | --- | |  | a. | access management | |  | b. | authorization management | |  | c. | identity management | |  | d. | risk management | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. The use of one authentication credential to access multiple accounts or applications is referred to as which of the following?   |  |  |  | | --- | --- | --- | |  | a. | individual Sign On | |  | b. | single Sign On | |  | c. | unilateral Sign On | |  | d. | federated Sign On | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. What technology is an open source federation framework and supports the development of authorization protocols?   |  |  |  | | --- | --- | --- | |  | a. | Shibboleth | |  | b. | OAuth | |  | c. | SAML | |  | d. | Kerberos | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. What federation system technology uses federation standards to provide SSO and exchanging attributes?   |  |  |  | | --- | --- | --- | |  | a. | OAuth | |  | b. | Open ID Connect | |  | c. | Windows Live ID | |  | d. | Shibboleth | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. What federated identity management (FIM) relies on token credentials?   |  |  |  | | --- | --- | --- | |  | a. | OAuth | |  | b. | OpenID | |  | c. | Shibboleth | |  | d. | OpenPass | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. A U.S. Department of Defense (DoD) smart card that is used for identification of active-duty and reserve military personnel along with civilian employees and special contractors is called:   |  |  |  | | --- | --- | --- | |  | a. | Common Access Card (CAC) | |  | b. | Identity Validation Card (IVC) | |  | c. | Credential Validation Card (CVC) | |  | d. | Personal Credential Card (PCC) | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. What can be used to increase the strength of hashed passwords?   |  |  |  | | --- | --- | --- | |  | a. | salt | |  | b. | key stretching | |  | c. | double hashing | |  | d. | single crypting | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. A list of the available nonkeyboard characters can be seen in Windows by opening what utility?   |  |  |  | | --- | --- | --- | |  | a. | charmap.exe | |  | b. | charlist.exe | |  | c. | chardump.exe | |  | d. | listchar.exe | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. What type of attack conducts a statistical analysis of the stolen passwords that is then used to create a mask to break the largest number of passwords?   |  |  |  | | --- | --- | --- | |  | a. | character set attack | |  | b. | binary attack | |  | c. | mask attack | |  | d. | rule attack | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. If a user has more than one type of authentication credential, what type of authentication is being used?   |  |  |  | | --- | --- | --- | |  | a. | pattern authentication | |  | b. | verified authentication | |  | c. | multifactor authentication | |  | d. | token authentication | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. What type of authentication is based on what the user has?   |  |  |  | | --- | --- | --- | |  | a. | software token | |  | b. | hardware token | |  | c. | security token | |  | d. | identity token | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. What type of card contains an integrated circuit chip that can hold information, which then can be used as part of the authentication process?   |  |  |  | | --- | --- | --- | |  | a. | smart card | |  | b. | SIM card | |  | c. | E-card | |  | d. | BioCard | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. Which of the following is NOT a valid biometric disadvantage?   |  |  |  | | --- | --- | --- | |  | a. | crossover error rate | |  | b. | false acceptance rate | |  | c. | false error rate | |  | d. | false rejection rate | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. What option below represents an example of behavioral biometrics?   |  |  |  | | --- | --- | --- | |  | a. | user dynamics | |  | b. | keystroke dynamics | |  | c. | facial recognition | |  | d. | fingerprint recognition | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What specific type of authentication can be based on where the user is located?   |  |  |  | | --- | --- | --- | |  | a. | GPS | |  | b. | somewhere locating | |  | c. | geocache | |  | d. | geolocation | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. Which of the following account lockout policy settings determines the number of failed login attempts before a lockout occurs?   |  |  |  | | --- | --- | --- | |  | a. | system lockout threshold | |  | b. | account lockout threshold | |  | c. | administrator lockout threshold | |  | d. | user lockout threshold | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. What term best describes managing the login credentials such as passwords in user accounts?   |  |  |  | | --- | --- | --- | |  | a. | account management | |  | b. | user management | |  | c. | credential management | |  | d. | password management | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. Which of the following options prevents a logon after a set number of failed logon attempts within a specified period and can also specify the length of time that the lockout is in force?   |  |  |  | | --- | --- | --- | |  | a. | password lock | |  | b. | logon lock | |  | c. | password lockout | |  | d. | logon lockout | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. Which of the following accounts is a user account that is created explicitly to provide a security context for services running on a server?   |  |  |  | | --- | --- | --- | |  | a. | service account | |  | b. | shared account | |  | c. | system account | |  | d. | privileged account | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. Which of the following is a is a two-way relationship that is automatically created between parent and child domains in a Microsoft Active Directory forest?   |  |  |  | | --- | --- | --- | |  | a. | double trust | |  | b. | federated trust | |  | c. | transitive trust | |  | d. | domain trust | |

|  |
| --- |
| **Multiple Response** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. Which of the following is a category of group password settings in Microsoft Windows? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | Password Policy Settings | |  | b. | Account Policy Settings | |  | c. | Password Lockout Policy | |  | d. | Account Lockout Policy | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. Which of the following are key stretching password hash algorithms? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | bcrypt | |  | b. | PBKDF2 | |  | c. | seq02 | |  | d. | SHA-256 | |

|  |
| --- |
| **Subjective Short Answer** |

|  |
| --- |
| 41. What is a dictionary attack? |

|  |
| --- |
| 42. Why do passwords place a heavy load on human memory? |

|  |
| --- |
| 43. Discuss the types of shortcuts that users take to help them recall their passwords. |

|  |
| --- |
| 44. Describe how rainbow tables work. |

|  |
| --- |
| 45. What are the three advantages of a rainbow table over other password attacks? |

|  |
| --- |
| 46. What is the difference between multifactor authentication and single-factor authentication? |

|  |
| --- |
| 47. Why should account passwords be disabled instead of the account being immediately deleted? |

|  |
| --- |
| 48. How does an iris scanner work? |

|  |
| --- |
| 49. How does a retina scanner work? |

|  |
| --- |
| 50. What smartcard standard is used to cover all U.S. government employees? |