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

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

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

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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | False | |

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

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

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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |
| --- |
| **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 |  |  |  | | --- | --- | | *ANSWER:* | b | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | b | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | d | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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) |  |  |  | | --- | --- | | *ANSWER:* | a | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

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

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |
| --- |
| **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 |  |  |  | | --- | --- | | *ANSWER:* | a, d | |

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

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

|  |  |  |
| --- | --- | --- |
| 41. What is a dictionary attack?   |  |  | | --- | --- | | *ANSWER:* | A dictionary attack begins with the attacker creating digests of common dictionary words as candidates and then comparing them against those in a stolen digest file. Dictionary attacks can be successful because users often create passwords that are simple dictionary words. | |

|  |  |  |
| --- | --- | --- |
| 42. Why do passwords place a heavy load on human memory?   |  |  | | --- | --- | | *ANSWER:* | First, long and complex passwords (the most effective ones) can be difficult to memorize and can strain our ability to accurately recall them. Most users have difficulty remembering these types of strong passwords. Second, users today must remember passwords for many different accounts. Most users have accounts for different computers at work, school, and home, multiple e-mail accounts, plus online banking and Internet site accounts. | |

|  |  |  |
| --- | --- | --- |
| 43. Discuss the types of shortcuts that users take to help them recall their passwords.   |  |  | | --- | --- | | *ANSWER:* | Because of the burdens that passwords place on human memory, users take shortcuts to help them memorize and recall their passwords. One shortcut is to create and use a weak password. Weak passwords use a common word as a password (princess), a short password (desk), a predictable sequence of characters (abc123), or personal information (Hannah) in a password. Even when users attempt to create stronger passwords, they generally follow predictable patterns. | |

|  |  |  |
| --- | --- | --- |
| 44. Describe how rainbow tables work.   |  |  | | --- | --- | | *ANSWER:* | Rainbow tables make password attacks easier by creating a large pre-generated data set of encrypted passwords. There are two steps to using rainbow tables. First is creating the table itself. Next, that table is used to crack a password. A rainbow table is a compressed representation of plaintext passwords that are related and organized in a sequence (called a chain). To create a rainbow table, each chain begins with an initial password that is encrypted, and then that is fed into a function that produces a different plaintext password. This process is repeated for a set number of rounds. The initial password and the last encrypted value of the chain comprise a rainbow table entry. | |
| 45. What are the three advantages of a rainbow table over other password attacks?   |  |  | | --- | --- | | *ANSWER:* | A rainbow table can be used repeatedly for attacks on other passwords. Rainbow tables are much faster than dictionary attacks. The amount of memory needed on the attacking machine is greatly reduced. | |

|  |  |  |
| --- | --- | --- |
| 46. What is the difference between multifactor authentication and single-factor authentication?   |  |  | | --- | --- | | *ANSWER:* | Multifactor authentication uses multiple types of authentication credentials, such as what a user knows and what a user has, whereas single-factor authentication uses only one type of authentication. | |

|  |  |  |
| --- | --- | --- |
| 47. Why should account passwords be disabled instead of the account being immediately deleted?   |  |  | | --- | --- | | *ANSWER:* | Account passwords should be disabled (made inactive) instead of the account being immediately deleted. This serves to create an audit trail to conform with compliance issues, and also makes the reestablishment of an account easier if it becomes necessary. | |

|  |  |  |
| --- | --- | --- |
| 48. How does an iris scanner work?   |  |  | | --- | --- | | *ANSWER:* | An iris scanner, which can use a standard computer webcam, uses the unique characteristic of the iris, which is a thin, circular structure in the eye. Iris recognition identifies the unique random patterns in an iris for authentication. | |

|  |  |  |
| --- | --- | --- |
| 49. How does a retina scanner work?   |  |  | | --- | --- | | *ANSWER:* | A retinal scanner uses the human retina as a biometric identifier. The retina is a layer at the back (posterior) portion of the eyeball that contains cells sensitive to light, which trigger nerve impulses that pass these through the optic nerve to the brain, where a visual image is formed. Due to the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. | |

|  |  |  |
| --- | --- | --- |
| 50. What smartcard standard is used to cover all U.S. government employees?   |  |  | | --- | --- | | *ANSWER:* | The smart card standard covering all U.S. government employees is the Personal Identity Verification (PIV) standard. | |