Chapter 11

1. Which authentication factor is based on a unique talent that a user possesses?
2. What you have
3. What you are
4. **What you do**
5. What you know
6. Which of these is NOT a characteristic of a weak password?
7. A common dictionary word
8. **A long password**
9. Using personal information
10. Using a predictable sequence of characters
11. Each of the following accounts should be prohibited EXCEPT:
12. Shared accounts
13. Generic accounts
14. **Privileged accounts**
15. Guest accounts
16. Ilya has been asked to recommend a federation system technology that is an open source federation framework that can support the development of authorization protocols. Which of these technologies would he recommend?
17. **OAuth**
18. Open ID Connect
19. Shibboleth
20. NTLM
21. How is key stretching effective in resisting password attacks?
22. **It takes more time to generate candidate password digests**.
23. It requires the use of GPUs.
24. It does not require the use of salts.
25. The license fees are very expensive to purchase and use it.
26. Which of these is NOT a reason why users create weak passwords?
27. A lengthy and complex password can be difficult to memorize.
28. A security policy requires a password to be changed regularly.
29. Having multiple passwords makes it hard to remember all of them.
30. **Most sites force users to create weak passwords even though they do not want to**.
31. What is a hybrid attack?
32. An attack that uses both automated and user input
33. **An attack that combines a dictionary attack with a mask attack**
34. A brute force attack that uses special tables
35. An attack that slightly alters dictionary words
36. A TOTP token code is generally valid for what period of time?
37. Only while the user presses SEND
38. **For as long as it appears on the device**
39. For up to 24 hours
40. Until an event occurs
41. What is a token system that requires the user to enter the code along with a PIN called?
42. Single-factor authentication system
43. Token-passing authentication system
44. Dual-prong verification system
45. **Multifactor authentication system**
46. Which of these is a U.S. Department of Defense (DoD) smart card that is used for identification of active-duty and reserve military personnel?
47. Personal Identity Verification (PIV) card
48. Secure ID Card (SIDC)
49. **Common Access Card (CAC)**
50. Government Smart Card (GSC)
51. Which of the following should NOT be stored in a secure password database?
52. Iterations
53. Password digest
54. Salt
55. **Plaintext password**
56. Creating a pattern of where a user accesses a remote web account is an example of which of the following?
57. Keystroke dynamics
58. **Geolocation**
59. Time-Location Resource Monitoring (TLRM)
60. Cognitive biometrics
61. Timur was making a presentation regarding how attackers break passwords. His presentation demonstrated the attack technique that is the slowest yet most thorough attack that is used against passwords. Which of these password attacks did he demonstrate?
62. Dictionary attack
63. Hybrid attack
64. Custom attack
65. **Brute force attack**
66. Which human characteristic is NOT used for biometric identification?
67. Retina
68. Iris
69. **Height**
70. Fingerprint
71. \_\_\_\_\_ biometrics is related to the perception, thought processes, and understanding of the user.
72. **Cognitive**
73. Standard
74. Intelligent
75. Behavioral
76. Using one authentication credential to access multiple accounts or applications is known as \_\_\_\_\_.
77. **single sign-on**
78. credentialization
79. identification authentication
80. federal login
81. What is a disadvantage of biometric readers?
82. Speed
83. **Cost**
84. Weight
85. Standards
86. Which type of password attack is a more targeted brute force attack that uses placeholders for characters in certain positions of the password?
87. Rainbow attack
88. **Mask attack**
89. Rule attack
90. Pass the hash attack
91. Why should the account lockout threshold not be set too low?
92. It could decrease calls to the help desk.
93. The network administrator would have to reset the account manually.
94. The user would not have to wait too long to have her password reset.
95. **It could result in denial of service (DoS) attacks**.
96. Which one-time password is event-driven?
97. **HOTP**
98. TOTP
99. ROTP
100. POTP