Chapter 12

1. What is the current version of TACACS?
2. XTACACS
3. **TACACS+**
4. TACACS v9
5. TRACACS
6. How is the Security Assertion Markup Language (SAML) used?
7. **It allows secure web domains to exchange user authentication and authorization data.**
8. It is a backup to a RADIUS server.
9. It is an authenticator in IEEE 802.1x.
10. It is no longer used because it has been replaced by LDAP.
11. A RADIUS authentication server requires the \_\_\_\_\_\_\_\_ to be authenticated first.
12. authenticator
13. user
14. authentication server
15. **supplicant**
16. Which of the following is NOT true regarding how an enterprise should handle an orphaned or dormant account?
17. A formal procedure should be in place for disabling accounts for employees who are dismissed, resign, or retire from the organization.
18. Access should be ended as soon as the employee is no longer part of the organization.
19. Logs should be monitored because current employees are sometimes tempted to use an older dormant account instead of their own account.
20. **All orphaned and dormant accounts should be deleted immediately whenever they are discovered.**
21. With the development of IEEE 802.1x port security, what type of authentication server has seen even greater usage?
22. **RADIUS**
23. Lite RDAP
24. DAP
25. RDAP
26. Which of the following is NOT part of the AAA framework?
27. Authentication
28. **Access**
29. Authorization
30. Accounting
31. What is the version of the X.500 standard that runs on a personal computer over TCP/IP?
32. Lite RDAP
33. DAP
34. **LDAP**
35. IEEE X.501
36. Raul has been asked to serve as the individual to whom day-to-day actions have been assigned by the owner. What role is Raul taking?
37. Privacy officer
38. End-user
39. **Custodian**
40. Operator
41. Which access control model is the most restrictive?
42. DAC
43. **MAC**
44. Role-Based Access Control
45. Rule-Based Access Control
46. Which type of access control model uses predefined rules that makes it flexible?
47. **ABAC**
48. DAC
49. MAC
50. Rule-Based Access Control
51. Which can be used to establish geographical boundaries where a mobile device can and cannot be used?
52. **Location-based policies**
53. Restricted access control policies
54. Geolocation policies
55. Mobile device policies
56. Which statement about Rule-Based Access Control is true?
57. It requires that a custodian set all rules.
58. It is considered obsolete today.
59. **It dynamically assigns roles to subjects based on rules.**
60. It is considered a real-world approach by linking a user’s job function with security.
61. Which of the following would NOT be considered as part of a clean desk policy?
62. **Do not share passwords with other employees.**
63. Lock computer workstations when leaving the office.
64. Place laptops in a locked filing cabinet.
65. Keep mass storage devices locked in a drawer when not in use.
66. Which of these is a set of permissions that is attached to an object?
67. **Access control list (ACL)**
68. Subject Access Entity (SAE)
69. Object modifier
70. Security entry designator
71. Which Microsoft Windows feature provides group-based access control for centralized management and configuration of computers and remote users who are using Active Directory?
72. Windows Registry Settings
73. AD Management Services (ADMS)
74. **Group Policy**
75. Resource Allocation Entities
76. What can be used to provide both file system security and database security?
77. RBASEs
78. LDAPs
79. CHAPs
80. **ACLs**
81. What is the least restrictive access control model?
82. **DAC**
83. ABAC
84. MAC
85. Rule-Based Access Control
86. What is the secure version of LDAP?
87. **LDAPS**
88. Secure DAP
89. X.500
90. 802.1x
91. Which of the following is the Microsoft version of EAP?
92. EAP-MS
93. **MS-CHAP**
94. PAP-MICROSOFT
95. AD-EAP
96. Which of the following involves rights given to access specific resources?
97. Identification
98. **Access**
99. Authorization
100. Accounting