**崑山科技大學資工系IPAS證照輔導班 練習**

**名稱:** *CompTIA SecurityPLUS\_Ch4\_Identity and Access Management*

|  |  |  |
| --- | --- | --- |
|  | | |
| 答案 | 編號 | 題目 |
|  | 1. | Jack is using smart cards for authentication. He is trying to classify the type of authentication for a report to his CIO. What type of authentication is Jack using?  A. Type I B. Type II C. Type III D. Strong |
|  | 2. | Carole is responsible for various network protocols at her company. The network time protocol has been intermittently failing. Which of the following would be most affected? A. Kerberos B. RADIUS C. CHAP D. LDAP |
|  | 3. | You are selecting an authentication method for your company’s servers. You are looking for a method that periodically reauthenticates clients to prevent session hijacking. Which of the following would be your best choice?  A. PAPB. SPAP C. CHAP D. OAUTH |
|  | 4. | Emiliano is working for a small company. His company is concerned about authentication and wants to implement biometrics using facial recognition and fingerprint scanning. How would this authentication be classified?  A. Type I B. Type II C. Type III D. Strong |
|  | 5. | Lisa is setting up accounts for her company. She wants to set up accounts for the Oracle database server. Which of the following would be the best type of account to assign to the database service? A. User B. Guest C. Admin D. Service |
|  | 6. | You have been asked to select an authentication method that will support single sign-on, integrate with SAML, and work well over the Internet. Which of the following would be your best choice?  A. Shibboleth B. OAUTH C. SPAP D. CHAP |
|  | 7. | Which authentication method was used as a native default for older versions of Microsoft Windows? A. PAP B. CHAP C. OAUTH D. NTLM |
|  | 8. | Carl has been asked to set up access control for a server. The requirements state that users at a lower privilege level should not be able to see or access files or data at a higher privilege level. What access control model would best fit these requirements? A. MAC B. DAC C. RBAC D. SAML |
|  | 9. | Clarice is concerned about an attacker getting information regarding network resources in her company. Which protocol should she implement that would be most helpful in mitigating this risk? A. LDAP B. TLS C. SNMP D. LDAPS |
|  | 10. | Ahmed is looking for an authentication protocol for his network. He is very concerned about highly skilled attackers. As part of mitigating that concern, he wants an authentication protocol that never actually transmits a user’s password, in any form. Which authentication protocol would be a good fit for Ahmed’s needs? A. CHAP B. Kerberos C. RBAC D. Type II |
|  | 11. | You work for a social media website. You wish to integrate your users’ accounts with other web resources. To do so, you need to allow authentication to be used across different domains, without exposing your users’ passwords to these other services. Which of the following would be most helpful in accomplishing this goal? A. Kerberos B. SAML C. OAUTH D. OpenID |
|  | 12. | Mary is trying to set up remote access to her network for salespeople in her company. Which protocol would be most helpful in accomplishing this goal?  A. RADIUS B. Kerberos C. CHAP D. OpenID |
|  | 13. | Victor is trying to identify the protocol used by Windows for authentication to a server that is not part of the network domain. Which of the following would be most useful for Victor? A. Kerberos B. NTLM C. OpenID D. CHAP |
|  | 14. | You have been asked to find an authentication service that is handled by a third party. The service should allow users to access multiple websites, as long as they support the third-party authentication service. What would be your best choice?  A. OpenID B. Kerberos C. NTLM D. Shibboleth |
|  | 15. | Abigail is implementing biometrics for her company. She is trying to get the false rejection rate and false acceptance rate to the same level. What is the term used for this? A. Crossover error rate B. Leveling C. Balanced error rate D. Remediation |
|  | 16. | Mia is responsible for website security for a bank. When a user forgets their password, she wants a method to give them a temporary password. Which of the following would be the best solution for this situation?  A. Facial recognition B. Digital certificate authentication C. RBAC D. TOTP |
|  | 17. | George wants a secure authentication protocol that can integrate with RADIUS and can use digital certificates. Which of the following would be his best choice?  A. CHAP B. 802.11i C. 802.1x D. OAUTH |
|  | 18. | Jacob is responsible for database server security in his company. He is very concerned about preventing unauthorized access to the databases. Which of the following would be the most appropriate for him to implement?  A. ABAC B. TOTP C. HIDS D. DAMP |
|  | 19. | Mason is responsible for security at a company that has traveling salespeople. The company has been using ABAC for access control to the network. Which of the following is an issue that is specific to ABAC and might cause it to incorrectly reject logins? A. Geographic location B. Wrong password  C. Remote access is not allowed by ABAC. D. Firewalls usually block ABAC. |
|  | 20. | You work for a U.S. defense contractor. You are setting up access cards that have chips embedded in them to provide access control for users in your company. Which of the following types of cards would be best for you to use?  A. CAC B. PIV C. NFC D. Smart card |
|  | 21. | Darrell is concerned that users on his network have too many passwords to remember and might write down their passwords, thus creating a significant security risk. Which of the following would be most helpful in mitigating this issue? A. OAUTH B. SSO C. OpenID D. Kerberos |
|  | 22. | Fares is a security administrator for a large company. Occasionally, a user needs to access a specific resource that they don’t have permission to access. Which access control methodology would be most helpful in this situation?  A. Mandatory Access Control B. Discretionary Access Control  C. Role-based Access Control D. Rule-based Access Control |
|  | 23. | You are comparing biometric solutions for your company, and the product you pick must have an appropriate False Acceptance Rate (FAR). Which of the following best describes FAR?  A. How often an unauthorized user is granted access by mistake  B. How readily users accept the new technology, based on ease of use  C. How often an authorized user is not granted access  D. How frequently the system is offline |
|  | 24. | Amelia is looking for a network authentication method that can use digital certificates and does not require end users to remember passwords. Which of the following would best fit her requirements?  A. OAUTH B. Tokens C. OpenID D. RBAC |
|  | 25. | You are responsible for setting up new accounts for your company network. What is the most important thing to keep in mind when setting up new accounts?  A. Password length B. Password complexity C. Account age D. Least privileges |
|  | 26. | Stefan just became the new security officer for a university. He is concerned that student workers who work late on campus could try and log in with faculty credentials. Which of the following would be most effective in preventing this?  A. Time of day restrictions B. Usage auditing C. Password length  D. Credential management |
|  | 27. | Jennifer is concerned that some people in her company have more privileges than they should. This has occurred due to people moving from one position to another, and having cumulative rights that exceed the requirements of their current jobs. Which of the following would be most effective in mitigating this issue?  A. Permission auditing B. Job rotation C. Preventing job rotation  D. Separation of duties |
|  | 28. | Chloe has noticed that users on her company’s network frequently have simple passwords made up of common words. Thus, they have weak passwords. How could Chloe best mitigate this issue? A. Increase minimum password length.  B. Have users change passwords more frequently.  C. Require password complexity. D. Implement Single Sign-On (SSO). |
|  | 29. | Bart is looking for a remote access protocol for his company. It is important that the solution he selects support multiple protocols and use a reliable network communication protocol. Which of the following would be his best choice?  A. RADIUS B. TACACS+ C. NTLM D. CHAP |
|  | 30. | You are looking for an authentication method that has one-time passwords and  works well with the Initiative for Open Authentication. However, the user should  have unlimited time to use the password. Which of the following would be your best choice? A. CHAP B. TOTP C. HOTP D. ABAC |
|  | 31. | Gerard is trying to find a flexible remote access protocol that can use either TCP or UDP. Which of the following should he select?  A. RADIUS B. DIAMETER C. TACACS+ D. TACACS |
|  | 32. | Emiliano is considering voice recognition as part of his access control strategy. What is one weakness with voice recognition?  A. People’s voices change. B. Systems require training.  C. High false negative rate D. High false positive rate |
|  | 33. | You are explaining facial recognition to a colleague. What is the most significant drawback to implementing facial recognition? A. These systems can be expensive.  B. These systems can be fooled with facial hair, glasses, etc.  C. These systems have a high false positive rate.  D. The systems require a long time to observe a face. |
|  | 34. | Mohanned is responsible for account management at his company. He is very concerned about hacking tools that rely on rainbow tables. Which of the following would be most effective in mitigating this threat? A. Password complexity  B. Password age C. Password expiration D. Password length |
|  | 35. | Mary is a security administrator for a mid-sized company. She is trying to securely offboard employees. What should she do with the network account for an employee who is being off-boarded? A. Disable the account. B. Delete the account. C. Change the account password. D. Leave the account as is. |
|  | 36. | Your supervisor tells you to implement security based on your users’ physical characteristics. Under which type of security would hand scanning and retina scanning fall? A. CHAP B. Multifactor C. Biometrics D. Token |
|  | 37. | What port does TACACS use?  A. TCP 143 B. TCP and UDP 49 C. TCP 443 D. UDP 53 |
|  | 38. | A company-wide policy is being created to define various security levels. Which of the following systems of access control would use documented security levels like Confidential or Secret for information? A. RBAC B. MAC C. DAC D. BBC |
|  | 39. | There is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and privileges than what is required for the tasks the user needs to fulfill. This is the opposite of what principle? A. Separation of duties B. Least privileges  C. Transitive trust D. Account management |
|  | 40. | Users in your network are able to assign permissions to their own shared resources. Which of the following access control models is used in your network?  A. DAC B. RBAC C. MAC D. ABAC |
|  | 41. | John is performing a port scan of a network as part of a security audit. He notices that the domain controller is using secure LDAP. Which of the following ports would lead him to that conclusion? A. 53 B. 389 C. 443 D. 636 |
|  | 42. | Which of the following access control methods grants permissions based on the user’s position in the organization? A. MAC B. RBAC C. DAC D. ABAC |
|  | 43. | Which of the following can be used as a means for dual-factor authentication?  A. Password and PIN number B. RADIUS and L2TP  C. LDAP and WPA D. Iris scan and password |
|  | 44. | Kerberos uses which of the following to issue tickets? A. Authentication service B. Certificate authority C. Ticket-granting service D. Key distribution center |
|  | 45. | A company requires that a user’s credentials include providing something they know and something they are in order to gain access to the network. Which of the following types of authentication is being described?  A. Token B. Two-factor C. Kerberos D. Biometrics |
|  | 46. | Samantha is looking for an authentication method that incorporates the X.509 standard and will allow authentication to be digitally signed. Which of the following authentication methods would best meet these requirements?  A. Certificate-based authentication B. OAUTH C. Kerberos D. Smart cards |
|  | 47. | Your company relies heavily on cloud and SaaS service providers such as salesforce.com, Office365, and Google. Which of the following would you have security concerns about? A. LDAP B. TACACS+ C. SAML D. Transitive trust |
|  | 48. | Greg is responsible for database security for his company. He is concerned about authentication and permissions. Which of the following should be his first step?  A. Implement minimum password length. B. Implement password lockout.  C. Conduct a permissions audit. D. Ensure least privileges |
|  | 49. | Which of the following is a step in account maintenance? A. Implement two-factor authentication. B. Check for time of day restrictions. C. Review onboarding processes. D. Check to see that all accounts are for active employees. |
|  | 50. | Tyrell works as a security officer for a mid-sized bank. All the employees only work in the office; there are no employees who work remotely or travel for company business. Tyrell is concerned about someone using an employee’s login credentials to access the bank’s network. Which of the following would be most effective in mitigating this threat? A. Kerberos authentication B. TOTP  C. Location-based policies D. Group-based access control |
|  | 51. | Henry is an employee at Acme Company. The company requires him to change his  password every three months. He has trouble remembering new passwords, so he keeps switching between just two passwords. Which policy would be most effective in preventing this? A. Password complexity B. Password history  C. Password length D. Password age |
|  | 52. | Sheila is concerned that some users on her network may be accessing files that they should not—specifically, files that are not required for their job tasks. Which of the following would be most effective in determining if this is happening?  A. Usage auditing and review B. Permissions auditing and review  C. Account maintenance D. Policy review |
|  | 53. | In which of the following scenarios would using a shared account pose the least security risk? A. For a group of tech support personnel B. For guest Wi-Fi access C. For students logging in at a university D. For accounts with few privileges |
|  | 54. | Which of the following is not a part of password complexity?  A. Using both uppercase and lowercase letters B. Minimum password length  C. Using numbers D. Using symbols (such as $, #, etc.) |
|  | 55. | Jane is setting up login accounts for federated identities. She wants to avoid requiring the users to remember login credentials and allow them to use their logins from the originating network. Which of the following technologies would be most suitable for implementing this? A. Credential management B. OAUTH  C. Kerberos D. Shibboleth |
|  | 56. | Sam is responsible for password management at a large company. Sometimes users cannot recall their passwords. What would be the best solution for him to address this? A. Changing password history length B. Implementing password recovery C. Eliminating password complexity D. Lengthening password age |
|  | 57. | You are a security administrator for an insurance company. You have discovered that there are a few active accounts for employees who left the company over a year ago. Which of the following would best address this issue?  A. Password complexity B. Offboarding procedures C. Onboarding procedures  D. Password expiration |
|  | 58. | Maria is responsible for security at a small company. She is concerned about unauthorized devices being connected to the network. She is looking for a device authentication process. Which of the following would be the best choice for her?  A. CHAP B. Kerberos C. 802.11i D. 802.1x |
|  | 59. | Laura is a security admin for a mid-sized mortgage company. She wants to ensure that the network is using the most secure login and authentication scheme possible. Which of the following would be her best choice? A. Iris scanning  B. Fingerprint scanning C. Multifactor authentication D. Smart cards |
|  | 60. | Charles is a CISO for an insurance company. He recently read about an attack wherein an attacker was able to enumerate all the network resources, and was able to make some resources unavailable. All this was done by exploiting a single protocol. Which protocol should Charles secure to mitigate this attack?  A. SNMP B. LDAP C. HTTP D. DHCP |
|  | 61. | Robert is using PAP for authentication in his network. What is the most significant weakness in PAP? A. Unsigned authentication B. Single factor  C. Credentials sent in cleartext D. PAP does not support TACACS+. |
|  | 62. | You are responsible for account access control and authorization at a large university. There are approximately 30,000 students and 1,200 faculty/staff for whom you must manage accounts. Which of the following would be the best access control/account management approach?  A. Group-based B. Location-based C. MAC D. DAC |
|  | 63. | Which of the following is most important in managing account permissions?  A. Account recertification B. Usage auditing  C. Standard naming conventions D. Account recovery |
|  | 64. | Which of the following would be the best choice for naming the account of John Smith, who is a domain administrator?  A. dm\_jsmith B. jsmithAdmin C. AdministratorSmith D. jsmith |
|  | 65. | Megan is very concerned about file system security on her network servers. Which of the following is the most basic form of file system security?  A. Encryption B. Access control C. Auditing D. RAID |
|  | 66. | Karen is responsible for account security in her company. She has discovered a receptionist whose account has a six-character password that has not been changed in two years, and her password history is not being maintained. What is the most significant problem with this account?  A. Nothing, this is adequate for a low-security position.  B. The password length is the most significant problem.  C. The lack of password history is the most significant problem.  D. The age of the password is the most significant problem. |
|  | 67. | When you’re offboarding an employee, which of the following is the first thing you should do? A. Audit their computer. B. Conduct an out-processing questionnaire. C. Disable accounts. D. Delete accounts |
|  | 68. | Which of the following is a difference between TACACS and TACACS+?  A. TACACS uses TCP, TACACS+ uses UDP  B. TACACS uses UDP, TACACS+ uses TCP  C. TACACS uses TCP or UDP, TACACS+ uses UDP  D. TACACS uses UDP, TACACS+ uses UDP or TCP |
|  | 69. | Greg is considering using CHAP or MS-CHAPv2 for authenticating remote users. Which of the following is a major difference between the two protocols?  A. CHAP uses a hash for the challenge, MS-CHAPv2 uses AES.  B. CHAP provides mutual authentication, MS-CHAPv2 does not.  C. CHAP uses AES for the challenge, MS-CHAPv2 uses a hash.  D. MS-CHAPv2 provides mutual authentication, CHAP does not. |
|  | 70. | Terrance is looking for a physical access solution that uses asymmetric cryptography (public key cryptography) to authorize the user. What type of solution is this? A. Asynchronous password token B. Challenge response token  C. TOTP token D. Static password token |
|  | 71. | Which access control model is based on the Trusted Computer System Evaluation Criteria (TCSEC)? A. ABAC B. MAC C. RBAC D. DAC |
|  | 72. | Mary is responsible for the security of database servers at a mortgage company. The servers are Windows Server 2016. She is concerned about file system security. Which of thefollowing Microsoft features would be most helpful to her in implementing file system security? A. Password policies B. EFS  C. Account lockout D. UAC |
|  | 73. | Santiago manages database security for a university. He is concerned about ensuring that appropriate security measures are implemented. Which of the following would be most important to database security? A. Password policies  B. Antivirus C. EFS D. Access control policies |
|  | 74. | Ingrid is reviewing her company’s recertification policy. Which of the following is the best reason to recertify? A. To audit usage B. To enhance onboarding  C. To audit permissions D. To manage credentials |
|  | 75. | Emma is concerned about credential management. Users on her network often have over a half-dozen passwords to remember. She is looking for a solution to this problem. Which of the following would be the best way to address this issue?  A. Implement a manager. B. Use shorter passwords.  C. Implement OAUTH. D. Implement Kerberos. |
|  | 76. | Magnus is concerned about someone using a password cracker on computers in his company. He is concerned that crackers will attempt common passwords in order to log in to a system. Which of the following would be best for mitigating this threat? A. Password age restrictions B. Password minimum length requirements  C. Account lockout policies D. Account usage auditing |
|  | 77. | Lucas is looking for an XML-based open standard for exchanging authentication information. Which of the following would best meet his needs?  A. SAML B. OAUTH C. RADIUS D. NTLM |
|  | 78. | Which of the following processes transpires when a user provides a correct username and password? A. Identification B. Authentication C. Authorization  D. Accounting |
|  | 79. | Min-seo is looking for a type of access control that enforces authorization rules by the operating system. Users cannot override authentication or access control policies. Which of the following best fits this description?  A. DAC B. MAC C. RBAC D. ABAC |
|  | 80. | Hinata is considering biometric access control solutions for her company. She is concerned about the crossover error rate (CER). Which of the following most accurately describes the CER? A. The rate of false acceptance  B. The rate of false rejection  C. The point at which false rejections outpace false acceptances  D. The point at which false rejections and false acceptances are equal |
|  | 81. | Joshua is looking for an authentication protocol that would be effective at stopping session hijacking. Which of the following would be his best choice? A. CHAP  B. PAP C. SPAP D. RADIUS |
|  | 82. | David is trying to select an authentication method for his company. He needs one that will support REST as well as multiple web-based and mobile clients. Which of the following would be his best choice? A. Shibboleth B. RADIUS  C. OpenID Connect D. OAuth |
|  | 83. | Phillip is examining options for controlling physical access to the server room at his company. He wants a hands-free solution. Which of the following would be his best choice? A. Smart cards B. Proximity cards C. Tokens D. Fingerprint scanner |
|  | 84. | Which of the following is the most significant disadvantage of federated identities?  A. They cannot be used with Kerberos. B. They don’t implement least privileges.  C. Poor password management D. Transitive trust |
|  | 85. | Max is implementing type II authentication for his company. Which of the following would be an example of type II authentication?A. Strong passwords  B. Retinal scan C. Smart cards D. Timed one-time passwords |
|  | 86. | Nicole is implementing a server authentication method that depends on a TPM in the server. Which of the following best describes this approach?  A. Hardware-based access control B. Software-based access control  C. Digital certificate–based access control D. Chip-based access control |