|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Authorization is granting permission for admittance.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. Authentication, authorization, and accounting are sometimes called AAA.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. With the Discretionary Access Control (DAC) model, no object has an owner; the system has total control over that object.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. Attribute-Based Access Control (ABAC) grants permissions by matching object labels with subject labels based on their respective levels.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. Rule-Based Access Control can be changed by users.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. Employee onboarding refers to the tasks associated with hiring a new employee.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7. Least privilege in access control means that only the minimum amount of privileges necessary to perform a job or function should be allocated.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. Permission auditing and review is intended to examine the permissions that a user has been given to determine if each is still necessary.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |
| 9. ACLs provide file system security for protecting files managed by the user.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10. A Local Group Policy (LGP) has more options than a Group Policy.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. A user or a process functioning on behalf of the user that attempts to access an object is known as the:   |  |  |  | | --- | --- | --- | |  | a. | subject | |  | b. | reference monitor | |  | c. | entity | |  | d. | label |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. The action that is taken by a subject over an object is called a(n):   |  |  |  | | --- | --- | --- | |  | a. | authorization | |  | b. | access | |  | c. | control | |  | d. | operation |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. What is the name for a predefined framework that can be used for controlling access, and is embedded into software and hardware?   |  |  |  | | --- | --- | --- | |  | a. | accounting and access model | |  | b. | user control model | |  | c. | access control model | |  | d. | authorization control model |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. What access control model below is considered to be the most restrictive access control model, and involves assigning access controls to users strictly according to the custodian?   |  |  |  | | --- | --- | --- | |  | a. | Mandatory Access Control | |  | b. | Role Based Access Control | |  | c. | Discretionary Access Control | |  | d. | Rule Based Access Control |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. Which access control model is considered to be the least restrictive?   |  |  |  | | --- | --- | --- | |  | a. | Role Based Access Control | |  | b. | Mandatory Access Control | |  | c. | Rule Based Access Control | |  | d. | Discretionary Access Control |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. Which access control model that uses access based on a user's job function within an organization?   |  |  |  | | --- | --- | --- | |  | a. | Role Based Access Control | |  | b. | Rule Based Access Control | |  | c. | Discretionary Access Control | |  | d. | Mandatory Access Control |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. Which access control model can dynamically assign roles to subjects based on a set of defined rules?   |  |  |  | | --- | --- | --- | |  | a. | Role Based Access Control | |  | b. | Mandatory Access Control | |  | c. | Rule Based Access Control | |  | d. | Discretionary Access Control |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. When using Role Based Access Control (RBAC), permissions are assigned to which of the following?   |  |  |  | | --- | --- | --- | |  | a. | Roles | |  | b. | Groups | |  | c. | Labels | |  | d. | Users |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. A vulnerable process that is divided between two or more individuals to prevent fraudulent application of the process is known as which of the following?   |  |  |  | | --- | --- | --- | |  | a. | separation of duties | |  | b. | process sharing | |  | c. | mandatory splitting | |  | d. | role reversal |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. A list that specifies which subjects are allowed to access an object and what operations they can perform on it is referred to as a(n):   |  |  |  | | --- | --- | --- | |  | a. | ACE | |  | b. | DAC | |  | c. | entity | |  | d. | ACL |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. User accounts that remain active after an employee has left an organization are referred to as being what type of accounts?   |  |  |  | | --- | --- | --- | |  | a. | abandoned | |  | b. | stale | |  | c. | orphaned | |  | d. | inactive |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. To assist with controlling orphaned and dormant accounts, what can be used to indicate when an account is no longer active?   |  |  |  | | --- | --- | --- | |  | a. | password expiration | |  | b. | account expiration | |  | c. | last login | |  | d. | account last used |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. Although designed to support remote dial-in access to a corporate network, what service below is commonly used with 802.1x port security for both wired and wireless LANs?   |  |  |  | | --- | --- | --- | |  | a. | RADIUS | |  | b. | ICMP | |  | c. | FTP | |  | d. | Telnet |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. During RADIUS authentication, what type of packet includes information such as identification of a specific AP that is sending the packet and the username and password?   |  |  |  | | --- | --- | --- | |  | a. | accounting request | |  | b. | access request | |  | c. | verification request | |  | d. | authentication request |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. What authentication service commonly used on UNIX devices involves communicating user authentication information to a centralized server?   |  |  |  | | --- | --- | --- | |  | a. | TACACS | |  | b. | RADIUS | |  | c. | Kerberos | |  | d. | FTP |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. Select the authentication system developed by the Massachusetts Institute of Technology (MIT) to verify the identity of network users.   |  |  |  | | --- | --- | --- | |  | a. | Aurora | |  | b. | Kerberos | |  | c. | CHAP | |  | d. | TACACS |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. The X.500 standard defines a protocol for a client application to access an X.500 directory known as which of the following options?   |  |  |  | | --- | --- | --- | |  | a. | DIB | |  | b. | DAP | |  | c. | DIT | |  | d. | LDAP |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. What kind of attack allows for the construction of LDAP statements based on user input statements, which can then be used to access the LDAP database or modify the database's information?   |  |  |  | | --- | --- | --- | |  | a. | LDAP poisoning | |  | b. | Kerberos injection | |  | c. | LDAP injection | |  | d. | DAP hijacking |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. Which of the following is a simpler subset of Directory Access Protocol?   |  |  |  | | --- | --- | --- | |  | a. | SDAP | |  | b. | X.500 Lite | |  | c. | DIB | |  | d. | ADS |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. When LDAP traffic is made secure by using Secure Sockets Layer (SSL) or Transport Layer Security (TLS), what is this process called?   |  |  |  | | --- | --- | --- | |  | a. | SAML | |  | b. | LDAPS | |  | c. | TACACS | |  | d. | SDML |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. Select the XML standard that allows secure web domains to exchange user authentication and authorization data and is used extensively for online e-commerce transactions.   |  |  |  | | --- | --- | --- | |  | a. | SAML | |  | b. | LDAPS | |  | c. | TACACS | |  | d. | SDML |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. What framework is used for transporting authentication protocols instead of the authentication protocol itself?   |  |  |  | | --- | --- | --- | |  | a. | CHAP | |  | b. | SAML | |  | c. | EAP | |  | d. | MS-CHAP |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What standard provides a greater degree of security by implementing port-based authentication and blocks all traffic on a port-by-port basis until the client is authenticated using credentials stored on an authentication server?   |  |  |  | | --- | --- | --- | |  | a. | IEEE 802.1a | |  | b. | IEEE 802.1x | |  | c. | LDAPS | |  | d. | TACACS |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. Which of the following is a database stored on the network itself that contains information about users and network devices?   |  |  |  | | --- | --- | --- | |  | a. | user permissions | |  | b. | network service | |  | c. | system registry | |  | d. | directory service |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. What type of computer can forward RADIUS messages between RADIUS clients and RADIUS servers?   |  |  |  | | --- | --- | --- | |  | a. | intermediate proxy | |  | b. | remote proxy | |  | c. | RADIUS proxy | |  | d. | translation proxy |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. Which of the following controls can be implemented so an organization can configure multiple computers by setting a single policy for enforcement?   |  |  |  | | --- | --- | --- | |  | a. | group-based access control | |  | b. | computer-based access control | |  | c. | role-based access control | |  | d. | system access control |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. Which major types of access involving system resources are controlled by ACLs? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | system access | |  | b. | remote access | |  | c. | user access | |  | d. | application access |  |  |  | | --- | --- | | *ANSWER:* | a, c, d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. What is an entry in an ACL known as?   |  |  |  | | --- | --- | --- | |  | a. | DACL | |  | b. | ACE | |  | c. | SQL | |  | d. | flag |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. What policy is designed to ensure that all confidential or sensitive materials, either in paper form or electronic, are removed from a user's workspace and secured when the items not in use or when employees leave their workspace?   |  |  |  | | --- | --- | --- | |  | a. | clean workspace | |  | b. | secure workspace | |  | c. | clean desk | |  | d. | secure desk |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. What process periodically validates a user's account, access control, and membership role or inclusion in a specific group?   |  |  |  | | --- | --- | --- | |  | a. | recertification | |  | b. | revalidation | |  | c. | control audit | |  | d. | group auditing |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |
| --- | --- | --- |
| 41. List three major access control models.   |  |  | | --- | --- | | *ANSWER:* | There are five major access control models: Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role Based Access Control (RBAC), Rule Based Access Control (RBAC), and Attribute-Based Access Control (ABAC). | |

|  |  |  |
| --- | --- | --- |
| 42. Describe the two key elements of the MAC model.   |  |  | | --- | --- | | *ANSWER:* | Labels. In a system using MAC, every entity is an object (laptops, files, projects, and so on) and is assigned a classification label. These labels represent the relative importance of the object, such as confidential, secret, and top secret. Subjects (users, processes, and so on) are assigned a privilege label (sometimes called a clearance). Levels. A hierarchy based on the labels is also used, both for objects and subjects. Top secret has a higher level than secret, which has a higher level than confidential. | |

|  |  |  |
| --- | --- | --- |
| 43. Describe the MAC lattice model.   |  |  | | --- | --- | | *ANSWER:* | Different "rungs" on the MAC lattice model have different security levels, and subjects are assigned a "rung" on the lattice just as objects are. Multiple lattices can even be placed beside each other to allow for different groups of labels. For example, one subject label lattice could use the clearances confidential, secret, and top secret, while a corresponding subject label lattice could use public, restricted, and top clearance. The rungs of each subject lattice would still align with the rungs on the object security lattice. | |

|  |  |  |
| --- | --- | --- |
| 44. Describe the Bell-LaPadula model.   |  |  | | --- | --- | | *ANSWER:* | Although this model is very similar to the lattice model, it contains an additional restriction not found in the original lattice model. This protection prevents subjects from creating a new object or performing specific functions on objects that are at a lower level than their own. For example, a user with clearance secret should not have the ability to open a document at the secret level and then paste its contents to a newly created document at the confidential level. | |

|  |  |  |
| --- | --- | --- |
| 45. Discuss the two significant weaknesses of DAC.   |  |  | | --- | --- | | *ANSWER:* | DAC has two significant weaknesses. First, although it gives a degree of freedom to the subject, DAC poses risks in that it relies on decisions by the end user to set the proper level of security. As a result, incorrect permissions might be granted to a subject or permissions might be given to an unauthorized subject. A second weakness is that a subject's permissions will be "inherited" by any programs that the subject executes. Attackers often take advantage of this inheritance because end users in the DAC model often have a high level of privileges. Malware that is downloaded onto a user's computer would then run in the same context as the user's high privileges. Trojans are a particular problem with DAC. | |

|  |  |  |
| --- | --- | --- |
| 46. Discuss the differences between DAP and LDAP.   |  |  | | --- | --- | | *ANSWER:* | Unlike X.500 DAP, LDAP was designed to run over TCP/IP, making it ideal for Internet and intranet applications. X.500 DAP requires special software to access the network. LDAP has simpler functions, making it easier and less expensive to implement. LDAP encodes its protocol elements in a less complex way than X.500 that enables it to streamline requests. | |

|  |  |  |
| --- | --- | --- |
| 47. Describe LDAP injection attacks.   |  |  | | --- | --- | | *ANSWER:* | A weakness of LDAP is that it can be subject to LDAP injection attacks. These attacks, similar to SQL injection attacks, can occur when user input is not properly filtered. This may allow an attacker to construct LDAP statements based on user input statements. The attacker could then retrieve information from the LDAP database or modify its content. The defense against LDAP injection attacks is to examine all user input before processing. | |

|  |  |  |
| --- | --- | --- |
| 48. Describe how Kerberos works.   |  |  | | --- | --- | | *ANSWER:* | Kerberos is typically used when a user attempts to access a network service and that service requires authentication. The user is provided a ticket that is issued by the Kerberos authentication server, much as a driver's license is issued by the DMV. This ticket contains information linking it to the user. The user presents this ticket to the network for a service. The service then examines the ticket to verify the identity of the user. If the user is verified, they are then accepted. Kerberos tickets share some of the same characteristics as a driver's license: tickets are difficult to copy (because they are encrypted), they contain specific user information, they restrict what a user can do, and they expire after a few hours or a day. Issuing and submitting tickets in a Kerberos system is handled internally and is transparent to the user. | |

|  |  |  |
| --- | --- | --- |
| 49. What authentication service was developed by Cisco and is an authentication service commonly used on UNIX devices that communicate by forwarding user authentication information to a centralized server?   |  |  | | --- | --- | | *ANSWER:* | Terminal Access Control Access Control System (TACACS) | |

|  |  |  |
| --- | --- | --- |
| 50. What is the purpose of an ACL?   |  |  | | --- | --- | | *ANSWER:* | ACLs provide file system security for protecting files managed by the OS. ACLs have also been ported to SQL and relational database systems so that ACLs can provide database security as well. ACLs are the oldest and most basic form of access control. | |