**Chapter 9 Review Questions**

1. A RADIUS authentication server requires that the \_\_\_\_\_\_\_\_ be authenticated first.

a. authentication server

b. supplicant – PG349

c. authenticator

d. user

2. Each of the following make up the AAA elements in network security, except \_\_\_\_\_\_\_\_.

a. controlling access to network resources (authentication)

b. enforcing security policies (authorization)

c. determining user need (analyzing) – PG348

d. auditing usage (accounting)

3. With the development of IEEE 802.1x port security, the authentication server \_\_\_\_\_\_\_ has seen even greater usage.

a. RDAP

b. DAP

c. RADIUS – PG348

d. AAA

4. \_\_\_\_\_\_\_\_\_\_\_\_\_ is an authentication protocol available as a free download that runs on Microsoft Windows 7/Vista, Windows Server 2008, Apple Mac OS X, and Linux.

a. IEEE 802.1x

b. RADIUS

c. Kerberos – PG350

d. LDAP

5. The version of the X.500 standard that runs on a personal computer over TCP/IP is \_\_\_\_\_\_\_\_\_.

a. DAP

b. LDAP – PG352

c. IEEE X.501

d. Lite RDAP

6. A user entering her username would correspond to the \_\_\_\_\_\_\_ action in access control.

a. authentication

b. identification – PG334

c. authorization

d. access

7. A process functioning on behalf of the user that attempts to access a file is known as a(n) \_\_\_\_\_\_\_\_\_\_.

a. object

b. subject – PG335

c. resource

d. operation check

8. The individual who periodically reviews security settings and maintains records of access by users is called the \_\_\_\_\_\_\_.

a. supervisor

b. owner

c. custodian – PG335

d. manager

9. In the \_\_\_\_\_\_ model, the end user cannot change any security settings.

a. Discretionary Access Control

b. Security Access Control

c. Mandatory Access Control – PG337

d. Restricted Access Control

10. Rule Based Access Control \_\_\_\_\_\_\_\_.

a. is considered obsolete today

b. dynamically assigns roles to subjects based on rules – PG340

c. is considered a real-world approach by linking a user’s job function with security

d. requires that a custodian set all rules

11. Separation of duties requires that \_\_\_\_\_\_\_.

a. processes should be divided between two or more individuals – PG341

b. end users cannot set security for themselves

c. managers must monitor owners for security purposes

d. jobs be rotated among different individuals

12. \_\_\_\_\_\_\_\_ in access control means that if a condition is not explicitly met, then access is to be rejected.

a. Denial of duties

b. Implicit deny – PG343

c. Explicit rejection

d. Prevention control

13. A(n) \_\_\_\_\_\_\_\_ is a set of permissions that is attached to an object.

a. access control list (ACL) – PG344

b. Subject Access Entity (SAE)

c. object modifier

d. security entry designator

14. \_\_\_\_\_\_\_\_ is a Microsoft Windows feature that provides centralized management and configuration of computers and remote users who are using Active Directory.

a. Windows Register Settings

b. Group Policy – PG345

c. Resource Allocation Entities

d. AD Management Services (ADMS)

15. A(n) \_\_\_\_\_\_\_ constructs LDAP statements based on user inputs in order to retrieve information from the database or modify its contents.

a. SQL/LDAP insert attack

b. modified Trojan attack

c. LDAP injection attack – PG353

d. RBASE plug-in attack

16. The least restrictive access control model is \_\_\_\_\_\_\_\_.

a. Role Based Access Control (RBAC)

b. Mandatory Access Control (MAC)

c. Discretionary Access Control (DAC) – PG338

d. Rule Based Access Control (RBAC)

17. The principle known as \_\_\_\_\_\_\_\_\_ in access control means that each user should only be given the minimal amount of privileges necessary for that person to perform their job function.

a. Enterprise Security

b. least privilege – PG342

c. deny all

d. Mandatory Limitations

18. A(n) \_\_\_\_\_\_\_ is the person responsible for the information and determines the level of security needed for the data and delegates security duties as required.

a. owner – PG335

b. custodian

c. end user

d. administrator

19. In the Mandatory Access Control (MAC) model, every subject and object \_\_\_\_\_\_\_.

a. is restricted and cannot be accessed

b. is assigned a label – PG336

c. can be changed by the owner

d. must be given a number from 200–900

20. A user account that has not been accessed for a lengthy period of time is called a(n) \_\_\_\_\_\_\_ account.

a. orphaned

b. limbo

c. static

d. dormant – PG346