

Congratulations! You passed!

Grade received 90.90%

Latest Submission Grade 90.91%

To pass 80% or higher

Go to next
item

1. Authn is short for _____.

1 / 1 point

- ☒ authentication
- ☐ authored
- ☐ authoritarian
- ☐ authorization

✓ Correct

2. Authz is short for _____.

1 / 1 point

- ☐ authoritarian
- ☐ authentication
- ☒ authorization
- ☐ authored

✓ Correct

3. Authentication is concerned with determining _____.

1 / 1 point

- ☐ validity
- ☒ identity
- ☐ access
- ☐ eligibility

☒ **Correct**

4. Authorization is concerned with determining _____ to resources.

1 / 1 point

- ☐ identity
- ☐ eligibility
- ☐ validity
- ☒ access

☒ **Correct**

5. In the three As of security, what is the process of proving who you claim to be?

1 / 1 point

- ☒ Authentication
- ☐ Authorization
- ☐ Accounting
- ☐ Authored

☒ **Correct**

6. Which of the following passwords is the strongest for authenticating to a system?

1 / 1 point

- ☐ P@ssword!
- ☐ P@55w0rd!

☒ P@w04d!\$\$L0N6

☐ Password!

☒ Correct

7. Which of the following are valid multi-factor authentication factors? Check all that apply.

1 / 1 point

☒ Something you know

☒ Correct

☒ Something you are

☒ Correct

☐ Something you did

☒ Something you have

☒ Correct

8. Which of the following are types of one-time-password tokens? Check all that apply.

1 / 1 point

☐ Password-based

☒ Counter-based

☒ Correct

☒ Time-based

☒ Correct

☐ Identity-based

9. Security Keys are more ideal than OTP generators because they are resistant to _____ attacks. 1 / 1 point

- ☐ brute force
- ☐ password
- ☒ phishing
- ☐ DDoS

☒ Correct

10. Security Keys utilize a secure challenge-and-response authentication system, which is based on _____. 1 / 1 point

- ☒ public key cryptography
- ☐ symmetric encryption
- ☐ steganography
- ☐ shared secrets

☒ Correct

11. Which of the following qualifies as a multifactor authentication, already having a password? Check all that apply. 1 / 1 point

☒ Bank card

☒ Correct

☒ Fingerprint

☒ Correct

☐ Passphrase

☐ PIN

12. Which of the following are examples of "something you have" for multifactor authentication? Check all that apply.

1 / 1 point

☒ One-Time-Password (OTP)

☒ Correct

☐ PING

☒ RSA SecureID token

☒ Correct

☐ Password

13. In addition to the client being authenticated by the server, certificate authentication also provides _____.

1 / 1 point

☐ authorization

☒ server authentication

☐ integrity

☐ malware protection

☒ Correct

14. An organization needs to setup a(n) _____ infrastructure to issue and sign client certificates.

1 / 1 point

☐ CRL

☐ ID

☐ LDAP

☒ CA

☒ Correct

15. In a Certificate Authority (CA) infrastructure, why is a client certificate used?

1 / 1 point

- ☐ To authenticate the CA
- ☐ To authenticate the subordinate CA
- ☐ To authenticate the server
- ☒ To authenticate the client

☒ Correct

16. A Lightweight Directory Access Protocol (LDAP) uses a(n) _____ structure to hold directory objects.

1 / 1 point

- ☐ Distinguished Name
- ☐ Bind
- ☐ Organizational Unit
- ☒ Data Information Tree

☒ Correct

17. Consider the following scenario:

0 / 1 point

A systems administrator is designing a directory architecture to support Linux servers using Lightweight Directory Access Protocol (LDAP). The directory needs to be able to make changes to directory objects securely. Which of these common operations supports these requirements?

- ☒ Search, modify
- ☐ Bind, add
- ☐ Bind, modify
- ☐ StartTLS, delete

☒ Incorrect

Please review the "[LDAP](#)" video for a refresher.

18. Consider the following scenario:

1 / 1 point

A network admin wants to use a Remote Authentication Dial-In User Service (RADIUS) protocol to allow 5 user accounts to connect company laptops to an access point in the office. These are generic users and will not be updated often. Which of these internal sources would be appropriate to store these accounts in?

- ☒ Flat file
- ☐ LDAP
- ☐ Active Directory
- ☐ SQL database

☒ Correct

19. Kerberos uses _____ as authentication tokens.

1 / 1 point

- ☐ certificates
- ☐ passwords
- ☐ cryptographic keys
- ☒ tickets

☒ Correct

20. What is used to request access to services in the Kerberos process?

1 / 1 point

- ☐ TGS session key
- ☒ Ticket Granting Ticket
- ☐ Client-to-Server ticket
- ☐ Client ID

☒ Correct

21. Kerberos enforces strict _____ requirements. Otherwise, authentication will fail.

1 / 1 point

- ☒ time
- ☐ strong password
- ☐ AES
- ☐ LDAP

☒ **Correct**

22. Consider the following scenario:

0 / 1 point

Multiple client switches and routers have been set up at a small military base. The network team decided to implement Terminal Access Controller Access-Control System Plus (TACACS+), along with Kerberos, and an external Lightweight Directory Access Protocol (LDAP) service. What is the primary reason TACACS+ was chosen for this?

- ☐ Device administration
- ☒ Single Sign-On
- ☐ NIPRNet
- ☐ Network access

☒ **Incorrect**

Please review the "[TACACS+](#)" video for a refresher.

23. What are the benefits of using a Single Sign-On (SSO) authentication service?
Check all that apply.

1 / 1 point

- ☐ The need for multiple passwords
- ☒ Reduce overhead of password assistance

☒ **Correct**

- ☒ One set of credentials for the user

✓ Correct

✓ Reduce time spent on re-authenticating to services

✓ Correct

24. Which of these are examples of a Single Sign-On (SSO) service? Check all that apply. 1 / 1 point

✓ OpenID

✓ Correct

☐ Relying Parties

✓ Kerberos

✓ Correct

☐ Tokens

25. The authentication server is to authentication as the ticket granting service is to _____. 1 / 1 point

☐ identification

☐ integrity

☒ authorization

☐ verification

✓ Correct

26. Consider the following scenario: 1 / 1 point

A company is utilizing Google Business applications for their marketing department. These applications should be able to temporarily access a user's email account to send links for review. Why should the company use Open Authorization (OAuth) in this situation?

- ☐ Administer multiple network devices
- ☐ Utilize a Key Distribution Center server
- ☒ Compatibility with third party apps
- ☐ Gain access through a wireless access point

✓ **Correct**

27. An Open Authorization (OAuth) access token would have a(n) _____ that tells what the third party app has access to.

0 / 1 point

- ☐ scope
- ☐ request
- ☐ template
- ☒ e-mail

✗ **Incorrect**

Please review the "[Access Control](#)" video for a refresher.

28. Which of these are examples of an access control system? Check all that apply.

1 / 1 point

☒ TACACS+

✓ **Correct**

☒ OAuth

✓ **Correct**

☐ OpenID

☒ RADIUS

☒ Correct

29. A(n) _____ defines permissions or authorizations for objects.

1 / 1 point

- ☐ Access Control Entries
- ☐ Extensible Authentication Protocol
- ☒ Access Control List
- ☐ Network Access Server

☒ Correct

30. Access control entries can be created for what types of file system objects?

1 / 1 point

Check all that apply.

☒ Files

☒ Correct

☒ Folders

☒ Correct

☒ Programs

☒ Correct

☐ APIs

31. In the three As of security, which part pertains to describing what the user account does or doesn't have access to?

1 / 1 point

- ☐ Authentication

- ☒ Authorization
- ☐ Accessibility
- ☐ Accounting
- ☒ **Correct**

32. Consider the following scenario:

1 / 1 point

A network admin deployed a Terminal Access Controller Access Control System Plus (TACACS+) system so other admins can properly manage multiple switches and routers on the Local Area Network (LAN). The system will keep track and log admin access to each device and the changes made. This “logging” satisfies which part of the three As of security?

- ☐ Authentication
- ☐ Authorization
- ☒ Accounting
- ☐ Administration
- ☒ **Correct**

33. What does a Terminal Access Controller Access Control System Plus (TACACS+) keep track of? Check all that apply.

1 / 1 point

- ☐ Bandwidth and resource usage
- ☒ Commands that were run

☒ **Correct**

- ☒ Track user authentication

☒ **Correct**

- ☒ Systems users authenticated to

✓ Correct