[Updated Constantly]

HERE

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 8 Exam Answers

1. A web server administrator is configuring access settings to require users to authenticate first before accessing certain web pages. Which requirement of information security is addressed through the configuration?

- availability
- **confidentiality**
- integrity
- scalability

2. What component of a security policy explicitly defines the type of traffic allowed on a network and what users are allowed and not allowed to do?

- password policies
- identification and authentication policies
- remote access policies
- **acceptable use policies**

3. What is the principle of least privilege access control model?

- User access to data is based on object attributes.
- **Users are granted rights on an as-needed approach.**
- Users are granted the strictest access control possible to data.
- Users control access to data they own.

4. Which statement describes a difference between RADIUS and TACACS+?

- RADIUS is supported by the Cisco Secure ACS software whereas TACACS+ is not.
- **RADIUS encrypts only the password whereas TACACS+ encrypts all communication.**
- RADIUS separates authentication and authorization whereas TACACS+ combines them as one process.
- RADIUS uses TCP whereas TACACS+ uses UDP.

5. What is the purpose of mobile device management (MDM) software?

- It is used to create a security policy.
- **It is used to implement security policies, setting, and software configurations on mobile devices.**
- It is used by threat actors to penetrate the system.
- It is used to identify potential mobile device vulnerabilities.

6. What service determines which resources a user can access along with the operations that a user can perform?

- authentication
- biometric
- **authorization**
- accounting
- token

7. A company has a file server that shares a folder named Public. The network security policy specifies that the Public folder is assigned Read-Only rights to anyone who can log into the server while the Edit rights are assigned only to the network admin group. Which component is addressed in the AAA network service framework?

- automation
- accounting
- **authentication**
- authorization

8. In threat intelligence communications, what set of specifications is for exchanging cyberthreat information between organizations?

- Trusted automated exchange of indicator information (TAXII)
- **Structured threat information expression (STIX)**
- Automated indicator sharing (AIS)
- Common vulnerabilities and exposures (CVE)

9. What three items are components of the CIA triad? (Choose three.)

- **integrity**
- **availability**
- **confidentiality**
- access
- scalability
- intervention

10. A company is experiencing overwhelming visits to a main web server. The IT department is developing a plan to add a couple more web servers for load balancing and redundancy. Which requirement of information security is addressed by implementing the plan?

- integrity
- scalability
- **availability**
- confidentiality

11. Which AAA component can be established using token cards?

- authorization
- **authentication**
- auditing
- accounting

12. Which method is used to make data unreadable to unauthorized users?

- **Encrypt the data.**
- Fragment the data.
- Add a checksum to the end of the data.
- Assign it a username and password.

13. Which two areas must an IT security person understand in order to identify vulnerabilities on a network? (Choose two.)

- number of systems on each network
- network baseline data
- data analysis trends
- **hardware used by applications**
- **important applications used**

14. Which three services are provided by the AAA framework? (Choose three.)

- autoconfiguration
- automation
- **authorization**
- **authentication**
- **accounting**
- autobalancing

15. How does BYOD change the way in which businesses implement networks?

- **BYOD provides flexibility in where and how users can access network resources.**
- BYOD requires organizations to purchase laptops rather than desktops.
- BYOD users are responsible for their own network security, thus reducing the need for organizational security policies.
- BYOD devices are more expensive than devices that are purchased by an organization.

16. Which technology provides the framework to enable scalable access security?

- AutoSecure
- role-based CLI access
- **authentication, authorization, and accounting**
- Simple Network Management Protocol
- Cisco Configuration Professional communities

17. Which device is usually the first line of defense in a layered defense-in-depth approach?

- access layer switch
- internal router
- **edge router**
- firewall

19. In a defense-in-depth approach, which three options must be identified to effectively defend a network against attacks? (Choose three.)

- **assets that need protection**
- location of attacker or attackers
- total number of devices that attach to the wired and wireless network
- **threats to assets**
- **vulnerabilities in the system**
- past security breaches

20. Which section of a security policy is used to specify that only authorized individuals should have access to enterprise data?

- statement of authority
- statement of scope
- campus access policy
- Internet access policy
- **identification and authentication policy**
- acceptable use policy

21. Which type of access control applies the strictest access control and is commonly used in military or mission critical applications?

- **mandatory access control (MAC)**
- discretionary access control (DAC)
- attribute-based access control (ABAC)
- Non-discretionary access control