CCNA Cyber Ops (Version 1.1) – Chapter 8 Exam Answers Full

itexamanswers.net/ccna-cyber-ops-chapter-8-exam-answers-full.html

May 13, 2019

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. With the evolution of borderless networks, which vegetable is now used to describe a defense-in-depth approach?

- **Artichoke** *
- Lettuce
- Onion
- Cabbage

A. The artichoke is now used to provide a visual analogy to describe a defense-in-depth security approach. The onion used to be descriptive because the attacker would "peel away" each layer of the network defense mechanisms. Now the artichoke is used because a single petal or leaf can be moved or removed to reveal sensitive information.

2. What is a characteristic of a layered defense-in-depth security approach?

- Three or more devices are used.
- Routers are replaced with firewalls.
- When one device fails, another one takes over.
- **One safeguard failure does not affect the effectiveness of other safeguards.** *

D. When a layered defense-in-depth security approach is used, layers of security are placed through the organization—at the edge, within the network, and on endpoints. The layers work together to create the security architecture. In this environment, a failure of one safeguard does not affect the effectiveness of other safeguards.

3. Passwords, passphrases, and PINs are examples of which security term?

- Identification

- Authorization
- **Authentication** *
- Access

C. Authentication methods are used to strengthen access control systems. It is important to understand the available authentication methods.

4. What is privilege escalation?

- Someone is given rights because she or he has received a promotion.
- **Vulnerabilities in systems are exploited to grant higher levels of privilege than someone or some process should have.** *
- A security problem occurs when high-ranking corporate officials demand rights to systems or files that they should not have.
- Everyone is given full rights by default to everything and rights are taken away only when someone abuses privileges.

B. With privilege escalation, vulnerabilities are exploited to grant higher levels of privilege. After the privilege is granted, the threat actor can access sensitive information or take control of the system.

5. What are two characteristics of the RADIUS protocol? (Choose two.)

- Encryption of the entire body of the packet
- The use of TCP port 49
- **The use of UDP ports for authentication and accounting** *
- **Encryption of the password only** *
- The separation of the authentication and authorization processes

C, D. RADIUS is an open-standard AAA protocol using UDP port 1645 or 1812 for authentication and UDP port 1646 or 1813 for accounting. It combines authentication and authorization into one process.

6. Which component of AAA is used to determine which resources a user can access and which operations the user is allowed to perform?

- Auditing
- Accounting
- **Authorization** *
- Authentication

C. One of the components in AAA is authorization. After a user is authenticated through AAA, authorization services determine which resources the user can access and which operations the user is allowed to perform.

7. Which type of business policy establishes the rules of conduct and the responsibilities of employees and employers?

- **Company** *
- Data
- Employee
- Security

A. Business policies set a baseline of acceptable use. Company policies establish the rules and conduct and the responsibilities of both employees andthe employer. Company policies protect the rights of the workers as well as the business interests of the company.

8. Which component of AAA allows an administrator to track individuals who access network resources and any changes that are made to those resources?

- Accessibility
- **Accounting** *
- Authentication
- Authorization

B. One of the components in AAA is accounting. After a user is authenticated through AAA, AAA servers keep a detailed log of exactly what actions the authenticated user takes on the device.

9. Which of the following offers a free service called Automated Indicator Sharing that enables the real-time exchange of cyberthreat indicators?

- FireEye
- **Department of Homeland Security** *
- The MITRE Corporation
- Talos

B. The U.S. Department of Homeland Security (DHS) offers a free service called Automated Indicator Sharing (AIS). AIS enables the real-time exchange of cyberthreat indicators (e.g., malicious IP addresses, the sender address of a phishing email, etc.) between the U.S. federal government and the private sector.

10. The security policy of an organization allows employees to connect to the office intranet from their homes. Which type of security policy is this?

- Acceptable use
- Incident handling
- Network maintenance
- **Remote access** *

D. The remote access policy section of a corporate security policy identifies how remote users can access a network and what is accessible via remote connectivity.

11. During the AAA process, when will authorization be implemented?

- **Immediately after successful authentication against an AAA data source** *
- Immediately after AAA accounting and auditing receives detailed reports
- Immediately after an AAA client sends authentication information to a centralized server
- Immediately after the determination of which resources a user can access

A. AAA authorization is implemented immediately after the user is authenticated against a specific AAA data source.

12. 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

Confidentiality ensures that data is accessed only by authorized individuals. Authentication will help verify the identity of the individuals.

13. 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**

Security policies specify requirements and provide a baseline for organizations. Security policies may include the following:
Identification and authentication policies that specify authorized individuals that have access to network resources and verification procedures
Password policies that ensure minimum requirements are met and authentication methods are being enforced and updated
Remote access policies that identify how remote users can access a network and to what they are allowed to connect
Acceptable use policies that identify network applications and network usage that are allowed within the organization

14. 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.

The principle of least privilege is an access control model that specifies a limited and as-needed approach to user access to data.

15. 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.

TACACS+ uses TCP, encrypts the entire packet (not just the password), and separates authentication and authorization into two distinct processes. Both protocols are supported by the Cisco Secure ACS software.

16. 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.

Mobile device management (MDM) software is used with mobile devices so that corporate IT personnel can track the devices, implement security settings, as well as control software configurations.

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

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

Authorization determines whether a user has certain access privileges.

18. 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**

After a user is successfully authenticated (logged into the server), the authorization is the process of determining what network resources the user can access and what operations (such as read or edit) the user can perform.

19. 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)

The two common threat intelligence-sharing standards are as follows:
Structured Threat Information Expression (STIX) – This is a set of specifications for exchanging cyberthreat information between organizations. The Cyber Observable Expression (CybOX) standard has been incorporated into STIX.
Trusted Automated Exchange of Indicator Information (TAXII) – This is the specification for an application layer protocol that allows the communication of CTI over HTTPS. TAXII is designed to support STIX.

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

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

The CIA triad contains three components: confidentiality, integrity, and availability. It is a guideline for information security for an organization.

21. 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

Availability ensures that network services are accessible and performing well under all conditions. By load balancing the traffic destined to the main web servers, in times of a huge volume of visits the systems will be well managed and serviced.

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

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

The authentication component of AAA is established using username and password combinations, challenge and response questions, and token cards. The authorization component of AAA determines which resources the user can access and which operations the user is allowed to perform. The accounting and auditing component of AAA keeps track of how network resources are used.

23. 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.

Network data can be encrypted using various cryptography applications so that the data is made unreadable to unauthorized users. Authorized users have the cryptography application so the data can be unencrypted.

24. 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**

In order to identify security vulnerabilities, a cybersecurity expert must understand the applications being used and their associated vulnerabilities, as well as the hardware used.

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

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

The authentication, authorization, and accounting (AAA) framework provides services to help secure access to network devices.

26. 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.

A BYOD environment requires an organization to accommodate a variety of devices and access methods. Personal devices, which are not under company control, may be involved, so security is critical. Onsite hardware costs will be reduced, allowing a business to focus on delivering collaboration tools and other software to BYOD users.

27. 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

AAA network security services (authentication, authorization, and accounting) provide the primary framework to set up access control on a network device. It provides a higher degree of scalability than the con, aux, vty and privileged EXEC authentication commands alone by using centrally managed Cisco Secure ACS servers using TACACS+ and RADIUS protocols.

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

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

The edge router connects an organization to a service provider. The edge router has a set of rules that specify which traffic is allowed or denied.

29. 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

Access control models are used to define the access controls implemented to protect corporate IT resources. The different types of access control models are as follows:Mandatory access control (MAC) – The strictest access control that is typically used in military or mission critical applications.
Discretionary access control (DAC) – Allows users to control access to their data as owners of that data. Access control lists (ACLs) or other security measures may be used to specify who else may have access to the information.
Non-discretionary access control – Also known as role-based access control (RBAC). Allows access based on the role and responsibilities of the individual within the organization.
Attribute-based access control (ABAC) – Allows access based on the attributes of the resource to be accessed, the user accessing the resource, and the environmental factors such as the time of day.

30. 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

In order to prepare for a security attack, IT security personnel must identify assets that need to be protected such as servers, routers, access points, and end devices. They must also identify potential threats to the assets and vulnerabilities in the system or design.

31. 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

The identification and authentication policy section of the security policy typically specifies authorized persons that can have access to network resources and identity verification procedures.

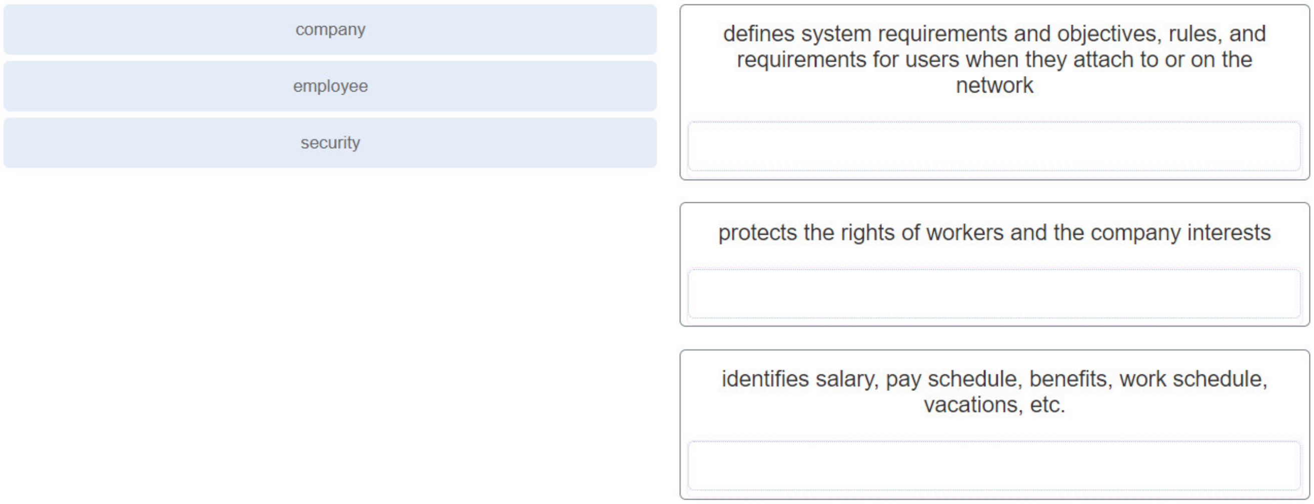
32. What device is usually the first line of defense in a layered defense-in-depth approach?

Edge router

33. 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?

Acceptable use policies

34. Match the type of business policy to the description.



company

employee

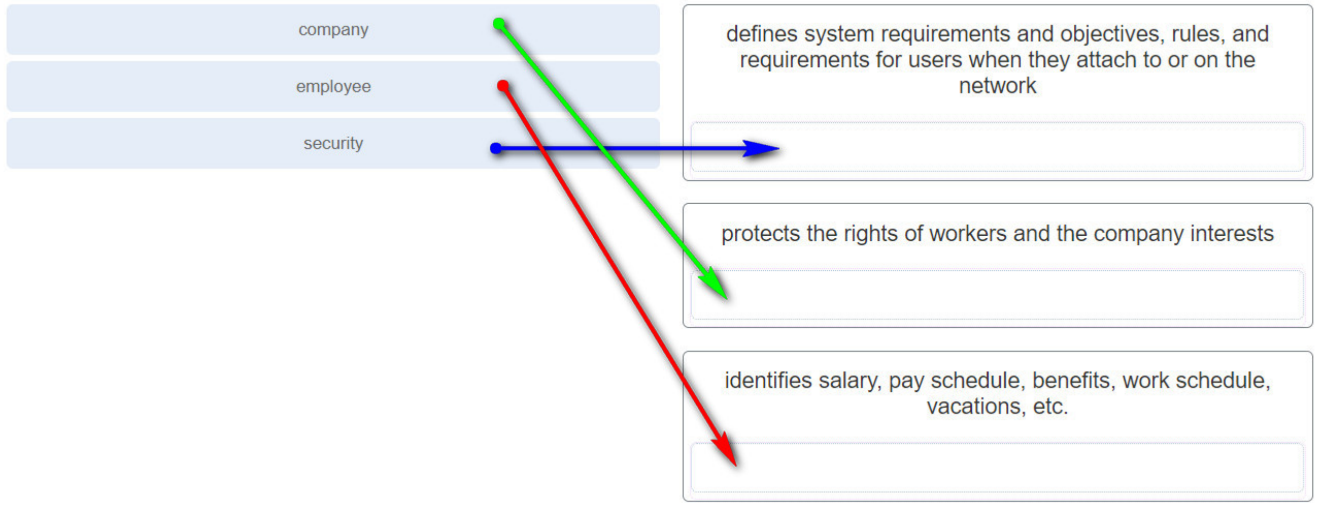
security

defines system requirements and objectives, rules, and requirements for users when they attach to or on the network

protects the rights of workers and the company interests

identifies salary, pay schedule, benefits, work schedule, vacations, etc.

Answer



company

employee

security

defines system requirements and objectives, rules, and requirements for users when they attach to or on the network

protects the rights of workers and the company interests

identifies salary, pay schedule, benefits, work schedule, vacations, etc.

Download PDF File below:

[sociallocker id="54558″]

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 8 Exam Answers.pdf 361.96 KB 1087 downloads

…

Download

[/sociallocker]