DSST CYBERSECURITY FUNDAMENTALS PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://dsstcybersecurityfund.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1
Table of Contents 2
Introduction 3
How to Use This Guide 4
Questions 5
Answers 8
Explanations 10
Next Steps 16

SAMPLE

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

SAMPLE

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

SAMPLE

Questions

SAMPLE

1. What does egress refer to in networking?

A. Data entering a network

B. Network communications going out

C. Internal data processing

D. Data storage on a server

2. What is a Certificate Revocation List (CRL) used for?

A. To list expired digital certificates

B. To verify the validity of certificates issued by a CA

C. To issue new security certificates

D. To hold records of user credentials

3. What does multifactor authentication involve?

A. A combination of one authentication method

B. A single authentication method for security

C. A combination of more than one authentication method

D. Only biometric authentication

4. What is meant by the term 'security perimeter'?

A. A geographical location of the data center

B. The boundary that defines the area of security concern

C. A type of software that prevents malware

D. The physical barriers around servers

5. What is the primary function of a write blocker?

A. Forcing data deletion on a drive

B. Allowing data modification on a drive

C. Preventing accidental damage to a drive during information acquisition

D. Enhancing the storage capacity of a drive

6. Layer 3 and 4 switches operate primarily at which model layers?

A. Physical and Data Link layers

B. Network and Transport layers

C. Application and Session layers

D. Presentation and Application layers

SAMPLE

7. Who is typically responsible for both physical and digital security in an organization?

A. A Cybersecurity Analyst

B. A Chief Security Officer (CSO)

C. A Systems Administrator

D. An IT Support Specialist

8. How does a BIA prioritize resources needed for recovery?

A. By estimating market demand

B. By evaluating the criticality and sensitivity of assets

C. By focusing on employee needs

D. By assessing regulatory compliance

9. What is the purpose of Network Address Translation (NAT)?

A. Encrypting network traffic for security

B. Modifying network address information in datagram headers

C. Providing communication between wireless devices

D. Controlling bandwidth in a network

10. In digital security, what does nonrepudiation mean?

A. The sender cannot deny sending the message

B. Only the sender can read the message

C. The recipient can alter the message

D. Access to the message is restricted

SAMPLE

Answers

SAMPLE

1. B
2. B
3. C
4. B
5. C
6. B
7. B
8. B
9. B
10. A

SAMPLE

Explanations

SAMPLE

1. What does egress refer to in networking?

A. Data entering a network

B. Network communications going out

C. Internal data processing

D. Data storage on a server

Egress in networking specifically refers to the flow of data leaving or exiting a network. This term encompasses the outbound traffic that is transmitted from an internal network to external destinations, such as the internet, other networks, or end-user devices. Understanding egress is critical for managing network security, monitoring, and data flow effectively. In the context of network management and security, monitoring egress traffic is crucial because this is often where data breaches occur or sensitive information may be leaked. By identifying and controlling egress points, organizations can implement security measures to prevent unauthorized data transfers. The other concepts presented in the options do not accurately describe egress. Data entering a network is generally referred to as ingress. Internal data processing and data storage on a server pertain to different aspects of network functionality and do not specifically define the concept of egress. Thus, the correct understanding aligns directly with the definition of egress as the movement of data out of a network.

2. What is a Certificate Revocation List (CRL) used for?

A. To list expired digital certificates

B. To verify the validity of certificates issued by a CA

C. To issue new security certificates

D. To hold records of user credentials

A Certificate Revocation List (CRL) serves as a crucial mechanism in public key infrastructure (PKI) for maintaining secure communications. It is primarily used to verify the validity of digital certificates that have been issued by a Certificate Authority (CA). The CRL contains a list of certificates that have been revoked before their expiration date, indicating that they should no longer be trusted for establishing secure connections. When a system or service checks the validity of a certificate, it can refer to the CRL to determine whether the certificate in question is still valid or has been revoked. This process is essential to ensure that compromised certificates do not continue to provide access or authentication, thereby enhancing overall security. Understanding the role of a CRL within the context of certificate management helps reinforce why the correct answer is focused on the verification of the validity of issued certificates, reflecting its role in ensuring ongoing trust in digital communications.

3. What does multifactor authentication involve?

A. A combination of one authentication method

B. A single authentication method for security

C. A combination of more than one authentication method

D. Only biometric authentication

Multifactor authentication involves utilizing a combination of more than one authentication method to verify a user's identity. This approach enhances security by requiring multiple forms of verification that generally fall into three categories: something you know (like a password), something you have (like a security token or smartphone), and something you are (like a fingerprint or facial recognition). The idea behind multifactor authentication is that even if one factor is compromised, the additional factors provide an extra layer of security. For instance, even if a password is stolen, an attacker would still need access to the second factor (like a physical token) or the biometric data to gain access. The incorrect options do not capture the essence of multifactor authentication adequately. A single authentication method does not provide the robustness required for secure access, and relying solely on biometric authentication would neglect other viable forms of verification that enhance security.

SAMPLE

4. What is meant by the term 'security perimeter'?

A. A geographical location of the data center

B. The boundary that defines the area of security concern

C. A type of software that prevents malware

D. The physical barriers around servers

The term 'security perimeter' refers to the boundary that defines the area of security concern. This concept encompasses all the elements of security controls, both physical and digital, that protect an organization's information systems and data. The security perimeter can include firewalls, intrusion detection systems, and other security measures that are configured to anonymize and shield the internal network from external threats. This boundary is crucial because it delineates what is considered secure versus what is not, and is the focal point for implementing security policies, monitoring, and incident response. Understanding the security perimeter helps organizations to manage risks effectively and to design their systems to protect critical assets against unauthorized access and threats. The other choices, such as the geographical location of a data center or physical barriers around servers, while related to security, do not encompass the broader, more strategic definition of a security perimeter which includes all protective measures and assets inside and outside an organization's network. Furthermore, describing a type of software that prevents malware does not accurately capture the essence of what security perimeter signifies in the context of cybersecurity.

5. What is the primary function of a write blocker?

A. Forcing data deletion on a drive

B. Allowing data modification on a drive

C. Preventing accidental damage to a drive during information acquisition

D. Enhancing the storage capacity of a drive

The primary function of a write blocker is to prevent accidental damage to a drive during information acquisition. Write blockers are critical tools in digital forensics and data recovery; they enable investigators to access data on a storage device without altering or overwriting any of the data present on that device. This is essential for maintaining the integrity of the evidence, ensuring that any analysis or examination is based solely on the original data as it was found. When using a write blocker, all write operations are blocked, meaning no changes can be made to the drive, thus preserving the original data in its untouched state. This is vital in legal and investigative contexts where the authenticity and reliability of the data could be challenged if there is any indication that the data has been altered or tampered with. Other options, while related to data management in various ways, do not accurately capture the primary purpose of a write blocker in the context of data protection and forensic investigations.

SAMPLE

6. Layer 3 and 4 switches operate primarily at which model layers?

A. Physical and Data Link layers

B. Network and Transport layers

C. Application and Session layers

D. Presentation and Application layers

Layer 3 and 4 switches operate primarily at the Network and Transport layers of the OSI model. Layer 3 switches function by using logical addressing (such as IP addresses) to route packets between different networks, which is characteristic of the Network layer. They are capable of making forwarding decisions based on layer 3 information, allowing for traffic management and path selection based on the destination IP address. Layer 4 switches, on the other hand, extend this functionality by incorporating session management and looking at transport layer protocols (like TCP and UDP). They can make decisions based on layer 4 information, such as port numbers, which enables a more refined control over the streamed packets, enhancing data flow and application performance. This ability to handle "intelligent" traffic management at these layers makes Layer 3 and 4 switches vital in networks where efficient routing and switching are required, especially in environments that need varied levels of Quality of Service (QoS) based on the transport layer characteristics. This dual function helps manage not just where to send packets, but also how they are prioritized and managed across networks.

7. Who is typically responsible for both physical and digital security in an organization?

A. A Cybersecurity Analyst

B. A Chief Security Officer (CSO)

C. A Systems Administrator

D. An IT Support Specialist

The Chief Security Officer (CSO) is typically responsible for both physical and digital security in an organization. This role encompasses a broad range of security concerns, ensuring that the organization's information assets are protected both from digital threats, such as cyberattacks, and from physical threats, such as unauthorized access to facilities. A CSO develops and implements security policies and strategies, oversees security personnel, and coordinates efforts to safeguard critical infrastructure, data integrity, and compliance with relevant laws and regulations. This position requires a comprehensive understanding of security requirements and risks related to all aspects of an organization's operation, making the CSO uniquely qualified to handle both realms of security effectively. While other roles, such as cybersecurity analysts, systems administrators, and IT support specialists, may focus on specific aspects of digital security or support operations, they do not typically hold the overarching responsibility that a CSO does for an organization's security landscape.

SAMPLE

8. How does a BIA prioritize resources needed for recovery?

A. By estimating market demand

B. By evaluating the criticality and sensitivity of assets

C. By focusing on employee needs

D. By assessing regulatory compliance

A Business Impact Analysis (BIA) essential for disaster recovery and business continuity planning emphasizes identifying and evaluating the criticality and sensitivity of assets. By understanding which business processes and resources are vital for continued operations, organizations can prioritize recovery efforts more effectively. This means determining what assets are most essential to the functioning of the organization and the potential impact of their loss. In this context, analyzing critical and sensitive assets enables a business to not only safeguard its most important functions but also allocate resources more efficiently during recovery efforts. It ensures that the most significant risks are addressed first, which can minimize downtime and the financial impact of disruptions. Other options do not align as effectively with the primary goal of a BIA. Estimating market demand is more related to sales strategy than recovery prioritization. Employee needs, while important, are often a component of broader recovery considerations rather than a direct measure of asset criticality. Assessing regulatory compliance is necessary for staying compliant but does not prioritize resources for recovery in the immediate sense.

9. What is the purpose of Network Address Translation (NAT)?

A. Encrypting network traffic for security

B. Modifying network address information in datagram headers

C. Providing communication between wireless devices

D. Controlling bandwidth in a network

Network Address Translation (NAT) serves the main purpose of modifying network address information in datagram headers as they pass through a routing device, allowing for the efficient management of IP address usage and providing an added layer of security. When a device on a private network wants to communicate with the outside world, NAT translates the private IP address of the device to a public IP address that can be recognized on the internet. This process helps conserve the number of public IP addresses a network uses, as multiple devices can share a single public IP for outbound connections. NAT also helps to hide the internal IP addresses of devices within a private network, making it more challenging for external attackers to reach these devices directly, thus enhancing network security. By keeping the internal network structure hidden, NAT provides a fundamental element of security in network design. The translation occurs seamlessly and allows replies from the internet to be redirected back to the correct internal device. While the other choices mention important networking concepts, they do not accurately capture the primary function of NAT: modifying the network address information within data packets to facilitate communication between private and public networks.

SAMPLE

10. In digital security, what does nonrepudiation mean?

A. The sender cannot deny sending the message

B. Only the sender can read the message

C. The recipient can alter the message

D. Access to the message is restricted

Nonrepudiation is a key concept in digital security that ensures that a sender can be held accountable for the transmission of a message or the execution of a transaction. It means that once a message has been sent, the sender cannot deny having sent it. This is particularly crucial in scenarios involving legal contracts or critical transactions where accountability is vital. Nonrepudiation is typically achieved through cryptographic methods, such as digital signatures, which authenticate the sender's identity and provide proof that the message has not been altered in transit. This assurance protects parties from disputes and provides evidence of actions taken, thereby fostering trust in electronic communications. In contrast, the other options do not accurately represent the concept of nonrepudiation. The focus on reading messages, altering content, or restricting access speaks to different aspects of data integrity and confidentiality rather than the sender's accountability for their actions.

SAMPLE

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://dsstcybersecurityfund.examzify.com

We wish you the very best on your exam journey. You've got this!

SAMPLE