Kenzie Academy Network Defense Essentials (NDE) Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

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

Table of Contents

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.

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!

Questions

1. **Which of the following describes the Point-to-Point Protocol (PPP)?**
   - **A. A communication protocol between multiple hosts over a network**
   - **B. A data link layer communication protocol between routers**
   - **C. An encryption protocol for wireless communications**
   - **D. A framework for secure authentication in local networks**

2. **What is the purpose of a Redundant Array of Independent Disks (RAID)?**
   - **A. To store data on a single hard drive**
   - **B. To enhance computing speed without fault tolerance**
   - **C. To combine multiple drives for fault tolerance**
   - **D. To increase the physical size of storage devices**

3. **Which method describes an incremental data backup?**
   - **A. All data is copied to the backup media.**
   - **B. Only files changed or created since the last backup are copied.**
   - **C. Data is compressed before being backed up.**
   - **D. Full system images are created in each backup.**

4. **Retrospective approaches are used to achieve what outcome?**
   - **A. Prevent future attacks**
   - **B. Document user behavior**
   - **C. Enhance user satisfaction**
   - **D. Analyze software performance**

5. **What is the purpose of deterrent controls?**
   - **A. To facilitate rapid incident response**
   - **B. To discourage attackers from attempting intrusions**
   - **C. To provide detailed logs of all network activity**
   - **D. To conduct security audits**

6. What is the purpose of a Proxy Server?

A. To filter network traffic based on rules

B. To serve as an intermediary during network connections

C. To monitor TCP sessions

D. To create logs of network intrusions

7. What does PCI-DSS requirement 1.2.1 focus on regarding traffic?

A. Allowing unrestricted traffic for analysis

B. Restricting traffic to what is necessary for cardholder data

C. Monitoring outbound traffic for anomalies

D. Using firewalls to increase bandwidth

8. What does a registry contain for an organization?

A. A collection of encryption algorithms

B. All images deployed by the organization

C. A list of employees and their roles

D. All network security incidents

9. What is one feature of a Distributed Intrusion Detection System (DIDS)?

A. It consists of a single IDS for a large network

B. It incorporates multiple IDSs across a large network

C. It is limited to local area networks only

D. It operates without any network segmentation

10. Which policy defines a set of rules for storing and maintaining data for operational and regulatory purposes?

A. Data retention policy

B. Access control policy

C. Incident response policy

D. Data encryption policy

Answers

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

Explanations

1. Which of the following describes the Point-to-Point Protocol (PPP)?

A. A communication protocol between multiple hosts over a network

B. A data link layer communication protocol between routers

C. An encryption protocol for wireless communications

D. A framework for secure authentication in local networks

The chosen answer accurately captures the core function of the Point-to-Point Protocol (PPP). PPP is specifically designed as a data link layer communication protocol that operates primarily between two nodes, which can be routers, over a point-to-point link. This makes it suitable for establishing direct connections that enable the exchange of data between two distinct endpoints. PPP is commonly used in various networking types, such as dial-up Internet connections, and is known for its ability to encapsulate network layer protocols, providing features like error detection and the negotiation of link configuration parameters. By functioning at the data link layer, PPP facilitates a reliable means of communication over a single physical link. Understanding this context clarifies why some choices do not align with PPP's definition. For instance, while the first option suggests that PPP works between multiple hosts, it is specifically a point-to-point protocol, focusing only on a direct link between two points. The other options, which refer to encryption protocols and secure authentication frameworks, do not accurately describe the primary purpose of PPP, reinforcing that the correct choice pertains to its role in facilitating communication between routers or similar devices in a direct manner.

2. What is the purpose of a Redundant Array of Independent Disks (RAID)?

A. To store data on a single hard drive

B. To enhance computing speed without fault tolerance

C. To combine multiple drives for fault tolerance

D. To increase the physical size of storage devices

RAID, or Redundant Array of Independent Disks, is primarily designed to combine multiple physical disk drives into a single logical unit for the purpose of improving data redundancy (fault tolerance) and/or performance. The correct choice highlights that the core purpose of RAID is to provide a mechanism that allows data to be stored across multiple disks in a way that, if one drive fails, the data can still be recovered from the other drives in the array. This fault tolerance is achieved through various RAID configurations, such as RAID 1 (mirroring) or RAID 5 (striping with parity), which ensure that data is duplicated or distributed in a way that protects against data loss due to hardware failures. The emphasis on combining multiple drives is fundamental, as it not only enhances data safety but can also improve read/write speeds through parallel processing, depending on the specific RAID level implemented. Other options do not reflect the primary purposes of RAID adequately. Storing data on a single hard drive does not take advantage of the benefits that RAID provides. Enhancing speed without fault tolerance overlooks one of the critical features of RAID, which is to ensure data safety alongside performance improvements. Increasing the physical size of storage devices is not directly related to RAID; rather, it focuses on

3. Which method describes an incremental data backup?

A. All data is copied to the backup media.

B. Only files changed or created since the last backup are copied.

C. Data is compressed before being backed up.

D. Full system images are created in each backup.

An incremental data backup refers to the process of only backing up the files that have been changed or created since the last backup was performed. This method is efficient because it minimizes the amount of storage space required and reduces the time needed for the backup process. By focusing solely on the differences between the current state of the data and the last backup, incremental backups ensure that only the necessary updates are saved, allowing for a quicker backup and restore process while maintaining a complete data set over time. In contrast, a complete backup of all data, regardless of any changes, would require significantly more time and storage, which is not the focus of an incremental backup. Additionally, compressing data before backing it up is a technique that can be applied to any backup type but does not define incremental backups specifically. Creating full system images involves capturing the entire system state, which is a more comprehensive approach and does not align with the incremental method's purpose of efficiency and minimizing redundancy.

4. Retrospective approaches are used to achieve what outcome?

A. Prevent future attacks

B. Document user behavior

C. Enhance user satisfaction

D. Analyze software performance

Retrospective approaches focus on analyzing past events and incidents to gain insights that can help in preventing similar occurrences in the future. This methodology is essential in the field of network defense, where understanding the details of previous attacks or security breaches can inform better security measures and policies. By examining what went wrong, how an attack was executed, and what vulnerabilities were exploited, organizations can strengthen their defenses and implement strategies that reduce the risk of future attacks. In contrast, documenting user behavior, enhancing user satisfaction, and analyzing software performance dive into different aspects of operations rather than addressing the primary goal of retrospective analyses, which is to learn from the past to improve future security outcomes. While these areas are important in their own right, they do not specifically target the prevention of future attacks through an analysis of previous incidents.

5. What is the purpose of deterrent controls?

A. To facilitate rapid incident response

B. To discourage attackers from attempting intrusions

C. To provide detailed logs of all network activity

D. To conduct security audits

The purpose of deterrent controls is to discourage attackers from attempting intrusions. These controls are designed to create a perception of risk or potential consequences for malicious actors, thus making them think twice before attempting an attack. By implementing visible security measures such as surveillance cameras, warning signs, and security personnel, organizations can effectively reduce the likelihood of unauthorized access or cyber threats. Deterrent controls serve as a proactive approach in cybersecurity by establishing barriers that are meant to prevent threats from materializing in the first place. When attackers see that a system has robust security in place, they may choose to target less secure systems instead, effectively reducing the organization's risk exposure.

6. What is the purpose of a Proxy Server?

A. To filter network traffic based on rules

B. To serve as an intermediary during network connections

C. To monitor TCP sessions

D. To create logs of network intrusions

The purpose of a proxy server as an intermediary during network connections is fundamental to its functionality. When a client makes a request to access a resource on the internet, the request goes to the proxy server first instead of directly to the destination server. The proxy server then forwards the client's request to the internet, retrieves the requested resource, and sends it back to the client. This process provides several benefits, such as improved security, anonymity, and potentially caching content to minimize load times for frequently requested resources.   Additionally, the use of a proxy server can enable network administrators to enforce policies, such as access control and content filtering, by determining what content should or shouldn't be accessed. Although filtering network traffic, monitoring sessions, and creating logs are functions associated with network management tools, they do not encompass the primary role of a proxy server, which is to facilitate and manage the connections between clients and external resources.

7. What does PCI-DSS requirement 1.2.1 focus on regarding traffic?

A. Allowing unrestricted traffic for analysis

B. Restricting traffic to what is necessary for cardholder data

C. Monitoring outbound traffic for anomalies

D. Using firewalls to increase bandwidth

The focus of PCI-DSS requirement 1.2.1 is on restricting traffic to what is necessary for cardholder data, as this is integral to maintaining the security of sensitive information. This requirement emphasizes the importance of limiting network traffic flow to only what is essential for the processing and transmission of cardholder data. By doing so, organizations minimize the potential attack surface and reduce the likelihood of unauthorized access to sensitive data. Restricting traffic ensures that only approved and secure channels are used for data transfer, thereby preventing exposure to unnecessary risks. It aligns with best practices for network segmentation and access control, which are critical in safeguarding payment card information. This approach is a fundamental aspect of a strong security posture within any organization that handles cardholder data. The options that suggest allowing unrestricted traffic, monitoring outbound traffic for anomalies, or increasing bandwidth through firewalls all deviate from the core objective of protecting cardholder data by controlling access and minimizing exposure to threat vectors.

8. What does a registry contain for an organization?

A. A collection of encryption algorithms

B. All images deployed by the organization

C. A list of employees and their roles

D. All network security incidents

The correct answer is that a registry in the context of an organization typically contains all images deployed by the organization. A registry serves as a centralized repository where various versions of software applications, including container images, are stored. This allows organizations to manage, distribute, and maintain their software images efficiently. By maintaining a registry, organizations can ensure that they have a consistent and controlled environment for deploying applications. This is particularly critical in environments that utilize containerization, such as Docker, where images are essential for creating and running containers that encapsulate applications and their dependencies. The other choices do not accurately reflect what a registry contains. While encryption algorithms may be a part of a security policy or system, they are not stored in a standard registry. A list of employees and their roles is typically found in human resources databases or management systems, not in a registry. Similarly, while a registry might keep logs of deployments or version histories, it does not typically track all network security incidents; that would be recorded in a different system, such as a security information and event management (SIEM) system.

9. What is one feature of a Distributed Intrusion Detection System (DIDS)?

A. It consists of a single IDS for a large network

B. It incorporates multiple IDSs across a large network

C. It is limited to local area networks only

D. It operates without any network segmentation

A Distributed Intrusion Detection System (DIDS) is characterized by its use of multiple intrusion detection systems deployed across different segments of a large network. This architecture allows for a more comprehensive monitoring capability, enabling the detection of potential intrusion attempts across various devices and locations within the network. By distributing the detection processes, a DIDS can efficiently analyze traffic and respond to threats in real time, improving the overall security posture. This approach also enhances scalability, as additional sensors can be integrated into various parts of the network as needed. It also improves resilience, because if one detection point fails or is compromised, others can continue to monitor and protect the network. In contrast, the other options do not accurately reflect the nature of a Distributed Intrusion Detection System. A single IDS serving a large network would not harness the benefits of distribution, limiting its effectiveness. Similarly, by being restricted to local area networks or lacking network segmentation, these alternatives would hinder the DIDS's intended capabilities and responsiveness essential for monitoring a complex network environment.

10. Which policy defines a set of rules for storing and maintaining data for operational and regulatory purposes?

A. Data retention policy

B. Access control policy

C. Incident response policy

D. Data encryption policy

The correct choice is a data retention policy. This policy outlines the guidelines and procedures for how an organization manages its data, including how long data should be stored, when it can be deleted, and the requirements for maintaining data for compliance with legal and regulatory standards. A well-defined data retention policy helps ensure that necessary data is preserved for operational needs while also addressing any legal obligations related to data storage. The other options relate to different aspects of data management and security. An access control policy focuses on regulating who can access certain data and the conditions under which they can access it. An incident response policy deals with the procedures to follow when a security breach occurs, ensuring that the organization can respond effectively to mitigate any impact of the incident. A data encryption policy specifies how sensitive data should be encrypted to protect it from unauthorized access, but it does not pertain to the retention or maintenance of that data over time.

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://kenziende.examzify.com

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