Network Security Vulnerability Technician (NSVT) Module 2 Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit: https://nsvtmodule2.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

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 type of networking device is primarily responsible for forwarding, filtering, and flooding packets between networks?

A. Switch

B. Router

C. Bridge

D. Hub

2. What is a key aspect of risk management in cybersecurity?

A. Simply increasing network speed

B. Identifying, assessing, and prioritizing risks

C. Maximizing the number of users

D. Reducing hardware costs

3. Why are security policies important in an organization?

A. They provide guidelines for financial budgeting

B. They ensure proper security measures are implemented

C. They improve employee productivity

D. They minimize hardware costs

4. What is the primary function of a firewall?

A. To store sensitive information

B. To amplify network traffic

C. To control incoming and outgoing network traffic

D. To monitor system performance

5. In networking, what term is used to describe the feasibility of a specific path?

A. Bandwidth

B. Latency

C. Cost

D. Throughput

SAMPLE

6. What type of attack seeks to overwhelm a system with traffic?

A. Brute Force Attack

B. Denial-of-Service (DoS) Attack

C. Phishing Attack

D. Man-in-the-Middle Attack

7. Who are referred to as script kiddies in the context of network security?

A. Experts developing sophisticated malware

B. Individuals using readily available tools to conduct attacks

C. Highly trained security professionals performing simulations

D. Corporate spies collecting sensitive data

8. What is a botnet?

A. A type of anti-virus software

B. A network of compromised computers used to perform coordinated tasks

C. A method for encrypting data

D. A form of malware

9. What is a common function of both standard and extended ACLs?

A. Both can log traffic

B. Both can filter traffic based on source IP

C. Both can be applied to routers only

D. Both are used for network address translation

10. What is the primary function of a security information and event management (SIEM) system?

A. To enhance software performance

B. To monitor and improve user satisfaction

C. To aggregate and analyze security data for threat detection

D. To manage hardware configurations

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What type of networking device is primarily responsible for forwarding, filtering, and flooding packets between networks?

A. Switch

B. Router

C. Bridge

D. Hub

In networking, a router is fundamentally designed to manage traffic between different networks by forwarding data packets based on their destination IP addresses. This ability to route packets makes routers critical for connecting disparate networks, such as a local area network (LAN) to a wide area network (WAN) or the internet. Routers utilize routing tables and protocols to determine the best path for forwarding packets, ensuring efficient data transmission. While switches, bridges, and hubs play roles in local network communications, they do not possess the same capabilities as routers. Switches operate primarily within a single network, forwarding packets based on MAC addresses and creating a more efficient communication environment by only sending data to the intended recipient. Bridges connect multiple networks but still focus on filtering traffic at the data link layer rather than making complex routing decisions. Hubs, on the other hand, operate at the physical layer and simply transmit incoming data to all ports without any filtering or traffic management, leading to increased collisions and reduced efficiency. Thus, routers are distinctly positioned to handle the complexities of multiple networks, making them essential for forwarding, filtering, and flooding packets appropriately across different networks.

2. What is a key aspect of risk management in cybersecurity?

A. Simply increasing network speed

B. Identifying, assessing, and prioritizing risks

C. Maximizing the number of users

D. Reducing hardware costs

A key aspect of risk management in cybersecurity is identifying, assessing, and prioritizing risks. This process is crucial because it allows organizations to understand their security posture and determine which vulnerabilities could have the most significant impact on their operations. By effectively identifying potential threats and vulnerabilities, cybersecurity professionals can assess the likelihood of these risks materializing and evaluate the potential consequences. Prioritization helps organizations allocate resources efficiently to mitigate the most critical risks first. This systematic approach enables effective decision-making regarding security controls, investments in technology, and allocation of personnel, ensuring that the most pressing risks are managed before addressing less critical ones. In this way, organizations can maintain a stronger security posture while optimizing their resource usage, ultimately leading to better overall risk management. The other choices do not directly relate to the central tenets of risk management in cybersecurity. Increasing network speed, for example, does not inherently address security vulnerabilities, nor does it reduce risk. Similarly, maximizing the number of users can introduce additional risks without necessarily managing or mitigating them. Reducing hardware costs may affect the ability to implement adequate security measures. Thus, focusing on risk identification, assessment, and prioritization is integral to an effective cybersecurity strategy.

SAMPLE

3. Why are security policies important in an organization?

A. They provide guidelines for financial budgeting

B. They ensure proper security measures are implemented

C. They improve employee productivity

D. They minimize hardware costs

Security policies are crucial for organizations because they establish a framework to ensure that proper security measures are implemented throughout the organization. These policies outline the protocols and procedures that employees must follow to protect sensitive information and maintain the integrity, confidentiality, and availability of data. By having a well-defined set of security policies, organizations can enforce compliance, prevent security breaches, and create a culture of security awareness among employees. Security policies also serve as a roadmap for responding to security incidents, defining roles and responsibilities, and guiding the handling of sensitive information. This structured approach helps organizations mitigate risks effectively and ensure that all personnel are aware of their obligations regarding security. The other options, while they may have some impact on aspects of organizational performance, do not directly relate to the primary purpose of security policies. Financial budgeting, employee productivity, and hardware costs are not the central focus of security policies; rather, the emphasis is on safeguarding an organization's assets and information.

4. What is the primary function of a firewall?

A. To store sensitive information

B. To amplify network traffic

C. To control incoming and outgoing network traffic

D. To monitor system performance

The primary function of a firewall is to control incoming and outgoing network traffic. Firewalls act as a barrier between a trusted internal network and untrusted external networks, such as the Internet. They enforce security policies by allowing or blocking data packets based on a set of predetermined rules. This is crucial for protecting the integrity and confidentiality of the data within the network while also preventing unauthorized access and potential attacks. By controlling the flow of data packets, firewalls help prevent malicious activities, such as unauthorized access attempts, data breaches, and other security threats. This function is essential in maintaining a secure network environment, ensuring that only legitimate traffic is allowed while potentially harmful traffic is effectively managed. Other choices do not align with the primary purpose of a firewall. Storing sensitive information relates more to data storage solutions than network security. Amplifying network traffic does not contribute to security and could even lead to increased vulnerabilities. Monitoring system performance is a separate function often associated with network management rather than specifically with the role of a firewall in security.

SAMPLE

5. In networking, what term is used to describe the feasibility of a specific path?

A. Bandwidth

B. Latency

C. Cost

D. Throughput

The term that describes the feasibility of a specific path in networking is often referred to as "Cost." In networking, particularly in the context of routing algorithms, the cost may represent various factors that determine how optimal a route is for data transmission. This could include metrics such as the number of hops between nodes, the bandwidth available on the path, administrative distances, or even monetary costs. Using “Cost” as a measure allows network administrators and routing protocols to make informed decisions about which path to use for data packets, with the goal of optimizing performance based on the criteria defined in the network's routing strategy. Other terms listed, like bandwidth, latency, and throughput, are measures of network performance rather than path feasibility. Bandwidth refers to the maximum data transfer capacity, latency indicates the time delay in data transmission, and throughput measures how much data is successfully transmitted in a given time frame. However, these do not directly relate to the feasibility of choosing a path within network routing. Cost effectively encapsulates the various influences that can affect path selection.

6. What type of attack seeks to overwhelm a system with traffic?

A. Brute Force Attack

B. Denial-of-Service (DoS) Attack

C. Phishing Attack

D. Man-in-the-Middle Attack

A Denial-of-Service (DoS) attack is characterized by its objective to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of traffic. The primary goal of the attacker is to make the targeted resource unavailable to legitimate users, often by saturating the bandwidth or crashing the system resources. In a DoS attack, various methods may be employed to generate an excessive amount of traffic, which can overwhelm the capabilities of the server or network. This causes legitimate requests to be dropped or delayed, effectively denying access to users. Understanding this is crucial in network security, as it helps in implementing proper defenses such as rate limiting, traffic analysis, and other mitigation strategies. The other types of attacks mentioned—brute force, phishing, and man-in-the-middle—do not focus on overwhelming a system with traffic. A brute force attack involves attempting multiple combinations to guess passwords, phishing is about tricking users into revealing sensitive information, and a man-in-the-middle attack is centered on intercepting communication between two parties. Therefore, the specific nature and intent of a DoS attack align perfectly with the description provided in the question.

SAMPLE

7. Who are referred to as script kiddies in the context of network security?

A. Experts developing sophisticated malware

B. Individuals using readily available tools to conduct attacks

C. Highly trained security professionals performing simulations

D. Corporate spies collecting sensitive data

In the context of network security, the term "script kiddies" refers to individuals who use existing and readily available tools and scripts to conduct cyber attacks rather than developing their own sophisticated methods or malware. These individuals typically lack the advanced skills or knowledge necessary to create custom exploits but can execute attacks by leveraging the tools created by others. This practice allows them to exploit vulnerabilities in systems without a deep understanding of the underlying technologies. Therefore, the identification of script kiddies highlights their reliance on pre-written software and tools available on the internet, reflecting a lower skill level compared to seasoned hackers or security professionals. This distinction helps in understanding the varying levels of expertise present in the cybersecurity landscape.

8. What is a botnet?

A. A type of anti-virus software

B. A network of compromised computers used to perform coordinated tasks

C. A method for encrypting data

D. A form of malware

A botnet refers specifically to a network of compromised computers or devices that are infected with malware and can be controlled remotely by an attacker. These devices, often called "bots" or "zombies," are typically utilized to perform coordinated tasks without the knowledge of the device owners. Common uses of botnets include conducting distributed denial-of-service (DDoS) attacks, distributing spam emails, or stealing personal information. Understanding this definition is crucial for recognizing the broader implications of botnets in network security, as they can pose significant threats and challenges to both individuals and organizations. By employing various tactics, attackers can exploit these compromised systems to launch attacks on other networks or serve malicious purposes. While other options describe different concepts related to cybersecurity, they do not accurately define the workings or functions of a botnet. For example, anti-virus software is intended to protect devices from malware, encryption methods secure data transmission, and forms of malware refer to harmful software in general. None of these encapsulate the operational structure of a botnet.

SAMPLE

9. What is a common function of both standard and extended ACLs?

A. Both can log traffic

B. Both can filter traffic based on source IP

C. Both can be applied to routers only

D. Both are used for network address translation

The correct answer highlights a fundamental capability of both standard and extended Access Control Lists (ACLs): their ability to filter traffic based on source IP addresses. This is a crucial aspect of how ACLs manage and regulate traffic flow in network environments. Standard ACLs primarily focus on filtering traffic based solely on the source IP address, allowing or denying packets from specific hosts or networks. This capability is essential for enforcing security policies by controlling which devices can access the network or communicate with others. Extended ACLs, on the other hand, while having additional filtering features such as the ability to evaluate destination IP addresses, protocols, and even port numbers, still retain the functionality to filter based on the source IP address. This feature enables network administrators to create more granular rules that can specify not only the source but also the type of traffic and the communication endpoints, allowing for complex traffic management strategies. The other options do not accurately represent a shared function of both types of ACLs. For instance, the ability to log traffic is more prevalent in extended ACLs, while standard ACLs do not inherently offer this feature. Also, both standard and extended ACLs can be applied beyond just routers; they can also be used on switches and various network devices that support ACL configurations. Lastly

10. What is the primary function of a security information and event management (SIEM) system?

A. To enhance software performance

B. To monitor and improve user satisfaction

C. To aggregate and analyze security data for threat detection

D. To manage hardware configurations

The primary function of a security information and event management (SIEM) system is to aggregate and analyze security data for threat detection. SIEM systems are designed to collect and correlate data from various sources within an organization's IT infrastructure, such as log files from servers, firewall records, and intrusion detection systems. By consolidating this information, a SIEM can provide real-time analysis of security alerts generated by applications and network hardware. The key aspect of SIEM is its ability to detect potential threats and incidents. Through advanced analytics and correlation rules, the system can identify unusual patterns or anomalies that may indicate a security breach or other malicious activity. For example, if multiple failed login attempts from different IP addresses are logged, a SIEM can flag this as a potential brute force attack. This functionality is essential for organizations looking to improve their overall security posture, respond swiftly to incidents, and comply with regulatory requirements regarding the monitoring and reporting of security events. The other options refer to functions that do not align with the primary objectives of a SIEM; performance enhancement, user satisfaction, and hardware management are outside the main scope of what a SIEM system is designed to do.

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://nsvtmodule2.examzify.com

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

SAMPLE