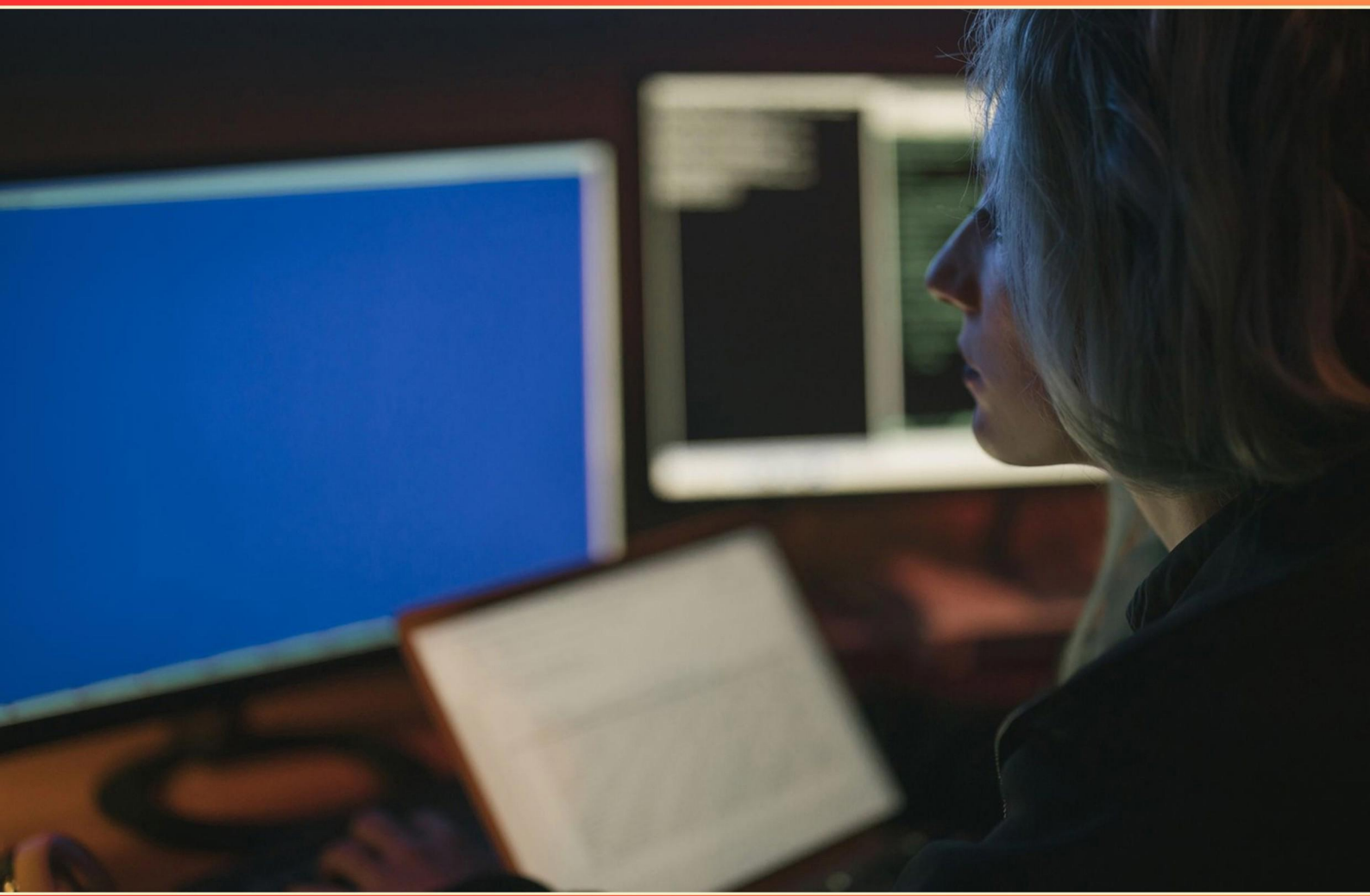
NETWORK SECURITY VULNERABILITY TECHNICIAN (NSVT) MODULE 2 PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

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

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. **Which of the following tools is commonly used for penetration testing?**
   - A. An employee scheduling tool
   - B. Metasploit
   - C. A financial analysis software
   - D. An email marketing platform

2. **Which method is used to ensure timely detection of connection failures in TCP?**
   - A. Ping
   - B. Keepalives
   - C. SNMP traps
   - D. Heartbeat signals

3. **What is the primary function of a VPN?**
   - A. To speed up internet connection
   - B. To create a secure connection over the internet
   - C. To monitor network traffic
   - D. To store data remotely

4. **What should organizations regularly conduct to enhance their security posture?**
   - A. Updated user training sessions
   - B. Routine vulnerability assessments
   - C. Frequent social media campaigns
   - D. Increased advertising for their services

5. **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

SAMPLE

6. How does Restrict mode of port security operate?

A. It drops all incoming traffic

B. It behaves like Protect Mode and increments SecurityViolation

C. It allows all traffic but flags violations

D. It sends all MAC address information to the main server

7. What is the role of the physical layer in a router's defense strategy?

A. First layer of defense

B. Second layer of defense

C. Last layer of defense

D. Application layer defense

8. What are the main types of network vulnerabilities?

A. Economic vulnerabilities, software vulnerabilities, and physical vulnerabilities

B. Software vulnerabilities, hardware vulnerabilities, and human vulnerabilities

C. Cloud vulnerabilities, network design vulnerabilities, and application vulnerabilities

D. Political vulnerabilities, infrastructure vulnerabilities, and service vulnerabilities

9. What is the function of WSAV in network security?

A. To block unauthorized access from external networks

B. To serve as a proxy server for shipboard networks

C. To act as a firewall for all internal communications

D. To provide internet access to all onboard systems

10. What is an exploit?

A. A software update designed to fix vulnerabilities

B. A piece of software that takes advantage of vulnerabilities

C. A type of anti-virus software

D. A network monitoring tool

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which of the following tools is commonly used for penetration testing?

A. An employee scheduling tool

B. Metasploit

C. A financial analysis software

D. An email marketing platform

Metasploit is a widely used penetration testing tool that enables security professionals to identify and exploit vulnerabilities in systems and networks. It provides a robust framework for developing and executing exploit code against remote targets, making it a vital resource in the field of cybersecurity. In the context of penetration testing, Metasploit offers a variety of pre-built exploits, payloads, and auxiliary modules that allow testers to simulate attacks and assess the security posture of an organization. This capability helps organizations understand their vulnerabilities and mitigate potential risks before they can be exploited by malicious actors. The other options are unsuitable for penetration testing as they serve entirely different purposes. An employee scheduling tool is designed for workforce management, financial analysis software focuses on managing and analyzing financial data, and an email marketing platform is used for creating and managing email campaigns. None of these tools have any functionality relevant to testing the security of networks or systems.

2. Which method is used to ensure timely detection of connection failures in TCP?

A. Ping

B. Keepalives

C. SNMP traps

D. Heartbeat signals

Using keepalives is a method that provides timely detection of connection failures in TCP. This mechanism involves sending periodic signals or packets at predefined intervals to ensure that a connection is still alive and functional. If the sender does not receive a response from the receiver within a certain timeframe, it can determine that the connection has failed and take appropriate action, such as attempting to reconnect or alerting the necessary systems or users to the issue. Ping, while useful for checking if a host is reachable, does not provide the same level of ongoing connection management as keepalives. Simple pings may indicate that a host is alive, but they do not necessarily confirm that an established connection is still active. Similarly, SNMP traps are more about monitoring network devices and responding to specific events rather than directly managing TCP connection states. Heartbeat signals can serve a similar function to keepalives but are generally more associated with application-level protocols rather than the inherent TCP protocol itself. Hence, keepalives are specifically designed for the purpose of connection status monitoring within the TCP protocol framework.

SAMPLE

3. What is the primary function of a VPN?

A. To speed up internet connection

B. To create a secure connection over the internet

C. To monitor network traffic

D. To store data remotely

The primary function of a VPN, or Virtual Private Network, is to create a secure connection over the internet. VPNs achieve this by encrypting the user's internet traffic and routing it through a secure server, which helps protect sensitive data from being intercepted by hackers or unauthorized entities. This secure tunnel not only safeguards private information but also allows users to access resources on the internet as if they were connected to a local network, improving privacy and security. By establishing a secure connection, VPNs are particularly beneficial for users who are accessing the internet over unsecured networks, such as public Wi-Fi, where data is more vulnerable to interception. In contrast, while other choices might touch on aspects of internet connectivity or security, they do not encapsulate the core purpose of a VPN, which is primarily focused on ensuring a secure communication channel.

4. What should organizations regularly conduct to enhance their security posture?

A. Updated user training sessions

B. Routine vulnerability assessments

C. Frequent social media campaigns

D. Increased advertising for their services

Routine vulnerability assessments are essential for organizations to regularly conduct as they systematically identify, evaluate, and prioritize security weaknesses within their infrastructure. These assessments allow organizations to discover potential vulnerabilities before they can be exploited by malicious actors, thereby enhancing their overall security posture. By engaging in these assessments, organizations can implement necessary updates, patches, or remedial actions to mitigate risks effectively. This proactive approach not only protects sensitive data and systems but also helps in complying with industry regulations and standards, fostering a culture of ongoing security awareness and vigilance. Thus, routine vulnerability assessments form a critical component of a comprehensive cybersecurity strategy.

5. 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.

EXAMPLE

6. How does Restrict mode of port security operate?

A. It drops all incoming traffic

B. It behaves like Protect Mode and increments SecurityViolation

C. It allows all traffic but flags violations

D. It sends all MAC address information to the main server

In the context of port security on networking devices, Restrict mode operates similarly to Protect mode, with an important distinction regarding how it handles security violations. When port security is configured in Restrict mode, if a violation occurs—meaning an unauthorized device attempts to connect to the port—the switch will not only drop the traffic from this device but also increment the SecurityViolation counter. This provides a way to monitor and register instances where policies are breached, which can aid in network management and security compliance. The ability to flag violations while still allowing legitimate traffic makes Restrict mode particularly useful for maintaining network security without completely blocking valid connections. This mode thus serves as a proactive measure to protect the network while also keeping an eye on security breaches, which can help in making informed decisions about network access and potential adjustments needed in security policies.

7. What is the role of the physical layer in a router's defense strategy?

A. First layer of defense

B. Second layer of defense

C. Last layer of defense

D. Application layer defense

The physical layer plays a crucial role in a router's defense strategy as it serves as the first line of defense against various types of attacks and vulnerabilities. This layer is responsible for the actual physical connection between devices, including how data is transmitted over cables, fibers, or wirelessly. By securing the physical layer, organizations can mitigate risks such as unauthorized access to network hardware, interception of data, and environmental threats. For instance, ensuring that routers and switches are in secure environments helps prevent physical tampering or theft, which could otherwise lead to breaches or data loss. Furthermore, the integrity and security of communication at the physical layer lay the groundwork for higher layers of defense since all data and services depend on a functional and safeguarded physical medium. This foundational role makes it essential for maintaining the overall security posture of the network. In contrast, designations like second layer, last layer, or application layer defense do not accurately reflect the physical layer's position in the defense sequence. The emphasis on higher layers typically pertains to software and network protocols, but without secure physical infrastructure, those measures could easily be undermined.

SAMPLE

8. What are the main types of network vulnerabilities?

A. Economic vulnerabilities, software vulnerabilities, and physical vulnerabilities

B. Software vulnerabilities, hardware vulnerabilities, and human vulnerabilities

C. Cloud vulnerabilities, network design vulnerabilities, and application vulnerabilities

D. Political vulnerabilities, infrastructure vulnerabilities, and service vulnerabilities

The identification of software vulnerabilities, hardware vulnerabilities, and human vulnerabilities as the main types of network vulnerabilities is a widely recognized classification in the field of network security. Software vulnerabilities pertain to flaws or weaknesses in software applications, operating systems, or services that can be exploited by attackers. This can involve anything from coding errors to misconfigurations that allow unauthorized access or denial of service. Keeping software up to date and employing security measures like patching can mitigate these vulnerabilities. Hardware vulnerabilities relate to the physical components of the network, including routers, switches, and computers. These may involve security weaknesses in the design, manufacturing, or configuration of devices, which can be exploited through physical access or remote attacks. Ensuring that hardware components are secured and monitored is crucial to maintaining network integrity. Human vulnerabilities encompass the actions and behaviors of individuals that can lead to security breaches. This includes inadequate security awareness, social engineering attacks, and insider threats. By providing proper training, implementing strict access controls, and fostering a security-conscious culture within an organization, many human vulnerabilities can be addressed effectively. Comparatively, the other choices include terms that either point to less standard categories or merge unrelated domains, such as economic and political vulnerabilities, which do not directly pertain to network security itself

9. What is the function of WSAV in network security?

A. To block unauthorized access from external networks

B. To serve as a proxy server for shipboard networks

C. To act as a firewall for all internal communications

D. To provide internet access to all onboard systems

The correct answer pertains to the role of WSAV (Web Security Application Virtualization) in network security, particularly its function as a proxy server. In the context of shipboard networks, using WSAV allows for effective management and filtering of internet traffic. As a proxy server, WSAV can monitor and control the data that enters and leaves the network. This helps enhance security by preventing direct access to the internal network from external sources while still allowing users onboard to access the internet safely. By serving as a mediator, WSAV not only helps in protecting sensitive information and systems from potential cyber threats but also optimizes bandwidth usage and improves the overall efficiency of internet connectivity for onboard systems. This is crucial in a maritime environment where both usability and security are of high importance. In contrast, other roles such as blocking unauthorized access, acting as a firewall for internal communication, or providing general internet access don't accurately represent the specific responsibilities or capabilities of WSAV as a proxy server. The focus here is on its function to manage and filter traffic, which is central to maintaining security in the context described.

SAMPLE

10. What is an exploit?

A. A software update designed to fix vulnerabilities

B. A piece of software that takes advantage of vulnerabilities

C. A type of anti-virus software

D. A network monitoring tool

An exploit is defined as a piece of software or a sequence of commands that takes advantage of vulnerabilities or weaknesses in a system, application, or software. Its primary purpose is to manipulate the system in a way that the creator intends, which often leads to unauthorized access, control, or data theft. Exploits are critical for understanding cyber threats, as they highlight how attackers can leverage existing flaws to compromise security. The other options do not accurately define an exploit. Software updates designed to fix vulnerabilities aim to enhance security and prevent exploits from succeeding. Anti-virus software is crafted to detect and mitigate threats, including exploits, while a network monitoring tool is used to oversee and analyze network traffic. These tools serve protective or managerial functions rather than taking advantage of vulnerabilities. Thus, understanding an exploit centers on recognizing its role in cyber security threats rather than the preventive or supportive measures represented by the other options.

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