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

Study Guide

Everything you need from our exam experts!

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 type of logging can provide messages for multiple sessions simultaneously?**
   - **A. Terminal Line Logging**
   - **B. Console Logging**
   - **C. Event Logging**
   - **D. System Console Logging**

2. **What is the primary function of Keepalives in a TCP connection?**
   - **A. To enhance data throughput**
   - **B. To ensure the connection is still active**
   - **C. To verify data integrity**
   - **D. To increase connection speed**

3. **What VPN protocol is known for its robust encryption and policy-based traffic determination?**
   - **A. IPSEC (Internet Protocol Security)**
   - **B. SSL/TLS Protocol**
   - **C. PPTP (Point-to-Point Tunneling Protocol)**
   - **D. L2TP (Layer 2 Tunneling Protocol)**

4. **What is the common key length used in AES for encryption?**
   - **A. 128 bits**
   - **B. 256 bits**
   - **C. 512 bits**
   - **D. 1024 bits**

5. **What is the process of determining if access can be granted based on a credential?**
   - **A. Authentication**
   - **B. Authorization**
   - **C. Identification**
   - **D. Access Control**

6. Which factors are considered in the authentication method?

A. Knowledge and location

B. Knowledge; possession; inherence

C. Behavior and identification

D. All of the above

7. 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

8. What does POP3 do in its default state regarding username and password information?

A. Encrypts it for security

B. Sends it in plain text

C. Stores it securely

D. Obfuscates it for safety

9. What is referred to as "something you have" in network security?

A. Knowledge Factor

B. Inherence Factor

C. Tokens and Certificates

D. Access Control

10. What encryption algorithm is primarily used by the Department of Defense?

A. AES

B. RSA

C. SHA-256

D. Blowfish

Answers

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

Explanations

1. Which type of logging can provide messages for multiple sessions simultaneously?

A. Terminal Line Logging

B. Console Logging

C. Event Logging

D. System Console Logging

Terminal Line Logging is the correct choice because it is specifically designed to capture logging messages from multiple sessions concurrently. This type of logging enables the monitoring and recording of events occurring across different terminal sessions, making it suitable for environments where multiple administrators may be accessing the system at the same time, such as in network device management. Terminal Line Logging allows each session's output to be logged independently, which can be essential for troubleshooting, auditing, and forensic analysis. This capability makes it an effective tool in a multi-user setting, as it ensures that logs from various sessions do not overlap and can be traced back to specific user activities. In contrast, console logging typically provides access to log messages directed to the device's console but usually reflects the output of only one active console session. Event logging primarily focuses on logging specific system events and may not be designed for session-based logging. System console logging is similar to console logging in that it captures output from the system console, generally limited to a single session's output at any moment. Each of these other options has its specific use cases but does not provide the simultaneous multi-session logging capability that Terminal Line Logging offers.

2. What is the primary function of Keepalives in a TCP connection?

A. To enhance data throughput

B. To ensure the connection is still active

C. To verify data integrity

D. To increase connection speed

The primary function of Keepalives in a TCP connection is to ensure that the connection remains active. This mechanism is particularly important in long-lived connections where idle periods may occur. Keepalives help to confirm that both ends of the connection are still responsive, which is crucial for maintaining the reliability that TCP offers. When Keepalive messages are sent, they serve as a way for the sending device to check if the receiving device is still available and functioning properly. If the receiving device is down or if there are issues with network connectivity, the sender can detect this through the absence of a response to the Keepalive messages. This proactive monitoring helps to prevent scenarios where the connection appears to be active when, in fact, it has silently failed. In contrast, enhanced data throughput, verification of data integrity, and increases in connection speed are related to different aspects of TCP operation, such as congestion control and flow control mechanisms, but they do not pertain directly to the role of Keepalive messages. The focus of Keepalives is primarily about maintaining the status of the connection rather than performance enhancements or data verification.

3. What VPN protocol is known for its robust encryption and policy-based traffic determination?

A. IPSEC (Internet Protocol Security)

B. SSL/TLS Protocol

C. PPTP (Point-to-Point Tunneling Protocol)

D. L2TP (Layer 2 Tunneling Protocol)

IPSec is well-regarded for its strong encryption capabilities and ability to enforce policy-based traffic determination. It works at the network layer and can secure both IPv4 and IPv6 traffic, providing a framework for authenticating and encrypting data communications. This robust encryption is one of the key differentiators for IPSec, as it utilizes protocols such as AH (Authentication Header) and ESP (Encapsulating Security Payload) to ensure confidentiality, integrity, and authenticity of data packets being transmitted. Additionally, IPSec allows for intricate configuration options, enabling network administrators to implement policies that determine how specific types of traffic are handled, including how to route traffic and which encryption methods to use based on various criteria. This level of customization makes IPSec particularly suitable for organizations that need to implement specific security policies alongside its strong encryption features. The other protocols listed do not have the same level of focus on both robust encryption and policy-based traffic management. For instance, SSL/TLS is primarily used for securing web traffic, PPTP is known for its ease of use but lacks strong security features compared to IPSec, and L2TP without IPSec does not provide encryption on its own. This context illustrates why IPSec stands out as the best choice among the options provided

4. What is the common key length used in AES for encryption?

A. 128 bits

B. 256 bits

C. 512 bits

D. 1024 bits

The common key length used in AES (Advanced Encryption Standard) for encryption is indeed 128 bits. AES is a symmetric encryption algorithm widely used across various security applications and protocols. It supports key lengths of 128, 192, and 256 bits, with 128 bits being the most frequently used in practice. This key length provides a strong level of security, balancing performance and encryption strength. Choosing 128 bits as the key length in AES is sufficient for most applications, as it has been found to be secure against brute-force attacks, while also offering better performance compared to the larger key sizes. The longer key sizes, such as 192 and 256 bits, are used in specific contexts where heightened security is paramount, but they come at a cost of increased processing overhead. Using key lengths of 512 or 1024 bits does not apply to AES, as the algorithm does not support those key sizes. Instead, such lengths may be associated with other encryption methodologies or specific cryptographic practices that are not standard within AES.

5. What is the process of determining if access can be granted based on a credential?

A. Authentication

B. Authorization

C. Identification

D. Access Control

The process of determining if access can be granted based on a credential is known as authorization. Authorization takes place after identification and authentication have occurred. During this phase, the system evaluates whether a user has the permissions necessary to access a specific resource or perform a certain action based on their credentials. For example, once a user has been authenticated (their identity confirmed) using their credentials, the system checks against predefined access control policies to ensure that this user is authorized to access the requested resource. This process is critical in ensuring that users only have access to information and resources they are permitted to interact with, thus maintaining security and integrity within the network. In contrast, the other options relate to different aspects of security. Identification refers to the process of claiming an identity, while authentication is about verifying that identity. Access control encompasses both authorization and the rules governing how access is granted or restricted. Therefore, authorization is the specific process that directly addresses the question regarding granting access based on credentials.

6. Which factors are considered in the authentication method?

A. Knowledge and location

B. Knowledge; possession; inherence

C. Behavior and identification

D. All of the above

The correct choice focuses on the primary factors involved in the authentication method, which are knowledge, possession, and inherence. Knowledge refers to something the user knows, such as a password or PIN. Possession relates to something the user has, like a security token or a smart card. Inherence involves biological traits specific to the user, such as fingerprints or voice recognition. Together, these three factors encompass the core principles of authentication that ensure users can be reliably verified before gaining access to systems or information. This multifactor approach enhances security, as it requires various types of verification to be successful. In contrast, while the other mentioned factors such as behavior and identification can play a role in security processes, they do not encompass the fundamental aspects of authentication methods as directly as knowledge, possession, and inherence do. Therefore, the focus on the latter trio in the correct answer provides a clearer and more comprehensive understanding of authentication methodologies.

7. 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.

8. What does POP3 do in its default state regarding username and password information?

A. Encrypts it for security

B. Sends it in plain text

C. Stores it securely

D. Obfuscates it for safety

In its default state, POP3 (Post Office Protocol version 3) sends username and password information in plain text. This means that when a client connects to the mail server to retrieve emails, the credentials are transmitted without any form of encryption. As a result, anyone monitoring the network traffic can easily capture and read this sensitive information, which poses significant security risks. Consequently, it's generally recommended to use a more secure protocol, such as POP3 over SSL/TLS (known as POP3S), which encrypts the connection and provides a much higher level of security for transmitting credentials and email data.

9. What is referred to as "something you have" in network security?

A. Knowledge Factor

B. Inherence Factor

C. Tokens and Certificates

D. Access Control

In network security, the term "something you have" pertains to physical objects or unique digital assets that a user possesses, which can be used to authenticate their identity. Tokens and certificates are classic examples of these assets. They can take the form of smart cards, key fobs, or digital certificates stored on a device. When a user presents a token or certificate as part of a multi-factor authentication process, they demonstrate physical possession of the item, enhancing the security of access control measures. This concept is associated with one of the three factors of authentication: something you know (passwords), something you have (tokens and certificates), and something you are (biometric identifiers). By utilizing "something you have," security systems can ensure that even if a password is compromised, an unauthorized user still would not be able to gain access without also possessing the physical token or certificate. This dual-layer of security significantly mitigates risks of unauthorized access.

10. What encryption algorithm is primarily used by the Department of Defense?

A. AES

B. RSA

C. SHA-256

D. Blowfish

The encryption algorithm primarily used by the Department of Defense is Advanced Encryption Standard, or AES. It was established as a standard to ensure secure encryption for sensitive government data. AES is recognized for its robust security features, efficiency in performance, and support for various key lengths (128, 192, and 256 bits), which allows for a flexible balance between security and performance. AES was selected through a rigorous process that evaluated multiple algorithms, making it a trusted choice for secure communications within government and military operations. Its widespread adoption stems from its resistance to known cryptographic attacks and the commitment to continual improvement against advancing technology. Other algorithms listed, while significant in their own right, serve different purposes or have different strengths. RSA is primarily used for encryption and digital signatures rather than bulk data encryption. SHA-256 is a hashing algorithm, not an encryption algorithm, used to generate a fixed-size hash from input data. Blowfish is an older symmetric key cipher known for speed but is not the current standard for securing sensitive government data.

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!