Network Security Vulnerability Technician (NSVT) Module 6 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. **What is the primary purpose of conducting regular security audits?**
   - A. To ensure software updates are regularly applied
   - B. To evaluate the effectiveness of security measures and identify areas for improvement
   - C. To develop a comprehensive IT strategy
   - D. To train staff on compliance regulations

2. **Which account is used for Master Repository replication and off-ship communications?**
   - A. eposql
   - B. proxy.epo
   - C. database.account
   - D. master.repos

3. **What is a significant characteristic of the password complexity for the CANES ESS account?**
   - A. Must include a username
   - B. Must have lowercase and uppercase letters
   - C. Must include an even number of characters
   - D. Must be no more than 12 characters long

4. **Describe what a brute-force attack entails.**
   - A. A method of gaining access to accounts through exhaustive guesswork of passwords or encryption keys
   - B. A technique to cause network congestion intentionally
   - C. A type of denial-of-service attack targeting specific applications
   - D. A strategy to encrypt files for ransom

5. **What does the term "social engineering" refer to in cybersecurity?**
   - A. The psychological manipulation of people to divulge confidential information
   - B. The design of secure systems based on user behavior
   - C. A method for encoding data to ensure privacy
   - D. The process of physically reinforcing secure access points

6. What is an encryption key?

A. A special code for accessing encrypted files

B. A string of bits used by an encryption algorithm to transform plaintext into ciphertext

C. A password used to gain entry to secure systems

D. A protocol for secure communication over the internet

7. How are CANES security boundaries separated?

A. ADNS Router Policies

B. Firewall Configurations

C. Network Address Translation

D. Intrusion Prevention Systems

8. Which tool is recognized as an open source software for collecting and preserving volatile data?

A. Helix Pro

B. Dumpit

C. Wireshark

D. FTK Imager

9. What is defined as a network security device that monitors and controls network traffic?

A. A router

B. A firewall

C. An IDS

D. A switch

10. What is the primary function of the Domain Name System (DNS) in network security?

A. It secures network connections from unauthorized access

B. It translates domain names into IP addresses

C. It stores user passwords securely

D. It monitors network traffic for breaches

Answers

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

Explanations

1. What is the primary purpose of conducting regular security audits?

A. To ensure software updates are regularly applied

B. To evaluate the effectiveness of security measures and identify areas for improvement

C. To develop a comprehensive IT strategy

D. To train staff on compliance regulations

Conducting regular security audits is crucial for evaluating the effectiveness of existing security measures and identifying areas for improvement. The primary purpose of a security audit is to assess whether current protocols, controls, and defenses are successfully protecting assets and data against threats. By systematically examining the security framework, organizations can uncover vulnerabilities, weaknesses, or misconfigurations that may have been overlooked. This process aids in ensuring compliance with security policies and regulations, making it easier to enhance overall security posture over time. While ensuring software updates, developing IT strategies, and training staff on compliance are important aspects of security management, they do not directly address the overarching goal of security audits. Audits specifically focus on analyzing security controls and validating their effectiveness, enabling organizations to take informed action based on the findings. Therefore, option B accurately represents the primary objective of regular security audits.

2. Which account is used for Master Repository replication and off-ship communications?

A. eposql

B. proxy.epo

C. database.account

D. master.repos

The account used for Master Repository replication and off-ship communications is proxy.epo. This account is specifically designed for managing communication between the ePolicy Orchestrator (ePO) server and other elements of the environment, such as agents or repositories across different servers or environments. In the context of ePO, this account plays a critical role in ensuring that data synchronization and replication functions properly, maintaining the integrity and consistency of security policies and other related data across the network. By utilizing this account, the system can effectively manage the flow of information and commands, allowing for seamless updates and communication. Understanding the function of proxy.epo helps clarify its importance in a network security framework, where efficient communication and data handling are vital for maintaining a secure and compliant environment.

3. What is a significant characteristic of the password complexity for the CANES ESS account?

A. Must include a username

B. Must have lowercase and uppercase letters

C. Must include an even number of characters

D. Must be no more than 12 characters long

The password complexity requirement for the CANES ESS account mandates that passwords must include both lowercase and uppercase letters. This characteristic enhances security by increasing the potential combinations of characters, making it more difficult for attackers to guess or crack the password using brute force methods. By requiring the use of both types of letters, the complexity of the password is significantly improved, thereby reducing the risk of unauthorized access. While there are other factors that may also play a role in password requirements, such as length or the inclusion of specific character types, the combination of lowercase and uppercase letters serves as a critical foundation for establishing stronger passwords. This practice aligns with widely accepted security guidelines that advocate for diverse character usage to protect sensitive accounts.

4. Describe what a brute-force attack entails.

A. A method of gaining access to accounts through exhaustive guesswork of passwords or encryption keys

B. A technique to cause network congestion intentionally

C. A type of denial-of-service attack targeting specific applications

D. A strategy to encrypt files for ransom

A brute-force attack involves systematically trying every possible combination of passwords or encryption keys until the correct one is found. This method relies on the computational power available to attempt numerous combinations in a relatively short period, making it a straightforward yet often effective way to compromise accounts if proper security measures are not in place. The attacker may use automated tools to accelerate this process, allowing them to test hundreds or thousands of potential passwords per second. In contrast, other methods mentioned involve different forms of attack. Network congestion and denial-of-service attacks focus on overwhelming services to disrupt availability rather than gaining access, while encryption for ransom refers to malware tactics aimed at extorting money rather than compromising passwords through guesswork. Therefore, the definition of a brute-force attack specifically aligns with exhaustive password or encryption key guessing, which directly pertains to the integrity and confidentiality of accounts.

5. What does the term "social engineering" refer to in cybersecurity?

A. The psychological manipulation of people to divulge confidential information

B. The design of secure systems based on user behavior

C. A method for encoding data to ensure privacy

D. The process of physically reinforcing secure access points

The term "social engineering" in cybersecurity specifically refers to the psychological manipulation of individuals to convince them to disclose confidential information. This technique relies on exploiting human psychology rather than technical hacking methods, making it a particularly insidious threat. Social engineers often create a sense of urgency, trust, or fear in order to trick individuals into providing sensitive data, such as passwords or account information. This understanding is crucial because it highlights the importance of user education and awareness in an organization's security posture. While technical safeguards are essential, addressing the human factor through training and awareness programs is vital in reducing the risk of social engineering attacks.

6. What is an encryption key?

A. A special code for accessing encrypted files

B. A string of bits used by an encryption algorithm to transform plaintext into ciphertext

C. A password used to gain entry to secure systems

D. A protocol for secure communication over the internet

An encryption key is fundamentally defined as a string of bits that is utilized by an encryption algorithm to convert plaintext into ciphertext. This process is essential in cryptography, as the algorithm uses the key to perform the transformation, ensuring that the information remains secure and can only be read by someone who possesses the corresponding decryption key. The strength and security of the encryption largely depend on the key's complexity and length; a longer and more random key tends to provide higher levels of security by making it more difficult for unauthorized parties to decrypt the information without access to the key. This concept underscores the vital role encryption keys play in securing data transmission and storage, making them an integral part of cybersecurity strategies. While other choices may touch on related concepts, they do not accurately capture the specific definition and function of an encryption key within the context of cryptography.

7. How are CANES security boundaries separated?

A. ADNS Router Policies

B. Firewall Configurations

C. Network Address Translation

D. Intrusion Prevention Systems

The separation of CANES (Converged Anti-jam Networking and Environmentally-Responsive Secure) security boundaries relies primarily on ADNS (Automatic Digital Network System) Router Policies. These policies are instrumental in defining how data flows within the network while maintaining secure boundaries. ADNS Router Policies provide a framework for routing decisions that consider both security and operational requirements. They help manage and enforce access controls and segmentation within the network, ensuring that sensitive information remains protected and is only accessible to authorized users and systems. By establishing distinct routing paths and configurations, these policies effectively delineate one security boundary from another within the CANES architecture. While other options like firewall configurations, network address translation, and intrusion prevention systems play significant roles in network security, they are not the primary tools for establishing the boundaries specific to CANES. Firewalls are typically used to monitor and control incoming and outgoing network traffic based on predetermined security rules. Network address translation maintains the integrity of private IP addresses while facilitating communication with external networks. Intrusion prevention systems are designed to detect and prevent potential threats within the network, focusing primarily on active threat management rather than boundary separation.

8. Which tool is recognized as an open source software for collecting and preserving volatile data?

A. Helix Pro

B. Dumpit

C. Wireshark

D. FTK Imager

Dumpit is recognized as an open-source tool specifically designed for collecting and preserving volatile data, such as data stored in RAM. It enables forensic investigators to capture memory images which can be critical for analysis, especially during investigations involving malware, rootkits, or running processes. By focusing on data that is temporarily stored in memory, Dumpit ensures that these ephemeral details are not lost when a system is powered down or when it is restarted. Other tools listed, while valuable for various aspects of data acquisition and analysis, do not specialize in the collection of volatile data in the same way. For instance, Helix Pro is a comprehensive forensic suite that may include capabilities for volatile data collection but is not solely recognized for this purpose. Wireshark is primarily a packet analysis tool used for network traffic examination rather than memory acquisition. FTK Imager is a powerful tool for imaging and forensic analysis of disk drives, and while it does offer some functionalities for memory acquisition, it is not an open-source software. Therefore, Dumpit stands out as the correct choice for the specific task of capturing volatile data.

9. What is defined as a network security device that monitors and controls network traffic?

A. A router

B. A firewall

C. An IDS

D. A switch

A firewall is specifically designed to monitor and control network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, filtering incoming and outgoing traffic to protect sensitive data and maintain the integrity of the network's resources. Firewalls can be hardware-based, software-based, or a combination of both, and they enforce policies to decide whether to allow or block specific traffic. While routers direct data packets between different networks, they do not inherently filter or monitor traffic for security purposes like a firewall does. Intrusion Detection Systems (IDS) also monitor network traffic but primarily focus on identifying potential security breaches, rather than controlling or filtering traffic directly. Switches operate at the data link layer and primarily manage the flow of data within a local area network (LAN) without focusing on security-driven traffic management. Thus, the role of a firewall in actively securing and controlling network access makes it the correct answer.

10. What is the primary function of the Domain Name System (DNS) in network security?

A. It secures network connections from unauthorized access

B. It translates domain names into IP addresses

C. It stores user passwords securely

D. It monitors network traffic for breaches

The primary function of the Domain Name System (DNS) is to translate domain names into IP addresses. This process is essential for the functioning of the internet, as users typically access websites via human-readable names, such as www.example.com, rather than numeric IP addresses like 192.0.2.1. When a user types a domain name into their web browser, the DNS resolution process occurs, whereby the DNS server converts that domain into its corresponding IP address, allowing the user's device to locate and connect to the necessary web server. This translation function is crucial for network security because it facilitates legitimate communications and connections across the internet. By ensuring that the correct IP addresses are resolved for requested domain names, DNS helps to maintain the integrity of network communications and can also play a role in mitigating certain types of cyber threats, such as phishing, by blocking malicious domain requests. While other options might touch on aspects of network security, they do not accurately reflect the fundamental role of DNS in this context. For instance, securing network connections and monitoring traffic involve different mechanisms and systems beyond the DNS's primary functionality.

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://nsvtmodule6.examzify.com

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