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 main function of the NCDOC?

A. Conduct cybersecurity training

B. Oversee malware analysis and reporting

C. Implement cybersecurity laws

D. Report financial impacts of cyber incidents

2. What is the key distinction between a threat and a vulnerability?

A. A threat is a potential cause of an unwanted incident, while a vulnerability is a weakness that can be exploited.

B. A vulnerability is always a natural disaster, while a threat is a man-made event.

C. A vulnerability can be eliminated, while a threat can be ignored.

D. A threat is always external, while a vulnerability is only internal.

3. How is CANES Agent deployment performed when Rogue Auto Push Task is disabled?

A. Automatically through system tree

B. Manually using frame package from system tree

C. System-generated scripts

D. Automatically from ePO

4. What type of cyber event is categorized as Cat 2?

A. User Level Intrusion (Incident)

B. Non-Compliance Activity (Event)

C. Investigating (Event)

D. Malicious Logic (Incident)

5. 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

6. What is the local logon account for the SQL Server Agent service in CANES?

A. sqlsrvagt

B. sqlagentuser

C. sqlsvragent

D. sqlagtadmin

7. What is meant by the term "attack surface"?

A. The number of users accessing a system

B. The totality of vulnerabilities in a system

C. The degree of system complexity

D. The range of security measures implemented

8. Which TCP port is related to the Domain Name System (DNS)?

A. 80

B. 53

C. 21

D. 443

9. What term describes unauthorized access to an information system?

A. Intrusion

B. Violation

C. Attack

D. Access

10. Which service in CANES is specifically designed for user authentication and identity verification?

A. Identification, Authentication, and Authorization Service CI

B. Database Security Service

C. User Session Management CI

D. Network Access Control System

Answers

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

Explanations

1. What is the main function of the NCDOC?

A. Conduct cybersecurity training

B. Oversee malware analysis and reporting

C. Implement cybersecurity laws

D. Report financial impacts of cyber incidents

The primary function of the National Cybersecurity and Communications Integration Center (NCDOC) is to oversee malware analysis and reporting. This role is crucial in the context of cybersecurity because it involves monitoring, analyzing, and disseminating information about malware threats. By understanding how different malware works and its impact on systems, the NCDOC helps to improve the overall security posture of organizations by providing them with actionable intelligence. This analysis is also pivotal in developing strategies to mitigate threats, enabling a swift and informed response to incidents. While conducting cybersecurity training, implementing laws, and reporting financial impacts are important aspects of broader cybersecurity efforts, they do not specifically define the core mission of the NCDOC. The center's focus is primarily on the technical aspects of cybersecurity threats, which reinforces its role in protecting national interests against malware and other cyber threats.

2. What is the key distinction between a threat and a vulnerability?

A. A threat is a potential cause of an unwanted incident, while a vulnerability is a weakness that can be exploited.

B. A vulnerability is always a natural disaster, while a threat is a man-made event.

C. A vulnerability can be eliminated, while a threat can be ignored.

D. A threat is always external, while a vulnerability is only internal.

The key distinction captured in the correct answer is fundamental to understanding the concepts of threat and vulnerability within the realm of network security. A threat is defined as a potential cause of an unwanted incident, which means it represents any circumstance or event that has the potential to cause harm to a system or organization. For instance, threats can include anything from natural disasters to cyberattacks, and they typically indicate something that might happen or could occur in the future. On the other hand, a vulnerability refers to a weakness in a system, application, or network that can be exploited by threats. Vulnerabilities may manifest in various forms, such as unpatched software, misconfigured security settings, or inherent flaws in the system architecture. When a vulnerability is present, it creates the opportunity for a threat to materialize and cause damage. Understanding this distinction is essential for effectively assessing risks and implementing appropriate security measures. An organization can focus on fortifying its defenses against known vulnerabilities to reduce the likelihood of a successful threat eventuating into a security incident.

3. How is CANES Agent deployment performed when Rogue Auto Push Task is disabled?

A. Automatically through system tree

B. Manually using frame package from system tree

C. System-generated scripts

D. Automatically from ePO

The deployment of the CANES Agent when the Rogue Auto Push Task is disabled involves a manual process. In this scenario, the administrator would need to utilize a frame package from the system tree to deploy the agent. This approach provides control over which systems receive the agent, allowing for targeted deployments rather than relying on an automated process that may not be in place due to the disabling of the Rogue Auto Push Task. This manual deployment could be necessary in environments where users want to ensure that only certain devices receive the agent or when specific configurations are needed before installation. Using the frame package, an administrator can download the necessary files and distribute them to chosen endpoints, ensuring compliance with the organization's policies. The other options involve automated processes, which are not applicable here given that the Rogue Auto Push Task has been disabled. This further affirms that manual intervention is required to ensure proper functionality and compliance with the deployment strategy.

4. What type of cyber event is categorized as Cat 2?

A. User Level Intrusion (Incident)

B. Non-Compliance Activity (Event)

C. Investigating (Event)

D. Malicious Logic (Incident)

A Cat 2 cyber event refers specifically to a user-level intrusion incident. This categorization indicates that a user, either maliciously or unintentionally, has gained unauthorized access to a system or network, potentially compromising sensitive data or resources. The classification system often recognizes user-level intrusions as significant threats because they can lead to data breaches or other harmful activities. User-level intrusions are typically characterized by actions taken by individuals who have legitimate access to a system but exploit their privileges improperly. This makes them dangerous as they can bypass certain security measures that guard against external threats. The other categories, while also relevant, do not match the definition for a Cat 2 event. Non-compliance activities involve falling short of compliance standards but do not necessarily indicate an active intrusion or incident. Investigating events pertain to the process of analyzing potential incidents rather than being classified as an incident themselves. Malicious logic incidents involve malicious code or software attacks but are categorized separately, emphasizing the nature of the attack rather than user behavior. Thus, the identification of user-level intrusion as a Cat 2 incident aligns with standards used to evaluate and respond to cybersecurity threats.

5. 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.

6. What is the local logon account for the SQL Server Agent service in CANES?

A. sqlsrvagt

B. sqlagentuser

C. sqlsvragent

D. sqlagtadmin

The local logon account for the SQL Server Agent service in a system such as CANES is designated as "sqlsrvagt." This specific account is created when SQL Server is installed and configured to manage tasks such as scheduling jobs, monitoring SQL Server, and alerting users. Using a dedicated service account like "sqlsrvagt" enhances security by segregating permissions and roles related to the SQL Server Agent from those of the actual SQL Server database engine. In practice, service accounts like this are critical for managing operational duties while ensuring that they adhere to the principle of least privilege, which minimizes the account's access to only what is necessary. The naming convention indicates that it is specifically linked to the SQL Server Agent functionality, making it easy to identify and manage. The other options do not represent the standard local logon account for SQL Server Agent, as they either imply different roles or are not recognized naming conventions for the SQL Server Agent service. Understanding the specific function and naming conventions of accounts is essential for efficient system management and security best practices in database environments.

7. What is meant by the term "attack surface"?

A. The number of users accessing a system

B. The totality of vulnerabilities in a system

C. The degree of system complexity

D. The range of security measures implemented

The term "attack surface" refers to the totality of vulnerabilities in a system. It encompasses all the different points where an unauthorized user can try to enter data or extract data from an environment. Understanding the attack surface is crucial for security professionals because it helps identify where an attacker might exploit weaknesses within the software, hardware, or network. By assessing the attack surface, organizations can strengthen their defenses by patching vulnerabilities, reducing exposed services, and minimizing the potential entry points that could be exploited during an attack. This understanding allows for more effective management of security risks, leading to a more robust and secure environment. The other choices, while related to different aspects of system security and management, do not directly capture the essence of the attack surface concept. For instance, the number of users accessing a system does not necessarily correlate to vulnerabilities, and system complexity can influence security but does not define the attack surface itself. Similarly, security measures implemented affect the overall security posture but do not quantify the attack surface either.

8. Which TCP port is related to the Domain Name System (DNS)?

A. 80

B. 53

C. 21

D. 443

The Domain Name System (DNS) primarily operates using port 53. DNS is a critical component of internet functionality, as it translates human-readable domain names (like www.example.com) into IP addresses that computers can use to identify each other on the network. When a DNS query is made, it typically utilizes User Datagram Protocol (UDP) on port 53 for the requests, while it may use Transmission Control Protocol (TCP) on the same port for larger queries and zone transfers. The other options correspond to different services: port 80 is used for HTTP web traffic, port 21 is used for FTP (File Transfer Protocol), and port 443 is designated for HTTPS, which is HTTP over SSL/TLS for secure communications. Each port serves specific purposes within the realm of networking, but for DNS, the appropriate port is exclusively port 53.

9. What term describes unauthorized access to an information system?

A. Intrusion

B. Violation

C. Attack

D. Access

The term that describes unauthorized access to an information system is "Intrusion." Intrusion occurs when an individual gains access to a system without permission, typically by exploiting vulnerabilities or weaknesses in security measures. This concept is fundamental to cybersecurity as it highlights the risk of unauthorized entities gaining access to sensitive information, which can lead to data breaches, system compromise, and a host of malicious activities. In contrast, while terms like "violation," "attack," and "access" relate to breaches of security, they carry different connotations. A violation often refers to a breach of policy or law rather than merely unauthorized technical access. An attack is more aggressive and may involve using various methods to disrupt or damage a system beyond just accessing it. Lastly, access is a general term that does not imply unauthorized entry; it can mean legitimate entry following proper protocols. Thus, "Intrusion" specifically encapsulates the essence of unauthorized access, making it the most accurate choice.

10. Which service in CANES is specifically designed for user authentication and identity verification?

A. Identification, Authentication, and Authorization Service CI

B. Database Security Service

C. User Session Management CI

D. Network Access Control System

The Identification, Authentication, and Authorization Service CI is specifically designed for user authentication and identity verification within the CANES framework. This service plays a critical role in ensuring that users are properly identified before granting access to network resources. It establishes user identities, confirms that these identities are legitimate, and manages the permissions associated with each user to ensure that they only have access to resources for which they are authorized. This service encompasses the processes of verifying user credentials, such as passwords or biometric data, and linking them to corresponding access rights, making it a foundational component for maintaining security and integrity in a networked environment. In the context of network security, ensuring robust authentication mechanisms is crucial to protecting sensitive data and preventing unauthorized access. Other services mentioned, such as Database Security Service and User Session Management CI, contribute to the overall security architecture but do not focus specifically on the processes of user authentication and identity verification. Similarly, a Network Access Control System is concerned with controlling network access based on established security policies but does not directly provide the user authentication functionalities that the Identification, Authentication, and Authorization Service CI does.

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!