Network Security Vulnerability Technician (NSVT) Module 4 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 type of ePo group is designated as non-removable?

A. Regular Group

B. Lost and Found

C. Temporary Group

D. Managed Group

2. Which of the following best describes an inactive system?

A. It is managed by the ePO server

B. It has an installed Trellix Agent and communicates regularly

C. It has not been detected by a sensor for a determined period

D. It is fully operational and monitored

3. In ESS, what mode is indicated when traffic is allowed and events are recorded and sent to the ePO server?

A. Standard Mode

B. Monitor Mode

C. Adaptive Mode

D. Safe Mode

4. Which of the following accurately describes the relationship between AC and other security applications?

A. They must be used together at all times

B. AC cannot operate without HIPS or ENS

C. Disabling AC memory-protection can prevent conflicts

D. They serve entirely different purposes

5. What type of packet filtering uses stateful inspection to maintain awareness of all connections?

A. Static Filtering

B. Stateful Filtering

C. Dynamic Filtering

D. Network Filtering

6. Signature-based detection compares signatures against which of the following?

A. Scheduled events

B. Known patterns

C. Observed events

D. Temporary logs

7. What type of packet filtering does a firewall perform when it pays no attention to whether a packet is part of an existing stream of traffic?

A. Stateful

B. Stateless

C. Full inspection

D. Deep packet inspection

8. Which term describes devices not managed under DLP but can be monitored?

A. Control Group

B. Unmanageable

C. Unmanaged

D. Unrestricted

9. What is defined as a pattern that corresponds to a known threat?

A. Signature

B. Protocol

C. Event

D. Broker

10. What can be a reason for a system to be classified as a rogue?

A. It has a functioning Trellix Agent

B. It is detected by the sensor regularly

C. It was not detected by a sensor within a determined timeframe

D. It is fully registered with the ePO server

Answers

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

Explanations

1. What type of ePo group is designated as non-removable?

A. Regular Group

B. Lost and Found

C. Temporary Group

D. Managed Group

The designation of the Lost and Found group as non-removable plays a crucial role in the management of devices and user accounts within an ePolicy Orchestrator (ePO) environment. This group is typically used to automatically collect systems that are not classified under any other existing group, ensuring that devices are not left unmanaged. When a system does not fit into any predefined categories, it is automatically assigned to this Lost and Found group. This design ensures that all devices are accounted for, allowing for better oversight and management from a security standpoint. Since it serves a unique purpose in maintaining visibility over potentially unclassified systems, the Lost and Found group is inherently non-removable, guaranteeing that administrators can always access these unassigned systems for analysis or reallocation into appropriate groups. In contrast, other types of groups like Regular, Temporary, and Managed groups serve specific purposes related to task allocations, permissions, or temporary assignments, all of which can be modified or removed as needed based on the organization's requirements. This key distinction emphasizes the critical importance of the Lost and Found group within the ePO framework, acting as a safeguard against unattended system management.

2. Which of the following best describes an inactive system?

A. It is managed by the ePO server

B. It has an installed Trellix Agent and communicates regularly

C. It has not been detected by a sensor for a determined period

D. It is fully operational and monitored

An inactive system is best described as one that has not been detected by a sensor for a determined period. This indicates that the system is not currently active within the monitored environment. Inactive systems generally do not generate any traffic or communicate with network services, leading to them being undetected by the monitoring systems for a set amount of time. The other options describe scenarios that imply the system is operational or active. An ePO server managing a system suggests an active management status. An installed Trellix Agent that communicates regularly indicates the system is active and functioning within the network. A fully operational and monitored system definitely does not align with the definition of an inactive system, as being monitored involves ongoing interaction and detection by security mechanisms. Thus, the definition of an inactive system hinges on the lack of detection or communication over a designated timeframe.

3. In ESS, what mode is indicated when traffic is allowed and events are recorded and sent to the ePO server?

A. Standard Mode

B. Monitor Mode

C. Adaptive Mode

D. Safe Mode

In the context of ESS (Endpoint Security Suite), the mode that indicates traffic is allowed and events are recorded and sent to the ePO (ePolicy Orchestrator) server is adaptive mode. This mode operates with a focus on adjusting to the environment and traffic patterns while maintaining security protocols. Adaptive mode allows the system to permit regular traffic to flow while actively monitoring for anomalies or threats. It records events related to the network traffic and sends this information to the ePO server for analysis and response, enabling a comprehensive approach to security management. This dynamic adaptation to network conditions is crucial for balancing usability and security, making adaptive mode particularly effective in environments where flexibility is needed without compromising safety. In contrast, other modes such as standard mode typically involve more rigid configurations, while monitor mode would primarily focus on observation rather than allowing traffic. Safe mode, on the other hand, tends to limit operations significantly in order to protect the system, thereby not meeting the criteria for allowed traffic while also sending alerts or events to ePO.

4. Which of the following accurately describes the relationship between AC and other security applications?

A. They must be used together at all times

B. AC cannot operate without HIPS or ENS

C. Disabling AC memory-protection can prevent conflicts

D. They serve entirely different purposes

The correct choice highlights a practical aspect of configuring security applications, specifically the relationship between access control (AC) and its interaction with memory protection features in other security solutions. Disabling memory protection can sometimes resolve conflicts that arise when multiple security applications attempt to operate in the same environment. This implies that these systems may interact in a way that leads to performance issues or errors if not configured correctly. By managing memory protection settings, administrators can ensure smoother operation and compatibility between the various security solutions. While other options suggest that security applications must always work in tandem, depend on one another, or serve completely separate functions, the reality is that while each application can have its own role, there can be situations where adjusting one aspect—such as memory protection settings—can facilitate better integration and performance among them. This understanding is crucial for maintaining an effective security posture while minimizing potential conflicts within the security ecosystem.

5. What type of packet filtering uses stateful inspection to maintain awareness of all connections?

A. Static Filtering

B. Stateful Filtering

C. Dynamic Filtering

D. Network Filtering

Stateful filtering is a type of packet filtering that utilizes stateful inspection technology to keep track of the state of active connections and to determine whether a packet is part of an established connection or a new connection attempt. This method enhances security by allowing or denying packets based on the context of a connection rather than just individual packet attributes. In stateful inspection, the firewall keeps a record of each connection and remembers the state of the connection, such as whether it is in the process of being setup, established, or terminated. This is contrasted with methods such as static filtering, which only examines individual packets based on predefined rules without accounting for the overall connection state. By utilizing this awareness, stateful filtering can provide more sophisticated and dynamic traffic control that adjusts to the behavior of network traffic, offering improved security by allowing certain kinds of traffic while blocking others based on the context of the traffic flow. This is particularly useful in distinguishing between legitimate and malicious traffic, ensuring that only packets related to authorized connections are permitted through the firewall.

6. Signature-based detection compares signatures against which of the following?

A. Scheduled events

B. Known patterns

C. Observed events

D. Temporary logs

Signature-based detection is a critical concept in network security and refers to the method of identifying malicious activity by comparing observed data or traffic against a database of known signatures or patterns of known threats. This approach relies heavily on the existence of predefined patterns that have been identified through previous threat analysis. When a system uses signature-based detection, it scans the incoming and outgoing data for specific patterns that match those contained in its signature database. If a match is found, it indicates a potential security threat, such as a virus, worm, or other types of malware. This method is effective because it can quickly identify known threats based on their unique byte sequences or behaviors. Known patterns are indeed what the signatures represent, but they are not the focal point of the comparison. Instead, the focus is on the real-time data that is actively observed on the network. This real-time observation allows for immediate action against threats, making it a crucial approach in cybersecurity practices. In contrast, scheduled events, observed events, and temporary logs may not provide the precise mechanism of matching known threat signatures to current data flows. Signature-based detection specifically targets active data to ensure prompt detection and response to potential threats based on prior knowledge of those threats.

7. What type of packet filtering does a firewall perform when it pays no attention to whether a packet is part of an existing stream of traffic?

A. Stateful

B. Stateless

C. Full inspection

D. Deep packet inspection

The type of packet filtering that a firewall performs when it disregards whether a packet is part of an existing stream of traffic is referred to as stateless filtering. In this method, the firewall analyzes each individual packet independently without considering the context of established sessions or connections. Stateless firewalls focus on the header information of each packet and assess it against predefined rules. This means they do not maintain a state table of active connections, which allows them to make decisions based solely on the rules defined for incoming and outgoing packets. They can be faster because they do not need to track ongoing connections, but they might be less effective at preventing some types of attacks that can exploit connection states. In contrast, stateful packet filtering keeps track of the state of active connections and uses this information to determine whether a packet is part of an established connection or a new attempt. This allows for a more nuanced understanding of the traffic flow and improves security against various types of attacks that might try to exploit the connection state. Options like full inspection and deep packet inspection involve more comprehensive examination of packets and their payloads, focusing on the content rather than just the headers, which further distinguishes them from stateless filtering.

8. Which term describes devices not managed under DLP but can be monitored?

A. Control Group

B. Unmanageable

C. Unmanaged

D. Unrestricted

The term "unmanaged" accurately describes devices that are not managed under Data Loss Prevention (DLP) policies but can still be monitored for activities related to data protection. In the context of DLP, devices that fall under the unmanaged category are typically those that do not have the necessary software or configurations in place to control or safeguard sensitive data actively. Although these devices cannot be directly controlled or restricted by DLP policies, organizations retain the ability to monitor them for any potential violations or unusual activities concerning sensitive data, which is crucial for maintaining overall data security. In contrast, terms like "control group" typically refer to a set of devices or systems that are actively managed and compared against a baseline, while "unmanageable" suggests that devices cannot be addressed at all, which differs from monitoring capabilities. The term "unrestricted" generally implies that there are no limitations or controls in place, which does not accurately reflect the status of monitoring capabilities for devices not managed under DLP. Thus, "unmanaged" is the most fitting term for describing the specific context of devices that are monitored but not actively governed by DLP policies.

9. What is defined as a pattern that corresponds to a known threat?

A. Signature

B. Protocol

C. Event

D. Broker

A signature is defined as a specific pattern or characteristic that corresponds to a known threat. In the context of cybersecurity, signatures are used by various detection systems, such as antivirus software and intrusion detection systems, to identify and respond to malicious activities. Each signature represents a unique fingerprint of a threat, whether it's a virus, exploit, or any other type of attack, allowing the system to recognize and mitigate the threat effectively. Signatures are essential for maintaining the security posture of an organization, as they help to quickly identify specific threats based on predefined rules. The use of signatures in security measures allows for faster and more accurate detection, as they rely on established knowledge of existing threats. In contrast, the other options do not accurately capture this concept. A protocol refers to a set of rules governing data transmission, an event is an occurrence of a significant event within a network, and a broker would typically refer to an intermediary that facilitates transactions or communications between different parties. None of these terms conveys the idea of a recognizable threat pattern the way a signature does.

10. What can be a reason for a system to be classified as a rogue?

A. It has a functioning Trellix Agent

B. It is detected by the sensor regularly

C. It was not detected by a sensor within a determined timeframe

D. It is fully registered with the ePO server

A system can be classified as a rogue primarily because it has not been detected by a sensor within a predetermined timeframe. This lack of detection typically indicates that the system is operating outside of the established security protocols and may not be managed or monitored by the organization's security infrastructure. Such a scenario raises concerns about potential security vulnerabilities, as an undetected device can lead to unregulated access to sensitive data or resources within the network, making it essential to identify and address it promptly. In contrast, having a functioning agent, being detected regularly, or being fully registered with the central management system (ePO server) typically signifies that the system is actively managed and compliant with network security policies. Therefore, these conditions would not classify a system as a rogue.

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://nsvtmodule4.examzify.com

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