DISA Assured Compliance Assessment Solution (ACAS) Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

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**

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. According to Best Practices, which types of scanning does Tenable.sc dashboards help identify the quality of?

A. Credentialed Windows Scanning

B. Credentialed Linux Scanning

C. Nessus Scan Summary

D. All of the above

2. Plugins are grouped into families, such as:

A. AIX Local Security Checks

B. Windows

C. Red Hat Local Security Checks

D. All of the above

3. Is it possible to customize dashboards in Tenable.sc?

A. Yes, fully customizable

B. No customizations allowed

C. Only by the IT department

D. Yes, but limited options

4. A vulnerability is a weakness or an attack that can compromise your system.

A. True

B. False

C. Cannot be determined

D. Depends on the context

5. Which of the following roles is NOT a predefined Tenable.sc role?

A. Administrator

B. Security Manager

C. Security Analyst

D. ISSO

6. What is the primary purpose of vulnerability queries in Tenable.sc?

A. To automate scanning processes

B. To provide saved views of data

C. To update plugins automatically

D. To log all user activity

7. Frequently used filters can be saved as what for use in various analyses?

A. scans, alerts

B. scans, policies

C. filters, queries

D. filters, alerts

8. What characteristic defines a Tenable.sc plugin?

A. It automates user logins

B. It assesses compliance and vulnerabilities

C. It manages network traffic

D. It encrypts data in transit

9. What two methods can you use to add a dynamic asset list?

A. Use a template or create a set of rules

B. Use a scan policy or a template

C. Create a set of rules or a scan policy

D. Both B and C

10. Can ACAS assess both on-premises and cloud environments?

A. Yes, it can assess only cloud environments

B. Yes, it can assess both types of infrastructures

C. No, it is limited to on-premises systems

D. No, it cannot assess any environments

Answers

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

Explanations

1. According to Best Practices, which types of scanning does Tenable.sc dashboards help identify the quality of?

A. Credentialed Windows Scanning

B. Credentialed Linux Scanning

C. Nessus Scan Summary

D. All of the above

The correct answer encompasses all the types of scanning identified within Tenable.sc dashboards, which include Credentialed Windows Scanning, Credentialed Linux Scanning, and the Nessus Scan Summary. Tenable.sc is designed to provide a comprehensive view of the security posture by integrating various data points from its scanning features. Credentialed scans, whether for Windows or Linux systems, allow Tenable to gather detailed information about the systems being assessed. These scans provide insights into software versions, configurations, and other critical factors that might be exploited. Additionally, the Nessus Scan Summary component aggregates results from multiple scans and presents them in a way that facilitates easy interpretation of the security status of the systems. By providing an overview that includes various scan types and the specific vulnerabilities found, Tenable.sc helps security teams pinpoint areas that may require immediate attention. Thus, the capability to identify the quality of all these scanning types supports best practices in vulnerability management, enabling organizations to prioritize remediation efforts effectively and enhance their overall security frameworks.

2. Plugins are grouped into families, such as:

A. AIX Local Security Checks

B. Windows

C. Red Hat Local Security Checks

D. All of the above

The grouping of plugins into families serves to categorize them based on the specific operating systems or environments they target. Each family is tailored to address particular security checks relevant to that system, allowing for organized and efficient scanning and assessment. In this case, "AIX Local Security Checks," "Windows," and "Red Hat Local Security Checks" represent different groups of plugins. Each family corresponds to a unique operating system, ensuring that the checks conducted are relevant and specific to the security posture of that system. By including all these options under a single choice, it acknowledges that plugins can indeed span multiple families, each critical for maintaining security compliance in their respective environments. This comprehensive grouping facilitates streamlined security assessments, as users can select the appropriate family based on the systems they are auditing. Thus, recognizing "All of the above" as the correct answer emphasizes the breadth of plugin families available for various platforms in the ACAS framework.

3. Is it possible to customize dashboards in Tenable.sc?

A. Yes, fully customizable

B. No customizations allowed

C. Only by the IT department

D. Yes, but limited options

Tenable.sc provides users with robust capabilities to customize dashboards, making it possible to tailor the information displayed based on individual or organizational needs. This level of customization allows users to create personalized views by selecting specific data visualizations, metrics, and reports that are most relevant to their roles or oversight responsibilities. The ability to fully customize dashboards enhances a user's experience and effectiveness by allowing them to focus on the most critical data points. Such flexibility in dashboard design is essential for organizations looking to prioritize specific vulnerabilities, compliance metrics, or other key performance indicators that align with their security posture or risk management strategies. While there may be various limitations based on user permissions, the overarching feature of full customization exemplifies Tenable.sc's goal to provide insightful and relevant security data. Thus, stating that dashboards are fully customizable accurately reflects the capabilities of the platform.

4. A vulnerability is a weakness or an attack that can compromise your system.

A. True

B. False

C. Cannot be determined

D. Depends on the context

The correct understanding is that a vulnerability is indeed a weakness in a system or network that can be exploited by an attacker to compromise the confidentiality, integrity, or availability of information. Therefore, the statement is accurate and should be considered true. The concepts of vulnerability encompass potential points of exploitation that could allow malicious actors to gain unauthorized access or cause harm to a system. For instance, unpatched software, misconfigured networks, or weak passwords are all vulnerabilities that can be targeted in an attack. In this context, indicating that the statement is false does not align with the widely accepted definition of vulnerability in cybersecurity. Each of the other options also fails to correctly reflect the established understanding of vulnerabilities in the realm of information security.

5. Which of the following roles is NOT a predefined Tenable.sc role?

A. Administrator

B. Security Manager

C. Security Analyst

D. ISSO

The correct answer is based on the understanding of the roles defined within the Tenable.sc framework, which has a set of predefined roles tailored to facilitate specific tasks and responsibilities within the application. The Administrator, Security Manager, and Security Analyst roles are foundational roles in Tenable.sc, each with distinct responsibilities. The Administrator typically has overarching control over the system, managing configurations, user permissions, and integrations. The Security Manager is focused more on the strategic aspects of vulnerability management and may handle policies and compliance checks. The Security Analyst performs detailed analyses of vulnerabilities and threats, working directly with data generated by scans. On the other hand, the role of ISSO (Information System Security Officer) is not a predefined role within Tenable.sc, indicating that it is not part of the standard set of roles offered by the platform. While an ISSO may have responsibilities that align with security management, this title is more commonly associated with broader organizational roles outside of the specific functionalities and structures offered by Tenable.sc. Understanding these roles is important for effectively managing security operations and ensuring compliance in environments utilizing the Tenable.sc platform.

6. What is the primary purpose of vulnerability queries in Tenable.sc?

A. To automate scanning processes

B. To provide saved views of data

C. To update plugins automatically

D. To log all user activity

The primary purpose of vulnerability queries in Tenable.sc is to provide saved views of data. This capability allows users to create and customize queries that extract specific information from the vulnerability data collected by the platform. By utilizing these queries, security professionals can analyze and visualize the vulnerability landscape of their organization, focusing on particular assets, severity levels, or compliance requirements. This functionality is crucial for risk management and reporting, as it helps stakeholders to quickly assess their security posture and prioritize remediation efforts based on the insights gathered from the customized views. Saved views can streamline the process of monitoring vulnerabilities over time, ensuring that teams can effectively respond to new findings or changes in the environment. The other options focus on different functionalities that, while useful, do not capture the essence of what vulnerability queries are meant to achieve in the context of Tenable.sc. For example, automating scanning processes pertains to the way vulnerabilities are detected rather than how they are queried and viewed. Updating plugins is a separate task related to keeping the system current, and logging user activity serves a different purpose entirely in terms of compliance and security monitoring.

7. Frequently used filters can be saved as what for use in various analyses?

A. scans, alerts

B. scans, policies

C. filters, queries

D. filters, alerts

The correct answer indicates that frequently used filters can be saved as filters and queries. This is important because filters allow users to narrow down the data they are working with based on specific criteria, while queries enable more complex requests for specific data sets or conditions to be analyzed. By saving these filters and queries, users can efficiently apply them in future analyses without the need to recreate them, thus streamlining the data processing and reviewing tasks in the ACAS environment. This capability enhances productivity and maintains consistency in data analysis, which is crucial for maintaining compliance and effective decision-making processes. Filters and queries work in tandem to help users extract the necessary insights rapidly, proving essential for effective security assessments and reporting within the ACAS framework.

8. What characteristic defines a Tenable.sc plugin?

A. It automates user logins

B. It assesses compliance and vulnerabilities

C. It manages network traffic

D. It encrypts data in transit

The defining characteristic of a Tenable.sc plugin is its ability to assess compliance and vulnerabilities within an organization's IT environment. These plugins are designed to carry out specific checks on systems, applications, and configurations to identify security weaknesses and ensure adherence to compliance standards. This capability is essential for maintaining a robust security posture, as it allows organizations to proactively discover and address potential risks before they can be exploited. In contrast, the other choices focus on functionalities that are not core to the purpose of Tenable.sc plugins. Automating user logins, managing network traffic, and encrypting data in transit are important security tasks, but these activities fall outside the scope of what Tenable.sc plugins are designed to accomplish. Rather, plugins are specifically tailored for scanning and evaluating environments for vulnerabilities and compliance metrics, which is what makes choice B the correct one.

9. What two methods can you use to add a dynamic asset list?

A. Use a template or create a set of rules

B. Use a scan policy or a template

C. Create a set of rules or a scan policy

D. Both B and C

Adding a dynamic asset list in the context of the DISA Assured Compliance Assessment Solution (ACAS) involves utilizing tools that can categorize and manage assets based on certain parameters or criteria. The correct answer highlights the importance of using either a template or a set of rules to create a dynamic asset list. Using a template allows users to define a standard format or structure for an asset list, ensuring consistency in how assets are categorized and displayed. This is particularly useful for organizations that need to maintain a uniform approach to asset management. In contrast, creating a set of rules allows for more flexibility and automation. By establishing rules, the system can dynamically update the asset list based on changing parameters such as asset status, compliance levels, or network changes. These methods emphasize the adaptability necessary for effective asset management, enabling organizations to respond to evolving requirements and conditions in their IT environment. The other options, while incorporating elements relevant to asset management, do not capture the full scope of dynamic list generation. For instance, scan policies are integral to the assessment but don't directly facilitate a dynamic asset list as effectively as templates or rules do.

10. Can ACAS assess both on-premises and cloud environments?

A. Yes, it can assess only cloud environments

B. Yes, it can assess both types of infrastructures

C. No, it is limited to on-premises systems

D. No, it cannot assess any environments

The correct answer highlights that ACAS is designed to be versatile and can effectively assess both on-premises and cloud environments. This capability is essential given the evolving landscape of IT infrastructure, where organizations increasingly utilize a mix of traditional data centers and cloud services. ACAS leverages various tools and frameworks to conduct security compliance assessments across these diverse environments. By doing so, it ensures comprehensive coverage and the ability to identify vulnerabilities and compliance issues whether the assets reside on-premises or in the cloud. This is particularly important for organizations that need to maintain security posture and compliance across different deployment models. The other options are limited in scope. One suggests that ACAS can only assess cloud environments, which would neglect the significant number of organizations that still operate on-premises systems. Another asserts that ACAS is restricted to on-premises systems, overlooking its intended functionality to address cloud security as well. Lastly, stating that ACAS cannot assess any environments disregards its established capability and purpose within security and compliance assessments altogether.

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://disaacas.examzify.com

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