

TENABLE VULNERABILITY MANAGEMENT SPECIALIST PRACTICE TEST (SAMPLE) STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR
THE FULL VERSION STUDY GUIDE

<https://tenablevulnerabilitymgmt.examzify.com>



Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

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	15

SAMPLE

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

SAMPLE

- 1. You can disable Safe Checks in the Host Discovery Scan template.**
 - A. True
 - B. False
 - C. Not configurable
 - D. Depends on scan type
- 2. Which statement best describes the automated update mechanism in Tenable Core?**
 - A. Updates are not supported and require reinstallation
 - B. Updates must be requested by email to support
 - C. Updates are automatically applied without configuration
 - D. Updates are managed via Update Management and applied as configured
- 3. Which types of files are supported for content auditing in Tenable Vulnerability Management?**
 - A. Video files, including MP4s and AVIs.
 - B. Audio files, such as MP3s and WAVs.
 - C. Text-like files, including Microsoft Office documents, PDF files, and plain text files.
 - D. Image files, such as JPEGs and PNGs.
- 4. What type of content can be found on the Tenable Product Education YouTube channel?**
 - A. Interviews with cybersecurity professionals
 - B. Full-length feature films on cybersecurity
 - C. Daily news on global cyber threats
 - D. Short how-to videos covering specific features for all Tenable Products
- 5. Which statement about agent grouping permissions is true?**
 - A. All users can select the agent group
 - B. Only Administrators can select the agent group
 - C. Only Scan Managers can select the agent group
 - D. New groups are hidden from all users by default

- 6. What is NOT a step in creating a network in Tenable Vulnerability Management?**
- A. Setting a network color code
 - B. Setting an age-out period
 - C. Assigning specific scanners or scanner groups
 - D. Naming the network and describing its purpose
- 7. Enabling brute force test options restricts the scan to using which credentials?**
- A. Many default credentials
 - B. Only user-provided credentials
 - C. No credentials
 - D. Credentials obtained from hash files
- 8. Which of the following statements is true regarding Nessus Agent deployment and linking?**
- A. They can report findings back to Tenable Vulnerability Management
 - B. They require a cloud-only management option
 - C. They can report findings back to Tenable Vulnerability Management
 - D. They never connect to the management system
- 9. What is the visibility behavior of new agent groups to users by default?**
- A. Can Use
 - B. No Access
 - C. Can Edit
 - D. New groups are hidden from all users by default
- 10. What do the Basic Network Scan and Advanced Network Scan discovery options have in common?**
- A. Both scans offer the same options, but defaults may vary
 - B. Both have unique sets of options unavailable in the other
 - C. Advanced Network Scan has fewer options than Basic Network Scan.
 - D. Basic Network Scan includes 'Wake on LAN,' which is absent in Advanced Network Scan.

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. You can disable Safe Checks in the Host Discovery Scan template.

- A. True
- B. False**
- C. Not configurable
- D. Depends on scan type

Safe Checks are a built-in safety mechanism in Host Discovery that keeps scanning gentle to avoid disrupting hosts or triggering protections. This safety layer is always enabled in the Host Discovery scan template and isn't exposed as a configurable option to turn off. Because there's no toggle to disable it, the idea that you can disable Safe Checks isn't supported. If you need more aggressive discovery, you'd use a different scan type or template, not disable Safe Checks.

2. Which statement best describes the automated update mechanism in Tenable Core?

- A. Updates are not supported and require reinstallation
- B. Updates must be requested by email to support
- C. Updates are automatically applied without configuration
- D. Updates are managed via Update Management and applied as configured**

Automated updates in Tenable Core are coordinated by Update Management. This component centralizes the process of obtaining and applying content updates, patches, and other vulnerability feeds according to the policies you configure—such as update channels, schedules, and maintenance windows. Because updates are applied as configured, you can automate routine updates while maintaining control over when and how they occur, reducing manual steps and ensuring consistency across the deployment. The mechanism is not about reinstalling the system or requesting updates from support, and updates aren't applied without any configured guidance. In Tenable Core, Update Management governs the lifecycle of updates, applying them automatically based on the defined configuration.

3. Which types of files are supported for content auditing in Tenable Vulnerability Management?

- A. Video files, including MP4s and AVIs.
- B. Audio files, such as MP3s and WAVs.
- C. Text-like files, including Microsoft Office documents, PDF files, and plain text files.**
- D. Image files, such as JPEGs and PNGs.

Content auditing in Tenable Vulnerability Management works by analyzing the actual text contained in files to detect sensitive data or policy violations. Formats that store readable, searchable text—such as Microsoft Office documents, PDFs, and plain text files—can be parsed to extract that text for the audit engine to analyze. Video, audio, and image files are binary media and don't reliably expose searchable text, so they aren't supported for this feature. This is why text-like files are the ones that can be audited for content.

4. What type of content can be found on the Tenable Product Education YouTube channel?

- A. Interviews with cybersecurity professionals
- B. Full-length feature films on cybersecurity
- C. Daily news on global cyber threats

D. Short how-to videos covering specific features for all Tenable Products

Learning how to use software features through concise instructional videos is what the Tenable Product Education YouTube channel is designed for. The content is typically short how-to videos that cover specific features across all Tenable products, providing step-by-step guidance, demonstrations, and practical tips. This makes it the best fit for users who want actionable, hands-on instruction on configuring and using product features. Interviews with cybersecurity professionals, full-length feature films on cybersecurity, and daily news on global threats don't align with the channel's purpose, which is to educate users through targeted, shareable demonstrations of product capabilities.

5. Which statement about agent grouping permissions is true?

- A. All users can select the agent group**
- B. Only Administrators can select the agent group
- C. Only Scan Managers can select the agent group
- D. New groups are hidden from all users by default

Agent grouping helps organize agents for scans, and the ability to choose an agent group is part of configuring an agent-based scan. This choice is available to any user who has permission to edit scans, so it isn't restricted to a specific admin role. In practice, that means all users with access to configure scans can select the agent group, making the grouping option broadly usable across teams. New groups show up in the list for users with scan-access, and they aren't hidden by default. So selecting the agent group is a capability available to all users who can configure scans.

6. What is NOT a step in creating a network in Tenable Vulnerability Management?

- A. Setting a network color code**
- B. Setting an age-out period
- C. Assigning specific scanners or scanner groups
- D. Naming the network and describing its purpose

In Tenable Vulnerability Management, creating a network centers on identifying what you're monitoring and how you'll monitor it. Giving the network a descriptive name and explaining its purpose helps everyone understand what assets are included. Assigning specific scanners or scanner groups ensures you have the right coverage to collect data from that network. An age-out period typically relates to how long inventory items or findings are kept before being retired or archived, which is part of how the network is managed over time. The color code, however, is just a visual cue used for organizing the UI and does not affect the actual configuration or data collection. So while naming, describing, and assigning scanners and retention settings are functional steps in creating a network, setting a color code is optional and not required for the network's creation.

7. Enabling brute force test options restricts the scan to using which credentials?

- A. Many default credentials
- B. Only user-provided credentials**
- C. No credentials
- D. Credentials obtained from hash files

Brute force credential testing is about trying to log in using a set of usernames and passwords that you provide for the scan. Enabling this option tells the scanner to restrict itself to those user-supplied credentials, so only the accounts you specify are tested. It won't automatically try a large pool of default credentials unless you explicitly include them, and it won't operate with no credentials because that would be an unauthenticated attempt rather than a credentialed brute-force test. It also isn't automatically pulling credentials from hash files unless you've configured a separate workflow for that; standard brute force relies on the plaintext credentials you supply for testing.

8. Which of the following statements is true regarding Nessus Agent deployment and linking?

- A. They can report findings back to Tenable Vulnerability Management
- B. They require a cloud-only management option
- C. They can report findings back to Tenable Vulnerability Management**
- D. They never connect to the management system

Nessus Agent deployment and linking centers on how the agent data reaches the central vulnerability management platform. The essential idea is that Nessus Agents can report findings back to Tenable Vulnerability Management, allowing centralized visibility and correlation with other scan data. This linking works with either cloud-based or on-prem TVM, so there is no requirement to use a cloud-only option. The agents are designed to collect data on endpoints and transmit it to the management system, even if the device was offline temporarily—the results are sent once connectivity is restored. In short, the primary function is to push findings to TVM, not to operate in isolation or never connect.

9. What is the visibility behavior of new agent groups to users by default?

- A. Can Use
- B. No Access
- C. Can Edit
- D. New groups are hidden from all users by default**

New agent groups are created with restricted visibility to prevent unintended access. By default, they are hidden from all users, so no one can see or use the group unless an administrator grants permission. This follows a principle of least privilege: new groups stay out of sight until someone with the right access explicitly makes them visible or assigns them to a role or user. If visibility is needed, an admin can adjust permissions or share the group with specific users or teams, after which those users can see and interact with the group as permitted.

10. What do the Basic Network Scan and Advanced Network Scan discovery options have in common?

- A. Both scans offer the same options, but defaults may vary
- B. Both have unique sets of options unavailable in the other**
- C. Advanced Network Scan has fewer options than Basic Network Scan.
- D. Basic Network Scan includes 'Wake on LAN,' which is absent in Advanced Network Scan.

Both discovery modes aim to identify devices on a network, but they expose different configuration knobs. The Basic Network Scan keeps things simple with a streamlined set of discovery methods and defaults, while the Advanced Network Scan offers a much richer, more granular set of controls for probing, timing, protocols, and features. Because each mode exposes its own specialized options, there isn't a single option set that's identical in both; each has options the other does not. That's why the statement describing unique option sets in each mode best captures their relationship. The other choices would imply identical option sets, fewer options in the advanced mode, or a feature like Wake on LAN being available in the basic mode, which isn't how these discovery options are structured.

SAMPLE

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://tenablevulnerabilitymgmt.examzify.com>

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

SAMPLE