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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. Which statement about connectivity troubleshooting is true?

A. You must ensure access to SPAN port, cloud.tenable.com on port 443, and no local firewall rules interfering with traffic

B. DHCP server availability is sufficient

C. VPN must be configured with split tunneling

D. Correct subnet mask is set on all interfaces

2. Which permission is generally reserved only for administrators?

A. Can View

B. Can Scan

C. Can Edit

D. Can Use

3. Which do not perform network checks during scans?

A. Regular vulnerability scans with targets

B. Scans that include a Targets field

C. Traditional network scans

D. Tenable Nessus Agents

4. What does the absence of an Audits tab in a scan result suggest?

A. No audit checks were run.

B. The audits tab is hidden for security reasons.

C. Audit checks are still running.

D. The system passed all checks successfully

5. What role within Tenable Vulnerability Management has the capability to perform all functions?

A. Scan Manager

B. Standard User

C. Administrator

D. Custom Role

SAMPLE

6. In Tenable, how does the role assigned to a user impact object permissions?

A. Roles only determine access to dashboard functions, not object user permissions

B. Roles have no impact on object user permissions

C. Roles limit object visibility but not the permissions on those objects

D. The functions of an assigned role will always supersede any object user permissions

7. How do Nessus Agents report their findings?

A. Directly to cloud storage

B. Via email to the security administrator

C. Through a third-party integration tool

D. They report back to Tenable Vulnerability Management

8. Which statement is true about the basic Host Discovery scan content?

A. Plugin 19506, Nessus Scan Information is included.

B. It excludes Nessus Scan Information.

C. It includes patch management data.

D. It includes vulnerability scans.

9. Which scan template is recommended for compliance scans in Tenable Vulnerability Management?

A. Host Discovery

B. Basic Network Scan

C. Credentialed Patch Audit

D. Policy Compliance Auditing

10. For what purpose does Nessus Network Monitor (NNM) support custom Secure Sockets Layer (SSL) certificates?

A. To ensure secure communication by allowing use of custom SSL certificates for its instance

B. To secure the login credentials

C. To encrypt the monitored network traffic

D. To facilitate encrypted backups

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which statement about connectivity troubleshooting is true?

A. You must ensure access to SPAN port, cloud.tenable.com on port 443, and no local firewall rules interfering with traffic

B. DHCP server availability is sufficient

C. VPN must be configured with split tunneling

D. Correct subnet mask is set on all interfaces

Connecting to Tenable's cloud service and diagnosing issues hinges on making sure the device can reach the service reliably and that nothing in the local network blocks that path. Access to cloud.tenable.com on port 443 is essential because this is the HTTPS channel Tenable uses for its cloud communications, updates, and data transfer. The SPAN port is about having a dedicated port where you can mirror and observe traffic for troubleshooting, so you can see exactly what's being sent and received between the scanner and the cloud. And ensuring there are no local firewall rules interfering with traffic removes a common local barrier that can silently block outbound connections or responses. Relying solely on DHCP overlooks the bigger picture: IP configuration alone doesn't guarantee reachability to the cloud or that DNS, routing, and outbound policies won't block traffic. VPN split tunneling is a configuration detail that isn't universally required for connectivity in all environments, so it isn't a universal truth for this scenario. Likewise, having the correct subnet mask is part of basic IP setup, but even with that correct, if there's no route to cloud.tenable.com or if a firewall blocks port 443, connectivity will fail.

2. Which permission is generally reserved only for administrators?

A. Can View

B. Can Scan

C. Can Edit

D. Can Use

The ability to edit is the most privileged in this context because it lets someone change the configurations that control how vulnerability scans are run and managed. With edit rights, a user can modify scan policies, schedules, credentials, assets, and even user access. Those kinds of changes directly affect what gets scanned, how results are interpreted, and who can see or alter sensitive settings, so they're typically restricted to administrators who manage risk, auditing, and change control. Viewing is simply read only access to results, which most users can have without risking configuration changes. Using or applying permissions (like Can Use or Can Scan) enable execution of tasks but don't inherently grant the power to modify the system's configuration. Therefore, the permission reserved for administrators is the ability to edit.

3. Which do not perform network checks during scans?

A. Regular vulnerability scans with targets

B. Scans that include a Targets field

C. Traditional network scans

D. Tenable Nessus Agents

Network checks mean actively probing other machines across the network to see which hosts are reachable and which services are exposed. Regular vulnerability scans with targets are designed to test defenses across those specified hosts by performing those network probes and scans. Scans that include a Targets field operate in the same way, identifying and probing the listed hosts. Traditional network scans are built around discovering hosts and services on the network through active probing as well. Tenable Nessus Agents behave differently: they run vulnerability checks on the host where the agent is installed, locally on that machine, and then report the findings back. They do not perform network-wide probing of other hosts or scanning across the network. That's why Nessus Agents do not conduct network checks during scans.

SAMPLE

4. What does the absence of an Audits tab in a scan result suggest?

A. No audit checks were run.

B. The audits tab is hidden for security reasons.

C. Audit checks are still running.

D. The system passed all checks successfully

Audits are separate checks from vulnerability findings, and the Audits tab only appears when audit checks have been configured and run for that scan. If no audit checks are configured (or none were executed), there's nothing to display, so the tab won't be shown. So the absence of the Audits tab signals that no audit checks were run for this scan. It doesn't imply security reasons for hiding the tab, that checks are still in progress, or that everything passed; those outcomes would be indicated in other parts of the scan results if audit checks were involved.

5. What role within Tenable Vulnerability Management has the capability to perform all functions?

A. Scan Manager

B. Standard User

C. Administrator

D. Custom Role

In Tenable Vulnerability Management, roles define what a user can do across the platform. The Administrator is the highest-privilege role and is built to cover every function—configuring the platform, managing users and permissions, creating and running scans, viewing and exporting reports, setting policies, and integrating with other systems. Because of this, the Administrator inherently has access to all features and settings, making it the most capable role for performing all functions. A Scan Manager can create and run scans and handle scan results but doesn't grant access to system-wide configurations. A Standard User has limited access, typically to view data and run assigned tasks but not to change settings. A Custom Role can be tailored, but unless it's explicitly granted all permissions, it won't automatically have complete control.

6. In Tenable, how does the role assigned to a user impact object permissions?

A. Roles only determine access to dashboard functions, not object user permissions

B. Roles have no impact on object user permissions

C. Roles limit object visibility but not the permissions on those objects

D. The functions of an assigned role will always supersede any object user permissions

In Tenable, the role assigned to a user defines the actions they can perform and the scope of access they have, and those role-based capabilities take precedence over per-object permissions. The role sets what you can do (view, edit, create, delete, manage, etc.) and which areas you can access, while object permissions control visibility on individual objects. However, object-level permissions cannot grant additional rights beyond what the role allows; if the role restricts an action, that restriction wins, and if the role permits an action, it enables it within the object's context. This means the functions of the assigned role will always supersede any object-level permissions, ensuring consistent access control across the system.

SAMPLE

7. How do Nessus Agents report their findings?

A. Directly to cloud storage

B. Via email to the security administrator

C. Through a third-party integration tool

D. They report back to Tenable Vulnerability Management

Nessus Agents are designed to collect scan results on the endpoint and then send those results to the central vulnerability management system. When an agent is connected to Tenable Vulnerability Management, it securely reports its findings back to TVM, where the data is ingested, correlated, and presented in the console. This centralized reporting flow is what makes TVM the single source of truth for vulnerability data across the environment. Emailing results, writing to cloud storage directly, or routing data through a separate third-party integration tool aren't the standard reporting path for Nessus Agents. They're primarily meant to push results into Tenable Vulnerability Management, with other workflows available later via APIs or exports if needed.

8. Which statement is true about the basic Host Discovery scan content?

A. Plugin 19506, Nessus Scan Information is included.

B. It excludes Nessus Scan Information.

C. It includes patch management data.

D. It includes vulnerability scans.

The key idea is that Host Discovery results carry metadata about the scan itself. In the basic Host Discovery content, you'll find information provided by the Nessus Scan Information plugin (Plugin 19506). This plugin captures details about how the scan was run—things like the policy used, target hosts included, scan engine version, and timing data. This metadata is what helps you understand and reproduce how the discovery was performed, and it's included with the discovery results to provide context. Patch management data or vulnerability scan results aren't part of the basic Host Discovery content because discovery focuses on identifying live hosts and reachable services, not evaluating patch status or listing vulnerability findings. That's why including Nessus Scan Information is the correct and most appropriate piece of content for this scenario.

9. Which scan template is recommended for compliance scans in Tenable Vulnerability Management?

A. Host Discovery

B. Basic Network Scan

C. Credentialed Patch Audit

D. Policy Compliance Auditing

Evaluating systems against security policies and benchmarks is what this template is designed for. Policy Compliance Auditing runs checks that compare a system's actual configurations and settings to defined policies (such as CIS, DISA STIG, or custom policies). It reports on how many checks pass or fail, highlights noncompliant settings, and provides guidance for remediation, which is exactly what a compliance scan requires. Other templates serve different aims: Host Discovery inventories assets on the network; Basic Network Scan analyzes reachable hosts and basic vulnerabilities without credentials; Credentialed Patch Audit checks whether patches are installed on hosts but focuses on patch state rather than overall policy conformance. Therefore, Policy Compliance Auditing is the appropriate choice for scanning to verify compliance with security policies.

SAMPLE

10. For what purpose does Nessus Network Monitor (NNM) support custom Secure Sockets Layer (SSL) certificates?

A. To ensure secure communication by allowing use of custom SSL certificates for its instance

B. To secure the login credentials

C. To encrypt the monitored network traffic

D. To facilitate encrypted backups

The main idea is that SSL certificates on Nessus Network Monitor are used to secure the management plane by encrypting and authenticating the connection between clients and the NNM instance. By allowing a custom certificate, you can install a certificate issued by your organization's CA, so browsers and integrations trust the NNM server and all communications over HTTPS are encrypted. This ensures confidential, tamper-proof interaction with the NNM interface and APIs. It isn't about encrypting the actual network traffic being monitored, which is separate from the management traffic. It's also not specifically about storing login credentials or encrypted backups—the certificate's purpose here is to secure the communication channel to the NNM instance.

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