COMPTIA PENTEST+ PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://comptia-pentestplus.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 16

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 risk involves unauthorized handling of sensitive information within a web application?**

   A. Insecure Configuration

   B. Sensitive Data Exposure

   C. Broken Authentication

   D. Security Misconfiguration

2. **Which option specifies the task name when creating a scheduled task?**

   A. /tc

   B. /tr

   C. /tn

   D. /sc

3. **What is the process of stripping user-supplied input of unwanted or untrusted data called?**

   A. Input validation

   B. Input parsing

   C. Input sanitization

   D. Input filtering

4. **Which framework is known for its focus on penetration testing and includes development and debugging components?**

   A. Covenant

   B. Pentest+ Framework

   C. Metasploit

   D. Nessus

5. **What is a notable feature of the Immunity Debugger?**

   A. Exclusively uses command line

   B. Includes a graphical user interface

   C. Is only compatible with Linux

   D. Does not allow script modifications

SAMPLE

6. What type of SQL injection is typically more difficult for vulnerability scanners to detect due to the nature of the attack?

A. Simple SQL injection

B. Union-based SQL injection

C. Blind SQL injection

D. Time-based SQL injection

7. Which tool is specifically designed for website enumeration?

A. Nmap

B. Dirbuster

C. Nessus

D. Burp Suite

8. What is a key action in the aftermath of a penetration test concerning initial findings?

A. Immediately start a retest

B. Review and finalize the report

C. Archive all data collected

D. Update the client on findings

9. What command is used to create a scheduled task in Windows?

A. schtasks

B. tasklist

C. crontab

D. start

10. What functionality does the '-t' option in Metagoofil provide?

A. Scans for text files

B. Searches for PDF documents

C. Downloads file metadata from URLs

D. Initiates a network scan

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which risk involves unauthorized handling of sensitive information within a web application?

A. Insecure Configuration

B. Sensitive Data Exposure

C. Broken Authentication

D. Security Misconfiguration

Sensitive Data Exposure refers to the risk when sensitive information — such as personal data, payment details, or confidential business information — is improperly handled or disclosed within a web application. This can occur if the application does not adequately protect data during transmission and storage, resulting in unauthorized access by attackers. Proper security measures typically involve encryption, secure data handling practices, and robust access controls to prevent this risk. Remediation strategies may include ensuring that sensitive data is encrypted both in transit and at rest, implementing secure application coding practices, and regularly testing for vulnerabilities that could lead to data leaks. While the other options encompass important aspects of web application security, they do not specifically address the unauthorized handling of sensitive information. Insecure Configuration relates to poor security settings that can be exploited, Broken Authentication pertains to flaws in the authentication mechanisms that might allow unauthorized users to gain access, and Security Misconfiguration refers to a broader category of security mishaps due to improperly configured security settings. All of these can contribute to attacks, but Sensitive Data Exposure specifically calls out instances where sensitive information is not adequately protected against unauthorized access.

2. Which option specifies the task name when creating a scheduled task?

A. /tc

B. /tr

C. /tn

D. /sc

When creating a scheduled task, specifying the task name is essential for identifying the task within the Task Scheduler. The correct option indicates that the task name is designated using the "/tn" parameter. This allows system administrators and users to define a specific and recognizable name for the task, facilitating easier management and retrieval of scheduled tasks. In contrast, other options refer to different parameters. The "/tr" option indicates the task to run, specifying the path of the executable or script that should be executed. The "/sc" option is used to set the schedule frequency (for example, daily, weekly, or monthly) for running the task. The "/tc" option is not a standard parameter associated with creating scheduled tasks, which further clarifies the role of the "/tn" parameter in this context.

SAMPLE

3. What is the process of stripping user-supplied input of unwanted or untrusted data called?

A. Input validation

B. Input parsing

C. Input sanitization

D. Input filtering

The process of stripping user-supplied input of unwanted or untrusted data is known as input sanitization. This practice involves cleaning and processing the input to remove or neutralize any potentially harmful data before it is processed or stored by an application. Input sanitization is critical in preventing security vulnerabilities such as SQL injection, cross-site scripting (XSS), and other forms of injection attacks, which exploit unsanitized input. In this context, input sanitization helps ensure that only the acceptable and expected data is retained, effectively improving the security posture of an application. By implementing sanitization practices, developers can reduce the risk associated with utilizing data that might be manipulated or crafted by an attacker. While input validation, input parsing, and input filtering are related concepts, they serve different roles in the context of data handling. Input validation typically involves checking that the data meets certain criteria (like format or type), while input parsing breaks data into manageable parts. Input filtering, on the other hand, may include broader actions like rejecting or allowing certain types of data based on predefined rules, but it doesn't specify the act of cleaning the data in the same focused manner that sanitization does.

4. Which framework is known for its focus on penetration testing and includes development and debugging components?

A. Covenant

B. Pentest+ Framework

C. Metasploit

D. Nessus

The Covenant framework is particularly notable for its emphasis on penetration testing while also incorporating development and debugging components. It is designed to facilitate the testing process, providing tools and functionalities that help security professionals simulate attacks, manage sessions, and maintain a high degree of control during engagements. Covenant's architecture allows for the customization of payloads and provides a user-friendly interface to streamline many of the tedious aspects of penetration testing, such as managing the communication between tools and scripting various aspects of the attack. This flexibility and focus on real-world application in penetration testing set it apart from other frameworks that may concentrate on network scanning or vulnerability management rather than offering comprehensive testing capabilities with integrated development aspects. In contrast, other frameworks like Metasploit are well-recognized for their extensive exploitation capabilities but may not emphasize development and debugging to the same extent as Covenant. Nessus is primarily known for vulnerability scanning, while Pentest+ is more of an exam or certification rather than a dedicated framework for penetration testing operations. This distinct focus on both penetration testing and development is what makes Covenant the correct choice in this context.

SAMPLE

5. What is a notable feature of the Immunity Debugger?

A. Exclusively uses command line

B. Includes a graphical user interface

C. Is only compatible with Linux

D. Does not allow script modifications

The Immunity Debugger is well-known for its graphical user interface, which provides a user-friendly environment for users when analyzing and debugging applications. This UI allows for easier manipulation and visualization of data, helping security professionals and developers to observe the program flow and inspect variables in a way that is more intuitive than using purely command-line tools. The graphical interface facilitates various functionality such as drag-and-drop features, real-time data interaction, and integrated plugin support, which significantly enhances the debugging experience. By having a GUI, users can more efficiently navigate through complex information, making it especially valuable in penetration testing and reverse engineering contexts. Other features, like its compatibility across multiple operating systems (not just Linux) and its allowance for scripting and modifications, demonstrate the flexibility and capability of the Immunity Debugger beyond just a command-line tool.

6. What type of SQL injection is typically more difficult for vulnerability scanners to detect due to the nature of the attack?

A. Simple SQL injection

B. Union-based SQL injection

C. Blind SQL injection

D. Time-based SQL injection

Blind SQL injection is typically more challenging for vulnerability scanners to detect due to the way it operates. In this type of attack, the attacker is unable to see the actual output of the SQL queries being executed. Instead, they infer information based on the application's response behavior, such as changes in the application's output or response times. This lack of visible output makes it harder for automated tools to identify vulnerabilities, as these scanners often rely on the ability to directly observe and analyze the results of queries. For example, in blind SQL injection, an attacker might ask a yes/no question that modifies the query and then analyze whether the application behaves differently based on the input. Since vulnerability scanners may not be adept at handling such indirect methods of information retrieval, they can miss these vulnerabilities while detecting more straightforward injection techniques. The reasons the other types of SQL injections are detected more easily relate to their direct visibility in query responses. Simple SQL injection often results in error messages or visible data extraction, Union-based SQL injection uses direct output from queries, and Time-based SQL injection gives clear indicators through timing delays, making them easier for scanners to identify compared to the subtlety of blind SQL injection.

SAMPLE

7. Which tool is specifically designed for website enumeration?

A. Nmap

B. Dirbuster

C. Nessus

D. Burp Suite

Dirbuster is specifically designed for website enumeration, making it the correct choice in this context. It is a tool used to identify hidden directories and files on web servers through brute force attacks. By employing wordlists, Dirbuster systematically attempts to access different paths on a website, enabling penetration testers to discover resources that may not be immediately visible. This capability is essential in web application testing as it helps uncover potential vulnerabilities or misconfigurations that could be exploited. Other tools listed serve different purposes. For example, Nmap is primarily a network scanning tool that can help discover hosts and services on a network, but it does not specialize in website enumeration. Nessus is a vulnerability scanner that assesses systems and applications for known vulnerabilities instead of focusing on finding directories or files on a web server. Burp Suite is a comprehensive web application security testing tool, which includes features for scanning and analyzing web applications, but its primary focus is broader than just enumeration, offering functionalities like intercepting proxy and vulnerability assessments.

8. What is a key action in the aftermath of a penetration test concerning initial findings?

A. Immediately start a retest

B. Review and finalize the report

C. Archive all data collected

D. Update the client on findings

In the aftermath of a penetration test, reviewing and finalizing the report is a crucial action to ensure that all findings are documented accurately and comprehensively. This report serves as a key deliverable that summarizes the vulnerabilities identified, the methodologies used to uncover them, and the potential impact of those vulnerabilities on the organization. Finalizing the report allows for clarity and ensures it meets the expectations of the stakeholders involved. It provides a structured way to present the issues found, recommendations for remediation, and any other relevant insights that may aid in enhancing the security posture of the organization. This detailed report can guide discussions in future action plans or strategic updates to security policies and controls. The other actions, while still important, do not hold the same priority immediately following the test. For instance, updating the client on findings is essential for communication and transparency, but the information must be accurately captured and reviewed in the report first. Archiving all data collected is typically done later in the process when all elements of the test are complete and documented. Meanwhile, starting a retest is not advisable until the initial findings have been thoroughly assessed and addressed based on the report's conclusions.

SAMPLE

9. What command is used to create a scheduled task in Windows?

A. schtasks

B. tasklist

C. crontab

D. start

The command used to create a scheduled task in Windows is "schtasks". This command is part of the Windows operating system and allows users to schedule and manage tasks that run at specified times or intervals. With "schtasks", users can create, delete, configure, or display scheduled tasks. The versatility of "schtasks" allows for various options, such as setting the task to run on a particular day or time, running the task under specific user accounts, and even specifying the action the task should perform when triggered. It is an essential tool for system administrators and IT professionals who need to automate processes within the Windows environment. In contrast, the command "tasklist" is used to display a list of currently running processes, while "crontab" is specific to Unix-based systems for similar scheduling tasks. The "start" command is utilized to start a separate window to run a specified program or command, but it does not relate to scheduling tasks. Therefore, "schtasks" is clearly the correct choice for creating scheduled tasks in Windows.

10. What functionality does the '-t' option in Metagoofil provide?

A. Scans for text files

B. Searches for PDF documents

C. Downloads file metadata from URLs

D. Initiates a network scan

The '-t' option in Metagoofil is specifically designed to search for files of a certain type, and when it comes to identifying document formats, one of the most common uses is to specify the type of file the user is interested in. In this case, the focus is on PDF documents, which are widely used for sharing and disseminating information in a secure format. By using the '-t' option alongside the relevant file type, users can instruct Metagoofil to hone in on such documents, effectively helping in information gathering during a penetration test. This targeted searching capability allows penetration testers to collect metadata from specific documents, which can include valuable information such as author names, software used, and other intellectual property details. It enhances the efficiency of the information gathering process by filtering results based on the document types that are of interest, making it a critical feature for those conducting digital reconnaissance.

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://comptia-pentestplus.examzify.com

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

SAMPLE