# CERTMASTER PENTEST+ PRACTICE TEST (SAMPLE)

## STUDY GUIDE




## SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

**VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE**

https://certmasterpentest.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 of the following topics is typically covered in a Master Service Agreement?**

   A. Safety guidelines and environmental concerns

   B. Employee benefits and bonuses

   C. Annual budgets for projects

   D. Advertising campaigns for service promotion

2. **What is the purpose of PowerSploit?**

   A. Software installation management

   B. Web server vulnerability scanning

   C. Post-exploitation tasks using PowerShell scripts

   D. Network traffic monitoring

3. **How does manipulating the "kid" value in JWTs pose a security risk?**

   A. It leads to the generation of invalid tokens.

   B. It allows attackers to fetch keys without validation, pointing to unauthorized sources.

   C. It disables the overall security features of the server.

   D. It can reset the encryption methods used for user sessions.

4. **What does the scan_ports function primarily check for on a given IP address?**

   A. Open ports

   B. Network traffic

   C. User activity

   D. System performance

5. **What type of information does the ServiceEnumerator class retrieve?**

   A. User credentials

   B. Service banner

   C. Network statistics

   D. File permissions

SAMPLE

**6. Which programming concept allows you to evaluate conditions and execute code accordingly?**

A. Variables

B. Flow control

C. Functions

D. Classes

**7. In cybersecurity, what does the term 'threat' usually include?**

A. Only software vulnerabilities

B. Human errors exclusively

C. Malware and natural disasters

D. Security policies

**8. In the context of a pass-the-hash attack, what should the pentester do if they cannot gain administrative access?**

A. Run a Metasploit module to gather further intelligence

B. Disable Windows Firewall completely

C. Edit the User Account Control (UAC) policy settings

D. Use a brute-force tool to crack the password

**9. In pentesting, what can be selected as targets by stakeholders?**

A. Specific applications only

B. Only external networks

C. IP addresses and URLs

D. Single-user applications only

**10. What type of logs show successful exploitation during penetration testing?**

A. Security incident reports

B. Terminal outputs

C. Network performance metrics

D. Event logs from the operating system

SAMPLE

# Answers

SAMPLE

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

SAMPLE

# Explanations

SAMPLE

## 1. Which of the following topics is typically covered in a Master Service Agreement?

A. Safety guidelines and environmental concerns

B. Employee benefits and bonuses

C. Annual budgets for projects

D. Advertising campaigns for service promotion

*A Master Service Agreement (MSA) typically outlines the general terms and conditions governing the relationship between two parties in any ongoing or future projects. It serves as a foundational document that sets standard procedures, responsibilities, and expectations for the services to be provided. Safety guidelines and environmental concerns fall within the realm of terms that need to be addressed in an MSA, particularly in industries where operations may pose risks to health, safety, or the environment. Including such guidelines helps ensure compliance with legal and regulatory standards and protects both parties from potential liabilities. This aspect is important for managing risks and fostering a safe working environment, particularly in sectors like construction, manufacturing, or services that may involve physical labor or ecological impact. While employee benefits and bonuses, annual budgets for projects, and advertising campaigns are indeed essential elements in the context of business agreements, they are typically addressed in separate contracts or documents rather than being foundational components of an MSA. This focus allows the MSA to maintain a broad scope for the overall partnership rather than delving into the specific operational details that may change over time.*

## 2. What is the purpose of PowerSploit?

A. Software installation management

B. Web server vulnerability scanning

C. Post-exploitation tasks using PowerShell scripts

D. Network traffic monitoring

*PowerSploit is a collection of PowerShell scripts designed specifically for post-exploitation tasks in the context of penetration testing and ethical hacking. Once a system has been compromised, these scripts can be utilized to maintain control over the system, gather information, escalate privileges, and perform other tasks that help the tester accomplish their objectives within the compromised environment. The framework allows security professionals to leverage PowerShell's capabilities to automate complex processes that might otherwise require manual intervention, thereby enhancing their efficiency and effectiveness during a penetration test. It aims to provide tools for tasks such as credential harvesting, privilege escalation, and command-and-control functionality, which are critical to understanding the security posture of the systems being assessed. The other options do not align with PowerSploit's purpose: it does not focus on software installation management, web server vulnerability scanning, or network traffic monitoring. These areas may involve different tools and technologies aimed at different phases of the security assessment process.*

SAMPLE

## 3. How does manipulating the "kid" value in JWTs pose a security risk?

A. It leads to the generation of invalid tokens.

B. It allows attackers to fetch keys without validation, pointing to unauthorized sources.

C. It disables the overall security features of the server.

D. It can reset the encryption methods used for user sessions.

*Manipulating the "kid" value in JSON Web Tokens (JWTs) is a significant security concern because it can lead to unauthorized access to sensitive data. The "kid" (key ID) header parameter in a JWT is used to indicate which key should be used to verify the token's signature. By altering the "kid" value, an attacker may be able to point the token verification process to a vulnerable or malicious key, leading the server to accept a forged token as valid without proper validation of the token's authenticity. If an attacker can retrieve or generate a valid JWT using their manipulated "kid," they could potentially gain access to resources or data that they are not authorized to access. This could compromise the integrity and confidentiality of information, making the system vulnerable to various attacks, such as session hijacking or data leakage. In contrast, the other options do not accurately represent the risk associated with tampering with the "kid" value. For instance, changing the "kid" does not inherently disable server security features or reset encryption methods. Additionally, while it may result in some invalid tokens under certain conditions, the more pressing issue is the unauthorized access that can occur when validation is bypassed by an incorrect "kid." This makes option B the most*

## 4. What does the scan_ports function primarily check for on a given IP address?

A. Open ports

B. Network traffic

C. User activity

D. System performance

*The scan_ports function is designed to check for open ports on a given IP address. Open ports are crucial in network security and management because they signify points of entry for network services, applications, or potential vulnerabilities. By identifying which ports are open, security professionals can assess potential risks, evaluate the services running on those ports, and determine if any unauthorized access attempts could occur. This process is often a fundamental part of penetration testing and security assessments, as it helps to establish the attack surface and allows for appropriate defenses to be put in place. The other options relate to different aspects of network monitoring and performance. Network traffic involves analyzing data packets being transmitted, user activity focuses on monitoring the behavior and actions of users on a network, and system performance pertains to the evaluation of how efficiently a system is operating. While all these areas are important in the overall context of cybersecurity, they are not the primary function of the scan_ports operation, which is specifically targeted at identifying open ports.*

SAMPLE

## 5. What type of information does the ServiceEnumerator class retrieve?

A. User credentials

B. Service banner

C. Network statistics

D. File permissions

*The ServiceEnumerator class is designed to retrieve information specifically about the services running on a system, including their status, names, and configurations. One critical piece of information it can obtain is the service banner, which generally includes the service's name, description, and version details. This is particularly useful for penetration testing and enumeration as it helps security professionals identify the services present on a machine, assess their potential vulnerabilities, and plan further actions. User credentials, network statistics, and file permissions relate to other aspects of system and security management but do not pertain to the primary focus of the ServiceEnumerator class. Each of these other choices falls under different categories of information that might be gathered using other classes or tools, but they are not functions of the ServiceEnumerator specifically.*

## 6. Which programming concept allows you to evaluate conditions and execute code accordingly?

A. Variables

B. Flow control

C. Functions

D. Classes

*Flow control is a programming concept that is essential for managing the execution of code based on certain conditions. It allows developers to direct the flow of a program's execution by evaluating conditions, using structures such as if statements, switch cases, loops (like for and while), and more. When a condition evaluates to true or false, flow control statements determine which block of code should be executed. For instance, in an if statement, the code within the block will only run if the specific condition is met, allowing for tailored responses based on the state of the program or input provided. This capability is fundamental in programming as it enables the creation of dynamic, responsive applications that can adapt to different scenarios and user inputs. In contrast, variables are used to store data, functions are used to encapsulate reusable code, and classes represent blueprints for objects in object-oriented programming. While all these concepts are crucial to programming, they do not inherently evaluate conditions and dictate the execution path of code in the manner that flow control does.*

SAMPLE

## 7. In cybersecurity, what does the term 'threat' usually include?

A. Only software vulnerabilities

B. Human errors exclusively

C. Malware and natural disasters

D. Security policies

*The term 'threat' in cybersecurity encompasses any potential danger that could exploit a vulnerability to harm an asset. This includes a wide variety of elements, such as malware, which refers to malicious software designed to harm, exploit, or otherwise negatively impact systems and data. Additionally, natural disasters fall under this definition as they can lead to data loss or system outages, thereby threatening the integrity, confidentiality, or availability of information systems. By recognizing that threats include a diverse array of risks, organizations can better prepare by implementing comprehensive security measures. The inclusion of both malware and natural disasters reflects the broad spectrum of potential threats that cybersecurity must address, which is essential for developing effective defense strategies. Human errors, software vulnerabilities, and security policies are crucial components of cybersecurity, but they specifically pertain to the causes of security incidents or factors affecting security management, rather than being classified as threats themselves.*

## 8. In the context of a pass-the-hash attack, what should the pentester do if they cannot gain administrative access?

A. Run a Metasploit module to gather further intelligence

B. Disable Windows Firewall completely

C. Edit the User Account Control (UAC) policy settings

D. Use a brute-force tool to crack the password

*In the context of a pass-the-hash attack, if a pentester cannot gain administrative access, it is important to understand how the User Account Control (UAC) settings play a role in privilege management. By editing the UAC policy settings, the pentester can potentially lower the protection mechanisms that restrict access to certain administrative functions. UAC is designed to prevent unauthorized changes to the operating system, and modifying these settings can enable the execution of higher privilege tasks that are normally restricted. This approach allows the pentester to elevate privileges or bypass certain security controls in place, which can facilitate further penetration testing activities. Adjusting UAC settings might create a more favorable environment for further exploitation, making it a strategic choice when other avenues for gaining access are not available. Other options, while they might be useful in different scenarios, do not necessarily align with the immediate goal of gaining administrative access in the context of a pass-the-hash attack. For instance, running a Metasploit module may not lead to higher privileges, simply gathering intelligence without increasing the access level. Disabling the Windows Firewall is typically not an advisable strategy, as it could easily alert security teams or impact system stability. Likewise, using a brute-force tool to crack a password is often time*

SAMPLE

## 9. In pentesting, what can be selected as targets by stakeholders?

A. Specific applications only

B. Only external networks

C. IP addresses and URLs

D. Single-user applications only

*In penetration testing, stakeholders identify and select specific targets that align with their security assessment objectives. Choosing IP addresses and URLs is essential because these targets encompass a broader range of potential vulnerabilities within an organization's infrastructure. This selection allows pentesters to explore various attack surfaces, including both web applications and network devices, thus providing a more comprehensive evaluation of the organization's security posture. Focusing on individual applications or single-user applications would limit the scope of the penetration test. Stakeholders typically aim to assess their overall security, which includes multiple components, rather than just specific applications or user-level contexts. Additionally, restricting the targets to only external networks does not consider internal assets that are vital for a thorough assessment. Therefore, selecting IP addresses and URLs provides the necessary breadth and flexibility to effectively evaluate an organization's security vulnerabilities.*

## 10. What type of logs show successful exploitation during penetration testing?

A. Security incident reports

B. Terminal outputs

C. Network performance metrics

D. Event logs from the operating system

*Successful exploitation during penetration testing is typically best reflected in terminal outputs. When a penetration tester successfully exploits a vulnerability, the terminal output can provide direct feedback on the actions taken and the results observed. This includes command execution results, error messages, or confirmation of access to systems and data, which helps the tester assess the effectiveness of their exploitation techniques in real-time. In contrast, security incident reports summarize incidents after they occur and are not directly used during penetration testing to show real-time exploitation success. Network performance metrics focus on the throughput, latency, and general health of the network, not on exploitation events. Operating system event logs mainly detail system-level activities and statuses, which can include successful logins or errors but do not capture the nuances of exploitation as effectively as terminal outputs do.*

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://certmasterpentest.examzify.com

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

SAMPLE