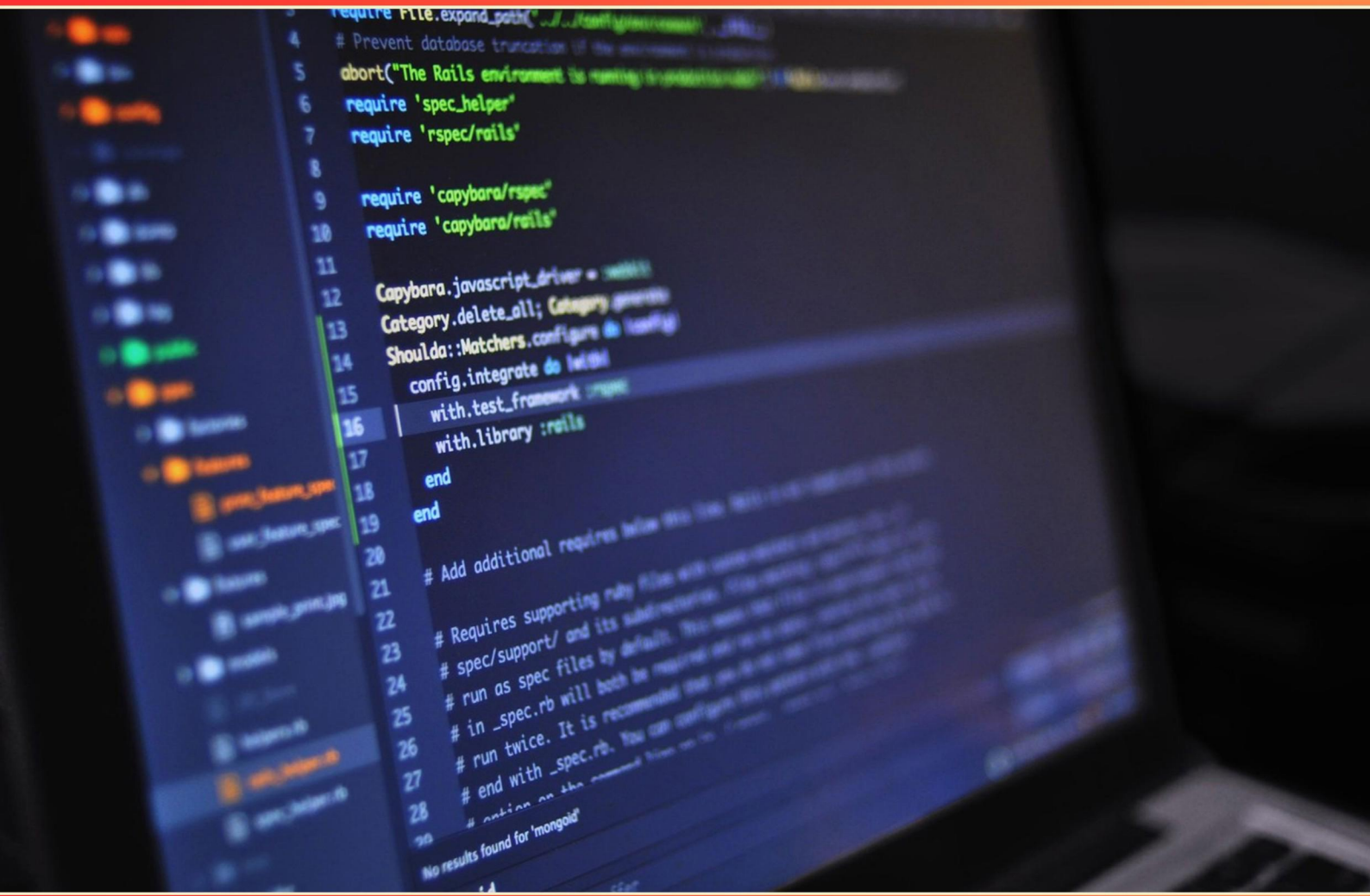
ETHICAL HACKING ESSENTIALS PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://ethicalhackingessentials.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 best describes Level 3 of the Purdue model?

A. Enterprise systems for decision-making

B. Control and monitoring systems

C. Physical processes

D. Manufacturing execution systems

2. Which GDPR protection principle promotes collecting only data necessary for its purpose?

A. Data Integrity

B. Data Minimization

C. Accountability

D. Data Portability

3. Which country has implemented "The Copyright Act 1968" and "The Patents Act 1990"?

A. New Zealand

B. Canada

C. Australia

D. United Kingdom

4. In ethical hacking, what is the ultimate purpose of a denial of service attack?

A. To steal sensitive data

B. To disable services and networks

C. To gain unauthorized access

D. To monitor user behavior

5. Which attack method is commonly used to trick users into revealing sensitive information?

A. Denial-of-service attack

B. SQL Injection

C. Phishing

D. Brute force attack

SAMPLE

6. Which layer of a web application includes the functional programming that can be implemented using .NET, Java, and Python?

A. Service layer

B. Presentation layer

C. Business logic layer

D. Data layer

7. What tool could be used by an attacker to perform a man-in-the-middle attack over a public Wi-Fi network?

A. Aircrack

B. zANTI

C. Wireshark

D. Burp Suite

8. What technique involves keyword stuffing, inserting doorway pages, page swapping, and adding unrelated keywords to boost malware page rankings?

A. Black hat search engine optimization

B. White hat optimization

C. Content marketing

D. Social media promotion

9. David's attack involved using a botnet to launch a DDoS attack. What does DDoS stand for?

A. Distributed Denial of Service

B. Direct Denial of Service

C. Distributed Data Service

D. Dynamic Denial of Service

10. What common practice exposes devices and networks to OT attacks?

A. Regular software updates

B. Using default factory-set passwords

C. Network segmentation

D. Two-factor authentication

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which of the following best describes Level 3 of the Purdue model?

A. Enterprise systems for decision-making

B. Control and monitoring systems

C. Physical processes

D. Manufacturing execution systems

Level 3 of the Purdue model best represents Manufacturing Execution Systems (MES), which serve as a bridge between the control level and enterprise level operations within a manufacturing environment. These systems are crucial in managing and monitoring work-in-progress on the factory floor, ensuring that production runs efficiently and effectively. Manufacturing Execution Systems provide real-time data regarding production metrics, allowing for immediate adjustments to processes based on the performance of machinery, workforce, and materials. This level integrates the physical processes directly with enterprise systems, ensuring that the information flow facilitates informed decision-making and helps optimize operations. The other levels in the Purdue model correspond to different operational aspects; for instance, other options focus on higher-level enterprise systems or physical processes without encapsulating the critical functions performed at Level 3 within the context of production management. This distinction underlines why Manufacturing Execution Systems are specifically identified as defining features of Level 3 in the Purdue model.

2. Which GDPR protection principle promotes collecting only data necessary for its purpose?

A. Data Integrity

B. Data Minimization

C. Accountability

D. Data Portability

The principle that promotes collecting only the data necessary for a specific purpose is known as Data Minimization. This principle is fundamental to the General Data Protection Regulation (GDPR) as it ensures organizations gather only the information that is essential for the intended processing activities. By limiting data collection to what is strictly necessary, Data Minimization helps to reduce the risk of exposing individuals' personal information and enhances user privacy. Organizations are encouraged to carefully evaluate the data they collect, ensuring it aligns with the purpose for which it is intended and avoiding unnecessary accumulation of personal data. This not only fosters trust among users but also complies with GDPR mandates, which emphasize the importance of respecting individuals' privacy and protecting personal data from misuse. In comparison, other principles such as Data Integrity focus on ensuring that personal data is accurate and up-to-date, Accountability requires organizations to take responsibility for their data handling practices, and Data Portability allows individuals to transfer their data between service providers. While all these principles are important, Data Minimization specifically addresses the amount of data collected and its necessity for achieving the stated purpose.

SAMPLE

3. Which country has implemented "The Copyright Act 1968" and "The Patents Act 1990"?

A. New Zealand

B. Canada

C. Australia

D. United Kingdom

Australia is the country that has implemented "The Copyright Act 1968" and "The Patents Act 1990." These laws form the basis of intellectual property rights in Australia, establishing legal frameworks for the protection of creative works and inventions. The Copyright Act 1968 was significant as it set the foundations for copyright law in Australia, regulating how literary, artistic, and other types of work are used and reproduced. Similarly, the Patents Act 1990 provides the legal structure for patenting inventions, giving patent holders the right to exclude others from exploiting their inventions without permission, thereby fostering innovation and creativity in the country. Understanding intellectual property laws like these is crucial for ethical hackers and cybersecurity professionals, as it emphasizes the importance of respecting and protecting intellectual property rights while navigating the digital landscape.

4. In ethical hacking, what is the ultimate purpose of a denial of service attack?

A. To steal sensitive data

B. To disable services and networks

C. To gain unauthorized access

D. To monitor user behavior

The ultimate purpose of a denial of service (DoS) attack is to disable services and networks. This type of attack overwhelms a target system—be it a website, server, or network—by flooding it with excessive requests or malicious traffic, rendering it unable to respond to legitimate user requests. The goal is to disrupt normal functioning, often leading to downtime that can affect availability for users, damage an organization's reputation, and incur financial losses. In contrast, other options such as stealing sensitive data, gaining unauthorized access, or monitoring user behavior are not the primary objectives of a DoS attack. While these actions may be associated with other types of attacks (e.g., data breaches, intrusions, or phishing), they do not align with the fundamental intent of a denial of service, which is specifically focused on making resources unavailable.

SAMPLE

5. Which attack method is commonly used to trick users into revealing sensitive information?

A. Denial-of-service attack

B. SQL Injection

C. Phishing

D. Brute force attack

Phishing is an attack method specifically designed to deceive users into divulging sensitive information, such as usernames, passwords, or credit card numbers. It typically involves the attacker masquerading as a trustworthy entity, often through fraudulent emails or websites that resemble legitimate ones. This manipulation preys on human psychology, prompting users to click on links or provide information under the false pretense of security or urgency. Unlike denial-of-service attacks, which aim to overwhelm systems and disrupt services; SQL injection, which exploits database vulnerabilities to access or manipulate data; and brute force attacks, which involve systematically trying various passwords to gain unauthorized access, phishing uniquely targets the user through emotional and psychological manipulation. This focus on user interaction makes phishing a prevalent and effective method for attackers seeking confidential data.

6. Which layer of a web application includes the functional programming that can be implemented using .NET, Java, and Python?

A. Service layer

B. Presentation layer

C. Business logic layer

D. Data layer

The business logic layer is the component of a web application that handles the core functionality and operational rules of the application. This layer is crucial because it defines the business rules, workflows, and processes that dictate how data can be created, stored, and changed. Languages like .NET, Java, and Python are commonly used to implement this functionality due to their robust frameworks and libraries that support the development of web applications. By handling the logic that governs application behavior, this layer interacts with the presentation layer (which manages user interface elements) and the data layer (which is responsible for data storage and retrieval). The service layer, while important for managing the interaction between the business logic layer and other parts of the application (like APIs), does not itself contain the primary business logic functionality. The presentation layer focuses on what the user sees and interacts with, while the data layer handles the database management, making the business logic layer the correct choice in this context.

SAMPLE

7. What tool could be used by an attacker to perform a man-in-the-middle attack over a public Wi-Fi network?

A. Aircrack

B. zANTI

C. Wireshark

D. Burp Suite

The use of zANTI as a tool for performing a man-in-the-middle attack on a public Wi-Fi network is well-founded. zANTI is specifically designed for penetration testing and assessing the security of Wi-Fi networks. One of its features allows an attacker to intercept and manipulate communications between users on the network, effectively placing them in a man-in-the-middle position. This enables the attacker to capture sensitive information such as login credentials or session cookies. While other tools listed can be utilized for various aspects of network security assessment, they do not focus specifically on man-in-the-middle techniques within the same context as zANTI. For instance, Aircrack is primarily used for cracking WEP and WPA/WPA2 encryption keys, making it a tool for securing or breaking Wi-Fi rather than conducting man-in-the-middle attacks. Wireshark, on the other hand, is a network protocol analyzer that captures traffic for analysis but does not actively manipulate that traffic as required for a man-in-the-middle attack. Burp Suite is mostly used for web application security testing and is not applicable to intercepting network traffic in the manner required for a typical man-in-the-middle attack over Wi-Fi. Thus, zANTI stands out because it effectively combines multiple functionalities required to perform

8. What technique involves keyword stuffing, inserting doorway pages, page swapping, and adding unrelated keywords to boost malware page rankings?

A. Black hat search engine optimization

B. White hat optimization

C. Content marketing

D. Social media promotion

The technique that involves keyword stuffing, inserting doorway pages, page swapping, and adding unrelated keywords to boost malware page rankings is black hat search engine optimization. This approach refers to unethical practices that aim to manipulate search engine algorithms to achieve higher rankings for a website without regard for quality or relevance. Techniques like keyword stuffing involve overloading a webpage with an excessive number of keywords designed to mislead search engines about the content of a page, while doorway pages are created solely for the purpose of ranking high for specific terms and redirecting users to another site. Black hat SEO practices are generally aimed at deceiving both search engines and users, which can lead to penalties or blacklisting from search engine results. In contrast, white hat optimization involves ethical strategies focused on providing valuable content and improving user experience, content marketing emphasizes creating valuable content to attract and engage an audience, and social media promotion utilizes social platforms to increase visibility and engagement. Each of these alternatives operates within ethical guidelines and prioritizes quality and user satisfaction, unlike black hat techniques.

SAMPLE

9. David's attack involved using a botnet to launch a DDoS attack. What does DDoS stand for?

A. Distributed Denial of Service

B. Direct Denial of Service

C. Distributed Data Service

D. Dynamic Denial of Service

DDoS stands for Distributed Denial of Service. This term is used to describe a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of traffic. In a DDoS attack, the traffic is generated from multiple compromised computer systems, which make up the botnet. This distributed approach makes it more challenging to thwart the attack, as the incoming traffic originates from many different sources rather than just one. The pattern of distributing the attack allows the perpetrator to cast a wider net and utilize the power of numerous machines—often unwittingly compromised by malware—to carry out the attack. This is distinct from other forms of denial of service attacks, which may originate from a single source. Understanding the nature of DDoS attacks is essential for both defensive strategies and for recognizing the scale and complexity often associated with such cyber threats.

10. What common practice exposes devices and networks to OT attacks?

A. Regular software updates

B. Using default factory-set passwords

C. Network segmentation

D. Two-factor authentication

Using default factory-set passwords is a significant security vulnerability that can expose devices and networks to operational technology (OT) attacks. Most devices come with standardized usernames and passwords that are well-documented and frequently shared among users, making it easy for attackers to gain unauthorized access if these credentials are not changed. When default credentials are not altered, malicious actors can exploit this weakness to infiltrate systems and devices, leading to potential control over critical infrastructure and sensitive data. This practice undermines the security posture of an organization, making it more susceptible to a myriad of cyber threats. In contrast, implementing regular software updates helps protect against known vulnerabilities, network segmentation limits access to certain parts of the network to enhance security, and two-factor authentication adds an extra layer of security, making it significantly harder for attackers to breach systems. Each of these practices contributes to strengthening defenses against OT attacks, unlike the use of factory-set passwords, which can lead to severe security risks.

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://ethicalhackingessentials.examzify.com

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

SAMPLE