OPERATING SYSTEM SECURITY (OPSEC) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://operatingsystemsecurity.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. How do companion viruses operate?

A. They completely replace the targeted program

B. They embed their code into the targeted program

C. They reside in data files and activate upon file opening

D. They capture user data for malicious purposes

2. What should be the default access level of a file owner?

A. Read-only access.

B. Full access.

C. No access at all.

D. Limited access.

3. What does an Access Control List (ACL) specify for an asset?

A. Which devices can be connected

B. Which users may perform particular actions

C. What software can be installed

D. How many users can access the asset

4. Files in computing are best described as:

A. Different hardware components of a computer

B. Any chunk of data stored in the file system

C. Layers of an operating system

D. Processes executed by the OS

5. What is an operating system?

A. A software system that manages all of the hardware and other software in a system

B. A system that is used to track the progress of IT managers and resources

C. A system used to optimize distribution of network resources

D. A system that is used to track the monetary disbursements

6. Which file system is commonly used by Microsoft Windows?

A. FAT32.

B. ext4.

C. HFS+.

D. NTFS.

SAMPLE

7. What does the security level associated with a process determine?

A. The priority of executing the process.

B. The access rights to system resources.

C. The memory allocation for the process.

D. The execution time of the process.

8. Why are Trojans considered less harmful than viruses?

A. They cannot propagate on their own

B. They only encrypt files

C. They are more visible to antivirus software

D. They are always benign

9. Which layer of the operating system structure handles the actual user applications?

A. Kernel layer

B. Application layer

C. Hardware layer

D. System services layer

10. Which of the following is a key protection offered by a 'trusted' operating system?

A. User Protection

B. Network Speed

C. Software Optimization

D. User Accessibility

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. How do companion viruses operate?

A. They completely replace the targeted program

B. They embed their code into the targeted program

C. They reside in data files and activate upon file opening

D. They capture user data for malicious purposes

Companion viruses operate by embedding their code into a targeted program, which allows them to execute when the legitimate program is launched. This method leverages the trust users have in the original application, as the companion virus is typically designed to have a similar name to the legitimate program. As a result, when a user attempts to run the trusted application, the malicious code embedded in the companion file can run instead, potentially leading to the compromise of the system or the installation of additional malware. The design of companion viruses exploits vulnerabilities in how operating systems handle file execution and can effectively evade detection by users who expect the legitimate program to run without issues. By focusing on embedding their code, these viruses can manipulate the host program's operations, rather than replacing it entirely or residing only in data files. This method makes companion viruses particularly insidious, as they can remain undetected while they execute their malicious tasks.

2. What should be the default access level of a file owner?

A. Read-only access.

B. Full access.

C. No access at all.

D. Limited access.

The default access level for a file owner should be full access. This is because the owner of a file is typically the person who created it and therefore has the most knowledge and responsibility regarding that file. Full access allows the owner to read, write, and execute the file, enabling them to manage its content as needed. Granting full access facilitates efficient file management since the owner can modify or delete the file, share it with others, and adjust permissions as required without needing to seek additional permissions. This default setting aligns with common practices in operating systems to support both usability and control for the file owner, emphasizing the principle of ownership that underlies many permission settings in file management systems. In contrast, read-only access would significantly limit the owner's ability to interact with their own files, while having no access or limited access would be counterproductive, undermining the core intent of file ownership.

3. What does an Access Control List (ACL) specify for an asset?

A. Which devices can be connected

B. Which users may perform particular actions

C. What software can be installed

D. How many users can access the asset

An Access Control List (ACL) specifically indicates which users have permission to perform particular actions on an asset. ACLs are critical components of access control in operating systems and network security. They define the permissions associated with specific resources, such as files or devices, and outline the allowed actions for each user or group of users. By specifying individual users or groups and the actions they are authorized to take—such as read, write, or execute—ACLs enhance security by ensuring that only permitted users can access or modify sensitive assets. This focuses on managing user privileges effectively within the system, which is essential for maintaining data integrity and confidentiality. The other options pertain to different aspects of system security. While connecting devices, installing software, and limiting user access numbers are all relevant to security and resource management, they do not accurately encapsulate the role of an Access Control List. ACLs are specifically concerned with user permissions rather than device connections, software management, or user capacity on resources.

SAMPLE

4. Files in computing are best described as:

A. Different hardware components of a computer

B. Any chunk of data stored in the file system

C. Layers of an operating system

D. Processes executed by the OS

Files in computing are best described as any chunk of data stored in the file system because this definition encompasses the fundamental nature of what a file represents within the context of operating systems. A file serves as a collection of information, which could be text, images, audio, or any other type of data that is stored on a storage device. The file system is the component of the operating system that manages how data is stored and retrieved, organizing files in a manner that allows users and applications to access them efficiently. Files are identified by unique names and can include metadata that provides information about the content, size, and creation date, among other attributes. This description effectively captures the essence of a file, as it highlights the diversity of data types and their organization within the file system. In contrast, the other choices do not accurately encapsulate what files are: different hardware components refer to the physical elements that make up a computer (such as CPU, RAM, etc.), layers of an operating system describe the various abstract levels at which the operating system operates (such as kernel and user space), and processes executed by the operating system relate to active programs or tasks that are being executed, not static collections of data. Therefore, choice B is the most fitting definition

5. What is an operating system?

A. A software system that manages all of the hardware and other software in a system

B. A system that is used to track the progress of IT managers and resources

C. A system used to optimize distribution of network resources

D. A system that is used to track the monetary disbursements

An operating system is fundamentally defined as a software system that manages all of the hardware and other software in a system. It acts as an intermediary between users and the computer hardware, facilitating the running of applications and various processes. By managing hardware resources such as CPU, memory, storage, and input/output devices, the operating system ensures that all components work together smoothly and efficiently. This includes scheduling tasks, managing file systems, and providing a user interface, whether it be command-line or graphical. While the other options describe specific functions or systems related to IT management or network resource optimization, they do not encapsulate the core role of an operating system. Tracking progress, optimizing distribution of resources, or financial disbursement management falls under specific applications or functionalities that might operate on an underlying operating system, rather than defining what an operating system actually is.

SAMPLE

6. Which file system is commonly used by Microsoft Windows?

A. FAT32.

B. ext4.

C. HFS+.

D. NTFS.

The file system commonly used by Microsoft Windows is NTFS (New Technology File System). NTFS offers several advantages over older file systems like FAT32, making it the standard for modern Windows operating systems. NTFS supports larger file sizes and volumes than FAT32, accommodating files larger than 4GB, which is a limitation of FAT32. It also provides enhanced security features, such as file permissions, encryption support, and the ability to log changes to the file system, which improves recovery options in case of corruption or system failure. Additionally, NTFS supports advanced data management features like disk quotas and compression, further showcasing its robustness and suitability for both personal and enterprise environments. In contrast, ext4 is predominantly used by Linux operating systems, and HFS+ is mainly associated with Apple's file systems. While FAT32 is still used in some applications for compatibility reasons, especially with removable media, NTFS is the definitive choice for Windows systems, particularly for their built-in functionality and enhanced features.

7. What does the security level associated with a process determine?

A. The priority of executing the process.

B. The access rights to system resources.

C. The memory allocation for the process.

D. The execution time of the process.

The security level associated with a process primarily determines the access rights to system resources. In operating systems, every process can be assigned a security level that defines what resources it can access and what operations it can perform on those resources. This is a critical aspect of maintaining security, as it allows the system to enforce permissions and protect sensitive data from being accessed or modified by unauthorized processes. When processes run with different security levels, the operating system uses these levels to control which data or resources can be interacted with. For instance, processes with higher security levels may have access to critical system resources while those with lower levels may be restricted to user-level resources. This helps in preventing potential security breaches and ensures that only authorized processes can access sensitive information. The other choices relate to different aspects of process management but do not directly tie into the concept of security levels. For example, process priority is generally managed independently of its security level and is more aligned with how the operating system schedules processes for execution. Memory allocation pertains to how much memory is allocated to a process for its execution, which also does not directly correlate with security levels. Execution time is influenced by various factors, including system load and scheduling algorithms, rather than the security level of a process.

SAMPLE

8. Why are Trojans considered less harmful than viruses?

A. They cannot propagate on their own

B. They only encrypt files

C. They are more visible to antivirus software

D. They are always benign

Trojans are considered less harmful than viruses primarily because they cannot propagate on their own. While both Trojans and viruses can cause damage to systems, the nature of how they spread is fundamentally different. Trojans are deceptive software that tricks users into installing them, often masquerading as legitimate applications or files. They rely on social engineering or user interaction for installation, which means that they cannot replicate or spread to other systems independently. In contrast, viruses attach themselves to legitimate executables and can self-replicate, making them more capable of widespread damage once they infect a hosting system. Understanding this key distinction helps to clarify why Trojans may be viewed as less of a threat in terms of contagion compared to viruses. Their harm often comes from the actions they perform after installation, such as stealing data or creating backdoors, rather than from their ability to spread across networks or systems unassisted.

9. Which layer of the operating system structure handles the actual user applications?

A. Kernel layer

B. Application layer

C. Hardware layer

D. System services layer

The application layer is responsible for managing and executing user applications within the operating system structure. This layer interacts directly with the user and provides the necessary interfaces for software applications to function. It focuses on providing services, processes, and resources such as memory and CPU time that applications need to operate effectively. The application layer encompasses various types of programs, including web browsers, word processors, and games, enabling end-users to perform tasks and access functionalities provided by these user applications. It includes software applications and environments within which they run, facilitating a user-friendly experience. In contrast, the kernel layer manages system resources and is responsible for core functions such as process management, memory management, and hardware interaction but does not directly engage with user applications. The hardware layer consists of the physical components of the computer system, and the system services layer provides essential services for the effective execution of applications but does not directly run user applications themselves. Thus, the application layer is correctly identified as the layer that handles actual user applications.

SAMPLE

10. Which of the following is a key protection offered by a 'trusted' operating system?

A. User Protection

B. Network Speed

C. Software Optimization

D. User Accessibility

A trusted operating system is designed with a focus on security and reliability, crucial for environments that handle sensitive information. User protection in this context refers to the capability of the operating system to enforce access controls and secure user data from unauthorized access. This involves implementing user authentication mechanisms, managing permissions effectively, and ensuring that actions by users do not compromise the security of the system. Trusted operating systems often provide mechanisms like mandatory access control, which helps to restrict the capabilities of users and applications based on predefined policies, thereby protecting user data and the overall integrity of the system. This is essential for maintaining confidentiality, preventing data breaches, and ensuring that users operate within their defined roles in a secure manner. In contrast, the other options, such as network speed, software optimization, and user accessibility, focus on performance and usability rather than security. While these aspects are important for general operating system functionality, they do not address the core function of protecting user data and enforcing secure access controls, which is the hallmark of a trusted operating system.

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://operatingsystemsecurity.examzify.com

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

SAMPLE