WESTERN GOVERNORS UNIVERSITY (WGU) ITAS6291 D488 CYBERSECURITY ARCHITECTURE AND ENGINEERING PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://wgu-itas6291d488.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. **What method can be used to verify that new code changes do not adversely affect existing system functionalities?**

   A. Integration test

   B. Regression test

   C. Acceptance test

   D. Unit test

2. **Which blockchain technology assigns a hash value to each block and includes the hash value of the previous block in the next block's calculation, linking them cryptographically?**

   A. Multiparty computation

   B. Distributed consensus

   C. Hashing

   D. Object storage

3. **APIs play a major role in interacting with which technology that allows applications to run independently in virtual instances?**

   A. SOAR (Security orchestration, automation, and response)

   B. IdP (identity provider)

   C. Containers

   D. Traditional VMs

4. **Which security tool monitors network traffic from a SPAN port but does not block traffic, instead analyzing it for suspicious activity?**

   A. Network intrusion prevention system

   B. File Integrity Monitoring

   C. Network intrusion detection system

   D. Data Loss Prevention

5. **Which Cloud Access Security Broker (CASB) method directs traffic from users at the client network to cloud services but only forwards traffic that complies with organizational policy?**

   A. Forward proxy

   B. Reverse proxy

   C. API-based

   D. Dispersed

SAMPLE

6. What issue occurs when the system checks the state of a resource, but the resource's state changes after the initial check?

A. TOC (Time of Check)

B. Cron

C. Atomic execution

D. TOU (Time of Use)

7. Which network application protocol supports communications within an Operational Technology (OT) network?

A. CAN (Controller Area Network)

B. DDS (Data Distribution Service)

C. SIS (Safety Instrumented System)

D. Modbus

8. What type of data is considered the safest when it is encrypted and stored properly?

A. Data in transit

B. Data in use

C. Data at rest

D. Data in motion

9. What describes the process of bundling certain libraries with an application at compile time?

A. Volatility

B. Exiftool

C. Statically linked library

D. Aircrack-ng

10. Which standard addresses IT security techniques, including the introduction and general model, as well as functional and assurance components?

A. NIST 800-61 (Computer Security Incident Handling Guide)

B. ISO standard 15408

C. NIST 800-84

D. NIST 800-53 (Security and Privacy Controls for Information Systems)

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What method can be used to verify that new code changes do not adversely affect existing system functionalities?

A. Integration test

B. Regression test

C. Acceptance test

D. Unit test

Using a regression test is essential for verifying that new code changes do not negatively impact existing functionalities within a system. The primary focus of regression testing is to ensure that recent updates, enhancements, or bug fixes have not introduced any new faults in previously functioning features. When code changes are made, they can inadvertently affect existing code due to interdependencies or shared components. Regression testing involves re-running a suite of previously conducted tests against the modified codebase to check for any discrepancies in functionality, performance, or security issues that may arise due to the changes. This process ensures that while new features are introduced or existing ones modified, the integrity of the system remains intact, thus confirming that no unintended side effects have occurred. Although integration tests, acceptance tests, and unit tests also play significant roles in the software development life cycle, they serve different purposes. Integration tests focus on verifying interaction between combined units of code, acceptance tests validate the system against business requirements, and unit tests check the functionality of individual components in isolation. However, only regression tests explicitly target the validation of existing features in light of new changes, making it the most appropriate method in this scenario.

2. Which blockchain technology assigns a hash value to each block and includes the hash value of the previous block in the next block's calculation, linking them cryptographically?

A. Multiparty computation

B. Distributed consensus

C. Hashing

D. Object storage

The correct choice addresses the foundational principle of blockchain technology, which relies on hashing to ensure the integrity and security of the data within the chain. In a blockchain, each block contains a unique hash value that represents the data it holds. This hash is generated through a cryptographic hash function, which takes the block's data and produces a fixed-size string of characters. Additionally, each block also includes the hash of the previous block in its own data. This creates a chain of blocks wherein each block is intrinsically linked to its predecessor. This method of linking prevents alterations to any block in the chain, as even a minor change in the data of a block would result in a different hash value. Consequently, the subsequent block, which references the altered hash, would also be invalidated. This ensures a high level of security and trust within the system, as altering any single block requires recalculating the hashes of all following blocks, which is computationally impractical in a well-distributed network. The other options, while related to various aspects of data handling and security, do not specifically describe this unique characteristic of blockchain technology. Multiparty computation refers to a method enabling parties to jointly compute a function without revealing their private inputs. Distributed consensus deals with the mechanisms

SAMPLE

3. APIs play a major role in interacting with which technology that allows applications to run independently in virtual instances?

A. SOAR (Security orchestration, automation, and response)

B. IdP (identity provider)

C. Containers

D. Traditional VMs

APIs are crucial for interacting with containers, as they facilitate communication between containerized applications and the orchestration systems that manage them. Containers are a form of lightweight virtualization that allow applications to run in isolated environments, enabling them to be packaged with all necessary dependencies while sharing the underlying operating system kernel. This design promotes efficiency and scalability. The use of APIs in orchestrating containers, such as through platforms like Kubernetes, allows developers to automate deployment, scaling, and management of containerized applications seamlessly. This can enhance the development lifecycle by enabling continuous integration and continuous deployment (CI/CD) practices. In contrast, while traditional virtual machines (VMs) and technologies like SOAR and identity providers also utilize APIs, they do not provide the same level of efficiency and resource utilization that containers offer. Traditional VMs require more overhead because they run entire operating systems alongside applications, leading to increased resource consumption. SOAR may utilize APIs for integration and automation within security workflows, but it does not focus on application independence in virtual instances. Similarly, an identity provider leverages APIs for authentication and authorization, but it is not related to the architecture of running applications in isolated environments.

4. Which security tool monitors network traffic from a SPAN port but does not block traffic, instead analyzing it for suspicious activity?

A. Network intrusion prevention system

B. File Integrity Monitoring

C. Network intrusion detection system

D. Data Loss Prevention

The correct response, which identifies the tool that monitors network traffic from a SPAN port without blocking it, is indeed a Network Intrusion Detection System (NIDS). NIDS is specifically designed to passively monitor and analyze network traffic in real-time, identifying potentially malicious activity by examining data packets and looking for known attack signatures or anomalies. This capability is crucial for detecting intrusions and suspicious behavior without interfering with network operations, as it functions in a "monitoring-only" capacity. The importance of NIDS lies in its ability to provide alerts on detected threats, allowing security teams to investigate incidents without disrupting normal traffic flows. By analyzing the data captured through a SPAN (Switched Port Analyzer) port, a NIDS can focus on comprehensive traffic analysis, contributing effectively to an organization's security posture. In contrast, other tools listed do not serve the same monitoring purpose without active intervention. A Network Intrusion Prevention System (NIPS) actively blocks or prevents detected threats, which is not what the question describes. File Integrity Monitoring focuses on tracking changes to files and does not analyze network traffic. Data Loss Prevention solutions are concerned with preventing the unauthorized transmission of sensitive information and typically don't monitor traffic at a general level like NIDS. Each of these tools plays unique

SAMPLE

5. Which Cloud Access Security Broker (CASB) method directs traffic from users at the client network to cloud services but only forwards traffic that complies with organizational policy?

A. Forward proxy

B. Reverse proxy

C. API-based

D. Dispersed

The correct choice is a forward proxy because this method actively mediates and controls user traffic to cloud services. When users within an organization's network attempt to access cloud applications, the forward proxy intercepts this traffic and evaluates it against the organization's predefined security policies. Only the traffic that adheres to these policies is allowed to be forwarded to the cloud services, ensuring that any potentially harmful activities or unauthorized access attempts are blocked. This functionality is essential for organizations that need to enforce security measures, such as data loss prevention and compliance with regulatory standards, while enabling cloud adoption. The forward proxy acts as a gatekeeper, facilitating secure access while maintaining control over the data being transmitted. In contrast, a reverse proxy serves a different purpose by sitting in front of cloud services rather than client traffic, managing requests to the cloud. API-based approaches focus on interacting with software interfaces between the cloud and on-premises systems, rather than controlling traffic directly. The dispersed model refers to a hybrid approach that spreads security controls but does not specifically manage traffic compliance as a forward proxy does.

6. What issue occurs when the system checks the state of a resource, but the resource's state changes after the initial check?

A. TOC (Time of Check)

B. Cron

C. Atomic execution

D. TOU (Time of Use)

The issue described in the question pertains to the concept of potential vulnerabilities that arise due to the timing of operations concerning resource states. When a system checks the state of a resource and that state changes after the initial check but before it can utilize the resource, it results in a situation known as a Time of Use (TOU) vulnerability. In this context, the Time of Use condition emphasizes the time gap between checking the resource's state and actually using it. During this interval, the state of the resource may change, leading to unexpected behavior or security vulnerabilities, such as race conditions. This situation is a critical consideration in cybersecurity, where ensuring that resources remain in a consistent state between checks and usage is vital for maintaining system integrity and security. The other concepts mentioned, such as Time of Check (TOC), specifically refer to potential security vulnerabilities that occur at the moment when the state is first checked, potentially creating confusion when associating with TOU vulnerabilities. Cron is related to scheduling tasks and does not directly connect with state checking issues in resource management. Atomic execution, while an important concept in ensuring that operations complete without interruption, is not directly tied to the concern raised in the question regarding state changes between check and use.

SAMPLE

7. Which network application protocol supports communications within an Operational Technology (OT) network?

A. CAN (Controller Area Network)

B. DDS (Data Distribution Service)

C. SIS (Safety Instrumented System)

D. Modbus

Modbus is a widely used network application protocol specifically designed for communication in Operational Technology (OT) environments, particularly in industrial settings. It facilitates the interaction between devices such as programmable logic controllers (PLCs), sensors, and actuators, enabling them to communicate over serial lines or TCP/IP networks. The strength of Modbus lies in its simplicity and ease of implementation, making it a common choice for industrial automation systems. It operates on a master/slave architecture, where a master device controls communication with one or more slave devices, allowing for efficient data exchange. This protocol supports monitoring and control tasks in various industrial applications, including manufacturing systems and process control. Additionally, Modbus is widely recognized for its interoperability across different manufacturers' equipment, aiding in the integration of varied devices in industrial environments. Its ability to facilitate straightforward and reliable communications makes it particularly well-suited for OT networks, where real-time data exchange is crucial for operational efficiency and safety.

8. What type of data is considered the safest when it is encrypted and stored properly?

A. Data in transit

B. Data in use

C. Data at rest

D. Data in motion

Data at rest refers to inactive data stored physically in any digital form (such as databases, data warehouses, and file systems) that is not currently being used or processed. When this type of data is encrypted and stored properly, it is generally considered the safest because encryption renders the data unreadable to unauthorized users. Even if an attacker gains access to the storage medium, the encrypted data will not be useful to them without the appropriate decryption keys. Proper storage practices, including physical security measures and robust encryption protocols, reinforce the security of data at rest. This means that sensitive information can be stored safely and protected effectively against unauthorized access and breaches, leading to a lower risk of data loss or exposure. In contrast, data in transit, data in use, and data in motion each present various vulnerabilities that require specific protections to guard against interception, unauthorized access, or corruption while being transmitted or processed. Therefore, while all types of data need appropriate security measures, data at rest offers a more stable and secure environment when encrypted and properly stored.

SAMPLE

9. What describes the process of bundling certain libraries with an application at compile time?

A. Volatility

B. Exiftool

C. Statically linked library

D. Aircrack-ng

The process of bundling certain libraries with an application at compile time is best described as using a statically linked library. In this approach, all the code from the libraries that the application needs is included directly into the final compiled binary. This means that when the application is run, it does not require the libraries to be present separately on the system, which can simplify deployment and reduce issues related to library versioning. Static linking results in a single executable file that contains all the necessary components for the application to run. This can enhance performance since the program doesn't need to dynamically load libraries at runtime, and it also increases compatibility by ensuring that the application is self-contained. In contrast, the other terms do not pertain to the bundling of libraries at compile time. Volatility refers to the property of data that determines how long it can be stored before it is lost, Exiftool is a tool used for reading and writing metadata from image files, and Aircrack-ng is a suite of tools for assessing the security of Wi-Fi networks. Each of these concepts operates in different domains and does not relate to the static linking process.

10. Which standard addresses IT security techniques, including the introduction and general model, as well as functional and assurance components?

A. NIST 800-61 (Computer Security Incident Handling Guide)

B. ISO standard 15408

C. NIST 800-84

D. NIST 800-53 (Security and Privacy Controls for Information Systems)

The correct choice relates to ISO standard 15408, also known as the Common Criteria for Information Technology Security Evaluation. This standard provides a comprehensive framework for evaluating the security features and capabilities of IT products and systems. It introduces a general model of IT security and delineates functional components, specifying what a product or system needs to have in order to meet certain security standards. ISO 15408 focuses on defining security assurance requirements and evaluating the security functionality of various IT products. This standard serves as a benchmark for product security evaluations, enabling organizations to assess whether products meet specific security requirements. Its structured approach assists in the design, development, and evaluation stages of IT systems, ensuring that they are robust against potential security threats. The other options discuss different aspects of IT security but do not encompass the same breadth. For instance, NIST 800-61 is focused on incident handling procedures rather than a holistic evaluation framework. NIST 800-84 deals with the creation of contingency plans, while NIST 800-53 specifies security and privacy controls for federal information systems but does not provide an overarching model or standard for the evaluation process. Each of these has its specific focus, making ISO 15408 the most suitable choice for addressing comprehensive IT security techniques.

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://wgu-itas6291d488.examzify.com

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

SAMPLE