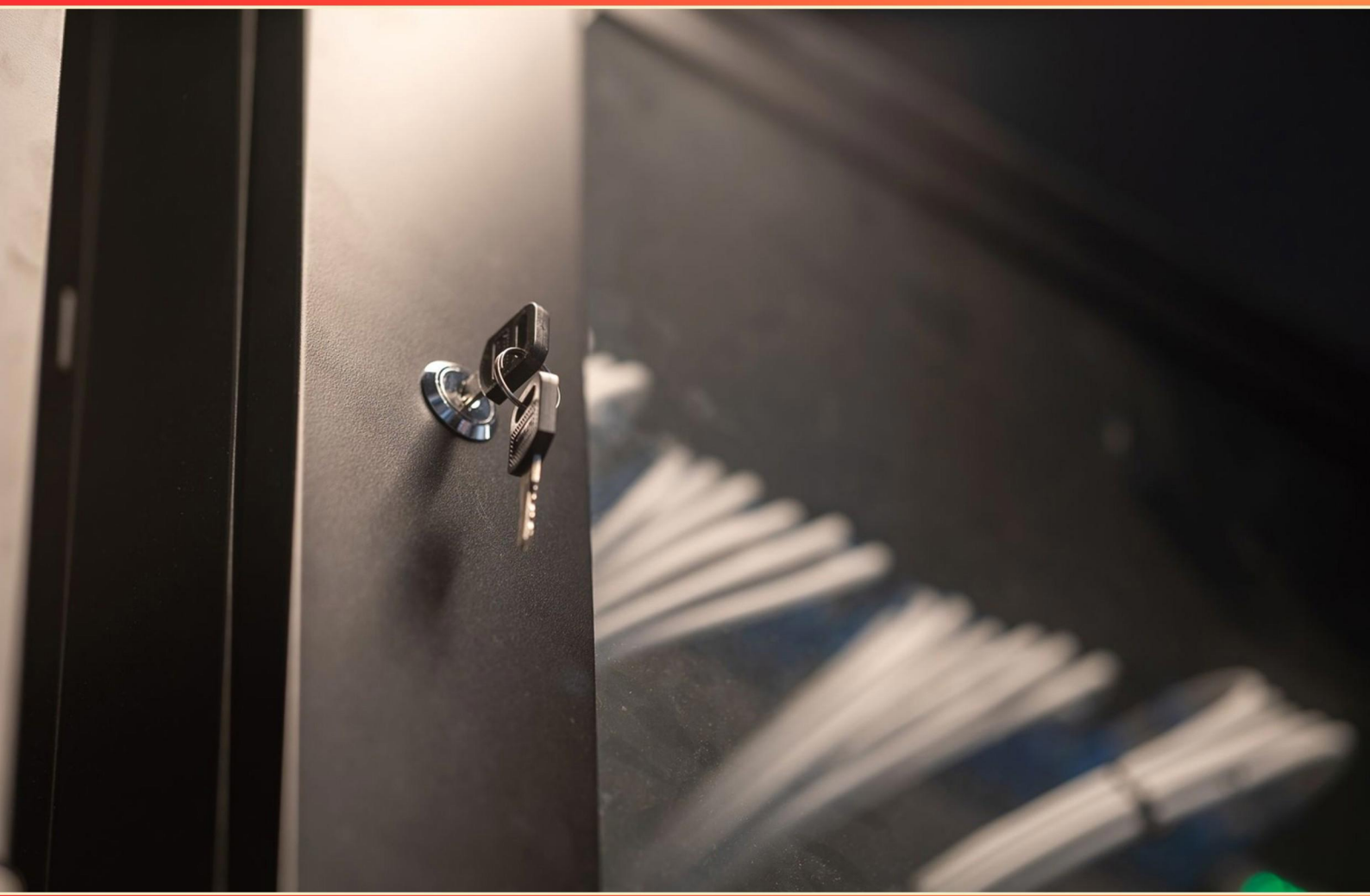
WESTERN GOVERNORS UNIVERSITY (WGU) ITEC2801 D415 SOFTWARE DEFINED NETWORKING PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://wgu-itec2801-d415.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 does the changing attack surface primarily focus on?

A. Identifying existing threats

B. Remediating detected vulnerabilities

C. Adapting to evolving threats

D. Monitoring network traffic

2. Which type of virtual networks are based on logical local area networks?

A. Virtual Private Networks

B. Virtual LANs

C. Cloud Virtual Networks

D. Logical Subnets

3. Which type of attack is based on the intention of the attacker and involves directly interacting with the target?

A. Passive Attack

B. Active Attack

C. Malicious Attack

D. Network Attack

4. What is GRE primarily used for in networking?

A. Establishing encrypted links

B. Transporting data over public networks

C. Optimizing VLAN traffic

D. Defining maximum data sizes for transmission

5. Which version of the OpenFlow protocol is considered the most widespread implementation of SDN?

A. OpenFlow 1.0

B. OpenFlow 1.3

C. OpenFlow 1.5

D. OpenFlow 1.1

SAMPLE

6. What is the role of NFV Management and Orchestration (NFV-MANO)?

A. To provide physical security for network functions

B. To manage and orchestrate Virtual Network Functions and the NFVI

C. To develop hardware specifications

D. To monitor network traffic

7. Which OpenStack module is formerly known as Savanna?

A. Sahara

B. Trove

C. Manila

D. Murano

8. What does NIST 800-125B indicate about firewall rules for better functionality?

A. Use of basic 5-tuple only

B. Support for higher-level components or abstractions

C. Strict adherence to existing configurations

D. Lack of support for dynamic customization

9. What is one of the main goals of network-level Moving Target Defense (MTD)?

A. To improve user interface experience

B. To alter network parameters like configuration and routing

C. To enhance data storage capabilities

D. To implement fixed network pathways

10. What type of service does the DHCP protocol enable on a network?

A. Network tunneling

B. Dynamically assigns IP addresses

C. Manages traffic load balancing

D. Ensures secure communication

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What does the changing attack surface primarily focus on?

A. Identifying existing threats

B. Remediating detected vulnerabilities

C. Adapting to evolving threats

D. Monitoring network traffic

The focus on the changing attack surface is centered around adapting to evolving threats. As technology and network configurations change, so do the potential vulnerabilities and threats that can exploit them. This concept recognizes that new attack vectors can emerge as systems are updated, new applications are deployed, or as user behaviors shift. Staying updated with the changing dynamics of the threat landscape is essential for organizations to maintain effective security postures. Continuous adaptation involves not only recognizing and responding to new threats but also anticipating future vulnerabilities that could arise as a result of these changes. Monitoring existing threats or remediating vulnerabilities are important components of a security strategy; however, they do not fully address the proactive aspect of adapting security measures to align with the constantly changing attack surface. Similarly, while monitoring network traffic is crucial for detecting suspicious activity, it is just one piece of the larger picture that involves adjusting security approaches to counter evolving threats effectively. Therefore, focusing on adapting to evolving threats is vital for staying ahead of potential security risks.

2. Which type of virtual networks are based on logical local area networks?

A. Virtual Private Networks

B. Virtual LANs

C. Cloud Virtual Networks

D. Logical Subnets

Virtual LANs, or VLANs, are designed to create logically segmented networks within a physical network infrastructure. They allow for multiple distinct networks to coexist on a single physical network, effectively enabling separate broadcast domains. This logical segmentation can improve management, security, and efficiency by ensuring that devices within different VLANs cannot directly communicate with each other without a router, even if they are on the same physical network. VLANs operate at the data link layer (Layer 2) of the OSI model, which is why they are closely associated with local area networking concepts. They rely on tagging frames with VLAN identifiers, allowing network devices such as switches to route traffic appropriately based on these tags, rather than solely based on physical connections. The other options, while relevant to networking, do not specifically describe networks that are fundamentally based on the logical structure of local area networks. Virtual Private Networks (VPNs) focus on secure communication over the internet, Cloud Virtual Networks pertain to networks offered within cloud service infrastructures, and Logical Subnets are divisions within an IP network that are used for organization but do not specifically denote the same concept as VLANs.

SAMPLE

3. Which type of attack is based on the intention of the attacker and involves directly interacting with the target?

A. Passive Attack

B. Active Attack

C. Malicious Attack

D. Network Attack

The correct choice refers to an active attack, which is characterized by the attacker's direct interaction with the target. In an active attack, the attacker seeks to alter or disrupt the normal operations of a system. This often involves unauthorized access, data manipulation, or other interference with the system's functions. In active attacks, the intention is clear: to cause harm, manipulate data, or gain unauthorized control, which requires the attacker to engage directly with the target system—whether through exploiting vulnerabilities, injecting malicious code, or conducting denial-of-service attacks. The direct interaction aspect differentiates it from other attack types. In contrast, passive attacks involve monitoring or eavesdropping on communication without altering the data. They do not require engaging with the target system in a manner that could potentially modify it or disrupt services. While malicious attacks can be seen as a broader term encompassing various forms of attacks, it lacks the specificity regarding the attacker's interaction with the target. Network attacks are similarly broad and refer to any attack that targets network infrastructure rather than directly addressing the nature of the attacker's actions. Active attacks specifically highlight the proactive element of the attacker's engagement with their target, solidifying the reason why this option is the most appropriate choice.

4. What is GRE primarily used for in networking?

A. Establishing encrypted links

B. Transporting data over public networks

C. Optimizing VLAN traffic

D. Defining maximum data sizes for transmission

GRE, or Generic Routing Encapsulation, is primarily utilized in networking for transporting a wide variety of network protocols over a specific type of network, particularly public networks such as the internet. It encapsulates packets from various protocols, allowing those packets to be sent over an IP network, which simplifies communication between different types of network architectures. By using GRE, organizations can establish a virtual point-to-point link that can carry data packets from one network to another without needing to define the specifics of the encapsulated protocol. This versatility makes GRE an excellent choice for scenarios where heterogeneous network support is crucial, and it enables the transport of protocols that may not be natively supported by the underlying network. Other choices listed do not accurately describe GRE's primary function: it does not inherently establish encrypted links, optimize VLAN traffic specifically, or define maximum data sizes for transmission. Instead, GRE focuses on providing a method for encapsulation, facilitating the transport of data regardless of the protocol being used.

SAMPLE

5. Which version of the OpenFlow protocol is considered the most widespread implementation of SDN?

A. OpenFlow 1.0

B. OpenFlow 1.3

C. OpenFlow 1.5

D. OpenFlow 1.1

OpenFlow 1.3 is recognized as the most widespread implementation of the Software Defined Networking (SDN) protocol due to its significant enhancements over earlier versions. Released in 2012, this version expanded the functionalities and flexibility of OpenFlow, allowing for more complex network configurations and improved capabilities to manage network traffic. OpenFlow 1.3 introduced support for multiple tables and group actions, which facilitated better handling of different types of network traffic and policies. This level of sophistication made it more appealing for both developers and network administrators, leading to its broader adoption in commercial and research environments. While other versions like OpenFlow 1.0 and 1.1 laid the groundwork for SDN and provided foundational capabilities, they lacked the comprehensive feature set that 1.3 offered. OpenFlow 1.5 made further improvements, but it did not achieve the same level of widespread deployment as 1.3. Therefore, OpenFlow 1.3 stands out as the version that propelled SDN into more practical and extensive usage.

6. What is the role of NFV Management and Orchestration (NFV-MANO)?

A. To provide physical security for network functions

B. To manage and orchestrate Virtual Network Functions and the NFVI

C. To develop hardware specifications

D. To monitor network traffic

The role of NFV Management and Orchestration (NFV-MANO) is crucial in the context of Network Functions Virtualization (NFV). It is primarily responsible for managing and orchestrating Virtual Network Functions (VNFs) along with the underlying Network Functions Virtualization Infrastructure (NFVI). This means that NFV-MANO oversees the deployment, scaling, and interconnection of VNFs, ensuring that they operate efficiently and effectively within the virtualized environment. By managing VNFs, NFV-MANO enables dynamic service provisioning and orchestration, allowing network operators to automate the deployment and management of network services without being tied to physical hardware. NFV-MANO encompasses several components including VNF Managers, NFV Orchestrators, and Virtualized Infrastructure Managers, all of which work together to optimize the utilization of resources and provide flexibility in network service deployment. In contrast, the other options presented do not capture the essence of NFV-MANO's responsibilities. While physical security and hardware specifications are important in networking, they fall outside the specific realm of NFV-MANO's focused task, which is about virtualized network functions rather than physical infrastructure or operational security. Similarly, monitoring network traffic, while critical for network operations, is not a direct responsibility of

SAMPLE

7. Which OpenStack module is formerly known as Savanna?

A. Sahara

B. Trove

C. Manila

D. Murano

The correct choice is Sahara, which is the rebranding of the Savanna project. Sahara is an OpenStack project designed for managing and provisioning big data frameworks, such as Apache Hadoop and Apache Spark. The purpose of Sahara is to simplify the deployment and management of these frameworks within OpenStack environments, allowing users to quickly and efficiently set up clusters for big data processing. The renaming from Savanna to Sahara was part of an effort to better align the project name with its functionality and mission. By adopting a new name, the project aimed to increase clarity and understanding around its objectives and capabilities within the OpenStack ecosystem, making it more accessible to users looking to leverage big data technologies. The other options each represent different OpenStack projects that focus on various functionalities, such as database management, shared file systems, and application management, but are not related to the big data management capabilities served by Sahara.

8. What does NIST 800-125B indicate about firewall rules for better functionality?

A. Use of basic 5-tuple only

B. Support for higher-level components or abstractions

C. Strict adherence to existing configurations

D. Lack of support for dynamic customization

NIST 800-125B emphasizes the importance of utilizing higher-level components or abstractions in the context of firewall rules to enhance their functionality. This approach allows for the implementation of policies and rules that can be managed more easily, adapting to the complex environments often encountered in software-defined networking. By supporting higher-level components, administrators can work with policy-driven configurations instead of just low-level technical parameters. This facilitates a more flexible and efficient management strategy, enabling firewalls to adjust more effectively in response to changing network architectures or security requirements. Moreover, this abstraction can streamline the deployment of security policies across various network segments, increasing the overall effectiveness of the security infrastructure while simplifying monitoring and adjustments. Adopting higher-level abstractions aligns with the goals of NIST in promoting best practices and improving security posture through more adaptable configurations.

SAMPLE

9. What is one of the main goals of network-level Moving Target Defense (MTD)?

A. To improve user interface experience

B. To alter network parameters like configuration and routing

C. To enhance data storage capabilities

D. To implement fixed network pathways

The main goal of network-level Moving Target Defense (MTD) is indeed to alter network parameters like configuration and routing. MTD is a proactive security approach that continuously changes the attack surface to make it more difficult for adversaries to exploit vulnerabilities. By dynamically adjusting configurations, such as routing paths and IP addresses, MTD creates a moving target that attackers must constantly adapt to, thereby increasing the complexity and effort required to successfully launch an attack. This strategy aims to minimize the window of opportunity for attackers, as they are faced with a constantly changing environment. By shifting parameters regularly, the network becomes less predictable, complicating the attackers' task of gathering enough information to execute their attacks effectively. This dynamic nature of MTD is crucial in enhancing the security posture of networks against various cyber threats.

10. What type of service does the DHCP protocol enable on a network?

A. Network tunneling

B. Dynamically assigns IP addresses

C. Manages traffic load balancing

D. Ensures secure communication

The DHCP (Dynamic Host Configuration Protocol) is responsible for dynamically assigning IP addresses to devices on a network. This service simplifies the process of managing IP addresses within a network by automatically providing devices with the necessary configuration parameters, such as their unique IP address, subnet mask, default gateway, and DNS server information. When a device connects to a network, rather than requiring manual configuration of its network settings, DHCP allows for this process to be automated. The DHCP server maintains a pool of various IP addresses and assigns them to client devices on an as-needed basis. This efficiency is particularly beneficial in environments where devices frequently connect and disconnect from the network, as it ensures that IP addresses are utilized effectively and reduces administrative overhead. For the other choices, network tunneling refers to a method of encapsulating data packets within other packets, which is not something that DHCP does. Traffic load balancing involves distributing workloads across multiple resources, which is unrelated to the primary function of DHCP. Ensuring secure communication is typically managed by protocols focused on encryption and authentication, rather than the address assignment tasks addressed by DHCP.

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-itec2801-d415.examzify.com

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

SAMPLE