Western Governors University (WGU) ITEC2112 D315 Network and Security - Foundations Pre-assessment Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

Table of Contents

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.

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!

Questions

1. **Who uses Nessus software to scan servers and network devices for known vulnerabilities?**
    - **A. Script Kiddies**
    - **B. Insider threats**
    - **C. Vulnerability testers**
    - **D. Black hat hackers**

2. **Which of the following are transport layer protocols?**
    - **A. ICMP**
    - **B. TCP and UDP**
    - **C. TFTP**
    - **D. IP**

3. **What is the goal of a Denial of Service (DoS) attack?**
    - **A. To steal data from a system**
    - **B. To disrupt service to intended users**
    - **C. To extort money from users**
    - **D. To gain unauthorized access**

4. **What is the best example of using a public cloud?**
    - **A. A network admin virtualizes a computer on an onsite server for increased reliability.**
    - **B. A cloud engineer moves an application to a company-owned datacenter to increase bandwidth.**
    - **C. An enterprise architect recommends encryption for data in geographically separate datacenters.**
    - **D. A consultant recommends moving a server to AWS to save on costs.**

5. **What can increase the chances of success in a brute force attack?**
    - **A. Strong password policy**
    - **B. Account lockout after failed attempts**
    - **C. Longer password lengths**
    - **D. Commonly used, weak passwords**

6. What are the seven layers of the OSI model in order?

A. Application, Presentation, Session, Transport, Network, Data Link, Physical

B. Session, Presentation, Data Transport, MAC, Network, Physical

C. Physical, Data Link, Network, Transport, Session, Presentation, Application

D. Presentation, Application, Session, Network, Transport, Data Link, Physical

7. What approach is commonly used to provide additional security for user sessions?

A. Two-factor authentication

B. Single sign-on

C. End-to-end encryption

D. LAN segmentation

8. During a cybersecurity exercise, what role involves defending the network during an attack simulation?

A. Red Team

B. Blue Team

C. Black Team

D. White Team

9. Which attack tricks a client into mapping an IP address to a spoofed MAC address?

A. ARP spoofing

B. Evil-twin attack

C. Rogue DHCP server

D. IP starvation

10. Which cloud-hosting model provides exclusive cloud access for a single company?

A. Private

B. Public

C. Community

D. Hybrid

Answers

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

Explanations

1. Who uses Nessus software to scan servers and network devices for known vulnerabilities?

A. Script Kiddies

B. Insider threats

C. Vulnerability testers

D. Black hat hackers

Nessus software is utilized primarily by vulnerability testers. These professionals are tasked with identifying, evaluating, and mitigating security vulnerabilities within systems and networks. By employing Nessus, vulnerability testers can conduct thorough scans that report known weaknesses, enabling organizations to fortify their security posture proactively.   The role of vulnerability testers is rooted in a legitimate desire to enhance security, making use of established, widely respected tools like Nessus to both analyze and provide remediation strategies for discovered flaws. This type of activity is fundamental in maintaining a proactive security framework and ensuring compliance with industry standards. In contrast, the other options represent entities that typically operate outside of authorized security assessments. For instance, script kiddies may use basic tools for malicious activities without a deep understanding of the underlying technology, insider threats are typically individuals within an organization who may misuse access privileges, and black hat hackers engage in unauthorized attacks for personal gain. Each of these groups does not align with the ethical and rigorous approach that vulnerability testers embody when using tools such as Nessus.

2. Which of the following are transport layer protocols?

A. ICMP

B. TCP and UDP

C. TFTP

D. IP

The correct choice identifies TCP and UDP as transport layer protocols, which is a fundamental aspect of network communication. The transport layer is responsible for providing communication services directly to the application processes running on different hosts. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are the two primary protocols operating at this layer, each serving distinct purposes. TCP is a connection-oriented protocol, meaning it establishes a connection before transmitting data and ensures that packets are delivered in order and without errors. It performs error checking through various mechanisms, such as sequence numbers and acknowledgments. This makes TCP ideal for applications where data integrity and order are critical, such as web browsing or file transfers. UDP, on the other hand, is a connectionless protocol that does not establish a dedicated end-to-end connection prior to data transmission. It is faster than TCP because it has minimal overhead, which is beneficial for applications like real-time video or gaming where speed is more important than complete reliability. Other choices reference protocols that do not operate at the transport layer. For instance, ICMP (Internet Control Message Protocol) works at the network layer, primarily used for error reporting and operational information (like the ping command). TFTP (Trivial File Transfer Protocol) is an application layer protocol and

3. What is the goal of a Denial of Service (DoS) attack?

A. To steal data from a system

B. To disrupt service to intended users

C. To extort money from users

D. To gain unauthorized access

The goal of a Denial of Service (DoS) attack is to disrupt service to intended users. In a DoS attack, the attacker aims to make a computer, network, or service unavailable to its intended users by overwhelming it with a flood of illegitimate requests, thereby preventing legitimate users from accessing the services. This disruption is often achieved by exploiting vulnerabilities or consuming resources, which can lead to downtime, degraded performance, or complete unavailability of the target service. While some other types of attacks may focus on stealing data, extorting money, or gaining unauthorized access, the core characteristic of a Denial of Service attack lies specifically in its objective to obstruct user access, rendering the system or service effectively incapacitated. This can have significant ramifications for businesses and individuals who rely on that service, making it a particularly disruptive form of cyber attack.

4. What is the best example of using a public cloud?

A. A network admin virtualizes a computer on an onsite server for increased reliability.

B. A cloud engineer moves an application to a company-owned datacenter to increase bandwidth.

C. An enterprise architect recommends encryption for data in geographically separate datacenters.

D. A consultant recommends moving a server to AWS to save on costs.

The best example of using a public cloud is the recommendation to move a server to AWS to save on costs. Public cloud services, like Amazon Web Services (AWS), provide resources over the internet, allowing businesses to access scalable computing power without the need for physical infrastructure investment and management. This shift can result in significant cost savings since organizations can take advantage of the pay-as-you-go model, paying only for the resources they consume. Utilizing a public cloud such as AWS offers several benefits, including increased scalability, flexibility, and the ability to quickly deploy applications globally. As businesses grow or experience fluctuations in demand, they can easily scale their resources up or down without the financial burden of maintaining excess infrastructure. Furthermore, AWS and other public cloud providers often offer better performance and security than a company might achieve on their own, making this option highly attractive for organizations looking to optimize their IT spending.

5. What can increase the chances of success in a brute force attack?

A. Strong password policy

B. Account lockout after failed attempts

C. Longer password lengths

D. Commonly used, weak passwords

The option regarding commonly used, weak passwords significantly increases the chances of success in a brute force attack because such passwords are easier for attackers to guess. Brute force attacks rely on systematically trying all possible combinations until the correct one is found. If target accounts use weak passwords—like "123456" or "password"—the attacker can quickly crack them without extensive computing power or time. In contrast, strong password policies, account lockouts after multiple failed attempts, and longer password lengths are designed specifically to enhance security. They make brute force attacks more challenging by either preventing repeated attempts, increasing the complexity required to guess passwords, or introducing longer combinations that substantially extend the time it takes to achieve a successful attack. Therefore, weak and common passwords present a vulnerability that attackers can exploit, making this option the most relevant in understanding how to increase success rates in such attacks.

6. What are the seven layers of the OSI model in order?

A. Application, Presentation, Session, Transport, Network, Data Link, Physical

B. Session, Presentation, Data Transport, MAC, Network, Physical

C. Physical, Data Link, Network, Transport, Session, Presentation, Application

D. Presentation, Application, Session, Network, Transport, Data Link, Physical

The correct order of the seven layers of the OSI model is: Physical, Data Link, Network, Transport, Session, Presentation, and Application. This sequence is fundamental to understanding how data communication occurs across networks. Starting from the lowest layer, the Physical layer deals with the physical connection between devices, including the hardware and electrical signals. The Data Link layer is responsible for node-to-node data transfer and error detection/correction. The Network layer is crucial for determining how data is routed from the source to the destination across multiple networks. The Transport layer ensures that data is transferred reliably and in the correct order. Following that, the Session layer establishes, maintains, and terminates connections between applications. The Presentation layer translates the data format from application to network format or vice versa, managing encryption and data compression. Finally, the Application layer interacts directly with end-user applications, providing a way to communicate with the underlying services. This structured approach to networking is essential in diagnosing and troubleshooting network communication issues, as it provides a clear framework for understanding how data moves through the complexities of network systems.

7. What approach is commonly used to provide additional security for user sessions?

A. Two-factor authentication

B. Single sign-on

C. End-to-end encryption

D. LAN segmentation

Two-factor authentication is a widely used approach to enhance the security of user sessions. This method adds an additional layer of security beyond just a username and password, requiring users to present two forms of identification before accessing their accounts. The first factor is typically something the user knows, such as a password, while the second factor might be something the user has, like a smartphone that receives a time-sensitive code, or a hardware token. This dual requirement helps to mitigate the risk of unauthorized access to user accounts, as even if a malicious actor were to obtain the username and password, they would still need the second factor to successfully log in. This increased difficulty in gaining access means that two-factor authentication significantly strengthens the overall security of user sessions, making it a critical practice for protecting sensitive information and preventing data breaches. In contrast, while single sign-on provides convenience by allowing users to authenticate once across multiple applications, it does not necessarily enhance security in the same way. End-to-end encryption focuses on securing data in transit and at rest, but does not address session authentication directly. LAN segmentation is primarily a network security strategy aimed at controlling traffic within networks rather than securing individual user sessions.

8. During a cybersecurity exercise, what role involves defending the network during an attack simulation?

A. Red Team

B. Blue Team

C. Black Team

D. White Team

The role that involves defending the network during an attack simulation is known as the Blue Team. In a cybersecurity context, the Blue Team is responsible for the proactive defense measures, incident response, and maintaining the security posture of an organization's information systems. This includes monitoring network activities, identifying vulnerabilities, and responding to threats in real time. During attack simulations, which are often referred to as red team vs. blue team exercises, the Red Team acts as the attackers trying to breach security defenses, while the Blue Team works to detect and respond to those attacks in order to protect the network. This dynamic not only helps to enhance the security measures in place but also provides valuable insight into how well the organization's defenders can respond to actual threats. The other roles mentioned serve different functions: the Red Team simulates attacks to test security measures, the Black Team generally refers to those who manage operations within a penetration testing framework without an explicit offense/defense label, and the White Team usually oversees the entire process, ensuring that rules are followed and maintaining the integrity of the exercise.

9. Which attack tricks a client into mapping an IP address to a spoofed MAC address?

A. ARP spoofing

B. Evil-twin attack

C. Rogue DHCP server

D. IP starvation

ARP spoofing is the technique that tricks a client into mapping an IP address to a spoofed MAC address by sending forged ARP (Address Resolution Protocol) messages over a local area network. This attack allows an attacker to associate their MAC address with the IP address of another device, often the default gateway. As a result, any data that is intended for that IP address is instead sent to the attacker, which can lead to data interception, session hijacking, or man-in-the-middle attacks. This technique exploits weaknesses in the ARP protocol, which does not provide authentication for ARP messages, making it vulnerable to manipulation. By continuously sending out these spoofed ARP replies, the attacker can maintain the deception over time, effectively controlling the flow of data between devices on the network. In contrast, the other options involve different types of network attacks or configurations. An evil-twin attack involves setting up a fraudulent Wi-Fi network that mimics a legitimate one to capture sensitive data from unsuspecting users. A rogue DHCP server provides incorrect IP configuration, potentially leading to connectivity issues or exposure to attacks. IP starvation refers to the practice of consuming all available IP addresses within a DHCP scope to prevent legitimate devices from obtaining an IP address. Though these are notable threats

10. Which cloud-hosting model provides exclusive cloud access for a single company?

A. Private

B. Public

C. Community

D. Hybrid

The private cloud-hosting model is designed to provide exclusive cloud access for a single organization. This means that all the resources and services in a private cloud environment are dedicated to one company, ensuring that sensitive data is kept secure within its own infrastructure. This exclusivity allows for a high level of customization and control over the cloud environment, enabling organizations to tailor the system to meet their specific needs, governance, and compliance requirements. In a private cloud, the infrastructure can be hosted on-premises or through a third-party service provider, but the key aspect is that the resources are not shared with other organizations. This model is particularly appealing for businesses that handle sensitive data, such as those in healthcare, finance, or government sectors, where security and compliance are paramount. In contrast, the public cloud model is shared among multiple users and organizations, while the community cloud involves collaboration between multiple organizations with shared concerns. A hybrid cloud combines elements of both private and public models, allowing for greater flexibility but still does not provide the exclusivity that the private cloud offers.

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-itec2112-d315-preassessment.examzify.com

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