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

Study Guide

Everything you need from our exam experts!

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. Don’t worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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. **Which protocol is specifically used to protect data over the internet in transit?**

   A. HTTP

   B. FTP

   C. TCP

   D. TLS

2. **Which attack allows an attacker to take control of a database by inserting special commands instead of the intended data?**

   A. SQL Injection

   B. Cross-site scripting

   C. Phishing

   D. Buffer overflow

3. **What type of information does the ipconfig command provide?**

   A. Network settings

   B. User account information

   C. Hardware specifications

   D. Software versions

4. **Which command should be used to manually enter the default gateway for a computer?**

   A. route

   B. ipconfig

   C. arp

   D. netstat

5. **A network admin is configuring an application and needs to be sure that port 4432 is open. Which tool should the admin use?**

   A. Ping

   B. netstat

   C. nmap

   D. TCP_Function

6. Which type of attack sends an email claiming to be from a reputable business in order to entice the recipient to provide sensitive information?

A. Denial-of-service

B. Phishing

C. Password attacks

D. Man-in-the-middle

7. What value does a switch use to determine where to forward data packets?

A. Conf value

B. IP address

C. Port Number

D. MAC Address

8. Which exploit involves breaching the network cable and using a packet sniffer to record traffic?

A. Wiretapping

B. ARP poisoning

C. Port scanning

D. Session hijacking

9. What type of protocol is used to ensure the integrity and reliability of data communications on IP networks?

A. UDP

B. TCP

C. IP

D. HTTP

10. Which network topology has every node connected to every other node?

A. Full mesh

B. Star

C. Bus

D. Ring

Answers

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

Explanations

1. Which protocol is specifically used to protect data over the internet in transit?

A. HTTP

B. FTP

C. TCP

D. TLS

The choice of TLS as the protocol specifically designed to protect data over the internet in transit is accurate. TLS, or Transport Layer Security, provides encryption, authentication, and integrity for communications over a network, ensuring that data sent between clients and servers remains confidential and secure from eavesdropping or tampering. While HTTP is a protocol used for transferring hypertext over the internet, it does not include any security features by default. This makes it vulnerable to various types of attacks, such as man-in-the-middle attacks. FTP is another protocol for transferring files, but like HTTP, it lacks built-in security measures for protecting the data during transmission. TCP (Transmission Control Protocol) is fundamental for data transmission across networks but does not provide encryption or security features on its own. TLS adds a crucial layer of security by encrypting the data, ensuring that only the intended recipients can read it. This makes TLS the appropriate choice for protecting internet communications, as it secures the data in transit effectively.

2. Which attack allows an attacker to take control of a database by inserting special commands instead of the intended data?

A. SQL Injection

B. Cross-site scripting

C. Phishing

D. Buffer overflow

The correct choice addresses a specific type of web security vulnerability that occurs in applications that use SQL databases. SQL Injection involves executing arbitrary SQL code through the input fields of a web application. This method allows attackers to manipulate database queries by injecting malicious SQL statements, which can lead to unauthorized access, data leaks, or even complete control over the database. One of the defining features of SQL Injection is that it exploits flaws in the application's input validation process. When user input is not properly sanitized, attackers can craft inputs that include SQL commands, tricking the application into executing those commands rather than treating them as regular data. This can allow them to retrieve sensitive information, alter data, or perform administrative operations on the database. Understanding SQL Injection is crucial for developing secure applications, as it highlights the importance of implementing proper input validation and utilizing prepared statements or parameterized queries to mitigate this risk.

3. What type of information does the ipconfig command provide?

A. Network settings

B. User account information

C. Hardware specifications

D. Software versions

The ipconfig command is a powerful utility used in Windows operating systems that provides detailed information about network settings. When executed, it displays various configuration settings related to network interfaces, including the IP address, subnet mask, default gateway, and other network-related parameters for all network adapters on the device. This command is essential for troubleshooting network connectivity issues, as it allows users to quickly assess their current network configuration and determine whether any changes are needed. Additionally, the output can help in diagnosing problems such as IP address conflicts and DNS resolution issues. The other choices refer to different types of information that are not associated with the ipconfig command. User account information would relate to user profiles and permissions on the system, hardware specifications pertain to the physical components of the computer like CPU and RAM, and software versions would involve details about installed applications and their versions. Thus, only the option related to network settings accurately describes the information provided by the ipconfig command.

4. Which command should be used to manually enter the default gateway for a computer?

A. route

B. ipconfig

C. arp

D. netstat

The command that is used to manually enter the default gateway for a computer is the route command. This command interacts with the IP routing tables in a computer's operating system. By using route, you can add, delete, or modify the routes that dictate how packets find their way to the specified destination, including the default gateway. Setting the default gateway is crucial for enabling a computer to communicate outside its local network. The default gateway serves as a routing device that forwards packets from the local network to other networks. While ipconfig can display the current configuration of the default gateway and other network settings, it does not allow for manual entry or modification of those settings. The arp command is used for managing the Address Resolution Protocol cache, which maps IP addresses to MAC addresses, but it does not deal with routing. Netstat is primarily used for displaying network connections and statistics, which also does not involve setting the default gateway.

5. A network admin is configuring an application and needs to be sure that port 4432 is open. Which tool should the admin use?

A. Ping

B. netstat

C. nmap

D. TCP_Function

Using nmap is a highly effective choice for determining whether a specific port, such as 4432, is open on a network host. nmap, short for Network Mapper, is a powerful tool for network discovery and security auditing. It allows administrators to scan a specified IP address or range of addresses and list the open ports, services running, and potentially even identify the operating system of the host. When the network admin uses nmap to check port 4432, the tool sends SYN packets to that port on the target system. Depending on the response received, nmap can determine if the port is open, closed, or filtered by a firewall. This level of detail is crucial for administrators to verify that the necessary services are accessible and to ensure proper functioning of the application. While other tools like ping or netstat have their uses, they are not designed to check for open ports in the same comprehensive manner. Ping simply tests connectivity and response time to a system but does not provide detailed information about port status. Netstat reflects current TCP/IP connections and listening ports on the local machine but does not scan or probe other systems. Therefore, for the specific task of checking if a particular port is open, nmap is the most appropriate and effective tool

6. Which type of attack sends an email claiming to be from a reputable business in order to entice the recipient to provide sensitive information?

A. Denial-of-service

B. Phishing

C. Password attacks

D. Man-in-the-middle

The attack described involves sending an email that pretends to be from a reputable business, aimed at tricking the recipient into revealing sensitive information, such as passwords or credit card details. This method is characteristic of phishing attacks, which exploit social engineering techniques to impersonate trusted entities. Phishing often involves emails that may contain links to fake websites designed to look legitimate, where unsuspecting users are prompted to enter their personal information. The success of phishing relies on creating a sense of urgency or trust, leveraging the familiar branding of the impersonated organization. It is one of the most common cyber threats, highlighting the importance of user awareness and caution when handling emails that request personal data. In contrast, a denial-of-service attack focuses on overwhelming a system with traffic to make it unavailable, while password attacks typically involve trying to gain unauthorized access to accounts through various techniques such as brute force. A man-in-the-middle attack involves the interception of communication between two parties without their knowledge, rather than directly soliciting information through deceptive communications.

7. What value does a switch use to determine where to forward data packets?

A. Conf value

B. IP address

C. Port Number

D. MAC Address

A switch uses the MAC address to determine where to forward data packets. Each device on a network has a unique Media Access Control (MAC) address assigned to its network interface. When a switch receives a data packet, it examines the packet's destination MAC address and checks its MAC address table (also known as a forwarding table or content addressable memory). This table lists the MAC addresses of devices on the network along with the ports on which they are connected. By consulting this table, the switch can intelligently forward the packet only to the port that leads to the intended recipient device, thereby minimizing unnecessary traffic on other ports and improving overall network efficiency. The reliance on MAC addresses allows switches to operate at Layer 2 of the OSI model, which focuses on data link layer functionalities. Using MAC addresses for forwarding is fundamental to the operation of Ethernet networks, where switches play a crucial role in facilitating communication between devices.

8. Which exploit involves breaching the network cable and using a packet sniffer to record traffic?

A. Wiretapping

B. ARP poisoning

C. Port scanning

D. Session hijacking

Wiretapping is the correct answer because it refers to the interception of communications through a physical connection to a network cable. In the context of network security, wiretapping involves an unauthorized individual physically breaching the integrity of a network cable with the intent to capture the data packets that flow through it. Using a packet sniffer, they can record and analyze this traffic, potentially gaining access to sensitive information. The context surrounding this topic includes various network attacks. For instance, ARP poisoning involves sending falsified Address Resolution Protocol messages over a local area network, which can redirect traffic but does not specifically entail breaching a physical cable. Port scanning is a method for identifying active ports and services on a host, which relies on probing rather than capturing already transmitted data. Session hijacking occurs when an attacker takes control of a user session after successfully exploiting it, which also doesn't involve direct access to network cables or real-time traffic interception through physical means. Thus, wiretapping distinctly captures the act of snatching data directly from a physical connection, making it the most appropriate choice.

9. What type of protocol is used to ensure the integrity and reliability of data communications on IP networks?

A. UDP

B. TCP

C. IP

D. HTTP

The correct answer is TCP, which stands for Transmission Control Protocol. TCP is designed to provide reliable and ordered delivery of data packets over an IP network. It establishes a connection between the sender and the receiver before data transmission begins, allowing it to monitor the communication process and ensure that all packets arrive in the correct order and without any errors. If any packets are lost or corrupted during transmission, TCP has built-in mechanisms to request retransmission, further enhancing data integrity and reliability. Unlike UDP (User Datagram Protocol), which is connectionless and does not guarantee delivery or order, TCP is focused on providing a robust communication channel by implementing flow control, error checking, and acknowledgment of received packets. This makes TCP ideal for applications where data accuracy is critical, such as web browsing, file transfers, and email communications. While IP (Internet Protocol) is essential for routing and addressing packets across networks, it does not provide reliability or integrity checks on its own. HTTP (Hypertext Transfer Protocol), on the other hand, operates on top of TCP and is specifically designed for transferring web pages and related content but does not inherently ensure data integrity in the same way TCP does.

10. Which network topology has every node connected to every other node?

A. Full mesh

B. Star

C. Bus

D. Ring

A full mesh topology is the correct answer because, in this topology, each node has a direct connection to every other node within the network. This design ensures that there is a dedicated link between any pair of devices, facilitating high redundancy and reliability. If one connection fails, the other nodes can still communicate with one another through alternative paths. This topology is particularly beneficial for applications where performance and fault tolerance are critical, although it can be expensive and complex to implement due to the requirements for numerous network cables and ports. In contrast, other topologies like star, bus, and ring each have distinct connection methods that do not involve direct connections among all nodes. For instance, a star topology connects all nodes to a single central hub, a bus topology has all nodes connected along a single communication line, and a ring topology connects nodes in a circular path. These structural differences lead to various impacts on performance, reliability, and scalability compared to a full mesh topology.

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!