CodeHS Cybersecurity Level 1 Certification Practice Test (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. 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. Which protocol is specifically used for changing configuration parameters in network devices?

A. DHCP

B. SNMP

C. HTTP

D. FTP

2. What is a common defense against phishing attempts?

A. Updating software regularly

B. Using two-factor authentication

C. Only opening emails from known senders

D. Disconnecting from the internet

3. What is a primary purpose of using encryption like WPA3?

A. To speed up the connection

B. To make the network publicly accessible

C. To secure wireless communication against unauthorized access

D. To improve device compatibility

4. What does the 'nbstat' command provide information about?

A. Wireless signal strength

B. TCP/IP statistics and information

C. Router configurations

D. Internet speed tests

5. What is an exploit in cybersecurity terms?

A. A vulnerability in operating systems

B. A method for data recovery

C. A sequence of commands that takes advantage of vulnerabilities

D. A tool for scanning networks

6. What is the significance of a digital signature?

- **A. It is used to encrypt sensitive information**
- **B. It verifies the authenticity and integrity of a message or document**
- **C. It helps in data compression for storage**
- **D. It creates a backup of important files**

7. What aspect of cybersecurity does social media primarily impact?

- **A. Data encryption practices**
- **B. Physical building security**
- **C. Personal information availability that can be exploited**
- **D. Network hardware performance**

8. What technology does Near Field Communication (NFC) use?

- **A. Long-range radio waves**
- **B. Short-range communication between compatible devices**
- **C. Infrared signals**
- **D. Cable connections**

9. What does phishing refer to in the context of cybersecurity?

- **A. A type of malware**
- **B. A technique to steal devices**
- **C. A method of deceiving individuals into providing personal information**
- **D. A form of network monitoring**

10. Which of the following is a resizable container that stores an ordered collection of items?

- **A. Array**
- **B. Float**
- **C. Vector**
- **D. Object**

Answers

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

Explanations

1. Which protocol is specifically used for changing configuration parameters in network devices?

A. DHCP

B. SNMP

C. HTTP

D. FTP

The correct choice, which is SNMP, stands for Simple Network Management Protocol. This protocol is widely used for network management, allowing administrators to monitor and configure network devices such as routers, switches, and servers. SNMP facilitates the collection of data from these devices, enabling the updating of configuration parameters, monitoring performance, and managing network operations from a centralized location. SNMP operates by allowing devices (agents) to send and receive information through a management station, which can request changes or report on the status of the device. This functionality is crucial for maintaining and managing networks efficiently. The use of SNMP helps ensure devices are configured correctly and can be modified as necessary to optimize performance or address security concerns. Other options like DHCP, HTTP, and FTP serve different purposes. For example, DHCP (Dynamic Host Configuration Protocol) is used for assigning IP addresses to devices on a network, rather than changing configuration settings. HTTP (Hypertext Transfer Protocol) is designed for transferring web pages and data over the internet, while FTP (File Transfer Protocol) is primarily focused on transferring files between computers. None of these protocols provide the specific capability for changing configuration parameters in network devices in the same way SNMP does.

2. What is a common defense against phishing attempts?

A. Updating software regularly

B. Using two-factor authentication

C. Only opening emails from known senders

D. Disconnecting from the internet

A common defense against phishing attempts involves being cautious about the emails one interacts with, particularly in only opening emails from known senders. Phishing emails typically impersonate trustworthy entities, hoping to deceive recipients into clicking on malicious links or providing sensitive information. By only engaging with emails from trusted sources, individuals can significantly reduce the likelihood of falling victim to these types of scams. While the other options may enhance overall cybersecurity practices, they do not specifically target phishing. Regular software updates help to patch vulnerabilities but do not prevent phishing attempts themselves. Two-factor authentication provides an extra layer of security for account access but does not stop phishing from occurring. Disconnecting from the internet is not a practical or effective strategy, as it would inhibit normal online activities while leaving other aspects of security unaddressed. Therefore, maintaining vigilance regarding the source of emails is an essential and direct approach to combatting phishing.

3. What is a primary purpose of using encryption like WPA3?

A. To speed up the connection

B. To make the network publicly accessible

C. To secure wireless communication against unauthorized access

D. To improve device compatibility

The primary purpose of using encryption methods like WPA3 is to secure wireless communication against unauthorized access. WPA3 (Wi-Fi Protected Access 3) enhances the security of Wi-Fi networks by employing advanced encryption protocols that protect the data being transmitted over the network. This encryption helps to ensure that only authorized users can access the network and its resources, safeguarding sensitive information from eavesdropping or interception by malicious actors. By securing wireless communication, WPA3 also promotes trust and integrity in the way data is shared and transmitted over the airwaves, which is particularly important in an increasingly connected world where cyber threats are prevalent. The focus on securing data helps to maintain privacy and confidentiality for users connected to the network. Other options are not aligned with the fundamental purpose of WPA3. Speeding up the connection and improving device compatibility do not relate directly to encryption, while making the network publicly accessible contradicts the primary intention of securing the connection.

4. What does the 'nbstat' command provide information about?

A. Wireless signal strength

B. TCP/IP statistics and information

C. Router configurations

D. Internet speed tests

The 'nbstat' command is specifically designed to provide information about the NetBIOS over TCP/IP protocol. This command is useful for troubleshooting and monitoring in networks that utilize NetBIOS, which is commonly used in Windows environments. It can display various types of information such as the name table for a computer, active sessions, and any NetBIOS names registered on the local machine. While the options touch on a variety of network-related topics, the 'nbstat' command is not related to wireless signal strength, router configurations, or internet speed tests. Instead, it focuses specifically on TCP/IP statistics and details related to NetBIOS, making it a valuable tool for network administrators dealing with problems in LANs or needing to assess NetBIOS communications. Understanding the function of this command can aid in diagnosing issues and assessing the health of a network.

5. What is an exploit in cybersecurity terms?

A. A vulnerability in operating systems

B. A method for data recovery

C. A sequence of commands that takes advantage of vulnerabilities

D. A tool for scanning networks

In cybersecurity, an exploit is defined as a sequence of commands or code specifically crafted to take advantage of a vulnerability present in software, hardware, or a network system. This often involves unauthorized access or control over a system, allowing an attacker to perform malicious actions such as stealing data, injecting malware, or disrupting services. An exploit exploits a weakness, leveraging it to achieve a specific, often harmful outcome. Understanding this concept is vital as it emphasizes the relationship between vulnerabilities (flaws or weaknesses in a system) and exploits (the methods attackers use to take advantage of these weaknesses). While vulnerabilities are the targets, exploits are the means of attack. This understanding helps cybersecurity professionals fortify systems by patching vulnerabilities before they can be exploited.

6. What is the significance of a digital signature?

A. It is used to encrypt sensitive information

B. It verifies the authenticity and integrity of a message or document

C. It helps in data compression for storage

D. It creates a backup of important files

A digital signature plays a crucial role in cybersecurity by verifying the authenticity and integrity of a message or document. When a digital signature is applied, it establishes that the message or document comes from a specific sender and has not been altered in transit. This is accomplished through cryptographic techniques, typically involving a public and private key pair. When a sender creates a digital signature, they use their private key to generate a unique string of data. The recipient, or any other party, can then use the sender's public key to verify that the signature matches the original message, confirming that it has not been tampered with. This process enhances trust in digital communications and transactions, which is especially important in environments where secure data exchange is critical, such as financial institutions or legal documents. The other choices represent different aspects of data handling and security that do not align with the primary function of a digital signature. While encryption is essential for protecting the confidentiality of information, it does not directly relate to authenticity or integrity verification. Data compression is unrelated to the verification process, as it deals with reducing file sizes rather than confirming their integrity. Additionally, creating backups does not involve signatures but focuses on preserving data for recovery purposes. Thus, the significance of a digital signature is central to

7. What aspect of cybersecurity does social media primarily impact?

A. Data encryption practices

B. Physical building security

C. Personal information availability that can be exploited

D. Network hardware performance

Social media has a significant impact on the availability of personal information that can be exploited, as individuals often share a wealth of details about their lives online. This information can include location data, personal interests, and even sensitive information such as birthdays, contact details, and employment status. Cybercriminals can utilize this openly shared information for various malicious purposes, including identity theft, phishing attacks, and social engineering tactics to deceive individuals. The nature of social media encourages users to connect and share, but this can inadvertently create vulnerabilities. By understanding an individual's online presence and the information disclosed, attackers can craft targeted attacks that are more likely to succeed. Therefore, the relationship between social media and the exposure of personal information plays a critical role in the field of cybersecurity, making the choice regarding personal information availability particularly relevant.

8. What technology does Near Field Communication (NFC) use?

A. Long-range radio waves

B. Short-range communication between compatible devices

C. Infrared signals

D. Cable connections

Near Field Communication (NFC) technology operates through short-range communication between compatible devices. This capability allows two devices, such as smartphones or contactless payment systems, to exchange data when they are placed within a few centimeters of each other. The design of NFC enables secure connections suitable for transactions and information sharing by maintaining a very limited communication range. This makes it ideal for applications like mobile payments, ticketing, and pairing devices effortlessly, as the close proximity reduces the risk of interception by outside parties. The emphasis on short-range ensures convenience without sacrificing security, as it limits the scope of potential vulnerabilities associated with longer-range communication technologies. Thus, the ability to connect and communicate within such a short distance is a fundamental characteristic of NFC technology.

9. What does phishing refer to in the context of cybersecurity?

A. A type of malware

B. A technique to steal devices

C. A method of deceiving individuals into providing personal information

D. A form of network monitoring

Phishing refers to a method of deceiving individuals into providing personal information by impersonating legitimate entities. In the context of cybersecurity, this often involves the use of deceptive emails, messages, or websites that appear authentic, tricking users into revealing sensitive information such as passwords, credit card numbers, or social security numbers. The aim is to exploit trust and manipulate individuals into taking actions that compromise their personal data security. The other choices do not accurately describe phishing. While malware involves malicious software designed to harm or exploit devices, phishing typically focuses on human interaction rather than software attacking a system. Stealing devices is associated with physical theft and is not related to the deceptive practices characteristic of phishing. Network monitoring is a legitimate practice used for security purposes, differing greatly from the intent to deceive and solicit personal information that defines phishing.

10. Which of the following is a resizable container that stores an ordered collection of items?

A. Array

B. Float

C. Vector

D. Object

A resizable container that stores an ordered collection of items is known as a vector. In programming, a vector is designed to grow and shrink as items are added or removed, making it flexible and dynamic in use. This characteristic allows vectors to manage collections of varying sizes effectively, unlike static data structures such as arrays, which have a fixed size once declared. Vectors also maintain the order of the elements as they were inserted, allowing for easy access and manipulation of the items stored within. This makes them ideal for scenarios where the number of elements is not known beforehand and can change during execution. On the other hand, arrays have a set size that cannot be altered after creation. Floats are a data type for representing decimal numbers and do not function as containers for collections. Objects, while they can encapsulate various groups of data and methods, do not inherently provide the resizable collection capability that vectors do. Thus, the defining characteristics of vectors make it the correct answer in this context.

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://codehscyberseclvl1.examzify.com

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