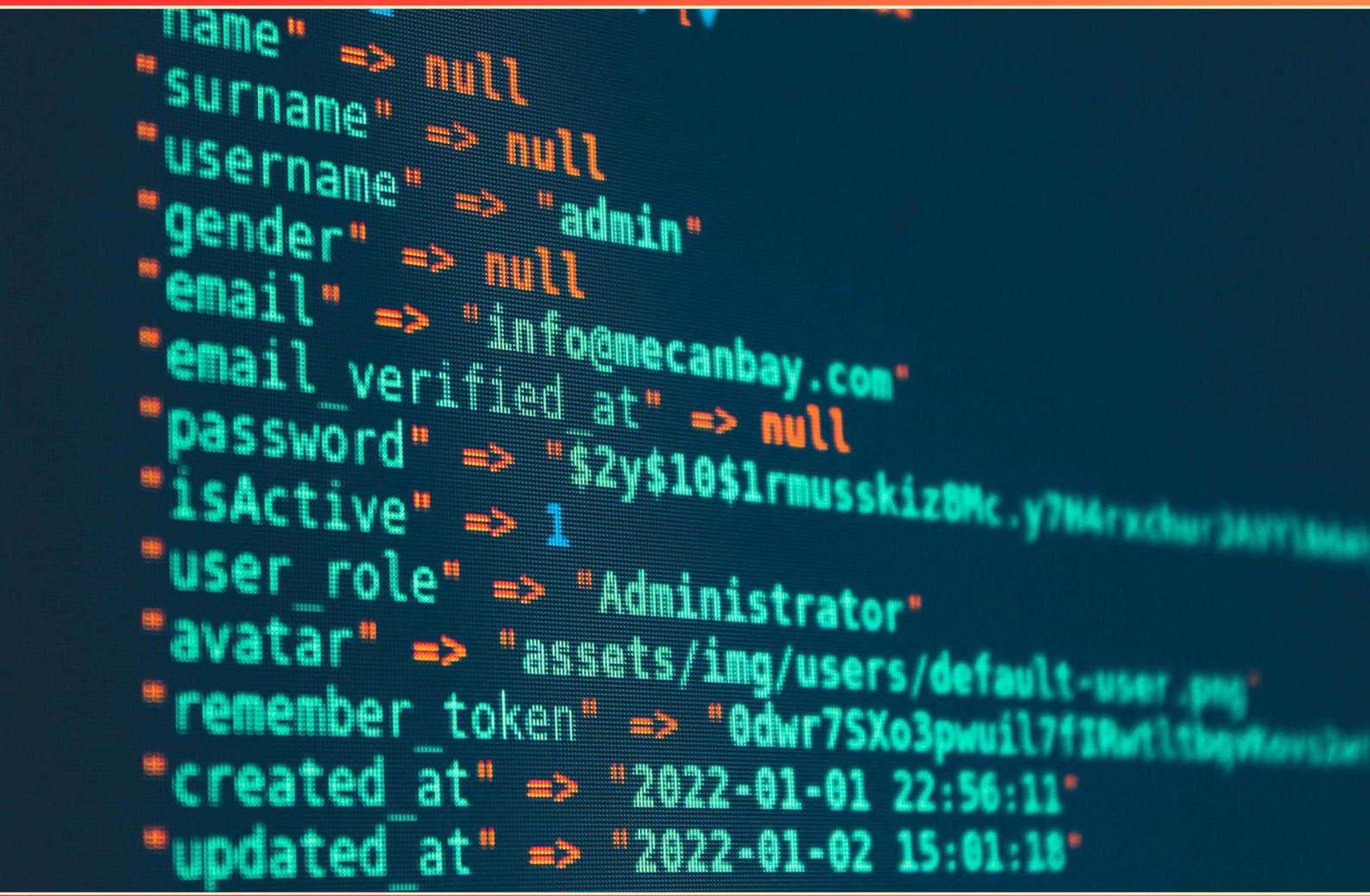
CCST CYBERSECURITY PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://ccstcybersec.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 15

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. **Which Cisco solution provides protection before, during, and after an attack?**

   A. Cisco Advanced Malware Protection

   B. Cisco Web Security Appliance

   C. Cisco Identity Services Engine

   D. Cisco AnyConnect

2. **Knowingly accessing any computer used in or affecting interstate or foreign commerce without permission is a CFAA violation.**

   A. Reading a book about cybersecurity

   B. Accessing a computer you own without permission

   C. Accessing a government computer with permission

   D. Knowingly accessing any computer used in or affecting interstate or foreign commerce without permission

3. **Which of the following is a recognized threat source type?**

   A. Accidental

   B. Structural or Environmental

   C. Strategic

   D. Adversarial

4. **Which of the following statements correctly describes ipconfig on Windows?**

   A. A Linux command that can be used to display IP address configuration parameters on a PC.

   B. A Mac command that can be used to renew DHCP leases.

   C. A Microsoft Windows command that can be used to display IP address configuration parameters on a PC.

   D. A Windows command to format a disk.

5. **The Gramm-Leach-Bliley Act (GLBA) primarily governs privacy and protection of what type of information?**

   A. Financial information of consumers

   B. Medical records

   C. Educational records

   D. Criminal history

SAMPLE

6. Which statement best describes camouflage in security coding techniques?

A. The process of hiding original data within random characters or data.

B. Camouflage replaces sensitive data with realistic fictional data.

C. Rigorously checking user inputs before processing.

D. Ensuring safe display through encoding.

7. Which technology protects the integrity of data in transit?

A. Encrypting data with strong ciphers

B. Digitally signing the data

C. Reducing data size through compression

D. Hashing

8. Which of the following is a packet sniffing tool?

A. Tcpdump

B. Fiddler

C. Nping

D. NetStumbler

9. What is the default number of lines displayed by the head command?

A. Five lines

B. Ten lines

C. Fifteen lines

D. Twenty lines

10. TCP port 21 is used by:

A. FTP - Control

B. SSH

C. DNS

D. SFTP

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which Cisco solution provides protection before, during, and after an attack?

A. Cisco Advanced Malware Protection

B. Cisco Web Security Appliance

C. Cisco Identity Services Engine

D. Cisco AnyConnect

Protection across the entire attack lifecycle is what Cisco Advanced Malware Protection is designed to deliver. It provides pre-execution defenses to block threats before they run by using file reputation and cloud-based analysis, so unknown files can be stopped before any harm occurs. It continues to work during an attack by real-time detection and containment for active threats, preventing them from spreading or executing further. And it extends after an incident with retrospective security, which analyzes past activity to uncover stealthy or dormant threats, pinpoint affected endpoints, and guide remediation. This end-to-end capability across prevention, detection/containment, and post-incident analysis is what makes it the best fit for protection before, during, and after an attack. The other options focus on narrower areas: a web security appliance guards web traffic and downloads, not the full lifecycle across all endpoints; identity services engine handles access control and posture assessment rather than malware protection; and AnyConnect is a secure remote access client, primarily for connectivity, with only limited integrated endpoint protection.

2. Knowingly accessing any computer used in or affecting interstate or foreign commerce without permission is a CFAA violation.

A. Reading a book about cybersecurity

B. Accessing a computer you own without permission

C. Accessing a government computer with permission

D. Knowingly accessing any computer used in or affecting interstate or foreign commerce without permission

Unauthorized access to computers that are involved in or affect interstate or foreign commerce is what the CFAA criminalizes when done knowingly and without permission. The statement matches this exact prohibition: it describes knowingly accessing a computer that plays a role in interstate or foreign commerce without authorization. The key elements—intent, lack of permission, and the broad protected computer scope—are all present, which is why this choice is correct. Reading a book about cybersecurity doesn't involve accessing a computer. Accessing a computer you own without permission could be a violation only if you don't have authorization for that specific access, but ownership isn't itself a guarantee of CFAA coverage. Accessing a government computer with permission is clearly authorized, not a violation.

SAMPLE

3. Which of the following is a recognized threat source type?

A. Accidental

B. Structural or Environmental

C. Strategic

D. Adversarial

Threats are categorized by where they come from, which helps you understand who or what could exploit a vulnerability. An adversarial threat source is about deliberate, intentional acts by people or groups aiming to harm, steal, or disrupt. This makes it a recognized threat source type because it focuses on purposeful attacks and the actions an attacker might take, such as hacking, social engineering, or insider abuse. Understanding this helps you design defenses that specifically address intentional wrongdoing, like strong authentication, continuous monitoring, and robust incident response. Other categories—accidental threats from human error, structural or environmental threats from physical conditions or disasters, and strategic threats from high-level decisions or competition—describe different ways risks can arise, but the key concept here is recognizing that intentional, malicious actors are a distinct and important threat source.

4. Which of the following statements correctly describes ipconfig on Windows?

A. A Linux command that can be used to display IP address configuration parameters on a PC.

B. A Mac command that can be used to renew DHCP leases.

C. A Microsoft Windows command that can be used to display IP address configuration parameters on a PC.

D. A Windows command to format a disk.

ipconfig is the Windows command-line utility used to view the IP address configuration of your PC. When you run it in Command Prompt, it shows the IP address, subnet mask, and default gateway for each network adapter. Using the /all option provides additional details like the MAC (physical) address, DNS servers, DHCP server, and lease information. It's not a Linux or Mac command, and it isn't used to format disks. So the statement that describes it as a Microsoft Windows command to display IP address configuration parameters on a PC is correct.

5. The Gramm-Leach-Bliley Act (GLBA) primarily governs privacy and protection of what type of information?

A. Financial information of consumers

B. Medical records

C. Educational records

D. Criminal history

GLBA focuses on protecting consumers' financial information held by financial institutions. It defines nonpublic personal information and requires financial institutions to provide clear privacy notices, implement safeguards to protect that data, and limit how such information can be shared with others (often with an opt-out option). The safeguards, privacy, and pretexting protections collectively address the privacy of financial data across banks, securities firms, insurance companies, and other entities that handle consumer financial information. This is why the correct choice describes financial information of consumers. Medical records, educational records, and criminal history are covered by different laws and regulatory frameworks.

SAMPLE

6. Which statement best describes camouflage in security coding techniques?

A. The process of hiding original data within random characters or data.

B. Camouflage replaces sensitive data with realistic fictional data.

C. Rigorously checking user inputs before processing.

D. Ensuring safe display through encoding.

Camouflage in security coding means masking real values by substituting them with believable, fake data so the system or its outputs still look realistic without exposing actual sensitive information. This approach preserves the structure and context of the data, which is important for testing, debugging, or sharing data with third parties while keeping sensitive values safe. The option that describes this idea—replacing sensitive data with realistic fictional data—best captures camouflage. This differs from encoding, which is about transforming data for safe display or transmission rather than substituting real values with substitutes. It also isn't about input validation, which focuses on checking data correctness, nor about hiding data inside random characters, which resembles steganography rather than creating plausible substitutes.

7. Which technology protects the integrity of data in transit?

A. Encrypting data with strong ciphers

B. Digitally signing the data

C. Reducing data size through compression

D. Hashing

Protecting integrity in transit means being able to detect if the data was altered while moving from sender to receiver. A cryptographic hash function creates a small, fixed-size digest from the data. If any part of the data changes, the hash changes drastically. The sender can share the data along with its hash, and the receiver recomputes the hash and compares it to the original. A mismatch signals tampering, so the data's integrity is verified. Encryption mainly shields confidentiality, not integrity on its own. Digital signatures do ensure integrity plus authenticity, but they require key management and introduce additional overhead. Compression affects size, not whether the content was tampered with. Hashing provides a straightforward, effective way to detect alterations during transit.

8. Which of the following is a packet sniffing tool?

A. Tcpdump

B. Fiddler

C. Nping

D. NetStumbler

Packet sniffing involves capturing and analyzing network traffic on an interface to inspect headers and payloads for troubleshooting or security work. Tcpdump is a command-line tool that embodies this capability, capturing traffic on a network interface via libpcap and printing packet headers and payloads for inspection. It also lets you filter traffic with BPF syntax to focus on particular protocols, ports, or addresses, and you can save captures for later analysis. That ability to observe actual packets at the data-link and network layers makes it the best fit. The other tools serve different purposes: Fiddler acts as a web debugging proxy, capturing HTTP(S) traffic between a browser and a server but not providing raw packet captures of all network traffic. Nping is used to generate and analyze network packets to test reachability and performance rather than capturing traffic. NetStumbler focuses on discovering wireless networks and their signal strengths, not on sniffing arbitrary packets on a general network.

SAMPLE

9. What is the default number of lines displayed by the head command?

A. Five lines

B. Ten lines

C. Fifteen lines

D. Twenty lines

Viewing the start of a file is what the head command does, and its default behavior is to show the first 10 lines. This gives a quick snapshot without overwhelming the screen. If you want a different amount, use the -n or --lines option. For example, head -n 5 filename displays the first five lines, head -n 15 filename shows the first fifteen, and head -n 20 filename shows the first twenty.

10. TCP port 21 is used by:

A. FTP - Control

B. SSH

C. DNS

D. SFTP

TCP port 21 is the standard control channel for FTP. This is where the FTP client connects to send commands (like login, list, retrieve, store) and receive responses from the server. The actual file transfers use a separate data channel, which can be port 20 in active FTP or a negotiated range in passive FTP, not port 21. The other options map to different services: SSH uses port 22, DNS uses port 53, and SFTP runs over SSH (also port 22).

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://ccstcybersec.examzify.com

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

SAMPLE