CCST Cybersecurity 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. **Standards provide mandatory requirements for how policies are carried out. Which option best describes this concept?**

   A. Optional tips

   B. Auditing schedules

   C. Hardware inventories

   D. Mandatory requirements

2. **Which category includes policies, procedures, standards, user education, incident response, disaster recovery, compliance and physical security?**

   A. Physical Controls

   B. Administrative Controls

   C. Technical Controls

   D. Operational Controls

3. **Which phase focuses on preparation and prevention to minimize security incidents?**

   A. Preparation and Prevention

   B. Monitoring and Investigation

   C. Response

   D. Recovery

4. **What are the two important components of a PKI used in network security?**

   A. Certificate Authority and Digital Certificates

   B. Certificate Authority

   C. Digital Certificates

   D. Private Keys

5. **A sandbox in cybersecurity is best described as...**

   A. An isolated environment used to run untrusted or potentially harmful code safely

   B. A central repository for user credentials

   C. A router feature

   D. A malware signature database

6. Which command is used to display the IP routing table on Windows hosts?

A. nslookup

B. route

C. nbstat

D. grep

7. What does an A record map?

A. A record

B. CNAME

C. TXT

D. MX

8. Which item is NOT a listed type of cyber threat?

A. Theft

B. Data Exfiltration

C. Software Attacks

D. Hardware Failures

9. What parameter identifies the application when a client requests a service from a remote server?

A. Destination port number

B. Source IP address

C. MAC address

D. Frame length

10. Which statement best describes the function of a protocol analyzer?

A. It blocks all traffic and prevents communications.

B. It captures packets on the network and analyzes their contents to detect network problems.

C. It encrypts data for secure transmission.

D. It inspects only the header fields without payload.

Answers

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

Explanations

1. Standards provide mandatory requirements for how policies are carried out. Which option best describes this concept?

A. Optional tips

B. Auditing schedules

C. Hardware inventories

D. Mandatory requirements

Standards specify mandatory requirements for how to implement policies. They turn the policy's intent into concrete, enforceable rules that must be followed, ensuring consistent and auditable compliance across systems and teams. This is what makes compliance measurable: you can verify that the required criteria are met, not just follow optional advice. Think of the contrast with other ideas: optional tips are recommendations, not enforceable rules; auditing schedules concern when you check for compliance rather than what must be done; hardware inventories are lists of assets, not guidelines for carrying out policies. Standards provide the exact criteria you must meet—encryption requirements, access controls, configuration baselines—so everyone implements policies in the same way.

2. Which category includes policies, procedures, standards, user education, incident response, disaster recovery, compliance and physical security?

A. Physical Controls

B. Administrative Controls

C. Technical Controls

D. Operational Controls

Administrative controls focus on governance, policy, and planning that shape how security is implemented. This category covers the rules, procedures, and programs that guide behavior and establish how security is managed across the organization. Policies, procedures, and standards are the documents that define what must be done and the rules to follow. User education changes how people behave, reducing human-caused risk. Incident response and disaster recovery are prewritten plans for how to detect, respond to, and recover from incidents. Compliance ensures the organization follows laws, regulations, and internal policies. Even physical security fits here when it's managed through governance and programmatic oversight rather than through hardware alone. Altogether, these elements are about management, oversight, and the overall approach to security. Technical controls, by contrast, are the actual technologies that enforce security (like encryption, access control mechanisms, and firewalls). Operational controls cover the day-to-day execution and maintenance of security tasks (such as routine monitoring and change management). The items in this set are focused on policy, planning, and governance, which is why they belong to administrative controls.

3. Which phase focuses on preparation and prevention to minimize security incidents?

A. Preparation and Prevention

B. Monitoring and Investigation

C. Response

D. Recovery

Preparing and preventing focuses on getting ready before any incident occurs—putting in place policies, training, preventive controls, and plans that reduce the chance of an incident and lessen its impact if one happens. This phase builds the foundation: incident response plans, security awareness, tabletop drills, patch management, access controls, and robust backups all aim to prevent incidents or minimize damage when events arise. The other phases are more reactive or restorative. Monitoring and Investigation deals with spotting potential issues and analyzing alerts to determine if an incident is happening and what it entails. Response is about taking immediate actions to contain and mitigate the threat while it's active. Recovery centers on restoring services and learning from the event after containment. Since the question highlights preparation and prevention, this phase best fits that focus.

4. What are the two important components of a PKI used in network security?

A. Certificate Authority and Digital Certificates

B. Certificate Authority

C. Digital Certificates

D. Private Keys

Two essential components in a PKI are the Certificate Authority and Digital Certificates. The Certificate Authority acts as a trusted issuer that signs and manages certificates, vouching that a given public key belongs to the stated entity. Digital certificates are the data that bind that public key to an identity, containing the key, the identity information, the issuer, and validity details. Together, they enable systems to verify that a public key actually belongs to the person or service it claims to represent, which is what makes secure communications possible, such as TLS handshakes. Relying on the certificate authority alone wouldn't connect a specific key to an identity without a certificate to bind them. Relying on digital certificates alone wouldn't provide the trusted mechanism to confirm authenticity unless there's an issuer whose signature can be verified. Private keys are essential cryptographic secrets, but they are not the trust framework themselves; the PKI's trust comes from the relationship between the certificate authority and the certificates it signs.

5. A sandbox in cybersecurity is best described as...

A. An isolated environment used to run untrusted or potentially harmful code safely

B. A central repository for user credentials

C. A router feature

D. A malware signature database

In cybersecurity, a sandbox is an isolated environment used to run untrusted or potentially harmful code safely. The key idea is containment: the code executes in a contained space where its actions can be observed without risking the rest of the system or network. This setup often includes restricted permissions, controlled network access, and thorough logging so analysts can study behavior, file changes, and network activity without letting anything escape or damage real systems. Sandboxes are especially useful for malware analysis, testing risky software, and safely deterring harmful behavior before it reaches production environments. The other options describe different concepts: a central repository for user credentials is a credential store or password manager, not a sandbox; a router feature relates to network routing capabilities; and a malware signature database is used for detection, not execution or safe analysis in isolation.

6. Which command is used to display the IP routing table on Windows hosts?

A. nslookup

B. route

C. nbstat

D. grep

Displaying the IP routing table on Windows is done with the route command. Use route print to view the current IPv4 and IPv6 routes, including destination networks, subnet masks, gateways, the interface used, and the metric that influences route selection. The other options serve different purposes: nslookup queries DNS, nbstat shows NetBIOS over TCP/IP status, and grep is a text-search tool from Unix-like systems, not a Windows routing viewer. You can also modify routes with route add or route delete, but for simply viewing the routing information, route print is the correct approach.

7. What does an A record map?

A. A record

B. CNAME

C. TXT

D. MX

This tests how DNS translates a domain name into a network address. An A record maps a domain name to an IPv4 address, so when you look up that name, your system learns the specific IPv4 address to connect to. If a domain has multiple servers, there can be several A records for the same name, providing options for load distribution. Other DNS types serve different purposes: a CNAME creates an alias to another domain name (not an IP address), a TXT record stores text data (often for validation or policy), and an MX record designates the mail server for the domain and its priority. For IPv6 addresses, you'd use an AAAA record instead.

8. Which item is NOT a listed type of cyber threat?

A. Theft

B. Data Exfiltration

C. Software Attacks

D. Hardware Failures

Understanding how cyber threats are categorized helps here. A threat type is a broad category of danger that can affect systems, such as someone stealing data or an attacker exploiting software. Data exfiltration, though crucial in many breaches, is the act of moving data out of a network. It's typically described as a technique or outcome within an attack rather than a standalone threat category. Because of that, it isn't usually listed as its own distinct cyber threat type in many risk taxonomies, making it the item that doesn't fit the common list. The other options align with widely recognized threat categories: theft covers unauthorized taking of data or assets, and software attacks describe exploits targeting software. Hardware failures, while not a cyber threat, are physical/operational issues—distractors that rely on a different domain.

9. What parameter identifies the application when a client requests a service from a remote server?

A. Destination port number

B. Source IP address

C. MAC address

D. Frame length

The ability to pick which service or application handles incoming data on the destination host comes from the destination port in the transport layer header (TCP or UDP). Each service listens on a specific port, so when a client sends a request, the destination port tells the receiving system which process to deliver the data to—examples are port 80 for HTTP and port 443 for HTTPS. The source IP address identifies who sent the request, the MAC address is used for local network addressing, and the frame length is just the size of the data frame, not the service being requested.

10. Which statement best describes the function of a protocol analyzer?

A. It blocks all traffic and prevents communications.

B. It captures packets on the network and analyzes their contents to detect network problems.

C. It encrypts data for secure transmission.

D. It inspects only the header fields without payload.

A protocol analyzer, often called a packet sniffer, is used to gain visibility into network traffic by capturing the packets that traverse the network and decoding their contents. This lets you see headers and payloads, the sequence and timing of packets, and how different protocols behave, so you can diagnose issues such as misconfigurations, latency, dropped packets, and unusual traffic patterns. Because it's meant to observe, it typically operates passively and doesn't block or disrupt communications. The other statements don't fit because blocking all traffic is the job of firewalls or intrusion prevention systems, not a protocol analyzer. Encrypting data is the role of cryptographic techniques and devices, not packet capture and analysis. And while some tools can show headers, many protocol analyzers also examine payloads to provide the full context needed to diagnose problems, so limiting inspection to headers would miss important details.

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!