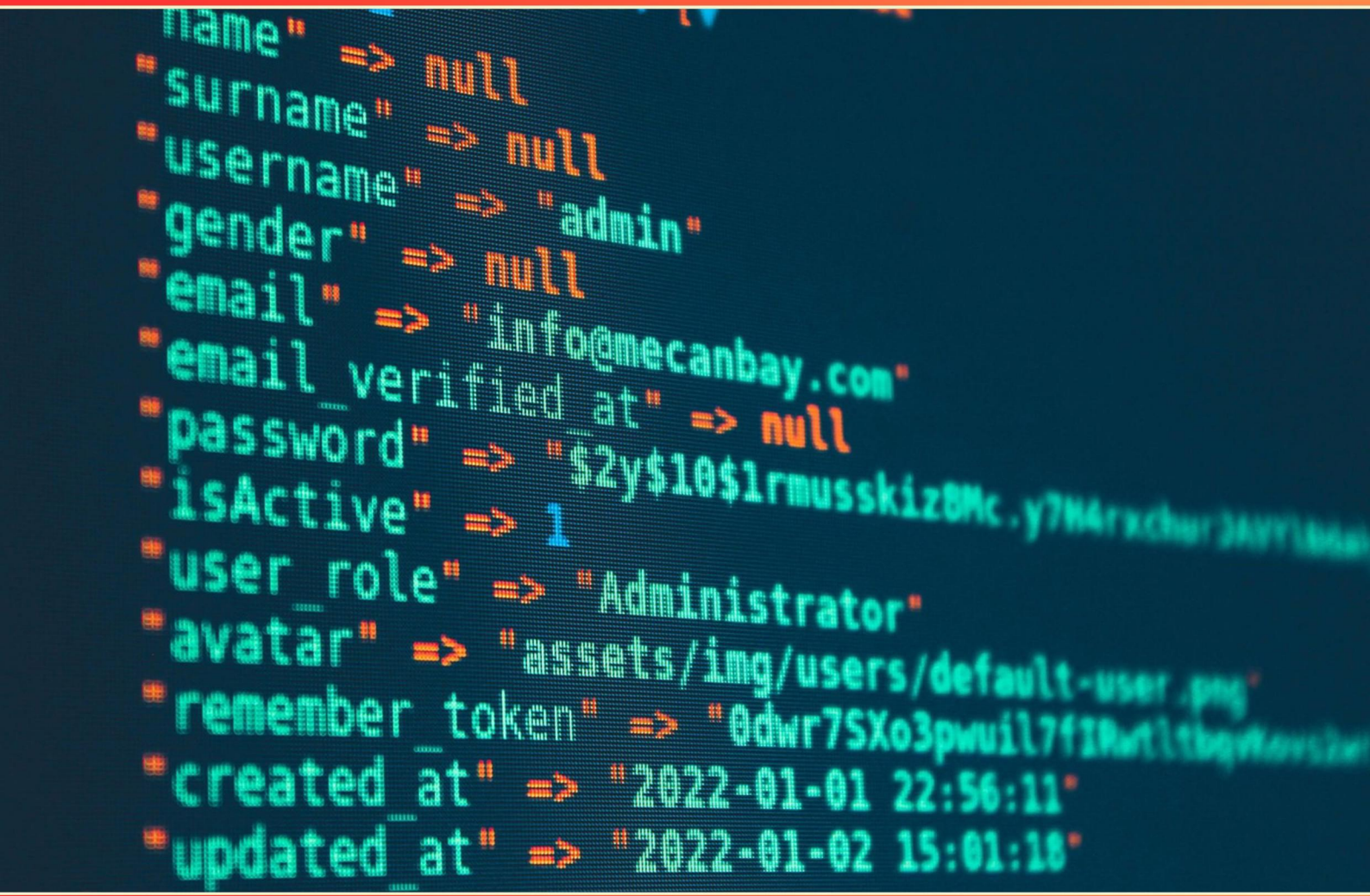
CCST CYBERSECURITY PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://ccstcybersec.examzify.com

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 tool is a packet sniffer?**

   A. Wireshark

   B. Nmap

   C. Hping

   D. Scapy

2. **Which term describes a more complex decoy system used mainly by research, military, and government organizations?**

   A. Canary Trap

   B. Honeypot

   C. DNS Record

   D. Firewall

3. **Which protocol is used by the Cisco Cyber Threat Defense Solution to collect information about the traffic that traverses the network?**

   A. IPFIX

   B. NetFlow

   C. SNMP

   D. sFlow

4. **Which command is commonly used to troubleshoot domain name servers and retrieve DNS resource records?**

   A. Nslookup

   B. Netstat

   C. Grep

   D. Route

5. **FTK Imager is a forensic tool that can**

   A. FTK Imager is a forensic tool that can perform a forensically sound acquisition, verify it with an MD5 hash, and preview files in read-only mode

   B. monitor live network traffic for anomalies

   C. recover deleted files from a logical partition without consent

   D. patch operating system vulnerabilities automatically

6. DNS uses which port and transport protocols?

A. DNS uses TCP port 53 and UDP port 53

B. DNS uses only UDP port 53

C. DNS uses TCP port 53 only

D. DNS uses port 67 for servers

7. Which DNS record would an email server query to locate the destination mail server for a domain?

A. A record

B. MX record

C. NS record

D. TXT record

8. Which remote access method is considered secure according to policy?

A. Telnet

B. FTP

C. HTTP

D. SSH or VPN

9. Which Exploitability criterion expresses the presence or absence of a user interaction requirement?

A. Attack complexity.

B. Privileges required.

C. Scope.

D. User interaction.

10. Which protocol runs over port 22 as a subsystem?

A. SSH

B. FTP

C. SFTP

D. Telnet

Answers

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

Explanations

1. Which tool is a packet sniffer?

A. Wireshark

B. Nmap

C. Hping

D. Scapy

Packet sniffing involves capturing live network traffic and inspecting the contents of packets. Wireshark is designed exactly for that: it captures packets from the network, decodes many protocols, and presents them in a searchable, filterable interface for analysis. This makes it the primary tool for sniffing and traffic analysis. The other tools serve different purposes. Nmap focuses on discovering hosts and services on a network. Hping is used to craft and send custom packets to test defenses or measure network responses. Scapy is a flexible packet manipulation toolkit that can sniff as part of its capabilities but is primarily aimed at building and sending packets in Python.

2. Which term describes a more complex decoy system used mainly by research, military, and government organizations?

A. Canary Trap

B. Honeypot

C. DNS Record

D. Firewall

A honeypot is a deliberately vulnerable resource placed inside a network to attract attackers, with the purpose of observing their methods, tools, and behavior. This makes it a more complex decoy system, especially when scaled into a honeynet—multiple interlinked decoys that mimic real systems. Researchers, military, and government organizations use this approach to study threats, gather intelligence on attack techniques, and improve defenses. In contrast, a DNS record is just data within the Domain Name System, a firewall is a protective device that blocks or filters traffic, and a canary trap is a leakage-detection deception tactic aimed at identifying insiders rather than providing a monitored decoy environment for threat actors.

3. Which protocol is used by the Cisco Cyber Threat Defense Solution to collect information about the traffic that traverses the network?

A. IPFIX

B. NetFlow

C. SNMP

D. sFlow

NetFlow is the protocol used to export flow-based visibility into traffic traversing the network. A flow is defined by identifiers like source and destination IP addresses and ports, the transport protocol, and other fields; NetFlow records also include statistics such as bytes, packets, and duration. This flow-level data lets Cisco CTD see who is talking to whom, when, and how much, enabling effective threat detection and traffic analysis without capturing full packet contents. SNMP is for device management, not traffic flows; sFlow provides sampled data which can miss many flows; IPFIX is the standard version of flow data, but NetFlow is the protocol most closely associated with Cisco CTD in this context.

4. Which command is commonly used to troubleshoot domain name servers and retrieve DNS resource records?

A. Nslookup

B. Netstat

C. Grep

D. Route

When diagnosing name resolution problems, you want a tool that talks directly to DNS servers to ask for specific records. That's what nslookup does. It's a command-line utility built to query DNS servers and retrieve resource records, such as A records (mapping a domain to an IP), MX records (mail servers), NS records (name servers), CNAMEs, and more. You can run it simply to see what IP address a domain resolves to, or specify the record type to verify particular DNS data, for example asking for MX records for a domain or pointing nslookup at a specific DNS server to compare results. This targeted capability makes it the go-to tool for DNS troubleshooting and validation. Tools like netstat focus on current network connections, not DNS data; grep is a text-search utility; and route deals with routing tables. None of those directly retrieve DNS resource records to diagnose name resolution.

5. FTK Imager is a forensic tool that can

A. FTK Imager is a forensic tool that can perform a forensically sound acquisition, verify it with an MD5 hash, and preview files in read-only mode

B. monitor live network traffic for anomalies

C. recover deleted files from a logical partition without consent

D. patch operating system vulnerabilities automatically

Preserving evidence integrity during acquisition is essential in digital forensics. FTK Imager is a forensic tool that can create a forensically sound image of storage media, verify the copy using an MD5 hash, and allow you to preview files in read-only mode. This combination ensures the collected data is an exact, unaltered replica and lets investigators inspect contents without risking modification to the source. It does not monitor live network traffic, it does not recover deleted files without proper authorization, and it does not automatically patch operating system vulnerabilities.

6. DNS uses which port and transport protocols?

A. DNS uses TCP port 53 and UDP port 53

B. DNS uses only UDP port 53

C. DNS uses TCP port 53 only

D. DNS uses port 67 for servers

DNS relies on port 53 and uses both UDP and TCP as transport protocols. For typical queries, UDP to port 53 is used because it's fast and lightweight. If a response is too large to fit in a UDP packet or a zone transfer between DNS servers is required, DNS switches to a TCP connection on port 53 to ensure reliable delivery. That combination—port 53 with both UDP and TCP—best reflects how DNS operates. The notion of using only UDP or only TCP misses important cases (UDP for standard queries, TCP for large responses and zone transfers). Port 67 belongs to DHCP servers, not DNS.

7. Which DNS record would an email server query to locate the destination mail server for a domain?

A. A record

B. MX record

C. NS record

D. TXT record

Email delivery relies on DNS MX records to locate the destination mail server for a domain. An MX record specifies which host is responsible for receiving mail for that domain and includes a priority so mail can be routed to the preferred server first. When a message is sent, the sender's mail server queries DNS for the recipient domain's MX records, then connects to the host named in the MX entry, using A or AAAA records to resolve that host to an IP address as needed. If a domain has no MX record, some systems will fall back to using the domain's A record for delivery. Other DNS records have different roles: A records map a domain to an IP address, NS records identify the authoritative DNS servers for a zone, and TXT records hold text data (often used for SPF/DKIM), not for directing mail delivery.

8. Which remote access method is considered secure according to policy?

A. Telnet

B. FTP

C. HTTP

D. SSH or VPN

Remote access should be conducted over encrypted, authenticated channels to protect credentials and data. The insecure options transmit data in plaintext, making interception easy. Telnet sends commands and usernames in clear text; FTP does not encrypt file transfers or authentication by default; HTTP is not encrypted and not appropriate for remote administration. SSH encrypts the session and authenticates both ends for secure command-line access, and a VPN creates an encrypted tunnel that secures all traffic between the remote user and the internal network. Because of these protections, using SSH or a VPN is considered secure for remote access according to policy.

9. Which Exploitability criterion expresses the presence or absence of a user interaction requirement?

A. Attack complexity.

B. Privileges required.

C. Scope.

D. User interaction.

The idea being tested is whether exploiting a vulnerability requires a user to take action. In CVSS and similar models, the User Interaction metric answers exactly that: does exploitation depend on a user performing some action (like opening a file or clicking a link) or can it occur without any user involvement? If user interaction is required, that is noted by this criterion and influences the overall exploitability score. The other criteria describe different aspects—Attack Complexity looks at how hard it is to exploit, Privileges Required indicates the level of access needed before exploitation, and Scope determines whether the exploit can affect resources beyond the original scope. So the criterion that expresses the presence or absence of a user interaction requirement is the User Interaction metric.

10. Which protocol runs over port 22 as a subsystem?

A. SSH

B. FTP

C. SFTP

D. Telnet

SFTP is the file transfer protocol that is implemented as a subsystem of SSH. SSH creates an encrypted channel over port 22, and SFTP operates inside that same SSH connection to transfer files securely without needing a separate port. This relationship—SFTP riding on the SSH transport—is why it uses port 22. In contrast, FTP uses port 21 with separate control and data connections, and Telnet uses port 23 and is not secure. SSH handles remote command execution, but SFTP is the dedicated file transfer mechanism within SSH, hence it runs over port 22 as a subsystem.

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!