EC-COUNCIL CERTIFIED ETHICAL HACKER (CEH) V13 (312-50V13) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://eccouncil31250v13.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. What is the primary communication method for NTP?

A. Transmission Control Protocol (TCP) on port 80.

B. User Datagram Protocol (UDP) on port 123.

C. Stream Control Transmission Protocol (SCTP) on port 123.

D. ICMP Echo on port 0.

2. In a network security context, what should be regularly monitored and tested?

A. Networks and security systems

B. Web content

C. End-user devices only

D. Only firewall rules

3. What is the main purpose of a vulnerability scanner?

A. To maintain hardware inventory

B. To identify security weaknesses in a system or network

C. To monitor user activity

D. To log network traffic

4. During a vulnerability scan, which activity is typically not performed?

A. Automated vulnerability checks

B. Active exploitation of vulnerabilities

C. Credentialed checks

D. Reporting discovered weaknesses

5. Which UDP port is used by the Network Time Protocol (NTP) for communication?

A. Port 53

B. Port 123

C. Port 161

D. Port 67

SAMPLE

6. How does Tcpdump function?

A. It prevents traffic

B. It blocks packets

C. It displays TCP/IP and other packets transmitted or received over a network.

D. It encrypts traffic

7. What is the main purpose of enabling auditing on a system that processes sensitive information?

A. To track and monitor access and changes to sensitive data.

B. To speed up data processing.

C. To simplify user provisioning.

D. To improve encryption algorithms.

8. What risk is associated with misconfiguring DNS zone transfers?

A. All DNS records are hidden.

B. Exposes all DNS zone data for the domain.

C. Query performance increases.

D. It causes DNS to stop resolving.

9. What is the role of a Proxy server in a network?

A. To act as an intermediary for requests from clients seeking resources from other servers.

B. To assign IP addresses to devices on the LAN automatically.

C. To monitor and log user activity for policy enforcement.

D. To decrypt encrypted traffic for the network administrator.

10. What are the initial two commands an IRC client sends to join an IRC network?

A. NICK, USER

B. JOIN, NICK

C. PASS, NICK

D. USER, NICK.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the primary communication method for NTP?

A. Transmission Control Protocol (TCP) on port 80.

B. User Datagram Protocol (UDP) on port 123.

C. Stream Control Transmission Protocol (SCTP) on port 123.

D. ICMP Echo on port 0.

Time synchronization thrives on fast, small exchanges rather than establishing a full connection. NTP uses UDP on port 123 because UDP provides a lightweight, connectionless datagram service ideal for sending time-stamped messages quickly. This low overhead keeps latency low, and NTP's own algorithms handle clock offset and delay even when some packets are lost, so guaranteed delivery isn't required. The other options point to protocols or ports not used for NTP (TCP on port 80, SCTP on 123, or ICMP Echo), so UDP on port 123 is the correct primary communication method.

2. In a network security context, what should be regularly monitored and tested?

A. Networks and security systems

B. Web content

C. End-user devices only

D. Only firewall rules

Regularly monitoring and testing must cover the entire network and its security systems. The idea is to maintain visibility across all parts of the infrastructure and the defenses that protect it, not just a single component. Continuous monitoring involves collecting and analyzing logs, traffic patterns, alerts, device health, and configuration compliance across routers, switches, servers, endpoints, and security controls like IDS/IPS, firewalls, and access controls. Regular testing includes activities such as vulnerability assessments, penetration testing, configuration reviews, patch management validation, and incident response drills to verify that controls function as intended and gaps are identified and addressed. Why this is the best fit: focusing only on web content misses the backbone of the network and the security controls that protect it. End-user devices matter, but isolating monitoring to them ignores network infrastructure, servers, and centralized defenses. Limiting testing to firewall rules overlooks misconfigurations, software vulnerabilities, patch levels, and detection capabilities elsewhere in the environment. A holistic approach ensures you detect changes, new threats, and misconfigurations across the whole security posture.

3. What is the main purpose of a vulnerability scanner?

A. To maintain hardware inventory

B. To identify security weaknesses in a system or network

C. To monitor user activity

D. To log network traffic

A vulnerability scanner's main purpose is to automatically identify security weaknesses in a system or network by scanning hosts, services, and applications against databases of known vulnerabilities, misconfigurations, and missing patches. This produces a report that helps prioritize remediation based on severity, so you can reduce risk before attackers exploit flaws. It isn't about maintaining hardware inventory (asset management), monitoring user activity (user behavior auditing), or logging network traffic (traffic capture or IDS/IPS functions).

SAMPLE

4. During a vulnerability scan, which activity is typically not performed?

A. Automated vulnerability checks

B. Active exploitation of vulnerabilities

C. Credentialed checks

D. Reporting discovered weaknesses

Vulnerability scanning is all about discovering weaknesses without taking control of systems. The goal is to identify what needs remediation, not to prove what an attacker could break into. That makes the step of actively exploiting vulnerabilities outside the typical scan process. Scanners perform automated vulnerability checks against known issues and, if allowed, credentialed checks using valid access to see deeper configuration problems. After scanning, a report is generated to guide remediation efforts. Exploitation, on the other hand, is a later phase associated with penetration testing or controlled attack simulations. It involves attempting to exploit found weaknesses to verify impact, which carries higher risk and requires explicit authorization and safeguards. So, actively exploiting vulnerabilities is not part of a standard vulnerability scan; it belongs to a broader testing activity conducted separately.

5. Which UDP port is used by the Network Time Protocol (NTP) for communication?

A. Port 53

B. Port 123

C. Port 161

D. Port 67

NTP uses UDP for lightweight, time-critical communication and standardizes on port 123 for all its traffic. This means clients send their time requests to a server listening on UDP port 123, and the server responds from its own UDP port 123 back to the client's ephemeral port. Defining a single, well-known port makes handshakes and time exchange predictable across devices and networks, which is essential for accurate clock synchronization. RFC 5905 documents this usage, so you'll frequently see NTP traffic on UDP 123 in real networks. By contrast, the other ports are tied to different protocols—port 53 is DNS, port 161 is SNMP, and port 67 is DHCP server—so they don't apply to NTP.

6. How does Tcpdump function?

A. It prevents traffic

B. It blocks packets

C. It displays TCP/IP and other packets transmitted or received over a network.

D. It encrypts traffic

Tcpdump is a network packet analyzer that captures and displays the packets traveling on a network interface. It uses a capture library (libpcap) to sniff traffic, often in promiscuous mode, and prints a readable summary of each packet's headers—covering protocols like IP, TCP, UDP, ICMP, and more. You can apply filters so you only see specific traffic, which makes it a powerful tool for diagnosing issues, verifying protocol behavior, or understanding network flows. This is why the correct choice fits best: it describes the tool as something that shows the actual packets being transmitted or received, not something that stops, alters, or encrypts the traffic.

SAMPLE

7. What is the main purpose of enabling auditing on a system that processes sensitive information?

A. To track and monitor access and changes to sensitive data.

B. To speed up data processing.

C. To simplify user provisioning.

D. To improve encryption algorithms.

Auditing a system that processes sensitive information is about maintaining an evidentiary trail of who accessed data, what actions they took, and when those actions occurred. This makes accountability possible, enables early detection of unusual or unauthorized activity, and provides logs for investigations, incident response, and regulatory compliance. For example, audit records show user IDs, timestamps, resources accessed, and the outcomes of operations, helping verify policy adherence and support forensic analysis. The other options don't fit the purpose: auditing isn't meant to speed up data processing, streamline user provisioning, or directly improve encryption algorithms.

8. What risk is associated with misconfiguring DNS zone transfers?

A. All DNS records are hidden.

B. Exposes all DNS zone data for the domain.

C. Query performance increases.

D. It causes DNS to stop resolving.

DNS zone transfers are meant to copy the DNS zone data to trusted secondary servers. When this capability is misconfigured to permit transfers to any host, an attacker can perform a zone transfer and retrieve the entire zone data. That means every record in the domain—hostnames, IP mappings, subdomains, mail servers, and other records—becomes exposed, giving a complete map of the domain's infrastructure for reconnaissance or exploitation. The risk isn't that records are hidden or that performance improves; it's that the entire DNS zone data is exposed to anyone who requests it, which is why this misconfiguration is a serious security flaw.

9. What is the role of a Proxy server in a network?

A. To act as an intermediary for requests from clients seeking resources from other servers.

B. To assign IP addresses to devices on the LAN automatically.

C. To monitor and log user activity for policy enforcement.

D. To decrypt encrypted traffic for the network administrator.

A proxy server sits between clients and the resources they request, acting as an intermediary that forwards client requests to the target server and then returns the responses back to the client. This mediation is the defining function of a proxy and enables features like content caching to speed up repeated requests, as well as applying access policies and filtering. Assigning IP addresses automatically is the job of a DHCP server, not a proxy. Monitoring and logging can be a capability of a proxy, but it's an auxiliary function rather than the core role. Decrypting encrypted traffic is not a standard, everyday role of a proxy and is only done in specialized setups (TLS interception), which goes beyond the typical proxy function.

SAMPLE

10. What are the initial two commands an IRC client sends to join an IRC network?

A. NICK, USER

B. JOIN, NICK

C. PASS, NICK

D. USER, NICK.

When an IRC client connects, it first registers with the server by exchanging the basic identification commands. The USER command supplies the user's identity (username, host, server, and real name), and the NICK command then assigns the nickname that will be used in chats. This pair establishes who you are on the network and is required before you can do anything else. The PASS command would only come into play if the server requires a password for registration, in which case it would be sent before USER. The JOIN command comes later—after registration—to enter channels. So the initial two commands are USER followed by NICK.

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://eccouncil31250v13.examzify.com

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

SAMPLE