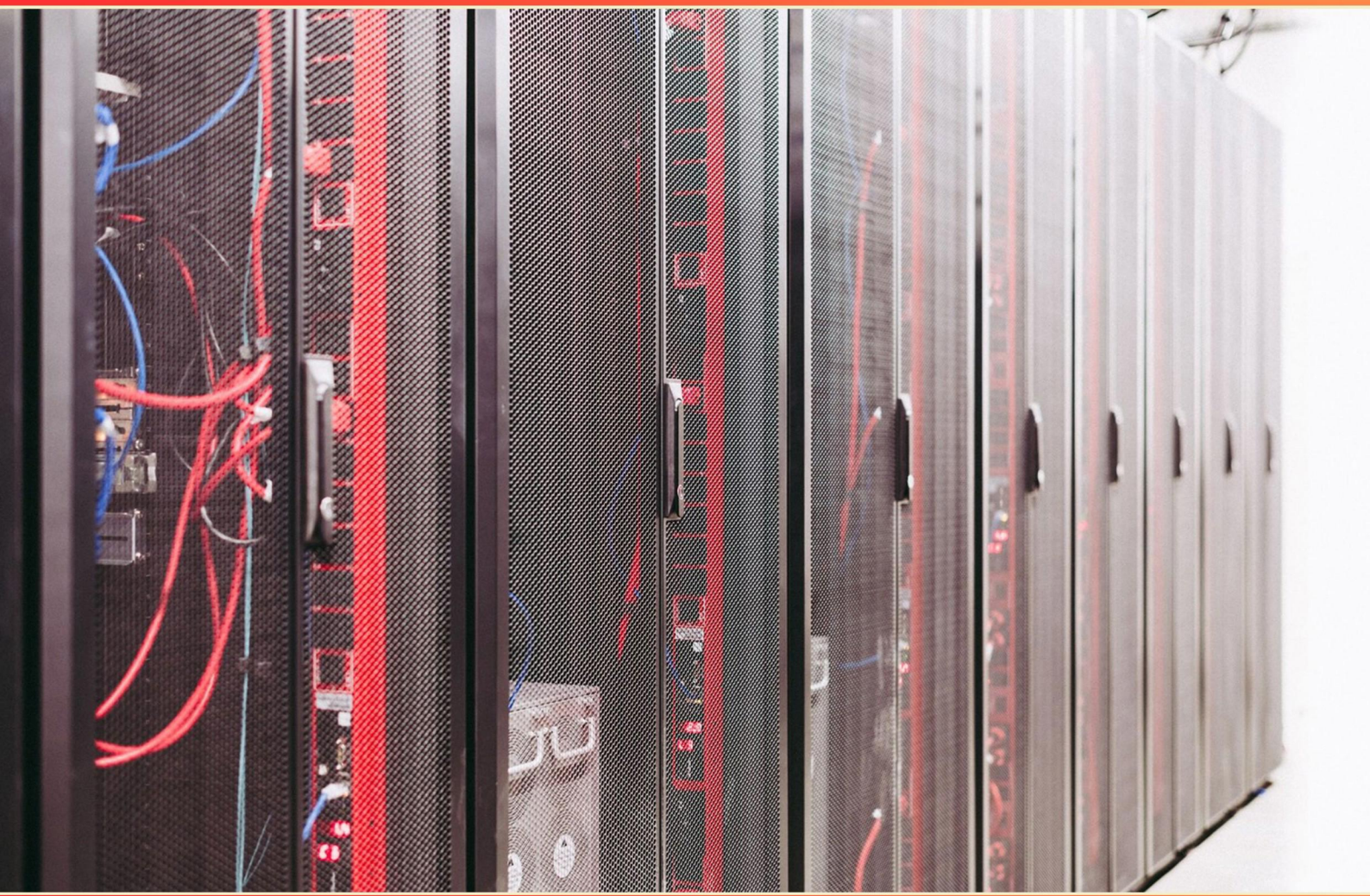
CYBER FUNDAMENTALS BLOCK 5 PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cyberfundamentalsblock5.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. It's necessary to maintain a/an _____ to revert the system after changes if needed.

A. Baseline

B. Restore Point

C. Snapshot

D. Checkpoint

2. Proxy servers are typically associated with controlling which type of communication by limiting which websites an employee can visit?

A. Outbound

B. Inbound

C. Internal

D. Peer-to-peer

3. What's the first incident response phase where the AF detects activity with a variety of means and capabilities?

A. Preparation

B. Containment

C. Detection and Reporting Events

D. Analysis

4. File permissions do not protect the file contents from being read while the files are _____.

A. At rest

B. Transit

C. In memory

D. On disk

5. Which term best describes software designed to disrupt, damage, or gain unauthorized access to computer systems?

A. Virus

B. Worm

C. Malware

D. Trojan

SAMPLE

6. Which of the following best describes the capabilities typically provided by a proxy server?

A. Security, privacy and web filtering

B. Caching, load balancing, and uptime

C. Data encryption, integrity, and non-repudiation

D. User authentication, auditing, and policy enforcement

7. Which description best defines a Distributed Denial of Service (DDoS) attack?

A. An attack where multiple systems overwhelm a target with traffic

B. An attack that steals credentials

C. An attack that hijacks sessions

D. An attack that injects malware into software

8. Which measures can determine whether someone attempted to break into a system and what they may have done?

A. Audit Logs

B. Detection Measures

C. Intrusion Alarms

D. Security Audits

9. During Agile, when is it permissible to revisit or repeat steps?

A. Only during planning

B. Never

C. At any time

D. At the end of each sprint

10. Which protocol is commonly used to enforce that anyone who connects supplies valid credentials before access is allowed?

A. SSH

B. IEEE 802.1X

C. FTP

D. TLS

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. It's necessary to maintain a/an _____ to revert the system after changes if needed.

A. Baseline

B. Restore Point

C. Snapshot

D. Checkpoint

Maintaining a baseline means keeping a known good, approved state of the system that you can revert to after changes. This baseline serves as a reference point for what the system should look like in terms of configuration, patches, and settings. When issues arise from updates or edits, you can restore or reapply that baseline to bring the system back to a trusted, functioning state. Why this is the best fit: the baseline embodies the standard configuration that has been tested and authorized. It supports consistency across environments and provides a clear target for restoration or reconfiguration. While other options like restore points, snapshots, or checkpoints can revert to a previous moment, they're often tied to specific platforms or virtualization contexts. A baseline, by contrast, represents the intended, constant reference state you can aim to return to after any change.

2. Proxy servers are typically associated with controlling which type of communication by limiting which websites an employee can visit?

A. Outbound

B. Inbound

C. Internal

D. Peer-to-peer

Proxy servers act as an intermediary for outbound requests from inside the network to the internet. Because employee requests to access external websites pass through the proxy, it can inspect the destination, enforce access rules, block or permit sites, and log activity. This setup is what makes proxies effective at limiting where employees can go on the web. Inbound traffic, by contrast, is external systems connecting to internal resources and is generally handled by firewalls or reverse proxies. Internal communication stays within the organization, and while some traffic types like peer-to-peer can be restricted, the primary association of proxies in this context is with outbound web access control.

3. What's the first incident response phase where the AF detects activity with a variety of means and capabilities?

A. Preparation

B. Containment

C. Detection and Reporting Events

D. Analysis

Detecting activity from a mix of tools and data sources is the focus of the Detection and Reporting Events phase. After preparation sets up the monitoring landscape, this phase is when signals from multiple means—network sensors, host-based analytics, SIEM correlations, logs, and user reports—converge to indicate something is happening. It's the point at which incidents become observable and are reported to the incident response team so a response can begin. Containment and analysis come afterward to limit impact and determine root cause, but the first moment you actually see and report an incident using diverse detection capabilities is this phase.

SAMPLE

4. File permissions do not protect the file contents from being read while the files are _____.

A. At rest

B. Transit

C. In memory

D. On disk

File permissions control who can access a file when it is stored on disk and being accessed locally. They provide protection for data at rest and during normal file access on the system. But when a file is moving over a network—data in transit—there's no file on a local filesystem for those permissions to govern. The contents must be protected by encryption and secure transfer protocols rather than by filesystem permissions. Data in memory is governed by memory isolation and process protections, not by file permissions, since the file has already been loaded into RAM. So data in transit is the state where file permissions don't protect the contents.

5. Which term best describes software designed to disrupt, damage, or gain unauthorized access to computer systems?

A. Virus

B. Worm

C. Malware

D. Trojan

This question tests recognizing the broad term for software designed to disrupt, damage, or gain unauthorized access to computer systems. That broad term is malware, which covers any software created to harm or exploit devices, including actions like replication, evasion of defenses, or opening backdoors for attackers. Malware is the umbrella category for all such malicious software. Within it are specific types like viruses, which attach to legitimate files and spread when those files are executed; worms, which self-propagate across networks without user action; and Trojans, which disguise themselves as harmless or useful programs to trick users into running them. Each of these is a form of malware, but the description in the question points to malware as the overall class—the best fit for software designed to disrupt, damage, or gain unauthorized access.

6. Which of the following best describes the capabilities typically provided by a proxy server?

A. Security, privacy and web filtering

B. Caching, load balancing, and uptime

C. Data encryption, integrity, and non-repudiation

D. User authentication, auditing, and policy enforcement

Proxies act as gatekeepers between users and resources, so the most characteristic capabilities are authenticating users, auditing their activity, and enforcing access policies. Verifying who can access the network ensures only authorized individuals pass through. Auditing creates logs of who did what and when, which supports security reviews and compliance. Policy enforcement applies rules about what is allowed or blocked, such as restricting sites or limiting certain actions. While proxies can also cache content and filter some traffic, these features are supplementary. Encryption, integrity, and non-repudiation are cryptographic concepts not inherent to a proxy's core function.

SAMPLE

7. Which description best defines a Distributed Denial of Service (DDoS) attack?

A. An attack where multiple systems overwhelm a target with traffic

B. An attack that steals credentials

C. An attack that hijacks sessions

D. An attack that injects malware into software

A DDoS attack centers on using many devices to flood a target with traffic, overwhelming its bandwidth and resources so legitimate users can't access the service. The distributed nature means the sources come from numerous compromised machines, making it harder to block and mitigate than a single-source attack. The other descriptions describe different goals—stealing credentials, hijacking an active session, or injecting malware into software—rather than exhausting a service's availability. That combination of widespread traffic and resource exhaustion is what defines a Distributed Denial of Service attack.

8. Which measures can determine whether someone attempted to break into a system and what they may have done?

A. Audit Logs

B. Detection Measures

C. Intrusion Alarms

D. Security Audits

Detecting and understanding attempted intrusions relies on detection measures that continuously monitor systems, correlate events, and raise alerts when something unusual happens. These measures don't just record what occurred; they synthesize data from multiple sources to indicate an attempt and to map out the attacker's activities. Think of tools like centralized log analysis, intrusion detection systems, and security information and event management as the components that gather audit logs, monitor network traffic, and watch system telemetry, then apply rules to flag potential breaches and build a timeline of actions. This combination makes it possible to determine that someone tried to break in and to infer what they did, such as probing credentials, escalating privileges, or exfiltrating data. Audit logs by themselves are essential evidence, but they need detection measures to interpret them and connect disparate events. Intrusion alarms can signal a possible event but often don't provide the full, reconstructed picture. Security audits assess controls and compliance at a point in time, not the ongoing detection and forensic recovery of an incident.

9. During Agile, when is it permissible to revisit or repeat steps?

A. Only during planning

B. Never

C. At any time

D. At the end of each sprint

In Agile, work is iterative and adaptive, and teams continuously learn and adjust as new information comes in. Because requirements, insights, and technology can change during a project, you can and should revisit or repeat steps whenever it's needed to incorporate what you've learned. This is why the idea of doing revisits "at any time" best captures how Agile teams operate: planning, design, and even scope can be revisited during the course of the project, not just at fixed points. In practice, you'll see this happen through ongoing backlog refinement, sprint reviews, and retrospectives, as well as any mid-sprint adjustments if new information warrants it. The other options imply rigid timing—only at planning, never, or only at the end of a sprint—which runs counter to Agile's emphasis on continuous feedback and adaptation.

SAMPLE

10. Which protocol is commonly used to enforce that anyone who connects supplies valid credentials before access is allowed?

A. SSH

B. IEEE 802.1X

C. FTP

D. TLS

Port-based network access control is the concept at work here. IEEE 802.1X is the protocol used to enforce that any device trying to connect must first present valid credentials. In this setup, the switch or wireless access point acts as the authenticator and blocks traffic on the port until authentication succeeds. The client (supplicant) sends credentials, carried using EAP over LAN, to the authenticator, which forwards them to an authentication server (commonly a RADIUS server) for verification. Only after a successful check is the port opened, allowing access to the network. Other protocols like SSH, FTP, and TLS are used to secure sessions after a connection is established; they do not enforce credentials before access to the network itself is granted.

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://cyberfundamentalsblock5.examzify.com

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

SAMPLE