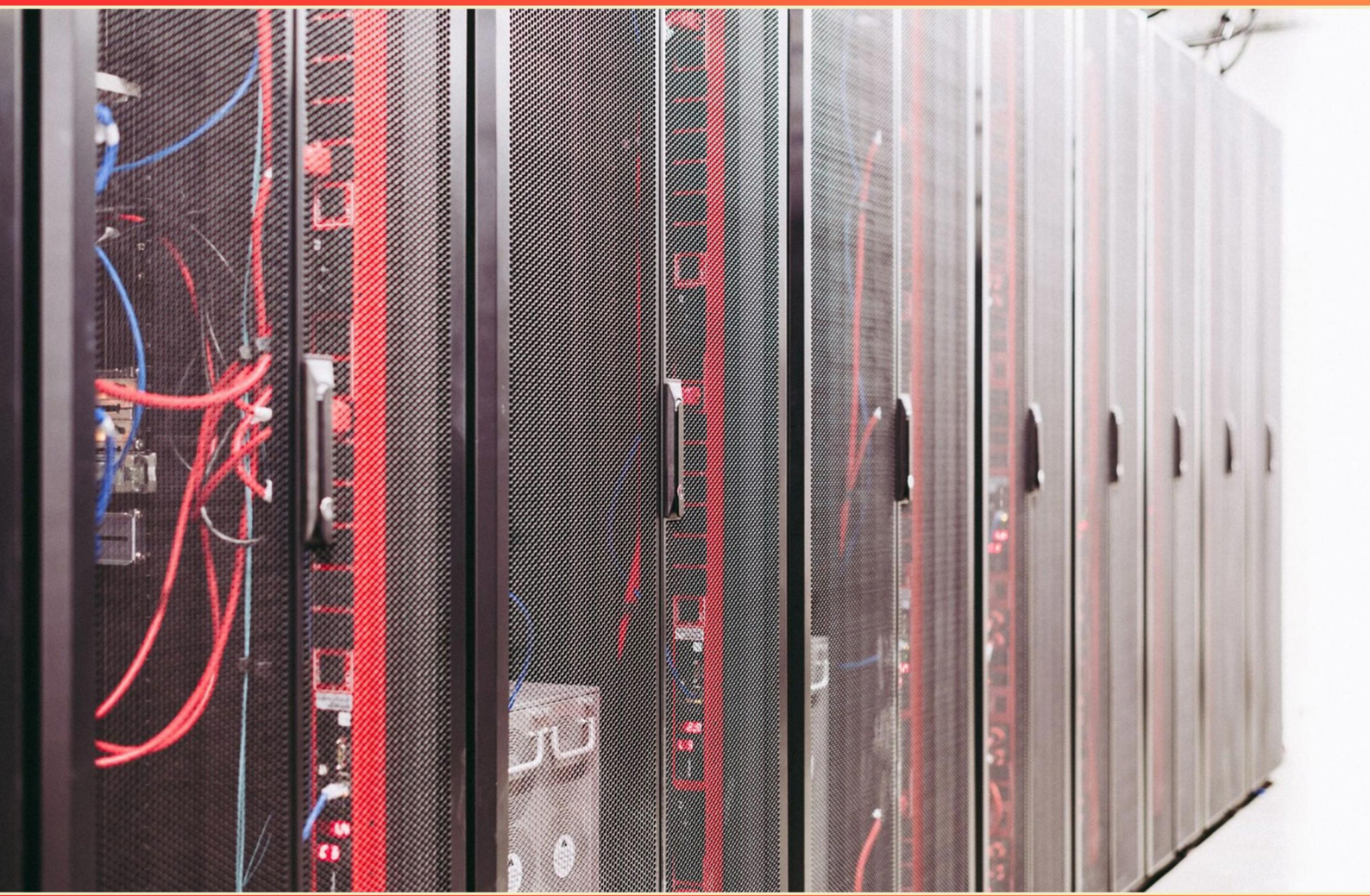
CYBER FUNDAMENTALS BLOCK 5 PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cyberfundamentalsblock5.examzify.com

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. **In incident response, which document outlines each member's roles and responsibilities?**

   A. Incident Response Plan

   B. Acceptable Use Policy

   C. Data Handling Procedure

   D. Continuity Plan

2. **Baselining is concerned with establishing a known state of the system's what?**

   A. Performance metrics

   B. Network topology

   C. Configuration

   D. User accounts

3. **A worm has the unique characteristic of being able to replicate without needing _____ to activate the virus.**

   A. An email

   B. A password

   C. A user

   D. A network connection

4. **After credentials are verified, which AAA component governs granting access rights?**

   A. Authentication

   B. Authorization

   C. Identification

   D. Accounting

5. **When should gathering information take place during root cause analysis?**

   A. First step

   B. After remediation

   C. During the analysis phase

   D. During the final step

6. Proxy servers are also known as what?

A. Network-layer routers

B. Stateful firewalls

C. IDS

D. Application-layer firewalls

7. Which statement best describes multi-factor authentication?

A. It requires a single factor for access

B. It requires at least two different factors

C. It requires two of the same type for stronger security

D. It is the same as two-step verification

8. Within the BIOS, _____ setup program determines what storage device to boot the system from.

A. Complementary metal-oxide-semiconductor (CMOS)

B. Central processing unit (CPU)

C. RAM

D. Graphics processing unit (GPU)

9. A third party in a supply chain is a/an _____, subcontracted individual, or company that provides a product or a/an _____ in support of the primary objectives of an organization.

A. Client

B. Intermediary

C. Supplier

D. Regulator

10. Which area may be threatened by computer worms, viruses, and other malware incidents such as the ILOVEYOU worm or the Storm Worm?

A. National Security

B. Public Health

C. Educational Systems

D. Financial Markets

Answers

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

Explanations

1. In incident response, which document outlines each member's roles and responsibilities?

A. Incident Response Plan

B. Acceptable Use Policy

C. Data Handling Procedure

D. Continuity Plan

Assigning who does what during an incident is the purpose of an incident response plan. This document clearly lays out the incident response team's structure, who has authority to make decisions, who leads the response, who handles technical analysis, who communicates with stakeholders, and how escalation should occur. It also specifies contact lists, the sequence of actions at each stage (detection, containment, eradication, recovery, and lessons learned), and the overall workflow to keep the response organized and efficient. Other documents serve different purposes. An Acceptable Use Policy defines what users may and may not do with IT resources. A Data Handling Procedure explains how data should be classified and protected. A Continuity Plan focuses on keeping critical business functions running or restoring them after a disruption, rather than detailing the incident response roles and day-to-day actions during a security incident.

2. Baselining is concerned with establishing a known state of the system's what?

A. Performance metrics

B. Network topology

C. Configuration

D. User accounts

Baselining establishes a known state of how the system is configured. This means capturing the exact setup: hardware and software inventory, installed patches and updates, enabled or disabled services, startup configurations, security settings, and user accounts and permissions. By documenting this configuration, you create a reference point to compare against future states and quickly detect any changes, drift, or unauthorized modifications. While performance metrics or network topology can have their own baselines in other contexts, the fundamental idea here is to know and compare the system's setup—its configuration.

3. A worm has the unique characteristic of being able to replicate without needing _____ to activate the virus.

A. An email

B. A password

C. A user

D. A network connection

Worms spread autonomously, needing no user to trigger replication. Their defining trait is that they can copy themselves to other systems and propagate across networks without someone clicking an attachment or running a program. This contrasts with many other malware types that rely on a user action to activate. While a worm may use network connections to move around or even be delivered via email in some cases, the essential property is that no user is required to start its replication. The missing element in the statement is a user.

4. After credentials are verified, which AAA component governs granting access rights?

A. Authentication

B. Authorization

C. Identification

D. Accounting

Authorization determines what you are allowed to do once your identity has been confirmed. After credentials are verified (authentication), authorization applies access-control policies to grant specific rights to resources or actions—like which files you can read, which systems you can access, or which commands you can run. Accounting then logs your activity for auditing. So the reason authorization is correct is that it translates a verified identity into the permissions that define your access rights.

5. When should gathering information take place during root cause analysis?

A. First step

B. After remediation

C. During the analysis phase

D. During the final step

Gathering information at the outset is essential because it provides the facts, timeline, and context needed to understand what happened and what's affected. Collecting logs, configurations, witness accounts, and process data early helps distinguish symptoms from the true root cause and prevents jumping to conclusions too soon. This initial data collection sets the boundaries of the investigation, preserves evidence, and informs what questions to ask during analysis. You can and should continue gathering information as needed during the analysis, but starting with information collection ensures the analysis is grounded in real data rather than assumptions. Waiting until after remediation risks losing important evidence and biases the investigation toward the fix rather than understanding the underlying cause.

6. Proxy servers are also known as what?

A. Network-layer routers

B. Stateful firewalls

C. IDS

D. Application-layer firewalls

Proxy servers act as intermediaries between clients and servers, handling traffic at the application layer by interpreting protocol data (like HTTP requests) to enforce policies, filter content, and cache responses. This application-layer handling is what makes them effective application-layer firewalls, since they control and secure traffic based on the specifics of the application data. In contrast, network-layer routers forward packets based on IP, stateful firewalls inspect connections at the transport layer without proxying application content, and IDS monitor for suspicious activity rather than sit in the data path as a proxy. So the best match is application-layer firewalls.

7. Which statement best describes multi-factor authentication?

A. It requires a single factor for access

B. It requires at least two different factors

C. It requires two of the same type for stronger security

D. It is the same as two-step verification

Multi-factor authentication is about verifying identity using more than one credential from different categories. The best statement says you need at least two different factors, because security is strengthened by combining independent forms of proof, such as something you know (a password), something you have (a one-time code from a hardware token or phone), or something you are (a biometric). By requiring factors from different categories, compromising one factor does not automatically grant access. The other options fall short because a single factor isn't enough to verify identity, two factors that are the same type don't provide true multi-factor protection, and while two-step verification can involve two steps, it isn't always about distinct factor types in practice.

8. Within the BIOS, _____ setup program determines what storage device to boot the system from.

A. Complementary metal-oxide-semiconductor (CMOS)

B. Central processing unit (CPU)

C. RAM

D. Graphics processing unit (GPU)

Boot device priority is set in the BIOS configuration stored in CMOS. The CMOS holds the BIOS setup settings, including the boot order, which tells the firmware which storage device to try first during startup. When the system powers on, the BIOS reads that order and attempts to boot from the first available device. The CPU runs the firmware, RAM provides working memory, and GPU handles graphics; none of these directly decide which storage device to boot from. So the CMOS setup is the element that determines the boot device.

9. A third party in a supply chain is a/an _____, subcontracted individual, or company that provides a product or a/an _____ in support of the primary objectives of an organization.

A. Client

B. Intermediary

C. Supplier

D. Regulator

In a supply chain, an intermediary is a third party that sits between the organization and its suppliers or customers, often contracted to provide goods or services that help the organization meet its objectives. This term fits because the description highlights a subcontracted individual or company whose role is to facilitate or supply what the organization needs to achieve its goals. A client is the recipient of outputs, not a middleman. A regulator oversees rules and does not deliver products or services. A supplier provides inputs but isn't necessarily the contracted middleman that supports the organization's objectives through ongoing facilitation.

10. Which area may be threatened by computer worms, viruses, and other malware incidents such as the ILOVEYOU worm or the Storm Worm?

A. National Security

B. Public Health

C. Educational Systems

D. Financial Markets

Malware incidents—worms, viruses, and botnets—pose threats that go beyond individual computers and into the functioning of a nation. They can cripple critical infrastructure, disrupt communications, and undermine public safety and emergency response. The ILOVEYOU and Storm Worm examples show how quickly malware can spread and be weaponized to create large botnets or overwhelm networks, potentially targeting government systems or essential services. National security encompasses protecting these core capabilities and the nation's ability to respond to cyber incidents, making it the area most at risk from such malware. While public health, educational systems, or financial markets can be affected, the broader impact on national stability and defense is why national security is the best fit.

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!