CYBER FUNDAMENTALS BLOCK 1 PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cyberfundamentalsblock1.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 statement about wireless networks is true?

A. Connecting unsanctioned devices to a wireless network is easier.

B. Connecting unsanctioned devices to a wireless network is harder.

C. Wireless networks cannot be connected via Ethernet.

D. Wireless networks are always slower than wired.

2. Affected equipment will sometimes work correctly and sometimes not describes what type of ESD damage?

A. Intermittent

B. Permanent

C. Catastrophic

D. Inconsistent

3. What is the typical security risk associated with a rogue access point?

A. Brute force password cracking

B. DDoS attack on a router

C. Man-in-the-middle attack

D. SSL/TLS certificate spoofing

4. Which term describes communications that do not require a pre-established end-to-end connection?

A. Connectionless

B. Connection-oriented

C. Circuit-switched

D. Reliable

5. Connectionless protocols are also known as _____ communications since _____ is involved.

A. Datagram, UDP

B. Datagram, TCP

C. Datagram, IP

D. Datagram, ICMP

6. Which statement about FTP is true?

A. Connection-oriented and uses TCP for file transfer.

B. Operates over UDP and provides error-free delivery by default.

C. Primarily used for email transmission over the internet.

D. Translates domain names into IP addresses.

7. Which OSI layer ensures that information is reformatted back into the original format?

A. Presentation

B. Physical

C. Application

D. Session

8. Which OSI layer is named 'Session'?

A. Physical

B. Presentation

C. Session

D. Application

9. Well-Known ports, also known as system ports, range from:

A. 1024 - 49151

B. 1 - 1023

C. 0 - 1023

D. 49152 - 65535

10. Which of the following is NOT a proper handling precaution for Electrostatic Discharge Sensitive items (PICK ONE)?

A. Use ESD-safe work surfaces and mats.

B. Handle ESD items by their leads only.

C. Wear grounding wrist straps when handling.

D. Store ESD items in anti-static bags.

Answers

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

Explanations

1. Which statement about wireless networks is true?

A. Connecting unsanctioned devices to a wireless network is easier.

B. Connecting unsanctioned devices to a wireless network is harder.

C. Wireless networks cannot be connected via Ethernet.

D. Wireless networks are always slower than wired.

Wireless networks are a broadcast medium, with signals traveling through the air. Because of that, a device within range can discover the network and attempt to connect without needing a physical cable. If the network has weak security or a simple password, an unsanctioned device can join more easily than on a wired network, which requires physical access to a port and usually stricter controls. Strong security like WPA3 or 802.1X can restrict access, but the basic trait of air-based access makes it easier for unauthorized devices to connect. The other statements aren't generally true: wireless networks use Ethernet for backhaul to the broader network, so they are not isolated from wired infrastructure, and with current standards, wireless speeds can be very high and sometimes rival or surpass older wired connections, so it isn't accurate to say wireless is always slower.

2. Affected equipment will sometimes work correctly and sometimes not describes what type of ESD damage?

A. Intermittent

B. Permanent

C. Catastrophic

D. Inconsistent

Intermittent faults describe problems that appear, disappear, and reappear under the same conditions. In ESD events, a strike can temporarily alter a circuit so it misbehaves for a while and then returns to normal without lasting damage. This can happen due to momentary changes in transistor behavior, a marginal contact that briefly opens or closes, or a charge path that dissipates after power conditions settle. Because the issue isn't constant and can recur unpredictably, it fits the idea of intermittent damage. If the damage were permanent, the device would fail steadily after the event; if catastrophic, the device would be destroyed. The term inconsistent isn't the standard way to describe this scenario.

3. What is the typical security risk associated with a rogue access point?

A. Brute force password cracking

B. DDoS attack on a router

C. Man-in-the-middle attack

D. SSL/TLS certificate spoofing

Rogue access points create a network under the attacker's control, so the traffic from users connected to it passes through the attacker's device. That enables a man-in-the-middle scenario, where the attacker can observe, capture, or even alter the data as it travels between the user and its intended destination. This means credentials, personal information, and session data can be exposed, especially if users don't rely on strong encryption or if the attacker tricks devices into trusting a fake certificate. In short, the main risk is interception and potential manipulation of traffic between the user and services, which is the essence of a man-in-the-middle attack.

4. Which term describes communications that do not require a pre-established end-to-end connection?

A. Connectionless

B. Connection-oriented

C. Circuit-switched

D. Reliable

Communications that do not require a pre-established end-to-end connection are described as connectionless. In this mode, each data unit (packet) is sent independently, with no setup of a session or circuit before transmission. Because there's no handshake or ongoing connection, resources aren't reserved for the entire exchange, and delivery and ordering aren't guaranteed by the network. This is typical of IP networks using UDP, where packets can take different routes and arrive out of order or not at all, leaving reliability to higher-layer protocols or applications. In contrast, a connection-oriented approach establishes a session first, providing a stable path and often in-order, reliable delivery (think TCP). Circuit-switched networks create a dedicated path for the duration of the communication. Reliability isn't about the mode itself; it's a property that can apply in different modes, but it doesn't define whether a connection is established.

5. Connectionless protocols are also known as _____ communications since _____ is involved.

A. Datagram, UDP

B. Datagram, TCP

C. Datagram, IP

D. Datagram, ICMP

Datagram communications describe sending data as independent packets without establishing a connection first. UDP is the transport-layer protocol that provides this connectionless, datagram-based service, so this pairing fits best. TCP is connection-oriented and creates a reliable stream rather than discrete datagrams; IP operates at the network layer and, while it routes datagrams, it isn't the transport service described here; ICMP is for control messages, not delivering application data.

6. Which statement about FTP is true?

A. Connection-oriented and uses TCP for file transfer.

B. Operates over UDP and provides error-free delivery by default.

C. Primarily used for email transmission over the internet.

D. Translates domain names into IP addresses.

FTP transfers files by built-in reliance on TCP, which is a connection-oriented transport. TCP sets up a reliable session, ensures data arrives in order, and handles retransmissions if any packets are lost. That reliability is exactly what FTP needs to move whole files accurately across a network, so using TCP makes this statement true. The other ideas don't fit FTP's design. FTP does not operate over UDP, since UDP is connectionless and does not guarantee delivery by default. It isn't primarily used for email; email relies on protocols like SMTP, IMAP, and POP3. And translating domain names into IP addresses is the job of DNS, not FTP.

7. Which OSI layer ensures that information is reformatted back into the original format?

A. Presentation

B. Physical

C. Application

D. Session

The layer that handles how data is formatted for the receiving application is responsible for reconstituting it back to the original form. It takes any transformations applied for transport—such as character encoding, data compression, or encryption—and undoes them so the application can interpret the data correctly. This means translating between different data representations, decompressing, and decrypting as needed before handing the data up to the application layer. Other layers deal with the mechanics of transmission, managing sessions, or providing services to apps, but reformatting into the original format happens at this layer. So the correct choice is the layer that handles data presentation, formatting, and translation.

8. Which OSI layer is named 'Session'?

A. Physical

B. Presentation

C. Session

D. Application

The session management concept is tested here. The layer named Session is responsible for coordinating and controlling the dialogue between two communicating endpoints. It establishes, maintains, and terminates conversations, manages who can talk when, and can insert synchronization points so communication can resume smoothly after interruptions. In the OSI model, this layer sits between the Transport layer above it and the Presentation layer below it. The other layers handle different duties: Physical covers the actual hardware signaling, Presentation handles data formatting and encryption/compression, and Application provides network services to user software. Since this layer is literally called "Session," it's the one that fits the question.

9. Well-Known ports, also known as system ports, range from:

A. 1024 - 49151

B. 1 - 1023

C. 0 - 1023

D. 49152 - 65535

Well-known ports are the standard service ports that are reserved for system and widely used services. They range from 0 through 1023. These ports are assigned by IANA to specific services—for instance, HTTP on 80, HTTPS on 443, SSH on 22, and DNS on 53—and on many systems they require elevated privileges to bind, reflecting their privileged status. The other ranges serve different purposes: 1024 through 49151 are registered ports used by specific applications but not as universally standardized; 49152 through 65535 are dynamic or private ports used for short-lived client connections. Therefore, the well-known ports are 0 to 1023.

10. Which of the following is NOT a proper handling precaution for Electrostatic Discharge Sensitive items (PICK ONE)?

A. Use ESD-safe work surfaces and mats.

B. Handle ESD items by their leads only.

C. Wear grounding wrist straps when handling.

D. Store ESD items in anti-static bags.

Handling Electrostatic Discharge Sensitive items involves keeping them at a controlled, low-static potential and avoiding contact with sensitive circuitry. Using ESD-safe work surfaces and mats helps dissipate static charges so devices don't accumulate a damaging potential. Wearing grounding wrist straps ties your body to ground, preventing you from carrying a charge onto the device. Storing ESDS in anti-static bags protects them from accumulating charges when not in use. The practice of handling ESDS items by their leads is not proper because touching the leads can mechanically damage them, introduce oils or contaminants, and concentrates any residual static energy into the most sensitive parts of the device. Instead, handle the item by its edges or use appropriate non-conductive tools, keeping yourself grounded and surfaces controlled to minimize risk.

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://cyberfundamentalsblock1.examzify.com

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