Security Blue Team Level 1 Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

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. What is Whaling?

A. General phishing

B. Spam email

C. Malware-laden attachments

D. Highly-targeted phishing against management

2. Which term describes the grouping of sectors within a disk by which files are organized?

A. Platter

B. Sectors

C. Clusters

D. Slack Space

3. What distinguishes SEM from SIM in security software?

A. real-time identification, collection, monitoring, evaluation, notification and correlation of events and alerts

B. Storing user passwords

C. Monitoring only network traffic

D. Automated software updates

4. Which algorithm is an example of symmetric cryptography?

A. RSA

B. ECC

C. AES

D. SHA-256

5. Which Linux commands are commonly used to compute file hashes such as SHA-256, MD5, and SHA-1?

A. get-filehash <file>

B. sha256sum, md5sum, sha1sum

C. hashsum <file>

D. hashfile <file>

6. Which statement best describes Precursors?

A. They are encryption keys

B. They are dashboards

C. They are patch management steps

D. They are elements of incident identification and response that help determine the existence of flaws and vulnerabilities

7. What is the purpose of an incident response playbook?

A. To replace the incident response team

B. To provide step-by-step, pre-approved actions for responders to follow during incidents, ensuring consistency and speed

C. To log access attempts

D. To document network devices

8. Which ACPO principle requires an audit trail or other record of all processes applied to computer-based electronic evidence to be created and preserved, with an independent third party able to examine those processes?

A. ACPO Principle 1

B. ACPO Principle 2

C. ACPO Principle 4

D. ACPO Principle 3

9. Threat Exposure Check involves using multiple tools to look for indicators of compromise retrieved from which sources?

A. Internal security logs only

B. A single vendor feed

C. Public vulnerability databases

D. Intelligence vendors, information sharing partners, government alerts, OSINT sources

10. Why is log normalization important in a SIEM system?

A. To ensure logs can be compared and correlated across disparate sources

B. To encrypt logs for transport

C. To delete duplicates to save storage

D. To increase log verbosity

Answers

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

Explanations

1. What is Whaling?

A. General phishing

B. Spam email

C. Malware-laden attachments

D. Highly-targeted phishing against management

Whaling is a targeted phishing attack aimed at high-level individuals like executives or managers to trick them into revealing credentials or authorizing fraudulent transfers. Attackers do background work to learn about the target and craft messages that look legitimate, often impersonating a trusted figure such as the CEO or CFO. The goal is to exploit authority and urgency to bypass normal scrutiny, steering the victim toward revealing sensitive information or approving a money transfer. This is different from general phishing, which casts a wide net with generic messages to many people. It's not simply about a spam email or about sending malware-infected attachments; whaling centers on highly personalized social engineering directed at leadership to achieve significant financial or access goals.

2. Which term describes the grouping of sectors within a disk by which files are organized?

A. Platter

B. Sectors

C. Clusters

D. Slack Space

Grouping of sectors into an allocation unit called clusters explains how files are organized on a disk. A cluster is the smallest unit the file system uses to allocate space, and it consists of one or more sectors. Files are stored in one or more clusters, and the file system keeps track of which clusters belong to which file, making data retrieval and space management possible. Slack space is the unused portion of the final cluster of a file, while a platter is simply a physical disk surface, not an organizational unit. So the term that describes the grouping of sectors by which files are organized is clusters.

3. What distinguishes SEM from SIM in security software?

A. real-time identification, collection, monitoring, evaluation, notification and correlation of events and alerts

B. Storing user passwords

C. Monitoring only network traffic

D. Automated software updates

SEM focuses on real-time handling of security events. It continuously collects events from multiple sources, analyzes them as they occur, correlates related events to identify incidents, and notifies responders or triggers automated actions. This live, proactive approach is what differentiates SEM from SIM, which is about storing and organizing security data (logs, alerts) for later analysis and reporting rather than immediate detection. So the option that mentions real-time identification, collection, monitoring, evaluation, notification and correlation of events and alerts best captures SEM's purpose. The other choices miss the real-time, event-driven aspect or describe unrelated functions (like merely storing passwords, or only monitoring network traffic, or software updates).

4. Which algorithm is an example of symmetric cryptography?

A. RSA

B. ECC

C. AES

D. SHA-256

Symmetric cryptography uses the same secret key to both encrypt and decrypt data. AES is a symmetric block cipher that uses one key for both directions, making it efficient for protecting large amounts of data. The other options are not symmetric: RSA and ECC are asymmetric algorithms that rely on a key pair (public and private keys) for encryption and decryption, and SHA-256 is a cryptographic hash function used for integrity, not encryption. So AES best fits the idea of symmetric cryptography among these choices.

5. Which Linux commands are commonly used to compute file hashes such as SHA-256, MD5, and SHA-1?

A. get-filehash <file>

B. sha256sum, md5sum, sha1sum

C. hashsum <file>

D. hashfile <file>

Computing file hashes on Linux is done with dedicated sum utilities that implement common algorithms like MD5, SHA-1, and SHA-256. The standard tools are sha256sum, md5sum, and sha1sum, each producing the hex digest for a file (and the file name) when run, for example: sha256sum myfile.txt. These commands are part of GNU coreutils and are designed to help verify integrity by comparing the generated digest to a known value or by using a checksum file with --check. The other options aren't standard Linux commands for computing these hashes (get-filehash is not a typical Linux tool; it resembles PowerShell usage, while hashsum and hashfile are not standard GNU utilities).

6. Which statement best describes Precursors?

A. They are encryption keys

B. They are dashboards

C. They are patch management steps

D. They are elements of incident identification and response that help determine the existence of flaws and vulnerabilities

Precursors are early warning signals in security monitoring that point to potential problems before a full incident occurs. They help determine that there may be flaws or vulnerabilities in the environment and guide responders to investigate, verify, and remediate before exploitation escalates. They aren't encryption keys, dashboards, or patch-management steps, which serve different roles in security operations. For example, unusual login patterns, unexpected new user accounts, or unusual outbound connections can act as precursors signaling possible weaknesses being exploited and prompting further investigation.

7. What is the purpose of an incident response playbook?

A. To replace the incident response team

B. To provide step-by-step, pre-approved actions for responders to follow during incidents, ensuring consistency and speed

C. To log access attempts

D. To document network devices

An incident response playbook provides a pre-planned, step-by-step set of actions for responders to follow during security incidents, written and pre-approved to ensure everyone acts in a consistent and fast way. It guides who to contact, what communications to send, when to escalate, and how to collect evidence, so the team can move through containment, eradication, and recovery efficiently and with less confusion under pressure. It complements the incident response team rather than replacing it, and it isn't about logging access attempts or listing network devices—that information lives in logging systems and asset management, not in the playbook itself.

8. Which ACPO principle requires an audit trail or other record of all processes applied to computer-based electronic evidence to be created and preserved, with an independent third party able to examine those processes?

A. ACPO Principle 1

B. ACPO Principle 2

C. ACPO Principle 4

D. ACPO Principle 3

This tests the requirement for auditable handling of electronic evidence with independent verification. In digital investigations, every action taken on the evidence—who did it, when, and what tools or methods were used—must be recorded in a traceable log. Preserving this audit trail and making it available for inspection by an independent third party guarantees the processes were followed correctly and that the evidence hasn't been tampered with. This transparency supports the integrity and admissibility of the evidence in court, and it helps prevent bias or improper alterations during analysis. While other principles focus on preventing changes, proper authorization, or securing access, this one specifically emphasizes documented, verifiable, and reviewable processing by an impartial observer.

9. Threat Exposure Check involves using multiple tools to look for indicators of compromise retrieved from which sources?

A. Internal security logs only

B. A single vendor feed

C. Public vulnerability databases

D. Intelligence vendors, information sharing partners, government alerts, OSINT sources

The idea being tested is that a thorough threat exposure check looks for indicators of compromise across a broad mix of sources, not just one place. Pulling IOCs from intelligence vendors, information-sharing partners, government alerts, and OSINT sources gives a wide view of active threats and campaigns. This diverse feed captures a range of indicators—malicious domains, IPs, file hashes, and TTPs—from vendors who aggregate telemetry, partners who share industry-specific intel, official government advisories, and open-source intelligence. Relying on a single source like internal logs or one vendor limits visibility and may miss new or broader threats. Public vulnerability databases are useful for vulnerabilities themselves but don't always provide the live IOC signals associated with active compromises. So the best approach is a multi-source intake that includes those intelligence channels, which is why that option is the correct one.

10. Why is log normalization important in a SIEM system?

A. To ensure logs can be compared and correlated across disparate sources

B. To encrypt logs for transport

C. To delete duplicates to save storage

D. To increase log verbosity

Log normalization standardizes diverse logs into a uniform schema with common field names, formats, and time representations. This lets logs from different sources be compared and correlated because the SIEM can map each vendor's fields into the same model, such as user, source IP, destination, timestamp, and event type. With a unified format, detection rules can be written once and applied across all data, searches become reliable, and timelines align when timestamps are normalized to a common timezone (often UTC). This improves detection accuracy, reduces parsing errors, and enables meaningful dashboards and investigations. Encrypting logs for transport, deduplicating for storage, or simply increasing verbosity are separate concerns not achieved by normalization.

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://securityblueteamlvl1.examzify.com

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