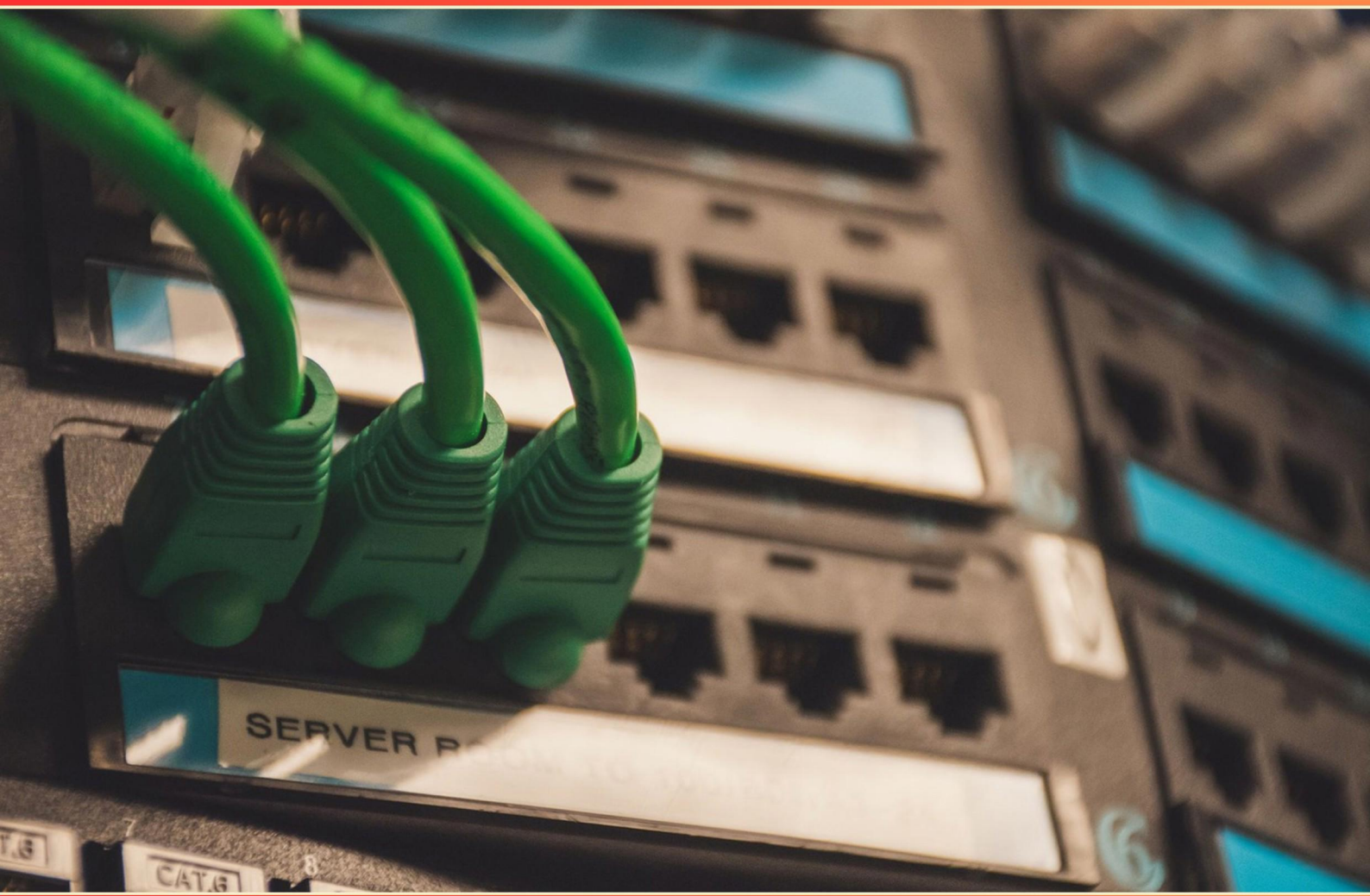
SECURITY BLUE TEAM LEVEL 1 PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://securityblueteamlvl1.examzify.com

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

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 stage involves setting goals and stakeholders for the intelligence project?

A. Planning & Direction

B. Collection

C. Processing

D. Dissemination

2. What are the key components of a cybersecurity incident report?

A. Incident facts and timeline only.

B. Affected assets, containment actions, and remediation steps.

C. Incident facts, timeline, affected assets, containment actions, root cause, remediation steps, evidence, lessons learned, stakeholders.

D. Only the stakeholders need to be identified.

3. What is Attribution?

A. The legal process for prosecuting attackers

B. A vulnerability assessment method

C. Determination of who, what or where a cyber breach or intrusion has occurred

D. A method for patch deployment

4. What describes Hosted Malware?

A. Malware hosted on websites that users click to download

B. A malicious domain or compromised site hosting malware

C. Malware embedded in image files

D. Malware delivered via USB drives

5. Which log file contains information about failed login attempts?

A. /var/log/btmp

B. /var/log/auth.log

C. /var/log/secure

D. /var/log/faillog

6. Which Windows command computes the SHA-256 hash of a file?

A. sha256sum <file>

B. md5sum <file>

C. get-filehash -algorithm md5 <file>

D. get-filehash <file> (SHA256)

7. Which phase requires proven techniques and methodology to be reproducible by other forensic examiners?

A. Preservation

B. Collection

C. Identification

D. Reporting

8. What does TAXII define?

A. A standard for sharing cyber threat information using services and message exchanges designed to handle STIX information

B. A standard for threat data encryption

C. A language for describing malware behaviors

D. A method for secure password storage

9. Which phishing category involves impersonating a known source to obtain financial advantage?

A. Spear Phishing

B. Impersonation

C. Business Email Compromise (BEC)

D. Typosquatting

10. What is the Windows hibernation file used for?

A. memory.dmp

B. hiberfil.sys

C. swapfile

D. pagefile.sys

Answers

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

Explanations

1. Which stage involves setting goals and stakeholders for the intelligence project?

A. Planning & Direction

B. Collection

C. Processing

D. Dissemination

Setting goals and identifying who has a stake in the effort happens in the planning and direction stage. This is the point in the intelligence process where the problem is defined, intelligence requirements are established, objectives are set, and the key stakeholders and their needs are outlined. It also covers deciding on scope, priorities, timelines, and resource allocation, which then guides what data to collect and how to analyze it. Once these plans are in place, the next stages focus on gathering data (collection), turning it into usable information (processing), and sharing the results with the right people (dissemination).

2. What are the key components of a cybersecurity incident report?

A. Incident facts and timeline only.

B. Affected assets, containment actions, and remediation steps.

C. Incident facts, timeline, affected assets, containment actions, root cause, remediation steps, evidence, lessons learned, stakeholders.

D. Only the stakeholders need to be identified.

A cybersecurity incident report should capture a full, actionable record of what happened, when it happened, and how it was handled. This means documenting incident facts and the timeline to establish what occurred and in what order, the assets that were affected to show the scope and impact, the containment actions taken to stop the incident, and the remediation steps to restore operations and prevent recurrence. It also includes a root-cause analysis to identify underlying vulnerabilities or failures, evidence collected for forensics and accountability, lessons learned to improve future response, and the stakeholders who need to be informed or involved. This comprehensive set of elements ensures the report is useful for post-incident review, regulatory or legal needs, and ongoing security improvements. Leaving out any of these parts—such as the timeline, affected assets, containment, or lessons learned—can leave gaps in understanding, accountability, or the ability to prevent similar incidents in the future.

3. What is Attribution?

A. The legal process for prosecuting attackers

B. A vulnerability assessment method

C. Determination of who, what or where a cyber breach or intrusion has occurred

D. A method for patch deployment

Attribution is the process of determining who, what, or where a cyber breach or intrusion originated. It involves linking the attack to a specific actor or group, the tools they used, and the source infrastructure or geography involved. In practice, analysts combine indicators, threat intelligence, observed TTPs (tactics, techniques, and procedures), malware signatures, reclaimed infrastructure, and digital forensics to form a reasoned assessment about the responsible party and the origin of the intrusion. It's not about prosecuting attackers—that's a legal process that may follow attribution—nor is it a vulnerability assessment method or a patch deployment technique. Understanding attribution helps security teams contextualize threats and prioritize defenses, but it's often probabilistic and can be influenced by deception, false flags, or use of compromised intermediaries.

4. What describes Hosted Malware?

A. Malware hosted on websites that users click to download

B. A malicious domain or compromised site hosting malware

C. Malware embedded in image files

D. Malware delivered via USB drives

Hosted malware means the attacker places the malicious payload on a remote host so it can be served to victims from that location. A malicious domain or a compromised site hosting the malware fits this idea perfectly because the site acts as the delivery point, storing the payload and distributing it to users who visit or interact with it. This setup enables techniques like drive-by downloads or exploit-driven redirects, where simply visiting the site can trigger the delivery of the malware. Why the other ideas don't fit as well: embedding malware in image files is a different tactic (steganography or payload concealment within media), and malware delivered via USB drives involves physical media rather than a remote hosting site. The description about malware hosted on websites that users click to download is close, but the defining feature of hosted malware is that the malicious code is hosted on a domain or compromised site acting as the hosting point for the payload.

5. Which log file contains information about failed login attempts?

A. /var/log/btmp

B. /var/log/auth.log

C. /var/log/secure

D. /var/log/faillog

Failed login attempts are tracked in a dedicated log that records each failed attempt as an individual event, including when and from where it occurred. That specific log is /var/log/btmp, a binary file that you read with the lastb command to see the failed logins. This makes it the primary source for listing failed login activity. Other logs play different roles: /var/log/auth.log and /var/log/secure capture authentication-related messages, including both successes and failures, so they're broader audit trails rather than a focused record of failed attempts. /var/log/faillog stores per-user failure counts and is less useful for reviewing every failed attempt, since it doesn't present the events as a straightforward log. So for information about failed login attempts, /var/log/btmp is the best and most direct source.

6. Which Windows command computes the SHA-256 hash of a file?

A. sha256sum <file>

B. md5sum <file>

C. get-filehash -algorithm md5 <file>

D. get-filehash <file> (SHA256)

To verify a file's integrity on Windows, you compute a SHA-256 hash using the built-in PowerShell tool Get-FileHash. This cmdlet is designed specifically for generating file hashes, and you can specify the algorithm, including SHA256, to produce the correct hash value for comparison. Two of the options point to Linux-style utilities (sha256sum and md5sum), which aren't part of Windows by default. One option uses a Windows command but requests MD5 instead of SHA-256, which would give you a different hash. The remaining option is Get-FileHash with SHA256, which is the standard Windows approach for this task. In PowerShell, you'd typically run something like Get-FileHash -Algorithm SHA256 -Path "C:\path\to\file" to obtain the SHA-256 hash for verification. This makes it the correct choice because it uses Windows' native hashing tool and specifies the SHA-256 algorithm.

7. Which phase requires proven techniques and methodology to be reproducible by other forensic examiners?

A. Preservation

B. Collection

C. Identification

D. Reporting

Focusing on the ability for proven techniques and methodology to be repeated by other examiners is all about documenting and communicating the process so others can reproduce it. The reporting phase is where the examiner lays out exactly what was done, with precise details: the methods used, tools and software versions, calibration data, parameter settings, controls, and the logical reasoning that connects the evidence to the conclusions. This level of detail makes the approach transparent and verifiable, which is essential for validation, peer review, and admissibility in court. Preservation and collection are about maintaining the integrity of the evidence and gathering it without introducing changes, not about proving that others can reproduce the entire procedure and result. Identification relies on established criteria to determine what an item is, but without a thorough, repeatable account of the steps taken and the rationale, others cannot reproduce the conclusion. Reporting, by contrast, provides the reproducible trail—methods, decisions, and documentation—so another examiner can follow the same path and arrive at the same outcome.

8. What does TAXII define?

A. A standard for sharing cyber threat information using services and message exchanges designed to handle STIX information

B. A standard for threat data encryption

C. A language for describing malware behaviors

D. A method for secure password storage

TAXII defines a standard for sharing cyber threat information through a suite of services and message exchanges designed to carry STIX data. It provides the transport, discovery, and collection mechanisms that enable security teams to exchange indicators, tactics, techniques, and other threat intel in a consistent, automatable way. STIX supplies the data model for describing the threat information, while TAXII handles how that information is moved between producers and consumers. This is not about encrypting threat data, describing malware behaviors in a dedicated language, or securely storing passwords, which is why TAXII is the best-fit description for what the standard defines.

9. Which phishing category involves impersonating a known source to obtain financial advantage?

A. Spear Phishing

B. Impersonation

C. Business Email Compromise (BEC)

D. Typosquatting

Impersonating a trusted business contact to push for a money transfer is a classic Business Email Compromise scenario. In BEC, the attacker poses as someone the recipient knows and respects—such as a CEO, supplier, or finance contact—and convinces them to wire funds or disclose banking details. The strength of this tactic lies in exploiting legitimate-looking emails and internal processes to bypass suspicion, making financial gain the primary goal. Spear phishing targets credentials or data and isn't always aimed directly at transferring money; typosquatting is about tricking victims with a fake domain to harvest information, not necessarily about impersonating a known source to steal funds. So the category that best fits the situation described is Business Email Compromise.

10. What is the Windows hibernation file used for?

A. memory.dmp

B. hiberfil.sys

C. swapfile

D. pagefile.sys

The concept being tested is how Windows preserves a full system state when you power off by using a dedicated on-disk image of RAM. The file used for this is hiberfil.sys. When you put your computer into hibernation, Windows saves the entire contents of memory to this file so the exact state of all running programs and open documents can be restored when you resume. This allows a complete power-off without losing work, unlike sleep which keeps RAM active in a low-power state. This is different from a crash-dump file like memory.dmp, which is created to analyze a system crash after it occurs. It's also distinct from a swap or page file (swapfile or pagefile.sys), which are used for virtual memory paging to disk during normal operation, not to store a full RAM image for hibernation. hiberfil.sys is the specific file Windows uses for hibernation, typically on the system drive, and its size is tied to the amount of RAM.

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!