CYBERSECURITY AND DIGITAL FORENSICS PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cybersecdigiforensics.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 risk assessment, which step involves monitoring after controls are in place?**

   A. Identify assets

   B. Assess likelihood and impact

   C. Monitor residual risk

   D. Select controls to treat risks

2. **During ransomware containment, why is it important that backups be offline?**

   A. To prevent backups from being encrypted by the ransomware.

   B. To increase backup speed

   C. To ensure backups are always online

   D. To prevent backups from being used for testing

3. **What is the purpose of a Certificate Revocation List (CRL)?**

   A. To publish new certificates

   B. To bind a public key to an identity

   C. To revoke certificates that should no longer be trusted

   D. To renew expired certificates

4. **What is threat modeling and which method is commonly used in practice?**

   A. Process to identify, characterize, and mitigate potential threats; commonly uses STRIDE or PASTA.

   B. A method for deploying security patches quickly.

   C. A cognitive approach to risk assessment unrelated to systems.

   D. A standard for code formatting.

5. **What is the difference between log correlation and event correlation in SIEMs?**

   A. Log correlation analyzes individual events only.

   B. Event correlation uses broader dataset across logs.

   C. Event correlation links single events in time; log correlation analyzes patterns across logs for anomalies; both enable detection.

   D. They are unrelated processes.

6. What is the principle of least privilege in access control?

A. Grant all users full access.

B. Grant only minimal rights required; implement RBAC/ABAC, need-to-know, just-in-time access, and regularly review permissions.

C. Only admins get access.

D. Access is granted based on job title alone.

7. Which is not a phase in the SANS incident response process?

A. Avoidance

B. Preparation

C. Containment

D. Eradication

8. Which mechanism ensures that a client connects to a legitimate server by validating the server's certificate during a secure session?

A. TLS certificate validation.

B. Password policy.

C. IP address filtering.

D. Two-factor authentication.

9. Which statement about symmetric cryptography is true?

A. It uses public/private key pairs

B. It is best for digital signatures

C. It uses the same key for encryption and decryption, suitable for bulk confidentiality

D. It requires certificates for operation

10. Which statement best describes what log data can help with security investigations?

A. Log data can reveal when a specific event or error occurred

B. Log data contains full user passwords

C. Log data is irrelevant to application behavior

D. Log data is only useful for billing

Answers

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

Explanations

1. In risk assessment, which step involves monitoring after controls are in place?

A. Identify assets

B. Assess likelihood and impact

C. Monitor residual risk

D. Select controls to treat risks

Monitoring residual risk is about watching the risk that remains after controls are in place. Once safeguards are implemented, threats can evolve, controls can degrade, or new vulnerabilities can appear, so ongoing monitoring helps determine whether the remaining risk is acceptable and whether controls need adjustment or additional measures. This kind of continuous oversight keeps the risk level aligned with what the organization is willing to accept. The other steps focus on identifying what to protect, analyzing how severe the risk could be, and selecting and implementing safeguards before monitoring occurs.

2. During ransomware containment, why is it important that backups be offline?

A. To prevent backups from being encrypted by the ransomware.

B. To increase backup speed

C. To ensure backups are always online

D. To prevent backups from being used for testing

When ransomware containment is in play, backups must be offline to stay safe from the attack. Keeping backups disconnected from the network or stored on removable media that isn't mounted means the malware cannot reach them to encrypt or tamper with them. This air-gapped setup preserves clean restore points, allowing you to recover systems from a known good state after the incident. Testing and verification of those backups should still be done, but the core protection during containment is that offline backups are immune to the encryption that the ransomware is deploying. The other options don't fit the scenario: offline status doesn't inherently speed up backup; making backups always online would expose them to encryption; and the idea of keeping backups from testing isn't relevant to safeguarding recoverability during an attack.

3. What is the purpose of a Certificate Revocation List (CRL)?

A. To publish new certificates

B. To bind a public key to an identity

C. To revoke certificates that should no longer be trusted

D. To renew expired certificates

A Certificate Revocation List is used to explicitly mark certificates as no longer trustworthy before their planned expiration. It's published by the certificate authority and contains the serial numbers of certificates that have been revoked, for reasons such as key compromise, change of affiliation, or policy violations. When validating a certificate, clients (like browsers or servers) can check the CRL to see if the certificate in question appears on the list; if it does, it must be rejected even if the certificate hasn't expired yet. This protects security by ensuring that compromised or misissued certificates aren't trusted. Publishing new certificates is what happens when a CA issues a fresh certificate, not when revoking one. Binding a public key to an identity is the purpose of the certificate itself, which occurs during issuance. Renewing expired certificates is a separate process involving reissuing or extending validity, not revocation.

4. What is threat modeling and which method is commonly used in practice?

A. Process to identify, characterize, and mitigate potential threats; commonly uses STRIDE or PASTA.

B. A method for deploying security patches quickly.

C. A cognitive approach to risk assessment unrelated to systems.

D. A standard for code formatting.

Threat modeling is a structured approach to identifying and addressing security threats early in a system's design. It starts by clarifying what needs to be protected—assets, data, and services—and then analyzes how attackers might compromise those elements through the system's architecture and data flows. The goal is to surface potential threats, assess their potential impact, and determine mitigations before implementation, guiding safer design choices and prioritizing security fixes. In practice, teams commonly use established methods to organize and standardize this analysis. STRIDE provides a taxonomy of threat types—Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege—so designers can systematically consider different attack vectors. PASTA, on the other hand, is a risk-centric, seven-stage process that aligns threat identification with business impact and likelihood to help prioritize defenses. These methodologies help ensure threat modeling covers comprehensive scenarios and produces actionable security controls, rather than focusing on patch deployment, cognitive risk assessments, or coding style standards.

5. What is the difference between log correlation and event correlation in SIEMs?

A. Log correlation analyzes individual events only.

B. Event correlation uses broader dataset across logs.

C. Event correlation links single events in time; log correlation analyzes patterns across logs for anomalies; both enable detection.

D. They are unrelated processes.

In SIEM, correlation means connecting pieces of security data to reveal what happened, rather than treating each event in isolation. Event correlation links related events that occur over time to form a sequence or chain that indicates an incident, such as a login attempt followed by a successful access from a new IP. Log correlation looks across many logs and data sources to detect patterns or anomalies that emerge only when you compare information from different systems, like unusual activity spanning authentication, network, and endpoint logs. Together, these approaches enable detection by capturing both the temporal relationships between events and cross-source patterns. For example, a series of failed logins and then a successful breach on the same host is the kind of sequence event correlation highlights, while a cross-source pattern of suspicious behavior across multiple logs is what log correlation detects. The other options misstate the scope or relationship: log correlation is not limited to single events, event correlation is not confined to a broad dataset across logs, and they are not unrelated processes.

6. What is the principle of least privilege in access control?

A. Grant all users full access.

B. Grant only minimal rights required; implement RBAC/ABAC, need-to-know, just-in-time access, and regularly review permissions.

C. Only admins get access.

D. Access is granted based on job title alone.

At the heart of access control is giving each user just enough permissions to do their job, no more. This limits what a compromised account or a misused credential can access or do, reducing risk and the potential damage of mistakes. In practice, this means using models like RBAC or ABAC to assign permissions based on roles or attributes, applying need-to-know principles so people only access information essential to their tasks, providing just-in-time access for temporary elevated rights, and regularly reviewing and revoking permissions to prevent privilege creep as roles change. Why this is the best answer: it captures both the mindset (minimal rights) and practical methods (roles/attributes, need-to-know, temporary access, and ongoing review) that together enforce least privilege. The alternative ideas—granting full access to everyone, restricting access to admins only, or judging access by job title alone—do not align with the principle because they either broaden access unnecessarily or fail to reflect actual task needs and dynamic changes.

7. Which is not a phase in the SANS incident response process?

A. Avoidance

B. Preparation

C. Containment

D. Eradication

Recognizing the official incident response lifecycle helps you see which activities are real phases. In the SANS model, the stages include Preparation, Containment, and Eradication (along with other steps like Identification, Recovery, and Lessons Learned). Avoidance is not a named phase within this lifecycle. Preparation sets up plans, tools, and training before an incident; Containment focuses on stopping the incident from spreading; Eradication involves removing the threat and fixing underlying issues so the environment can be restored. Because Avoidance isn't part of the formal SANS incident response stages, it's the correct choice for what is not a phase.

8. Which mechanism ensures that a client connects to a legitimate server by validating the server's certificate during a secure session?

A. TLS certificate validation.

B. Password policy.

C. IP address filtering.

D. Two-factor authentication.

Validating the server's certificate during a secure session is what lets the client trust the server's true identity. In TLS, the server presents a certificate that asserts who it is, issued by a trusted certificate authority. The client then performs certificate validation: it follows the certificate chain to a trusted root, verifies the certificate's signature, checks that it hasn't expired, confirms the hostname in the certificate matches the server's address, and may check revocation status (via OCSP or CRLs). If all these checks pass, the client establishes an encrypted channel with the legitimate server, preventing imposters from intercepting or tampering with the connection. The other options don't perform this server-identity verification during a secure session. A password policy governs user credentials, not server identity. IP address filtering controls which network endpoints can be reached but doesn't validate the server's certificate during the TLS handshake. Two-factor authentication strengthens user authentication, but it doesn't verify the server's identity in the TLS process.

9. Which statement about symmetric cryptography is true?

A. It uses public/private key pairs

B. It is best for digital signatures

C. It uses the same key for encryption and decryption, suitable for bulk confidentiality

D. It requires certificates for operation

Symmetric cryptography relies on a single shared secret for both encryption and decryption, which makes it fast and well-suited for protecting large amounts of data (bulk confidentiality). Once the shared key is securely exchanged, you can encrypt and decrypt big datasets efficiently using algorithms like AES. The other ideas belong to different approaches: public/private key pairs are fundamental to asymmetric cryptography, which handles key exchange and digital signatures rather than bulk data encryption; digital signatures rely on private keys to create a verifiable signature, something symmetric schemes cannot provide; and certificates are part of PKI to bind public keys to identities, not needed when you only use a shared secret key. So using the same key for both directions and applying it to bulk confidentiality is the correct characterization.

10. Which statement best describes what log data can help with security investigations?

A. Log data can reveal when a specific event or error occurred

B. Log data contains full user passwords

C. Log data is irrelevant to application behavior

D. Log data is only useful for billing

Logs provide a timeline of events that helps investigators reconstruct what happened during a security incident. Each log entry records something that occurred in the system along with a timestamp, such as a login attempt, access to a file, a service starting or stopping, an error, or a configuration change. That time-stamped sequence lets investigators place events in the correct order, see how a breach began, what actions followed, and which resources were affected. This temporal context is essential for understanding the scope of an incident, tracing attacker movements, and validating what happened. It's also important to recognize that security-friendly logging does not store full passwords; exposing secrets in logs is a major risk, so credentials and other sensitive data aren't kept in plain form. Logs are used to observe behavior and security-relevant activity, not for billing purposes, and they should be maintained and protected to preserve their integrity for investigations.

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://cybersecdigiforensics.examzify.com

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