DIGITAL FORENSIC CERTIFICATION PRACTICE EXAM (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://digitalforensic.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. What is the first step when analyzing suspicious MS Office documents?

A. Dumping macro streams

B. Finding suspicious components

C. Identifying suspicious VBA keywords

D. Finding macro streams

2. What type of attack involves flooding a switch's interface with Ethernet frames from various fake hardware addresses?

A. ARP spoofing

B. MAC flooding

C. Denial of Service

D. Packet sniffing

3. In a forensics investigation report, which section deals with the analysis of evidence and the techniques used?

A. Evidence information

B. Post-investigation phase

C. Evaluation and analysis process

D. Data analysis

4. What type of information would typically be included in the "Supporting Files" section of a forensics investigation report?

A. Evidence information

B. Attachments and appendices

C. Executive summary

D. Investigation process

5. Which built-in Windows utility is designed to detect errors in the file system and disk media?

A. Defrag command

B. Disk Cleanup

C. chkdsk command

D. System File Checker

6. In what phase of a computer forensics investigation is it necessary for the investigator to document observations of the electronic crime scene?

A. Evidence preservation

B. Data acquisition

C. Documentation of the electronic crime scene

D. Data analysis

7. Which log file in a Mac system contains information related to network interface history?

A. /var/log/daily.out

B. /var/log/network.log

C. /var/log/syslog

D. /var/log/events.log

8. When attackers inject malicious scripts into web pages by bypassing client security mechanisms, what attack are they employing?

A. Cross-site scripting

B. Cookie snooping

C. SQL injection

D. Unvalidated input

9. In which attack does an authenticated user unknowingly perform tasks for an attacker?

A. Cross-site request forgery

B. SQL injection

C. Authentication hijacking

D. Unvalidated forwarding

10. Which user-created evidence source can help in analyzing malicious links or URLs?

A. Email history

B. Internet bookmarks

C. Browser cache

D. Download history

Answers

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

Explanations

1. What is the first step when analyzing suspicious MS Office documents?

A. Dumping macro streams

B. Finding suspicious components

C. Identifying suspicious VBA keywords

D. Finding macro streams

When analyzing suspicious Microsoft Office documents, the first step typically involves finding suspicious components within the document. This approach allows the examiner to gain insights into any potentially malicious elements embedded in the document, such as macros, embedded objects, or hidden content. By identifying these components early in the analysis, the forensic investigator can determine which areas require deeper scrutiny and further investigative actions. This initial step is crucial because it establishes a foundation for the analysis. Once suspicious components are identified, the analyst can then proceed to evaluate the specific elements of the document, including examining macro streams, identifying VBA keywords, or dumping macro streams for detailed investigation. Thus, focusing first on the broader range of suspicious components enables a more structured and efficient analysis of the document, setting the stage for identifying potential threats that align with the investigative goals.

2. What type of attack involves flooding a switch's interface with Ethernet frames from various fake hardware addresses?

A. ARP spoofing

B. MAC flooding

C. Denial of Service

D. Packet sniffing

The correct answer is focused on the technique of overwhelming a switch's interface by sending a large number of Ethernet frames, each with different fake hardware addresses (MAC addresses). This practice is known as MAC flooding. In a switching network, each switch maintains a MAC address table that maps MAC addresses to their corresponding switch ports. When the table becomes full due to excessive fake addresses being sent, the switch can no longer properly process legitimate traffic. Instead of forwarding packets based on the MAC address table, the switch will enter what's called "fail-open mode," broadcasting incoming frames to all ports. This leads to network congestion and can substantially degrade the performance of the switch and the network overall. While the other options may involve network attacks or monitoring, they do not specifically describe the act of flooding a switch with frames that feature numerous fabricated MAC addresses, which is the defining characteristic of MAC flooding.

3. In a forensics investigation report, which section deals with the analysis of evidence and the techniques used?

A. Evidence information

B. Post-investigation phase

C. Evaluation and analysis process

D. Data analysis

The section that addresses the analysis of evidence and the techniques used during a forensic investigation is aptly termed the evaluation and analysis process. This part of the report is critical as it meticulously describes how the evidence was examined, the methodologies employed, and the reasoning behind the conclusions drawn from the analysis. It highlights the forensic techniques applied to corroborate findings, whether through data recovery, pattern analysis, or any specific tools utilized during the investigation. Understanding this section is vital for ensuring transparency and reproducibility in forensic work. It is essential for legal proceedings as well, as it provides the basis for expert testimony regarding how the evidence was handled and interpreted. The thoroughness of this section reflects the quality and credibility of the forensic investigation as a whole, serving to bolster the integrity of the conclusions presented in the report.

4. What type of information would typically be included in the "Supporting Files" section of a forensics investigation report?

A. Evidence information

B. Attachments and appendices

C. Executive summary

D. Investigation process

The "Supporting Files" section of a forensics investigation report is intended to provide additional materials that support the findings and conclusions of the main report. This typically includes attachments and appendices, which may contain detailed data, complex analyses, raw data, diagrams, charts, and other supplementary documentation that enriches the content of the report. These supporting files are essential for providing context and transparency, allowing reviewers to understand the evidence and methodologies applied during the investigation comprehensively. They serve as a reference point for the main findings without cluttering the main report text, ensuring that the core narrative remains clear and focused. In contrast, other sections of the report, such as evidence information, an executive summary, and the investigation process, are more about presenting the findings, summarizing the report, and outlining the steps taken during the investigation, rather than providing supplementary materials.

5. Which built-in Windows utility is designed to detect errors in the file system and disk media?

A. Defrag command

B. Disk Cleanup

C. chkdsk command

D. System File Checker

The chkdsk command is specifically designed to check the integrity of the file system and disk media in Windows environments. When executed, it scans the file system for logical file system errors and checks disk media for physical errors. This utility can also fix any issues it encounters, helping to ensure that the file system remains healthy and functional. The chkdsk command can be run from a command prompt and can provide detailed information about the status of the disk, including sectors that may be marked as bad and potentially recoverable data. It is an essential tool in digital forensics as it helps in identifying issues that could affect data integrity during an investigation. Other utilities mentioned serve different purposes; for example, the defrag command is intended to optimize disk performance by reorganizing fragmented data. Disk Cleanup is a tool for removing unnecessary files from the disk to free up space, and the System File Checker verifies the integrity of system files but does not address file system errors on disks. Therefore, chkdsk is the most appropriate utility for detecting errors in the file system and disk media.

6. In what phase of a computer forensics investigation is it necessary for the investigator to document observations of the electronic crime scene?

A. Evidence preservation

B. Data acquisition

C. Documentation of the electronic crime scene

D. Data analysis

The phase in which it is essential for the investigator to document observations of the electronic crime scene is during the documentation of the electronic crime scene stage. This phase is critical because it involves capturing the state of the scene as it was found, including noting the layout of evidence, the condition of devices, and any other relevant details that could assist in understanding the context of the investigation. Documenting the scene accurately ensures that all evidence can be accounted for and referenced later in the investigation. This thorough documentation is necessary to support the integrity and validity of the forensic process and to provide a clear record that can be used in court if needed. Observations made during this phase can include photographs, sketches, and written notes that detail the setup and any potential evidence or anomalies present at the scene. While evidence preservation, data acquisition, and data analysis are all critical phases of a forensic investigation, they focus on different objectives. Evidence preservation is primarily concerned with maintaining the integrity of the evidence, data acquisition involves collecting and imaging data from devices, and data analysis focuses on examining the data to uncover information pertinent to the investigation. However, it is during the documentation phase that the investigator captures the initial conditions and observations that lay the foundation for the entire forensic process.

7. Which log file in a Mac system contains information related to network interface history?

A. /var/log/daily.out

B. /var/log/network.log

C. /var/log/syslog

D. /var/log/events.log

The log file that contains information related to network interface history on a Mac system is actually not the one selected. The correct choice for network interface history would typically be found in the system logs collecting various network-related information. The file located at /var/log/network.log specifically records events and messages pertaining to network activity, including configurations and interface statuses. This makes it the most relevant file for tracking changes and history associated with network interfaces. Conversely, while /var/log/daily.out captures general system status and processes run on a daily basis, it does not focus solely on network interface history. Similarly, /var/log/syslog logs a variety of system messages but may not provide detailed insights specifically related to network interface activities. Finally, /var/log/events.log focuses on system events and notifications, which may not always include detailed chronological network interface changes. Thus, for tracking network interface history, network.log is the appropriate log file on a Mac system, as it is specifically designed to capture the relevant events and information regarding network interfaces over time.

8. When attackers inject malicious scripts into web pages by bypassing client security mechanisms, what attack are they employing?

A. Cross-site scripting

B. Cookie snooping

C. SQL injection

D. Unvalidated input

The attack being described is known as Cross-site Scripting (XSS). This type of attack occurs when an attacker is able to inject malicious scripts into content that is served to users in a web application. The injected script typically runs in the context of the user's browser, executing actions that can compromise user data, hijack sessions, or redirect users to potentially harmful sites. In the context of bypassing client security mechanisms, XSS exploits vulnerabilities in the way a web application processes user input and reflects it back to clients without sufficient validation or sanitization. Attackers can craft malicious payloads that, when executed by unsuspecting users, may manipulate the webpage or steal information. The other options describe different types of security issues or attacks. Cookie snooping refers to unauthorized access to web session cookies, which can lead to session hijacking but does not specifically involve script injection. SQL injection targets databases by inserting or "injecting" malicious SQL queries into a web application, which is a different attack vector altogether. Unvalidated input refers to the general concept of failing to properly validate user input, which can lead to various vulnerabilities including XSS, but it does not specifically define the method of injecting scripts into web pages.

9. In which attack does an authenticated user unknowingly perform tasks for an attacker?

A. Cross-site request forgery

B. SQL injection

C. Authentication hijacking

D. Unvalidated forwarding

Cross-site request forgery (CSRF) involves an authenticated user unknowingly executing actions on behalf of an attacker without their consent. This occurs when a user, while logged into a web application, is tricked into performing requests that benefit the attacker, such as changing account settings or initiating transactions. The attack leverages the user's active session and trust in the web application, as the requests do not require the attacker to directly compromise the user's credentials. In contrast, SQL injection targets the database behind a web application by sending malicious SQL statements to manipulate data. Authentication hijacking focuses on taking over an active session by stealing session tokens, allowing attackers to act as legitimate users without the need for the user's participation. Unvalidated forwarding refers to a flaw whereby users are redirected to untrusted sites without proper validation, posing risks but not necessarily involving the user performing tasks for an attacker. CSRF specifically highlights the scenario of user involvement in an unintended action, making it the correct answer.

10. Which user-created evidence source can help in analyzing malicious links or URLs?

A. Email history

B. Internet bookmarks

C. Browser cache

D. Download history

Internet bookmarks serve as valuable user-created evidence sources in the analysis of malicious links or URLs for several reasons. Bookmarks are often saved by users when they encounter websites they find interesting or useful, and they can provide insight into what sites the user regularly accesses. When examining bookmarks in a forensic investigation, analysts can identify URLs that may lead to malicious content. Users may accidentally bookmark a harmful site, or they may store links to phishing sites, which can be critical in understanding user behavior and potential security breaches. Moreover, the presence of specific bookmarks can help establish a timeline of user activity, indicating when a user may have been exposed to malicious content. While email history can provide information about links sent via email, browser cache can reveal URLs accessed but may not always clearly indicate user intent. Similarly, download history may show files obtained from malicious sites but does not necessarily point directly to the URLs themselves. Therefore, internet bookmarks offer a clear and direct indication of user engagement with various web resources, making them particularly useful in analyzing malicious links.

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://digitalforensic.examzify.com

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