GIAC FOUNDATIONAL CYBERSECURITY TECHNOLOGIES PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://gfact.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 of the following is not a type of malware?

A. Virus

B. Spyware

C. Firewall

D. Trojan horse

2. What could occur as a result of a successful Directory Traversal attack?

A. Improved application performance

B. Unlimited access to the server's filesystem

C. A reduction in web traffic

D. Increased data integrity

3. What type of exploit allows an attacker to execute arbitrary code remotely, as described in CVE-2019-9874?

A. Remote Code Execution (RCE)

B. Heap corruption

C. Information disclosure

D. Buffer over-read

4. What is the best way to defend against a Directory Traversal attack?

A. Regularly update software

B. Limit user input during system calls

C. Utilize complex passwords

D. Enable multifactor authentication

5. In the context of web application security, what role do tokens play?

A. They authenticate users every session

B. They secure sensitive information during transfer

C. They prevent CSRF by providing unique identifiers

D. They track user behavior for analytics

6. What can an Apache server administrator do to prevent version information from leaking?

A. Run Apache as a non-root user

B. Enable HTTPS

C. Set permission on /var/www/html to 700

D. Disable the banner

7. Which of the following is a likely source of logs for HTTP network traffic data?

A. Layer 2 switch

B. Firewall

C. DNS Server

D. Active Directory Server

8. A GIAC administrator has configured their company's web server with X-Frame-Options. What attack is being addressed?

A. SQL injection

B. Cross-Site request forgery

C. Cross-Site scripting

D. Clickjacking

9. What role does user input sanitization play in web security?

A. It improves user experience on the website

B. It prevents unauthorized access to system files

C. It protects against Cross Site Scripting vulnerabilities

D. It facilitates faster database queries

10. A Red Team would use the following command for which purpose? # nmap -vv -sS -p- 10.10.1.1

A. Identifying open ports that could be used to compromise a host

B. Determining updates needed for the host's asset inventory record

C. Identifying unauthorized open ports to disable on the host

D. Determining version information for services running on the host

Answers

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

Explanations

1. Which of the following is not a type of malware?

A. Virus

B. Spyware

C. Firewall

D. Trojan horse

The choice identified as correct is indeed the appropriate selection as it highlights that a firewall is not a type of malware. A firewall serves as a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its primary function is to protect systems from unauthorized access and threats, distinguishing it fundamentally from malware, which is designed to harm, exploit, or otherwise compromise systems. In contrast, a virus, spyware, and a Trojan horse all fall under the category of malware. A virus is a self-replicating program that attaches itself to clean files and spreads throughout a computer system. Spyware collects personal information without users' knowledge, often serving the purpose of financial theft or identity fraud. A Trojan horse disguises itself as legitimate software but, when executed, can cause harm or grant unauthorized access to attackers.Therefore, recognizing these differences helps to clarify the nature of firewalls as protective measures rather than harmful entities like malware.

2. What could occur as a result of a successful Directory Traversal attack?

A. Improved application performance

B. Unlimited access to the server's filesystem

C. A reduction in web traffic

D. Increased data integrity

A successful Directory Traversal attack allows an attacker to manipulate the URL or input parameters in such a way that they can navigate outside the intended directories of a web application. By exploiting this vulnerability, the attacker gains the ability to access restricted areas of the server's filesystem, thereby achieving unlimited access to the server's filesystem. This means that the attacker could potentially view, modify, or download sensitive files that should not be accessible to unauthorized users, including configuration files, user data, and other critical resources. This type of attack is particularly concerning because it can lead to further exploitation of the server or application, as the attacker may then gain more information about the server's structure, access sensitive data, or install malicious software. Therefore, the risk posed by a successful Directory Traversal attack should be treated with a high level of urgency in cybersecurity practices.

3. What type of exploit allows an attacker to execute arbitrary code remotely, as described in CVE-2019-9874?

A. Remote Code Execution (RCE)

B. Heap corruption

C. Information disclosure

D. Buffer over-read

The reason Remote Code Execution (RCE) is the correct answer is that it specifically refers to the ability of an attacker to execute arbitrary code on a target system from a remote location. In the context of CVE-2019-9874, this vulnerability is characterized by an attacker exploiting a flaw to run their own malicious code without requiring direct access to the victim's machine. RCE vulnerabilities are particularly severe because they allow attackers to take control of systems, steal sensitive information, or even disrupt services. The other options do not apply to this scenario. Heap corruption involves issues with memory management that can lead to various security problems but does not inherently imply the execution of arbitrary code by an attacker. Information disclosure refers to vulnerabilities that expose sensitive data without necessarily allowing code execution. Buffer over-read entails reading more data than allocated, which could result in sensitive information being exposed but does not allow for arbitrary code execution like an RCE does. Thus, the key aspect of RCE is the ability to execute malicious code remotely, making it the most fitting classification for the exploit in question.

4. What is the best way to defend against a Directory Traversal attack?

A. Regularly update software

B. Limit user input during system calls

C. Utilize complex passwords

D. Enable multifactor authentication

Defending against a Directory Traversal attack primarily involves limiting user input during system calls. A Directory Traversal attack enables an attacker to access files and directories that are stored outside the intended directory. This typically occurs when an application takes user inputs, such as file path requests, and does not properly validate or sanitize those inputs. By limiting the type and format of user input—like implementing strict validation checks and ensuring that only legitimate, expected input is processed—systems can prevent unauthorized access to sensitive files. Regularly updating software is essential for overall security hygiene, but it does not specifically address the vulnerability related to Directory Traversal attacks. While complex passwords and multifactor authentication are vital components of access control and protection against unauthorized access, they do not directly mitigate the specific risks posed by Directory Traversal. Thus, focusing on user input is the most effective strategy for preventing such attacks.

5. In the context of web application security, what role do tokens play?

A. They authenticate users every session

B. They secure sensitive information during transfer

C. They prevent CSRF by providing unique identifiers

D. They track user behavior for analytics

Tokens play a critical role in preventing Cross-Site Request Forgery (CSRF) attacks by providing unique identifiers that ensure the authenticity of requests made by a user. CSRF is a type of attack that tricks the user into executing unwanted actions on a web application where they are authenticated. When a user logs into a web application, a token is generated and stored, often within the user's session. This token is then included in each request made to the server. The server checks for the authenticity of the received token against what it has stored. If the token is valid, the request is processed; if not, it is rejected. Having this unique identifier ensures that only requests originating from the legitimate user are processed, effectively mitigating CSRF vulnerabilities. Tracking user behavior for analytics or securing sensitive information during transfer may utilize tokens in some capacity, but they are not the primary function of tokens in the context of web application security. Similarly, while tokens may be used in authentication processes, their direct implication in session-based authentication does not specifically address their role in CSRF prevention as accurately as the correct choice does.

6. What can an Apache server administrator do to prevent version information from leaking?

A. Run Apache as a non-root user

B. Enable HTTPS

C. Set permission on /var/www/html to 700

D. Disable the banner

To prevent version information from leaking from an Apache server, disabling the banner is the most effective method. The "banner" in this context refers to the HTTP response headers that can disclose server version details, which could be exploited by attackers looking for specific vulnerabilities associated with that version. By disabling the server signature and server tokens, the administrator can hide this information, thereby making it more difficult for an attacker to gather intelligence about the server's configuration and potential weaknesses. While running Apache as a non-root user, enabling HTTPS, and setting strict permissions on the web directory are all important security practices, they do not specifically address the issue of version information leakage. Running as a non-root user limits the potential damage an attacker can cause if they gain access, HTTPS secures the data in transit, and setting directory permissions protects file access. However, these actions do not directly manage the visibility of version details that could inform a malicious actor about vulnerabilities in the server software. Thus, the action of disabling the banner is targeted specifically at mitigating this risk.

7. Which of the following is a likely source of logs for HTTP network traffic data?

A. Layer 2 switch

B. Firewall

C. DNS Server

D. Active Directory Server

The selection of a firewall as a likely source of logs for HTTP network traffic data is appropriate as firewalls are specifically designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. They often maintain logs that capture data about HTTP requests and responses, including details like source and destination IP addresses, ports, and protocols used, which are critical for understanding web traffic patterns and identifying potential security threats. A firewall inspects the content of the HTTP traffic, providing insights into which websites are being accessed and which users are generating that traffic. This capability makes firewalls an integral part of network security, as they help in detecting and logging suspicious activities that could indicate malicious behavior, such as unauthorized access attempts or data exfiltration. In contrast, the other options do not serve primarily as sources of HTTP traffic logging. A Layer 2 switch primarily operates at the data link layer, managing data frames and does not log the higher-level protocols such as HTTP. A DNS Server is focused on resolving domain names to IP addresses, not tracking HTTP traffic directly. Similarly, an Active Directory Server primarily handles authentication and directory services and does not log HTTP traffic as part of its core functions. Hence, firewalls stand out as the most relevant source for HTTP network traffic

8. A GIAC administrator has configured their company's web server with X-Frame-Options. What attack is being addressed?

A. SQL injection

B. Cross-Site request forgery

C. Cross-Site scripting

D. Clickjacking

The correct answer is addressing the Clickjacking attack because the X-Frame-Options header is specifically designed to mitigate this type of vulnerability. Clickjacking occurs when an attacker tricks a user into clicking on something different from what the user perceives, effectively hijacking the click actions. By including the X-Frame-Options in the HTTP response headers, the web server informs the browser whether or not it is permitted to display the content in a frame or iframe. When configured correctly, X-Frame-Options can prevent the webpage from being loaded within a frame on another site, thereby thwarting attempts at clickjacking. This enhances user security by ensuring that malicious websites cannot overlay their content on top of legitimate interfaces, which could deceive users into performing unintended actions. Other options refer to different types of attacks that are not directly addressed by X-Frame-Options. For instance, SQL injection involves manipulating a server's database through malicious input, Cross-Site Request Forgery exploits the trust that a site has in a user's browser, and Cross-Site Scripting allows attackers to inject malicious scripts into web pages. Therefore, X-Frame-Options is specifically relevant to preventing Clickjacking.

9. What role does user input sanitization play in web security?

A. It improves user experience on the website

B. It prevents unauthorized access to system files

C. It protects against Cross Site Scripting vulnerabilities

D. It facilitates faster database queries

User input sanitization plays a critical role in web security by specifically protecting against Cross Site Scripting (XSS) vulnerabilities. XSS attacks occur when an attacker is able to inject malicious scripts into a web application through user input fields, which can then be executed in the context of another user's browser. When user input is not properly sanitized, it can allow an attacker to introduce scripts that can manipulate or steal sensitive information, such as session cookies or user credentials. By implementing effective sanitization measures on user input, developers can ensure that any special characters or potentially harmful code are stripped or encoded before they are processed by the web application. This minimizes the risk of executing unintended commands and safeguards users' data and privacy. In essence, proper sanitization transforms potentially dangerous input into harmless text, thereby thwarting XSS attempts and enhancing overall web security. While user experience, unauthorized access prevention, and database query performance are important considerations in web development, they do not directly address the specific vulnerabilities posed by XSS as effectively as user input sanitization does.

10. A Red Team would use the following command for which purpose? # nmap -vv -sS -p- 10.10.1.1

A. Identifying open ports that could be used to compromise a host

B. Determining updates needed for the host's asset inventory record

C. Identifying unauthorized open ports to disable on the host

D. Determining version information for services running on the host

The command provided utilizes Nmap, a well-known network scanning tool, which is particularly effective for identifying open ports on a target host. The specific flags in the command have distinct purposes: - The `-vv` option enables verbose mode, providing more detailed output about the scan's progress and results. - The `-sS` option indicates a stealth SYN scan, which is a common technique used to detect open ports without establishing a full TCP connection, thus minimizing detection by the target. - The `-p-` option specifies to scan all 65535 TCP ports, rather than just the common ones, ensuring a comprehensive assessment. Given this context, the primary purpose of running this command is to identify open ports on the host at the specified IP address (10.10.1.1). Open ports can be potential entry points for attackers, providing opportunities to exploit vulnerabilities in running services. Therefore, the command is fundamentally about reconnaissance to discover which ports are accessible and could potentially be used to compromise the host.

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://gfact.examzify.com

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