Ethical Hacking Essentials Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

This is a sample study guide. To access the full version with hundreds of questions,

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

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. Don’t worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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 wireless standard prioritizes data, voice, and video transmissions to improve Quality of Service (QoS)?**

   A. 802.11n

   B. 802.11e

   C. 802.11ac

   D. 802.15

2. **What is the primary goal of ARP poisoning?**

   A. To disrupt DNS queries

   B. To overburden a network switch

   C. To intercept communications between devices

   D. To hijack DHCP leases

3. **Which countermeasure helps secure a database against SQL injection attacks?**

   A. Avoid constructing dynamic SQL with concatenated input values

   B. Use static SQL queries

   C. Implement user authentication

   D. Encrypt all database fields

4. **What is the name of the U.S. government repository that focuses on standards-based vulnerability management data?**

   A. Common Vulnerabilities and Exposures (CVE)

   B. National Vulnerability Database (NVD)

   C. Open Web Application Security Project (OWASP)

   D. Security Content Automation Protocol (SCAP)

5. **Which of the following is NOT a function of Wireshark?**

   A. Network troubleshooting

   B. Password cracking

   C. Packet analysis

   D. Communications protocol development

6. In which phase of the cyber kill chain does an adversary distribute USB drives with malicious payloads?

A. Reconnaissance

B. Delivery

C. Exploitation

D. Action on objectives

7. What countermeasure assists in defending against SQL injection attacks?

A. Run services with full rights

B. Run a database service account with minimal rights

C. Utilize a VPN

D. Regularly change database passwords

8. What type of attack involves capturing packets over a network to retrieve sensitive information like usernames and passwords?

A. Interception attack

B. Wiretapping

C. SQL injection

D. Cross-site request forgery

9. Which tool is best known as a brute force password cracker?

A. Wireshark

B. Burp Suite

C. Medusa

D. HashCat

10. Which attack technique would involve spoofing an ID to gain unauthorized access to a secure location?

A. Tailgating

B. Vishing

C. Social engineering

D. Phishing

Answers

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

Explanations

1. Which wireless standard prioritizes data, voice, and video transmissions to improve Quality of Service (QoS)?

A. 802.11n

B. 802.11e

C. 802.11ac

D. 802.15

The wireless standard that prioritizes data, voice, and video transmissions to improve Quality of Service (QoS) is 802.11e. This standard introduces mechanisms for differentiating traffic types and managing their bandwidth to ensure that time-sensitive data, like voice and video calls, receive the priority they need for optimal performance. One of the key features brought by 802.11e is the Enhanced Distributed Channel Access (EDCA), which establishes various access categories for traffic, allowing for better management of congestion and reducing latency for real-time applications. This prioritization is essential in environments where multiple types of data are being transmitted simultaneously, as it helps maintain a consistent quality of experience for users. The other standards mentioned do not specifically focus on QoS improvement through traffic prioritization in the same manner. For example, 802.11n and 802.11ac primarily enhance data throughput and overall network performance rather than explicitly addressing QoS features. Meanwhile, 802.15 refers to wireless personal area networks, which are designed for different applications and do not prioritize traffic in the same way as 802.11e.

2. What is the primary goal of ARP poisoning?

A. To disrupt DNS queries

B. To overburden a network switch

C. To intercept communications between devices

D. To hijack DHCP leases

The primary goal of ARP poisoning is to intercept communications between devices on a local area network. ARP, or Address Resolution Protocol, is used to map IP addresses to MAC addresses, allowing devices to communicate with each other over a network. In ARP poisoning, an attacker sends falsified ARP messages onto the network. These messages associate the attacker's MAC address with the IP address of a legitimate device, effectively tricking devices into sending their traffic to the attacker instead of the intended recipient. This interception enables the attacker to monitor, modify, or disrupt the communications between the devices, leading to potential data breaches or further exploits. Understanding this attack is crucial in ethical hacking and network security as it highlights the importance of network monitoring and protected ARP mechanisms to safeguard against such tactics. In relation to the other options, while DNS disruption, network switch overloading, and DHCP lease hijacking are all forms of attacks in network exploitation, they do not directly relate to the specific mechanics and objectives of ARP poisoning, which revolves exclusively around manipulating the ARP protocol for intercepting data.

3. Which countermeasure helps secure a database against SQL injection attacks?

A. Avoid constructing dynamic SQL with concatenated input values

B. Use static SQL queries

C. Implement user authentication

D. Encrypt all database fields

The recommended countermeasure to secure a database against SQL injection attacks is to avoid constructing dynamic SQL with concatenated input values. SQL injection occurs when an attacker is able to manipulate a SQL query by injecting malicious input, which can happen particularly when user inputs are concatenated directly into SQL statements. By avoiding dynamic SQL, which often involves directly embedding user input within a query string, the risk of injection is mitigated. In contrast, using static SQL queries may enhance security, but it is not a standalone solution. Static queries can still be vulnerable if not implemented correctly. While implementing user authentication adds an important layer of security to protect access to the database, it does not directly prevent SQL injection vulnerabilities from occurring. Similarly, encrypting all database fields is related to data security but does not address the primary vector through which SQL injection attacks occur, which is the construction of the SQL query itself. Hence, focusing on the construction of SQL queries is pivotal in protecting against SQL injection attacks.

4. What is the name of the U.S. government repository that focuses on standards-based vulnerability management data?

A. Common Vulnerabilities and Exposures (CVE)

B. National Vulnerability Database (NVD)

C. Open Web Application Security Project (OWASP)

D. Security Content Automation Protocol (SCAP)

The National Vulnerability Database (NVD) serves as a comprehensive U.S. government repository dedicated to standards-based vulnerability management data. It provides a wealth of information regarding vulnerabilities, including the CVE Identifiers for each entry. The NVD enhances the visibility of potential security weaknesses in software and firmware, making it an essential resource for security professionals. The NVD presents data in a structured format, which allows organizations to assess the impact and severity of vulnerabilities, prioritize remediation efforts, and ensure compliance with security standards. It builds on the CVE list by offering additional metadata, which includes references, fix information, and scoring metrics that inform vulnerability management processes. In contrast, Common Vulnerabilities and Exposures (CVE) is a standardized list of publicly documented cybersecurity vulnerabilities and exposures, but it does not serve as a comprehensive repository as the NVD does. Open Web Application Security Project (OWASP) focuses on improving the security of software through community-driven initiatives and best practices rather than vulnerability management data. The Security Content Automation Protocol (SCAP) is a framework used for automated vulnerability management but does not act as a repository itself. Thus, the National Vulnerability Database is the most relevant and accurate choice when it comes to a repository for standards-based vulnerability

5. Which of the following is NOT a function of Wireshark?

A. Network troubleshooting

B. Password cracking

C. Packet analysis

D. Communications protocol development

Wireshark is a powerful tool primarily utilized for network protocol analysis, capturing packets, and providing insights into network traffic. It serves numerous important functions that are essential for network administrators, cybersecurity professionals, and developers. Network troubleshooting is one of the core functions of Wireshark, as it allows users to analyze packet data to identify network issues, monitor performance, and diagnose problems. Packet analysis is another key capability, enabling users to inspect individual packets in detail to understand the flow of data across the network. Moreover, Wireshark is valuable in communications protocol development because it lets developers view the actual data being sent over the network, providing a clear picture of how protocols perform and allowing for debugging and improvements. In contrast, password cracking is not a function of Wireshark. While the tool can capture packets that may include password transmissions, it does not have built-in functionality for cracking passwords. Password cracking typically involves other specialized tools focused specifically on breaking encryption or hashes, which is outside the scope and purpose of Wireshark. Thus, identifying Wireshark's non-function aligns with understanding its capabilities and limitations.

6. In which phase of the cyber kill chain does an adversary distribute USB drives with malicious payloads?

A. Reconnaissance

B. Delivery

C. Exploitation

D. Action on objectives

The correct choice is associated with the phase in which an adversary actively transmits or sends malicious content to the target. The Delivery phase involves the transfer of the payload—such as malware—onto a target environment. In this context, distributing USB drives containing malicious payloads is a tactic employed during this phase. The USB drives serve as the medium for delivery, allowing the adversary to reach potential victims directly. This activity aims to successfully convey the malicious content to the target, which can lead to subsequent exploitation once the drive is connected to a computer system. Understanding this phase is crucial because it highlights how attackers leverage physical means, like USB drives, to facilitate attacks, illustrating the diverse methodologies used in cyber threats.

7. What countermeasure assists in defending against SQL injection attacks?

A. Run services with full rights

B. Run a database service account with minimal rights

C. Utilize a VPN

D. Regularly change database passwords

Running a database service account with minimal rights is an effective countermeasure against SQL injection attacks because it limits the potential damage an attacker can cause if they successfully exploit a vulnerability. When a database service operates under a set of minimal privileges, even if an attacker injects malicious SQL code, their access is restricted, preventing them from executing harmful operations such as deleting tables or accessing sensitive data. By employing the principle of least privilege, the service account only has the necessary rights to perform its required tasks. This reduces the attack surface, making it more difficult for malicious actors to gain escalated access to the database's resources. In contrast, running services with full rights exposes the system to greater risk. A VPN provides secure access over the internet, but it does not directly mitigate the risk associated with SQL injection. Regularly changing database passwords can enhance security but does not address the fundamental weaknesses in application code that allow SQL injection to occur in the first place. Therefore, utilizing a database service account with minimal rights stands out as a proactive defense mechanism against potential SQL injection attacks.

8. What type of attack involves capturing packets over a network to retrieve sensitive information like usernames and passwords?

A. Interception attack

B. Wiretapping

C. SQL injection

D. Cross-site request forgery

The correct choice captures the essence of network vulnerabilities where sensitive data can be intercepted. Wiretapping refers to the unauthorized interception of communications, typically involving the monitoring of data packets as they travel across a network. This method allows an attacker to gain access to sensitive information such as usernames and passwords by “listening in” on the data traffic. In contrast, the other options describe different types of attacks. Interception attacks cover a broad category that may include various methods but are not specifically focused on the act of monitoring communications as wiretapping is. SQL injection involves exploiting vulnerabilities in a database layer by injecting malicious SQL code, which is unrelated to capturing network packets. Cross-site request forgery is a technique that tricks a user into executing unwanted actions on a web application in which they are authenticated, which has no direct correlation with packet capture. Hence, wiretapping is specifically aligned with the act of capturing packets over a network to retrieve sensitive information.

9. Which tool is best known as a brute force password cracker?

A. Wireshark

B. Burp Suite

C. Medusa

D. HashCat

The tool known for its capabilities as a brute force password cracker is Medusa. Medusa is specifically designed for speed and parallelism in cracking passwords across various protocols, making it effective for brute force attacks. It utilizes multiple threads, allowing it to attempt numerous password combinations simultaneously, which significantly reduces the time it takes to crack passwords. While both Wireshark and Burp Suite are powerful tools in the realm of network security and ethical hacking, they serve different functions. Wireshark is primarily a network packet analyzer used for network troubleshooting and monitoring, while Burp Suite is mainly focused on web application security testing, including penetration testing but not specifically password cracking. HashCat, while not the correct answer in this instance, is also a well-known password recovery tool that specializes in cracking password hashes rather than performing brute force attacks on live systems. It utilizes the processing power of both CPUs and GPUs to recover passwords and is particularly effective for hash-based attacks. In summary, Medusa stands out for its brute force capabilities and efficiency in tackling password cracking tasks across various protocols, making it the most appropriate choice for this question.

10. Which attack technique would involve spoofing an ID to gain unauthorized access to a secure location?

A. Tailgating

B. Vishing

C. Social engineering

D. Phishing

Tailgating is a physical security breach technique where an unauthorized individual follows an authorized person into a restricted area. This often involves mimicking the authorized user’s behavior, which could include spoofing an ID, to gain access to secure locations. The technique relies on the trust that authorized personnel may inadvertently place in that individual, allowing them to enter areas without proper clearance. This method of attack exploits human trust and the often lax enforcement of physical access controls, making it particularly effective in environments where employees are accustomed to holding doors open for others. By entering behind a legitimate credential holder, the attacker can bypass security measures that would otherwise prevent unauthorized access. In contrast, the other techniques listed—such as vishing, social engineering, and phishing—are primarily focused on digital or psychological manipulation rather than physical entry. Vishing relates to voice phishing targeting individuals over the phone; social engineering encompasses a broader range of manipulative tactics to deceive individuals; and phishing typically involves deceitful emails or messages aimed at acquiring sensitive information. While these methods can certainly be part of an overall security threat, they do not specifically involve the physical act of gaining unauthorized access to secure areas through spoofing an ID.

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://ethicalhackingessentials.examzify.com

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