Certified Ethical Hacker (CEH) Practice Exam (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 encryption standard is known for being faster than the others mentioned?**

    A. International Data Encryption Standard (IDEA)

    B. Digital Encryption Standard (DES)

    C. Triple Data Encryption Standard (3DES)

    D. Advanced Encryption Standard (AES)

2. **In which year was the Computer Fraud and Abuse Act enacted?**

    A. 1984

    B. 1990

    C. 1996

    D. 2001

3. **What do application-level attacks focus on?**

    A. Network security protocols

    B. Underlying hardware vulnerabilities

    C. Programming codes of an application

    D. User authentication processes

4. **Which of the following is a component of the SOA record?**

    A. IP Address

    B. Source Host

    C. Domain Name

    D. DNSSEC Key

5. **During which phase do security professionals apply tools and techniques to gather in-depth information?**

    A. Gaining Access

    B. Covering Tracks

    C. Scanning and Enumeration

    D. Reconnaissance

6. What is the primary function of the Secure Hash Algorithm 1 (SHA-1)?

A. To develop secure digital certificates

B. To produce a 160-bit hash

C. To create symmetric encryption keys

D. To manage certificate revocation lists

7. What is a cracker in cybersecurity terms?

A. A security expert focused on data protection

B. A hacker who violates security for personal gain

C. An ethical hacker performing risk assessments

D. A user authorized to manipulate data

8. In the context of risk management, what is a vulnerability?

A. An attack that targets systems

B. A potential source of harm

C. A weakness that can be exploited

D. A valuable asset

9. Which command is used to test a DNS query and report back the results in Unix-based systems?

A. nslookup

B. dig

C. ping

D. traceroute

10. What challenges does the RIPE NCC primarily address?

A. Network configuration

B. Internet number resource registration

C. Website domain management

D. Data loss prevention

Answers

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

Explanations

1. Which encryption standard is known for being faster than the others mentioned?

A. International Data Encryption Standard (IDEA)

B. Digital Encryption Standard (DES)

C. Triple Data Encryption Standard (3DES)

D. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is recognized for its speed and efficiency compared to other encryption methods. AES utilizes a symmetric key encryption algorithm, meaning that the same key is used for both encryption and decryption. Its design allows it to take advantage of modern computer architecture, making it significantly faster in both software and hardware implementations. One of the key features that contribute to the speed of AES is its block size and key lengths, which can be 128, 192, or 256 bits. This flexibility allows it to be efficiently processed in parallel, enabling quicker encryption and decryption processes. Additionally, AES employs a simpler structure with fewer rounds compared to Triple DES, which adds to its performance advantages. On the other hand, although IDEA and DES were widely used in the past, they are slower and less efficient due to their older design and larger computational requirements. 3DES, while an improvement over single DES, still encrypts data in multiple passes, making it slower than AES. Thus, AES stands out as the fastest of the encryption standards, making it the choice for many modern applications that require both security and speed.

2. In which year was the Computer Fraud and Abuse Act enacted?

A. 1984

B. 1990

C. 1996

D. 2001

The Computer Fraud and Abuse Act (CFAA) was enacted in 1984. This legislation was established to address computer-related offenses, particularly those involving fraud and unauthorized access to computer systems. It was one of the first federal laws to address the growing concern of computer crimes, which were becoming more prevalent with the increase in computer usage and dependence. The Act has undergone several amendments since its initial passage, reflecting the evolving nature of technology and cybercrime. The original intent was to provide law enforcement with the tools necessary to combat unauthorized access to computers and protect sensitive data, laying the groundwork for more comprehensive legislation in the years that followed. Understanding the CFAA and its historical context is crucial for anyone studying cybersecurity and ethical hacking, as it is foundational in shaping current laws and regulations that govern computer use and security.

3. What do application-level attacks focus on?

A. Network security protocols

B. Underlying hardware vulnerabilities

C. Programming codes of an application

D. User authentication processes

Application-level attacks primarily target the programming codes of an application. These types of attacks exploit vulnerabilities found within the application’s software itself, which could arise from coding errors, improper input validation, or business logic flaws. Attackers aim to manipulate the application in ways that it was not designed for, potentially leading to unauthorized access, data breaches, or denial of service. Focusing on the underlying programming allows attackers to carry out specific actions such as SQL injection, cross-site scripting (XSS), or buffer overflow attacks, which can compromise the integrity, confidentiality, or availability of the application and the data it processes. The other choices do not align with the primary focus of application-level attacks. Network security protocols pertain to the defense mechanisms in place for network security rather than vulnerabilities in application coding. Underlying hardware vulnerabilities are more related to physical device weaknesses rather than the software code itself. User authentication processes involve securing access controls within an application but are not the main target of application-level attacks, which center more on the application’s programming rather than its authentication mechanisms.

4. Which of the following is a component of the SOA record?

A. IP Address

B. Source Host

C. Domain Name

D. DNSSEC Key

The Start of Authority (SOA) record is a crucial component of the Domain Name System (DNS). It defines certain parameters for a domain and indicates which DNS server is the authoritative source for that domain's DNS records.   An SOA record typically contains several fields, including the primary authoritative name server for the domain, the email address of the domain administrator, various timers relating to refreshing the zone, and a serial number that helps with the versioning of the zone file. However, it does not include fields such as a source host or other elements related to specific IP addresses. When considering the choices, the one that is part of the SOA record is indeed the DNSSEC Key, as this relates to the cryptographic security practices surrounding DNS, though it may not be present in older implementations since it's a relatively newer addition. The fundamental attributes of an SOA record are critical for DNS operations and are necessary for maintaining authoritative records. The selection of "Source Host" as part of the SOA record is not accurate, as it doesn't align with what elements are actually found within that record.   This understanding clarifies the structure and significance of SOA records in the DNS hierarchy, along with their role in ensuring the consistency and reliability of domain data

5. During which phase do security professionals apply tools and techniques to gather in-depth information?

A. Gaining Access

B. Covering Tracks

C. Scanning and Enumeration

D. Reconnaissance

The correct answer is the phase referred to as Reconnaissance. During this initial phase, security professionals focus on collecting extensive information about the target, which can include details about systems, networks, and potential vulnerabilities. This can involve various techniques like passive reconnaissance, where publicly available information is gathered, or active reconnaissance, which may involve probing the target's network to uncover specific details. The goal of this phase is to create a comprehensive profile of the target, which can significantly inform subsequent phases like Scanning and Enumeration. In contrast, while Scanning and Enumeration do involve the application of tools and techniques, they are typically used after initial reconnaissance has provided foundational knowledge about the target. This means that Scanning and Enumeration build upon the insights gained during the Reconnaissance phase rather than serve as a primary means of gathering in-depth information.

6. What is the primary function of the Secure Hash Algorithm 1 (SHA-1)?

A. To develop secure digital certificates

B. To produce a 160-bit hash

C. To create symmetric encryption keys

D. To manage certificate revocation lists

The primary function of the Secure Hash Algorithm 1 (SHA-1) is to produce a 160-bit hash. This algorithm takes an input message and generates a fixed-size string of text that appears random. This output, known as a hash or digest, uniquely represents the data input, making it useful for verifying data integrity and ensuring that even the slightest change in the input will yield a significantly different hash. SHA-1 is widely used in various security applications and protocols, including TLS (Transport Layer Security) and digital signatures. Its ability to create a unique and fixed-length hash helps in ensuring that original data can be verified without needing to check the entire dataset, thus providing a way to detect alterations or errors. While developing digital certificates, creating symmetric encryption keys, and managing certificate revocation lists are important components of cryptographic systems, they do not specifically relate to the purpose of SHA-1. The focus of SHA-1 is purely on hashing, making option B the most accurate representation of its primary function.

7. What is a cracker in cybersecurity terms?

A. A security expert focused on data protection

B. A hacker who violates security for personal gain

C. An ethical hacker performing risk assessments

D. A user authorized to manipulate data

In the context of cybersecurity, a cracker is specifically defined as a hacker who breaks into computer systems or networks, primarily for personal gain. This can involve activities such as stealing sensitive information, deploying malware, or otherwise compromising the integrity and confidentiality of data. Crackers operate outside ethical boundaries, contrasting sharply with ethical hackers and security professionals who aim to protect and secure systems. The other choices highlight different roles within the cybersecurity landscape. A security expert dedicated to data protection emphasizes safeguarding systems rather than breaking into them. An ethical hacker, by definition, conducts authorized testing and risk assessments to improve security measures, reflecting a fundamentally different purpose than that of a cracker. Lastly, a user authorized to manipulate data acts within defined permissions and responsibilities, which aligns with accepted practices rather than illicit activities. Thus, the characterization of a cracker as someone violating security for personal gain is accurate in capturing the essence of this malicious role in cybersecurity.

8. In the context of risk management, what is a vulnerability?

A. An attack that targets systems

B. A potential source of harm

C. A weakness that can be exploited

D. A valuable asset

A vulnerability refers to a weakness in a system, network, or application that can be exploited by threats to gain unauthorized access or cause harm. In the context of risk management, identifying and mitigating vulnerabilities is crucial for protecting organizational assets against potential attacks. When a system has a vulnerability, it could be a flaw in the software code, misconfiguration, or any other aspect that could be taken advantage of by an attacker. By recognizing these weaknesses, security professionals can implement measures to strengthen the system and reduce the likelihood of a successful exploit. The other options relate to different concepts in risk management. An attack is a deliberate action taken to exploit a vulnerability; a potential source of harm is typically referred to as a threat; and a valuable asset refers to important data or resources that need protection but does not directly define what a vulnerability is. Understanding the distinction between these concepts is key to effective risk analysis and mitigation strategies.

9. Which command is used to test a DNS query and report back the results in Unix-based systems?

A. nslookup

B. dig

C. ping

D. traceroute

The command used to test a DNS query and report back the results in Unix-based systems is 'dig'. This command, which stands for "domain information groper," is specifically designed to retrieve DNS information, allowing users to query DNS records for a given domain. It provides a detailed output, showing various types of DNS records such as A, AAAA, MX, and TXT, among others. 'Dig' is favored by network administrators and security professionals because it offers more flexibility and provides additional options for troubleshooting and analyzing DNS issues compared to other commands. For instance, it can be tailored to perform specific types of queries or to query different DNS servers. In contrast, while 'nslookup' is another command used for checking DNS information, it is generally less powerful and less versatile than 'dig'. The 'ping' command is primarily used to test network connectivity rather than to query DNS records, and 'traceroute' is intended for analyzing the path packets take through a network, making it unrelated to DNS queries.

10. What challenges does the RIPE NCC primarily address?

A. Network configuration

B. Internet number resource registration

C. Website domain management

D. Data loss prevention

The RIPE NCC, which stands for Réseaux IP Européens Network Coordination Centre, primarily addresses the challenge of internet number resource registration. This entails managing and distributing Internet Protocol (IP) addresses and Autonomous System Numbers (ASNs) within its service region, which is primarily Europe, the Middle East, and parts of Central Asia. The RIPE NCC plays a critical role in ensuring that IP addresses are allocated efficiently and in compliance with established policies to maintain the stability and functionality of the internet. The organization also provides support for Internet resource management through various services, including maintaining a public database that provides information about IP address and ASN allocations. This is crucial for network operators, researchers, and policy makers, as it helps to prevent issues such as address conflicts and enables better coordination in network management. The aspects addressed by the other options do not align with the primary objectives of the RIPE NCC. While network configuration, website domain management, and data loss prevention are significant technical challenges in the internet ecosystem, they fall outside the specific domain of resource registration that the RIPE NCC specializes in. By focusing on internet number resource registration, the RIPE NCC ensures a foundational aspect of internet infrastructure, which is vital for operational integrity and sustainability.

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://ceh.examzify.com

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