Certified Ethical Hacker (CEH) Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

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 RIR responsible for Asia?

A. AFRINIC

B. LACNIC

C. APNIC

D. RIPE NCC

2. What is a hash in the context of data security?

A. Two-way encryption algorithm

B. A mathematical function that generates a fixed-length number

C. A form of key for data access

D. A method of data transmission

3. What is the main task of an Address (A) Record in DNS?

A. Translate email addresses to usernames

B. Identify the authoritative nameserver for a domain

C. Map a hostname to its corresponding IP address

D. Provide aliases for subdomains

4. Which of the following is NOT a function of DNS?

A. Providing a mapping of hostnames to IP addresses

B. Managing email server settings

C. Enabling the replication of websites

D. Translating internet hostnames into numeric IP addresses

5. What type of cipher is Twofish classified as?

A. Stream Cipher

B. Block Cipher

C. Asymmetric Cipher

D. Hash Function

6. What does a Certificate Authority (CA) primarily do?

A. Create secure encryption algorithms

B. Track digital certificates within a system

C. Maintain a public key infrastructure

D. Issue security patches for software

7. What utility traces a packet from your computer to an internet host?

A. Traceroute

B. nslookup

C. dig

D. ping

8. What organization is responsible for managing IP address allocation?

A. ICANN

B. DNS Authority

C. Anti-Phishing Working Group

D. Internet Society

9. What operator is used to search for files of a specific type in Google?

A. index of

B. filetype

C. cache

D. site

10. Which of the following features describes RSA?

A. Does not use prime numbers

B. Key sizes up to 4096 bits

C. Public domain

D. Produces a 128-bit hash

Answers

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

Explanations

1. What is the RIR responsible for Asia?

A. AFRINIC

B. LACNIC

C. APNIC

D. RIPE NCC

The correct answer is APNIC, which stands for the Asia-Pacific Network Information Centre. APNIC is the Regional Internet Registry (RIR) responsible for the Asia-Pacific region, which includes countries such as China, Japan, India, and Australia. Its primary role involves the allocation and management of IP address space, providing support and training for network operators, and contributing to the overall development of the internet in the region. APNIC plays a crucial role in the governance of internet resources in Asia by ensuring that addresses are allocated efficiently and that members have the necessary support to manage their networks. This helps maintain stability within the region's internet infrastructure. The organization also promotes best practices and collaborates with stakeholders to foster the growth of the internet community. Other regional internet registries, such as AFRINIC, LACNIC, and RIPE NCC, serve different geographical areas. AFRINIC is responsible for Africa, LACNIC covers Latin America and the Caribbean, and RIPE NCC operates in Europe, the Middle East, and parts of Central Asia. Each RIR has distinct responsibilities based on their respective regions, which is why APNIC is specifically identified as the RIR for Asia.

2. What is a hash in the context of data security?

A. Two-way encryption algorithm

B. A mathematical function that generates a fixed-length number

C. A form of key for data access

D. A method of data transmission

In the context of data security, a hash refers to a mathematical function that takes an input (or 'message') and produces a fixed-length string of characters, which is typically a sequence of numbers and letters. This output is known as a hash value or digest. The key characteristic of a hash function is that it is deterministic, meaning that the same input will always produce the same output. Additionally, it is designed to be a one-way function, which means that it is computationally difficult, if not impossible, to reverse the process and retrieve the original input from the hash value. Hash functions are extensively used in various aspects of data security, such as verifying data integrity, storing passwords securely, and ensuring that data has not been altered. For instance, when storing passwords, applications often store the hash of the password rather than the password itself, which helps improve security. In contrast, other options refer to different concepts within data security. Two-way encryption algorithms are designed to encrypt data, allowing it to be decrypted later, which is not the case for hashes. A hash does not serve as a key for data access but rather as a means to ensure data integrity. Lastly, the method of data transmission focuses on the process by which data is sent

3. What is the main task of an Address (A) Record in DNS?

A. Translate email addresses to usernames

B. Identify the authoritative nameserver for a domain

C. Map a hostname to its corresponding IP address

D. Provide aliases for subdomains

The main task of an Address (A) Record in DNS is to map a hostname to its corresponding IP address. When a user wants to access a website, their computer needs to convert the human-readable domain name (like www.example.com) into an IP address (like 192.0.2.1) that the internet can use to find the server hosting that website. The A Record provides this essential function, enabling the resolution of domain names into numerical addresses that computers understand, which is a critical part of how DNS facilitates the operation of the internet. The other options represent different DNS record types and functions. For instance, translating email addresses to usernames is not the role of an A Record; this usually involves other mechanisms like an MX record. Identifying the authoritative nameserver for a domain is the responsibility of NS (Name Server) records, which provide information about which servers are authoritative for a particular domain. Providing aliases for subdomains relates to CNAME (Canonical Name) records that allow one domain to be an alias for another. Thus, these roles are distinct from the fundamental function of A Records in the DNS architecture.

4. Which of the following is NOT a function of DNS?

A. Providing a mapping of hostnames to IP addresses

B. Managing email server settings

C. Enabling the replication of websites

D. Translating internet hostnames into numeric IP addresses

The correct choice highlights that enabling the replication of websites is not a function of the Domain Name System (DNS). DNS primarily serves to resolve human-readable domain names, like www.example.com, into machine-readable IP addresses, facilitating the connection to servers where the websites are hosted. Additionally, DNS plays a crucial role in managing email server settings through mechanisms such as MX (Mail Exchange) records, which dictate how email is routed based on the domain used. Furthermore, mapping hostnames to IP addresses and translating those addresses is fundamentally what DNS is all about. The replication of websites, however, involves techniques related to web hosting, load balancing, or content delivery networks (CDNs), which are entirely separate from the responsibilities of the DNS.

5. What type of cipher is Twofish classified as?

A. Stream Cipher

B. Block Cipher

C. Asymmetric Cipher

D. Hash Function

Twofish is classified as a block cipher. This means that it processes data in fixed-size blocks, typically 128 bits at a time, as it encrypts or decrypts information. Block ciphers such as Twofish use symmetric key algorithms, where the same key is used for both encryption and decryption. This is in contrast to stream ciphers, which encrypt data one bit or byte at a time and do not process fixed-size blocks. Additionally, asymmetric ciphers involve a pair of keys—public and private—whereas hash functions represent a one-way transformation to produce a fixed-size output from variable input, without the intention of reversing the process. Therefore, Twofish's classification as a block cipher highlights its design for secure symmetric encryption of large amounts of data in structured blocks.

6. What does a Certificate Authority (CA) primarily do?

A. Create secure encryption algorithms

B. Track digital certificates within a system

C. Maintain a public key infrastructure

D. Issue security patches for software

The primary role of a Certificate Authority (CA) is to maintain a public key infrastructure (PKI), which is crucial for the management and validation of digital certificates. A CA issues digital certificates used to establish the authenticity of entities, such as individuals or organizations, in online communications. By verifying the identities of the entities requesting a certificate and associating their public keys with this verified identity, the CA helps create a trustworthy environment for secure communication over untrusted networks like the internet. While options related to creating encryption algorithms, tracking digital certificates within a system, or issuing security patches may seem relevant to the realm of cybersecurity, they don't accurately capture the central function of a Certificate Authority. The issuance and management of digital certificates to ensure the integrity and authenticity of communications is a critical aspect of PKI and underpins many security protocols, making the maintenance of a public key infrastructure the correct answer.

7. What utility traces a packet from your computer to an internet host?

A. Traceroute

B. nslookup

C. dig

D. ping

Traceroute is the utility specifically designed to trace the path that packets take from one computer to a specified internet host. It works by sending a series of packets with incrementally increasing Time to Live (TTL) values. Each time a packet reaches a router, the router decreases the TTL by one. When the TTL reaches zero, the router drops the packet and sends an Internet Control Message Protocol (ICMP) "Time Exceeded" message back to the originating computer. This process helps identify each hop along the way to the destination, allowing users to see the route and the time taken for each segment of the journey. In contrast to traceroute, nslookup and dig are tools primarily used for querying Domain Name System (DNS) records to obtain domain name or IP address mapping, not for tracing packet paths. Ping, while useful for checking the reachability of a host and measuring round-trip time, does not provide detailed path information between the source and destination. It simply sends ICMP Echo Request packets and listens for Echo Reply packets. Thus, traceroute is the appropriate tool for tracing the route of packets through the network.

8. What organization is responsible for managing IP address allocation?

A. ICANN

B. DNS Authority

C. Anti-Phishing Working Group

D. Internet Society

The organization responsible for managing IP address allocation is ICANN, which stands for the Internet Corporation for Assigned Names and Numbers. ICANN plays a critical role in the global coordination of the Domain Name System (DNS) and in the allocation of IP addresses. It oversees the registration of domain names and the assignment of top-level domains while also managing the allocation of IP addresses through its direct oversight of five regional Internet registries (RIRs). These RIRs are responsible for distributing IP addresses to internet service providers and other organizations in specific geographical regions. In contrast, the DNS Authority focuses on the resolution of domain names into IP addresses but does not manage IP address allocation itself. The Anti-Phishing Working Group is dedicated to combatting phishing attacks and does not deal with IP addresses, while the Internet Society is more centered around promoting the open development and use of the internet rather than directly managing IP address assignments.

9. What operator is used to search for files of a specific type in Google?

A. index of

B. filetype

C. cache

D. site

The correct operator used to search for files of a specific type in Google is "filetype." This operator allows users to refine their search results to include only files of a designated format, such as PDF, DOCX, PPT, etc. By incorporating "filetype" followed by the desired extension into a search query, users can effectively filter their search to target specific types of documents, which can be particularly useful for researchers, students, or anyone seeking specialized information in format-specific files. The other options serve different purposes in a search context: "index of" is commonly used in conjunction with file directory searches but is not a Google search operator. "cache" allows you to view Google's cached version of a web page but does not filter by file type. Lastly, "site" restricts search results to a particular website or domain rather than focusing on the file type. Each of these operators has its unique utility, but for searching specific file types, "filetype" is the one that accurately meets the requirement.

10. Which of the following features describes RSA?

A. Does not use prime numbers

B. Key sizes up to 4096 bits

C. Public domain

D. Produces a 128-bit hash

The feature that describes RSA accurately is the key size capability, which can extend up to 4096 bits. RSA, which stands for Rivest-Shamir-Adleman, is an asymmetric cryptographic algorithm that relies heavily on the mathematics of large prime numbers for its security. As a result, the size of the keys used in RSA is critical to its robustness; larger keys provide a higher level of security against brute-force attacks and other forms of cryptanalysis. In practical terms, RSA key sizes commonly used include 2048 bits and 3072 bits, with 4096 bits being an option for those seeking even stronger security. This ability to scale up key sizes makes RSA suitable for various applications in security protocols, such as secure email and digital signatures. The other options do not accurately reflect key aspects of RSA. For instance, RSA fundamentally relies on prime numbers for its algorithm, as it is based on the mathematical challenge of factoring the product of two large primes. Additionally, RSA is not in the public domain in the sense that it is patented technology, and while it can be used in conjunction with hashing algorithms, RSA itself does not produce hashes directly; it operates on the encryption and decryption of data. Thus, the key size feature being

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!