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 do application-level attacks focus on?

A. Network security protocols

B. Underlying hardware vulnerabilities

C. Programming codes of an application

D. User authentication processes

2. Which encryption method is best at scaling for larger cryptographic systems?

A. Symmetric encryption

B. Asymmetric encryption

C. Hash functions

D. None of the above

3. Which type of attack is specifically designed to disrupt service to legitimate users?

A. Phishing Attacks

B. Denial of Service Attacks

C. Man-in-the-Middle Attacks

D. Malware Attacks

4. What is the correct syntax to use the nslookup command?

A. nslookup {hostname} [-options]

B. nslookup [-server] {hostname}

C. nslookup [-options] {hostname | [-server]}

D. nslookup {hostname} {options}

5. What is the purpose of the TTL in an SOA record?

A. Defines the time to live for DNS records

B. Specifies the source host address

C. Indicates the retry time for DNS queries

D. Stores the contact email for the domain

6. What term describes ethical hackers who are hired for security assessments?

A. Crackers

B. White Hats

C. Black Hats

D. Cyber Criminals

7. What challenges does the RIPE NCC primarily address?

A. Network configuration

B. Internet number resource registration

C. Website domain management

D. Data loss prevention

8. Which of the following is a phase of a standard hacking process?

A. Threat Modeling

B. Exploitation

C. Gaining Access

D. Patching

9. Which of the following RIRs is NOT associated with any part of North America?

A. ARIN

B. LACNIC

C. RIPE NCC

D. APNIC

10. What is the result when User B decrypts the hash using User A's public key?

A. Accesses User A's message

B. Confirms message integrity

C. Generates a new public key

D. Invalidates the digital certificate

Answers

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

Explanations

1. 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.

2. Which encryption method is best at scaling for larger cryptographic systems?

A. Symmetric encryption

B. Asymmetric encryption

C. Hash functions

D. None of the above

Asymmetric encryption is best at scaling for larger cryptographic systems due to its unique properties that facilitate secure communications and key distribution without the need for a pre-shared secret. In asymmetric encryption, a pair of keys—a public key and a private key—are used. The public key can be distributed widely, allowing anyone to encrypt messages for the key's owner, while the private key remains securely with the owner to decrypt those messages. This scalability is particularly beneficial in environments where there are many users needing to securely exchange information with one another. For example, if each user in a large system had to share a unique key for symmetric encryption, managing and securely distributing those keys would become increasingly complex as the number of users grows. Asymmetric encryption mitigates this issue, simplifying the key management process. Additionally, asymmetric encryption is inherently suited for establishing secure connections over the internet, such as in SSL/TLS protocols that are foundational for secure web communications. Its ability to work with digital signatures also aids in ensuring integrity and authenticity, further enhancing its utility in expansive environments. While symmetric encryption is generally faster and more efficient for encryption and decryption of large volumes of data, it does not scale as well for larger systems since each pair of users needs to securely exchange and

3. Which type of attack is specifically designed to disrupt service to legitimate users?

A. Phishing Attacks

B. Denial of Service Attacks

C. Man-in-the-Middle Attacks

D. Malware Attacks

Denial of Service (DoS) attacks are specifically designed to disrupt service to legitimate users by overwhelming a target system, network, or service with a flood of traffic or requests, thus making it unavailable to intended users. The primary goal of a DoS attack is to render a system inoperable or significantly degrade its performance, thereby denying legitimate users access to the service. In contrast, phishing attacks are aimed at tricking individuals into revealing sensitive information, such as usernames, passwords, and credit card numbers, rather than disrupting service. Man-in-the-Middle attacks focus on intercepting and altering communications between two parties without their knowledge, which does not inherently disrupt access but compromises confidentiality and integrity. Malware attacks can also cause damage or disruption but are generally broader in scope and can involve stealing data, damaging files, or spying on the user rather than specifically targeting service disruption. Thus, the defining characteristic of DoS attacks is their explicit intention to block legitimate access, distinguishing them from other types of cyber threats.

4. What is the correct syntax to use the nslookup command?

A. nslookup {hostname} [-options]

B. nslookup [-server] {hostname}

C. nslookup [-options] {hostname | [-server]}

D. nslookup {hostname} {options}

The nslookup command is a widely used tool for querying Domain Name System (DNS) records and retrieving information such as IP addresses associated with a domain name or the domain name associated with an IP address. The correct syntax allows for flexibility in specifying the hostname or server along with various options, which is crucial for effectively using the tool in different scenarios. In the correct syntax, options are available for users to modify the behavior of the command according to their specific needs. Using brackets indicates that these elements are optional. The ability to specify either a hostname or a server adds to the adaptability of the command, allowing a user to direct queries to different DNS servers if necessary. This comprehensive approach enables users to leverage nslookup for a variety of tasks related to DNS management and troubleshooting, making it a powerful tool in network analysis and system administration. The correct option captures this flexibility and applicability of the nslookup command, which is vital for ethical hackers and network professionals alike.

5. What is the purpose of the TTL in an SOA record?

A. Defines the time to live for DNS records

B. Specifies the source host address

C. Indicates the retry time for DNS queries

D. Stores the contact email for the domain

The purpose of the Time to Live (TTL) in a Start of Authority (SOA) record is to define the duration that a DNS record can be cached by resolvers before it must be discarded and re-queried from the authoritative nameserver. This value is crucial for controlling how long DNS information is considered valid and determines how frequently DNS data is updated across the internet. A shorter TTL means that changes to DNS records propagate more quickly, while a longer TTL can improve performance by reducing the number of queries sent to nameservers, at the risk of outdated information being held longer if changes occur. Understanding the function of TTL is critical for managing DNS effectively, especially in dynamic environments where IP addresses or domain configurations may frequently change. Other elements of the SOA record, such as the source host address or the retry time for DNS queries and the contact email, serve different purposes and do not relate directly to the lifespan of the cached DNS records.

6. What term describes ethical hackers who are hired for security assessments?

A. Crackers

B. White Hats

C. Black Hats

D. Cyber Criminals

The term that describes ethical hackers who are hired for security assessments is "White Hats." These individuals are cybersecurity professionals who use their skills to identify and address vulnerabilities in systems, applications, and networks before malicious actors can exploit them. White Hat hackers work within the boundaries of the law and often have explicit permission from the organizations they are testing. Their goal is to enhance security, protect sensitive data, and ultimately help organizations mitigate risks associated with cyber threats. In contrast, the other terms refer to individuals or groups with different motivations and ethical standings. "Crackers" typically refer to individuals who break into systems with malicious intent but are not necessarily recognized as ethical hackers. "Black Hats" are those who exploit security vulnerabilities for personal gain or to cause harm. "Cyber Criminals" is a broader term that encompasses anyone engaged in illegal activities online, often with a focus on theft, fraud, or other malicious acts. White Hats, therefore, represent the ethical side of hacking, emphasizing the importance of security and collaboration between hackers and organizations.

7. 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.

8. Which of the following is a phase of a standard hacking process?

A. Threat Modeling

B. Exploitation

C. Gaining Access

D. Patching

In the context of the standard hacking process, gaining access is a critical phase where a hacker successfully infiltrates a target system after successfully gathering information and discovering vulnerabilities. This step typically follows reconnaissance and scanning activities, where the hacker identifies weaknesses that can be exploited. Gaining access often involves using specific exploits or payloads to take advantage of these vulnerabilities, thus allowing the hacker to execute commands, steal data, or install additional malicious software. Threat modeling, while important in understanding and identifying potential threats during the security planning process, is more of a preparatory activity rather than a phase of hacking itself. Exploitation is indeed closely related to gaining access, as it refers to the methods employed to achieve that access, but it falls under the broader umbrella of tactics. Patching, on the other hand, refers to the process of fixing vulnerabilities and is more aligned with defensive cybersecurity measures, not part of the hacking process. Overall, gaining access is a fundamental part of the hacking cycle that denotes a successful breach of a system, making it a key phase in any hacking attempt.

9. Which of the following RIRs is NOT associated with any part of North America?

A. ARIN

B. LACNIC

C. RIPE NCC

D. APNIC

The response indicating that RIPE NCC is not associated with any part of North America is accurate because RIPE NCC (Réseaux IP Européens Network Coordination Centre) is the Regional Internet Registry that primarily serves Europe, the Middle East, and parts of Central Asia. It focuses on the allocation of IP addresses and other Internet resources within its designated regions, which do not include North America. In contrast, ARIN (American Registry for Internet Numbers) specifically serves Canada, the United States, and parts of the Caribbean. LACNIC (Latin America and Caribbean Network Information Centre) caters to the Latin American and Caribbean regions, while APNIC (Asia-Pacific Network Information Centre) serves the Asia-Pacific region. Each of these organizations is associated with specific geographical areas, and RIPE NCC's scope excludes North America. Understanding the roles and regional responsibilities of these RIRs is crucial for anyone involved in networking, cybersecurity, or internet infrastructure management, as it highlights how IP address allocation is organized globally.

10. What is the result when User B decrypts the hash using User A's public key?

A. Accesses User A's message

B. Confirms message integrity

C. Generates a new public key

D. Invalidates the digital certificate

When User B decrypts the hash using User A's public key, the result is a confirmation of the message's integrity. This process typically involves a digital signature, where User A creates a hash of the message and then encrypts that hash with their private key. When User B receives the message, they can use User A's public key to decrypt the hash. By decrypting the hash, User B can then compare it to a newly generated hash of the received message. If the two hashes match, it confirms that the message has not been altered in transit and that it indeed came from User A. This confirmation process is a fundamental component of digital communication, providing both authenticity and integrity to the transmitted message. The other options relate to aspects which are not relevant to the action performed in this scenario. For example, accessing User A's message does not occur merely by decrypting the hash, because User B would still need the original message alongside the hash to complete the verification process. Generating a new public key and invalidating a digital certificate do not connect to the action of decrypting a hash, as they pertain to key management and certification rather than the integrity checking process.

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!