Cyber Hero Certification Practice Test (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 does ThreatLocker use to profile drivers?

A. The name of the driver

B. The version number of the driver

C. The hash of the file

D. The size of the driver file

2. What is the primary goal of a security awareness program?

A. To increase employee productivity

B. To educate employees about security risks

C. To assess employee performance

D. To implement new technology

3. What is the consequence of not creating a custom application and policy for frequently changing hashes?

A. The program will always be allowed

B. The program may face regular blocks

C. The program's functionality might be enhanced

D. No consequence if it is a trusted application

4. What does "password cracking" involve?

A. The process of creating strong passwords

B. A method to recover lost passwords from users

C. The process of recovering passwords from stored or transmitted data

D. A technique to log password attempts

5. What fallback security measure is implied by saving policies locally?

A. Offline protection for computers

B. Centralized backup management

C. Standard logging of activity

D. Cloud-based security services

6. ThreatLocker does not automatically create certificate rules for applications in folders located at what location?

A. C: drive

B. The root of C:

C. The system32 folder

D. The user profile folder

7. What does incident response involve?

A. The process of developing software applications

B. Detecting, investigating, and responding to cybersecurity incidents

C. Creating firewalls for data protection

D. Storing data securely in the cloud

8. What does "BYOD" stand for and what is a concern associated with it?

A. Bring Your Own Device; it raises security concerns

B. Backup Your Own Data; it increases storage issues

C. Build Your Own Database; it complicates access

D. Borrow Your Own Device; it enhances user experience

9. How are default policies categorized after the deployment?

A. Allow and deny policies

B. Mandatory and optional policies

C. Standard and custom policies

D. Default allow and deny policies

10. Why is it important for employees to understand security risks?

A. To comply with legal regulations

B. To protect organizational assets

C. To enhance corporate profits

D. To develop new security technologies

Answers

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

Explanations

1. What does ThreatLocker use to profile drivers?

A. The name of the driver

B. The version number of the driver

C. The hash of the file

D. The size of the driver file

ThreatLocker uses the hash of the file to profile drivers because file hashing is a reliable method of ensuring file integrity and authenticity. A hash function generates a unique string of characters (the hash) based on the contents of the file. This means even a slight change in the file will result in a completely different hash value. By using hashes, ThreatLocker can accurately identify and manage drivers, distinguishing between safe and potentially harmful software. This approach provides a strong defense against malicious modifications or tampering, as it is based on an unalterable representation of the file's data. In comparison, factors such as the name or version number of the driver may not be unique or could be easily spoofed, while the size of the driver file does not sufficiently account for the content's integrity. Thus, relying on the hash of the file ensures a more robust and secure method for profiling drivers.

2. What is the primary goal of a security awareness program?

A. To increase employee productivity

B. To educate employees about security risks

C. To assess employee performance

D. To implement new technology

The primary goal of a security awareness program is to educate employees about security risks. This educational focus is vital because employees are often seen as the first line of defense in an organization's security posture. By equipping them with knowledge about potential threats, such as phishing attacks, social engineering, or malware, organizations can foster a culture of security awareness. This education helps employees recognize suspicious activities and take appropriate actions to protect sensitive information. Increasing employee productivity, assessing performance, or implementing new technology are not the main objectives of a security awareness program. While employee productivity is important, it is not directly influenced by security awareness training. Similarly, while assessing employee performance is a valuable practice, it does not align with the fundamental aim of promoting security awareness. Finally, implementing new technology is an essential aspect of cybersecurity, but it does not directly contribute to enhancing employee understanding of security risks. The focus of a security awareness program is specifically on education and risk understanding, positioning employees to better protect themselves and the organization.

3. What is the consequence of not creating a custom application and policy for frequently changing hashes?

A. The program will always be allowed

B. The program may face regular blocks

C. The program's functionality might be enhanced

D. No consequence if it is a trusted application

Failing to create a custom application and policy for frequently changing hashes can lead to the program experiencing regular blocks. When an application has constantly changing hashes, it signals to security systems that the application might be suspicious or non-compliant with established policies. Without a tailored policy that accounts for these changes, the application may be flagged more often, leading to unintentional disruptions in its functionality. This could hinder the performance, availability, or user experience associated with the application, as it might face repeated denials of access or execution. In contrast, when a custom policy is established to accommodate the specific nature of the application's hash changes, the application can function smoothly without being blocked by security mechanisms that react to what they perceive as abnormal behavior.

4. What does "password cracking" involve?

A. The process of creating strong passwords

B. A method to recover lost passwords from users

C. The process of recovering passwords from stored or transmitted data

D. A technique to log password attempts

The correct answer involves the process of recovering passwords from stored or transmitted data, which is fundamentally what password cracking entails. This process is typically employed by individuals or software to decode encrypted passwords or to break into systems where the password is unknown. It utilizes various techniques, such as brute force attacks, dictionary attacks, and more sophisticated methods aimed at exploiting vulnerabilities in the security system to retrieve password information. Understanding this concept is essential in the context of cybersecurity, as it highlights the importance of strong password policies, encryption methods, and overall security measures to protect sensitive information. Recognizing how password cracking works can help organizations to fortify their defenses against unauthorized access and improve their data protection strategies. In contrast, the other options do not accurately define password cracking. Creating strong passwords, recovering lost passwords from users, and logging password attempts represent different aspects of password management and security, but they do not encapsulate the act of recovering passwords through cracking techniques.

5. What fallback security measure is implied by saving policies locally?

A. Offline protection for computers

B. Centralized backup management

C. Standard logging of activity

D. Cloud-based security services

Saving policies locally implies a fallback security measure that provides offline protection for computers. When policies are stored locally, they ensure that a device can still function with security measures in place even in the absence of an internet connection or access to centralized management systems. This is particularly important for maintaining the integrity and security of the system, as local policies can enforce security protocols, user permissions, and other critical settings without relying on real-time communication with external servers. In scenarios where a network failure might occur, local policies act as a safeguard, ensuring that basic security functions remain operational. This means that even if the external systems become unreachable, the locally stored policies will continue to govern how the device operates and protects itself from potential threats. The other options do not directly relate to the concept of local policy storage and its implications for offline security. Centralized backup management pertains to data safety and retention strategies rather than real-time security enforcement when connectivity is not possible. Standard logging of activity is about monitoring and recording actions in a system, which does not inherently provide a fallback in the absence of connectivity. Cloud-based security services depend heavily on internet access and are not applicable when considering the security of devices that must operate independently of external connections.

6. ThreatLocker does not automatically create certificate rules for applications in folders located at what location?

A. C: drive

B. The root of C:

C. The system32 folder

D. The user profile folder

ThreatLocker is designed to establish certificate rules to manage application execution through a process called application whitelisting. However, it prioritizes security by not automatically creating these rules for applications located directly at the root of the C:\ drive. This decision is rooted in the desire to prevent potential exploitation; the root directory is a common target for malware. By not automatically allowing applications from the root of the C:\ drive, ThreatLocker effectively enhances the security posture of a system. Applications in this location could potentially be less trustworthy, and automating permissions could inadvertently allow malicious software to run. In contrast, applications in other specified areas, like system folders or user profile folders, are more likely to be legitimate and come from known sources, thus allowing ThreatLocker to create rules for them automatically when appropriate. Therefore, the rationale for not creating certificate rules for the applications in the root of the C:\ drive aligns with best security practices aimed at minimizing risks from potentially untrusted sources.

7. What does incident response involve?

A. The process of developing software applications

B. Detecting, investigating, and responding to cybersecurity incidents

C. Creating firewalls for data protection

D. Storing data securely in the cloud

Incident response involves a systematic approach to managing and responding to cybersecurity incidents, which encompasses detecting, investigating, and taking action to address threats or breaches in security. This process is critical in minimizing damage, reducing recovery time and costs, and preventing future incidents. The detection phase often involves monitoring systems for unusual activity that could indicate a breach. Following detection, the investigation phase determines the nature and extent of the incident, enabling responders to assess the impact and the necessary response measures. The response phase involves implementing strategies to contain and remediate the incident, restoring affected systems and services, and eventually reviewing the incident to improve future response efforts. This comprehensive approach ensures that organizations can effectively manage cybersecurity incidents, which is essential given the increasing complexities and threats faced in the digital landscape. The other options focus on unrelated aspects of cybersecurity or information technology, such as software development, firewall creation, and data storage, which are not part of the incident response process.

8. What does "BYOD" stand for and what is a concern associated with it?

A. Bring Your Own Device; it raises security concerns

B. Backup Your Own Data; it increases storage issues

C. Build Your Own Database; it complicates access

D. Borrow Your Own Device; it enhances user experience

"BYOD" stands for "Bring Your Own Device," a practice where employees are allowed or encouraged to use their personal devices—such as smartphones, tablets, and laptops—for work purposes. This trend has gained popularity as it can lead to increased productivity and convenience, as employees are often more comfortable using their personal devices. However, a significant concern associated with BYOD is security. When personal devices are used to access company data, it opens up various vulnerabilities. These devices may not have the same level of security measures as the organization's managed devices, which can lead to data leakage, unauthorized access, and other security breaches. This situation is particularly problematic if employees are accessing sensitive information while connected to unsecured networks, such as public Wi-Fi. Organizations must implement strict policies, such as data encryption and mobile device management, to mitigate the risks posed by the BYOD approach.

9. How are default policies categorized after the deployment?

A. Allow and deny policies

B. Mandatory and optional policies

C. Standard and custom policies

D. Default allow and deny policies

Default policies are categorized as default allow and deny policies, which play a crucial role in security frameworks and access control systems. This categorization reflects the fundamental operational philosophy employed in many systems regarding permissions and restrictions. When a system is set up, default allow policies grant access to users or processes unless explicitly denied. Conversely, default deny policies deny access by default, requiring specific permissions to be granted for access. Understanding this categorization is essential because it helps professionals ensure that the right level of access is maintained while minimizing the risk of unauthorized access. Using default allow or deny frameworks helps organizations easily implement their security strategy based on their risk management preferences. Such categorization simplifies the application of rules, making it easier to manage and understand the overall security posture of an organization. By focusing on how the default policies function and their implications for security, individuals can effectively analyze and adapt their policies to suit organizational needs and compliance requirements.

10. Why is it important for employees to understand security risks?

A. To comply with legal regulations

B. To protect organizational assets

C. To enhance corporate profits

D. To develop new security technologies

Understanding security risks is crucial for employees primarily because it directly relates to the protection of organizational assets. Employees are the first line of defense against security threats; their awareness and understanding of potential risks empower them to identify, report, and mitigate such threats effectively. This includes everything from physical assets like equipment to intangible assets such as sensitive data and intellectual property. When employees recognize the various security vulnerabilities that can affect their organization, they are better equipped to take proactive measures. This can include following protocols for data protection, using strong passwords, recognizing phishing attempts, and adhering to security policies. By safeguarding organizational assets, employees contribute to the overall resilience and integrity of the organization, ensuring that it can operate effectively without interruption from security breaches or data losses. While compliance with legal regulations is important, enhancing corporate profits or developing new technologies does not directly pertain to the core necessity of understanding security risks in the same practical and immediate way that protecting assets does. Hence, the focus on asset protection not only secures the organization but also fosters a culture of security awareness that can lead to more informed and responsible employee behavior regarding cybersecurity.

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://cyberherocert.examzify.com

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