Ethical Hacking Essentials 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. **Which form of identity theft can include selling stolen identity information for benefits such as loans and credit?**

   A. Social Identity Theft

   B. Tax Identity Theft

   C. Medical Identity Theft

   D. Child Identity Theft

2. **In which level of the Purdue model is the physical process analyzed and altered?**

   A. Level 0

   B. Level 1

   C. Level 2

   D. Level 3

3. **What attack is characterized by sending a malicious text message to collect sensitive information from mobile devices?**

   A. Phishing

   B. SMiShing

   C. Vishing

   D. Malware injection

4. **Which protocol is utilized for accessing and manipulating electronic mail messages on a server?**

   A. Internet Message Access Protocol (IMAP)

   B. Network File System (NFS)

   C. Hypertext Transfer Protocol (HTTP)

   D. Secure Copy Protocol (SCP)

5. **What do IDS and IPS systems do when malicious traffic enters a target machine or server?**

   A. Drop the packets

   B. Raise alarms

   C. Log the traffic

   D. Redirect traffic

6. What type of cloud deployment model combines two or more clouds while maintaining their unique identities and includes both in-house and externally obtained resources?

A. Public Cloud

B. Private Cloud

C. Hybrid Cloud

D. Multi-Cloud

7. Which of the following practices can help security teams protect the web server from cyberattacks?

A. Limit the server functionality to support only the web technologies to be used

B. Implement broad network access to promote flexibility

C. Enable all functionalities to allow for future scalability

D. Provide unrestricted access to all users

8. What BYOD risk is demonstrated when an employee transfers project details over an unsecured Wi-Fi network?

A. Data encryption failure

B. Sharing confidential data on unsecured networks

C. Malware infection from personal devices

D. Use of inadequate device passwords

9. What practice helps security specialists protect the network against password cracking attempts?

A. Use weak passwords

B. Check any suspicious application that stores passwords in memory

C. Disable account lockout

D. Allow password storage in unsecured locations

10. In penetration testing, what is the consequence of not using appropriate testing tools?

A. Improved security posture

B. Increased network vulnerability

C. Reduced testing time

D. Enhanced system performance

Answers

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

Explanations

1. Which form of identity theft can include selling stolen identity information for benefits such as loans and credit?

A. Social Identity Theft

B. Tax Identity Theft

C. Medical Identity Theft

D. Child Identity Theft

The correct choice, which identifies identity theft that involves the selling of stolen identity information for benefits like loans and credit, pertains to Social Identity Theft. This type refers specifically to the misuse of someone's personal information, such as their Social Security number, to commit financial fraud. Criminals may use this information to open new credit accounts, take out loans in the victim's name, or sell this data to other criminals for similar purposes. In contrast, Tax Identity Theft revolves around the unauthorized use of someone's personal information to file fraudulent tax returns and claim refunds. Medical Identity Theft involves using someone else's identity to obtain medical services or products, which can lead to complications with health records and billing. Child Identity Theft focuses on using a child's identity for fraud, often going unnoticed for years as the child is too young to be involved in financial transactions. Each of these categories has distinct characteristics and methods of exploitation, but Social Identity Theft is specifically tied to financial gains from securing loans and credit under someone else's identity.

2. In which level of the Purdue model is the physical process analyzed and altered?

A. Level 0

B. Level 1

C. Level 2

D. Level 3

The correct choice refers to Level 1 of the Purdue model, which is specifically focused on the control systems that manage the physical processes in an industrial environment. In this level, real-time data from the physical operations are collected, and the systems through which these operations are monitored and controlled are analyzed and adjusted. This level is where the interaction between the physical processes and the control algorithms takes place, enabling the necessary alterations to improve efficiency, safety, and performance. While Level 0 deals with the physical processes themselves, such as the machinery and the operations they perform, it does not focus on the analysis or modification of these processes. Higher levels in the model, like Level 2 and Level 3, deal more with data aggregation and decision-making processes but do not engage directly with the physical process control as Level 1 does. Thus, it's on Level 1 that specific adjustments to how the physical processes are managed occur.

3. What attack is characterized by sending a malicious text message to collect sensitive information from mobile devices?

A. Phishing

B. SMiShing

C. Vishing

D. Malware injection

The focus of this question centers around the specific type of attack that involves sending malicious text messages to target individuals and gather sensitive information from their mobile devices. SMiShing is a term specifically coined to describe SMS phishing, where cybercriminals send text messages that appear legitimate but are designed to provoke recipients into providing personal details, such as passwords or financial information. These messages often contain links to fake websites or instruct the user to reply with sensitive information, exploiting the trust associated with text communications on mobile devices. By understanding that SMiShing is a targeted approach leveraging SMS technology, it is clear why this answer accurately aligns with the characteristics described in the question. The other options represent different forms of social engineering attacks: phishing generally refers to similar tactics using email instead of text messages, vishing uses voice communication via phone calls, and malware injection pertains to compromising systems through malicious software, none of which involve the specific use of SMS to bait victims.

4. Which protocol is utilized for accessing and manipulating electronic mail messages on a server?

A. Internet Message Access Protocol (IMAP)

B. Network File System (NFS)

C. Hypertext Transfer Protocol (HTTP)

D. Secure Copy Protocol (SCP)

The Internet Message Access Protocol (IMAP) is specifically designed for accessing and managing email messages on a mail server. With IMAP, users can retrieve, read, and organize their emails while leaving the messages stored on the server. This allows users to maintain access to their email from multiple devices without having to download the messages each time. IMAP also supports folder manipulation, message searching, and synchronization between the server and the email client, ensuring that actions taken in one client are reflected across all clients. This makes it an ideal protocol for modern email usage, where users often check their email on various devices. In contrast, other protocols like the Network File System (NFS) are used for file sharing between systems, and the Hypertext Transfer Protocol (HTTP) is designed for transferring hypertext and web content rather than email. The Secure Copy Protocol (SCP) is utilized for securely transferring files over a network but is not related to email access or manipulation. This distinction highlights IMAP's unique role in email management.

5. What do IDS and IPS systems do when malicious traffic enters a target machine or server?

A. Drop the packets

B. Raise alarms

C. Log the traffic

D. Redirect traffic

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) serve critical roles in network security when it comes to handling malicious traffic. An IDS is designed to monitor network traffic and identify potential threats by analyzing patterns and signatures of malicious activities. When such activity is detected, the system will typically raise alarms to alert administrators about the potential intrusion, enabling a rapid response to the threat. On the other hand, while both systems may log the traffic for further analysis, the primary focus of an IDS is on detection, which involves raising alerts rather than taking direct action like blocking or dropping packets. This distinction is essential, as the purpose of an IDS is to inform and allow for human intervention. In summary, the role of raising alarms for malicious traffic aligns with the primary function of an IDS, supporting security teams in keeping networks safe by providing critical visibility into potential threats. Logging, while also a function, is secondary to the priority of alerting security personnel so they can respond accordingly.

6. What type of cloud deployment model combines two or more clouds while maintaining their unique identities and includes both in-house and externally obtained resources?

A. Public Cloud

B. Private Cloud

C. Hybrid Cloud

D. Multi-Cloud

The correct answer is a hybrid cloud deployment model. This model is specifically designed to provide a flexible and scalable cloud environment by combining both private and public cloud services. In a hybrid cloud setup, organizations can seamlessly integrate their in-house infrastructure with external cloud services, allowing them to retain unique identities for each cloud while enabling data and application portability. The hybrid cloud model offers several advantages, such as enhanced security for sensitive data through the private cloud while utilizing public cloud resources for scalability and cost-effectiveness. This dual structure allows organizations to optimize their IT resources, balancing workload demands efficiently between private and public environments. While the public cloud is based entirely on services offered over the internet with shared resources, and the private cloud consists solely of infrastructure dedicated to a single organization, the hybrid cloud uniquely blends both models. A multi-cloud strategy, on the other hand, involves the use of services from multiple cloud providers but does not necessarily integrate them into a unified deployment like the hybrid cloud does. Thus, the hybrid cloud's fundamental characteristic of combining distinct cloud environments while preserving their identities distinguishes it from the other models.

7. Which of the following practices can help security teams protect the web server from cyberattacks?

A. Limit the server functionality to support only the web technologies to be used

B. Implement broad network access to promote flexibility

C. Enable all functionalities to allow for future scalability

D. Provide unrestricted access to all users

Limiting the server's functionality to support only the web technologies that are necessary is a fundamental security practice known as "minimizing the attack surface." By reducing the number of services and functionalities that run on a web server, the potential points of entry for a cyberattack are decreased. This means that attackers have fewer vulnerabilities to exploit, making it significantly harder for them to succeed in compromising the server. For example, if a web server only needs to serve HTML pages and needs a database connection, it should be configured to disable any additional services like FTP, SSH, or test web applications that may not be needed. This kind of focused configuration reduces the risk of undetected vulnerabilities present in unnecessary services and also simplifies the management and monitoring of the server's security posture. In contrast, broader strategies such as implementing wide network access can introduce significant vulnerabilities by exposing the server to more potential threats and reducing the ability to control and monitor incoming traffic. Enabling all functionalities for future scalability can lead to unnecessary complexities that could become entry points for attackers. Providing unrestricted access to all users contradicts the principle of least privilege and poses severe security risks, as it allows unauthorized individuals to exploit server vulnerabilities easily.

8. What BYOD risk is demonstrated when an employee transfers project details over an unsecured Wi-Fi network?

A. Data encryption failure

B. Sharing confidential data on unsecured networks

C. Malware infection from personal devices

D. Use of inadequate device passwords

The scenario presented involves an employee transferring sensitive project details over an unsecured Wi-Fi network, which highlights a significant risk associated with Bring Your Own Device (BYOD) policies: sharing confidential data on unsecured networks. When data is transmitted over a network that lacks proper security measures, it is vulnerable to interception by malicious actors. This is particularly concerning for businesses handling sensitive or proprietary information, as this kind of exposure could lead to data breaches or loss of intellectual property. In this context, using unsecured networks means that the data being transferred is not protected by encryption, making it accessible to anyone within range of the network. Employees may not realize the risks associated with using public Wi-Fi or unsecured connections for sensitive transactions, which can lead to unauthorized access to confidential information. The other options, such as data encryption failure, malware infection from personal devices, and the use of inadequate device passwords, relate to important cybersecurity issues but do not directly address the specific risk presented by the act of sharing data over an unsecured network. Understanding the implications of unsecured network use is crucial for mitigating risks in a BYOD environment.

9. What practice helps security specialists protect the network against password cracking attempts?

A. Use weak passwords

B. Check any suspicious application that stores passwords in memory

C. Disable account lockout

D. Allow password storage in unsecured locations

The practice of checking any suspicious application that stores passwords in memory is vital for protecting the network against password cracking attempts because it helps identify potential vulnerabilities in the system. Applications that store passwords in memory can be targets for attackers who may use various techniques, such as memory scraping or process injection, to extract those passwords. By actively monitoring and examining these applications, security specialists can take proactive measures to ensure that sensitive information is not being exposed, particularly if an application is behaving unusually or has not been appropriately secured. This vigilance can help prevent attackers from gaining unauthorized access through compromised credentials, making it a crucial aspect of maintaining robust security measures within a network. In contrast, using weak passwords, disabling account lockout, and allowing password storage in unsecured locations would significantly increase the risk of password cracking and should be avoided, as these practices leave systems more vulnerable to access by malicious actors.

10. In penetration testing, what is the consequence of not using appropriate testing tools?

A. Improved security posture

B. Increased network vulnerability

C. Reduced testing time

D. Enhanced system performance

In penetration testing, the use of appropriate testing tools is critical to accurately assess and identify vulnerabilities in a system or network. When the correct tools are not employed, one of the primary consequences is the increased network vulnerability. This happens because the testing may miss critical weaknesses that could be exploited by malicious actors, leading to an inadequate security assessment. Using inadequate tools may not reveal all the potential entry points or known exploits, leaving systems exposed to attacks. Moreover, without the effective identification of vulnerabilities, organizations might wrongly assume their security measures are robust, resulting in an unpreparedness for actual security threats. Thus, utilizing unsuitable tools can directly contribute to a heightened state of network vulnerability, as it prevents comprehensive vulnerability assessment and remediation efforts. The other options do not align with the consequences of not using appropriate testing tools in penetration testing. Improved security posture suggests a stronger security state, which contradicts the outcomes of inadequate testing. Reduced testing time does not imply thoroughness or effectiveness, and enhanced system performance is unrelated to the objectives of penetration testing. Therefore, the direct link between inappropriate tools and increased vulnerabilities is evident in the context of penetration testing.

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!