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 tool is known for its capability to capture traffic from various networks, including Bluetooth and Ethernet?

   A. bettercap

   B. Wireshark

   C. hping3

   D. Nbtstat

2. What type of attack was performed when a malicious link tricked an employee into exposing their device?

   A. Phishing attack

   B. User-initiated code

   C. Replay attack

   D. Sniffing attack

3. Which of the following countermeasures can assist users in reducing the chances of identity theft?

   A. Enable two-factor authentication on all online accounts

   B. Making passwords publicly known

   C. Using the same password across multiple sites

   D. Storing passwords in plain text files

4. Which password cracking tool was used by Malcolm to gain unauthorized access?

   A. Medusa

   B. hashcat

   C. John the Ripper

   D. THC Hydra

5. Identify the trojan that uses port number 443 to infect systems and propagate malware.

   A. Silencer

   B. WebEx

   C. Emotet

   D. Defacement trojan

6. What guideline helps users identify and secure sensitive data on their mobile devices?

A. Implement two-factor authentication

B. Apply validation of the security of API calls to the sensitive data

C. Regularly update software applications

D. Use strong passwords for all accounts

7. In which hacking phase do attackers gather information about the target system such as port status and OS details?

A. Gaining Access

B. Reconnaissance

C. Scanning

D. Maintaining Access

8. Which of the following describes a DHCP starvation attack?

A. An attacker floods the DHCP server with requests

B. An attacker spoofs ARP replies

C. An attacker hijacks DNS responses

D. An attacker floods a switch with packets

9. What is the name of the attack where an attacker takes control of an existing TCP connection?

A. Session fixation

B. Session hijacking

C. Session desynchronization

D. TCP spoofing

10. Which of the following describes extraneous functionality in software development?

A. Inclusion of unnecessary code that does not serve a security purpose

B. Implementation of rigorous access controls

C. Use of secure coding techniques during development

D. Documenting all source code changes

Answers

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

Explanations

1. Which tool is known for its capability to capture traffic from various networks, including Bluetooth and Ethernet?

A. bettercap

B. Wireshark

C. hping3

D. Nbtstat

Wireshark is recognized for its powerful packet analysis capabilities, allowing users to capture and display network traffic in real-time. It is versatile, supporting a wide range of protocols across different types of networks, including Ethernet, Wi-Fi, and even Bluetooth under certain configurations. The reason Wireshark stands out is due to its extensive protocol dissectors, which enable it to decode a multitude of protocols as they traverse the network. This functionality is critical for network administrators and security professionals to analyze communications and diagnose network issues, as well as for ethical hackers conducting assessments of system vulnerabilities. Other tools mentioned, while useful, have more specific functions. Bettercap is generally used for network attacks and penetration testing rather than a broad approach to traffic capturing. Hping3 is primarily a packet crafting tool and is utilized for creating custom TCP/IP packets for testing network security rather than passive traffic capture. Nbtstat, on the other hand, is specifically geared towards NetBIOS over TCP/IP, allowing users to troubleshoot and enjoy limited functionality in terms of network traffic analysis. Thus, Wireshark is the preferred tool for comprehensive traffic capture across diverse network types.

2. What type of attack was performed when a malicious link tricked an employee into exposing their device?

A. Phishing attack

B. User-initiated code

C. Replay attack

D. Sniffing attack

The attack described, where a malicious link tricks an employee into exposing their device, aligns with a phishing attack. In this scenario, phishing typically involves deceiving a user into clicking a link or providing sensitive information, which can lead to malware installation or data theft. User-initiated code would imply that the user intentionally executed a piece of code that resulted in unintended consequences, but in the context of this question, we are looking at how an attack was specifically orchestrated to manipulate the user into taking action, rather than the consequence of them executing code themselves. Phishing is the term that captures the essence of this deceptive act, where social engineering is leveraged to gain access to a device or data. Replay attacks involve capturing and replaying valid data transmissions, while sniffing attacks focus more on intercepting network traffic. Neither of these accurately reflects the behavior described in the question, which focuses on the pivotal role of user deception through a malicious link.

3. Which of the following countermeasures can assist users in reducing the chances of identity theft?

A. Enable two-factor authentication on all online accounts

B. Making passwords publicly known

C. Using the same password across multiple sites

D. Storing passwords in plain text files

Enabling two-factor authentication on all online accounts is an effective countermeasure for reducing the chances of identity theft. This security process requires users to provide two different types of information to verify their identity. Typically, the first factor is something the user knows, like a password, while the second factor is something the user possesses, such as a mobile device that receives a one-time code. This additional layer of security significantly enhances the protection of online accounts, making it more difficult for unauthorized individuals to gain access, even if they have obtained the user's password. In contrast, making passwords publicly known, using the same password across multiple sites, and storing passwords in plain text files all pose serious security risks. Publicly sharing passwords opens accounts to anyone who sees them. Using the same password across different accounts increases vulnerability; if one account is compromised, all accounts using that same password are at risk. Similarly, storing passwords in plain text files makes them easily accessible to anyone who gains access to the computer or storage device.

4. Which password cracking tool was used by Malcolm to gain unauthorized access?

A. Medusa

B. hashcat

C. John the Ripper

D. THC Hydra

Hashcat is recognized for its efficient and innovative approach to password cracking, leveraging the power of GPUs to handle massive amounts of data quickly. It supports a wide array of hashing algorithms, making it exceptionally versatile for various password recovery scenarios. This capability makes it suitable for attacking both simple and complex hashed passwords. In the context of unauthorized access, the effectiveness of Hashcat can be attributed to its speed and ability to utilize different cracking methods, such as dictionary attacks and brute force, to crack passwords. Users can find themselves able to run multiple threads in parallel, significantly reducing the time taken to discover passwords compared to CPU-based methods. While other tools like John the Ripper, THC Hydra, Medusa, and similar programs have their own strengths, Hashcat stands out due to its performance on large datasets and complex hash types, enabling it to effectively assist in pentesting scenarios where password strength is tested. This makes it a likely choice for someone attempting to gain unauthorized access using password cracking techniques.

5. Identify the trojan that uses port number 443 to infect systems and propagate malware.

A. Silencer

B. WebEx

C. Emotet

D. Defacement trojan

The trojan known to utilize port number 443 for infection and malware propagation is Emotet. This particular malware family is notorious for leveraging encrypted communication over HTTPS to evade detection and facilitate its malicious activities. By using port 443, Emotet can often bypass traditional network defenses that monitor unencrypted traffic, making it a particularly stealthy type of trojan. Emotet originally appeared as a banking trojan but has evolved into a versatile delivery mechanism for various types of malware, including ransomware and other forms of trojans. Its ability to exploit port 443 plays a crucial role in its operation, allowing it to communicate with command and control servers securely. This makes it difficult for security systems to analyze the traffic for malicious content, thereby enhancing its effectiveness in spreading malware. In contrast, the other options do not specifically associate with the use of port 443 in the same way as Emotet does. For instance, while some may use alternative communication methods or target different types of vulnerabilities, they don't share the same notoriety and functionality tied to this specific port.

6. What guideline helps users identify and secure sensitive data on their mobile devices?

A. Implement two-factor authentication

B. Apply validation of the security of API calls to the sensitive data

C. Regularly update software applications

D. Use strong passwords for all accounts

The guideline that is most pertinent to helping users identify and secure sensitive data on their mobile devices is focused on applying validation of the security of API calls to sensitive data. This approach is crucial because mobile applications often rely on APIs to communicate with back-end services, especially when handling sensitive data. Ensuring that these API calls are properly validated helps to safeguard data in transit, preventing unauthorized access and potential data breaches. While strong passwords, regular software updates, and two-factor authentication are all important elements of a comprehensive security strategy, they do not specifically address the unique challenges related to data security in the context of mobile applications. Strong passwords help to secure accounts, and two-factor authentication adds an additional layer of security for user logins, but neither directly aids in the identification and protection of sensitive data itself. Similarly, updating software is critical for security patches and fixing vulnerabilities, but it does not inherently provide a mechanism for securing sensitive data during its transmission via APIs.

7. In which hacking phase do attackers gather information about the target system such as port status and OS details?

A. Gaining Access

B. Reconnaissance

C. Scanning

D. Maintaining Access

The phase in which attackers gather information about the target system, such as port status and operating system details, is best described by scanning. During this phase, various scanning techniques are employed to identify active devices, open ports, and services running on those ports. This is a critical part of the hacking process as it allows attackers to assess vulnerabilities and potential entry points into the target system. Reconnaissance, while also focused on gathering information, typically precedes scanning and involves gathering intelligence without direct interaction with the target system, such as using publicly available information. Gaining access refers to the actual attempt to exploit identified vulnerabilities to breach the system, while maintaining access involves methods to ensure continued control over a compromised system. Therefore, scanning represents a more technical and active approach to retrieving specific data about the system's status and configurations.

8. Which of the following describes a DHCP starvation attack?

A. An attacker floods the DHCP server with requests

B. An attacker spoofs ARP replies

C. An attacker hijacks DNS responses

D. An attacker floods a switch with packets

A DHCP starvation attack involves an attacker overwhelming the DHCP server by flooding it with a large number of requests. This is done by spoofing the MAC addresses in each request, making it appear as if there are many different clients requesting IP address assignments. The goal of this attack is to exhaust the pool of available IP addresses the server can allocate, preventing legitimate users from obtaining an IP address and accessing the network. Once the DHCP server runs out of addresses, the attacker can control the network traffic or execute further malicious activities. The other options describe different types of attacks that do not align with the concept of DHCP starvation. For instance, spoofing ARP replies involves intercepting traffic using ARP spoofing, which targets communication between two devices rather than aiming to exhaust IP address assignment. Similarly, hijacking DNS responses targets name resolution rather than the DHCP process itself. Lastly, flooding a switch with packets is a different method of denial of service that focuses on the switch infrastructure, not the DHCP service specifically. Each of these attacks has its own method and target, but they do not relate to the depletion of IP addresses in the DHCP server as a starvation attack does.

9. What is the name of the attack where an attacker takes control of an existing TCP connection?

A. Session fixation

B. Session hijacking

C. Session desynchronization

D. TCP spoofing

Session hijacking is the process by which an attacker takes control of an existing TCP connection between two parties. This is accomplished by intercepting and manipulating the session token, which allows the attacker to access and control the communication without the knowledge of either legitimate party. In a typical session hijacking attack, the attacker can achieve unauthorized access to a user's session by exploiting vulnerabilities in the network or the target application's session management. This can lead to various harmful consequences such as impersonating the user, stealing sensitive information, or executing transactions on behalf of the user. The term "session hijacking" is often used specifically in the context of web applications, where attackers might steal cookies or session tokens, but its essence is rooted in the control over an ongoing TCP connection. Other options like session fixation involve the attacker tricking the user into using a session ID known to the attacker before the user logs in, while TCP spoofing relates more to the creation of fake TCP packets pretending to be from a trusted source, rather than taking control of an existing connection. Session desynchronization generally refers to a condition arising from the mismatch of states on both ends of a connection but does not describe the direct takeover of a session as hijacking does.

10. Which of the following describes extraneous functionality in software development?

A. Inclusion of unnecessary code that does not serve a security purpose

B. Implementation of rigorous access controls

C. Use of secure coding techniques during development

D. Documenting all source code changes

Extraneous functionality in software development refers to the inclusion of unnecessary code that does not fulfill a specific purpose, particularly in relation to the software's core functionality or security requirements. This unnecessary code can introduce vulnerabilities, as it may not have been adequately tested or maintained, leading to potential exploitation by malicious actors. In ethical hacking, identifying such extraneous features is critical, as they can provide an attack surface for techniques such as code injection or privilege escalation. Therefore, option A accurately captures the essence of extraneous functionality by highlighting the risk posed by superfluous elements in the codebase, which does not contribute to its intended performance or security.

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!