Security+ Master Deck 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 an application allow list help to manage in a security context?**

   A. Network traffic

   B. Software installations

   C. User authentication

   D. Data encryption

2. **Which of the following is an attack that seeks to manipulate a website based on the site's trust in an authenticated user?**

   A. XSRF

   B. SQL Injection

   C. Phishing

   D. Punking

3. **Which term describes a web application vulnerability that allows attackers to escalate privileges?**

   A. Denial of service

   B. Exploitation

   C. Privilege escalation

   D. Data leakage

4. **What situation is indicated by an empty audit.log file on a Linux system despite active uptime?**

   A. A configuration error

   B. A system malfunction

   C. A wiped log

   D. A scheduled maintenance period

5. **What two files are commonly attacked using offline brute-force attacks?**

   A. The Windows SAM and the Linux /etc/shadow file

   B. The Windows registry and the Linux /etc/passwd file

   C. The Windows config file and the Linux /var/log/auth.log file

   D. The Windows users file and the Linux /etc/group file

6. What action should an end user take to install an application in an environment utilizing an application allow list?

A. Download the application directly

B. Request that the application be added to the allow list

C. Contact the vendor of the application

D. Install the application without permission

7. What type of malware is characterized by sending private workstation information to a central server?

A. A virus

B. Trojan

C. Spyware

D. Adware

8. Which of the following is not typically a threat vector associated with SMS-based attacks?

A. SMS phishing links

B. SMS-delivered images

C. SMS text message spoofing

D. SMS account verification codes

9. What characterizes ransomware?

A. Spying on user activities

B. Encrypting files for ransom

C. Displaying unwanted advertisements

D. Altering system settings to cause harm

10. What type of deception technology involves planting documents that appear to contain sensitive information?

A. Honeyfile

B. Honeynet

C. Firewall lure

D. Decoy protocol

Answers

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

Explanations

1. What does an application allow list help to manage in a security context?

A. Network traffic

B. Software installations

C. User authentication

D. Data encryption

An application allow list is a security measure that specifically helps in managing software installations. This approach involves creating a list of approved applications that are permitted to run within an organization's environment. By doing so, it prevents unauthorized or potentially harmful software from being installed or executed. This method enhances security posture by reducing the risk of malware infections and other malicious activities that can occur when unapproved applications are allowed to run. It ensures that only known and trusted software is used, which can significantly decrease vulnerabilities and exposure to security threats. Consequently, an application allow list is vital in controlling the software landscape within an organization, ensuring compliance with security policies, and protecting sensitive data from being accessed or manipulated by unauthorized applications.

2. Which of the following is an attack that seeks to manipulate a website based on the site's trust in an authenticated user?

A. XSRF

B. SQL Injection

C. Phishing

D. Punking

The attack that seeks to manipulate a website based on the site's trust in an authenticated user is referred to as Cross-Site Request Forgery (XSRF). This type of attack works by convincing the authenticated user to execute unwanted actions on a web application where they are currently authenticated. Since the website inherently trusts the authenticated user, it processes the request as legitimate, leading to potential harmful consequences. In XSRF attacks, the attacker usually sends a crafted request to the victim while they are logged into a session with the target website, often exploiting forms, links, or other interactive components. This method relies on the trust that the application has in the user's session and bypasses typical security mechanisms by leveraging cookies and other forms of user authentication that are automatically included in the request made by the authenticated user. Understanding XSRF is critical in the context of web security as it emphasizes the need for additional safeguards such as anti-CSRF tokens and proper validation of user actions to ensure that requests are genuinely initiated by the authenticated user.

3. Which term describes a web application vulnerability that allows attackers to escalate privileges?

A. Denial of service

B. Exploitation

C. Privilege escalation

D. Data leakage

The correct answer is privilege escalation, which refers to a specific type of vulnerability in web applications where an attacker can gain elevated access to resources that should normally be restricted. This can occur through various means, such as exploiting a flaw in the application's code, misconfigurations, or using social engineering techniques. Privilege escalation allows an attacker to perform actions beyond what the application is designed to permit, such as accessing sensitive data, modifying user privileges, or executing administrative commands. It typically arises from issues like inadequate validation of user input or improper access controls, making it essential for developers to implement strong security measures to mitigate these risks. In contrast, denial of service refers to an attack that aims to make a service unavailable to its intended users, often through overwhelming traffic or exploiting vulnerabilities that crash the system. Exploitation is a broader term that encompasses any action taken to leverage a vulnerability, including but not limited to privilege escalation, making it less specific. Data leakage involves unauthorized access to actual data rather than gaining elevated privileges, focusing instead on the loss or exposure of sensitive information rather than the ability to perform unauthorized actions. This distinction highlights why privilege escalation is the most appropriate term for the scenario where an attacker increases their permission level within a web application.

4. What situation is indicated by an empty audit.log file on a Linux system despite active uptime?

A. A configuration error

B. A system malfunction

C. A wiped log

D. A scheduled maintenance period

An empty audit.log file on a Linux system, despite the system being actively used, suggests that the log file has been wiped or erased. This can occur for various reasons, such as a system administrator intentionally clearing the log files for management purposes, compliance with retention policies, or as a result of a security incident where an attacker might erase logs to cover their tracks and avoid detection. In normal operations, an active and correctly configured logging system should continuously append new entries to the audit.log file, reflecting events and activities on the system. Therefore, finding this file empty implies an action that specifically removed its contents rather than a misconfiguration, malfunction, or regular maintenance activity. A configuration error would typically lead to logs not being generated at all, but not necessarily result in an existing log file being empty. A system malfunction might prevent logging, but that would usually also affect the overall logging mechanism rather than just one file being empty. Scheduled maintenance could temporarily alter logging behavior, but it does not typically include the deletion or clearing of logs.

5. What two files are commonly attacked using offline brute-force attacks?

A. The Windows SAM and the Linux /etc/shadow file

B. The Windows registry and the Linux /etc/passwd file

C. The Windows config file and the Linux /var/log/auth.log file

D. The Windows users file and the Linux /etc/group file

The two files commonly attacked using offline brute-force attacks are the Windows Security Account Manager (SAM) and the Linux /etc/shadow file. The Windows SAM file stores hashed passwords for local user accounts on a Windows operating system. When an attacker gains access to the SAM file, they can perform an offline brute-force attack, attempting to guess the passwords by comparing potential passwords against the hashed values stored in the SAM. This method is particularly effective since it does not require the attacker to interact with the system in real-time, allowing them to use significant computational resources to attempt to crack the hashes. Similarly, the /etc/shadow file in Linux contains hashed password information along with relevant password expiry data. This file is generally more secure because it is accessible only by privileged users. However, when an attacker can access the /etc/shadow file, they can also perform offline brute-force attacks to identify user passwords based on the hash values. The other options include files that either do not contain password information or are structured in a way that makes them less viable targets for offline brute-force attacks. For example, the Windows registry contains various system settings rather than password hashes, while /etc/passwd, while containing user account information, generally holds less secure, non-h

6. What action should an end user take to install an application in an environment utilizing an application allow list?

A. Download the application directly

B. Request that the application be added to the allow list

C. Contact the vendor of the application

D. Install the application without permission

In an environment that utilizes an application allow list, the correct action for an end user to take when they wish to install a new application is to request that the application be added to the allow list. This is because the allow list is a security measure that specifies which applications are permitted to run on the system. By requesting the addition of the application to the allow list, the end user is following established protocols that ensure only approved and vetted software can be installed and executed. This helps maintain system security and integrity by preventing unauthorized or potentially harmful applications from being installed. Other choices may not align with best practices for security management in such an environment. Downloading applications directly could lead to the installation of malicious software if the application is not vetted. Contacting the vendor might provide information about the software but does not address the need for permissions within the allow list framework. Installing the application without permission ignores the guidelines set forth for the environment and could introduce security vulnerabilities.

7. What type of malware is characterized by sending private workstation information to a central server?

A. A virus

B. Trojan

C. Spyware

D. Adware

Spyware is specifically designed to collect information about a user and send that data to a central server without the user's consent. This type of malware can monitor user activities, track movements and preferences, and capture sensitive information such as passwords, credit card numbers, and other private data. The primary characteristic that differentiates spyware from other types of malware is its focus on stealthy data gathering. It operates in the background, usually without the victim's knowledge, to harvest information that can be sold or used for malicious purposes. This makes it particularly dangerous, as it can compromise personal privacy and security while remaining undetected for long periods. In contrast, other types of malware, such as viruses and Trojans, may also be harmful, but they typically have different operational goals. For instance, a virus is designed to replicate and spread to other systems, while a Trojan disguises itself as legitimate software to deceive users into executing it. Adware, on the other hand, primarily focuses on delivering advertisements and may not involve the covert collection of personal data to the same extent as spyware does.

8. Which of the following is not typically a threat vector associated with SMS-based attacks?

A. SMS phishing links

B. SMS-delivered images

C. SMS text message spoofing

D. SMS account verification codes

SMS-delivered images are not typically considered a primary threat vector associated with SMS-based attacks. While it's possible for malicious content to be included in images sent via SMS, the primary threats in the context of SMS attacks often revolve around direct actions that can compromise user security or personal information. For instance, SMS phishing links actively lure users into clicking on harmful links that can lead to credential theft or malware installation. SMS text message spoofing is another significant concern, where attackers can send messages that appear to come from trusted sources, manipulating recipients into providing sensitive information. SMS account verification codes, while primarily legitimate, can also be exploited in social engineering attacks, where attackers may attempt to intercept these codes to gain unauthorized access to accounts. In contrast, SMS-delivered images do not inherently carry the same level of risk as they do not directly lead to user actions that could compromise security without further context or manipulation.

9. What characterizes ransomware?

A. Spying on user activities

B. Encrypting files for ransom

C. Displaying unwanted advertisements

D. Altering system settings to cause harm

Ransomware is primarily characterized by its method of operation, which involves encrypting files on a victim's system and demanding a ransom payment for the decryption key. This malicious software takes control of essential data, making it inaccessible to the user, and threatens to permanently delete or expose the data if the ransom is not paid. The encryption process is typically rapid and can affect a large number of files within a short time frame, leading to significant disruption for individuals or organizations. The ransom demand often comes with a time constraint, adding urgency to the situation. This technique is distinctly different from other types of malware that have varying objectives, such as spying on user activities, displaying unwanted advertisements, or altering system settings without the express intent of extorting money for the decryption of files. Thus, the main defining feature of ransomware is its focus on encrypting files with the goal of extracting a financial payment from the victim.

10. What type of deception technology involves planting documents that appear to contain sensitive information?

A. Honeyfile

B. Honeynet

C. Firewall lure

D. Decoy protocol

Honeyfiles are a type of deception technology specifically designed to enhance security by misleading potential attackers. They involve creating fake documents that are crafted to look like they contain sensitive or valuable information. When an attacker accesses these honeyfiles, they think they have found something of importance, which not only distracts them but can also trigger alerts for cybersecurity teams. The purpose of honeyfiles is to detect unauthorized access attempts, providing insight into the methods and intentions of attackers, and allowing organizations to respond proactively. By offering a bait that resembles real data, honeyfiles help to protect actual sensitive data and can deter or delay attackers by creating confusion. Other options, while related to cybersecurity, serve different purposes; for instance, honeynets consist of a network of decoy systems designed to attract, trap, and analyze attacks, but do not specifically focus on individual documents. Firewall lures and decoy protocols do not pertain directly to the planting of seemingly sensitive information, making honeyfiles the answer that best fits the question.

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://secplusmasterdeck.examzify.com

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