Security+ Master Deck Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

This is a sample study guide. To access the full version with hundreds of questions,

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

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. Don’t worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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 protocol is most commonly associated with credential relaying attacks?**

   A. LDAP

   B. NTLM

   C. Kerberos

   D. SSL

2. **If malware is exploiting unsecured network services to spread, what type of malware is most likely involved?**

   A. Ransomware

   B. Spyware

   C. Worm

   D. Virus

3. **What holds the position of the root of trust in a certificate chain?**

   A. A subordinate certificate

   B. Root certificate

   C. End-user certificate

   D. Intermediate certificate

4. **What is the best mitigation technique for keeping data and applications of different sensitivity secure in a virtualization environment?**

   A. Encryption

   B. Segmentation

   C. Redundancy

   D. Access controls

5. **What can be done to limit attack vectors associated with messaging tools like Discord and Slack?**

   A. Allow open access to all chat tools

   B. Use personal messaging accounts for discussions

   C. Deploy an organizational communication tool

   D. Monitor chats without restrictions

6. **What should Sally create to handle the possibility of a failed change in her change management process?**

   A. A backout plan

   B. A risk assessment

   C. A change approval document

   D. A communication plan

7. **What is the primary difference between agent client-based and agentless software deployments?**

   A. Agent-based systems require more maintenance

   B. Agentless software lacks a potentially vulnerable agent

   C. Agent software is always more secure

   D. Agentless systems are easier to deploy

8. **Which of the following is not considered a common vulnerability in cryptography?**

   A. Magic key attacks

   B. Key reuse

   C. Weak encryption algorithms

   D. Man-in-the-middle attacks

9. **What is the main downside of using consumer-grade routers in a business setting?**

   A. Insufficient user documentation

   B. Limited networking features

   C. Firmware patch management vulnerabilities

   D. Incompatibility with enterprise software

10. **What distinguishes phishing from other types of spam?**

    A. It is more widespread

    B. It is intended to acquire credentials or other data

    C. It is often nonsensical

    D. It targets random users

Answers

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

Explanations

1. Which protocol is most commonly associated with credential relaying attacks?

A. LDAP

B. NTLM

C. Kerberos

D. SSL

The protocol most commonly associated with credential relaying attacks is NTLM (NT LAN Manager). This is primarily due to its design and the way it handles authentication. NTLM is an authentication protocol used in Windows environments, where it has been known to be susceptible to various attacks that exploit how it processes authentication requests. In a credential relaying attack, an adversary captures NTLM hashes or tokens from one session and then reuses them to authenticate to another service as a different user. This happens because NTLM does not incorporate strong mutual authentication; it allows attackers to send authentication requests with NTLM credentials over the network without needing the original user's password. Also, because NTLM supports protocols that can be used to perform relay attacks, such as HTTP, SMB, and others, attackers can leverage these protocols to hijack credentials effectively. This highlights the vulnerabilities inherent in NTLM, especially in mixed environments using both NTLM and other more secure protocols. In contrast, LDAP (Lightweight Directory Access Protocol) is generally used for directory services and lacks the same vulnerabilities in relation to credential relaying. Kerberos, which uses tickets for authentication, provides stronger security features compared to NTLM and is designed to prevent replay attacks. SSL (Secure Sockets Layer) is

2. If malware is exploiting unsecured network services to spread, what type of malware is most likely involved?

A. Ransomware

B. Spyware

C. Worm

D. Virus

The type of malware that is most likely involved when exploiting unsecured network services to spread is a worm. Worms are designed specifically to replicate themselves and transmit from one computer to another across a network without any user intervention. Unlike viruses, which require a host file to propagate, worms take advantage of vulnerabilities in network services, allowing them to move rapidly and exploit multiple systems simultaneously. Worms can enter a network through various unsecured services, such as open ports, and they often employ techniques to find and compromise other devices connected to the same network. This capability to spread independently makes worms particularly dangerous in environments where network security is lax. While ransomware, spyware, and viruses involve compromising systems and can cause harm, their propagation mechanisms differ significantly. Ransomware typically encrypts data and demands payment to unlock it, while spyware is used primarily for surveillance and collecting information without the user’s knowledge. Viruses need to attach themselves to other executable files, requiring a host to operate, which limits their ability to spread as freely as worms do through unsecured services.

3. What holds the position of the root of trust in a certificate chain?

A. A subordinate certificate

B. Root certificate

C. End-user certificate

D. Intermediate certificate

The root of trust in a certificate chain is represented by the root certificate. This certificate is at the top of the hierarchy and serves as the foundational trust anchor for the entire chain of certificates. The root certificate is self-signed and is often embedded in browsers and operating systems, allowing them to trust certificates signed by that root authority. When a digital certificate is issued, it is typically signed by a subordinate or intermediate certificate that in turn is issued by the root certificate. This create a hierarchy that allows for a secure means of verifying the identities of entities (like websites) that hold certificates. The integrity and validity of the entire certificate chain hinge on the root certificate, which is why it is termed the "root of trust." Subordinate certificates and intermediate certificates are part of the structure that helps establish trust but do not serve as the trust anchor themselves. An end-user certificate is issued to an individual or entity, but without the root certificate, it cannot be trusted independently. Thus, the root certificate holds a unique and critical role in the certificate hierarchy.

4. What is the best mitigation technique for keeping data and applications of different sensitivity secure in a virtualization environment?

A. Encryption

B. Segmentation

C. Redundancy

D. Access controls

Segmentation is the best mitigation technique for keeping data and applications of different sensitivity secure in a virtualization environment because it involves dividing the virtualized environment into distinct segments or sections. This separation ensures that sensitive data and applications are isolated from less sensitive ones, which limits the risk of unauthorized access and potential data leaks. In a virtualized environment, multiple virtual machines (VMs) often operate on the same physical hardware. By applying segmentation, each VM can have its own set of security policies, resources, and access controls tailored to the specific sensitivity of the data it handles. This means that even if one segment is compromised, the breach is contained, preventing it from affecting more sensitive segments. Moreover, segmentation can be implemented through various means, such as creating virtual LANs (VLANs) or using firewalls to enforce rules between segments, further enhancing security. Segmentation also helps in compliance with regulatory requirements, as it allows organizations to demonstrate that they are taking appropriate measures to safeguard sensitive information. In contrast, while encryption, redundancy, and access controls are also important security measures, they serve different purposes or operate on different principles. Encryption protects data at rest or in transit by making it unreadable without the appropriate keys, but it does not inherently isolate different

5. What can be done to limit attack vectors associated with messaging tools like Discord and Slack?

A. Allow open access to all chat tools

B. Use personal messaging accounts for discussions

C. Deploy an organizational communication tool

D. Monitor chats without restrictions

Deploying an organizational communication tool is an effective strategy to limit attack vectors associated with messaging tools such as Discord and Slack. When organizations use dedicated communication platforms, they can implement tailored security measures suited to their specific needs. These tools often come with built-in security features, such as encryption, access controls, user authentication, and audit logs, which are designed to minimize risks like data breaches, unauthorized access, and phishing attempts. Furthermore, using an organizational tool allows for better compliance with regulatory requirements regarding data handling and privacy since they can be configured to meet specific compliance standards. In contrast, allowing open access to all chat tools can lead to insecure use of potentially unmonitored applications, increasing the risk of data leakage. Using personal messaging accounts for discussions can create challenges in data governance and security, as these platforms lack organizational oversight, making sensitive information vulnerable. Monitoring chats without restrictions can raise privacy concerns and might not adequately address potential security risks, as it does not involve proactive measures to secure the communications themselves. Thus, opting for an organizational communication tool provides a structured and secure environment for interaction, significantly mitigating risks associated with messaging applications.

6. What should Sally create to handle the possibility of a failed change in her change management process?

A. A backout plan

B. A risk assessment

C. A change approval document

D. A communication plan

To effectively manage the risks associated with changes in a system or network, it is essential to have a structured way to address potential failures during the change process. A backout plan serves this purpose by outlining the necessary steps to revert to the previous state if the change results in unforeseen issues or failures. Having a backout plan ensures that if a change does not produce the desired outcome or creates problems, there is a predefined path to restore the system to its last known good configuration. This minimizes downtime and service disruption, thereby helping maintain operational continuity. While a risk assessment helps identify potential risks before a change is implemented, and a change approval document formalizes the authorization for the implementation of changes, these do not directly address the actions needed to recover from a failed change. Furthermore, a communication plan is crucial for keeping stakeholders informed but does not provide a method for handling failures. Thus, the creation of a backout plan is a proactive measure specifically designed to manage the consequences of unsuccessful changes.

7. What is the primary difference between agent client-based and agentless software deployments?

A. Agent-based systems require more maintenance

B. Agentless software lacks a potentially vulnerable agent

C. Agent software is always more secure

D. Agentless systems are easier to deploy

The primary difference between agent client-based and agentless software deployments revolves around the presence of an agent on the client device. In an agent-based deployment, software requires the installation of a dedicated agent on each individual client machine. These agents facilitate communication and data collection between the client device and the management server, making it possible to monitor and manage the system more effectively. However, this means that the software can also introduce potential vulnerabilities, as the agents themselves can become targets of attacks. In contrast, agentless software deployment does not require installing an agent on client devices. Instead, it typically utilizes existing protocols or services, which can significantly reduce the attack surface. By eliminating the need for an installed agent, agentless solutions inherently lack a potentially vulnerable component that could be exploited. This feature not only enhances security by reducing possible entry points for threats but also simplifies management since there are no agents needing regular updates, patches, or configurations on individual client machines. While it's true that agent-based systems may require more ongoing maintenance and that agentless systems can generally be easier to deploy, these elements are secondary to the fundamental architectural cornerstone that defines the difference: the presence or absence of an agent. The option indicating that agentless software lacks a potentially vulnerable agent succinctly encapsulates

8. Which of the following is not considered a common vulnerability in cryptography?

A. Magic key attacks

B. Key reuse

C. Weak encryption algorithms

D. Man-in-the-middle attacks

Magic key attacks are not commonly recognized as standard vulnerabilities in cryptography. The term is somewhat ambiguous and does not refer to a specific, well-documented attack methodology within cryptographic practices. Instead, it may imply problems related to key handling or management in a more speculative or informal way. In contrast, key reuse is a significant vulnerability where the same cryptographic key is used across multiple sessions or systems, increasing the risk that if that key is compromised, all associated data becomes vulnerable. Weak encryption algorithms pose a crucial threat as they are easier to break using modern computing power, rendering encrypted information insecure. Man-in-the-middle attacks represent a significant risk in communication channels, where an unauthorized entity intercepts and possibly alters messages between two parties, thereby undermining the integrity and confidentiality of the data being transmitted. Understanding these vulnerabilities helps in implementing better security practices and selecting robust cryptographic methods.

9. What is the main downside of using consumer-grade routers in a business setting?

A. Insufficient user documentation

B. Limited networking features

C. Firmware patch management vulnerabilities

D. Incompatibility with enterprise software

Using consumer-grade routers in a business setting primarily presents the downside of firmware patch management vulnerabilities. This stems from the fact that consumer-grade devices are often not designed with the same level of security in mind as enterprise-grade equipment. Manufacturers may not provide regular firmware updates or adequate support for security patches, leaving the devices susceptible to exploitation from newly discovered vulnerabilities. In a business environment, where data security is paramount, relying on consumer-grade routers can expose the network to significant risks. These devices may not receive timely updates to protect against emerging threats, which can compromise sensitive business data and lead to breaches. Consequently, the lack of robust firmware management and patching contributes to a weaker overall security posture compared to dedicated business solutions, which typically prioritize regular updates and security patches to safeguard network environments.

10. What distinguishes phishing from other types of spam?

A. It is more widespread

B. It is intended to acquire credentials or other data

C. It is often nonsensical

D. It targets random users

Phishing is specifically designed with the intent of acquiring sensitive information, such as usernames, passwords, and financial details, from individuals. This distinguishes it from other forms of spam, which may aim to advertise products or services rather than directly steal personal information. In phishing attacks, the perpetrator typically poses as a trustworthy entity, such as a bank or a well-known company, to manipulate targets into divulging their credentials or clicking on malicious links. This targeted approach is what sets phishing apart as a more serious threat compared to general spam, which may be less focused and often lacks the intent to gather sensitive information.   While phishing can indeed be widespread, and it sometimes targets random users, these characteristics do not define what phishing is. The nonsensical nature of some spam is also not a defining factor since phishing attempts are usually crafted to appear legitimate.

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!