# CompTIA Security+ (SY0-601) 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. 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 of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?**

   **A. OWASP**

   **B. Vulnerability scan results**

   **C. NIST CSF**

   **D. Third-party libraries**

2. **Which of the following attacks is likely associated with changes made to a vendor's IP address during an investigation?**

   **A. Man-in-the middle**

   **B. Evil twin**

   **C. DNS poisoning**

   **D. Spear-phishing**

3. **If an attacker is using a zero-day exploit, what does this imply?**

   **A. It's a previously known vulnerability.**

   **B. The software has a patch available.**

   **C. It is newly discovered and unpatched.**

   **D. The vulnerability has been documented and published.**

4. **What security principle focuses on limiting a user's access to only what is necessary to perform their job?**

   **A. Least privilege**

   **B. Defense in depth**

   **C. Segregation of duties**

   **D. Separation of concerns**

5. **When negotiating with a new vendor, what should be included to address response times to major incidents?**

   **A. MOU**

   **B. MTTR**

   **C. SLA**

   **D. NDA**

**6. In response to a data breach, what immediate action should be taken?**

**A. Review user permissions**

**B. Change passwords for all accounts**

**C. Notify affected individuals**

**D. Conduct a threat assessment**

**7. Which of the following BEST describes a method to ensure ongoing assessments of security program effectiveness?**

**A. Regular audits**

**B. Ad-hoc penetration testing**

**C. Annual policy reviews**

**D. Vulnerability scanning**

**8. What biometrics are MOST likely to be used for authentication at country borders without the need for enrollment?**

**A. Voice and Vein**

**B. Gait and Facial**

**C. Vein and Retina**

**D. Gait and Facial**

**9. What should a security administrator implement to prevent unauthorized program installations by users with administrative access?**

**A. Application code signing**

**B. Application whitelisting**

**C. Data loss prevention**

**D. Web application firewalls**

**10. What should a security administrator do upon discovering unknown devices connected to a company's wireless network?**

**A. Enable MAC filtering on the switches**

**B. Deploy multifactor authentication for access**

**C. Scan the network for rogue access points**

**D. Run a vulnerability scan on all devices**

# Answers

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

# Explanations

## 1. Which of the following would be the BEST resource for a software developer who is looking to improve secure coding practices for web applications?

**A. OWASP**

**B. Vulnerability scan results**

**C. NIST CSF**

**D. Third-party libraries**

**The most suitable resource for a software developer aiming to enhance secure coding practices for web applications is the OWASP (Open Web Application Security Project). OWASP is a well-respected organization that provides a wealth of information specifically focused on improving the security of software, particularly web applications. Their resources include foundational guidelines, best practices, and tools that address common security vulnerabilities, such as those outlined in their OWASP Top Ten Project, which highlights the most critical security risks to web applications. By utilizing OWASP's resources, a developer can gain insight into not only what vulnerabilities to look out for, but also how to implement secure practices in coding to mitigate those risks right from the start. The comprehensive guides and checklists available through OWASP can significantly aid developers in integrating security-focused code practices into their application development lifecycle. Other options, while valuable in different contexts, do not specifically cater to improving secure coding practices in the same targeted way. Vulnerability scan results provide insights into existing issues but do not offer proactive guidance on coding practices. The NIST CSF (Cybersecurity Framework) is a broader framework meant for organizational risk management and cybersecurity practices and is less focused on coding specifics. Third-party libraries are critical for functionality but may not necessarily address security best practices,**

## 2. Which of the following attacks is likely associated with changes made to a vendor’s IP address during an investigation?

**A. Man-in-the middle**

**B. Evil twin**

**C. DNS poisoning**

**D. Spear-phishing**

**The attack most likely associated with changes made to a vendor’s IP address during an investigation is DNS poisoning. This type of attack manipulates DNS (Domain Name System) records to redirect users from legitimate sites to fraudulent ones. During an investigation, if the IP address associated with a vendor's domain is altered, this could indicate that the DNS records were compromised—enabling attackers to control and divert traffic meant for a legitimate destination to a malicious site. In the context of an investigation, examining changes in a vendor's IP address might reveal attempted DNS poisonings, where attackers aim to exploit vulnerabilities in the DNS system to mislead users or conduct further attacks. This aligns with the nature of DNS poisoning, which fundamentally relies on altering IP address mappings in DNS records to disrupt normal operations and lead users to harmful sites.**

## 3. If an attacker is using a zero-day exploit, what does this imply?

**A. It’s a previously known vulnerability.**

**B. The software has a patch available.**

**C. It is newly discovered and unpatched.**

**D. The vulnerability has been documented and published.**

**Selecting the option that indicates a zero-day exploit refers to a newly discovered and unpatched vulnerability captures the essence of what a zero-day exploit signifies. A zero-day exploit takes advantage of a security flaw that has been identified by attackers before the software developer has created and released a fix. This means that there are no defensive measures or patches available at the time of the attack, leaving systems vulnerable to exploitation. The term "zero-day" derives from the fact that the software vendor has had zero days to address and patch the vulnerability since it was discovered. This underscores the urgency and danger associated with zero-day exploits, as they can be utilized for various malicious activities before defenses can be established. Since these vulnerabilities are unpatched, they represent significant risks for organizations maintaining the affected software. Understanding this concept is crucial for security professionals, as it indicates the need for proactive security measures, such as intrusion detection systems and continuous monitoring, to identify and mitigate potential attacks exploiting such vulnerabilities.**

## 4. What security principle focuses on limiting a user’s access to only what is necessary to perform their job?

**A. Least privilege**

**B. Defense in depth**

**C. Segregation of duties**

**D. Separation of concerns**

**The principle of least privilege is fundamental in security practices, aiming to minimize the access rights for users to only those necessary for them to fulfill their specific job functions. This approach reduces the risk of accidental or malicious misuse of permissions and helps protect sensitive information by ensuring that users cannot access data or systems they do not need for their work. By implementing least privilege, organizations limit the potential attack surface, making it more difficult for unauthorized users to exploit vulnerabilities within systems. In a workplace environment, applying this principle would mean that if an employee requires access to a particular database to perform their duties, they would be granted permissions only for that database and not for any other systems or data that they don't need. This not only strengthens overall security but also aids in compliance with various regulations that may govern data protection and privacy, as it ensures that individuals only handle data pertinent to their roles.**

## 5. When negotiating with a new vendor, what should be included to address response times to major incidents?

**A. MOU**

**B. MTTR**

**C. SLA**

**D. NDA**

**Including a Service Level Agreement (SLA) in negotiations with a new vendor is essential when addressing response times to major incidents. An SLA is a formal contract that outlines the expected level of service between a service provider and a customer. It specifically defines metrics such as response times, availability, and responsibilities regarding service delivery. In the context of incidents, the SLA will typically specify how quickly the vendor must respond to different severity levels of incidents, which ensures that both parties have a clear understanding of the expectations. This can be critical for maintaining business continuity and ensuring that any disruptions are minimized. In contrast, a Memorandum of Understanding (MOU) is generally a non-binding agreement that outlines the intentions of the parties involved but does not provide the detailed service metrics that an SLA does. Mean Time to Recovery (MTTR) is a specific metric that measures how quickly a system can be restored after a failure but does not constitute an agreement itself. A Non-Disclosure Agreement (NDA) is focused on confidentiality and protecting sensitive information rather than service performance metrics. Therefore, while all these documents have their importance in vendor relationships, the SLA is the appropriate choice for addressing response times in the context of major incidents.**

## 6. In response to a data breach, what immediate action should be taken?

**A. Review user permissions**

**B. Change passwords for all accounts**

**C. Notify affected individuals**

**D. Conduct a threat assessment**

**Changing passwords for all accounts is a crucial and immediate action to take in response to a data breach. This step helps to secure accounts that may have been compromised during the breach, especially if there's a chance that attackers have gained access to specific credentials. By changing passwords, organizations can reduce the risk of further unauthorized access and control the situation more effectively. While reviewing user permissions, notifying affected individuals, and conducting a threat assessment are important parts of the broader response plan to a data breach, they typically follow the immediate need to secure access through password changes. Effectively, communication and audits are critical, but they do not provide instant mitigation of a breach's immediate impact. The priority must be to safeguard sensitive information by ensuring that all accounts are secure against further access.**

## 7. Which of the following BEST describes a method to ensure ongoing assessments of security program effectiveness?

**A. Regular audits**

**B. Ad-hoc penetration testing**

**C. Annual policy reviews**

**D. Vulnerability scanning**

**Regular audits represent a systematic approach to evaluating the effectiveness of a security program over time. By conducting audits on a consistent basis, organizations can assess compliance with established security policies and standards, identify gaps in security controls, and evaluate the overall performance of their security measures. This method provides insights into how well the security program is working and highlights areas that may need improvement or adjustment. While ad-hoc penetration testing, annual policy reviews, and vulnerability scanning are all important components of a comprehensive security strategy, they don't offer the same level of ongoing oversight as regular audits. Ad-hoc penetration testing typically occurs sporadically and focuses on specific vulnerabilities rather than the broader effectiveness of security measures. Annual policy reviews may not capture real-time changes in the threat landscape or security posture. Vulnerability scanning is useful for identifying weaknesses but does not necessarily evaluate the operational impact or the effectiveness of the security program as a whole. Regular audits, therefore, provide a continuous assessment framework that is vital for maintaining an effective security program.**

## 8. What biometrics are MOST likely to be used for authentication at country borders without the need for enrollment?

**A. Voice and Vein**

**B. Gait and Facial**

**C. Vein and Retina**

**D. Gait and Facial**

**The selection of gait and facial recognition as the most likely biometrics for authentication at country borders without enrollment highlights the strengths of these modalities in real-world applications. Facial recognition technology can quickly identify individuals based on their unique facial features, and many border control systems are already equipped with cameras capable of capturing and processing facial images in real-time. This technology allows for rapid verification against a database of known individuals without requiring prior enrollment, making it particularly advantageous in high-traffic areas like international borders. Gait recognition adds another layer of passive identification, analyzing how a person walks. This biometric does not require cooperation from the individual, making it useful for surveillance and automated border control systems. It functions effectively in conjunction with facial recognition to help enhance accuracy and speed in identifying individuals as they move through border checkpoints. In contrast, other options such as voice, vein, and retina recognition typically require more specialized equipment and may necessitate pre-enrollment to create a template for verification. Voice recognition is often prone to variations due to emotional state or background noise, while vein and retina recognition require close-range and specific conditions for accuracy. Therefore, the combination of gait and facial recognition stands out as practical and implementable for border authentication without the need for enrollment, facilitating smoother and more**

## 9. What should a security administrator implement to prevent unauthorized program installations by users with administrative access?

**A. Application code signing**

**B. Application whitelisting**

**C. Data loss prevention**

**D. Web application firewalls**

**Application whitelisting is the correct method for preventing unauthorized program installations by users with administrative access. This approach involves creating a list of approved applications that are authorized to run on a system. Only the programs that are explicitly included in this list can be executed. This means that even if a user has administrative rights, they will not be able to install or run any software that has not been pre-approved and entered into the whitelist. This technique is particularly effective in environments where security needs to be tightly controlled, as it minimizes the risk posed by malicious software or unauthorized applications, which can lead to security breaches or system vulnerabilities. By enforcing that only whitelisted applications can be installed or executed, the security administrator significantly reduces the attack surface available to potential threats. While application code signing can validate the authenticity and integrity of applications, it does not inherently prevent installation. Data loss prevention focuses on protecting sensitive data rather than controlling software installations, and web application firewalls are designed to protect web applications from various attack vectors but do not restrict the installation of software on a system.**

## 10. What should a security administrator do upon discovering unknown devices connected to a company's wireless network?

**A. Enable MAC filtering on the switches**

**B. Deploy multifactor authentication for access**

**C. Scan the network for rogue access points**

**D. Run a vulnerability scan on all devices**

**Enabling MAC filtering on the switches is one potential method for managing unknown devices connected to a company's wireless network. This approach allows the security administrator to define which devices are permitted to connect to the network based on their Media Access Control (MAC) addresses. By doing so, it can help in restricting access to only trusted devices, essentially blocking unknown or rogue devices from utilizing network resources. However, while MAC filtering can be a useful layer of security, it is important to note that it has its limitations, such as being susceptible to MAC address spoofing, where an attacker can mimic the MAC address of an approved device. Therefore, it should be used in conjunction with other security measures. Scanning the network for rogue access points addresses the immediate concern of unauthorized connections by identifying any potentially malicious devices that could intercept or manipulate data on the network. Deploying multifactor authentication strengthens access security further by requiring multiple forms of verification before granting network access, which is important but does not directly resolve the issue of unknown devices already connected. Running a vulnerability scan on all devices is also valuable for identifying potential security weaknesses but may not address the more pressing concern of how unknown devices gained initial access to the network. In summary, enabling MAC filtering can be an initial step to mitigate**

# 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://comptiasecplussy0601.examzify.com**

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