# CompTIA Security+ (SY0-601) Certification Practice Test (Sample)

## Study Guide


**Everything you need from our exam experts!**

# 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. **What is the most likely cause of a forensic examiner receiving an error while attempting to dump passwords from physical memory?**

   **A. The examiner does not have administrative privileges to the system**

   **B. The system must be taken offline before a snapshot can be created**

   **C. Checksum mismatches are invalidating the disk image**

   **D. The swap file needs to be unlocked before it can be accessed**

3. **What is an important function of a security control matrix?**

   **A. To define security policies**

   **B. To map vulnerabilities to specific security controls**

   **C. To implement security measures**

   **D. To ensure network connectivity**

4. **For a company that handles sensitive data, which access control model is BEST to implement for data protection?**

   **A. Discretionary**

   **B. Rule-based**

   **C. Role-based**

   **D. Mandatory**

5. **What type of attack is likely responsible for multiple failed logins before a successful entry occurs?**

   **A. Dictionary**

   **B. Credential-stuffing**

   **C. Password-spraying**

   **D. Brute-force**

**6. 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**

**7. What is the primary purpose of using a mantrap in physical security?**

**A. To alert security personnel to unauthorized access**

**B. To control access to secure areas**

**C. To provide surveillance of entrances**

**D. To enhance lighting in a facility**

**8. After a ransomware attack, a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. What will the company MOST likely review to trace this transaction?**

**A. The public ledger**

**B. The NetFlow data**

**C. A checksum**

**D. The event log**

**9. What control is likely recommended for restricting access to certain network segments using data-link layer security?**

**A. MAC**

**B. ACL**

**C. BPDU**

**D. ARP**

**10. After a security issue with website access, what attack most likely occurred on the original DNS server?**

**A. Domain hijacking**

**B. DNS cache poisoning**

**C. Distributed denial-of-service**

**D. DNS tunneling**

# Answers

**1. A**
**2. A**
**3. B**
**4. D**
**5. D**
**6. A**
**7. B**
**8. A**
**9. A**
**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. What is the most likely cause of a forensic examiner receiving an error while attempting to dump passwords from physical memory?

**A. The examiner does not have administrative privileges to the system**

**B. The system must be taken offline before a snapshot can be created**

**C. Checksum mismatches are invalidating the disk image**

**D. The swap file needs to be unlocked before it can be accessed**

**Administrative privileges are often necessary for tasks that involve accessing protected system resources, such as memory. When analyzing memory or dumping passwords from physical memory, the forensic examiner needs the right level of access to perform these operations. Without administrative privileges, the system may restrict access to sensitive areas of memory that contain the password data, leading to errors during the process. The other options, while they may address different potential issues, do not directly relate to the common requirement for sufficient access rights when working with system memory. For example, taking a system offline may help to ensure a clean snapshot, but it's not a requirement in all cases, especially for live analysis. Checksum mismatches are relevant to the integrity of disk images rather than memory access issues, and the swap file needing to be unlocked pertains to virtual memory management rather than the immediate access to physical memory for password retrieval.**

## 3. What is an important function of a security control matrix?

**A. To define security policies**

**B. To map vulnerabilities to specific security controls**

**C. To implement security measures**

**D. To ensure network connectivity**

**A security control matrix serves a crucial role in the realm of risk management and information security by mapping vulnerabilities to specific security controls. This mapping allows organizations to identify which security measures are applicable to particular risks and vulnerabilities they face. By establishing a clear relationship between identified security vulnerabilities and their corresponding controls, a security control matrix enables organizations to prioritize their security efforts effectively. It also helps in ensuring that adequate safeguards are in place to mitigate potential threats, thus enhancing overall security posture. In contrast, while defining security policies is essential for guiding an organization's security approach, it is not the primary function of a security control matrix. Implementing security measures is an operational task that stems from the planning and analysis performed using a matrix, but the matrix itself does not directly implement controls. Similarly, ensuring network connectivity is not related to the function of a security control matrix, as it primarily focuses on security rather than connectivity concerns.**

## 4. For a company that handles sensitive data, which access control model is BEST to implement for data protection?

**A. Discretionary**

**B. Rule-based**

**C. Role-based**

**D. Mandatory**

**The mandatory access control model is particularly suitable for organizations that manage sensitive data due to its stringent and predefined control mechanisms that limit user access based on classification levels and security clearances. In this model, access to resources is determined by the system, not the user, which significantly reduces the risk of unauthorized access. Mandatory access control designs are built around a clear set of policies that dictate access levels to data, ensuring that only users with the appropriate clearance can access sensitive information. This is crucial in environments dealing with highly sensitive data, as it prevents users from unilaterally granting access or modifying permissions that could lead to data breaches or leaks. Additionally, this model enhances compliance with regulatory requirements relevant to data protection, which is vital for companies handling sensitive information. The automated and enforced nature of the access control also aids in auditing and monitoring access attempts, which contributes further to data security. In contrast, other models such as discretionary access control allow users to manage permissions, which can lead to inconsistencies and vulnerabilities. Rule-based models offer specific criteria for access based on conditions but may lack the comprehensive controls present in mandatory access. Role-based access control, while effective, is still based on user roles that may not cover every aspect of data sensitivity and security clearance,**

## 5. What type of attack is likely responsible for multiple failed logins before a successful entry occurs?

**A. Dictionary**

**B. Credential-stuffing**

**C. Password-spraying**

**D. Brute-force**

**A brute-force attack involves systematically attempting every possible combination of passwords until the correct one is found. This method often leads to multiple failed login attempts being recorded before a successful login occurs, as the attacker tries a wide range of potential passwords. In contrast, a dictionary attack uses a pre-defined list of likely passwords (such as common words or phrases) and operates in a similar way to brute-force but is typically faster because it does not attempt every possible combination. Credential stuffing exploits users' reused passwords across different sites; thus, it aims for success with minimal failed attempts since attackers use passwords obtained from previous data breaches. Password spraying, on the other hand, involves using a smaller set of commonly used passwords across many accounts, resulting in a few failed attempts before potentially hitting a successful login. Brute-force attacks are characterized by their exhaustive nature and are the type of attack most responsible for the pattern of many failed attempts followed by eventual success.**

## 6. 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**

## 7. What is the primary purpose of using a mantrap in physical security?

**A. To alert security personnel to unauthorized access**

**B. To control access to secure areas**

**C. To provide surveillance of entrances**

**D. To enhance lighting in a facility**

**The primary purpose of using a mantrap in physical security is to control access to secure areas. A mantrap is a physical security mechanism that consists of a small space with two interlocking doors, where an individual must pass through one door before the other can open. This design prevents individuals from bypassing security measures, as they cannot enter the secure area without proper authentication or verification. By controlling access in this way, mantraps enhance overall security by ensuring that only authorized personnel can enter sensitive areas. They reduce the risk of unauthorized entry and help maintain a secure environment by making it easy to monitor and manage who is granted access. This is particularly valuable in high-security environments such as data centers, laboratories, or secure government facilities. Other options serve different purposes. For instance, alerting security personnel to unauthorized access involves monitoring systems like alarms or surveillance cameras, while enhancing lighting improves visibility but does not directly control access. Similarly, providing surveillance of entrances helps in observation but lacks the restrictive physical control that a mantrap offers.**

## 8. After a ransomware attack, a forensics company needs to review a cryptocurrency transaction between the victim and the attacker. What will the company MOST likely review to trace this transaction?

**A. The public ledger**

**B. The NetFlow data**

**C. A checksum**

**D. The event log**

**The public ledger is the most suitable option for tracing a cryptocurrency transaction following a ransomware attack because cryptocurrencies like Bitcoin use a decentralized ledger known as the blockchain. This ledger records all transactions publicly, allowing anyone to view and verify the movement of funds. Each transaction is linked to a specific public address, enabling forensic analysts to trace the flow of funds between the victim and the attacker by examining the detailed transaction history. The public nature of the ledger means that even though the transaction details do not reveal the identities of the parties involved, they provide a fixated pathway of the transaction, which forensic investigators can analyze to potentially identify the sender or recipient addresses. Additionally, if the attacker converts the cryptocurrency to another asset or fiat currency, tracking those transactions along the public ledger can provide crucial evidence. While NetFlow data is useful for monitoring network traffic and can provide insights into malicious activity, it does not directly detail cryptocurrency transactions. A checksum checks the integrity of data but does not pertain to transaction verification. The event log typically records system or application activities, which is not specifically aligned with tracing the movement of cryptocurrency.**

## 9. What control is likely recommended for restricting access to certain network segments using data-link layer security?

**A. MAC**

**B. ACL**

**C. BPDU**

**D. ARP**

**The recommended control for restricting access to certain network segments using data-link layer security is based on the use of MAC (Media Access Control) addresses. MAC addresses are unique identifiers assigned to network interfaces for communications on the physical network segment. By implementing MAC address filtering, network administrators can define which devices are allowed access to a specific network segment and which are not. This control operates at the data-link layer (Layer 2) of the OSI model, where it can specifically allow or deny traffic based on the MAC address of devices attempting to connect. This approach is effective in scenarios where you want to limit access to physical network segments based on the device's MAC address, ensuring that only authorized devices can communicate on that part of the network. Other options like ACL (Access Control List) usually operate at higher layers and are not focused solely on the data-link layer, making them less applicable in this specific context. BPDU (Bridge Protocol Data Unit) is related to maintaining loop-free topologies in networks and does not serve the purpose of access control in the same way. ARP (Address Resolution Protocol) is used for mapping IP addresses to MAC addresses but is not a control mechanism for restricting access. Therefore, using MAC addresses aligns perfectly with restricting access**

## 10. After a security issue with website access, what attack most likely occurred on the original DNS server?

**A. Domain hijacking**

**B. DNS cache poisoning**

**C. Distributed denial-of-service**

**D. DNS tunneling**

**The context of this question revolves around vulnerability in the DNS server that impacts website access. The best option that aligns with the described scenario is DNS cache poisoning. When a DNS cache is poisoned, the DNS server caches fraudulent entries, allowing an attacker to redirect traffic from a legitimate site to a malicious one. When users attempt to access the original website, they are unknowingly sent to a different, potentially harmful location, which aligns with the issue of compromised access. This attack exploits the way DNS servers temporarily store resolved entries to enhance efficiency. If an attacker can supply false information to the server, it can create a situation where users encounter incorrect or dangerous sites without their knowledge, leading to the described "security issue with website access." In contrast, options like domain hijacking involve taking control of a domain name itself, which does not directly affect DNS server functionality. A distributed denial-of-service attack targets the availability of services but does not alter DNS records. Lastly, DNS tunneling is a technique used to encapsulate data within DNS queries but isn't directly related to impairing access due to compromised DNS entries. Thus, the focus on the alteration of DNS cache entries makes DNS cache poisoning the most appropriate answer.**