



**CertsMania**

## **Free Questions for SY0-701**

Shared by **Balaji** on **Feb 10, 2026**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**



**CertsMania**

## Questions # 1:

A small business uses kiosks on the sales floor to display product information for customers. A security team discovers the kiosks use end-of-life operating systems. Which of the following is the security team most likely to document as a security implication of the current architecture?

### Options:

- A.  
Patch availability
- B.  
Product software compatibility
- C.  
Ease of recovery
- D.  
Cost of replacement



CertsMania

### Answer

A

### Explanation

End-of-life operating systems are those that are no longer supported by the vendor or manufacturer, meaning they do not receive any security updates or patches. This makes them vulnerable to exploits and attacks that take advantage of known or unknown flaws in the software. Patch availability is the security implication of using end-of-life operating systems, as it affects the ability to fix or prevent security issues. Other factors, such as product software compatibility, ease of recovery, or cost of replacement, are not directly related to security, but rather to functionality, availability, or budget. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 29 1

## Questions # 2:

Which of the following involves an attempt to take advantage of database misconfigurations?

**Options:**

A.

Buffer overflow

B.

SQL injection

C.

VM escape

D.

Memory injection



CertsMania

**Answer**

B

**Explanation**

SQL injection is a type of attack that exploits a database misconfiguration or a flaw in the application code that interacts with the database. An attacker can inject malicious SQL statements into the user input fields or the URL parameters that are sent to the database server. These statements can then execute unauthorized commands, such as reading, modifying, deleting, or creating data, or even taking over the database server. SQL injection can compromise the confidentiality, integrity, and availability of the data and the system. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215 1

Questions # 3:

Which of the following vulnerabilities would likely be mitigated by setting up an MDM platform?

**Options:**

A.

TPM

B.



CertsMania

Buffer overflow

C.

Jailbreaking

D.

SQL injection



CertsMania

## Answer

C

## Explanation

A Mobile Device Management (MDM) platform protects organizational mobile devices by enforcing security policies, restricting unauthorized configuration changes, and detecting compromised devices. One of the major vulnerabilities MDM mitigates is jailbreaking, which occurs when a user removes manufacturer restrictions to gain unrestricted access to the file system and install unapproved apps.

Security+ SY0-701 explains that jailbroken devices:

Bypass built-in security protections

Are more susceptible to malware

Can be used for data exfiltration

Violate corporate mobile security policies

MDM solutions detect jailbroken or rooted devices and automatically block them from accessing corporate resources, enforce compliance rules, and remotely wipe devices if necessary.

TPM (A) is a hardware security chip unrelated to MDM. Buffer overflow (B) and SQL injection (D) are software development vulnerabilities, not mobile device policy issues.

Thus, the correct answer is C: Jailbreaking.

## Questions # 4:

Which of the following should a security team do first before a new web server goes live?

**Options:**

A.

Harden the virtual host.

B.

Create WAF rules.

C.

Enable network intrusion detection.

D.

Apply patch management



CertsMania

**Answer**

D

Questions # 5:

Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.

**INSTRUCTIONS**

Not all attacks and remediation actions will be used.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

>



CertsMania

**Options:**

**Answer**

Answer: >

**Explanation**

Web server Botnet Enable DDoS protection User RAT Implement a host-based IPS Database server Worm Change the default application password Executive Keylogger Disable

vulnerable servicesApplication Backdoor Implement 2FA using push notification

> A screenshot of a computer program Description automatically generated with low confidence

#### Questions # 6:

Which of the following is the most effective way to protect an application server running software that is no longer supported from network threats?

#### Options:

A.

Air gap

B.

Barricade

C.

Port security

D.

Screen subnet

#### Answer

A

#### Explanation

Air-gapping is the most effective way to protect an application server running unsupported software from network threats. By physically isolating the server from any network connection (no wired or wireless communication), it is protected from external cyber threats. While other options like port security or a screened subnet can provide some level of protection, an air gap offers the highest level of security by preventing any network-based attacks entirely.

References =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.

CompTIA Security+ SY0-601 Study Guide: Chapter on Secure System Design.

## Questions # 7:

Which of the following enables the use of an input field to run commands that can view or manipulate data?

### Options:

A.

Cross-site scripting

B.

Side loading

C.

Buffer overflow

D.

SQL injection



CertsMania

### Answer

D

### Explanation

= SQL injection is a type of attack that enables the use of an input field to run commands that can view or manipulate data in a database. SQL stands for Structured Query Language, which is a language used to communicate with databases. By injecting malicious SQL statements into an input field, an attacker can bypass authentication, access sensitive information, modify or delete data, or execute commands on the server. SQL injection is one of the most common and dangerous web application vulnerabilities. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 195. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1, page 8.

## Questions # 8:

A company is adding a clause to its AUP that states employees are not allowed to modify the operating system on mobile devices. Which of the following vulnerabilities is the organization addressing?

**Options:**

A.

Cross-site scripting

B.

Buffer overflow

C.

Jailbreaking

D.

Side loading



CertsMania

**Answer**

C

**Explanation**

Jailbreaking is the process of removing the restrictions imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking allows users to install unauthorized applications, modify system settings, and access root privileges. However, jailbreaking also exposes the device to potential security risks, such as malware, spyware, unauthorized access, data loss, and voided warranty. Therefore, an organization may prohibit employees from jailbreaking their mobile devices to prevent these vulnerabilities and protect the corporate data and network. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Mobile Device Security, page 507 2

Questions # 9:

A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

**Options:**

A.

Place posters around the office to raise awareness of common phishing activities.

○ B.

Implement email security filters to prevent phishing emails from being delivered

○ C.

Update the EDR policies to block automatic execution of downloaded programs.

○ D.

Create additional training for users to recognize the signs of phishing attempts.

## Answer

C

## Explanation

An endpoint detection and response (EDR) system is a security tool that monitors and analyzes the activities and behaviors of endpoints, such as computers, laptops, mobile devices, and servers. An EDR system can detect, prevent, and respond to various types of threats, such as malware, ransomware, phishing, and advanced persistent threats (APTs). One of the features of an EDR system is to block the automatic execution of downloaded programs, which can prevent malicious code from running on the endpoint when a user clicks on a link in a phishing message. This can reduce the impact of a phishing attack and protect the endpoint from compromise. Updating the EDR policies to block automatic execution of downloaded programs is a technical control that can mitigate the risk of phishing, regardless of the user's awareness or behavior. Therefore, this is the best answer among the given options.

The other options are not as effective as updating the EDR policies, because they rely on administrative or physical controls that may not be sufficient to prevent or stop a phishing attack. Placing posters around the office to raise awareness of common phishing activities is a physical control that can increase the user's knowledge of phishing, but it may not change their behavior or prevent them from clicking on a link in a phishing message. Implementing email security filters to prevent phishing emails from being delivered is an administrative control that can reduce the exposure to phishing, but it may not be able to block all phishing emails, especially if they are crafted to bypass the filters. Creating additional training for users to recognize the signs of phishing attempts is an administrative control that can improve the user's skills of phishing detection, but it may not guarantee that they will always be vigilant or cautious when receiving an email. Therefore, these options are not the best answer for this question. References = Endpoint Detection and Response - CompTIA Security+ SY0-701 - 2.2, video at 5:30; CompTIA Security+ SY0-701 Certification Study Guide, page 163.

A software development manager wants to ensure the authenticity of the code created by the company. Which of the following options is the most appropriate?

**Options:**

A.

Testing input validation on the user input fields

B.

Performing code signing on company-developed software

C.

Performing static code analysis on the software

D.

Ensuring secure cookies are use

**Answer**

B

**Explanation**

Code signing is a technique that uses cryptography to verify the authenticity and integrity of the code created by the company. Code signing involves applying a digital signature to the code using a private key that only the company possesses. The digital signature can be verified by anyone who has the corresponding public key, which can be distributed through a trusted certificate authority. Code signing can prevent unauthorized modifications, tampering, or malware injection into the code, and it can also assure the users that the code is from a legitimate source. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 74. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 3.2, page 11. Application Security - SY0-601 CompTIA Security+ : 3.2

**Questions # 11:**

Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

**Options:**

A.

Compensating control

B.

Network segmentation

C.

Transfer of risk

D.

SNMP traps



CertsMania

**Answer**

A

**Explanation**

A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a weakness that cannot be resolved by the primary control. A compensating control does not prevent or eliminate the vulnerability or weakness, but it can reduce the likelihood or impact of an attack. A host-based firewall on a legacy Linux system that allows connections from only specific internal IP addresses is an example of a compensating control, as it can limit the exposure of the system to potential threats from external or unauthorized sources. A host-based firewall is a software application that monitors and filters the incoming and outgoing network traffic on a single host, based on a set of rules or policies. A legacy Linux system is an older version of the Linux operating system that may not be compatible with the latest security updates or patches, and may have known vulnerabilities or weaknesses that could be exploited by attackers. References = Security Controls - SY0-601 CompTIA Security+ : 5.1, Security Controls - CompTIA Security+ SY0-501 - 5.7, CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 240. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

**Questions # 12:**

Which of the following is the best reason to perform a tabletop exercise?

**Options:**

A.

To address audit findings

B.

To collect remediation response times

C.

To update the IRP

D.

To calculate the ROI



**Answer**

C

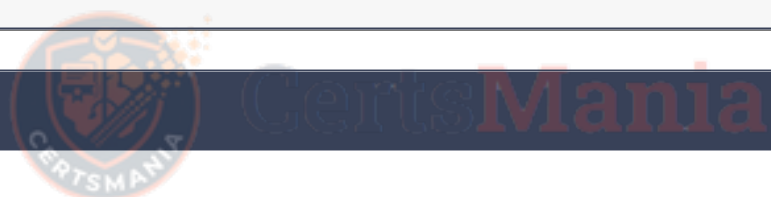
**Explanation**

A tabletop exercise simulates incident scenarios to test and validate the effectiveness of an organization's Incident Response Plan (IRP), identifying gaps and areas needing updates. It promotes team readiness without disrupting operations.

Addressing audit findings (A), collecting remediation times (B), and calculating ROI (D) are separate activities and not the primary purpose of tabletop exercises.

This practice is an integral part of Security Operations and Incident Response training in SY0-701 [6:Chapter 14+CompTIA Security+ Study Guide].

Questions # 13:



Which of the following methods will most likely be used to identify legacy systems?

**Options:**

A.

Bug bounty program

B.

Vulnerability scan

C.

Package monitoring

D.

Dynamic analysis

## Answer

B

## Explanation

A vulnerability scan is the most effective method for identifying legacy systems within an environment. Vulnerability scanners assess hosts for outdated operating systems, unsupported software versions, missing patches, deprecated services, and known Common Vulnerabilities and Exposures (CVEs). CompTIA Security+ SY0-701 highlights vulnerability scanning as a foundational security operation used to gain visibility into system age, patch status, and configuration weaknesses.

Legacy systems often stand out in scan results because they run end-of-life operating systems, use deprecated protocols, or lack current security updates. These indicators allow security teams to quickly flag systems that require isolation, compensating controls, or replacement.

Bug bounty programs (A) rely on external researchers and are not designed to inventory internal assets. Package monitoring (C) tracks software behavior and changes but does not identify system age or support status. Dynamic analysis (D) evaluates running applications for vulnerabilities, not infrastructure lifecycle status.

Because vulnerability scans provide broad visibility into system versions and supportability, the correct answer is B: Vulnerability scan.

## Questions # 14:

Which of the following should a systems administrator use to decrease the company's hardware attack surface?

### Options:

A.

Replication

B.

Isolation

C.

Centralization

D.

Virtualization



CertsMania

### Answer

D

### Explanation

Virtualization (D) allows multiple systems and services to be hosted on fewer physical machines, thereby reducing the total number of physical devices and consequently the hardware attack surface. This also allows for better patching, monitoring, and control.

The fewer devices you manage physically, the fewer entry points there are for attackers to exploit hardware-level vulnerabilities.

[Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.4 - "Reducing attack surface: Use of virtualization to consolidate systems." , , , , ]

### Questions # 15:

A company's accounts payable clerk receives a message from a vendor asking to change their bank account before paying an invoice. The clerk makes the change and sends the payment to the new account. Days later, the clerk receives another message from the same vendor with a request for a missing payment to the original bank account. Which of the following has most likely occurred?

### Options:

A.

Phishing campaign

B.

Data exfiltration

C.

Pretext calling

D.

Business email compromise

### Answer

D

### Explanation



CertsMania

Business email compromise (BEC) is a type of targeted phishing attack where an attacker gains access to a legitimate business email account (or convincingly impersonates one) to manipulate financial transactions, such as redirecting payments to a fraudulent bank account. The scenario described matches this pattern.

[Reference:, CompTIA Security+ SY0-701 Official Study Guide, Domain 2.2: "Business email compromise involves manipulating legitimate business communications to divert funds or sensitive information.", Exam Objectives 2.2: "Given a scenario, analyze potential indicators associated with application attacks.", , , , , ]

### Questions # 16:

A business is expanding to a new country and must protect customers from accidental disclosure of specific national identity information. Which of the following should the security engineer update to best meet business requirements?

### Options:

A.

SIEM

B.

SCAP

C.

DLP

D.

WAF



CertsMania

## Answer

C

## Explanation

The requirement is to prevent the accidental disclosure of national identity information—highly sensitive personal data. The best solution is DLP (Data Loss Prevention). DLP tools monitor, detect, and block unauthorized transmission or exposure of sensitive data across:

Email

Cloud storage

Endpoints

Networks

Databases

In Security+ SY0-701, DLP is specifically recommended for ensuring compliance with privacy regulations, including those related to national identifiers (e.g., Social Security numbers, national ID numbers).

A SIEM (A) aggregates logs but does not prevent data leakage. SCAP (B) provides standardized security configuration assessments, unrelated to data protection. A WAF (D) helps protect web applications but does not prevent sensitive data exfiltration.

Since the requirement focuses on preventing accidental disclosure, DLP is the only technology capable of detecting, labeling, blocking, and reporting attempts to move or expose sensitive national identity data. Therefore, the correct answer is C.

## Questions # 17:

A company wants to update its disaster recovery plan to include a dedicated location for immediate continued operations if a catastrophic event occurs. Which of the following options is best to include in the disaster recovery plan?

### Options:

A.

Hot site

B.

Warm site

C.

Geolocation

D.

Cold site



CertsMania

## Answer

A

## Explanation

A hot site is a fully operational data center equipped with hardware, software, and network connectivity, ready for immediate use after a disaster. It allows near-zero downtime, making it ideal for critical systems needing continuous operations.

Warm sites (B) have some infrastructure but require additional setup time. Cold sites (D) provide space and power but no equipment, leading to longer recovery. Geolocation (C) is unrelated.

Hot sites are a key disaster recovery solution discussed in SY0-701's Resilience and Recovery domain [6:Chapter 9] CompTIA Security+ Study Guide [1].

## Questions # 18:

A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

### Options:

A.

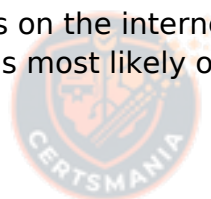
A worm is propagating across the network.

B.

Data is being exfiltrated.

C.

A logic bomb is deleting data.



CertsMania

D.

Ransomware is encrypting files.

## Answer

B

## Explanation



# Cert'sMania

Data exfiltration is a technique that attackers use to steal sensitive data from a target system or network by transmitting it through DNS queries and responses. This method is often used in advanced persistent threat (APT) attacks, in which attackers seek to persistently evade detection in the target environment. A large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours is a strong indicator of data exfiltration. A worm, a logic bomb, and ransomware would not use DNS queries to communicate with their command and control servers or perform their malicious actions. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 487; Introduction to DNS Data Exfiltration; Identifying a DNS Exfiltration Attack That Wasn't Real — This Time

## Questions # 19:

A group of developers has a shared backup account to access the source code repository. Which of the following is the best way to secure the backup account if there is an SSO failure?

## Options:

A.

RAS

B.

EAP

C.

SAML

D.

PAM



# Cert'sMania

## Answer

D

## Explanation

Detailed Explanation: Privileged Access Management (PAM) solutions enhance security by enforcing strong authentication, rotation of credentials, and access control for shared accounts. This is especially critical in scenarios like SSO failures. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Privileged Access and Identity Management".

## Questions # 20:

Which of the following describes a situation where a user is authorized before being authenticated?

### Options:

A.

Privilege escalation

B.

Race condition

C.

Tailgating

D.

Impersonation



CertsMania

## Answer

D

## Explanation

Impersonation occurs when an attacker or unauthorized user is granted access (authorized) by masquerading as a legitimate user, effectively bypassing or exploiting the authentication process. This means authorization is mistakenly granted before proper authentication.

Privilege escalation (A) involves gaining higher access after authentication. Race conditions (B) are timing vulnerabilities. Tailgating (C) refers to physical unauthorized access by following an authorized person.

Impersonation is a well-known identity attack vector detailed in the Threats and Vulnerabilities domain of SY0-701 [6:Chapter 4] CompTIA Security+ Study Guide [ ].

#### Questions # 21:

Which of the following actors attacking an organization is the most likely to be motivated by personal beliefs?

#### Options:

- A.  
Nation-state
- B.  
Organized crime
- C.  
Hacktivist
- D.  
Insider threat

#### Answer

C

#### Questions # 22:

In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password. Which of the following best describes this technique?

**Options:**

A.

Key stretching

B.

Tokenization

C.

Data masking

D.

Salting



CertsMania

**Answer**

D

**Explanation**

Adding a random string of characters, known as a "salt," to a password before hashing it is known as salting. This technique strengthens passwords by ensuring that even if two users have the same password, their hashes will be different due to the unique salt, making it much harder for attackers to crack passwords using precomputed tables. References: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

Questions # 23:

Which of the following allows a systems administrator to tune permissions for a file?

**Options:**

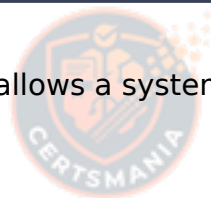
A.

Patching

B.

Access control list

C.



CertsMania

Configuration enforcement

D.

Least privilege

### Answer

B

### Explanation



CertsMania

Detailed Explanation: Access control lists (ACLs) allow administrators to fine-tune file permissions by specifying which users or groups have access to a file and defining the level of access. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Access Control Mechanisms".

### Questions # 24:

The Cruel Information Security Officer (CISO) asks a security analyst to install an OS update to a production VM that has a 99% uptime SLA. The CISO tells me analyst the installation must be done as quickly as possible. Which of the following courses of action should the security analyst take first?

### Options:

A.

Log in to the server and perform a health check on the VM.

B.

Install the patch Immediately.

C.

Confirm that the backup service is running.

D.

Take a snapshot of the VM.



CertsMania

## Answer

D

## Explanation

Before applying any updates or patches to a production VM, especially one with a 99% uptime SLA, it is crucial to first take a snapshot of the VM. This snapshot serves as a backup that can be quickly restored in case the update causes any issues, ensuring that the system can be returned to its previous state without violating the SLA. This step mitigates risk and is a standard best practice in change management for critical systems.

References = CompTIA Security+ SY0-701 study materials, focusing on change management and backup strategies.

## Questions # 25:

A company with a high-availability website is looking to harden its controls at any cost. The company wants to ensure that the site is secure by finding any possible issues. Which of the following would most likely achieve this goal?

### Options:

A.

Permission restrictions

B.

Bug bounty program

C.

Vulnerability scan

D.

Reconnaissance



CertsMania

## Answer

B

## Explanation

A bug bounty program encourages ethical hackers to find and report vulnerabilities, helping

organizations discover security flaws before they are exploited by malicious actors. Unlike vulnerability scans, bug bounty programs use real-world testing techniques.

[Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Operations domain., , , , , ]

#### Questions # 26:

Which of the following is a common data removal option for companies that want to wipe sensitive data from hard drives in a repeatable manner but allow the hard drives to be reused?

#### Options:

A.

Sanitization

B.

Formatting

C.

Degaussing

D.

Defragmentation

#### Answer

A

**To Get Premium Files for SY0-701 Visit**

**<https://www.certsmania.com/comptia/sy0-701-practice>**

**For More Free Questions Visit**

**<https://www.certsmania.com/comptia/pdf/sy0-701>**



**CertsMania**