Free Questions for SY0-701

Shared by Rios on 16-04-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

During a SQL update of a database, a temporary field used as part of the update sequence was modified by an attacker before the update completed in order to allow access to the system. Which of the following best describes this type of vulnerability?

Options:

A- Race condition
B- Memory injection
C- Malicious update
D- Side loading

Answer:

A

Explanation:

Arace conditionoccurs whentwo or more processes attempt to access and modify a shared resource simultaneously, leading to unintended behavior. In this scenario, the attacker was able to modify a temporary fieldbefore the SQL update completed, indicating atime-of-check to time-of-use (TOCTOU) vulnerability, which is a type of race condition.

Memory injection (B)refers to inserting malicious code into a running process's memory, but that isnotwhat is happening here.

Malicious update (C)is too broad and does not specifically describe this scenario.

Side loading (D)is a technique where malicious software is loaded via a trusted application, unrelated to this case.

Question 2

Question Type: MultipleChoice

Which option best receives logs from various devices and services, and then presents alerts?

Options:

A- SIEM
B- SCADA
C- SNMP
D- SCAP

Answer:

A

Explanation:

A SIEM (Security Information and Event Management) system aggregates logs from diverse sources, analyzes them, and generates alerts on suspicious activities. It provides centralized monitoring and incident detection.

SCADA (B) is industrial control, SNMP (C) is a protocol for network management, and SCAP (D) is a standard for security content automation.

SIEMs are foundational in Security Operations monitoring6:Chapter 14CompTIA Security+ Study Guide.

Question 3

Question Type: MultipleChoice

A systems administrator notices that one of the systems critical for processing customer transactions is running an end-of-life operating system. Which option best techniques would increase enterprise security?

Options:

A- Installing HIDS on the system
B- Placing the system in an isolated VLAN
C- Decommissioning the system
D- Encrypting the system's hard drive

Answer:

B

Explanation:

To enhance security for a system running an end-of-life operating system, placing the system in an isolated VLAN is the most effective approach. By isolating the system from the rest of the network, you can limit its exposure to potential threats while maintaining its functionality. This segmentation helps protect the rest of the network from any vulnerabilities in the outdated system.

Installing HIDS (Host-based Intrusion Detection System) can help detect intrusions but won't mitigate the risks posed by an unsupported OS.

Decommissioning may not be feasible if the system is critical.

Encrypting the system's hard drive protects data at rest but doesn't address vulnerabilities from an outdated OS.

Question 4

Question Type: MultipleChoice

A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the best option?

Options:

A- Send out periodic security reminders.
B- Update the content of new hire documentation.
C- Modify the content of recurring training.D Implement a phishing campaign

Answer:

C

Explanation:

Recurring training is a type of security awareness training that is conducted periodically to refresh and update the knowledge and skills of the users. Recurring training can help improve the situational and environmental awareness of existing users as they transition from remote to in-office work, as it can cover the latest threats, best practices, and policies that are relevant to their work environment. Modifying the content of recurring training can ensure that the users are aware of the current security landscape and the expectations of their roles.=CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page

232. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

Question 5

Question Type: MultipleChoice

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

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.=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.

Question 6

Question Type: MultipleChoice

While conducting a business continuity tabletop exercise, the security team becomes concerned by potential impacts if a generator fails during failover. Which option best is the team most likely to consider in regard to risk management activities?

Options:

A- RPO
B- ARO
C- BIA
D- MTTR

Answer:

D

Explanation:

Detailed Mean Time to Repair (MTTR) is a key metric in risk management, reflecting the time required to repair a failed component, such as a generator, and restore operations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: 'Business Continuity Metrics'.

Question 7

Question Type: MultipleChoice

A company is implementing a policy to allow employees to use their personal equipment for work. However, the company wants to ensure that only company-approved applications can be installed. Which of the following addresses this concern?

Options:

A- MDM
B- Containerization
C- DLP

D- FIM

Answer:

A

Explanation:

Comprehensive and Detailed In-Depth

Mobile Device Management (MDM) is a security solution that allows organizations to enforce policies on employee-owned or company-issued mobile devices. It can restrict the installation of unauthorized applications, ensuring that only company-approved apps are used.

Containerizationisolates work applications from personal applications but does not enforce app restrictions.

Data Loss Prevention (DLP)focuses on preventing sensitive data leaks rather than managing app installations.

File Integrity Monitoring (FIM)tracks changes to files and system configurations but does not control app installations.

Therefore,MDMis the best solution for restricting unauthorized applications on personal devices.

Question 8

Question Type: MultipleChoice

Various company stakeholders meet to discuss roles and responsibilities in the event of a security breach affecting offshore offices. Which of the following is this an example of?

Options:

A- Tabletop exercise
B- Penetration test
C- Geographic dispersion
D- Incident response

Answer:

A

Explanation:

Detailed

A tabletop exercise is a discussion-based activity where stakeholders simulate a security breach scenario to identify gaps in response plans and clarify roles and responsibilities. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: 'Incident Response Planning and Exercises'.

Question 9

Question Type: MultipleChoice

Which option best security principles most likely requires validation before allowing traffic between systems?

Options:

A- Policy enforcement
B- Authentication
C- Zero Trust architecture
D- Confidentiality

Answer:

C

Explanation:

Zero Trust architecture is based on the principle of 'never trust, always verify,' meaning all traffic between systems must be authenticated and authorized before communication is allowed, regardless of network location.

Policy enforcement (A) is important but broader. Authentication (B) is a component of Zero Trust, and confidentiality (D) refers to data protection, not access validation.

Zero Trust is a modern security framework emphasized in Security Architecture for securing enterprise environments6:Chapter 3CompTIA Security+ Study Guide.

Question 10

Question Type: MultipleChoice

A security analyst is reviewing logs and discovers the following:

```
149.34.228.10 - - [28/Jan/2023:16:32:45 -0300] "GET / HTTP/1.0" User-Agent: ${/bin/sh/ id} 200 397
```

Which of the following should be used lo best mitigate this type of attack?

Options:

A- Input sanitization
B- Secure cookies
C- Static code analysis
D- Sandboxing

Answer:

A