Free Questions for SY0-701

Shared by Lane on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An administrator needs to perform server hardening before deployment. Which of the following steps should the administrator take? (Select two).

Options:

A- Disable default accounts.
B- Add the server to the asset inventory.
C- Remove unnecessary services.
D- Document default passwords.
E- Send server logs to the SIEM.
E- Join the server to the corporate domain.

Answer:

A, C

Explanation:

To perform server hardening before deployment, the administrator should disable default accounts and remove unnecessary services. These steps are crucial to reducing the attack surface and enhancing the security of the server.

Disable default accounts: Default accounts often come with default credentials that are well-known and can be exploited by attackers. Disabling these accounts helps prevent unauthorized access.

Remove unnecessary services: Unnecessary services can introduce vulnerabilities and be exploited by attackers. Removing them reduces the number of potential attack vectors.

Add the server to the asset inventory: Important for tracking and management but not directly related to hardening.

Document default passwords: Documentation is useful, but changing or disabling default passwords is the hardening step.

Send server logs to the SIEM: Useful for monitoring and analysis but not a direct hardening step.

Join the server to the corporate domain: Part of integration into the network but not specific to hardening.

Question 2

Question Type: MultipleChoice

Which of the following actions could a security engineer take to ensure workstations and servers are properly monitored for unauthorized changes and software?

Options:

A- Configure all systems to log scheduled tasks.
B- Collect and monitor all traffic exiting the network.
C- Block traffic based on known malicious signatures.
D- Install endpoint management software on all systems.

Answer:

D

Explanation:

Endpoint management software is a tool that allows security engineers to monitor and control the configuration, security, and performance of workstations and servers from a central console. Endpoint management software can help detect and prevent unauthorized changes and software installations, enforce policies and compliance, and provide reports and alerts on the status of the endpoints.The other options are not as effective or comprehensive as endpoint management software for this purpose.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1371

Question 3

Question Type: MultipleChoice

A systems administrator wants to prevent users from being able to access data based on their responsibilities. The administrator also wants to apply the required access structure via a simplified format. Which of the following should the administrator apply to the site recovery resource group?

Options:

A- RBAC
B- ACL
C- SAML
D- GPO

Answer:

A

Explanation:

RBAC stands for Role-Based Access Control, which is a method of restricting access to data and resources based on the roles or responsibilities of users. RBAC simplifies the management of permissions by assigning roles to users and granting access rights to roles, rather than to individual users. RBAC can help enforce the principle of least privilege and reduce the risk of unauthorized access or data leakage.The other options are not as suitable for the scenario as RBAC, as they either do not prevent access based on responsibilities, or do not apply a simplified format.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1331

Question 4

Question Type: MultipleChoice

Which of the following would help ensure a security analyst is able to accurately measure the overall risk to an organization when a new vulnerability is disclosed?

Options:

A- A full inventory of all hardware and software
B- Documentation of system classifications
C- A list of system owners and their departments
D- Third-party risk assessment documentation

Answer:

A

Explanation:

A full inventory of all hardware and software is essential for measuring the overall risk to an organization when a new vulnerability is disclosed, because it allows the security analyst to identify which systems are affected by the vulnerability and prioritize the remediation efforts. Without a full inventory, the security analyst may miss some vulnerable systems or waste time and resources on irrelevant ones.Documentation of system classifications, a list of system owners and their departments, and third-party risk assessment documentation are all useful for risk management, but they are not sufficient to measure the impact of a new vulnerability.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; Risk Assessment and Analysis Methods: Qualitative and Quantitative3

Question 5

Question Type: MultipleChoice

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

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.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 2151

Question 6

Question Type: MultipleChoice

An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment. Which of the following solutions would mitigate the risk?

Options:

A- XDR
B- SPF
C- DLP
D- DMARC

Answer:

C

Explanation:

To mitigate the risk of sensitive data being exfiltrated from the environment, the IT manager should implement a Data Loss Prevention (DLP) solution. DLP monitors and controls the movement of sensitive data, ensuring that unauthorized transfers are blocked and potential data breaches are prevented.

XDR (Extended Detection and Response) is useful for threat detection across multiple environments but doesn't specifically address data exfiltration.

SPF (Sender Policy Framework) helps prevent email spoofing, not data exfiltration.

DMARC (Domain-based Message Authentication, Reporting & Conformance) also addresses email security and spoofing, not data exfiltration.

Question 7

Question Type: MultipleChoice

A manager receives an email that contains a link to receive a refund. After hovering over the link, the manager notices that the domain's URL points to a suspicious link. Which of the following security practices helped the manager to identify the attack?

Options:

A- End user training
B- Policy review
C- URL scanning
D- Plain text email

Answer:

A

Explanation:

The security practice that helped the manager identify the suspicious link is end-user training. Training users to recognize phishing attempts and other social engineering attacks, such as hovering over links to check the actual URL, is a critical component of an organization's security awareness program.

End user training: Educates employees on how to identify and respond to security threats, including suspicious emails and phishing attempts.

Policy review: Ensures that policies are understood and followed but does not directly help in identifying specific attacks.

URL scanning: Automatically checks URLs for threats, but the manager identified the issue manually.

Plain text email: Ensures email content is readable without executing scripts, but the identification in this case was due to user awareness.

Question 8

Question Type: MultipleChoice

Visitors to a secured facility are required to check in with a photo ID and enter the facility through an access control vestibule Which of the following but describes this form of security control?

Options:

A- Physical

B- Managerial
C- Technical
D- Operational

Answer:

A

Explanation:

A physical security control is a device or mechanism that prevents unauthorized access to a physical location or asset. An access control vestibule, also known as a mantrap, is a physical security control that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens. This prevents unauthorized individuals from following authorized individuals into the facility, a practice known as piggybacking or tailgating. A photo ID check is another form of physical security control that verifies the identity of visitors.Managerial, technical, and operational security controls are not directly related to physical access, but rather to policies, procedures, systems, and processes that support security objectives.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 341; Mantrap (access control) - Wikipedia2

Question 9

Question Type: MultipleChoice

An organization would like to store customer data on a separate part of the network that is not accessible to users on the main corporate network. Which of the following should the administrator use to accomplish this goal?

Options:

A- Segmentation
B- Isolation
C- Patching
D- Encryption

Answer:

A

Explanation:

Segmentation is a network design technique that divides the network into smaller and isolated segments based on logical or physical boundaries. Segmentation can help improve network security by limiting the scope of an attack, reducing the attack surface, and enforcing access control policies. Segmentation can also enhance network performance, scalability, and manageability.To accomplish the goal of storing customer data on a separate part of the network, the administrator can use segmentation technologies such as subnetting, VLANs, firewalls, routers, or switches.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-3091

Question 10

Question Type: MultipleChoice

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

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. Reference: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

Question 11

Question Type: MultipleChoice

Which of the following is used to quantitatively measure the criticality of a vulnerability?

Options:

A- CVE
B- CVSS
C- CIA
D- CERT

Answer:

B

Explanation:

CVSS stands for Common Vulnerability Scoring System, which is a framework that provides a standardized way to assess and communicate the severity and risk of vulnerabilities. CVSS uses a set of metrics and formulas to calculate a numerical score ranging from 0 to 10, where higher scores indicate higher criticality. CVSS can help organizations prioritize remediation efforts and compare vulnerabilities across different systems and vendors.The other options are not used to measure the criticality of a vulnerability, but rather to identify, classify, or report them.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 39