Free Questions for SY0-701 by braindumpscollection

Shared by Irwin on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company would like to provide employees with computers that do not have access to the internet in order to prevent information from being leaked to an online forum. Which of the following would be best for the systems administrator to implement?

Options:

A- Air gap

B- Jump server

C- Logical segmentation

D- Virtualization

Answer:

A

Explanation:

To provide employees with computers that do not have access to the internet and prevent information leaks to an online forum, implementing an air gap would be the best solution. An air gap physically isolates the computer or network from any outside connections, including the internet, ensuring that data cannot be transferred to or from the system.

Air gap: A security measure that isolates a computer or network from the internet or other networks, preventing any form of electronic communication with external systems.

Jump server: A secure server used to access and manage devices in a different security zone, but it does not provide isolation from the internet.

Logical segmentation: Segregates networks using software or network configurations, but it does not guarantee complete isolation from the internet.

Virtualization: Creates virtual instances of systems, which can be isolated, but does not inherently prevent internet access without additional configurations.

Question 2

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 3

Question Type: MultipleChoice

Which of the following tasks is typically included in the BIA process?

Options:

A- Estimating the recovery time of systems

B- Identifying the communication strategy

C- Evaluating the risk management plan

D- Establishing the backup and recovery procedures

E- Developing the incident response plan

Answer:

A

Explanation:

Estimating the recovery time of systems is a task typically included in the Business Impact Analysis (BIA) process. BIA involves identifying the critical functions of a business and determining the impact of a disruption. This includes estimating how long it will take to recover systems and resume normal operations.

Estimating the recovery time of systems: A key component of BIA, which helps in understanding the time needed to restore systems and services after a disruption.

Identifying the communication strategy: Typically part of the incident response plan, not BIA.

Evaluating the risk management plan: Part of risk management, not specifically BIA.

Establishing the backup and recovery procedures: Important for disaster recovery, not directly part of BIA.

Developing the incident response plan: Focuses on responding to security incidents, not on the impact analysis.

Question 4

Question Type: MultipleChoice

Which of the following describes effective change management procedures?

Options:

A- Approving the change after a successful deployment

B- Having a backout plan when a patch fails

C- Using a spreadsheet for tracking changes

D- Using an automatic change control bypass for security updates

Answer:

B

Explanation:

Effective change management procedures include having a backout plan when a patch fails. A backout plan ensures that there are predefined steps to revert the system to its previous state if the new change or patch causes issues, thereby minimizing downtime and mitigating potential negative impacts.

Having a backout plan when a patch fails: Essential for ensuring that changes can be safely reverted in case of problems, maintaining system stability and availability.

Approving the change after a successful deployment: Changes should be approved before deployment, not after.

Using a spreadsheet for tracking changes: While useful for documentation, it is not a comprehensive change management procedure.

Using an automatic change control bypass for security updates: Bypassing change control can lead to unapproved and potentially disruptive changes.

Question 5

Question Type: MultipleChoice

A security administrator is configuring fileshares. The administrator removed the default permissions and added permissions for only users who will need to access the fileshares as part of their job duties. Which of the following best describes why the administrator performed these actions?

Options:

A- Encryption standard compliance

B- Data replication requirements

C- Least privilege

D- Access control monitoring

Answer:

C

Explanation:

The security administrator's actions of removing default permissions and adding permissions only for users who need access as part of their job duties best describe the principle of least privilege. This principle ensures that users are granted the minimum necessary access to perform their job functions, reducing the risk of unauthorized access or data breaches.

Least privilege: Limits access rights for users to the bare minimum necessary for their job duties, enhancing security by reducing potential attack surfaces.

Encryption standard compliance: Involves meeting encryption requirements, but it does not explain the removal and assignment of specific permissions.

Data replication requirements: Focus on duplicating data across different systems for redundancy and availability, not related to user permissions.

Access control monitoring: Involves tracking and reviewing access to resources, but the scenario is about setting permissions, not monitoring them.

Question 6

Question Type: MultipleChoice

A systems administrator would like to deploy a change to a production system. Which of the following must the administrator submit to demonstrate that the system can be restored to a working state in the event of a performance issue?

Options:

A- Backout plan

B- Impact analysis

C- Test procedure

D- Approval procedure

Answer:

A

Explanation:

To demonstrate that the system can be restored to a working state in the event of a performance issue after deploying a change, the systems administrator must submit a backout plan. A backout plan outlines the steps to revert the system to its previous state if the new deployment causes problems.

Backout plan: Provides detailed steps to revert changes and restore the system to its previous state in case of issues, ensuring minimal disruption and quick recovery.

Impact analysis: Evaluates the potential effects of a change but does not provide steps to revert changes.

Test procedure: Details the steps for testing the change but does not address restoring the system to a previous state.

Approval procedure: Involves obtaining permissions for the change but does not ensure system recovery in case of issues.

Question 7

Question Type: **MultipleChoice**

An organization wants to ensure the integrity of compiled binaries in the production environment. Which of the following security measures would best support this objective?

Options:

A- Input validation

B- Code signing

C- SQL injection

D- Static analysis

Answer:

B

Explanation:

To ensure the integrity of compiled binaries in the production environment, the best security measure is code signing. Code signing uses digital signatures to verify the authenticity and integrity of the software, ensuring that the code has not been tampered with or altered after it was signed.

Code signing: Involves signing code with a digital signature to verify its authenticity and integrity, ensuring the compiled binaries have not been altered.

Input validation: Ensures that only properly formatted data enters an application but does not verify the integrity of compiled binaries.

SQL injection: A type of attack, not a security measure.

Static analysis: Analyzes code for vulnerabilities and errors but does not ensure the integrity of compiled binaries in production.