Free Questions for SY0-701

Shared by Carney on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

During the onboarding process, an employee needs to create a password for an intranet account. The password must include ten characters, numbers, and letters, and two special characters. Once the password is created, the company will grant the employee access to other company-owned websites based on the intranet profile. Which of the following access management concepts is the company most likely using to safeguard intranet accounts and grant access to multiple sites based on a user's intranet account? (Select two).

Options:

A- Federation

B- Identity proofing

C- Password complexity

D- Default password changes

E- Password manager

F- Open authentication

Answer:

A, C

Explanation:

Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations. Federation relies on a trusted third party that stores the user's credentials and provides them to the requested resources or services without exposing them. Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness.Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 and 312-3131

Question 2

Question Type: MultipleChoice

An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use. Each application has a separate log-in. so the security team wants to reduce the number of credentials each employee must maintain. Which of the following is the first step the security team should take?

Options:

A- Enable SAML

B- Create OAuth tokens.

C- Use password vaulting.

D- Select an IdP

Answer:

D

Explanation:

The first step in reducing the number of credentials each employee must maintain when using multiple SaaS applications is to select an Identity Provider (IdP). An IdP provides a centralized authentication service that supports Single Sign-On (SSO), enabling users to access multiple applications with a single set of credentials.

Enabling SAML would be part of the technical implementation but comes after selecting an IdP.

OAuth tokens are used for authorization, but selecting an IdP is the first step in managing authentication.

Password vaulting stores multiple passwords securely but doesn't reduce the need for separate logins.

Question 3

Question Type: MultipleChoice

A security analyst scans a company's public network and discovers a host is running a remote desktop that can be used to access the production network. Which of the following changes should the security analyst recommend?

Options:

A- Changing the remote desktop port to a non-standard number
B- Setting up a VPN and placing the jump server inside the firewall
C- Using a proxy for web connections from the remote desktop server
D- Connecting the remote server to the domain and increasing the password length

Answer:

B

Explanation:

A VPN is a virtual private network that creates a secure tunnel between two or more devices over a public network. A VPN can encrypt and authenticate the data, as well as hide the IP addresses and locations of the devices. A jump server is a server that acts as an intermediary between a user and a target server, such as a production server. A jump server can provide an additional layer of security and access control, as well as logging and auditing capabilities. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can protect the internal network from external threats and limit the exposure of sensitive services and ports. A security analyst should recommend setting up a VPN and placing the jump server inside the firewall to improve the security of the remote desktop access to the production network.This way, the remote desktop service will not be exposed to the public network, and only authorized users with VPN credentials can access the jump server and then the production server.Reference: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 382-3831; Chapter 9: Network Security, page 441-4421

Question 4

Question Type: MultipleChoice

Which of the following teams combines both offensive and defensive testing techniques to protect an organization's critical systems?

Options:

A- Red
B- Blue
C- Purple
D- Yellow

Answer:

C

Explanation:

Purple is the team that combines both offensive and defensive testing techniques to protect an organization's critical systems. Purple is not a separate team, but rather a collaboration between the red team and the blue team. The red team is the offensive team that simulates attacks and exploits vulnerabilities in the organization's systems. The blue team is the defensive team that monitors and protects the organization's systems from real and simulated threats. The purple team exists to ensure and maximize the effectiveness of the red and blue teams by integrating the defensive tactics and controls from the blue team with the threats and vulnerabilities found by the red team into a single narrative that improves the overall security posture of the organization. Red, blue, and yellow are other types of teams involved in security testing, but they do not combine both offensive and defensive techniques.The yellow team is the team that builds software solutions, scripts, and other programs that the blue team uses in the security testing.Reference:CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1331; Penetration Testing: Understanding Red, Blue, & Purple Teams3

Question 5

Question Type: MultipleChoice

The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

Options:

A- Shadow IT

B- Insider threat

C- Data exfiltration

D- Service disruption

Answer:

A

Explanation:

The marketing department setting up its own project management software without informing the appropriate departments is an example of Shadow IT. Shadow IT refers to the use of IT systems, devices, software, applications, and services without explicit approval from the IT department.

Shadow IT: Involves the use of unauthorized systems and applications within an organization, which can lead to security risks and compliance issues.

Insider threat: Refers to threats from individuals within the organization who may intentionally cause harm or misuse their access, but this scenario is more about unauthorized use rather than malicious intent.

Data exfiltration: Involves unauthorized transfer of data out of the organization, which is not the main issue in this scenario.

Service disruption: Refers to interruptions in service availability, which is not directly related to the marketing department's actions.

Question 6

Question Type: MultipleChoice

A company hired a security manager from outside the organization to lead security operations. Which of the following actions should the security manager perform first in this new role?

Options:

A- Establish a security baseline.
B- Review security policies.
C- Adopt security benchmarks.
D- Perform a user ID revalidation.

Answer:

B

Explanation:

When a security manager is hired from outside the organization to lead security operations, the first action should be to review the existing security policies. Understanding the current security policies provides a foundation for identifying strengths, weaknesses, and areas that require improvement, ensuring that the security program aligns with the organization's goals and regulatory requirements.

Review security policies: Provides a comprehensive understanding of the existing security framework, helping the new manager to identify gaps and areas for enhancement.

Establish a security baseline: Important but should be based on a thorough understanding of existing policies and practices.

Adopt security benchmarks: Useful for setting standards, but reviewing current policies is a necessary precursor.

Perform a user ID revalidation: Important for ensuring user access is appropriate but not the first step in understanding overall security operations.