SY0-701 Q&As

CompTIA Security+

Pass CompTIA SY0-701 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/sy0-701.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

The management team notices that new accounts that are set up manually do not always have correct access or permissions.

Which of the following automation techniques should a systems administrator use to streamline account creation?

A. Guard rail script

B. Ticketing workflow

C. Escalation script

D. User provisioning script

Correct Answer: D

A user provisioning script is an automation technique that uses a predefined set of instructions or commands to create, modify, or delete user accounts and assign appropriate access or permissions. A user provisioning script can help to streamline account creation by reducing manual errors, ensuring consistency and compliance, and saving time and resources12. The other options are not automation techniques that can streamline account creation: Guard rail script: This is a script that monitors and enforces the security policies and rules on a system or a network. A guard rail script can help to prevent unauthorized or malicious actions, such as changing security settings, accessing restricted resources, or installing unwanted software3. Ticketing workflow: This is a process that tracks and manages the requests, issues, or incidents that are reported by users or customers. A ticketing workflow can help to improve the communication, collaboration, and resolution of problems, but it does not automate the account creation process4. Escalation script: This is a script that triggers an alert or a notification when a certain condition or threshold is met or exceeded. An escalation script can help to inform the relevant parties or authorities of a critical situation, such as a security breach, a performance degradation, or a service outage.

References: 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: User Provisioning -CompTIA Security+ SY0-701 -5.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 1034: CompTIA Security+ SY0-701 Certification Study Guide, page 104. : CompTIA Security+ SY0-701 Certification Study Guide, page 105.

QUESTION 2

The security operations center is researching an event concerning a suspicious IP address. A security analyst looks at the following event logs and discovers that a significant portion of the user accounts have experienced faded log-In attempts when authenticating from the same IP address:

184.168.131.241 – userA – failed authentication
184.168.131.241 – userA – failed authentication
184.168.131.241 – userB – failed authentication
184.168.131.241 – userB – failed authentication
184.168.131.241 – userC – failed authentication
184.168.131.241 – userC – failed authentication

Which of the following most likely describes attack that took place?

A. Spraying

B. Brute-force

C. Dictionary

D. Rainbow table

Correct Answer: A

Password spraying is a type of attack where an attacker tries a small number of commonly used passwords across a large number of accounts. The event logs showing failed login attempts for many user accounts from the same IP address

are indicative of a password spraying attack, where the attacker is attempting to gain access by guessing common passwords.

References: CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management and common attack vectors like password spraying.

QUESTION 3

Which of the following describes a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system?

A. SIEM

B. DLP

C. IDS

D. SNMP

Correct Answer: A

SIEM stands for Security Information and Event Management. It is a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system. SIEM can analyze the collected data, correlate events, generate alerts, and provide reports and dashboards. SIEM can also integrate with other security tools and support compliance requirements. SIEM helps organizations to detect and respond to cyber threats, improve security posture, and reduce operational costs.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Monitoring and Auditing, page 393. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 10: Monitoring and Auditing, page 397.

QUESTION 4

Which of the following is a reason why a forensic specialist would create a plan to preserve data after an modem and prioritize the sequence for performing forensic analysis?

A. Order of volatility

B. Preservation of event logs

C. Chain of custody

D. Compliance with legal hold

Correct Answer: A

When conducting a forensic analysis after an incident, it\\'s essential to prioritize the data collection process based on the "order of volatility." This principle dictates that more volatile data (e.g., data in memory, network connections) should be

captured before less volatile data (e.g., disk drives, logs). The idea is to preserve the most transient and potentially valuable evidence first, as it is more likely to be lost or altered quickly.

References:

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations. CompTIA Security+ SY0-601 Study Guide: Chapter on Digital Forensics.

QUESTION 5

A company must ensure sensitive data at rest is rendered unreadable. Which of the following will the company most likely use?

A. Hashing

B. Tokenization

C. Encryption

D. Segmentation

Correct Answer: C

Encryption is a method of transforming data in a way that makes it unreadable without a secret key necessary to decrypt the data back into plaintext. Encryption is one of the most common and effective ways to protect data at rest, as it prevents unauthorized access, modification, or theft of the data. Encryption can be applied to different types of data at rest, such as block storage, object storage, databases, archives, and so on. Hashing, tokenization, and segmentation are not methods of rendering data at rest unreadable, but rather of protecting data in other ways. Hashing is a one-way function that generates a fixed-length output, called a hash or digest, from an input, such that the input cannot be recovered from the output. Hashing is used to verify the integrity and authenticity of data, but not to encrypt it. Tokenization is a process that replaces sensitive data with non-sensitive substitutes, called tokens, that have no meaning or value on their own. Tokenization is used to reduce the exposure and compliance scope of sensitive data, but not to encrypt it. Segmentation is a technique that divides a network or a system into smaller, isolated units, called segments, that have different levels of access and security. Segmentation is used to limit the attack surface and contain the impact of a breach, but not to encrypt data at rest. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, pages 77-781; Protecting data at rest - Security Pillar3

QUESTION 6

An IT manager is putting together a documented plan describing how the organization will keep operating in the event of a global incident. Which of the following plans is the IT manager creating?

A. Business continuity

B. Physical security

C. Change management

D. Disaster recovery

Correct Answer: A

The IT manager is creating a Business Continuity Plan (BCP). A BCP describes how an organization will continue to operate during and after a disaster or global incident. It ensures that critical business functions remain operational despite

adverse conditions, with a focus on minimizing downtime and maintaining essential services. Physical security relates to protecting physical assets. Change management ensures changes in IT systems are introduced smoothly, without

disrupting operations.

Disaster recovery is a subset of business continuity but focuses specifically on recovering from IT-related incidents.

QUESTION 7

Which of the following methods to secure credit card data is best to use when a requirement is to see only the last four numbers on a credit card?

A. Encryption

B. Hashing

C. Masking

D. Tokenization

Correct Answer: C

Masking is a method to secure credit card data that involves replacing some or all of the digits with symbols, such as asterisks, dashes, or Xs, while leaving some of the original digits visible. Masking is best to use when a requirement is to see only the last four numbers on a credit card, as it can prevent unauthorized access to the full card number, while still allowing identification and verification of the cardholder. Masking does not alter the original data, unlike encryption, hashing, or tokenization, which use algorithms to transform the data into different formats.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2: Compliance and Operational Security, page 721. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2: Compliance and Operational Security, page 722.

QUESTION 8

A legacy device is being decommissioned and is no longer receiving updates or patches. Which of the following describes this scenario?

A. End of business

B. End of testing

C. End of support

D. End of life

Correct Answer: D

QUESTION 9

A company is utilizing an offshore team to help support the finance department. The company wants to keep the data secure by keeping it on a company device but does not want to provide equipment to the offshore team. Which of the following should the company implement to meet this requirement?

A. VDI

B. MDM

C. VPN

D. VPC

Correct Answer: A

Virtual Desktop Infrastructure (VDI) allows a company to host desktop environments on a centralized server. Offshore teams can access these virtual desktops remotely, ensuring that sensitive data stays within the company\\'s infrastructure

without the need to provide physical devices to the team. This solution is ideal for maintaining data security while enabling remote work, as all data processing occurs on the company\\'s secure servers.

References:

CompTIA Security+ SY0-701 Course Content: VDI is discussed as a method for securely managing remote access to company resources without compromising data security.

QUESTION 10

A security administrator is deploying a DLP solution to prevent the exfiltration of sensitive customer data. Which of the following should the administrator do first?

A. Block access to cloud storage websites.

B. Create a rule to block outgoing email attachments.

C. Apply classifications to the data.

D. Remove all user permissions from shares on the file server.

Correct Answer: C

Data classification is the process of assigning labels or tags to data based on its sensitivity, value, and risk. Data classification is the first step in a data loss prevention (DLP) solution, as it helps to identify what data needs to be

protected and

how. By applying classifications to the data, the security administrator can define appropriate policies and rules for the DLP solution to prevent the exfiltration of sensitive customer data.

References:

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Data Protection, page 323. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 8: Data Protection, page 327.

QUESTION 11

An employee fell for a phishing scam, which allowed an attacker to gain access to a company PC. The attacker scraped the PC\\'s memory to find other credentials. Without cracking these credentials, the attacker used them to move laterally through the corporate network. Which of the following describes this type of attack?

A. Privilege escalation

B. Buffer overflow

C. SQL injection

D. Pass-the-hash

Correct Answer: D

The scenario describes an attacker who obtained credentials from a compromised system\\'s memory and used them without cracking to move laterally within the network. This technique is known as a "pass-the-hash" attack, where the

attacker captures hashed credentials (e.g., NTLM hashes) and uses them to authenticate and gain access to other systems without needing to know the plaintext password. This is a common attack method in environments where weak

security practices or outdated protocols are in use.

References:

CompTIA Security+ SY0-701 Course Content: The course discusses credential- based attacks like pass-the-hash, emphasizing their impact and the importance of protecting credential stores.

QUESTION 12

After conducting a vulnerability scan, a systems administrator notices that one of the identified vulnerabilities is not present on the systems that were scanned. Which of the following describes this example?

A. False positive

B. False negative

C. True positive

D. True negative

Correct Answer: A

A false positive occurs when a vulnerability scan identifies a vulnerability that is not actually present on the systems that were scanned. This means that the scan has incorrectly flagged a system as vulnerable.

False positive: Incorrectly identifies a vulnerability that does not exist on the scanned systems.

False negative: Fails to identify an existing vulnerability on the system. True positive: Correctly identifies an existing vulnerability. True negative: Correctly identifies that there is no vulnerability. Reference: CompTIA Security+ SY0-701 Exam

Objectives, Domain 4.3 - Explain various activities associated with vulnerability management (False positives and false negatives).

QUESTION 13

Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?

A. Insider

B. Unskilled attacker

C. Nation-state

D. Hacktivist

Correct Answer: C

A nation-state is a threat actor that is sponsored by a government or a political entity to conduct cyberattacks against other countries or organizations. Nation- states have large financial resources, advanced technical skills, and strategic objectives that may target critical systems such as military, energy, or infrastructure. Nation-states are often motivated by espionage, sabotage, or warfare12.

References: 1: CompTIA Security+ SY0-701 Certification Study Guide, page 542: Threat Actors -CompTIA Security+ SY0-701 ?2.1, video by Professor Messer.

QUESTION 14

After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

A. Console access

B. Routing protocols

C. VLANs

D. Web-based administration

Correct Answer: D

Web-based administration is a feature that allows users to configure and manage routers through a web browser interface. While this feature can provide convenience and ease of use, it can also pose a security risk, especially if the web interface is exposed to the internet or uses weak authentication or encryption methods. Web-based administration

can be exploited by attackers to gain unauthorized access to the router\\'s settings, firmware, or data, or to launch attacks such as cross-site scripting (XSS) or cross-site request forgery (CSRF). Therefore, disabling web-based administration is a good practice to harden the routers within the corporate network. Console access, routing protocols, and VLANs are other features that can be configured on routers, but they are not the most appropriate to disable for hardening purposes. Console access is a physical connection to the router that requires direct access to the device, which can be secured by locking the router in a cabinet or using a strong password. Routing protocols are essential for routers to exchange routing information and maintain network connectivity, and they can be secured by using authentication or encryption mechanisms. VLANs are logical segments of a network that can enhance network performance and security by isolating traffic and devices, and they can be secured by using VLAN access control lists (VACLs) or private VLANs (PVLANs).

References: CCNA SEC: Router Hardening Your Router\\'s Security Stinks: Here\\'s How to Fix It

QUESTION 15

During a recent breach, employee credentials were compromised when a service desk employee issued an MFA bypass code to an attacker who called and posed as an employee. Which of the following should be used to prevent this type of incident in the future?

A. Hardware token MFA

B. Biometrics

C. Identity proofing

D. Least privilege

Correct Answer: C

To prevent the issuance of an MFA bypass code to an attacker posing as an employee, implementing identity proofing would be most effective. Identity proofing involves verifying the identity of individuals before granting access or providing

sensitive information.

Identity proofing: Ensures that the person requesting the MFA bypass is who they claim to be, thereby preventing social engineering attacks where attackers pose as legitimate employees.

Hardware token MFA: Provides an additional factor for authentication but does not address verifying the requester\\'s identity.

Biometrics: Offers strong authentication based on physical characteristics but is not related to the process of issuing MFA bypass codes. Least privilege: Limits access rights for users to the bare minimum necessary to perform their work but

does not prevent social engineering attacks targeting the service desk.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 4.6 - Implement and maintain identity and access management (Identity proofing).