SY0-701 Q&As

CompTIA Security+ 2024

Pass CompTIA SY0-701 Exam with 100% Guarantee

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

https://www.pass4itsure.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

Which of the following best practices gives administrators a set period to perform changes to an operational system to ensure availability and minimize business impacts?

A. Impact analysis

B. Scheduled downtime

C. Backout plan

D. Change management boards

Correct Answer: B

Scheduled downtime is a planned period of time when a system or service is unavailable for maintenance, updates, upgrades, or other changes. Scheduled downtime gives administrators a set period to perform changes to an operational

system without disrupting the normal business operations or affecting the availability of the system or service. Scheduled downtime also allows administrators to inform the users and stakeholders about the expected duration and impact of the

changes.

References:

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 12: Security Operations and Administration, page 579 1

QUESTION 2

Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?

A. To track the status of patching installations

B. To find shadow IT cloud deployments

C. To continuously the monitor hardware inventory

D. To hunt for active attackers in the network

Correct Answer: A

Running daily vulnerability scans on all corporate endpoints is primarily done to track the status of patching installations. These scans help identify any missing security patches or vulnerabilities that could be exploited by attackers. Keeping

the endpoints up-to-date with the latest patches is critical for maintaining security. Finding shadow IT cloud deployments and monitoring hardware inventory are better achieved through other tools.

Hunting for active attackers would typically involve more real-time threat detection methods than daily vulnerability scans.

QUESTION 3

A company tested and validated the effectiveness of network security appliances within the corporate network. The IDS detected a high rate of SQL injection attacks against the company\\'s servers, and the company\\'s perimeter firewall is at capacity. Which of the following would be the best action to maintain security and reduce the traffic to the perimeter firewall?

A. Set the appliance to IPS mode and place it in front of the company firewall.

B. Convert the firewall to a WAF and use IPSec tunnels to increase throughput.

C. Set the firewall to fail open if it is overloaded with traffic and send alerts to the SIEM.

D. Configure the firewall to perform deep packet inspection and monitor TLS traffic.

Correct Answer: A

Given the scenario where an Intrusion Detection System (IDS) has detected a high rate of SQL injection attacks and the perimeter firewall is at capacity, the best action would be to set the appliance to Intrusion Prevention System (IPS) mode and place it in front of the company firewall. This approach has several benefits: Intrusion Prevention System (IPS): Unlike IDS, which only detects and alerts on malicious activity, IPS can actively block and prevent those activities. Placing an IPS in front of the firewall means it can filter out malicious traffic before it reaches the firewall, reducing the load on the firewall and enhancing overall security. Reducing Traffic Load: By blocking SQL injection attacks and other malicious traffic before it reaches the firewall, the IPS helps maintain the firewall\\'s performance and prevents it from becoming a bottleneck. Enhanced Security: The IPS provides an additional layer of defense, identifying and mitigating threats in real-time. Option B (Convert the firewall to a WAF and use IPSec tunnels) would not address the primary issue of reducing traffic to the firewall effectively. Option C (Set the firewall to fail open) would compromise security. Option D (Deep packet inspection) could be resource- intensive and might not alleviate the firewall capacity issue effectively. Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 2.5 - Mitigation techniques used to secure the enterprise.

QUESTION 4

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

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.

F. Join the server to the corporate domain.

Correct Answer: AC

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.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1 - Compare and contrast various types of security controls (Server hardening).

QUESTION 5

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 6

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 7

An administrator is reviewing a single server\\'s security logs and discovers the following:

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	09/16/2022 11:13:05 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:07 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:09 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:11 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:13 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:15 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:17 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:19 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:21 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:23 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:25 AM	Microsoft Windows security	4625	Logon
Audit Failure	09/16/2022 11:13:27 AM	Microsoft Windows security	4625	Logon

Which of the following best describes the action captured in this log file?

A. Brute-force attack

B. Privilege escalation

C. Failed password audit

D. Forgotten password by the user

Correct Answer: A

A brute-force attack is a type of attack that involves systematically trying all possible combinations of passwords or keys until the correct one is found. The log file shows multiple failed login attempts in a short amount of time, which is a

characteristic of a brute-force attack. The attacker is trying to guess the password of the Administrator account on the server. The log file also shows the event ID 4625, which indicates a failed logon attempt, and the status code 0xC000006A,

which means the user name is correct but the password is wrong. These are indicators of compromise (IoC) that suggest a brute- force attack is taking place.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 and 223 1

QUESTION 8

An organization recently updated its security policy to include the following statement:

Regular expressions are included in source code to remove special characters such as $, |, ;. and, `, and ? from variables set by forms in a web application.

Which of the following best explains the security technique the organization adopted by making this addition to the policy?

A. Identify embedded keys

B. Code debugging

C. Input validation

D. Static code analysis

Correct Answer: C

Input validation is a security technique that checks the user input for any malicious or unexpected data before processing it by the application. Input validation can prevent various types of attacks, such as injection, cross-site scripting, buffer overflow, and command execution, that exploit the vulnerabilities in the application code. Input validation can be performed on both the client-side and the server-side, using methods such as whitelisting, blacklisting, filtering, sanitizing, escaping, and encoding. By including regular expressions in the source code to remove special characters from the variables set by the forms in the web application, the organization adopted input validation as a security technique. Regular expressions are patterns that match a specific set of characters or strings, and can be used to filter out any unwanted or harmful input. Special characters, such as $, |, ;, and, `, and ?, can be used by attackers to inject commands or scripts into the application, and cause damage or data theft. By removing these characters from the input, the organization can reduce the risk of such attacks.

Identify embedded keys, code debugging, and static code analysis are not the security techniques that the organization adopted by making this addition to the policy. Identify embedded keys is a process of finding and removing any hard-coded keys or credentials from the source code, as these can pose a security risk if exposed or compromised. Code debugging is a process of finding and fixing any errors or bugs in the source code, which can affect the functionality or performance of the application. Static code analysis is a process of analyzing the source code without executing it, to identify any vulnerabilities, flaws, or coding standards violations. These techniques are not related to the use of regular expressions to remove special characters from the input.

References: CompTIA Security+ SY0-701 Certification Study Guide, page 375-376; Professor Messer\\'s CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 8:00 - 9:08; Application Security -SY0-601 CompTIA Security+ : 3.2, 0:00 - 2:00.

QUESTION 9

In which of the following scenarios is tokenization the best privacy technique 10 use?

A. Providing pseudo-anonymization tor social media user accounts

B. Serving as a second factor for authentication requests

C. Enabling established customers to safely store credit card Information

D. Masking personal information inside databases by segmenting data

Correct Answer: C

Tokenization is a process that replaces sensitive data, such as credit card information, with a non-sensitive equivalent (token) that can be used in place of the actual data. This technique is particularly useful in securely storing payment

information because the token can be safely stored and transmitted without exposing the original credit card number.

References:

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture. CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptography and Data Protection.

QUESTION 10

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?

A. Physical

B. Managerial

C. Technical

D. Operational

Correct Answer: A

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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 341; Mantrap (access control) - Wikipedia2

QUESTION 11

A company\\'s web filter is configured to scan the URL for strings and deny access when matches are found. Which of the following search strings should an analyst employ to prohibit access to non-encrypted websites?

A. encryption=off\

B. http://

C. www.*.com

D. :443

Correct Answer: B

A web filter is a device or software that can monitor, block, or allow web traffic based on predefined rules or policies. One of the common methods of web filtering is to scan the URL for strings and deny access when matches are found. For example, a web filter can block access to websites that contain the words "gambling", "porn", or "malware" in their URLs. A URL is a uniform resource locator that identifies the location and protocol of a web resource. A URL typically consists of the following components: protocol://domain:port/path?query#fragment. The protocol specifies the communication method used to access the web resource, such as HTTP, HTTPS, FTP, or SMTP. The domain is the name of the web server that hosts the web resource, such as www.google.com or www.bing.com. The port is an optional number that identifies the specific service or application running on the web server, such as 80 for HTTP or 443 for HTTPS. The path is the specific folder or file name of the web resource, such as /index.html or /images/logo.png. The query is an optional string that contains additional information or parameters for the web resource, such as ?q=security or ?lang=en. The fragment is an optional string that identifies a specific part or section of the web resource, such as #introduction or #summary. To prohibit access to non-encrypted websites, an analyst should employ a search string that matches the protocol of non-encrypted web traffic, which is HTTP. HTTP stands for hypertext transfer protocol, and it is a standard protocol for transferring data between web servers and web browsers. However, HTTP does not provide any encryption or security for the data, which means that anyone who intercepts the web traffic can read or modify the data. Therefore, non-encrypted websites are vulnerable to eavesdropping, tampering, or spoofing attacks. To access a non-encrypted website, the URL usually starts with http://, followed by the domain name and optionally the port number. For example, http:// www.example.com or http://www.example.com:80. By scanning the URL for the string http://, the web filter can identify and block non-encrypted websites. The other options are not correct because they do not match the protocol of non-encrypted web traffic. Encryption=off is a possible query string that indicates the encryption status of the web resource, but it is not a standard or mandatory parameter. Https:// is the protocol of encrypted web traffic, which uses hypertext transfer protocol secure (HTTPS) to provide encryption and security for the data. Www.*.com is a possible domain name that matches any website that starts with www and ends with .com, but it does not specify the protocol. :443 is the port number of HTTPS, which is the protocol of encrypted web traffic.

References: CompTIA Security+ Study Guide (SY0-701), Chapter 2: Securing Networks, page 69. Professor Messer\\'s CompTIA SY0-701 Security+ Training Course, Section 2.1: Network Devices and Technologies, video: Web Filter (5:16).

QUESTION 12

A systems administrator is working on a solution with the following requirements:

1.

Provide a secure zone.

2.

Enforce a company-wide access control policy.

3.

Reduce the scope of threats.

Which of the following is the systems administrator setting up?

A. Zero Trust

B. AAA

C. Non-repudiation

D. CIA

Correct Answer: A

Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company- wide access control policy by applying the principle of least privilege and granular segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.

References:

5: This source explains the concept and benefits of Zero Trust security and how it differs from traditional security models.

8: This source provides an overview of Zero Trust identity security and how it can help verify the identity and integrity of users and devices.

QUESTION 13

A security team is setting up a new environment for hosting the organization\\'s on-premises software application as a cloud-based service. Which of the following should the team ensure is in place in order for the organization to follow security best practices?

A. Visualization and isolation of resources

B. Network segmentation

C. Data encryption

D. Strong authentication policies

Correct Answer: A

When hosting an on-premises software application in a cloud-based service, ensuring visualization and isolation of resources is crucial for maintaining security best practices. This involves using virtualization techniques to create isolated

environments (e.g., virtual machines or containers) for different applications and services, reducing the risk of cross-tenant attacks or resource leakage.

Network segmentation is important but pertains more to securing network traffic rather than isolating computing resources.

Data encryption is also essential but doesn\\'t specifically address resource isolation in a cloud environment.

Strong authentication policies are critical for access control but do not address the need for isolating resources within the cloud environment.

QUESTION 14

Which of the following is most likely to be deployed to obtain and analyze attacker activity and techniques?

A. Firewall

B. IDS

C. Honeypot

D. Layer 3 switch

Correct Answer: C

A honeypot is most likely to be deployed to obtain and analyze attacker activity and techniques. A honeypot is a decoy system set up to attract attackers, providing an opportunity to study their methods and behaviors in a controlled

environment without risking actual systems.

Honeypot: A decoy system designed to lure attackers, allowing administrators to observe and analyze attack patterns and techniques. Firewall: Primarily used to block unauthorized access to networks, not for observing attacker behavior. IDS

(Intrusion Detection System): Detects and alerts on malicious activity but does not specifically engage attackers to observe their behavior. Layer 3 switch: Used for routing traffic within networks, not for analyzing attacker techniques.

Reference: CompTIA Security+ SY0-701 Exam Objectives, Domain 2.4 - Indicators of malicious activity (Honeypots).

QUESTION 15

A network manager wants to protect the company\\'s VPN by implementing multifactor authentication that uses:

1.

Something you know

2.

Something you have

3.

Something you are

Which of the following would accomplish the manager\\'s goal?

A. Domain name, PKI, GeoIP lookup

B. VPN IP address, company ID, facial structure

C. Password, authentication token, thumbprint

D. Company URL, TLS certificate, home address

Correct Answer: C

The correct answer is C. Password, authentication token, thumbprint. This combination of authentication factors

satisfies the manager\\'s goal of implementing multifactor authentication that uses something you know, something you have, and something you are. Something you know is a type of authentication factor that relies on the user\\'s knowledge of a secret or personal information, such as a password, a PIN, or a security question. A password is a common example of something you know that can be used to access a VPN12 Something you have is a type of authentication factor that relies on the user\\'s possession of a physical object or device, such as a smart card, a token, or a smartphone. An authentication token is a common example of something you have that can be used to generate a one-time password (OTP) or a code that can be used to access a VPN12 Something you are is a type of authentication factor that relies on the user\\'s biometric characteristics, such as a fingerprint, a face, or an iris. A thumbprint is a common example of something you are that can be used to scan and verify the user\\'s identity to access a VPN12

References:

1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Identity and Access Management, page 177 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4: Identity and Access Management, page