Don't Miss Up to 365 Days of Free Updates - Buy CompTIA SY0-701 Questions Now

CompTIA

Security+

SY0-701

305 Practice Test Questions

in PDF Format with Verified Answers

DOWNLOAD the newest SurePassExams SY0-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1KtP0YyA7vjcuw_auSbRB8d-0nniE7yin

The best news is that during the whole year after purchasing, you will get the latest version of our SY0-701 exam prep for free, since as soon as we have compiled a new version of the study materials, our company will send the latest one of our SY0-701 study materials to your email immediately. And you will be satisfied by our service for we will auto send it to you as long as we update them. If you have to get our SY0-701 learning guide after one year, you can still enjoy 50% discounts off on the price.

CompTIA SY0-701 Exam Syllabus Topics:

Topic	Details
Topic 1	• Security Operations: This topic delves into applying common security techniques to computing resources, addressing security implications of proper hardware, software, and data asset management, managing vulnerabilities effectively, and explaining security alerting and monitoring concepts. It also discusses enhancing enterprise capabilities for security, implementing identity and access management, and utilizing automation and orchestration for secure operations.
Topic 2	• General Security Concepts: This topic covers various types of security controls, fundamental security concepts, the importance of change management processes in security, and the significance of using suitable cryptographic solutions.
Topic 3	• Security Program Management and Oversight: Finally, this topic discusses elements of effective security governance, the risk management process, third-party risk assessment, and management processes. Additionally, the topic focuses on security compliance requirements, types and purposes of audits and assessments, and implementing security awareness practices in various scenarios.

Topic 4	- Threats, Vulnerabilities, and Mitigations: In this topic, you'll find discussions comparing threat actors and motivations, explaining common threat vectors and attack surfaces, and outlining different types of vulnerabilities. Moreover, the topic focuses on analyzing indicators of malicious activity in scenarios and exploring mitigation techniques used to secure enterprises against threats.
Topic 5	- Security Architecture: Here, you'll learn about security implications across different architecture models, applying security principles to secure enterprise infrastructure in scenarios, and comparing data protection concepts and strategies. The topic also delves into the importance of resilience and recovery in security architecture.

>> Training SY0-701 Solutions <<

SY0-701 Latest Test Camp | SY0-701 Popular Exams

I think our SY0-701 test torrent will be a better choice for you than other study materials. We all known that most candidates will worry about the quality of our product, In order to guarantee quality of our study materials, all workers of our company are working together, just for a common goal, to produce a high-quality product; it is our SY0-701 Exam Questions. If you purchase our SY0-701 guide torrent, we can guarantee that we will provide you with quality products, reasonable price and professional after sales service.

CompTIA Security+ Certification Exam Sample Questions (Q611-Q616):

NEW QUESTION # 611
Which of the following phases of the incident response process attempts to minimize disruption?

- A. Recovery
- B. Preparation
- C. Containment
- D. Analysis

Answer: C

Explanation:
Containment is the phase where an organization attempts to minimize the damage caused by a security incident. This may involve isolating affected systems, blocking malicious traffic, or temporarily shutting down compromised services to prevent further impact.
Recovery (A) focuses on restoring normal operations after an incident.
Preparation (C) involves planning and readiness before an incident occurs.
Analysis (D) involves investigating the root cause and assessing the damage.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Security Operations domain.

NEW QUESTION # 612
An employee receives from a vendor a marketing communication email that includes an attachment. When the employee opens the attachment, the employee's screen displays odd text requesting payment in order to recover data. Within moments, a company-wide email is sent to employees requesting that employees disconnect their computers from the internet and shut them down. Which of the following describes this type of malware?

- A. Virus
- B. Worm
- C. Ransomware
- D. Trojan

Answer: C

Explanation:
Ransomware encrypts a user's files (displaying garbled text) and demands payment to restore access, matching the behavior described.

NEW QUESTION # 613

Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).

- A. The device's encryption level cannot meet organizational standards.
- B. The device is unable to receive authorized updates.
- C. The device is moved to a different location in the enterprise.
- D. The device is moved to an isolated segment on the enterprise network.
- E. The device is configured to use cleartext passwords.
- F. The device has been moved from a production environment to a test environment.

Answer: A

Explanation:

An engineer should recommend the decommissioning of a network device when the device poses a security risk or a compliance violation to the enterprise environment. A device that cannot meet the encryption standards or receive authorized updates is vulnerable to attacks and breaches, and may expose sensitive data or compromise network integrity. Therefore, such a device should be removed from the network and replaced with a more secure and updated one.

References

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, Section 2.2, page 671 CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 2, Question 16, page 512

NEW QUESTION # 614

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. :443
- B. encryption=off\
- C. www.*.com
- D. http://

Answer: D

Explanation:

Explanation

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).

NEW QUESTION # 615

A penetration test identifies that an SMBvl Is enabled on multiple servers across an organization. The organization wants to remediate this vulnerability in the most efficient way possible. Which of the following should the organization use for this purpose?

- A. ACL
- B. SFTP
- C. GPO
- D. DLP

Answer: C

Explanation:
"Group Policy Objects (GPOs) are a feature of Microsoft Windows Active Directory that allow administrators to centrally manage and configure settings across multiple systems in an efficient manner. When a vulnerability such as SMBv1 (Server Message Block version 1) is identified onmultiple servers, GPOs can be used to disable this outdated and insecure protocol across all affected systems simultaneously. By creating a GPO to enforce a policy that disables SMBv1, the organization can ensure consistent remediation without manually configuring each server individually, making it the most efficient solution for domain-joined environments." Reference:CompTIA Security+ SY0-701 Study Guide, Domain 3.0: Implementation, Section: "Secure System Configuration" (GPOs are covered under centralized management tools for implementing security policies).
Explanation:SMBv1 is an outdated and vulnerable protocol that should be disabled to mitigate risks, such as exploitation by attacks like WannaCry. The question emphasizes efficiency across multiple servers. Option A (GPO) allows an organization to push a policy to disable SMBv1 across all servers in an Active Directory environment with minimal effort, making it the most efficient choice. Option B (ACL) refers to Access Control Lists, which manage permissions but aren't designed for protocol configuration. Option C (SFTP) is a secure file transfer protocol unrelated to SMBv1 remediation. Option D (DLP) focuses on data loss prevention, not protocol vulnerabilities. Thus, A is the correct and most efficient solution.

NEW QUESTION # 616

......

- Valid SY0-701 Exam Simulator ♣ Test SY0-701 Questions Fee □ SY0-701 Latest Exam Papers □ Easily obtain ☀ SY0-701 □☀□ for free download through □ www.pdfvce.com □ □SY0-701 Exam Sims
- Clear SY0-701 Exam 🗟 SY0-701 Books PDF □ Valid SY0-701 Exam Dumps □ Open website [www.testkingpass.com] and search for ✔ SY0-701 □✔□ for free download □Test SY0-701 Dumps Demo
- 100% Pass Quiz 2026 SY0-701: Professional Training CompTIA Security+ Certification Exam Solutions □ Immediately open " www.pdfvce.com " and search for ➥ SY0-701 □ to obtain a free download □SY0-701 Reliable Test Syllabus
- 100% Pass Quiz SY0-701 - Authoritative Training CompTIA Security+ Certification Exam Solutions □ Search for [SY0-701] and download it for free immediately on ➠ www.prep4away.com □ □SY0-701 Exam Format
- www.stes.tyc.edu.tw, forum.phuongnamedu.vn, learn.raphael.ac.th, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes