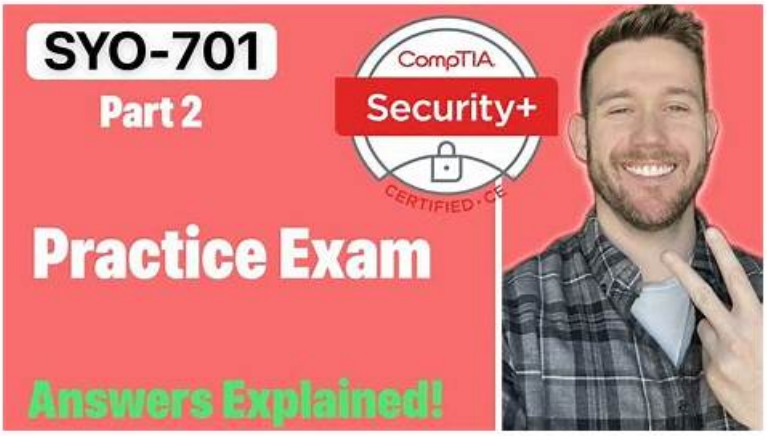
How Can ExamDiscuss SY0-701 Practice Questions be Helpful in Exam Preparation?



BTW, DOWNLOAD part of ExamDiscuss SY0-701 dumps from Cloud Storage: https://drive.google.com/open?id=1c-M1i8Rwk7TpCnJgtLh19iGsvO4Nd6Nu

It is indeed not easy to make a decision. SY0-701 study engine is willing to give you a free trial. If you have some knowledge of our SY0-701 training materials, but are not sure whether it is suitable for you, you can email us to apply for a free trial version. You know, we have provided three versions of SY0-701 practice quiz: the PDF, Software and APP online. Accordingly, we have three free trial versions as well.

Our SY0-701 exam materials have three different versions: the PDF, Software and APP online. All these three types of SY0-701 learning quiz win great support around the world and all popular according to their availability of goods, prices and other term you can think of. SY0-701 practice materials are of reasonably great position from highly proficient helpers who have been devoted to their quality over ten years to figure your problems out and help you pass the exam easily.

>> Free SY0-701 Practice Exams <<

Online SY0-701 Training Materials, SY0-701 Valid Braindumps Sheet

Likewise, Web-Based CompTIA SY0-701 exam questions are supported by all the major browsers like Chrome, Opera, Safari, Firefox, and IE. In the same way, the Web-based CompTIA Security+ Certification Exam pdf exam requires no special plugin. Lastly, the web-based CompTIA Security+ Certification Exam (SY0-701) practice exam is customizable and requires an active Internet connection.

CompTIA SY0-701 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• 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.
Topic 5	• 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.

CompTIA Security+ Certification Exam Sample Questions (Q699-Q704):

NEW QUESTION # 699
A penetration tester visits a client's website and downloads the site's content. Which of the following actions is the penetration tester performing?

- A. Vulnerability scan
- B. Unknown environment testing
- C. Passive reconnaissance
- D. Due diligence

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The described activity-visiting a website and downloading publicly accessible content-is a classic example of passive reconnaissance. Passive reconnaissance involves gathering information about a target without interacting with its internal systems or generating traffic that could be detected by security monitoring tools.
According to SY0-701, passive recon uses open-source intelligence (OSINT), such as:
* Public websites
* DNS records
* News articles
* Metadata
* Public document repositories
The key distinction is that passive reconnaissance does not probe the system for vulnerabilities, nor does it send active scanning traffic.
Vulnerability scanning (B) requires active probing. Unknown environment testing (A) applies to black-box testing but still may involve active scanning. Due diligence (C) refers to risk assessment or compliance reviews, not technical reconnaissance.
Therefore, downloading the website's content is a non-intrusive information-gathering technique, perfectly matching passive reconnaissance as defined in the exam materials under Threats, Vulnerabilities, Attack Vectors, and Pen Testing Phases.

NEW QUESTION # 700
A user downloaded software from an online forum. After the user installed the software, the security team observed external network traffic connecting to the user's computer on an uncommon port. Which of the following is the most likely explanation of this unauthorized connection?

- A. The software was ransomware.
- B. The user's computer had a fileless virus.
- C. The software contained a backdoor.
- D. The software had a hidden keylogger.

Answer: C

Explanation:
The software contained a backdoor bypassing normal authentication method.

NEW QUESTION # 701
Which of the following are cases in which an engineer should recommend the decommissioning of a network device? (Select two).

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

Answer: F

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 # 702
A security analyst is investigating an alert that was produced by endpoint protection software. The analyst determines this event was a false positive triggered by an employee who attempted to download a file. Which of the following is the most likely reason the download was blocked?

- A. A supply chain attack on the endpoint protection vendor
- B. A zero-day vulnerability in the file
- C. Incorrect file permissions
- D. A misconfiguration in the endpoint protection software

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Endpoint protection systems rely on policy rules, signatures, behavioral analytics, and heuristics. When the analyst identifies the event as a false positive, this indicates the file itself was not malicious, but the endpoint protection solution incorrectly identified it as a threat. According to CompTIA Security+ SY0-701 concepts, false positives commonly occur due to overly aggressive configuration settings, outdated rules, unrefined behavioral baselines, or incorrect threat signatures.
Zero-day vulnerabilities (B) would cause a true positive because the file contains unknown malware, not a false alert. A supply chain attack (C) would impact the vendor or update delivery, not a user download event.
Incorrect file permissions (D) prevent access but do not trigger malware alerts.
Misconfigurations are identified in SY0-701 under Security Operations # Monitoring, alerting, tuning, and false positives, which emphasizes the need for refining security controls to reduce erroneous blocks.
Therefore, the most likely cause of a blocked benign download is a misconfigured endpoint protection policy.

NEW QUESTION # 703
Which of the following can assist in recovering data if the decryption key is lost?

- A. CSR
- B. Escrow
- C. Salting
- D. Root of trust

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Key escrow is the process of storing encryption keys (or copies of them) with a trusted third party so data can be recovered if the primary decryption key is lost. In Security+ SY0-701, escrow is emphasized as a required safeguard for organizations that rely heavily on encryption, especially for regulated data or systems requiring guaranteed recoverability.
A CSR (A) is a Certificate Signing Request and does not store keys. Salting (B) is used with hashing to prevent password attacks and does not assist in data recovery. A root of trust (C) ensures secure hardware initialization but does not store backup decryption keys.
Key escrow directly addresses scenarios where encryption keys are misplaced, corrupted, deleted, or lost due to employee departure or system failure. Without escrow, encrypted data could become permanently inaccessible.
Thus, the correct answer is Escrow, the only mechanism specifically designed to allow recovery when decryption keys are unavailable.

NEW QUESTION # 704
.....

Users of this format don't need to install excessive plugins or software to attempt the CompTIA Security+ Certification Exam (SY0-701) web-based practice exams. Another format of the CompTIA Security+ Certification Exam (SY0-701) practice test is the desktop-based software. This SY0-701 Exam simulation software needs installation only on Windows computers to operate. The third format of the ExamDiscuss CompTIA SY0-701 exam dumps is the SY0-701 Dumps PDF.