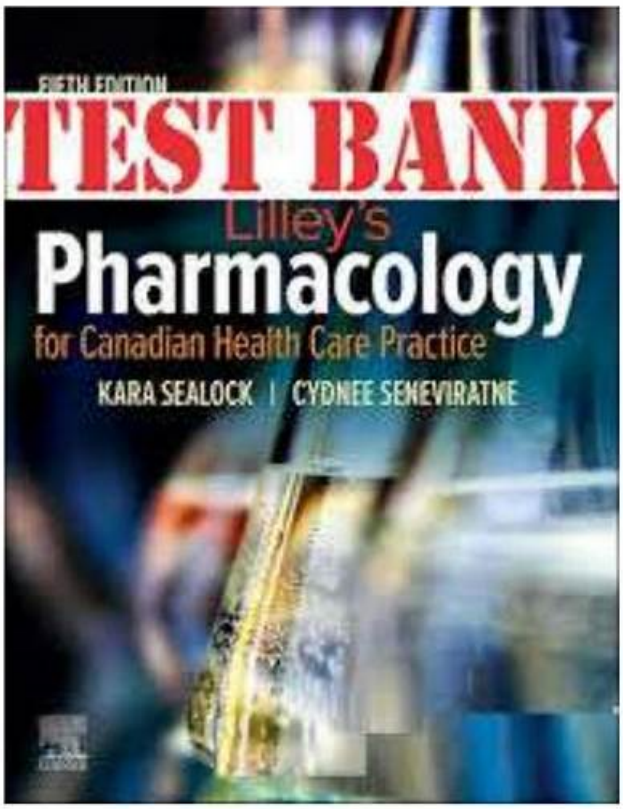
Practice Test CompTIA SY0-701 Pdf | SY0-701 Valid Test Tips



BTW, DOWNLOAD part of Lead2PassExam SY0-701 dumps from Cloud Storage: https://drive.google.com/open?id=1RQ4F2y7iViu1EJp0h2__H1CbF1vYyf-u

Our SY0-701 cram materials will help you gain the success in your career. You can be respected and enjoy the great fame among the industry. When applying for the jobs your resumes will be browsed for many times and paid high attention to. The odds to succeed in the job interview will increase. So you could see the detailed information of our SY0-701 Exam Questions before you decide to buy them on our web. Also we have free demo of our SY0-701 exam questions for you to try before you make the purchase.

CompTIA SY0-701 Exam Syllabus Topics:

Topic	Details

Topic 1	• 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 2	• 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 3	• 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 4	• 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 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 SY0-701 Valid Test Tips & SY0-701 Valid Exam Format

The only goal of all experts and professors in our company is to design the best and suitable study materials for all people. According to the different demands of many customers, they have designed the three different versions of the SY0-701 Study Materials for all customers. They sincerely hope that all people who use the SY0-701 study materials from our company can pass the exam and get the related certification successfully.

CompTIA Security+ Certification Exam Sample Questions (Q21-Q26):

NEW QUESTION # 21
Which of the following activities should a systems administrator perform to quarantine a potentially infected system?

- A. Disable remote log-in through Group Policy.
- B. Move the device into an air-gapped environment.
- C. Convert the device into a sandbox.
- D. Remote wipe the device using the MDM platform.

Answer: B

Explanation:
Quarantining a potentially infected system by placing it into an air-gapped environment physically disconnects it from the network. This prevents the spread of malware while maintaining the integrity of forensic evidence.

NEW QUESTION # 22
A systems administrator is redesigning now devices will perform network authentication. The following requirements need to be met:
* An existing Internal certificate must be used.
* Wired and wireless networks must be supported
* Any unapproved device should be Isolated in a quarantine subnet
* Approved devices should be updated before accessing resources

Which of the following would best meet the requirements?

- A. WPA2
- B. EAP
- C. RADIUS
- D. 802.IX

Answer: D

Explanation:
802.1X is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. It supports the use of certificates for authentication, can quarantine unapproved devices, and ensures that only approved and updated devices can access network resources. This protocol best meets the requirements of securing both wired and wireless networks with internal certificates.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of network security and authentication protocols.

NEW QUESTION # 23
Which of the following best describe a penetration test that resembles an actual external attach?

- A. Bug bounty
- B. Unknown environment
- C. Known environment
- D. Partially known environment

Answer: B

Explanation:
An unknown environment in penetration testing, also known as a black-box test, simulates an actual external attack where the tester has no prior knowledge of the system. This type of penetration test is designed to mimic real-world attack scenarios, where an attacker has little to no information about the target environment. The tester must rely on various reconnaissance and attack techniques to uncover vulnerabilities, much like a real-world attacker would. This approach helps organizations understand their security posture from an external perspective, providing insights into how their defenses would hold up against a true outsider threat.
Reference =
CompTIA Security+ SY0-701 Course Content: The course highlights the importance of understanding different penetration testing environments, including black-box testing, which aligns with the "unknown environment" in the provided answer.
CompTIA Security+ SY0-601 Study Guide: The guide details penetration testing methodologies, including black-box testing, which is crucial for simulating real external attacks.

NEW QUESTION # 24
A security administrator needs to create firewall rules for the following protocols: RTP, SIP,
H.323. and SRTP. Which of the following does this rule set support?

- A. VoIP
- B. HVAC
- C. RTOS
- D. SoC

Answer: A

Explanation:
The protocols RTP (Real-time Transport Protocol), SIP (Session Initiation Protocol), H.323, and SRTP (Secure Real-time Transport Protocol) are commonly used in Voice over IP (VoIP) communications. RTP handles the transport of media streams, SIP manages call setup and control, H.323 is a standard for multimedia communication, and SRTP provides encryption for RTP. Therefore, the firewall rules for these protocols support VoIP.

NEW QUESTION # 25
An employee in the accounting department receives an email containing a demand for payment tot services performed by a vendor

However, the vendor is not in the vendor management database. Which of the following in this scenario an example of?

- A. Invoice scam
- B. Pretexting
- C. Ransomware
- D. Impersonation

Answer: A

Explanation:
The scenario describes an instance where an employee receives a fraudulent invoice from a vendor that is not recognized in the company's vendor management system. This is a classic example of an invoice scam, where attackers attempt to trick organizations into making payments for fake or non-existent services. These scams often rely on social engineering tactics to bypass financial controls.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the context of social engineering attacks and common scams.

NEW QUESTION # 26
......

The CompTIA Security+ Certification Exam (SY0-701) practice test software also keeps a record of attempts, keeping users informed about their progress and allowing them to improve themselves. This feature makes it easy for SY0-701 desktop-based practice exam software users to focus on their mistakes and overcome them before the original attempt. Overall, the Windows-based CompTIA Security+ Certification Exam (SY0-701) practice test software has a user-friendly interface that facilitates candidates to prepare for the CompTIA Security+ Certification Exam (SY0-701) exam without facing technical issues.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

P.S. Free & New SY0-701 dumps are available on Google Drive shared by Lead2PassExam: https://drive.google.com/open?id=1RQ4F2y7iViu1EJp0h2__H1CbF1vYyf-u