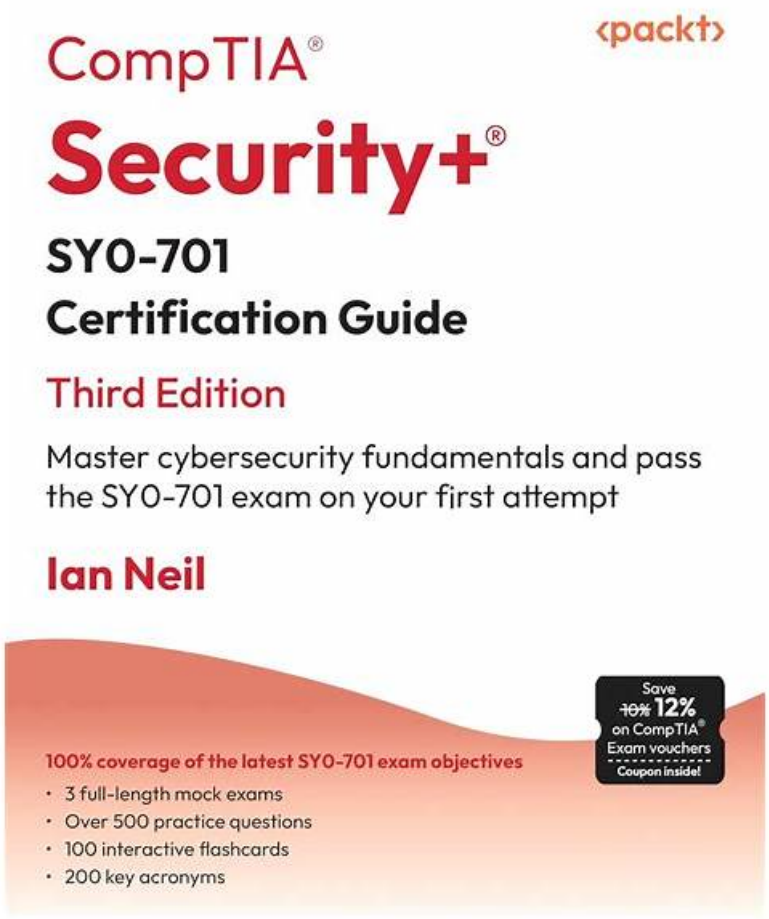
Hot Exam SY0-701 Guide | Professional SY0-701: CompTIA Security+ Certification Exam 100% Pass



DOWNLOAD the newest BraindumpsPrep SY0-701 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1NkylUM2cXPzrBJ-cX61xGyQmWRgigRmk

Under the tremendous stress of fast pace in modern life, this version of our SY0-701 test prep suits office workers perfectly. It can match your office software and as well as help you spare time practicing the SY0-701 exam. As for its shining points, the PDF version can be readily downloaded and printed out so as to be read by you. It's really a convenient way for those who are fond of paper learning. With this kind of version, you can flip through the pages at liberty and quickly finish the check-up SY0-701 Test Prep. And you can take notes on this version of our SY0-701 exam questions.

Choosing BraindumpsPrep's SY0-701 exam training materials is the best shortcut to success. It will help you to pass SY0-701 exam successfully. Everyone is likely to succeed, the key lies in choice. Under the joint efforts of everyone for many years, the passing rate of BraindumpsPrep's CompTIA SY0-701 Certification Exam has reached as high as 100%. Choosing BraindumpsPrep is to be with success.

>> Exam SY0-701 Guide <<

Latest Exam SY0-701 Guide for Real Exam

After your payment is successful, you will receive an e-mail from our system within 5-10 minutes, and then, you can use high-quality SY0-701 exam guide to learn immediately. Everyone knows that time is very important and hopes to learn efficiently to pass the SY0-701 exam. Once they discover SY0-701 practice materials, they will definitely want to seize the time to learn. So after payment, downloading into the exam database is the advantage of our products. The sooner you download and use SY0-701 guide torrent, the sooner you get the SY0-701 certificate.

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	• 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 3	• 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 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	• 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.

CompTIA Security+ Certification Exam Sample Questions (Q250-Q255):

NEW QUESTION # 250
A bank insists all of its vendors must prevent data loss on stolen laptops. Which of the following strategies is the bank requiring?

- A. Masking
- B. Permission restrictions
- C. Encryption at rest
- D. Data classification

Answer: C

Explanation:
Encryption at rest is a strategy that protects data stored on a device, such as a laptop, by converting it into an unreadable format that can only be accessed with a decryption key or password. Encryption at rest can prevent data loss on stolen laptops by preventing unauthorized access to the data, even if the device is physically compromised. Encryption at rest can also help comply with data privacy regulations and standards that require data protection. Masking, data classification, and permission restrictions are other strategies that can help protect data, but they may not be sufficient or applicable for data stored on laptops. Masking is a technique that obscures sensitive data elements, such as credit card numbers, with random characters or symbols, but it is usually used for data in transit or in use, not at rest. Data classification is a process that assigns labels to data based on its sensitivity and business impact, but it does not protect the data itself. Permission restrictions are rules that define who can access, modify, or delete data, but they may not prevent unauthorized access if the laptop is stolen and the security controls are bypassed. References: CompTIA Security+ Study Guide:
Exam SY0-701, 9th Edition, page 17-18, 372-373

NEW QUESTION # 251
Which of the following should a security administrator adhere to when setting up a new set of firewall rules?

- A. Business continuity plan

- B. Disaster recovery plan
- C. Incident response procedure
- D. Change management procedure

Answer: D

Explanation:
Explanation
A change management procedure is a set of steps and guidelines that a security administrator should adhere to when setting up a new set of firewall rules. A firewall is a device or software that can filter, block, or allow network traffic based on predefined rules or policies. A firewall rule is a statement that defines the criteria and action for a firewall to apply to a packet or a connection. For example, a firewall rule can allow or deny traffic based on the source and destination IP addresses, ports, protocols, or applications. Setting up a new set of firewall rules is a type of change that can affect the security, performance, and functionality of the network. Therefore, a change management procedure is necessary to ensure that the change is planned, tested, approved, implemented, documented, and reviewed in a controlled and consistent manner. A change management procedure typically includes the following elements:
A change request that describes the purpose, scope, impact, and benefits of the change, as well as the roles and responsibilities of the change owner, implementer, and approver.
A change assessment that evaluates the feasibility, risks, costs, and dependencies of the change, as well as the alternatives and contingency plans.
A change approval that authorizes the change to proceed to the implementation stage, based on the criteria and thresholds defined by the change policy.
A change implementation that executes the change according to the plan and schedule, and verifies the results and outcomes of the change.
A change documentation that records the details and status of the change, as well as the lessons learned and best practices.
A change review that monitors and measures the performance and effectiveness of the change, and identifies any issues or gaps that need to be addressed or improved.
A change management procedure is important for a security administrator to adhere to when setting up a new set of firewall rules, as it can help to achieve the following objectives:
Enhance the security posture and compliance of the network by ensuring that the firewall rules are aligned with the security policies and standards, and that they do not introduce any vulnerabilities or conflicts.
Minimize the disruption and downtime of the network by ensuring that the firewall rules are tested and validated before deployment, and that they do not affect the availability or functionality of the network services or applications.
Improve the efficiency and quality of the network by ensuring that the firewall rules are optimized and updated according to the changing needs and demands of the network users and stakeholders, and that they do not cause any performance or compatibility issues.
Increase the accountability and transparency of the network by ensuring that the firewall rules are documented and reviewed regularly, and that they are traceable and auditable by the relevant authorities and parties.
The other options are not correct because they are not related to the process of setting up a new set of firewall rules. A disaster recovery plan is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency. An incident response procedure is a set of steps and guidelines that aim to contain, analyze, eradicate, and recover from a security incident, such as a cyberattack, data breach, or malware infection. A business continuity plan is a set of strategies and actions that aim to maintain the essential functions and operations of an organization during and after a disruptive event, such as a pandemic, power outage, or civil unrest. References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.3: Security Operations, video: Change Management (5:45).

NEW QUESTION # 252
Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?

- A. Watering-hole
- B. Impersonation
- C. Disinformation
- D. Smishing

Answer: A

Explanation:
A watering-hole attack is a type of cyberattack that targets groups of users by infecting websites that they commonly visit. The

attackers exploit vulnerabilities to deliver a malicious payload to the organization's network. The attack aims to infect users' computers and gain access to a connected corporate network. The attackers target websites known to be popular among members of a particular organization or demographic. The attack differs from phishing and spear-phishing attacks, which typically attempt to steal data or install malware onto users' devices1 In this scenario, the compromised industry blog is the watering hole that the attackers used to spread malware across the company's network. The attackers likely chose this blog because they knew that the employees of the company were interested in its content and visited it frequently. The attackers may have injected malicious code into the blog or redirected the visitors to a spoofed website that hosted the malware. The malware then infected the employees' computers and propagated to the network.
Reference1: Watering Hole Attacks: Stages, Examples, Risk Factors & Defense ...

NEW QUESTION # 253
Which of the following scenarios describes a possible business email compromise attack?

- A. An employee receives a gift card request in an email that has an executive's name in the display field of the email.
- B. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.
- C. Employees who open an email attachment receive messages demanding payment in order to access files.
- D. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.

Answer: D

Explanation:
In a BEC attack, the attacker typically impersonates a high-ranking executive or authority figure within the organization and requests sensitive information or actions from employees. In this case, the HR director is requesting log-in credentials for a cloud administrator account, which is a classic example of BEC where the attacker seeks to gain access to privileged accounts through deception.

NEW QUESTION # 254
Which of the following data protection strategies can be used to confirm file integrity?

- A. Masking
- B. Obfuscation
- C. Hashing
- D. Encryption

Answer: C

Explanation:
Hashing (C)is aone-way cryptographic functionthat produces afixed-length digestrepresenting the original data. If the file changes-even by one bit-the hash will change, making it ideal for verifyingdata integrity.
While encryption protectsconfidentiality, and masking/obfuscation protectdata visibility, onlyhashing ensures integrity.

NEW QUESTION # 255
.....

- SY0-701 Clearer Explanation □ Customizable SY0-701 Exam Mode □ SY0-701 Clearer Explanation □ Enter ➤ www.pdfvce.com □ and search for ➤ SY0-701 □ to download for free □Reliable SY0-701 Exam Preparation
- CompTIA - Fantastic SY0-701 - Exam CompTIA Security+ Certification Exam Guide □ Search for ▹ SY0-701 ◃ and download it for free immediately on □ www.dumpsquestion.com □ □Valid SY0-701 Study Guide
- Pass Leader SY0-701 Dumps □ SY0-701 Latest Test Labs □ Valid SY0-701 Study Guide □ Search on □ www.pdfvce.com □ for ➠ SY0-701 □ to obtain exam materials for free download □New SY0-701 Test Tutorial
- CompTIA Security+ Certification Examlatest test questions - SY0-701 reliable braindumps - CompTIA Security+ Certification Examfree practice dumps □ The page for free download of [SY0-701] on ➤ www.exam4labs.com □ will open immediately □Customizable SY0-701 Exam Mode
- Top Exam SY0-701 Guide 100% Pass | Efficient Reliable SY0-701 Braindumps Pdf: CompTIA Security+ Certification Exam □ Download 【 SY0-701 】 for free by simply searching on [www.pdfvce.com] □SY0-701 Preparation
- SY0-701 Books PDF □ SY0-701 Valid Test Voucher □ SY0-701 Valid Test Voucher □ ➽ www.pass4test.com □ □ is best website to obtain ▸ SY0-701 ◂ for free download □Latest SY0-701 Exam Dumps
- SY0-701 Sample Questions Pdf □ SY0-701 Valid Exam Bootcamp □ SY0-701 Latest Braindumps Files □ Search on [www.pdfvce.com] for （ SY0-701 ） to obtain exam materials for free download □SY0-701 Reliable Exam Practice
- Top Exam SY0-701 Guide 100% Pass | Efficient Reliable SY0-701 Braindumps Pdf: CompTIA Security+ Certification Exam □ Search for " SY0-701 " and easily obtain a free download on 《 www.troytecdumps.com 》 ↴SY0-701 Reliable Exam Practice
- 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, wealthwisdomschool.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, shortcourses.russellcollege.edu.au, www.wcs.edu.eu, 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, www.stes.tyc.edu.tw, 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

BTW, DOWNLOAD part of BraindumpsPrep SY0-701 dumps from Cloud Storage: https://drive.google.com/open?id=1NkylUM2cXPzrBJ-cX61xGyQmWRgigRmk