Quiz 2025 SY0-701: Professional CompTIA Security+ Certification Exam Exam Sample Questions

What's more, part of that NewPassLeader SY0-701 dumps now are free: https://drive.google.com/open?id=1cQOxDzF89KGTnGu7Zvs3uLxU7jPZCYI6

Our website is a worldwide dumps leader that offers free valid SY0-701 braindumps for certification tests, especially for CompTIA practice test. We focus on the study of SY0-701 real exam for many years and enjoy a high reputation in IT field by latest study materials, updated information and, most importantly, SY0-701 Top Questions with detailed answers and explanations.

Our SY0-701 learning guide materials have won the favor of many customers by virtue of their high quality. Started when the user needs to pass the qualification test, choose the SY0-701 real questions, they will not have any second or even third backup options, because they will be the first choice of our practice exam materials. Our SY0-701 Practice Guide is devoted to research on which methods are used to enable users to pass the test faster. Therefore, through our unremitting efforts, our SY0-701 real questions have a pass rate of 98% to 100%.

>> SY0-701 Exam Sample Questions <<

CompTIA Security+ Certification Exam free download braindumps & SY0-701 latest exam test

The web-based SY0-701 practice test is accessible via any browser. This SY0-701 mock exam simulates the actual CompTIA SY0-701 exam and does not require any software or plugins. Compatible with iOS, Mac, Android, and Windows operating systems, it provides all the features of the desktop-based SY0-701 Practice Exam software.

CompTIA SY0-701 Exam Syllabus Topics:

Topic	Details

Topic 1	• 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 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 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 4	• 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 5	• 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.

CompTIA Security+ Certification Exam Sample Questions (Q633-Q638):

NEW QUESTION # 633
A security team is reviewing the findings in a report that was delivered after a third party performed a penetration test. One of the findings indicated that a web application form field is vulnerable to cross-site scripting. Which of the following application security techniques should the security analyst recommend the developer implement to prevent this vulnerability?

- A. Version control
- B. Code signing
- C. Secure cookies
- D. Input validation

Answer: D

Explanation:
Input validation is a technique that checks the user input for any malicious or unexpected data before processing it by the web application. Input validation can prevent cross-site scripting (XSS) attacks, which exploit the vulnerability of a web application to execute malicious scripts in the browser of a victim. XSS attacks can compromise the confidentiality, integrity, and availability of the web application and its users.
Input validation can be implemented on both the client-side and the server-side, but server-side validation is more reliable and secure. Input validation can use various methods, such as whitelisting, blacklisting, filtering, escaping, encoding, and sanitizing the input data. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 70. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 3.2, page 11. Application Security - SY0-601 CompTIA Security+ : 3.2

NEW QUESTION # 634
A technician wants to improve the situational and environmental awareness of existing users as they transition from remote to in-office work. Which of the following is the best option?

- A. Send out periodic security reminders.
- B. Update the content of new hire documentation.
- C. Modify the content of recurring training.

Answer: C

Explanation:
D Implement a phishing campaign
Explanation:
Recurring training is a type of security awareness training that is conducted periodically to refresh and update the knowledge and skills of the users. Recurring training can help improve the situational and environmental awareness of existing users as they transition from remote to in-office work, as it can cover the latest threats, best practices, and policies that are relevant to their work environment. Modifying the content of recurring training can ensure that the users are aware of the current security landscape and the expectations of their roles. Reference = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 232. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

NEW QUESTION # 635
A security analyst finds a rogue device during a monthly audit of current endpoint assets that are connected to the network. The corporate network utilizes 002.1X for access control. To be allowed on the network, a device must have a Known hardware address, and a valid user name and password must be entered in a captive portal. The following is the audit report:

IP address	MAC	Host	Account
10.18.04.42	BE-AC-11-F1-E4-44	PC-NY	user1
10.18.04.30	EB-AC-11-02-42-F3	PC-GA	user3
10.18.04.59	20-BB-5A-11-[illegible]	PC-PA	user2
10.18.04.58	20-[illegible]-E9-D1	PC-TX	user4
10.18.04.22	EB-AC-11-02-42-F3	WIN10	user3
10.18.04.26	BB-20-11-2[illegible]	[illegible]N3	admin

Which of the following is the most likely way a rogue device was allowed to connect?

- A. A user performed a MAC cloning attack with a personal device.
- B. DNS hijacking let an attacker intercept the captive portal traffic.
- C. A DMCP failure caused an incorrect IP address to be distributed
- D. An administrator bypassed the security controls for testing.

Answer: A

Explanation:
The most likely way a rogue device was able to connect to the network is through a MAC cloning attack. In this attack, a personal device copies the MAC address of an authorized device, bypassing the 802.1X access control that relies on known hardware addresses for network access. The matching MAC addresses in the audit report suggest that this technique was used to gain unauthorized network access.
Reference =
CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
CompTIA Security+ SY0-601 Study Guide: Chapter on Network Security and MAC Address Spoofing.

NEW QUESTION # 636
A company purchased cyber insurance to address items listed on the risk register. Which of the following strategies does this represent?

- A. Transfer
- B. Mitigate
- C. Accept
- D. Avoid

Answer: A

Explanation:
Cyber insurance is a type of insurance that covers the financial losses and liabilities that result from cyberattacks, such as data breaches, ransomware, denial-of-service, phishing, or malware. Cyber insurance can help a company recover from the costs of restoring data, repairing systems, paying ransoms, compensating customers, or facing legal actions. Cyber insurance is one of the possible strategies that a company can use to address the items listed on the risk register. A risk register is a document that records the identified risks, their probability, impact, and mitigation strategies for a project or an organization. The four common risk mitigation strategies are:

Accept: The company acknowledges the risk and decides to accept the consequences without taking any action to reduce or eliminate the risk. This strategy is usually chosen when the risk is low or the cost of mitigation is too high.
Transfer: The company transfers the risk to a third party, such as an insurance company, a vendor, or a partner. This strategy is usually chosen when the risk is high or the company lacks the resources or expertise to handle the risk.
Mitigate: The company implements controls or measures to reduce the likelihood or impact of the risk. This strategy is usually chosen when the risk is moderate or the cost of mitigation is reasonable.
Avoid: The company eliminates the risk by changing the scope, plan, or design of the project or the organization. This strategy is usually chosen when the risk is unacceptable or the cost of mitigation is too high.
By purchasing cyber insurance, the company is transferring the risk to the insurance company, which will cover the financial losses and liabilities in case of a cyberattack.
Therefore, the correct answer is B. Transfer. Reference = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 377. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.1: Risk Management, video: Risk Mitigation Strategies (5:37).

NEW QUESTION # 637
An external vendor recently visited a company's headquarters tor a presentation. Following the visit a member of the hosting team found a file that the external vendor left behind on a server. The file contained detailed architecture information and code snippets. Which of the following data types best describes this file?

- A. Critical
- B. Proprietary
- C. Government
- D. Public

Answer: B

Explanation:
The file left by the external vendor, containing detailed architecture information and code snippets, is best described as proprietary data. Proprietary data is information that is owned by a company and is essential to its competitive advantage. It includes sensitive business information such as trade secrets, intellectual property, and confidential data that should be protected from unauthorized access.
Reference = CompTIA Security+ SY0-701 study materials, particularly in the domain of data classification and protection.

NEW QUESTION # 638
.....

- Save Time and Money with www.dumps4pdf.com CompTIA SY0-701 Actual Questions □ Open □ www.dumps4pdf.com □ enter ➠ SY0-701 □ and obtain a free download □SY0-701 Valid Test Bootcamp
- SY0-701 - Efficient CompTIA Security+ Certification Exam Exam Sample Questions ▸ Search for □ SY0-701 □ on ▹ www.pdfvce.com ◃ immediately to obtain a free download □SY0-701 Certification Test Questions
- Study SY0-701 Plan □ SY0-701 Pass4sure Exam Prep □ Test SY0-701 Free □ Go to website 【 www.vceengine.com 】 open and search for { SY0-701 } to download for free □SY0-701 Online Exam
- 40bbk.com, www.huajiaoshu.com, phdkhulani.com, 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, deepcyclepower.com, arrayholding.com, www.pcsq28.com, study.stcs.edu.np, 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 NewPassLeader: https://drive.google.com/open?id=1cQOxDzF89KGTnGu7Zvs3uLxU7jPZCYI6