

CompTIA Penetration testers simulate SY0-701 Latest Dumps Book



P.S. Free & New SY0-701 dumps are available on Google Drive shared by TestkingPDF: <https://drive.google.com/open?id=1M8oIK-s0dBL-AnLcQZqCtu4X0Vz4iom0>

Our CompTIA Security+ Certification Exam study questions are suitable for a variety of levels of users, no matter you are in a kind of cultural level, even if you only have high cultural level, you can find in our SY0-701 training materials suitable for their own learning methods. So, for every user of our study materials are a great opportunity, a variety of types to choose from, more and more students also choose our SY0-701 Test Guide, then why are you hesitating? As long as you set your mind to, as long as you have the courage to try a new life, yearning for life for yourself, then to choose our CompTIA Security+ Certification Exam study questions, we will offer you in a short period of time effective way to learn, so immediately began to revise it, don't hesitate, let go to do!

CompTIA SY0-701 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">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	<ul style="list-style-type: none"> • 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 3	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.

>> Latest SY0-701 Dumps Book <<

SY0-701 Practice Online | Latest SY0-701 Test Voucher

The product we provide with you is compiled by professionals elaborately and boosts varied versions which aimed to help you learn the SY0-701 study materials by the method which is convenient for you. They check the update every day, and we can guarantee that you can get a free update service from the date of purchase. Once you have any questions and doubts about the SY0-701 Exam Questions we will provide you with our customer service before or after the sale, you can contact us if you have question or doubt about our exam materials and the professional personnel can help you solve your issue about using SY0-701 study materials.

CompTIA Security+ Certification Exam Sample Questions (Q798-Q803):

NEW QUESTION # 798

Users at a company are reporting they are unable to access the URL for a new retail website because it is flagged as gambling and is being blocked.

Which of the following changes would allow users to access the site?

- A. Tuning the DLP rule that detects credit card data
- B. Configuring the IPS to allow shopping
- **C. Updating the categorization in the content filter**
- D. Creating a firewall rule to allow HTTPS traffic

Answer: C

Explanation:

A content filter is a device or software that blocks or allows access to web content based on predefined rules or categories. In this case, the new retail website is mistakenly categorized as gambling by the content filter, which prevents users from accessing it. To resolve this issue, the content filter's categorization needs to be updated to reflect the correct category of the website, such as shopping or retail. This will allow the content filter to allow access to the website instead of blocking it.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Technologies and Tools, page 1221.

CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 3:

Technologies and Tools, page 1222.

NEW QUESTION # 799

In order to strengthen a password and prevent a hacker from cracking it, a random string of 36 characters was added to the password. Which of the following best describes this technique?

- A. Salting
- B. Tokenization
- C. Data masking
- D. Key stretching

Answer: A

Explanation:

Adding a random string of characters, known as a "salt," to a password before hashing it is known as salting. This technique strengthens passwords by ensuring that even if two users have the same password, their hashes will be different due to the unique salt, making it much harder for attackers to crack passwords using precomputed tables.

NEW QUESTION # 800

A security administrator needs a method to secure data in an environment that includes some form of checks so that the administrator can track any changes. Which of the following should the administrator set up to achieve this goal?

- A. GPO
- B. FIM
- C. SPF
- D. NAC

Answer: B

Explanation:

Explanation

FIM stands for File Integrity Monitoring, which is a method to secure data by detecting any changes or modifications to files, directories, or registry keys. FIM can help a security administrator track any unauthorized or malicious changes to the data, as well as verify the integrity and compliance of the data. FIM can also alert the administrator of any potential breaches or incidents involving the data.

Some of the benefits of FIM are:

It can prevent data tampering and corruption by verifying the checksums or hashes of the files.

It can identify the source and time of the changes by logging the user and system actions.

It can enforce security policies and standards by comparing the current state of the data with the baseline or expected state.

It can support forensic analysis and incident response by providing evidence and audit trails of the changes.

References:

CompTIA Security+ SY0-701 Certification Study Guide, Chapter 5: Technologies and Tools, Section

5.3: Security Tools, p. 209-210

CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 2: Technologies and Tools, Objective 2.4: Given a scenario, analyze and interpret output from security technologies, Sub-objective:

File integrity monitor, p. 12

NEW QUESTION # 801

A user needs to complete training at <https://comptiatraining.com>. After manually entering the URL, the user sees that the accessed website is noticeably different from the standard company website. Which of the following is the most likely explanation for the difference?

- A. Vishing
- B. Pretexting
- C. Typosquatting
- D. Cross-site scripting

Answer: C

Explanation:

Typosquatting (also known as URL hijacking) is a type of attack where cybercriminals register domain names similar to legitimate sites but with slight misspellings (e.g., comptiatraining.com instead of comptiatraining.com). Attackers use these fake sites to steal credentials or distribute malware. Since the user manually entered the URL and reached an unexpected website, this strongly indicates a typosquatting attack.

Reference:

NEW QUESTION # 802

A nation-state attacker gains access to the email accounts of several journalists by compromising a website that the journalists frequently use. Which of the following types of attacks describes this example?

- A. Brand impersonation
- **B. Watering-hole**
- C. Typosquatting
- D. On-path

Answer: B

Explanation:

The correct answer is Watering-hole because the attack involves compromising a legitimate website that is regularly visited by a specific group of targeted users—in this case, journalists—in order to indirectly infect or compromise them. The Security+ SY0-701 study guide defines watering-hole attacks as targeted attacks where adversaries identify websites frequented by their intended victims and then compromise those sites to deliver malware, steal credentials, or conduct further exploitation.

In this scenario, the attacker does not directly target the journalists' email systems. Instead, the attacker compromises a trusted website that the journalists frequently access. When the journalists visit the site, malicious code can be delivered through drive-by downloads, malicious scripts, or credential-harvesting mechanisms. This technique is particularly effective for nation-state attackers because it leverages trust and normal user behavior, making detection more difficult.

Option A, On-path, is incorrect because on-path (man-in-the-middle) attacks involve intercepting or altering communications between two parties in transit, rather than compromising a third-party website. Option C, Typosquatting, involves registering domains with misspelled names to trick users into visiting malicious sites, which is not described here. Option D, Brand impersonation, typically refers to phishing or spoofing attacks that mimic a trusted brand to deceive users, often via email or fake websites, rather than compromising a legitimate one.

The SY0-701 objectives emphasize that watering-hole attacks are commonly associated with advanced persistent threats (APTs), including nation-state actors, because they allow precise targeting of specific industries, professions, or organizations. This attack method highlights the importance of browser security, threat intelligence, web filtering, and user awareness to reduce exposure to trusted-but-compromised resources.

In summary, compromising a frequently used website to gain access to a targeted group's accounts is a textbook example of a watering-hole attack.

NEW QUESTION # 803

.....

We can say that the CompTIA SY0-701 practice questions are the top-notch CompTIA Security+ Certification Exam (SY0-701) dumps that will provide you with everything that you must need for instant SY0-701 exam preparation. Take the right decision regarding your quick CompTIA Security+ Certification Exam (SY0-701) exam questions preparation and download the real, valid, and updated CompTIA SY0-701 exam dumps and start this journey.

SY0-701 Practice Online: <https://www.testkingpdf.com/SY0-701-testking-pdf-torrent.html>

- 100% Pass 2026 CompTIA - SY0-701 - Latest CompTIA Security+ Certification Exam Dumps Book Immediately open www.dumpsquestion.com and search for [SY0-701] to obtain a free download SY0-701 Official Cert Guide
- Reliable SY0-701 Dumps Valid SY0-701 Test Online SY0-701 Questions Answers Simply search for SY0-701 for free download on www.pdfvce.com SY0-701 Official Cert Guide
- SY0-701 Practice Exam Questions Valid SY0-701 Test Online Exam SY0-701 Bootcamp Search for SY0-701 and download exam materials for free through “www.pass4test.com” SY0-701 Exam Experience
- Latest SY0-701 Test Pass4sure Exam Sample SY0-701 Questions Reliable SY0-701 Dumps Simply search for [SY0-701] for free download on [www.pdfvce.com] Exam SY0-701 Topic
- SY0-701 Valid Test Answers New SY0-701 Dumps Files SY0-701 Instant Download Enter www.practicevce.com and search for SY0-701 to download for free SY0-701 Valid Test Answers
- SY0-701 Latest Exam Guide New SY0-701 Dumps Files SY0-701 Valid Test Answers The page for free download of SY0-701 on www.pdfvce.com will open immediately SY0-701 Official Cert Guide
- Hot Latest SY0-701 Dumps Book | Reliable SY0-701: CompTIA Security+ Certification Exam 100% Pass Search for SY0-701 and obtain a free download on www.troytecdumps.com Exam Sample SY0-701 Questions

- SY0-701 Valid Test Answers Exam SY0-701 Bootcamp Valid SY0-701 Test Online The page for free download of “SY0-701 ” on ✓ www.pdfvce.com ✓ will open immediately SY0-701 Questions Answers
- 100% Pass 2026 CompTIA - SY0-701 - Latest CompTIA Security+ Certification Exam Dumps Book Search for ➔ SY0-701 and easily obtain a free download on www.torrentvce.com SY0-701 Torrent
- New SY0-701 Dumps Files ⇄ Exam Sample SY0-701 Questions SY0-701 Reliable Test Online Easily obtain free download of 「 SY0-701 」 by searching on ➔ www.pdfvce.com SY0-701 Practice Mock
- Hot Latest SY0-701 Dumps Book Pass Certify | Pass-Sure SY0-701 Practice Online: CompTIA Security+ Certification Exam Search for ➔ SY0-701 and download it for free immediately on ➔ www.pdfdumps.com SY0-701 Exam Experience
- www.stes.tyc.edu.tw, bicyclebuysell.com, www.xunshuzhilian.com, www.maoyestudio.com, bbs.t-firefly.com, bbs.agenew.cn, 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, mawada.om, devfolio.co, Disposable vapes

BONUS!!! Download part of TestkingPDF SY0-701 dumps for free: <https://drive.google.com/open?id=1M8oIK-s0dBL-AnLcQZqCtu4X0Vz4iomo>