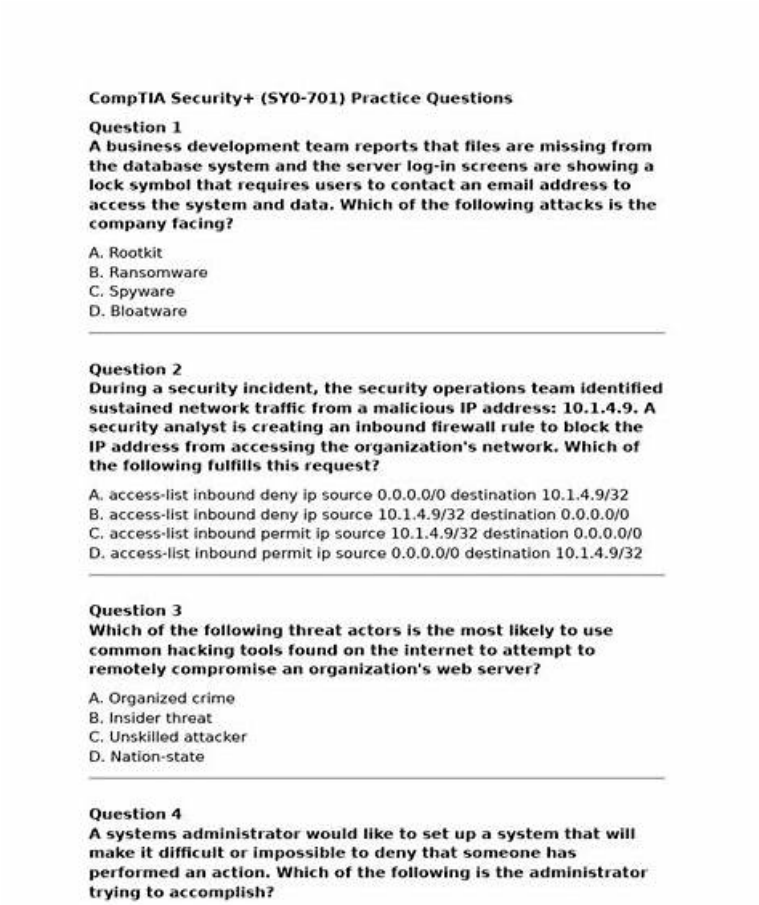
SY0-701 Exam Topics - New SY0-701 Exam Pdf



CompTIA Security+ (SY0-701) Practice Questions

Question 1
A business development team reports that files are missing from the database system and the server log-in screens are showing a lock symbol that requires users to contact an email address to access the system and data. Which of the following attacks is the company facing?

A. Rootkit
B. Ransomware
C. Spyware
D. Bloatware

Question 2
During a security incident, the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9. A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?

A. access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32
B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0
C. access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0
D. access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32

Question 3
Which of the following threat actors is the most likely to use common hacking tools found on the internet to attempt to remotely compromise an organization's web server?

A. Organized crime
B. Insider threat
C. Unskilled attacker
D. Nation-state

Question 4
A systems administrator would like to set up a system that will make it difficult or impossible to deny that someone has performed an action. Which of the following is the administrator trying to accomplish?

P.S. Free & New SY0-701 dumps are available on Google Drive shared by ExamTorrent: https://drive.google.com/open?id=1dUm6mXIoA8YvbNfUTHFa3lp6XBiw6-5z

With the help of ExamTorrent CompTIA SY0-701 dumps torrent, it is more time-saving effort to get CompTIA SY0-701 certification. In fact, you are not far from success. With ExamTorrent CompTIA SY0-701 exam dumps, you must be IT talent. We provide you with free demo and pdf real questions and answers for further acquaintance. If you make use of our CompTIA SY0-701 Exam Dumps, we will accompany you on your road to success.

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	• 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 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	• 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.

>> SY0-701 Exam Topics <<

New SY0-701 Exam Pdf & SY0-701 Study Material

Another thing you will get from using the SY0-701 Exam study material is free to support. If you encounter any problem while using the SY0-701 material, you have nothing to worry about. The solution is closer to you than you can imagine, just contact the support team and continue enjoying your study with the CompTIA Security+ Certification Exam preparation material.

CompTIA Security+ Certification Exam Sample Questions (Q209-Q214):

NEW QUESTION # 209
Prior to implementing a design change, the change must go through multiple steps to ensure that it does not cause any security issues. Which of the following is most likely to be one of those steps?

- A. Load testing
- B. Procedure updates
- C. Management review
- D. Maintenance notifications

Answer: C

Explanation:
Management review is a critical step in the change management process. Before implementing any design change, management reviews help evaluate the potential impact, security implications, and alignment with organizational goals and policies. This review ensures that the change is justified, risks are understood, and proper approvals are obtained.
Load testing is a performance test, maintenance notifications are communication steps, and procedure updates are documentation activities - all important but generally occur after management has approved the change.
The significance of management involvement in change governance is a foundational concept in the Security Program Management and Oversight domain of the SY0-701 exam#6:Chapter 16 CompTIA Security+ Study Guide#.

NEW QUESTION # 210
An auditor notices that, before logging into the firewall, an employee opens a document in a shared folder that contains administrative credentials. Which of the following should the auditor recommend implementing?

- A. Situational awareness
- B. Operational security
- C. Acceptable use policy
- D. Password management

Answer: D

Explanation:
Password management solutions securely store and manage credentials, preventing risky practices like keeping administrative credentials in shared folders, which can lead to unauthorized access.

NEW QUESTION # 211
A company identified the potential for malicious insiders to harm the organization. Which of the following measures should the organization implement to reduce this risk?

- A. Unified threat management
- B. User behavior analytics
- C. Intrusion detection system
- D. Web application firewall

Answer: B

Explanation:
User Behavior Analytics (UBA)is specifically designed to detectanomalous or suspicious behaviorsby users that may indicate insider threats. UBA toolsestablish a baseline of normalbehaviorfor users and alert security teams when deviations occur (e.g., accessing sensitive files at odd hours, downloading large volumes of data, etc.).
Malicious insiders often bypass perimeter defenses like firewalls or IDS/IPS systems because they arelegitimate users. UBA offersvisibility into internal behavior patterns, which is essential for detecting these threats.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.2 - "Insider threats and behavioral analytics (e.g., UBA, UEBA)."

NEW QUESTION # 212
A company is reviewing options to enforce user logins after several account takeovers. The following conditions must be met as part of the solution:
- Allow employees to work remotely or from assigned offices around the world.
- Provide a seamless login experience.
- Limit the amount of equipment required.
Which of the following best meets these conditions?

- A. Geotagging
- B. Trusted devices
- C. Time-based logins
- D. Smart cards

Answer: B

Explanation:
Trusted devices allow users to log in seamlessly from devices that are already recognized and trusted by the system. It supports remove and global access as the device does not need to be in a specific location or equipped with extra hardware. It minimizes the need for additional equipment and provides for a streamlined login experience.

NEW QUESTION # 213
Which of the following is a technical security control?

- A. Policy
- B. Firewall
- C. Security guard
- D. Fence

Answer: B

Explanation:
Firewalls are classic examples of technical controls as they use technology to restrict or permit network traffic based on security policies. Technical controls are implemented through hardware or software solutions.
Security guards (A) and fences (C) are physical controls, while policies (B) are administrative controls.

Technical controls like firewalls are fundamental in securing network perimeters and endpoints as covered in the Security Architecture domain#6:Chapter 3 CompTIA Security+ Study Guide#.

NEW QUESTION # 214

.....

Our SY0-701 Study Guide is famous for its instant download, we will send you the downloading link to you once we receive your payment, and you can down right now. Besides the SY0-701 study guide is verified by the professionals, so we can ensure that the quality of it. We also have free update, you just need to receive the latest version in your email address. If you don't have it, you can check in your junk mail or you can contact us.

New SY0-701 Exam Pdf: https://www.examtorrent.com/SY0-701-valid-vce-dumps.html

- SY0-701 Instant Discount □ Practical SY0-701 Information □ SY0-701 Test Labs □ Open website ➡ www.exam4labs.com □□□ and search for [SY0-701] for free download □SY0-701 Instant Discount
- Trusted SY0-701 Exam Topics - Realistic New SY0-701 Exam Pdf - Valid CompTIA CompTIA Security+ Certification Exam ✴ Easily obtain ➡ SY0-701 □□□ for free download through □ www.pdfvce.com □ □SY0-701 Reliable Test Sims
- Latest SY0-701 Test Format □ Valid SY0-701 Exam Test □ SY0-701 Reliable Test Question □ Search on ⇛ www.verifieddumps.com ⇚ for ➡ SY0-701 □□□ to obtain exam materials for free download □SY0-701 Test Labs
- Trusted SY0-701 Exam Topics - Realistic New SY0-701 Exam Pdf - Valid CompTIA CompTIA Security+ Certification Exam □ Easily obtain free download of ➡ SY0-701 □□□ by searching on ☀ www.pdfvce.com □☀□ □Latest SY0-701 Test Format
- Test SY0-701 Valid □ SY0-701 New Exam Camp □ SY0-701 Reliable Braindumps Ebook □ Open ▸ www.pass4test.com ◂ enter （ SY0-701 ） and obtain a free download □Practical SY0-701 Information
- Training SY0-701 Tools □ Test SY0-701 Valid □ PDF SY0-701 Cram Exam □ □ www.pdfvce.com □ is best website to obtain ➠ SY0-701 □ for free download □SY0-701 Reliable Exam Tutorial
- SY0-701 Reliable Test Sims □ SY0-701 Test Labs □ SY0-701 Instant Discount □ Copy URL { www.examdiscuss.com } open and search for ➥ SY0-701 □ to download for free □SY0-701 Related Content
- SY0-701 Reliable Test Sims □ SY0-701 Instant Discount □ SY0-701 PDF Download □ Search for 《 SY0-701 》 and easily obtain a free download on ➤ www.pdfvce.com □ □Latest SY0-701 Test Format
- Get the Latest SY0-701 Exam Topics for Immediate Study and Instant Success □ Easily obtain ➥ SY0-701 □ for free download through （ www.exam4labs.com ） □Test SY0-701 Valid
- 2026 SY0-701: Trustable CompTIA Security+ Certification Exam Exam Topics □ Search for 【 SY0-701 】 on ☀ www.pdfvce.com □☀□ immediately to obtain a free download □PDF SY0-701 Cram Exam
- Reliable SY0-701 Real Test □ SY0-701 Related Content □ SY0-701 Exam Sample Questions □ ➡ www.exam4labs.com □□□ is best website to obtain 《 SY0-701 》 for free download □SY0-701 Real Brain Dumps
- faithlife.com, www.slideshare.net, scalar.usc.edu, disqus.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, scalar.usc.edu, telegra.ph, freestyler.ws, pixabay.com, scalar.usc.edu, Disposable vapes

What's more, part of that ExamTorrent SY0-701 dumps now are free: https://drive.google.com/open?id=1dUm6mXIoA8YvbNfUTHFa3lp6XBiw6-5z