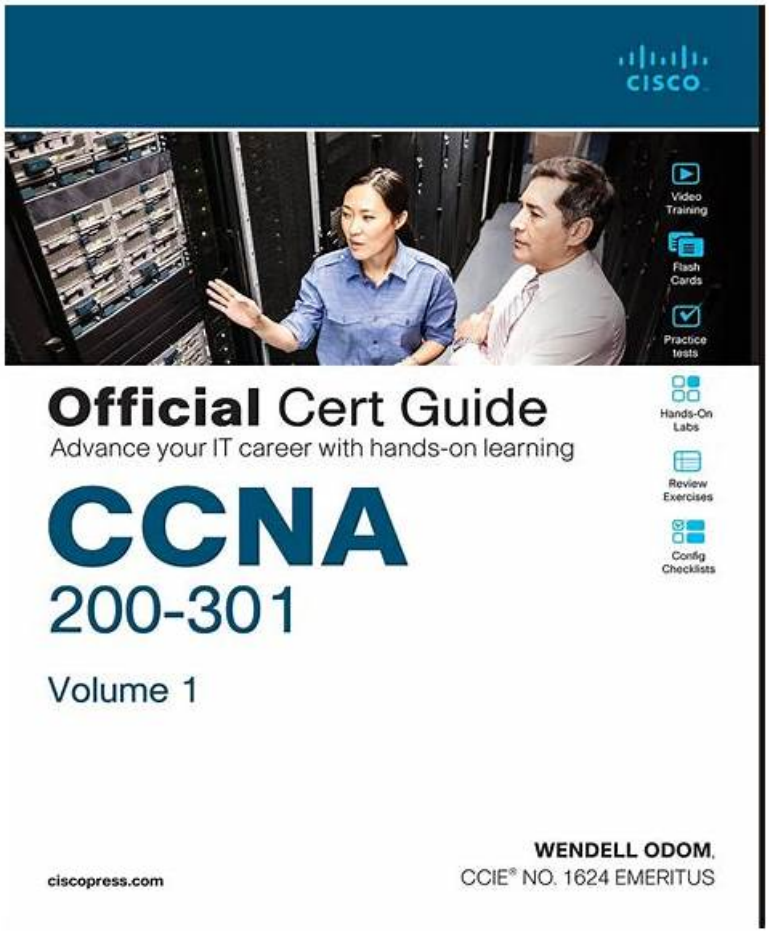
New SY0-701 Exam Labs | SY0-701 Exam Consultant



BTW, DOWNLOAD part of ActualtestPDF SY0-701 dumps from Cloud Storage: https://drive.google.com/open?id=10kPI-q7-kjFmH-ZD1y1dzzihl3FClYqO

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.

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	• 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	• 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 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 SY0-701 Desktop Practice Exam Software

This desktop practice exam software completely depicts the CompTIA SY0-701 exam scenario with proper rules and regulations and any other plugins to access CompTIA SY0-701 Practice Test. One such trustworthy point about exam preparation material is that it first gains your trust, and then asks you to purchase it.

CompTIA Security+ Certification Exam Sample Questions (Q452-Q457):

NEW QUESTION # 452
Which of the following must be considered when designing a high-availability network? (Choose two).

- A. Extensible authentication
- B. Responsiveness
- C. Attack surface
- D. Ability to patch
- E. Ease of recovery
- F. Physical isolation

Answer: B,E

Explanation:
Ease of recovery: High-availability networks should be designed in a way that allows for quick and easy recovery in the event of a failure. Redundancy, failover mechanisms, and backup systems are some of the components that can help facilitate smooth recovery.
Responsiveness: High-availability networks need to be responsive to ensure that any potential issues or failures are quickly detected, and appropriate actions are taken promptly to minimize downtime and impact.

NEW QUESTION # 453
A security administrator receives multiple reports about the same suspicious email. Which of the following is the most likely reason for the malicious email's continued delivery?

- A. Employees are forwarding personal emails to company email addresses.
- B. Employees are flagging legitimate emails as spam.
- C. Employees are using shadow IT solutions for email.
- D. Information from reported emails is not being used to tune email filtering tools.

Answer: D

Explanation:
If email filtering tools are not tuned based on reported emails, malicious emails will continue to bypass filters. Effective filtering depends on feedback and updating rules with real threat data.
Flagging legitimate emails (A) would cause false positives, shadow IT (C) and forwarding personal emails (D) are less relevant to the filtering bypass.
Tuning email filters is part of continuous Security Operations processes#6:Chapter 14 CompTIA Security+ Study Guide#.

NEW QUESTION # 454
A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

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

Answer: B

Explanation:
Ransomware-as-a-service is a type of cybercrime where hackers sell or rent ransomware tools or services to other criminals who use them to launch attacks and extort money from victims. This is a typical example of organized crime, which is a group of criminals who work together to conduct illegal activities for profit. Organized crime is different from other types of threat actors, such as insider threats, hacktivists, or nation-states, who may have different motives, methods, or targets. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 17 1

NEW QUESTION # 455
Which of the following has been implemented when a host-based firewall on a legacy Linux system allows connections from only specific internal IP addresses?

- A. Transfer of risk
- B. SNMP traps
- C. Compensating control
- D. Network segmentation

Answer: C

Explanation:
A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a weakness that cannot be resolved by the primary control. A compensating control does not prevent or eliminate the vulnerability or weakness, but it can reduce the likelihood or impact of an attack. A host-based firewall on a legacy Linux system that allows connections from only specific internal IP addresses is an example of a compensating control, as it can limit the exposure of the system to potential threats from external or unauthorized sources. A host-based firewall is a software application that monitors and filters the incoming and outgoing network traffic on a single host, based on a set of rules or policies. A legacy Linux system is an older version of the Linux operating system that may not be compatible with the latest security updates or patches, and may have known vulnerabilities or weaknesses that could be exploited by attackers. References = Security Controls - SY0-601 CompTIA Security+ : 5.1, Security Controls - CompTIA Security+ SY0-501 - 5.7, CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 240. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

NEW QUESTION # 456
An administrator notices that several users are logging in from suspicious IP addresses. After speaking with the users, the administrator determines that the employees were not logging in from those IP addresses and resets the affected users' passwords. Which of the following should the administrator implement to prevent this type of attack from succeeding in the future?

- A. Multifactor authentication
- B. Permissions assignment
- C. Access management
- D. Password complexity

Answer: A

Explanation:
The correct answer is A because multifactor authentication (MFA) is a method of verifying a user's identity by requiring more than one factor, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access even if the user's password is compromised, as the attacker would need to provide another factor to log in. The other options are incorrect because they do not address the root cause of the attack, which is weak authentication. Permissions assignment (B) is the process of granting or denying access to resources based on the user's role

or identity. Access management is the process of controlling who can access what and under what conditions. Password complexity (D) is the requirement of using strong passwords that are hard to guess or crack, but it does not prevent an attacker from using a stolen password. Reference = You can learn more about multifactor authentication and other security concepts in the following resources:
CompTIA Security+ SY0-701 Certification Study Guide, Chapter 1: General Security Concepts1 Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.2: Security Concepts2 Multi-factor Authentication - SY0-601 CompTIA Security+ : 2.43 TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 3: Identity and Access Management, Lecture 15: Multifactor Authentication4 CompTIA Security+ Certification SY0-601: The Total Course [Video], Chapter 3: Identity and Account Management, Section 2: Enabling Multifactor Authentication5

NEW QUESTION # 457
.....

Just choose the right ActualtestPDF CompTIA SY0-701 exam questions format demo and download it quickly. Download the CompTIA SY0-701 exam questions demo now and check the top features of CompTIA SY0-701 Exam Questions. If you think the CompTIA SY0-701 exam dumps can work for you then take your buying decision. Best of luck in exams and career!!!

P.S. Free 2026 CompTIA SY0-701 dumps are available on Google Drive shared by ActualtestPDF: https://drive.google.com/open?id=10kPI-q7-kjFmH-ZD1y1dzzihl3FClYqO