Free SY0-701 Updates & Valid Test SY0-701 Testking

BTW, DOWNLOAD part of ActualTestsIT SY0-701 dumps from Cloud Storage: https://drive.google.com/open?id=1ABVaskJSgCpHVUzGbnohr21tlxohQnfa

For candidates who are going to attend the exam, the pass rate is quite important. SY0-701 training materials of us are pass guaranteed, and if you can't pass the exam one time, we are money back guaranteed. Besides SY0-701 training materials are verified by skilled experts, therefore the quality and accuracy can be guaranteed, and you can use the SY0-701 Exam Dumps at ease. We also have online and offline chat service stuff, if any other questions, please contact us, we will give a reply to you as quickly as possible.

CompTIA SY0-701 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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 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 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.

>> Free SY0-701 Updates <<

Valid Test CompTIA SY0-701 Testking & SY0-701 Dumps Vce

The internet is transforming society, and distance is no longer an obstacle. You can download our SY0-701 exam simulation from our official website, which is a professional platform providing the most professional SY0-701 practice materials. You can get them within 15 minutes without waiting. What is more, you may think these high quality SY0-701 Preparation materials require a huge investment on them. Yes, we do invest a lot to ensure that you can receive the best quality and service.

CompTIA Security+ Certification Exam Sample Questions (Q112-Q117):

NEW QUESTION # 112
A security administrator needs to create firewall rules for the following protocols: RTP, SIP, H.323. and SRTP. Which of the following does this rule set support?

- A. SoC
- B. RTOS
- C. HVAC
- D. VoIP

Answer: D

Explanation:
The protocols RTP (Real-time Transport Protocol), SIP (Session Initiation Protocol), H.323, and SRTP (Secure Real-time Transport Protocol) are commonly used in Voice over IP (VoIP) communications. RTP handles the transport of media streams, SIP manages call setup and control, H.323 is a standard for multimedia communication, and SRTP provides encryption for RTP. Therefore, the firewall rules for these protocols support VoIP.

NEW QUESTION # 113
The internal audit team determines a software application is no longer in scope for external reporting requirements. Which of the following will confirm that the application is no longer applicable?

- A. Due care and due diligence
- B. Data inventory and retention
- C. Right to be forgotten
- D. Acknowledgement and attestation

Answer: B

NEW QUESTION # 114
An administrator is Investigating an incident and discovers several users' computers were Infected with malware after viewing files mat were shared with them. The administrator discovers no degraded performance in the infected machines and an examination of the log files does not show excessive failed logins. Which of the following attacks Is most likely the cause of the malware?

- A. Cryptojacking
- B. Malicious flash drive
- C. Brute-forced password
- D. Remote access Trojan

Answer: A

Explanation:
Cryptojacking is the likely cause in this scenario. It involves malware that hijacks the resources of infected computers to mine cryptocurrency, usually without the user's knowledge. This type of attack doesn't typically degrade performance significantly or result in obvious system failures, which matches the situation described, where the machines showed no signs of degraded performance or excessive failed logins.

NEW QUESTION # 115
An enterprise is trying to limit outbound DNS traffic originating from its internal network. Outbound DNS requests will only be

allowed from one device with the IP address 10.50.10.25. Which of the following firewall ACLs will accomplish this goal?

- A. Access list outbound permit 0.0.0.0/0 10.50.10.25 32 port 53 Access list outbound deny 0.0.0.0 0 0.0.0.0/0 port 53
- B. Access list outbound permit 10.50.10.25 32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0.0.0.0.0.0.0/0 port 53
- C. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 10.50.10.25 32 0.0.0.0/0 port 53
- D. Access list outbound permit 0.0.0.0 0 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 10.50.10.25 32 port 53

Answer: B

Explanation:
Explanation
The correct answer is D because it allows only the device with the IP address 10.50.10.25 to send outbound DNS requests on port 53, and denies all other devices from doing so. The other options are incorrect because they either allow all devices to send outbound DNS requests (A and C), or they allow no devices to send outbound DNS requests (B). References = You can learn more about firewall ACLs and DNS in the following resources:
* CompTIA Security+ SY0-701 Certification Study Guide, Chapter 4: Network Security1
* Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 3.2: Firewall Rules2
* TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 6: Network Security, Lecture 28: Firewall Rules3

NEW QUESTION # 116
A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours.
Which of the following is most likely occurring?

- A. Data is being exfiltrated.
- B. Ransomware is encrypting files.
- C. A worm is propagating across the network.
- D. A logic bomb is deleting data.

Answer: A

Explanation:
Data exfiltration is a technique that attackers use to steal sensitive data from a target system or network by transmitting it through DNS queries and responses. This method is often used in advanced persistent threat (APT) attacks, in which attackers seek to persistently evade detection in the target environment. A large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours is a strong indicator of data exfiltration. A worm, a logic bomb, and ransomware would not use DNS queries to communicate with their command and control servers or perform their malicious actions.

NEW QUESTION # 117
......

Three Formats of Actual CompTIA SY0-701 Exam Questions Offered By ActualTestsIT! CompTIA Security+ Certification Exam SY0-701 genuine dumps are designed in the three best formats. The name of these three formats of ActualTestsIT CompTIA SY0-701 exam questions is SY0-701 PDF Questions formats, Web-based and desktop CompTIA SY0-701 practice exam software. CompTIA SY0-701 dumps pdf format will help you to immediately prepare for the CompTIA SY0-701 exam.

Valid Test SY0-701 Testking: https://www.actualtestsit.com/CompTIA/SY0-701-exam-prep-dumps.html

- Test SY0-701 Question 🠾 Guaranteed SY0-701 Questions Answers 🠾 SY0-701 Exam Preview ❊ Open ✔ www.validtorrent.com 🠾✔🠾 and search for ➡ SY0-701 🠾 to download exam materials for free 🠾SY0-701 Preparation Store
- Fantastic SY0-701 Study Questions deliver you high-quality Exam Brain Dumps - Pdfvce 🠾 Search for 🠾 SY0-701 🠾 and easily obtain a free download on 🠾 www.pdfvce.com 🠾 ⚒ SY0-701 Reliable Exam Voucher
- SY0-701 Latest Exam Labs 🠾 SY0-701 Preparation Store 🠾 SY0-701 Preparation Store 🠾 Search for ⇒ SY0-701