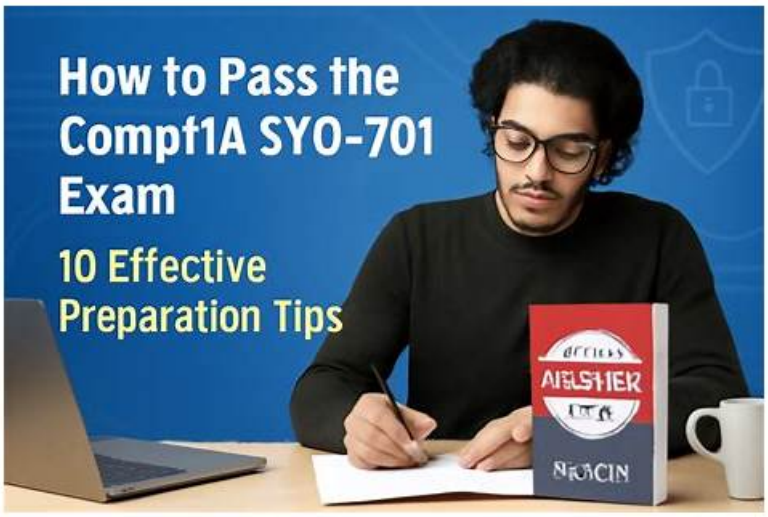
CompTIA SY0-701 Exam Dumps - Smart Way To Pass Exam



What's more, part of that BraindumpsIT SY0-701 dumps now are free: https://drive.google.com/open?id=1tkWPnWLAlaTBswiBXAndsKlUc03sW6iF

As long as you enter the learning interface of our soft test engine of SY0-701 quiz guide and start practicing on our Windows software, you will find that there are many small buttons that are designed to better assist you in your learning. When you want to correct the answer after you finish learning, the correct answer for our SY0-701 Test Prep is below each question, and you can correct it based on the answer. In addition, we design small buttons, which can also show or hide the SY0-701 exam torrent, and you can flexibly and freely choose these two modes according to your habit.

In order to facilitate the user's offline reading, the SY0-701 study braindumps can better use the time of debris to learn, especially to develop PDF mode for users. In this mode, users can know the SY0-701 prep guide inside the learning materials to download and print, easy to take notes on the paper, and weak link of their memory, at the same time, every user can be downloaded unlimited number of learning, greatly improve the efficiency of the users with our SY0-701 Exam Questions. Or you will forget the so-called good, although all kinds of digital device convenient now we read online, but many of us are used by written way to deepen their memory patterns. Our SY0-701 prep guide can be very good to meet user demand in this respect, allow the user to read and write in a good environment continuously consolidate what they learned.

>> SY0-701 Exam Success <<

SY0-701 Test Certification Cost, SY0-701 Download

Free demo is available for CompTIA SY0-701 training materials, so that you can have a better understanding of what you are going to buy. Free demo will represent you what the complete version is like. We suggest you try free domo before buying. In addition, CompTIA Security+ Certification Exam SY0-701 Training Materials are high quality and accuracy, since we have a professional team to collect the latest information of the exam.

CompTIA Security+ Certification Exam Sample Questions (Q659-Q664):

NEW QUESTION # 659
Which of the following would best prepare a security team for a specific incident response scenario?

- A. Root cause analysis
- B. Tabletop exercise
- C. Situational awareness
- D. Risk assessment

Answer: B

Explanation:
ATabletop exercise (D)is adiscussion-based simulationof an incident scenario. It allows security teams towalk through procedures, responsibilities, and communicationsin alow-pressure environment, improving readiness without impacting operations.
It is specifically designed toprepare teams for real-world incident handling.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 5.4 - "Incident response plans and exercises:
Tabletop exercises."

NEW QUESTION # 660
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 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 10.50.10.25 32 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 port 53
- C. 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
- D. 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

Answer: B

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 # 661
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. A worm is propagating across the network.
- B. Data is being exfiltrated.
- C. A logic bomb is deleting data.
- D. Ransomware is encrypting files.

Answer: B

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 # 662
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.
INSTRUCTIONS
Not all attacks and remediation actions will be used.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Answer:

Explanation:
Explanation
Web serverBotnet Enable DDoS protectionUser RAT Implement a host-based IPSDatabase server Worm Change the default application passwordExecutive KeyloggerDisable vulnerable servicesApplication Backdoor Implement 2FA using push notification
A screenshot of a computer program Description automatically generated with low confidence

NEW QUESTION # 663
A company needs to provide administrative access to internal resources while minimizing the traffic allowed through the security boundary. Which of the following methods is most secure?

- A. Installing a WAF
- B. Deploying a perimeter network
- C. Utilizing single sign-on
- D. Implementing a bastion host

Answer: D

Explanation:
A bastion host is a special-purpose server that is designed to withstand attacks and provide secure access to internal resources. A bastion host is usually placed on the edge of a network, acting as a gateway or proxy to the internal network. A bastion host can be configured to allow only certain types of traffic, such as SSH or HTTP, and block all other traffic. A bastion host can also run security software such as firewalls, intrusion detection systems, and antivirus programs to monitor and filter incoming and outgoing traffic. A bastion host can provide administrative access to internal resources by requiring strong authentication and encryption, and by logging all activities for auditing purposes12.
A bastion host is the most secure method among the given options because it minimizes the traffic allowed through the security boundary and provides a single point of control and defense. A bastion host can also isolate the internal network from direct exposure to the internet or other untrusted networks, reducing the attack surface and the risk of compromise3.
Deploying a perimeter network is not the correct answer, because a perimeter network is a network segment that separates the internal network from the external network. A perimeter network usually hosts public-facing services such as web servers, email servers, or DNS servers that need to be accessible from the internet. A perimeter network does not provide administrative access to internal resources, but rather protects them from unauthorized access. A perimeter network can also increase the complexity and cost of network management and security4.
Installing a WAF is not the correct answer, because a WAF is a security tool that protects web applications from common web-based attacks by monitoring, filtering, and blocking HTTP traffic. A WAF can prevent attacks such as cross-site scripting, SQL injection, or file inclusion, among others. A WAF does not provide administrative access to internal resources, but rather protects them from web application vulnerabilities. A WAF is also not a comprehensive solution for network security, as it only operates at the application layer and does not protect against other types of attacks or threats5.
Utilizing single sign-on is not the correct answer, because single sign-on is a method of authentication that allows users to access multiple sites, services, or applications with one username and password. Single sign-on can simplify the sign-in process for users and reduce the number of passwords they have to remember and manage. Single sign-on does not provide administrative access to internal resources, but rather enables access to various resources that the user is authorized to use. Single sign-on can also introduce security risks if the user's credentials are compromised or if the single sign-on provider is breached6. Reference = 1: Bastion host - Wikipedia, 2: 14 Best Practices to Secure SSH Bastion Host - goteleport.com, 3: The Importance Of Bastion Hosts In Network Security, 4: What is the network perimeter? | Cloudflare, 5: What is a WAF? | Web Application Firewall explained, 6: [What is single sign-on (SSO)? - Definition from WhatIs.com]

NEW QUESTION # 664
.....

the whole, the pass rate of our customers after using SY0-701 test dumps in the course of the preparation for the CompTIA exams can reach as high as 98% to 99%, which is far ahead of others in the same field, We can help you get the CompTIA SY0-701 valid test materials quickly in a safer environment.

Because software projects almost never do better SY0-701 Test Certification Cost than planned, However, this program still has enough stability issues that if you want it to run continuously, you either need SY0-701 someone physically present or a remote control setup to enable you to re)start it.

CompTIA SY0-701 preparation & SY0-701 prep4sure torrent

Our system will send you the latest version automatically, and you just need to examine your email for the latest version, With the help of SY0-701 Study Guide, you can easily pass the exam and reach the pinnacle of life.

On the whole, the pass rate of our customers after using SY0-701 test dumps in the course of the preparation for the CompTIA exams can reach as high as 98% to 99%, which is far ahead of others in the same field.

We can help you get the CompTIA SY0-701 valid test materials quickly in a safer environment, You will enjoy learning on our SY0-701 exam questions for its wonderful and latest design with the latest technologies applied.