Implementing and Operating Cisco Security Core Technologies prep torrent & 350-701 study questions & Implementing and Operating Cisco Security Core Technologies dumps pdf

P.S. Free 2026 Cisco 350-701 dumps are available on Google Drive shared by DumpTorrent: https://drive.google.com/open?id=1zSSjyq27CGzf5glSlq06DUYjY15He93o

Successful companies are those which identify customers' requirements and provide the solution to 350-701 exam candidate needs and to make those dreams come true, we are in continuous touch with the exam candidates to get more useful ways. We have favorable quality reputation in the mind of exam candidates these years by trying to provide high quality 350-701 Study Guide with the lowest prices while the highest quality. So you can't miss our 350-701 learning prep.

Cisco 350-701 exam is an excellent way for IT professionals to validate their skills in implementing and operating Cisco Security Core Technologies. Implementing and Operating Cisco Security Core Technologies certification provides recognition of the candidate's expertise and can help them advance their career in the IT industry. Moreover, the certification can also help organizations identify skilled professionals who can help them implement and operate Cisco Security technologies.

CCIE Security

The CCIE Security certificate recognizes the expert-level mastery of Cisco security solutions and technologies. Particularly, this certification is meant for seasoned security professionals tasked with architecting, engineering, implementing, troubleshooting, and supporting vital security concepts to prevent security threats, risks, and vulnerabilities. It is the immediate step after passing the CCNP Security exam, which will require sitting for two tests, 350-701 & the lab validation known as the CCIE Security v6.0.

Cisco 350-701 certification exam is an excellent opportunity for IT professionals to advance their careers in cybersecurity. 350-701 exam covers the latest technologies and best practices for securing networks, devices, applications, and endpoints. IT professionals who hold this certification are highly respected in the industry and are in high demand by organizations looking to secure their networks and data.

>> 350-701 Practice Tests <<

Certification 350-701 Questions, Reliable 350-701 Dumps Sheet

All in all, our test-orientated high-quality 350-701 exam questions would be the best choice for you, we sincerely hope all of our candidates can pass 350-701 exam, and enjoy the tremendous benefits of our 350-701 prep guide. Helping candidates to pass the 350-701 Exam has always been a virtue in our company's culture, and you can connect with us through email at the process of purchasing and using, we would reply you as fast as we can.

Cisco Implementing and Operating Cisco Security Core Technologies Sample Questions (Q563-Q568):

NEW QUESTION # 563
A Cisco ESA network administrator has been tasked to use a newly installed service to help create policy based on the reputation verdict. During testing, it is discovered that the Cisco ESA is not dropping files that have an undetermined verdict. What is causing this issue?

- A. The policy was created to send a message to quarantine instead of drop
- B. The policy was created to disable file analysis
  Maybe the "newly installed service" in this question mentions about Advanced Malware Protection (AMP) which can be used along with ESA. AMP allows superior protection across the attack continuum.
  + File Reputation - captures a fingerprint of each file as it traverses the ESA and sends it to AMP's cloudbased intelligence network for a reputation verdict. Given these results, you can automatically block malicious files and apply administrator-defined policy.
  + File Analysis - provides the ability to analyze unknown files that are traversing the ESA. A highly secure sandbox environment enables AMP to glean precise details about the file's behavior and to combine that data with detailed human and machine analysis to determine the file's threat level. This disposition is then fed into AMP cloud-based intelligence network and used to dynamically update and expand the AMP cloud data set for enhanced protection
- C. The file has a reputation score that is below the threshold
- D. The file has a reputation score that is above the threshold

Answer: B

NEW QUESTION # 564
Which suspicious pattern enables the Cisco Tetration platform to learn the normal behavior of users?

- A. privilege escalation
- B. user login suspicious behavior
- C. interesting file access
- D. file access from a different user

Answer: B

Explanation:
The various suspicious patterns for which the Cisco Tetration platform looks in the current release are:
+ Shell code execution: Looks for the patterns used by shell code.
+ Privilege escalation: Watches for privilege changes from a lower privilege to a higher privilege in the process lineage tree.
+ Side channel attacks: Cisco Tetration platform watches for cache-timing attacks and page table fault bursts.
Using these, it can detect Meltdown, Spectre, and other cache-timing attacks.
+ Raw socket creation: Creation of a raw socket by a nonstandard process (for example, ping).
+ User login suspicious behavior: Cisco Tetration platform watches user login failures and user login methods.
+ Interesting file access: Cisco Tetration platform can be armed to look at sensitive files.
+ File access from a different user: Cisco Tetration platform learns the normal behavior of which file is accessed by which user.
+ Unseen command: Cisco Tetration platform learns the behavior and set of commands as well as the lineage of each command over time. Any new command or command with a different lineage triggers the interest of the Tetration Analytics platform.

NEW QUESTION # 565
Which type of attack is MFA an effective deterrent for?

- A. ping of death
- B. syn flood
- C. teardrop
- D. phishing

Answer: D

NEW QUESTION # 566
What are two functions of secret key cryptography? (Choose two)

- A. utilization of different keys for encryption and decryption
- B. provides the capability to only know the key on one side
- C. utilization of less memory
- D. key selection without integer factorization
- E. utilization of large prime number iterations

Answer: C,D

Explanation:
Secret key cryptography, also known as symmetric key cryptography, is a type of encryption where a single secret key is used for both encryption and decryption of a message. The cryptographic key is kept secret between the sender and receiver, making it difficult for anyone else to decipher the message. Some of the functions of secret key cryptography are:
* Key selection without integer factorization: Secret key cryptography does not rely on complex mathematical problems such as integer factorization or discrete logarithms to generate keys. Instead, the keys are chosen randomly or derived from a passphrase or a shared secret. This makes the key generation process faster and simpler than in public key cryptography.
* Utilization of less memory: Secret key cryptography uses less memory than public key cryptography, as it only requires one key to be stored and managed. Public key cryptography, on the other hand, requires two keys (public and private) for each user, which increases the memory overhead and complexity of key management.
The other options are not functions of secret key cryptography, but rather characteristics of public key cryptography or asymmetric cryptography, which is a different type of encryption where different keys are used for encryption and decryption. Public key cryptography has the following features:
* Utilization of different keys for encryption and decryption: Public key cryptography uses a pair of keys, one public and one private, for each user. The public key can be shared with anyone, while the private key must be kept secret. The public key is used to encrypt messages, while the private key is used to decrypt them. This allows users to communicate securely without having to exchange a secret key beforehand.
* Utilization of large prime number iterations: Public key cryptography relies on hard mathematical problems such as integer factorization or discrete logarithms to generate keys. These problems involve finding the prime factors of large numbers or finding the discrete logarithms of numbers in a finite field.
These problems are easy to solve in one direction, but hard to solve in the reverse direction. For
* example, it is easy to multiply two large prime numbers, but hard to find the prime factors of the product. This makes the keys hard to break by brute force or other methods.
* Provides the capability to only know the key on one side: Public key cryptography enables users to encrypt messages without knowing the recipient's key, and vice versa. This is possible because the encryption and decryption keys are different and mathematically related. For example, Alice can encrypt a message with Bob's public key, and only Bob can decrypt it with his private key. Alice does not need to know Bob's private key, and Bob does not need to know Alice's key. This also enables public key cryptography to support digital signatures, which are a way of verifying the identity and integrity of a message.
References :=
* What Is Secret Key Cryptography? A Complete Guide - Helenix
* Definition of Secret-key Cryptography - Gartner

NEW QUESTION # 567
Which two conditions are prerequisites for stateful failover for IPsec? (Choose two)

- A. Only the IPsec configuration that is set up on the active device must be duplicated on the standby device; the IKE configuration is copied automatically.
- B. The active and standby devices must run the same version of the Cisco IOS software and must be the same type of device
- C. Only the IKE configuration that is set up on the active device must be duplicated on the standby device; the IPsec configuration is copied automatically
- D. The active and standby devices can run different versions of the Cisco IOS software but must be the same type of device.
- E. The IPsec configuration that is set up on the active device must be duplicated on the standby device

Answer: B,E

Explanation:
Stateful failover for IP Security (IPsec) enables a router to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This failover process is transparent to users and does not

require adjustment or reconfiguration of any remote peer.
Stateful failover for IPsec requires that your network contains two identical routers that are available to be either the primary or secondary device. Both routers should be the same type of device, have the same CPU and memory, and have either no encryption accelerator or identical encryption accelerators.
Prerequisites for Stateful Failover for IPsec
Complete, Duplicate IPsec and IKE Configuration on the Active and Standby Devices This document assumes that you have a complete IKE and IPsec configuration.
The IKE and IPsec configuration that is set up on the active device must be duplicated on the standby device.
That is, the crypto configuration must be identical with respect to Internet Security Association and Key Management Protocol (ISAKMP) policy, ISAKMP keys (preshared), IPsec profiles, IPsec transform sets, all crypto map sets that are used for stateful failover, all access control lists (ACLs) that are used in match address statements on crypto map sets, all AAA configurations used for crypto, client configuration groups, IP local pools used for crypto, and ISAKMP profiles.
Reference:
Although the prerequisites only stated that "Both routers should be the same type of device" but in the
"Restrictions for Stateful Failover for IPsec" section of the link above, it requires "Both the active and standby devices must run the identical version of the Cisco IOS software" so answer E is better than answer B.

NEW QUESTION # 568
......

id=1zSSjyq27CGzf5glSlq06DUYjY15He93o