Exam 350-701 Tips - 350-701 Test Pass4sure

What's more, part of that TrainingDump 350-701 dumps now are free: https://drive.google.com/open?id=1OpqHOYeentMj5cV_0w-NByfMgd0eF5zY

With our customer-oriented 350-701 actual question, you can be one of the former exam candidates with passing rate up to 98 to 100 percent. You will pay just a small amount of money on our 350-701 exam guide but harvest colossal success with potential bright future. And we have confidence that your future aims will come along with this successful exam as the beginning. So choosing 350-701 actual question is choosing success.

To prepare for the Cisco 350-701 exam, candidates can attend Cisco training courses, read Cisco documentation, and practice with Cisco labs. Cisco also provides study materials, such as exam dumps, practice tests, and study guides, to help candidates prepare for the exam. It is recommended that candidates have at least 3-5 years of experience in the IT industry before attempting the exam.

Cisco 350-701 exam covers a wide range of security topics, including network security, cloud security, endpoint protection, secure access, visibility, and enforcement. Candidates are tested on their understanding of security concepts, as well as their ability to implement and operate security solutions using Cisco technologies. 350-701 Exam is intended to validate the expertise of security professionals and help organizations identify individuals who possess the necessary skills to secure their networks.

>> Exam 350-701 Tips <<

Get Fantastic Exam 350-701 Tips and Pass Exam in First Attempt

The passing rate of our 350-701 study material is very high, and it is about 99%. We provide free download and tryout of the 350-701 question torrent, and we will update the 350-701 exam torrent frequently to guarantee that you can get enough test bank and follow the trend in the theory and the practice. We provide 3 versions for you to choose thus you can choose the most convenient method to learn. Our 350-701 Latest Questions are compiled by the experienced professionals elaborately. So it will be very convenient for you to buy our product and it will do a lot of good to you.

Cisco Implementing and Operating Cisco Security Core Technologies Sample Questions (Q699-Q704):

NEW QUESTION # 699
What is the difference between a vulnerability and an exploit?

- A. An exploit is a hypothetical event that causes a vulnerability in the network
- B. A vulnerability is a hypothetical event for an attacker to exploit
- C. A vulnerability is a weakness that can be exploited by an attacker
- D. An exploit is a weakness that can cause a vulnerability in the network

Answer: C

Explanation:
vulnerability is a flaw or gap in the security of a system or network that can be exploited by an attacker to compromise its

functionality, integrity, confidentiality, or availability. A vulnerability can exist in the design, implementation, configuration, or operation of a system or network, and can be caused by human errors, software bugs, hardware defects, or environmental factors. A vulnerability can be exploited by an attacker using various methods, such as malware, phishing, brute force, denial-of-service, or injection attacks. A vulnerability can also be exploited by an insider who has legitimate access to the system or network, but abuses their privileges for malicious purposes. A vulnerability can be discovered by security researchers, ethical hackers, or malicious hackers, and can be reported to the vendor or the public for remediation or exploitation. A vulnerability can be mitigated by applying patches, updates, or configuration changes, or by using security tools such as firewalls, antivirus, or encryption.
An exploit is a piece of code, data, or technique that takes advantage of a vulnerability to perform unauthorized or malicious actions on a system or network. An exploit can be used to gain access, escalate privileges, execute commands, steal data, disrupt services, or damage resources. An exploit can be delivered by various means, such as email attachments, web links, removable media, or network packets. An exploit can be developed by security researchers, ethical hackers, or malicious hackers, and can be shared or sold on the dark web or other platforms for testing or attacking purposes. An exploit can be detected by security tools such as intrusion detection systems, antivirus, or anti-exploit software.
The difference between a vulnerability and an exploit is that a vulnerability is a potential weakness that can be exploited, while an exploit is an actual attack that uses a vulnerability. A vulnerability can exist without being exploited, but an exploit cannot exist without a vulnerability. A vulnerability can be fixed or prevented, but an exploit can only be blocked or stopped. References :=
* Exploit vs Vulnerability: What's the Difference? - InfoSec Insights
* Difference Between Vulnerability and Exploit - GeeksforGeeks
* Exploit vs. Vulnerability: What Is the Difference? - Coralogix
* Exploit vs Vulnerability: What's the Difference? - Cybers Guards

NEW QUESTION # 700
Refer to the exhibit.

```
ntp authentication-key 10 md5 cisco123
ntp trusted-key 10
```

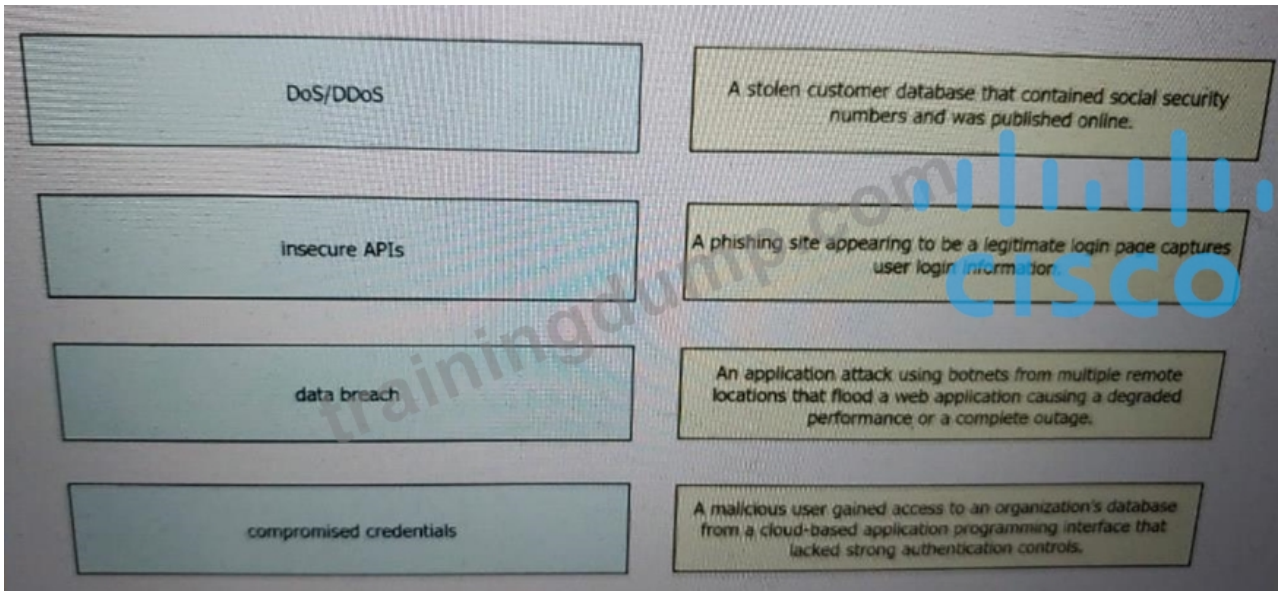
A network engineer is testing NTP authentication and realizes that any device synchronizes time with this router and that NTP authentication is not enforced What is the cause of this issue?

- A. NTP authentication is not enabled.
- B. The router was not rebooted after the NTP configuration updated.
- C. The key was configured in plain text.
- D. The hashing algorithm that was used was MD5. which is unsupported.

Answer: A

Explanation:
The cause of this issue is that NTP authentication is not enabled on the router. The commands shown in the exhibit only define the authentication key and mark it as trusted, but they do not enable NTP authentication globally or on a per-peer basis. To enable NTP authentication globally, the command ntp authenticate must be used. To enable NTP authentication on a per-peer basis, the command ntp server ip-address key key-id or ntp peer ip-address key key-id must be used, where key-id is the same as the one defined by the ntp authentication-key command. Without enabling NTP authentication, any device can synchronize time with this router, regardless of whether it has the same authentication key or not.
The other options are incorrect because:
* The key was configured in plain text, but this is not the cause of the issue. Although it is recommended to use the ntp authentication-key key-id md5 key [encrypted] command to encrypt the key, using plain text does not prevent NTP authentication from working, as long as the same key is configured on both the router and the peer.
* The hashing algorithm that was used was MD5, which is supported by NTP. MD5 is the default algorithm for NTP authentication and it can be used with any key length from 1 to 16 characters. Other algorithms, such as SHA and SHA1, are also supported by NTP if the OpenSSL library is installed, but they are not required for NTP authentication to work.
* The router was not rebooted after the NTP configuration updated, but this is not necessary for NTP authentication to take effect. NTP authentication is applied immediately after the configuration commands are entered, and no reboot is required.
References:
Configuring NTP
Authentication Support
NTP Authentication Explained

NEW QUESTION # 701
Drag and drop the threats from the left onto examples of that threat on the right



Answer:

Explanation:

NEW QUESTION # 702
Which two endpoint measures are used to minimize the chances of falling victim to phishing and social engineering attacks? (Choose two.)

- A. Protect systems with an up-to-date antimalware program.
- B. Perform backups to the private cloud.
- C. Install a spam and virus email filter.
- D. Patch for cross-site scripting.
- E. Protect against input validation and character escapes in the endpoint.

Answer: A,E

NEW QUESTION # 703
Which feature is configured for managed devices in the device platform settings of the Firepower Management Center?

- A. network address translations
- B. quality of service

- C. intrusion policy
- D. time synchronization

Answer: D

Explanation:
Time synchronization is one of the features that can be configured for managed devices in the device platform settings of the Firepower Management Center (FMC). Time synchronization ensures that the FMC and its managed devices have the same date and time settings, which is important for accurate event logging and reporting. The FMC can act as a Network Time Protocol (NTP) server for its managed devices, or it can use an external NTP server as a time source1. The FMC can also synchronize its time with the system clock of the device where it is installed2. References := 1: Firepower Management Center Device Configuration Guide, 7.1
- Platform Settings 2: Firepower Management Center Configuration Guide, Version 6.6 - Device Management Basics

NEW QUESTION # 704
.....

If you buy our 350-701 training quiz, you will find three different versions are available on our test platform. According to your need, you can choose the suitable version for you. The three different versions of our 350-701 study materials include the PDF version, the software version and the online version. We can promise that the three different versions are equipment with the high quality. If you purchase our 350-701 Preparation questions, it will be very easy for you to easily and efficiently find the exam focus and pass the 350-701 exam.