Free Download 350-701 Brain Dump Free–The Best Valid Exam Dumps for your Cisco 350-701

P.S. Free & New 350-701 dumps are available on Google Drive shared by Itcertmaster: https://drive.google.com/open?id=1GQ8aQaPUxqKIEY3Ym4skGUeIFGP-F-lU

I am glad to introduce a secret weapon for all of the candidates to pass the exam as well as get the related certification without any more ado-- our 350-701 study materials. You can only get the most useful and efficient study materials with the most affordable price. With our 350-701 practice test, you only need to spend 20 to 30 hours in preparation since there are all essence contents in our 350-701 Study Materials. What's more, if you need any after service help on our 350-701 exam guide, our after service staffs will always offer the most thoughtful service for you.

Cisco 350-701 (Implementing and Operating Cisco Security Core Technologies) Certification Exam is a popular certification program designed for individuals who want to build a career in cybersecurity. Implementing and Operating Cisco Security Core Technologies certification exam is ideal for security professionals who are involved in the implementation and operation of core security technologies. 350-701 exam tests candidates on their knowledge of security technologies, including network security, cloud security, content security, endpoint protection, secure network access, visibility, and enforcement. Implementing and Operating Cisco Security Core Technologies certification program is recognized globally and is widely accepted by employers as a measure of a candidate's knowledge and skills in security technologies.

Upon passing the Cisco 350-701 Certification Exam, candidates earn the Cisco Certified Specialist - Security Core certification. Implementing and Operating Cisco Security Core Technologies certification demonstrates to employers that the candidate has a solid understanding of network security concepts and skills in implementing and operating Cisco Security Core Technologies.

>> 350-701 Brain Dump Free <<

Free PDF Quiz 2026 Cisco 350-701: Implementing and Operating Cisco Security Core Technologies Updated Brain Dump Free

To some extent, to pass the 350-701 exam means that you can get a good job. The 350-701 exam materials you master will be applied to your job. The possibility to enter in big and famous companies is also raised because they need outstanding talents to serve for them. Our 350-701 Test Prep is compiled elaborately and will help the client get the 350-701 certification. To get a better

and full understanding of our 350-701 quiz torrent, you can just free download the demo of our 350-701 exam questions.

Cisco 350-701 Certification Exam is a highly sought-after certification for IT professionals in the field of cybersecurity. 350-701 exam is designed to test the skills and knowledge of candidates in implementing and operating Cisco Security Core Technologies. Implementing and Operating Cisco Security Core Technologies certification exam is a comprehensive test that covers all the essential topics required to be proficient in cybersecurity and network security.

Cisco Implementing and Operating Cisco Security Core Technologies Sample Questions (Q696-Q701):

NEW QUESTION # 696
What two mechanisms are used to redirect users to a web portal to authenticate to ISE for guest services?(Choose two)

- A. central web auth
- B. multiple factor auth
- C. local web auth
- D. TACACS+
- E. single sign-on

Answer: A,C

Explanation:
Local web authentication (LWA) and central web authentication (CWA) are two mechanisms that are used to redirect users to a web portal to authenticate to ISE for guest services.
Both methods involve the use of a redirect access control list (ACL) that allows the user to access only the web portal URL and blocks all other traffic until the user is authenticated.
The difference between LWA and CWA is where the web portal and the authentication logic are hosted.
* LWA: The web portal and the authentication logic are hosted on the wireless LAN controller (WLC).
The WLC sends a RADIUS access-accept message to the network access device (NAD) along with the redirect ACL and the web portal URL.
The NAD then redirects the user to the web portal on the WLC, where the user enters their credentials. The WLC verifies the credentials with the ISE and grants or denies access to the user.
The advantage of LWA is that it does not require any configuration on the ISE, but the disadvantage is that it does not support advanced features such as posture assessment, profiling, or authorization policies.
* CWA: The web portal and the authentication logic are hosted on the ISE.
The WLC sends a RADIUS access-challenge message to the NAD along with the redirect ACL and the web portal URL. The NAD then redirects the user to the web portal on the ISE, where the user enters their credentials. The ISE verifies the credentials and sends a RADIUS access-accept message to the WLC with the authorization profile and the final ACL. The WLC then applies the authorization profile and the final ACL to the user session. The advantage of CWA is that it supports advanced features such as posture assessment, profiling, or authorization policies, but the disadvantage is that it requires more configuration on the ISE.
References:
* Configure Guest Access
* Web Authentication Redirection to Original URL
* Configure Local Web Authentication with External Authentication

NEW QUESTION # 697
Which two application layer preprocessors are used by Firepower Next Generation Intrusion Prevention System? (Choose two)

- A. inline normalization
- B. modbus
- C. SIP
- D. packet decoder
- E. SSL

Answer: C,E

Explanation:
Explanation Application layer protocols can represent the same data in a variety of ways. The Firepower System provides application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules

to packets whose data is represented differently and obtain meaningful results. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Application_Layer_Preprocessors.html#ID-2244-0000080c FirePower uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.
Application layer protocols can represent the same data in a variety of ways. The Firepower System provides application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results.
Reference:
Explanation Application layer protocols can represent the same data in a variety of ways. The Firepower System provides application layer protocol decoders that normalize specific types of packet data into formats that the intrusion rules engine can analyze. Normalizing application-layer protocol encodings allows the rules engine to effectively apply the same content-related rules to packets whose data is represented differently and obtain meaningful results. Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guidev60/Application_Layer_Preprocessors.html#ID-2244-0000080c FirePower uses many preprocessors, including DNS, FTP/Telnet, SIP, SSL, SMTP, SSH preprocessors.

NEW QUESTION # 698
Which protocol provides the strongest throughput performance when using Cisco AnyConnect VPN?

- A. DTLSv1
- B. TLSv1
- C. TLSv1.2
- D. TLSv1.1

Answer: A

Explanation:
Explanation/Reference: https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/215331-anyconnect-implementation-and-performanc.html

NEW QUESTION # 699
What are two Trojan malware attacks? (Choose two)

- A. Smurf
- B. Rootkit
- C. Backdoor
- D. Sync
- E. Frontdoor

Answer: B,C

Explanation:
A Trojan malware attack is a type of malicious code or software that disguises itself as a legitimate program or file to trick users into executing it. Once executed, the Trojan can perform various harmful actions on the infected system or network, such as stealing data, deleting files, or installing other malware. There are different types of Trojan malware attacks, depending on their purpose and behavior. Two common types are:
* Rootkit: A rootkit is a type of Trojan that hides itself and other malware from detection and removal by antivirus software or system tools. A rootkit can modify the operating system or the firmware of the device to gain persistent and privileged access to the system. A rootkit can also intercept and manipulate system calls, network traffic, or user input to conceal its activities or redirect them to malicious servers.
* Backdoor: A backdoor is a type of Trojan that creates a secret or unauthorized access point to the infected system or network. A backdoor can allow an attacker to remotely control the system, execute commands, upload or download files, or monitor the system activity. A backdoor can also be used to install other malware or launch further attacks on other systems or networks.
References:
[Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0], Module 1: Malware Threats, Lesson 1: Identifying Malware Threats, Topic: Trojan Horse What is a Trojan? Is it a virus or is it malware? - Norton™ Trojan Horse Examples (2024): The 6 Worst Attacks Ever - SoftwareLab

NEW QUESTION # 700
When network telemetry is implemented, what is important to be enabled across all network infrastructure devices to correlate different sources?

- A. NTP
- B. syslog
- C. DNS
- D. CDP

Answer: A

Explanation:
Network telemetry is the collection, measurement, and analysis of data related to the behavior and performance of a network1. It involves gathering information about routers, switches, servers, and applications to gain insights into how they function and how data moves through them. To correlate different sources of network telemetry data, it is important to enable Network Time Protocol (NTP) across all network infrastructure devices. NTP is a protocol that synchronizes the clocks of network devices to a common reference time source2. This ensures that the network telemetry data has consistent timestamps and can be compared and correlated accurately. NTP also helps with troubleshooting network issues, as it allows network administrators to pinpoint the exact time of events and anomalies. NTP is a core security technology that is covered in the Implementing and Operating Cisco Security Core Technologies (SCOR) course3, which helps you prepare for the Cisco CCNP Security and CCIE Security certifications and for senior-level security roles. References: 1: Network Telemetry Explained: Frameworks, Applications & Standards - Splunk 2: [Network Time Protocol (NTP) - Cisco] 3: Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

NEW QUESTION # 701
......

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myspace.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes

P.S. Free 2026 Cisco 350-701 dumps are available on Google Drive shared by Itcertmaster: https://drive.google.com/open?id=1GQ8aQaPUxqKIEY3Ym4skGUeIFGP-F-lU