350-201 Advanced Testing Engine & New 350-201 Test Notes

P.S. Free & New 350-201 dumps are available on Google Drive shared by Free4Dump: https://drive.google.com/open?id=1Y-saM7R6PmooPKzAXYkP3-Z7TwRDJ0PA

The key trait of our product is that we keep pace with the changes of syllabus and the latest circumstance to revise and update our 350-201 study materials, and we are available for one-year free updating to assure you of the reliability of our service. Our company has established a long-term partnership with those who have purchased our 350-201 Exam guides. We have made all efforts to update our product in order to help you deal with any change, making you confidently take part in the exam.

Cisco 350-201 Exam is a two-hour test that consists of 60-70 multiple-choice questions. To pass the exam, candidates must receive a score of at least 70%. 350-201 exam can be taken online or at a testing center, and it costs $400. Candidates must have a solid understanding of cybersecurity concepts and Cisco security technologies to pass the exam.

>> 350-201 Advanced Testing Engine <<

New 350-201 Test Notes - 350-201 Certification Practice

With the rapid development of IT technology, the questions in the IT certification exam are also changing. Therefore, Free4Dump also keeps updating test questions and answers. And if you purchase Free4Dump Cisco 350-201 Practice Test materials, we will provide you with free updates for a year. As long as the questions updates, Free4Dump will immediately send the latest questions and answers to you which guarantees that you can get the latest materials at any time. Free4Dump can not only help you pass the test, but also help you learn the latest knowledge. Never pass up a good chance to have the substantial materials.

Cisco 350-201 Exam consists of 90-110 multiple-choice and performance-based questions and must be completed within 120 minutes. 350-201 exam is available in English and Japanese and can be taken at Pearson VUE testing centers worldwide or online through the Pearson VUE online proctoring platform. 350-201 exam fee is $400, and candidates must achieve a passing score of 825 out of 1000 to earn the certification. Performing CyberOps Using Cisco Security Technologies certification is valid for three years, after which candidates must recertify by passing the current exam or another qualifying exam.

Cisco Performing CyberOps Using Cisco Security Technologies Sample Questions (Q17-Q22):

NEW QUESTION # 17
A logistic company must use an outdated application located in a private VLAN during the migration to new technologies. The IPS blocked and reported an unencrypted communication. Which tuning option should be applied to IPS?

- A. Allow list traffic to application's IP from the internal network at a specific port.
- B. Allow list only authorized hosts to contact the application's IP at a specific port.
- C. Allow list only authorized hosts to contact the application's VLAN.

- D. Allow list HTTP traffic through the corporate VLANS.

Answer: C

NEW QUESTION # 18
How does Wireshark decrypt TLS network traffic?

- A. by observing DH key exchange
- B. using an RSA public key
- C. with a key log file using per-session secrets
- D. by defining a user-specified decode-as

Answer: C

Explanation:
Wireshark decrypts TLS network traffic by using a key log file that contains per-session secrets1. This method is effective even when Diffie-Hellman (DH) key exchange is used, which is common in modern encrypted communications. The key log file is typically generated by applications like web browserswhen the SSLKEYLOGFILE environment variable is set. This file records the necessary per-session secrets that Wireshark can then use to decrypt the traffic1.
It's important to note that while this method is universal and works across different TLS versions, including TLS 1.3, other methods such as using an RSA private key are limited to certain conditions and do not work with TLS 1.3 or when (EC)DHE cipher suites are selected1. Therefore, the key log file method is the most reliable and widely applicable approach for decrypting TLS in Wireshark.

NEW QUESTION # 19
How is a SIEM tool used?

- A. To collect security data from authentication failures and cyber attacks and forward it for analysis
- B. To compare security alerts against configured scenarios and trigger system responses
- C. To collect and analyze security data from network devices and servers and produce alerts
- D. To search and compare security data against acceptance standards and generate reports for analysis

Answer: C

Explanation:
A Security Information and Event Management (SIEM) tool is primarily used to collect and analyze security data from various sources, such as network devices and servers, and then produce alerts based on this analysis.
SIEM tools aggregate and correlate data to identify patterns that may indicate a security incident, allowing organizations to respond to threats more effectively.

NEW QUESTION # 20
Refer to the exhibit.
Which code snippet will parse the response to identify the status of the domain as malicious, clean or undefined?

- A. Option A
- B. Option C
- C. Option B
- D. Option D

Answer: C

Explanation:
The correct code snippet that will parse the response to identify the status of the domain as malicious, clean, or undefined is Option B. This option containsconditional checks for the domain status and prints out the result accordingly. If the domain_status is 'malicious', it prints that the domain is found malicious; if the domain_status is 'clean', it prints that the domain is found clean; and for any other case, it prints that the domain status is undefined or risky. This aligns with the typical structure of a response parser that handles different statuses and provides a corresponding output.

References :=
* Python's conditional statements documentation for handling multiple conditions.
* Best practices for parsing JSON responses in Python, which often involve checking for various statuses and handling each one appropriately.

NEW QUESTION # 21
A threat actor used a phishing email to deliver a file with an embedded macro. The file was opened, and a remote code execution attack occurred in a company's infrastructure. Which steps should an engineer take at the recovery stage?

- A. Determine the systems involved and deploy available patches
- B. Identify the attack vector and update the IDS signature list
- C. Review access lists and require users to increase password complexity
- D. Analyze event logs and restrict network access

Answer: A

Explanation:
After a remote code execution attack, it is crucial to determine which systems were involved in the incident and to deploy any available patches to those systems. This step is part of the recovery stage, where the focus is on restoring the integrity of the systems and preventing the same vulnerability from being exploited again. Patching the systems helps to close the security gaps that the threat actor exploited and is a key measure in the process of recovering from such an attack

NEW QUESTION # 22
.....

What's more, part of that Free4Dump 350-201 dumps now are free: https://drive.google.com/open?id=1Y-saM7R6PmooPKzAXYkP3-Z7TwRDJ0PA