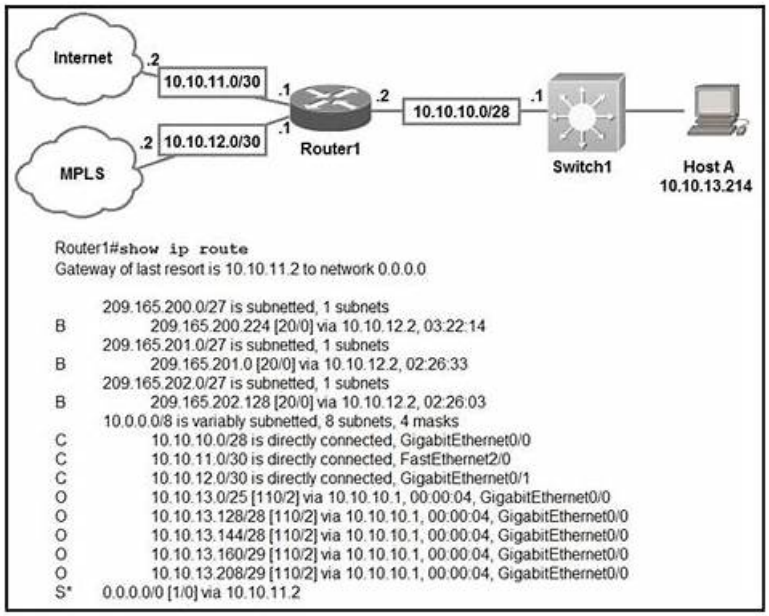
Latest Cisco 300-215 Test Question, 300-215 Dump Torrent



P.S. Free & New 300-215 dumps are available on Google Drive shared by Exam4PDF: https://drive.google.com/open?id=1k5V677Kq_7faOD5T6JZ3znoBrKoYrmq2

We don't just want to make profitable deals, but also to help our users pass the 300-215 exams with the least amount of time to get a certificate. Choosing our 300-215 exam practice, you only need to spend 20-30 hours to prepare for the exam. Maybe you will ask whether such a short time can finish all the content, we want to tell you that you can rest assured ,because our 300-215 Learning Materials are closely related to the exam outline.

Cisco 300-215 exam covers a wide range of topics related to cyber forensics and incident response, including threat analysis, network security, malware analysis, and incident response planning. 300-215 exam consists of multiple-choice questions, simulations, and hands-on labs that test the candidate's ability to analyze and respond to security incidents. 300-215 Exam is designed to test the candidate's knowledge of the latest Cisco technologies and best practices for conducting forensic analysis and incident response.

>> Latest Cisco 300-215 Test Question <<

100% Pass Quiz 2025 Cisco 300-215 – High Pass-Rate Latest Test Question

Checking our 300-215 free demo is a great way of learning the pattern of exam materials and if it suits what you wanted. There are valid 300-215 test questions and accurate answers along with the professional explanations in our study guide. All real questions just need to practice one or two days and remember the answers will save you much time in 300-215 Real Exam. Come and join us.

Cisco Conducting Forensic Analysis & Incident Response Using Cisco Technologies for CyberOps Sample Questions (Q75-Q80):

NEW QUESTION # 75
A threat actor has successfully attacked an organization and gained access to confidential files on a laptop.
What plan should the organization initiate to contain the attack and prevent it from spreading to other network devices?

- A. attack surface
- B. incident response
- C. root cause
- D. intrusion prevention

Answer: B

Explanation:
Once an incident has occurred, the appropriate course of action is to engage the organization's Incident Response (IR) plan. This is a structured approach to contain, analyze, and eradicate threats before they spread across the network.
The Cisco CyberOps Associate study guide emphasizes:
* "Incident response and handling are essential within an organization... The main objective of implementing an incident handling process is to reduce the impact of a cyber-attack, ensure the damages caused are assessed, and implement recovery procedures".
* In particular, the containment phase of IR is focused on isolating the threat and preventing lateral movement or further compromise.
Options such as "root cause" or "attack surface" are relevant at later stages of analysis and mitigation, not immediate containment.
Therefore, the correct answer is C.

NEW QUESTION # 76

Refer to the exhibit. An engineer is analyzing a TCP stream in a Wireshark after a suspicious email with a URL. What should be determined about the SMB traffic from this stream?

- A. It is exploiting redirect vulnerability
- B. It is redirecting to a malicious phishing website,
- C. It is requesting authentication on the user site.
- D. It is sharing access to files and printers.

Answer: A

NEW QUESTION # 77
Refer to the exhibit.

A cybersecurity analyst is presented with the snippet of code used by the threat actor and left behind during the latest incident and is asked to determine its type based on its structure and functionality. What is the type of code being examined?

- A. basic web crawler for indexing website content
- B. network monitoring script for capturing incoming traffic
- C. simple client-side script for downloading other elements
- D. socket programming listener for TCP/IP communication

Answer: D

Explanation:
The Python code snippet:
* Usessocket.socket(AF_INET, SOCK_STREAM), which indicatesTCP communication
* Connects to a remote server (192.168.1.10on port 80)
* Sends a manual HTTPGETrequest
* Receives the response usings.recv()
This is a classic example ofTCP/IP socket programming, specifically creating asimple TCP clientto communicate with a web server.
It does not monitor traffic or crawl websites - it sends a crafted request and prints the response.
Thus, this code best fits:
D). socket programming listener for TCP/IP communication.

NEW QUESTION # 78
Over the last year, an organization's HR department has accessed data from its legal department on the last day of each month to create a monthly activity report. An engineer is analyzing suspicious activity alerted by a threat intelligence platform that an authorized user in the HR department has accessed legal data daily for the last week. The engineer pulled the network data from the legal department's shared folders and discovered above average-size data dumps. Which threat actor is implied from these artifacts?

- A. internal user errors
- B. privilege escalation
- C. malicious insider
- D. external exfiltration

Answer: C

Explanation:
A "malicious insider" is someone within the organization who has authorized access but intentionally misuses that access to extract or exfiltrate data. In this case:
* The HR user has legitimate access but deviates from their normal behavior pattern (accessing legal data daily instead of monthly).
* The presence of large data dumps and the alert from a threat intelligence platform suggest intentional misuse rather than accidental behavior.
According to the Cisco CyberOps Associate guide, insider threats are identified by behavioral anomalies, especially involving sensitive data access patterns inconsistent with role-based access and historical usage profiles.

NEW QUESTION # 79
What are YARA rules based upon?

- A. IP addresses
- B. HTML code
- C. network artifacts
- D. binary patterns

Answer: D

Explanation:
YARA rulesare primarily used for malware classification and detection based onbinary pattern matchingwithin files. They describe sequences of bytes, strings, and other file characteristics found in malicious binaries.
The Cisco CyberOps Associate guide explains:"YARA rules operate by inspecting binary data using conditions and string matches to identify specific patterns that indicate known malware samples.".

NEW QUESTION # 80
.....

Through the stimulation of the 300-215 real exam the clients can have an understanding of the mastery degrees of our 300-215 exam practice question in practice. Thus our clients can understand the abstract concepts in an intuitive way. In the answers, our experts will provide the authorized verification and detailed demonstration so as to let the learners master the latest information timely and follow the trend of the times. All we do is to integrate the most advanced views into our 300-215 Test Guide.