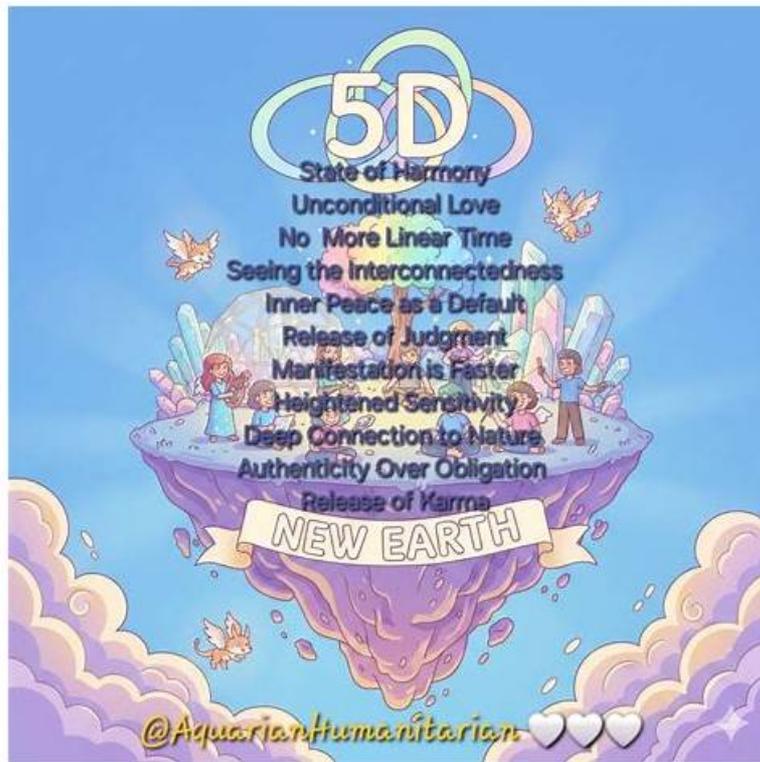# Latest 200-201 Test Testking | Dumps 200-201 Guide

BTW, DOWNLOAD part of ActualCollection 200-201 dumps from Cloud Storage: https://drive.google.com/open?id=18C8ABf-CmwTQD3-ptNU-TpWzRzkprhFQ

Our 200-201 study materials have won many people's strong support. And our 200-201 learning quiz is famous all over the world. Now, our loyal customers have gained wealth and respect with the guidance of our 200-201 learning materials. At the same time, the price is not so high. You totally can afford them. Do not make excuses for your laziness. Please take immediate actions. Our 200-201 Study Guide is extremely superior.

Cisco 200-201 exam is designed to validate the foundational knowledge and skills required for individuals who want to pursue a career in cybersecurity operations. Understanding Cisco Cybersecurity Operations Fundamentals certification exam focuses on equipping candidates with the necessary skills to identify and respond to cybersecurity incidents. 200-201 Exam covers a wide range of topics, including security concepts, network infrastructure and technologies, security monitoring and analysis, and incident response.

>> Latest 200-201 Test Testking <<

Dumps 200-201 Guide & 200-201 Test Sample Questions

ActualCollection is so popular for the reason that our 200-201 exam preparations are infallible to offer help and we will offer incessant help. On one hand, all content of our 200-201 study materials can radically give you the best backup to make progress. All related updates of the 200-201 learning guide will be sent to your mailbox. In a sense, our 200-201 training questions are classy and can broaden your preview potentially.

Cisco 200-201 Practice Test Questions, Cisco 200-201 Exam Practice Test Questions

Passing the Cisco 200-201 exam is the major requirement for obtaining the Cisco Certified CyberOps Associate certification. This test is all about the understanding of the Cisco Cybersecurity Operations fundamentals. To take it, the individuals must show that they have the skills and knowledge related to the security concepts, security policies and procedures, network intrusion analysis, hot-based analysis, and security monitoring.

Cisco Understanding Cisco Cybersecurity Operations Fundamentals Sample Questions (Q85-Q90):

NEW QUESTION # 85
An engineer receives a security alert that traffic with a known TOR exit node has occurred on the network. What is the impact of this traffic?

- A. user circumvention of the firewall
- B. data exfiltration
- C. users downloading copyrighted content
- D. ransomware communicating after infection

Answer: A

NEW QUESTION # 86
Which are two denial-of-service attacks? (Choose two.)

- A. TCP connections
- B. ping of death
- C. UDP flooding
- D. code-red
- E. man-in-the-middle

Answer: B,C

NEW QUESTION # 87
What does cyber attribution identity in an investigation?

- A. exploit of an attack
- B. vulnerabilities exploited
- C. cause of an attack
- D. threat actors of an attack

Answer: D

NEW QUESTION # 88
Refer to the exhibit.
Which stakeholders must be involved when a company workstation is compromised?

- A. Employee 1 Employee 2, Employee 3, Employee 4, Employee 5, Employee 7
- B. Employee 1, Employee 2, Employee 4, Employee 5
- C. Employee 2, Employee 3, Employee 4, Employee 5
- D. Employee 4, Employee 6, Employee 7

Answer: D

Explanation:
When a company workstation is compromised, the stakeholders that must be involved are the ones who are responsible for the security incident response process. According to the table, these are Employee 4 (Security Operation Center Analyst), Employee 6 (Head of Network and Security Infrastructure Services), and Employee 7 (Technical Director). The other employees have different roles that are not directly related to the incident response process, such as accounting, financial management, or system administration. Reference := Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0, Module 1: Security Concepts, Lesson 1.4: Security Monitoring, Topic 1.4.1: Security Operations Center

NEW QUESTION # 89

What is the difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN)?

- A. TAPS interrogation is more complex because traffic mirroring applies additional tags to data and SPAN does not alter integrity and provides full duplex network.
- B. SPAN results in more efficient traffic analysis, and TAPS is considerably slower due to latency caused by mirroring.
- C. TAPS replicates the traffic to preserve integrity, and SPAN modifies packets before sending them to other analysis tools
- D. SPAN ports filter out physical layer errors, making some types of analyses more difficult, and TAPS receives all packets, including physical errors.

Answer: D

Explanation:
The main difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN) lies in how they handle network traffic for analysis purposes. TAPS, or Test Access Points, are hardware devices that create a copy of the traffic between two network points without altering the data. This means TAPS can transmit both send and receive data streams simultaneously on separate dedicated channels, ensuring all data, including physical layer errors, is received by the monitoring or security device in real-time. On the other hand, SPAN, or Switch Port Analyzer, is a feature that duplicates network packets seen on one port to another port for analysis. However, SPAN ports can filter out physical layer errors, which may limit the types of analyses that can be performed as some errors will not be represented in the mirrored traffic.

NEW QUESTION # 90
......

Dumps 200-201 Guide: https://www.actualcollection.com/200-201-exam-questions.html