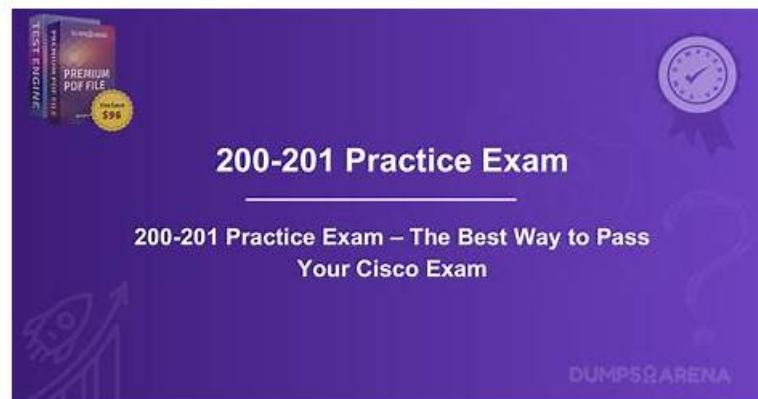


# 100% Pass 2026 Cisco Trustable 200-201 Practice Exam Questions



2026 Latest NewPassLeader 200-201 PDF Dumps and 200-201 Exam Engine Free Share: <https://drive.google.com/open?id=1n9O5dLTL7dZuzAa4XDFlg1xtgizmD9Xp>

Our 200-201 study materials are closely linked with the test and the popular trend among the industries and provide all the information about the test. The answers and questions seize the vital points and are verified by the industry experts. Diversified functions can help you get an all-around preparation for the test. Our online customer service replies the clients' questions about our 200-201 Study Materials at any time. So our 200-201 study materials can be called perfect in all aspects.

Cisco 200-201 exam consists of multiple-choice questions that cover a wide range of topics related to cybersecurity operations. 200-201 exam is designed to test the candidate's ability to apply concepts and principles to real-world scenarios. 200-201 Exam is also designed to test the candidate's ability to analyze data and make informed decisions based on that data. Candidates must pass the exam to obtain the Cisco CyberOps Associate certification.

>> 200-201 Practice Exam Questions <<

## 200-201 Exam Braindumps & 200-201 Key Concepts

If you are a child's mother, with 200-201 test answers, you will have more time to stay with your if you are a student, with 200-201 exam torrent, you will have more time to travel to comprehend the wonders of the world. In the other worlds, with 200-201 guide tests, learning will no longer be a burden in your life. You can save much time and money to do other things what meaningful. You will no longer feel tired because of your studies, if you decide to choose and practice our 200-201 Test Answers. Your life will be even more exciting.

Cisco 200-201 exam is part of the Cisco Certified CyberOps Associate certification program. This program is designed to provide candidates with the skills and knowledge needed to become effective cybersecurity analysts. The program covers a wide range of topics, including threat analysis, network security, incident response, and ethical hacking. By passing the Cisco 200-201 exam, candidates demonstrate that they have a strong foundation in these areas.

Cisco 200-201 Certification Exam is intended for individuals who are looking to start a career in cybersecurity or want to enhance their existing cybersecurity skills. 200-201 Exam is suitable for security analysts, network administrators, security operations center (SOC) personnel, and anyone who is interested in understanding the basic concepts of cybersecurity. 200-201 exam tests the candidate's ability to identify security threats, evaluate network vulnerabilities, and implement effective security solutions.

## Cisco Understanding Cisco Cybersecurity Operations Fundamentals Sample Questions (Q325-Q330):

### NEW QUESTION # 325

Refer to the exhibit.

A suspicious IP address is tagged by Threat Intelligence as a brute-force attempt source After the attacker produces many of failed login entries, it successfully compromises the account. Which stakeholder is responsible for the incident response detection step?

- A. employee 2
- **B. employee 4**
- C. employee 5
- D. employee 3

**Answer: B**

Explanation:

In the context of incident response, the detection step involves identifying potential security incidents. The Security Operation Center (SOC) Analyst, which in this case is Employee 4, is typically responsible for monitoring and analyzing security alerts to detect suspicious activities such as brute-force attempts.

Therefore, Employee 4 would be the stakeholder responsible for the incident response detection step. References: The role of a SOC Analyst in incident response is outlined in cybersecurity frameworks and best practices, which describe the responsibilities of various stakeholders in detecting and responding to security incidents.

### NEW QUESTION # 326

An engineer needs to discover alive hosts within the 192.168.1.0/24 range without triggering intrusive portscan alerts on the IDS device using Nmap. Which command will accomplish this goal?

- **A. nmap -sP 192.168.1.0/24**
- B. nmap -sL 192.168.1.0/24
- C. nmap --top-ports 192.168.1.0/24
- D. nmap -sV 192.168.1.0/24

**Answer: A**

Explanation:

<https://explainshell.com/explain?cmd=nmap+-sP>

### NEW QUESTION # 327

Refer to the exhibit.

Which technology produced the log?

- **A. IPS/IDS**
- B. firewall
- C. proxy
- D. antivirus

**Answer: A**

Explanation:

The log in the exhibit is generated by an Intrusion Prevention System (IPS) or Intrusion Detection System (IDS). It contains information about a TCP connection attempt, including the source IP address, destination IP address, and other details related to the connection. The presence of "TCP MISS" indicates that the system detected an anomaly or potential threat during the connection attempt. References: Cisco Cybersecurity Operations Fundamentals

### NEW QUESTION # 328

Refer to the exhibit.

Which application-level protocol is being targeted?

- A. TCP
- **B. HTTP**
- C. FTP
- D. HTTPS

**Answer: B**

