



# 200-201<sup>Q&As</sup>

Understanding Cisco Cybersecurity Operations Fundamentals  
(CBROPS)

**Pass Cisco 200-201 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/200-201.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Which of these is a defense-in-depth strategy principle?

- A. Identify the minimum resource required per employee.
- B. Provide the minimum permissions needed to perform job functions.
- C. Disable administrative accounts to avoid unauthorized changes.
- D. Assign the least network privileges to segment network permissions.

Correct Answer: D

---

**QUESTION 2**

An engineer is analyzing a recent breach where confidential documents were altered and stolen by the receptionist. Further analysis shows that the threat actor connected an external USB device to bypass security restrictions and steal data. The engineer could not find an external USB device. Which piece of information must an engineer use for attribution in an investigation?

- A. list of security restrictions and privileges boundaries bypassed
- B. external USB device
- C. receptionist and the actions performed
- D. stolen data and its criticality assessment

Correct Answer: C

---

**QUESTION 3**

An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the link launched, it infected machines and the intruder was able to access the corporate network.

Which testing method did the intruder use?

- A. social engineering
- B. eavesdropping
- C. piggybacking
- D. tailgating



Correct Answer: A

---

#### QUESTION 4

Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key?

- A. forgery attack
- B. plaintext-only attack
- C. ciphertext-only attack
- D. meet-in-the-middle attack

Correct Answer: C

---

#### QUESTION 5

What is a threat actor?

- A. an external party, typically a business partner with the capability to accidentally or intentionally compromise computer systems
- B. an internal individual, typically an insider with the capability to accidentally or intentionally compromise computer systems
- C. an individual or group that is external or internal and may include nation-states, hackers, organized crime, and trusted insiders
- D. an unauthorized person, such as script kiddies or hackers who attempt to breach network systems

Correct Answer: C

[Latest 200-201 Dumps](#)

[200-201 Study Guide](#)

[200-201 Braindumps](#)