



# 210-255<sup>Q&As</sup>

Cisco Cybersecurity Operations

## Pass Cisco 210-255 Exam with 100% Guarantee

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

<https://www.geekcert.com/210-255.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 the following are the three broad categories of cybersecurity investigations?

- A. Public, private, and individual investigations
- B. Judiciary, private, and individual investigations
- C. Public, private, and corporate investigations
- D. Government, corporate, and private investigations

Correct Answer: A

---

### QUESTION 2

Refer to the following packet capture. Which of the following statements is true about this packet capture?

00:00:04.549138 IP omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq 3152949738, win 29200,

options [mss 1460,sackOK,TS val 1193148797 ecr 0,nop,wscale 7], length 0 00:00:05.547084 IP  
omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq 3152949738, win 29200,

options [mss 1460,sackOK,TS val 1193149047 ecr 0,nop,wscale 7], length 0 00:00:07.551078 IP  
omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq 3152949738, win 29200,

options [mss 1460,sackOK,TS val 1193149548 ecr 0,nop,wscale 7], length 0 00:00:11.559081 IP  
omar.cisco.com.34548 > 93.184.216.34.telnet: Flags [S], seq 3152949738, win 29200,

options [mss 1460,sackOK,TS val 1193150550 ecr 0,nop,wscale 7], length 0

- A. The host with the IP address 93.184.216.34 is the source.
- B. The host omar.cisco.com is the destination.
- C. This is a Telnet transaction that is timing out and the server is not responding.
- D. The server omar.cisco.com is responding to 93.184.216.34 with four data packets.

Correct Answer: D

---

### QUESTION 3

According to NIST what option is unnecessary for containment strategy?

- A. The delayed containment
- B. Monitoring with methods other than sandboxing



---

Correct Answer: AB

---

#### QUESTION 4

How do you enforce network access control automatically?

- A. IGMP
- B. SNMP
- C. 802.1X
- D. Port Security

Correct Answer: C

---

#### QUESTION 5

Employees are allowed access to internal websites. An employee connects to an internal website and IDS reports it as malicious behavior. What is this example of?

- A. true positive
- B. false negative
- C. false positive
- D. true negative

Correct Answer: C

---

[210-255 VCE Dumps](#)

[210-255 Practice Test](#)

[210-255 Exam Questions](#)