210-255$^{\text{Q\&As}}$

Cisco Cybersecurity Operations

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