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

Cisco Cybersecurity Operations

QUESTION 1

A user on your network receives an email in their mailbox that contains a malicious attachment. There is no indication that the file was run. Which category as defined in the Diamond Model of Intrusion does this activity fall under?

A. reconnaissance

B. weaponization

C. delivery

D. installation

Correct Answer: C

QUESTION 2

How do you verify that one of your hosts is potentially compromised based on their communication destinations?

A. Search the communication destinations of the host in the Talos IP and Domain Reputation Center.

B. Analyze how much traffic the host sent and received from each IP address or domain.

C. See if any Stealthwatch alarms were triggered for the host communicating with internal hosts.

D. Check the Firepower appliance to see if malicious files were downloaded.

Correct Answer: A

QUESTION 3

An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group. Which term defines the initial event in the NIST SP800- 61 r2?

A. instigator

B. precursor

C. online assault

D. trigger

Correct Answer: B

QUESTION 4

Which event artifact can be used to identify HTTP GET requests for a specific file?

A. HTTP status code

B. TCP ACK

C. destination IP

D. URI

Correct Answer: D

QUESTION 5

Which element can be used by a threat actor to discover a possible opening into a target network and can also be used by an analyst to determine the protocol of the malicious traffic?

A. TTLs

B. ports

C. SMTP replies

D. IP addresses

Correct Answer: B