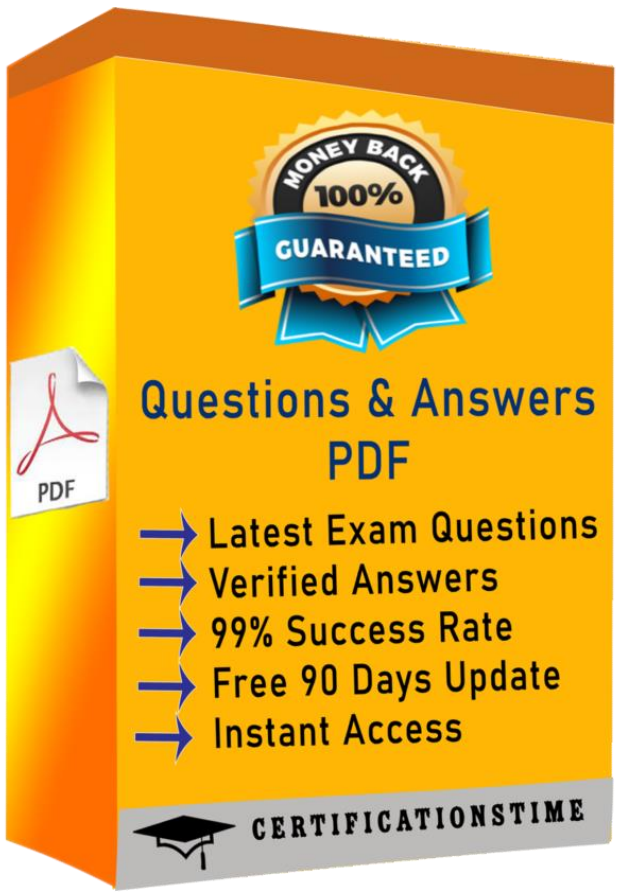
Cisco

Exam Questions 210-255

SECOPS Implementing Cisco Cybersecurity Operations

https://certificationstime.com/



Question: 1

Refer to the exhibit.
We have performed a malware detection on the Cisco website. Which statement about the result is true?
A. The website has been marked benign on all 68 checks.
B. The threat detection needsto run again.
C. The website has 68 open threats.
D. The website has been marked benign on 0 checks.
Answer: A
Explanation:
https://www.virustotal.com/en/url/df05d8e27bd760c33dc709951a5840cc6578d78d544d869890b7b94ea21e46b0/analysis/1368183553/

Question: 2

During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?
A. collection
B. examination
C. reporting
D. investigation
Answer: A

Question: 3

Refer to the Exhibit.
A customer reports that they cannot access your organization's website. Which option is a possible reason that the customer cannot access the website?
A. The server at 10.33.1.5 is using up too much bandwidth causing a denial- of-service.
B. The server at 10.67.10.5 has a virus.
C. A vulnerability scanner has shown that 10.67.10.5 has been compromised.
D. Web traffic sent from 10.67.10.5 has been identified as malicious by Internet sensors.
Answer: D
Explanation:
Every firewall has its own database where it maintains the website reputation on terms of security, ease of access, performance etc and below certain score (generally 7 in case of Cisco), firewalls block access to the sites. For example, you can visit www.senderbase.org and enter name of any website and you will see the reputation of that website.

Question: 4

You see 100 HTTP GET and POST requests for various pages on one of your web servers. The user agent in the requests contain php code that, if executed, creates and writes to a new php file on the webserver. Which category does this event fall under as defined in the Diamond Model of Intrusion?
A. delivery
B. reconnaissance
C. action on objectives
D. installation
E. exploitation
Answer: A

Question: 5

Which two options can be used by a threat actor to determine the role of a server? (Choose two.)
A. PCAP
B. tracert

C. running processes
D. hard drive configuration
E. applications
Answer: C, E

Question: 6

DRAG DROP
Drag and drop the type of evidence from the left onto the correct deception(s) of that evidence on the right.
Answer:
Questions & Answers PDF Page 5
https://certificationstime.com/updated/210-255-exam-dumps-pdf/

Question: 7

Which process is being utilized when IPS events are removed to improve data integrity?
A. data normalization
B. data availability
C. data protection
D. data signature
Answer: A
Explanation:
Data normalization is the process of intercepting and storing incoming data so it exists in one form only. This eliminates redundant data and protects the data's integrity.
Link: https://www.helpnetsecurity.com/2013/01/07/the-importance-of-data-normalization-in-ips/