

KillTest

更に上のクオリティ 更に上のサービス



問題集

<http://www.killtest.jp>

1年で無料進級することに提供する

Exam : **200-201**

Title : Understanding Cisco
Cybersecurity Operations
Fundamentals (CBROPS)

Version : DEMO

1.What are the two characteristics of the full packet captures? (Choose two.)

- A. Identifying network loops and collision domains.
- B. Troubleshooting the cause of security and performance issues.
- C. Reassembling fragmented traffic from raw data.
- D. Detecting common hardware faults and identify faulty assets.
- E. Providing a historical record of a network transaction.

Answer: C,E

2.A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver.

Which event category is described?

- A. reconnaissance
- B. action on objectives
- C. installation
- D. exploitation

Answer: C

3.How is attacking a vulnerability categorized?

- A. action on objectives
- B. delivery
- C. exploitation
- D. installation

Answer: C

4.What is the difference between the ACK flag and the RST flag in the NetFlow log session?

- A. The RST flag confirms the beginning of the TCP connection, and the ACK flag responds when the data for the payload is complete
- B. The ACK flag confirms the beginning of the TCP connection, and the RST flag responds when the data for the payload is complete
- C. The RST flag confirms the receipt of the prior segment, and the ACK flag allows for the spontaneous termination of a connection
- D. The ACK flag confirms the receipt of the prior segment, and the RST flag allows for the spontaneous termination of a connection

Answer: D

5.Which data format is the most efficient to build a baseline of traffic seen over an extended period of time?

- A. syslog messages
- B. full packet capture
- C. NetFlow
- D. firewall event logs

Answer: C

