600-199 Q&As

Securing Cisco Networks with Threat Detection and Analysis

Pass Cisco 600-199 Exam with 100% Guarantee

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

https://www.passapply.com/600-199.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

Refer to the exhibit.

What does the tcpdump command do?

A. Capture all packets sourced from TCP port 1514, resolve DNS names, print all TCP packets with the SYN flag not equaling 0, and print the Ethernet header and all version information.

B. Capture all packets sourced from TCP port 1514, resolve DNS names, print all TCP packets except those containing the SYN flag, and print the Ethernet header and all version information.

C. Capture up to 1514 bytes, do not resolve DNS names, print all TCP packets except for those containing the SYN flag, and print the Ethernet header and be very verbose.

D. Capture up to 1514 bytes, do not resolve DNS names, print only TCP packets containing the SYN flag, and print the Ethernet header and be very verbose.

Correct Answer: D

QUESTION 2

Which publication from the ISO covers security incident response?

A. 1918

B. 2865

C. 27035

D. 25012

Correct Answer: C

QUESTION 3

Which four tools are used during an incident to collect data? (Choose four.)

A. Sniffer

B. TCPDump

C. FTK

D. EnCase

E. ABC

F. ASA

G. Microsoft Windows 7

Correct Answer: ABCD

QUESTION 4

Which three statements are true about the IP fragment offset? (Choose three.)

A. A fragment offset of 0 indicates that it is the first in a series of fragments.

B. A fragment offset helps determine the position of the fragment within the reassembled datagram.

C. A fragment offset number refers to the number of fragments.

D. A fragment offset is measured in 8-byte units.

E. A fragment offset is measured in 16-byte units.

Correct Answer: ABD

QUESTION 5

In the context of a network security device like an IPS, which event would qualify as having the highest severity?

A. remote code execution attempt

B. brute force login attempt

C. denial of service attack

D. instant messenger activity

Correct Answer: A