https://www.lead4pass.com/600-199.html

VCE & PDF
Lead4Pass.com

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.lead4pass.com/600-199.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
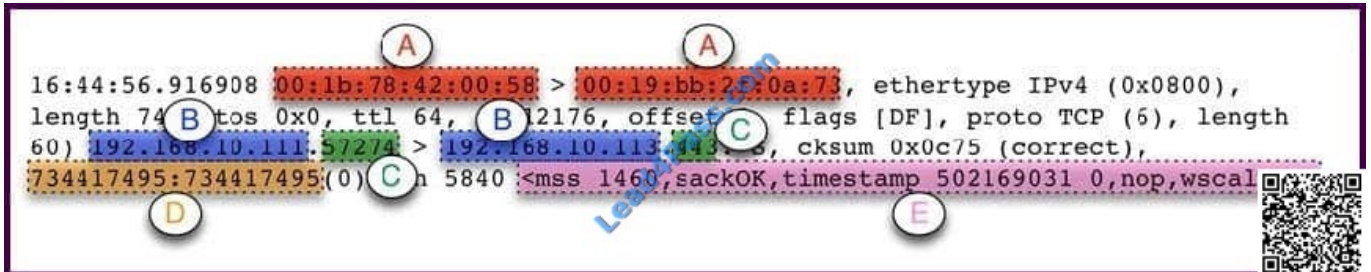Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibit.

In the packet captured from tcpdump, which fields match up with the lettered parameters?

A. A. Source and destination IP addresses, B. Source and destination Ethernet addresses, C. Source and destination TCP port numbers, D. TCP acknowledgement number, E. IP options

B. A. Source and destination Ethernet addresses, B. Source and destination IP addresses, C. Source and destination TCP port numbers, D. TCP sequence number, E. TCP options

C. A. Source and destination Ethernet addresses, B. Source and destination IP addresses, C. Source and destination TCP port numbers, D. TCP acknowledgement number, E. IP options

D. A. Source and destination Ethernet addresses, B. Source and destination IP addresses, C. Source and destination TCP port numbers, D. TCP sequence number, E. IP options

Correct Answer: B

QUESTION 2

What is the most effective way to save the data on a system for later forensic use?

A. Use a hard duplicator with write-block capabilities.

B. Copy the files to another disk.

C. Copy the disk file by file.

D. Shut down the system.

Correct Answer: A

QUESTION 3

Refer to the exhibit.

Exhibit: 3240

Which two personal administrators should be involved to investigate further? (Choose two.)

A. email administrator

B. IPS administrator

C. DNS administrator

D. desktop administrator

E. security administrator

Correct Answer: CD

QUESTION 4

Which two statements about the IPv4 TTL field are true? (Choose two.)

A. If the TTL is 0, the datagram is automatically retransmitted.

B. Each router that forwards an IP datagram reduces the TTL value by one.

C. It is used to limit the lifetime of an IP datagram on the Internet.

D. It is used to track IP datagrams on the Internet.

Correct Answer: BC

QUESTION 5

Refer to the exhibit.

Protocol	Total Flows	Flows /Sec	Packets Bytes /Flow /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
-------						

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr SrcP DstP	Pkts
Gi0	10.18.97.104	Local	10.22.9.98	06 FD3A 0016	63

Which protocol is used in this network traffic flow?

A. SNMP

B. SSH

C. DNS

D. Telnet

Correct Answer: B

To Read the Whole Q&As, please purchase the Complete Version from Our website.
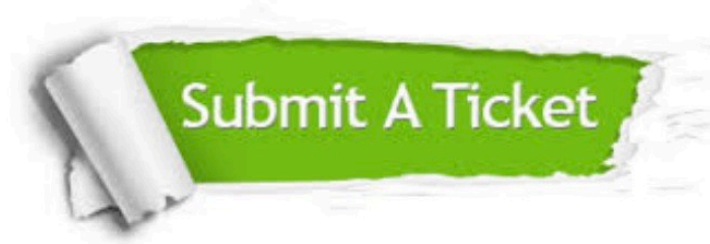
Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.lead4pass.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © lead4pass, All Rights Reserved.