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

Which is considered to be anomalous activity?

A. an alert context buffer containing traffic to amazon.com

B. an alert context buffer containing SSH traffic

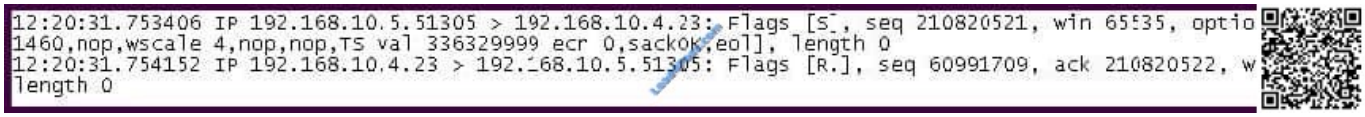
C. an alert context buffer containing an FTP server SYN scanning your network

D. an alert describing an anonymous login attempt to an FTP server

Correct Answer: C

QUESTION 2

Refer to the exhibit.



Based on the traffic captured in the tcpdump, what is occurring?

A. The device is powered down and is not on the network.

B. The device is reachable and a TCP connection was established on port 23.

C. The device is up but is not responding on port 23.

D. The device is up but is not responding on port 51305.

E. The resend flag is requesting the connection again.

Correct Answer: C

QUESTION 3

Which three symptoms are best used to detect a TCP SYN flood attack? (Choose three.)

A. high memory utilization on target server

B. large number of sockets in SYN_RECV state on target server

C. network monitoring devices report large number of unACKed SYNs sent to target server

D. target server crashes repeatedly

E. user experience with target server is slow or unresponsive

Correct Answer: BCE

QUESTION 4

When investigating potential network security issues, which two pieces of useful information would be found in a syslog message? (Choose two.)

A. product serial number

B. MAC address

C. IP address

D. product model number

E. broadcast address

Correct Answer: BC

QUESTION 5

Which two types of data are relevant to investigating network security issues? (Choose two.)

A. NetFlow

B. device model numbers

C. syslog

D. routing tables

E. private IP addresses

Correct Answer: AC

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: