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 publication from the ISO covers security incident response?

A. 1918

B. 2865

C. 27035

D. 25012

Correct Answer: C

QUESTION 2

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.

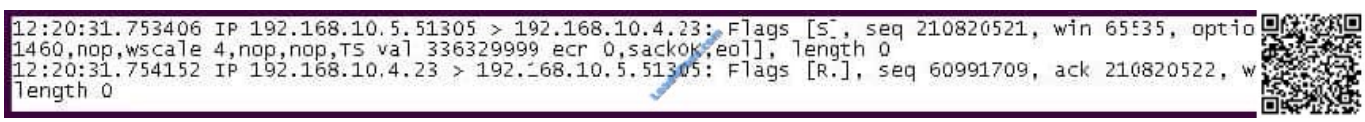
C. Capture up to 1514 bytes, do not resolve DNS names, print all TCP packets except for those containing the SYN flag, and print the Ethernet header and be very verbose.

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 3

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 4

Given a Linux machine running only an SSH server, which chain of alarms would be most concerning?

A. brute force login attempt from outside of the network, followed by an internal network scan

B. root login attempt followed by brute force login attempt

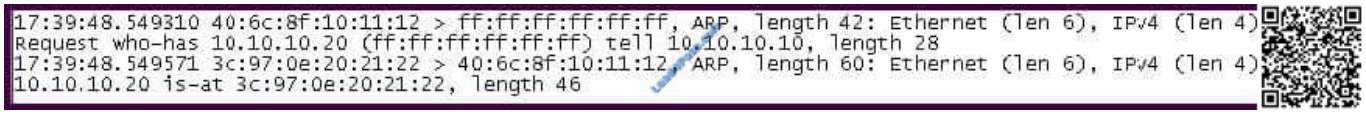
C. Microsoft RPC attack against the server

D. multiple rapid login attempts

Correct Answer: A

QUESTION 5

Refer to the exhibit.



Based on the tcpdump capture, which three statements are true? (Choose three.)

A. Host 10.10.10.20 is requesting the MAC address of host 10.10.10.10 using ARP.

B. Host 10.10.10.10 is requesting the MAC address of host 10.10.10.20.

C. The ARP request is unicast.

D. The ARP response is unicast.

E. The ARP request is broadcast.

F. Host 10.10.10.20 is using the MAC address of ffff.ffff.ffff.

Correct Answer: BDE

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: