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.pass4lead.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

In a network security policy, which procedure should be documented ahead of time to speed the communication of a network attack?

A. restoration plans for compromised systems

B. credentials for packet capture devices

C. Internet service provider contact information

D. risk analysis tool credentials

E. a method of communication and who to contact

Correct Answer: E

QUESTION 2

Refer to the exhibit.


```
12:20:31.753406 IP 192.168.10.5.51305 > 192.168.10.4.23: Flags [S], seq 210820521, win 65535, options [mss
1460,nop,wscale 4,nop,nop,TS val 336329999 ecr 0,sackOK,eol], length 0
12:20:31.754152 IP 192.168.10.4.23 > 192.168.10.5.51305: Flags [R.], seq 60991709, ack 210820522, win 0,
length 0
```

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

What is the purpose of the TCP SYN flag?

A. to sequence each byte of data in a TCP connection

B. to synchronize the initial sequence number contained in the Sequence Number header field with the other end of the connection

C. to acknowledge outstanding data relative to the byte count contained in the Sequence Number header field

D. to sequence each byte of data in a TCP connection relative to the byte count contained in the Sequence Number header field

Correct Answer: B

QUESTION 4

Which event is actionable?

A. SSH login failed

B. Telnet login failed

C. traffic flow started

D. reverse shell detected

Correct Answer: D

QUESTION 5

A server administrator tells you that the server network is potentially under attack. Which piece of information is critical to begin your network investigation?

A. cabinet location of the servers

B. administrator password for the servers

C. OS that is used on the servers

D. IP addresses/subnets used for the servers

Correct Answer: D

Latest 600-199 Dumps   600-199 Study Guide   600-199 Braindumps

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.pass4lead.com/allproducts

Need Help

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

One Year Free Update
Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee
To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy
We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.