



# 600-199<sup>Q&As</sup>

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.

```
tcpdump -vvv -s 1514 -e -n 'tcp[tcpflags] & tcp-syn !
```



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.

```
12:20:31.753406 IP 192.168.10.5.51305 > 192.168.10.4.23: Flags [S], seq 210820521, win 65535, optio  
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, w  
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 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.

```
17:39:48.549310 40:6c:8f:10:11:12 > ff:ff:ff:ff:ff:ff, ARP, length 42: Ethernet (len 6), IPv4 (len 4)
Request who-has 10.10.10.20 (ff:ff:ff:ff:ff:ff) tell 10.10.10.10, length 28
17:39:48.549571 3c:97:0e:20:21:22 > 40:6c:8f:10:11:12, ARP, length 60: Ethernet (len 6), IPv4 (len 4)
10.10.10.20 is-at 3c:97:0e:20:21:22, length 46
```



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:



 <p><b>One Year Free Update</b> 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.</p>	 <p><b>Money Back Guarantee</b> To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p><b>Security &amp; Privacy</b> We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; peace of mind.</p>
---	---	--

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.