600-199$^{Q\&As}$

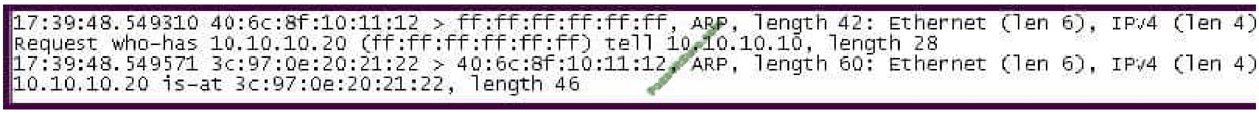
Securing Cisco Networks with Threat Detection and Analysis

Pass Cisco 600-199 Exam with 100% Guarantee

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

QUESTION 1

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

QUESTION 2

Which step should be taken first when a server on a network is compromised?

A. Refer to the company security policy.

B. Email all server administrators.

C. Determine which server has been compromised.

D. Find the serial number of the server.

Correct Answer: A

QUESTION 3

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 4

Which two tools are used to help with traffic identification? (Choose two.)

A. network sniffer

B. ping

C. traceroute

D. route table

E. NetFlow

F. DHCP

Correct Answer: AE

QUESTION 5

Which four tools are used during an incident to collect data? (Choose four.)

A. Sniffer

B. TCPDump

C. FTK

D. EnCase

E. ABC

F. ASA

G. Microsoft Windows 7

Correct Answer: ABCD

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

Try our product !

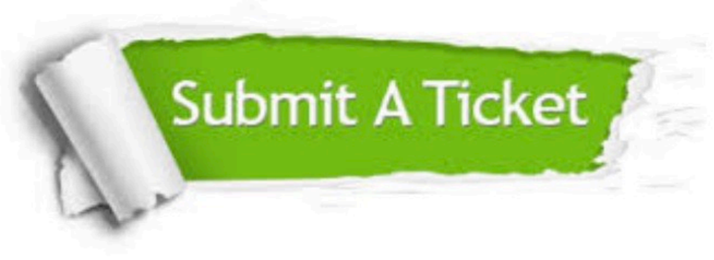
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.pass4itsure.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.

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.