[2017-New-DumpsFull Version 600-199 Exam Dump (VCE & PDF) 60Q for Free Download[Q11-Q20

2017 Feb. New Cisco 600-199 Exam Questions and Answers Updated Today!Free Download 600-199 Dumps and 600-199 VCE 60Q&As from www.braindump2go.com Today! 100% Real Exam Questions! 100% Exam Pass Guaranteed! 1.|NEW 600-199 Dumps and 600-199 PDF 60Q&As Download:http://www.braindump2go.com/600-199.html 2.|NEW 600-199 Exam Questions and 600-199 VCE Download:https://1drv.ms/f/s!AvI7wzKf6QBjgkm_DtWXO9h1Xwmc QUESTION 11Given the signature "SQL Table Manipulation Detected", which site may trigger a false positive? A. a company selling discount dining-room table insertsB. a large computer hardware companyC. a small networking companyD. a biotech company Answer: A QUESTION 12Which is considered to be anomalous activity? A. an alert context buffer containing traffic to amazon.comB. an alert context buffer containing SSH trafficC. an alert context buffer containing an FTP server SYN scanning your networkD. an alert describing an anonymous login attempt to an FTP server Answer: C QUESTION 13If an alert that pertains to a remote code execution attempt is seen on your network, which step is unlikely to help? A. looking for anomalous trafficB. looking for reconnaissance activityC. restoring the machine to a known good backupD. clearing the event store to see if future events indicate malicious activity Answer: D QUESTION 14Refer to the exhibit. In the tcpdump output, what is the sequence number that is represented by XXXXX?

A. 82080B. 82081C. 83448D. 83449E. 98496F. 98497 Answer: C QUESTION 15Refer to the exhibit. Based on the traffic captured in the tcpdump, what is occurring?

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. Answer: C QUESTION 16Which three statements are true about the IP fragment offset? (Choose three.) A. A fragment offset of 0 indicates that it is the first in a series of fragments.B. A fragment offset helps determine the position of the fragment within the reassembled datagram.C. A fragment offset number refers to the number of fragments.D. A fragment offset is measured in 8-byte units.E. A fragment offset is measured in 16-byte units. Answer: ABD QUESTION 17Which two tools are used to help with traffic identification? (Choose two.) A. network snifferB. pingC. tracerouteD. route tableE. NetFlowF. DHCP Answer: AE QUESTION 18Refer to the exhibit. Based on the tcpdump capture, which three statements are true? (Choose three.)

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. Answer: BDE QUESTION 19Refer to the exhibit. Based on the tcpdump output, which two statements are true? (Choose two.)

```
18:07:12.618698 40:6c:8f:11:20:20 > ff:ff:ff:ff:ff:ff, ARP,
Request who-has 192.168.10.7 tell 192.168.10.8, length 28
```

B. All devices in the same subnet on a switched network will see the reply because it was broadcast.C. The device is coming up for the first time and is requesting an IP address.D. The ARP request is being sent as a broadcast.E. The device is requesting an ARP.F. Host 192.168.10.7 is requesting the operational status of host 192.168.10.8. Answer: AD QUESTION 20Refer to the exhibit. Which two options does the following tcpdump command do? (Choose two.)

```
tcpdump -nvw arp host 10.10.10.10 and not port 80
```

A
.

R

e

a

d

f

r

o

m

n

V

r

a

m

n

o

n

V

o

l

a

t

l

e

)

a

n

d

p

a

r

S

e

t

e

s

t

r

e

a

m

B. Capture traffic based on host 10.10.10.10 and HTTP traffic.C. Capture traffic based on host 10.10.10.10 and everything but HTTP traffic.D. Capture ARP traffic only.E. Write the capture as a file.F. Read the capture from a file. Answer: CE