

## [2017-New-DumpsExam 600-199 Dumps VCE 60q Free Offered by Braindump2go[Q21-Q30]

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](http://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](https://1drv.ms/f/s!AvI7wzKf6QBjgkm_DtWxO9h1Xwmc) QUESTION 21 What is the maximum size of an IP datagram? A. There is no maximum size. B. It is limited only by the memory on the host computers at either end of the connection and the intermediate routers. C. 1024 bytes D. 65535 bytes E. 32768 bytes Answer: D QUESTION 22 The IHL is a 4-bit field containing what measurement? A. the number of 32-bit words in the IP header B. the size of the IP header, in bytes C. the size of the entire IP datagram, in bytes D. the number of bytes in the IP header E. the number of 32-bit words in the entire IP datagram Answer: A QUESTION 23 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 Answer: B QUESTION 24 Refer to the exhibit. What does the tcpdump command do?

A screenshot of a terminal window with a black background and white text. The text shows a command being entered: `tcpdump -vvv -s 1514 -e -n 'tcp[tcpflags] & tcp-syn != 0'`. The command is highlighted with a red rectangular box. The background of the terminal window has a faint, repeating watermark that reads "Braindump2go.com".

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. Answer: D QUESTION 25 What is the most effective way to save the data on a system for later forensic use? A. Use a hard duplicator with write-block capabilities. B. Copy the files to another disk. C. Copy the disk file by file. D. Shut down the system. Answer: A QUESTION 26 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 Answer: E QUESTION 27 Which data is the most useful to determine if a network attack was occurring from inbound Internet traffic? A. syslogs from all core switches B. NetFlow data from border firewall(s) C. VPN connection logs D. DNS request logs E. Apache server logs Answer: B QUESTION 28 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. Answer: A QUESTION 29 After an attack has occurred, which two options should be collected to help remediate the problem? (Choose two.) A. packet captures B. NAT translation table C. syslogs from affected devices D. connection table information E. NetFlow data Answer: CE QUESTION 30 Which source should be used to recommend preventative measures against security vulnerabilities regardless of operating system or platform? A. Microsoft security bulletins B. Cisco PSIRT notices C. Common Vulnerabilities and Exposure website D. Mozilla Foundation security advisories E. zero-day attack wiki

Answer: C    !!!RECOMMEND!!! 1.|NEW 600-199 Dumps and 600-199 PDF 60Q&As Download:  
<http://www.braindump2go.com/600-199.html> 2.|NEW 600-199 Study Guide: YouTube Video:  
[YouTube.com/watch?v=AgHGXRa9L1M](https://www.youtube.com/watch?v=AgHGXRa9L1M)