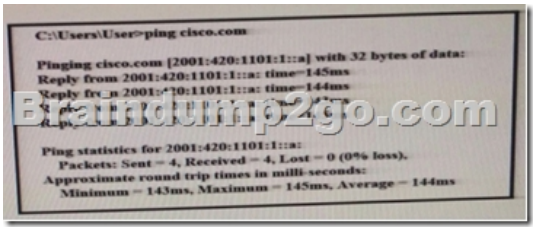
[2017-New-ExamsInstant 210-255 VCE Free Download in Braindump2go(21-30)

2017 March Cisco New 210-255: Implementing Cisco Cybersecurity Operations Exam Dumps (Full Version) Released Today!Free INSTANT Download 210-255 Exam Dumps (PDF & VCE) 70Q&As Download from www.Braindump2go.com **Today!** 100% REAL Exam Questions! 100% Exam Pass Guaranteed! 1.|NEW 210-255 Exam Dumps (PDF & VCE) 70Q&As Download http://www.braindump2go.com/210-255.html 2.|NEW 210-255 Exam Questions & Answers: https://1drv.ms/f/s!AvI7wzKf6QBjgn5gut7hxGLZ6xws QUESTION 21



Refer to the exhibit. What can be determined from this ping result? A. The public IP address of cisco.com is 2001:420:1101:1::a. B. The Cisco.com website is down.C. The Cisco.com website is responding with an internal IP.D. The public IP address of cisco.com is an IPv4 address. Answer: D QUESTION 22Which element is part of an incident response plan? A. organizational approach to incident responseB. organizational approach to securityC. disaster recoveryD. backups Answer: A QUESTION 23 Which source provides reports of vulnerabilities in software and hardware to a Security Operations Center? A. Analysis CenterB. National CSIRTC. Internal CSIRTD. Physical Security Answer: D QUESTION 24What information from HTTP logs can be used to find a threat actor? A. refererB. IP addressC. user-agentD. URL Answer: C QUESTION 25An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group. Which term defines the initial event in the NIST SP800- 61 r2? A. instigatorB. precursorC. online assaultD. trigger Answer: D QUESTION 26You have run a suspicious file in a sandbox analysis tool to see what the file does. The analysis report shows that outbound callouts were made post infection. Which two pieces of information from the analysis report are needed or required to investigate the callouts? (Choose two.) A. file sizeB. domain namesC. dropped filesD. signaturesE. host IP addresses Answer: AE QUESTION 27Which option filters a LibPCAP capture that used a host as a gateway? A. tcp|udp] [src|dst] port <port>B. [src|dst] net <net> [{mask <mask>}|{len <len>}]C. ether [src|dst] host <ehost>D. gateway host <host> Answer: D QUESTION 28Which type of analysis allows you to see how likely an exploit could affect your network? A. descriptiveB. casualC. probabilisticD. inferential Answer: C QUESTION 29Which network device creates and sends the initial packet of a session? A. sourceB. originationC. destinationD. network Answer: B QUESTION 30When performing threat hunting against a DNS server, which traffic toward the affected domain is considered a starting point? A. HTTPS trafficB. TCP trafficC. HTTP trafficD. UDP traffic Answer: B !!!RECOMMEND!!! 1.|NEW 210-255 Exam Dumps (PDF & VCE) 70Q&As Download http://www.braindump2go.com/210-255.html 2.|NEW 210-255 Study Guide Video: YouTube Video: YouTube.com/watch?v=3fI6ShLlZQo