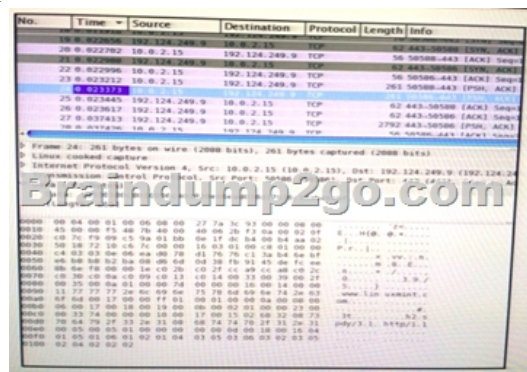


[2017-New-Exams100% Exam Pass-210-255 Dumps VCE and PDF Free from Braindump2go(31-40)

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: <http://1drv.ms/f/s!AvI7wzKf6QBjgn5gut7hxGLZ6xws> QUESTION 31

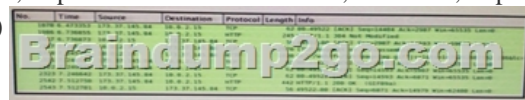


No.	Time	Source	Destination	Protocol	Length	Info
20	0.027982	192.124.249.9	192.124.249.9	TCP	60	65430->65430 [ACK] Seq=261505880
21	0.027982	192.124.249.9	192.124.249.9	TCP	60	65430->65430 [ACK] Seq=261505880
22	0.027982	192.124.249.9	192.124.249.9	TCP	60	65430->65430 [ACK] Seq=261505880
23	0.027982	192.124.249.9	192.124.249.9	TCP	60	65430->65430 [ACK] Seq=261505880
24	0.027982	192.124.249.9	192.124.249.9	TCP	60	65430->65430 [ACK] Seq=261505880
25	0.027982	192.124.249.9	192.124.249.9	TCP	60	65430->65430 [ACK] Seq=261505880
26	0.027982	192.124.249.9	192.124.249.9	TCP	60	65430->65430 [ACK] Seq=261505880
27	0.027982	192.124.249.9	192.124.249.9	TCP	60	65430->65430 [ACK] Seq=261505880
28	0.027982	192.124.249.9	192.124.249.9	TCP	60	65430->65430 [ACK] Seq=261505880

Refer to the exhibit. Which application protocol is in this PCAP file? A. TCPB. SSHC. HTTPD. SSL Answer: C QUESTION 32You see confidential data being exfiltrated to an IP address that is attributed to a known Advanced Persistent Threat group. Assume that this is part of a real attach and not a network misconfiguration. Which category does this event fall under as defined in the Diamond Model of Intrusion? A. reconnaissanceB. weaponizationC. deliveryD. action on objectives Answer: A QUESTION 33Refer to the exhibit.



We have performed a malware detection on the Cisco website. Which statement about the result is true? A. The website has been marked benign on all 68 checks.B. The threat detection needs to run again.C. The website has 68 open threats.D. The website has been marked benign on 0 checks. Answer: A QUESTION 34Which option has a drastic impact on network traffic because it can cause legitimate traffic to be blocked? A. true positiveB. true negativeC. false positiveD. false negative Answer: A QUESTION 35Which CVSSv3 metric value increases when the attacker is able to modify all files protected by the vulnerable component? A. confidentialityB. integrityC. availabilityD. complexity Answer: A QUESTION 36During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity? A. collectionB. examinationC. reportingD. investigation Answer: A QUESTION 37Which information must be left out of a final incident report? A. server hardware configurationsB. exploit or vulnerability usedC. impact and/or the financial lossD. how the incident was detected Answer: B QUESTION 38Which two components are included in a 5-tuple? (Choose two.) A. port numberB. destination IP addressC. data packetD. user nameE. host logs Answer: BC QUESTION 39In VERIS, an incident is viewed as a series of events that adversely affects the information assets of an organization. Which option contains the elements that every event is comprised of according to VERIS incident model? A. victim demographics, incident description, incident details, discovery & responseB. victim demographics, incident details, indicators of compromise, impact assessmentC. actors, attributes, impact, remediationD. actors, actions, assets, attributes Answer: D QUESTION 40



Refer to the exhibit. Which packet contains a file that is extractable within Wireshark? A. 1986B. 2318C. 2542D. 2317 Answer: D !!!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=3fI6ShLIZQo](https://www.youtube.com/watch?v=3fI6ShLIZQo)