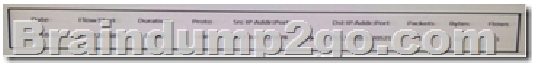
[2017-New-Exams!100% Success-Braindump2go 210-255(SECOPS) Exam PDF 70q Instant Download[Q1-Q9

2017 New Cisco 210-255: Implementing Cisco Cybersecurity Operations Exam Questions Released by Braindump2go.com Today! 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 Downoad:https://1drv.ms/f/s!AvI7wzKf6QBjgn5gut7hxGLZ6xws QUESTION 1Which option can be addressed when using retrospective security techniques? A. if the affected host needs a software updateB. how the malware entered our networkC. why the malware is still in our networkD. if the affected system needs replacement Answer: A QUESTION 2Refer to the exhibit. Which type of log is this an example of? A. IDS logB. proxy logC. NetFlow logD. syslog Answer: A QUESTION 3Which option is a misuse variety per VERIS enumerations? A. snoopingB. hackingC. theftD. assault Answer: B QUESTION 4In the context of incident handling phases, which two activities fall under scoping? (Choose two.) A. determining the number of attackers that are associated with a security incidentB. ascertaining the number and types of vulnerabilities on your networkC. identifying the extent that a security incident is impacting protected resources on the networkD. determining what and how much data may have been affectedE. identifying the attackers that are associated with a security incident Answer: DE QUESTION 5Which regular expression matches "color" and "colour"? A. col[0-9]+ourB. colo?urC. colou?rD.]a-z]{7} Answer: C QUESTION 6Which component of the NIST SP800-61 r2 incident handling strategy reviews data? A. preparationB. detection and analysisC. containment, eradication, and recoveryD. post-incident analysis Answer: B QUESTION 7Which option is generated when a file is run through an algorithm and generates a string specific to the contents of that file? A. URLB. hashC. IP addressD. destination port Answer: C QUESTION 8Which data type is protected under the PCI compliance framework? A. credit card typeB. primary account numberC. health conditions D. provision of individual care Answer: C QUESTION 9Which kind of evidence can be considered most reliable to arrive at an analytical assertion? A. directB. corroborativeC. indirectD. circumstantialE. textual Answer: A !!!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



Date	Flow Start	Durati	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]