[June-2019-NewHigh Quality Braindump2go 210-255 Exam Dumps PDF and VCE 170Q Free Share

June/2019 Braindump2go Cisco CCNA Cyber Ops 210-255 SECOPS Dumps with PDF and VCE New Updated Today! Following are some new 210-255 Exam Questions:1.|2019 Laetst 210-255 Exam Dumps (PDF & VCE) Instant Download:https://www.braindump2go.com/210-255.html2.|2019 Laetst 210-255 Exam Questions & Answers Instant Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNMTN5bVpTMFFJMXM?usp=sharingNew QuestionWhat is the difference between deterministic and probabilistic assessment method?A. At deterministic method we know the facts beforehand and at probabilistic method we make assumptionsB. At probabilistic method we know the facts beforehand and at deterministic method we make assumptionsC. Probabilistic method has an absolute natureD. Determinstc method has an absolute nature **Answer: AD**New QuestionWhich of the following is not an example of the VERIS main schema categories?A. Incident tracking B. Victim demographicsC. Incident descriptionsD. Incident forensics ID**Answer: D**New QuestionWhat is Data mapping used for? (Choose two)A. data accuracy (integrity)B. data availabilityC. data normalizationD. data confidentialityE. data visualisation**Answer: AE**New QuestionWhich type of intrusion event is an attacker retrieving the robots. txt file from target site?A. exploitationB. weaponizationC. scanningD. reconnaissance**Answer: D**New QuestionWhich two potions about deterministic and probabilistic analysis are true? (Choose two.)A. probabilistic analysis uses data known beforehand and deterministic analysis is based off assumptions.B. Deterministic analysis uses data known beforehand and probabilistic analysis based off of assumptions.C. Deterministic analysis is based off of assumptionsD. Probabilistic analysis result in a result that is definitive.E. probabilistic analysis results in a result that is not definitive.**Answer: BE**New QuestionRefer to exhibit. Which option is the logical source device for these events? A. web serverB. NetFlow collectorC. proxy serverD. IDS/IPS**Answer: D**New Question Which option is the common artifact used to uniquely identify a detected file?A. file sizeB. file extensionC. file timestampD. file hash**Answer: D**New QuestionWhich two useful pieces of information can be collected from the IPv4 protocol header? (Choose two.)A. UDP port which the traffic is destinedB. source IP address of the packetC. UDP port from which the traffic is sourced D. TCP port from which the traffic was sourceE. destination IP address of the packet**Answer: BE**New QuestionWhich option is unnecessary for determining the appropriate containment strategy according to NIST.SP800-61 r2?A. effectiveness of the strategy B. time and resource needed to implement the strategyC. need for evidence preservationD. attack vector used to compromise the system**Answer: D**New QuestionWhich type verification typically consists of using tools to compute the message digest of the original and copies data, then comparing the digests to make sure that they are the same?A. evidence collection orderB. data integrityC. data preservationD. volatile data collection**Answer: B**New QuestionWhich function does an internal CSIRT provide?A. incident handling services across various CSIRTsB. incident handling services for a country's governmentC. incident handling services for a parent organizationD. incident handling services as a service for other organization**Answer: C**
!!!RECOMMNED!!!1.|2019 Laetst 210-255 Exam Dumps (PDF & VCE) Instant Download:https://www.braindump2go.com/210-255.html2.|2019 Laetst 210-255 Study Guide Video Instant Download: YouTube Video: YouTube.com/watch?v=mD4Ho8oM37g