

[June-2019-NewHigh Quality Braindump2go 210-255 PDF and VCE Dumps 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.html>2.|2019 Laetst 210-255 Exam Questions & Answers Instant

Download:<https://drive.google.com/drive/folders/0B75b5xYLjSSNMTN5bVpTMFFJMXM?usp=sharing>What 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. Deterministic method has an absolute nature

Answer: ANew QuestionWhich of the following is not an example of the VERIS main schema categories?A. Incident trackingB. Victim demographicsC. Incident descriptionsD. Incident forensics ID

Answer: DNew QuestionWhat is Data mapping used for? (Choose two)A. data accuracy (integrity)B. data availabilityC. data normalizationD. data confidentialityE. data visualisation

Answer: ANew QuestionWhich type of intrusion event is an attacker retrieving the robots. txt file from target site?A. exploitationB. weaponizationC. scanningD. reconnaissance

Answer: DNew QuestionWhich two options 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: BNew QuestionRefer to exhibit. Which option is the logical source device for these events? A. web serverB. NetFlow collectorC. proxy serverD. IDS/IPS

Answer: DNew QuestionWhich option is the common artifact used to uniquely identify a detected file?A. file sizeB. file extensionC. file timestampD. file hash

Answer: DNew 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 sourcedD. TCP port from which the traffic was sourceE. destination IP address of the packet

Answer: BNew QuestionWhich option is unnecessary for determining the appropriate containment strategy according to NIST.SP800-61 r2?A. effectiveness of the strategyB. time and resource needed to implement the strategyC. need for evidence preservationD. attack vector used to compromise the system

Answer: DNew 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: BNew 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

!!!RECOMMENDED!!!1.|2019 Laetst 210-255 Exam Dumps (PDF & VCE) Instant

Download:<https://www.braindump2go.com/210-255.html>2.|2019 Laetst 210-255 Study Guide Video Instant Download: YouTube

Video: [YouTube.com/watch?v=mD4Ho8oM37g](https://www.youtube.com/watch?v=mD4Ho8oM37g)