[Sep-2020Exam Pass 100%!Braindump2go 200-201 Dumps 200-201 113Q Instant Download[Q40-Q60

2020/Sep Latest Braindump2go 200-201 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 200-201 Real Exam Questions!QUESTION 40Which type of data typically consists of connection level, application-specific records generated from network traffic?A. location dataB. statistical dataC. alert dataD. transaction dataAnswer: BQUESTION 41 What are three key components of a threat-centric SOC? (Choose three.)A. peopleB. compliancesC. processesD. regulations E. technologiesAnswer: ACEQUESTION 42An analyst is investigating an incident in a SOC environment.Which method is used to identify a session from a group of logs?A. sequence numbersB. IP identifierC. 5-tupleD. timestampsAnswer: CQUESTION 43Refer to the exhibit. Which type of log is displayed?

A. proxy B. NetFlowC. IDSD. sysAnswer: BQUESTION 44What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?A. Tapping interrogation replicates signals to a separate port for analyzing trafficB. Tapping interrogations detect and block malicious trafficC. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policiesD. Inline interrogation detects malicious traffic but does not block the trafficAnswer: AQUESTION 45Which two components reduce the attack surface on an endpoint? (Choose two.)A. secure bootB. load balancingC. increased audit log levelsD. restricting USB portsE. full packet captures at the endpointAnswer: ADQUESTION 46An analyst discovers that a legitimate security alert has been dismissed.Which signature caused this impact on network traffic?A. true negativeB. false negativeC. false positiveD. true positiveAnswer: BQUESTION 47 Which event artifact is used to identity HTTP GET requests for a specific file?A. destination IP addressB. TCP ACKC. HTTP status codeD. URIAnswer: DQUESTION 48Which security principle requires more than one person is required to perform a critical task?A. least privilegeB. need to knowC. separation of dutiesD. due diligenceAnswer: CQUESTION 49What are two differences in how tampered and untampered disk images affect a security incident? (Choose two.)A. Untampered images are used in the security investigation processB. Tampered images are used in the security investigation processC. The image is tampered if the stored hash and the computed hash matchD. Tampered images are used in the incident recovery processE. The image is untampered if the stored hash and the computed hash matchAnswer: BEQUESTION 50What makes HTTPS traffic difficult to monitor?A. SSL interceptionB. packet header sizeC. signature detection timeD. encryptionAnswer: DQUESTION 51An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture the analyst cannot determine the technique and payload used for the communication.

Which obfuscation technique is the attacker using?A. Base64 encodingB. transport layer security encryptionC. SHA-256 hashingD. ROT13 encryptionAnswer: BQUESTION 52What best describes the Security Operations Center (SOC)?A. The SOC is usually responsible for monitoring and maintaining the overall network infrastructure, its primary function is to ensure uninterrupted network service.B. A SOC is related to the people, processes, and technologies that are involved in providing situational awareness through the detection, containment, and remediation of information security threats.C. The SOC is responsible for the physical security of a building or installation location.D. The SOC and NOC are the same entity, with different names. They are responsible for the health and security of the network infrastructure.Answer: BQUESTION 53Which term represents a potential danger that could take advantage of a weakness in a system?A. vulnerabilityB. riskC. threatD. exploitAnswer: CQUESTION 54Which artifact is used to uniquely identify a detected file?A. file timestampB. file extensionC. file sizeD. file hashAnswer: DQUESTION 55How does an attacker observe network traffic exchanged between two users?A. port scanningB. man-in-the-middleC. command injectionD. denial of serviceAnswer: BQUESTION 56Refer to the exhibit. Which event is occurring?

A. A binary named "submit" is running on VM cuckoo1.B. A binary is being submitted to run on VM cuckoo1C. A binary on VM cuckoo1 is being submitted for evaluationD. A URL is being evaluated to see if it has a malicious binaryAnswer: CQUESTION 57What is a benefit of agent-based protection when compared to agentless protection?A. It lowers maintenance costsB. It provides a centralized platformC. It collects and detects all traffic locallyD. It manages numerous devices simultaneouslyAnswer: BQUESTION 58Which principle is being followed when an analyst gathers information relevant to a security incident to determine the appropriate course of action?A. decision makingB. rapid responseC. data miningD. due diligenceAnswer: AQUESTION 59An engineer runs a suspicious file in a sandbox analysis tool to see the outcome. The analysis report shows that outbound callouts were made post infection.Which two pieces of information from the analysis report are needed to investigate the callouts? (Choose two.)A. signaturesB. host IP addressesC. file sizeD. dropped filesE. domain namesAnswer: BEQUESTION 60An analyst is exploring the functionality of different operating systems. What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?A. queries Linux devices that have Microsoft Services for Linux installedB. deploys Windows Operating Systems in an automated fashionC. is an efficient tool for working with Active DirectoryD. has a Common Information Model, which describes installed hardware and softwareAnswer: DResources From:1.2020 Latest Braindump2go 200-201 Exam Dumps (PDF & VCE) Free Share: https://www.braindump2go.com/200-201.html2.2020 Latest Braindump2go 200-201 PDF and 200-201 VCE Dumps Free Share: https://drive.google.com/drive/folders/1fTPALtM-eluHFw8sUjNGF7Y-ofOP3s-M?usp=sharing3.2020 Free Braindump2go 200-201 PDF Download:https://www.braindump2go.com/free-online-pdf/200-201-Dumps(43-55).pdf
https://www.braindump2go.com/free-online-pdf/200-201-PDF(30-42).pdf
https://www.braindump2go.com/free-online-pdf/200-201-PDF-Dumps(1-15).pdf
https://www.braindump2go.com/free-online-pdf/200-201-VCE(16-29).pdf
https://www.braindump2go.com/free-online-pdf/200-201-VCE-Dumps(56-69).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!