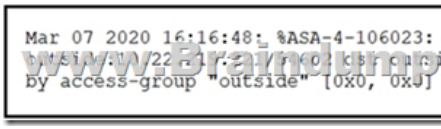
# [April-2021Braindump2go 200-201 PDF Free Instant Download[Q144-Q171

April/2021 Latest Braindump2go 200-201 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 200-201 Real Exam Questions!QUESTION 144Which action should be taken if the system is overwhelmed with alerts when false positives and false negatives are compared?A. Modify the settings of the intrusion detection system.B. Design criteria for reviewing alerts.C. Redefine signature rules.D. Adjust the alerts schedule.Answer: AQUESTION 145What is the impact of false positive alerts on business compared to true positive?A. True positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.B. True positive alerts are blocked by mistake as potential attacks affecting application availability.C. False positives affect security as no alarm is raised when an attack has taken place, resulting in a potential breach.D. False positive alerts are blocked by mistake as potential attacks affecting application availability.Answer: CQUESTION 146An engineer needs to fetch logs from a proxy server and generate actual events according to the data received. Which technology should the engineer use to accomplish this task?A. FirepowerB. Email Security ApplianceC. Web Security ApplianceD. StealthwatchAnswer: CQUESTION 147Refer to the exhibit. Which technology generates this log?



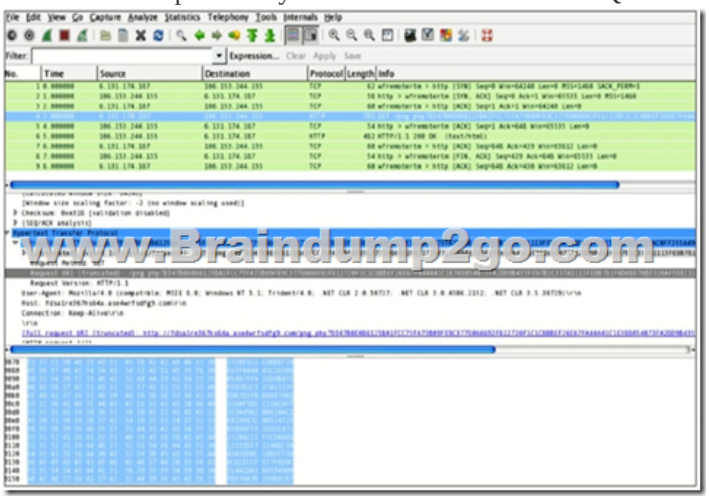

A. NetFlowB. IDSC. web proxyD. firewallAnswer: DQUESTION 148Which filter allows an engineer to filter traffic in Wireshark to further analyze the PCAP file by only showing the traffic for LAN 10.11.x.x, between workstations and servers without the Internet?A. src=10.11.0.0/16 and dst=10.11.0.0/16B. ip.src==10.11.0.0/16 and ip.dst==10.11.0.0/16C. ip.src=10.11.0.0/16 and ip.dst=10.11.0.0/16D. src==10.11.0.0/16 and dst==10.11.0.0/16Answer: BQUESTION 149Which tool provides a full packet capture from network traffic?A. NagiosB. CAINEC. HydraD. WiresharkAnswer: DQUESTION 150A company is using several network applications that require high availability and responsiveness, such that milliseconds of latency on network traffic is not acceptable. An engineer needs to analyze the network and identify ways to improve traffic movement to minimize delays. Which information must the engineer obtain for this analysis?A. total throughput on the interface of the router and NetFlow recordsB. output of routing protocol authentication failures and ports usedC. running processes on the applications and their total network usageD. deep packet captures of each application flow and durationAnswer: CQUESTION 151Refer to the exhibit. What is depicted in the exhibit?


A. Windows Event logsB. Apache logsC. IIS logsD. UNIX-based syslogAnswer: DQUESTION 152Which technology should be used to implement a solution that makes routing decisions based on HTTP header, uniform resource identifier, and SSL session ID attributes?A. AWSB. IISC. Load balancerD. Proxy serverAnswer: BQUESTION 153An organization has recently adjusted its security stance in response to online threats made by a known hacktivist group.What is the initial event called in the NIST SP800-61?A. online assaultB. precursorC. triggerD. instigatorAnswer: BQUESTION 154Which NIST IR category stakeholder is responsible for coordinating incident response among various business units, minimizing damage, and reporting to regulatory agencies?A. CSIRTB. PSIRTC. public affairsD. managementAnswer: DQUESTION 155Which incidence response step includes identifying all hosts affected by an attack?A. detection and analysisB. post-incident activityC. preparationD. containment, eradication, and recoveryAnswer: DQUESTION 156Which two elements are used for profiling a network? (Choose two.)A. session durationB. total throughputC. running processesD. listening portsE. OS fingerprintAnswer: DEQUESTION 157Which category relates to improper use or disclosure of PII data?A. legalB. compliance C. regulatedD. contractualAnswer: CQUESTION 158Which type of evidence supports a theory or an assumption that results from initial evidence?A. probabilisticB. indirectC. bestD. corroborativeAnswer: DQUESTION 159Which two elements are assets in the role of attribution in an investigation? (Choose two.)A. contextB. sessionC. laptopD. firewall logsE. threat actorAnswer: AEQUESTION 160What is personally identifiable information that must be safeguarded from unauthorized access?A. date of birthB. driver's license numberC. genderD. zip codeAnswer: BQUESTION 161In a SOC environment, what is a vulnerability management metric?A. code signing enforcementB. full assets scanC. internet exposed devicesD. single factor authenticationAnswer: CQUESTION 162A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS

format. Which type of evidence is this file?A. CD data copy prepared in WindowsB. CD data copy prepared in Mac-based systemC. CD data copy prepared in Linux systemD. CD data copy prepared in Android-based systemAnswer: CQUESTION 163 Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)A. detection and analysisB. post-incident activityC. vulnerability managementD. risk assessmentE. vulnerability scoringAnswer: ABQUESTION 164Refer to the exhibit. What does this output indicate?

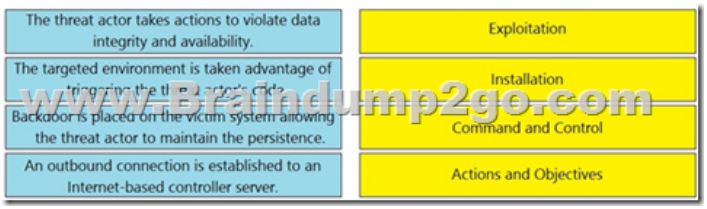



A. HTTPS ports are open on the server.B. SMB ports are closed on the server.C. FTP ports are open on the server.D. Email ports are closed on the server.Answer: AQUESTION 165Which metric should be used when evaluating the effectiveness and scope of a Security Operations Center?A. The average time the SOC takes to register and assign the incident.B. The total incident escalations per week. C. The average time the SOC takes to detect and resolve the incident.D. The total incident escalations per month.Answer: CQUESTION 166A developer is working on a project using a Linux tool that enables writing processes to obtain these required results:- If the process is unsuccessful, a negative value is returned. - If the process is successful, 0 value is returned to the child process, and the process ID is sent to the parent process.Which component results from this operation?A. parent directory name of a file pathnameB. process spawn scheduledC. macros for managing CPU setsD. new process created by parent processAnswer: DQUESTION 167An engineer discovered a breach, identified the threat's entry point, and removed access. The engineer was able to identify the host, the IP address of the threat actor, and the application the threat actor targeted. What is the next step the engineer should take according to the NIST SP 800-61 Incident handling guide?A. Recover from the threat.B. Analyze the threat.C. Identify lessons learned from the threat.D. Reduce the probability of similar threats.Answer: DQUESTION 168 Refer to the exhibit. What is shown in this PCAP file?

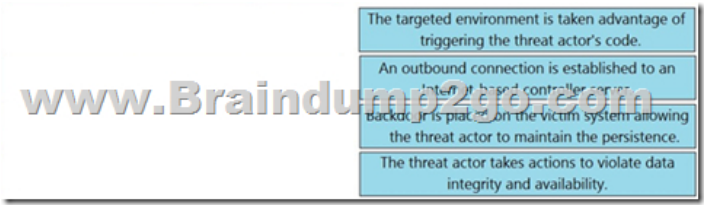




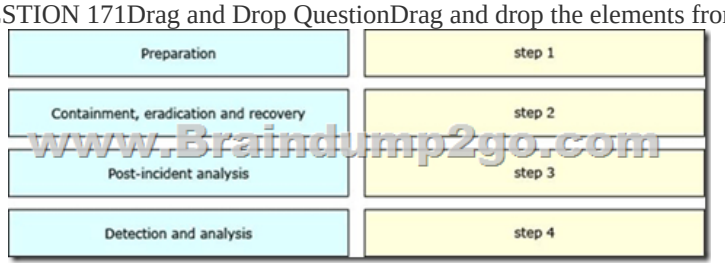
A. Timestamps are indicated with error.B. The protocol is TCP.C. The User-Agent is Mozilla/5.0.D. The HTTP GET is encoded.Answer: AQUESTION 169What is a difference between tampered and untampered disk images?A. Tampered images have the same stored and computed hash.B. Tampered images are used as evidence.C. Untampered images are used for forensic investigations.D. Untampered images are deliberately altered to preserve as evidenceAnswer: BQUESTION 170Drag and Drop QuestionDrag and drop the definition from the left onto the phase on the right to classify intrusion events according to the Cyber Kill Chain model.



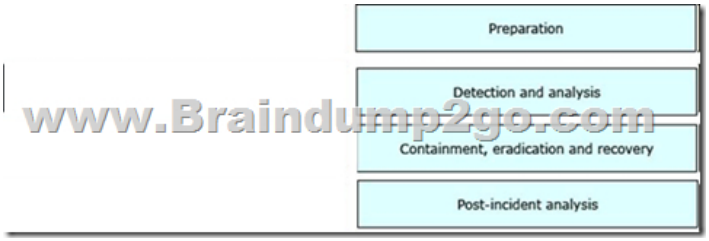

Answer:




QUESTION 171Drag and Drop QuestionDrag and drop the elements from the left into the correct order for incident handling on the right.




Answer:




Resources From:1.2021 Latest Braindump2go 200-201 Exam Dumps (PDF & VCE) Free Share: https://www.braindump2go.com/200-201.html2.2021 Latest Braindump2go 200-201 PDF and 200-201 VCE Dumps Free Share: https://drive.google.com/drive/folders/1fTPALtM-eluHFw8sUjNGF7Y-ofOP3s-M?usp=sharing3.2021 Free Braindump2go 200-201 Exam Questions Download:https://www.braindump2go.com/free-online-pdf/200-201-PDF-Dumps(144-171).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!