[September-2021Braindump2go 200-201 Exam PDF and VCE Dumps 200-201 200Q Offered for Free Download[Q172-Q191

September/2021 Latest Braindump2go 200-201 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 200-201 Real Exam Questions!QUESTION 172The SOC team has confirmed a potential indicator of compromise on an endpoint. The team has narrowed the executable file's type to a new trojan family. According to the NIST Computer Security Incident Handling Guide, what is the next step in handling this event?A. Isolate the infected endpoint from the network.B. Perform forensics analysis on the infected endpoint.C. Collect public information on the malware behavior.D. Prioritize incident handling based on the impact.Answer: CQUESTION 173Which technology on a host is used to isolate a running application from other applications?A. sandboxB. application allow listC. application block listD. host-based firewallAnswer: AQUESTION 174An analyst received a ticket regarding a degraded processing capability for one of the HR department's servers. On the same day, an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?A. RecoveryB. DetectionC. EradicationD. AnalysisAnswer: BQUESTION 175Which data type is necessary to get information about source/destination ports?A. statistical dataB. session dataC. connectivity dataD. alert dataAnswer: CQUESTION 176Refer to the exhibit. Which type of attack is being executed?A. SQL injectionB. cross-site scriptingC. cross-site request forgeryD. command injectionAnswer: AQUESTION 177Which attack represents the evasion technique of resource exhaustion?A. SQL injectionB. man-in-the-middle C. bluesnarfingD. denial-of-serviceAnswer: DQUESTION 178A threat actor penetrated an organization's network. Using the 5-tuple approach, which data points should the analyst use to isolate the compromised host in a grouped set of logs?A. event name, log source, time, source IP, and host nameB. protocol, source IP, source port, destination IP, and destination portC. event name, log source, time, source IP, and usernameD. protocol, log source, source IP, destination IP, and host nameAnswer: BQUESTION 179Which event is a vishing attack?A. obtaining disposed documents from an organizationB. using a vulnerability scanner on a corporate networkC. setting up a rogue access point near a public hotspotD. impersonating a tech support agent during a phone callAnswer: DQUESTION 180What is indicated by an increase in IPv4 traffic carrying protocol 41 ?A. additional PPTP traffic due to Windows clientsB. unauthorized peer-to-peer trafficC. deployment of a GRE network on top of an existing Layer 3 networkD. attempts to tunnel IPv6 traffic through an IPv4 networkAnswer: DQUESTION 181What 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, while false positives are alerts raised appropriately to detect and further mitigate them.B. True-positive alerts are blocked by mistake as potential attacks, while False-positives are actual attacks Identified as harmless.C. False-positive alerts are detected by confusion as potential attacks, while true positives are attack attempts identified appropriately.D. False positives alerts are manually ignored signatures to avoid warnings that are already acknowledged, while true positives are warnings that are not yet acknowledged.Answer: CQUESTION 182An organization's security team has detected network spikes coming from the internal network. An investigation has concluded that the spike in traffic was from intensive network scanning How should the analyst collect the traffic to isolate the suspicious host?A. by most active source IPB. by most used portsC. based on the protocols used D. based on the most used applicationsAnswer: CQUESTION 183What is an incident response plan?A. an organizational approach to events that could lead to asset loss or disruption of operationsB. an organizational approach to security management to ensure a service lifecycle and continuous improvementsC. an organizational approach to disaster recovery and timely restoration ot operational servicesD. an organizational approach to system backup and data archiving aligned to regulationsAnswer: CQUESTION 184An engineer is addressing a connectivity issue between two servers where the remote server is unable to establish a successful session. Initial checks show that the remote server is not receiving an SYN-ACK while establishing a session by sending the first SYN.What is causing this issue?A. incorrect TCP handshakeB. incorrect UDP handshakeC. incorrect OSI configurationD. incorrect snaplen configurationAnswer: AQUESTION 185A security incident occurred with the potential of impacting business services. Who performs the attack?A. malware authorB. threat actorC. bug bounty hunterD. direct competitorAnswer: AQUESTION 186Refer to the exhibit. An analyst received this alert from the Cisco ASA device, and numerous activity logs were produced.



How should this type of evidence be categorized?A. indirectB. circumstantialC. corroborativeD. bestAnswer: DQUESTION 187W[t is vulnerability management?A. A security practice focused on clarifying and narrowing intrusion points.B. A security

practice of performing actions rather than acknowledging the threats.C. A process to identify and remediate existing weaknesses. D. A process to recover from service interruptions and restore business-critical applicationsAnswer: CQUESTION 188A user received an email attachment named "Hr405-report2609-empl094.exe" but did not run it. Which category of the cyber kill chain should be assigned to this type of event?A. installationB. reconnaissanceC. weaponizationD. deliveryAnswer: AQUESTION 189An engineer needs to configure network systems to detect command and control communications by decrypting ingress and egress perimeter traffic and allowing network security devices to detect malicious outbound communications. Which technology should be used to accomplish the task?A. digital certificatesB. static IP addressesC. signaturesD. cipher suiteAnswer: DQUESTION 190What is a difference between data obtained from Tap and SPAN ports?A. Tap mirrors existing traffic from specified ports, while SPAN presents more structured data for deeper analysis.B. SPAN passively splits traffic between a network device and the network without altering it, while Tap alters response times.C. SPAN improves the detection of media errors, while Tap provides direct access to traffic with lowered data visibility.D. Tap sends traffic from physical layers to the monitoring device, while SPAN provides a copy of network traffic from switch to destinationAnswer: AQUESTION 191Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?A. availabilityB. confidentialityC. scopeD. integrityAnswer: DResources 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(172-191).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!