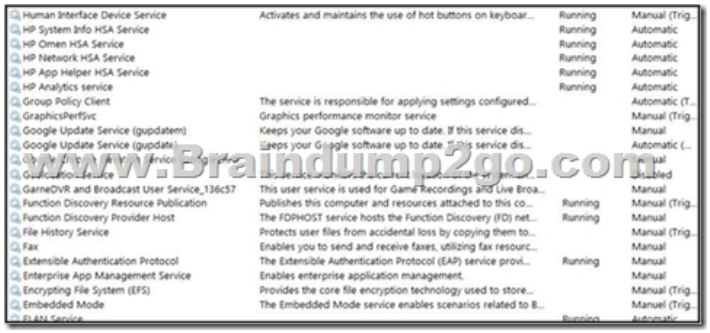
[November-2021Download Braindump2go Valid 350-201 Dumps in PDF and VCE[Q106-Q142

November/2021 Latest Braindump2go 350-201 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 350-201 Real Exam Questions!QUESTION 106An analyst wants to upload an infected file containing sensitive information to a hybrid-analysis sandbox. According to the NIST.SP 800-150 guide to cyber threat information sharing, what is the analyst required to do before uploading the file to safeguard privacy?A. Verify hash integrity.B. Remove all personally identifiable information.C. Ensure the online sandbox is GDPR compliant.D. Lock the file to prevent unauthorized access.Answer: BQUESTION 107 Refer to the exhibit. An engineer received multiple reports from employees unable to log into systems with the error: The Group Policy Client service failed to logon ?Access is denied. Through further analysis, the engineer discovered several unexpected modifications to system settings. Which type of breach is occurring?



A. malware breakB. data theftC. elevation of privilegesD. denial-of-serviceAnswer: CQUESTION 108What is needed to assess risk mitigation effectiveness in an organization?A. analysis of key performance indicatorsB. compliance with security standardsC. cost-effectiveness of control measuresD. updated list of vulnerable systemsAnswer: CQUESTION 109Refer to the exhibit. Where is the MIME type that should be followed indicated?

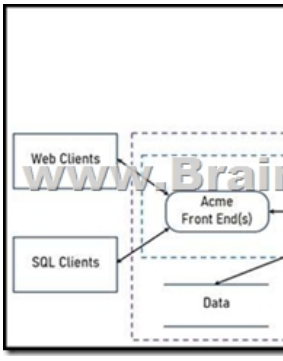
A. x-test-debugB. strict-transport-securityC. x-xss-protectionD. x-content-type-optionsAnswer: AQUESTION 110Refer to the exhibit. Based on the detected vulnerabilities, what is the next recommended mitigation step?

Severity	Name	Family
Critical	Bash Incomplete Fix Remote Code Execution Vulnerability	Gain a shell remotely
Critical	Bash Remote Code Execution (Shellshock)	Gain a shell remotely
Critical	[illegible] (CESA-2012:0465)	[illegible] Checks
Critical	Rexecd Service Detection	Service detection
High	Mozilla Foundation Unsupported Application	MacOS X Local Sec Checks
High	SMB Signing Disabled	Misc
Medium	SSL Certificate Cannot Be Trusted	General

A. Evaluate service disruption and associated risk before prioritizing patches.B. Perform root cause analysis for all detected vulnerabilities.C. Remediate all vulnerabilities with descending CVSS score order.D. Temporarily shut down unnecessary services until patch deployment ends.Answer: BQUESTION 111An engineer received an incident ticket of a malware outbreak and used antivirus and malware removal tools to eradicate the threat. The engineer notices that abnormal processes are still occurring in the system and determines that manual intervention is needed to clean the infected host and restore functionality. What is the next

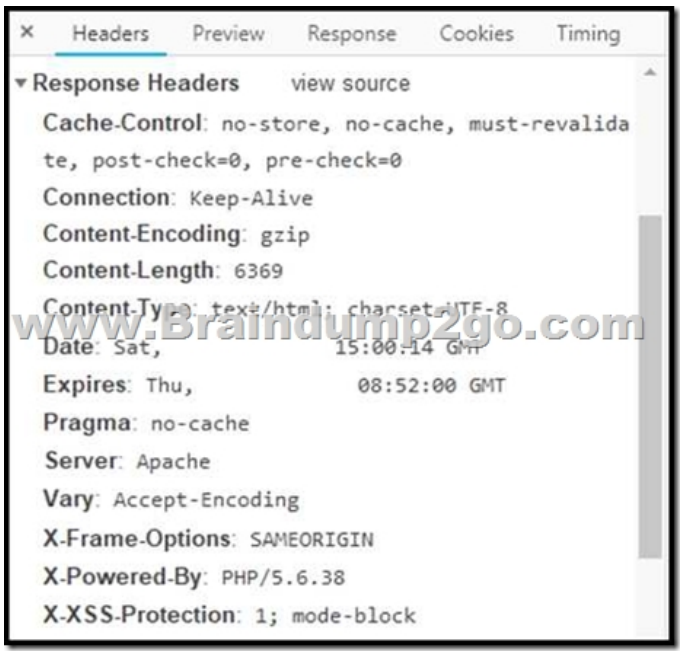
step the engineer should take to complete this playbook step?A. Scan the network to identify unknown assets and the asset owners.B. Analyze the components of the infected hosts and associated business services.C. Scan the host with updated signatures and remove temporary containment.D. Analyze the impact of the malware and contain the artifacts.Answer: BQUESTION 112The SIEM tool informs a SOC team of a suspicious file. The team initializes the analysis with an automated sandbox tool, sets up a controlled laboratory to examine the malware specimen, and proceeds with behavioral analysis. What is the next step in the malware analysis process?A. Perform static and dynamic code analysis of the specimen.B. Unpack the specimen and perform memory forensics.C. Contain the subnet in which the suspicious file was found.D. Document findings and clean-up the laboratory.Answer: BQUESTION 113A logistic company must use an outdated application located in a private VLAN during the migration to new technologies. The IPS blocked and reported an unencrypted communication. Which tuning option should be applied to IPS?A. Allow list only authorized hosts to contact the application's IP at a specific port.B. Allow list HTTP traffic through the corporate VLANS.C. Allow list traffic to application's IP from the internal network at a specific port.D. Allow list only authorized hosts to contact the application's VLAN.Answer: DQUESTION 114A company recently started accepting credit card payments in their local warehouses and is undergoing a PCI audit. Based on business requirements, the company needs to store sensitive authentication data for 45 days. How must data be stored for compliance?A. post-authorization by non-issuing entities if there is a documented business justificationB. by entities that issue the payment cards or that perform support issuing servicesC. post-authorization by non-issuing entities if the data is encrypted and securely storedD. by issuers and issuer processors if there is a legitimate reasonAnswer: CQUESTION 115A security engineer discovers that a spreadsheet containing confidential information for nine of their employees was fraudulently posted on a competitor's website. The spreadsheet contains names, salaries, and social security numbers. What is the next step the engineer should take in this investigation?A. Determine if there is internal knowledge of this incident.B. Check incoming and outgoing communications to identify spoofed emails.C. Disconnect the network from Internet access to stop the phishing threats and regain control.D. Engage the legal department to explore action against the competitor that posted the spreadsheet.Answer: DQUESTION 116An engineer notices that every Sunday night, there is a two-hour period with a large load of network activity. Upon further investigation, the engineer finds that the activity is from locations around the globe outside the organization's service areA. What are the next steps the engineer must take?B. Assign the issue to the incident handling provider because no suspicious activity has been observed during business hours.C. Review the SIEM and FirePower logs, block all traffic, and document the results of calling the call center.D. Define the access points using StealthWatch or SIEM logs, understand services being offered during the hours in Question:, and cross-correlate other source events.E. Treat it as a false positive, and accept the SIEM issue as valid to avoid alerts from triggering on weekends.Answer: AQUESTION 117An organization had an incident with the network availability during which devices unexpectedly malfunctioned. An engineer is investigating the incident and found that the memory pool buffer usage reached a peak before the malfunction. Which action should the engineer take to prevent this issue from reoccurring?A. Disable memory limit.B. Disable CPU threshold trap toward the SNMP server.C. Enable memory tracing notifications.D. Enable memory threshold notifications.Answer: DQUESTION 118A SOC analyst detected a ransomware outbreak in the organization coming from a malicious email attachment. Affected parties are notified, and the incident response team is assigned to the case. According to the NIST incident response handbook, what is the next step in handling the incident?A. Create a follow-up report based on the incident documentation.B. Perform a vulnerability assessment to find existing vulnerabilities.C. Eradicate malicious software from the infected machines.D. Collect evidence and maintain a chain-of-custody during further analysis.Answer: DQUESTION 119A security manager received an email from an anomaly detection service, that one of their contractors has downloaded 50 documents from the company's confidential document management folder using a company- owned asset al039-ice-4ce687TL0500. A security manager reviewed the content of downloaded documents and noticed that the data affected is from different departments. What are the actions a security manager should take?A. Measure confidentiality level of downloaded documents.B. Report to the incident response team.C. Escalate to contractor's manager.D. Communicate with the contractor to identify the motives.Answer: BQUESTION 120An engineer detects an intrusion event inside an organization's network and becomes aware that files that contain personal data have been accessed. Which action must be taken to contain this attack?A. Disconnect the affected server from the network.B. Analyze the source.C. Access the affected server to confirm compromised files are encrypted.D. Determine the attack surface.Answer: CQUESTION 121 The network operations center has identified malware, created a ticket within their ticketing system, and assigned the case to the SOC with high-level information. A SOC analyst was able to stop the malware from spreading and identified the attacking host. What is the next step in the incident response workflow?A. eradication and recoveryB. post-incident activityC. containmentD. detection and analysisAnswer: AQUESTION 122A SOC engineer discovers that the organization had three DDOS attacks overnight. Four servers are reported offline, even though the hardware seems to be working as expected. One of the offline servers is

affecting the pay system reporting times. Three employees, including executive management, have reported ransomware on their laptops. Which steps help the engineer understand a comprehensive overview of the incident?A. Run and evaluate a full packet capture on the workloads, review SIEM logs, and define a root cause.B. Run and evaluate a full packet capture on the workloads, review SIEM logs, and plan mitigation steps.C. Check SOAR to learn what the security systems are reporting about the overnight events, research the attacks, and plan mitigation step.D. Check SOAR to know what the security systems are reporting about the overnight events, review the threat vectors, and define a root cause.Answer: DQUESTION 123Which action should be taken when the HTTP response code 301 is received from a web application?A. Update the cached header metadata.B. Confirm the resource's location.C. Increase the allowed user limit.D. Modify the session timeout setting.Answer: AQUESTION 124 Employees receive an email from an executive within the organization that summarizes a recent security breach and requests that employees verify their credentials through a provided link. Several employees report the email as suspicious, and a security analyst is investigating the reports. Which two steps should the analyst take to begin this investigation? (Choose two.)A. Evaluate the intrusion detection system alerts to determine the threat source and attack surface.B. Communicate with employees to determine who opened the link and isolate the affected assets.C. Examine the firewall and HIPS configuration to identify the exploited vulnerabilities and apply recommended mitigation.D. Review the mail server and proxy logs to identify the impact of a potential breach.E. Check the email header to identify the sender and analyze the link in an isolated environment.Answer: CEQUESTION 125A SOC team is investigating a recent, targeted social engineering attack on multiple employees. Cross- correlated log analysis revealed that two hours before the attack, multiple assets received requests on TCP port 79. Which action should be taken by the SOC team to mitigate this attack?A. Disable BIND forwarding from the DNS server to avoid reconnaissance.B. Disable affected assets and isolate them for further investigation.C. Configure affected devices to disable NETRJS protocol.D. Configure affected devices to disable the Finger service.Answer: DQUESTION 126What is idempotence?A. the assurance of system uniformity throughout the whole delivery processB. the ability to recover from failures while keeping critical services runningC. the necessity of setting maintenance of individual deployment environmentsD. the ability to set the target environment configuration regardless of the starting stateAnswer: AQUESTION 127A security architect in an automotive factory is working on the Cyber Security Management System and is implementing procedures and creating policies to prevent attacks. Which standard must the architect apply?A. IEC62446B. IEC62443C. IEC62439-3D. IEC62439-2Answer: BQUESTION 128An organization suffered a security breach in which the attacker exploited a Netlogon Remote Protocol vulnerability for further privilege escalation. Which two actions should the incident response team take to prevent this type of attack from reoccurring? (Choose two.)A. Implement a patch management process.B. Scan the company server files for known viruses.C. Apply existing patches to the company servers.D. Automate antivirus scans of the company servers.E. Define roles and responsibilities in the incident response playbook.Answer: DEQUESTION 129Refer to the exhibit. Two types of clients are accessing the front ends and the core database that manages transactions, access control, and atomicity. What is the threat model for the SQL database?



A. An attacker can initiate a DoS attack.B. An attacker can read or change data.C. An attacker can transfer data to an external server.D. An attacker can modify the access logs.Answer: AQUESTION 130Which bash command will print all lines from the "colors.txt" file containing the non case-sensitive pattern "Yellow"?A. grep -i "yellow" colors.txtB. locate "yellow" colors.txtC. locate -i "Yellow" colors.txtD. grep "Yellow" colors.txtAnswer: AQUESTION 131An engineer received multiple reports from users trying to access a company website and instead of landing on the website, they are redirected to a malicious website that asks them to fill in sensitive personal datA. Which type of attack is occurring?B. Address Resolution Protocol poisoningC. session hijacking attackD. teardrop attackE. Domain Name System poisoningAnswer: DQUESTION 132Refer to the exhibit. An engineer is performing static analysis of a file received and reported by a user. Which risk is indicated in this STIX?

A. The file is redirecting users to a website that requests privilege escalations from the user.B. The file is redirecting users to the website that is downloading ransomware to encrypt files.C. The file is redirecting users to a website that harvests cookies and stored account information.D. The file is redirecting users to a website that is determining users' geographic location.Answer: DQUESTION 133A SOC team receives multiple alerts by a rule that detects requests to malicious URLs and informs the incident response team to block the malicious URLs requested on the firewall. Which action will improve the effectiveness of the process?A. Block local to remote HTTP/HTTPS requests on the firewall for users who triggered the rule.B. Inform the user by enabling an automated email response when the rule is triggered.C. Inform the incident response team by enabling an automated email response when the rule is triggered.D. Create an automation script for blocking URLs on the firewall when the rule is triggered.Answer: AQUESTION 134A cloud engineer needs a solution to deploy applications on a cloud without being able to manage and control the server OS. Which type of cloud environment should be used?A. IaaSB. PaaSC. DaaSD. SaaSAnswer: AQUESTION 135Engineers are working to document, list, and discover all used applications within an organization. During the regular assessment of applications from the HR backup server, an engineer discovered an unknown application. The analysis showed that the application is communicating with external addresses on a non- secure, unencrypted channel. Information gathering revealed that the unknown application does not have an owner and is not being used by a business unit. What are the next two steps the engineers should take in this investigation? (Choose two.)A. Determine the type of data stored on the affected asset, document the access logs, and engage the incident response team.B. Identify who installed the application by reviewing the logs and gather a user access log from the HR department.C. Verify user credentials on the affected asset, modify passwords, and confirm available patches and updates are installed.D. Initiate a triage meeting with department leads to determine if the application is owned internally or used by any business unit and document the asset owner.Answer: ADQUESTION 136A security incident affected an organization's critical business services, and the customer-side web API became unresponsive and crashed. An investigation revealed a spike of API call requests and a high number of inactive sessions during the incident. Which two recommendations should the engineers make to prevent similar incidents in the future? (Choose two.)A. Configure shorter timeout periods.B. Determine API rate-limiting requirements.C. Implement API key maintenance.D. Automate server-side error reporting for customers.E. Decrease simultaneous API responses.Answer: BDQUESTION 137What is the impact of hardening machine images for deployment?A. reduces the attack surfaceB. increases the speed of patch deploymentC. reduces the steps needed to mitigate threatsD. increases the availability of threat alertsAnswer: AQUESTION 138What is the difference between process orchestration and automation?A. Orchestration combines a set of automated tools, while automation is focused on the tools to automate process flows.B. Orchestration arranges the tasks, while automation arranges processes.C. Orchestration minimizes redundancies, while automation decreases the time to recover from redundancies.D. Automation optimizes the individual tasks to execute the process, while orchestration optimizes frequent and repeatable processes.Answer: AQUESTION 139An analyst received multiple alerts on the SIEM console of users that are navigating to malicious URLs. The analyst needs to automate the task of receiving alerts and processing the data for further investigations. Three variables are available from the SIEM console to include in an automation script: console_ip, api_token, and reference_set_name. What must be added to this script to receive a successful HTTP response?#!/usr/bin/python import sys import requestsA. {1}, {2}B. {1}, {3}C. console_ip, api_tokenD. console_ip, reference_set_nameAnswer: CQUESTION 140After a recent malware incident, the forensic investigator is gathering details to identify the breach and causes. The investigator has isolated the affected workstation. What is the next step that should be taken in this investigation?A. Analyze the applications and services running on the affected workstation.B. Compare workstation configuration and asset configuration policy to identify gaps.C. Inspect registry entries for recently executed files.D. Review audit logs for privilege escalation events.Answer: CQUESTION 141Refer to the exhibit. Where are the browser page rendering permissions displayed?



A. X-Frame-OptionsB. X-XSS-ProtectionC. Content-TypeD. Cache-ControlAnswer: CQUESTION 142Refer to the exhibit. Rapid Threat Containment using Cisco Secure Network Analytics (Stealthwatch) and ISE detects the threat of malware-infected 802.1x authenticated endpoints and places that endpoint into a quarantine VLAN using Adaptive Network Control policy.Which method was used to signal ISE to quarantine the endpoints?

A. SNMPB. syslogC. REST APID. pxGridAnswer: CResources From:1.2021 Latest Braindump2go 350-201 Exam Dumps (PDF & VCE) Free Share:https://www.braindump2go.com/350-201.html2.2021 Latest Braindump2go 350-201 PDF and 350-201 VCE Dumps Free Share:https://drive.google.com/drive/folders/1AxXpeiNddgUeSboJXzaOVsnt5wFFoDnO?usp=sharing3.2021 Free Braindump2go 350-201 Exam Questions Download:
https://www.braindump2go.com/free-online-pdf/350-201-Dumps(126-142).pdf
https://www.braindump2go.com/free-online-pdf/350-201-PDF-Dumps(1-20).pdf
https://www.braindump2go.com/free-online-pdf/350-201-PDF-Dumps(43-63).pdf
https://www.braindump2go.com/free-online-pdf/350-201-VCE-Dumps(21-42).pdf
https://www.braindump2go.com/free-online-pdf/350-201-VCE-Dumps(106-125).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!