[December-2020SY0-601 Exam Dumps PDF and VCE Free Download in Braindump2go[Q49-Q70

December/2020 Latest Braindump2go SY0-601 Exam Dumps with PDF and VCE Free Updated Today! Following are some new SY0-601 Real Exam Questions!QUESTION 49In which of the following situations would it be BEST to use a detective control type for mitigation?A. A company implemented a network load balancer to ensure 99.999% availability of its web application.B. A company designed a backup solution to increase the chances of restoring services in case of a natural disaster.C. A company purchased an application-level firewall to isolate traffic between the accounting department and the information technology department.D. A company purchased an IPS system, but after reviewing the requirements, the appliance was supposed to monitor, not block, any traffic.E. A company purchased liability insurance for flood protection on all capital assets.Correct Answer: DQUESTION 50The IT department's on-site developer has been with the team for many years. Each time an application is released, the security team is able to identify multiple vulnerabilities. Which of the following would BEST help the team ensure the application is ready to be released to production?A. Limit the use of third-party libraries.B. Prevent data exposure queries.C. Obfuscate the source code.D. Submit the application to QA before releasing it.Correct Answer: DQUESTION 51A cybersecurity analyst needs to implement secure authentication to third-party websites without users' passwords. Which of the following would be the BEST way to achieve this objective?A. OAuthB. SSOC. SAMLD. PAPCorrect Answer: CQUESTION 52An analyst needs to identify the applications a user was running and the files that were open before the user's computer was shut off by holding down the power button. Which of the following would MOST likely contain that information?A. NGFWB. PagefileC. NetFlowD. RAMCorrect Answer: CQUESTION 53A remote user recently took a two-week vacation abroad and brought along a corporate-owned laptop. Upon returning to work, the user has been unable to connect the laptop to the VPN. Which of the following is the MOST likely reason for the user's inability to connect the laptop to the VPN?A. Due to foreign travel, the user's laptop was isolated from the network.B. The user's laptop was quarantined because it missed the latest path update.C. The VPN client was blacklisted.D. The user's account was put on a legal hold.Correct Answer: AQUESTION 54In which of the following common use cases would steganography be employed?A. ObfuscationB. IntegrityC. Non-repudiationD. BlockchainCorrect Answer: AQUESTION 55To secure an application after a large data breach, an e-commerce site will be resetting all users' credentials. Which of the following will BEST ensure the site's users are not compromised after the reset?A. A password reuse policyB. Account lockout after three failed attemptsC. Encrypted credentials in transitD. A geofencing policy based on login historyCorrect Answer: CQUESTION 56In which of the following risk management strategies would cybersecurity insurance be used?A. TransferenceB. AvoidanceC. AcceptanceD. MitigationCorrect Answer: AQUESTION 57An organization has implemented a policy requiring the use of conductive metal lockboxes for personal electronic devices outside of a secure research lab. Which of the following did the organization determine to be the GREATEST risk to intellectual property when creating this policy?A. The theft of portable electronic devicesB. Geotagging in the metadata of imagesC. Bluesnarfing of mobile devicesD. Data exfiltration over a mobile hotspotCorrect Answer: DQUESTION 58A security analyst is using a recently released security advisory to review historical logs, looking for the specific activity that was outlined in the advisory. Which of the following is the analyst doing?A. A packet captureB. A user behavior analysisC. Threat huntingD. Credentialed vulnerability scanningCorrect Answer: CQUESTION 59Which of the following would MOST likely support the integrity of a voting machine?A. Asymmetric encryption B. BlockchainC. Transport Layer SecurityD. Perfect forward secrecyCorrect Answer: DQUESTION 60A Chief Information Security Officer (CISO) needs to create a policy set that meets international standards for data privacy and sharing. Which of the following should the CISO read and understand before writing the policies?A. PCI DSSB. GDPRC. NISTD. ISO 31000Correct Answer: BQUESTION 61The IT department at a university is concerned about professors placing servers on the university network in an attempt to bypass security controls. Which of the following BEST represents this type of threat? A. A script kiddieB. Shadow ITC. HacktivismD. White-hatCorrect Answer: BQUESTION 62A commercial cyber-threat intelligence organization observes IoCs across a variety of unrelated customers. Prior to releasing specific threat intelligence to other paid subscribers, the organization is MOST likely obligated by contracts to:A. perform attribution to specific APTs and nation-state actors.B. anonymize any PII that is observed within the IoC data.C. add metadata to track the utilization of threat intelligence reports.D. assist companies with impact assessments based on the observed data.Correct Answer: BQUESTION 63 While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?A. A RAT was installed and is transferring additional exploit tools.B. The

workstations are beaconing to a command-and-control server.C. A logic bomb was executed and is responsible for the data transfers.D. A fireless virus is spreading in the local network environment.Correct Answer: AQUESTION 64An organization is developing a plan in the event of a complete loss of critical systems and data. Which of the following plans is the organization MOST likely developing?A. Incident responseB. CommunicationsC. Disaster recoveryD. Data retentionCorrect Answer: CQUESTION 65Which of the following is the purpose of a risk register?A. To define the level or risk using probability and likelihoodB. To register the risk with the required regulatory agenciesC. To identify the risk, the risk owner, and the risk measuresD. To formally log the type of risk mitigation strategy the organization is usingCorrect Answer: CQUESTION 66A university with remote campuses, which all use different service providers, loses Internet connectivity across all locations. After a few minutes, Internet and VoIP services are restored, only to go offline again at random intervals, typically within four minutes of services being restored. Outages continue throughout the day, impacting all inbound and outbound connections and services. Services that are limited to the local LAN or WiFi network are not impacted, but all WAN and VoIP services are affected.Later that day, the edge-router manufacturer releases a CVE outlining the ability of an attacker to exploit the SIP protocol handling on devices, leading to resource exhaustion and system reloads. Which of the following BEST describe this type of attack? (Choose two.)A. DoSB. SSL strippingC. Memory leakD. Race conditionE. ShimmingF. RefactoringCorrect Answer: ADQUESTION 67A company recently set up an e-commerce portal to sell its product online. The company wants to start accepting credit cards for payment, which requires compliance with a security standard. Which of the following standards must the company comply with before accepting credit cards on its e-commerce platform?A. PCI DSSB. ISO 22301C. ISO 27001D. NIST CSFCorrect Answer: AQUESTION 68Which of the following BEST describes a security exploit for which a vendor patch is not readily available?A. Integer overflowB. Zero-dayC. End of lifeD. Race conditionCorrect Answer: BQUESTION 69The Chief Financial Officer (CFO) of an insurance company received an email from Ann, the company's Chief Executive Officer (CEO), requesting a transfer of $10,000 to an account. The email states Ann is on vacation and has lost her purse, containing cash and credit cards. Which of the following social- engineering techniques is the attacker using?A. PhishingB. WhalingC. Typo squattingD. PharmingCorrect Answer: BQUESTION 70An organization wants to implement a third factor to an existing multifactor authentication. The organization already uses a smart card and password. Which of the following would meet the organization's needs for a third factor?A. Date of birthB. FingerprintsC. PIND. TPMCorrect Answer: BResources From:1.2020 Latest Braindump2go SY0-601 Exam Dumps (PDF & VCE) Free Share:https://www.braindump2go.com/sy0-601.html2.2020 Latest Braindump2go SY0-601 PDF and SY0-601 VCE Dumps Free Share:
https://drive.google.com/drive/folders/1VvH3gDuiIKHw7Kx_vZmMM4mpCRWbTVq4?usp=sharing3.2020 Free Braindump2go SY0-601 PDF Download:https://www.braindump2go.com/free-online-pdf/SY0-601-Dumps(38-54).pdf
https://www.braindump2go.com/free-online-pdf/SY0-601-PDF(26-37).pdf
https://www.braindump2go.com/free-online-pdf/SY0-601-PDF-Dumps(1-13).pdf
https://www.braindump2go.com/free-online-pdf/SY0-601-VCE(14-25).pdf
https://www.braindump2go.com/free-online-pdf/SY0-601-VCE-Dumps(55-67).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!