[March-2022Instant Download Braindump2go SY0-601 Exam PDF and VCE SY0-601 497Q[Q540-Q569

March/2022 Latest Braindump2go SY0-601 Exam Dumps with PDF and VCE Free Updated Today! Following are some new SY0-601 Real Exam Questions!QUESTION 540A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasional disappears.The task list shows the following results

Name	CPU %
Calculator	0%
Explorer	99.7%
Notepad	0%

Which of the following is MOST likely the issue?A. RATB. PUPC. SpywareD. KeyloggerAnswer: AQUESTION 541 Which of the following attacks MOST likely occurred on the user's internal network?Name: Wikipedia.orgAddress: 208.80.154.224A. DNS poisoningB. URL redirectionC. ARP poisoningD. /etc/hosts poisoningAnswer: AQUESTION 542A company currently uses passwords for logging in to company-owned devices and wants to add a second authentication factor. Per corporate policy, users are not allowed to have smartphones at their desks. Which of the following would meet these requirements?A. Smart cardB. PIN codeC. Knowledge-based questionD. Secret keyAnswer: BQUESTION 543A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?A. Implement input validationsB. Deploy MFAC. Utilize a WAFD. Configure HIPSAnswer: CQUESTION 544Which of the following would be used to find the MOST common web-application vulnerabilities?A. OWASPB. MITRE ATTACKC. Cyber Kill ChainD. SDLCAnswer: AQUESTION 545The board of doctors at a company contracted with an insurance firm to limit the organization's liability. Which of the following risk management practices does the BEST describe?A. TransferenceB. AvoidanceC. MitigationD. AcknowledgementAnswer: AQUESTION 546Which of the following would be MOST effective to contain a rapidly attack that is affecting a large number of organizations?A. Machine learningB. DNS sinkholeC. BlocklistD. HoneypotAnswer: DQUESTION 547An analyst just discovered an ongoing attack on a host that is on the network. The analyst observes the below taking place:- The computer performance is slow- Ads are appearing from various pop-up windows- Operating system files are modified- The computer is receiving AV alerts for execution of malicious processesWhich of the following steps should the analyst consider FIRST?A. Check to make sure the DLP solution is in the active stateB. Patch the host to prevent exploitationC. Put the machine in containmentD. Update the AV solution on the host to stop the attackAnswer: CQUESTION 548Security analysts are conducting an investigation of an attack that occurred inside the organization's network. An attacker was able to connect network traffic between workstation throughout the network. The analysts review the following logs: The layer 2 address table has hundred of entries similar to the ones above.Which of the following attacks has MOST likely occurred?A. SQL injectionB. DNS spoofingC. MAC floodingD. ARP poisoningAnswer: CQUESTION 549The chief compliance officer from a bank has approved a background check policy for all new hires. Which of the following is the policy MOST likely protecting against?A. Preventing any current employees' siblings from working at the bank to prevent nepotismB. Hiring an employee who has been convicted of theft to adhere to industry complianceC. Filtering applicants who have added false information to resumes so they appear better qualifiedD. Ensuring no new hires have worked at other banks that may be trying to steal customer informationAnswer: BQUESTION 550Which biometric error would allow an unauthorized user to access a system?A. False acceptanceB. False entranceC. False rejectionD. False denialAnswer: AQUESTION 551Which of the following would produce the closet experience of responding to an actual incident response scenario?A. Lessons learnedB. SimulationC. Walk-throughD. TabletopAnswer: BQUESTION 552An organization is concerned about intellectual property theft by employee who leave the organization. Which of the following will be organization MOST likely implement?A. CBTB. NDA C. MOUD. AUPAnswer: BQUESTION 553An organization maintains several environments in which patches are developed and tested before deployed to an operation status. Which of the following is the environment in which patches will be deployed just prior to being put into an operational status?A. DevelopmentB. TestC. ProductionD. StagingAnswer: BQUESTION 554Which of the following control types would be BEST to use to identify violations and incidents?A. DetectiveB. CompensatingC. DeterrentD. CorrectiveE. RecoveryF. PreventiveAnswer: AQUESTION 555A security manager runs Nessus scans of the network after every maintenance window. Which of the following is the security manger MOST likely trying to accomplish?A. Verifying that system patching has effectively removed knows vulnerabilitiesB. Identifying assets on the network that may not exist on the network asset inventoryC. Validating the hosts do not have vulnerable ports exposed to the internetD. Checking the

status of the automated malware analysis that is being performedAnswer: AQUESTION 556A penetration tester gains access to the network by exploiting a vulnerability on a public-facing web server. Which of the following techniques will the tester most likely perform NEXT?A. Gather more information about the target through passive reconnaissanceB. Establish rules of engagement before proceedingC. Create a user account to maintain persistenceD. Move laterally throughout the network to search for sensitive informationAnswer: CQUESTION 557A news article states that a popular web browser deployed on all corporate PCs is vulnerable a zero-day attack. Which of the following MOST concern the Chief Information Security Officer about the information in the new article?A. Insider threats have compromised this networkB. Web browsing is not functional for the entire networkC. Antivirus signatures are required to be updated immediatelyD. No patches are available for the web browserAnswer: DQUESTION 558DDoS attacks are causing an overload on the cluster of cloud servers. A security architect is researching alternatives to make the cloud environment respond to load fluctuation in a cost- effective way. Which of the following options BEST fulfils the architect's requirements?A. An orchestration solution that can adjust scalability of cloud assetsB. Use of multipath by adding more connections to cloud storageC. Cloud assets replicated on geographically distributed regionsD. An on-site backup that is deployed and only used when the load increasesAnswer: AQUESTION 559Administrators have allowed employee to access their company email from personal computers. However, the administrators are concerned that these computes are another attach surface and can result in user accounts being breached by foreign actors.Which of the following actions would provide the MOST secure solution?A. Enable an option in the administration center so accounts can be locked if they are accessed from different geographical areasB. Implement a 16-character minimum length and 30-day expiration password policyC. Set up a global mail rule to disallow the forwarding of any company email to email addresses outside the organizationD. Enforce a policy that allows employees to be able to access their email only while they are connected to the internet via VPNAnswer: DQUESTION 560A security engineer needs to build a solution to satisfy regulatory requirements that state certain critical servers must be accessed using MFA. However, the critical servers are older and are unable to support the addition of MFA.Which of the following will the engineer MOST likely use to achieve this objective?A. A forward proxyB. A stateful firewallC. A jump serverD. A port tapAnswer: BQUESTION 561A security analyst wants to fingerprint a web server. Which of the following tools will the security analyst MOST likely use to accomplish this task?A. nmap -p1-65535 192.168.0.10B. dig 192.168.0.10C. curl --head http://192.168.0.10D. ping 192.168.0.10Answer: CExplanation:curl - Identify remote web serverType the command as follows:$ curl -I http://www.remote-server.com/$ curl -I http://vivekgite.com/Output:HTTP/1.1 200 OKContent-type: text/html Content-Length: 0Date: Mon, 28 Jan 2008 08:53:54 GMTServer: lighttpdQUESTION 562Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?A. GDPRB. PCI DSSC. ISO 27000D. NIST 800-53Answer: DExplanation:NIST Special Publication 800-53 provides a catalog of security and privacy controls for all U.S. federal information systems except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce.QUESTION 563An information security policy stales that separation of duties is required for all highly sensitive database changes that involve customers' financial data. Which of the following will this be BEST to prevent?A. Least privilegeB. An insider threatC. A data breachD. A change control violationAnswer: BExplanation:Separation of duties - is a means of establishing checks and balances against the possibility that critical system or procedures can be compromised by insider threats. Duties and responsibilities should be divided among individuals to prevent ethical conflicts or abuse of powers.QUESTION 564A security analyst receives an alert from the company's SIEM that anomalous activity is coming from a local source IP address of 192.168.34.26. The Chief Information Security Officer asks the analyst to block the originating source. Several days later another employee opens an internal ticket stating that vulnerability scans are no longer being performed properly. The IP address the employee provides is 192.168.34.26. Which of the following describes this type of alert?A. True positiveB. True negativeC. False positiveD. False negativeAnswer: C Explanation:Traditional SIEM Log AnalysisTraditionally, the SIEM used two techniques to generate alerts from log data: correlation rules, specifying a sequence of events that indicates an anomaly, which could represent a security threat, vulnerability or active security incident; and vulnerabilities and risk assessment, which involves scanning networks for known attack patterns and vulnerabilities. The drawback of these older techniques is that they generate a lot of false positives, and are not successful at detecting new and unexpected event typesQUESTION 565Hackers recently attacked a company's network and obtained several unfavorable pictures from the Chief Executive Officer's workstation. The hackers are threatening to send the images to the press if a ransom is not paid. Which of the following is impacted the MOST?A. Identify theftB. Data lossC. Data exfiltrationD. ReputationAnswer: CExplanation:Data exfiltration occurs when malware and/or a malicious actor carries out an unauthorized data transfer from a computer. It is also commonly called data extrusion or data exportation. Data exfiltration is also considered a form of data theft.QUESTION 566A software company is analyzing a process that detects software vulnerabilities at the earliest stage

possible. The goal is to scan the source looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. Which of the following would BEST assist the company with this objective?A. Use fuzzing testingB. Use a web vulnerability scannerC. Use static code analysisD. Use a penetration-testing OSAnswer: CExplanation:FuzzingFuzzing or fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes, failing built-in code assertions, or potential memory leaks.Static program analysisStatic program analysis is the analysis of computer software performed without executing any programs, in contrast with dynamic analysis, which is performed on programs during their execution.What is static code analysis? Static code analysis is a method of debugging by examining source code before a program is run. It's done by analyzing a set of code against a set (or multiple sets) of coding rules. ... This type of analysis addresses weaknesses in source code that might lead to vulnerabilities.Penetration testA penetration test, colloquially known as a pen test or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system; this is not to be confused with a vulnerability assessment.QUESTION 567A company is providing security awareness training regarding the importance of not forwarding social media messages from unverified sources. Which of the following risks would this training help to prevent?A. HoaxesB. SPIMs C. Identity fraudD. Credential harvestingAnswer: DExplanation:HoaxA hoax is a falsehood deliberately fabricated to masquerade as the truth. It is distinguishable from errors in observation or judgment, rumors, urban legends, pseudo sciences, and April Fools' Day events that are passed along in good faith by believers or as jokes.Identity theftIdentity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The term identity theft was coined in 1964. Identity fraud (also known as identity theft or crime) involves someone using another individual's personal information without consent, often to obtain a benefit.Credential HarvestingCredential Harvesting (or Account Harvesting) is the use of MITM attacks, DNS poisoning, phishing, and other vectors to amass large numbers of credentials (username / password combinations) for reuse.QUESTION 568A penetration tester was able to compromise an internal server and is now trying to pivot the current session in a network lateral movement. Which of the following tools, if available on the server, will provide the MOST useful information for the next assessment step?A. AutopsyB. CuckooC. MemdumpD. NmapAnswer: DExplanation:MemdumpA display or printout of all or selected contents of RAM. After a program abends (crashes), a memory dump is taken in order to analyze the status of the program. The programmer looks into the memory buffers to see which data items were being worked on at the time of failure.NmapNmap is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.QUESTION 569A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?A. Add a deny-all rule to that host in the network ACLB. Implement a network-wide scan for other instances of the malware.C. Quarantine the host from other parts of the networkD. Revoke the client's network access certificatesAnswer: BExplanation:What is Malware? Malware, short for "malicious software," refers to any intrusive software developed by cybercriminals (often called "hackers") to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. Recent malware attacks have exfiltrated data in mass amounts.How do I protect my network against malware?Typically, businesses focus on preventative tools to stop breaches. By securing the perimeter, businesses assume they are safe. Some advanced malware, however, will eventually make their way into your network. As a result, it is crucial to deploy technologies that continually monitor and detect malware that has evaded perimeter defenses. Sufficient advanced malware protection requires multiple layers of safeguards along with high-level network visibility and intelligence.How do I detect and respond to malware?Malware will inevitably penetrate your network. You must have defenses that provide significant visibility and breach detection. In order to remove malware, you must be able to identify malicious actors quickly. This requires constant network scanning. Once the threat is identified, you must remove the malware from your network. Today's antivirus products are not enough to protect against advanced cyber threats. Learn how to update your antivirus strategy.Resources From:1.2022 Latest Braindump2go SY0-601 Exam Dumps (PDF & VCE) Free Share:https://www.braindump2go.com/sy0-601.html2.2022 Latest Braindump2go SY0-601 PDF and SY0-601 VCE Dumps Free Share: https://drive.google.com/drive/folders/1VvH3gDuiIKHw7Kx_vZmMM4mpCRWbTVq4?usp=sharing3.2021 Free Braindump2go SY0-601 Exam Questions Download:https://www.braindump2go.com/free-online-pdf/SY0-601-PDF-Dumps(520-545).pdf https://www.braindump2go.com/free-online-pdf/SY0-601-VCE-Dumps(546-569).pdfFree Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!