[Dec/2020 Updated PassLeader Valid 120q Security+ SY0-601 Exam Dumps with New Added Questions and Answers

New Updated SY0-601 Exam Questions from PassLeader SY0-601 PDF dumps! Welcome to download the newest PassLeader SY0-601 VCE dumps: https://www.passleader.com/sy0-601.html (120 Q&As) Keywords: SY0-601 exam dumps, SY0-601 exam questions, SY0-601 VCE dumps, SY0-601 PDF dumps, SY0-601 practice tests, SY0-601 study guide, SY0-601 braindumps, CompTIA Security+ Exam P.S. New SY0-601 dumps PDF: https://drive.google.com/drive/folders/1sL-8ZFvw64qUe6RBi7t0rJ9DZRNu88tJ NEW QUESTION 1 On which of the following is the live acquisition of data for forensic analysis MOST dependent? (Choose two.) A.   Data accessibility. B.   Value and volatility of data. C.   Cryptographic or hash algorithm. D.   Data retention legislation. E.   Legal hold. F.   Right-to-audit clauses. Answer: BF NEW QUESTION 2 Which of the following incident response steps involves actions to protect critical systems while maintaining business operations? A.   Investigation B.   Containment C.   Recovery D.   Lessons learned Answer: B NEW QUESTION 3 A network engineer needs to build a solution that will allow guests at the company's headquarters to access the Internet via WiFi. This solution should not allow access to the internal corporate network, but it should require guests to sign off on the acceptable use policy before accessing the Internet. Which of the following should the engineer employ to meet these requirements? A.   Implement open PSK on the APs. B.   Deploy a WAF. C.   Configure WIPS on the APs. D.   Install a captive portal. Answer: D NEW QUESTION 4 Which of the following cloud models provides clients with servers, storage, and networks but nothing else? A.   SaaS B.   PaaS C.   IaaS D.   DaaS Answer: C NEW QUESTION 5 A network administrator needs to build out a new datacenter, with a focus on resiliency and uptime. Which of the following would BEST meet this objective? (Choose two.) A.   Dual power supply. B.   Off-site backups. C.   Automatic OS upgrades. D.   NIC teaming. E.   Scheduled penetration testing. F.   Network-attached storage. Answer: AB NEW QUESTION 6 An organization is developing an authentication service for use at the entry and exit ports of country borders. The service will use data feeds obtained from passport systems, passenger manifests, and high- definition video feeds from CCTV systems that are located at the ports. The service will incorporate machine-learning techniques to eliminate biometric enrollment processes while still allowing authorities to identify passengers with increasing accuracy over time. The more frequently passengers travel, the more accurately the service will identify them. Which of the following biometrics will MOST likely be used, without the need for enrollment? (Choose two.) A.   Voice B.   Gait C.   Vein D.   Facial E.   Retina F.   Fingerprint Answer: BD NEW QUESTION 7 After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review? A.   The vulnerability scan output. B.   The IDS logs. C.   The full packet capture data. D.   The SIEM alerts. Answer: A NEW QUESTION 8 An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state? A.   The system was configured with weak default security settings. B.   The device uses weak encryption ciphers. C.   The vendor has not supplied a patch for the appliance. D.   The appliance requires administrative credentials for the assessment. Answer: C NEW QUESTION 9 A pharmaceutical sales representative logs on to a laptop and connects to the public WiFi to check emails and update reports. Which of the following would be BEST to prevent other devices on the network from directly accessing the laptop? (Choose two.) A.   Trusted Platform Module B.   A VPN C.   A DLP solution D.   Full disk encryption E.   A host-based firewall F.   Antivirus software Answer: AE NEW QUESTION 10 The CSIRT is reviewing the lessons learned from a recent incident. A worm was able to spread unhindered throughout the network and infect a large number of computers and servers. Which of the following recommendations would be BEST to mitigate the impacts of a similar incident in the future? A.   Install a NIDS device at the boundary. B.   Segment the network with firewalls. C.   Update all antivirus signatures daily. D.   Implement application

blacklisting. Answer: B NEW QUESTION 11 A cybersecurity administrator needs to add disk redundancy for a critical server. The solution must have a two-drive failure for better fault tolerance. Which of the following RAID levels should the administrator select? A.   0 B.   1 C.   5 D.   6 Answer: B NEW QUESTION 12 A small company that does not have security staff wants to improve its security posture. Which of the following would BEST assist the company? A.   MSSP B.   PaaS C.   IaaS D.   SOAR Answer: D NEW QUESTION 13 A cybersecurity manager has scheduled biannual meetings with the IT team and department leaders to discuss how they would respond to hypothetical cyberattacks. During these meetings, the manager presents a scenario and injects additional information throughout the session to replicate what might occur in a dynamic cybersecurity event involving the company, its facilities, its data, and its staff. Which of the following describes what the manager is doing? A.   Developing an incident response plan. B.   Building a disaster recovery plan. C.   Conducting a tabletop exercise. D.   Running a simulation exercise. Answer: C NEW QUESTION 14 A network administrator has been asked to install an IDS to improve the security posture of an organization. Which of the following control types is an IDS? A.   Detective B.   Physical C.   Corrective D.   Administrative Answer: A NEW QUESTION 15 A startup company is using multiple SaaS and IaaS platforms to stand up a corporate infrastructure and build out a customer-facing web application. Which of the following solutions would be BEST to provide security, manageability, and visibility into the platforms? A.   SIEM B.   DLP C.   SWG D.   CASB Answer: D NEW QUESTION 16 ?? NEW QUESTION 106 A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions? A.   Nmap B.   Wireshark C.   Autopsy D.   DNSEnum Answer: A NEW QUESTION 107 An organization with a low tolerance for user inconvenience wants to protect laptop hard drives against loss or data theft. Which of the following would be the MOST acceptable? A.   SED B.   HSM C.   DLP D.   TPM Answer: A NEW QUESTION 108 A 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.   OAuth B.   SSO C.   SAML D.   PAP Answer: C NEW QUESTION 109 In which of the following risk management strategies would cybersecurity insurance be used? A.   Avoidance B.   Transference C.   Acceptance D.   Mitigation Answer: B NEW QUESTION 110 An 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 response B.   Communications C.   Data retention D.   Disaster recovery Answer: D NEW QUESTION 111 Which of the following is the purpose of a risk register? A.   To define the level or risk using probability and likelihood. B.   To register the risk with the required regulatory agencies. C.   To identify the risk, the risk owner, and the risk measures. D.   To formally log the type of risk mitigation strategy the organization is using. Answer: C NEW QUESTION 112 Which of the following BEST describes a security exploit for which a vendor patch is not readily available? A.   Integer overflow B.   Zero-day C.   End of life D.   Race condition Answer: B NEW QUESTION 113 A company processes highly sensitive data and senior management wants to protect the sensitive data by utilizing classification labels. Which of the following access control schemes would be BEST for the company to implement? A.   Discretionary B.   Rule-based C.   Role-based D.   Mandatory Answer: D NEW QUESTION 114 ?? Download the newest PassLeader SY0-601 dumps from passleader.com now! 100% Pass Guarantee! SY0-601 PDF dumps & SY0-601 VCE dumps: https://www.passleader.com/sy0-601.html (120 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. New SY0-601 dumps PDF: https://drive.google.com/drive/folders/1sL-8ZFvw64qUe6RBi7t0rJ9DZRNu88tJ