[24/July/2019 Updated PassLeader 373q CS0-001 Exam VCE Dumps For Free Share

New Updated CS0-001 Exam Questions from PassLeader CS0-001 PDF dumps! Welcome to download the newest PassLeader CS0-001 VCE dumps: https://www.passleader.com/cs0-001.html (373 Q&As) Keywords: CS0-001 exam dumps, CS0-001 exam questions, CS0-001 VCE dumps, CS0-001 PDF dumps, CS0-001 practice tests, CS0-001 study guide, CS0-001 braindumps, CompTIA Cybersecurity Analyst (CSA+) Exam P.S. New CS0-001 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpaXd6TXJ4T3ItSDQ NEW QUESTION 349 Joe, a user, is unable to launch an application on his laptop, which he typically uses on a daily basis. Joe informs a security analyst of the issue. After an online database comparison, the security analyst checks the SIEM and notices alerts indicating certain .txt and .dll files are blocked. Which of the following tools would generate these logs? A.   Antivirus B.   HIPS C.   Firewall D.   Proxy Answer: C NEW QUESTION 350 Employees at a manufacturing plant have been victims of spear phishing, but security solutions prevented further intrusions into the network. Which of the following is the MOST appropriate solution in this scenario? A.   Continue to monitor security devices. B.   Update antivirus and malware definitions. C.   Provide security awareness training. D.   Migrate email services to a hosted environment. Answer: C NEW QUESTION 351 A new security manager was hired to establish a vulnerability management program. The manager asked for a corporate strategic plan and risk register that the project management office developed. The manager conducted a tools and skill sets inventory to document the plan. Which of the following is a critical task for the establishment of a successful program? A.   Establish continuous monitoring. B.   Update vulnerability feed. C.   Perform information classification. D.   Establish corporate policy. Answer: D NEW QUESTION 352 Malicious users utilized brute force to access a system. An analyst is investigating these attacks and recommends methods to management that would help secure the system. Which of the following controls should the analyst recommend? (Choose three.) A.   Multifactor authentication B.   Network segmentation C.   Single sign-on D.   Encryption E.   Complexity policy F.   Biometrics G.   Obfuscation Answer: AEF NEW QUESTION 353 A cyber-incident response team is responding to a network intrusion incident on a hospital network. Which of the following must the team prepare to allow the data to be used in court as evidence? A.   Computer forensics form B.   HIPAA response form C.   Chain of custody form D.   Incident form Answer: B NEW QUESTION 354 A user received an invalid password response when trying to change the password. Which of the following policies could explain why the password is invalid? A.   Access control policy B.   Account management policy C.   Password policy D.   Data ownership policy Answer: C NEW QUESTION 355 A corporation has implemented an 802.1X wireless network using self-signed certificates. Which of the following represents a risk to wireless users? A.   Buffer overflow attacks B.   Cross-site scripting attacks C.   Man-in-the-middle attacks D.   Denial of service attacks Answer: C NEW QUESTION 356 Which of the following command line utilities would an analyst use on an end-user PC to determine the ports it is listening on? A.   tracert B.   ping C.   nslookup D.   netstat Answer: D NEW QUESTION 357 During a quarterly review of user accounts and activity, a security analyst noticed that after a password reset the head of human resources has been logging in from multiple locations, including several overseas. Further review of the account showed access rights to a number of corporate applications, including a sensitive accounting application used for employee bonuses. Which of the following security methods could be used to mitigate this risk? A.   RADIUS identity management B.   Context-based authentication C.   Privilege escalation restrictions D.   Elimination of self-service password resets Answer: B NEW QUESTION 358 The human resources division is moving all of its applications to an IaaS cloud. The Chief Information Officer (CIO) has asked the security architect to design the environment securely to prevent the IaaS provider from accessing its data-at-rest and data-in-transit within the infrastructure. Which of the following security controls should the security architect recommend? A.   Implement a non-data breach agreement. B.   Ensure all backups are remote outside the control of the IaaS provider. C.   Ensure all of the IaaS provider's workforce passes stringent background checks. D.   Render data unreadable through the use of appropriate tools and techniques. Answer: D NEW QUESTION 359 A threat intelligence analyst who is working on the SOC floor has been forwarded

an email that was sent to one of the executives in business development. The executive mentions the email was from the Chief Executive Officer (CEO), who was requesting an emergency wire transfer. This request was unprecedented. Which of the following threats MOST accurately aligns with this behavior? A.   Phishing B.   Whaling C.   Spam D.   Ransomware Answer: B NEW QUESTION 360 The security team has determined that the current incident response resources cannot meet management's objective to secure a forensic image for all serious security incidents within 24 hours. Which of the following compensating controls can be used to help meet management's expectations? A.   Separation of duties B.   Scheduled reviews C.   Dual control D.   Outsourcing Answer: D NEW QUESTION 361 Which of the following describes why it is important for an organization's incident response team and legal department to meet and discuss communication processes during the incident response process? A.   To comply with existing organization policies and procedures on interacting with internal and external parties. B.   To ensure all parties know their roles and effective lines of communication are established. C.   To identify which group will communicate details to law enforcement in the event of a security incident. D.   To predetermine what details should or should not be shared with internal or external parties in the event of an incident. Answer: A NEW QUESTION 362 The Chief Information Security Officer (CISO) has decided that all accounts with elevated privileges must use a longer, more complicated passphrase instead of a password. The CISO would like to formally document management's intent to set this control level. Which of the following is the appropriate means to achieve this? A.   A control B.   A standard C.   A policy D.   A guideline Answer: C NEW QUESTION 363 During a physical penetration test at a client site, a local law enforcement officer stumbled upon the test questioned the legitimacy of the team. Which of the following information should be shown to the officer? A.   Letter of engagement B.   Scope of work C.   Timing information D.   Team reporting Answer: A NEW QUESTION 364 A security analyst is performing a stealth black-box audit of the local WiFi network and is running a wireless sniffer to capture local WiFi network traffic from a specific wireless access point. The SSID is not appearing in the sniffing logs of the local wireless network traffic. Which of the following is the best action that should be performed NEXT to determine the SSID? A.   Set up a fake wireless access point. B.   Power down the wireless access point. C.   Deauthorize users of that access point. D.   Spoof the MAC addresses of adjacent access points. Answer: A NEW QUESTION 365 An analyst is detecting Linux machines on a Windows network. Which of the following tools should be used to detect a computer operating system? A.   whois B.   netstat C.   nmap D.   nslookup Answer: C NEW QUESTION 366 A security analyst has performed various scans and found vulnerabilities in several applications that affect production data. Remediation of all exploits may cause certain applications to no longer work. Which of the following activities would need to be conducted BEFORE remediation? A.   Fuzzing B.   Input validation C.   Change control D.   Sandboxing Answer: C NEW QUESTION 367 A cybersecurity analyst is investigating an incident report concerning a specific user workstation. The workstation is exhibiting high CPU and memory usage, even when first started, and network bandwidth usage is extremely high. The user reports that applications crash frequently, despite the fact that no significant changes in work habits have occurred. An antivirus scan reports no known threats. Which of the following is the MOST likely reason for this? A.   Advanced persistent threat B.   Zero day C.   Trojan D.   Logic bomb Answer: B NEW QUESTION 368 During a tabletop exercise, it is determined that a security analyst is required to ensure patching and scan reports are available during an incident, as well as documentation of all critical systems. To which of the following stakeholders should the analyst provide the reports? A.   Management B.   Affected vendors C.   Security operations D.   Legal Answer: A NEW QUESTION 369 Which of the following is a vulnerability that is specific to hypervisors? A.   DDoS B.   VLAN hopping C.   Weak encryption D.   WMescape Answer: D NEW QUESTION 370 During a red team engagement, a penetration tester found a production server. Which of the following portions of the SOW should be referenced to see if the server should be part of the testing engagement? A.   Authorization B.   Exploitation C.   Communication D.   Scope Answer: D NEW QUESTION 371 The IT department at a growing law firm wants to begin using a third-party vendor for vulnerability monitoring and mitigation. The executive director of the law firm wishes to outline the assumptions and expectations between the two companies. Which of the following documents might be referenced in the event of a security breach at the law firm?

A.   SLA B.   MOU C.   SOW D.   NDA Answer: A NEW QUESTION 372 ..... Download the newest PassLeader CS0-001 dumps from passleader.com now! 100% Pass Guarantee! CS0-001 PDF dumps & CS0-001 VCE dumps: https://www.passleader.com/cs0-001.html (373 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. New CS0-001 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpaXd6TXJ4T3ItSDQ