Free Download Latest 2014 Pass4sure&Lead2pass CompTIA SY0-401 Dumps (51-60)

QUESTION 51 A security administrator is reviewing the company's continuity plan. The plan specifies an RTO of six hours and RPO of two days. Which of the following is the plan describing? A.   Systems should be restored within six hours and no later than two days after the incident. B.   Systems should be restored within two days and should remain operational for at least six hours. C.   Systems should be restored within six hours with a minimum of two days worth of data. D.   Systems should be restored within two days with a minimum of six hours worth of data. Answer: C QUESTION 52 The incident response team has received the following email message. From: monitor@ext-company.com To: security@company.com Subject: Copyright infringement A copyright infringement alert was triggered by IP address 13.10.66.5 at 09: 50: 01 GMT. After reviewing the following web logs for IP 13.10.66.5, the team is unable to correlate and identify the incident. 09: 45: 33 13.10.66.5 http: //remote.site.com/login.asp?user=john 09: 50: 22 13.10.66.5 http: //remote.site.com/logout.asp?user=anne 10: 50: 01 13.10.66.5 http: //remote.site.com/access.asp?file=movie.mov 11: 02: 45 13.10.65.5 http: //remote.site.com/download.asp?movie.mov=ok Which of the following is the MOST likely reason why the incident response team is unable to identify and correlate the incident? A.   The logs are corrupt and no longer forensically sound. B.   Traffic logs for the incident are unavailable. C.   Chain of custody was not properly maintained. D.   Incident time offsets were not accounted for. Answer: D QUESTION 53 A server dedicated to the storage and processing of sensitive information was compromised with a rootkit and sensitive data was exfiltrated. Which of the following incident response procedures is best suited to restore the server? A.   Wipe the storage, reinstall the OS from original media and restore the data from the last known good backup. B.   Keep the data partition, restore the OS from the most current backup and run a full system antivirus scan. C.   Format the storage and reinstall both the OS and the data from the most current backup. D.   Erase the storage, reinstall the OS from most current backup and only restore the data that was not compromised. Answer: A QUESTION 54 Which of the following describes a type of malware which is difficult to reverse engineer in a virtual lab? A.   Armored virus B.   Polymorphic malware C.   Logic bomb D.   Rootkit Answer: A QUESTION 55 Using a heuristic system to detect an anomaly in a computer's baseline, a system administrator was able to detect an attack even though the company signature based IDS and antivirus did not detect it. Further analysis revealed that the attacker had downloaded an executable file onto the company PC from the USB port, and executed it to trigger a privilege escalation flaw. Which of the following attacks has MOST likely occurred? A.   Cookie stealing B.   Zero-day C.   Directory traversal D.   XML injection Answer: B QUESTION 56 After copying a sensitive document from his desktop to a flash drive, Joe, a user, realizes that the document is no longer encrypted. Which of the following can a security technician implement to ensure that documents stored on Joe's desktop remain encrypted when moved to external media or other network based storage? A.   Whole disk encryption B.   Removable disk encryption C.   Database record level encryption D.   File level encryption Answer: D QUESTION 57 A security administrator must implement a system to allow clients to securely negotiate encryption keys with the company's server over a public unencrypted communication channel. Which of the following implements the required secure key negotiation? (Select TWO). A.   PBKDF2 B.   Symmetric encryption C.   Steganography D.   ECDHE E.   Diffie-Hellman Answer: DE QUESTION 58 Acme Corp has selectively outsourced proprietary business processes to ABC Services. Due to some technical issues, ABC services wants to send some of Acme Corp's debug data to a third party vendor for problem resolution. Which of the following MUST be considered prior to sending data to a third party? A.   The data should be encrypted prior to transport B.   This would not constitute unauthorized data sharing C.   This may violate data ownership and non-disclosure agreements D.   Acme Corp should send the data to ABC Services' vendor instead Answer: C QUESTION 59 An organization has introduced token-based authentication to system administrators due to risk of password compromise. The tokens have a set of numbers that automatically change every 30 seconds. Which of the following type of authentication mechanism is this? A.   TOTP B.   Smart card C.   CHAP D.   HOTP Answer: A QUESTION 60 A security technician at a small business is worried about the Layer 2 switches in the network suffering from a DoS style attack caused by staff incorrectly cabling network connections between switches. Which of the following will BEST mitigate the risk if implemented on

the switches? A.   Spanning tree B.   Flood guards C.   Access control lists D.   Syn flood Answer: A If you want to pass CompTIA SY0-401 successfully, donot missing to read latest lead2pass CompTIA SY0-401 exam questions. If you can master all lead2pass questions you will able to pass 100% guaranteed. http://www.lead2pass.com/SY0-401.html