[Nov-2017 Dumps Collection of SY0-501 Exam Questions With Free VCE and PDF Download (Section B)

New Updated SY0-501 Exam Questions from PassLeader SY0-501 PDF dumps! Welcome to download the newest PassLeader SY0-501 VCE dumps: https://www.passleader.com/sy0-501.html (166 Q&As) Keywords: SY0-501 exam dumps, SY0-501 exam questions, SY0-501 VCE dumps, SY0-501 PDF dumps, SY0-501 practice tests, SY0-501 study guide, SY0-501 braindumps, CompTIA Security+ Exam P.S. New SY0-501 dumps PDF: https://drive.google.com/open?id=1Ei1CtZKTLawI_2jpkecHaVbM_kXPMZAu >> New SY0-401 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpcG9CWHp3bXlNTTg QUESTION 31Which of the following characteristics differentiate a rainbow table attack from a brute force attack? (Select TWO.) A. Rainbow table attacks greatly reduce compute cycles at attack time.B. Rainbow tables must include precompiled hashes.C. Rainbow table attacks do not require access to hashed passwords.D. Rainbow table attacks must be performed on the network.E. Rainbow table attacks bypass maximum failed login restrictions. Answer: BD QUESTION 32Which of the following BEST describes a routine in which semicolons, dashes, quotes, and commas are removed from a string? A. Error handling to protect against program exploitationB. Exception handling to protect against XSRF attacksC. Input validation to protect against SQL injectionD. Padding to protect against string buffer overflows Answer: C QUESTION 33Which of the following is an important step to take BEFORE moving any installation packages from a test environment to production? A. Verify the hashes of filesB. Archive and compress the filesC. Update the secure baseline Answer: A QUESTION 34Which of the following cryptographic attacks would salting of passwords render ineffective? A. DictionaryB. Rainbow tablesC. Birthday Answer: A QUESTION 35A network administrator wants to implement a method of securing internal routing. Which of the following should the administrator implement? A. DMZB. NATC. VPND. PAT Answer: A QUESTION 36Which of the following types of keys is found in a key escrow? A. PublicB. PrivateC. SharedD. Session Answer: B QUESTION 37A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours. Which of the following types of malware is MOST likely causing this issue? A. BotnetB. RansomwareC. Polymorphic malwareD. Armored virus Answer: A QUESTION 38A company is currently using the following configuration:* IAS server with certificate-based EAP-PEAP and MSCHAP.* Unencrypted authentication via PAP.A security administrator needs to configure a new wireless setup with the following configurations:* PAP authentication method.* PEAP and EAP provide two-factor authentication.Which of the following forms of authentication are being used? (Select TWO.) A. PAPB. PEAPC. MSCHAPD. PEAP-MSCHAPE. EAPF. EAP-PEAP Answer: EF QUESTION 39A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate? A. It can protect multiple domainsB. It provides extended site validationC. It does not require a trusted certificate authorityD. It protects unlimited subdomains Answer: B QUESTION 40After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition. Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Select TWO.) A. Monitor VPN client accessB. Reduce failed login out settingsC. Develop and implement updated access control policiesD. Review and address invalid login attemptsE. Increase password complexity requirementsF. Assess and eliminate inactive accounts Answer: CF QUESTION 41A new mobile application is being developed in-house. Security reviews did not pick up any major flaws, however vulnerability scanning results show fundamental issues at the very end of the project cycle. Which of the following security activities should also have been performed to discover vulnerabilities earlier in the lifecycle? A. Architecture reviewB. Risk assessmentC. Protocol analysisD. Code review Answer: D QUESTION 42A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts. Which of the following subnets would BEST meet the requirements? A. 192.168.0.16255.25.255.248B. 192.168.0.16/28C. 192.168.1.50255.255.25.240D. 192.168.2.32/27 Answer: B QUESTION 43 A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have cause many executives in the company to travel with mini tablet devices instead of laptops. These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network. Which of the following should be implemented in order to meet the security policy requirements? A. Virtual Desktop Infrastructure (VDI)B. WS-security and geo-fencingC. A Hardware Security Module (HSM)D. RFID tagging systemE. MDM softwareF. Security Requirements Traceability Matrix (SRTM) Answer: E QUESTION 44The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers

with the PIN. Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data? A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted.B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance.C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files.D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share. Answer: C QUESTION 45A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network. Which of the following security measures did the technician MOST likely implement to cause this scenario? A. Deactivation of SSID broadcastB. Reduction of WAP signal output powerC. Activation of 802.1X with RADIUSD. Implementation of MAC filteringE. Beacon interval was decreased Answer: A QUESTION 46A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production. Which of the following would correct the deficiencies? A. Mandatory access controlsB. Disable remote loginC. Host hardeningD. Disabling services Answer: C QUESTION 47Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field. Which of the following has the application programmer failed to implement? A. Revision control systemB. Client side exception handlingC. Server side validationD. Server hardening Answer: C QUESTION 48An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware the attacker is provided with access to the infected machine. Which of the following is being described? A. Zero-day exploitB. Remote code executionC. Session hijackingD. Command injection Answer: A QUESTION 49A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine. Which of the following can be implemented to reduce the likelihood of this attack going undetected? A. Password complexity rulesB. Continuous monitoringC. User access reviewsD. Account lockout policies Answer: B QUESTION 50A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening. In order to implement a true separation of duties approach the bank could do what? A. Require the use of two different passwords held by two different individuals to open an account.B. Administer account creation on a role based access control approach.C. Require all new accounts to be handled by someone else other than a teller since they have different duties.D. Administer account creation on a rule based access control approach. Answer: C QUESTION 51A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day. Which of the following could the security administrator implement to reduce the risk associated with the finding? A. Implement a clean desk policyB. Security training to prevent shoulder surfingC. Enable group policy based screensaver timeoutsD. Install privacy screens on monitors Answer: C QUESTION 52Company policy requires the use if passphrases instead if passwords. Which of the following technical controls MUST be in place in order to promote the use of passphrases? A. ReuseB. LengthC. HistoryD. Complexity Answer: D QUESTION 53During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could best prevent this from occurring again? A. Credential managementB. Group policy managementC. Acceptable use policyD. Account expiration policy Answer: B QUESTION 54Which of the following should identify critical systems and components? A. MOUB. BPAC. ITCPD. BCP Answer: D QUESTION 55Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met? A. Logic bombB. TrojanC. ScarewareD. Ransomware Answer: A QUESTION 56A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account. This is an example of which of the following attacks? A. SQL injectionB. Header manipulationC. Cross-site scriptingD. Flash cookie exploitation Answer: C QUESTION 57Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures. Which of the following should be implemented to correct this issue? A. Decrease the room temperatureB. Increase humidity in the roomC. Utilize

better hot/cold aisle configurationsD. Implement EMI shielding Answer: B QUESTION 58A portable data storage device has been determined to have malicious firmware. Which of the following is the BEST course of action to ensure data confidentiality? A. Format the deviceB. Re-image the deviceC. Perform virus scan in the deviceD. Physically destroy the device Answer: C QUESTION 59A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable. Which of the following MUST be implemented to support this requirement? A. CSRB. OCSPC. CRLD. SSH Answer: C QUESTION 60A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients. Which of the following is being used? A. Gray box vulnerability testingB. Passive scanC. Credentialed scanD. Bypassing security controls Answer: A Download the newest PassLeader SY0-501 dumps from passleader.com now! 100% Pass Guarantee! SY0-501 PDF dumps & SY0-501 VCE dumps: https://www.passleader.com/sy0-501.html (166 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) P.S. New SY0-501 dumps PDF: https://drive.google.com/open?id=1Ei1CtZKTLawI_2jpkecHaVbM_kXPMZAu >> New SY0-401 dumps PDF: https://drive.google.com/open?id=0B-ob6L_QjGLpcG9CWHp3bXlNTTg