[Lead2pass New New Lead2pass CompTIA SY0-401 New Questions Free Download (751-775)

Took the SY0-401 exams yesterday and scored 9xx. Lead2pass SY0-401 exam dumps are valid. Almost all of the multiple choice came out. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 751Which of the following protocols provides transport security for virtual terminal emulation? A. TLSB. SSHC. SCPD. S/MIMEAnswer: BExplanation:Secure Shell (SSH) is a tunneling protocol originally designed for Unix systems. It uses encryption to establish a secure connection between two systems. SSH also provides alternative, security- equivalent programs for such Unix standards as Telnet, FTP, and many other communications- oriented applications. SSH is available for use on Windows systems as well. This makes it the preferred method of security for Telnet and other cleartext oriented programs in the Unix environment. QUESTION 752A security engineer is asked by the company's development team to recommend the most secure method for password storage.Which of the following provide the BEST protection against brute forcing stored passwords? (Select TWO). A. PBKDF2B. MD5C. SHA2D. BcryptE. AESF. CHAP Answer: ADExplanation:A: PBKDF2 (Password-Based Key Derivation Function 2) is part of PKCS #5 v. 2.01. It applies some function (like a hash or HMAC) to the password or passphrase along with Salt to produce a derived key.D: bcrypt is a key derivation function for passwords based on the Blowfish cipher. Besides incorporating a salt to protect against rainbow table attacks, bcrypt is an adaptive function: over time, the iteration count can be increased to make it slower, so it remains resistant to brute-force search attacks even with increasing computation power. The bcrypt function is the default password hash algorithm for BSD and many other systems. QUESTION 753Deploying a wildcard certificate is one strategy to: A. Secure the certificate's private key.B. Increase the certificate's encryption key length.C. Extend the renewal date of the certificate.D. Reduce the certificate management burden. Answer: DExplanation:A wildcard certificate is a public key certificate which can be used with multiple subdomains of a domain. This saves money and reduces the management burden of managing multiple certificates, one for each subdomain. A single Wildcard certificate for *.example.com, will secure all these domains:payment.example.comcontact.example.com login-secure.example.comwww.example.com Because the wildcard only covers one level of subdomains (the asterisk doesn't match full stops), these domains would not be valid for the certificate:test.login.example.com QUESTION 754A certificate authority takes which of the following actions in PKI? A. Signs and verifies all infrastructure messagesB. Issues and signs all private keysC. Publishes key escrow lists to CRLsD. Issues and signs all root certificates Answer: DExplanation:A certificate authority can issue multiple certificates in the form of a tree structure. A root certificate is part of a public key infrastructure (PKI) scheme. The most common commercial variety is based on the ITU-T X.509 standard, which normally includes a digital signature from a certificate authority (CA).Note: In cryptography and computer security, a root certificate is an unsigned public key certificate (also called self-signed certificate) that identifies the Root Certificate Authority (CA). QUESTION 755Which of the following is used to certify intermediate authorities in a large PKI deployment? A. Root CAB. Recovery agentC. Root userD. Key escrow Answer: A Explanation:The root CA certifies other certification authorities to publish and manage certificates within the organization.In a hierarchical trust model, also known as a tree, a root CA at the top provides all of the information. The intermediate CAs are next in the hierarchy, and they trust only information provided by the root CA. The root CA also trusts intermediate CAs that are in their level in the hierarchy and none that aren't. This arrangement allows a high level of control at all levels of the hierarchical tree. . QUESTION 756Which of the following components MUST be trusted by all parties in PKI? A. Key escrowB. CAC. Private keyD. Recovery key Answer: BExplanation:A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. In a simple trust model all parties must trust the CA. In a more complicated trust model all parties must trust the Root CA. QUESTION 757Company employees are required to have workstation client certificates to access a bank website. These certificates were backed up as a precautionary step before the new computer upgrade. After the upgrade and restoration, users state they can access the bank's website, but not login.Which is the following is MOST likely the issue? A. The IP addresses of the clients have changeB. The client certificate passwords have expired on the serverC. The certificates have not been installed on the workstationsD. The certificates have been installed on the CA Answer: CExplanation:The computer certificates must be installed on the upgraded client computers. QUESTION 758A company's security administrator wants to manage PKI for internal systems to help reduce costs. Which of the following is the FIRST step the security administrator should take? A. Install a registration server.B. Generate shared public and private keys.C. Install a CAD. Establish a key escrow policy. Answer: CExplanation:PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. When you implement a PKI you should start by installing a CA. QUESTION 759Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a

certificate? A. Certification authorityB. Key escrowC. Certificate revocation listD. Registration authority Answer: A Explanation:A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. QUESTION 760When reviewing a digital certificate for accuracy, which of the following would Matt, a security administrator, focus on to determine who affirms the identity of the certificate owner? A. Trust modelsB. CRLC. CAD. Recovery agent Answer: CExplanation:A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. The CA affirms the identity of the certificate owner. QUESTION 761Joe, a user, reports to the system administrator that he is receiving an error stating his certificate has been revoked. Which of the following is the name of the database repository for these certificates? A. CSRB. OCSPC. CAD. CRL Answer: DExplanation:A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key. QUESTION 762A systems administrator has implemented PKI on a classified government network. In the event that a disconnect occurs from the primary CA, which of the following should be accessible locally from every site to ensure users with bad certificates cannot gain access to the network? A. A CRLB. Make the RA availableC. A verification authorityD. A redundant CA Answer: AExplanation:A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.By checking the CRL you can check if a particular certificate has been revoked. QUESTION 763A CRL is comprised of. A. Malicious IP addresses.B. Trusted CA's.C. Untrusted private keys.D. Public keys. Answer: D Explanation:A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.By checking the CRL you can check if a particular certificate has been revoked. The certificates for which a CRL should be maintained are often X.509/public key certificates, as this format is commonly used by PKI schemes. QUESTION 764Which of the following MUST be updated immediately when an employee is terminated to prevent unauthorized access? A. RegistrationB. CAC. CRLD. Recovery agent Answer: CExplanation:Certificates or keys for the terminated employee should be put in the CRL. A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.By checking the CRL you can check if a particular certificate has been revoked. QUESTION 765Which of the following provides a static record of all certificates that are no longer valid? A. Private keyB. Recovery agentC. CRLsD. CA Answer: CExplanation:The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release. When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user. QUESTION 766A CA is compromised and attacks start distributing maliciously signed software updates. Which of the following can be used to warn users about the malicious activity? A. Key escrowB. Private key verificationC. Public key verificationD. Certificate revocation list Answer: DExplanation:If we put the root certificate of the comprised CA in the CRL, users will know that this CA (and the certificates that it has issued) no longer can be trusted. The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release. QUESTION 767The finance department works with a bank which has recently had a number of cyber attacks. The finance department is concerned that the banking website certificates have been compromised. Which of the following can the finance department check to see if any of the bank's certificates are still valid? A. Bank's CRLB. Bank's private keyC. Bank's key escrowD. Bank's recovery agent Answer: AExplanation:The finance department can check if any of the bank's certificates are in the CRL or not. If a certificate is not in the CRL then it is still valid.The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release. QUESTION 768A security administrator needs a locally stored record to remove the certificates of a terminated employee. Which of the following describes a service that could meet these requirements? A. OCSPB. PKIC. CAD. CRL Answer: DExplanation: A CRL is a locally stored record containing revoked certificates and revoked keys. QUESTION 769Public key certificates and keys that are compromised or were issued fraudulently are listed on which of the following? A. PKIB. ACLC. CAD. CRL Answer: DExplanation:A CRL is a locally stored record containing revoked certificates and revoked keys. QUESTION 770Which of the following identifies certificates that have been compromised or suspected of being compromised? A. Certificate revocation listB. Access control listC. Key escrow registryD. Certificate authority Answer: AExplanation:Certificates that have been compromised or are suspected of being compromised are revoked. A CRL is a locally stored record containing revoked certificates and revoked keys. QUESTION 771When employees that use certificates leave the company they should be added to which of the following? A. PKIB. CAC. CRLD. TKIP Answer: CExplanation:The certificates of the leaving employees must be made unusable. This is done by revoking them.The revoke certificates end up in the CRL.Note: The CRL (Certificate revocation list) is

exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release. QUESTION 772Which of the following should a security technician implement to identify untrusted certificates? A. CAB. PKIC. CRLD. Recovery agent Answer: CExplanation:Untrusted certificates and keys are revoked and put into the CRL. Note: The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. QUESTION 773Which of the following is true about the CRL? A. It should be kept publicB. It signs other keysC. It must be kept secretD. It must be encrypted Answer: AExplanation:The CRL must be public so that it can be known which keys and certificates have been revoked. In the operation of some cryptosystems, usually public key infrastructures (PKIs), a certificate revocation list (CRL) is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted. QUESTION 774A system administrator is notified by a staff member that their laptop has been lost. The laptop contains the user's digital certificate. Which of the following will help resolve the issue? (Select TWO). A. Revoke the digital certificateB. Mark the key as private and import itC. Restore the certificate using a CRL D. Issue a new digital certificateE. Restore the certificate using a recovery agent Answer: ADExplanation:The user's certificate must be revoked to ensure that the stolen computer cannot access resources the user has had access to.To grant the user access to the resources he must be issued a new certificate. QUESTION 775Which of the following protocols is used to validate whether trust is in place and accurate by returning responses of either "good", "unknown", or "revoked"? A. CRLB. PKIC. OCSPD. RA Answer: CExplanation:The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.An OCSP responder (a server typically run by the certificate issuer) may return a signed response signifying that the certificate specified in the request is 'good', 'revoked', or 'unknown'. If it cannot process the request, it may return an error code. More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E Piece of advice. Memorize the dumps inside out but still be careful, some questions are tweaked as in options differ and your answers will be different. Read the question before answering!!!! 2017 CompTIA SY0-401 (All 1868 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]