[2017 New Lead2pass Latest CompTIA SY0-401 Exam Questions Free Download (276-300)

2017 August CompTIA Official New Released SY0-401 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!
2017 latest released CompTIA official SY0-401 exam question free download from Lead2pass! All new updated questions and answers are real questions from CompTIA Exam Center! Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 276A software developer wants to prevent stored passwords from being easily decrypted. When the password is stored by the application, additional text is added to each password before the password is hashed. This technique is known as: A. Symmetric cryptography.B. Private key cryptography.C. Salting.D. Rainbow tables.Answer: CExplanation:Salting can be used to strengthen the hashing when the passwords were encrypted. Though hashing is a one-way algorithm it does not mean that it cannot be hacked. One method to hack a hash is though rainbow tables and salt is the counter measure to rainbow tables. With salt a password that you typed in and that has been encrypted with a hash will yield a letter combination other than what you actually types in when it is rainbow table attacked. QUESTION 277 Which of the following concepts describes the use of a one way transformation in order to validate the integrity of a program? A. HashingB. Key escrowC. Non-repudiationD. Steganography Answer: AExplanation:Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables and its main characteristics are:It must be one-way ?it is not reversible. Variable-length input produces fixed-length output ?whether you have two characters or 2 million, the hash size is the same.The algorithm must have few or no collisions ?in hashing two different inputs does not give the same output. QUESTION 278The security administrator is implementing a malware storage system to archive all malware seen by the company into a central database. The malware must be categorized and stored based on similarities in the code. Which of the following should the security administrator use to identify similar malware? A. TwoFishB. SHA-512C. Fuzzy hashesD. HMAC Answer: CExplanation: Hashing is used to ensure that a message has not been altered. It can be useful for positively identifying malware when a suspected file has the same hash value as a known piece of malware. However, modifying a single bit of a malicious file will alter its hash value. To counter this, a continuous stream of hash values is generated for rolling block of code. This can be used to determine the similarity between a suspected file and known pieces of malware. QUESTION 279An Information Systems Security Officer (ISSO) has been placed in charge of a classified peer-to- peer network that cannot connect to the Internet. The ISSO can update the antivirus definitions manually, but which of the following steps is MOST important? A. A full scan must be run on the network after the DAT file is installed.B. The signatures must have a hash value equal to what is displayed on the vendor site.C. The definition file must be updated within seven days.D. All users must be logged off of the network prior to the installation of the definition file. Answer: BExplanation:A hash value can be used to uniquely identify secret information. This requires that the hash function is collision resistant, which means that it is very hard to find data that generate the same hash value and thus it means that in hashing two different inputs will not yield the same output. Thus the hash value must be equal to that displayed on the vendor site. QUESTION 280Which of the following would a security administrator use to verify the integrity of a file? A. Time stampB. MAC timesC. File descriptorD. Hash Answer: DExplanation:Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables and it is a one-way transformation in order to validate the integrity of data. QUESTION 281 Sara, a security administrator, manually hashes all network device configuration files daily and compares them to the previous days' hashes. Which of the following security concepts is Sara using? A. ConfidentialityB. ComplianceC. IntegrityD. Availability Answer: CExplanation:Integrity means the message can't be altered without detection. QUESTION 282Matt, a forensic analyst, wants to obtain the digital fingerprint for a given message. The message is 160-bits long. Which of the following hashing methods would Matt have to use to obtain this digital fingerprint? A. SHA1B. MD2C. MD4D. MD5 Answer: AExplanation:The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. This algorithm produces a 160-bit hash value. SHA (1 or 2) is preferred over Message Digest Algorithm. QUESTION 283Company A submitted a bid on a contract to do work for Company B via email. Company B was insistent that the bid did not come from Company A. Which of the following would have assured that the bid was submitted by Company A? A. SteganographyB. HashingC. EncryptionD. Digital Signatures Answer: DExplanation:A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message. QUESTION 284An email client says a digital signature is invalid and the sender cannot be verified. The recipient is concerned with which of the following concepts? A. IntegrityB. AvailabilityC. ConfidentialityD. Remediation Answer: AExplanation:A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender.

The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message. Digital Signatures is used to validate the integrity of the message and the sender. Integrity means the message can't be altered without detection. QUESTION 285A software firm posts patches and updates to a publicly accessible FTP site. The software firm also posts digitally signed checksums of all patches and updates. The firm does this to address: A. Integrity of downloaded software.B. Availability of the FTP site.C. Confidentiality of downloaded software.D. Integrity of the server logs. Answer: A Explanation:Digital Signatures is used to validate the integrity of the message and the sender. In this case the software firm that posted the patches and updates digitally signed the checksums of all patches and updates. QUESTION 286It is important to staff who use email messaging to provide PII to others on a regular basis to have confidence that their messages are not intercepted or altered during transmission. They are concerned about which of the following types of security control? A. IntegrityB. SafetyC. AvailabilityD. Confidentiality Answer: AExplanation:Integrity means that the messages/ data is not altered. PII is personally identifiable information that can be used to uniquely identify an individual. PII can be used to ensure the integrity of data/messages. QUESTION 287Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit. This concern relates to which of the following concepts? A. AvailabilityB. IntegrityC. AccountingD. Confidentiality Answer: BExplanation:Integrity means ensuring that data has not been altered. Hashing and message authentication codes are the most common methods to accomplish this. In addition, ensuring nonrepudiation via digital signatures supports integrity. QUESTION 288Which of the following is used by the recipient of a digitally signed email to verify the identity of the sender? A. Recipient's private keyB. Sender's public keyC. Recipient's public keyD. Sender's private key Answer: B Explanation:When the sender wants to send a message to the receiver. It's important that this message not be altered. The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The recipient uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic. Thus the recipient uses the sender's public key to verify the sender's identity. QUESTION 289Digital signatures are used for ensuring which of the following items? (Select TWO). A. ConfidentialityB. IntegrityC. Non-RepudiationD. AvailabilityE. Algorithm strength Answer: BCExplanation:A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message. Nonrepudiation prevents one party from denying actions that they carried out and in the electronic world nonrepudiation measures can be a two-key cryptographic system and the involvement of a third party to verify the validity. This respected third party `vouches' for the individuals in the two- key system. Thus non-repudiation also impacts on integrity. QUESTION 290Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify that the email came from Joe and decrypt it? (Select TWO). A. The CA's public keyB. Ann's public keyC. Joe's private keyD. Ann's private keyE. The CA's private keyF. Joe's public key Answer: DFExplanation:Joe wants to send a message to Ann. It's important that this message not be altered. Joe will use the private key to create a digital signature. The message is, in effect, signed with the private key. Joe then sends the message to Ann. Ann will use the public key attached to the message to validate the digital signature. If the values match, Ann knows the message is authentic and came from Joe. Ann will use a key provided by Joe--the public key--to decrypt the message. Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidently, in transit. Thus Ann would compare the signature area referred to as a message in the message with the calculated value digest (her private key in this case). If the values match, the message hasn't been tampered with and the originator is verified as the person they claim to be. QUESTION 291Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify the validity's of Joe's certificate? (Select TWO). A. The CA's public keyB. Joe's private keyC. Ann's public keyD. The CA's private keyE. Joe's public keyF. Ann's private key Answer: AEExplanation:Joe wants to send a message to Ann. It's important that this message not be altered. Joe will use the private key to create a digital signature. The message is, in effect, signed with the private key. Joe then sends the message to Ann. Ann will use the public key attached to the message to validate the digital signature. If the values match, Ann knows the message is authentic and came from Joe. Ann will use a key provided by Joe--the public key--to decrypt the message. Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidently, in transit. Thus Ann would compare the signature area referred to as a message in the message with the calculated value digest (her private key in this case). If the values match, the message hasn't been tampered with and the originator is verified as the person they claim to be. This process provides message integrity, nonrepudiation, and authentication. A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. A certificate is nothing more than a mechanism that associates the public key with an individual.If Joe wants to send Ann an encrypted e-mail, there should be a mechanism to verify to Ann that the message received from Mike is really from Joe. If a third party (the CA) vouches for Joe and

Ann trusts that third party, Ann can assume that the message is authentic because the third party says so. QUESTION 292A user was reissued a smart card after the previous smart card had expired. The user is able to log into the domain but is now unable to send digitally signed or encrypted email. Which of the following would the user need to perform? A. Remove all previous smart card certificates from the local certificate store.B. Publish the new certificates to the global address list.C. Make the certificates available to the operating system.D. Recover the previous smart card certificates. Answer: BExplanation:CAs can be either private or public, with VeriSign being one of the best known of the public variety. Many operating system providers allow their systems to be configured as CA systems.These CA systems can be used to generate internal certificates that are used within a business or in large external settings. The process provides certificates to the users. Since the user in question has been re-issued a smart card, the user must receive a new certificate by the CA to allow the user to send digitally signed email. This is achieved by publishing the new certificates to the global address list. QUESTION 293Which of the following could cause a browser to display the message below? "The security certificate presented by this website was issued for a different website's address." A. The website certificate was issued by a different CA than what the browser recognizes in its trusted CAs.B. The website is using a wildcard certificate issued for the company's domain.C. HTTPS://127.0.01 was used instead of HTTPS://localhost.D. The website is using an expired self signed certificate. 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. In typical public key infrastructure (PKI) arrangements, a digital signature from a certificate authority (CA) attests that a particular public key certificate is valid (i.e., contains correct information). Users, or their software on their behalf, check that the private key used to sign some certificate matches the public key in the CA's certificate. Since CA certificates are often signed by other, "higher-ranking," CAs, there must necessarily be a highest CA, which provides the ultimate in attestation authority in that particular PKI scheme.Localhost is a hostname that means this computer and may be used to access the computer's own network services via its loopback network interface. Using the loopback interface bypasses local network interface hardware. In this case the HTTPS://127.0.01 was used and not HTTPS//localhost QUESTION 294Certificates are used for: (Select TWO). A. Client authentication.B. WEP encryption.C. Access control lists.D. Code signing.E. Password hashing. Answer: ADExplanation:Certificates are used in PKI to digitally sign data, information, files, email, code, etc. Certificates are also used in PKI for client authentication. QUESTION 295Some customers have reported receiving an untrusted certificate warning when visiting the company's website. The administrator ensures that the certificate is not expired and that customers have trusted the original issuer of the certificate. Which of the following could be causing the problem? A. The intermediate CA certificates were not installed on the server.B. The certificate is not the correct type for a virtual server.C. The encryption key used in the certificate is too short.D. The client's browser is trying to negotiate SSL instead of TLS. Answer: AExplanation: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. QUESTION 296Digital certificates can be used to ensure which of the following? (Select TWO). A. AvailabilityB. ConfidentialityC. VerificationD. AuthorizationE. Non-repudiation Answer: BEExplanation: Digital Signatures is used to validate the integrity of the message and the sender. Digital certificates refer to cryptography which is mainly concerned with Confidentiality, Integrity, Authentication, Nonrepudiation and Access Control. Nonrepudiation prevents one party from denying actions they carried out. QUESTION 297A certificate used on an ecommerce web server is about to expire. Which of the following will occur if the certificate is allowed to expire? A. The certificate will be added to the Certificate Revocation List (CRL).B. Clients will be notified that the certificate is invalid.C. The ecommerce site will not function until the certificate is renewed.D. The ecommerce site will no longer use encryption. Answer: B Explanation:A similar process to certificate revocation will occur when a certificate is allowed to expire. Notification will be sent out to clients of the invalid certificate. The process of revoking a certificate begins when the CA is notified that a particular certificate needs to be revoked. This must be done whenever the private key becomes known. The owner of a certificate can request that it be revoked at any time, or the administrator can make the request. QUESTION 298An administrator has successfully implemented SSL on srv4.comptia.com using wildcard certificate *.comptia.com, and now wishes to implement SSL on srv5.comptia.com. Which of the following files should be copied from srv4 to accomplish this? A. certificate, private key, and intermediate certificate chainB. certificate, intermediate certificate chain, and root certificateC. certificate, root certificate, and certificate signing requestD. certificate, public key, and certificate signing request Answer: AExplanation:a wildcard certificate is a public key certificate which can be used with multiple subdomains of a domain. In public-key cryptography, the receiver has a private key known only to them; a public key corresponds to it, which they make known to others. The public key can be sent to all other parties; the private key is never divulged. A symmetric algorithm requires that receivers of the message use the same private key. Thus you should copy the certificate, the private key and the intermediate certificate chain from srv4 to srv5. QUESTION 299

An encrypted message is sent using PKI from Sara, a client, to a customer. Sara claims she never sent the message. Which of the following aspects of PKI BEST ensures the identity of the sender? A. CRLB. Non-repudiationC. Trust modelsD. Recovery agents Answer: BExplanation:Nonrepudiation prevents one party from denying actions they carried out. This means that the identity of the email sender will not be repudiated. QUESTION 300Ann, a newly hired human resource employee, sent out confidential emails with digital signatures, to an unintended group. Which of the following would prevent her from denying accountability? A. Email EncryptionB. SteganographyC. Non RepudiationD. Access Control Answer: CExplanation:Nonrepudiation prevents one party from denying actions they carried out. Lead2pass offers the latest CompTIA SY0-401 exam questions and answers in PDF & VCE. We promise 100% SY0-401 exam pass or full money back (Have a try- If success, you will get a high pay job! Failed, nothing, money back!)! We provide instant download of our SY0-401 dumps after payment so you can study earlier than others! SY0-401 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDVzFZWExUbFM0YU0 2017 CompTIA **SY0-401** exam dumps (All 1868 Q&As) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]