[Lead2pass New Lead2pass SY0-401 New Questions For Passing The SY0-401 Certification Exam (726-750)

I passed the SY0-401 exam today with 9xx. Lead2pass SY0-401 exam question is valid. Thank you all and special thanks to Lead2pass. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 726Which of the following MUST Matt, a security administrator, implement to verify both the integrity and authenticity of a message while requiring a shared secret? A. RIPEMDB. MD5C. SHAD. HMACAnswer: DExplanation:HMAC (Hash-Based Message Authentication Code) uses a hashing algorithm along with a symmetric key. The hashing function provides data integrity, while the symmetric key provides authenticity. QUESTION 727Which of the following cryptographic algorithms is MOST often used with IPSec? A. BlowfishB. TwofishC. RC4D. HMAC Answer: DExplanation:The HMAC-MD5-96 (also known as HMAC-MD5) encryption technique is used by IPSec to make sure that a message has not been altered. QUESTION 728When creating a public / private key pair, for which of the following ciphers would a user need to specify the key strength? A. SHAB. AESC. DESD. RSA Answer: DExplanation:RSA (an asymmetric algorithm) uses keys of a minimum length of 2048 bits. QUESTION 729Which of the following uses both a public and private key? A. RSAB. AESC. MD5D. SHA Answer: AExplanation:The RSA algorithm is an early public-key encryption system that uses large integers as the basis for the process.RSA uses both a public key and a secret.RSA key generation process:1. Generate two large random primes, p and q, of approximately equal size such that their product, n = pq, is of the required bit length (such as 2048 bits, 4096 bits, and so forth).Let n = pqLet m = (p-1)(q-1)2. Choose a small number e, co-prime to m (note: Two numbers are co-prime if they have no common factors).3. Find d, such thatde % m = 14. Publish e and n as the public key. Keep d and n as the secret key. QUESTION 730Which of the following ciphers would be BEST used to encrypt streaming video? A. RSAB. RC4C. SHA1D. 3DES Answer: BExplanation:In cryptography, RC4 is the most widely used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS). While remarkable for its simplicity and speed in software, RC4 has weaknesses that argue against its use in new systems. It is especially vulnerable when the beginning of the output keystream is not discarded, or when nonrandom or related keys are used; some ways of using RC4 can lead to very insecure protocols such as WEP. Because RC4 is a stream cipher, it is more malleable than common block ciphers. If not used together with a strong message authentication code (MAC), then encryption is vulnerable to a bit- flipping attack. The cipher is also vulnerable to a stream cipher attack if not implemented correctly. Furthermore, inadvertent double encryption of a message with the same key may accidentally output plaintext rather than ciphertext because the involutory nature of the XOR function would result in the second operation reversing the first.It is noteworthy, however, that RC4, being a stream cipher, was for a period of time the only common cipher that was immune to the 2011 BEAST attack on TLS 1.0. The attack exploits a known weakness in the way cipher block chaining mode is used with all of the other ciphers supported by TLS 1.0, which are all block ciphers. QUESTION 731Due to hardware limitation, a technician must implement a wireless encryption algorithm that uses the RC4 protocol. Which of the following is a wireless encryption solution that the technician should implement while ensuring the STRONGEST level of security? A. WPA2-AESB. 802.11acC. WPA-TKIPD. WEP Answer: CExplanation:WPA-TKIP uses the RC4 cipher.TKIP and the related WPA standard implement three new security features to address security problems encountered in WEP protected networks. First, TKIP implements a key mixing function that combines the secret root key with the initialization vector before passing it to the RC4 initialization. WEP, in comparison, merely concatenated the initialization vector to the root key, and passed this value to the RC4 routine. This permitted the vast majority of the RC4 based WEP related key attacks. Second, WPA implements a sequence counter to protect against replay attacks. Packets received out of order will be rejected by the access point. Finally, TKIP implements a 64-bit Message Integrity Check (MIC)To be able to run on legacy WEP hardware with minor upgrades, TKIP uses RC4 as its cipher. TKIP also provides a rekeying mechanism. TKIP ensures that every data packet is sent with a unique encryption key. QUESTION 732A security administrator must implement a wireless encryption system to secure mobile devices' communication. Some users have mobile devices which only support 56-bit encryption. Which of the following wireless encryption methods should be implemented? A. RC4B. AESC. MD5D. TKIP Answer: AExplanation:RC4 is popular with wireless and WEP/WPA encryption. It is a streaming cipher that works with key sizes between 40 and 2048 bits, and it is used in SSL and TLS. QUESTION 733Which of the following can use RC4 for encryption? (Select TWO). A. CHAPB. SSLC. WEPD. AESE. 3DES Answer: BCExplanation: B: In cryptography, RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4) is the most widely used software stream cipher and is used in popular Internet protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS).C: WEP also uses RC4, however WEP is still unsecure. QUESTION 734Which of the following would provide the STRONGEST encryption? A. Random one-time padB. DES with a 56-bit keyC. AES with a 256-bit keyD. RSA

with a 1024-bit key Answer: AExplanation:One-time pads are the only truly completely secure cryptographic implementations. They are so secure for two reasons. First, they use a key that is as long as a plaintext message. That means there is no pattern in the key application for an attacker to use. Also, one-time pad keys are used only once and then discarded. So even if you could break a one-time pad cipher, that same key would never be used again, so knowledge of the key would be useless. QUESTION 735Which of the following symmetric key algorithms are examples of block ciphers? (Select THREE). A. RC4B. 3DESC. AESD. MD5E. PGPF. Blowfish Answer: BCFExplanation:B: Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.C: Advanced Encryption Standard (AES) is a block cipher that has replaced DES as the current standard, and it uses the Rijndael algorithm. It was developed by Joan Daemen and Vincent Rijmen. AES is the current product used by U.S. governmental agencies.F: Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64- bit block cipher at very fast speeds. QUESTION 736Which of the following should be used when a business needs a block cipher with minimal key size for internal encryption? A. AESB. BlowfishC. RC5D. 3DES Answer: BExplanation:Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64-bit block cipher at very fast speeds. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits). QUESTION 737Sara, a security engineer, is testing encryption ciphers for performance. Which of the following ciphers offers strong encryption with the FASTEST speed? A. 3DES B. BlowfishC. SerpentD. AES256 Answer: BExplanation:Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64-bit block cipher at very fast speeds. Blowfish is a fast, except when changing keys. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits). QUESTION 738Jane, a VPN administrator, was asked to implement an encryption cipher with a MINIMUM effective security of 128-bits. Which of the following should Jane select for the tunnel encryption? A. BlowfishB. DESC. SHA256D. HMAC Answer: AExplanation:Blowfish is an encryption system that performs a 64-bit block cipher at very fast speeds. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits). Among the alternatives listed above, it is the only cipher that can use a 128-bit key and which does provide additional security through a symmetric key. QUESTION 739When using PGP, which of the following should the end user protect from compromise? (Select TWO). A. Private keyB. CRL detailsC. Public keyD. Key passwordE. Key escrowF. Recovery agent Answer: ADExplanation:A: In PGP only the private key belonging to the receiver can decrypt the session key. PGP combines symmetric-key encryption and public-key encryption. The message is encrypted using a symmetric encryption algorithm, which requires a symmetric key. Each symmetric key is used only once and is also called a session key.D: PGP uses a passphrase to encrypt your private key on your machine. Your private key is encrypted on your disk using a hash of your passphrase as the secret key. You use the passphrase to decrypt and use your private key. QUESTION 740A 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. PBKDF2B. Symmetric encryptionC. SteganographyD. ECDHEE. Diffie-Hellman Answer: DEExplanation:Elliptic curve DiffieHellman (ECDH) is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. This shared secret may be directly used as a key, or better yet, to derive another key which can then be used to encrypt subsequent communications using a symmetric key cipher. It is a variant of the Diffie?ellman protocol using elliptic curve cryptography. Note: Adding an ephemeral key to Diffie-Hellman turns it into DHE (which, despite the order of the acronym, stands for Ephemeral Diffie-Hellman).Adding an ephemeral key to Elliptic Curve Diffie-Hellman turns it into ECDHE (again, overlook the order of the acronym letters, it is called Ephemeral Elliptic Curve Diffie-Hellman). It is the ephemeral component of each of these that provides the perfect forward secrecy. QUESTION 741Connections using point-to-point protocol authenticate using which of the following? (Select TWO). A. RIPEMDB. PAPC. CHAPD. RC4E. Kerberos Answer: BCExplanation:B: A password authentication protocol (PAP) is an authentication protocol that uses a password. PAP is used by Point to Point Protocol to validate users before allowing them access to server resources.C: CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three- way handshake. QUESTION 742Which of the following offers the LEAST secure encryption capabilities? A. TwoFishB. PAPC. NTLMD. CHAP Answer: BExplanation:PAP transmits unencrypted ASCII passwords over the network and is therefore considered insecure. It is used as a last resort when the remote server does not support a stronger authentication protocol, like CHAP or EAP. QUESTION 743Which of the following algorithms has well documented collisions? (Select TWO). A. AESB. MD5C. SHAD. SHA-256E. RSA Answer: BCExplanation:B: MD5 biggest weakness is that it does not have strong collision resistance, and thus it is no longer recommended for use.C: SHA-1 (also known as SHA) is being retired from most government uses; the U.S. National Institute of Standards and Technology said, "Federal agencies should stop using SHA-1 for...applications that require

collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010", though that was later relaxed. Note: The hashing algorithm must have few or no collisions. This means that hashing two different inputs does not give the same output.Cryptographic hash functions are usually designed to be collision resistant. But many hash functions that were once thought to be collision resistant were later broken. MD5 and SHA-1 in particular both have published techniques more efficient than brute force for finding collisions. QUESTION 744Which of the following protocols is the security administrator observing in this packet capture? 12:33:43, SRC 192.168.4.3:3389, DST 10.67.33.20:8080, SYN/ACK A. HTTPSB. RDPC. HTTPD. SFTP Answer: BExplanation:Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.Example of RDP tracing output: No. Time Delta Source Destination Protocol Length Info 5782, 2013-01-06 09:52:15.407, 0.000 , SRC 10.7.3.187 , DST 10.0.107.58, TCP, 62, 3389 > 59193 [SYN, ACK] QUESTION 745Which of the following cryptographic related browser settings allows an organization to communicate securely? A. SSL 3.0/TLS 1.0B. 3DESC. Trusted SitesD. HMAC Answer: A Explanation:Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. Transport Layer Security (TLS) is a security protocol that expands upon SSL. Many industry analysts predict that TLS will replace SSL in the future. TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As of February 2015, the latest versions of all major web browsers support TLS 1.0, 1.1, and 1.2, have them enabled by default. QUESTION 746Recent data loss on financial servers due to security breaches forced the system administrator to harden their systems. Which of the following algorithms with transport encryption would be implemented to provide the MOST secure web connections to manage and access these servers? A. SSLB. TLSC. HTTPD. FTP Answer: BExplanation:Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Transport Layer Security (TLS) is a security protocol that expands upon SSL. Many industry analysts predict that TLS will replace SSL in the future. TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As of February 2015, the latest versions of all major web browsers support TLS 1.0, 1.1, and 1.2, have them enabled by default. QUESTION 747A security administrator has been tasked with setting up a new internal wireless network that must use end to end TLS. Which of the following may be used to meet this objective? A. WPAB. HTTPSC. WEPD. WPA 2 Answer: DExplanation:Wi-Fi Protected Access 2 (WPA2) was intended to provide security that's equivalent to that on a wired network, and it implements elements of the 802.11i standard. In April 2010, the Wi-Fi Alliance announced the inclusion of additional Extensible Authentication Protocol (EAP) types to its certification programs for WPA- and WPA2- Enterprise certification programs. EAP-TLS is included in this certification program.Note: Although WPA mandates the use of TKIP, WPA2 requires Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP uses 128-bit AES encryption with a 48-bit initialization vector. With the larger initialization vector, it increases the difficulty in cracking and minimizes the risk of a replay attack. QUESTION 748Which of the following protocols encapsulates an IP packet with an additional IP header? A. SFTPB. IPSecC. HTTPSD. SSL Answer: B Explanation:Authentication Header (AH) is a member of the IPsec protocol suite. AH operates directly on top of IP, using IP protocol number 51. QUESTION 749A new MPLS network link has been established between a company and its business partner. The link provides logical isolation in order to prevent access from other business partners. Which of the following should be applied in order to achieve confidentiality and integrity of all data across the link? A. MPLS should be run in IPVPN mode.B. SSL/TLS for all application flows.C. IPSec VPN tunnels on top of the MPLS link.D. HTTPS and SSH for all application flows. Answer: C Explanation:IPSec can very well be used with MPLS. IPSec could provide VPN tunnels on top if the MPLS link. Internet Protocol Security (IPSec) isn't a tunneling protocol, but it's used in conjunction with tunneling protocols. IPSec is oriented primarily toward LAN-to-LAN connections, but it can also be used with dial-up connections. IPSec provides secure authentication and encryption of data and headers; this makes it a good choice for security. QUESTION 750Which of the following would be used as a secure substitute for Telnet? A. SSHB. SFTPC. SSLD. HTTPS Answer: AExplanation: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. More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E Only get 2 new Qs and some Qs are variant of the Qs in this Lead2pass SY0-401 pdf dumps, but they just changed server names or the orders of the options of the case. Good luck you all. 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]