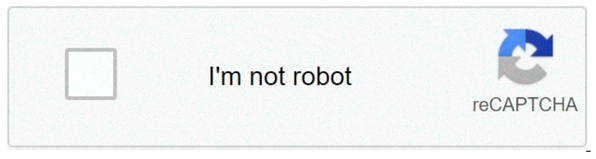

Continue

Chapter 7 exam cisco

1 A PC is downloading a large file from a server. The TCP window is 1000 bytes. The server is sending the file using 100-byte segments. How many segments will the server send before it requires an acknowledgment from the PC?1 segment10 segments*100 segments1000 segments 2 A host device needs to send a large video file across the network while providing data communication to other users. Which feature will allow different communication streams to occur at the same time, without having a single data stream using all available bandwidth?multiplexing *window sizeacknowledgmentsport numbers 3 A technician wishes to use TFTP to transfer a large file from a file server to a remote router. Which statement is correct about this scenario? The file is segmented and then reassembled in the correct order by TCP.The file is not segmented, because UDP is the transport layer protocol that is used by TFTP.Large files must be sent by FTP not TFTP.The file is segmented and then reassembled in the correct order at the destination, if necessary, by the upper-layer protocol.* 4 5 Which scenario describes a function provided by the transport layer?A student is using a classroom VoIP phone to call home. The unique identifier burned into the phone is a transport layer address used to contact another network device on the same network.A corporate worker is accessing a web server located on a corporate network. The transport layer formats the screen so the web page appears properly no matter what device is being used to view the web site.A student has two web browser windows open in order to access two web sites. The transport layer ensures the correct web page is delivered to the correct browser window.*A student is playing a short web-based movie with sound. The movie and sound are encoded within the transport layer header. 6 Which transport layer feature is used to guarantee session establishment?UDP ACK flagTCP 3-way handshake*UDP sequence numberTCP port number 7 What is the complete range of TCP and UDP well-known ports?0 to 255256 – 10230 to 1023*1024 – 49151 8 Which two TCP header fields are used to confirm receipt of data?checksumacknowledgment number*FIN flagsequence number*SYN flag 9 What is a beneficial feature of the UDP transport protocol?acknowledgment of received datatracking of data segments using sequence numbersfewer delays in transmission*the ability to retransmit lost data 10 Which two flags in the TCP header are used in a TCP three-way handshake to establish connectivity between two network devices? (Choose two.)RSTFINSYN*ACK*URGPSH 11 What happens if the first packet of a TFTP transfer is lost?The TFTP application will retry the request if a reply is not received.*The next-hop router or the default gateway will provide a reply with an error code.The client will wait indefinitely for the reply.The transport layer will retry the query if a reply is not received. 12 Compared to UDP, what factor causes additional network overhead for TCP communication?the identification of applications based on destination port numbersthe checksum error detectionthe encapsulation into IP packetsnetwork traffic that is caused by retransmissions* 13 14 Which factor determines TCP window size?the amount of data the destination can process at one time*the number of services included in the TCP segmentthe amount of data the source is capable of sending at one timethe amount of data to be transmitted 15 16 During a TCP session, a destination device sends an acknowledgment number to the source device. What does the acknowledgment number represent?the last sequence number that was sent by the sourceone number more than the sequence numberthe next byte that the destination expects to receive*the total number of bytes that have been received 17 What is a socket?the combination of the source and destination sequence numbers and port numbersthe combination of the source and destination sequence and acknowledgment numbersthe combination of a source IP address and port number or a destination IP address and port number*the combination of the source and destination IP address and source and destination Ethernet address 18 Fill in the blank.During a TCP session, the “SYN” field is used by the client to request communication with the server. 19 Fill in the blank using a number. A total of “4” messages are exchanged during the TCP session termination process between the client and the server. 20 A host device sends a data packet to a web server via the HTTP protocol. What is used by the transport layer to pass the data stream to the proper application on the server?source port numberdestination port number*sequence numberacknowledgment 21 What does a client do when it has UDP datagrams to send?It just sends the datagrams.*It queries the server to see if it is ready to receive data.It sends a simplified three-way handshake to the server.It sends to the server a segment with the SYN flag set to synchronize the conversation. 22 What does a client application select for a TCP or UDP source port number?a predefined value in the dynamic port rangea predefined value in the range of the registered portsa predefined value in the well-known port rangea random value in the dynamic port rangea random value in the range of the registered ports*a random value in the well-known port range Last updated Feb 18, 2019 CCNA Security Chapter 7 Exam Answers An online retailer needs a service to support the nonrepudiation of the transaction. Which component is used for this service? the private key of the retailer the unique shared secret known only by the retailer and the customer the public key of the retailer the digital signatures* Digital signatures, generated by hash function, can provide the service for nonrepudiation of the transaction. Both public and private keys are used to encrypt data during the transaction. Shared secrets between the retailer and customers are not used. In which situation is an asymmetric key algorithm used? Two Cisco routers authenticate each other with CHAP. User data is transmitted across the network after a VPN is established. An office manager encrypts confidential files before saving them to a removable device. A network administrator connects to a Cisco router with SSH.* The SSH protocol uses an asymmetric key algorithm to authenticate users and encrypt data transmitted. The SSH server generates a pair of public/private keys for the connections. Encrypting files before saving them to a storage device uses a symmetric key algorithm because the same key is used to encrypt and decrypt files. The router authentication with CHAP uses a symmetric key algorithm. The key is pre-configured by the network administrator. A VPN may use both an asymmetric key and a symmetric encryption algorithm. For example in an IPSec VPN implementation, the data transmission uses a shared secret (generated with an asymmetric key algorithm) with a symmetric encryption algorithm used for performance. What is the purpose of a nonrepudiation service in secure communications? to ensure that encrypted secure communications cannot be decoded to confirm the identity of the recipient of the communications to provide the highest encryption level possible to ensure that the source of the communications is confirmed* Nonrepudiation uses the unique characteristics of the sender of a message to confirm that the reputed sender is in fact the actual sender. Which objective of secure communications is achieved by encrypting data? integrity authentication confidentiality* availability When data is encrypted, it is scrambled to keep the data private and confidential so that only authorized recipients can read the message. A hash function is another way of providing confidentiality. Which encryption protocol provides network layer confidentiality? IPsec protocol suite* Transport Layer Security Secure Hash Algorithm 1 Secure Sockets Layer Keyed MD5 Message Digest 5 Cryptographic encryption can provide confidentiality at several layers of the OSI model. For example, network layer protocols, such as the IPsec protocol suite, provide network layer confidentiality. Secure Sockets Layer (SSL) or Transport Layer Security (TLS), provide session layer confidentiality. MD5, Keyed MD5, and Secure Hash Algorithm 1 are examples of hash functions. They provide data integrity but not data confidentiality. Refer to the exhibit. Which encryption algorithm is described in the exhibit? 3DES is a good choice to protect data because it has an algorithm that is very trusted and has security strength. Why is the 3DES algorithm often preferred over the AES algorithm? 3DES is more trusted because it has been proven secure for a longer period than AES.* AES is more expensive to implement than 3DES. 3DES performs better in high-throughput, low-latency environments than AES. Major networking equipment vendors such as Cisco have not yet adopted AES. Despite its advantages, AES is a relatively young algorithm. An important rule of cryptography is that a mature algorithm is always more trusted. 3DES is therefore a more trusted choice in terms of strength, because it has been tested and analyzed for 35 years. AES can be used in high-throughput, low-latency environments, especially when 3DES cannot handle the throughput or latency requirements. AES is available in a number of Cisco VPN devices as an encryption transform. What is the most common use of the Diffie-Helman algorithm in communications security? to create password hashes for secure authentication to provide routing protocol authentication between routers to encrypt data for secure e-commerce communications to secure the exchange of keys used to encrypt data* Diffie-Helman is not an encryption mechanism and is not typically used to encrypt data. Instead, it is a method to securely exchange the keys used to encrypt the data. What is the focus of cryptanalysis? hiding secret codes developing secret codes* breaking encrypted codes implementing encrypted codes How many bits does the Data Encryption Standard (DES) use for data encryption? 40 bits 56 bits* 64 bits 72 bits DES uses a fixed length key. The key is 64-bits long, but only 56 bits are used for encryption. The remaining 8 bits are used for parity. A DES encryption key is always 56 bits long. When DES is used with a weaker encryption of a 40-bit key, the encryption key is 40 secret bits and 16 known bits, which make the key length 56 bits. Which statement describes the Software-Optimized Encryption Algorithm (SEAL)? SEAL is a stream cipher.* It uses a 112-bit encryption key. It is an example of an asymmetric algorithm. It requires more CPU resources than software-based AES does. SEAL is a stream cipher that uses a 160-bit encryption key. It is a symmetric encryption algorithm that has a lower impact on the CPU resources compared to other software-based algorithms, such as software-based DES, 3DES, and AES. Which encryption algorithm is an asymmetric algorithm? DH is an asymmetric algorithm. AES, 3DES, and SEAL are all symmetric algorithms. Which type of encryption algorithm uses public and private keys to provide authentication, integrity, and confidentiality? symmetric shared secret IPsec asymmetric* An asymmetric encryption algorithm uses two keys, namely a public key and a private key. A symmetric encryption algorithm uses an identical key for both encryption and decryption. A shared secret is an example of using symmetric algorithm. How do modern cryptographers defend against brute-force attacks? Use statistical analysis to eliminate the most common encryption keys. Use a keyspace large enough that it takes too much money and too much time to conduct a successful attack.* Use an algorithm that requires the attacker to have both ciphertext and plaintext to conduct a successful attack. Use frequency analysis to ensure that the most popular letters used in the language are not used in the cipher message. In a brute-force attack, an attacker tries every possible key with the decryption algorithm knowing that eventually one of them will work. To defend against the brute-force attacks, modern cryptographers have as an objective to have a keyspace (a set of all possible keys) large enough so that it takes too much money and too much time to accomplish a brute-force attack. A security policy requiring passwords to be changed in a predefined interval further defend against the brute-force attacks. The idea is that passwords will have been changed before an attacker exhausts the keyspace. Which statement describes asymmetric encryption algorithms? They have key lengths ranging from 80 to 256 bits. They include DES, 3DES, and AES. They are also called shared-secret key algorithms. They are relatively slow because they are based on difficult computational algorithms.* DES, 3DES, and AES are examples of symmetric encryption algorithms (also known as shared secret key algorithms). The usual key length for symmetric algorithms is 80-256 bits. Asymmetric algorithms are relatively slow because they are based on difficult computational algorithms. Which two non-secret numbers are initially agreed upon when the Diffie-Hellman algorithm is used? (Choose two.) binomial coefficient generator* elliptic curve invariant prime modulus* topological index pseudorandom nome DH is a mathematical algorithm that allows two hosts to generate an identical shared secret on both systems without having communicated before. To start a DH exchange, both hosts must agree on two nonsecret numbers. The first number is a base number, also called the generator. The second number is a prime number that is used as the modulus. These numbers are usually public and are chosen from a table of known values. What type of encryption algorithm uses the same key to encrypt and decrypt data? Diffie-Hellman Shared-secret* Public-key Asymmetric Symmetric encryption algorithms use the same key (also called shared secret) to encrypt and decrypt the data. In contrast, asymmetric encryption algorithms (also called public-key) use a pair of keys, one for encryption and another for decryption. How many bits does the Data Encryption Standard (DES) use for data encryption? 40 bits 56 bits* 64 bits 72 bits In what situation would an asymmetric algorithm most likely be used? logging onto a computer making an online purchase* uploading a networking book chapter using FTP transferring a large stream of data between two corporate locations Asymmetric algorithms are slow, so they are commonly used in low-volume transactions such as making online purchases or logging into a financial website. Why is asymmetric algorithm key management simpler than symmetric algorithm key management? It uses fewer bits. Only one key is used. Two public keys are used for the key exchange. One of the keys can be made public.* Asymmetric algorithms use two keys, a public and a private key. Key management is simpler because one of the keys can be made public. What is the purpose of code signing? source identity secrecy integrity of source .EXE files* reliable transfer of data data encryption Code signing is used to verify the integrity of executable files downloaded from a vendor website. Code signing uses digital certificates to authenticate and verify the identity of a website. Which algorithm can ensure data confidentiality? Data confidentiality is ensured through symmetric encryption algorithms, including DES, 3DES, and AES What is the purpose of a digital certificate? It guarantees that a website has not been hacked. It authenticates a website and establishes a secure connection to exchange confidential data.* It provides proof that data has a traditional signature attached. It ensures that the person who is gaining access to a network device is authorized. Digital signatures commonly use digital certificates that are used to verify the identity of the originator in order to authenticate a vendor website and establish an encrypted connection to exchange confidential data. One such example is when a person logs into a financial institution from a web browser. Fill in the blank. A shared secret is a symmetric key used in a encryption algorithm.