Passed Cisco 350-018 Exam with Pass4sure and Lead2pass PDF & VCE (191-200)

QUESTION 191
Which three statements about triple DES are true? (Choose three.)

A. For 3DES, ANSI X9.52 describes three options for the selection of the keys in a bundle, where all keys are independent.
B. A 3DES key bundle is 192 bits long.
C. A 3DES keyspace is168 bits.
D. CBC, 64-bit CFB, OFB, and CTR are modes of 3DES.
E. 3DES involves encrypting a 64-bit block of plaintext with the 3 keys of the key bundle.

Answer: BCD

QUESTION 192
Which three options correctly describe the AH protocol? (Choose three.)

A. The AH protocol encrypts the entire IP and upper layer protocols for security.
B. The AH protocol provides connectionless integrity and data origin authentication.
C. The AH protocol provides protection against replay attacks.
D. The AH protocol supports tunnel mode only.
E. The AH protocol uses IP protocol 51.
F. The AH protocol supports IPv4 only.

Answer: BCE

QUESTION 193
Which three features are supported with ESP? (Choose three.)

A. ESP uses IP protocol 50.
B. ESP supports Layer 4 and above encryption only.
C. ESP provides confidentiality, data origin authentication, connectionless integrity, and antireplay service.
D. ESP supports tunnel or transport modes.
E. ESP has less overhead and is faster than the AH protocol.
F. ESP provides confidentiality, data origin authentication, connection-oriented integrity, and antireplay service.

Answer: ACD

QUESTION 194
Which three statements are true about TLS? (Choose three.)

A. TLS protocol uses a MAC to protect the message integrity.
B. TLS data encryption is provided by the use of asymmetric cryptography.
C. The identity of a TLS peer can be authenticated using public key or asymmetric cryptography.
D. TLS protocol is originally based on the SSL 3.0 protocol specification.
E. TLS provides support for confidentiality, authentication, and nonrepudiation.

Answer: ACD

QUESTION 195
Which three RADIUS protocol statements are true? (Choose three.)

A. RADIUS protocol runs over TCP 1645 and 1646.
B. Network Access Server operates as a server for RADIUS.
C. RADIUS packet types for authentication include Access-Request, Access-Challenge, Access- Accept, and Access-Reject.
D. RADIUS protocol runs over UDP 1812 and 1813.
E. RADIUS packet types for authentication include Access-Request, Access-Challenge, Access- Permit, and Access-Denied.
F. RADIUS supports PPP, PAP, and CHAP as authentication methods.

Answer: CDF

QUESTION 196
Which three statements about OCSP are correct? (Choose three.)

A. OCSP is defined in RFC2560.
B. OCSP uses only http as a transport.
C. OCSP responders can use RSA and DSA signatures to validate that responses are from trusted entities.
D. A response indicator may be good, revoked, or unknown.
E. OCSP is an updated version SCEP.

Answer: ACD

QUESTION 197
Which three statements describe the security weaknesses of WEP? (Choose three.)

A. Key strength is weak and non-standardized.
B. The WEP ICV algorithm is not optimal for cryptographic integrity checking.
C. There is no key distribution mechanism.
D. Its key rotation mechanism is too predictable.
E. For integrity, it uses MD5, which has known weaknesses.

Answer: ABC

QUESTION 198
In HTTPS session establishment, what does the server hello message inform the client?

A. that the server will accept only HTTPS traffic
B. which versions of SSL/TLS the server will accept
C. which ciphersuites the client may choose from
D. which ciphersuite the server has chosen to use
E. the PreMaster secret to use in generating keys

Answer: D

QUESTION 199

Refer to the exhibit. Which statement regarding the output is true?

A. Every 1800 seconds the secondary name server will query the SOA record of the primary name server for updates.
B. If the secondary name server has an SOA record with the serial number of 10973815, it will initiate a zone transfer on the next cycle.
C. Other DNS servers will cache records from this domain for 864000 seconds (10 days) before requesting them again.
D. Email queries concerning this domain should be sent to "admin@postmaster.cisco.com".
E. Both primary and secondary name servers will clear (refresh) their caches every 7200 seconds to ensure that up-to-date information is always in use.

Answer: B

QUESTION 200
DHCPv6 is used in which IPv6 address autoconfiguration method?

A. stateful autoconfiguration
B. stateless autoconfiguration
C. EUI-64 address generation
D. cryptographically generated addresses

Answer: A

If you want to pass Cisco 350-018 successfully, donot missing to read latest lead2pass Cisco 350-018 practice exams.
If you can master all lead2pass questions you will able to pass 100% guaranteed.

http://www.lead2pass.com/350-018.html