C. Determining the algorithm(s) to use for the IPsec services.
D. Putting in place any cryptographic keys required to provide the requested services.

Correct Answer: A

QUESTION 919
Which of the following Internet Protocol (IP) security headers are defined by the Security Architecture for IP (IPSEC)?

A. The IPv4 and IPv5 Authentication Headers.
B. The Authentication Header Encapsulating Security Payload.
C. The Authentication Header and Digital Signature Tag.
D. The Authentication Header and Message Authentication Code.

Correct Answer: B

QUESTION 920
Which of the following statements are true of IPSec Transport mode?

A. It is required for gateways providing access to internal systems.
B. It can be set-up when end-point is host or communications terminates at end-points.
C. If used in gateway-to-host communication, gateway must act as host.
D. Detective/Administrative Pairing.

Correct Answer: BC

QUESTION 921
What is called the standard format that was established to set up and manage Security Associations (SA) on the Internet in IPSec?

A. Internet Key Exchange
B. Secure Key Exchange Mechanism
C. Oakley
D. Internet Security Association and Key Management Protocol

Correct Answer: D

Download Full Version CISSP Exam Dumps(Updated in Feb/2023)

QUESTION 922

What is the purpose of the Encapsulation Security Payload (ESP) in the Internet Protocol (IP) Security Architecture for Internet Protocol Security?

A. To provide non-repudiation and confidentiality for IP transmission.
B. To provide integrity and confidentiality for IP transmissions.
C. To provide integrity and authentication for IP transmissions.
D. To provide key management and key distribution for IP transmissions.

Correct Answer: B

QUESTION 923

Which one of the following is a circuit level application gateway and works independent of any supported TCP/IP application protocol?

A. SOCK-et-S (SOCKS)
B. Common Information Model (CIM)
C. Secure Multipurpose Internet Mail Extension (S/MIME)
D. Generic Security Service Application Programming Interface (GSS-API)

Correct Answer: A

QUESTION 924

How does the SOCKS protocol secure Internet Protocol (IP) connections?

A. By negotiating encryption keys during the connection setup.
B. By attaching Authentication Headers (AH) to each packet.
C. By distributing encryption keys to SOCKS enabled applications.
D. By acting as a connection proxy.

Correct Answer: D

QUESTION 925

In the TCP/IP protocol stack, at what level is the SSL (Secure Sockets Layer) protocol provided?

A. Application
B. Network
C. Presentation
D. Session

Correct Answer: A

CISSP Exam Dumps CISSP PDF Dumps CISSP VCE Dumps CISSP Q&As
https://www.ensurepass.com/CISSP.html

QUESTION 926

SSL (Secure Sockets Layer) has two possible 'session key' lengths, what are they?

A. 40 bit & 54 bit

B. 40 bit & 128 bit

C. 64 bit & 128 bit

D. 128 bit & 256 bit

Correct Answer: B

QUESTION 927

Which of the following is NOT true of SSL?

A. By convention is uses ‘s-http://’ instead of ‘http://’.

B. It stands for Secure Sockets Layer.

C. It was developed by Netscape.

D. IT is used for transmitting private documents over the internet.

Correct Answer: A

QUESTION 928

Which SSL version offers client-side authentication?

A. SSL v1

B. SSL v2

C. SSL v3

D. SSL v4

Correct Answer: B

QUESTION 929

In which way does a Secure Socket Layer (SSL) server prevent a “man-in-the-middle” attack?

A. It uses signed certificates to authenticate the server’s public key.

B. A 128 bit value is used during the handshake protocol that is unique to the connection.

C. It uses only 40 bits of secret key within a 128 bit key length.

D. Every message sent by the SSL includes a sequence number within the message contents.

Correct Answer: A

QUESTION 930

Secure Shell (SSH) and Secure Sockets Layer (SSL) are very heavily used for protecting

A. Internet transactions

B. Ethernet transactions

C. Telnet transactions

D. Electronic Payment transactions

Correct Answer: A

QUESTION 931

Which one of the following CANNOT be prevented by the Secure Shell (SSH) program?

A. Internet Protocol (IP) spoofing.

B. Data manipulation during transmissions.

C. Network based birthday attack.

D. Compromise of the source/destination host.

Correct Answer: D

QUESTION 932

Another name for a VPN is a:

A. tunnel

B. one-time password

C. pipeline

D. bypass

Correct Answer: A

QUESTION 933

Which one of the following attacks is MOST effective against an Internet Protocol Security (IPSEC) based virtual private network (VPN)?

A. Brute force

B. Man-in-the-middle

C. Traffic analysis

D. Replay

Correct Answer: B

QUESTION 934

Which of the following is NOT an essential component of a VPN?

A. VPN Server
B. NAT Server
C. authentication
D. encryption

Correct Answer: B

QUESTION 935

Virtual Private Network software typically encrypts all of the following EXCEPT

A. File transfer protocol
B. Data link messaging
C. HTTP protocol
D. Session information

Correct Answer: B

QUESTION 936

Which of the following is less likely to be used in creating a Virtual Private Network?

A. L2TP
B. PPTP
C. IPSec
D. L2F

Correct Answer: D

QUESTION 937

Which one of the following instigates a SYN flood attack?

A. Generating excessive broadcast packets.
B. Creating a high number of half-open connections.
C. Inserting repetitive Internet Relay Chat (IRC) messages.
D. A large number of Internet Control Message Protocol (ICMP) traces.

Correct Answer: B