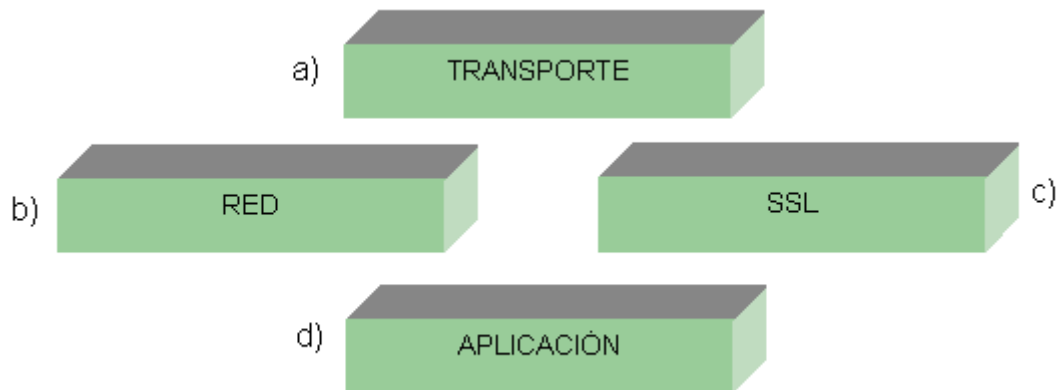


Parcial de Seguridad (sólo la parte de IPsec y SSL):

Pregunta 1:



Establezca el orden correcto (descendiente) de las capas mostradas en la figura siguiendo la secuencia establecida para conexiones seguras utilizando el esquema del Secure Sockets Layer.

Repuesta: d, c, a, b.

Pregunta 2:

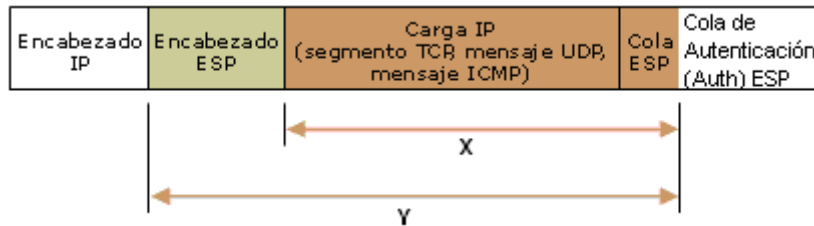
Encabezado IP	Encabezado ESP	Carga IP (segmento TCP, mensaje UDP, mensaje ICMP)	Cola ESP	Cola de Autenticación (Auth) ESP
---------------	----------------	--	----------	-------------------------------------

El paquete mostrado en la figura representa una conexión:

- a) Segura a nivel de capa 3, en modo transporte, con cifrado.
- b) Segura a nivel de capa 4, en modo túnel, con autenticación.
- c) Insegura a nivel de capa 2, en modo transporte, con cifrado y autenticación.
- d) Ninguna de las anteriores.

Respuesta: a)

Pregunta 3:

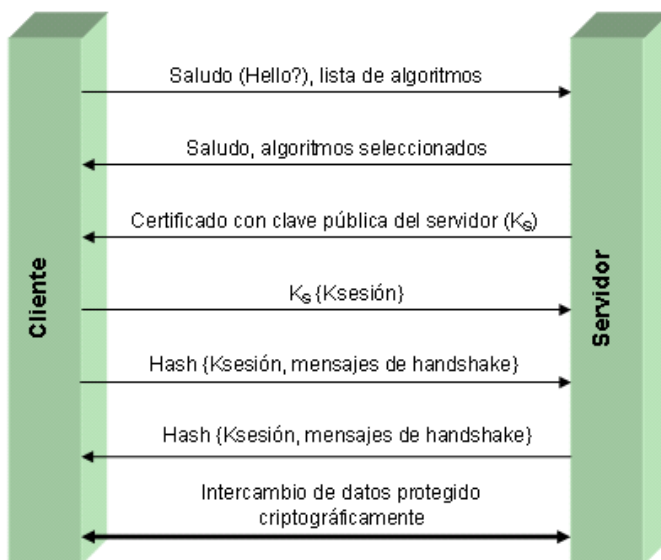


En la figura la X y la Y representan:

- X = Cifrado con el encabezado ESP, Y = Firmado por la cola de autenticación ESP.
- X = Cifrado con la cola ESP, Y = Firmado por la cola de autenticación ESP.
- X = Firmado por la cola de autenticación ESP, Y = Cifrado con el encabezado ESP.
- X = Firmado por el encabezado ESP, Y = Cifrado con el encabezado ESP.
- Ninguna de las anteriores.

Respuesta: a)

Pregunta 4:



La figura anterior representa:

- Los protocolos de SSL: Handshake y Change-Cipher-Spec
- Los protocolos de IPSec: Handshake y Alert
- Los protocolos de SSL: Handshake y Record
- Los protocolos de IPSec: Handshake y Record
- Ninguna de las Anteriores

Respuesta: a)

Pregunta 5:

¿Cuál es la secuencia correcta para el protocolo Record?:

- a) Fragmenta, Comprime, Agrega MAC, Cifra, Añade Cabeceras
- b) Fragmenta, Comprime, Cifra, Agrega MAC, Añade Cabeceras
- c) Fragmenta, Comprime, Añade Cabeceras, Agrega MAC, Cifra
- d) Fragmenta, Agrega MAC, Cifra, Comprime, Añade Cabeceras

Respuesta: a)