Navegación por la prueba de conocimiento
Mostrar una página cada vez
Finalizar revisión

| | |
|---|---|
| Comenzado el | lunes, 21 de enero de 2019, 21:21 |
| Estado | Finalizado |
| Finalizado en | lunes, 21 de enero de 2019, 21:23 |
| Tiempo empleado | 1 minuto 52 s |
| Calificación | 4,00/21,00 |
| Calificación | 1,90 de 10,00 (19%) |

**Pregunta 1**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Donde se sitúa el protocolo TLS?

Selecciona una:
- a. En la capa de red. ✗
- b. En la capa de transporte, por encima de TCP.
- c. En la capa de transporte, por encima de UDP.
- d. En la capa de aplicación.

La respuesta correcta es: En la capa de transporte, por encima de TCP.

**Pregunta 2**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Para qué utiliza el protocolo SSL/TLS la criptografía de clave pública?

Selecciona una:
- a. Para intercambiar claves entre el cliente y el servidor.
- b. Para negociar el algoritmo de cifrado simétrico que debe utilizarse. ✗
- c. Para la autenticación de los datos (mensajes) y para el cifrado de los mismos.
- d. Para la autenticación de las entidades y para el establecimiento de claves.

La respuesta correcta es: Para la autenticación de las entidades y para el establecimiento de claves.

**Pregunta 3**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuál es la función del protocolo "SSL Change Cipher Spec"?

Selecciona una:
- a. Permitir a los puntos de comunicación negociar un cipher suite y (opcionalmente) un método de compresión.
- b. Permitir a los puntos de comunicación indicar posibles problemas potenciales.
- c. Permitir a los puntos de comunicación activar el cipher suite.
- d. Permitir que los puntos de comunicación se autentiquen mutuamente. ✗

La respuesta correcta es: Permitir a los puntos de comunicación activar el cipher suite.

**Pregunta 4**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Que es lo que el protocolo "SSL Handshake Protocol" permite al servidor y al cliente?

Selecciona una:
- a. Autenticarse mutuamente.
- b. Negociar un algoritmo de cifrado y una función MAC. ✗
- c. Negociar las claves a usar para proteger los datos del SSL record.
- d. Todos los anteriores.

La respuesta correcta es: Todos los anteriores.

**Pregunta 5**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

Indica aquella respuesta en el que las fases del protocolo "SSL Handshake Protocol" se encuentren en orden:

Selecciona una:
- a. client_hello, server_key_exchange, client_key_exchange, change_cipher_spec.
- b. client_hello, server_hello_done, server_client_done, change_cipher_spec.
- c. client_hello, client_key_exchange, server_key_exchange, change_cipher_spec. ✗
- d. client_hello, server_start_negotiation, server_finish_negotiation, change_cipher_spec.

La respuesta correcta es: client_hello, server_key_exchange, client_key_exchange, change_cipher_spec.

**Pregunta 6**
Correcta
Puntúa 1,00 sobre 1,00
Marcar pregunta

¿Cuál es la propiedad principal que proporciona DHE (Diffie Hellman Efímero)?

Selecciona una:
- a. Backward secrecy.
- b. Ephemeral secrecy.
- c. Key Management.
- d. Forward secrecy. ✓

La respuesta correcta es: Forward secrecy.

**Pregunta 7**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuál es el orden de las operaciones en el SSL Record Protocol?

Selecciona una:
- a. Fragmentar paquete, añadir MAC, cifrar, comprimir. ✗
- b. Fragmentar paquete, cifrar, comprimir, añadir MAC.
- c. Fragmentar paquete, comprimir, añadir MAC, cifrar.
- d. Fragmentar paquete, cifrar, añadir MAC, comprimir.

La respuesta correcta es: Fragmentar paquete, comprimir, añadir MAC, cifrar.

**Pregunta 8**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuáles son las novedades de TLSv1.3 con respecto a las versiones anteriores?

Selecciona una:
- a. Reduce el tiempo de "handshake", reduce el número de modos de operación soportados (limitándolo a GCM y CCM).
- b. Incluye SHA-256 y SHA-3 (Keccak) dentro del cipher suite.
- c. Rediseña completamente el "SSL Handshake Protocol".
- d. Incluye AES en el cipher suite, y añade la criptografía de clave pública basada en curvas elípticas. ✗

La respuesta correcta es: Reduce el tiempo de "handshake", reduce el número de modos de operación soportados (limitándolo a GCM y CCM).

**Pregunta 9**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Donde se puede utilizar IPsec?

Selecciona una:
- a. Únicamente sobre IPv6. ✗
- b. Sobre IPv4 e IPv6.
- c. Sobre TCP.
- d. Únicamente sobre IPv4.

La respuesta correcta es: Sobre IPv4 e IPv6.

**Pregunta 10**
Correcta
Puntúa 1,00 sobre 1,00
Marcar pregunta

¿Qué es lo que proporciona el protocolo ESP?

Selecciona una:
- a. Todos los anteriores.
- b. Generación y distribución de claves criptográficas.
- c. Integridad y autenticación del origen de datos.
- d. Confidencialidad, integridad y autenticación del origen de datos. ✓

La respuesta correcta es: Confidencialidad, integridad y autenticación del origen de datos.

**Pregunta 11**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuando se utiliza el modo túnel?

Selecciona una:
- a. Para proporcionar acceso remoto seguro sobre Internet. ✗
- b. Para comunicar sucursales de forma segura a través de Internet.
- c. Para establecer conectividad extranet e intranet con socios.
- d. Todos los anteriores.

La respuesta correcta es: Todos los anteriores.

**Pregunta 12**
Correcta
Puntúa 1,00 sobre 1,00
Marcar pregunta

En el modo de transporte, si se utiliza ESP,...

Selecciona una:
- a. Se autentica el payload y algunas porciones de la cabecera.
- b. Se autentica todo el paquete original y algunas partes de la cabecera externa.
- c. Se cifra y opcionalmente autentica todo el paquete IP original.
- d. Se cifra y opcionalmente autentica el payload, pero no la cabecera. ✓

La respuesta correcta es: Se cifra y opcionalmente autentica el payload, pero no la cabecera.

**Pregunta 13**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

En el protocolo AH, ¿Cómo se indica que estamos en modo túnel?

Selecciona una:
- a. El campo "proto" de la cabecera IP indica "AH".
- b. El campo "proto" de la cabecera IP indica "ESP".
- c. El campo "next" de la cabecera AH indica "TCP". ✗
- d. El campo "next" de la cabecera AH indica "IP".

La respuesta correcta es: El campo "next" de la cabecera AH indica "IP".

**Pregunta 14**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Qué es una política de seguridad, o "Security Policy", en IPsec?

Selecciona una:
- a. Define el modo en el que va a viajar el tráfico entre dos puntos (IP origen y destino, puerto origen y destino, modo de protección).
- b. Define el modo en el que se protege el tráfico IPsec (modo túnel o transporte, protocolos a utilizar). ✗
- c. Es un conjunto de reglas que definen las acciones a tomar dentro de una empresa en materia de seguridad.
- d. Es una base de datos que almacena las asociaciones de seguridad temporales.

La respuesta correcta es: Define el modo en el que va a viajar el tráfico entre dos puntos (IP origen y destino, puerto origen y destino, modo de protección).

**Pregunta 15**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuál es el orden de los campos del protocolo ESP con soporte de autenticación?

Selecciona una:
- a. SPI, Sequence number, Encrypted payload, Padding, Pad length, Next header. ✗
- b. SPI, Sequence number, Encrypted payload, Padding, Pad length, Authentication data, Next header.
- c. SPI, Sequence number, Encrypted payload, Padding, Pad length, Next header, Authentication data.
- d. Next header, Header length, SPI, Sequence number, Authentication data.

La respuesta correcta es: SPI, Sequence number, Encrypted payload, Padding, Pad length, Next header, Authentication data.

**Pregunta 16**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuáles son los mensajes intercambiados en el modo principal de ISAKMP?

Selecciona una:
- a. g^a mod p + "Alice" + Crypto offered; g^b mod p + Crypto selected, proof_bob; proof_alice
- b. Crypto offered; Crypto selected; g^a mod p; g^b mod p; K("Alice", proof_alice); K("Bob", proof_bob)
- c. g^a mod p + "Alice" + Crypto offered; g^b mod p + Crypto selected, K(proof_bob); K(proof_alice)
- d. g^a mod p; g^b mod p; K("Alice", proof_alice); K("Bob", proof_bob) ✗

La respuesta correcta es: Crypto offered; Crypto selected; g^a mod p; g^b mod p; K("Alice", proof_alice); K("Bob", proof_bob)

**Pregunta 17**
Correcta
Puntúa 1,00 sobre 1,00
Marcar pregunta

¿Qué es una zona desmilitarizada en una red informática?

Selecciona una:
- a. Una subred que permite a una empresa acceder de forma segura a Internet.
- b. Un área donde la actividad militar no está permitida.
- c. Una subred situada entre la red interna de un organización y las redes externas como Internet. ✓
- d. Una subred que divide las redes internas de las organizaciones en varios compartimentos.

La respuesta correcta es: Una subred situada entre la red interna de un organización y las redes externas como Internet.

**Pregunta 18**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuando se puede ejecutar una regla POSTROUTING en iptables?

Selecciona una:
- a. Después de NAT ✗
- b. Después de OUTPUT
- c. Después de FORWARD
- d. Después de OUTPUT y FORWARD

La respuesta correcta es: Después de OUTPUT y FORWARD

**Pregunta 19**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuál es el tamaño de la clave secreta en WEP?

Selecciona una:
- a. 80 bits.
- b. 40 bits.
- c. 128 bits.
- d. 64 bits. ✗

La respuesta correcta es: 40 bits.

**Pregunta 20**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuál es el protocolo de autenticación definido en el estándar 802.1X?

Selecciona una:
- a. PSK.
- b. IAP.
- c. TKIP. ✗
- d. EAP.

La respuesta correcta es: EAP.

**Pregunta 21**
Incorrecta
Puntúa 0,00 sobre 1,00
Marcar pregunta

¿Cuántas claves son necesarias para proteger las comunicaciones en 802.11i en caso de utilizar el modo AES-CBC?

Selecciona una:
- a. 1. ✗
- b. 802.11i no utiliza el modo AES-CBC.
- c. Ninguna.
- d. 2.

La respuesta correcta es: 2.

Finalizar revisión


© Todos los derechos reservados