

[UMA](#) / [CV](#) / [E.T.S. de Ingeniería Informática](#) / [Mis asignaturas en este Centro](#) / [Curso académico 2023-2024](#)

/ [Grado en Ingeniería Informática. Plan 2010](#)

/ [Seguridad de la Información \(2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B\)](#)

/ [Tema 5: Seguridad en redes TCP/IP](#) / [Test 5 - Tema 5](#)

Comenzado el	jueves, 21 de diciembre de 2023, 16:38
Estado	Finalizado
Finalizado en	jueves, 21 de diciembre de 2023, 16:43
Tiempo empleado	5 minutos 24 s
La puntuación	21,00/21,00
Calificación	10,00 de 10,00 (100%)

Pregunta 1

Correcta

Puntúa 1,00 sobre 1,00

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

Selecciona una:

- ☐ a. Ninguna.
- ☒ b. 2.
- ☐ c. 1.
- ☐ d. 802.11i no utiliza el modo AES-CBC.



La respuesta correcta es: 2.

Pregunta 2

Correcta

Puntúa 1,00 sobre 1,00

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

Selecciona una:

- ☒ a. Forward secrecy.
- ☐ b. Backward secrecy.
- ☐ c. Key Management.
- ☐ d. Ephemeral secrecy.



La respuesta correcta es: Forward secrecy.

Pregunta 3

Correcta

Puntúa 1,00 sobre 1,00

¿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, añadir MAC, comprimir.
- ☒ c. Fragmentar paquete, comprimir, añadir MAC, cifrar.
- ☐ d. Fragmentar paquete, cifrar, comprimir, añadir MAC.



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

Pregunta 4

Correcta

Puntúa 1,00 sobre 1,00

¿Cuándo se utiliza el modo túnel?

Selecciona una:

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



La respuesta correcta es: Todos los anteriores.

Pregunta 5

Correcta

Puntúa 1,00 sobre 1,00

¿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 autenticuen mutuamente.



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

Pregunta 6

Correcta

Puntúa 1,00 sobre 1,00

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

Selecciona una:

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



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

Pregunta 7

Correcta

Puntúa 1,00 sobre 1,00

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

Selecciona una:

- ☒ a. Crypto offered; Crypto selected; $g^a \text{ mod } p$; $g^b \text{ mod } p$; K("Alice", proof_alice); K("Bob", proof_bob)
- ☐ b. $g^a \text{ mod } p$ + "Alice" + Crypto offered; $g^b \text{ mod } p$ + Crypto selected, K(proof_bob); K(proof_alice)
- ☐ c. $g^a \text{ mod } p$; $g^b \text{ mod } p$; K("Alice", proof_alice); K("Bob", proof_bob)
- ☐ d. $g^a \text{ mod } p$ + "Alice" + Crypto offered; $g^b \text{ mod } p$ + Crypto selected, proof_bob; proof_alice



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

Pregunta 8

Correcta

Puntúa 1,00 sobre 1,00

¿Qué es una zona desmilitarizada en una red informática?

Selecciona una:

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



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


Pregunta 9

Correcta

Puntúa 1,00 sobre 1,00

¿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. Es un conjunto de reglas que definen las acciones a tomar dentro de una empresa en materia de seguridad.
- ☐ c. Es una base de datos que almacena las asociaciones de seguridad temporales.
- ☐ d. Define el modo en el que se protege el tráfico IPsec (modo tunel o transporte, protocolos a utilizar).

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 10

Correcta

Puntúa 1,00 sobre 1,00

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

Selecciona una:

- ☐ a. 80 bits.
- ☐ b. 64 bits.
- ☐ c. 128 bits.
- ☒ d. 40 bits. 

La respuesta correcta es: 40 bits.


Pregunta 11

Correcta

Puntúa 1,00 sobre 1,00

¿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, Authentication data, Next header.
- ☒ b. SPI, Sequence number, Encrypted payload, Padding, Pad length, Next header, Authentication data. 
- ☐ c. Next header, Header length, SPI, Sequence number, Authentication data.
- ☐ d. SPI, Sequence number, Encrypted payload, Padding, Pad length, Next header.

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

Pregunta 12

Correcta

Puntúa 1,00 sobre 1,00

¿Qué es lo que proporciona el protocolo ESP?

Selecciona una:

- ☒ a. Confidencialidad, integridad y autenticación del origen de datos.
- ☐ b. Integridad y autenticación del origen de datos.
- ☐ c. Todos los anteriores.
- ☐ d. Generación y distribución de claves criptográficas.



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

Pregunta 13

Correcta

Puntúa 1,00 sobre 1,00

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

Selecciona una:

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



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

Pregunta 14

Correcta

Puntúa 1,00 sobre 1,00

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

Selecciona una:

- ☐ a. TKIP.
- ☐ b. IAP.
- ☒ c. EAP.
- ☐ d. PSK.



La respuesta correcta es: EAP.

Pregunta 15

Correcta

Puntúa 1,00 sobre 1,00

¿Donde se puede utilizar IPsec?

Selecciona una:

- ☐ a. Únicamente sobre IPv4.
- ☒ b. Sobre IPv4 e IPv6.
- ☐ c. Únicamente sobre IPv6.
- ☐ d. Sobre TCP.



La respuesta correcta es: Sobre IPv4 e IPv6.

Pregunta 16

Correcta

Puntúa 1,00 sobre 1,00

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

Selecciona una:

- ☐ a. El campo "proto" de la cabecera IP indica "ESP".
- ☐ b. El campo "next" de la cabecera AH indica "TCP".
- ☐ c. El campo "proto" de la cabecera IP indica "AH".
- ☒ d. El campo "next" de la cabecera AH indica "IP".



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

Pregunta 17

Correcta

Puntúa 1,00 sobre 1,00

¿Donde se sitúa el protocolo TLS?

Selecciona una:

- ☐ a. En la capa de aplicación.
- ☒ 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 red.



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

Pregunta 18

Correcta

Puntúa 1,00 sobre 1,00

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

Selecciona una:

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



La respuesta correcta es: Todos los anteriores.

Pregunta 19

Correcta

Puntúa 1,00 sobre 1,00

¿Cuando se puede ejecutar una regla POSTROUTING en iptables?

Selecciona una:

- ☐ a. Después de FORWARD
- ☐ b. Después de NAT
- ☐ c. Después de OUTPUT
- ☒ d. Después de OUTPUT y FORWARD



La respuesta correcta es: Después de OUTPUT y FORWARD

Pregunta 20

Correcta

Puntúa 1,00 sobre 1,00

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

Selecciona una:

- ☐ a. client_hello, client_key_exchange, server_key_exchange, change_cipher_spec.
- ☐ b. client_hello, server_start_negotiation, server_finish_negotiation, change_cipher_spec.
- ☐ c. client_hello, server_hello_done, server_client_done, change_cipher_spec.
- ☒ d. client_hello, server_key_exchange, client_key_exchange, change_cipher_spec.



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

Pregunta 21

Correcta

Puntúa 1,00 sobre 1,00

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

Selecciona una:

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



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

◀ Tema 5: Seguridad en redes TCP/IP (parte 4) - Caso de uso - redes inalámbricas

Saltar a...



Relación de ejercicios - TLS ►