DATOS PERSONALES		FIRMA
Nombre: DNI:		
Apellidos:		
ESTUDIO	**ASIGNATURA**	**CONVOCATORIA**
MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD (PLAN 2022)	14135.- SEGURIDAD EN REDES Y ANÁLISIS INTELIGENTE DE AMENAZAS	Ordinaria Número periodo 5732
FECHA	**MODELO**	**CIUDAD DEL EXAMEN**
03-05/03/2023	Modelo - C	
Etiqueta identificativa		

INSTRUCCIONES GENERALES

1. **Lee atentamente** todas las preguntas antes de empezar.
2. La duración del examen es de **2 horas**.
3. Escribe únicamente con **bolígrafo azul o negro**.
4. No está permitido utilizar más hojas de las que te facilita la UNIR (puedes utilizar folios para hacerte esquemas u organizarte, pero **no se adjuntarán al examen**).
5. **El examen** PRESENCIAL **supone el 60%** de la calificación final de la asignatura. Es necesario aprobar el examen, para tener en cuenta la evaluación continua, aunque esta última sí se guardará para la siguiente convocatoria en caso de no aprobar el examen.
6. No olvides **rellenar EN TODAS LAS HOJAS los datos del cuadro** que hay en la parte superior con tus datos personales.
7. El **DNI/NIE/PASAPORTE debe estar sobre la mesa** y disponible para su posible verificación.
8. **Apaga el teléfono móvil**.
9. Las preguntas se contestarán en **CASTELLANO**.
10. El profesor tendrá muy en cuenta las **faltas de ortografía** en la calificación final.
11. **No se permite el uso de calculadora.**

Puntuación

Test

- Puntuación máxima 4.00 puntos

Desarrollo teórico.

- Puntuación máxima 6.00 puntos

Tenga en cuenta que:

- Cada pregunta vale 0,4 puntos.
- Las preguntas sin contestar ni suman ni restan.
- Las preguntas mal contestadas NO restan.
- Solamente hay opción válida en cada pregunta.

1. ¿Cuál de los siguientes campos de un paquete ESP permite identificar la asociación de seguridad a emplear?

A. ESP Payload.
B. Security Parameter Index.
C. Sequence Number Field.
D. Encrypted Data And Paramenters.

2. Selecciona la opción VERDADERA sobre el protocolo WPA:

A. Usa el algoritmo de cifrado DES.
B. Usa claves que van cambiando con el tiempo.
C. El vector de inicialización es de 16 bits.
D. Sus fallos de seguridad fueron corregidos con la publicación del protocolo WEP.

3. De las siguientes listas selecciona la que se corresponde únicamente con mecanismos de seguridad:

A. Firma digital, no repudio, confidencialidad.
B. Control de acceso, cifrado y autenticación.
C. Confidencialidad, integridad y no repudio.
D. Cifrado, firma digital y mecanismo de control de acceso.

4. ¿Cuál de las siguientes afirmaciones es FALSA acerca de IPv6?

A. IPv6 tiene integrado IPSec.

B. IPv6 permite multicast.
C. Las direcciones en IPv6 tienen un tamaño de 128 bytes.
D. Permite paquetes con una carga útil de hasta 4GiB.

5. Los sistemas del tipo Padded Cell:

A. Funcionan de manera independiente a los IDS.
B. Funcionan de manera independiente a los NIDS (IDS en red).
C. Cuando detectan un ataque desencadenan acciones preventivas.
D. El sistema "Bait and Switch" de Snort es un ejemplo real.

6. ¿Cuál de las siguientes opciones no es un ataque activo?

A. Captura de tráfico.
B. Repetición.
C. Suplantación de identidad.
D. Modificación de mensajes.

7. Los sistemas NIDS:

A. Impiden que un atacante pueda penetrar en un sistema de información.
B. Solamente analizan el tráfico que tiene como destino el equipo en el que están desplegados.
C. Bloquean conexiones que sean sospechosas de formar parte de un ataque.
D. Ninguna de las anteriores.

8. ¿Cuál de las siguientes afirmaciones es VERDADERA acerca de una zona demilitarizada (DMZ)?

A. En ella se ubican los servidores que deben permanecer accesibles desde el exterior
B. Su uso evita la colocación de cortafuegos del tipo router de filtrado de paquetes
C. Se trata de una red de la empresa donde no existen protecciones a los sistemas en ella ubicados.
D. Ninguna de las anteriores

9. El protocolo TCP:

A. Es un protocolo de la capa de red.
B. Es un protocolo que no está orientado a conexión.
C. Es un protocolo de la capa de transporte.
D. Ninguna de las anteriores.

10. ¿Cuál de las siguientes funcionalidades no son provistas por un cortafuegos?

A. Bloqueo de tráfico no deseado.
B. Ocultación de sistemas vulnerables.
C. Proporcionar un repositorio unificado de incidentes de red de todo tipo.
D. Control de tráfico hacia y desde la red privada.

PLANTILLA DE RESPUESTAS

Preguntas / Opciones	A	B	C	D
1	X			
2		X		
3		X		
4			X	
5				X
6	X			
7				X
8	X			
9			X	
10			X	

Código de examen: 203205

Tenga en cuenta que:

- Debe contestar de la forma más detallada posible a las siguientes preguntas.
- Cada pregunta vale 3 puntos.

1. (3 puntos: la puntuación de cada apartado se especifica en el enunciado)

HoneyPots e IDS:

1. (1 punto) Describa qué son los honeypots y cómo pueden ayudar a mejorar la seguridad de un sistema de información.
2. (1 punto) Describa qué son los IDS y qué servicios de seguridad suministran.
3. (1 punto)Describa las diferencias entre un IPS y un IDS y cuales son las principales ventajas y desventajas de la utilización de un IPS frente a un IDS.

(Responder en 2 caras)

R:

1.1 **Honeypots:** Son sistemas de seguridad tipo trampa donde son redirigidos los atacantes y permite que estos no ingresen como tal a la red e ingresan a una red secundaria donde estos pueden ser monitorizados en sus actividades y/o intrucciones, estos mejoran la seguridad de un sistema de información en base a la redirección de los atacantes a este sistema trampa impidiendo así que ingresen a la información principal, adicional tambien son de ayuda segun la monitorización de estos atacantes para ver sus modelos y niveles de ataque, se puede crear un sistema de seguridad a traves de lo que se visualiza.

1.2 **IDS:** Intuction Detection System o Sistema de detección de Intrusos actua de forma de monitor de la red reportando detecciones de intrusos al sistema, cabe recalcar que no bloquea, solo genera reportes ya sea a un administrador a otros dispositivos configurados en la red, alertando que se detectaron accesos o intrucciones no debidas los cuales pueden ser un peligro para el sistema, estos deben estar siempre actualizados y se dividen en dos tipos:

- NIDS: Sistema de deteccion de intrusos de red, actuan de monitor de toda la red en la cual fueron configurados.
- HIDS: Sistema de deteccion de intrusos de host, actuan sobre un equipo específico en el que fueron configurados.

1.3 **IPS vs IDS:** La diferencia entre un sistema de deteccion de intrusos y un sistema de protección de intrusos radica en su nombre, mientras el uno actua solamente de sniffer o monitor de la red esperando una anomalía, el otro actua en cuanto se detecta esta anomalía bloueando o a su vez redirigiendo el trafico detectado a un sistema trampa para salvaguardar la red y/o monitorizar las acciones del atacante.
Como ventaja de IPS se puede dar en su concepto, es un sitema que bloquea al posible atacante segun sus criterios configurados, mientras que IDS solamente es un monitor de la red que da alertas al detectar.
Se puede recalcar que como desventaja la mejor opción es un trabajo en conjunto de los dos sistemas, minetras que un IDS detecta el intruso, alerta al IPS y este bloquea al intruso como tal.

2. (3 puntos: la puntuación de cada apartado se especifica en el enunciado)

1. (1 punto) Describa cuáles son los objetivos del subprotocolo Handshake de TLS/SSL.
2. (2 puntos) Realice un gráfico de la comunicación entre un cliente y un servidor durante la ejecución del subprotocolo Handshake en el que se detallen los mensajes que se intercambian, indicando los mensajes que son opcionales.

(Responder en 2 caras)

2.1. Objetivo protocolo Handshake de TLS/SSL

El objetivo principal del protocolo Hansshake es ofrecer una autenticación segura y confiable entre una negociación entre el cliente y el servidor, donde se comparte y verifica tanto certificados como claves para proceder a establecer la conección segura y teniendo en cuenta la autenticidad, confidencialidad y disponibilidad.

2.2. Gráfico de comunicación Handshake

FASE	Cliente	Servidor
1	Client Hello	Server Hello
2		Certificate Server Key Exchange Certificate Server Hello Done
3	Certificate Client Key Exchange Certificate	
4	Change Chipper Spec Finished	Change Chipper Spec Finished
Comunicación	Data	Data