Comenzado el	viernes, 27 de septiembre de 2024, 09:01
Estado	Finalizado
Finalizado en	viernes, 27 de septiembre de 2024, 09:22
Tiempo empleado	21 minutos 30 segundos
Puntos	24,67/30,00
Calificación	**8,22** de 10,00 (**82,22**%)

Pregunta **1**

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

Los sistemas habituales utilizados para la detección y contención de código malicioso son los IPS/IDS, Antivirus y Firewall

- (•) Verdadero
- ( ) Falso

La respuesta correcta es 'Verdadero'

Pregunta **2**

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

Un incidente de seguridad es cualquier evento que puede afectar a la integridad, confidencialidad y disponibilidad de la información

- (•) Verdadero
- ( ) Falso

La respuesta correcta es 'Verdadero'

Pregunta **3**

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

La CONTENCIÓN DE UN INCIDENTE es devolver los sistemas, dispositivos y equipos a su estado original antes de producirse el incidente

- ( ) Verdadero
- (•) Falso

La respuesta correcta es 'Falso'

Pregunta **4**

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

En el análisis forense informático, las EVIDENCIAS VOLÁTILES son las que se almacenan en el sistema de ficheros y no se pierden al apagar el equipo

- ( ) Verdadero
- (•) Falso

La respuesta correcta es 'Falso'

Pregunta **5**

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

Dentro de los incidentes de seguridad informática, los ingresos y operaciones no autorizadas a los sistemas son incidentes de DENEGACIÓN DE SERVICIO

- ( ) Verdadero
- (•) Falso

La respuesta correcta es 'Falso'

Pregunta **6**

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

La colocación sistemas NIDPS delante del cortafuegos externo permite una monitorización de los ataques contra la infraestructura de una organización, principalmente los dirigidos contra el firewall de la red

- (•) Verdadero
- ( ) Falso

La respuesta correcta es 'Verdadero'

Pregunta **7**

Correcta

Se habla de POLÍTICA DE RESPUESTA ACTIVA cuando el sistema IDS/IPS detecta una intrusión, además de generar una alarma, modifica el entorno para evitar que la intrusión tenga éxito

Se puntúa 1,00 sobre 1,00

Marcar pregunta

- (•) Verdadero
- ( ) Falso

La respuesta correcta es 'Verdadero'

Pregunta 8

Incorrecta

Se puntúa 0,00 sobre 1,00

Marcar pregunta

Se habla de VERDADERO POSITIVO cuando el IDS/IPS detecta como ataque el tráfico de datos que en verdad es inofensivo

- (•) Verdadero
- ( ) Falso

La respuesta correcta es 'Falso'

Pregunta 9

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

LOS ARCHIVOS DE REGISTRO O ARCHIVOS DE LOG son una fuente importante de seguridad y de solución de problemas

- (•) Verdadero
- ( ) Falso

La respuesta correcta es 'Verdadero'

Pregunta 10

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

Un CERT/CSIRT está formado por un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información

- (•) Verdadero
- ( ) Falso

La respuesta correcta es 'Verdadero'

Pregunta 11

Incorrecta

Se puntúa -0,33 sobre 1,00

Marcar pregunta

Los IDS que tienen como función principal la detección de comportamientos inusuales que sucedan en un host de una red son los IDS…

- ( ) a. de detección de anomalías
- (•) b. basados en host (HIDS)
- ( ) c. de detección de abusos o firmas
- ( ) d. basados en red (NIDS)

Respuesta incorrecta.
La respuesta correcta es: de detección de anomalías

Pregunta 12

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

Dentro de la Gestión de Incidentes, el momento en el que se aplican las medidas correctivas para restaurar el sistema a la situación inicial antes de producirse el incidente, es la fase de…

- ( ) a. Prevención del incidente
- ( ) b. Registro del incidente
- (•) c. Respuesta al incidente
- ( ) d. Análisis del incidente

Respuesta correcta
La respuesta correcta es: Respuesta al incidente

Pregunta 13

Incorrecta

Se puntúa -0,33 sobre 1,00

Para la ubicación de un sistema IDS/IPS, la zona de confianza, en la que cualquier tipo de acceso anómalo que haya en la red hay que considerarlo como acceso hostil, es la Zona…

- ( ) a. Amarilla

Marcar pregunta

b. Azul
c. Verde
d. Roja

Respuesta incorrecta.
La respuesta correcta es: Azul

Pregunta 14
Correcta
Se puntúa 1,00 sobre 1,00
Marcar pregunta

El orden en el que se realizan las fases de un Plan de Prevención de Incidentes es…

a. Preparación y prevención, investigación, análisis preliminar, erradicación y recuperación, contención, detección y notificación y actividades posteriores
b. Preparación y prevención, erradicación y notificación
c. Preparación y prevención, detección y notificación, análisis preliminar, contención, erradicación y recuperación, investigación y actividades posteriores
d. Preparación y prevención, análisis preliminar, contención, erradicación y recuperación, investigación, detección y notificación y actividades posteriores

Respuesta correcta
La respuesta correcta es: Preparación y prevención, detección y notificación, análisis preliminar, contención, erradicación y recuperación, investigación y actividades posteriores

Pregunta 15
Correcta
Se puntúa 1,00 sobre 1,00
Marcar pregunta

Los IPS que tienen como funcionalidad principal bloquear direcciones IP que puedan ser causantes de algún tipo de ataque, son los IPS…

a. de bloqueo de IP
b. con acción de decepción
c. de filtrado de paquetes
d. de autodefinición de firmas

Respuesta correcta
La respuesta correcta es: de bloqueo de IP

Pregunta 16
Correcta
Se puntúa 1,00 sobre 1,00
Marcar pregunta

La capacidad del IDS/IPS para resistir a los ataques y a los fallos del sistema (cortes de electricidad, etc.), es…

a. La precisión
b. El tiempo de respuesta
c. La tolerancia a fallos
d. La completitud

Respuesta correcta
La respuesta correcta es: La tolerancia a fallos

Pregunta 17
Correcta
Se puntúa 1,00 sobre 1,00
Marcar pregunta

Dentro de los códigos maliciosos, las aplicaciones diseñadas con el fin de registrar el comportamiento de un usuario en un ordenador de modo remoto se denominan…

a. Keyloggers
b. Gusanos
c. troyanos
d. Cookies

Respuesta correcta
La respuesta correcta es: Keyloggers

Pregunta 18

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

En el ANÁLISIS FORENSE INFORMÁTICO, la fase en la que se realiza un análisis exhaustivo para reconstruir el timeline del ataque y llegar a su inicio para detectar al atacante, es la fase de…

a. Adquisición de datos y recopilación de evidencias
b. Confirmación de las pruebas realizadas y realización del informe
c. Análisis e investigación de las evidencias
d. Estudio preliminar

Respuesta correcta

La respuesta correcta es: Análisis e investigación de las evidencias

Pregunta 19

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

Cuando el IDS/IPS detecta como ataque el tráfico de datos que en verdad es inofensivo, se habla de...

a. Ataque detectado correctamente
b. Falso positivo
c. Verdadero positivo
d. Falso negativo

Respuesta correcta

La respuesta correcta es: Falso positivo

Pregunta 20

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

En el análisis forense informático, el criterio de admisibilidad de evidencias electrónicas de COMPLETITUD o SUFICIENCIA es…

a. La evidencia debe estar completa, tiene que hacerse manteniendo su integridad
b. El sistema no fue vulnerado y funcionaba correctamente cuando se recibió, almacenó o generó la prueba
c. Las técnicas de recolección y tratamiento de la evidencia deben cumplir las normativas legales vigentes en el ordenamiento jurídico
d. La evidencia debe haber sido generada y registrada en la escena del crimen y debe mostrar que los medios utilizados no se han modificado

Respuesta correcta

La respuesta correcta es: La evidencia debe estar completa, tiene que hacerse manteniendo su integridad

Pregunta 21

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

La ……. es devolver los sistemas, dispositivos y equipos a su estado original antes de producirse el incidente

Respuesta: RESTAURACIÓN

La respuesta correcta es: recuperación

Pregunta 22

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

los ……. Son centros de respuesta a incidentes de seguridad en tecnologías de información formados por expertos encargados de diseñar medidas preventivas y reactivas ante incidentes de seguridad

Respuesta: CSIRT

La respuesta correcta es: cert

Pregunta 23

Incorrecta

Se puntúa 0,00 sobre 1,00

Marcar pregunta

Cuando los intrusos en este caso falsifican la información del sistema atacando a su autenticidad, se habla de un ataque de …….

Respuesta: SUPLANTACIÓN

La respuesta correcta es: fabricación

Pregunta 24
Correcta
Se puntúa 1,00 sobre 1,00
Marcar pregunta

El objetivo principal del análisis ..... es recoger las evidencias digitales presentes en cualquier tipo de incidencia y delito informático

Respuesta: FORENSE

La respuesta correcta es: forense

Pregunta 25
Correcta
Se puntúa 1,00 sobre 1,00
Marcar pregunta

Un ..... es un sistema para detectar accesos no autorizados a un equipo o una red que ante cualquier actividad sospechosa emiten una alerta, pero no tratan de mitigar la intrusión

Respuesta: IDS

La respuesta correcta es: ids

Pregunta 26
Correcta
Se puntúa 1,00 sobre 1,00
Marcar pregunta

Relaciona los términos con las definiciones

Es una solución híbrida centralizada que engloba la gestión de información de seguridad (Security Information Management) y la gestión de eventos (Security Event Manager). es una herramienta en la que se centraliza la información y se integra con otras herramientas de detección de amenazas	SIEM
Es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Además de lanzar alarmas, puede descartar paquetes y desconectar conexiones	IPS
Es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, Ante cualquier actividad sospechosa, emiten una alerta, pero no tratan de mitigar la intrusión	IDS

Respuesta correcta
La respuesta correcta es: Es una solución híbrida centralizada que engloba la gestión de información de seguridad (Security Information Management) y la gestión de eventos (Security Event Manager). es una herramienta en la que se centraliza la información y se integra con otras herramientas de detección de amenazas → SIEM, Es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Además de lanzar alarmas, puede descartar paquetes y desconectar conexiones → IPS, Es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, Ante cualquier actividad sospechosa, emiten una alerta, pero no tratan de mitigar la intrusión → IDS

Pregunta 27
Parcialmente correcta
Se puntúa 0,33 sobre 1,00
Marcar pregunta

Relaciona los términos con sus funciones correspondientes

Sistemas para la recogida, correlación y el análisis de la información de seguridad en diferido	HIDS
Analizando un equipo para comprobar si ha habido algún tipo de alteración de los archivos del sistema operativo y para localizar actividades sospechosas	SIM
Detectan los ataques mediante la captura y análisis de los paquetes de la red. Una vez capturados y analizados los paquetes de la red, los IDS se encargan de buscar patrones que supongan algún tipo de ataque	NIDS

Respuesta parcialmente correcta.
Ha seleccionado correctamente 1.
La respuesta correcta es: Sistemas para la recogida, correlación y el análisis de la información de seguridad en diferido → SIM, Analizando un equipo para comprobar si ha habido algún tipo de alteración de los archivos del sistema operativo y para localizar actividades sospechosas → HIDS, Detectan los ataques mediante la captura y análisis de los paquetes de la red. Una vez capturados y analizados los paquetes de la red, los IDS se encargan de buscar patrones que supongan algún tipo de ataque → NIDS

Pregunta 28
Correcta
Se puntúa 1,00 sobre 1,00
Marcar pregunta

Relaciona las fases de un plan de gesión de incidentes con su definición

Análisis de la amenaza para ver si es una amenaza real o es una falsa alarma. En caso de ser real, análisis de la incidencia para conocer los detalles y los daños ocasionados	ANÁLISIS PRELIMINAR:
Establecimiento de medidas correctivas que minimicen los daños ocasionados y puedan restaurar el sistema a situaciones anteriores a la aparición de la amenaza	CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN
Análisis profundo de la incidencia para conocer detalladamente su procedimiento de ataque y cómo ha podido acceder al sistema	INVESTIGACIÓN

Establecimiento de medidas preventivas que minimicen el riesgo de incidentes en los sistemas de la organización	PREPARACIÓN Y PREVENCIÓN DE INCIDENTES
La investigación del incidente se utiliza para llevar a cabo un procedimiento de aprendizaje que permita el establecimiento de medidas correctivas que impidan que la amenaza sucedida no pueda volver a acceder a los sistemas de la organización	ACTIVIDADES POSTERIORES
Establecimiento de medidas de detección de posibles amenazas y sean capaces de notificar a los responsables su detección	DETECCIÓN Y NOTIFICACIÓN:

Respuesta correcta

La respuesta correcta es: Análisis de la amenaza para ver si es una amenaza real o es una falsa alarma. En caso de ser real, análisis de la incidencia para conocer los detalles y los daños ocasionados → ANÁLISIS PRELIMINAR:, Establecimiento de medidas correctivas que minimicen los daños ocasionados y puedan restaurar el sistema a situaciones anteriores a la aparición de la amenaza → CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN, Análisis profundo de la incidencia para conocer detalladamente su procedimiento de ataque y cómo ha podido acceder al sistema → INVESTIGACIÓN, Establecimiento de medidas preventivas que minimicen el riesgo de incidentes en los sistemas de la organización → PREPARACIÓN Y PREVENCIÓN DE INCIDENTES, La investigación del incidente se utiliza para llevar a cabo un procedimiento de aprendizaje que permita el establecimiento de medidas correctivas que impidan que la amenaza sucedida no pueda volver a acceder a los sistemas de la organización → ACTIVIDADES POSTERIORES, Establecimiento de medidas de detección de posibles amenazas y sean capaces de notificar a los responsables su detección → DETECCIÓN Y NOTIFICACIÓN:

Pregunta **29**

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

Ordene las fases del análisis forense informático

ADQUISICIÓN DE DATOS Y RECOPILACIÓN DE EVIDENCIAS	FASE 2
D. ESTUDIO PRELIMINAR	FASE 1
CONFIRMACIÓN DE LAS PRUEBAS REALIZADAS Y REALIZACIÓN DEL INFORME	FASE 4
ANÁLISIS E INVESTIGACIÓN DE LAS EVIDENCIAS	FASE 3

Respuesta correcta

La respuesta correcta es: ADQUISICIÓN DE DATOS Y RECOPILACIÓN DE EVIDENCIAS → FASE 2, D. ESTUDIO PRELIMINAR → FASE 1, CONFIRMACIÓN DE LAS PRUEBAS REALIZADAS Y REALIZACIÓN DEL INFORME → FASE 4, ANÁLISIS E INVESTIGACIÓN DE LAS EVIDENCIAS → FASE 3

Pregunta **30**

Correcta

Se puntúa 1,00 sobre 1,00

Marcar pregunta

Relaciona los términos con los tipos de sistemas

Sistemas de prevención de incidentes	IPS
Equipos de respuesta de incidentes de seguridad informática	CSIRT
Sistemas de detección y eliminación de código malicioso	ANTIVIRUS
Sistemas de gestión de información y eventos de seguridad	SIEM
Sistemas de detección de intrusos	IDS

Respuesta correcta

La respuesta correcta es: Sistemas de prevención de incidentes → IPS, Equipos de respuesta de incidentes de seguridad informática → CSIRT, Sistemas de detección y eliminación de código malicioso → ANTIVIRUS, Sistemas de gestión de información y eventos de seguridad → SIEM, Sistemas de detección de intrusos → IDS