Examen para IDC06

Intento 1.

Pregunta 1

¿Cuáles de las siguientes labores se asocian con el segundo principio pragmático de la Ciberseguridad?

Seleccione una:

a. La detección y análisis rápido de los incidentes de seguridad.
b. La instalación de la última versión del software infraestructural y de aplicación.
c. La dotación de políticas de respaldo.

Pregunta 2

¿Qué capa de la Torre ISO-OSI se compone de los servicios de comunicación estándar a disposición de cualquier usuario?

Seleccione una:

a. Capa Aplicación.
b. Capa Enlace de Datos.
c. Capa Presentación.
d. Capa Sesión.
e. Capa Física.
f. Capa Red.
g. Capa Transporte.

Pregunta 3

¿En qué capa de la Torre ISO-OSI se sitúa el protocolo ICMP?

Seleccione una:

a. Capa Red.
b. Capa Enlace de Datos.
c. Capa Transporte.
d. Capa Sesión.

Pregunta 4

¿Para qué sirve el protocolo ICMP?

Seleccione una:

a. Para transmitir información de señalización.
b. Para ninguna opción de las anteriores.
c. Para implementar las primitivas de mantenimiento remoto.
d. Para comprobar la alcanzabilidad de una máquina.

Pregunta 5

¿Con qué reglas de detección puede trabajar Snort?:

Seleccione una:

a. Con las reglas de la comunidad si se arranca en Modo Community.
b. Con las reglas personalizadas si se arranca en Modo Custom.
c. Siempre funciona con las reglas de la comunidad y las personalizadas a la vez.

Pregunta 6

¿En qué posición de una regla Snort se sitúa la "Dirección IP Origen"?

Seleccione una:

a. Header.
b. No Aplica.
c. Trailer.

Pregunta 7

¿Qué capa de la Torre ISO-OSI define el hardware de conexión?

Seleccione una:

a. Capa Red.
b. Capa Aplicación.
c. Capa Transporte.
d. Capa Física.
e. Capa Sesión.
f. Capa Enlace de Datos.
g. Capa Presentación.

Pregunta 8

¿Qué capa de la Torre ISO-OSI introduce el concepto de Integridad, asegurando que los datos no se deterioran durante la transferencia?

Seleccione una:

a. Capa Sesión.
b. Capa Aplicación.
c. Capa Presentación.
d. Capa Enlace de Datos.
e. Capa Transporte.
f. Capa Física.
g. Capa Red.

Pregunta 9

¿En qué posición de una regla Snort se sitúa el "Puerto IP Origen"?

Seleccione una:

a. No Aplica.
b. Trailer.
c. Header.

Pregunta 10

¿Qué entidad técnica utiliza Snort para enviar la información de logging a una máquina remota?

Seleccione una:

a. Una Linux Facility.
b. Un Socket.
c. Un Linux Pipe.

Intento 2.

Pregunta 1

¿En qué posición de una regla Snort se sitúa el "Opciones"?

Seleccione una:

a. No Aplica.
b. Trailer.
c. Header.

Pregunta 2

¿En qué posición de una regla Snort se sitúa el "Mensaje"?

Seleccione una:

a. No Aplica.
b. Trailer.
c. Header.

Pregunta 3

¿En qué posición de una regla Snort se sitúa el "Protocolo"?

Seleccione una:

a. No Aplica.
b. Trailer.
c. Header.

Pregunta 4

¿En qué posición de una regla Snort se sitúa la "Acción de la Regla"?

Seleccione una:

a. No Aplica.
b. Trailer.
c. Header.

Pregunta 5

¿Qué estrategia permite estar preparado ante cualquier incidente?

Seleccione una:

a. Las políticas consistentes de respaldos.
b. Las instalaciones gemelas que pueden entrar en acción en cualquier momento.
c. Todas las anteriores.
d. Los planes de acción.
e. Los planes de respuesta.
f. El análisis forense.

Pregunta 6

¿Qué capa de la Torre ISO-OSI introduce el direccionamiento y la comunicación entre diferentes redes?

Seleccione una:

a. Capa Enlace de Datos.
b. Capa Física.
c. Capa Red.
d. Capa Sesión.
e. Capa Aplicación.
f. Capa Presentación.
g. Capa Transporte.

Pregunta 7

¿Para qué se utiliza el protocolo SSH?

Seleccione una:

a. Para las dos funciones anteriores.
b. Para abrir sesiones en máquinas remotas.
c. Para transferir archivos entre máquinas remotas.

Pregunta 8

¿Qué capa de la Torre ISO-OSI habilita el inicio, desarrollo y fin de una transmisión?

Seleccione una:

a. Capa Enlace de Datos.
b. Capa Física.
c. Capa Red.
d. Capa Sesión.
e. Capa Aplicación.
f. Capa Presentación.
g. Capa Transporte.

Pregunta 9

¿Qué capa de la Torre ISO-OSI controla la transferencia de datos en la red?

Seleccione una:

a. Capa Enlace de Datos.
b. Capa Física.
c. Capa Red.
d. Capa Sesión.
e. Capa Aplicación.
f. Capa Presentación.
g. Capa Transporte.

Pregunta 10

¿En qué posición de una regla Snort se sitúa el "Puerto IP Destino"?

Seleccione una:

a. No Aplica.
b. Trailer.
c. Header.

Pregunta 3.

Pregunta 1

¿Qué capa de la Torre ISO-OSI asegura que la información se transfiere de forma comprensible para un sistema?

Seleccione una:

a. Capa Enlace de Datos.
b. Capa Física.
c. Capa Red.
d. Capa Sesión.
e. Capa Aplicación.
f. Capa Presentación.
g. Capa Transporte.

Pregunta 2

¿Cuál es la condición básica para activar Snort como un IPS?

Seleccione una:

a. Que Snort esté en la misma máquina que el SIEM.
b. Disponer de una máquina con al menos dos interfaces de red.
c. Que Snort esté conectado con una base de datos relacional.

Pregunta 3

¿Cuál es la misión de Snort en el SOC?

Seleccione una:

a. Filtrado de la información de los logs.
b. Monitorización de la información.
c. Almacenamiento de la información.
d. Detección y Prevención de Intrusiones.

Pregunta 4

¿En qué posición de una regla Snort se sitúa la "Dirección de la Operación"?

Seleccione una:

a. No Aplica.
b. Trailer.
c. Header.

Pregunta 5

¿Qué funcionalidad tiene Snort?

Seleccione una:

a. Es un IDS con algunas funciones de IPS.
b. Es sólo un IDS.
c. Es un IDS/IPS totalmente funcional.