Examen para IC03

Intento 1.

Pregunta 1

¿Cuáles son las claves del procedimiento de almacenamiento de evidencias?:

a. La Cadena de Custodia de la información.
b. Ambas cosas son claves en este proceso.
c. El almacén lógico/físico de la información.

Pregunta 2

La labor del Equipo Rojo se efectúa:

a. Antes de la aparición del incidente en el entorno.
b. Tras la finalización del incidente.
c. Durante la manifestación del incidente.

Pregunta 3

Señalar el tipo de información que tiene mayor volatilidad:

a. Logs del sistema.
b. Configuración física y topología de la red.
c. Registros y contenido de la caché.
d. Información temporal del sistema.

Pregunta 4

¿Qué se debe hacer para no invalidar el proceso de recolección de información?:

a. No ejecutar programas que modifiquen la fecha y hora de acceso de los ficheros del sistema.
b. No confiar en la información proporcionada por los programas del sistema.
c. Todas las anteriores.
d. No apagar el ordenador hasta que se haya recopilado toda la información.

Pregunta 5

La mejor ventaja posible en la contención de incidentes es:

a. La precisión de la información recopilada.
b. Ninguna de las anteriores.
c. Los metadatos contenidos en la información.
d. El factor tiempo.

Pregunta 6

La mayor parte de las labores de investigación de incidentes tienen por objeto:

a. Identificar Patrones para Prevención de Intrusiones.
b. Búsqueda de Firmas del Malware involucrado.
c. Obtener Información con Valor Legal.
d. Enviar información al Sistema de Gestión de Compliance.

Pregunta 7

Un Sistema de Almacenamiento en red:

a. Tiene por defecto un cifrado de tres niveles.
b. Por defecto no tiene ningún tipo de cifrado.
c. Tiene por defecto un cifrado de dos niveles.
d. Tiene por defecto un cifrado simple.

Pregunta 8

El Principio de Incertidumbre de Heisenberg propugna que:

a. El caos siempre va en aumento.
b. Toda medida causa una interferencia.
c. El gato puede estar simultáneamente vivo y muerto.
d. El universo está en plena expansión.

Pregunta 9

La labor del Equipo Azul se efectúa:

a. Antes de la aparición del incidente en el entorno.
b. Durante la manifestación del incidente.
c. Tras la finalización del incidente.

Pregunta 10

¿Qué se debe hacer con la información recopilada una vez concluido el análisis del incidente?:

a. Respaldar cuidadosamente todos los datos, de cara a las auditorías.
b. Una vez constatada la necesidad de guardar la información, descartar los datos inútiles.
c. Respaldar la información personal durante 7 años, por imperativo legal.

Intento2.

Pregunta 1

¿En qué consiste la correlación de información durante el análisis de evidencias?:

a. En complementar la información filtrada con información adicional que resulte valiosa o imprescindible.
b. Ninguna de las anteriores.
c. En enlazar la información con otra información semejante que pueda facilitar la extracción de conclusiones.

Pregunta 2

¿Qué características deben tener los procesos que recopilan información con valor legal?:

a. Deben estar previamente validados por los auditores de calidad.
b. Deben ser conocidos, replicables y no deben alterar la información al recogerla.
c. Deben estar previamente validados por los analistas legales.

Pregunta 3

El triaje es:

a. La búsqueda de ternas de patrones.
b. La recopilación de al menos tres evidencias de un incidente.
c. Un filtrado primario de incidentes con base en informacion preliminar.
d. La agrupación de incidentes en conjuntos de tres.

Pregunta 4

¿Cuál es el documento más utilizado cuando se trata de recolectar información confidencial?:

a. El documento de autorización expresa.
b. El acuerdo de hacking ético.
c. El acuerdo de no divulgación.
d. El contrato formal con el pentester.

Pregunta 5

¿Qué es la Gestión de Incidentes de Ciberseguridad de la Información?:

a. Son todas las acciones anteriores.
b. Es el conjunto de acciones que se centran en la prevención de ciberincidentes.
c. Es el conjunto de acciones que se centran en la restauración de los niveles de operación.

Pregunta 6

El grupo de defensa proactiva de los sistemas frente a los incidentes es el:
a. Equipo Blanco.
b. Equipo Morado.
c. Equipo Rojo.
d. Equipo Azul.

Pregunta 7

¿Cuáles son las fases del procedimiento del CSIRT de referencia?:

a. Apertura, Priorización y Resolución.
b. Notificación, Análisis y Conclusiones.
c. Detección, Alerta y Mitigación.

Pregunta 8

Los Pilares Fundamentales para la Recopilación de Evidencias son:

a. Los Procedimientos.
b. La Tecnología.
c. Las Personas.
d. Todos los anteriores.

Pregunta 9

¿Cuál es el último paso de la recolección de evidencias, que además se suele olvidar?:

a. Fijar el orden de volatilidad para cada sistema.
b. No olvidar a las personas involucradas.
c. Documentar cada paso.
d. Comprobar el grado de sincronización del reloj del sistema.

Pregunta 10

El estándar para la recopilación de información de incidentes de Ciberseguridad es:

a. La Norma ISO 27001.
b. La Norma ISO/IEC 27032.
c. La Norma RFC3227.
d. La Norma ISO 9001.

Pregunta 11

Para evitar el potencial deterioro de información valiosa se deberá:

a. Analizar la información directamente sobre el sistema y recoger después lo que resulte relevante.
b. Recoger la información inmediatamente y analizarla después.
c. Primero estabilizar el sistema y luego recoger la información.

Pregunta 12

Un Kit de Análisis debe incluir los siguientes tipos de herramientas:

a. Programas para examinar el estado del sistema.
b. Programas para listar y examinar procesos.
c. Programas para realizar copias bit a bit.
d. Todas las anteriores.

Pregunta 13

La labor del Equipo Morado se efectúa:

a. Durante la manifestación del incidente.
b. Antes de la aparición del incidente en el entorno.
c. Tras la finalización del incidente.