3.a..e - Reflexión y Resumen sobre la Unidad

Pablo Painceiras Martínez
13/05/2024

Índice

Preguntas

¿Qué te ha parecido los temas tratados?

Los temas tratados sobre recopilación y almacenamiento de evidencias, así como análisis de evidencias e investigación de incidentes, han sido muy relevantes y útiles para comprender cómo se lleva a cabo la gestión de incidentes de seguridad cibernética de manera efectiva.

¿Qué te ha parecido más útil para tu futuro puesto de trabajo en un equipo de seguridad?

Lo más útil ha sido aprender sobre la importancia de la preservación de la escena del incidente, la adquisición adecuada de evidencias y la documentación detallada de cada paso del proceso. Además, entender cómo se realiza el análisis forense digital y la investigación de incidentes proporciona una visión clara de cómo identificar, reconstruir y temporalizar los eventos relacionados con posibles incidentes de seguridad.

¿Conocías todos los puntos tratados en la unidad? ¿Cuáles no?

Algunos de los puntos tratados eran conocidos para mí, como la importancia de la cadena de custodia y la necesidad de trabajar con copias de evidencias en lugar de los datos originales. Sin embargo, otros puntos, como la creación de una línea temporal detallada de los eventos y los métodos para determinar la autoría del incidente, me resultaron especialmente interesantes y enriquecedores.

¿Alguno te ha llamado especialmente la atención? ¿Por qué?

La creación de una línea temporal detallada de los eventos me llamó especialmente la atención porque proporciona una estructura clara para comprender cómo ocurrieron los eventos en un incidente y facilita la identificación de las acciones realizadas por los atacantes.

¿Descartarías algún punto de la unidad? ¿Cuál y por qué?

No descartaría ningún punto de la unidad, ya que todos son fundamentales para comprender el proceso completo de gestión de incidentes de seguridad cibernética. Cada uno aporta una perspectiva única y necesaria para llevar a cabo una investigación exhaustiva y efectiva.

¿Has echado en falta algún tema?

No he echado en falta ningún tema en particular, ya que la unidad cubre de manera integral los aspectos clave relacionados con la recopilación, análisis e investigación de evidencias en incidentes de seguridad cibernética. Sin embargo, sería interesante profundizar en temas específicos, como técnicas avanzadas de análisis forense digital o casos de estudio de incidentes reales y su gestión.

Recopilación y almacenamiento de evidencias

Recopilación de evidencias

Evidencias

Las evidencias son información utilizada para probar algo. Su recopilación es fundamental para estar preparado ante cualquier suceso.

Metodologías de recolección y almacenamiento

- Preservación: Se inicia con la preservación de la escena del incidente para evitar alteraciones en las evidencias.
- Adquisición: Consiste en recopilar la información relevante de manera detallada y precisa.
- Documentación: Es esencial documentar cada paso del proceso de recopilación de evidencias.
- Análisis: Una vez recopiladas, las evidencias son analizadas para extraer conclusiones.
- Presentación: Finalmente, se presentan las evidencias de manera clara y comprensible.

La RFC 3227 es un estándar ampliamente utilizado que proporciona directrices para la recopilación y almacenamiento de evidencias. Incluye principios fundamentales durante la recolección, como la captura precisa de imágenes del sistema, la toma de notas detalladas y la minimización de cambios en la información recopilada.

Se destacan los siguientes puntos:

- Orden de volatilidad: Se establece un orden para la recopilación de información, priorizando los datos más volátiles.

- Acciones a evitar: Se mencionan acciones que podrían invalidar el proceso de recolección de evidencias, como apagar el ordenador antes de recopilar toda la información.

- Consideraciones sobre la privacidad: Es importante respetar la privacidad de las personas y obtener autorización por escrito cuando sea necesario.

El procedimiento de recolección debe ser detallado y transparente, documentando cada paso y considerando a las personas involucradas. Además, se enfatiza en la importancia de la cadena de custodia para el almacenamiento seguro de evidencias, detallando quién ha manejado la evidencia y cómo.

Para el almacenamiento de evidencias, se deben seleccionar cuidadosamente las herramientas, priorizando aquellas externas al sistema y ubicadas en dispositivos de solo lectura.

Se recomienda tener un kit básico de herramientas según el sistema operativo, que incluya funciones como listar y examinar procesos, examinar el estado del sistema y realizar copias bit a bit.

Análisis de evidencias e investigación de incidente

Análisis de evidencias

Análisis de evidencias e investigación del incidente

Objetivo

- Identificar o detectar ciber incidentes mediante una monitorización completa.
- Diferenciar entre eventos normales y ciber incidentes.

Investigación del Incidente:

- Define los incidentes como eventos que no son parte de la operación estándar y que causan o pueden causar interrupciones en los servicios.
- Recopila evidencias digitales y las analiza para reconstruir y temporalizar los hechos.

Premisas del Análisis de Evidencias:

- No trabajar con los datos originales.
- Respetar las leyes vigentes.
- Obtener resultados verificables y reproducibles.

Documentación Adicional:

- Sistema operativo, programas, hardware y conectividad del equipo.
- Información sobre configuración que pueda ser relevante para la investigación.

Pasos del Análisis de Evidencias:

- No hay un procedimiento estándar; cada caso debe ser estudiado individualmente.
- Preparación de un entorno de trabajo adecuado.
- Creación de una línea temporal de los hechos ocurridos.
- Determinación de cómo se llevó a cabo el ataque.
- Identificación de los autores del incidente.
- Evaluación del impacto causado y posibilidad de recuperación del sistema.

Aspectos Destacados:

- Precauciones al trabajar con dispositivos originales vs. copias.
- Importancia de crear una línea temporal precisa.
- Métodos para determinar la autoría del incidente, incluyendo el análisis de conexiones abiertas y perfiles de posibles atacantes.
- Evaluación del impacto económico del incidente, incluyendo gastos directos e indirectos.

Conclusiones:

- El análisis de evidencias e investigación de incidentes requiere una combinación de métodos técnicos y análisis crítico para determinar el origen, la autoría y el impacto de los incidentes de seguridad cibernética.