Actividad 2 - Análisis Forense

Cristóbal Suárez Abad

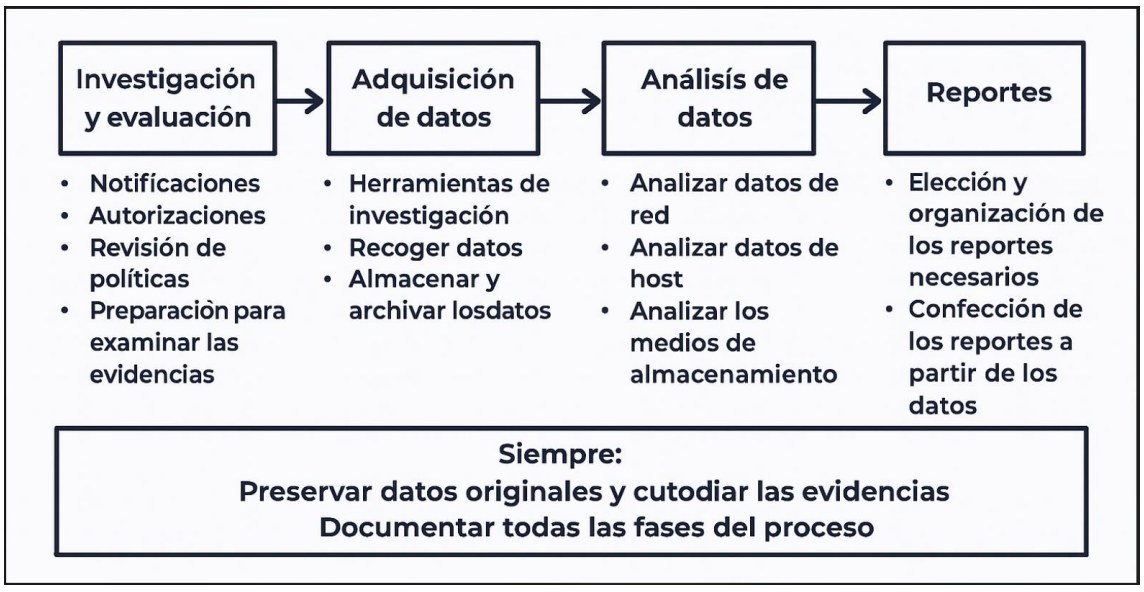
Seguridad y alta disponibilidad – 2º ASIR.

Elige un contexto realista de un ataque que se haya producido. Y lleva a cabo de forma simulada las distintas fases para realizar un Análisis Forense.

*"**Análisis Forense Digital***

Cuando las medidas de seguridad fallan, el análisis forense rastrea información sobre el ataque en el sistema comprometido para diseñar contramedidas futuras y determinar el agente atacante.

- ***Identificación y Evaluación***
  Descubrir señales del ataque, vía de entrada, origen y perjuicios ocasionados
- ***Preservación de Evidencia***
  Recopilación no destructiva de datos como prueba judicial potencial
- ***Análisis de Evidencia***
  Reconstrucción temporal del ataque e identificación del medio, técnica o vía específica utilizada
- ***Documentación y Reporte***
  Documentar incidente y solución para responsables pertinentes".



Contexto: En una oficina de desarrollo web se ha producido una brecha en la seguridad por la cual se ha accedido a la base de datos de clientes y a varios servidores donde se encuentran las aplicaciones que dan servicio a los clientes:

1) **Identificación y Evaluación:**

- Identificar hora en la que se produce la brecha: logs de acceso, volumen de tráfico inusual, etc.
- Identificar acciones y ficheros comprometidos por los intrusos: logs (las bases de datos tienen registros tanto para los accesos como para las acciones que se llevan a cabo). Tanto los propios sistemas como la mayoría de las aplicaciones cuentan con archivos de registros para identificar las actividades que se han llevado a cabo[1].

2) **Preservación y Evidencia:**

Aislar los hosts mediante firewall, desplazar a VLAN de cuarentenas, etc. No apagar los equipos una vez aislados, puede haber datos en la RAM que se puedan usar como prueba.

Se deben hacer copias de seguridad de los discos con software especializado de análisis forenses: FTK Imager[2], The Sleuth Kit, etc[3]. En Máquinas Virtuales además podemos hacer "snapshots". Podemos hacer también volcado de la RAM[4]. También podemos solamente copias de los "logs" necesarios que hemos mencionado en la fase anterior.

NOTA: genera "hash" de los logs, imágenes o de cualquier otro archivo que vayas a usar como posible prueba. De esta manera se podrá verificar que la evidencia que llega a las autoridades es la misma que generaste en el momento inicial.

Por último, según el volumen de pruebas que se tenga, se debería confeccionar un archivo de registro (Excel o similares) donde anotar ficheros, programa y máquinas a las que pertenece, fecha de recogida, técnico que la recogió, hash, observaciones, etc.

[1] https://www.plesk.com/blog/product-technology/linux-logs-explained/
[2] https://fidelissecurity.com/cybersecurity-101/learn/digital-forensic-investigation-process/#:~:text=Identification%20Phase&text=This%20involves%20identifying%20a%20range,that%20may%20hold%20relevant%20data.
[3] https://www.bluevoyant.com/knowledge-center/get-started-with-these-9-open-source-tools
[4] https://viviendolared.blogspot.com/2014/07/como-hacer-un-volcado-de-memoria-memory.html

3) Análisis de Evidencia:

Algunas de las técnicas más habituales son[5]:

- Análisis en vivo: son aquellos que se realizan cuando el equipo sigue en funcionamiento. Permite examinar datos volátiles (memoria RAM, caché, procesos activos). Esencial para capturar evidencias que se perderían al apagar el sistema (o cuando no se puede hacer un volcado de memoria).
- File carving o Recuperación de archivos borrados: Se buscan fragmentos de datos residuales en el sistema de archivos o en sectores no reutilizados del disco. Útil para reconstruir evidencia eliminada por el atacante.
- Técnicas estocásticas: Permite reconstruir y analizar actividades digitales que no dejan rastros visibles. Se usa sobre todo para investigar ataques internos, los cuales suelen dejar pocas pruebas. Se basa en inferencias estadísticas o patrones de comportamiento del sistema.
- Análisis cruzado: Busca correlaciones y anomalías entre múltiples dispositivos y/o discos. Permite detectar comportamientos sospechosos o conexiones entre equipos implicados en un incidente. Se usa para establecer un contexto común o línea base que facilite la detección de irregularidades.

4) Documentación y Reporte.

Se debe llevar a cabo una documentación meticulosa de los hechos acaecidos; tanto por interés de evitar futuras incidencias en la empresa, como para base para posible presentación ante un juzgado[6].

Los técnicos forenses deben llevar a cabo una serie de protocolos legales que permitan validar la integridad de las evidencias recolectadas y sus averiguaciones. Por eso en la documentación se deben exponer claramente acciones como: cadena de custodia de cada evidencia, herramientas utilizadas, técnicas llevadas a cabo y nombre y titulación de los técnicos (en el caso de que este proceso lo haga una compañía externa, esta deberá incluir esa información).

Toda esta información debe ser presentada en documentos o presentaciones a las partes involucradas: empleados, clientes y/o proveedores involucrados, autoridades jurídicas, etc.

---

[5] https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools

[6] https://fidelissecurity.com/cybersecurity-101/learn/digital-forensic-investigation-process/