Auditoria Forense

Alejandro Corletti Estrada
acorletti@darfe.es

Temario

1. Qué es la informática Forense
2. Metodología Forense (Fases)
3. Herramientas
4. Normativa

1. Qué es la Informática Forense

La informática forense es una ciencia, de reciente aparición, que se encarga de asegurar, identificar, preservar, analizar y presentar un conjunto de datos, también llamados, prueba digital, de tal modo que ésta pueda llegar a ser aceptada en un proceso legal y/o judicial.

Fines de la informática forense

- Preventivos
- Correctivos
- Probatorios
- Auditores

Regulación estatal:

- Ley de enjuiciamiento civil
- Ley de protección de datos de carácter personal.
- Ley de Conservación de Datos Relativos a las Comunicaciones y las Redes Públicas.
- Ley de la SOciedad de la Información y del Comercio Electrónico.
- Código penal.
- Regulaciones de la Secretaría de Telecomunicaciones.

2. Metodología Forense (Fases)

1. Asegurar la escena
2. Identificar y recolectar las evidencias
3. Preservar las evidencias
4. Analizar las evidencias obtenidas
5. Redactar informes sobre los resultados

Fase 1: Asegurar la escena. (Medidas físicas, horarias, periféricos, conexiones/desconexiones eléctricas y de red

Fase 2: Recolección de evidencias (Identificación y recolección).

Se debe proceder de lo más volátil a lo menos volátil:

- Registros, caché
- Tabla de enrutamiento, Caché ARP, tabla de procesos, estadísticas del kernel, la memoria.
- Archivos temporales
- Discos
- Logs de los sistemas.
- Configuración física y topología de red
- Documentación

Recolección: Fuente datos original:

→ 1ª Copia (Hash - Judicial) Se compara su Hash con el de la fuente

→ 2ª Copia (Hash – Respaldo Laboratorio)

→ 3ª Copia (Hash – trabajo en laboratorio)

Recolección de evidencia.

- Fuentes de información (Registros, Logs, IDSs, sondas, Honey Pots, Sistemas de autenticación y control de accesos, máquinas de salto, configuraciones, gestores documentales, sistemas de control de integridad, sistemas de backups).
- Mantenimiento de la integridad y cadena de custodia.
  - Asegurar que la evidencia no ha sido alterada.

- ¿Podemos garantizarlo? (Hash, copias bit a bit, imágenes de discos y sistemas, sincronismos y sellados de tiempo, redundancia de Logs, protección física, procedimientos)

➢ Volatibilidad (Memoria RAM - Procesos - Conexiones de red)

- Si los dispositivos se apagan (perdemos lo volátil)
- Si los dispositivos no se apagan (se puede alterar la evidencia)…….. Compromiso.

➢ Coordinación con fuerzas judiciales y policiales.

Análisis de la evidencia.

➢ Metódico y reproducible

➢ ¿Qué es relevante?

➢ Líneas temporales.

➢ Análisis de Logs y registros.

Fase 3: Preservación de las evidencias

Una mala preservación puede invalidar toda la investigación. Cadena de custodia, procedimientos controlados

Fase 4: Análisis de las evidencias

Se pueden destacar varios pasos, que habrá que adaptar en cada caso:

- Preparar un entorno de trabajo adaptado a las necesidades del incidente.
- Reconstruir una línea temporal con los hechos sucedidos.
- Determinar qué procedimiento se llevó a cabo por parte del atacante.
- Identificar el autor o autores de los hechos.
- Evaluar el impacto causado y si es posible la recuperación del sistema.

Fase 5: Informes.

- Informe ejecutivo
- Informe técnico
- Informe pericial.
  - ➢ Riguroso, claro y precisoa

3. Herramientas.

1. Herramientas específicas para análisis forense.

   - **The Sleuth Kit** es un conjunto de herramientas open source para el análisis de imágenes de discos. Inicialmente desarrollada para plataformas UNIX, esta suite actualmente se encuentra disponible también para OS X y Windows. Además, TSK cuenta con una interfaz gráfica conocida como **Autopsy** que agrupa todas sus herramientas y plugins.

   - **CAINE** (Computer Aided INvestigate Environment)

2. Análisis de red
   - nmap
   - tcpdump
   - Wireshark
   - Xplico

3. Trabajo con discos
   - Dcdd3
   - Mount Manager
   - Guymager

4. Tratamiento de memoria
   - Volatily
   - Memoryze
   - RedLine

5. Análisis de aplicaciones
   - OllyDbg
   - Radare
   - Process explorer

6. Detección de intrusiones.
   - Snort
   - Check Point Intrusion Prevention System
   - Cisco Next Generation IPS
   - McAfee Network Security Platform
   - Se pueden considerar aquí los FWs de nueva generación de Palo Alto

7. Gestión de FWs.
   - Algosec
   - Tuffin
   - Firemon

8. Centralización y correlación de Logs (SIEM: Security Information and Event Management) del tipo.
   - ArcSight de HP
   - RSA Security Analytics
   - Splunk (Puede discutirse si es o no un SIEM…)

9. Herramientas de control de acceso, tipo.
   - ACS de Cisco
   - Series SRC de Juniper
   - NAKINA
   - Access Control de Fortinet
   - HPNA
   - CITRIX

4. Normativa.

RFC 3227 "Guidelines for Evidence Collection and Archiving"

Recoge directrices para recopilar y almacenar evidencias sin ponerlas en riesgo.

UNE 71505 Gestión de evidencias electrónicas

UNE 71506 Metodología para el análisis forense de las evidencias electrónicas

Estas normas, publicadas por la Asociación Española de Normalización y Certificación tienen como finalidad dar una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales.

Familia ISO 27000

- 27001 y 27002
- 27035 (Sustituye a la TR 18044:2004)
- 27037 Directrices para la identificación, recolección, adquisición y preservación de la prueba digital (Renueva con bastante detalle la RFC 3227)

ISO/IEC 27035:2011 "Information technology — Security techniques — Information security incident management

ISO/IEC 27035-1: principles of incident management (draft)

ISO/IEC 27035-2: guidelines to plan and prepare for incident response (draft)

ISO/IEC 27035-3: guidelines for incident response operations (draft)

ISO/IEC 27037:2012 "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence"

Los principios en que se basa esta norma son:

- Aplicación de Métodos:

  La evidencia digital debe ser adquirida del modo menos intrusivo posible tratando de preservar la originalidad de la prueba y en la medida de lo posible obteniendo copias de respaldo.

- Proceso Auditable:

  Los procedimientos seguidos y la documentación generada deben haber sido validados y contrastados por las buenas prácticas profesionales. Se debe proporcionar trazas y evidencias de lo realizado y sus resultados.

- Proceso Reproducible:

  Los métodos y procedimientos aplicados deben de ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas.

- Proceso defendible:

  Las herramientas utilizadas deben de ser mencionadas y éstas deben haber sido validadas y contrastadas en su uso para el fin en el cual se utilizan en la actuación.

Para cada tipología de dispositivo la norma divide la actuación o su tratamiento en tres procesos diferenciados como modelo genérico de tratamiento de las evidencias

- La identificación:

  Es el proceso de la identificación de la evidencia y consiste en localizar e identificar las potenciales informaciones o elementos de prueba en sus dos posibles estados, el físico y

el lógico según sea el caso de cada evidencia.

- La recolección y/o adquisición:

  Este proceso se define como la recolección de los dispositivos y la documentación (incautación y secuestro de los mismos) que puedan contener la evidencia que se desea recopilar o bien la adquisición y copia de la información existente en los dispositivos.

- La conservación/preservación:

  La evidencia ha de ser preservada para garantizar su utilidad, es decir, su originalidad para que a posteriori pueda ser ésta admisible como elemento de prueba original e íntegra, por lo tanto, las acciones de este proceso están claramente dirigidas a conservar la Cadena de Custodia, la integridad y la originalidad de la prueba.

ISO 27002

A.13 Administración de los incidentes de seguridad

lo que trata de dejar claro este punto de la norma a través de los cinco controles que agrupa, y subdivide en:

- Reportes de eventos de seguridad de la información y debilidades.

  Como su nombre lo indica, este apartado define el desarrollo de una metodología eficiente para la generación, monitorización y seguimiento de reportes, los cuales deben reflejar, tanto eventos de seguridad como debilidades de los sistemas. Estas metodologías deben ser ágiles, por lo tanto se presupone el empleo de herramientas automatizadas que lo hagan. En estos momentos se poseen muchas de ellas.

  En concreto para que estos controles puedan funcionar de manera eficiente, lo mejor es implantar herramientas de detección de vulnerabilidades, ajustarlas a la organización, para saber con total certeza dónde se es débil y donde no, y a través de estas desarrollar un mecanismo simple de difusión de las mismas a los responsables de su administración y solución, los cuales deberán solucionarlas o justificar las causas para no hacerlo, ante lo cual, esta debilidad pasará a ser tratada por el segundo grupo de este control, es decir una metodología de detección de intrusiones, que será la responsable de generar la alerta temprana, cuando una de esas debilidades sea explotada por personal no autorizado. Estas alertas necesitan también un muy buen mecanismo de gestión, para provocar la respuesta inmediata.

- Administración de incidentes de seguridad de la información y mejoras.

  Si se poseen los dos mecanismos mencionados en el punto anterior, la siguiente tarea es disponer de una metodología de administración de incidentes, lo cual no es nada más que un procedimiento que describa claramente: pasos, acciones, responsabilidades, funciones y medidas concretas. Todo esto no es eficaz si no se realiza la preparación adecuada, por lo tanto es necesario difundirlo, practicarlo y SIMULARLO, es decir generar incidentes que no hagan peligrar los elementos en producción, tanto sobre maquetas como en planta y poner a prueba todos los eslabones de la metodología. Seguramente aparecerán fallos, zonas grises o brechas de seguridad metodológicas, las cuales la mejor manera de solucionarlas es en “situaciones de paz” y no durante un conflicto

real……como se pueda apreciar he escrito en terminología muy militar, pues esto no es ni más ni menos que lo que hacen (o deberían hacer….) durante todo el tiempo de paz las fuerzas armadas, "prepararse para incidencias", pues esta actividad no puede ser improvisada cuando llega la misma sino no hace falta ser militar para deducir que será catastrófico. La preparación militar, en los casos defensivos hace principalmente esto, es decir analizar las posibles metodologías que puede aplicar un enemigo y practicar su contramedida, esto es el entrenamiento militar y a su vez son los denominados "ejercicios militares" en el terreno o en mesas de arena (Léase planta y/o maqueta), que no son otra cosa que simulaciones sobre qué sucedería si reacciono des esta forma u otra. La doctrina militar es milenaria, tiene millones de situaciones vividas, practicadas y estandarizadas, por así llamarlas, por los tantos en los casos en que su analogía con la informática es evidente, no se debe re inventar la rueda, sino aprovechar lo que ya existe, y la preparación ante incidencias es uno de los casos más evidentes de esto. Existe un muy antiguo refrán que dice "Si quieres vivir en paz, prepárate para la guerra". Es decir, si quieres evitar problemas de seguridad, prepárate para ellos.