Análisis forense

Vista de pájaro

Info

ReD

- Especialista en seguridad
- Cofundador de M4H
- Cofundador de Hacklabs
- Defensor de la privacidad

analisisforense.com

- Referencia de manuales.
- Referencia de herramientas.
- Referencia de comunidades hispanas.

¿Qué es la ciencia forense?

La evidencia digital

- No se ve.
- No se puede evaluar sin conocimiento técnico.
- Se puede duplicar infinitamente.
- La copia es 100% igual que el original.
- Es muy volátil

¿Qué es la ciencia forense digital?

- “ Obtención y análisis de datos empleando métodos que distorsionen lo menos posible la información con el objetivo de reconstruir todos los datos y/o los eventos que ocurrieron sobre un sistema en el pasado ”

Dan Farmer y Wietse Venema, 1999

¿En que entornos se usa?

- Máquinas atacadas
- Trabajadores
- Máquinas de atacantes
- Grupo de personas con conductas “ilegales” (terrorismo, pederastas, militantes...)

¿Sobre qué se usa?

- Ordenadores
- Redes
- Móviles
- Otros dispositivos

¿Qué quiere responder?

¿Dónde?

¿Cómo?

¿Cuándo?

¿Quién?

¿Por qué?

Clasificación personal del forense

- Técnico (hace que no pase de nuevo)
- Experto en leyes (pide responsabilidades)

¿Preservar o salvar?

VS

Fases del análisis

- Identificación del incidente
- Preservar
- Recolectar
- Analizar
- Presentar

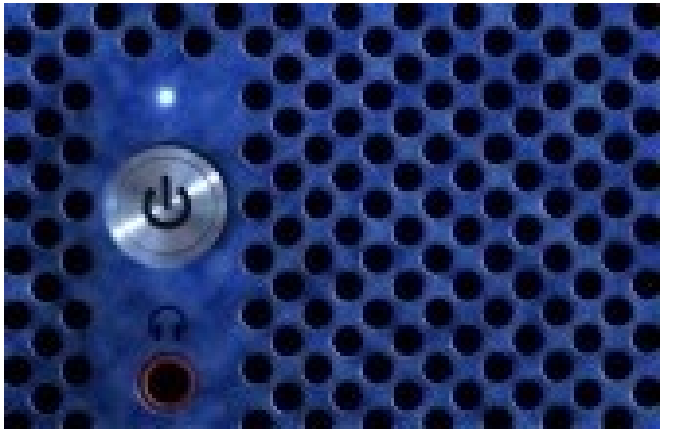
Siempre presente la cadena de custodia.

Identificación del incidente

- Búsqueda y recopilación de evidencias
- Hasta qué punto están afectados los sistemas

Preservar

- Si no está encendido
  no se enciende



- Si está encendido
  no se apaga inmediatamente

Recolectar

- obtención de imágenes forenses
  - ***dd*** es tu amigo
  - ***nc*** también
- Sellar las imágenes (md5 sha)

Analizar

SIEMPRE SE TRABAJA SOBRE LA COPIA

- Análisis “físicos”
  - Reconocimiento de particiones
  - Recuperación de estructuras.
    - Sectores defectuosos, particiones...
  - Recuperación de ficheros.
  - Enumeración de dispositivos y estados.

Analizar

SIEMPRE SE TRABAJA SOBRE LA COPIA

- Análisis lógicos
  - Determinar ficheros modificados
  - Aplicaciones usadas
  - Tareas realizadas
  - Etc

Analizar

SIEMPRE SE TRABAJA SOBRE LA COPIA

- Análisis de ficheros
  - Buenos (estáticos)
  - Buenos (modificados)
  - Malos (troyanos, backdoors...)
  - Extensión modificada.

Analizar

SIEMPRE SE TRABAJA SOBRE LA COPIA

- Análisis de ficheros malos
  - Funcionamiento
  - Llamada a casa
  - Canales de actualización
  - Etc

Analizar

SIEMPRE SE TRABAJA SOBRE LA COPIA

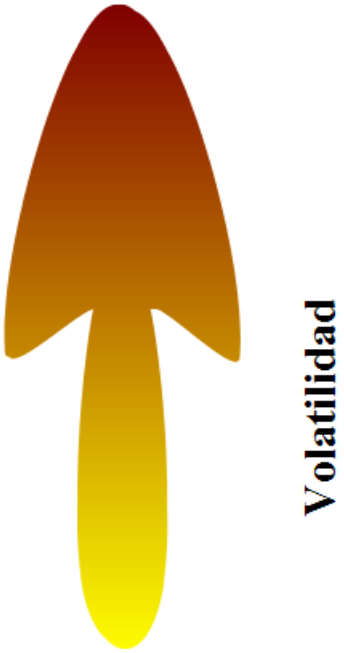
- Línea de tiempo

Presentar

- Documentación de la cadena de custodia

Recolecta de evidencias

- Registros CPU
- Memoria Cache
- Memoria
  - Módulos del SO
  - Controladores dispositivos
  - Programas en ejecución
  - Conexiones activas
- Disco



Manos a la obra
Tipos de sistemas

- Sistemas “vivos”
  - Memoria
  - Flujos de red
  - Procesos
  - Ficheros

Manos a la obra
Tipos de sistemas

- Sistemas “muertos”
  - Almacenamiento

Manos a la obra
Tipos de sistemas

- Información complementaria
  - Logs IDS
  - Logs Firewalls
  - Logs de servidores intermedios
  - Logs de aplicaciones

Ejemplos de atacantes
Virus - Cronología

- Se descubre una vulnerabilidad en el sistema.
- Se crea un virus que la explote.
- El fabricante corrige la vulnerabilidad

Ejemplos de atacantes
Virus - Características

- Suelen desactivar el antivirus, al menos de forma puntual
- No se ocultan demasiado
- No suele afectar a equipos actualizados

Ejemplos de atacantes Persona física - Cronología

- Aprovechan vulnerabilidades más o menos recientes
- La intrusión se adapta al equipo asaltado
- Incluye varias puertas traseras y herramientas de administración remota (Dameware, VNC, etc.)
- Ocultan todos sus procesos, ficheros, conexiones, etc
    - Para ello, utilizan rootkits conocidos
    - En algunos casos incluyen key-loggers

Equipo comprometido

- No utilizar las herramientas del sistema (podría haber sido alteradas).
- NO SER INTRUSIVO
- Usar dispositivo solo lectura (CDROM).
  Ejecutables estáticos
- NO ALTERAR INFORMACIÓN DEL DISCO.
- No instalar programas.
- No volcar salida de programas a disco duro.
- Utilizar soporte externo o por red para almacenar la salida.

Caso práctico

Herramientas

- Passware Password Recovery Kit Forensics

  ~800$, entre otros, rompe bitlocker y truecrypt

- COFEE (Computer Online Forensic Evidence Extractor)

  recolectar historial de navegación archivos temporales y otros datos sensibles de la mayoría de las máquinas basadas en win.

- EnCase (http://www.guidancesoftware.com)
- Sleuthkit (http://www.sleuthkit.org)
- Helix 3 (http://www.e-fense.com)

EnCase®

Continuar aprendiendo

- RFC 3227 Directrices para la recopilación de evidencias y su almacenamiento

Muchas gracias

¿Preguntas?

red@nosoloaulas.com