Seguridad en Sistemas Informáticos (SSI)

Análisis forense

Carlos Pérez Conde

Departament d'Informàtica

Escola Técnica Superior d'Enginyeria

Universitat de València

Bibliografía específica

- **Forensic Discovery**
  D. Farmer, W. Venema
  Addison-Wesley
- **File System Forensic Analysis**
  B. Carrier
  Addison-Wesley

Guión

- **Conceptos básicos**
- Análisis de sistemas de ficheros
- Análisis de programas malintencionados (*malware*)

¿Qué es el análisis forense?

- **Proceso científico (elaboración y verificación/refutación de hipótesis) mediante el que**
  - se identifican posibles fuentes de evidencias
  - se preservan estas evidencias
  - se analizan (buscando respuestas a preguntas sobre un hecho)
  - se presentan las conclusiones y las evidencias que las sustentan
- **Objetivos**
  - demanda legal
  - investigación judicial
  - parte del proceso de seguridad
    - las evidencias pueden no ser válidas en un juicio
    - pero pueden ayudar a mejorar la seguridad

Estilos de análisis

- **Obtención de evidencias**
  - el funcionamiento del sistema las destruye
  - el proceso de copia puede destruirlas
- **¿Cómo analizar un sistema? ¿Vivo o muerto?**
  - ¿Estirar del cable de alimentación? (muerto)
    - reduce las probabilidades de modificación del sistema
    - aumenta la aceptabilidad de las pruebas obtenidas
    - reduce el riesgo de propagación de daños
    - destruye evidencias (procesos, ficheros abiertos, conexiones...)
  - ¿Continuar con la ejecución del sistema? (vivo)
    - permite (tal vez) aprender más (*honeypots*)
    - ¿podemos confiar en los programas o el núcleo?
    - ejecutar copias del disco en otra máquina (probablemente virtual)
  - El botón de pausa
    - máquinas virtuales, suspend-to-RAM, suspend-to-disk, shutdown

Herramientas para el análisis

- EnCase, Guidance Software
  http://www.encase.com
- The Coroner's Toolkit (TCT), W. Venema, D. Farmer
  http://www.porcupine.org/forensics/tct.html
- The Sleuth Kit (TSK)/Autopsy, B. Carrier
  http://www.sleuthkit.org
- Helix Live CD, e-fense
  http://www.e-fense.com/helix/
- Más información:
  - http://www.e-evidence.info/vendors.html
  - http://www.forensics.nl

The Sleuth Kit (TSL) / Autopsy
http://www.sleuthkit.org

- Sistema de ficheros: **fsstat**
- Nombres de ficheros: **ffind, fls**
- Metadata: **icat, ifind, ils, istat**
- Data: **dcat, dls, dstat, dcalc**
- Registro (file system journal): **jcat, jls**
- Medios: **mmls**
- Imágenes: **img_stat, img_cat**
- Discos: **disk_sreset, disk_stat**
- Otros: **hfind, mactime, sorter, sigfind**

Guión

- Conceptos básicos
- **Análisis de sistemas de ficheros**
- Análisis de programas malintencionados (*malware)*

Obtención de datos de discos duros

- **Nivel de abstracción de la copia**
  - copia de seguridad
  - partición
  - disco
- **Aspectos a considerar**
  - gestión de errores
  - generación de resúmenes digitales (MD5, SHA-1...)
  - datos ocultos (ej: HPA, DCO en discos ATA)
  - formato de la imagen
  - compresión
  - transmisión a través de la red (integridad, confidencialidad)
- **Recomendado: cap. 3 de FS Forensic Analysis**

Ejemplo: análisis con Autopsy

- **Planteamiento**
  - imagen del sistema de ficheros raíz de una máquina con Linux
  - detectar actividad inusual reciente
- **A destacar**
  - generación de un listado temporal de eventos
  - identificación de actividad sospechosa
  - obtención de evidencias

Guión

- Conceptos básicos
- Análisis de sistemas de ficheros
- **Análisis de programas malintencionados (*malware*)**