Informática Forense

Teoría y Práctica

Daniel Fernández Bleda

dfernandez@isecauditors.com

Sevilla, Hackmeeting 2004

1/11/2004

Índice (Teoría)

- Introducción:
  - Hagamos un poco de Historia
  - ¿Qué es la Informática Forense?
  - ¿Qué es Evidencia Digital?
  - Orígenes de la I.F.
- Estado actual de la I.F.
  - Situación actual.
  - El reto
- Procedimientos en el Análisis Forense
  - RFC3227 / CP_4DF
  - El Proyecto CTOSE
  - La cadena de custodia
  - Proceso pre-investigación
  - Entornos de trabajo
- Aplicación del A.F.:
  - Aplicación Real
  - Modos de A.F.
  - Información útil en el A.F.
- Herramientas Open Source:
  - The Coroner's Toolkit
  - The Sleuth Kit / Autopsy
  - Mac-robber
  - Foundstone Forensic Toolkit
  - FLAG
  - Foremost
  - HELIX / FIRE
- Conociendo al enemigo
- El Futuro de la I.F.

Índice (Práctica)

- Análisis post-mortem de un sistema comprometido
- Análisis en caliente de un sistema comprometido
- Recuperación de pruebas de un disquete

Hagamos un poco de historia

- La ciencia informática data de los años 40, es una de las más recientes.
- Su evolución e integración en la sociedad a sido muy rápida.
  - 40s: Se investiga para saber qué es computable.
  - 60s: Se investiga para reducir coste y potencia.
  - 80s: Se investiga para hacerla fiable y robusta.
  - 00s: Se investiga cómo controlar qué hacen los usuarios con los ordenadores y qué sucede dentro de estos.
  - 01s (12 de Septiembre): Control total. Se quiere poder investigar y monitorizar la actividad en los Sistemas de Información e Internet: Informática Forense.

¿Qué es la Informática Forense?

- La Informática Forense es la ciencia de:
  - Adquirir
  - Preservar
  - Obtener
  - Presentar

  datos que hayan sido procesados electrónicamente y almacenados en soportes informáticos.

¿Qué es una Evidencia Digital?

- Información almacenada digitalmente que puede llegar a ser utilizada como prueba en un proceso judicial.
- Para que esto sea viable será necesario seguir unos procedimientos en su recuperación, almacenamiento y análisis.
- Es muy importante seguir una cadena de custodia lo suficientemente robusta y permita asegurar la inmutabilidad de la evidencia digital.

El Principio de Locard

- Cada contacto deja un rastro.
- En el mundo físico:
  - Cristal roto con la mano: cristal en la mano, sangre en el cristal.
  - Cesped pisado: tierra en el zapato, huella en el cesped.
- En el mundo digital:
  - Conexión SSH: claves públicas en cliente y servidor.
  - Exploits compilados: MD5 único de un “único” atacante.

Delitos Informáticos

- Según las Naciones Unidas tenemos estos:
  - Fraudes cometidos mediante manipulación de ordenadores.
  - Manipulación de programas.
  - Manipulación de datos de salida.
  - Fraude efectuado por manipulación informática o por medio de dispositivos informáticos.
  - Falsificaciones informáticas.
  - Sabotaje informático.
  - Virus, gusanos y bombas lógicas.
  - Acceso no autorizado a Sistemas o Servicios de Información.
  - Reproducción no autorizada de programas informáticos de protección legal.
  - Producción / Distribución de pornografía infantil usando medios telemáticos.
  - Amenazas mediante correo electrónico.
  - Juego fraudulento on-line.

Orígenes (I)

- En los últimos 20 años, la cantidad de información almacenada en sistemas informáticos ha tenido un crecimiento casi exponencial.
- El hecho que la información deje de estar en papel para estar en formato digital requiere un cambio de mentalidad en la obtención de pruebas en investigaciones.
- Es necesario saber cómo obtener pruebas de forma eficiente y útil. Debe aparecer el forense del mundo digital a semejanza del mundo físico.

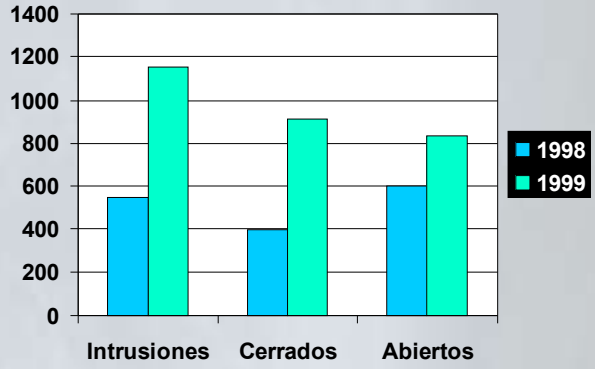
Orígenes (II)

- La I.F. no aparece a causa de Internet.
  - “Al principio no había redes”.
  - Los virus fueron los primeros “investigados”: 90s.
  - La I.F. se inicia con la Ingeniería Inversa.
- Con la apertura de las redes a los usuarios cambia la casuística.
  - A finales de los 90 y principios del milenio la cantidad de redes interconectadas facilita delitos informáticos.
  - Ahora sí existen delitos propios sólo de Internet (p.e. Intrusiones en sistemas != robo mundo físico).
  - La gente miente, roba, falsifica, escucha, ataca, destruye y hasta organiza asesinatos y actos terroristas

Orígenes (III)

- La ciencia de la Informática Forense fue creada para cubrir las necesidades específicas de las fuerzas de la ley para aprovechar al máximo esta forma nueva de evidencia electrónica.
- Las fuerzas del orden no eran capaces de absorber, por falta del personal cualificado y de infraestructura adecuada, la avalancha de delitos informáticos a finales de los 90.
- Un ejemplo:

Intrusiones/casos cerrados/
casos abiertos en el FBI



Situación actual (I)

- Existen multitud de empresas dedicadas a la obtención de evidencias digitales.
- Se publica gran cantidad de bibliografía cada año.
- Las fuerzas del orden cuentan en sus equipos de delitos informáticos o de forma externa con expertos en I.F.
- Los mayores problemas actualmente son:
  - No existe un estándar para la recuperación de Evidencias Digitales: juicios perdidos.
  - La mayoría de jueces no son expertos en informática.
  - Las actuaciones no se realizan con suficiente rapidez.

Situación actual (II)

- Los juicios para los que se realiza análisis forense no es, en la mayoría, para casos de intrusiones.
- Las intrusiones, en su mayoría, o no se detectan, o se detectan demasiado tarde, o no se quieren investigar.
- Las investigaciones vienen relacionadas con:
  - Pornografía infantil
  - Derechos de autor
  - Litigios entre empresas por robo de información, envío de mails “perdidos” no recibidos, etc.
  - Acciones dañinas llevadas a cabo por empleados, expleados o personal externo.
  - Sólo en aquellos casos en los que realmente merece la pena la inversión de dinero, se realizan investigaciones forenses de intrusiones: su coste puede ser muy elevado, pueden no conducir a nada concluyente, las conclusiones pueden no permitir capturar al atacante o que este no esté al alzance.

El reto

- Los soportes informáticos que son examinados y las técnicas disponibles para el investigador son productos resultado de un sector determinado por el mercado privado.
- En contraste con el análisis forense tradicional, en la I.F. las investigaciones deben llevarse a cabo en prácticamente cualquier situación o dispositivos físico, no sólo en un entorno controlado de laboratorio.

Procedimientos en el Análisis Forense

- Para llevar a cabo una investigación forense es adecuado conocer ciertos aspectos:
  - Normativas o “estandares de facto” existentes para la obtención de las pruebas o resultados.
  - Conocer las condiciones bajo las cuales, la evidencia será considerada como tal:
    - Adminisible
    - Autentica
    - Completa
    - Confiable
    - Creible
  - Conocer el procedimiento para llevar a cabo una investigación, cuándo debe llevarse a cabo y las cuestiones legales a tener en cuenta, dependiendo del país donde se lleve a cabo.

RFC3227

- Es un breve documento de 10 páginas que define una “Guidelines for Evidence Collection and Archiving”.
- Se publica en Febrero de 2002.
- Define ciertos aspectos llamativos:
  - Define un orden para recabar información a partir de su “Order of Volatility”.
  - Ofrece instrucciones de que NO se debe hacer cuando se tiene que obtener la información de un sistema.
  - Expone unas normas éticas que deberían cumplirse.

Codes of Practises for Digital Forensics (CP_4DF)

CP4DF codes of practices for digital forensics

- Es una iniciativa española para el desarrollo de una metodología de procedimientos para Análisis Forense.
- Es un proyecto abierto a cualquiera en Sourceforge.
- El 14 de Noviembre se hizo publica la tercera revisión v1.3 durante el 1er Flash mob sobre Digital Forensics en Barcelona.
- Cubre cuatro fases del A.F.:
  - Fase 1: Aseguramiento de la escena
  - Fase 2: Identificación de las Evidencias Digitales
  - Fase 3: Preservación de la Evidencias Digitales
  - Fase 4: Análisis de las Evidencias Digitales
  - Fase 5: Presentación y Reportes

Proyecto CTOSE

Cyber Tools On-Line Search for Evidence

- CTOSE (Cyber Tools On-Line Search for Evidence) es un proyecto de investigación mantenido por la Comisión Europea.
- El propósito del proyecto es recopilar el conocimiento disponible de diferentes fuentes expertas en todos aquellos procesos relacionados en la recuperación de evidencias digitales y crear una metodología para definir como debe llevarse a cabo dicha recuperación cuando sea necesaria como resultado de cualquier tipo de disputa en la que se vean envueltas transacciones electrónicas u otro tipo de crímenes relacionados con las nuevas tecnologías.
- Esto también incluye todas las preguntas sobre cómo ser capaz cada uno en su empresa de manejar este tipo de incidentes y la información asociada a éstos.

La cadena de custodia (I)

- La cadena de custodia el es conjunto de pasos o procedimientos seguidos para preservar la prueba digital que permita convertirla y usarla como evidencia digital en un proceso judicial.
- No existe un estándar reconocido públicamente.
- Existen procedimientos reconocidos públicamente como robustos a la hora de preservar la información digital.
- Existen diferentes procesos de estandarización en los que colaboran fuerzas de la ley, investigadores y expertos (p.e. CTOSE, CP4DF).

La cadena de custodia (II)

- La cadena de custodia debe:
  - Reducir al máximo la cantidad de agentes implicados en el manejo o tratamiento de evidencias.
  - Mantener la identidad de las personas implicadas desde la obtención hasta la presentación de las evidencias.
  - Asegurar la inmutabilidad de las evidencias en los traspasos de estas entre agentes.
  - Registros de tiempos, firmados por los agentes, en los intercambios entre estos de las evidencias. Cada uno de ellos se hará responsable de las evidencias en cada momento.
  - Asegurar la inmutabilidad de las evidencias cuando las evidencias están almacenadas asegurando su protección.

La cadena de custodia (III)

- Es la “secuencia” de la cadena de la evidencia en el siguiente orden:
  - Recolección e identificación
  - Análisis
  - Almacenamiento
  - Preservación
  - Transporte
  - Presentación en el juzgado
  - Retorno a su dueño
- La cadena de la evidencia muestra:
  - Quién obtuvo la evidencia
  - Dónde y cuando la evidencia fue obtenida
  - Quién protegió la evidencia
  - Quién ha tenido acceso a la evidencia

Proceso pre-investigación (I)

- Fotografiar el equipo sin desmontar (apagado con el cartel de número de serie).
- Fotografiar el equipo desmontado (con el cartel visualizando números de serie de hardware).
- Fotografiar la configuración del equipo por dentro.
- Apuntes en el cuaderno de todos los pasos.
- Montar el disco (nodev, noexec, ro): de modo que no se pueda realizar ninguna modificación sobre él.
- Imágenes del disco (3): copias o clones idénticos del contenido y estructura.

Proceso pre-investigación (II)

- Generación de md5sum del disco de cada una de las particiones: cálculo del código que identifica cada una de las particiones del disco duro a partir de su contenido de forma única.
- Generación de md5sum de cada de las 3 imágenes del disco (tienen coincidir): cálculo del mismo código de los clones para asegurar que no han sufrido alteración en la copia.
- Grabación de las 2 imágenes en una cinta magnética (comprobar MD5 tiene que coincidir con la imagen y del disco) u otro soporte: para poder realizar el análisis a partir de una de ellas, disponiendo de otra en caso de error o alteración de la primera.

Proceso pre-investigación (III)

- Etiquetar el disco duro original y las 2 cintas (etiqueta, iniciales analista, acompañante, MD5): para mantener una identificación de los componentes físicos.
- Fotografiar el disco duro original y las 2 cintas juntas (se tiene que ver la fecha, hora y las etiquetas): pasa corroborar la existencia de las copias y originales entregados al custodio.
- Guardar el disco duro original y las cintas en una caja fuerte. Entregar las llaves al Cliente o Autoridades.

Proceso pre-investigación (IV)

- Desde este momento, cuando sea necesario, y bajo la supervisión del testigo adecuado, podrá extraer la copia necesaria para llevar a cabo los análisis para la obtención de las pruebas digitales necesarias.
- Una opción muy recomendable es seguir todos estos pasos con un testigo que dé fe que se han seguido todas las indicaciones para realizar las copias y no se ha realizado ninguna otra acción sobre los sistemas o los datos más que los puramente necesarios para realizar las copias imagen o clon de los discos duros.

¡Y todavía no hemos empezado a investigar!

Entornos de trabajo

- El Análisis Forense debe realizarse en una red aislada, con equipos preparados para tal fin, pero no es imprescindible emplear un equipo comercial de A.F. Podemos construir uno con los mismos requerimientos nosotros mismos.

Aplicación real del Análisis Forense

- La aplicación real de la I.F. Suele tener dos aplicaciones que muchos expertos prefieren diferenciar:
  - **Computer forensics**: es aquel Análisis Forense relacionado con la investigación de situaciones donde está implicado el uso de un sistema informático o de una evidencia digital, pero donde el crimen cometido puede ser de cualquier tipo, no sólo propio de los Sistemas de Información (robos de información, fraudes, delitos a la propiedad intelectual, etc.)
  - **Intrusion forensics**: es aquel Análisis Forense relacionado con la investigación de ataques o comportamientos sospechosos contra sistemas informáticos o de crímenes propios únicamente de estos (intrusiones, ataques DoS, etc.).

Modos de Análisis Forense

- **Análisis post-mortem**: Es el análisis que se realiza con un equipo dedicado específicamente para fines forenses para examinar discos duros, datos o cualquier tipo de información recabada de un sistema que ha sufrido un incidente. En este caso, las herramientas de las que podemos disponer son aquellas que tengamos en nuestro laboratorio para el análisis de discos duros, archivos de logs de firewalls o IDS, etc.

- **Análisis en caliente**: Es el análisis que se lleva a cabo de una sistema que se presume a sufrido un incidente o está sufriendo un incidente de seguridad. En este caso, se suele emplear un CD con las herramientas de Respuesta ante Incidentes y Análisis Forense compiladas de forma que no realicen modificaciones en el sistema. Una vez hecho este análisis en caliente, y confirmado el incidente, se realiza el análisis post-mortem.

Información útil en A.F. (I)

Ficheros eliminados / Espacio libre en disco:

- Cuando un fichero es eliminado, no quiere decir que su contenido se haya borrado. Esta acción simplemente puede querer decir que la entrada de este fichero se ha eliminado de la tabla de ficheros en disco.
- Cuando se realiza A.F. sobre un disco es importante no realizar ningún tipo de modificación de manera que sea posible recuperar la mayor cantidad de ficheros eliminados.
- Además, cuando los ficheros se eliminan, el espacio que ocupaban puede ser ocupado parcialmente, permaneciendo partes de estos ficheros todavía en disco.

Información útil en A.F. (II)

MAC Times:

- Cada entrada del Sistema de Ficheros mantiene tres fechas y horas de todas las entradas que se encuentran en este (ficheros, directorios, links, etc.).
- Éstos son muy importantes en el análisis de máquinas comprometidas o analizadas.
- Los MAC Times son:
  - Modificación (Modification): Cambios en el fichero o directorio a nivel de su contenido.
  - Acceso (Access): Acciones de lectura, escritura (puede no implicar cambio), etc.
  - Cambio (Change): Cambio a nivel de características del fichero (permisos, usuario propietarios, etc.)

Información útil en A.F. (III)

Ficheros de Logging:

- Casi todos los sistemas registran la actividad de sus usuarios, servicios, aplicaciones, etc.
- Si analizamos estos registros, e incluso si podemos correlar eventos entre varios de estos ficheros (IDS+Firewall, Firewall+HTTP Server, etc.), el análisis puede ser mucho más concluyente.

Información útil en A.F. (IV)

System State:

- Es la información más fácilmente modificable y eliminable, dado que si el sistema se apaga o se realiza alguna acción prematura, puede modificarse.
- El System State o Estado de la Máquina engloba los programas que se están ejecutando, las conexiones establecidas (estableciéndose, abiertas, cerrándose o cerradas), los datos temporales, etc.
- Existen dos opciones en A.F. una de ellas afirma que esta información es demasiado importante como para perderla y debe intentar obtenerse antes de apagar o aislar el sistema, aún corriendo el riego de alertar a un posible atacante o de realizar alguna modificación sobre ella. La otra opción del A.F. Afirma que cualquier modificación sobre el sistema no es justificable, con lo que aboga por la desconexión del sistema (no apagado con botón ni mediante S.O.) para un posterior análisis.

Herramientas Open Source

- Desde finales de los 90, la Informática Forense se ha hecho popular (sobretodo en USA).
- En España, la informática forense empezó a aparecer en congresos o meetings de eventos relacionadas con seguridad y el hacking en el 2001 (Hackmeeting (Leioa, Euskadi), NcN (Mallorca), Securmática (Madrid), etc.).
- La comunidad en Internet ha ido desarrollando gran cantidad de herramientas, que pueden equipararse (si no por separado, si de forma conjunta) a las herramientas comerciales, con unos costes por licencia al alcance de muy pocos.

The Coroner's Toolkit (TCT)

- TCT es un suite de programas creados por dos de los pioneros en la I.F. Dan Farmer and Wietse Venema.
- Fue presentado en Agosto de 1999 en un curso de Análisis Forense.
- Están pensadas para realizar el análisis de un sistemas *NIX después de una intrusión.
  - **grave-robber**: captura información del sistema
  - **ils** / **mactime**: muestran los MAC times de ficheros.
  - **unrm** / **lazarus**: permiten recuperar ficheros borrados.
  - **findkey**: recupera claves criptográfica de un proceso en ejecución o de ficheros.

The Sleuth Kit (TSK) (I)

- Es un conjunto de herramientas de linea de comandos para sistemas *NIX.
- Su primer desarrollo, llamado TASK, fue mantenido por @stake. De aquí su nombre The @stake Sleuth Kit.
- Actualmente su desarrollo es independiente y abierto.
- Está basado en The Coroner's Toolkit y en los añadidos a éste que hacia tct-utils, ampliando las funcionalidades de ambos.

TSK: Las herramientas (I)

- **File System Layer Tools**: Estas herramientas permiten el análisis de los sistemas de ficheros, su estructura, tablas de índices, ficheros, bloques de arranque, etc.
  - **fsstat**: Muestra detalles sobre el sistema de ficheros y datos sobre su uso, estructura, etiquetas, etc.

TSK: Las herramientas (II)

- **File Name Layer Tools**: Estas herramientas de análisis de sistema de ficheros permiten procesar estructuras de nombres de ficheros, que suelen estar localizadas en los directorios padre.

  - **ffind**: Localiza nombres de ficheros en uso o eliminados que apunten a una estructura útil de información.

  - **fls**: Localiza los ficheros en uso o elimiandos dentro de una entrada de directorio.

TSK: Las herramientas (III)

- **Data Unit Layer Tools**: Estas herramientas de sistemas de ficheros procesan las unidades de datos donde se encuentra almacenado el contenido de los ficheros (p.e. clusters en FAT y NTFS y bloques y fragmentos en EXTxFS y UFS).
  - **dcat**: Extrae el contenido de una unidad de datos.
  - **dls**: Lista los detalles sobre una unidad de datos y extrae el espacio no reservado del sistema de ficheros.
  - **dstat**: Muestra las estadísticas de una unidad de datos dada en un formato legible.
  - **dcalc**: Calcula donde se encuentran las unidades de datos de una imagen de espacio no ocupado (obtenida mediante dls) en la imagen original. Es muy útil cuando se recuperan evidencias en espacio no ocupado y quiere obtenerse su posición original.

TSK: Las herramientas (IV)

- **Media Management Tools**: Estas herramientas toman como entrada una imagen de disco (u otro medio) y analizan las estructuras de datos en que se organiza. Pueden ser utilizadas para encontrar datos ocultos en particiones y extraer las particiones de un disco de forma que el Sleuth Kit las pueda utilizar.
- Soportan particiones DOS, etiquetas de disco BSD, Sun VTOC () y particiones Mac.
  - **mmls**: Muestra la estructura de un disco, incluyendo el espacio no ocupado. La salida identifica el tipo de partición y su tamaño, facilitando la utilización del comando ‘dd’ para extraer particiones. La salida se ordena basándose en el sector de inicio de forma que es fácil identificar huecos en la estructura del disco.

TSK: Las herramientas (V)

- **Otras Herramientas**:
  - **hfind**: Utiliza un algoritmo de ordenación binario para realizar búsquedas de hashes en base de datos de hashes creadas con md5sum (Ej. NIST NSRL, Hashkeeper y otras propietarias).
  - **mactime**: Recibe la entrada de las herramientas fls y ils, creando una línea temporal en la actividad de un fichero.
  - **sorter**: Ordena ficheros basándose en el tipo, chequea extensiones y realiza búsqueda en base de datos de hashes.

Autopsy

- Es una interfaz gráfica para las herramientas de línea de comandos utilizadas para el análisis forense digital y contenidas en el Sleuth Kit.
- En conjunto, Sleuth Kit y Autopsy proporcionan muchas de las características que productos comerciales para el análisis de sistemas de ficheros Windows y UNIX (NTFS, FAT, FFS, EXT2FS y EXT3FS).
- Debido a que Autopsy está basada en HTML, es posible realizar una conexión al servidor Autopsy desde cualquier plataforma utilizando un navegador Web. Autopsy proporciona una interfaz similar a un gestor de ficheros, mostrando al detalle información sobre datos eliminados y estructuras del sistema de ficheros.

mac-robber

- Es una herramienta que recopila información de ficheros localizados en un sistema de ficheros montado (mounted). Estos datos pueden ser utilizados por la herramienta mactime, contenida en el Sleuth Kit, para elaborar una línea temporal de actividad de los ficheros.
- Está basado en grave-robber (contenido en TCT) y está escrita en lenguaje C en lugar de Perl.
- Requiere que el sistema de ficheros esté montado por el sistema operativo, a diferencia de otras herramientas como el Sleuth Kit que procesan el sistema de ficheros ellos mismos. Por lo tanto, mac-robber no recopilará datos de ficheros eliminados o ficheros que están ocultos por rootkits. mac-robber también modificará los tiempos de acceso a directorios que están montados con permisos de escritura.
- Es útil cuando demos con un sistema de ficheros que no está soportado por el Sleuth Kit u otras herramientas de análisis forense.
- Se puede ejecutar en sistema de ficheros UNIX que hayan sido montados en sólo lectura en un sistema de confianza. También se puede utilizar durante la investigación de sistema UNIX comunes como es el caso de AIX.

Foundstone Forensic Utilities

- **Pasco**: Herramienta para analizar la actividad realizada con el navegador web Internet Explorer de MS .
- **Galleta**: Examina el contenido del fichero de cookies de IE.
- **Rifiuti**: Examina el contenido del fichero INFO2 de la papelera de reciclaje de Windows.
- **Vision**: Lista todas los puertos TCP y UDP en escuha (abiertos) y los mapea a las aplicaciones o procesos que se encuentran detrás.
- **Forensic Toolkit**: Es una suite de herramientas para el análisis de las propiedades de ficheros Examina los ficheros de un disco en busca de actividad no autorizada y los lista por su última fecha de acceso, permitiendo realizar búsquedas en franjas horarias, busqueda de archivos eliminados y data streams (utilizados para ocultar información en sistemas NT/2K). Obtener atributos de seguridad de ficheros. Ver si un servidor revela información mediante NULL Sessions. Y un largo etcétera.

Forensic and Log Analysis GUI (FLAG)

- Diseñado para simplificar el proceso de análisis de ficheros de log en investigaciones forenses.
- Cuando se realizan investigaciones con grandes volúmenes de información, los eventos deben ser correlados para facilitar la obtención de resultados. FLAG emplea bases de datos para facilitar este tratamiento de información
- Está basado en web, por lo que puede instalarse en un servidor donde se centralice toda la información de los análisis, de forma que puede ser consultada por todo el equipo forense
- FLAG se inició como un proyecto del “Australian Department of Defence”.
- Ahora es un proyecto abierto al público en Sourceforge.
- pyFlag es la implementación (empleada actualmente) en Python. Es una revisión/reescritura completa de FLAG, más potente, versátil y robusta.

Foremost

- Permite recuperar ficheros basándose en sus cabeceras y sus pies. is a console program to recover files based on their headers and footers.
- Puede trabajar sobre archivos de imágenes, como los generados con dd, Safeback, Encase, etc. o directamente sobre un disco o partición.
- Las cabeceras y pies pueden especificarse a través de su archivo de configuración, por lo que podemos especificar busquedas para formatos específicos para nosotros.
- Su desarrollo inicial fue encabezado por la “United States Air Force Office of Special Investigations”, pero ahora es un proyecto GPL abierto al público.

HELIX

- HELIX es una customización basada en KNOPPIX.
- Esta distribución permite elegir entre usar los kernels 2.4.26 o 2.6.5).
- Emplea el gestor de ventanas Fluxbox.
- Tiene una excellente detección de hardware.
- HELIX está pensado específicamente para no realizar ningún tipo de alteración sobre los sistemas en los que se usa.
- También tiene una configuración autorun para Windows con herramientas para este SO.
- HELIX es la distribución empleada por SANS en el Track 8 de su curso de “System Forensics, Investigation and Response”.

FIRE (Forensic and Incident Response Environment)

- FIRE es una distribución de un único cdrom, portable y bootable cuyo objetivo es proveer de las herramientas adecuadas para una actuación rápida en casos de análisis forense, respuesta ante incidentes, recuperación de datos, ataque de virus o intrussion testing.

- Uno de los aspectos más llamativos es que a parte de ser un CD bootable Linux, también contiene gran cantidad de herramientas de análisis forense para win32, sparc solaris y Linux usable para análisis en caliente de sistemas, con lo que únicamente montando el CD podemos usar herremientas compiladas estáticamente sin necesidad de realizar un reboot de la máquina.

Conociendo al enemigo (I)

- La mejor manera de conocer como actúa un atacante es analizando un ataque.
- La mejor manera de capturar estos ataques es mediante Honeypots.
- Un Honeypot es una máquina preparada para funcionar como un cebo para atacantes.
- Cuando se sufre un ataque o una intrusión efectiva todo la actividad queda registrada para poder llevar a cabo un posterior análisis.
- El proyecto más famoso en este sentido es Honeynet.org

Conociendo al enemigo (II)

- Honeynet.org es un punto de encuentro para la realización y publicación de investigaciones sobre ataques e intrusiones y otro tipo de situaciones donde aplicar análisis forense.
- Existen retos abiertos a todo aquel que quiera participar, siendo un gran método de aprendizaje, aprendiendo de expertos de todo el mundo: Scan of the Month Challenges.

El futuro (I)

- La investigación forense debe extenderse a los nuevos dispositivos donde se almacena información digital y debe conocer los nuevos métodos empleados en intrusión.
- Debe aprender cuales son los métodos de ocultación de información en los ordenadores (TCT no era capaz de descubrir información oculta aprovechando una deficiencia del sistema de ficheros en Linux).
- Es necesario incrementar la eficiencia en el A.F. De grandes volúmenes de información.
- Es necesario concienciar y formar a usuarios, miembros de la justicia y empresas que la I.F. Es una ciencia más para obtener y resolver crímenes o delitos en los que se empleó un ordenador.

El futuro (II): PDAs

- El análisis forense de PDA pertenece al presente.
- Las PDAs tienen más memoria, más vías de acceso (WiFi, Bluetooth, USB, etc.) esto implica el aumento de la capacidad para realizar intrusiones a dispositivos personales.

El Futuro (III): Móviles

- Los teléfonos móviles, cada vez se parecen más a los PDAs, esto implica que pueden almacenar más información: agendas, mensajes de diferentes tipos (SMS, MMS, emails, etc.), contactos, etc.

El Futuro (IV): Dispositivos de Almacenamiento

- En los dos últimos años han proliferado pequeños dispositivos de almacenamiento altamente portátiles, con formas, diseños y ergonomía muy dispares, pero con capacidades enormes.

El Futuro (IV): Electrodomésticos

- Si los electrodomésticos que encontremos en una casa se conectan a Internet...
- ¡HE TENIDO UNA INTRUSIÓN EN MI NEVERA Y ME HAN ROBADO RECETAS SECRETAS!

Técnicas Anti-forenses:

- Las técnicas de Análisis Forense están basadas en la recuperación y análisis de información existente, borrada u oculta en disco.
- ¿Y si el intruso no usa el disco para comentar la intrusión ni durante esta?
- Se han desarrollado diversos métodos para explotar máquinas sin tener que escribir en disco nada.
- Existen herramientas de pen-testing que emplean estas técnicas (comerciales) y también algún proyecto Open-Source.

Bibliografía

- Mohay, George; Anderson, Alison; Collie, Byron; de Vel, Olivier; McKemmish, Rodney: "**Computer and intrusion forensics**". Artech House. 2003. ISBN 1-58053-369-8.
- Marcella, Albert J.; Greenfield, Robert S.; Abraham, Abigail; Deterdeing, Brent; Rado , John W.; Sampias , William J.; Schlarman, Steven; Stucki, Carol: "**Cyber Forensics—A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes**". Auerbach Publications (CRC Press). 2002. ISBN 0−8493−0955−7.
- Littlejohn Shinder, Debra; Tittel, Ed: "**Scene of the Cybercrime: Computer Forensics Handbook**". Syngress Publishing, Inc. 2002. ISBN: 1-931836-65-5.
- Schweitzer, Douglas: "**Incident Response: Computer Forensics Toolkit**". Wiley Publishing, Inc. 2003. ISBN: 0-7645-2636-7.

Bibliografía (Herramientas (I))

- The Coroner's Tookit (TCT):
  http://www.porcupine.org/forensics/tct.html
- The Sleuth Kit (TSK) :
  http://www.sleuthkit.org/sleuthkit/index.php
- Autopsy:
  http://www.sleuthkit.org/autopsy/index.php
- mac-robber:
  http://www.sleuthkit.org/mac-robber/index.php
- Foundstone Forensic Utilities:
  http://www.foundstone.com/resources/forensics.htm
  http://odessa.sourceforge.net/

Bibliografía (Herramientas (II))

- Forensic and Log Analysis GUI (FLAG):
  http://pyflag.sourceforge.net/
- Foremost:
  http://foremost.sourceforge.net/
- HELIX Live CD:
  http://www.e-fense.com/helix/
- FIRE Live CD:
  http://fire.dmzs.com/
- Foreinsect (índice muy completo de herramientas de A.F.):
  http://www.forinsect.de

Bibliografía (Proyectos y más)

- Honeynet Project:
  http://www.honeynet.org
- SANS Institute (SANS InfoSec Reading Room):
  http://www.sans.org/rr/
- Página web de Wietse Venema
  http://www.porcupine.org/
- Forensics-es:
  http://www.forensics-es.org
- Codes of Practices for Digital Forensics:
  http://cp4df.sourceforge.net
- Phrack:
  http://www.phrack.org
- Códigos éticos en I.F. y seguridad en general:
  http://www.isc2.org/
  http://www.osstmm.org/
  http://www.thesedonaconference.org/

Daniel Fernández Bleda

dfernandez@isecauditors.com

Sevilla, Hackmeeting 2004

1/11/2004