Análisis forense de sistemas Windows

Raúl Siles
Consultor de Seguridad, HP

David Pérez Conde
Consultor independiente de seguridad

Ponentes

- **Raúl Siles**

  Consultor de Seguridad, HP

  GCIH, GCIA, GSNA, GCUX, GCFW, GCFA

  raul.siles@hp.com

- **David Pérez Conde**

  Consultor independiente de seguridad

  GCIH, GCIA, GSNA, GCWN, GCFW, GCFA

  david.perez.conde@gmail.com

Agenda (I)

PARTE I:

Análisis forense de **sistemas de ficheros** de Windows

- Definición y términos
- Respuesta e investigación de incidentes
- Metodología y tipos de análisis forenses
- Situación en España
- Análisis forense en Windows: mitos
- Capas de almacenamiento
- Almacenamiento en Windows: estructuras y funcionamiento
- Demostración

Agenda (II)

PARTE II:

Análisis forense de **binarios desconocidos** de Windows

- Análisis estático
- Análisis de comportamiento
- Análisis de código

PARTE I
Análisis forense de sistemas de ficheros de Windows

Definición de "*forense*"

forense1.(Del lat. *forensis*).

1. adj. Perteneciente o relativo al foro.

2. adj. ant. Público y manifiesto.

3. com. **médico forense:**

1. m. y f. médico encargado por la justicia para dictaminar los problemas de medicina legal.

Medicatura forense:

1. f. *Ven.* Organismo que actúa en los casos que tienen implicación legal.

forense2.(Del lat. *foras*, fuera).**1.** adj. p. us. forastero**.**

Real Academia Española, 2005

Definición de "*análisis forense*" (I)

"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 qué ocurrieron sobre un sistema en el pasado".

Farmer y Venema, 1999

"El proceso de identificar, preservar, analizar y presentar evidencias digitales que puedan ser aceptadas legalmente".

McKemmish, 1999

Definición de "*análisis forense*" (II)

Ciencia centrada en la búsqueda de la VERDAD

¿Qué, Dónde, Cuándo, Porqué, Quién, Cómo?

Términos

- Evidencia: ¿Cúal es la mejor evidencia?
- Cadena de custodia.
- Lista de términos asociados a la investigación.
- Imágenes.
- Integridad: *hashes.*
- Principio de intercambio de Locard:

  "*Cada contacto deja un rastro*"

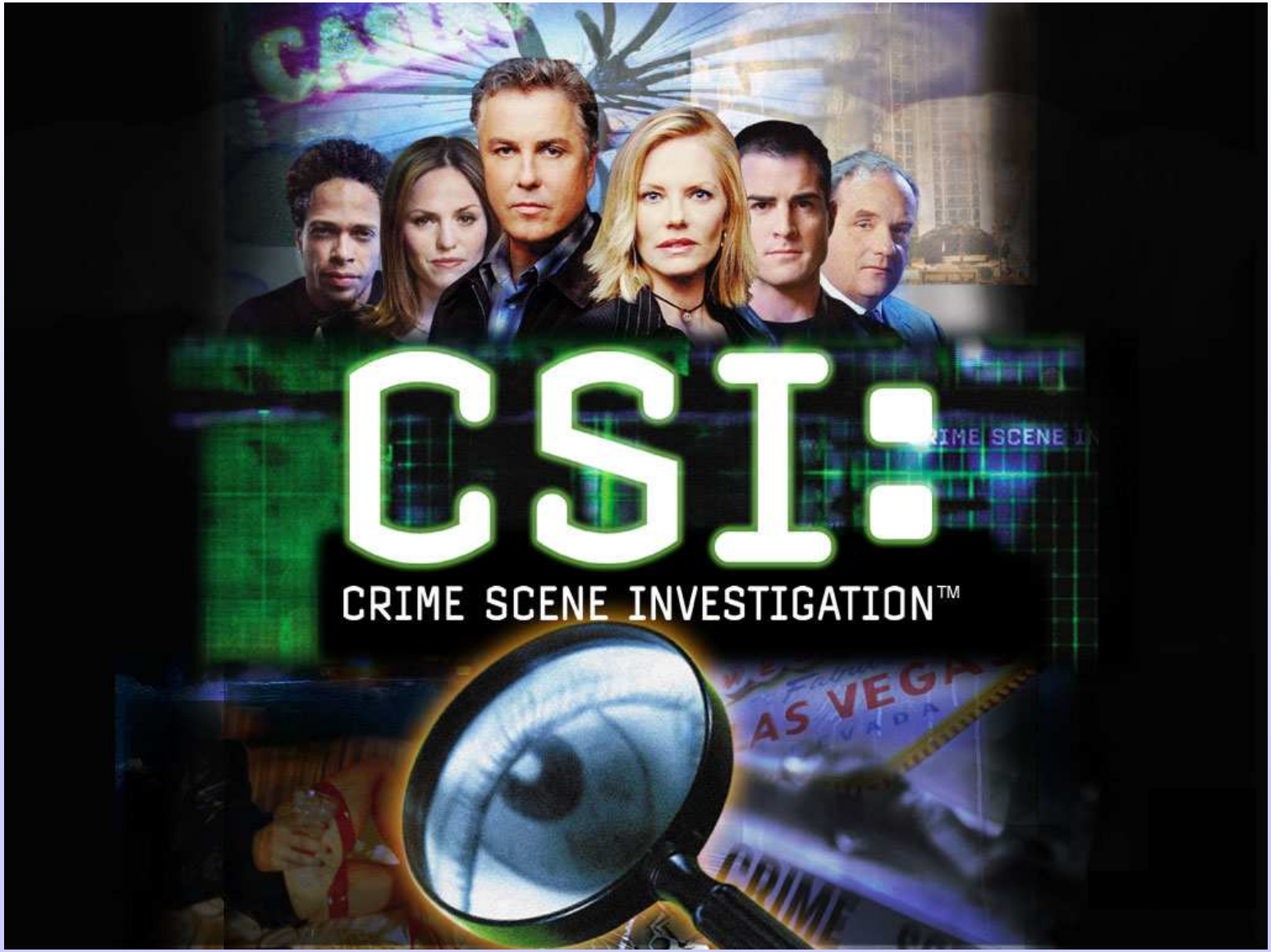
Respuesta ante incidentes

- Investigación de **incidentes de seguridad**:
  - Política y procedimientos de respuesta ante incidentes.
  - Configuración de la infraestructura informática:

    NTP, logs, backups, BBDD integridad…

  - **Verificación del incidente**…

"… fotografiar la *escena del crimen*."



Investigación y/o respuesta ante incidentes de seguridad

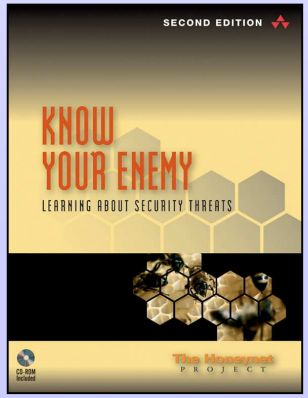
Primeros auxilios vs Forenses

1º) Salvar vidas
2º) Preservar la evidencia

¿Dónde está el cadaver en la informática forense?

Metodología

- Adquisición de evidencias:
  - **Minimizar la pérdida de datos** y de evidencias.
  - Evitar modificar/añadir datos al sistema: acciones.
- Análisis de las evidencias: “encontrar la verdad”.
  - **Mantener un registro exhaustivo** del análisis.
  - **Analizar todos los datos recolectados**.
- **Informes** de resultados: descubrimientos.



Tipos de análisis forenses

- Sistemas “vivos”:
  - Memoria física, memoria virtual (*pagefile*), conexiones de red, procesos en ejecución, ficheros abiertos…
  - Análisis forense del tráfico de red.
- Sistemas “muertos”:
  - Adquisición de imágenes de los discos: fijos y extraibles.
  - Adquisición de datos de logs: IDS, firewalls, routers, servidores, clientes, aplicaciones… ¡¡correlación!!

¿Apagar o no apagar? Esa es la cuestión ;-)

Principio de indeterminación de Heisenberg

España: Legalidad e Instituciones

- Código Penal.
- "Convenio sobre Ciberdelincuencia". Consejo de Europa. 2001.

- Guardia Civil: "Grupo de delítos telemáticos"
  http://www.guardiacivil.org/telematicos/index.htm
- Cuerpo Nacional de Policía: "Brigada de Investigación Tecnológica (BIT)"
  http://www.mir.es/policia/bit/index.htm

Análisis forense en Windows: mitos

- Funcionalidades no documentadas.
- Acceso nativo al disco: “complejo/herramientas”.
- Interfaz gráfico de usuario: “falta de pistas”.
- Plataforma muy común hoy en día en incidentes de seguridad.

Capas de almacenamiento

- Física: “el disco”.
- Datos: “bloques o *clusters* (unidades direccionables)”.
  - Sectores: 512 bytes.
- Metadatos: “información de las estructuras del SF”.
  - Punteros, *MAC times*, seguridad…
- Sistema de ficheros: “información del SF”.
  - Tamaño de las unidades de datos, información de montaje, sector arranque, localización de áreas críticas…
- Nombrado de ficheros: “nombres”.

Almacenamiento en Windows (I)

- Particiones DOS (x86)
- Sistemas de ficheros:
  - FAT12, FAT16, FAT32, NTFS.
  - EFS, compresión, *NT disksets* (spanned, striped, mirrored, RAID 5).
- Metadatos:
  - FAT (File Allocation Table): *FAT*
  - MFT (Master File Table): *NTFS*
- MFTE (MFT Entries) y DE (Directory Entries).

A. Windows (II): estructuras

- **FAT16** (16 bits): 2^{16} = 65536 clusters
- Max. cluster = 32KB
- Max. tamaño = 2GB

Tamaño partición (MB):	32	64	128	256	512…
Tamaño cluster (KB):	0.5	1	2	4	8…

- **FAT32** (32 bits): 2^{28} = 256x 2^{20} clusters (G#)
- Max. cluster = 4KB (< 8GB) o 8KB (> 8GB)
- Max. tamaño = 2TB
- Según versión sistema operativo Windows: 32KB – 8TB

A. Windows (III): estructuras

- **NTFS** (64bits): "MFT Entries"
  - Atributos residentes (información estándar (tiempos), nombre fichero, seguridad, datos…) y no residentes (datos ficheros largos, descriptores de seguridad, índices…).
  - $STANDARD_INFORMATION, $FILENAME, $DATA
- Timestamps: 4 ($FILENAME) + 4 ($STANDARD)
- Unicode/ASCII.

Tamaño partición (GB):	<0.5	<1	<2	>2
Tamaño cluster (KB):	0.5	1	2	4

A. Windows (IV): funcionamiento

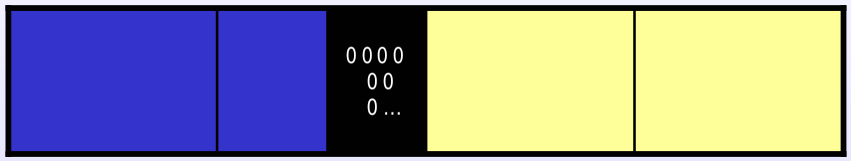
- Creación y borrado de ficheros:
  - **Metadatos:**
    - Gestión de entradas MFT (árboles ordenados) o FAT (listas).
    - Actualización de tiempos.
    - Gestión de estructuras y atributos:

      NTFS: IN_USE *flag, $MFT, $MFTMIRR, $BITMAP…*

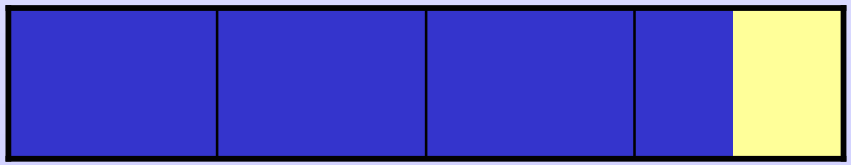
      FAT: FAT0, FAT1, Root Directory…
  - **Datos:**
    - Redistribución de clusters.
    - Reescritura de las áreas de datos.
    - Relación entre datos y metadatos.

A. Windows (V): funcionamiento

- *Slack space* en Windows*:*
  - NTFS: Escritura basada en sectores/cluster (ceros).



  - FAT: Escritura basada en datos/cluster.



Demostración

Sistema: "muerto" (análisis de un disco USB).
Sistema de ficheros: FAT16.
Tamaño del disco: 64MB.

- Análisis de Windows mediante Linux (herramientas *open source*):
  - comandos del SO, TSK + Autopsy, hexedit, ethereal, clientes estándar (navegador Web, MS Word…), compilador cygwin, herramientas de análisis de *malware* en Windows…

"SANS/GIAC **GCFA**"

Análisis completo disponible en:
www.raulsiles.com

DEMO: Metodología

- Verificación y descripción del incidente
- Adquisión de evidencias
- Obtención de imágenes de las evidencias
- Análisis inicial
- Creación y análisis del *timeline*
- Análisis específico de Windows
- Recuperación de datos
- Análisis del los datos recuperados
- Análisis de *strings*
- Informe

DEMO: Verificación y descripción del incidente

- Caso de acoso entre empleados de una compañía.
- Acoso en persona y a través de e-mail.
- Encuentro físico en una cafetería.
- Evidencia: “disco de memoria USB”.

DEMO: Adquisición de evidencias

```
- Tag #: USBFD-64531026-RL-001
- Description: 64M Lexar Media JumpDrive
- Serial #: JDSP064-04-5000C
- Image: USBFD-64531026-RL-001.img
- MD5: 338ecf17b7fc85bbb2d5ae2bbc729dd5
```

Figure A.1: Original chain of custody form

Raul Siles - GCFA

Evidence feature	Description
Date and time evidence was seized:	October 29th, 2004 - 22:30h.
Location and who it was obtained from:	Robert Lawrence's cubicle - Sales department.
Make and model:	64M Lexar Media JumpDrive.
Serial number:	JDSP064-04-5000C.
Name and signature of individual(s) who collected evidence:	Mark Mawer, security administrator (**signature**)
Description:	Standard USB flashdrive (Capacity: 64MB).
Name and signature of person receiving evidence:	Raul Siles, forensic investigator (**signature**)
Case number:	GCFA-v2.0-Option1-11-2004.
Number of evidence (tag):	USBFD-64531026-RL-001.
Hash values (MD5):	338ecf17b7fc85bbb2d5ae2bbc729dd5.
Technical data:	"See text outside this table"
Image name:	USBFD-64531026-RL-001.img
Image size:	62439424 bytes

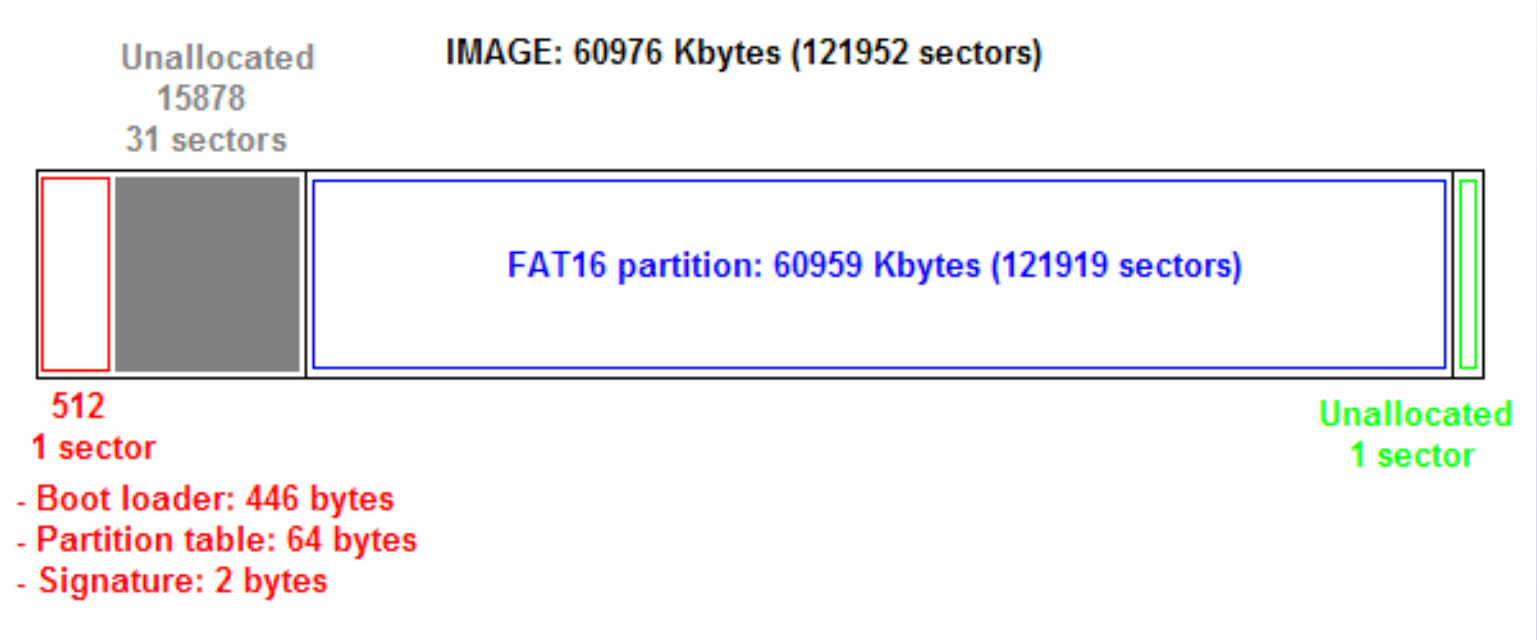
Table A.1: Evidence chain of custody form (extended)

DEMO: Obtención de imágenes de las evidencias

- Minimizar la modificación de la evidencia original.
- Obtención de la firma (integridad) de la evidencia.
- Imagen: copia binaria (bit a bit) de la evidencia.
- Comprobación de la integridad de la imagen.
- Minimizar la modificación de la imagen.
- Cadena de custodía: formularios.

DEMO: Análisis inicial

- Identificación del tipo de disco.
- Identificación de las particiones:



- Extracción de las particiones.

DEMO: Creación y análisis del *timeline*

- Obtención de datos de los ficheros/directorios existentes.
- Obtención de datos de las áreas libres del sistema de ficheros.
- Generación del listado de eventos ocurridos a lo largo del tiempo.
- **Análisis de los eventos…**

DEMO: Análisis específico de Windows

- Autopsy: “Creación del caso”.
- Capas:
  - Física.
  - Sistema de ficheros.
  - Nombrado de ficheros.
  - Metadatos.
  - Datos.

DEMO: Recuperación de datos

- Capa de **datos**.
- Información en el sistema de ficheros:

  ficheros existentes/ocultos, ficheros borrados, fragmentos, memoria virtual (*pagefile*), *slack space*, ficheros encubiertos: *alternate data streams* (ADS) o esteganografía…
- Obtención de **ficheros** (y directorios).

DEMO: Análisis del los datos recuperados

- Herramientas: clientes estándares.
- Información relevante para el caso.
- Nuevas vías de investigación.

PARTE II: Análisis forense de **binarios desconocidos** de Windows

DEMO: Análisis de *strings*

- Lista de términos asociados a la investigación.
- Búsquedas en cantidades de datos elevadas.
- Priorizar las tareas de búsqueda.
- Direcciones IP, fechas, e mails, nombres…
- Confirmación de las evidencias encontradas.

Particiones

- Identificación de las evicencias encontradas.
- Cadenas de texto legibles.

Ficheros

DEMO: Informe

- Características: análisis meticuloso, exahustivo, verificable, reproducible…
- Resumen ejecutivo: comprensible en un juicio.
- Aspectos legales.
- Investigación de incidentes: lecciones aprendidas-recomendaciones de mejora.
- Conexión con el mundo real…

Muchas gracias

"The evidence only knows one thing:
***the truth**. It is what it is."*

Grissom
CSI

PARTE II
Análisis forense de binarios desconocidos de Windows

RaDa.exe

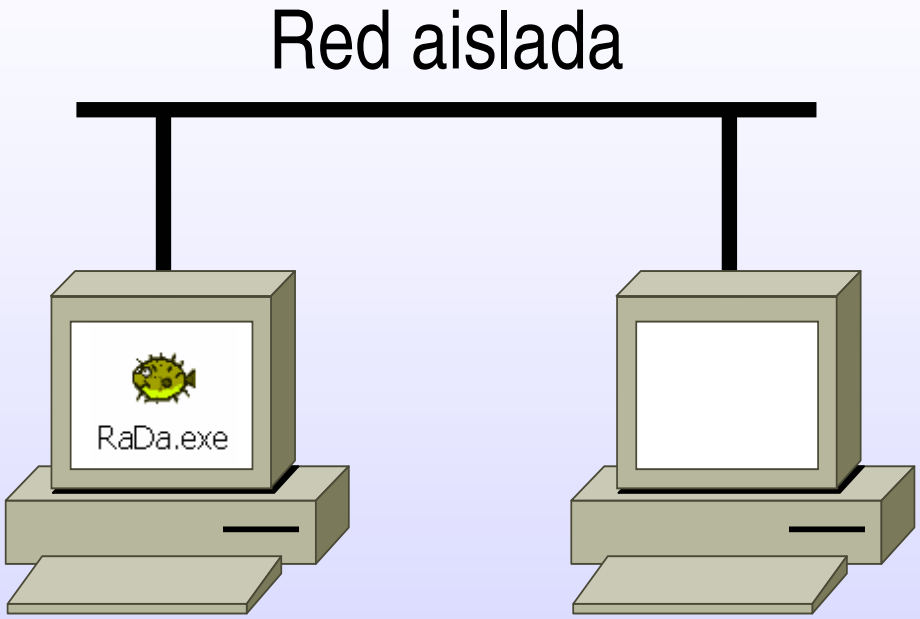
Problema y metodología

- **PROBLEMA:**
  - ¿Qué propósito tiene un determinado fichero ejecutable?

- **METODOLOGÍA DE INVESTIGACIÓN:**
  - Análisis estático
  - Análisis de comportamiento
  - Análisis de código

¡ Entorno estéril y aislado !

Entorno estéril y aislado: ¿virtual?



Sistema "víctima"

Sistema para interacción

Análisis estático (1 de 3)

- **Definición:**
  - Análisis de las características del fichero ejecutable sin ejecutarlo ni desensamblar su código.
- **Importancia:**
  - Comparar resultados.
  - Determinar herramientas e hipótesis para otros análisis posteriores.
  - Documentar, documentar, documentar.

Análisis estático (2 de 3)

- **Datos:**
  - Hash (MD5 y SHA1)
  - Timestamps
  - Sistema operativo
  - Dependencias (compilado dinámica vs. estáticamente)
  - Formato (¿empaquetado?)
  - Cadenas de texto (ASCII, unicode)
  - Información adicional (iconos, compañía, versión, etc.)

Análisis estático (3 de 3)

- **Herramientas:**
  - explorer (NO iexplore.exe)
  - fciv (MS File Checksum Integrity Verifier– No soportado)
  - bintext
  - pexe
  - file (GNU/Linux)

Análisis de comportamiento (1 de 4)

- **Definición:**
  - Análisis de la interacción del fichero ejecutable con su entorno mediante su ejecución en un entorno controlado.
- **Importancia:**
  - Obtener información sobre el programa de manera fácil y rápida.
  - Determinar herramientas e hipótesis para otros análisis posteriores.

Análisis de comportamiento (2 de 4)

- **Datos:**
  - Interacción con el sistema de ficheros.
  - Interacción con el registro.
  - Interacción con la red.
  - Interacción con la lista de procesos.

Análisis de comportamiento (3 de 4)

- **Herramientas:**
  - Filemon
  - Regmon
  - Tdimon
  - Regshot
  - Taskmgr
  - Bintext
  - Ethereal
  - Sistema auxiliar para interacción a través de la red.

Análisis de comportamiento (4 de 4)

- **Procedimiento:**
  1. Arrancar herramientas de monitorización
  2. Capturar el estado inicial del sistema
  3. Ejecutar el binario
  4. Esperar
  5. Terminar la ejecución del binario
  6. Detener las herramientas de monitorización
  7. Capturar el estado final del sistema
  8. Analizar la información obtenida
  9. Realizar modificaciones al entorno y … GOTO 1

DEMOSTRACION: Análisis de comportamiento de RaDa.exe

- RaDa.exe:
  - Ejecutable para S.O. Windows XP/2000/2003.
  - Creado por Raúl Siles y David Pérez para mostrar un ejemplo de troyano puerta trasera.
  - Analizado en el reto “Scan of the month #32”:

    http://www.honeynet.org/scans/scan32/
  - Disponibles en dicha web se encuentran tanto el ejecutable como los análisis realizados.

Análisis de código (1 de 4)

- **Definición:**
  - Análisis del código (ensamblador) del fichero ejecutable.
- **Importancia:**
  - TODA la información sobre lo que hace y no hace el programa está en su código.
  - "TODA" puede ser "DEMASIADA".
  - Permite determinar herramientas e hipótesis para otros análisis posteriores.

Análisis de código (2 de 4)

- **Datos:**
  - Todos:
    - empaquetado/desempaquetado
    - cifrado/descifrado de datos
    - interacciones locales y remotas

Análisis de código (3 de 4)

- **Herramientas:**
  - OllyDbg (Depurador y desensamblador: libre y gratuito)
  - IDA Pro (Depurador y desensamblador: comercial)

Análisis de código (4 de 4)

- **Procedimiento:**
  - Como en PERL: “Hay más de una manera de hacerlo.”
- **Posibles aproximaciones:**
  - Divide y vencerás
  - De lo particular a lo general
  - De lo general a lo particular

DEMOSTRACIÓN: Análisis de código de RaDa.exe

- **RaDa.exe:**
  - Mismo ejecutable que en la demostración anterior.
- **Ejemplos:**
  - Desempaquetado de RaDa.exe.
  - Formato de la página web “RaDa_commands.html”
  - Verificación de un argumento de línea de comandos: *“—authors”.*

¿Preguntas?

¡Muchas gracias!