iSOFT
An IBA Health Group Company

Análisis Forense de un Sistema Windows

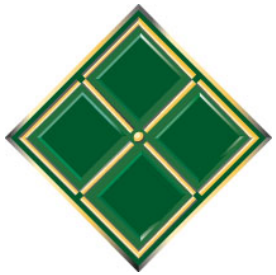
3ª Jornada Tecnológica inFORMANdo

Ismael Valenzuela Espejo
Information Security Specialist
Ismael.valenzuela@isoftplc.com

Agenda

- Introducción al Análisis Forense
- Fases de una investigación
  - Verificación
  - Obtención
  - Análisis
  - Elaboración de informes y custodia de evidencias
- Obtención de evidencias en un sistema Windows
- Aspectos Legales
- Referencias

Acerca de mí



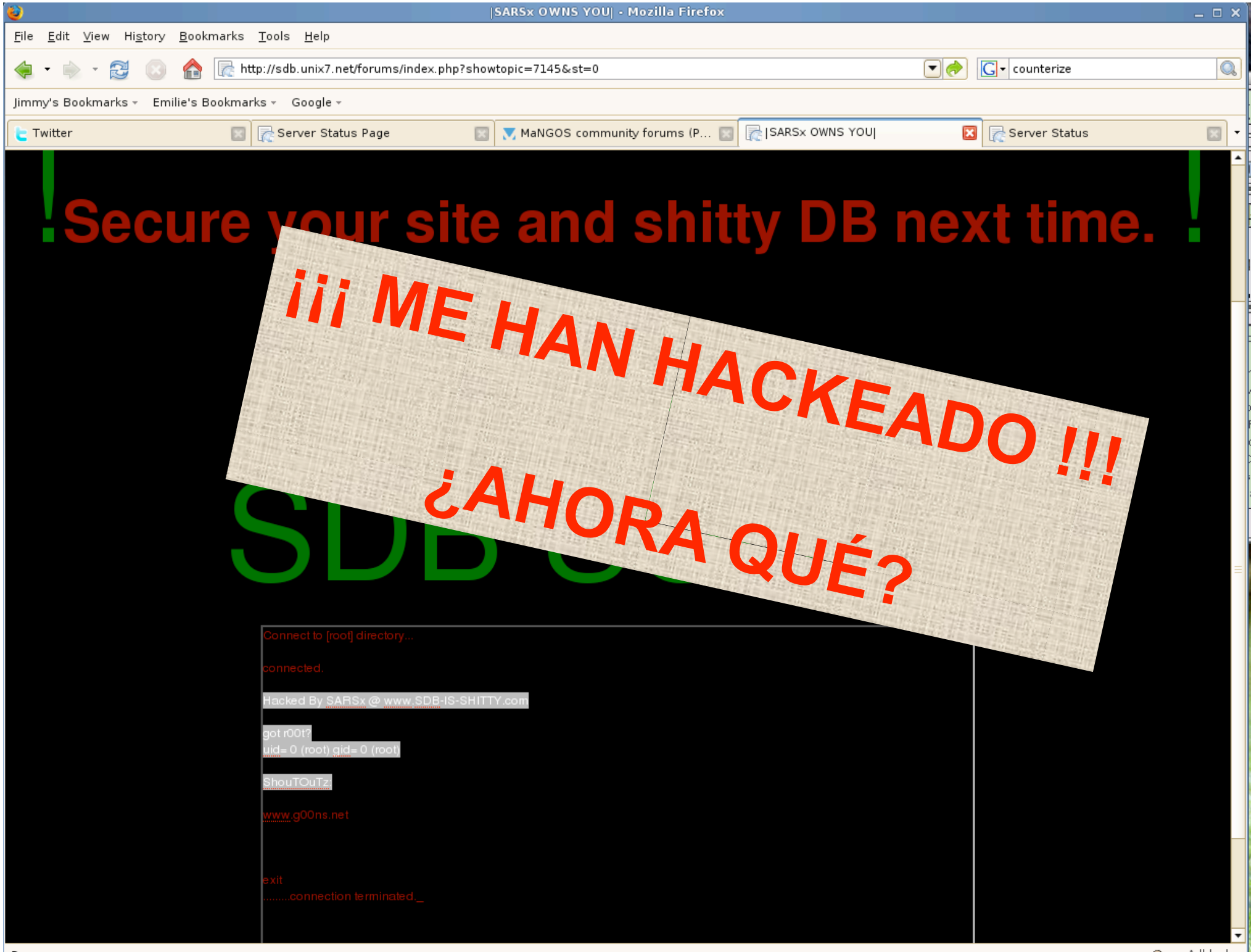
- Information Security Specialist en iSOFT, una compañía del Grupo IBA Health
  - Presente en 5 continentes
  - Más de 3.500 empleados
- Responsabilidades
  - Respuesta ante incidentes
  - Investigaciones forenses / Log Analysis
  - Auditorías de seguridad / Pentests
  - Diseño e implementación de políticas, arquitecturas de seguridad, implementación de ISO 27001, etc..

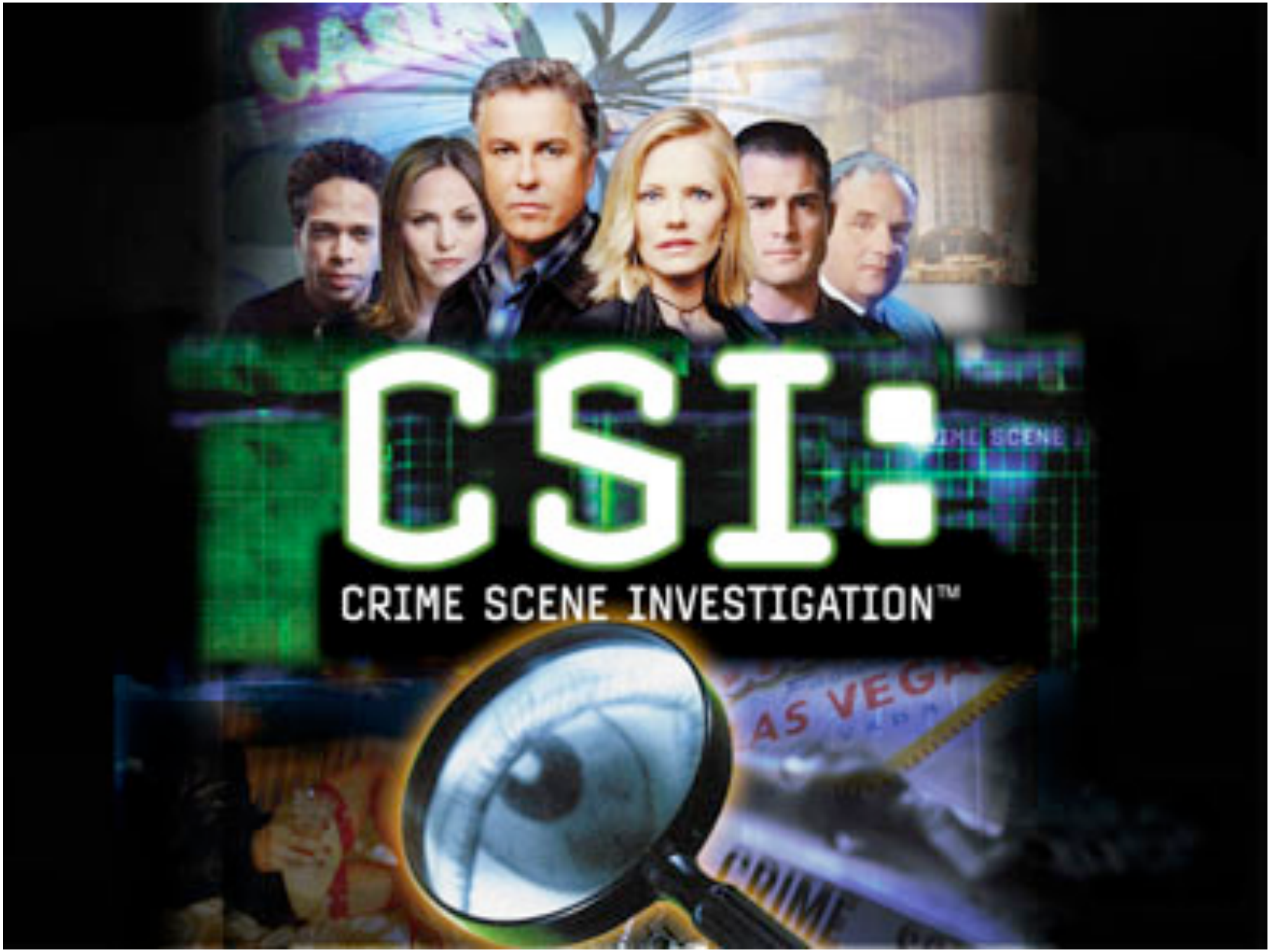
- Certified Information Systems Security Professional (**CISSP**)
- Certified Information Security manager (**CISM**)
- SANS GIAC Certified Intrusion Analyst (**GCIA**)
- SANS GIAC Certified Forensic Analyst (**GCFA**)
- IRCA accredited **ISO 27001** Lead Auditor
- **ITIL** Certified
- Miembro del **SANS GIAC Advisory Board**
- Instructor de **BSi** en ISO 27001, ISO 20000 y BS 27999

Introducción al Análisis Forense

Respuesta a Incidentes vs Análisis Forense

- Fases habituales de la Respuesta a Incidentes:
  - Planificar y preparar
  - Detección del Incidente
  - Contención y Respuesta
  - Recuperación
  - **Análisis (post-mortem)**


|SARSx OWNS YOU| - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://sdb.unix7.net/forums/index.php?showtopic=7145&st=0
counterize
Jimmy's Bookmarks
Emilie's Bookmarks
Google
Twitter
Server Status Page
MaNGOS community forums (P...
|SARSx OWNS YOU|
Server Status
!Secure your site and shitty DB next time. !
¡¡¡ ME HAN HACKEADO !!!
¿AHORA QUÉ?
SDB
Connect to [root] directory...
connected.
Hacked By SARSx @ www.SDB-IS-SHITTY.com
got r00t?
uid= 0 (root) gid= 0 (root)
ShouTOuTz!
www.g00ns.net
exit
.....connection terminated._


CSI:
CRIME SCENE INVESTIGATION™

Introducción al Análisis Forense

¿Qué es un Análisis Forense?

- En “dos palabras”…

- “***Forensic Computing is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable***” (Rodney McKemmish 1999)

- Se basa en el principio “de intercambio de *Locard* ”
  - Edmun Locard (1877-1966), criminalista francés.

Introducción al Análisis Forense

¿Qué es un Análisis Forense?

- **Principio de intercambio de LOCARD**
  - *"siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto"*

Introducción al Análisis Forense

¿Qué es un Análisis Forense?

- **Una investigación forense consta de:**
  - Identificación de la evidencia (verificación)
  - Obtención de la evidencia
  - Análisis y evaluación de evidencias
  - Presentación y almacenamiento de evidencias

- **Incluye los siguientes aspectos:**
  - IDENTIFICAR, PRESERVAR, ANALIZAR y PRESENTAR la **evidencia** de manera adecuada.
  - Debe realizarse siguiendo los estándares apropiados, especialmente si los resultados tienen que poder admitirse en un juicio.

Introducción al Análisis Forense

¿Qué es un Análisis Forense?

- **Tipos de evidencias:**
  - Testimonio humano
  - Tráfico de red
  - Dispositivos de red
  - Sistemas Operativos
  - Bases de Datos
  - Aplicaciones
  - Periféricos
  - Ficheros en discos internos, externos, USB, CD-ROM, etc…
  - Teléfonos
  - Impresoras
  - …¡TODO!

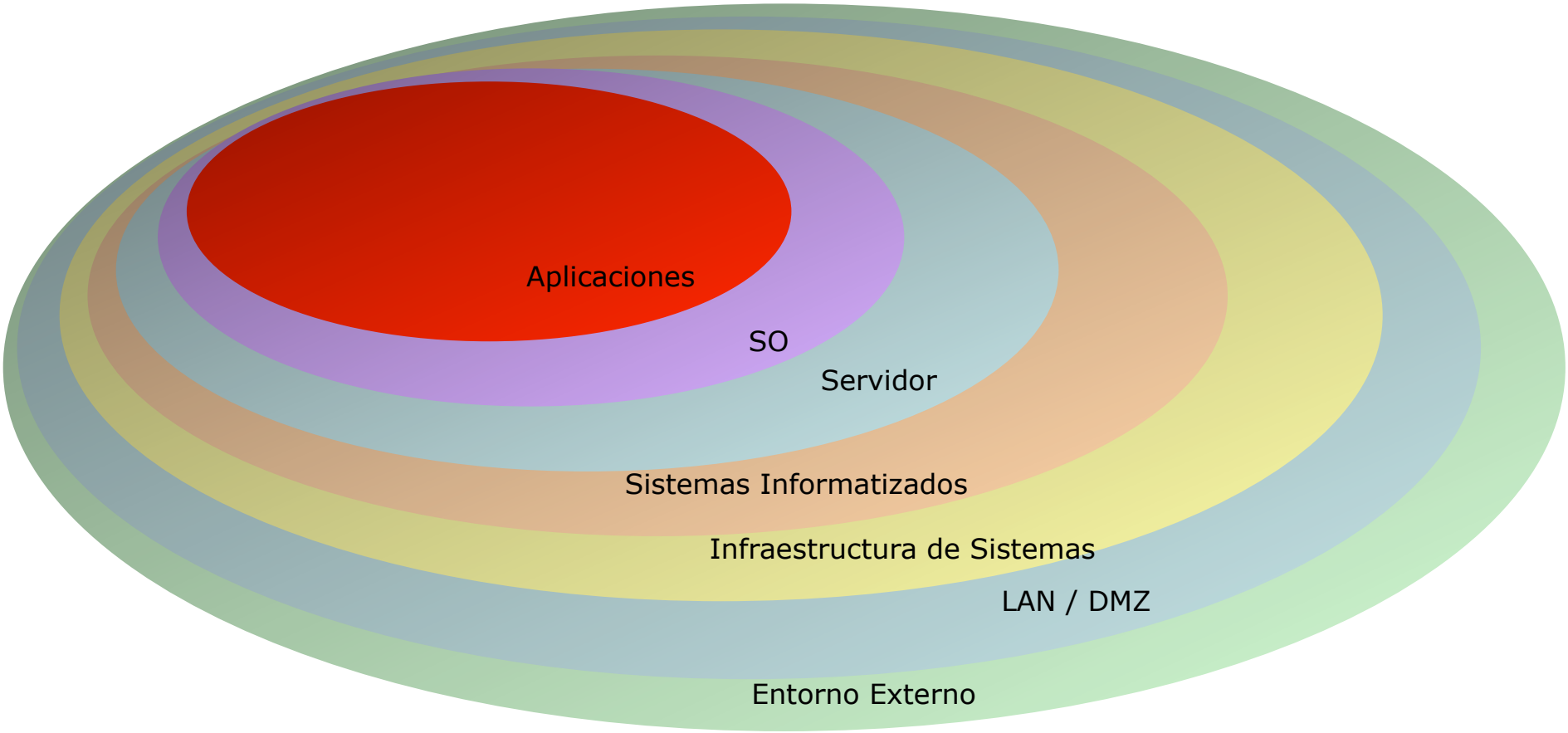
Fases de una Investigación

Inicio

- Usuarios o personal de TI informan de un posible incidente
  - Cuentas bloqueadas, funcionamiento errático o incorrecto de aplicaciones, ficheros desaparecidos, etc.
- Alerta generada por los sistemas de gestión de sistemas
  - Disponibilidad de sistemas, espacio en disco, utilización CPU, intentos de logon, conexiones anómalas, etc.
- Alerta generada por los sistemas de gestión de la seguridad
  - Firewall, IDS, Antivirus, etc.
- Por aviso de terceros
  - Policía, prensa, competidores, etc.
- Por encargo directo

Fases de una Investigación

Verificación - ¿Tienes TODA la información?



Fases de una Investigación

Verificación del incidente

- Los fraudes internos pueden implicar diferentes elementos de un sistema:
  - Múltiples Aplicaciones
  - Sistemas relacionados
    - Infraestructura de red (DNS, DHCP, routers, switches, ...)
    - Sistemas de soporte (directorio, backup, monitorización)
  - Múltiples *hosts*
    - Clientes
    - Front-end
    - Middleware
    - Back-end, Bases de datos

Fases de una Investigación

Obtención de la evidencia

1. Sistema “muerto”
   - Sin corriente eléctrica
   - Sistema ap
   - Disco Duro
   - Discos Extern CD-ROMs, disqueteras, etc...

2. Siste ión
   - Accesos a disco
   - Dispositivos removibles en contínuo cambio

¿TIRO DEL CABLE?

¿APAGO LA MÁQUINA?

Fases de una Investigación

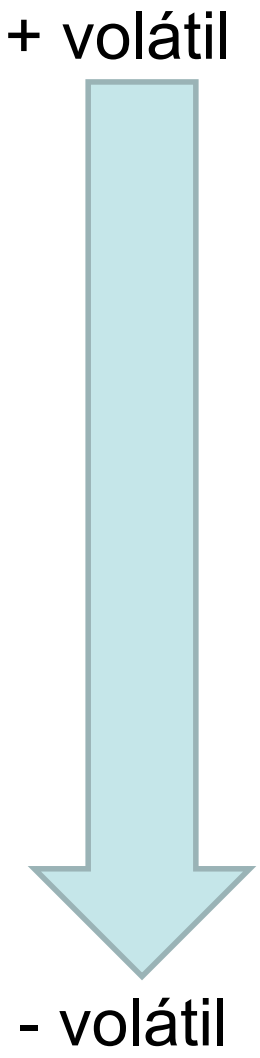
Obtención de la evidencia

- Respuesta inicial es CRÍTICA
  - Apagar el sistema a analizar puede destruir evidencia crítica (en Unix es posible recuperar información del espacio *swap*).
  - Los atacantes pueden aprovechar las ventajas de la volatilidad de la memoria (hay malware que solo se ejecuta en memoria).
  - El nivel de ocultación de datos dependerá del nivel de acceso conseguido y de la pericia del atacante.

Fases de una Investigación

Obtención de la evidencia

- Recabar conexiones de red y desconectar de la red
- Adquirir procesos en ejecución y memoria del Sistema
- Adquirir imágenes de discos
- Fotografías de hw y lugares
- Continuar verificación del incidente
    - Logs, IDS, entrevistas, logs de SO, aplicaciones, correlación, etc...



Fases de una Investigación

Obtención de la evidencia

- Información volátil importante:
  - Hora y fecha del sistema
  - Procesos en ejecución
  - Conexiones de red
  - Puertos abiertos y aplicaciones asociadas
  - Usuarios logados en el sistema
  - Contenidos de la memoria y ficheros *swap* o *pagefile*

Fases de una Investigación

Obtención de la evidencia

- Nunca confíes en el sistema que se está analizando. El atacante puede haberlo comprometido.
- Las herramientas usadas para examinar un sistema en marcha deben
  - Ser copias "limpias" (en un CD)
    - Copias de comandos de sistema
      - Diferentes versiones de OS
      - En Unix/Linux, "statically linked"
    - Otras herramientas
  - Usar el mínimo de recursos del propio sistema
  - Alterar el sistema lo mínimo

Fases de una Investigación

Obtención de la evidencia

- Imágenes de un sistema “vivo”
  - Uso de "dd" y "netcat" para enviar una copia bit-a-bit a un sistema remoto
    - Tanto Windows como Unix/Linux
  - Para Windows puede ser más cómodo usar HELIX
    - http://www.e-fense.com/helix/
    - Permite realizar imagen de la memoria física
  - Una vez realizada la imagen se computa un hash MD5 y SHA-1

Fases de una Investigación

Obtención de la evidencia

- Imágenes de un sistema apagado
  - Extraer disco duro
  - Si el disco tiene un *jumper* para "*read-only*" se puede usar
    - si no, un "*write blocker*" por hardware es necesario (IDE/SATA/SCSI/USB/Firewire/...)
  - Conecta el disco a la *workstation* de análisis forense
    - es recomendable que sea Linux (permite montar los discos manualmente y en modo "read-only")
  - Realiza copia con "dd"
    - la imagen se puede guardar en discos externos Firewire/USB, almacenamiento SAN, etc
  - Por supuesto, hashes MD5 y SHA-1 de original y copia para garantizar integridad

Fases de una Investigación

Obtención de la evidencia

- Fraude interno / Espionaje industrial
  - Periodo de verificación previo, sin alertar al culpable
  - Información sobre conexiones se obtiene de firewalls, IDS, sniffers, etc
  - Confiscación de hardware
  - Obtención de imágenes de discos
- Intrusión Externa
  - Desconectar red
  - Obtener información volátil (memoria, registro, conexiones, etc.)
  - Verificar incidente (logs, IDS, firewalls, etc.)
  - Obtención de imágenes de discos

Fases de una Investigación

Obtención de la evidencia

- Se puede desconectar siempre la red o la alimentación en sistemas críticos?
  - Coste de downtime vs. coste del incidente
  - Coste de reinstalación y puesta en marcha
  - Coste de revalidación, recertificación
- Es factible siempre el hacer imágenes de todos los discos?
  - Almacenamiento en SAN/NAS
  - Configuraciones RAID
  - Volúmenes de >200GB comunes (incluso TB)
  - Distinción de disco físico y lógico cada vez menos clara

Fases de una Investigación

Obtención de la evidencia

- ¿Cómo se preserva la evidencia original?
  - Si se puede parar el sistema y tenemos acceso físico
    - Se hacen dos copias de todos los discos (usando discos de idéntico modelo)
    - Se guardan los originales
    - Se arranca el sistema desde una de las copias
    - Se investiga sobre otra copia
  - Si no tenemos acceso físico
    - Procedimiento de obtención de la imagen sencillo para que un técnico remoto pueda hacerlo
  - Si no se puede parar el sistema
    - Se realiza imagen online, que pasa a ser considerada "original"

Fases de una Investigación

Análisis de la evidencia

- El procedimiento de análisis dependerá del caso y tipo de incidente
- En general se trabaja con las imágenes de los sistemas de ficheros
  - Análisis de Secuencia Temporal ("*timeline*")
  - Búsqueda de contenido
  - Recuperación de binarios y documentos (borrados o corruptos)
  - Análisis de código (virus, troyanos, rootkits, etc.)

Fases de una Investigación

Análisis de la evidencia

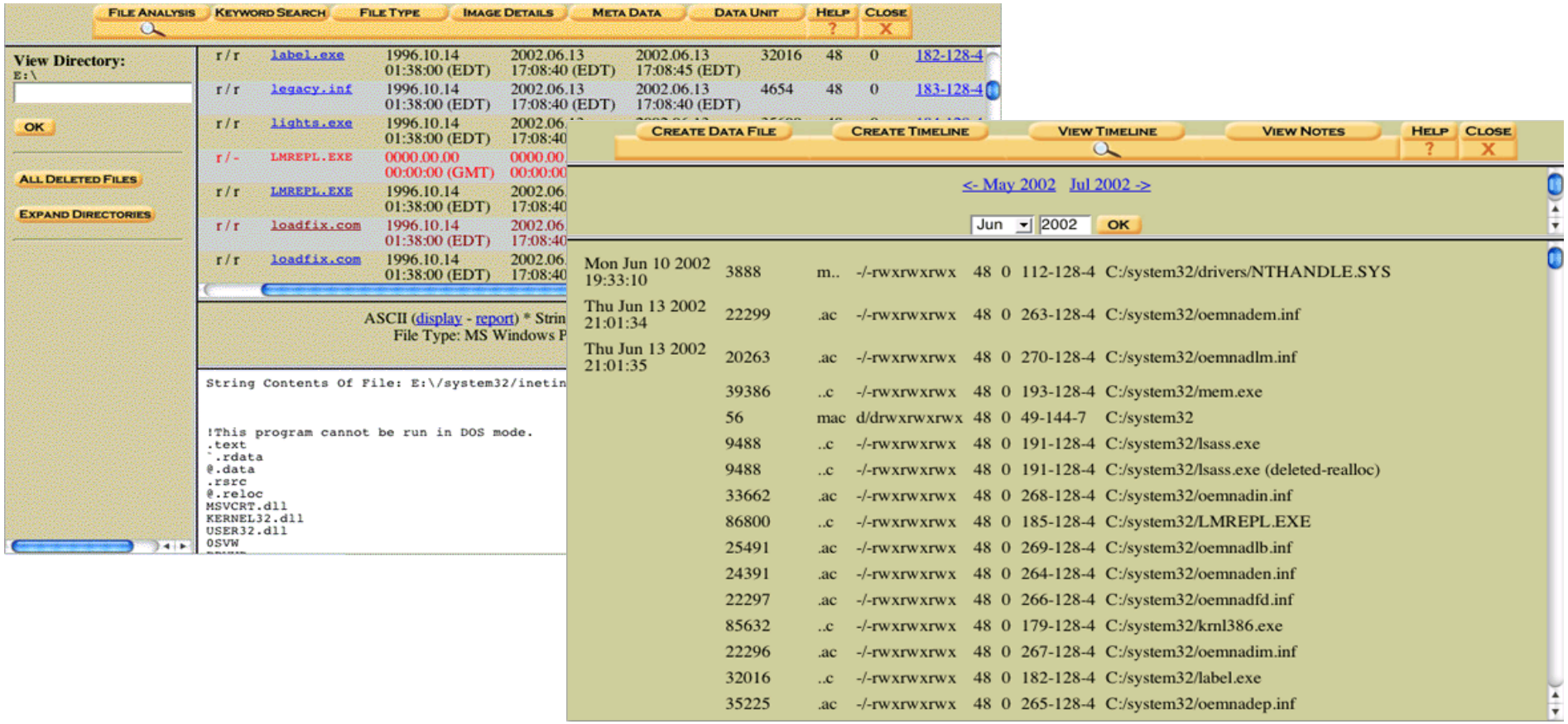
- El objetivo es llegar al:
  - Qué
  - Cuándo (secuencia temporal de eventos)
  - Cómo (punto de entrada, vulnerabilidad explotada, etc…)
  - Quién (?)
  - Porqué (??)

- Análisis Inicial:
  - Buscar archivos ocultos o no usuales (*slack space*)
  - Buscar procesos no usuales y sockets abiertos
  - Buscar cuentas de usuario extrañas
  - Determinar el nivel de seguridad del sistema, posibles agujeros, etc…

Fases de una Investigación

Análisis de la evidencia

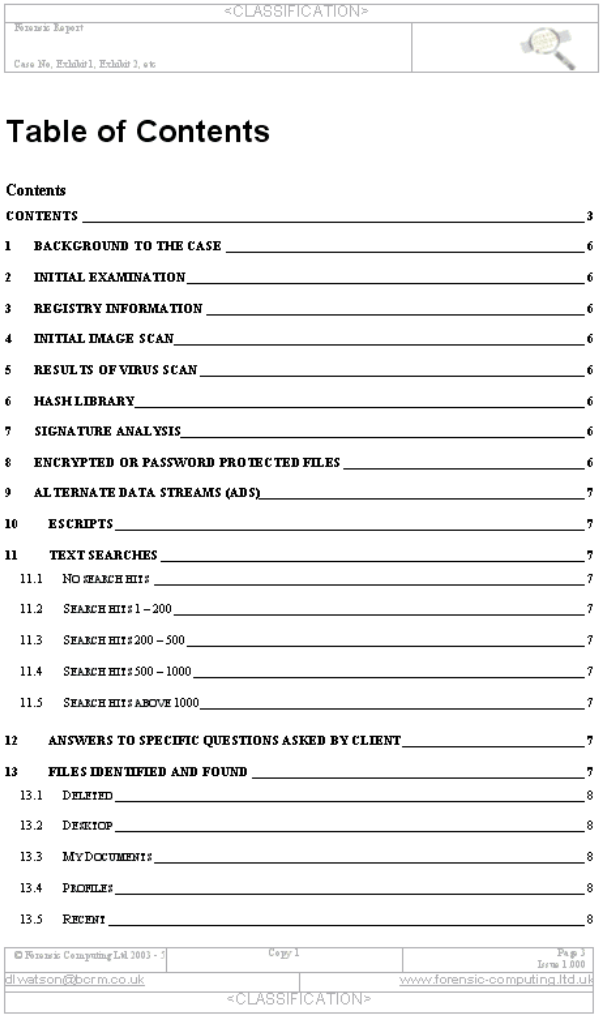
SleuthKit + Autopsy



Fases de una Investigación

Elaboración del informe

- Detalla TODO
  - Antecedentes
  - Procedimientos
  - Evidencias
  - Hashes, etc…
- Utiliza formatos pre-diseñados para no olvidar nada
- Debe ser <u>imparcial</u> y <u>objetiva</u> (no se puede SUPONER nada)
- Es probablemente la parte más importante junto con la defensa en un juicio



<CLASSIFICATION>

Forensic Report

Case No, Exhibit 1, Exhibit 2, etc

Table of Contents

Contents

Fases de una Investigación

Almacenamiento de informes y evidencias

- Calcula los hashes MD5 y SHA1 de todas las evidencias adquiridas, tan pronto como puedas.
- Apunta toda la información del hardware analizado (fabricante, modelo, número de serie, número de inventario, configuración de los jumpers,etc...)
- Toma fotos, y si es necesario graba en video!
- Si es posible, acompáñate de un notario o un abogado que presencie el proceso.

Fases de una Investigación

Almacenamiento de informes y evidencias

- Cadena de custodia:
  - Concepto jurídico sobre la manipulación de una evidencia y su integridad
  - Documento en papel que registra la adquisición, custodia, control, transferencia, análisis y destrucción de la evidencia
  - Las evidencias deben manipularse de forma escrupulosa para evitar cualquier acusación de negligencia
  - Debe detallar dónde se encontraba la evidencia y quién tuvo acceso a ella desde el momento en que se recogió hasta el momento en el que se presenta a juicio

Fases de una Investigación

Almacenamiento de informes y evidencias

Date	Type of Incident	Case#
Consent Required Y/N	Signature of Consenting Person	Tag#
Model#	Manufacturer#	Serial#
Description of Form		
Person Receiving Evidence	Signature	

Chain of Custody

From Location	Date	Reason	To Location
From Location	Date	Reason	To Location
From Location	Date	Reason	To Location
From Location	Date	Reason	To Location
From Location	Date	Reason	To Location
Final Disposition of Evidence		Date	

Obtención de evidencias en un Sistema Windows

Obtención de evidencias en un Sistema Windows

Kit de Adquisición de Datos

- Crea un CD-ROM con herramientas “de confianza”
  - Al menos incluye una versión “limpia” de CMD.EXE que corresponda al sistema operativo a analizar
  - netcat o cryptcat
  - Herramientas de sistema (ipconfig, netstat, date, time, net, arp ...) para las diferentes versiones de Windows y Service Pack
  - pstools, listdlls, filemon*, regmon*, autoruns...
  - hfind, fport, ntlast, ...
  - Windows resource kit tools
  - Un buen sniffer (wireshark, windump, ...)
  - md5sum / md5deep

Obtención de evidencias en un Sistema Windows

Adquisición de Datos +Volátiles

- Conectar la estación forense a la red del equipo a analizar
- Configurar netcat o cryptcat en la estación forense para que escuche en un puerto local y vuelque en un fichero la evidencia recibida
- Montar el Kit de Adquisición de Datos en el sistema a analizar
- Abrir una consola confiable (cmd.exe)

Obtención de evidencias en un Sistema Windows

Adquisición de Datos +Volátiles

- ¿Qué obtener?
  - Fecha y hora del sistema
  - Procesos en ejecución
  - Conexiones de red
  - Puertos abiertos
  - Aplicaciones “escuchando” en puertos abiertos
  - Usuarios logados
  - Información almacenada en la memoria

Obtención de evidencias en un Sistema Windows

Adquisición de Datos +Volátiles

date /t & time /t

fecha y hora

ipconfig /all

información tcp/ip

netstat -aon

conexiones abiertas y puertos en espera, con PID asociado

psinfo -shd

informacion del sistema (hardware, software, hotfixes, versiones, etc.)

pslist -t

lista de procesos

at

lista de tareas programadas (también mirar en %windir%\tasks\ folder)

Obtención de evidencias en un Sistema Windows

Adquisición de Datos +Volátiles

psloggedon

usuarios logados y hora de logon

psloglist

volcado de log de eventos

psservice

información de servicios de sistema

net use, net accounts, net session, net share, net user

conexiones netbios/smb

listdlls

lista de DLLs cargadas en sistema

sigcheck -u -e c:\windows

lista de ficheros (.exe, .dll) no firmados

Obtención de evidencias en un Sistema Windows

Adquisición de Datos +Volátiles

streams -s c:

lista ficheros con alternate data streams (ads)

logonsessions -p

sesiones actuales y procesos por sesión

arp -a

muestra tabla de caché ARP

ntlast

muestra eventos de logon correctos y fallidos

route print

muestra tabla de rutado IP

Obtención de evidencias en un Sistema Windows

Adquisición de Datos +Volátiles

autorunsc

muestra elementos de autoejecución

```
Usage: autorunsc [-a] | [-c] [-b] [-d] [-e] [-h] [-i] [-l] [-m] [-p] [-s] [-v] [
-w] [user]
    -a          Include empty locations.
    -b          Boot execute.
    -c          Print output as CSV.
    -d          Appinit DLLs.
    -e          Explorer addons.
    -h          Image hijacks.
    -i          Internet Explorer addons.
    -l          Logon startups (this is the default).
    -m          Hide signed Microsoft entries.
    -p          Winsock protocol providers.
    -s          Autostart services.
    -t          Scheduled tasks.
    -v          Verify digital signatures.
    -w          Winlogon entries.
    user        Specifies the name of the user account for which
                autorun items will be shown.
```

hfind c:

ficheros ocultos

promiscdetect

detecta interfaces de red en modo "PROMISCUO"

Obtención de evidencias en un Sistema Windows

Adquisición de Datos +Volátiles

volume_dump

muestra información sobre volumenes, mount points, filesystem, etc.

pwdump2

muestra hashes (nthash/lmhash) de cuentas locales

lsadump2

muestra LSA secrets (necesita SeDebugPrivilege)

strings

busca cadenas ASCII/Unicode en ficheros

Obtención de evidencias en un Sistema Windows

Adquisición de Datos +Volátiles

- **Herramientas con interfaz gráfico:**

rootkit revealer

detecta rootkits (usermode o kernelmode)

process explorer (procexp y procmon)

información útil sobre procesos, librerías que usan, recursos accedidos, conexiones de red, etc.

tcpview

muestra conexiones de red y aplicaciones asociadas

Obtención de evidencias en un Sistema Windows

Adquisición de Datos +Volátiles

- Nombres de Dispositivos en Windows:

• \\.	Local machine
• \\.\C:	C: volume
• \\.\D:	D: volume
• \\.\PhysicalDrive0	First physical disk
• \\.\PhysicalDrive1	Second physical disk
• \\.\CdRom0	First CD-Rom
• \\.\Floppy0	First floppy disk
• \\.\PhysicalMemory	Physical memory

Obtención de evidencias en un Sistema Windows

Adquisición de Datos +Volátiles

- **Tipo de información almacenada en la memoria:**
  - Password en la cache
  - Malware residente en memoria (Slammer)
  - Fragmentos de ficheros y procesos abiertos
  - Datos no cifrados (en claro)

Realizar imagen completa de la memoria (de un sistema “vivo”)

dd if=\\.\PhysicalMemory | nc -w 3 10.0.0.1 9000

Obtener los procesos en memoria (de un sistema “vivo”)

Utilizar ‘pmdump’ para volcar a un fichero el espacio de memoria de un proceso

Obtención de evidencias en un Sistema Windows

Adquisición de Datos +Volátiles

- ¿Se puede obtener el fichero de paginación?
  - No se puede copiar 'pagefile.sys' en un sistema en marcha
  - Si se apaga el ordenador, se modifica el fichero de paginación (o opcionalmente se borra)
  - Si es necesario este fichero, quitar cable de alimentación y obtener imágenes del disco

Obtención de evidencias en un Sistema Windows

Adquisición de Datos +Volátiles

```
C:\Local\Tools>pslist -e ftp

PsList 1.26 - Process Information Lister
Copyright (C) 1999-2004 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for RMAMWPDCE08Q:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
ftp                 408   8   1   29    620     0:00:00.060     0:19:10.879

C:\Local\Tools>pmdump 408 ftpprocess.img

pmdump 1.2 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
           - http://ntsecurity.nu/toolbox/pmdump/


C:\Local\Tools>strings.exe ftpprocess.img | findstr /i PASS | more
wPASS secretpassordd
d file - password.... - Mozilla Firefox
PASS %s@%s
PASS %s
Usage: %1 username [password] [account]
Error reading password.
Password: %0.
530 Login or Password incorrect.
secretpassordd
password
gSanTcpBypass
Password (%1:%2):
```

Obtención de evidencias en un Sistema Windows

Adquisición de Datos de Red

- Algunos fuentes importantes de información:
  - Logs de IDS/IPS
  - Logs de Firewall
  - Logs de VPN / Radius
  - Logs del servidor DHCP
  - Logs de otras aplicaciones que puedan estar relacionadas (ftp, www, base de datos, etc…)

Obtención de evidencias en un Sistema Windows

Adquisición de Datos de Red

- En algunos casos es necesario recoger durante unos días la actividad de la red “sospechosa” para detectar posible actividad ilícita (malware o “asesino volviendo a la escena del crimen”)

- Para registrar el tráfico desde/hacia el sistema analizado:
  - Utiliza un sniffer, a ser posible con un TAP
  - Si esto no es posible, utiliza haz un “mirror” del puerto del switch
  - Si no utiliza un hub o usa arp-spoofing para redirigir el tráfico hacia el sniffer (ethereal) **** OPCIÓN MENOS RECOMENDADA ***

Obtención de evidencias en un Sistema Windows

Adquisición de Datos de Red

- En algunos casos es necesario recoger durante unos días la actividad de la red “sospechosa” para detectar posible actividad ilícita (malware o “asesino volviendo a la escena del crimen”)

- Para registrar el tráfico desde/hacia el sistema analizado:
  - Utiliza un sniffer, a ser posible con un TAP
  - Si esto no es posible, utiliza haz un “mirror” del puerto del switch
  - Si no utiliza un hub o usa arp-spoofing para redirigir el tráfico hacia el sniffer (ethereal) **** OPCIÓN MENOS RECOMENDADA ***

Obtención de evidencias en un Sistema Windows

Adquisición y Duplicado de Discos

- Los duplicados de disco son admisibles en un juicio si corresponden a alguno de estos dos tipos:
  - Duplicado forense (‘dd’):
    - Contiene una imagen “cruda”
    - Copia bit a bit
    - No se añade ningún dato extra
  - Duplicado cualificado (Encase)
    - Se añaden metadatos (hashes, timestamps,etc…)
    - Compresión de bloques vacios.

Obtención de evidencias en un Sistema Windows

Adquisición y Duplicado de Discos

- Adquisición física:
  - Apagar la máquina (desconectar cable)
  - Quitar el disco duro
  - Ponerlo en modo sólo lectura (jumper or IDE/SCSI block-writer)
  - Conectarlo a la estación forense y realizar una copia bit a bit con ‘dd’ a un disco externo (firewire/USB)

- Adquisición a través de la red (máquina apagada):
  - En la estación forense: nc -l -p 9000 > disk1.dd
  - Iniciar la máquina a analizar con una distribución LiveCD de Linux (p.ej. Helix) y ejecutar: dd if=/dev/sda | nc 10.0.0.1 9000

Obtención de evidencias en un Sistema Windows

Adquisición y Duplicado de Discos

- Adquisición a través de la red (máquina encendida):
  - No es la opción más recomendable (el SO no es fiable y el sistema de ficheros está en un estado 'estable').
  - En la estación forense: nc -l -p 9000 > disk1.dd
  - En la máquina a analizar, ejecutar 'dd' para windows desde un CD limpio: dd if=\\.\PhysicalDrive0 bs=2k | nc -w 3 10.0.0.1 9000

Obtención de evidencias en un Sistema Windows

Otras fuentes de información

Log de eventos (Application, System, Security, DNS)

IIS/webserver/FTP logs/URLScan

Windows Firewall log (%windir%\pfirewall.log)

Dr. Watson logs

contiene información sobre procesos que corrían cuando una aplicación falló

setupapi.log

información sobre instalación de aplicaciones y dispositivos

schedlgu.txt

información sobre tareas programadas

Antivirus / IDS / IAS / ISA Server / ... logs

Obtención de evidencias en un Sistema Windows

Otras fuentes de información

CARPETA PREFETCH:

Usada por Windows para almacenar información sobre ejecutables, para optimizar el rendimiento

- En WinXP se realiza prefetches al arrancar y al lanzar aplicaciones. Win2003 realiza el prefetch sólo al arrancar (por defecto)
- Los ficheros .pf en %systemroot%/prefetch contienen información sobre el path de los ficheros
- La fecha y hora (MAC) del fichero .pf nos da información sobre cuándo una aplicación ha sido ejecutada

Obtención de evidencias en un Sistema Windows

Otras fuentes de información

LastWrite en claves de registro

- Se puede usar 'lsreg.pl' para extraer esta información

```
Key -> CurrentControlSet\Control\Windows\ShutdownTime
LastWrite : Tue Aug 2 12:06:56 2005
Value : ShutdownTime;REG_BINARY;c4 96 a0 ad 5a 97 c5 01
```

Ficheros INFO2

- Información sobre ficheros borrados
- Se puede usar 'rifiuti' para extraer información
- C:\Recycler\%USERSID%\INFO2

Documentos recientes

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Directorios temporales

Caché navegador web

- Se puede usar 'pasco' para analizar
- Cache y cookies
- Browser history

Aspectos Legales

- Diferentes modelos (Europa/USA)
- Tanto la empresa “víctima” como el Estado pueden solicitar una investigación forense (en todos los países de la EU no es necesaria “todavía” licencia de investigador)
- ¿Cuándo involucrar a la Policía? Depende de:
  - Tipo de delito
  - Política interna (ISO 27001)
  - Obligaciones legales (PCI, SOX, BASEL II, etc…)
  - Existencia de víctimas externas (empresas, clientes, usuarios, etc.)
  - LOPD
- Honeypots (area “gris”) ¿inducción al delito? ¿contenido ilegal?

Aspectos Legales

- Contactos:

  Brigada de Investigación Tecnológica (Policía Nacional)
  http://www.mir.es/policia/bit/

  Grupo de Delitos Telemáticos (Guardia Civil)
  http://www.guardiacivil.org/telematicos/

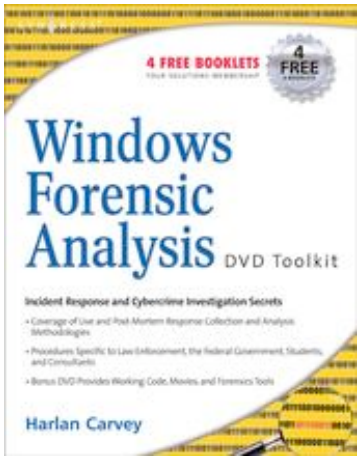
Referencias

- Algunas herramientas citadas en la presentación:

autorunsc	www.sysinternals.com
cryptcat	sourceforge.net/projects/cryptcat
dd for windows	users.erols.com/gmgarner/forensics/
encase	www.guidancesoftware.com
ethereal	www.ethereal.com
forensics browser	www.sleuthkit.org
ftimes	ftimes.sourceforge.net/FTimes
helix	www.e-fense.com/helix
hfind	www.foundstone.com
knoppix	www.knoppix.org
lepton crack	usuarios.lycos.es/reinob/
listdlls	www.sysinternals.com
logonsession	www.sysinternals.com
lophtcrack	www.atstake.com/products/lc
lsadump2	www.bindview.com/Services/RAZOR/Utilities/Windows/
lsreg.pl	www.windows-ir.com
md5deep	md5deep.sourceforge.net
netcat	www.vulnwatch.org/netcat
ntlast	www.foundstone.com
pasco	www.foundstone.com
pmdump	ntsecurity.nu
pref, prev_ver	www.windows-ir.com
process explorer	www.sysinternals.com
promiscdetect	ntsecurity.nu
pstools	www.sysinternals.com
pwdump2	www.bindview.com/Services/RAZOR/Utilities/Windows/
rifiuti	www.foundstone.com
rootkit revealer	www.sysinternals.com
sigcheck	www.sysinternals.com
streams	www.sysinternals.com
strings	www.sysinternals.com
tcpview	www.sysinternals.com
the sleuth kit	www.sleuthkit.org
volume_dump	users.erols.com/gmgarner/forensics/

Referencias

- Windows Incident Response Blog:
  - http://windowsir.blogspot.com/
- Windows Forensic Analysis, Harlan Carvey (2007, Syngress).
- http://www.jessland.net/KB/Forensics/
- http://computer.forensikblog.de/en/
- Parte del contenido de esta presentación está basado en el trabajo de Alfredo Reino (http://www.areino.com)
- http://blog.ismaelvalenzuela.com



¡Gracias!

Ismael Valenzuela Espejo
Information Security Specialist
ismael.valenzuela@isoftplc.com

Podrás descargar esta presentación de:
http://blog.ismaelvalenzuela.com/papers-presentations/