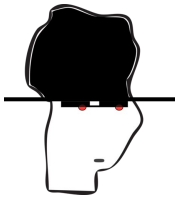
Introduccion a la Forensia

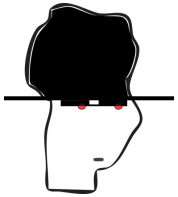
Seguridad Ofensiva



Expectativ

Realidad

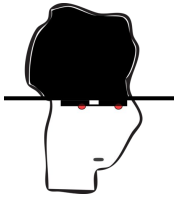
Concepto: Forensic Computing



Es el proceso de identificar, preservar, analizar y presentar evidencia digital de manera tal que sea legalmente aceptable.

Rodney McKemmish,1999

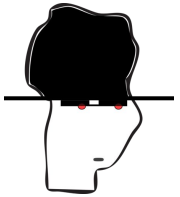
Principio de intercambio de Locard



"siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto"

Rodney McKemmish,1999

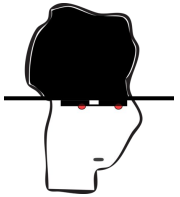
Proceso: Investigacion Forense



se encarga de aplicar cualesquiera de las técnicas propias de la Criminalística en el estudio de la escena de un delito, ejecutando cuantas observaciones, comprobaciones y operaciones técnico criminológicas se pueden realizar

Proceso de investigación forense

Proceso: Investigacion Forense

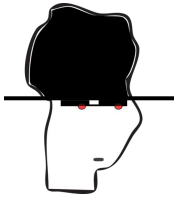


- Identificación de la evidencia (verificación)
- Obtención de la evidencia
- Análisis y evaluación de evidencias
- Presentación y almacenamiento de evidencias

IDENTIFICAR, PRESERVAR, ANALIZAR y PRESENTAR

Debe realizarse siguiendo los estándares apropiados, especialmente si los resultados tienen que poder admitirse en un juicio.

Proceso: Investigacion Forense

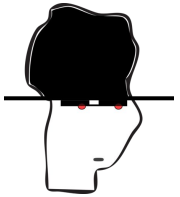


- Identificación de la evidencia (verificación)
- Obtención de la evidencia
- Análisis y evaluación de evidencias
- Presentación y almacenamiento de evidencias

IDENTIFICAR, PRESERVAR, ANALIZAR y PRESENTAR

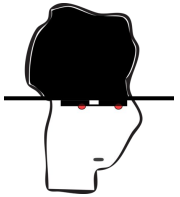
Debe realizarse siguiendo los estándares apropiados, especialmente si los resultados tienen que poder admitirse en un juicio.

Fases de una investigación



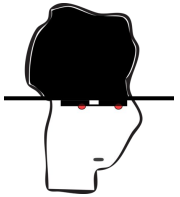
- Inicio / Detección de un incidente
- Verificación del incidente
- Obtención de la evidencia
- Análisis de la evidencia
- Almacenamiento de informes y evidencias

Inicio / Deteccion



- Usuarios o personal de IT informan de un posible incidente
- Alerta generada por los sistemas de gestión de la seguridad
- Por aviso de terceros

Verificación



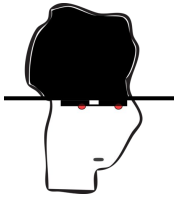
Es importante evaluar cuánta información es posible de recolectar.

Hay diferentes niveles (Aplicación, SO, Servidor, Infraestructura, LAN/DMZ, Entorno Externo, dispositivos relevantes)

Los fraudes internos pueden implicar diferentes elementos de un sistema:

- Múltiples aplicaciones
- Sistemas relacionados
- Múltiples hosts

Obtención de la evidencia



Posibilidades:

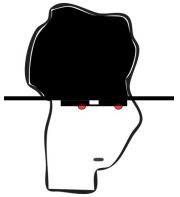
1. Sistema muerto:

    Sin corriente, sistema apagado, dispositivos off.

2. Sistema vivo:

    Con corriente, procesos en ejecución, accesos a disco, dispositivos removibles en continuo cambio.

Obtencion de la evidencia: Primer acción

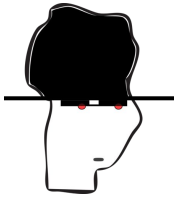


- Apagar el sistema a analizar puede destruir evidencia crítica (en Unix es posible recuperar información del espacio swap).

- 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.

Obtención de la evidencia

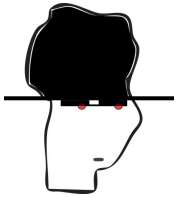


+ volátil
    1. Recabar conexiones de red y desconectar de la red
    2. Adquirir procesos en ejecución y memoria del Sistema
    3. Adquirir imágenes de discos
    4. Fotografías de hw y lugares
    5. Continuar verificación del incidente:

    Logs, IDS, entrevistas, logs de SO, aplicaciones, correlación,

    etc...
- volátil

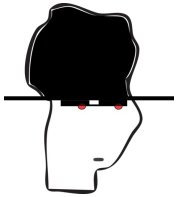
Obtención de la evidencia



Información importante:

- Hora y fecha del sistema
- Procesos en ejecución
- Conexiones de red
- Puertos abiertos y aplicaciones asociadas
- Usuarios logueados en el sistema
- Contenidos de la memoria y ficheros swap o pagefile

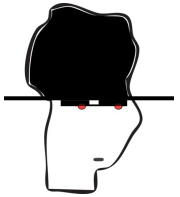
TIP (obvio) del día:



"Nunca confiar en el sistema que está siendo analizado"

Las herramientas a usar deben "estar limpias"(CD?), usar el mínimo de recursos, alterar lo mínimo

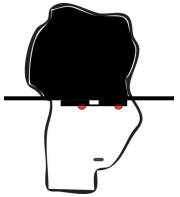
Obtención de la evidencia



Obtención de un sistema "vivo":

- Uso de "dd" y "netcat" para transmitir una copia bit a bit a un sistema remoto.
- En windows puede ser más cómodo usar distribuciones especiales como HELIX, que además permite dumpear la memoria física. (www.e-fense.com/helix)
- Una vez que se realizaron las imágenes: Hashear todo!

Obtención de la evidencia

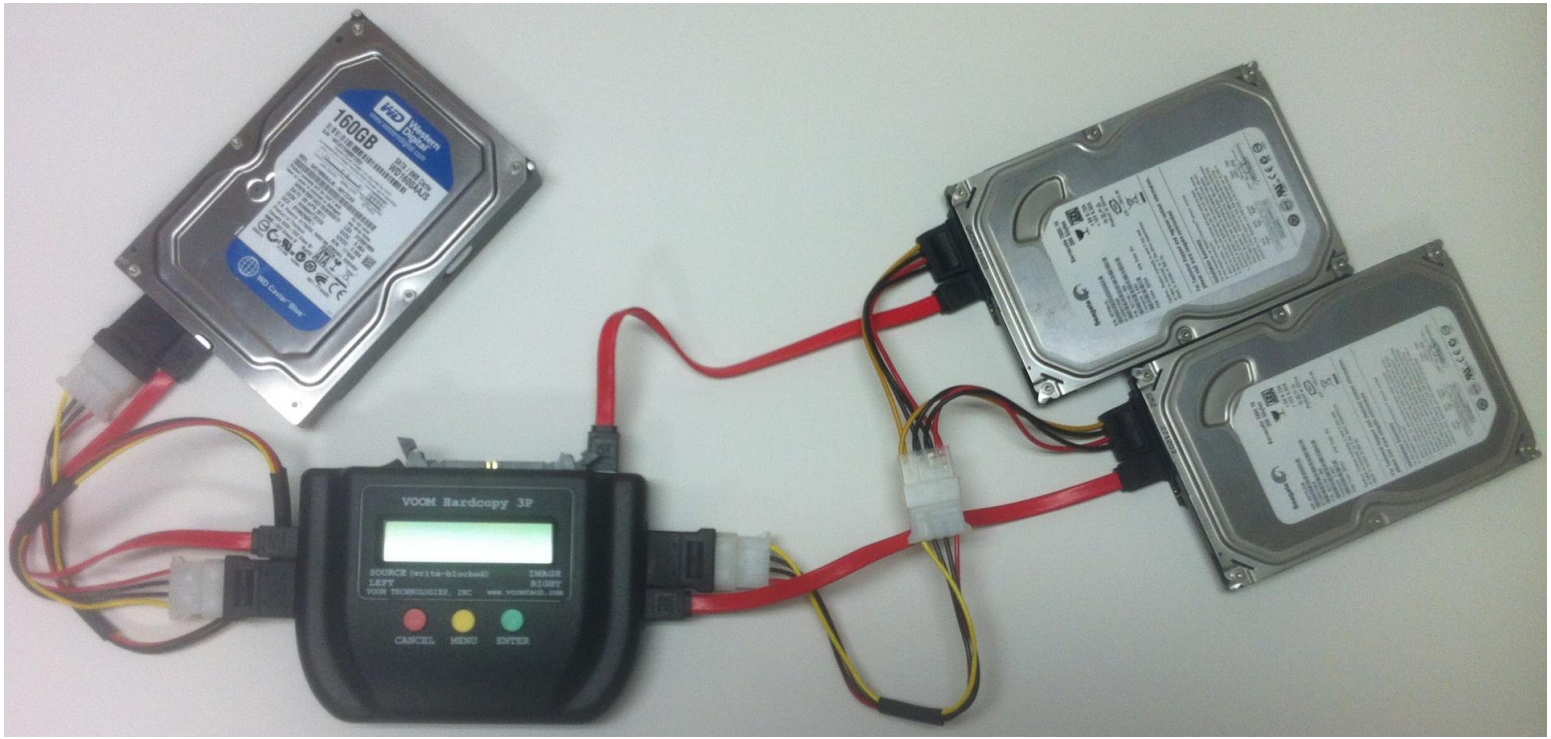


Obtención de un sistema "muerto":

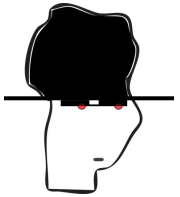
- Extraer disco
- Si el disco tiene jumper para RO, usarlo. Sino habría que usar un "write blocker" por hw
- Conectar el disco a la "Workstation de análisis forense"
- Copiar con dd y guardar la imágen en unidades externas
- Una vez que se realizaron las imágenes: Hashear todo!

Obtención de la evidencia

WRITE
BLOCKER



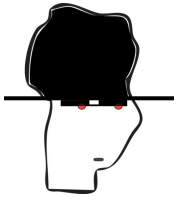
Obtención de la evidencia



Ejemplo: Caso de ataque interno o espionaje

- Periodo de verificación previo, sin alertar al sospechoso.
- Información sobre conexiones se obtiene de firewalls, IDS, sniffers, etc
- Confiscación de hardware
- Obtención de imágenes de discos

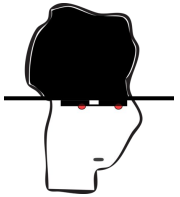
Obtención de la evidencia



Ejemplo: Caso de ataque externo

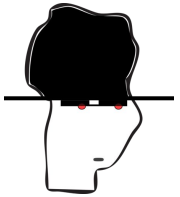
- Desconectar la red
- Obtener toda la información volátil
- Verificar (logs, IDs, firewall, etc)
- Obtener imágenes de los discos

Obtención de la evidencia: Costos



- Se puede siempre desconectar la red?
- Se puede siempre apagar?
- Reinstalacion, puesta en marcha, revalidación, recertificación
- Almacenamiento!

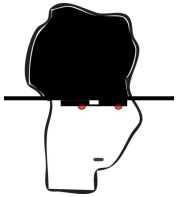
Análisis de la evidencia



- El procedimiento de análisis dependerá del caso y tipo del incidente
- En gral siempre que se puede, se trabaja con la imágenes obtenidas de los sistemas

1. Análisis de secuencia temporal (Timeline)
2. Búsqueda de contenido
3. Recuperación de binarios y documentos(borrados y/o corruptos)
4. Análisis de binarios(virus, troyanos, rootkits)

Análisis de la evidencia



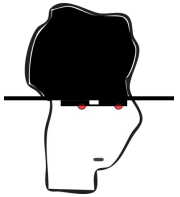
Objetivo:

Llegar al Qué, cuándo, cómo, quién, por qué ...

Una investigación tendría que intentar responder "alguna" pregunta y buscar evidencia de todas las explicaciones(razonables).

Explicación razonable: Un virus (ataque) lo hizo.

Análisis de la evidencia

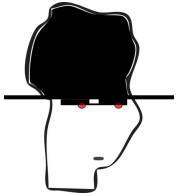


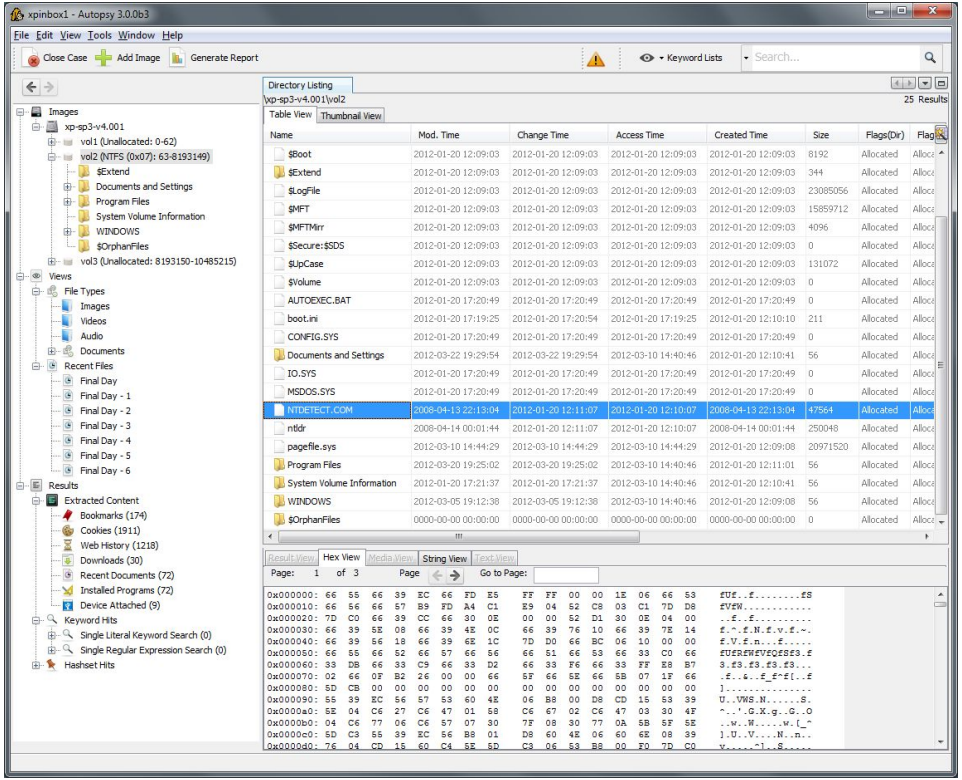
Cómo empiezo el análisis?

1. Buscar archivos, archivos ocultos, no usuales (slack space)
2. Buscar procesos no usuales o sockets abiertos
3. Buscar cuentas de usuario extrañas
4. Determinar el nivel de seguridad del sistema, posibles agujeros, etc.

Aca nos puede ayudar SleuthKit + Autopsy.

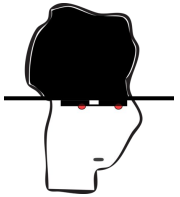
Análisis de la evidencia: Tools






```
E:\>"E:\volatility_2.4.win.standalone\volatility-2.4.standalone.exe" --profile=Win7SP0x86 cmdscan -f memdump3.raw
Volatility Foundation Volatility Framework 2.4
**************************************************
CommandProcess: conhost.exe Pid: 3612
CommandHistory: 0x2b4410 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 12 LastAdded: 11 LastDisplayed: 11
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 @ 0x2ae770: tasklist
Cmd #1 @ 0x2b87a8: cd C:\Users\Alina\AppData\Local\Temp
Cmd #2 @ 0x2af160: dir
Cmd #3 @ 0x2a81c0: more _lt112.spn
Cmd #4 @ 0x2ae7b0: iexplorer
Cmd #5 @ 0x2a8238: iexplorer.exe
Cmd #6 @ 0x2a8260: iexplore.exe
Cmd #7 @ 0x2b4568: cd "c:\Program Files\Internet Explorer"
Cmd #8 @ 0x2af190: dir
Cmd #9 @ 0x2a8288: iexplore.exe
Cmd #10 @ 0x2ae7d0: tasklist
Cmd #11 @ 0x2a7430: regedit
**************************************************
CommandProcess: conhost.exe Pid: 3472
CommandHistory: 0x144a68 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 @ 0x13e9d0: cd c:\lab
Cmd #1 @ 0x13e9f0: DumpIt.exe
**************************************************
CommandProcess: conhost.exe Pid: 3472
CommandHistory: 0x149540 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x54
```

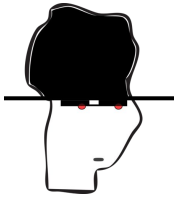
Elaboración del informe



Importante:

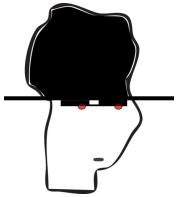
- Detallar TODO (antecedentes, procedimientos, evidencias, hashes)
- Usar formatos prediseñados para no olvidar nada. (Checklists)
- Ser imparcial y objetivos (ojo a las suposiciones sin pruebas)
- Es probablemente la parte más importante (junto con la defensa) en un juicio

Almacenamiento de informes y evidencias



- Hashear todo(tan pronto como se pueda)
- Apuntar toda la información del hw analizado (fabricante, modelo, s/n, inventario, configuración de jumpers, etc)
- Fotos (y si es necesario grabar)
- Si la causa lo amerita, que un notario o abogado presencie el proceso.

Almacenamiento de informes y evidencias

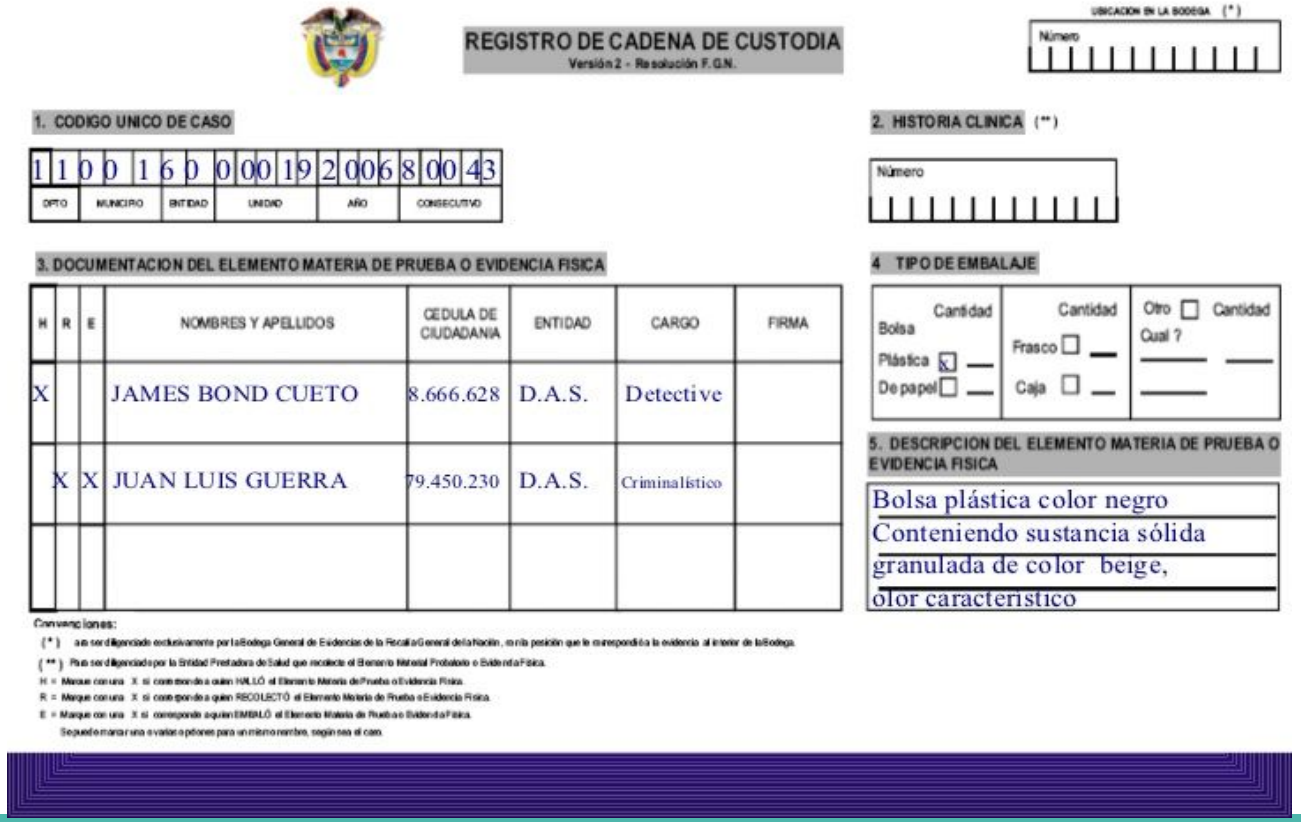


CADENA DE CUSTODIA:

- 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

Almacenamiento de informes y evidencias

CADENA DE CUSTODIA:



REGISTRO DE CADENA DE CUSTODIA
Versión 2 - Resolución F.G.N.

UBICACION EN LA BODEGA (*)
Número

1. CODIGO UNICO DE CASO

1	1	0	0	1	6	0	0	00	19	2	006	8	00	43
DPTO		MUNICIPIO		ENTIDAD		UNIDAD			AÑO			CONSECUTIVO		

2. HISTORIA CLINICA (**)
Número

3. DOCUMENTACION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

H	R	E	NOMBRES Y APELLIDOS	CEDULA DE CIUDADANIA	ENTIDAD	CARGO	FIRMA
X			JAMES BOND CUETO	8.666.628	D.A.S.	Detective	
	X	X	JUAN LUIS GUERRA	79.450.230	D.A.S.	Criminalístico	

4 TIPO DE EMBALAJE

Cantidad		Cantidad		Otro ☐	Cantidad
Bolsa				Cual ?	
Plástica ☒		Frasco ☐			
De papel ☐		Caja ☐			

5. DESCRIPCION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

Bolsa plástica color negro
Conteniendo sustancia sólida
granulada de color beige,
olor característico

Convenciones:
(*) Será diligenciado exclusivamente por la Bodega General de Evidencias de la Fiscalía General de la Nación, en la posición que le corresponda a la evidencia al interior de la Bodega.
(**) Será diligenciado por la Entidad Prestadora de Salud que recolecte el Elemento Material Probatorio o Evidencia Física.
H = Marque con una X si corresponde a quien HALLÓ el Elemento Material de Prueba o Evidencia Física.
R = Marque con una X si corresponde a quien RECOLECTÓ el Elemento Material de Prueba o Evidencia Física.
E = Marque con una X si corresponde a quien EMBALÓ el Elemento Material de Prueba o Evidencia Física.
Se puede marcar una o varias opciones para un mismo nombre, según sea el caso.

Obtención de evidencia (ej: Windows)

Obtencion: Requisitos

Se requiere crear un "kit de adquisición de datos", un CD-ROM / PEN-RO con herramientas de "confianza" que debería incluir:

- CMD.exe / Powershell (correspondiente al SO)
- netcat o cryptcat
- Herramientas del sistema (ipconfig, netstat, date, time, net, arp,...) de las diferentes versiones de lindows (y service packs)
- pstools, listdlls, filemon*, regmon*, autoruns...
- hfind, fport, ntlast, ...
- Un buen sniffer
- Windows resource kit tools
- md5sum, sha256sum, etc...

Obtención: Datos volátiles

1. Conectar la estación forense a la red del equipo a analizar

2. Configurar cryptcat en la estación forense para que escuche en un puerto local y vuelque en un fichero la evidencia recibida.

3. Montar el "Kit de adquisición de datos" en el sistema a analizar.

4. Abrir una consola confiable y comenzar a obtener los datos enviandolos a la estación forense.

Obtención: Datos volátiles

En la estación forense:

cryptcat -l -p 6543 -k key >> evidence-file.txt

En el sistema a analizar:

<command> | cryptcat <IP foresnic station> 6543 -k key

Recordar: Siempre correr los comandos desde una unidad confiable.

Obtención: Datos volátiles

En la estación forense:

cryptcat -l -p 6543 -k key >> evidence-file.txt

En el sistema a analizar:

<command> | cryptcat <IP foresnic station> 6543 -k key

Comandos para obtener: Fecha y hora del sistema, procesos, conexiones de red, puertos abiertos(y aplicaciones que estén escuchando), usuarios logueados, más info almacenada en memoria.

Obtención: Comandos 1/5

date /t & time /t : fecha y hora

ipconfig /all : info tcp/ip

netstat -aon : conexiones abiertas, puertos en espera y PID asociado

psinfo -shd : info del sistema (hw, sw, hotfixes, version, etc)

pslist -t : procesos

at , schtasks: tareas programadas (tambien revisar en %windir% tasks folder)

sysinternals: varias tools más...

Obtención: Comandos 2/5

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: Comandos 3/5

arp -a: muestra tabla de caché ARP

ntlast: muestra eventos de logon correctos y fallidos

route print: muestra tabla de ruteo IP

hfind c: ficheros ocultos

promiscdetect: detecta interfaces de red en modo "PROMISCUO"

Obtención: Comandos 4/5

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

rootkit revealer: detecta rootkits (usermode o kernelmode)

Obtención: Comandos 5/5

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

etc, etc, etc.

Obtención: Dispositivos

• \\.	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: Datos de memoria

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 | cryptcat 10.0.0.1 9000

Obtener los procesos en memoria (de un sistema 'vivo'):

Utilizar 'pmdump' para volcar a un fichero el espacio dememoria de un proceso.

Obtención: Pagefile

No se puede copiar ’pagefile.sys’ en un sistema en marcha:

- Si se apaga el sistema, 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: Datos de la 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: Datos de la Red

- En algunos casos es necesario recoger durante unos días la actividad de la red "sospechosa" para detectar posible actividad ilícita (malware o "atacante en la escena del crimen")
-
- Para registrar el tráfico desde/hacia el sistema analizado:

  1. Utiliza un sniffer, por ahi con un TAP

  2. Si esto no es posible, utiliza haz un "mirror" del puerto del switch

  3. Si no utiliza un hub o usa arp-spoofing para redirigir el tráfico hacia el sniffer (ethereal) **** OPCION MENOS RECOMENDADA ***

-

Fin

Practico en construcción!