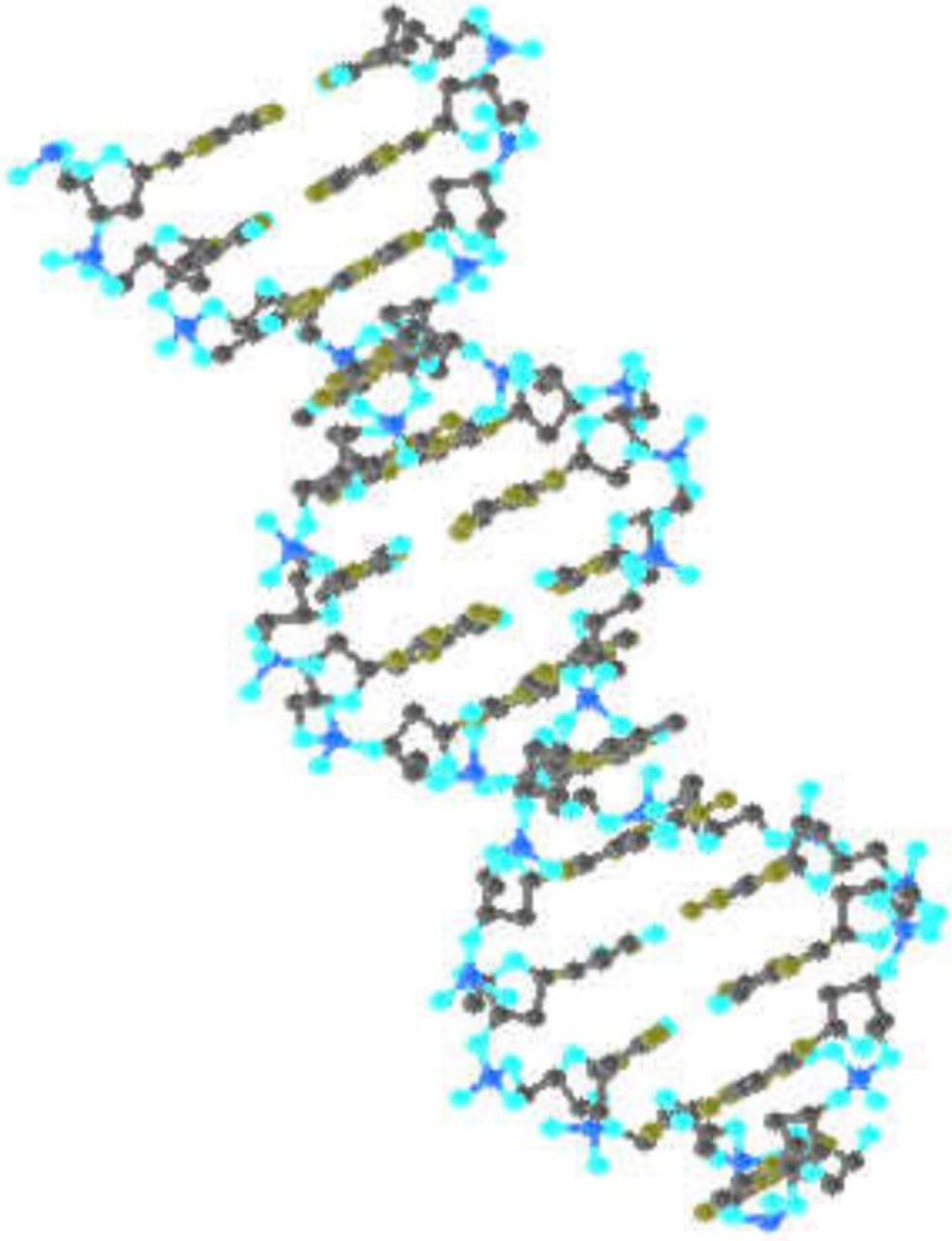
Análisis Forense Digital

Miguel López Delgado



Hackers & Seguridad

Edición 2ª - junio 2007

LICENCIA

Análisis Forense Digital
Computer Forensics

"Análisis Forense Digital"

Segunda Edición: **junio 2007, revisada y adaptada para su publicación en CriptoRed**
Primera Edición: **junio 2.006**

Autor: **Miguel López Delgado**
Ingeniero Técnico Industrial
Experto Profesional en Seguridad Informática
Web: www.codemaster.es
e-mail: codemaster@telefonica.net

A mis hijos Manuel y Paula, por ser una fuente constante de inspiración.

1
Índice

2
Introducción

Antecedentes

Un jueves por la tarde comienza a circular por Internet un nuevo "gusano". Éste aprovecha una vulnerabilidad de Microsoft Windows XP que había sido publicada oficialmente un par de semanas atrás y que se acompañó del correspondiente "parche". Se conoce que el "gusano" se extiende auto enviándose por e-mail usando todas las direcciones que encuentra en el sistema infectado, además está programado para generar diferentes nombres de archivos adjuntos y sus extensiones pueden variar, al tiempo que elige entre un centenar de asuntos y cuerpos de mensaje diferentes. Cuando el "gusano" infecta un sistema realiza una escalada de privilegios hasta obtener derechos de Administrador, realizando entonces la descarga, desde diferentes direcciones IP y vía FTP, de un agente para la ejecución de ataques de denegación de servicio distribuido (DDoS). Aunque los fabricantes de software antivirus alertan inmediatamente del "gusano" su expansión ha sido muy rápida y aún no se dispone de su firma. *Su organización ya ha sufrido una infección importante por la ejecución del "gusano" unas tres horas antes de que dispusiese de la firma para su antivirus y este se encuentra activo en algunos sistemas de su red.*

Ante un escenario de este tipo, podríamos hacernos las siguientes preguntas:

- ✓ ¿Tiene su organización un equipo de respuesta a incidentes como parte de su política de seguridad?
- ✓ ¿Es capaz de identificar los sistemas infectados y proceder a su desconexión y recuperación?
- ✓ ¿Podría informar y justificar a sus empleados una anulación temporal de sus cuentas de correo electrónico para su investigación?
- ✓ Si el ataque DDoS está programado para atacar al servidor Web de otra organización, por ejemplo a la mañana siguiente, ¿sería capaz de manejar una situación en la que dicha organización le pidiese responsabilidades tras detectar que el ataque se ha producido desde direcciones IP suyas?

Este tipo de situaciones no son ni mucho menos casos aislados o anecdóticos, según un estudio realizado por McAfee, compañía centrada en soluciones de prevención de intrusiones y de gestión de riesgos, revela el grado de desprotección de las organizaciones a la hora de gestionar su seguridad. Casi la mitad (el 45 por ciento) de los 600 ejecutivos TI europeos pertenecientes a compañías de más de 250 empleados encuestados durante el 2.005, afirmaron que su infraestructura informática nunca está protegida al 100 por cien frente a las vulnerabilidades.

La inclusión en la política de seguridad de procedimientos capaces de recibir, analizar y posteriormente responder a este tipo de incidentes, ya sean inminentes o en curso, se convierte en un componente indispensable de la infraestructura de los sistemas informáticos de la

organización, pues los ataques a dichos sistemas no sólo ha aumentado en número sino que también lo han hecho en variedad y capacidad destructiva.

Veremos a lo largo del presente trabajo, como la aplicación de técnicas forenses al análisis de sistemas proporciona una metodología adecuada en el proceso de respuesta ante incidentes.

Conceptos y terminología

Organizar un equipo de respuesta a incidentes requiere establecer, entre otros aspectos, unos procedimientos y métodos de análisis que nos permitan identificar, recuperar, reconstruir y analizar evidencias de lo ocurrido y una de las ciencias que cubren estas necesidades es la Ciencia Forense, la cual nos aporta las técnicas y principios necesarios para realizar nuestra investigación, ya sea criminal o no.

Si llevamos al plano de los sistemas informáticos a la Ciencia Forense, entonces hablamos de ***Computer Forensics***, o para nosotros **Análisis Forense Digital**. Esta disciplina es relativamente nueva y se aplica tanto para la investigación de delitos "tradicionales", (homicidios, fraude financiero, narcotráfico, terrorismo, etc.), como para los propiamente relacionados con las tecnologías de la información y las comunicaciones, entre los que destacan piratería de software y comunicaciones, distribución de pornografía infantil, intrusiones y "hacking" en organizaciones, spam, phishing, etc.

De manera más formal podemos definir el Análisis Forense Digital como un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial. Por evidencia digital se entiende al conjunto de datos en formato binario, esto es, comprende los ficheros, su contenido o referencias a éstos (metadatos) que se encuentren en los soportes físicos o lógicos del sistema atacado.

Dentro del Análisis Forense Digital (en adelante AFD), podemos destacar las siguientes fases, que serán desarrolladas con más detalle a lo largo deeste documento:

1ª. Identificación del incidente.
2ª. Recopilación de evidencias.
3ª. Preservación de la evidencia.
4ª. Análisis de la evidencia.
5ª. Documentación y presentación de los resultados.

Por otro lado, hay que definir otro concepto importante, el de Incidente de Seguridad Informática, pues éste ha evolucionado en los últimos tiempos. En principio un incidente de este tipo se entendía como cualquier evento anómalo que pudiese afectar a la seguridad de la información, como podría ser una pérdida de disponibilidad, su integridad o confidencialidad, etc. Pero la aparición de nuevos tipos de incidentes ha hecho que este concepto haya ampliado su definición. Actualmente un **Incidente de Seguridad Informática** puede considerarse como una violación o intento de violación de la política de seguridad, de la política de uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos.

Tras esta definición cabe ahora una categorización de dichos incidentes que nos aporte una base para su valoración y nos de una visión de cómo afrontarlos. Aunque se han propuesto varios tipos de clasificaciones sobre taxonomías de incidentes, no existe ningún consenso al respecto y ni mucho menos sobre cual de ellas es la más acertada. La que se propone a continuación tiene la finalidad de ayudar a una mejor comprensión de apartados siguientes del documento:

Incidentes de Denegación de Servicios (DoS): Son un tipo de incidentes cuya finalidad es obstaculizar, dañar o impedir el acceso a redes, sistemas o aplicaciones mediante el agotamiento de sus recursos.

Incidentes de código malicioso: Cualquier tipo de código ya sea, virus, gusano, "caballo de Troya", que pueda ejecutarse en un sistema e infectarlo.

Incidentes de acceso no autorizado: Se produce cuando un usuario o aplicación accede, por medio de hardware o software, sin los permisos adecuados a un sistema, a una red, a una aplicación o los datos.

Incidentes por uso inapropiado: Se dan cuando los usuarios se "saltan" la política de uso apropiado de las sistemas (por ejemplo ejecutando aplicaciones P2P en la red interna de la organización para la descarga de música).

Incidente múltiple: Se produce cuando el incidente implica varios de los tipos anteriores.

La mayoría de los incidentes que se dan en la realidad, pueden enmarcarse en varias de las categorías expuestas, por lo que una buena forma de identificarlos es por el **mecanismo de transmisión empleado**. Por ejemplo un virus que crea en el sistema atacado una puerta trasera debe ser manejado como un incidente de *código malicioso* y no como un acceso no autorizado, ya que el virus es el mecanismo de transmisión.

Prevención de ataques a sistemas

Detectar un ataque a sus sistemas informáticos antes de que se produzca, o en el peor de los casos en el instante en el que comienza, siempre será mejor que tener que recuperar el sistema recurriendo a sus copias de seguridad... por que las hace ¿verdad?.

Piense que es muy importante para proteger su actividad productiva, mantener el número de incidentes razonablemente bajo. Si sus controles de seguridad son insuficientes y sufre continuos ataques a sus sistemas, éstos pueden repercutir negativamente en sus actividad, tanto desde el punto de vista económico como el de imagen.

Existen multitud de libros y artículos que le proporcionarán información sobre como asegurar sus sistemas, y dado que este aspecto queda fuera del alcance del trabajo, se van a exponer de forma breve algunas recomendaciones para asegurar sus sistemas, redes, aplicaciones y datos.

- ✓ Disponer de una correcta gestión de parches y actualizaciones de su hardware y software, ya que gran parte de los ataques se basan en explotar un número reducido de vulnerabilidades en sistemas y aplicaciones.

- ✓ Asegurar los servidores basándose en el concepto de privilegio mínimo, esto es, configurarlos para que proporcionen un número limitado de servicios y con un nivel de acceso restringido según el tipo de usuario. Además deben evitarse configuraciones por defecto, como claves predefinidas, recursos compartidos, etc. También sería interesante disponer de medios de notificación al administrador cuando se produzcan accesos a niveles de privilegio no autorizados.
- ✓ Mantener la seguridad de la red, configurando un filtro perimetral en modo "paranoico", esto es, denegando cualquier tipo de acceso no autorizado expresamente, y manteniendo sólo el tráfico necesario para la actividad diaria normal. Esto incluirá instalación de cortafuegos, detectores de intrusos (IDS), monitores de red, uso de redes privadas virtuales (VPNs), uso de protocolos seguros (IPSec, SSL).
- ✓ Prevenir la ejecución de código malicioso (*malware*), utilizando programas antivirus capaces de parar este tipo de código como virus, caballos de Troya, gusanos y además "especies".
- ✓ Formar e informar a sus usuarios para que conozcan, acepten y sean capaces de aplicar las directrices de su política de seguridad. Hágales ver lo que ha ocurrido en otras organizaciones o entidades, cómo han "aprendido la lección", cómo ha afectado un incidente a sus actividades (y a sus sueldos). Informando y formando a los usuarios reducirá la frecuencia de los incidentes, sobre todo aquellos que impliquen la ejecución de código malicioso, o el saltarse la política de uso adecuado de los sistemas.

Preparación y respuesta ante incidentes

Si ya ha tomado las medidas descritas en el apartado anterior, y quizás alguna más, y aunque a nadie la agrade tener que preparar actuaciones ante desastres en sus sistemas informáticos, siendo realista, no estaría de más incluir dentro de su política de seguridad un **Plan de Respuesta ante Incidentes**. Éstos planes dependerán en gran medida de las características de su organización, y de su política, pero en base y sin extendernos en ello pues no es objetivo de este documento, deberían contener los siguientes puntos:

- ✓ Alcance, propósitos y objetivos del plan de acción.
- ✓ Estructura organizativa del equipo de respuesta a incidentes, responsabilidades, autoridad, departamentos implicados.
- ✓ Actuaciones para la contención del problema.
- ✓ Procedimientos de recuperación y restauración de sistemas SIN eliminación de posibles evidencias del ataque.
- ✓ Índices para la valoración de los daños, tanto desde el punto de vista económico como de imagen corporativa.
- ✓ Determinar en qué casos se tratará el incidente internamente y en qué casos se dará aviso a las Autoridades.
- ✓ Sopesar la contratación de personal externo para llevar a cabo la investigación.
- ✓ Establecer las fases de la investigación.
- ✓ Elaboración de informes y formularios tipo para comunicación del incidente tanto dentro como fuera de la organización si fuese necesario.

Por otro lado, y debido a que la recopilación de evidencias digitales puede llegar a ser una tarea bastante difícil, será necesario preparar sus sistemas para obtener buenos datos forenses. La implantación de procedimientos adecuados en la gestión de archivos, registros y

copias de seguridad pueden ayudar al quipo investigados en esta labor. Se exponen a continuación algunas recomendaciones:

- ✓ Conocer y monitorizar los parámetros de funcionamiento normal de los sistemas, tales como tráfico IP usual, carga de transacciones, ancho de banda consumido, usuarios conectados, etc.
- ✓ Utilizar un servidor de registros central y establecer una política de mantenimiento y retención de esos registros que permitan su estudio pasado el tiempo.
- ✓ Activar al máximo de detalle la información que contendrán los archivos de registro, lo que permitirá facilitar el proceso de reconstrucción de lo sucedido.
- ✓ Sincronizar todos los relojes de los servidores mediante, por ejemplo, el protocolo NTP (Network Time Protocol), permitiendo que los registros contengan todos la misma hora.
- ✓ Disponer de una base de conocimientos sobre incidentes, basta algo tan sencillo como enlaces páginas de software antivirus, o empresas y organizaciones especializadas en seguridad informática, así como suscribirse a sus listas e-mail de notificacionesde alertas y vulnerabilidades.
- ✓ Considere la experiencia como un factor irremplazable, esto le permitirá distinguir rápidamente un ataque de un simple problema técnico.

Aspectos legales

Si tras la realización de un primer análisis existen sospechas de que el incidente se ha provocado desde el interior de su red, tendrá que plantearse la posibilidad de llevar a cabo una investigación interna a la organización para depurar responsabilidades, bastará para este propósito recopilar información suficiente tanto en cantidad como calidad para poder tomar acciones disciplinarias posteriores, sin llegar a los tribunales. En esta situación además del equipo técnico de respuesta a incidentes, tendrá que contar con otros departamentos como el de Recursos Humanos e incluso con la Sección Sindical, pues no puede permitirse que por una mala gestión del caso el incidente se vuelva contra usted y acabe siendo acusado, por ejemplo, de despido improcedente.

Si los indicios llevan a su equipo forense a un ataque externo, habitualmente no merece la pena llevar a cabo acciones legales cuando los daños producidos son mínimos debido al alto coste económico que esto puede suponerle. Por ejemplo una deformación de su página Web corporativa que se subsana rápidamente o intentos de intrusión sin mayores consecuencias que algunas molestias para sus usuarios, pueden resolverse enviando un aviso de uso inapropiado al proveedor o proveedores de los servicios de conexión de los presuntos atacantes. Si documenta suficientemente bien su queja adjuntando históricos detallados de conexiones, del escaneado de sus equipos, etc., puede conseguir que el ISP desconecte o anule las cuentas de sus atacantes. La mayoría de los proveedores tienen direcciones de e-mail para estos casos y los más importantes suelen ser muy estrictos en cuanto a la política de uso de sus servicios.

Pero si el incidente, realizado por atacantes internos o externos, ha provocado daños importantes a su organización ya sean económicos, de imagen corporativa o su reputación ha quedado en entredicho, puede considerar abrir un proceso judicial contra sus atacantes. En este caso la investigación técnica deberá ser tratada como una investigación pericial técnica, incorporando procedimientos en materia de probatoria judicial, pues una evidencia digital no será considerada como prueba en un proceso judicial hasta que el juez así lo determine. Por

ello tendremos que convencerle de que hemos actuado de forma profesional, científica, veraz, con cautela e imparcial, y además explicárselo para que lo entienda pues es muy probable que el juez no tenga conocimientos avanzados en estos temas.

Para ampliar información sobre estos conceptos, en el Nuevo Código Penal, encontrará las siguientes referencias:

Ataques que se producen contra el derecho a la intimidad: Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal).

Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor: Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal).

Falsedades: Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (Artículos 386 y ss. del Código Penal).

Sabotajes informáticos: Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal).

Fraudes informáticos: Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal).

Amenazas: Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal).

Calumnias e injurias: Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal).

Pornografía infantil: Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.

- La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art 187).
- La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (art 189).
- El facilitamiento de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición, etc.) (art 189).
- La posesión de dicho material para la realización de dichas conductas.(art 189)

Fuente: Policía Nacional Española

Por otro lado, en cuanto a métodos de probatoria y demás tecnicismos legales se puede acudir a la Ley de Enjuiciamiento Criminal, La Nueva Ley de Enjuiciamiento Civil, etc.

3

Fases de un Análisis Forense Digital

Identificación del incidente: búsqueda y recopilación de evidencias

Una de las primeras fases del análisis forense comprende el proceso de identificación del incidente, que lleva aparejado la búsqueda y recopilación de evidencias.

Si sospecha que sus sistemas han sido comprometidos lo primero que tiene que hacer es ¡NO PERDER LA CALMA!, piense que no es el primero y que menos aún va a ser el último al que le ocurre. Antes de comenzar una búsqueda desesperada de señales del incidente que lo único que conlleve sea una eliminación de "huellas", actúe de forma metódica y profesional.

Asegúrese primero que no se trata de un problema de hardware o software de su red o servidor, no confunda un "apagón" en su router con un ataque DoS.

Descubrir las señales del ataque

Para iniciar una primera inspección del equipo deberá tener en mente la premisa de que debe conservar la evidencia, por ello NO HAGA NADA QUE PUEDA MODIFICARLA. Deberá utilizar herramientas que no cambien los sellos de tiempo de acceso (*timestamp*), o provoquen modificaciones en los archivos, y por supuesto que no borren nada.

Un inciso importante es que si no hay certeza de que las aplicaciones y utilidades de seguridad que incorpora el Sistema Operativo, o las que se hayan instalado se mantienen intactas deberemos utilizar otras alternativas. Piense que en muchos casos los atacantes dispondrán de herramientas capaces de modificar la información que el administrador verá tras la ejecución de ciertos comandos. Por ejemplo podrán ocultarse procesos o puertos TCP/UDP en uso. Cuestione siempre la información que le proporcionen las aplicaciones instaladas en un sistema que crea comprometido.

No estría de más en este momento crear un CD o DVD como parte de sus herramientas para la respuesta a incidentes, y si trabaja en entornos mixtos UNIX/Linux y Windows, tendrá que preparar uno para cada plataforma. Aunque existen gran cantidad de utilidades a continuación propongo una relación de aquellas que considero debería incluir en su ToolKit, y que le permitan, al menos, realizar las siguientes tareas:

- ✓ Interpretar comandos en modo consola (`cmd, bash`)
- ✓ Enumerar puertos TCP y UDP abiertos y sus aplicaciones asociadas (`fport, lsoft`)
- ✓ Listar usuarios conectados local y remotamente al sistema
- ✓ Obtener fecha y hora del sistema (date, time)
- ✓ Enumerar procesos activos, recursos que utilizan, usuarios o aplicaciones que los lanzaron (`ps, pslist`)

- ✓ Enumerar las direcciones IP del sistema y mapear la asignación de direcciones físicas MAC con dichas IP (`ipconfig, arp, netstat, net`)
- ✓ Buscar ficheros ocultos o borrados (`hfind, unrm, lazarus`)
- ✓ Visualizar registros y logs del sistema (`reg, dumpel`)
- ✓ Visualizar la configuración de seguridad del sistema (`auditpol`)
- ✓ Generar funciones hash de ficheros (`sah1sum, md5sum`)
- ✓ Leer, copiar y escribir a través de la red (`netcat, crypcat`)
- ✓ Realizar copias bit-a-bit de discos duros y particiones (`dd, safeback`)
- ✓ Analizar el tráfico de red (`tcpdump, windump`)

Supongamos que ya dispone de su ToolKit, ahora se hará la siguiente pregunta ¿dónde puedo buscar indicios de un ataque?. Evidentemente, uno de los primeros lugares donde comenzar la búsqueda de indicios es en los equipos que consideremos comprometidos pero no se limite sólo a éstos, piense que sus atacantes han podido borrar algunos registros locales en esos equipos, pero aún así, puede haber indicios en otras máquinas próximas tales como escaneado de puertos o tráfico inusual en cortafuegos y routers de la red.

Al iniciar la investigación nunca sabremos con qué nos vamos a topar, de hecho al principio puede que no se aprecie, a simple vista ninguna huella o indicio del ataque especialmente si para realizarlo han empleado e instalado en sus equipos un rootkit.

Como primera opción de búsqueda podemos realizar una verificación de integridad de los ficheros del sistema, utilidades como Tripwire o AIDE (Advance Intrusion Detection Enviroment) podrán arrojar algo de luz sobre sus sospechas. Otra opción es realizar una serie de verificaciones sobre del equipo.

Primero sería interesante conocer los procesos que se están ejecutando actualmente en el equipo, en busca de alguno que le resulte extraño, deberán llamarnos la atención aquellos que consuman recursos en exceso, con ubicaciones poco frecuentes en el sistema de archivos, que mantengan conexiones de red en puertos TCP o UDP no habituales, etc.

Este último punto nos llevará a realizar otra comprobación de interés, listar todos los puertos TCP y UDP abiertos además de los procesos (PID), usuarios y aplicaciones que los utilizan, siempre con la idea de identificar actividad no usual, recuerde la importancia de que el administrador conozca muy bien los parámetros de actividad normal del sistema. La aparición en el listado de procesos sin nombre o que emplean puertos altos (por encima del 1024) pueden ser indicios de la ejecución de un *troyano* o puerta trasera (backdoor) en el equipo. Una buena opción sería buscar en Internet (especialmente en Google) alguna referencia sobre el puerto o proceso que le resulta sospechoso.

Si tras estas consultas sus temores aumentan, pase ahora a editar los archidos de registro del sistema y logs en busca de entradas y avisos sobre fallos de instalación, accesos no autorizados, conexiones erróneas o fallidas, etc. Dependiendo de la plataforma que emplee encontrará estos archivos en distintas ubicaciones.

> **Microsoft Windows:** Este sistema operativo le proporciona un entorno para realizar estas pesquisas puede consultar, si considera que se trata aún de una aplicación segura, dentro del menú Herramientas administrativas, el Visor de sucesos, el de Servicios o el de la Directiva de seguridad local. Si no entiende bien la información que estos visores le

aporten puede consultar la base de datos de ayuda de Microsoft. Otro lugar donde se esconde gran cantidad información es el registro de Windows. La aplicación del sistema `regedit.exe` puede ayudarle en esta tarea, pero si no se fía de ella use las herramientas de su CD tales como `reg` (permite hacer consultas al registro sin modificarlo), o `regdmp` (exporta el registro en formato de texto plano, .txt), para su posterior consulta. En estos archivos tendrá que buscar "una aguja en un pajar", debido a la ingente cantidad de información que almacena y que se mezcla. Un punto de partida podría ser buscar en las claves del registro Run, RunOnce, RunOnceEx, RunServices, RunServicesOnce, Winlogon, pues bajo estas claves se encuentran los servicios, programas y aplicaciones que se cargarán en el inicio del sistema. Si ve algo raro, acuda nuevamente a Google.

UNIX/Linux: En este tipo de sistemas se dispone de una serie de archivos de registro (logs), que podremos encontrar habitualmente bajo el directorio `/var/log`, siendo los más importantes los que se detallan a continuación:

`/var/log/messages`	contiene los mensajes generales del sistema
`/var/log/secure`	guarda los sistemas de autenticación y seguridad
`/var/log/wmtp`	guarda un historial de inicio y cierres de sesión pasadas
`/var/run/utmp`	guarda una lista dinámica de quien ha iniciado la sesión
`/var/log/btmp`	guarda cualquier inicio de sesión fallido o erróneo (sólo para Linux)

Además los programas y aplicaciones crean normalmente sus propios archivos de registro, que podrá encontrar bajo el directorio `/var`. Todos estos archivos están en modo texto, por lo que podrá utilizar cualquier editor o visor de texto para buscar indicios del ataque. Observe el siguiente fragmento de un archivo `/var/log/messages`, en una máquina comprometida:

```
.....
Aug 22 23:37:55 localhost ftpd[7020]: FTP session closed
Aug 23 00:12:15 localhost ftpd[7045]: FTP session closed
Aug 23 00:19:19 localhost ftpd[7046]: FTP session closed
Aug  22  22:21:05  localhost  ftpd[7049]:  Anonymous  FTP  login  from
200.47.186.114 [200.47.186.114], mozilla@
Aug  22  22:22:48  localhost  ftpd[7052]:  Anonymous  FTP  login  from
200.47.186.114 [200.47.186.114], mozilla@
Aug 23 00:25:03 localhost kernel: Kernel logging (proc) stopped.
Aug 23 00:25:03 localhost kernel: Kernel log daemon terminating.
.....
```

¿No aprecia nada raro?, fíjese en la 4ª y 5ª entradas del archivo, éste parece haber sido modificado pues aparece un salto en la secuencia de fechas, con dos entradas fechadas el 22 de agosto tras dos entradas con fecha 23 de agosto. Este tipo de detalles, aunque no son determinantes, si pueden ser síntomas de que han estado "trasteando" en sus sistemas.

Además de estos archivos de registro, también pueden contener indicios los archivos de claves, usuarios y grupos, podrá encontrarlos en `/etc/passwd`, `/etc/shadow`,

`/etc/group`. También pude encontrar indicios de actividad anómala al editar el archivo `/root/.bash_history` que contiene los comandos ejecutados por el usuario roo el intérprete vas.

Para el propósito inicial de confirmación del ataque o compromiso de sus sistemas estas primeras pesquisas serán suficientes, aunque tendrá que volver a utilizar de forma más exhaustiva estos datos tal y como veremos en el apartado de análisis de evidencias.

Recopilación de evidencias

Bien, ya está seguro de que sus sistemas informáticos han sido atacados. En este punto deberá decidir cuál es su prioridad:

A.- Tener nuevamente operativos sus sistemas rápidamente.
B.- Realizar una investigación forense detallada.

Piense que la primera reacción de la mayoría de los administradores será la de intentar devolver el sistema a su estado normal cuanto antes, pero esta actitud sólo hará que pierda casi todas las evidencias que los atacantes hayan podido dejar en "la escena del crimen", eliminando la posibilidad de realizar un análisis forense de lo sucedido que le permita contestar a las preguntas de ¿qué?, ¿cómo?, ¿quién?, ¿de dónde? y ¿cuándo? se comprometió el sistema, e impidiendo incluso llevar a cabo acciones legales posteriores si se diese el caso. Esto también puede que le lleve a volver a trabajar con un sistema vulnerable, exponiéndolo nuevamente a otro ataque.

Si no está seguro de lo que está haciendo, ¡NO HAGA NADA!, y póngase en contacto con expertos en la materia.

Asumamos que elige el *"Plan B"*, que el análisis forense es su prioridad y que está capacitado para realizarlo, así que a partir de ahora tendrá que seguir una serie de pasos encaminados a **recopilar evidencias** que le permitan determinar el método de entrada al sistema, la actividad de los intrusos, su identidad y origen, duración del compromiso y todo ello extremando las precauciones para evitar alterar las evidencias durante el proceso de recolección.

Este es un buen momento para hacerse con un cuaderno donde comenzar a tomar apuntes detallados de todas las operaciones que realice sobre los sistemas atacados, no se fíe de su memoria, anote la fecha y hora de inicio y fin de cada uno de los pasos que dé, anote también características como números de serie de cada equipo, de sus componentes, de su S.O., etc. No escatime en la recopilación de datos incluso haga fotografías de los equipos y del entorno, nunca se sabe si tendrá que vérselas con sus atacantes en un juicio, y cualquier evidencia puede ser definitiva. También sería recomendable que le acompañase otra persona durante el proceso de recopilación de evidencias, ésta actuaría como testigo de sus acciones, así que si es alguien imparcial mejor, y si puede permitirse que le acompañe un Notario mejor que mejor, recuerde los requisitos legales para que una evidencia pase a ser considerada como prueba en un juicio. No sería la primera vez que un excelente análisis técnico de un incidente es rechazado en un juicio por no guardar las debidas garantías procesales.

Ahora que ya está preparado para la recolección de evidencias tendrá que decidir si comienza a tomar muestras sobre el sistema "vivo" o "muerto". Tenga presente que en el sis-

tema habrá pruebas ocultas con diferentes niveles de volatilidad, como los registros del procesador, estructuras de datos en la memoria RAM o memoria de tipo caché, conexiones de red activas, usuarios y procesos actuales, sistema de archivos, etc. Será muy difícil reunir toda esta información a la vez y gran parte de esta se perderá si decide apagar el equipo de la forma habitual, ya que en este proceso se realizan una serie de pasos programados para cerrar el sistema de forma limpia, pero si además el atacante ha instalado las herramientas adecuadas éste podría eliminar, modificar y sustituir ficheros a su antojo durante el apagado, y se "limpiarán" también del equipo las huellas de su atacante. Además si el atacante sigue on-line, puede detectar su actividad y actuar con una acción evasiva o, peor aún, destructiva eliminando todo tipo de información. Pero si por la severidad del ataque o por la importancia de los datos comprometidos decide apagar el equipo, no lo dude ¡DESCONÉCTELO DIRECTAMENTE DE LA RED ELÉCTRICA!, si ha leído bien, de esta forma perderá la información volátil de la RAM, micro, etc. Pero conservará aún bastante información sobre el ataque.

Supongamos que puede mantener su equipo "vivo" un poco más, comience a recopilar evidencias siguiendo el orden de mayor a menor volatilidad. Este proceso se describe muy bien e el RFC 3227, .Estableceremos el siguiente orden de volatilidad y por tanto de recopilación de evidencias:

- ✓ Registros y contenidos de la caché.
- ✓ Contenidos de la memoria.
- ✓ Estado de las conexiones de red, tablas de rutas.
- ✓ Estado de los procesos en ejecución.
- ✓ Contenido del sistema de archivos y de los discos duros.
- ✓ Contenido de otros dispositivos de almacenamiento.

Observe que los cuatro primeros puntos representan un tipo de datos, volátil, que se perderán o modificarán si apaga o reinicia el sistema, es por tanto muy fácil eliminar evidencias de forma inadvertida.

Dentro de las evidencias volátiles será de interés recuperar los siguientes datos del sistema en tiempo real:

- ✓ Fecha y hora.
- ✓ Procesos activos.
- ✓ Conexiones de red.
- ✓ Puertos TCP/UDP abiertos y aplicaciones asociadas "a la escucha".
- ✓ Usuarios conectados remota y localmente.

Durante este proceso de recopilación de evidencias, tendrá que hacer uso de su Tool-Kit, pero como se indicó anteriormente, deberá tener precaución pues el atacante aún puede estar fisgoneando por sus sistemas. Con un buen entrenamiento será capaz de recopilar toda esta información con un número de comandos mínimo, haciendo su labor casi desapercibida, incluso sería recomendable que tuviese preparado un script en Perl para sistemas UNIX/Linux o un archivo de proceso por lotes para entornos Windows que realizase todas estas operaciones de forma automatizada y que, además, enviase la información a un lugar seguro.

Y ahora viene otra cuestión , a la hora de recopilar estas evidencias volátiles, ¿dónde las almacenamos?, ¿dónde está ese lugar seguro?. Las salidas de algunos comandos pueden ocupar poco espacio, pero otros pueden generar tal cantidad de información que sea necesario

el uso de medios de almacenamiento con una capacidad considerable (desde cientos de Mbytes hasta decenas de Gbytes). Una Opción interesante sería usar discos externos USB, muy económicos y que le permiten gran flexibilidad de manejo y transporte de grandes cantidades de información. Otra opción es emplear herramientas de transmisión de datos por la red tipo `netcat`, que le permitiría enviar toda la información recopilada a un sistema seguro, como por ejemplo un equipo conectado en la misma red o un portátil conectado directamente al sistema afectado.

En cualquier caso tenga en cuenta el siguiente consejo, NUNCA almacene la información volátil en el equipo comprometido con la idea de recuperarla más tarde para su análisis... ¡puede que ya no esté ahí cuando vuelva a buscarla!.

Tan pronto como haya obtenido toda la información volátil del sistema tendremos que recopilar la información contenida en los discos duros, teniendo en cuenta que estos dispositivos no sólo contienen las particiones, los archivos, directorios, etc. Sino que también contienen otro tipo de datos que hacen referencia a los propios archivos y a flujos de información, son los metadatos que serán de gran importancia en el análisis forense.

En este punto cabe hacer una aclaración muy importante, cuando se realiza una **copia de seguridad** de un disco o soporte en general se procede a copiar los archivos tal cual el sistema operativo los “ve”, perdiéndose gran cantidad de información oculta en el disco. Por el contrario si realizamos una **imagen del disco**, creamos una copia bit-a-bit del disco original preservando toda la información que contenga, incluyendo los bloques de los ficheros eliminados, espacio libre tras cada bloque, inodos (metadatos), etc.

Como norma general, obtendremos siempre imágenes de los discos duros para su posterior análisis y, siempre sobre medios de sólo lectura.

Una de las herramientas más empleadas en entornos UNIX/Linux es `dd`, ésta permite crear imágenes de discos bit-a-bit, además de ofrecer otras opciones como obtención del hash MD5 de la copia, etc. Si además la combinamos con la herramienta `netcat`, podríamos transferir las imágenes completas a través de la red.

Preservación de la evidencia

Aunque el primer motivo que le habrá llevado a la recopilación de evidencias sobre el incidente sea la resolución del mismo, puede que las necesite posteriormente para iniciar un proceso judicial contra sus atacantes y en tal caso deberá documentar de forma clara cómo ha sido preservada la evidencia tras la recopilación. En este proceso, como se expondrá a continuación, es imprescindible definir métodos adecuados para el almacenamiento y etiquetado de las evidencias.

Muy bien, ya tenemos la **evidencia del ataque**, ahora veremos que ha de continuar siendo metódico y sobre todo conservando intactas las “huellas del crimen”, debe asegurar esa evidencia a toda costa, por lo tanto ¡NI SE LE OCURRA COMENZAR EL ANÁLISIS SOBRE ESA COPIA!.

Como primer paso deberá realizar dos copias de las evidencias obtenidas, genere una suma de comprobación de la integridad de cada copia mediante el empleo de funciones *hash*

tales como MD5 o SHA1. Incluya estas firmas en la etiqueta de cada copia de la evidencia sobre el propio CD o DVD, incluya también en el etiquetado la fecha y hora de creación de la copia, nombre cada copia, por ejemplo "COPIA A", "COPIA B" para distinguirlas claramente del original. Traslade estos datos a otra etiqueta y péguela en la caja contenedora del soporte, incluso sería conveniente precintar el original para evitar su manipulación inadecuada.

Si además decide extraer los discos duros del sistema para utilizarlos como evidencia, deberá seguir el mismo procedimiento, coloque sobre ellos la etiqueta "EVIDENCIA ORIGINAL", incluya además las correspondientes sumas *hash*, fecha y hora de la extracción del equipo, datos de la persona que realizó la operación, fecha, hora y lugar donde se almacenó, por ejemplo en una caja fuerte. Piense, además, que existen factores externos como cambios bruscos de temperatura o campos electromagnéticos que pueden alterar la evidencia. Toda precaución es poca, incluso si decide enviar esos discos a que sean analizados por empresas especializadas solicite que los aseguren por un importe similar a los daños causados en sus equipos.

Otro aspecto a tener en cuenta, y que está relacionado con el comentario anterior, es el proceso que se conoce como la **cadena de custodia**, donde se establecen las responsabilidades y controles de cada una de las personas que manipulen la evidencia. Deberá preparar un documento en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento. Sería interesante documentar:

- ✓ Dónde, cuándo y quién manejo o examinó la evidencia, incluyendo su nombre, su cargo, un número identificativo, fechas y horas, etc.
- ✓ Quién estuvo custodiando la evidencia, durante cuanto tiempo y dónde se almacenó.
- ✓ Cuando se cambie la custodia de la evidencia también deberá documentarse cuándo y como se produjo la transferencia y quién la transportó.

Todas estas medidas harán que el acceso a la evidencia sea muy restrictivo y quede claramente documentado, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas a intentos de acceso no autorizados.

Análisis de la evidencia

Una vez que disponemos de las **evidencias digitales** recopiladas y almacenadas de forma adecuada, pasemos a la fase quizás más laboriosa, el Análisis Forense propiamente dicho, cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque o *timeline*, determinando la cadena de acontecimientos que tuvieron lugar desde el instante inmediatamente anterior al inicio del ataque, hasta el momento de su descubrimiento.

Este análisis se dará por concluido cuando conozcamos cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc.

En el siguiente apartado se describirá este **proceso de análisis** empleando las herramientas propias del sistema operativo que se emplee como anfitrión y las que recopiló en su ToolKit, de esta forma se pretende dar una visión amplia del proceso que ayudará a compren-

der mejor el funcionamiento de las herramientas específicas para el análisis forense de sistemas que se expondrán más adelante.

Preparación para el análisis: El entorno de trabajo

Antes de comenzar el **análisis de las evidencias** deberá acondicionar un entorno de trabajo adecuado al estudio que desee realizar. Si se decanta por no tocar los discos duros originales ¡muy recomendable!, y trabajar con las imágenes que recopiló como evidencias, o mejor aún con una copia de éstas, tenga en cuenta que necesitará montar esas imágenes tal cual estaban en el sistema comprometido.

Si dispone de recursos suficientes prepare dos estaciones de trabajo, en una de ellas, que contendrá al menos dos discos duros, instale un sistema operativo que actuará de anfitrión y que le servirá para realizar el estudio de las evidencias . En ese mismo ordenador y sobre un segundo disco duro, vuelque las imágenes manteniendo la estructura de particiones y del sistema de archivos tal y como estaban en el equipo atacado. En el otro equipo instale un sistema operativo configurado exactamente igual que el del equipo atacado, además mantenga nuevamente la misma estructura de particiones y ficheros en sus discos duros. La idea es utilizar este segundo ordenador como "conejillo de Indias" y realizar sobre él pruebas y verificaciones conforme vayan surgiendo hipótesis sobre el ataque.

Si no dispone de estos recursos, puede utilizar software como VMware, que le permitirá crear una plataforma de trabajo con varias máquinas virtuales (varios equipos lógicos independientes funcionando sobre un único equipo físico). También puede decantarse por una versión LIVE de sistemas operativos como Linux, que le permitirá interactuar con las imágenes montadas pero sin modificarlas. Pero si tuvo la "feliz idea" de hacer que su ToolKit en CD o DVD fuese autoarrancable, ahora es el momento de utilizarlo.

Si está muy seguro de sus posibilidades y de lo que va a hacer, puede conectar los discos duros originales del sistema atacado a una estación de trabajo independiente para intentar hacer un análisis "en caliente" del sistema, deberá tomar la precaución de montar los dispositivos en modo sólo lectura, esto se puede hacer con sistemas anfitriones UNIX/Linux, pero no con entornos Windows.

Reconstrucción de la secuencia temporal del ataque

Supongamos que ya tenemos montadas las imágenes del sistema comprometido en nuestra estación de trabajo independiente y con un sistema operativo anfitrión *de confianza*. El primer paso que deberá dar es crear una línea temporal de sucesos o *timeline*, para ello recopile la siguiente información sobre los ficheros:

- ✓ Inodos asociados.
- ✓ Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).
- ✓ Ruta completa.
- ✓ Tamaño en bytes y tipo de fichero.
- ✓ Usuarios y grupos a quien pertenece.
- ✓ Permisos de acceso.
- ✓ Si fue borrado o no.

Sin duda esta será la información que más tiempo le llevará recopilar, pero será el punto de partida para su análisis, podría plantearse aquí dedicar un poco de tiempo a preparar un *script* que automatizase el proceso de creación del *timeline*, empleando los comandos que le proporciona el sistema operativo y su ToolKit.

Para comenzar ordene los archivos por sus fechas MAC, esta primera comprobación, aunque simple, es muy interesante pues la mayoría de los archivos tendrán la fecha de instalación del sistema operativo, por lo que un sistema que se instaló hace meses y que fue comprometido recientemente presentará en los ficheros nuevos, inodos y fechas MAC muy distintas a las de los ficheros más antiguos.

La idea es buscar ficheros y directorios que han sido creados, modificados o borrados recientemente, o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. Piense que la mayoría de los atacantes y sus herramientas crearán directorios y descargarán sus "aplicaciones" en lugares donde no se suele mirar, como por ejemplo en los directorios temporales.

A modo de guía céntrese primero en buscar los archivos de sistema modificados tras la instalación del sistema operativo, averigüe después la ubicación de los archivos ocultos y écheles un vistazo a ver dónde están y de qué tipo son, busque también los archivos borrados o fragmentos de éstos, pues pueden ser restos de logs y registros borrados por sus atacantes. Aquí cabe destacar nuevamente la importancia de realizar imágenes de los discos pues podremos acceder al espacio residual que hay detrás de cada archivo, (recordemos que los ficheros suelen almacenarse por bloques cuyo tamaño de *clúster* depende del tipo de sistema de archivos que se emplee), y leer en zonas que el sistema operativo *no ve*.

Piense que está buscando "una aguja en un pajar", por lo que deberá ser metódico, vaya de lo general a lo particular, por ejemplo parta de los archivos borrados, intente recuperar su contenido, anote su fecha de borrado y cotéjela con la actividad del resto de los archivos, puede que en esos momentos se estuviesen dando los primeros pasos del ataque.

Sin perder de vista ese *timestamp* anterior, comience a examinar ahora con más detalle los ficheros *logs* y de registros que ya ojeó durante la búsqueda de indicios del ataque, intente buscar una correlación temporal entre eventos. Piense que los archivos log y de registro son generados de forma automática por el propio sistema operativo o por aplicaciones específicas, conteniendo datos sobre accesos al equipo, errores de inicialización, creación o modificación de usuarios, estado del sistema, etc. Por lo que tendremos que buscar nuevamente entradas anómalas y compararlas con la actividad de los ficheros. Edite también el archivo de contraseñas y busque la creación de usuarios y cuentas extrañas sobre la hora que considere se inició el compromiso del sistema

Siguiendo con el ejemplo que se expuso en el apartado 3.1.1., en el fragmento del archivo `/var/log/messages` se detectaron dos accesos FTP, al examinar la actividad de los ficheros se descubrió que sobre esa fecha y hora se crearon varios archivos bajo el directorio `/var/ftp` de la máquina comprometida (directorio raíz del servicio ftp en sistemas UNIX/Linux), que además había sido borrado por el atacante. Al ser recuperado, se encontró la descarga de archivos que eran propiedad de usuario root (administradores del sistema) surgiendo la pregunta ¿qué hacía el administrador descargando archivos a esas horas?, el archivo recuperado era un conocido *rootkit*, se comprobó mediante el estudio del archivo de registro, que momentos después el atacante descomprimió, compiló y ejecutó sus "herramientas", acto

seguido (segundos después) se observa que un gran número de archivos de comandos del sistema operativo son modificados.

Este pequeño ejemplo es representativo de cómo ha de utilizar el *timestamp* para hacerse una idea más o menos certera de la cadena de eventos que se produjo.

Determinación de cómo se realizó el ataque

Una vez que disponga de la cadena de acontecimientos que se han producido, deberá determinar cuál fue la vía de entrada a su sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal brecha. Estos datos, al igual que en el caso anterior, deberá obtenerlos de forma metódica, empleando una combinación de consultas a archivos de logs, registro, claves, cuentas de usuarios, etc.

Un buen punto de partida es repasar los servicios y procesos abiertos que recopiló como evidencia volátil, así como los puertos TCP/UDP y conexiones que estaban abiertas cuando el sistema estaba aún "vivo". Examine con más detalle aquellas circunstancias que le resultaron sospechosas cuando buscó indicios sobre el ataque, y realice con ellos un búsqueda de vulnerabilidades a través de Internet, emplee Google o utilice páginas específicas donde encontrará perfectamente documentadas cientos de vulnerabilidades, como por ejemplo el CERT, www.cert.org o en la base bugtraq en www.securityfocus.com.

Siguiendo con el ejemplo anterior, se sospechaba que al ataque se inició a través del servicio FTP que ejecutaba la máquina comprometida, se conocía una vulnerabilidad en dicho servicio y al realizar la consulta correspondiente se descubrió que efectivamente, ésta máquina era vulnerable pues no había sido instalado el parche de seguridad correspondiente, ¿recuerda el punto 1 del apartado Prevención de ataques a sistemas?. Pero no se confíe piense que si existía esa vulnerabilidad puede que haya otras, realice el proceso de búsqueda cuantas veces crea necesario, se imagina que ocurriría si volviese a instalar el sistema y dejase otra brecha de seguridad.

Si ya tiene claro cuál fue la vulnerabilidad que dejó su sistema "al desnudo", vaya un paso más allá y busque en Internet algún *exploit* anterior a la fecha del compromiso, que utilice esa vulnerabilidad. Generalmente lo encontrará en forma de rootkit y un buen lugar donde comenzar su búsqueda es, nuevamente, Google aunque también le será de utilidad anotar la siguiente dirección www.packetstormsecurity.org.

En este punto es muy importante que sea metódico, refuerce cada una de sus hipótesis empleando una formulación causa-efecto, también es el momento de arrancar y comenzar a utilizar nuestra máquina "conejillo de Indias". Pruebe sobre ella los exploits que ha encontrado, si he leído bien, NO TENGA MIEDO, recuerde que en el análisis forense una premisa es que los hechos han de ser reproducibles y sus resultados verificables, por lo tanto compruebe si la ejecución de ese exploit sobre una máquina igual que la comprometida y en perfecto estado (causa posible), genera los mismos eventos que ha encontrado entre sus evidencias (efecto verificable).

Si no es tan atrevido, puede recurrir a las bases de datos sobre ataques de los *honeypots*, herramientas de seguridad informática (implantadas por hardware o por software), cuya intención es atraer a crackers o spammers, simulando ser sistemas vulnerables o débiles a los

ataques, permitiendo recoger información sobre los atacantes y sus técnicas, permitiendo un examen en profundidad del atacante, durante y después del ataque al honeypot.

Identificación del autor o autores del incidente

Si ya ha logrado averiguar cómo entraron en sus sistemas, ahora le toca saber quién o quiénes lo hicieron. Para este propósito le será de utilidad consultar nuevamente algunas evidencias volátiles que recopiló en las primeras fases, revise las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además busque entre las entradas a los logs de conexiones. También puede indagar entre los archivos borrados que recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

La **identificación de sus atacantes** será de especial importancia si tiene pensado llevar a cabo acciones legales posteriores o investigaciones internas a su organización. Si no va a seguir estos pasos, puede saltarse esta fase y dedicar ese tiempo a otros menesteres, como por ejemplo recuperar completamente el sistema atacado y mejorar su seguridad.

Pero si decide perseguir a sus atacantes, deberá realizar algunas pesquisas como parte del proceso de identificación. Primero intente averiguar la dirección IP de su atacante, para ello revise con detenimiento los registros de conexiones de red y los procesos y servicios que se encontraban a la escucha. También podría encontrar esta información en fragmentos de las evidencias volátiles, la memoria virtual o archivos temporales y borrados, como restos de e-mail, conexiones fallidas, etc.

Si cree tener una IP sospechosa, compruebe en el registro RIPE NCC (www.ripe.net) a quién pertenece. Pero ojo, no saque conclusiones prematuras, muchos atacantes falsifican la dirección IP con técnicas de *spoofing*. Suponga que encuentra una dirección IP y tras consultar el registro RIPE, le aparece que está asignada a una importante entidad bancaria ¿cree sinceramente que un empleado de banca le ha atacado?. Otra técnica de ataque habitual consiste en utilizar “ordenadores zombis”, éstos son comprometidos en primera instancia por el atacante y posteriormente son utilizados como lanzaderas del ataque final sin que sus propietarios sepan que están siendo cómplices de tal hecho. Por ello, para identificar a su atacante tendrá que verificar y validar la dirección IP obtenida.

También puede emplear **técnicas hacker**, eso sí ¡DE FORMA ÉTICA!, para identificar a su atacante, piense que si este dejó ejecutándose en el equipo comprometido “un regalito” como una puerta trasera o un troyano, está claro que en el equipo del atacante deberán estar a la escucha esos programas y en los puertos correspondientes, bien esperando noticias o buscando nuevas víctimas. Aquí entra en juego nuevamente nuestro ordenador “conejillo de indias”.

Si procede de esta forma, use una de las herramientas más impresionantes y baratas que encontrará `nmap`, este “mapeador de redes” es una utilidad de código abierto (por lo tanto gratuita) para exploración de redes y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" de forma novedosa, para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando y así hasta como docenas de características.... Una auténtica joya para los analistas de sistemas.

En este apartado también cabe la posibilidad de adentrarse en los "bajos fondos" de Internet para intentar buscar a sus atacantes, pues en ocasiones algunos de ellos se jactan de sus hazañas públicamente en foros y Chat, visite estos lugares y verá lo que uno puede llegar a aprender.

Otro aspecto que le interesaría averiguar es el perfil de sus atacantes, aunque sin entrar en detalles podrá encontrarse con los siguientes tipos de "tipos":

Hackers: Son los más populares y tienen hasta su propia película (*HACKERS* de Iain Softley, 1995). Se trata de personas con conocimientos en técnicas de programación, redes, Internet y sistemas operativos. Sus ataque suelen tener motivaciones de tipo ideológico (pacifistas, ecologistas, anti globalización, anti Microsoft, etc.) o simplemente lo consideran como un "desafío intelectual".

SciptKiddies: Son una nueva especie que ha saltado a la escena de la delincuencia informática recientemente. Se trata de jóvenes que con unos conocimientos aceptables en Internet y programación emplean herramientas ya fabricadas por otros para realizar ataques y "ver que pasa". Su nombre viene de su corta edad y del uso intensivo que haces de los scrpts (guiones) de ataque que encuentran por Internet.

Profesionales: Son personas con muchísimos conocimientos en lenguajes de programación, en redes y su equipamiento (routers, firewall, etc.), Internet y sistemas operativos tipo UNIX. Suelen realizar los ataques taques bajo encargo, por lo que su forma de trabajar implica una exhaustiva preparación del mismo, realizando un estudio meticuloso de todo el proceso que llevará a cabo, recopilando toda la información posible sobre sus objetivos, se posicionará estratégicamente cerca de ellos, realizará un tanteo con ataques en los que no modificará nada ni dejará huellas... cuando lo tenga todo bien atado entonces atacará... pero tranquilo, este tipo de atacantes se encuentra muy poco y además se dedica a dar grandes golpes.

Evaluación del impacto causado al sistema

Para poder evaluar el impacto causado al sistema, el análisis forense le ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron a sus sistemas. Esto le permitirá evaluar el compromiso de sus equipos y realizar una estimación del impacto causado. Generalmente se pueden dar dos tipos de ataques:

Ataques pasivos: en los que no se altera la información ni la operación normal de los sistemas, limitándose el atacante a fisgonear por ellos.
Ataques activos, en los que se altera, y en ocasiones seriamente, tanto la información como la capacidad de operación del sistema.

Deberá tener en cuanta, además otros aspectos del ataque como los efectos negativos de tipo técnico que ha causado el incidente, tanto inmediatos como potenciales además de lo crítico que eran los sistemas atacados. Por ejemplo ataques al cortafuegos, el router de conexión a Internet o Intranet, el servidor Web corporativo, los servidores de bases de datos, tendrán diferente repercusión según el tipo de servicio o negocio que preste su organización y las relaciones de dependencia entre sus usuarios. Piense que una manipulación de una Web corporativa que realiza funciones meramente publicitarias tendrá un impacto mucho menor

que si eso mismo ocurre por ejemplo en eBay, que su negocio está basado totalmente en las subastas por Internet y un parón en su servidor Web puede traducirse en miles de euros de pérdidas por cada hora.

Puede también recurrir a métodos como BIA (Bussines Impact Analysis) que le indicarán como determinar el impacto de eventos específicos, permitiéndole valorar los daños en cantidades monetarias, que podrá presentar dado el caso, a su compañía de seguros.

Pero no piense sólo en los daños y pérdidas actuales, sino que tendrá que pensar en daños potenciales, si no conoce qué actividades han llevado a cabo los atacantes, no sabrá hasta dónde han podido "fastidiarle" sus sistemas, o peor aún, hasta dónde pueden llegar, pues ¿qué ocurriría si desconoce que su atacante consiguió descargarse un archivo que contenía datos de carácter personal de sus empleados?, y peor aún, ¿qué pasaría si el atacante alardeando de su proeza publica esos ficheros en Internet?. Pues bien, el artículo 44.3.h de la Ley Orgánica 15/1999,de 13 de Diciembre, de Protección de Datos de Carácter Personal se lo aclarará rápidamente:

"Artículo 44. Tipos de infracciones

...

3. Son infracciones graves:

...

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

...."

Sólo comentar que las sanciones para este tipo de infracciones son de 60.000 a 600.000 €.

Documentación del incidente

Tan pronto como el incidente haya sido detectado, es muy importante comenzar a tomar notas sobre todas las actividades que se lleven a cabo. Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finalice el proceso de análisis forense, esto le hará ser más eficiente y efectivo al tiempo que reducirá las posibilidades de error a la hora de gestionar el incidente.

Por otro lado, cuando se haya concluido el análisis y durante éste, tendrá que mantener informados a las personas adecuadas de la organización, por lo que será interesante que disponga de diversos métodos de comunicación. Además como se verá necesitará tener preparados una serie de formularios y presentar tras la resolución del incidente al menos dos tipos de informes uno Técnico y otro Ejecutivo.

Utilización de formularios de registro del incidente

Al hilo de lo comentado anteriormente, el empleo de formularios puede ayudarle bastante en este propósito. Éstos deberán ser rellenados por los departamentos afectados por el compromiso o por el propio equipo que gestionará el incidente. Alguno de los formularios que debería preparar serán:

- ✓ Documento de custodia de la evidencia.
- ✓ Formulario de identificación del equipos y componentes.
- ✓ Formulario de incidencias tipificadas.
- ✓ Formulario de publicación del incidente.
- ✓ Formulario de recogida de evidencias.
- ✓ Formulario de discos duros.

El Informe Técnico

Este informe consiste en una exposición detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense. A modo de orientación, deberá contener, al menos, los siguientes puntos:

- ✓ Antecedentes del incidente.
- ✓ Recolección de los datos.
- ✓ Descripción de la evidencia.
- ✓ Entorno del análisis .
  - Descripción de las herramientas.
- ✓ Análisis de la evidencia .
  - Información del sistema analizado .
    - Características del SO.
    - Aplicaciones.
    - Servicios.
    - Vulnerabilidades.
    - Metodología.
- ✓ Descripción de los hallazgos.
  - Huellas de la intrusión.
  - Herramientas usadas por el atacante.
  - Alcance de la intrusión.
  - El origen del ataque
- ✓ Cronología de la intrusión.
- ✓ Conclusiones.
- ✓ Recomendaciones específicas.
- ✓ Referencias.

El Informe Ejecutivo

Este informe consiste en un resumen del análisis efectuado pero empleando una explicación no técnica, con lenguaje común, en el que se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Constará de pocas páginas, entre tres y cinco, y será de especial interés para exponer lo sucedido a personal no especializado en sistemas informáticos, como pueda ser el departamento de Recursos Humanos, Administración, e incluso algunos directivos. En este informe deberá, donde se describir, al menos, lo siguiente:

- ✓ Motivos de la intrusión.
- ✓ Desarrollo de la intrusión
- ✓ Resultados del análisis.
- ✓ Recomendaciones.

4

Herramientas para Análisis Forense Digital

Hasta ahora se han desarrollado las fases del análisis forense de sistemas centrándonos en la utilización bien herramientas del sistema operativo o las propias del ToolKit que creamos como parte de nuestro plan de respuestas ante incidentes, por lo que hemos realizado la investigación de forma manual. Pero habrá podido comprobar que una de las dificultades que se encontrará el investigador a la hora de analizar determinadas evidencias digitales es que los atacantes emplean cada vez herramientas más sigilosas y perfeccionadas para realizar sus asaltos. Por lo tanto no estará de más disponer de un conjunto de herramientas específicas para el análisis de evidencias que nos ayudaran a completar de forma más eficiente nuestra investigación.

Dejando a parte el software comercial, en el que podrá encontrar herramientas específicas como EnCase de la empresa Guidance Software, considerado un estándar en el análisis forense de sistemas, nos centraremos en herramientas de código abierto (Open Source) que podrá descargar libremente desde la página sus correspondientes autores o miembros del proyecto.

Software de Libre Distribución y Open Source

Vamos a comenzar con una recopilación de herramientas que necesitan ser ejecutadas bajo un sistema operativo anfitrión, bien sea MS Windows o UNIX/Linux.

The Forensic ToolKit

Se trata de una colección de herramientas forenses para plataformas Windows, creado por el equipo de Foundstone. Puede descargarlo desde www.foundstone.com, donde además encontrará gran cantidad de herramientas de seguridad. Este ToolKit le permitirá recopilar información sobre el ataque, y se compone de una serie aplicaciones en línea de comandos que permiten generar diversos informes y estadísticas del sistema de archivos a estudiar. Para poder utilizarlos deberá disponer de un intérprete de comandos como cmd.exe.

Comando	Función
`afind`	Realiza búsqueda de archivos por su tiempo de acceso, sin modificar la información de acceso al mismo.
`hfind`	Busca archivos ocultos en el Sistema Operativo.
`sfind`	Busca flujos de datos ocultos en el disco duro, éstos son distintos de los archivos ocultos y no aparecerán con herramientas normales del sistema operativo. Su importancia radica en que pueden usarse para ocultar datos o software dañino.
`filestat`	Ofrece una lista completa de los atributos del archivo que se le pase como argumento (uno cada vez).
`hunt`	Permite obtener información sobre un sistema que utiliza las opciones de sesión NULL, tal como usuarios, recursos compartidos y servicios.

The Sleuth Kit y Autopsy

Este conjunto, cuyo autor es Brian Carrier, consiste en una colección de herramientas forenses para entornos UNIX/Linux, que incluye algunas partes del conocido The Coroners ToolKit (TCT) de Dan Farmer. Puede analizar archivos de datos de evidencias generadas con utilidades de disco como por ejemplo dd. Pese a ser de libre distribución (puede descargarlo del sitio Web www.sleuthkit.org) ofrece más detalle que algunos programas de pago. Incluye funciones como registro de casos separados e investigaciones múltiples, acceso a estructuras de archivos y directorios de bajo nivel y eliminados, genera la línea temporal de actividad de los archivos (timestamp), permite buscar datos dentro de las imágenes por palabras clave, permite crear notas del investigador e incluso genera informes... y mucho más.

Este ToolKit puede funcionar conjuntamente con el Autopsy Forensic Browser, consistente en una interfaz gráfica que le facilitará notablemente su labor a la par que le permitirá generar vistosos salidas gráficas para sus informes.

Para analizar sus datos empleando este ToolKit dedique el tiempo necesario a su configuración inicial, que luego agradecerá, pues dispondrá de una poderosa herramienta forense para organizar y estudiar sus evidencias. Debido a la gran cantidad de opciones se necesitaría un documento solamente dedicado a esta herramienta, así que a modo de resumen, algunas de las funciones básicas con las que podrá contar son las siguientes opciones de análisis:

Opción	Descripción
Análisis de archivos	Muestra la imagen como archivos y directorios, permitiendo ver incluso aquellos que estarían ocultos por el sistema operativo.
Búsqueda por palabra clave	Permite buscar dentro de la imagen palabras clave, pueden ser archivos o cualquier otra referencia que se le pase como argumento.
Tipo de archivo	Permite tanto la búsqueda como la ordenación de archivos según su tipo.
Detalles de la imagen	Muestra en detalle la imagen a examinar, permitiendo saber dónde se encuentran físicamente los datos dentro de ella.
Matadatos	Permite ver elementos del sistema de archivos que no se muestran habitualmente, como las referencias a directorios o los archivos eliminados.
Unidad de datos	Ofrece la posibilidad de entrar en el máximo detalle de cualquier archivo, permitiendo examinar el contenido real del mismo, ya sea en ASCII o en hexadecimal.

Como se indicó al inicio de este apartado, las herramientas expuestas anteriormente necesitan de la ejecución sobre un sistema operativo ya instalado. En ocasiones le será de gran utilidad disponer de un entorno tipo *Live*, que le permita realizar un examen forense de imágenes sin tener que dedicar un equipo específico para ello y sin necesidad cargar otro sistema operativo. Estas soluciones suelen encontrarse en CDs o DVDs preparados para tal fin, veamos alguno de ellos.

HELIX CD

Se trata de un Live CD de respuesta ante incidentes, basado en una distribución Linux denominada *Knoppix* (que a su vez está basada en Debian). Posee la mayoría de las herramientas necesarias para realizar un análisis forense tanto de equipos como de imágenes de discos. Puede descargarlo gratuitamente de:

http://www.e-fense.com/helix/.

Este CD ofrece dos modos de funcionamiento, tras ejecutarlo nos permitirá elegir entre arrancar un entorno MS Windows o uno tipo Linux. En el primero de ellos disponemos de un entorno con un conjunto de herramientas, casi 90 Mb, que nos permitirá principalmente interactuar con sistemas "vivos", pudiendo recuperar la información volátil del sistema. En el arranque Linux, disponemos de un Sistema Operativo completo, con un núcleo modificado para conseguir una excelente detección de hardware, no realiza el montaje de particiones swap, ni ninguna otra operación sobre el disco duro del equipo sobre el que se arranque. Es ideal para el análisis de equipos "muertos", sin que se modifiquen las evidencias pues montará los discos que encuentre en el sistema en modo sólo lectura. Además de los comandos de análisis propios de los entornos UNIX/Linux, se han incorporado una lista realmente interesante de herramientas y ToolKits, alguno de ellos comentados anteriormente como el Sleuth Kit y Autopsy.

F.I.R.E. Linux

Se trata de otro CD de arranque que ofrece un entorno para respuestas a incidentes y análisis forense, compuesto por una distribución Linux a la que se le han añadido una serie de utilidades de seguridad, junto con un interfaz gráfico que hace realmente fácil su uso. Al igual que el kit anterior, por su forma de montar los discos no realiza ninguna modificación sobre los equipos en los que se ejecute, por lo que puede ser utilizado con seguridad. Este live CD está creado y mantenido por William Salusky y puede descargarse gratuitamente desde la dirección http://biatchux.dmzs.com. En esta interesantísima distribución podrá disponer de una serie de funcionalidades que le aportará muchas ventajas en su análisis, entre las que cabe destacar:

- ✓ Recolección de datos de un sistema informático comprometido y hacer un análisis forense.
- ✓ Chequear la existencia de virus o malware en general desde un entorno fiable.
- ✓ Posibilidad de realización de test de penetración y vulnerabilidad.
- ✓ Recuperación datos de particiones dañadas.

Las herramientas que posee F.I.R.E son conocidas y muy recomendables, aunque sin entrar en detalles sobre cada una de ellas, podrá encontrar las siguientes:

- ✓ `Nessus, nmap, whisker, hping2, hunt, fragrouter.`
- ✓ `Ethereal, Snort, tcpdump, ettercap, dsniff, airsnort.`
- ✓ `Chkrootkit, F-Prot.`
- ✓ TCT, Autopsy.
- ✓ `Testdisk, fdisk, gpart.`
- ✓ SSH (cliente y servidor), VNC (cliente y servido)
- ✓ Mozilla, ircII, mc, Perl, biew, fenris, pgp.

5

Conclusiones

Con este trabajo se ha pretendido realizar una primera incursión en el apasionante y novedoso mundo del Análisis Forense Digital, exponiendo aquellas características y particularidades propias de esta disciplina de la seguridad informática. Se ha enfocado el tema desde el punto de vista de una herramienta indispensable que toda organización debe contemplar dentro de su política de seguridad y enmarcada dentro del proceso de respuesta a incidentes en los sistemas informáticos.

Se ha intentado destacar la necesidad imperiosa de aplicar metodologías y procedimientos específicos con el fin de asegurar la garantía de calidad de las evidencias durante todo el proceso forense, haciendo hincapié en la recopilación y custodia de las evidencias digitales. Se han expuesto también las diferencias a la hora de llevar a cabo un análisis forense en dos de los sistemas operativos más extendidos, MS Windows y UNIX/Linux, y cómo podemos disponer de herramientas software específicas que nos pueden ayudar en el análisis, sin entrar en las de tipo hardware por motivos de espacio y tiempo.

Desde el punto de vista de la situación actual de la disciplina, se destaca una falta de unicidad de criterios tanto a la hora de definir estándares para las herramientas a emplear, como para el proceso de certificación y acreditación de los profesionales del sector. Aunque si se ha encontrado una importante comunidad de desarrollo, tanto por parte de organizaciones como por parte de grupos de software de libre distribución, que están continuamente aportando nuevas herramientas y procedimientos.

Destacar en este campo el Concurso de Reto Forense que se viene celebrando desde el año 2004, en el que los participantes deben analizar un sistema informático comprometido. Éste reto está patrocinado por las dos principales entidades académicas de seguridad informática de España y México, la UNAM a través de la DGSCA y el UNAM-CERT y la organización pública Red.es a través del Grupo de Seguridad de RedIRIS, con el apoyo de organizaciones y organismos de seguridad informática iberoamericanos y mundiales.

También cabe mencionar los proyectos como el "Spanish Honeynet Project", http://www.honeynet.org.es/ organización de investigación no lucrativa compuesta por profesionales de seguridad informática dedicada a temas de seguridad centrados en tecnologías de redes trampa. Su objetivo principal es estudiar, comprender y avisar sobre los motivos y tácticas de la comunidad *hacker*, además comparten los conocimientos sobre las distintas herramientas y prácticas utilizadas por los atacantes en Internet.

6
Bibliografía y referencias

Libros

“Seguridad en las Comunicaciones y en la Información”, G. Díaz Orueta y otros. Ed. UNED
“Software Libre. Herramientas de Seguridad”. Tony Howlet. Ed. Anaya Multimedia.
“Hackers 2”. J. Scambray, S. McClure y G. Kurtz. ED. Osborne-McGraw-Hill.
“Extreme Exploits”. V. Oppleman, Brett Watson. Ed. Anaya Multimedia.

Referencias

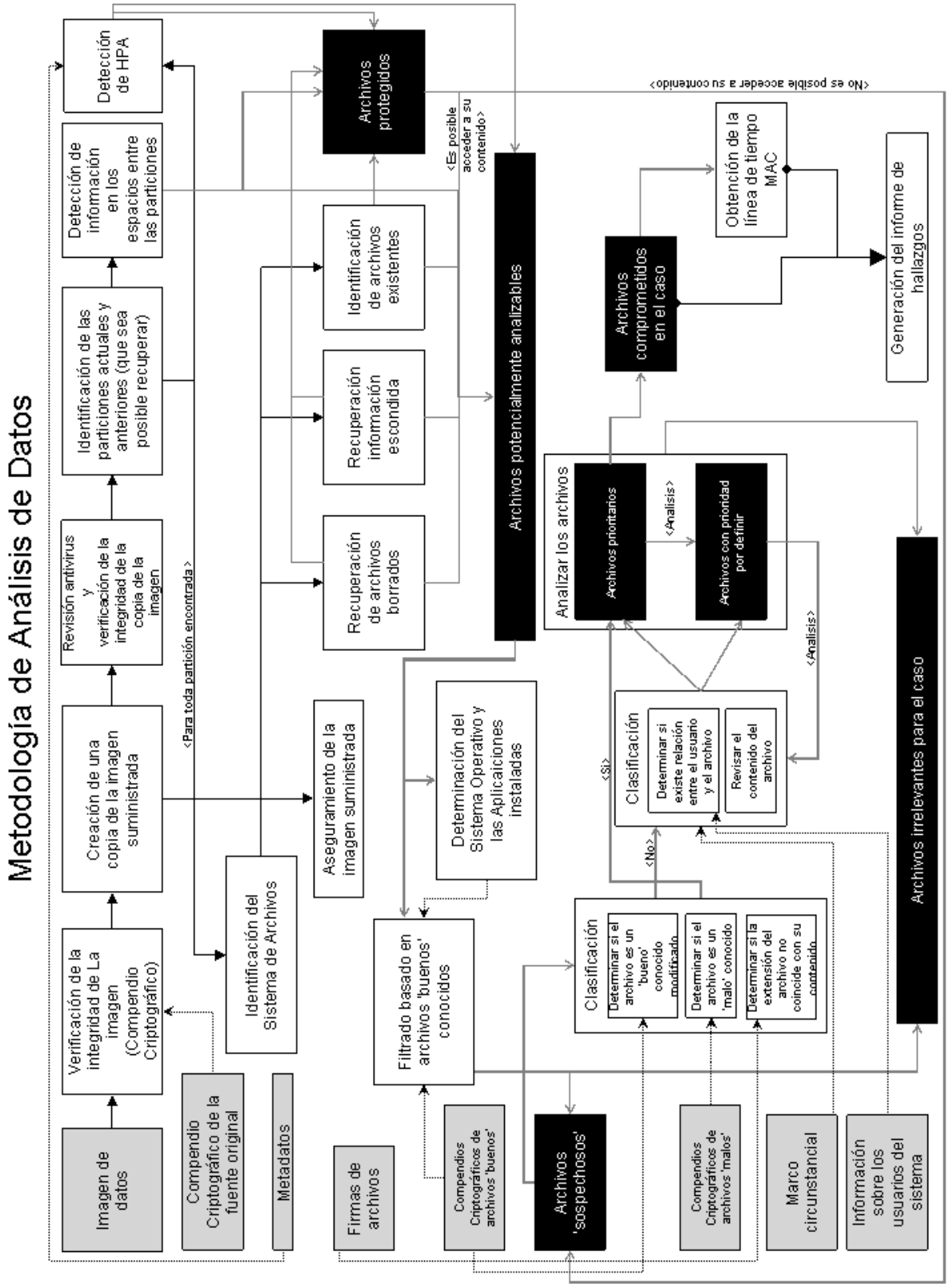
SP-800-61 ”Computer Security Incident Handling Guide”. T. Grance. NIST-USA. 2002
"GIAC Security Essentials, Practical Assignment" Version 1.4b. Tan Koon Yaw. SANS Institute 2003.
"Forensic Examination of Digital Evidence: A Guide for Law Enforcement". John Ashcroft. U.S. Dep. of Justice, Apr. 2004
"Helix 1.7 for Beginners". BJ Gleason and Drew Fahey. Manual Version Mar. 2006
"First Responder’s Manual". U.S. Dep. of Energy Computer Forensic Laboratory. 1999.
“Análisis Forense Digital GNU/Linux”. David Ditrich y Ervin Sarkisov. 2002
RFC-3227. “Guidelines for Evidence Collection and Archiving”. Feb. 2002.
Análisis técnicos del Reto Forense ediciones 1 y 2 (comunidad RedIris). 2004 y 2005.
CoBIT 4.0 “Control Objective for Information and Related Technology”. IT Governance Institute 2005.
“Una Propuesta Metodológica y su Aplicación en The Sleuth Kit y EnCase Descargar en disco”. Octubre de 2005. Jonathan Córdoba; Ricardo Laverde; Diego Ortiz; Diana Puentes.

7
URLs

www.auditoresdesistemas.com
www.criptored.upm.es
www.dfrws.org
www.e-fense.com
www.enfsi.org
www.forensics-es.org
www.foundstone.com
www.google.es
www.ioce.org
www.isaca.org
www.opensourceforensics.org
www.red.es
www.securityfocus.com
www.wikipedia.org

Apéndices

A.1.- Esquema del proceso de respuesta a incidentes.



Fuente: "Una Propuesta Metodológica y su Aplicación en The Sleuth Kit y EnCase Descargar en disco". Octubre de 2005. Jonathan Córdoba; Ricardo Laverde; Diego Ortiz; Diana Puentes.

A.2.- Ejemplo de e-mail de notificación sobre incidentes a un ISP.

TO: abuse_email@example-isp.com
Ref: Intrusion notification

Please be advised that on the [date of compromise] an intrusion took place into and against our systems.

Upon a thorough analysis of the systems involved, evidence appeared that the intrusion in questiontook place from two IP addresses pertaining to a rank monitored by your company.

IP addresses and time and hour mentioned in our report are the following:

Time	Ip Address
01:18:47	xxx.xxx.xxx.xxx
09:29:17	xxx.xxx.xxx.xxx

These times and hours correspond to GMT+1. Correspondence with regard to your time GMT+2 is as follows:

Time	Ip Address
02:18:47	xxx.xxx.xxx.xxx
10:29:17	xxx.xxx.xxx.xxx

We beg you please take the adequate and proper administrative and/or legal steps in order to avoid, in the future, as far as you possibly can, these type and kind of unfair & elegal actions.

Should you require / need any additional clarification / information, please do not hesitate to contact us through any o the below quoted means:

Phone:
E-mail:

We most earnestly thank you for your attention and coorperation towards a balanced and profitable business running.

A.3.- Glosario de términos.

Exploit

Exploit (del inglés to exploit, explotar, aprovechar) es el nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa. El fin puede ser la destrucción o inhabilitación del sistema atacado, aunque normalmente se trata de violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros. Los exploits se pueden caracterizar según las categorías de vulnerabilidades utilizadas para su ataque.

Honeypot

Se denomina Honeypot al software o conjunto de computadores cuya intención es atraer a crackers o spammers, simulando ser sistemas vulnerables o débiles a los ataques. Es una herramienta de seguridad informática utilizada para recoger información sobre los atacantes y sus técnicas. Los Honeypots pueden distraer a los atacantes de las máquinas más importantes del sistema, y advertir rápidamente al administrador del sistema de un ataque, además de permitir un examen en profundidad del atacante, durante y después del ataque al honeypot.

Algunos honeypots son programas que se limitan a simular sistemas operativos no existentes en la realidad y se les conoce como honeypots de baja interacción y son usados fundamentalmente como medida de seguridad. Otros sin embargo trabajan sobre sistemas operativos reales y son capaces de reunir mucha más información; sus fines suelen ser de investigación y se los conoce como honeypots de alta interacción.

También se llama honeypot a un website o sala de chat, que se ha creado para descubrir a otro tipo de usuarios con intenciones criminales, (e.j., pedofilia).

Inodo

En informática, un inodo o (i-node en inglés) es una estructura de datos propia de los sistemas de archivos tradicionalmente empleados en los sistemas operativos tipo UNIX como es el caso de Linux.

Un inodo contiene las características (permisos, fechas, ubicación, pero NO el nombre) de un archivo regular, directorio, o cualquier otro objeto que pueda contener el sistema de ficheros.

El término "inodo" refiere generalmente a inodos en discos (dispositivos en modo bloque) que almacenan archivos regulares, directorios, y enlaces simbólicos. El concepto es particularmente importante para la recuperación de los sistemas de archivos dañados.

Cada inodo queda identificado por un número entero, único dentro del sistema de ficheros, y los directorios recogen una lista de parejas formadas por un número de inodo y nombre identificativo que permite acceder al archivo en cuestión: cada archivo tiene un único inodo, pero puede tener más de un nombre en distintos o incluso en el mismo directorio para facilitar su localización.

Rootkit

Un rootkit es un conjunto de herramientas usadas frecuentemente por los intrusos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos. Hay rootkits para una amplia variedad de sistemas operativos, como Linux, Solaris o Microsoft Windows.

Fuente: www.wikipedia.org