Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN, CIENCIA Y EMPLEO

AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación
Análisis Forense Digital tras Incidentes de Seguridad

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-4973-131202*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*02/12/2013*
N° de Páginas	*1 de 18*

1 TABLA DE CONTENIDOS

2 OBJETO

Este documento está desarrollado con objeto de aportar al personal de la Junta de Andalucía, tengan o no conocimientos técnicos, una introducción sobre análisis forense digital.

3 ALCANCE

Este documento va destinado al personal técnico de la Junta de Andalucía y al público en general. En él se proporciona fundamentos básicos del análisis forense digital.

4 INTRODUCCIÓN

"Sí la perfección no existe, el crimen perfecto tampoco".

Gil Grissom. CSI

¿Que es el análisis forense? De una forma muy general, es el conjunto de técnicas científicas y analíticas que permiten identificar, recolectar, preservar, analizar y presentar evidencias sobre la ocurrencia de un cierto suceso, y que de ser necesario puedan ser presentadas en un proceso legal. Los métodos forenses se ocupan principalmente de la recuperación y el análisis de la evidencia latente. Ésta puede tomar muchas formas, desde huellas digitales en una ventana, ADN recuperado de una mancha de sangre o, archivos en un disco duro.

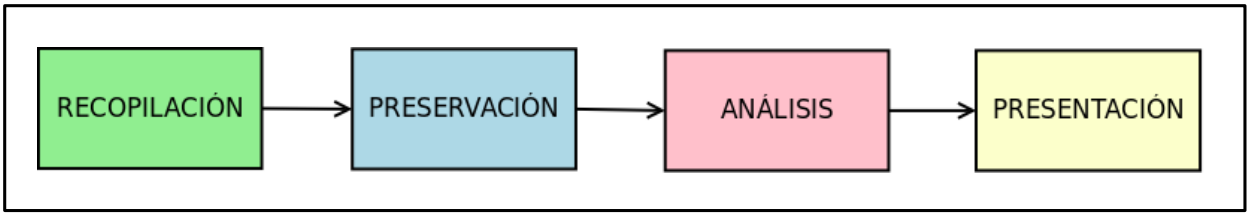
Ligado al ámbito de las TIC, existe lo que se conoce como **Análisis forense digital** ó Computer Forensics. Se define como el conjunto de principios y técnicas que comprende el proceso de extracción, conservación, análisis, documentación y presentación de **evidencias digitales** sobre un determinado escenario TI con objeto de saber qué es lo que ha ocurrido tras un incidente de seguridad, y que llegado el caso, puedan ser aceptadas legalmente en un proceso judicial. Por **evidencia digital** se entiende como cualquier información en formato digital que pueda establecer una relación entre el suceso bajo análisis y su autor. Por ejemplo, un archivo de log, una cookie en el disco duro, un proceso en ejecución o un acceso a una aplicación.

Las técnicas forenses sirven de apoyo a la hora de reconstruir y analizar evidencias de lo ocurrido en un **incidente de seguridad**. En este documento se pretende mostrar cómo su aplicación al análisis de sistemas proporciona una metodología afín dentro del proceso de respuesta a incidentes.

5 FASES DE UN ANÁLISIS FORENSE

A grandes rasgos, la realización de una investigación forense digital se puede dividir en 4 fases:

- **Identificación del incidente: Búsqueda y recopilación**: La primera fase del proceso es identificar el incidente de seguridad. Esto engloba buscar y recopilar los datos de todas las fuentes posibles que sean relevantes para el estudio del incidente, incluyendo las humanas.
- **Preservación**: Una vez obtenidos los datos es muy importante mantener y preservarlos sin alteración. Para ello debe realizarse un procedimiento denominado "Cadena de Custodia".
- **Análisis**: En esta fase es necesario analizar los datos adquiridos. Se usarán técnicas y métodos legalmente justificables con la idea de obtener información útil que responda a las preguntas que fueron el motivo para llevar a cabo la recolección y el examen.
- **Documentación y presentación**: La fase final es informar de los resultados obtenidos en el análisis, que incluye la descripción de las acciones realizadas, el motivo de la selección de ciertas herramientas y procedimientos, así como señalar que otros tipos de acciones necesitan ser realizadas (análisis de otros orígenes de datos, resolver vulnerabilidades identificadas) y proporcionar recomendaciones para la mejora de políticas, directrices, procedimientos, herramientas, etc.



Al final de todo el proceso, de la información recopilada, tras su paso por todas las fases indicadas, deben sacarse pruebas o evidencias que permitan elaborar conclusiones.

Rigor durante un forense

Es muy importante desde el comienzo del proceso de análisis plantearse las siguientes preguntas:

- ¿Cuál es el objetivo final de la toma de datos?
- ¿Se pretenden usar los resultados del análisis en un proceso judicial?

En muy frecuente que en los casos forenses se conozca cuales son los inicios de la investigación, pero no cuál puede ser su final. Es interesante conocer si las partes interesadas en la investigación tienen intención de llevar el caso a los juzgados. La recogida de evidencias será condicionada teniendo en cuenta esta circunstancia. Cabe resaltar que hablamos de posibilidades de que se lleve a juicio, ya que las intenciones de los interesados pueden variar a medida de que la información va saliendo a la luz.

Aquellos análisis que puedan derivar en un juicio deben ser atendidos con mayor pulcritud y rigor procedimental para que las conclusiones obtenidas a partir de las evidencias, sean válidas, creíbles y lo más importante: "rotundas" e irrefutables sea cuáles fueren los argumentos utilizados. Los criterios a seguir en este caso variarán dependiendo de la legislación bajo la que estemos actuando.

Aquellas actuaciones cuyo objetivo no es atender a un proceso judicial, sino obtener una determinada información, permiten una mayor flexibilidad, reduciendo con ello los tiempos dedicados a la recogida y tratamiento de evidencias.

5.1 IDENTIFICACIÓN DEL INCIDENTE. BÚSQUEDA Y RECOPILACIÓN

El primer paso en el proceso forense es recolectar los datos relevantes para el estudio del incidente. Para ello es necesario lo siguiente:

- Identificar los potenciales orígenes de datos.
- Proceder a su adquisición.

5.1.1 IDENTIFICACIÓN DE ORÍGENES DE DATOS

En esta fase del proceso forense nos interesará encontrar todas aquellas fuentes de información que nos puedan permitir identificar las señales del incidente. La pregunta es, ¿donde puedo buscar los indicios del incidente?

Como es evidente, el primer sitio donde se podrá buscar es en aquellos equipos que hayan estado en la primera línea del incidente y hayan podido ser comprometidos. Pero no debemos limitarnos únicamente a éstos. Como máquinas que han sido comprometidas, su información puede haber sido alterada. Es posible que existan otras máquinas cercanas donde podamos encontrar información relacionada con el incidente durante fases como el reconocimiento del escenario bajo ataque (escaneos de puertos), equipamiento usado para pivotar entre máquinas o en dispositivos de interconexión que puedan haber registrado actividad.

En primer lugar habrá que identificar qué **orígenes físicos** (equipos de sobremesa, portátiles, unidades extraíbles, móviles, ...) pueden haber estado implicados en el incidente y por tanto deberían ser estudiados.

A continuación, para cada origen físico tendremos que identificar los posibles **orígenes lógicos**. Éstos variarán en función de la complejidad del dispositivo y del software que tenga instalado. En general, algunos orígenes de información lógica comunes son:

- Archivos de logs.
- Usuarios creados en el sistema.
- Historial de comandos del sistema.
- Procesos activos, junto con los recursos que los usan, usuarios o aplicaciones que los ejecutaron.

- Fechas y horas de de creación, modificación y acceso de los archivos.
- Integridad de los archivos del sistema.
- Puertos abiertos y aplicaciones asociadas.
- Direccionamiento de red.
- Ficheros ocultos o borrados.
- Configuración de seguridad del sistema.

Los analistas deberían también pensar en orígenes de **datos ubicados en otras localizaciones** más allá del entorno físico de la organización, como por ejemplo los logs de actividad de red del proveedor de servicio (ISP). Es necesario contar con que cada origen de datos tiene un dueño, por lo que hay que tener en mente las posibles acciones a tomar para adquirir la información de cada fuente. Por ejemplo, para solicitar los datos a un ISP sería necesario una orden judicial. En ocasiones, no será posible obtener los datos desde una fuente de manera directa, por lo que los analistas deberán considerar fuentes de datos alternativas que puedan contener algunos o la totalidad de los datos buscados y utilizar estas fuentes en lugar de la fuente directa.

5.1.2 ADQUISICIÓN DE DATOS

Tras la identificación de los orígenes de datos, los analistas deben proceder a la adquisición. La adquisición debe ser realizada mediante un proceso que contemple lo siguiente:

- Desarrollo de un plan de adquisición de datos.
- Adquisición de datos.
- Verificación de la integridad de los datos adquiridos.

Plan de adquisición de datos

El desarrollo de un plan para la adquisición de los datos es importante debido a que habitualmente existe una gran cantidad de orígenes de datos posibles. El analista debería crear un plan que **priorice las fuentes disponibles**, estableciendo un orden de adquisición.

A la hora de priorizar, es necesario tener en cuenta los siguientes factores:

- **Valor de la fuente:** Partiendo de la comprensión de la situación por parte del analista y su experiencia previa en situaciones similares, el analista debe ser capaz de estimar el valor de cada posible fuente de datos.

- **Volatilidad:** La volatilidad referida a los datos, se refiere a los datos que existen en un sistema en ejecución y se pierden tras ser apagado o por el paso del tiempo. La adquisición de los datos volátiles en un sistema deben tener prioridad sobre los no-volátiles.

- **Cantidad de esfuerzo requerido:** La cantidad de esfuerzo que se requiere para adquirir diferentes fuentes de datos puede variar ampliamente. El esfuerzo implica, no sólo el tiempo invertido por los analistas y otro personal del organismo (incluidos asesores legales) sino también el coste del equipamiento y los servicios (personal externo). Por ejemplo, la adquisición de datos de un servidor de la organización habitualmente requerirá menos esfuerzo que intentar conseguir los datos desde un ISP.

Considerando estos tres factores para cada potencial origen de datos, los analistas pueden tomar decisiones fundamentadas con respecto a la interiorización de la adquisición del origen de datos, así como determinar qué orígenes de datos tomar. En algunos casos existen tantas posibilidades para la adquisición de datos, que no es práctico adquirirlos todos. Las organizaciones deben considerar cuidadosamente las complejidades de la priorización en la adquisición de los orígenes de datos y desarrollar planificaciones documentadas, directrices y procedimientos que puedan ayudar a los analistas a realizar la priorización de manera eficiente.

Adquisición de datos

Para la adquisición de los datos, se seguirán una serie de pasos encaminados a recopilar posibles evidencias que permitan la determinación del método de entrada al sistema, la actividad de los intrusos, su identidad y origen y duración del compromiso. Es fundamental no alterar las posibles evidencias durante todo el proceso, por lo que habrá que hacer uso de las herramientas adecuadas.

En este punto será muy recomendable disponer de un registro en el que se recoja todo el detalles de las operaciones que se realicen sobre los sistemas bajo estudio. Cuanto más detalle, mucho mejor (imagine lo útil que puede resultar si se ve las caras con el presunto intruso en un juicio).

Una decisión importante a tomar es si los datos se van a recoger sobre el sistema apagado o funcionando. Para el caso de los datos volátiles (memoria RAM, caché, conexiones de red activas,procesos en ejecución, etc.), será casi imperativo que el sistema esté en funcionamiento. En el otro lado, imagine que el intruso está dentro del sistema. Si decide actuar en el sistema funcionando, el atacante podría detectar su actividad y reaccionar con una acción evasiva o destructiva, borrando todo tipo de huellas.

Lo ideal, para no perder detalle, sería realizar lo siguiente:

- Recopilar los datos volátiles
  - Registros y contenidos de la caché.
  - Contenido de la memoria RAM.
  - Estado de las conexiones de red y tablas de ruta.
  - Estado de los procesos en ejecución.

- La recolección de datos no-volátiles mediante su duplicado.
  - Contenido del sistema de archivos y de los discos duros.
  - Contenido de otros dispositivos de almacenamiento.

- Protección de los datos no-volátiles originales.

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.

Con respecto a los datos no-volatiles, su copiado se deberá realizar mediante una imagen de disco ya que es el método que copia bit a bit la información original preservando toda la información. Con un copiado estándar desde el propio sistema operativo se perdería mucha información.

Ahora se presenta otra cuestión. ¿Dónde almacenamos todos estos datos? En un lugar seguro, por supuesto. ¿Y dónde está ese lugar seguro? Una opción podrían ser discos duros externos USB. Otra sería emplear herramientas a través de la red, aunque se recomienda más el modo local. Sea como sea, se deberán usar dispositivos de almacenamiento **en modo sólo lectura** para no alterar la información a posteriori.

5.2 PRESERVACIÓN

Una vez contamos con toda la información que se ha considerado que puede contener las evidencias del incidente, el siguiente paso será **asegurar y etiquetar toda la información adquirida**. Es particularmente importante para un analista demostrar que los datos no han sido alterados ya que, por ejemplo, en un proceso judicial podrían provocar la invalidación de los mismos como evidencias.

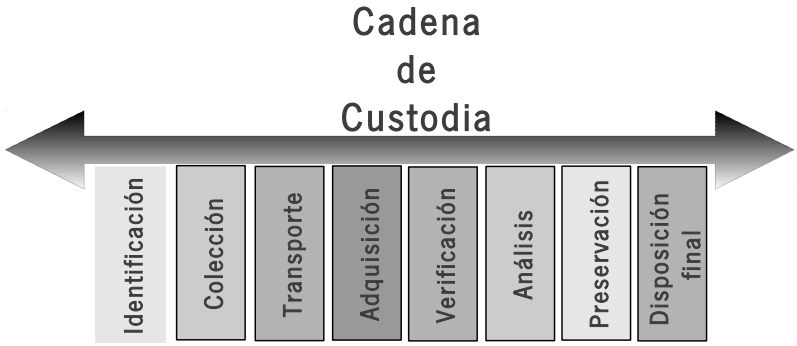
Esta fase está inevitablemente **condicionada por la legislación** bajo la que se esté trabajando.

Una recomendación a nivel global es realizar 2 copias de los datos, además del original. Cada una la etiquetaremos con información que permita comprobar su inalterabilidad y trazabilidad, como:

- Suma de comprobación (mediante función hash).
- Fecha y hora de la copia.
- Nombre de la copia.
- Persona que realizó la copia.

Se recomienda guardar la copia original aparte, bien asegurada, etiquetada, e incluso precintada.

Un aspecto de suma importancia y que está relacionado con lo anterior es el proceso conocido como **cadena de custodia**. En éste se establecen las responsabilidades y controles de cada una de las personas que manipulan la evidencia. El objetivo es documentar el traslado y posesión de los dispositivos digitales o medios de donde se obtuvo la información para la realización de la investigación, desde que inicia el proceso, durante la investigación y hasta que finalice el juicio o la investigación para garantizar que no exista contaminación, daño, alteración o manipulación de la evidencia y de esta forma mantener la confiabilidad en el proceso.

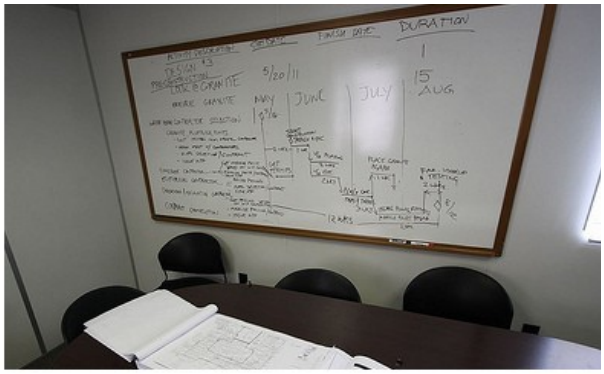


Algunos aspectos interesantes a documentar son:

- Dónde, cuando y quién manejó o examinó la evidencia.
- Información de los dispositivos de los cuales se realizaron copias digitales como números de serie, marcas, modelos, firmas digitales
- Nombre y firma con fecha de la persona que entrega el dispositivo original, así como de la persona que lo recibe.

5.3 ANÁLISIS

El objetivo es reconstruir, con toda la información extraída, 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.

5.3.1 PREPARACIÓN DEL ENTORNO DE TRABAJO

Antes de comenzar el análisis de las evidencias deberá acondicionar un entorno de trabajo adecuado al estudio que desee realizar. Si nos decantamos 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.

Como entorno de trabajo para el análisis, es recomendable preparar 2 estaciones de trabajo:

- **Estación de análisis**. Ésta se usará para el estudio de las evidencias recopiladas. Puede ser útil montar en este equipo 2 discos duros. Uno con un sistema operativo a nuestra elección que usaremos como anfitrión para trabajar con él, y otro donde volcar las imágenes del equipo bajo estudio.
- **Estación de pruebas**. Equipo con las mismas características que el atacado. La idea es utilizar este segundo equipo para realizar sobre él pruebas y verificaciones conforme vayan surgiendo hipótesis sobre el ataque.

Aunque no se recomienda, una opción es también conectar los discos duros originales del sistema atacado a una estación de trabajo independiente para intentar hacer un análisis "en caliente" del sistema. Se deberá tomar la precaución de **montar los dispositivos en modo sólo lectura**.

5.3.2 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 se recopilará la siguiente información sobre los ficheros:

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

Sin duda, ésta será la información que más tiempo llevará recopilar, pero será el punto de partida para el análisis. Podría ser interesante en este punto dedicar un poco de tiempo a preparar un script que automatizase el proceso de creación del timeline.

Para comenzar, se ordenarán los archivos por sus fechas MACD. 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 MACD 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.

Pensemos que se está buscando "una aguja en un pajar", por lo que se deberá ser metódico, llendo de lo general a lo particular. Por ejemplo, podríamos partir de los archivos borrados, intentando recuperar su contenido, anotando su fecha de borrado y cotejándola 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, podríamos continuar examinando en detalle los ficheros logs y de registros que ya se ojearon durante la recopilación de datos. Hay que buscar una correlación temporal entre eventos. 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.

También puede ser interesante buscar la creación de usuarios y cuentas extrañas sobre la hora que se piense que se inició el compromiso del sistema.

5.3.3 DETERMINANDO 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 que causó el agujero de seguridad y qué 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 una búsqueda de vulnerabilidades a través de Internet, emplee

Google o utilice páginas específicas donde encontrará perfectamente documentadas cientos de vulnerabilidades, como por ejemplo www.cvedetails.com

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.

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. 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).

5.3.4 IDENTIFICACIÓN DEL AUTOR DEL INCIDENTE

Si ya ha logrado averiguar cómo entraron en sus sistemas, ahora le toca saber quién o quienes 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. 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 de hacking ético para identificar a su atacante. Piense que si éste 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".

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 chats, visite estos lugares y verá lo que uno puede llegar a aprender.

Además de la IP origen del ataque, durante el análisis del sistema comprometido, nos habremos encontrado seguramente con más de un archivo malicioso dejado por los intrusos. En ocasiones, éstos muestran los nombres de los autores que lo han creado, lo cual puede ser útil para rastrear la persona o el grupo de delincuentes tras el ataque.

5.3.5 EVALUACIÓN DEL IMPACTO

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?. El artículo 44.3.h de la Ley Orgánica 15/1999,de 13 de Diciembre, de Protección de Datos de Carácter Personal indica lo siguiente:

"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 determine
...."

5.4 DOCUMENTACIÓN

Es muy importante ir documentando todas las actividades que se vayan llevando a cabo durante todo el procedimiento. Una vez concluida la investigación, con todos los hallazgos encontrados en el análisis se prepararán los informes correspondientes respaldados con evidencia robusta y confiable.

Existen informes que incluyen contenido altamente técnico o aquellos que sólo resaltan los aspectos más importantes de la investigación sin contener información muy técnica y en un lenguaje más cotidiano.

Lo más usual es desarrollar 2 modelos de informe:

- Informe técnico, con mucho detalle sobre el análisis realizado.
- Informe ejecutivo, que muestra un resumen a alto nivel de los resultados obtenidos.

6 PROBLEMAS HABITUALES

Durante la realización de un forense digital nos podemos encontrar diversos problemas, con diversas consecuencias. Algunos de los más habituales son los siguientes:

- Si la copia del dispositivo a analizar no ha sido formateada a bajo nivel previamente, puede que la información presente ruído, y de lugar a la invalidez del estudio. Es recomendable usar un dispositivo de almacenamiento nuevo, formatearlo a bajo nivel y etiquetar todos los dispositivos involucrados.
- En la fase de análisis e investigación, determinar el sujeto tras el incidente puede ser un problema, así como obtener pruebas válidas para demostrarlo.

- Complejidades técnicas y legales que dificultan el trabajo. Por ejemplo, a nivel legal podemos vulnerar alguno de los derechos fundamentales del individuo, con lo que podría presentar una denuncia. Además, al vulnerar un derecho fundamental (inviolabilidad de las comunicaciones, e-mail, sniffer, de las carpetas personales, etc.) podemos estropear toda la investigación e incluso podría acarrear consecuencias legales para el analista.
- Determinar la conexión entre la causa y el efecto.
- Si los relojes del sistema no están sincronizados (con NTP) se complicará obtener la línea de tiempo y la trazabilidad hasta el origen del incidente.

7 BENEFICIOS DEL ANÁLISIS FORENSE EN UNA ORGANIZACIÓN

Durante la pasada década, el incremento de delitos relacionados con los sistemas de información ha crecido exponencialmente, estimulando un incremento de compañías y productos focalizados en ayudar a los cuerpos de seguridad a la hora de determinar el quién, el qué, el dónde, el cuándo y el cómo de los incidentes. Como resultado de todo esto, los métodos de análisis forense digital han evolucionado para asegurar una correcta presentación de los datos probatorios de delitos informáticos ante un tribunal.

Es muy común pensar que las herramientas y técnicas forenses son usadas exclusivamente en un contexto de investigación criminal y/o a la hora del gestionar incidentes de seguridad. Sin embargo, las técnicas y herramientas forenses pueden ser útiles en otros tipos de tareas, como por ejemplo:

- **Solución de problemas de la operatoria del servicio:** Muchas de las técnicas y herramientas forenses pueden ser aplicadas a solucionar problemas de tipo operativo, como encontrar la localización virtual y física de un equipo con una configuración de red incorrecta, resolver problemas de aplicaciones o grabar y revisar las configuraciones del sistema operativo y la configuración de las aplicaciones actuales para un sistema.
- **Monitorización de logs:** Muchas de las herramientas pueden ser usadas para analizar y correlacionar entradas de logs de distintos sistemas. Esto puede ser de ayuda a la hora de gestionar incidentes de seguridad, identificar violaciones de políticas, auditorías, etc.
- **Recuperación de datos:** Existen diferentes aplicaciones para recuperar datos eliminados de los sistemas que son usados en procedimientos forenses y que pueden ser de extrema utilidad para poder acceder a datos que hayan podido ser borrados por accidente o a propósito.
- **Obtención de datos:** Algunas organizaciones utilizan herramientas forenses para obtener la información de equipos que se encuentran siendo retirados o redistribuidos. Por ejemplo, se puede querer obtener y almacenar los datos de los sistemas de un usuario que deja la organización por si son útiles en el futuro. Dichos sistemas pueden ser reinstalados y redistribuidos posteriormente.
- **Cumplimiento normativo:** Con la creación de nuevas normativas y regulaciones, nace la necesidad para las organizaciones de proteger la información sensible y mantener ciertos registros para fines de auditoría. Además, cuando la información es expuesta a terceros, las organizaciones pueden ser obligadas a notificar a otras agencias o personas afectadas. Los métodos forenses

pueden ayudar a las organizaciones actúen con la debida diligencia y a cumplir con los requisitos exigidos.

Por tanto, para casi cualquier organización tener la capacidad de realizar análisis forenses de red y sistemas informáticos resulta extremadamente útil, ya que de no ser así pueden presentarse dificultades a la hora de determinar que eventos han ocurrido dentro de sus sistemas que administra.

Es necesario puntualizar que no es necesario contar con un equipo permanente para estas cuestiones. Algunas organizaciones son capaces de realizar tareas estándar de análisis forense (interpretación de logs, obtención de datos, etc...) contratando los servicios a terceros en el caso de que se necesite asistencia muy especializada ya que en ocasiones se hace necesario requerir de programas, hardware o procedimientos especializados. Las organizaciones deberían determinar de antemano qué tipos de incidentes deberían requerir acciones por parte de los agentes de la autoridad, así como de consultoría o testimonio de expertos externos (por ejemplo, en los procedimientos legales).

A la hora de determinar si un análisis forense (o parte de este) es realizado por partes internas a la organización o externas a ella, se deben tener en cuenta los siguientes aspectos:

- **Coste:** Contratar equipo técnico especializado puede parecer caro, sin embargo, es necesario pensar que para realizar ciertos tipos de análisis, puede ser necesario realizar una importante inversión en equipamiento y programas especializados, así como en formación para los técnicos que vayan a realizar el análisis. En general, las acciones que son poco frecuentes pueden realizarse de manera más rentable por un equipo externo mientras que las acciones que se necesitan con frecuencia puede ser más rentable realizarlas internamente.
- **Tiempo de respuesta:** Habitualmente, un equipo localizado en las mismas dependencias de la organización tiene la capacidad de comenzar más rápidamente la actividad forense que un equipo externo. Sin embargo, si la organización es geográficamente dispersa, los equipos externos cercanos a la localización en cuestión podrían ser capaces de responder de manera más rápida que el personal localizado en otra sede de la organización.
- **Confidencialidad de los datos:** Debido a las preocupaciones de confidencialidad y la privacidad de los datos, muchas organizaciones son reacias a permitir que equipos externos tengan acceso a ciertos datos importantes. Es necesario tener en cuenta que siempre depende del caso en cuestión, por ejemplo, si se trata de información financiera o estratégica de la empresa, es lícito pensar que la organización quiera tenerla bajo control, sin embargo, si se sospecha que el incidente pueda haber sido realizado por alguien del equipo técnico interno, podría ser útil realizar las acciones forenses externamente.

8 CONCLUSIONES

Las organizaciones deberían contar con la capacidad de llevar a cabo un proceso a análisis forense digital. Es necesario para la investigación de delitos, comportamiento inapropiado, reconstrucción de incidentes de seguridad, solución de problemas y recuperación de información y material dañado. El manejo de evidencias de una forma correcta abre la posibilidad a tomar decisiones basándose en ellas.

Mediante el análisis forense de un incidente de seguridad será posible:

- Descubrir el origen y el autor del ataque.
- Descubrir vulnerabilidades que han hecho posible el ataque.
- Identificar y determinar las acciones realizadas y las herramientas y métodos utilizados en el ataque.
- Determinar medidas adecuadas para que la situación no se repita.

La capacidad de realizar tareas forenses enriquece la gestión de incidentes de seguridad ya que se trata de un proceso que permite investigar con gran profundidad los incidentes de seguridad y dar respuesta a la múltiples incógnitas que se presentan alrededor de un incidente.

Los análisis forenses constituyen una herramienta indispensable que toda organización debe contemplar dentro de su política de seguridad. Para maximizar la eficiencia de la investigación, las organizaciones deberían estar preparadas para proporcionar a los analistas forenses cualquier tipo de información relevante que se pueda necesitar.

9 REFERENCIAS

- Guide to Integrating Forensic Techniques into Incident Response. NIST. 2006
- Un forense llevado a juicio. Jesús Luis García Rambla. 2012
- First Responders. Guide to Computer. Forensics. CERT. 2005
- Computer Forensics. Part 1: An Introduction to Computer Forensics. ISFS. 2004
- Forensics Wiki
- Linux Forensics Tools Repository
- Hacking Exposed Computer Forensics, Second Edition: Computer Forensics Secrets & Solutions. Aaron Philipp. 2009 McGrawHill.