Autor:
Xombra
www.xombra.com

El mundo de la Informática Forense

(Capitulo I)

La ciencia forense es sistemática y se basa en hechos premeditados para recabar pruebas para luego analizarlas. La tecnología, en caso de análisis forense en sistemas informáticos, son aplicaciones que hacen un papel de suma importancia en recaudar la información y pruebas necesarias. La escena del crimen es el computador y la red a la cual éste está conectado. Gran cantidad de documentos son elaborados digitalmente en computadores para ser a continuación impresos.

Las nuevas leyes sobre delitos informáticos y la de firmas electrónicas y mensajes de datos abren procesalmente y definitivamente los medios probatorios informáticos. Las operaciones comerciales tienden claramente a reducir costos y ampliar mercados a través de las redes informáticas.

Ya se han producido algunas experticias en Venezuela (Proyecto de Ley de Delitos Informaticos en Venezuela) y otros países de habla hispana uno de los más destacados es España, en las cuales se ha solicitado la determinación de la autenticidad e integridad por ejemplo de mensajes de e-mail pudiéndose relacionar con un remitente, dirección de correo, computador y hasta con una persona determinada e inclusive la relación entre estos elementos y los datos anexos (attachments) que se encontraban en el email almacenado previamente en el equipo incurso.

Es posible investigar (aún cuando internet permite el anonimato y el uso de nombres falsos) quien es el dueño de sitios web, quienes son los autores de determinados artículos y otros documentos enviados a través de redes o publicados en la misma. El rastreo depende en sí de quien y como realizó el ataque o cualquier otra acción, es posible buscar atacantes exteriores de sistemas e incluso se conocen casos donde se ha determinado la autoría de virus.

Son igualmente investigables las modificaciones, alteraciones y otros manejos dolosos de bases de datos de redes internas o externas, así como de cualquier sistemas de redes, ataques internos. Por supuesto, para realizar esta fragosa tarea se debe poseer un conocimiento sólido (normalmente quienes hacen de Informáticos forenses han realizados ataques anteriormente o conocen el uso de herramientas, dispositivos y software de incursión en redes, por lo que tienen una idea de las posibles intrusiones por parte de terceros en un sistema).

La destrucción de datos y la manipulación de los mismos también pueden rastrearse. Los hábitos de los usuarios de los computadores y las actividades realizadas pueden ayudar a la reconstrucción de hechos, siendo posible saber de todas las actividades realizadas en un computador determinado.

Los archivos informáticos pueden guardar información sobre su autor, la compañía, fecha y otros datos de interés jurídico. Esta información es almacenada a espaldas del usuario pudiendo determinarse en algunos casos en que computador/estación fue redactado el archivo (esto es poco fiable, ya que cualquier otra persona pudo trabajar con la pc, falsificando la identidad del usuario propietario de la estación, pero es usado como base del procedimiento).

Las imágenes digitales y otros medios audiovisuales pueden estar protegidos no solo por derechos

de autor (copyright) sino por las llamadas marcas de agua digitales que servirían para determinar el origen del archivo aunque hayan sido modificados para disfrazarlos y darle una apariencia distinta.

Ya son frecuentes las inspecciones judiciales sobre páginas Webs y archivos, tendientes a la fijación de hechos que ocurren dentro del vasto mundo electrónico digital.

La promoción, evacuación y control de estas experticias informáticas es especial y bajo las normas de naciente, pero desarrollada informática forense que se pone al servicio inmediato del derecho para afrontar nuevas tareas probatorias y lo más importante es que ya se puede contar en Venezuela y en otros países con este tipo de pericias útiles en los procesos judiciales del presente y del futuro.

El objetivo de un análisis forense informático es realizar un proceso de búsqueda detallada y minuciosa para reconstruir a través de todos los medios el log de acontecimientos que tuvieron lugar desde el mismo instante cuando el sistema estuvo en su estado integro hasta el momento de detección de un estado comprometedor.

Esalabor debe ser llevada acabo con máxima cautela y de forma detallada, asegurándose que se conserva intacta, en la medida posible, la información contenida en el disco de un sistema comprometido, de forma similar que los investigadores policiales intentan mantener la escena del crimen intacta, hasta que se recogen todas las pruebas posibles.

Juan Carlos Guel, jefe del Departamento de Seguridad en Cómputo de la Dirección General de Servicios de Cómputo Académico y Coordinador del Equipo de Respuesta a Incidentes en Seguridad en Cómputo UNAM-CERT (no estoy al tanto que aún posea este cargo), señala: “informática o cómputo forense es un conjunto de técnicas especializadas que tiene como finalidad la reconstrucción de hechos pasados basados en los datos recolectados, para lo cual se procesa la información que pueda ser usada como evidencia en un equipo de cómputo”.

Es decir, el cómputo forense opera diversas herramientas informáticas para determinar el estado de un sistema luego de que sus medidas de seguridad han sido sobrepasadas y vulneradas, con la finalidad de encontrar evidencias que permitan definir, con toda certeza, los mecanismos que los intrusos utilizaron para acceder a ella, así como de desarrollar las mejoras y/o técnicas que deben seguirse para evitar futuras incursiones ajenas en el sistema.

En una entrevista realizada por virusprot al Doctor Jeimy J.Cano, Ingeniero de Sistemas y Computación Universidad de los Andes (Colombia) en el año 2002, y cito textualmente:"¿Cuánto se puede tardar en reunir las suficientes pistas que den con el autor de un ataque?
Es una pregunta complicada de responder, pues muchas veces el informático forense debe prepararse para fallar en la identificar la persona real que cometió el ataque. Pues la versatilidad que ofrece Internet para enmascarar direcciones IP, correos electrónicos, entre otros aspectos, sugiere un gran conocimiento técnico y paciencia por parte de los atacantes, los cuales también consideran estrategias "anti-forenses" que limiten las investigaciones y la efectividad de las mismas. Luego, la recolección de pista puede ser demorada, algunos casos pueden llevar años en esta labor."

Las herramientas que utilizan los peritos forenses en materia de cómputo para dar con los intrusos, y saber a ciencia cierta qué hicieron en el sistema, se han desarrollado al paso del tiempo, para que nos ayuden en cuestiones de velocidad y faciliten identificar lo que realmente le pasó al sistema y qué es lo que le puede suceder, en su contra parte igualmente se han desarrollado herramientas bastantes sofisticadas en contra de los análisis forenses (herramientas y técnicas que intentan no dejar rastros, camuflarlos o borrarlos, de tal manera que se dificulte una posterior investigación.), tal como lo indica el Dr. Jeimi Cano.

De allí el personal que labore en la informática forense deberá poseer sólidos conocimientos

técnicos y prácticos y conocer las herramientas de uso, estar al día en bugs (vulnerabilidades) de sistemas (Sistemas operativos, software y hardware)

El campo de la seguridad informática es inmensamente heterogéneo e interesante. Analizar un entorno atacado y comprometido es un desafiante ejercicio de aplicación de ingeniería inversa, para el cual es necesario tener gran conocimiento del funcionamiento de los sistemas involucrados, las técnicas de ataque y los rastros que dejan las mismas.

Se puede leer en diferente sitios web notas similares a estas: "Espero que los nuevos empleados tengan un mínimo de conocimientos de informática y software forense antes de que lleguen a la puerta", apunta Marc Kirby, detective inspector para la sección de informática forense de la británica Unidad Nacional de Crimen de Alta Tecnología (NHTCU)". Saque sus conclusiones de ese párrafo.

Debemos tener en cuenta que la prioridad es preservar lo más íntegramente posible las evidencias del crimen en un estado íntegro. Eso significa colocar el sistema fuera de servicio (offline) cuando todos los usuarios del sistema están presionando para volver a ponerlo on-line.

Sí el sistema, por parte del administrador, fue forzado a seguir funcionando, eliminando las posibles vulnerabilidades o cualquier otra supuesta vía de acceso al servidor, la investigación forense no podrá seguir el rumbo correcto ya que:

1. Se eliminaría cualquier posibilidad de persecución del intruso en un futuro ya que se modifica la "escena del crimen" y no se podría calcular los daños estimados con un grado elevado de certeza.

2. Hay muchas posibilidades de que se le paso algo importante por alto al administrador y el intruso (o intrusos) siguen teniendo acceso al sistema. Por lo tanto es mejor sufrir un "downtime" de red, mientras que se realiza el análisis forense del sistema.

Se tiene que establecer una prioridad entre:

(a) Funcionamiento inmediato, teniendo presente que las huellas dejadas por el/los intruso(s) pueden haberse eliminado por descuido del administrador y su equipo, y que el servidor puede seguir teniendo puertas traseras bien ocultas. Esta opción permite estar operativo en poco tiempo.

(b) Investigación forense detallada. Esta opción supone un mayor tiempo de permanencia offline sí no existen planes de contingencia y procedimientos para el backup del servicio.

Bases de la Informática Forense:
1. Experticias, Auditoria e Inspecciones en Computadores y Páginas Web.
2. Ubicación de origen de correos anónimos y archivos anexos.
3. Determinación de propietarios de Dominios .com .net .org y otros.
4. Pruebas de violación de derechos de autor.
5. Control preventivo y restricción de uso de computadores e Internet.
6. Protección de información y derechos de autor.
7. Recuperación de data y archivos borrados intencionalmente o por virus.
8. Recuperación y descifrado de las claves.

Al realizar un análisis de informática forense es necesario tomar notas de lo que se hace con el disco duro, y a que hora, almacenándolo en una ubicación segura como por ejemplo una caja fuerte. Es recomendable que siempre que se trabaje con el medio original esté acompañado por un colega, para que conste a los efectos legales y el testimonio pueda ser confirmado por alguien con un nivel

de conocimientos similar.

Las copias deben ser hechas bit-por-bit, es decir será necesario hacer imágenes del disco. La investigación debe ser llevada sobre una copia y nunca sobre el disco original. Se debe hacer tres copias del disco duro original. Sobre todas las copias y original se debe llevar acabo una verificación criptográfica - un checksum. En lo posible realizar dumps de memoria y almacenarlos al igual que los discos.

Es importante todos los hechos pertinentes al caso durante la preparación, recuperación y análisis de las pruebas sobre un ataque sean anotados para poder desarrollar un informe detallado de incidencia que se debe preparar una vez terminado el análisis. Este documento deberá servir como una prueba del incidente o compromiso. Siempre que se realiza cualquier apunte al cuaderno, el asistente debe tener completo conocimiento y entendimiento de lo que ha sido apuntado.

Antes de apagar el sistema, será útil recoger algunos ejemplos de aquella información que posiblemente no ha sido cambiada por los intrusos, como la organización de sistema de ficheros logs, el nombre del host, su dirección IP del fichero e información de algunos dispositivos.

El análisis de la comunicación de datos es realmente importante allí se trabajaran en dos actividades:

1. Intrusión en una red de computadoras o mal uso de la misma.
2. Interceptación de datos.

La intrusión en una red de computadoras o mal uso de la misma es la actividad de la informática forense principal cuando el análisis se hace sobre estructuras de esta naturaleza. Consiste en las funciones siguientes:

a) Detección de la intrusión.
b) Detectar la evidencia, capturarla y preservarla; y
c) Reconstrucción de la actividad específica o del hecho en sí.

El descubrimiento de la intrusión generalmente involucra la aplicación de software especializado y en algunos casos hardware, para supervisar la comunicación de los datos y conexiones a fin de identificar y aislar un comportamiento potencialmente ilegal.

Este comportamiento incluye el acceso no autorizado, modificación del sistema en forma remota y el monitoreo no autorizado de paquetes de datos.

La captura de la evidencia y su preservación, generalmente tiene lugar después del descubrimiento de una intrusión o un comportamiento anormal, para que la actividad anormal o sospechosa pueda conservarse para el posterior análisis.

La fase final, la reconstrucción de la intrusión o comportamiento anormal, permite un examen completo de todos los datos recogidos durante la captura de la evidencia.

Para llevar a cabo con éxito estas funciones, el investigador forense debe tener experiencia en comunicación de datos y el apoyo de ingenieros y/o técnicos de software.

Antes de realizar un análisis se debe tener en cuenta la siguiente información:
a) sistema operativo afectado.
b) inventario de software instalado en el equipo
c) tipo de hardware del equipo
d) accesorios y/o periféricos conectados al equipo
e) si posee firewall
f) si esta en el ámbito del DMZ (Zona desmilitarizada)

g) conexión a internet
h) configuración
i) parches y/o actualizaciones de software
j) políticas de seguridad implementadas
k) forma de almacenamiento de la información (cifrada o no)
l) personas con permisos de acceso al equipo
m) el pc esta dentro del DMZ
n) existe IDS
o) cuantos equipos en red

Recomiendo como lectura interesante a:
Sistemas de Detección de Intrusiones de Diego González Gómez
http://www.dgonzalez.net/pub/ids/html/

Interesante artículo enviado por Antonio Javier G.M.
http://www.analisisforense.net/SIC59_074-084.pdf

Algunos Software/herramientas aplicables en la informática forense:

. F.I.R.E.: Destaca dentro de las distribuciones linux específicas para informática forense
Sitio web: http://biatchux.dmzs.com

. WinHex: Software para informática forense y recuperación de archivos, Editor Hexadecimal de Archivos, Discos y RAM
Sitio web: http://www.x-ways.net (shareware)

. Encase: Herramienta propietaria, la cual ha demostrado ser un dispositivo útil a los peritos forenses en diferentes casos.
sitio web: http://www.guidancesoftware.com/

. Snort Herramienta libre por excelencia una de las mejores
Sitio web: http://www.snort.org

. Ossim: Herramienta de monitorización
Sitio web:http://www.ossim.net

. Ettercap: Excelente sniffer de redes
Sitio web: http://ettercap.sourceforge.net/

. NMap: Potente localizador de vulnerabilidades
Sitio web: http://www.insecure.org/nmap/

. Nessus: Otro proyecto para scanear vulnerabilidades
Sitio web: http://www.nessus.org

. Ethereal: Otro potente sniffer
Sitio web: http://www.ethereal.com

.Fport: Identifica puertos abiertos y aplicaciones asociadas a ellos.
Sitio web: http://foundstone.com/

. putty: Escelente cliente SSH
Sitio web: http://www.chiark.greenend.org.uk/~sgtatham/putty/

. Stunnel: Programa que cifra las conexiones TCP bajo SSL
Sitio web: http://www.stunnel.org/

. AirSnort: Herramienta wireless para recuperar claves cifradas
Sitio web: http://airsnort.shmoo.com/

. Aircrack: sniffer y WEP craqueador de wirless
Sitio web: http://www.cr0.net:8040/code/network/
Stio web: http://www.xombra.com/descargas.php?cat=7
http://www.xombra.com/descargas.php?cat=7
. Achilles: Herramienta para testear la seguridad de las aplicaciones web
sitio web: http://www.mavensecurity.com/achilles

. NetStumbler Localizador de los puntos de acceso wirless (debes poseer tarjeta wirless para q funcione)
Sitio web: http://www.stumbler.net/

.Dsniff: sniffer
Sitio Web: http://www.datanerds.net/~mike/dsniff.html

.VNC Administrador remoto
Sitio web: http://www.realvnc.com/

.The Autopsy: Browser para la informatica forense
Sitio web: http://www.sleuthkit.org

.PyFlag: Herramienta para recuperar discos en RAID
Sitio web: http://pyflag.sourceforge.net/

Herramientas Microsoft:
. Promqry 1.0 (linea de comandos, 113 KB):
http://download.microsoft.com/download/b/b/6/bb6ea193-2880-43c3-b84b-b487a6454a17/promqrycmd.exe

. PromqryUI 1.0 (interfaz gráfico, 255 KB):
http://download.microsoft.com/download/7/2/6/7262f637-81db-4d18-ab90-97984699d3bf/promqryui.exe

Sitios web de seguridad (recomendados)

http://www.kb.cert.org
http://www.securityfocus.com
http://www.sqlsecurity.com
http://www.secunia.com
http://www.securitytracker.com
http://www.forensicfocus.com/
http://www.frsirt.com
http://www.infohackers.org
http://www.hispasec.com
http://www.seguridad0.com
http://www.forensic-es.org
http://www.synacksecurity.com

Fuentes consultadas:
tecnoiuris.com

informaticaforense.com
criptored.upm.es
loquefaltaba.com
grafotecnica.com
virusprot.com
obm.corcoles.net
dgonzalez.net
vnunet.es
unam-cert.unam.mx
alfa-redi.org
ausejo.net
symantec.com
pandasoftware.com
monografias.com
criminalista.net
delitosinformaticos.com
hispasec.com
synacksecurity.com
unmanarc.synacksecurity.com