INFORMÁTICA FORENSE

Bonilla Pérez, Diana Marcela - Sierra Rodríguez, Leonardo
dianabon87@gmail.com
lsierrarodriguez@gmail.com
Universidad Piloto de Colombia

Resumen - Hoy en día se busca garantizar la protección de la información, teniendo en cuenta que es uno de los activos fundamentales en muchas compañías a nivel mundial.

Actualmente las organizaciones están siendo afectadas por el constante reporte y explotación de vulnerabilidades; asimismo, el aprovechamiento de las fallas humanas, tecnológicas y la no adecuada ejecución de los procedimientos que pueden comprometer la infraestructura tecnológica y la información, generando un escenario propicio para que los intrusos informáticos utilicen diferentes técnicas y estrategias que muchos ingenieros, especialistas y consultores desconocen teniendo en cuenta que los ataques en los sistemas siempre varían de un caso a otro. [1]

Debido a la importancia de la información y las pérdidas que pueden ocasionar para una empresa, nació la Informática Forense, que es la aplicación de técnicas científicas y analíticas que se especializan en la infraestructura tecnológica para Identificar, preservar, analizar y presentar datos que sean válidos en un proceso legal. [2]

Abstract - Today it seeks to ensure the protection of information, considering that is one of the key assets in many companies worldwide.

Currently the organizations are being affected by the constant reporting and vulnerability exploitation; also leveraging human failings, inadequate technological and implementation of procedures that can compromise and information technology infrastructure, creating a scenario for the Hackers use different techniques and strategies that many engineers, specialists and consultants know considering that the attacks on systems always vary from case to case. [1]

Because of the importance of information and can cause losses for a company, Computer Forensics born, which is the application of scientific and analytical techniques that specialize in technology infrastructure to identify, preserve, analyze and present data that are valid in a legal proceeding. [2]

Índice de Términos - Incidente, Información, Informática Forense, Seguridad.

I. INTRODUCCIÓN

El análisis forense es una rama de la seguridad informática que surge a raíz del incremento de los diferentes incidentes, fraudes y eventos de seguridad. El análisis forense busca averiguar lo ocurrido por acciones no autorizadas que se producen en una compañía, se identifican los posibles autores, causas, y métodos empleados con los cuales se trata de reconstruir como han penetrado o vulnerado el sistema. Por tanto, lo que se quiere es dar respuesta a los interrogantes que nacen cuando se presenta un incidente permitiéndonos responder preguntas tales como:

- ¿Quién realizo el ataque?
- ¿Cómo se realizó?
- ¿Desde dónde?
- ¿Cuándo se realizó el ataque?
- ¿Para que se realizo el ataque?
- ¿Por qué se realizo el ataque?
- ¿Cuáles fueron las Vulnerabilidades que se explotaron?[3]

El Análisis Forense comprende de dos fases, la primera es recolección de las evidencias y su protección, la segunda es el análisis y la metodología empleada para obtener la máxima información sin alterar los datos originales.

II. INFORMÁTICA FORENSE

Fig. 1 Polígrafo Medellín

La Informática Forense es el proceso de extracción de información relevante almacenada en dispositivos electrónicos como computadores portátiles, teléfonos móviles, discos duros, memorias extraíbles, correos electrónicos o servidores, con el fin de analizar información disponible, borrada u ocultada que pueda ser utilizada cuando se han perdido datos por fallas accidentales o en un proceso judicial, respetando el marco legal existente y los derechos fundamentales de las personas implicadas

Cuando se presenta una investigación, el responsable que realiza esta actividad debe tener en cuenta el reporte inicial, como recibimos la información si es una fuente formal o no formal, cuales son los objetivos frente a la investigación, formular un problema y realizar una serie de preguntas (modo, lugar tiempo), plantear una hipótesis para saber que paso y sustentar con más información, definir actividades a realizar (Modelo Cualitativo y modelo Cuantitativo)

Adicionalmente el especialista en informática forense se encarga de recolectar la evidencia digital utilizando herramientas y procedimientos adecuados (recolección de datos volátiles, volcamiento de memoria, metadatos entre otros) para garantizar que los datos extraídos se puedan utilizar como evidencia para los casos de delitos informáticos o para otro tipo de crimen. [4].

El especialista en informática forense debe:

- Recolectar la evidencia de forma rápida, segura, eficiente y precisa.
- Realizar imágenes forenses (mínimo dos copias y siempre debe sacar el hash (huella digital del archivo).
- Recuperar de manera parcial o total los datos que han sido borrados, alterados o sobrescritos.
- Analizar la evidencia para determinar el origen y contenido de la información y su valor probatorio.

Presentar apropiadamente la información ante un ente judicial de tal modo que se pueda aplicar la ley que tipifica los delitos informáticos.

III. NECESIDAD DE INFORMATICA FORENSE

Fig. 2 Informática Forense

Hoy en día las compañías ven la necesidad de la informática forense debido a los avances tecnológicos (internet) y la propagación de dispositivos electrónicos los cuales van acompañados de una alta tendencia de delitos informáticos.

La informática forense se ha vuelto vital ya que muchas veces los dispositivos son vulnerados sin que el sin que el dueño se dé cuenta en donde posteriormente se puede presentar pérdida o robo de información ocasionando grandes pérdidas económicas y de imagen corporativa.

Por esta razón la Informática Forense se utiliza ya que ayuda a esclarecer los hechos y maneja herramientas en hardware y software especializado que emplea las medidas de seguridad correspondientes con el fin de encontrar y restaurar evidencia más rápido y con más exactitud logrando garantizar la integridad de los mismos [5]

IV. III EVIDENCIA DIGITAL

Fig. 2 Evidencia Digital

Actualmente la demanda y utilización de dispositivos digitales generan gran cantidad de información como una fotografía, registro de geo localización GPS, documento, mensaje de texto, correo electrónico o incluso un número telefónico registrado como parte de una llamada, pueden llegar a convertirse en una evidencia útil de una investigación correspondiente a incidentes de seguridad relacionados con actividades cibercriminales o de ataques informáticos. [6]

La mayoría de las empresas no están debidamente preparadas para atender de manera oportuna incidentes de seguridad, que puedan comprometer la confidencialidad, integridad y disponibilidad de la información, teniendo en cuenta los altos costos que presentan para la compañía, y a la poca experiencia y nivel de conocimiento requerido para la adquisición, preservación, análisis y presentación de la evidencia.

Generalmente las personas implicadas en los incidentes buscan alterar la evidencia digital tratando de borrar cualquier rastro en el cual se pueda detectar el daño ocasionado.

La evidencia digital es el input que genera la investigación y la revisión de las diversas evidencias las cuales se pueden categorizar en:

- Registros almacenados en el equipo de tecnología informática, Por ejemplo E-mail, archivos de ofimática, imágenes, entre otros
- Registros generados por los equipos de tecnología informática, logs de auditoría, transacciones o de eventos etc.
- Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática, hojas de cálculo, consultas especializadas en bases entre otros.

Sin embargo hay que tener en cuenta que se debe manejar un vasto conocimiento en las regulaciones jurídicas y legales que concierne a la investigación basada en evidencia digital [7]

V. PRIMERA RESPUESTA

Fig. 3 Campus Party

1. Fijación de la escena – para el investigador su prioridad es preserva la zona de pruebas físicas tradicionales (huellas digitales, etc.); el dispositivos como por ejemplo (Discos duros, USB, Celulares, etc.) y fuentes de evidencia digital, restringiendo el acceso a estos.

2. Si el computador está apagado, no se debe encender ya que se deber tener un entrenamiento adecuado.

3. Si el equipo está prendido, el especialista antes de realizar cualquier acción debe verificar los procedimientos y metodologías a aplicar, ya que un procedimiento inadecuado puede causar daños al sistema y crear responsabilidad por parte del investigador o funcionario.

4. Se debe fotografiar o grabar videos asegurando que todas las partes del equipo de computo sobre todo las conexiones son fotografiadas, siempre se debe documentar todo lo que se realice en la escena.

5. Si el equipo es un Windows o Macintosh. (No-Unix, Linux o Server), desconecte el cable de alimentación de la parte posterior del equipo. NO apague el interruptor de encendido, esto va a cambiar los datos críticos. Los sospechosos pueden haber conectado el interruptor de alimentación para destruir los datos.

6. Coloque cinta adhesiva en todas las ranuras de las unidades y la caja de la evidencia.

7. Use bolsas antiestáticas y protección de los campos magnéticos. NO la transporte cerca de equipos electrónicos o radios [8].

VI. ADQUISICION DE DATOS

Fig. 4 Adquisición y Análisis de la Evidencia.

Se debe tener en cuenta que cualquier prueba puede ser contaminada, por lo tanto es recomendable realizar como mínimo dos (2) imágenes forenses del medio a investigar, con el fin de poder conservar la integridad de la información y garantizar que corresponde a la imagen original, se debe generar el hash (huella digital del archivo), bloquear los medios de almacenamiento antes de realizar el análisis respectivo, asegurando que la información no sea alterada, borrada o modificada. [9]

La recolección de la evidencia la podemos efectuar de dos maneras:

- Cuando una maquina este encendida (en caliente) es el momento más apropiado para extraer la información teniendo en cuenta los datos almacenados de manera temporal

Cuando la maquina está apagada (en frio) se puede realizar una copia bit a bit, para analizar el contenedor y poder extraer los datos requeridos

Es de aclarar que siempre se debe calcular el valor del hash, utilizando herramientas adecuadas tales como MD5, SHA-1 y SHA-2, ya que nos permite identificar de manera posterior si el archivo ha sido modificado debido a que el hash debe ser el mismo si el archivo no ha sufrido algún tipo de alteración.

VII. ANÁLISIS

Después de recolectar la evidencia que es la fase en que el investigador le debe dedicar su mayor esfuerzo teniendo en cuenta lo extensa e importante para presentar los mejores resultados, en el análisis de los datos obtenidos el investigador se fundamenta en su conocimiento y percepción del entorno tecnológico actual con el fin de identificar la evidencia relevante que pueda ayudar a esclarecer los hechos [10]

Fig. 5 Análisis Forense.

Para realizar un buen análisis se debe contar con un check list que garantice.

- Geometría del disco
- Recuperación de archivos que tengan estructura.
- Data carving (Archivos sin estructura)
- File mounter (montaje de archivos)

- Descifrar archivos que tengan contraseñas cifradas, esteganografia etc.
- Reconstruir archivos de impresión relacionados con la papelera
- Búsqueda de palabras clave
- Ejecutar antivirus, análisis de huella y hash

VIII. INFORME

El experto en informática forense quien realizo la investigación, es el custodio de su propio proceso, por lo tanto cada paso realizado, las herramientas utilizadas deben estar especificadas en el informe (versiones, licencias y limitaciones), se detalla cada paso y a su vez se especifican datos de gran importancia como la hora, fecha, nombres de archivos, entre otros, se describen los hallazgos y la cronología de los hechos.

La eficacia de este informe se basa fundamentalmente en la continuidad del aseguramiento de la evidencia, siendo objetivo y preciso, documentando todo el proceso forense sin omitir información ya que si se presenta alguna confrontación en las evidencias estas pueden ser eliminadas en un proceso jurídico por no contar con la integridad correspondiente.

IX. CONCLUSIONES

La informática forense nos permite esclarecer los hechos o los delitos informáticos mediante el conocimiento y con la ayuda de herramientas forenses.

Es importante documentar cada paso realizado con la evidencia digital ya que se garantiza la integridad de la misma y sirva como elemento probatorio ante el ente judicial.

Se debe utilizar herramientas apropiadas para la extracción de los datos analizados, siempre se debe manejar una metodología alineada con los estándares que regulen la informática forense.

Las organizaciones deben conocer la tendencia en el incremento de los ataques informáticos teniendo en cuenta los avances tecnológicos a nivel mundial y tomar decisiones para incrementar la seguridad de la información y contar con un plan de acción que le permita atender de forma oportuna y eficiente en caso de presentarse un incidente de seguridad.

REFERENCIAS

[1] C. Jeimy, "*Introducción a la informática Forense"* [En Línea]. Disponible en: Http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

[2] G. A. Luis, Titulo. "*La informática forense, una herramienta para combatir la ciberdelincuencia*" Oct 1999, [En Línea]. Disponible: http://www.minseg.gob.ar/download/file/fid/893

[3] [8] L. R. Jose, (Sep. 2009) Titulo. "*Análisis forense de sistemas informáticos"* (1ra ed.) [En Línea]. Disponible en: http://webs.uvigo.es/jlrivas/downloads/publicaciones/Analisis%20forense%20de%20sistemas%20informaticos.pdf

[4] (Blog En Línea) (2008, Jun 27) Titulo. "*Informática Forense"*, Disponible en: http://www.informaticaforense.com/criminalistica/categoryblog/69-que-es-la-informatica-forense

[5] (Blog En Línea) (2011, Sep. 3) "*Informática forense como una disciplina"*, Disponible en: http://www.informaticaforense.com.co/index.php?option=com_content&view=article&id=46&Itemid=53

[6] M. Roberto, (2012, Abr 24) "*La importancia de la evidencia y el análisis forense digital*" [En Línea]. Disponible en: http://La importancia de la evidencia y el análisis forense digital - http://www.bsecure.com.mx/opinion/la-importancia-de-la-evidencia-y-el-analisis-forense-digital/

[7] C. Jeimy, "*Introducción a la informática Forense"* [En Línea]. Disponible en: Http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

[8] (Blog En Línea) (2011, Oct 11) Titulo. *"Informática Forense"*, Disponible en: http://www.informaticaforense.com.co/index.php?option=com_content&view=article&id=57&Itemid=64

[9] (Blog En Línea) (2008, Oct 11) Titulo. *"Adquisición de Datos Forenses",* Montevideo, Disponible en: http://www.cert.uy/documentos/pdf/certuy-first-tc-mvd08-v081.pdf

[10](Blog En Línea) (2012, Jun 13), "*Análisis forense de sistemas informáticos"* Disponible en: http://blog-es.seh-technology.com/entradas/analisis-forense-de-sistemas-informaticos.html

Autores

Diana Marcela Bonilla Pérez, es egresada del programa de Ingeniería de Sistemas de la Universidad Autónoma de Colombia, actualmente culmino la Especialización en Seguridad Informática y el Diplomado en Informática Forense de la Universidad Piloto de Colombia, Auditor Interno en ISO 27001, conocimiento de la norma ISO27001, ha realizado cursos en Check Point Security Administrator (CCSA) R70,

Check Point II Security Expert (CCSE) R70 , EC Council Network Security Administrator (ENSA), Mejores prácticas para la implementación ISO27002 y Gestión del riesgo basado en la guía ISO27005:2008

Enfocada en Seguridad de la Información desde hace 5 años en donde se ha desempeñado como Information Secutity Officer en Etek International, Network Management Analyst I en Fiduciaria Bogotá, desde hace un año y nueve meses se desempeña como Analista de Seguridad de la Información en la Corporación Financiera Colombiana S.A. Empresa del Grupo Aval en donde apoya a las Empresas Filiales en la implementación del Modelo de Seguridad de la Información bajo la norma ISO27001.

Leonardo Sierra Rodríguez, egresado de la Universidad Fundación Universitaria los Libertadores, actualmente termino su Postgrado como Experto en Seguridad Informática, y realizo un diplomado en Informática Forense, en la Universidad Piloto de Colombia, lo que lo certifica como Perito Forense.

Actualmente trabaja en O4it, como Ingeniero de Servicios en la nube, administrando Citrix y Windows Server, aplica su conocimiento en seguridad informática para asegurar los diferentes dispositivos.