UNIVERSIDAD
DE BURGOS

Informática Forense

Eduardo Mora González

Contenido

1. INTRODUCCIÓN

La sociedad actual está sujeta a continuos cambios sociales, políticos, económico… y sobre todo en referencia al tratamiento de la comunicación y de la información, cuyo crecimiento se está produciendo de una forma exponencial.

El uso de Internet en diferentes instituciones y empresas ha llevado a reconocer no sólo los beneficios que conlleva sino a entender los riesgos inherentes a la seguridad. Es por ello, que surge la necesidad de un estilo de informática cuya finalidad sea solucionar los conflictos tecnológicos relacionados con la informática y la protección de datos.

2. INFORMATICA FORENSE

2.1. DEFINICIÓN

Si buscamos el significado de informática y forense obtenemos las siguientes definiciones:

- **Informática:** "*Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras*." [R1]
- **Forense:** *"De la administración de justicia o relacionado con ella."* [R2]

Juntando las dos definiciones anteriores aparece le termino de Informática Forense, este término puede tener varias acepciones en la definición:

- La Informática Forense es el proceso de investigar dispositivos electrónicos o computadoras con el fin de descubrir y de analizar información disponible, suprimida, u ocultada que puede servir como evidencia en un asunto legal. [R3]
- Según el FBI, La informática forense se define como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

2.2. OBJETIVOS

El análisis forense informático agrupa las técnicas científicas y de análisis especializadas en las infraestructuras tecnológica. El uso de estas técnicas posibilita la identificación, preservación, análisis y presentación tanto de datos como de documentación, para poder ser aceptados en un proceso legal.

Por ello, el análisis se realiza una vez detectada la amenaza, analizando las consecuencias que ha producido en los sistemas y averiguar quién ha sido el autor, las causas, la metodología empleada y detectar los puntos débiles de los sistemas informáticos que han sido atacados.

Por estas razones, el principal objetivo de la informática forense es la protección de datos de empresas, personales, redes sociales o cualquier ámbito. De este objetivo principal se deducen los siguientes objetivos parciales:

- ✓ Compensar daños causados
- ✓ Crear y aplicar medidas de prevención de casos similares.
- ✓ Generar programas más seguros.
- ✓ Utilizar la informática forense con un fin preventivo.
- ✓ Detectar la vulnerabilidad de seguridad.
- ✓ Corregir dicha vulnerabilidad.
- ✓ Redactar y elaborar las políticas sobre uso de los sistemas de información.
- ✓ No atentar contra el derecho a la intimidad.
- ✓ Garantizar la efectividad de las políticas de seguridad.

2.3. LA INFORMÁTICA FORENSE Y EL HACKING ÉTICO

El hacking ético es el recurso utilizado para probar y valorar la seguridad de una red. Se centra en conocer la red de los sistemas y las interacciones de los equipos, usuarios, procedimientos, políticas y ciberseguridad.

Su motivo es mejorar la protección de las redes y los sistemas actuales, sabiendo las estrategias y herramientas táctica a fin de combatir la cibercriminalidad, examinando,

reforzando y optimizando la seguridad informática. Por ello se diseña un plan para eliminar los puntos débiles del sistema o para reducirlos en la medida de lo posible.

Por eso hacking ético y la informática forense son dos campos de la informática que están muy relacionadas ya que ambas persiguen encontrar vulnerabilidades.

2.3.1. VULNERABILIDADES INFORMÁTICAS

Una vulnerabilidad [R4] es un estado en un sistema informático (o conjunto de sistemas) que:

- ✓ Permite a un hacker ejecutar comandos como otro usuario.
- ✓ Permite a un hacker acceder a datos contrarios a las restricciones de acceso especificados para estos datos.
- ✓ Permite a un hacker hacerse pasar por otra entidad.
- ✓ Permite a un hacker realizar una denegación de servicio.

Existen diversas vulnerabilidades informáticas, las más comunes son:

- ❖ **Buffer Overflow:** Error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto [R5].
- ❖ **Inyección de código:** La inyección de código es la explotación de un error de la computadora causado por el procesamiento de datos no válidos. El atacante usa la inyección para introducir (o inyectar) código en un programa informático vulnerable y cambiar el curso de ejecución [R6].
- ❖ **Cross Site XSS:** Es un tipo de vulnerabilidad muy común en las aplicaciones web que permite a los atacantes colocar secuencias de comandos maliciosos en páginas web e instalen malware en los navegadores web de los usuarios.

  Estos ataques no se limitan a las páginas web, también a las aplicaciones que sean vulnerables. Esta vulnerabilidad permite a los atacantes ejecutar un script en el navegador y secuestrar las sesiones de usuario, contraseña o datos personales, pudiendo acceder al correo electrónico, cuenta bancaria, … [R7]

2.4. PASOS DE LA INFORMÁTICA FORENSE

Cuando se identifica un caso en el que se deba aplicar la informática forense, esta tiene definido una serie de pasos a seguir. Estos pasos son:

2.4.1. IDENTIFICACIÓN

Es muy importante conocer los antecedentes, situación actual y el proceso que se quiere seguir para poder tomar la mejor decisión con respecto a las búsquedas y la estrategia de investigación.

Incluye muchas veces la identificación del bien informático, su uso dentro de la red, el inicio de la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia), la revisión del entorno legal que protege el bien y del apoyo para la toma de decisión con respecto al siguiente paso una vez revisados los resultados.

2.4.2. PRESERVACIÓN

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta para poder mantener la integridad de la evidencia y la cadena de custodia que se requiere.

Al realizar una imagen forense, nos referimos al proceso que se requiere para generar una copia “bit-a-bit” de todo el disco, el cual permitirá recuperar en el siguiente paso, toda la información contenida y borrada del disco duro.

Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios.

2.4.3. ANÁLISIS

Proceso de aplicar técnicas científicas y analíticas a los medios duplicados por medio del proceso forense para poder encontrar pruebas de ciertas conductas. Se pueden realizar búsquedas de cadenas de caracteres, acciones específicas del o de los usuarios de la máquina como son el uso de dispositivos de USB (marca, modelo), búsqueda de archivos

específicos, recuperación e identificación de correos electrónicos, recuperación de los últimos sitios visitados, recuperación del caché del navegador de Internet, etc.

2.4.4. PRESENTACIÓN

Es el recopilar toda la información que se obtuvo a partir del análisis para realizar el reporte y la presentación a los abogados, la generación (si es el caso) de una pericial y de su correcta interpretación sin hacer uso de tecnicismos.

3. CASOS FAMOSOS DEL USO DE LA INFORMATICA FORENSE

Actualmente la informática forense se usa a diario para resolver casos, alguno de estos casos que han sido mas sonados y conocidos son los siguientes. [R8].

3.1. BTK (BIND, TORTURE, KILL)

Durante más de 30 años, la identidad de esta persona fue un misterio para la policía de Wichita, Kansas y el FBI. BTK (Bind, Torture, Kill) como se hacía llamar, estranguló a diez personas entre 1974 y 1991.

El asesino se burló de la policía con notas extrañas dejadas en lugares extraños (atrapados en un libro en la biblioteca, en una caja de cereales), poemas incomprensibles que envió a los medios locales junto con rompecabezas e imágenes. La policía local y el FBI hicieron un seguimiento de miles de pistas, tomaron 1300 muestras de ADN, entrevistaron a innumerables personas y analizaron sus escritos depravados, todo fue en vano ya que el caso se detuvo.

Luego, después de trece años de silencio, BTK reanudó las comunicaciones con los medios locales y la policía. Sorprendentemente, en un acto de psicótica, BTK contactó a la policía por carta y les preguntó si se podía rastrear o no un disquete. La policía se comunicó en un anuncio de periódico publicado en el Wichita Eagle que no se podían rastrear por lo que BTK envió su siguiente mensaje en un disquete.

Los expertos forenses en informática analizaron los metadatos del disquete y recuperaron los documentos. Los metadatos son datos sobre datos. Entre muchas piezas de información registradas en metadatos, se encuentra cuándo y quién modificó por última vez un archivo; en este caso, encontraron el nombre "Dennis" y la frase "Christ Lutheran Church".

Una búsqueda en el sitio web de la iglesia mostró que Dennis Rader era el presidente del consejo de congregación. La policía estableció vigilancia y obtuvo una muestra de ADN de su hija. Dennis Rader fue arrestado en febrero de 2005; se declaró culpable de los asesinatos y ahora cumple diez cadenas perpetuas consecutivas.

3.2. EL GRUPO CORCORAN

La importancia de este caso no se basa en lo que encontraron los expertos forenses en informática, sino en lo que no encontraron.

El Grupo Corcoran es uno de los corredores de bienes raíces más grandes de Nueva York. La compañía tiene su sede en Manhattan y vende propiedades que van desde un millón de dólares para un estudio hasta áticos de varios pisos que pueden costar hasta 80 millones de dólares. Fue una de sus ventas más bajas las que alertaron a todas las empresas sobre cómo se maneja el correo electrónico.

El caso involucra a una pareja casada con dos niños pequeños que compraron un apartamento de tres dormitorios y 1,600 pies por $ 1.3 millones en junio de 2007. Cada vez que llovió, se produjeron fugas masivas en su unidad (y otras) que dañaron muebles, ropa y electrodomésticos. Se quejaron con Corcoran, quien se negó a remediar la situación, alegando que las filtraciones ocurrieron después de la venta. El agua inundó la unidad hasta el punto de que la familia tuvo que mudarse, pero todavía estaban sujetos a la hipoteca y los cargos comunes. La pareja decidió demandar.

Los abogados contratados por la pareja encontraron un informe de un ingeniero que mostraba que el edificio había sido ensamblado con un material llamado "Wonderboard", que se utiliza en proyectos de construcción que se sabe que tienen fugas. También había

moho generalizado y niveles muy altos de monóxido de carbono en la sala de calderas. Parte de la demanda involucró un análisis forense de las computadoras del Grupo Corcoran.

El experto forense en informática estaba buscando evidencia de irregularidades, pero descubrió que los correos electrónicos y otros archivos que deberían haber estado en el disco duro habían desaparecido. Cuando se recuperaron los datos eliminados, revelaron que los agentes de Corcoran cancelaron las citas con los compradores en días lluviosos para ocultar las filtraciones de agua previamente conocidas.

El juez dictaminó que Corcoran fue "gravemente negligente" por no preservar y cambiar la evidencia electrónica que mostraba conocimiento previo de las fugas de agua. La multa para el gigante inmobiliario fue insignificante: $ 35,000.00 en honorarios legales y costos judiciales acumulados por el demandante. Sin embargo, se estableció un nuevo precedente legal para preservar la evidencia electrónica en casos legales.

4. CONCLUSIÓN

Realizar este trabajo me ha ayudado a conocer más sobre la informática forense, aclarando sus conceptos y sus fases. Además, el estudio de caso reales me ha dado una visión de lo importante que es la seguridad.

REFERENCIAS

R1: https://dle.rae.es/inform%C3%A1tico#S2qtrce

R2: https://diccionario.leyderecho.org/forense/

R3: https://cld.bz/bookdata/ddZw8Zo/basic-html/page-154.html#

R4: https://encyclopedia.kaspersky.es/knowledge/software-vulnerabilities/

R5: https://es.wikipedia.org/wiki/Desbordamiento_de_b%C3%BAfer

R6: http://www.alegsa.com.ar/Dic/inyeccion_de_codigo.php

R7: https://es.godaddy.com/blog/que-es-el-cross-site-scripting-xss-y-como-puedes-evitarlo

R8: https://cso.computerworld.es

BIBLIOGRAFIA Y WEBGRAFIA

https://www.ecured.cu/Desbordamiento_de_b%C3%BAfer

https://indalics.com/peritaje-informatico/herramientas-de-informatica-forense

https://cld.bz/bookdata/ddZw8Zo/basic-html/page-154.html#

http://www.alegsa.com.ar/Dic/inyeccion_de_codigo.php

https://www.rae.es/

https://javiermarques.es/libro-gratuito-el-rastro-digital-del-delito

http://www.criptored.upm.es/descarga/ConferenciaJavierPagesTASSI2013.pdf