¿QUÉ ES UN PERITO INFORMÁTICO FORENSE?

AUTOR: RICARDO CASTILLO B

NOVIEMBRE: 2020

San Marcos

Introducción

Parte de la importancia sobre conocer qué es un perito informático forense incluye saber cuál es la mayor dificultad de su trabajo. Dado que una de las principales complicaciones es descubrir al ciberdelincuente. Es vital tener en cuenta que las herramientas de los hackers suelen ir un paso por delante de la seguridad informática.

Aparte, uno de los motivos por lo que esto es una de las funciones más complicadas es que el delincuente no necesita un motivo para realizar un ataque y unirse a la ciberguerra. Basta con tener ciertos conocimientos y ganas de experimentar para poner en marcha un ataque informático, lo que hace que el móvil de los crímenes sea múltiple, haciendo aún más compleja la tarea de los peritos informáticos.

En general, la siguiente lectura hace referencia a qué es un perito informático forense, y sus funciones.

¿Qué es un perito informático forense?

Un perito informático forense es el profesional encargado de realizar análisis de todos los elementos tecnológicos. Esto le permite llevar a cabo una recopilación de datos que harán posible realizar una evidencia digital. Estas se emplean para esclarecer el litigio que tengan asignadas.

Las funciones de un perito informático forense son las siguientes:

- Realizar informes judiciales o extrajudiciales.
- Asesoramiento.
- Ser auxiliar de magistrados, abogados, jueces y tribunales.

¿Qué hace un perito informático forense?

Dentro de esta profesión encontramos tres puntos fundamentales:

- El anonimato en la red depende de forma directa de los medios a nuestro alcance.
- Lo más complicado, de todos los procesos de la informática forense, es la atribución de un ataque informático.
- Existen algoritmos que sirven para comprobar si hay archivos que sufrieron algún tipo de manipulación.

El trabajo del perito tiene como función realizar exámenes minuciosos para comprobar cómo se realizó la ejecución de un ataque informático. El objetivo es reparar los daños, prevenir los que aun no se produjeron y detectar quién es el responsable.

La ciencia forense digital

También es importante conocer qué es la ciencia forense digital. Se puede definir como aquella que posee el objetivo de conseguir, conservar y analizar datos. Dichos datos deben de haber sido procesados de forma electrónica y deben de estar almacenados en un sistema digital.

Esta ciencia posee tres ramas principales:

- Computadores.
- Redes.

- Evidencias digitales.

De las características dentro de lo qué es un perito informático forense, esta es su principal herramienta: las evidencias digitales. Estos son los datos que se encuentran en los sistemas informáticos. Dan la opción de determinar lo que ocurrió en un cibercrimen. También la posibilidad de conectar a la víctima con el agresor y el crimen en sí.

Dentro de la informática forense, como en la mayoría de las ciencias, se intenta responder a preguntas básicas dentro de la disciplina forense:

- Quién.
- Cómo.
- Dónde.
- Por qué.
- Cuándo.

Cualquier objeto o persona que entren en la escena del crimen deja pistas a su paso. Es aquí donde se produce la trasferencia de evidencias forenses. Debido a esto, se podrán analizar por el perito informático.

Complicaciones en el peritaje informático forense

Hay que tener en cuenta que el peritaje informático no sigue la misma línea que otras disciplinas forenses. Existen diferentes particularidades en el ámbito digital que son importantes de destacar:

- Las evidencias digitales son frágiles y fáciles de perder de forma irremediable.
- Una de las principales ventajas de las evidencias digitales es que se pueden copiar todas las veces que sea necesario. También es destacable que, sobre dichas copias, se puede demostrar de forma sencilla que son exactas a las originales.
- Existen circunstancias donde es muy difícil demostrar que se copió un archivo determinado. Esto suele ocurrir, por ejemplo, en casos de robo de la propiedad intelectual. Se debe a que los archivos originales quedan inalterados.

Descubrir al ciberdelincuente

Hay que conocer también los métodos de seguridad que emplea el perito, en especial para proteger los datos digitalizados.

Uno de los métodos más interesantes son los llamados honeypots. Estos nos dan la posibilidad de interactuar con los ciberdelincuentes.

Por ejemplo, un honeypot puede ser un servidor que este conectado a Internet. Este simulara ser parte del sistema, esto lo hará "vulnerable" a que alguien lo intente atacar. La trampa es para que el ciberdelincuente piense que está atacando al sistema original. El honeypot se encargará de detenerlo antes de que consiga acceder a la información vulnerable.

Hay muchas herramientas que, gracias al trabajo del perito informático forense, nos dan la posibilidad de engañar a los delincuentes. Esto para poder obtener información sobre sus procedimientos y métodos de actuación.

Cuando se logra extraer información sobre la forma determinada en la que se ataca un sistema, podemos estudiar diferentes técnicas, tácticas y procedimientos para poder mantenernos seguros.

Servicios que ofrece el peritaje informático

- Extracción y recuperación de de información de dispositivos. Esto puede darse incluso luego de borrada.
- Análisis forense.
- Barridos electrónicos. Tanto para particulares como para empresas.
- Peritaje de mensajería instantánea. Aplicaciones como WhatsApp o correos electrónicos.
- Auditorias informáticas.

Es importante tener en cuenta también que el perito informático forense trabaja con información delicada o incluso con delitos. Por ejemplo, el mal uso del correo electrónico, la suplantación de identidad, manipulación de softwares.

Conclusiones y recomendaciones

En conclusión, como se logra apreciar en la lectura, la labor del Perito Informático Forense es de suma importancia debido a que logra extraer y recuperar información, contribuye a mejorar la seguridad digital, realiza auditorias informáticas y pese a que los delincuentes utilizan estrategias cada vez más avanzadas para realizar sus fechorias, los peritos informáticos forenses tambien utilizan herramientas para conocer cómo trabajan estos. Por ello, poseen una ardua tarea, misma que consiste en investigar y poder identificar cómo, cuándo y quién cometió el ataque, ayudar a identificar el objetivo que buscaba el atacante, saber cuántos sistemas se vieron comprometidos, e identificar y cuantificar la información que fue vulnerada, así como estudiar a la forma de actuar de estos criminales para mejorar la seguirdad digital.

Podemos afirmar que, el perito cumple una función primordial, dentro del mundo moderno y globalizado, en donde tanto los individuos como organizaciones utilizan la tecnología para uso cotidiano o bien, para realizar negocios, por lo que requieren que sus datos estén seguros y en caso de ser victimas de un ataque, minimizar los riesgos y pérdidas, dar con los delincuentes y mejorar su seguirdad digital y para todo ello es necesario contar con un experto en el tema, es decir, con un perito informático digital.

Referencias bibliográficas

Informático Forense (2019). Recuperado de https://www.informatico-forense.es/que-es-un-perito-informatico-forense/

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica