ALGUNAS DE LAS MEJORES HERRAMIENTAS GRATUITAS DE INFORMÁTICA FORENSE

AUTOR: JOSÉ ANTONIO LORENZO.

AGOSTO: 2020

San Marcos

Introducción

El análisis forense digital es una especialidad muy importante de la seguridad informática, debido a que consiste en un conjunto de técnicas que permiten extraer información de los discos y memorias de un equipo, sin alterar el estado de los mismos.

Al buscar datos se pretende detectar un patrón o descubrir información que no está a simple vista. Es por ello que, ante un incidente de seguridad, es sumamente importante efectuar un análisis forense digital a todos los soportes de información, como discos duros, SSD, memorias USB y otro tipo de almacenamiento interno y externo.

Contents

Algunas de las mejores herramientas gratuitas de informática forense

Introducción a la informática forense digital

Aunque en un primer momento se podría pensar que el análisis forense digital solo se limita a computadores, dispositivos móviles como smartphones y tablets, y otros, lo cierto es que también se extiende a los datos que enviamos y transmitimos a través de la red cableada o inalámbrica, por lo que es muy importante disponer de herramientas de este tipo.

Para realizar el trabajo de análisis forense y la recoleccion de los datos, se requiere de un perito. Su labor consiste en hacer uso de herramientas de software gratuitas, o bien, de pago; así como herramientas hardware para clonado de discos. Este último es muy importante, debido a que se requiere tener una copia exacta de los discos, y acceder al sistema de archivos completo, para lograr analizar en detalle el sistema de archivos, los documentos, registros internos del sistema operativo y mucho más. Una vez que el experto ha recabado toda la información, analizará en detalle todos los datos obtenidos, e intentará averiguar qué ha ocurrido en el sistema para que se haya visto expuesto, y también cómo han conseguido hacerse con todos los datos

Sistemas Operativos

A continuación, se hace referencia a los diferentes sistemas operativos que disponen de la gran mayoría de herramientas de informática forense:

CAINE es un sistema operativo completo que está orientado específicamente a la informática forense, está basado en Linux e incorpora la gran mayoría de herramientas necesarias para realizar un análisis forense completo. Dispone de una interfaz gráfica de usuario, es muy fácil de utilizar, aunque lógicamente se requieren los conocimientos adecuados para utilizar todas y cada una de sus herramientas. Se puede utilizar en modo LiveCD sin tocar el almacenamiento del ordenador donde se desea arrancarlo, de esta manera, toda la información del disco duro permanecerá intacta para posteriormente realizar la copia de toda la información. Entre las herramientas incluidas con CAINE tenemos las siguientes: The Sleuth Kit, Autopsy, RegRipper, Wireshark, PhotoRec, Fsstat y muchas otras.

Un aspecto muy importante de CAINE es que también dispone de herramientas que se pueden ejecutar directamente en sistemas operativos Windows, por lo que, si se baja la imagen ISO y se extrae el contenido, se logra acceder al software para Windows, sin necesidad de arrancar el LiveCD o utilizar una máquina virtual.

Kali Linux es uno de los sistemas operativos relacionados con seguridad informáticas más utilizados, tanto para pentesting como también para informática forense, ya que en su interior posee una gran cantidad de herramientas preinstaladas y configuradas para realizar un análisis forense lo antes posible.
Este sistema operativo no solo tiene una gran cantidad de herramientas forenses en su interior, sino que dispone de un modo Live específico para análisis forense, y no escribir absolutamente nada en el disco duro o almacenamiento interno que se posea en los equipos. También impide que, al introducir un dispositivo de almacenamiento extraíble, se monte automáticamente, sino que el usuario lo realiza manualmente.

DEFT Linux y DEFT Zero

El sistema operativo DEFT Linux está también orientado específicamente a análisis forense, incorpora la gran mayoría de herramientas de CAINE y Kali Linux, es una alternativa más disponible para utilizar. Lo más destacable de DEFT es que dispone de una gran cantidad de herramientas forenses listas para manejar.
DEFT Zero es una versión mucho más ligera y reducida de DEFT, está orientada a exactamente lo mismo, pero requiere menos recursos para poder utilizarla sin problemas, además, es compatible tanto con sistemas de 32 bits y 64 bits, así como sistemas UEFI.

Herramientas gratuitas de análisis forense

Ahora se detallará algunas de las herramientas gratuitas para la realización de tareas forenses. Como se mencionó, todas las herramientas son completamente gratuitas, y están incorporadas en las distribuciones Linux.:

Autopsy y The Sleuth Kit

La herramienta Autopsy es una de las más utilizadas y recomendadas, permite localizar muchos de los programas y plugins de código abierto, es como una biblioteca de Unix y utilidades basadas en Windows, lo que facilita enormemente el análisis forense de

sistemas informáticos.
Autopsy es una interfaz gráfica de usuario que muestra los resultados de la búsqueda forense. Esta herramienta es muy utilizada por la policía, los militares y las empresas cuando quieren investigar qué es lo que ha pasado en un equipo.
Uno de los aspectos más interesantes es que es extensible, esto significa que los usuarios pueden agregar nuevos complementos de manera fácil y rápida. Incorpora algunas herramientas de manera predeterminada como PhotoRec para recuperar archivos, e incluso permite extraer información EXIF de imágenes y vídeos.
En cuanto a The Sleuth Kit, es una colección de herramientas de comandos en línea para investigar y analizar el volumen y los sistemas de archivos utilizados en investigaciones forenses digitales. Con su diseño modular, se puede utilizar para obtener los datos correctos y encontrar evidencias. Además, es compatible y funciona en Linux y se ejecuta en plataformas Windows y Unix.

Magnet Encrypted Disk Detector

Esta herramienta funciona a través de la línea de comandos, verifica de manera rápida y no intrusiva los volúmenes cifrados en un ordenador, para saber si existen para posteriormente intentar acceder a ellos con otras herramientas. La última versión disponible es la 3.0, y es la que se recomienda utilizar, además, es recomendable usar el sistema operativo Windows 7 o superior. Esta herramienta permite detectar discos físicos cifrados con TrueCrypt, PGP, VeraCrypt, SafeBoot, o Bitlocker de Microsoft. Magnet Encrypted Disk Detector es totalmente gratuita, pero se requiere hacer un registro en su web oficial para proceder con la descarga.

Magnet RAM Capture y RAM Capturer

Magnet RAM Capture es una herramienta que está diseñada para obtener la memoria física del computador donde la utilicemos. Al usarla, se logra recuperar y analizar datos muy valiosos que se almacenan en la memoria RAM y no en un disco duro o SSD. Es posible que, en determinados casos, se deba buscar la evidencia directamente en la memoria RAM. Recordar que la RAM es volátil y que se borra cada vez que apagamos el equipo.

¿Qué se puede encontrar en la memoria RAM?

Procesos, programas ejecutándose en el sistema, conexiones de red, evidencias de

malware, credenciales de usuario y mucho más. Esta herramienta permite exportar los datos de memoria en bruto, sin procesar, para posteriormente cargar esta información en otras herramientas específicamente diseñadas para ello. Por supuesto, este software también es gratis.

Otra herramienta similar es **RAM Capturer**. Es un instrumento que consigue volcar los datos de la memoria RAM de un computador a un disco duro, pendrive u otro dispositivo de almacenamiento extraíble. Esta herramienta permite acceder a las credenciales de usuario de volúmenes cifrados como TrueCrypt, BitLocker, PGP Disk o credenciales de inicio de sesión de cuenta para muchos servicios de correo web y redes sociales, ya que toda esta información suele almacenarse en la memoria RAM.

Conclusiones y recomendaciones

En conclusión, existen muchos tipos de herramientas que pueden ser utilizadas para la informatica forense, Hay muchas herramientas, mismas que acompañadas del perito informático forense, ofrecen la posibilidad de lograr obtener información sobre los procedimientos y métodos de actuación de los delincuentes.
Por otra parte, al extraer información sobre la forma determinada en la que se ataca un sistema, se puede estudiar diferentes técnicas, tácticas y procedimientos y de esta manera crear metodos más eficases que logren mantener seguros a los individuos, o bien, a las organizaciónes de los delitos digitales.

Referencias bibliográficas

Lorenzo. J.A (2020). Mejores herramientas gratuitas de informática forense. Recuperado de https://www.redeszone.net/tutoriales/seguridad/mejores-herramientas-gratuitas-informatica-forense/

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica