Informática Forense

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Miércoles 4 de Noviembre del 2015

Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling.

Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de doce años de experiencia en el área y desde hace ocho años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz y al Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Informática Forense, GNU/Linux y Software Libre.

@Alonso_ReYDeS www.facebook.com/alonsoreydes

pe.linkedin.com/in/alonsocaballeroquezada/

Informática Forense

- Es un campo altamente especializado y de rápido crecimiento de la ciencia forense.
- Abarca un amplio espectro de dispositivos, como computadoras, teléfonos móviles, reproductores de músicas, y cualquier medio.
- Aplica procesos y procedimientos forenses tradicionales a la evidencia digital.
- Es utilizado en casos civiles y criminales o cualquier otra área en disputa. Cada una de estos tiene su propio conjunto de requerimientos relevantes a la jurisdicción del caso.
- Un procedimiento típico implica recuperar datos desde dispositivos de almacenamiento digital perdidos u ocultos después de un incidente o hecho, ya sea accidental o deliverado.

Procedimiento

No son relevantes los detalles específicos del caso, pues el procedimiento general sigue la misma serie de procesos, los cuales deben ser métodos probados y repetibles científicamente, para reconstruir los eventos relacionados a un caso.

- Preservar la evidencia
- Identificar la evidencia
- Extraer la evidencia
- Documentar la evidencia recuperada y como se recuperó.
- Interpretar la evidencia
- Presentar la evidencia (Ya sea para un cliente o juzgado)

Utilización

La informática Forense puede ser utilizada en una diversidad de escenarios, incluyendo investigaciones criminales, juicios civiles, etc.

Investigaciones Criminales

La evidencia electrónica puede ser encontrada en cualquier investigación criminal realizada.

- Pornografía Infantil
- Robo de Identidad
- Homicidio
- Abuso sexual
- Robos
- Etc.

Litigios Civiles

Ambas partes implicadas deben examinar evidencia. (Descubrimiento)

Sistema de Archivos

- El sistema de archivos rastrea el espacio libre como también la ubicación de cada archivo sobre el dispositivo de almacenamiento.

- El espacio libre también es conocido como espacio sin asignar. Y al espacio ocupado se le conoce como espacio asignado.

Existen diversos tipos de sistemas de archivos, como los siguientes:

- **FAT (File Allocation Table)**

  El mas antiguo y común sistema de archivos. FAT12, FAT16, FAT32, FATX. Utilizado también en medios de almacenamiento (USB).

- **NTFS (New Technology File System)**

  Utilizado en las más recientes versiones de los sistemas operativos. Es más poderoso comparado con FAT.

Recuperación de Archivos

- Para el usuario promedio existe la falsa sensación de seguridad al realizar la acción para borrar un archivo.
- Los archivos “no” son borrados completamente cuando el Sistema Operativo expone haber realizado este proceso.
- El “Borrar” únicamente permite indicar a la computadora la disponibilidad del espacio ocupado por el archivo.
- Los datos del archivo permanecerán hasta ser escritos nuevamente, lo cual puede implicar bastante tiempo.

File Carving

Extraer datos desde el dispositivo de almacenamiento, basándose en ciertas características únicas de los archivos, como las cabeceras de los archivos.

Memoria Volátil (RAM)

- La memoria RAM almacena todos los datos actualmente siendo utilizados por el CPU (Unidad Central de Procesamiento).
- Los datos son alimentados desde la RAM hacia el CPU, donde son ejecutados.
- La memoria RAM existe únicamente cuando se proporciona energía eléctrica. Desconectado esto (se apaga la máquina), los datos empiezan a desaparecer.
- El forense tradicional se enfocaba en analizar dispositivos de almacenamiento (Discos Duros).
- En la actualidad una gran cantidad de evidencia puede ser encontrada en la memoria RAM, la cual no es escrita hacia un disco duro.
- Por lo tanto es vital capturar la memoria RAM de un sistema en funcionamiento, para luego proceder con su análisis.

Más Contenidos

Videos de 30 Webinars Gratuitos sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

http://www.reydes.com/d/?q=videos

Diapositivas utilizadas en los Webinars Gratuitos.

http://www.reydes.com/d/?q=node/3

Artículos y documentos publicados

http://www.reydes.com/d/?q=node/2

Mi Blog sobre temas de mi interés.

http://www.reydes.com/d/?q=blog/1

Informática Forense

¡Muchas Gracias!

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Miércoles 4 de Noviembre del 2015