Webinar Gratuito
Evidencia Volátil

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Jueves 27 de Febrero del 2014

¿Quién Soy?

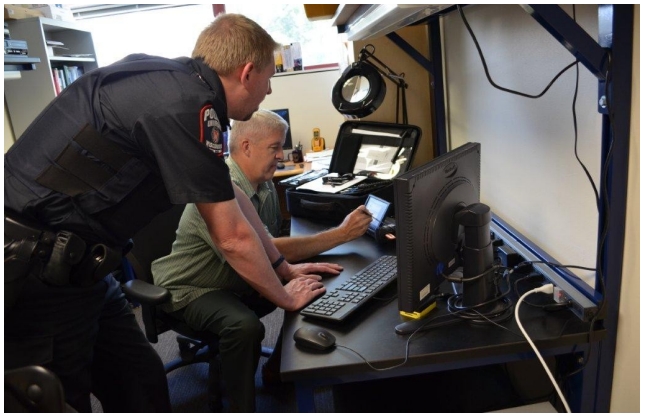
- Consultor e Instructor Independiente en Hacking Ético, Informática Forense y GNU/Linux.
- Ex Integrante de RareGaZz y actual integrante de PeruSEC.
- Ex Redactor en la Revista Linux+ DVD (ES).
- Creador del II Reto Forense Digital Sudamericano - Chavín de Huantar 2012.
- Brainbench Certified Network Security, Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General). CNHE, CNCF, CNHAW.
- Más de 11 años de experiencia en el área.
- @Alonso_ReYDeS
- pe.linkedin.com/in/alonsocaballeroquezada/

Primera Respuesta

Se refiere a las primeras acciones que se realizan cuando se llega a la escena de un hecho y se accede a los sistemas de cómputo de los implicados, una vez que se ha reportado el incidente.

A la persona que interviene se le denomina “El primer respondedor”. Esta persona es la responsable de proteger, integrar, y preservar la evidencia obtenida desde la escena de un hecho.

Además, necesita tener un conocimiento completo de los procedimientos de investigación forense. De tal manera que se preserve toda la evidencia digital. Luego deberá realizar la investigación de tal manera que la evidencia capturada sea aceptada en un juzgado.



* First Responders Guide To Computer Forensics - http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=7261

Evidencia Digital

La Evidencia Digital es un dato relevante para una investigación que es transferida o almacenada sobre un dispositivo electrónico. Este tipo de evidencia es encontrada cuando se recolectan los datos de cualquier dispositivo electrónico para su análisis.

La Evidencia Digital usualmente se almacena en dispositivos de almacenamiento, como discos duros, CDs, DVDs, tarjetas de memoria, unidades USB.

Evidencia Volátil

La Evidencia Volátil es aquella que se pierde al momento en el cual un sistema es desconectado o apagado (Pierde suministro de poder). Este tipo de evidencia existe generalmente en la memoria física, o RAM, y está constituida de información sobre procesos, conexiones de red, archivos abiertos, etc. Este tipo de información describe el estado de un sistema en un punto del tiempo particular.

Cuando se realiza una respuesta en vivo, una de las primeras cosas que hará el investigador será la recolección del contenido de la RAM.

- Tiempo del Sistema
- Usuarios “Logueados”
- Archivos Abiertos
- Información de la Red
- Conexiones de Red
- Información sobre Procesos
- Mapeo de Procesos y Puertos
- Procesos en Memoria
- Estado de la red, etc.

Curso Virtual de Informática Forense

Días:

Grupo 1: Sábados 1, 8, 15 y 22 de Marzo del 2014
Grupo 2: Domingos 2, 9, 16 y 23 de Marzo del 2014

Horario:

De 9:00am a 12:30m (UTC -05:00)

Más Información:

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

caballero.alonso@gmail.com

@Alonso_ReYDeS

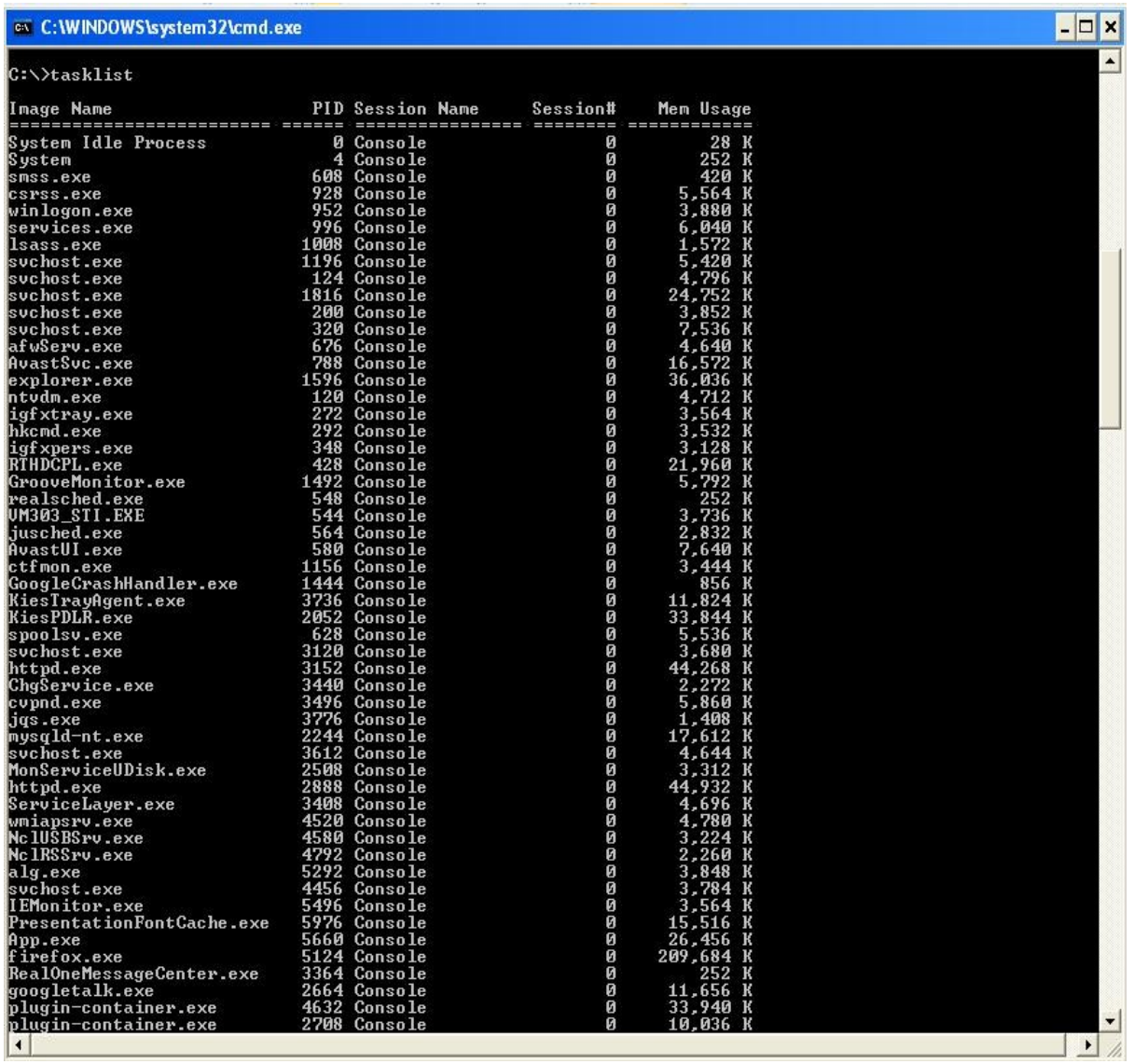
http://pe.linkedin.com/in/alonsocaballeroquezada/

ReYDeS

http://www.reydes.com

Demostraciones

A continuación se presentan algunas demostraciones prácticas para la captura de evidencia volátil en un sistema Windows.



Más Material

Los invito a visualizar los 18 Webinars Gratuitos que he dictado hasta el momento, sobre temas de Hacking Ético, Pruebas de Penetración, Hacking Aplicaciones Web e Informática Forense.

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

Pueden obtener todas las diapositivas utilizadas en los Webinars Gratuitos desde la siguiente página:

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

Pueden obtener todos los artículos y documentos que he publicado.

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

Mi blog personal:

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

¡Muchas Gracias!

Evidencia Volátil

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Jueves 27 de Febrero del 2014