Webinar Gratuito
Informática Forense & GNU/Linux

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Cómputo Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Jueves 8 de Agosto del 2013

¿Quién Soy?

- Consultor e Instructor Independiente en Hacking Ético, Cómputo 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 - Chavin de Huantar 2012.

- Brainbench Certified Network Security, Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General). CNHE, CNCF, CNHAW.

- Más de 10 años de experiencia en el área.

- Twitter: @Alonso_ReYDeS

- LinkedIn: pe.linkedin.com/in/alonsocaballeroquezada/

Informática Forense & GNU/Linux

El propósito de este Webminar es proporcionar una introducción al Sistema Operativo GNU/Linux como plataforma forense para investigación digital y análisis forense.

Linux

Cuando hablamos del Sistema Operativo Linux, nos estamos refiriendo a GNU/Linux. Una combinación del Kernel Linux y utilidades GNU.

¿Porqué GNU/Linux?

* Control: No solo sobre el software forense, sino también sobre el Sistema Operativo y el hardware adjunto

* Flexibilidad: Se pude iniciar desde un CD/DVD (Un Sistema Operativo completo), soporte de sistemas de archivos, soporte plataformas, etc.

* Poder: Una distribución de Linux es (o puede ser) una herramienta forense.

Informática Forense & GNU/Linux (Cont.)

1. Creando una imagen forense de un disco sospechoso
2. Montando una imagen
3. Montando una imagen utilizando el dispositivo loopback
4. Hash de archivo

5. Análisis
6. Haciendo un listado de archivos
7. Haciendo un listado por tipos de archivo.
8. Visualizando archivos
9. Buscando texto en el espacio de holgura o sin asignar

Herramientas Forenses

1. dd: Comando utilizado para copiar desde un archivo o dispositivo de entrada a un archivo o dispositivo de salida. Réplica sencilla de flujo de bits.

2. sfdisk y fdisk: Utilizado para determinar la estructura de un disco.

3. grep: Busca archivos por coincidencias de una expresión o patrón.

4. loop device: Permite asociar un archivos regulares con nodos de dispositivo. Este permite montar un imagen de flujo de bits sin tener que reescribir la imagen a un disco

5. md5sum & sha1sum: Crear y almacenar un hash MD5 o SHA de un archivo o lista de archivos (incluyendo dispositivos)

6. file: Lee la información de la cabecera de los archivos en un intento de acertar su tipo, sin relación al nombre o extensión.

7. xxd: Herramienta en línea de comando para visualizar un archivo en modo hexadecimal.

Demostraciones

Este Webminar está basado en la Guía de Linux LEO. (The Beginner's Guide v3.78)

Sitio Web: http://linuxleo.com/

1. Descargar los siguientes archivos:

http://linuxleo.com/Files/practical.floppy.dd

http://linuxleo.com/Files/md5sums.txt

2. Tener el documento “The Law Enforcement and Forensics Examiner's Introduction to Linux”.

3. Una Instalación de GNU/Linux. Se recomienda tener una Máquina Virtual con SIFT, DEFT o CAINE.

Curso Online de Informática Forense

Días:

Sábados 17, 24, 31 de Agosto y 7, 14 de Setiembre del 2013

Horario:

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

Más Información:

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

Correo electrónico: caballero.alonso@gmail.com
Twitter: https://twitter.com/Alonso_ReYDeS
LinkedIn: http://pe.linkedin.com/in/alonsocaballeroquezada/
Skype: ReYDeS
Sitio Web: http://www.reydes.com

¡Muchas Gracias!

Informática Forense & GNU/Linux

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Cómputo Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Jueves 8 de Agosto del 2013