Análisis Forense a GNU/Linux

Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Jueves 4 de Junio del 2015

Presentación

Alonso Eduardo Caballero Quezada es 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 y Miembro de Open Web Application Security Project (OWASP).

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 e integra actualmente el Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos en Perú y Ecuador, 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/

Sistema de Archivos ext2 / ext3

En un ext2 el disco se divide en particiones, estas en grupos (particiones de partición). Cada grupo contiene.

Superbloque: Almacena todos los metadatos sobre el sistema de archivos. Cada grupo tiene su propio superbloque y un superbloque maestro almacena los datos son el sistema de archivos completo.

Descriptores de Grupo: Contiene información sobre el grupo. Aquí se encuentra a tabla de inodos y los mapas de bits de asignación para los inodos y bloques de datos.

Inodos y Estructura de Archivo: Los archivos son representados por inodos. Cada inodo apunto hacia un conjunto de bloques de datos los cuales contienen los datos en el archivo.

Directorios: Son simples archivos conteniendo una lista de entradas y punteros hacia los archivos lo cuales se encuentran en el directorio.

ext3 y ext4 son referidos como “ext2 + Journaling”.

Análisis a GNU/Linux

Para realizar un análisis forense a un sistema GNU/Linux se requiere conocer como mínimo la estructura de los sistemas de archivos ext2 y ext3. Adicionalmente también conocer el funcionamiento de la memoria de intercambio.

Conocido lo anterior, se puede iniciar una investigación real de la actividad del usuario y rastrear actividad maliciosa.

Como en toda investigación se debe tener una teoría, para luego revisar en el sistema de archivos real, y ver como esta teoría se traduce en uso.

Existen diversas herramientas open source o de fuente abierta, todas ellas factibles de ser utilizadas juntas para realizar una investigación forense completa.

Estas herramientas requieren utiliza una imagen forense compatible “dd” o una imagen forense en bruto o cruda. La cual es una copia byte a byte no comprimida del dispositivo de almacenamiento.

Procesos a Realizar

A continuación se detallan algunos de los procedimientos a realizar durante el análisis forense a un sistema GNU/Linux.

Encontrar Firmas del Sistema de Archivos.

Localizar y Recuperar Archivos Borrados.

Detectar las Diferencias entre Distribuciones GNU/Linux

Rastrear la Actividad del Usuario

Actividad de Impresión

Montar la Imagen Forense

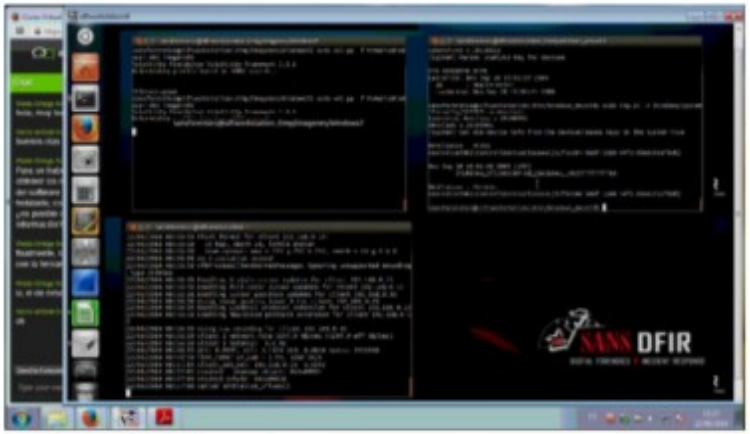
Buscar el Espacio sin Asignar

Analizar el Espacio Swap

Curso Virtual de Informática Forense

Curso Virtual de Informática Forense

2015



Grupo Sábado:
6, 13, 20 y 27 de Junio del 2015
De 3:30pm a 7:15pm (UTC -05:00)

Grupo Domingo:
7, 14, 21 y 28 de Junio del 2015
De 9:00am a 12:45pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Más Información: http://www.reydes.com/d/?q=Curso_de_Informatica_Forense
E-mail: **caballero.alonso@gmail.com** / Sitio Web: http://www.reydes.com

Cursos Virtuales

Todos los Cursos Virtuales dictados están disponibles en Video.

Curso Virtual de Hacking Ético

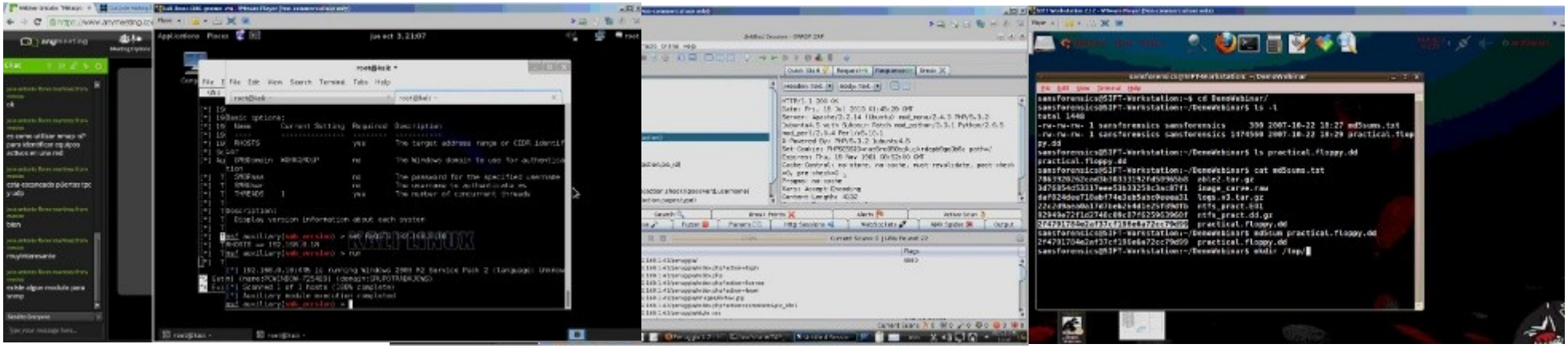
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web

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

Curso Virtual de Informática Forense

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



Más Contenidos

Videos de 27 Webinars Gratuitos sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

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

Diapositivas utilizadas en los Webinars Gratuitos.

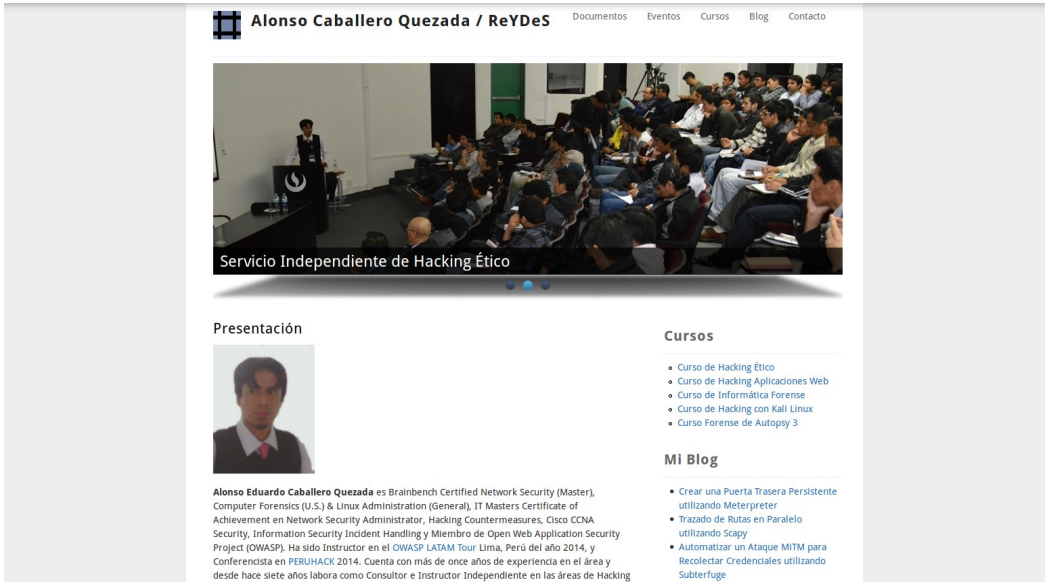
http://www.reydes.com/d/?q=node/3

Artículos y documentos publicados

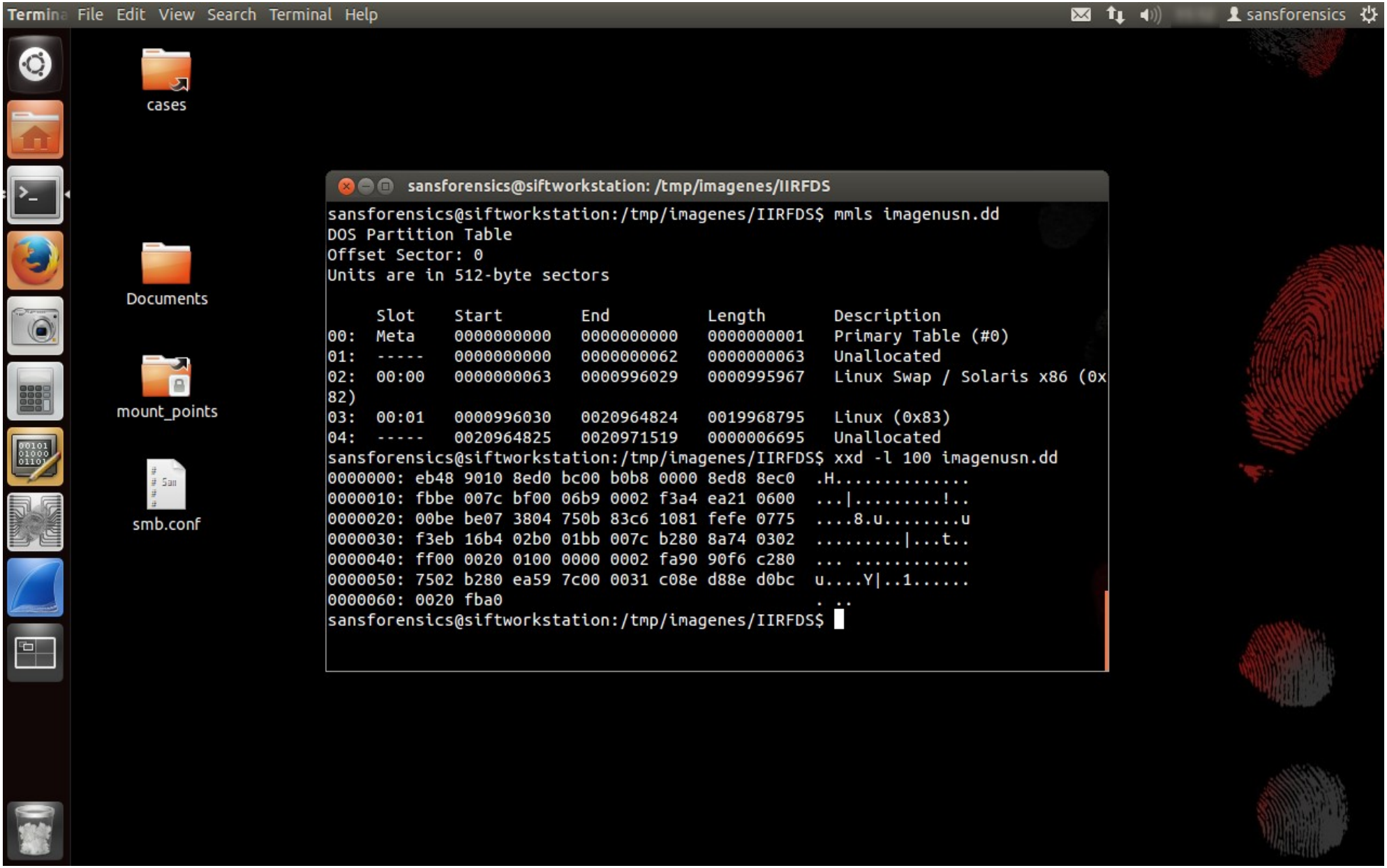
http://www.reydes.com/d/?q=node/2

Mi Blog sobre temas de mi interés.

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



Demostraciones



Análisis Forense a GNU/Linux

Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

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

e-mail: ReYDeS@gmail.com

Jueves 4 de Junio del 2015