Técnicas Antiforenses Básicas

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 3 de Setiembre 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/

Técnicas Antiforenses

Una técnica antiforense es cualquier cambio intencional o accidental obscureciendo, cifrando, u ocultando datos de las herramientas forenses.

Cuando se intenta ocular rastros considerar el hecho de estar ayudando al investigador forense conocer donde buscar por evidencia digital.

La mayoría de herramientas forenses actuales para la examinación, no confían en los datos o vistas de estos en la misma manera la cual lo hacían antes.

Por ejemplo, versiones antiguas de herramientas open source podían perder archivos o datos debido a errores lógicos de codificación.

- Métodos para Obscurecer

- Medidas de Privacidad

Métodos para Obscurecer

Es utilizado para intentar obscurecer la verdadera naturaleza o significado de algún dato, típicamente cambiando su nombre o su contenido.

Se refiere al escenario donde se intenta intencionalmente o accidentalmente cambiar el nombre o contenido de un archivo, lo cual resulta en un archivo el cual podría ya sea ser mal interpretado o ignorado en un posterior análisis forense.

- Renombre de la Extensión de un Archivo

- Métodos de Codificación

- Métodos de Compresión

- Flujos de Datos Alternos (ADS)

- Espacio de Holgura o Residual (Slack)

Medidas de Privacidad

Algunas de las técnicas forenses reconocidas son intentos legítimos para intentar proteger la privacidad de las personas. Esto de hecho no ayuda al análisis forense de un sistema, por lo tanto se necesita ser capaz de identificar y acceder a esta información protegida.

No es relevante en este punto eliminadores de spyware, herramientas antispam, o herramienta las cuales protegen la privacidad de la información dejada en una computadora.

Nuestro interés se centra en software de privacidad la cual protege o borra los datos existentes sobre un disco duro o dispositivo de almacenamiento.

- Cifrado (Encryption)

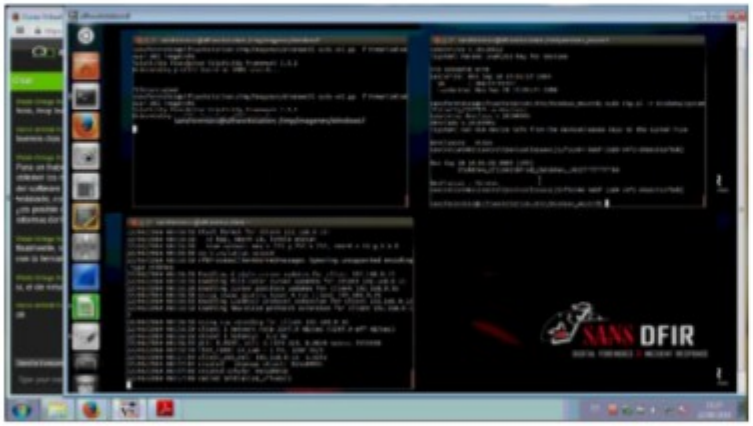
- Esteganografía

- Limpieza (Wiping)

Curso Virtual de Informática Forense

Curso Virtual de Informática Forense

2015



Último Curso del año 2015

Grupo Sábado:

5, 12, 19 y 26 de Setiembre del 2015
De 3:30pm a 7:15pm (UTC -05:00)

Grupo Domingo:

6, 13, 20 y 27 de Setiembre 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

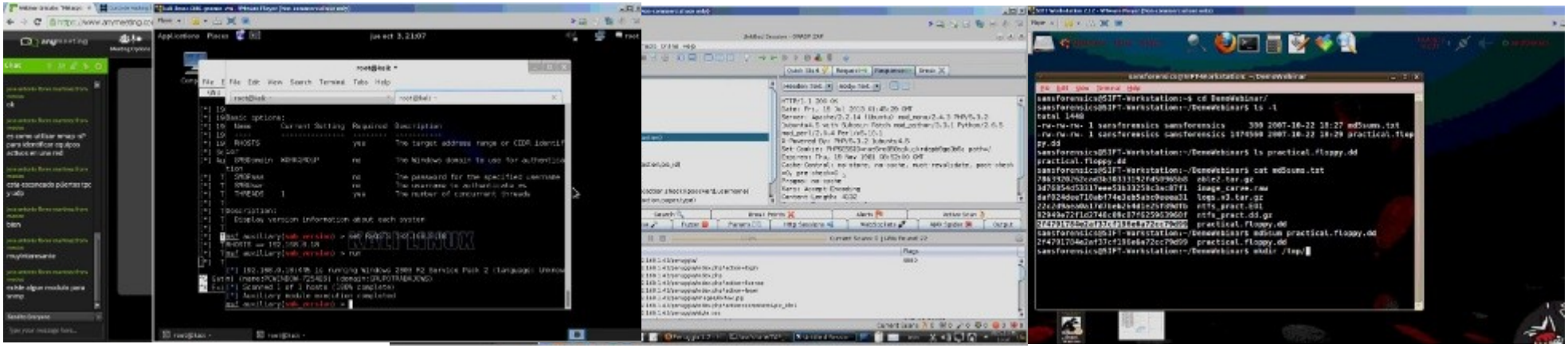
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

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 29 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

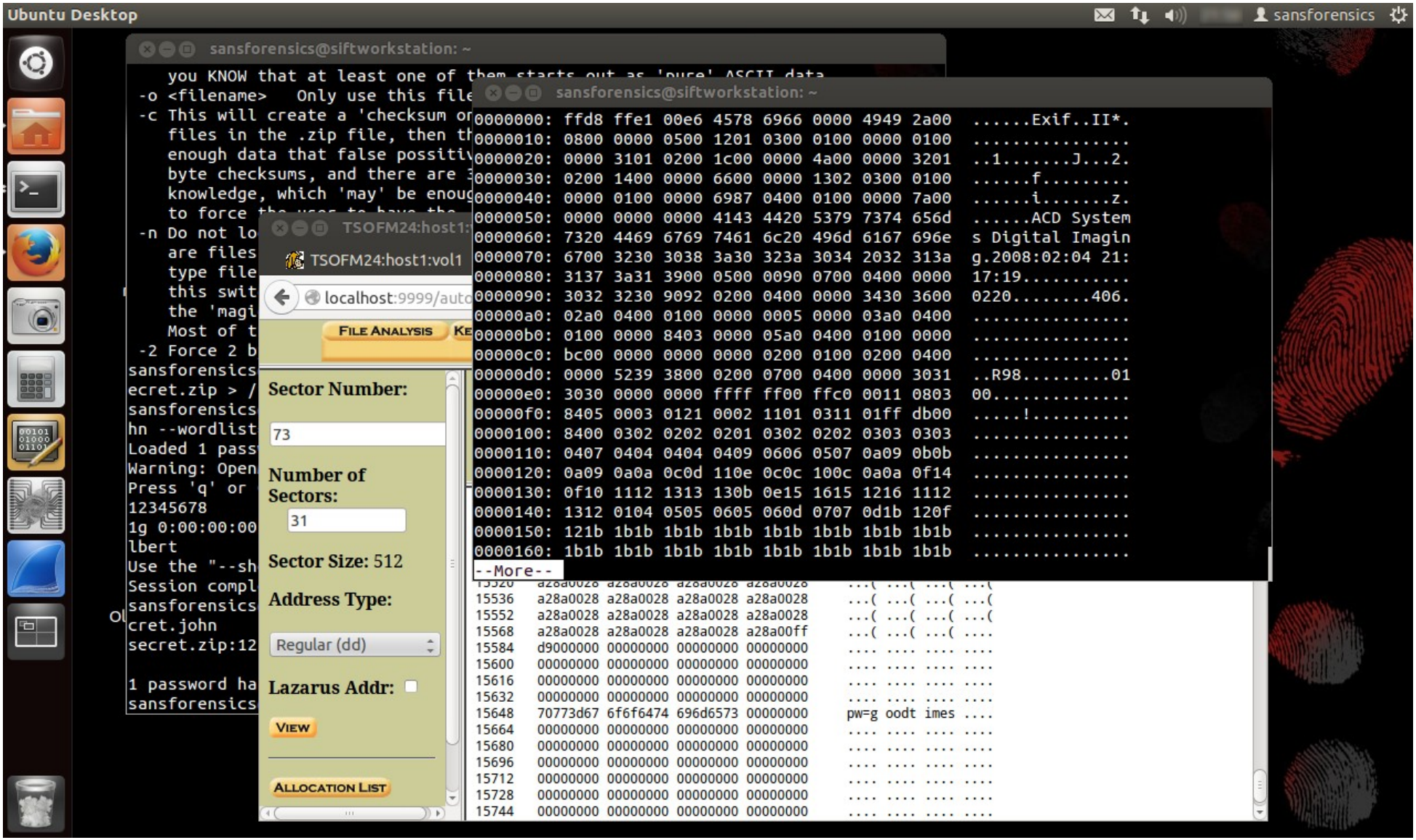
Artículos y documentos publicados

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

Mi Blog sobre temas de mi interés.

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

Demostraciones



Técnicas Antiforenses Básicas

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 3 de Setiembre del 2015