Webinar Gratuito

Análisis Forense a Linux

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: https://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 3 de Marzo 2022

Alonso Eduardo Caballero Quezada

EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures Pen Testing, Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist y OSEH.

Más de 18 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

Redes Sociales

https://www.linkedin.com/in/alonsocaballeroquezada/

https://twitter.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.instagram.com/alonso_reydes/

reydes@gmail.com

https://www.reydes.com

+51 949 304 030

@ReYDeS

¿Porqué Forense a Linux?

Aunque Linux es el sistema operativo de escritorio más utilizado, está presente en muchos lugares. Aunque en muchos países Windows es el sistema operativo dominante en escritorios, muchas organizaciones ejecutan Linux en sus servidores. Linux también es elegido por muchos proveedores de servicios en Internet, como también grandes compañías como Google. Siendo Linux extremadamente popular en organizaciones de desarrollo.

Linux es la elección estándar para cualquiera quien labore en seguridad de la información o forense. Consecuentemente es altamente probable si un incidente se relaciona con estas áreas, se deberá analizar un sistema Linux.

Muchos otros dispositivos ejecutan alguna versión de Linux, puntos de acceso inalámbricos, controlares de temperatura, teléfonos móviles, etc.

* https://www.kernel.org/

Sistema de Archivos Extendido

El sistema de archivo extendido es encontrado en la mayoría de sistemas Linux. Son comúnmente referenciados como extN, donde N representa la versión (usualmente 2, 3, 4).

Existen una razón para ext2 sea reservado normalmente para sistemas de archivos estáticos. ext3 y ext4 tienen sistemas de archivos con jornal, pero ext2 no es un sistema de archivos con jornal. El jornal se utiliza para mejorar el rendimiento y reducir las posibilidad de cambios por corrupción de datos.

Así es como funciona el sistema de archivos con jornal. Las escrituras hacia el medio no son hechas inmediatamente, en lugar de esto los cambios son escritos hacia un jornal. En el evento de una computadora no sea apagada correctamente, el jornal puede ser utilizado para retornar las cosas hacia un estado consistente.

Sistema de Archivos Extendido (Cont.)

La información se almacena en bloques, organizados en bloques de grupos

Superbloque: Describe el sistema de archivos y le indica al sistema operativo donde encontrar varios elementos (inodos, etc.)

Descriptores de Grupo: Describen la disposición para cada grupo de bloques

Inodos: (index nodes) contiene todos los metadatos para un archivo excepto su nombre.

Bloques de dato: Son utilizados para almacenar archivos y directorios

Mapas de bits: Indican cuales inodos y bloques de datos están en uso.

Procedimientos Fundamentales

- Obtener información sobre los sistemas de archivos contenidos en las imágenes forenses
- Montar los sistemas de archivos contenidos en las imágenes forenses
- Localizar a intentar recuperar los archivos borrados en los sistemas de archivos
- Intentar reconstruir los archivos eliminados en los sistemas de archivos
- Realizar una análisis forense a la memoria RAM del sistema
- Reconstruir actividad de los usuarios y del propio sistema operativo
- Encontrar, analizar, e interpretar los diversos artefactos forenses de Linux

Curso Virtual de Informática Forense

Domingos 6, 13, 20 y 27 de Marzo del 2022. De 9:00 am a 12:00 pm (UTC -05:00)

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

Presentación

En la actualidad todas las empresas y organizaciones deben estar preparadas para enfrentar exitosamente diversos tipos de crímenes cibernéticos, los cuales se suscitan y afectan sus sistemas de cómputo y redes. Consecuentemente se ha incrementado la demanda por profesionales forenses debidamente entrenados y experimentados, quienes estén en la capacidad investigar crímenes cibernéticos relacionados a fraudes, amenazas internas, espionaje industrial, inadecuado uso de los empleados, e intrusiones hacia computadoras y redes Las agencias del gobierno a nivel mundial también requieren profesionales forenses debidamente entrenados y con amplia experiencia en el ámbito del forense digital.

Objetivos

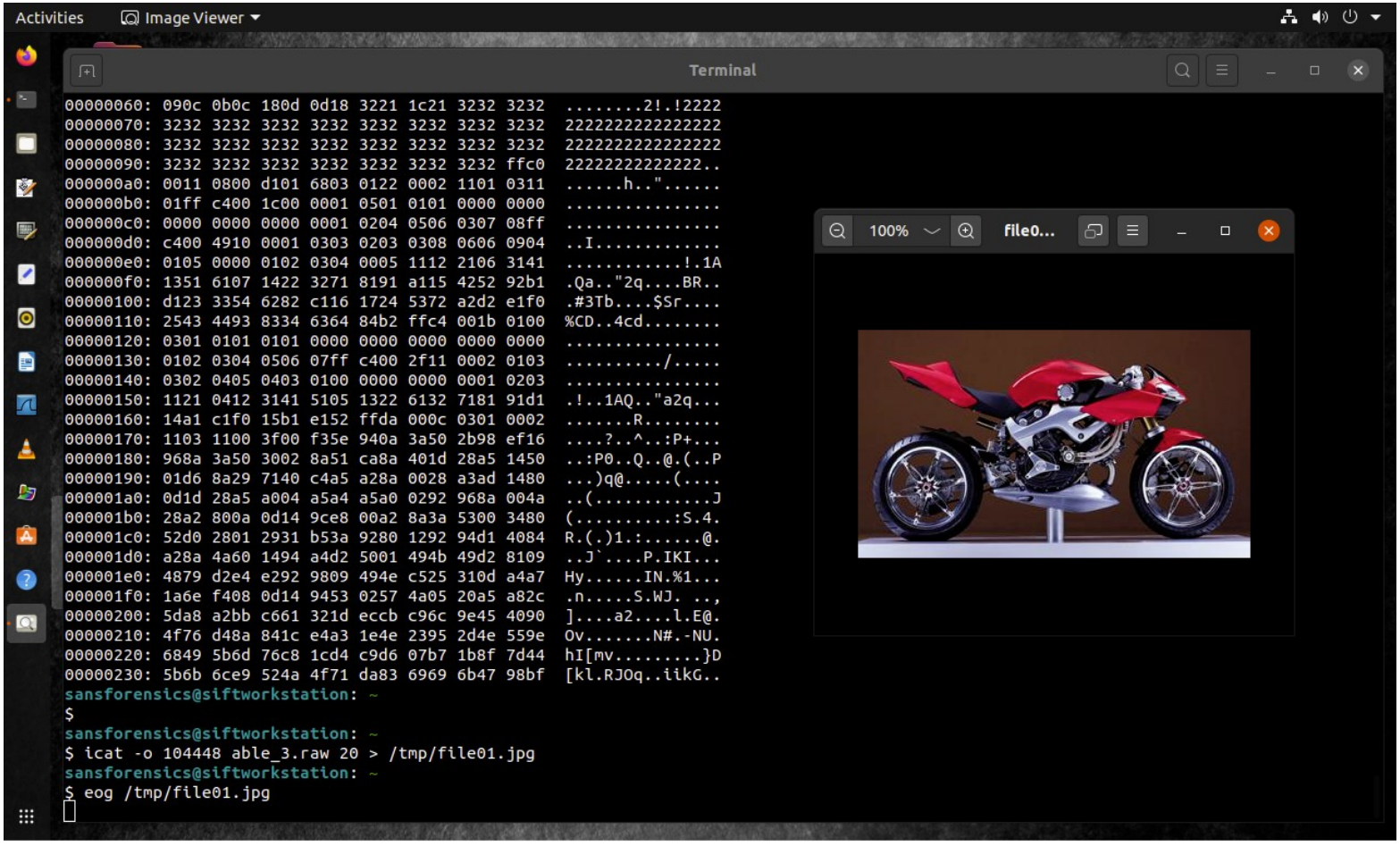
Este curso enseña a los participantes a desarrollar un profundo

Alonso Eduardo Caballero Quezada. EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). He sido instructor, expositor y conferencista en el OWASP LATAM Tour,

Más Información: https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

e-mail: reydes@gmail.com Sitio Web: https://www.reydes.com

Demostraciones



Cursos Virtuales Disponibles en Video

Curso Virtual de Hacking Ético
https://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web
https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense
https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

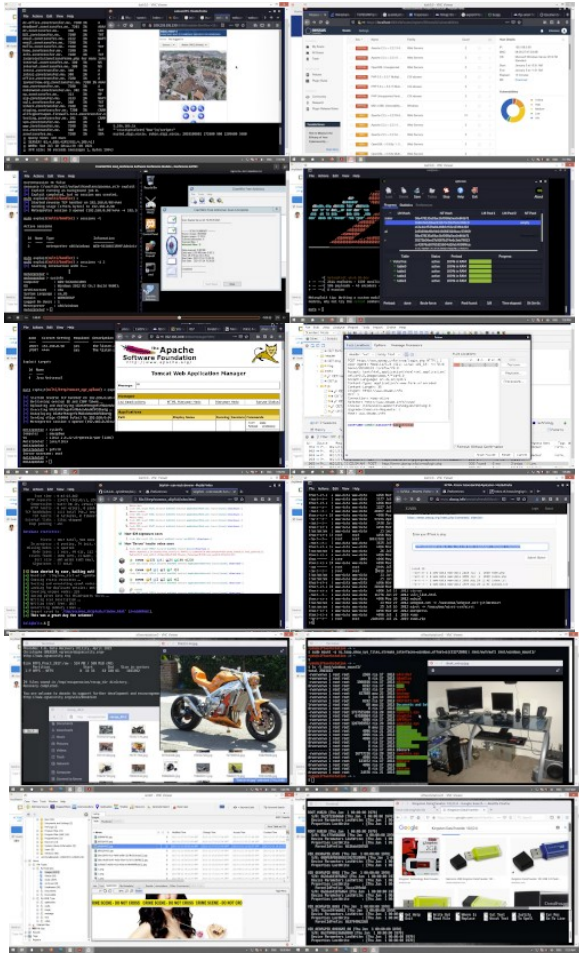
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

Curso Virtual OSINT - Open Source Intelligence
https://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes
https://www.reydes.com/d/?q=Curso_Forense_de_Redes

Y todos los cursos virtuales:

https://www.reydes.com/d/?q=cursos



Más Contenidos

Videos de 74 webinars gratuitos

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

Diapositivas de los webinars gratuitos

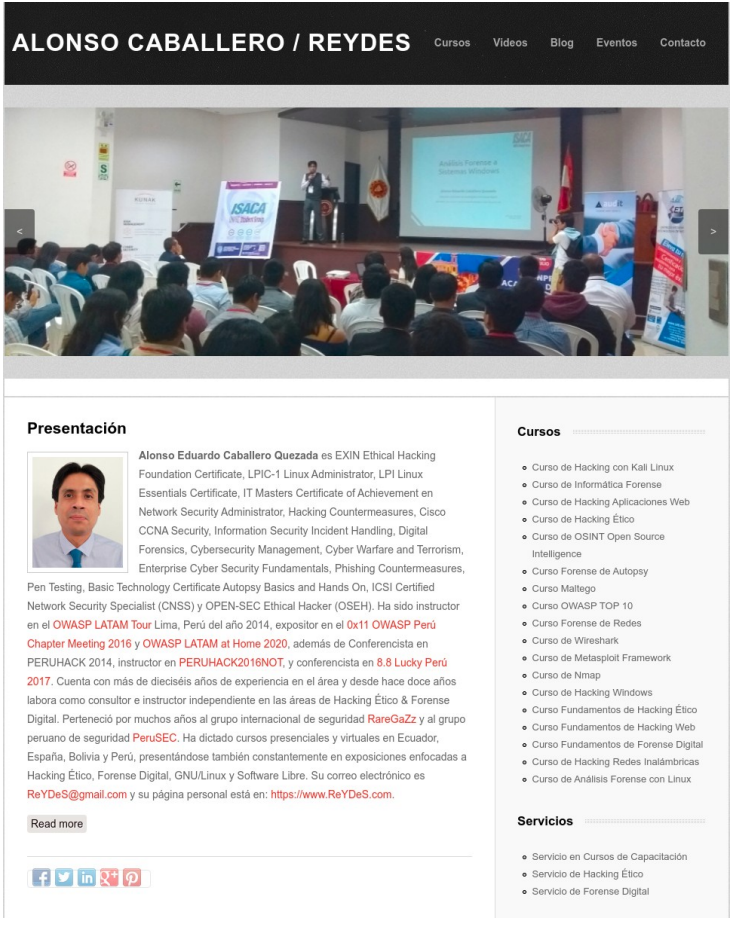
https://www.reydes.com/d/?q=eventos

Artículos y documentos publicados

https://www.reydes.com/d/?q=documentos

Blog sobre temas de mi interés

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



Webinar Gratuito

Análisis Forense a Linux

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: https://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 3 de Marzo 2022