

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/>

Alonso Eduardo Caballero Quezada :- Sitio web: <https://www.reydes.com> :- e-mail: reydes@gmail.com

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 journal, pero ext2 no es un sistema de archivos con journal. El journal 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 journal. Las escrituras hacia el medio no son hechas inmediatamente, en lugar de esto los cambios son escritos hacia un journal. En el evento de una computadora no sea apagada correctamente, el journal 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 e intentar recuperar los archivos borrados en los sistemas de archivos
- Intentar reconstruir los archivos eliminados en los sistemas de archivos
- Realizar un 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>

Alonso Eduardo Caballero Quezada :- Sitio web: <https://www.reydes.com> :- e-mail: reydes@gmail.com

Demostraciones

The screenshot shows a Linux desktop environment with a terminal window open. The terminal displays a hex dump of a file named 'able_3.raw'. The hex dump consists of 24 lines of hexadecimal data, each followed by a corresponding ASCII representation. The ASCII column contains various characters, including spaces, dots, and letters, which are the beginning of a text file. Below the hex dump, the user runs the command `icat -o 104448 able_3.raw 20 > /tmp/file01.jpg` to convert the hex data into a JPEG image. The terminal then shows the command `eog /tmp/file01.jpg` being executed. An image viewer window titled 'file0...' is open, displaying a red and black motorcycle on a stand. The terminal window title is 'Terminal' and the desktop background is dark.

```
00000060: 090c 0b0c 180d 0d18 3221 1c21 3232 3232 .....21..!2222
00000070: 3232 3232 3232 3232 3232 3232 3232 3232 22222222222222222222
00000080: 3232 3232 3232 3232 3232 3232 3232 3232 22222222222222222222
00000090: 3232 3232 3232 3232 3232 3232 3232 3232 2222222222222222..
000000a0: 0011 0800 d101 6803 0122 0002 1101 0311 .....h..".....
000000b0: 01ff c400 1c00 0001 0501 0101 0000 0000 .....
000000c0: 0000 0000 0000 0001 0204 0506 0307 08ff .....
000000d0: c400 4910 0001 0303 0203 0308 0606 0904 ..I.....
000000e0: 0105 0000 0102 0304 0005 1112 2106 3141 .....!.1A
000000f0: 1351 6107 1422 3271 8191 a115 4252 92b1 .Qa.."2q...BR..
00000100: d123 3354 6282 c116 1724 5372 a2d2 e1f0 .#3Tb....$Sr....
00000110: 2543 4493 8334 6364 84b2 ffc4 001b 0100 %CD..4cd.....
00000120: 0301 0101 0101 0000 0000 0000 0000 0000 .....
00000130: 0102 0304 0506 07ff c400 2f11 0002 0103 ...../.....
00000140: 0302 0405 0403 0100 0000 0000 0001 0203 .....
00000150: 1121 0412 3141 5105 1322 6132 7181 91d1 .!.1AQ.."a2q...
00000160: 14a1 c1f0 15b1 e152 ffd a00c 0301 0002 .....R.....
00000170: 1103 1100 3f00 f35e 940a 3a50 2b98 ef16 ....?..^...:P+...
00000180: 968a 3a50 3002 8a51 ca8a 401d 28a5 1450 ...:P0..Q..@.(.P
00000190: 01d6 8a29 7140 c4a5 a28a 0028 a3ad 1480 (... )q@.....(....
000001a0: 0d1d 28a5 a004 a5a4 a5a0 0292 968a 004a ..(.....J
000001b0: 28a2 800a 0d14 9ce8 00a2 8a3a 5300 3480 (. ....S.4.
000001c0: 52d0 2801 2931 b53a 9280 1292 94d1 4084 R.(.)1:.....@.
000001d0: a28a 4a60 1494 a4d2 5001 494b 49d2 8109 ..J'....P..IKI...
000001e0: 4879 d2e4 e292 9809 494e c525 310d a4a7 Hy.....IN.%1...
000001f0: 1a6e f408 0d14 9453 0257 4a05 20a5 a82c .n....S.WJ. .,
00000200: 5da8 a2bb c661 321d eccb c96c 9e45 4090 ]...a2....L.E@.
00000210: 4f76 d48a 841c e4a3 1e4e 2395 2d4e 559e Ov.....N#.-NU.
00000220: 6849 5b6d 76c8 1cd4 c9d6 07b7 1b8f 7d44 hI[mv.....]D
00000230: 5b6b 6ce9 524a 4f71 da83 6969 6b47 98bf [kl.RJQoq..iikG..

sansforensics@siftworkstation: ~
$
sansforensics@siftworkstation: ~
$ icat -o 104448 able_3.raw 20 > /tmp/file01.jpg
sansforensics@siftworkstation: ~
$ eog /tmp/file01.jpg
```

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

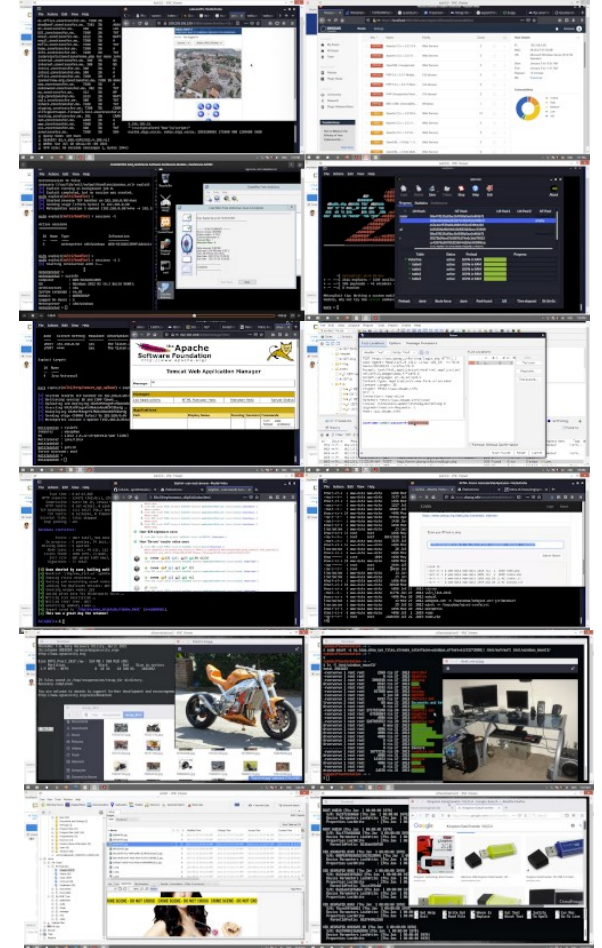
https://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes

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

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

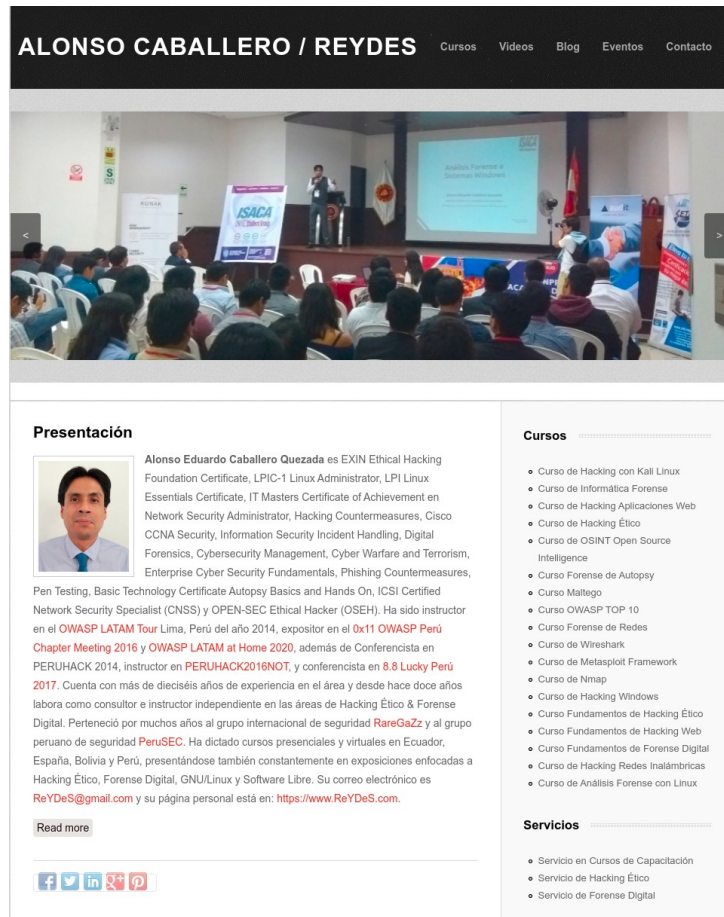
<https://www.reydes.com/d/?q=eventos>

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>




ALONSO CABALLERO / REYDES Cursos Videos Blog Eventos Contacto

Presentación

 **Alonso Eduardo Caballero Quezada** es 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). Ha sido instructor en el **OWASP LATAM Tour** Lima, Perú del año 2014, expositor en el **0x11 OWASP Perú Chapter Meeting 2016** y **OWASP LATAM at Home 2020**, además de Conferencista en **PERUHACK 2014**, instructor en **PERUHACK2016NOT**, y conferencista en **8.8 Lucky Perú 2017**. Cuenta con más de dieciséis años de experiencia en el área y desde hace doce años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. 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, Forense Digital, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: <https://www.ReYDeS.com>.

[Read more](#)



Cursos

- Curso de Hacking con Kali Linux
- Curso de Informática Forense
- Curso de Hacking Aplicaciones Web
- Curso de Hacking Ético
- Curso de OSINT Open Source Intelligence
- Curso Forense de Autopsy
- Curso Maltego
- Curso OWASP TOP 10
- Curso Forense de Redes
- Curso de WireShark
- Curso de Metasploit Framework
- Curso de Nmap
- Curso de Hacking Windows
- Curso Fundamentos de Hacking Ético
- Curso Fundamentos de Hacking Web
- Curso Fundamentos de Forense Digital
- Curso de Hacking Redes Inalámbricas
- Curso de Análisis Forense con Linux

Servicios

- Servicio en Cursos de Capacitación
- Servicio de Hacking Ético
- Servicio de Forense Digital

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