Webinar Gratuito

Análisis Forense a Linux

Alonso Eduardo Caballero Quezada

Instructor y Consultor Independiente en Ciberseguridad

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Jueves 29 de Febrero 2024

Alonso Eduardo Caballero Quezada

ISC2 Certified in Cybersecurity (CC), LPI Security Essentials Certificate, EXIN Ethical Hacking Foundation Certificate, 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, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE).

Más de 20 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético, Forense Digital, GNU/Linux, y áreas relacionadas.

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

www.reydes.com

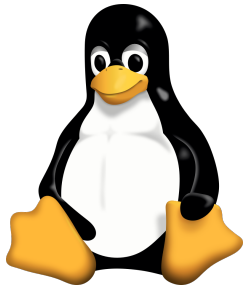
+51 949 304 030

@ReYDeS

¿Qué es GNU/Linux?

GNU/Linux es una familia de sistemas operativos tipo Unix compuesto por software libre y de fuente abierto. Surge de las contribuciones de varios proyectos de software, entre los cuales destacan GNU (iniciado por Richard Stallman en 1983) y el núcleo Linux (iniciado por Linus Torvalds en 1991).

Se encuentran normalmente como distribuciones. Entre las más populares se encuentran Debian, Ubuntu, Red Hat y SUSE. Su propósito es ofrecer GNU/Linux como un producto final para instalar o probar en un ordenador, cubriendo una diversidad de necesidades, las cuales que van desde el uso cotidiano personal hasta aplicaciones muy específicas en ambientes especializados.



* https://es.wikipedia.org/wiki/GNU/Linux

Sistemas de Archivos extX

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 del sistema de archivos completo.

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

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

Sistemas de Archivos extX (Cont.)

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

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

Feature	Ext2	Ext3	Ext4
Individual File Size	16GB-2TB	16GB-2TB	16GB-16TB
Volume file system size	4TB-32TB	4TB-32TB	4TB-1EB
Default inode size	128 bytes	128 bytes	256 bytes
Time Stamp	No support	Second	Nanosecond
Defragmentation	No	No	Yes
Directory Indexing	Disabled	Disabled	Enabled
Multiple Block Allocation	Basic	Basic	Advanced
Preallocation	No	In-core reservation	For extend file
Delayed Allocation	No	No	Yes

Análisis Forense a GNU/Linux

Se requiere conocer como mínimo la estructura de los sistemas de archivos extX También conocer el funcionamiento de la memoria de intercambio. En base a esto se puede iniciar una investigación sobre la actividad del usuario y rastrear actividad maliciosa.

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

Existen diversas herramientas de fuente abierta, todas factibles de ser utilizadas para realizar una investigación forense completa.

Estas herramientas requieren utilizar una imagen forense (dd) o una imagen forense en bruto o cruda. La cual es una copia byte a byte no comprimida del dispositivo de almacenamiento.

Tareas Base a Realizar

Algunas de las tareas fundamentales 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
- Generar Cronologías
- Analizar el Espacio Swap
- Analizar la RAM

Curso Informática Forense

Curso Virtual Informática Forense 2024

Domingos 3, 10, 17 y 24 de Marzo del 2024. De 9:00 am a 12:00 pm (UTC -05:00)

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 conocimiento sobre forense digital aplicado al sistema operativo Microsoft Windows. Es fundamental comprender las capacidades forenses y artefactos en estos sistemas. Aprender a identificar, capturar, autenticar, y analizar datos forenses. Entender como se puede rastrear detalladamente la actividad realizada del usuario a través de la red, además de como organizar sus hallazgos para ser utilizado en una respuesta de incidentes, investigaciones internas, y litigios civiles o penales. Utilizar los nuevos conocimientos adquiridos para validar las herramientas de seguridad, mejorando las evaluaciones de seguridad, identificar amenazas internas, rastrear atacantes, y mejorar las políticas de seguridad. Aunque se conozca o no, el sistema operativo Windows silenciosamente registra una gran cantidad de datos sobre el propio sistema y los usuarios. Este curso enseña una metodología para forense de computadoras con etapas de identificación, preservación, análisis y documentación. Se exponen técnicas y procedimientos de investigación manuales, también se utilizan herramientas forenses.

Fechas & Horarios

Duración: Catorce (14) horas. Una (1) sesión previamente grabada de dos (2) horas, y cuatro (4) sesiones en vivo de tres (3) horas de duración cada una.

Fechas:

Domingos 3, 10, 17, y 24 de Marzo del 2024

Horarios:

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

Alonso Eduardo Caballero Quezada.

ISC2 Certified in Cybersecurity (CC), Certificate, 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, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), y Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE). He sido instructor, expositor y conferencista en el OWASP LATAM Tour, OWASP Perú Chapter Meeting, OWASP LATAM at Home, PERUHACK, PERUHACKNOT, 8.8 Lucky Perú, Ekoparty University Talks Perú. Cuento con más de veinte años de experiencia en el área, y desde hace dieciséis años laboro como consultor e instructor en Hacking Ético & Forense Digital. Perteneci por muchos años al grupo internacional RareGaZz y grupo Peruano PeruSEC. He dictado cursos para España, Ecuador, México, Bolivia y PerúMi correo electrónico es ReYDeS@gmail.com y mi página personal está en: www.ReYDeS.com

Más Información

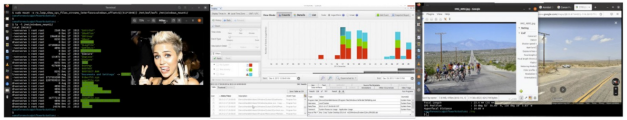
Para obtener más información sobre este curso, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

reydes@gmail.com

Teléfono: +51 949 304 030

Sitio Web: www.reydes.com



Temario

- Proceso Investigación Forense
- Evolución del Sistema de Archivos Windows
- FTK Imager
- Adquisición de la Memoria RAM
- Evidencia Encriptada
- Obtener Archivos Protegidos
- Imagen con Contenidos Personalizado
- Discos de Estado Sólido (SSD)
- Nivelación de Uso y SSD Trim
- Artefactos Forenses en SSD
- Adquisición de un Disco Duro
- Adquisición de un USB
- Montar una Imagen
- Visualización Previa de una Unidad
- Recuperar Archivos Borrados
- The Sleuth Kit (TSK)
- Autopsy 2
- Autopsy
- Búsqueda de Cadenas
- Reconstrucción de Datos
- Análisis Forense a la Memoria RAM
- Volatility Framework
- Forense de Correos Electrónicos
- Forense al Registro de Windows
- Lo Esencial del Registro
- Análisis de Información de Usuarios y Grupos
- Análisis de la Configuración del Sistema
- Análisis de la Actividad del Usuario
- Análisis de la Actividad USB
- Archivos de Enlace
- Metadatos en Documentos Office
- Metadatos en Documentos PDF
- Metadatos en Archivos de Medios (EXIF)
- Análisis de Miniaturas
- Análisis de la Papelera de Reciclaje
- Análisis de Archivos Prefetch
- Fundamentos del Registro de Eventos
- Análisis del Registro de Eventos (Logs)
- Registro de Eventos en Windows
- Forense al Navegador Web
- Fundamentos de los Navegadores
- Internet Explorer
- Archivos del Historial Cache / Archivos Temporales
- Cookies, Historial de Descarga

Material

- SIFT Workstation
- Imágenes Forenses Windows
- Herramientas Windows

Beneficios e Inversión

- Acceso a las sesiones en vivo
- Acceso al aula virtual por 45 días
- Video de las cinco (5) sesiones
- Material utilizado durante el desarrollo del curso
- Asesoría personalizada
- Libro "Fundamentos de Forense Digital" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación (CMIF). Puntuación mínima 70/100). Por una duración total de 24 horas

S/. 450 Soles o $ 140 Dólares

El pago del curso se realiza:

Residentes en Perú

Depósito bancario Scotiabank

Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada

O también pagos con Yape o Plin. Escriba un mensaje de correo electrónico a reydes@gmail.com para proporcionarle los datos pertinentes.

Residentes en otros países

Pago a través de Paypal PayPal

O también transferencia de dinero mediante Western Union y MoneyGram

Escriba por favor un mensaje de correo electrónico a reydes@gmail.com para proporcionarle los datos.

Confirmado el pago se enviará los datos para conectarse hacia la plataforma

Certificados

Certificados; constancias de participación y aprobación; expedidos a nombre de la empresa Peruana MILESEC EIRL.

Sitio Web:

www.reydes.com

Correo:

reydes@gmail.com

Más Información:

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

Prácticas

Activities Document Viewer

```
$
sansforensics@siftworkstation: ~
$ ls -l /tmp/recuperados/pdf/
total 6236
-rw-rw-r-- 1 sansforensics sansforensics 3075794 Feb 26 16:
-rw-rw-r-- 1 sansforensics sansforensics 3075897 Feb 26 16:
-rw-rw-r-- 1 sansforensics sansforensics  120613 Feb 26 16:
-rw-rw-r-- 1 sansforensics sansforensics  110428 Feb 26 16:
sansforensics@siftworkstation: ~
$
sansforensics@siftworkstation: ~
$ exiftool /tmp/recuperados/pdf/*
======== /tmp/recuperados/pdf/01017992_1.pdf
ExifTool Version Number         : 12.40
File Name                       : 01017992_1.pdf
Directory                       : /tmp/recuperados/pdf
File Size                       : 2.9 MiB
File Modification Date/Time     : 2024:02:26 16:40:27-05:00
File Access Date/Time           : 2024:02:26 16:40:27-05:00
File Inode Change Date/Time     : 2024:02:26 16:40:27-05:00
File Permissions                : -rw-rw-r--
Error                           : File format error
======== /tmp/recuperados/pdf/01017992.pdf
ExifTool Version Number         : 12.40
File Name                       : 01017992.pdf
Directory                       : /tmp/recuperados/pdf
File Size                       : 2.9 MiB
File Modification Date/Time     : 2024:02:26 16:40:27-05:00
File Access Date/Time           : 2024:02:26 16:40:27-05:00
File Inode Change Date/Time     : 2024:02:26 16:40:27-05:00
File Permissions                : -rw-rw-r--
Error                           : File format error
======== /tmp/recuperados/pdf/01751880.pdf
ExifTool Version Number         : 12.40
File Name                       : 01751880.pdf
Directory                       : /tmp/recuperados/pdf
File Size                       : 118 KiB
```

/ tmp / rec... os / pdf

Recent
Starred
Home
Desk
Docu
Down
Musi
Pictu
Vide
Trash
Imag
Othe

01017992.pdf 01017992_1.pdf 01751880.pdf 01752144.pdf

1 of 7 01751880.... 54.7%

Abstract 1
Introduction 1
Basic error ar... 1
Soft errors v... 2
Logging 3
Error account... 3
Bad page offl... 4
Cache error h... 5
Deployment 6
Conclusion 6

mcelog: memory error handling in user space

Andi Kleen
Intel®Corporation
andi@firstfloor.org

1 Abstract

Memory error handling is an increasingly important topic. The paper describes memory error handling in user space on Linux systems using the mcelog daemon. It describes features like bad page offlining or cache error handling that improve the uptime of server systems.

2 Introduction

Servers and high-performance computing systems contain more and more memory to handle bigger data sets. But with more and larger memory modules, and more transistors in them, combined with larger clusters of systems, the rate of memory errors in operation is also increasing.

Modern server systems generally use ECC memory and other ways to detect and correct many memory errors in the hardware. When the hardware corrects an error it generates corrected error events. These events can be also used by specialized software to prevent future failures.

mcelog is a daemon for handling and reporting hardware errors. It is able to use trends in corrected error reports to implement specific error prevention algorithms.

3 Basic error architecture

A modern x86 server CPU with an integrated memory controller memory and ECC memory constantly checks for memory data errors and corrects and reports them. For this it uses techniques like patrol scrubbing and demand scrubbing and also computes the checksum of all data read from memory.[1]. Errors will be usually reported to the operating system using the standard x86 machine check architecture (MCA) registers. Uncorrected memory errors – that is data corruption – are reported using a machine check exception and handled directly by the kernel, for example by killing the affected process or shutting down the system down.

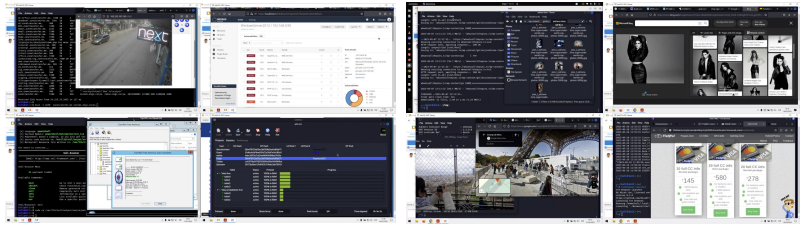
Corrected errors are polled by a timer or interrupt handler[1] and reported to the mcelog daemon. The mcelog daemon decodes the error and does accounting and other book keeping. The rest of the paper will discuss the various actions implemented in the mcelog daemon.

Traditionally mcelog was run as a crontjob, but in newer distributions it supports a daemon mode started by an init script. It is recommended to ensure the daemon is always running on every system with ECC memory. [2]

More information on the basic architecture can be found in [1] and the hardware architecture is described in [3].

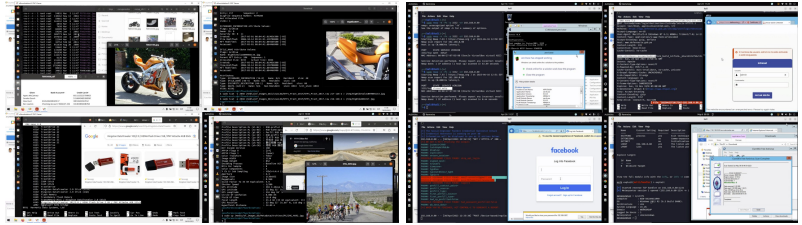
Cursos Disponibles en Video

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



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

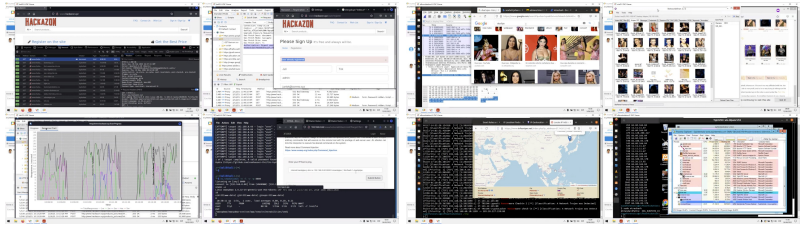
Curso Informática Forense
https://www.reydes.com/d/?q=Curso_de_Informatica_Forense



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

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

Curso 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 webinars

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

Diapositivas de webinars

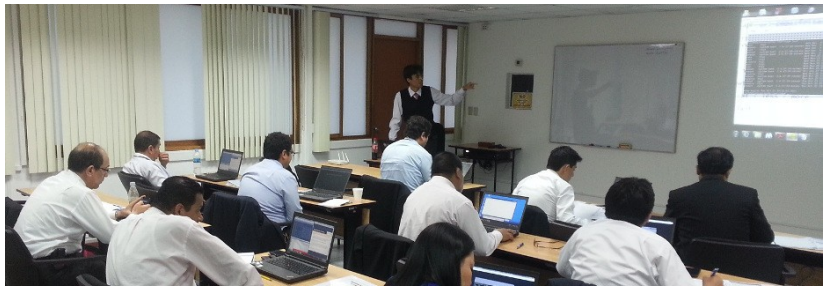
https://www.reydes.com/d/?q=eventos

Libros y artículos

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

Blog

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



Webinar Gratuito

Análisis Forense a Linux

Alonso Eduardo Caballero Quezada

Instructor y Consultor Independiente en Ciberseguridad

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Jueves 29 de Febrero 2024