Webinar Gratuito

REMnux

Alonso Eduardo Caballero Quezada

| Hacking | Forense | Linux | OSINT | Ciberseguridad |

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

Miércoles 20 de Agosto 2025

Alonso Eduardo Caballero Quezada

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). Cuento con más de dieciocho años de experiencia en el área y desde hace catorce años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital.

Redes Sociales

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

https://x.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

REMnux

REMnux es un conjunto de herramientas GNU/Linux para realizar ingeniería inversa (reversa) y análisis de software malicioso (malware).

REMnux proporciona una colección seleccionada de herramientas libres creadas por la comunidad.

Los profesionales pueden utilizarlo para investigar malware sin el requerimiento de buscar, instalar, ni configurar las herramientas.

* REMnux: https://remnux.org/

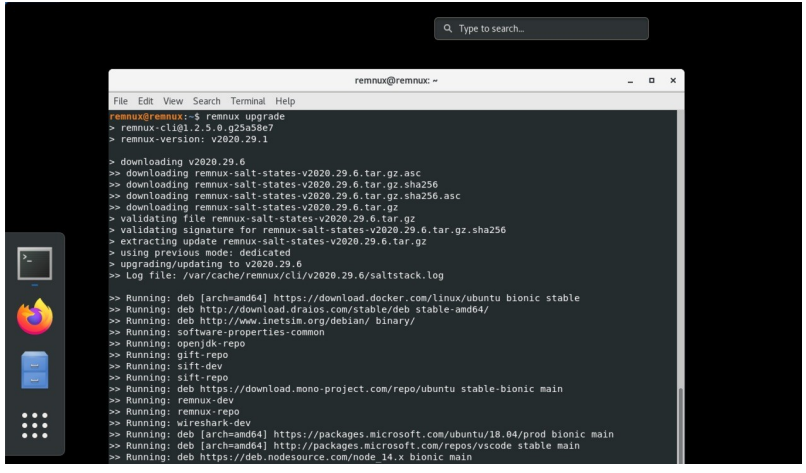
REMnux (Cont.)

REMnux está basada en Ubuntu, el cual incorpora muchas herramientas utilizadas por los profesionales en malware para:

- Examinar las propiedades estáticas de un archivo sospechoso
- Analizar estáticamente el código malicioso
- Realizar Ingeniería inversa dinámica a código malicioso
- Realizar forense de memoria de un sistema infectado
- Explorar las interacciones de red para realizar análisis de comportamiento

REMnux (Cont.)

- Investigar las interacciones a nivel del sistema del malware
- Analizar documentos maliciosos
- Recopilar y analizar datos sobre amenazas



Iniciar con REMnux

Para empezar a utilizar REMnux se puede:

- Descargar el appliance virtual de la distribución REMnux
- Instalar la distribución REMnux desde cero en un sistema dedicado
- Añadir la distribución REMnux hacia una máquina existente
- Ejecutar la distribución REMnux como un contenedor Docker

* REMnux Documentation: https://docs.remnux.org/

Curso Análisis de Malware

Curso Análisis de Malware

Sábado 23 y Sábado 30 de Agosto del 2025
De 9:00am a 12:00pm (UTC -05:00)

Las clases en vivo se quedan grabadas en el aula virtual

Presentación

El avance de la tecnología e Internet ha revolucionado la forma en la cual las organizaciones realizan sus negocios. Esta evolución consecuentemente genera también actividades maliciosas. La creciente amenaza de los ciberataques contra infraestructuras críticas, centros de datos, sector privado y público, defensa, energía, gobierno y finanzas, son un reto para todos los involucrados, desde una persona hasta las grandes empresas. Estos ciberataques utilizan software malicioso (también conocido como Malware) para realizar robo financiero, espionaje, sabotaje, robo de propiedad intelectual, o por motivos políticos.

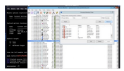
Dado el hecho los ciberdelincuentes son cada vez más sofisticados y realizan ataques de malware avanzados, detectar y responder a estas intrusiones es fundamental para los profesionales en ciberseguridad. El análisis de malware se ha convertido en una habilidad imprescindible para enfrentar el malware avanzado y los ataques dirigidos. El análisis de malware requiere un conocimiento equilibrado de muchas habilidades y temas diferentes.

Este curso proporciona los conceptos, herramientas y técnicas para comprender el comportamiento y las características de malware para Windows, realizando análisis de malware. Para comprender mejor los conceptos, se utilizan ejemplos y demostraciones prácticas durante todo el curso. Además se proporciona suficiente información para comprender los conceptos necesarios. Este curso ayuda a iniciarse en el ámbito del análisis de Malware, o si tiene experiencia en este campo, ayudará a mejorar conocimientos.

Temario

- ¿Qué es Malware?
- ¿Qué es el Análisis de Malware?
- ¿Porque Análisis de Malware?
- Tipos de Análisis de Malware
- REMnux
- theZoo
- Análisis Estático
- Determinar el Tipo de Archivo
- Identificar Tipo de Archivos con Métodos Manuales
- Huella del Malware
- Generar Hashes Criptográficos utilizando Herramientas
- Escaneo con Múltiples Antivirus
- Escanear el Archivo Sospechoso con VirusTotal
- Factores / Riesgos a Considerar
- Extraer Cadenas
- Extracción de Cadenas utilizando Herramientas
- Decodificar Cadenas Ofuscadas utilizando FLOSS
- Determinar Ofuscación del Archivos
- Packets y Cryptos
- Detectar Ofuscación de Archivos

- Inspeccionar la Información de la Cabecera PE
- Inspeccionar Dependencias e Importación del Archivo
- Inspeccionar Exportación
- Examinar Tabla de Sección y Secciones PE
- Examinar Marca de Tiempo de Compilación
- Examinar Recursos PE
- Comparar y Clasificar Malware
- Clasificar Malware utilizando Hashes Difusos
- Clasificar Malware utilizando Hashes Importados
- Clasificar Malware utilizando Hashes de Sección
- Clasificar Malware utilizando YARA
- Análisis Dinámico
- Vigilancia del Sistema y Red
- Herramientas para el Análisis Dinámico
- Determinar la Interacción del Sistema
- Registrar las Actividades del Sistema
- Capturar Tráfico de Red
- Etapas para un Análisis Dinámico
- Análisis de las DLLs
- Porque los Atacantes utilizan DLLs
- Analizar DLLs



Fechas y Horario

El Curso Análisis de Malware tiene una duración total de seis (6) horas, las cuales se dividen en dos (2) sesiones de un tres (3) horas de duración cada una.

- **Fechas:**

  Sábado 23 y Sábado 30 de Agosto del 2025

- **Horario:**

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

Beneficios e Inversión

- Acceso al aula virtual por 60 días
- Acceso a las sesiones en vivo
- Video de las dos (2) sesiones
- Acceso libre a las sesiones en vivo del siguiente curso a dictarse
- Material utilizado durante el desarrollo del curso
- Dos (2) horas de asesoría en vivo personalizada por videoconferencia
- Libro "Fundamentos de Forense Digital" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación por una duración total de 16 horas

S/. 225 Soles o $ 70 Dólares

El pago del curso se realiza mediante alguno de los siguientes mecanismos:

Residentes en Perú	Residentes en Otros Paises
Deposito bancario o transferencia interbancaria en la siguiente cuenta. O también YAPE o PLIN. Scotiabank yape plin	Pago a través de PayPal. O también transferencia de dinero mediante Western Union y MoneyGram PayPal
Escriba por favor un mensaje al WhatsApp https://wa.me/51949304030 o reydes@gmail.com para proporcionarle los datos pertinente para realizar el pago.	Escriba por favor un mensaje al WhatsApp https://wa.me/51949304030 o reydes@gmail.com para proporcionarle los datos pertinente para realizar el pago.

Confirmado el pago se enviará al correo electrónico del participante, los datos necesarios para conectarse hacia la plataforma, además de toda la información pertinente para su participación en el curso

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 | (WhatApp): https://wa.me/51949304030

Sitio Web: https://www.reydes.com

Instructor

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 on 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). Cuento con más de dieciocho años de experiencia en el área y desde hace catorce años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Pertenecí por muchos años al grupo internacional RaredaCE y grupo Peruano PeruSEC. He dictado cursos para España, Ecuador, México, Bolivia y Perú, presentándome también en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Mi correo electrónico es ReYDeS@gmail.com y mi página personal está en: https://www.ReYDeS.com

Sitio Web:

www.reydes.com

Correo:

reydes@gmail.com

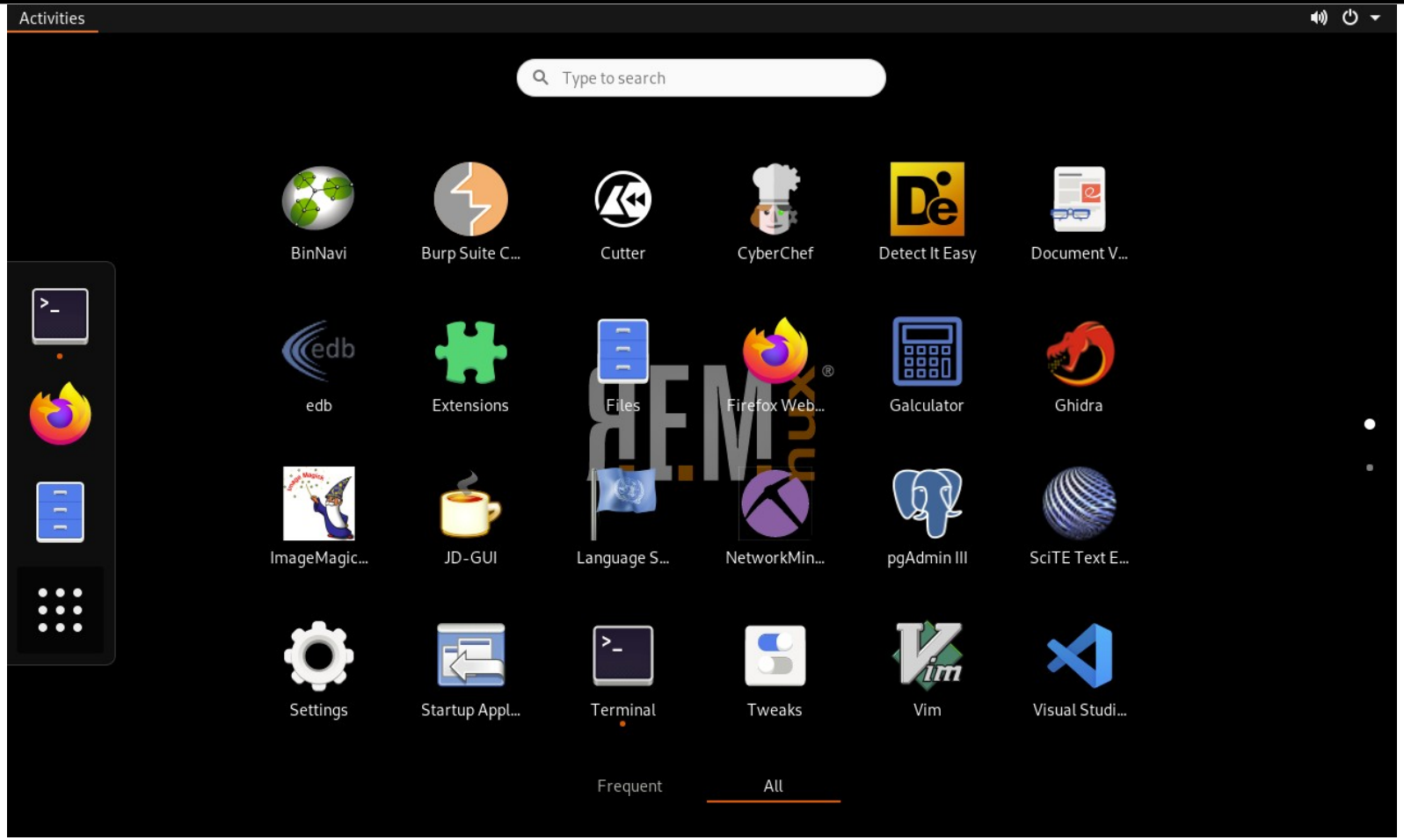
WhatsApp:

https://wa.me/51949304030

Más Información:

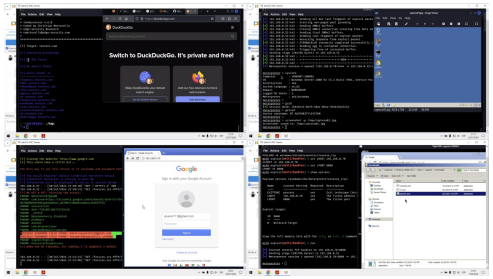
https://www.reydes.com/e/Curso_Analisis_Malware

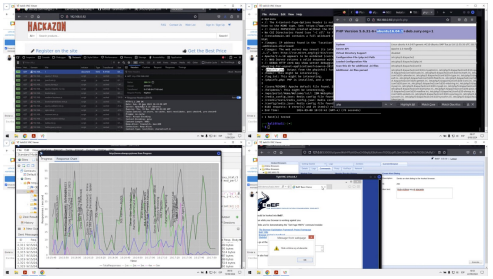
Prácticas

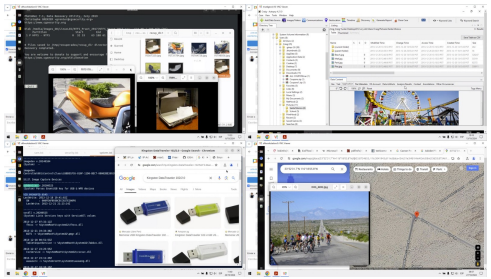

Activities
Type to search
BinNavi
Burp Suite C...
Cutter
CyberChef
Detect It Easy
Document V...
edb
Extensions
Files
Firefox Web...
Galculator
Ghidra
ImageMagic...
JD-GUI
Language S...
NetworkMin...
pgAdmin III
SciTE Text E...
Settings
Startup Appl...
Terminal
Tweaks
Vim
Visual Studi...
Frequent
All

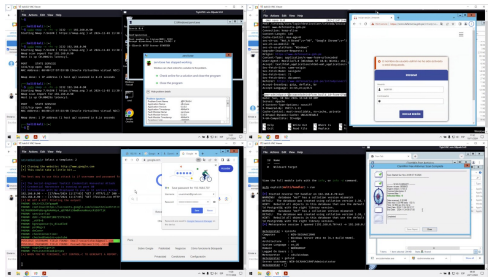
Cursos (Aula Virtual)

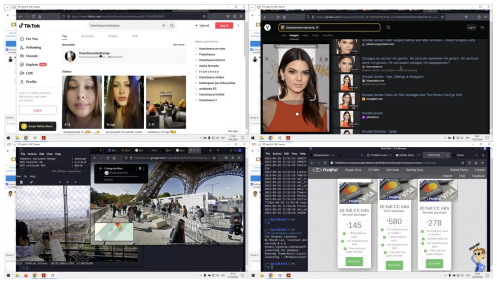
- Curso Hacking Ético
- Curso Hacking Aplicaciones Web
- Curso Informática Forense
- Curso Hacking con Kali Linux
- Curso OSINT - Open Source Intelligence
- Curso Forense de Redes
- Curso CiberSeguridad
- Curso Bug Bounty
- Curso OWASP Top 10
- Curso Análisis de Malware
- Curso Hacking OT
- Curso Maltego CE
- Y más...

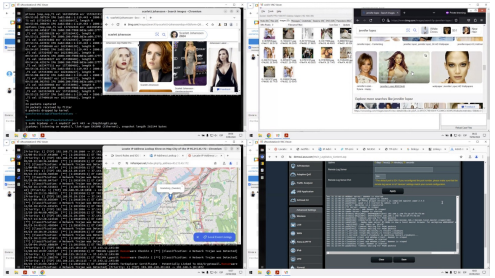












Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Más Contenidos

Videos de webinars

https://www.reydes.com/e/videos

Diapositivas de webinars

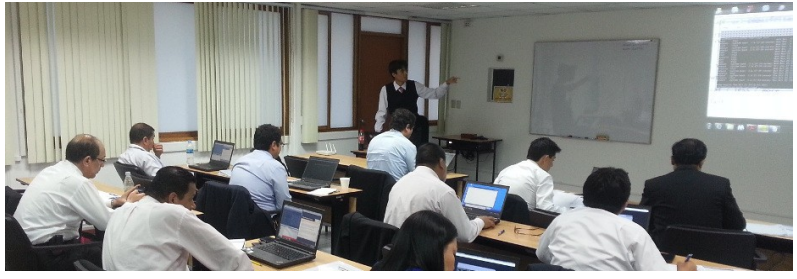
https://www.reydes.com/e/eventos

Libros y artículos

https://www.reydes.com/e/documentos

Blog

https://www.reydes.com/e/blog



Webinar Gratuito

REMnux

Alonso Eduardo Caballero Quezada

| Hacking | Forense | Linux | OSINT | Ciberseguridad |

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

Miércoles 20 de Agosto 2025