Taller Introducción al Pentesting

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 1ero de Setiembre 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

¿Qué es una Prueba de Penetración?

Se define como un intento legal y autorizado de encontrar y explotar infraestructura tecnológica, con el propósito de mejorar su seguridad.

El proceso incluye probar vulnerabilidades, como también proporcionar pruebas de concepto (PoC) de los ataques, para demostrar la existencia de las mismas.

Una Prueba de Penetración siempre finaliza con recomendaciones específicas para remediar y solucionar lo encontrado durante el desarrollo de la prueba.

“Este proceso es utilizado para ayudar a asegurar las redes y computadoras contra futuros ataques.”

Muchas veces se le denomina como pentesting, hacking, hacking ético, etc.

Conceptos Importantes

Los Hackers Éticos realizan procedimientos utilizando las mismas herramientas utilizadas por los atacantes maliciosos. El Hacker Ético debe pensar como un atacante malicioso.

Las Pruebas de Penetración simulan ataques reales, lo cual beneficia al cliente quién requiere estos servicios. Existe una palabra clave importante a considerar; **Autorización.**

La autorización implica obtener la aprobación antes de realizar las pruebas o ataques. Cuando se la obtiene, ambas partes acuerdan el alcance de la prueba, lo cual incluye los sistemas y recursos a evaluar. Siendo importante ambas partes entiendan el alcance y la autorización.

Otra manera de diferenciar a un Hacker Ético de un atacante malicioso son la Motivación y la Intención.

Laboratorio para Pruebas

Se debe tener un lugar para practicar y explorar. Pues NO es “Ético” atacar sistemas o redes sin autorización.

Un laboratorios de hacking es un entorno donde los ataques pueden ser realizados sin temor a quebrantar alguna ley o política. Siendo libre de explorar todas las herramientas y técnicas requeridas.

Como un paso extra de protección se puede crear un laboratorio aislado, donde no se permita ningún tipo de tráfico entrante o saliente desde/hacia el exterior.

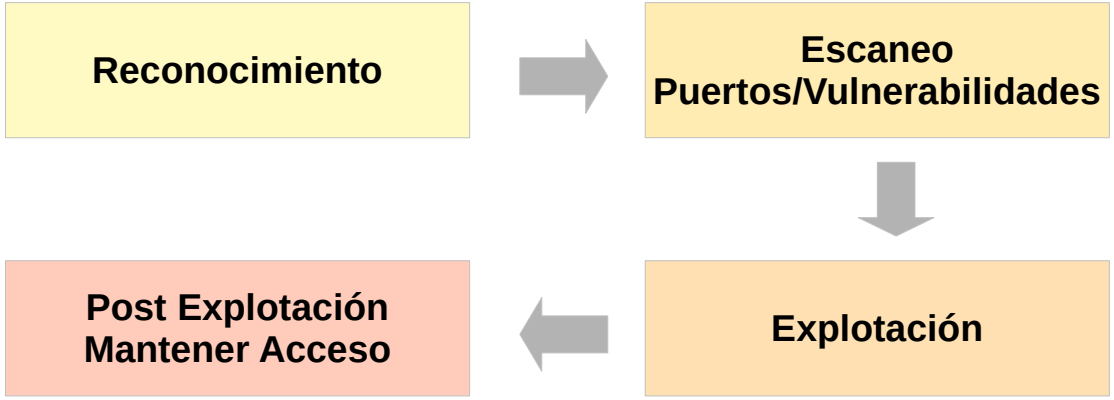
Se recomienda utilizar software para virtualización, los cuales permiten crear diversos escenarios de prácticas con diferentes sistemas operativos.

Las Pruebas de Penetración son un proceso destructivo, muchas herramientas y exploits puede generar mucho daño a los sistemas.

Etapas para una Prueba de Penetración

Existe un procedimiento para realizar una Prueba de Penetración. Siendo dividida en una serie de etapas o fases. Todas estas forman una metodología completa de una Prueba de Penetración.

Su utilización es importante, pues no solo mantiene la prueba enfocada y avanzando, sino porque permite utilizar los resultados de cada etapa en las etapas posteriores.



Kali Linux

Kali Linux es una distribución basada en el sistema operativo Linux Debian, de fuente abierta.

Esta distribución esta orientada a realizar auditorías de seguridad y pruebas de penetración.

Kali Linux contiene cientos de herramientas orientadas hacia las más diversas tareas relacionadas con la seguridad, como pruebas de penetración, investigación en seguridad, forense de computadoras, e ingeniería reversa.

Kali Linux es una solución multiplataforma, accedible y libremente disponible para todos los profesionales y aficionados a la seguridad de la información.

Características de Kali Linux

- Más de 300 herramientas para Pruebas de Penetración
- Es libre y siempre lo será
- Árbol Git de Fuente Abierta
- Cumplimiento con FHS (Filesystem Hierarchy Standard)
- Amplio soporte para dispositivos inalámbricos
- Kernel personalizado parchado para inyección
- Desarrollado en un entorno seguro
- Paquetes y repositorios firmados con GPG
- Soporte para múltiples lenguajes
- Completamente personalizable
- Soporte ARMEL y ARMHF

Reconocimiento

Es la más importante de las etapas, pues si más tiempo se invierte recolectando información, son más las probabilidades de tener éxito en las fases posteriores.

Irónicamente es también una de las etapas más obviadas, menos utilizadas, y menos comprendidas, en una metodología de Pruebas de Penetración.

Reconocimiento Activo

Implica interactuar directamente la infraestructura. Existen altas probabilidades de ser detectados durante este procedimiento.

Reconocimiento Pasivo

Utiliza una amplia cantidad de información disponible en la web. No se interactúa directamente con la infraestructura.

Curso Virtual Análisis de Malware

Domingos 11 y 18 de Setiembre del 2022. De 9:00am a 12:00am (UTC -05:00)

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

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.

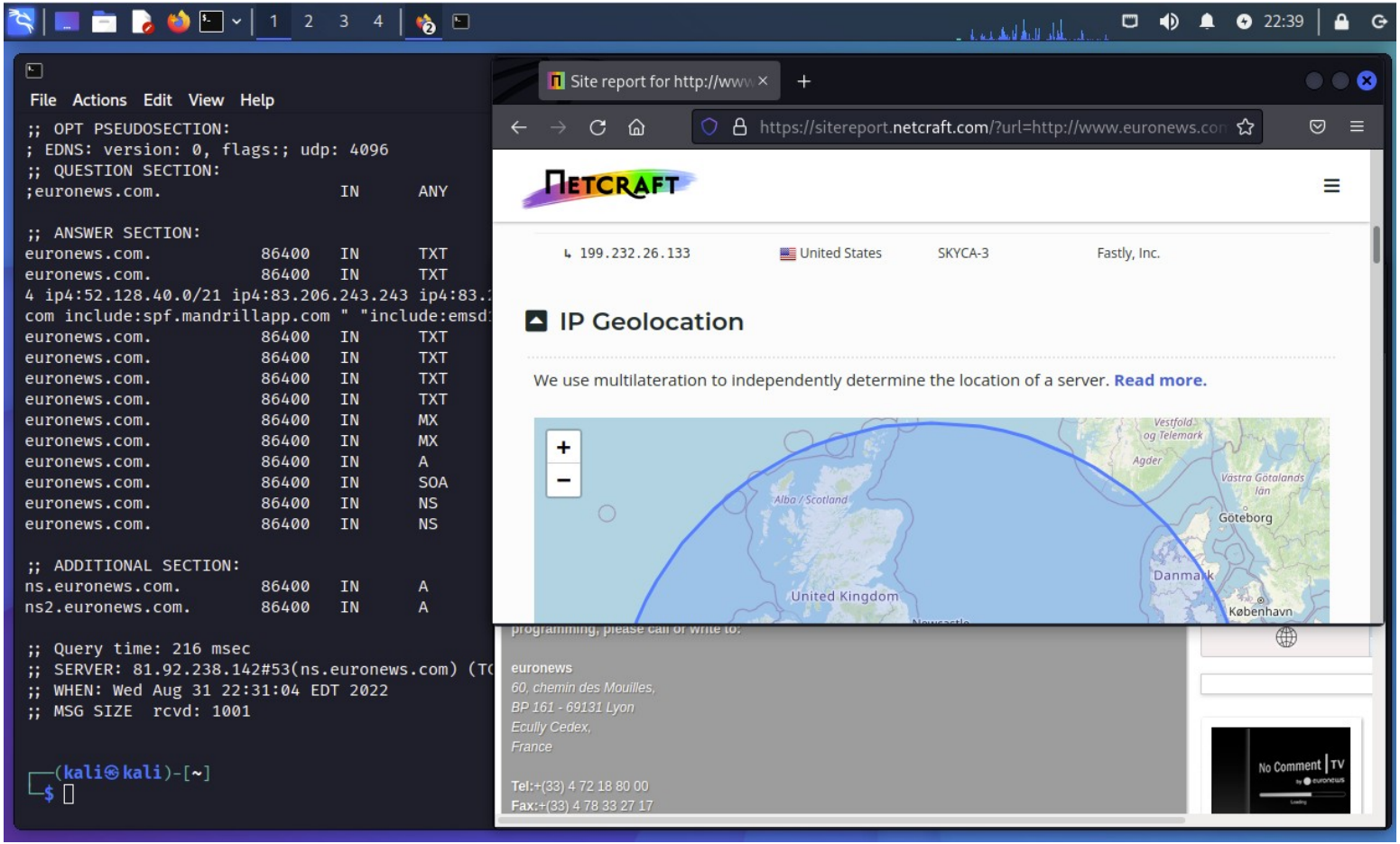
Dado el hecho los ciberdelincuentes son cada vez más sofisticados y realizan ataques de malware avanzados, detectar y responder a estas intrusiones es fundamental para los profesionales en ciberseguridad. El análisis de malware se ha convertido en una habilidad imprescindible para enfrentar el malware 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.

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

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

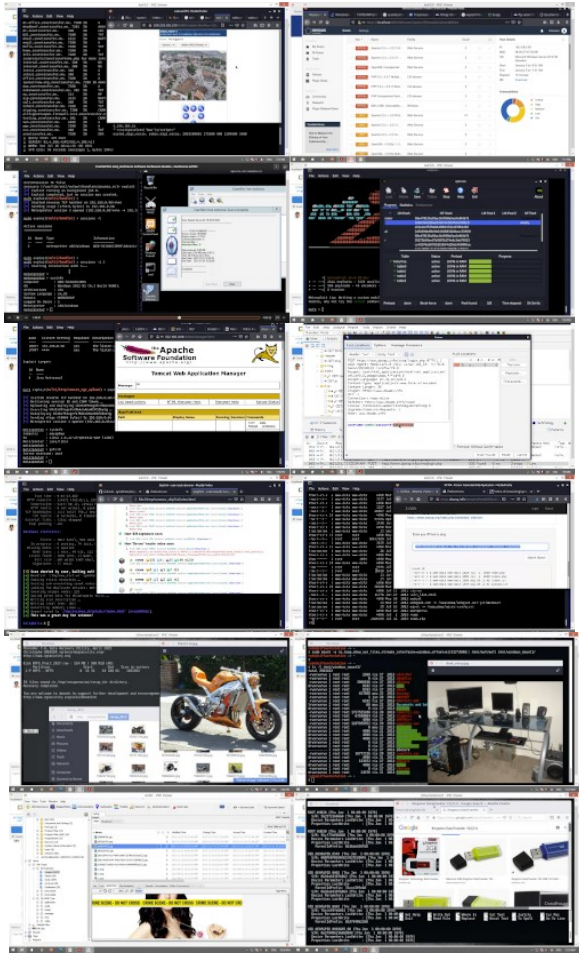
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

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 77 webinars gratuitos

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

Diapositivas de los webinars gratuitos

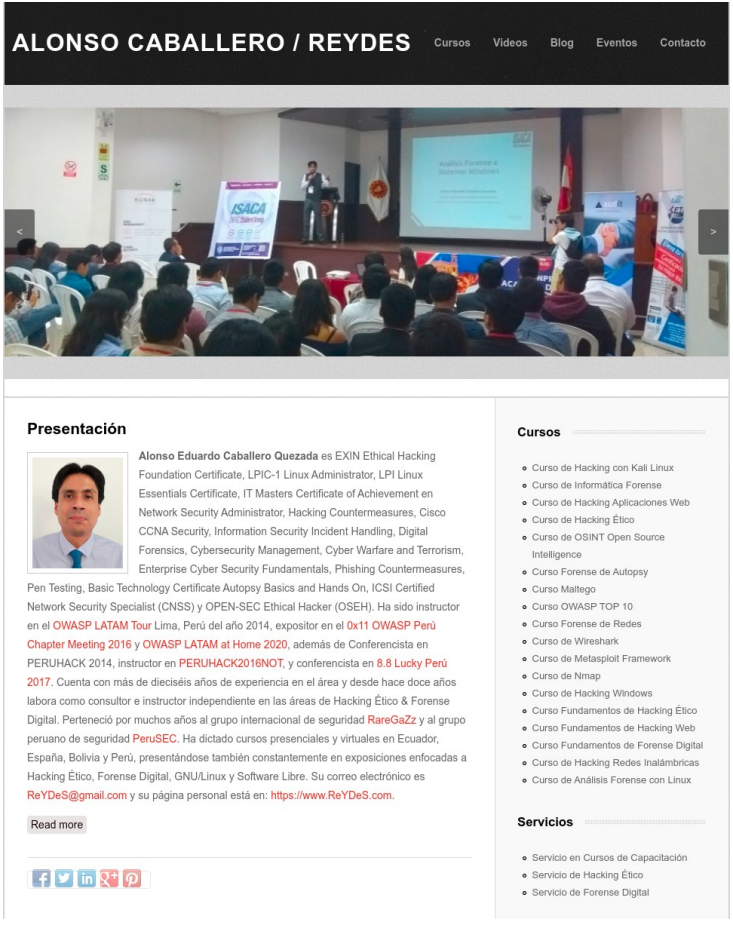
https://www.reydes.com/d/?q=eventos

Artículos y documentos publicados

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

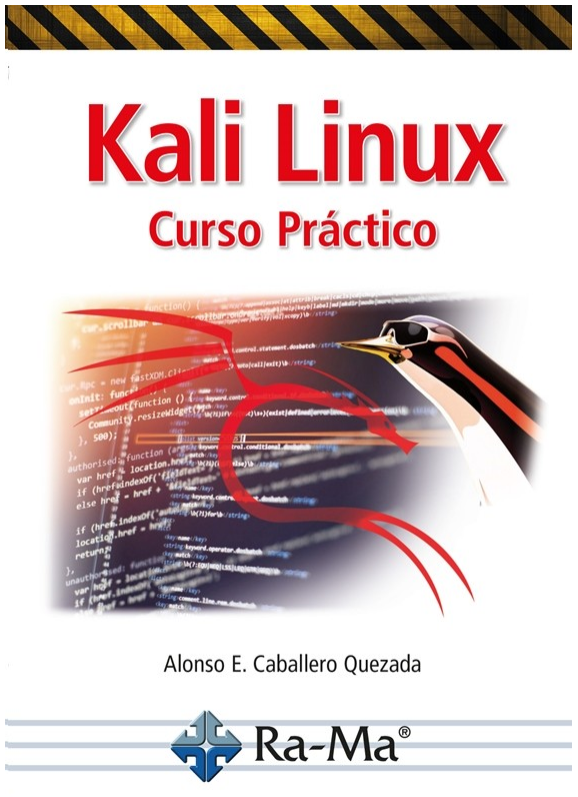
Blog sobre temas de mi interés

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



Kali Linux Curso Práctico

Mi propósito con el presente libro es mostrar las principales características y funcionalidades incluidas en Kali Linux. Todo esto realizado desde la perspectiva del Hacking Ético y Pruebas de Penetración, aunque de hecho también los contenidos expuestos pueden ser aplicados a diversos ámbitos, como auditorías de seguridad, evaluaciones de vulnerabilidades o seguridad, administración de redes y sistemas, entre otros.



En la siguiente página se puede comprar el Libro, ya sea en su edición en papel, como también en su versión electrónica (eBook).

* https://www.reydes.com/d/?q=Libro_Kali_Linux_Curso_Practico

Taller Introducción al Pentesting

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 1ero de Setiembre 2022