Taller Introducción al Pentesting Web

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 13 de Octubre 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

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

Aplicaciones Web

Las aplicaciones web son los objetivos más buscados para explotarlos, esto debido a su amplia utilización.

En la actualidad la web y por consiguiente las aplicaciones web, se integran en la vida diaria. Uno de sus principales beneficios es su portabilidad, y su adecuada funcionalidad en un amplio espectro de sistemas operativos.

Las aplicaciones web pueden ser utilizadas en una amplia variedad de escenarios, como almacenar, gestionar, y acceder a datos financieros sensibles o información personal. Los clientes pueden acceder a sus cuentas bancarias. Las empresas pueden utilizarlas para compartir propiedad intelectual, etc.

El alto valor de los datos accedidos mediante la utilización de aplicaciones web, incrementa su valor para su ataque.

Seguridad en Aplicaciones Web

Una gran cantidad de organizaciones se centra en realizar pruebas sobre la funcionalidad de las aplicaciones desarrolladas para la empresa, pero raramente realizan pruebas de seguridad.

Diariamente se reportan un gran cantidad de vulnerabilidades relacionadas y enfocadas en las aplicaciones web. Además con la creciente utilización de nuevas tecnologías, los sitios web hacen más de lo “perceptible”, lo cual añade nuevos vectores de ataque.

Típicamente el usuario hace clic en un enlace o imagen, la petición va hacia el servidor, y luego se devuelve un resultado conteniendo la página web. Para el caso de Ajax por ejemplo, se interactua con el sitio, se ejecuta código JavaScript para realizar llamadas y recabar datos desde el servidor. De esta manera las páginas son actualizadas dinámicamente con los datos recibidos.

Pruebas de Penetración contra Aplicaciones Web

Para realizar pruebas de penetración exitosamente contra aplicaciones web, se requiere tener un buen conocimiento; más allá del nivel de un usuario normal; sobre las tecnologías web. Entender como su funcionamiento desde la perspectiva del desarrollador o administrador web.

De esta manera los profesionales en pruebas de penetración deben pensar de manera maliciosa pero actuando profesionalmente. Deben preguntarse como sería factible evadir las restricciones, analizar cuales podrían ser los errores cometidos por los desarrolladores, administradores, y operadores del sistema.

Esta es una perspectiva de pensamiento completamente diferente a la de los desarrolladores o administradores. Lo cual permite enfocarse en evadir los controles de la aplicaciones, o encontrar problemas en lógica del negocio.

Pruebas de Penetración contra Aplicaciones Web

Una prueba de penetración debe seguir una metodología aprobada. Sin esto se perderían vulnerabilidades y no se completaría el trabajo. Esta metodología deben ser aprobada, repetible y explicable.

Además del utilizar una metodología, es fundamental conocer las herramientas. No es necesario recordar sus mil opciones, es suficiente estar familiarizado con las herramientas existentes para realizar el trabajo.

El obtener permiso es el elemento más crítico, debido a la existencia de legislaciones sobre hacking. Si no se tiene permiso para evaluar la seguridad de una aplicación entonces no se debe evaluarla.

Ejemplo: “Accidentalmente” se descubrió una falla de inyección “SQL” en el sitio web de una página del gobierno.

Tipos de Pruebas de Penetración

- **Caja Negra:** Implica una evaluación sin conocimiento, lo cual es bastante atípico.

- **Caja Blanca:** Una prueba de seguridad con completo conocimiento, con acceso hacia el código fuente, cuentas de la aplicación, conocimiento sobre la arquitectura de la aplicación, y acceso hacia los desarrolladores.

- **Caja Gris:** Muchas pruebas legítimas aterrizan en un área gris entre pruebas negras (sin conocimiento), y blancas (completo conocimiento).

Cuanto más oscuro es el color, más oscuro está el profesional en pruebas de penetración, sobre aquello lo cual está evaluando.

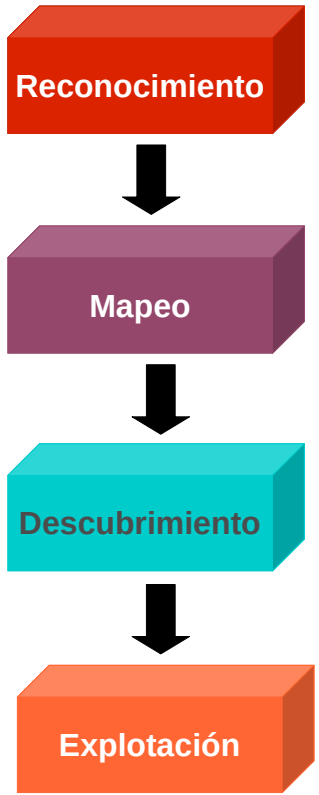
Metodología para una Prueba de Penetración

Reconocimiento: Proporciona los fundamentos para un ataque satisfactorio y eficiente. Se trata de identificar aquello a evaluar mediante diversos recursos.

Mapeo: Implica entender como funciona la aplicación (lógica) y su infraestructura subyacente. Identificar los diversos elementos de la aplicación y sus relaciones.

Descubrimiento: Se inicia una exploración más profunda de la aplicación; ya sea manual o automática; para encontrar las potenciales vulnerabilidades e información para el ataque.

Explotación: Se utiliza toda la información obtenida para explotar las vulnerabilidades identificadas en la aplicación.



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

Curso Virtual Bug Bounty

Domingos 16 y 23 de Octubre 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

Un programa de Bug Bounty o recompensa por fallas, es un acuerdo ofrecido por muchos sitios web, organizaciones, y desarrolladores de software, por el cual los profesionales en hacking reciben un reconocimiento y compensación económica por descubrir y reportar con éxito fallas, especialmente aquellas relacionadas con vulnerabilidades y explotación en ciberseguridad.

Los profesionales en hacking a nivel mundial cazan fallas, y en algunos casos obtienen ingresos económicos a tiempo completo. Los programas de bug bounty atraen una amplia diversidad de profesionales con diferentes niveles de habilidades y experiencia, lo cual permite a las empresas aprovecharse de pruebas factibles de ser utilizadas por equipos de seguridad menos experimentados para identificar vulnerabilidades.

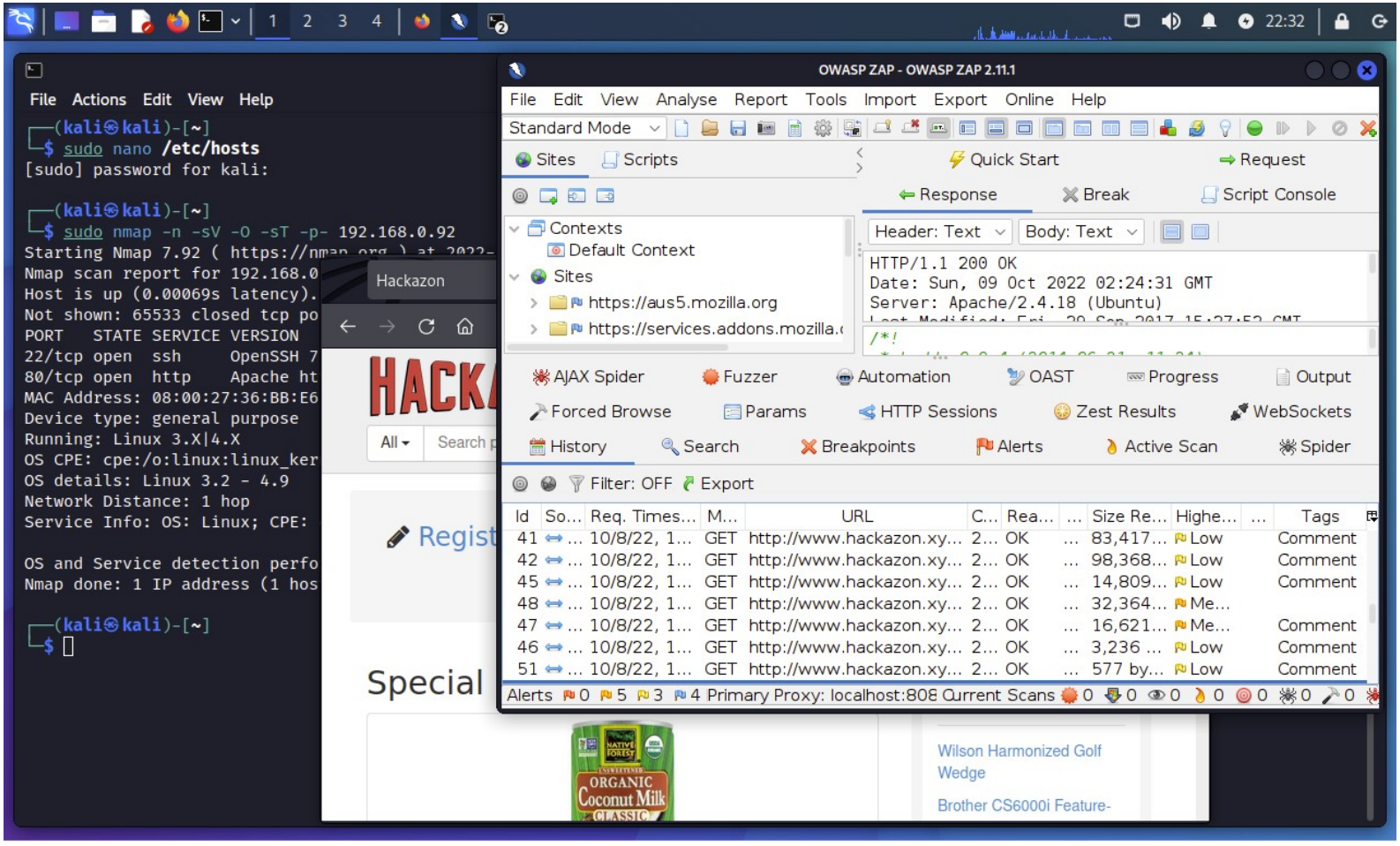
Los programas de recompensas frecuentemente complementan las pruebas de penetración, y proporcionan una manera para las organizaciones prueben la seguridad de sus aplicaciones a través de un ciclo de vida para desarrollo.

El propósito del curso es proporcionar a los participantes los conocimientos necesarios para convertir su interés en ciberseguridad, en una actividad divertida y rentable. Aplicando los conocimientos adquiridos para centrarse en descubrir vulnerabilidades en entornos reales.

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

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

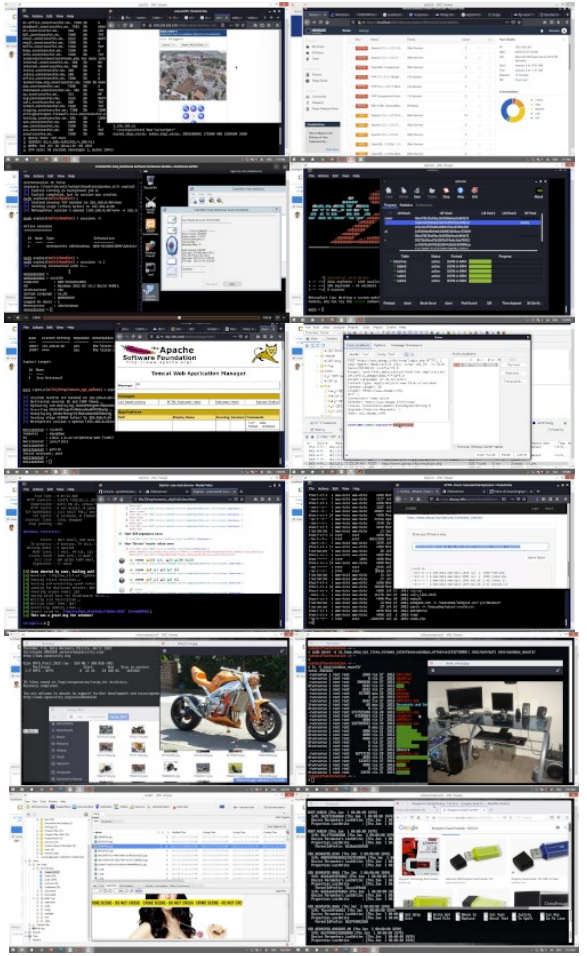
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

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

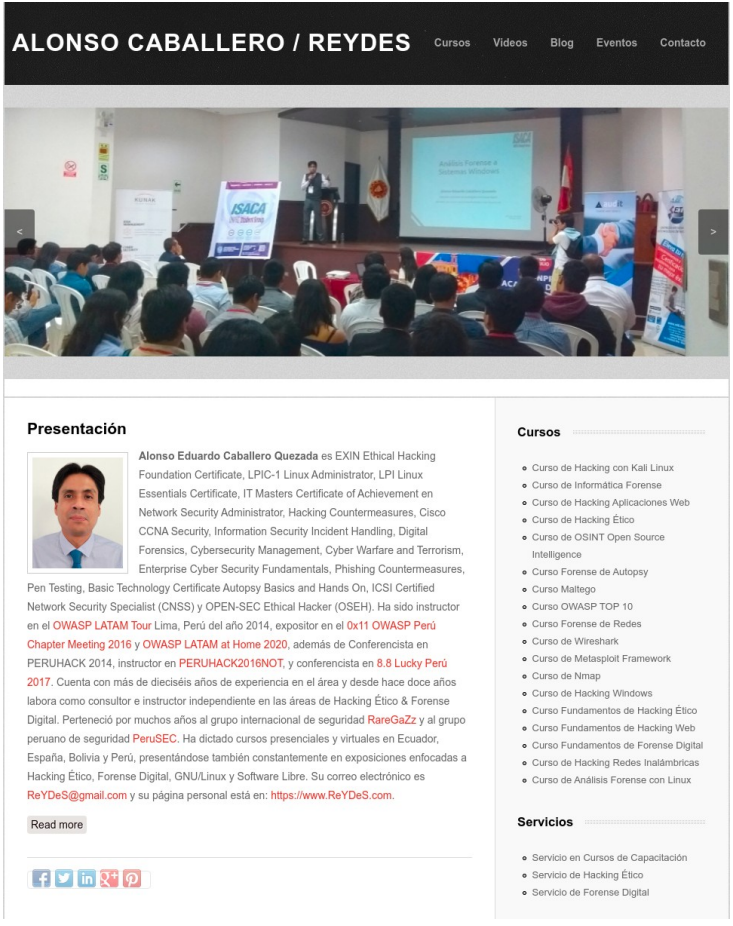
https://www.reydes.com/d/?q=eventos

Artículos y documentos publicados

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

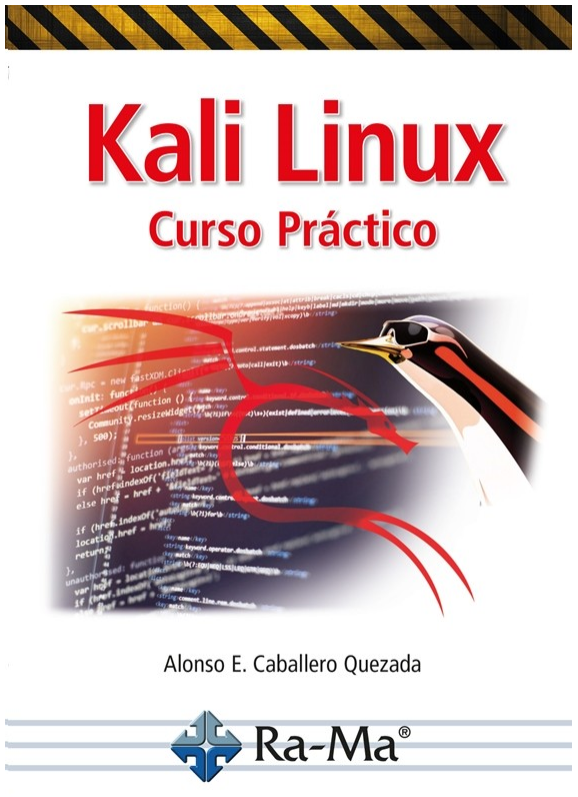
Blog sobre temas de mi interés

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 Web

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 13 de Octubre 2022