Webinar Gratuito

Escaneos con Scripts de Nmap para Hacking Web

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

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

Jueves 15 de Junio 2023

Alonso Eduardo Caballero Quezada

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 19 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

Nmap

Es una utilidad gratuita de fuente abierta para el descubrimiento de redes, auditoría en seguridad. Muchos administradores de sistemas y redes lo utilizan para tareas como; inventario de redes, gestión de programas para actualización de servicios, y supervisión del tiempo de actividad del host o servicio.

Nmap utiliza paquetes de IP en bruto para determinar cuales hosts están disponibles en la red, cuales servicios ofrecen estos hosts, cuales sistemas operativos están ejecutando, cual tipo de filtros para paquetes/cortafuegos utilizan, y docenas de otras características.

Diseñado para escanear rápidamente grandes redes, pero funciona bien contra hosts individuales.

* Nmap: https://nmap.org/

Nmap Scripting Engine

El Motor de Guiones para Nmap (NSE), es una de las funcionalidades más potentes y flexibles de Nmap. Permite a los usuarios escribir (y compartir) scripts sencillos para automatizar una amplia variedad para tareas de red. Luego estos scripts se ejecutan en paralelo con la velocidad y eficiencia esperada de Nmap. Los usuarios confían en el creciente y diverso conjunto de scripts distribuidos con Nmap, o escribir los propios para satisfacer necesidades personalizadas.

- Deteccion de redes
- Detección más sofisticada de versiones
- Detección de vulnerabilidades
- Detección de puerta trasera (backdoor)
- Explotación de vulnerabilidades

* Nmap Scripting Engine: https://nmap.org/book/nse.html

Tipos de Scripts y Fases

NSE soporta cuatro tipos de scripts, los cuales se distinguen por el tipo de objetivo los cuales toman, y la fase de escaneo en el cual son ejecutados. Scripts individuales pueden soportar múltiples tipo de operación

- **Scripts previas a la regla:** Se ejecuta antes de cualquier fase de escaneo de Nmap, por lo cual Nmap no ha recolectado ninguna información
- **Scripts para host:** Se ejecutan durante el proceso de escaneo, después de haberse realizado descubrimiento, escaneo de puertos, versiones, OS.
- **Scripts para el servicio:** Se ejecutan contra servicios específicos atendiendo en el host
- **Scripts posteriores a la regla:** Se ejecutan después de escanear todos los hosts

Hacking Web

Una aplicación web es accedida por los usuarios a través de una red. El término también puede significar una aplicación de software codificada en HTML, JavaScript, y otras tecnologías.

Hacking web se refiere a la explotación de aplicaciones mediante HTTP, lo cual se puede realizar manipulando la aplicación a través de su interfaz web gráfica, manipulando el Identificador Uniforme de Recursos (URI), o manipulando elementos HTTP no contenidos en el URI. Los métodos factibles de utilizar para "hackear" aplicaciones web son; ataques de inyección SQL, Cross Site Scripting (XSS), Cross Site Request Forgeries (CSRF), comunicaciones inseguras, etc.

Como profesional en hacking ético, se debe evaluar las aplicaciones web buscando diferentes tipos de vulnerabilidades, para consecuentemente intentar proteger las aplicaciones web de tales ataques.

Curso Virtual Fundamentos Hacking Web

Sitio Web:

www.reydes.com

Correo:

reydes@gmail.com

Más Información:

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

Fundamentos de Hacking Web

Domingos 18 y 25 de Junio del 2023. 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

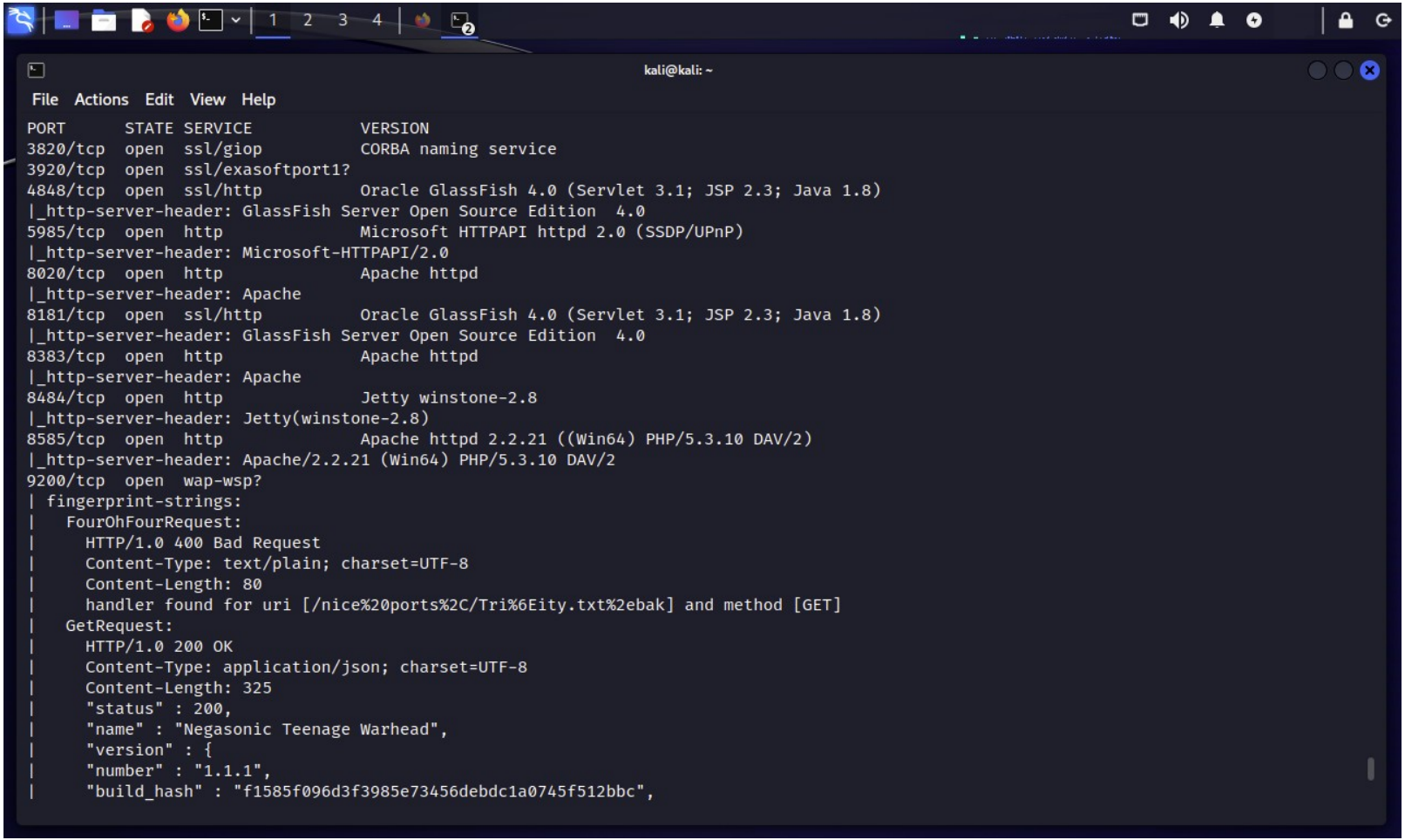
En la actualidad todos nosotros confiamos en las aplicaciones web para realizar diversas tareas diarias, ya sea en el trabajo, en casa, o para diversión; siendo posible accederlas numerosas veces al día desde; utilizando laptops, computadoras, tablets, teléfonos inteligentes, y otros dispositivos. Estas aplicaciones web son utilizadas para realizar compras, transacciones bancarias, pagos de cuentas, interactuar a través de redes sociales, y muchos otros propósitos. El problema con las aplicaciones web es no ser tan seguras como se piensa, y la mayoría de las veces los ataques utilizados para ganar acceso son relativamente sencillos y simples. De hecho cualquiera puede utilizar herramientas de hacking para realizar ataques devastadores.

Objetivos

Este curso enseña a los participantes como realizar evaluaciones de seguridad contra aplicaciones web, de tal manera se pueda también prevenir los ataques. Se abarca la teoría, herramientas, y tecnologías utilizadas para identificar y explotar las vulnerabilidades web más frecuentes y dañinas presentes en las aplicaciones web. Esto significa tener la capacidad de obtener información sensible desde una base de datos, evadir una página de autenticación, o realizar la suplantación de usuarios. Se aprenderá sobre la selección del objetivo a evaluar, como realizar los ataques, cuales herramientas son necesarias, y como utilizarlas adecuadamente.

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

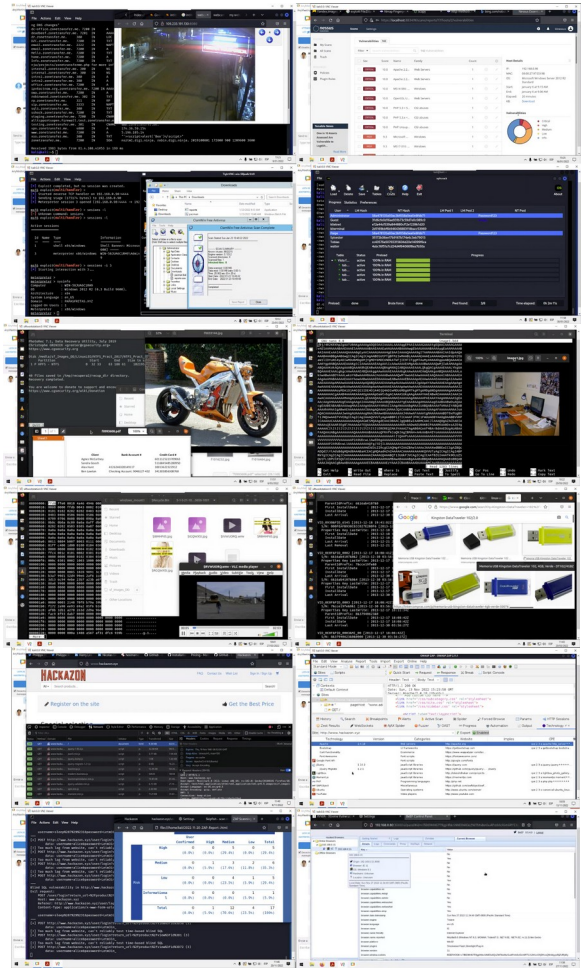
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

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 84 webinars gratuitos

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

Diapositivas de los webinars gratuitos

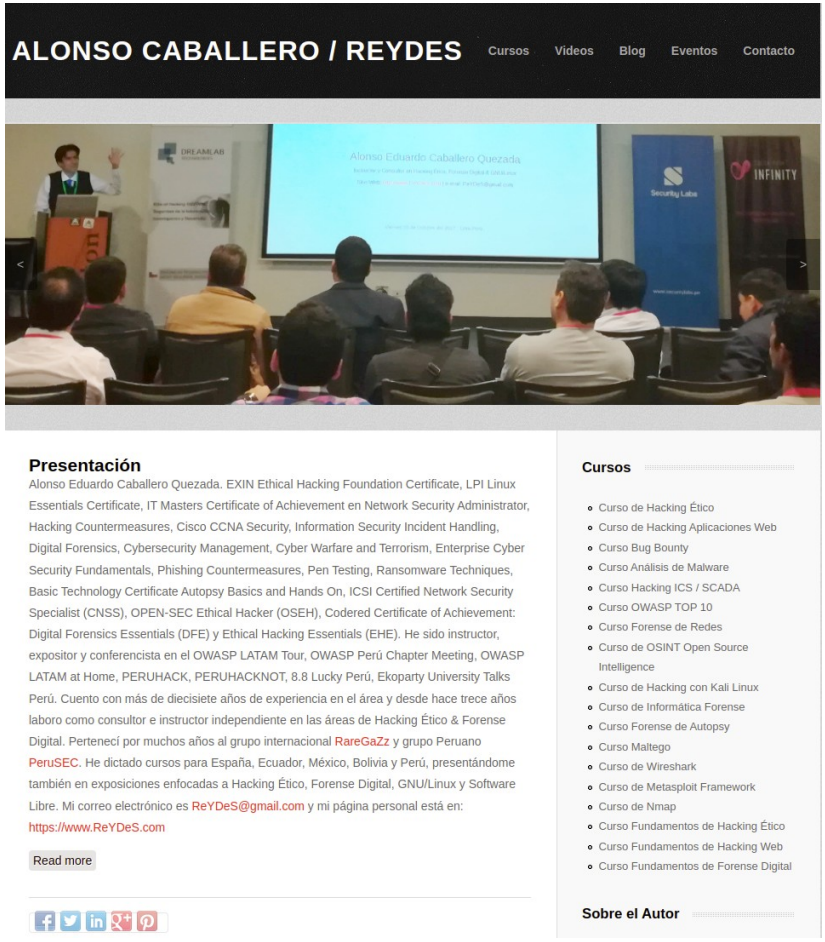
https://www.reydes.com/d/?q=eventos

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



Webinar Gratuito

Escaneos con Scripts de Nmap para Hacking Web

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

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

Jueves 15 de Junio 2023