Webinar Gratuito

Metasploit Framework

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 30 de Junio 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

Metasploit Framework

Es una plataforma modular para pruebas de penetración basada en Ruby, la cual permite escribir, evaluar, y ejecutar códigos para explotación.

Contiene un conjunto de herramientas factibles de ser utilizadas para evaluar vulnerabilidades de seguridad, enumerar redes, ejecutar ataques, y evadir detección.

En su núcleo Metasploit Framework es una colección de herramientas comúnmente utilizadas, para proporciona un completo entorno para pruebas de penetración y desarrollo de exploits.

* https://github.com/rapid7/metasploit-framework
* https://docs.rapid7.com/metasploit/msf-overview/

Módulos

Exploit

Un modulo exploit ejecuta una secuencia de comandos contra una vulnerabilidad específica encontrada en un sistema o aplicación. Un módulo exploit se aprovecha de una vulnerabilidad para proporcionar acceso hacia el sistema. Los módulos exploits incluyen desbordamiento de buffer, inyección de código, y exploit de aplicación web.

Auxiliary

Un módulo auxiliar no ejecuta un payload. Puede ser utilizado para realizar acciones arbitrarias, las cuales pueden no estar directamente relacionadas con la explotación. Ejemplos de módulos auxiliares incluyen escáneres, fuzzers, y ataque para negación de servicio.

Módulos (Cont.)

Post

Un modulo de post explotación permite obtener más información, o ganar más acceso hacia el sistema explotado. Ejemplos de módulos para post explotación incluyen volcar hashes, además de enumerar servicios y aplicaciones.

Payload

Un payload es un código shell el cual se ejecuta después de un exploit exitosamente compromete un sistema. El payload permite definir como se desea conectar hacia la shell, y aquello lo cual se requiere hacer en el sistema después de tomar control. Un payload puede abrir un Meterpreter o shell de comandos. Meterpreter es un payload avanzado el cual permite escribir archivos DLL para dinámicamente crear nuevas funcionalidades conforme se requieran.

Interfaces

MSFVenom

MSFvenom es una combinación de las herramientas msfpayload y msfencode, colocando ambas herramientas en una sola instancia del Framework. Msfvenom reemplaza ambas herramientas desde junio del año 2015.

MSFconsole

MSFonsole es probablemente la interfaz más popular de Metasploit Framework. Proporciona una consola centralizada “todo en uno”, lo cual permite un acceso eficiente hacia virtualmente todas las opciones disponibles en el Framework. Podría resultar intimidatorio al inicio, pero una aprendida la sintaxis de los comandos se apreciará su poder.

Curso Virtual de Hacking Ético

Domingos 3, 10, 17 y 24 de Julio del 2022. De 9:00 am a 12:00 pm (UTC -05:00)

Este curso virtual ha sido dictado a profesionales de los siguientes países:

Presentación

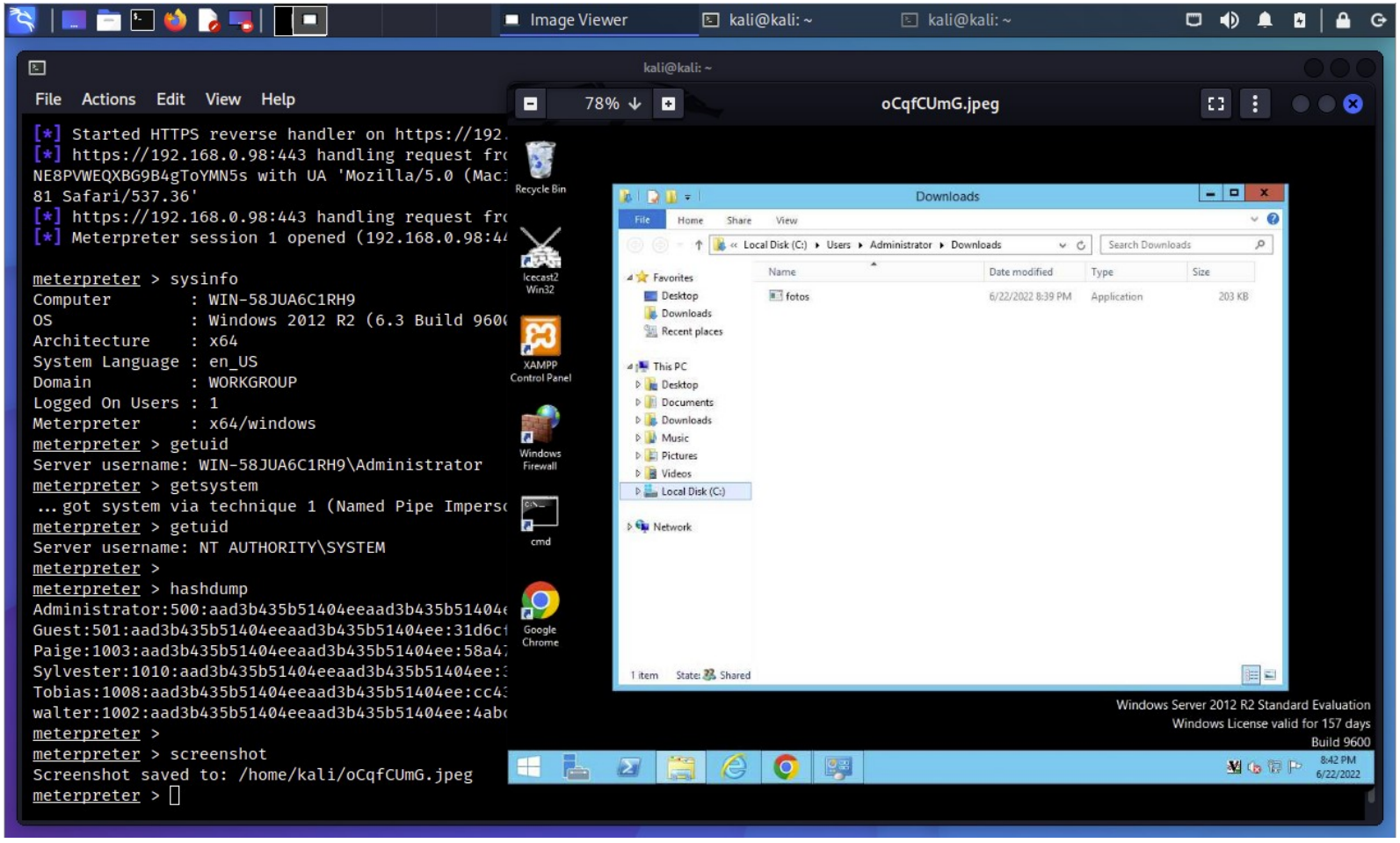
Como profesionales en ciberseguridad, se tiene la responsabilidad de encontrar y entender los riesgos de seguridad existentes en las organizaciones; para posteriormente trabajar de manera diligente en su mitigación; antes de estos riesgos sean aprovechados por los ciberatacantes. Este curso abarca las herramientas, técnicas, y metodologías para realizar pruebas de penetración contra redes y sistemas, preparándolo para realizar etapa por etapa pruebas de penetración y hacking ético. Todas las organizaciones necesitan profesionales experimentados en ciberseguridad, quienes estén en la capacidad de encontrar diversos tipos de vulnerabilidades, para así poder mitigar sus efectos. Este curso está específicamente diseñado desde esta perspectiva, siendo realizado con una gran cantidad de ejemplos y demostraciones prácticas.

Alonso Eduardo Caballero Quezada. EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, 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, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). He sido instructor, expositor y conferencista en el OWASP LATAM Tour,

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

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

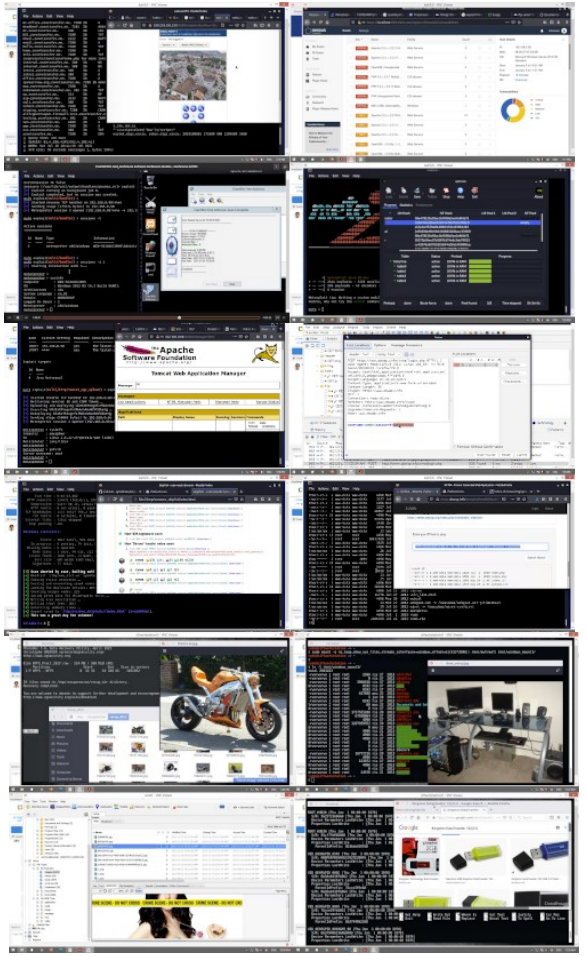
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

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

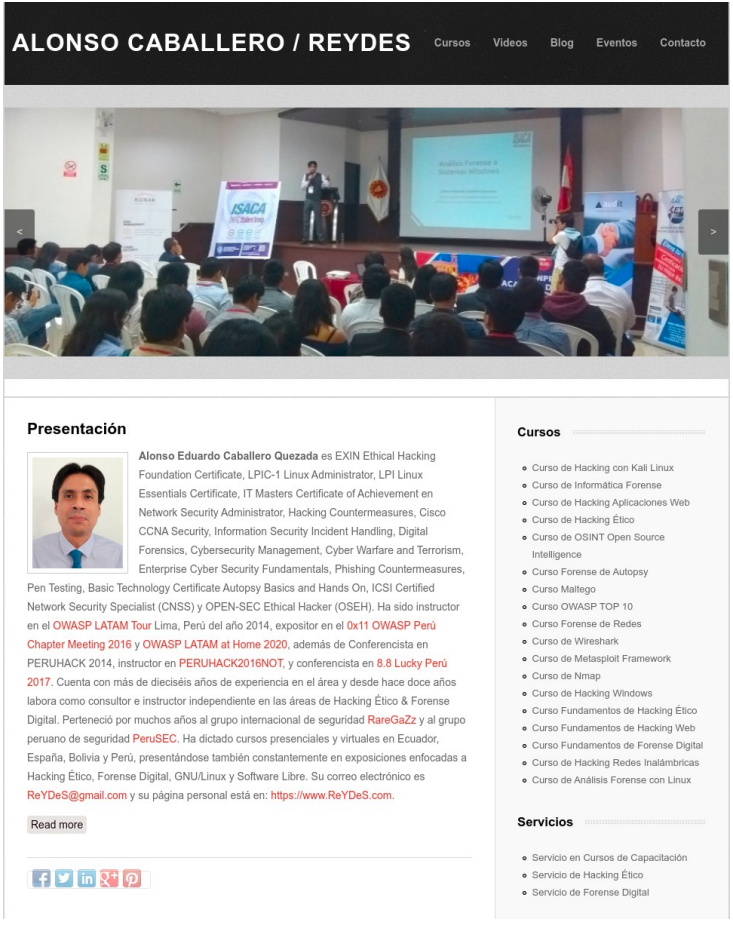
https://www.reydes.com/d/?q=eventos

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



Webinar Gratuito

Metasploit Framework

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 30 de Junio 2022