Webinar Gratuito

Metasploit Framework y el Firewall de Windows

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 8 de Julio del 2021

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.reydes.com

reydes@gmail.com

+51 949 304 030

Metasploit Framework

Es más a únicamente una colección de códigos para la explotación “Exploits”. Es una base muy sólida sobre la cual se puede fácilmente construir y personalizar requerimientos propios.

Metasploit Framework se considera una de las mejores y más útiles herramientas libremente disponibles para los profesionales de seguridad.

Incluye una amplia diversidad de exploits de nivel comercial, además de un amplio entorno para el desarrollo de exploits.

Incluyen módulos denominados; exploits, payloads, auxiliaries, encoders, etc.

* Metasploit Framework: https://github.com/rapid7/metasploit-framework

Payloads

Un Payload es un código shell el cual se ejecuta después de una explotación exitosa para comprometer un sistema. Un Payload permite definir como conectarse hacia la shell, además de aquello a realizar sobre el sistema después de controlarlo.

Puede abrir un Meterpreter o shell de comandos. Meterpreter es un Payload avanzado, el cual permite escribir archivos DLL para crear de manera dinámica nuevas funcionalidades conforme se requieran.

Un Payload puede ser reverso o enlazado. La principal diferencia entre estos Payloads es la dirección de la conexión después de ocurrida la explotación.

* Working with Payloads:
https://docs.rapid7.com/metasploit/working-with-payloads

Payloads Single y Staged

Un Payload Staged implica el Payload está constituido de dos componentes principales; un cargador pequeño y el cargador de etapa final. Cuando se entrega “windows/shell/reverse_tcp” hacia una máquina, se está enviando primero un cargador pequeño. Luego cuando este es ejecutado, solicitará al manejador (en el lado del atacante) enviar la etapa final (el cargador más grande), para finalmente obtener una shell.

Un Payload Single implica debe ser un tipo de cargador de “disparar y olvidar”. Este puede ser utilizado cuando aquello atacando no tiene acceso hacia la red.

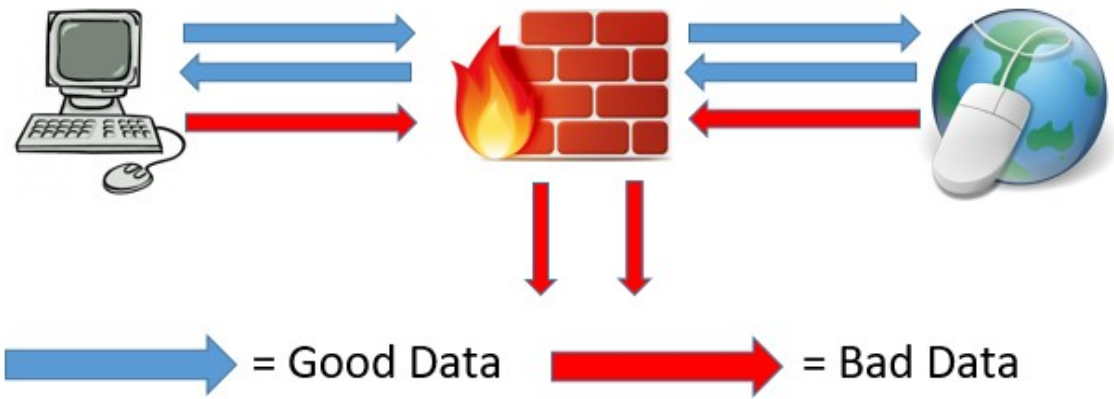
Meterpreter generalmente es el Payload más popular utilizando por Metasploit Framework.

* Working with Payloads:
https://docs.rapid7.com/metasploit/working-with-payloads

Firewall

Un cortafuegos es un sistema para la seguridad de redes, el cual vigila y controla tráfico de red entrante y saliente, basándose en reglas de seguridad previamente determinadas.

Un típico cortafuego establece una barrera entre una red fiable y una red no fiable, como Internet.



* Firewall: https://en.wikipedia.org/wiki/Firewall_(computing)

Firewall de Windows

Es una parte importante de un modelo para seguridad por capas. Proporciona filtrado para tráfico de red de dos direcciones basado en host para una computadora, bloqueando tráfico no autorizado fluyendo desde y hacia la computadora local.

Entre sus aplicaciones prácticas se tienen:

- Reduce el riesgo sobre amenazas de seguridad en redes
- Salvaguarda los datos sensibles y de propiedad intelecual
- Extiende el valor de la inversión existente

* Windows Firewall with Advanced Security Overview: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831365(v=ws.11
)

Curso

Curso Virtual Hacking Ético 2021

Sábados 10, 17, 24 y 31 de Julio 2021. De 9:00 am a 12:15 pm (UTC -05:00)

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

Presentación

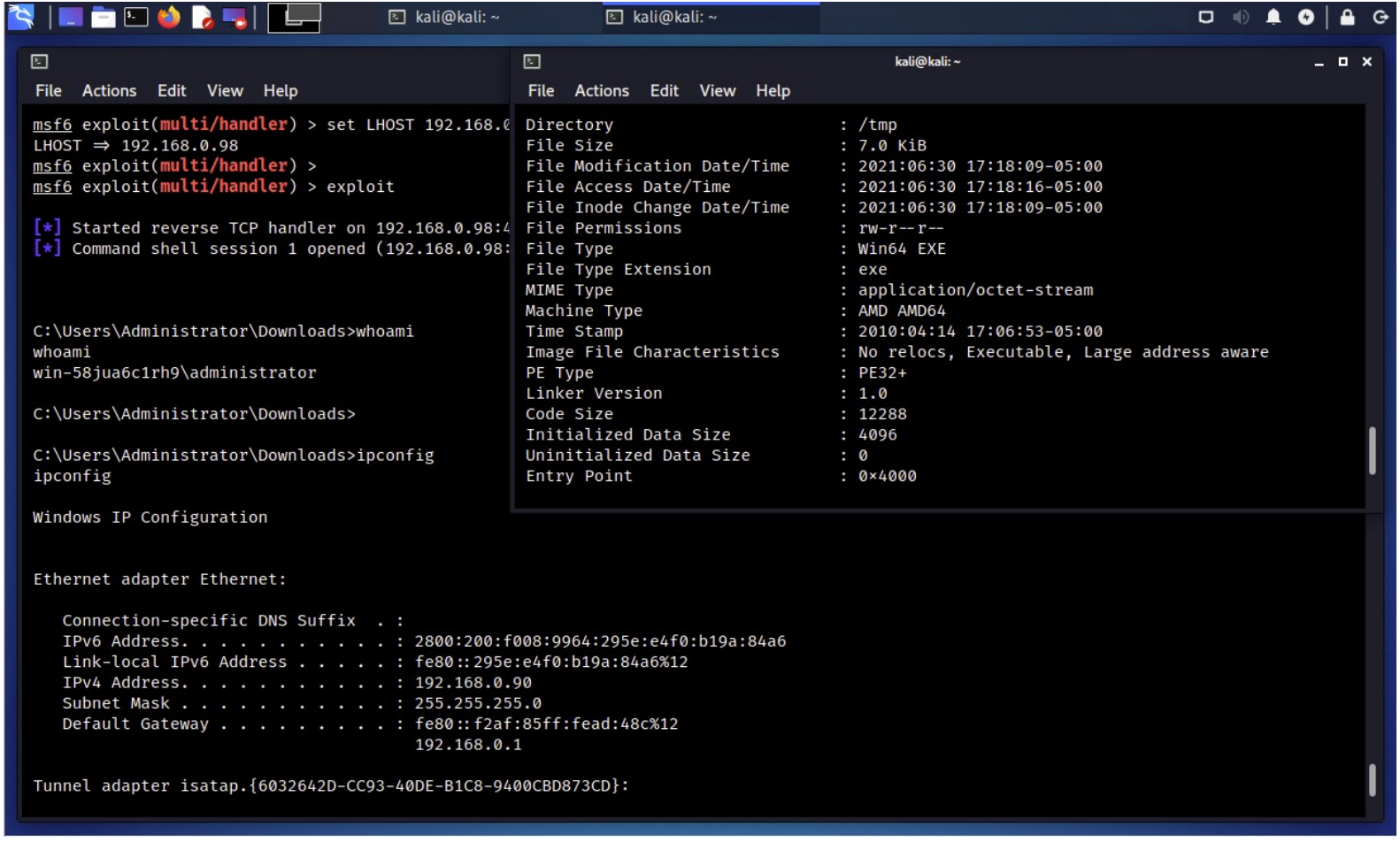
Como profesionales en ciberseguridad, se tiene la única responsabilidad de encontrar y entender las vulnerabilidades presentes en la organización, para luego trabajar diligentemente en mitigarlas antes de estas sean aprovechadas por los atacantes maliciosos. Este curso abarca las herramientas, técnicas y metodologías para realizar pruebas de penetración contra redes y sistemas, y así estar en la capacidad de realizar proyectos de pruebas de penetración exitosamente. Todas las organizaciones necesitan personal experimentado en seguridad de la información, quienes puedan encontrar vulnerabilidades y mitigar sus efectos. Con este curso se estará en la capacidad de realizar pruebas de penetración y hacking ético, aplicando los conocimientos, herramientas, y técnicas explicadas detalladamente. Consecuentemente descubrir y explotar vulnerabilidades en entornos reales, demostrando así todos los conocimientos adquiridos.

Alonso Eduardo Caballero Quezada es 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). Ha sido instructor en el OWASP LATAM Tour, expositor en OWASP Perú Chapter Meeting y OWASP LATAM at Home , además de Conferencista

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

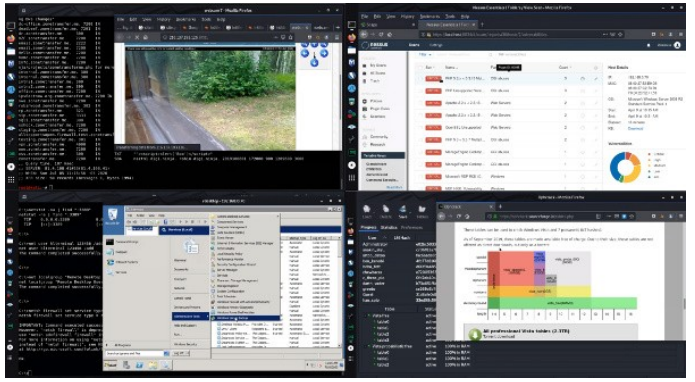
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

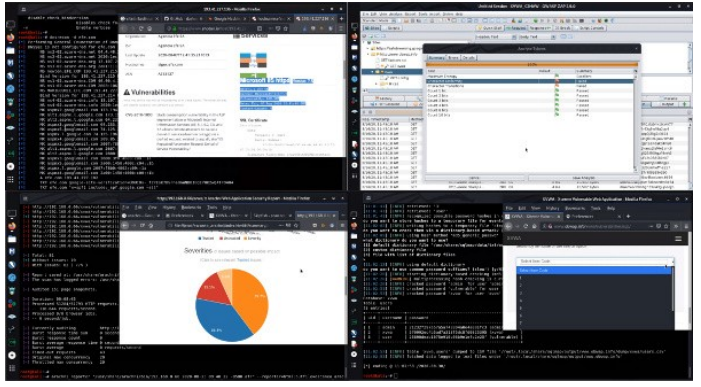
Curso Virtual OSINT - Open Source Intelligence
https://www.reydes.com/d/?q=Curso_de_OSINT

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 67 webinars gratuitos

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

Diapositivas de los webinars gratuitos

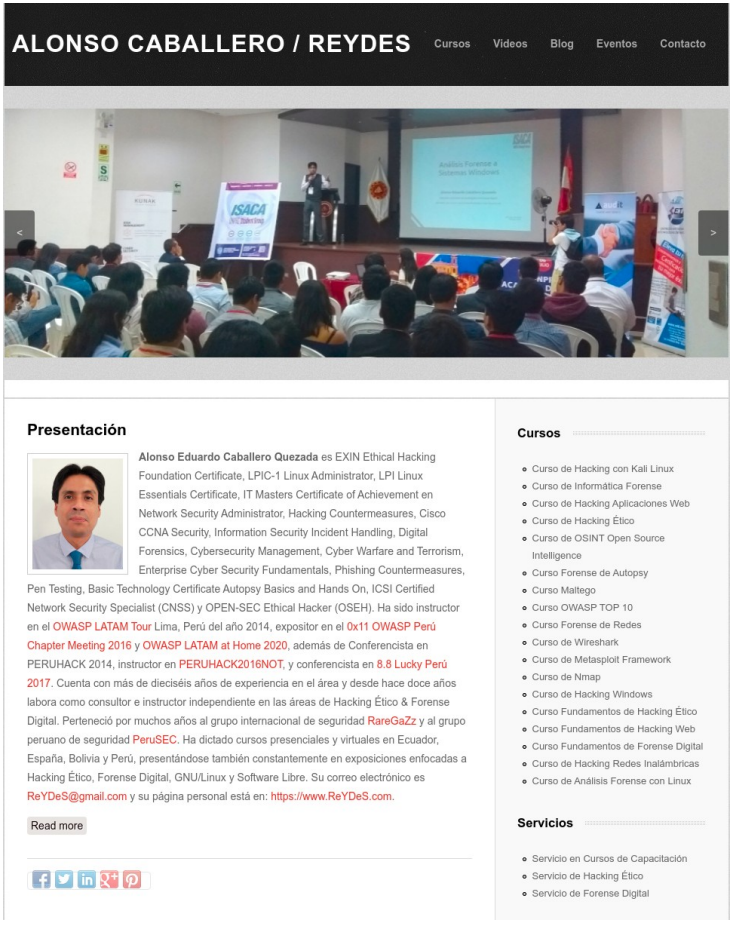
https://www.reydes.com/d/?q=eventos

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 y el Firewall de Windows

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 8 de Julio del 2021