Webinar Gratuito

Explorando Kali Linux

Alonso Eduardo Caballero Quezada

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

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

Jueves 2 de Noviembre 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

Kali Linux

Es una distribución de Linux basada en Debian, orientada a pruebas de penetración avanzadas y auditorías de seguridad. Proporciona herramientas, configuraciones, y automatizaciones comunes, las cuales permiten al usuario centrarse en la tarea a completar, y no en la actividad circundante.

Kali Linux contiene varios cientos de herramientas dirigidas a las diversas tareas en seguridad de la información, como pruebas de penetración, investigación de seguridad, forense digital, ingeniería inversa, gestión de vulnerabilidades, y pruebas del equipo rojo.

Kali Linux es una solución multiplataforma, accesible y de libre disposición para profesionales y aficionados en seguridad de la información.

* Kali: https://www.kali.org/

exploit-db

Es un archivo cumpliendo con CVEs de exploits públicos, y software vulnerable correspondiente, desarrollado para ser utilizado por profesionales en pruebas de penetración e investigadores de vulnerabilidades.

Su propósito es brindar la colección más completa de exploits recopilados a través de envíos directos, listas de correo, y otras fuentes públicas, además de presentarlos en una base de datos de fácil navegación y disponible gratuitamente.

La base de datos de exploits es un repositorio de exploits y pruebas de conceptos en lugar de avisos, convirtiéndolo en un recurso valioso para quienes necesitan datos factibles de ser procesados de inmediato.

Exploit-db: https://www.exploit-db.com/

Webshells

Son aplicaciones basadas en web, las cuales brindan a un actor de amenazas la capacidad de interactuar con un sistema, desde el acceso y carga de archivos hasta la capacidad de ejecutar código arbitrario en el servidor explotado.

Están escritos en una variedad de lenguajes, incluidos PHP, ASP, Java y JavaScript, aunque el más común es PHP (pues la mayoría de los sistemas soportan PHP).

Una vez están en el sistema, el actor de amenazas puede usarlos para robar datos o credenciales, obtener acceso hacia servidores más importantes de la red, o como conducto para cargar malware más peligroso y extenso.

* Web shells 101: Detection and Prevention
https://www.rapid7.com/blog/post/2016/12/14/webshells-101/

Wordlist

Es un archivo (texto) conteniendo un conjunto de valores.

Cuando se enfrenta ante un mecanismo de autenticación, se pueden probar algunas credenciales conocidas con el propósito de adivinar las correctas.

Esta lista de credenciales a probar es una lista de palabras. En lugar de ingresar manualmente los valores uno por uno, se utiliza una herramienta o script para automatizar el proceso.

De manera similar en el caso de hashes, se utiliza listas de palabras para codificarlas con el mismo hash, y luego comparar cadenas para coincidir los hashes. Si se encuentra una coincidencia, se obtuvo el hash.

Wordlists: https://www.kali.org/tools/wordlists/

Windows Binaries

Incluye diversos binarios útiles cuando se realizan pruebas de penetración contra sistemas operativos Windows.

La mayoría de estos binarios son importantes para la etapa denominada como post-explotación o explotación posterior.

Entre los procesos a realizar utilizando estar herramientas se incluyen; recolección de información, escaneos, enumeración, mantener el acceso, y borar rastros.

* Windows Binaries: https://www.kali.org/tools/windows-binaries/

Impacket

Es una colección de clases de Python para trabajar con protocolos de red.

Impacket se centra en proporcionar acceso programático de bajo nivel hacia los paquetes, y para algunos protocolos (por ejemplo, SMB1-3 y MSRPC), la implementación del protocolo en sí.

Los paquetes se pueden construir desde cero, como también analizarse a partir desde datos en bruto, y la API orientada a objetos simplifica el trabajo con jerarquías profundas de protocolos. La biblioteca proporciona un conjunto de herramientas como ejemplos de aquello lo cual se puede hacer dentro del contexto de esta librería.

* Impacket: https://github.com/fortra/impacket
* Impacket: https://www.kali.org/tools/impacket/

Curso Virtual Hacking con Kali Linux

Sitio Web:

www.reydes.com

Correo:

reydes@gmail.com

Curso Virtual Hacking Kali Linux 2023

Domingos 5, 12, 19 y 26 de Noviembre 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

Kali Linux es una distribución basada en el sistema operativo GNU/Linux Debian, diseñada específicamente para realizar auditorias de seguridad y pruebas de penetración avanzadas. Kali Linux contiene cientos de herramientas destinadas a las más diversas tareas en seguridad de la información, tales como pruebas de penetración, investigación de seguridad, forense digital e ingeniería inversa. Kali Linux incluye más de 600 herramientas para pruebas de penetración, es libre, tiene un árbol GIT open source, cumple con FHS, tiene un amplio soporte para dispositivos inalámbricos, incluye un kernel parchado para inyección, es desarrollado en un entorno seguro, sus repositorios y paquetes están firmados con GPG, tiene soporte para múltiples lenguajes, incluye soporte para ARMEL, y ARMHF, además de ser completamente personalizable.

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), yCodered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials

Más Información:

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

Demostraciones

-

```
kali@kali: /usr/share/impacket
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[/usr/share/impacket]
└─$ ls /usr/share/wordlists
amass  dirbuster      fern-wifi  legion      nmap.lst     rockyou.txt.gz  sqlmap.txt  wifite.txt
dirb   fasttrack.txt  john.lst   metasploit  rockyou.txt  seclists        wfuzz

┌──(kali㉿kali)-[/usr/share/impacket]
└─$

┌──(kali㉿kali)-[/usr/share/impacket]
└─$ ls /usr/share/doc/python3-impacket/examples/
addcomputer.py     getArch.py          karmaSMB.py       mssqlinstance.py      raiseChild.py     samrdump.py     sniffer.py
atexec.py          Get-GPPPassword.py  keylistattack.py  netview.py            rbcd.py           secretsdump.py  sniff.py
dcomexec.py        GetNPUsers.py       kintercept.py     nmapAnswerMachine.py  rdp_check.py      services.py     split.py
dpapi.py           getPac.py           lookupsid.py      ntfs-read.py          registry-read.py  smbclient.py    ticketConverter.py
esentutl.py        getST.py            machine_role.py   ntlmrelayx.py         reg.py            smbexec.py      ticketer.py
exchanger.py       getTGT.py           mimikatz.py       ping6.py              rpcdump.py        smbpasswd.py    wmiexec.py
findDelegation.py  GetUserSPNs.py      mqtt_check.py     ping.py               rpcmap.py         smbrelayx.py    wmipersist.py
GetADUsers.py      goldenPac.py        mssqlclient.py    psexec.py             sambaPipe.py      smbserver.py    wmiquery.py

┌──(kali㉿kali)-[/usr/share/impacket]
└─$

┌──(kali㉿kali)-[/usr/share/impacket]
└─$ searchsploit
  Usage: searchsploit [options] term1 [term2] ... [termN]

==========
 Examples
==========
  searchsploit afd windows local
  searchsploit -t oracle windows
  searchsploit -p 39446
```

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

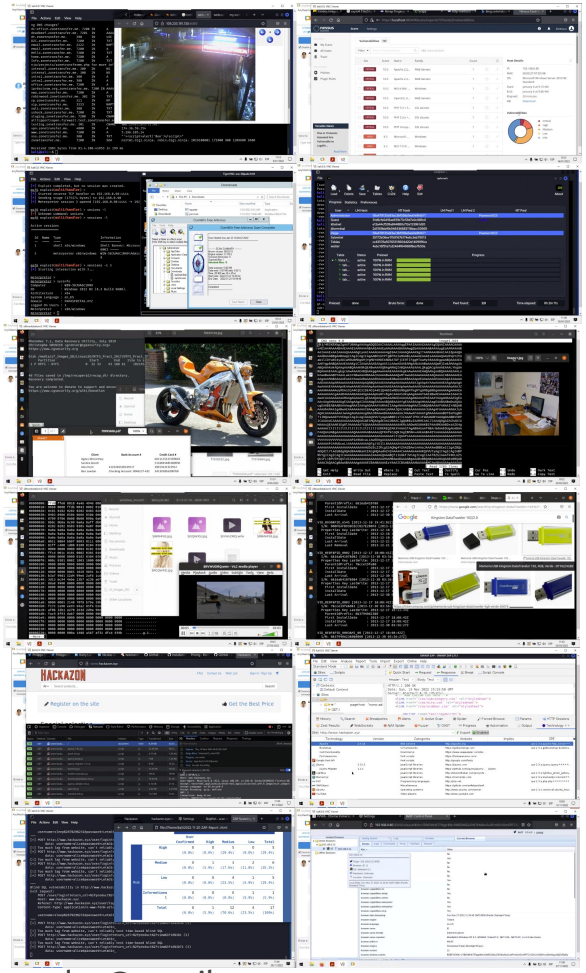
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

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 87 webinars gratuitos

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

Diapositivas de los webinars gratuitos

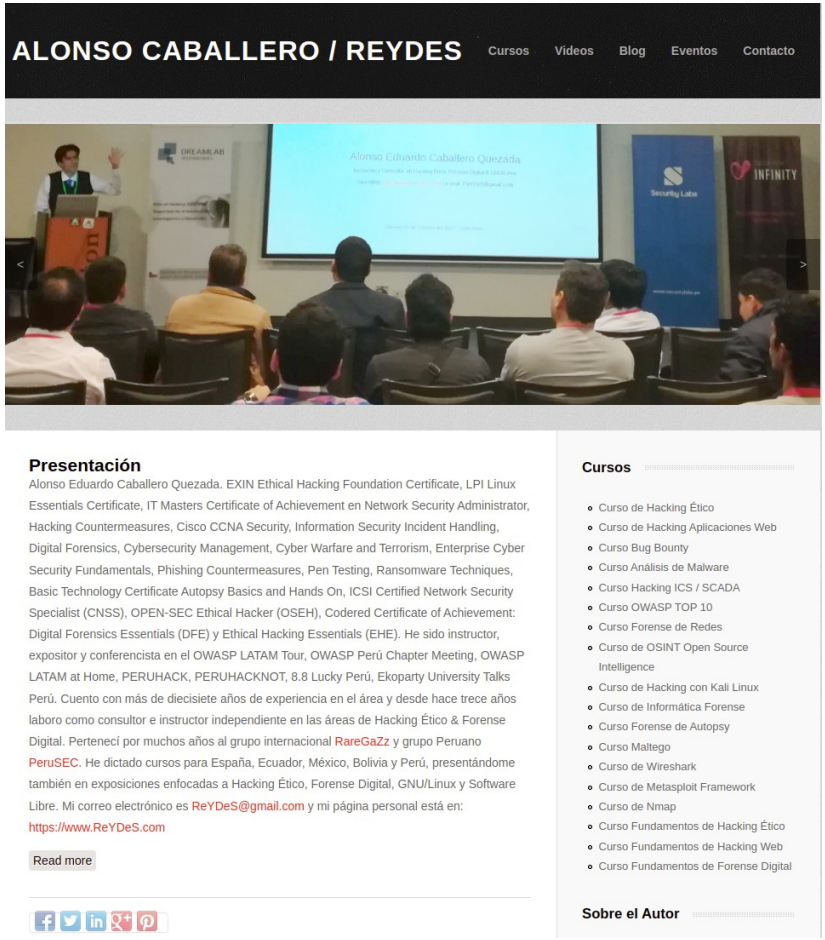
https://www.reydes.com/d/?q=eventos

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

Explorando Kali Linux

Alonso Eduardo Caballero Quezada

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

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

Jueves 2 de Noviembre 2023