Webinar Gratuito

Evaluar Contraseñas con Kali Linux

Alonso Eduardo Caballero Quezada

Instructor y Consultor Independiente en Ciberseguridad

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

Jueves 4 de Abril 2024

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).

Más de 20 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético, Forense Digital, GNU/Linux, y áreas relacionadas.

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

www.reydes.com

+51 949 304 030

@ReYDeS

Contraseñas

Es un secreto memorizado utilizado para confirmar la identidad de un usuario.

Generalmente es una cadena de caracteres arbitraria, la cual incluye letras, dígitos, y otros símbolos.

No debería ser una palabra; en el sentido estricto de estar incluida en un diccionario, para sea difícil de adivinar. Fundamental al elegir una contraseña.

Se sugiere una contraseña sea una “frase”, es decir texto separado por espacios o caracteres especiales.

Así mismo utilizar las primeras letras de una frase para construir la contraseña, incluyendo número y caracteres especiales.

Ataques a Contraseñas

Es factible atacar las contraseñas en dos escenarios fundamentales.

Intentar adivinar la contraseña

Realizar ataques contra un servicio en funcionamiento, utilizando un nombre de usuario válido. Esto con el propósito de intentar identificar la contraseña correcta.

Intentar romper la contraseña

Realizar ataques contra las contraseñas encriptadas. El requisito previo es haber obtenido los hashes de las contraseñas. El propósito es obtener el texto plano desde el hash de la contraseña.

Herramientas para Contraseñas en Kali Linux

Kali Linux proporciona diversas herramientas relacionadas con las contraseñas:

- John The Ripper
- THC-Hydra
- hashcat
- medusa
- 0phrack
- crunch
- cewl
- ncrack
- Johnny
- etc.

* https://www.kali.org/tools/kali-meta/#kali-tools-passwords

Fuentes de Contraseñas

Algunas de las herramientas incluidas en Kali Linux, incluyen sus propios archivos conteniendo nombres de usuario y contraseñas.

- Nmap
- Metasploit Framework
- Sqlmap
- DNSmap

Así mismo incluye proyectos autónomos los cuales proporcionan diversos archivos relacionados a las contraseñas.

- Seclists
- FuzzDB (*)

Curso Hacking con Kali Linux

Curso Virtual Hacking Kali Linux 2024

Domingos 7, 14, 21 y 28 de Abril del 2024. De 9:00 am a 12:00 pm (UTC -05:00)

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. Proporciona herramientas, configuraciones, y automatizaciones comunes las cuales permiten centrarse en el trabajo a realizar, y no en la actividad circundante. Kali Linux contiene cientos de herramientas destinadas a las más diversas tareas correspondientes a 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.

Objetivos

Este curso proporciona una gran cantidad de conocimientos para iniciarse en el área del Hacking Ético y Pruebas de Penetración, además de ser una guía práctica para la utilización de las herramientas más populares durante la realización Auditorias de Seguridad, ejercicios de Red Team, y Bug Bounty. Así mismo este curso proporciona conocimientos sobre diversos aspectos de Kali Linux, conceptos sobre programación, metasploit framework, captura de información, búsqueda de vulnerabilidades, técnicas para la captura de tráfico, explotación de vulnerabilidades, técnicas manuales de explotación, ataques a contraseñas, ataques para el lado del cliente, ingeniería social, técnicas para evadir antivirus y técnicas posteriores a la explotación.

Fechas & 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:

Domingos 7, 14, 21 y 28 de Abril del 2024

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). He sido instructor, expositor y conferencista en el OWASP LATAM Tour, OWASP Perú Chapter Meeting, OWASP LATAM at Home, PERUHACK, PERUHACKNOT, 8.8 Lucky Perú, Ekoparty University Talks Perú. Cuento con más de veinte años de experiencia en el área, y desde hace dieciséis 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 PerúMi 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

Teléfono: +51 949 304 030

Sitio Web: www.reydes.com

Temario

- Configurar un Laboratorio Virtual
- Introducción a Kali Linux
- Bases de Programación y Scripting con Bash y Python
- Utilizando Metasploit Framework
- Payloads y Tipos de Shells
- Configurar Manualmente un Payload
- Utilizar Módulos Auxiliares
- Captura de Información
- Captura OSINT
- Escaneo de Puertos
- Encontrar Vulnerabilidades
- Nessus
- Nmap Scripting Engine NSE
- Módulos para el Escaneo en Metasploit
- Escaneo de Aplicaciones Web y Análisis Manual
- Captura de Tráfico y Utilizando Wireshark
- Envenenamiento del Cache ARP
- Envenenamiento del Cache DNS
- Ataques SSL
- Explotación Remota
- Explotación a WebDAV y PhpMyAdmin
- Descargar Archivos Sensibles
- Explotar Aplicaciones Web de Terceros, Servicios Comprometidos, Recursos Compartidos NFS.
- Ataques en Línea de Contraseñas
- Ataques Fuera de Línea de Contraseñas
- Explotación del Lado del Cliente
- Evadiendo Filtros con Payloads de Metasploit
- Ataques del Lado del Cliente
- Ingeniería Social y Social Engineer Toolkit SET
- Ataques Web
- Evadir Antivirus
- Como Funcionan los Antivirus
- Evadiendo un Programa Antivirus
- Post Explotación
- Meterpreter y Scripts de Meterpreter
- Módulos de Post Explotación en Metasploit
- Escalado de Privilegios Locales
- Captura de Información Local
- Movimiento Lateral
- Pivoting
- Persistencia

Material

- Kali Linux
- Metasploitable 3
- Windows Server

Beneficios e Inversión

- Acceso a las sesiones en vivo
- Acceso al aula virtual por 45 días
- Video de las cinco (5) sesiones
- Material utilizado durante el desarrollo del curso
- Asesoría personalizada
- Libro "Fundamentos de Hacking Ético" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación (CMKL). Puntuación mínima 70/100).

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 de correo electrónico a reydes@gmail.com 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 por favor un mensaje de correo electrónico a reydes@gmail.com para proporcionarle los datos.

Confirmado el pago se enviará los datos para conectarse hacia la plataforma

Certificados

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

Sitio Web:

www.reydes.com

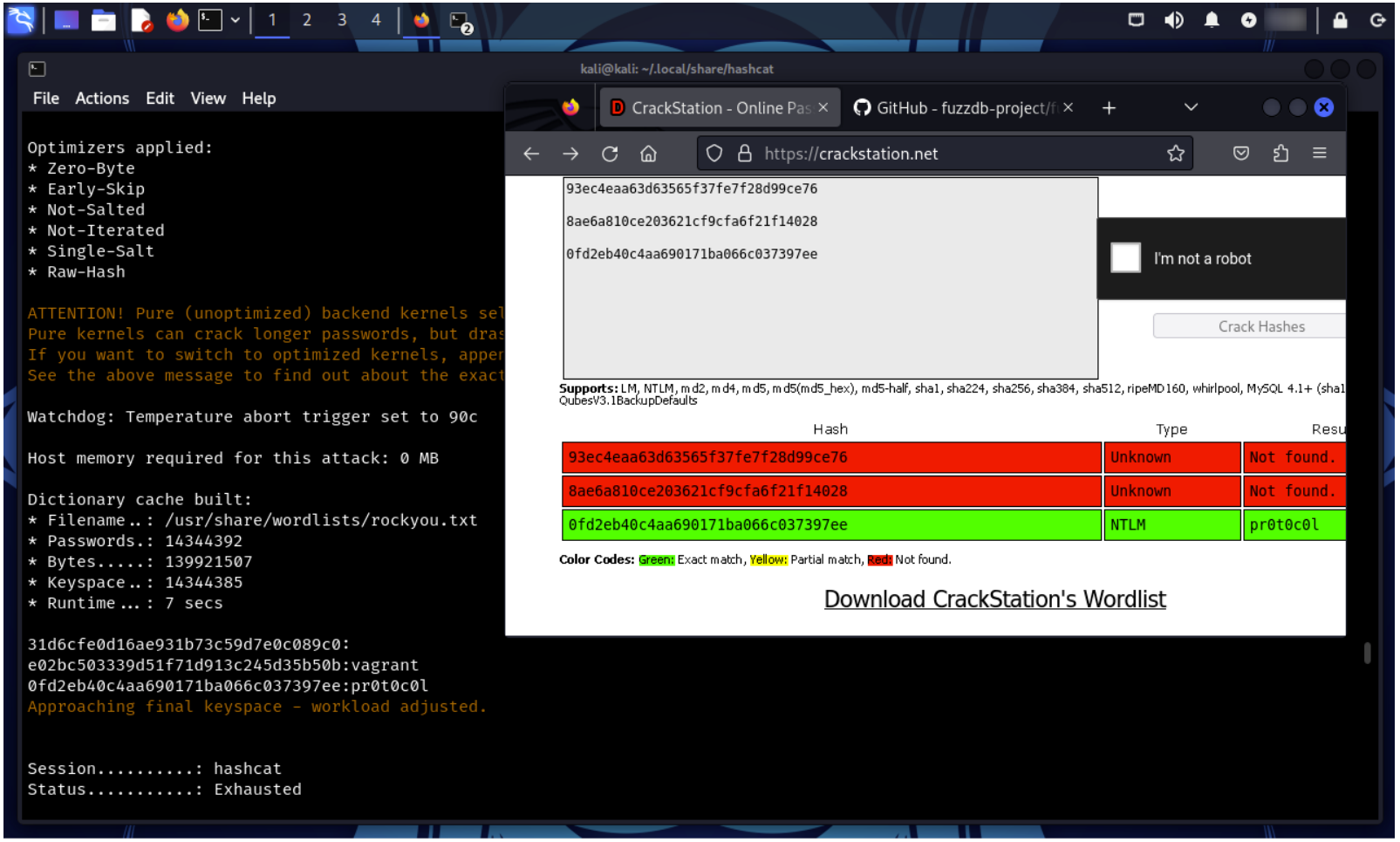
Correo:

reydes@gmail.com

Más Información:

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

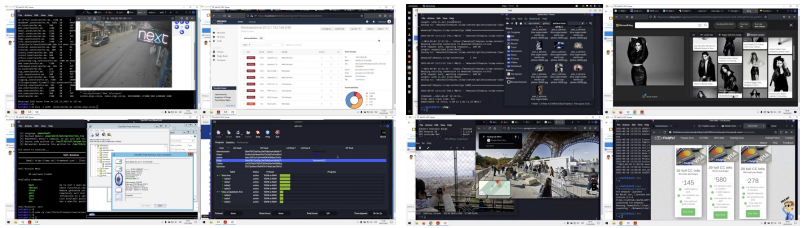
Prácticas


kali@kali: ~/.local/share/hashcat
File Actions Edit View Help
Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash
ATTENTION! Pure (unoptimized) backend kernels sel
Pure kernels can crack longer passwords, but dras
If you want to switch to optimized kernels, apper
See the above message to find out about the exact
Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 7 secs
31d6cfe0d16ae931b73c59d7e0c089c0:
e02bc503339d51f71d913c245d35b50b:vagrant
0fd2eb40c4aa690171ba066c037397ee:pr0t0c0l
Approaching final keyspace - workload adjusted.
Session.....: hashcat
Status.....: Exhausted
CrackStation - Online Pas
GitHub - fuzzdb-project/f
https://crackstation.net
93ec4eaa63d63565f37fe7f28d99ce76
8ae6a810ce203621cf9cfa6f21f14028
0fd2eb40c4aa690171ba066c037397ee
I'm not a robot
Crack Hashes
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1
QubesV3.1BackupDefaults
Hash
Type
Resu
93ec4eaa63d63565f37fe7f28d99ce76
Unknown
Not found.
8ae6a810ce203621cf9cfa6f21f14028
Unknown
Not found.
0fd2eb40c4aa690171ba066c037397ee
NTLM
pr0t0c0l
Color Codes: Green: Exact match, Yellow: Partial match, red: Not found.
Download CrackStation's Wordlist

Cursos Disponibles en Video

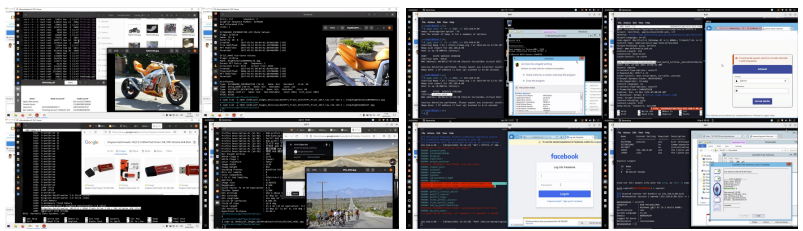
Curso Hacking Ético
https://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Hacking Aplicaciones Web
https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web



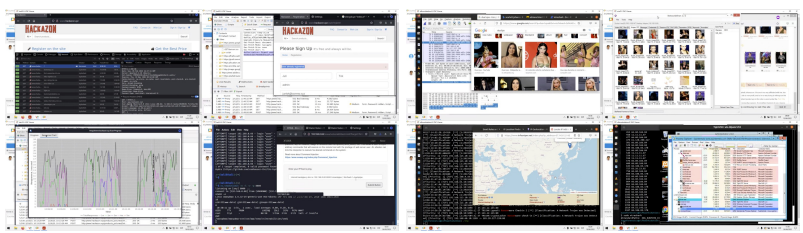
Curso Informática Forense
https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

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



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

Curso 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 webinars

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

Diapositivas de webinars

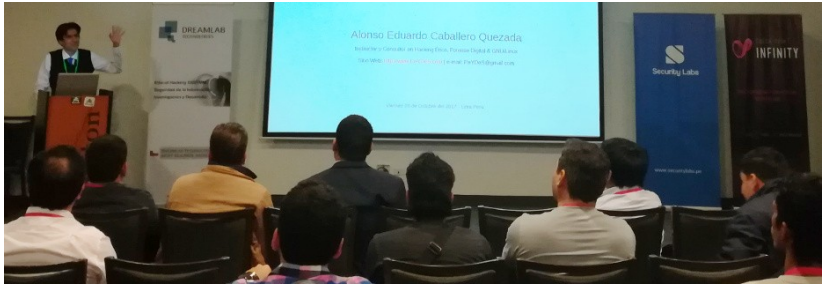
https://www.reydes.com/d/?q=eventos

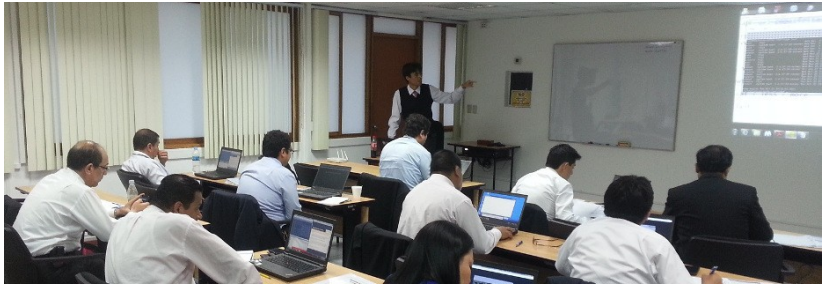
Libros y artículos

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

Blog

https://www.reydes.com/d/?q=blog/1





Webinar Gratuito

Evaluar Contraseñas con Kali Linux

Alonso Eduardo Caballero Quezada

Instructor y Consultor Independiente en Ciberseguridad

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

Jueves 4 de Abril 2024