

Curso Hacking Kali Linux 2024

Domingos 3, 10, 17 y 24 de Noviembre 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 auditorías 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 Auditorías 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 3, 10, 17 y 24 de Noviembre 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. Pertencí 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

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
- 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 (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



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**



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.

