Curso CiberSeguridad Windows y Linux 2025

Sábados 29 Noviembre, 6, 13, y 20 Diciembre 2025. De 9:00 am a 12:00 pm (UTC -05:00)

Las clases en vivo se quedan grabadas en el aula virtual

Presentación

La ciberseguridad es una inversión esencial para la continuidad y supervivencia de cualquier empresa. La infraestructura moderna se construye sobre una base dual, utilizando la versatilidad de los sistemas operativos Windows y GNU/Linux. Un fallo en cualquiera de estas plataformas puede paralizar las operaciones de una empresa. La falta de hardening adecuado permite ciberataques exitosos buscando comprometer información confidencial, propiedad intelectual, y datos de los clientes. El riesgo de un ciberataque de ransomware o una filtración de datos es constante. Proteger ambos entornos es crucial, pues esto garantiza incluso si un sistema es comprometido, los demás no sean utilizados como un vector de ataque más profundo. La implementación de auditorías avanzadas y sistemas para vigilancia proactiva intentan garantizar la integridad de la empresa. Una estrategia de ciberseguridad robusta en Windows y Linux protege los activos, mantiene la confianza de los clientes, y asegura el cumplimiento normativo.

Objetivos

Este curso enseña a los participantes a realizar a establecer las bases operativas para un entorno seguro, garantizando únicamente lo necesario esté activo y sea factible de ser accedido. Implementar políticas rigurosas para control de acceso, limitando el poder de las cuentas de usuario y de servicios. Fortalecer las barreras perimetrales del sistema, controlando estrictamente todo el tráfico entrante y saliente. Asegurar los puntos de entrada más sensibles del servidor, desde la etapa de inicio hasta la configuración de protecciones internas. Configurar los mecanismos de registro del sistema para capturar todas las acciones críticas. Desarrollar una mentalidad proactiva, yendo de la reacción a la detección temprana de ciberamenazas. Además de cumplir con las mejores prácticas en la industria para la gestión de seguridad en servidores.

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

Fechas y Horarios

Duración: Doce (12) horas. Cuatro (4) sesiones en vivo de tres (3) horas de duración cada una.

Fechas:

Sabados 29 Noviembre, 6, 13, y 20 Diciembre 2025

Horario:

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

Más Información

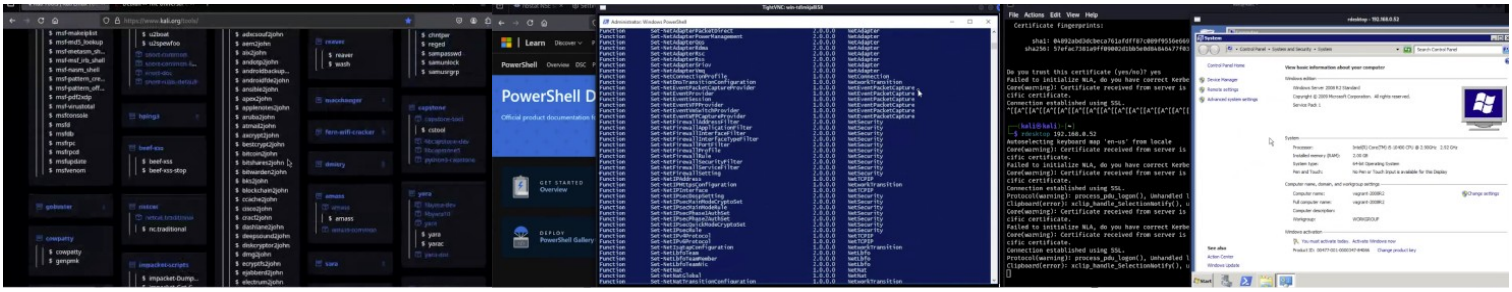
Para obtener más información sobre este curso, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

reydes@gmail.com

WhatsApp: https://wa.me/51949304030

Sitio Web: www.reydes.com



Temario

- Confidencialidad, Integridad y Disponibilidad
- Amenazas y Vulnerabilidades
- Riesgo y Superficie de Ataque
- ISO/IEC 27001 y NIST CSF
- Ciclo de Vida para Gestión de Riesgos
- Principio de Mínimo Privilegio
- Defensa en Profundidad
- CIS Benchmarks
- Proceso de Hardening
- Vulnerabilidades más Comunes en Sistemas Operativos
- Política de Contraseñas Robustas
- Bloqueo de Cuenta y Auditoría
- Autenticación Multifactor
- Gestión de Cuentas Privilegiads
- Control de Cuentas de Usuarios
- Firewall de Windows Defender
- Deshabilitar Servicios Innecesarios
- Configuración Segura de Escritorio Remoto
- Seguridad Powershell y Logging
- Encriptación Completa del Disco con BitLocker
- Gestión de Claves para Recuperación
- Permisos NTFS y Principio de Menor Privilegio
- Auditoría de Acceso hacia Objetos
- Windows Security y Control de Aplicaciones
- Manejo Seguro del Usuario root
- sudo y el Principio de Mínimo Privilegio
- Cuentas de Servicio / Sistemas en Linux
- Hardening de SSH
- Configuración del Firewall en Linux
- Deshabilitar Servicios de Red Innecesarios
- Hardening al Kernel y Configuración de Red
- Permisos Estándar y Permisos Especiales de Archivos
- Módulos para Seguridad del Kernel
- Proteger Archivos Críticos de Configuración
- Protección del BootLoader
- Vigilancia y Detección
- Configuración del Visor de Eventos
- Eventos Críticos a Vigilar en Windows
- Análisis de Logs en Linux
- Política para Gestión de Parches
- Proceso para Actualización de Windows y Linux
- Escaneo de Vulnerabilidades
- Backup Seguro
- Plan para Recuperación ante Desastres

Material

- Windows Server 2022
- Ubuntu Server 22.04
- Kali Linux

Beneficios e Inversión

- Acceso al aula virtual por 60 días
- Acceso a las sesiones en vivo
- Video de las cuatro (4) 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.