Alonso Eduardo
Caballero Quezada
(ReYDeS)

Curso Ciberseguridad Windows y Linux 2026

4	12	En vivo, Virtual, o Personalizado
Sesiones	Horas	

Alonso Eduardo Caballero Quezada

Tengo más de veintidós años de experiencia, y desde hace dieciocho años realizo capacitaciones y consultorías en Hacking, Forense, OSINT, CiberSeguridad, y GNU/Linux

Redes Sociales

LinkedIn

X (Twitter)

YouTube

Facebook

Sitio Web

e-mail

WhatsApp

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 establecer las bases operativas para el funcionamiento de 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 desde la reacción hasta la detección temprana de ciberamenazas. Además de cumplir con las mejores prácticas en la industria para la gestión adecuada de seguridad en servidores Windows y GNU/Linux.

Alonso Eduardo
Caballero Quezada
(ReYDeS)

Curso Ciberseguridad Windows y Linux 2026

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

Beneficios

- 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 de los siguientes cursos a dictarse
- Material utilizado durante el desarrollo del curso
- Dos (2) horas de asesoría personalizada en vivo 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

Inversión

Perú: S/. 350 Soles

- Depósito o transferencia interbancaria a Scotiabank
- Pago mediante YAPE o PLIN

Otros países: $ 110 Dólares

- Pago mediante PayPal

Escriba un mensaje al WhatsApp https://wa.me/51949304030 para proporcionarle los datos pertinentes.

Información

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

WhatsApp: https://wa.me/51949304030

Correo electrónico: reydes@gmail.com