Hardening de Servidores

Objetivos

- Entender el proceso de fortalecimiento de servidores para mantener infraestructuras seguras

- Proporcionar herramientas para mejorar la seguridad física y lógica de los servidores y sistemas operativos clientes

Dirigido a

Técnicos, Ingenieros, Jefes de Infraestructura de TI, entusiastas de ciberseguridad, personal de SOC, entre otros.

Metodología

Curso virtual, donde se explican conceptos relacionados y se realizan las prácticas con diferentes herramientas para ejemplificar los mismos.

Requisitos

- Equipos de computo
- Acceso a Internet
- Máquinas virtuales que serán entregadas por nosotros

16 Horas

80% PRACTICO

20% TEORICO

CRlabsec Cyber Security

Contenido

Modulo 1 – Introducción a la ciberseguridad
- Ciberseguridad en Sistemas operativos y redes
- Protección de equipos físicos
- Sistemas de Archivos

Modulo 2 – Seguridad en sistemas Windows
- Cifrado y mecanismos de protección
- Proceso de arranca en Windows
- Ficheros importantes, contraseñas y hashes
- Gestión de usuarios y permisos
- Protección de Memoria
- NAP, tools y powershell

Modulo 3 – Seguridad en Windows Server
- Procesos de Monitoreo y directorio activo
- Políticas de Grupo y LAPS
- Auditoría y Control de Acceso
- Gestión de identidades
- Roles y Servicios de Seguridad

Modulo 4 – Seguridad en Sistemas GNU/Linux
- Permisos, usuarios , contraseñas y cifrado
- Herramientas (cron, trpwire/ossec ,iptables, proxys, vpn)
- Port-Knocking
- Fortificación web
- Fail2ban
- Pfsense
- OSSIM

Modulo 5 – Seguridad en Redes Internas
- VLAN y topologías
- Ipsec
- NIDS
- NAT
- HoneyPot

Modulo 6 – Protección de capas de aplicación y servicio
- Jaulas chroot
- Hardening de servicios (ssh, smtp, otros)
- Virtualización
- Limitación de recursos

Inscripción

Precio $250 + iva

Contacto: +506 83342943 / Info@crlabsec.com