



Curso de Seguridad Informática

Descripción

El Curso de Seguridad informática brinda un amplio conocimiento y práctica real en equipos de las más actuales herramientas y técnicas de ataque y defensa, permitiéndonos consecuentemente actuar profesionalmente sobre el tema. Tiene un enfoque totalmente práctico basado en distintos tipos de ataques y sobre diversos entornos.

I-SEC forma desde hace mas de 15 años a nivel internacional a los mas importantes lideres del sector de seguridad de la información, mediante programas de alcance mundial con visión estratégica de las ultimas tendencias del mercado.

Usted obtendrá los conocimientos teóricos, una visión estratégica, y aplicación practica, con los cuales profesionales especializados trabajan en el campo de la seguridad informática de los más altos niveles de complejidad a nivel internacional.

El enfoque de los contenidos estará en constante correlación con los estándares internacionales de seguridad informática.

Objetivo: Capacitar a los profesionales de Seguridad Informática en tecnologías y herramientas de implementación y control de medidas de seguridad de la información en concordancia con estándares internacionales.

Requisitos:

Conocimientos básicos de Sistemas y/o Auditoria de Sistemas.



Plan de estudios:

1. Seguridad de las redes

- Composición de una red de información
- Vulnerabilidades de las redes
- High availability/load sharing
- Topología de una red segura
- Vulnerabilidades y consideraciones de seguridad para cada componente de una red

2. Seguridad en servidores Windows

- Métodos para armar un servidor seguro
- Hardening
- Seguridad hasta el nivel de la aplicación
- Cómo saber si un hacker entró en los servidores de la organización
- Manejo de parches y service packs
- PKI, IPsec, Kerberos, Radius

3. Seguridad de servidores Unix/Linux

- Hardening de servidores Unix/Linux
- Herramientas para detectar intrusiones
- Tripwire
- Encriptación
- Maneras de asegurar servidores Unix/linux

4. Seguridad en Routers/Switches

- Metodologías y herramientas para atacar switches/routers
- Arp poisoning
- VLANs
- Mac lucking
- 802.1x



5. Optimizar los Firewalls

- Principales tipos de Firewalls
- Cómo crear una base de reglas fuerte.
- Problemas con Firewalls
- VPN
- Dos Factores autenticación
- Firewalls de Open Source
- Leer y entender los logs del Firewall para detectar intrusiones

6. IDS/IPS-Best practice

- Principales tipos de IPS/IDS
- Dónde colocar IPS/IDS en la red.
- Maneras en que los hackers atacan redes protegidas por IDS/IPS
- Estrategia para evitar falsos positivos/falsos negativos
- Cómo configurar nuestros IDS/IPS para evitar ataques de Hackers

7. Arquitectura de red segura

- Autenticación
- Redundancia
- Security in depth (seguridad en etapas)
- Cómo evitar un único punto de falla
- Aceptación por default
- Negación por default

8. Seguridad en Wireless

- Diferentes algoritmos
- Certificados, Radius, Tacacs
- Hardening de Access points y red inalámbrica
- Penetration test en una red gíreles



9. Seguridad en base de datos

- Topología de base de datos.
- Herramientas para penetrar diferentes bases de datos
- SQL injection
- Input validation

10. Seguridad en servidores Web

- Hardening de servidores Web
- Web applications
- Penetration Test de servidores Web
- Remote command execution
- Cookie poisoning
- Code review
- Rootkits
- XSS (cross site scripting)

11. Ethical Hacking/Penetration Test

- Herramientas
- Live cd's
- Diferencia entre auditoria y Penetration Tests
- Diferencias entre un Penetration Test interno y externo
- Social engineering (Ingeniería social)

12. Implementación de herramientas de seguridad de Open Source

¿Por qué Open Source?

Herramientas líderes en el mercado de seguridad informática basadas en Open Source

13. Google Hacking para penetration testers



Material de apoyo: Presentaciones en Power Point proporcionada en un CD.

Bibliografía en formato Digital (Provista por I-SEC):

1. Prentice Hall - The Practice Of Network Security. Deployment Strategies For Production Environments.
2. Matthehw Strebe -Sybex - Network Security Foundations.

Los Alumnos deberán aprobar un examen final que otorgara la Certificación correspondiente de I-SEC Education Center.

Instructor:

Juan Baby Cissp Ccna Ccsa Mcse Scsa

Es un especialista en seguridad informática, con 12 años de experiencia en sólidas técnicas de Penetration tests, habilidades y métodos de operaciones. Tiene una amplia formación en tecnologías de seguridad, entre otras: IDS/IPS, Firewalls, Application Security, Buffer Overflows, Microsoft Security, Linux Security, IDS evasion Attacks, Assessment Services y Penetration Tests.

Mr. Baby tiene las siguientes certificaciones: Check Point System Administrator (CCSA), Microsoft Certified System Engineer (MCSE), Cisco Certified Network Administrator (CCNA), Sun Certified System administrator (SCSA) y ISC2 Certified Information Systems Security Professional (CISSP), Certified Ethical Hacking (CEH)