Temario del curso:

Seguridad Informática

Índice

Curso de Seguridad Informática

Descripción general del Curso

Hoy en día es casi imposible que no utilicen fuertemente recursos informáticos en cualquier campo o profesión donde se esté implementando o desarrollando un nuevo sistema, ya sea para agilizar trámites, contabilizar procesos, distribución de contenido, fábricas inteligentes, equipos de comunicación, o cualquier otro uso imaginable.

Y sin importar lo inmerso que nos encontramos en sistemas de información, el conocimiento que tienen los usuarios o inclusive los mismos administradores del sistema no es lo suficientemente avanzado para evitar que seamos atacados por agentes externos de forma maliciosa.

El presente curso pretende introducir al estudiante en el tipo de pensamiento de hackers y crackers, al mismo tiempo, introducirle herramientas informáticas en el campo de seguridad necesarias para que pueda entender de forma sencilla como encontrar puntos vulnerables y como crear diseños con las mejores prácticas, para proteger la continuidad de los sistemas, así como la privacidad e integridad de la información confidencial.

También se estudia a nivel práctico las metodologías estándar del campo para aprendizaje de penetración de diferentes tipos, técnicas forenses y documentación de evidencia para fines legales así como una sana dosis de información ética y legal para formar profesionales en el área de Seguridad Informática.

El violentar un sistema informático es en la actualidad el método preferido de ataque por parte de las redes criminales modernas, pudiendo alcanzar objetivos en cualquier parte del mundo y con técnicas masivas de recolección de información, ataque y botnets.

Las empresas que son atacadas por error así como desconocimiento deciden esconder cualquier evidencia pública y visible de un ataque, lo cual crea un problema todavía mayor y que en ocasiones se deban pagar secuestros y rescates de información (ransomware), ataques de denegación de servicio, o lo más común, que sus secretos industriales sean entregados a la competencia sin tener el menor conocimiento de haber recibido un ataque.

La caída temporal o permanente de un servicio puede hacer que un país entero regrese tecnológicamente a la edad de piedra en cuestión de semanas, alcanzando este objetivo para los equipos con el peor diseño en cuanto a seguridad posible; estando gran parte de nuestra infraestructura pública vulnerable a desastres artificiales.

Metodología del Curso

Consiste en un curso que balancea la parte teórica y práctica en cada clase, donde primero se introduce a estudiante en conceptos importantes ya sea de criptografía, protocolos o técnicas de ataque, para luego ejecutar diversos laboratorios donde se pone en práctica lo aprendido.

La información provista al estudiante y la documentación de los laboratorios es suficiente para que pueda replicar los resultados en su propia red de pruebas, o luego del proceso legal adecuado, realizar pruebas en redes de producción bajo su responsabilidad y con la debida autorización por parte de todos los actores involucrados.

Fuente: elaboración propia.

Objetivo General

Otorgar al estudiante los conocimientos generales de seguridad informática suficientes para poder encontrar puntos débiles en la periferia, para crear políticas y diseños de seguridad resistente a ataques conocidos así como técnicas para que logre investigar y documentar incidentes de seguridad.

Requisitos para asistencia al curso

- Conocimiento básico en el sistema operativo GNU/Linux.
- Conocimiento intermedio/avanzado en redes.
- Conocimiento intermedio en componentes de Hardware.
- Conocimiento intermedio de administración de sistemas informáticos.
- Fundamentos básicos de seguridad informática.
- Conocimiento básico del idioma inglés, principalmente para lectura y su debida comprensión.

Duración del curso

- 12 semanas.
- 36 horas en total.

Costo

- $990 por persona.

Detalles adicionales

- El curso cuenta con certificado de participación al finalizar.

Cronograma de estudio

SESIÓN	TEMAS:
Sesión 1	➢ Ética de hacking. ➢ Introducción a Kali Linux.
Sesión 2	➢ Criptografía básica. ➢ SSL/TLS.
Sesión 3	➢ Penetración I ➢ Escucha de paquetes.
Sesión 4	➢ Penetración II.
Sesión 5	➢ Penetración III.
Sesión 6	➢ Diseño resistente a ataques.
Sesión 7	➢ Aplicaciones web.
Sesión 8	➢ Técnicas forenses.
Sesión 9	➢ Redes inalámbricas
Sesión 10	➢ Redes inalámbricas.
Sesión 11	➢ Seguridad física. ➢ Dispositivos móviles.
Sesión 12	➢ Proyecto final.