JUSTIFICACIÓN (*)

El pentesting (o pruebas de penetración) es una herramienta útil para prepararse contra las ciberamenazas. El pentesting es una simulación de ataque autorizada contra un sistema informático con el fin de hallar deficiencias de seguridad, obteniendo acceso a los datos y a las características de un sistema. Este tipo de prueba se desarrolla en 5 fases: reconocimiento, escaneo, obtención de acceso, mantenimiento de acceso y cobertura de rastros.

OBJETIVO GENERAL (*)

- Aprender las distintas técnicas utilizadas para llevar a cabo la primera fase de una prueba de intrusión (el reconocimiento) en sistemas Microsoft Windows.

OBJETIVOS ESPECIFICOS

- Realizar Tareas de Reconocimiento
- Conocer Técnicas de Fingerprinting
- Aprender los Métodos de Seguridad para Resguardo de Información.
- Conocer los Tipos de Ataque Contra los SO Microsoft Windows

1. DESCRIPCION GENERAL DE LA ESTRUCTURA DEL PROGRAMA (*)

Curso 1: Auditorías de Sistemas en Microsoft Windows
Módulo 1: Fase de Reconocimiento
Módulo 2: Herramientas para la Fase de Reconocimiento
Módulo 3: Fingerprinting
Módulo 4: Fingerprinting Activo y Pasivo

Curso 2: Explotación y Tipos de Ataque
Módulo 1: Metasploit
Módulo 2: Postexplotación
Módulo 3: Ataques a la Plataforma Windows
Módulo 4: Ataques a Servicios y Aplicaciones