## Audiencia

Este curso básico sobre ethical hacking está dirigido a estudiantes y Profesionales de áreas de Sistemas, Consultores de Tecnología, Auditores Internos y Externos de Sistemas, Administradores y Responsables de Seguridad Informática que deseen aprender cómo realizar Pruebas de Penetración.

## Perfil adquirido después del curos:

Después del curso el estudiante será capaz de entender el pensamiento y las técnicas que utiliza un hacker malicioso (black hat) en contra de una determinada organización para así poder intentar resguardar la información de la misma.

## Objetivo general

Capacitar al asistente con los conceptos de la metodología y técnicas utilizadas por hackers maliciosos con el fin de comprender los ataques que podrían ir dirigidos hacia su organización y aplicar las contramedidas respectivas.

## Objetivos específicos

* Comprender y manejar conocimientos profundos acerca de la seguridad informática
* Entender el funcionamiento de técnicas, herramientas y métodos usados en la intrusión de sistemas.
* Detectar puntos débiles y vulnerabilidades en la seguridad implementada.
* Utilizar un marco metodológico para realizar pruebas de intrusión autorizadas.

## Metodología

El curso será una combinación de breves clases teóricas, donde se incluirán varias definiciones, y a continuación se procederá a realizar casos prácticos relacionados con el tema.

## Conocimientos Previos

Conocimiento medio en computación y redes de datos.

## Requisitos Tecnológicos

1 Computador por cada asistente con conexión a Internet

## Material Auxiliar

Artículos técnicos (generalmente en el idioma ingles) para discusión general.

Silabo del módulo 1

Día 1: Introducción al hacking ético

* ¿Qué es la seguridad informática?
* Terminología básica
* Pentesting
* Tipos de ataques a un sistema
* Clases de hackers
* Fases del hacking
* ¿Por qué hackers éticos son necesarios?
* Alcance y limitaciones de un hacker ético
* Habilidades de un hacker ético

Día 2: Técnicas de búsquedas de huellas (Footprinting)

* El arte del footprinting
* ¿Qué tipo de información busca un hacker?
* Métodos para obtener información
* Herramientas básicas
* Herramientas avanzadas

Día 3: Escaneo

* Introducción
* Tipos de pruebas
* Metodología
* Escaneo de puertos
* Escaneo de vulnerabilidades
* Escaneo de red
* Técnicas de evasión

Día 4: Obtener acceso y mantener acceso

* Introducción
* Métodos básicos para romper contraseñas en Windows
* Utilización de rainbow tables para romper contraseñas
* Fuerza bruta
* Obtención de exploits
* Backdoors