# Syllabus del curso de Ethical Hacking y Seguridad Ofensiva

## MODULO 1 – INTRODUCCION AL ETHICAL HACKING

- Introducción al Ethical Hacking , Tendencias Actuales. Dónde Apuntan los ataques hoy, Riesgos y Componentes Asociados. Nuevos Riesgos
- Metodologías de Penetration Testing - Ethical Hacking , Introducción a OSSTM, OWASP, CVSS.
- Como platear un proyecto y/o servicio de Ethical Hacking, documentación y formatos requeridos.
-

## MODULO 2 – ETHICAL HACKING NETWORKING

- Footprint y reconocimiento con Google Hacking e Interrogación DNS .
- Escaneo de red redes con Nmap
- Enumeración de servicios
- Ataques de password craking a servicios
- CTF 1 : Obteniendo información del objetivo

## MODULO 3 - EXPLOITS Y VULNERABILIDADES

- Trabajando con exploits
- Introducción a Metasploit como framework de ataque
- Ataques a sistemas operativos Windows
- Ataques del lado Cliente
- Creando ejecutables infectados (Virus) , para conseguir control de Windows.

## MODULO 4 – ESCANEO DE VULNERABILIDADES

- Instalación y personalización de Nessus
- Escaneo de Vulnerabilidades avanzada con Nessus a nivel de Plataforma y aplicaciones
- Entendiendo reportes de Nesuss , detección de falsos positivos y falsos negativos
- CTF 2 : Detectando y explotando vulnerabilidades de un servidor

## MODULO 5 - ETHICAL HACKING A APLICACIONES WEB

- Introductorio a vulnerabilidades web
- Uso de proxys de interceptación Burp Suite, ZAP Proxy
- Explotando vulnerabilidades, en PHP y .NET ASP
- Ataques a servidores Web con Sql Inyection
- Explotando vulnerabilidades XSS, LFI, RFI, Upload, SQLI POST, Evacion de Login, HTML inyection, Ataques de fuerza bruta contra formularios de autenticacion, Acceso inseguro de objetos.
- Ataques de robo de sesión o session hijacking
- Haciendo un defacement (defaceo) de una pagina web

## MODULO 6 - ETHICAL HACKING DE API, SERVICIOS WEB Y MICROSERVICIOS

- Introductorio a los servicios web, SOAP, REST
- Ataques contra servicios web SOAP, SQL Inyection, WSDL Scanning, Web Service SAX Injection.
- Ataques contra API REST, divulgacion de información, Roptura de acceso, Inyecciones de SQL, devibilidad en token JSON, Mongo inyection, API google Hacking.
- Ataques contra microservicios en contenedores Docker

## MODULO 7 - ETHICAL HACKING A APLICACIONES MOVILES

- Introductorio a las aplicaciones Moviles en Andrioid y iOS

- Instalación de emulador para aplicaciones Android
- Análisis, descarga y descompresión de APK
- Crear archivos .java y analisis de métodos de la aplicación
- Análisis de dexfiles
- Capturar credenciales mediante log de la aplicación
- Análisis de bases de datos SQLITE
- Análisis de almacenamiento externo
- Ataques de inyeccion de SQL
- Captura de paquetes con ZAP Proxy
- Análisis dinámico de aplicaciones móviles con Frida
- Envenenamiento de aplicaciones móviles con Metasploit