



ENHACKE ETHICAL HACKING CERTIFICATION - EEHC

OBJETIVO GENERAL

- Capacitar al asistente con los conceptos profundos en 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

Al finalizar el Curso los alumnos estarán en capacidad de:

- Comprender y manejar conocimientos profundos acerca del funcionamiento de redes telemáticas y la seguridad informática.
- Entender el funcionamiento de técnicas, herramientas y métodos usados en la intrusión de sistemas.
- Ejecutar ataques con herramientas open source para el testeado de vulnerabilidades de la organización.

DESCRIPCIÓN DEL CURSO

El curso está orientado a desarrollar la metodología empleada por hackers maliciosos para penetrar los sistemas, utilizando determinadas herramientas para cada fase de la metodología.

Con este curso el participante estará en capacidad de encontrar las vulnerabilidades de las redes telemáticas de una organización desde el punto de vista de seguridad, con el fin de analizar y decidir si las configuraciones de los sistemas son las adecuadas o si las tecnologías cuentan con las actualizaciones recientes de forma que no puedan ser explotadas y originen pérdida de la información o indisponibilidad de servicio en las organizaciones.

Para ello las clases serán 70% práctica y 30% teórica. Los instructores enseñaran las técnicas más comunes y recientes del mundo del hacking.

Las clases cuentan con 2 profesores, los cuales se encargan de dictar la clase y hacer el seguimiento de los asistentes en la parte práctica.



Se proveerán a los asistentes las herramientas necesarias para hacer las técnicas que se vayan realizando en cada fase.

DURACIÓN

- 40 horas

TEMARIO

- Introducción al Hacking Ético
- Footprinting

Tipo de información que busca un hacker

Métodos para obtener información: Transferencia de Zona, ingeniería social

Herramientas Nslookup, dig

- Google Hacking
- Scanning

Nmap, angryIpScan, NetScan, PortScan, hping, barridos ping

- Enumeración

Herramientas de enumeración enum, smtputil, nbtstat

- Hacking de Windows

Explotando contraseñas: Rainbow Tables, Brutus

Protocolos de autenticación: NTLM, Kerberos, LM

Explotando con Metasploit

Arp Spoofing: Cain

- Troyanos y Backdoors

Netcat



Joiners
Rootkits

- Análisis de Vulnerabilidades

Introducción al análisis de vulnerabilidades
Alertas de seguridad
Escanners de vulnerabilidades
Nessus

- Cross Site Scripting e Inyección SQL

Técnicas más utilizadas para vulnerar servidores web

- Hacking de Linux

Comandos Linux
Estructura de archivos
Compilación de programas en Linux
Vulnerabilidades en Linux
Linux Rootkits
Exploando passwords: Hydra

- Wireless Hacking

- Firewall Iptables

Concepto
Instalación y configuración

- Sistema de detección de Intrusos

Concepto
Instalación y configuración de IDS Snort
Modos de funcionamiento

- Criptografía