Pentesting y Auditoria de Aplicaciones Web (24 Hrs)

DESCRIPCION DEL CURSO:

Este curso está diseñado para capacitar a profesionales y técnicos en TI en las técnicas y herramientas disponibles, usadas por los hackers para realizar un ataque desde Internet, redes internas a aplicaciones web y entornos basados en servidores web y de aplicaciones.

Objetivo:

Proporcionar al participante los conocimientos teóricos-prácticos que permita desarrollar las competencias necesarias realizar un proceso controlado de Pentesting que permite conocer las vulnerabilidades y de esta manera tomar las medidas preventivas en contra de agresiones maliciosas, valiéndose para ello de los tests de intrusión, que evalúan la seguridad técnica de los sistemas de información, redes de datos, aplicaciones web y servidores expuestos.

Competencias:

- Comprende un ataque a servidores web y aplicaciones a través de Internet
- Realiza una prueba de penetración
- Utiliza las herramientas idóneas para realizar un proceso de Auditoria
- Entender el funcionamiento de los ataques más comunes desde Internet como SQL Injection, Cross Site Scripting, Path Traversal, Session Hijacking, entre otros
- Comprende cómo protegerse de los ataque implementando medida de seguridad
- Reconoce las ventajas de la tecnología y los peligros al no tener una cultura de seguridad

Dirigido a:

- Profesionales en Tecnologías de la Información
- Desarrolladores de Aplicaciones Web
- Administradores de TI, Programadores
- Ingenieros de Testing de Aplicaciones Web

DETALLES DEL CURSO

Tema 1: Introducción a las Aplicaciones Web

- Funcionamiento de las Aplicaciones Web
- Seguridad de las Aplicaciones Web
- Owasp Top 10
- Owasp Testing Guide

Tema 2: Denegación de Servicio y Session Hijacking

- Técnicas de ataque DoS
- Herramientas de Ataque DoS
- Ataques basado en Session Hijacking
- Técnicas de Session Hijacking
- Tipos de Session Hijacking

Tema 3 : Pentesting de Servidores Web

- Arquitectura de Servidores Web
- Metodología para ataques a servidores web
- Recopilación de Información
- Analizando Metadata
- Footprinting de Servidores Web
- Mirroring de Sitios Web
- Hacking de Contraseñas en Aplicaciones Web
    - ❖ Hydra
    - ❖ DirBuster / WebSlayer

Tema 4: Análisis de Vulnerabilidades de Servidores Web

- Analizadores a Nivel Plataforma
- Analizadores a Nivel Aplicación
- Análisis de Vulnerabilidades a Nivel Plataforma
- Análisis de Vulnerabilidades a Nivel Aplicación

    - ❖ Nessus
    - ❖ Acunetix Web Vulnerability Scanner
    - ❖ Webshag
    - ❖ Skipfish
    - ❖ Nikto
    - ❖ Owasp-Zap

Tema 5: Pentesting de Aplicaciones Web

- Cómo funcionan las aplicaciones Web
- Como empezar a hackear una Aplicación Web
- Frameworks de Aprendizaje
- Métodos, Header, Body
- Entradas Inválidas
- Ataques de Directory Traversal
- URL encoding
- Cross Site Scripting
- SQL Injection
- Ejecución de Comandos
- Manejos de Shell

Tema 6: Explotación de Vulnerabilidades

- Trabajando con Exploits
- Metasploit Framework
- La Navaja Suiza del Hacker
- Proceso de Explotación de Vulnerabilidades

Duración: 24 horas.