CAPACITACIÓN

SEGURIDAD WIRELESS

HACKING OFENSIVO & PENTEST

En este curso el participante va a adquirir los conocimientos necesarios en **Hacking, Pentest** y protección en redes inalámbricas **Wi-Fi,** en donde se revisan aspectos como: protocolos, estándares, algoritmos de cifrado, análisis de señal, escaneo y monitoreo de tráfico y para buscar objetivos e implementar los diferentes ataques (**hacking**) y protección en redes **Wi-Fi.**

Este curso se impartirá en un laboratorio controlado en donde el participante aprenderá a utilizar herramientas para realizar ataques, auditar y proteger redes **Wi-Fi.**

Dirigido a: Aquellos profesionales que necesitan adquirir las habilidades necesarias para proteger y auditar la seguridad de Redes **Wi-Fi** y también para aquellos usuarios que están siempre conectados a la red desde cualquier lugar y momento.

Duración: 18 Horas.

Requisitos: Conocimientos básico de redes

TEMARIO:

Tecnología Wi-Fi

- Protocolos
- El estándar **IEEE 802.11** (**802.11b, 802.11g, 802.11n**)
- Radiofrecuencia, señal y riesgos
- Espectro, bandas, canales, frecuencias y modulación
- Legalidad y aplicación

Infraestructura de Redes y topologías

- Infraestructuras disponibles
- **Wi-Fi** y la inseguridad inherente
- La seguridad actual en **Wi-Fi: WEP, WPA y WPA2**
- Conexión a la red
- Proceso de asociación y autenticación

- Tramas de gestión (**managementframes**)
- Tramas de control (**control frames**)
- Tramas de datos (**data frames**)

Hacking & Cracking enredes Wi-Fi

- Terminología
- **Hackers** y **Crackers** legales
- **Hackers** y **Crackers** ilegales
- **Phreakers**
- **Lammers**
- Legalidad

Creando el equipo de Pentesting

- Hardware y Software para**Pentesting**
- Adaptadores **Wi-Fi** y Antenas **Wi-Fi**
- Accesorios (conversores, extras)
- Herramientas y programas
- Redes **Wi-Fi** y Linux
- **Kismet, Netstumbler** y **kali Linux**
- Instalación de Software y utilidades
- Configuración de puntos de acceso
- Configuración de tarjetas inalámbricas
- El primer escaneo
- Detectando los clientes
- Volcando las capturas a fichero
- Captura dirigida
- Sintonizar y análisis de la señal
- Analizar la señal con **airodump-ng**
- Analizar la señal con**Kismet**
- Buenas prácticas

Ataques en Redes Wi-Fi

- Crear una interface en modo monitor
- Ocultación de huellas y ataques a redes abiertas
- Falseando direcciones **MAC**

Capturando y analizando el tráfico del objetivo

- **Sniffing** de paquetes inalámbricos
- **Sniffing** de paquetes de datos de la red
- Inyección de paquetes

- Descubriendo SSIDS ocultos

Otros ataques en redes abiertas (ataques HOTSPOT)

- Ataque de denegación de servicio a clientes
- Ataque de suplantación a clientes
- Captura de credenciales de acceso al**hotspot**

Ataques a redes WEP

- Encriptación **WEP**
- Debilidades del cifrado **WEP**
- Cracking **WEP**
- Tipos de ataques a redes **WEP**
- Ataque pasivo y ruptura por estadística y diccionario
- Ataque activo de reinyección **ARP**
- Ataque activo de reinyección mediante selección interactiva

Ataques a WPA/WPA2 y WPS

- Ataques en redes **WPA/WPA2**
- Ataque de fuerza bruta mediante diccionario
- Buscar el objetivo: punto de acceso + clientes conectados
- Ataque de de-autenticación
- Capturando el **handshake**
- Ruptura de la clave por diccionario
- Diccionario de claves
- Ataque a **WPS**
- **Fake AP**
- Herramientas de monitorización

Ataques a la infraestructura Wi-Fi

- Hacking de cuentas por defecto en el punto de acceso
- Hacking de cuentas usando ataques de fuerza bruta
- Ataque de denegación de servicio
- Ataque de de-autenticación **DOS**
- Ataque de desasociación
- **Evil Twin** y suplantación de identidad de punto de acceso **MAC**
- **Evil Twin** y suplantación de **MAC**

- Evil Twin y saltos de canal
- Punto de acceso renegado
- Punto de acceso ilegitimo
- Atacando a los clientes
- **Honeypot**y ataque **MIS Assoctiation**

Ataques avanzados Wi-Fi

- **Man-in-the-Middle**
- Ataque **man-in-the-middle**
- **Man-in-the-middle**bajo**Wireless**
- Espionaje inalámbrico mediante **MITM**
- Secuestro de sesión sobre redes inalámbricas
- **Hijacking**de sesión bajo Wireless
- Desafío secuestro de aplicación o**hijacking**
- Enumeración de perfiles de seguridad inalámbrica

Buenas prácticas para proteger Redes Wi-Fi

- Establecer políticas y procedimientos de seguridad **Wi-Fi**
- Cambio del **SSID**
- Desactivación del broadcast del **SSID**
- **RADIUS**, **VPN,** y **Firewalls**
- Utilización de **802.1x/EAP** y **RADIUS**
- Resumen