Informática Integrada
Internetworking

La Certificación de Seguridad, Hacking y Pentest más demandada de la industria.

Master en Seguridad & Hacking Ético

EXIN

PEARSON VUE-Authorized Test Center

PRESENTACIÓN

Este **Diplomado** es perfecto para aquellos profesionales que quieran incursionar en la **Seguridad y Hacking** de **Tecnologías deTI e Internet**, donde se examinarán técnicas de **Blindaje, Encriptación, Autenticación, Control de Acceso, Análisis de tráfico**, **Firewall/VPNs**, **Seguridad Wireless**, **Google Hacking**, **Pentest, SQL Injection,** etc.. y medidas de prevención utilizando herramientas avanzadas de seguridad y de clase mundial.

Este entrenamiento se lleva a cabo en un laboratorio extremadamente desafiante utilizando escenarios reales que enfrentan los profesionales en **Offensive Security** durante las pruebas de penetración en vivo.

DIRIGIDO A:

Gerentes de TI, **Auditores de Ciberseguridad**, **CISO** (**Chief Information Security Officer)** especialistas en TI, proveedores de Internet, ingenieros que trabajan como **Pentester**, profesionales de las áreas de **Computació**n, **Sistemas**, **Electrónica** y **Telecomunicaciones** que deseen actualizar sus conocimientos e implementar seguridad en sus **Centros de Datos.**

REQUISITOS:

- Conocimientos básicos de **Networking, Linux y Windows**
- Los candidatos deben ser muy conscientes de la diferencia entre el **Hacking legal** el **Hacking ilegal** y las consecuencias del mal uso.

BENEFICIOS:

- El participante estará listo para hacer frente a vulnerabilidades y amenazas **Cibernéticos** de las empresas y darle un solución
- Detectará vulnerabilidades e intrusos y realizara pruebas de penetración, para encontrar fallos en el sistema
- Evitara el espionaje o el robo de información de los sistemas informáticos
- Evitara cualquier contratiempo o daño a la infraestructura informática, o continuidad de negocio
- Aprenderá a utilizar pruebas de penetración con metodología y estándares como: **OSSTMM**, **OWASP** etc..
- Sera reconocido como **Hacker Ético**, **Pentester** y **Experto en Seguridad**
- Será capaz de implementar los nuevos esquemas de seguridad y buenas prácticas bajo la norma **ISO/IEC 27001**.
- Estará apto para desarrollar estrategias que enfaticen la seguridad y resguardo de la información de su empresa.
- Estará listo para aprobar el examen de certificación: **EXIN ETHICAL HACKING FOUNDATION®**

Informática Integrada
Internetworking

Esta **Certificación** de **Seguridad y Hacking Ético** está desarrollada bajo la firme convicción de que la mejor manera de lograr una **Seguridad Defensiva** es a través de un **Enfoque Ofensivo**.

Nuestros instructores están altamente capacitados en **Seguridad y Pruebas de Penetración** que tienen una amplia experiencia en sistemas de ataque para ver cómo responden.

Master en Seguridad & Hacking Ético

EXIN

PEARSON VUE-Authorized Test Center

En este Diplomado aprenderás a

- Que es el **Hacking** y consecuencias
- Las metodologías de **Pentest** y **Hacking Ético** mas reconocidas
- Blindaras servidores **Linux/Windows** contra cualquier tipo de ataque
- Configuraras **Firewalls**, **Seguridad perimetral** y **DMZ**
- Configuraras de Redes Privadas Virtuales **(VPNs)**
- Identificar IP, Servidores de **Mail** y **DNS** de un objetivo
- Realizar escaneos de puertos e identificar vulnerabilidades de los sistemas
- Identificar sistemas operativos y versiones de software instalado
- Comprender los conceptos de **Buffer Overflow**, **Exploit** y **Shellcode**
- Realizar pruebas de ataque tanto externas como internas
- Utilizar la herramienta de explotación **Metasploit**
- Comprenderás que es una sesión **Hijacking** y sus modalidades
- Comprenderás que es **Spoofing** (suplantación) y como evitarlo
- Comprenderás que es un ataque de hombre en medio (**man-in-the-middle**)
- Capturar tráfico de una red y su análisis con **Wireshark**
- Comprender que es desbordamiento de **Buffer** (**Buffer Overflow**) y como evitarlo
- Comprender ataque de denegación de Servicios **DoS/DDoS y** como mitigarlos
- Comprender ataques a servidores y aplicaciones Web y como evitarlos
- Comprender los tipo de ataque en **Bases de Datos SQL**
- Realizar ataques **XSS**, **CSRF**, **SQL Injection** y como evitarlos

Master en Seguridad & Hacking Ético

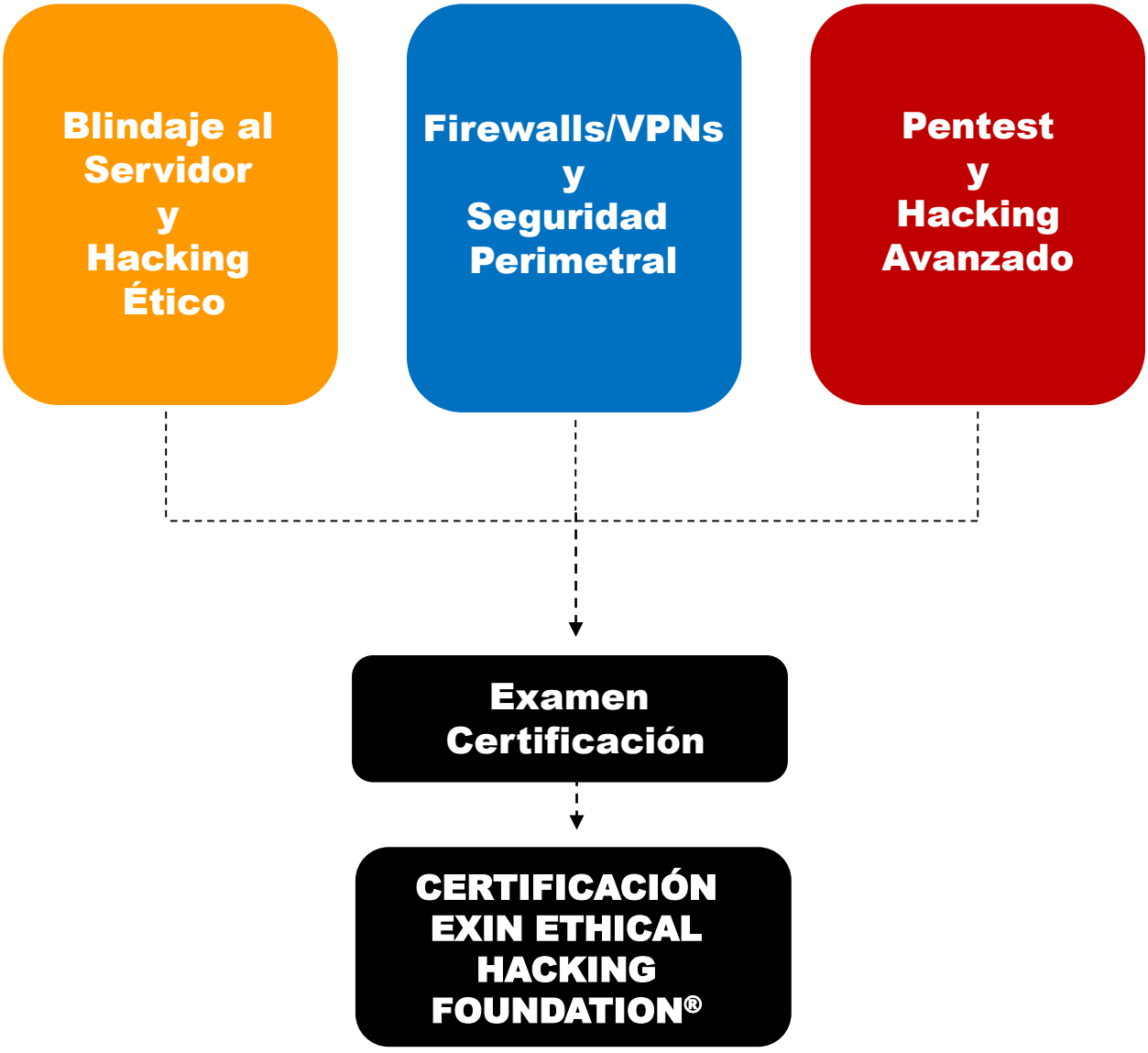
En este Diplomado aprenderás a

- Aspectos de **Hacking** en redes **Wireless** y como evitarlo
- Realizar ataques a dispositivos móviles (**Google Android OS y iOS Apple**) y su mitigación
- Entender que es la **Criptografía Simétrica**, **Asimétrica** y **Hash** y su aplicación
- Comprenderás técnicas de ataque de **Ingeniería social y prevención**

Master en Seguridad & Hacking Ético

Informática Integrada
Internetworking

Módulos:



EXIN

PEARSON VUE-Authorized Test Center

Blindaje al Servidor y Hacking Ético

Objetivo:

Proveer al participante bases sólidas en **Blindaje del servidor** y **Hacking Ético** utilizando la **metodologías de penetración,** usando herramientas de búsqueda de **reconocimiento**, **detección de vulnerabilidades**, **análisis de tráfico**, además de revisar las últimas técnicas de **ataque a contraseñas**, **ingeniería social,** puertas traseras (**Backdoors**) y **Seguridad Ofensiva** terminando con la toma de control de sistemas a través de la explotación de vulnerabilidades y las medidas de protección necesarios para evitarlos además de la implementación de buenas prácticas basadas en **ISO/IEC 27001**.

Dirigido a: Profesionales en el área de **TI**, **Pentester**, **Hackers Éticos**, profesionales de las áreas de **Computación, Informática, Sistemas, Electrónica, Sistemas y Telecomunicaciones** que deseen Blindar su centro de datos y realizar **pruebas de penetración.**

Requisitos: Conocimientos básicos de **Linux/Windows**

Duración: 22 hrs.

TEMARIO: **Blindaje al Servidor y Hacking Ético**

Introducción al Hacking Ético

- Introducción
- Elementos de seguridad
- Diferencia entre pruebas de penetración y **Ethical Hacking**
- Importancia del **Hacker Ético**
- Consideraciones

Objetivos de la seguridad en TI

- Confidencialidad
- Disponibilidad
- Integridad
- No repudio

Metodologías para realizar pruebas de penetración

- **PTES** (Penetration Testing Execution Standard)
- **OSSTMM** (Open Source Security Testing Methodology)
- **NIST 800-115** (National Institute Standards and Technology)
- **ISSAF** (Information Systems Security Assessment Framework)
- **PTF** (Penetration Test Framework)

Amenazas y fraudes en los sistemas de la información

Leyes y la seguridad de la información

TEMARIO: **Blindaje al Servidor y Hacking Ético**

..continuación

Blindaje del Sistema Operativo

- Instalación segura de servidores **Linux/Unix**
- Estándares de seguridad básicos para S.O de red
- Instalación, particiones y seguridad
- Particiones primarias, extendidas y lógicas
- Sistema **RAID (Redundant Array of Inexpensive Disks)**
- **Hardware RAID** vs. **Software RAID**
- Elección del método de arranque
- Implementación de Sistemas **RAID**
- Creación de **LVM (Logical Volume Management)** paso a paso

Configuración de Networking en Linux

- Configuración de **interfaces**
- Configuración **routing** y rutas estáticas
- Manejo y monitoreo de interfaces de red
- Configuración de direcciones **IPv4** e **IPv6**
- Uso de: **ifconfig**, **ifup**, **ifdown**, **route**, **netstat**, **tcpdump**, **ping**, **hostname**, **traceroute**, etc..

Recolección de datos del objetivo (footprinting)

- Reconocimiento
- **Whois** y Registros Regionales de Internet
- Servidores y **Zonas DNS**
- Rango de Red y sub-red (**Network Range y subnet mask**)

TEMARIO: **Blindaje al Servidor y Hacking Ético**

*..**continuación***

- Nombres de Dominios (**Domain Names**)
- Bloques de Red (**Network Blocks**)
- Direcciones IP específicas
- País y Ciudad donde se encuentran los Servidores
- Información de Contacto (números telefónicos, emails, etc.)
- Tipos de DNS Records: **A** (**address**), **MX** (mail exchange) **NS** (**name server**), **CNAME** (canonical name), **SOA** (**start of authority**), **TXT** (text), **HINFO** (**host info**)

Herramientas de recolección de datos

- **Nslookup**, **dig**, **host**
- Redes sociales y buscadores de personas
- **Google Hacking®**, **Google operadores**
- Herramientas en línea (**Online**) **netcraf**, **archive.org**
- Análisis de vulnerabilidades

Escaneo de puertos para realizar ataques

- Test de puertos abiertos
- **Técnicas de escaneo de puertos**
- **TCP Connect , TCP SYN, Stealth,** (**FIN Scan**), **ACK Scan**, **Null Scan, TCP Xmas Scan**, **Idle Scan**, **UDP ICMP Port Scan**, **ICMP ping-sweeping**

Herramientas de escaneo

- **Nmap, Hping3, Scapy, SolarWinds, etc..**

TEMARIO: **Blindaje al Servidor y Hacking Ético**

..continuación

Herramientas para evitar escaneo

- Configurar **Firewall**(**IPTABLES**) e **IDS** (**SNORT**)
- **PortScanDetector, PortSentry**
- **Sistema de detección de intrusos (IDS)**
- Arquitectura de un **IDS**
- Sistema de detección de intrusos en Host (**HIDS**) y Red (**NIDS**)
- Dónde colocar el **IDS**
- **Snort** como **IDS**
- **Snort** en modo **Sniffer**, registro de paquetes y **NDIS**

Recolección de información (Enumeración)

- Entendiendo: **/etc/passwd, /etc/group, /etc/shadow y /etc/skel**
- **Login/password**
- Entendiendo y aplicando permisos a archivos y directorios con: **chmod, chown, chgrp, lsattr, chattr, umask**
- Manejo de Entradas y Salidas
- Filtros y herramientas de usuario
- Seguridad en la consola del servidor
- Manejo de cuentas de Administrador y súper-usuario
- Seguridad en cuentas y grupos de trabajo
- Administración del control de acceso
- Manejo de permisos y atributos de archivos y directorios
- Seguridad en la consola del servidor
- Enumeración de equipos
- Acertar maquinas activas

TEMARIO: **Blindaje al Servidor y Hacking Ético**

..continuación

- Detección versiones de Sistemas Operativos
- Enumeración de recursos compartidos
- Enumeración **NetBIOS, SNMP, UNIX/Linux, LDAP, NTP, SMTP, DNS**
- Herramientas de enumeración y uso

Ataque a contraseñas (password)

- Ataque a contraseñas
- Tecnicas de ataque a contraseña
- Ataque basado en diccionario, fuerza bruta y basado en reglas
- Ataque a contraseña mediante técnica hombre en medio (**Man-in-the-Middle**)
- Ataque a contraseña mediante **Troyanos**, **Spyware** y **Keyloggers**
- Ataque atreves de **Rainbow Tables** mediante valor **hash**
- Crakeando algoritmos de cifrado: **DES, MD5 y Blowfish**
- Crack de contraseñas con **John the Ripper**

Metasploit Framework

- **Metasploit** a profundidad
- Arquitectura de **Metasploit**
- Manejo de **Mestasploit framework**
- Kali Linux y **Metasploit framework**
- Detección de redes y ejecución de **exploits**
- **Information gathering**
- Interactuando con **MSF** (**msfconsole**, **msfcli**, **msfgui**, **msfweb**)
- Obteniendo Información y Análisis de Vulnerabilidades

TEMARIO: **Blindaje al Servidor y Hacking Ético**

..continuación

Criptografía

- ¿Qué es la **Criptografía**?
- Criptografía Simétrica: **DES, 3DES, Blowfish, IDEA**
- Criptografía Asimétrica: **Diffie-Hellman, RSA, DSA**
- Certificados digitales
- **Hashing**: **MD5, SHA**
- Implantación

Ingeniería social

- Comportamiento vulnerables a ataques
- Fases de la ingeniería social
- Ataques de ingeniería social
- Ataque basada en relación humana(**Impersonalización, Shoulder Surfing**, **Dumpters Diving**)
- Ataque basado en la computadora (**Phishing**, **Online Scams**)
- **Tailgating** y **Piggybacking**
- Robo de identidad
- Ingeniería social inversa
- Contramedidas para ataque de ingeniería social

Firewalls/VPNs y Seguridad Perimetral

Objetivo:

Proveer al participante los conocimientos para el manejo de tecnologías de **filtrado de paquetes** asociados a servicios de Internet, detección de puntos vulnerables, además del diseño, implementación y administración de **Firewalls** e implementación de Redes **Privadas Virtuales** (**VPNs**) que permitan proteger las redes corporativas frente a posibles ataques.

Dirigido a: Profesionales en el área de **TI**, **Pentester**, **Hackers Éticos**, profesionales de las áreas de **Computación, Informática, Sistemas, Electrónica** y Telecomunicaciones que deseen implementar **Firewalls** y **VPNs**

Requisitos: Conocimientos de **Linux/Windows** y redes **TCP/IP**.

Duración: 18 hrs.

TEMARIO: **Firewalls/VPNs y Seguridad Perimetral**

Introducción

- Funciones del **Firewall**
- Clasificación de **Firewalls**
- Firewalls y el modelo **OSI/DOD**
- Análisis de la seguridad de **TCP/IP**

Aspectos importantes de TCP/IP: Datagramas y segmentos

- Datagramas: **ICMP**, **UDP**, **TCP**
- Herramientas **TCP/IP**: **ifconfig, ping, route, traceroute, host, nslookup, tcpdump, tcpshow**
- Diseño e Implementación de **Firewalls**

Introducción a las VPNs

- Qué son las VPNs
- Requerimientos básicos
- Conceptos de tunneling
- Repaso a los protocolos **PPP**, **PPTP** y **L2TP**

Tecnologías de encriptación

- Encriptación simétrica vs. asimétrica
- Funciones hash

TEMARIO: **Firewalls/VPNs y Seguridad Perimetral**

..continuación

- Algoritmos de encriptación y fortalezas relativas
- **DES**, **3DES**, **AES**, **3AES**, **Diffie-Hellman**, **El-Gamal**, **DSS**
- Firmas digitales y Certificados digitales
- Autoridades independientes vs. autoridades comerciales
- Criterios de diseño de redes **VPNs**

Arquitectura de Firewalls y VPNs

- Reenvío de paquetes y filtrado de paquetes
- **Firewalls**, Intranets y Zonas Desmilitarizadas (**DMZ**)
- Soluciones **Firewall**

Topología Host a Host OpenVPN

- Generación de clave de encriptación
- Configuración del servidor y cliente

Topología RoadWarrior OpenVPN

- Consideraciones preliminares
- Creando el CA
- Generación del certificado para el servidor
- Generación de la clave de encriptación para el servidor
- Generando certificados y claves privadas para los clientes
- El parámetro de **Diffie-Hellman**
- Configuración del servidor y cliente

TEMARIO: **Firewalls/VPNs y Seguridad Perimetral**

..continuación

Funcionamiento de Firewall IPTables

- La tabla **Filter** y sus operaciones (**FORWARD**, **INPUT**, **OUTPUT**)
- Configuración de reglas **IPTables**
- Configuración de cadenas **INPUT**, **OUTPUT**, **IN**, **OUT**
- Arranque y baja de **IPTables**
- Objetivos **IPTables**: **ACCEPT**, **DROP**, **REJECT**, **LOG**
- Seguridad perimetral y Zona Desmilitarizada (**DMZ**)

Introducción a la seguridad perimetral y DMZ

- Diseñando un perímetro seguro y **DMZ**
- Reforzando la seguridad del perímetro y **DMZ**
- Monitoreo de la seguridad del perímetro y **DMZ**

Implementación de seguridad perimetral y DMZ con IPTables

- Reenvío de paquetes Traducción de direcciones (**NAT**)
- La tabla **NAT** (**Network address Translation**) y sus funciones **PREROUTING**, **POSTROUTING**
- Manejo de traducción de direcciones (**DNAT**, **SNAT**)
- Redireccionamiento de puertos y enmascaramiento
- Optimización del **Firewall** y manejo de errores
- Evaluando la seguridad perimetral y **DMZ**
- Prueba de **Firewalls** y Resolución de problemas

TEMARIO: **Firewalls/VPNs y Seguridad Perimetral**

..continuación

Protección avanzada de IPTables

- Buscar y detener tráfico sospechoso
- Definir reglas de acceso basadas en tiempo
- Protegemos de un tipo de **"buffer overflow exploits"**
- Limitar el tamaño del registro
- Bloque de tráfico entrante de host o dominio

Herramientas de comprobación del Firewall

Pentest y Hacking Avanzado

Objetivo:

Proveer al participante los conocimientos avanzados en ataques: Denegación de servicios **DoS/DDoS**, secuentro de sesiones (**Hijacking), Suplantación(Spoofing), SQL Injection, Servidores Web, Dispositivos Móviles (Google Android® OS** y **iOS Apple®) Seguridad Wireless** .etc.. Este curso te presenta las últimas herramientas de **Hacking** y técnicas en el campo e incluye laboratorios donde se realizan pruebas de principio a fin.

Dirigido a:

Aquellos profesionales de seguridad que desean realizar **Tests de Intrusión**, **Hacking Ético avanzado**

Requisitos:

Conocimientos de Linux/Windows y redes TCP/IP.

Duración: 24 Horas

TEMARIO: **Pentest y Hacking Avanzado**

Ataque de denegación de servicio (Dos/DDoS)

- Que es un ataque de denegación **(DoS/DDoS)**
- Tipos de ataque **DoS**
- Inundación **SYN** (**SYN Flood**), **ICMP** (**ICMP Flood**)
- Ataque **Smurf**
- Inundación **UDP** (**UDP Flood**)
- **Buffer Overflow**
- Ataque **DDoS**
- Estrategia de defensa en ataques **DoS/DDoS**

Hijacking (secuestro de sesiones)

- Que es ataque **Hijacking**
- **Spoofing** vs. **Hijacking**
- **IP hijakers**
- **Page hijacking**
- **Secuestro de dominio**
- **Secuestro de sesión**
- **Browser hijacking**
- **Contramedidas**

TEMARIO: **Pentest y Hacking Avanzado**

..continuación

Spoofing (suplantación)

- Que es el **Spoofing**
- Tipos de **Spoofing**
- **IP Spoofing**
- **ARP Spoofing**
- **DNS Spoofing**
- **Web Spoofing**
- Contramedidas para **Spoofing**

Ataque y defensa a servidores Web

- Por qué hackean los sitios Web?
- Vulnerabilidades del servidor Web y manipulación de **URL**
- Aprovechamiento de las debilidades de los identificadores de sesión
- Aprovechamiento de las debilidades de sistemas de autenticación
- Ataque por Inyección (**Structured Query Language Injection**)
- Ataque de Denegación de Servicio (**DoS**)
- Ataque de fuerza bruta
- Inyección de scripts maliciosos **Cross-site Scripting** (**XSS**)

TEMARIO: **Pentest y Hacking Avanzado**

..continuación

Ataque a bases de datos SQL

- Bases de datos y vulnerabilidades
- Tipos de inyección y usuarios malintencionados
- **OWASP** (**Open Web Application Security Project**)
- Cómo funciona **SQL Injection**
- Ataque **Blind SQL Injection**
- Atacando base de datos realizar consultas
- Realización de accesos ilegítimos
- Ejecución de comandos en el servidor, subida y lectura de archivos
- Rompiendo la integridad de datos almacenados
- Revisando el código para vulnerabilidades de inyección por **SQL**
- Probando las Vulnerabilidades de Inyección **SQL Contents**
- Cómo evitar las vulnerabilidades por inyección **SQL**

Ataque a Redes Wireless

- La familia de protocolos **IEEE 802.11**
- Wireless y la inseguridad inherente
- La seguridad actual en Wireless: **WEP, WPA** y **WPA2**
- Ataques a redes **WEP**
- Debilidades del cifrado **WEP**
- Tipos de ataques a redes **WEP**
- **Cracking WEP**
- Ataque pasivo y ruptura por estadística y diccionario
- Ataque activo de reinyección **ARP**

TEMARIO: **Pentest y Hacking Avanzado**

..continuación

- 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** y **Fake AP**
- Herramientas de monitorización
- Ataques a la infraestructura Wireless
- **Evil Twin** y suplantación de identidad de punto de acceso **MAC**
- Punto de acceso renegado e ilegitimo
- Atacando a los clientes
- **Honeypot** y ataque **MIS Assoctiation**
- Ataques avanzados **Wireless**
- Buenas prácticas para proteger Redes **Wireless**

TEMARIO: **Pentest y Hacking Avanzado**

..continuación

Ataque a Dispositivos móviles

- Arquitectura y sistemas operativos
- Modelo se seguridad en sistemas operativos
- **Google Android OS** y **iOS Apple**
- Problemas de Seguridad en Dispositivos Móviles
- Pruebas de penetración en dispositivos Móviles
- Contramedidas

www.informaticaintegrada.com.mx