



POSTGRADO EN SEGURIDAD INFORMÁTICA Y HACKING DE SISTEMAS

*La mayor amenaza de la sociedad moderna
no tira bombas, ni grita, no tiene identidad:
es el hacking y su medio es la red.*



INTRODUCCIÓN

El conocimiento informático y los sistemas digitales han probado sobradamente su utilidad como herramienta de apoyo en numerosas áreas del saber. Un área de conocimiento emergente, como es la seguridad informática de redes y sistemas, no debería ser una excepción. El desarrollo de las arquitecturas telemáticas que hoy gestionan servicios de vital importancia para el avance de la sociedad y su continuo funcionamiento, se tiene que beneficiar de metodología y conocimiento aplicado para asegurar el correcto y fiable comportamiento de dichos servicios. El postgrado pretende transmitir el conocimiento y el correcto uso de herramientas que faciliten el análisis de riesgo de la información y protección de la continuidad del negocio que empresas e instituciones pueden demandar con el objeto de mejorar la seguridad de las infraestructuras informáticas que nos rodean.

Demanda Social y Profesional:

El diseño del curso obedece a una amplia y creciente necesidad en el mundo empresarial y de las instituciones públicas de proteger, asegurar y resguardar la información sensible o confidencial que manejan y almacenan. A su vez, esta necesidad se refleja también en la creciente demanda de personal cualificado para establecer métodos de protección y de fiabilidad de los sistemas informáticos susceptibles de ser comprometidos o asaltados con intenciones maliciosas.

El actual desarrollo de las nuevas tecnologías de la información y la comunicación (NTIC), así como su accesibilidad a un amplio número de usuarios, ha simplificado tanto el problema de entender el funcionamiento de los ordenadores y las redes que ha abierto una nueva puerta a conductas criminales y antisociales, imposibles de concebir hace unas décadas. Así, ha aparecido un nuevo tipo de intrusos en empresas e instituciones con la consecuencia obvia de una demanda de formación en perfiles profesionales cuyo objetivo sea la creación de una barrera de contención contra ellos, disponiendo de metodologías aplicables para gestionar y mantener los sistemas en niveles fiables.

El alumno adquirirá a lo largo del curso los conocimientos necesarios para ser capaz de sustentar, analizar, mejorar y proponer políticas de seguridad contra el intrusismo informático en redes corporativas, empresariales e institucionales mediante la utilización de las técnicas y metodologías aprendidas durante su formación con el objetivo de enfrentar el problema del aseguramiento continuo.

El curso proporcionará también a los alumnos los conocimientos necesarios para:

- analizar las técnicas de hacking utilizadas por intrusos maliciosos cuando planean e intentan un ataque a servidores, sistemas de redes de ordenadores o la propia Internet.
- establecer determinadas políticas de seguridad en su empresa o puesto de trabajo.
- detectar puntos débiles y fisuras en la seguridad implementada.
- subsanar los problemas detectados, manteniendo un correcto control sobre las medidas implementadas.
- conocer las ventajas e inconvenientes de las tecnologías inalámbricas en términos de seguridad con el objeto de poder enfrentar proyectos complejos que requieran de seguridad.

Actividades Complementarias:

Tratándose de un curso eminentemente práctico, a lo largo de él se pondrán en práctica, para cada uno de los módulos en que está estructurado, técnicas aplicadas a la recreación de situaciones reales de intrusismo, detección de incidencias, predicción y seguridad de la confiabilidad de sistemas del mundo empresarial.

Además, se incluirá un trabajo tutorado de final de curso donde los alumnos deberán aplicar las técnicas y metodologías aprendidas con el objeto de superar el curso y obtener su acreditación.



Programa de **POSTGRADO EN SEGURIDAD INFORMÁTICA Y HACKING DE SISTEMAS**

INFORMACIÓN general

OBJETIVOS :

Desarrollar un nuevo perfil de profesional que, haciendo uso de las tecnologías digitales y sus aplicaciones concretas, así como de sus conocimientos de seguridad informática, pueda detectar, subsanar y predecir fisuras de seguridad informática. Elaborar planes de contingencia basados en el método científico y dar respuesta a una amplia y creciente necesidad en el mundo empresarial y de las instituciones de proteger y resguardar la información sensible o confidencial que manejan y almacenan.

DIRIGIDO :

Diplomados o licenciados universitarios y alumnos de último año de carrera.
Profesionales con experiencia demostrable en el campo de las nuevas tecnologías.

METODOLOGÍA:

La metodología de trabajo es activa y participativa para conseguir una integración entre la teoría y la práctica y así potenciar las dos vertientes. Se proponen casos reales y ejercicios prácticos para poder resolver en grupos de trabajo y se realizarán aplicaciones y simulaciones de diferentes temas tratados en los distintos módulos.

CALENDARIO :

- Inicio : 6 de noviembre de 2009
- Final: 8 de mayo de 2010

Los módulos se realizarán en sesiones de 4 y 5 horas, los viernes de 17:00 a 21:00 y los sábados de 09:30 a 14:30.

DIRECCIÓN ACADÉMICA:

Joan Gil.
Director de la Esc. Universitaria Politécnica de Mataró.
Ingeniero

DIRECCIÓN TÉCNICA:

Sílvia Pont Monsó.
Licenciada en Psicología y Máster en Dirección de Recursos Humanos. Responsable del área de Formación de Cetemmsa.

DURACIÓN :

198 horas

EVALUACIÓN:

La evaluación de los alumnos se hará teniendo en cuenta el nivel de aprovechamiento de los conocimientos adquiridos durante el curso, quedando reflejado en parte con un trabajo práctico en el que aplicarán los conocimientos expuestos durante el curso. El trabajo deberá ser entregado en un plazo fijado al finalizar el curso.

TITULACIÓN:

Diploma de Postgrado UNIVERSITARIO otorgado por la Escuela Universitaria Politécnica de Mataró adscrita a la Universidad Politécnica de Cataluña.

Para obtener el título es necesaria la asistencia a las sesiones de formación y superar las pruebas de evaluación previstas.

LUGAR DE REALIZACIÓN :

- Escuela Universitaria Politécnica de Mataró



PROGRAMA

MÓDULO 1:

IDENTIFICACIÓN DE PROBLEMAS Y PRIMERAS TÉCNICAS

(9 horas)

OBJETIVOS DEL MÓDULO :

Se establecerán las bases necesarias para una correcta comprensión de los mecanismos que entran en juego en Internet y las redes informáticas. Se dará una visión general y a la vez aplicada de la seguridad informática en la sociedad actual y las organizaciones empresariales. Iniciación a primeras técnicas.

Introducción y conceptos previos.

- ¿Qué es la seguridad informática?
- Campos de acción de la seguridad informática.
- Tipos de protección.
- Seguridad de los sistemas operativos.
- Seguridad en redes.
- Herramientas de seguridad informática.
- La utilización de sitios Web indispensables para trabajar en seguridad informática.

Seguridad de los sistemas de información.

- Seguridad en el acceso a la información
- Niveles de servicio
- Medidas
- Salvaguarda de la información

Teoría de redes, Protocolos imprescindibles y el protocolo TCP/IP.

- Capas de red.
- Direcciones IP, Intranet, Extranet. Internet.
- Mascara de subred.
- Protocolo ARP.
- Protocolo IP.
- Protocolo ICMP.
- Encaminamiento.
- Capa de transporte.
- Puertos.
- Protocolo UDP.
- Protocolo TCP.
- Nombre de dominio.

MÓDULO 2:

HACKING E INTRUSIÓN A SISTEMAS INFORMÁTICOS

(36 horas)

OBJETIVOS DEL MÓDULO :

Se analizarán y llevarán a la práctica los pasos y procedimientos que se utilizan a la hora de introducirse o auditar un sistema informático. Pasando desde la obtención de información del objetivo hasta técnicas de análisis de tráfico con objetivos maliciosos. Se aprenderá a auditar sistemas y su seguridad a la vez que a implementar medidas que mitiguen riesgos.

PROFESOR : Antonio Ramos Varón

Técnicas de Rastreo, Exploración y Enumeración.

- ¿Qué es seguir el rastro a un objetivo?
- Seguir el rastro en Internet.
- Determinación del ámbito de actividades.
- Enumeración de la red.

- Interrogaciones DNS.
- Reconocimiento de la red y su topología previo al ataque.
- Ejercicios prácticos de rastreo, exploración y enumeración.
- Interpretación de resultados, fisuras y contramedidas a adoptar.

Exploración del objetivo.

- Barridos ping, consultas ICMP.
- Exploración de puertos.
- Tipos de escaneos a realizar sobre el objetivo.
- Detección del sistema operativo, versiones y servicios en ejecución.
- Herramientas automáticas de descubrimiento y contramedidas.
- Utilización de herramientas (vulnerability scanners) para la auditoria de sistemas y detección de vulnerabilidades.
- Interpretación de resultados y fisuras.
- Medidas a adoptar ante las fisuras.

Enumeración.

- Enumeración Windows NT/2000/2003/2008.
- Enumeración Linux/Unix.

Técnicas de hacking contra los sistemas y contramedidas.

- Introducción.
- Métodos para engañar a los ficheros .log en la ofensiva.
- Técnicas de suplantación de IP atacantes en Internet (looping spoofing ip).
- Medidas a implementar de prevención.
- Obtención de exploits (el problema buffer overflow).
- Compilación y utilización de exploits sobre vulnerabilidades.
- Escalada de privilegios.
- Detección de la utilización de exploits contra nuestra red.
- Métodos utilizados para descargar herramientas de prospección.
- Cómo se recaba información una vez en el sistema.
- Medidas de seguridad a que se deben implementar.
- Alteración, falsificación e intoxicación de ficheros .log.
- Establecimiento de puertas traseras (backdoors).
- Metodología para la detección de puertas traseras.

Metodología de la intrusión en sistemas (Ampliación de Métodos intrusivos).

- Introducción.
- Incursión en sistemas por Netbios
- Ocultación de ficheros mediante streaming.
- Prácticas de stream sobre ficheros.
- Técnicas de ocultación avanzadas mediante Rootkits.
- Prácticas sobre Rootkits.
- Obtención Consolas reversas.
- Prácticas sobre reverse shell.
- La troyanización de programas con fines maliciosos.
- Prácticas sobre troyanización.
- Anulando la efectividad de los antivirus (generación de herramientas indetectables)
- Desarrollo de la metodología expuesta.
- Discusión de contramedidas a adoptar.

Con la colaboración de:



Programa de **POSTGRADO EN SEGURIDAD INFORMÁTICA Y HACKING DE SISTEMAS**

Auditoría sobre políticas de usuario y contraseñas.

- Análisis del problema en la organización.
- Métodos de descifrado y ruptura de contraseña (passwords).
- Herramientas para el análisis de contraseñas.
- Implementación de políticas confiables.

Auditorías sobre los servicios en Internet con sistemas de validación.

- Análisis de servicios con sistemas de validación que pueden ser comprometidos: ftp, webmail, mail, sitios Web.
- Ataques de fuerza bruta.
- Otros tipos de ataques.
- Introducción a la inyección de código (ataques SQL).

Monitorización y ataques al tráfico en redes (Sniffers).

- Introducción.
- Características de diseño.
- Implementación de sniffers.
- Sniffers en redes conmutadas.
- Ejercicios de análisis de tráfico y detección de marcas con Sniffers.
- Análisis de los resultados registrados.
- Ataques de envenenamiento de la redes.

MODULO 3:

TECNOLOGÍA DE SEGURIDAD EN REDES Y ROUTING.

(18 horas)

OBJETIVOS DEL MÓDULO :

Se aprenderá sobre dispositivos de enrutamiento, se trabajará sobre su configuración, administración y protocolos. Se analizarán parámetros de disponibilidad y tráfico. Se analizarán recomendaciones y buenas prácticas a la hora de su configuración.

- Tecnologías de seguridad, Arquitecturas de red.
- Dispositivos.
- Introducción a routers.
- Configuración de enrutamientos.
- Protocolos de seguridad.
- Administración de routers.
- Prácticas de configuración en routers.
- Análisis de tráfico, disponibilidad y QoS.

MÓDULO 4:

MÉTODOS DE PENETRACIÓN WIFI CON EL OBJETO DE COMPROMETER LA SEGURIDAD INFORMÁTICA.

(27 horas)

OBJETIVOS DEL MÓDULO :

Se fundamentarán las bases técnicas y conceptos necesarios para entender el funcionamiento de redes inalámbricas. Se aprenderá sobre materiales, electrónica y equipamiento necesario para auditorías y/o test de penetración inalámbricos. Se realizarán prácticas de auditoría y ruptura de seguridad en redes wifi, se analizarán las configuraciones y mecanismos recomendados para su protección.

Introducción y conceptos previos.

- Tipos (Wi-Fi, DECT, UMTS, GPRS, GSM, Laser, Infrarrojos, Bluetooth, RFID).
- Asociaciones y estándares.
- Ventajas e inconvenientes en su funcionamiento, dificultades en su configuración.
- Futuras tendencias: VoIP, Wimax, QoS, Monitorización video.

Parámetros de estudio, Estructura y Tipología de redes inalámbricas

- Cobertura, Alcance, Propagación, Interferencia, ganancia. Banda de uso civil. Canales. Potencia de transmisión. Sistemas de codificación.
- Canales disponibles de uso sin solapamiento, legalidad e ilegalidad.
- Implementación y cobertura.
- BSSID, ESSID, Células, IBSS.
- Adhoc e infraestructura.
- Repeater y WDS.

Equipos inalámbricos Wifi a utilizar y realización de rastreos sobre posibles víctimas.

- NIC, Adaptadores (tipos según interface, chipsets, amplificación).
- Equipos todo en uno, Adaptador o Router monopuesto, Hotpots.
- Antenas direccionales, medida, polarización.
- Amplificadores, Cables, Conectores, Adaptadores y Pigtailes. Adaptadores PoE.
- Utilizando equipos de medida y diagnostico.
- Analizadores de espectro, scanners, medidores de potencia, inhibidores de frecuencia.
- Correcta configuración de las tarjetas inalámbrica a utilizar en el ataque.
- Utilizaron de los scanners e interpretación de resultados.
- Comprendiendo la estructura de transmisión de paquetes.
- Autenticación y asociación, el tipo de encriptación de canal un factor determinante en el ataque.

Fase de ataque.

- Objetivo fijado.
- Estudio pasivo del objetivo.
- Búsqueda de la mejor situación de cobertura, estudio de la señal.
- Estudio activo de la infraestructura (APS, clientes, SSIDs, MACs, Encriptación, Marcas, Canales, relación entre equipos, velocidades de trabajo, autenticación, Rangos IP).
- Tipos de ataques a realizar.
- Elección del mejor ataque.
- Realización del ataque. Ruptura de la seguridad wifi.
- Conectándonos a red comprometida. Dentro de la red.
- Creación de empresas: formas jurídicas, localización. Creación de un plan de negocio.
- Financiación y subvenciones.

MÓDULO 5:

IMPLEMENTACIÓN DE SISTEMAS CONFIABLES.

(18 horas)

OBJETIVOS DEL MÓDULO :

Se analizarán los correctos pasos a seguir para realizar y mantener una correcta configuración en términos de seguridad en servidores y dispositivos informáticos. Se utilizarán procedimientos definidos y herramientas que permitan verificar el estado y mantener la integridad de la información que contienen los servidores.

Instalación, configuración y mantenimiento de servidores confiables.

- Introducción.
- Vulnerabilidades básicas tras la instalación del sistema.
- Vulnerabilidades en los servicios del sistema.

Con la colaboración de:



Programa de **POSTGRADO EN SEGURIDAD INFORMÁTICA Y HACKING DE SISTEMAS**

- Montar la seguridad.
- Mantenimiento y actualizaciones de las medidas de seguridad.
- Auditorias periódicas de seguridad y análisis de resultados.
- Localización de ficheros de datos registrados imprescindibles para análisis estadísticos posteriores.

Endurecimientos y búsqueda de evidencias en de sistemas

Windows/Linux.

- Seguridad, herramientas y técnicas recomendadas en sistemas Windows.
- Seguridad, herramientas y técnicas recomendadas en sistemas Linux.
- Herramientas para búsqueda de evidencias en servidores y ordenadores afectados.
- Realización de ejercicios prácticos con las herramientas analizadas.

MODULO 6:

ASEGURAMIENTO PERIMETRAL.

(18 horas)

OBJETIVOS DEL MÓDULO :

Se aprenderá sobre el diseño de cortafuegos en empresas, arquitecturas recomendadas en implementaciones y configuración de estos dispositivos. Se realizarán prácticas aprendiendo a instalar, configurar y administrar desde sus consolas distintos tipos de firewalls comerciales y de software libre.

Teoría y práctica con Cortafuegos (Firewalls).

- Introducción.
- Características de diseño.
- Componentes de un firewall.
- Arquitecturas de firewalls.
- Ejercicios de configuración paso a paso de firewalls en laboratorio.
- Análisis de comportamientos en las reglas implementadas.
- Localización de ficheros de datos registrados imprescindibles para análisis estadísticos posteriores.
- Primeras estadísticas básicas suministradas por las aplicaciones.

MODULO 7:

DETECTORES DE INTRUSOS Y MONITORIZACIÓN DE TRÁFICO.

(18 horas)

OBJETIVOS DEL MÓDULO :

Se analizará la importancia de los detectores de intrusos (ids) y la monitorización del tráfico de red en empresas aplicados a la detección o seguimiento de incidencias. Se estudiarán modelos, arquitectura y funcionalidades. Se realizarán prácticas para instalar, configurar y utilizar monitorizadores de red y detectores de intrusos.

Teoría y práctica con detectores de intrusos (IDS).

- Introducción.
- Características de diseño.
- Componentes IDS.
- Implementación de sensores.
- Ejercicios de configuración paso a paso de IDS.
- Análisis de comportamientos de las reglas implementadas.
- Análisis de resultados registrados.
- Localización de ficheros de datos registrados imprescindibles para análisis estadísticos posteriores.

- Primeras estadísticas básicas suministradas por las aplicaciones.

Teoría y práctica con monitorizadores de redes (Sniffers).

- Introducción.
- Características de diseño.
- Implementación de sniffers.
- Ejercicios de configuración paso a paso de Sniffers.
- Análisis de resultados registrados.
- Localización de los ficheros de datos registrados imprescindibles para análisis estadísticos posteriores.
- Primeras estadísticas básicas suministradas por las aplicaciones.

MODULO 8:

CANALES DE COMUNICACIÓN SEGUROS.

(9 horas)

OBJETIVOS DEL MÓDULO :

Se analizará la importancia actual del cifrado de datos y el uso de servicios de comunicación que usen canales seguros para la transferencia de datos en empresas. Se realizarán prácticas de instalación, configuración y uso de software de cifrado. Se analizará el uso de servicios seguros y su implementación en la empresa.

Comunicaciones seguras y cifradas en redes e Internet.

- Introducción.
- La importancia de la encriptación en las comunicaciones.
- La importancia del cifrado en servicios: correo electrónico, e-commerce, transmisiones de datos entre los sistemas, validaciones sobre servicios de red y servidores.
- Desarrollo teórico de algunos modelos de encriptación.
- Limitaciones y uso.
- Realización de ejercicios prácticos con programas de encriptación de datos.
- Sustitución de servicios vulnerables por servicios equivalentes pero que utilizan métodos de encriptación.

MODULO 9:

AUDITORÍAS DE SITIOS WEB Y TÉCNICAS DE INYECCIÓN DE CÓDIGO

(18 horas)

OBJETIVOS DEL MÓDULO :

Se aprenderá como analizar y auditar el contenido de un sitio Web en Internet en términos de seguridad. Se estudiará como se comprueba la posibilidad de inyección de código en sitios Web. Se analizará y practicará sobre técnicas de inyección de código contra datos en páginas Web. Se aprenderán métodos y buenas prácticas a la hora del desarrollo de sitios Web que permitan mitigar riesgos.

Aprendiendo sobre el problema.

- Introducción a TSQL.
- Aprendiendo SQL orientado a la inyección de código.
- Entendiendo porque la aplicación es vulnerable a la inyección de código.
- Localización y análisis de la fisura en el aplicativo.
- Explotación del bug.
- Inyecciones de código básicas.
- Realización y construcción de inyecciones de código paso a paso.
- Blind SQL.
- Analizando y comprendiendo inyecciones avanzadas.
- Recomendaciones a seguir para minimizar riesgos.

Con la colaboración de:



Programa de **POSTGRADO EN SEGURIDAD INFORMÁTICA Y HACKING DE SISTEMAS**

Prácticas de inyección SQL.

- Metodología de una auditoría Web.
- Herramientas de auditoría y detección de vulnerabilidades de inyección de código en aplicativos Web.
- Uso de herramientas e interpretación de resultados encontrados.
- Trabajos sobre una aplicación vulnerable.
- Realización de inyecciones de código sobre la aplicación y su base de datos.
- Realización de inyecciones blind SQL sobre la aplicación y su base de datos.

MODULO 10:

INTRODUCCIÓN AL ANÁLISIS FORENSE

(9 horas)

OBJETIVOS DEL MÓDULO :

Se estudiará la metodología y pasos a realizar en un análisis forense informático en la búsqueda de evidencias. Se utilizarán herramientas de recuperación de datos, reconstrucción de mails y búsqueda de información. Se aprenderá a elaborar un informe objetivo sobre el análisis realizado y los resultados obtenidos.

METODOLOGÍA DEL ANÁLISIS FORENSE.

- Planteamiento del problema.
- Definición de evidencias a buscar.
- Clonación de discos/dispositivos y generación de los checksum md5.
- Herramientas para la recuperación y reconstrucción de la información.
- Recuperación de información y datos borrados.
- Generación y uso de scripts de rastreo en la búsqueda de evidencias.
- Presentación de informes objetivos como resultado del peritaje.

MODULO 11:

SISTEMAS SEM/SIEM (CORRELACIÓN EN TIEMPO REAL DE LOGS)

(9 horas)

OBJETIVOS DEL MÓDULO :

Se estudiará la importancia de la gestión de los logs en empresas en términos de cumplimiento normativo y legal. Se analizará y discutirá el problema del tratamiento masivo de logs. Se aprenderá sobre sistemas de consolidación de logs. Se estudiará el análisis, correlación de logs y la generación de informes y cuadros de mando.

- Introducción a la correlación de logs.
- Sistemas de correlación de logs proactivos o reactivos.
- Sistemas SEM/SIEM.
- La monitorización de sistemas multiplataforma en un punto unificado.
- Aplicando los sistemas SEM/SIEM para reforzar las normas de cumplimiento legales nacionales e internacionales.
- Correlaciones de logs.
- Generación de tickets de incidencias.
- Gestión de incidencias.
- Maqueta práctica de un sistema SEM/SIEM paso a paso.

MODULO 12:

ASPECTOS JURÍDICOS DE LA SEGURIDAD Y LA LOPD

(9 horas)

OBJETIVOS DEL MÓDULO :

Conocer la normativa legal y su aplicación tanto en lo referente a estándares de calidad de una explotación informática, como en lo referente al uso comercial de Internet y la protección de datos personales de los usuarios del sistema,

- Marco jurídico.
- Legislación nacional e internacional en las relaciones
- Ley de Firma electrónica, Delitos informáticos
- Régimen jurídico de los servicios de la sociedad de la información y el comercio electrónico.
- Aplicación de la legislación en seguridad en entorno empresarial.
- Ámbitos de aplicación de la normativa LOPD.
- Adaptación de la empresa a la LOPD, relaciones con la Agencia de Protección de Datos.
- Aplicación en la política de seguridad de la empresa.



Programa de **POSTGRADO EN SEGURIDAD INFORMÁTICA Y HACKING DE SISTEMAS**

PROFESORES

Antonio Ramos Varón

Profesor titular del título propio de la Universidad Complutense de Madrid “Experto en técnicas estadísticas aplicadas a las seguridad informática de redes de ordenadores”, en el módulo de metodología de la intrusión a sistemas. Profesor titular del “Master ejecutivo en dirección de seguridad global”, editado en conjunto por: Belt ibérica y la Universidad Europea de Madrid. Autor de libros como: “Hacker 2006”, “Hacking Práctico”, “Protege tu PC”, entre otros publicados por la editorial Anaya Multimedia. Director del programa de radio “Mundo Hacker” programa divulgativo de seguridad e inseguridad informática. Ha impartido diferentes seminarios y talleres de hacking de sistemas y seguridad informática en España e Iberoamérica. Realiza su labor en Stack Overflow como formador y consultor en seguridad informática, hacking y sistemas SEM.

Jean Paul García Moran

Profesor titular del “Máster Oficial en Ingeniería de Seguridad de la Información y las Comunicaciones” Universidad Alfonso X el sabio - UAX

Especialista en tecnologías Open Source, además de contar con amplia experiencia en plataformas Microsoft y una demostrada experiencia en implementación de sistemas SEM/SIEM a nivel nacional e internacional. Autor de libros como: “Hacking y Seguridad en Internet”, “Instala, configura, securiza y virtualiza entornos Linux” entre otros publicados por la editorial RAMA. Ha realizado diferentes seminarios y talleres de hacking y seguridad informática en España e Ibero América. Actualmente participa en varios proyectos dedicados a la seguridad de sistemas y redes de ordenadores como consultor de Stack Overflow

Yago Fernandez Hansen

Cuenta con master en ingeniería de software, además de contar con más de 8 años de experiencia en tecnologías inalámbricas. Es especialista en la implementación y auditoria de redes Wi-Fi. Cuenta con amplia experiencias en motores de datos, sistemas Microsoft, Linux y Networking. Formador y consultor en seguridad informática y métodos de penetración en redes Wi-Fi para empresas e instituciones. Finalista en el concurso IBM Leonardo DaVinci 1995, cuenta con publicaciones y artículos de informática en revistas como “hakin9”, además de ser autor del libro: Radius/AAA/802.1x de la editorial Rama. Ha impartido diferentes talleres y seminarios de hacking ético y seguridad/inseguridad en Wi-Fi para empresas, organizaciones públicas y universidades.

Fernando Picouto Ramos

Responsable de sistemas High-End/Mid-Range en Sun Microsystems y anteriormente lo hizo para Fujitsu-Siemens Computer, HP, Compaq, Magirus, Diasa, IOS, TSAI y la CECA. Cuenta con una experiencia de más de 15 años en el mundo de IT. Ha trabajado en distintos puestos y responsabilidades en áreas como sistemas, almacenamiento, backup, bases de datos y seguridad. Cuenta con titulaciones universitarias, másters en finanzas y marketing además de certificaciones de diversos fabricantes de plataformas y software. Una de sus aficiones es la formación por lo que ha impartido clases en la Universidad Complutense de Madrid y grandes empresas. Autor de publicaciones de seguridad y hacking para la editorial RAMA.

Jacinto Grijalva

Titulado por la Universidad Rey Juan Carlos. En la actualidad desarrolla su labor en Novell Suse Linux en el área dedicada a productos de seguridad corporativa. Programador de software de bases de datos y redes en diversos lenguajes C, Delphi y Java. Es coautor de libros como: “Hacking y Seguridad en Internet”, “Instala, configura, securiza y virtualiza entornos Linux” publicados por la editorial RAMA. Colaborador habitual del programa de radio “Mundo Hacker” programa divulgativo dedicado a la seguridad e inseguridad informática. Ha impartido diferentes talleres y seminarios de hacking ético y seguridad/inseguridad orientados a la inyección de código en Internet para empresas, organizaciones públicas y universidades.

Maikel Mayan Alonso

Cuenta con 4 años de experiencia en el CNC (Centro Nacional de Control) de Telefónica Data en el departamento de Supervisión de Red, administrando y manteniendo redes nacionales de Routers Juniper y Cisco todos los modelos así como equipos de Nortel Passport y DPN.

Experiencia en el mismo puesto en el CNSO (Centro Nacional de Supervisión y Operaciones) de Telefónica de España. Experiencia en el departamento de Servicios VPN del CIC (Centro Internacional de Control) de Telefónica Whole-Sale Services administrando y manteniendo la red mundial de telefónica internacional con equipos Juniper y Cisco de todos los modelos así como equipos de Nortel como Passports, DPNs, etc.

Actualmente trabaja auditorias de seguridad y análisis de vulnerabilidades en redes contando con experiencia en el campo de la forense informática y el análisis forense de equipos.

Ruben Martinez

Ingeniero en Informática por la Universidad Politécnica de Madrid especializándose durante ella en el desarrollo de algoritmos para la optimización y eficiencia así como Inteligencia Artificial. Con un perfil orientado a la Ingeniería del Software ha desarrollado amplios cursos titulados sobre UML por la Universidad Politécnica. Experto en lenguajes de programación web, Java, C, Cobol, programación concurrente así como funcional (Lisp, CAML) y SQL. Actualmente ha focalizado su trabajo en el ámbito de la seguridad informática, especializándose en el hacking de Bases de Datos, inseguridad endpoint, seguridad en redes WiFi e inyección de código maligno. Compagina su labor en auditorías de seguridad informática e implementador de soluciones de seguridad con el desarrollo de tecnologías Intel VPro.

Manel López Seuba

Engineer de sistemas de Microsoft (Microsoft Certified Systems Engineer) i Professor autoritzat de Microsoft (Microsoft Certified Trainer)

Cisco CCNA i Cisco CCAI (Cisco Certified Authorised Instructor)



CONFERENCIANTES:

Juan Zamora

Titulado en ingeniería informática, ha desarrollado su labor profesional en empresas relacionadas con las tecnologías Linux, actualmente desarrolla su trabajo como Linux Business Development Manager para España y Portugal de Suse Linux. Experto en código abierto y sistemas Linux, así como en la gestión de proyectos de implementación de tecnologías de virtualización y plataformas de alta disponibilidad y rendimiento. Ha realizado talleres tecnológicos en España orientados a la difusión de soluciones de código abierto para empresas e instituciones.

Francisco Martín Vázquez

Titulado por la Universidad Complutense de Madrid en ingeniería informática. Cuenta con más de 8 años de experiencia en el campo del diseño e implementación de software en entornos Microsoft y Linux y desarrollos a bajo nivel en ensamblador. Ha desarrollado software de control y gestión de la información para las empresas más importantes del sector logístico en España. Cuenta también con amplia experiencia en metodologías de intrusión y hacking ético, así como en despliegue y administración de infraestructuras de entornos corporativos Microsoft y Linux.

Actualmente colabora en diferentes proyectos de software libre de desarrollo de aplicaciones de seguridad y soluciones de seguridad para clientes de la firma Fujitsu.

Santiago Lopez Bro

Cuenta con mas de 10 años como administrador de sistemas durante 10 años en empresa multinacional alemana, pasando posteriormente a desarrollar labores de ingeniería y consultoría especializada en el campo de la integración IT. En los últimos dos años se ha especializado en la seguridad y gestión de puesto final, habiendo realizado proyectos en ambas vertientes. Cuenta con amplios conocimientos en tecnologías de Single Sign On (SSO), Contraseña Única, y Gestión de Identidades, todos ellos orientados a securizar y simplificar los entornos corporativos de grandes empresas.

Xavier Martorell Rams

Titulado en ingeniería de sistemas por la Universidad Autónoma de Barcelona, MBA por ESERP y con mas de 22 años de experiencia en el sector de las tecnologías IT. Desarrolla su labor desde el año 2001 en la firma Novell desarrollando su labor inicialmente como ingeniero de sistemas en proyectos de gestión de identidades y plataformas de pre-venta para proyectos tecnológicos. Actualmente realiza su labor como encargado del desarrollo de negocio de soluciones de Novell para Cataluña y Levante.

Angel García Moreno

Titulado por la Universidad Carlos III de Madrid en ingeniería informática, donde colaboró en distintos proyectos con el Grupo de Seguridad de las Tecnologías de la Información y de las Comunicaciones. Cuenta con las correspondientes certificaciones: MCP en distintos productos concedido por Microsoft y CEH del EC-Council.

Coautor del libro "Instala, administra, securiza y virtualiza entornos Linux" de la editorial RAMA, además de escribir y colaborar en diversos artículos sobre fortificación de sistemas, hacking ético y análisis forense en distintos medios, tanto de Internet como impresos. Realiza su labor profesional actualmente en el Tiger Team de SIA, departamento especializado en fortificación de sistemas, hacking ético y análisis forense.

Santiago Fernández López

Titulado por la Universidad Politécnica de Madrid en ingeniería informática, cuenta con Bachelor of Science in Systems & Networks por la Bircham International University. Actualmente desarrolla su labor en el Departamento de Estrategia Tecnológica de Indra como responsable del Equipo Técnico de Infraestructuras y Sistemas a nivel nacional e internacional. Dispone de amplios conocimientos en sistemas, dispositivos de protección perimetral, comunicaciones y sistemas biométricos de reconocimiento facial, control de huellas, firma e iris.



Programa de **POSTGRADO EN SEGURIDAD INFORMÁTICA Y HACKING DE SISTEMAS**

ADMISIÓN

Periodo de inscripción:

A partir del 1 de septiembre queda abierto el periodo de inscripción en el que el alumno deberá rellenar el correspondiente formulario y aportar la documentación necesaria que servirá para formalizar la matrícula.

Esta inscripción se formalizará a través de:

CETEMMSA
Fundació Privada Cetemmsa
c/ Jaume Balmes, 37-39
08301 MATARO
Tel. 93.741.91.00 - Fax 93.741.92.28
e-mail: formacio@cetemmsa.com
<http://www.cetemmsa.com>

Para formalizar la inscripción es necesaria una entrevista previa.

Documentación necesaria:

- 2 fotografías recientes.
- Fotocopia del D.N.I. o del pasaporte.
- Fotocopia de la titulación académica.
- Currículum Vitae.

Precio:

5.500 € (30% al efectuar la inscripción y el resto al formalizar la matrícula antes de empezar el curso).

Los ex alumnos de la EUM, la EUPM y de CETEMMSA, así como las empresas colaboradoras con las entidades organizadoras tendrán un 15% de descuento en el importe de la matrícula.

Forma de pago:

El alumno deberá realizar el pago del 30% del importe de la matrícula al efectuar la inscripción al curso. El resto deberá ser abonado al formalizar la matrícula -6 días antes del inicio del curso-. Estos pagos pueden ser realizados por transferencia, mediante cheque nominativo o domiciliación bancaria (hoja de inscripción).

La dirección del curso se reserva el derecho de anular o aplazar el curso si no hay un número mínimo de alumnos. En este caso se reembolsará el importe del curso pagado por el alumno.

Posibilidad de bonificación parcial mediante la Fundación Tripartita para empresas.

Para obtener más INFORMACIÓN



CETEMMSA
Fundació Privada Cetemmsa
c/ Jaume Balmes, 37-39
08301 MATARO
Tel. 93.741.91.00 - Fax 93.741.92.28
e-mail: postgrau@cetemmsa.com
<http://www.cetemmsa.com>



Escola Universitària Politècnica de Mataró
Avda. Puig i Cadafalch 101-111
08303 Mataró
Tel. 93.741.50.75
Fax 93.757.05.24
e-mail: escola@eupmt.es