TÉCNICO EN SEGURIDAD DE REDES Y SISTEMAS

DATOS GENERALES DEL CURSO

1. FAMILIA PROFESIONAL: SERVICIOS A LAS EMPRESAS

ÁREA PROFESIONAL: INFORMÁTICA

2. DENOMINACIÓN DEL CURSO: TÉCNICO EN SEGURIDAD DE REDES Y SISTEMAS

3. CÓDIGO: EMIN21

4. CURSO: OCUPACIÓN

5. OBJETIVO GENERAL:

El alumno será capaz de supervisar la administración y las políticas de seguridad de los sistemas y redes, mediante la implantación y gestión de medidas de seguridad ante posibles ataques o usos inapropiados de los usuarios, evaluando riesgos y garantizando la confidencialidad y la integridad de las transacciones electrónicas.

6. REQUISITOS DEL PROFESORADO:

6.1 Nivel académico:

Titulación universitaria (preferentemente ingeniero, licenciado o diplomado en Informática) o en su defecto, capacitación profesional equivalente en la ocupación relacionada con el curso.

6.2 Experiencia profesional:

Deberá tener al menos tres años de experiencia en la ocupación.

6.3 Nivel pedagógico:

Formación metodológica y/o experiencia docente.

7. REQUISITOS DEL ACCESO PARA EL ALUMNO:

7.1 Nivel académico o de conocimientos generales:

- Titulación universitaria de Grado Medio o Superior en Informática
- Ciclo Superior de Informática

7.2 Nivel profesional o técnico:

- Conocimientos en los sistemas operativos UNIX y Windows NT (o similares).
- Conocimientos sobre protocolos de redes de computadoras.
- Conocimientos en servicios de Internet.
- No se requiere experiencia profesional.

7.3 Condiciones físicas:

Ninguna en particular, salvo aquellas que impidan un normal desarrollo de la profesión.

8. NÚMERO DE ALUMNOS:

15 Alumnos.

9. RELACIÓN SECUENCIAL DE BLOQUES DE MÓDULOS FORMATIVOS:

- Introducción a la Seguridad Informática
- Técnicas y Herramientas de Ataque a Redes TCP/IP
- Técnicas y Herramientas de Ataque a Sistemas UNIX
- Técnicas y Herramientas de Protección de Redes, Sistemas y Servicios
- Políticas y Prácticas de Seguridad de Redes y Sistemas en las Organizaciones. El Plan de Contingencias y la Evaluación de riesgos.

10. DURACIÓN:

Prácticas .....260 horas
Conocimientos profesionales .....120 horas

Evaluaciones.....20 horas

Total..... 400 horas

11. INSTALACIONES:

11.1. Aula de clases teóricas:

- Superficie: el aula deberá tener un mínimo de 45 m^2 para grupos de 15 alumnos (3 m^2 por alumno y profesor).
- Mobiliario: El aula estará equipada con mobiliario docente para 15 plazas, además de los elementos auxiliares.

11.2. Instalaciones para prácticas:

- Superficie: para el desarrollo de las prácticas descritas se usará indistintamente el aula de clases teóricas.
- Iluminación: uniforme, de 250 a 300 lux aproximadamente.
- Condiciones ambientales: temperatura climatizada (20-22 ºC).
- Ventilación: natural o controlada asegurando un mínimo de cuatro-seis renovaciones/ hora.
- Mobiliario: estarán equipadas con mobiliario para 15 plazas, además de los elementos auxiliares.

11.3. Otras instalaciones:

- Un espacio mínimo de 50 m^2 para despachos de dirección, sala de profesores y actividades de coordinación.
- Una secretaría.
- Aseos y servicios higiénico-sanitarios en número adecuado a la capacidad del centro.
- Los centros deberán reunir las condiciones higiénicas, acústicas, de habitabilidad y de seguridad exigibles por la legislación vigente, y disponer de licencia municipal de apertura como centro de formación.

12. EQUIPO Y MATERIAL:

12.1. Equipo:

- 16 PCs con sus respectivos monitores (15 para los alumnos, 1 para el profesor que hará las veces de servidor) de características suficientes para la utilización de las herramientas informáticas necesarias para el desarrollo del curso. Se recomienda que tengan como mínimo, procesador tipo PC Pentium III 400 MHZ 128 MB de RAM y 20-40 Gb de disco duro, y sistema operativo de tipo Windows en una versión actualizada. Tendrán instalado un navegador WWW y un procesador de textos.

- 1-2 estaciones de trabajo UNIX que actuarán como objetivo de los ataques en las prácticas de los alumnos. Estarán debidamente configurados para que puedan explotarse diversos tipos de vulnerabilidades.
- 1 estación de trabajo Windows en la que estará instalado un servidor WWW.
- 1 estación de trabajo para ser utilizada como máquina señuelo.
- Todos los ordenadores estarán conectados en red.
- Routers y firewalls.
- Varias herramientas y utilidades software que serán empleadas en las prácticas para ilustrar diversos mecanismos de ataque y defensa.
- Software de PKI.
- Software de directorio.
- Software de correo electrónico.
- Software PGP.
- Acceso a Internet (ADSL o similar).
- Switch o concentrador de cableado, con bocas suficientes para conectar a todos los equipos disponibles en el aula.
- Impresora láser ó de inyección.

12.2. Herramientas y utillaje:

- 50 disquetes.

12.3. Material de consumo:

- Cartuchos de tinta para la impresora de inyección.
- Tóner para la impresora láser.

12.4. Material didáctico:

- Manual/es por cada alumno, que contemplen todos los contenidos del curso.
- A los alumnos se les proporcionará los medios didácticos y el material imprescindible para el desarrollo del curso.

12.5. Elementos de protección:

En el desarrollo de las prácticas se utilizarán los medios necesarios de seguridad e higiene en el trabajo y se observarán las normas legales al respecto.

13. INCLUSIÓN DE NUEVAS TECNOLOGÍAS:

Este curso se considera en su totalidad como nuevas tecnologías en el área Informática.

DATOS ESPECÍFICOS DEL CURSO

14. DENOMINACIÓN DEL MÓDULO:

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA.

15. OBJETIVO DEL MÓDULO:

Conocer los fundamentos de criptografía, así como los principales mecanismos de identificación y control de accesos sobre los que se apoya la seguridad informática.

16. DURACIÓN DEL MÓDULO:

80 horas

17. CONTENIDOS FORMATIVOS DEL MÓDULO:

A) Contenidos prácticos:

- Instalar una PKI.
- Instalar un servidor de directorio.
- Emitir un certificado digital de usuario:
  - Introducir los datos de usuario y el certificado en el directorio.
- Emitir un certificado digital de servidor:
  - Instalar un certificado digital de servidor en un servidor WWW.
  - Instalar un servidor WWW con SSL de servidor.
  - Configurar un servidor WWW con SSL de servidor y de cliente basado en directorio.
- Preparar un servicio de firma de formularios en el servidor WWW.
- Utilizar un certificado digital de usuario:
  - Para autenticación ante un servidor WWW.
  - Para firma de un formulario HTML.
  - Para envío de correo cifrado y firmado.
- Uso de sistema PGP para generar una firma digital.

B) Conocimientos teóricos:

- Seguridad y Protección de la Información.
  - Gestión de la seguridad física y lógica.
  - Niveles de Medidas de Seguridad.

- Seguridad en comunicaciones y redes.
- Disponibilidad de sistemas y aplicaciones.
- Seguridad en transacciones a través de Internet.
- Planes de contingencia: Recuperación de desastres y continuidad del negocio.
- Obligaciones del Responsable de Seguridad.

- Criptografía.
  - Qué es el cifrado. Métodos criptográficos clásicos.
  - Algoritmos de cifrado simétricos (DES).
  - Algoritmos de clave pública (RSA).
  - Algoritmos de cifrado en bloque y de flujo.
  - La firma digital. Hashing.
- La criptografía de clave pública: Utilidades.
  - Confidencialidad.
  - Integridad.
  - Autenticación.
  - No repudio.
- PKI.
  - Concepto.
  - Arquitectura y componentes.
    - CA, RA, otros servicios (OCSP).
  - Acuerdo de prácticas de certificación.
- Certificados digitales.
  - Concepto y definición.
  - Estructura de un certificado digital.
  - Ciclo de vida de un certificado.
  - Listas de certificados revocados, CRLs.
- Directorio.
  - Concepto y definición.
  - Utilidades.
  - Contenidos.
- Aplicaciones básicas de la certificación digital.
  - Autenticación.
    - Desafío/respuesta.
  - Cifrado.
    - Simple cifrado de ficheros, problemática.
    - Key recovery.
    - Cifrado en almacenamiento.
    - Sistemas con capacidad de recuperación de información.
  - Firma digital.
    - De formularios HTML.
    - De ficheros.
- Aplicaciones de alto nivel de la certificación digital.
  - S/MIME.
    - Ensobrado.
    - Firma de correo.
  - SSL y TLS.
    - Negociación del protocolo (hand-shake).
    - HTTPS.
  - IPSEC.
  - SET.

- Confidencialidad e Integridad en Transacciones Electrónicas.
  - La Ley de Protección de Datos de Carácter Personal (LOPD).
  - La Ley de Firma Electrónica.
- Mecanismos de Identificación y Control de Accesos.
  - Passwords.
  - Frases clave.
  - Tickets de acceso.
  - Protocolos de desafío/respuesta.
  - Certificados Digitales como mecanismo de autenticación, firma digital.
  - Módulos de seguridad, tokens criptográficos, tarjetas inteligentes.
  - Sistemas biométricos.
  - Pruebas de zero-knowledge.
  - Control de acceso en servidores Web y de correo electrónico.
  - El WAP (Wireless Access Protocol) y sus extensiones de seguridad.
  - Control de acceso en telefonía GSM.

C) Contenidos relacionados con la profesionalidad:

- Fomentar la capacidad de solución de problemas complejos de seguridad informática abordados desde múltiples niveles.
- Favorecer la utilización de conceptos, herramientas y modos de trabajo nuevos y tecnológicamente diferentes.
- Fomentar una actitud responsable ante la seguridad de redes y sistemas.

14. DENOMINACIÓN DEL MÓDULO:

TÉCNICAS Y HERRAMIENTAS DE ATAQUE A REDES TCP/IP.

15. OBJETIVO DEL MÓDULO:

Conocer las principales amenazas de seguridad y vulnerabilidades que pueden afectar a redes de computadoras bajo protocolo TCP/IP, así como los procesos y herramientas de ataque.

16. DURACIÓN DEL MÓDULO:

90 horas

17. CONTENIDOS FORMATIVOS DEL MÓDULO:

A) Contenidos prácticos:

- Funcionamiento y detección de rastreadores con topología de red HUB.
  - Instalar y utilizar un rastreador genérico para capturar el tráfico de una red.
  - Instalar y utilizar un rastreador especializado en contraseñas y espionaje de actividad.
- Funcionamiento y detección de rastreadores con topología de red SWITCH:
  - Realizar un secuestro de sesiones y captura de tráfico entre dos estaciones con topología tipo SWITCH.
  - Falsificar tablas ARP mediante la técnica de ARP spoofing.
- Denegación de servicio:
  - Inundar de una red mediante la técnica de SYN flooding.
  - Buscar redes con direcciones de difusión (broadcast) para realizar ataques de magnificación.
  - Realizar de ataques de magnificación del tipo Smurf.
  - Enlazar servidores en los puertos Echo y Chargen.
- DNS:
  - Utilizar una herramienta para secuestro de sesiones DNS.
  - Emplear una herramienta para falsificación de caché de DNS.
- SNMP:
  - Utilizar una herramienta para búsqueda de sistemas con agentes SNMP y comunidades de fácil adivinación.
- Búsqueda de objetivos para un ataque:
  - Buscar información general sobre un objetivo mediante las bases de datos Whois y RIPE.
  - Buscar información sobre los servidores de una organización mediante solicitud de transferencia de zonas DNS y resolución inversa.
  - Realizar búsquedas mediante ICMP de los servidores activos (hping y fping).
  - Ejecutar rastreos de puertos mediante diferentes sistemas.
  - Utilizar técnicas de ocultación de rastreos.
  - Rastrear sistemas operativos mediante detección pasiva (Siphon).

- Rastrear sistemas operativos mediante detección activa (Nmap).

- Obtención de información acerca de un objetivo:
  - Utilizar herramientas no intrusivas para averiguar los usuarios de un sistema (finger, rwho, rsusers).
  - Emplear métodos intrusivos para conseguir la lista de usuarios de un sistema.
  - Realizar una conexión mediante Telnet a distintos puertos para averiguar el software servidor en ejecución tras cada puerto abierto en un sistema.
  - Obtener información sobre servicios RPC.
  - Utilizar herramientas SMB en UNIX para identificar sus deficiencias de seguridad.

B) Conocimientos teóricos:

- Tipos de Ataques en TCP/IP.
  - Rastreadores de red (sniffers), topología HUB.
  - Rastreadores de red, topología SWITCH.
  - Falsificación de la IP (IP spoofing).
  - Denegación de servicio.
    - Tipos, técnicas y herramientas de inundación (SYN flood, ICMP, UDP).
    - Ataques de magnificación: Smurf y Fraggle.
    - Denegación de servicio distribuida.
  - Secuestro y falsificación de DNS.
  - Protocolo SNMP.
- Técnicas para la búsqueda de objetivos de un ataque.
  - Obtención de información general (Web, Whois, news).
  - Búsqueda de servidores de la organización.
  - Búsqueda de servidores accesibles.
  - Técnicas de rastreo de puertos y ocultación de rastreos.
  - Técnicas de rastreo de sistemas operativos.
- Mecanismos para obtención de información acerca de objetivos.
  - Averiguación de nombres de usuarios y grupos.
  - Averiguación de recursos importados y exportados.
  - Averiguación de software instalado y servicios abiertos.
  - Samba: nombres NetBIOS y Dominios.
  - Ingeniería social.

C) Contenidos relacionados con la profesionalidad:

- Fomentar la capacidad de solución de problemas identificando puntos débiles en una red.
- Favorecer la utilización de conceptos, herramientas y modos de trabajo nuevos y tecnológicamente diferentes.

14. DENOMINACIÓN DEL MÓDULO:

TÉCNICAS Y HERRAMIENTAS DE ATAQUE A SISTEMAS UNIX.

15. OBJETIVO DEL MÓDULO:

Conocer las principales amenazas de seguridad y vulnerabilidad que pueden afectar a un sistema UNIX, familiarizándose con las herramientas utilizadas habitualmente por los “hackers” para acceder y tomar control del sistema.

16. DURACIÓN DEL MÓDULO:

70 horas

17. CONTENIDOS FORMATIVOS DEL MÓDULO:

A) Prácticas:

- Obtención de acceso a un servidor UNIX:
  - Confeccionar un diccionario para un ataque contra servicios con autenticación.
  - Utilizar desbordamientos de memoria en aplicaciones servidoras para comprobar las posibilidades de ejecución remota de comandos.
  - Buscar servidores con vulnerabilidades en servidores Apache/Netscape.
  - Explotar vulnerabilidades en servicios FTP, IMAP, SMTP, PROXY, Xwindow.
  - Comprobar vulnerabilidades de navegadores web.
  - Observar el uso de diferentes tipos de caballos de troya.
  - Utilizar varios analizadores de seguridad.
- Obtención de control total a un servidor UNIX:
  - Emplear un averiguador de contraseñas.
  - Realizar ataques mediante diccionario y mediante fuerza bruta.
  - Instalar en remoto una puerta trasera.
  - Obtener una interfaz gráfica de la máquina atacada.
  - Instalar un rootkit para que las herramientas del intruso pasen inadvertidas.

B) Conocimientos teóricos:

- Mecanismos para obtener acceso a un servidor UNIX.
  - Ataques contra servicios con autenticación por fuerza bruta.
  - Ataques a módulos PAM: Pluggable Authentication Modules.
  - Desbordamiento de memoria (buffer overflow).
  - Vulnerabilidades en scripts.

- Vulnerabilidades de las aplicaciones servidoras.
- Vulnerabilidades en clientes.
- Caballos de Troya.
- Analizadores de seguridad.

- Mecanismos para obtener control total de un servidor UNIX.
  - Aumento de privilegios.
  - Localización de contraseñas y uso (password cracking).
  - Secuestro de sesión con comandos r (hijacking de sesión).
  - Sudo, seguid y setguid.
  - Instalación de control remoto. Puertas traseras.
  - Kernel hacks.
  - Ocultación de puertas traseras. Rootkit.
  - Borrado de pistas y logs (wipe, zappers).

C) Contenidos relacionados con la profesionalidad:

- Fomentar la capacidad de solución de problemas identificando puntos débiles en una red.
- Favorecer la utilización de conceptos, herramientas y modos de trabajo nuevos y tecnológicamente diferentes, con precisión.

14. DENOMINACIÓN DEL MÓDULO:

TÉCNICAS Y HERRAMIENTAS DE PROTECCIóN DE REDES, SISTEMAS Y SERVICIOS.

15. OBJETIVO DEL MÓDULO:

Conocer las principales técnicas y herramientas de protección aplicables en redes, sistemas y servicios más habituales (correo y servidores).

16. DURACIÓN DEL MÓDULO:

110 horas

17. CONTENIDOS FORMATIVOS DEL MÓDULO:

A) Prácticas:

- Monitorización y búsqueda de síntomas de ataque contra sistemas y redes sin una protección especial:
  - Monitorizar un syslog.
  - Buscar otros síntomas.
- Protección completa de una red:
  - Configurar un firewall.
  - Configurar un router.
  - Configurar las pilas TCP/IP en equipos finales.
  - Utilizar un filtro anti-rastreo.
  - Utilizar un filtro anti-SPAM en un firewall.
  - Configurar una conexión IPSEC entre un cliente y un firewall.
    - Proteger completamente un servidor UNIX en sus diferentes aspectos.
    - Configurar y proteger los Servicios más habituales.
- Comprobar la efectividad de las protecciones intentando atacar a los sistemas y redes protegidos previamente.
- Monitorizar y comprobar intentos de ataque contra los sistemas y redes protegidos.
- Instalar una máquina señuelo.

B) Conocimientos teóricos:

- Protección en nivel de Red:
  - Segmentación de redes y uso de bridges, hubs, switches y routers.

- Filtrado de paquetes en firewalls y routers. Definición de servicios disponibles y condiciones de acceso:
  - Servicios Chargen y Echo.
  - DNS.
  - TFTP.
  - Comandos r de BSD UNIX.
  - SunRPC y NFS.
  - SMTP (correo electrónico).
  - NetBIOS (redes Microsoft).
  - SNMP.
  - Filtro de datagramas IP.
  - Números de red privada reservados.
  - Redes broadcast.
- Configuración de las pilas TCP/IP en equipos finales.
- Monitorización de Routers y equipos de acceso.
  - Comprobación de intentos de conexión no autorizados.
  - Caídas.
  - Monitorización SNMP.
- Filtros anti-rastreo (anti-sniffing).
- Filtros anti-SPAM.
- Conexiones IPSEC.

- Protección de Sistemas: Protección de un servidor Unix (Servidor Bastión).
  - Directivas generales:
    - Comandos r y archivos .rhosts y /etc/hosts.equiv.
    - Administración segura SSH.
    - Declaración de terminales seguros.
    - Conexión a la cuenta del administrador.
    - Desactivación de IP forwarding y source routing.
    - Deshabilitar la posibilidad de ejecución de código en pila de usuario.
    - Manejo del correo a root.
    - Desactivación de ejecución de comandos en dispositivos montables.
    - Aislamiento de las máquinas de usuario y de los servidores.
    - Prevención de escuchas y rastreos.
    - Protección de contraseñas.
    - Revisión del path del root.
  - Seguridad en sistemas de archivos:
    - Monitorización de los modos de acceso suid y Said.
    - Limitación del acceso a recursos según el tipo de usuario.
    - Restricción de NFS.
    - Máscaras.
    - Restricción de Samba.
    - Archivos de dispositivo.
    - Revisión de permisos en archivos.
    - Propiedad de directorios especiales. Sticky bit.
    - Comparación con versiones válidas de programas.
    - Detección de Caballos de Troya (checksum criptográfico).
  - Configuración y filtrado de los servicios:
    - Servicios dependientes del demonio inetd.
    - Uso de TCPWrappers (tcpd) para monitorizar accesos.
    - Servicios dependientes de RPC (Remote Procedure Control).

        - Arranque de servicios en los scripts de inicio.
- Configuración y protección de los Servicios más habituales.
    - Sistema de correo:
        - Equipos de usuario.
        - Equipos de almacenamiento de correo.
        - Equipos de intercambio de correo.
        - Filtros anti-SPAM.
    - Servidores de nombres (DNS).
    - Servidores WWW.
    - Servidores FTP.
    - Servidores de ficheros.
        - Servidores NFS.
        - Servidores NetBIOS .
- Señuelos (honeypots).

C) Contenidos relacionados con la profesionalidad:

- Fomentarla la capacidad de resolución de problemas.
- Favorecer la utilización de conceptos, herramientas y modos de trabajo nuevos y tecnológicamente diferentes.

14. DENOMINACIÓN DEL MÓDULO:

POLÍTICAS Y PRÁCTICAS DE SEGURIDAD DE REDES Y SISTEMAS EN LAS ORGANIZACIONES. EL PLAN DE CONTINGENCIAS Y LA EVALUACIÓN DE RIESGOS.

15. OBJETIVO DEL MÓDULO:

Establecer políticas de seguridad adecuadas a las necesidades y características de una organización.

16. DURACIÓN DEL MÓDULO:

50 horas

17. CONTENIDOS FORMATIVOS DEL MÓDULO:

A) Prácticas:

- Ante varios supuestos de organización:
  - Elegir y redactar políticas de seguridad para varios supuestos de organización, indicando:
    - Puntos de contacto y responsables de seguridad.
    - Política de contraseñas.
    - Política de cuentas.
    - Permisos y derechos de usuarios y grupos.
    - Compartición de recursos.
    - Política de copias de seguridad.
    - Monitorización de archivos de registro (syslog).
    - Protección frente a ataques internos.
    - Auditoria de sistema y de red.
    - Comprobación de integridad (Tripwire).
    - Recomendaciones para usuarios finales.
    - Monitorización de nuevas vulnerabilidades.
    - Instalación de parches de seguridad y actualización de software.
  - Evaluar los posibles riesgos.
  - Redactar un plan de contingencia para varios tipos de riesgos.
- Buscar información a través de Internet acerca de las Organizaciones para la vigilancia de los sistemas y redes informáticos (CERT) y de las fuentes de información sobre seguridad.

B) Conocimientos teóricos:

- Establecimiento de puntos de contacto y responsables de seguridad.

- Política de contraseñas:
  - Contraseñas fuertes frente a ataques de diccionario y de fuerza bruta.
  - Cambios periódicos.
  - Reutilización de contraseñas.
  - Cifrado de contraseñas.
  - Uso de crackers.
  - Cuentas sin contraseña, contraseñas por omisión.
  - Cancelación de cuentas no usadas.
- Política de cuentas:
  - Administración de usuarios y grupos.
  - Cuotas de disco.
  - Cuentas especiales.
  - Usuario root.
- Permisos y derechos de usuarios y grupos.
- Compartición de recursos.
- Espacios con máquinas de uso compartido.
- Política de copias de seguridad.
- Monitorización de archivos de registro (syslog):
  - Configuración.
  - Uso desde programas.
  - Rotación de ficheros.
- Separación de servicios de Internet y servicios multiusuario.
- Protección frente a ataques internos.
- Auditoría de sistema y de red.
- Comprobación de integridad (Tripwire).
- Recomendaciones para usuarios finales.
  - Elección del sistema operativo.
  - Virus.
  - Correo electrónico.
  - Macros.
  - Protección del acceso físico a las máquinas.
- Monitorización de nuevas vulnerabilidades.
- Instalación de parches de seguridad y actualización de software.
- Organizaciones para la vigilancia de los sistemas y redes informáticos (CERT).
- Fuentes de información sobre seguridad.
- Planes de contingencia.

C) Contenidos relacionados con la profesionalidad:

- Favorecer la orientación al cliente.
- Favorecer el desarrollo de la capacidad de toma de decisiones.
- Fomentar las habilidades de comunicación.
- Favorecer la utilización de conceptos, herramientas y modos de trabajo nuevos y tecnológicamente diferentes.