Gestión de la seguridad y hacking de equipos informáticos

OBJETIVOS

Proteger y auditar la seguridad en la red de una empresa o institución. Los asistentes conocerán los riesgos que implica el tener los sistemas de la institución donde desarrollan su labor cara a Internet. Los asistentes se familiarizarán con los posibles tipos de ataques, técnicas maliciosas que los intrusos informáticos pueden utilizar sobre los sistemas de la empresa. Aprenderán las técnicas utilizadas por intrusos maliciosos cuando planean e intentan un ataque a páginas Web, servidores de correo, bases de datos y sistemas de redes de ordenadores atentando contra la continuidad del negocio, así como las medidas necesarias para abortar dichos ataques. Aprenderán a establecer medidas preventivas, políticas de seguridad en su empresa o puesto de trabajo, detectar puntos débiles y fisuras en la seguridad implementada de empresa. Adquirirán los conocimientos para la toma de decisiones cuando se trata de salvaguardar la información sensible y datos confidenciales de clientes, la institución o empresa a la que pertenecen. Desarrollaran los conocimientos para planificar un correcto control sobre las medidas implementadas o a implementar, acompañado del correspondiente beneficio operacional en términos financieros para la empresa.

BREVE INTRODUCCIÓN Y CONCEPTOS PREVIOS

¿Qué es la seguridad informática? ¿Por qué es necesaria la seguridad informática en la organización? Campos de acción de la seguridad informática. Programas malignos y tipos de intrusos. 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.

CONCEPTOS IMPRESCINDIBLES Y EL PROTOCOLO TCP/IP

Introducción Capas de red Dirección IP Intranet Extranet Internet Mascara de subred Protocolo IP Protocolo ICMP Encaminamiento Capa de transporte Puertos Protocolo UDP Protocolo TCP Nombre de dominio

PROBLEMAS DE SEGURIDAD EN LAS EMPRESAS

Casos documentados de ataques. Los nuevos caminos del crimen en Internet. Tipos de Ataque que comprometen la seguridad global de la organización.

¿Qué es seguir el rastro a una organización? Seguir el rastro en Internet. Determinación del ámbito de actividades de la víctima (empresa). Enumeración de la red Interrogaciones DNS Reconocimiento de la red y su topología previo al ataque Ejercicios prácticos de rastreo. Interpretación de resultados y fisuras. Contramedidas a adoptar ante las fisuras.

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. Ejercicios prácticos y de análisis. Interpretación de resultados y fisuras. Medidas a adoptar ante las fisuras. Herramientas automáticas de descubrimiento y contramedidas.

TÉCNICAS DE HACKING CONTRA LOS SISTEMAS Y CONTRAMEDIDAS

Introducción Firewalls y routers Técnicas de firewalking (atravesar cortafuegos) Métodos para engañar a los ficheros .log en la ofensiva. Como los intrusos se hacen invisibles en Internet. Técnicas de suplantación de IP atacantes en Internet (looping spoffing ip) Medidas a implementar de prevención. Obtención de exploits (el problema buffer overflow). Compilación y utilización de exploits sobre vulnerabilidades. Ataques distribuidos desde Internet. Entrando en los sistemas y la escalada de privilegios. Detección de la utilización de exploits contra nuestra red. Métodos de descarga de herramientas de prospección en el servidor comprometido Anulando la efectividad de los antivirus (generación de herramientas indetectables) Como se recaba información una vez en los sistemas. Medidas de seguridad a implementar. Alteración, falsificación e intoxicación de ficheros .log. Establecimiento de puertas traseras (backdoors). Metodología para la detección de puertas traseras.
Enumeración Windows NT/2000/2003Buscando Usuarios validos y recursos accesibles. Ataques contra contraseñas.

INSTALACIÓN, CONFIGURACIÓN Y MANTENIMIENTO DE SERVIDORES CONFIABLES.

Introducción. Vulnerabilidades básicas tras la instalación del sistema. Vulnerabilidades en los servicios del sistema. Montar la seguridad. Mantenimiento y actualizaciones de las medidas de seguridad. Escaneadores de vulnerabilidades en redes de ordenadores. Uso de los escaneadores de vulnerabilidades Auditorias periódicas de seguridad y análisis de resultados.

AUDITORIA SOBRE POLÍTICAS DE USUARIOS Y CONTRASEÑAS

Análisis del problema en la organización. Métodos de descifrado y ruptura de contraseñas. Herramientas para la auditoria de contraseñas. Herramientas para ruptura de contraseñas y métodos de cracking de contraseñas Implementación de políticas confiables

HERRAMIENTAS PARA AUDITORIAR LA SEGURIDAD DE LA RED DE LA EMPRESA, MONITORIZADORES DE TRÁFICO Y DETECTORES DE INTRUSOS

Introducción a los escaneadores de vulnerabilidades. Configuración de las plantillas de auditoría. Práctica realización de auditorías sobres sistemas internos. Práctica realización de auditorías sobres sistemas cara a Internet. Generación de informes. Introducción a Sniffers. Instalación y uso de Sniffers. Configuración de filtros de monitorización. Análisis y monitorización de segmentos críticos de red. Interpretación de los paquetes monitorizados.

HERRAMIENTAS DE CONTRAMEDIDAS Y HACKING QUE SE UTILIZAN DURANTE EL CURSO

Herramientas on line. Herramientas de exploración. Herramientas de enumeración. Herramientas de footprinting (rastreado). Herramientas para conseguir accesos. Herramientas de penetración y puertas traseras. Ocultación de huellas. Herramientas de auditoría de redes y ordenadores.

El curso incluye documentación perteneciente al libro: Hacker 2006, así como un CD para cada alumno como complemento a su formación, con las herramientas utilizadas a lo largo del curso.

Profesor: ANTONIO ANGEL RAMOS VARON
Antonio Ángel Ramos, es diplomado por la Universidad Complutense de Madrid, fundador y presidente honorífico del club de Informática de la E.U.E. Profesor titular del titulo propio de la Universidad Complutense de Madrid "Experto en seguridad informática de redes de ordenadores y antihacking", en el módulo de metodología de la intrusión a sistemas informáticos. Ha participado en diversas colaboraciones informáticas universitarias y publicaciones de libros. Autor de libros como: Hacker 2006, Hacking Práctico, Protege tu PC, entre otros, de la editorial Anaya Multimedia. Cuenta con formación amplia en sistemas Windows y Linux, así como en el área de la ingeniería social y comportamientos de usuarios en Internet. Ha impartido diferentes seminarios y talleres de hacking de sistemas y seguridad informática en España e Ibero América. Realiza parte de su labor como formador y asesor a departamentos de IT de empresas e instituciones.

Profesor: JEAN PAUL GARCIA MORAN
Jean-Paul García-Moran, actualmente cursa su diplomado en la Universidad Complutense de Madrid. Profesor ayudante del curso “Experto en seguridad informática” impartido por la Universidad Complutense en las instalaciones de la E.U.E. Cuenta con amplia experiencia en el mundo Open Source y sistemas Linux, así como conocimientos de redes Microsoft. Desarrolla su labor profesional como parte del team de consultores en seguridad de RedHat - España, en el área de implementación de detectores de intrusos y firewalls. Es partícipe activo de foros y canales IRC, tanto de programación como administración de sistemas, seguridad informática y hacking, cofundador del grupo underground Made in Hell. Actualmente participa en varios proyectos dedicados a la formación e implementación de seguridad en sistemas y redes de ordenadores.

FICHA TÉCNICA DEL CURSO

Certificado final: Diploma de asistencia acreditativo, avalado por las diferentes marcas que Ceina representa, más el soporte específico de **Novell / Suse Security Partner**

Subvención: Posibilidad de subvención parcial del curso Vía FORCEM. Consultar con nuestro departamento de formación contínua, al teléfono 964340326

Duración: 35 horas
Lugar: Help Sistemas Informáticos SL (CASTELLON)
Nº Mínimo de inscripciones: 8 plazas
Nº Máximo de inscripciones: 12 plazas

FORMATO 1:

7 sesiones de 5 horas en Sábado (de 9 a 14 horas)

FORMATO 2:

3 fines de semana en sesiones de viernes (6 horas) y sábado (6 horas)

Precio (incluye material): 975 €
Cantidad subvencionable: 455 €