Seguridad de sistemas y redes, nivel 1

Curso práctico de 4 días - 28h
Ref.: FRW - Precio 2024: 2 090€ sin IVA

Este curso práctico le mostrará cómo aplicar los principales medios de seguridad de los sistemas y las redes. Tras estudiar algunas amenazas al sistema de información, aprenderá el papel de los distintos equipos de seguridad en la protección de la empresa para poder diseñar una arquitectura de seguridad y llevar a cabo su despliegue.

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Conocer los fallos y amenazas de los sistemas de información

Dominar la función de los distintos equipos de seguridad

Diseñar e implementar una arquitectura de seguridad adaptada

Poner en marcha los principales medios de seguridad de las redes

Proteger un sistema Windows y Linux

Despliegue de una solución de proxy HTTP en Windows o Linux y de una solución antivirus en los flujos de red. Diseño e implantación de una arquitectura multifirewalls y multi-DMZ. Aplicación de técnicas básicas de seguridad del sistema operativo.

PROGRAMA

última actualización: 01/2023

1) Riesgos y amenazas

- Introducción a la seguridad.
- Situación actual de la seguridad informática.
- El vocabulario de la seguridad informática.
- Ataques de «capas bajas».
- Puntos fuertes y débiles del protocolo TCP/IP.
- Ilustración de ataques de tipo ARP e IP Spoofing, TCP-SYNflood, SMURF, etc.
- Denegación de servicio y denegación de servicio distribuido.
- Ataques a la aplicación.
- Recogida de información.
- HTTP, un protocolo especialmente expuesto (SQL injection, Cross Site Scripting, etc.).
- DNS: ataque Dan Kaminsky.

Trabajo práctico : Instalación y uso del analizador de redes Wireshark. Despliegue de un ataque a la aplicación.

2) Arquitecturas de seguridad

- ¿Qué arquitecturas son necesarias?
- Proceso de direccionamiento seguro: RFC 1918.
- Traslado de direcciones (FTP como ejemplo).
- El papel de las zonas desmilitarizadas (DMZ).
- Ejemplos de arquitecturas.
- Proteger la arquitectura mediante la virtualización.
- Cortafuegos: piedra angular de la seguridad.
- Acciones y límites de los cortafuegos de redes tradicionales.
- Evolución tecnológica de los cortafuegos (Appliance, VPN, IPS, UTM, etc.).

PARTICIPANTES

Responsables y arquitectos de seguridad. Técnicos y administradores de sistemas y redes.

REQUISITOS PREVIOS

Buen conocimiento de redes y sistemas.

COMPETENCIAS DEL FORMADOR

Los expertos que imparten la formación son especialistas en las materias tratadas. Han sido validados por nuestros equipos pedagógicos, tanto en el plano de los conocimientos profesionales como en el de la pedagogía, para cada curso que imparten. Cuentan al menos con entre cinco y diez años de experiencia en su área y ocupan o han ocupado puestos de responsabilidad en empresas.

MODALIDADES DE EVALUACIÓN

El formador evalúa los progresos pedagógicos del participante a lo largo de toda la formación mediante preguntas de opción múltiple, escenificaciones de situaciones, trabajos prácticos, etc.
El participante también completará una prueba de posicionamiento previo y posterior para validar las competencias adquiridas.

MEDIOS PEDAGÓGICOS Y TÉCNICOS

• Los medios pedagógicos y los métodos de enseñanza utilizados son principalmente: ayudas audiovisuales, documentación y soporte de cursos, ejercicios prácticos de aplicación y ejercicios corregidos para los cursillos prácticos, estudios de casos o presentación de casos reales para los seminarios de formación.
• Al final de cada cursillo o seminario, ORSYS facilita a los participantes un cuestionario de evaluación del curso que analizarán luego nuestros equipos pedagógicos.
• Al final de la formación se entrega una hoja de presencia por cada media jornada de presencia, así como un certificado de fin de formación si el alumno ha asistido a la totalidad de la sesión.

MODALIDADES Y PLAZOS DE ACCESO

La inscripción debe estar finalizada 24 horas antes del inicio de la formación.

ACCESIBILIDAD DE LAS PERSONAS CON DISCAPACIDAD

¿Tiene alguna necesidad específica de accesibilidad? Póngase en contacto con la Sra. FOSSE, interlocutora sobre discapacidad, en la siguiente dirección psh-accueil@orsys.fr para estudiar de la mejor forma posible su solicitud y su viabilidad.

- Cortafuegos y entornos virtuales.
- Servidor proxy y relé de aplicaciones.
- Proxy o cortafuegos: ¿competencia o complementariedad?
- Proxy inverso, filtrado de contenido, caché y autenticación.
- Relé SMTP: ¿una obligación?

Trabajo práctico : Implementación de un proxy Caché/Autenticación.

3) Seguridad de los datos

- Criptografía.
- Cifrado simétrico y asimétrico. Funciones de resumen.
- Servicios criptográficos.
- Autenticación de usuarios.
- La importancia de la autenticación recíproca.
- Certificados X509. Firma electrónica. Radius. LDAP (protocolo ligero de acceso a directorios=.
- Gusanos, virus, troyanos, malware y keyloggers.
- Tendencias actuales. La oferta antivirus, complementariedad de elementos. EICAR, un «virus» a conocer.

Trabajo práctico : Despliegue de un relé SMTP y un proxy antivirus HTTP/FTP. Implementación de un certificado de servidor.

4) Seguridad de los intercambios

- Seguridad del wifi.
- Riesgos inherentes a las redes inalámbricas.
- Los límites del WEP. El protocolo WPA y WPA2.
- Tipos de ataques.
- Ataque de intermediario (Man in the Middle) con el rogue AP.
- El protocolo IPSec.
- Presentación del protocolo.
- Modos túnel y transporte. ESP y AH.
- Análisis del protocolo y tecnologías relacionadas (SA, IKE, ISAKMP, ESP, AH, etc.).
- Los protocolos SSL/TLS.
- Presentación del protocolo. Detalles de la negociación.
- Análisis de las principales vulnerabilidades.
- Ataques sslstrip y sslsnif.
- El protocolo SSH. Presentación y características.
- Diferencias con SSL.

Trabajo práctico : Realización de un ataque Man in the Middle en una sesión SSL. Implementación del modo transporte IPSec/PSK.

5) Protección de un sistema, «Hardening»

- Presentación.
- Inadecuación de las instalaciones por defecto.
- Criterios de evaluación (TCSEC, ITSEC y criterios comunes).
- Proteger Windows.
- Gestión de cuentas y autorizaciones.
- Control de servicios.
- Configuración de red y auditoría.
- Proteger Linux.
- Configuración del núcleo.
- Sistema de archivos.
- Gestión de servicios y redes.

Trabajo práctico : Ejemplo de seguridad de un sistema Windows y Linux.

6) Auditoría y seguridad cotidiana

- Herramientas y técnicas disponibles.
- Pruebas de intrusión: herramientas y medios.

- Detección de vulnerabilidades (escáneres, sondas IDS, etc.).
- Herramientas de detección en tiempo real IDS-IPS, agente, sonda o corte.
- Reaccionar con eficacia en cualquier circunstancia.
- Supervisión y administración.
- Impactos organizativos.
- Vigilancia tecnológica.

7) Estudio de caso
- Estudio preliminar.
- Análisis de las necesidades.
- Elaborar una arquitectura.
- Definir el plan de acción.
- Despliegue.
- Procedimiento de instalación de elementos.
- Aplicación de la política de filtrado.

Trabajo práctico : Elaboración de un control de flujo.

FECHAS

Contacto