Seguridad de sistemas y redes, nivel 2

Curso práctico de 4 días - 28h
Ref.: SEA - Precio 2024: 2 000€ sin IVA

Este curso avanzado le permitirá medir el nivel de seguridad de su Sistema de Información mediante herramientas de detección de intrusiones, detección de vulnerabilidades, auditoría, etc. Le proporcionará conocimientos sobre soluciones avanzadas para mantener y actualizar el nivel de seguridad deseado a lo largo del tiempo, en función de sus necesidades.

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Medir el nivel de seguridad de los sistemas de información

Utilizar herramientas de detección de intrusos, detección de vulnerabilidades y auditoría

Reforzar la seguridad de los sistemas de información

Comprensión del funcionamiento de la arquitectura AAA (autenticación, autorización y contabilidad)

Implementación de SSL/TLS

Los participantes utilizarán una amplia gama de herramientas. Sonda SNORT IDS, exploración de vulnerabilidades con NESSUS, análisis y exploración de redes con ETHEREAL y NMAP. Protección de una red Wi-Fi.

PROGRAMA

última actualización: 02/2024

1) Recordatorios

- El protocolo TCP/IP.
- Traducción de direcciones.
- Arquitectura de red.
- El cortafuegos: ventajas y limitaciones.
- Proxies, proxies inversos: protección de aplicaciones.
- Zonas desmilitarizadas (DMZ).

2) Herramientas de ataque

- Paradigmas de seguridad y clasificación de los ataques.
- Principios de ataque: spoofing, flooding, inyección, captura, etc.
- Bibliotecas : Libnet, Libpcap, Winpcap, Libbpf, Nasl, lua.
- Herramientas: Scapy, Hping, Ettercap, Metasploit, Dsnif, Arpspoof, Smurf.

Trabajo práctico : Análisis de protocolos con Wireshark. Uso de Scapy y Arpspoof.

3) Criptografía, aplicación

- Los servicios de seguridad.
- Principios y algoritmos criptográficos (DES, 3DES, AES, RC4, RSA, DSA, ECC).
- Certificados y perfiles específicos para varios servidores y clientes (X509).
- Protocolo IPSEC y redes privadas virtuales (VPN).
- Protocolos SSL/TLS y VPN-SSL. Problemas de compresión de datos.

Trabajo práctico : Manejo de openssl e implementación de OpenPGP. Generación de certificados X509 v3.

PARTICIPANTES

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

REQUISITOS PREVIOS

Buenos conocimientos de TCP/IP y de seguridad de redes corporativas. O conocimientos equivalentes a los adquiridos en el curso "Seguridad de sistemas y redes, nivel 1" (ref. FRW).

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.

4) Arquitectura AAA (autenticación, autorización y contabilidad)

- La red AAA: autenticación, autorización y trazabilidad.
- Contraseña de un solo uso: OTP, HOTP, Google Authentificator, SSO (protocolo Kerberos).
- El lugar del directorio LDAP en las soluciones de autenticación.
- Los módulos PAM y SASL.
- Arquitectura y protocolo Radius (Autenticación, Autorización, Contabilidad).
- Posibles ataques.
- ¿Cómo puedo protegerme?

Trabajo práctico : Ataque a un servidor AAA.

5) Detección de intrusiones

- Principios de funcionamiento y métodos de detección.
- Actores del mercado, visión general de los sistemas y aplicaciones implicados.
- Escáneres de red (Nmap) y de aplicaciones (aplicaciones Web).
- IDS (Sistema de detección de intrusos).
- Ventajas y limitaciones de estas tecnologías.
- ¿Cómo deben situarse en la arquitectura empresarial?
- Visión general del mercado, estudio detallado de SNORT.

Trabajo práctico : Instalación, configuración y puesta en marcha de SNORT, redacción de firmas de ataque.

6) Comprobación de la integridad de un sistema

- Principios de funcionamiento.
- ¿Qué productos hay disponibles?
- Presentación de Tripwire o AIDE (Entorno Avanzado de Detección de Intrusiones).
- Auditorías de vulnerabilidad.
- Principios, métodos y organizaciones de gestión de la vulnerabilidad.
- Sitio de referencia y visión general de las herramientas de auditoría.
- Definición de una política de seguridad.
- Estudio e implantación de Nessus (estado, funcionamiento, desarrollo).

Trabajo práctico : Auditoría de vulnerabilidades de redes y servidores mediante Nessus y Nmap. Auditoría de vulnerabilidades de sitios web.

7) Gestión de eventos de seguridad

- Procesamiento de la información comunicada por los distintos dispositivos de seguridad.
- Consolidación y correlación.
- Presentación de SIM (Gestión de la Información de Seguridad).
- Gestión y protocolo SNMP: puntos fuertes y débiles en materia de seguridad.
- Solución de seguridad SNMP.

Trabajo práctico : Configuración de ataque SNMP.

8) Seguridad de la red WiFi

- ¿Cómo proteger una red WiFi?
- Las debilidades intrínsecas de las redes WiFi.
- SSID Broadcast, MAC Filtering, ¿en qué nos beneficia?
- ¿Sigue teniendo sentido la WEP?
- El protocolo WPA, la primera solución aceptable.
- ¿Es suficiente la implementación de WPA en modo de clave compartida?
- WPA, servidor Radius y AAA, implantación empresarial.
- 802.11i y WPA2: ¿qué solución tiene más éxito hoy en día?
- Inyección de tráfico, crackeo de claves WiFi.

Trabajo práctico : Configuración de herramientas de captura de tráfico, escaneo de red y análisis de tráfico WIFI. Configuración de un AP (Access Point) e implementación de soluciones de seguridad.

9) La seguridad de la telefonía IP

- Conceptos de voz sobre IP. Visión general de las aplicaciones.
- La arquitectura de un sistema VoIP.
- El protocolo SIP, una norma abierta para voz sobre IP.
- Los puntos débiles del protocolo SIP.
- Problemas de NAT.
- Ataques a la telefonía IP.
- ¿Cuáles son las soluciones de seguridad?

10) Seguridad del correo electrónico

- Arquitectura y funcionamiento de la mensajería.
- Protocolos y acceso al correo electrónico (POP, IMAP, Webmail, SMTP, etc.).
- Problemas y clasificaciones de los ataques por correo electrónico (spam, pesca, usurpación de identidad, etc.).
- Actores en la lucha contra el SPAM.
- Métodos, arquitecturas y herramientas de lucha contra el SPAM.
- Herramientas para recopilar direcciones de correo electrónico.
- Soluciones aplicadas para combatir el SPAM.

FECHAS

Contacto