

Fundamentos de sistemas para desarrolladores

Curso teórico práctico que ofrece los conocimientos básicos de sistemas orientados a un perfil desarrollador, con el fin de que conozcan los elementos de seguridad y administración que pueden afectar a sus desarrollos.

Objetivos

Ofrecer a los asistentes la formación necesaria para ser capaces de:

- ▶ Explicar los ataques comunes contra la red y las amenazas y vulnerabilidades asociadas
- ▶ Asegurar la información usando el control de autenticación y de acceso
- ▶ Despliegue y manejo de los certificados
- ▶ Asegurar la transmisión de datos, asegurar los servidores, proteger la mensajería
- ▶ Identificar las amenazas al perímetro de la red, los tipos de política de seguridad
- ▶ Identificar, responder y asistir a la investigación de los incidentes de seguridad
- ▶ Monitorizar los sistemas

Perfil del alumno

Desarrollador.

Temario

1. Preparación para asegurar la información
 - ▶ Explicar cómo se atacan los activos
 - ▶ Explicar cómo se aseguran los activos
2. Implementar en computadoras una línea base de seguridad
 - ▶ Introducción a las bases de computadoras seguras
 - ▶ Establecer la línea base
 - ▶ Supervisión de la línea base
 - ▶ *Microsoft Baseline Security Analyzer*
 - ▶ Asegurando las computadoras físicamente
 - ▶ Mantenimiento de línea base
3. Fundamentos básicos de TCP/IP
 - ▶ Redes, subredes, máscaras.
 - ▶ NAT y problemáticas de seguridad en firewalls
 - ▶ Protocolos de resolución de nombres (DNS) en Windows y/o Linux

4. Autenticación y acceso

- ▶ Introducción al control de acceso
- ▶ Poner en ejecución la autenticación
- ▶ Poner en ejecución el control de acceso
- ▶ Conceptos básicos de directorios, servicios y protocolos de autenticación

5. Usar la criptografía para asegurar la información

- ▶ Introducción a la criptografía
- ▶ Cifrado simétrico
- ▶ Funciones Hash
- ▶ Cifrado asimétrico (*Public Key Encryption*)
- ▶ Introducción a los certificados X.509
- ▶ Despliegue y manejo de certificados

6. Seguridad en la transferencia de información

- ▶ Seguridad en servidores Web
- ▶ Seguridad para los protocolos
- ▶ Seguridad en los navegadores
- ▶ Seguridad en los servidores de bases de datos
- ▶ Seguridad en los servidores de correo electrónico
- ▶ Seguridad en los clientes de correo electrónico
- ▶ Seguridad en la mensajería instantánea

7. Manejo de las operaciones de seguridad

- ▶ Ataques más comunes
- ▶ Establecer políticas y procedimientos de seguridad
- ▶ Educar a usuarios sobre políticas de seguridad
- ▶ Aplicación de políticas de seguridad en las operaciones administrativas
- ▶ Resolución de dilemas éticos al asegurar activos

8. Monitorización

- ▶ Análisis de rendimiento HW
- ▶ Análisis de rendimiento del Sistema Operativo
 - ▶ Memoria y procesador
 - ▶ Sistema de red y disco
- ▶ WMI
- ▶ SNMP
- ▶ Syslog

9. Preservar continuidad del negocio

- ▶ Preparación para recuperación de desastres
- ▶ Arquitecturas
- ▶ Estrategias de backup según la arquitectura
- ▶ Escalabilidad y *clustering*
- ▶ Replicación

10. Responder a los incidentes de seguridad

- ▶ Identificar incidentes de seguridad
- ▶ Responder a los incidentes de seguridad
- ▶ Investigar incidentes de seguridad