SEGURIDAD INFORMÁTICA

Objetivos

- Este curso proporciona a los asistentes los conocimientos necesarios para ser capaces de identificar los riesgos de seguridad, así como asegurar la red, sus recursos y planificar una estructura administrativa.
- En este curso el alumno será capaz de configurar, modificar y gestión una red inalámbrica. También podrá diferenciar las diferentes los diferentes tipos de redes wifi.
- Las redes informáticas están creciendo constantemente y se están conectando a Internet como consecuencia del e-commerce, de la productividad y del acceso a la información. Por ello, este curso quiere ilustrar a los estudiantes los posibles riesgos que pueden padecer en Internet. Con dicho objeto, en este curso se habla de todo aquello que hace referencia a la seguridad en Internet. firmas digitales, encriptación, firewalls, riesgos en la seguridad s básicos sobre conexión con bases de datos a través de ADO .NET y por último aprenderá a crear componentes.

Contenido

MÓDULO 1: SEGURIDAD INTERNET

1. Introducción a la seguridad

2. Introducción al firewall

3. Instalar un firewall

4. Usar un firewall

5. Criptografía

6. Redes privadas virtuales

7. Firma Digital

8. Actualizaciones

9. Seguridad en dominios

10. Instalar una Autoridad de Certificación

11. Crear un sitio web seguro

12. Recursos e información adicional

Test de evaluación

MÓDULO 2: SEGURIDAD EN REDES WIFI

1. Fundamentos de WIFI

2. Seguridad en WIFI

3. Fases de una conexión

4. WPA Escena con tres escenarios

5. Despliegue de WIFI

6. Tipos de intrusos de la red

7. Tipos de ataques

8. Tipos de intrusos según su actuación

9. Tipos de programas maliciosos y virus

10. ¿Qué hacer para evitar daños en el sis?

Práctica1

Práctica2

Test Final

MÓDULO 3: SEGURIDAD EN LAS REDES

1. Evaluación de riesgos de seguridad
1.1. Datos
1.2. Servicios
1.3. Ataques
1.4. Certificaciones de seguridad
1.5. Seguridad en la red

2. Conceptos de Windows 2000
2.1. Estructuras lógicas de Active Directory
2.2. Relaciones de confianza
2.3. Administrar utilizando la Directiva de grupo (Group Policy)
2.4. Proceso de autenticación Kerveros v5
2.5. Validación utilizando certificados
2.6. Validación NTLM
2.7. SID de seguridad
2.8. Acceso a los recursos
2.9. Grupo de usuarios

3. Administración
3.1. Modelos administrativos
3.2. Tareas administrativas
3.3. Grupos de usuarios
3.4. Administración remota

4. Cuentas de usuario
4.1. Diseño de directivas
4.2. Niveles de aplicación de directivas
4.3. Aplicación efectiva de directivas
4.4. Cuentas de usuario
4.5. Auditorías
4.6. Plan de auditorías

5. Seguridad de equipos Windows 2000
5.1. Seguridad de red física
5.2. Seguridad de passwords
5.3. Requisitos de seguridad
5.4. Seguridad por defecto de las máquinas W2K
5.5. Compatibilidad de aplicaciones no certificadas W2K
5.6. Uso de plantillas incrementales
5.7. Configuración de plantillas
5.8. Nuevas directivas

6. Seguridad de recursos

6.1. Siss de ficheros
6.2. Uso de la DACL
6.3. Permisos compartidos
6.4. Permisos NTFS
6.5. Recursos de impresión
6.6. Protección del registro
6.7. Encriptación de datos
6.8. Auditar el acceso a los recursos
6.9. Tareas de Backus

7. Asegurar los canales de comunicación

7.1. Riesgos de comunicaciones
7.2. Encriptación de canales de comunicación
7.3. Seguridad de protocolos de aplicación
7.4. Transmisiones seguras de ficheros
7.5. Transmisiones Web
7.6. Transmisiones e-mail
7.7. Uso de IPSec

8. Acceso de clientes No-Microsoft

8.1. UNIX
8.2. Autenticación de clientes UNIX
8.3. Asegurar acceso a ficheros
8.4. Interoperabilidad con Novell
8.5. Autenticación de clientes en Novell
8.6. Acceso seguro a los recursos Novell
8.7. Interoperabilidad con Macintosh
8.8. Autenticación de clientes Mac
8.9. Riesgos de servicios en redes heterogéneas

9. Acceso de clientes remotos

9.1. Riesgos de los servicios RAS
9.2. Autenticación de RAS
9.3. Autorizar conexiones remotas
9.4. Directivas de acceso remoto
9.5. Modelo de directivas RAS
9.6. Soportar accesos remotos de servidores NT 4.0
9.7. Definición de seguridad de llamada
9.8. Beneficios de la conexión VPN
9.9. Utilización de RADIUS

10. Acceso a oficinas remotas

10.1. Redes públicas y privadas
10.2. Seguridad de router
10.3. Routers Windows 2000
10.4. Requisitos de seguridad

11. Acceso de usuarios de Internet

11.1. Ataques comunes
11.2. Ataques de denegación del servicio
11.3. Escaneo de puertos

11.4. Protección de red interna
11.5. Filtro de protocolos a través de Firewall
11.6. Entrada de clientes desde Internet
11.7. Topologías de firewalls, screened subnets
11.8. Disponibilidad
11.9. Seguridad de tráfico de Internet a la Sceened

12. Acceso de usuarios a Internet

12.1. Protección de la red interna
12.2. Directivas de acceso a Internet
12.3. Planificación de los firewalls (ISA Server)
12.4. Acceso a Internet

13. Extensión de la red a socios del negocio

13.1. Intercambios de información
13.2. Seguridad de servicios
13.3. Partners remotos
13.4. Organizaciones lógicas de seguridad
13.5. Autenticación

14. Diseño del PKI

14.1. Infraestructura de claves
14.2. Ciclos de vida de certificados
14.3. Distribución de certificados
14.4. Auditorías del PKI
14.5. CA's comerciales
14.6. Directivas de CA's
14.7. Jerarquías de CA's
14.8. Seguridad de CA's
14.9. Mapeo de certificados

15. Planes de seguridad

15.1. Diseño de planes de seguridad
15.2. Requisitos de seguridad
15.3. Modificación del plan de seguridad

Preguntas y Respuestas

Test de conocimientos