

TÍTULO: Planificación De La Seguridad Informática En La Empresa

HORAS: 80

OBJETIVOS:

Planificar la seguridad informática en la empresa

CONTENIDOS:

1. DEBILIDADES, AMENAZAS Y ATAQUES
 - 1.1. Tipos de atacantes.
 - 1.2. Motivaciones del atacante.
 - 1.3. Metodología de un atacante determinado.
 - 1.4. Vulnerabilidades y ataques comunes.
 - 1.5. Herramientas de hacking.
 - 1.6. Ingeniería social.
 - 1.7. Prevención de ataques.
 - 1.8. Respuesta a contingencias.
2. ADMINISTRACIÓN DE LA SEGURIDAD EN REDES.
 - 2.1. Diseño e implantación de políticas de seguridad.
3. TECNOLOGÍAS CRIPTOGRÁFICAS.
 - 3.1. Encriptación simétrica.
 - 3.2. Encriptación asimétrica.
 - 3.3. Firmas digitales.
 - 3.4. Certificados digitales.
 - 3.5. SSL/TLS. La herramienta de encriptación multiusuarios.
 - 3.6. Navegación segura: HTTPS.
4. SISTEMAS DE AUTENTIFICACIÓN.
 - 4.1. Tecnologías de Identificación.
 - 4.2. PAP y CHAP.
 - 4.3. RADIUS.
 - 4.4. El protocolo 802.1X.
 - 4.5. La suite de protocolos EAP: LEAP, PEAP, EAP-TLS.
 - 4.6. Sistemas biométricos.

5. REDES VIRTUALES PRIVADAS.

5.1. Beneficios y características.

5.2. IP Sec.

5.3. VPNs con SSL-TLS.

6. FIREWALLS

6.1. Arquitectura de Firewalls

6.2. Filtrado de paquetes sin estados

6.3. Servidores Proxy

6.4. Filtrado dinámico o "stateful"

6.5. Firewalls de siguiente generación

6.6. Funciones avanzadas

7. DETECCIÓN Y PREVENCIÓN AUTOMATIZADA DE INTRUSIONES (IDS-IPS)

7.1. Arquitectura de sistemas IDS

7.2. Herramientas de software

7.3. Captura de intrusos con Honeypots