

TEMARIO DE SEGURIDAD EN REDES Y ETHICAL HACKING

1. Conceptos básicos
Introducción
2. Seguridad de la organización
Evaluación y gestión de la seguridad
Familia de las ISO/IEC 27000
Políticas
Organización de la seguridad
Clasificación y control de activos
Seguridad del personal
Seguridad física y ambiental
3. Seguridad de las comunicaciones (I)
Gestión de comunicaciones y operaciones
Control de acceso
4. Seguridad de los sistemas
Desarrollo y mantenimiento de sistemas
Administración de la continuidad
Cumplimiento
5. Seguridad de la información en las pymes
6. IS2ME (seguridad de la información a la mediana empresa) Criptología
Introducción a la criptología aplicada
7. Seguridad de las comunicaciones (II)
Código malicioso
Virus, Gusanos, Troyanos, Bombas lógicas, Traps, Spyware
Seguridad en los componentes de redes e Internet
Enmascaramiento, vulnerabilidades de software, SQL Injection, Cross Site Scripting, Buffer Overflow, Sniffing, Scanning, Spoofing, Flooding, DOS, DDOS.
Firewall y proxy.
8. Herramientas de seguridad
Ataque:
sniffers
escaneo de puertos y vulnerabilidades
keyloggers
busqueda en la red (google hacks, wikto, dns, etc.)
ataques de contraseña
9. Defensa:
antivirus
antispyware
acceso remoto
actualizaciones
backups
mensajería seguro
anti phishing
gestión de contraseñas
logs