

SEGURIDAD WIRELESS WIFI

SEGURIDAD INALAMBRICA :¿ CÒMO PROTEGER MI RED INALAMBRICA?

- Herramientas para cuidar tu red inalámbrica
- Técnicas utilizadas para detectar intrusos en nuestra red
- Software que te ayudara a detectar intrusos en tu red en tiempo real

SEGURIDAD INALAMBRICA BASICA:

- Control de acceso (autenticación)
- Open system
- Sharedkey
- Hiddenssid
- Filtros por Mac
- Privacidad de información:
- Wep (algoritmo rc4)
- Seguridad avanzada: wpa /wpa2
- Control de acceso
- Privacidad de información
- Tkip
- Aes
- Auditoria inalámbrica:
- ¿Qué tan segura es mi red inalámbrica?
- ¿Qué es un CHIPSET y para qué sirve?
- ¿Qué chipset son los más recomendables?
- ¿Qué programas podrían vulnerar mi seguridad wireless?
- (Backtrack 5, comview, wifiewey.)

BACKTRACK 5:

- ¿Por qué utilizar backtrack 5?
- ¿Qué es el modo monitor? ¿Por qué usarlo?
- Aircrack, airodump, aireplay, airdecap.
- Wireshark (analizador de ip,pe,dns)
- Webside-ng
- Spoonwep

HERRAMIENTAS UTILIZADAS EN EL BACKTRACK 5

- Sniffers comotcpdump, WireShark, ettercap o snort
- El generador de paquetes nemesis,
- Escáneres de puertos como nmap o su interfaz zenmap,
- sistemas de OS fingerprinting como el espectacular y casi imprescindible p0f,
- Herramientas forenses para recuperación de datos
- Metasploit, un entorno de generación y gestión de exploit
- kernel 2.6.38 y el entorno de escritorio Gnome

CIFRADO WEP

- Sniffer software que permitirá detectar SSID AP , MAC AP, CANAL AP y MAC cliente
- Software para la asociación del intruso
- Software para generar tráfico entre el intruso y el AP
- Software para descifrar las claves WEP
- Clonación MAC

SSID OCULTO

- Sniffer que detecta el ssid oculto

CIFRADO WPA-PSK / WPA2-PSK

- Software denegación de servicio
- Software para determinar el HANDSHAKE
- Software para descifrar la claves WPA y WPA2
- Diccionarios utilizados- Software.
- Programa para poder usar el ataque de fuerza bruta