

Wireless



- Wireless LANs
- IEEE 802.11.
- Permite la conexión de dispositivos de manera inalámbrica.
- Se transmiten los datos por medio de ondas electromagnéticas.



Wireless

Esquemas de autenticación:

- Autenticación abierta
- Clave compartida
- Clave compartida empresarial



WEP

Wired Equivalency Privacy

 No protege la conexión por completo sino solamente el paquete de datos.

Cifrar la información que se transmite.

 Poco tiempo después de implementado se encontraron vulnerabilidades.

 En el sistema WEP se pueden utilizar dos métodos de autenticación: Sistema Abierto y Clave Compartida.



Surge como remplazo a WEP. El WPA posee un protocolo denominado TKIP (Temporal Key Integrity Protocol). **WPA-Personal** WPA-Enterprise

Temporal Key Integrity Protocol} Se le conoce como hashing de WPA. Se aplica al protocolo WPA. También se puede incluir en WEP.

WAP2

- Wi-Fi Protected Access 2
- WPA2-Personal y WPA2-Enterprise.
- La primera otorga seguridad a través de contraseña y la segunda autentificando a los usuarios a través de un servidor.
- Utiliza el algoritmo de cifrado AES.



Debilidades

Las redes inalámbricas tienden a ser aún más vulnerables que las redes con cables.

Wardriving:

El objetivo es detectar la presencia de redes inalámbricas pertenecientes al cliente e identificar vulnerabilidades que permitan el ingreso



Debilidades



Cambiar MAC para hacerse pasar por otro dispositivo.

ARP Poisoning:

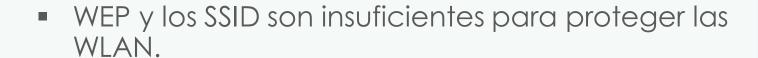
Es un ataque al protocolo ARP.

Access Point Spoofing:

El atacante finge ser un punto de acceso.



Hardening



- Utiliza una contraseña segura.
- Habilitar el filtrado de direcciones MAC.
- Habilitar cifrado de red.
- Habilitar el firewall del enrutador.



Hardening



- Configure el enrutador inalámbrico para usar direcciones IP estáticas.
- Apague su red inalámbrica doméstica cuando no esté en uso.

