1. Reconocimiento (Recon)

1. Reconocimiento (Recon)

¿Qué es el reconocimiento en pentesting inalámbrico?

El reconocimiento es la fase inicial de cualquier auditoría de redes WiFi. Consiste en identificar qué redes existen, qué dispositivos están conectados, y qué características técnicas tienen (canal, tipo de cifrado, potencia, etc.). Sin reconocimiento, es como disparar al aire sin saber a qué altura vuelan los pájaros.

¿Por qué es crítico?

- Permite mapear el territorio inalámbrico antes de atacar.
- Identifica objetivos viables (redes con clientes activos y señal suficiente).
- Revela configuraciones débiles (WEP, WPA2 con PSK, WPS activado…).

Conceptos básicos de 802.11

Antes de usar herramientas, necesitamos entender los **tipos de tramas(equivalente a paquetes en red cableada)** que circulan en WiFi:

1. **Beacons**
    - Tramas periódicas enviadas por cada **Access Point (AP)**.
    - Anuncian parámetros: SSID (nombre), canal, capacidades (WPA2, HT, VHT), tasas, etc.
    - Son el “anuncio público” del router.
2. **Probe Requests / Responses**
    - **Probe Requests**: envía un cliente buscando un SSID específico (o “broadcast” para descubrir redes).
    - **Probe Responses**: el AP responde con información parecida a las beacons, útil para redes ocultas.
3. **Data Frames**
    - Tráfico real del usuario: paquetes de navegación, descargas, etc. Indican actividad y permiten capturar handshakes.

Herramienta clave: `airodump-ng`

Parte de la suite **aircrack-ng**, `airodump-ng` es tu **escáner universal**.
Funciona así:

1. **Pone la tarjeta en modo monitor**
   - Escucha TODO el aire sin asociarse a redes.
2. **Muestra en pantalla**
   - **BSSID**: MAC del AP.
   - **PWR**: fuerza de señal (dBm).
   - **Beacons**: número de beacons recibidas.
   - **#Data**: paquetes de datos capturados.
   - **CH**: canal.
   - **MB**: tasas máximas anunciadas.
   - **ENC/CIPHER/AUTH**: detalles de cifrado.
   - **ESSID**: nombre de la red.

Flujo típico

1. **Arrancar monitor mode**

   ```
   sudo airmon-ng start wlan0
   ```

   Esto crea `wlan0mon` (o similar).
2. **Escanear todo el espectro**

   ```
   sudo airodump-ng wlan0mon
   ```

   Aparecerán decenas de APs y clientes.
3. **Filtrar por canal** (reduce ruido)

   ```
   sudo airodump-ng --channel 6 wlan0mon
   ```

   Solo escanea el canal 6, mejora velocidad de refresco.
4. **Focalizar en un objetivo**

   ```
   sudo airodump-ng -c 6 --bssid E4:47:B3:F0:E9:30 -w target wlan0mon
   ```

   Guarda en `target-01.cap` y `.csv`.

Ejemplo práctico de recon

Supongamos que quieres mapear todas las redes en **canal 11**:

1. Poner tu Alfa en modo monitor:

   ```
   sudo ip link set wlan0 down
   sudo iw dev wlan0 set type monitor
   sudo ip link set wlan0 up
   ```

2. Ejecutar `airodump-ng` en canal 11:

```
sudo airodump-ng --channel 11 wlan0
```

3. Analizar el output y elegir un AP con:
    - **PWR** ≥ -70 dBm (señal decente).
    - **#Data** > 5 (clientes activos).
    - **ENC** = WPA2 (objetivo clásico).

Por ejemplo, si ves:

```
BSSID              PWR  Beacons  #Data  CH  MB   ENC   CIPHER  AUTH  ESSID
28:77:77:74:B1:AC  -58      120     30  11  1733  WPA2  CCMP    PSK  Oficina
```

Tienes:

- AP “Oficina” en canal 11.
- Señal fuerte, tráfico activo.
- Cifrado WPA2-PSK.

¡Listo! Con eso terminas tu fase de reconocimiento y preparas el terreno para los siguientes ataques (deauth, handshake, etc.).
