Wireless Injection: Deauthentication Attack

- The Deauthentication Attack which is an attack of type DoS that targets the communication between a WiFi client and the WiFi AP or Router.
- The IEEE 802.11 protocol defines a special management frame called **deauthentication frame** which is sent by the AP to a station as a sanction technique to inform the station it has to disconnect from the network immediately.
- The deauthentication attack works on WPA2 despite encryption.

Deauthentication attack is the first step of other attacks like:

- Cracking the WPA2 Password by capturing the WPA2 4-Way Handshake by forcing the user to reconnect to the network.
- Forcing the users to connect to the hacker's rogue AP or to a Captive Portal (Evil Twin Attack).