Pre-Connection attack

A deauth attack, also known as a deauthentication attack, is a type of attack that is used to disrupt the communication between a device and a wireless access point (WAP). This attack can be used to disconnect devices from a WAP, effectively denying them access to the network.

To perform a deauth attack, you can use the **`aireplay-ng`** tool, which is part of the Aircrack-ng suite of tools. This tool allows you to send deauthentication packets to a target WAP in order to disconnect connected devices.

To use `aireplay-ng`, you will first need to put your wireless card into monitor mode. You can do this using the following command:

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

Replace "wlan0" with the name of your wireless interface.

Next, you will need to identify the target WAP and the clients that are connected to it. You can do this using the `airodump-ng` tool, like this:

```
sudo airodump-ng wlan0mon
```

Replace "wlan0mon" with the name of your wireless interface in monitor mode. This will show you a list of WAPs and clients in the area. Look for the target WAP and note its BSSID (MAC address) and the client's MAC address.

Once you have the BSSID and client MAC address, you can use `aireplay-ng` to send deauthentication packets to the target WAP and disconnect the client. The syntax for this command is as follows:

```
sudo aireplay-ng --deauth [number of deauth packets] -a [BSSID] -c [client MAC] wlan0mon
```

Replace "[number of deauth packets]" with the number of deauthentication packets you want to send (e.g. 10), "[BSSID]" with the target WAP's BSSID, and "[client MAC]" with the client's MAC address.

It's important to note that deauth attacks are illegal in most countries and should only be used for educational or testing purposes. They can cause serious disruptions to networks and should not be used maliciously.