**DE-AUTHENTICATION ATTACK**

**(pre-connection attack)**

This is a small attack that can be used as a plugin in order to make other attacks possible

**Allows us to disconnect any device from any network without us connected to the network and not even knowing the password**

To do this we must pretend to be the client that we want to disconnect by changing our MAC Address to the MAC Address of that client and tell the router i want to disconnect from you

Then we are going to pretend to be the router again by changing our MAC Address to the router's MAC Address and tell the client that you requested to be disconnected so im going to disconnect you

We won't do this manually, we are going to use a toll called **aireplay-ng** to do that

aireplay-ng --deauth 100000000 -a 00:11:22:33:44:55 -c 55:44:33:22:11:00 wlan0

(name of program)(deauth attack)(large number of packets so it keeps sending the de-auth packets to both the client and the router and keep the client disconnected)(-a to specify the MAC Address of the target router or the target access point)(-c to specify the MAC Address of the client)(the wireless adapter in monitor mode)

**!! This would work but in very rare cases this command will fail unless airodump-ng is running against the target network !!**

**(so use terminator)**

This attack is very useful in social engineering cases, you could pretend that you are form the IT Department and ask them to install a virus or a backdoor and tell them it would fix their issue

**You can also use this to capture the handshake, this is VITAL when it comes to WPA cracking**