Hacking WPA2-PSK

- WPA and WPA2 are replacements for WEP which has been proved flawed and easy to crack. Nowadays WPA2 with a PSK or Enterprise protects all WiFi communications.
- WPA2 uses AES as the encryption protocol which is very secure and impossible to crack. If you use a strong password the wifi network will be extremely secure.
- The weakness in the WPA2-PSK protocol is that the encrypted password is shared in what is known as the 4-way handshake.

Hacking WPA2-PSK consists of 3 different phases:

1. Injecting deauthentication packets to make a WiFi client to deauthenticate from the network.

2. Once deauthenticated the client will try to reconnect to the network. This is when we grab the WPA2 4-way handshake.

3. Offline cracking the 4-way handshake which is encrypted with AES.