**WPA/WPA2 ENCRYPTION CRACKING**

**GETTING THE HANDSHAKE**

**- Fixed all weaknesses in WEP**

**- Packets contain no useful data**

**- Only packets that can aid with the cracking process are the handshake packets**

**There are 4 packets sent when a client connects to the network**

**The keys in WPA2 are unique, temporary and much longer than those in WEP so the packets are useless for us**

**Even if we capture 1 million of packets they would still be useless**

**To do so first:**

use airodump-ng to list the networks and target the network with airodump-ng and we want to write the packets

**!! If a new device connects we will automatically capture the handshake !!**

so if(new device connects)

{

handshake found;

}

else

{

run deauthentication attack;

}

**(this if check is not real)**

We know that deathentication attack disconnect a device for a period of time

**The device will automatically connect once we stop the attack**

**When he connects, the handshake will be sent in the air and we will capture it**

**That way we wont have to wait for a device to connect to the network**

**To do that we run deauthentication attack**

aireplay-ng --deauth 4 -a 00:11:22:33:44:55 -c 55:44:33:22:11 wlan0

(aireplay-ng)(run deauth attack)(4 so nobody would notice the disconnection)(-a to specify the targeted MAC Address)(-c to specify the MAC Address of the client connected to the network)(our wireless adapter in monitor mode)

**Once the client connected again, we receive the handshake**

**We can quit airodump-ng because the handshake is saved in the written .cap file**

After this we can use the handshake to crack the network

**The handshake does not contain any information that can help us to recover or recalculate the WPA key**

**The information in it can only be used to check whether a password is valid or not**

Therefore we are going to create a **wordlist** which is basically a big text file that contain a large number of passwords

Then go through the file, go through the passwords one by one and use them with the handshake in order to check whether this password is valid or not

You can download ready wordlists from the internet or create your own