**CRACKING WPA/WPA2**

**USING WORDLIST ATTACK**

**Things we need:**

**1. Handshake**

**2. Wordlist**

**To crack the network:**

**aircrack-ng is going to unpack the handshake and extract the useful information**

**The MIC or the message integrity code is whats used by the access point to verify whether a password is correct or not**

Its going to seperate and put it to the side and then its going to use all of the other information combined with the first password from the wordlist to generate a MIC, another message integrity code

Then its going to compare the new MIC to the one thats already in the handshake

**If the MIC generated using this information + the first password is the same then the password used to generate the new MIC is the password for the network**

Otherwise the password is wrong and it will move to the next password and will do the same

**!! Thats why the success of this attack really depends on your Wordlist !!**

Now to crack..

**first:**

**Make sure you have the handshake as .cap**

**Make sure you have the Wordlist ready**

**second:**

use aircrack-ng

aircrack-ng handshake.cap -w Wordlist.txt

(name of program)

(name of the file containing handshake)

(-w to specify the Wordlist file)

**The speed of the cracking depends on your processor and the size of your Wordlist file**

**There are also online services that you can try where you upload the handshake and they have huge Wordlists and super computers to run through these Wordlists and try to give you the password(they can be easily found in Google)**

After aircrack-ng is done it will tell us the key is found ;)

**! This is the only practical way known so far to crack WPA/WPA2 keys except WPS crack !**

**There are methods to speed up this process, so you can use the GPU for cracking because its much faster than the CPU(If you have a GPU)**

**You can also use rainbow tables**

**You can also pipe the Wordlist as its being created in Crunch to Aircrack-ng, this way you can create bigger Wordlists without using any storage on your computer**

There are also methods so that you can pause your cracking progress and then come back after awhile without losing your progress

**You can use social engineering to get the password using an evil twin attack where you trick one of the users to give you the password**