2. Pre Connection Attacks

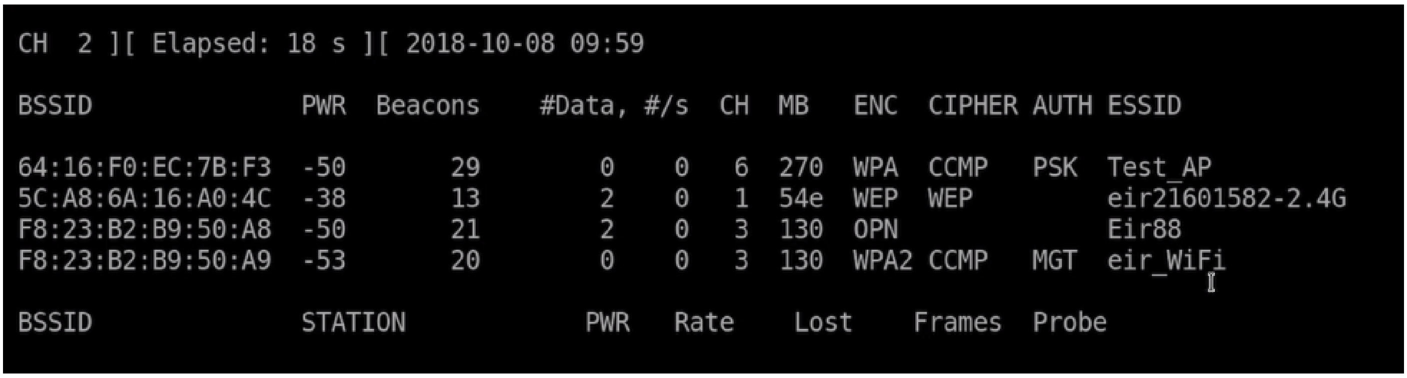
I am assuming you already did this:

>>you need to prepare your network card like here<<

Scan Networks

```
airodump-ng wlan0
```

You should see something like this:



```
CH  2 ][ Elapsed: 18 s ][ 2018-10-08 09:59

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

64:16:F0:EC:7B:F3  -50       29        0    0   6  270  WPA  CCMP   PSK  Test_AP
5C:A8:6A:16:A0:4C  -38       13        2    0   1  54e  WEP  WEP         eir21601582-2.4G
F8:23:B2:B9:50:A8  -50       21        2    0   3  130  OPN              Eir88
F8:23:B2:B9:50:A9  -53       20        0    0   3  130  WPA2 CCMP   MGT  eir_WiFi

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

let's break this down:

BSSID

Is the MAC Address of the Network

PWR

Is the signal strenght or power. The higher the number, the better signal we have

Beacons

Are the frames send from the Network to broadcast it's existance. Every Network, even if it's hidden, sends this frames to tell the wireless devices that it exists and it's MAC Address, it's channel, it's encryption and it's name

Data

This are the data packages or data frames. They are the packages which get interesting when it comes to wireless hacking

#/s

Are the packages which were collected the last 10 seconds

CH

Is the wireless Channel of the Network

MB

Is the Maxinum Speed supported

ENC

Is the Encryption used

CIPHER

Cipher used in the Network

Auth

is the authentications used in this network. For example PSK (Pre shared key) or MGT

ESSID

Is the Network Name

Don't worry just jet about **ENC, CIPHER and Auth** just yet, it will be a part in the gaining Access part of this Wiki

---

Revision #5
Created 10 February 2023 16:59:06 by tinfoil-hat
Updated 9 March 2023 18:06:05 by tinfoil-hat