How to crack a WEP network

This guide will show the steps needed to cracking a WiFi network protected by a WEP key.

The steps are the following:

1. **Run your network card in monitor mode**
2. **Sniff AP traffic**
3. **Send ARP Message in order to generate traffic with the AP**
4. **Crack the network**

The first step is to put your card in monitor mode, in order to sniff AP traffic

1) Become administrator
   a) **$sudo su**
2) Stop network manager and create and put network card in monitor mode
   a) **$/etc/init.d/network-manager stop**
   b) **$iw dev <<YOUR_NETWORK_CARD_NAME>> interface add wlan0mon type monitor wlan0mon**

Sniff AP Traffic

1) If not present install aircrack-ng
   a. **$sudo apt install aircrack-ng**
2) As administrator run airodump-ng
   a. **$airodump-ng wlan0mon**
3) Look at the AP informations, like channel and bssid, will be useful later
4) Relaunch airodump-ng with more informations
   a. **$airodump-ng -c <<N_CHANNEL>> --bssid <<YOUR_AP_BSSID>> -w wep_capture**
5) In another terminal, run aircrack-ng (as admin) in order to obtain the network password
   a. **$aircrack-ng wep_capture.cap**

Send ARP message to generate traffic on the AP

If, in your AP, there is a lot amount of traffic we could trigger it in order to obtain more so that we can exploit it to retrieve the password

1) Open another terminal, as admin, and run aireplay-ng to send package
   a. **$aireplay-ng -3 wlan0mon -b <<YOUR_AP_MAC>>**

Aireplay, in mode -3 will send ARP traffic at the hosts connected to the AP. This will trigger traffic through AP giving us the right amount of IV (Initialization Vector) in order to retrieve the password

2) We could send data also for specific hosts, connected to the AP. The connected hosts could be seen on airodump-ng capture
   a. **$aireplay-ng 3 wlan0mon -b<<YOUR_AP_MAC>> -h <<HOST_MAC_ADDRESS>>**

Crack the network

Now is time to retrieve password letting aireplay running. At this steps airodump will continue to collect data, analyzed from aircrack (both running in different shell) that try to know the password of the AP. So, we just must wait until aircrack is able to find it.

After some time on aircrack-ng shell our password will be visible!