WEP Cracking

STEPS WE WILL BE USING TO CRACKING WEP KEY

1. Start the wireless interface in monitor mode on the specific AP channel
2. Test the injection capability of the wireless device to the AP
3. Use aireplay-ng to do a fake authentication with the access point
4. Start airodump-ng on AP channel with a bssid filter to collect the new unique Ivs (Initialization Vectors)
5. Start aireplay-ng in ARP request replay mode to inject packets
6. Run aircrack-ng to crack key using the IVs collected

WEP Cracking

In order to crack wireless passwords and test insecure Access point, we need to capture the IVs.

We will capture using aireplay-ng replay an ARP packet to generate new unique IVs.

You need to be familiar with ARP (#See ARP in google)

We will use aircrack-ng suite to test the weak AP security