# WEP Cracking

* To crack WEP we need to
  + Capture a large number of packets/ IVs (Initialization Vector – sent in plain text) – using airodump-ng
  + Analyse the captured IVs and crack the key – using aircrack-ng

Steps:

* Airodump-ng –bssid [] – channel [] –write []
* Aircrack-ng filename
* Can connect through key or ASCII password (may not always get ASCII password)
* If using key then remove colons between numbers

Fake authentication:

* When cracking WEP if the network is not busy you will not be able to capture enough “data” to crack WEP
* We need to associate with the AP before launching the attack
  + NOT CONNECTING
  + Sending fake requests – telling the network “I want to communicate with you don’t ignore me”

Steps:

* Airodump-ng –bssid [] – channel [] –write []
* Aireplay-ng –fakeauth 0 -a MAC ADDRESS/ BSSID -h MAC ADDRESS OF WIRELESS ADAPTER mon0
* Replace “ - ” with “ : ” on mac address of wireless adapter

Now we have associated ourselves with the AP we can now force the AP to generate new IVs

ARP Request replay

* Wait for an ARP packet
* Capture it, and replay it
* Causes the ap to produce another packet with a new IV
* Keep doing this until we have enough IVs to crack the key

Steps:

* Aireplay-ng –arpreplay -b MAC ADDRESS/ BSSID -h MAC ADDRESS OF WIRELESS ADAPTER mon0
* Aireplay-ng –fakeauth 0 -a MAC ADDRESS/ BSSID -h MAC ADDRESS OF WIRELESS ADAPTER mon0
* Aircrack-ng filename