**GAINING ACCESS**

**NOT BUSY WEP CRACKING**

**Problem:**

**- if network is not busy it would take hours to capture enough IVs**

**Solution:**

**Force the AP to generate new IVs**

Before doing this we need to **associate** with this network(we want to communicate with it) because by default access points ignore any requests they get unless the device has connected to this network or associated with it this means **we dont have to be connected**(because we dont have the password)

**What we are doing is we are telling the network hey, i want to communicate to you dont ignore my requests**

**first:**

run airodump-ng and target the wanted network

**second:**

**To associate with the target network we are going to use** aireplay-ng

**MAC Address of your wireless adapter is the first 6 combinations in unspec**

**The reason why we dont see it clearly is because it is in monitor mode**

aireplay-ng --fakeauth 0 -a 00:11:22:33:44:55 –h 55:44:33:22:11:00 wlan0

(program used for a number of attacks)(telling it we want to run fake authentication attack)(0 because we want to do it once)(-a MAC Address of the target network)(-h MAC Address of my wireless adapter)(the adapter in monitor mode)

**Use association everytime before doing stuff**

It will make the **AUTH** of the network **OPN** and our wireless adapter will show as client of the target network so now we can communicate with the network and **it wont ignore us without even connected to it**

**Now we can start injecting packets into the traffic to force the access point to generate new packets with new IVs**

This will increase the number of data really really quickly allowing us to crack **WEP** network in minutes even if the network was not busy

**There are many ways to do this but we are going to use the most reliable method which is using an ARP request replay attack**

**The method:**

**Wait for an ARP packet(special type of packet that we are going to be waiting on)**

**Once this packet is sent in the network, we are going to capture it and retransmit it**

**Once we do this, the router is forced to generate a new packet with a new IV**

**So by repeating this process, we will be forcing the router to continously generate new packets with new IVs**

**When we have enough data, we have enough IVs we can run aircrack-ng exactly as we did before and crack the key**

**third:**

use aireplay-ng again but differently

aireplay-ng --arpreplay -b 00:11:22:33:44:55 -h 55:44:33:22:11:00 wlan0

**Now we dont want to do fakeauth attack but instead arp request replay attack**

**The 0 is not there because it doesnt need to be run more than once and we changed -a to -b**

**After we do this the wireless adapter is waiting for an ARP packet, once there is an ARP packet transmitted in this network, its going to capture it and its going to retransmit it**

Once it does that, the access point will be forced to generate a new packet with a new IV and we will keep doing this, forcing the access point to continually generate new packets with new IVs

**Now we just wait, we are literally just waiting for an ARP packets to be sent in the air**

The number of packets in **#Data** should increase really quick which means that we managed to capture ARP packet, the ARP packet got retransmitted, forced the router to generate a new packet with a new IV

**fourth:**

**Once we have enough packets(could be around 47 000 but also more)**

use aircrack-ng and you are done

Note: the key after KEY FOUND! is in hex