**GAINING ACCESS**

**BUSY WEP CRACKING**

**- WEP == Wired Equivalent Privacy**

**- Old encryption that can be easily broken**

**- Uses an algorithm called RC4 to encrypt its data**

**- Each packet is ecrypted using a unique key stream**

**- Random initialization vector(IV) is used to generate the keys streams**

**- The initialization vector is only 24 bits**

**- IV + Key(password) = Key stream**

**Router has the Key but not the IV so the package contains the IV so the router can decrypt the packet**

**The data is encrypted but the IV is not**

In order to crack **WEP** we need to first capture a **large number of packets(airodump-ng)** that means we will capture a **large numbers of IVs** and because they are short they will be repeated so we will use **Aircrack-ng** to run statistical attacks and crack the **WEP** **key**

**!! This works for busy network !!**

**To do so first enable monitor mode**

**second:**

use airodump-ng to list all the networks

**third:**

use airodump-ng for this network only and **WRITE** the info

**- The higher the #Data number the higher chance to crack the key**

**fourth:**

use aircrack-ng **test-01.cap**

(program)**(the written file)**

**After that it will show the Key and the ASCII password**

**Sometimes the ASCII password won't show so use the key it will always show**

If you want to connect to the network from Kali, first reboot it, sometimes it will get bugs otherwise

**To connect using the Key, to do that just remove the dots**

**11:22:33:44:55 == 1122334455**

Now you can connect with it like normal password