(1)

# iwconfig

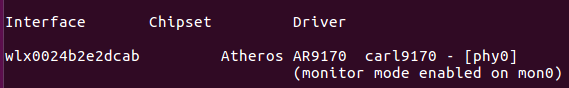
查看无线设备。如果全是no wireless extensions就表示机子没有无线设备，需要装个无线网卡。如果有非no wireless extensions行就表示这是无线设备，可以用来抓包。

(2)

有可以使用的无线网卡

# (sudo) airmon-ng start (无线网卡名)

然后有一行(monitor mode enabled on mon0)

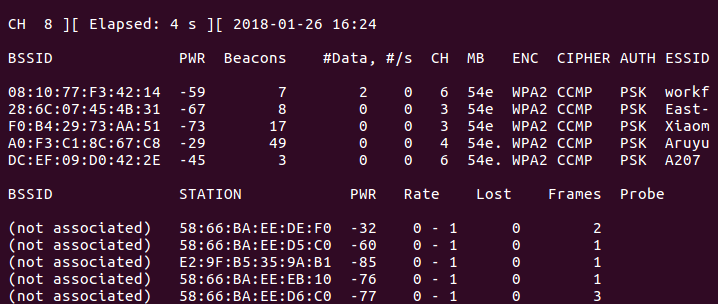


表示开启监听模式，以后用mon0来表示监听网卡。

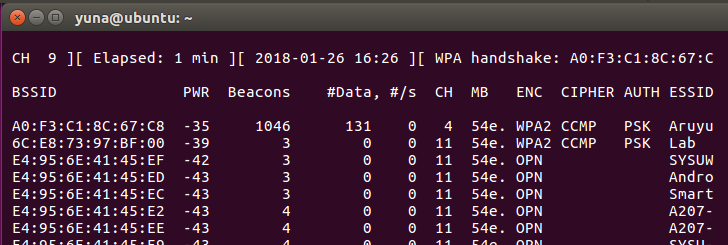
(3)

# (sudo) airodump-ng mon0

然后就开始搜附近的WiFi



如果右上角出现了[WPA handshake: xx:xx:……]，就表明抓到了握手包。



拿右上角那个Mac地址和BSSID列表的进行比较，一致的就是那个AP的握手包，可以盯着这个抓。

(4)

# (sudo) airodump-ng –w (文件路径/文件名) --bssid xx:xx:…… mon0

监听特定AP。文件保存在-w后面的参数里，如果不指定路径，则保存在用户主目录上（~）