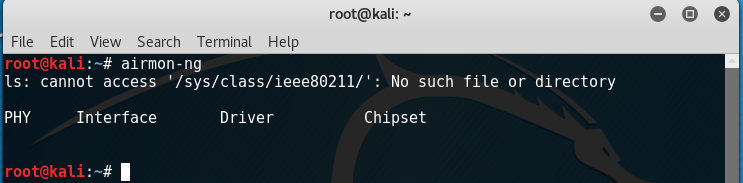
基于KALI虚拟机破解WIFI密码

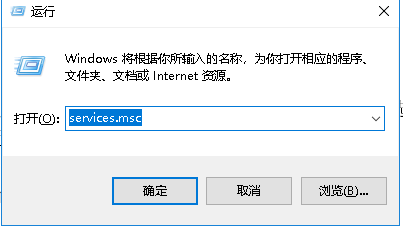
# 第一步：在VMware虚拟机上打开Kali虚拟机

# 第二步：连接无线网卡

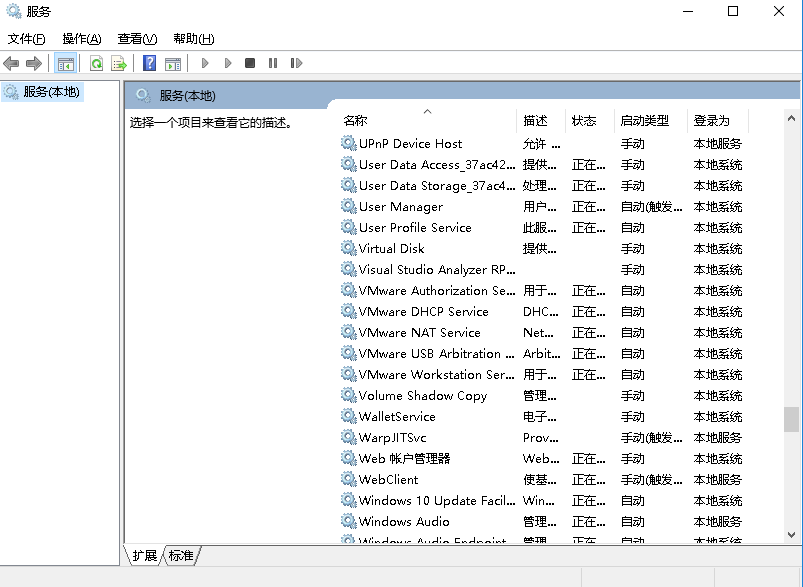
在虚拟机上使用kali无法访问本机的网卡用airmon-ng命令查看



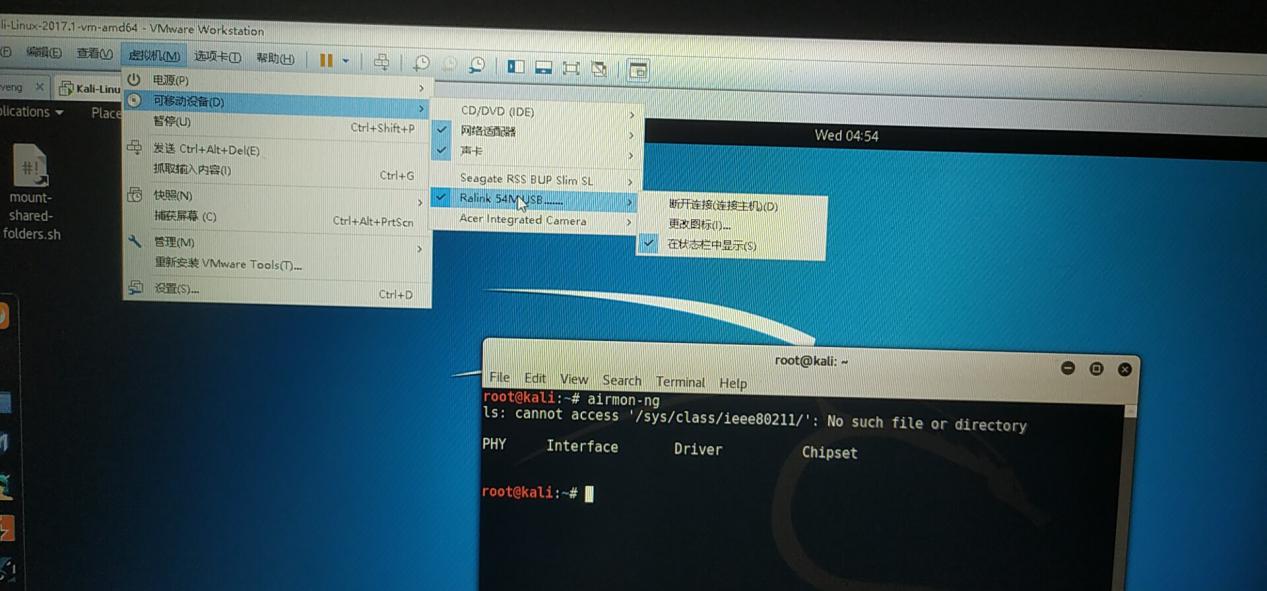
发现虚拟机无法访问网卡，所以需要使用外接的USB无线网卡，首先在主机上按win+r键然后输入services.msc 然后回车



确定后见下图：找到VMware USB Aribitration...选项，并将其设置为启动



打开虚拟机，在上面的虚拟机选项中->选择可自动设备->中的->usb无线网卡->连接



然后看右下角的U盘图标是否是灰色，如果是灰色，则右键选择链接



# 第三步：开启无线网卡

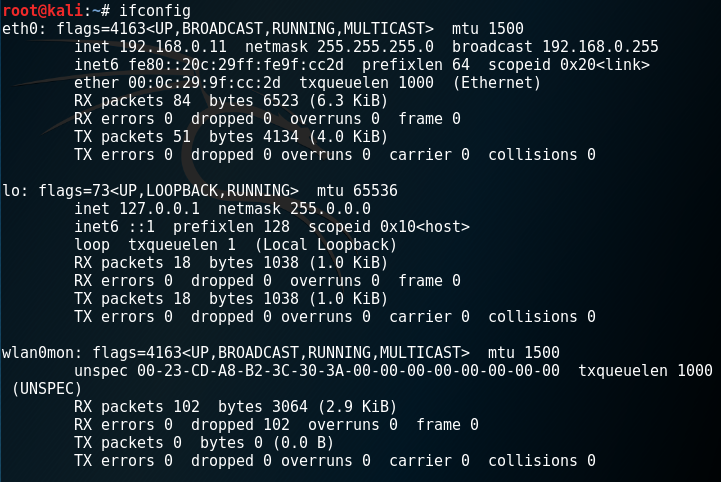
输入ifconfig查看网卡信息



  输入airmon-ng start wlan0开启网卡监听模式



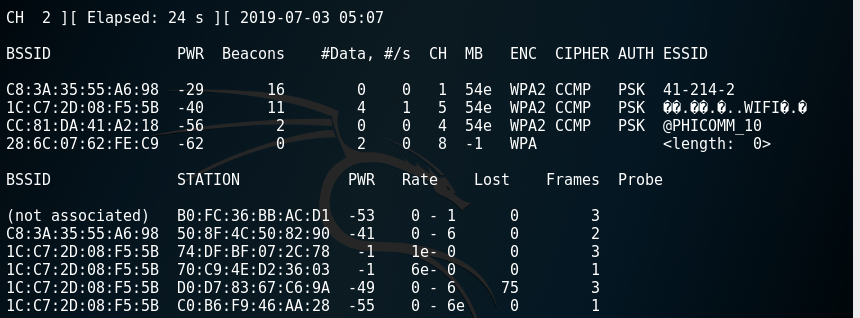
启动后再次查看网卡信息



网卡名加了 mon后缀则表示成功

# 第四步：扫描周围WIFI,发起攻击，截取秘钥数据包

输入airodump-ng wlan0mon(此处为网卡名），扫描结束后（短时间内没其他多的项目加入即可视为扫描结束）按ctrl+c结束任务



此时如上图，显示附近wifi的信息，其中：

BSSID为wifi的MAC地址

PWR为信号强弱程度，数值越小信号越强

#DATA为数据量，越大使用的人就越多

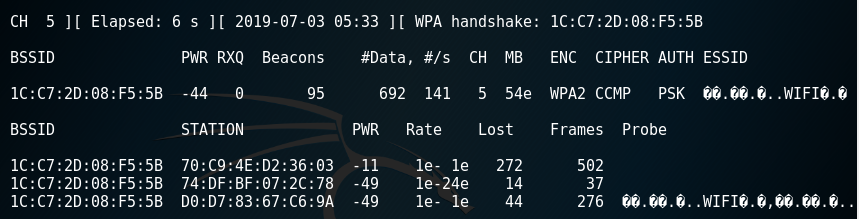
CH为信道频率（频道），

在一个频道上才能进行后续操作，此时客户机与主机断开的连接，主机断开的网络，在进行网络通信时，虚拟机的网络配置应该为桥接或者NAT模式，ESSID为wifi的名称，中文可能会有乱码，

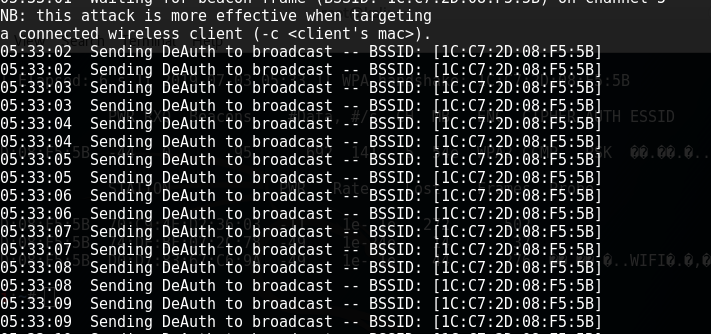
退出扫描后输入命令airodump-ng -c 5 --bssid 1C:C7:2D:08:F5:5B -w/home/root wlan0mon

注意此处的5是频道，1C:C7:2D:08:F5:5B为mac地址，/home为抓取的数据包存储的目录，/root为包的名字，wlanmon为网卡名

回车后，所破解的wifi处于断网状态，此时用户会重新连接，便可以抓取数据包，抓到包后一定要ctrl+c结束任务否则wifi将一直处于断网状态。（此图为抓包成功后所截取的图,区别仅在于窗口右上角出现的WPA handshake）

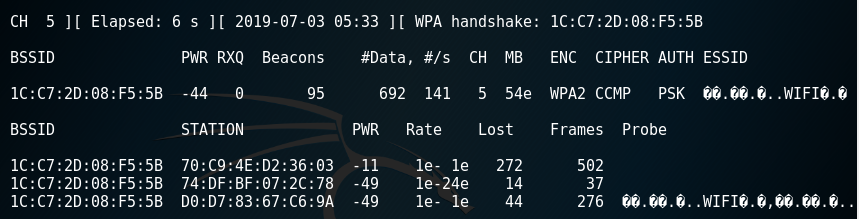


此时，新建一个窗口 ，输入aireplay-ng -0 0 -a mac地址 网卡名 （蓝色部分根据实际情况填写）



不停的发包

当窗口右上角出现 WPA handshake：时说明抓包成功，如下图：

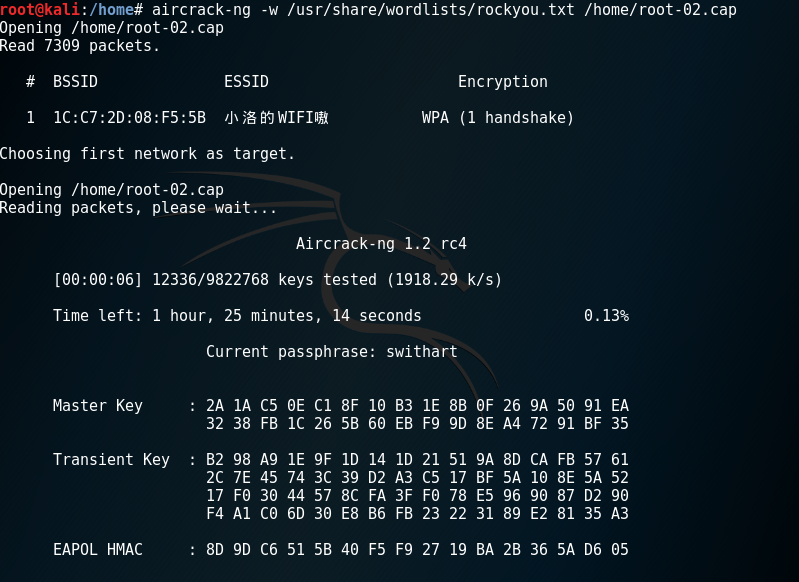


# 第五步：利用字典破解WIFI密码

新打开个窗口输入aircrack-ng -w /usr/share/wordlists/rockyou.txt /home/root-02.cap

/usr/share/wordlists/rockyou.txt为kali自带的字典（使用时确保字典已经被解压），也可以用自己的字典， /home/root-02.cap为所抓的数据包的位置

回车后数据包与字典比较查询密码



下图为上课时破解老师靶机的WIFI密码，得知靶机密码为（12345678）

