Kali Linux破解WIFI密码教程

目录

- 1、前言
- 2、暴力破解所需要的工具
  - 2.1、Kali Linux操作系统
  - 2.2、支持Kali Linux的无线网卡
  - 2.3、密码字典
- 3、Aircrack-ng介绍
- 4、WIFI破解教程

回到顶部

1、前言

使用Kali Linux暴力破解WIFI密码，说白了暴力破解就是穷举法，将密码字典中每一个密码依次去与握手包中的密码进行匹配，直到匹配成功。所以能否成功破解WIFI密码取决于密码字典本身是否包含了这个密码。破解的时间取决于CPU的运算速度以及密码本身的复杂程度。如果WIFI密码设得足够复杂，即使有一个好的密码字典，要想破解成功可能也需要花上个几天或者几十天甚至更久的时间。（注：私自破解他人WIFI属于违法行为，我这里使用自己的手机热点作为学习和测试）

回到顶部

2、暴力破解所需要的工具

2.1、Kali Linux操作系统

如果需要安装Kali Linux操作系统，请参考以下连接：
https://www.cnblogs.com/x1234567890/p/14859889.html

2.2、支持Kali Linux的无线网卡

淘宝、京东都有卖的，但是一定要看清楚买，需要支持Kali Linux操作系统，建议最好买免驱的。

2.3、密码字典

试验中用到的密码字典，是Kali Linux自带的密码字典，使用密码字典之前需要先将其进行解压，或者你也可以用自己准备好的密码字典将其传到Kali Linux中。

回到顶部

3、Aircrack-ng介绍

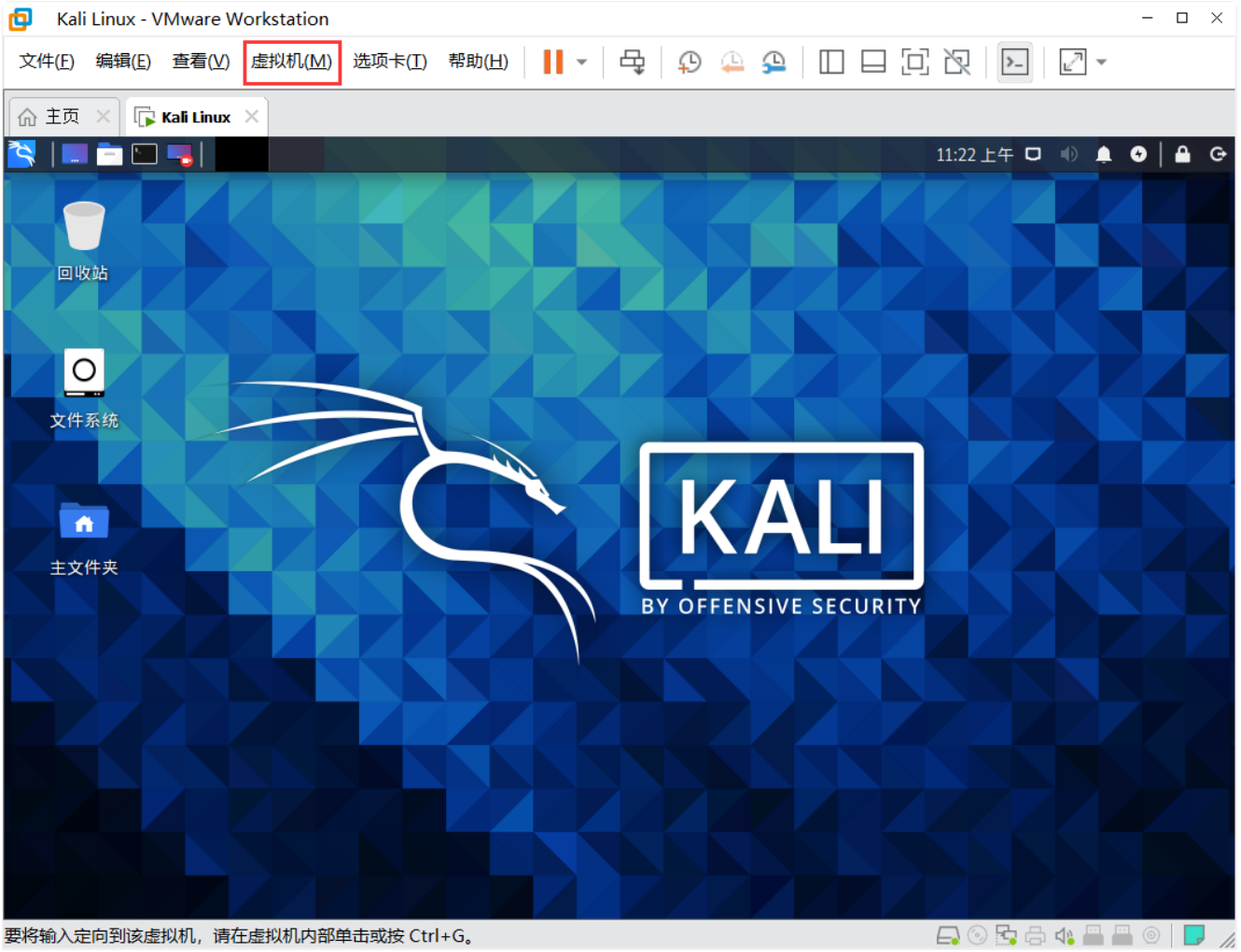
Aircrack-ng是一个与802.11标准的无线网络分析有关的安全软件，主要功能有：网络侦测，数据包嗅探，WEP和WPA/WPA2-PSK破解。

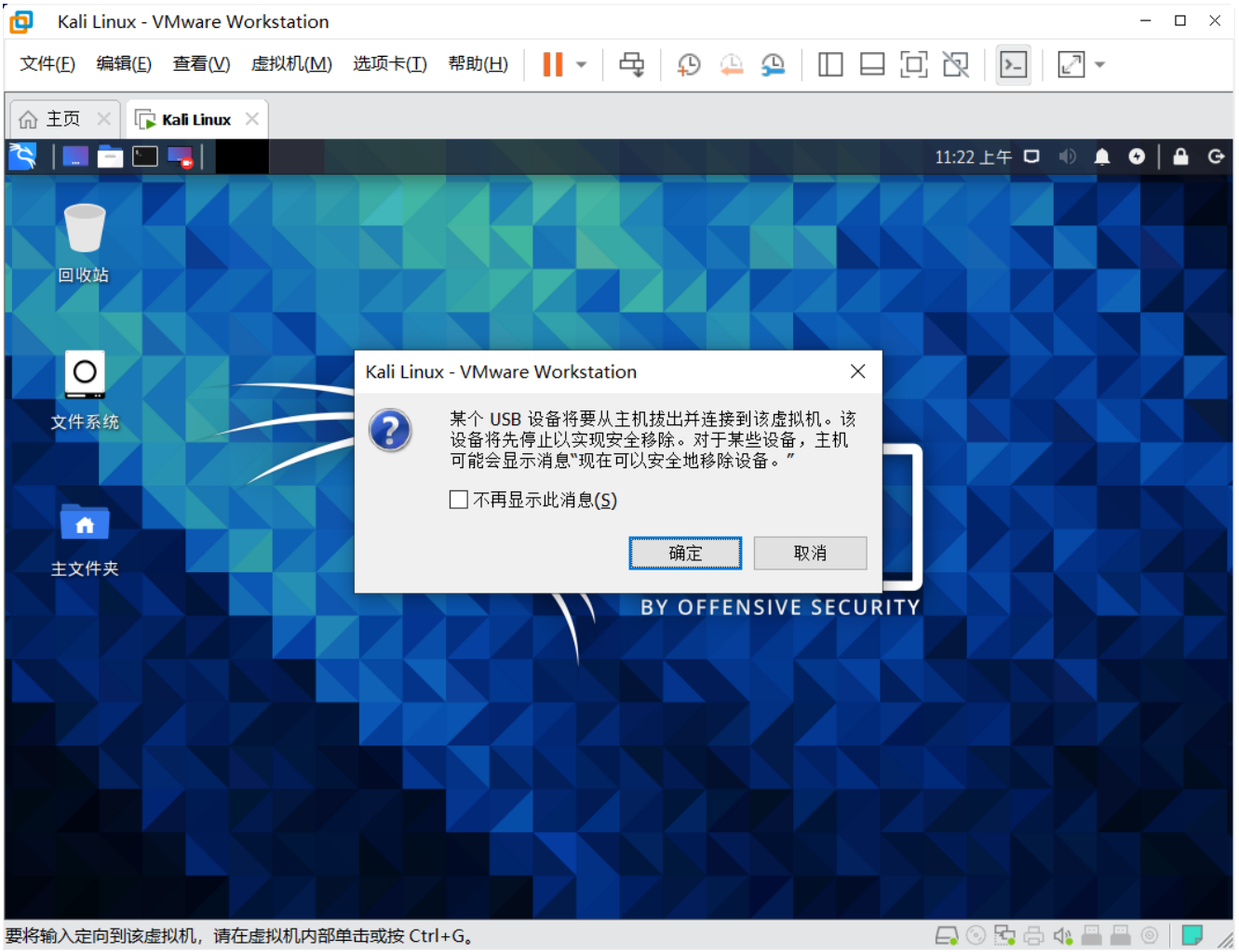
Aircrack-ng可以工作在任何支持监听模式的无线网卡上（设备列表请参阅其官方网站）并嗅探802.11a，802.11b，802.11g的数据。

回到顶部

4、WIFI破解教程

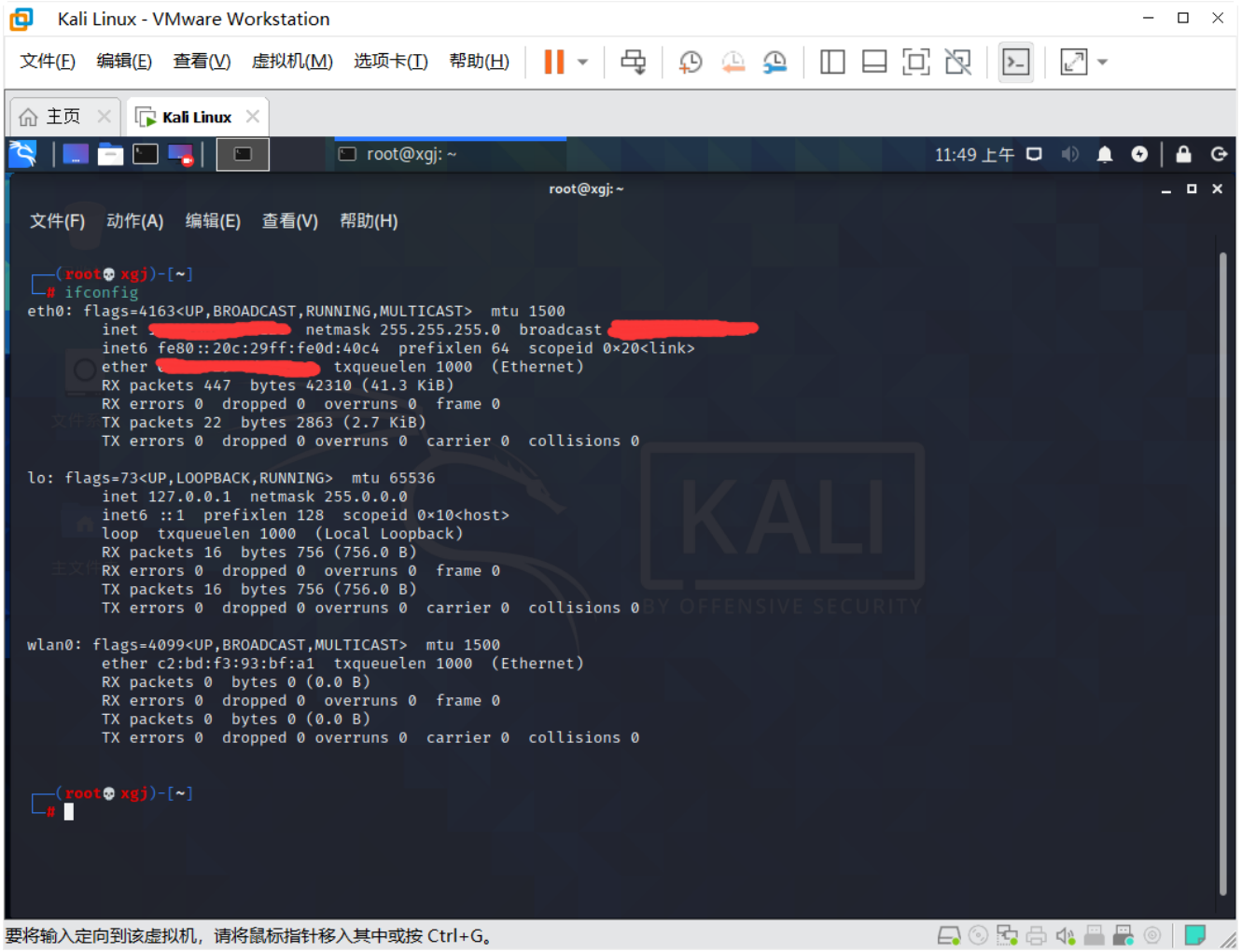
4.1、插上无线网卡，点击“虚拟机”→“可移动设备”→选中你的无线网卡→“连接（断开与主机的连接）”，在弹出的对话框中点击“确定”，如图所示。





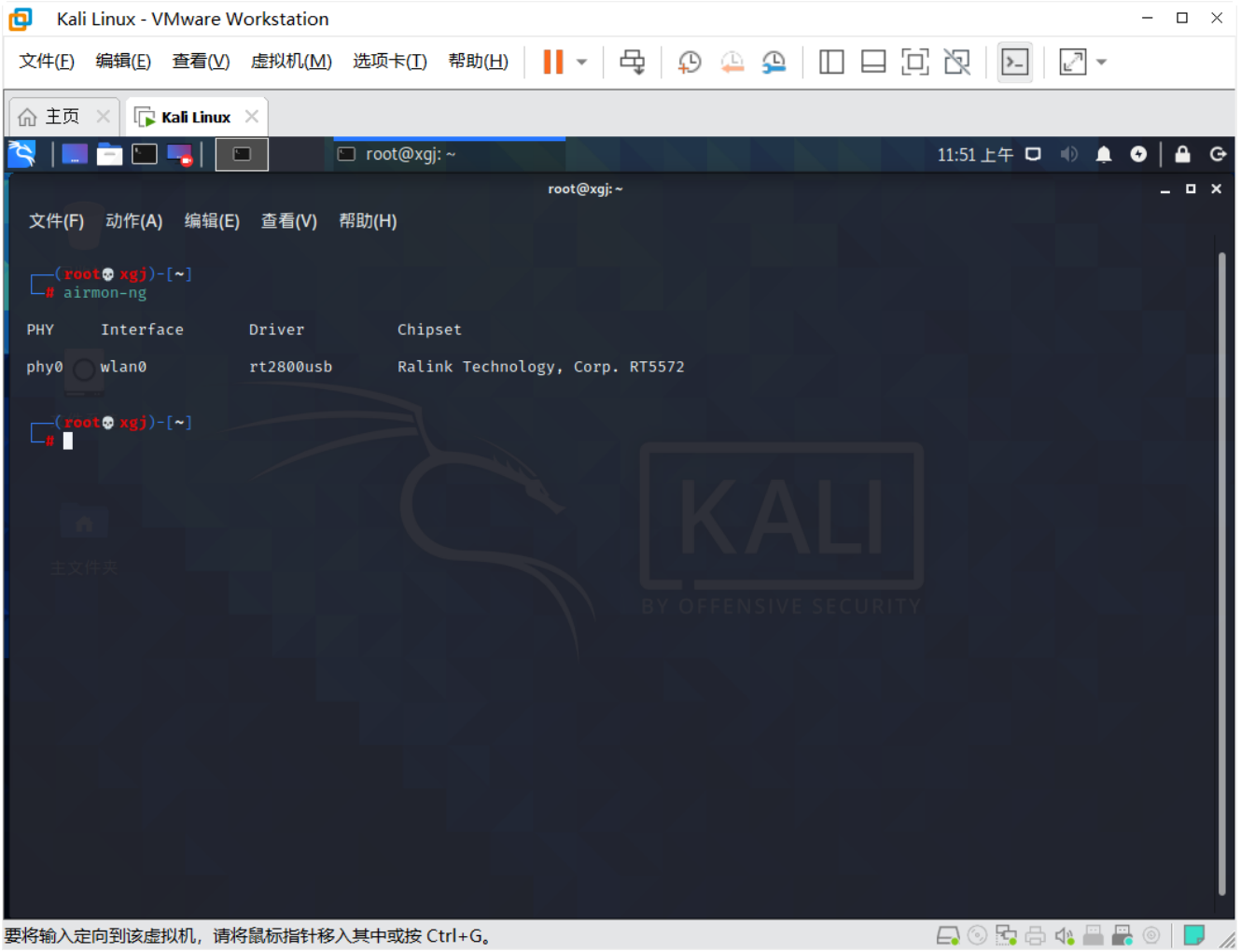
4.2、查看你的网卡信息

使用 `ifconfig` 命令查看网卡信息。可以看到里面有个wlan0，那就是我的无线网卡，如果没有的话就把无线网卡拔了再插一下，直到出现wlan0为止。一定要保证它现在没有连接到任何wifi，wlan0里面没有ip地址什么的，就说明未连接任何WIFI。



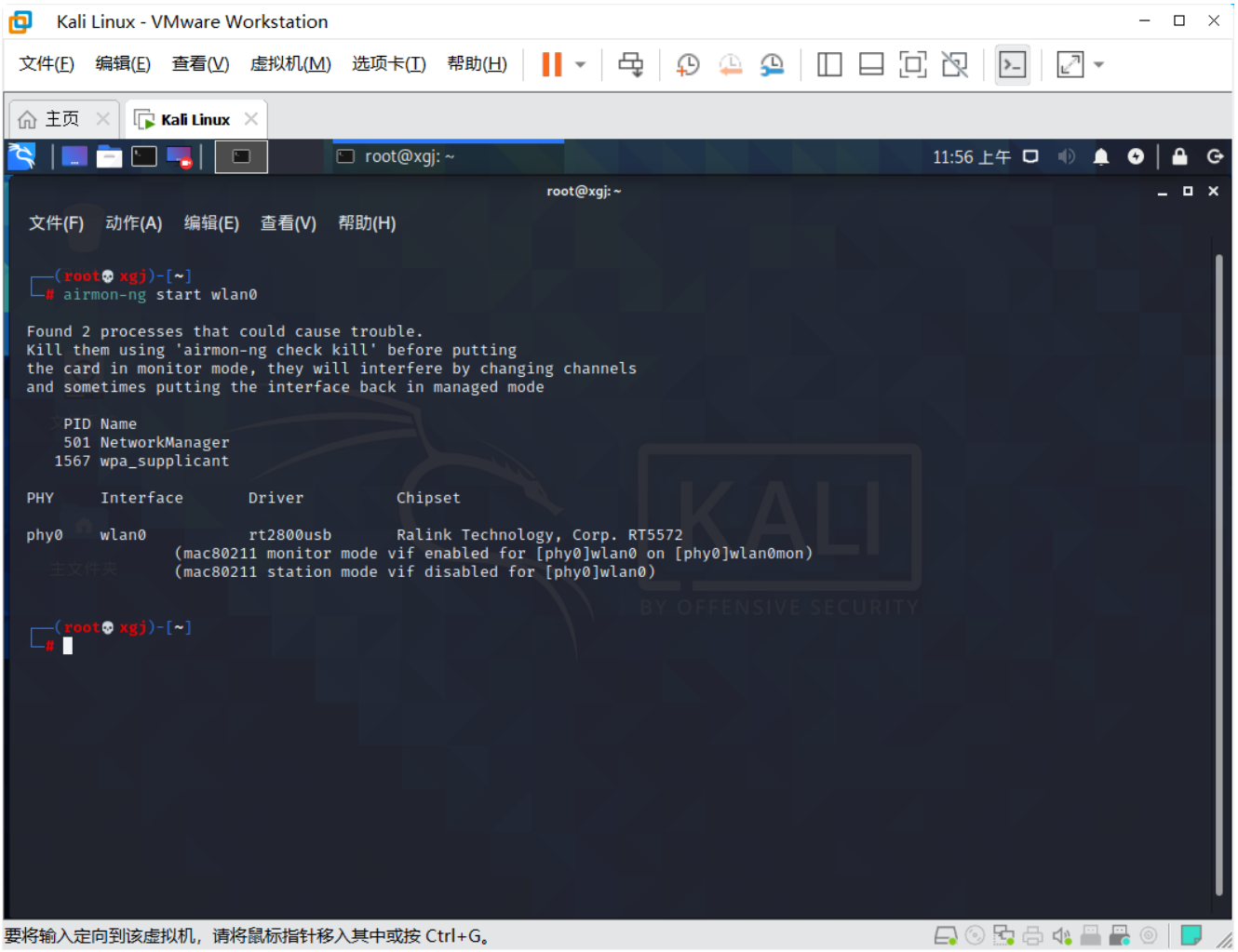
4.3、检查网卡是否支持监听功能，如图所示。

使用 `airmon-ng` 命令检查网卡是否支持监听功能。这里显示可以看到无线网卡wlan0，即代表支持监听模式的。（没有显示则代表没有可以支持监听的网卡）

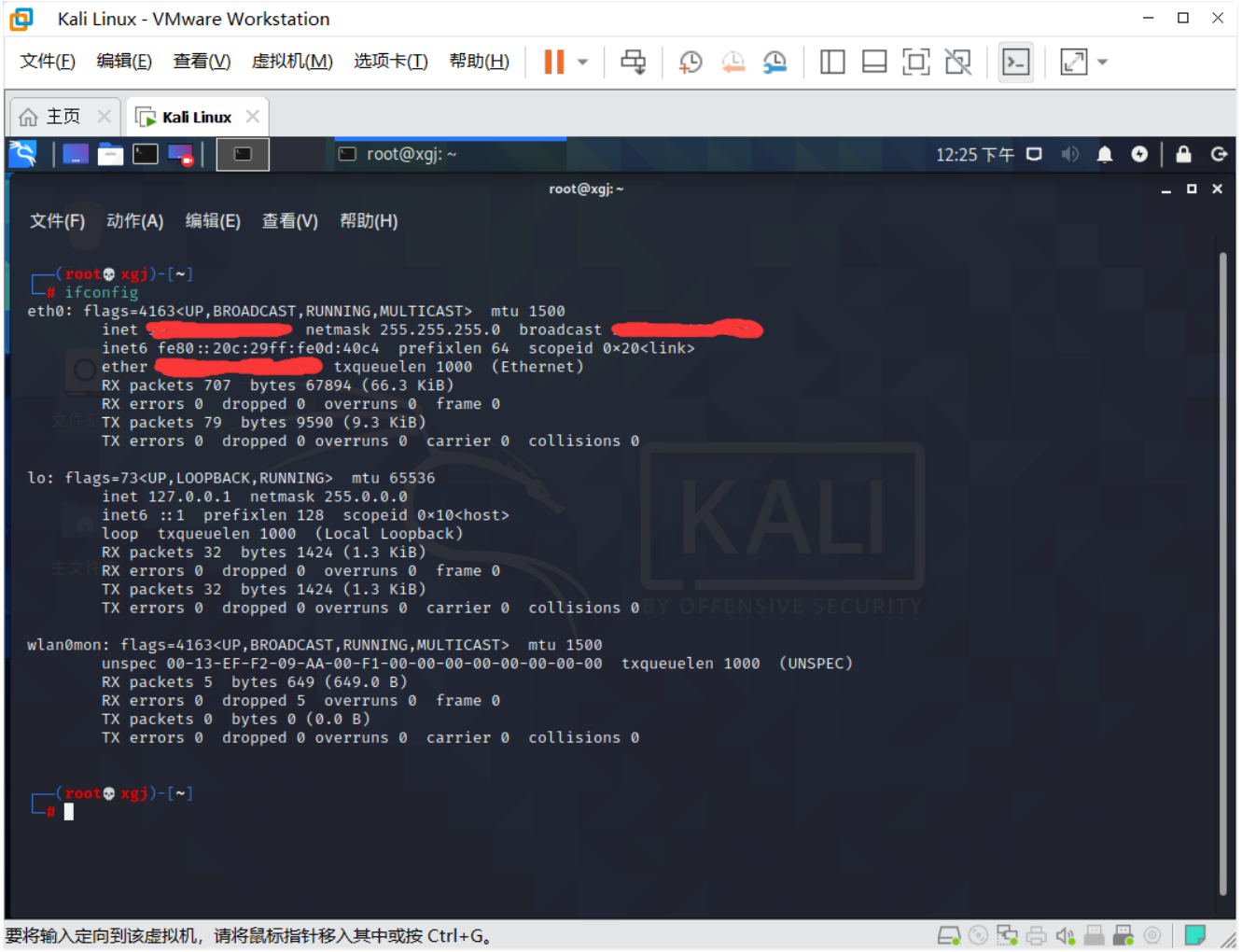


4.4、激活无线网卡，开启网卡的监听模式。

使用命令 `airmon-ng start wlan0` 激活无线网卡至monitor即监听模式。

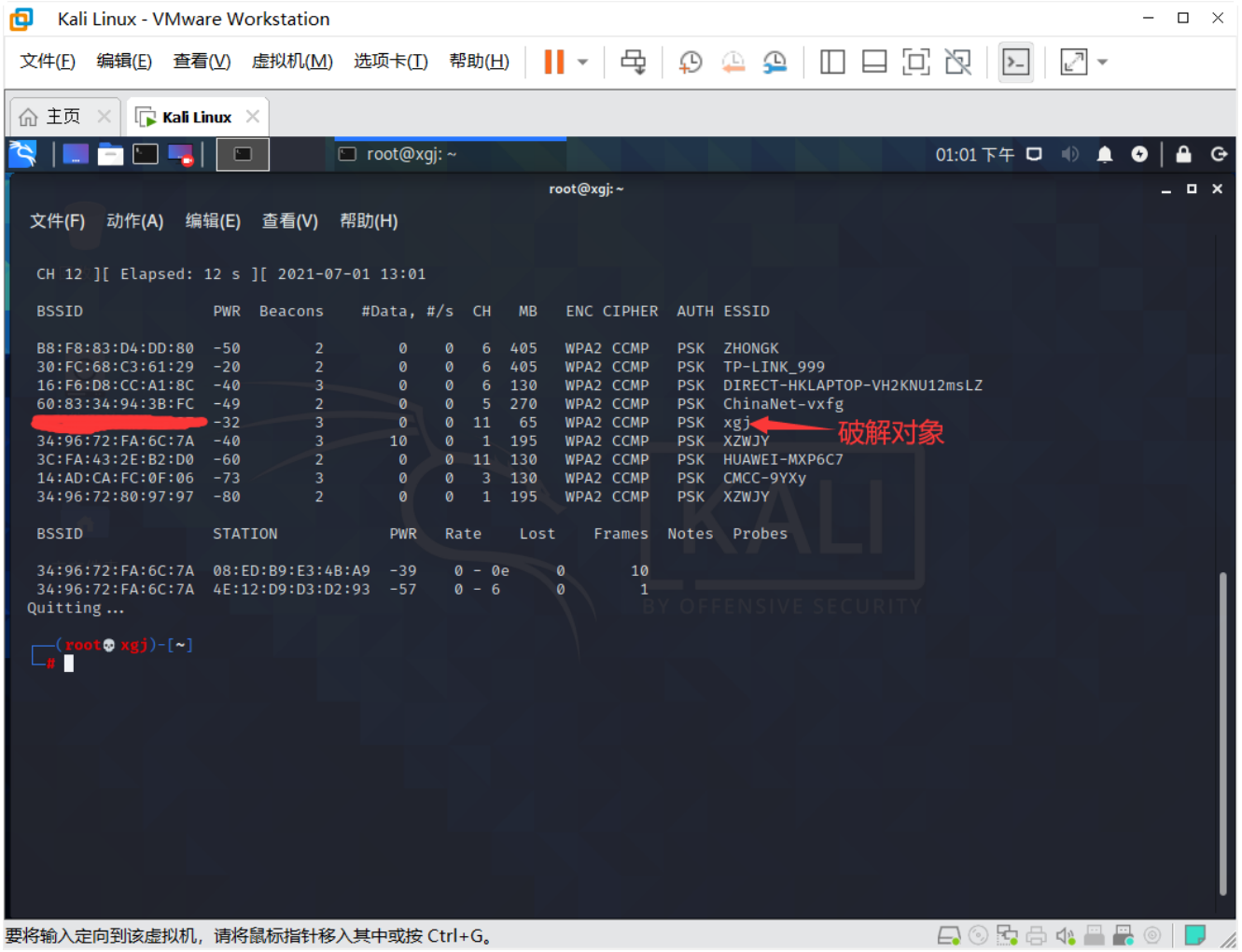


再次使用 `ifconfig` ，可以发现无线网卡已经被重命名为wlan0mon。



4.5、扫描当前环境中WIFI信号

使用 `airodump-ng wlan0mon` 获取当前网络概况。当搜索到我们想破解的WIFI时，按Ctrl+C停止搜索。



4.6、探测无线网络，抓取无线数据包。

具体命令如下：`airodump-ng -c 11 -w qwer wlan0mon`，按Enter开始执行。

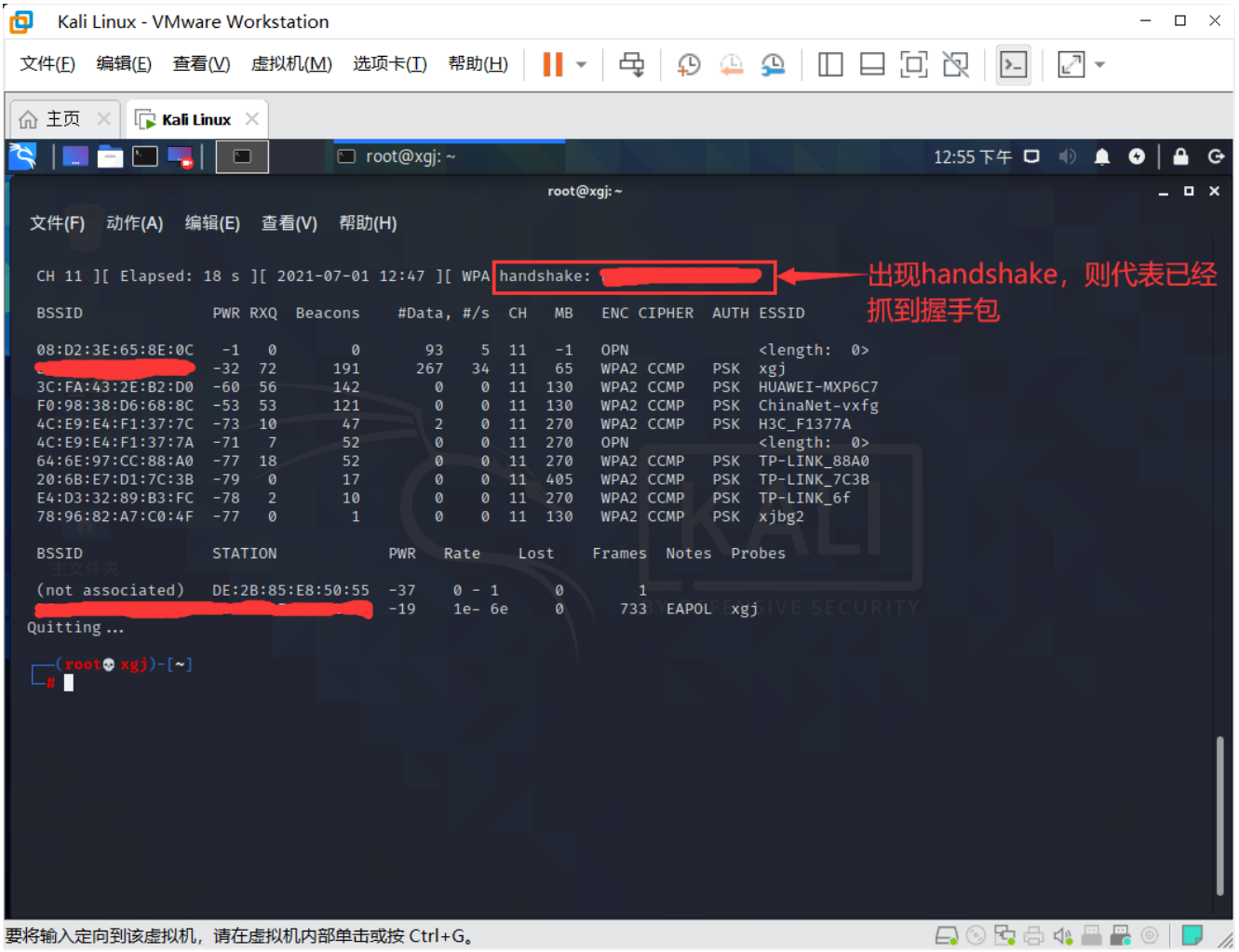
参数解释：

-c 设置目标AP的工作信道。

-w 后面紧跟要保存的文件的文件名，注意：生成的文件名是qwer-01.cap，后面破解密码时需要用到文件名。

wlan0mon：为之前已经开启监听的网卡名。

在右上角出现handshake的提示证明获得了包含WPA-PSK密码的4次握手数据报文。



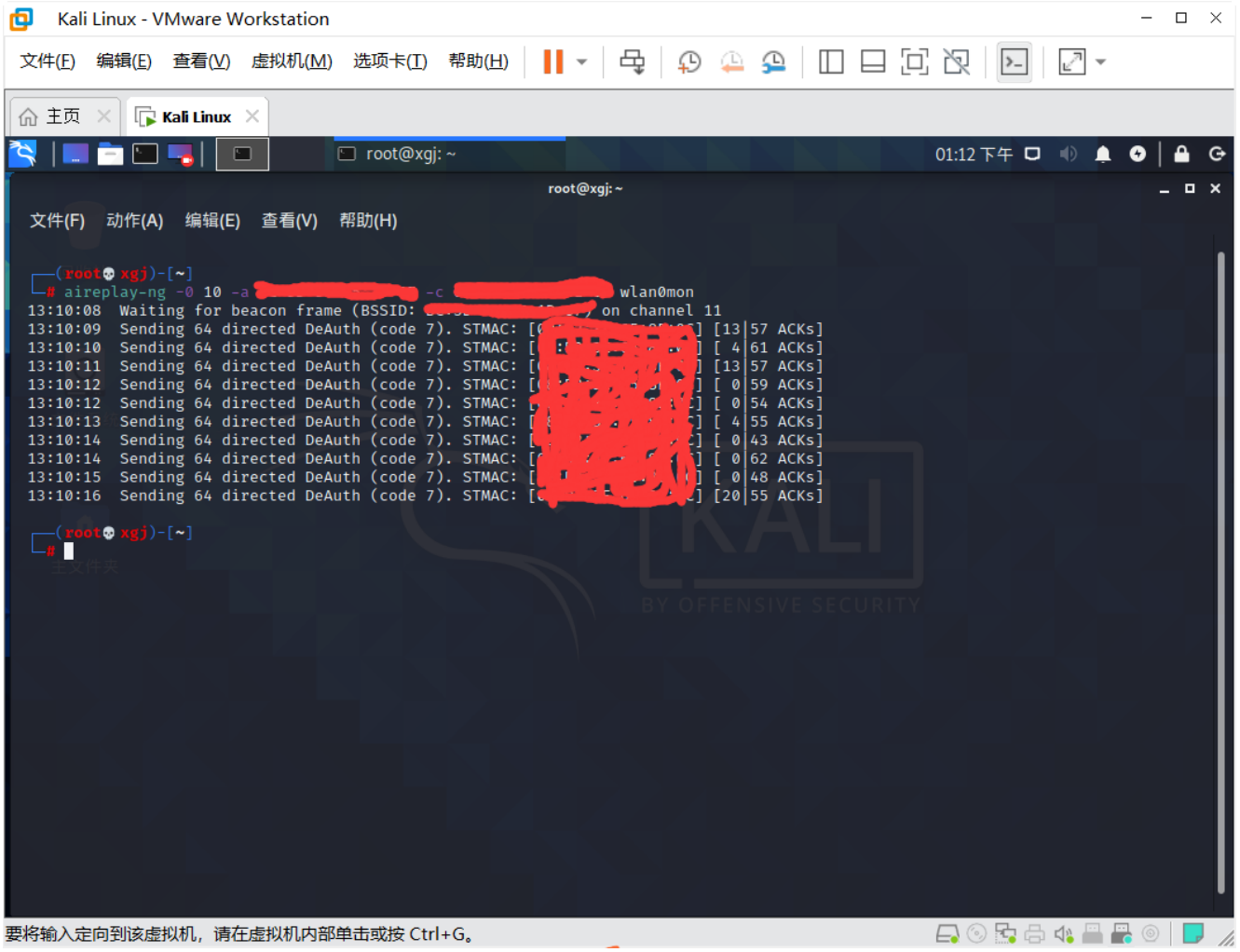
如未出现，进行deauth攻击加速破解过程，不要关闭当前shell，打开另一个shell进行下一步，输入命令：`aireplay-ng -0 10 -a AP的MAC -c 客户端的mac wlan0mon` 注意如果抓不到握手包就把对方踢下线，这样就会抓包成功

参数解释：

-0：采用Deauth攻击模式，后面紧跟攻击次数，这里设置为10，大家可以根据实际情况设置，如果设置为0，则会导致对方一直掉线。

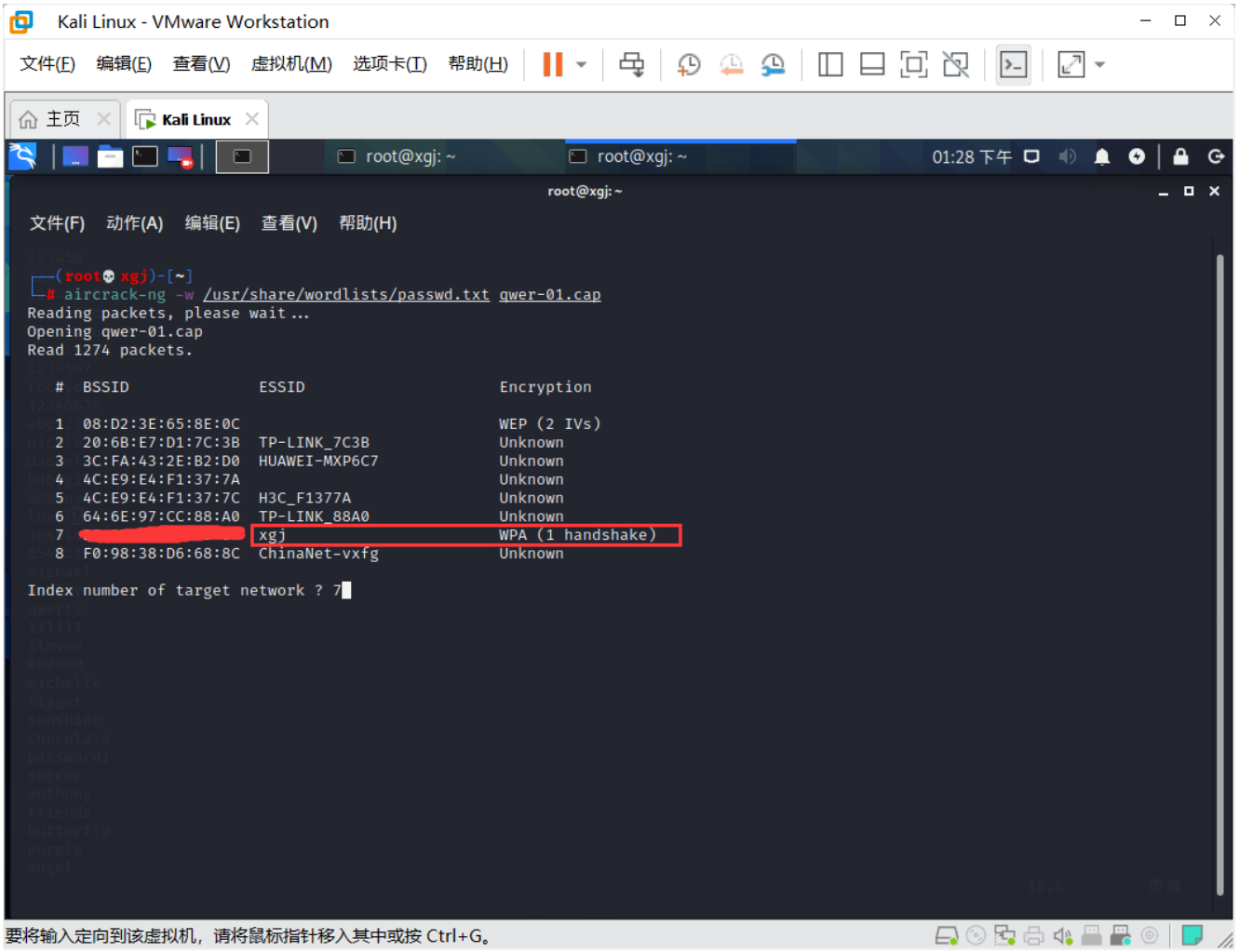
-a：后面跟AP的mac地址。

-c：后面跟客户端的mac地址。



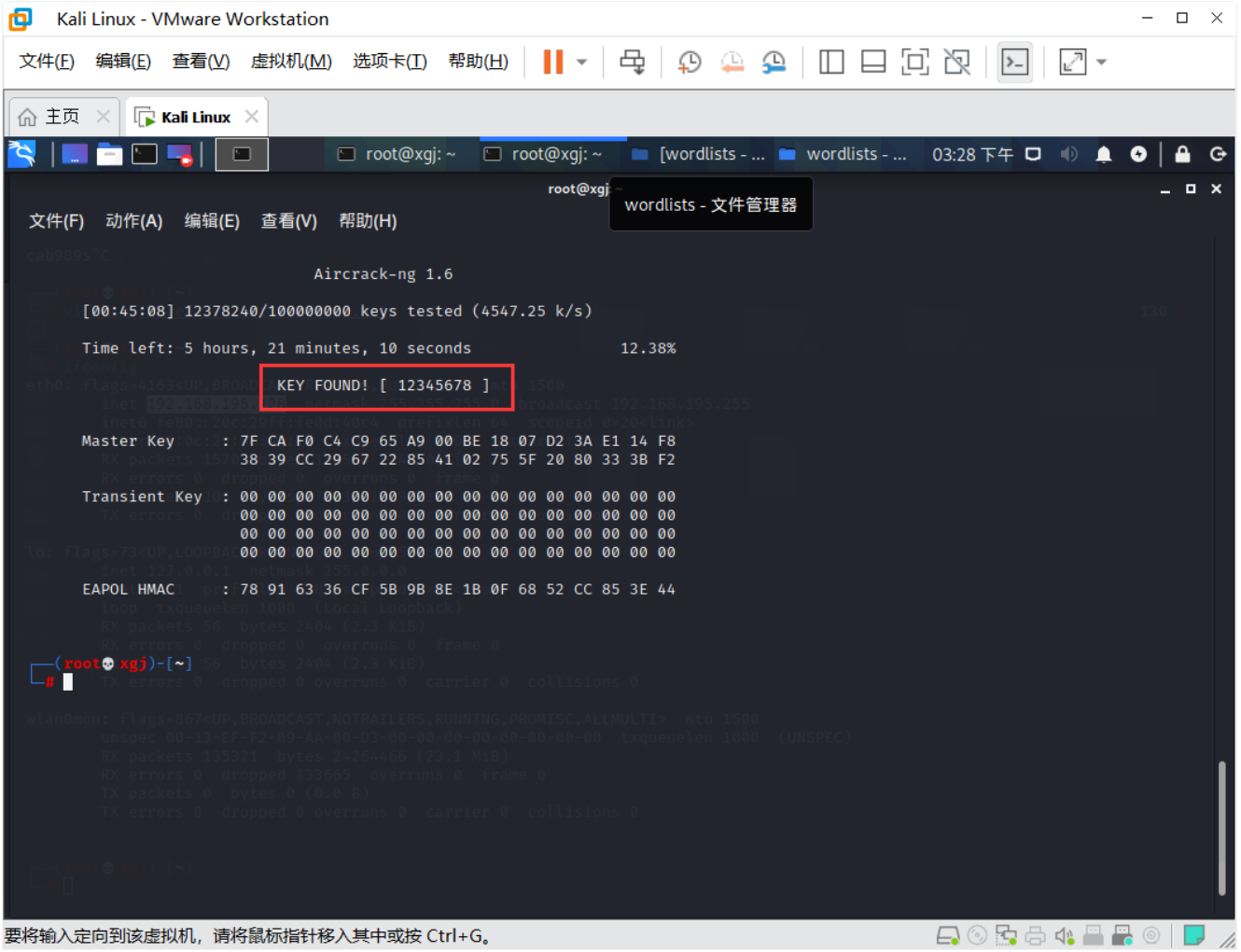
4.7、破解WIFI握手包。

使用命令：`aircrack-ng -w 密码字典的路径 捕获的.cap文件`，按Enter开始执行。之前抓到的握手包会显示在内，选择7，按Enter进行破解。



开始进行密码破解，能否成功破解WIFI密码取决于密码字典本身是否包含了这个密码，破解的时间取决于CPU的运算速度以及密码本身的复杂程度。

KEY FOUND！便是破解成功，密码就是[]里面的值。



技术让生活更美好。

分类: 技术类

好文要顶 关注我 收藏该文

BK小君
粉丝 - 6 关注 - 0
+加关注

1 推荐

0 反对

posted @ 2021-07-01 15:33 BK小君 阅读(12102) 评论(2) 编辑 收藏 举报