

# Bugku CTF 每日一题 想蹭网先解开密码

原创

彼岸花苏陌 于 2022-02-03 14:23:40 发布 2342 收藏

分类专栏: [ctf](#) 文章标签: [安全](#) [网络](#) [ctf](#) [wifi](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_42263820/article/details/122775645](https://blog.csdn.net/qq_42263820/article/details/122775645)

版权



[ctf 专栏收录该内容](#)

39 篇文章 1 订阅

订阅专栏

## 想蹭网先解开密码

学到了新知识和新工具

下载下来是个cap文件 用wireshark打开

由题目得知是wifi的文件, 上网学习了一下 wifi的四次握手协议

用eapol搜索wireshark中的文件 确实存在四个包

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

No.	Time	Source	Destination	Protocol	Length	Info
3066	45.138762	D-LinkIn_9e:4e:a3	LiteonTe_68:5f:7c	EAPOL	155	Key (Message 1 of 4)
3068	45.154148	LiteonTe_68:5f:7c	D-LinkIn_9e:4e:a3	EAPOL	155	Key (Message 2 of 4)
3070	45.168458	D-LinkIn_9e:4e:a3	LiteonTe_68:5f:7c	EAPOL	213	Key (Message 3 of 4)
3072	45.195620	LiteonTe_68:5f:7c	D-LinkIn_9e:4e:a3	EAPOL	133	Key (Message 4 of 4)

CSDN @彼岸花苏陌

题目中又有提示要我们猜后面四位

所以了解wifi破解方法后 可以用cap文件加密码文件组合的方式暴力破解

于是有两种方式, 一种是kali下的aircrack, 第二种是windows下的EWSA

1.aircrack

首先得构建出11位的手机号码密码

因为只用猜后面四位, 所以可以用python写脚本或者用字典生成器, kali下用crunch生成字典即可

这里给出crunch的命令

```
crunch 11 11 +0123456789 -t 1391040%%%% >>tt.txt
```

11 11就是最小11位, 最大11位

+0123456789

设定暴力的范围

% 代表插入数字

最后一段代表输出到tt.txt文件中

然后用aircrack命令

```
aircrack-ng -w tt.txt wifi.cap
```

即可破解密码

```
root@kali: ~/文档
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~/文档# aircrack-ng -w tt.txt wifi.cap
Opening wifi.cap please wait...
Read 4257 packets.

#主 BSSID          ESSID          Encryption
1 3C:E5:A6:20:91:60 CATR           No data - WEP or WPA
2 3C:E5:A6:20:91:61 CATR-GUEST    None (10.2.28.31)
3 BC:F6:85:9E:4E:A3 D-Link_DIR-600A WPA (1 handshake, with PMKID)

Index number of target network ? y
Opening wifi.cap please wait...
Read 4257 packets.

1 potential targets

Aircrack-ng 1.5.2

[00:00:04] 9904/9999 keys tested (1983.37 k/s)

Time left: 0 seconds 99.05%

KEY FOUND! [ 13910407686 ]

Master Key      : 0C 2F 14 10 BF 71 7E 40 DD AB 64 93 73 60 6C 4F
                  5B 75 61 20 2A 10 57 E4 6D D6 59 C8 2C 49 B3 4C

Transient Key   : BF F2 72 59 E8 37 FA A0 F6 A0 EF 02 AA 8E D5 DC
                  0C B6 1B 6C 53 AE 36 60 FF 98 0E D2 8A 95 13 EF
                  BC 21 34 03 19 EC FD 3C 9D 8B D1 7A C8 64 B4 72
                  DC E8 A3 8B B1 0E D5 69 0F 63 E8 32 19 77 2D BF

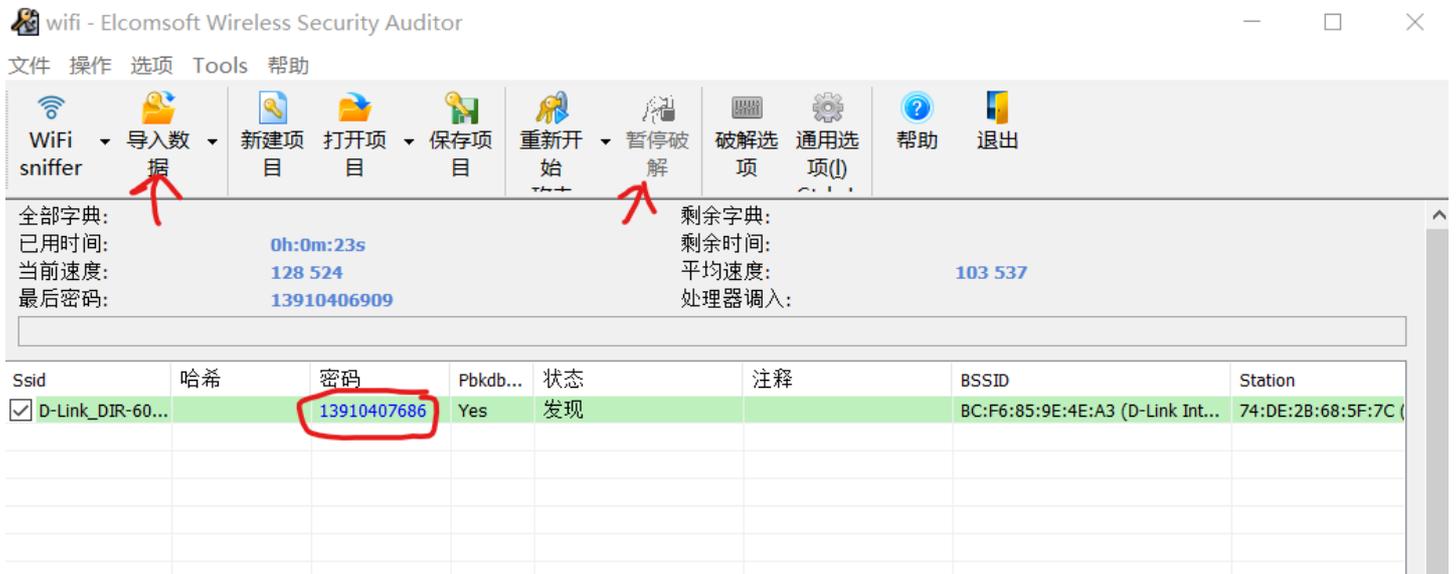
FAPQI HMAC      : 98 0B 1F 76 AD BF 7D 77 4A D9 84 15 DB 1A A4 24
```

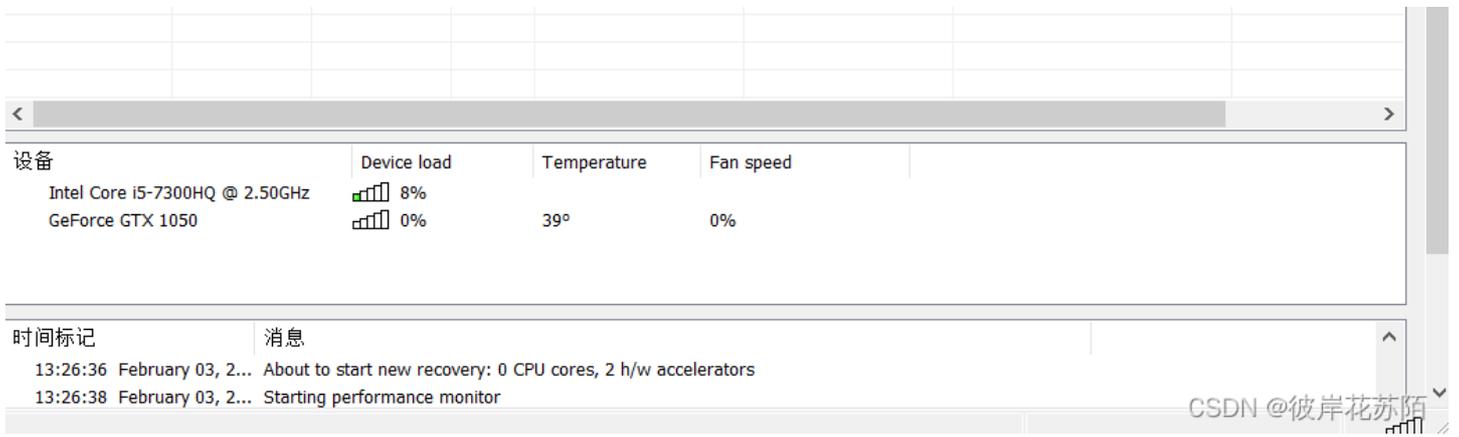
## 2.EWSA

新工具 先下载破解掉后

导入数据->导入TCPDUMP文件->把cap文件放入

点击破解 放入字典文件 点即破解即可





学到了新东西，改天试试抓下家里的wifi包破解下