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

本文链接：https://blog.csdn.net/qq_42263820/article/details/122775645

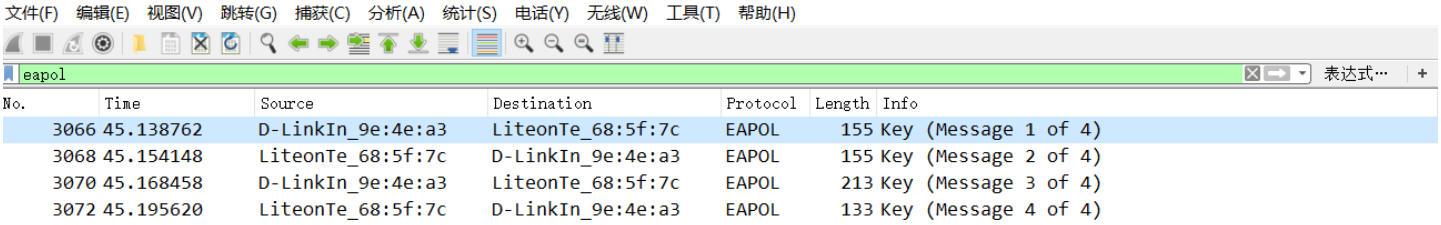
想蹭网先解开密码

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



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

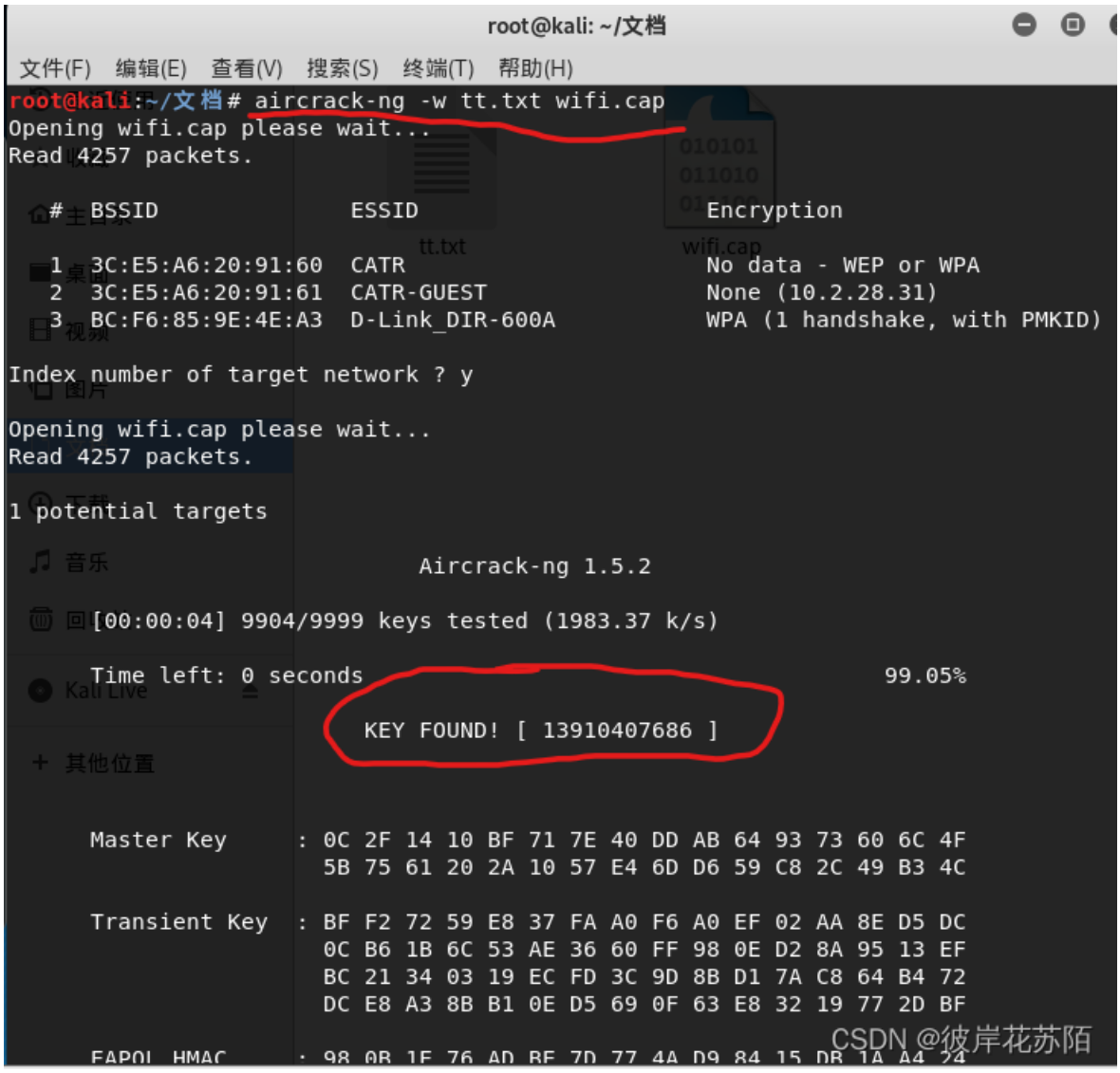
% 代表插入数字

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

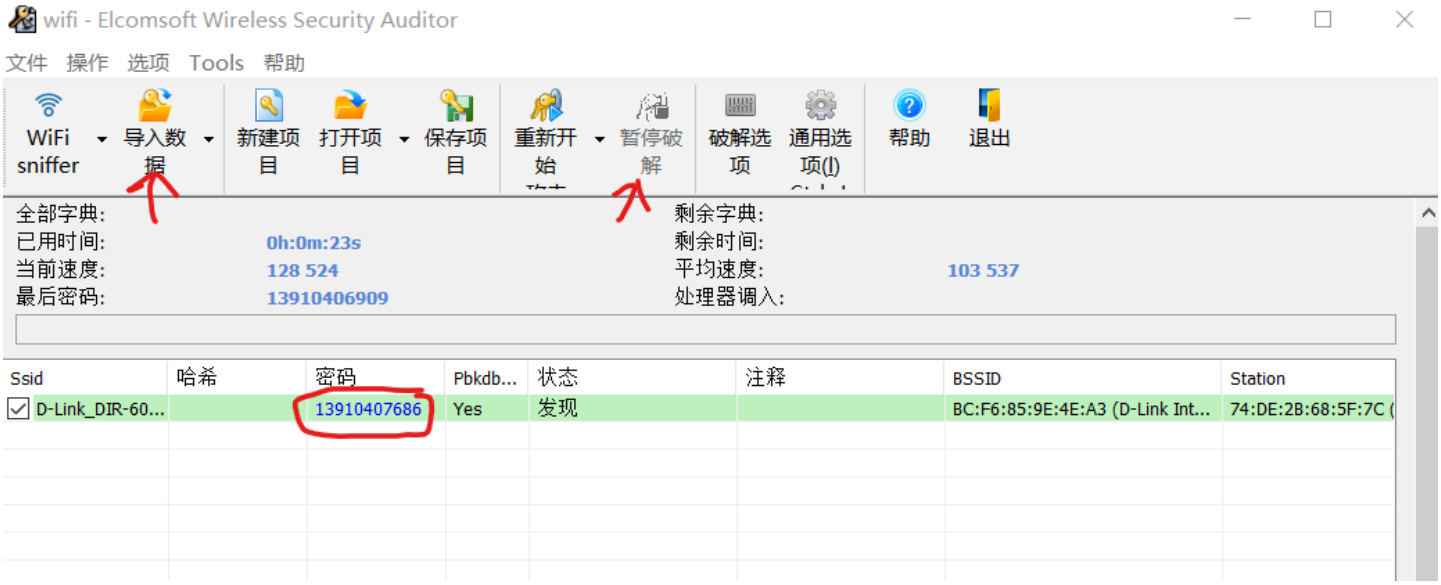


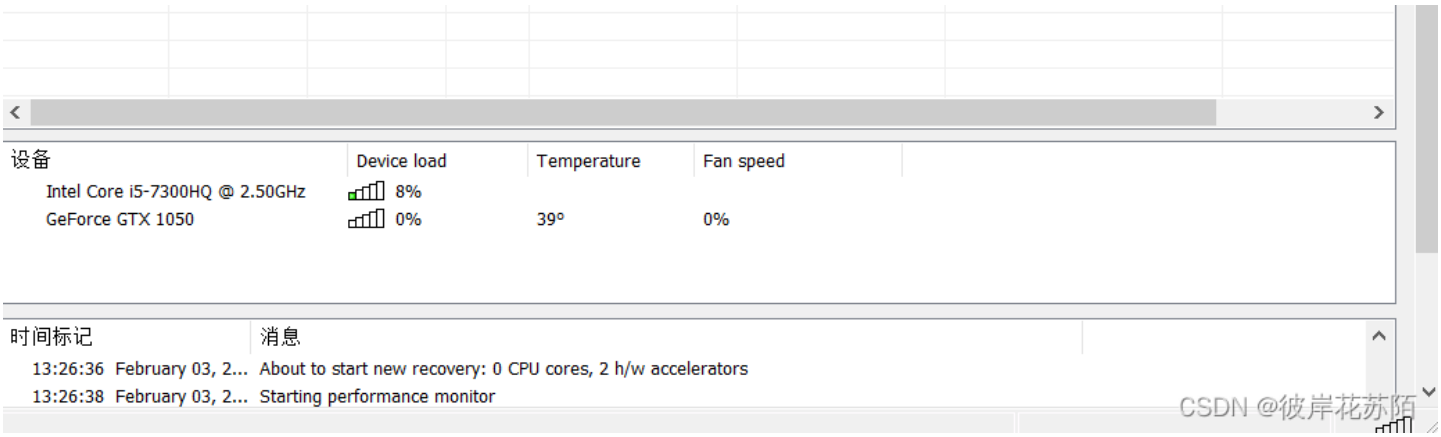
2.EWSA

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