2021年春秋杯网络安全联赛秋季赛 传说殿堂赛道misc部分writeup

原创

是Mumuzi 于 2021-11-28 00:00:00 发布 6421 收藏 4

分类专栏： ctf 文章标签： 网络安全 信息安全

本文链接：https://blog.csdn.net/qq_42880719/article/details/121582376

队伍属性： 全部 高校 企业 社会参赛人员 输入队伍名称查询

排名	队伍名称	学校/单位名称	队伍属性	总分	与前一名分差	队伍强项	攻克题目数	一血数量	状态
1	T**d	保密	社会参赛人员	2449	0	Reverse	6	2	正常
2	o**1	AHDX	企业	1934	515	Reverse	5	1	正常
3	喵**搭	中山大学	高校	1215	719	Crypto	3	2	正常
4	4**r	成都七中	高校	1150	65	Web	3	2	正常
5	t**t	长沙职业技术学院	高校	1115	35	PWN	2	1	正常
6	你喜欢击剑还是PY	四川警察学院	高校	1004	111	Misc	3	1	正常
7	c**k	华南师范大学	高校	988	16	Misc	3	0	正常
8	h**o	hello	社会参赛人员	955	33	Misc	3	1	正常
9	N**N	浙江经济职业技术学院	高校	610	345	PWN	2	1	正常
10	Y**Y	个人	社会参赛人员	590	20	Web	2	1	正常

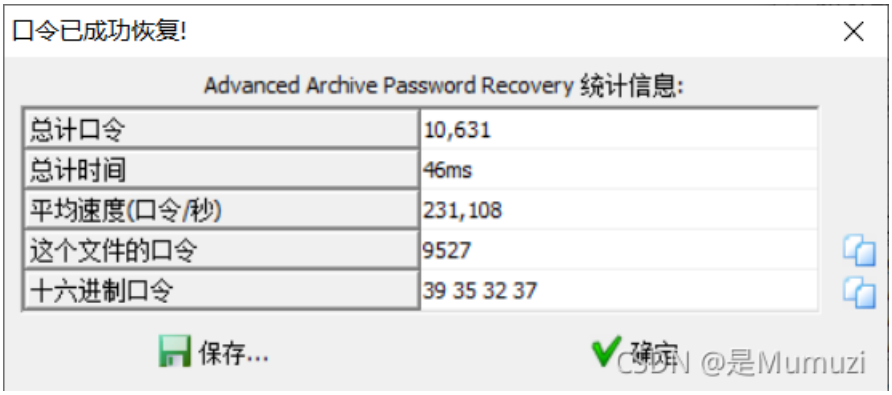
Misc

问卷调查

略

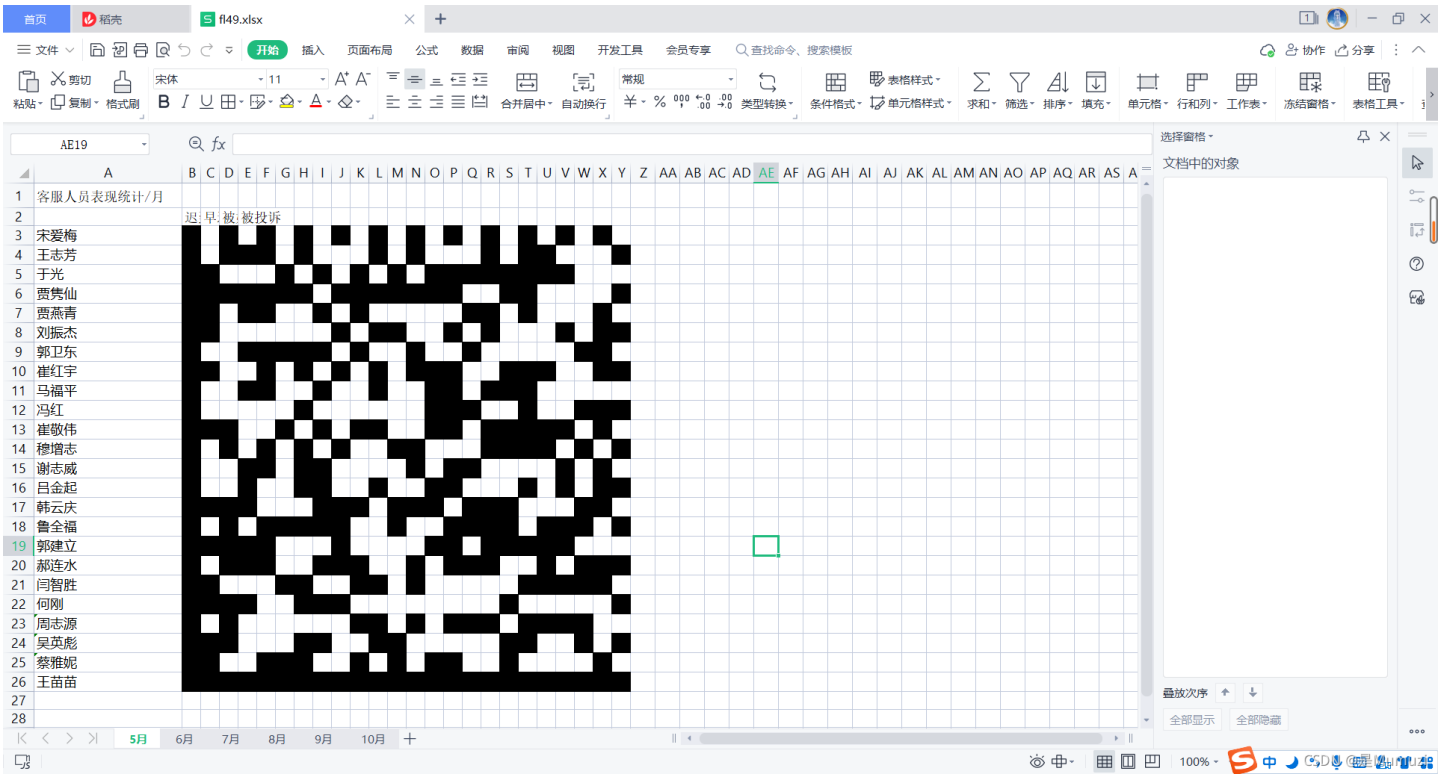
secret_chart

解压出来一张图片，图片后面有个ZIP，手动分离出来之后去看图片发现没有LSB，准备去爆破一下然后就被我爆出来了

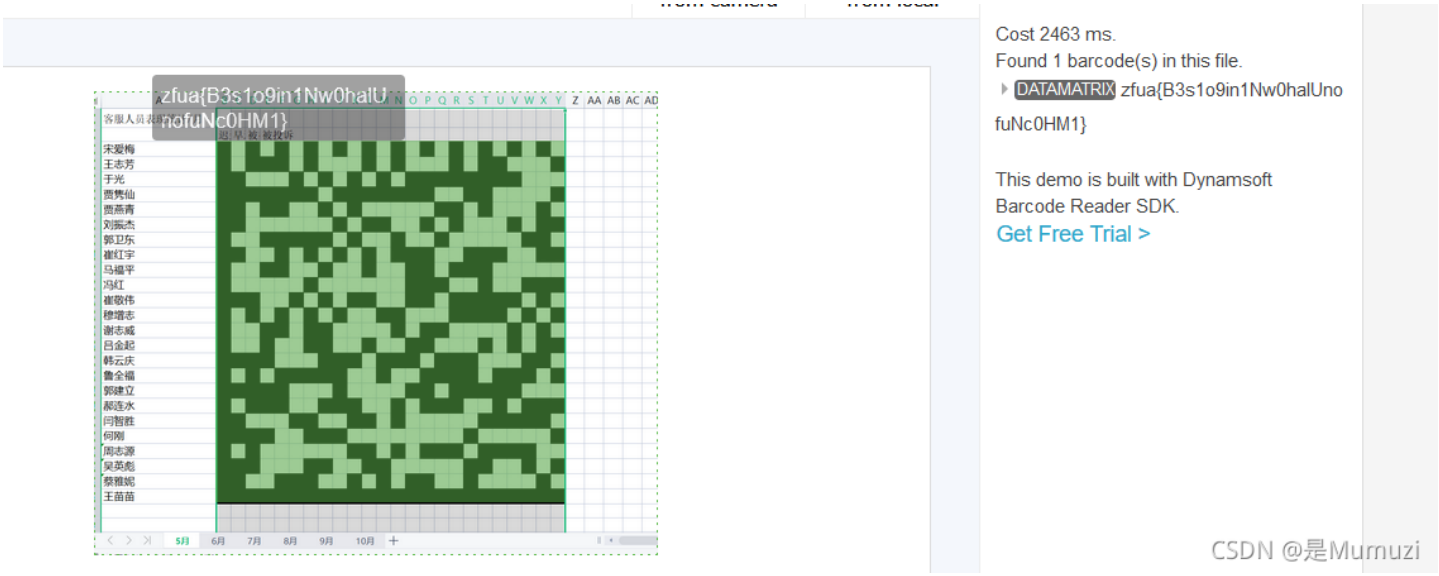


解压之后发现还真是chart，发现表格是由6个月份构成的，于是乎第一反应就是把题拼起来，结果发现左侧和底边都是1

直接猜二维码了，为其添加个条件格式，字符串包含1的时候背景为黑色，然后把列宽统一一下，如图



太Data Matrix了



rot13 偏移6（凯撒20）即可得到flag

```
flag{H3y1u9ot1Tc0ngrAtulaTi0NS1}
```

ezchat

最后找到flag的那一刻！太舒服了！题目其实本身并不难，问题应该是出在我太菜了

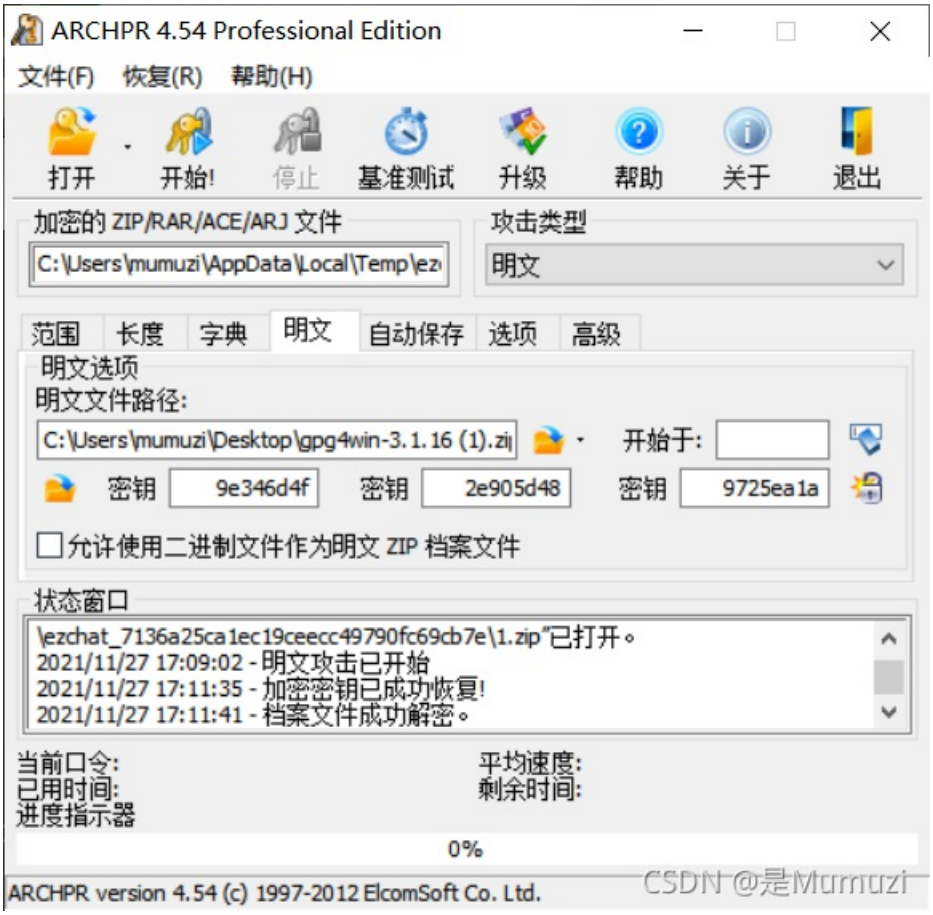
首先能观察到irc流1和流2分别是站在alice和bob的视角来看的，在交谈中，他们说密码是用的约定好的密码，就这个问题困扰了许久

因为在第3个流里面可以发现传输了一个zip，当然保存原始数据的时候要选择这个对话

```
fd47:67ac:60f9::19b:1026 → fd47:67ac:60f9::67a:42706 (30MB)
```

导出来之后一直是在找密码，但是没有找到

最后还是从gpg4win-3.1.16下手，因为都有这个文件，且已知压缩方式是zip标准压缩。就去官网下载一个gpg4win-3.1.16进行明文爆破

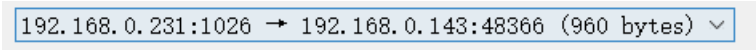


打开之后，有个txt是他们的操作过程

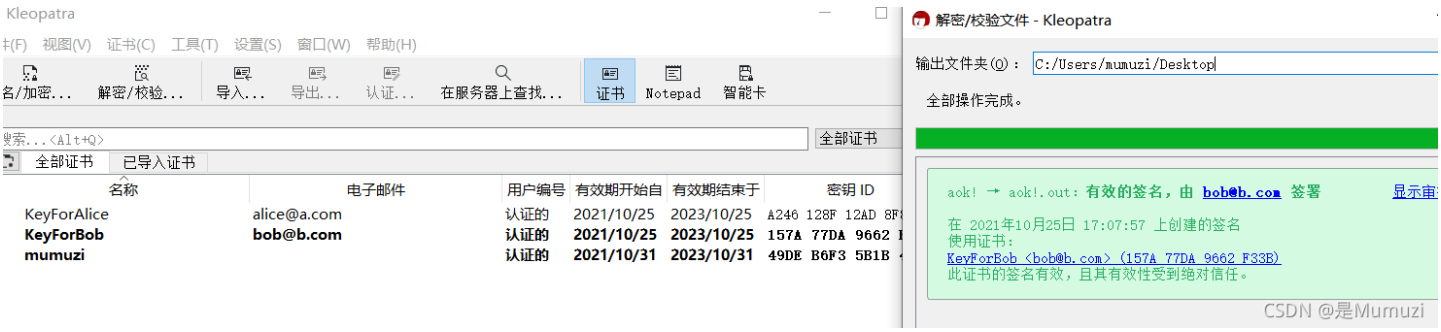
```
First, run gpg4win-3.1.16.exe, follow the default steps install it.
Then, open "Kleopatra" on desktop.
Import "bob_secret_key.txt" and "alice_public_key.txt", certify it.
Encrypt your flag.txt. (Don't forget to select "encrypt for others" and add Alice)
Send the encrypted file to me.
```

于是安装好软件之后导入alice和bob的秘钥

导出之后现在就差密文了，发现还有tcp的第5个流和第6个流没用到，于是都选择



将其放入文件解密



解密成功之后生成aok!.out文件，打开就是flag

```
flag{a2449a02-975b-4b25-ad44-3157c3fcb571}
```