DMCTF部分题目writeup

原创

凉彧LEM 于 2020-11-29 17:49:37 发布 621 收藏

分类专栏： CTF菜鸡wp

本文链接：https://blog.csdn.net/qq_51429131/article/details/110340393

DMCTF部分题目writeup

文章目录

首先说明本蒟蒻是大一菜鸡，刚刚入门CTF，啥也不会，就凭着Google硬搜硬写，混了些许分数

大部分题都能在网上找到类似的题目或者相应的轮子，跟着先辈们一步一步就能混到些许分数

这些writeup是我个人的写法，如果有更好的更绝妙的写法请大佬手下留情，希望大佬们不吝赐教|·ω·`)

一、Reverse

就做了一道题，我太菜了，真的还有写wp的必要么（悲）

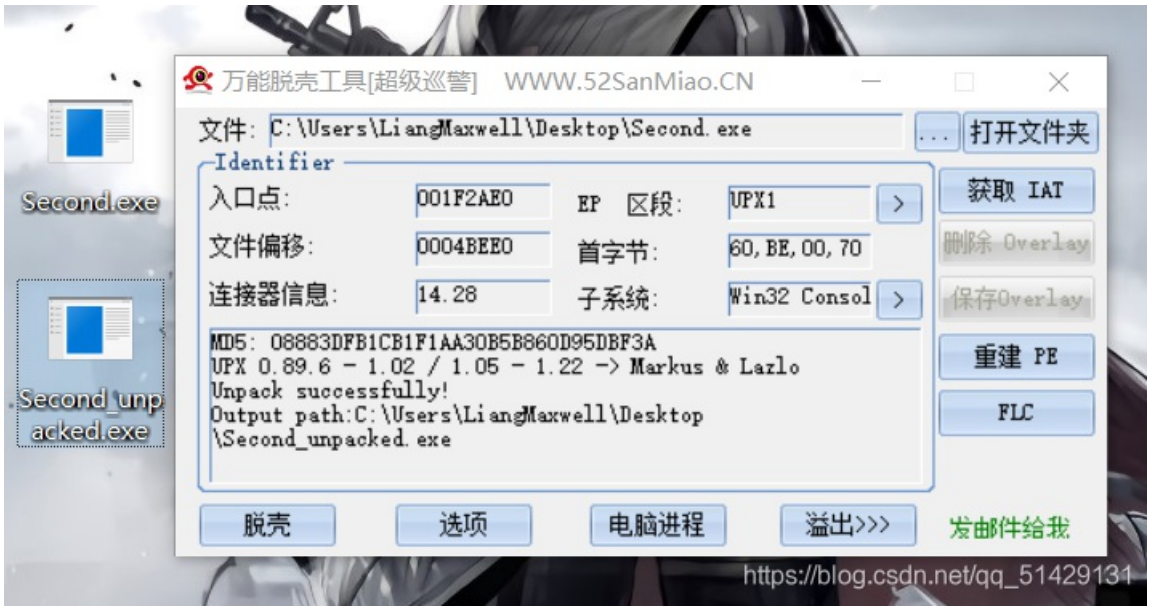
_(:3」∠).

题目是second.exe

1.首先放进exeinfope里面看一下，可以发现程序有壳，32位

2.在网上可以轻松找到脱壳工具，这里使用的是File Format Identifier v1.4，拖进去后得到新的无壳程序

（当然大佬可以直接OD一路找到程序入口）



3.这时候启动无敌的IDA，直接反编译

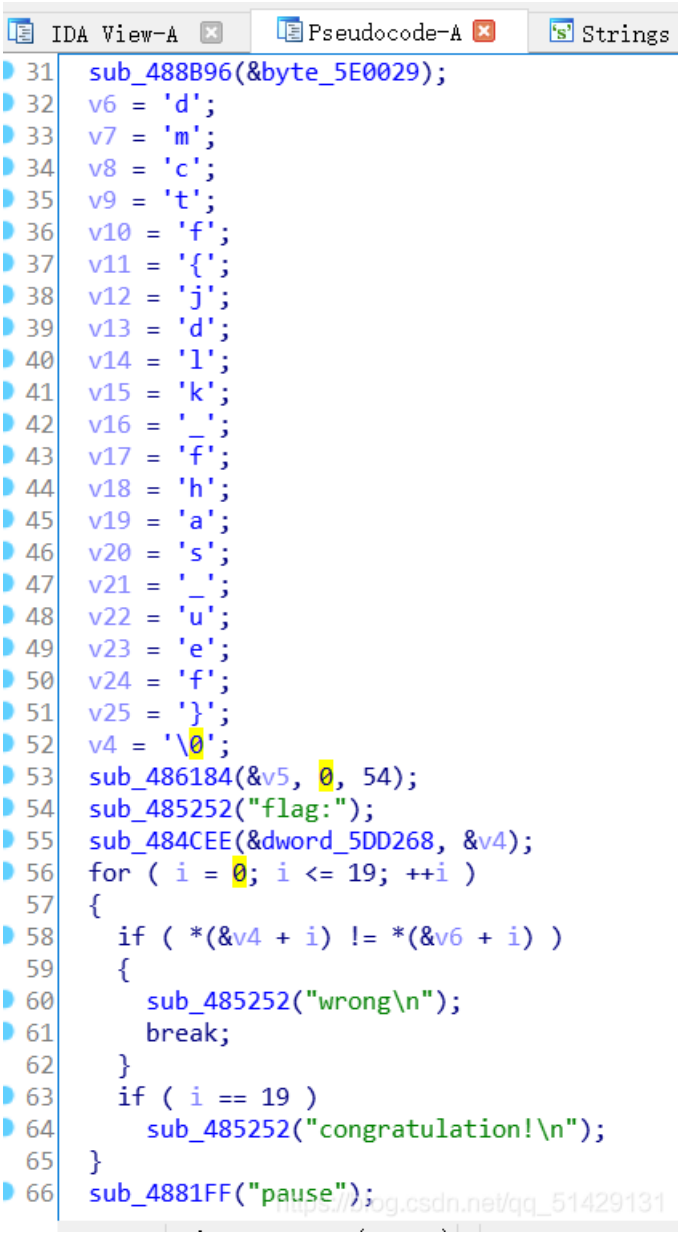
4.shift+F12打开字符串窗口

可以找到congratulation这一句话

双击打开，CTRL+X打开，F5进入伪代码界面

5.可以看到上面一大串V1V2的字符

通过R键将其转化成字符，拼起来得到dmctf{jdlk_fhas_uef}即为flag



然后其他的题就不会做了，easymaze那题的flag函数也太复杂了吧qwq

二、Web

整了两道web,PHP那一题挑战失败，从来没学过web干拉太难了，球球大佬带带孩子吧_(:з」∠).

1. weak type

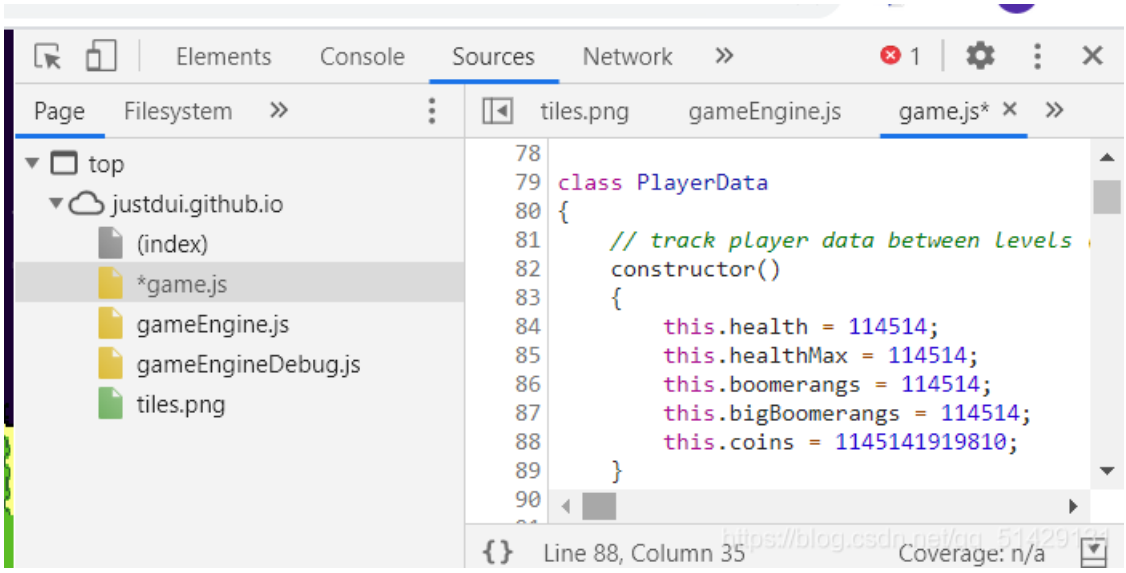
通过标题可以猜出来是PHP的弱类型

1. 阅读代码，构造合适语句，这次使用的是?num=0xc0a94b4&v1=s878926199a&v2=s155964671a，将其添加到网页地址后面
2. 过来level1和level2，在网上可以了解到相关工具是hackbar，启用
3. post message={“key”:0}，在网页最下方可以得到flag

2. fungame

启动游戏后，F12打开源文件

在game.js里面84行修改血量，武器，金币，然后一路乱杀，通关最后一关拿到flag



还可以直接跳关，不过好像会因为设备的问题而卡死？还是一关一关虐杀过去爽一些

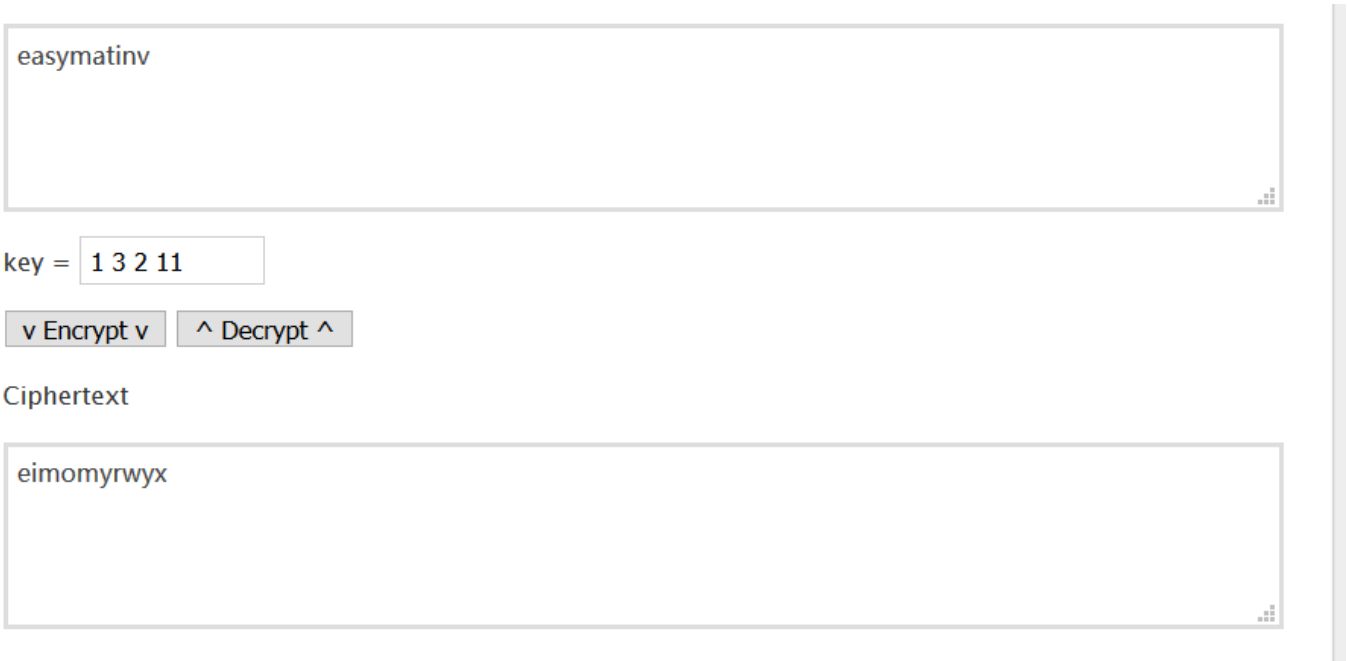
三、Crypto

1. HillCipher：

这里使用一个在线hill密码破译

首先要对hill密码有个初步了解，知道哪个是密钥，哪个是密文（这次要考虑密文的排列方式233333）

http://www.practicalcryptography.com/ciphers/hill-cipher/



输入之后得到easymatinv,加上flag就拿下了

2. 单表替换：

有个网站可以直接进行转换

https://quipqiup.com/

可以看到题目最下面就是flag的形式，直接丢进去转换，加上flag=ecbi这个字典，轻松拿下

3. RSA:

朋友们好啊，

我是刚刚打CTF的菜鸡凉彧，

刚才有个朋友问我凉老师发生什么事了，

我说怎么回事？

给我发了一个张截图，我一看！

噢，原来是有两个年轻人，19岁，

一个900多分，一个1000多分。

塔们说，

有一个说我在暴力分解RSA，把CPU算坏了，

凉老师你能不能教教共模攻击？

帮助救救我的DMCTF。

我说可以，

我说你暴力破解练死劲不好用，他不服气，

我说小朋友你两个大质数来加密我一个明文，

他破解不动，

他说你这也没用，

我说我这个有用。

这是化劲，传统密码学是讲化劲的，四两拨千斤，

309位的英文大N都用不过我的一秒，

他说要和我试试，

我说可以。

我一说，

他啪就站起来了，很快啊。

然后上来就是一个N，

一个e1e2，

一个c1c2！

我全部算出去了，

算出去以后自然是传统功夫宜点到为止，明文放在了txt里，没转化。我笑一下，准备收手。

因为这时间按传统密码的点到为止他已经输了，如果转化之后，一下就ac了，放在网页上没有转换他。

他也承认我拿到十进制密文了，他不知道flag已经拿到了。他承认我先打到他面部。我收手的时间不打了，他突然来了个单密文RSA来打我脸，

我大意了啊，不会算。

他的密文给我算，但没关系啊。

他也说啊，他截图也说了，

yafu跑了两小时以后，当时算不出来了，捂着发热的CPU我就停停。

然后两分多钟以后就好了。

我说出题人你不讲武德你不懂，

他忙说对不对不起，我不懂规矩啊，他说他是乱打的。

他可不是乱打的啊，铮铮鞭腿左刺拳训练有素，后来他说他练过三四年CTF，是个老赛棍，看来是有备而来。

这两个出题人，

不讲武德，

来，

骗！

来，

偷袭！

我17岁的菜鸡。

这好吗？这不好。

我劝这位出题人，

耗子尾汁。

好好反思。

以后不要再出这样狡猾的题。

CTF要以和为贵，要讲武德，

不要搞窝里斗。

谢谢朋友们！

刚拿到后啥也不会，直接搁到yafu里面暴力分解，然后跑了几个小时候我清醒的认识到了自己的愚蠢

换个思路，在网上找到类似的结构，发现是共模攻击，学习了相关算法后，用python编写脚本

```
from gmpy2 import invert


def gongmogongji(n, c1, c2, e1, e2):
    def egcd(a, b):
        if b == 0:
            return a, 0
        else:
            x, y = egcd(b, a % b)
            return y, x - (a // b) * y
    s = egcd(e1, e2)
    s1 = s[0]
    s2 = s[1]
    if s1 < 0:
        s1 = - s1
        c1 = invert(c1, n)
    elif s2 < 0:
        s2 = - s2
        c2 = invert(c2, n)
    m = pow(c1, s1, n) * pow(c2, s2, n) % n
    return m

n= 109092500864595845114356630625328297767713025924094249976449401034106396861526567859066095035738171723963628165131268565179744032726769306584954540556739587142036687035768179963743146203647400910033167151193129143612640525631087415497640037622056569366118603994258110128844010432969361080656938768081671319447
e1= 65537
e2= 1048583
c1= 614805266112761623919293980150516832792477080525549846531462159673564899145938437590279440707108430475891444988068218296382774868199104055934102640819760628158265221338978118469668669596765727865840396613022425971617708960200156724702642734898162681821384457376041620164719932611865860765507907627844859513291

c2= 309285150803709355022720845896678421352424559613575030863293910186134315000556911363686189014381071288067778654857699189101901054839763242885344766823554895781705168093404575495439385619207152940920289374644600205366858787148965430527818916555839073603708608111526786269433270696966856354408594124678199033821
result = gongmogongji(n, c1, c2, e1, e2)
print result
```

用py2跑出来结果，转换成16进制，然后转换成flag，拿下

四、Misc

misc is so fucking easy！！！！！

1. Check In：

签到题，复制粘贴，我起了，一枪秒了，有什么好说的

2. SimpleQrcode：

秒杀题，只是在晚上放出来太骚了，没抢到一血_(:з」∠).

网上有很多gif分解的网站，分解，扫描，over

也可以放pr里看一下

（更改成1分是最骚的操作了）

3.fakezip：

没有人比我更懂压缩包，改后缀成rar，或者winhex修改伪加密字节，然后得到一串音乐字符

https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=yinyue

解码得到flag

4. Base family：

题目可知是base家族，观看题目

```
XUZbB{fp}U)=ql[n%GCbk9RZ7!XD$D)f1G{011LN(TSlXCJT:4nxQ[8Y#I:=k.Qi4t3/S!,N/%[I}^8jjP|0&whvi88gpQce(2lKt9ZHiT^g1.nZH,k=kjTT16pHJ_DrW,Td"^w$Q8+8T])e.llK?*z`gS:+C]llUG:z1=ekEN}8DmJf&GP<Rk:o_Jk<J.zp8%H0g7sYSTJ9p."duRBGj`g0!I+xjm(fh)]IF:>omN8=m+Xp(X0:U*8Sj5|8p._o[i0:%.qu}%_=<D
```

可知是base91加密，转换后得到

```
3G6MzYGwFwTsqcb3MWzTdQBTHZWBZ2LUBprZ3P62T2nsbt1R7o6a7PEsXsBvSFvoexeZJEkhW9Wv1VusvpWK1nfWsVHDypW2j3MMEygzSYLmwxKV5kNwWomvXc5ohX2Jgj6bMRnu6JXkasXdbbw3Aw8Pvh6vWwPfTZ4mpkpNU9fDhyNi1bciCZMXeLiCWL67BVupHPobQcFWkpftgLPggB8wgwW
```

可知是base58（字符串）

得到

```
JZVFSMSZPJMXQTTKMMZVS2TDGVGXUQJTJZKFM3KONJCTEWL2MN4U26SNGJGVIWJQJZ5GWMK2NJNGSTTNKV5E2RDDGNHFOWJTJZCFSNCNPJGTCWTKKF4U42SFGNGXUWJRJZVFSMSNKRNGWTL2IUZFS6TDGVHDEUJ5
```

base32

```
NjY2YzYxNjc3Yjc5MzA3NTVmNjE2YzcyMzM2MTY0Nzk1ZjZiNmUzMDc3NWY3NDY4MzM1ZjQyNjE3MzY1NjY2MTZkMzE2Yzc5N2Q=
```

base64

```
666c61677b7930755f616c72336164795f6b6e30775f7468335f4261736566616d316c797d
```

hex

```
flag{y0u_alr3ady_kn0w_th3_Basefam1ly}
```

可以使用这个网站

http://ctf.ssleye.com/

快速拿下

5. SlientEye：

下载slienteye软件，图片拖进去，轻松拿到flag

6. 编码之王：

打开后看见一堆社会主义核心价值观，可知是价值观编码，使用下网站

https://sym233.github.io/core-values-encoder/

然后看到“如是我闻”可知是佛文加密

http://www.keyfc.net/bbs/tools/tudoucode.aspx

看到“新佛曰”可知是新佛文加密（这玩意还有新的就离谱）

新佛文解码后看到一堆括号，是js的一种编码

F12放进去，console

弹出来“DMCTF{Wow_you_kn0w_more_eNcoding}”

拿下

7. Collision：

看见四个小文档，而且题目叫Collision，说明是CRC32爆破

科普一下CRC32（大佬请忽略）

CRC全称Cyclic Redundancy Check，又叫循环冗余校验。CRC32跟md5，sha1一样都是哈希算法的一种。crc32的优势是速度快，它被设计的目的是用来检测数据在网络传输过程中可能出现的随机错误。它跟md5和sha1有本质的区别就是它不是一种加密hash算法或者叫not cryptographically secure或者not cryptographic hashing。加密哈希算法的特征比如空间极大，碰撞概率极低，对于给定的哈希值难以找到另一个哈希值相同的字符串等crc32都不具备。

对于这种几个字符的文本，因为CRC32值在小范围内不会重复，完全可以穷举，来得到相同的CRC32校验值

下面所示的脚本是4个字节的，其他字节可以更改循环数目来得到

```
import string
import threading
import binascii
import sys


def crc(_crc):
    l = 1
    dic = string.printable
    _input = _crc
    _input = "0X" + _input
    for i in dic:
        for n in dic:
            for h in dic:
                for m in dic:
                    s = i + n + h + m
                    s = s.encode()
                    # print(str(binascii.crc32(s)), _input)
                    if hex(binascii.crc32(s)).upper() == _input.upper():
                        print(_crc, ':', s.decode())
                        print(l)
                        sys.exit()
                    l = l + 1


def crc32():
    print("四字节碰撞")
    num = int(input("你可能需要多个文件同时进行碰撞，请输入文件数："))
    _thread = []
    _args = []
    print("输入CRC32值，不需要0x")
    for i in range(num):
        print(i+1, end=':')
        _args.append(input())
    # print(_args)
    for i in range(num):
        t = threading.Thread(target=crc, args=(_args[i],))
        _thread.append(t)
    # print(_thread)
    for i in range(num):
        _thread[i].start()
    for i in range(num):
        _thread[i].join()
    input()


if __name__ == '__main__':
    crc32()
```

但是，上述脚本只适合5位一下的，六位需要特殊的算法，七位以上就放弃吧，穷举计算CRC32的算法复杂度太大了，很难计算，就算算出来也有很多重复

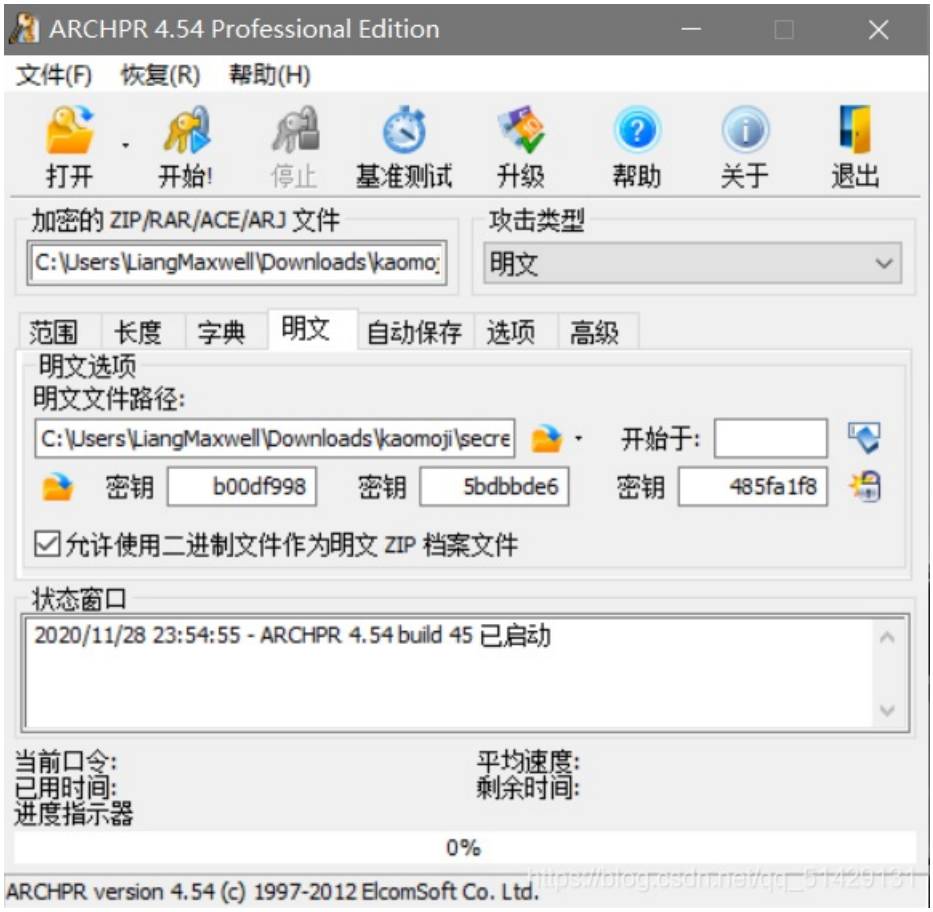
六位请使用

https://github.com/theonlypwner/crc32

非常快速，非常方便

8. kaomoji：

下载之后可以看到一个加密文件夹和secret.txt,而flag.zip里面也有secret.txt，故显然使用明文攻击



工具位ARCHPR ,将secret.txt压缩，用作明文攻击文件

（注意破解完毕之后就可以停止了，不必等待恢复密钥，我当初就是傻傻挂机跑了几个小时发现不对劲，错失了一血）

解压之后打开，对里面的文本进行解码就可以得到flag

9. ARCHPR：

看题目可知是压缩密码爆破，用ARCHPR可以轻松得到密码8531

打开之后一个flag.png，一个hint.txt

hint告诉我们要使用LSB隐写查看，同时加密密码用莫斯密码给出，即“password”

关于LSB 的详细信息请自行Google

因为这是加密过的，所以使用常用工具stegsolve等也看不出来

Google可以发现一个GitHub项目

https://github.com/cyberinc/cloacked-pixel

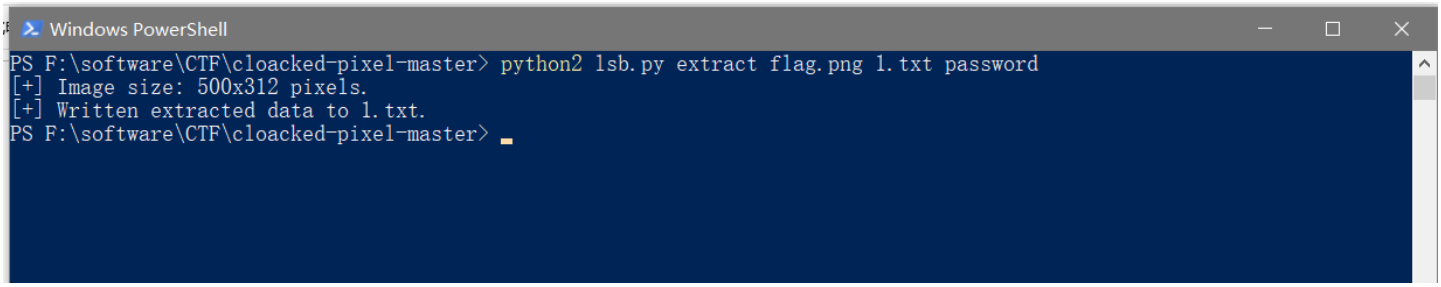
于是通过这个项目来实现

kali Linux等命令差不多，这次以萌新常用Windows实现

shift加右键打开powershell，命令：

```
python2 lsb.py extract flag.png 1.txt password
```

其中flag.png要放进该文件夹，1.txt是存放输出解码的文件，password是上文得到的密码



在1.txt里面得到flag{th1s_15_f1aggggggg}

（对于本蒟蒻来说最难的地方在于安装python2，安装pip2，同时在运行时还得安装各种库，对于形形色色的报错还得网上寻找解决方法，整了半天才弄好，还是我太菜了qwq）

10. outguess：

看题目outguess，在kali Linux里使用outgess，直接解码flag.jpg，得到一个TXT，可以看出来上面是一种凯撒密码，根据提示对下面的文本AES解密，轻松得到结果，拿下

11. SSTV：

当初直接干拉的时候没有看题目SSTV，直接搁Audacity和AU里面看频谱，看波形，看电平，用了所有方法都毫无头绪，Google之后才发现是"慢扫描电视"，不愧是"一种古老而又有趣的技术 "，kali Linux安装Qsstv，选择从文件导入信号，解出来的图片就是flag

E·N·D

总结一下这次的比赛还是学到了很多东西，拿到的分数基本上都是Google得到的（Google is always your friend）,然鹅对于那些技术性的web，bin之类的还是无从下手，毕竟大一啥也没学过，啥也不会，现在自学的程度又不足以拿来用，只能跟在大佬后面走先人走过的路， 看来今后还得继续努力，唉，打了七天就做了这么点题，果然还是太菜了，慢慢学吧