bugku CTF-练习平台 部分writeup

原创

qq_26317875 于 2017-11-15 10:37:15 发布 4963 收藏 4
分类专栏： writeup 文章标签： CTF writeup bugku CTF-练习平台

本文链接：https://blog.csdn.net/qq_26317875/article/details/78538227

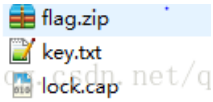

writeup 专栏收录该内容
3 篇文章 0 订阅
订阅专栏

MISC

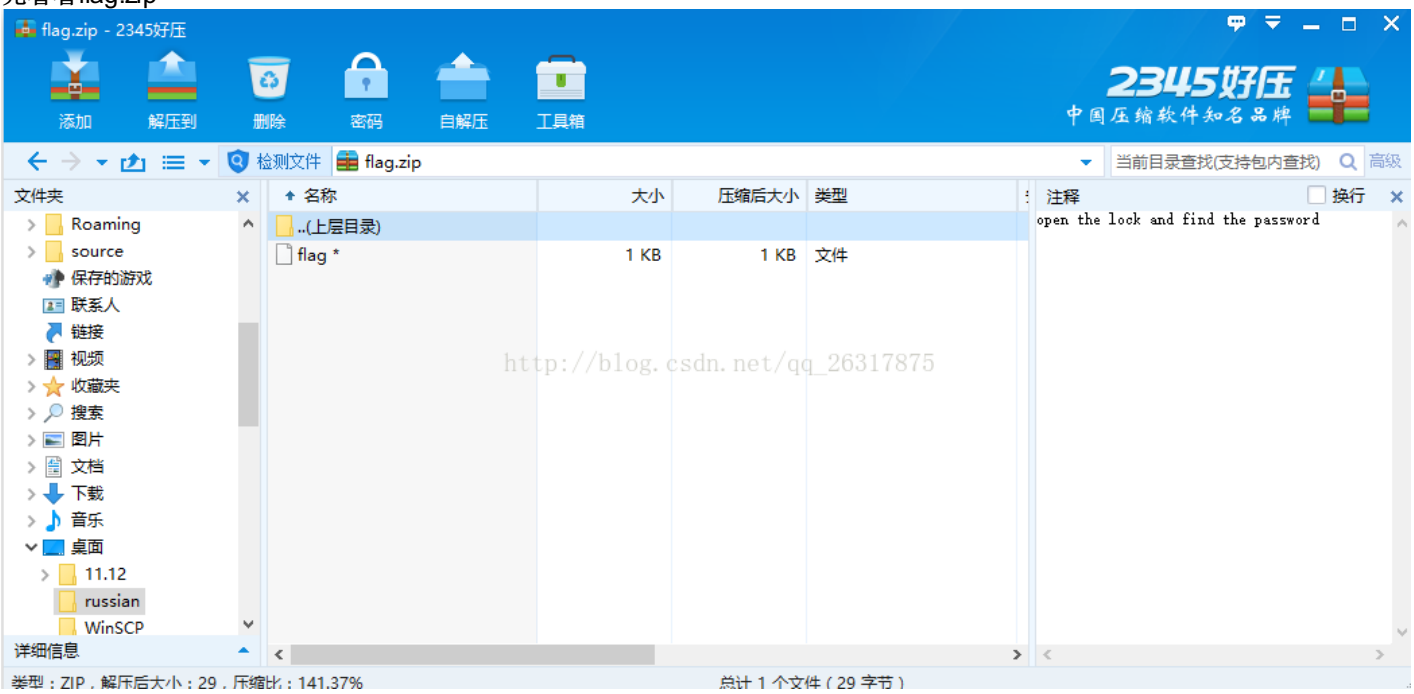
1.俄罗斯套娃

下载下来一个压缩包 题目是bc957e26ff41470c556ee5d09e96880b 好像是MD5解出来是misc。。。杂项题

包里三个文件 试了试常规找不到密码，就试试伪加密 解压出来了。



先看看flag.zip



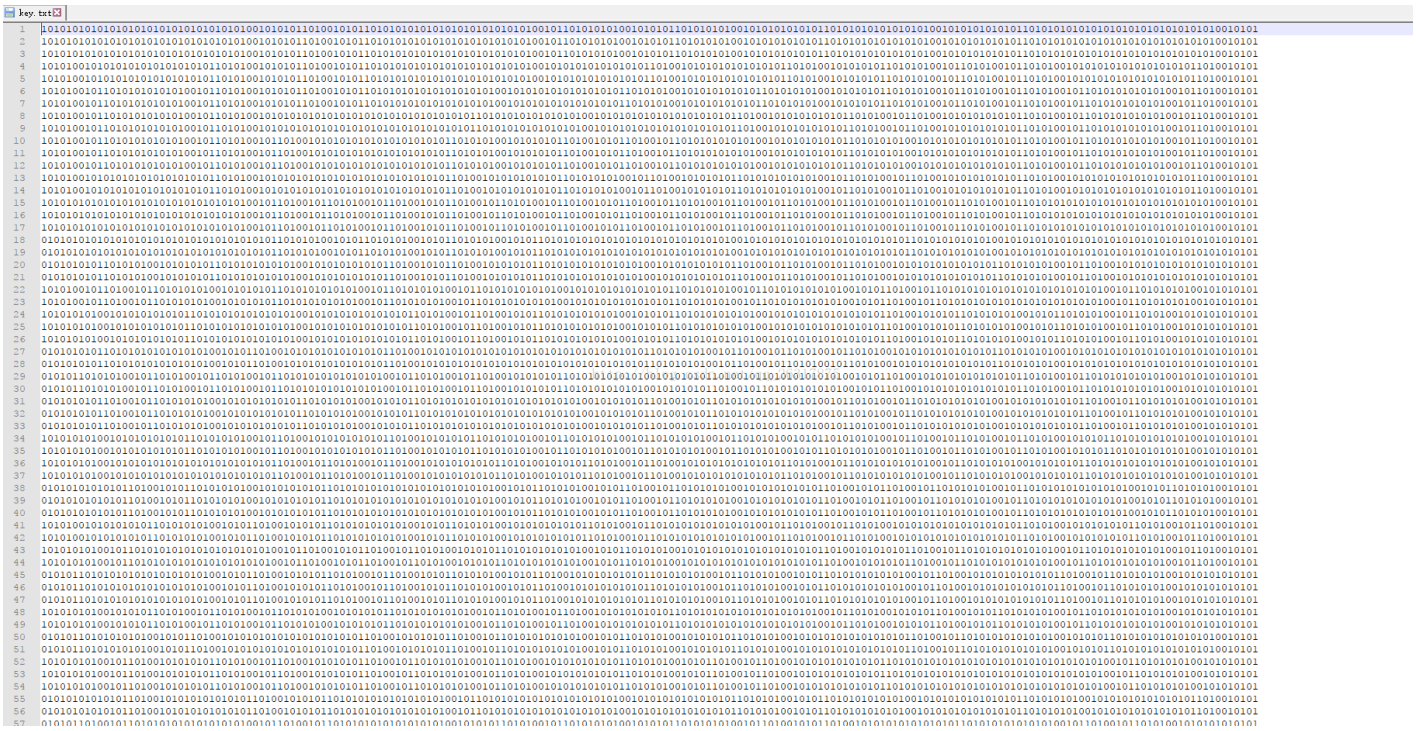
提示打开lock.cap找到密码

cap，扔到wireshark里看一下，基本上都是802.11协议的包

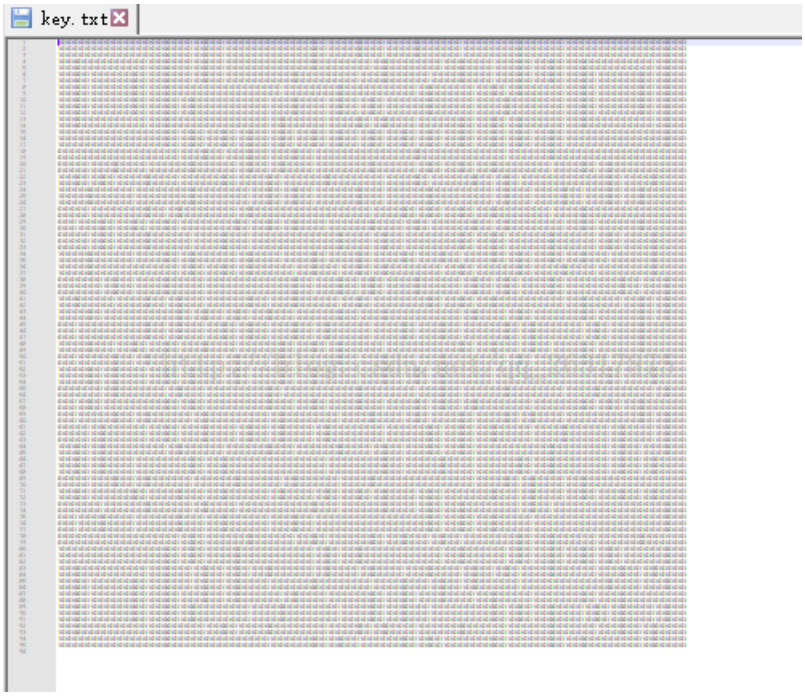
过滤eapol协议发现4次握手包

准备上air-crackng

但是需要一个字典，就打开key.txt先看看



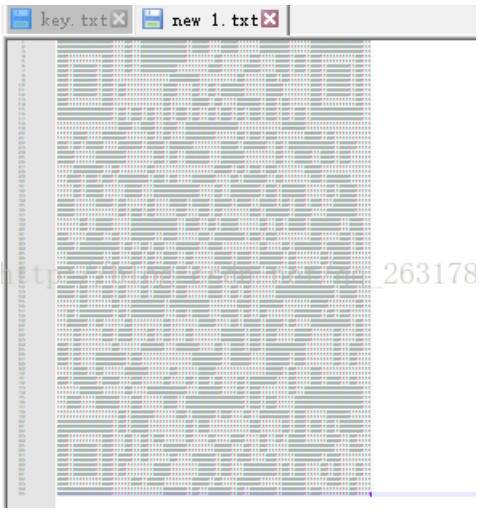
刚开始一头雾水，但是，缩小后一看！



二维码！

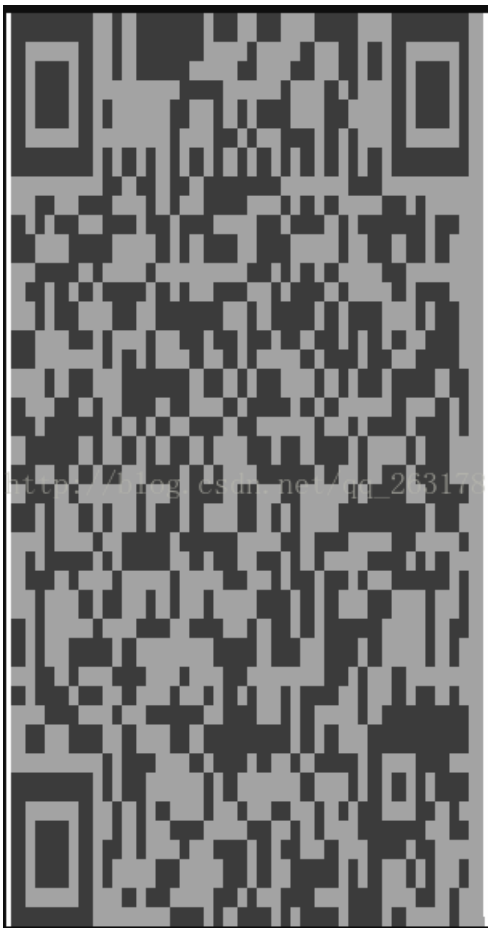
但要怎么转换呢？当时08067CTF比赛的时候有这道题，提示曼彻斯特编码。

转换以后



找了一个text2img的网站

得到一个图片



扫一下得到：

http://47.93.205.124/d39ed8ea9184468644ed90dd20b10cc5.html(现在貌似进不去了)

进去之后是一段颜文字，直接控制台，得到：

broken key:O42G4*3MOUYGYMJUJZGT*TTHGEYDCM*7KNQWSS*POU======

看起来是损坏的base32，base32的范围是A~Z&2~7,=补全

写一个脚本恢复成key

base32.cpp

```cpp
#include<stdio.h>
int main()
{
char str[]="ABCDEFGHIJKLMNOPQRSTUVWXYZ234567";
char str2[]="O42G4*3MOUYGYMJUJZGT*TTHGEYDCM*7KNQWSS*POU======";
int i,m,x,n;
FILE *fpWrite=fopen("codedbase32.txt","w");
for(i=0;i<=31;i++)
{
    for(m=0;m<=31;m++)
    {
        for(x=0;x<=31;x++)
        {
            for(n=0;n<=31;n++)
            {
            str2[5]=str[i];
            str2[20]=str[m];
            str2[30]=str[x];
            fprintf(fpWrite,"%s\n",str2);
            }
        }
    }
}
fclose(fpWrite);
return 0;
}
```


再写一个python批量解密base32

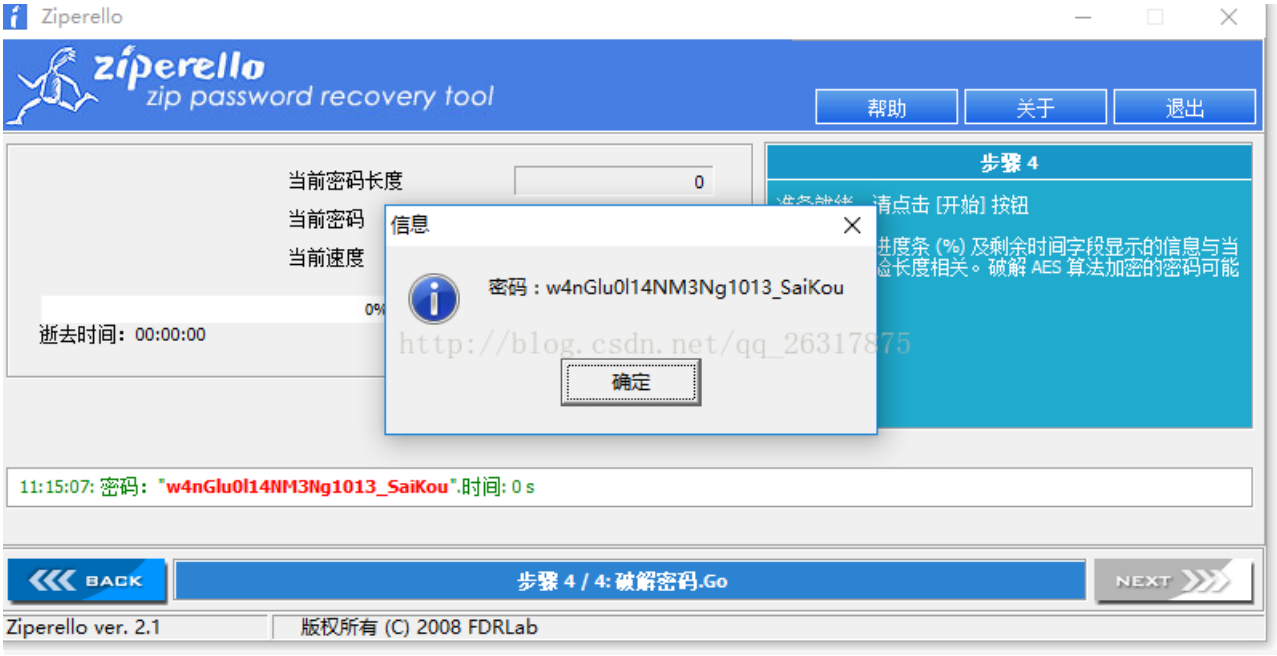
```python
import base64

filea = open(r'.\codedbase32.txt','r')
lines = filea.readlines()
writefile=open(r'.\deocoded32.txt','w')
for i in lines:
        word = i.strip()
        b = base64.b32decode(word)
        print b
        writefile.write(b)
        writefile.write('\n')
writefile.close()
filea.close()
```


得到了这个字典，上aircrack

```
   1  F2:79:60:CC:CF:5D  iphone6s plus            WPA (1 handshake)

Choosing first network as target.

Opening lock.cap
Reading packets, please wait...
                              Aircrack-ng 1.2 rc4

     [00:00:10] 55296/1042532 keys tested (5130.28 k/s)

     Time left: 0 seconds                                      5.30%

                     Current passphrase: w4n 1u0114NM>Ng1011 SaiHOu

                        http://blog.csdn.net/qq_26317875
     Master Key     : 16 A5 7C 54 88 45 7D DF 2C 43 03 1E 72 69 02 CA
                      34 3E AC 18 93 C6 B6 E3 47 54 75 3C A4 EE 7F 65

     Transient Key  : D3 42 76 61 B7 C4 42 57 BE 37 DF 5E D7 8B F0 E1
                      A8 39 2B A6 C0 4E 68 91 6B D2 40 9F CC 4E F7 72
                      C1 FD F6 DF 2D B0 3C 36 38 C9 DB 60 CF F3 AC A9
                      9D CF 72 C2 BD 8D 31 18 82 36 9B A9 04 C4 D0 7B

     EAPOL HMAC     : 78 D3 6F 0C A5 DB 69 DB A5 87 4C 5F 92 84 05 13

Passphrase not in dictionary
```

不知道为啥，测试了一点就自动退出，试了很久发现不行。
决定直接用这个字典跑那个加密了的flag.zip

得到密码：



解压出来，flag文件，直接用notepad++打开
得到flag！

flag{D3cUd[redacted]_1t}

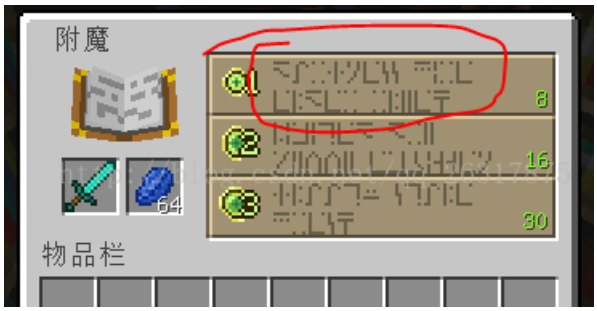
Crypto

来自宇宙的信号

一个图：

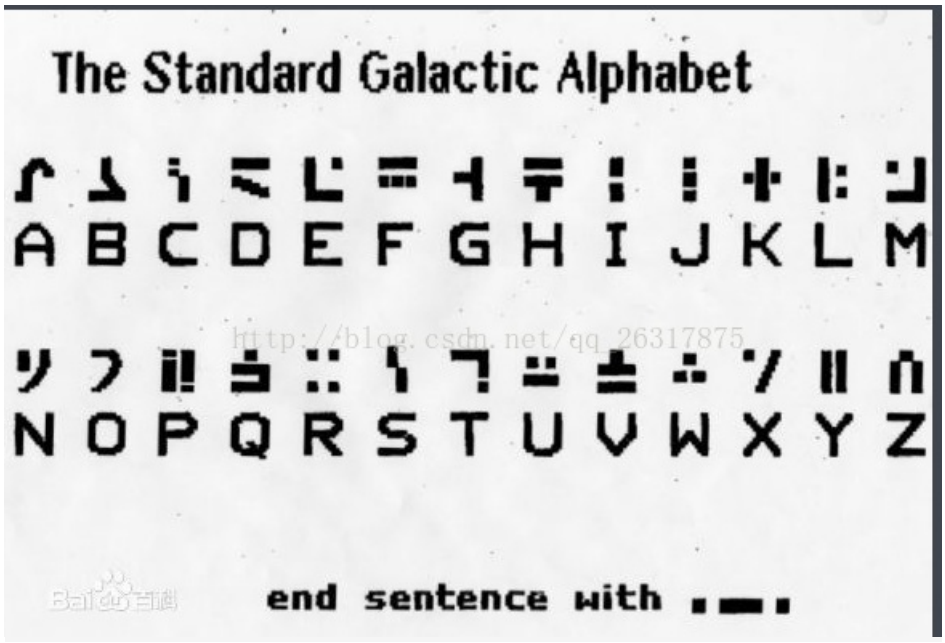
百度谷歌都识不出来

仔细想想，和minecraft里的这个有点相似！



百度一下minecraft 附魔台 语言

查到了 标准银河字母(SGA) (果然像hints里说的一样:"银河战队出击")



直接对应小写字母，提交完成！