实验吧杂项记错本

原创

Wh0ale 于 2018-05-06 18:09:02 发布
分类专栏： 安全技术 文章标签： 杂项

1.小白鼠与蝙蝠的故事
下载题目压缩包解出来是一个vbs文件，这题就是考验vbs能力了，如果是学c语言的人会感觉有点吃力。

第一步千万!千万！千万！不要直接运行vbs（不管是不是这题还是其他vbs），这会有风险，先复制个副本在虚拟机（当然本题没那么危险啦）运行下，弹出框显示"this_is_key"，(⊙ 0 ⊙)如果有那么简单就好了，这里要注意下，当运行后这个vbs，原文件会被改写（幸好运行的是副本）。用txt等打开最早的原文件，是只有一长行的代码。VB中的冒号(:)起分隔语句的作用，使得一行可以有几个语句。看着一长串比较麻烦，自己手动格式化下：

```
code="..."
key=9
code=rev
Execute code
Function rev()
 For i=1 To Len(code) Step key
 rev=rev+strReverse(Mid(code,i,key))
 Next
End Function
```

0) 用两个双引号转义表示字符串内容中的一个双引号。
1) 看到rev=rev+这种操作函数名的行为不要慌，因为VB中是通过给函数名赋值来返回值的。
2) For 变量名=初值 To 终值(有包含) Step 步长 （每一个For要对应每一个Next）
3) Mid(str,M,N) 截取字符串中从第M位(包含)起N个长，记得起始位置是从第1开始。
4) StrReverse是字符串逆序
5) Execute是个函数，执行一个或多个语句，忽略语句的返回值。

有这些语法知识傍身，稍微理解下就是把code字符串每key个长度逆序，然后再执行这个code，而我们要解题的话只要把

Execute code:
替换为

```
Set objfso=CreateObject("scripting.filesystemobject"):Set objTextFile
```

2.你有记日志的习惯吗
附件的压缩包下载后，解压后有不少文件，起初我找了一些log文件和config文件，都看得晕晕的。最后经人提醒mysql有一个配置文件my.cnf，搜索它，也就是在www\lampp\etc里面，打开它就看到KEY了。
Flag:
http://127.0.0.1/CMS/www/lampp/etc/my.cnf

3.西普CTF-可启动的磁盘镜像
http://hebin.me/2017/09/09/%E8%A5%BF%E6%99%AEctf-%E5%8F%AF%E5%90%AF%E5%8A%A8%E7%9A%84%E7%A3%81%E7%9B%98%E9%95%9C%E5%83%8F/

4.ruby

5.这是捕获的黑客攻击数据包，Administrator用户的密码在此次攻击中泄露了，你能找到吗？

很简单，题目意思简单明了，用wireshark分析数据包就行了

ip.addr == 192.168.30.101 and http
查看数据包发现是菜刀链接

```
z0:@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$p=base64_decode($_POST["z1"]);$s=base64_decode($_POST["z2"]);$d=dirname(
z1:Y21k
z2:cd /d "c:\inetpub\wwwroot\"&net use \\192.168.30.184\C$ "Test!@#123" /u:Administrator&echo [S]&cd&echo [E]
```

6.内网攻击数据包，请分析
```
   Session Setup AndX Request (0x73)
      Word Count (WCT): 13
      AndXCommand: Tree Connect AndX (0x75)
      Reserved: 00
      AndXOffset: 292
      Max Buffer: 4356
      Max Mpx Count: 2
      VC Number: 0
      Session Key: 0x00000000
      ANSI Password Length: 24
      Unicode Password Length: 24
      Reserved: 00000000
      Capabilities: 0x000000d4, Unicode, NT SMBs, NT Status Codes, Level 2 Oplocks
      Byte Count (BCC): 231
      ANSI Password: 9e94258a03356914b15929fa1d2e290fab9c8f9f01999448
      Unicode Password: 013f3cb06ba848f98a6ae6cb4a76477c5ba4e45cda73b475
      Account: syclover
```

Primary Domain: ROOT-53DD5427BC
Native OS: Windows Server 2003 3790 Service Pack 2
Native LAN Manager:
Extra byte parameters: 570069006e0064006f00770073002000530065007200760 0...

彩虹表跑
ANSI Password: 9e94258a03356914b15929fa1d2e290fab9c8f9f01999448
Unicode Password: 013f3cb06ba848f98a6ae6cb4a76477c5ba4e45cda73b475
wp：https://bbs.pediy.com/thread-176189.htm
wp：http://www.freebuf.com/articles/web/54176.html

7.抓到你了

8.女神
先使用base64把下载的txt解码
写个脚本来解开

```
import base64
open('nvshen.png','wb').write(base64.decodestring(open('nvshen.txt','rb').read()))
```

9.Broken Heart

http://www.shiyanbar.com/ctf/writeup/63

首先用到了两次file查询指令

导出所有的http对象

使用grep 查找其中的content-Range包括文件的字节位置
linux中执行：strings myheart.pcap | grep 'Content-Range' | awk '{print NR,$3}' > myheart.txt
输出到文件myheart.txt，将txt和导出的23个文件放在一个文件夹下
编写代码，输出到文件，后来观察头包含HDR，前面缺少13个字节，猜测可能是个PNG图片，补充PNG头的前13个字节。打开图片。

```
f=open('myheart.txt','r')
x=list(f.readlines())
f.close()
listvalues=[]
indexlist=[]
for i in xrange(len(x)):
d=x[i].split()[1].split('/')[0].split('-') #提取前后两个数
flag=True
for kline in listvalues:
if (int(d[0])>=kline[0] and int(d[1])<=kline[1]):#若数在已存在的列表中，则取消存储
flag=False
break
if flag:
listvalues.append((int(d[0]),int(d[1])))#存储
indexlist.append(i) #存储原顺序，以得到文件名


sortedpos=sorted([xx[0] for xx in listvalues]) #排序


fresult=open('resultx.png','wb')
fresult.write('89504E470D0A1A0A0000000D49'.decode('hex')) #写入png头，共13个字节
for i in xrange(len(sortedpos)):
index=0
for searchnums in listvalues:
if(sortedpos[i]==searchnums[0]): #在存储的范围列表中找到位置序号
break
else:
index+=1
f=open('LoiRLUoq(%d)'%(indexlist[index]),'rb') #打开文件
if(i!=len(sortedpos)-1):
fresult.write(f.read()[:sortedpos[i+1]-sortedpos[i]])
else:
fresult.write(f.read())
f.close()
fresult.close()
print '执行完毕，请查看图片得到key'
```

看了wp还是不懂　杂项题真难！

10.misc100
不会

11.misc200
考的点挺多的，都是我看wp、才明白的
此题已经提示是明文攻击，自然说的就是zip的"Known-plaintext attack"，也就说明我们要从文件中提取出加密的zip文件和对应的部分明文文件。关于明文攻击知识请自行查阅资料。大概意思就是：如果拥有加密包中任意一个文件内容的前提下，对该明文文件进行同样算法的无加密压缩，然后对比两个压缩包中相同文件，得出差异值获取这个加密包的三个Key，压缩包中的每个文件都是通过这三个Key进行加密压缩的，只要得到了这三个Key就能解压整个加密的压缩包（这个方法只适用于ZIP的加密压缩）。
先看下提供的是什么。如图，像是vmware的镜像文件，但是和目前vmware的镜像文件不一样，如果是此类文件，也似乎经过修改或其它原因已经破坏镜像文件的分区等信息，无法映射成磁盘了。

再尝试使用foremost提取文件，似乎文件较为完整。其它文件略过，直接看zip文件。一共有两个zip。一个是未加密，另一个加密。对比下就能看到里面都有readme.txt文件，且CRC值相同，则认定为同一文件。此文件就是我们需要的明文文件。

binwalk '/root/Desktop/MISC/areyoukidding'

foremost '/root/Desktop/MISC/areyoukidding'
两个readme.txt的CRC相同，所以这应该就是相应的明文和密文
2700是可以解压的，将解压出的readme.txt压缩成readme.zip,作为明文去破解
使用ARCHPR

解的00008257_decrypted.zip
For this question,the flag is XDCTF{biiubiiiiiiiiiiiiiiu&ddddyu}

这道题刚开始的时候我直接把下载的文件改成7z，当然这样做是失败的
拿到这道题的时候，应该先用winhex查看一下信息，然后在拖入kali file命令查看一下。确定了文件信息后在判断下一步该如何行动
然后使用binwalk和foremost将文件的内容分割出来
我之前因为这两个工具看起来很难操作就放弃学习了
没想到这么简单binwalk是看文件信息（判断分割出来的内容）foremost是把文件分割，binwalk也能分割但好像不稳定
｛但是，在后续的操作过程中发现提取的加密zip文件有问题，不完整。我均是在win下使用的工具，所以请尝试在linux下提取文件。（第一次做似乎没有这么麻烦，直接能得到完整文件，具体也忘了）无法，缺失的部分是包含文件内容的，过了许久才发现binwalk提取的zip文件里有我需要的部分。直接16进制编辑器整过来。除此之外，还用16进制编译器纠正下文件压缩后的大小，删除了文件多余的一个字节0x00。下面两张图，前一张是修复前的zip结构图，后面是修复后的zip结构图。｝这是他不稳定的地方，所以多数情况下我用foremost

12.NSCTF misc250

这题考的是分析数据包、暴力破解zip密码、python脚本...
下载来的pcapng用wireshark打开，然后在右上角点击，文件—导出对象—http—save all
得到两个文件，一个是%5c,一个是压缩文件，压缩文件需要密码

我们先看%5c，用的是winhex，发现是html,改后缀打开 告诉我们密码是nsfocus+5位数字

这应该就是rar的密码，我们按照要求生成字典，然后APCHPR爆破即可
（字典可以用python生成）

```
f=open('1.txt','w')
s= 'nsfocus'
for i in range(100000):
 m = '%05d'%i
 f.write(s+m+'\n')
```

破解出密码nsfocus56317
解压
flag{NCTF_R4r_Cr4ck}

13.2015RCTF（misc50）
遇到这种杂项题，不知道文件是什么，首先就先用file命令查看下，或者用记事本打开，看文件头格式

将log_log该文log.rar可以解压出来一个真正的log文件

然后就是查找flag

这里有技巧避免一个个的查找flag
现将ctrl+f查找flag
然后发现规律查找 misc.flag
然后放入linux下正则： cat log | grep "misc.flag" > log1
发现是sqlmap的注入语法
这是通常当找到!=的时候就是正确的ASCII值
cat log | grep "!=" > log2

分析文件log3需要对!=后边的ASCII提取并且转换成字符

编写python脚本，对文件log3进行处理

```
number = [82,79,73,83,123,109,105,83,99,95,65,110,64,108,121,83,105,115,95,110,71,49,110,120,95,83,105,109,125,5]
string2=''
for i in number:
    string=chr(i)
    string2=string2+string
print(string2)
```

wp:http://www.shiyanbar.com/questions/867

13.抓到你了
这题考的是16 进制的数据包
ping 程序是用来探测主机到主机之间是否可通信，如果不能ping到某台主机，表明不能和这台主机建立连接。ping 使用的是ICMP协议，它发送icmp回送请求消息给目的主机。ICMP协议规定：目的主机必须返回ICMP回送应答消息给源主机。如果源主机在一定时间内收到应答，则认为主机可达。
过滤器选择icmp

抓到包分析，发现也就第一个包没有data
剩下的都有徐局 数据的内容就是flag

14.BAT公司信息查询系统
好久没做湖杂项了

首先是扫二维码，正常人都会扫的
然后打开二维码网址（rootpadding.txt）--可以在CSS里看到jpg的链接

打开链接发现
http://ctf5.shiyanbar.com/misc/5/rootpadding.txt
```
$usera = ($_POST['userid']);
 if(isset($usera)){
   if ($usera == "1"){
       $usera = (int)($usera);
       if($usera == "0"){
          header('Location: ./bhjskdfiffeswdwe.php');
       }
    }
```
./bhjskdfiffeswdwe.php打开这个php

<!-- ┼擁數畣整爓煥敵瑮∨灯捲≤┤ > -->发现这段话
保存为unicode文件
然后用winhex打开（一般这种乱码文件就是用winhex或者binwalk打开）

15.矛盾的in2
这题做的我想哭....
拼接在一起49416772656549446F（15就是16进制的F）
用火狐的firebar解码
lAgreelDo
这里有个坑的地方 就是lAgreeldo do小写

其实看到这种题啥也没有的情况下，就应该是从源码找答案

16.保险箱
遇到杂项题应该先把文件下下来
①是个图片，用magicexif分析 查看有什么可用信息，然后放入文件夹，用winhex打开
②拖入binwalk分析，foremost分离
③查看jpg文件（看里面是否隐藏文件），果不其然，这道题里面有个2.txt,那是为zip文件呢，我们把后缀改成zip，然后解压，发现需要密码，ARCHPR暴力破解即可。

17.雌黄出其唇吻

题目的“雌黄出其唇吻”出自南朝梁刘峻的《广绝交论》中，“雌黄出其唇吻”是表示对世人的信口雌黄不屑。

不知道为什么取这个题目

试过debase64（）两次解题链接所显示的字符，乱码，看到一点规律都没有，刷新网页字符串还会变 随即放弃这有个想法。

首先打开当前目录的robots.txt，发现拉到最底下有xml目录，打开就有个base64编码的一串字符

18.理查德
看这题刚开始还以为要社工
听完音频才知道是摩斯电码
1.下载文件
2.对文件进行分析
文件扩展名为.flac，百度一下，发现是个音频文件，类似MP3
3.用Audacity软件打开它
（高段音频查看，不要像我一样傻傻的从第一句开始看）

然后-。-。-。-。-。
最后放入http://www.zhongguosou.com/zonghe/moErSiCodeConverter.aspx 解密

19.绕
首先打开网站 发现只有一个登录框
然后查看源码（这里用chrome，chrome比火狐显示界面友好）
以下是代码
```
_='function $(){e=getEleByld("c").value;length==16^22a60b0b310e5ece$0ebe5){tU2FsdGS481hY7lo/lBh2Waw==nVkX1829lDS37Dtcv78qFewreA/kNjZ1UZ6LuMTMoP2i8U/2KZtCckgQoGAmEapD0Ys=
[t,n,r,i];for(o=0;o<13;++o){  [0]);.splice(0,1)}}}  \'<input id="c"><  onclick=$()>Ok</>\');delete _var ","docu.)match(/"];/)!=null=["  write(s[o%4]buttonif(e.ment';for(Y in $='
 ')with(_.split($[Y]))_=join(pop());console.log(_)
```
将eval()转化为console.log()
```
function $(){var e=document.getElementByld("c").value;if(e.length==16)if(e.match(/^22a60b/)!=null)if(e.match(/0b310/)!=null)if(e.match(/e5ece$/)!=null)if(e.match(/0ebe5/)!=null){var t=
["U2FsdG","S481hY","7lo/","lBh2Waw=="];var n=["VkX182","9lDS37","Dtcv78qFew"];var r=["eA/","kNjZ1UZ","6LuMTMoP2"];var i=["8U/2KZ","tCckgQoGA","mEapD0Y"];var s=[t,n,r,i];for(var o=0;o<13;++o)
{document.write(s[o%4][0]);s[o%4].splice(0,1)}}document.write('<input id="c"><button onclick=$()>Ok</button>');delete _
```

根据其中的if(e.length==16)
if(e.match(/^22a60b/)!=null)
if(e.match(/0b310/)!=null)
if(e.match(/e5ece$/)!=null)
if(e.match(/0ebe5/)!=null)

简单拼接下就得到符合要求的字符串22a60b310ebe5ece，填入form即可得到U2FsdGVkX182eA/8U/2KZS481hY9lDS37kNjZ1UZtCckgQoGA7lo/Dtcv78qFew6LuMTMoP2mEapD0YlBh2Waw==

好像是base64嘛，其实不是的
观察头部，其实是AES对称加密算法加密的，加密后的密文都是以U2FsdGVkX开头
既然是AES，解密就必须有密钥
hint说把出题人的名字拿去加密，也就是说出题人的名字是密钥
解密发现不对
多次尝试后发现出题人名字 iFurySt 的MD5就是22a60b310ebe5ece，拿它解密就行了

20.snake
这题算是我自己做出来的吧，感觉成就感还是很高的

杂项题感觉还是比web题简单点
首先binwalk检测里面有什么文件

发现有snake.jpg还有一个安装包
解压发现有个key
V2hhdCBpcyBOaWNraSBNaW5haidzlGZhdm9yaXRlIHNvbmcgdGhhdCByZWZlcnMgdG8gc25ha2VzPwo=
base64解密发现
What is Nicki Minaj's favorite song that refers to snakes?
百度一下是Anaconda
接下来的难题是cipher

密码学：
https://blog.csdn.net/h0_0p/article/details/78247774
https://blog.csdn.net/21aspnet/article/details/7249401
https://blog.csdn.net/ly0303521/article/details/53391741
https://blog.csdn.net/lz710117239/article/details/71119032
https://blog.csdn.net/moxiajuzi/article/details/52749562

21.64格
首先解压出来的是一个gif文件
打不开GIF文件
这里我们需要注意文件头，一般打不开某个文件，有两种情况
一种是里面包含的别的文件
另一种是文件头格式不对

这道题是格式不对
我们使用C32asm修改文件头（winhex我不会用）
修改完后就可以打开gif图
但是我们仍然没有知道这张图有什么信息
使用gifsplitter分离得到十九张图片

然后看到每张图片的小黄人都在不同的地方，并且64格
然后我们百度64进制（也就是base64()）
发现了一些规律
对应这维尼所在的格子求得18个数字
16，53，17。。。。。。。
再将数字对应百度百科下的表解得字母
得到Q1RGe2FiY19kZWZfZ30
base64解码之
得到CTF{abc_def_g}
--我感觉我做到解开字母，提交答案的时候就不会继续往下想了
也不会想到最后还需要base64()解码

22.功夫秘籍
这道题不像想象中那么简单，刚开始查看文件头是png，除此以外没有得到更多消息了

我这里我用winhex看不到文件头信息，用C32ASM还可以，以后得多用c32asm

这里看wp发现文件的最下面有一串信息，base64解密得T_ysK9_5rhk__uFMt}3El{nu@E

这就很明显了有}和{，估计是栅栏加密，解得：

Th3_kEy_Is_{Kun9Fu_M@5tEr}

23.解码磁带
这道题应该挺容易想出来的
查看_o_o_o的规律，发现每次都只有五个字符。这像不像二进制的文件
然后根据_o的规律，一个个敲出字符（至于0是o还是_就要百度ASCII来查看规律了）

然后在记事本替换
写一个脚本判断ASCII
```
# -*- coding: utf8 -*-
#author:woniu
import binascii
file=open('bin.txt','rb')
t=''
for line in file.readlines():
    t+=chr(int(line,2))
print t
```

C:\Users\49974\Desktop>1.py
Where there is a will,there is a way.
simCTF{}提交即刻

24.A记录
首先是命令行模式的教程
（1）用aircrack-ng检查cap包：
aircrack-ng.exe shipin.cap
可见这里是wpa加密，并且bssid：00:1D:0F:5D:D0:EE，essid：0719

（2）使用弱口令字典破解wpa加密
aircrack-ng.exe shipin.cap -w wordlist.txt
这里wordlist.txt是弱口令字典，包含了常见的路由器密码，可以网上下载到，也可以自动生成

可见破解到的密码是88888888

（3）用密码解密cap
这里用到airdecap-ng解密cap报文，使用到了刚才的essid和破解的密码
airdecap-ng.exe shipin.cap -e 0719 -p 88888888

于是在目录下生成一个shipin-dec.cap，使用wireshark打开

4、查看DNS记录
在筛选器（filter）中输入“dns”查看

题目提示是第一条A记录，那么就是flag了

25.ROT-13变身了
lst=
[83,89,78,84,45,86,96,45,115,121,110,116,136,132,132,132,108,128,117,118,134,110,123,111,110,127,108,112,124,122,108,118,128,108,131,114,127,134,108,116,124,124,113,108,76,76,76,76,138,2
lst=[chr(i-13) for i in lst]
print "".join(lst)

26. Canon

下载一个压缩包，解压得两个文件
一个加密的压缩包，一个音频文件，想都不用想，音频文件一定包含压缩包的解密密码
使用MP3stego

Decode.exe -X -P mimimi music.mp3
用mimimi密码破解无果
Decode.exe -X -P Canon music.mp3
破解成功
我们打开这个music.mp3.txt文件看看里面的内容
用文件内容解压缩包pqiem*zoei$%h
发现是一串字符 放到我们的zip里面看看是不是解压密码，发现确实是一个解压密码。

这个zip文件里面的内容我感觉很像base64位的东西 于是去解密base64

发现解密出来的内容有点像网页代码 于是复制出来里面的内容 新建文本为html结尾的文件 在打开网页 搜索关键词CTF得到flag

27.flag.xls
一打开下载好的execl文件就可以看到加密
但是我也不知道什么东东可以破解excel文件密码
于是乎就用winhex打开文件查找flag

四下【F3】就看到了

一般来说winhex和C32Asm都可以看到文件内容，如果实在找不出来密码的话就用这两个工具吧

28.紧急报文
1.分析密文：FA XX DD AG FF XG FD XG DD DG GA XF FA
密文都由ADFGX
2.百度一下，发现有个ADFGX密码
3.简介：
ADFGX密码(ADFGX Cipher)是结合了改良过的Polybius方格替代密码与单行换位密码的矩阵加密密码，使用了5个合理的密文字母：A，D，F，G，X，这些字母之所以这样选择是因为当转译成摩尔斯电码(ADFGX密码是德国军队在一战发明使用的密码)不易混淆，目的是尽可能减少转译过程的操作错误。
加密矩阵示例：(密文两个一组，先竖后横)
4.对上述密文进行解密：
FA XX DD AG FF XG FD XG DD DG GA XF FA
flagxidianctf
5.根据格式要求：提交flag_Xd{xidianctf},发现错误！！！
6.问题出在格式上，吐槽一下实验吧的格式说明，正确格式是：flag_Xd{hSh_ctf:}
7.提交flag_Xd{hSh_ctf:flagxidianctf}

29.deeeeeeaaaaaadbeeeeeeeeeef-200
有意思的一道题

首先用ie才能打开的图片，打开发现是一个普通的图片没什么别的信息

查看exif，binwalk也没能找到什么有用的照片

yongbinwalk、Hxd、C32asm查看倒是看到了是iPhone5拍出来的
但是看wp发现还要看分辨率...这点我怎么也想不到

检查png文件crc，发现错误，线索来了。
CRC error in chunk IHDR (computed fcc410a8, expected c1d0b3e4)
修改回来先。
修改后没没有什么下一步线索，回到winhex检查一下发现
tEXtSource iPhone 5
既然是手机照的，图片怎么被这么难看，要不就是照相水平太差，要不就是隐藏了一部分
查了一下iphone 5手机的照相功能
iphone5后置摄像头是3264×2448，前置摄像头是960×1280，截屏是640×1136，全景照片最大分辨率是10800×2410。
是不是感觉找到了组织
照片的分辨率是3264×1681,猫腻在此。
结合png文件结构高度应该是4个字节
winhex把文件前面的0691改0990，就是分辨率1681改成2448，改完发现flag

原来这张图是被裁减的图，把他还原，就可以看到信息了

30.pilot-logic

很简单拖到C32Asm找到pass字段就好了

31.spaceport-map

这道题还是有意思的，打开链接是个gif图片
有个key：**********一闪而过
然后就使用gifsplitter分离图片
然后我们查看到了key的值
提交的时候把问号去掉就好了
Do passports let you fly interstellar

tip：这里用C32asm看不出什么 查找flag和key、pass都找不到
随即放弃这个想法

32.损坏的U盘镜像
参考：https://blog.csdn.net/xingyyn78/article/details/79993878
使用winhex打开CTF.hdd
选择选项--通过文件类型恢复
恢复两个压缩包（一个加密，一个没加密）
Password：checksum的32位MD5（checksum取前4字节）
例：checksum为AABBCCDD则密码为B631050B08627046D47E0CC16250BA2E

SD卡 3.0 标准推出后，SD卡往高容量发展，这个时候 FAT，FAT32 已经不符合SDHD的需求了，
这时引进了新的文件系统 ---> exFAT。
通过查看exFAT文件系统格式可以得知如何计算checksum

python代码进行计算checksum值。计算结果为0x81c6fa94。

[python] view plain copy
```
# -*- coding:utf8 -*-

file = open('/root/Downloads/CTF.hdd', 'rb')
content = file.read()
checksum = 0
for i in range(0, 11*512):
    if i == 106 or i == 107 or i == 112:
        continue
    checksum = (((checksum << 31) & int('0xFFFFFFFF', 16)) | (checksum >> 1))+content[i]
print(hex(checksum))
```

使用81c6fa94计算MD5值得到的password是错误的。查看了一下其他人的WriteUp。是因为与文件的大小端存储有关。正确的顺序为94FAC681。

计算出正确的password为C9737665D39274F6C5A256B943748068。

解压获得Key.txt.flag为CTF{ExFat-Checksum}

36.CTF-MD5之守株待兔，你需要找到和系统锁匹配的钥匙
Unix时间戳（英文为Unix epoch, Unix time, POSIX time 或 Unix timestamp）
是从1970年1月1日（UTC/GMT的午夜）开始所经过的秒数，不考虑闰秒。
UNIX时间戳的0按照ISO 8601规范为 ：1970-01-01T00:00:00Z.
一个小时表示为UNIX时间戳格式为：3600秒；一天表示为UNIX时间戳为86400秒，闰秒不计算。
在大多数的UNIX系统中UNIX时间戳存储为32位，这样会引发2038年问题或Y2038。