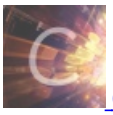
【i春秋 竞赛训练营】Misc 杂项 Recreators

原创

Kal1 于 2020-08-14 15:52:47 发布 136 收藏 2

分类专栏： CTF刷题 杂项 CTF刷题 密码学 文章标签： base64 信息安全 安全

本文链接：https://blog.csdn.net/weixin_45844670/article/details/108005591



CTF刷题 杂项 同时被 2 个专栏收录

19 篇文章 0 订阅

订阅专栏

CTF刷题 密码学

4 篇文章 0 订阅

订阅专栏

题目链接：https://www.ichunqiu.com/battalion?q=2743

下载附件，得到一个无后缀文件

先用file命令看一下是什么类型的文件

```
root@kali:~/Desktop# file ReCREATORS
ReCREATORS: VMware4 disk image
root@kali:~/Desktop#
```

发现是虚拟盘文件

那么再分解一下看看能不能有什么收获

```
foremost Recreator
```

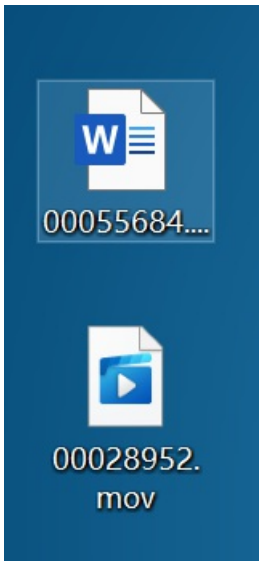
```
root@kali:~/Desktop# foremost ReCREATORS
Processing: ReCREATORS
|foundat=_rels/.rels ◆(◆
foundat=word/_rels/document.xml.rels ◆(◆
*|
```

很好

分离出来一个docx文件和mov文件

但是kali打不开docx文件。。。。

用word打开



是一大串数字

```
3441344134383435353532353334453442354134413535333435333332344634413445343
3353533235363433353434413541343435353535353434333436344233353443343643735
3634333443344235413434343534443536344235343439344534433535353536353334423
4393541343435363435353533323531343933353443343534443536344234453442353634 36
3436344235333442344634413445343335363446353533235343442333534363536343535 3
2353335373439353634413534343535363332344234413541343634353442353234423533 4
4134413442353535393532353334383439353535413436343735333332353734413532343 43
4353539353234423534344135353541343534393533354135363439353634433436344235 35
3532353334423335343634353334353334333536344233353441343634373534343334444 344
1344134343436344235343442353334413445344235353446353335333444344235361441 35
3634463535333234443441353234323435353335363533344534423444354134363531353 33
5333446343935413433353634423535353235333441353234343535353535343533343734 41
3536344135353537353633323442344234413433343534423535333235363441344534423 43
5353735343533343734423541344235363435353133323438344134453443343535336346 34
3334363442354134363535333635333332344234393541343335353332353634333443344 23
5363436343533343532343334363441333534433436343735373533344334433441344343 36
3444353434423532343734413435343535353533344135333442353634443536343535333 33
2344434393335343535363535353635333534344234443541343634373533335333537343 935
3634333535343735363533344234423445343635353535353334333436343734413437353 63
4373536353334423442354134373435343935323442353834413445343934353533353335 33
3436343935413437353634393533333235343441344534383435344435363442353434423 54
1344135353539353334413536344135363443343535373536344135333443343234363435 35
3535343433343634393335344334353437353634333443344334413434343634443534332 34
4234413541343334363442353633323534344234453437343535333536353334383442354 13
4353535333234443533343834413441344534353535353234423538344233353432353634 39
3533333233323439344534333536353335353541353334413445343634363435353133323 53
5343935363442353634373536343334423441354134343436344435343423535343934453 4
3435353537353234413533343935363434353634423531333234443441353234363435343 53
5363533353034423541344534363444353233323442344135323433353434393536344235 34
3441344534353536353535333433353734413445344234353437353434423441343735363 43
7343534423533344235333442344534363435353735373533343334423536343435363437 35
3535333537344134453438343535393536353335343442353634413536343735333541353 63
```


然后依次解密即可得到最后的flag

```
b'flag{wh4t_a_w0nderfu1_d4y}'
```

解密过程：

hex

hex

base32

base32

base32

base64

base64

hex

base32

base64

base64

解题经验：

1. 一上来一大串数字或者数字掺杂英文的（不是base家族的规律），一般都是十六进制转字符串，比如

```
c='4B355754434E4442495A5858555A43454A5A55464552534A4F354C55495353484C4A5756454E53524E5A4C47435552524C4932564F334A564B5A53554D5A335A4B564B4545334358495241545533D3D3D'
```

2. 遇到等号一般都是base家族，但要看清楚是base多少，连着三个等号是base32，连着两个等号一般是base64
3. 做的多了就熟了

编码方式	字符集
base64	a-z,A-Z,+,/ 共64个以及补位的=
base32	A-Z,2-7 共32个以及补位的=
base16	0-9,A-F 共16个以及补位的=

base16就是hex，只不过hex没有=