实验吧隐写术WP(二）

原创

Neil-Yale 于 2017-03-28 15:15:40 发布 6113 收藏

文章标签： 解密 数据 cmd wp ctf

本文链接：https://blog.csdn.net/yalecaltech/article/details/67637275

1.Rose（http://www.shiyanbar.com/ctf/1814）

这题目我做不出来，经过提示，才知道这是steghide

rose.jpg是用steghide加password来隐藏数据的，但是我们不知道password，所以需要爆破

在爆破前，我们要知道手工是怎么做的，大概就是：和mp3steg的使用方法差不多，也是在cmd里代入一个可能的password来解密，并导出key带指定文件。知道流程了，我们就用python来跑

这里用的代码来自pcat

from subprocess import *

```
    def foo():
        stegoFile='rose.jpg'
        extractFile='hide.txt'
        passFile='english.dic'

        errors=['could not extract','steghide --help','Syntax error']
        cmdFormat="steghide extract -sf %s -xf %s -p %s"
        f=open(passFile,'r')

        for line in f.readlines():
            cmd=cmdFormat %(stegoFile,extractFile,line.strip())
            p=Popen(cmd,shell=True,stdout=PIPE,stderr=STDOUT)
            content=unicode(p.stdout.read(),'gbk')
            for err in errors:
                if err in content:
                    break
            else:
                print content,
                print 'the passphrase is %s' %(line.strip())
                f.close()
                return

    if __name__ == '__main__':
        foo()
        print 'ok'
        pass
```

.py,.dic,steghide,rose.jpg需要在同一个文件夹中

运行即可得到flag

2.BrainFuck(http://www.shiyanbar.com/ctf/1821)
之前在杂项写个一个bf的题目，这题也是同理

```
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation。保留所有权利。

C:\Users\hasee>cd C:\Users\hasee\Desktop\CTF工具\bftools

C:\Users\hasee\Desktop\CTF工具\bftools>bftools.exe decode braincopter doge.png --output --dogeout.png
```



```
C:\Users\hasee\Desktop\CTF工具\bftools>bftools.exe decode braincopter doge.png --output --dogeout.png

C:\Users\hasee\Desktop\CTF工具\bftools>bftools.exe run --dogeout.png
Q1RGe0JyYW1uZnVja18xc19TaW1wMWV9
C:\Users\hasee\Desktop\CTF工具\bftools>
```


将字符串base64解码即可

3.认真你就输了(http://www.shiyanbar.com/ctf/1849)
下载后直接在winhex里最开头就看到flag了

beyond | excel_data.xlsx

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	50	4B	03	04	0A	00	00	00	00	00	F4	A4	9E	47	79	F7	PK ô¤▮Gy÷
00000016	80	DE	0A	00	00	00	0A	00	00	00	12	00	00	00	78	6C	▮Þ xl
00000032	2F	63	68	61	72	74	73	2F	66	6C	61	67	2E	74	78	74	/charts/flag.txt
00000048	7B	53	68	31	59	61	6E	42	61	7D	50	4B	03	04	0A	00	{Sh1YanBa}PK
00000064	00	00	00	00	AC	65	5C	46	00	00	00	00	00	00	00	00	¬e\F
00000080	00	00	00	00	09	00	00	00	64	6F	63	50	72	6F	70	73	docProps
00000096	2F	50	4B	03	04	14	00	00	00	08	00	00	00	21	00	83	/PK ! ▮
00000112	6C	B2	07	94	01	00	00	68	03	00	00	10	00	00	00	64	l² ▮ h d
00000128	6F	63	50	72	6F	70	73	2F	61	70	70	2E	78	6D	6C	9D	ocProps/app.xml
00000144	93	CD	6E	DB	30	10	84	EF	05	FA	0E	02	EF	31	E5	C4	▮ÍnÛ0 ▮ï ú ï1åÄ
00000160	28	0A	63	C5	A0	B1	5B	E4	90	A2	06	24	27	E7	35	B5	(cÅ ±[ä ¢ $'ç5µ
00000176	B2	88	50	A4	40	32	82	DD	A7	2F	15	41	B6	9C	F8	D4	²▮P¤@2▮Ý§/ A¶▮øÔ
00000192	DB	EE	CE	60	F8	F1	0F	EE	0F	8D	4E	3A	72	5E	59	93	ÛîÎ`øñ î N:r^Y▮
00000208	B1	F9	2C	65	09	19	69	4B	65	F6	19	DB	16	BF	6E	BE	±ù,e iKeö Û ¿n¾
00000224	B3	C4	07	34	25	6A	6B	28	63	47	F2	EC	5E	7C	FD	02	³Ä 4%jk(cGòì^|ý
00000240	1B	67	5B	72	41	91	4F	62	84	F1	19	AB	43	68	97	9C	g[rA'Ob▮ñ «Ch▮▮
00000256	7B	59	53	83	7E	16	65	13	95	CA	BA	06	43	6C	DD	9E	{YS▮~ e ▮Êº ClÝ▮
00000272	DB	AA	52	92	D6	56	BE	35	64	02	BF	4D	D3	6F	9C	0E	ÛªR'ÖV¾5d ¿MÓo▮
00000288	81	4C	49	E5	4D	7B	0A	64	43	E2	B2	0B	FF	1B	5A	5A	LIåM{ dCâ² ÿ ZZ
00000304	D9	F3	F9	E7	E2	D8	C6	3C	01	3F	DA	56	2B	89	41	59	Ùóùçâ0Æ< ?ÚV+▮AY
00000320	23	7E	2B	E9	AC	B7	55	48	7E	1E	24	69	E0	53	11	62	#~+é¬·UH~ $iàS b
00000336	50	4E	F2	CD	A9	70	14	29	F0	69	0B	B9	44	4D	AB	18	PNòÍ©p)ði ¹DM«
00000352	2C	2A	D4	9F	80	9F	07	F0	48	D8	1F	DA	06	95	E3	02	*Ô▮▮▮ ðHØ Ú ▮ã

4.复杂的QR_code（http://www.shiyanbar.com/ctf/1856）

用kali

binwalk发现zip

-e 提取

发现需要密码，这是发现提取中的文件夹的txt提示4Number,也就是4个数字，于是暴力得到密码

解压即可