bugku的杂项writeup（一）

原创

「已注销」 于 2019-08-12 22:20:15 发布 222 收藏 2

分类专栏： bugku 杂项 writeup 文章标签： bugku 杂项 前8题

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_43342135/article/details/99305659

版权

bugku 同时被 2 个专栏收录

6 篇文章 0 订阅

订阅专栏

杂项 writeup

1 篇文章 0 订阅

订阅专栏

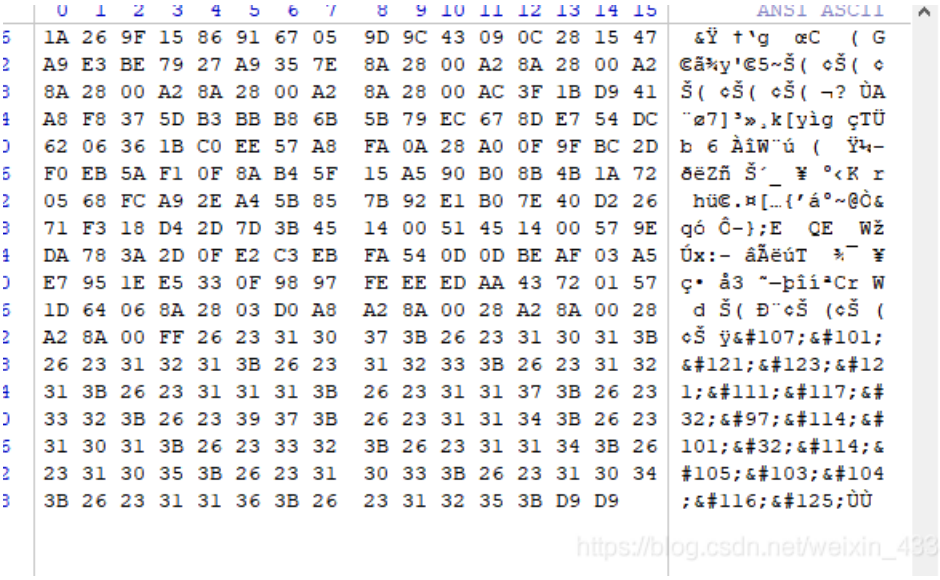
1.签到题：

关注公众号Bugku得到flag：

flag{BugKu-Sec-pwn!}

2.这是一张单纯的图片

拿到这张图片后，用winhex打开，发现文件的末尾多出异常的字符：



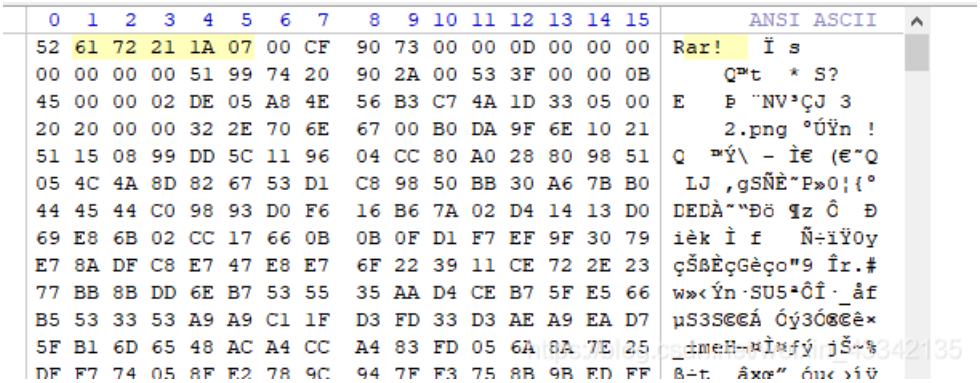
```
          0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15        ANSI ASCII
5   1A 26 9F 15 86 91 67 05  9D 9C 43 09 0C 28 15 47   &Ÿ †'g  œC  ( G
2   A9 E3 BE 79 27 A9 35 7E  8A 28 00 A2 8A 28 00 A2  ©ã¾y'©5~Š( ¢Š( ¢
3   8A 28 00 A2 8A 28 00 A2  8A 28 00 AC 3F 1B D9 41  Š( ¢Š( ¢Š( ¬? ÙA
4   A8 F8 37 5D B3 BB B8 6B  5B 79 EC 67 8D E7 54 DC  ¨ø7]³»¸k[yìg çTÜ
D   62 06 36 1B C0 EE 57 A8  FA 0A 28 A0 0F 9F BC 2D  b 6 ÀîW¨ú (  Ÿ¼-
5   F0 EB 5A F1 0F 8A B4 5F  15 A5 90 B0 8B 4B 1A 72  ðëZñ Š´_ ¥ °‹K r
2   05 68 FC A9 2E A4 5B 85  7B 92 E1 B0 7E 40 D2 26   hü©.¤[…{'á°~@Ò&
3   71 F3 18 D4 2D 7D 3B 45  14 00 51 45 14 00 57 9E  qó Ô-};E  QE  Wž
4   DA 78 3A 2D 0F E2 C3 EB  FA 54 0D 0D BE AF 03 A5  Úx:- âÃëúT  ¾¯ ¥
D   E7 95 1E E5 33 0F 98 97  FE EE ED AA 43 72 01 57  ç• å3 ˜—þîíªCr W
5   1D 64 06 8A 28 03 D0 A8  A2 8A 00 28 A2 8A 00 28   d Š( Ð¨¢Š (¢Š (
2   A2 8A 00 FF 26 23 31 30  37 3B 26 23 31 30 31 3B  ¢Š ÿ&#107;&#101;
3   26 23 31 32 31 3B 26 23  31 32 33 3B 26 23 31 32  &#121;&#123;&#12
4   31 3B 26 23 31 31 31 3B  26 23 31 31 37 3B 26 23  1;&#111;&#117;&#
D   33 32 3B 26 23 39 37 3B  26 23 31 31 34 3B 26 23  32;&#97;&#114;&#
5   31 30 31 3B 26 23 33 32  3B 26 23 31 31 34 3B 26  101;&#32;&#114;&
2   23 31 30 35 3B 26 23 31  30 33 3B 26 23 31 30 34  #105;&#103;&#104
3   3B 26 23 31 31 36 3B 26  23 31 32 35 3B D9 D9     ;&#116;&#125;ÙÙ
```

https://blog.csdn.net/weixin_43342135

拿去unicode解码后得到flag：

3.隐写

下载文件之后，用winhex打开查看文件是否存在隐藏文件，结果发现没有隐藏文件只有一张图片。



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar! Ï s
	00	00	00	00	51	99	74	20	90	2A	00	53	3F	00	00	0B	Q™t * S?
	45	00	00	02	DE	05	A8	4E	56	B3	C7	4A	1D	33	05	00	E Þ ¨NV³ÇJ 3
	20	20	00	00	32	2E	70	6E	67	00	B0	DA	9F	6E	10	21	2.png °ÚŸn !
	51	15	08	99	DD	5C	11	96	04	CC	80	A0	28	80	98	51	Q ™Ý\ – Ì€ (€˜Q
	05	4C	4A	8D	82	67	53	D1	C8	98	50	BB	30	A6	7B	B0	LJ ,gSÑÈ˜P»0¦{°
	44	45	44	C0	98	93	D0	F6	16	B6	7A	02	D4	14	13	D0	DEDÀ˜"Ðö ¶z Ô Ð
	69	E8	6B	02	CC	17	66	0B	0B	0F	D1	F7	EF	9F	30	79	ièk Ì f Ñ÷ïŸ0y
	E7	8A	DF	C8	E7	47	E8	E7	6F	22	39	11	CE	72	2E	23	çŠßÈçGèço"9 Îr.#
	77	BB	8B	DD	6E	B7	53	55	35	AA	D4	CE	B7	5F	E5	66	w»‹Ýn·SU5ªÔÎ·_åf
	B5	53	33	53	A9	A9	C1	1F	D3	FD	33	D3	AE	A9	EA	D7	µS3S©©Á Óý3Ó®©ê×
	5F	B1	6D	65	48	AC	A4	CC	A4	83	FD	05	6A	8A	7E	25	_±meH¬¤Ì¤ƒý jŠ~%
	DF	F7	74	05	8F	E2	78	9C	94	7F	E3	75	8B	9B	ED	FF	ß÷t âxœ" ãu‹›íÿ

解压图片后，用winhex打开，发现了图片的长宽高并不一样，将A4修改成F4，于是进行修改，再次打开文件发现flag：

BUGKU{a1e5aSA}

4.telnet

下载文件发现文件为pcap文件，用Wireshark打开后，先tcp流看一下，发现了flag：

5.眼见非实(ISCCCTF)

下载文件，用winhex打开，发现是zip文件，修改文件名，加个前缀改为1.zip文件，解压后得到了眼见非实.docx，丢进winhex里面，发现还是个压缩包，修改文件名后，打开zip文件，解压后，一个一个的word寻找flag，最终在：

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
_rels			文件夹	2016/8/15 4:06	
theme			文件夹	2016/8/15 4:06	
document.xml	1,912	661	XML 文件	1980/1/1 0:00	8B729375
fontTable.xml	1,552	521	XML 文件	1980/1/1 0:00	0C6EBA5F
settings.xml	2,844	1,089	XML 文件	1980/1/1 0:00	BFDC20...

发现了flag：

6.啊哒

下载文件后，用winhex打开，发现只有一张图片，将图片解压下来之后：

https://blog.csdn.net/weixin_43342135

用winhex打开，发现隐藏zip文件，直接修改文件名字zip格式，发现了flag.txt:（后来看题解说是丢到虚拟机用binwalk分理处zip文件，再解压得到flag.txt,同样要密码）

https://blog.csdn.net/weixin_43342135

密码藏得很深，看完writeup后知道在文件的属性里面，有密码key是被加密了的

```
73646E6973635F32303138
```

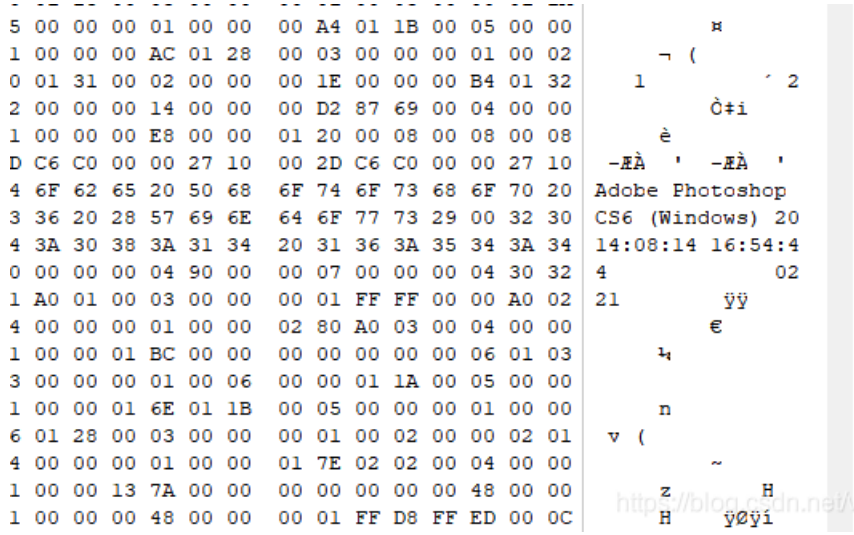
16进制转换字符串得到密码：`sdnisc_2018`

https://www.sojson.com/hexadecimal.html

zip解密得到flag

7.又一张图片，还单纯吗

下载图片后，用winhex打开，发现了隐藏文件决定，修改成zip，但是这里失败了，无法打开文件。于是就决定了采用binwalk来



分离图片，提取隐藏的图片。

```
binwalk命令：
ls

binwalk 2.jpg

dd if=2.jpg of=2-1.jpg skip=158792 bs=1
```

falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

https://blog.csdn.net/weixin_43342135

这里转载一篇写的比较好的博客：https://www.jianshu.com/p/176d12355d74

8.猜

在用一堆工具和修复长宽高无效后，参考writeup才知道直接百度识图就行了，
识别出来是刘亦菲，直接提交就ok
key{liuyifei}

创作打卡挑战赛

赢取流量/现金/CSDN周边激励大奖