Bugku杂项题目解析



<u>北岸冷若冰霜</u> ● 于 2020-07-31 20:17:18 发布 ● 5255 ☆ 收藏 14 分类专栏: <u># CTF夺旗 安全</u> 文章标签: <u>信息安全</u> 网络安全 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/u013469753/article/details/107720551</u> 版权



CTF夺旗同时被2个专栏收录

7篇文章2订阅 订阅专栏



34 篇文章 3 订阅 订阅专栏

Bugku杂项

目录

Bugku杂项

9. 苋 审 信 忌 准 路 10.隐写2 11、多种方法解决 12.闪的好快 13.Come_game 14.linux 15、隐写3 16、做个游戏 17、想蹭网先解开密码 18、Linux2 19、号被盗了 20、细心的大象 21、爆照 22、猫片(安恒) 23.多彩 24、旋转的跳跃 25.普通的二维码 26.乌云邀请码 27、神秘的文件 28图穷匕见 29、convert 30.听首音乐 31.好多数值 32、很普通的数独 33.PEN_AND_APPLE 34.你见过彩虹吗 35.好多压缩包 36.一个普通胡的压缩包 37.2B 40妹子的陌陌 41.就五层你能解开吗? 论剑

1.签到题

2.这是一张单纯的图片

解析: 直接使用命令cat 1.jpg 最后一行的的信息,可知使用了base解密。

key{you are right}

在站长之家base解密

答案:

key{you are right}

3.隐写

参考链接

解析:

urar e 2.rar



https://blog.csdn.net/u013469753

然后,用winhex打开2.png,将A4改成F4,则接触flag

🚟 WinHex - [2.png]

Eile Edit Search Navigation View Tools Specialist Options Window Help

Case Data	🗅 🛃 🔚 🤩 📚 💕 📑 🗍 🐃 🐚	🛅 🖻 🐎 🎮 🛤 🎎 🎎 → 🕀 🖛 → 🥃	è 🕹 🖗 🎟 🔎 🦚 🕍 🏶 👯 🖬 🖌 🚩
Fi <u>l</u> e E <u>d</u> it	2.png		
	Offset 0 1 2 3 4	56789ABCDEF	ANSI ASCII 🔺
Data Interpreter ×	00000000 89 50 4E 47 0D	0A 1A 0A 00 00 00 0D 49 48 44 52 %	bPNG IHDR
9 Dit (+): 02	00000010 00 00 01 F4 00	00 01 A4 08 06 00 00 00 CB D6 DF	ô 🚥 ËÖß
$16 \text{ Pit}(\pm): 2 212$	00000020 8A 00 00 00 09	70 48 59 73 00 00 12 74 00 00 12 š	Š pHYs t
32 Bit (+): 205 /28	00000030 74 01 DE 66 1F	78 00 00 0A 4D 69 43 43 50 50 68 t	t Þf x MiCCPPh
52 bit (±), 555,420	00000040 6F 74 6F 73 68	6F 70 20 49 43 43 20 70 72 6F 66 c	otoshop ICC prof
	00000050 69 60 65 00 00	78 DA 9D 53 77 58 93 F7 16 3E DF i	ile xÚ SwX"÷ >ß
	00000060 F7 65 0F 56 42	D8 F0 B1 97 6C 81 00 22 23 AC 08 ÷	÷e VBØð±−1 "#¬
	00000070 C8 10 59 A2 10	92 00 61 84 10 12 40 C5 85 88 0A È	È Y¢ / a,, @A



BUGKU{a1e5aSA}

https://blog.csdn.net/u013469753

4.telnet

参考链接

解析:

下载压缩包,	发现里面是pcap文件格式,	使用wireshark打开,	右击杳看TCP数据流
	次·加王田之中000户入111日207		

1 0.0000 192.168.221.128	192.168.2	21.1 TCP	66 1146 → 23 [SYN] Seq=0 Win=8192 Len=0 MSS=14
3 0.0468 192.168.221.128	192.168.2	21.1 TCP	54 1146 → 23 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4 0.0780 192.168.221.128	192.168.2	21.1 TEL	75 Telnet Data
7 4.5552 192.168.221.128	192.168.2	21.1 TEL	57 Telnet Data
9 4.6488 192.168.221.128	192.168.2	21.1 TEL	63 Telnet Data
11 4.7268 192.168.221.128	标记/取消标记分组(M)	Ctrl+M	71 Telnet Data
12 4.7580 192.168.221.128	忽略/取消忽略 分组(<u>l</u>)	Ctrl+D	60 Telnet Data
13 4.7892 192.168.221.128	设置/取消设置 时间参考	Ctrl+T	65 Telnet Data
16 4.8984 192.168.221.128	时间平移	Ctrl+Shift+T	57 Telnet Data
17 4.9296 192.168.221.128	分组注释	Ctrl+Alt+C	57 Telnet Data
18 4.9608 192.168.221.128	疟 姆解析的 2 秒		57 Telnet Data
21 5.0232 192.168.221.128	9册+时用11日31日1157		54 1146 → 23 [ACK] Seq=77 Ack=72 Win=65536 Len
23 5,0388 192,168,221,128	作为过滤器应用	•	54 1146 → 23 [ACK] Seq=77 Ack=108 Win=65536 Le
24 16,114 192,168,221,128	准备过滤器	•	55 Telnet Data
26 16.177 192.168.221.128	对话过滤器	•	54 1146 → 23 [ACK] Seq=78 Ack=109 Win=65536 Le
	对话着色	•	EE Tolnot Data
	SCTP	•	
rame 9: 63 bytes on wire (504 bits), 63 bytes	追踪流	•	
thernet II, Src: Vmware_84:86:5f (00:0c:29:84	复制	•	:0c:29:26:7e:0e)
ternet Protocol Version 4, Src: 192.168.221.	SKIPS		
ransmission Control Protocol, Src Port: 1146,	协议首选项	•	Len: 9
Source Port: 1146	解码为(<u>A</u>)		
Destination Port: 23	在新窗口显示分组(<u>W)</u>		https://blog.cedp.pet/u012/60752
[Stream index: 0]			- nups.//biog.csun.netuo15403755

答案:

flag{d316759c281bf925d600be698a4973d5}

5.眼见非实(ISCCCTF)

下载文件后修改文件,将zip文件名添加文件类型即zip.zip

	Microsoft Word 很抱歉,无法打开 眼见非实.docx,因为内容有问 确定	? ×)题。 详细信息(<u>D</u>) >>>	
名称	修改日期	类型	大小
🗋 zip	2018/11/1 18:00	文件	11 KB
🔋 zip.zip	2018/11/1 18:00	压缩(zipped)文件	11 KB
名称	类型	压缩大小	密码保护
🚽 眼见非实.docx	Microsoft Word 文档		11 KB 否

解析:

解压后得到一个图片,先使用binwalk分析图片,图片里面隐藏一段tiff信息以及一个压缩包且压缩包被加密

			a	dmin@kali: ~/ada	×
文件(F)	编辑(E) 查看	f(V) 搜索(S)	终端(T)	帮助(H)	
admin@k	ali:~/ada\$	pwd			
admin@k	ali:~/ada\$	binwalk 1c	df3a75-	21ed-4b91-8d49-1b348d44dcf.zip	
DECIMAL	HEXA	DECIMAL	DESC	RIPTION	
0 ssed si 201880	0x0 ze: 201754, 0x31	uncompres	Zip a sed siz End c	archive data, at least v2.0 to e ze: 218957, name: ada.jpg of Zip archive, footer length: 2	xtract, compre
admin@k Archive infla admin@k 1cdf3a7 admin@k	ali:~/ada\$:: 1cdf3a75 ting: ada.j ali:~/ada\$ 5-21ed-4b91 ali:~/ada\$	unzip 1cdf 5-21ed-4b93 pg ls L-8d49-1b34 binwalk ac	3a75-21 -8d49-1 8 <mark>8d44dc1</mark> la.jpg	Led-4b91-8d49-1b348d44dcf.zip Lb348d44dcf.zip f .zip ada.jpg	
DECIMAL	. HEXA	DECIMAL	DESCR	RIPTION	
0 30 direct	0x0 0x1E ory: 8		JPEG TIFF	image data, JFIF standard 1.01 image data, big-endian, offset	of first image
5236 218773 ct, com 218935	0x14 0x35 pressed siz 0x35	174 5695 2e: 34, uno 5737	Copyr Zip a compress End c	right string: "Copyright Apple I archive data, encrypted at least sed size: 22, name: flag.txt of Zip archive, footer length: 2	nc., 2018" v2.0 to extra 22
admin@k	ali:~/ada\$			https://blog.csd	In.net/u013469753

查看图片文件属性

	8									
基本	权限	打开方式	图像							
图像类型	jpeg (JPEG)									
宽度	826 像素	826 像素								
高度	672 像素	672 像素								
相机型号	73646E6973635F	32303138								

73646E6973635F32303138

然后进行:十六进制转字符串

16进制到文本字符串的转换,在线实时转换 16进制到文本字符串的转换,在线实时转换(支持中文转换)							
加密或解密字符串长度不可以超过10M							
73646E6973635F32303138							
	/						
16进制转字符 字符转16进制 清空结果							
sdnisc_2018							

得到解压密码sdnisc_2018

解压: unzip

`[w<mark>admin@kali:~/ada</mark>\$ ls lcdf3a75-21ed-4b91-8d49-1b348d44dcf.zip ada.jpg _ada.jpg.extracted min@kali:~/ada\$ cd _ada.jpg.extracted/
min@kali:~/ada/_ada.jpg.extracted\$ ls min@kati://doc/______ 695.zip flag.txt min@kali:~/ada/_ada.jpg.extracted\$ cat flag.txt min@kali:~/ada/_ada.jpg.extracted\$ unzip 35695.zip Archive: 35695.zip [35695.zip] flag.txt password: skipping: flag.txt incorrect password in@kali:~/ada/_ada.jpg.extracted\$ ls
95.zip flag.txt @kali:~/ada/_ada.jpg.extracted\$ unzip 35695.zip Archive: 35695.zip [35695.zip] flag.txt password: replace flag.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y extracting: flag.txt li:~/ada/_ada.jpg.extracted\$ cat flag.txt flag{3XiF iNf0rM@ti0n}admin@kali:~/ada/_ada.jpg.extracted\$ https://blog.csdn.net/u013469753

答案: flag{3XiF_iNf0rM@ti0n}

7.又一张图片,还单纯吗

解析: 放进kali, binwalk查看里面竟然还有有个图片,使用foremost 分离文件 拿到flag!

foremost 2.jpg

进入output文件夹, flag图片已分离

答案:

falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

8.猜

解析: 直接百度识图

答案**:** key{liuyifei}

9.宽带信息泄露

解析:

下载routerpassview工具

然后使用该工具查看,即可得到flag

<x_tp_ifname val="eth1"></x_tp_ifname>				
<wanipconnection nextinstance="3"></wanipconnection>				
<wanpppconnection instance="1"></wanpppconnection>				
<enable val="1"></enable>	***		×	
<defaultgateway val="10.177.144.1"></defaultgateway>	重找		×	
<name val="pppoe_eth1_d"></name>				
<uptime val="671521"></uptime>	查找内容(N): name		查找下一个(F)	
<user<mark>name val=053700357621 /></user<mark>				
<password val="210265"></password>		古向	取選	
<x_tp_ifname val="ppp0"></x_tp_ifname>	□ 全子匹配(<u>W</u>)	1 Control of the second	40(16)	
<x_tp_l2ifname val="eth1"></x_tp_l2ifname>				
<x_tp_connectionid val="1"></x_tp_connectionid>	□区分大小写(C)	CHIG CHIG		
<pre><externalipaddress val="10.177.150.82"></externalipaddress></pre>				
<pre><remoteipaddress val="10.177.144.1"></remoteipaddress></pre>				
<pre><dnsservers <="" pre="" val="202.102.152.3,202.102.154.3"></dnsservers></pre>	>			
<macaddress val="D0:C7:C0:43:53:69"></macaddress>				
<wanpppconnection nextinstance="2"></wanpppconnection>				
<wanconnectiondevice nextinstance="2"></wanconnectiondevice>				
<wandevice nextinstance="2"></wandevice>				
<x firewall="" tp=""></x>				
<pre></pre> <pre></pre> <pre></pre>				
<refcnt val="1"></refcnt>				
<tune val="1"></tune>				
<pre><entryname val="childMac1"></entryname></pre>				
<pre><cntryname val="childMac1"></cntryname> <isparentctrl val="1"></isparentctrl></pre>				
<entryname val="childMac1"></entryname> <isparentctrl val="1"></isparentctrl> 				
<pre><entryname val="childMac1"></entryname> <isparentctrl val="1"></isparentctrl> <internalhost instance="2"></internalhost></pre>				
<pre><entryname val="childMac1"></entryname> <isparentctrl val="1"></isparentctrl> <internalhost instance="2"> <refcnt val="1"></refcnt></internalhost></pre>				
<pre><entryname val="childMac1"></entryname> <isparentctrl val="1"></isparentctrl> <internalhost instance="2"> <refcnt val="1"></refcnt> <tupe val="1"></tupe></internalhost></pre>				
<pre><entryname val="childMac1"></entryname> <isparentctrl val="1"></isparentctrl> <internalhost instance="2"> <refcnt val="1"></refcnt> <type val="1"></type> <entrvname val="childMac2"></entrvname></internalhost></pre>				
<pre><entryname val="childMac1"></entryname> <isparentctrl val="1"></isparentctrl> <internalhost instance="2"> <refcnt val="1"></refcnt> <type val="1"></type> <entryname val="childMac2"></entryname> <isparentctrl val="1"></isparentctrl></internalhost></pre>				
<pre><entryname val="childMac1"></entryname> <isparentctrl val="1"></isparentctrl> <internalhost instance="2"> <refcnt val="1"></refcnt> <type val="1"></type> <entryname val="childMac2"></entryname> <isparentctrl val="1"></isparentctrl> </internalhost></pre>				
<pre><entryname val="childMac1"></entryname> <isparentctrl val="1"></isparentctrl> <internalhost instance="2"> <refcnt val="1"></refcnt> <type val="1"></type> <entryname val="childMac2"></entryname> <isparentctrl val="1"></isparentctrl> </internalhost></pre>				

答案: flag{053700357621}

10.隐写2

解析:

```
28 binwalk Welcome_.jpg
29 binwalk -e Welcome_.jpg
30 ls
31 cd _Welcome_.jpg.extracted/
32 ls
33 unrar e flag.rar
34 ls
35 crunch 3 3 1234567890 -o pass.txt
36 fcrackzip -D -p pass.txt -u flag.rar -v
37 cat 3.jpg
```

		admin@kali: ~/9	
文件(F) 编	辑(E) 查看(V) 搜索(S)	终端(T) 帮助(H)	
admin@kali	i:∼/9\$ binwalk Wel	comejpg	^
DECIMAL	HEXADECIMAL	DESCRIPTION	
0 30 directory	0x0 0x1E /: 8	JPEG image data, JFIF standard 1.0 TIFF image data, big-endian, offset	L t of first image
52516 ssed size: 59264 147852	0xCD24 : 6732, uncompress 0xE780 0x2418C	Zip archive data, at least v1.0 to ed size: 6732, name: flag.rar End of Zip archive, footer length: End of Zip archive, footer length:	extract, compre 22 22
admin@kali	i:~/9\$ binwalk -e	Welcomejpg	
DECIMAL	HEXADECIMAL	DESCRIPTION	
0 30 directory	0x0 0x1E v: 8	JPEG image data, JFIF standard 1.0 TIFF image data, big-endian, offset	L t of first image
52516 ssed size: 59264 147852	0xCD24 : 6732, uncompress 0xE780 0x2418C	Zip archive data, at least v1.0 to ed size: 6732, name: flag.rar End of Zip archive, footer length: End of Zip archive, footer length:	extract, compre 22 22
admin@kali	i:~/9\$	https://blog.c	csdn.net/u01346975

admin@kali: ~/9/_Welcome_.jpg.extracted 00 8 文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H) kali:~/9/_Welcome_.jpg.extracted\$ unrar e flag.rar UNRAR 5.50 freeware Copyright (c) 1993-2017 Alexander Roshal flag.rar is not RAR archive No files to extract admin@kali:~/9/_Welcome_.jpg.extracted\$ ls CD24.zip flag.rar 提示.jpg admin@kali:~/9/_Welcome_.jpg.extracted\$ crunch 3 3 1234567890 -o pass.txt Crunch will now generate the following amount of data: 4000 bytes 0 MB 0 GB 0 TB 0 PB Crunch will now generate the following number of lines: 1000 crunch: 100% completed generating output dmin@kali:~/9/_Welcome_.jpg.extracted\$ frag fragroute fragrouter fragtest kali:~/9/_Welcome_.jpg.extracted\$ fcrackzip -D -p pass.txt -u flag.rar -v found file '3.jpg', (size cp/uc 6588/ 6769, flags 801, chk 102c) PASSWORD FOUND!!!!: pw == 871 https://blog.csdn.net/u013469753 akali:~/9/ Welcome .ipg.extracted\$

9 _Welcomeg.ex	xtracted 🔻		C III ▼ III ■ C C HINCO-444, HIED/484. HINI ■ E III ■ C C HINI ■ E IIII ■ C C HINI ■ E IIIII ■ C C HINI ■ E IIIIII ■ C C HINI ■ C C C C C C C C C C C C C C C C C C
CD24.zip	flag.rar	pass.txt	提示.jpg
	取消(C)	提取文件	确定(O)
	"flag.rar"需要密码	冯	
	密码(P):		
	•••		0



cat 3.jpg之后,对做base解密, base64解密: https://base64.supfree.net/ http://tool.chinaz.com/tools/base64.aspx

f1@g{eTB1IEFyZSBhIGhAY2tlciE=}

输入: eTB1IEFyZSBhIGhAY2tlciE=

答案: flg{y0u Are a h@cker!}

11、多种方法解决

解析: 先使用unzip 3.zip解压得到KEY.exe cat KEY.exe 根据提示有一张二维码

 CatKEY.exe,然后做base64转码

 

 9rX03941LV76cbeH88dvtP-3pnD94/FrheQvmcZu/21f78zh45i50yx4137200/

 9rX03941LV76cbeH88dvtP-3pnD94/FrheQvmcZu/21f78zh45i50yx4137200/

 9rX03941LV76cbeH88dvtP-3pnD94/FrheQvmcZu/21f78zh45i50yx4137200/

 9rX03941LV76cbeH88dvtP-3pnD94/FrheQvmcZu/21f78zh45i50yx4137200/

 9rX03941LV76cbeH88dvtP-3pnD94/FrheQvmcZu/21f78zh45i50yx4137200/

 9rX03941LV76cbeH88dvtP-3pnD94/FrheQvmcZu/21f78zh45131247835

 9rX03941LV76cbeH88dvtP-3pnD94/FrheQvmcZu/21f7124H710x513141835

 9rX03941LV76cbeH88dvtP-3pnD948428kd47tu3129yx304897XrH4L876rM212hH8453x002

 9rX03941LV76cbeH884016m428kd47tu3129yx304897XrH4L876rM212hH8453x002

 9rX0498428kd47tu3129yx304897XrH4L876rM212hH8478x484784b3x002

 9rX049877H1vct54mvM84b38647tu31c9yx304897XrH4L8767V412hH8478x487414b35x002



3LCft01/ae9Z1To+2

410W051F+/00MJC500 k0jbaYkdaansfttbpK 5vApyd+8y5/29c4cPi ZbpDfepr0imlieZaGd

答案: KEY{dca57f966e4e4e31fd5b15417da63269}

12.闪的好快

解析: 将git图片逐帧分解,扫描一堆二维码的到flag, GIF分解工具: 在线分解https://tu.sioe.cn/gj/fenjie 本地分解: GifSplitter

答案: SYC{F1aSh_so_f4sT}

13.Come_game

Bugku Come_game 参考链接

SYC{6E23F259D98DF153}

14.linux

tar -xvf 1.tar.gz

🥘 flag - 记事本		_	\times
文件(F) 编辑(E) 格式(C	D) 査看(V) 帮助(H)		
[Trash	Info]Path=gameDeletionDate=2016-06-27T12:27:37		^
	查找 ×		
	查找内容(N): key 查找下一个(E) 方向 取消		
		key{}	
	key{feb81d3834e2423c9903f4755464060b}		
			1697 <mark>53</mark>
	http		169753

key{feb81d3834e2423c9903f4755464060b}

15、隐写3

🚃 winnex - [dabai.png]

<u>File Edit Search Navigation View Tools Specialist Options Window Help</u>

Case Data	🗅 🚬 🗔 😂 8	ء 🖻		-) 🗈	1	ī B	010 010	2	A M	HEX	16 (ie×	-	-100			ا 🕂 ⊾ 🔝 🖇 🕍 🕸 🖉 🏈 😂 🗳
Fi <u>l</u> e E <u>d</u> it	2.png dabai.	png																
	Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII 🔺
Data Interpreter	00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
$9 \text{ Pit}(+) \cdot 17$	00000016	00	00	02	Α7	00	00	1 1	00	80	06	00	00	00	6D	7C	71	§ m q
$16 \text{ Bit } (\pm) \cdot 17$	00000032	35	00	00	00	01	73	52	47	42	00	AE	CE	1C	Ε9	00	00	5 sRGB ©Î é
32 Bit (+): 101 187 601	00000048	00	04	67	41	4D	41	00	00	B1	8F	0B	\mathbf{FC}	61	05	00	00	gAMA ± üa
32 Bit (1), 101,107,001	00000064	00	09	70	48	59	73	00	00	0E	C4	00	00	0E	C4	01	95	pHYs Ä Ä •
	00000080	2B	0E	1B	00	00	FF .	A5	49	44	41	54	78	5E	EC	BD	07	+ ÿ¥IDATx^ì½
	00000096	A 0	A5	57	59	EE	FF	EE	BE	4F	9B	DE	93	4C	7A	0F	84	¥WYîÿî¾O>Þ"Lz "
	00000112	24	24	60	0C	04	A5	2в	20	45	10	10	BB	88	8A	A 8	57	\$\$` ¥+ E ≫^Ѝ₩
	00000128	BD	\mathbf{FC}	EF	BD	7A	F5	5A	AE	7A	BD	5E	СВ	BD	2A	62	05	¼üï¾zõZ®z¼^˽*b
	00000144	04	69	52	04	E9	01	42	48	48	42	7A	EF	7D	52	A6	CF	iR é BHHBzï}R¦Ï
	00000160	9C	7E	76	FD	ЗF	BF	F7	DB	EF	39	6B	76	F6	4C	26	C9	œ~vý?;÷Ûï9kvöL&É
	00000176	4C	32	E5	7в	CE	59	7в	F5	DE	9E	6F	7D	6В	AD	AF	D0	L2å{ÎY{õÞžo}k- Đ
	00000192	15	2C	47	8E	1C	39	72	1C	90	60	88	2E	14	0A	3D	DD	,GŽ 9r `^. =Ý
	00000208	DE	63	6F	FD	A5	53	C0	93	8D	Α7	D3	Ε9	F4	54	66	C5	Þcoý¥SÀ" §ÓéôTfÅ
	00000224	62	D1	E5	34	BC	34	0D	AD	56	СВ	1A	8D	86	35	9B	4D	bÑå4¼4 -VË †5>M
	00000240	17	в3	в3	в3	36	37	37	E7	72	98	21	70	87	DC	6E	в7	***677çr~!p‡Ün•
	00000256	ЗD	FC	90	01	E1	11	0F	61	22	CA	E5	в2	8B	4A	A5	62	=ü á a"Êå° <j¥b<sup>ips"/blog.csdn.net/u013469753</j¥b<sup>

```
保存,再次打开图片可知
```

🐠 🖬 🦻 ୯	≂ dabai.png - 画图														-
文件 主武	查看														
▲ 剪切 約 复制 粘贴	ば 裁剪 「」重新调整大小 选 选 译 子 "↓ 旋转 •	/ & A / / & Q	↓ <		企鄭 - 真充 - 粗 细 -	颜 ē 61 色				使用画图 3 D 进行编辑	〕 产品 提醒				
剪贴板	图像	工具		形状				颜色							
0	100 200	300	400	500	700	800	900	1000	1100	1200	1300	1400	1500	1600	1700
500	0~~		flag(He	10_d4_be1}											

flag{He1I0_d4_ba1}

16、做个游戏

jd-gui工具 https://github.com/java-decompiler/jd-gui/releases Java环境 https://www.java.com/zh_CN/download/windows-64bit.jsp 直接用jd-jui打开heihei.jar文件



flag{RGFqaURhbGlfSmlud2FuQ2hpamk=} 直接输入后提示错误,现对: RGFqaURhbGlfSmlud2FuQ2hpamk= 做base64进行编码 http://tool.chinaz.com/Tools/Base64.aspx

DajiDali_JinwanChiji

所以flag为

flag{DajiDali_JinwanChiji}

17、想蹭网先解开密码

(1) 生成长度为4位,且以"R开头+三位数字"的密码

crunch 4 4 -t R%%%

(2) 生成长度为6的纯数字密码

crunch 6 6 -t %%%%%%

按提示生成1391040开头的手机号码并存入pass.txt

crunch 11 11 -t 1391040%%%% -o pass.txt

aircrack-ng wifi.cap -w pas<u>s.txt</u>



选择3,即WPA

人件 开始 储入	
[00:00:01] 768	8/9999 keys tested (4927.40 k/s)
Time left: 0 s	aconds - 页面标题 新建大小 缩小 放大 有1.89% 新建窗口 新建 新建快速笔记 停靠窗口
视图	KEY FOUND! [13910407686] 富二
🔟 OneNote 笔i	
Master Key	: C4 60 FE 8B 14 7D 58 00 91 D7 0A 9C 3C DE 44 69 0B E1 CD 81 07 F8 28 DB EA 76 1E ED 81 A3 FF FD
Transient Kev	
安全课程问题	
基础课程	
攻防平台 EAPOL HMAC	: 1C E7 D0 96 DE 87 93 56 88 1D 08 C8 B9 AA B3 B0
admin@kali:~/16\$	
NetEP	2. 生成长度为6的纯数字镭https://blog.csdn.net/u013469753

flag{13910407686}

18、Linux2

依然是记事本打开 📗 brave - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) 見像 羧mWコRA鼈銒?<?2e险聪5×罟K□M□€□伽?□□GO?II辒F)8 ?蘑 惉(凵g;荮笲焮豼傤rsc?変□?牸Q霆?v|sp钉 幼F/T□穒9垉烃/?□饩魆破駊□6□?汛□哟□ 季□?r}?(⑷□隍h姕Z圀"◆T?□陈??饰荪?□?e瀱p猲*渶鯦衢g崆4 S??□c?臗縭vG錤2葛舟?8tnHN涀糖暢紙獵铒杌??绞膉夽i{涫?t恒婈|芭輦xqr镡N┥?ykF);;;[] :騌岲??□啼?k?輻?霚鏡'?譇G汁0k晅 □硊? p浵t渆蝤'F衃1A{H灃%??}-給??7輵%Y?-Q菱碴#历?g啅u%擡磲y_傐?1\鯍?4?肝蹢鳃琜礋泵?(辔阑5儢%2□釹]o? 伐"#f□&^慗~诟0々<\$Q?讐硲Q桚^?M★寙}^睶??古譲晵???*㎝□∕\愍N炷P袢@R 巤佑?D燣Y7/□鵌縷W"C庒p0鐣=骤暆, [櫨 ┅□=阺?;□圄?`v报邹萯 厱;呗? \$8:稑臰U42?佖晝I □z6+ □D€\ ■ b棴◎?耡d&佧~刿e饺蜪槒\$□u?尟堩□搜I余秛[E□□莳?帾?r胭楆Gk #}啖闆?擛1疌3?焓^A?□暘y12観邴□~fi嶙j峴n空 喔? ›B}@圳僧A龐♠ BwF ?R;DRkO\$?r□5錫At BI矇□啊□z殮沣f滪&+煭Bd?-L勖\$N♠?"闎維v襳宮R□朴\$a9,?ow苫B~K漲挢□9I嚔痖 K♠?t寠;?□'□?p{t泗Tl□c敃□豴 :6.矮□飐\K_崳□餅扐aY]□鯔峧?蔃i踏)廻□嘩篚?[□???fE?X狜輮□X蹟{鴒搌0□?譎絧bo1s□?u]?8鋕□銑~ㄣ曑 :?□□ 赶器C Box?疛乏□W:!m□~ ??嵖?鐸兌h銜 尤 OPH 查找 × p\$兒紩律割j ?鞸?G芪l圮x! 廫洏″%?9挒%楮?wof:owo#o鱔?a楅i蘉m濾珚k桪湈8唧麐躿 k 續? 插 ?)+ 血u 缡 鹊 ≈?8 褌 vm/? 擋 @K 紪 **ぃ** 軭 附 V □ 綬 獧 曝, 駪? □ □ c? 骐 [L, 翕 □ m; j □ 鸭 扄?? 灰?H\$![查找下一个(E) 查找内容(<u>N</u>): key WKs=¤]e鰪□LiC鑑?k碠x舋p□越?□?豛Y澖?X□?髬ヾv??□爵\$i醹餑1 帘?梛??Q?Z媅侷[h涉J?虞萘& B8鏡: #}≔?6p%?j?C?堈鞱□?D敂呍?n-□6洚|农!鏓uNV钂?h媔■蠏[湯/?6K^韖厨)'.7(□? 銩烕筱□ 方向 取消 九)'診3蒼 KEY{24f3627a86fc740a7f36ee2c7a1c124a} ○向上(U) ●向下(D) □区分大小写(C)

19、号被盗了

https://www.jianshu.com/p/9d8269ca2da4

http://123.206.87.240:9001/

burp suite 将isadmin=false改为isadmin=true,

找到一个文件

http://123.206.87.240:9001/123.exe





http://120.24.86.145:9001/123.exe

🕞 💼 📔 Elements Console	Sources Network Performance Memory Application	Security Audits							○ 1 : >
Application	C 🛇 × Filter								
Manifest	Name	Value	 Domain 	Path	Expires / Max-Age	Size	HTTP	Secure	SameSite
Service Workers	isadmin	true	123.206.87.240	1	2018-11-05T09:0	11			
Clear storage									
Storage									

```
<html><head><style>

span {

display: block;

margin: auto;

height: 25px;

text-align: center;

font-size: 30px;

}

</style>

<title>bugku</title>

link href="style.css" rel="stylesheet" type="text/css">

</head>

<body>

<span>http://120.24.86.145:9001/123.exe</span>
```

```
</body></html>
```



下载后运行,并用wireshark抓包,

250-SIZE 73400320 250-STARTTLS 250-AUTH LOGIN PLAIN 250-AUTH=LOGIN 250-MAILCOMPRESS 250 8BITMIME AUTH LOGIN 334 VXN1cm5hbWU6 YmtjdGZ0ZXN0QDE2My5jb20= 334 UGFzc3dvcmQ6 YTEyMzQ1Ng== 535 Error:: http: subtype=1&&id=28&&no=1001256 QUIT 221 Bye

YmtjdGZ0ZXN0QDE2My5jb20= 解密: bkctftest@163.com YTEyMzQ1Ng0KDQo= 解密a123456 邮箱: 红旗邮件 flag{182100518+725593795416}

20、细心的大象



TVNEUzQ1NkFTRDEyM3p6做base解密得到: MSDS456ASD123zz

http://tool.chinaz.com/Tools/Base64.aspx

文字加密解密	MD5加密/解密	URL加密	JS加/解密	JS混淆加密压缩	ESCAPE加/解密	BASE64	散列/哈希	迅雷,快车,旋风URL加解密
MSDS456ASD12	23zz				TVNEUzQ1NkFT	RDEyM3p6		

1.jpg放到kali,

binwalk 1.jpg

发现有压缩包, ok, 执行分离:

binwalk -e 1.jpg

输入密码: MSDS456ASD123zz



winhex分析,修改高度并保存,

......

图片上具 UJP9		
共享 查看 管理	🎬 WinHex - [2.png]	
// mice > 10 细心的士母 > 1 ing	🚟 <u>F</u> ile <u>E</u> dit <u>S</u> earch <u>N</u> avigatio	n <u>V</u> iew <u>T</u> ools Spec <u>i</u> alist <u>O</u> ptions <u>W</u> indow <u>H</u> elp
- "misc > 19.细心的人家 > 1.jpg V	Case Data	〕 D. ₹ 🔜 😂 🕸 🚺 → 🖽 🖾 🖾 🗠 🐃 🙈 🗰 🎎 → 🕀 🗲 → -
	Fi <u>l</u> e E <u>d</u> it	2.png
		Offset 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
		00000000 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52
Bu		00000016 00 00 01 F4 00 00 01 A4 08 06 00 00 00 CB D6 DF
*		00000032 8A 00 00 00 09 70 48 59 73 00 00 12 74 00 00 12
		00000048 74 01 DE 66 1F 78 00 00 0A 4D 69 43 43 50 50 68
* 1100 2000		00000064 6F 74 6F 73 68 6F 70 20 49 43 43 20 70 72 6F 66
r.jpg 2.png	Data Interpreter	00000080 69 6C 65 00 00 78 DA 9D 53 77 58 93 F7 16 3E DE
	b d d interpreter	00000096 F7 65 0F 56 42 D8 F0 B1 97 6C 81 00 22 23 AC 08
	8 Bit (±): -92	00000112 C8 10 59 A2 10 92 00 61 84 10 12 40 C5 85 88 0A
	16 Bit (±): 2,212	00000112 56 14 15 11 9C 48 55 C4 82 D5 05 48 9D 88 F2 50
	32 Bit (±): 395,428	00000120 30 14 13 11 30 40 33 C4 02 53 0A 40 55 00 E2 A0
		00000144 20 20 00 41 0A 00 3A 0B 35 30 30 EE 11 20 A 03 00000160 7D 7A EE ED ED ED D7 EB D7 EB D7 E7 97 E7 E7 79 78
		00000176 0F 80 11 12 26 91 E6 A2 1004 00 390528655 5645A556
	I	

共	享 查看 管理	理		WinHex - [2.png]										
	micc > 10 细心的	十争 \ 1 ing		🚟 <u>F</u> ile <u>E</u> dit <u>S</u> earch <u>N</u> avigat	on <u>V</u> iew <u>T</u> ools Sp	ec <u>i</u> alist <u>O</u> pt	ions <u>W</u> indow	<u>H</u> elp						
-	1111SC / 19.50/0/03	Nak / 1.jpg	~	Case Data	🗋 🛎 🖏 🖬 🎝 🛍	📫 👘 🐚	🔁 🔂 🛍 1012	$\underset{\texttt{AB}}{\texttt{AA}} \overset{\texttt{AB}}{\twoheadrightarrow} \overset{\texttt{C}}{\circledast} \overset{\texttt{C}}{\twoheadrightarrow} \overset{\texttt{C}}{{}} \texttt{$	l 🕹 🤹 📾 🔎 🦚 🕍 😫 👘 8					
				Fi <u>l</u> e E <u>d</u> it	2.png									
					Offset 0	1 2 3	4 5 6 7	8 9 10 11 12 13 14 15	ANSI ASCII 🔺					
	and South	Bu			00000000 89	50 4E 47	0D 0A 1A 0A	00 00 00 0D 49 48 44 52	%PNG IHDR					
	- OL				00000016 00	00 01 F4	00 00 01 54	08 06 00 00 00 CB D6 DF	ô ô ËÖß					
*	A CONTRACTOR OF THE OWNER					00000032 8A	00 00 00	09 70 48 59	73 00 00 12 74 00 00 12	Š pHYs t				
	- And a second second	BUGKU{a1e5aSA}			00000048 74	01 DE 66	1F 78 00 00	0A 4D 69 43 43 50 50 68	t Þf x MiCCPPh					
N.	1 ing	2 ppg								00000064 6F	74 6F 73	68 6F 70 20	49 43 43 20 70 72 6F 66	otoshop ICC prof
*	1969	z.prig		Data Interpreter ×	00000080 69	6C 65 00	00 78 DA 9D	53 77 58 93 F7 16 3E DF	ile xÚ SwX"÷ >ß					
					00000096 F7	65 OF 56	42 D8 F0 B1	97 6C 81 00 22 23 AC 08	÷e VBØð±−1 "#¬					
				8 Bit (±): -12	00000112 C8	10 59 A2	10 92 00 61	84 10 12 40 C5 85 88 0A	È Y¢′а" @Å…^					
				16 Bit (±): 2,292	00000128 56	14 15 11	9C 48 55 C4	82 D5 0A 48 9D 88 E2 A0	V œHUÄ,ÕH ^â					
				32 Bit (±): 395,508	00000144 28	B8 67 41	8A 88 5A 8B	55 5C 38 EE 1F DC A7 B5	(,gAŠ^Z≮U\8î Ü\$u					
					00000160 7D	7A EF ED	ED FB D7 FB	BC E7 9C E7 FC CE 79 CF	}zïííû×û¼cœcüÎvÏ					

BUGKU{a1e5aSA}

21、爆照

依然放进kali

admin@ka admin@ka	li:~/20\$ li:~/20\$ ls	
8.jpg		
admin@ka	li:~/20 \$ binwalk 8.	jpg
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0×0	JPEG image data, JFIF standard 1.01
40499	0x9E33	Zip archive data, encrypted at least v2.0 to extract, compr
essed si	ze: 8362, uncompres	ssed size: 92278, name: 8
48892	0xBEFC	Zip archive data, at least v2.0 to extract, compressed size
: 14906,	uncompressed size:	: 15739, name: 88
63830	0×F956	Zip archive data, at least v2.0 to extract, compressed size
: 11129,	uncompressed size:	: 18479, name: 888
74992	0x124F0	Zip archive data, at least v2.0 to extract, compressed size
: 10371,	uncompressed size:	11782, name: 8888
85397	0x14D95	Zip archive data, at least v2.0 to extract, compressed size
: 6945,	uncompressed size:	92278, name: 88888
92377	0x168D9	Zip archive data, at least v2.0 to extract, compressed size
: 6824,	uncompressed size:	92278, name: 888888
99237	0x183A5	Zip archive data, at least v2.0 to extract, compressed size
: 7076,	uncompressed size:	92278, name: 8888888
106350	0x19F6E	Zip archive data, at least v2.0 to extract, compressed size
: 8219,	uncompressed size:	92278, name: 888888888
168452	0x29204	End of Zip archive, footer lengthttp22/blog.csdn.net/u013469/53

foremost 8.jpg

~/20\$ foremost 8.jpg 1: Processing: 8.jpg |foundat=80]000dv|00v00w0r0(0)hA0H0=00[]Dv00|00n00G000#0/r0000000;0l8000000'000A80Gu,0g]0b 10009000[00u~000|00000>9000/00000w_00000070|s000000}0000000000000000000/00r000_0000000? 8888?888}888/88888988888 ~0883888888 80H88889-8ktm 88 881:88t8/M8;|8^|86|8888881,88,<888 ŶКТ 'ONO`0|000T:|0000z# 00U06 0y000/00 |000F0080x-000s 0E/000000J0]0/A1v0000F0,]00+?00,00N10 00|0000Z|0j00LX> 0m0]04″)0Z> Y00N000000000000000. 0v?0w0|0x-0[000q0|0QWex 0000tN0/A6.0~0 0~000V0J0<# 0jE0 00. 0500Z< 00ojC^00>010{00[0000=00000000000000]C;040W075I0+0;0000"_y0g0E000/]0ku0Z0lw0\$00 =00j - 8888 0000000(0{g0s0@]Y00000!00(i000j00d90en0[000HXF0ZQ0\0000j500';000000000000000e0P%000000 0b00300000000000>[00L00k06 Y0:0000,I0000F0r 0 foundat=88ØZ <TQ0c006B00000PI^0(ea0f,E00"0-"b00[ž0c)0r020f0no0~o0f00000[[[[[[000000]][[[00000][[[[00000][[[[00000][[[[00000] 000 foundat=8880ZgTSA~06&R\$Hij0000000000,]:B0]pE0 0000000 0\$!AJ")0c{;0三00G撵 70團000000~000N0[0LLL0;0000%0E00 foundat=88880Zw\ 000H00I0"00049ң]0J00P0*0O<0"0HW0)%ŭ"0\$00%Q00p00000000u/;o70o000vo00>81~0 foundat=888880]K00000;0000^0001b00Y000 Ô٢ foundat=88888880]000T0001?0bD02\$\$\$ 0m00000001000007000000 000=0;Fqt0x00000 ?0 00[0w0y00000?00000|0000000/08~003000000_00000~{000000~8000ä~00000<u>?00ttt 0z000_0000?0800</u> 矧 \$\$\$ E 9\$\$?\$g \$ ∰\$w\$\$\$k\$9 h00000s0000f0:0005000)00m0c000e00"LwJ0:^04.5004c000(e0x50?[&jW/?00 2q00Y004 $\hat{\mathbf{2}}$ 0+00L0J0%00 foundat=888888880];00Tv0~000v[:D0hR0w@EAM00=k`0,0000 0 00s0q00000&00{0003030h 0 ?0~0000?00000_v000000~00000?00c000000/0000/~ foundat=88888888889]900T0K0,[0d00K EBØØP+ 0;0000.,0.00]Cp0`00<\$0m000000003g000,/+\$l000🌐 000 000JJJ000jjj00000ZZZP(0000000000000000000;;000000000{xxxzz0000U!Whhh?00`QQQqq 000000000

<mark>admin@kali:</mark>~/20\$ cd output/ <mark>admin@kali:</mark>~/20/output\$ ls <u>audit.txt jpg</u> zip

admin@kali:~,	/20/output/zip\$	ls	
00000079.zip			
admin@kali:~,	20/output/zip\$	unzip	00000079
Archive: 000	000079.zip		
inflating:	8		
inflating:	88		
inflating:	888		
inflating:	8888		
inflating:	88888		
inflating:	888888		
inflating:	8888888		
inflating:	88888888		
inflating:	88+88-++8=8+88	0000.g:	if
admin@kali:~,	20/output/zip\$		
	admin@kali:~/ 00000079.zip admin@kali:~/ Archive: 000 inflating: inflating: inflating: inflating: inflating: inflating: inflating: inflating: inflating: admin@kali:~/	admin@kali:~/20/output/zip\$ 00000079.zip admin@kali:~/20/output/zip\$ Archive: 00000079.zip inflating: 8 inflating: 88 inflating: 8888 inflating: 88888 inflating: 888888 inflating: 8888888 inflating: 8888888 inflating: 88888888 inflating: 88888888 inflating: 00+00-++0=0+000 admin@kali:~/20/output/zip\$	admin@kali:~/20/output/zip\$ ls 00000079.zip admin@kali:~/20/output/zip\$ unzip Archive: 00000079.zip inflating: 8 inflating: 88 inflating: 888 inflating: 8888 inflating: 88888 inflating: 888888 inflating: 8888888 inflating: 8888888 inflating: 8888888 inflating: 00+00-++0=0+000000.g: admin@kali:~/20/output/zip\$





zip

逐个查看文件

应用程序 ▼	位置▼ 🖸 终端▼		星期一16:43					1 💉 🗉) () -
			admin@kali: ~/20/output	t/zip				٥	
文件(F) 编辑	(E) 查看(V) 搜索(S)	终端(T) 帮助(H) bipy(a) k 8	10 是近体田	THE REAL PROPERTY AND INCOME.					
adminieka (1.)	-/20/0000000000000					6.9		\square	
DECIMAL	HEXADECIMAL	DESCRIPTION	★ 收藏	· • • • • •	(<u>`</u> •)	5	· · ·)	· · · ·)	
θ	0×0	PC bitmap, Windows 3.x format,, 303 x 300 x 8	☆ 主目录			770		ミン	
admin@kali:	~/20/output/zip\$	binwalk 88	■ 桌面	\$\$+\$\$-+	8	00000079.zip	88	888	
DECIMAL	HEXADECIMAL	DESCRIPTION	日视频 +	�=�+���� Ø oif (无效的编码)					
0 30	0×0 0×1E	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image director	y:喧g图片						
admin@kali:	~/20/output/zip\$	binwalk 888	□ 文档				'	··· ·)	
DECIMAL	HEXADECIMAL	DESCRIPTION	④ 下载	(* +.) 👘		*)			
0 30	0x0 0x1E	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image director	♪ 音乐 y:8 回りわた	8888	88888	888888	8888888	88888888	
admin@kali:	~/20/output/zip\$	binwalk 8888							
DECIMAL	HEXADECIMAL	DESCRIPTION	+ 其他位置						
0 30 10976 11760	0x0 0x1E 0x2AE0 0x2DF0	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image director Zip archive data, at least v2.0 to extract, compressed size End of Zip archive, footer length: 22	y: 8 : 644, uncompressed size:						
admin@kali:	~/20/output/zip\$	binwalk 86888							
DECIMAL	HEXADECIMAL	DESCRIPTION							
θ	0×0	PC bitmap, Windows 3.x format,, 303 x 300 x 8						已选中"8"(92.3 KB)	
admin@kali:	~/20/output/zip\$	binwalk 888888							
DECIMAL	HEXADECIMAL	DESCRIPTION							
θ	0×0	PC bitmap, Windows 3.x format,, 303 x 300 x 8							
admin@kali:	~/20/output/zip\$	binwalk 8888888							
DECIMAL	HEXADECIMAL	DESCRIPTION							
θ	0×0	PC bitmap, Windows 3.x format,, 303 x 300 x 8							
admin@kali:	~/20/output/zip\$							https://blog.csdn.net/u013	3469753



现在分析: (1)8 就一张图 (2)88 扫描二维码得到: bilibili



bninwalk -e 8888





扫描的到: panama

根据gif提示: 愉快的排序吧

猜测flag为: flag{bilibili_silisili_panama}

22、猫片(安恒)

bugkuCTF——猫片(安恒)

来自 https://blog.csdn.net/x947955250/article/details/81482471

https://www.jianshu.com/p/f84b33bf04a7

使用工具 http://www.caesum.com/handbook/Stegsolve.jar

来自 https://github.com/manisashank/stegsolve/blob/master/process to install stegsolve



疑似二维码,保存当前为png 使用winhex打开,修改高度





flag.txt

1 KB

ntfstreamseditor 查看数据流

来自 https://www.jianshu.com/p/f84b33bf04a7

	SEditor	http	o://blog.sina.co advn	– 🗆 m.cn/advnetsoft etsoft@sina.com by XGQ
按索	數据流名称匹配 *	✓	停止	
文件 ☑ F:\迅雷下载\CTF\flag.bt:flag.pyc	數据液名称 fiag.pyc	大小(字节) 755	可疑度(0-5) 1	
○ 新除 - ○ 前か +/ ○ ○ ○ ○ ○ □	入 <	>> 还原<<		导出列表

pyc解密 在线反编译 https://tool.lu/pyc/

选择文件 未选择任何文件	python if i/usr/bin/ew python if i/usr/bin/ew python
<pre>#!/usr/bin/env python # visit http://tool.lu/pyc/ for more information import base64 def encode(): flag = '***********************************</pre>	<pre></pre>

flag{Y@e_Cl3veR_C1Ever!}

23.多彩

Lipstick

来自 https://www.secpulse.com/archives/69465.html

直接用Stegsolve file/open,



发现YSL口红品牌,继续深入,使用Analyse







SaveBin林村为一个zip压缩包

直接解压有错,放到kali

应用程序 ▼ 位置 ▼ ▶ 终端 ▼ 星期三14:34 1 С **ا**((admin@kali: ~/22 8 文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H) 🐻這酸近使用~/22\$ binwalk out.zip DESCRIPTION DECIMA直 HEXADECIMAL ZIP ① 主目录 0x8 Zin archive data, encrypted at least v2.0 to e tracta compressed size: 77, uncompressed size: 67, name: flag.txt 13 0xD5 End of Zip archive, footer length: 22 日 视频 dmindkali:~/22\$ □ 图片 文档
 ④ 下载 □ 音乐 💮 回收站 + 其他位置 🔚 📄 🕅 🧝 🛃 👀 🖾 to 🎜 loc 👼 n. n 2700 (3489753) 9

尝试伪加密,无果。于是整个过程就剩下一个密码。一般来说图片隐写的话,要么是二进制里藏了东西,要么就是图形藏了东 西。这里二进制里藏了zip包,剩下的密码就只能从图形里入手。

图形里是21个颜色格,分别取色

BC0B28 D04179 D47A6F C2696F EB8262 CF1A77 C0083E BC0B28 BC0B28 D13274 6A1319 BC0B28 BC0B28 D4121D D75B59 DD8885 CE0A4A D4121D 7E453A D75B59 DD8885

来自 https://www.secpulse.com/archives/69465.html

YSL色号

https://www.yslbeautyus.com/on/demandware.store/Sites-ysl-us-Site/en_US/Product-Variation?pid=194YSL

-*- coding:utf8 -*-
author='pcat@chamd5.org'
import requestsimport re
import libnum
def foo():
url=r'https://www.yslbeautyus.com/on/demandware.store/Sites-ysl-us-Site/en_US/Product-Variation?pid=194YSL'
cont=requests.get(url).content
print cont
pattern=r'YSL_color=(.*?)%20[sS]*?background-color: #(.*?)"'
rst=re.findall(pattern,cont)
dYSL={}
for num,color in rst:
dYSL[color]=int(num.lstrip('0'))
lst=['BC0B28','D04179','D47A6F','C2696F','EB8262', 'CF1A77','C0083E','BC0B28','BC0B28','D13274', '6A1319','BC0B2
8','BC0B28','D4121D','D75B59', 'DD8885','CE0A4A','D4121D','7E453A','D75B59', 'DD8885']
<pre>flag=''.join('{:b}'.format(dYSL[i]) for i in lst)</pre>
print libnum.b2s(flag)
pass
ifname == 'main':
foo()
print 'ok'

打印出来是 白学家,即,解压密码。

7z x out.zip

使用命令解压出错可能是编码格式的问题

这里使用2345好压打开,来自 https://www.secpulse.com/archives/69465.html

TFtools jd-gui	为加密的文件输入密码 8.zip 白学家 正 ● 显示密码(勾选可支持中) 解当前密码应用到所有加 算 确定 跳过 22.多彩 ▶ out.zip.extracted ▶	■文密码输入) □密文件 〕跳过所有加密文件		
组织 🕶 🚔 打开 🔻	共享▼ 新建文件夹		•	≣ • 🔟 🔞
☆ 收藏夹	名称	修改日期	类型	大小
🔰 下载	🚔 8.zip	2018/11/7 16:13	好压 ZIP 压缩文件	577 KB
🗾 桌面 💱 最近访问的位置	📄 flag.txt	2018/11/7 16:18	文本文档	0 KB
[] 库				
🦉 🧸 视频			S 🕈 🔋 🕲	♥ 📾 🛎 ¥ 🏥

flag{White_Album_is_Really_worth_watching_on_White_Valentine's_Day}

24、旋转的跳跃

wget https://www.petitcolas.net/fabien/software/MP3Stego_1_1_19.zip

.\Decode.exe -X -P syclovergeek sycgeek-mp3.mp3

): 🗾 V	/indows PowerSh	nell				_		\times	
-a	- 2000/1	11/30	12:13	14	hidden_text.txt			1	
-a	- 2018/	/11/6	14:37	2481 5470	MP3Stego.sln PEADWE +++				
-a	- 2018/	$\frac{11}{0}$	15.23	1823640	README. IXI SVEGA WAV				1
-a	- 2016/1	10/10	12:03	2479748	sycgeek-mp3.mp3				
PS D: PS D: PS sy MP3St See R Input the b HDR: alg. = [Fram Decod The d PS D:	\security\emul clovergeek syc egoEncoder 1.1 EADME file for file = 'sycge attempt to ext it stream file s=FFF, id=1, 1 MPEG-1, layer= stereo, sblim= e 5932]Avg slo ing of "sycgee ecoded PCM out \security\emul	lation\qu cgeek-mp2 i. 19 r copyrig eek-mp3.r tract hid e sycgeel l=3, ep=c =III, to =32, jsb6 =32, jsb6 ek-mp3.rm tput file lation\qu	uestionban 3. mp3 ght info mp3' outp dden infor <-mp3. mp3 off, br=9, t bitrate= d=32, ch=2 e = 417.88 of fine e name is uestionban	k\bugku\misc\ ut file = 'sy mation. Outpu is a BINARY f sf=0, pd=1, 128, sfrq=44. 9; b/smp = 2. ished "sycgeek-mp3. k\bugku\misc\	<pre>\23旋转的跳跃\MP3Stego_1_1_19\MP3Stego_1_1_19\MP3Ste ycgeek-mp3.mp3.pcm' ut: sycgeek-mp3.mp3.txt file pr=0, m=0, js=0, c=0, o=0, e=0 .1 .90; br = 127.979 kbps .mp3.pcm" \23旋转的跳跃\MP3Stego_1_1_19\MP3Stego_1_1_19\MP3St whymics\23旋转的跳跃\MP3Stego_1_1_10\MP3Stego_1_1_19\MP3Stego_1_1_19\MP3Stego_1_1_10\MP3Steg_1_1_10\MP3Steg_1_1_10\MP3Steg_1_1_10\MP3Stego</pre>	ego> .\Deco ego> 1s	de. exe	-X	:e c c l l
ļ	∃來: D:\securi	ity\emula	ation\ques	tionbank\bugł	ku\m1sc\23厩特的跳跃\MP3Stego_1_1_19\MP3Stego_1_1_1	9\MP3Stego			ł
Mode		LastWr	iteTime	Length	Name				
d	- 2018/	/11/6	22:20		Decoder				
d	- 2018/	/11/7	19:06		Encoder				
d	- 2018/	/11/6	14:36		tables				
-a	- 2018/	11/6	22:11	556032	Decode. exe				
-a	- 2018/	/11/6	22:11	707584	Encode. exe				
-a	- 2000/1	11/30	12:13	14	hidden_text.txt				
-a	- 2018/	/11/0	14:37	2481 5470	MPSStego.sin PEADME +++				
a -a	- 2014	$\frac{11}{0}$	15.23	1823640	NEADME. IXI				
-a	- 2016/1	10/10	12:03	2479748	svogeek-mn3 mn3				
-a	- 2018/	/11/7	19:10	27337600	svcgeek-mp3. mp3. pcm				
-a	- 2018/	/11/7	19:10	22	sycgeek-mp3.mp3.txt				
PS D: 3.mp3 SYC {M PS D:	\security\emu] .txt p3_B15b1uBiu_V \security\emu]	lation\qu YOW} lation\qu	uestionban uestionban	k\bugku\misc\ k\bugku\misc\	\23旋转的跳跃\MP3Stego_1_1_19\MP3Stego_1_1_19\MP3Ste \23旋转的跳跃\MP3Stego_1_119\MP3Stego_1_1_19\MP3Ste	ego> cat .\ ego> _	sycgeek	-mp	
					http://www.aliana.com	s://blog.csdn.r	net/u0134	697 <u>8</u>	1

SYC{Mp3_B15b1uBiu_W0W}

25.普通的二维码

直接解压,使用微信扫描得到

扫描到以下内容

哈哈!就不告诉你flag就在这里!

使用winhex打开

http://www.cnblogs.co	om/le	ixiad	o-/p/9	9825	5703	.html											
00002992	FF	\mathbf{FF}	\mathbf{FF}	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	\mathbf{FF}	FF	FO	00	\mathbf{FF}	\mathbf{FF}	\mathbf{FF}	\mathbf{FF}	\mathbf{FF}	FF	<u> </u>
00003008	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	FF	$\mathbf{F}\mathbf{F}$	FF	FF	F0	00	31	<mark>3</mark> 4	<u> ΥΥΥΥΥΥΥΥΥΥΥΥ</u> δ 14
00003024	36	31	35	34	31	34	31	31	34	37	31	37	33	31	31	30	6154141147173110
00003040	31	34	31	31	36	36	31	34	35	31	33	37	31	37	31	30	1411661451371710
00003056	36	30	31	32	35	31	33	37	31	32	30	31	37	31	31	33	6012513712017113
00003072	37	31	36	33	31	34	33	31	36	32	31	35	31	31	36	30	7163143162151160
00003088	31	36	34	31	33	37	31	31	37	31	36	34	31	34	33	31	1641371171641431
00003104	33	37	31	32	34	31	35	37	31	33	37	31	32	34	31	34	3712415713712414
00003120	35	31	35	36	31	33	37	31	30	31	31	36	33	31	34	33	5156137101163143
00003136	31	35	31	31	35	31	30	34	31	31	37	35	40	78	6A	73	151151041175@xjs
00003152	65	63	6В	21													eck!
																	://blog.csdn.net/u013469753

这段数据发现只有0-7,没有8和9,很容易想到是8进制数据,可以将其转换成10进制,然后再转成ascii字符。一开始看这个数 字总长126个,2的倍数,加上以前转换16进制的惯性思维,让我以为这里也是两两一对的转换,转换出来自然不正确,一堆乱 码,后来发现两位的8进制数据最大077(数字前加0表示8进制),转换成10进制63也表示不完ascii码表上的字符啊,而且126 刚好也是3的倍数,所以三个一组来转换,如下脚本:

破解这串数字了,这里有两点,第一,都是小于8的数,第二,每三个数似乎是一个可以转成字符的集体,于是写脚本 https://blog.csdn.net/csdn_Pade/article/details/82779112



/security/emulation/questionbank/bugku/misc/24普的维\$ touch misc80.py /security/emulation/questionbank/bugku/misc/24普的维\$ nano misc80.py /security/emulation/questionbank/bugku/misc/24普通的二维码\$ python misc80.py

flag{Have_y0U_Py_script_0tc_To_Ten_Ascii!}

flag{Have_y0U_Py_script_Otc_To_Ten_Ascii!}

26.乌云邀请码

直接放到stegsolve, data extract一下	
StegSolve 1.3 by Caesum	
File Analyse Help	
Green plane 5	
Extract Preview	
0017666c61677b50 6e675f4c73625f59 flag{P ng Lsb_Y 30755f4b306e7721 7dfffffffffff 0u_K0nw! } fffffffffffffffffffffffff	Order settings
Alpha 7 6 5 4 3 2 1 0	Extract By Row Column
Green 7 6 5 4 3 2 1 0	Bit Order III Mess First III LSB First
Blue ☐ 7 ☐ 6 ☐ 5 ☐ 4 ☐ 3 ☐ 2 ☐ 1 🗹 0	
Preview Settings Include Hex Dump In Preview	
Preview Save Text Save B	Bin Cancel https://blog.csdn.net/u01346975

flag{Png_Lsb_Y0u_K0nw!}

27、神秘的文件

要点: 明文破解 + doc隐写 解题过程: 将题目解压出来,题目压缩包里有个logo.png和一个加密压缩包,很明显的明文破解,使用题目压缩包作为key和writeup压缩包 进行明文破解(或者使用2345好压的标准压缩算法压缩logo.png),得到密码:

http://www.sdnisc.cn/detail_285_286_747.html

28图穷匕见

🕵 WinHex - [paintpaintpaint.jpg]		1000		1 4 4 1 A	
🎇 File Edit Search Navigation	n View To	ols Specialist Options Wi	indow Help		19.7 – <i>B</i> ×
	1012	AA AA AA AA → +€ <	> 🛛 🕹 🕹 🚔 🔳 🔎 👘	🔬 🦀 🕴 🏭 🖌 🛛	▶ ♦
paintpaintpaint.jpg					
r 1. 19	Offset	0 1 2 3 4 5 6 7	8 9 A B C D E F	ANSI ASCII	A
[unregistered]	000050E0	A8 47 7C F3 4F 10 23 65	27 E3 38 4D A3 E1 39 52	"G∣óO #e'ã8M£á9R	
paintpaintpaint.jpg	000050F0	06 30 3F A2 0C 48 22 10	01 DD 33 B2 D0 0E C7 AA	0?¢ H" Ý3°Ð ǰ	=
C:\Users\admin\Desktop\题目\26	00005100	82 OF 45 52 4E C1 1C 40	03 38 85 2C 0C 6C 10 04	, ERNÁ @ 8, 1	-
File sizes CEE KR	00005110	1C A0 10 44 8D 90 7A 14	12 E3 3E 88 C0 07 A2 0E	D z ã>^A ¢	
File size: 655 KB	00005120	73 18 43 84 B3 74 13 12	71 B0 48 83 27 18 4C OE	s C"'t q°Hf' L	
670,804 bytes	00005130	1D C6 EA 9A 54 12 46 31	22 56 41 B2 4E 20 2D 88	Rest F1"VA*N -^	
DOS name: PAINTP~1.JPG	00005140	CC C2 4E 6C 1F 55 2C 59	49 82 3D 55 10 42 4C 05	IANI U,YI,=U BL	
	00005150	AA 89 56 70 22 62 06 77	00 47 69 94 46 FD D1 B7	- 5: V) "D WIN ~ & H	
Default Edit Mode	00005180	69 20 60 42 10 84 02 51	09 FE A5 ED E2 6C 71 16	i 'B O î¥iâlo	
State: original	00005180	F7 06 13 02 A9 4D 8F 10	F6 35 DF A2 55 AC 4D BB	- @M ö5bell→M≫	
	00005190	OF FE A8 7F EF 1D FD 52	16 B4 39 D2 68 BF E6 CA	î∵ïvR 19ÒkzæÊ	
Undo level: 0	000051A0	0D 5C F6 B7 E6 70 1E A6	14 1B 9B 76 FC D5 E9 8F	\ö∙æp ¦ >vüÕé	
Undo reverses: n/a	000051B0	57 80 81 6F 40 0F 86 8D	31 E8 D0 B4 OD OD F9 40	W€ o@ † 1èĐ′ ù@	
	000051C0	13 EC 83 2F CD 5B 9D AA	B4 9E C6 50 2E 68 C4 87	ìf∕Í[ª′žÆP.hć	
Creation time: 2018/11/08	000051D0	13 E8 D2 56 C8 41 88 B8	A6 46 05 42 3B 53 77 F4	èÒVÈA^,¦F B;Swô	
14:34:12	000051E0	47 E6 A9 FF 00 76 B7 FE	4B FF 00 A2 D9 1C D0 63	Gæ©ÿ v∙þKÿ ¢Ù Đc	
Last write time: 2018/11/08	000051F0	F9 AA 7F DD AD FF 00 92	FF 00 E8 B2 A0 69 53 73	ùª Ý-ÿ ′ÿ èª iSs	
14:33:20	00005200	DF FC 57 3E A1 92 4D 27	7D 36 5C B4 20 C8 57 A7	ßüW>¦'M'}6\′ÈW§	
14.00.20	00005210	80 4B 81 EE D2 3F 64 FC	FA 5F F5 8D 1E EB 44 2A	€K îÓ?düú_õ ëD*	
Attributes: A	00005220		51 93 PA 1C 21 CO 1F 50	%µ ï•í'±T``š !A P	
Icons: 0	00005230		AL DEVEL F2 8D 3F FE 9C	€ÐNð€=0 ; Ao ?þœ	
	00005240	DF 42 BB 4F E6 67 AA 10	B8 47 E8 DD BD 3F 92 92	BB»Oag ,Geix?"	
Mode: hexadecimal	00005250	DU /C AF F/ 42 16 9E 2E	DE SE DE FE SE 4E FE SI	DI -D Z.PZSP UPU	
Offsets: hexadecimal	00005270	52 A7 98 42 12 A8 3F 2A	63 92 10 74 0F 92 76 71	D6"B "2*c' X / .	
Bytes per page: 38x16=608	00005280	0A FE 81 C9 14 21 52 10	DC AC F9 A1 0B 30 6E 84	bÉ!Rܬù: 0n	
Window #	00005290	21 69 02 93 89 42 11 54	36 49 08 44 07 E6 F6 50	!i [™] B T6I D æöP	
Window #.	000052A0	EE 5E A8 42 95 6 3C 95	OD 8A 10 80 6E E8 76 E8	î^″B•`<• Š €nèvè	
Data Interpreter	000052B0	42 7E 03 98 52 HE 68 42	80 3F 2A 63 72 84 20 A6	B~ ~RîhB€?*cr, ¦	
8 Bit (+): -1	000052C0	EC 87 21 0B 47 9 1D D5	72 42 13 F4 09 0E 48 42	ì‡! Gé ÕrB ô HB	
16 Bit (+): -9 729	000052D0	06 A2 A7 2F 54 21 11 68	42 15 02 10 85 00 84 21	¢§/T! hB "!	
32 Bit (+): 942.856.703 free	000052E0	00 84 21 50 24 84 28 1A	10 84 02 10 85 40 84 21	"!P\$"(" …@"!	
e mp	000052F0	00 84 21 07 FF D9 32 38	33 37 32 63 33 37 32 39	"! ¥Ů28372c3729	
	00005300	30 61 32 38 33 37 32 63	33 38 32 39 30 61 32 38	0a28372c38290a28	
	00005310	33 37 32 63 33 39 32 39	30 61 32 38 33 37 32 63	372c39290a28372c	
	00005320	33 31 33 30 32 39 30 61	32 38 33 37 32 63 33 31	3130290a28372c31	
	00005330	22 21 22 29 20 61 32 38	33 37 32 63 33 31 33 32	51290828372C3132	https://blog.csdn.net/u013469753
D 3F -£1 104	<u>0</u> 4	5054	OFF DIA - In		

可以看到FF D9是jpg的结尾,后面明显是追加的一些值,备份原图,删掉原图的数据 paintpaintpaintjpg

					_	-		-	-	-	_	_	-	_	~	-	-	-		2007 20077	
	[unregistered]	UIISet	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	Ľ.	10	ANSI ASCII	-
naintnaintnainti	ing	00005137	31	22	56	41	82	4E	20	2D	88	cc	C2	4E	6C	1F	55	20	59	I"VA*N - IANI U,Y	
paintpaintpaint.		00005148	49	82	3D	55	10	42	4C	05	AA	89	56	7D	22	62	06	77	54	I,=U BL =%V}"b wT	
C:\Users\admin\	Desktop\26图务比	00005159	D1	01	1C	BA	26	08	48	08	CA	60	23	74	76	5A	OD	09	4A	N °& H E`#tvZ J	
		0000516A	68	84	46	FD	D1	BA	69	20	60	42	10	84	02	51	09	EE	A5	h"FýN°i `B " Q î¥	
File size:	655 KB	0000517B	ED	E2	6C	71	16	F7	06	13	02	A9	4D	8F	10	F6	35	DE	A2	iâlg÷ ©M ö5⊉≎	
	670,804 bytes	0000518C	55	AC	4D	BB	0E	EE	A8	7F	EF	1D	FD	52	16	B4	39	D2	6B	U⊣M≫ î″ ï ýR '9Ók	
DOC	DAINITE 1 IDC	0000519D	BF	E6	CA	OD	5C	F6	B7	E6	70	1E	Α6	14	1B	9B	76	FC	D5	¿æĒ∖ö∙æp¦ >vüÖ	
DOS name:	PAINTP~1.JPG	000051AE	E9	8F	57	80	81	6F	40	OF	86	8D	31	E8	DO	B4	0D	OD	F9	é W€ o@ † 1èÐ′ù	
Distante Data Mari		000051BF	40	13	EC	83	2 F	CD	5B	9D	AA	B4	9E	C6	50	2E	68	C4	87	@ lf/Í[⁴´žÆP.hć	
Default Edit Mod	ie	000051D0	13	E8	D2	56	C8	41	88	B8	A6	46	05	42	3B	53	77	F4	47	èČVÈA^,¦F B;SwôG	
State:	original	000051E1	E6	A9	FF	00	76	B7	FE	4B	FF	00	A2	D9	1C	D0	63	F9	AA	æ©ÿ v∙þKÿ ¢Ù Đcù≞	
Undo level:	0	000051F2	7F	DD	AD	FF	00	92	FF	00	E8	B2	A0	69	53	73	DF	FC	57	Ý-ÿ 'ÿ è* iSsßüW	
Undo level.	- (-	00005203	3E	A1	92	4D	27	7D	36	5C	B4	20	C8	57	A7	80	4B	81	EE	>;'M'}6\' ÈW§€K î	
Undo reverses:	n/a	00005214	D2	3F	64	FC	FA	5F	F5	8D	1E	EB	44	2A	25	B5	18	EF	95	Ò?düú_õ ëD*%µï∙	
a	2010/11/00	00005225	ED	27	B1	54	93	9A	1C	21	CO	1F	50	80	DO	D1	FO	80	3D	í'±T"š !À P€ÐÑð€=	
Creation time:	2018/11/08	00005236	30	81	A1	80	41	F2	8D	ЗF	FE	9C	DF	42	BB	4F	E6	67	AA	0 ; Aò ?þœßB»Oæg*	
	14:33:16	00005247	10	B8	47	E8	DD	BD	ЗF	92	92	DO	7C	AF	F7	42	16	9E	2E	,GèÝ∺?′′Đ ÷B ž.	
Last write time:	2019/11/09	00005258	DE	8E	DF	FE	8F	4F	FE	51	F6	5A	21	0B	A3	E4	DF	B2	6E	₽Žßþ OþQöZ! £äß*n	
Last write time.	2010/11/00	00005269	E9	37	9A	10	Α4	03	FE	52	A7	98	42	12	A8	3F	2A	63	92	é7š × þR§~B ∵?*c'	
	14:33:20	0000527A	10	A4	OF	92	A6	A1	AO	FE	81	C9	14	21	52	10	DC .	AC	F9	×′¦; þÉ !R ܬù	
Attributes:	Δ	0000528B	A1	0B	30	6E	84	21	69	02	93	B9	42	11	54	36	49	80	44	; 0n,,!i "'B T6I D	
Iconci		0000529C	07	E6	F6	50	EE	5E	A8	42	95	60	3C	95	0D	8A	10	80	6E	æöPî^~B•`<• Š €n	
icons.	U	000052AD	E8	76	E8	42	7E	03	98	52	EE	68	42	80	3F	2A	63	72	84	èvèB~ ~RîhB€?*cr"	
Mada	Taut	000052BE	20	A6	EC	87	21	0B	47	E9	1D	D5	72	42	13	F4	09	0E	48	!ì‡! Gé ÕrB ô H	
wode:	Text	000052CF	42	06	A2	A7	2F	54	21	11	68	42	15	02	10	85	00	84	21	B ¢§/T! hB "!	
Offsets:	hexadecimal	000052E0	00	84	21	50	24	84	28	1A	10	84	02	10	85	40	84	21	00	"!P\$"(" "@"!	
Bytes per page:	45x18=810	000052F1	84	21	07	FF	D9	32	38	33	37	32	63	33	37	32	39	30	61	"! VÜ28372c37290a	
Window #	1	00005302	32	38	33	37	32	63	33	38	32	39	30	61	32	38	33	37	32	28372c38290a28372	
Window #.		00005313	63	33	39	32	39	30	61	32	38	33	37	32	63	33	31	33	30	c39290a28372c3130	
Data Interprete	er 🛛 🕄 🗌 🕹	00005324	32	39	30	61	32	38	33	37	32	63	33	31	33	31	32	39	30	290a28372c3131290	
0.011 (1) 00		00005335	61	32	38	33	37	32	63	33	31	33	32	32	39	30	61	32	38	a28372c3132290a28	
8 BIT (±): -39	hpty	00005346	33	37	32	63	33	31	33	33	32	39	30	61	32	38	33	37	32	372c3133290a28372	
16 Bit (±): 13,0	1/	00005357	63	33	31	33	34	32	39	30	61	32	38	33	37	32	63	33	31	c3134290a28372c31	
32 Bit (±): 859	,321,049	00005368	33	35	32	30	30	61	32	38	33	37	32	63	33	31	33	36	32	35290=28372c31362	
	, emp	00005379	30	30	61	32	38	33	37	32	63	33	31	33	37	32	30	30	61	90a28372c3137290a	
		00005387	32	38	33	37	32	63	33	31	30	38	32	30	30	61	32	38	33	28372631382008292	
		ACCOUDD	22	20	22	57	22	00	22	21	20	20	22	29	20	01	22	20	22	20312031302904203	

https://blog.csdn.net/u013469753

WinHex - [paintpaintpaint.jpg]				COLUMN AND AND AND AND AND AND AND AND AND AN	A CONTRACT OF						
🚟 File Edit Search Navigation	🖀 File Edit Search Navigation View Tools Specialist Options Window Help										
🗅 📦 🗔 👙 📾 👔 📔 👘 🐚	a 🖪 🖻 🐎 👭 👭 🖧 😘 🖌 →	H) 🗲 🔶 🕹 🍪 🚥 🔎 👘 🔬 🏟	81 🖽 🖊 🕨 🥔								
paintpaintpaint.jpg											
[upregistered]	Offset 0 1 2 3 4 5 6	7 8 9 A B C D E F 10 11	12 13 14 15 16 17 18 19 1A	1B 1C 1D 1E 1F ANSI ASCII	A						
paintpaintpaint ing	00000000 32 38 33 37 32 63 33	37 32 39 30 61 32 38 33 37 32 63	33 38 32 39 30 61 32 38 33	37 32 63 33 39 28372c37290a28372c38290a2	8372c39						
C:\Users\admin\Deskton\26@@F	00000020 32 39 30 61 32 38 33	37 32 63 33 31 33 30 32 39 30 61	. 32 38 33 37 32 63 33 31 33 3	51 32 39 30 61 290a28372c3130290a28372c3	131290a						
C. (Osers (admin) Desktop (20) 20)	00000060 32 63 33 31 33 34 32	39 30 61 32 38 33 37 32 63 33 31	33 35 32 39 30 61 32 38 33 3	37 32 63 33 31 2c3134290a28372c3135290a2	8372c31						
File size: 634 KB	00000080 33 36 32 39 30 61 32	38 33 37 32 63 33 31 33 37 32 39	30 61 32 38 33 37 32 63 33 3	31 33 38 32 39 36290a28372c3137290a28372	c313829						
649,566 bytes	000000A0 30 61 32 38 33 37 32	63 33 31 33 39 32 39 30 61 32 38	33 37 32 63 33 32 33 30 32	39 30 61 32 38 0a28372c3139290a28372c323	0290a28						
DOC	000000C0 33 37 32 63 33 32 33	31 32 39 30 61 32 38 33 37 32 63	33 32 33 32 32 39 30 61 32 3	38 33 37 32 63 372c3231290a28372c3232290	a28372c						
DOS name: PAINTP~1.JPG	000000E0 33 32 33 33 32 39 30	61 32 38 33 37 32 63 33 32 33 34	32 39 30 61 32 38 33 37 32	63 33 32 33 35 3233290a28372c3234290a283	72c3235						
Default Edit Mode	00000100 32 39 30 61 32 38 33	37 32 63 33 32 33 36 32 39 30 61	. 32 38 33 37 32 63 33 32 33 3	37 32 39 30 W标.txt - 记事本							
State: modified		20 20 51 22 29 30 51 32 36 33 30 52 33 30 52 39 30 61 32 36 33 30	32 63 33 32 33 39 32 39 30 9								
	00000160 33 32 32 39 30 61 32	38 33 37 32 63 33 33 33 33 32 39	30 61 32 38 33 37 32 63 33	33 33 34 32 1	Ē(∇) 帝助(H)						
Undo level: 1	00000180 30 61 32 38 33 37 32	63 33 33 33 35 32 39 30 61 32 38	33 37 32 63 33 33 33 36 32 3	39 30 61 32 28372c37290a28372c382	90a28372c39290a28372c3130290a28372 🔺						
Undo reverses: block removal	000001A0 33 37 32 63 33 33 33	37 32 39 30 61 32 38 33 37 32 63	33 33 33 38 32 39 30 61 32 3	38 33 37 32 35290a28372c313336290a	a28372c313337290a28372c313338290a2 🗐						
Creation time: 2018/11/08	000001C0 33 33 33 39 32 39 30	61 32 38 33 37 32 63 33 34 33 30	32 39 30 61 32 38 33 37 32	63 33 34 33 36290a28372c323337290a	a28372c323338290a28372c323339290a2						
14.22.16	000001E0 32 39 30 61 32 38 33	37 32 63 33 34 33 32 32 39 30 61	32 38 33 37 32 63 33 34 33	33 32 39 30 382c3430290a28382c343	1290a28382c3432290a28382c3433290a2						
14.33.10		34 33 34 32 39 30 61 32 38 33 3	32 63 33 34 33 35 32 39 30	61 32 38 33 2c313732290a28382c313	733290a28382c313734290a28382c31373						
Last Data Interpreter	00000220 32 63 33 34 33 36 32	39 30 61 32 36 33 37 32 63 33 39	33 37 32 39 30 61 32 38 33 .	2c323635290a28382c323	636290a28382c323637290a28382c32363						
9 Pit (+): 55	000002			0a28392c313239290a283	92c313330290a28392c313331290a28392						
Attr 16 Dit (±): 33	000002			0a28392c323330290a283	92c323331290a28392c323332290a28392						
Icor 32 Bit (+): 842 609 463	000002 ((二)(二)(二)(二)(二)(二)(二)(二)(二)(二)(二)(二)(二)	2见		302c3239290a2831302c3	330290a2831302c3331290a2831302c333						
S2 Bit (1), 042,003,403	000002			31302c313437290a28313	02c313438290a2831302c313439290a283						
Mode: hexadecimal	000002 组织▼ → 打开▼	共享▼ 打印 新建文件夹		2831302c323431290a283	1302c323432290a2831302c323433290a2						
Offsets: hexadecimal	000003	243 3311 30a224174		3336290a2831312c33372	90a2831312c3338290a2831312c3339290						
Bytes per page: 37x32=1184		provered by		3533290a2831312c31353	4290a2831312c313535290a2831312c313						
Window #	000003	4		323437290a2831312c323	438290a2831312c323439290a2831312c3						
Window #: 1	000003 📙 下载			290a2831322c3434290a2	R31322c3435290a2831322c3436290a283						
No. of windows:	000003 🛛 🗾 桌面			283132263136382006283	1322c313630200a2831322c313730200a2						
Clipboard: 634 KB	000003	國穷已見		0.0003132200100002504200.00	291900-909595000-0091900-909596000						
004 10	000003 🔊 藏近访问的位置	CITATE C		002102002521000000212	00000000000000000000000000000000000000						
TEMP folder: 18.8 GB free	000004	a sinta sinta sint		263135203531290828313	9769997780876919976999958085891997 +						
sers\admin\AppData\Local\Temp	000004	paintpaintpaint. 坐标.txt			hitps://blog.osdn.nei/u013469759						

/www.rapidtables.com/convert/number/hex-to-ascii.html	
TRY LIS RISK ARE	

Uluel NOW:

Hex to ASCII text converter

Enter 2 digits hex numbers with any prefix / postfix / delimiter and press the Convert button (e.g. 45 78 61 6d 70 6C 65 21):

$\begin{array}{l} 8372 c_{3}7290 a_{2}8372 c_{3}8290 a_{2}8372 c_{3}9290 a_{2}8372 c_{3}130290 a_{2}8372 c_{3}131290 a_{2}8372 c_{3}132290 a_{2}8372 c_{3}133290 a_{2}8372 c_{3}134290 a_{2}8372 c_{3}135290 a_{2}8372 c_{3}135290 a_{2}8372 c_{3}135290 a_{2}8372 c_{3}135290 a_{2}8372 c_{3}135290 a_{2}8372 c_{3}139290 a_{2}8372 c_{3}230290 a_{2}8372 c_{3}23290 a_{2}8372 c_{3}23290 a_{2}8372 c_{3}23290 a_{2}8372 c_{3}23290 a_{2}8372 c_{3}23290 a_{2}8372 c_{3}23290 a_{2}8372 c_{3}233290 a_{2}8372 c_{3}233290 a_{2}8372 c_{3}233290 a_{2}8372 c_{3}233290 a_{2}8372 c_{3}233290 a_{2}8372 c_{3}233290 a_{2}8372 c_{3}334290 a_{2}8372 c_{3}335290 a_{2}8372 c_{3}336290 a_{2}8372 c_{3}336290 a_{2}8372 c_{3}33290 a_{2}8372 c_{3}334290 a_{2}8372 c_{3}33290 a_{2}837$	*
Convert Reset 13 Swap	•
(7, 10) (7, 11) (7, 12) (7, 13) (7, 14)	•
Select	2



ASCII to hex converter ►

4	/
_	0
7	9
7	10
7	11
7	12
7	13
7	14
7	15
7	16
7	17
7	18
7	19
7	20
7	21
7	22
7	23
7	24
7	25
7	26
7	27
7	28

去掉括号和逗号的txt放到kali中进行绘图。 gnuplot这个工具比较方便,因此将坐标转为gnuplot能识别的格式坐标1坐标2

来自 https://www.cnblogs.com/WangAoBo/p/6950547.html

安装gnuplot

来自 https://www.jianshu.com/p/6eef7dfe51bf

gnuplot

plot "qukongge.txt"

admin@kali: ~/26 0 0 6 文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H) 1@kali:~/26\$ pwd /home/admin/26 dmin@kali:~/26\$ ls qukongge.txt dmin@kali:~/26\$ gnuplot GNUPLOT Version 5.2 patchlevel 5 last modified 2018-10-06 Copyright (C) 1986-1993, 1998, 2004, 2007-2018 Thomas Williams, Colin Kelley and many others gnuplot home: http://www.gnuplot.info
faq, bugs, etc: type "help FAQ"
immediate help: type "help" (plot window: hit 'h') Terminal type is now 'wxt' gnuplot> plot "qukongge.txt" https://blog.csdn.net/u013469753



flag{40fc0a979f759c8892f4dc045e28b820}

29、convert

convert

来自 https://blog.csdn.net/yaofeiNO1/article/details/78459569#t3

txt文件內都是二进制01字串 将二进制转为16进制,再把16进制符写入winhex文件中,发现rar文件, 另存为rar文件解压得到一张图片,查看属性有base64编码,解码得到flag bintohex的demo以及存入rar包的代码

来自 https://blog.csdn.net/yaofeiNO1/article/details/78459569#t3

flag{01a25ea3fd6349c6e635a1d0196e75fb}

30. 听首音乐

用Audacity音频分析软件打开,猜测是摩尔斯电码,

放大

长的用"-"表示,短的用"."表示,中间用空格隔开。

..... -... -.-. ----. ..--- -.... -.... -.-. -.-. -... -... ---- ---.. ---.. ---.. -...

http://tool.bugku.com/mosi/

space方式为空格

5BC925649CB0188F52E617D70929191C

31.好多数值

数值很多255,猜测与RGB有关,下使用RGB值转化为图片的脚本

flag{youc@n'tseeme}

32、很普通的数独

使用binwalk查看发现有25张图片

binwalk -e zip

提取

下载解压后一堆数独图片,把所有带数字的方框改成黑色

来自 https://ctf.yuanlichenai.cn/2018/05/03/Bugku/Misc-3/

应该是是一张二维码,刚好是25张,5X5组合起来。

样子好像有点不对,这里需要把第1张、第5张和第21张互换位置

扫码得到

Vm0xd1NtUX1Wa1pPV1doVF1US1NjRlJVVGtOamJGWn1WMjFHV1UxV1ZqT1dNakZIWVcxS1IxTnNhRmhoTVZweVdWUkdXbVZHWkhOWGJGcHBWa1p aZWxac1pEUmhNVXBYVW14V2FHVnFRVGs9

使用base64多次解码7次

flag{yOud1any1s1}

33.PEN_AND_APPLE

PEN_AND_APPLE

来自 http://www.nsoad.com/Article/CTF/20161109/726.html 必须吐槽出题人的视频素材/捂脸 核心 利用NTFS交换数据流隐藏文件来自 https://www.qingsword.com/qing/812.html 原题提供的素材无法解析到文件

```
联想到视频隐写,搜索之,但只查到WAV格式的。提示是Windows下命令行,查阅《数据隐藏技术解密》一书的Windows相关
内容,了解到是NTFS数据流隐写
```

34.你见过彩虹吗

要点: 考点 拉长图片,二进制转字符串。

来自 http://www.sdnisc.cn/detail_285_286_747.html 查看每张图片的最低位,发现有变化。组成之后是一句话: 可以参考: https://blog.csdn.net/CoolD_/article/details/83793060#MiscCrack_it8pts_33

得到七串二进制

发现原来图像下部,有黑白块儿,按照黑->1,白->0转化成二进制数。

经过多次尝试之后发现,每一列,七个数字组成一个字符,进行二进制转化之后即可得到flag。

横着解不出来 尝试竖着解

脚本



print flag 作者: Coo1D 来源: CSDN 原文: https://blog.csdn.net/CoolD_/article/details/83793060 版权声明:本文为博主原创文章,转载请附上博文链接!

35.好多压缩包

binwalk 123.zip

编写脚本,进行爆破

编写脚本,通过CRC32碰撞,暴力破解出值

打开out.txt,可以看出碰撞出的结果是经过base64编码的,进行base64解码 待解码

z5BzAAANAAAAAAAAAAAAKo+egCAIwBJAAAAVAAAAAKGNKv+a2MdSR0zAwABAAAAQ01UCRUUy91BT5UkSNPoj5hFEVFBRvefHSBCfG0ruGnKnygsMyj 8SBaZHxsYHY84LEZ24cXtZ01y3k1K1YJ0vpK9HwqUzb6u9z8igEr3dCCQLQAdAAAAHQAAAAJi0efVT2MdSR0wCAAgAAAAZmxhZy50eHQAsDRpZmZ peCB0aGUgZmlsZSBhbmQgZ2V0IHRoZSBmbGFnxD17AEAHAA==

https://www.qqxiuzi.cn/bianma/base64.htm

结果按16进制显示

00	80	23	00	49	00	00	00
54	00	00	00	02	86	34	ab
fe	6b	63	1d	49	1d	33	03
00	01	00	00	00	43	4d	54
09	15	14	cb	dd	41	4f	95
24	48	d3	e8	8f	98	45	11
51	41	46	f7	9f	1d	20	42
7c	6d	2b	b8	69	са	9f	28
2c	33	28	fc	48	16	99	1f
1b	18	1d	8f	38	2c	46	76
e1	c5	ed	67	4d	72	de	4d
4a	d5	82	74	be	92	bd	1f
0a	94	cd	be	ae	f7	3f	22
80	4a	f7	74	20	90	2d	00
1d	00	00	00	1d	00	00	00
02	62	d1	e7	d5	4f	63	1d
49	1d	30	08	00	20	00	00
00	66	6c	61	67	2e	74	78
74	00	b0	34	69	66	66	69
78	20	74	68	65	20	66	69
6c	65	20	61	6e	64	20	67
65	74	20	74	68	65	20	66
6c	61	67	c4	3d	7b	00	40
07	~~						

cf 90 73 00 00 0d 00 00 00 00 00 00 00 aa 3e 7a

去掉 \x

\xcf \x90 \x73 \x00 \x00 \x0d \x00 \x00 \x00 \x00 \x00 \x00 \x00 \x00 \xaa \x3e \x7a \x00 \x80 \x23 \x00 \x49 \x00 \x00 \x00 \x54 \x00 \x00 \x00 \x02 \x86 \x34 \xab \xfe \x6b \x63 \x1d \x49 \x1d \x33 \x03 \x00 \x01 \x00 \x00 \x00 \x43 \x4d \x54 \x09 \x15 \x14 \xcb \xdd \x41 \x4f \x95 \x24 \x48 \xd3 \xe8 \x8f \x98 \x45 \x11 \x51 \x41 \x46 \xf7 \x9f \x1d \x20 \x42 \x7c \x6d \x2b \xb8 \x69 \xca \x9f \x28 \x2c \x33 \x28 \xfc \x48 \x16 \x99 \x1f \x1b \x18 \x1d \x8f \x38 \x2c \x46 \x76 \xe1 \xc5 \xed \x67 \x4d \x72 \xde \x4d \x4a \xd5 \x82 \x74 \xbe \x92 \xbd \x1f x0a x94 xcd xbe xae xf7 x3f x22\x80 \x4a \xf7 \x74 \x20 \x90 \x2d \x00 \x1d \x00 \x00 \x00 \x1d \x00 \x00 \x00 \x02 \x62 \xd1 \xe7 \xd5 \x4f \x63 \x1d \x49 \x1d \x30 \x08 \x00 \x20 \x00 \x00 \x00 \x66 \x6c \x61 \x67 \x2e \x74 \x78 \x74 \x00 \xb0 \x34 \x69 \x66 \x66 \x69 \x78 \x20 \x74 \x68 \x65 \x20 \x66 \x69 \x6c \x65 \x20 \x61 \x6e \x64 \x20 \x67 \x65 \x74 \x20 \x74 \x68 \x65 \x20 \x66 \x6c \x61 \x67 \xc4 \x3d \x7b \x00 \x40 \x07 \x00

fix the file and get the flag, 需要进行文件修复 根据末尾以及rar压缩包固定的结束字符串c4 3d 7b 00 40 07 00,进行以下修改 上rar的文件头526172211A0700

参考链接

flag{nev3r_enc0de_t00_sm4ll_fil3_w1th_zip}

36.一个普通胡的压缩包

检查下文件的头尾结构是否有问题,根据文件头判断这是个zip压缩的文件,改后缀名zip,直接解压得到一个目录,目录中两个 文件flag.rar和flag.txt,flag.txt文件很小,二进制、属性内容各种查看确定没有隐藏信息,这样重点就是flag.rar

下载解压得到一个flag.txt打开写着flag不在里面。

用HxD打开压缩包,发现文件头PK,

修改后缀为zip解压, 得到flag.rar文件,解压依然不行

将7A改成74后保存,解压得到一张secret.png图片,用HxD打开发现其实是gif图片

使用stegsolve打开图片,发现R通道含有半个二维码,

使用gifsplitter将gif图片进行分离,得到2张图片,这2张再放进stegsolve分析 得到二维码的一半,将2张图片合并补齐,扫描二维码得到flag

手机扫描二维码得到flag flag{yanji4n_bu_we1shi}

37.2B

binwalk 2B

git clone https://github.com/linyacool/blind-watermark.git

提取水印

python2.7 decode.py --original ./_2B.extracted/B2.png --image 2B --result B2extract.png

得到flag

NUST{I_10v3_2B_F0r3v3r}

40妹子的陌陌

binwalk momo.jpg,

有压缩包

binwalk -e momo.jpg

得到一个rar压缩包,双击发现里面一个txt文件,但是加密了,再次查看题目有没有其他的提示 只有一个,图片上的文字:喜欢我吗.

输入解压密码: 喜欢我吗.

内容: http://c.bugku.com/U2FsdGVkX18tl8Yi7FaGiv6jK1SBxKD30eYb52onYe0=

AES Key: @#@#¥%......¥¥%%.....&¥ 先解开摩斯电码 解密得到网址: HTTP://ENCODE.CHAHUO.COM/ 来自 http://atool.org/morse.php 打开后发现是一个在线加解密的网站。再根据后边的AES key猜想,应该是对进行AES解密得到 momoj2j.png

这样网址就变成了

http://c.bugku.com/momoj2j.png 2018年11月19日15点23分目前该网站已经无法访问。使用已有的图片WriteUP博客 得到一章二维码的图片,但黑白进行了反转。 使用Windows自带的画图工具打开,组合键 crtl+shift+i 来自 https://www.cnblogs.com/zaqzzz/p/9480060.html

扫描得到flag 即KEY{nitmzhen6}

41.就五层你能解开吗?

链接: http://pan.baidu.com/s/1i4TQoz7 密码: w65m 提示: 第一层: CRC32 碰撞 第二层: 维吉尼亚密码 第三层: sha1 碰撞 第四层: md5 相同文件不同 第五层: RSA

来自参考链接

bugku-就五层你能解开吗WP

来自 https://www.cnblogs.com/Byqiyou/p/9410885.html https://blog.csdn.net/preserphy/article/details/79599397 https://www.cnblogs.com/Byqiyou/p/9410885.html

直接解压需要密码

下面试试第一层碰撞

第一层: 第一层: CRC32 碰撞

git clone https://github.com/theonlypwner/crc32

可查看pw1.txt/pw2.txt文件内容 选取: _CRC32_i5_n0t_s4f3 作为解压密码

7z e Challengs: Cryptography+500.7z

第二层: 维吉尼亚密码

继续解压

7z e CRC32\ Collision.7z

cat tips

cat ciphertext.txt

我们来看一下密文。开头是三个字母的单词,常用的三个字母的单词作为开头的就是the、her、she、his、but、and等等, 试一下,假如rla对应的明文是the,那么它的密钥就是YEW

cat keys.txt

密钥: YEWCQGEWCYBNHDHPXOYUBJJPQIRAPSOUIYEOMTSV

解密:

https://www.ctftools.com/down/

the vigenere cipher is a method of encrypting alphabetic text by using a series of different caesar ciphers based on the letters of a keyword it is a simple form of polyalphabetic substitution so password is vigenere cipher funny

vigenere cipher funny

第三层: sha1 碰撞

用密码解密压缩包 vigenere cipher funny

import string import hashlib a=string.maketrans('', '')[33:127] for key1 in a: for key2 in a: for key3 in a: for key4 in a: keys=key1+"7"+key2+"5"+"-"+key3+"4"+key4+"3"+"?" sha1=hashlib.sha1(keys) flag=sha1.hexdigest() if "619c20c" and "a4de755" and "9be9a8b" and "b7cbfa5"and "e8b4365"i\$ print keys break

解压 试试,解压密码 17~5-s4F3?

第四层: md5 相同文件不同 MD5

Hello World □ MD5校验真的安全吗? 有没有两个不同的程序MD5却相同呢? 如果有的话另一个程序输出是什么呢? 解压密码为单行输出结果。

Hello World MD5 check is really safe? There are two different procedures MD5 is the same? If so what is the output of another program? The decompression password is a single-line output.

百度搜索这段话

http://www.win.tue.nl/hashclash/SoftIntCodeSign/HelloWorld-colliding.exe

运行

http://www.win.tue.nl/hashclash/SoftIntCodeSign/GoodbyeWorld-colliding.exe

运行 得到解压密码 Goodbye World □ 来自 https://www.cnblogs.com/alexyuyu/articles/3508110.html

7ze

第五层: RSA 使用Openssl导入公钥,查看模数n和指数e openssl rsa -inform PEM -in rsa_public_key.pem -noout -modulus -text -pubin

可以看到指数(Exponent)很大,在RSA中如果n确定,e非常大,会导致d很小,从而出现维纳攻击,使用连分式(Continued fraction)去求得d。

n= 28FFF9DD3E6FE9781649EB7FE5E9303CF696347C4110BC4BA3969F0B11669840C51D81A6842B6DF2B090F21CD76D4371A8C0E47048C96 5ECA5B46913AFBB8DA052072A0566D7039C618ABA9065759B059E29E485DC5061A16AC63129438D9354E65DF5747546B85DB3D699819C4B7 732DF927C7084A5D52D6E6D6AAC144623425 e= 01:f8:fb:a4:10:05:2d:f7:ed:a3:46:2f:1a:ac:d6: 9e:40:76:04:33:ca:33:57:67:cd:73:05:a3:d0:90: 80:5a:5f:d4:05:dd:6e:ea:70:e9:8f:0c:a1:e1:cf: 25:47:48:67:1b:f0:c9:80:06:c2:0e:ee:1d:62:79: 04:35:09:fe:7a:98:23:8b:43:91:60:a5:61:2d:a7: 1e:90:45:14:e8:12:80:61:7e:30:7c:3c:d3:31:3f: a4:c6:fc:a3:31:59:d0:44:1f:bb:18:d8:3c:af:4b: d4:6f:6b:92:97:a8:0a:14:2d:d6:9b:f1:a3:57:cc: b5:e4:c2:00:b6:d9:0f:15:a3

去掉冒号:

e= 01f8fba410052df7eda3462f1aacd6 9e40760433ca335767cd7305a3d090 805a5fd405dd6eea70e98f0ca1e1cf 254748671bf0c98006c20eee1d6279 043509fe7a98238b439160a5612da7 1e904514e81280617e307c3cd3313f a4c6fca33159d0441fbb18d83caf4b d46f6b9297a80a142dd69bf1a357cc b5e4c200b6d90f15a3

维纳攻击工具

git clone https://github.com/pablocelayes/rsa-wiener-attack.git

修改一下RSAwienerHacker.py中的n值和e值,添上16进制:0x

python RSAwienerHacker.py

Hacked!

得到私钥

d= 8264667972294275017293339772371783322168822149471976834221082393409363691895

知道了私钥d那么就可以生成私钥文件来破解flag,在github上面找的rsatool,根据d,n,e生成私钥rsa private key.pem文件。

git clone https://github.com/ius/rsatool.git

pip install gmpy

python rsatool.py -d 8264667972294275017293339772371783322168822149471976834221082393409363691895 -n 0x28fff9dd3 e6fe9781649eb7fe5e9303cf696347c4110bc4ba3969f0b11669840c51d81a6842b6df2b090f21cd76d4371a8c0e47048c965eca5b46913a fbb8da052072a0566d7039c618aba9065759b059e29e485dc5061a16ac63129438d9354e65df5747546b85db3d699819c4b7732df927c708 4a5d52d6e6d6aac144623425 -e 0x1f8fba410052df7eda3462f1aacd69e40760433ca335767cd7305a3d090805a5fd405dd6eea70e98f0 ca1e1cf254748671bf0c98006c20eee1d6279043509fe7a98238b439160a5612da71e904514e81280617e307c3cd3313fa4c6fca33159d04 41fbb18d83caf4bd46f6b9297a80a142dd69bf1a357ccb5e4c200b6d90f15a3 -o key.pem -f PEM

openssl rsautl -decrypt -in flag.enc -inkey key.pem -out flag.txt

实际命令:

openssl rsautl -decrypt -in ../flag.enc -inkey ./key.pem -out ../get_the_flag.txt cat ../get_the_flag.txt

flag{W0rld_Of_Crypt0gr@phy}

论剑

题解参考 https://www.52pojie.cn/thread-854349-1-1.html

继续用binwalk分析,发现里面有两张图片,

Base16解密 https://www.qqxiuzi.cn/bianma/base.php?type=16

注意: 文件头,base编码,考虑往上一步分析,二进制,jpeg图片高度的修改(不要只掌握png文件的哦) 需要有常见文件头的积累哦,下面附上一部分(也可以去百度,一大把呢。)JPEG(jpg),文件头:FFD8FFE0 PNG(png),文件头: 89504E47 GIF(gif),文件头: 474946383961 ZIP Archive(zip),文件头: 504B0304 RAR Archive(rar),文件头: 52617221 Wave (wav),文件头: 57415645 AVI(avi),文件头: 41564920 Real Audio (ram),文件头: 2E7261FD Real Media (rm),文件头: 2E524D46 MPEG(mpg),文件头: 000001BA MPEG(mpg),文件头: 000001B3 7z文件头: 37 7A BC AF 27 1C



创作打卡挑战赛 赢取流量/现金/CSDN周边激励大奖