BugkuCTF~Misc~WriteUp



50

关注微信公众号:Bugku 即可获取flag

下面也有二维码

qrcode_for_gh_...

get flag:

Qftm{You should sign in}

2、这是一张单纯的图片

这是一张单纯的图片

50

http://123.206.87.240:8002/misc/1.jpg

FLAG在哪里??

查看图片十六进制

1 ±	гэ	то	DЧ	20	10	ച	чэ	тч	00	JТ	чэ	14	00	ы	9 11	40.0-1,b%bwz
DA	78	ЗA	2D	0F	E2	C3	EB	FA	54	0D	0D	BE	AF	03	A 5	Úx:–.âÃëúT¾¯.¥
E7	95	1E	E5	33	0F	98	97	FE	EE	$\mathbf{E}\mathbf{D}$	AA	43	72	01	57	ç•.å3.~-þîíªCr.W
1D	64	06	8 A	28	03	D0	8	A 2	8 A	00	28	A 2	8 A	00	28	.d.Š(.Ш¢Š.(¢Š.(
A 2	8 A	00	$\mathbf{F}\mathbf{F}$	26	23	31	30	37	3B	26	23	31	30	31	3B	¢Š.ÿ& <mark>#107;e</mark>
26	23	31	32	31	3B	26	23	31	32	33	ЗB	26	23	31	32	y{
31	3B	26	23	31	31	31	3В	26	23	31	31	37	3В	26	23	1;ou&#
33	32	3в	26	23	39	37	3в	26	23	31	31	34	3в	26	23	32;ar&#</td></tr><tr><td>31</td><td>30</td><td>31</td><td>3В</td><td>26</td><td>23</td><td>33</td><td>32</td><td>3в</td><td>26</td><td>23</td><td>31</td><td>31</td><td>34</td><td>3В</td><td>26</td><td>101; r&</td></tr><tr><td>23</td><td>31</td><td>30</td><td>35</td><td>3B</td><td>26</td><td>23</td><td>31</td><td>30</td><td>33</td><td>3В</td><td>26</td><td>23</td><td>31</td><td>30</td><td>34</td><td>#105;gh</td></tr><tr><td>3в</td><td>26</td><td>23</td><td>31</td><td>31</td><td>36</td><td>3в</td><td>26</td><td>23</td><td>31</td><td>32</td><td>35</td><td>3B</td><td>D9</td><td>D9</td><td></td><td>;t}<mark>ÙÙ</mark></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></tbody></table>

提去特殊字符串进行解码

ASCII转换到 ASCII (例: a b c)		
key{you are right}		
添加空格 删除空格 译空白字符制	专换	
十六进制转换到十六进制(例:0x61或61或61/62)	□ #	删除 0x
0x6b 0x65 0x79 0x7b 0x79 0x6f 0x75 0x61 0x72 0x65 0x72 0x69 0x67 0x68 0x74 0x7d		
+进制转换到 十进制 (例: 97 98 99)		
107 101 121 123 121 111 117 32 97 114 101 32 114 105 103 104 116 125		
jet flag:		

key{you are right}

3、隐写



2.rar

解压压缩包得到一张图片



打开图片发现只有一个"Bu"可能缺少了什么东西,尝试更改其宽高,得到flag

2. png	x																		
∓ Edit	As:	Hex	Ψ.	Run	Scr	ipt	- F	lun 1	[emp]	late	-								
	Ó	1	2	3	4	5	6	7	8	9	Ą	B	Ç	D	Ę	F	0123456789ABCDEF		
0000h:	89	50	4E	47	0D	A 0	1A	A0	00	00	00	0D	49	48	44	52	%PNGIHDR		
0010h:	00	00	01	F4	00	00	11	Α4	08	06	00	00	00	CB	D6	DF	ô¤ËÖß		
0020h:	8 A	0	00	00	09	70	48	59	73	00	00	12	74	00	00	12	ŠpHYst		
0030h:	74	01	DE	66	1F	78	00	0 0-	A 0	4D	69	43	43	50	50	68	t.Þf.xMiCCPPh		
0040h:	6F	苋4	6F	73	68	бF	70	20	49	43	43	20	70	72	бF	66	otoshop ICC prof		
0050h:	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ilexÚ.SwX"÷.>ß		
0060h:	F7	65	0F	56	42	D8	F0	В1	97	6C	81	00	22	23	AC	08	÷e.VBØð±−l"#¬.		
0070h:	C8	10	59	A 2	10	92	00	61	84	10	12	40	C5	85	88	A 0	È.Y¢.'.a"@Å…^.		
0080h:	56	14	15	11	9C	48	55	C4	82	D5	A 0	48	9D	88	E2	A 0	VœHUÄ,Õ.H.^â		
0090h:	28	в8	67	41	8 A	88	5A	8B	55	5C	38	EE	1F	DC	Α7	B5	(,gAŠ^Z∢U\8î.ܧµ		
00A0h:	7D	7A	\mathbf{EF}	$^{\rm ED}$	\mathbf{ED}	\mathbf{FB}	D7	\mathbf{FB}	BC	E7	9C	E7	\mathbf{FC}	CE	79	CF	}zïííû×û¼çœçüÎyÏ		
00B0h:	0F	80	11	12	26	91	E6	A 2	6A	00	39	52	85	3C	ЗA	D8	.€&`æ¢j.9R…<:Ø		
00C0h:	1F	8F	4 F	48	C4	C9	BD	80	02	15	48	E0	04	20	10	E6	OHÄɽ€Hàæ		
00D0h:	CB	C2	67	05	C5	00	00	F0	03	79	78	7E	74	B0	3F	FC	ËÂg.Åð.yx~t°?ü		
00E0h:	01	AF	6F	00	02	00	70	D5	2E	24	12	C7	E1	FF	83	BA	. opõ.ş.Çáÿf°		

PS: 从第二行开始, 前四位是宽, 后四位是高。

Bu

BUGKU{a1e5aSA}

get flag:

BUGKU{a1e5aSA}

4、telnet



http://123.206.87.240:8002/misc/telnet/1.zip

wires hark打开数据包进行分析,根据提示对telnet进行过滤,get flag。

	telnet											
N	o. Time	Source	Destination	Protocol	Length Info							
	33 16.785629	192.168.221.128	192.168.221.164	TELNET	55 Telnet Data							
	34 16.801229	192.168.221.164	192.168.221.128	TELNET	60 Telnet Data							
	36 17.924431	192.168.221.128	192.168.221.164	TELNET	56 Telnet Data							
	37 17.940031	192.168.221.164	192.168.221.128	TELNET	60 Telnet Data							
	39 17.986831	192.168.221.164	192.168.221.128	TELNET	64 Telnet Data							
	41 18.423632	192.168.221.128	192.168.221.164	TELNET	92 Telnet Data							
	43 19.921235	192.168.221.128	192.168.221.164	TELNET	56 Telnet Data							
	45 19.968035	192.168.221.164	192.168.221.128	TELNET	60 Telnet Data							
	47 21.886838	192.168.221.164	192.168.221.128	TELNET	109 Telnet Data							
	49 26.317246	192.168.221.128	192.168.221.164	TELNET	55 Telnet Data							
	50 26.332846	192.168.221.164	192.168.221.128	TELNET	60 Telnet Data							
	52 27.924049	192.168.221.128	192.168.221.164	TELNET	55 Telnet Data							
	53 27.939649	192.168.221.164	192.168.221.128	TELNET	60 Telnet Data[Malformed Packet]							
	54 27.986449	192.168.221.164	192.168.221.128	TELNET	60 Telnet Data							
	55 27.986449	192.168.221.164	192.168.221.128	TELNET	60 Telnet Data							
>	> Frame 41: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)											
>	Ethernet II, Src: Vm	ware_84:86:5f (00:0c:	29:84:86:5f), Dst: Vm	ware_26:	7e:0e (00:0c:29:26:7e:0e)							
>	Internet Protocol Ve	ersion 4, Src: 192.168	3.221.128, Dst: 192.16	8.221.16	4							
>	Transmission Control	Protocol, Src Port:	1146, Dst Port: 23, S	eq: 83,	Ack: 124, Len: 38							
~	Telnet	· · · · · · · · · · · · · · · · · · ·										
	Data: flag{d31675	9c281bf925d600be698a4	973d5}									
6	1000 00 0c 29 26 7e 0	0e 00 0c 29 84 86 5f	08 00 45 00)&~	.)	F -							
6	0010 00 4e 07 b0 40 0	00 80 06 00 00 c0 a8	dd 80 c0 a8 • N••@••	· · · · - · ·	-							
6	020 dd a4 04 7a 00 1	17 46 01 d4 4e 68 f0	2a 7a 50 18 ····z··F	· ·Nh·*z	ε Ρ -							
6	0030 01 00 3c b7 00 0	00 66 6c 61 67 7b 64	33 31 36 37 ···<···	⁼ l ag{d31	167							
6	0040 35 39 63 3 <mark>2</mark> 38 3	31 62 66 39 32 35 64	36 30 30 62 59c281	of 925d60	00b							
6	0050 65 36 39 38 61 3	34 39 37 33 64 35 7d	e698a49)7 3d5}								

get flag:

flag{d316759c281bf925d600be698a4973d5}

5、眼见非实(ISCCCTF)



解压得到一个word, vi查看文件内容,可以看到有许多目录,猜测word是一个压缩包



word---->zip

									1	终端	1						
File: 1.d	ocx								ASCII	Of	fset	t:)	0x00(000	900	1	0x000036AB (%00)
000000000	50	4B	03	04	0A	00	00	00	00	00	E2	20	0 F	49	00	00	PK
00000010	00	00	00	00	00	00	00	00	00	00	09	00	16	00	D1	DB	
00000020	BC	FB	Β7	C7	CA	B5	2F	75	70	12	00	01	19	91	Α4	C1	/up
00000030	E7	9C	BC	E8	A7	81	E9	9D	9E	E5	AE	9E	2F	50	4B	03	/PK.
00000040	04	0A	00	00	00	00	00	C1	20	0 F	49	00	00	00	00	00	I
00000050	00	00	00	00	00	00	00	13	00	20	00	D1	DB	BC	FB	Β7	
00000060	C7	CA	Β5	2F	63	75	73	74	6F	6D	58	6D	6C	2F	75	70	<pre>/customXml/up</pre>
00000070	1C	00	01	7D	DA	81	AF	E7	9C	BC	E8	Α7	81	E9	9D	9E	}
00000080	E5	AE	9E	2F	63	75	73	74	6F	6D	58	6D	6C	2F	50	4B	/customXml/PK
00000090	03	04	14	00	00	00	08	00	00	00	21	00	35	65	18	58	
000000A0	9D	00	00	00	FE	00	00	00	10	00	29	00	D1	DB	BC	FB)
000000B0	Β7	C7	CA	B5	2F	63	75	73	74	6F	6D	58	6D	6C	2F	69	/customXml/i
000000000	74	65	6D	31	2E	78	6D	6C	75	70	25	00	01	9C	87	34	tem1.xmlup%4
000000D0	11	E7	9C	BC	E8	Α7	81	E9	9D	9E	E5	AE	9E	2F	63	75	/cu
000000E0	73	74	6F	6D	58	6D	6C	2F	69	74	65	6D	31	2E	78	6D	<pre>stomXml/item1.xm</pre>
000000F0	6C	AD	CF	4D	0A	83	30	10	86	Ε1	7D	A1	77	08	39	80	lM0}.w.9.
00000100	91	2E	5C	88	0A	42	DD	D6	42	AO	AB	6E	92	38	9A	40	\BBn.8.@
00000110	7E	24	19	41	6F	DF	20	Α5	27	E8	72	F8	1E	5E	98	46	~\$.Ao'.r^.F
00000120	DG	20	60	51	41	22	10	20	20	0.4	00	E2	61	Λ 1	45	CC	<104" (2

解压word压缩包,得到许多xml文件,遍历内容得到flag



get flag:

flag{F1@g}

6、啊哒

啊哒 50

有趣的表情包

来源:第七届山东省大学生网络安全技能大赛

1cdf3a75-21ed-... Flag

Submit

查看图片属性,得到特殊数据

	ada.j	pg 属性					\times
堂	¢‡∏	安全	详细信息	以前的版本			
		~		-9433B31041			
	属性		值				^
	高度		672 像素				
	水平	分辨率	96 dpi				
	垂直	分辨率	96 dpi				
	位深	度	24				
	压缩						
	分辨	率单位					
	颜色	表示					
	压缩	的位/像素					
	照相	퇘					
	照相	机制造商					
	照相	机型号	73646E69	973635F323	03138		
	光圈	值					
	曝光	时间					
	ISO	速度					
	曝光	补偿					
	焦距						
	最大	光圈					
	测光	模式					
	目标	距离					
	闪光	灯模式					
	闪光	灯能量					~
			(左自				
	加州的东方						
				确定	取消	J.	应用(A)

解码十六进制得到一个字符串

ASCII转换到 ASCII (例: a b c)
sdnisc_2018
1
添加空格 删除空格 网络空白字符转换
十六进制转换到十六进制(例:0x61或61或61/62) 🗏 删除 0x
0x730x640x6e0x690x730x630x5f0x320x300x310x38
十进制转换到 十进制 (例: 97 98 99)
115100110105115999550484956

提交,发现并不是flag,binwalk分析得到压缩包里面有一个flag.txt被加密,使用上面解出的字符串作为密码得到 flag

ada.jpg	 ○ 最近使用 	ZIP 35695.zip	flag.txt							
tracted			终端							
	→_∮录片:~/桌面# binwalk ada.jpg -e									
	DECIMAL	HEXADECIMAL	DESCRIPTION							
	0 ^{公 下載} 30 _{7 音乐} directory:	0x0 0x1E 8	JPEG image data, JFIF st TIFF image data, big-end	andard 1.01 ian, offset of first image						
	5236回收站 7782 > <td>0x1474 0x1E66 a></td> <td colspan="5">Copyright string: "Copyright Apple Inc., 2018" Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns</td>	0x1474 0x1E66 a>	Copyright string: "Copyright Apple Inc., 2018" Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns							
	218773	0x35695 sed size: 34. un	Zip archive data, encrypted at least v2.0 to a compressed size: 22. name: flag.txt							
	218935	0x35737	End of Zip archive							
	û 位置(L):	i /								
			▼ 大小	۱						

打开(O) - 凡	flag.txt ~/.cache/.fr-ymz6dC	保存(S)	≡	•••
flag{3XiF_iNf0rM@ti0n}				

get flag:

flag{3XiF_iNf0rM@ti0n}

7、又一张图片,还单纯吗

又一张图片,还单纯吗

http://123.206.87.240:8002/misc/2.jpg

好像和上一个有点不一样

Flag		Submit
------	--	--------

binwalk分析可知里面存在其它图片,利用foremost快速得到其中的图片



get flag:

falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

猜 60

http://123.206.87.240:8002/misc/cai/QQ20170221-132626.png

flag格式key{某人名字全拼}

Flag	Submit

根据提示,尝试进行图片识别



识图得到: 刘亦菲





刘亦菲(华语影视女演员、...

刘亦菲,1987年8月25日出生于湖北省武汉市,华语影视女演员、歌手,毕业于北京电影学院2002级表演系本科 班。2002年主演个人首部电视剧《金粉世家》,从而踏入演艺圈。2003年因主演或侠剧《天龙八部》崭露头角。2 004年凭借仙侠剧《仙剑奇侠传》起灵儿一角获得了高人气与关注度。2005年因在或侠剧《神雕侠侣》中饰演小龙 女受到广泛关注。2006年发行首张国语专辑《刘亦菲》和日文专辑《A... **百度百升** 搜索更多相关结果 → 9、宽带信息泄露

宽带信息泄露	
60	

flag格式: flag{宽带用户名}

conf.bin
Flag

根据提示,则需要找到某个用户,下载的文件是一个配置文件,可能是路由器的配置文件,使用工具 RouterPassView打开查看宽带用户

File	Edit View Options Help	
🚔	e 🔚 🗈 🖆 🖏 📲	
	<addressingtype val="DHCP"></addressingtype>	
	<externalipaddress val="0.0.0.0"></externalipaddress>	
	<subnetmask val="0.0.0.0"></subnetmask>	
	<defaultgateway val="0.0.0.0"></defaultgateway>	
	<dnsservers val="0.0.0.0,0.0.0.0"></dnsservers>	
	<macaddress val="D0:C7:C0:43:53:69"></macaddress>	
	<x_tp_ifname_val=eth1></x_tp_ifname_val=eth1>	
	<pre><wanipconnection nextinstance="3"></wanipconnection></pre>	
	<pre><wanpppconnection instance="1"></wanpppconnection></pre>	
	<pre><enable val="1"></enable></pre>	
	<pre><defaultgateway val="10.177.144.1"></defaultgateway></pre>	
	<name val="pppoe_eth1_d"></name>	
	<uptime val="6/1521"></uptime>	
	<pre><username val="053/0035/621"></username></pre>	
	<pre><password val="210205"></password></pre>	
	<x_ip_ifname_val=ppp0></x_ip_ifname_val=ppp0>	
	<x_ip_l2i+name_val=eth1></x_ip_l2i+name_val=eth1>	
	<pre><x_ip_connectionic val="1"></x_ip_connectionic> </pre>	
	<pre>(ExternallPhooress val=10.1//.150.82 /) (Deach-IDAdduese val 40.427 4bb 4 /)</pre>	
	<pre><kemotelrhooress val="10.1//.144.1"></kemotelrhooress> </pre>	
-		

PS: RouterPassView可以帮助你从你的路由器恢复您丢失密码的文件。

get flag;

flag{053700357621}

隐写2 60



foremost分离图片中存在文件,根据提示进行压缩包爆破



ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

取出图片查看其十六进制得到flag



eTB11EFyZSBh1GhAY2t1ciE=
加容 解容 ■解容结果以1人进制显子
y0u Are a h@cker!

get flag:

flag{y0u Are a h@cker!}

11、多种方法解决

多种方法解决 60

在做题过程中你会得到一个二维码图片

http://123.206.87.240:8002/misc/3.zip

查看key.exe十六进制得到二维码,扫描get flag

S	tartup 💿 KEY. exe 🗃
Ŧ	Edit As: Text /wrap - Run Script - Run Template -
	<u>0 10 20</u> 30 40 50 60 70 80
1	
-	ARRQUIBAACH;wv0YQUAAAA;DcEhZcwAADsMAAA7DAcdvqGQAAArZSURBVHhe7ZKBitxIFgTv/396Tx564G1Uouic
-	Kg19hwPCDcrMJ9m7/7n45zfdxe5z3sJ7prHbf9rX03P4lLvYPctbeM80dvtP+3pnDp9yF7tneQvvmcZu/21f78z
-	hU+5i9yxv4T3T200/7eud680T2H3LCft01/ae9Z1To+23pPvX7/rwJHbfcsI+3aW9Z33m1Gj7Len+9bs+PIndt5
-	ywT3dp71mfoTXafku6f/2uD09i9y0n7NNd2nvWZ06Ntt+S71+/68MJc5000SWpcyexnFjfcsI+JW1ukpRfv+vDC
-	XOTtDklqXMnsZxY33LCPiVtbpKUX7/rwwlzk7Q5JalzJ7GcWN9ywj4lbW6SlF+/68MJc5000SWpcyexnFjfcsI+
-	JW1ukpRfv+vDCXOTWE7a/i72PstJ2zfsHnOTpPz6XR9OmJvEctL2d7H3WU7avmH3mJsk5dfv+nDC3CSWk7a/i73
-	PctL2DbvH3CQpv37XhxPmJrGctP1d7H2Wk7Zv2D3mJkn59bs+nDA3ieWEfdNImylJnelp7H6bmyT11+/6cMLcJJ
-	YT9k0jbaYkdaansfttbpKUX7/rwwlzk1h02DeNtJmS1Jmexu63uUlSfv2uDyfMTWI5Yd800mZKUmd6Grvf5iZJ+
-	fW7PjzJ7v12b33LSdtvsfuW75LuX7/rw5Ps3m/31rectP0Wu2/5Lun+9bs+PMnu/XZvfctJ22+x+5bvku5fv+vD
-	k+zeb/fWt5y0/Ra7b/ku6f71+++HT0v+513+tK935vApyd+8y5/29c4cPiX5m3f5077emcOnJH/zLn/ar3d+/f1
-	BpI+cMDeNtJkSywn79BP5uK+yfzTmppE2U2I5YZ9+Ih/3VfaPxtw00mZKLCfs00/k477K/tGYm0baTInlhH36is
-	xflT78TpI605bdPbF7lhvct54mvWOaWJ6m4Z0kdaYtu3ti9yw3uG89TXrHNLE8TcM7SepMW3b3xO5ZbnDfepr0j
-	mlieZqGd5LUmbbs7onds9zgvvU06R3TxPXcSxPrW07YpyR1pqTNKUmdKUmdk5LUaXzdWB/eYX3LCfuUpM6UtDk1
-	qTMlqXNSkjqNrxvrwzusbzlhn5LUmZI2pyR1piR1TkpSp/F1Y314h/UtJ+xTkjpT0uaUpM6UpM5JSeo0ft34+v0

点击这里选择选择要转换成Base64的图片

复制 清空

ח/דיט+paitk90/15113//////wb3L5f508/000210///wxxxcy/tyrcb+x1w/qvvk/Zr1u9be9dzL+1g9y0n/דיט+paitk90 71sT1/P7EnOTWG5wb5LUmRptn3D/6b6+eX04YW4Syw3uTZI6U6PtE+4/3dc3rw8nzE1iucG9SVJnarR9wv2n+/rm9eGE $uUksN7g3SepMjbZPuP90X9+8PpwwN0mb72pYfzcn1rf8NHwffXXWhxPmJmnzXQ3r7+bE+pafhu+jr876cMLcJG2+q2Particle{2} and a strength of the strength of the$ H93ZxY3/LT8H301VkfTpibpM13Nay/mxPrW34avo++OuvDCXOT7OZGu7e+5YT9XYnIhH36DlfvfsTcJLu50e6tbzIhf1diinester the standard staOWG fvsPVux8xN8 lubrR761 tO2N + VWE7Yp + 9w9e5HzE2ymxvt3vqWE/Z3JZYT9uk7XL1 + 1GD3LX8avt8klhu2t5yc6F + / 6W22M24000 + 2W22M24000 + 2W22M24000 + 2W22M24000 + 2W22M2400 + 2W22W2400 + 2W22M2400 + 2W22W2400 + 2W2400 + 2W22W24000 + 2W2400 + 2W24000 + 2W22W24000 + 2W22W24000 + 2W22W2400 + 2W2400 + 2W22W2400 + 2W2400 + 2W2400 + 2W22W2400 + 2W2400 + 2W24000 + 2W2400 + 2W2400 + 2W2400 + 2W2408OT2H3Ln4bvN4nlhu0tJyf61+/68CR23/Kn4ftNYrlhe8vJif71uz48id23/Gn4fpNYbtjecnKif/3+++HTnub0fd4zieUtvLfrO1 wAAAABJRU5ErkJggg==

还原生成的Base64编码为图片:



get flag:

KEY{dca57f966e4e4e31fd5b15417da63269}

12、闪的好快

闪的好快

60

这是二维码吗? 嗯。。。是二维码了, 我靠, 闪的好快。。。

题目来源: 第七季极客大挑战

masterGO.gif

打开图片发现是动图,并且每一帧的动画都是一个二维码,尝试分离每一帧,使用工具GifSplitter进行分离,但 是分离出来的二维码不完整



















MG00007.bmp

IMG00008.bmp

DXD IMG00009.bmp



IMG00010.bmp IMG00011.bmp



此时可以利用工具Stegsolve进行每一帧的浏览



通过扫码发现每一帧都存在一个字符,将这18个字符进行拼接得到flag

get flag:

SYC{F1aSh_so_f4sT}

13、come_game



听说游戏通关就有flag 题目来源:第七季极客大挑战

game_1.zip

通过玩游戏(当游戏玩到第二关的时候)可以得到游戏配置文件 save1,十六进制查看 save1,猜测字符2为通关的数字

	Q	1	2	3	4	5	6	7	8	9	A	B	Ċ	D	E	F	0123456789ABCDEF
:	00	01	32	00	00	41	00	05	43	00	00	00	00	00	00	00	.2AC
:	00	00	00	00	00	00	00	00	00	00	00	00	00				L

尝试将其修改为33 34 35,当到了第5关的时候可以得到flag,游戏通关



get flag:

SYC{6E23F259D98DF153} #flag格式有问题

14、白哥的鸽子

白哥的鸽子 60

咕咕咕

jpg

将文件放入十六进制编辑器中,在后面得到一串特殊字符串

8D 47 DA 3E D1 EE CF 94 1A E6 2A C5 8E 3C F8 00 .GÚ>Ñîï".æ*ÅŽ<ø. EA 03 A8 35 12 39 F0 8E 6C A2 9E 1D 66 E2 BB 87 ê."5.90Ž1¢ž.f⻇ 74 F7 4B 65 B0 58 2F 01 3A 92 BF 1E 73 2A C7 49 t÷Ke°X/.:'¿.s*ÇI E6 03 A7 9D 14 11 1D 79 D0 9D 28 0E A5 1D 40 20 æ.syD.(.¥.@ 78 DC 59 69 DA 8F 64 6E E6 7B A3 57 31 EE 8D DC CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67 2ivyiú.dnæ{£W11.Ü Ebb‰î[ܶs.ăÿÙfg 2ivyo]1{2s3_0@aw 5F 5F 72 63 6C 40 E																	
EA 03 A8 35 12 39 F0 8E 6C A2 9E 1D 66 E2 BB 87 74 F7 4B 65 B0 58 2F 01 3A 92 BF 1E 73 2A C7 49 E6 03 A7 9D 14 11 1D 79 D0 9D 28 0E A5 1D 40 20 78 DC 59 69 DA 8F 64 6E E6 7B A3 57 31 EE 8D DC CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67 32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77 SF 5F 72 63 6C 40 F 5F	8D	47	DA	3E	D1	EE	CF	94	1A	Eб	2A	C5	8E	3C	F 8	00	.GÚ>ÑîÏ″.æ*ÅŽ<ø.
74 F7 4B 65 B0 58 2F 01 3A 92 BF 1E 73 2A C7 49 t÷Ke°X/.:'¿.s*ÇI E6 03 A7 9D 14 11 1D 79 D0 9D 28 0E A5 1D 40 20 78 DC 59 69 DA 8F 64 6E E6 7B A3 57 31 EE 8D DC xÜYiÚ.dmæ{£W11.Ü CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67 32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77 21 29 67 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77 21 29 67 67 66 74 6	EA	03	A 8	35	12	39	F0	8E	6C	A 2	9E	1D	66	E2	BB	87	ê.¨5.9ðžl¢ž.f⻇
E6 03 A7 9D 14 11 1D 79 D0 9D 28 0E A5 1D 40 20 78 DC 59 69 DA 8F 64 6E E6 7B A3 57 31 EE 8D DC CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67 32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77 5F 5F 72 63 6C 40 E223 0@aw rcl@	74	F7	4B	65	в0	58	2F	01	ЗA	92	BF	1E	73	2A	C7	49	t÷Ke°X/.:'¿.s*ÇI
78 DC 59 69 DA 8F 64 6E E6 7B A3 57 31 EE 8D DC xÜYiÚ.dnæ{£W1î.Ü CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67 32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77 EbEb‰î[ܶs.ãÿÙfg 32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77 Event Event 5F 5F 72 63 6C 40 rcl@	E6	03	Α7	9D	14	11	1D	79	D0	9D	28	0E	A 5	1D	40	20	æ.§yÐ.(.¥.@
CB 62 45 62 89 EE 5B DC B6 73 01 E3 FF D9 66 67 32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77 5F 5F 72 63 6C 40 Crcl@	78	DC	59	69	DA	8F	64	6E	E6	7B	A3	57	31	EE	8D	DC	xÜYiÚ.dnæ{£Wlî.Ü
32 69 76 79 6F 7D 6C 7B 32 73 33 5F 6F 40 61 77 5F 5F 72 63 6C 40 	CB	62	45	62	89	EE	5B	DC	в6	73	01	E3	FF	D9	66	67	ËbEb‰î[ܶs.ãÿÙ <mark>fg</mark>
5F 5F 72 63 6C 40	32	69	76	79	6F	7D	6C	7в	32	73	33	5F	6F	40	61	77	2ivyo}l{2s3_0@aw
	5F	5F	72	63	6C	40											rcl@

将字符串进行栅栏解密得到flag

栅栏密码

在下面的文本框输入明文或密文, 点加密或解密, 文本框中即可出现所得结果

加密 解密 列举加密 列举解密 栏数: 2	☑ 只列举完整匹配的												
密文框:													
fg2ivyo}l{2s3_o@awrcl@													
2栏:													
f3g_2oi@vaywo_}_lr{c2ls@													
3栏:													
4栏: fo3_g}2lori{@cv2alysw@													
6栏: fvl3argy{_wc2o2o_li}s0_0													
8栏: fio{30_cgv}2_a_l2ylsowr0													
12栏: f2vol23oa_rlgiy}{s_@w_c@													

get flag:

flag{w22_is_v3ry_cool}

15、linux



http://123.206.87.240:8002/misc/1.tar.gz linux基础问题

终端下cat flag得到flag



get flag:

16、隐写3



58d54bd3e134...

下载图片发现图片高度不正常,尝试更改,得到flag



get flag:

flag{He1l0_d4_ba1}

17、做个游戏(08067CTF)



坚持60秒

heiheihei.jar

懂点Android逆向的人都会很快做出来,使用jd-gui查看Java代码,在PlaneGameFrame.class文件中得到flag

MANIFEST. MF	
🖨 🌐 cn. bjsxt	m hreak!
🛱 🖶 plane	
🕀 🌆 Bullet. class	case 4:
🕀 🎰 Explode. class	nrintInfo(g "加油你就是下一个考末" 50 150 300);
🖨 🍈 GameObject. class	
🗄 🕒 GameObject	71 break;
🕀 🄚 Plane. class	CORD ET
🖨 🚮 PlaneGameFrame. class 🦳	Case 5.
🕀 🕒 PlaneGameFrame	┃ 73 printInfo(g, "如果撑过一分钟我岂不是很没面子", 40, 30, 300);
🖨 🌐 util	heady
Constant, class	74 Dreak;
H G Constant	case b:
E-& Gamelltil class	
Gamelitil	$\frac{printinto(g, "tiag{RGFqaURnbGitSmiud2FuQ2npamk=}", 50, 150, 300);}{printinto(g, "tiag{RGFqaURnbGitSmiud2FuQ2npamk=}", 50, 150, 300);}$
	77 break:
H G WyFrane	
- # inages	
- # evplode	Ъ.
ol gif	
elo.gli	
ell.gli	
eiz.gii	public void printInfo(Graphics g, String str, int size, int x, int y)
e14.g11	• 1
elb.git	20 Color c = g.getColor():
	g.setColor(Color.RED);
e3.g1t	92 Font f = new Font("宋体", 1, size):
e4. gif	
e5. gif	93 g.setFont(+);
e6. gif	σ σ σ σ
e7. gif	B. G. G. G. C. J. K. J.
e8.gif	<pre>g.setColor(c);</pre>
ball.png	1
bg. jpg	
plane.png	public static void main(String[] ange)
	public static void main(string[] args)
	•
	new Dispectane Energy () lower because ().
	101 new <u>PlaneGamerrame().launchrrame();</u>
RGFgaURhbGlfSmlud2FuQ2hpamk=	

加密 解密 □解密结果以16进制显示

DajiDali_JinwanChiji

get flag:

flag{DajiDali_JinwanChiji}

18、想蹭网先解开密码

想蹭网先解开密码 100

flag格式: flag{你破解的WiFi密码}

tips: 密码为手机号,为了不为难你,大佬特地让我悄悄地把前七位告诉你 1391040** Goodluck!!

作者@NewBee

wifi.cap

根据tips密码为手机号,现在知道密码前7位,后四位可通过爆破得到,利用Linux下的crunch工具辅助爆破。

PS: Crunch是一种创建密码字典工具,该字典通常用于暴力破解。使用Crunch工具生成的密码可以发送到终端、文件或另一个程序。

crunch [minimum length] [maximum length] [character set] [options]

crunch命令常用的选项如下所示。

-o: 用于指定输出字典文件的位置。 -b: 指定写入文件最大的字节数。该大小可以指定KB、MB或GB, 但是必须与-o START选项一起使用。 -t: 设置使用的特殊格式。 -1: 该选项用于当-t选项指定@、%或^时,用来识别占位符的一些字符。

生成Wifi.txt字典



PS: 命令解析

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

最小11 最大11

-t	指定模式
@	插入小写字母
ر	插入大写字母
%	插入数字

^ 插入特殊符号

利用Linux下Wifi破解工具aircrack-ng破解wifi.cap密码

						丝	端										
[00:00:03] 7688/	9999) ke	eys	te	ste	d (:	224	7.1	1 k,	/s)							
Time left: 1 sec	ond														76.8	89%	
	[KE١	(F(ואטכ	D !	[1:	391	940	768	6]							
Master Key :	C4 0B	60 E1	FE CD	8B 81	14 07	7D F8	58 28	00 DB	91 EA	D7 76	0A 1E	9C ED	3C 81	DE A3	44 FF	69 FD	
Transient Key :	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00	00 00 00	00 00 00 00								
EAPOL HMAC : →∮←:~/桌面# aircrad	1C ck-r	E7 1g -	D0 •w V	96 Vif:	DE i.t:	87 kt \	93 wif:	56 i.c	88 ap	1D	08	С8	B9	AA	В3	BO	

get flag:

flag{13910407686}

19、Linux2

Linux2 100

给你点提示吧: key的格式是KEY{} 题目地址: 链接:http://pan.baidu.com/s/1skJ6t7R 密码:s7jy

根据提示,使用Linux下grep搜索关键字KEY得到flag

→ ∮ ← :~/桌面# grep "KEY" -an brave

PS: a代表二进制问价、n代表字符串出现的位置

.→∮ ← :~/桌面# grep "KEY" -an b <u>rave</u>	
94:0q00)'.7(🗊 🗊 00A000000'0p3000HKEY{24f3627a86fc740a7f36ee2c7a1c124a}	
7535:08L000~B00000 0?0)Y0 🔠 🔠 😽 😽 😽 😽 🕹 🖬 🖓 🖬 🖉 🖉 🖉 👘 🖉 🖉 👘 👘 👘 👘 🖓 👘 👘 👘 🖓 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘	'ûØZ'ØØØ
U3210#"! 🔚 Utp 🗊 🔚 adôô 🔢 🕅 KEY { } ô 🖩 NÔ 🗊 Pô 🔚 🛛 Ô 🗊 Ô 2 Vôô Sô 🗒 Ô 2 V 🖩	
Ô <u></u> ₩- ⊡ ₽₩-{00\	w@? 000 00
Û;ÛÛÛÎÛFrgx3Ûr[]]Û[]]]	
0	888888888
000000000000000000000000000000000000000	000000000

get flag:

KEY{24f3627a86fc740a7f36ee2c7a1c124a}

20、账号被盗了

http://123.206.87.240:9001/

修改cookie得到新的Url

http://123.206.87.240:9001/123.exe

Login游戏界面



填写信息进行抓包,真的可以刷枪,你信不233333

过滤TCP可以看到特殊流量

📕 tc	p.stream eq 5						
No.	Time	Source	Destination	Protocol Le	ngth Inf∘		
	15 0.744293	192.168.2.129	183.232.93.144	TCP	62 61437 → 25 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK	_PERM=1	
	16 0.787505	183.232.93.144	192.168.2.129	ТСР	58 25 → 61437 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M	SS=1460	
	17 0.788305	192.168.2.129	183.232.93.144	TCP	54 61437 → 25 [ACK] Sea=1 Ack=1 Win=64240 Len=0		
	18 0.841664	183.232.93.144	192.168.2.129	SMTP	92 S: 220 smtp.qq.com Esmtp QQ Mail Server		
	19 0.944333	Winschart, Falley, TCD Street		luuran Naturada Arlan	+ \/\/ # - + 0		
	20 0.944862	Wileshark · Follow TCP Strea	in (tcp.stream eq 5) · viv	Iware Network Adap	ter vivilleto		^
	25 1.055798	220 amta az azm Famta (no Mail Camura				
	26 1.056274		y mail server				
	35 1.097540	250-smtp gg com					
	36 1.193756	250-PTPELINING					
	37 1.194271	250-SIZE 73400320					
	38 1.313610	250-STARTTLS					
	39 1.314194	250-AUTH LOGIN PLAIN					
	40 1.416838	250-AUTH=LOGIN					
	41 1.519603	250-MAILCOMPRESS					
	42 1.520121	250 8BITMIME	_				
> F	rame 18: 92 bvt	AUTH LOGIN					
> E	thernet II. Src	334 VXN1cm5hbWU6					
> 1	nternet Protoco	YMTJOGZOZXNOQDE2My5jb20	ð=				
> T	ransmission Con						
> s	imple Mail Tran	535 Error:	h	ttn://service.m	ail.gg.com/cgi-bin/belp?subtype=1&&id=28&&po=1001256		
		OUIT		repr//servicen	arriggroom, cgr orn, herp, subtype=raara=20aano=1001250		
		221 Bye					
000	0 00 01 20 hf						
000	0 00 0C 29 DT						

YmtjdGZOZXNOQDE2My5jb20=	YTEyMzQ1Ng==						
1. 赤 47 赤 「47 赤ム 日 い142 洗生」日二							
加留 解留 ■ 解密结末以10近前业小 bkctftest@163 com	加密 解密 ■解密结果以16进制显示						
	a123456						

利用账号登陆163邮箱得到flag

★ KEY值所在处(1)
 ■ 1.7析飞含岛 价格塔比高铁系 立即出发>>
 草稿箱(1)
 flag{182100518+725593795416}

get flag:

flag{182100518+725593795416}

21、细心的大象

细心的大象 100

https://share.weiyun.com/9287be0a629971ac53d97f39727eee18

Flag

Submit

查看图片属性

属性	值	^
说明		
标题	出题人已经跑路了	
主题	出题人已经跑路了	
分级	$\diamondsuit \diamondsuit \diamondsuit \diamondsuit \diamondsuit$	
标记		
备注	TVNEUzQ1NkFTRDEyM3p6	
来源	-	
作者		
拍摄日期		
程序名称	×	
获取日期		
版权		
图像 ———		
图像 ID		
分辨率	3016 x 4032	
中庄	2016	

foremost分离处压缩包,利用图片备注信息base64解码进行解密得到图片,修改图片高度得到flag

	Y	+	4	4	-	~	Y	1	Y	1	4.4	4	×.	4		-	944919919910910900
:	89	50	4E	47	0D	A 0	1A	A 0	00	00	00	0D	49	48	44	52	%PNGIHDR
:	00	00	01	F4	00	00	11	Α4	08	06	00	00	00	CB	D6	DF	ô¤ËÖß
:	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	ŠpHYst
:	74	01	DE	66	1F	78	00	00	A 0	$4\mathrm{D}$	69	43	43	50	50	68	t.Þf.xMiCCPPh
:	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	otoshop ICC prof
:	69	6C	65	00	00	78	$\mathbf{D}\mathbf{A}$	9D	53	77	58	93	F7	16	3E	DF	ilexÚ.SwX"÷.>ß
:	F7	65	0F	56	42	D8	F0	B1	97	6C	81	00	22	23	$\mathbf{A}\mathbf{C}$	80	÷e.VBØð±−1"#¬.
:	C8	10	59	Α2	10	92	00	61	84	10	12	40	C5	85	88	A 0	È.Y¢.'.a"@Å…^.
:	56	14	15	11	9C	48	55	C4	82	D5	A 0	48	9D	88	E2	A 0	VœHUÄ,Õ.H.^â
:	28	B8	67	41	8 A	88	5A	8B	55	5C	38	EE	1F	DC	Α7	B5	(,gAŠ^Z <u\8î.ܧµ< th=""></u\8î.ܧµ<>
:	7D	7A	\mathbf{EF}	\mathbf{ED}	\mathbf{ED}	FB	D7	FB	BC	E7	9C	Е7	FC	CE	79	CF	}zïííû×û¼çœçüÎyÏ
:	0F	80	11	12	26	91	E6	A 2	6A	00	39	52	85	3C	ЗA	D8	.€&`æ¢j.9R…<:Ø
:	1F	8F	$4 \mathrm{F}$	48	C4	C9	BD	80	02	15	48	$\mathbf{E0}$	04	20	10	E6	OHÄɽ€Hàæ
:	CB	C2	67	05	C5	00	00	F0	03	79	78	7E	74	в0	3F	FC	ËÂg.Åð.yx~t°?ü
:	01	AF	6F	00	02	00	70	D5	2E	24	12	C7	E1	$\mathbf{F}\mathbf{F}$	83	BA	.¯opÕ.\$.Çáÿf°
•	50	26	57	00	20	91	00	F.O	22	12	F.7	0R	01	90	52	00	P&W `à" ຕ R

Value

Bu

BUGKU{a1e5aSA}

get flag:

Address

BUGKU{a1e5aSA}

22、爆照(08067CTF)



flag格式flag{xxx_xxx_xxx}

8.jpg
lag

binwalk分析图片发现隐藏文件,利用binwalk和foremost分离隐藏文件,只能得到88文件其他的不到,此时利用 dd命令进行分离

→ ∮ / 桌面	# binwalk 8.jpg	☆ 主目录	00000079.
_8.jpg. DECIMAC ^{ted}	HEXADECIMAL	■ 桌面 TTON ■ 视频	
0		nagalata, JF	
40499 4889 ^{901put}		L 文档data, e	encrypted at least v2.0 to extr act, compressed size: 8362, uncompressed size: 92278, name: 8.
63830		chǎivīc载data, a	at least v2.0 to extract, compressed size: 1129, uncompressed size: 18479, name: 888
74992		以 _{皆乐} data, a	at least v2.0 to extract, compressed size: 10371, uncompressed size: 11782, name: 8888
92377 ⁸⁸		雷、圆收稿ta, a	at least v2.0 to extract, compressed size: 0445, uncompressed size: 92270, name: 00000 at least v2.0 to extract, compressed size: 0824, uncompressed size: 92278, name: 888888
99237		chive data, a 	at least v2.0 to extract, compressed size: 7076, uncompressed size: 92278, name: 8888888
168452			n t teast vz.o to extract, compressed size, dei9, uncompressed size, 92270, name, 00000000
→ ∮ ← :~/桌面			

dd if=8.jpg of=11 skip=48892 bs=1



得到几张图片



binwalk分析这几张图片,发现前三张存在被修改的记录



第一张包含二维码直接扫描得到: bilibili



第二张图片属性中存在特殊字符串,对其进行解码

🤮 888.jpg 屬性		c2lsaXNpbGk=
常规 安全	详细信息 以前的版本	
属性	值 ^	
标题		
主题		
分级	$ \diamondsuit \ \diamondsuit \ \diamondsuit \ \checkmark \ \diamondsuit \ \checkmark \ \checkmark \ \checkmark \ \checkmark \ \checkmark \$	
标记		
备注 来源 ———	c2lsaXNpbGk=	加密 解密 □解密结果以16进制显示
作者		
拍摄日期		silisili
程序名称		
获取日期		
版权		

第三张图片binwalk分析,分离出压缩包,得到一张二维码,扫描得到: panama

QR Research	– 🗆 X
文件(F) 工具(T) 帮助(H)	
🔜 🔛 🞑 🔌 📀	
	纠错等级 H(30%) ▼ Auto Auto Auto Auto
	^
一口般现物捉。	×
	- -
解码完成	

根据题目flag提示,将上述得到的三个字符串组合成最终的flag

get flag:

flag{bilibili_silisili_panama}

猫片(安恒) 100

hint:LSB BGR NTFS



根据提示LSB隐写得到新的二维码

(Geo	_	- 🗆	×
Extract Preview			
Extract Preview fffe89504e470d0a 1a0a000000d4948 PNGIH 445200001180000 008c08020000008 DR	⊖ I irst	Column	
Blue 7 6 5 4 3 2 1 0 Bit Plane Order Blue 7 6 5 4 3 2 1 0 Preview Settings	RB		
Include Hex Dump In Preview 🗹	UN		
Preview Save Text Save Bin Cancel			

修改图片头部得到二维码

As: Hex - Run Script - Run Template -^ 0 1 2 3 4 5 6 7 8 9 A B C D E F 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 01 18 00 00 00 8C 08 02 00 00 00 8 EC 7E 0123456789ABCDEF DNG.....IHDRì~ Û...œIDATxœíÝQj. DB 00 00 05 9C 49 44 41 54 78 9C ED DD 51 6A 1C
 B
 B
 C
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 D
 <thD</th>
 <thD</th>
 <thD</th>
 <thD</th>
 ;.@Á8dÿ[v...P87' ìªß7⁻ÝîñA.<ô?~..ÀŸ>Vÿáóóó.ÞÇ ?ûøXþ.‰ÕsØý¹ó×Y© 00.png 9E CF EE FD 57 9F BF CD EA FE 7F FE E7 FB 80 2F žÎîýWŸ;Íêþ.þçû€/ IH...,.!A@H... .~íþ.ós>•Ý9ÃôŨcú 49 48 10 10 12 04 84 04 01 21 41 40 48 10 10 12 04 7E ED FE OF D3 73 9B 95 DD 39 C3 F4 DC 63 FA E7 AE 9C 9A 5F 4D 7F 7E FA 3A BB 76 BF 17 2B 12 箜š_M.∼ú:»v;.+. 04 84 04 01 21 41 40 48 10 10 12 04 84 04 01 21 ."..!A@H...."..!

下意识修改图片高度,得到完整二维码

	ŭ,	-	-	<u> </u>	Ť	~	,	1	, i	-			<u> </u>	-		-	
h:	89	50	4E	47	0D	A 0	1A	0 A	00	00	00	0D	49	48	44	52	%PNGIHDR
h:	00	00	01	18	00	00	01	8C	08	02	00	00	00	08	EC	7E	ì~
h:	DB	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	6A	1C	ÛœIDATxœíÝQj.
h:	3B	14	40	C1	38	64	FF	5B	76	16	10	14	50	38	37	92	;.@Á8dÿ[vP87′
h:	EC	AA	DF	37	AF	DD	EE	F1	41	90	8B	D4	3F	7E	00	00	ìªß7 [—] ÝîñA.∢Ô?~
h:	00	00	00	00	C0	9F	3E	56	FF	E1	F3	F3	F3	7F	DE	C7	ÀŸ>Vÿáóóó.⊅Ç
h:	3F	FB	F8	58	FE	A 0	89	D5	73	D8	FD	в9	D3	D7	59	A9	?ûøXþ.‰ÕsØý¹Ó×Y©
h:	9E	CF	EE	FD	57	9F	BF	CD	EA	FE	7F	FE	E7	FB	80	2F	žÏîý₩Ÿ;Íêþ.þçû€/
h:	49	48	10	10	12	04	84	04	01	21	41	40	48	10	10	12	IH"!A@H
h:	04	7E	ED	FE	0F	D3	73	9B	95	DD	39	C3	F4	DC	63	FA	.~íþ.Ós≯•Ý9ÃôÜcú
h:	E7	AE	9C	9A	5F	4 D	7F	7E	FA	3A	BB	76	BF	17	2B	12	箜š_M.∼ú:»v;.+.
h:	04	84	04	01	21	41	40	48	10	10	12	04	84	04	01	21	."!A@H"!
h:	41	60	7B	8E	В4	52	\mathbf{ED}	27	39	35	37	58	99	9E	F3	4C	A`{Ž´Rí'957X™žóL
h:	EF	47	AA	AE	73	6A	7E	B5	7B	FD	5D	D5	FD	58	91	20	ïGª®sj~µ{ý]ÕýX`
h:	20	24	08	08	09	02	42	82	80	90	20	20	24	08	08	09	ŞB,€. Ş
h•	02	D9	10	E9	75	Δ7	CE	75	DB	35	BD	ΔF	69	75	9D	53	ມີ ≜ນ&ີ ມີ5₩ີ່ານ S

扫描二维码得到云盘连接: https://pan.baidu.com/s/1pLT2J4f

QR Research – \Box X
文件(F) 工具(T) 帮助(H)
🔤 🔝 🞑 🕸 🖉 🗾 🖊
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
^
· · · · · · · · · · · · · · · · · · ·
已解码数据 1: ^
位置:(6.0,8.0)-(270.0,8.0)-(6.0,272.0)-(270.0,272.0) 颜色反色,正像 版本: 4 纠错等级:H, 掩码:1 内容: https://pan.baidu.com/s/1pLT2J4f

链接下载得到flag.rar压缩包,使用WinRAR解压,得到flag.txt,发现并不是flag,依据题目提示还有一个提示 NTFS没有用到,于是利用工具ntfsstreamseditor进行提取,得到一个pyc文件,将pyc反编译回去,得到一个 python的flag加密函数。

名称	修改日期	类型	大小	
🗎 flag.txt	6/12/2017 上午	文本文档	1 KB	
☐ flag.txt - 记事本 文件(E) 编辑(E) 格式(O) 查看(O) 帮助(U)				
flag不在这里哦 你猜猜flag在	E哪里呢? 找	找看吧		

NTFS数据提取

	 全部MTFS磁盘 	*	▼ / 搜索	停止
	* 文件	数据流名称	大小(字节)	可疑度(0-5)
flag.ixt	C:\Users\Rose\Desktop\flag.bd:flag.pyc	flag.pyc	755	1

pyc反编译

C:\WINDOWS\system32\cmd.exe	_		×
loads>uncompyle6 flagg.pyc # uncompyle6 version 3.3.4 # Python bytecode 2.7 (62211) # Decompiled from: Python 3.7.0 (v3.7.0:1bf9cc5093, Jun 27 2018, 04:06:47) [MSC v.1914 32 bit (Intel)] # Embedded file name: flag.py # Compiled at: 2017-12-05 23:42:15 import base64			^
<pre>def encode(): flag = '***********************************</pre>			
return ciphertext[::-1]			
ciphertext = ['96', '65', '93', '123', '91', '97', '22', '93', '70', '102', '94', '132', '46', '112', '64', '97', '88' 137', '90', '109', '99', '112'] # okay decompiling flagg.pyc	, '80'	, '82',	, , , ,

编写相应的解密函数得到解密的flag



get flag:

flag{Y@e_Cl3veR_C1Ever!}



该题脑洞很大!!!!

附上安全脉搏一篇详细的writeup

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

25、旋转跳跃

旋转跳跃 100

熟悉的声音中貌似又隐藏着啥, key: syclovergeek 题目来源: 第七季极客大挑战

sycgeek-mp3_2...

利用音频分析工具MP3Steno,结合key直接进行解码得到 sycgeek-mp3.mp3.txt

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

🥘 sycgeek-mp3.mp3.txt - 记事本	隐写\音频隐写>Decode.exe -X -P syclovergeek sycgeek-mp3.mp3
文件(F) 编辑(F) 格式(O) 杳看(V) 帮助(H)	MP3StegoEncoder 1.1.15
	See README file for copyright info
SYC{Mp3_B15b1uB1u_WOW}	Input file = 'sycgeek-mp3.mp3' output file = 'sycgeek-mp3.mp3.pcm'
	Will attempt to extract hidden information. Output: sycgeek-mp3.mp3.txt
	the bit stream file sycgeek-mp3 mp3 is a BINARY file
	HDR: s=FFF, id=1, 1=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
	alg.=MPEG-1, layer=III, tot bitrate=128, sfrg=44.1
	mode=stereo, sblim=32, jsbd=32, ch=2
	[Frame 5932]Avg slots/frame = 417.889; b/smp = 2.90; br = 127.979 kbps
	Decoding of "sycgeek-mp3.mp3" is finished
	The decoded PCM output file name is "sycgeek-mp3.mp3.pcm"

get flag:

SYC{Mp3_B15b1uBiu_W0W}

普通的二维码

100

来源: XJNU

misc80.zip

查看图片十六进制得到特殊字符串

	Ó	1	2	3	4	- 5	6	7	8	9	Ą	B	Ç	Ď	E	F	0123456789ABCDEF
h:	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF	FF	F0	00	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF	FF	YYYYYYY ð. YYYY Y
h:	FF	FF	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	F0	00	FF	FF	<u>ŸŸŸŸŸŸŸŸŸŸŸŸ</u> Ŏ.ŸŸ
h:	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF	FF	<u>YYYYYYYYYYYYYYYY</u>
h:	F0	00	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	FF	ð. ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ						
h:	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	F0	00	FF	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF	FF	<u>ŸŸŸŸŎ.ŸŸŸŸŶŶŶŶŶ</u>
h:	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	F0	00	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	FF	FF	FF	<u> YYYYYYYYÖ.YYYY</u>
h:	FF	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	$\mathbf{F}\mathbf{F}$	FF	$\mathbf{F}\mathbf{F}$	F0	00	31	34	ŸŸŸŸŸŸŸŸŸŸŸŸŸ Ŏ. <mark>14</mark>						
h:	36	31	35	34	31	34	31	31	34	37	31	37	33	31	31	30	6154141147173110
h:	31	34	31	31	36	36	31	34	35	31	33	37	31	37	31	30	1411661451371710
h:	36		31	32	35	31	33	37	31	32		31	37	31	31	33	6012513712017113
h:	37	31		33	31	34	33	31		32	31	35	31	31	36	30	7163143162151160
h:	31	36	34	31	33	37	31	31	37	31		34	31	34	33	31	1641371171641431
h:	33	37	31	32	34	31	35	37	31	33	37	31	32	34	31	34	3712415713712414
h:	35	31	35	36	31	33	37	31		31	31		33	31	34	33	5156137101163143
h:	31	35	31	31	35	31	30	34	31	31	37	35	40	78	6A	73	151151041175 <mark>@xjs</mark>
h:	65	63	6B	21													eck!

ate Results - BMP.bt

分析这一串数字,每三个数的前面大部分都是1,可能是8进制对应的Ascii值,将其转码



get flag:

flag{Have_y0U_Py_script_Otc_To_Ten_Ascii!}

27、乌云邀请码

乌云邀请码

100

来源: XJNU

misc50.zip

LSB隐写

StegSolve 1.3 by (X
File Analyse Help	×
Normal Image	Extract Preview
	0017666c61677b50 6e675f4c73625f59flag(P ng Lsb Y
您好:	30755f4b306e7721 7dfffffffffff 0u_K0nw! }
这是来自于WooYun的	fffffffffffffffffffffffffffffffffffff
http://www.wooyun.	ffffffffffffffffffffffffffffffffffffff
WooYun会给你发送	
Woord Hand and Stades	
	Bit Planes Order settings
漏洞处理流程: <u>http://</u>	
白帽注意事项: <u>http://</u>	Alpha 7 6 5 4 3 2 1 0 Extract By • Row Column
	Red 1 / 6 5 4 3 2 1 ≥ 0 Bit Order O MSB First @ LSB First
	Green 7 6 5 4 3 2 1 2 0 Bit Plane Order
本邮件由WooYun自动	
WooYun是一个自由平	Blue 7 6 5 4 3 2 1 ≥ 0 ○ RGB ○ GRB
甘油关于WooVun的雨	
	Draview Settinge
	GBR
谢谢	Include Hex Dump in Preview 🕑
	Preview Save Text Save Bin Cancel

get flag:

flag{Png_Lsb_Y0u_K0nw!}

28、神秘的文件

神秘的文件 100

来源:第七届山东省大学生网络安全技能大赛

5ee325f5-44c6-..

分析压缩包,可知明文攻击,利用WinRAR解压,并且压缩图片logo.png作为明文攻击



A	ARC	HPR 4.5	4 - 0%					_		\times
文	:件(F)	恢复(P	() 帮助	力(H)						
		. <i>R</i>		//	S	ல் சில	2 #08t			退中
-+	su ar Instates	713 713 סאס <i>ו</i> סזק ו		ᅝᄔ	座/田沢川	14 /13×	-#1	人.		ющ
	UN SECTION				zio		£			
Ŀ	-		Ownioa	aus (ilag.	zip	明又				~
ŝ	范围	长度	字典	明文	自动保	存 选项	高级			
	明文	先项								
t	明文文	(件路径:						-		
			Pownlo	ads Vogo	.zip		• 开頭	37:0		\$
	<u>1</u>	密钥	0f3b	8dbf	密钥	bc1ad2b6	密钥	03b	d7740	- A
	□�E	成功恢复	₹ !				_			×
	□令E	成功恢复	₹ !	an end A	rehive Dec			≥白.		×
		2成功恢复	₹! Adv	anced A	rchive Pas	sword Recov	/ery 统计(言息:		×
]令E 总计	記成功恢复	₹! Adv	anced A	rchive Pas	sword Reco	/ery 统计(言息:		×
	_令E 总计 总计	3.成功恢复 ·口令 ·时间	₹! Adv	anced A	rchive Pas	sword Recov n/a 18s 467ms	/ery 统计f	言息:		×
	_□○	R成功恢复 ・口令 时间 速度(口4	夏! Adv 令/秒)	anced A	rchive Pas	n/a 18s 467ms n/a	very 统计f	言息:		×
	□< (1 (1 (1) (1) (1) (1) (1) (1)	3.成功恢复 ·口令 ·时间 ·速度(口 ·文件的口	夏! Adv 令/秒) 1令	anced A	rchive Pas	n/a 18s 467ms n/a q1w2e3r4	very 统计f	言息:		×
מעוויג יישעאיי	□ 令 E 説 计 説 功 水 十 六	· 口令 时间 速度(口 ・ 注制口令	夏! Adv 令/秒) 1令	anced A	rchive Pas	n/a 18s 467ms n/a q1w2e3r4 71 31 77 32	very 统计(65 33 72 :	言息: 34		×

得到口令:q1w2e3r4,解压得到word文档发现并没有什么



利用binwalk分析word文档得到发现存在隐藏文件

- デー・~/ 未回	# DIHWALK ZOIOU	
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0×0	Zip archive data, at least v2.0 to extract, compressed size
672 ^{ackup.sh}	0x2A0	Zip archive data, at least v2.0 to extract, compressed size
1370 il.ipeg	0×55A	Zip archive data, at least v1.0 to extract, compressed size
37875	0x93F3	Zip archive data, at least v2.0 to extract, compressed size
39207	0x9927	Zip archive data, at least v2.0 to extract, compressed size
397 31 ae1. ^{misc50.}	0×9B33	Zip archive data, at least v1.0 to extract, compressed size
262627	0x401E3	Zip archive data, at least v2.0 to extract, compressed size
2637 <mark>91</mark>	0x4066F	Zip archive data, at least v2.0 to extract, compressed size
2667 56 xmboreut#	0×41204	Zip archive data, at least v2.0 to extract, compressed size
26831的主网	0x4181F	Zip archive data, at least v2.0 to extract, compressed size
268656 ⁵	0×41970	Zip archive data, at least v2.0 to extract, compressed size
xml.rels		
269244	0x41BBC	Zip archive data, at least v2.0 to extract, compressed size
270175	0x41F5F	Zip archive data, at least v2.0 to extract, compressed size
270991	0x4228F	Zip archive data, at least v2.0 to extract, compressed size
272048	0x426B0	End of Zip archive

分离文件找到flag.txt解码得到flag



ZmxhZ3tkMGNYXzFzX3ppUF9maWxlfQ==
加密 解密 □解密结果以16进制显示
flag{d0cX_1s_ziP_file}

get flag:

flag{d0cX_1s_ziP_file}

update+ing

转载于:https://www.cnblogs.com/qftm/p/11037200.html