MOCTF ---- MISC -----WriteUp





<u>ctf 专栏收录该内容</u> 22 篇文章 0 订阅 订阅专栏

1.我可是黑客

打开题目是一张图片,将他保存到本地,即:



一般第一题都是是道签到题,所以使用文档打开这张图片,小编用的是nodepad++,在文档的最后面,即:

INUL称眙檧NULNULACK€埓k?ESV这族锋蕍 ? 氧NUL斎[尪诋虀_SI ETXKū櫣p??n誥;嬳%"SDI)STX" ""SD 敎Z ??=ŇAKRS们飼DCIj禾沯赌?肠* 瀿?~溛螳鷆翩w漘?=\1 ULNULNULNULmoctf{e4sy_1ma9e_m1sc}

2.假装安全

同上题,先将图片保存到本地,再用nodepad++打开,即:



UENUENUENUE NUENUENUENUENUENUEflag.txt

https://blog.csdn.net/qq_42133828

可以看到,在文档的最后面有flag.txt,这说明,这个图片不是一张简单的图片,他里面包含了文件,需要分离出来。

这里我使用的是kali 里的binwalk工具进行分离

在图片所在目录下,命令框执行语句:

binwalk -e carefully.jpg //分离出carefully.jpg里的文件

ls

cd _carefully.jpg.extracted/ //进入分离出来的文件

ls

cat flag.txt //查看flag

root@kali:	~/Desktop#.binwalk	_{ldē} e carefully.jpg	291字节	2018年8月21日
	HEXADECIMAL	DESCRIPTION		
0 30 ^{0ads} 32255 32407	0x0 0x1E 0x7DFFefully.jpg.ex 0x7E97	JPEG image data, TIFF image data, b TacZip archive data, End of Zip archive	IFIF standard 1. Dig-endian, offs at least v2π0 1 e, footer length	01 Set of first im to extract ⁰⁵ .com n: 22
root@kali: 1.jpg car root@kali: bash: cd: root@kali: root@kali: 7DFF.zip	<pre>~/Desktop# ls refully.jpg _caref ~/Desktop# cd: 没有那个文件或目 ~/Desktop# cd _car ~/Desktop# cd _car flag.txt</pre>	ully.jpg.extracted 目录 efully.jpg.extracted ly.jpg.extracted# ls	27.9 KB mount-shared-fo	2018年12月25日 Dlders.sh rest
<pre>root@kali: mcfCrflyS1</pre>	<pre>~/Desktop/_careful leot{@eul ld}root@k</pre>	ly.jpg.extracted# ca ali:~/Desktop/ caref	at flag.txt fullyhtps://blog.com	n net/ gd_42133828

3.扫扫出奇迹

同上题,先将图片保存到本地。可以看到,这是一张二维码,首先的反应一般都是先扫一扫



但是,不论你是正着扫,倒着扫,还是各种姿势扫,我先你会怀疑你的手机是不是wa掉了。。。 这时候,或许就不是你的问题了,该是二维码的问题了,从二维码可以很明显的看出"黑白分明", 那会不会他是反着来的,上工具。StegSolve



这回,在扫一扫,flag就出来了。。。。。。

4.光阴似箭

同上题,先将图片保存到本地。打开图片,可以看到,有flag闪过。。。。

Where is the flag?

直接上工具, StegSolve, 在Analyse的 Frame Brower 里, 即:



5.杰斯的魔法

打开题目,这道题看来并不是一道图片题,并且页面给出了一串代码,瞅着像是JS代码。。。

额。。那就尝试在console里运行,即:



6.流量分析

下载好题目给的文件,是一个以.pcapng结尾的文件,用wireshark打开,可以看到是一道流量分析题。。。

No.	Time	Source	Destination	Protocol	Length Info	^
	28 55.307368	192.168.1.1	192.168.1.2	ICMP	114 Echo (ping) reply id=0x0001, s	
	29 55.318549	192.168.1.2	192.168.1.1	ICMP	114 Echo (ping) request id=0x0001, s	
	30 55.328988	192.168.1.1	192.168.1.2	ICMP	114 Echo (ping) reply id=0x0001, s	-
	31 55.339576	192.168.1.2	192.168.1.1	ICMP	114 Echo (ping) request id=0x0001, s	
	32 55.340578	192.168.1.1	192.168.1.2	ICMP	114 Echo (ping) reply id=0x0001, s	
	33 55.351160	192.168.1.2	192.168.1.1	ICMP	114 Echo (ping) request id=0x0001, s	
	34 55.361168	192.168.1.1	192.168.1.2	ICMP	114 Echo (ping) reply id=0x0001, s	þ
	35 59.995629	cc:00:06:ec:00:00	cc:00:06:ec:00:00	LOOP	60 Reply	
	36 60.913517	cc:01:06:ec:00:00	cc:01:06:ec:00:00	LOOP	60 Reply	
	37 62.292951	192.168.1.1	192.168.1.2	TCP	60 37465 → 23 [SYN] Seq=0 Win=4128 L	
	38 62.313940	192.168.1.2	192.168.1.1	TCP	60 23 → 37465 [SYN, ACK] Seq=0 Ack=1	
	39 62.334450	192.168.1.1	192.168.1.2	TCP	60 37465 → 23 [ACK] Seq=1 Ack=1 Win=	
	40 62.335453	192.168.1.1	192.168.1.2	TELNET	63 Telnet Data	
	41 62.355984	192.168.1.1	192.168.1.2	тср	60 [TCP Dup ACK 39#1] 37465 → 23 [AC	
	42 62.355984	192.168.1.2	192.168.1.1	TELNET	66 Telnet Data	
	43 62.366482	192.168.1.1	192.168.1.2	TELNET	60 Telnet Data	
	44 62.366482	192.168.1.1	192.168.1.2	TELNET	60 Telnet Data	
	45 62.366482	192.168.1.1	192.168.1.2	TELNET	63 Telnet Data	
	46 62.376992	192.168.1.2	192.168.1.1	TELNET	96 Telnet Dataps://blog.csdn.net/qc_4213 <mark>88</mark>	28

可以看到,有几种类型的协议,但是一眼望去,我想telnet这个协议,或许更具有吸引力,过滤一下协议,并且 打开他的数据包,即:

_							
4	🚺 flag.pcapng						
F	ile Edit View Go Ca	pture Analyze S	tatistics Telep	hony Wi	reless Tools	Help	
	(🔳 🔬 💿 📙 🛅 🗙	🔄 🤇 🗢 🔿 🖻	T 🕹 📃	Θ.Θ.	0, 🎹		
ſ,	telnet						
No	. Time	Source	Destina	tion	Protoco	l Length	Info
	214 96.733492	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	216 97.178847	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	218 98.018533	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	222 103.012596	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	224 104.298076	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	227 106.198578	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	229 107.536592	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	231 108.961444	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	233 109.582636	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	237 111.436721	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	239 113.170536	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	241 113.907941	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	243 114.276073	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	245 114.722890	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	247 114.969284	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	249 116.036783	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	251 116.974873	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	253 117.570422	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	255 118.244820	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	257 119.112469	192.168.1.2	192.1	58.1.1	TELNE	T 60	Telne
	258 119.132977	192.168.1.1	192.1	58.1.2	TELNE	T 60	Telne
F	Ename 227, 60 buter	- on uino (190	hitc) 60 h	the con	turad (190 k	ita) on into	nfaca
Ľ	Ethorpot TT Spcie	5 ON WINE (400	00 (cc.01.0	vies cap	00) Det co		.00 (
Ľ	Internet II, Src. (Vancian A Snc:	102 168 1	D. ec.00.	102 169 1 1		.00 (0
Ľ	Internet Protocol	Protocol Sec	192.100.1.	2, DSC:	192.100.1.1	at 71 Acke	116
Ľ	Tolpot	51 FR0C0C01, 51	C FUIL: 156	bo, DSC	FUEL 25, 56		110, 1
ľ	Data: N						
	Data. N						

可以很清楚看到有Date这个参数,并且有值,在随意打开telnet的包几个看看,亦是如此,而且之都不一样,那 么连续几个的呢?额。。小编想这里就不需要演示怎么一个个拼接成flag了吧,可以友情提示,他的flag在最后 面的几个包内,别问我怎么知道的,因为小编就是一个个点出来的。。。。

7.女神的告白

hint: 李华的女神美美(meimei)给李华发了一个压缩包,却只告诉了李华压缩包密码是以她的名字开头,你能帮李华获得真爱吗?

提示的重点我想是,压缩包的解压密码开头几个是meimei

解压压缩包,即:

🚷 love.zip - Bai	ndizip 6.2	22		_		\times
文件(F) 编辑(E)	查找(I)	选项(O)	视图(V)	帮助(H)	
→ × 打开	解压		「し」	「 + 添加		
읅 love.zip	名称			~		
	📄 fla	g.txt*				
輸入密码						×
flag.txt						
请输入密码						_
□用星号隐藏	密码(H)					
	htt	ps://blog	j.cs <mark>rin.∛</mark>	龍山	21 . 21.0	満 28

这是需要密码的,小编我是先使用一个字典生成器,先生成适应的密码字典,再用另一个工具爆破密码,话不 多说,上图:

· · · · · · · · · · · · · · · · · · ·	
关于 其木宝符 白完义 生日 生成字典	9 修改字曲】注册 】
保存路径: superdic.txt	浏览
密峭1立数 1 2 3 ✔ 4	
	_
	White a sector and from And and and
nups:	//biog.csch.net/qq_42133828
M 是优软件招级字曲生成器 V3 35 Div Crack T	eam — 🗆 X
Storesting set and the store of the	
关于 基本字符 自定义 生日 生成字典	修改字典 注册
▼ 在每个密码前插入字符串 meim	ei
源字典路径:	浏览
1朱仔商行: c:\superdicl.txt	测觉
修动之曲	
修改字典	
修改字典 https://	/blog.esdn.net/cg_42133828
修改字典 https://	/blog.csdn.net/qq_42133828
修改字典 https://	/blog.csdn.net/qq_42133828
	/blog.csdn.nat/qq_42133828 — — — — >
	/blog.csdn.nat/qq_42133828 — — — >
修改字典 https:// ARCHPR 4.54 - 4% File Recovery Help	/blog.csdn.net/qg_42133828 — — — >
<u>修改字典</u> Attps:// ARCHPR 4.54 - 4% File Recovery Help デー パ パ パ パ	/blog.csdn.nel/qg_42133828 >
修改字典 Attps:// ARCHPR 4.54 - 4% File Recovery Help ご ARCHPR 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5	/blog.csdn.nel/qq_42133823 — — — >
修改字典 https:// ARCHPR 4.54 - 4% File Recovery Help	/blog.csdn.net/qg_42(13382) — — — — — — — — — — — — — — — — — — —
修改字典 https:// ARCHPR 4.54 - 4% File Recovery Help	/block.csdni.net/cjci_42:1338223 — >
修改字典 https:// ARCHPR 4.54 - 4% File Recovery Help	(bloc) cscln.net/cjc.42(193822) >
修改字典 Attps:// Attps:// ARCHPR 4.54 - 4% File Recovery Help	Alloci codn. net/cjc. 42:133823
修改字典 Attps:// Attps:// Attps:// Attps:// Attps:// Attps:// Attps:// Attps:// File Recovery Help ② Pen Start ! Stop Benchmark F Encrypted ZIP/RAR/ACE/ARJ-file [C:\Users\DELL\Pownloads\Jove.zip Range Length Dictionary Plain-text Autor Dictionary options Dictionary file path:	Abloct codm.net/(qr. 42:133822)
修改字典	/block.codm.net/qg_/12/13/38223 — — — > Purchase Help About Qu Type of attack Dictionary o-save Options Advanced t - > Start line # 0
修改字典 https:// ARCHPR 4.54 - 4% File Recovery Help	Alloci codin net/act 2133823
修改字典 Attps://	Alloci codin net/act 2133823
修改字典 https:// ARCHPR 4.54 - 4% File Recovery Help	(blockeechn net/qg /2/13/382) — — >
修改字典 https:// ARCHPR 4.54 - 4% File Recovery Help	(blockeschnine) (qc 24243382)
修改字典 Attos:// ARCHPR 4.54 - 4% File Recovery Help	(block code in not light 2424 33382)
修改字典 Attos:// ARCHPR 4.54 - 4% File Recovery Help シーン・シーン・シーン・シーン・ Open Start I Stop Benchmark F Encrypted ZIP/RAR/ACE/ARJ-file [C:\Users\DELL\Downloads\Jove.zip Range Length Dictionary Plain-text Autor Dictionary options Dictionary options Dictionary file path: C:\phpStudy\PHPTutorial\WWW\superdic1.txt Smart mutations Password successfully recovered I Advanced Archive Passwords 「Total passwords 5,43 Total time Sms	Allocheschrinel/qr. 4213382
修改字典 Attops:// ARCHPR 4.54 - 4% File Recovery Help シーン・ディン・Stop Benchmark F Encrypted ZIP/RAR/ACE/ARJ-file [C:\Users\DELL\Downloads\Jove.zip Range Length Dictionary Plain-text Autor Dictionary options Dictionary file path: C:\phpStudy\PHPTutorial\WWW\superdic1.tot Smart mutations Password successfully recovered ! Advanced Archive Password Total passwords 5,43 Total time 5ms Average speed (passwords per second) 1,08	Ablach eschninel/(nr. 42/19982) Image: sechninel/(nr. 42/19982)
能改字典 Attops:// ARCHPR 4.54 - 4% File Recovery Help Provide a start 1 Stop Benchmark F Encrypted ZIP/RAR/ACE/ARJ-file [C:\Users\PELL\Downloads\Jove.zip Range Length Dictionary Plain-text Autor Dictionary options Dictionary options Dictionary file path: C:\phpStudy\PHPTutorial\WWW\superdic1.txd Smart mutations Password successfully recovered 1 Advanced Archive Password S,43 Total time Sins Average speed (passwords per second) 1,06 Password for this file mein	Ablach eschnine l/qn 42/193822 Image: second sec
能改字典 Attops:// ARCHPR 4.54 - 4% File Recovery Help Password ZIP/RAR/ACE/ARJ-file C:\Users\DELL\Downloads\Jove.zip Range Length Dictionary Plain-text Autor Dictionary options Dictionary options Dictionary file path: C:\phpStudy\PHPTutorial\WWW\superdic1.bdl Smart mutations Password successfully recovered ! Advanced Archive Password Total time Sns Average speed (passwords per second) 1,06 Password for this file mission	Ablach eschnine //qr. 2/2/193822 Image: sechnine //qr. 2/2/19382 Image: sechnine //qr
(修改字典 https:// ARCHPR 4.54 - 4% File Recovery Help Open Start I Stop Benchmark F Encrypted ZIP/RAR/ACE/ARJ-file C:\Users\PELL\Downloads\Jove.zip Range Length Dictionary Plain-text Autor Dictionary options Dictionary file path: C:\phpStudy\PHPTutorial\WWW\superdic1.bxt Smart mutations Password successfully recovered I Advanced Archive Passwo Total passwords 5,43 Total time Sms Average speed (passwords per second) 1,08 Password for this file mein Password in HEX 6d 6	Alloci codni nel/qri 42/19382

爆破的出来的密码,即:meimei5435

输入密码, 解压文件得:

🚷 love	zip - Bar	ndizip 6.2	22		_		\times
文件(F)	编辑(E)	查找(I)	选项(O)	视图(V)	帮助(ŀ	H)	
→ IJĦ		民 び 解压	~ (「日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日	 添	- - 10	82
<u> a</u> love.	zip	名称 iii flag	g.txt*	•	~		
📃 flag.t	txt - 记事:	本					
文件(F)	编辑(E)	格式(O)	查看(V)	帮助(H)			
moctf	F{Y0u	_@re	_A_g()0d_m	an} et/qq		

8.捉迷藏

下载,并解压题目给的压缩包,可以看到:



打开flag.txt,里面有一串字符串,但是小编没解码出来,所以目标转为图片,先把图片foremat一下,并打开,即:

0000022	4.zip - Bar	dizip 6.22									- 🗆	×
文件(F) 编辑	髴(E) 查找	l) 选项(O)	视图(V)	帮助(H)								
→ ±777	✓ 【U 」 解⊞] ~	下 新建	— + 添加		/	。 。 。 查					
会 00000224	4.zip 名称	尔	Ň	/		压缩	后大小	原始大小	类型		修改日期	
		flag.txt					48	69	文本文档		2017/11/29	15:16:09
📗 flag.txt -	记事本											
文件(F) 编辑	贔(E) 格式	O) 查看(V) 帮助(H)									
109 111	1 99 [·]	16 10	2 123	104	49 100	51 95	97 78	100 9	5 115 51	51 7	5 125	

https://blog.csdn.net/gq_42133828

这个小编看得懂,一串ascii值,用python跑一下,即:

```
f = open('C:\\Users\DELL\\Desktop\\zhuomicang\\outfile\\zip\\flag.txt').read().split(' ')
a = []
n = 0
for 1 in f:
    print 1
    a.append(int(1))
    n+=1
for i in range(n):
    print chr(a[i]),
```



9.是兄弟就来干我

下载,并解压题目给的压缩包,可以看到:



flag.zip打开里面的文件需要密码,则,先对图片分析一波,使用StegSolve里的Analyse里的Data Extract:

2											– 🗆 ×
								Extra	act Pre	view	
0000	00000	00023	6f 8	9504e	470d	0ala0	a	#	0 .P	IG	
0000	000d4	94844	52 0	00001	7200	0000f	f	IHD	R	r	
0802	00000	0631f	ca e	c0000	00001	73524	7	c.		sRG	
4200	aecel	ce900	00 0	00467	1414d	41000	0 в.		·9	JAMA	
b18f	0bfc6	10500	00 0	00970)4859	73000	0	a	· · · P	HYs	
1625	00001	62501	49 5	224f0	0000	23044	9.8		I R\$.	#.I	
4441	54785	eed9d	41 8	e2c2b	9245	6b213	d DA	Tx^	A., 4	Ek!=	
ec55	e4126	ad4ab	78 4	be875	ie4b0	57929	3 .U	j	x K.u	1W	
52ad	24556	d831e	b4 7	a5452	249bt	3130e	0 R.	\$U	. zTF	XI.10.	
1418	38/81	03223	12 0	ITA32I	:1a/U	10003	3	8x.2#	:/	.p3	
-	Rit Dlar	105									Order settings
	Ditria	103									order settings
	Alpha	7		6 5	i 🗆 4	4 🗆 3	2	1	0		Extract By Row Column
			-					<u> </u>			
	Red	7		6 🗆 5		. 🗆 1	2	1			Bit Order O MSB Einst @ LSB Einst
	neu	· ·		, [] ,		. 🗆 🤉			P V		Bit Order O MSB First O LSB First
	Creen	7									
	Green	<u> </u>		, <u> </u>	,	· 🔲 🤉	<u> </u>		VU		Bit Plane Order
	Disc	7									
	Blue			5 5	, 🖂 4	1 🗌 3	2	1			○ RGB ○ GRB
-	Desident										
Γ	Preview	v settin	gs								🔾 GBR 💿 BGR 🛛 💙
		1	nclud	e Hex [)ump I	n Previ	ew 🖌		. T.		
					Pre	view	S	ave Tex	d I	Save F	in Cancel
									··	ouro c	

保存图片,并修改一下图片的值,删除头部多余的东西,打开图片,即:



红色得地方,有提示 zhazhahui,我想这应该是密码吧,解密得:



栅栏密码解密得:

🕹 米斯特安全团队 CTFCrakTools pro v2.1 Beta
解码方式 进制转换 插件 妹子
Crypto Image UnZip
填写所需检测的密码:(已输入字符数统计:26)
f_hfv7m_y8{kThk43a_xrk0?n}
结果:(字符数统计: 81)
得到因数(排除1和字符串长度),
2 13
第1栏: fhymy{Tk3 rOn f7 8kh4axk?}
第2世,fb kb4f2up7 my ryk00[2kmT]
y724≈; III_KII413Va/_IIIX_fYKOU[:KIII]
https://blog.csdn.net/qq_42133828

凯撒密码解密得:

▲ 米斯特安全团队 CTFCrakTools pro v2.1 Beta 解码方式 进制转换 插件 妹子 Crypto Image UnZip 填写所需检测的密码:(已输入字符数统计:26) fhvmy{Tk3_r0n_f7_8kh4axk?} 结果: (字符数统计: 676) giwnz{UI3_sOo_g7_8Ii4byl?} hjxoa{Vm3_tOp_h7_8mj4czm?} ikypb{Wn3_u0q_i7_8nk4dan?} jlzqc{Xo3_v0r_j7_8ol4ebo?} kmard{Yp3_w0s_k7_8pm4fcp?} Inbse{Zq3_x0t_I7_8qn4gdq?} moctf{Ar3_yOu_m7_8ro4her?} stas3_z0v_n7_8sp4ifs?} oqevh{Ct3_a0w_o7_8tq4jgt?} prfwi{Du3_b0x_p7_8ur4khu?} qsgxj{Ev3_c0y_q7_8vs4liv?} rthyk{Fw3_d0z_r7_8wt4mjw?} suizl{Gx3_eOa_s7_8xu4nkx?} tvjam{Hy3_f0b_t7_8yv4oly?} uwkbn{lz3_g0c_u7_8zw4pmz?} vxlco{Ja3_h0d_v7_8ax4qna?}

10.百变flag

打开链接,发现只有一个小正方框,但是也不妨碍他是照片的事实,在离小方框远一点的黑色地方,点击保存 图片。

此处使用的是kali完成的操作的。在window上有一些伪加密得文件打不开,在linux却可以直接解压。。。

先在图片所在得目录下执行以下语句:

binwalk -e f1ag.png

然后:

root@kali:~/Desktop# ls 1.jpg±:flag.pngesk_flag.png.extracted mount-shared-fold	lers.sh	restart-vm-too	ols.sh
<pre>root@kal1:~/Desktop# cd _Tlag.png.extracted/ root@kal1:~/Desktop/ flag.png.extracted# ls</pre>			
<pre>0.zip 1.py flag.exe root@kali:~/Desktop/_flag.png.extracted# cat flag.exe</pre>	130字节	2018年8月21日	☆



如果你细心一点,你会发现他里面的东西倒过来了。所以,我们需要把她正回来,python代码如下:



运行后,是一张图片,打开,得:



11.蒙娜丽萨的微笑

下载图片,使用StegSolve对图片进行分析,发现无果,在对图片修改大小,即:

c2ltbGVpc2ludGVyaW5n

base64解下得到: simleisintering

解出来一串字符,但不知道有啥用,那么再对图片分析一波

root@kali:	~/Desktop/smile# b	inwalk -e pixel.png
DECIMAL	HEXADECIMAL =	DESCRIPTION
0 1654 120297 120453	(大小 _{0x0}) 都改白動 225 0x676 0x1D5E9 0x1D685	PNG image, 500 x 372, 8-bit colormap, non-interla Zlib compressed data, best compression Zip archive data, encrypted at least v1.0 to extr End of Zip archive, footer length: 22
root@kali:- pixel.png root@kali:- bash: cd:	118.8KB ~/Desktop/smile# ls _pixel.png.extrac ~/Desktop/smile# co _: 没有那个文件或目 -(Desktop(smilo#)	7:07 ☆ 5 ted do _{⊟ ☆} 录
root@kali: 1D5E9.zip	<pre>~/Desktop/smite# cc ~/Desktop/smile/_p 676 676.zlib fl</pre>	ixel.png.extracted/ ixel.png.extracted# ls aghttps://blog.csdn.net/qq_42133828

打开zip文件,输入刚才得到的密码,即:

名称		▼ 大小	类型
🔚 flag		🗎 24字节	未知
	打开(0) 👻 🖪		
	moctf{Int3restir	ng_piXe1}	
2			

12.李华的双十一

下载,并打开压缩包,会发现里面得两个文件都需要密码解密,意味着没有任何线索来获取密码

那么就只能粗暴一点,直接爆破出他的密码,即:



解密money.zip,并打开里面得文件,在文件的最底部,即:

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

摩斯密码解密得:

솔 米斯特安全团队 CTFCrakTools pro v2.1 Beta
解码方式 进制转换 插件 妹子
Crypto Image UnZip
填写所需检测的密码:(已输入字符数统计:38)
) 结果: (字符数统计: 7)
B0Y1111 https://blog.csdn.net/qq_42133828

解压包里面还有一个mp3的文件,又得到密码,那么使用工具MP3Stego,运行以下命令,即:

D:\MP3Stego_1_1_18	\MP3Stego>Decode.exe -X -P	BOY1111 singledog.mp3				
MP3StegoEncoder 1.	1. 17					
See README file fo:	r copyright info					
Input file = 'sing	ledog.mp3' output file = '	singledog.mp3.pcm'				
Will attempt to ex	tract hidden information. O	utput: singledog.mp3.	txt			
the bit stream file singledog.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 7866]Avg slots/frame = 417.906; b/smp = 2.90; br = 127.984 kbps						
Decoding of "singl	edog.mp3″ is finished					
音乐	singledog.mp3	2019/4/26 16:00	MP3 文件	3,212 KB		
- <u>-</u>	singledog.mp3.pcm	2019/4/26 19:31	PCM 文件	35,400 KB		
三 杲田	sinaledoa mp3 txt	2019/4/26 19:31	では で格 loop	ando pot/act KBd		
🏪 系统 (C:)		2010/4/2015.51	Preparentering.	csuninei/qq <u>142</u> i		
	THE PROPERTY FOR A L	10100 <i>0</i> 0014016016010	17 x 1722	1 1/10		

打开singledog.txt,得一串base64的密文,解密得:

ਭ 米斯特安全团队 CTFCrakTools pro v2.1 Beta
解码方式 进制转换 插件 妹子
Crypto Image UnZip
填写所需检测的密码:(已输入字符数统计:28)
bW9jdGZ7l1MxbmdsM19EMGcjfQ==
结果: (字符数统计: 19)
moctf{#S1ngI3_D0g#}
https://blog.csdn.net/qq_42133828

13.李华的疑惑

下载,并打开压缩包,可以看到一个password.txt,以及一个flag.zip(需密码)

打开password.txt是一串字符串,使用python读取,每一行有三个字符,一共有22500行

说实话,小编一开始还是不知道的,去网上搜索才造,原来这是RGB的图像

所以,我们需要还原它,即:

```
from PIL import Image
x = 150
y = 150
im = Image.new("RGB",(x,y))
f = open('C:\\Users\\DELL\\Desktop\\yihuo\\password.txt')
for i in range(0,x):
  for j in range(0,j):
    l = f.readline()
    rgb = l.split(',')
    im.putpixel((i,j),(int(rgb[0]),int(rgb[1]),int(rgb[2])))
im.show()
```

得到的图像是这样的:

KEY: PPPPPPass_w ord

通过得到的key,去解压flag.zip,可得一串字符:

U2FsdGVkX18R9EylBVacP/j0XpClSh9nZth6TFwoh5GUv0edeVp3ZV9gXVqd/rlH66OlZgSHn2Mock4hcdqFEg=

进行AES解码(https://www.sojson.com/encrypt_aes.html),得:

moctf{D0_You_1ik3_t0_pAinH_wi4h_pi8e1}