Bugku writeup 猫片(安恒)



3篇文章 0 订阅 订阅专栏

Bugku writeup 猫片(安恒)

题目:



解题:

1、首先打开题目附件,得到一个png的二进制文件。用010editor打开,发现头部内容显示为png,因此修改文件后缀,得到一张 图片。

																OTFOID 100 LODER
89		4E	47	0D		1A					0D	49	48	44	52	PNGIHDR
		02	80	00	00	02	80	08	02		00	00	83	AF	5E	€f^^
74	00	00	20	00	49	44	41	54	78	01	AC	C1	E1	8E	1C	t IDATxÁáŽ.
E9	81	9D	E9	F7	9C	EF	AB	60	B2	9A	CD	A6	DA	B2	2C	éé÷œï«`*ší¦Ú²,
CC	7A	EF	FF	76	FC	6B	в1	68	03	C6	C2	3F	34	42	8F	Ìzïÿvük±h.ÆÂ?4B.
46	E2	B0	8B	C9	AC	C8	88	73	36	32	C9	EA	6E	C9	94	Fâ°<ɬÈ^s62ÉênÉ″
								-	-			-	-			3 (A.) - (



打开虚拟机跑一下binwalk,没有任何其他收获;打开pngcheck检查一下,也无异常。



了preview部分出现了"PNG"信息,因此选择"Save bin",保存为png文件。

I	11 12	- 🗆 X
	Extract Preview	N
	fffe89504e470d0a la0a0000000d4948PNG	.IH
I	4452000001180000 008c08020000008 DR	
	ec7edb0000059c49 444154789ceddd51 .~I DATx.	Q
1	6alc3b1440c13864 ff5b761610145038 j.;.@.8d .[v	.P8
1	3792ecaadf37afdd eef141908bd43f7e 77A	.?~
1	000000000000c09f 3e56ffe1f3f3f37f >V	
1	dec73ffbf858fe0a 89d573d8fdb9d3d7?Xs	
I	59a99ecfeefd579f bfcdeafe7ffee7fb YWD	
1	802f494810101204 8404012141404810 ./IH !A	@H.
1	1012047eedfe0fd3 739b95dd39c3f4dc~ s9	••••
	Bit Planes	Order settings
	Alpha 7 6 5 4 3 2 1 0	Extract By Row Column
	Red 7 6 5 4 3 2 1 2 0	Bit Order 🔾 MSB First 💿 LSB First
	Green 7 6 5 4 3 2 1 1 0	Bit Plane Order
	Blue 7 6 5 4 3 2 1 2 0	○ RGB ○ GRB
		RBG OBRG
	Preview Settings	0.000
	Include Hex Dump In Preview	ht 93%% log %%% net/gc_40737798

用010editor将头部信息矫正,将"FFFE"删除并保存,打开修改后的图片,发现是一张二维码,但是此二维码高度需要修改。再次运行010editor,通过变量窗口修改高度。



https://blog.csdn.net/qq_40737798

			变量		▼ ×	
	102.01	Ì	名称	值	开始	
Ę	F	<u>0</u>	struct PNG SIGNATURE sig	Conserve and an and the	0h	
44	52		struct PNG CHUNK chunk[0]	IHDR (Critical, Pu	8h	-
EC	7E		uint32 length	13	8h	(?)
6A	1C	6	> union CTYPE type	IHDR	Ch	
37	92		struct PNG CHUNK IHDR ihdr	280 x 140 (x8)	10h	
00	00		uint32 width	280	10h	-
DF	07		uint32 height	280	14h	m
EG	20		ubyte bits	B TrueColor (2)	100	8
29	AS	1	enum PNG COMPR MET	Deflate (0)	14h	0
80	2F	2	enum PNG FILTER METH.	AdaptiveFiltering (0)	1Bh	
10	12	I	enum PNG INTERLACE	NoInterlace (0)	1Ch	
63	FA	•	uint32 crc	8EC7EDBh	1Dh	
2B	12	ç	struct PNG CHUNK chunk[1]	IDAT (Critical, Pu	21h	
01	21		uint32 length	1436	21h	
F3	4C	A	union CTYPE type	IDAT	25h	
91	20	8	ubyte data[1436]	10510000	29h	
08	09		uint32 crc	4851302Dh	5C5h	
9D	52		struct PNG CHUNK chunk[2]	IEND (Critical, Pu	5D5h	
0.4	0.4		struct PNG CHONK chunk[s]		50511	
04	84	ç				
6D	D7					
12	04	24				
5E	39	"				
2B	12	Ï				
01	21					
7E	E5	A				
80	90	P				
32	30				10707	
10	10	100	https://b	log.csdn.net/qq	_40737	
10	10					

QR Research直接打开获取内容,得到一个百度网盘链接:



3、打开网盘后,发现是个flag.rar文件,下载之后打开压缩包,里面有个flag.txt文件。直接打开txt文件,却发现:

flag不在这里哦 你猜猜flag在哪里呢? 找找看吧

尝试解压,也没问题;打开binwalk跑,也没结果。苦想想不出,就直接去看大手子写的WP了,发现这居然是个坑:用winrar解 压会提示解压错误(PS:本人一向来只用7-zip,这个坑我fo了)。这时还剩一个hint:NTFS,根据大佬的WP,这是一个NTFS 文件流隐写的问题,可以使用ADS或者NtfsStreamEditor。下载NtfsStreamEditor这软件之后win10内打不开,于是又临时搞了个 win7虚拟机。打开之后导入flag.txt,发现确实隐含了一个pyc文件,但是开头用的是v1.0版本又导出不出来,于是只能去下v2.0版 本,得到以下结果:

🔠 HtfsStreamsEditor2				_ 🗆 ×
NSE NtfsStreamsE	ditor	http	://blog.sina.co advn	om.cn/advnetsoft etsoft@sina.com
	流处理工具			by XGQ
	* 新博奇名称兀西			
C 全部NTFS磁盘	*	○ 坤志	信止	
○ 自定义磁盘/文件(夹) C:\Users\root\Desktop		P 1X.M	191L	
搜索结果:共1个;用时0.031s				
* 文件	数据流名称	大小(字节)	可疑度(0-5)	
C:\Users\root\Desktop\flag\flag.bd:flag.pyc	flag.pyc	755	1	
			1	
◎ 删除 – 八〇 一 一 一 一 一 一 附加 +/ 导入 <- 一 一 一 附加 +/ 导入 <- 一	🯹 备份 >>	还原<<		导出列表
选择搜索结果,然后进行处理				.net/qg_40737798

4、将得到的pyc文件用uncompyle6反编译之后得到py文件。



得到的py文件内容如下:



这显然是个对称加密,因此写个解密函数:



最终获取得到flag。

D:\code\CTF-tools\venv\Scripts\python.exe flag{Y@e_Cl3veR_C1Ever!}

Process finished with exit code 0