BugkuCTF_杂项004

原创

FAFU小宋 ● 于 2020-11-04 22:49:48 发布 ● 75 ☆ 收藏
 分类专栏: BugkuCTF 文章标签: 安全
 版权声明:本文为博主原创文章,遵循 CC 4.0 BY-SA 版权协议,转载请附上原文出处链接和本声明。
 本文链接: https://blog.csdn.net/FAFUxiaosong/article/details/109400979
 版权



BugkuCTF 专栏收录该内容

6 篇文章 0 订阅 订阅专栏

BugkuCTF_杂项

猫片(安恒)

多彩

旋转跳跃

普通的二维码

猫片(安恒)

(1) 将下载的文件后缀名改为png(注: png正常文件头: 89 50 4E 47)

Dump	f	е	d	С	b	а	9	8	7	6	5	4	3	2	1	0	Address
塒NGIHDRE	52	44	48	49	0d	00	00	00	0a	1a	0a	0d	47	4e	50	89	00000000
€(黛^[5e	af	83	00	00	00	02	08	80	02	00	00	80	02	00	00	00000010

(2) 根据提示LSB和BGR,用stegsolve工具打开,发现一张png图片

<u>لا</u>	– 🗆 X
Extract Preview	
fffe89504e470d0a la0a000000d4948 PNGIH 4452000001180000 008c08020000008 DRIH ec7edb0000059c49 444154789ceddd51 .~I DATxQ 6alc3b1440c13864 ff5b761610145038 j.;.0.8d [vP8 3792ecaadf37afdd eef141908bd43f7e 77A?~ 000000000c09f 3e56ffelf3f3f37f >VD dec73ffbf858fe0a 89d573d8fdb9d3d7 .?.Xs 59a99ecfeefd579f bfcdeafe7ffee7fb YW. 802f494810101204 8404012141404810 ./TH	
1012047eedfe0fd3 739b95dd39c3f4dc~ s9	_
Bit Planes Order setting Alpha 7 6 5 4 3 2 1 0 Red 7 6 5 4 3 2 1 0 Bit Order 0 Green 7 6 5 4 3 2 1 0 Bit Order 0 Blue 7 6 5 4 3 2 1 0 0 RGB 	gs Row Column MSB First ELSB First Order GRB BRG
Preview Settings GBR	• BGR

	• •				
Preview	Save Text	Save E	Bin	hCancello	J

 (2) 将其保存下来,并修改后缀名为.png,但无法打开。用notepad++打开,发现文件头错误

 Address
 0
 1
 2
 3
 4
 5
 6
 7
 8
 9
 a
 b
 c
 d
 e
 f
 Dump

 000000000
 ff
 fe
 89
 50
 4e
 47
 0d
 0a
 1a
 0a
 00
 00
 0d
 49
 48

 PNG.....
 IF

 000000010
 44
 52
 00
 00
 01
 18
 00
 00
 8c
 08
 02
 00
 00
 08
 DR...................
 IF

(3) 将前面的ff fe删掉并保存,打开图片,是半张二维码



(4)修改图片高度试试,改为和长度一样。

Address	0	1	2	З	4	5	б	7	8	9	а	b	С	d	е	f	Dump
00000000	89	50	4e	47	0d	0a	1a	0a	00	00	00	0d	49	48	44	52	塒NGIHDRE
00000010	00	00	01	18	00	00	00	8c	08	02	00	00	00	08	ec	7e	靱ロ
00000020	db	00	00	05	9c	49	44	41	54	78	9c	ed	dd	51	ба	1c	?淚DATx滍軶j.OC
71 -1		-1	0	2	4	E	~	7	0	0		1-		-1	_	1 6	D



(5)看到了完整的二维码,但和正常的有些不一样,中间的正方形应为黑色。用画图工具反色一下(新建->粘贴来源->右键-反色->裁剪)







(6) 扫描器扫描,得到一个网址,是一个百度云链接

😳 QR Research	- 🗆 ×	
文件(F) 工具(T) 帮助(H)		
	 H(30%) ▼ Auto ▼ 版本 尺寸 Auto ▼ 4 ↓ Auto	
	^	
	272.0)	
https://pan.baidu.com/s/1pLT2J4f	https://blog.csdn.net/FAFUxiaosong	
□	更多 ▼	<u>SVIP新人礼!最低仅1? 元</u>

🔗 百度网盘	网盘	分享	一刻相册	更多 🔻		<u>SVIP新人礼!最低</u>	<u>新文1?</u> 元
	flag.rar (1) 2017-12-06	07:23 失效时间	间: 永久有效	▶ 保存到网盘	⊥ 下载(766B)	副保存到手机	举报 赞(5)



(7)下载下来后,是一个rar压缩包,但解压时出现了问题,可以用WinRAR打开

▲ WinRAR:诊断信息	- 0	×
信息 A 无法设置 D:\CTF靶场\BugkuCTF\杂项\022\flag.txt 的安全数据 这个安全 ID 不能分配为此对象的所有者。	压缩文件 flag.rar (D:\CTF靶场\BugkuCTF\杂项\022\fla	ag.rar)

(8) 不过依然得到一个flag.txt文件

flag.	.txt - 记争	4			
文件(F)	编辑(E)	格式(O)	查看(V)	帮助(H)	
flag不不	在这里明	も 你猜	青flag在	哪里呢?	找找看吧

(9) 根据hint里的提示"NTFS",用NtfsStreamsEditor查看数据流,然后导出。

#flag.rar这个压缩文件一定要用winrar来解压才能找得到数据流。

MtfsStreamsEditor 2.0.2 \times _ treamsEditor http://blog.sina.com.cn/advnetsoft advnetsoft@sina.com Ntfs数据流处理工具 🦙 搜索 📿 信息 编辑 记录 选择搜索类型 数据流名称匹配 ○全部NTFS磁盘 * 搜索 停止 ~ ● 自定义磁盘/文件(夹)
D:\CTF靶场\BugkuCTF\杂项\022 搜索结果:共1个;用时0.016 s * 文件 数据流名称 大小(字节) 可疑度(0-5) D:\CTF靶场\BugkuCTF\杂项\022\flag.txt:flag.pyc 755 flag.pyc 1

(10) 一个.pyc文件, 放到在线工具https://tool.lu/pyc/

```
γp边洋pyc乂1+进行胜省。文持所有Python版本
 选择文件 未选择任何文件
           2 = 0LO(2) + TO
       else:
           s = ord(s) - 10
       ciphertext.append(str(s))
   return ciphertext[::-1]
ciphertext = [
    '96',
    '65',
    '93',
    '123',
    '91',
    '97',
    '22',
    '93',
    '70'
```

(M)	
'102',	
'94',	
'132',	
'46',	
'112',	
'64',	
'97',	
'88'	https://bioglesdminev/ Ar Oxidosong

(11) 根据这个加密脚本,再写一个解密脚本

def	decode():
	ciphertext = [
	'96',
	'65',
	'93',
	'123',
	'91',
	'97',
	'22',
	'93',
	'70',
	'102',
	'94',
	'132'.
	'46',
	'112'.
	'64'.
	'97',
	'88',
	'80',
	'82',
	'137'.
	'90'.
	'109'.
	'99'.
	'112']
	ciphertext.reverse()
	flag = ''
	for i in range(len(cinhertext)):
	if i $\% 2 == 0$.
	s = int(cinhertext[i]) - 10
	else:
	<pre>s = int(ciphertext[i]) + 10</pre>
	s=chr(i^s)
	flag += s
	return flag
lef	main():
	flag = decode()
	nrint(flag)
	F(
if	name == ' main ':
-	

(12) 用代码在线工具执行一下https://tool.lu/coderunner/

在线工具



多彩

(1)得到一张.png的图片,在notepad++里没有发现有用信息



(2) 放到stegsolve里分析,发现了图片中隐藏的数据,是一个压缩包,将其抽取出来

— □	×
Extract Preview	
000000000000000000000000000000000000	
Bit Planes Order settings Alpha 7 6 5 4 3 2 1 0 Red 7 6 5 4 3 2 1 0 Bit Order MSB First Image: Contract By I	
Preview Settings OBR BGR	
Preview Save Text Save Bin hiCanceblog.csdn.net/FAFUXia	iosong

(3) 先用notepad++打开这个压缩包,删掉文件头前面的东西,然后保存

Address	0	1	2	3	4	5	б	7	8	9	а	b	С	d	е	f	Dump
00000000	00							e3	50	4b	03	04	14	00	01	08	
00000010	08	00	70	42	67	4c	37	20	ff	48	4d	00	00	00	43	00	pBgL7 HMC.
00000020	00	00	08	00	00	00	66	бc	61	67	2e	74	78	74	ce	98	flaq.txt?□

D

(4)把后缀名改为zip,解压,但出错了,后缀名改为.rar也是这样(不执行第3步也会出错)

🔺 WinRAR:诊断信息			-	×
信息 ▲ 压缩文件已损坏	压缩文件 1.zip (D:\CTF靶	场\BugkuCTF\杂顶\023\1.zip)		

(5)看了一些大佬的writeup,压缩文件是加密的,需要用到图片中的色号。但我这里直接显示出错,没让我输入密码。后面就不会做了。(嘤嘤嘤)

1,27,59,11,23,7,57,1,1,76,222,1,1,50,214,6,77,50,53,214,6

旋转跳跃

	Challenge	1781 Solves	:	×							
		旋转跳跀	Ę								
100											
<u>笑</u> 是	熟悉的声音中貌似 顾目来源: 第七調	以又隐藏着啥 <mark>、</mark> key:syclove 季极客大挑战	ergeek g.osdn.net/FAFUxiao								
(1)附件是一个音频文件,使用 cmd打开运行窗口。输入如下命令	工具MP3Steg ∽解码	o来对音频进行解码。将	该音频文件拷贝到MP	3Stego目录下,在目录标	兰里输入						
Decode.exe -X -P syclovergeek	sycgeek-mp3	.mp3 //-P后面	即为题目提示的密码								
醽 C:\Windows\System32\cmd.exe Microsoft Windows [版本 10.0.183 (c) 2019 Microsoft Corporation。	62.1139] 保留所有权利。			-							
D:\安全工具\Misc工具配置\音频分析 MP3StegoEncoder 1. 1. 19 See README file for copyright in Input file = 'sycgeek-mp3.mp3' Will attempt to extract hidden i the bit stream file sycgeek-mp3. HDR: s=FFF, id=1, 1=3, ep=off, b alg.=MPEG-1, layer=III, tot bitr mode=stereo, sblim=32, jsbd=32, [Frame 5932]Avg slots/frame = 41 Decoding of "sycgeek-mp3.mp3" is The decoded PCM output file name	f关工具\MP3St output file = nformation. 0 mp3 is a BINA r=9, sf=0, pd ate=128, sfrq ch=2 7.889; b/smp finished is ″sycgeek∹	ego_1_1_19\MP3Stego)Dec 'sycgeek-mp3.mp3.pcm' utput: sycgeek-mp3.mp3.mp3. RY file =1, pr=0, m=0, js=0, c== =44.1 = 2.90; br = 127.979 kbj mp3.mp3.pcm″	ode.exe -X -P syclove txt 0, o=0, e=0 ps	ergeek sycgeek-mp3.mp3							
D:\安全工具\Misc工具配置\音频分析	f类工具\MP3St	ego_1_1_19\MP3Stego>									
(2)解码完后,在MP3Stego目录	录下多了一个s	ycgeek-mp3.mp3.txt文件	,打开即可看到flag。								
	📃 sy	/cgeek-mp3.mp3.txt - 记事本									
文件(F) 編辑(E) 格式(O) 查看(V) 帮助(H) SYC{Mp3 B15b1uBiu W0W}											
	(,								

普通的二维码

(1) 下载附件,得到一张二维码,扫描后没有flag。用notepad++打开看看 📔 D:\CTF靶场\BugkuCTF\杂项\025\misc100.bmp - Notepad++ ٥ File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ? Х 📄 misc100. bmp 🔀 - 蘇侁煒縣侊煒蘇侊煒蘇侊煒福和147173120141146145137171060125137120171137163143162151160164137117164143137124145156137101163143151151041175 (2)在最后发现一串数字,想到ASCII码,146作为八进制时对应的是f。然后把这串数字转换成对应的字符,得到flag。 Ascii Encoding Text flag{Have_y0U_Py_script_Otc_To_Ten_Ascii!} Bin 1011111 1010000 1111001 1011111 1110011 1100011 1110010 1101001 1110000 1110100 1011111 1001111 Oct 146 154 141 147 173 110 141 166 145 137 171 60 125 137 120 171 137 163 143 162 151 160 164 137 117 164 143 137 124 157 137 124 145 156 137 101 163 143 151 151 41 175

Dec

102 108 97 103 123 72 97 118 101 95 121 48 85 95 80 121 95 115 99 114 105 112 116 95 79 116 99 95 84 111 95 84 101 110 95 65 115 99 105 105 33 125

Hex

66 6c 61 67 7b 48 61 76 65 5f 79 30 55 5f 50 79 5f 73 63 72 69 70 74 5f 4f 74 63 5f 54 6f 5f 54 65 6e 5f 41 73 63 69 69 21 7d https://blog.csdn.net/FAFUxiaosory