## BugKu CTF(杂项篇MISC)—赛博朋克



<u>M络安全研究所</u> ● 于 2021-02-02 11:13:36 发布 文章标签: <u>乱码 css html 微软 md5</u> 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/zjzqxzhj/article/details/113578023</u> 版权 CTF

BugKu CTF

(杂项篇MISC)

攻与防



赛博朋克

描述: flag{}

下载之后是一个压缩包,包含一个txt文本文件。

🖀 file.zip - WinRAR					-		×
文件(图命令)(C) 工具(S) 收藏夹(Q) 接项(N) 報助(H)							
Image: The state of the sta							~
名称 ガンジョン ブラン ガン ブラン ガン ブラン ガン ブラン ジョン ション ブラン ション ション ション ション ション ション ション ション ション ショ	小压缩后大	ト 美型	修改时间	CRC32			
		文件夹					
Cyberpunk.txt * 428,1	97 428,43	7 文本文档		<u>お安全</u>	研究	所	

一、工具

十六进制工具 010 editor

图片分析工具 Stegsolve

二、解题思路

1.先尝试把压缩包解压,提示需要密码。看看压缩包属性也没有发现特殊字段。

輸入密码 ×	(
为加密的文件输入密码 C:\Users\ADMINI~1\AppData\Local\Temp\\cyberpunk.t; 在压缩文件 file.zip 里	xt
输入密码(E)	
~ ·	
□显示密码( <u>s</u> )	
□ 用于所有压缩又件(A) 	
整理密码(0)	
确定 取消 影助 影动	л

2.考虑有没有可能是zip压缩包的伪加密了。用010 editor编辑器打开看一看。找到从504B0102字节,从50开始 算,第9和第10个字节改为0000

6:89B0	h: BC	36	29	2A	2A	38	2A	9A	14	16	AD	FD	7F	E7	FF	0B	¼6)**8*šý.çÿ.
6:89C0	h: 50	4B	01	02	1F	00	14	00	09	00	08	00	BC	Α9	33	52	PK
6:89D0	h: 68	E0	0E	46	95	89	06	00	6D	89	06	00	0D	00	24	00	hà.F•‰m‰\$.
6:89E0	h: 00	00	00	00	00	00	20	00	00	00	00	00	00	00	63	79	cy
6:89F0	h: 62	65	72	70	75	6E	6B	2E	74	78	1	0A	00	20	00	00	berpunk.txt
6:8A00	h: 00	00	00	01	00	18	00	7F	D0	6D		64	EE	D6	01	7F	ĐmñdîÖ
6:8A10	h: DO	6D		64	EE	D6	01		2A	80		4	EE	D6	01	50	ÐmñdîÖ.;*€¹dîÖ.P
6:8A20	h: 4B	05	06	00	00	00	00	01		01	00	5 F	00	00	00	C0	кÀ
6:8A30	h: 89		00	00	00												
															不日		0字节
																	_
																	🕐 网络安全研究所

3.压缩包可以正常解压了。确实是伪加密。但是打开之后是一堆乱码。发现头部有个NG,猜测可能是png图片。

	🥘 cyberpunk.txt - 记事本	_		$\times$	٦
	文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H)				
	塒NG				^
	IHDR □? □?□ _橣? € IDATx^鞚?□ 隹馏鶣□(	ば覗□□			
	!	悥禓	z挽武	ŧ	
	儋莩?讅顂??d? r^粿□□抆篁鍉?鯥?踶縯暭~厁汿N	紡[	亘玎}		
	鈣晗-适鯧鐠痶濿E孱廾?枿P1D□□猆IQ猨妑5Z猉	?v6₿	方伅蜜	ġ	
	繅□娬毂W?{殮b?昳銏]?n>□;i吡娈丨j?旺!肫?摅煈鴛	≣H辊	?遄		
	珷□□?珇)/'楛竼\$?F桷=T~飥妎霶虻□J坎E?□ ?瀛	鞵掌□	U瓬P		
e	遮I? 幨:℃隵(o鍘?O ??舳k捑□䴙轊吟?I?□掫=僵.	終? ?[	路,	誩	
p	?笢TOg+塤穗曜\??交>屣??阝)W蘅鲖{.?w ?嚉Z	谝?蔜l	Pl	吟	
	?(U□T6矴 筲□\$?^?浊 厵?H崄糛P.+/邩?y?鱌美	le la			
	者鰿征. ?錩;□造Q鷯□J[;牑?*□ve喘黐[贠0 塦鲮	店掫o	贅 á	硫	
	髹\$□Bc`愶 '\$ /)C酠抇护w呍粬kH襬行g惍嵥)卓	7罫蓐	熞鱟		
l	赃? 丝' 娄鲞I ¥2 姓瀍 α2 I 広 铜 萜 2 拉 O 芹 濯 2 mi NIN 2	2-服	約須爾	<b>汉</b> 所	2
	Windows (CRI 第 4 行	Se 12 h	00%	2311	

4.用010 editor编辑器打开看看,前面讲过89504E47是PNG文件头标识。这应该是一张图片被改后缀了。因此将txt后缀改为png。

							-									•••	
起始页	fi	file.zip cyberpunk.txt ×															
	ð				4									D			0123456789ABCDEF
0000h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	PNGIHDR
0010h:	00	00	01	<b>B</b> 3	20	00	01	CC	08	06	00	00	00	5F	99	46	³Ì™F
0020h:	93	00	00	80	5	49	44	41	54	78	5E	EC	9D	F5	7F	14	"€.IDATx^ì.õ
0030h:	D7	FB	F6	BF	7F	<u>C1</u>	F3	FA	40	12	A4	D0	D2	96	16	0F	×ûö¿.Áóú@.¤ĐÒ
0040h:	09	21	09	C4	DD	91	04	77	B7	04	E2	EE	1E	42	20	81	.!.ÄÝw∙.âî.B .
0050h:	78	02	C1	9D	52	B4	88	6B	5C	71	77	2B	EE	2D	5C	CF	x.Á.R´,k\qw+î-\Ï
0060h:	7D	9F	CD	DO	65	48	90	96	B6	40	F9	E1	7A	CD	EC	CC	}ŸÍÐeH¶@ùázÍìÌ
0070h:	99	D9	D9	DD	B3	E7	ЗD	D7	7D	EE	73	E6	FF	B2	01	64	™ÙÙݳç=×}îsæÿ².d
0080h:	BF	00	72	5E	BC	40	0E	14	92	5E	F3	F2	E5	7E	DE	2E	¿.r^¼@. 📣◊渤波安山瓜志能
0090h:	F6	49	FB	15	DB	79	BF	74	AC	F2	7E	85	78	9B	54	4E	öIû.Ûy¿t=灵资料及主听九川
00A0h:	F9	FC	7F	BC	8F	D8	CF	E7	E0	7D	E2	7D	EA	CF	2D	CA	ùü.¼.ØÏçà}â}êÏ-Ê

5.打开看到一张图片。用010打开之后未看到报错信息,没有CRC错误之类的。



6.考虑图片隐写,用Stegsolve工具看一看吧。最常见的就是LSB隐写,RGB模式。设置完之后往上翻,发现最上面就是flag了。



3.总结

本题需要掌握010 editor编辑器,zip压缩包文件头和伪加密方式,图片隐写查看器Stegsolve,LSB隐写等。 常用文件的文件头如下(16进制):

- JPEG (jpg), 文件头: FFD8FFE1
- PNG (png), 文件头: 89504E47
- GIF (gif), 文件头: 47494638
- TIFF (tif), 文件头: 49492A00
- CAD (dwg), 文件头: 41433130
- Adobe Photoshop (psd), 文件头: 38425053
- Rich Text Format (rtf), 文件头: 7B5C727466
- MS Word/Excel (xls.or.doc), 文件头: D0CF11E0
- ZIP Archive (zip), 文件头: 504B0304
- RAR Archive (rar), 文件头: 52617221

## END

扫码关注

网络安全研究所

更多精彩等着你

