# 欢迎来到地狱 WriteUp(2019暑假CTF第一周misc)



- 0707, 0708, 0709
  - 题目地址: 欢迎来到地狱
    - 1.地狱伊始.jpg
    - 1.5地狱之声.wav
    - 2.第二层地狱.docx
    - 3.快到终点了.zip
  - 参考

## 0707, 0708, 0709

#### 题目地址:欢迎来到地狱

下载下来有3个文件,地狱伊始.jpg,第二层地狱.wav,快到终点了.zip。依次解之。

1.地狱伊始.jpg

使用hexeditor查看发现缺少正确的.jpg文件头,	于是添加之。	方法是先复制全部
------------------------------	--------	----------



然后新建Hex文件, 敲入FFD8FFE0, 再把复制的内容粘进去

File	Edi	it S	earc	h ۱	View	/ Fo	orma	at S	Scrip	ots	Tem	ıplat		Too	ls '	Win	dow	Help
L 🗋	~ 🗖	<b>-</b> ~		1	J 1	1	11	‰∎	h í	n e	) (	۱.,	•	8 🍃	• ->		A₁ I	📐 🔤 📰 🗉 📰 । 🔜 📦 🗱 🔽 🚹 🐼 🏭
Star			地狱	伊始	. ipg		HELI	L1. j	ipg >	ĸ								
¥ E	dit	As:	Hex		Run	Scri	.pt `	∕ R	un T	enpl	late							
																		0123456789ABCDEF
0000		FF		FF	EE	00			46		46							yøyîJFIF`
0010						FF	E1											.`ÿá."ExifMM
0020		00		00	00	00	08	00			12	00	03	00	00	00		
0030		00	01	00	00	00	00	00	00	FF		00	43	00		01	01	ÿÛ.C
0040		02	01	01	02	02	02	02	02	02	02	02	03	05	03	03	03	
0050		03	03	06	04	04	03		07	06	07	07	07	06	07	07		
0060		09	0B	09		08	0A	08	07	07	<b>0</b> A		0A	0A	0B	0C	0C	
0070				07	09										FF			·····.ÿÛ.
0080		43				02	03	03	03	06	03	03	06	0C	08	07	08	
0090		00	00	00	00	00	00	00	00	00	00	00	00	00	00		00	
0070		00	00	00	00	00	0C	00	00	0C	00	00	00	0C	00	0C	00	
OORO		00	00	00	00	00	nc.	00	00	0C	00	00	00	0C	00	0C	00	
00000		00	00	50	C0	00	11	00	00	70	02	15	02	01	22	00	02	
0000		11	00	0.2	11	00	11	00	00	1.5	0.0	40	03	01	01	00	02	yA
0000		11	01	03	11	01	00	0.0	00	11	00	00	01	05	01	01	01	уд
0060		01	01	01	00	00	00	00	00	00	700	10	01	02	03	04	05	
00100		00	07	00	09	AU	0B	E E	0.4	00	<u>БЭ</u>	10	00	02	01	03	03	yA.µ
0100		02	04	103	05	05	04	04	10	00	01	70	01	02	14	00	04	
0110		11	05	12	21	31	41	06	13	51	61	07	22	/1	14	32	81	!IAQa."q.2.
0120		91	AL	08	23	42	BL	CI	15	52	DI	FO	24	33	62	12	82	';.#B±A.RNO\$3br,
0130		09	AU	16	17	18	19	1A	25	26	27	28		2A	34	35	36	
0140		37	38	39	3A	43	44	45	46	47	48	49	4A	53	54	55	56	789:CDEFGHIJSTUV
0150			58	59	5A	63	64	65	66		68	69	6A		74			WXYZcdefghijstuv
0160		77		79	7A	83	84		86	87	88		8A	92	93	94		wxyzf,,†‡^%S'``'•
0170		96	97			9A	A2	A3	Α4	A5	A6	Α7	<b>A</b> 8	A9	AA	в2	в3	~m𢣤¥¦§"©ª23
0180		В4	в5	В6	в7	B8	В9	BA	C2	C3	C4	C5	C6	C7	C8	C9	CA	´μ¶·,¹°ÂĂĂĂÆÇÈÉÊ
0190		D2	D3	D4	D5	D6		D8	D9	DA	E1	E2	Е3	E4	E5	Е6	Е7	ÒÓÔÕÖרÙÚáâãäåæç
01A0		E8	Ε9		F1	F2	F3	F4	F5	Fб	F7	F8	F9		FF	C4	00	èéêñòóôõö÷øùúÿÄ.
01B0																		
01C0								04								FF	C4	ÿÄ
01D0																		
01E0				77					11	04		21			12	41		w!1AQ
01F0					13					14	42		A1				23	.aq."2B`;±Á.#
0200		33		FO	15		72				24	34	E1		F1	17		3Rð.brÑ\$4á%ñ
0210			1A												43	44		&'()*56789:CDE
0220		46	47	48	49	4A	53	54		56	57				63	64		FGHIJSTUVWXYZcde
0230		66						74		76					82	83	84	fghijstuvwxyz,f"
0240		85	86	87	88	89	8A	92	93	94	95	96	97	98	99	9A	A2	t+^&Š'``″•~**š¢
0250		A3	A4	A5	Aб	A7	<b>A</b> 8	A9	AA	B2	В3	В4	в5	в6	в7	в8	В9	£¤¥¦S"© <sup>a23</sup> 'u¶· 1
0260		BA	C2	C3	C4	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5	D6	D7	°ÂÃĂĂÆCÈÉÊÒÓÔÕÖ×
0270		D8	D9	DA	E2	E3	E4	E5	Eб	E7	E8	E9	EA	F2	F3	F4	F5	ØÙÚâãaåæçèéêòóôő

保存为.jpg文件,就可以正常打开了。

打开图片,复制里面的网盘链接,下载下来是一个.wav文件。

1.5地狱之声.wav

Í.	<b>)</b>	
hans 5.0 10.0 15.0 20.0 25.0 30.0 35.0 40.0 45.0 50.0	GD dB	
	6 12	
<u></u>		
	р , с !	
	dB 6	
<u></u>		
and present of a proper state of the	– Hz	
	- 1k - Hz	
all an an ann ann ann ann ann ann ann an	- 1k 2, {}Q,	

用au打开,查看频率部分,由一长一短两种固定长短的线条组成,可联想到摩斯码。

a · -	i • •	r	1 ·
ä · - · -	1	s · · ·	2 · ·
b - • • •	к-·-	t -	3 · · ·
C - · - ·	1	u · · -	4 · · · · -
ch	m	ü · ·	5 · · · ·
d - • •	n - ·	v · · · -	6 - • • • •
e ·	0	w ·	7 · · ·
f··-·	ö'	x - · · -	8 • •
g ·	D ' '	v - ·	9
h • • • •	<b>0</b>	7	0

翻译得keyletusgo。

2.第二层地狱.docx



需要输入密码打开,我们输入用地狱之声解出来的lesusgo





在word中文件>>选项>>显示,勾选"隐藏文字"



发现多了一句话: image steganography,是图片隐写。 搜索之找到一个在线网站image steganography,虽然解不了本题,但是码一下吧。 然后我又下载了一个叫image steganography的软件,还是解不了。 网上说使用在线网站: http://www.atool.org/steganography.php 可以解,但是我的电脑打不开这个网址。 用手机就能打开了。顺便贴一下其代码参考地址: https://github.com/oakes/PixelJihad 但是手机解不了。

ATOOL在线工具 www.atool.org

.、、解密带隐藏信息的图片

1. 从电脑中选择一张带有隐藏信息的图片:

选择文件 mmexport1562571264720.jpg

2. 输入需要解开信息的密码(如果没有密码可以

不填):

信息查看密码,可以为



## 说明 | Introduce

 隐写术算是一种加密技术,权威的wiki说法 是"隐写术是一门关于信息隐藏的技巧与科 学,所谓信息隐藏指的是不让除预期的接收 者之外的任何人知晓信息的传递事件或者信 息的内容。

 $\langle \rangle$   $\triangle$   $\Box$   $\equiv$ 

这时候我奇思妙想,用手机给电脑开热点,然后就能用电脑进入这个网址了。

ATOOL在线工具	PS/编辑器	多媒体	站长工具	开发者工具	便民工具	关于&合作	🐣 QQ登录
二、、解密带隐藏信息的图片							
1.从电脑中选择一张带有隐藏信息的图片: 浏	览 helldog.png						
2. 输入需要解开信息的密码(如果没有密码可以	(不填): 信息查看密码	,可以为	空即为图片	解密不需要密	码		
解密出隐藏的信息							
图片中隐藏的信息为:key{you are in finally h	ell now}						

不容易不容易啊。得到key{you are in finally hell now}

3.快到终点了.zip

解压之发现需要密码,输入you are in finally hell now,解压。

解压出来有一个图片和一个文本文件,文本文件里面是一串01串,使用converter转成text发现是ruokouling,也就是弱口令的拼音。



全部清除				$\sim$
	输出格式	None	🗆 小数位填零	

在kali中对图片"地狱大门.jpg"使用binwalk,发现藏了个.zip文件,用dd分离出来。

root@yutia 地狱大门.j	<mark>nhack:/mnt/hgfs/y</mark> pg	utianhackshare/CTF培训作业 /欢迎来到地狱 /快到终点了#binwalk
DECIMAL	HEXADECIMAL	DESCRIPTION
0 62584	0x0 0xF478	JPEG image data, JFIF standard 1.01 End of Zip archive, footer length: 22
<b>root@yutia</b> 狱大门 . jpg 记录了 22+0 记录了 22+0	nhack:/mnt/hgfs/yu of=开门.zip skip 的读入 的写出	utianhackshare/CTF培训作业/欢迎来到地狱/快到终点了# dd if=地 =62584 bs=1
22 bytes c root@yutia 地狱大门.i	opied, 0.00705583 nhack:/mnt/hgfs/yu pg 开门.zip 最后	s, 3.1 kB/s utianhackshare/CTF培训作业/欢迎来到地狱/快到终点了#ls i一层地狱.txt

### 发现这个.zip文件坏了,解压不了。

用winhex改其文件头为504B0304,在文件尾部添加504B进行修复。 然后发现还是显示损坏。



整这么多花里胡哨的无果,其实改一下后缀名就能解决。。

ARCHPR 4.54 Professional Edition

文件(F) 恢复(R) 帮助(H)

	_
0% 輸入密码 ×	:00:00
小姐姐诶.txt	
0% 请输入密码	:00:00
小姐姐诶.txt ✓ 用星号隐藏密码(H)	
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	

然后要输入密码,所以根据弱口令的提示,我们进行弱口令爆破就可以了。 爆破发现不是.zip文件,所以应该这个时候修改文件头才对(多谢马老师指点)。



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

结果修改后保存显示"请确信文件夹存在和文件未被写保护"的错误。

然后在选项>>常规,修改临时文件目录和保存镜像和备份的目录为一个我自己建的目录,点确定后退出 winhex。



见鬼的是再次打开winhex后发现这两个目录竟然没有变化。 尝试半天无果我决定去它的,用010editor吧。

然后还是各种失败,,,好吧,换一个破解工具ziperello。

👔 Ziperello					
Jan zipere	llo assword recovery to	ol	帮助	关于	退出
	字符类型: 固定:	字符集			E.
字符集 ▼ 数字(0-9) ▼ 小写字母(a-z) ▼ 大写字母(A-Z)	<ul> <li>✓ 特殊符号(!@)</li> <li>✓ 空格</li> <li>✓ 所有印刷字符</li> </ul>	最小密码长度 = 1 最大密码长度 = 20 全	- 起始密码		
	步骤 3				
1. 选择字符集类型: 固新	定或自设。				
定义可能存在于密码中的	的字符集。				
3. 设置最小及最大密码	长度。				
4. 输入起始密码(非必续	需)				
		步骤 3 / 4: 暴力破解设定			
Ziperello ver. 2.1	版权所有 (C) 2008	FDRLab			

暴力破解48小时都搞不完,我破了几个小时后想了想放弃了,改成用字典破,结果第二个字典就秒出了。

7 Ziperello			_	
ziperello				
		帮助		
当前恋孤长度	7		步骤 4	
		准备就绪,请点击 [开	始] 按钮	

逝去时间: 04:13:59	当前密码 当前速度 0%	信息	× assword 耗	意:搜索进度条(%)及剩余时 的密码效验长度相关。破解 AE 时较长。	间字校显示的信息与当 5 算法加密的密码可能
22:29:03: 密码: "Pass	word".时间: 0 s				
		步骤 4 / 4: 破解	窨码.Go		NEXT
Ziperello ver. 2.1					7 → (字句子)、
<b>锏</b> 八密码,	<b>解</b> 压出米 是 凶	.样一个又人	41人4	(我于动换行)	「, 万便观有)
文件(F) 編編(E) 橋式(O) 重都	■(V)  蜀助(H) (flag) 已经被贝斯家族的 の小姐姐被这个家族的化力	9人劫持了, 、带向了地狱的另一	-个名门望族	田斯家族	- 0 ×

中途他们还经历了兔子洞穴。

最后你从那个家族的sixfour手里拿到了面目全非的小姐姐

(VTJGc2RHVmtYMTlwRG9yWjJoVFArNXcwelNBOWJYaFZlekp5MnVtRIRTcDZQZE42elBLQ01BPT0=)。

你能帮小姐姐恢复容貌吗?

可见是一个连环加密,我们要解密需要按与加密时相反的顺序,所以先base64(贝斯、sixfour),再rabbit解密 (兔子洞穴),再凯撒密码(凯撒家族)。

**8**登录

#### base64转文本:



#### rabbit解密: O A https://www.so \$\$ □ ☆ ☆ 在线工具 生活工具 技术博客 备案查询 免费 JSON API 在线教程 iQuery下载 CDN加速 垃圾分类查询 C-3阿里云 <u>618</u> SO JSON<sup>®</sup>在线 → か 密/餅 密 内网穿透 爆款云产品低至 1折 首页 / 加密 & 解密 / Rabbit加密 & Rabbit解密 加密解密 AES加密解密 DES加密解密 RC4加密解密 Rabbit加密解密 TripleDes加密解密 MD5加解密 Base64加解密 Hash加解密 JS 加密 fxbqrwrvnwmngrjxsrnsrnh> 在此输入密钥 U2FsdGVkX19pDorZ2hTP+5w0zSA9bXhVezJy2umFTSp6PdN6zPKCMA=

凯撒加密,一个一个偏移值的试,试到17时发现是一句拼音"我是你们的小姐姐哟"

17			
	8除标点 (Remove Punc	tuation)	
	加密	解 密	

### 提交之,本题完成。



参考

1.码一下常见的文件头: 常用文件的文件头如下(16进制): JPEG (jpg), 文件头: FFD8FFE0或FFD8FFE1或FFD8FFE8 GIF (gif), 文件头: 47494638PNG (png), 文件头: 89504E47 TIFF (tif), 文件头: 49492A00 Windows Bitmap (bmp), 文件头: 424DC001 CAD (dwg), 文件头: 41433130 Adobe Photoshop (psd), 文件头: 38425053 Rich Text Format (rtf), 文件头: 7B5C727466 XML (xml), 文件头: 3C3F786D6C HTML (html), 文件头: 68746D6C3E Email [thorough only] (eml), 文件头: 44656C69766572792D646174653A Outlook Express (dbx), 文件头: CFAD12FEC5FD746F Outlook (pst), 文件头: 2142444E MS Word/Excel (xls.or.doc), 文件头: D0CF11E0 MS Access (mdb), 文件头: 5374616E64617264204A WordPerfect (wpd), 文件头: FF575043 Adobe Acrobat (pdf), 文件头: 255044462D312E Quicken (qdf), 文件头: AC9EBD8F Windows Password (pwl), 文件头: E3828596 ZIP Archive (zip), 文件头: 504B0304 RAR Archive (rar), 文件头: 52617221 Wave (wav), 文件头: 57415645 AVI (avi), 文件头: 41564920 Real Audio (ram), 文件头: 2E7261FD Real Media (rm), 文件头: 2E524D46 MPEG (mpg), 文件头: 000001BA MPEG (mpg), 文件头: 000001B3 Quicktime (mov), 文件头: 6D6F6F76 Windows Media (asf), 文件头: 3026B2758E66CF11 MIDI (mid), 文件头: 4D546864

还有一个含文件尾的: 文件头文件尾总结

2.凯撒加密 3.rabbit解密

转载于:https://www.cnblogs.com/hardcoreYutian/p/11155774.html