MISC-图片隐写



隐写同时被3个专栏收录

2篇文章0订阅

订阅专栏



30 篇文章 6 订阅

订阅专栏



4 篇文章 0 订阅 订阅专栏

MISC-图片隐写

MISC1: Paint&Scan

标题的意思是画图和扫描

...



贴图库中找不到该图片 可能已被删除或者服务到期

题目提示也是。下载题目文件并解压,得到txt文件。打开





贴图库中找不到该图片 可能已被删除或者服务到期

很明显就是画图了。用到画图工具gnuplot。所以先替换,将坐标转换成gnuplot能识别的格式



贴图库中找不到该图片 可能已被崩除或者服务到期

...



贴图库中找不到该图片 可能已被删除或者服务到期

然后开始画图, 画图命令 plot "Paint&Scan.txt"



贴图库中找不到该图片 可能已被删除或者服务到期

画出了张二维码

...

404

贴图库中找不到该图片 可能已被删除或者服务到期

二维码扫一下,得到flag

...



贴图库中找不到该图片 可能已被删除或者服务到期

MISC2: 九连环



题目没有提示。打开链接保存jpg图片



binwalk分析一下

MINGW64:/d/	网安/网安工具/隐写工	具/图片隐写/分离工具/binwalk-master/binwalk-master/build/scripts-3.7			×
ASUS@LAPTOP-5I	08T0UO2 MINGW64	/d/网安/网安工具/隐写工具/图片隐写/分离工具/binwalk-master/binwalk-master/bui	ld/scri	pts-3.	. 7
\$ python3 binw	valk 123456cry.	jpg			
DECIMAL	HEXADECIMAL	DESCRIPTION			
0 19560 48454 name: asd/qwe. 48657 48962	0x0 0x4C68 0xBD46 zip 0xBE11 0xBF42	JPEG image data, JFIF standard 1.01 Zip archive data, at least vl.0 to extract, name: asd/ Zip archive data, at least vl.0 to extract, compressed size: 184, uncompress End of Zip archive, footer length: 22 End of Zip archive, footer length: 22	ed size	: 184,	

图片里隐藏了文件,foremost分离一下。为了方便,可以直接用winRAR打开jpg图片,并解压隐藏文件。

123456cry.jpg (评估版本)	1		×
文件(F) 命令(C) 工具(S) 收藏 输入密码 ×			
 参加密的文件输入密码 添加解压到测试 查看 个 123456cry.jpg\asd 	留 压格式		×
名称 输入密码(E)	CRC32	2	
■ ~ · · · · · · · · · · · · · · · · ·	E0C61 7ED53	3D3 3A	
□显示密码(s)			
□用于所有压缩文件(A)			
■ ● 已经选择 29,992 字节(1 确定 取消 帮助		-	

有一个加密了。先看是不是伪加密

00	01	00	18	00	69	B8	48	34	83	48	D3	01	69	в8	48		i,H4	4∫HÓ	i,H
34	83	48	D3	01	E9	FC	59	31	83	48	D3	01	50	4B	01	4fHÓ	éüY:	lfhó	PK
02	3F	00	14	00	01	08	08	00	48	4E	53	4B	8C	3A	D5	?		HNSE	KŒ:Õ
7E	88	70	00	00	28	75	00	00	16	00	24	00	00	00	00	~^p	(u	Ş	
00	00	00	20	00	00	00	22	00	00	00	61	73	64	2F	67		"	as	sd/g
6F	6F	64	2D	E5	в7	B2	E5	90	88	E5	B9	B6	2E	6A	70	ood-a	a ∙²å	^å19	I.jp
67	0A	00	20	00	00	00	00	00	01	00	18	00	69	31	23	g			i1#
00	70	10	52	01	20	7 17	TE	OF	00	10	52	01	00	75	10	mIIIÓ	165	τιć	2.2

是伪加密,把504B0102后第五、第六位0108改为0000,即可破解伪加密

🌌 123456cry.jpg (诩	P估版本)						83 - 3	I	o x
文件(F) 命令(C) 工具	【(S) 收藏夹(O)	选项(N) 帮	帮助(H)						
添加 解压到 测试		↓ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	向导	〔 信息	() 扫描病毒	E 注释 e	4月1日日本	各式	
123456cry	.jpg\asd - 自解/	玉格式 ZIP 日	缩文件,	解包大	小为 30,176	字节			~
名称	大小	压缩后大小	类型		修改	时间	CR	C32	ana-
			文件夹						
🔳 qwe.zip	184	184	zip		2017	7/10/19 1	EO	C613D)3
good-宸插悎骞	29,992	28,808	文件		2017	7/10/19 9	7E	D53A.	
				总计	30,176 字节	ī(2 个文件)		

解压



这应该是张jpg图片,用winHex查看果然是。加文件后缀.jpg,打开图片



i qwe.zip (评估版本	(4		- 🗆 X
文件(F) 命令(C) 工具	具(S) 收藏夹(O) 选项(N)	帮助(H)	
添加 解压到 测试	正 近 查看 删除 查找	① ② ● 向导 信息 扫描病毒 注	
↑ 🔳 qwe.zip -	ZIP 压缩文件, 删除文件 22	字节	~
名称	大小 压缩后大小	类型 修改时间	可 CRC32
III		文件夹	
ilag.txt *	22 34	又本又档 201//1	0/19 9 B635C4
		总计 22 字节(1 个文	(件)

发现加密的flag.txt文件。用winHex打开qwe.zip,发现并不是伪加密。好像进行不下去了,于是参考了下大牛的博客。发现要用 到一个工具**steghide**。

用法: steghide extract -sf picture.jpg

然后输入密码,没有密码则回车跳过

于是刚才那张图片就可以用到了

MINGW64:/d/网安/网安工具/隐写工具/steghide			
ASUS@LAPTOP-5D8T0U02 MINGW64 /d/网安/网安工具/隐写工具/s \$ steghide extract -sf good-宸插悎骞.jpg Enter passphrase: wrote extracted data to "ko.txt".	steghi	de	
🥘 ko.txt - 记事本	<u>, 111</u>		×
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)			
看到这个图片就是压缩包的密码:			~
bV1g6t5wZDJif^J7			
			~

🥘 flag.txt - 记事本		×
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)		
flag{1RTo8w@&4nK@z*XL}		^
		~

MISC3: 欢迎来到地狱

	25				
来源: HTTPERROR404	难度:中	参与人数: 9741人	Get Flag: 1963人	答题人数: 2119人	解题通过率: 93%
连环套哦。格式CTF{xxxx] 解题链接: http://ctf5.sh	• iiyanbar.com/s	tega/hell/欢迎来到地狱	ť.zip		

下载题目文件并解压

	欢迎来到地	狱			85 .	- 🗆	×
文件 主页	共享	查看					~ 🕐
★ 复制 固定到"复制 快速访问"	● お貼 メ 剪切 前時板	【复制路径 】粘贴快捷方式	 ▶移动到 · × 删除 · ●复制到 · ● 重命名 	1 新建 文件夹		 全部选择 会部取消 反向选择 	
	、星個	、十一星個第一[割、 欢迎来到地狱 、 欢	0 来到他粉	171	搜索"欢迎	Q
 ☆ 快速访问 ▲ 桌面 ▲ 下载 〇 文档 〇 図片 ● Paint&So ● Snake ● 欢迎来到 ● 九连环 ⑦ OneDrive 	★ ★ ★ can	 名称 地狱伊 第二层 第二层 中)約 	个 地狱.docx 经点了.zip		修改日期 2017/10/16 12:2 2017/10/15 8:30 2017/10/13 18:5	类型 1 JPG 文件 Microsof 4 zip	t Worc
耐件 3 个项目		~ <					> ===

打开**地狱伊始.jpg**



无法打开,用winHex查看一下文件格式,发现缺少文件头

🇱 WinHex - [地狱伊	始.jpg]																					
🧱 文件(F) 编辑(E)	搜索(S) 导航(N) 1	查看((V)	工具	(T)	专业	工具	(I)	选项((D) i	窗口((W)	帮助)(H)							
案件数据) 🗅 🏹 🗔 🖉 🖉	۱ 🖻	1			•	6	101 010	7	A 44	HEX	¢.,₽	MEX	-	-121	÷ -	▶	3	3 췌 🛙	n 🔎	🤊 📐 🥨)
文件(L) 编辑(D)	地狱伊始.jpg								_													
	Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	Е	F		A	NSI	ASCII	~
	00000000	00	10	4A	46	49	46	00	01	01	01	00	60	00	60	00	00	C	JFIF		N N	
	00000010	FF	E1	00	22	45	78	69	66	00	00	4D	4D	00	2A	00	00	ÿá	"Exi	f M	M *	
	00000020	00	08	00	01	01	12	00	03	00	00	00	01	00	01	00	00	1 1990				
	00000030	00	00	00	00	FF	DB	00	43	00	02	01	01	02	01	01	02		ÿÛ	С		
	00000040	02	02	02	02	02	02	02	03	05	03	03	03	03	03	06	04					
	00000050	04	03	05	07	06	07	07	07	06	07	07	08	09	0B	09	08	5				
	00000060	08	0A	08	07	07	0A	0D	0A	0A	0B	0C	0C	0C	0C	07	09					
	00000070	0E	OF	0D	00	0E	0B	0C	0C	0C	FF	DB	00	43	01	02	02			ÿÛ	C	

jpg图片的文件头是FFD8FF,添加文件头

插入	(的0字节数:
ঝ	

保存图片并打开

照片 - 地狱(尹始.jpg							ı ×
	ŗ	€	Ì	\heartsuit	ୢ	‰ ~	Ŀ	
很久很	<u> </u>	。。。小姐	姐。。。。。	。。。扑通	一下子。。。。	。。。。掉进了地	b狱。(别	问
我为咱	舍,因为 <u>她沉行不行</u>)。。 是这个小姐姐呢,还是	总之 举	と。。。。 う你快:	有一位河泊 主教她四	伸有一天对作 !"对了 我	尔说:"年轻的 这里有舟舟的	樵夫呀, 资源呦!	你
htt	p://pan.baidu	.com/	s/1i4	9Jhlj	·	心王书置西的	风际型	+
								2

图片里有个百度云盘链接, 输入浏览器打开



下载wav音频文件,播放,发现比较有规律。应该是音频隐写了。使用音频分析工具Audacity打开wav文件,然后



▲ 地脉之声	- 0 ×
文件(F) 编辑(E) 视题(V) 攝录(R) 轨道(T) 生成(G) 效果(C) 分析(A) 帮助(H)	
MME - 🎤 麦売风 (Realtek(R) / ~ 2 (立体声) 🗐 🗤 🚸 扬声器 (Realtek(R) , ~	
- 4.0 0.0 2.0 4.0 6.0 8.0 10.0 12.0 14.0 16.0 18.0 20.0 22.0 24.0 26.0 28.0 30.0 32.0 34.0 36.0 38.0 40.0 42.0 44.0 46.0 48.	0 50.0 52.0
■ 地紀之声.txt - 记事本 - □ × 文件(f) 編輯(E) 格式(O) 查看(V) 帮助(H) /,//// ^ ^ ^ ^ ^ ^ ^ ^ ^ ^ ^ ^ ^ ^ ^	

摩斯电码解密得到

众果搜首页>>摩尔斯电码转换
英文字母:
KEYLETUSGO
转换为摩斯电码 清除 生成摩斯代码的分隔方式: ● 空格分隔 ● 单斜杠/分隔 摩斯电码: (格式要求:可用空格或单斜杠/来分隔摩斯电码,但只可用一种,不可混用) /./////
转换为英文字母

打开**第二层地狱.docx**,发现被加密了。上面应该就是密码了,有点坑的是密码小写,即letusgo 打开之后,选择显示隐藏文字

Word 选项		?	×
常规 显示	更改文档内容在屏幕上的显示方式和在打印时的显示方式。		
校对	页面显示选项		
保存	☑ 在页面视图中显示页面间空白(W) ^①		
版式	☑ 显示突出显示标记(出)①		
语言	☑ 悬停时显示文档工具提示(L)		
轻松访问	始终在屏幕上显示这些格式标记		
高级	□ 制表符(I) →		
自定义功能区	□ 空格(<u>S</u>) ····		
快速访问工具栏	☑ 段落标记(M)		
加载项	✓ 隐藏文字(D) abc		
信任中心	□ 可选连字符(Y) □		
	☑ 对象位置(C) 业		
	□ 可选分隔符(<u>O</u>) □		
	□ 显示所有格式标记(<u>A</u>)		
	打印选项		
	☑ 打印在 Word 中创建的图形(<u>R</u>) ^①		
	□ 打印背景色和图像(B)		
	□ 打印文档属性(P)		
	✓ 打印隐藏文字(X)		
	□ 打印前更新域(E)		
	□ 打印前更新链接数据(K)		
	确定	取	湖

发现

你现在在第二层地狱中,凶猛的。。。。 额。。。。哈士奇。。。。把守着通向第三 层地狱的钥匙,那么。。。。。。。你要 用你手中的剑(握草,老子剑呢,

image steganography,,,是不是掉在 第二层地狱的哪里了)。

image steganography(图片隐写术)

解密网站: http://www.atool.org/steganography.php

所以保存word文档里的图片,用上面网站解密

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	A 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:	选择文件 1.png						
2. 输入需要解开信息的密码 (如果没有密码	马可以不填): 信息查看密码	3, 可以为	n空即为图片	計解密不需要密	四		
解密出隐藏的信息							

National Action (评估版本	·····································	×
文件(F) 命令(C) 上具(S)	为加密的文件输入密码 C:\Users\ASUS\AppData\Local\Temp\Rar\$D\最后一层地狱.bt 在压缩文件 快到终点了.zip 里	自解压格式
↑ ■ 快到终点了.zip -	输入密码(E)	~
名称	you are in finally hell now \sim	CRC32
 ■ 地狱大门.jpg * ■ 最后一层地狱.tx	☑显示密码(S)	3 1 BF50482B 3 1 C96A84
	□用于所有压缩文件(A)	
	整理密码(0)	
■ 🐨 已经选择 124 字节(1_	确定 取消 帮助	

同理解压**地狱大门.jpg**

打开**最后一层地狱.txt**

☐ 最后一层地狱.txt - 记事本			×
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)			
这里有一个大门,勇士把它轰开吧。 (tips:			^
011100100111010101101111011010110110111	1011	11010 ⁻	10
1101100011010010110111001100111)			
			,

8位二进制一组,二进制转ASCII码

文本 复制
ruokouling
十六进制 去除空格 复制 v autospace
十进制复制
二进制复制
01110010 01110101 01101111 01101011 0110101 0110100 01101001 011011

发现解密结果是: 弱口令

将**地狱大门.jpg**用winRAR打开,发现txt加密文件。并不是伪加密,应该就是上边提示的是弱口令。改**地狱大门.jpg**后缀为 **.zip**,用Ziperello和弱口令字典破解得

当前密码 当前密码 当前速度 逝去时间:00:00:00	HK度 Gaceword 信息 0% 密码: P 确定 开始	0	步骤 4 点击 [开始] 按钮 度条 (%) 及剩余时间 长度相关。破解 AES	9字段显示的信息与当 算法加密的密码可能;
J:4/:30:密码: "Passworu",时间:0 s				

输入密码解压txt文件,并打开

🦳 小姐姐诶.txt - 记事本			×
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)			
呀呀呀呀!小姐姐 (flag) 已经被贝斯家族的人劫持了 家族发现小姐姐被这个家族的仆人带向了地狱的另一 贝斯家族。中途他们还经历了兔子洞穴。最后你从那么 sixfour手里拿到了面目全非的小姐姐	7,你 1名门 12家游	戌到割]望族, 家的	し撒 ^
(VTJGc2RHVmtYMTlwRG9yWjJoVFArNXcwelNB 5MnVtRIRTcDZQZE42elBLQ01BPT0=)。你能帮小吗?	OWJ 姐姐	YaFZle 恢复容	kp 貌

很明显Base64解码

Base64编码转换

UT TO ODIW + VUT I WDCOW + TO VEANIV and I	NDOW TV-E71 - Im EM-U	+ D1DT - D707D49 - 1DI001DDT0 -
VI IGCZRHVIILIMIIWKG9VWIIOVFATNACWEI	NBUW HAFZIEKDOMIN	LKIKICDZWZE4ZeIBLWUIBFIU-

加密 解密 ■ 解密结果以16进制显示

U2FsdGVkX19pDorZ2hTP+5w0zSA9bXhVezJy2umFTSp6PdN6zPKCMA==

继续转

Base64编码转换

U2FsdGVkX19pDorZ2hTP+5w0zSA9bXhVezJv2umFTSp6PdN6zPXCMA== 加密 解密 ■解密结果以16进制显示 Salted_i□□M4至mxU{2r.sM*z=F0

发现Salted,应该就是所谓的"加盐"了

在线加密解密(采用Crypto-JS实现)



🔀 Feedback

试了之后发现是加密算法是Rabbit

看到明文,结合txt文件里"凯撒家族"和"sixfour",应该要凯撒解密,且偏移量可能是10或6或4。为了方便,我直接找到解密所有结果的

			解密	
fxt	oarwrynwmner i xsrnsrnhx			
		解密	使用英文字典智能分析	-
第第第第第第第第第第第第第第第第第第第第第第第第第第第第第第第第第第第第第第第	1次解密:fxbarwrvnwurgrixsrnsrr 2次解密:ewapayawvlmfgiwrgmram 3次解密:dvzopuptluklephydplqpl 4次解密:cuvpotosktikdogupokook 5次解密:btxmnsrrisiicnftonioni 6次解密:aswlmrmgirhibmesnmirmi 7次解密:zryklalphoghaldrmlhmlh 8次解密:vgulkpkogpfgzkcalkglkg 9次解密:vgulkpkogpfgzkcalkglkg 9次解密:vgulkpkogpfgzkcalkglkg 9次解密:vgulkpkogpfgzkcalkglkg 9次解密:vgulkpkogpfgzkcalkglkg 13次解密:vnrshmbldmedwhanihdih 12次解密:unofglgkelbevsymbechg 13次解密:tlpefkfibkabufxlgfbgf 14次解密:skodeieiaizatewkfeafe 15次解密:rinedidhzivzsdyledzec 16次解密:ogkzafaewfywpassbawba 19次解密:nfizezdveuvorrfazvaz 20次解密:fildewcxbtcstmxpdvxtvx 21次解密:hlabgbfxgwxqbthcbxcb 18次解密:infizezdveuvorrfazvaz 20次解密:fildewcxbtcstmxpdvxtvx 22次解密:hlabgbfxgwxqbthcbxcb 23次解密:hlabgbfxgwxqbthcbxcb 23次解密:hlabgbfxgwxqbthcbxcb 23次解密:hlabgbfxgwxqbthcbxcb 23次解密:hlabgbfxgwxqbthcbxcb 23次解密:hlabgbfxgwxqbthcbxcb 23次解密:hlabgbfxgwxqbthcbxcb 23次解密:hlabgbfxgwxqbthcbxcb 23次解密:hlabgbfxgwxqbthcbxcb 23次解密:hlabgbfxgwxqbthcbxcb 24次解密:secubwasbrstmxpdvxtvx 22次解密:hgthytypypitlzutput 26次解密:hzdstvtxpyppitlzutput	hx ww fy fy seu dt lcs br aaa izp cyo dxn izp izp idxn izp izp idxn izp izp idxn izp idxn izp idxn izp idxn izp idxn izp idxn izp idxn izp idxn izp idxn izp idxn izp idxn izp idxn izp idxn izp idxn izp idxn id		

得到flag了。

做了三道题,总结完毕。 小白进阶ing