CTF-隐写术(一)

原创

<u>红烧兔纸</u> 于 2020-09-11 14:32:43 发布 702 收藏 7 分类专栏: <u>CTF-隐写术</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/weixin_39934520/article/details/108528738</u> 版权



CTF-隐写术 专栏收录该内容

14 篇文章 2 订阅 订阅专栏

声明:以下CTF题均来自网上收集,在这里主要是给新手们涨涨见识,仅供参考而已。需要题目数据包的请私信或在下方留言。

1.欢迎来到地狱(来源:实验吧)

1.关卡描述

欠迎来到地狱 分值:25				
k源: HTTPERROR404	参与人数:3603人	Get Flag:605人	答题人数:680人	解题通过率:89%
;环赛哦。格式CTF{xxxx}。 ;题链接: http://ctf5.shiyanbar.co	n/stega/hell/欢迎来到地	狱.zip		
		h the est		

2.解题步骤

分析:

查看压缩包文件:

← → ▾ 🛃 ≔ ▾ 📙 欢迎来到地狱.zip\欢迎来到地狱\欢迎来到地狱			▼ 当前目录	查找(支持(e 🖌 🖍
◆ 名称	大小	压缩后大小	类型	安全	修改时间
(上层目录)					
➡ 快到终点了.zip	61.28 KB	61.24 KB	好压 ZIP 压缩文件		2017-10-13 18:54
nng 地狱伊始.jpg	53.59 KB	51.63 KB	看图王 JPG 图片		2017-10-16 12:21
回 第二层地狱.docx	969.50 KB	957.44 KB	DOCX 文档		2017-10-15 08:30

发现一张图片和word文档,并打开:



图片打不开(猜测密钥就在图片中),把图片拖入winhex中,发现缺少文件头(.jpg FFD8FF),粘贴3字节修改一下即可。

意件数据	0 3 6 3	01 0	8 3	3	5		55				#	M .		1		-	-1:1 4	++	3	33	۵ 🖬	P
文件(1) 编辑(12)	地狱(Philipg																					
	Offset	0	1	2	3	4	5	6	7	8	9	A	В	C	D	Ε	F					
	00000000	FF	D8	FF	00	10	4A	46	49	46	00	01	01	01	00	60	00	ÿØÿ	JF.	IF	•	
	00000010	60	00	00	FF	E1	00	22	45	78	69	66	00	00	4D	4D	00	- 9	á =1	Exif	MM	
	00000020	2A	00	00	00	08	00	01	01	12	00	03	00	00	00	01	00					
	00000030	01	00	00	00	00	00	00	FF	DB	00	43	00	02	01	01	02		1	ÿÛ C	1	
	00000040	01	01	02	02	02	02	02	02	02	02	03	05	03	03	03	03					
	00000050	03	06	04	04	03	05	07	06	07	07	07	06	07	07	08	09					
	00000060	0B	09	08	08	0A	08	07	07	0A	OD	0A	0A	0B	0C	0C	0C					
	00000070	0C	07	09	0E	0F	0D	0C	0E	0B	0C	0C	0C	FF	DB	00	43				ÿÛ (2
	08000000	01	02	02	02	03	03	03	06	03	03	06	0C	08	07	08	0C					
	00000090	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C					
	000000A0	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C					
	000000B0	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C					
	00000000	0C	FF	CO	00	11	08	00	7D	03	45	03	01	22	00	02	11	УA		} E		
	00000000	01	03	11	01	FF	C4	00	1F	00	00	01	05	01	01	01	01		уA			
	000000E0	01	01	00	00	00	00	00	00	00	00	01	02	03	04	05	06					
	000000F0	07	80	09	0A	OB	FF	C4	00	85	10	00	02	01	03	03	02		yА	μ		
	00000100	04	03	05	05	04	04	00	00	01	7D	01	02	03	00	04	11			.)		
	00000110	05	12	21	31	41	06	13	51	61	07	22	71	14	32	81	91	11	A	la "	q z .	
	00000120	A1	08	23	92	81	CI	15	52	01	20	24	33	02	72	82	09	1 #5	IA I	RENOS	3DTI	.
	00000130	UA	10	1/	18	19	18	25	20	21	28	29	28	39	35	36	3/	00.0	74 D.E.E.	P. ()	*450/	
	00000140	30	39	38	93		45	40	47	98	49	48	53	24	55	50	57	89:0	DEF	UPILJ	SIUVA	1
	00000150	20	20	28	03	04	00	00	07	00	09	0.4	/3	/4	/5	70	06	ATZC	101	gnij	stuve	<u>.</u>
	00000160	07	79	/A 00	03	24	00	30	2.5	80	3.7	20	92	93	99	95	96	xyz	A C #1	LU C	0423	
	000001/0	21	70	23	28	n.c	A 3	~ 1	61G	419	100	60	-12-2	15/5	12	11.2	17.71		42.7	5.3	26.0	204

📔 地狱伊始.jpg (837×125像素, 54KB) - 2345看图王 - 第1/2张 100%

很久很久以前,有一位。。。。。。。小姐姐。。。。。。 扑通一下子。。。。。。 掉进了地狱。(别问 我为啥,因为<u>她沉行不行</u>)。。。。。总之。。。。有一位河神有一天对你说:"年轻的樵夫呀,你 掉的是这个小姐姐呢,还是。。。。。总之你快去救她吧!"对了,我这里有盘盘的资源<u>呦!。</u> *http://pan.baidu.com/s/1i49Jhlj*

https://pan.baidu.com/s/1i49Jhlj



是一段音频 使用audacity 来处理这段音频:地狱之声.wav

🔒 地狱之声																	-		×
文件(F) 编辑(E)) 视图(V) 摄录	(R) 轨i	≣(T) 生	.威(G)	效果(C)	分析(A)	鞣助(H)											
(m) (s	NG	10	1		-	I	- 0	2	-57-54-51	-48-4	5-42-36	-12	由开始	eių ja	-21-1	-15-1	2-9-	6 -3 0	
00	1	10	シー	<u> </u>	9	2+	* *	り五	-57-54-51	-48-4	5-42-36	-36-1	ia-30-	27-24	-21-1	-15-1	2-9-	6 -3 0	
P		. () +)	ī.			8 B	h 🐴 -11	+ 01-10	50	٢	Þ	P	2.1	2	1	0		•	
MME	·p	麦克风 (Realtek	Audio)	~ 2 ((立体声) 录	181 ~ 40	扬声音	/%ft (Rea	Itek A	v bu								
		9				15				3	0					45	5		
× 地狱之声 ▼	1.0																		<u> </u>
立体角,48000H1 32位 洋点	0.5																		
静音 独奏	0.0		_							_		_			-			-	
	0.0																		
- O	-0.5																		
	-1.0	_																	
	1.0																		
	0.5																		
	0.0												++		-				-
	0.5																		
	-0.5																		
	-1.0		_	_	_	_	_	_		_	_	_	_	_	_	_	_	_	
																			~
		<																	>
项目采样率(Hz): 43	: 候旅	选区	的起点:			●结尾	O KI		-	音频位	责:							
48000 ~		[#]	~ 100	h 00 :	n 00.	000 s*	100 h	00 m	00.000	S*	100 1	1 00	R 00	0.00	0 5*		- 245)	1010171	nom
已停止.																			

发现其类似莫斯电码,

将音频听到的声音,按照摩斯电码的规律记录下来"---.--.--.---",用CTFCrackTools工具进 行转换得到一串字符"KEYLETUSGO"

🚳 米斯特安全团队 CTFCrakTools pro v2.1 Beta
解码方式 进制转换 插件 妹子
Crypto Image UnZip
填写所需检测的密码: (已输入字符数统计: 36)
结果:(字符数统计:10)
KEYLETUSGO https://blog.csdn.net/weixin_39934520

KEYLETUSGO 得到word密码:letusgo(小写有点坑)

打开word后:



看看 word里面有没有隐藏文字

文件--》选项---》隐藏文字的勾 勾上 出来了 steganography 上工具。。。

	₽ • <mark>₩</mark>	第二层地狱.do	CX	° × +					2	5 嘿 —	ð
) 插入 → A ⁺	页面布局 · · · · · · · · · · · · · · · · · · ·	引用 审阅		が 开发工具 ・ 会↓ きょ 田	特色功能 AaBbCcDc	् _{0 ईर्य} AaBl	AaBb(AaBbC	ÅA			
≦ A + ab	з- <u>А</u> - А				Ē文	标题 1	标题 2 标题 3 Ţ	新样式 * 文語	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□		
		K		T TAN PAR NOR R.			第二层地狱的哪	<u>Jiapiny</u> ,,,,, 『里了)			
	W N	🖂 选项									×
	a start of the start	视图	页面	显示选项							- 1
B -		编辑		启动时展开任务管 隐藏空白(B)]格(R)	⊻ i ⊻ a	选择时显示浮动工具栏(D) 键时显示浮动工具栏(G)	导航	窗格(P): E	•	
		常规与保存		垂直标尺(C)			₽幕提示(N)				- 11
		文件位置		状态栏(U) 进入页眉页脚提示	. (Q)		自用实时预览(V)				
		修订	显示	文档内容		-+		100	201201		-11
		中文版式		突出显示(H)		P *	或代码(F)	域底	纹(E): □时局云 ▼		- 11
	1	输出PDF		正文边框(X)		P -	书签(K)				- 11
	10 M	用户信息		裁剪标记(R)				71	4音块(U)		- 11
	你现在在	打印	格式	标记 空格(S)			制表符(T)				-1
	额。。。。	拼写检查		段落标记(M)			隐藏文字(I)				- 11
	三层地狱	安全性		对象位置(J)			全部(L)				
	你要用你	信任中心	功能	区选项 双击选项卡时隐藏	功能区(A)			https://b	log.csdn.net/v	eixin_3993	4520

文档文字中说这张狗是通向第三层的钥匙,所以把狗的图片复制出来进行分析。



推荐两个在线解读隐藏信息的图片:

http://www.atool.org/steganography.php

😸 audacity 📄 在线图=	👬 🛕 页面载入: 🔛 audacity_	📸 audacity_	<mark>祕 实验吧</mark> -欢	⊆ 实验吧		吧-杂 t 图)	HR X
← → ♂ ŵ	i 🔏 www.atool.org/s	steganography.pl	hp		~	题 … ☆	QI
☆ 最常访问 ◎ 系统装机大	师 () 百度 () hao123 () 淘宝	◎ 天猫 ◎ 京东	● 头条新闻	● 在线购彩	◎ 系统下载	O VPN #X10	æ () i
	ATOOL在线工具			PS / 编辑器	8 多媒体	站长工具	开发者
股	市铁一般的定律	t 約0遍! yrtzgl.c	com				
	1. 从电脑中选择一张带有隐藏	總信息的图片:[浏览 狗.	png			
	2. 输入需要解开信息的密码 (如果没有密码可	可以不填):	信息查看感	码,可以为	的空即为图片	解密不
	解密出隐藏的信息						
	图片中隐藏的信息为:key{	you are in fin	ally hell no) Mg.esdn			

http://tools.jb51.net/aideddesign/img_add_info

📓 audacity 🛛 🗃 在銀門 🗙 🛕 页面载入: 📓 4	audacity_ 📓 audacity_ 📓 实验吧-永 🧲 实验吧 📓 实验吧-杂 🦿 图片隐写》 🐼 地狱之声。 🎎 CTF题库 🎎 S
$(\leftarrow \rightarrow$ C $\hat{\mathbf{G}}$ $(\hat{0} \not \underline{\mathbf{a}} \text{ tools.jb})$	51.net/aideddesign/img_add_info 🗸 👷 🗉 🕶 🌪 🔍 搜索
☆ 最常访问 ⊕ 系统装机大师 ⊕ 百度 ⊕ hao123	◎ 海宝 ◎ 天猫 ◎ 京东 ◎ 头条新闻 ◎ 在线购彩 ◎ 系統下载 ◎ VPN 激励加速 ◎ 激励娱乐 ◎ 驱动精灵 ◎ 系统优化大师
IP地址归屋地在线查询工具	
ICO图标在线生成工具	1. 从电脑中选择一张带有隐藏信息的图片: 浏览 狗.png
CSS3 Box Shadow(阴影)效果在线调试工具	2. 输入需要解开信息的容码(如果没有容码可以不值): 信息查看率码。可以为空肌为图片解率不需要应
CSS3 Text Shadow(文本阴影)效果在线调试工具	
CSS3 Text Stroke(文本描边)和text-fill-color(文本描述	解密出隐藏的信息
CSS3 border-radius(固角)效果在线调试工具	图片中隐藏的信息为 key(you are in finally hell now)/jale glosdn.nei/weixin_39934520

密钥: key{you are in finally hell now}

根据刚才的经验,知道这个key肯定是最后一个压缩包所要用到的

			🔹 輸入密码 - 2345好压	×
			为加密的文件輸入密码 快到终点了.zip	_
ľ			******	
	← → ▼ [Z] := ▼ ■ 快到终点 ∫.zip		- 显示密码(勾选可支持中文密码输入)	
	◆ 名称	大小	□ 终当前李和应用到底有加密立件	
	(上层目录)			
	imi 地狱大门 jpg *	61.13 KB 1 KB	· 精定:://2 (3.5 跳过,18 小跳过所有加速2	(#

解压后有两个文件:



一张图片和一个txt文本信息,打开这个txt文档



通过里面的文字说明可以知道这个文档是那张图片所需要的秘钥,而文档理由提出按二进制数字,将其 8个一组进行转换ASCII码,得到"ruokouling",翻译成中文就是"弱口令",好吧,这个的意思要么这个拼 音是图片的秘钥,要么就是图片的解密需要弱口令,而需要弱口令的通常是爆破的时候,也就是说这张图 片可能隐藏了一个压缩文件,所以用kali里的binwalk工具查看

٤,	×1+(F) 納井	4(C) 尽力(V)目1日(V) 1支承(O	/ 於油(1) 刊刊(二)	-
s	root@kali: 公共 模板 snakroot@kali:	#ls 视频 图片 文档 #cd 桌面	当下载 音乐 桌面	
2	root@kali:	~/桌面# ls Misc.jpg snake. ~/桌面# binwalk 地	jpg warmup.bmp 地狱大门.jpg b狱大门.jpg	
*	DECIMAL	HEXADECIMAL	DESCRIPTION	
<u> </u>	10 62584	0×0 0×F478	IPEG image data, JFIF standard 1.01 End of Zip archive	
€	root@kali:	~/桌面#		
31	地狱大门。		https://blog.csdn.net/weixin_3993452	0

把图片 地狱大门.jpg 的后缀改成 地狱大门.zip



然后打开:

事 地狱	大门.zip - 2345好历	Æ							ም ₹ - ⊑	×
二 添加	a 解压到	U H	3 19:	全 密码			中国	2345 , 压缩软件知	好任 4	
\leftrightarrow	・ 也 ≡ ・	曲地	狱大门.zip	,				当前目录查找()	支持包内查找) Q	高级
文件夹		×	+ 名称			大小	压缩后大小	类型	安全	修改
~	笔记3	^	(上层	目录)						
>			/小姐姐	i)溴.txt *		1 KB	1 KB	TXT 文件		2017
>	CTF-实验吧									

需要解密:

通过之前的解密得到的提示,需要使用弱口令,所以打开工具**Ziperello**,进行弱口令字典爆破得出密码: (需要一个好的字典)

逝去时间:00:00:00 4:27:33: 密码: [*] Passwo	当前密码长度 当前密码 当前速度 o% md*.时间: 0 s	0 信息 × ● ERE : Password 用	步輩 4 准备就场,请点击(开始) 按钮 注意: 搜索进度条 (%) 及射体时再交投显示的信息与当 前的运程效验长度相关。破解 AES 算法加密的密码可能 相时极长。
--	---	------------------------------------	---

输入密码Password,打开这个文件,发现一段说明:

问 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,你找到凯撒家族发现小姐姐被这个家族的仆人带向了地狱的另一个名 家族。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 (VTJGc2RHVmtYMT1wRG9yWjJoVFArNXcwe1NBOWJYaFZ1ekp5MnVtR1RTcDZQ2B42e1BLQ01BPTO=)。你能帮小姐姐恢复容貌吗?	门望族	,贝邦	斩

贝斯即base sixfour即64

根据文字的提示说明,知道需要用到base64解码,rabbit解码和凯撒解码,所以将里面的字符串一步步进行解码:

Base64===>字符串

Crypto Image UnZi	>	
填写所需检测的密码:(巴	输入字符数统计:76)	
/TJGc2RHVmtYMTIwRG9yW	JoVFArNXcwelNB0WJYaFZlekp5MnVt	RIRTcDZQZE42eIBLQ01BPT0=

U2FsdGVkX19pDorZ2hTP+5w0zSA9bXhVezJy2umFTSp6PdN6zPKCMA==

rabbit解码

https://www.sojson.com/encrypt_rabbit.html



fxbqrwrvnwmngrjxsrnsrnhx

凯撒解码



最终发现flag: woshinimendexiaojiejieyo

CTF{woshinimendexiaojiejieyo}

2.guess(来源:实验吧) 1.关卡描述

来源: (ゴーローゴ 建度:易 参与人数: 3203人 Get Flag: 806人 管题人数: 930人 解题通过率: 87% guess guess guess不出你就out了 flag格式:flag(xoox) 解题链接: http://ctf5.shiyanbar.com/misc/angrybird.jpg https://blog.csdn.net/weixin_399344520	 来源: (ブーの)ブ 建度:易 参与人数: 3203人 Get Flag: 806人 管題人数: 930人 解题通过率: 87% guess guess Guess不出你就のut了
guess guess不出你就out了 flag格式:flag{xxx} 解题链接: http://ctf5.shiyanbar.com/misc/angrybird.jpg	guess guess不出你就out了
解题链接: http://ctf5.shiyanbar.com/misc/angrybird.jpg	Haguar_Hag(xxx)
https://blog.csdn.net/weixin <mark>_399\$45</mark> 20	解题链接: http://ctf5.shiyanbar.com/misc/angrybird.jpg
https://blog.csdn.net/weixin <mark>_399\$45</mark> 20	
https://blog.csdn.net/weixin_399\$4520	
	https://blog.csdn.net/weixin_399\$452

分析:

这题题目就提示了guess,又在隐写术里,搜索一下,可以看到以下这一段: Neils Provos的隐写研究是基于统计分析技术的,他开发的Stegdetect程序主要用于分析JPEG文件。因此用Stegdetect可以检测到通过JSteg、JPHide、OutGuess、Invisible Secrets、F5、appendX和 Camouflage等这些隐写工具隐藏的信息。

所以这题应该是用了OutGuess隐写。

outguess.org 用于对jpeg彩色图像添加密文,和读取通过outguess添加在jpg图像中的密文。

outguess是一个图片隐写软件,可以在github上下载: <u>https://github.com/crorvick/outguess</u>,

根据说明编译使用

google找到的使用方法

下载后,在linux里cd到outguess目录下

./configure && make && make install

这样就可以使用outguess命令了。

自己输入个outguess -help就会显示其用法,

root@kal12†28:~# outg	juess -help
outguess: invalid opt	tion 'h'
OutGuess 0.2 Universa	l Stego (c) 1999-2001 Niels Provos
outquess [options] [<	input file> [<output file="">]]</output>
-[sS] <n></n>	iteration start, capital letter for 2nd dataset
-[iI] <n></n>	iteration limit
-[kK] <key></key>	key
-[dD] <name></name>	filename of dataset
-[eE]	use error correcting encoding
-p <param/>	parameter passed to destination data handler
- r	retrieve message from data
-x <n></n>	number of key derivations to be tried
- m	mark pixels that have been modified
-t	collect statistic information
- F [+ -]	turns statistical steganalysis foiling on/off. The default is on.

-r retrieve message from data

所以解答本题,只需要在angrybird.jpg所在目录下运行下面语句即可:

outguess -r angrybird.jpg outfile.txt

或者:

Kail终端命令输入git clone <u>https://github.com/crorvick/outguess</u>

安装包随即下载到文件夹。双击打开文件夹,右键点击空白区域选终端打开。(<mark>或者</mark>切换到outguess目录 下)

随后输入以下命令./configure && make && make install 进行安装

```
root@kali:~# git clone https://github.com/crorvick/outguess
Cloning into 'outguess'...
remote: Enumerating objects: 217, done.
remote: Total 217 (delta 0), reused 0 (delta 0), pack-reused 217
Receiving objects: 100% (217/217), 535.91 KiB | 67.00 KiB/s, done.
Resolving deltas: 100% (72/72), done.
root@kali:~#
```



输入命令outguess -help 即可获得使用格式如下图

```
kali:~/outguess# outguess -help
outguess: invalid option -- 'h'
OutGuess 0.2 Universal Stego (c) 1999-2001 Niels Provos
        -[sS] <n> iteration start, capital letter for 2nd dataset
-[iI] <n> iteration limit
outguess [options] [<input file> [<output file>]]
        -[kK] <key> key
        -[dD] <name> filename of dataset
        -[eE] use error correcting encoding
        -p <param> parameter passed to destination data handler
       - r
                  retrieve message from data
                     number of key derivations to be tried
        -x <n>
                     mark pixels that have been modified
                     collect statistic information
        -F[+-]
                     turns statistical steganalysis foiling on/off.
                     The default is on https://blog.csdn.net/weixin_39934520
 ot@kali:~/outguess#
```

把图片放到根目录下:



对图片信息进行破解的命令如下: outguess -r /root/angrybird.jpg -t 123.txt

```
root@kali:~/outguess# outguess -r /root/angrybird.jpg -t 123.txt
Reading /root/angrybird.jpg....
Extracting usable bits: 36252 bits
Steg retrieve: seed: 152, len: 14
root@kali:~/outguess#
```

解密信息如下:



flag{0ut_Gas}



创作打卡挑战赛 赢取流量/现金/CSDN周边激励大奖