CTF MP3音频隐写



 GunnerXiang
 ● ± 2019-02-10 02:53:20 发布
 ● 6728 ◆ 收藏 8

 分类专栏:
 CTF 文章标签:
 MISC CTF 隐写

 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/qq_41620646/article/details/86860656

版权

CTF 专栏收录该内容

1 篇文章 0 订阅 订阅专栏 最近作为新人(=菜鸡)参加杭电vidar的hgame寒假ctf培训,碰到一道音频隐写题。

描述

一首MP3,好好听哦,flag由大写英文字母、数字以及下划线组成,记得添加hgame{} URL http://plir4axuz.bkt.clouddn.com/hgame2019/a80509c91f30027ca21b069e7d94fa7718ab2e40684628c41943bf647f3d7c6a/stego.mp3

打开url,发现是一个mp3文件:

i plir4axuz.bkt.clouddn.com/hgame2019/a80509c91f30027ca21b069e7d94fa7718ab2e40684628c41943bf647f3d7c0	驟 … ☆	$\overline{\mathbf{A}}$
▶ ●	— 0:00 / 0:49	(*)•
	https://blog.	csdn.net/qq_41620646

将其下载到本地。然后百度ctf mp3相关内容,下载工具MP3stego,并将下载来的音频文件放到MP3stego的文件目录下。然后 以txt文件格式打开下载来的mp3文件,在最后发现:

🥘 stego - 记事本	_		×
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)			
E瞀驢窃罒 連?海?! □2□kR冈嶠媃 麙?€□□5??G ぁ攻Ζ懭槲	吳岯	J觾窊珇	痪1 ^
изүн∞ лппип+аело, «иза, тын, ойпоолпешастать не ▲+поти	□ 680 ∩		

此明Ⅰ빅贝,(凵凵Ⅰ凵┘目�ノィℿ吲□☆Ⅲᠺ忉町∖ィ物□ムィ∩凵╹顎Ū捾尼族ル♥Ψ凵衂フС凵ノ╚U∩∖ィィ凵 坒,???x?9 牠穠?c?姳?湊PZ籎UC蟧wP1)甤v荇裐龌?. 揣鏰揌x?a鑲洫Z牏(?{箮u嗅?惴\$ E?嘒楶??Xa□□□□U:]?J\$€hYh{0Tq??o□??Y蝹9鞹6嵫?F襍N璨訪 ?=?qo□c?W&g?E? 蟄)壅5枈?p僇闈\$t□[聀z!QF蠢璨?崨o問?鶮 € □舃鏚 ? î ? î □ 夾 崶 ? H # 懁 」 菀 cf]XeV裴慖諵□C婮d嘡D衼□p?jL?菶v□□/鄜d螯瑡D□?]凲?{40-M□匔?幀xt8L#鐖 1□□?1藪懸□□儕7□□8?T?层資♠f%1?寅うjt 继?} 荡?岰9 PB 穴:逞菪瘟☆*H负c シu9篷;V曐5彆鞌0MN妳□顟H護,?? ?□\婭驸?蔣E糷p□(8?磚d?姅屵!e×恠Xcb??鰗5 豍q"??!□0z8y銒□#□((bp+f巖□?□□C褪?碅?婿?dh丕* 忍O郦Xa□?xs奀??\$H 諚□堸□- g疻c鏥t軹坠虴竬砕麫X?}&玵 b\$矆?(躊? 铼?燥s1PY獭]=?0?觡 v?0禹 麙?€□??-??懁ス澆L\惛鯄7嵁? 陵*虚?蕴袻?□□?h □悸□□缆□dJ□ ₩+廬 濉 臫R6裊U)??7裁&?速%?gQ?.碳5♠惫壬銿 紕 犢f皂7;?T嗑6鯏ゃ\$?燉I?6客侬□%?□R 鳎☉,怠Y#艉飻□?3?箂grP呾蹃?铐J湶t唑?鮈?镮0a錝渗畀c^玊碮汋騎詆□?L跰b谙g3鏜 寐鯒m?c?-丂-4瓸□㖞[^]□□梽桃 □P□r?麙?€□?5談 □2?w″p□m踜m[^]F?:)
 □壩z″ 幞焠鱬倖P牕?E傽?\]?蟰 ?□♠qAD?? 金擷v?□僺飾b□?d□庘倐?繺?□ □ □P□r?麙?€□?5談 □2?w″p□m踜m~F?: 兏謦 p?&衆?Q*]□泟M□ ?7□□<€n煝G饒浕 . 飄..}牋 □镍JqAD梥?细遛□峡邍{炕蒿 · 彅瘎□1?□囙0□□□□□伬鄍8□□鑎鸨犲孭□ c1z9KYy??□□併諤 欌,uVyaK□? .MA?' 辩?(豹1T″□K ?`?□剶j54j5氟□y??□□金?'□砾}M ┝F鉺 玲□□?1 |tjs殼u A粒□?%1?□K□C 姑b隳愱# 3\耾榓缦y?鐬b瀀} 荊?R□E □□c DQ猆'□岮h鹭? passwd is 123

这个password我们马上会用到。

接下来打开cmd命令窗口, cd 进MP3stego的目录下, 输入以下指令: Decode -X stego.mp3 -P 123 其中-X参数后跟同目录下的mp3文件名, -P后面跟密码, 然后如图:

C:\Users\Administrator>cd C:\Users\Administrator\Desktop\MP3Stego C:\Users\Administrator\Desktop\MP3Stego>Decode -X stego.mp3 -P 123 MP3StegoEncoder 1.1.19 See README file for copyright info Input file = 'stego.mp3' output file = 'stego.mp3.pcm' Will attempt to extract hidden information. Output: stego.mp3.txt the bit stream file stego.mp3 is a BINARY file HDR: s=FFF, id=1, 1=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0 alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1 mode=single-ch, sblim=32, jsbd=32, ch=1 [Frame 1863]Avg slots/frame = 417.736; b/smp = 2.90; br = 127.932 kbps Decoding of "stego.mp3" is finished The decoded PCM output file name is "stego.mp3.pcm"

C:\Users\Administrator\Desktop\MP3Stego>

https://blog.csdn.net/qq_41620646

会在同目录下生成1个txt文件,打开就应该能得到flag了(嗯,我本来是这样想的)

 ■ stego.mp3 - 记事本
 □
 ×

 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

 ✓

 Maybe you think you are right, but in fact, it's wrong.
 ✓

此时



于是此方法行不通,另想出路。

想起来那个MP3文件我只听了一点,于是先把它听完。发现前面是歌声,后面却是"滴滴滴"的声音,猜想可能是摩尔斯电码。于 是百度相关信息,下载工具Autacity,打开mp3文件:

文件(F) 编	辑(E) 视图	图(V) 攝录(R) 制	h道(T) 生成(G) 效	果(C) 分析(A) 素	8助(H)							
(m)	1			I 🛃 🖉 🎝	♀左 右 -57-54-51	48 -45 -42 -39 -3 点击开	始监视 4 -21 -18 -15	5-12-9-6-3-0	10左 -57-54-5	-48 -45 -42 -39 <mark>-</mark> 36 -3	3 - 30 - 27 - 24 - 21 - 18 -	15 -12 -9 -6 -3 0
\odot	9		00	<u> + + </u>	<u> </u>	• •		- 🖦 🧠 Hut vHu	n a 🙆	P P P P		<u></u>
MME	MME V 多表現 (Realtek High Defin V 2 (立体声) 录制 V 4) 扬声器 (Realtek High Defin V											
18.0		18.5	19.0	19.5	20.0	20.5	21.0	21.5	22.0	22.5	23.0	23.5
× stego 单吉道,441	▼ 1.0											
32位浮点	0.9											
	接 0.8・											
= 0	2 0.0											
	0.0											
	0.5											
	0.3											
	0.2											
	0.1-	-	-									
	0.0-		A CONTRACTOR OF THE OWNER OF THE									
	-0.1	and the second second										
	-0.2											
	-0.3											
	-0.4											
	-0.5-											
	-0.6											
	-0.7											
	-0.8											
	-0.9											g.csdn.net/qq_41620646

前面的应该是歌声,后面的就是摩尔斯电码了。那些窄一点的就代表摩尔斯电码中的...而宽的就代表摩尔斯电码中的_,长的

· · ⁻ · · · · · · · · · · · · · · · · · · ·	F L A
· 	: 1 T
· · · · · · · · · · · · · · · · · · ·	J U 5 T
····	4



间隔将2个字符分开。于是查表,写出对应的字符:

其中,并没有在表中找到...--- 代表的字符,又因为flag包含大写字母,数字,下划线,所以猜想应该是下划线。于是最后的 flag就应该是: hgame{1T_JU5T_4_EASY_WAV}。提交,发现正确。本题完。