

【T-Star赛事笔记】腾讯安全应急响应中心

(TSRC) +WriteUp赛题四+比赛评价+小彩蛋--by wjl110

原创

爬虫数据分析师



已于 2022-04-26 21:10:51 修改



158



收藏

分类专栏: [ctf 学习笔记](#) [渗透笔记](#) 文章标签: [web安全](#) [网络安全](#)

于 2022-04-26 21:00:46 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-NC-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_37092496/article/details/124436910

版权



[ctf 同时被 3 个专栏收录](#)

1 篇文章 0 订阅

订阅专栏



[学习笔记](#)

12 篇文章 0 订阅

订阅专栏



[渗透笔记](#)

7 篇文章 0 订阅

订阅专栏

文章在腾讯云+社区同步上线

前言:

(.▽.) / ^ hello, 不出意外,各位小伙伴已经完成了这次的T-Star赛事,不知道各位心情如何(我反正觉得比赛很nice),体验不错,就像是周末跟小伙伴去玩儿密室逃脱一样,惊险刺激哈哈哈哈哈,下面□是我在解第四题的思路和方法,提供给各位小伙伴参考,最近在练听力,所以摩斯密码纯考听滴~哈哈哈哈哈,听说还有别的小伙伴用在线音频文件解密的方式也是可以滴,方便快捷~, let's go~~~

0x01赛题描述

赛题描述

人去楼空

终于成功解开了门禁！进入了紧闭的房间，这里似乎曾经是一个总部实验室，然而此刻已是人去楼空，房间里空荡荡的，一个人都没有。

看来，不管这里曾经是谁在这里，房间里的秘密都已经随着主人一起离开了。

突然，一股刺耳的闹钟铃声划破寂静——

竟然有人在这里留了一部手机？难道说，你的一举一动都在人的意料之中？

铃声不知疲倦地响着，似乎笃定了你会接。

你拿起了手机。

这里面有什么信息吗？

<http://175.178.148.197/b378603d0266d73e743c8d05f5bc3ebe.zip>

提示：需要修复二维码与压缩包，分析出压缩包密码，答案为解压后的TXT内容

提交结果

当前赛题今日已提交0/5次

请输入赛题答案

CSDN @爬虫数据

跳转下载zip

<http://175.178.148.197/b378603d0266d73e743c8d05f5bc3ebe.zip>

提示

需要修复二维码与压缩包，分析出压缩包密码，答案为解压后的TXT内容

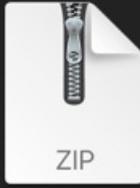
0x02解压缩zip包

解压缩zip包后，得到两个文件，第一个是二维码，第二个是压缩包zip

返回/前进 破镜重圆 2



残缺的二维码.jpg
500×500



我真是一个压缩包.zip
109 KB

CSDN @爬虫数据

修复第一个二维码文件

我在此是将其截图放置于WPS的word文档内

分析可以知道二维码构造由三个（左上、左下、右上）相同部分组成，此图缺失左上角部分。

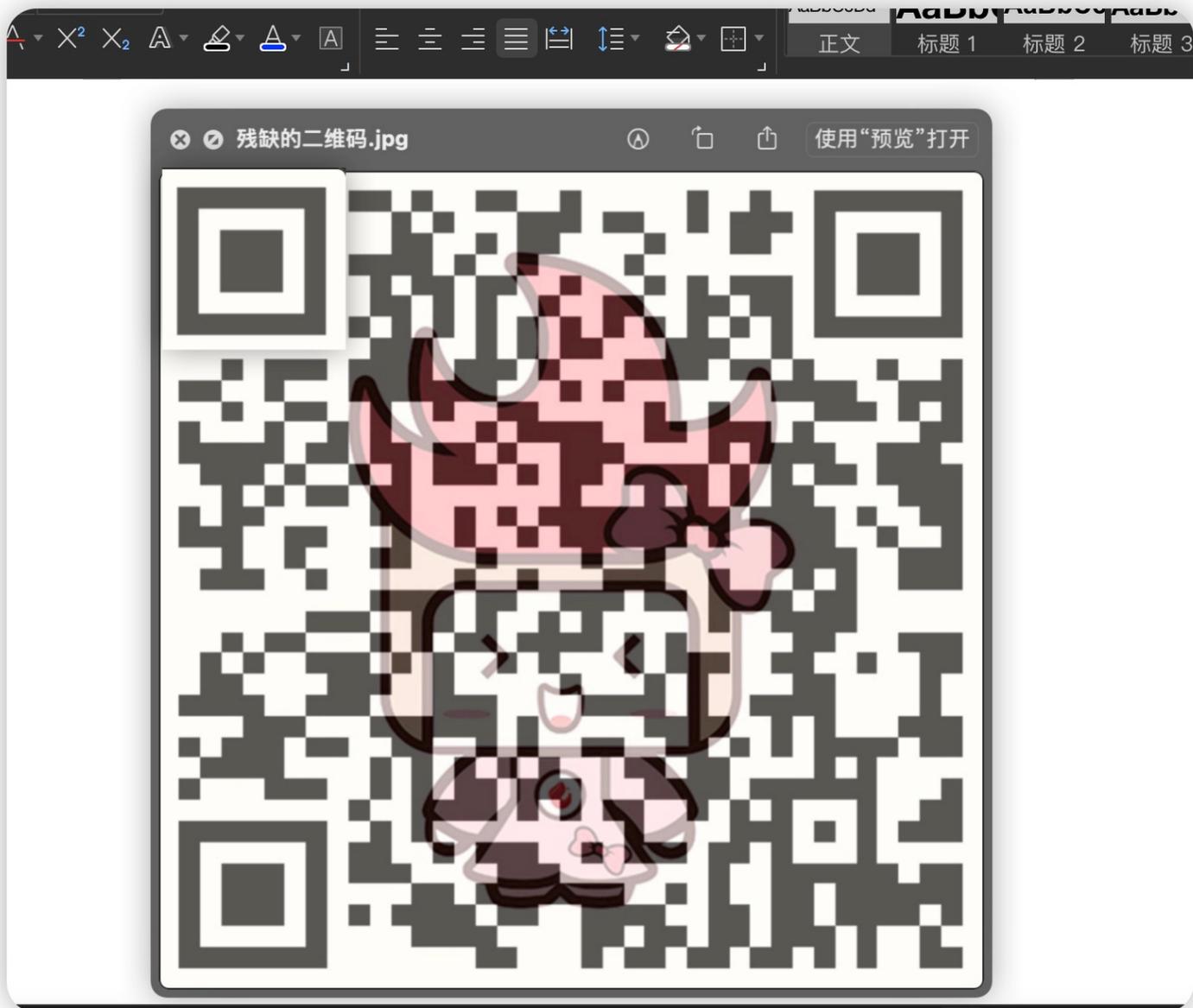
将右上角截取出来，拼凑到左上，如下图所示。

截取右上角



CSDN @爬虫数据

拼凑左上角



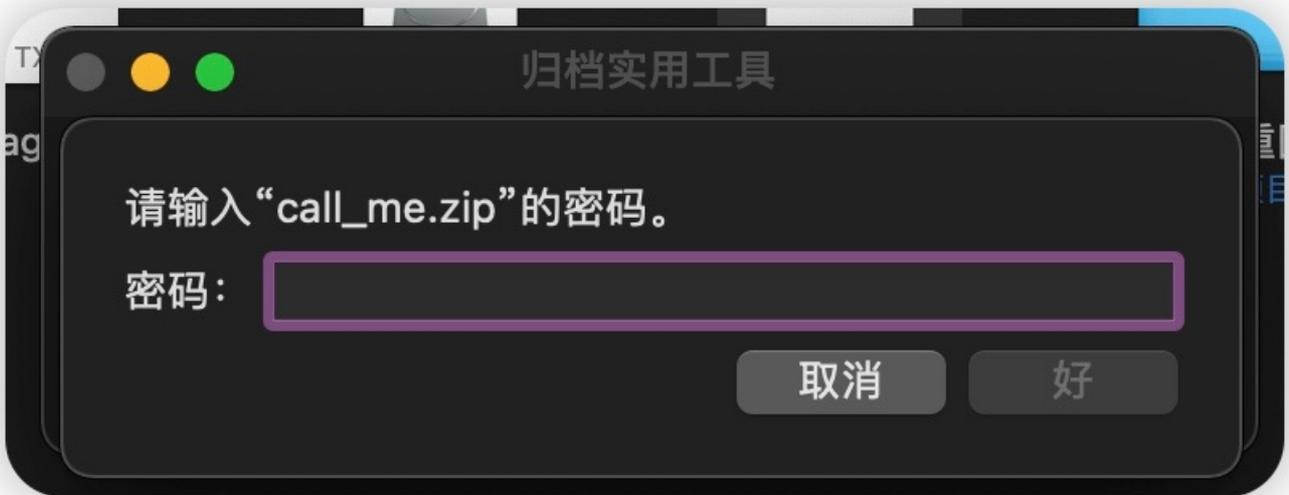
CSDN @爬虫数据

扫描二维码后得到一个zip文件



CSDN @爬虫数据

打开需要解压密码



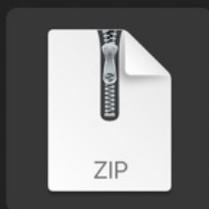
CSDN @爬虫数据

此时将思路转到第二个“破镜重圆”压缩包

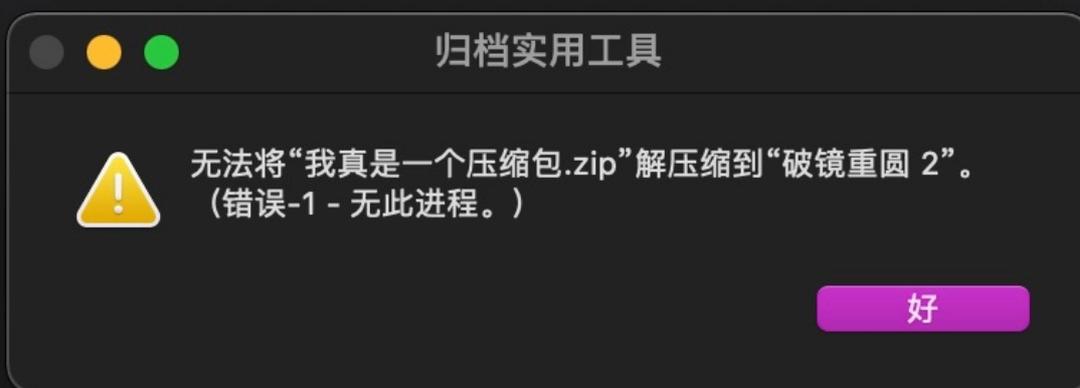
0x03解压缩zip包



残缺的二维码.jpg
500×500



我真是一个压缩包.zip
109 KB



解压报错，将其用VScode自带的hex editor编辑器打开zip文件查看hex编码并分析原因

Tips:

压缩文件头数据区hex

50 4B 03 04: 这是头文件标记为zip文件

14 00: 解压文件所需 pkware 版本

00 00: 全局方式位标记 (有无加密) 头文件标记后2bytes

08 00: 压缩方式

5A 7E: 最后修改文件时间

F7 46: 最后修改文件日期

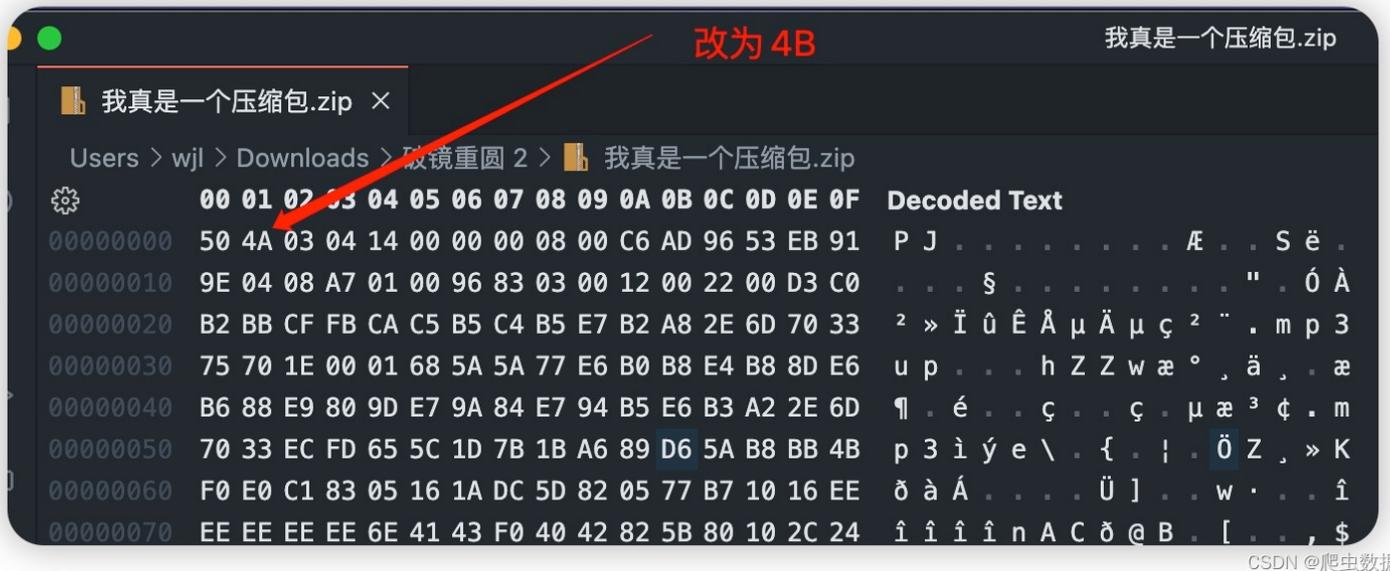
16 B5 80 14: CRC-32校验 (1480B516)

19 00 00 00: 压缩后尺寸 (25)

17 00 00 00: 未压缩尺寸 (23)

07 00: 文件名长度

00 00: 扩展记录长度



分析可知第二位错误，将其更改为4B，然后保存，解压缩zip包，得到一个.mp3文件



CSDN @爬虫数据

0x04对.mp3文件进行分析

播放后发现是一段摩斯密码

对比摩斯密码对照图表可以将其内容复现出来

1{- - - - -}	A{-}滴答	B{----}答滴滴滴
2{- - - - -}	C{----}答滴答滴	D{-}答滴滴
3{- - - - -}	E{-}滴	F{- - -}滴滴答滴
4{- - - - -}	G{- - -}答答滴	H{----}滴滴滴滴
5{- - - - -}	I{-}滴	J{- - - -}滴答答答
6{- - - - -}	K{----}答滴答	L{- - -}滴答滴滴
7{- - - - -}	M{- -}答答	N{- -}答滴
8{- - - - -}	O{- - -}答答答	P{- - -}滴答答滴
9{- - - - -}	Q{----}答答滴答	R{- - -}滴答滴
0{- - - - -}	S{---}滴滴滴	T{-}答
	U{- - -}滴滴答	V{---}滴滴滴答
	W{- - -}滴答答	X{----}答滴滴答
	Y{----}答滴答答	Z{- - -}答答滴滴

--===== 1

===== 9

===== 9

--===== 1

===== 0

---=== 3

====--8

====-6

====-7

====- 9

====-7

19910386797



得到密码19910386797

0x05解压后得到flag

将得到的密码输入得到flag.txt文件



CSDN @爬虫数据

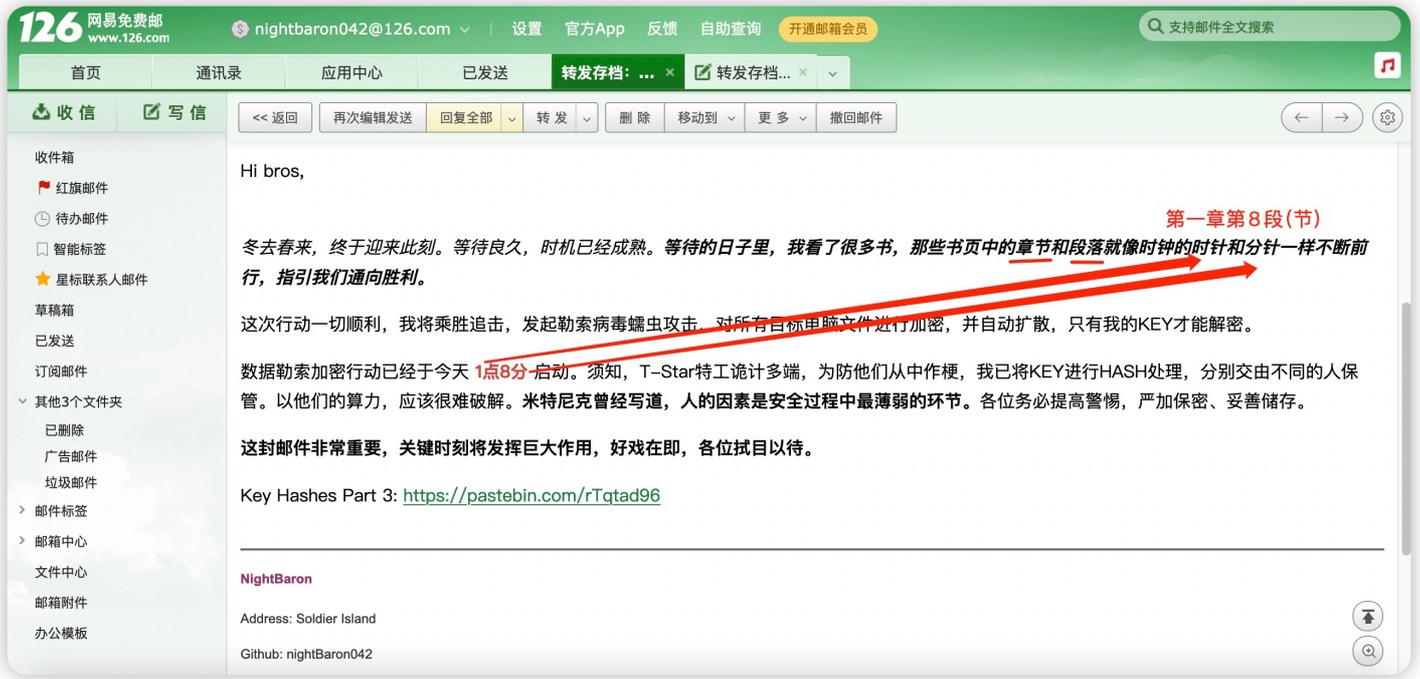


CSDN @爬虫数据

flag:

<https://darknet.hacker5t2ohub.com/>

比赛小彩蛋:



书名:《反欺骗的艺术: 世界传奇黑客的经历分享》



夜男爵042

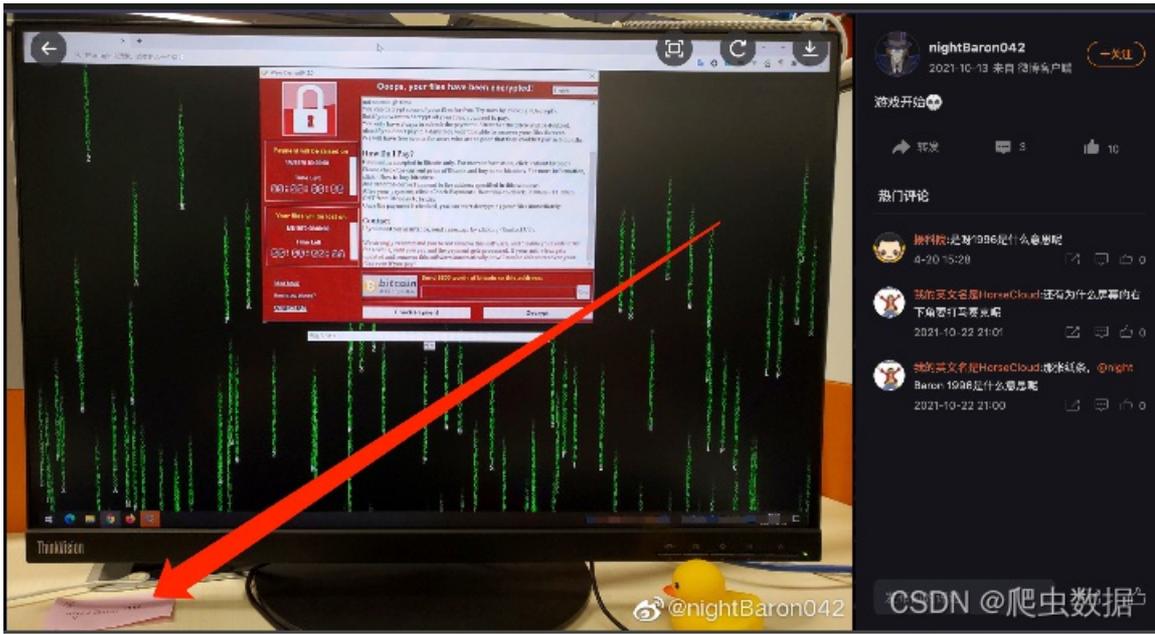
跟随

微博: nightBaron042

17 位关注者 · 0位 关注者

nightbaron042@126.com

阻止或报告



匿名者的微博（邮箱密码）

比赛评价：

优点：

- 1、比赛有序进行，中途未出现服务器宕机等严重问题。（除了第一个题有许多小伙伴可能不知道做法，用扫描器导致服务器拥堵以外，剩下5道题的体验很好~）
- 2、开放实时排行榜的功能，能让小伙伴们实时了解自己的答题rank情况，清楚明了~
- 3、比赛时间合适，能给小伙伴足够的时间去解题，去学习，去探索

需改进地方和一些建议：

- 1、提供一个大数据可视化屏幕，将小伙伴解题first blood，second blood等在可视屏上展出，将题目的解出人数进行统计~
- 2、比赛前提前开放服务器入口测试服务器压力和阈值（防cc攻击，ban ip等），再根据预期人数进行调整和配置优化~
- 3、关于剧情内容上，建议可以丰富一下，多用解密和蛛丝马迹探寻的方法，例如我在nightbaron042的微博，github等地方找到的彩蛋等等~

此次比赛很给力，期待主办方下一次的举办（公众号里蹲src，希望能多多举行类似比赛,主要是开心啦~）

——end