CTF-music

原创

烟涛微茫信难求 于 2021-09-29 21:08:43 发布 1099 收藏

文章标签： 网络安全 unctf

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_43611848/article/details/120555895

版权

题目描述：

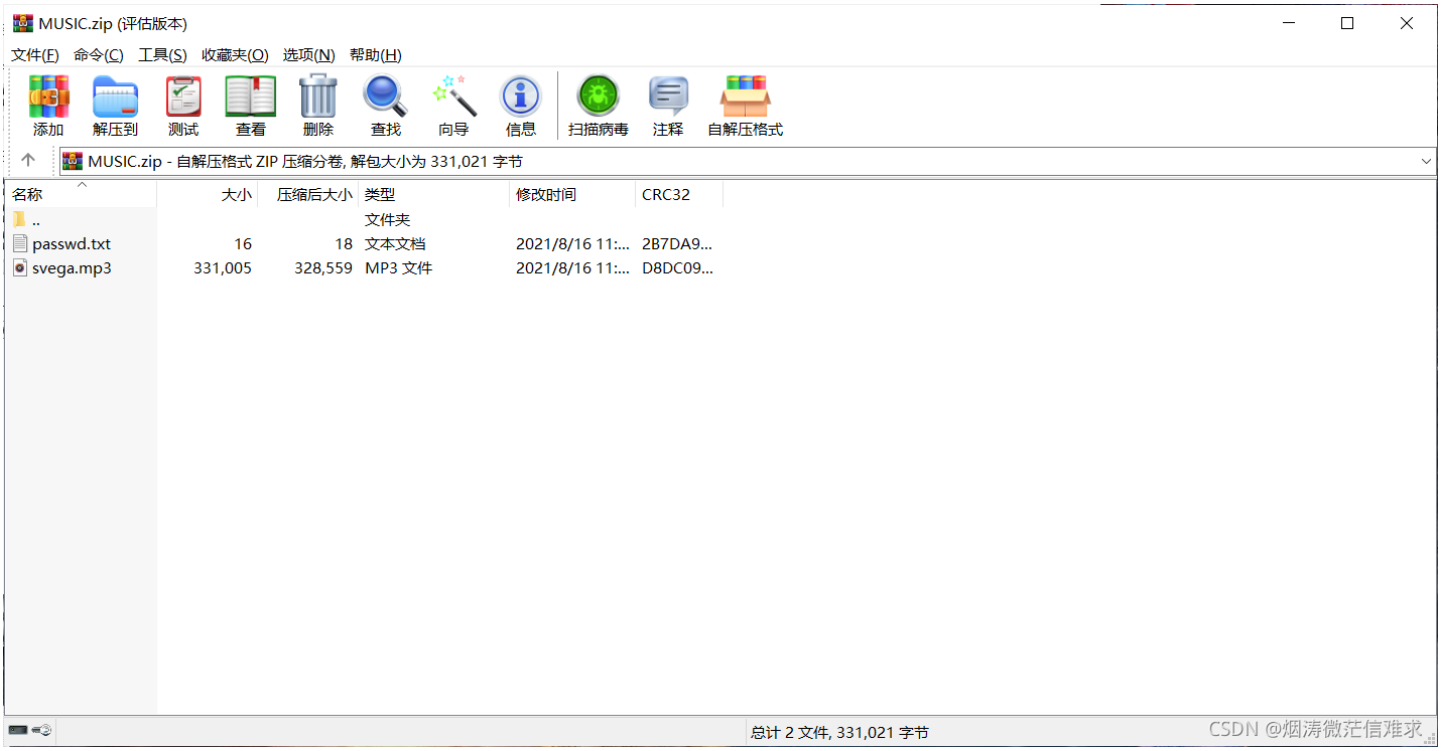
链接：https://pan.baidu.com/s/1EJ5hUHEyaC1M2WrZ2EOu8A

提取码：yln1

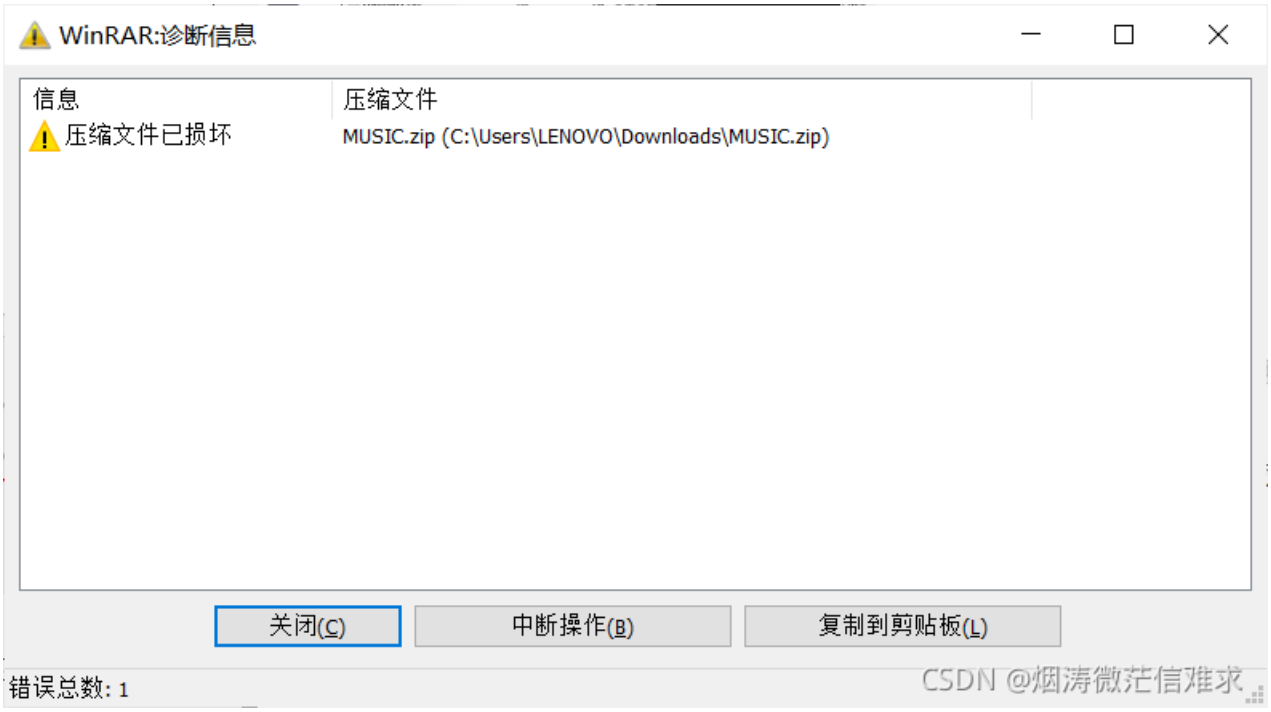
TIPS:注意告警

解题过程：

1.下载文件后尝试解压



压缩包内有两个文件，一个svega.mp3一个passwd.txt，解压时却提示错误，只有svega.mp3被解压出来。



2.用winhex打开压缩包查看文件头标志位

MUSIC.zip

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	50	4B	01	02	14	00	00	00	08	00	8E	5A	10	53	00	A9	PK ŽZ S ©
00000016	7D	2B	12	00	00	00	10	00	00	00	0A	00	00	00	70	61	}+ pa
00000032	73	73	77	64	2E	74	78	74	33	4F	4B	33	32	35	49	36	sswd.txt3OK325I6
00000048	36	B5	34	36	49	32	4A	B6	04	00	50	4B	03	04	14	00	6µ46I2J¶ PK
00000064	00	00	08	00	C7	5B	10	53	D0	09	DC	D8	6F	03	05	00	Ç[SÐ ÜØo
00000080	FD	0C	05	00	09	00	00	00	73	76	65	67	61	2E	6D	70	ý svega.mp
00000096	33	9C	FD	53	74	65	DD	F7	C6	0F	9E	D8	D6	09	2A	B6	3œýSteÝ÷Æ žØÖ *¶
00000112	ED	54	6C	DB	B6	ED	8A	6D	DB	B6	6D	DB	76	52	71	C5	íTlÛ¶íŠmÛ¶mÛvRqÅ
00000128	95	8A	DD	6F	BE	BF	7F	8F	D1	17	7D	D3	BD	AF	CF	39	•ŠÝo¾¿ Ñ }Ó½¯Ï9
00000144	63	CD	F3	59	73	CD	67	CD	FD	EC	B5	BF	DE	12	FB	01	cÍóYsÍgÍýìµ¿Þ û
00000160	00	0C	05	10	15	74	64	7F	38	39	09	4A	30	9C	79	10	td 89 J0œy
00000176	80	BF	87	87	F1	D0	D0	FB	4F	2E	7F	80	0F	00	F0	DB	

CSDN @烟涛微茫信难求

发现文件头标志位出错，zip文件开头应为50 4B 03 04，将01 02 改为03 04后解压。

Windows-SSD (C:) › 用户 › LENOVO › 下载 › MUSIC

名称	#	标题	参与创作的艺术家	唱
passwd.txt				
svega.mp3				

成功解压出两个文件

3.查看passwd.txt

passwd.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
7ff254c35934b2c9
```

一个mp3文件，一个密码，上网查询得知有一个工具叫MP3Stego，可以将txt文件隐写到mp3文件中，并可以设置密码，接受者可再利用此工具，通过密码将txt文件分离出。

4.下载MP3Stego工具并根据教程尝试解压。

```
C:\Users\LENOVO\Desktop\tools\MP3Stego_1_1_16\Development\MP3Stego>Decode.exe -X svega.mp3 -P 7ff254c35934b2c9
MP3StegoEncoder 1.1.16
See README file for copyright info
Input file = 'svega.mp3'  output file = 'svega.mp3.pcm'
Will attempt to extract hidden information. Output: svega.mp3.txt
the bit stream file svega.mp3 is a BINARY file
HDR: s=FFF, id=1, l=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  791]Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
[ERROR]Encrypt: unexpected end of cipher message.
```

CSDN @烟涛微茫信难求

并未解压出txt文件来，应该是密码错了

5.把passwd.txt里的密码用MD5解密得出新密码

解密的结果为"qwerasdfzxcv"!

用新密码重新分离

```
C:\Users\LENOVO\Desktop\tools\MP3Stego_1_1_16\Development\MP3Stego>Decode.exe -X svega.mp3 -P qwerasdfzxcv
MP3StegoEncoder 1.1.16
See README file for copyright info
Input file = 'svega.mp3'  output file = 'svega.mp3.pcm'
Will attempt to extract hidden information. Output: svega.mp3.txt
the bit stream file svega.mp3 is a BINARY file
HDR: s=FFF, id=1, l=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  791]Avg slots/frame = 417.434; b/smp = 2.90; br = 127.839 kbps
Decoding of "svega.mp3" is finished
The decoded PCM output file name is "svega.mp3.pcm"
```

CSDN @烟涛微茫信难求

成功分离出svega.mp3.txt文件，得到flag