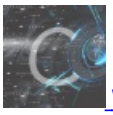
“百度杯”CTF比赛 十二月场 - misc3-枯竭

原创

Daren_f0 于 2021-01-14 13:34:41 发布 74 收藏

分类专栏： Writeups # Misc

本文链接：https://blog.csdn.net/qq_34423381/article/details/112602999


Writeups 同时被 2 个专栏收录

37 篇文章 0 订阅

订阅专栏


Misc

35 篇文章 0 订阅

订阅专栏

题目内容：

讲真的，才华已经枯竭

大家好好答题

也许这道题一点都不坑

也许。。。。。

附件下载

解题思路

```
oot@kali:~/Desktop# file misc3_BDAE109BD7B51BF98BA9BB501C0F45C2-2.zip
isc3_BDAE109BD7B51BF98BA9BB501C0F45C2-2.zip: Zip archive data, made by v6.3, extract using at least v1.0, last
modified Sun Feb 15 05:52:17 2009, uncompressed size 42, method=store
oot@kali:~/Desktop# binwalk misc3_BDAE109BD7B51BF98BA9BB501C0F45C2-2.zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
4             0x4             Zip archive data, encrypted at least v1.0 to extract, compressed size: 54, uncomp
ressed size: 42, name: misc3.txt
188           0xBC            End of Zip archive, footer length: 22
```


确定文件类型，以及有文件加密

打开 `010` 查看是否是伪加密

Startup misc3_BDAE109BD7B51BF98BA9BB501C0F45C2.zip

Edit As: Hex Run Script Run Template: ZIPTemplate.bt

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	50	4B	03	04	0A	00	01	08	00	00	91	AD	97	49	70	90	PK.....Ip.
0010h:	16	EC	36	00	00	00	2A	00	00	00	09	00	00	00	6D	69	..6...*.....mi
0020h:	73	63	33	2E	74	78	74	F6	13	72	C8	FE	8A	4B	6E	5B	sc3.txt..r...Kn[
0030h:	10	B2	F5	F2	EE	9C	1A	9D	2D	40	E3	1F	63	F5	70	B0	....-@..c.p.
0040h:	32	EA	AE	8C	F3	E4	51	E5	75	60	FB	86	52	16	53	F1	2.....Q.u`..R.S.
0050h:	32	C5	D8	0C	E5	40	D6	7F	67	AD	1E	76	44	50	4B	01	2....@..g..vDPK.
0060h:	02	3F	00	0A	00	01	08	00	00	91	AD	97	49	70	90	16	.?.....Ip..
0070h:	EC	36	00	00	00	2A	00	00	00	09	00	24	00	00	00	00	.6...*.....$....

```
0080h: 00 00 00 20 00 00 00 04 00 00 00 6D 69 73 63 33  ... .......misc3
0090h: 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00 18 00  .txt.. .........
00A0h: 8C C0 71 B1 22 5D D2 01 DB 5A D9 4A 1F 5D D2 01  ..q."]...Z.J.]..
00B0h: DB 5A D9 4A 1F 5D D2 01 50 4B 05 06 00 00 00 00  .Z.J.]..PK......
00C0h: 01 00 01 00 5B 00 00 00 61 00 00 00 00 00        ....[...a.....
```

Template Results - ZIPTemplate.bt

Name	Value	Start	Size	Color
struct ZIPDIRENTRY dirEntry	misc3.txt	5Dh	5Bh	Fg: Bg:
char deSignature[4]	PK	5Dh	4h	Fg: Bg:
ushort deVersionMadeBy	63	61h	2h	Fg: Bg:
ushort deVersionToExtract	10	63h	2h	Fg: Bg:
ushort deFlags	2049	65h	2h	Fg: Bg:
enum COMPTYPE deCompression	COMP_STORED (0)	67h	2h	Fg: Bg:
DOSTIME deFileTime	21:44:34	69h	2h	Fg: Bg:

到这里已经没有任何想法，一点意思也没有了呀

撑不住了，找 `writeup` 看完之后懵逼了，原来是脑洞爆破，我佛了

参考资料：

“百度杯”CTF比赛 十二月场misc3-枯竭