CTF-MISC-ZIP伪加密

原创

哈哈哈神经病啊 于 2021-09-17 15:06:23 发布 836 收藏 1

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/qq_37387187/article/details/120348908

一个zip文件由三部分组成：压缩源文件数据区+压缩源文件目录区+压缩源文件目录结束标志。

例子：

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	50	4B	03	04	14	00	01	00	08	00	5A	7E	F7	46	16	B5
00000010	80	14	19	00	00	00	17	00	00	00	07	00	00	00	6B	65
00000020	79	2E	74	78	74	0B	CE	CC	75	0E	71	AB	CE	48	CD	C9
00000030	C9	57	28	CE	CC	2D	C8	49	AD	28	4D	AD	05	00	50	4B
00000040	01	02	3F	00	14	00	09	00	08	00	5A	7E	F7	46	16	B5
00000050	80	14	19	00	00	00	17	00	00	00	07	00	24	00	00	00
00000060	00	00	00	00	20	00	00	00	00	00	00	00	6B	65	79	2E
00000070	74	78	74	0A	00	20	00	00	00	00	00	01	00	18	00	65
00000080	58	F0	4A	1C	C5	D0	01	BD	EB	DD	3B	1C	C5	D0	01	BD
00000090	EB	DD	3B	1C	C5	D0	01	50	4B	05	06	00	00	00	00	01
000000A0	00	01	00	59	00	00	00	3E	00	00	00	00	00			

压缩源文件数据区：

50 4B 03 04：这是头文件标记（0x04034b50）

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

…

压缩源文件目录区：

50 4B 01 02：目录中文件文件头标记(0x02014b50)

3F 00：压缩使用的 pkware 版本

14 00：解压文件所需 pkware 版本

00 00：全局方式位标记（有无加密，伪加密的关键） 目录文件标记后4bytes

…

压缩源文件目录结束标志：

50 4B 05 06：目录结束标记

00 00：当前磁盘编号

00 00：目录区开始磁盘编号

01 00：本磁盘上纪录总数

01 00：目录区中纪录总数

59 00 00 00：目录区尺寸大小

3E 00 00 00：目录区对第一张磁盘的偏移量

00 00：ZIP 文件注释长度

ctf伪加密：

一般只需要关注前面两个部分，将文件拖入winhex中，找到第二个50 4B （蓝色部分），修改全局方式位标记第一个字节为00（蓝色部分，09改为00），保存即可。

如第一个50 4B后的全局方式位标记第一个字节不为00（黄色部分），需将其改成00