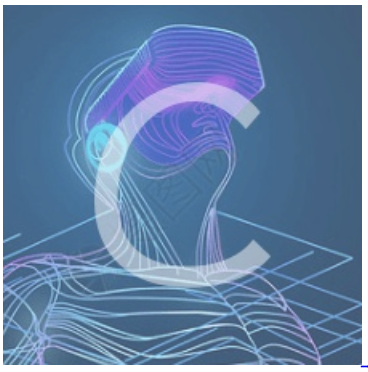
CTF misc zip、rar文件伪加密

原创

H4ppyD0g 于 2019-09-12 08:26:42 发布 1980 收藏 6

分类专栏： CTF 文章标签： 其他

本文链接：https://blog.csdn.net/weixin_42172261/article/details/100760375



zip伪加密

zip伪加密是在文件头的加密标志位做修改，进而再打开文件时识被别为加密压缩包。但实际是没有密码的，所以使用任何密码都破解不了。

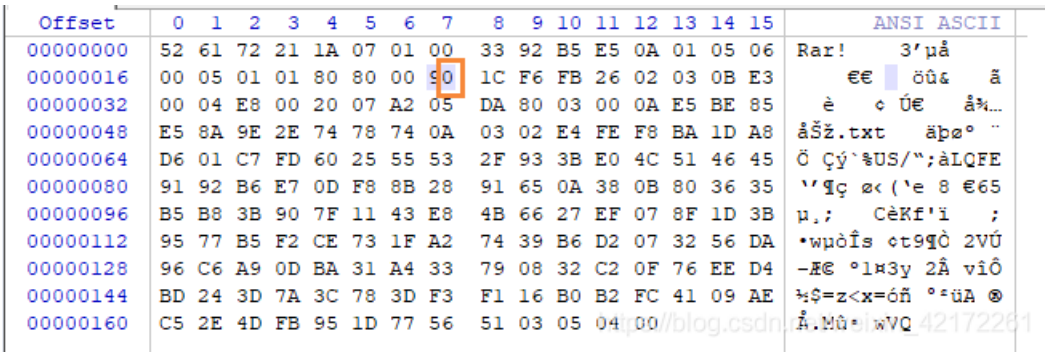
一个 zip文件由三个部分组成：

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

当压缩源文件**目录区**的全局方位标记为0900(表示为加密)，

并且压缩文件**数据区**的全局方式位标记为0000(未加密)则会被识别为加密，但是文件并没有真正的加密，也就是所说的伪加密。

rar文件伪加密



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	52	61	72	21	1A	07	01	00	33	92	B5	E5	0A	01	05	06	Rar! 3’µå
00000016	00	05	01	01	80	80	00	90	1C	F6	FB	26	02	03	0B	E3	€€ öû& ã
00000032	00	04	E8	00	20	07	A2	05	DA	80	03	00	0A	E5	BE	85	è ¢ Ú€ å¾…
00000048	E5	8A	9E	2E	74	78	74	0A	03	02	E4	FE	F8	BA	1D	A8	åŠž.txt äþø° ¨
00000064	D6	01	C7	FD	60	25	55	53	2F	93	3B	E0	4C	51	46	45	Ö Çý`%US/“;àLQFE
00000080	91	92	B6	E7	0D	F8	8B	28	91	65	0A	38	0B	80	36	35	‘’¶ç ø‹(‘e 8 €65
00000096	B5	B8	3B	90	7F	11	43	E8	4B	66	27	EF	07	8F	1D	3B	µ¸; CèKf'ï ;
00000112	95	77	B5	F2	CE	73	1F	A2	74	39	B6	D2	07	32	56	DA	•wµòÎs ¢t9¶Ò 2VÚ
00000128	96	C6	A9	0D	BA	31	A4	33	79	08	32	C2	0F	76	EE	D4	–Æ© º1¤3y 2Â vîÔ
00000144	BD	24	3D	7A	3C	78	3D	F3	F1	16	B0	B2	FC	41	09	AE	½$=z<x=óñ °²üA ®
00000160	C5	2E	4D	FB	95	1D	77	56	51	03	05	04	00				Å.Mû• wVQ

找到第24个字节，该字节尾数为4表示加密，0表示无加密，将尾数改为0即可破解伪加密。