

buuctf-misc-九连环

原创

~Venus 于 2021-07-17 22:13:03 发布 136 收藏

分类专栏: [misc](#)

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/weixin_46079186/article/details/118863196

版权



[misc](#) 专栏收录该内容

38 篇文章 1 订阅

订阅专栏

1. 下载文件是一张图片

留下了委屈的泪水



https://blog.csdn.net/weixin_46079186

2. 拿到kali 里面进行分离 使用命令binwalk -e 123456cry.jpg
得到一个zip文件, 文件是加密过的, 尝试使用123456cry 解密, 解密没成功
丢到winhex 里面发现伪加密□
把01 08 修改为00 00 保存

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI	ASCII
000070E0	03	04	0A	00	00	08	00	00	F1	52	53	4B	D3	13	C6	E0	ñ	RSKÓ Æà
000070F0	B8	00	00	00	B8	00	00	00	0B	00	00	00	61	73	64	2F	,	asd/
00007100	71	77	65	2E	7A	69	70	50	4B	03	04	0A	00	01	08	00	q	we.zipPK
00007110	00	0E	4E	53	4B	8A	C4	35	B6	22	00	00	00	16	00	00	I	NSKIA5"
00007120	00	08	00	00	00	66	6C	61	67	2E	74	78	74	A7	A0	9B	f	lag.txt\$
00007130	A6	BC	37	21	E7	B0	A7	B4	E2	22	B9	1A	43	31	BB	C4	!	47!ç°S'á"1 C1»Ä
00007140	33	37	FD	B7	17	B5	6D	A1	FC	F0	1D	10	E9	C9	56	50	3	7y· µmiüð éÉVP
00007150	4B	01	02	3F	00	0A	00	01	08	00	00	8E	4E	53	4B	8A	K	? INSKIA5"
00007160	C4	35	B6	22	00	00	00	16	00	00	00	08	00	24	00	00	ä	5"

00007170	00 00 00 00 00 20 00 00 00 00 00 00 00 00 66 6C 61	fla
00007180	67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00 18	g.txt
00007190	00 29 39 FE E9 7C 48 D3 01 D9 46 44 DC 7C 48 D3)9pé HÓ ÛFDÜ HÓ
000071A0	01 D9 46 44 DC 7C 48 D3 01 50 4B 05 06 00 00 00	ÛFDÜ HÓ PK
000071B0	00 01 00 01 00 5A 00 00 00 48 00 00 00 00 00 50	Z H P
000071C0	4B 01 02 3F 00 0A 00 00 08 00 00 AE 54 53 4B 00	K ? @TSK
000071D0	00 00 00 00 00 00 00 00 00 00 00 04 00 24 00 00	\$
000071E0	00 00 00 00 00 10 00 00 00 00 00 00 00 61 73 64	asd
000071F0	2F 0A 00 20 00 00 00 00 00 01 00 18 00 69 B8 48	/ i,H
00007200	34 83 48 D3 01 69 B8 48 34 83 48 D3 01 E9 FC 59	4IHÓ i,H4IHÓ éüY
00007210	31 83 48 D3 01 50 4B 01 02 3F 00 14 00 01 08 08	1IHÓ PK ?
00007220	00 48 4E 53 4B 8C 3A D5 7E 88 70 00 00 28 75 00	HNSKI:õ~lp (u
00007230	00 16 00 24 00 00 00 00 00 00 00 20 00 00 00 22	\$ "
00007240	00 00 00 61 73 64 2F 67 6F 6F 64 2D E5 B7 B2 E5	asd/good-â·²â
00007250	90 88 E5 B9 B6 2E 6A 70 67 0A 00 20 00 00 00 00	!â¹! .jpg
00007260	00 01 00 18 00 69 31 23 9C 7C 48 D3 01 29 AE F6	i1# HÓ)@ö
00007270	8F 82 48 D3 01 89 7E E8 D2 7C 48 D3 01 50 4B 01	IHÓ I~èÒ HÓ PK
00007280	02 3F 00 0A 00 00 08 00 00 F1 52 53 4B D3 13 C6	? ñRSKÓ Æ
00007290	E0 B8 00 00 00 B8 00 00 00 0B 00 24 00 00 00 00	à, , \$
000072A0	00 00 00 20 00 00 00 DE 70 00 00 61 73 64 2F 71	bp asd/q
000072B0	77 65 2E 7A 69 70 0A 00 20 00 00 00 00 00 01 00	we.zip
000072C0	18 00 D9 DB B7 42 81 48 D3 01 39 D5 F6 8F 82 48	ÛÛ·B HÓ 9õö IH
000072D0	D3 01 49 83 5B 0F 81 48 D3 01 50 4B 05 06 00 00	Ó I [HÓ PK
000072E0	00 00 03 00 03 00 1B 01 00 00 BF 71 00 00 00 00	¿q

https://blog.csdn.net/weixin_46079186

3. 解压之后拿到一个qwe.zip 发现又是加密文件

The screenshot shows a Windows File Explorer window for a folder named 'asd'. The address bar shows the path: < 389a0c11-d0df-4180-829a-b52... > asd. The search bar contains '搜索"asd"'. The file list is as follows:

名称	修改日期	类型	大小
good-宸插怙寒.jpg	2017/10/19 9:50	文件	30 KB
qwe.zip	2017/10/19 10:23	ZIP 压缩文件	1 KB

https://blog.csdn.net/weixin_46079186

