

【WhaleCTF逆向题】第一期不可能的使命writeup

原创

iqiqiya 于 2018-09-17 19:12:15 发布 674 收藏

分类专栏: [我的逆向之路](#) [我的CTF之路](#) [-----WhaleCTF](#) [我的CTF进阶之路](#) 文章标签: [不可能的使命](#) [不可能的使命writeup](#)

【WhaleCTF逆向题】第一期不可能的使命writeup

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/xiangshangbashaonian/article/details/82747394>

版权



[我的逆向之路](#) 同时被 3 个专栏收录

108 篇文章 10 订阅

订阅专栏



[我的CTF之路](#)

92 篇文章 5 订阅

订阅专栏



[-----WhaleCTF](#)

8 篇文章 0 订阅

订阅专栏

题目信息:



提示我们是一个dump文件 刚开始我根据经验 猜测里边可能有图片什么的东西

结果binwalk不行 自己搜索文件头也不可以

```
root@kali:~/qiqi# binwalk MissionImprobable.TEENSY31.hex
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
2660         0xA64       Windows CE image header, image start: 0x46464646, image length: 1179010630
9140         0x23B4      Windows CE image header, image start: 0x46383337, image length: 875901764
12020        0x2EF4      Windows CE image header, image start: 0x44303340, image length: 1178022960
25700        0x6464      Windows CE image header, image start: 0x46303537, image length: 927085113
```

就在里边找可疑的数据

结果找着找着 就看到了flag。。。

```

MissionImpossible.TEENSY31* x 无标题1
编辑为: Hex 运行脚本 运行模板
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
20h: 4B 68 80 10 01 25 05 FA 00 F0 03 43 4B 60 13 46 Kh€..%.ú.ð.CK`.F
30h: 98 E7 54 2A 03 D8 18 0B 6E 30 41 00 82 E7 B2 F5 ~çT*.ø..n0A.,ç²ð
40h: AA 7F 03 D8 D8 0B 77 30 41 00 7B E7 40 F2 54 51 a..øø.w0A.{çèòTQ
50h: 8A 42 03 D8 98 0C 7C 30 41 00 73 E7 FC 21 7E 20 ŠB.ø~.|0A.sçü!~
60h: 70 E7 00 BF 74 8D FF 1F 7C 8D FF 1F 7C 91 FF 1F pç.çt.ÿ.|.ÿ.|.ÿ.
70h: 90 94 FF 1F F0 B5 27 4C 26 68 D6 F8 48 41 85 B0 ."ÿ.øµ'L&h0øHA...°
80h: 07 46 00 2C 41 D0 65 68 1F 2D 1E DD 22 48 18 B9 .F.,Aðeh.-.ÿ"H.¹
90h: 4F F0 FF 30 05 B0 F0 BD 4F F4 C8 70 03 91 02 92 Oðÿ0.°ð²OðÈp.`.´
A0h: 01 93 FF F7 B9 FB 03 99 02 9A 01 9B 04 46 00 28 ."ÿ÷¹û.™.š.>.F.(
B0h: EE D0 D6 F8 48 51 25 60 00 20 60 60 05 46 C6 F8 îð0øHQ%`.``FEø
C0h: 48 41 C4 F8 88 01 C4 F8 8C 01 3F B9 AB 1C 00 20 HAÄø^..ÄøE.?¹«..
D0h: 01 35 65 60 44 F8 23 10 05 B0 F0 BD 04 EB 85 00 .5e`Dø#..°ð².ë...
E0h: 4F F0 01 0C C0 F8 88 20 D4 F8 88 61 0C FA 05 F2 Oð..Äø^ Ôø^a.ú.ò
F0h: 16 43 02 2F C4 F8 88 61 C0 F8 08 31 E6 D1 D4 F8 .C./Äø^aÄø.læÑ0ø
00h: 8C 31 1A 43 C4 F8 8C 21 E0 E7 06 F5 A6 74 C6 F8 çl.CÄøE!èç.ð!tEø
10h: 48 41 B8 E7 EC 3D 00 00 19 31 00 00 65 63 68 6F HA,çì=...l..echo
20h: 20 22 54 68 65 20 66 6C 61 67 20 69 73 20 42 49 "The flag is BI
30h: 54 43 54 46 7B 42 34 64 5F 62 61 64 5F 55 35 42 TCTF{B4d bad U5B
40h: 7D 22 00 00 65 63 68 6F 20 22 54 68 69 73 20 6D }"..echo "This m
50h: 65 73 73 61 67 65 20 77 69 6C 6C 20 73 65 6C 66 essage will self
60h: 20 64 65 73 74 72 75 63 74 20 69 6E 20 35 20 73 destruct in 5 s
70h: 65 63 6F 6E 64 73 22 00 72 6D 20 2D 72 20 2F 00 econds".rm -r /

```

没想到这么简单，其实我因该先搜索一下ASCII的。。。

```

3A10h: 48 41 B8 E7 EC 3D 00 00 19 31 00 00 65 63 68 6F HA,çì=...l..echo
3A20h: 20 22 54 68 65 20 66 6C 61 67 20 69 73 20 42 49 "The flag is BI
3A30h: 54 43 54 46 7B 42 34 64 5F 62 61 64 5F 55 35 42 TCTF{B4d bad U5B
3A40h: 7D 22 00 00 65 63 68 6F 20 22 54 68 69 73 20 6D }"..echo "This m
3A50h: 65 73 73 61 67 65 20 77 69 6C 6C 20 73 65 6C 66 essage will self
3A60h: 20 64 65 73 74 72 75 63 74 20 69 6E 20 35 20 73 destruct in 5 s
3A70h: 65 63 6F 6E 64 73 22 00 72 6D 20 2D 72 20 2F 00 econds".rm -r /
3A80h: 40 08 FE 43 40 A0 04 40 44 08 FE 43 44 A0 04 40 @.pC@ .@D.pCD .@
3A90h: 00 18 FE 43 00 C0 04 40 30 00 FE 43 30 90 04 40 ..pC.À.@0.pC0..@
3AA0h: 34 00 FE 43 34 90 04 40 1C 18 FE 43 1C C0 04 40 4.pC4..@..pC.À.@

```

查找结果

地址	值
发现 1 出现 'flag'.	
3A26h	flag

<https://blog.csdn.net/xiangshangbashaonian>

20181018今天登陆发现这道题换了 把思路写在这里了

<https://blog.csdn.net/xiangshangbashaonian/article/details/83148583>