

## 原 hackme inndy reverse rc87cipher writeup

2018年02月01日 11:14:10 charlie\_heng 阅读数 : 151

话说这题真的挺难折腾出来的

首先这个程序是有upx壳的

但是这个壳被魔改了，关键的信息都被删除了，在google搜了半天linux upx upack 都找不到什么有用的信息

有两条路，一条是修复关键信息，一条路是像windows那些程序那样手动脱壳脱下来

两条路其实都试了一下，不过最终行得通的是第二条路

这里说下第一条路，如果你们有兴趣的话，可以去试试

首先作者把0xB4~0xB7处的UPX!填充为0xff了，然后把代码段有一个copyright的声明用nop给填掉了（话说查的时候看到upx的github上有人po了rctf的-然后被upx的人吐槽copyright被改了，违反了规则hhhhh

然后去看了下github上upx的源码，源码里有一个函数 canUnpack，这里貌似是会检查文件尾的32个字节，具体的可以去看源码，然后如果想修的话，找-的upx程序，把文件尾的32个字节复制上去，然后根据报错信息来慢慢改

然后来说下第二条路

首先upx壳在解压的过程中是不会加载so的，只会一直用syscall，这里用到一个神器，radare2（用得爽

然后upx壳的规律是，最后一个syscall肯定是munmap，所以只要试一下就知道oep在哪里了

我这里写个简单的radare2脚本来找oep

对于静态链接的程序

```
1 9dcs
2 ds
```

对于动态链接的程序

```
1 15dsc
2 ds
```

这样就能找到oep，或者可以参考一下别人找oep的脚本

<https://asciinema.org/a/35005>

找到oep之后，也是按照上面链接里面的方式dump下来

dump下来之后用ida解析一波，有可能是我不会dump吧。。很多函数都没识别出来，但是无所谓，大概都能猜出来

这里的oep是\_start，所以最后那个call是\_\_libc\_start\_main，所以第一个参数，也就是rdi，就是真正的main的地址

这里大概说下程序做了什么

这个程序只实现了加密的功能

加密的过程是，首先读取8个byte随机字符

然后根据这8个byte的字符来生成sbox

之后把这8个byte写到加密文件的开头

然后每次从被加密的文件读一个字符，就用password中的一个字符来对sbox操作一波

这里有rc87和rc87.enc，于是就可以暴力dfs破出password，这里的password其实就是flag

最后给出解题的脚本



0



```

1
2 f = open('./rc87', 'rb')
3 rc87_data = f.read()
4 f.close()
5
6 f = open('./rc87.enc', 'rb')
7 rc87enc_data = f.read()
8 f.close()
9
10
11 rc87enc_random_seed = rc87enc_data[:8]
12 rc87enc_data = rc87enc_data[8:]
13
14
15 def sbbox_loop(v1, v2, sbbox):
16     for q in range(36):
17         v2 = (13 * (~v2)) & 0xff
18         v1 = (17 * (~v1)) & 0xff
19         t1 = sbbox[v1]
20         t2 = sbbox[v2]
21         sbbox[v1] = t2
22         sbbox[v2] = t1
23
24
25 def generate_sbox(seed):
26     sbbox = []
27     for i in range(256):
28         sbbox.append(i)
29
30     for i in range(8):
31         sbbox_loop(seed[i], i, sbbox)
32     return sbbox
33
34
35 rc87enc_sbox = generate_sbox(rc87enc_random_seed)
36
37 password = ""
38 password_length = 40
39
40 def get_xor_value(tsbox):
41     v9 = 0xdeadbeef
42     for w in range(256):
43         v11 = tsbox[w]
44         v9 = 821091 * v11 ^ 23159 * v9
45         v9 &= 0xffffffff
46     return v9
47
48
49
50 def find_password(pas, tsbox):
51     if len(pas) >= password_length:
52         if(pas[39]=='\n'):
53             return [pas]
54         else:
55             return []
56     possible_pas = []
57     for i in range(32,127):
58         ttsbox = [i for i in tsbox]
59         sbbox_loop(i, len(pas), ttsbox)
60         v9 = get_xor_value(ttsbox)
61         v15 = (17 * rc87_data[len(pas)]) ^ v9
62         v15 &= 0xff
63         if v15 == rc87enc_data[len(pas)]:
64             possible_pas += find_password(pas + chr(i), ttsbox)
65     return possible_pas
66

```



0



```
67
68 print(find_password('', rc87enc_sbox))
```

0

收藏

分享

## Writeup of Imageprc(reverse) in reversing.kr

做这道题.....收获是.....了解了几个WINAPI吧0x00 Program Logic首先运行程序，发现出现一个空白画板，用光标作图，再点击'Check'But...

想对作者说点什么

## Writeup of x64Lotto(reverse) in reversing.kr

120

此题风格诡异，有一种野生逆向的既视感（疯狂改跳转）不扯别的，先下载附件。... 来自：cossack9989的...

## hackme inndy reverse termvis writeup

122

这题其实还算简单 首先分析下程序，估计是读取png里面的数据，然后打印出来一张... 来自：charlie\_heng的...

## Writeup of Ransomware(reverse) in reversing.kr

249

emmmm这道题就当复习了一下常规操作吧 首先下载附件，得到 readme.txt，file，... 来自：cossack9989的...

## hackme inndy reverse mov writeup

280

MOV instruction is turing complete! mov是图灵完备的！说真的，第一次看到这... 来自：charlie\_heng的...

## 全国大学生信息安全竞赛writeup--拯救地球(reverse500)

1637

描述什么？地球要爆炸了，据说拯救地球的代码就在这个程序里。使命貌似光荣又艰... 来自：jmp esp

## 下载 XDCTF2014题目writeup

11-12

内含reverse，code部分题目，官方writeup

## 全国大学生信息安全竞赛writeup--珍贵资料(reverse200)

4004

描述你无意间得到了一些珍贵资料，可惜他们看起来不知道是什么，据说解开它可以... 来自：jmp esp

## 全国大学生信息安全竞赛writeup--暗号(reverse300)

4510

描述 George是一名FBI特工，昨天他获得了一个命令，在今天晚上纽约林肯中心的大... 来自：jmp esp

## 实验吧CTFreverse题目该题不简单writeup

167

题目链接：http://ctf5.shiyanbar.com/crack/3/ 运行 显示密钥无效 查壳无壳 ... 来自：iqiqiya的博客

文章热词 机器学习 机器学习课程 机器学习教程 深度学习视频教程 深度学习学习

## 相关热词

c++ reverse()函数 c++ 中reverse方法 c++string函数reverse c++ reverse() 库 c++ reverse头文件 python教程+


## 实验吧-reverse入门writeup


151

逆向入门笔记 第一题：是要提交hello的注册码 首先想到的是用IDA打开，使用Gra... 来自：ishandsomedo...

 **Anxiety**  
186篇文章  
排名:8000+  
[关注](#)

 **iqiqiya**  
236篇文章  
排名:千里之外  
[关注](#)

 **ishandsomedog**  
10篇文章  
排名:千里之外  
[关注](#)

 **niexinming**  
153篇文章  
排名:千里之外  
[关注](#)

## rop和rop2的题目的wp

1870

https://hackme.inndy.tw/scoreboard/ 题目很有趣，我做了rop和rop2这两个题目... 来自：一个码农的笔记