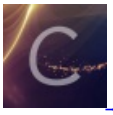
【reversing.kr逆向之旅】Easy Unpack的writeup

原创

iqiqiya 于 2018-10-31 20:08:05 发布 469 收藏
分类专栏： 我的逆向之路 ------reversing.kr 我的CTF之路 文章标签： 【reversing.kr逆向之旅】Easy Unpack的 Easy Unpack的writeup


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

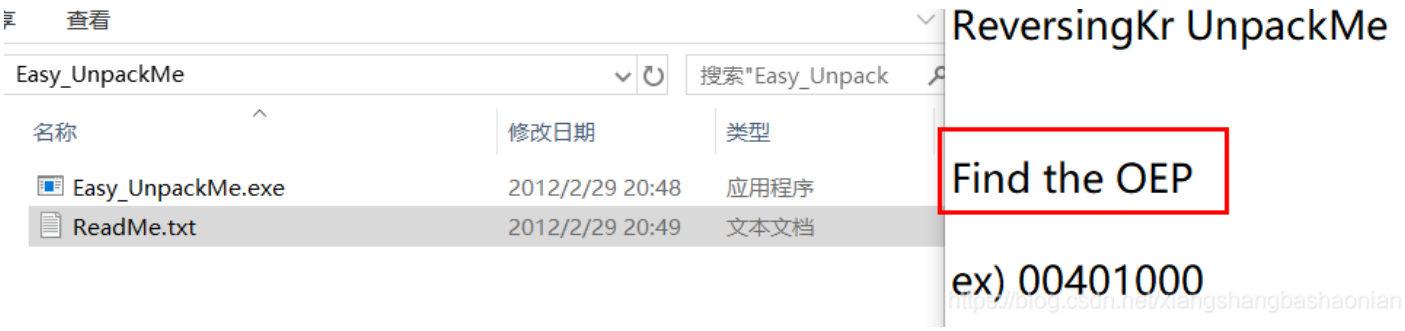

------reversing.kr
11 篇文章 0 订阅
订阅专栏


我的CTF之路
92 篇文章 5 订阅
订阅专栏

查壳工具貌似不好使啊

不过OD和IDA都提示 还有题目名字 明显告诉我们加了壳

下载的压缩包解压后可以看到ReadMe.txt 提示我们只要找到像00401000这样的OEP即可



这个用OD动态调试吧(ps:耐心点就好)

先来一个ESP定律 然后单步跟踪即可

遇到向上跳转就在它的下面一行按F4 就好

我记得我好像nop了一个向上的jmp 还好没事)

```
00401150    55              push ebp                                 ; OEP
00401151    8BEC            mov ebp,esp
00401153    6A FF           push -0x1
00401155    68 D0504000     push Easy_Unp.004050D0
0040115A    68 1C1E4000     push Easy_Unp.00401E1C
0040115F    64:A1 00000000  mov eax,dword ptr fs:[0]
00401165    50              push eax
00401166    64:8925 0000000>mov dword ptr fs:[0],esp
0040116D    83EC 58         sub esp,0x58
00401170    53              push ebx                                 ; user32.745E0000
00401171    56              push esi                                 ; Easy_Unp.<ModuleEntryPoint>
00401172    57              push edi                                 ; Easy_Unp.<ModuleEntryPoint>
```