ASPack 2.x**脱壳小记**

作者: Delort

备注:此题脱壳简单,无需手工

1.x64dbg

x64dbg运行找到

```
call <JMP.&RegisterClassA>
call <JMP.&DialogBoxParamA>
                                                                                                                                                                                                                                                                                                            <user
                                                                                                                                                                                                                                                                                                           <user
                     call <JMP.&GetDlgItemTextA>
                                                                                                                                                                                                                                                                                                            <user
                     call <JMP.&wsprintfA>
call <JMP.&wsprintfA>
call <JMP.&wsprintfA>
call <JMP.&GetDlgItemTextA>
                                                                                                                                                                                                                                                                                                           <user
                                                                                                                                                                                                                                                                                                           <user:
                     call <JMP.&MessageBoxA>
                     call <JMP.&MessageBoxA>
                     call <JMP.&EndDialog>
call <JMP.&EndDialog>
                                                                                                                                                                                                                                                                                                           <user
                                                                                                                                                                                                                                                                                                           <user:
00401691
                     call <JMP.&GetCommandLineA>
                     call <JMP.&strchr>
call <JMP.&GetModuleHandleA>
                                                                                                                                                                                                                                                                                                           <crtdl
                                                                                                                                                                                                                                                                                                           <kerne
                    call <JMP.&GetModuleHandleA>
call dword ptr ds:[<&GetModuleFileNameA>]
call dword ptr ds:[<&LoadLibraryA>]
call dword ptr ds:[<&GetCommandLineA>]
call dword ptr ds:[<&GetEnvironmentStrings>]
call dword ptr ds:[<&GetVersion>]
call dword ptr ds:[<&EvironeMandledExceptionFilter>]
call dword ptr ds:[<&ExitProcess>]
                                                                                                                                                                                                                                                                                                            <kerne
                                                                                                                                                                                                                                                                                                           <kerne
                                                                                                                                                                                                                                                                                                           <kerne
                                                                                                                                                                                                                                                                                                           <kerne
                                                                                                                                                                                                                                                                                                            <kerne
```

2.纠正指令

纠正前:

```
401683
             5E
                                             esi
                                        pop
                                            ebx
            C9
            C2 1000
            00 00
                                        add byte ptr
                                                        ds:[eax],al
401689 <
                                                                                          sub_401689
            00 55 89
                                        add byte ptr
                                                        ss:[ebp -77],dl
            E8 5A 00 00 00
                                        call <JMP.&GetCommandLineA>
401691
             89 C7
                                             edi ,eax
401696
            80 3F 22
                                                        ds:[edi],22
                                             byte ptr
            75 23
6A 22
40169D
            89 F8
             50
             E8 08 01 00 00
             83 C4 08
                                        add esp,8
             89 45 FC
                                        mov dword ptr
                                                         ss:[ebp-4],eax
             09 C0
4016AE
            74 29
```

纠正后:

```
nop
0040168B
                                                        push ebp
0040168C
                   89 E5
                   51
0040168F
                                                        push ecx
00401690
                                                       call <JMP.&GetCommandLineA>
mov edi ,eax
cmp byte ptr ds:[edi],2:
jne crackme6.4016C0
                   E8 5A 00 00 00
00401696
                   89 C7
                   80 3F 22
                                                                             ds:[edi],22
00401698
                   75 23
6A 22
                   89 F8
0040169F
                   40
                                                        push eax
call <JMP.&strchr>
                    50
                   E8 08 01 00 00
```

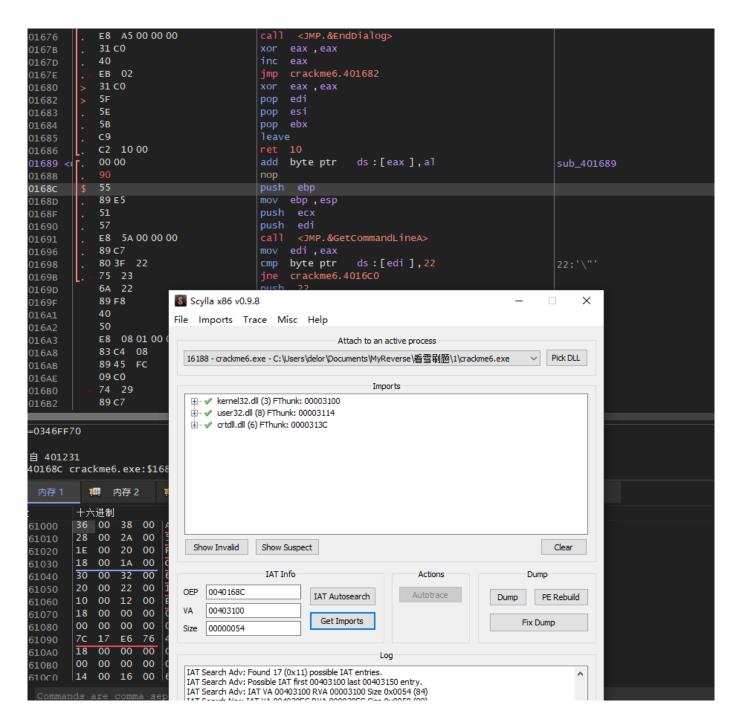
此处即为OEP。

3.**使用**Scylla

dump:

新开一个CrackMe进程。

然后使用独立版进行dump:



然后fix dump.