

实验吧CTF逆向题目easycreakme题解

原创

iqiqiya 于 2017-12-24 19:57:00 发布 2624 收藏 3

分类专栏: [-----实验吧CTF 我的CTF进阶之路](#) 文章标签: [easycreakme](#) [逆向](#) [实验吧CTF](#) [西普](#) [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/78886805>

版权



[-----实验吧CTF 同时被 2 个专栏收录](#)

6 篇文章 0 订阅

订阅专栏

[我的CTF进阶之路](#)

108 篇文章 18 订阅

订阅专栏

在实验吧看到这道题

题目链接

http://ctf5.shiyanbar.com/reverse/easycreakme/Easy_CrackMe.exe.bak



hanyuhang

运行不了时啥情况==!



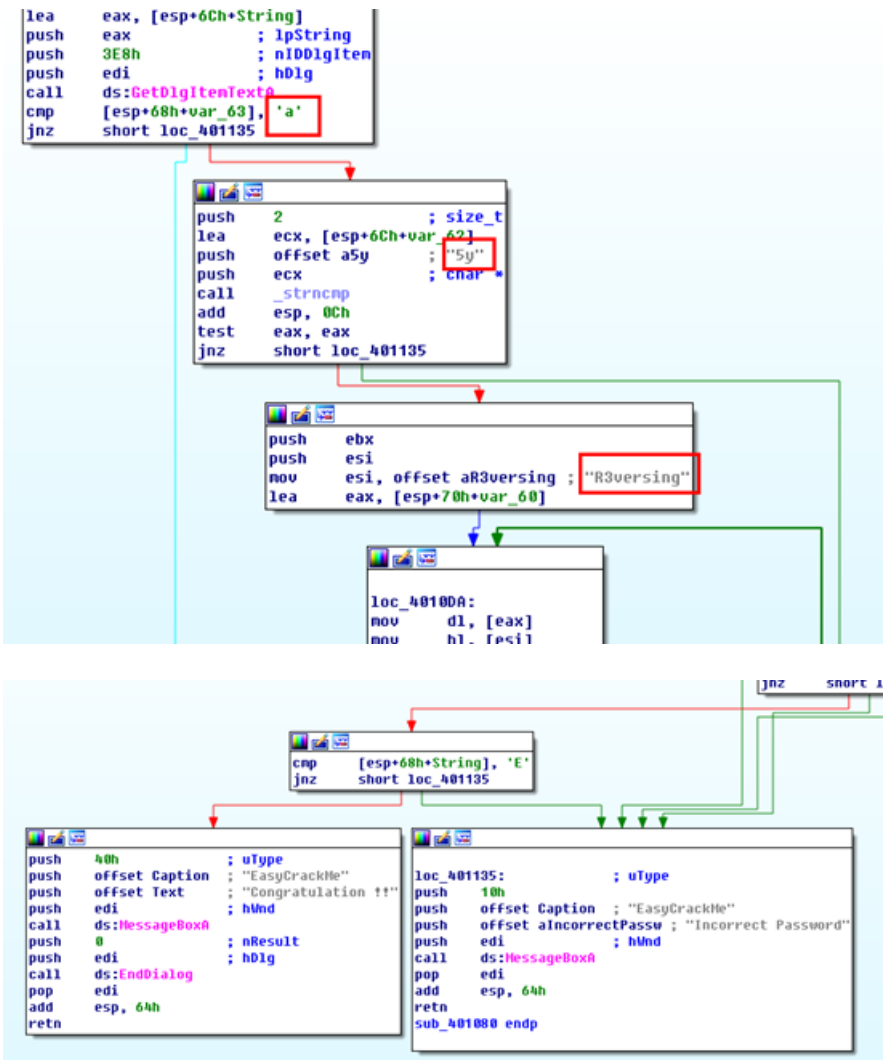
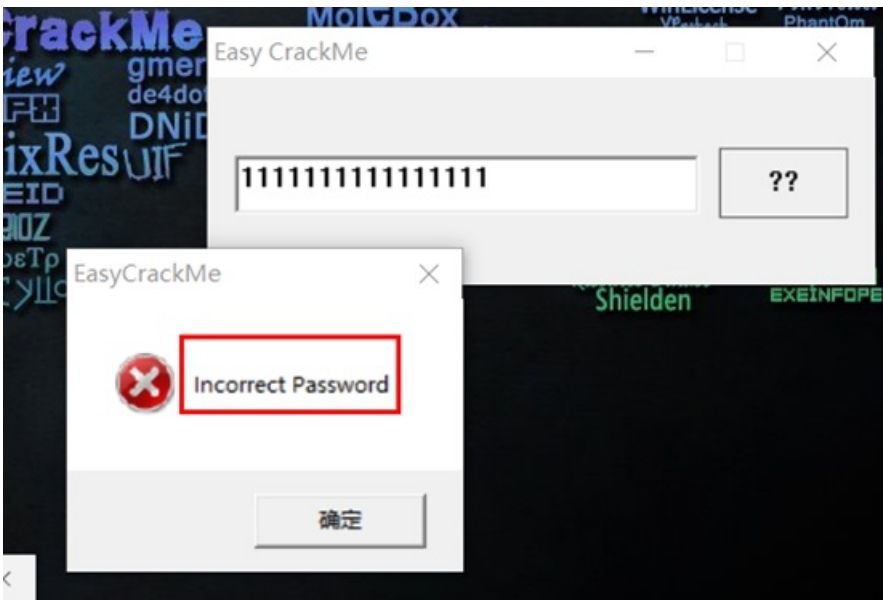
墨流云

回复:hanyuhang

加壳了, 而且我对文件的格式进行了更改, 原来是exe格式的

我是直接用的脱壳后的

<https://pan.baidu.com/s/1qYLZaXm>



IDA载入很清楚的可以发现先后与a,5y,R3versing,E进行比较

若都符合 输出congratulation!!

那么我们的flag就是Ea5yR3versing

最后记得加上ctf{}再提交

载入OD看看

```
004010AA - FF15 9C504000 call dword ptr ds:[<USER32.GetDlgItemText@EasyCrackMe>]
004010B0 - 807C24 05 61 cmp byte ptr ss:[esp+0x5],0x61
004010B5 - 75 7E jnz short Easy_Cra.00401135
004010B7 - 6A 02 push 0x2
004010B9 - 8D4C24 0A lea ecx,dword ptr ss:[esp+0xA]
004010BD - 68 78604000 push Easy_Cra.00406078
004010C2 - 51 push ecx
004010C3 - E8 88000000 call Easy_Cra.00401150
004010C8 - 83C4 0C add esp,0xC
004010CB - 85C0 test eax,eax
004010CD - 75 66 jnz short Easy_Cra.00401135
004010CF - 53 push ebx
004010D0 - 56 push esi
004010D1 - BE 6C604000 mov esi,Easy_Cra.0040606C
004010D6 - 8D4424 10 lea eax,dword ptr ss:[esp+0x10]
004010DA - 8A10 mov dl,byte ptr ds:[eax]
004010DC - 8A1E mov bl,byte ptr ds:[esi]
004010DE - 8ACA mov cl,dl
004010E0 - 3AD3 cmp dl,bl
004010E2 - 75 1E jnz short Easy_Cra.00401102
004010E4 - 84C9 test cl,cl
004010E6 - 74 16 je short Easy_Cra.004010FE
004010E8 - 8A50 01 mov dl,byte ptr ds:[eax+0x1]
004010EB - 8A5E 01 mov bl,byte ptr ds:[esi+0x1]
004010EE - 8ACA mov cl,dl
004010F0 - 3AD3 cmp dl,bl
004010F2 - 75 0E jnz short Easy_Cra.00401102
004010F4 - 83C0 02 add eax,0x2
```

```
> . 8B 05 jmp short Easy_Cra.00401107
> . 18C0 sbb eax,eax
> . 83D8 FF sbb eax,-0x1
> . 5E pop esi
> . 5B pop ebx
> . 85C0 test eax,eax
> . 75 28 jnz short Easy_Cra.00401135
> . 807C24 04 45 cmp byte ptr ss:[esp+0x4],0x45
> . 75 21 jnz short Easy_Cra.00401135
> . 6A 40 push 0x40
> . 68 58604000 push Easy_Cra.00406058
> . 68 44604000 push Easy_Cra.00406044
> . 57 push edi
```

每个跳转前都有一个cmp 把串拼接一下就好

作者题解:

<https://www.52pojie.cn/thread-639741-1-1.html>