

攻防世界 逆向 IgniteMe

原创

与日平肩以头抢地 于 2020-02-19 11:00:27 发布 505 收藏 1

分类专栏: [逆向](#) 文章标签: [安全](#)

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/fool_best/article/details/104387959

版权



[逆向](#) 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

攻防世界 逆向 IgniteMe

(原创)

原题如下:

IgniteMe 最佳Writeup由admin提供

难度系数: ★ 1.0

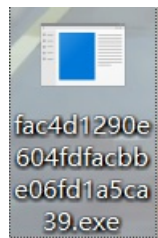
题目来源: 高校网络信息安全运维挑战赛

题目描述: 暂无

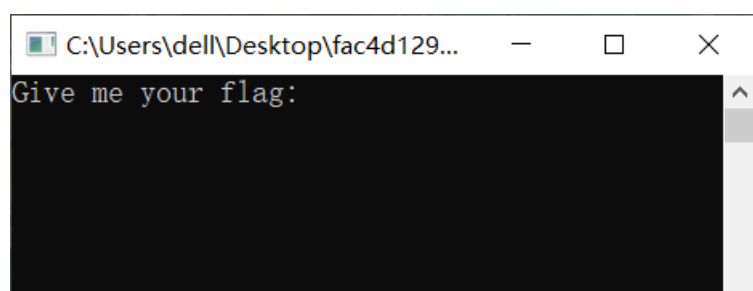
题目场景: 暂无

题目附件: 附件1
https://blog.csdn.net/fool_best

下载文件:

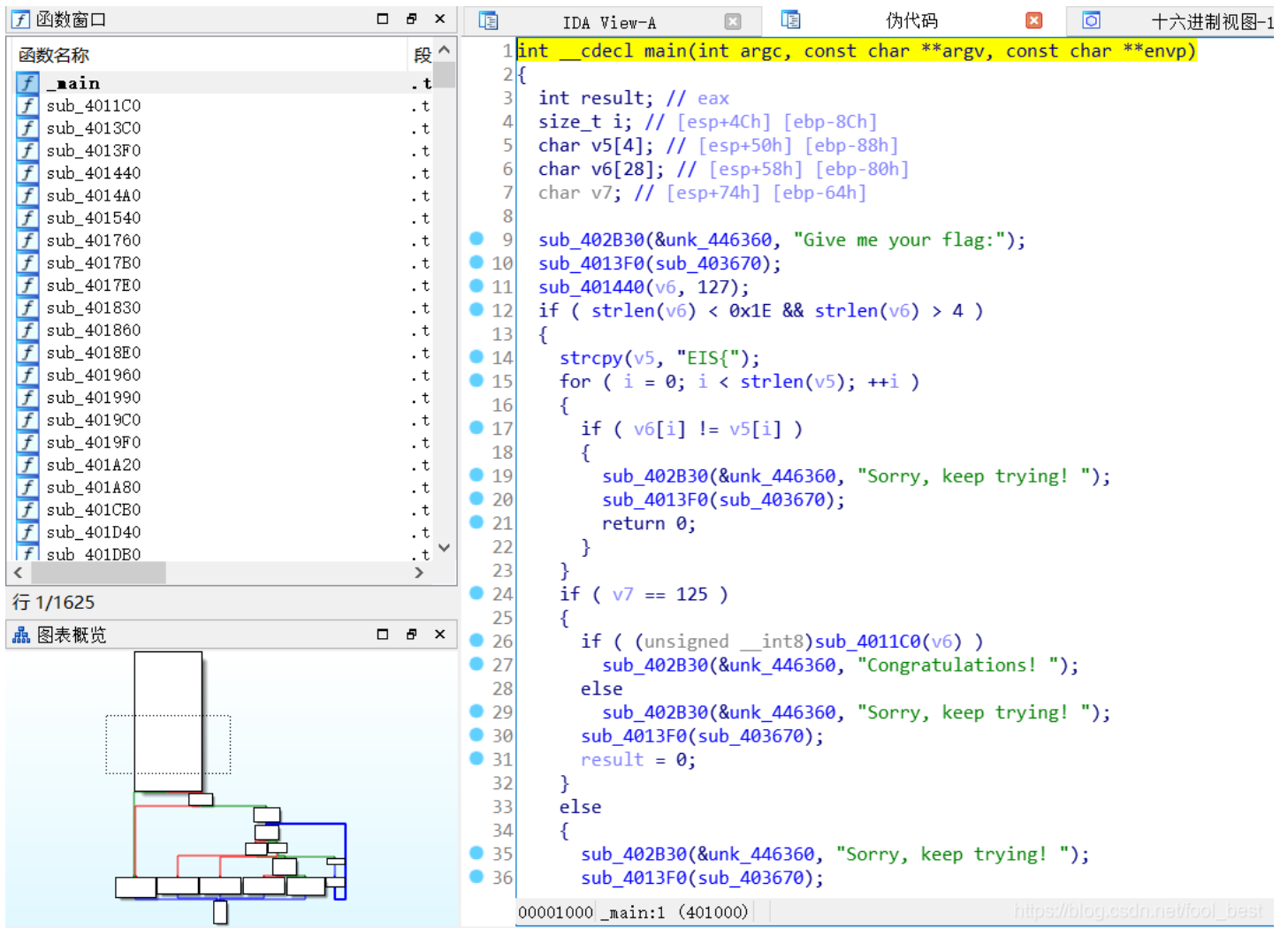


运行exe程序。



https://blog.csdn.net/fool_best

我随便输入了一串，enter之后当场退出程序。我们来用IDA打开这个文件。
找到main函数，F5反编译。



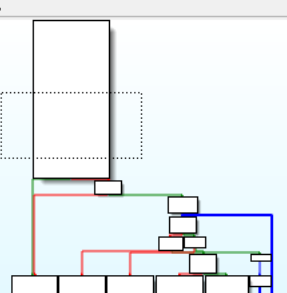
函数窗口

函数名称	段
_main	.t
sub_4011C0	.t
sub_4013C0	.t
sub_4013F0	.t
sub_401440	.t
sub_4014A0	.t
sub_401540	.t
sub_401760	.t
sub_4017B0	.t
sub_4017E0	.t
sub_401830	.t
sub_401860	.t
sub_4018E0	.t
sub_401960	.t
sub_401990	.t
sub_4019C0	.t
sub_4019F0	.t
sub_401A20	.t
sub_401A80	.t
sub_401CB0	.t
sub_401D40	.t
sub_401DB0	.t

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     int result; // eax
4     size_t i; // [esp+4Ch] [ebp-8Ch]
5     char v5[4]; // [esp+50h] [ebp-88h]
6     char v6[28]; // [esp+58h] [ebp-80h]
7     char v7; // [esp+74h] [ebp-64h]
8
9     sub_402B30(&unk_446360, "Give me your flag:");
10    sub_4013F0(sub_403670);
11    sub_401440(v6, 127);
12    if ( strlen(v6) < 0x1E && strlen(v6) > 4 )
13    {
14        strcpy(v5, "EIS{");
15        for ( i = 0; i < strlen(v5); ++i )
16        {
17            if ( v6[i] != v5[i] )
18            {
19                sub_402B30(&unk_446360, "Sorry, keep trying! ");
20                sub_4013F0(sub_403670);
21                return 0;
22            }
23        }
24    }
25    if ( v7 == 125 )
26    {
27        if ( (unsigned __int8)sub_4011C0(v6) )
28            sub_402B30(&unk_446360, "Congratulations! ");
29        else
30            sub_402B30(&unk_446360, "Sorry, keep trying! ");
31        sub_4013F0(sub_403670);
32        result = 0;
33    }
34    else
35    {
36        sub_402B30(&unk_446360, "Sorry, keep trying! ");
37        sub_4013F0(sub_403670);
38    }
39    return result;
40 }
```

行 1/1625

图表概览



00001000 _main:1 (401000) https://blog.csdn.net/fool_best

第27行就是我们程序运行时一定要运行的一句代码。

输入的字符串就是v6，

根据14行的strcpy函数和15行的for语句可以知道前4个字符是“EIS{”。

接下来是26行的sub_4011C0函数，这个函数返回的直应该是“1”，也就是true。我们看sub_4011C0函数的伪代码。

```
{
    size_t v2; // eax
    signed int v3; // [esp+50h] [ebp-B0h]
    char v4[32]; // [esp+54h] [ebp-ACh]
    int v5; // [esp+74h] [ebp-8Ch]
    int v6; // [esp+78h] [ebp-88h]
    size_t i; // [esp+7Ch] [ebp-84h]
    char v8[128]; // [esp+80h] [ebp-80h]

    if ( strlen(a1) <= 4 )
        return 0;
```

```

    return v;
    i = 4;
    v6 = 0;
    while ( i < strlen(a1) - 1 )
        v8[v6++] = a1[i++];
    v8[v6] = 0;
    v5 = 0;
    v3 = 0;
    memset(v4, 0, 0x20u);
    for ( i = 0; ; ++i )
    {
        v2 = strlen(v8);
        if ( i >= v2 )
            break;
        if ( v8[i] >= 97 && v8[i] <= 122 )
        {
            v8[i] -= 32;
            v3 = 1;
        }
        if ( !v3 && v8[i] >= 65 && v8[i] <= 90 )
            v8[i] += 32;
        v4[i] = byte_4420B0[i] ^ sub_4013C0(v8[i]);
        v3 = 0;
    }
    return strcmp("GONDPHyGjPEKruv{{pj]X@rF", v4) == 0;
}

```

https://blog.csdn.net/fool_best

得到v4="GONDPHyGjPEKruv{{pj]X@rF"，上一个函数带入的参数是v6，也就是flag。在sub_4011C0函数中就是参数*a1，下面的while语句将flag复制到了v8。。。。这样一步一步分析。

写出脚本：

```

import string

result = ''
tmp = ['0x0D', '0x13', '0x17', '0x11', '0x2', '0x1', '0x20', '0x1D',
       '0x0C', '0x2', '0x19', '0x2F', '0x17', '0x2B', '0x24', '0x1F',
       '0x1E', '0x16', '0x9', '0xF', '0x15', '0x27', '0x13', '0x26',
       '0x0A', '0x2F', '0x1E', '0x1A', '0x2D', '0x0C', '0x22', '0x4']
f = 0
r = ''
comp = 'GONDPHyGjPEKruv{{pj]X@rF'
s = string.printable
print(s)
for i in range(24):
    for x in s:
        j = x
        if 97 <= ord(j) <= 122:
            x = chr(ord(j) - 32)
            f = 1
        if f == 0 and 65 <= ord(j) <= 90:
            x = chr(ord(j) + 32)
        r = chr(int(tmp[i], 16) ^ (ord(x) ^ 0x55) + 72)
        f = 0
        if r == comp[i]:
            result += j
            break
print(result)

```

得到flag。

可能有大佬有更好的方法，多谢指点。