攻防世界 逆向 EasyRE

原创

与日平肩以头抢地 于 2020-02-25 19:05:36 发布 2344 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/104503159

版权

逆向 专栏收录该内容

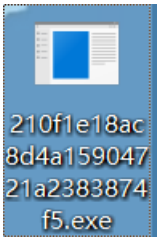
12 篇文章 0 订阅

订阅专栏

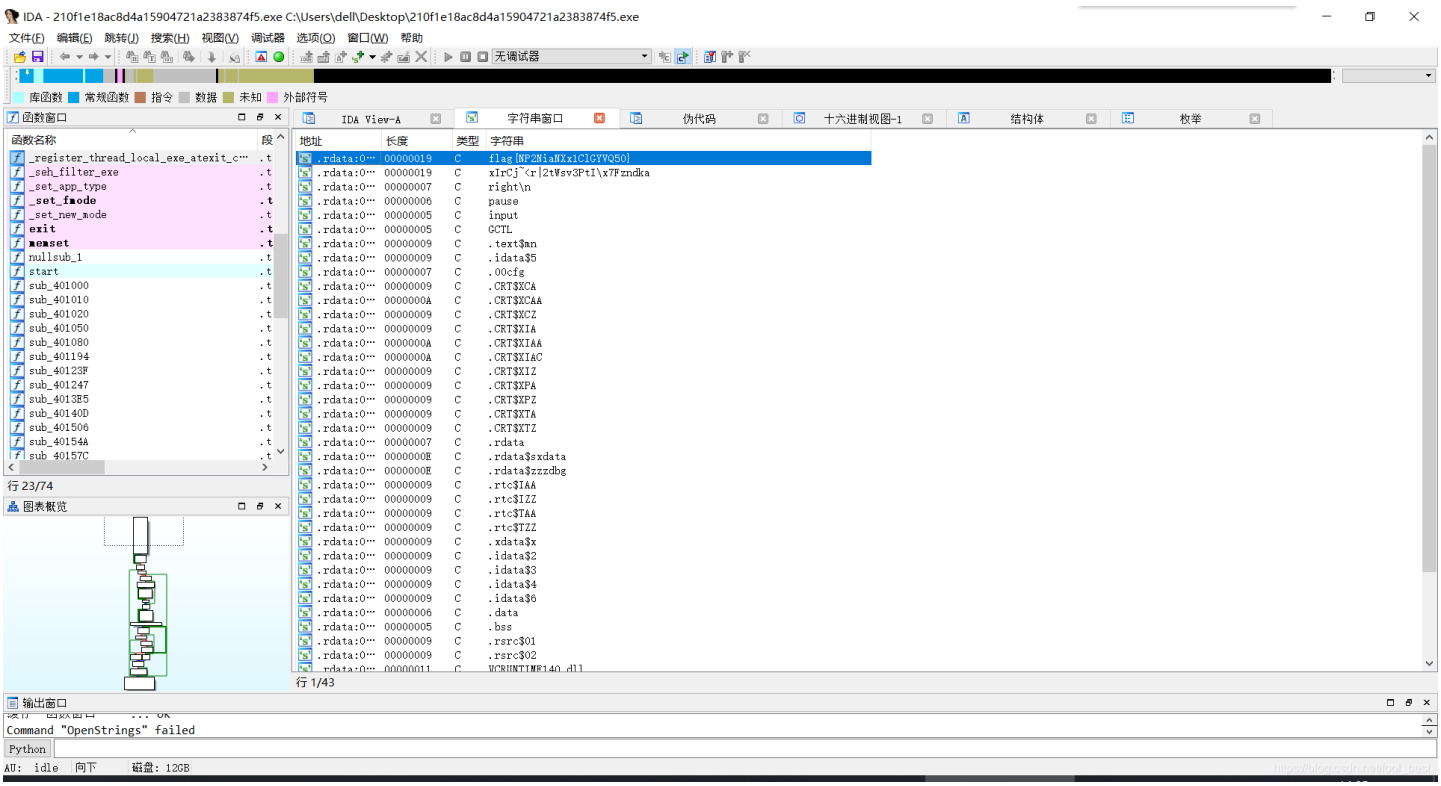
攻防世界 逆向 EasyRE

（原创）
原题如下：

下载文件：



查看exe文件的脱壳信息并用IDA打开。



Shift+F12查看字符串窗口，发现flag，但是并不对。
注意到下面的right\n，查看其伪代码。
此函数源代码如下：

```
int sub_401080()
{
  unsigned int v0; // kr00_4
  signed int v1; // edx
  char *v2; // esi
  char v3; // al
  unsigned int v4; // edx
  int v5; // eax
  __int128 v7; // [esp+2h] [ebp-24h]
  __int64 v8; // [esp+12h] [ebp-14h]
  int v9; // [esp+1Ah] [ebp-Ch]
  __int16 v10; // [esp+1Eh] [ebp-8h]

  sub_401020(&unk_402150, v7);
  v9 = 0;
  v10 = 0;
  v7 = 0i64;
  v8 = 0i64;
  sub_401050((const char *)&unk_402158, (unsigned int)&v7);
  v0 = strlen((const char *)&v7);
  if ( v0 >= 0x10 && v0 == 24 )
  {
    v1 = 0;
    v2 = (char *)&v8 + 7;
    do
    {
      v3 = *v2--;
      byte_40336C[v1++] = v3;
    }
    while ( v1 < 24 );
    v4 = 0;
    do
    {
      byte_40336C[v4] = (byte_40336C[v4] + 1) ^ 6;
      ++v4;
    }
    while ( v4 < 0x18 );
    v5 = strcmp(byte_40336C, "xIrCj~<r|2tWsv3PtI\x7Fzndka");
    if ( v5 )
      v5 = -(v5 < 0) | 1;
    if ( !v5 )
    {
      sub_401020("right\n", v7);
      system("pause");
    }
  }
  return 0;
}
```

主要部分为下图中的代码。

```
3
4  sub_401020(&unk_402150, v7);
5  v9 = 0;
6  v10 = 0;
7  v7 = 0i64;
8  v8 = 0i64;
9  sub_401050((const char *)&unk_402158, (unsigned int)&v7);
0  v0 = strlen((const char *)&v7);
1  if ( v0 >= 0x10 && v0 == 24 )
2  {
3    v1 = 0;
4    v2 = (char *)&v8 + 7;
5    do
6    {
7      v3 = *v2--;
8      byte_40336C[v1++] = v3;
9    }
0    while ( v1 < 24 );
1    v4 = 0;
2    do
3    {
4      byte_40336C[v4] = (byte_40336C[v4] + 1) ^ 6;
5      ++v4;
6    }
7    while ( v4 < 0x18 );
8    v5 = strcmp(byte_40336C, "xIrCj~<r|2tWsv3PtI\x7Fzndka");
9    if ( v5 )
0      v5 = -(v5 < 0) | 1;
1    if ( !v5 )
2    {
3      sub_401020("right\n", v7);
4      system("pause");
5    }
```

https://blog.csdn.net/fool_best

主要的变量为v5、byte_40336C和其他几个表示位序的变量。
编写C语言的代码，如下。

```
#include<iostream>
#include<string>
using namespace std;

int  main()
{
    const char* tar = "xIrCj~<r|2tWsv3PtIzndka";
    char flag[25] = { 0 };
    for (int i = 0; i < 24; i++)
    {
        flag[i] = tar[23 - i] ^ 0x6;
        flag[i]--;
    }
    cout << flag;
    return 0;
}
/*
```

https://blog.csdn.net/fool_best

运行得到flag。