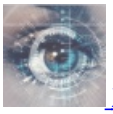
XCTF IgniteMe

原创

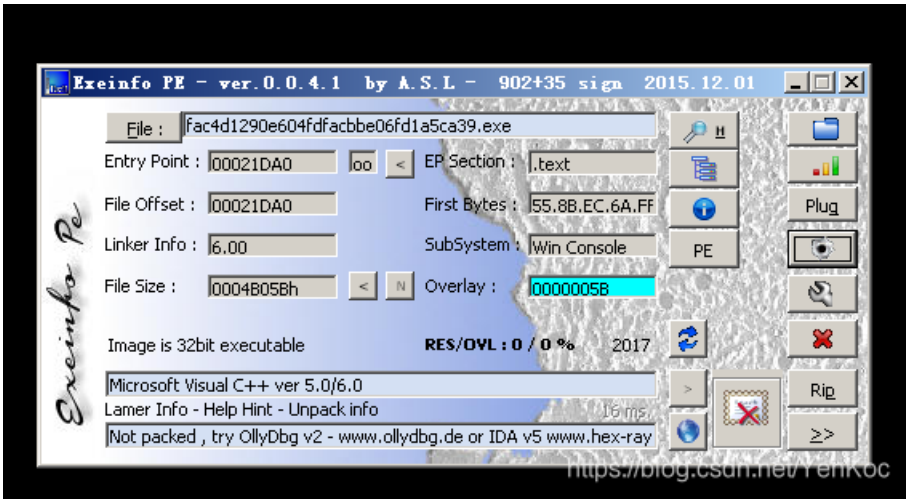
YenKoc 于 2020-03-22 10:38:53 发布 142 收藏

分类专栏： XCTF

本文链接：https://blog.csdn.net/YenKoc/article/details/105023645



一.查壳



结论：

```
1.用vc++编译的。
2.无壳，毕竟是一分的题
```

二.点击运行，发现不是爆破，而是找出注册机，汇编功力还在提升中，只能拖入ida来静态调试了

具体的见注释：

```
char v9[28]; // [sp+58h] [bp-80h]@1
char v10; // [sp+74h] [bp-64h]@9

memset(&v6, 0xCCu, 0xCCu);
sub_402B30((int)&unk_446360, "Give me your flag:");
sub_4013F0(sub_403670);
sub_401440((int)&dword_4463F0, v3, (int)v9, 127);// 输入字符串到v9
                                                 // 为首地址的内存里
                                                 //
if ( strlen(v9) < 30 && strlen(v9) > 4 )         // flag长度大于4小于30
{
  strcpy(v8, "EIS{");                            // 将常量赋值给v8
  for ( i = 0; ; ++i )
  {
    v5 = strlen(v8);
    if ( i >= v5 )
      break;
    if ( v9[i] != v8[i] )
    {
      sub_402B30((int)&unk_446360, "Sorry, keep trying! ");
      sub_4013F0(sub_403670);
      return 0;
    }
  }                                              // 说明flag开头字符串为EIS{
  if ( v10 == 125 )
  {
    if ( sub_4011C0(v9) )
    {
      sub_402B30((int)&unk_446360, "Congratulations! ");
      sub_4013F0(sub_403670);
      result = 0;
    }
    else
    {
      sub_402B30((int)&unk_446360, "Sorry, keep trying! ");
      sub_4013F0(sub_403670);
      result = 0;
    }
  }
  else
  {
    sub_402B30((int)&unk_446360, "Sorry, keep trying! ");
    sub_4013F0(sub_403670);
    result = 0;
  }
}
```


二.1点击进入关键函数

```
sub_4011C0(v9)
```

注意！这里有个坑，

```
if ( v10 == 125 )
```

```
2    }                                                  // 说明
3    if ( v10 == '}' )
4    {
5      if ( sub_4011C0(v9) )
```

将125转换成字符,

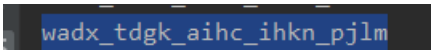
说明最后一个字符是}这点，可能会被很多人给忽视了,三分逆向，七分猜2333

三.见注释

```
3  bool result; // al@2
4  size_t v2; // eax@4
5  size_t v3; // eax@7
6  char v4; // [sp+Ch] [bp-F4h]@1
7  int v5; // [sp+4Ch] [bp-B4h]@15
8  int v6; // [sp+50h] [bp-B0h]@6
9  char v7[32]; // [sp+54h] [bp-ACh]@6
0  int v8; // [sp+74h] [bp-8Ch]@6
1  int i; // [sp+78h] [bp-88h]@3
2  unsigned int j; // [sp+7Ch] [bp-84h]@3
3  char v11[128]; // [sp+80h] [bp-80h]@5
4
5  memset(&v4, 0xCCu, 0xF4u);
6  if ( strlen(a1) > 4 )
7  {
8    j = 4;
9    for ( i = 0; ; ++i )
0    {
1      v2 = strlen(a1);
2      if ( j >= v2 - 1 )
3        break;
4      v11[i] = a1[j++];                          // 将字符串第5位开始到倒数第二位赋值给v11
5    }
6    v11[i] = 0;
7    v8 = 0;
8    v6 = 0;
9    memset(v7, 0, 0x20u);
0    for ( j = 0; ; ++j )
1    {
2      v3 = strlen(v11);
3      if ( j >= v3 )
4        break;
5      if ( v11[j] >= 'a' && v11[j] <= 'z' )
6      {
7        v11[j] -= 32;                            // 小写字母变大写字母
8        v6 = 1;
9      }
0      if ( !v6 && v11[j] >= 'A' && v11[j] <= 'Z' )
1        v11[j] += 32;                            // 大写变小写
2      v5 = sub_4013C0(v11[j]);                   // 异或0x55,再加上72
3      v7[j] = dword_4420B0[j] ^ v5;              // v5异或对应数组
4      v6 = 0;
5    }
6    result = strcmp("GONDPHyGjPEKruv{{pj]X@rF", v7) == 0;
7  }
8  else
9  {
0    result = 0;
```


四.脚本上：

```python
v7="GONDPHyGjPEKruv{{pj]X@rF"
byte=[0xD,0x13,0x17,0x11,0x2,0x1,0x20,0x1D,0x0C,0x2,0x19,0x2F,0x17,0x2B,0x24,0x1F,0x1E,0x16,0x9,0xF,0x15,0x27,0x
13,0x26,0xA,0x2F,
      0x1E,0x1A,0x2D,0xC,0x22,0x4]
v5=""
str=""
for i in range(24):
    v5+=chr(ord(v7[i])^byte[i])
for j in v5:
    str+=chr((ord(j)-72)^0x55)
res=""
for a in str:
    if a>='A' and a<='Z':
        res+=chr(ord(a)+32)
    elif a>='a' and a<='z':
        res+=chr(ord(a)-32)
    else:
        res+=a
print(res)
```



五.FLAG:

flag=EIS{wadx_tdgk_aihc_ihkn_pjlm}