攻防世界 Reverse高手进阶区 2分题 elrond32

原创

思源湖的鱼 于 2020-12-13 14:28:33 发布 127 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 reverse

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111111593

前言

继续ctf的旅程

攻防世界Reverse高手进阶区的2分题

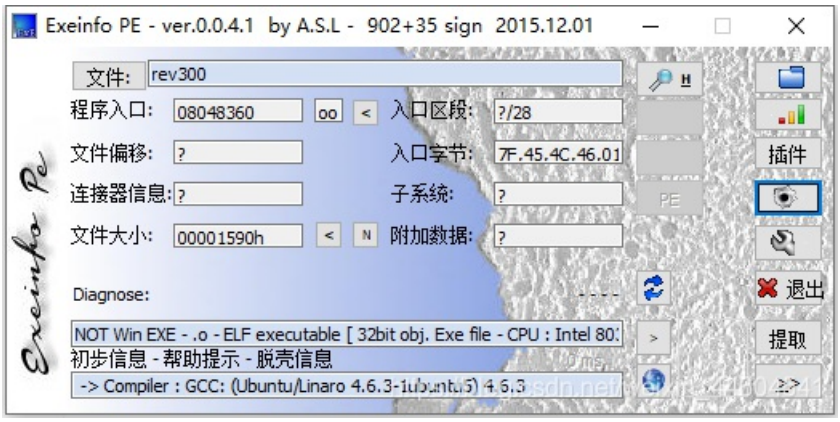
本篇是elrond32的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

PE查壳



扔进IDA

```
int __cdecl main(int a1, char **a2)
{
  if ( a1 > 1 && sub_8048414(a2[1], 0) )
```

```
  puts("Access granted");
  sub_8048538(a2[1]);
 }
 else
 {
  puts("Access denied");
 }
 return 0;
}
```



```
signed int __cdecl sub_8048414(_BYTE *a1, int a2)
{
  signed int result; // eax

  switch ( a2 )
  {
    case 0:
      if ( *a1 == 105 )
        goto LABEL_19;
      result = 0;
      break;
    case 1:
      if ( *a1 == 101 )
        goto LABEL_19;
      result = 0;
      break;
    case 3:
      if ( *a1 == 110 )
        goto LABEL_19;
      result = 0;
      break;
    case 4:
      if ( *a1 == 100 )
        goto LABEL_19;
      result = 0;
      break;
    case 5:
      if ( *a1 == 97 )
        goto LABEL_19;
      result = 0;
      break;
    case 6:
      if ( *a1 == 103 )
        goto LABEL_19;
      result = 0;
      break;
    case 7:
      if ( *a1 == 115 )
        goto LABEL_19;
      result = 0;
      break;
    case 9:
      if ( *a1 == 114 )
LABEL_19:
        result = sub_8048414(a1 + 1, 7 * (a2 + 1) % 11);
      else
        result = 0;
      break;
    default:
      result = 1;
      break;
```



```
int __cdecl sub_8048538(int a1)
{
  int v2[33]; // [esp+18h] [ebp-A0h]
  int i; // [esp+9Ch] [ebp-1Ch]

  qmemcpy(v2, &unk_8048760, sizeof(v2));
  for ( i = 0; i <= 32; ++i )
    putchar(v2[i] ^ *(char *)(a1 + i % 8));
  return putchar(10);
}
```

一个验证输入

一个负责输出

跟进 8048769，这里需要 `33*4=132=16*8+1` 个字节的内容，即需要前往 hex 窗口中找 8 行加 1 个 4 字节的数据，还要注意小端序的问
题（还好这里每个 32bit 的前 3 个字节都是 0x00）

```
08048760  0F 00 00 00 1F 00 00 00  04 00 00 00 09 00 00 00  ................
08048770  1C 00 00 00 12 00 00 00  42 00 00 00 09 00 00 00  ........B.......
08048780  0C 00 00 00 44 00 00 00  0D 00 00 00 07 00 00 00  ....D...........
08048790  09 00 00 00 06 00 00 00  2D 00 00 00 37 00 00 00  ........-...7...
080487A0  59 00 00 00 1E 00 00 00  00 00 00 00 59 00 00 00  Y...........Y...
080487B0  0F 00 00 00 08 00 00 00  1C 00 00 00 23 00 00 00  ............#...
080487C0  36 00 00 00 07 00 00 00  55 00 00 00 02 00 00 00  6.......U.......
080487D0  0C 00 00 00 08 00 00 00  41 00 00 00 0A 00 00 00  ........A.......
080487E0  14 00 00 00 41 63 63 65  73 73 20 67 72 61 6E 74  ....Access grant
```

根据题意
得到脚本

```
a='ie ndags r'
x=0
s=[]
for i in range(8):
    x=7*x%11
    s.append(a[x])
    x+=1
print(''.join(s))
data=[15, 31, 4, 9, 28, 18, 66, 9, 12, 68, 13, 7, 9, 6, 45, 55, 89, 30, 0, 89, 15, 8, 28, 35, 54, 7, 85, 2, 12,
8, 65, 10, 20]
for i in range(33):
    print(chr(ord(s[i%8])^data[i]),end='')
```

得到flag：`flag{s0me7hing_S0me7hinG_t0lki3n}`

结语

逻辑比较清晰