攻防世界 Reverse高手进阶区 2分题 Shuffle

原创

思源湖的鱼 于 2020-12-03 13:50:42 发布 128 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/110529072

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

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Shuffle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

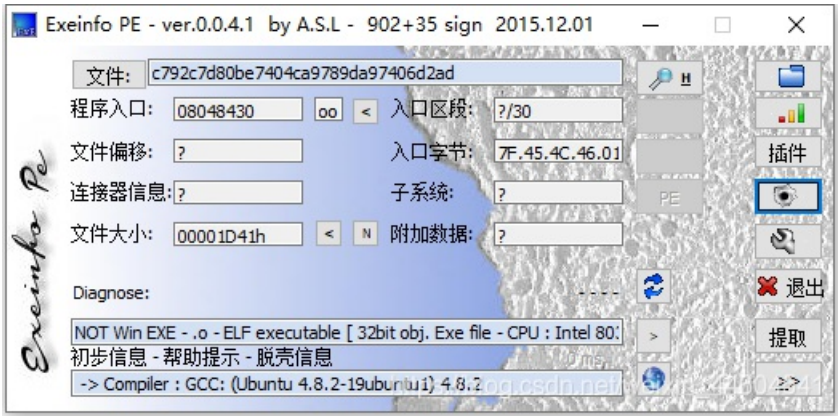
下下来一个无后缀文件

扔进winhex

```
00000000  7F 45 4C 46 01 01 01 00  00 00 00 00 00 00 00 00   ELF
00000016  02 00 03 00 01 00 00 00  30 84 04 08 34 00 00 00          0„  4
00000032  60 11 00 00 00 00 00 00  34 00 20 00 09 00 28 00  `       4      (
00000048  1E 00 1B 00 06 00 00 00  34 00 00 00 34 80 04 08          4   4€
00000064  34 80 04 08 20 01 00 00  20 01 00 00 05 00 00 00  4€
00000080  04 00 00 00 03 00 00 00  54 01 00 00 54 81 04 08          T   T
00000096  54 81 04 08 13 00 00 00  13 00 00 00 04 00 00 00  T
```

是个ELF

PE查壳



扔进IDA

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  time_t v3; // ebx
  __pid_t v4; // eax
  unsigned int v5; // ST18_4
  unsigned int v6; // ST1C_4
  char v7; // ST20_1
  signed int i; // [esp+14h] [ebp-44h]
  char s; // [esp+24h] [ebp-34h]
  char v11; // [esp+25h] [ebp-33h]
  char v12; // [esp+26h] [ebp-32h]
  char v13; // [esp+27h] [ebp-31h]
  char v14; // [esp+28h] [ebp-30h]
  char v15; // [esp+29h] [ebp-2Fh]
  char v16; // [esp+2Ah] [ebp-2Eh]
  char v17; // [esp+2Bh] [ebp-2Dh]
  char v18; // [esp+2Ch] [ebp-2Ch]
  char v19; // [esp+2Dh] [ebp-2Bh]
  char v20; // [esp+2Eh] [ebp-2Ah]
  char v21; // [esp+2Fh] [ebp-29h]
  char v22; // [esp+30h] [ebp-28h]
  char v23; // [esp+31h] [ebp-27h]
  char v24; // [esp+32h] [ebp-26h]
  char v25; // [esp+33h] [ebp-25h]
  char v26; // [esp+34h] [ebp-24h]
  char v27; // [esp+35h] [ebp-23h]
  char v28; // [esp+36h] [ebp-22h]
  char v29; // [esp+37h] [ebp-21h]
  char v30; // [esp+38h] [ebp-20h]
  char v31; // [esp+39h] [ebp-1Fh]
  char v32; // [esp+3Ah] [ebp-1Eh]
  char v33; // [esp+3Bh] [ebp-1Dh]
  char v34; // [esp+3Ch] [ebp-1Ch]
  char v35; // [esp+3Dh] [ebp-1Bh]
  char v36; // [esp+3Eh] [ebp-1Ah]
  char v37; // [esp+3Fh] [ebp-19h]
  char v38; // [esp+40h] [ebp-18h]
  char v39; // [esp+41h] [ebp-17h]
  char v40; // [esp+42h] [ebp-16h]
  char v41; // [esp+43h] [ebp-15h]
  char v42; // [esp+44h] [ebp-14h]
  char v43; // [esp+45h] [ebp-13h]
  char v44; // [esp+46h] [ebp-12h]
```

```
char v45; // [esp+47h] [ebp-11h]
char v46; // [esp+48h] [ebp-10h]
char v47; // [esp+49h] [ebp-Fh]
char v48; // [esp+4Ah] [ebp-Eh]
char v49; // [esp+4Bh] [ebp-Dh]
unsigned int v50; // [esp+4Ch] [ebp-Ch]

v50 = __readgsdword(0x14u);
s = 83;
v11 = 69;
v12 = 67;
v13 = 67;
v14 = 79;
v15 = 78;
v16 = 123;
v17 = 87;
v18 = 101;
v19 = 108;
v20 = 99;
v21 = 111;
v22 = 109;
v23 = 101;
v24 = 32;
v25 = 116;
v26 = 111;
v27 = 32;
v28 = 116;
v29 = 104;
v30 = 101;
v31 = 32;
v32 = 83;
v33 = 69;
v34 = 67;
v35 = 67;
v36 = 79;
v37 = 78;
v38 = 32;
v39 = 50;
v40 = 48;
v41 = 49;
v42 = 52;
v43 = 32;
v44 = 67;
v45 = 84;
v46 = 70;
v47 = 33;
v48 = 125;
v49 = 0;
v3 = time(0);
v4 = getpid();
srand(v3 + v4);
for ( i = 0; i <= 99; ++i )
{
  v5 = rand() % 0x28u;
  v6 = rand() % 0x28u;
  v7 = *(&s + v5);
  *(&s + v5) = *(&s + v6);
  *(&s + v6) = v7;
}
```

```
  puts(&s);
  return 0;
}
```

转换为字符

```
52  s = 'S';
53  v11 = 'E';
54  v12 = 'C';
55  v13 = 'C';
56  v14 = 'O';
57  v15 = 'N';
58  v16 = '{';
59  v17 = 'W';
60  v18 = 'e';
61  v19 = 'l';
62  v20 = 'c';
63  v21 = 'o';
64  v22 = 'm';
65  v23 = 'e';
66  v24 = ' ';
67  v25 = 't';
68  v26 = 'o';
69  v27 = ' ';
70  v28 = 't';
71  v29 = 'h';
72  v30 = 'e';
73  v31 = ' ';
74  v32 = 'S';
75  v33 = 'E';
76  v34 = 'C';
77  v35 = 'C';
78  v36 = 'O';
79  v37 = 'N';
80  v38 = ' ';
81  v39 = '2';
82  v40 = '0';
83  v41 = '1';
84  v42 = '4';
85  v43 = ' ';
86  v44 = 'C';
87  v45 = 'T';
88  v46 = 'F';
89  v47 = '!';
90  v48 = '}';
91  v49 = '\0';
92  v3 = time(0);
93  v4 = getpid();
94  srand(v3 + v4);
```

得到flag：`SECCON{Welcome to the SECCON 2014 CTF!}`

结语

签到题？