ISCC reverse writeup-301

原创

HONKONE 于 2017-05-12 10:07:16 发布 965 收藏

分类专栏： CTF 文章标签： CTF

拿到这个文件的时候，看了下东西，并没有什么exe什么的后缀，就丢到kali看下

```
reverse: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld
```

```
/lib64/ld-linux-x86-64.so.2
libc.so.6
__isoc99_scanf
puts
__stack_chk_fail
printf
__libc_start_main
__gmon_start__
GLIBC_2.7
GLIBC_2.4
GLIBC_2.2.5
UH-P
0urH
/uOH
AWAVA
AUATL
[]A\A]A^A_
Keep thinking!
Please input your password(5 words):
Good Job!
The password:%s
Wrong!
;*3$"
GCC: (Ubuntu 5.4.0-6ubuntu1~16.04.2) 5.4.0 20160609
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.jcr
.dynamic
.got.plt
.data
.bss
.comment
```

由此可见里面有个要输入五个字符，但是当我们进行运行的时候，会发现段错误，我们吧东西拖到IDA了里面查看，在main里面发现一个sub_400646函数，进去看看

```
 v5 = 108;
  v6 = 49;
  v7 = 110;
  v8 = 117;
  v9 = 120;
  v10 = 99;
  v11 = 114;
  v12 = 97;
  v13 = 99;
  v14 = 107;
  for ( i = 0; i <= 4; ++i )
  {
    if ( *(*(a1 + 8) + i) != *(&v5 + i) )
    {
      result = '\x01';
      goto LABEL_12;
    }
  }
  for ( j = 0; j <= 4; ++j )
  {
    if ( *(*(a1 + 16) + j) != *(&v10 + j) )
    {
      result = 1LL;
      goto LABEL_12;
    }
  }
  result = 0LL;
LABEL_12:
  v2 = *MK_FP(__FS__, - -40LL) ^ v15;
  return result;
```

这里其实是有点代码混淆，实际上，转换过来简化下就是

```
int arry[108, 49, 110, 117, 120, 99, 114, 97, 99, 107]
for (i=0;i<4;i++)
{
    if( *(*(a1 + 8) + i) != arry [0+i] )//对第一个参数判断
    /*后面我看了下a1是我们传进去的参数，然后这里有两个for的话，也就是我们要传输进去两个参数，但是在这里之前，有对参数
    {
        result =1;
    }
}
for （j=0; j<4;j++）
{
    if( *(*(a1 + 16) + j) != arry [5+j] )//第二个
    {
        result =1;
    }
}
这样就可以得出两个输入的参数
```

然后运行之后，会让你再输入一个

```
Please input your password(5 words):
```

验证了之前我判断，然后这个也及其简单

```
__int64 __usercall sub_400755@<rax>(__int64 a1@<rax>)
{
  __int64 result; // rax@6

  if ( *a1 + *(a1 + 4) != 106 || *a1 != 73 )
  {
    result = 0LL;
  }
  else if ( *(a1 + 1) == 76 )
  {
    result = *(a1 + 2) + *(a1 + 3) == 137 && *(a1 + 3) == 70;
  }
  else
  {
    result = 0LL;
  }
  return result;
}
```

简单的一个算数题，这题就结束了

Good Job!