攻防世界 Reverse logmein

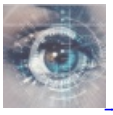
原创

==Microsoft== 已于 2022-03-12 14:06:03 修改 320 收藏

分类专栏： Reverse 文章标签： c语言 开发语言 ctf reverse

于 2022-03-12 14:05:53 首次发布

本文链接：https://blog.csdn.net/MrTreebook/article/details/123442889



攻防世界 Reverse logmein

1.file查看文件格式

```
lwj@ubuntu:~/Desktop/git/ctf-reverse/logmein$ checksec logmein
[*] '/home/lwj/Desktop/git/ctf-reverse/logmein/logmein'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

64位程序

2.IDA64打开

```
strcpy(v8, ":\"AL_RT^L*.?+6/46");
v7 = 0x65626D61726168LL;
v6 = 7;
printf("Welcome to the RC3 secure password guesser.\n");
printf("To continue, you must enter the correct password.\n");
printf("Enter your guess: ");
__isoc99_scanf("%32s", s);
v3 = strlen(s);                                 // s的长度
if ( v3 < strlen(v8) )
  incorrcet_password();
for ( i = 0; i < strlen(s); ++i )
{
  if ( i >= strlen(v8) )
    incorrcet_password();
  if ( s[i] != (char)(*((_BYTE *)&v7 + i % v6) ^ v8[i]) )
    incorrcet_password();
}
correct_password();
```

我们的目标是拿到密码

异或加密v7

v7 = 0x65626D61726168LL;

3.exp

```
k=str(bytes.fromhex(hex(28537194573619560)[2:]))[-2:1:-1]
#LL长整型数，需要转成十六进制再转换成字符，又因为是小端储存，所以要将字符串倒置
v= ":\"AL_RT^L*.?+6/46"
flag=''
for i in range(len(v)):
      flag+=chr(ord(v[i])^(ord(k[(i%7)])))
print(flag)
```

随便找个在线网站