Jarvis oj 文件数据修复 writeup

原创

charlie_heng 于 2017-11-25 20:40:46 发布 308 收藏

分类专栏： 二进制-逆向工程

本文链接：https://blog.csdn.net/charlie_heng/article/details/78634051

感觉这题把逆向玩成了misc。。。。

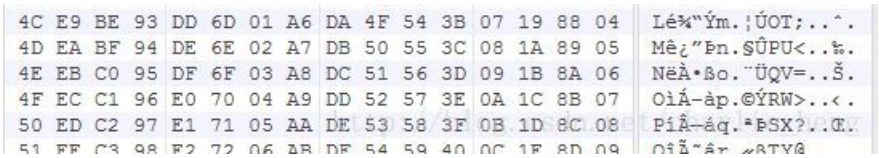
首先用mfc工具找到处理解密的函数

看了下代码，是把输入的密码一顿操作之后生成16位的key

然后用这个key异或一波文件的内容，异或完一次之后+1

但是关键是我们不知道密码是什么。。。虽然提示了8位纯数字，但是爆破依然很浪费时间

于是就发呆看着屏幕。。。结果看到有几列东西是每一列+1。。。于是大胆猜测全部都是0，这些就是key加了n异或后的结果



于是写个脚本，解出文件，binwalk一波就能拿到一个thumbnail.jpeg 里面就有flag，脚本如下

```
w=[68, 225, 182, 139, 213, 101, 249, 158, 210, 71, 76, 51, 255, 17, 128, 252]

f=open('CTF_300_1.ctf','rb')
da=f.read()
p=[]
for i in range(len(da)):
    p.append(da[i]^w[i%16])
    w[i%16]+=1
    w[i%16]%=256
f.close()
f=open('dec','wb')
f.write(bytes(p))
f.close()
```