hackme inndy reverse mov writeup

原创

charlie_heng 于 2018-01-30 15:42:27 发布 764 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/79206863

MOV instruction is turing complete!

mov是图灵完备的！

说真的，第一次看到这题的时候感觉真的完全震惊。。。一大堆mov，还以为是把代码写到一个地方，之后跳到那里，但是debug的时候并没有。。。

然后过了一阵子，在油管上无意中看到一个视频，讲的是怎么只用mov来写程序的。。。。然后想起这题。。。

看完那个视频之后，油管又推了一个怎么解这种movfuscator的视频(笑

在视频结尾有个github，可以去github搜下demovfuscator，下载之后配好环境。。。结果解失败了。。。。

然后在油管搜了一下0ctf那道momo的解题视频，发现有人用qira来解，qira这东西也是个神器。。。用起来真的挺爽

然后用qira来解，这个时候想吐槽玄学解题，真的三分技术，七分运气。。。

首先很明显，程序会将输入的字符map到另外一个字符，然后这个movfuscator其实也相当于一个虚拟机，但是就是比较难解而已，用上面那个demovfuscator可以解析出xor，or，之类的表在哪个地方，然后我玄学找到了要比较的那一串字符。。。就解出来了。。。。（qira如果有个搜索内存的功能多好

下面就是解题的代码

```
s=b'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789{}_/*-+'
sa=b'\x3e\x3d\x3c\x3b\x3a\x39\x38\x36\x37\x34\x35\x32\x33\x30\x31\x2d\x2c\x2f\x2e\x29\x28\x2b\x2a\x24\x

ans=b'\x39\x32\x3e\x38\x03\x33\x41\x2b\x39\x0c\x0a\x18\x3e\x0d\x15\x2f\x23\x40\x44\x23\x1a\x14\x14\x41\

a=''
for i in ans:
    r=False
    for q in range(len(sa)):
        if sa[q]==i:
            a+=chr(s[q])
            r=True
            break
    if(not r):
        print('not found')
print(a)
```