《漏洞利用及渗透测试基础》实验报告

姓名：王亦辉 学号：2310764 班级：计科1班

**实验名称：**

OLLYDBG软件破解实验

**实验要求：**

**1.请在XP VC6生成课本第三章软件破解的案例(DEBUG模式，示例3-1）。进而，使用OllyDBG进行单步调试，获取verifyPWD函数对应flag==0的汇编代码，并对这些汇编代码进行解释。**

**2. 对生成的DEBUG程序进行破解，复现课本上提供的两种破解方法。**

**实验过程：**

1.flag == 0 对应汇编代码如下

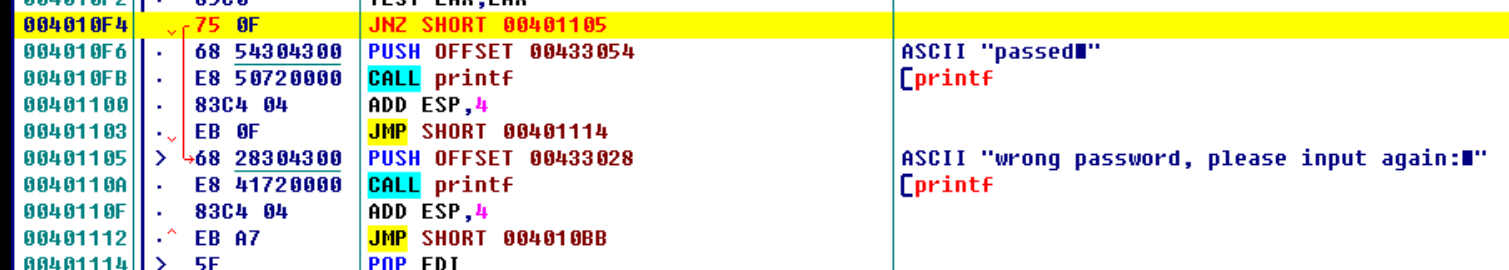
CMP DWORD PTR SS:[LOCAL.1],0

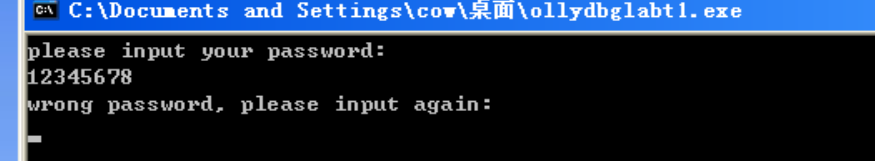
SETE AL

将flag 与0 对比。如果相等，AL会被设置为1；如果不等，AL会被设置为0.

2. 1. 第一种方法，改变分支跳转的逻辑，从而在密码错误时，跳入正确时的分支。

将JZ SHORT 00401105改成 JNZ SHORT 00401105

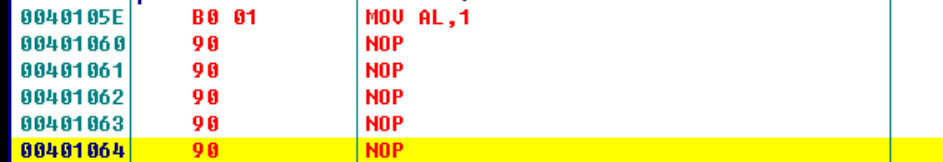




这样会在输入错误密码时，通过；输入正确密码时，不通过。

2. 第二种方法，改变验证函数的返回值，让它始终返回1.将这两行修改成直接设置AL寄存器为1，然后多余代码空间填充为NOP。这样，输入任何密码，都会通过。





**心得体会：**

由于可执行文件里，指令的地址都是写死的，所以我们修改汇编语句的时候，尽量不能增加或减少代码空间，应当使没被修改的语句的位置不改变。