OllyDBG 软件破解实验

姓名：汤清云 学号：2013536

实验步骤：

- 使用 OllyDBG 实现单步调试，获取 verifyPwd 函数的汇编代码，并且对代码做出解释
- 对生成的 debug 程序实现两种方式的破解

实验报告：

1. 获取 verifyPwd 汇编代码如下：

00401030 |> \55 push ebp 将主函数栈帧栈底值入栈

00401031 |. 8BEC mov ebp,esp 将主函数栈帧栈顶指针值赋给 ebp，即调整栈帧

00401033 |. 83EC 44 sub esp,44 将 esp 上调 44 字节，此时为 verifyPwd 栈顶

00401036 |. 53 push ebx 将 ebx 寄存器入栈

00401037 |. 56 push esi 将 esi 指针（源地址指针）入栈

00401038 |. 57 push edi 将 edi 指针（目的地址指针）入栈

00401039 |. 8D7D BC lea edi,[ebp-44] 相对寻址，将 esp 地址赋给 edi

0040103C |. B9 11000000 mov ecx,11 给 ecx 赋值 11，循环 11 次

00401041 |. B8 CCCCCCCC mov eax,CCCCCCCC 给 eax 赋值为 CCCCCCCC 即 int3 中断，用来初始化 verifyPwd 函数栈

00401046 |. F3:AB rep stos dword ptr [edi] 将 eax 的值拷贝到 edi 指向地址处，

00401048 |. 68 1C504300 push offset 0043501C 将字符串“12345678”地址入栈

0040104D |. 8B45 08 mov eax,dword ptr [ebp+8] 将栈基址寄存器 ebp＋8 所指向双字

栈单元值赋给 eax

00401050 |. 50 push eax eax 入栈

00401051 |. E8 DA710000 call strcmp 调用 strcmp 函数

00401056 |. 83C4 08 add esp,8 将 eax，字符串“12345678”出栈

00401059 |. 8945 FC mov dword ptr [ebp-4],eax 将 eax 的值赋给栈基址寄存器 ebp-4 所指向双字栈单元值

0040105C |. 33C0 xor eax,eax 清零 eax 的值

0040105E |. 837D FC 00 cmp dword ptr [ebp-4],0 比较 0 与栈基址寄存器 ebp-4 所指向双字栈单元值

00401062 |. 0F94C0 sete al 相等的话则将 al 置为 1

00401065 |. 5F pop edi 将 edi 指针（目的地址指针）出栈

00401066 |. 5E pop esi 将 esi 指针（源地址指针）出栈

00401067 |. 5B pop ebx 将 ebx 出栈

00401068 |. 83C4 44 add esp,44 将 esp 调回主函数栈帧栈顶处

0040106B |. 3BEC cmp ebp,esp 比较 esp 与 ebp 的值

0040106D |. E8 4E720000 call _chkesp 检查 esp 的值是否等于函数调用前的值，不相等则报错

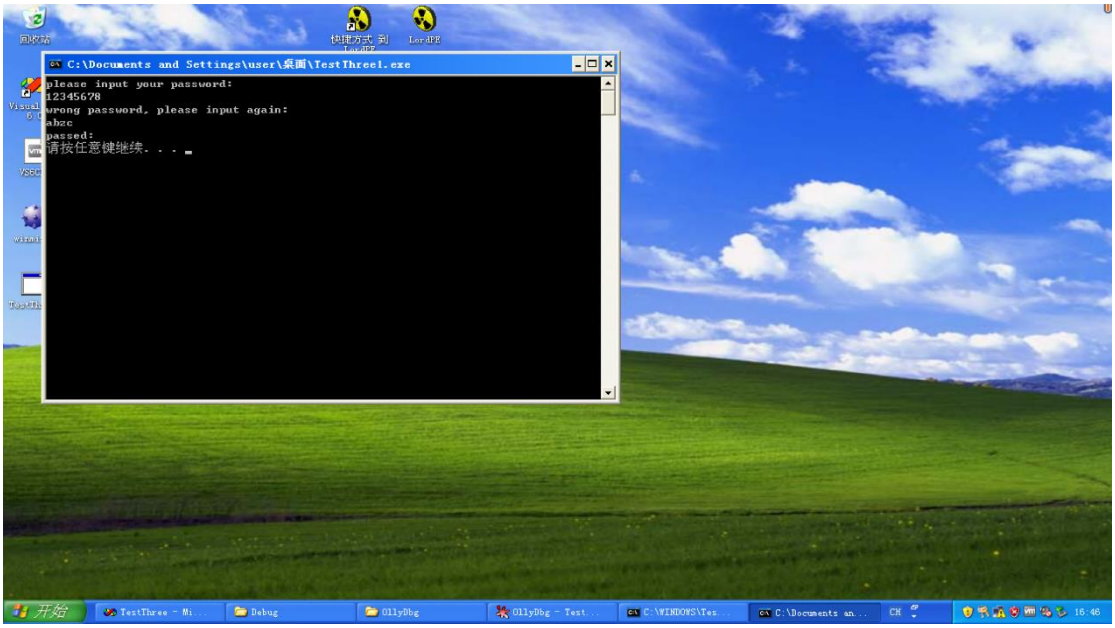
00401072 |. 8BE5 mov esp,ebp 将 ebp 的值赋给 esp

00401074 |. 5D pop ebp ebp 出栈，调整栈帧

00401075 \. C3 retn 返回主函数引用处

2. 使用两种方式破解 debug 程序结果图如下：

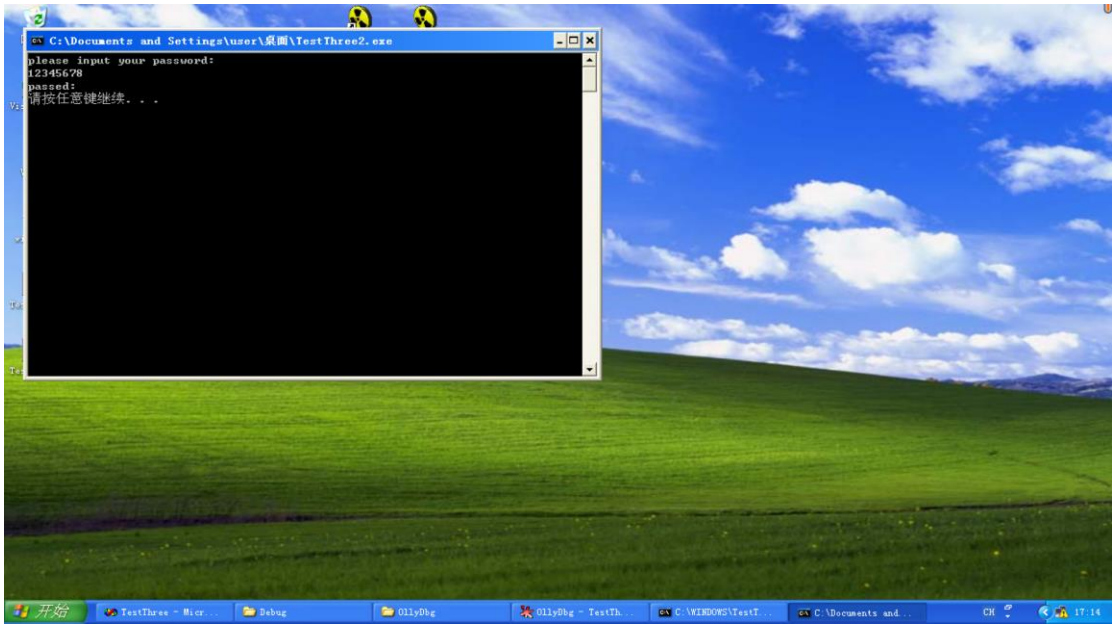
修改 jz short 00401105 为：jnz short 00401105 结果为：



（注：此处由于无法截图，在源代码中加入了 system(“pause”)命令，故有如上结果。）

修改 verifyPwd 函数汇编代码 al 值结果如下：

（注：此处由于无法截图，在源代码中加入了 system(“pause”)命令，故有如上结果。）



（注：此处由于无法截图，在源代码中加入了 system(“pause”)命令，故有如上结果。）