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

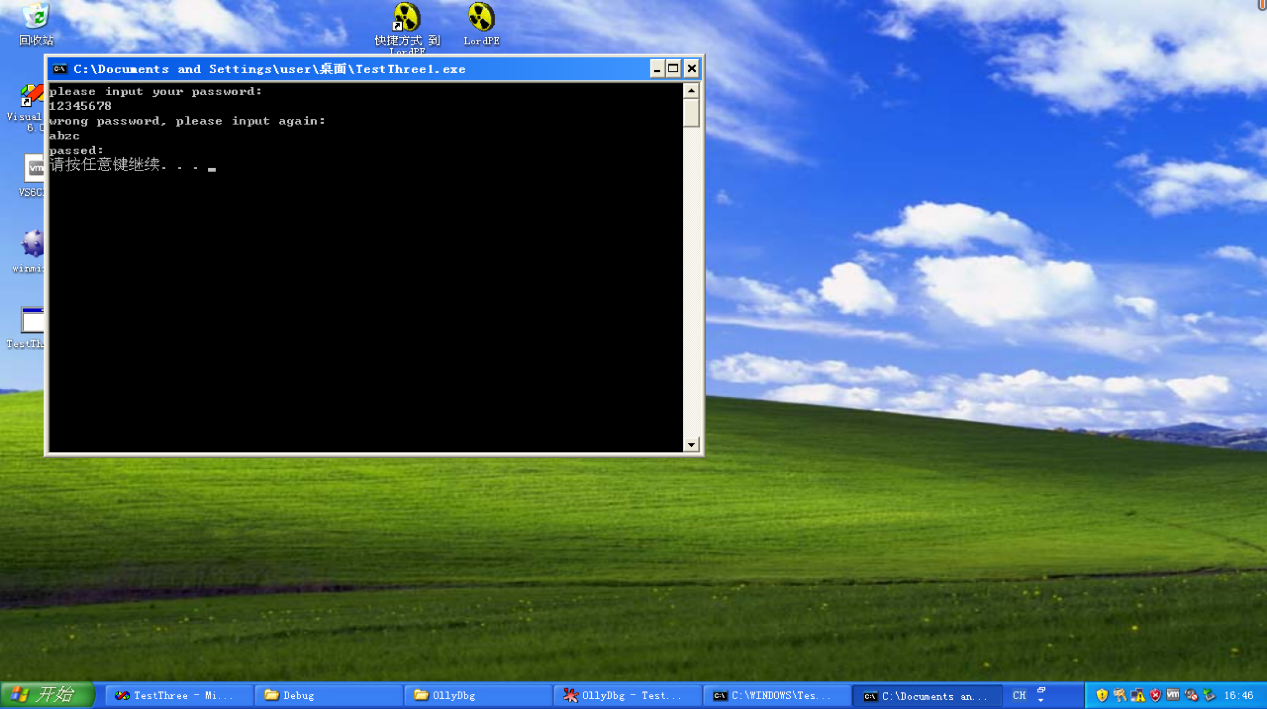
00401072 |. 8BE5 mov esp,ebp 将ebp的值赋给esp

00401074 |. 5D pop ebp ebp出栈，调整栈帧

00401075 \. C3 retn 返回主函数引用处

1. 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。）