

《漏洞利用及渗透测试基础》实验报告

林晖鹏 2312966

March 2025

1 实验名称

OLLYDBG 软件破解

2 实验要求

1. 请在 XP VC6 生成课程本第三章软件破解的案例（DEBUG 模式，示例 3-1）。进行时，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。

3 实验过程 1-Ollydbg 调试

3.1 生成 Debug 模式的 exe 文件

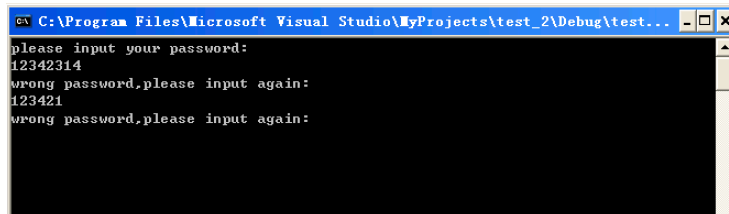


图 1: exe 程序

3.2 Ollydbg 打开 exe 文件

用 VS6 生成可执行文件之后，用 Ollydbg 打开该可执行文件，打开后如下图所示：

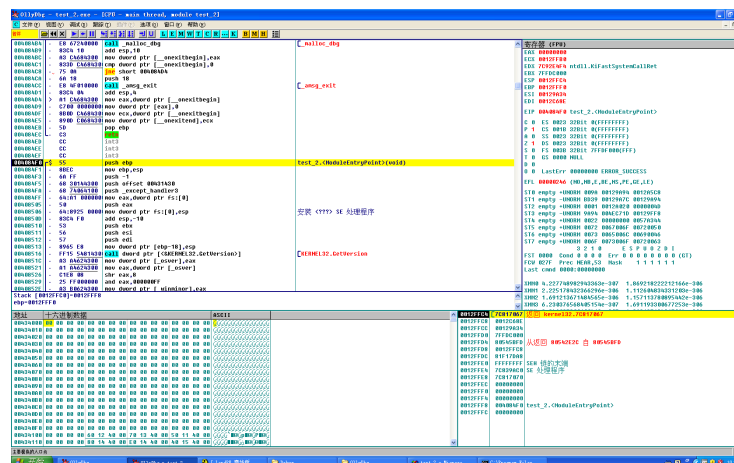


图 2: Ollydbg 打开 exe

3.3 获取 verifyPwd 函数的汇编代码

在 Ollydbg 中运行该文件，用 F2 或者工具栏里面的按钮进行单步调试，进入 verifyPwd 函数处，查看其汇编代码：

00401030	> 55	push ebp	test_2.verifyPwd(void)
00401031	- 88EC	mov ebp,esp	
00401033	- 83EC 44	sub esp,44	
00401036	- 53	push ebx	
00401037	- 56	push esi	
00401038	- 57	push edi	
00401039	- 8D7D BC	lea edi,[ebp-44]	
0040103C	- B9 11000000	mov ecx,11	
00401041	- B8 CCCCCCCC	mov eax,CCCCCCCC	
00401046	- F3:AB	rep stos dword ptr [edi]	
00401048	- 8B45 08	mov eax,dword ptr [ebp+8]	
0040104B	- 50	push eax	
0040104C	- 68 1C104300	push offset 0043101C	ASCII "12345678"
00401051	- E8 C8710000	call strcmp	[strcmp
00401056	- 83C4 08	add esp,8	
00401059	- 8945 FC	mov dword ptr [ebp-4],eax	
0040105C	- 33C0	xor eax,eax	
0040105E	- 837D FC 00	cmp dword ptr [ebp-4],0	
00401062	- 0F9AC0	sete al	
00401065	- 5F	pop edi	
00401066	- 5E	pop esi	
00401067	- 5B	pop ebx	
00401068	- 83C4 44	add esp,44	
0040106B	- 3BEC	cmp ebp,esp	
0040106D	- E8 3E720000	call _chkesp	
00401072	- 8BE5	mov esp,ebp	
00401074	- 5D	pop ebp	
00401075	- C3	ret	

图 3: verifyPwd 函数汇编代码

3.4 汇编代码解释

下面对这个函数的汇编代码进行解释，特别是对应 flag==0 的汇编代码处：

1	push ebp	
2	mov ebp,esp	
3	sub esp,44	
4	push ebx	
5	push esi	
6	push edi	
7	lea edi,[ebp-44]	
8	mov ecx,11	
9	mov eax,cccccccc	
10	rep stos dword ptr [edi]	
11	mov eax,dword ptr [ebp+8]	
12	push eax	
13	push offset 0043101C	
14	call strcmp	//进入比较函数
15	add esp,8	
16	mov dword ptr [ebp-4],eax	//将比较函数的返回值（存在 eax 中）赋值给 bFlag
17	xor eax,eax	//清空 eax 为 0
18	cmp dword ptr [ebp-4],0	//比较 bFlag 是不是为 0
19	sete al	//如果 cmp 结果为相等，则设置，否则不设置
20	pop edi	

```

21  pop esi
22  pop ebx
23  add esp,44
24  cmp ebp,esp
25  call _chkes
26  mov esp,ebp
27  pop ebp
28  ret

```

4 实验过程 2-复现破解案例

4.1 方法 1: 修改 bFlag 的返回值

思路： 希望将 verifyPwd 的返回值修改，固定返回值永远为 1，这样程序无论输入什么密码，都会显示正确并结束进程。

我们找到 verify 函数的汇编代码，上面实验分析已知，返回的是 al 的状态，这里我们直接把下面这部分代码

```

1  cmp dword ptr [ebp-4],0
2  sete al

```

修改为下图所示，直接把 al 的值赋值为 1，让返回值始终为 1。

<pre> . 0000 80 01 90 90 90 90 90 90 . </pre>	<pre> mov eax,ecx mov al,1 nop nop nop nop nop nop </pre>
---	---

图 4: way1

保存文件，并查看修改后的文件，如下图所示：

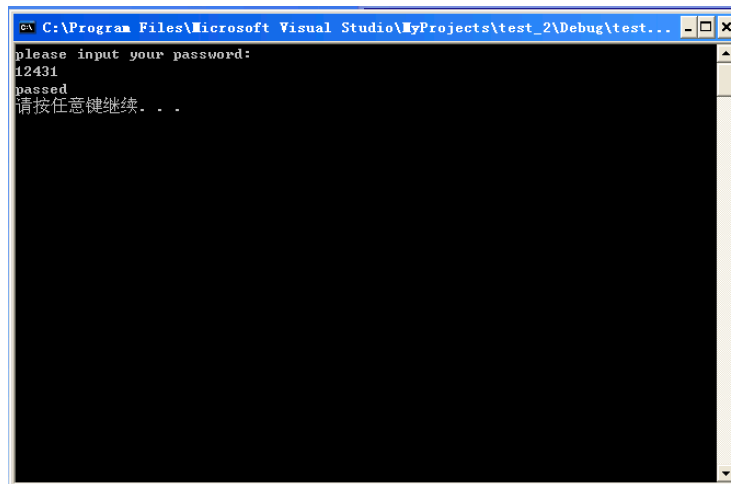


图 5: output1

4.2 方法 2: 判断处取反

思路: 希望将 if 判断结果修改, 对结果取反, 这样程序输入正确密码时显示错误, 而输入任何错误代码时都会显示正确并结束进程。

观察代码, 不难发现判断的核心代码在下面这部分, 当 `eax` 的值 (也就是 `flag`) 为 0 时, 会跳转到 `else` 的代码处 (00401105)。

```

1  test  eax, eax
2  jz     short 00401105

```

我们修改其代码, 将这里的 `jz` 改为 `jnz`, 表示如果上面的 `eax` 不是 0, 就跳转到 `else` 处, 正好与程序的正确功能相反。

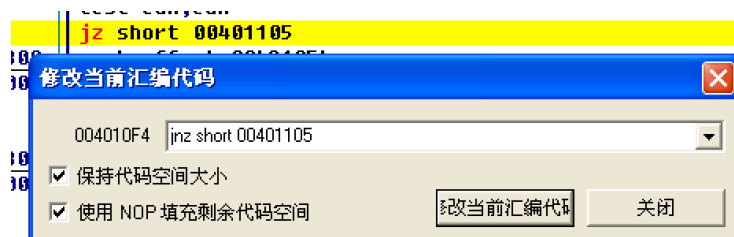


图 6: way2 修改

然后要保存这个修改后的文件, 打开这个破解文件, 结果如下图

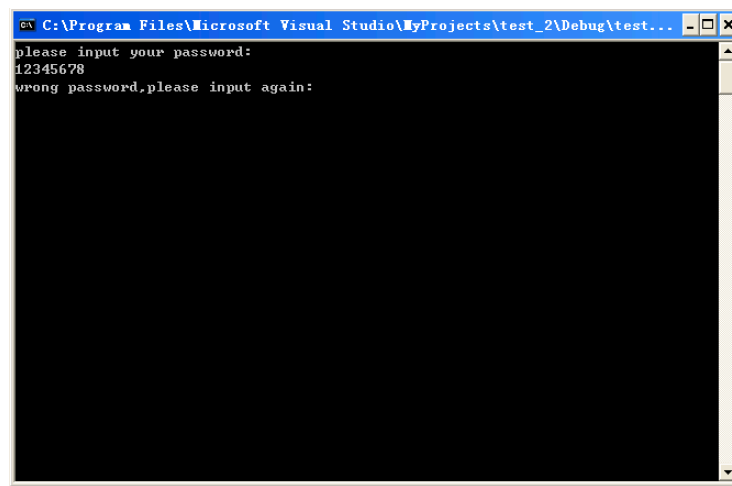


图 7: 方法二结果图

1.

5 心得体会

- 掌握了 Ollydbg 的使用方法，包括查找功能、调试功能、打断点等等，并且调试的过程中，进一步熟悉了汇编代码。
- 学习了两个破解文件的方法，扩展了关于破解文件并设置 bug 的思路，并且在过程中掌握了如何在汇编代码中修改代码并保存文件。