

课程报告模板

1、作业说明

说明：使用IDA或xldb逆向分析给定的exe程序。在命令行中运行程序，输入学号和key，实现成功打印：success

提交：必须以Markdown格式撰写报告，并导出PDF格式报告，以：“姓名-学号.pdf”格式命名，提交到学习通当中。

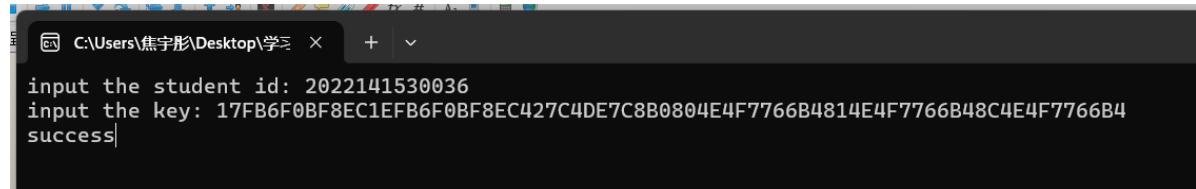
2、实验结果

输入的学号是：2022141530036

输入的key是：

17FB6F0BF8EC1EFB6F0BF8EC427C4DE7C8B0804E4F7766B4814E4F7766B48C4E4F7766B4

实验截图：



```
C:\Users\焦宇彤\Desktop\学习 > input the student id: 2022141530036
input the key: 17FB6F0BF8EC1EFB6F0BF8EC427C4DE7C8B0804E4F7766B4814E4F7766B48C4E4F7766B4
success
```

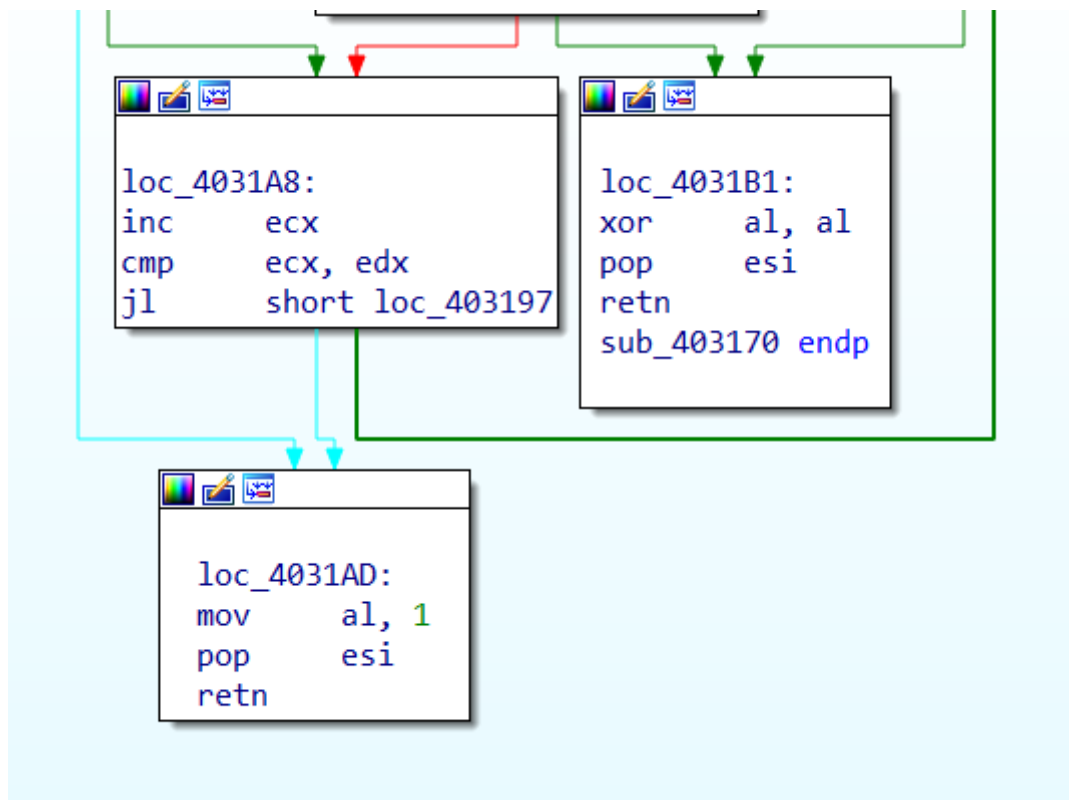
3、实验步骤解析

用IDA分析main代码，首先，要让al不为0，否则跳转到error代码段

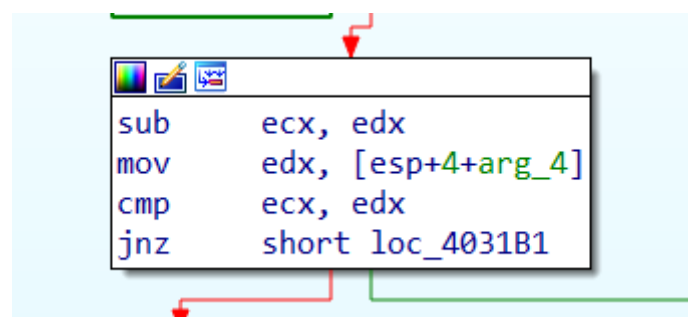


```
push    esi
call    sub_4015BE
add     esp, 28h
test    al, al
jz      loc_407C15
```

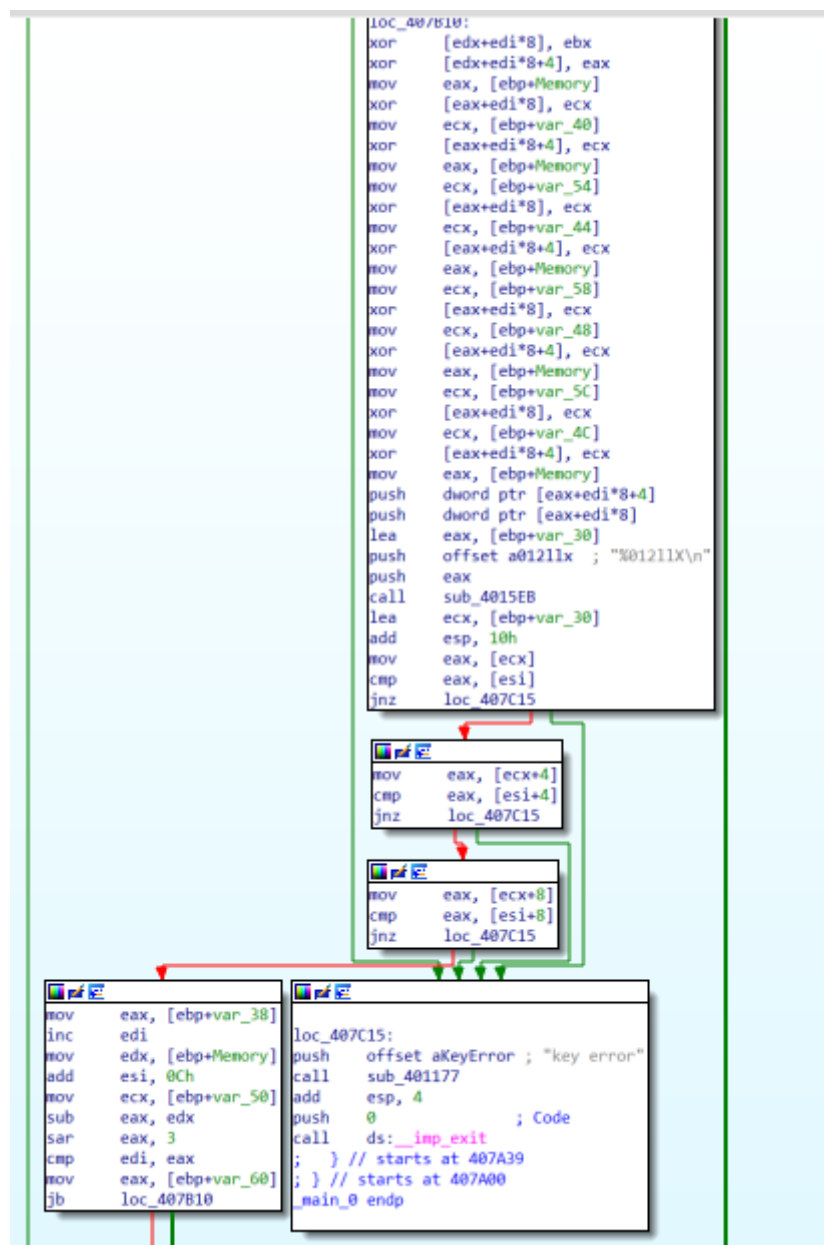
要知道al的值，逐步向上寻找，进入sub_函数，发现应该通过循环控制，控制在这段代码中最终al为1（走到最下面那个模块里）



分析这几段，发现ecx和edx必须相等，然后才进入循环，发现edx是个定值72，ecx随着输入变化而变化，是输入的长度



发现循环检查



运行到sub时，发现ecx是输入的长度，edx是4*16+8=72位，说明一共要输入72位

ECX	00000005	
EDX	00000048	'H'

输入72个A进行验证，发现可以通过这轮检验。

```

test    al, al
jne     assembleproject.9B3180
sub     ecx, edx
mov     edx, dword ptr ss:[esp+c]
cmp     ecx, edx
jne     assembleproject.9B31B1
xor     ecx, ecx
test    edx, edx
jle     assembleproject.9B31AD
mov     al, byte ptr ds:[ecx+esi]
cmp     al, 30

```

然后再往下看循环检验部分，最终要达成的目的就是【esi】（应该是输入的密码）=【eax】，所以继续动态调试

```

lea     ecx, [ebp+var_30]
add     esp, 10h
mov     eax, [ecx]
cmp     eax, [esi]
jnz     loc_B67C15

```

发现第一组密码17FB6F0BF8EC

Address	Disassembly	Comment
009B7B6F	83C4 10	add esp,10
009B7B72	8B01	mov eax,dword ptr ds:[ecx]
009B7B74	3B06	cmp eax,dword ptr ds:[esi]
009B7B76	0F85 99000000	jne assembleproject.9B7C15
009B7B7C	8B41 04	mov eax,dword ptr ds:[ecx+4]
009B7B7F	3B46 04	cmp eax,dword ptr ds:[esi+4]
009B7B82	0F85 8D000000	jne assembleproject.9B7C15
009B7B88	8B41 08	mov eax,dword ptr ds:[ecx+8]
009B7B8B	3B46 08	cmp eax,dword ptr ds:[esi+8]
009B7B8E	0F85 81000000	jne assembleproject.9B7C15
009B7B94	8B45 C8	mov eax,dword ptr ss:[ebp-38]
009B7B97	47	inc edi

同理得第二组为1EFB6F0BF8EC

<pre>mov eax,dword ptr ds:[ecx] cmp eax,dword ptr ds:[esi] jne assembleproject.9B7C15 mov eax,dword ptr ds:[ecx+4] cmp eax,dword ptr ds:[esi+4] jne assembleproject.9B7C15 mov eax,dword ptr ds:[ecx+8] cmp eax,dword ptr ds:[esi+8] jne assembleproject.9B7C15</pre>	<pre>ecx:"1EFB6F0BF8EC\n" esi:"17FB6F0BF8EC17FB6F0BF8EC17FB6F0BF8EC17FB6F0BF8EC17FB6F0BF8EC" ecx+4:"6F0BF8EC\n" esi+4:"6F0BF8EC17FB6F0BF8EC17FB6F0BF8EC17FB6F0BF8EC17FB6F0BF8EC" ecx+8:"F8EC\n" esi+8:"F8EC17FB6F0BF8EC17FB6F0BF8EC17FB6F0BF8EC17FB6F0BF8EC" main.cpp:71</pre>
---	--

共调试六轮，最终得最终密码为：

17FB6F0BF8EC1EFB6F0BF8EC427C4DE7C8B0804E4F7766B4814E4F7766B48C4E4F7766B4