

ctf.360.cn第二届，逆向部分writeup——第一题

转载

[weixin_34112181](#) 于 2014-11-26 12:04:37 发布 107 收藏
原文链接: <http://blog.51cto.com/cugou/1582721>
版权
题目: 见附件

这是个MFC程序，关于MFC调试有许多可以学习的地方，比如ALT+F9。希望有大牛能指导一二。

就这个题目来说，提示非常明确

提示：已限定为用户名为：strawberry。请分析该程序算法，得出该用户名所对应的Key

search for all referenced text strings

在找到的strawberry引用处00401456处下断点。

F8到004014d9，可以看到接下来的指令就是显示“success”or“Done”。

此时eax只想一串字符“K\$q*a_+@Xt”，这个就是key。

具体比较算法没有分析。

004014D7	.\xEB 05	JMP SHORT CrackMe.004014DE	
004014D9	> 1BC0	SBB EAX,EAX	
004014DB	. 83D8 FF	SBB EAX,-1	
004014DE	> 85C0	TEST EAX,EAX	
004014E0	. 6A 00	PUSH 0	
004014E2	. 6A 00	PUSH 0	
004014E4	.\x75 07	JNZ SHORT CrackMe.004014ED	
004014E6	. 68 E0A04400	PUSH CrackMe.0044A0E0	ASCII "success"
004014EB	.\xEB 05	JMP SHORT CrackMe.004014F2	
004014ED	> 68 D8A04400	PUSH CrackMe.0044A0D8	ASCII "Done"

```
EAX: 00963908 ASCII "K$q*a_+@Xt"
```

转载于:<https://blog.51cto.com/cugou/1582721>