**IDA介绍与快捷键的使用**

IDA 是一款功能强大的静态反汇编工具，可以帮助安全研究人员、黑客和软件开发人员理解和分析各 种编译 后的程序文件（如EXE、DLL、ELF等）。同时也拥有动态分析功能，可以跟踪运行时的程序行为。我 们新手

先学习IDA就足够了。

**快捷键**

静态反汇编快捷键：

Shift + F12 Ctrl + X

X G

ALT + T N

Ctrl + Z /

\ D A C U

Shift + E Ctrl + E R

Ctrl + k ALT + M Ctrl + M

ESC

//进入字符串窗口，所有字符串都在这 //可以知道那个函数引用了这个字符串 //查看函数在哪里被引用了 //将地址复制下来之后，如果想要回去，按G输入地址即可 //文本搜索

//修改函数、变量的名称 //撤销操作

//添加注释 //隐藏系统自己写上的注释 //转化为数据的形式 //转化为字符类型 //转化为汇编代码形式 //转化为原始的字节模式 //导出数据 //找到程序的起始位置 //将常量转化为单个字符

//打开函数的栈，查看用到了那些变量 //添加标记

//查看标记，双击跳转

//回退键，能够倒回上一部操作的视图（只有在反汇编窗口才是

这个作用，如果是在其他窗口按下esc，会关闭该窗口）

Tab //会从反汇编代码跳转到反汇编代码 Y //修改类型

动态调试快捷键：

**做题思路**

1、先找main函数

2、或者通过 Shift + F12 来查看字符串，了解大概的意思找到特殊的字符串（input，correct 等字样）双击

可以到达汇编的文本代码然后通过交叉引用 Ctrl + X 来查看那些函数引用了这个代码，也可以定 位到main函数

或其他重要函数

3、通过 F5 反汇编成我们看得懂的代码

4、然后看到下面的(\_DWORD \*)这个括号里面的是注释，我们可以右键点击"Hide casts"隐藏起 来，或者通过 \ 键

**使用IDA**

**最后**

IDA的入门使用在bilibli上有更加详细实操的教程，欢迎大家参考学习。

**bilibili视频教程**

[十分钟带你快速入门CTF逆向（保姆级教程）](https://www.bilibili.com/video/BV1n2tkeSEcx/?share_source=copy_web)