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
                   //进入字符串窗口, 所有字符串都在这
Ctrl + X
                   //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
Χ
                   //将地址复制下来之后,如果想要回去,按G输入地址即可
ALT + T
                   //文本搜索
                   //修改函数、变量的名称
N
Ctrl + Z
                   //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
D
                   //转化为字符类型
Α
C
                   //转化为汇编代码形式
                   //转化为原始的字节模式
U
Shift + E
                   //导出数据
Ctrl + E
                   //找到程序的起始位置
R
                   //将常量转化为单个字符
Ctrl + k
                   //打开函数的栈,查看用到了那些变量
ALT + M
                   //添加标记
                   //查看标记,双击跳转
Ctrl + M
                   //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
ESC
这个作用,如果是在其他窗口按下esc,会关闭该窗口)
                   //会从反汇编代码跳转到反汇编代码
Tab
Υ
                   //修改类型
```

动态调试快捷键:

快捷键	效果
F2	下断点
F7	单步步入 (进入子函数内部)
F8	单步步过 (不进入子函数内部)
F5	查看伪代码
F9	运行程序, 直到遇到断点或者程序结束
Esc	返回到跳转前的位置

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

使用IDA打开.

1.提示使用什么格式打开

Load a new fil	е				
Load file E:\第	三阶段\第三阶段代码\证	逆向知识\逆向知识	第一讲,IDA的熟悉使用,以及	GTEB, PEB结构\text\Release\text. exe	
Portable execu	table for 80386 (PE) [pe.ldw]			
MS-DOS execu	table (EXE) [dos.ldw]				
Binary file					
Processor type					
MetaPC (disasse	emble all opcodes) [m	etapc]		▼ Set	
			Analysis		
Loading <u>s</u> egment	0x00000000		▼ Enabled	Kernel options 1 Kernel options	
Loading o <u>f</u> fset	0x00000000		✓ Indicator enabled	Processor options	
Options					
Loading options			Load resources		
✓ Fill segment gaps			✓ Rename DLL entries		
✓ Create segn	nents		Manual load		
Create FLAT group			✓ Create imports segment		
Load as co	de segment				
		OK	Cancel Help		

因为是PE格式,所以我们选择PE即可.点击OK

2.重新打开一下



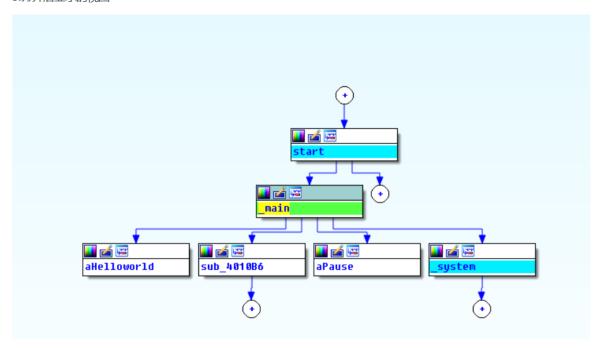
如果以前已经打开过这个PE,那么重新打开,则会显示这三个按钮,

1.overwrite 重新写入,代表覆盖以前的.(联系中常用这个,工作中不常用)

2.load existing 加载已经存在,这个很常用,因为有的时候汇编的注释很多,或者样本分析不会是一天完成,那么加载这个已经存在的即可.

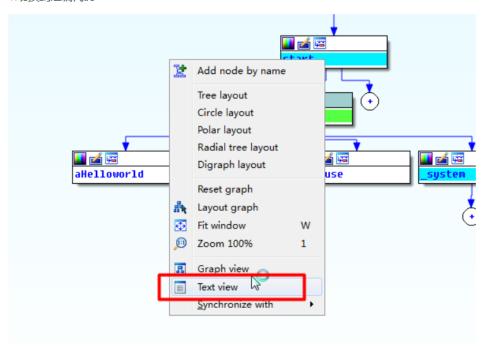
3.取消.

3.打开后显示的视图



我们不看这个,主要是看汇编代码.

1.切换到汇编代码



右键,点击Text View

2.查看汇编代码.

```
xt:00401000
xt:00401000
xt:00401000 _main
xt:00401000
                             offset aHelloworld ; "HelloWorld"
                       push
xt:00401005
                      call
                             sub_4010B6
                      push
                                          ; "pause"
xt:0040100A
                             offset aPause
xt:0040100F
                       call
                              system
xt:00401014
                       add
                             esp, 8
xt:00401017
                             eax, eax
                      xor
xt:00401019
                       retn
xt:00401019 _main
                      endp
xt:00401019
xt:00401019
```

这里有代码提醒功能,那么我们要学会怎么做,IDA是读取.sig文件,然后显示出来的.

那么我们更学全怎么做

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)