IDA使用指南

2018-04-08 | pwn |

0x01 前言

IDA之于逆向人员、PWN手的重要性几乎等同于左右手之于人。所以学好IDA是我们关键的一步。

0x02 基本快捷键

2.1 View

2.2 Jump

- Esc jump to previous position
- Ctrl+Enter jump to next postion

0x03 patch

以前逆向的时候，为了将有些部分的jz改为jnz，我们很可能会关闭IDA-gui，在UltraEdit中找到指定位置进行更改。这种操作十分麻烦，而且费时，所以产生了一下的方法！

1. **在IDA安装目录中，找到cfg/idagui.cfg，更改“ApplyPatches”改为1**

```
1  原来：
2  "ApplyPatches"          =       0           // apply patches to input file
3  现在
4  "ApplyPatches"          =       1           // apply patches to input file
```

2. 如果想patch某个代码段，在**IDA View窗口**将光标指向对应的汇编代码，这时会发现在**Hex View窗口** 中对应汇编代码的16进制会突出显示。**右键选择Edit（或者直接用F2）**，即可对目标代码进行更改；**最后右键选择Apply Changes（或者使用F2）** 即可完成更改
3. patch之后，你可以直接看到patch更改后对应的汇编代码，也能继续调试

3.1 Change byte

在Hex View窗口中右键更改

Edit->Patch Program ->Change byte

3.2 Change word

改字节 Edit->Patch Program ->Change word

3.3 Assemble

Edit->Patch Program ->Assemble

3.4 Apply patches to input file

Edit->Patch Program ->Apply patches to input file

0x04 Debug

4.1 远程调试

> 1. IDA 7.0给了很多远程调试器（dbgsrv文件夹下），只需要将与系统程序对应的server放到被调试的文件目录下即可。
> 2. 运行该server
> 3. 在IDA中启动对应的远程调试器，选择Debugger->Process Options，更改Application、Input File、Directory、Parameters、Hostname、Port、Password

4.2 调试快捷键

- F7 - step into
- F8 - step over
- F9 - start Process
- F4 - Run to Cursor
- Ctrl + F7 - Run until Return
- Ctrl + F2 - Terminate Process

4.3 Debug View

如果你调试过程序，你会发现调试窗口其实是一个独立的多窗口环境，这里面有IDA View-RIP，General registers，Hex View，Stack View，Output window，Python输入框

4.3.1 窗口布局

建议使用

```
{           [IDA View-RIP]                  } { [General registers] [Hex View] [St
{           output window
{Python [
```

4.3.2 IDA View-RIP

该窗口支持多种显示，其中有静态分析的跳转图(Graph View)，也有汇编文本(Text View)

所有调整都可以通过右键触发

调试　# ida

‹ 线性分析法　　shell之后的操作 ›