【看雪】第四课 静态分析技术

原创

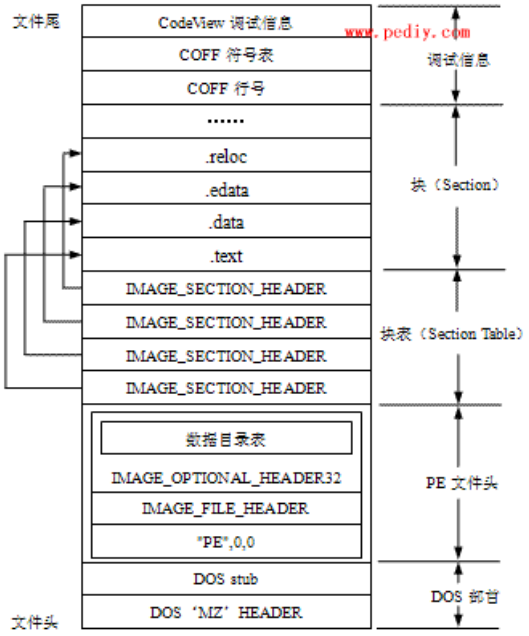
yeomanry 于 2010-02-03 10:21:00 发布 575 收藏
文章标签： 工具 microsoft windows 汇编 数据结构 磁盘

第四课 静态分析技术

所谓静态分析即从反汇编出来的程序清单上分析，从提示信息入手进行分析。目前，大多数软件在设计时，都采用了人机对话方式。所谓人机对话，即在软件运行过 程中，需要由用户选择的地方，软件即显示相应的提示信息，并等待用户按键选择。而在执行完某一段程序之后，便显示一串提示信息，以反映该段程序运行后的状态，是正常运行，还是出现错误，或者提示用户进行下一步工作的帮助信息。为此，如果我们对静态反汇编出来的程序清单进行阅读，可了解软件的编程思路，以便 顺利破解。 常用的静态分析工具有W32DASM、C32Asm和IDA Pro等。

4.1 认识PE格式

在Win32平台上（包括Windows 95/98/ME/NT/2000/XP/2003/CE），可执行文件是 PE（Portable Executable）格式。PE文件使用的是一个平面地址空间，所有代码和数据都被合并在一起，组成一个很大的结构。文件的内容被分割为不同的区块（Section，又称区段、节等），块中包含代码或数据。



PE 文件框架结构

刚接触这块的朋友只需要简单了解一下PE格式，更具体的PE格式请参考**脱壳基础知识入门（2006年版）**

PE相关名词解释如下：
1．入口点（Entry Point）
程序在执行时的第一行代码的地址应该就是这个值。

2．文件偏移地址（File Offset）
PE文件在磁盘上储存时，各数据的地址称文件偏移地址（File Offset）。用十六进制工具（例如Hex Workshop、WinHex等）打开 文件显示的地址就是文件偏移地址。

Hex Workshop、WinHex等）打开文件显示的地址就是文件偏移地址。

3．虚拟地址（Virtual Address，VA）
由于Windows程序是运行在386保护模式下，在保护模式下，程序访问存储器所使用的逻辑地址称为虚拟地址（Virual Address，VA）。 与实地址模式下的分段地址类似，虚拟地址也可写成"段：偏移量"的形式，这里的段是指段选择器。

4．基地址（ImageBase）
文件执行时将被映像到指定内存地址中，这个初始内存地址称为基址（ImageBase）。在Windows NT中，缺省的值是10000h；对于 DLLs，缺省值为400000h。在Windows 9x中，10000h不能用来装入32位的执行文件，因为该地址处于所有进程共享的线性地址区域， 因此Microsoft将Win32可执行文件的缺省基地址改变为400000h。

5．相对虚拟地址
相对虚拟地址（Relative Virual Address，RVA）表示此段代码在内存中相对于基地址的偏移。即：相对虚拟地址(RVA)=虚拟地 址（VA）-基址（ImageBase）。

4.2 虚拟地址和偏移量转换

在OllyDBG,IDA和W32Dasm下显示的地址值是虚拟地址（Virual Address，VA）。而十六进制工具里，如：Hiew、 Hex Workshop等显示的地址就是文件地址，称之为偏移量（File offset）。

其转换原理是因为PE文件在磁盘上的数据结构与在内存中的结构是一致的，如下图：

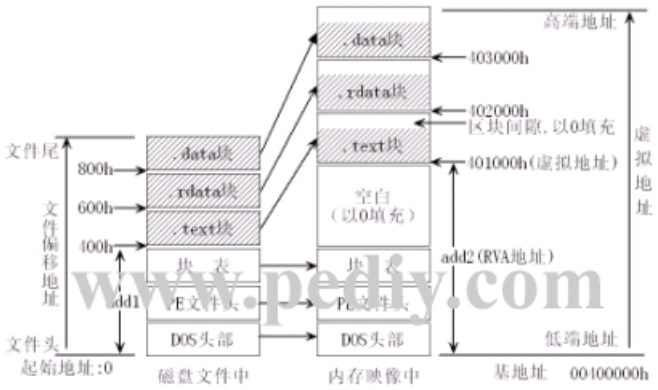
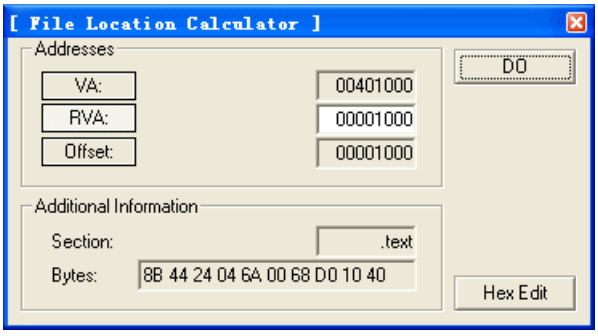


图 3.11 应用程序加载映射示意图

具体见：http://bbs.pediy.com/showthread.php?s=&threadid=18022

在实际操作时，使用 LordPE等工具很容易进行File offset与VA的转换。LordPE打开目标文件，点击FLC按钮，打开如下图的对 话框，填入相应地址，点击DO按钮即可转换：



4.3 文件类型分析

文件分析是静态分析程序的第一步，通过相关工具显示欲调试文件的信息，如它是用什么语言写的，是否加壳等。常用的文件分析工具有PEID，FileInfo等。有关壳的相关知识等入门后，再参考相关教学，如 **脱壳基础知**

识入门（2006年版） 。 如果查到文件有壳，此时静态分析是没意义的，但可以用OD动态调试，分析程序算法。

1.PEiD

PEiD的GUI界面操作非常方便直观。它的原理是利用查特征串搜索来完成识别工作的。各种开发语言都有固定的启动代码部分，利用这点就可识别出是何种语 言编编译的。同样，不同的壳也有其特征码，利用这点就可识别是被何种壳所加密。下面PEiD识别出这个软件是用Asprotect 1.2x加的壳。

2.FileInfo

FileInfo（简称Fi）另一款不错的文件检测工具。
FI的具体用法

4.4 W32Dasm简介

W32Dasm简介

4.5 IDA pro操作

IDA简易教程
IDA里的中文字串

4.6 keymaker内存注册机

Q：什么是某个软件的中段地址，指令长度，第一字节，这些数据怎么得到，这些数据在内存注册机中怎么应用？
A:
青色代表着注册码的保存模式
绿色的是中断地址，中断地址一般选择注册码保存模式的下一句，或下几句地址，但必须保证程 序中断到这个地址时注册码保存的值没有被任何东西修改或改变。如下面的例子，中断地址可以选在00401205和00401207，但不能选在 0040120C这个地址，因为00401207这个Call过后会修改eax的值。
红色的是中断的第一个字节
红色加上蓝色的字节就是指令长度，如下面的例 子选的中断地址是00401207，这个地址上有5个字节，所以指令长度是5

```
00401205    50          PUSH EAX        ;eax 中保存着真注册码
00401206    52          PUSH EDX        ; edx中保存着假注册码
```

00401207 E8 68 FF FF FF CALL 00401174 ; 比较真假注册码
0040120C 85 C0 TEST EAX,EAX ; 测试注册码真假结果
0040120E 75 42 JNZ SHORT 00401252 ; 假则跳向错误，真则不跳
（小虾回答）