汇编语言与逆向技术实验报告

Lab 3 peviewer

peviewer 程序的设计说明和控制流图

根据实验指导书上的实验要求：

> （1） 输入PE文件的文件名，peviewer程序调用Windows API函数，打开指定的PE文件；
>
> （2） 从文件的头部开始，读取IMAGE_DOS_HEADER结构中的e_magic和e_lfanew字段的值，按照实验演示的方式输出到命令行窗口；
>
> （3） 继续读取PE文件的IMAGE_NT_HEADER结构中的Signature字段的值，按照实验演示的方式输出到命令行窗口；
>
> （4） 继续读取IMAGE_NT_HEADER结构中的IMAGE_FILE_HEADER结构，从中读取出字段NumberOfSections、TimeDateStamp、Characteristics的值，按照实验演示的方式输出到命令行窗口；
>
> （5） 继续读取IMAGE_NT_HEADER结构中的IMAGE_OPTIONAL_HEADER结构，从中读取字段AddressOfEntryPoint、ImageBase、SectionAlignment、FileAlignment的值，按照实验演示的方式输出到命令行窗口；

结合实验指导书上给出的数据结构，不难得出需要读取需要的字段的地址的值。

- IMAGE_DOS_HEADER结构中的e_magic和e_lfanew字段分别位于相对于程序开始地址的 +0h 和 +3ch。
- e_lfanew字段保存了 PE 文件头开始的位置。需要跳到该地址开始读取 PE 文件头中的字段内容
- Signature 相对 PE 文件头开始地址 +0h
- NumberOfSections 相对 PE 文件头开始地址 +06h
- TimeDateStamp 相对 PE 文件头开始地址 +08h
- Characteristics 相对 PE 文件头开始地址 +16h
- AddressOfEntryPoint 相对 PE 文件头开始地址 +28h
- ImageBase 相对 PE 文件头开始地址 +34h
- SectioniAlignment 相对 PE 文件头开始地址 +38h
- FileAlignment 相对 PE 文件头开始地址 +3ch

具体文件操作也是参考实验指导书上的内容。

peviewer.asm 的源代码和注释

```
.386
.model flat , stdcall
option casemap :none
include .\masm32\include\windows.inc
include .\masm32\include\kernel32.inc
include .\masm32\include\masm32.inc
includelib .\masm32\lib\kernel32.lib
includelib .\masm32\lib\masm32.lib

.data
    txt_nl byte 0Dh, 0Ah, 0
```

```
    txt_tab byte "    ", 0
    txt_input byte "Please input a PE file: ", 0
    txt_image_dos_header byte "IMAGE_DOS_HEADER", 0
    txt_image_nt_header byte "IMAGE_NT_HEADER", 0
    txt_image_file_header byte "IMAGE_FILE_HEADER", 0
    txt_image_optional_header byte "IMAGE_OPTIONAL_HEADER", 0
    filename byte 10h dup(0), 0
    txt_e_magic byte "e_magic(single word): ", 0
    txt_e_lfanew byte "e_lfanew: ", 0
    txt_signature byte "Signature: ", 0
    txt_numberofsections byte "NumberOfSections(single word): ", 0
    txt_timedatestamp byte "TimeDateStamp: ", 0
    txt_characteristics byte "Characteristics(single word): ", 0
    txt_addressofentrypoint byte "AddressOfEntryPoint: ", 0
    txt_imagebase byte "ImageBase: ", 0
    txt_sectionalignment byte "SectionAlignment: ", 0
    txt_filealignment byte "FileAlignment: ", 0
    buf dword 20000h dup(0)
    hfile dword 0
    singleword word 0
.code
main proc
    invoke StdOut, addr txt_input
    invoke StdIn, addr filename, 10h
    invoke CreateFile, addr filename, GENERIC_READ, FILE_SHARE_READ,\
 0, OPEN_EXISTING, FILE_ATTRIBUTE_ARCHIVE, 0
    mov hfile, eax
    invoke SetFilePointer, hfile, 0, 0, FILE_BEGIN
    invoke ReadFile, hfile, addr buf, 400000, 0, 0
    mov eax, dword ptr buf;开头就是4D 5A 对应 MZ
    and eax, 0FFFFh;取低字
    ;invoke dw2hex, ax, addr singleword
    invoke dw2hex, eax, addr buf

    invoke StdOut, addr txt_image_dos_header
    invoke StdOut, addr txt_nl
    invoke StdOut, addr txt_tab
    invoke StdOut, addr txt_e_magic
    invoke StdOut, addr buf
    ;invoke StdOut, addr singleword
    invoke StdOut, addr txt_nl
    invoke StdOut, addr txt_tab
    invoke StdOut, addr txt_e_lfanew

    mov eax, dword ptr buf[3Ch];3Ch是e_lfanew在文件中的位置
    mov ebx, eax
    invoke dw2hex, eax, addr buf
    invoke StdOut, addr buf

    invoke StdOut, addr txt_nl
    invoke StdOut, addr txt_image_nt_header
    invoke StdOut, addr txt_nl
    invoke StdOut, addr txt_tab
    invoke StdOut, addr txt_signature

    mov eax, dword ptr buf[ebx];ebx存的是e_lfanew的值，是指向PE头文件的指针
    invoke dw2hex, eax, addr buf;PE头文件开始就存了signnature，值为4550h
    invoke StdOut, addr buf
```

```
invoke StdOut, addr txt_nl
;invoke StdOut, addr txt_tab
invoke StdOut, addr txt_image_file_header
invoke StdOut, addr txt_nl
invoke StdOut, addr txt_tab
invoke StdOut, addr txt_numberofsections

add ebx, 6h;PE头文件signnature的6字节之后存的就是NumberOfSections
mov eax, dword ptr buf[ebx]
and eax, 0FFFFh;取低字
invoke dw2hex, eax, addr buf
invoke StdOut, addr buf

invoke StdOut, addr txt_nl
invoke StdOut, addr txt_tab
invoke StdOut, addr txt_timedatestamp

add ebx, 2h;PE头文件NumberOfSections的2字节之后存的就是时间戳
mov eax, dword ptr buf[ebx]
invoke dw2hex, eax, addr buf
invoke StdOut, addr buf

invoke StdOut, addr txt_nl
invoke StdOut, addr txt_tab
invoke StdOut, addr txt_characteristics

add ebx, 0Eh;PE头文件时间戳的14字节之后存的就是characteristics
mov eax, dword ptr buf[ebx]
and eax, 0FFFFh;取低字
invoke dw2hex, eax, addr buf
invoke StdOut, addr buf

invoke StdOut, addr txt_nl
;invoke StdOut, addr txt_tab
invoke StdOut, addr txt_image_optional_header
invoke StdOut, addr txt_nl
invoke StdOut, addr txt_tab
invoke StdOut, addr txt_addressofentrypoint

sub ebx, 16h
add ebx, 28h; 第28h字节对应的是AddressOfEntryPoint
mov eax, dword ptr buf[ebx]
invoke dw2hex, eax, addr buf
invoke StdOut, addr buf

invoke StdOut, addr txt_nl
invoke StdOut, addr txt_tab
invoke StdOut, addr txt_imagebase

sub ebx, 28h
add ebx, 34h; 第34h字节对应的是ImageBase
mov eax, dword ptr buf[ebx]
invoke dw2hex, eax, addr buf
invoke StdOut, addr buf

invoke StdOut, addr txt_nl
invoke StdOut, addr txt_tab
```

```
    invoke StdOut, addr txt_sectionalignment

    add ebx, 4h;第38h字节对应的是SectionAlignment
    mov eax, dword ptr buf[ebx]
    invoke dw2hex, eax, addr buf
    invoke StdOut, addr buf

    invoke StdOut, addr txt_nl
    invoke StdOut, addr txt_tab
    invoke StdOut, addr txt_filealignment

    add ebx, 4h;第3Ch字节对应的是FileAlignment
    mov eax, dword ptr buf[ebx]
    invoke dw2hex, eax, addr buf
    invoke StdOut, addr buf

    invoke StdOut, addr txt_nl
    invoke CloseHandle, hfile
    ret
main endp
end main
```

peviewer.exe 运行截图

写好汇编代码，保存为 peviewer.asm。

将peviewer要读取的可执行文件放在本地目录。本次实验将对第一次汇编实验生成的命令行程序 hello.exe 进行读取。

在当前目录下打开命令提示符 CMD。

输入汇编命令`.\masm32\bin\ml /c /coff peviewer.asm`，对写好的汇编代码进行汇编，得到 peviewer.obj 文件。

```
D:\dyt\Studie\5Junior\D_Assemblersprache\Zuordnung\lab3>.\masm32\bin\ml  /c  /coff peviewer.asm
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997.  All rights reserved.

 Assembling: peviewer.asm

**********
ASCII build
**********
```

输入链接命令`.\masm32\bin\link /SUBSYSTEM:CONSOLE peviewer.obj`

```
D:\dyt\Studie\5Junior\D_Assemblersprache\Zuordnung\lab3>.\masm32\bin\link /SUBSYSTEM:CONSOLE peviewer.obj
Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.
```

在命令行运行程序 peviewer.exe，输入待读取的可执行文件名 hello.exe。实验结果如下，对比实验指导书上的实验，输出结果正确。

```
D:\dyt\Studie\5Junior\D_Assemblersprache\Zuordnung\lab3>peviewer.exe
Please input a PE file: hello.exe
IMAGE_DOS_HEADER
    e_magic(single word): 00005A4D
    e_lfanew: 000000B0
IMAGE_NT_HEADER
    Signature: 00004550
IMAGE_FILE_HEADER
    NumberOfSections(single word): 00000003
    TimeDateStamp: 6153A814
    Characteristics(single word): 0000010F
IMAGE_OPTIONAL_HEADER
    AddressOfEntryPoint: 00001000
    ImageBase: 00400000
    SectionAlignment: 00001000
    FileAlignment: 00000200
```