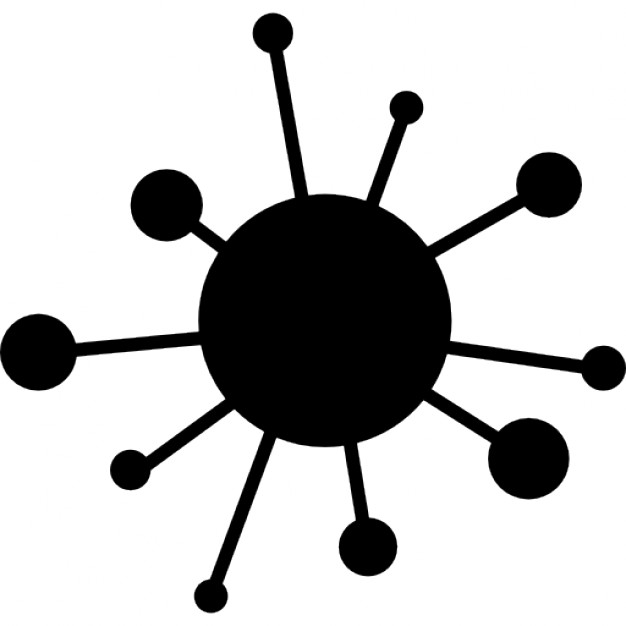
# 计算机病毒学

实验7 PE文件制作



学号：0x091395

姓名：uknowho

实验目的

1、 掌握PE格式可执行文件的结构。

2、 掌握PE格式可执行文件的设计原理。

3、 掌握PE格式可执行文件的生成方法。

4、 进一步熟悉debug、debug32的使用。

实验内容

1、得到系统文件mscdexnt.exe的磁盘存储分布图。

2、得到系统文件mscdexnt.exe内存中的运行分布图。

3、写入病毒代码，感染系统文件mscdexnt.exe，得到感染病毒XX的感染文件INFECTED.exe.

实验步骤

1. 通过平台软件获得“hello.exe”的磁盘数据映像。

表1 hello.ext磁盘文件存储结构

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 结构名称 | 起始偏移 | 长度 | 意义 |
| 1 | DOS残余头 | 0000h | 0040h | DOS文件头结构数据 |
| 2 | DOS文件体 | 0040h | 0070h | DOS执行程序与数据 |
| 3 | PE标准头 | 00B0h | 0017h | PE头结结构数据 |
| 4 | 可选头1 | 00C8h | 0061h | 不太清楚 |
| 5 | 可选头2 | 0128h | 0080h | 不太明了 |
|  | PE三段表 | 01A8h | 0078h | 0028h\*3 |
| 6 | PE文件段表 | 0400h | 0200h | .text数据 |
| 7 | 0600h | 0200h | .rdata数据 |
| 8 | 0800h | 0200h | .data数据 |
|  | user32.dll导入表 | 0610h | 0014h |  |
|  | user32.dll导入函数 | ？？ | ？？ | RAW地址=065C  MESSAGEBOXA() |
|  | kernal32.dll导入表 | 0624H | 0014H |  |
|  | kernal32.dll导入函数 |  |  | RAW地址=0676  ExitPreocess |

00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ 

00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ? @

00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000030 00 00 00 00 00 00 00 00 00 00 00 00 B0 00 00 00 ?

00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ? ???L?Th

00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno

00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS

00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode. $

00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000000A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000000B0 50 45 00 00 4C 01 03 00 98 67 F8 51 00 00 00 00 PE L 榞鳴

000000C0 00 00 00 00 E0 00 0F 01 0B 01 05 0C 00 02 00 00 ?

000000D0 00 04 00 00 00 00 00 00 00 10 00 00 00 10 00 00

000000E0 00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00 @

000000F0 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00

00000100 00 40 00 00 00 04 00 00 00 00 00 00 02 00 00 00 @

00000110 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00

00000120 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00

00000130 10 20 00 00 3C 00 00 00 00 00 00 00 00 00 00 00 <

00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00000180 00 00 00 00 00 00 00 00 00 20 00 00 10 00 00 00

00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000001A0 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00 .text

000001B0 27 00 00 00 00 10 00 00 00 02 00 00 00 04 00 00 '

000001C0 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 `

000001D0 2E 72 64 61 74 61 00 00 92 00 00 00 00 20 00 00 .rdata ?

000001E0 00 02 00 00 00 06 00 00 00 00 00 00 00 00 00 00

000001F0 00 00 00 00 40 00 00 40 2E 64 61 74 61 00 00 00 @ @.data

第2扇区，data结构数据后半部分------------------------------------------------------------------------

00000200 24 00 00 00 00 30 00 00 00 02 00 00 00 08 00 00 $ 0

00000210 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0 @ ?

00000220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

（全零区域）

000003F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

第3扇区 .text段，程序运行入口点-----------------------------------------------------------------------

00000400 6A 00 68 10 30 40 00 68 00 30 40 00 6A 00 E8 08 j h 0@ h 0@ j ?

00000410 00 00 00 6A 00 E8 07 00 00 00 CC FF 25 08 20 40 j ? ?% @

00000420 00 FF 25 00 20 40 00 00 00 00 00 00 00 00 00 00 % @

00000430 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

（全零区域）

000005F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

第4扇区 .rdata段---------------------------------------------------------------------------------------

00000600 76 20 00 00 00 00 00 00 5C 20 00 00 00 00 00 00 v \

00000610 54 20 00 00 00 00 00 00 00 00 00 00 6A 20 00 00 T j

00000620 08 20 00 00 4C 20 00 00 00 00 00 00 00 00 00 00 L

00000630 84 20 00 00 00 20 00 00 00 00 00 00 00 00 00 00 ?

00000640 00 00 00 00 00 00 00 00 00 00 00 00 76 20 00 00 v

00000650 00 00 00 00 5C 20 00 00 00 00 00 00 B1 01 4D 65 \ ?Me

00000660 73 73 61 67 65 42 6F 78 41 00 75 73 65 72 33 32 ssageBoxA user32

00000670 2E 64 6C 6C 00 00 9B 00 45 78 69 74 50 72 6F 63 .dll ?ExitProc

00000680 65 73 73 00 6B 65 72 6E 65 6C 33 32 2E 64 6C 6C ess kernel32.dll

00000690 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

（全零区域）

000007F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

第5扇区 .data数据--------------------------------------------------------------------------------------

00000800 48 6F 6C 61 20 4D 69 20 61 6D 69 67 6F 21 00 00 Hola Mi amigo!

00000810 32 30 31 34 34 36 37 35 21 20 20 20 20 20 20 20 20144675!

00000820 69 6F 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 ion

00000830 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

（全零区域）

000009F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

1. 对获得的磁盘数据进行数据分析

例如表1

1. 加载hello.exe后内存逻辑空间数据映像分析。

表2 hello.exe内存分布

|  |  |  |  |
| --- | --- | --- | --- |
| 虚拟地址偏移量 | 分配长度 | 实际长度 | 逻辑空间分布 |
| 0ADD0000 | 1000H | 220H | 0000🡪文件头部 |
| 0ADD1000 | 1000H | 27H | 0400🡪.text |
| 0ADD2000 | 1000H | 92H | 0600🡪.rdata |
| 0ADD3000 | 1000H | 24H | 0800🡪.data |

Debug hello.exe 与 winhex数据不一致。遂….

4、PE版“Hello”可执行文件的制作过程。附录A给出了设计操作过程，设计原理请参考附录B。

5、画出hello.exe使用的导入表结构。

6、总结实验数据及过程，写出实验报告。

**附录A PE版HELLOWORLD 2.0制作过程**

hello.txt的内容：

F 1000 L0A00 00

E 1000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00

E 1010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

E 1030 00 00 00 00 00 00 00 00 00 00 00 00 B0 00 00 00

E 1040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68

E 1050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F

E 1060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20

E 1070 6D 6F 64 65 2E 0D 0D 0A 24

E 10B0 50 45 00 00 4C 01 03 00 98 67 F8 51 00 00 00 00

E 10C0 00 00 00 00 E0 00 0F 01 0B 01 05 0C 00 02 00 00

E 10D0 00 04 00 00 00 00 00 00 00 10 00 00 00 10 00 00

E 10E0 00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00

E 10F0 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00

E 1100 00 40 00 00 00 04 00 00 00 00 00 00 02 00 00 00

E 1110 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00

E 1120 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00

E 1130 10 20 00 00 3C 00 00 00 00 00 00 00 00 00 00 00

E 1180 00 00 00 00 00 00 00 00 00 20 00 00 10 00 00 00

E 11A0 00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00

E 11B0 27 00 00 00 00 10 00 00 00 02 00 00 00 04 00 00

E 11C0 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60

E 11D0 2E 72 64 61 74 61 00 00 92 00 00 00 00 20 00 00

E 11E0 00 02 00 00 00 06 00 00 00 00 00 00 00 00 00 00

E 11F0 00 00 00 00 40 00 00 40 2E 64 61 74 61 00 00 00

E 1200 24 00 00 00 00 30 00 00 00 02 00 00 00 08 00 00

E 1210 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 C0

E 1400 6A 00 68 10 30 40 00 68 00 30 40 00 6A 00 E8 08

E 1410 00 00 00 6A 00 E8 07 00 00 00 CC FF 25 08 20 40

E 1420 00 FF 25 00 20 40 00

E 1600 76 20 00 00 00 00 00 00 5C 20 00 00 00 00 00 00

E 1610 54 20 00 00 00 00 00 00 00 00 00 00 6A 20 00 00

E 1620 08 20 00 00 4C 20 00 00 00 00 00 00 00 00 00 00

E 1630 84 20 00 00 00 20 00 00 00 00 00 00 00 00 00 00

E 1640 00 00 00 00 00 00 00 00 00 00 00 00 76 20 00 00

E 1650 00 00 00 00 5C 20 00 00 00 00 00 00 B1 01 4D 65

E 1660 73 73 61 67 65 42 6F 78 41 00 75 73 65 72 33 32

E 1670 2E 64 6C 6C 00 00 9B 00 45 78 69 74 50 72 6F 63

E 1680 65 73 73 00 6B 65 72 6E 65 6C 33 32 2E 64 6C 6C

E 1800 48 6F 6C 61 20 4D 69 20 61 6D 69 67 6F 21 00

E 1810 32 30 31 34 34 36 37 35 21 20 20 20 20 20 20 20

E 1820 69 6F 6E 00

N c:\hello.dat

R BX

0

R CX

0A00

W 1000

Q

1. 获得制作好hello.txt文件。

⑵ 执行debug的批处理文件hello.txt获得hello.dat文件：

debug < hello.txt

⑶ 复制hello.dat获得hello.exe文件：

copy hello.dat hello.exe

⑷ 运行hello.exe文件，可以看到在窗口中显示的字符串“Hola Mi amigo！”：

