第 3 章

计算机病毒

本章学习目标

- 掌握计算机病毒的概念
- 了解常见的计算机病毒
- 掌握计算机病毒的特征
- 熟悉计算机病毒的危害及防护措施
- 了解计算机病毒的工作原理
- 掌握计算机病毒的分类
- 掌握冰河木马程序的使用

3.1 计算机病毒概述

3.1.1 计算机病毒的概念

“计算机病毒”的概念最初来源于 20 世纪 70 年代美国作家雷恩出版的《P1 青春》一书。世界上公认的第一个在个人计算机上广泛流行的病毒是 1987 年诞生的大脑(C-Brain)病毒,这个病毒程序是由一对巴基斯坦兄弟巴斯特和阿姆捷特所写。他们在当地经营一家贩卖个人计算机的商店,由于当地盗拷软件的风气非常盛行,为了防止软件被任意盗拷,他们编写了该病毒程序。只要有人盗拷他们的软件,C-Brain 就会发作,将盗拷者的剩余硬盘空间给“吃掉”。

计算机病毒是编制者在计算机程序中插入的破坏计算机功能或者数据、影响计算机使用并能自我复制的一组计算机指令或程序代码。计算机病毒不但会破坏计算机软件,也会损坏计算机硬件,如破坏计算机操作系统、损坏计算机硬盘等。它有独特的复制能力,可以很快地蔓延,又常常难以根除。

计算机病毒一般不独立存在,而是隐蔽在其他可执行的程序之中。计算机感染病毒后,轻则影响机器运行速度,破坏系统,导致系统死机,重则盗取用户隐私(如账号信息)、加密用户文件,从而导致经济损失,甚至导致系统瘫痪。

计算机病毒有自己的传输模式和不同的传输路径。通常有以下 3 种传输方式。

(1) 通过移动存储设备传播:如 U 盘、移动硬盘等。移动存储设备能成为病毒传播的路径,是因为它们经常被移动和使用。它们更容易得到计算机病毒的青睐,成为计算机病毒的携带者。

(2) 通过网络传播：随着网络技术的发展，计算机病毒可以方便地通过网络传播，并且传播速度也越来越快。

(3) 利用计算机系统和应用软件的弱点传播：越来越多的计算机病毒利用计算机系统和应用软件的弱点来传播。

下面介绍几款典型的计算机病毒。

1. CIH 病毒

1998 年开始爆发的 CIH 病毒，被认为是有史以来第一款在全球范围内造成巨大破坏的计算机病毒，该病毒导致无数计算机的数据遭到破坏。CIH 病毒属于文件型病毒，其别名有 Win95.CIH、Spacefiller、Win32.CIH、PE_CIH，是陈盈豪编写的，主要感染 Windows 95、Windows 98 下的可执行文件。其发展过程经历了 v1.0、v1.1、v1.2、v1.3、v1.4 几个版本。

CIH 病毒的文件长度虽然只有 1KB，但因它写入的是文件的空闲区，人们很难从外表观察到文件内容的增加。CIH 病毒不但可以感染可执行文件，真正可怕的是该病毒可以直接攻击、破坏计算机的硬件设备(如通过清除主板 Flash ROM 中的信息导致主板不能正常使用)。该病毒每月 26 日都会爆发(有一种版本是每年 4 月 26 日爆发)。CIH 病毒感染后的症状如图 3.1 所示。

图 3.1　CIH 病毒感染后的症状

2. 莫里斯蠕虫

蠕虫也是一种计算机程序，它的特点是可以独立存在和运行。蠕虫的目的是反复复制自身，从而消耗计算机内存及网络系统资源。

1998 年 11 月 2 日，是一个令计算机界震惊的日子。在这之前，人们很少注意蠕虫程序。这一天，美国康奈尔大学研究生罗伯特·塔潘·莫里斯编写并传播取名为 Internet Worm 的程序。美国东部时间下午 5 点，美国康奈尔大学的计算机系统突然降低了速度，当时该大学的计算机是美国乃至全世界最先进的计算机系统，一般情况下，即使所有终端全部运行，也不会对计算机系统运行造成太大的影响。当时使用计算机的工作人员就此事立即向计算机系统管理中心咨询，管理中心人员发现此特异情况，并开始着手调查。计

算机系统专用检测软件发现系统内多了一小段能自我复制、并占用系统资源堵塞系统通道的小程序——后来被计算机专家称为“蠕虫”。令人始料不及的是,“蠕虫”以闪电般的速度复制,大量繁殖,不到 10 小时就从美国东海岸传输到西海岸,使众多的美国军用计算机网络受到侵犯。

莫里斯蠕虫(Morris worm)是一小段程序,它采用截取口令,并在系统中试图做非法动作的方式直接攻击计算机系统。蠕虫与一般的计算机病毒不同,它并不是通过自身复制附加到其他程序中的方式来复制自己,而是借助系统的缺陷进行破坏。它窃取口令字,然后伪装成一个合法用户复制甚至发送到远处的另外一台终端上,结果导致蠕虫不受控制地疯狂复制,致使占当时互联网计算机通信网络 10%、大约 6000 多台终端受到感染并瘫痪。

应该说,计算机界对计算机病毒的重新认识并极为重视就从莫里斯蠕虫病毒开始,人们开始认识到病毒的危害。莫里斯蠕虫事件引起了巨大的混乱,也有一些好的作用,它改变了人们对系统弱点的看法。莫里斯蠕虫事件促使美国军方组建了计算机紧急反应小组(computer emergency response team,CERT),以应付此类事件,也促使时任美国总统的里根签署了《计算机安全法令》。

3. 梅丽莎病毒

梅丽莎病毒(Melissa virus)是通过微软公司的 Outlook 电子邮件软件向用户通讯簿名单中的 50 位联系人发送邮件来传播自身。该邮件包含一句话:“这就是你请求的文档,不要给别人看”,此外夹带一个 Word 文档附件。单击这个文件,就会使病毒感染主机并进行自我复制。

梅丽莎病毒 1999 年 3 月爆发,尽管这种病毒不会删除计算机系统文件,但它引发的大量电子邮件会阻塞电子邮件服务器,使之瘫痪。病毒传播速度之快令英特尔公司、微软公司以及其他许多使用 Outlook 软件的公司措手不及。为了防止损失,它们被迫关闭整个电子邮件系统。

4. 爱虫病毒

2000 年 5 月 4 日,爱虫病毒(I Love You)开始在全球迅速传播。该病毒通过 Outlook 电子邮件系统传播,邮件的主题为 I Love You,并包含附件 Love-Letter-for-you.txt.vbs,如图 3.2 所示。打开病毒附件后,该病毒会自动向通讯簿中的所有电子邮件地址发送病毒邮件副本,阻塞邮件服务器,同时感染扩展名为 vbs、hta、jpg、mp3 等文件。

图 3.2 发送邮件传播爱虫病毒

爱虫病毒通过 Outlook 传播，打开病毒邮件附件，使用者会观察到计算机的硬盘灯不停闪烁，系统速度显著变慢，计算机中出现大量扩展名为 vbs 的文件。所有快捷方式被改变为与系统目录下 w.exe 文件建立关联，进一步消耗系统资源，造成系统崩溃。

5. 红色代码病毒

红色代码(code red)是一种计算机蠕虫病毒，能够通过网络服务器和互联网传播。2001 年 7 月，红色代码病毒感染运行 Microsoft IIS Web 服务器的计算机。它采用了一种叫作“缓冲区溢出”的黑客技术，利用微软 IIS 的漏洞进行病毒的感染和传播。

被它感染后，遭受攻击主机发布的网络站点会显示 Welcome to http://www.worm.com!，如图 3.3 所示。随后，病毒便会主动寻找其他易受攻击的主机进行感染。不到一周，该病毒感染了近 40 万台服务器。

6. 冲击波病毒

冲击波病毒(Worm.Blaster)是利用微软公司在 2003 年 7 月 21 日公布的 RPC 漏洞传播的，该病毒于当年 8 月爆发。病毒运行时会不停地利用扫描技术寻找网络上安装操作系统为 Windows 2000 以及 Windows XP 的计算机，找到后就利用 DCOM/RPC 缓冲区漏洞攻击该系统，一旦攻击成功，病毒体便会被传送到对方计算机中进行感染，使系统操作异常、不停重启甚至导致系统崩溃。具体感染冲击波病毒的症状如图 3.4 所示。

图 3.3　感染红色代码病毒的症状

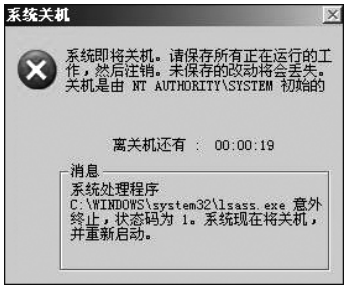

图 3.4　感染冲击波病毒的症状

另外，该病毒还会对系统升级网站进行拒绝服务攻击，导致用户无法通过该网站升级系统。只要是计算机上有 RPC 服务并且没有打安全补丁的计算机都存在 RPC 漏洞。具体涉及的操作系统有 Windows 2000、Windows XP、Windows Server 2003、Windows NT 4.0。

7. 巨无霸病毒

2003 年出现的巨无霸病毒(Worm.Sobig)通过局域网传播，该病毒通过查找局域网上的所有计算机，并试图将自身写入网络中计算机的启动目录中，从而使计算机自动启动该病毒程序。该病毒一旦运行，在计算机联网的状态下，每隔两小时就会到某一指定网址自动下载病毒，同时会查找计算机中所有的邮件地址，并向这些地址发送标题为 Re: Movies、Re: Sample、Re: Details 等字样的病毒邮件，从而进行邮件传播，如图 3.5 所示。该病毒还会将用户的隐私发到指定的邮箱。由于邮件内容的一部分是来自于被感染计算机中的资料，因此有可能泄露用户的机密文件。

8. 震荡波病毒

2004 年 5 月 1 日，震荡波病毒(Worm.Sasser)在网络上出现，该病毒是通过微软高危

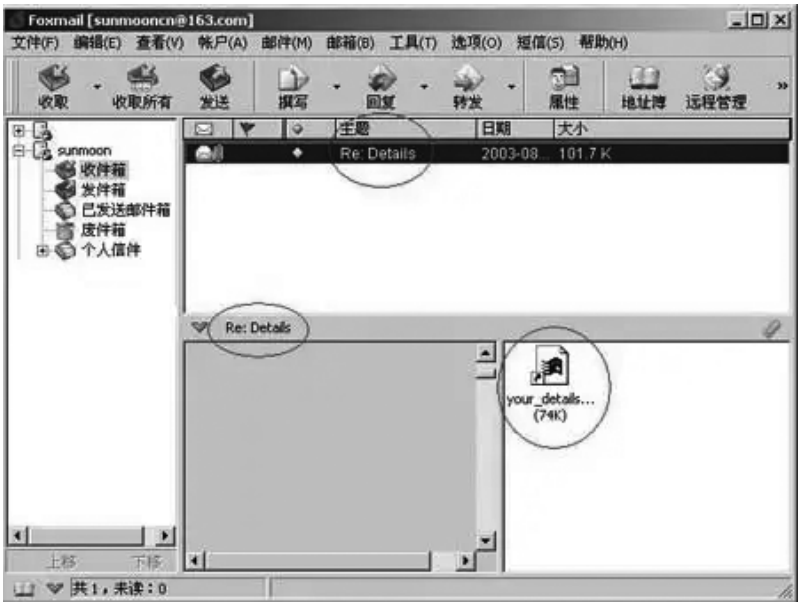

图 3.5　巨无霸病毒通过邮件传播

漏洞——LSASS 漏洞(微软 MS04-011 公告)传播，感染病毒的计算机会出现系统反复重启、机器运行缓慢，出现系统异常的出错框等现象。

震荡波病毒感染的系统包括 Windows 2000、Windows Server 2003 以及 Windows XP，病毒运行后会巧妙地将自身复制为%WinDir%\napatch.exe。该病毒随机在网络上搜索机器，并向远程计算机的 445 端口发送包含后门程序的非法数据。远程计算机如果存在 MS04-011 漏洞，将会自动运行后门程序，打开后门端口 9996。

9. 熊猫烧香病毒

熊猫烧香病毒是由李俊制作并肆虐网络的一款计算机病毒，在 2006 年年底开始大规模爆发。它是一款拥有自动传播、自动感染硬盘能力和强大的破坏能力的病毒，感染系统中的 *.exe、*.com、*.html、*.asp、*.pif 文件，导致用户一打开这些网页文件，IE 自动连接到指定病毒网址下载病毒，在硬盘各分区下生成文件 autorun.inf 和 setup.exe。病毒还可以通过 U 盘和移动硬盘传播，并且利用 Windows 系统的自动播放功能来运行。

熊猫烧香病毒还会修改注册表启动项，被感染的文件图标变成“熊猫烧香”的图案，如图 3.6 所示。病毒还可以通过共享文件夹、系统弱口令等多种方式传播。

10. 网游大盗

网游大盗(爆发于 2007 年)是一款专门盗取网络游戏账号和密码的病毒，该病毒属于木马病毒，可以从指定的网址下载木马病毒或其他恶意软件，还可以通过网络和移动存储介质传播。当系统接入互联网，会将盗取的用户账号、密码等信息发送到指定的邮箱或指定的远程服务器的 Web 站点中，最终导致网络游戏玩家无法正常运行游戏，蒙受不同程度的经济损失。

11. 勒索病毒

勒索病毒是通过锁定被感染者计算机的系统或文件，并施以敲诈勒索的新型计算机

图 3.6　熊猫烧香病毒

病毒，通过计算机漏洞、邮件投递、恶意木马程序、网页后门等方式进行传播。一旦感染，磁盘上几乎所有格式的文件都会被加密，造成企业、学校和个人用户的大量重要文件无法使用甚至外泄，严重影响日常工作和生活。感染勒索病毒的计算机如图 3.7 所示。

图 3.7　勒索病毒

2017 年 5 月，一种名为“想哭”的勒索病毒袭击全球 150 多个国家和地区，影响领域包括政府部门、医疗服务、公共交通、邮政、通信和汽车制造业。2017 年 6 月，欧洲、北美地区多个国家遭到 NotPetya 勒索病毒攻击，乌克兰受害严重，影响领域包括政府部门、国有企业。2017 年 10 月，俄罗斯、乌克兰等国遭到勒索病毒“坏兔子”攻击，影响领域包括

乌克兰敖德萨国际机场、首都基辅的地铁支付系统以及俄罗斯的三家媒体。随后德国、土耳其等国也发现此病毒。2018 年 2 月，多家互联网安全企业截获了 Mind Lost 勒索病毒，同时我国发生多起勒索病毒攻击事件，感染勒索病毒的文件被加密，同时这些文件被重命名为扩展名为 GOTHAM、Techno、DOC、CHAK、FREEMAN 等的文件，并通过邮件来告知受害者付款方式，使获利更加容易、更加方便。2020 年 4 月，网络上出现一种名为 WannaRen 的新型勒索病毒，与此前的“想哭”病毒的行为类似，加密 Windows 系统中几乎所有文件的扩展名为 WannaRen。

3.1.2 计算机病毒的特征

任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响。轻者会占用系统资源，降低计算机的工作效率；重者可导致数据丢失，系统崩溃。计算机病毒和其他程序一样，是一段可执行程序，是寄生在其他可执行程序上的一段代码，只有其他程序运行时，病毒程序代码才会被执行，病毒才会起到破坏作用。病毒程序一旦执行，就会搜索其他符合条件的环境，确定目标后再将自身复制其中，达到自我繁殖的目的。因此，传染性是判断计算机病毒的重要条件。病毒只有在满足其特定条件时，才会对计算机产生致命的破坏。

计算机病毒的特征主要表现为以下 6 方面。

(1) 隐蔽性。计算机病毒不易被发现，这是由于计算机病毒具有较强的隐蔽性，它通常以隐含文件或程序代码的方式存在。一些病毒被设计成病毒修复程序，诱导用户使用，进而实现病毒植入，入侵计算机。因此，计算机病毒的隐蔽性使得安全防范处于被动状态，造成严重的安全隐患。

(2) 破坏性。病毒入侵计算机往往造成极大的破坏，能够破坏计算机的数据信息，甚至造成大面积的计算机瘫痪，对计算机用户造成较大损失。如常见的木马、蠕虫等计算机病毒。

(3) 传染性。计算机病毒具有传染性，它能够通过 U 盘、网络等途径入侵计算机。入侵之后，往往可以实现病毒扩散，感染其他计算机，进而造成大面积瘫痪等事故。随着计算机网络技术的不断发展，在短时间之内，病毒能够实现较大范围的恶意入侵。因此，在计算机病毒的安全防御中，如何面对快速的病毒传染，成为有效防御病毒的重要基础，也是构建防御体系的关键。

(4) 寄生性。计算机病毒具有寄生性。计算机病毒需要在宿主中寄生才能生存，更好地发挥其功能。通常情况下，计算机病毒都是在其他正常程序或数据中寄生，在此基础上利用一定媒介实现传播，在宿主计算机实际运行过程中，一旦达到某种设置条件，计算机病毒就会被激活。

(5) 可执行性。计算机病毒与其他合法程序一样，是一段可执行程序，但它不是一个完整的程序，而是寄生在其他可执行程序上，因此它享有一切程序所具有的权力。

(6) 可触发性。编制计算机病毒的人通常都为计算机病毒程序设定一些触发条件。例如，系统时钟的某个时间或日期、系统运行了某些程序等。一旦条件满足，计算机病毒就会“发作”。因此，计算机病毒具有因某个事件或数值的出现，诱使病毒实施感染或进行

攻击的特征。

3.1.3　计算机病毒的危害及防范措施

如今，计算机和计算机网络已经成为人们生活中重要的组成部分，而病毒会导致计算机数据遭到破坏、篡改、盗取甚至造成严重的计算机网络安全问题，影响网络的使用效益。认识到计算机病毒的破坏性和毁灭性，增强对计算机病毒的防范意识是非常重要的。

计算机病毒的危害主要表现在以下几方面。

1. 病毒能够直接破坏计算机数据信息

大部分计算机病毒发作时可以直接破坏计算机的重要数据，采用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件、用无意义的“垃圾”数据改写文件、破坏CMOS设置等。如磁盘杀手病毒(DISK KILLER)，该病毒内含计数器，硬盘感染病毒后，开机时间累计48小时内激发该病毒，激发时屏幕上显示“Warning!! Don't turn off power or remove diskette while Disk Killer is Processing!”(警告!! DISK KILLER在工作，不要关闭电源或取出磁盘!)该病毒激发时会直接破坏硬盘数据信息。

2. 占用磁盘空间

寄生在磁盘上的病毒总要非法占用一部分磁盘空间。引导型病毒侵占磁盘的方式是由病毒本身占据磁盘引导扇区，而把原来的引导区转移到其他扇区，也就是引导型病毒要覆盖一个磁盘扇区。被覆盖的扇区数据永久性丢失，无法恢复。文件型病毒利用一些DOS功能进行传染，这些DOS功能能够检测出磁盘的未用空间，把病毒的传染部分写到该空间。所以在传染过程中，通常不破坏磁盘上的原有数据，但侵占了磁盘空间。一些文件型病毒传染速度很快，在短时间内感染大量文件，每个文件都不同程度地加长了，造成磁盘空间的严重浪费。

3. 抢占系统资源

除VIENNA(维埃纳)、CASPER(卡死脖)等少量病毒外，大多数病毒在动态下都常驻内存，抢占系统资源，导致内存减少，使得一部分软件不能运行。除占用内存外，病毒还抢占中断，干扰系统运行。计算机操作系统的很多功能是通过中断调用技术来实现的。病毒为了传染激发，往往修改一些中断地址，在正常中断过程中加入病毒，从而干扰系统的正常运行。

4. 影响计算机运行速度

病毒进驻内存后不但干扰系统运行，还影响计算机运行速度，主要表现在以下几方面。

(1) 病毒为了判断传染激发条件，总要对计算机的工作状态进行监视，影响计算机的正常运行。

(2) 有些病毒为了保护自己，不但对磁盘上的静态病毒进行加密，也对进驻内存的动态病毒进行加密，CPU每次寻址到病毒处时，都要运行一段解密程序，把加密的病毒解密成合法的CPU指令再执行；而病毒运行结束时再用一段程序对病毒进行加密。这样导致CPU额外执行数千条甚至上万条指令。

(3) 病毒在进行传染时，同样要插入非法的额外操作，影响计算机的运行速度。

5. 计算机病毒错误导致不可预见的危害

计算机病毒与其他计算机软件的一大区别是计算机病毒的无责任性。开发一个完善的计算机软件需要耗费大量的人力、物力和财力，并且需要经过长时间调试完善，最后才能推出。但在病毒编制者看来，既没有必要这样做，也不可能这样做。很多计算机病毒都是个别程序员在计算机上匆匆编制调试后就开始使用。反病毒专家在分析大量计算机病毒后发现，绝大部分病毒都存在不同程度的错误。错误病毒的另一个主要来源是病毒的变种。有些计算机的初学者尚不具备独立编制软件的能力，出于好奇或其他原因修改别人的病毒程序，从而造成病毒程序的错误。计算机病毒程序的错误所产生的后果往往是不可预见的。反病毒工作者曾经详细指出“黑色星期五”病毒存在 9 处错误，“乒乓”病毒存在 5 处错误等。但是人们不可能花费大量时间去分析数万种病毒的错误所在。大量含有未知错误的病毒扩散传播，其后果是难以预料的。

6. 计算机病毒的兼容性对系统运行的影响

兼容性是计算机软件的一项重要指标，兼容性好的软件可以在各种计算机环境下运行，反之，兼容性差的软件则对运行条件有一定的要求，如对计算机的机型和操作系统的版本等有特别的要求。病毒的编制者一般不会针对各种计算机环境对病毒进行测试，因此病毒的兼容性较差会影响系统的正常运行。

7. 窃取用户的隐私数据以及加密用户文件

木马病毒大部分都是以窃取用户信息、获取经济利益为目的，如窃取用户资料，窃取用户的网银账号和密码、网游账号和密码等。这些信息一旦失窃，将给用户直接带来不可估量的经济损失。

前面谈到的勒索病毒是一种新型计算机病毒，该病毒性质恶劣、危害极大，计算机系统一旦感染这种病毒，将给用户带来无法估量的损失。它利用各种加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解，而要解密文件就需要支付比特币。

8. 计算机病毒给用户造成严重的心理压力

据计算机售后服务部门统计，计算机用户怀疑“计算机有病毒”而提出咨询约占售后服务工作量的 60％以上。经检测确实存在病毒的约占 70％，另有 30％的情况只是用户怀疑，而实际上计算机并没有感染病毒。用户怀疑计算机感染病毒的理由大部分是计算机出现死机、软件运行异常等现象。这些现象确实很有可能是计算机病毒造成的，但又不全是。实际上，在计算机工作“异常”的时候，很难要求一位普通用户去准确判断是否是病毒所为。大多数用户对病毒采取宁可信其有的态度，这对保护计算机安全无疑是十分必要的，但这往往需要付出时间、金钱等方面的代价。而仅仅怀疑病毒而贸然格式化磁盘所带来的损失更是难以弥补。不仅是个人单机用户，对网络病毒的甄别同样给用户造成严重的心理负担和财产损失。总之，计算机病毒像“幽灵”一样笼罩在广大计算机用户的心头，给人们造成巨大的心理压力，极大地影响了计算机的使用效率，由此带来的无形损失是难以估量的。

做好计算机病毒的预防，是防治计算机病毒的关键，计算机病毒的防范措施具体表现在以下几方面。

(1) 安装最新的杀毒软件,及时升级杀毒软件的病毒库,定时对计算机进行病毒查杀,上网时开启杀毒软件全部监控。

(2) 使用正版软件以及从权威的正规网站下载软件,不使用盗版及来历不明的软件。

(3) 养成良好的上网习惯,如对不明邮件及附件慎重打开,尽量不访问不明网站,使用较为复杂的密码。

(4) 及时修复系统漏洞,同时将应用软件升级到最新版本,避免病毒从网页木马的方式入侵到系统或通过其他应用软件漏洞来传播。

(5) 对已经感染病毒的计算机尽快隔离,立即切断网络,以免病毒在网络中传播。

(6) 培养自觉的网络安全意识,在使用移动存储设备时,尽可能不要共享这些设备。移动存储设备是计算机病毒传播的主要途径,也是计算机病毒攻击的主要目标,在对网络安全要求比较高的场所,应将计算机的 USB 接口封闭,在有条件的情况下尽量做到专机专用。

3.2　计算机病毒的工作原理

计算机病毒本质上是人为编制的计算机程序代码。这段程序代码一旦进入计算机并得以执行,会对计算机的使用造成不同程度的影响。它会搜寻符合传染条件的程序或存储介质,确定目标后再将自身代码插入其中,达到自我繁殖的目的。计算机一旦感染病毒,若不及时处理,病毒会迅速扩散,导致大量文件(一般是可执行文件)被感染。而被感染的文件又成了新的传染源,与其他计算机进行数据交换或通过网络进行数据传输。程序通常是由用户调用,再由系统分配资源,完成用户交给的任务。其目的对用户是可见的、透明的。而计算机病毒具有正常程序的一切特性,它隐藏在正常程序中,当用户调用程序时,病毒程序窃取到系统的控制权,先于正常程序执行。病毒的动作、目的对用户是未知的,是未经用户允许的。

计算机病毒一般是具有很高的编程技巧、短小精悍的程序。通常附在正常程序中或磁盘较隐蔽的地方,也有个别的以隐含文件形式出现,目的是不让用户发现它的存在。如果不经过代码分析,病毒程序与正常程序不容易区分。一般在没有防护措施的情况下,计算机病毒程序取得系统控制权后,可以在短时间里传播。受到传染的计算机系统通常仍能正常运行,用户感觉不到任何异常。正是由于具有隐蔽性,计算机病毒才得以在用户不知不觉的情况下扩散到其他计算机中。

大部分计算机系统感染病毒之后不会马上发作,它可以长期隐藏在系统中,只有在满足其特定条件时才启动表现(破坏)模块,进行传播。

计算机病毒通常是由以下 3 个模块组成的。

(1) 引导模块。引导模块将计算机病毒程序引入计算机内存,并使得感染和表现模块处于活动状态。引导模块需要提供自我保护功能,避免在内存中的代码被覆盖或清除。计算机病毒程序引入内存后为感染模块和表现模块设置相应的启动条件,以便在适当的时候或合适的条件下激活感染模块或表现模块。

(2) 感染模块。感染模块分为感染条件判断子模块和感染功能实现子模块两个模块。感染条件判断子模块依据引导模块设置的传染条件判断当前系统环境是否满足传染

条件。如果传染条件满足,感染功能实现子模块则启动传染功能,将计算机病毒程序附加在其他宿主主程序上。

(3) 表现模块。表现模块分为条件判断子模块和功能实现子模块两个模块。判断子模块依据引导模块设置的触发条件判断当前系统环境是否满足触发条件。如果触发条件满足,实现子模块则启动计算机病毒程序,按照预定的计划执行。

3.3 计算机病毒的分类

按照计算机病毒的特点及特性,可以将计算机病毒划分为多种。同一种病毒可能属于多个不同的类型。通常将计算机病毒划分为以下几种类型。

1. 传统单机病毒

单机病毒在单台计算机中感染并发作,破坏单台计算机。该类型病毒通过 U 盘或磁盘传播。常见的单机病毒包括引导型病毒、文件型病毒、宏病毒以及复合型病毒。

1) 引导型病毒

引导型病毒是指寄生在磁盘引导区或主引导区的计算机病毒。此种病毒利用系统引导时不对主引导区的内容正确与否进行判别的缺点,在引导系统的过程中侵入系统,驻留内存,监视系统运行,伺机传染和破坏。按照引导型病毒在硬盘上的寄生位置,又可细分为主引导记录病毒和分区引导记录病毒。主引导记录病毒感染硬盘的主引导区,如大麻病毒、火炬病毒等;分区引导病毒感染硬盘的活动分区,如小球病毒等。

2) 文件型病毒

文件型病毒是指能够寄生在文件中的计算机病毒。这类病毒程序主要感染计算机中的可执行文件(.exe)和命令文件(.com)。该病毒对计算机的源文件进行修改,使其成为新的带毒文件。一旦计算机运行该文件,就会被感染,从而达到传播的目的。1575 病毒又称毛毛虫病毒,属于 PC-DOS 系统上的文件型病毒,该病毒仅传染可执行文件,并随被传染文件的执行而常驻内存。

3) 宏病毒

宏病毒是一种寄存在文档或模块的宏中的计算机病毒。一旦打开这样的文档,其中的宏就会被执行,于是宏病毒就会被激活,从而转移到计算机上,并驻留在 Normal 模板中,之后所有自动保存的文档都会“感染”这种宏病毒。若其他用户打开了感染病毒的文档,宏病毒又会转移到该用户的计算机上。宏病毒主要利用 Microsoft Office 的开放性,即 Word 中提供的 VBA 编程接口,专门制作一个或多个具有病毒特点的宏的集合。其特点是传播快,破坏性大。

4) 复合型病毒

复合型病毒是指同时具有引导型病毒和文件型病毒寄生方式的计算机病毒。这种病毒扩大了病毒程序的传染途径,它既感染磁盘的引导记录,又感染可执行文件。当感染此种病毒的磁盘用于引导系统或调用执行染毒文件时,病毒就会被激活。因此在检测、清除复合型病毒时,必须全面彻底地根治,如果只发现该病毒的一个特性,把它只当作引导型或文件型病毒进行清除,虽然好像是清除了,但还留有隐患,这种经过消毒后的“洁净”系

统更富有攻击性。这种病毒有 Flip 病毒、新世纪病毒、One-half 病毒等。

2. 现代网络病毒

与单机病毒相对应的是网络病毒，网络病毒可以通过网络传播。常见的网络病毒包括蠕虫病毒、木马病毒等。

1）蠕虫病毒

蠕虫是一种可以自我复制的程序代码，且通过网络传播，通常无须人为干预就能传播。蠕虫病毒入侵并完全控制一台计算机之后，就会把这台计算机作为宿主，扫描并感染其他计算机。当这些被蠕虫入侵的计算机被控制之后，蠕虫会以这些计算机为宿主，继续扫描并感染其他计算机，这种行为会一直延续下去。蠕虫使用这种递归的方法传播，按照指数增长的规律分布自己，进而及时控制越来越多的计算机。

蠕虫病毒的特点表现在以下 6 方面。

（1）较强的独立性。计算机病毒一般都需要宿主程序，病毒将自己的代码写到宿主程序中，当该程序运行时，先执行写入的病毒程序，从而造成感染和破坏。而蠕虫病毒不需要宿主程序，它是一段独立的程序或代码，因此也就避免了受宿主程序的牵制，可以不依赖于宿主程序而独立运行，实施攻击。

（2）利用漏洞主动攻击。由于不受宿主程序的限制，蠕虫病毒可以利用操作系统的各种漏洞进行主动攻击。如“尼姆达”病毒利用 IE 浏览器漏洞，使感染病毒的邮件附件在不被打开的情况下就能激活病毒；“红色代码”病毒利用微软 IIS 服务器软件的漏洞来传播；而“蠕虫王”病毒则是利用微软数据库系统的漏洞进行攻击。

（3）传播更快、更广。蠕虫病毒比传统病毒具有更大的传染性，它不仅感染本地计算机，还会以本地计算机为基础感染网络中所有的服务器和客户端。蠕虫病毒可以通过网络中的共享文件夹、电子邮件、恶意网页以及存在着大量漏洞的服务器等途径肆意传播，几乎所有的传播手段都被蠕虫病毒运用得淋漓尽致。因此，蠕虫病毒的传播速度可以是传统病毒的几百倍，甚至可以在几小时之内蔓延全球。

（4）更好的伪装和隐藏方式。为了使蠕虫病毒在更大范围内传播，病毒的编制者非常注重病毒的隐藏方式。在通常情况下，人们在接收、查看电子邮件时，都采取双击打开邮件主题的方式来浏览邮件内容，如果邮件中带有病毒，用户的计算机就会立刻被病毒感染。

（5）技术更加先进。一些蠕虫病毒与网页的脚本相结合，利用 VBScript、Java、Active X 等技术隐藏在 HTML 页面里。当用户浏览含有病毒代码的网页时，病毒会自动驻留内存，并伺机触发。还有一些蠕虫病毒与后门程序或木马程序相结合，比较典型的是“红色代码”病毒，病毒的传播者可以通过这个程序远程控制被病毒感染的计算机。这类与黑客技术相结合的蠕虫病毒具有更大的潜在威胁。

（6）使追踪变得更困难。当蠕虫病毒感染了大部分系统之后，攻击者便能发动多种攻击方式对付一个目标站点，并通过蠕虫病毒隐藏攻击者的位置，这样要抓住攻击者会非常困难。

2）木马病毒

木马病毒是指隐藏在正常程序中一段具有特殊功能的恶意代码，是具备破坏和删除

文件、发送密码、记录键盘等特殊功能的后门程序。木马病毒是计算机黑客用于远程控制计算机的程序，将控制程序寄生于被控制的计算机系统中，内应外合，对被感染木马病毒的计算机实施操作。一般的木马病毒程序主要是寻找计算机后门，伺机窃取被控计算机中的密码和重要文件等，可以对被控计算机实施监控、资料修改等非法操作。木马病毒具有很强的隐蔽性，可以根据黑客意图突然发起攻击。

木马病毒是一种程序，这种程序会做一些文档中没有明确声明的事，也就是说，程序编写者编写的特洛伊木马程序表面上在做有用的事，实际上它隐含盗用进程，在做有损计算机安全的罪恶勾当，包括复制、滥用或者销毁数据等非法活动。一个典型的例子是“复活节彩蛋(easter eggs)”，它通常是可以被一些神秘的击键组合激活的简短程序，程序员将其置入商品化软件中。而利用特洛伊木马背后窃取用户资料并破坏计算机系统，从而导致计算机安全保密事件的发生，在网络出现以后已经屡见不鲜。

木马病毒的特点表现在以下几方面。

(1) 隐蔽性。木马病毒可以长期存在的主要原因是它可以将自己伪装成合法应用程序来隐匿自己，使用户难以识别，这是木马病毒首要也是最重要的特征。与其他病毒一样，木马病毒隐蔽的期限往往较长。经常采用的方法是：①寄生在合法程序之中；②将自身修改为合法程序名或图标；③不在进程中显示出来；④伪装成系统进程；⑤与其他合法文件关联起来等。

(2) 欺骗性。木马病毒隐蔽的主要手段是欺骗，经常使用伪装的手段将自己合法化。如：①使用合法的文件类型扩展名 dll、sys、ini；②使用已有的合法系统文件名，然后保存在其他文件目录中；③使用容易混淆的字符命名，例如字母 O 与数字 0，字母 I 与数字 1 等。

(3) 顽固性。木马病毒为了保障自己可以不断蔓延，往往像毒瘤一样驻留在被感染的计算机中，有多份备份文件存在，一旦主文件被删除，便可以马上恢复。尤其是采用文件的关联技术，只要被关联的程序被执行，木马病毒便被执行，并产生新的木马程序甚至变种。顽固的木马病毒给木马清除带来巨大的困难。

(4) 危害性。木马病毒的危害性是毋庸置疑的。只要计算机被木马病毒感染，别有用心的黑客便可以任意操纵计算机，就像在本地使用计算机一样，对被控计算机的破坏性可想而知。黑客可以肆意妄为，盗取系统的重要资源，如系统密码、股票交易信息、机票数据等。

3. 其他病毒

其他病毒可以根据不同角度分为不同类型，下面分别按攻击系统、破坏性以及连接方式进行分类。

1) 按攻击系统分类

按照攻击系统分类，可将计算机病毒分为 DOS 病毒、Windows 病毒、UNIX 病毒以及 OS/2 病毒。

(1) DOS 病毒。这类病毒通常只能在 DOS 操作系统下运行并传染。DOS 病毒是最早出现的计算机病毒，典型地感染主引导扇区和引导扇区的 DOS 病毒称为引导型病毒。

(2) Windows 病毒。Windows 病毒是指感染 Windows 可执行程序，并可在 Windows 下运行的一类病毒。目前 Windows 图形用户界面(graphical user interface，GUI)和多任务操作系统完全取代了 DOS 操作系统，因此 Windows 操作系统环境成为病毒攻击的主

要对象，如1998年出现的影响比较大的CIH病毒就属于Windows病毒。

(3) UNIX病毒。针对UNIX操作系统的病毒称为UNIX病毒，UNIX操作系统是一个强大的多用户、多任务操作系统，支持多种处理器架构，该操作系统除了作为网络操作系统之外，还可以作为单机操作系统使用。因此，UNIX操作系统病毒的出现对人类的信息处理也是一个严重的威胁。

(4) OS/2病毒。OS/2(operating system/2)是由微软和IBM公司共同开发，后来由IBM公司单独开发的一套操作系统。该系统作为IBM第二代个人计算机PS/2的理想操作系统，最大规模的发行版本是于1996年发行的OS/2 Warp 4.0。针对OS/2操作系统的病毒称为OS/2病毒。

2) 按破坏性分类

(1) 良性病毒。良性病毒是指那些只是为了表现自身，并不彻底破坏系统和数据，但会大量占用CPU时间，增加开销，降低系统工作效率的一类计算机病毒。这类病毒多数是恶作剧者的产物，他们的目的不是为了破坏系统和数据，而是为了让使用染有病毒的计算机用户通过显示器或扬声器看到或听到病毒设计者的编程技术。

(2) 恶性病毒。恶性病毒是指破坏系统或数据，造成计算机系统瘫痪的一类计算机病毒。感染恶性病毒后计算机一般没有异常表现，病毒会想方设法将自己隐藏得更深。恶性病毒一旦发作，将会对计算机数据或硬件造成无法挽回的损失。

3) 按连接方式分类

(1) 源码型病毒。该类病毒攻击高级语言编写的源程序，在源程序编译之前插入其中，并随源程序一起编译、连接成可执行文件。源码型病毒较为少见，亦难以编写。

(2) 嵌入型病毒。嵌入型病毒可用自身代替正常程序中的部分模块或堆栈区。因此这类病毒只攻击某些特定程序，针对性强。一般情况下也难被发现，清除起来也较困难。

(3) 外壳型病毒。外壳型病毒通常将自身附在正常程序的开头或结尾，相当于给正常程序加了个外壳。大部分文件型病毒都属于这一类。

(4) 操作系统型病毒。操作系统型病毒可用其自身部分加入或替代操作系统的部分功能。因其直接感染操作系统，这类病毒的危害性也较大。

3.4　实验：冰河

冰河是国产木马的标志和代名词。冰河的服务器端程序为G-server.exe，客户端程序为G-client.exe，默认连接端口为7626。一旦运行G-server.exe，该程序就会在C:/windows/system目录下生成Kernel32.exe和sysexplr.exe，并删除自身。

Kernel32.exe在系统启动时自动加载运行，在注册表中，sysexplr.exe和TXT文件关联，即使删除了Kernel32.exe，但只要打开TXT文件，sysexplr.exe就会被激活，将再次生成Kernel32.exe。

冰河软件的安装使用过程如下。

(1) 安装客户端程序。

客户端的安装过程比较简单，安装完成后的执行界面如图3.8所示。

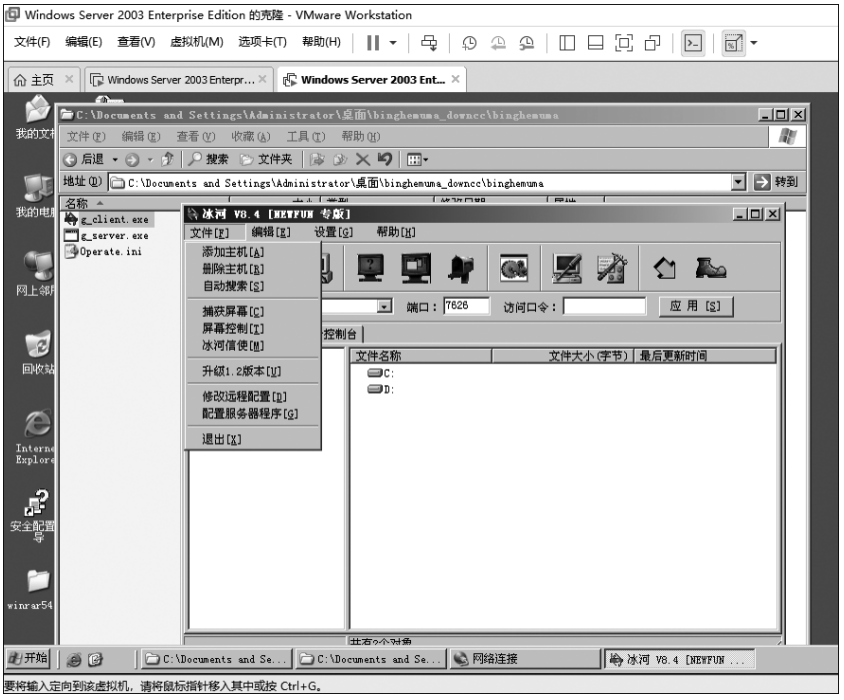

图 3.8　客户端执行界面

（2）接下来配置服务器程序，如图 3.9～图 3.14 所示。

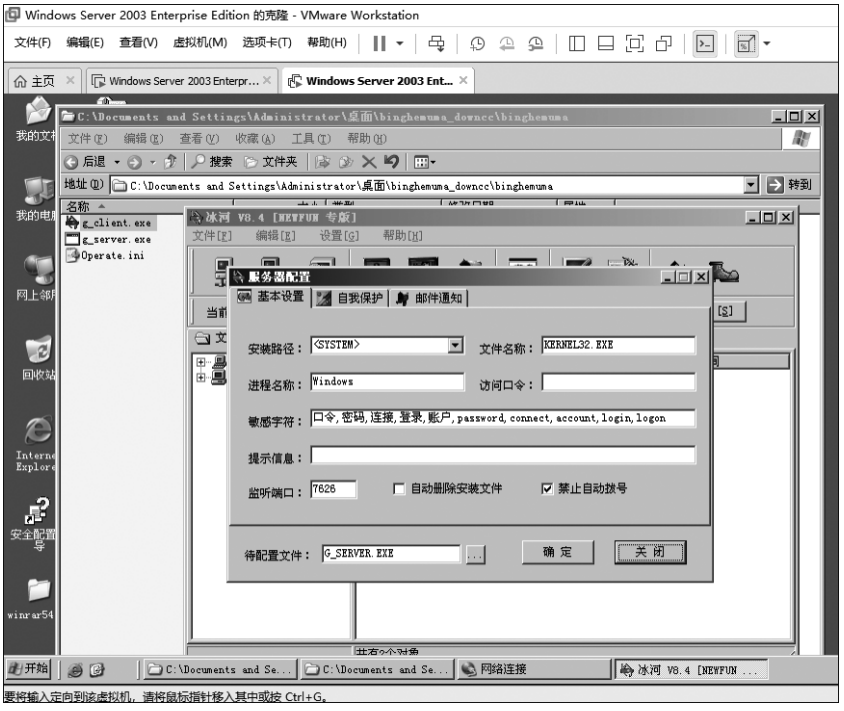

图 3.9　执行服务器端程序

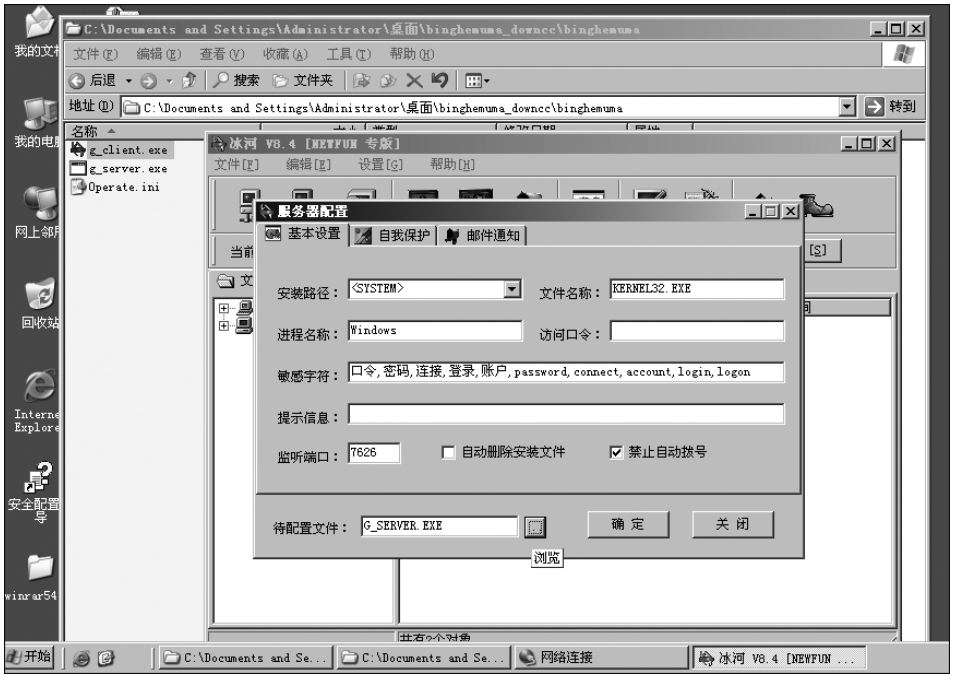

图 3.10　服务器配置

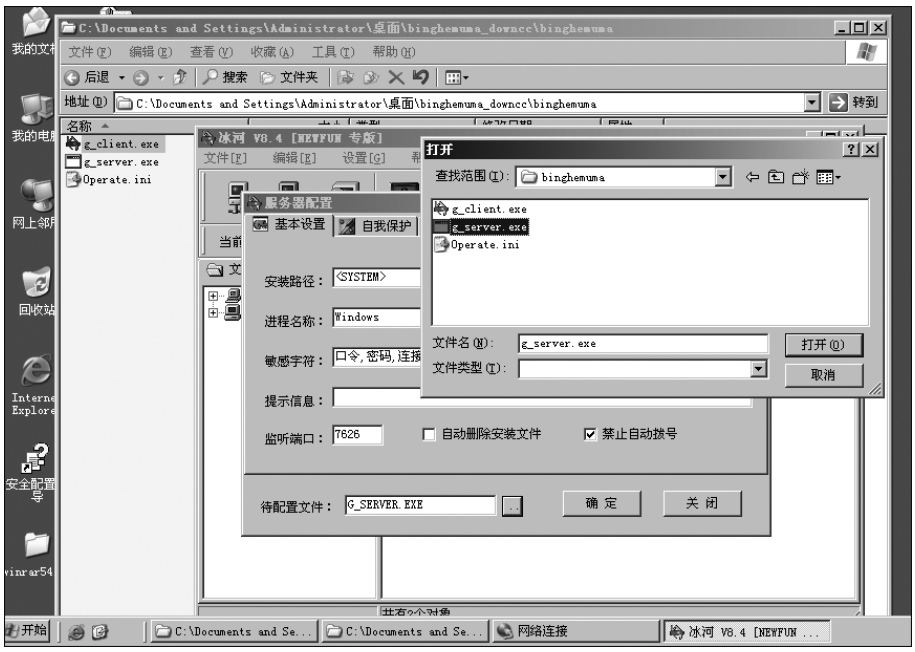

图 3.11　设置待配置文件

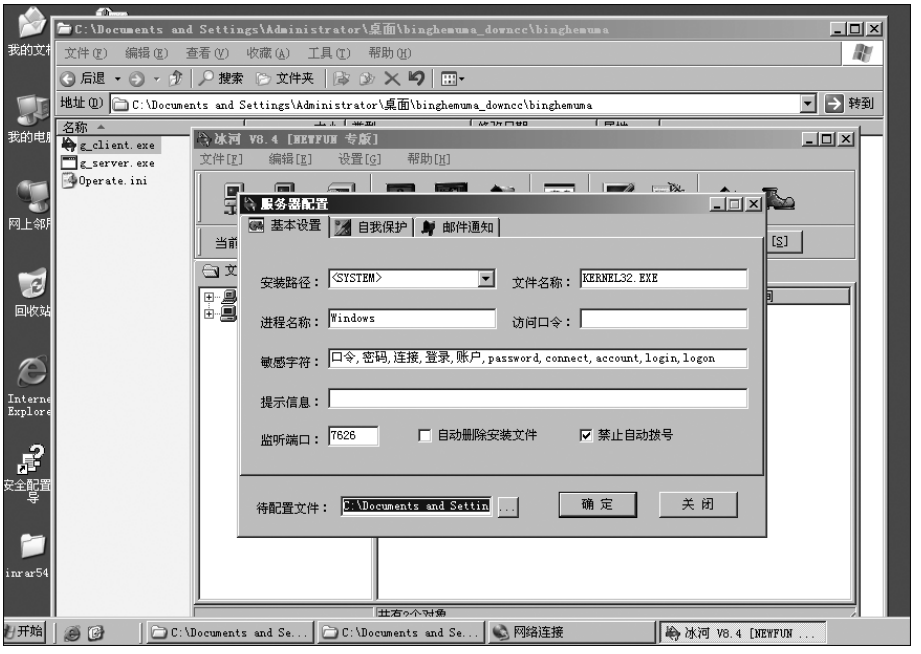

图 3.12　指定待配置文件路径

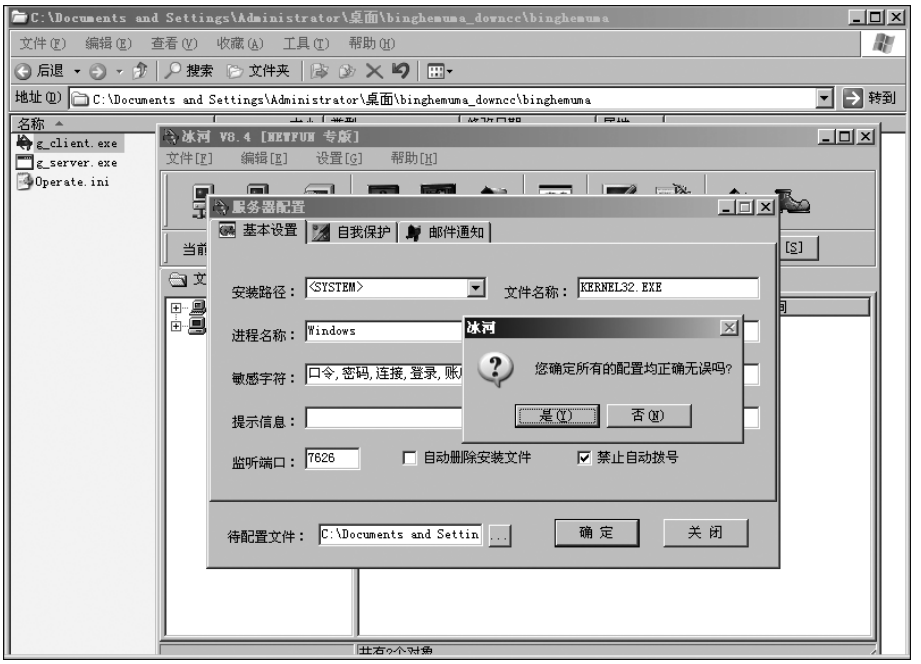

图 3.13　确定配置信息

(3) 创建账号,设置文件夹共享。

右击“我的电脑”,在弹出的快捷菜单中选择“管理”,在“计算机管理”窗口中选择“用户”,为管理员 administrator 设置密码,在弹出的窗口中输入管理员密码。

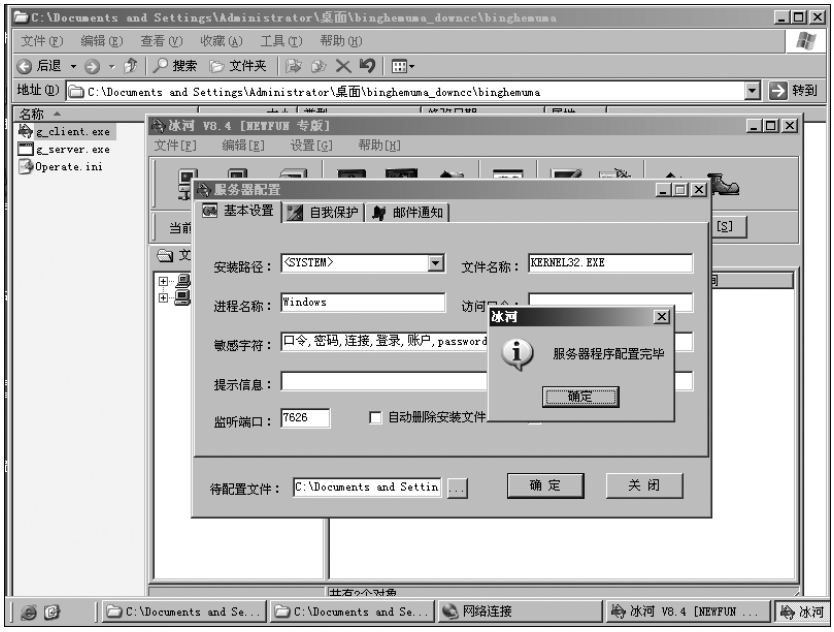

图 3.14　服务器程序配置完毕

将冰河文件夹设置为共享，右击冰河文件夹，在弹出的快捷菜单中选择“共享和安全”，将该文件夹进行共享。

(4) 在被入侵计算机中设置服务器端程序，如图 3.15～图 3.18 所示。

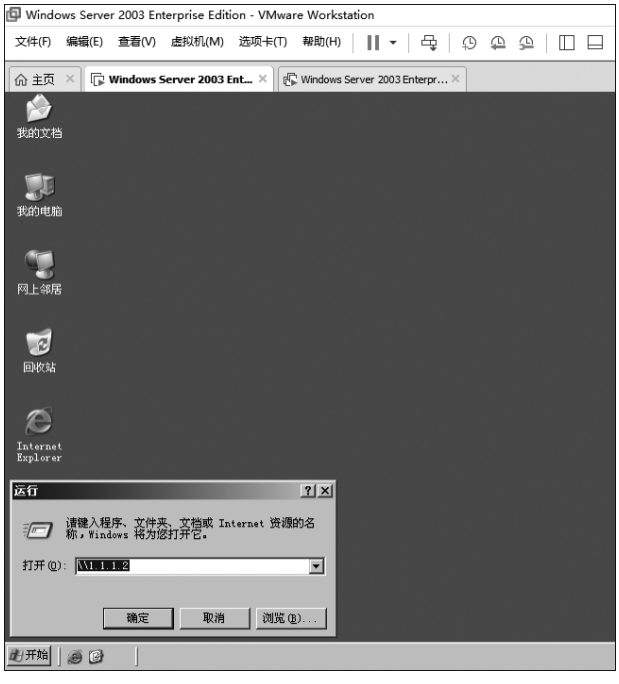

图 3.15　在另一台主机中访问网络

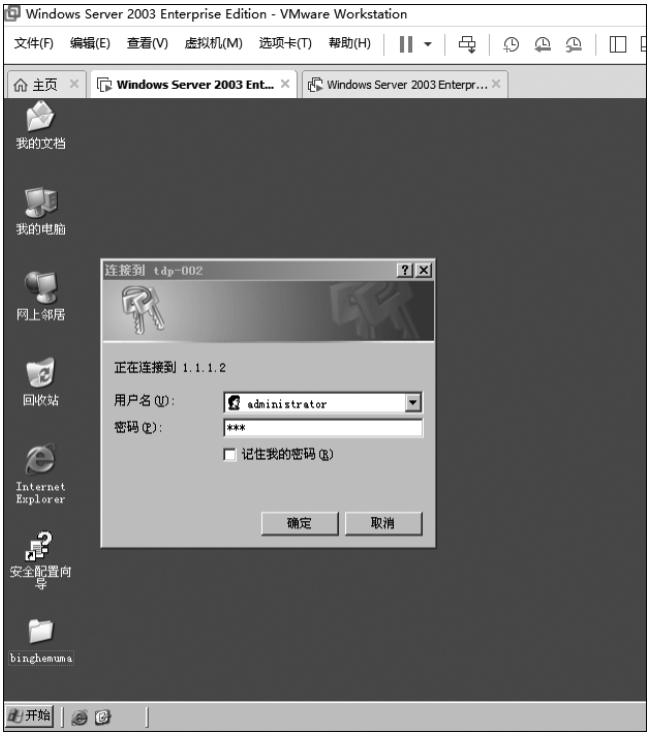

图 3.16　在弹出的对话框中输入密码

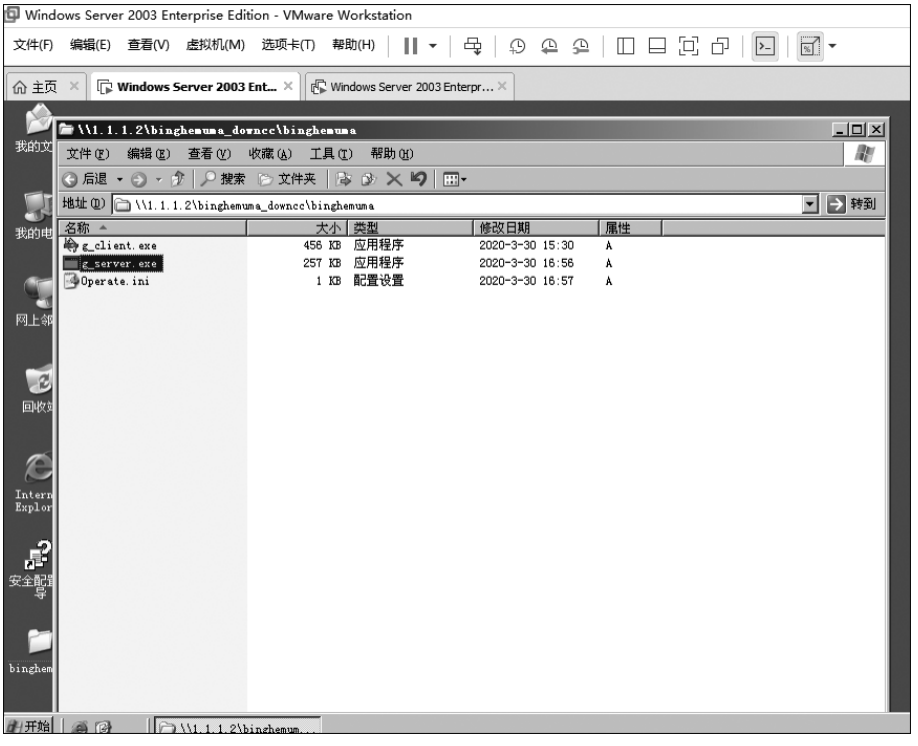

图 3.17　打开共享文件夹

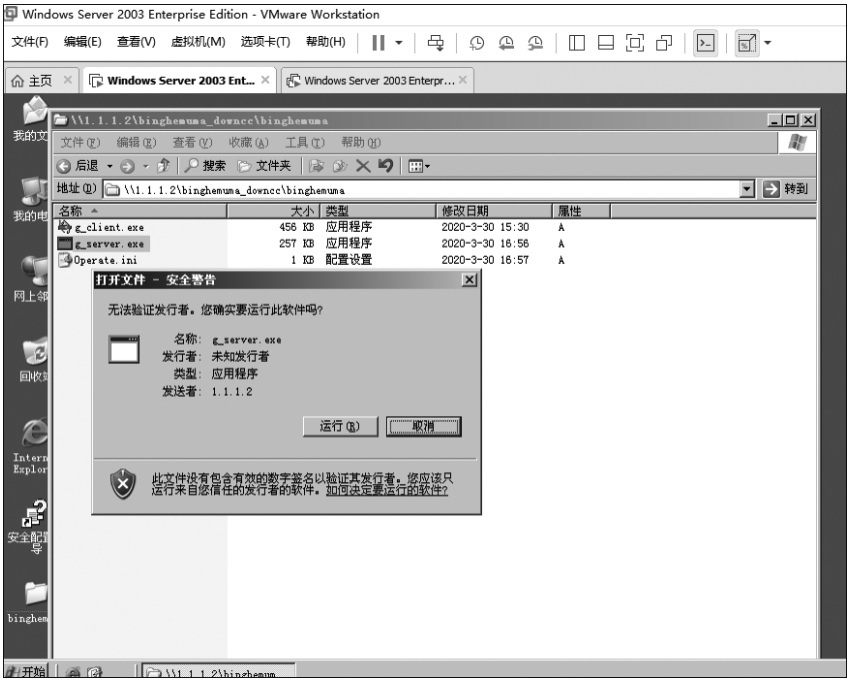

图 3.18　运行服务器端程序

(5) 用客户端计算机控制服务器端计算机,如图 3.19～图 3.30 所示。

图 3.19　在客户端程序中选择文件菜单中的“添加主机”