第5章 计算机病毒及其防治

随着计算机技术的普及和发展，计算机系统的安全已成为计算机用户普遍关注的问题。而计算机病毒是计算机系统的巨大威胁之一，计算机病毒一旦发作，轻则破坏文件、损害系统，重则造成网络瘫痪。因此，势必要了解计算机病毒，使计算机免受其恶意的攻击与破坏。

学习目标

- 了解计算机病毒的定义及特征。
- 熟悉计算机病毒的传播途径及其主要危害。
- 熟悉计算机病毒发作后的症状。
- 掌握 CIH 病毒、宏病毒、蠕虫病毒、特洛伊木马的主要特征及防治对策。
- 掌握木马程序的工程原理，以及手工清除木马的常见方法。
- 掌握企业版杀毒软件的安装及配置。

课业任务

本章通过一个实际课业任务，介绍企业版杀毒软件部署的相关原理，以及如何安装企业杀毒软件的服务器端与客户端。

课业任务 5-1

WYL 公司采用 Symantec Endpoint Protection 作为安全防护解决方案，网络管理员需要在一台安装 Windows Server 2008 操作系统的计算机上安装 Symantec Endpoint Protection 服务器端软件，然后对其受管的所有客户端进行部署。

能力观测点

企业版杀毒软件部署原理；企业版杀毒软件服务器端的安装；企业版杀毒软件客户端的生成与安装。

5.1 计算机病毒概述

5.1.1 计算机病毒的概念

1994 年 2 月 18 日，计算机病毒(Computer Virus)在《中华人民共和国计算机信息系统安全保护条例》中进行了明确的定义："指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。"

也就是说，计算机病毒就是一段程序，但是它具有自己的特殊性。首先，计算机病毒利用计算机资源的脆弱性破坏计算机系统；其次，计算机病毒不断地进行自我复制，在潜伏期内，通过各种途径传播到其他系统并隐藏起来，当达到触发条件时被激活，从而导致系统被

恶意破坏。

5.1.2 计算机病毒的发展

1. 计算机病毒的起源

20 世纪 60 年代初，在美国贝尔实验室里，3 个年轻的程序员编写了一个名为“磁芯大战”的游戏，游戏中通过复制自身来摆脱对方的控制，这就是所谓“病毒”的第一个雏形。

20 世纪 70 年代，美国作家雷恩在其出版的《P.1 的青春》一书中构思了一种能够自我复制的计算机程序，并第一次称为“计算机病毒”。

2. 第一个病毒

1983 年 11 月，在国际计算机安全学术研讨会上，美国计算机专家首次将病毒程序在 VAX/750 计算机上进行了实验，世界上第一个计算机病毒就这样出生在实验室中。

20 世纪 80 年代后期，巴基斯坦有两个以编软件为生的兄弟为了打击那些盗版软件的使用者，设计出了一个名为“巴基斯坦”的病毒，该病毒只传染软盘引导。这就是最早在世界上流行的一个真正的病毒。

3. DOS 阶段

1988—1989 年，我国也相继出现了能感染硬盘和软盘引导区的 Stoned(石头)病毒。该病毒体代码中有明显的标志“Your PC is now Stoned!”、“LEGALISE MARIJUANA!”，也称为“大麻病毒”等。该病毒感染软硬盘 0 面 0 道 1 扇区，并修改部分中断向量表。该病毒不隐藏也不加密自身代码，所以很容易被查出和解除。类似这种特性的还有小球、Azusa/Hong Kong/2708、Michaelangelo，这些都是从国外传染进来的。国产的 Bloody、Torch、Disk Killer 等病毒，实际上它们大多数是 Stoned 病毒的翻版。

20 世纪 90 年代初，感染文件的病毒有 Jerusalem(黑色 13 号星期五)、YankeeDoole、Liberty、1575、Traveller、1465、2062、4096 等，主要感染.com 和.exe 文件。这类病毒修改了部分中断向量表，被感染的文件明显地增加了字节数，并且病毒代码主体没有加密，也容易被查出和解除。在这些病毒中，略有对抗反病毒手段的只有 YankeeDoole 病毒，当发现用户用 DEBUG 工具跟踪它时，它会自动从文件中逃走。

接着，一些能对自身进行简单加密的病毒相继出现，有 1366(DaLian)、1824(N64)、1741(Dong)、1100 等病毒。它们加密的目的主要是防止跟踪或掩盖有关特征等。

以后又出现了引导区、文件型“双料”病毒，这类病毒既感染磁盘引导区，又感染可执行文件，常见的有 Flip/Omicron(颠倒)、XqR(New Century 新世纪)、Invader/侵入者、Plastique/塑料炸弹、3584/郑州(狼)、3072(秋天的水)、ALFA/3072.2、Ghost/One_Half/3544(幽灵)、Natas(幽灵王)、TPVO/3783 等。如果只解除了文件上的病毒，而没解除硬盘主引导区的病毒，系统引导时又将病毒调入内存，会重新感染文件。如果只解除了主引导区的病毒，而可执行文件上的病毒没解除，一执行带病毒的文件，就会又将硬盘主引导区感染。

1992 年以来，DIR2.3、DIR2.6、NEW DIR2 病毒以一种全新的面貌出现，具有的感染力极强，无任何表现，不修改中断向量表，而直接修改系统关键中断的内核，修改可执行文件的首簇数，将文件名称与文件代码主体分离。在系统有此病毒的情况下，一切就像没发生一样。而在系统无病毒时，当用户用无病毒的文件去覆盖有病毒的文件时，灾难就会发生，全盘所有被感染的可执行文件内容都是刚覆盖进去的文件内容，这就是病毒“我死你也活不

成”的罪恶伎俩。该病毒的出现，使病毒又多了一种新类型。

20 世纪的绝大多数病毒是基于 DOS 系统的，约 80％的病毒能在 Windows 中传染。TPVO/3783 病毒是“双料性”(传染引导区、文件)、“双重性”(DOS、Windows)病毒，这就是病毒随着操作系统发展而发展起来的病毒。

4. Windows 阶段

随着 Windows 9x、Windows 2000 操作系统的发展，病毒种类也随着它的变化而变化。下面介绍几种典型的 Windows 病毒。

(1) Win32. CAW. 1XXX 病毒。Win32. CAW. 1XXX 病毒是驻留内存的 Win32 病毒，它感染本地和网络中的 PE 格式文件。该病毒来源于一种 32 位的 Windows“CAW 病毒生产机”，该“CAW 病毒生产机”是国际上一家有名的病毒编写组织开发的。

“CAW 病毒生产机”能生产出各种各样的 CAW 病毒，有加密的和不加密的，其字节数一般在 1000～2000。目前在国内流行的有 CAW. 1531、CAW. 1525、CAW. 1457、CAW. 1419、CAW. 1416、CAW. 1335、CAW. 1226 等，在国际上流行的 CAW. 1XXX 病毒种类更多。

Win32. CAW. 1XXX 病毒可进行以下破坏。

当病毒驻留在内存中时，病毒会在每日的整点时间，如 1:00、6:00、10:00 等，删除一些特定的文件，如. bmp、. jpg、. doc、. wri、. bas、. sav、. pdf、. rtf、. txt 文件，以及 WINWORD. EXE。

当 7 月 7 日的时候，CAW 病毒就会发作，删除硬盘上的所有文件。

某些 CAW. 1XXX 病毒有缺陷，当感染上该病毒的文件被破坏后，杀毒后的文件也无法修复，只能用正常文件覆盖坏文件。有些病毒还有重复多层次感染文件的缺陷，容易将文件写坏。

(2) Win32. Funlove. 4099 病毒。Win32. Funlove. 4099 病毒感染本地和网络中的 PE. EXE 文件。

病毒本身就是只具有“. code”部分 PE 格式的可执行文件。

当染毒的文件被运行时，该病毒将在 Windows\system 目录下创建 FLCSS. EXE 文件，在其中只写入病毒的纯代码部分，并运行这个生成的文件。

一旦在创建 FLCSS. EXE 文件时发生错误，病毒将从感染病毒的主机文件中运行传染模块。该传染模块将作为独立的线程在后台运行，主机程序在执行时几乎没有可察觉的延时。

传染模块将扫描本地从 C: 到 Z:的所有驱动器，然后搜索网络资源，扫描网络中的子目录树并感染具有. ocx、. scr 或者. exe 扩展名的 PE 文件。

这个病毒类似于 Bolzano 病毒，可修补 NTLDR 和 Winnt\system32\ntoskrnl. exe，被修补的文件自己不可以恢复，只能通过备份来恢复。

(3) Win32. KRIZ. 4250 病毒。Win32. KRIZ. 4250 病毒已大面积传播，这是一种变形病毒，变化多端。每年的 12 月 25 日，该病毒可像 CIH 病毒一样，破坏硬盘数据与主板 BIOS。该病毒目前也有许多字节数不同的变种。

病毒的种类、传染和攻击的手法越来越高超，在 Windows 环境下最为知名的就属寄存在文档或模板的宏中的宏病毒。

近几年，出现了近万种 Word(Macro 宏)病毒，并以迅猛的势头发展，已形成了病毒的

另一大派系。由于宏病毒编写容易，不分操作系统，再加上 Internet 上的 Word 格式文件的大量交流，宏病毒会潜伏在这些 Word 文件里，被人们在 Internet 上传来传去。

5. Internet 阶段

随着 Internet 的发展，激发了病毒更加广泛的活力。病毒通过网络的快速传播，为世界带来了一次一次的巨大灾难。

1999 年 3 月 6 日，一个名为“美丽杀”的计算机病毒席卷了欧、美各国的计算机网络。这种病毒利用邮件系统大量复制、传播，造成网络阻塞，甚至瘫痪。并且，这种病毒在传播过程中还会泄密。在美国，白宫等政府部门、微软和 Intel 等一些大公司，为了避免更大的损失，紧急关闭了网络服务器，检查、清除“美丽杀”病毒。由于“美丽杀”病毒损害了美国政府和大型企业的利益，美国联邦调查局(FBI)迅速行动。经过四五天的技术侦察，将病毒制造者史密斯抓获。但是“美丽杀”病毒已使 300 多家大型公司的服务器瘫痪，这些公司的业务依赖于计算机网络，服务器瘫痪后造成公司正常业务停顿，损失巨大。并且，随后“美丽杀”病毒的源代码在互联网上公布，功能类似于“美丽杀”的其他病毒或蠕虫接连出台，如 PaPa、Copycat 等。然而，这仅仅是计算机病毒肆虐网络的序曲。

1998 年 2 月，台湾的陈盈豪编写出了破坏性极大的 Windows 恶性病毒 CIH v1.2 版，并定于每年的 4 月 26 日发作，然后悄悄地潜伏在网上的一些供人下载的软件中。

可是，两个月的时间内，被人下载得不多，到了 4 月 26 日，病毒只在台湾省少量发作，并没引起重视。心理扭曲的陈盈豪不甘心，又炮制了 CIH v1.3 版，并将破坏时间设在 6 月 26 日。

还是两个月的时间，CIH v1.3 版被人下载得也不多，6 月 26 日也没多大破坏。心理扭曲到极点的陈盈豪有点恼怒，没看到很大的破坏，心里很不痛快。7 月，他又炮制出了 CIH v1.4 版。这次，他干脆将破坏时间设为每月的 26 日，他要月月看到人们遭殃。

很不巧的是，就在那一年，在国内外上映的台湾电视剧女主角“小龙女”的肖像被广泛用在计算机的屏幕保护程序中，CIH v1.2、CIH v1.4 病毒也被悄悄注进该程序，大量的用户从网上下载使用。同时，该程序也被广泛地装进各种各样的盗版光盘中，3 种版本的 CIH 病毒被广泛地扩散，当时的反病毒公司也没有及时发现。因此，这种全新的 Windows 病毒到处传播，危机的阴影迅速笼罩着四方。

一个月后，也就是 1998 年 8 月 26 日，CIH v1.4 病毒首先跳出来发作，我国部分地区遭到袭击，但损害面积不大。事后，为了避免更大灾害，我国政府职能部门公安部发出了通缉 3 种 CIH 病毒的通告。当时，使用正版杀毒软件不被一些用户重视，又不经常升级杀毒软件，又经过一年的传播，CIH v1.2 病毒已传遍全世界，世界性的巨大杀机潜伏下来了，一场人类史无前例的信息大劫难即将暴发。

1999 年 4 月 26 日，一个计算机行业难以忘却的日子，也就是到了 CIH v1.2 病毒第二年的发作日，人们一上班便轻松地打开计算机准备工作，可是，打开一台计算机后，屏幕一闪就黑暗一片。再打开另外几台，也同样一闪后就再也启动不起来。计算机史上，病毒造成的又一次巨大的浩劫发生了。

一大早，反病毒软件公司所有的电话铃声响个不停，急促的报警电话蜂拥而来。门外，需要修复数据而手持硬盘和抬着机器的人们排列得一条长龙，从楼上到楼下，一直排到大街上。“谁能给我修复好数据，我出高价!”的叫喊声到处可听见。

据报道，此次病毒的浩劫在东方的亚洲国家最严重。欧美国家嘲笑东方国家，一种说法是该病毒由于盗版严重而带来的，第二种说法是反病毒软件落后。可是，在此前的一个月，欧美的“美丽杀”病毒在西方造成了更为严重的灾难，其经济损失远远超过 CIH 病毒对亚洲造成的损失，而 CIH 病毒造成的破坏绝大部分可以修复。

由于欧美国家早一个月发生“美丽杀”病毒灾难，引起欧亚国家媒体爆炒“美丽杀”病毒，在一定程度上起了误导作用。国内的老牌反病毒公司北京江民公司，通过国内强大的病毒反馈网，以灵敏的嗅觉警惕到 CIH v1.2 病毒要在 4 月 26 日大发作！便不惜重金在报纸上用广告和文章的形式在 4 月 26 日前连篇提醒人们重视防范 CIH 病毒。这在当时可能是国内唯一的一家提醒人们重视防范 CIH 病毒的反病毒公司，但是，还是被淹没在爆炒“美丽杀”病毒的文章中。只有部分人看到防范 CIH 病毒的报纸后，并即时升级查杀了 CIH 病毒，才幸免于难。

随着 Internet 的发展，病毒传播更加方便、广泛，网络蠕虫病毒已成为病毒主力，这应使人们严加防范。

5.2 计算机病毒的特征及传播途径

5.2.1 计算机病毒的特征

1. 非授权可执行性

用户在调用并执行一个程序时，通常把系统控制权交给这个程序，并为其分配相应的系统资源，如内存，从而使之能够完成用户的需求。因此，程序执行的过程对用户是透明的。而计算机病毒是非法程序，正常用户是不会明知是病毒程序，而故意调用并执行的。计算机病毒具有正常程序的一切特性：可存储性、可执行性。它隐藏在合法的程序或数据中，当用户运行正常程序时，病毒伺机窃取到系统的控制权，得以抢先运行，然而此时用户还认为在执行正常程序。

2. 隐蔽性

计算机病毒是一种具有很高编程技巧、短小精悍的可执行程序。它通常粘附在正常程序、磁盘引导扇区中，或者磁盘上标为坏簇的扇区中，以及一些空闲概率较大的扇区中，这是它的非法可存储性。病毒想方设法隐藏自身，就是为了防止用户察觉。

3. 传染性

传染性是计算机病毒最重要的特征，是判断一段程序代码是否为计算机病毒的依据。病毒程序一旦侵入计算机系统，就开始搜索可以传染的程序或者磁介质，然后通过自我复制迅速传播。由于目前计算机网络日益发达，计算机病毒可以在极短的时间内通过 Internet 传遍世界。

4. 潜伏性

计算机病毒具有依附于其他媒体而寄生的能力，这种媒体称为计算机病毒的宿主。依靠病毒的寄生能力，病毒传染合法的程序和系统后，不立即发作，而是悄悄隐藏起来，然后在用户不察觉的情况下进行传染。这样，病毒的潜伏性越好，它在系统中存在的时间也就越长，病毒传染的范围也越广，其危害性也越大。

5. 表现性或破坏性

无论何种病毒程序，一旦侵入系统都会对操作系统的运行造成不同程度的影响。即使不直接产生破坏作用的病毒程序也要占用系统资源（如占用内存空间、磁盘存储空间及系统运行时间等）。而绝大多数病毒程序要显示一些文字或图像，影响系统的正常运行。还有一些病毒程序删除文件，加密磁盘中的数据，甚至摧毁整个系统和数据，使之无法恢复，造成无可挽回的损失。因此，病毒程序的副作用轻则降低系统的工作效率，重则导致系统崩溃、数据丢失。病毒程序的表现性或破坏性体现了病毒设计者的真正意图。

6. 可触发性

计算机病毒一般都有一个或者几个触发条件。满足其触发条件或者激活病毒的传染机制，即可使之传染，也可以激活病毒的表现部分或破坏部分。触发的实质是一种条件的控制，病毒程序可以依据设计者的要求，在一定条件下实施攻击。这个条件可以是敲入特定字符、使用特定文件、某个特定日期或特定时刻，或者是病毒内置的计数器达到一定次数等。

5.2.2 计算机病毒的传播途径

传染性是计算机病毒最重要的特征，计算机病毒从已被感染的计算机到未被感染的计算机，必须通过某些方式来进行传播，最常见的就是以下两种方式。

第一种：通过移动存储设备来进行传播，包括软盘、光盘、移动硬盘和 U 盘等。

在计算机应用早期，计算机应用较简单，许多文件都是通过软盘来进行相互复制、安装，这时，软盘就是最好的计算机病毒的传播途径。光盘容量大、存储内容多，所以大量的病毒有可能藏匿在其中。对于只读光盘，不能进行写操作，其上的病毒更加不能查杀。目前，盗版光盘泛滥，这给病毒的传染带来了极大的便利。加之现在广泛使用移动硬盘和 U 盘来交换数据，因此这些存储设备也就成了计算机病毒的主要寄生的“温床”。

第二种：通过网络来进行传播。

毫无疑问，网络是现在计算机病毒传播的重要途径。人们平时浏览网页、下载文件、收发电子邮件、访问 BBS 等，都可能使计算机病毒从一台计算机传播到网络上的其他计算机。

5.3 计算机病毒的分类

计算机病毒的种类有很多，按照计算机病毒的特征可以将计算机病毒的分为许多种。

1. 按寄生方式分

按寄生方式分可分为引导型病毒、文件型病毒和混合型病毒。

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，在引导型系统的过程中侵入系统，驻留内存，监视系统运行，待机传染和破坏。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、2708 病毒、火炬病毒等；分区引导记录病毒感染硬盘的活动分区引导记录，如小球病毒、Girl 病毒等。

文件型病毒是指能够寄生在文件中的计算机病毒。这类病毒程序感染可执行文件或数据文件。如 1575/1591 病毒、848 病毒感染. com 和. exe 文件，Macro/Concept、Macro/Atoms 等宏病毒感染. doc 文件。

混合型病毒是指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。当感染有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、清除混合型病毒时，必须全面彻底地根治。如果只发现该病毒的一个特性，把它只当做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”系统更赋有攻击性。常见的这种类型的病毒有 Flip 病毒、新世纪病毒、One. half 病毒等。

2. 按破坏性分

按破坏性分可分为良性病毒和恶性病毒。

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，增加系统开销，降低系统工作效率的一类计算机病毒。这种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，而是为了让使用感染有病毒的计算机用户了解病毒设计者的编程技术。这类病毒常见的有小球病毒、1575/1591 病毒、救护车病毒、扬基病毒、Dabi 病毒等。还有一些人利用病毒的这些特点宣传自己的政治观点和主张，也有一些病毒设计者在其编制的病毒发作时进行人身攻击。

恶性病毒是指那些一旦发作，就会破坏系统或数据，造成计算机系统瘫痪的一类计算机病毒。这类病毒常见的有黑色星期五病毒、火炬病毒、米开朗·基罗病毒等。这种病毒的危害性极大，有些病毒发作后可以给用户造成不可挽回的损失。

5.4 计算机病毒的破坏行为及防御

5.4.1 计算机病毒的破坏行为

计算机病毒的破坏行为体现了病毒的杀伤能力。病毒破坏行为的激烈程度取决于病毒作者的主观愿望和其所具有的技术能量。数以万计、不断发展扩张的病毒，其破坏行为千奇百怪。根据常见的病毒特征，可以把病毒的破坏目标和攻击部位归纳如下。

1. 攻击系统数据区

攻击部位包括硬盘主引导扇区、Boot 扇区、FAT 表、文件目录。一般来说，攻击系统数据区的病毒是恶性病毒，受损的数据不易恢复。

2. 攻击文件

病毒对文件的攻击方式很多，一般包括删除、改名、替换内容、丢失部分程序代码、内容颠倒、写入时间空白、假冒文件、丢失文件簇、丢失数据文件等。

3. 攻击内存

内存是计算机的重要资源，也是病毒经常攻击的目标。病毒额外地占用和消耗系统的内存资源，可以导致一些程序受阻，甚至无法正常运行。

病毒攻击内存的方式有占用大量内存、改变内存容量、禁止分配内存、蚕食内存。

4. 干扰系统运行

病毒会干扰系统的正常运行，以此达到自己的破坏行为。一般表现为不执行命令、干扰内部命令的执行、虚假报警、打不开文件、内部栈溢出、占用特殊数据区、时钟倒转、重启动、死机、强制游戏、扰乱串并行口等。

5. 速度下降

病毒激活时，其内部的时间延迟程序启动。在时钟中载入了时间的循环计数，迫使计算机空转，计算机速度明显下降。

6. 攻击磁盘

攻击磁盘表现为攻击磁盘数据、不写盘、写操作变读操作、写盘时丢字节。

7. 扰乱屏幕显示

病毒扰乱屏幕显示一般表现为字符跌落、环绕、倒置、显示前一屏、光标下跌、滚屏、抖动、乱写、吃字符等。

8. 干扰键盘操作

病毒干扰键盘操作主要表现为响铃、封锁键盘、换字、抹掉缓存区字符、重复、输入紊乱等。

9. 使喇叭发声

许多病毒运行时，会使计算机的喇叭发出响声。有的病毒作者让病毒演奏旋律优美的世界名曲，在高雅的曲调中抹掉人们的信息财富。一般表现为演奏曲子、警笛声、炸弹噪声、鸣叫、咔咔声、嘀嗒声等。

10. 攻击 CMOS

在机器的 CMOS 中保存着系统的重要数据，如系统时钟、磁盘类型、内存容量等，并具有校验和。有些病毒激活时，能够对 CMOS 进行写入动作，破坏系统 CMOS 中的数据。

11. 干扰打印机

干扰打印机主要表现为假报警、间断性打印、更换字符。

5.4.2 计算机病毒的防御

怎样有效地防御计算机病毒呢？建议用户在自己的计算机上进行以下操作：

(1) 在计算机上安装杀毒软件和防火墙软件，这里以瑞星杀毒软件和瑞星防火墙软件为例。

(2) 及时升级杀毒软件，尤其在病毒盛行期间或者病毒突发的非常时期，这样做可以保证用户的计算机受到持续的保护。

(3) 使用流行病毒专杀工具。例如，一旦暴发恶性病毒，瑞星公司会第一时间在瑞星网站(http://www.rising.com.cn)上提供专杀工具下载，针对性强，速度快，防止病毒扩散。

(4) 开启杀毒软件的实时监控中心功能，系统启动后立即启用计算机监控功能，防止病毒侵入计算机。例如，瑞星监控中心是用户实时的、多层级的病毒防御体系，关闭瑞星监控中心将大大增加病毒侵入的风险，建议开启瑞星监控中心并设置密码，以防止别人关闭。

(5) 定期全面扫描系统(建议个人计算机每周一次，服务器每天深夜全面扫描一次系统)。

(6) 复制任何文件到本机时，建议使用杀毒软件的右键查杀功能进行专门查杀。

(7) 以纯文本方式阅读信件，不要轻易打开电子邮件附件，建议启动瑞星杀毒软件邮件监控功能。

(8) 从互联网下载任何文件时，需检查该网站是否具有安全认证。在通过即时通信软件(如 QQ、MSN Messenger)传送文件或者从互联网下载文件时，建议使用杀毒软件嵌入式

杀毒工具，接收文件后自动调用杀毒软件扫描病毒。

(9) 不要访问某些可能含有恶意脚本或者蠕虫病毒的网站，建议启用杀毒软件网页监控功能。

(10) 及时获得反病毒预报警示。例如，在病毒暴发前，用户可通过浏览瑞星反病毒资讯网站(http://www.rising.com.cn)、瑞星杀毒软件主界面中的信息中心或者手机短信来获得病毒暴发的预报信息。

(11) 建议使用 Windows Update 更新操作系统，或者使用杀毒软件系统漏洞扫描工具及时下载并安装补丁程序。

(12) 使用防火墙软件，防止黑客程序侵入计算机。

5.4.3 如何降低由病毒破坏所引起的损失

降低由病毒破坏所引起的损失主要有以下两种方法：

(1) 定期备份硬盘数据。万一硬盘数据损坏或丢失，可使用杀毒软件的硬盘数据备份功能恢复数据。

(2) 用户可以通过邮件、电话、传真等方式与杀毒软件的客户服务中心联系，由他们的技术中心提供专业的服务，尽量减少由病毒破坏造成的损失。

5.4.4 计算机病毒相关法律法规

为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行，制定了《中华人民共和国计算机信息系统安全保护条例》。

为了加强对计算机病毒的预防和治理，保护计算机信息系统安全，保障计算机的应用与发展，根据《中华人民共和国计算机信息系统安全保护条例》的规定，制定了《计算机病毒防治管理办法》。

为了加强计算机信息系统安全专用产品的管理，保证安全专用产品的安全功能，维护计算机信息系统的安全，根据《中华人民共和国计算机信息系统安全保护条例》第十六条的规定，制定了《计算机信息系统安全专用产品检测和销售许可证管理办法》。

5.5 常见病毒的查杀

5.5.1 CIH 病毒的查杀

CIH 病毒最早于 1998 年 6 月初在台湾被发现，它是一位名叫陈盈豪(Chen Ing. Halu)的台湾大学生所编写的，由于其名字的第一个字母分别为 C、I、H，所以称为 CIH 病毒。CIH 病毒的载体是一个名为“ICQ 中文 Ch_at 模块”的工具，并以热门盗版光盘游戏如“古墓奇兵”或 Windows 95/98 为媒介，经互联网中的网站互相转载，使其迅速传播。目前传播的主要途径是 Internet 和电子邮件。

CIH 病毒属文件型病毒，它主要感染 Windows 95/98 系统下的 EXE 文件。当一个染毒的 EXE 文件被执行，CIH 病毒便驻留在内存，当其他程序访问时可对它们进行感染。其发展过程经历了 v1.0、v1.1、v1.2、v1.3、v1.4 总共 5 个版本，目前较为流行的是 v1.2 版本，

在此期间，同时产生了不下十个的变种，但是没有流行起来的迹象。

CIH 病毒属恶性病毒，当其发作条件成熟时，将破坏硬盘数据，同时有可能破坏 BIOS 程序。其发作特征是，某些主板上的 Flash ROM 中的 BIOS 信息将被清除。

瑞星公司提供了针对硬盘的 CIH 病毒修复工具，用户可以到相关的网站上下载此修复工具，瑞星公司提供的本程序只针对 CIH 病毒破坏的硬盘进行修复，对于正常的硬盘不要使用此程序处理。此程序不能保证修复所有硬盘数据，也不能保证修复后的数据是完全正确的，只是尽可能地修复用户数据。此程序只修复第一块硬盘，如果有多块硬盘，需将其他硬盘摘下，一块一块地对其进行修复。

修复的操作步骤如下：

(1) 该软件包括两个程序：ANTICIH. EXE 和 RAV. REC。这两个程序必须复制到软盘的同一路径下。

(2) 用无毒的软盘启动计算机。

(3) 执行 ANTICIH. EXE，该程序将对硬盘进行扫描，以获得有关数据。

(4)扫描完成后，程序将显示如下提示。

```
Hard disk scanned result:
SIZE CYLS HEAD SECTOR
XXXX XXXX XXXX XXXX
Partition: C: D:
Drive C: FAT32
Recover partition table (Y/N)?
```

注意：SIZE 是硬盘的大小，以 MB 为单位；CYLS 是硬盘柱面数，HEAD 是硬盘的磁头数，SECTOR 是每道扇区数。对于大于 8GB 的硬盘，只显示硬盘大小。Partition 是找到的分区；Drive C：用于是说明 C 盘的格式，是 FAT16 或 FAT32。

针对不同的硬盘，提示信息不一样，此时确认是否要修复主引导记录，要修复请按 Y 键，否则按 N 键，本程序将退出。如果按了 Y 键，此程序将修复主引导记录，程序会进一步提示：

```
Recover drive C:(Y/N)?
```

如果修复 C 盘，请按 Y 键，否则按 N 键，程序将退出。

如果 C 盘是 FAT16，而且破坏比较严重，修复过程可能需要很长时间，需耐心等待。修复完成后，需重启系统。

5.5.2 宏病毒的查杀

宏病毒是一种寄存在文档或模板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，并转移到计算机上，驻留在 Normal 模板上。从此以后，所有自动保存的文档都会感染上这种宏病毒。如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。目前发现的几种主要宏病毒有 Wazzu、Concept、13 号病毒、Nuclear、July. killer(又名“七月杀手”)。

有些宏病毒对用户进行骚扰，但不破坏系统，比如，有一种宏病毒在每月的 13 日发作时会显示出 5 个数字连乘的心算数学题；有些宏病毒可使打印中途中断或打印出混乱信息，

如 Nuclear、Kompu 等属此类；有些宏病毒将文档中的部分字符、文本进行替换；但也有些“宏病毒”极具破坏性，如 MDMA. A，这种病毒既能感染中文版 Word，又能感染英文版 Word，发作时间是每月的 1 日。此病毒在不同的 Windows 平台上有不同的破坏性，轻则删除帮助文件，重则删除硬盘中的所有文件。另外，还有一种双栖复合型宏病毒，发作时可使计算机瘫痪。

1. 宏病毒的预防

宏病毒的预防要注意以下两点：

(1) 将常用的 Word 模板文件改为只读属性，可防止 Word 系统被感染；DOS 下的 autoexec. bat 和 config. sys 文件最好也都设为只读属性。

(2) 因为宏病毒是通过自动执行宏的方式来激活、进行传染破坏的，所以只要将自动执行宏功能禁止掉，此时即使有宏病毒存在，但无法被激活，也无法发作、传染、破坏，这样就起到了防毒的效果。

2. 宏病毒的制作以及查杀实例

下面通过简单制作一个宏病毒让大家对实际存在的宏病毒有一个了解，其具体制作步骤如下：

(1) 打开 Word 文字处理软件，在窗口菜单栏中选择【插入】→【对象】命令，在弹出的【对象】对话框中，选择【对象类型】列表框中的【包】选项，单击【确定】按钮，如图 5.1 所示。

图 5.1　设置对象类型

(2) 在如图 5.2 所示的【对象包装程序】窗口中选择【编辑】→【命令行】命令，在弹出的命令行区域中输入“ping －t localhost －l 60000”，完成后单击【确定】按钮，那么这条命令在永久地 ping 自己的计算机，并且每次发出的 ping 包都是 60 000 个字节，如此就会形成一个 DoS 攻击。黑客们编写的宏病毒往往比这个厉害，比如格式化硬盘的病毒等。

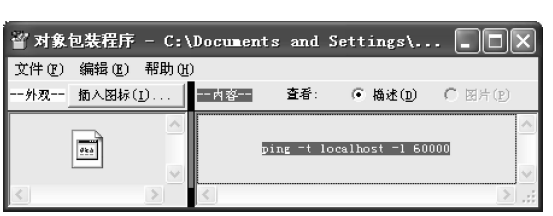

图 5.2　【对象包装程序】窗口

(3) 在如图 5.2 所示的【对象包装程序】窗口中，单击【插入图标】按钮，为该命令行选个有诱惑力的图标。在关闭【对象包装程序】窗口后，在文档的相关位置便出现了一个和命令关联的图标，如图 5.3 所示，这样一个宏病毒就制作成功了。

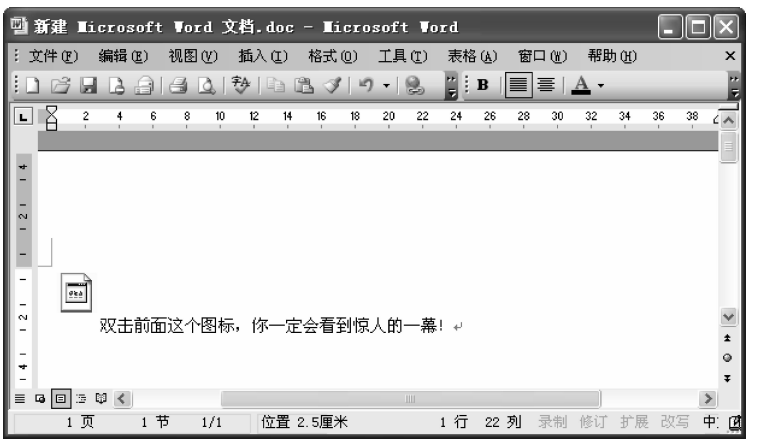

图 5.3 制作完成的 Word 中的宏病毒

真正的宏病毒不是这样制作的，真正的病毒会和宏指令相关联，如 FileOpen、FileSave、FileSaveAs 和 FilePrint 等命令，其内编写了可使系统瘫痪，能感染每一个 Word 文件的代码，并可以自动保存为模板文件。只要用户打开一次染毒的 Word 文件，则以后所有的 Word 文件都会被感染，看起来再正常不过的一个正规文档文件，很可能就暗藏着宏病毒。

刚才制作的宏病毒运行后的结果如图 5.4、图 5.5、图 5.6 所示。

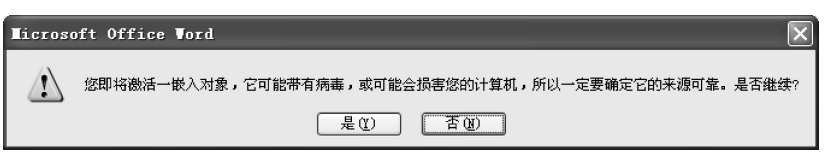

图 5.4 Word 中的宏病毒运行结果 1

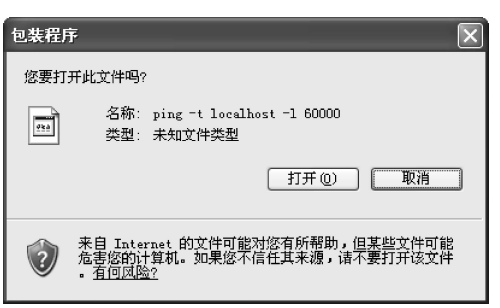

图 5.5 Word 中的宏病毒运行结果 2

3. 宏病毒的清除

清除宏病毒可通过手工或专业杀毒软进行，分别如下。

(1) 手工：以 Word 为例，最简单的就是禁止 Word 执行宏指令。方法是，在 Word 窗

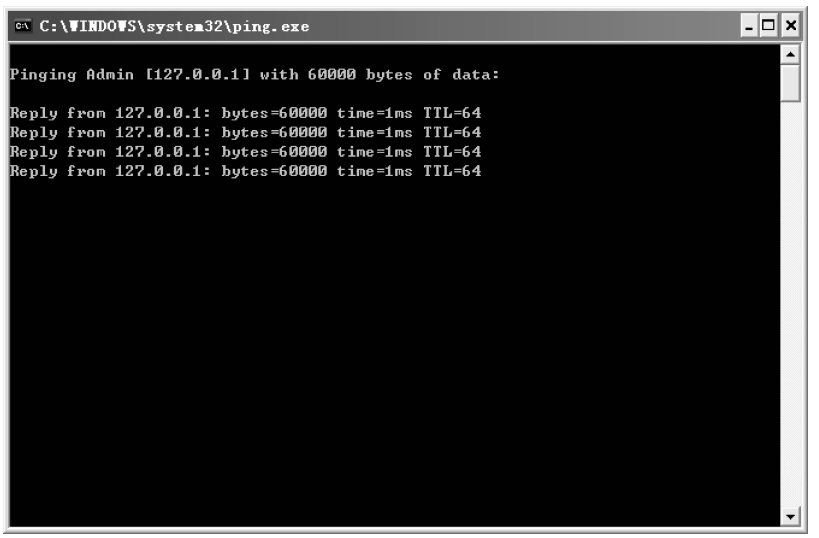

图 5.6　Word 中的宏病毒运行结果 3

口的菜单栏中选择【工具】→【宏】→【安全性】命令，在弹出的如图 5.7 的所示的对话框中将其安全性设置为高，这样，未经系统签署的宏指令将会被 Word 禁止执行，从而不利于宏病毒的运行。

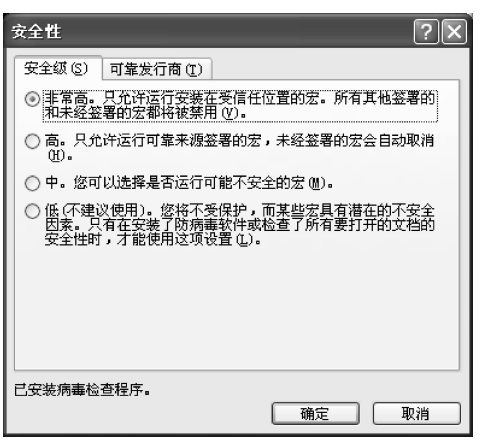

图 5.7　【安全性】对话框

(2) 使用专业杀毒软件：目前，杀毒软件公司都具备清除宏病毒的能力，当然也只能对已知的宏病毒进行检查和清除，对于新出现的病毒或病毒的变种则可能不能正常地清除。当有可能破坏文件的完整性时，建议还是手工清除。

5.5.3　蠕虫病毒的查杀

蠕虫病毒和一般的计算机病毒有着很大的区别。对于这种病毒，现在还没有一个成套的理论体系，但是一般认为，蠕虫病毒是一种通过网络传播的恶性病毒，它除了具有病毒的一些共性外，还具有自己的一些特征。例如不利用文件寄生(有的只存在于内存中)，对网络

造成拒绝服务，以及与黑客技术相结合等。蠕虫病毒主要的破坏方式是大量地复制自身，然后在网络中传播，严重地占用有限的网络资源，最终引起整个网络的瘫痪，使用户不能通过网络进行正常的工作。每一次蠕虫病毒的暴发都会给全球经济造成巨大损失，因此它的危害性是十分巨大的。有一些蠕虫病毒还具有更改用户文件、将用户文件自动作为附件转发的功能，更是严重危害用户的系统安全。

1. 蠕虫病毒常见的传播方式

蠕虫病毒常见的传播方式如下。

(1) 利用系统漏洞传播：蠕虫病毒利用计算机系统的设计缺陷，通过网络主动地将自己扩散出去。

(2) 利用电子邮件传播：蠕虫病毒将自己隐藏在电子邮件中，随电子邮件扩散到整个网络中，这也是个人计算机被感染的主要途径。

2. 蠕虫病毒感染的对象

蠕虫病毒一般不寄生在别的程序中，而多作为一个独立的程序存在。它感染的对象是网络中的所有的计算机，并且这种感染是主动进行的，所以总是让人防不胜防。在现今全球网络高度发达的情况下，一种蠕虫病毒在几个小时之内蔓延全球并不是什么困难的事情。

现在流行的蠕虫病毒主要有尼姆达、红色代码、冲击波、震荡波、求职信，以及 2007 年最为流行的熊猫烧香。本书以冲击波和熊猫烧香为例来讲解蠕虫病毒的危害及如何清除。

3. 冲击波(Worm. Blaster)病毒的介绍

病毒运行时会不停地利用 IP 扫描技术寻找网络上系统为 Windows 2000 或 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，病毒体将会被传送到对方计算机中进行感染，使系统操作异常、不停地重启，甚至导致系统崩溃，如图 5.8 所示。另外，该病毒还会对微软的一个升级网站进行拒绝服务攻击，导致该网站堵塞，使用户无法通过该网站升级系统。该病毒还会使被攻击的系统丧失更新该漏洞补丁的能力。

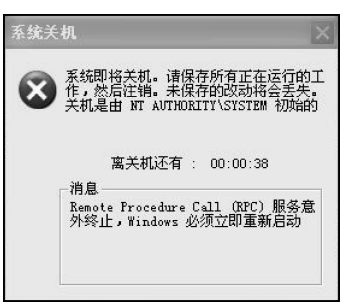

图 5.8　冲击波病毒的症状

4. 冲击波(Worm. Blaster)病毒的防范与查杀

具体步骤如下：

(1) 用户可以先进入微软网站，下载相应的系统补丁，给系统打上补丁。每个 Windows 都有相应的版本，下面是一个 Windows XP 的 32 位版本的下载补丁地址。

http://microsoft. com/downloads/details. aspx? FamilyId＝2354406C. C5B6. 44AC. 9532. 3DE40F69C074&displaylang＝en

(2) 病毒运行时会建立一个名为 BILLY 的互斥量，使病毒自身不重复进入内存，并且病毒在内存中建立一个名为 msblast 的进程，用户可以用任务管理器将该病毒进程终止。

(3) 病毒运行时会将自身复制为%systemdir%\msblast. exe，用户可以手动删除该病毒文件。

注意：%systemdir%是一个变量，它指的是操作系统安装目录中的系统目录，默认是“C:\Windows\system”或“C:\Winnt\system32”。

(4) 病毒会修改注册表的 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\

Windows\CurrentVersion\Run 项，在其中加入"windows auto update"="msblast.exe"，进行自启动，用户可以手工清除该键值。

(5) 病毒会用到 135、4444、69 等端口，用户可以使用 Windows 防火墙软件将这些端口禁止或者使用 TCP/IP 筛选功能禁止这些端口。

(6) 用户也可以使用瑞星专杀工具来进行查杀，图 5.9 所示就是【RPC 漏洞蠕虫专用查杀工具】窗口。

图 5.9 【RPC 漏洞蠕虫专用查杀工具】窗口

5. 熊猫烧香病毒的介绍

熊猫烧香(worm.nimaya)又称武汉男生或者尼姆亚，是一种蠕虫病毒，是由 Delphi 编程工具编写的，能终止大量的反病毒软件和防火墙软件。病毒会删除扩展名为.gho 的文件，使用户无法使用 Ghost 软件恢复操作系统。熊猫烧香病毒可感染系统的.exe .com. pif .src .html .asp 文件，添加病毒网址，导致用户一打开这些网页文件，IE 浏览器就会自动连接到指定的病毒网址中下载病毒，并在硬盘各个分区下生成文件 autorun.inf 和 setup.exe。该病毒可以通过 U 盘和移动硬盘等方式进行传播，并且利用 Windows 系统的自动播放功能来运行，搜索硬盘中的.exe 可执行文件并感染，感染后的文件图标变成"熊猫烧香"图案。熊猫烧香病毒还可以通过共享文件夹、系统弱口令等多种方式进行传播。这是中国近年来发生的比较严重的一次蠕虫病毒发作，影响了较多公司，造成了较大的损失。图 5.10 所示为感染病毒后的熊猫烧香图标。

6. 熊猫烧香病毒的防范

防范熊猫烧香病毒的具体步骤如下：

(1) 安装杀毒软件，并在上网时打开网页实时监控。

(2) 网站管理员应该更改机器密码，以防止病毒通过局域网传播。

(3) 当 QQ、UC 的漏洞已经被该病毒利用时，用户应该去相应的官方网站打好最新补丁。

(4)该病毒会利用 IE 浏览器的漏洞进行攻击，因此用户应该给 IE 浏览器打好所有的补丁。如果有必要，用户可以暂时使用 Firefox、Opera 等比较安全的浏览器。

7. 熊猫烧香病毒的清除

如果计算机中了熊猫烧香病毒，则可以采取以下步骤来对它进行清除：

图 5.10　熊猫烧香被感染后的文件图标

（1）断开网络。

（2）结束病毒进程“%System%\FuckJacks.exe”。

（3）删除病毒文件“%System%\FuckJacks.exe”。

（4）在分区盘符上单击右键，在弹出的快捷菜单中选择“打开”命令，进入分区根目录，删除根目录下的两个文件：X:\autorun.inf 和 X:\setup.exe。

（5）在注册表中删除病毒创建的启动项：

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"FuckJacks" = "%System%\FuckJacks.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"svohost" = "%System%\FuckJacks.exe"
```

（6）修复或重新安装反病毒软件。

（7）使用反病毒软件或专杀工具进行全盘扫描，清除恢复被感染的.exe 文件。图 5.11 所示为瑞星公司的熊猫烧香专杀工具窗口。

图 5.11　熊猫烧香专杀工具窗口

5.6 部署企业版杀毒软件

5.6.1 企业版杀毒软件概述

防病毒是网络安全的重中之重。当网络中的个别客户端感染病毒后，就有可能在极短的时间内感染整个网络，造成网络服务中断或瘫痪，所以局域网的防病毒工作非常重要。最常用的方法就是在网络中部署企业版杀毒软件，比如 Symantec AntiVirus、趋势科技与瑞星的网络版杀毒软件等。本节重点讲解 Symantec 公司推出的新一代企业版网络安全防护产品——Symantec Endpoint Protection(端点保护)。它将 Symantec AntiVirus 与高级威胁防御功能相结合，可以为笔记本电脑、台式机和服务器提供安全防护功能。它在一个代理和管理控制台中无缝集成了基本安全技术，不仅提高了防护能力，而且还有助于降低总拥有成本。

1. 主要功能

(1) 无缝集成了一些基本技术，如集成了防病毒、反间谍软件、防火墙、入侵防御和设备控制技术。

(2) 只需要一个代理，通过一个管理控制台，即可进行管理。

(3) 由端点安全领域的市场领导者提供无可匹敌的端点防护。

(4) 无须对每个端点额外部署软件，即可立即进行 NAC 升级。

2. 主要优势

(1) 阻截恶意软件，如病毒、蠕虫、特洛伊木马、间谍软件、恶意软件、零日威胁和 Rootkit。

(2) 防止安全违规事件的发生，从而降低管理开销。

(3) 降低保障端点安全的总拥有成本。

新一代 Symantec 安全防护产品主要包括 Symantec Endpoint Protection(端点保护)和 Symantec Network Access Control(端点安全访问控制)两种。每一种功能都可以提供强大的 Symantec Endpoint Protection Manager(端点保护管理)，以帮助管理员快速完成网络安全的统一部署和管理。

课业任务 5-1

WYL 公司采用 Symantec Endpoint Protection(端点保护)作为安全防护解决方案，网络管理员需要在一台安装 Windows Server 2008 操作系统的计算机上安装 Symantec Endpoint Protection 服务器端软件，然后对其受管的所有客户端进行部署。

下面通过 5.6.2、5.6.3、5.6.4、5.6.5 这 4 小节分别来讲解服务器端与客户端的安装与部署，以完成课业任务 5-1。

5.6.2 安装 Symantec Endpoint Protection Manager

安装步骤如下：

(1) 插入安装光盘，双击光盘根目录下的 Setup.exe 文件，启动安装程序，显示如图 5.12 所示的【Symantec Endpoint Protection 安装程序】窗口。

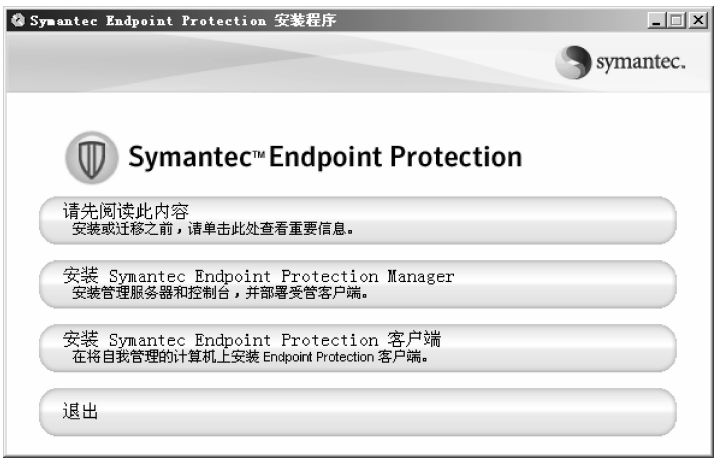

图 5.12 【Symantec Endpoint Protection 安装程序】窗口

(2) 在图 5.12 所示的窗口中单击【安装 Symantec Endpoint Protection Manager】按钮，启动 Symantec Endpoint Protection Manager 安装向导，弹出如图 5.13 所示的【欢迎使用 Symantec Endpoint Protection Manager 安装向导】对话框。

图 5.13 【欢迎使用 Symantec Endpoint Protection Manager 安装向导】对话框

(3) 在图 5.13 所示的对话框中单击【下一步】按钮，弹出如图 5.14 所示的【授权许可协议】对话框，选择【我接受该许可证协议中的条款】单选按钮。

(4) 在图 5.14 所示的对话框中单击【下一步】按钮，弹出如图 5.15 所示的【目录文件夹】对话框，单击【更改】按钮可以重新选择安装目录，建议使用默认安装路径。

(5) 在图 5.15 所示的对话框中单击【下一步】按钮，弹出如图 5.16 所示的【选择网站】对话框。若要在该服务器上使 Symantec Endpoint Protection Manager IIS Web 和原有的 Web 站点同时运行，则选择【使用默认 Web 站点】单选按钮；若要将 Symantec Endpoint Protection Manager IIS Web 配置为当前服务器上唯一的 Web 站点，则选择【创建自定义站点(建议)】单选按钮。为了提高服务器的安全性，建议选择【创建自定义站点(建议)】单选按钮。

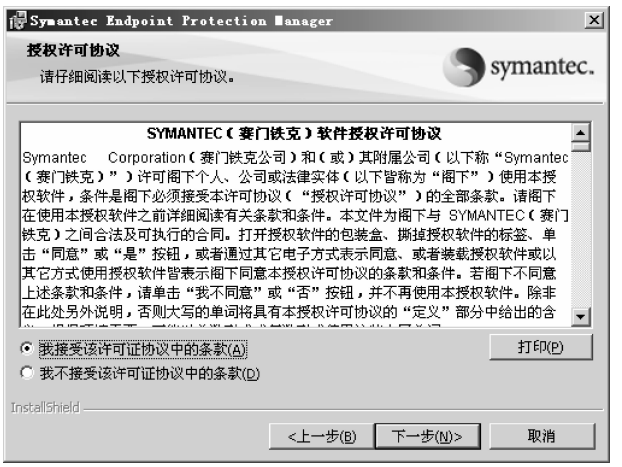

图 5.14 【授权许可协议】对话框

图 5.15 【目标文件夹】对话框

图 5.16 【选择网站】对话框

(6) 在图 5.16 所示的对话框中单击【下一步】按钮,弹出如图 5.17 所示的【准备安装程序】对话框,提示安装向导已经准备就绪。

图 5.17 【准备安装程序】对话框

(7) 在图 5.17 所示的对话框中单击【安装】按钮,即开始安装,需要等待几分钟时间,完成后弹出如图 5.18 所示的【安装向导已完成】对话框。

图 5.18 【安装向导已完成】对话框

(8) 在图 5.18 所示的对话框中单击【完成】按钮,即可完成 Symantec Endpoint Protection Manager 的安装。

5.6.3 配置 Symantec Endpoint Protection Manager

安装完成 Symantec Endpoint Protection Manager 后,还应该对其进行配置,包括创建服务器组,设置站点名称、管理员密码、客户端安装方式,以及制作客户端安装包等。其具体操作步骤如下:

(1) 选择【开始】→【程序】→Symantec Endpoint Protection Manager→【管理服务器配

置向导】命令，弹出如图 5.19 所示的【欢迎使用管理服务器配置向导】窗口。此处提供【简单】与【高级】两种配置类型。其区别在于，【简单】是指小于 100 个用户的情况，并且使用嵌入式数据库，而【高级】是指大于 100 个用户，同时可以使用 Microsoft SQL Server 作为数据库。本任务因为企业规划不大，因此选择【简单】单选按钮。

图 5.19 【欢迎使用管理服务器配置向导】窗口

（2）在图 5.19 所示的窗口中单击【下一步】按钮，弹出如图 5.20 所示的【创建系统管理员账户】窗口，设置登录 Symantec Endpoint Protection Manager 的用户名与密码。

图 5.20 【创建系统管理员账户】窗口

(3) 在图 5.20 所示的窗口中单击【下一步】按钮，弹出如图 5.21 所示的显示配置相关信息窗口，显示管理服务器使用的相关配置信息。

图 5.21　显示配置相关信息窗口

(4) 在图 5.21 所示的窗口中单击【下一步】按钮，等待系统创建好数据库之后，弹出如图 5.22 所示的【管理服务器配置向导已完成】窗口，完成 Symantec Endpoint Protection Manager 的配置。

图 5.22　【管理服务器配置向导已完成】窗口

5.6.4 迁移和部署向导

迁移和部署向导主要用来帮助管理员完成客户端的部署，或者将客户端从旧版本 Symantec AntiVirus 迁移到 Symantec Endpoint Protection 管理平台。

迁移和部署向导的具体操作步骤如下：

(1) 用户可以在完成管理服务器配置向导后立即开始部署，也可以选择【开始】→【迁移和部署向导】命令，弹出如图 5.23 所示的【欢迎使用迁移和部署向导】窗口。

图 5.23 【欢迎使用迁移和部署向导】窗口

(2) 在图 5.23 所示的窗口中单击【下一步】按钮，弹出如图 5.24 所示的【您选择何种操作】窗口，本任务选择【部署客户端】单选按钮。

图 5.24 【您选择何种操作】窗口

(3) 在图 5.24 所示的窗口中单击【下一步】按钮，弹出如图 5.25 所示的指定要部署的客户端组窗口，选择【指定您要部署客户端的新组名】单选按钮，本任务在文本框中输入组名“thxy”。

图 5.25　指定要部署的客户端组窗口

(4) 在图 5.25 所示的窗口中单击【下一步】按钮，弹出如图 5.26 所示的选择包含的功能窗口，通常情况下保持默认即可。如果客户端使用 Outlook 收发邮件，则也可以选择【Microsoft Outlook 扫描程序】复选框。

图 5.26　选择包含的功能窗口

(5) 在图 5.26 所示的窗口中单击【下一步】按钮，弹出如图 5.27 所示的定制客户端软件功能窗口，本任务选择无人参与的 32 位的.exe 文件，另外，还可以选择生成客户端软件存放的路径。

图 5.27　定制客户端软件功能窗口

(6) 在图 5.27 所示的窗口中单击【下一步】按钮，弹出如图 5.28 所示的是否立即部署到远程客户端窗口，如果选择【是】单选按钮，则立即开始在远程计算机上安装 SEP 客户端，本任务选择【否，只要创建即可，我稍后会部署】单选按钮。

图 5.28　是否立即部署到远程客户端窗口

(7) 在图 5.28 所示的窗口中单击【完成】按钮，关闭迁移与部署向导，默认情况下将弹出【Symantec Endpoint Protection Manager 控制台】窗口，显示如图 5.29 所示的登录界面。

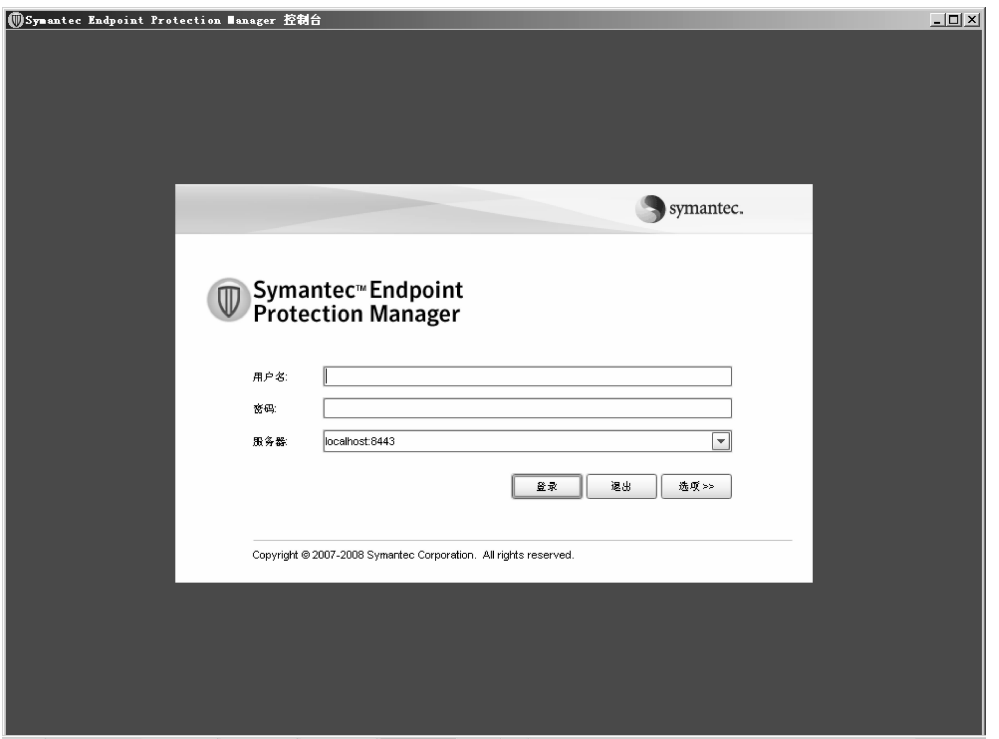

图 5.29　登录界面

5.6.5　安装 Symantec Endpoint Protection 客户端

Symantec Endpoint Protection 客户端分为受管理客户端与非受管理客户端，其中，受管理客户端可以通过 Symantec Endpoint Protection Manager 远程部署等方式安装，也可以在客户端上使用管理服务器创建的安装包安装。安装完成后将自动添加到指定的组中，并接受服务器的统一管理。而非受管理客户端则可以通过安装光盘完成，虽然同样可以被添加到服务器控制台中，但不接受服务器的管理。需要注意的是，Symantec Endpoint Protection 客户端在安装过程中至少需要 700MB 的硬盘空间，如果空间不足，将导致失败。

对于受管理客户端的安装，用户可以通过以下几种方法部署接受 Symantec Endpoint Protection Manager 服务器管理的客户端：

- 迁移和部署向导的“推”式安装；
- 客户端映射网络驱动安装；
- 使用“查找非受管计算机”部署；
- 客户端手动安装；
- 使用 Altiris 安装和部署软件安装。

本任务介绍使用迁移和部署向导的“推”式安装，具体步骤如下：

(1) 启动迁移与部署向导，连续单击【下一步】按钮，直至弹出如图 5.30 所示的【迁移和部署向导】窗口，选择【选择现有客户端安装软件包以进行部署】单选按钮。

图 5.30　选择现有客户端安装软件包以进行部署

(2) 在图 5.30 所示的窗口中单击【下一步】按钮，弹出如图 5.31 所示的【推式部署向导】对话框。单击该对话框中的【浏览】按钮，选择已经创建完成的安装程序所在的目录，在【指定并行部署数量上限】文本框中输入相应的值，默认是 10 个。

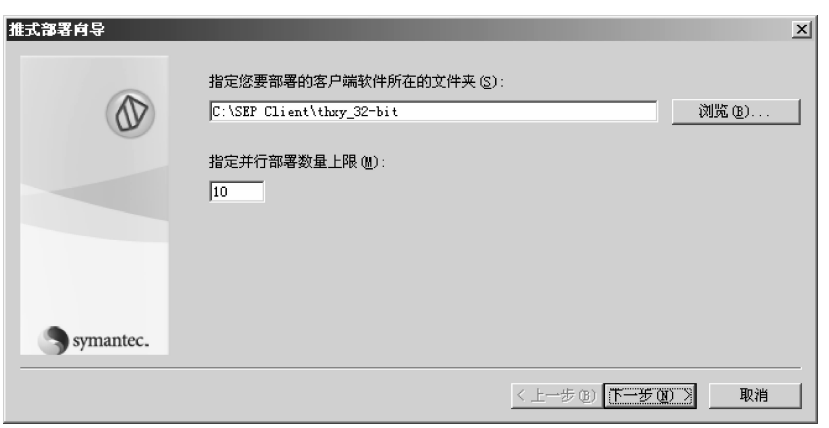

图 5.31　【推式部署向导】对话框

(3) 在图 5.31 所示的对话框中单击【下一步】按钮，弹出如图 5.32 所示的选择部署的计算机对话框，选择希望添加为客户端的计算机。

(4) 在图 5.32 所示的对话框中单击【添加】按钮，弹出如图 5.33 所示的【远程客户端验证】对话框，在【用户名】与【密码】文本框中输入远程登录目标计算机时使用的用户名信息，

图 5.32　选择部署的计算机

单击【确定】按钮，即可将其添加到图 5.32 所示的【要部署到的计算机】列表框中，重复操作可以添加多个客户端。

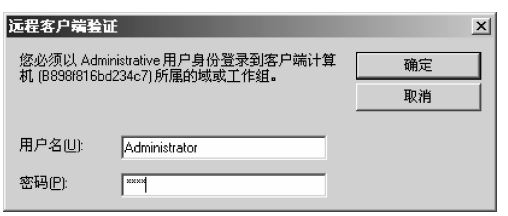

图 5.33　【远程客户端验证】对话框

(5) 添加完所有需要部署的客户端之后，在图 5.32 所示的对话框中单击【完成】按钮，即可以开始安装，弹出如图 5.34 所示的【远程客户端安装状态】对话框。

图 5.34　【远程客户端安装状态】对话框

(6) 安装完成后，弹出如图 5.35 所示的【推式部署向导】提示对话框，提示是否查看部署日志。如果并发部署多个客户端，则可能由于服务器性能导致部分客户端无法正常完成，此时可以通过日志确定完成情况。

至此，管理服务器上的远程部署工作完成了，客户端将开始自动安装，安装完成后将提示用户是否立即重新启动计算机。

图 5.35　提示对话框

5.6.6　升级病毒库

杀毒软件是根据提取的病毒特征来确定文件是否是病毒程序的，升级病毒库就是不断地更新能够识别的病毒库特征，增强杀毒软件与系统应用程序之间的兼容性。通常情况下，非受管理客户端每天从 Symantec LiveUpdate 站点下载病毒库。在新一代的 Symantec 安全防御系统中新增了 LiveUpdate 管理服务器，主要为大型网络提供客户端病毒库升级管理。

练　习　题

1. 选择题

(1) 计算机病毒是(　　)。

A. 编制有错误的计算机程序

B. 设计不完善的计算机程序

C. 已被破坏的计算机程序

D. 以危害系统为目的的特殊计算机程序

(2) 以下关于计算机病毒特征的说法正确的是(　　)。

A. 计算机病毒只具有破坏性，没有其他特征

B. 计算机病毒具有破坏性，不具有传染性

C. 破坏性和传染性是计算机病毒的两大主要特征

D. 计算机病毒只具有传染性，不具有破坏性

(3) 计算机病毒是一段可运行的程序，它一般(　　)保存在磁盘中。

A. 作为一个文件　　B. 作为一段数据

C. 不作为单独文件　　D. 作为一段资料

(4) 下列措施中，(　　)不是减少病毒传染和造成损失的好办法。

A. 重要的文件要及时、定期备份，使备份能反映出系统的最新状态

B. 外来的文件要经过病毒检测才能使用，不要使用盗版软件

C. 不与外界进行任何交流，所有软件都自行开发

D. 定期用杀毒软件对系统进行查毒、杀毒

(5) 下列关于计算机病毒的说法中，正确的是(　　)。

A. 计算机病毒是磁盘发霉后产生的一种会破坏计算机的微生物

B. 计算机病毒是患有传染病的操作者传染给计算机，影响计算机正常运行

C. 计算机病毒有故障的计算机自己产生的可以影响计算机正常运行的程序

D. 计算机病毒人为制造出来的干扰计算机正常工作的程序

(6) 计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，此特征为计算机病毒的(　　)。

A. 潜伏性　　B. 传染性

C. 欺骗性　　D. 持久性

(7) 计算机病毒的主要危害有(　　)。

A. 损坏计算机的外观　　B. 干扰计算机的正常运行

C. 影响操作者的健康　　D. 使计算机腐烂

2. 填空题

(1) Office 中的 Word、Excel、PowerPoint、Viso 等很容易感染_____病毒。

(2) _____是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

(3) 冲击波和震荡波都是属于_____病毒。

第6章 Windows 2008操作系统的安全

操作系统是连接计算机硬件与上层软件及用户的桥梁，也是计算机系统的核心。因此，操作系统的安全性与否直接决定着信息是否安全。作为网络操作系统或服务器操作系统，高性能、高可靠性和高安全性是其必备要素，尤其是日趋复杂的企业应用和Internet应用，对其提出了更高的要求。Windows Server 2008是新一代Windows Server操作系统，是专为强化新一代网络、应用程序和Web服务功能而设计的。Windows Server 2008操作系统不仅保留了Windows Server 2003的所有优点，而且还引进了多项新技术。该操作系统使用ASLR(Address Space Layout Randomization，随机地址空间分配)技术、更好的防火墙功能及BitLocker磁盘加密功能，还加入了加强诊断和监测的功能、存储及文件系统的改进功能，可自行恢复NTFS文件系统。同时，还加强了管理，改写了网络协议栈，其中包括支持IPv6等功能。

学习目标

- 掌握Windows 2008操作系统的用户安全管理、账号与密码设定，以及账号和密码安全设定的常用方法。
- 掌握文件系统安全管理，包括NTFS权限、共享权限、权限叠加，以及使用文件服务器资源管理器实现文件屏蔽的方法。
- 熟练掌握Windows 2008主机安全的配置。
- 熟练掌握常见的本地组策略的配置。

课业任务

本章通过8个实际课业任务，由浅入深、循序渐进地介绍Windows 2008操作系统的用户、文件及主机安全。

课业任务6-1

Bob是WYL公司的网络管理员，公司服务器安装的是Windows Server 2008操作系统，为了保证服务器的安全，Bob在服务器上更改了Administrator账户名称，并创建了一个名称为Administrator的陷阱账户。

能力观测点

Windows 2008账号与密码安全设置；创建陷阱账户。

课业任务6-2

WYL公司的文件服务器安装的是Windows Server 2008操作系统，服务器D盘使用NTFS格式。现要求网络管理员在D盘创建一个共享文件夹，命名为【开发部文件夹】，并通过设置合适的NTFS权限和共享权限，使开发部的员工能够通过网络在【开发部文件夹】内创建自己的文件夹，以用于保存个人的文件。每个员工对自己的文件夹有完全控制权限，