工业和信息化人才培养规划教材
Industry And Information Technology Training Planning Materials

Technical And Vocational Education
高职高专计算机系列

网络安全技术与实践

The Technique and Practice of Network Security

蒋亚军 ◎ 主编
詹增荣 王伟 曾青松 ◎ 副主编

本书依据岗位工作过程设计项目教学的内容，从网络“安管”的职业岗位能力为出发点，解决网络安全课程的教学难点

人民邮电出版社
POSTS & TELECOM PRESS

工业和信息化人才培养规划教材
Industry And Information Technology Training Planning Materials

Technical And Vocational Education
高职高专计算机系列

网络安全技术与实践

The Technique and Practice of Network Security

蒋亚军 ◎ 主编
詹增荣 王伟 曾青松 ◎ 副主编

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全技术与实践 / 蒋亚军主编. -- 北京 : 人民邮电出版社, 2012.8
工业和信息化人才培养规划教材. 高职高专计算机系列
ISBN 978-7-115-25976-9

Ⅰ. ①网… Ⅱ. ①蒋… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2011)第174990号

内 容 提 要

本书为项目式教学系列课改教材，教学内容源于计算机网络技术专业高职高专学生目标岗位群中“安全管理”所需的计算机网络安全知识与技能的要求。

全书设计了四篇教学内容，试图从认识和分析网络安全问题出发，让读者了解网络边界与内网安全的相关知识，掌握典型网络安全系统和设备的部署、安装与配置，熟悉典型计算机网络的安全设计。

本书可作为高职高专计算机信息、通信、网络及其相关专业的高年级的教材，也可作为相关技术领域专业技术人员的参考书。

工业和信息化人才培养规划教材——高职高专计算机系列

网络安全技术与实践

◆ 主　　编　蒋亚军
副 主 编　詹增荣　王　伟　曾青松
责任编辑　赵慧君

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京铭成印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：21.75　　2012年8月第1版
字数：565千字　　2012年8月北京第1次印刷

ISBN 978-7-115-25976-9

定价：43.80元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

随着网络通信技术的发展，计算机网络已经成了当代教学、科研、交通、银行、行政管理等各个行业工作中不可缺少的信息交换工具。人们对于计算机网络的依赖性越来越高，计算机网络正在影响着每个人的生活。

由于计算机网络存在开放性、互联性、连接形式的多样性以及终端分布的不均匀性等安全性问题，网络协议、操作系统与应用程序存在安全漏洞，无论是局域网还是广域网都存在着技术弱点和潜在威胁，致使网络很容易受黑客、恶意软件或病毒的攻击。近年来网络安全问题越来越严重，网络系统的建设需要考虑安全问题，网络的安全管理也成为了日常网络管理的重要内容，社会迫切需要网络安全技术人才。

本教材在教学内容的选取上以培养具体的网络“安全管理”的职业岗位能力为出发点，利用最新的教改成果，依据岗位工作过程设计项目教学的内容，解决网络安全课程的教学难点。全书分为网络安全分析、网络边界安全、内网安全与网络安全设计四篇，每篇都规定了明确的教学要求和目标。其中第一篇设计了“认识网络安全问题”和“网络安全检测”两个项目，试图通过这两个项目，让读者认识计算机网络中存在着如计算机病毒、木马、网络攻击、恶意软件等典型的安全问题，了解相关的知识；掌握判断网络安全性的网络安全检测技术，如网络扫描与嗅探技术，学会典型的扫描与嗅探工具的选取和使用。第二篇则介绍典型的网络边界安全技术，如防火墙、入侵检测系统、入侵防护系统、统一安全网关与网络隔离系统等技术，熟悉各种设备的类型、核心技术、功能特性、性能差异与产品线，通过课程的学习，让读者掌握这些安全设备的选型、部署与配置技术。第三篇介绍计算机内网的安全技术，包括操作系统的安全、内网应用服务的安全与内网安全管理。第四篇介绍典型网络的安全设计技术，包括政务网、企业网、校园网等。希望读者能够通过本教材学习，掌握实用的计算机网络安全的岗位知识与技能。

本书由广州番禺职业技术学院的蒋亚军任主编，詹增荣、王伟、曾青松任副主编。其中第一篇由曾青松编写，第二篇由蒋亚军编写，第三篇由詹增荣编写，第四篇由王伟编写，由蒋亚军统稿。书中的大部分插图由陈业友绘制。建议课堂教学为 72 学时，其中知识部分为 36 学时，实践部分为 36 学时。因为课程涉及的内容较多，全部教学内容很难在课程中完成，教材中每个项目中都设计有思考与练习，建议安排课余教学活动完成。

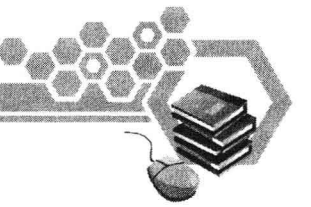
编写过程中得到了广州番禺职业技术学院网络中心的黄中伟、北京华夏创新科技有限公司的资深安全专家赵郁的大力协助，以及联想网御有关技术部门、易聆科信息技术有限公司的大力支持，在此表示感谢。

由于作者水平有限，书中难免出现错误与不当之处，恳请广大读者批评指正。

编　者

2012 年 5 月

目　录



第一篇

网络安全分析

网络安全分析就是分析网络存在的安全问题。本篇采用项目教学形式组织网络安全分析的教学内容，通过“认识网络安全问题”与“网络安全检测”两个项目的设计，让读者认识包括计算机病毒、木马、网络攻击、流氓软件等典型的网络安全问题，了解这些不同的网络安全问题的定义、特征、类型与对网络的破坏性，掌握一般的安全问题的检测与防护方法。了解网络端口扫描与网络监听的基本原理，熟悉典型的网络扫描与嗅探的工具。

项目一　认识网络安全问题

一、项目分析

【实施目标】

1. 知识目标

- 了解典型计算机病毒、类型与特征
- 了解木马的定义、类型与特点
- 熟悉典型网络攻击的类型与特点
- 了解流氓软件类型与特点

2. 技能目标

- 掌握常见杀毒软件工具的使用
- 掌握典型木马的安装、隐藏、启动与清除
- 掌握典型的网络攻击、检测与防护技术
- 掌握典型流氓软件的清除方法

【项目背景】

某企业存在严重的网络安全问题。网络主机病毒很严重，随便安装一个杀毒软件都可以查出很多病毒。网络攻击时有发生，网络经常无故出现阻塞，无法上网。员工反映主机上的流氓软件不少，干扰计算机的使用。企业经费比较紧张，需要懂网络安全技术的专业人士提出切实可行的解决方案。

【需求分析】

企业内部计算机主机病毒很严重，首先要了解该企业的网络系统主要存在一些什么样的病毒。这需要选用一些杀毒工具进行检测，可以用不同的杀毒软件进行比较测试。当然，作为一个只对网络组网有基本概念的初学者，需要加强网络安全问题方面的知识，对于网络安全软件也要有所了解。这样才能综合考虑企业的安全需求和经济能力，提出可行的病毒处理方案。

网络攻击有很多种，分为内网的攻击和外网的攻击。网络攻击的类型也有很多，如拒绝服务攻击、利用型攻击、信息收集型攻击等，对于不同的网络攻击需要采取不同的防护手段。对于一个计算机网络的初学者，需要学习相关的知识与掌握相关的技能。

流氓软件对网络安全影响也不可小视。虽然现在的很多杀毒软件都具有清除流氓软件的功能，而需要选择什么样的杀毒软件，需多认真考虑。

二、相关知识

（一）计算机病毒

1. 什么是计算机病毒

计算机病毒实际上就是一段附着在其他程序或文件上的可以执行的计算机程序，它就像生物病毒一样可自我繁殖，具“传染”能力，可透过存储媒体或者网络快速地蔓延，而且常常难以根除。不同计算机病毒的危害性是不一样的，轻者可能因占用资源导致系统运行速度的减慢，影响网络的可用性，严重时会破坏计算机系统文件，损坏重要的数据信息，使计算机系统出现故障或导致系统瘫痪。计算机病毒的重要特点是它的潜伏性，一般情况下对主机系统的影响不大，只有满足某种条件或时机成熟时才会对网络系统造成危害。

2. 计算机病毒的类型

依据其属性，计算机病毒可以分为不同的类型。

（1）按病毒存在的媒体分类

计算机病毒按病毒存在的媒体可划分为网络病毒、文件病毒、引导型病毒。网络病毒通过网络传播，感染主机的可执行文件。文件病毒感染主机中的文件（如 COM、EXE、DLL、BAT、SCR 等），每次执行受感染的文件时病毒便会发作，会将自己复制到其他可执行文件。引导型病毒一般只感染启动扇区（Boot）和硬盘的系统引导扇区（MBR），一般隐藏在磁盘内，当计算机启动时驻留在内存内，通过控制 DOS 中断，进行病毒传播和破坏活动。混合型病毒是上面 3 种情况的复合体，也称复合型病毒。复合型病毒具有引导区病毒和文件型病毒的双重特点。如多型病毒就可以感染文件和引导扇区两种目标，这样的病毒通常有比较复杂的算法，使用非常规的入侵手段。

（2）按病毒传染的方式分类

根据病毒传染的方法可分为驻留型传染病毒和非驻留型传染病毒。驻留型传染病毒感染了计算机

后，其自身只要计算机运行就部分驻留在内存（RAM）内，处于激活状态，只要激发条件满足就对系统进行危害。非驻留型病毒一般不驻留在内存内，即使得到机会激活时也不感染计算机内存，有一些病毒在内存中也留有小部分程序，但也不通过这一部分进行传染，这类病毒都称为非驻留型病毒。

（3）按病毒破坏的能力分类

根据病毒破坏的能力，计算机病毒又可分为无害型病毒、无危险病毒、危险型病毒和非常危险型病毒。除了传染时减少磁盘的可用空间外，对系统没有其他影响的称为无害型病毒。仅减少内存、显示图像、发出声音的称为无危险型病毒。造成计算机系统严重错误的病毒称为危险型病毒。删除程序、破坏数据、清除系统内存和操作系统重要信息的病毒称为非常危险型病毒。

另外，有些病毒对系统造成的危害，并不是本身存在危险的调用，而是当它们传染时会引起无法预料的灾难性破坏，如破坏文件和扇区。这类病毒也可按它们引起的破坏程度划分。当然病毒是有害还是无害也不是一成不变的，可能在这个环境下是无害的，在另一个环境下可能就是有害的。

（4）按照病毒攻击的操作系统分类

首先是攻击 DOS 系统的病毒。这类病毒出现最早、最多，变种也最多，早期我国出现的计算机病毒基本上都是这类病毒，但是随着 DOS 系统的退出，这类病毒的影响越来越小。

其次是攻击 Windows 系统的病毒。由于 Windows 的图形用户界面（GUI）和多任务操作系统深受广大用户的欢迎，Windows 已经取代了 DOS，从而成为目前病毒攻击的主要对象。发现的首例破坏计算机硬件的 CIH 病毒就是一个 Windows95/98 病毒。

然后是攻击 UNIX 系统的病毒。当前，UNIX 系统应用非常广泛，许多大型的操作系统均采用 UNIX 作为其操作系统，所以 UNIX 病毒的出现，对人类的信息处理是一个严重的威胁。

攻击 OS/2 系统的病毒。目前也发现一些攻击 OS/2 系统的病毒，但毕竟我们使用此类系统比较少，对于一般用户影响有限。

（5）按照病毒的链接方式分类

由于计算机病毒本身必须有一个攻击对象以实现对计算机系统的攻击，计算机病毒所攻击的对象是计算机系统可执行的部分。按照病毒的链接方式又可分为源码型病毒、嵌入型病毒、外壳型病毒和操作系统型病毒。

源码型病毒。该病毒攻击高级语言编写的程序，该病毒在高级语言所编写的程序编译前插入到源程序中，经编译成为合法程序的一部分。

嵌入型病毒。这种病毒是将自身嵌入到现有程序中，把计算机病毒的主体程序与其攻击的对象以插入的方式链接。这种计算机病毒是比较难编写的，一旦侵入程序体后也较难消除。如果同时采用多态性病毒技术、超级病毒技术和隐蔽性病毒技术，查杀这类病毒将是十分困难的。

外壳型病毒。外壳型病毒将其自身包围在主程序的四周，对原来的程序不做修改。这种病毒最为常见，易于编写，也易于发现，一般可通过测试文件的大小发现。

操作系统型病毒。这种病毒按照它自己的意图加入或取代部分操作系统文件，具有很强的破坏力，可导致系统瘫痪。圆点病毒和大麻病毒就是这类典型的病毒。这种病毒在运行时，用自己的逻辑部分取代操作系统的合法程序模块，对操作系统进行破坏。

3. 计算机病毒的特点

（1）易变性

许多病毒是利用最新的 Internet 编程语言或编程技术实现的，具有易修改的特点，容易产生新的变种，比较容易逃避反病毒软件的搜索。如“爱虫”病毒就是用 VBScript 语言编写的，只要

通过 Windows 操作系统下自带的编辑软件修改病毒代码中的一部分，就可轻易地制造病毒变种，躲避反病毒软件的追击。

有些新病毒利用 Java、ActiveX、VBScript 等技术，可以潜伏在 HTML 页面内，在上网浏览时触发。如“Kakworm”病毒就是利用 ActiveX 控件中存在的缺陷传播的，装有 IE 浏览器或 Office 软件的计算机都可能被感染。这个病毒的出现可使不打开就直接删除带毒邮件附件的邮件防病毒方法完全失效。

由于计算机病毒的易变性，再加上网络快速传播，病毒的防护难度超乎想象。

（2）人性化

现代病毒常常针对人们的好奇心与贪婪，在不经意间让人中招。Internet 上爆发的一种名为“MSN 性感相册”的蠕虫病毒，就是利用人们的好奇心在网上通过 MSN 传播的。该病毒自动搜索计算机中 MSN 的联系人名单，并随机发送名为“photos.zip”的压缩包。好奇者只要接收打开，计算机就会被感染病毒。

（3）隐蔽性

现代计算机病毒具有更好的隐藏能力与伪装能力。传播中的病毒会不断地改变，一般都会有极具诱惑性的主题、附件名。许多病毒会伪装成常用程序，有些病毒代码写入文件内，其长度都不会发生变化，使用户防不胜防。有一个主页病毒 homepage.html.vbs，它并非是一个 HTML 文档，而是一个恶意的 VB 脚本程序，一旦执行后，就会向用户地址簿中的所有电子邮件地址发送带毒的电子邮件副本。又如维罗纳病毒，会将病毒写入邮件正文，而且主题、附件名都极具诱惑性，主题众多，更替频繁，使用户麻痹大意而被感染。matrix 病毒则会自动隐藏、变形，甚至可以阻止受害用户访问反病毒网站和向病毒记录的反病毒地址发送电子邮件，阻止更新、升级后的相应杀毒软件的下载或发布病毒警告消息。有的病毒在本地没有代码，代码存在于远程的机器上，杀毒软件一般都很难发现病毒的踪迹。

（4）多样性

新病毒层出不穷，老病毒仍然充满活力，并呈现多样化的趋势。从普遍发作的计算机病毒分析显示，虽然新病毒不断产生，但较早的病毒发作仍很普遍。现在报道最多的病毒中就有 1996 年就首次发现并到处传播的宏病毒 Laroux。新病毒可通过可执行程序、脚本文件、HTML 网页、QQ、MSN 甚至网络游戏等多种形式传播。事实上，现在病毒的手段较之以前更加多样化，破坏性更强。如震荡波（Sasser）病毒被首次发现，短短一个星期内就感染了全球 1 800 万台计算机，给全球经济造成了数百亿美元的损失。

（5）平民化

由于脚本语言的广泛使用，专用病毒生成工具目前已经在网上广为流行，制造计算机病毒已经变成了非常简单的事情。以前的病毒制造者都是专家，编写病毒主要是为了表现自己高超的技术，而现在病毒的制造更多可能是为了商业目的。据报道，VBS 蠕虫孵化器被人们从 Internet 上下载了 1.5 万次以上，著名“库尔尼科娃”病毒就是下载的 VBS 蠕虫孵化器的产物，正是由于这类工具太容易得到，所以现在新病毒出现的频率超出预期。

（6）可触发性

因某个事件的发生而诱使病毒实施感染或进行攻击的特性称为可触发性。病毒为了隐蔽自己，一般都有一个潜伏期，病毒一般在潜伏期内既不会实施感染也不会进行破坏，只有满足触发条件时病毒才会发动攻击。触发条件就是用来控制病毒感染和破坏动作的频率的控制器，病毒的触发条件，可能是时间、日期、文件类型或某些特定数据等。

4. 典型的计算机病毒

（1）文件型病毒

目前，流行的 Windows 操作系统均采用 PE 文件格式作为可以执行的文件格式，PE 文件格式使用的是一个屏幕地址空间，所有的代码和文件都被合并在一起，组成一个很大的结构。文件的内容被分割为不同的区块，块中包含代码或数据，各个块按照页边界对齐，块没有大小限制，是一个连续的结构。每个块都有它在内存中的一套属性。每个块都有不同的名字，这个名字表示区块的功能。常见区块功能见表 1-1。

表 1-1　　PE 文件区块功能

区 块 名	内　容
.text	包含指令代码的区块
.rdata	包含运行期只读数据的区块
.data	包含初始化数据块的区块
.idata	包含其他外来 DLL 的函数及数据信息，即输入表的区块
.rsre	包含模块的全部资源，如图标、菜单、位图的区块等

典型的 PE 文件型病毒修改 PE 文件，将病毒代码写入 PE 文件之中，更新 PE 头部相关的数据结构，使得修改后的 PE 文件仍然是合法的 PE 文件。然后将 PE 文件的入口指针改为指向病毒的代码入口。在这样的系统中加载 PE 文件后，病毒代码会首先运行，获得控制权，且系统将首先执行病毒的感染与破坏工作，然后才能执行正常的程序代码。

这种病毒感染 PE 的过程是先在 PE 文件中写入一个新的段，然后修改 PE 的段表的大小和属性（包括文件头中文件大小属性值），再将病毒程序写入 PE 文件中各段保留的没有用的空间中。

Labor Day Virus 就是典型的文件型病毒。该病毒只感染和其自身在同一目录下的 PE 文件，当系统时间为 5 月 1 日时，病毒将发作。

（2）宏病毒

Word 宏病毒是病毒制作者利用 Microsoft Word 的开放性，即 Word 中提供的 Word BASIC 编程接口，专门制作的一个或多个具有病毒特点的宏的集合。这种病毒宏的集合可影响计算机使用，并能通过.doc 文档及.dot 模板进行自我复制与传播。如果某个文档中包含了宏病毒，我们称此文档感染了宏病毒；如果在 Word 系统中的模板包含了宏病毒，我们称 Word 系统感染了宏病毒。

宏病毒与一般的计算机病毒不同，它只感染 Microsoft 公司的 Word 文档、.doc 模板与.dot 文件。宏病毒与以往攻击 DOS 和 Windows 文件的病毒不一样，它以 VB 高级语言编写，直接嵌入文件中进行传播，它不感染程序文件，只感染文档文件。虽然 Microsoft Word 所生成的.doc 文件是数据文件，但由于.doc 文件是数据的综合体，它可由 Word 解释执行操作，也可以像 PE 文件一样可运行，因此也可成为病毒的载体。宏病毒就是针对 Microsoft 公司的字处理软件 Word 编写的一种病毒，Microsoft 公司的字处理软件是当前最为流行的编辑软件，可跨越多种系统平台，因此，宏病毒的危害较广。

Word 的文件建立是通过模板来创建的，模板是为了形成最终文档而提供的特殊文档，模板包括以下几个元素：菜单、宏、格式。模板是文本、图形和格式编排的蓝图，对于某一类型的文档来说，文本、图像和格式编排都是类似的。Word 能提供几种常见文档类型的模板，如备忘录、报告和商务信件。我们可以直接使用模板来创建或者修改文档，也可以创建新的模板。通常情况下，Word 会自动将新文档设置为缺省的公用模板（Normal.dot）。模板在建立整个文档中起重要作用。

作为基类，文档继承了模板的属性，包括宏、菜单、格式等。Word 处理文档需要同时进行各种不同的动作，如打开文件、关闭文件、读取数据资料以及储存和打印文件等。每一种动作都对应着特定的宏命令，如存文件对应 File Save，改名存文件对应 File Save AS，打印文件则对应着 File Print 等。Word 打开文件时，它首先要检查是否有 Auto Open 宏存在，假如有这样的宏，Word 才能启动它，除非在此之前系统已经“取消了宏（Disable Auto Macros）”命令，设置成无效宏。当然，如果有 Auto Close 宏存在，系统在关闭一个文件时，会自动执行它。

Mothers Day Virus 就是一种宏病毒。它只感染 Word 文档和 Normal.dot 文档。被感染的 Word 打开或者关闭时会首先弹出一个对话框。Labor Day Virus 使用 Document_Open 宏感染 Normal.dot 文档，使用 AutoClose 自动感染其他文档。

Mothers Day Virus 病毒的执行流程如下。

① 判断当前的.doc 文档和 Normal.dot 是否感染病毒。

② 如果 Normal.dot 未感染，清除 Normal.dot，复制病毒到 Normal.dot，将宏重命名为 AutoClose。

③ 如果当前的文档被感染，清空当前的宏命令，将病毒复制到当前文档，将宏重命名为 Document_Open。

④ 禁用 Word 的宏编辑功能。

⑤ 添加自动保存功能。病毒发作执行操作。

⑥ 返回到程序正常路径执行。

虽然不是所有包含宏的文档都包含了宏病毒，但当有下列情况之一时，您可以百分之百地断定您的 Office 文档或 Office 系统中有宏病毒。

在打开“宏病毒防护功能”的情况下，当打开一个自己写的文档时，系统弹出了警告框。而如果没有使用宏或不知道宏到底怎么用，可以肯定文档感染了宏病毒。

在打开“宏病毒防护功能”的情况下，Office 文档中一系列的文件都给出了宏警告。由于一般情况下很少使用到宏，所以当看到成串的文档有宏警告时，可以肯定这些文档有宏病毒。

如果启用了软件中关于宏病毒防护选择项，在下次开机时不能保存，则可以肯定系统一定已经感染了宏病毒。

实际上，Word 对宏病毒具有防护功能，该功能可在“工具/选项/常规”中进行设定。但有些宏病毒为了对付 Office 中提供的宏警告功能，它会在感染系统后，在您每次退出 Office 时自动屏蔽掉宏病毒防护功能。因此一旦发现机器中设置的宏病毒防护功能无法在下次启动时保持仍然有效，则系统一定已经感染了宏病毒，即本系统一系列的 Word 模板、特别是 normal.dot 已经被病毒感染。

鉴于绝大多数人不需要或不会使用“宏”这个功能，可以得出一个重要的结论：如果 Office 打开某个文档时，系统给出宏病毒警告，则应对这个文档保持高度警惕，因为它被感染的概率极大。请大家注意，简单地删除被宏病毒感染的文档并不能清除 Office 系统中的宏病毒。

（3）蠕虫病毒

蠕虫是一种能传播和拷贝其自身或某部分到其他计算机系统中，且能保住其原有功能，不需要宿主的病毒程序。目前流行的主要有两种类型的蠕虫，即主机蠕虫与网络蠕虫。主机蠕虫只存在它运行的计算机中，它可透过网络将自身拷贝到其他的计算机中，但主机蠕虫在将其自身拷贝到其他主机后，就会终止它自身的运行。实际上如果在任意时刻，只有一个蠕虫运行，这种蠕虫就是主机蠕虫。而网络蠕虫则没有主机蠕虫的限制，它的每个拷贝都可以运行，因此，网络蠕虫危害性比较大。蠕虫病毒一般是通过 1434 端口漏洞传播的。

前几年危害很大的“尼姆亚”、“熊猫烧香”病毒就是蠕虫病毒。这种病毒通常利用 Microsoft 视窗操作系统的漏洞，计算机只要感染了这类病毒，会不断地自动拨号上网，并利用文件中的地址信息或网络共享进行传播，破坏用户的数据。

蠕虫病毒和一般的病毒有很大的区别。一般认为蠕虫病毒是一种通过网络传播的恶性病毒，它具有病毒的一切共性，如传播性、隐蔽性、破坏性等，但它也具有自己的一些特征，如不利用文件寄生，对网络拒绝服务，引入了黑客技术等。在造成的破坏性上，蠕虫病毒也不是普通病毒可比的，网络的发展使得蠕虫病毒可以在短短的时间内迅速蔓延，造成大面积的网络瘫痪。

根据蠕虫病毒的活动范围可分为两类蠕虫病毒：一类是面向企业用户和局域网。这种蠕虫病毒利用系统漏洞，主动进行攻击，可以导致整个 Internet 瘫痪。这类蠕虫病毒以“红色代码”、“尼姆达”以及“SQL 蠕虫王”为代表；另一类是针对个人用户的蠕虫病毒。一般通过电子邮件、恶意网页迅速传播，如“爱虫”病毒、“求职信”病毒等就是这类蠕虫病毒。这两类蠕虫病毒中，第一类具有很强的攻击性，而且爆发有一定的突然性，但相对来说，查杀这种病毒并不是很难。第二类蠕虫病毒的传播方式比较复杂，少数利用了 Microsoft 的应用程序的漏洞，更多的是利用社会工程学对用户进行诱骗，这样的蠕虫病毒造成的损失是非常大的。如求职信这类病毒是很难根除的，在 2001 年就已经被各大杀毒厂商发现，但直到多年后依然排在病毒危害榜首就是证明。

蠕虫一般不利用 PE 格式嵌入病毒的方法传播，而是靠自身复制在 Internet 中进行传播。也不像病毒的传染那样主要是针对计算机内的文件系统，其传染的对象是 Internet 内的所有计算机，包括：网络内计算机的共享文件夹、电子邮件、网页、存在着漏洞的服务器等。目前的高速网络可使蠕虫病毒在几个小时内传遍全球。

目前，危害比较大的蠕虫病毒主要通过 3 种途径传播：系统漏洞、聊天软件和电子邮件。其中利用系统漏洞传播的病毒往往传播速度极快，如利用 Microsoft 04-011 漏洞的“震荡波”病毒，3 天之内就可感染全球至少 50 万台计算机。通过电子邮件传播，也是近年来病毒作者青睐的方式之一，像“恶鹰”、“网络天空”等都是危害巨大的邮件蠕虫病毒。这样的病毒往往会繁殖出大量的变种，用户中毒后往往会导致数据丢失、个人信息失窃、系统运行变慢等情况的发生。

蠕虫病毒的一般防治最好的办法是打好相应的系统补丁，使用具有实时监控功能的杀毒软件，启用“邮件发送监控”和“邮件接收监控”功能，在使用瑞星杀毒软件单机版、瑞星杀毒软件下载版的时候，一定要注意打开它们的 8 大监控功能，这样就可较好地防范蠕虫病毒的攻击。

5. 计算机病毒的防护

计算机病毒防护首先是要建立计算机网络病毒防护体系，包括单机防护、网络病毒防护、网关病毒防护、病毒追查防护等，如图 1-1 所示。单机病毒防御是传统防御模式，是固守网络终端的最后防线。单机防御对于广大家庭用户、小型网络用户而言，无论是在效果、管理、实用价值上都是有意义的，它可用来阻止来自 U 盘、光盘、共享文件、互联网病毒的入侵，实现重要数据备份的功能。

根据网络操作系统使用情况，局域网服务器必须配备相应防病毒软件，当然，基于 UNIX/Linux、Windows 2000/2003/2007 以及 DOS 等平台需要配置对应的操作系统的安全防范软件，全方位的防卫病毒的入侵。

在规模局域网内配备网络防病毒管理平台是必要的，如在网管中心配备病毒集中监控中心，集中管理整个网络的病毒疫情，在各分支网络也配备监控中心，提供整体防病毒策略配置、病毒集中监控、灾难恢复等管理功能，在工作站、服务器较多的网络可配备软件自动分发中心，可提高网管的工作效率。

在局域网病毒防御的基础上可以构建广域网中心病毒报警监测系统，监控本地、远程异地局

域网病毒防御情况，统计分析整个集团网络的病毒爆发种类、发生频度、发生源等信息。一般广域网病毒防御策略常采用三级管理模式：单机终端杀毒—局域网集中监控—广域网病毒中心管理。

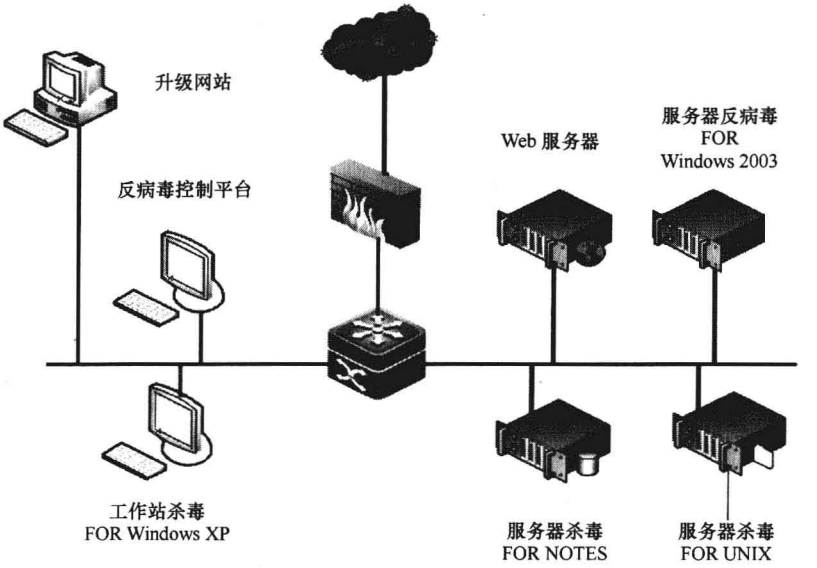


图 1-1　安全软件的布局图

网络中设置邮件网关病毒防御是必要的内容。政府机关、军队、金融、科研院校等机构的办公自动化（OA）系统中的邮件服务器是必不可少的，它既是内部网络用户邮件的中转站，也是病毒邮件、垃圾邮件进出的门户。如果在网络入口处将病毒邮件、垃圾邮件截杀掉，则可确保内部网络用户收到安全无病毒的邮件。邮件网关防病毒系统一般放置在邮件网关入口处，接收来自外部的邮件。对病毒、不良邮件等进行过滤，可保护内网用户的电子邮件安全。

在网络出口处可设置有效的病毒过滤系统，如安装带有防病毒网关的防火墙。防火墙可将接收的数据提交给网关杀毒系统检查，如有病毒入侵，网关防病毒系统可通知防火墙立刻阻断带有病毒的数据包流入内网，封锁攻击的 IP。因为采用的是同步查毒，几乎不影响网络带宽，此种过滤方式也可用于过滤多种数据库和邮件中的病毒。

思考与练习

1. 什么是病毒？简述计算机病毒的特征及危害。
2. 简述计算机病毒的分类及各自特点。
3. 目前常用的有哪些杀毒软件？杀毒软件的选购指标有哪些？
4. 怎样预防和消除计算机网络病毒？
5. 简述检测计算机病毒的常用方法。

（二）特洛伊木马

1. 特洛伊木马

“特洛伊木马”（Trojan horse）简称“木马”，据说这个名称源于希腊神话《木马屠城记》。古希腊有大军围攻特洛伊城，久攻不下。于是有人献计制造一只高二丈的大木马，假装成作战神马，

让士兵藏匿于巨大的木马中，大部队假装撤退而将木马弃于特洛伊城下。城中得知解围的消息后，遂将“木马”作为战利品拖入城内，全城饮酒狂欢。到午夜时分，全城军民尽入梦乡，匿于木马中的将士开秘门沿绳而下，打开城门并四处纵火，城外伏兵涌入，部队里应外合，焚屠特洛伊城。后人称这只大木马为“特洛伊木马”。如今黑客借用其名，编出具有类似功能的软件，也称为特洛伊木马，该软件取“一经潜入，后患无穷”之意。

特洛伊木马常伪装成某种有用的或有趣的程序，如屏保程序、算命程序、游戏程序等，但实际上却行破坏数据、骗取使用者密码的勾当。一般特洛伊木马不具有自我复制功能，也不会感染别的计算机。

完整的木马程序一般由两部分组成：一个是服务端程序，一个是控制端程序。“中了木马”是指某台计算机被安装了木马的服务端程序。若你的计算机中了木马，则拥有控制端程序的人就可以通过网络操控你的计算机，你计算机上的各种文件、程序、使用的账号、密码等都无安全可言。

特洛伊木马的明显特征是隐蔽性与非授权性。所谓隐蔽性是指木马的设计者为了防止木马被发现，会采用多种隐藏木马手段，这样即使受害者发现自己中了木马，也难确定其具体位置；所谓非授权性是指一旦控制端与服务端连接后，控制端将取得服务端的操作权限，可以随意修改文件，修改注册表，控制鼠标、键盘，甚至窃取信息等。

特洛伊木马与病毒的最大的区别是特洛伊木马不传染，它并不像病毒自我复制，也不“刻意”去感染其他文件，它只通过伪装，吸引用户下载执行。特洛伊木马中常包含有能够在触发时导致数据丢失甚至被窃的恶意代码。要使特洛伊木马传播，必须在计算机上有效地启用这些程序，如打开电子邮件附件或者将木马捆绑在软件中放到网络上吸引人下载执行。

现在的木马一般主要以窃取用户信息为主要目的，相对病毒而言，病毒破坏你的信息，而木马窃取你的信息。典型的特洛伊木马有灰鸽子、网银大盗等。特洛伊木马比任何其他恶意代码都危险，要保障网络安全，我们就需要首先熟悉特洛伊木马，包括木马的类型、典型木马的工作原理，并且掌握其检测和预防的方法。

2. 木马的类型与功能

木马的种类很多，限于篇幅不一一列举，这里只介绍几种典型的木马。

（1）远程控制木马

远程控制木马是一种数量最多、危害最大、知名度也最高的木马，攻击者通过这种木马可以完全控制被中木马的计算机，甚至完成一些即使是主机的主人也难进行的操作，其危害之大确实不容小觑。为了要达到远程控制的目的，这类木马往往具有多种木马的功能。使用这类木马，黑客可以任意访问文件，轻松获取机主的信用卡、银行账号之类重要的私人信息。

“冰河木马”就是一个远程控制型的特洛伊木马，该木马用起来非常简单，只需计算机运行服务端程序，黑客就可以访问到这台计算机，能在被种木马的机器上做任何事。

远程控制木马具备的基本功能包括：键盘记录，上传和下载数据文件，注册表操作，系统功能限制等。远程控制型木马常常会在你的计算机上打开一个端口，以便长期控制你的计算机。

（2）密码发送木马

在信息安全日益重要的今天，密码无疑是通向重要信息的一把有用的钥匙，谁掌握了对方的密码，谁就可以轻松地获得对方的信息。密码发送型的木马是专为盗取密码而编写的，该木马一旦被执行，会自动搜索内存、Cache、临时文件夹以及各种敏感的密码文件，一旦搜索到有用的密码，它就会通过免费的电子邮件服务将密码发送到指定的邮箱内，从而达到获取密码的目的。这类木马一般使用 25 号端口发送电子邮件，大多数不会在每次 Windows 启动时启动。这种木马在

找到隐藏的密码后，会在受害者不知道的情况下把它们发送到指定的信箱。如果采用普通密码，被这类木马攻击成功的可能性是非常之大的。由于要获得的密码可能是多种多样的，每台主机密码存放形式也各不相同，所以这类木马程序没有几个是完全相同的。

（3）键盘记录木马

键盘记录木马是非常简单的。它们只做一件事情，就是记录受害者的键盘敲击信息，并从 LOG 文件中发现密码。这种木马一般是随着 Windows 的启动而启动的，有在线和离线记录选项，可以分别记录主机的主人在线和离线状态下敲击键盘的情况。从按键信息中是很容易获得有用东西的，如主机密码和信用卡账号。当然，对于这种类型的木马，邮件发送功能也是必不可少的。

（4）破坏性木马

这种木马唯一的功能就是破坏被感染主机的文件系统，轻者损坏重要数据，重者导致系统崩溃。从其破坏性这一点上来说，它和病毒是很相似的。不过，这种木马的激活是由攻击者控制的，其传播能力比病毒也要逊色不少。

（5）DoS 攻击木马

随着 DoS 攻击越来越广泛地应用，被用作 DoS 攻击的木马也越来越流行。当黑客入侵了一台计算机时，常常会给它种上 DoS 攻击木马，使这台主机成为黑客 DoS 攻击的得力助手。黑客控制的“肉鸡”（安装了 DoS 木马的主机）数量越多，发动 DoS 攻击威力就越强。DoS 木马的危害不是体现在被感染计算机上的，而是体现在被攻击的计算机上。

还有一种类似 DoS 的木马叫做邮件炸弹木马。一旦机器感染上了这种木马，这台机器就会随机生成各种各样主题的信件，对特定的邮箱不停地发送邮件，一直到对方不能再接受邮件为止。

（6）代理木马

黑客在入侵时，为掩盖自己的足迹，会给被控制的“肉鸡”种上代理木马，让其变成发动攻击的跳板。通过代理木马，攻击者可以在匿名的情况下使用 Telnet、ICQ、IRC 等程序进行远程控制，而且隐蔽自己的踪迹。

（7）FTP 木马

这种木马是最简单和古老的木马，它的唯一功能就是打开 21 端口，实现与被攻击主机的连接。现在新 FTP 木马还加上了密码功能，这样，只有攻击者本人才知道正确的密码，从而进入对方的计算机。

（8）程序杀手木马

木马的功能虽然形形色色，不过到了对方机器上要发挥自己的作用，首先要过防木马软件这一关。常见的防木马软件有 Norton Anti-Virus、卡巴斯基与 360 安全卫士等。程序杀手木马的功能就是关闭对方机器上运行的这类安全程序，让木马能够发挥作用。在网上你能找到对付现在流行的绝大多数的防病毒软件的这类木马软件的名称以及使用它们的方法。

（9）反弹端口型木马

反弹端口型木马程序是木马开发者在分析了防火墙的弱点之后编制的。防火墙对于外网接入的链接往往有非常严格的过滤，但是对于内网对外的链接却常常疏于防范。反弹端口型木马的思路是让木马的服务器端设置为主动端口，客户端设置为被动端口。木马通过定时监测控制端的存在，发现控制端上线立即开放端口与之连接。为了隐蔽起见，一般会将控制端的被动端口设为 80，这样，即使用户使用端口扫描软件检查自己的端口，发现的也是类似 TCP User IP：1026 Controller IP：80 ESTAB LISHED 的情况，稍微疏忽一点，就会以为是自己在浏览网页。

当然，这种木马的服务器端与客户端的端口不是简单的连接，实际上，这种反弹端口的木马

常常会透过有固定 IP 的第三方存储设备来进行信息的传递。如事先设置一个个人主页空间，在其中放置一个文本文件，木马每分钟去 GET 一次这个文件，如果文件内容为空，就什么都不做，如果有内容，就按照文本文件中的数据计算出控制端的 IP 和端口，反弹一个 TCP 链接回去，这样，每次控制者上线只需要 FTP 一个 INI 文件，就可以告诉木马自己的位置。为了保险起见这个 IP 地址甚至可以经过一定的加密，除了服务端和控制端，其他的人就算拿到了也没有任何意义。当然，对于一些能够分析报文、过滤 TCP/UDP 的防火墙，反弹端口型木马同样有办法对付。如果控制端使用 80 端口的木马完全使用真的 HTTP 协议，将传送的数据包含在 HTTP 的报文中，那么一般的防火墙是不可能有能力分辨通过 HTTP 协议传送的究竟是网页，还是控制命令和数据的。

3. 木马的安装

一般来说，木马程序包括客户端与服务端两部分。其中，客户端运行在入侵者的操作系统上，是入侵者控制目标主机的平台；服务端则运行在目标主机上，是被控制的平台，一般发送给目标主机的就是服务端程序。

木马主要依靠邮件、下载等途径进行传播。木马常常通过一定的提示诱使目标主机使用者运行木马的服务端程序，完成木马的种植。例如，入侵者伪装成目标主机用户的朋友，发送一张捆绑有木马的电子贺卡，一旦目标主机用户打开贺卡后，屏幕上会出现贺卡的画面，木马服务端程序也会被安装，然后就在后台运行了。由于一般的木马都非常小，大部分只有几 KB 到几十 KB 之间，因此试图从文件大小上发现文件中是否捆绑有木马是很困难的。

木马也可以通过 Script、ActiveX、Asp 或 CGI 等交互脚本进行传播。比如，IE 浏览器在执行 Script 脚本时常常存在一些漏洞，入侵者可以利用这些漏洞进行木马的传播与种植。

只要目标主机执行了服务端程序之后，入侵者便可通过客户端程序与目标主机的服务端建立连接，进而控制目标主机。对于通信协议的选择，绝大多数木马使用的是 TCP 协议，当然，也有使用 UDP 协议的木马。

通常安装的服务器端的木马程序在客户主机上会尽可能地隐蔽自己的行踪，它会不断监听某个特定的端口，等待客户端的连接。当然，服务端程序为了在每次计算机重新启动后能够正常运行，会修改注册表实现其自启动功能。

4. 木马的隐藏与启动

（1）在应用程序中隐藏

木马的隐藏是指服务端的隐藏。最简单的隐藏方法是将木马嵌入应用程序之中，通过目标用户运行应用程序而启动木马程序。由于这类木马与应用程序捆绑在一起，用户不能轻易地删除，即使木马被删除了，只要运行了嵌入木马的应用程序，木马又会被安装上去。木马常常绑定到系统文件上，这样只要 Windows 启动均会启动木马程序。

（2）在配置文件中隐藏

木马也常常会隐藏在系统配置文件如 Autoexec.bat 和 Config.sys 中。采用这种隐藏方法的好处是可以利用配置文件的特殊作用，木马很容易在被攻击者的计算机中启动运行，从而控制计算机。不过，这种方式不是很隐蔽，容易被发现。

（3）在 Win.ini 文件中隐藏

木马要想达到控制或者监视计算机的目的，必须要运行，而且还要尽可能地避免被人发现，于是潜伏在 Win.ini 中是一个好方法。只要打开 Win.ini，就可以发现[Windows]字段中有启动命令“load=”和“run=”，在一般情况下“=”后面应该是空白的，如果后面跟着程序，很可能就是木

马，木马会随着 Win.ini 的启动命令的执行而启动。

（4）伪装在普通文件中

这个方法现在很流行，对于不熟练 Windows 的操作者，很容易上当。具体方法是把可执行文件伪装成图片或文本，如把文件名改为*.jpg.exe，由于 Windows 操作系统默认设置是“不显示已知的文件后缀名”，文件将会显示为*.jpg，不注意的人一点这个图标就会启动木马。

（5）嵌入到注册表中

上面的隐藏方法是比较容易发现的，而躲在注册表中是一个好方法。由于注册表比较复杂，木马常常喜欢藏在里面。观察一下：HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/Current Version 下所有以“run”开头的键值；以及 HKEY_CURRENT_USER/Software/Microsoft/Windows/ CurrentVersion 下所有以“run”开头的键值；HKEY-USERS/Default/Software/ Microsoft/Windows/CurrentVersion 下所有以“run”开头的键值。这些都隐藏木马的好地方。

（6）在 System.ini 中藏身

Windows 安装目录下的 System.ini 也是木马喜欢隐蔽的地方。打开这个文件可以发现在该文件的[boot]字段中，可能有如 shell=Explorer.exe file.exe 这样的内容，如果有这样的内容，那么这台计算机就不幸中木马了，这里的 file.exe 就是木马的服务端程序。另外，在 System.ini 中的[386Enh]字段中，要注意检查段内的“driver=路径程序名”，这里也是隐藏木马的地方。在 System.ini 中的[mic]、[drivers]、[drivers32]3 个字段是加载驱动程序的地方，注意这些地方也是可以加木马程序的。

（7）隐形于启动组中

有些木马并不在乎自己的行踪，它更注意能否自动加载到系统中，因为一旦木马加载到系统中，清除是非常困难的。因此，启动组也是木马可以藏身的好地方，因为这里程序可以很方便地加载运行。启动组对应的文件夹是：C:Windows start menu programs start up。在注册表中的位置是：HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/Shell Folders Startup=“C:Windows start menu programs start up”。因此，要注意经常检查启动组。

（8）隐蔽在 Winstart.bat 中

按照上面的逻辑，凡是木马能自动加载的地方，木马都喜欢。Winstart.bat 也是一个能自动被 Windows 加载运行的文件，多数情况下由应用程序及 Windows 自动生成，在执行了 Win.com 时，多数驱动程序加载之后开始执行。由于 Autoexec.bat 的功能可以由 Winstart.bat 代替完成，因此种入的木马完全可以像在 Autoexec.bat 中那样被加载运行，因此要保证计算机系统安全，这些地方也是要注意的。

（9）捆绑在启动文件中

应用程序的启动配置文件，控制端利用这些文件能启动程序的特点，将制作好的带有木马启动命令的同名文件上传到服务端覆盖这个启动配置文件，这样就可以达到启动木马的目的了。

（10）设置在超级连接中

木马的主人在网页上放置恶意代码，引诱用户点击，用户点击则安装和启动木马成功，这是隐藏和启动木马最常见的过程。因此不要随便点击网页上的链接。

当然，木马的隐藏和启动的方法还有很多，如通过任务栏图标隐藏启动木马，通过修改虚拟设备驱动程序（VXD）或修改动态链接库（DLL）启动加载木马，修改文件的关联隐藏启动木马等。

5. 木马的欺骗

木马是一个软件，它不会“长腿”自己跑到用户的机器上，正像《木马屠城记》剧情中描述的一样，木马往往是被攻击者将其带进自己的计算机中的，因此，欺骗是木马必须具备的一个重