飞思教育
FECIT-Education
www.fecit.com.cn

网络安全DIM

居安思危
——电脑防黑防毒急救

DO IT MYSELF

飞思科技产品研发中心　编著

防黑防毒完全攻略

- 揭开黑客神秘面纱
- 计算机软硬件系统安全
- 彻底查杀计算机病毒
- 重要数据的备份与恢复
- 全面维护网络安全
- 密码的攻击与防护
- 网络安全过滤及分级检查

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络安全

居安思危——电脑防黑防毒急救

飞思科技产品研发中心　编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

电脑的防黑、防毒问题是现在广大电脑爱好者普遍关心的问题，黑客与红客间的战争永不停息，而计算机病毒的快速繁衍又使我们措手不及。本书从防范的角度出发，全面详尽地介绍了黑客攻击和病毒入侵的种种防范技术，书中对每种防范方法都附有详细的安装步骤和操作方法。

本书试图从宏观到微观向读者介绍电脑防黑、防毒的原理及方法，主要包括计算机网络基础、黑客及其表现、计算机硬件系统安全、软件系统的安全、病毒的查杀、数据备份与恢复、网络安全、密码的攻击与防护、个人网络防火墙，以及网站安全过滤及分级审查等方面的内容。

本书适合于计算机网络管理员、系统维护人员、网络用户、计算机爱好者，以及大专院校有关专业的师生阅读参考

图书在版编目（CIP）数据

居安思危——电脑防黑防毒急救 / 飞思科技产品研发中心编著. —北京：电子工业出版社，2002.10
（网络安全 DIM）
ISBN 7-5053-8026-5

Ⅰ.居… Ⅱ.飞… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2002）第 073009 号

责任编辑：王树伟 王 蒙
印 刷：北京天宇星印刷厂
出版发行：电子工业出版社 http://www.phei.com.cn
北京海淀区万寿路 173 信箱 邮编：100036
经 销：各地新华书店
开 本：787×1092 1/16 印张：24.75 字数：633.6 千字
版 次：2002 年 10 月第 1 版 2002 年 10 月第 1 次印刷
印 数：5 000 册 定价：33.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077

前　言

关于丛书

几年来，电子工业出版社计算机研发部暨飞思科技产品研发中心，依靠在科技和教育行业的实践积累，以完善的图书产品结构，强大的技术力量，率先提出了“IT 教育全面解决方案”。依照此方案规划，飞思向广大读者、经销商和培训机构提供“标准培训　权威认证”教材、专业计算机科学技术类图书、东南亚精品图书、高品质的设计类产品、普及类图书、基于网络平台的多媒体教育课件，以及专业的市场动态分析和专业技术支持。

“Do It Myself”英文缩写为 DIM，是飞思人率先提出的概念：无论做什么事情，最重要的是自己动手亲身去体验，过程与结果同样值得珍惜。所以在普及类图书产品线的建设方面，继 2001 年成功推出“软件应用 DIM”、“电脑家装 DIM”（图书封面如下两图所示）系列之后，飞思人经过长期的市场调研与选题规划，将不断完善 DIM 的概念，近期奉献给读者的是“网络组建 DIM”、“网络安全 DIM”系列图书。

DIM 系列丛书的特色在于：

1．内容为王，面向应用，作者队伍是长期从事工作一线的实际操作人员，书中的每个例子都是他们宝贵经验的倾情奉献，使读者在操作中少走弯路。

2．高品质、低价位，面向大众读者。其中“电脑家装 DIM”系列全彩印刷仅定价 19 元。

3．系列图书得到读者的广泛认可。以“电脑家装 DIM”内容为蓝本的“飞思 MM 教.电脑”系列情景剧正在中国教育电视台一套“电脑之夜”栏目热播。以下两图为片中的精彩剧照。

关于本书

随着电脑应用的日益普及，网络的飞速发展，网络的安全问题开始受到大家的更多关注。一些不道德的黑客行为严重影响了我们的网络系统和网络生活，威胁着计算机网络系统的安全。事实上，越来越多的电脑用户已经开始意识到防范各种恶意攻击、保护个人数据和操作系统安全的重要性，但是却由于各种条件的限制，无法为自己的电脑提供足够的保护。因此，对黑客入侵的防范逐渐成为了计算机爱好者需要掌握的一门技术。

除了黑客的攻击，另外一个威胁计算机安全的就是病毒了。自从第一个病毒出世以来，究竟世界上有多少种病毒，恐怕无人知道。而且，几乎每天都有新的病毒出现，其数量在不断地增加。据国外统计，计算机病毒以 10 种/周的速度递增；另据我国公安部统计，国内以 4～6 种/月的速度递增。预防病毒、保护计算机系统和数据不被病毒侵害，是每一个计算机用户必须具备的知识。

本书从防范的角度出发，全面详尽地介绍了黑客攻击和病毒入侵的种种防范技术，可以说从宏观到微观讲述了电脑防黑、防毒的原理和方法，并结合了大量的应用工具进行讲解，对每种防范方法都附有详细的安装步骤和操作方法，具有很强的实战性。

本书试图详尽地介绍如何防范恶意破坏个人电脑数据和危害信息安全的行为，全书共分 10 章，分别介绍了计算机网络基础、黑客及其表现、计算机硬件系统安全、软件系统的安全、病毒的查杀、数据备份与恢复、网络安全、密码的攻击与防护、个人网络防火墙，以及网站安全过滤及分级审查等内容。

本书适合于那些电脑中高级用户，在阅读本书之前，读者最好要具备一定的电脑使用基础，对网络基础相关知识有一定的了解。

本书由飞思科技产品研发中心策划并组织编写，博雅工作室的陆炜、陈捷、王杜凛主笔，参加编写的还有李辉、任永正、邓建民、胡光耀、陈晓蓉、臧炜、胡松龄、郝捷等，全书由郝艳芬统稿。编者虽然未敢稍有疏虞，但纰缪和不尽如人意之处仍在所难免，诚请本书的读者提出意见或建议。

虽然飞思人不能在工作中与您同行，但我们可以用我们的智慧、汗水和心血凝结而成的书籍与您相伴，尽量帮您在工作中解决一些我们力所能及的技术问题。

我们的目标是把每一本书做精做细，以回报读者对我们的信任，衷心希望我们的读者为我们提供有价值的意见和建议，共筑飞思辉煌的明天。我们的联系方式如下：

电话：（010）68134545　　68131648

E-mail：support@fecit.com.cn

飞思在线：http://www.fecit.com.cn　　http://www.fecit.net

答疑网址：http://www.fecit.com.cn/question.htm

通用网址：计算机图书、FECIT、飞思教育、飞思科技、飞思在线

电子工业出版社计算机研发部

飞思科技产品研发中心

目　录

第 1 章　计算机网络基础

网络（Network）是将不同地理位置的多个计算机系统相互连接，通过一定的通信设备和通信线路，在网络应用软件的支持下实现数据通信和资源共享的计算机系统。正如交通网络方便了空间的沟通、通信网络实现了实时的交流一样，计算机的互联解决的核心问题是资源的共享。在计算机网络中，经过一定授权的用户可以在任何时候、任何地点自由地使用网络中的各种文字、图表、声音、图像以及影像等等数据资源，也可以使用相关的大型计算机、网络打印机等设备，甚至是其他计算机的组件（如光驱、硬盘等）。而最有意义的是，在极大的空间内，相当数量的计算机通过互联，相关的计算机用户即时地发布信息、搜集信息，使得信息的传播和获取达到了交互、实时、海量、实用等激动人心的效果，这将直接地改变人类生活的内容和方式，为千家万户带来一个崭新的生活空间。Internet（国际互联网）的普及，正是展示了这一美好的前景。

1.1　计算机网络的功能与应用

一个计算机系统联入网络以后，具有共享资源、提高可靠性、分担负荷和实现实时管理等优点。从上世纪 80 年代末开始，计算机网络技术进入新的发展阶段，它以光纤通信应用于计算机网络、多媒体技术、综合业务数据网络（ISDN）、人工智能网络的出现和发展为主要标志。上世纪 90 年代至本世纪初是计算机网络高速发展的时期，计算机网络的应用正向更高层次发展，尤其是 Internet 的建立，推动了计算机网络的飞速发展。据预测，今后计算机网络具有以下几个特点：

- 开放式的网络体系结构。使不同软硬件环境、不同网络协议的网可以互联，真正达到资源共享、数据通信和分布处理的目标。
- 向高性能发展。追求高速、高可靠和高安全性，采用多媒体技术，提供文本、声音、图像等综合性服务。
- 计算机网络的智能化。多方面提高网络的性能和综合的多功能服务，并更加合理地进行网络各种业务的管理，真正以分布和开放的形式向用户提供服务。

社会及科学技术的发展，为计算机网络的发展创造了更加有利的条件。计算机网络与通信网络的结合，可以使众多的个人计算机不仅能够同时处理文字、数据、图像、声音等信息，而且还可以使这些信息四通八达，及时地与全国乃至全世界的信息进行交换。一般来说，计算机网络的主要功能就是资源共享和信息交流。

1. 资源共享

计算机网络是以共享资源（硬件、软件和数据等）为目的而连接起来的，在协议控制下由一台或多台计算机、若干台终端设备、数据传输设备，以及便于终端和计算机之间或者若干台计算机之间数据流动的通信控制处理机等组成的系统之集合，这些计算机系统应

当具有独立自治的能力。

根据上述的描述，计算机网络的最主要功能是向用户提供资源的共享，而用户本身无需考虑自己及所用资源在网络中的位置。资源是指在有限时间内可为用户提供各种服务的软件硬件设施。资源共享包括硬件共享、软件共享和数据共享。

- 硬件共享：用户可以使用网络中任意一台计算机所附接的硬件设备，包括利用其他计算机的中央处理器来分担用户的处理任务。
- 软件共享：用户可以使用远地主机的软件（系统软件和用户软件），既可以将相应软件调入本地计算机执行，也可以将数据送至对方主机，执行软件，并返回结果。
- 数据共享：用户可以使用其他主机和用户的数据，例如数据库查询的情报检索等。

资源共享必须要有相应软件的支持。用户对于网络资源的需求具有突发性的特征，亦即难以预测用户何时需要何种网络资源，从而为网络资源的分配和共享带来一定的难度。如何合理地进行网络资源的分配和共享是用户和技术人员共同关心的问题，不少专家正在为此而努力。

2. 信息交流

网络中的机器通信十分方便，如利用 E-mail 进行通信，利用 FTP 传输文件，甚至可以利用某种应用软件（如 IP Phone）在 Internet 上打电话。其中，Internet 上的环球信息网（WWW，World Wide Web）服务就是一个最典型也是最成功的例子。又例如，综合业务数据网络（ISDN）就是将电话、传真机、电视机和复印机等办公设备纳入计算机网络中，提供了数字、语音、图形图像等多种信息的传输，给 Internet 用户带来了极大的方便。

计算机网络目前正处于迅速发展的阶段，网络技术不断更新，计算机网络的应用范围进一步扩大。计算机互联网络主要应用在以下两个大的方面：

（1）服务于企业

其核心问题也是资源共享（Resource Sharing），其主要目的是让网络上的用户都能使用网络中的程序、设备，尤其是数据。第二个目的是依靠可替代的资源来提供高可靠性，例如，所有的文件可以在两台或三台计算机上留有副本，如果其中之一不能使用（由于硬件故障），还可以使用其他的副本。另外，多处理机的出现，意味着如果其中一台机器出了故障，其余的处理机仍然可以分担它的任务，尽管性能可能有所下降。第三个目的是节约经费。许多系统设计者用多台功能强大的个人计算机来组建系统，每个用户使用一台个人计算机，数据则存放在一台或多台共享的文件服务器（File Server）里。在这一模式中，用户被称做客户（Client），而整个结构被称做客户/服务器模型（Client/Server Model）。在客户/服务器模型中，通信的方式通常是客户向服务器发送请求信息，指示需要完成的工作，服务器完成工作后送回应答。一般情况下，是多个客户使用少量服务器。网络的第四个目的是可扩充性，即当工作负荷加大时，只要增加更多的处理器，就能逐步改善系统的性能。在客户/服务器模型中，新的客户和服务器可以按需要随时加入。

建立网络的另一个目的与技术没有太大的关系。计算机网络可以为分布在各地的雇员提供强大的通信手段。这种速度上的提高使得广泛分布的人与人之间的合作很容易进行。从长远的观点来看，利用网络来增强人际沟通可能比它的技术目的（如增加可靠性）更重要。

（2）服务于公众

- 访问远程信息。访问远程信息有多种形式，一个常见的例子是访问财务部门。
- 个人间通信，基本上它是替代 19 世纪发明的电话的手段。电子邮件已在上百万人当中使用，并且将很快包含声音、图像，与文本一起传送。实时电子邮件使远程用户可以无延迟地通信，可以互相看到或听到对方。这种技术可以用来召开虚拟会议，即视频会议（Video Conference）。
- 交互式娱乐。这是一个巨大并且还在继续增长的工业，这里最吸引人的应用是视频点播（Video on Demand）和实时模拟游戏。

简单地说，综合信息、通信和娱乐的能力将造成一个新兴的、基于计算机网络的巨大工业。

1.2　Internet 的发展过程

计算机网络是计算机技术与通信技术发展的结晶，是在用户需求的促进下发展起来的。1946 年，第一台计算机问世，其后几年，计算机只能支持单用户使用，计算机的所有资源为单个用户所占用，直至分时多用户操作系统出现。分时多用户操作系统支持多个用户利用多台终端共享单台计算机的资源。出于应用的需求，人们开始利用通信线路将远程终端连至主机，不受地域限制地使用计算机的资源。为了支持这种应用的要求，出现了一系列的通信设备，例如：调制解调器（Modem）将计算机处理的数字信号转换成模拟信号，以适应模拟通信线路传输的要求；集中器采用多路复用技术将多个终端通过一条或几条通信线路连至主机，以提高通信线路的利用率；通信控制器将主机的通信独立出来，以保证通信质量和降低主机的通信功耗等。严格地说，这一时期的“终端—通信设备—主机”系统并不是计算机网络，因为终端本身并不具有智能功能，不是一台“独立自治”的设备。

1968 年，美国国防部高级研究计划局（ARPA）与麻省剑桥的 BBN 公司签订协议，进行计算机之间的远程互联研究，研究的成果是出现了著名的 ARPANET。ARPANET 的研建标志了世界上第一个计算机网络的诞生。

然而，真正促进计算机网络应用的还是在 70 年代中期，大规模和超大规模集成电路的应用，使得价廉物美的个人计算机（PC）问世了，也使得一个企业或者部门可以很容易地拥有一台或者多台计算机。由于 PC 机的资源和处理能力有限，用户希望共享资源的要求增加，促进了计算机联网的发展。

计算机网络的发展要求通信技术的支持，计算机网络的需求促进了通信技术的发展。反过来，通信技术的发展又促进了计算机网络技术的发展。

目前，计算机网络仍是一大热门课题，应用需求极为广泛。1993 年，美国政府提出的“信息高速公路”实质上是将计算机网络连至各家各户；我国政府提出的“八金工程”也是以计算机网络为基础，支持各行各业的应用要求。同样，目前一个企业同时拥有多台计算机已不再是不可及的事情，计算机联网以支持企业的应用已成为企业的一般要求。

从技术上讲，人们提出了“网络就是计算机”的概念，计算机网络伴随着计算机已成为家喻户晓的名词。

上世纪 80 年代中期以来，在计算机网络领域最引人注目的事就是在美国 Internet 的飞速发展。Internet 的本来意思就是互联网，有人也将其译为国际互联网，或按音译为因特网。现在 Internet 已成为世界上最大的国际性计算机互联网。到 1983 年，ARPANET 已连上了三百多台计算机，供美国各研究机构和政府部门使用。1984 年 ARPANET 分解成两个网络，一个仍称为 ARPANET，是民用科研网，另一个是军用计算机网络 MILNET。由于这两个网络都是由许多网络互联而成，因此它们都为 Internet。后来 ARPANET 就称为 Internet 的主干网。

美国国家科学基金会（NSF）认识到计算机网络对科学研究的重要性，因此从 1985 年起，NSF 就围绕其六个大型计算机中心建设计算机网络。1986 年，NSF 建立了国家科学基金网（NSFNET），它是一个三级计算机网络，分为主干网、地区网和校园网，覆盖了全美国主要的大学和研究所。同时，NSFNET 也和 ARPANET 相连。1989 年～1990 年，NSFNET 主干网成为 Internet 中的主要部分。到了 1990 年，鉴于 ARPANET 的实验任务已经完成，在历史上起过重要作用的 ARPANET 就正式宣布关闭。

1991 年，世界上的许多公司纷纷接入到 Internet，使网络上的通信量急剧增大，每日传送的分组数达 10 亿之多。于是美国政府决定将 Internet 主干转交给私人公司来经营，并开始对接入 Internet 的单位收费。然后，IBM、MERIT 和 MCI 成立了一个非营利的公司 ANS（Advanced Networks and Services）。ANS 公司于 1993 年建造了一个速率为 45Mbps 的主干网 ANSNET 来取代旧的 NSFNET。现在 NSF 已和 MCI 签订合同建造另一个更高速率（155Mbps）的主干网来代替现在的 ANSNET。

Internet 已经成为世界上规模最大和增长速率最快的计算机网络。根据 1995 年初的统计，有 12000 个网络连在 Internet 上，而每天约有 1200 台计算机入网。在 Internet 上的数据通信量每月约增加 10%，每天在世界范围有约 1500 万人直接使用 Internet。Internet 已连通了世界上的 137 个国家和地区。

目前，几乎所有的发达国家都相继建设了自己的国家级教育和科研计算机网络，并且与 Internet 互联在一起。实践表明，凡是建立了国家教育科研计算机网络的国家，其教育和科研事业都明显地得到迅速的发展。

1.3 计算机网络的分类和基本组成

计算机网络的分类方法有很多种，最主要的是以下两种分法：

1. 按通信传播方式划分

- 点对点传播方式网：它是以点对点的连接方式，把各个计算机连接起来的。这种传播方式的主要拓扑结构有星形、树形、环形和网形。
- 广播式传播方式网：它是用一个共同的传播介质把各个计算机连接起来的。主要有以同轴电缆连接起来的总线型网和以微波、卫星方式传播的广播型网。

2. 按距离划分

- 局域网（LAN——Local Area Network）。其作用范围通常为几米到几十千米。
- 广域网/远程网（WAN——Wide Area Network）。其作用范围一般为几十到几千千米。

以上两种为传统的划分方式，近年来在 LAN 与 WAN 之间又出现一种新的分类。

- 城域网（MAN——Metroplitan Area Network）。其作用范围界于 WAN 与 LAN 之间，运行方式与 LAN 相似。

下面将着重介绍局域网和广域网。

1.3.1 局域网

1.3.1.1 局域网络的基本拓扑结构

拓扑结构是指网络中的各个节点或站相互连接的方式。一种拓扑结构对应于一种通信线路连接和一种交换设备的分布方式。常用局域网络的拓扑结构有以下类型。

1. 星形结构

星形布局是以中央节点为中心与各节点连接而组成的，各节点与中央节点通过点与点方式连接，中央节点执行集中式通信控制策略，因此中央节点相当复杂，负担也重。目前流行的 PBX 就是星形拓扑结构的典型实例，如图 1-1 所示。

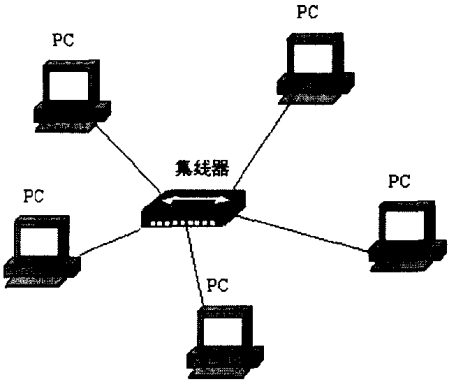

图 1-1　星形结构

以星形拓扑结构组网，其中任何两个站点要进行通信都必须经过中央节点控制。中央节点的主要功能有：

（1）为需要通信的设备建立物理连接；

（2）在两台设备通信过程中维持这一通路；

（3）在完成通信或不成功时，拆除通路。

在文件服务器/工作站(File Servers/Workstation)局域网模式中，中心点为文件服务器，存放共享资源。由于这种拓扑结构，中心点与多台工作站相连，为便于集中连线，目前多采用集线器（HUB）。HUB 具有信号再生转发功能，通常有 4 个、8 个、12 个、16 个、24 个端口等规格，每个端口相对独立。

星形拓扑结构的特点是：

（1）网络结构简单，便于管理和集中控制，组网容易；

（2）网络延迟时间短，误码率低；

（3）网络共享能力较差，通信线路利用率不高，中央节点负担过重；