21世纪 高等院校计算机系列教材

网络与信息安全实验指导

赖小卿 主编
彭广川 副主编

中国水利水电出版社
www.waterpub.com.cn

21世纪高等院校计算机系列教材

网络与信息安全实验指导

赖小卿　主　编

彭广川　副主编

中国水利水电出版社

内 容 提 要

本书是中国水利水电出版社出版的教材《网络与信息安全教程》的配套实验指导，也可以独立作为上机指导书使用。内容主要包括：密码技术、数字签名与身份认证技术、防火墙技术、入侵检测技术、计算机病毒的防治、黑客常用的攻击技术、网络站点的安全、操作系统的安全和数据库安全。

本书是为了适应应用型院校“网络与信息安全”课程教学，以解决和分析具体安全问题为目的，而编写的一本适合应用型院校学生培养特点的实验教材。书中的案例均已在真实环境或虚拟机环境下通过验证。

为方便读者使用，本书提供实验所需的大部分软件，需要的读者请与本书作者联系，联系方式：laixiaoqing@tom.com。

图书在版编目（CIP）数据

网络与信息安全实验指导 / 赖小卿主编. —北京：中国水利水电出版社，2008

（21 世纪高等院校计算机系列教材）

ISBN 978-7-5084-5493-1

Ⅰ. 网… Ⅱ. 赖… Ⅲ. 计算机网络－安全技术－高等学校－教学参考资料 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2008）第 048762 号

书　　名	**网络与信息安全实验指导**
作　　者	赖小卿　主　编　彭广川　副主编
出版　发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京诚顺达印刷有限公司
规　　格	787mm×1092mm　16 开本　12.5 印张　306 千字
版　　次	2008 年 4 月第 1 版　2008 年 4 月第 1 次印刷
印　　数	0001—4000 册
定　　价	20.00 元

前　言

现在社会上介绍网络安全方面的教材有很多，但针对应用型院校的网络安全教材不多，能指导学生动手做的网络安全实验方面的教材更少。学生往往上机时不知所措，或者在上机操作时碰到问题在理论课本上却找不到解决办法。该教材的最大特色就是集中了两位一线老师多年的实践教学资源，书中所有的实验均已经在学生实验过程中多方面验证。本书力求内容丰富、结构清晰、通俗易懂、图文并茂，每个实例都有较为详细的操作步骤，这样不仅能够减小教师的工作量，更有利于学生理解课本中的知识点。

密码学是网络安全的基础，相关的实验在一般教材中很难体现。本教材的另一特点就是不仅通俗地描述了密码学的一些基本知识点，而且还精心准备了一些相对应的案例，让学生对整个网络安全体系有一个完整的认识。

本书第 1～9 章由赖小卿编写，第 10 和 11 章由彭广川编写，另外黎佳花了大量的宝贵时间对本书进行了校稿工作。本书在编写过程中，得到了计算机工程技术学院领导的支持，神州数码公司的张学良工程师审阅了全稿并提出了一些宝贵意见，在此一并表示衷心的感谢。

本书是一本网络安全实验教材，也可以供各行各业从事计算机信息与网络安全的读者阅读和参考。

特别提醒：作者提供的实验用软件中有一部分含有病毒，在使用的时候请及时关闭杀毒软件。另外，这些软件不会影响系统的正常运行，一般的杀毒软件都可以清除，也请读者不要用于不良目的。

由于编者水平有限，加上本书涉及的知识点很广，很多知识点限于篇幅不能详细描述，在描述过程中也难免存在一些错误和疏漏之处，恳请广大读者和有关专家批评指正。作者联系方式：laixiaoqing@tom.com。

编　者

2008 年 3 月

目　　录

前言
第 1 章　网络安全概述 1
实验 1.1　利用动画理解网络面临的安全威胁类型 1
实验 1.2　利用“P2P 终结者”软件实现访问控制技术 3
第 2 章　密码技术 10
实验 2.1　对称加密算法 DES 的实现 10
实验 2.2　非对称加密算法 RSA 的实现 12
实验 2.3　Hash 算法的实现 14
实验 2.4　PGP 软件的使用 15
实验 2.5　VPN 的实现 23
第 3 章　数字签名与身份认证技术 31
实验 3.1　企业根 CA 的建立和证书的获取 31
实验 3.2　利用证书保障 Web 站点的安全性 35
实验 3.3　独立根 CA 的综合应用 42
第 4 章　防火墙技术 54
实验 4.1　利用 WinRoute 创建包过滤规则 54
第 5 章　入侵检测技术 58
实验 5.1　入侵检测系统的安装与使用 58
实验 5.2　“冰之眼”网络入侵检测系统 64
实验 5.3　Scorpio-I 入侵检测系统 67
第 6 章　计算机病毒 70
实验 6.1　VBS 病毒的产生 70
实验 6.2　利用自解压文件携带木马程序 73
实验 6.3　可执行程序捆绑及检测 75
实验 6.4　计算机病毒的检测 77
实验 6.5　杀毒软件的安装与使用 81
第 7 章　黑客常用的攻击技术 86
实验 7.1　信息收集 86
实验 7.2　查找开放服务器的 IP 地址 90
实验 7.3　账号口令的破解 92
实验 7.4　LC5 软件的使用 94
实验 7.5　扫描工具——Superscan 软件的应用 100
实验 7.6　流光软件的使用 102
实验 7.7　利用 Retina 软件探测系统安全弱点 109

实验 7.8　Sniffer 软件的使用 113
实验 7.9　Iris 软件的使用 118
实验 7.10　冰河木马的使用 122
实验 7.11　逻辑炸弹的制作 125
实验 7.12　缓冲区溢出 126
第 8 章　网络站点的安全 130
实验 8.1　伪造电子邮件 130
实验 8.2　破解电子邮箱密码 134
实验 8.3　DNS 的安全设置 137
第 9 章　操作系统的安全（基于 Windows 2003） 140
实验 9.1　安全配置账号策略 140
实验 9.2　用户权限分配 146
实验 9.3　文件系统安全性 149
实验 9.4　EFS 的应用 154
实验 9.5　安全审计 161
第 10 章　操作系统的安全（基于 Linux） 165
实验 10.1　Linux 用户管理 165
实验 10.2　Linux 用户组管理 166
实验 10.3　Linux 文件访问权限管理 167
第 11 章　数据库安全 169
实验 11.1　SQL Server 2000 用户登录账户管理 169
实验 11.2　SQL Server 2000 数据库用户管理 175
实验 11.3　SQL Server 2000 角色管理 177
实验 11.4　SQL Server 2000 权限管理 182
实验 11.5　SQL Server 2000 数据库的备份与恢复 187

第 1 章　网络安全概述

本章包括的实验

- 实验 1.1　利用动画理解网络面临的安全威胁类型
- 实验 1.2　利用“P2P 终结者”软件实现访问控制技术

实验 1.1　利用动画理解网络面临的安全威胁类型

一、实验目的与要求

利用 Flash 动画演示当前流行的一些网络攻击类型与种类，以使学生理解网络面临的安全威胁的类型。

二、实验原理

网络存在着形形色色的安全威胁，常见的网络安全威胁包括：计算机病毒，拒绝服务攻击，内部、外部泄密，蠕虫，逻辑炸弹，信息丢失、篡改、销毁，特洛伊木马，黑客攻击，后门、隐蔽通道等。

三、实验环境与方案

在 Windows 操作系统环境下直接运行相关的 Flash 动画，观察动画演示，理解动画所表达的含义。注意该动画软件所在的文件夹必须放在 D 盘的根目录下。

四、实验步骤

（1）直接运行软件 AttackType.exe，打开软件的主界面，如图 1-1 所示。

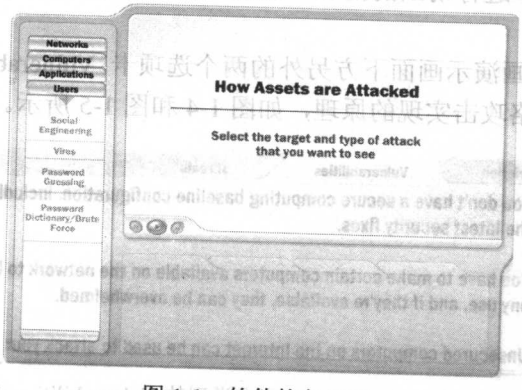

图 1-1　软件的主界面

（2）可以看出该动画将攻击类型分成四大类：Networks、Computers、Applications 和 Users。

（3）单击 Networks，出现一个下拉列表，如图 1-2 所示。可以看出 Networks 大类又分成 4 个小类：Denial of Service、Spoofing、Man-in-the-Middle、Replay 和 Packet Sniffing。

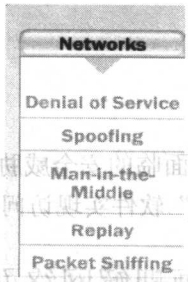

图 1-2 Networks 包括的 4 小类攻击类型

（4）单击其中的一个小类，如 Denial of Service，出现 Denial of Service 的动画演示及说明，如图 1-3 所示。

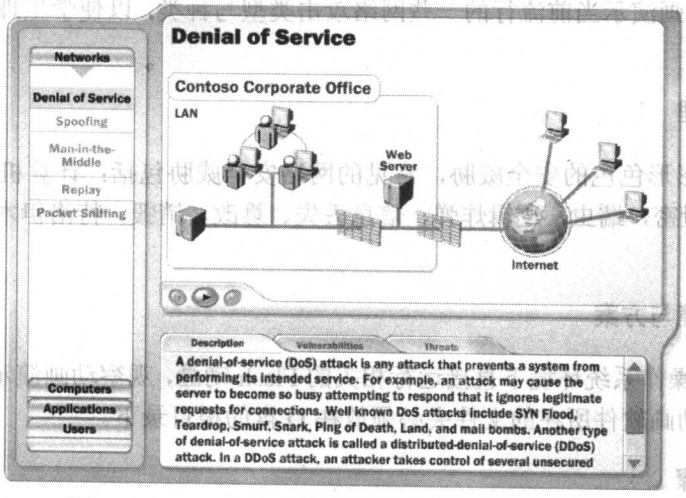

图 1-3 Denial of Service 攻击类型的动画演示及说明

（5）单击播放键进行动画的播放，通过动画的播放可以加深对该攻击类型基本实现过程的理解。

（6）再依次单击动画演示画面下方另外的两个选项卡 Vulnerabilities 和 Threats 来理解 Denial of Service 这种网络攻击实现的原理，如图 1-4 和图 1-5 所示。

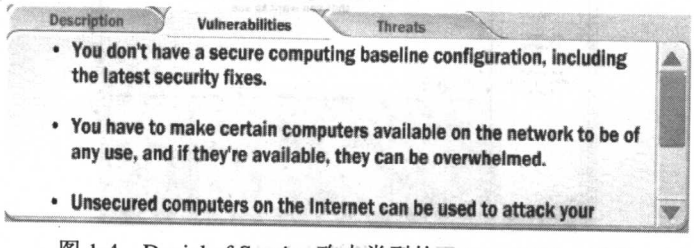

图 1-4 Denial of Service 攻击类型的 Vulnerabilities 说明

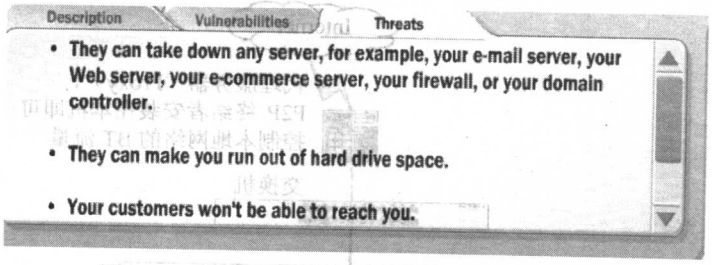

图 1-5　Denial of Service 攻击类型的 Threats 说明

五、思考题

1．Attack Type 软件总共包含了四大类 17 小类网络攻击类型的介绍，可以将全班学生分成若干个小组，分别将这些攻击类型的英文解释（包括 Description、Vulnerabilities 和 Threats 这 3 个选项卡）翻译成中文。

2．请根据表 1-1 所示的实际情况描述填写面临的安全威胁种类。

表 1-1　指出安全威胁种类

实际情况描述	面临的安全威胁种类
攻击者能够接触到服务器	
客户机到服务器的信息为明文	
服务器收到含有木马的邮件	
服务器没有应用可预防缓冲区溢出的更新	

实验 1.2　利用“P2P 终结者”软件实现访问控制技术

一、实验目的与要求

通过安装与使用“P2P 终结者”软件实现访问控制技术。

二、实验原理

访问控制技术就是通过不同的手段和策略实现网络上主体对客体的访问控制。在 Internet 上，客体是指网络资源，主体是指访问资源的用户或应用。访问控制的目的是保证网络资源不被非法使用和访问。“P2P 终结者”软件可以对网络中的其他主机进行限制与监控管理，例如带宽限制、自定义 ACL 规则控制、IP-MAC 绑定控制、FTP 下载限制、WWW 站点自定义控制、QQ、MSN、局域网非法 Sniffer 主机检测等。

三、实验环境及方案

P2P 终结者软件根据网络环境的不同有两种安装模式：

（1）安装于代理服务器上。这种安装方式适用于本地网络采用代理服务器方式接入公网，如图 1-6 所示。

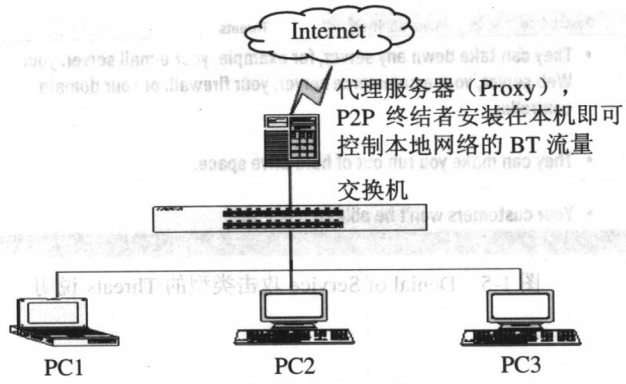

图 1-6　使用代理服务器

（2）安装于本地网络任意一台主机上。这种安装方式适用于任何公网接入方式，当然最佳环境是 ADSL 路由器共享上网环境，如图 1-7 所示。如果你有代理服务器，那么建议采用第一种方式。

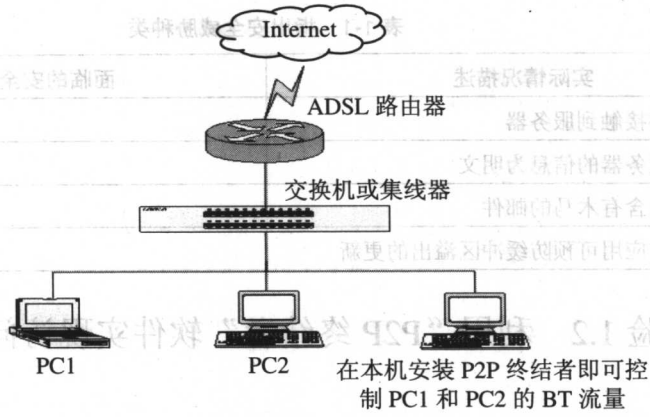

图 1-7　使用 ADSL 路由器共享上网

本次实验采用在虚拟环境下的 3 台 PC 机：A 机安装“P2P 终结者”软件，B 机作为被“P2P 终结者”软件控制的一台网络主机，C 机作为一台模拟的已搭建好的 Web 服务器。实验环境如表 1-2 所示。注意，由于本实验在虚拟机环境下完成，所以无法模拟使用 ADSL 路由器共享上网的环境，但可以利用 ISA Server 2004 模拟代理服务器。

表 1-2　3 台 PC 机的 IP 地址及角色与任务

	IP 地址	角色与任务
A 机	10.0.0.1 222.200.8.1	安装“P2P 终结者”软件和 ISA Server 2004
B 机	10.0.0.2	被“P2P 终结者”软件控制的一台内部网络主机
C 机	222.200.8.2	模拟外部网络一个已搭建好的 Web 服务器

四、实验步骤

（1）在 A 机上将软件包中的文件全部拷贝到 D:\program files\p2pzjz 中（如果没有该文件夹，需要在 D 盘的根目录下建立一个名为 program files 的文件夹），第一次使用前双击“用前

双击.cmd”文件，再双击 P2POver.exe 

以启动主程序，如图 1-8 所示。

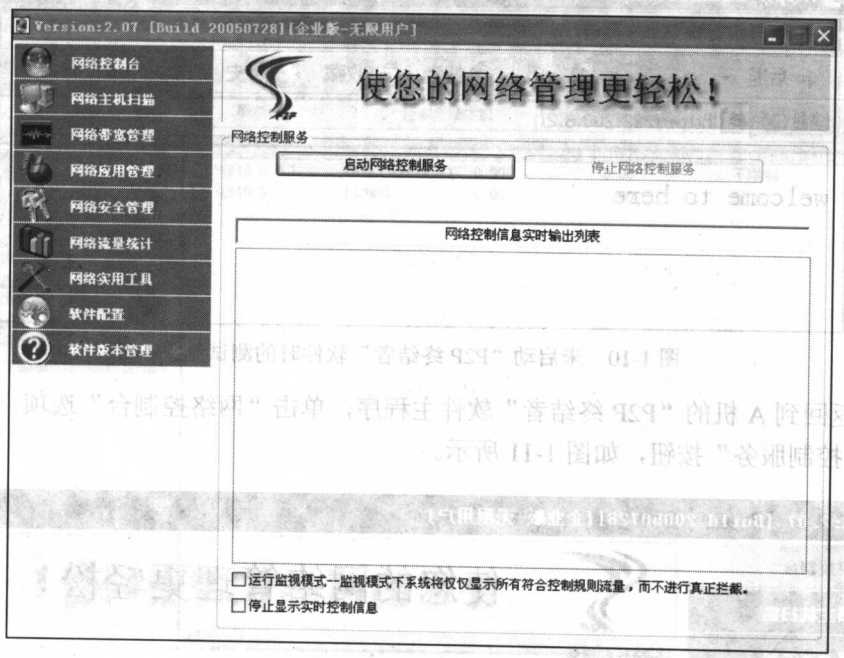

图 1-8　软件的主界面

（2）在“软件配置”界面中选择监测所使用的网卡，再单击“保存配置”按钮，如图 1-9 所示。

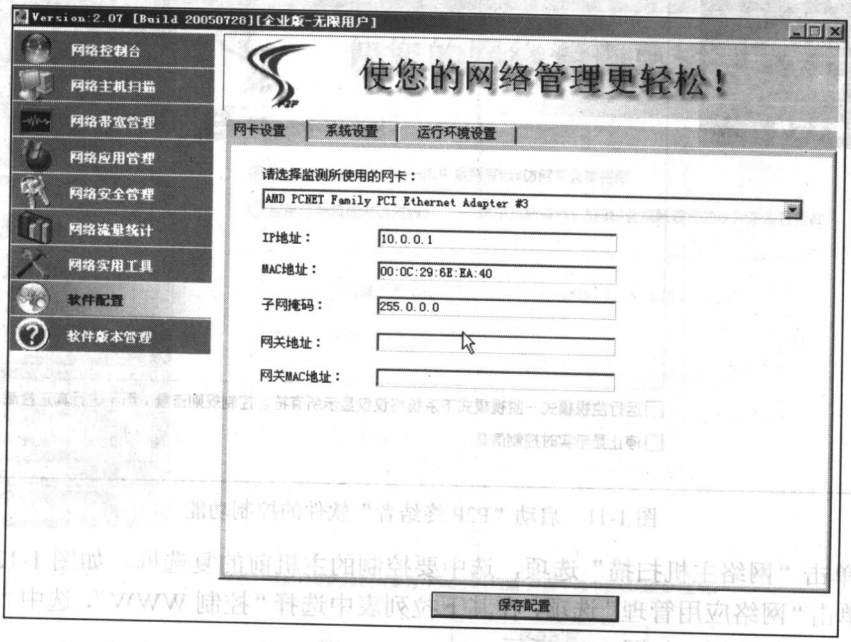

图 1-9　网卡的设置

（3）在 B 机上测试是否能够通过 IE 访问 C 机的 Web 服务器，如图 1-10 所示。

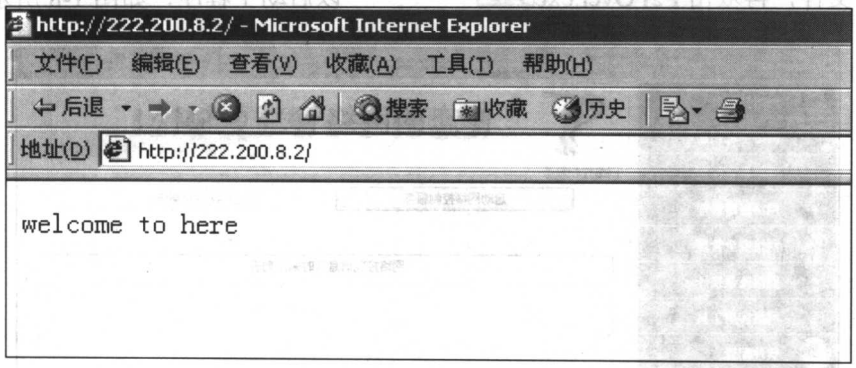

图 1-10 未启动“P2P 终结者”软件时的测试结果

（4）返回到 A 机的“P2P 终结者”软件主程序，单击“网络控制台”选项，在右侧单击“启动网络控制服务”按钮，如图 1-11 所示。

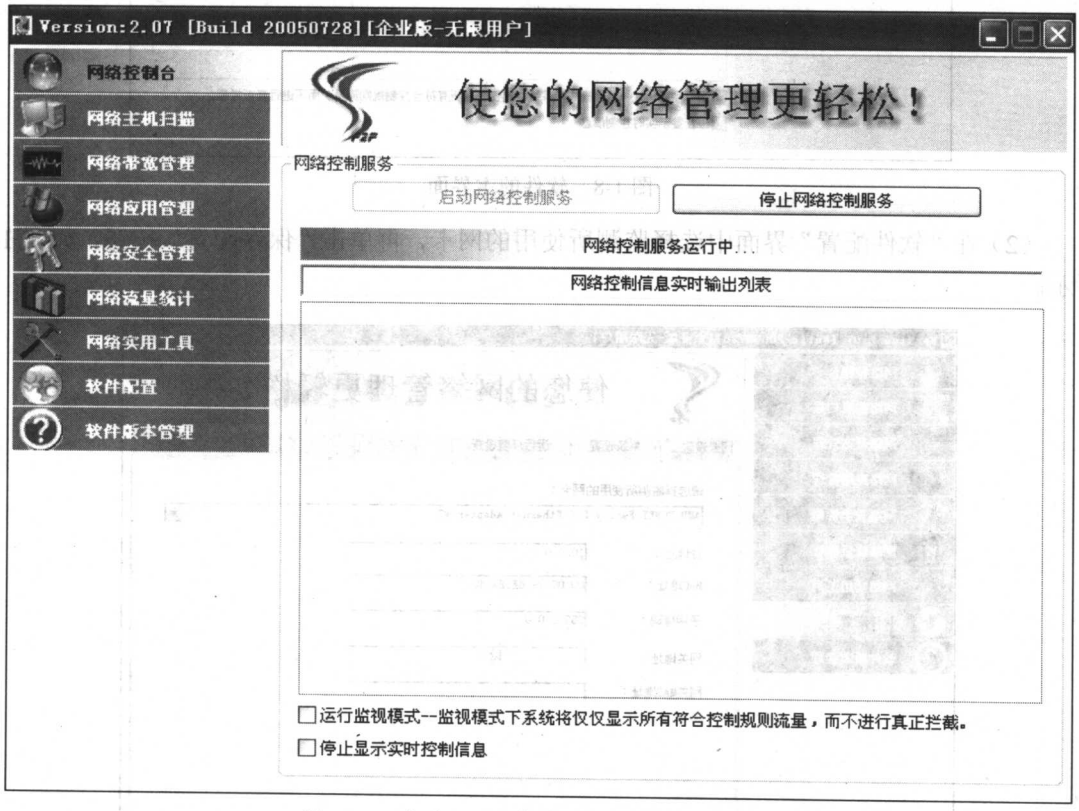

图 1-11 启动“P2P 终结者”软件的控制功能

（5）单击“网络主机扫描”选项，选中要控制的主机前的复选框，如图 1-12 所示。

（6）单击“网络应用管理”选项，在其下拉列表中选择“控制 WWW”，选中“启用 WWW 访问控制”前的复选框，如图 1-13 所示。

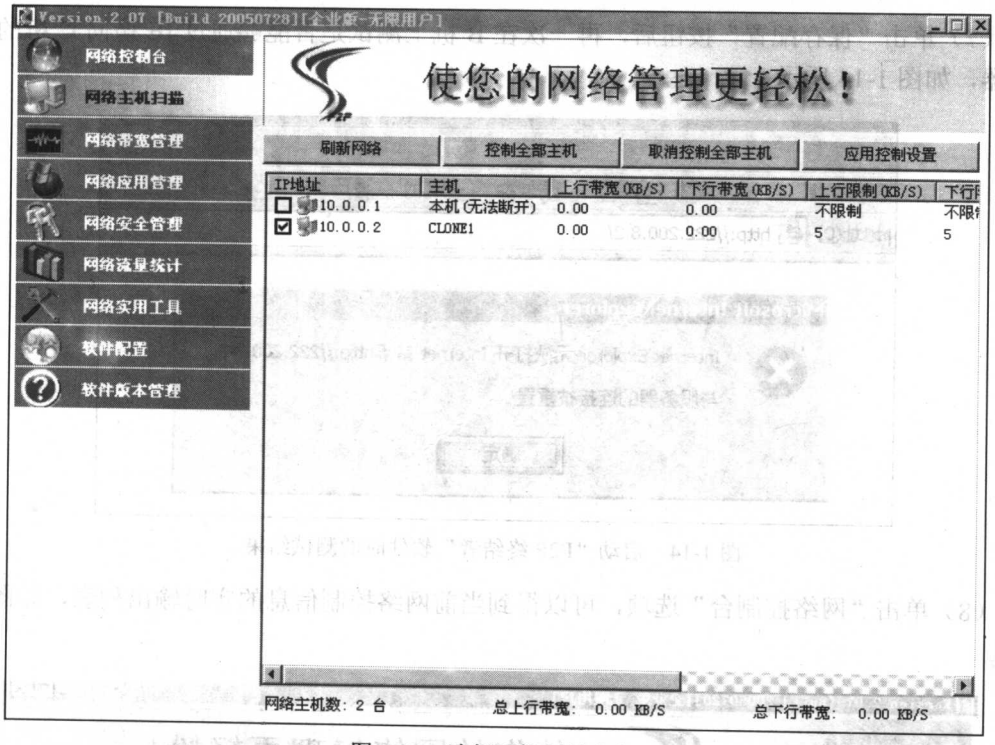

图 1-12　选择要控制的主机

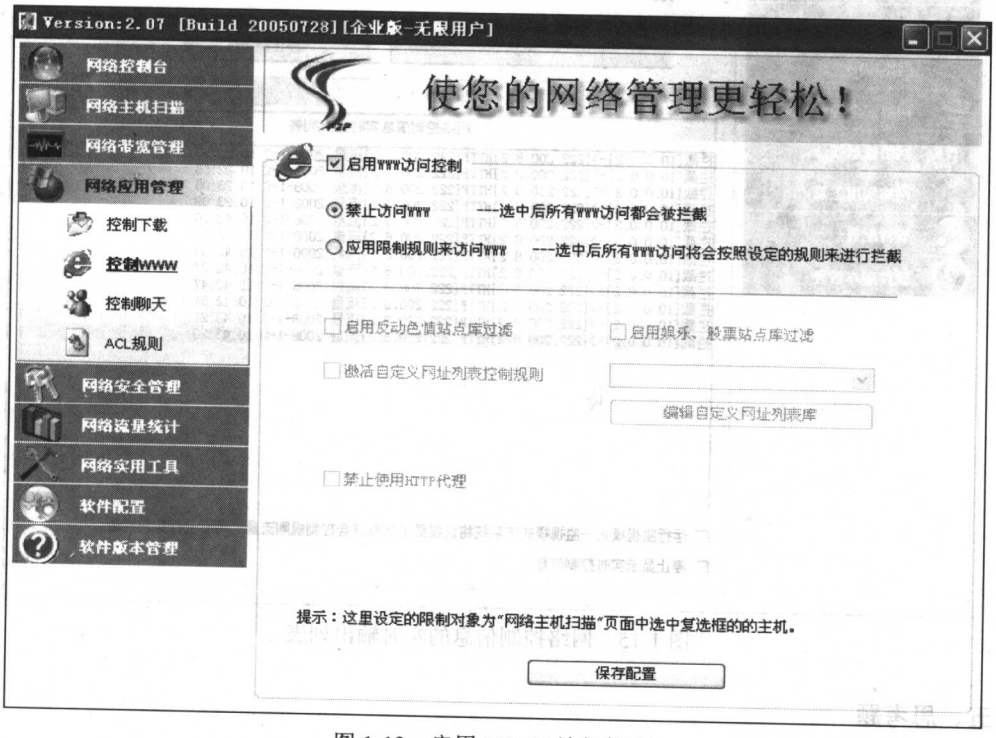

图 1-13　启用 WWW 访问控制

（7）单击“保存配置”按钮后，再一次在 B 机上测试是否能够通过 IE 访问 C 机的 Web 服务器，如图 1-14 所示。

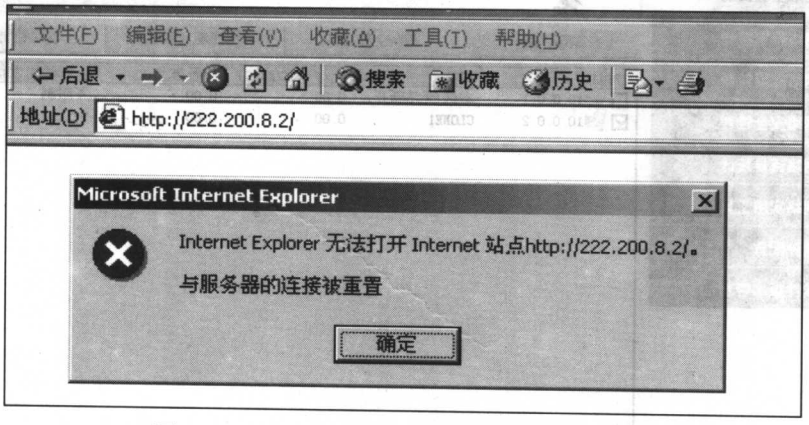

图 1-14 启动“P2P 终结者”软件时的测试结果

（8）单击“网络控制台”选项，可以得到当前网络控制信息的实时输出列表，如图 1-15 所示。

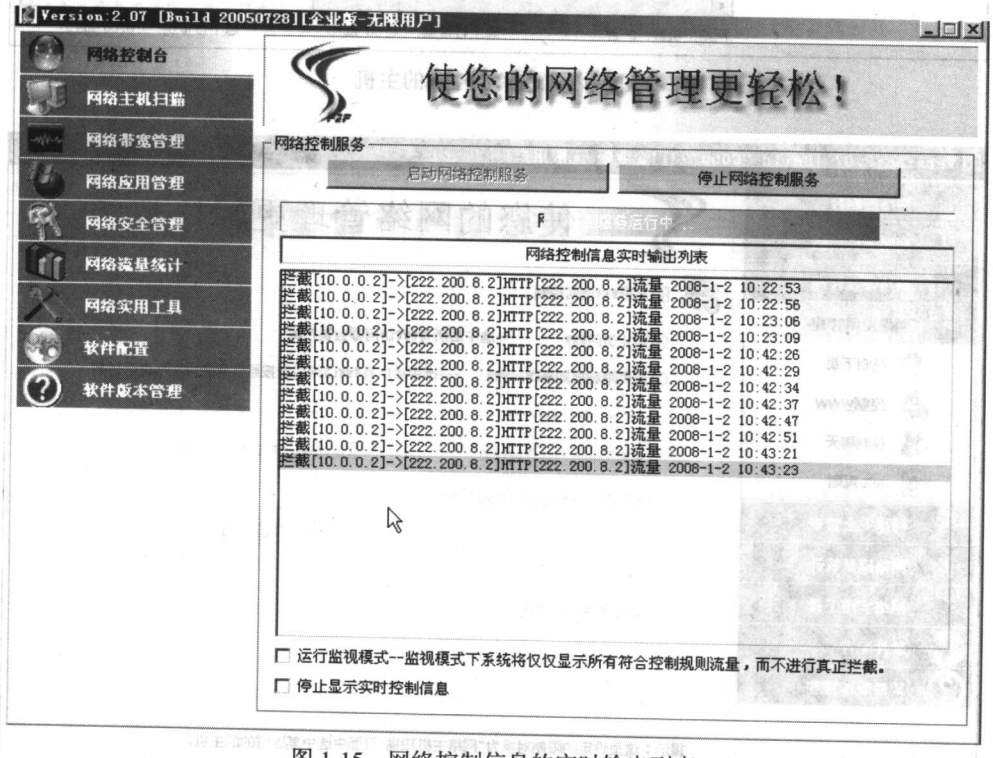

图 1-15 网络控制信息的实时输出列表

五、思考题

利用资源软件中给出的 WinPacp 3.0 软件和“反 P2P 终结者”软件可以成功清除网络内运

行的 P2P 终结者，如图 1-16 所示。请设计一个实验方案用来验证该功能，并写出实验步骤。

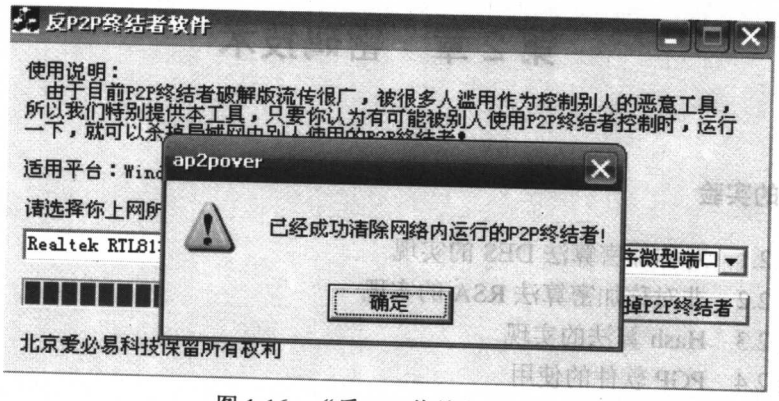

图 1-16　“反 P2P 终结者”软件

第 2 章　密码技术

本章包括的实验

- 实验 2.1　对称加密算法 DES 的实现
- 实验 2.2　非对称加密算法 RSA 的实现
- 实验 2.3　Hash 算法的实现
- 实验 2.4　PGP 软件的使用
- 实验 2.5　VPN 的实现

实验 2.1　对称加密算法 DES 的实现

一、实验目的与要求

通过 MixedCS 软件对实际数据进行加密和解密来了解 DES 的运行原理。

二、实验原理

DES 算法属于对称算法，即加密和解密使用同一密钥。DES 一个致命的缺陷就是密钥长度短，并且对于当前的计算能力，56 位的密钥长度已经抗不住穷举攻击，而 DES 又不支持变长密钥。但 DES 算法可以一次使用多个密钥，从而等同于更长的密钥。目前可以采用三重 DES 算法来解决这个缺陷。

三、实验环境与方案

在 Windows 操作系统环境下利用软件 MixedCS 验证 DES 算法的加密功能。

四、实验步骤

（1）直接运行软件 MixedCS.exe，打开软件的主界面，如图 2-1 所示。

（2）单击“浏览文件”按钮，选择要进行 DES 加密的源文件，选择成功后在“输出文件”文本框中将自动出现默认的文件名。

（3）选中“DES 加密”单选项，在“DES 密钥”文本框中输入 4 位密钥，在“确认密钥”文本框中重新输入相同的 4 位密钥。

（4）单击“加密”按钮，稍等片刻后弹出加密成功及时间说明提示对话框，如图 2-2 所示。

（5）将步骤 3 的密钥长度设为 10 位，重复加密过程，此时该软件将自动采用 3DES 算法进行加密，可以看出加密的时间明显增加了，如图 2-3 所示。

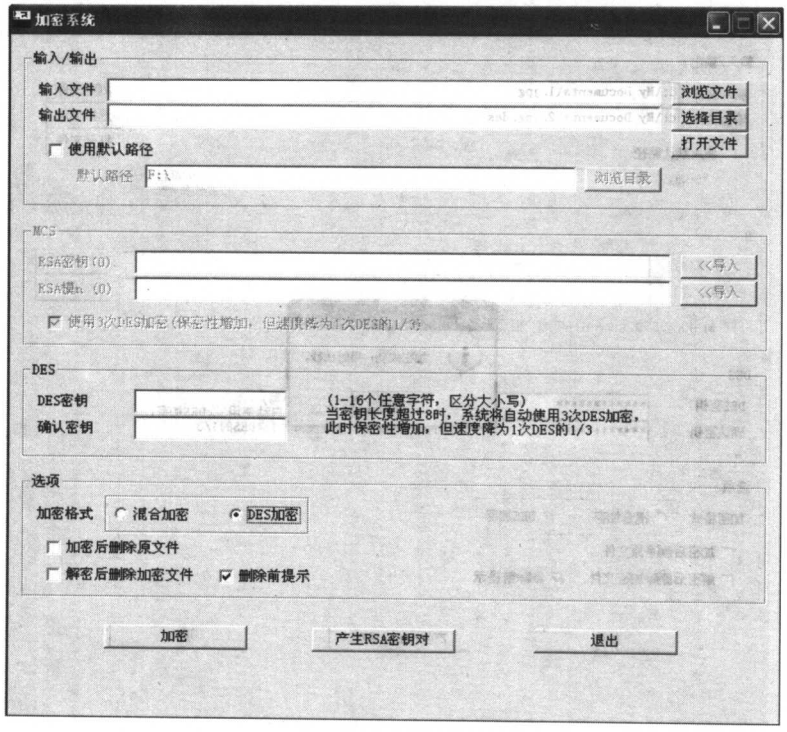

图 2-1　软件的主界面

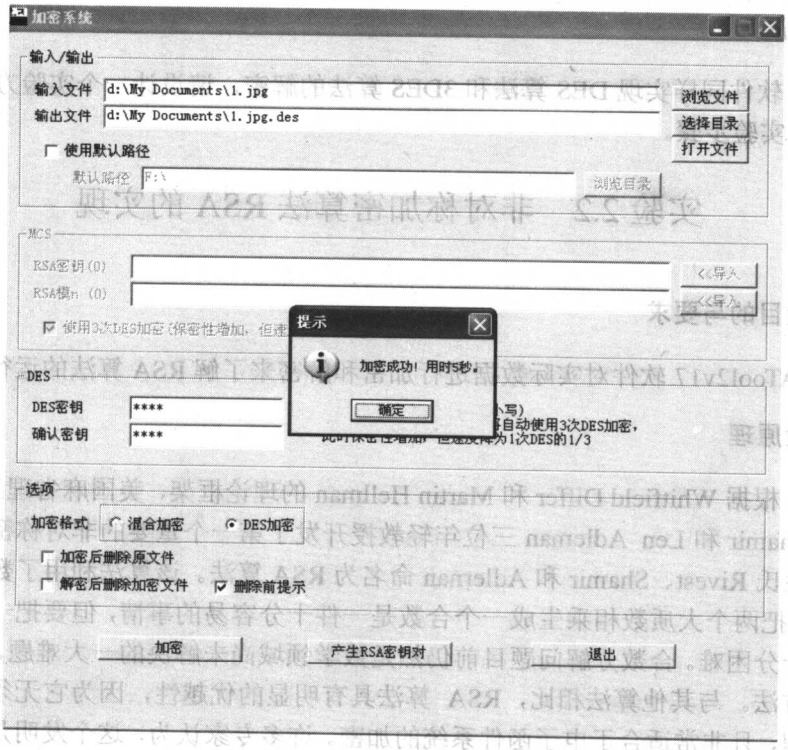

图 2-2　DES 加密算法