全国高等院校计算机职业技能应用规划教材

WANGLUO ANQUAN JISHU JI SHIXUN

# 网络安全技术及实训

童　均　陈学平◎编著

中国人民大学出版社

# 网络安全技术及实训

全国高等院校计算机职业技能应用规划教材

# 网络安全技术及实训

童 均 陈学平 编 著

中国人民大学出版社
·北京·

**图书在版编目（CIP）数据**

网络安全技术及实训/童均，陈学平编著. —北京：中国人民大学出版社，2013.1
全国高等院校计算机职业技能应用规划教材
ISBN 978-7-300-16401-4

Ⅰ.①网… Ⅱ.①童…②陈… Ⅲ.①计算机网络-安全技术-高等学校-教材 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2012）第 217843 号

全国高等院校计算机职业技能应用规划教材

**网络安全技术及实训**

童 均 陈学平 编 著

| | | | |
|---|---|---|---|
| **出版发行** | 中国人民大学出版社 | | |
| **社　　址** | 北京中关村大街 31 号 | **邮政编码** | 100080 |
| **电　　话** | 010-62511242（总编室） | | 010-62511398（质管部） |
| | 010-82501766（邮购部） | | 010-62514148（门市部） |
| | 010-62515195（发行公司） | | 010-62515275（盗版举报） |
| **网　　址** | http://www.crup.com.cn | | |
| | http://www.ttrnet.com(人大教研网) | | |
| **经　　销** | 新华书店 | | |
| **印　　刷** | 北京密兴印刷有限公司 | | |
| **规　　格** | 185 mm×260 mm　16 开本 | **版　　次** | 2013 年 1 月第 1 版 |
| **印　　张** | 20.25 | **印　　次** | 2013 年 1 月第 1 次印刷 |
| **字　　数** | 507 000 | **定　　价** | 38.00 元 |

# 前 言

本书依托中国电子教育学会高职高专计算机类专业2012年教学研究规划课题“高职计算机网络专业人才培养模式创新与实践”（课题编号：CESEZ2012-24），全面介绍了网络安全的基本框架、网络安全的基本理论以及交接机、路由器、防火墙、无线网络的安全。

本书注重实践技能的培养，以实训为依托，深入浅出地讲解理论知识的应用，因此既可作为高等院校计算机及相关专业的教材，也可作为计算机网络安全类的技术参考书或培训教材。

本书从实战出发，以应用为目的，防范手段为重点，理论讲述为基础，避免了传统网络安全教材理论过多、实用性不强的问题，紧密跟踪网络安全领域最新问题和技术运用。

本书的主要内容如下：

第1章　网络安全概述。主要介绍了网络安全的特征、现状，网络攻击手段，网络安全分析和网络安全防范措施，同时设置了3个实训来强化技能。

第2章　操作系统安全。主要介绍了用户账号安全、文件访问安全、端口安全与防范、软件安全、注册表安全、系统日志的安全审计、系统备份与恢复等内容，同时设置了7个实训来强化实践技能。

第3章　网络加密与认证技术。主要介绍了加密技术、数字证书、网络加密技术等内容，设置了5个上机实训进行操作。

第4章　交换机安全配置。主要介绍了交换机端口安全、IEEE 802.1x安全网络接入，设置了5个实训进行技能提高。

第5章　路由器安全配置。主要介绍了PPP协议、MD5认证技术、网络地址转换、访问控制列表等内容，设计了7个实训来强化技能。

第6章　防火墙安全配置。主要介绍了防火墙的相关知识如作用、类型、特性，并以锐

捷防火墙为例进行了实例介绍。全章安排了6个实训来巩固防火墙的知识。

第7章　虚拟专用网。主要介绍了远程VPN、站点到站点的VPN、服务器的VPN配置、路由器的VPN配置，并介绍了锐捷VPN的配置实例。全章安排了7个实训来进行操作。

第8章　无线网络安全。主要介绍了无线网络安全技术，并以锐捷无线交换机和无线路由器为例进行了实例介绍。全章安排了10个实训来进行上机操作。

第9章　入侵检测系统。主要介绍了入侵检测系统的相关概念，并介绍了使用Session-Wall监测ping flooding的相关技术。全章安排了1个实训来进行入侵检测的练习。

本书内容系统全面，结构清晰，注重实用性和应用性。主要特色如下：

1. 在本书写作中，作者力求做到理论与实践相结合，课程内容与实训相结合。通过实训，让读者加深对网络安全理论知识的理解，掌握网络安全管理的技能，以期达到活学活用的目的。

2. 本书是一本内容丰富、特色鲜明、实用性强的信息安全理实一体化教材。本书包含了主流网络安全技术的操作和使用，实训内容非常详细，可以拿来即用。

3. 本书从方便老师上课和学生学习的角度来进行各个知识点讲述和上机操作实训，立足于“看得懂、学得会、用得上”，重点突出最新网络安全技术的可操作性和实用性，强化读者的网络安全防护能力。

本书由重庆电子工程职业学院童均和陈学平老师编著，在编写过程中参考了网络上的相关资料，在此向原作者表示感谢。本书在编写和出版过程中得到出版社的支持与帮助，也得到了编者家人的支持，在此一并表示感谢。

**编　者**
**2012年秋**

# 目　录

# 第 1 章　网络安全概述

## 学习目标

- 了解网络安全的特征和现状；
- 熟悉常用的黑客攻击手段；
- 学会从不同方面分析网络的安全性；
- 掌握基本的网络安全防范措施；
- 能够使用网络监听器捕获网络的信息；
- 通过冰河木马远程控制掌握木马攻击的原理和过程；
- 掌握利用 IPC 漏洞进行网络攻击的方法。

## 1.1　网络安全的特征

网络安全是指通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。

网络安全的具体含义会随着“角度”的变化而变化。从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护。从网络运行和管理者的角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“后门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害、对国家造成巨大损失。从社会教育和意识形态角度来说，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

网络安全应具有保密性、完整性、可用性、可控性、可审查性五个方面的特征。

- 保密性：信息不泄露给非授权用户、实体或过程，或供其利用的特性。
- 完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。
- 可用性：可被授权实体访问并按需求使用的特性，即当需要时能够存取所需网络安全解决措施的信息。例如，网络环境下拒绝服务，破坏网络和相关系统正常运行都属于对可用性的攻击。
- 可控性：对信息的传播及内容具有控制能力。

● 可审查性：出现安全问题时提供依据与手段。

## 1.2 网络安全现状

网络已经成为生活的必备工具，经济、文化、军事和社会活动都强烈地依赖于网络。网络环境的复杂性、多变性以及信息系统的脆弱性、开放性和易受攻击性，决定了网络安全威胁的客观存在。人们在享受到各种生活便利和沟通便捷的同时，网络安全问题也日益突出。网络攻击、病毒传播、垃圾邮件等迅速增长，利用网络进行盗窃、诈骗、敲诈勒索、窃密等案件逐年上升，严重影响了网络的正常秩序，严重损害了网民的利益；网上色情、暴力等不良和有害信息的传播，严重危害了青少年的身心健康。网络系统的安全性和可靠性正在成为世界各国共同关注的焦点。在2011年，一些世界名企或重要部门也遭受了黑客攻击，造成重大的经济损失和社会影响。

(1) 2011年4月，索尼娱乐PlayStation和Qriocity服务网站受到黑客攻击，导致7 700万用户个人信息泄露，通过破解索尼数据库，黑客们窃取了数据库中的用户个人信息包括出生日期、邮件、家庭地址和登录信息，索尼至少失损失了1.78亿美元。

(2) 2011年5月健康网发现网站存在安全漏洞，可能会影响270万保单持有人的个人信息。这起事件是2009年5月以来的第二次伍德兰希尔斯事件后的首期医疗信息失窃事件，2009年5月的伍德兰希尔斯事件中，存有150万客户医疗和财务数据的便携式磁盘驱动器失踪。

(3) 2011年5月，Fidelity National Information Services报道说由于一些“未经授权的活动”，该公司损失了1300万美元。有媒体称是因为一些网络犯罪分子侵入该公司网络并进入了保存账号余额的中央数据库。

(4) 2011年6月，花旗集团报道黑客窃取了银行系统中21万卡持有人的姓名、账户号码和电子邮件地址信息，而其他一些信息如出生日期和社会安全号码没有泄露。

(5) 2011年8月，互联网激进组织Anonymous成功入侵旧金山地铁系统BART网站，公布了该网站数百个用户信息，与BART相关的网站都被篡改，各种精心设计的Anonymous黑客集团的标志出现在网站各处。该组织从BART数据库盗取的数据包括姓名、地址、电话号码和电子邮件账户。

(6) 2011年9月，街机和自动贩卖机供应商Vacationland Vendors宣布黑客从该公司系统窃取了信用卡和借记卡号码。

我国互联网网络安全状况继续保持平稳状态，基础信息网络防护水平明显提升，政府网站安全事件显著减少，网络安全事件处置速度明显加快，但以用户信息泄露为代表的与网民利益密切相关的事件，引起了公众对网络安全的广泛关注。

我国遭受境外的网络攻击持续增多，网上银行面临的钓鱼威胁愈演愈烈，工业控制系统安全事件呈现增长态势，手机恶意程序现多发态势，木马和僵尸网络活动越发猖獗，应用软件漏洞呈现迅猛增长趋势，DDoS攻击仍然呈现频率高、规模大和转嫁攻击的特点。

## 1.3 网络攻击手段

网络攻击手段可分为非破坏性攻击和破坏性攻击两类。非破坏性攻击一般是为了扰乱系统的运行，并不盗取系统资料，通常采用拒绝服务攻击或信息炸弹；破坏性攻击是以侵入他人计算机系统、盗取系统保密信息、破坏目标系统的数据为目的。下面为大家介绍几种常用

的攻击手段。

1. 后门程序

当程序员设计一些功能复杂的程序时，一般采用模块化的程序设计思想，将整个项目分割为多个功能模块，分别进行设计、调试，这时的后门就是一个模块的秘密入口。在程序开发阶段，后门便于测试、更改和增强模块功能。正常情况下，完成设计之后需要去掉各个模块的后门，不过有时由于疏忽或者其他原因（如将其留在程序中，便于日后访问、测试或维护）后门没有去掉，一些别有用心的人会利用穷举搜索法发现并利用这些后门，然后进入系统并发动攻击。

2. 拒绝服务

拒绝服务又叫 DDOS 攻击，它是使用超出被攻击目标处理能力的大量数据包消耗可用系统、带宽资源，最后致使网络服务瘫痪的一种攻击手段。作为攻击者，首先需要通过常规的黑客手段侵入并控制某个网站，然后在服务器上安装并启动一个可由攻击者发出的特殊指令来控制进程，攻击者把攻击对象的 IP 地址作为指令下达给进程的时候，这些进程就开始对目标主机发起攻击。这种方式可以集中大量的网络服务器带宽，对某个特定目标实施攻击，因而威力巨大，顷刻之间就可以使被攻击目标带宽资源耗尽，导致服务器瘫痪，比如 1999 年美国明尼苏达大学遭到的黑客攻击就属于这种方式。

3. 网络监听

网络监听是一种监视网络状态、数据流以及网络上传输信息的管理工具，它可以将网络接口设置在监听模式，并且可以截获网上传输的信息，也就是说，当黑客登录网络主机并取得超级用户权限后，若要登录其他主机，使用网络监听可以有效地截获网上的数据，这是黑客使用最多的方法，但是，网络监听只能应用于物理上连接于同一网段的主机，通常被用做获取用户口令。

4. 电子邮件炸弹

电子邮件炸弹（E-mail Bomb）是黑客常用的一种攻击手段，用伪造的 IP 地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的恶意邮件，也可称之为大容量的垃圾邮件。由于每个人的邮件信箱是有限的，当庞大的垃圾邮件到达信箱时，就会挤满信箱，把正常的邮件给冲掉。同时，因为它占用了大量的网络资源，常常导致网络堵塞，使用户不能正常工作，严重时会给电子邮件服务器操作系统带来危险，甚至瘫痪。

5. 特洛伊木马

特洛伊木马程序是黑客常用的攻击手段。它通过在你的计算机系统隐藏一个木马程序，在 Windows 启动时运行，采用服务器/客户机的运行方式，从而达到在上网时控制计算机的目的。黑客利用它窃取口令、浏览驱动器、修改文件、登录注册表，如流传极广的冰河木马和灰鸽子木马。现在流行的很多病毒也都带有黑客性质，如影响面极广的“Nimda”、“求职信”、“红色代码”及“红色代码 II”等。攻击者可以佯称自己为系统管理员（邮件地址和系统管理员完全相同），将这些病毒通过电子邮件的方式发送。如某些单位的网络管理员会定期给用户免费发送防火墙升级程序，这些程序多为可执行程序，这就为黑客提供了可乘之机，很多用户稍不注意就可能在不知不觉中遗失重要信息。

6. 网络钓鱼

黑客编写一些看起来“合法”的程序，上传到一些 FTP 站点或是提供给某些个人主页，

诱导用户下载。当用户下载软件时，黑客的软件一起下载到用户的机器上。该软件会跟踪用户的计算机操作，静静地记录着用户输入的每个口令，然后把它们发送到黑客指定的Internet邮箱。例如，有人发送给用户电子邮件，内容是用户需求调查，作为对填写表格的回报，允许用户免费使用软件。但是，该程序实际上却是搜集用户的口令，并把它们发送给某黑客。

## 1.4 网络安全分析

1. 物理安全分析

网络的物理安全是整个网络系统安全的前提。在网络工程建设中，由于网络系统属于弱电工程，耐压值很低，因此在网络工程的设计和施工中，必须优先考虑保护人和网络设备不受电、火灾和雷击的侵害；考虑布线系统与照明电线、动力电线、通信线路、暖气管道及冷热空气管道之间的距离；考虑布线系统与绝缘线、裸体线的安全，以及接地与焊接的安全；必须建设防雷系统，防雷系统不仅要考虑建筑物防雷，还必须要考虑计算机及其他弱电耐压设备的防雷。总体来说物理安全的风险主要有：地震、水灾、火灾等环境事故；电源故障；人为操作失误或错误；设备被盗、被毁；电磁干扰；线路截获；高可用性的硬件；双机多冗余的设计；机房环境及报警系统、安全意识等，因此要尽量避免网络的物理安全风险。

2. 网络结构的安全分析

网络拓扑结构设计也直接影响到网络系统的安全性。假如在外部和内部网络进行通信时，内部网络的机器安全就会受到威胁，同时也影响在同一网络上的许多其他系统。通过网络传播，还会影响连接 Internet/Intranet 的其他网络；还可能涉及法律、金融等安全敏感领域。因此，我们在设计时有必要将公开服务器（Web、DNS、E-mail 等）与外网/内部其他业务网络进行必要的隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他请求服务在到达主机之前就应该遭到拒绝。

3. 系统的安全分析

所谓系统的安全是指整个网络操作系统和网络硬件平台是否可靠且值得信任。目前恐怕没有绝对安全的操作系统可以选择，无论是 Microsoft 的 Windows NT 或者商用 UNIX 操作系统，其开发厂商必然留有 Back-Door。因此，我们可以得出结论：没有完全安全的操作系统。不同的用户应从不同的方面对网络做详尽的分析，选择安全性尽可能高的操作系统。同时必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性；严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

4. 应用系统的安全分析

应用系统的安全与具体的应用有关，涉及面非常广泛。应用系统的安全是动态的、不断变化的，应用的安全性也涉及信息的安全性。

5. 管理的安全风险分析

管理是网络中安全最最重要的部分。责权不明、安全管理制度不健全，以及缺乏可操作性都可能引起管理安全的风险。当网络出现攻击行为或网络受到其他安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索和破案依据，即缺乏对网络的可控性和可审查性。这就要求我们必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。建立全新网络安全

机制，必须深刻理解网络并能提供直接的解决方案，最可行的做法是将健全的管理制度与严格管理相结合，保障网络安全运行，使其成为一个具有良好的安全性、可扩充性和易管理性的信息网络。一旦上述的安全隐患成为事实，则对整个网络的损失是难以估计的。因此，网络的安全建设是网络建设过程中的重要一环。

## 1.5 网络安全防范措施

随着计算机技术的迅速发展，在计算机上处理的业务也由基于单机的数学运算、文件处理，基于简单连接的内部网络的业务处理、办公自动化等发展到基于复杂的内部网（Intranet）、企业外部网（Extranet）、全球互联网（Internet）的企业级计算机处理系统和世界范围内的信息共享和业务处理。在系统处理能力提高的同时，系统的连接能力也在不断地提高。但在连接能力、流通能力提高的同时，基于网络连接的安全问题也日益突出，整体的网络安全主要表现在：网络的物理安全、网络拓扑结构安全、网络系统安全、应用系统安全和网络管理安全等。因此，计算机安全问题应该像每家每户的防火防盗问题一样，做到防范于未然。不要认为你自己不会成为目标，以致一旦威胁出现，常常措手不及，造成极大的损失。

1. 采用安全防护技术

（1）物理措施防护。主要包括：保护网络关键设备，制订严格的网络安全规章制度，采取防辐射、防火以及安装不间断电源（UPS）等措施。

访问控制：对用户访问网络资源的权限进行严格的认证和控制。例如，进行用户身份认证，对口令加密、更新和鉴别，设置用户访问目录和文件的权限，控制网络设备配置的权限，等等。

（2）数据加密防护。加密是防护数据安全的重要手段，其作用是保障信息被人截获后不能读懂其含义。

（3）网络隔离防护。网络隔离有两种方式，一种是采用隔离卡来实现的，一种是采用网络安全隔离网来实现的。

（4）其他安全措施。其他措施包括信息过滤、容错、数据镜像、数据备份和审计等。

2. 提高安全防范意识

拥有网络安全意识是保证网络安全的重要前提。许多网络安全事件的发生都与缺乏安全防范意识有关。

3. 定期主机安全检查

要保证网络安全，进行网络安全建设，首先要全面了解系统，评估系统安全性，认识到自己的风险所在，从而迅速、准确解决内网安全问题。由安天实训室自主研发的国内首款创新型自动主机安全检查工具，彻底颠覆传统系统保密检查和系统风险评测工具操作的繁冗性，一键操作即可对内网计算机进行全面的安全保密检查及精准的安全等级判定，并对评测系统进行强有力的分析处置和修复。

## 1.6 实训 1—1：网络窃听

**【实训目的】**

掌握网络监视器的使用；

清楚 FTP 通信过程；

掌握 FTP 文件传输的相关命令。

**【实训背景】**

某公司为了实现员工之间共享文件，建立了 FTP 服务器，为每个员工分配账号和密码，员工可以使用自己的账号和密码通过 FTP 服务器下载和上传文件。黑客小黑了解到公司传递文件的方式，便将计算机连接到该公司的局域网上，利用微软自带的网络监听来捕获该公司员工的用户名和密码，然后窃取公司资料。

**【实训拓扑】**

实训拓扑如图 1—1 所示。

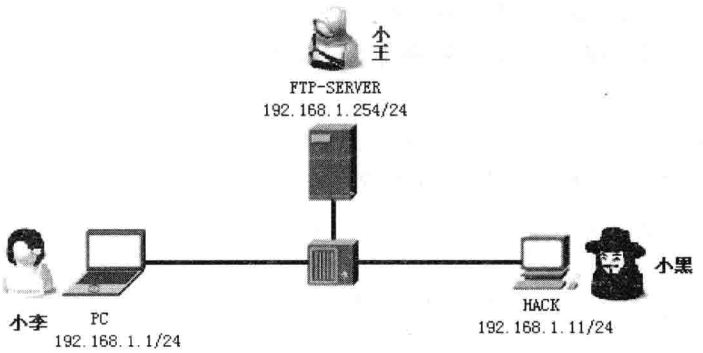


**图 1—1　实训拓扑**

**【实训设备】**

实训设备清单如表 1—1 所示。

**表 1—1　　实训设备清单**

| 设备类型 | | 数　量 |
|---|---|---|
| 计算机 | Windows 操作系统 | 1 台 |
| | Windows 2000/2003 操作系统（提供 FTP 服务） | 1 台 |
| | Windows 2000/2003 操作系统（提供网络监视） | 1 台 |
| 集线器 | | 1 台 |

**【实训步骤】**

1. 按拓扑图连接计算机和服务器，并配置计算机和服务器的 IP 地址，保证所有计算机之间畅通

2. 小李在服务器 FTP-SERVER 上配置 FTP 服务

（1）在 C 盘的 ftp 文件夹下创建文件 1. txt，其内容为“ftp test!”，如图 1—2 所示。

（2）配置服务器的 FTP 站点属性，将“C:\ftp”设置为主目录，如图 1—3 所示。

3. 小黑在计算机 HACK 上安装网络监视工具

（1）选择“开始→控制面板→添加或删除程序”，在“添加或删除程序”窗口中选择“添加/删除 Windows 组件”，打开“Windows 组件向导”窗口，如图 1—4 所示。

（2）选择“管理和监视工具”，单击“详细信息”按钮，进入“管理和监视工具”对话框，如图 1—5 所示。

（3）在窗口中勾选“网络监视工具”，单击“确定”按钮，返回到“Windows 组件向导”对话框，然后单击“下一步”按钮完成网络监视器的安装。


图 1—2　在 ftp 文件夹下创建文件

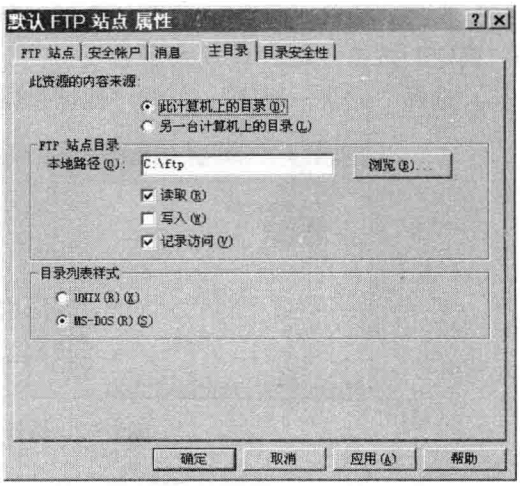


图 1—3　设置“C:\ftp”为主目录

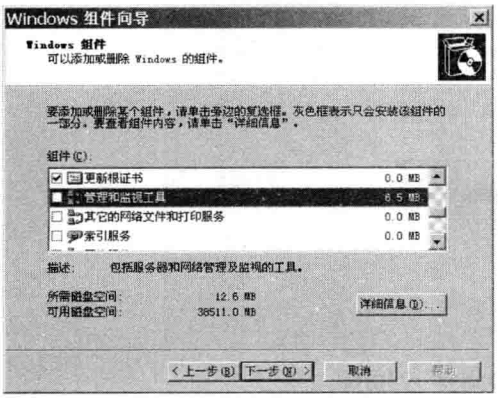


图 1—4　打开 Windows 组件向导

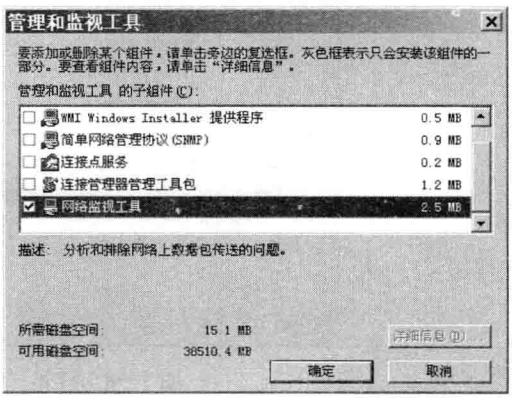


图 1—5　“管理和监视工具”对话框

4. 小黑在计算机 HACK 上配置网络监视器

(1) 双击“管理工具”窗口中的“网络监视器”，打开“Microsoft 网络监视器”窗口，如图 1—6 所示。

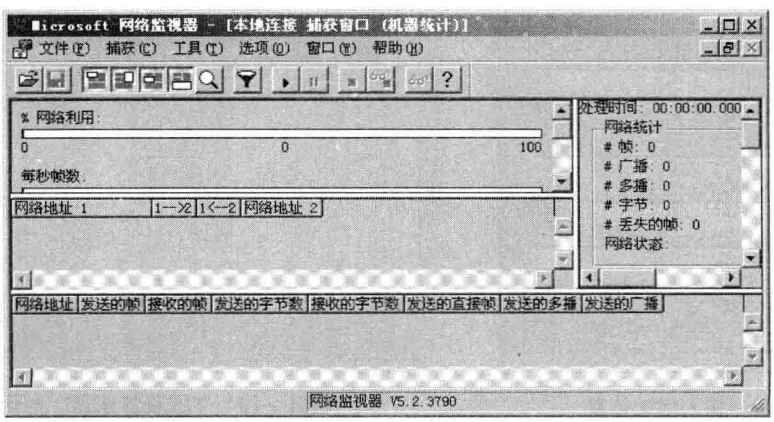


图 1—6　Microsoft 网络监视器

（2）选择“捕获→网络”，打开“选择一个网络”窗口，在窗口中选择“本地连接”，并单击‘确定”按钮，如图 1—7 所示。

（3）选择“捕获→地址”，打开“地址数据库”对话框，如图 1—8 所示。

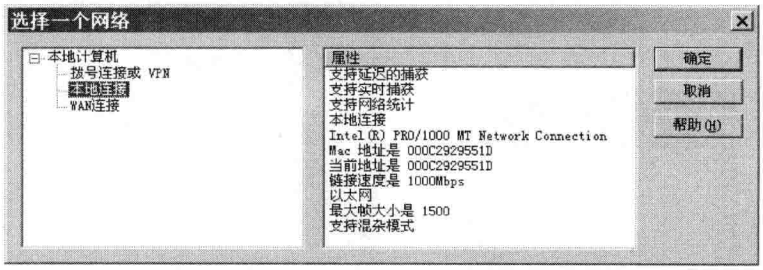


图 1—7　选择“本地连接”

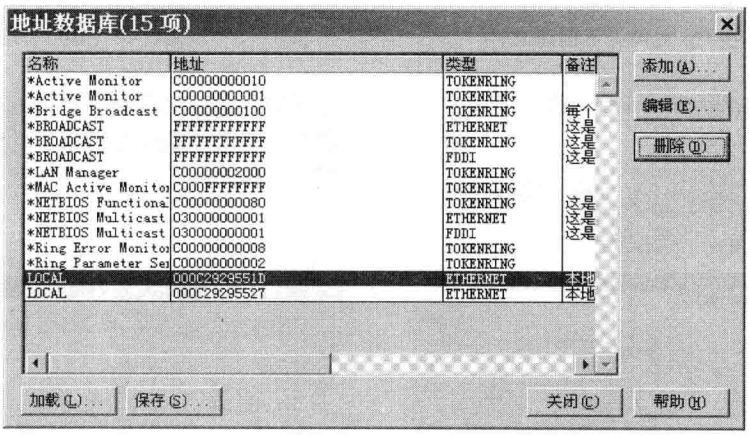


图 1—8　打开“地址数据库”对话框

（4）单击右侧的“添加”按钮，打开“地址信息”窗口，在窗口中输入名称“SERVER”信息，如图 1—9 所示。

（5）选择“捕获→筛选器”，打开“捕获筛选器”对话框，如图 1—10 所示。

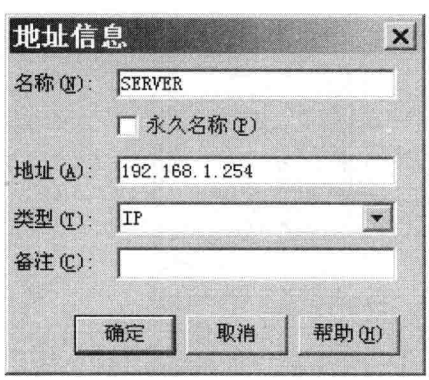


图 1—9　输入地址信息

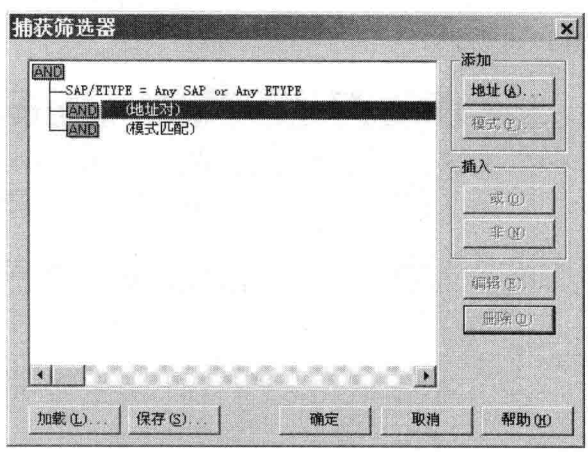


图 1—10　“捕获筛选器”对话框