“十三五”国家重点出版物出版规划项目
高等教育网络空间安全规划教材

信息安全概论

第 2 版

李 剑 主编

机 械 工 业 出 版 社

本书是一本信息安全专业知识的普及教材，以教育部高等学校网络空间安全类专业教学指导委员会所列知识点为基础，以帮助信息安全、网络空间安全专业学生全面了解信息安全知识为目的而编写。全书共 19 章，第 1 章讲解信息安全概述；第 2 章讲解网络安全基础；第 3 章讲解网络扫描与监听；第 4 章讲解黑客攻击技术；第 5 章讲解网络后门与网络隐身；第 6 章讲解计算机病毒与恶意软件；第 7 章讲解物理环境与设备安全；第 8 章讲解防火墙技术；第 9 章讲解入侵检测技术；第 10 章讲解虚拟专用网技术；第 11 章讲解 Windows 操作系统安全；第 12 章讲解 UNIX 与 Linux 操作系统安全；第 13 章讲解密码学基础；第 14 章讲解 PKI 原理与应用；第 15 章讲解数据库系统安全；第 16 章讲解信息安全管理与法律法规；第 17 章讲解信息系统等级保护与风险管理；第 18 章讲解信息系统应急响应；第 19 章讲解数据备份与恢复。

本书可作为信息安全、网络空间安全、计算机类相关专业的教材，也可用于从事信息安全工作的专业人员或爱好者参考。

本书配套授课电子课件，需要的教师可登录 www. cmpedu. com 免费注册，审核通过后下载，或联系编辑索取。QQ：2850823885。电话：010-88379739。

图书在版编目（CIP）数据

信息安全概论/李剑主编 . —2 版 . —北京：机械工业出版社，2019. 1
“十三五”国家重点出版物出版规划项目　高等教育网络空间安全规划教材
ISBN 978-7-111-61837-9

Ⅰ. ① 信…　Ⅱ. ① 李…　Ⅲ. ① 信息安全-高等学校-教材　Ⅳ. ① TP309

中国版本图书馆 CIP 数据核字（2019）第 028903 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
策划编辑：郝建伟　　责任编辑：郝建伟
责任校对：张艳霞　　责任印制：张　博
北京华创印务有限公司印刷

2019 年 3 月第 2 版 · 第 1 次印刷
184mm×260mm · 15. 25 印张 · 370 千字
0001-3000 册
标准书号：ISBN 978-7-111-61837-9
定价：49. 00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务	网络服务
服务咨询热线：(010) 88379833	机 工 官 网：www. cmpbook. com
读者购书热线：(010) 88379649	机 工 官 博：weibo. com/cmp1952
	教育服务网：www. cmpedu. com
封面无防伪标均为盗版	金　书　网：www. golden-book. com

高等教育网络空间安全规划教材
编委会成员名单

机械工业出版社版权所有，不得转载！

前　言

2014 年，随着斯诺登事件的不断发酵，世界各国更加重视网络安全。2014 年 2 月，中央网络安全和信息化领导小组宣告成立，并在北京召开了第一次会议。

在网络空间安全学科建设方面，2015 年 6 月，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予“工学”学位。2016 年初，国务院学位委员会正式下发《国务院学位委员会关于同意增列网络空间安全一级学科博士学位授权点的通知》，共有包括清华大学、北京邮电大学等 29 所高校获得我国首批网络空间安全一级学科博士学位授权点。2018 年初，教育部又公布了 7 所高校增设网络空间安全一级学科博士学位授权点。由此可见国家对信息安全的重视程度。

为了解决平时所遇到的信息安全问题，达到“普及信息安全知识”这一目的，作者编写了《信息安全概论》这本教材。它包含了目前信息安全领域常用的攻击技术和防护技术，以及信息安全管理的知识。在授课时，教师可以根据授课对象来选择教学的内容以及讲述的深度。对于那些没有学过计算机网络课程的学生，可以在课前适当加一些计算机网络、信息安全方面的知识。

本书共 19 章，第 1 章是信息安全概述，主要讲述了什么是信息安全、信息安全的历史、信息安全威胁等；第 2 章是网络安全基础，主要讲述了网络的 OSI 参考模型、TCP/IP 参考模型、常用的网络服务以及常用的网络命令等；第 3 章是网络扫描与监听，主要讲述了黑客的概念、网络扫描技术、网络监听技术等；第 4 章是黑客攻击技术，主要讲述了黑客攻击的流程以及常见的 8 种攻击行为；第 5 章是网络后门与网络隐身，主要讲述了木马攻击、网络后门等；第 6 章是计算机病毒与恶意软件，主要讲述了计算机病毒的概念、原理、特征，常见的计算机病毒、恶意软件等；第 7 章是物理环境与设备安全，主要讲述了信息系统的物理层安全知识；第 8 章是防火墙技术，主要讲述了防火墙的概念、作用、结构等；第 9 章是入侵检测技术，主要讲述了入侵检测的概念、误用入侵检测、异常入侵检测、主机入侵检测、网络入侵检测等；第 10 章是虚拟专用网技术，主要讲述了虚拟专用网的概念、作用、原理及虚拟专用网技术等；第 11 章是 Windows 操作系统安全，主要讲述了常见的 Windows 操作系统安全配置；第 12 章是 UNIX 与 Linux 操作系统安全，主要讲述 UNIX 和 Linux 操作系统安全配置；第 13 章是密码学基础，主要讲述什么是密码学、密码学的发展历史、古典密码学、对称密码学、公钥密码学、Hash 函数等；第 14 章是 PKI 原理与应用，主要讲述什么是 PKI、PKI 的体系结构、CA 证书等；第 15 章是数据库系统安全，主要讲述了针对数据库系统的攻击、数据库系统的防护等；第 16 章是信息安全管理与法律法规，主要讲述了信息安全管理的模式及意义、BS7799、常见信息安全法律法规等；第 17 章是信息系统等级保护与风险管理，主要讲述了信息系统的脆弱性、等级保护、风险管理、风险评估等；第 18 章是信息系统应急响应，主要讲述了信息系统应急响应的阶段、方法、组织，Windows 操作系统下的应急响应，计算机犯罪取证等；第 19 章是数据备份与恢复，主要讲述了数据备份和数据恢复。

本书第 3 章由山东省枣庄学院韦德泉教授编写；第 8 章由山东省枣庄学院梁兰菊教授编写；第 9 章由山东省枣庄学院吕凯凯老师编写；第 4、5、10～19 章由北京邮电大学王娜博士后编写；其余各章由北京邮电大学计算机学院李剑教授编写。

感谢北京邮电大学杨义先教授、钮心忻教授、罗群教授，上海交通大学李建华教授，他们对本书的写作提出了宝贵的意见和建议。感谢我的博士导师北京理工大学的曹元大教授，曹老师对于本书的写作给予了极大的支持与帮助。

其他参与本书编写和审阅工作的还有孟玲玉，这里一并感谢。

本书是国家自然科学基金（No. U1636106、No. 61472048）的资助成果。

由于本书作者水平有限，书中疏漏与不妥之处在所难免，恳请广大同行和读者指正。作者的电子邮箱是 lijian@ bupt. edu. cn。

李　剑

目　录

第 1 章　信息安全概述

本章从一些疑问和一个故事说起，进而讲述信息安全的定义、信息的安全威胁，以及信息安全发展的过程，然后讲述了信息安全的需求和信息安全实现，最后给出了本书的结构。

1.1　一些疑问

在使用计算机的时候，经常会遇到各种各样的安全疑问，比如：

1）现在市面上的病毒软件这么多，国外的有诺顿、卡巴斯基、Mcafee 等，国内的有江民、金山、瑞星等，究竟安装哪一款杀病毒软件，查杀病毒的效果会更好一些呢？

2）为什么 U 盘里经常会出现 Autorun. inf、RECYCLER、RavMonE. exe 等病毒相关文件呢？如何防止这些病毒的感染与发作呢？图 1-1 中所示为 U 盘病毒。

3）为什么计算机硬盘里经常会出现一个名为“runauto. .”的病毒文件夹，并且怎么删除都删除不掉呢？图 1-2 所示为 runauto. . 文件夹。

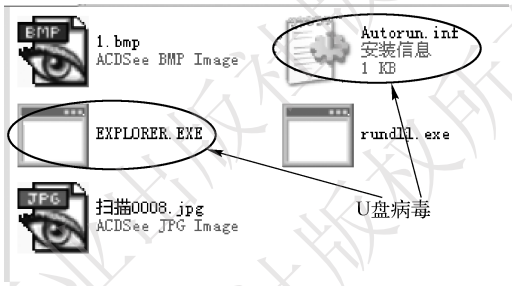

图 1-1　U 盘病毒

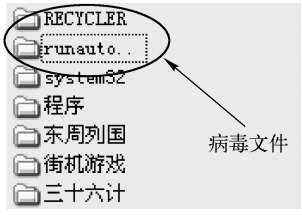

图 1-2　runauto. . 文件夹

4）为什么刚装好的 Windows 2000 专业版的计算机当中 C 盘、D 盘、E 盘等硬盘全是共享的，并且还有 IPC $空连接呢？如何去掉这些共享呢？图 1-3 为使用“net ␣ share”命令看到的操作系统中的共享信息（注：本书中所有的“␣”符号，代表空格的意思）。

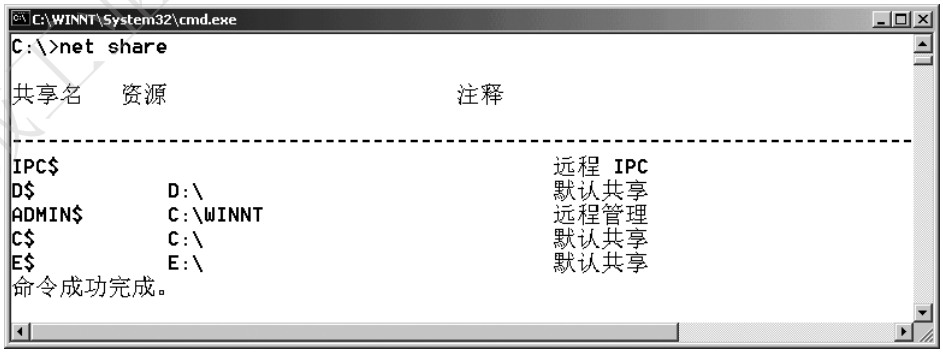

图 1-3　操作系统中的共享信息

5）如果有一天，发现自己的计算机运行很慢，鼠标乱动，并且硬盘灯在不停地闪动，这时怀疑自己的计算机中了病毒，那么应该怎样做应急处理呢？怎样找出病毒隐藏在什么地方呢？

6）如果有一天，自己的计算机在运行过程中死机了，重新启动不起来，安全模式也进不去。如果重新安装计算机的话，会删除计算机里许多重要的文件，这时应该怎样处理呢？

7）如何安装一台新的计算机？安装哪些软件才能使它更安全一些呢？安装的步骤是什么呢？对计算机的操作系统应该做怎样的设置呢？

8）如何一次性将计算机的所有补丁都安装上，而不是使用互联网慢慢下载，一个一个安装呢？

9）如何使用软件防火墙来封锁一个 IP 地址或一个端口呢？

10）当信息系统遭受攻击的时候，为什么经常会查到攻击人的 IP 地址在日本、美国或是在欧洲呢？难道真的有日本人、美国人或是欧洲人在攻击信息系统吗？

诸如此类的一系列安全问题，经常困扰着使用计算机的人们。以上这些问题正是本书要解决的问题。

1.2 一个故事

1. 故事的开始

在讲述信息安全之前，这里先讲述一个故事。这个故事发生在 2004 年 4 月 29 日。地点是德国北部罗滕堡镇的一个名叫沃芬森（Waffensen）的小村，这个村仅有 920 人。其中住着一家人，他们的房子如图 1-4 所示。

这个房子里住着一个小孩，名叫斯文-雅尚（Sven Jaschan），如图 1-5 所示。

图 1-4　德国沃芬森村的一个房子

图 1-5　斯文-雅尚

他的母亲叫维洛妮卡，开了一个门面不算大的以计算机维护修理为主的电脑服务部。4 月 29 日这一天是他 18 岁的生日。几天前，为了庆祝他的生日，他在网上下载了一些代码。修改之后将它放到了互联网上。

2. 故事的发展

第二天，这些代码开始在互联网上以一种“神不知鬼不觉”的特殊方式传遍全球。“中

招”后，计算机开始反复自动关机、重启，网络资源基本上被程序消耗，运行极其缓慢。如图 1-6 所示，计算机反复自动关机。如图 1-7 所示，病毒占用大量系统资源。

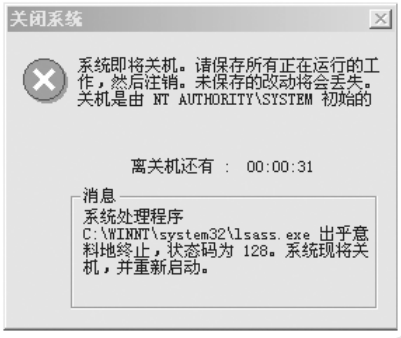

图 1-6　计算机反复自动关机

图 1-7　病毒占用大量系统资源

这就是全球著名的“震荡波”（Worm. Sasser）蠕虫病毒。自“震荡波”2004 年 5 月 1 日开始传播以来，不完全统计全球已有约 1800 万台计算机报告感染了这一病毒。

2004 年 5 月 3 日，“震荡波”病毒出现第一个发作高峰，当天先后出现了 B、C、D 三个变种，德国已有数以十万计的计算机感染了这一病毒。微软公司悬赏 25 万美元找元凶！

在我国，“五一”长假后的第一天，“震荡波”病毒的第二个高峰果然汹涌而来。仅 8 日上午 9 时到 10 时的短短一个小时内，瑞星公司就接到用户的求助电话 2815 个，且 30%为企业局域网用户，其中不乏大型企业局域网、机场、政府部门、银行等重要单位。9 日，“震荡波”病毒疫情依然没有得到缓解。

5 月的第一个星期（也就是“震荡波”迅速传播的时候），微软公司德国总部的热线电话就从每周 400 个猛增到 3. 5 万个。

3. 故事的结束

开始时，报道有俄罗斯人编写了这种病毒！因为这个小孩在编写这个病毒的过程中，加了一段俄罗斯语。

5 月 7 日，斯文-雅尚的同学为了 25 万美元，将其告发。斯文-雅尚被警察逮捕。

其实，这个小孩在最开始，并不是为了编写出一种病毒来危害别人，而是为了清除和对付“我的末日”（MyDoom）和“贝果”（Bagle）等计算机病毒。谁知，在编写病毒程序的过程中，他设计出一种名为“网络天空 A”（Net-sky）病毒变体。在朋友的鼓动下，他对“网络天空 A”进行了改动，最后形成了现在的“震荡波”病毒程序。

最后，由于这个小孩在传播病毒的时候不到 18 岁，所以没有受到过重的惩罚。再后来，据说他成了一名反病毒专家。

4. 病毒发作的原因

震荡波病毒是通过微软在 2004 年 4 月初发布的高危漏洞-LSASS 漏洞（微软 MS04-011 公告）进行传播的，危害性极大。那时的 Windows 2000/XP/Server 2003 等操作系统的用户都存在该漏洞，这些操作系统的用户只要一上网，就有可能受到该病毒的攻击。

只是大多数用户，对于微软所发布的这些漏洞，没有注意，或没有引起高度重视，从而不去打补丁，进而引起病毒的发作。

这已经是 10 多年前的病毒了。2004 年的时候从漏洞公布到病毒发作大概需要 1 个月左右的时间。现在这个时间段已经缩小到 1 天之内了。也就说漏洞公布的当天就有针对这个漏洞的病毒出现，这是多么可怕的事情。

5. 病毒的防治

震荡波病毒的防治很简单，只要安装上微软关于这个漏洞的补丁就行了。也可以使用流行的杀毒软件进行查杀。如图 1-8 所示为瑞星专杀工具。

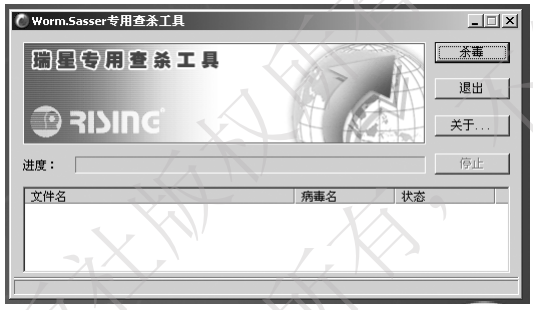

图 1-8　瑞星专杀工具

这种病毒由于太古老，已经不大可能入侵我们的计算机了。大家只要在计算机上安装上 360 安全卫士等杀毒软件，基本上已经不太可能感染早期的病毒了。

1.3　信息与信息安全

1.3.1　信息的定义

信息是一种消息，通常以文字或声音、图像的形式来表现，是数据按有意义的关联排列的结果。信息由意义和符号组成。信息就是指以声音、语言、文字、图像、动画、气味等方式所表示的实际内容。信息是客观事物状态和运动特征的一种普遍形式，客观世界中大量地存在、产生和传递着以这些方式表示出来的各种各样的消息。在谈到信息的时候，就不可避免地遇到信息的安全问题。

1.3.2　信息安全的定义

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多门学科的综合性学科。

从广义来说，凡是涉及信息的保密性、完整性、可用性等的相关技术和理论都是信息安全的研究领域。

信息安全本身包括的范围很大，大到国家军事政治等机密安全，小范围的当然还包括如防范商业企业机密泄露，防范青少年对不良信息的浏览，防止个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、信息认证和数据加密等），直至安全系统，其中任何一个安全漏洞便可以威胁全局安全。

1.3.3 P^2DR^2安全模型

基于闭环控制的动态信息安全理论模型在 1995 年开始逐渐形成并得到了迅速发展，学术界先后提出了 PDR、P^2DR 等多种动态风险模型，随着互联网技术的飞速发展，企业网的应用环境千变万化，现有模型存在诸多待发展之处。

P^2DR^2动态安全模型研究的是基于企业网对象、依时间及策略特征的（Policy，Protection，Detection，Response，Restore）动态安全模型结构，由策略、防护、检测、响应和恢复等要素构成，是一种基于闭环控制、主动防御的动态安全模型，通过区域网络的路由及安全策略分析与制定，在网络内部及边界建立实时检测、监测和审计机制，采取实时、快速动态响应安全手段，应用多样性系统灾难备份恢复、关键系统冗余设计等方法，构造多层次、全方位和立体的区域网络安全环境，如图 1-9 所示。

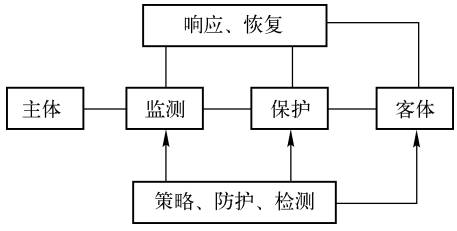

图 1-9　P^2DR^2动态安全模型

一个良好的网络安全模型应在充分了解网络系统安全需求的基础上，通过安全模型表达安全体系架构，通常具备以下性质：精确、无歧义、简单和抽象，具有一般性，充分体现安全策略。

该理论的最基本原理认为，信息安全相关的所有活动，不管是攻击行为、防护行为、检测行为和响应行为等都要消耗时间。因此可以用时间来衡量一个体系的安全性和安全能力。

作为一个防护体系，当入侵者要发起攻击时，每一步都需要花费时间。攻击成功花费的时间就是安全体系提供的防护时间 Pt；在入侵发生的同时，检测系统也在发挥作用，检测到入侵行为也要花费时间——检测时间 Dt；在检测到入侵后，系统会做出应有的响应动作，这也要花费时间——响应时间 Rt。

P^2DR^2模型就可以用一些典型的数学公式来表达安全的要求。

公式 1：Pt>Dt+Rt 。

Pt 代表系统为了保护安全目标设置各种保护后的防护时间；或者理解为在这样的保护下，黑客（入侵者）攻击安全目标所花费的时间。Dt 代表从入侵者开始发动入侵开始，系统能够检测到入侵行为所花费的时间。Rt 代表从发现入侵行为开始，系统能够做出足够的响应，将系统调整到正常状态的时间。那么，针对需要保护的安全目标，如果上述数学公式满足防护时间大于检测时间加上响应时间，也就是在入侵者危害到安全目标之前就能被检测

到并及时处理。

公式 2：Et = Dt + Rt，如果 Pt = 0。

公式的前提是假设防护时间为 0。Dt 代表从入侵者破坏了安全目标系统开始，系统能够检测到破坏行为所花费的时间。Rt 代表从发现遭到破坏开始，系统能够做出足够的响应，将系统调整到正常状态的时间。比如，对网页服务器被破坏的页面进行恢复。那么，Dt 与 Rt 的和就是该安全目标系统的暴露时间 Et。针对需要保护的安全目标，如果 Et 越小系统，就越安全。

通过上面两个公式的描述，实际上给出了安全一个全新的定义："及时的检测和响应就是安全""及时的检测和恢复就是安全"。而且，这样的定义为安全问题的解决给出了明确的方向：提高系统的防护时间 Pt，降低检测时间 Dt 和响应时间 Rt。

1.3.4 信息安全体系结构

在考虑具体的网络信息安全体系时，把安全体系划分为一个多层面的结构，每个层面都是一个安全层次。根据信息系统的应用现状情况和网络的结构，把信息安全问题可以定位在五个层次：物理层安全、网络层安全、系统层安全、应用层安全和管理层安全。如图 1-10 所示为信息安全体系结构以及这些结构层次之间的关系。

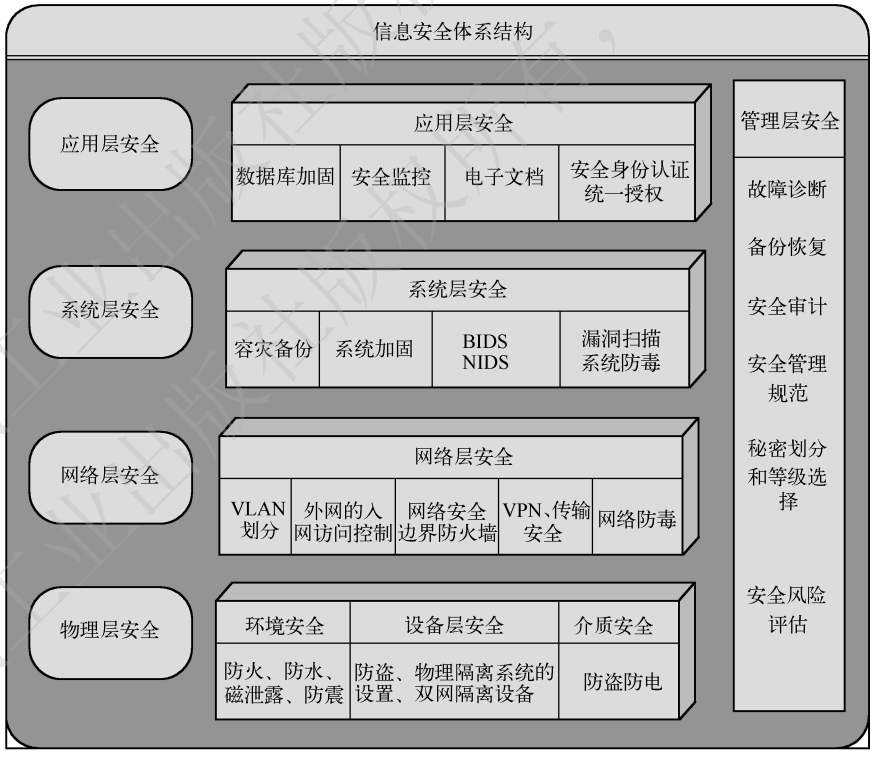

图 1-10　信息系统安全体系结构

1. 物理层安全

该层次的安全包括通信线路的安全、物理设备的安全、机房的安全等。物理层的安全主要体现在通信线路的可靠性（线路备份、网管软件、传输介质），软硬件设备安全性（替换

设备、拆卸设备、增加设备），设备的备份，防灾害能力、防干扰能力，设备的运行环境（温度、湿度、烟尘），不间断电源保障等。

2. 网络层安全

该层次的安全问题主要体现在网络方面的安全性，包括网络层身份认证，网络资源的访问控制，数据传输的保密与完整性，远程接入的安全，域名系统的安全，路由系统的安全，入侵检测的手段，网络设施防病毒等。网络层常用的安全工具包括防火墙系统、入侵检测系统、VPN 系统、网络蜂罐等。

3. 系统层安全

该层次的安全问题来自网络内使用的操作系统的安全，如 Windows XP、Windows 2010 等。其主要表现在三个方面，一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。

4. 应用层安全

应用层的安全考虑所采用的应用软件和业务数据的安全性，包括：数据库软件、Web 服务、电子邮件系统等。此外，还包括病毒对系统的威胁，因此要使用防病毒软件。

5. 管理层安全

俗话说“三分技术，七分管理”，管理层安全从某种意义上来说要比以上 4 个安全层次要重要。管理层安全包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化程度极大地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色定义都可以在很大程度上降低其他层次的安全威胁。

1.3.5 信息安全的目标

开始的时候，信息安全具有三个目标 CIA（Confidentiality、Integrity、Availability），即：保密性、完整性和可用性。后来，对信息安全的目标进行了扩展，将 CIA 三个目标扩展为：保密性、完整性、可用性、真实性、不可否认性、可追究性、可控性共 7 个信息安全技术目标。其中所增加的真实性、不可否认性、可追究性、可控性可以认为是完整性的扩展和细化。

1）保密性：保证机密信息不被窃听，或窃听者不能了解信息的真实含义。

2）完整性：保证数据的一致性，防止数据被非法用户篡改。

3）可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝。

4）真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别。

5）不可否认性：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的。

6）可控制性：对信息的传播及内容具有控制能力。

7）可追究性：对出现的网络安全问题提供调查的依据和手段。

1.4 信息的安全威胁

信息系统的安全威胁是永远存在的，下面从信息安全的五个层次，介绍信息安全中信息的安全威胁。

1.4.1 物理层安全风险分析

信息系统物理层安全风险主要包括以下方面：

- 地震、水灾、火灾等环境事故造成设备损坏。
- 电源故障造成设备断电以至操作系统引导失败或数据库信息丢失。
- 设备被盗、被毁造成数据丢失或信息泄露。
- 电磁辐射可能造成数据信息被窃取或偷阅。
- 监控和报警系统的缺乏或者管理不善可能造成原本可以防止的事故。

1.4.2 网络层安全风险分析

1. 数据传输风险分析

数据在传输过程中，线路搭载、链路窃听可能造成数据被截获、窃听、篡改和破坏，数据的机密性、完整性无法保证。

2. 网络边界风险分析

如果在网络边界上没有强有力的控制，则外部黑客就可以随意出入企业总部及各个分支机构的网络系统，从而获取各种数据和信息，那么泄露问题就无法避免。

3. 网络服务风险分析

一些信息平台运行 Web 服务、数据库服务等，如不加防范，各种网络攻击可能对业务系统服务造成干扰、破坏，如最常见的拒绝服务攻击 DoS 和 DDoS。

1.4.3 操作系统层安全风险分析

系统安全通常指操作系统的安全，操作系统的安装以正常工作为目标，在通常的参数、服务配置中，缺省地开放的端口中，存在很大安全隐患和风险。

而操作系统在设计和实现方面本身存在一定的安全隐患，无论是 Windows 还是 UNIX 操作系统，都不能排除开发商留有后门（Back-Door）。

系统层的安全同时还包括数据库系统以及相关商用产品的安全漏洞。

病毒也是系统安全的主要威胁，病毒大多利用了操作系统本身的漏洞，通过网络迅速传播。

1.4.4 应用层安全风险分析

1. 业务服务安全风险

在信息系统上运行着用于业务数据交互和信息服务的重要应用服务，如果不加以安全保护，不可避免地会受到来自网络的威胁、入侵、病毒的破坏，以及数据的泄密。

2. 数据库服务器的安全风险

信息系统通常需要基于数据库服务器提供业务服务，数据库服务器安全风险包括：

- 非授权用户的访问、通过口令猜测获得系统管理员权限。
- 数据库服务器本身存在漏洞容易受到攻击等。
- 数据库中数据由于意外而导致数据错误或者不可恢复等。

3. 信息系统访问控制风险

对于信息系统来说，在没有任何访问控制的情况下，非法用户的非法访问可能给信息系统造成严重干扰和破坏。因此，要采取一定的访问控制手段，防范来自非法用户的攻击，严格控制合法用户才能访问合法资源，以防范如下风险：

- 非法用户非法访问。
- 合法用户非授权访问。
- 假冒合法用户非法访问。

1.4.5 管理层安全风险分析

管理层安全是网络中安全得以保证的重要组成部分，是防止来自内部网络入侵必须的部分。责权不明、管理混乱、安全管理制度不健全及缺乏可操作性等都可能引起管理层安全的风险。

信息系统无论从数据的安全性、业务服务的保障性和系统维护的规范性等角度，需要严格的安全管理制度，从业务服务的运营维护和更新升级等层面加强安全管理能力。

1.5 信息安全的需求与实现

1.5.1 信息安全的需求

信息安全研究涵盖多项内容，其中包括网络自身的可用性、网络的运营安全、信息传递的机密性、有害信息传播控制等大量问题。然而通信参与的不同实体对网络安全关心的内容不同，对网络与信息安全又有不同的需求。在这里按照国家、用户、运营商以及其他实体来描述安全需求。

1. 国家对网络与信息安全的需求

国家对网络与信息安全有网络与应用系统可靠性和生存性的需求、网络传播信息可控性要求以及对网络传送的信息可知性要求。

1）网络与应用系统可靠性和生存性要求：国家要求网络与应用系统具有必要的可靠性，防范可能的入侵和攻击并具有必要的信息对抗能力，在攻击和灾难中具有应急通信能力，保障人民群众通信自由的需求以及重要信息系统持续可靠。

2）网络传播信息可控性要求：国家应当有能力通过合法监听得到通信内容；对于所得到的特定内容应当能获取来源与去向；在必要的条件下控制特定信息的传送与传播；此外国家应当制定必要的法律法规规范网络行为。

3）网络传送的信息可知性要求：国家应当有能力在海量的信息中筛选出需要的内容，分析并使用相应的信息内容。

2. 用户（企业用户、个人用户）对网络与信息安全需求

用户包括企业用户和个人用户，对网络与信息安全有通信内容机密性要求，用户信息隐私性要求，网络与应用系统可信任要求以及网络与应用系统可用性要求。

1）通信内容机密性要求：用户希望通信的内容应当通过加密或者隔离等手段，除国家授权机关以外只有通信对端能够获取并使用。

2）用户信息隐私性要求：用户希望用户留在网络上的个人信息、网络行为以及行为习惯等内容不被非授权第三方获取。

3）网络与应用系统可信任要求：用户希望网络能确认通信对端是希望与之通信的对端，应用系统应当有能力并有义务承担相应的责任。

4）网络与应用系统可用性要求：用户希望网络与应用系统达到所承诺的可用性，网络/应用系统不应具有传播病毒、发送垃圾信息和传播其他有害信息等行为。

3. 运营商（ISP、ICP 等）对网络与信息安全需求

运营商对网络与信息安全的要求包括满足国家安全需求、用户安全需求以及自身对网络与应用系统的可管理可运营需求。

1）满足国家安全需求：运营商满足国家安全需求包括应当提供合法监听点、对内容作溯源、控制特定信息的传送传播，提供必要的可用性等。

2）满足用户安全需求：运营商满足用户安全需求包括必要的认证和加密，有效的业务架构和商务模式保证双方有能力并有义务承担相应的责任，提供必要的可用性等。

3）网络与应用系统可管理可运营要求：运营商要求物力与系统资源只能由授权用户使用；资源由授权管理者调度；安全程度可评估可预警；风险可控；有效的商务模式保证用户和其他合作方实现承诺。

4. 其他实体对网络与信息安全的需求

其他参与实体对网络与信息安全还有如数字版权等其他安全需求。

1.5.2 信息安全的实现

信息安全的实现需要有一定的信息安全策略，它是指为保证提供一定级别的安全保护所必须遵守的规则。实现信息安全，不但靠先进的技术，也得靠严格的安全管理、法律约束和安全教育。

1. 先进的信息安全技术是网络安全的根本保证

用户对自身面临的威胁进行风险评估，决定其所需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术，形成一个全方位的安全系统。

2. 严格的安全管理

各计算机网络使用机构、企业和单位应建立相应的网络安全管理办法，加强内部管理，建立合适的网络安全管理系统，加强用户管理和授权管理，建立安全审计和跟踪体系，提高整体网络安全意识。

3. 制订严格的法律、法规

计算机网络是一种新生事物。它的许多行为仍无法可依，无章可循，导致网络上计算机犯罪处于无序状态。面对日趋严重的网络犯罪，必须建立与网络安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。

1.6 信息安全发展过程

信息安全自古以来就是受到人们关注的问题，但在不同的发展时期，信息安全的侧重点和控制方式有所不同。大致说来，信息安全在其发展过程中经历了三个阶段。

第一阶段：早在20世纪初期，通信技术还不发达，面对电话、电报、传真等信息交换过程中存在的安全问题，人们强调的主要是信息的保密性，对安全理论和技术的研究也只侧重于密码学，这一阶段的信息安全可以简单称为通信安全，即COMSEC（Communication Security）。

第二阶段：20世纪60年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息安全阶段，即INFOSEC（Information Security），具有代表性的成果就是美国的TCSEC和欧洲的ITSEC测评标准。

第三阶段：20世纪80年代开始，由于互联网技术的飞速发展，信息无论是对内还是对外都得到极大开放，由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经不仅仅是传统的保密性、完整性和可用性三个原则了，由此衍生出了诸如可控性、抗抵赖性、真实性等其他的原则和目标，信息安全也从单一的被动防护向全面且动态的防护、检测、响应、恢复等整体体系建设方向发展，即所谓的信息保障（Information Assurance）。这一点，在美国的IATF规范中有清楚的表述。

1.7 习题

1. 请说出平时在使用计算机的时候遇到的各种安全问题，以及当时的解决方案。
2. 什么是信息安全？
3. 什么是P^2DR^2动态安全模型？
4. 信息系统的安全威胁有哪些？
5. 信息安全实现需要什么样的策略？
6. 信息安全的发展可以分为哪几个阶段？

第 2 章　网络安全基础

本章将介绍最基本的网络安全参考模型、TCP/IP 协议族、常用的网络服务和常用的网络命令等，这些都是信息安全的基础知识。如果本章的内容已在其他课程中学习过，则本章可以选讲或不讲。

2.1　OSI 参考模型

在计算机网络产生之初，每个计算机厂商都有一套自己的网络体系结构，它们之间互不相容。为此，国际标准化组织（ISO）在 1979 年建立了一个分委员会来专门研究一种用于开放系统互联的体系结构（Open Systems Interconnection，OSI）。“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。这个分委员会提出了开放系统互联，即 OSI 参考模型，它定义了连接异种计算机的标准框架。

OSI 参考模型分为七层，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，图 2-1 所示为 OSI 参考模型及通信协议，其中 IMP 表示接口报文处理机(Interface Message Processor)。

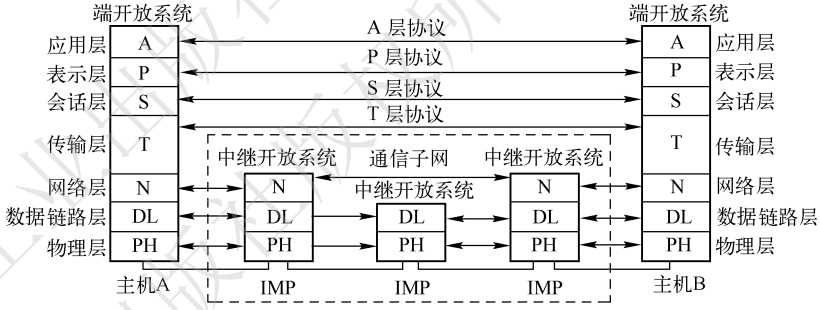

图 2-1　OSI 参考模型及通信协议

在这个 OSI 七层模型中，每一层都为其上一层提供服务，并为其上一层提供一个访问接口或界面。不同主机之间的相同层次称为对等层，如主机 A 中的表示层和主机 B 中的表示层互为对等层，主机 A 中的会话层和主机 B 中的会话层互为对等层。

对等层之间互相通信需要遵守一定的规则，如通信的内容、通信的方式，通常将其称为协议（Protocol）。

某个主机上运行的某种协议的集合称为协议栈，主机正是利用这个协议栈来接收和发送数据的。OSI 参考模型通过将协议栈划分为不同的层次，可以简化问题的分析、处理过程以及降低网络系统设计的复杂性。各层的主要功能及其相应的功能如下。

1. 物理层（Physical Layer）

要传递信息就要利用一些物理媒介，如双绞线、同轴电缆等，但具体的物理媒介并不在 OSI 的七层之内，有人把物理媒介当作第 0 层。物理层的任务就是为它的上一层提供一个物理

连接，以及它们的机械、电气、功能和过程特性，如规定使用电缆和接头的类型、传送信号的电压等。在这一层，数据还没有被组织，仅作为原始的比特流或电气电压处理，单位是比特。

2. 数据链路层（Data Link Layer）

数据链路层负责在两个相邻结点间的线路上，无差错地传送以帧为单位的数据。每一帧包括一定数量的数据和一些必要的控制信息。和物理层相似，数据链路层要负责建立、维持和释放数据链路的连接。在传送数据时，如果接收方检测到所传数据中有差错，就要通知发送方重发这一帧。

3. 网络层（Network Layer）

在计算机网络中进行通信的两个计算机之间可能会经过很多个数据链路，也可能还要经过很多通信子网。网络层的任务就是选择合适的网间路由和交换结点，确保数据及时传送。网络层将数据链路层提供的帧组成数据包，包中封装有网络层包头，其中含有逻辑地址信息，包括源站点和目的站点的网络地址。

4. 传输层（Transport Layer）

该层的任务是根据通信子网的特性最佳地利用网络资源，并以可靠和经济的方式，为两个端系统（也就是源站和目的站）的会话层之间，提供建立、维护和取消传输连接的功能，可靠地传输数据。在这一层，信息的传送单位是报文。

5. 会话层（Session Layer）

会话层也可以称为会晤层，在会话层及以上的高层中，数据传送的单位不再另外命名，统称为报文。会话层不参与具体的传输，它提供包括访问验证和会话管理在内的建立和维护应用之间通信的机制，如服务器验证用户登录便是由会话层完成的。

6. 表示层（Presentation Layer）

这一层主要解决用户信息的语法表示问题。它将欲交换的数据从适合于某一用户的抽象语法，转换为适合于 OSI 系统内部使用的传送语法，即提供格式化的表示和转换数据服务。数据的压缩和解压缩、加密和解密等工作都由表示层负责。

7. 应用层（Application Layer）

应用层确定进程之间通信的性质以满足用户需要，以及提供网络与用户应用软件之间的接口服务。

如图 2-2 所示，在 OSI 参考模型中，当一台主机需要传送用户的数据（DATA）时，数据首先通过应用层的接口进入应用层。在应用层，用户的数据被加上应用层的报头（Application Header，AH），形成应用层协议数据单元（Protocol Data Unit，PDU），然后被递交到下一层——表示层。

表示层并不“关心”上层——应用层的数据格式，而是把整个应用层递交的数据包看成是一个整体进行封装，即加上表示层的报头（Presentation Header，PH）。然后，递交到下一层——会话层。

同样，会话层、传输层、网络层、数据链路层也都要分别给上层递交下来的数据加上自己的报头。它们是：会话层报头（Session Header，SH）、传输层报头（Transport Header，TH）、网络层报头（Network Header，NH）和数据链路层报头（Data link Header，DH）。其中，数据链路层还要给网络层递交的数据加上数据链路层报尾（Data link Termination，DT），形成最终的一帧数据。

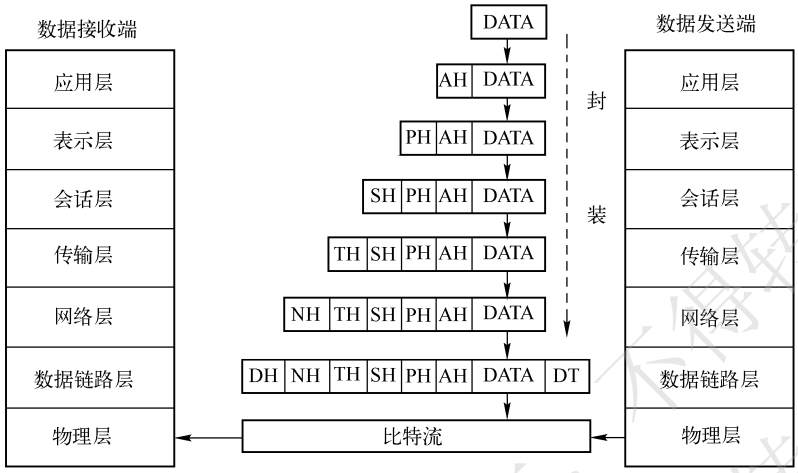

图 2-2　数据封装过程

当一帧数据通过物理层传送到目标主机的物理层时，该主机的物理层把它递交到上一层——数据链路层。数据链路层负责去掉数据帧的帧头部 DH 和尾部 DT，同时进行数据校验。如果数据没有出错，则递交到上一层，即网络层。

同样，网络层、传输层、会话层、表示层、应用层也要做类似的工作。最终，原始数据被递交到目标主机的具体应用程序中。

2.2　TCP/IP 参考模型

ISO 制定的 OSI 参考模型由于过于庞大、复杂招致了许多批评。与此对照，由技术人员自己开发的 TCP/IP 协议栈获得了更为广泛的应用。图 2-3 是 TCP/IP 参考模型和 OSI 参考模型的对比示意图。

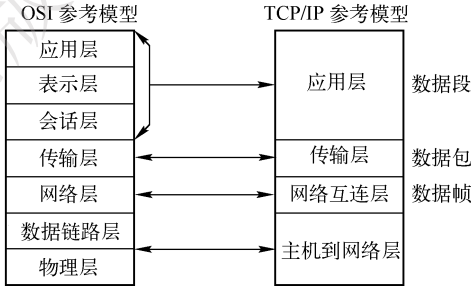

图 2-3　TCP/IP 参考模型

TCP/IP 协议栈是美国国防部高级研究计划局计算机网（Advanced Research Projects Agency Network，ARPANET）和其后继——因特网使用的参考模型。ARPANET 是由美国国防部赞助的研究网络。最初，它只连接了美国境内的四所大学。随后的几年中，它通过租用的电话线连接了数百所大学和政府部门。最终 ARPANET 发展成为全球规模最大的互连网

络——Internet。最初的 ARPANET 于 1990 年永久性地关闭。

TCP/IP 参考模型分为四个层次：应用层、传输层、网络互连层和主机到网络层，如图 2-4 所示。

<table>
<tr><td>应用层</td><td colspan="4">FTP、TELNET、HTTP</td><td>SNMP、TFTP、NTP</td></tr>
<tr><td>传输层</td><td colspan="4">TCP</td><td>UDP</td></tr>
<tr><td>网络互连层</td><td colspan="5">IP</td></tr>
<tr><td rowspan="2">主机到网络层</td><td rowspan="2">以太网</td><td rowspan="2">令牌环网</td><td>802.2</td><td colspan="2">HDLC、PPP、FRAME、RELAY</td></tr>
<tr><td>802.3</td><td colspan="2">EIA/TIA-232、449、V.35、V.21</td></tr>
</table>

图 2-4　TCP/IP 参考模型的层次结构

在 TCP/IP 参考模型中，去掉了 OSI 参考模型中的会话层和表示层（这两层的功能被合并到应用层实现）。同时将 OSI 参考模型中的数据链路层和物理层合并为主机到网络层。下面，分别介绍各层的主要功能。

1. 主机到网络层

实际上 TCP/IP 参考模型没有真正描述这一层的实现，只是要求能够提供给其上层——网络互连层一个访问接口，以便在其上传递 IP 分组。由于这一层未被定义，所以其具体的实现方法将随着网络类型的不同而不同。

2. 网络互连层

网络互连层是整个 TCP/IP 协议栈的核心，它的功能是把分组发往目标网络或主机。同时，为了尽快地发送分组，可能需要沿不同的路径同时进行分组传递。因此，分组到达的顺序和发送的顺序可能不同，这就需要上层对分组进行排序。

网络互连层定义了分组格式和协议，即 IP 协议（Internet Protocol）。网络互连层除了需要完成路由的功能外，也可以完成将不同类型的网络（异构网）互连的任务。除此之外，网络互连层还需要完成拥塞控制的功能。

3. 传输层

在 TCP/IP 模型中，传输层的功能是使源端主机和目标端主机上的对等实体可以进行会话。在传输层定义了两种服务质量不同的协议，即传输控制协议（Transmission Control Protocol，TCP）和用户数据报协议（User Datagram Protocol，UDP）。

TCP 协议是一个面向连接的、可靠的协议。它将一台主机发出的字节流无差错地发往互联网上的其他主机。在发送端，它负责把上层传送下来的字节流分成报文段并传递给下层；在接收端，它负责把收到的报文进行重组后递交给上层。TCP 协议还要处理端到端的流量控制，以避免缓慢接收的接收方没有足够的缓冲区接收发送方发送的大量数据。

UDP 协议是一个不可靠的、无连接协议，主要适用于不需要对报文进行排序和流量控制的场合。

4. 应用层

TCP/IP 模型将 OSI 参考模型中的会话层和表示层的功能合并到应用层实现。应用层面

向不同的网络应用引入了不同的应用层协议。其中，有基于 TCP 协议的，如文件传输协议（File Transfer Protocol，FTP）、虚拟终端协议（TELNET）、超文本链接协议（Hyper Text Transfer Protocol，HTTP）；也有基于 UDP 协议的，如 SNMP 协议等。

2.3 常用的网络服务

网络上的服务很多，这里介绍常用的四个服务，即 Web 服务、FTP 服务、E-Mail 服务和 Telnet 服务。

2.3.1 Web 服务

Web 服务也称为 WWW（World Wide Web）服务，主要功能是提供网上信息浏览服务。WWW 也可以简称为 Web，中文名字为“万维网”，它起源于 1989 年 3 月，是由欧洲量子物理实验室（CERN）所开发出来的主从结构分布式超媒体系统。通过万维网，人们只要通过简单的方法，就可以很迅速方便地取得丰富的信息资料。由于用户在通过 Web 浏览器访问信息资源的过程中，无需关心一些技术性的细节，而且界面非常友好，因而 Web 在 Internet 上一推出就受到了热烈的欢迎，并迅速得到了爆炸性的发展。图 2-5 所示为采用 WWW 方式浏览新浪网页。

图 2-5 新浪网页

在 UNIX 和 Linux 平台下使用最广泛的免费 Web 服务器是 W3C、NCSA 和 Apache 服务器，而 Windows 平台使用 IIS 的 Web 服务器。选择 Web 服务器应考虑的本身特性因素有：性能、安全性、日志和统计、虚拟主机、代理服务器、缓冲服务和集成应用程序等。下面介绍几种常用的 Web 服务器。

1. Microsoft IIS

Microsoft 的 Web 服务器产品为 Internet Information Server（IIS），IIS 是允许在公共 Intranet 或 Internet 上发布信息的 Web 服务器。IIS 是目前最流行的 Web 服务器产品之一，很多著名的网站都建立在 IIS 平台上。IIS 提供了一个图形界面的管理工具，称为 Internet 服务管理器，可用于监视、配置和控制 Internet 服务。图 2-6 所示为微软的 IIS 服务。

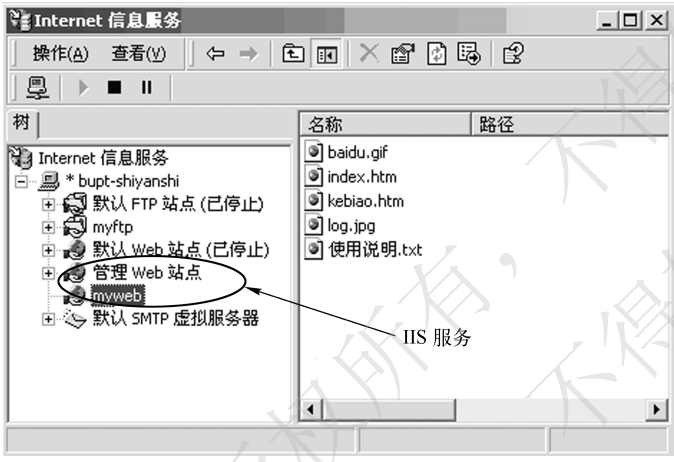

图 2-6　微软的 IIS 服务

IIS 是一种 Web 服务组件，其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面，它使得在网络（包括互联网和局域网）上发布信息成了一件很容易的事情。它提供 ISAPI（Intranet Server API）作为扩展 Web 服务器功能的编程接口；同时，它还提供一个 Internet 数据库连接器，可以实现对数据库的查询和更新。

2. IBM WebSphere

WebSphere Application Server 是一种功能完善、开放的 Web 应用程序服务器，是 IBM 电子商务计划的核心部分，它基于 Java 的应用环境，用于建立、部署和管理 Internet 和 Intranet Web 应用程序。这一整套产品进行了扩展，以适应 Web 应用程序服务器的需要，范围从简单、高级直到企业级。

WebSphere 针对以 Web 为中心的开发人员，他们都是基于 HTTP 服务器和 CGI 编程技术成长起来的。IBM 提供 WebSphere 产品系列，通过提供综合资源、可重复使用的组件、功能强大并易于使用的工具，以及支持 HTTP 和 IIOP 通信的可伸缩运行时环境，帮助这些用户从简单的 Web 应用程序转移到电子商务世界。

3. BEA WebLogic

BEA WebLogic Server 是一种多功能、基于标准的 Web 应用服务器，为企业构建自己的应用提供了坚实的基础。各种应用开发、部署等所有关键性的任务，无论是集成各种系统和数据库，还是提交服务、跨 Internet 协作，起始点都是 BEA WebLogic Server。由于它具有全面的功能、对开放标准的遵从性、多层架构、支持基于组件的开发，所以基于 Internet 的企业都选择它来开发、部署最佳的应用。图 2-7 为 WebLogic 的管理界面。

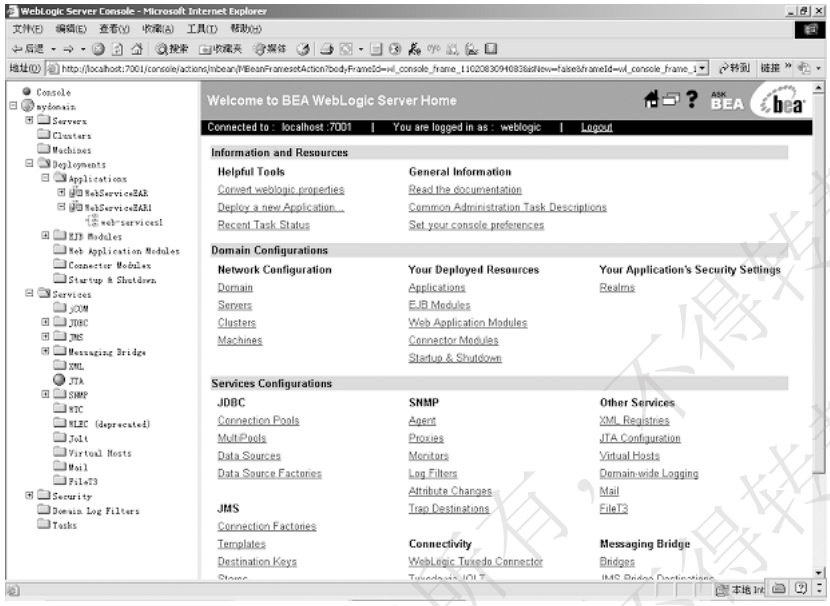

图 2-7　WebLogic 管理界面

BEA WebLogic Server 在作为企业应用架构的基础方面继续处于领先地位。BEA WebLogic Server 为构建集成化的企业级应用提供了稳固的基础，它们以 Internet 为基础，在联网的企业之间共享信息、提交服务，实现协作自动化。

4. Apache

Apache 是世界上用得最多的 Web 服务器，市场占有率达 60%左右。它源于 NCSA httpd 服务器，当 NCSA WWW 服务器项目停止后，那些使用 NCSA WWW 服务器的人们开始交换用于此服务器的补丁，这也是 Apache 名称的由来（a patchy）。世界上很多著名的网站都是 Apache 的产物，它的成功之处主要在于它的源代码开放、有一支开放的开发队伍、支持跨平台的应用（可以运行在几乎所有的 UNIX、Windows、Linux 系统平台上）以及它的可移植性等。图 2-8 所示为 Windows 下 Apache 服务启动后的界面。

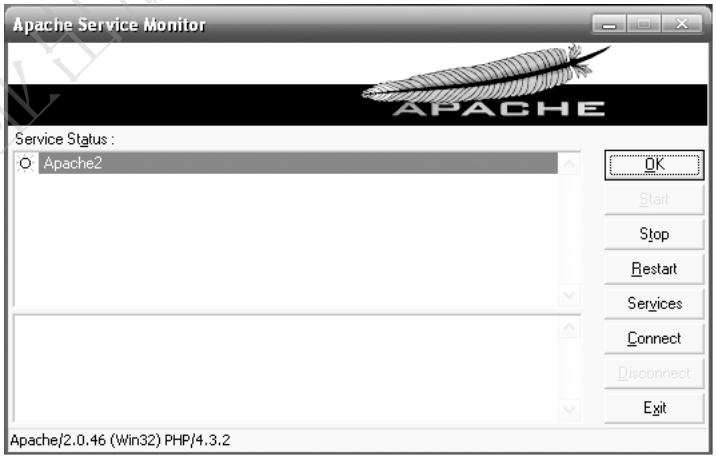

图 2-8　Windows 下 Apache 界面

5. Tomcat

Tomcat 是一个开放源代码、运行 Servlet 和 JSP Web 应用软件的基于 Java 的 Web 应用软件容器。Tomcat Server 是根据 Servlet 和 JSP 规范进行执行的，因此可以说 Tomcat Server 也实行了 Apache-Jakarta 规范且比绝大多数商业应用软件服务器要好。Tomcat 的 Logo 如图 2-9 所示。

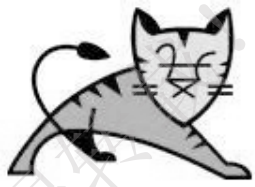

图 2-9　Tomcat 的 Logo

Tomcat 是 Java Servlet 和 JavaServer Pages 技术的标准实现，是基于 Apache 许可证下开发的自由软件。Tomcat 是完全重写的 Servlet API 和 JSP 兼容的 Servlet/JSP 容器。Tomcat 使用了 JavaServlet 的一些代码，特别是 Apache 服务适配器。随着 Catalina Servlet 引擎的出现，Tomcat 的性能得到提升，使得它成为一个颇具竞争力的 Servlet/JSP 容器，因此目前许多 Web 服务器都是采用 Tomcat。

2.3.2　FTP 服务

FTP（File Transfer Protocol）是文件传输协议的简称。正如其名所示，FTP 的主要作用就是让用户连接上一个远程计算机（这些计算机上运行着 FTP 服务器程序），查看远程计算机有哪些文件，然后把文件从远程计算机上复制到本地计算机，或把本地计算机的文件传送到远程计算机上。

FTP 协议是 Internet 文件传送的基础，它由一系列规格说明文档组成，目标是提高文件的共享性，提供非直接使用远程计算机，使存储介质对用户透明和可靠高效地传送数据。简单地说，FTP 就是完成两台计算机之间的复制，从远程计算机复制文件至自己的计算机上，称之为“下载（download）”文件。若将文件从自己计算机中复制到远程计算机上，则称之为“上载（upload）”文件。在 TCP/IP 协议中，FTP 标准命令 TCP 端口号为 21，Port 方式数据端口号为 20。

FTP 支持两种模式，一种方式叫作 Standard（也就是 Port——主动方式），一种是 Passive（也就是 PASV——被动方式）。Standard 模式 FTP 的客户端发送 PORT 命令到 FTP 服务器；Passive 模式 FTP 的客户端发送 PASV 命令到 FTP 服务器。

常用的 FTP 工具有很多，如 CuteFTP、LeapFTP、FlashFXP、TurboFTP、ChinaFTP、AceFTP 等。CuteFTP 5.0 界面如图 2-10 所示。

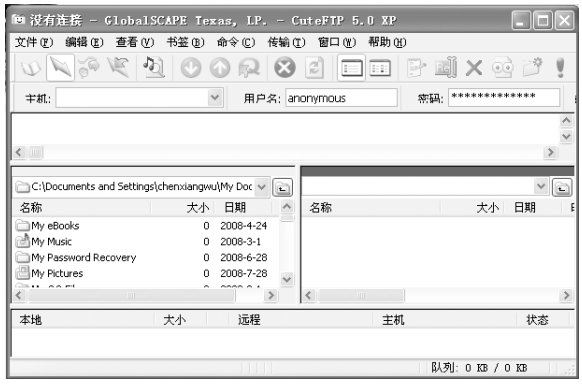

图 2-10　CuteFTP 5.0 界面

另外，微软也提供 FTP 服务，如图 2-11 所示。

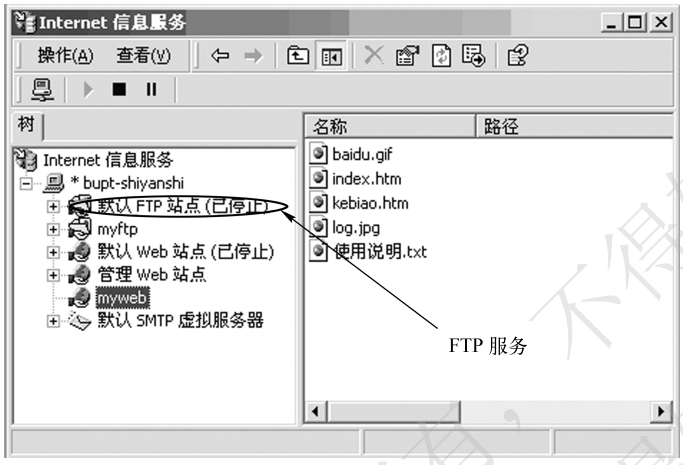

图 2-11　微软的 FTP 服务

2.3.3　电子邮件服务

电子邮件是 Internet 应用最广的服务。通过网络的电子邮件系统，可以用非常低廉的价格（不管发送到哪里，都只需负担电话费和网费），以非常快速的方式（几秒钟之内可以发送到世界上任何指定的目的地），与世界上任何一个角落的网络用户联系，这些电子邮件可以是文字、图像、声音等各种方式。同时，您可以得到大量免费的新闻、专题邮件，并实现轻松的信息搜索。这是任何传统的方式无法相比的。正是由于电子邮件的使用简易、投递迅速、收费低廉、易于保存、全球畅通无阻等特性，使得电子邮件被广泛地应用，它使人们的交流方式得到了极大的改变。

每一个申请 Internet 账户的用户都会有一个电子邮件地址，它是一个类似于用户家门牌号码的邮箱地址，或者更准确地说，相当于在邮局租用了一个信箱。传统的信件是由邮递员送到用户家门口，而电子邮件则需要自己去查看信箱，只是用户不用跨出家门一步。

电子邮件地址的典型格式是 abc@ xyz，这里@ 之前是用户选择代表本人的字符组合或代码，@ 之后是为用户提供电子邮件服务的服务商名称，如 lijian@ sina. com。常用的邮件系统包括 Outlook Express（如图 2-12 所示）和 Foxmail（如图 2-13 所示）等。

电子邮件不同于普通的信件，它的工作原理不像传统信件的传输那样仅仅需要火车或飞机就够了。但是，电子邮件的工作原理又和传统邮件的处理流程有相似之处。

首先，当将 E-mail 输入计算机开始发送时，计算机会将信件“打包”，送到所属服务商的邮件服务器（发信的邮局即为“SMTP 邮件服务器”，收信的邮局即为“POP3 邮件服务器”）上，这就相当于平时将信件投入邮筒后，邮递员把信从邮筒中取出来并按照地区分类。Foxmail 软件上的邮件服务器的设置如图 2-14 所示，Outlook 软件上邮件服务器的设置如图 2-15 所示。

图 2-12　Outlook Express 邮件系统

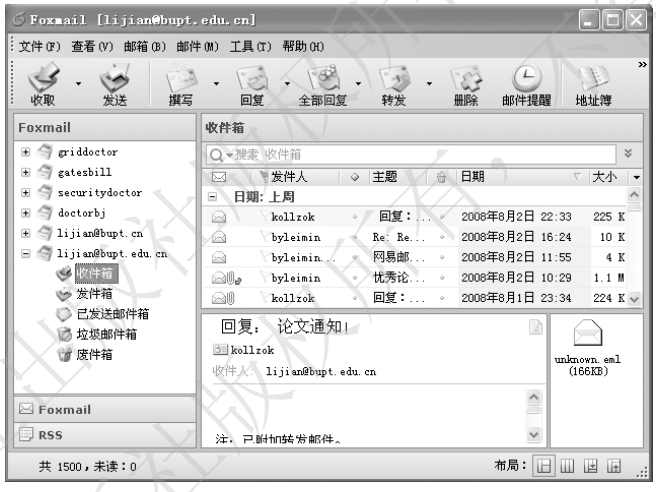

图 2-13　Foxmail 邮件系统

图 2-14　Foxmail 中的 SMTP 和 POP3 设置

图 2-15　Outlook 中的 SMTP 和 POP3 设置

然后，邮件服务器根据收件人地址，按照当前网上传输的情况，寻找一条最不拥挤的路径，将信件传送到下一个邮件服务器。接着，这个服务器也如法炮制，将信件往下传送。这一步相当于邮局之间的转信，即当邮件被分类以后，由始发地邮局运往目的地的省会邮局，然后由省会邮局转给下一级的地区邮局，这样层层向下传递，最终到达用户手中。

最后，E-mail 被传送到用户服务商的服务器上，保存在服务器上的用户 E-mail 信箱中。用户个人终端计算机通过与服务器的连接从其信箱中读取自己的 E-mail。这一步相当于信件已经被传送到了用户的个人信箱中，用户拿钥匙打开信箱就可以读取信件了。

2.3.4　Telnet 服务

Telnet 是 TCP/IP 网络的登录和仿真程序，它最初是由 ARPANET 开发的，现在主要用于 Internet 会话。Telnet 的基本功能是允许用户登录进入远程主机系统。起初，Telnet 只是让用户的本地计算机与远程计算机连接，从而成为远程主机的一个终端。Telnet 的应用方便了用户进行远程登录，但也给黑客们提供了又一种入侵手段和后门。图 2-16 所示为在 DOS 下使用 Telnet 进行登录。

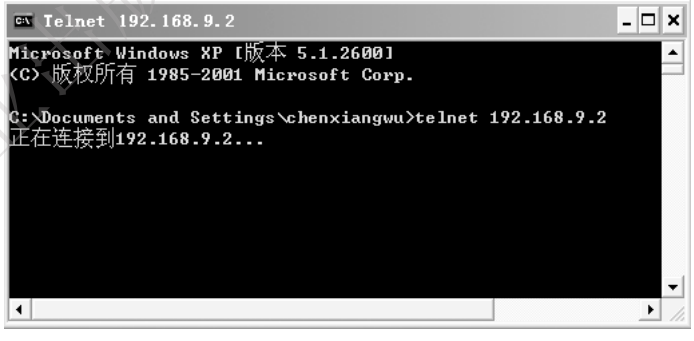

图 2-16　在 DOS 下使用 Telnet 进行登录

使用 Telnet 协议进行远程登录时需要满足以下条件：在本地计算机上必须装有包含 Telnet 协议的客户程序；必须知道远程主机的 IP 地址或域名；必须知道登录标识与口令。Telnet 远程登录服务分为以下 4 个过程：

1）本地与远程主机建立连接。该过程实际上是建立一个 TCP 连接，用户必须知道远程主机的 IP 地址或域名。

2）将本地终端上输入的用户名和口令，以及以后输入的任何命令或字符以 NVT（Net Virtual Terminal）格式传送到远程主机。该过程实际上是从本地主机向远程主机发送一个 IP 数据包。

3）将远程主机输出的 NVT 格式的数据转化为本地所接受的格式送回本地终端，包括输入命令回显和命令执行结果。

4）最后，本地终端对远程主机进行撤销连接，该过程是撤销一个 TCP 连接。

2.4 常用的网络命令

Windows 是从简单的 DOS 字符界面发展而来的，虽然平时在使用 Windows 操作系统的时候，主要是对图形界面进行操作，但是 DOS 命令仍然非常有用，特别是在计算机安全故障诊断与排除过程中，这些命令就显得更为重要。本节介绍这些命令的功能，同时学习如何使用这些命令的技巧。

2.4.1 ping 命令

ping 是 DOS 命令，一般用于检测网络是否通畅以及网络连接速度，其结果值越大，说明速度越慢。ping 发送一个 ICMP 回声请求消息给目的地，并报告是否收到所希望的 ICMP 回声应答，它使用网络层的 ICMP 协议。

对一个网络管理员或者黑客来说，ping 命令是第一个必须掌握的 DOS 命令，它所利用的原理是这样的：网络上的机器都有唯一确定的 IP 地址，给目标 IP 地址发送一个数据包，对方就要返回一个同样大小的数据包，根据返回的数据包可以确定目标主机的存在，可以初步判断目标主机的操作系统和连接对方主机的速度等。下面是 ping 命令一些常用的使用方法。

1. ping IP

例如 ping 127.0.0.1，如图 2-17 所示。

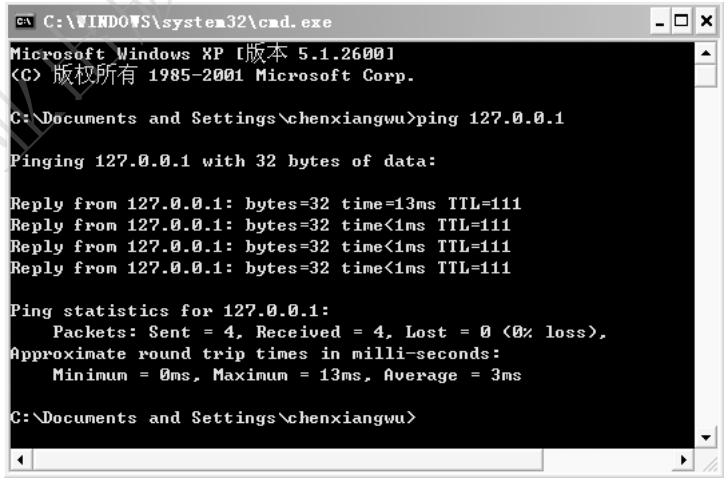

图 2-17　ping IP 命令的使用

2. ping URL

如 ping www. sina. com. cn，如图 2−18 所示。

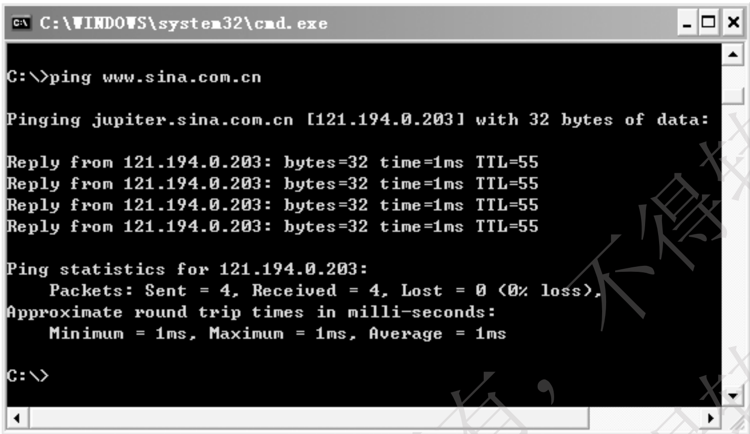

图 2−18　ping 新浪网站

3. ping IP-t

连续对 IP 地址执行 ping 命令，直到被用户以〈Ctrl+C〉键中断。例如 ping 127. 0. 0. 1-t，如图 2−19 所示。中断如图 2−20 所示。

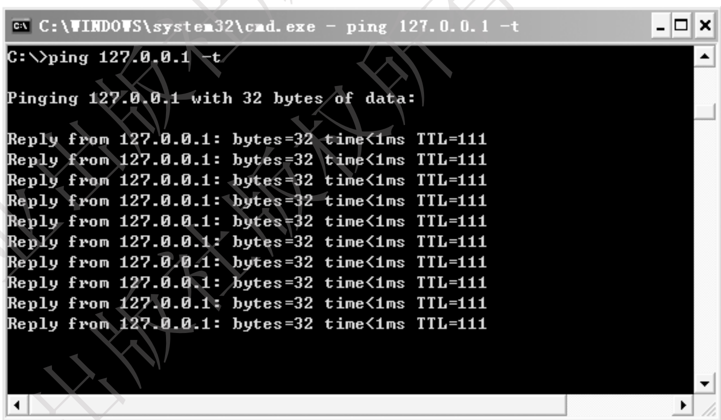

图 2−19　使用 ping IP-t 命令

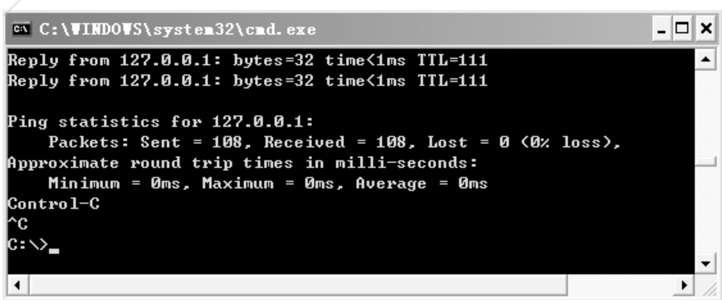

图 2−20　使用〈Ctrl+C〉键中断 ping IP-t 命令

4. ping IP-l 3000

指定 ping 命令中的数据长度为 3000 字节，而不是默认的 32 字节。该命令的使用如图 2-21 所示。

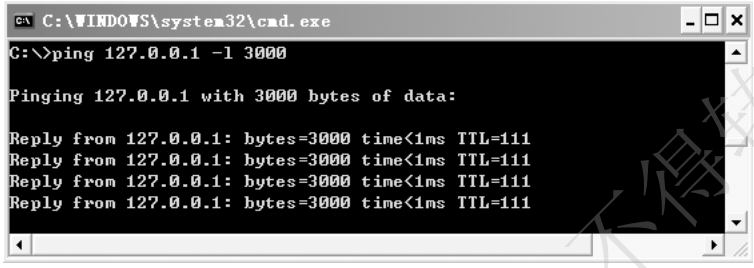

图 2-21　使用 ping IP-l 3000 命令

5. ping IP-n count

执行特定次数（count 次）的 ping 命令。图 2-22 所示为执行 100 次的 ping 命令。

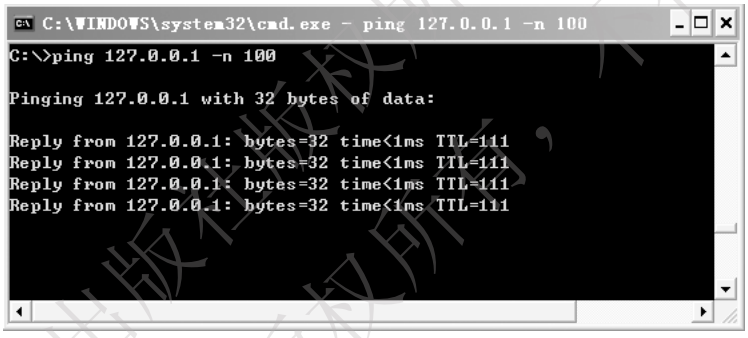

图 2-22　执行 100 次的 ping 命令

2.4.2　ipconfig 命令

ipconfig 可用于显示当前的 TCP/IP 配置的设置值，这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。如果计算机和所在的局域网使用了动态主机配置协议（DHCP），这个程序所显示的信息会更加实用。这时，ipconfig 可以了解自己的计算机是否成功地租用到一个 IP 地址，如果租用到则可以了解它目前分配到的是什么地址。了解计算机当前的 IP 地址、子网掩码和默认网关实际上是进行测试和故障分析的必要项目。ipconfig 最常用的使用方法如下。

1. ipconfig

当使用 ipconfig 不带任何参数选项时，它为每个已经配置了的接口显示 IP 地址、子网掩码和默认网关值。如图 2-23 所示，显示的 IP 地址为 59.64.158.190，子网掩码为 255.255.255.0，默认网关为 59.64.156.1。

2. ipconfig /all

当使用 all 参数时，ipconfig 能为 DNS 和 WINS 服务器显示它已经配置、所要使用的附加信息（如 IP 地址等），并且显示内置于本地网卡中的物理地址（MAC）。如果 IP 地址是从

DHCP 服务器租用的，ipconfig 将显示 DHCP 服务器的 IP 地址和租用地址预计失效的日期。图 2-24 所示为 ipconfig /all 命令的使用。

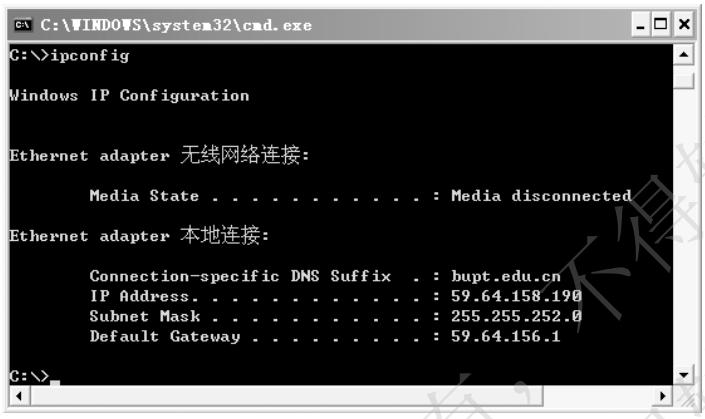

图 2-23　ipconfig 命令的使用

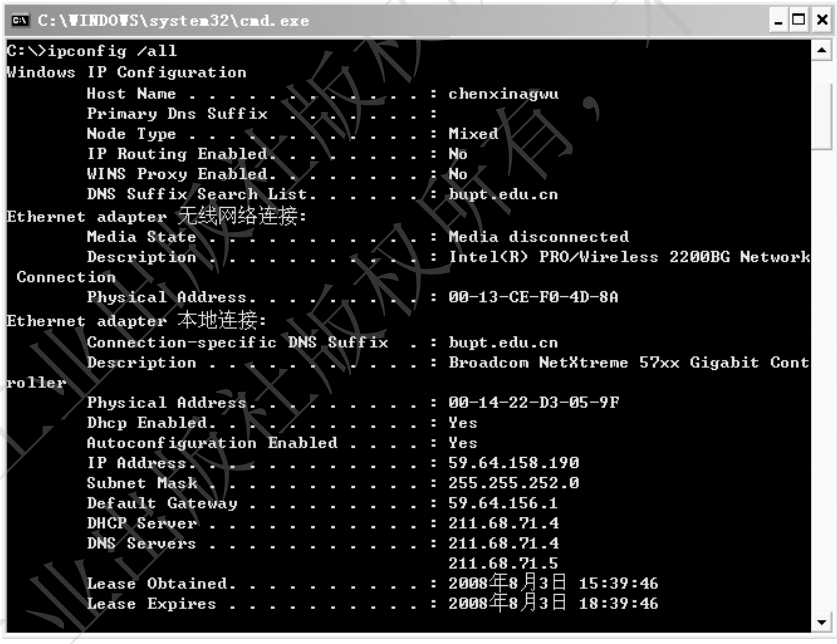

图 2-24　ipconfig /all 命令的使用

2.4.3　netstat 命令

netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。最常见的使用方法如下。

1. netstat-a

本选项显示一个所有的有效连接信息列表，包括已建立的连接（ESTABLISHED），也包括监听连接请求（LISTENING）的那些连接，如图 2-25 所示。

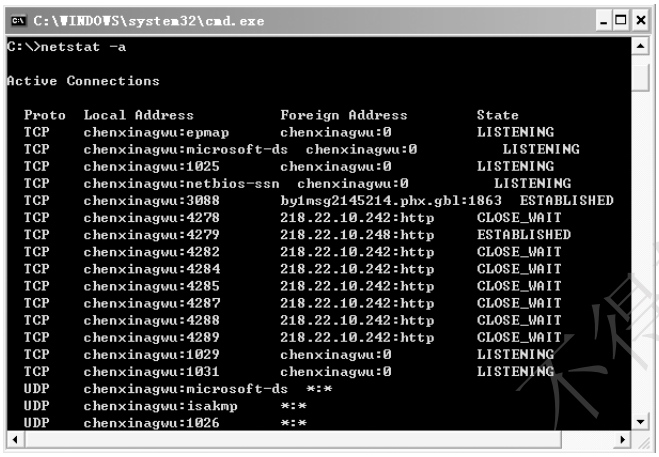

图 2-25　netstat-a 命令

2. netstat-n

本选项显示所有已建立的有效连接，如图 2-26 所示。

图 2-26　netstat-n 命令

3. netstat-r

本选项可以显示关于路由表的信息，类似于后面所讲的使用 route print 命令时看到的信息。除了显示有效路由外，还显示当前有效的连接，如图 2-27 所示。

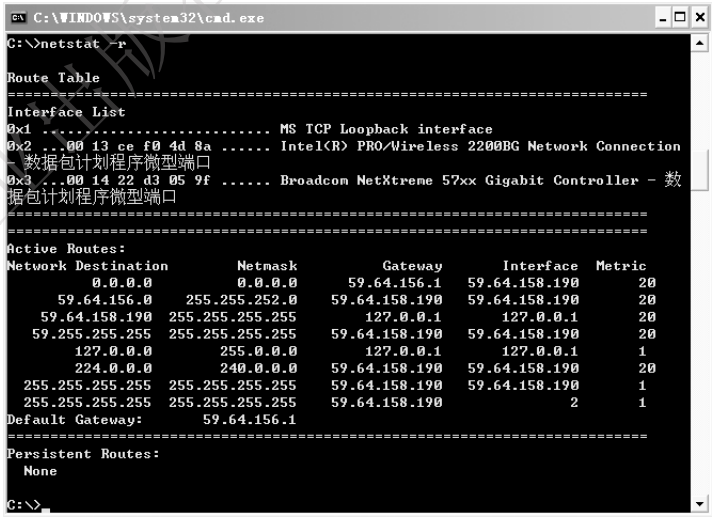

图 2-27　netstat-r 命令

这些命令也可以一起使用，如 netstat-an，如图 2-28 所示。

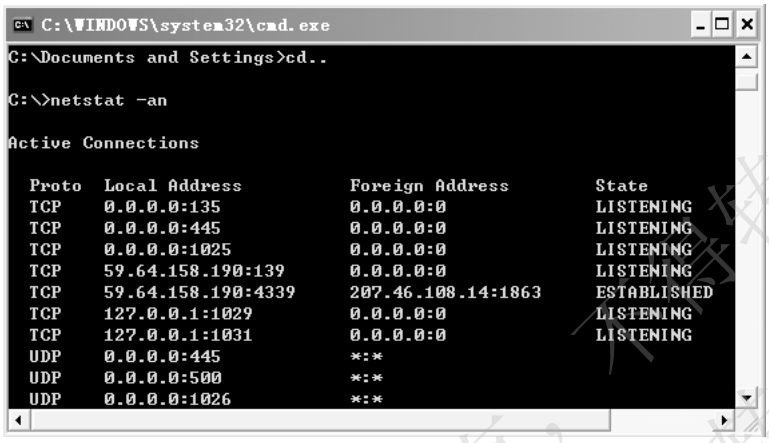

图 2-28　netstat-an 命令

2.4.4　arp 命令

arp 是地址转换协议的意思，它也是一个重要的命令，用于确定对应 IP 地址的网卡物理地址。用 arp 命令，能够查看本地计算机或另一台计算机的 arp 高速缓存中的当前内容。此外，也可以使用 arp 命令用人工方式输入静态的网卡物理/IP 地址对，通常会使用这种方式为默认网关和本地服务器等常用主机进行设置，这样有助于减少网络上的信息量。最常见的使用方法为 arp-a 或 arp-g 这种形式，用于查看高速缓存中的所有项目，-a 和-g 参数的执行结果是一样的。如图 2-29 所示，可以看到 IP 地址和物理地址。

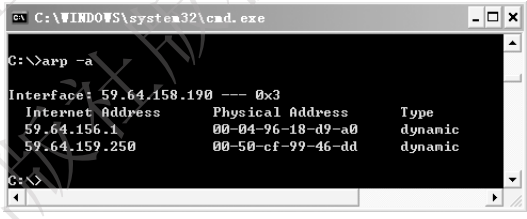

图 2-29　arp-a 命令

2.4.5　net 命令

net 命令有很多函数用于核查计算机之间的 NetBIOS 连接，可以查看管理网络环境、服务、用户、登录等信息内容。关于 net 命令的使用参数也很多，如 net view、net user、net use、net time、net start、net share、net print、net name、net group、net computer、net accounts 等。最常见的使用方法如下。

1. net share

它的作用是用来创建、删除或显示共享资源。如图 2-30 所示为查看系统中的共享资源，图中显示了一个 IPC $ 空连接共享。

图 2-30 net share 命令的使用

2. net start

它的作用是启动服务，或显示已启动服务的列表。命令格式为 net start，如图 2-31 所示。

图 2-31 net start 命令的使用

2.4.6 at 命令

at 命令是 Windows 系列操作系统中内置的命令。at 命令可在指定时间和日期、在指定计算机上运行命令和程序。单击“开始”→“运行”，在出现的 DOS 提示符下面输入 at 命令。下面就来看看 at 命令的一些实例分析。

1. 定时关机

命令：at 22：00 ShutDown-S-T40

该命令运行后，到了 22：00，计算机会出现“系统关机”对话框，并默认 40 s 延时自动关机。

2. 定时提醒

命令：at 11：00 net send 10.10.36.122“与朋友约会的时间到了，快点准备出发吧！”

其中 net send 是 Windows 内部程序，可以发送消息到网络上的其他用户、计算机。10.10.36.122 是本机的 IP 地址。这个功能在 Windows 中也称作“信使服务”。

3. 自动运行批处理文件

如果公司的数据很重要，要求在指定的日期/时间进行备份，那么运行：

命令：at 2：00 AM /Every：Saturday BackUp. bat

这样，在每个周六的早上 2：00，计算机定时启动 BackUp. bat 批处理文件。BackUp. bat 是一个自行编制的批处理文件，它包含能对系统进行数据完全备份的多条命令。

4. 取消已经安排的计划

命令：at 5 /delete

有时候，已经安排好的计划可能临时变动，这样可以及时地用上述命令删除该计划（5 为指派给已计划命令的标识编号），当然，删除该计划后，可以重新安排。

at 是 Windows 2000/XP/NT 当中的命令，然而在入侵当中是一个不可缺少的一项服务，它可以让某一个程序在一定的时间里自动执行，从而操控计算机。下面介绍它的几个实际用法，假设 hacker · exe 是一个程序。

1）如果想让对方在指定时间里启动某个程序，可在命令行里输入

At \\127. 0. 0. 1 23：00 c：\winnt \system32 /hacker. exe

提示：新加了一份作业，作业 id = 1。

2）让对方的计算机在每周一和周二的 23：00 启动某个程序，那么可以输入

At \\127. 0. 0. 1 23：00 /every：一，二 c：\winnt \system32 \hacker. exe

提示：新加了一份作业，作业 id = 2。

3）删除对方计算机上作业 id 为 1 的任务

At \\127. 0. 0. 1 1 /delete /yes

4）删除所有的任务

At \\127. 0. 0. 1 /delete

提示：是否要删除所有的操作？然后输入 Y。

2. 4. 7 tracert 命令

tracert 命令显示用于将数据包从计算机传递到目标位置的一组 IP 路由器，以及每个跃点所需的时间。如果数据包不能传递到目标，tracert 命令将显示成功转发数据包的最后一个路由器。当数据包从计算机经过多个网关传送到目的地时，tracert 命令可以用来跟踪数据包使用的路由（路径）。该实用程序跟踪的路径是源计算机到目的计算机的一条路径，不能保证或认为数据包总遵循这个路径。如果配置使用 DNS，那么常常会从所产生的应答中得到城市、地址和常见通信公司的名字。tracert 是一个运行得比较慢的命令（如果指定的目标地址比较远），每个路由器大约需要给它 15 s。如果有网络连通性问题，可以使用 tracert 命令来检查到达目标 IP 地址的路径并记录结果。tracert 命令最常见的使用方法如下。

1. tracert IP 或 tracert URL

该命令返回到达 IP 地址所经过的路由器列表，URL 表示网址。图 2-32 所示为本机到新浪网的所有路由器列表。

2. tracert IP-d 或 tracert URL-d

通过使用-d 选项，将更快地显示路由器路径，因为 tracert 不会尝试解析路径中路由器的名称。图 2-33 所示为 tracert IP-d 命令的使用。

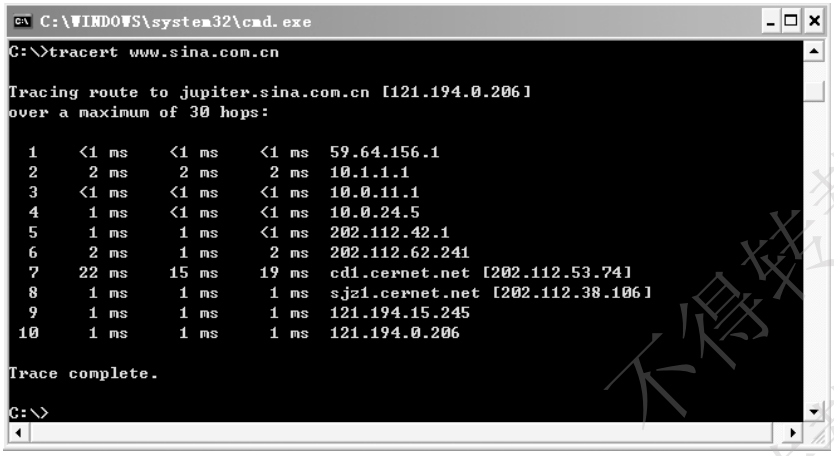

图 2-32　本机到新浪网的路由器列表

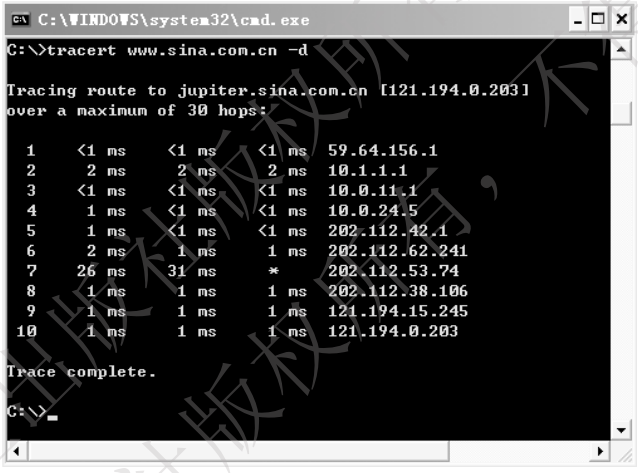

图 2-33　tracert IP-d 命令的使用

tracert 一般用来检测故障的位置，即检查在哪个环节上出了问题。

2.4.8　route 命令

route 命令是用来显示、添加和修改路由表项的。route 命令最常见的使用方法如下。

1. route print

该命令用于显示路由表中的当前项目，在单路由器网段上的输出；由于用 IP 地址配置了网卡，因此所有的这些项目都是自动添加的。如图 2-34 所示为 route print 命令的使用。

2. route add

使用该命令，可以将路由项目添加给路由表。例如，要设定一个到目的网络 219.98.32.33 的路由，其间要经过 5 个路由器网段，首先要经过本地网络上的一个路由器，其 IP 地址为 202.97.123.5，子网掩码为 255.255.255.224，那么应该输入以下命令：

route add 219.98.32.33 mask 255.255.255.224 202.97.123.5 metric 5

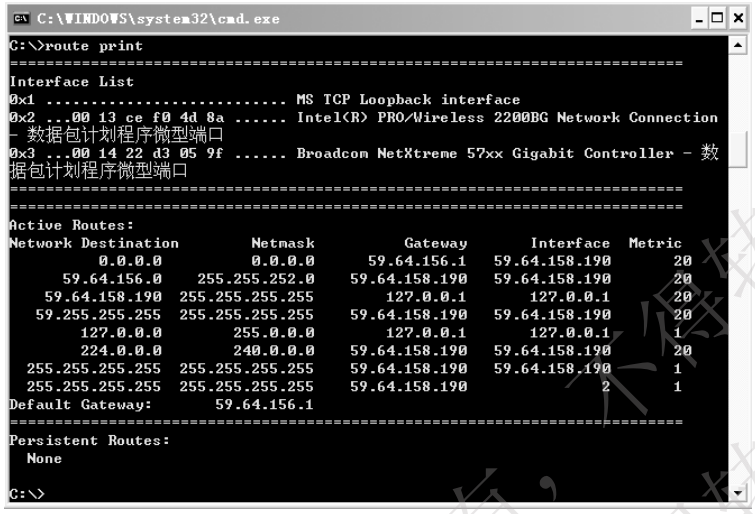

图 2-34　route print 命令

3. route change

可以使用该命令来修改数据的传输路由，但不能使用它来改变数据的目的地。下面这个例子可以将数据的路由改到另一个路由器，它采用一条包含 3 个网段的路径：

route change 219. 98. 32. 33 mask 255. 255. 255. 224 202. 97. 123. 250 metric 3

4. route delete

使用该命令可以从路由表中删除路由。例如：

route delete 219. 98. 32. 33

2. 4. 9　nbtstat 命令

可以使用 nbtstat 命令释放和刷新 NetBIOS 名称。nbtstat 用于提供关于 NetBIOS 的统计数据。运用 NetBIOS，可以查看本地计算机或远程计算机上的 nbtetBIOS 名称表格。nbtstat 命令最常见的使用方法如下。

1. nbtstat-n

该命令显示寄存在本地的名称和服务程序。图 2-35 所示为 nbtstat-n 命令的使用。

图 2-35　nbtstat-n 命令的使用

2. nbtstat-c

该命令用于显示 NetBIOS 名称高速缓存中的内容。NetBIOS 名称高速缓存用于存放与本计算机最近进行通信的其他计算机的 NetBIOS 名称和 IP 地址对。图 2-36 所示为 nbtstat-c 命令的使用。

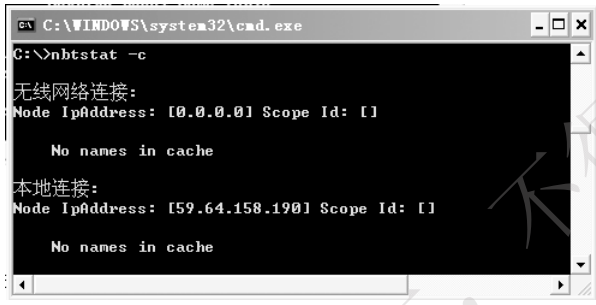

图 2-36　nbtstat-c 命令的使用

3. nbtstat-r

该命令用于清除和重新加载 NetBIOS 名称高速缓存。图 2-37 所示为 nbtstat-r 命令的使用。

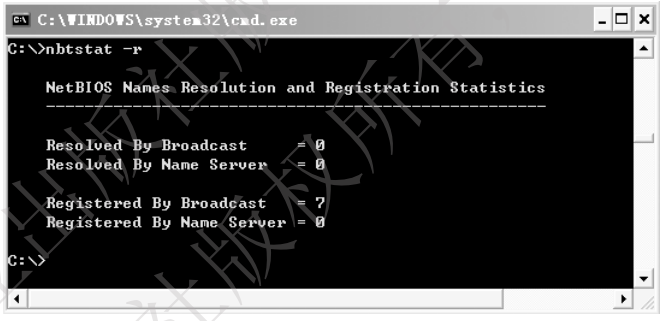

图 2-37　nbtstat-r 命令的使用

4. nbtstat-a IP

该命令通过 IP 显示另一台计算机的物理地址和名称列表，所显示的内容就像对方计算机自己运行 nbtstat-n 一样。

2.5　习题

1. 什么是计算机网络的 OSI 参考模型？它的主要内容是什么？
2. 什么是计算机网络的 TCP/IP 参考模型？它的主要内容是什么？
3. 什么是 Web 服务？
4. 什么是电子邮件服务？
5. 说明 ping 命令的作用是什么，常用的使用方法有哪些。
6. 说明 tracert 命令的作用是什么，常用的使用方法有哪些。

第 3 章　网络扫描与监听

本章主要讲述黑客攻击过程中扫描与监听的相关知识。扫描和监听是黑客攻击一个目标之前必须要做的事情。

3.1　黑客

本小节先介绍黑客的相关概念，然后介绍与之相关的一些红客、蓝客与骇客概念与区别。

3.1.1　黑客的概念

很多人经常说计算机被“黑”了，其实是电脑被黑客攻击了的意思。黑客是一个中文词语，源自英文 hacker。它泛指擅长 IT 技术的人群、计算机科学家，大部分的媒体习惯将“黑客”指作计算机入侵者。在信息安全领域黑客指的是研究智取计算机安全系统的人员。利用公共网路，如互联网、电话网络系统等，在未经授权许可的情况下，进入对方系统被称为黑帽黑客（英文：black hat，另称 cracker）；研究和分析计算机安全系统的称为白帽黑客（英语：white hat）。

很多人感受黑客的魅力是从 1995 年美国电影《Hackers》开始的。电影中达德是一名出色的天才黑客。曾经股市因为 11 岁的他的小小恶作剧而差点崩盘，达德因此被剥夺了使用网络的权利。后来成年的达德终于重新获得了这一权利，跃跃欲试的他摩拳擦掌，准备在网络上重新大展拳脚。凯特和乔伊都是如同达德一样的黑客，他们因为趣味相投而走到了一起成为好友。另一方面，普拉格曾经是一名技术高超的超级黑客，后来成为一家大公司的系统安全专家。背地里普拉格和黑恶势力勾结，谋取公司账户里的巨额财产。此外，他还发明了一种能令全球网络陷入瘫痪的可怕病毒。一次偶然中，达德一行人发现了普拉格的罪恶和阴谋，他们决定利用自己的力量，阻止普拉格……。感兴趣的同学可以在网上观看这部电影，以加深对电脑黑客的了解。

3.1.2　红客、蓝客与骇客

黑客早期在美国的电脑界是带有褒义的。他们都是水平高超的电脑专家，尤其是程序设计人员，算是一个统称。下面介绍下红客、蓝客与骇客，很多人容易把他们搞混。

1）红客：维护自己国家利益的计算机高手，他们热爱自己的祖国、民族，极力地维护国家安全与尊严。

2）蓝客：信仰自由，提倡爱国主义的黑客，他们用自己的力量来维护网络的和平。

3）骇客：很多人经常把黑客跟骇客搞混，实际区别很大，骇客，是“Cracker”的音译，就是“破解者”的意思。骇客从事恶意破解商业软件、恶意入侵别人的网站等事务。其实黑客与骇客本质上都是相同的，都是闯入计算机系统/软件者。黑客和骇客并没有一个

十分明显的界限，且随着两者含义越来越模糊，其含义已经显得不那么重要了。

3.1.3 典型的黑客事件

凯文·米特尼克（Kevin DavidMitnick，1964 年美国洛杉矶出生），如图 3-1 所示。很多人称他为世界上“头号电脑黑客”。这位“知名人物”传奇的黑客经历足以令全世界为之震惊。1983 年，凯文·米特尼克因被发现使用一台大学里的电脑擅自进入今日互联网的前身 ARPA 网，并通过该网进入了美国五角大楼的电脑，而被判在加州的青年管教所管教了 6 个月。1988 年，凯文·米特尼克被执法当局逮捕，原因是他从公司网络上盗取了价值 100 万美元的软件，并造成了 400 万美元的损失。

图 3-1 凯文·米特尼克

1993 年，自称为“骗局大师”的组织将目标锁定为美国电话系统，这个组织成功入侵美国国家安全局和美利坚银行，他们建立了一个能绕过长途电话呼叫系统而侵入专线的系统。

1995 年，来自俄罗斯的黑客弗拉季米尔·列宁在互联网上上演了精彩的偷天换日，他是历史上第一个通过入侵银行电脑系统来获利的黑客，1995 年，他侵入美国花旗银行并盗走 1000 万美元。

1999 年，梅利莎病毒（Melissa）使世界上 300 多家公司的电脑系统崩溃，该病毒造成的损失接近 4 亿美金，它是首个具有全球破坏力的病毒，该病毒的编写者戴维·斯密斯在编写此病毒的时候年仅 30 岁。戴维·斯密斯被判处 5 年徒刑。

2008 年，一个全球性的黑客组织利用 ATM 欺诈程序在一夜之间从世界 49 个城市的银行中盗走了 900 万美元。他们攻破了银行系统，用各种奇技取得了数据库内的银行卡信息，并在 2008 年 11 月 8 日午夜，利用团伙作案从世界 49 个城市总计超过 130 台 ATM 机上提取了 900 万美元。最关键的是此案现在还没破案，甚至据说连一个嫌疑人都没有找到。

2009 年 7 月 7 日，韩国遭受有史以来最猛烈的一次攻击。韩国总统府、国会、国情院和国防部等国家机关，以及金融界、媒体和防火墙企业网站都受到了攻击。9 日，韩国国家情报院和国民银行网站无法被访问。韩国国会、国防部、外交通商部等机构的网站一度无法打开。这是韩国遭遇的有史以来最强的一次黑客攻击。

2013 年 3 月 11 日，国家互联网应急中心（CNCERT）的数据显示，2013 年 1 月 1 日至 2 月 28 日不足 60 天的时间里，境外 6747 台木马或僵尸网络控制服务器控制了中国境内 190 万余台主机；其中位于美国的 2194 台控制服务器控制了中国境内 128.7 万台主机。

目前，网上的攻击事件层出不穷。据不完全统计，全球有几十万个网站在介绍黑客知识。这不得不引起高度重视。

3.1.4 相关法律法规

多数黑客入侵别人的系统都是想获取系统里的账号、口令、密码等信息。2011 年 8 月 29 日，最高人民法院和最高人民检察院联合发布《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》。该司法解释规定，黑客非法获取支付结算、证券交易、期

货交易等网络金融服务的账号、口令、密码等信息 10 组以上，处 3 年以下有期徒刑等刑罚；获取上述信息 50 组以上，处 3 年以上 7 年以下有期徒刑。

3.2 网络扫描

网络扫描是确认网络上运行的主机工作的一个工具或系统。它的目的是对主机进行攻击，或是为了发现漏洞以进行网络安全评估。

网络扫描程序，如 ping 扫描和端口扫描，返回关于哪个 IP 地址映射有主机连接到因特网上、并是工作的，这些主机提供什么样的服务等信息。另一种扫描方法是反向映射，返回关于哪个 IP 地址上没有映射出活动的主机的信息，这使攻击者能假设出可行的地址。

扫描是攻击者情报搜集的步骤之一。攻击者开始创建一个大概的目标，包含一些信息如它的域名系统（DNS）、电子邮件服务器，还有 IP 地址范围。这些信息中大部分可以在线得到。在扫描时，攻击者找到了关于特定 IP 地址的信息，该 IP 地址可以通过因特网进行评估，如其操作系统、系统结构和每台计算机上的服务等情况。在列举阶段，攻击者搜集关于网络用户、工作组名称、路由表和简单网络管理协议等资料。

扫描的主要工作原理是通过向目标机器发送数据报文信息，然后根据目标机器的响应情况获得想要的信息。根据网络扫描目的的不同，扫描可以分为三种类型，即 IP 地址扫描、端口扫描和漏洞扫描。

3.2.1 地址与端口扫描

要想了解地址与端口扫描问题，就首先需要了解 TCP/IP 协议族相关原理，它是地址与端口扫描的基础。如图 3-2 所示为 IP 数据报文格式。图 3-3 所示为 TCP 数据报文格式。

图 3-2 IP 数据报文格式

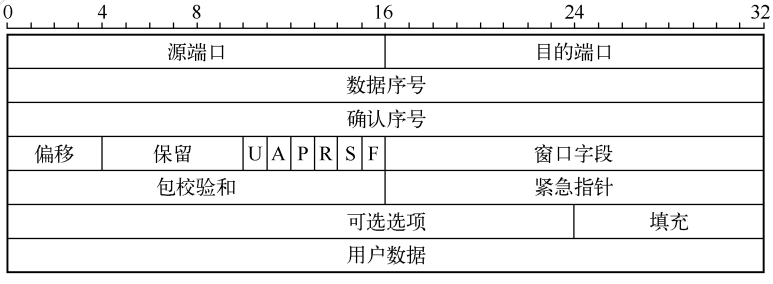

图 3-3 TCP 数据报文格式

IP 地址和端口被称作套接字，它代表一个 TCP 连接的一个连接端。为了获得 TCP 服务，必须在发送机的一个端口和接收机的一个端口之间建立连接。TCP 连接用两个连接端进行区别，也就是连接端 1、连接端 2，或叫发送端和接收端，也有叫客户端和服务器端。连接两端可以互相发送数据包。

一个 TCP 数据包包括一个 TCP 头，后面是选项和数据。一个 TCP 头包含 6 个标志位。它们的意义分别为：

1）SYN：标志位用来建立连接，让连接双方同步序列号。如果 SYN = 1 而 ACK = 0，则表示该数据包为连接请求，如果 SYN = 1 而 ACK = 1 则表示接受连接。

2）FIN：表示发送端已经没有数据要求传输了，希望释放连接。

3）RST：用来复位一个连接。RST 标志置位的数据包称为复位包。一般情况下，如果 TCP 收到的一个分段明显不是属于该主机上的任何一个连接，则向远端发送一个复位包。

4）URG：为紧急数据标志。如果它为 1，表示本数据包中包含紧急数据。此时紧急数据指针有效。

5）ACK：为确认标志位。如果为 1，表示包中的确认号是有效的；否则，包中的确认号无效。

6）PSH：如果置位，接收端应尽快把数据传送给应用层。

TCP 连接的建立过程如图 3-4 所示，很多地方也叫“三次握手协议”。地址和端口扫描很多都是基于这种 TCP 连接建立过程中的“三次握手协议”进行的。

图 3-4　TCP 建立连接的过程

大部分 TCP/IP 连接实现遵循以下原则：

1）当一个 SYN 或者 FIN 数据包到达一个关闭的端口，TCP 丢弃数据包同时发送一个 RST 数据包。

2）当一个 RST 数据包到达一个监听端口，RST 被丢弃。

3）当一个 RST 数据包到达一个关闭的端口，RST 被丢弃。

4）当一个包含 ACK 的数据包到达一个监听端口时，数据包被丢弃，同时发送一个 RST 数据包。

5）当一个 SYN 位关闭的数据包到达一个监听端口时，数据包被丢弃。

6）当一个 SYN 数据包到达一个监听端口时，正常的三阶段握手继续，回答一个 SYN | ACK 数据包。

7）当一个 FIN 数据包到达一个监听端口时，数据包被丢弃。“FIN 行为”（关闭的端口返回 RST，监听端口丢弃包），在 URG 和 PSH 标志位置位时同样要发生。所有的 URG、PSH 和 FIN，或者没有任何标记的 TCP 数据包都会引起“FIN 行为”。

下面介绍几种典型的扫描方法。

1. 全 TCP 连接扫描

全 TCP 连接扫描是 TCP 端口扫描的基础。扫描主机尝试（前面讲过的使用三次握手）与目的机指定端口建立正常的连接。连接由系统调用 connect( )开始。对于每一个正在监听的端口，connect( )会获得成功，否则返回-1，表示端口不可访问。由于通常情况下，这不需要什么特权，所以几乎所有的用户都可以通过 connect( )来实现这种扫描方法。这种扫描方法很容易检测出来（在日志文件中会有大量密集的连接和错误记录）。

2. 半 TCP 连接扫描或叫 TCP SYN 扫描

在这种方法中，扫描主机向目标主机的相关端口发送 SYN 数据段。如果应答是 RST，那么说明端口是关闭的，按照设定就继续扫描其他端口；如果应答中包含 SYN 和 ACK，说明目标端口处于监听状态。所有的扫描主机都需要知道这个信息，传送一个 RST 给目标机从而停止建立连接。由于在 SYN 扫描时，全连接尚未建立，所以这种技术通常被称为半连接扫描。

SYN 扫描的优点在于即使日志中对扫描有所记录，但是尝试进行连接的记录也要比全扫描少得多。缺点是在大部分操作系统下，发送主机需要构造适用于这种扫描的 IP 包，通常情况下，构造 SYN 数据包需要超级用户或者授权用户访问专门的系统调用。

3. 秘密扫描技术

由于这种技术不包含标准的 TCP 三次握手协议的任何部分，所以无法被记录下来，从而比 SYN 扫描隐蔽得多。秘密扫描技术使用 FIN 数据包来探听端口。当一个 FIN 数据包到达一个关闭的端口，数据包会被丢掉，并且会返回一个 RST 数据包；否则，当一个 FIN 数据包到达一个打开的端口，数据包只是简单地丢掉（不返回 RST）。

秘密扫描通常适用于 UNIX 目标主机。在 Windows95/NT 环境下，该方法无效，因为不论目标端口是否打开，操作系统都发送 RST。

4. Ping 扫描

如果需要扫描一个主机上甚至整个子网上的成千上万个端口，首先判断一个主机是否开机就非常重要了。这就是 IP 地址扫描器的目的，通常采用 Ping 来实现。Ping 扫描主要是发送 ICMP 请求包给目标 IP 地址，有响应的表示主机开机。

除了上述基于 TCP 连接建立过程中的“三次握手协议”进行的地址和端口扫描，还有基于 TCP 连接结束时“四次握手协议”进行扫描的，这里由于篇幅不再叙述，感兴趣的读者可以查看相关资料。

3.2.2 漏洞扫描

漏洞是指计算机系统软硬件包括操作系统和应用程序的固有缺陷或者配置错误，这些缺陷和错误很容易被黑客所利用对计算机系统进行攻击。

这里注意，漏洞的英文词语是 Vulnerability，而不是 Hole，很多读者容易拼写错误。漏洞是硬件、软件或策略上的缺陷，从而使得攻击者能够在未授权的情况下访问、控制系统。漏洞是软件在开发的过程中没有考虑到的某些缺陷，也叫软件的 bug。关于漏洞，我们要知道以下几个方面的事情：

- 漏洞一般指软件的（安全）漏洞。
- 漏洞存在通用的软件中。

- 漏洞是事先未知、事后发现的。
- 漏洞是安全隐患，如果被利用，其后果不可预知。
- 漏洞一般能够被远程利用。
- 漏洞一般是可以修补的。

漏洞产生的原因一般有两个方面。

1）设计上的缺陷。受编程人员的能力、经验和当时安全技术所限，在程序中难免会有不足之处，轻则影响程序效率，重则导致非授权用户的权限提升。

2）利益上的考虑。在程序编写过程中，为实现不可告人的目的，在程序代码的隐藏处保留后门。还有的是为了在软件系统完成后，方便进行测试而故意留的后门。

下面以缓冲区溢出漏洞为典型例子，介绍漏洞出现的原理及漏洞利用的方法。缓冲区溢出一直会引起许多严重的安全性问题。当前网络种种安全问题至少有 50%源自缓冲区溢出的攻击。前面讲的冲击波病毒就是利用操作系统里的缓冲区溢出，从而攻击了计算机。

缓冲区溢出漏洞之所以这么多，主要在于它的产生非常简单。只要 C/C++程序员稍微不注意，他的代码里面可能就出现了一个缓冲区溢出漏洞，甚至即使经过仔细检查的代码，也可能存在缓冲区溢出漏洞。例如下面的 C 语言代码：

```
#include<stdio. h>
void main( )
{
charbuf[ 8];
gets( buf) ;
}
```

上面的程序运行的时候，如果你输入“Hi”，或者“Dog”，那么一切正常，但是如果输入“Tomorrow is a good day”，那么程序就发生溢出了。因为这里的 buf 这个数组只申请到 8 个字节的内存空间，而输入的字符数却超过了这个数目，于是多余的字符将会占领程序中不属于自己的内存。因为 C/C++语言并不检查边界，所以程序将看似正常继续运行。如果被溢出部分占领的内存并不重要，或者是一块没有使用的内存，那么，程序将会继续看似正常运行到结束。但是，如果溢出部分占领的正好是存放了程序重要数据的内存，那么一切将会不堪设想。例如，有黑客利用缓冲区溢出攻击，将自己在被攻击者计算机里的权限从 Guest 权限提升到了 Administrator 权限，从而进行更严重的破坏。

实际上，缓冲区溢出通常有两种：堆溢出和堆栈溢出。尽管两者实质一样，但由于利用的方式不同，产生的结果也不同。这里由于篇幅所限不详细描述。

漏洞扫描，顾名思义是指基于数据库中的已有漏洞，采用扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现其中能够利用的漏洞的一种安全检测（渗透攻击）行为。

漏洞扫描主要是对计算机信息系统进行检查，发现其中可被黑客利用的漏洞。漏洞扫描的结果实际上就是系统安全性能的一个评估，它指出了哪些攻击是可能的，因此成为安全方案的一个重要组成部分。

漏洞扫描的原理是采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查。

漏洞扫描的目标是计算机工作站、服务器、交换机、数据库应用等各种对象。漏洞扫描的结果是向系统管理员提供周密可靠的安全性分析报告，为提高网络安全整体水平产生重要依据。

漏洞扫描主要分为基于网络的漏洞扫描和基于主机的漏洞扫描。它们的实现原理基本一致，但体系结构差距较大。

1. 基于主机的漏洞扫描

主机扫描器又称本地扫描器，它与待检查系统运行于同一结点，执行对自身的检查。它的主要功能为分析各种系统文件内容，查找可能存在的对系统安全造成威胁的配置错误。

2. 基于网络的漏洞扫描

网络扫描器又称远程扫描器。它和待检查系统运行于不同结点，通过网络远程探测目标结点，检查安全漏洞。远程扫描器检查网络和分布式系统的安全漏洞。与主机扫描器的扫描方法不同，网络扫描器通过执行一整套综合的渗透测试程序集，也称扫描方法集，发送精心构造的数据包来检测目标系统是否存在安全隐患。

漏洞扫描系统的主要组成如图 3-5 所示，主要包括：漏洞数据库模块、用户配置控制台模块、扫描引擎模块、结果存储器和报告生成工具。

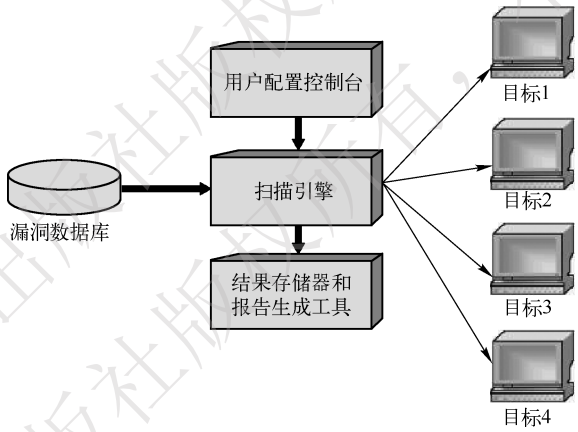

图 3-5　漏洞扫描系统主要组成模块

一般来说，基于网络的漏洞扫描工具可以看作一种漏洞信息收集工具，其根据不同漏洞的特性，构造网络数据包，发给网络中的一个或多个目标机，以判断某个特定的漏洞是否存在（实际上是进行一次没有危害的攻击）。

消除漏洞的主要方法是为有漏洞的系统及时安装补丁，或者直接更新系统。这和人们穿衣服类似，衣服不小心破了一个口子。解决办法一是缝补一个衣服的补丁，另一个办法是原来的破衣服直接扔掉，买一件新衣服穿上。

3.2.3　典型的扫描工具介绍

1. Pinger 网络 IP 地址扫描工具

如图 3-6 所示为 Pinger 网络 IP 地址扫描工具。它可以快速扫描一段网络 IP 地址，查看哪些主机处于工作状态。

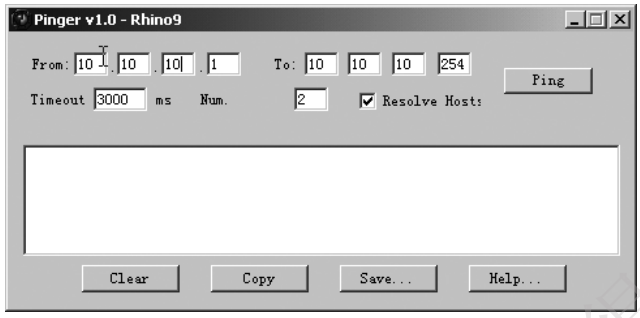

图 3-6　Pinger 网络 IP 地址扫描工具

2. 端口扫描工具

网上专业的端口扫描工具很多，这里介绍比较典型的三个。图 3-7 所示为 NetScanTools，图 3-8 所示为 WinScan，图 3-9 所示为 SuperScan。这三个端口扫描工具各有优缺点，感兴趣的读者可以下载使用。

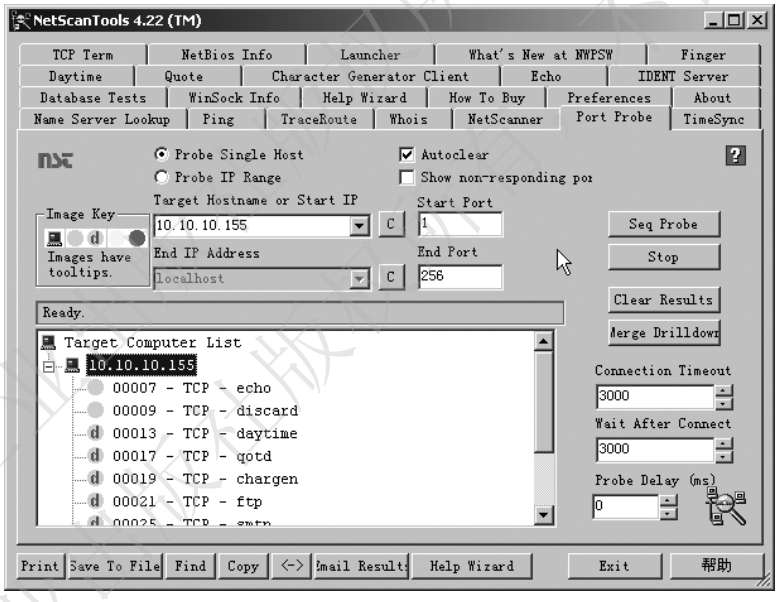

图 3-7　NetScanTools 扫描工具

3. 漏洞扫描工具

漏洞扫描工具有很多。由于篇幅所限，这里简单介绍两个典型漏洞扫描工具。一个是中国第一代著名黑客小榕的作品流光扫描软件；另一个是来自俄罗斯的安全扫描工具 Shadow Security Scanner。

流光是一款国产非常优秀的综合扫描工具，不仅具有完善的扫描功能，而且自带了很多猜解器和入侵工具，可方便地利用扫描的漏洞进行入侵。启动流光工具后可以看到它的主界面。如图 3-10 所示为流光 5.0 扫描器的主界面。

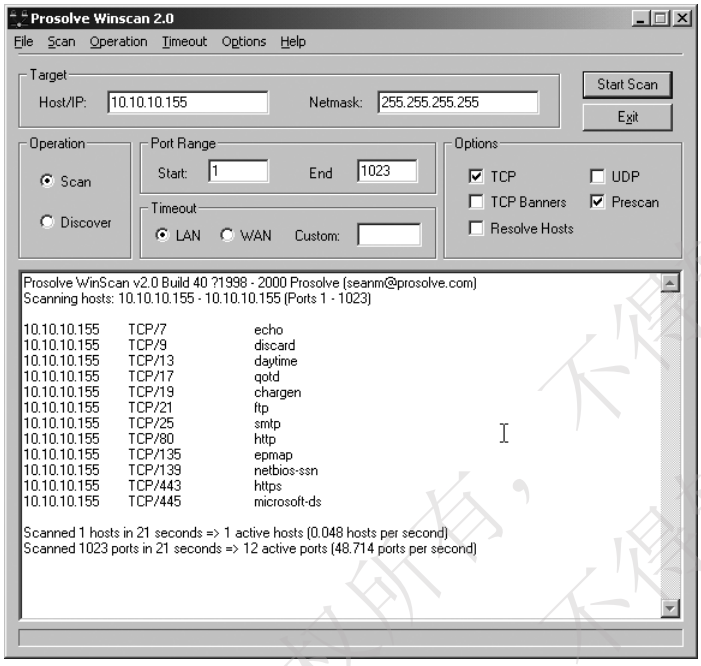

图 3-8　WinScan 扫描工具

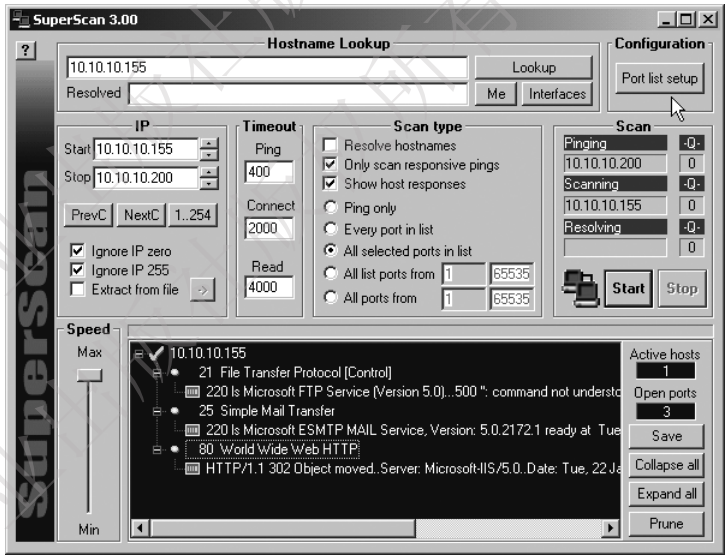

图 3-9　SuperScan 扫描工具

流光不仅能够支持 10 个字典同时检测，检测设置可作为项目保存，非常方便用户的使用。同时软件具有分析目标主机的信息的能力，支持探测 POP3、FTP、HTTP、PROXY、FROM 等各种漏洞，检测 POP3/FTP 主机中用户密码安全漏洞。

Shadow Security Scanner 扫描器简称 SSS 扫描器。它是非常专业的综合安全漏洞扫描软件，能扫描服务器各种漏洞，包括很多漏洞扫描、账号扫描、DOS 扫描等。安装好 SSS 后，打开 SSS，它会进行自动更新，然后启动主界面，如图 3-11 所示。

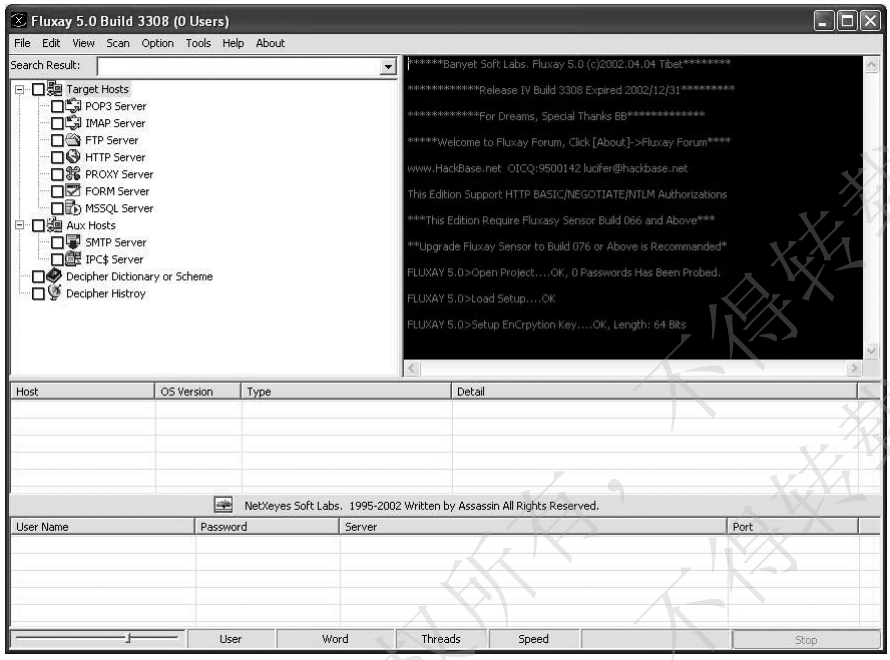

图 3-10　流光综合扫描工具的界面

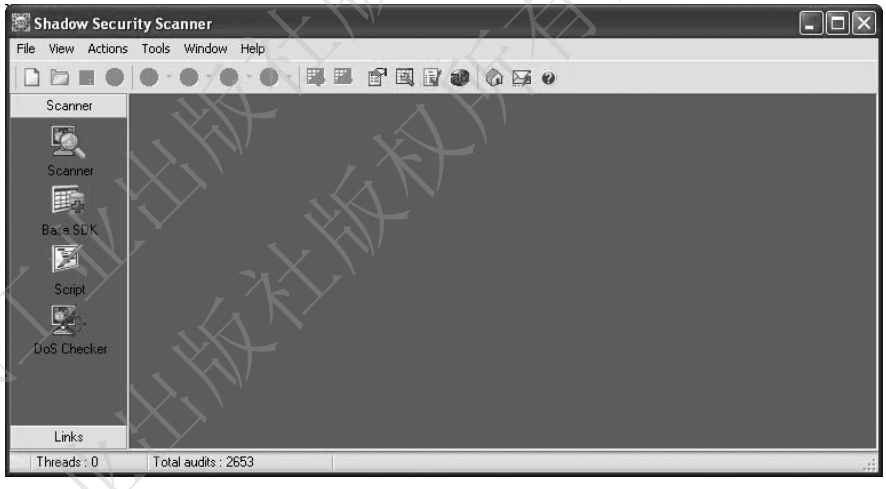

图 3-11　Shadow Security Scanner 扫描工具的界面

关于这两个综合漏洞扫描的详细使用方法，读者可以自己查找资料，本书只是概述，让大家知道有这两个比较典型的扫描工具。

3.3　网络监听

网络监听是一种监视网络所处状态、数据流向以及网络上信息传输的管理工具。它可以将网络界面设定为监听模式，并且可以截获网络所传输的信息。也就是说，当有人登录网络主机并取得超级用户权限后，若想要登录其他主机，使用网络监听工具便可以有效地截获网

络上的数据，这是黑客使用最好的方法。

3.3.1 网络监听的原理

世界上最早的窃听器是中国在2000多年前发明的。战国时代的《墨子》一书中就记载了一种“听瓮”工具，主要是用来听取是否有敌人从城外向城内挖掘地道用的。这种“听瓮”工具是用陶制成的，大肚小口，把它埋在地下，并在瓮口蒙上一层薄薄的皮革，人伏在上面就可以听到城外方圆数十里的动静，例如是否有人在挖掘地道。“听瓮”是用声学原理进行监听的。

在计算机网络中，对于目前使用的以太网协议，它的工作方式是：将要发送的数据包发往连接在一起工作的所有主机，其中包含着应该接收数据包主机的正确地址，只有与数据包中目标地址一致的那台主机才能接收。然而，当主机工作在监听模式下，无论数据包中目标地址是什么，主机都将接收。如图3-12所示，审计系统可以通过交换机监听网上所有的流量。

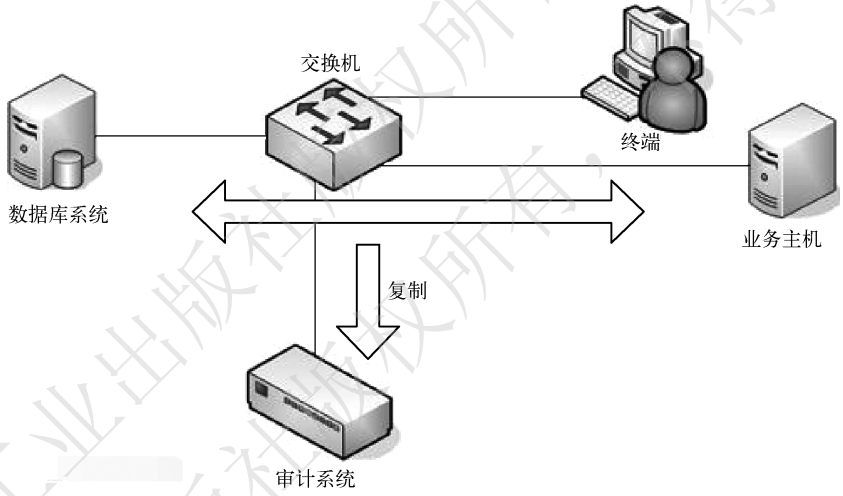

图3-12 网络监听原理

3.3.2 典型的网络监听工具

网上的网络监听工具有很多种，目前比较流行的就两个，一个是Sniffier，另一个是Wireshark。

1. Sniffer网络监听工具

Sniffer软件是NAI公司推出的功能强大的协议分析软件，它可以用来截获网络中传输的FTP、HTTP、Telnet等各种数据包，并进行分析。Sniffer软件启动后的界面如图3-13所示，感兴趣的读者可以在网上下载使用。

2. Wireshark网络监听工具

Wireshark在2006年6月叫作Ethereal，因为商标的问题，Ethereal在这一年更名为Wireshark。它是世界上最流行的网络分析工具之一。这个强大的工具可以捕捉网络中的数据，并为用户提供关于网络和上层协议的各种信息。这个软件可以在官网（地址：https://

www. wireshark. org/）上下载。Wireshark 的作用主要包括：

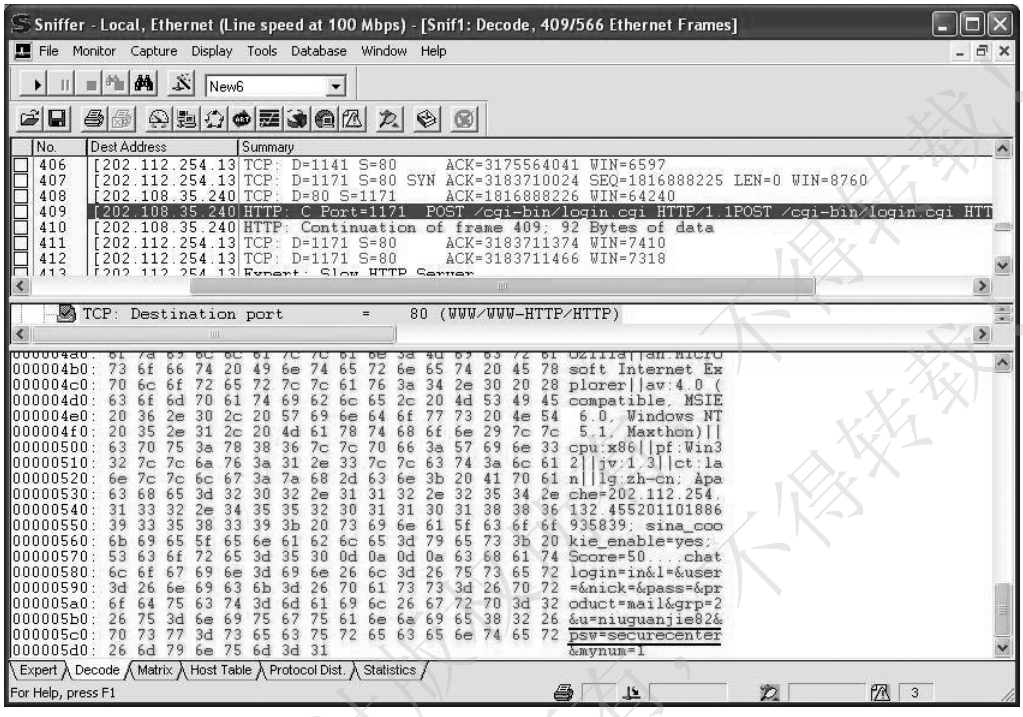

图 3-13　Sniffer 软件主界面

- 网络管理员用来解决网络问题。
- 网络安全工程师用来检测安全隐患。
- 开发人员用来测试协议执行情况。
- 用来学习网络协议。

相比于其他的流量捕获工具，Wireshark 有如下优点：

- 支持 UNIX 和 Windows 平台。
- 在接口实时捕获包。
- 能显示包的详细协议信息。
- 可以打开/保存捕捉的包。
- 可以导入导出其他捕捉程序支持的包数据格式。
- 可以通过多种方式过滤包。
- 多种方式查找包。
- 通过过滤以多种色彩显示包。
- 创建多种统计分析。

需要注意的是，Wireshark 不是入侵检测软件，本身不具备异常流量检测的功能；同时 Wireshark 也不能对数据包内容进行修改，不能发送数据包。如图 3-14 所示为 Wireshark 主界面。

以上介绍的两种网络监听工具各有优缺点，感兴趣的读者可以都试试。

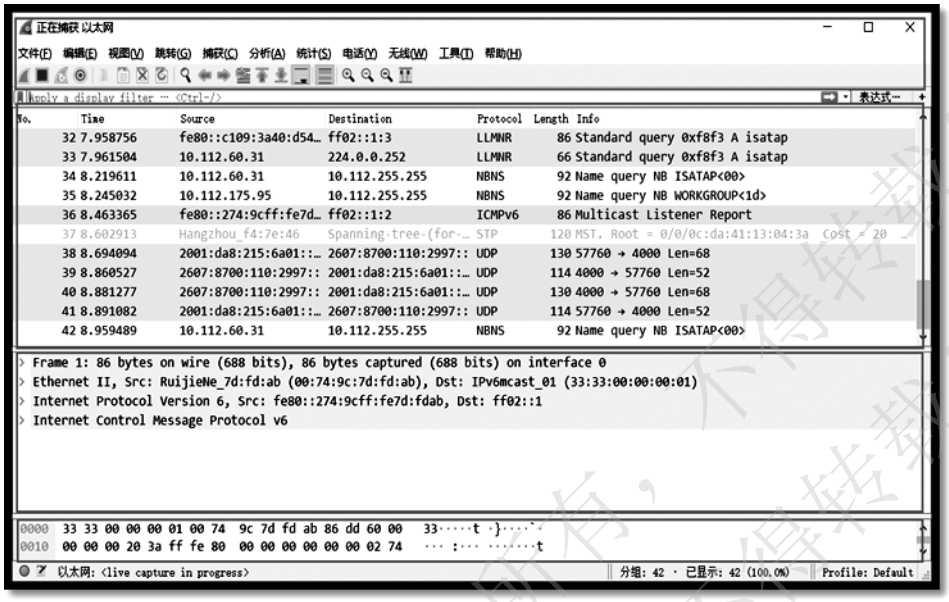

图 3-14　Wireshark 主界面

3.3.3　网络监听的防护

通常用于防护网络监听的方法主要是利用防火墙，还有网络加密，以及专业的防监听工具等。

1. 使用防火墙进行防护

防火墙型安全保障技术是基于被保护网络具有明确定义的边界和服务，并且网络安全的威胁仅来自外部的网络。通过监测、限制以及更改跨越“防火墙”的数据流，尽可能地对外部网络屏蔽有关被保护网络的信息、结构，实现对网络的安全保护，因此比较适合于相对独立、与外部网络互连途径有限并且网络服务种类相对单一、集中的网络系统。

对于个人用户，安装一套好的个人防火墙是非常实际而且有效的方法。现在有很多个人防火墙，这些防火墙往往具有智能防御核心，攻击并进行自动防御，保护内部网络的安全。

2. 对网络上传输的信息进行加密，可以有效地防止网络监听等攻击

目前有许多软件包可用于加密连接（如使用 SSL 加密等），使入侵者即使捕获到数据，但无法将数据解密而失去窃听的意义。

其他的防监听方法还有使用专业的防监听工具，如 SATAN 等。

3.4　习题

1. 什么是黑客？
2. 黑客为什么要进行扫描？
3. IP 扫描的原理是什么？
4. 网络监听的原理是什么？