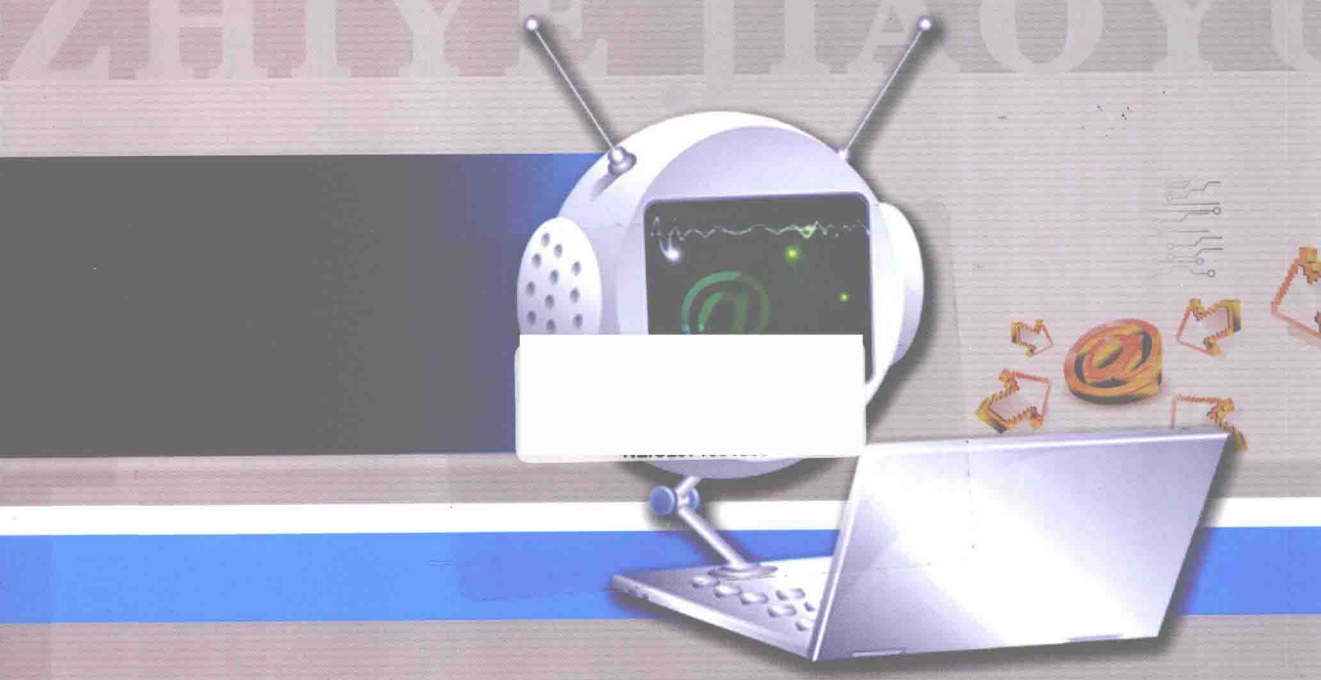
国家中等职业教育改革发展
示范学校建设项目成果教材

网络安全技术

常彩虹　程延周　主编

ZHIYE JIAOYU



配电子课件

机械工业出版社
CHINA MACHINE PRESS

国家中等职业教育改革发展示范学校建设项目成果教材

网络安全技术

主　编　常彩虹　程延周

副主编　赵勇利　柳　鑫

参　编　贺丽菲　张　杰　谢兰敏

机械工业出版社

本书以中等职业教育的培养目标为宗旨，按照理论知识“够用”、实践技能“先进、实用”的“能力本位”的原则确定教学内容，力图使学生学完全部内容后，能够自己实现网络维护、网络安全管理和网络故障排查。

本书通过项目引领的方式，介绍了网络安全中常见的黑客攻击技术以及如何搭建一个企业网络安全体系，使读者能够熟练地使用常用的黑客攻击和系统防御工具，了解信息安全的整个过程，掌握一定的网络安全管理技能，了解 Windows 系统的安全配置和管理；能承担中小型企业的网络安全管理工作任务。为方便教师授课，本书配有电子课件，读者可登录机械工业出版社教材服务网 www.cmpedu.com 下载或联系编辑（010-88379194）咨询。

本书既可以作为各类职业学校计算机及相关专业的教材，也可供从事网络安全方面的技术人员参考使用。

图书在版编目（CIP）数据

网络安全技术/常彩虹，程延周主编. —北京：
机械工业出版社，2014.5
国家中等职业教育改革发展示范学校建设项目成果教材
ISBN 978-7-111-43947-9

Ⅰ.①网… Ⅱ.①常…②程… Ⅲ.①计算机网络-安全技术-中等专业学校-教材 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2013）第 208898 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：梁 伟 李绍坤 责任编辑：蔡 岩
封面设计：赵颖喆
北京振兴源印务有限公司印刷
2014 年 5 月第 1 版第 1 次印刷
184mm×260mm · 10.5 印张 · 253 千字
标准书号：ISBN 978-7-111-43947-9
定价：27.00 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	
社服务中心：	（010）88361066	教材网：	http://www.cmpedu.com
销售一部：	（010）68326294	机工官网：	http://www.cmpbook.com
销售二部：	（010）88379649	机工官博：	http://weibo.com/cmp1952
读者购书热线：	（010）88379203	**封面无防伪标均为盗版**	

前　言

随着计算机网络与通信技术的发展，网络信息的安全已经成为各行各业中非常重要的环节，而随着网络服务器管理技术的不断发展，现在国内各行各业的网络大多只是处于组建内部网或接入公网，根本谈不上真正意义的网络管理。因此，能够掌握一定的网络信息安全知识已成为网络管理中的一种必备技能。

本书按照“以能力为本位、以职业实践为主线、以项目课程为主体的模块化专业课程体系”的总体设计要求，采用“理论+实战”的形式，全面介绍了网络安全工作可能涉及的多方面的内容。无论是初学者，还是有一定基础的读者，只要根据书中介绍的步骤操作，就能顺利完成相关工作。

本书教学建议主要采取以下方式：

1. 理论与实践相结合

本书将理论知识与实际应用相结合，通过实际应用案例讲解知识点，分析应用环境，演示操作方法，辅导学生练习。

2. 理论与实习相结合

对学生以小组的形式进行辅导，每 3～5 人为一个学习小组，并定期安排学生到企业参加实践活动。

3. 教学与工程实际相结合

利用学校和企业资源，为学生安排岗位培训和训练，使学生将理论知识与实际应用相结合，提高学习积极性，同时也检验了学习效果。

本书由常彩虹、程延周任主编，赵勇利、柳鑫任副主编，参与编写的还有贺丽菲、张杰、谢兰敏，编写人员均来自教学第一线，具有丰富的教学和实战经验。具体分工：邢台市农业学校常彩虹负责等 1 章的编写以及对全书的修改和审定，程延周负责第 3 章、第 7 章的编写，赵勇利负责第 4 章的编写，神州数码网络有限公司柳鑫负责第 2 章的编写，贺丽菲负责第 6 章的编写，张杰、谢兰敏负责第 5 章的编写。

由于编者水平有限，书中难免有错误之处，敬请读者批评指正。

编　者

目 录

第1章 计算机网络安全基础知识

教学目标

通过对本章的学习，学生应该了解网络安全环境的现状和成因以及网络安全的未来发展，熟悉常见的网络安全部件和安全标准，了解网络层次安全。

能力目标	知识目标	主要教学内容
熟悉网络安全特征	了解网络安全基础知识	网络安全概况
了解安全环境成因	熟悉网络安全部件	网络安全成因分析
掌握按层次分析问题的能力	熟悉网络安全标准	网络层次安全

案例引入

你有没有遇到过以下情况？

当你打开 QQ 的时候，发现密码总是无法通过审核，昨天还使用过的密码，今天就变成错误密码了。

当你打开邮箱时，发现邮箱被一些主题为“会议邀请”“代开发票”的信件所充斥，但是这些发件人你根本就不认识，信件来源也无法确定。

当你打开经常玩的网络游戏时，发现精心获得的一些装备突然不翼而飞，而且也没有丢失的任何痕迹。

当你上网时，突然发现自己的个人资料、照片、家庭住址、身份证号等信息没有经过你的许可而被公开。

当你打开计算机开始一天的学习工作时，发现计算机使用时总是有问题。经检查才发现感染了计算机病毒。

案例分析

这些现象就是经常提到的信息安全威胁，也称为网络安全。当然以上提到的这些现象只是网络安全问题的冰山一角，还有很多不安全因素需要进行学习和了解，以及在此基础上进行防治。

案例思考

除了上述的现象你还遇到过哪些类似现象，或者你周围的人遇到过类似的现象吗？遇到这些现象后，是如何去处理和解决的呢？

1.1 网络安全基础

网络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，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统可以连续、可靠、正常地运行，信息服务不中断。网络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、信息论等多种学科的综合性学科。

从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

1.1.1 网络安全的发展

网络安全的发展经历了以下 3 个阶段：

第 1 阶段：1969～1972 年。在这个阶段以 ARPANET 为代表的互联网刚诞生，一切应用还处于由军方向民事方向的迁移阶段，这个阶段网络安全处于一个相对安全的时期。一些网络不安全因素正处在萌芽期。

第 2 阶段：1972～1990 年。这个阶段网络在构成方面日益成熟，相关技术如 TCP/IP 等逐步成型，网络应用处于大爆发的前期。但是当时全世界范围内网络普及度还很低，网络互联的范围还很小。这个阶段以计算机病毒为主的不安全因素已经趋于显现，并且在一段时间内多次爆发，已经对信息技术行业产生了不小的影响。但是总体来看这个阶段的网络安全问题仍然是比较单一、可控的。

第 3 阶段：1990～现在。这个阶段因为互联网在技术成熟后，随着光纤通信技术的成熟，光纤线路价格逐渐被用户接受，网络带宽有了成倍的增长。同时作为软件技术的 HTML 超链接技术被应用于网站建设，以及后期的 ASP、PHP 等很多技术的投入使用。使得互联网有了很大的发展潜力，于是网络的各项服务蓬勃发展，例如，图像技术、视频流技术、即时通信技术等，都在网络中得到充分的利用。当然随之而来的逐步恶化的网络安全环境、网络攻击、木马、网络病毒等很多网络不安全因素，都体现出来并形成网络安全的很多具体威胁。这个阶段可以称为网络安全问题的大爆发阶段。

1.1.2 网络安全的未来

网络安全是一个综合学科，隶属于计算机网络技术这个大学科，是从网络管理和网络维

护这几个分支学科中衍生出来的。因此，网络安全学科不可能和网络管理、网络维护等分支学科彻底分离，这些学科都存在交集部分。网络安全学科发展到今天也有了很多子学科，这些子学科的发展都影响着网络安全整体学科的未来发展。

网络安全学科涉及通信学、编码学、密码学、数学、社会工程学等很多学科。随着时代的发展，网络安全也包括防火墙技术、加解密技术、网络病毒防御技术、垃圾邮件防治技术、上网行为管理技术、网络安全管理维护技术、日志分析技术等多项技术分类。而且随着移动互联网的大发展，网络安全还将涉及智能移动终端安全技术、通信安全技术、接入安全技术、无线广播网络安全技术等多项技术分支。

总之，随着人类生活越来越依赖网络，网络安全也就越来越显得更为重要。这个学科将不再只是行业内部的学科，而是涉及人类发展、生活等多方面的一个普及型学科。

1.2　网络安全现状分析

虽然当今有很多网络安全防护技术已经应用于网络安全中，但是当今的网络安全环境总体仍然不容乐观。现在的网络安全环境可以从以下近几年的网络安全事件中得到体现。

1.2.1　网络安全事件

1987 年，年仅 21 岁的康奈尔大学学生 Robert 释放了世界上首个“蠕虫”病毒，美国等接入互联网的计算机都受到了影响。

1996 年，以色列的黑客侵入美国花旗银行并盗走 2000 万美元，这是历史上第一个通过入侵银行计算机系统来获利的网络安全事件。

2001 年 6～7 月，江西万年县一名 39 岁的中学教师，在申银万国证券公司万年营业部，利用散户厅的计算机，破译出计算机信息系统中心股民账号交易密码 51 个，并自作主张，非法买卖他人股票 400 余万元，造成他人经济损失 17 万元。

2006 年我国互联网主干网上的所有路由器在同一时间都受到了 DDoS 攻击，造成全国范围内的断网，这是僵尸网络发起的一次针对我国主干网的大面积攻击。

2006 年 12 月，著名的“熊猫烧香”病毒，几乎一夜之间传遍大江南北。为此该病毒的始作俑者被判处 4 年有期徒刑。这是我国全国范围内的第一起病毒案件。

1.2.2　安全问题分析

就现在常见的网络连接形式而言，网络可以分为有线网络和无线网络，也可以分为企业外部网络和企业内部网络，还可以分为固定网络和移动网络。但是无论从哪个角度区分网络，其应用是一致的，所以综合来看网络安全存在以下几类问题，这些问题针对不同的网络可能具体显示的情况稍有差别。

（1）网络攻击

攻击者通过寻找未设防的路径进入网络或个人计算机，一旦进入，就会对计算机造成危害。这种攻击行为现在已经非常广泛，而且不再有具体的针对群体，而是针对所有使用计算机的人群。

（2）网络病毒

病毒经过多年的发展已经有新型病毒，而且新型网络病毒有和网络攻击进行小范围融合的趋势。

（3）数据泄密

一些小型企业在与第三方网络进行传输时，需要采取有效措施来防止重要数据被中途截获，如用户信用卡号码等。当信息进行传播时，攻击者可以利用工具，将网络接口设置在监听的模式，便可将网络中正在传播的信息截获或者捕获到，从而进行攻击。

（4）接入安全

802.11 无线联网技术为小型企业带来了巨大商机，使其能够以最低成本迅速构建一个高速网络。但是，由于其传输范围内配有大量带有无线接收设备的智能终端，很多无线局域网会对非授权用户开放。这就使得无线网络存在很大的安全隐患。

（5）垃圾邮件

垃圾邮件现在已经成为网络安全问题中的重要组成部分。国际上已经开始联手针对垃圾邮件进行统一的防治，例如，定期发布垃圾邮件服务器黑名单等。但是针对各国内部的垃圾邮件类型和垃圾邮件服务器还是要从各国内部做好防范，这些防范手段应该包含技术类和法律类、执行类等多种。简单靠技术实现已经越来越困难。

（6）上网行为安全

网上浏览也是网络系统被入侵的一个不安全因素。网上浏览的不安全因素包括从网上下载资料可能带来病毒程序或者是木马程序，还有利用假冒手段骗取关键信息等。除此之外企业内部网络使用人员会无意泄露系统管理员的用户名、密码等关键信息。在不知情的前提下泄露内部网的网络拓扑结构以及重要信息的分布情况也是常见的内部网安全问题。甚至存在有些内部人员故意把黑客程序放在共享目录里作为陷阱，乘机控制并入侵他人主机的问题。另外，企业内部网使用者对网络的滥用也对内网安全造成了很大的隐患。 因此，许多企业必须确定如何在允许员工无阻碍地访问互联网上有用信息的同时限制对网络不当内容的访问。

1.3 网络安全现状成因

网络安全形成原因很多，大体可以分为社会因素、技术因素甚至还包括一部分相互矛盾的技术因素。

1.3.1 网络安全现状社会因素

（1）网络安全标准不统一

虽然涉及网络安全的规范非常多，有ISO组织、行业协会、各个国家等很多规范，但是规范之间还是存在着一定差异。不同的国家、不同的民族有着不同的行为规范和思维方式。这样就使得许多代表先进技术的安全设备不能在某些安全环节发挥作用，妨碍了业内整体安全的实现。

（2）安全意识不到位

虽然现在网络安全问题已经世人皆知了，但是并不代表全民都具有了相应的安全意识。涉及网络安全的人员往往存在侥幸心理；不涉及安全工作的人员认为网络安全是维护人员的工作，缺乏自身安全的基本意识和技术。

（3）网络安全法律法规缺乏执行性

我国现行的信息网络安全法律法规还存在一些问题，如立法滞后、层次低、尚未形成完整体系、不具备开放性和兼容性、相关法律法规的操作性不是很好等。

（4）忽视网络管理

没有完善的网络管理就没有网络安全。网络管理和网络安全是相辅相成、相互促进且缺一不可的。有些中小企业在网络安全方面也进行了很大的投入，但是整体网络安全情况并没有明显改善就是因为网络管理不到位的原因。这个原因还是网络安全意识不到位，中小企业不愿意在投入了网络安全之后进行网络管理的投入，这种思想显然是错误的。

（5）虚拟世界和现实世界的结合

虚拟的网络世界和现实世界进行了结合从而形成了一种黑色产业链。这就使得网络安全问题不再只是技术人员的事情了，而且简单靠技术已经无法解决这些问题。要割断这种产业链必须依靠威严的法律、运用先进的技术、进行严格的管理，从各个方面杜绝这种产业链形成的可能性，才可以彻底根治网络安全问题。而且在病毒泛滥的时期就存在病毒黑色产业链，现在网络攻击也有网络攻击的黑色产业链，这些黑色产业链也正在逐步融合。如图1-1所示就是一种黑色产业链，从图中可以看到黑色产业链是如何获取利益的。

1.3.2 网络安全问题技术因素

（1）网络的开放性

互联网是开放性的网络，有别于常见的局域网或者企业内部网。开放性网络很难做到针对入网人员的审核，这就导致了针对接入互联网的用户不存在具体项目的约束。这是网络存在大量攻击者的主要原因。当然互联网也很难存在此项目的审核，因为这项审核会限制互联网的发展。

（2）网络安全行业的木桶原理

网络安全行业也符合木桶原理的特性，那就是木桶可以容纳水平面的高度是由最低的木板所决定的，而不是由最高的木板所决定。这就导致了在安全投资方面需要进行详细的风险

分析。这也决定了网络安全整体水平是由各项综合因素所决定的。

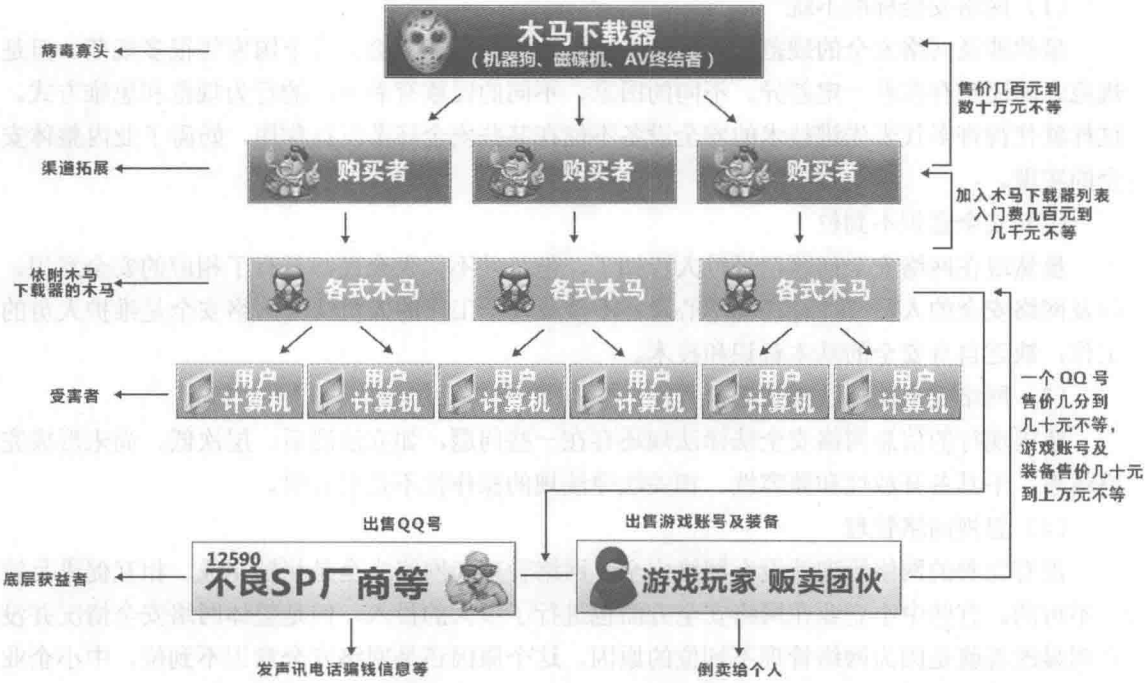


图 1-1　网络安全黑色产业链

（3）函数使用权限的问题

在浏览网站时经常会遇到这种情况，网站会显示用户的 IP 地址甚至是用户的操作系统版本等信息。表面上看这是由于 Cookie 文件的原因，但其实这是程序函数在起作用。有些函数是具有一定危险性的，尤其是有些函数可以获取主机或网络的一些具体设置。这些函数如果被攻击者使用则会造成不良的后果。

（4）辅助安全项目的自身安全问题

为了实现整体网络安全，行业研发了许多辅助安全部件。例如，防火墙、防毒墙等。将这些设备投入到正在运行的网络中确实可以提高整体网络安全水平，但是不可忽略的是这些设备自身也存在安全问题，如果这些设备的自身安全问题被利用，那么所带来的网络安全问题造成的损失也是难以估量的。

1.4　网络安全目的

网络安全目的归纳起来是为了实现更好的网络安全环境，更好地保证网络传输数据的安全性，更好地保证网络接入的速率、提供更高的网络使用率和带宽使用率等。总结起来归纳为 15 个字：进不来、拿不走、看不懂、改不了、走不脱。具体来讲就是网络的安全特性。

网络安全特性包括以下几个方面。

1）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。

2）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。

3）完整性：保证数据的一致性，防止数据被非法用户篡改。

4）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。

5）防抵赖性：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尤为重要。

6）可控性：对信息的传播及内容具有控制能力。

7）可审查性：对出现的网络安全问题提供调查的依据和手段。

1.4.1　网络安全部件

为了更好地实现网络安全环境，针对各类安全问题都有相对的解决方案和根据相应技术生成的相应产品。经过几年的发展，网络安全辅助部件已经门类繁多。包括防火墙、防毒墙、日志系统、审核系统等十几个大类，其中非常重要的有 5 大类。

1）防火墙：防火墙是针对网络攻击行为防范的主力设备，分为硬件防火墙和软件防火墙等几大类。技术相对成熟，在现有网络中的部署已经非常普及。如图 1-2 所示就是一款硬件防火墙。

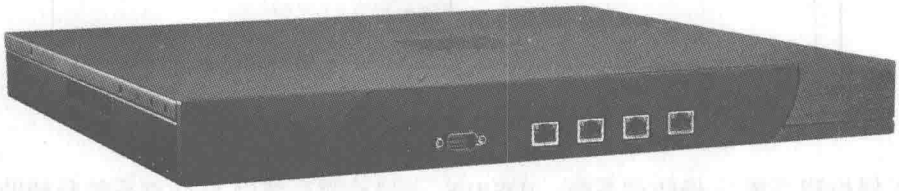


图 1-2　硬件防火墙

2）防毒墙：防毒墙是针对网络病毒进行防范的主力设备，现在多以软件为主，也有软、硬件配合的产品。在网络安全行业内防火墙和防毒墙是有着明显区别的。核心在于病毒是合法的数据包而攻击是非法的数据包。所以从这个角度讲，防火墙和防毒墙的工作原理是有很大差异的。如图 1-3 所示就是一款金山公司硬件防毒墙，硬件防毒墙和防火墙外观很类似，但是内部工作原理截然不同。

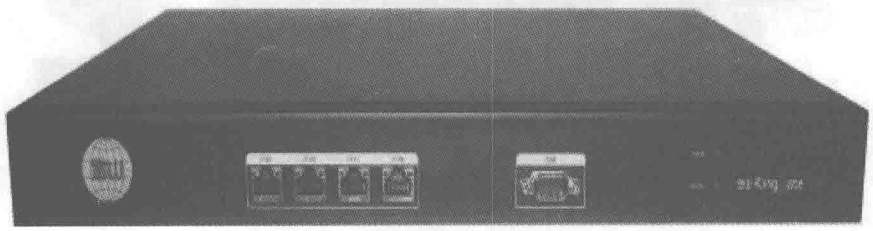


图 1-3　硬件防毒墙

3）扫描器：扫描器是针对网络中本机和远程机器安全弱点进行发现的工具。扫描器是一把双刃剑，用于自身扫描可以发现自身存在的网络安全隐患，如果用于攻击则可以发现对方存在的网络安全漏洞。如图 1-4 所示是一款软件端口扫描器，可以看出这款软件扫描器针对一段 IP 地址进行自定义端口的扫描。

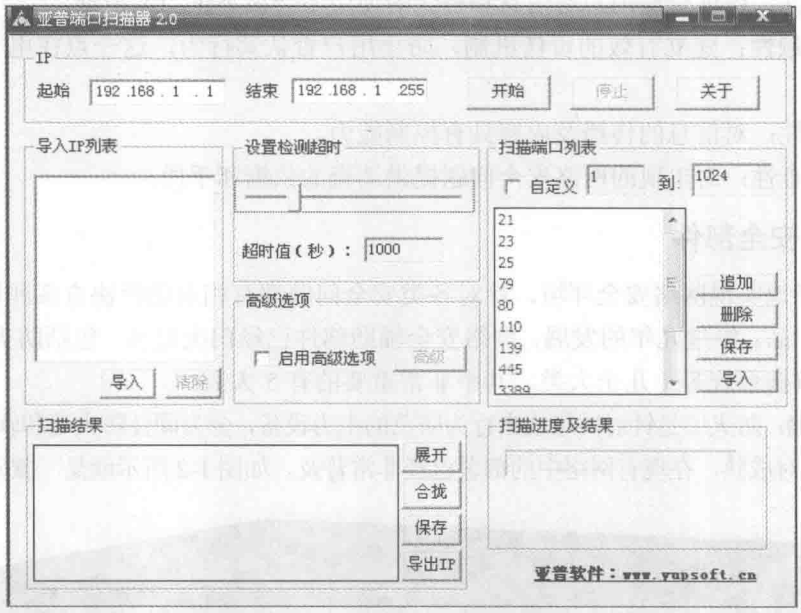


图 1-4　软件扫描器

4）入侵检测系统/入侵防御系统：IDS/IPS 入侵检测系统/入侵防御系统是辅助防火墙进行工作的安全部件。入侵检测系统只有检查的能力，具体的执行能力还是要依靠防火墙，所以入侵检测系统是旁路设备。入侵防御系统拥有查杀两种能力，可以与防火墙进行统一部署，属于主路设备。如图 1-5 所示是锐捷网络的一组 IDS 产品，适用于不同的环境。

图 1-5　入侵检测系统

5）安全审计系统：安全审计系统是一个总称，涉及很多方面。硬件部分包括类似指纹扫描系统、视网膜扫描系统。软件部分包括开机登录系统、日常操作记录系统等。安全审计系统是针对网络日常运行中存在的各项应用进行安全审核的网络安全部件。如图 1-6 所示是一款软件安全审计系统，从这款软件可以看出针对内部网络的每台计算机的安全设置所进行的检测以及针对检测结果的处理方向，也就是审计效果。

图 1-6　安全审计系统

1.4.2　网络安全标准

常见的网络安全标准包括行业协会标准、国家标准，也有相应组织的标准。但是现在业内被广泛承认而且得到具体应用的还是美国橘皮书标准。全称是可信任计算机标准评价准则（TCSEC），由美国国防部开发。网络安全业内俗称网络安全橘皮书。

橘皮书将网络安全标准分为 4 个等级：从高到低分别是 A、B、C、D。A 为最高，D 为最低。其中 B 级还分为 B1、B2、B3 3 个级别，B1 为最高，B3 为最低。C 级也分为 C1、C2 两个级别。C1 级别高于 C2。常见的网络操作系统 Windows 2003 Server 就是 C2 级别的，已经不再使用的 Windows 98 系统就是 D 级别的，网络中现在常用的 Linux 操作系统的安全级别基本在 C1 级。

除了 TCSEC 之外，我国目前主要使用的标准还有 ITSEC 标准和 GB17859-1999 标准。ITSEC 是欧洲的安全评价标准的简写，是英国、法国、德国和荷兰制定的 IT 安全评估准则，较美国军方制定的 TCSEC 准则在功能的灵活性和有关的评估技术方面均有很大的进步。

ITSEC 是欧洲多国安全评价方法的综合产物，应用领域为军队、政府和商业。该标准将

安全概念分为功能与评估两个部分。功能准则从 F1～F10 共分 10 级。1～5 级对应于 TCSEC 的 D～A。F6～F10 级分别对应数据和程序的完整性、系统的可用性、数据通信的完整性、数据通信的保密性以及机密性和完整性的网络安全。

GB17859-1999 标准是我国的国家标准，是我国针对计算机信息系统安全保护等级划分的准则。它于 1999 年发布，由 2001 年开始实施。本标准规定了计算机系统安全保护能力的 5 个等级。第 1 级：用户自主保护级；第 2 级：系统审计保护级；第 3 级：安全标记保护级；第 4 级：结构化保护级；第 5 级：访问验证保护级。本标准适用计算机信息系统安全保护技术能力等级的划分。计算机信息系统安全保护能力随着安全保护等级的增高而逐渐增强。

1.5 网络安全层次介绍

由引入案例不难发现，安全问题可能只涉及一个简单的电子文档，或者一个简单的应用，诸如 QQ。但是，有些安全问题可能会涉及一个特定群体的安全，一个国家的安全，一个社会的稳定等。因此，安全问题也分为低级安全问题和高级安全问题两大类。

1.5.1 网络安全威胁层次

网络安全问题层出不穷，包括感染网络病毒、主机被攻击、网站被攻击更换了主页显示等。这些攻击几乎每天发生，但是对整体网络安全环境带来的危害是有限度的。有些安全问题不是每天发生，但却对整体网络安全环境带来了巨大的危害。例如，各类软硬件的安全漏洞、僵尸网络、拒绝服务攻击、分布式拒绝服务攻击等。因此，行业将网络安全问题分为低级安全问题和高级安全问题。

1）低级安全问题：只涉及个人信息或者个人主机、某一个网站的安全类事件，没有造成大范围、大规模的传播，同时没有针对特定人群的生活产生影响的安全威胁都可以定义为低级安全问题。

2）高级安全问题：涉及一类特定人群、传播范围广、涉及面大。如果不加控制将涉及一个行业、一个民族、一个国家、一个社会的日常行为安全的问题为高级安全问题。

低级安全问题比较好理解，而高级安全问题可能不太容易理解。下面举出几个例子方便大家理解。

1991 年美国针对伊拉克进行的军事行动之前就通过中间商出售给伊拉克军方大量打印机。这些打印机里面都固化了病毒芯片，在战争之初被美国通过卫星信号进行唤醒，这些病毒从打印机直接侵入计算机并在伊拉克军方的指挥网络中进行破坏。导致伊拉克军方无法正常调度军队。

2006 年，我国全国范围内出现大规模僵尸网络破坏事件，此次破坏的对象是各省市区县的主干线路，造成全国范围内断网事件。和平时期僵尸网络的破坏能力都如此之大，如果在战争时期带来的影响将难以预料。

这些都隶属于高级安全问题的行列。但是仅靠上述特征分类还是很难说清楚高级安全和低级安全问题的区别，所以分析所有安全问题还是要从网络的层次定义开始。

在初学网络的时候，都接触过 OSI 网络七层结构，如图 1-7 所示。从这个结构中可以方便地理解网络中每一层的作用和功能。它被广泛地应用于网络的各个学科，例如，网络设备也是按照七层结构去分类的。所以网络安全也可以根据七层结构进行学习。网络安全层次和七层结构也有很大的联系。在七层结构中低五层属于不可见层，高两层属于可见层。但是和安全层次相反的是，网络层次安全中的高级安全问题往往是隶属于七层结构中的低五层，而网络安全层次中的低级安全问题往往是隶属于七层中的高两层。

图 1-7　OSI七层结构

1.5.2　各层网络安全问题

网络安全问题看起来复杂，分析起来往往感到不知道如何下手。其实网络安全问题也有其隶属的网络层次，如果从网络层次的角度去分析则不会感觉混乱。虽然有些问题可能涉及不止一个层次，但是分层处理问题的方式还是一个解决问题的好办法。针对网络层次分析网络安全问题，可以从以下 3 个方面进行考虑：本层在网络七层中的作用；本层的主力协议和设备；本层主要可见的网络应用。

根据以上这 3 个方面来逐层进行网络安全问题的分析。

（1）物理层安全问题分析

物理层的作用：传输数据比特流。

物理层的设备：传输线路包括有线和无线线路，网络设备包括集线器、中继器（现在都基本淘汰）。

物理层可见应用：物理存在，比如，登记用户名、记录密码的纸张，可见的传输线路，双绞线等。

根据上述分析可以定义物理层主要存在的网络安全问题如下。

废物搜寻：针对生成电子数据之前的纸质数据进行收集。

干扰：针对有线传输和无线传输进行信号干扰。

偷窃和损坏：针对登录网络设备进行损毁和偷窃导致无法实现上网行为等。