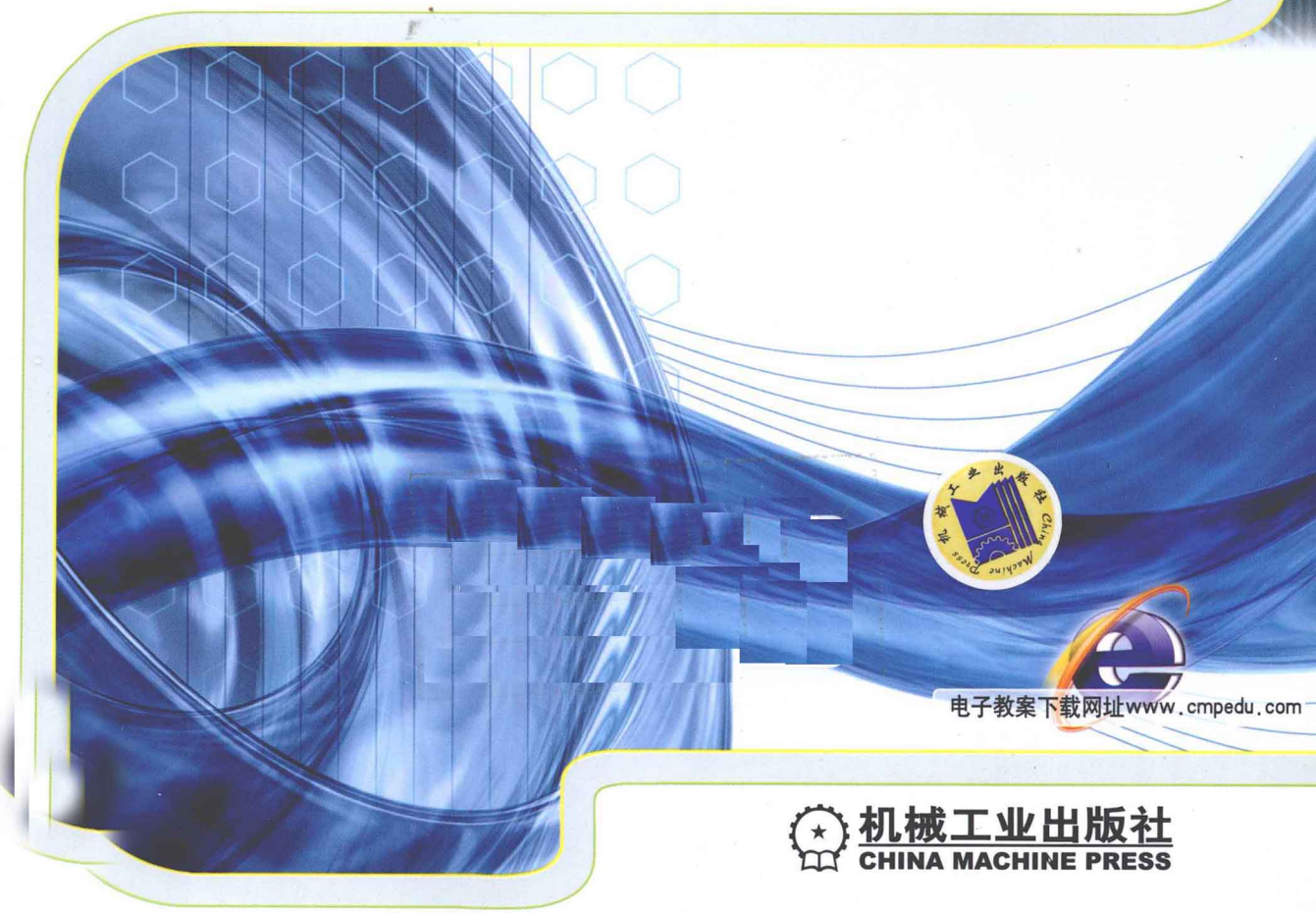
全国高等职业教育规划教材

计算机网络安全

主　编　鲁　立　龚　涛
副主编　严学军　任　琦



电子教案下载网址www.cmpedu.com

机械工业出版社
CHINA MACHINE PRESS

全国高等职业教育规划教材

计算机网络安全

主　编　鲁　立　龚　涛
副主编　严学军　任　琦
参　编　李安邦　宋焱宏　刘　桢　等
主　审　万　钢

机械工业出版社

本书围绕网络安全应用技术，由浅入深、循序渐进地介绍了计算机网络安全方面的知识，同时注重对学生的实际应用技能和动手能力的培养。全书共分 9 章，内容涵盖网络基础知识、计算机病毒、加密与数字签名技术、操作系统漏洞、防火墙技术、端口扫描技术、入侵检测以及无线局域网安全。本书内容丰富翔实，通俗易懂，以实例为中心，并结合大量的经验技巧。

本书既可作为各大高职高专院校计算机以及相关专业的教材，也可作为网络安全管理员指导用书。

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：1239258369，电话：010-88379739）。

图书在版编目（CIP）数据

计算机网络安全 / 鲁立，龚涛主编. —北京：机械工业出版社，2011.3
全国高等职业教育规划教材
ISBN 978-7-111-33505-4

Ⅰ. ①计… Ⅱ. ①鲁… ②龚… Ⅲ. ①计算机网络－安全技术－高等学校：技术学校－教材 Ⅳ ①TP393.08

中国版本图书馆 CIP 数据核字（2011）第 026761 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：鹿 征 马 超
责任印制：李 妍

北京诚信伟业印刷有限公司印刷

2011 年 4 月第 1 版 • 第 1 次印刷
184mm×260mm • 15.75 印张 • 388 千字
0001－ 3000 册
标准书号：ISBN 978-7-111-33505-4
定价：29.00 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
社服务中心：（010）88361066
销 售 一 部：（010）68326294
销 售 二 部：（010）88379649
读者购书热线：（010）88379203

网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com

封面无防伪标均为盗版

全国高等职业教育规划教材计算机专业
编委会成员名单

主　　任　周智文

副 主 任　周岳山　林　东　王协瑞　张福强
　　陶书中　龚小勇　王　泰　李宏达
　　赵佩华

委　　员　（按姓氏笔画顺序）
　　马　伟　马林艺　万雅静　万　钢
　　卫振林　王兴宝　王德年　尹敬齐
　　史宝会　宁　蒙　刘本军　刘新强
　　刘瑞新　余先锋　张洪斌　张　超
　　李　强　杨　莉　杨　云　罗幼平
　　贺　平　赵国玲　赵增敏　赵海兰
　　钮文良　胡国胜　秦学礼　贾永江
　　徐立新　唐乾林　陶　洪　顾正刚
　　康桂花　曹　毅　眭碧霞　梁　明
　　黄能耿　裴有柱

秘 书 长　胡毓坚

出 版 说 明

根据《教育部关于以就业为导向深化高等职业教育改革的若干意见》中提出的高等职业院校必须把培养学生动手能力、实践能力和可持续发展能力放在突出的地位，促进学生技能的培养，以及教材内容要紧密结合生产实际，并注意及时跟踪先进技术的发展等指导精神，机械工业出版社组织全国近60所高等职业院校的骨干教师对在2001年出版的“面向21世纪高职高专系列教材”进行了全面的修订和增补，并更名为“全国高等职业教育规划教材”。

本系列教材是由高职高专计算机专业、电子技术专业和机电专业教材编委会分别会同各高职高专院校的一线骨干教师，针对相关专业的课程设置，融合教学中的实践经验，同时吸收高等职业教育改革的成果而编写完成的，具有“定位准确、注重能力、内容创新、结构合理和叙述通俗”的编写特色。在几年的教学实践中，本系列教材获得了较高的评价，并有多个品种被评为普通高等教育“十一五”国家级规划教材。在修订和增补过程中，除了保持原有特色外，针对课程的不同性质采取了不同的优化措施。其中，核心基础课的教材在保持扎实的理论基础的同时，增加实训和习题；实践性较强的课程强调理论与实训紧密结合；涉及实用技术的课程则在教材中引入了最新的知识、技术、工艺和方法。同时，根据实际教学的需要对部分课程进行了整合。

归纳起来，本系列教材具有以下特点：

1）围绕培养学生的职业技能这条主线来设计教材的结构、内容和形式。

2）合理安排基础知识和实践知识的比例。基础知识以“必需、够用”为度，强调专业技术应用能力的训练，适当增加实训环节。

3）符合高职学生的学习特点和认知规律。对基本理论和方法的论述要容易理解、清晰简洁，多用图表来表达信息；增加相关技术在生产中的应用实例，引导学生主动学习。

4）教材内容紧随技术和经济的发展而更新，及时将新知识、新技术、新工艺和新案例等引入教材。同时注重吸收最新的教学理念，并积极支持新专业的教材建设。

5）注重立体化教材建设。通过主教材、电子教案、配套素材光盘、实训指导和习题及解答等教学资源的有机结合，提高教学服务水平，为高素质技能型人才的培养创造良好的条件。

由于我国高等职业教育改革和发展的速度很快，加之我们的水平和经验有限，因此在教材的编写和出版过程中难免出现问题和错误。我们恳请使用这套教材的师生及时向我们反馈质量信息，以利于我们今后不断提高教材的出版质量，为广大师生提供更多、更适用的教材。

机械工业出版社

前　言

计算机网络技术的迅猛发展以及网络系统应用的日益普及，给人们的生产方式、生活方式和思维方式带来极大的变化。但是，计算机网络系统是开放的系统，具有众多的不安全因素，如何保证网络中计算机和信息的安全是一个重要且复杂的问题。目前研究网络安全已经不仅仅只是为了信息和数据安全，它已经涉及国家发展的各个领域。

培养既掌握计算机网络的理论基础知识，又掌握计算机网络实际应用技能的人才，是网络教学工作者的责任。特别是对于大专院校计算机类专业的学生，更需要一本既具有一定的理论知识水平，又具有较强实际应用技术的教材。

本书以培养网络安全实用型人才为指导思想，在介绍具有一定深度的网络安全理论知识基础上，重点介绍网络安全应用技术，注重对学生的实际应用技能和动手能力的培养。

本书共分为 9 章，主要内容包括：计算机网络安全基础知识、网络安全威胁的特点、网络安全防护与安全策略的基础知识（第 1 章）；计算机网络协议的基础知识、网络协议对于网络安全体系结构、网络常用命令和协议分析工具（Sniffer）的使用方法（第 2 章）；计算机病毒的特性、计算机病毒的分类及传播途径、计算机病毒的检测和防御方法等基本操作技能（第 3 章）；加密算法的工作原理、数字签名技术的工作原理、公钥基础架构（PKI）、CA、数字证书的工作原理和相关概念、PGP 工具软件的应用、SSL 安全传输及安全 Web 站点的应用配置（第 4 章）；防火墙的功能、防火墙的实现技术、防火墙的工作模式和防火墙的实施方式（第 5 章）；Windows Server 2003 操作系统的网络安全构成、账户策略、访问控制配置和安全模板的应用（第 6 章）；端口的概念、各种端口扫描技术的工作原理、常见端口扫描工具应用方法、防范端口扫描技术的应用（第 7 章）；入侵检测系统模型和工作过程、入侵检测系统分类和工作原理、基于主机的入侵检测系统和基于网络的入侵检测系统部署（第 8 章）；介绍无线局域网的构成、无线局域网络的标准和无线网络安全的实现方式（第 9 章）。

本书由鲁立、龚涛任主编，严学军、任琦任副主编，参加编写的还有武汉软件工程职业学院李安邦、宋焱宏、刘颂、张恒、刘媛媛、何水艳、周雯、李晓泉和武汉市中等职业艺术学校刘桢。万钢主审本书，并在编写过程中给予了指导和帮助。

由于计算机网络安全技术发展迅速，加之编者水平有限，书中不足之处在所难免，恳请广大读者提出宝贵意见。

编　者

目　录

第1章　计算机网络安全概述

本章要点

- 计算机网络安全的概念。
- 计算机网络安全威胁。
- 计算机网络安全策略。
- 网络安全防护的主要措施。

目前网络的应用越来越普及，围绕网络安全方面的问题也越来越多。由于网络资源的开放性和计算机网络技术及计算机软硬件的不完善，计算机受到的攻击也越来越多。很多不法分子或者黑客利用网络进行不法操作和破坏，使得人们对网络正常的使用受到巨大的影响。对网络安全性能的改善和增强是相当有必要的，这需要人们去完善网络系统的各个环节，如完善网络设备功能和网络管理软件性能、提高网络性能的监控和管理能力等。

1.1　计算机网络安全的基本概念

1.1.1　网络安全的定义

广义的网络安全是指网络系统的硬件、软件及系统中数据受到保护，不因无意或故意威胁而遭到破坏、更改、泄露，保证网络系统连续、可靠、正常的运行。

国际标准化组织（ISO）对计算机网络安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。

从不同角度和应用解释网络安全可以得到不同的结果。

1．从不同角度解释网络安全

（1）用户

对用户而言，网络安全主要指网络系统可靠的运行，网络中存储和传输的信息的完整、可用和保密。

（2）网络管理者

对网络管理者而言，网络安全主要指网络资源的安全、访问控制的措施，以及有无“黑客”和病毒攻击。

（3）安全保密部门

对安全保密部门而言，网络安全主要指防范有害信息出现，防范敏感信息的泄露。

（4）社会教育

对社会教育而言，网络安全主要指控制有害信息的传播。

2．从不同应用解释网络安全

（1）运行系统安全

对运行系统安全而言，网络安全主要指保证信息处理和传输系统的安全，即保证网络系统环境、系统硬件的可靠运行，以及系统软件及数据库安全，提出系统结构的安全设计。

（2）系统信息安全

对系统信息安全而言，网络安全主要指保证在信息处理和传输系统中存储和传输的信息安全（即保证网络数据的完整性、可用性和机密性），如信息不被非法访问、散布、窃取、篡改、删除、识别和使用等。

1.1.2 网络安全的特性

在美国国家信息基础设施的文献中，提出了网络安全的 5 个特性：可用性、机密性、完整性、可靠性和不可抵赖性。这 5 个特性适用于国家信息设施的各个领域。

（1）可用性

得到授权的用户在需要时可访问数据，也就是说，攻击者不能占用资源而妨碍授权用户正常使用资源。授权的用户随时可以访问到需要使用的信息，这里的主要目的是确保硬件可以使用，信息能够被访问。黑客攻击可以导致系统资源被耗尽，这就是对可用性做的攻击。对用户而言，网络是支持工作的载体，网络资源和网络服务发生中断，可能带来巨大的经济和社会影响，因此网络安全体系必须保证网络资源和服务的连续、正常的运行，要防止破坏网络的可用性。

（2）机密性

确保信息不泄露给非授权用户、实体或进程；用于保障网络机密性的技术主要是密码技术；在网络的不同层次上有不同的机制来保障机密性。通过授权可以控制用户是否可以访问以及访问的程度。

（3）完整性

完整性是指信息在处理过程中不受到破坏、不会被修改。只有得到允许的用户才能修改数据，并可以判断数据是否被修改。即信息在存储或传输过程中保持不被修改、不被破坏和不丢失的特性。

（4）可靠性

可靠性是指系统在规定的条件下和规定的时间内，完成规定功能的概率。可靠性是网络安全最基本的要求之一。

（5）不可抵赖性

不可抵赖性（不可否认性）是指通信的双方在通信过程中，对于自己所发送或接收的消息不可抵赖；对出现的网络安全问题提供调查的依据和方法。

1.2 计算机网络安全的威胁

1.2.1 网络安全威胁的分类

网络安全威胁是指对网络设备的正常使用、网络中数据的完整性，以及网络正常通信等工作造成的威胁。这些威胁总体来说分为两大类：一类是主动攻击，如网络监听、黑客攻击，这些威胁是攻击者人为进行的；另一类就是被动攻击，如计算机病毒、木马、恶意软件等，这些威胁是用户通过某种途径感染的。

主动攻击和被动攻击有以下 4 种具体类型。

1．窃听

窃听是指攻击者通过非法手段对系统活动进行监视，并从中窃取有关安全方面关键的信息和服务，属于被动威胁，如图 1-1 所示。

2．中断

中断是指攻击者使网络系统的资源受损或不可用，从而使网络系统的通信服务不能进行，属于主动威胁，如图 1-2 所示。

图 1-1　窃听攻击方法

图 1-2　中断攻击方法

3．篡改

篡改是指攻击者未经授权对网络中的数据进行修改，从而使合法用户得到虚假的信息或错误的服务等，属于主动威胁，如图 1-3 所示。

4．伪造

伪造是指攻击者未经许可而在网络中制造出假的数据资源或网络服务，从而欺骗接收者，属于主动威胁，如图 1-4 所示。

图 1-3　篡改攻击方法

图 1-4　伪造攻击方法

1.2.2 计算机病毒的威胁

计算机病毒只是一段可执行的程序代码。它附在各种文件中，随着文件从一个用户复制给其他用户。目前来看，病毒传播的主要途径有：一是利用 U 盘和光盘传播；二是通过软件传播；三是通过网络，如电子邮件传播；四是靠计算机硬件等途径传播。而通过网络传播的病毒，无论是传播速度、破坏性，还是范围，都是其他传播方式所不能比拟的。

对于计算机病毒来说，防护可能永远只能是被动的。从 1986 年出现第一个计算机病毒

开始，计算机病毒经历了 3 个发展阶段：第一阶段为基于操作系统的传统病毒，主要有 CIH 病毒；第二阶段为基于网络的病毒，如冲击波、震荡波等；第三阶段，即目前面临的不再是简单病毒，而是包含病毒、木马、黑客攻击等多种攻击方法的网络威胁。计算机病毒的种类也在不断变化中，产生了许多攻击方法多样、破坏力不断增强的病毒变种。

1.2.3 木马程序的威胁

木马程序其实是一种远程控制程序，也称间谍程序或后门程序。木马程序一般是人为编程，它提供了用户不希望得到的功能，这些功能常常是有害的；它把有害的功能隐藏在可以公开的功能中，以达到掩盖真实目的的企图。

木马程序通过 UDP 建立与远程计算机的网络通信，使其可以通过网络控制本地计算机，在未经允许的情况下潜入用户的计算机，为下一步攻击创造条件。

但是需要说明的是，不是所有远程控制程序都是木马程序，如常用的 pcAnywhere、RemotelyAnyWhere 等都是正常用途的远程控制程序。

1.2.4 网络监听

网络监听是一种主动攻击，它是为了网络管理员管理网络设计的工具，用来监视网络状态和数据传输的，但是由于它具有截获网络数据的功能，常常被黑客使用从网络通信中获取所需的用户信息，从而分析用户的日常网络活动和习惯。

在网络中，当信息进行传播的时候，可以利用网络监听工具，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。在网络中，监听一般是在网关、路由器、防火墙一类的设备上，通常由网络管理员来操作。

1.2.5 黑客攻击

黑客攻击是未经授权就使用网络资源，且对网络设备和资源进行非正常的使用。黑客攻击是对计算机系统和网络的缺陷和漏洞的发现，以及针对这些缺陷和漏洞的攻击。这里所说的缺陷主要包括：软件缺陷、硬件缺陷、网络协议缺陷、管理缺陷等。

黑客攻击的主要目的如下。

1）控制目标主机，执行某些进程。危害主要表现在占用处理器大量时间，严重影响主机安全。

2）获取网络中重要数据和文件，达到暴露数据信息的目的。

3）获取超级用户权限。在网络中掌握了一台主机的超级用户权限，可以说掌握了整个网络，可以进行一些不被许可的操作。

4）对系统进行非法访问，可以随意修改、删除系统文件。

5）拒绝服务，使网络中服务无法正常进行。

黑客攻击中常使用的攻击方法包括：IP 地址欺骗、发送邮件攻击、网络文件系统攻击、网络信息服务攻击、扫描器攻击、密码破解、嗅探攻击、病毒攻击和破坏性攻击等。

1.2.6 恶意程序攻击

恶意程序也称为恶意软件或流氓软件，是指带有攻击意图的一段程序，它是对破坏或影

响系统运行的软件的统称。恶意程序介于病毒软件和正规软件之间，同时具备正常功能（下载、媒体播放等）和恶意行为（弹广告）。恶意软件主要包括：浏览器劫持、行为记录软件、自动拨号软件、网络钓鱼、垃圾邮件等。

1.3 网络安全威胁产生的根源

网络安全威胁若不及时得到有效遏制，产生的负面影响将会越来越大；为了最大限度地防范网络安全威胁，首先需要网络安全威胁产生的根源进行分析。

1.3.1 系统及程序漏洞

系统及程序漏洞是指应用软件或操作系统软件在编写时产生的逻辑错误，这个缺陷或错误可以被不法用户或者黑客利用。目前系统漏洞被发现的速度加快，攻击的时间变短。

对于这类漏洞和缺陷，人们能做的就是选择更安全的操作系统和软件，及时地更新操作系统或应用程序发布的补丁。

现在微软公司针对 Windows 操作系统已有了自动更新功能，人们只需开启自动更新功能，在保证连接互联网的情况下，Windows 操作系统会自动检测到最新的安装补丁。

具体操作如下。

1）在“控制面板”中双击“自动更新”功能选项（如图 1-5 所示）。

2）打开“自动更新”对话框，如图 1-6 所示，选择“自动”单选按钮，然后选择设置自动更新的频率。

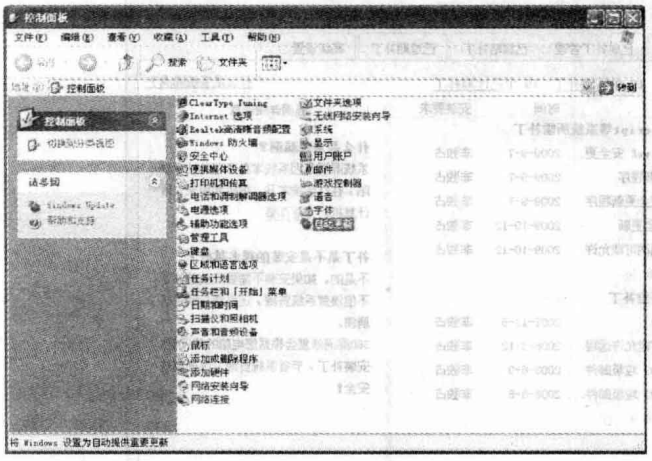


图 1-5 “自动更新”选项

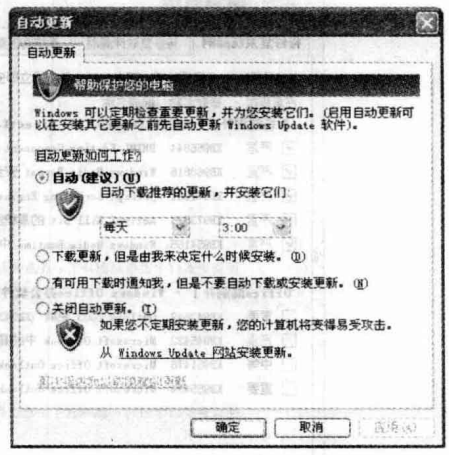


图 1-6 “自动更新”对话框

下面介绍几种常用的漏洞扫描工具。

1. 360 安全卫士

现在有一些安全工具可以帮助分析、扫描系统中存在的各种系统漏洞方面的安全隐患，360 安全卫士就是其中之一，如图 1-7 所示。它不仅可以自动搜索存在的系统漏洞，还可以自动搜索系统存在的其他漏洞，如注册表配置等。

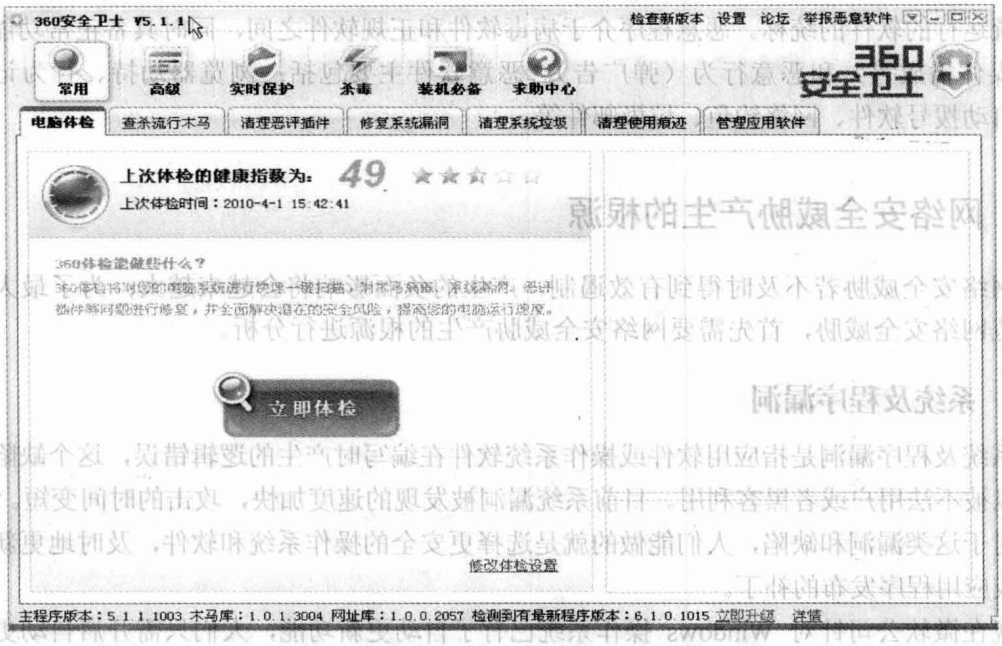


图 1-7　360 安全卫士界面

使用 360 安全卫士进行漏洞扫描的方法如下。

在 360 安全卫士的主界面中，选择“修复系统漏洞”选项卡，在图 1-8 中选择要修复的系统漏洞，单击“修复选中漏洞”按钮，就可以完成漏洞补丁的安装。

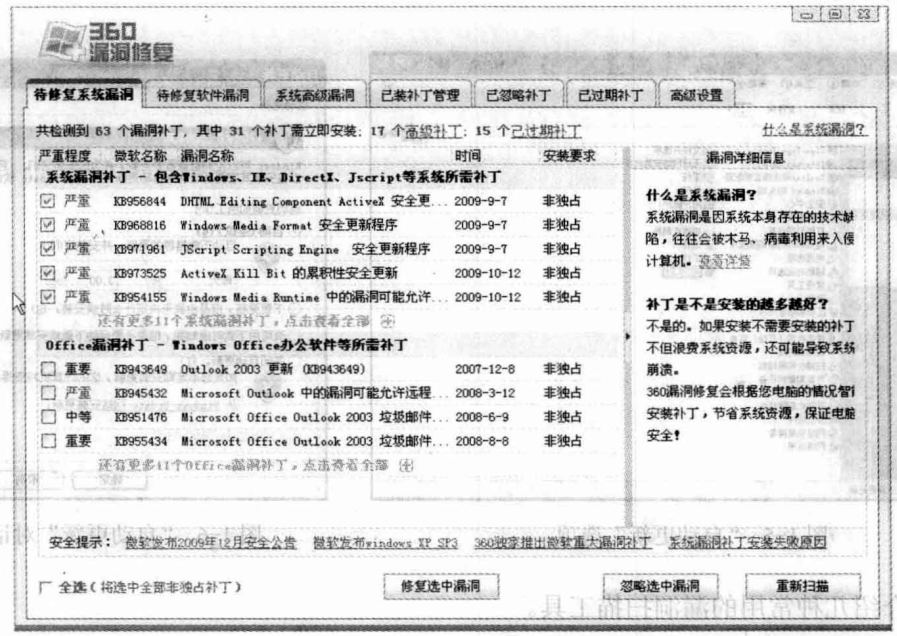


图 1-8　“待修复系统漏洞”选项卡

2. 瑞星漏洞扫描工具

瑞星漏洞扫描工具的使用方法如下。

1）运行瑞星杀毒软件得到如图 1-9 所示的界面。

图 1-9 瑞星杀毒软件运行界面

2）选择“安检”选项卡中的“扫描系统漏洞并升级补丁”选项，打开瑞星卡卡上网安全助手，单击“漏洞扫描与修复”按钮（如图 1-10 所示），在打开的“系统漏洞”选项卡中选择要修复的漏洞，单击“修复所选项”按钮即可。

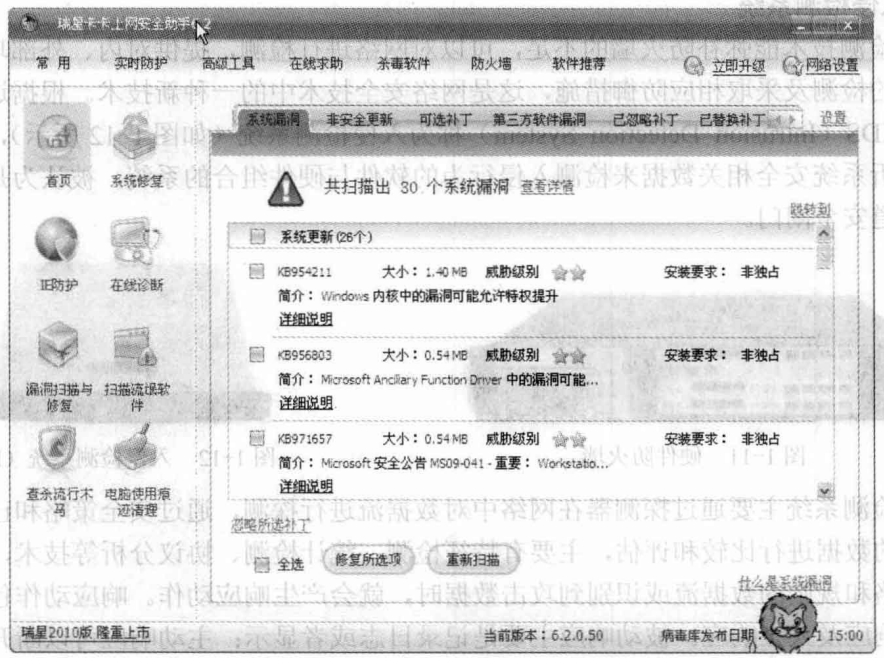


图 1-10 “系统漏洞”选项卡