软件职业技术学院“十二五”规划教材
——网络技术专业核心教材

网络安全技术

项目引导教程

主　编　鲁　立
副主编　任　琦　张松慧
主　审　王路群

中国水利水电出版社
www.waterpub.com.cn

软件职业技术学院“十二五”规划教材

——网络技术专业核心教材

网络安全技术项目引导教程

主　编　鲁　立

副主编　任　琦　张松慧

主　审　王路群

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

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。

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

本书所配电子教案可以从中国水利水电出版社网站和万水书苑上下载，网址为：http://www.waterpub.com.cn/softdown/和 http://www.wsbookshow.com。

图书在版编目（CIP）数据

网络安全技术项目引导教程 / 鲁立主编. -- 北京 : 中国水利水电出版社, 2012.6
软件职业技术学院“十二五”规划教材. 网络技术专业核心教材
ISBN 978-7-5084-9832-4

Ⅰ. ①网… Ⅱ. ①鲁… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2012)第117249号

策划编辑：杨庆川　责任编辑：陈洁　加工编辑：韩莹琳　封面设计：李　佳

书　名	软件职业技术学院“十二五”规划教材——网络技术专业核心教材 **网络安全技术项目引导教程**
作　者	主　编　鲁　立 副主编　任　琦　张松慧 主　审　王路群
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 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	北京蓝空印刷厂
规　格	184mm×260mm　16开本　16.25印张　414千字
版　次	2012年6月第1版　2012年6月第1次印刷
印　数	0001—3000册
定　价	29.80元

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，计算机网络系统是一个开放的系统，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的基础上，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 个项目，主要内容包括：

项目 1：计算机网络安全的基础知识、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。

项目 2：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。

项目 3：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。

项目 4：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。

项目 5：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。

项目 6：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。

项目 7：端口的概念、各种端口扫描技术的工作原理、常见端口扫描工具的应用方法、防范端口扫描技术的应用。

项目 8：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。

项目 9：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。

本书由鲁立任主编，任琦、张松慧任副主编，参加编写的还有武汉软件工程职业学院徐凤梅、刘颂、李安邦、严学军、何水艳、梁晓娅、杨威、王燕波以及武汉市中等职业艺术学校刘桢和武汉重工铸锻有限责任公司鲁芳。王路群教授担任主审。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

2012 年 3 月

21世纪 高职高专新概念规划教材

本套教材已出版百余种，发行量均达万册以上，深受广大师生和读者好评，近期根据作者自身教学体会以及各学校的使用建议，大部分教材已推出第二版，新版教材对原书内容进行了重新审核与更新，使其更能跟上计算机科学的发展、跟上高职高专教学改革的要求。

本套教材特色：

(1) 以《基本要求》和培养为编写依据，内容全面，结构合理，文字简练
(2) 采用“问题（任务）驱动”的编写方式，便于激发学习兴趣
(3) 精选实例并将知识点融于实例中，可读性、可操作性和实用性强
(4) 配有上机指导与实训教程，便于学生练习提高

21世纪 高职高专创新精品规划教材

引进高新技术，复合技术，培养创新精神和能力，教学资源丰富，满足教学一线的需求。

“教、学、做”一体化，强化能力培养
“工学结合”原则，提高社会实践能力
“案例教学”方法，增强可读性和可操作性

21世纪 高职高专规划教材

十一五 软件职业技术学院“十一五”规划教材

本套丛书特点：

(1) 以实际工程项目为引导来说明各知识点，使学生学为所用。
(2) 突出实习实训，重在培养学生的专业能力和实践能力。
(3) 内容衔接合理，采用项目驱动的编写方式，完全按项目运作所需的知识体系设置结构。
(4) 配套齐全，不仅包括教学用书，还包括实习实训材料、教学课件等，使用方便。

电脑美术与艺术设计实例教程丛书

21世纪高职高专教学做一体化规划教材

按照教育部2006年16号文件对高职高专的新要求，以服务为宗旨，以就业为导向，融“教、学、做”为一体，着重培养学生职业能力。

问题导入　　案例驱动　　理论够用　　突出实践

21世纪 中等职业教育规划教材

动漫游戏设计系列教程

美术基础+项目创意+程序设计+产品实训

目　　录

前言

项目 1　网络安全分析 …… 1

第一部分　项目学习引导 …… 1

1.1　网络安全的概念 …… 1

1.1.1　网络安全的定义 …… 1

1.1.2　网络安全的特性 …… 2

1.2　网络安全的威胁分析 …… 3

1.2.1　网络安全威胁的分类 …… 3

1.2.2　计算机病毒的威胁 …… 3

1.2.3　木马程序的威胁 …… 4

1.2.4　网络监听 …… 4

1.2.5　黑客攻击 …… 4

1.2.6　恶意程序攻击 …… 5

1.3　网络安全威胁的产生 …… 5

1.3.1　系统及程序漏洞 …… 5

1.3.2　网络安全硬件设备的问题 …… 8

1.3.3　安全防护知识的缺失 …… 9

1.4　网络安全策略 …… 9

1.4.1　网络安全策略原则 …… 9

1.4.2　几种网络安全策略介绍 …… 10

第二部分　知识拓展 …… 11

1.5　计算机网络安全的现状与发展 …… 11

1.5.1　计算机网络安全的现状 …… 11

1.5.2　计算机网络安全的发展方向 …… 12

项目 2　网络安全常用命令及协议分析工具 Sniffer 的应用 …… 14

第一部分　项目学习引导 …… 14

2.1　网络安全协议 …… 14

2.1.1　网络协议 …… 14

2.1.2　协议簇及行业标准 …… 15

2.1.3　协议的交互 …… 15

2.1.4　技术无关协议 …… 16

2.2　OSI 参考模型的安全体系 …… 16

2.2.1　计算机网络体系结构 …… 16

2.2.2　OSI 参考模型简介 …… 16

2.2.3　ISO/OSI 安全体系 …… 18

2.3　TCP/IP 参考模型的安全体系 …… 21

2.3.1　TCP/IP 参考模型 …… 21

2.3.2　TCP/IP 参考模型的安全体系 …… 22

2.4　常用网络协议和服务 …… 24

2.4.1　常用网络协议 …… 24

2.4.2　常用网络服务 …… 27

2.5　Windows 常用的网络命令 …… 28

2.5.1　ping 命令 …… 28

2.5.2　at 命令 …… 30

2.5.3　netstat 命令 …… 31

2.5.4　tracert 命令 …… 32

2.5.5　net 命令 …… 32

2.5.6　ftp 命令 …… 35

2.5.7　nbtstat 命令 …… 36

2.5.8　telnet 命令 …… 36

2.6　协议分析工具——Sniffer 的应用 …… 37

2.6.1　Sniffer 的启动和设置 …… 37

2.6.2　解码分析 …… 40

第二部分　典型项目实训任务 …… 42

2.7　典型任务 …… 42

2.7.1　典型任务一　常用网络命令实训 …… 42

2.7.2　典型任务二　Sniffer 软件的使用 …… 42

项目 3　病毒与木马的防护 …… 44

第一部分　项目学习引导 …… 44

3.1　计算机病毒基础知识 …… 44

3.1.1　计算机病毒的概念 …… 45

3.1.2　计算机病毒的发展史 …… 45

3.1.3　计算机病毒的特点 …… 46

3.2　计算机病毒的种类与传播方式 …… 47

3.2.1　常见计算机病毒 …… 47

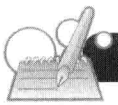
3.2.2　计算机病毒的种类 …… 47

3.2.3 计算机病毒的传播方式 …… 49
3.3 计算机病毒的防治方法 …… 49
3.3.1 普通计算机病毒的防治方法 …… 50
3.3.2 U 盘病毒的防治方法 …… 55
3.3.3 ARP 病毒的防治方法 …… 57
3.3.4 蠕虫病毒的防治方法 …… 60
3.4 木马的基础知识 …… 65
3.4.1 木马的概念 …… 65
3.4.2 木马的类型和功能 …… 65
3.4.3 木马的工作原理 …… 66
3.5 木马的防治方法 …… 67
3.5.1 被植入木马的计算机的表现 …… 67
3.5.2 木马查杀软件的使用 …… 67
3.5.3 手动检测和清除木马的常规方法 …… 70
第二部分 典型项目实训任务 …… 71
3.6 典型任务 …… 71
3.6.1 典型任务一 冰河木马的清除 …… 71
3.6.2 典型任务二 “广外男生”木马的清除 …… 73
3.6.3 典型任务三 “灰鸽子”木马的清除 …… 74
项目 4 数据加密与数字签名技术的应用 …… 76
第一部分 项目学习引导 …… 76
4.1 数据加密技术 …… 76
4.1.1 数据加密技术的基础知识 …… 76
4.1.2 数据加密的各种形式 …… 77
4.2 加密技术的算法 …… 80
4.2.1 古典加密算法 …… 80
4.2.2 现代加密算法 …… 82
4.3 数字签名技术 …… 84
4.3.1 数字签名技术的基础知识 …… 84
4.3.2 数字签名技术的原理 …… 85
4.3.3 数字签名技术的算法 …… 86
4.4 公钥基础架构（PKI） …… 86
4.4.1 PKI 的基础知识 …… 87
4.4.2 PKI 的工作原理 …… 87
4.4.3 证书颁发机构（CA） …… 87
4.4.4 数字证书 …… 88
第二部分 典型项目实训任务 …… 89
4.5 典型任务 …… 89
4.5.1 典型任务一 PGP 软件的使用方法 …… 89
4.5.2 典型任务二 EFS 的使用方法 …… 98
4.5.3 典型任务三 SSL 安全传输的使用方法 …… 104
项目 5 防火墙技术的应用 …… 116
第一部分 项目学习引导 …… 116
5.1 防火墙概述 …… 116
5.1.1 防火墙的基本准则 …… 117
5.1.2 防火墙的主要功能特性 …… 117
5.1.3 防火墙的局限性 …… 117
5.2 防火墙的实现技术 …… 118
5.2.1 数据包过滤 …… 118
5.2.2 应用层代理 …… 118
5.2.3 状态检测技术 …… 119
5.3 防火墙的体系结构 …… 119
5.3.1 双宿/多宿主机模式 …… 120
5.3.2 屏蔽主机模式 …… 120
5.3.3 屏蔽子网模式 …… 121
5.4 防火墙的工作模式 …… 121
5.5 防火墙的实施方式 …… 123
5.5.1 基于单个主机的防火墙 …… 123
5.5.2 基于网络主机的防火墙 …… 123
5.5.3 硬件防火墙 …… 124
5.6 瑞星个人防火墙的应用 …… 124
5.6.1 界面与功能布局 …… 124
5.6.2 常用功能 …… 125
5.6.3 网络监控 …… 128
5.6.4 访问控制 …… 132
5.6.5 高级设置 …… 135
5.7 ISA Server 2004 配置 …… 136
5.7.1 ISA Server 2004 概述 …… 136
5.7.2 ISA Server 2004 的安装 …… 136
5.7.3 ISA Server 2004 防火墙策略 …… 140
5.7.4 发布内部网络中的服务器 …… 145
5.7.5 ISA Server 2004 的系统和网络监控及报告 …… 150
5.8 iptables 防火墙 …… 154
5.8.1 iptables 中的规则表 …… 154

5.8.2 iptables 命令简介 …… 154
5.8.3 Linux 防火墙配置 …… 156
5.9 PIX 防火墙配置 …… 158
5.9.1 PIX 的基本配置命令 …… 160
5.9.2 PIX 防火墙配置实例 …… 163
第二部分 典型项目实训任务 …… 164
5.10 典型任务 ISA Server 2004 的使用 …… 164
项目 6 Windows Server 2003 的网络安全 …… 169
第一部分 项目学习引导 …… 169
6.1 Windows Server 2003 的安全特性 …… 169
6.1.1 用户身份验证 …… 169
6.1.2 基于对象的访问控制 …… 170
6.2 Windows Server 2003 系统安全的常规配置 …… 170
6.2.1 安装过程注意事项 …… 170
6.2.2 设置和管理账户 …… 170
6.2.3 设置目录和文件权限 …… 171
6.2.4 管理网络服务的安全 …… 171
6.2.5 关闭闲置端口 …… 172
6.2.6 配置本地安全策略 …… 173
6.2.7 配置审核策略 …… 177
6.2.8 保护 Windows 日志文件 …… 178
6.3 Windows Server 2003 访问控制技术 …… 179
6.3.1 访问控制技术概述 …… 179
6.3.2 配置 Windows Server 2003 访问控制 …… 179
6.4 Windows Server 2003 账户策略 …… 185
6.4.1 配置账户策略 …… 185
6.4.2 配置 Kerberos 策略 …… 187
6.5 Windows Server 2003 安全模板 …… 188
6.5.1 安全模板概述 …… 188
6.5.2 启用安全模板 …… 189
第二部分 典型项目实训任务 …… 191
6.6 典型任务 …… 191
6.6.1 典型任务一 文件及文件夹访问控制 …… 191
6.6.2 典型任务二 安全模板的使用 …… 192
6.6.3 典型任务三 配置复杂的口令和其他安全设置 …… 194
项目 7 端口扫描技术 …… 195
第一部分 项目学习引导 …… 195
7.1 端口概述 …… 195
7.1.1 TCP/IP 的工作原理 …… 195
7.1.2 端口概述 …… 197
7.1.3 端口分类 …… 197
7.2 端口扫描技术 …… 198
7.2.1 端口扫描概述 …… 198
7.2.2 常见的端口扫描技术 …… 199
7.3 扫描工具及应用 …… 200
7.3.1 扫描工具概述 …… 200
7.3.2 SuperScan 扫描工具及应用 …… 200
7.4 防御恶意端口扫描 …… 202
7.4.1 查看端口状态 …… 203
7.4.2 关闭闲置和危险端口 …… 205
7.4.3 隐藏操作系统类型 …… 207
第二部分 典型项目实训任务 …… 209
7.5 典型任务 …… 209
7.5.1 典型任务一 端口屏蔽 …… 209
7.5.2 典型任务二 NMAP 的使用 …… 214
项目 8 入侵检测系统 …… 217
第一部分 项目学习引导 …… 217
8.1 入侵检测概述 …… 217
8.1.1 入侵检测与入侵检测系统 …… 217
8.1.2 入侵检测系统模型 …… 218
8.1.3 入侵检测的工作过程 …… 218
8.2 入侵检测系统的分类 …… 219
8.2.1 基于检测对象划分 …… 219
8.2.2 基于检测技术划分 …… 219
8.2.3 基于工作方式划分 …… 220
8.3 入侵检测系统的部署方案 …… 220
8.3.1 基于主机的入侵检测系统部署 …… 221
8.3.2 基于网络的入侵检测系统部署 …… 221
8.3.3 常见入侵检测工具及应用 …… 222
8.4 入侵防护系统 …… 227
8.4.1 入侵防护系统的定义 …… 227
8.4.2 入侵防护系统的工作原理 …… 227
8.4.3 入侵防护系统的特性 …… 228
8.4.4 入侵防护系统的典型应用 …… 229

第二部分　典型项目实训任务 …… **230**
8.5　典型任务 …… 230
8.5.1　典型任务一　Snort 的安装 …… 230
8.5.2　典型任务二　Snort 规则的配置 …… 234
项目 9　无线局域网安全 …… 236
第一部分　项目学习引导 …… **236**
9.1　无线局域网 …… 236
9.1.1　无线局域网常见术语 …… 237
9.1.2　无线局域网的相关组件 …… 237
9.1.3　无线局域网的访问模式 …… 238
9.1.4　无线局域网的覆盖区域 …… 239
9.2　无线局域网的标准 …… 240
9.2.1　IEEE 802.11a …… 240
9.2.2　IEEE 802.11b …… 240
9.2.3　IEEE 802.11g …… 241
9.2.4　IEEE 802.11n …… 241
9.3　无线局域网安全解决方案 …… 242
9.3.1　无线局域网访问原理 …… 243
9.3.2　无线局域网的认证 …… 243
9.3.3　无线局域网的加密 …… 245
9.3.4　无线局域网的入侵检测系统 …… 247
第二部分　典型项目实训任务 …… **247**
9.4　典型任务　启用无线安全 …… 247
参考文献 …… 250

项目 1 网络安全分析



学习要点

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

学习情境

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。

第一部分　项目学习引导

1.1　网络安全的概念

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、正常地运行。

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，以及维护系统软件及数据库安全提出的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、正常地运行，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　网络安全的威胁分析

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的关键信息和服务，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。

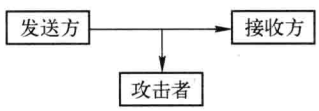


图 1-1　窃听攻击方法

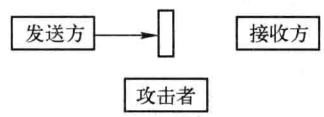


图 1-2　中断攻击方法

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。

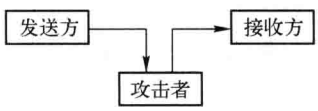


图 1-3　篡改攻击方法

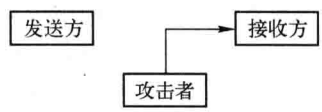


图 1-4　伪造攻击方法

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，它提供了合法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公开的功能中，以达到掩盖真实目的的企图。

木马程序一般通过UDP协议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。

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所设计的工具，用来监视网络状态和数据传输，但是由于它具有截获网络数据的功能，常常被黑客利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掘，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　网络安全威胁的产生

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，首先需要对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，攻击的时间也相应变短。

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。

其具体操作如下：

（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最后单击“确定”按钮。

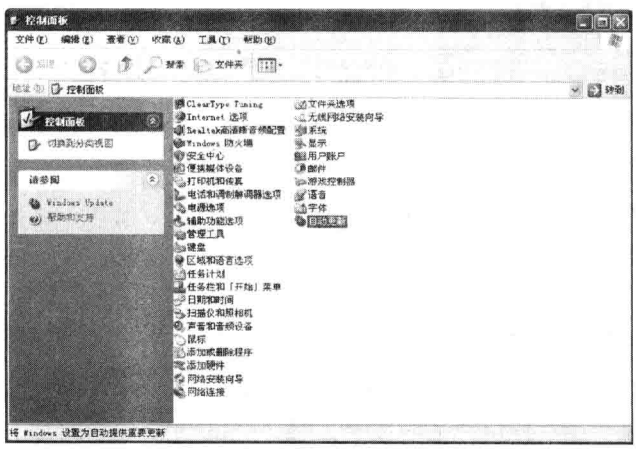


图 1-5　“自动更新”选项

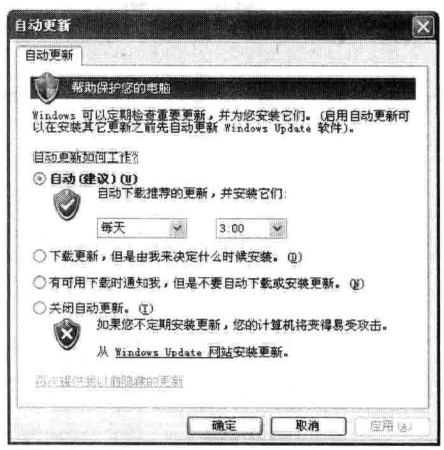


图 1-6　“自动更新”对话框

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，如图 1-8 所示，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。

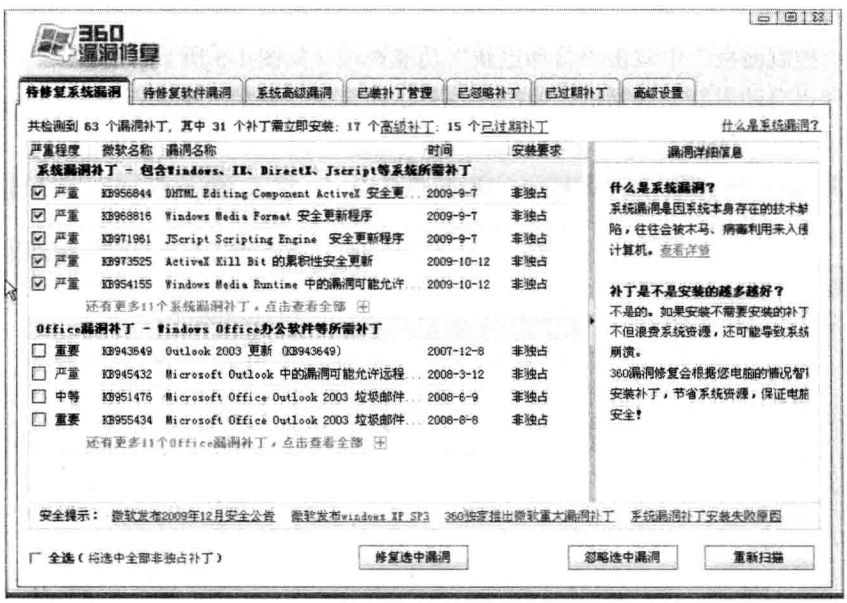


图 1-8 “待修复系统漏洞”选项卡

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，界面如图 1-9 所示。

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