21世纪高职高专规划教材

计算机系列

网络安全与维护

万振凯 苏 华 韩 清 编著

清华大学出版社
http://www.tup.tsinghua.edu.cn

北京交通大学出版社
http://press.bjtu.edu.cn

21世纪高职高专规划教材·计算机系列

网络安全与维护

万振凯　苏　华　韩　清　编著

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

计算机网络安全与维护是一门涉及计算机科学、网络技术、密码技术和应用数学等多种学科的综合性学科。计算机网络安全与维护已成为当今网络技术的一个重要研究课题。本书用通俗的语言介绍有关网络安全维护的实用方法，具体包括网络安全基础知识、操作系统安全漏洞及防范措施、入侵监测系统、黑客攻击与防范、防火墙技术等内容。

本书适合作为高等院校计算机及相关专业的教材，也适合于从事网络工程的初、中级工程技术人员参考。

版权所有，翻印必究。
本书封面贴有清华大学出版社激光防伪标签，无标签者不得销售。

图书在版编目（CIP）数据

网络安全与维护 / 万振凯，苏华，韩清编著.—北京：清华大学出版社；北京交通大学出版社，2004.6
（21 世纪高职高专规划教材·计算机系列）
ISBN 7-81082-207-1

Ⅰ.网… Ⅱ.①万… ②苏… ③韩… Ⅲ.计算机网络-安全技术-高等学校：技术学校-教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2004）第 009897 号

责任编辑：谭文芳
出 版 者：清华大学出版社　邮编：100084　电话：010-62776969
　　北京交通大学出版社　邮编：100044　电话：010-51686045，62237564
印 刷 者：北京东光印刷厂
发 行 者：新华书店总店北京发行所
开　本：185×260　印张：11.75　字数：297 千字
版　次：2004 年 6 月第 1 版　2004 年 6 月第 1 次印刷
书　号：ISBN 7-81082-207-1/TP·86
印　数：1～5000 册　定价：17.00 元

21世纪高职高专规划教材·计算机系列
编审委员会成员名单

主任委员 李兰友　边奠英

副主任委员 周学毛　崔世钢　王学彬　丁桂芝　赵　伟
韩瑞功　汪志达

委　　员 （按姓名笔画排序）

马　辉	万志平	万振凯	王永平	王建明
尤晓玮	丰继林	左文忠	叶　华	叶　伟
付晓光	付慧生	冯平安	江　中	佟立本
刘　炜	刘建民	刘　晶	曲建民	孙培民
邢素萍	华铨平	吕新平	陈小东	陈月波
李长明	李　可	李志奎	李　琳	李源生
李群明	李静东	邱希春	沈才梁	宋维堂
汪　繁	张文明	张权范	张宝忠	张家超
张　琦	金忠伟	林长春	林文信	罗春红
苗长云	竺士蒙	周智仁	孟德欣	柏万里
宫国顺	柳　炜	钮　静	胡敬佩	姚　策
赵英杰	高福成	贾建军	徐建俊	殷兆麟
唐　健	黄　斌	章春军	曹豫莪	程　琪
韩广峰	韩其睿	韩　劼	裘旭光	童爱红
谢　婷	曾瑶辉	管致锦	熊锡义	潘玫玫
薛永三	操静涛	鞠洪尧		

出 版 说 明

高职高专教育是我国高等教育的重要组成部分，它的根本任务是培养生产、建设、管理和服务第一线需要的德、智、体、美全面发展的高等技术应用型专门人才，所培养的学生在掌握必要的基础理论和专业知识的基础上，应重点掌握从事本专业领域实际工作的基本知识和职业技能，因而与其对应的教材也必须有自己的体系和特色。

为了适应我国高职高专教育发展及其对教学改革和教材建设的需要，在教育部的指导下，我们在全国范围内组织并成立了“21 世纪高职高专教育教材研究与编审委员会”（以下简称“教材研究与编审委员会”）。“教材研究与编审委员会”的成员单位皆为教学改革成效较大、办学特色鲜明、办学实力强的高等专科学校、高等职业学校、成人高等学校及高等院校主办的二级职业技术学院，其中一些学校是国家重点建设的示范性职业技术学院。

为了保证规划教材的出版质量，“教材研究与编审委员会”在全国范围内选聘“21 世纪高职高专规划教材编审委员会”（以下简称“教材编审委员会”）成员和征集教材，并要求“教材编审委员会”成员和规划教材的编著者必须是从事高职高专教学第一线的优秀教师或生产第一线的专家。“教材编审委员会”组织各专业的专家、教授对所征集的教材进行评选，对列选教材进行审定。

目前，“教材研究与编审委员会”计划用 2～3 年的时间出版各类高职高专教材 200 种，范围覆盖计算机应用、电子电气、财会与管理、商务英语等专业的主要课程。此次规划教材全部按教育部制定的“高职高专教育基础课程教学基本要求”编写，其中部分教材是教育部《新世纪高职高专教育人才培养模式和教学内容体系改革与建设项目计划》的研究成果。此次规划教材编写按照突出应用性、实践性和针对性的原则编写并重组系列课程教材结构，力求反映高职高专课程和教学内容体系改革方向；反映当前教学的新内容，突出基础理论知识的应用和实践技能的培养；适应“实践的要求和岗位的需要”，不依照“学科”体系，即贴近岗位群，淡化学科；在兼顾理论和实践内容的同时，避免“全”而“深”的面面俱到，基础理论以应用为目的，以必要、够用为度；尽量体现新知识、新技术、新工艺、新方法，以利于学生综合素质的形成和科学思维方式与创新能力的培养。

此外，为了使规划教材更具广泛性、科学性、先进性和代表性，我们希望全国从事高职高专教育的院校能够积极加入到“教材研究与编审委员会”中来，推荐“教材编审委员会”成员和有特色、有创新的教材。同时，希望将教学实践中的意见与建议及时反馈给我们，以便对已出版的教材不断修订、完善，不断提高教材质量，完善教材体系，为社会奉献更多更新的与高职高专教育配套的高质量教材。

此次所有规划教材由全国重点大学出版社——清华大学出版社与北京交通大学出版社联合出版。适合于各类高等专科学校、高等职业学校、成人高等学校及高等院校主办的二级职业技术学院使用。

21 世纪高职高专教育教材研究与编审委员会

2004 年 3 月

试读结束，需要全本PDF请购买 www.ertongbook.com

前　言

随着计算机及网络系统应用程度的扩展，计算机信息安全所面临的危险已经渗透到社会经济、军事技术、国家安全、知识产权、商业秘密乃至个人隐私等各个方面。尤其对于企业用户来说，能否保障网络安全的问题，更被提到了直接影响企业发展的高度。从全球范围来看，近年来企业因安全问题引起的损失成倍增长。有专家预言，网络安全问题将成为未来企业发展的瓶颈。影响计算机网络安全的因素很多，除了信息的不安全以外，层出不穷的网络病毒也给网络安全带来了威胁。此外，黑客对于网络安全的威胁也日益严重。当然，网络安全不仅是一个技术问题，也是一个社会问题和法律问题。要解决网络安全问题，必须采取技术和立法等多种手段进行综合治理。

本书作为高职高专教材，采用通俗的语言，围绕网络所涉及的安全问题讲述了相关的安全技术，各章内容如下：

第 1 章是网络安全的基础知识，包括网络安全简介、计算机安全的正式分级、信息系统安全的脆弱性。

第 2 章主要介绍操作系统的安全，包括漏洞、Windows 2000 的安全、Windows 2000 Server 的安全、UNIX 的安全。

第 3 章介绍入侵检测系统，包括入侵检测的概念、原理、模型等。

第 4 章介绍常见的黑客与防范，包括 IP 欺骗攻击与防范、Sniffer 与防范、端口扫描与防范、口令破解与防范、木马程序及其防范。

第 5 章介绍防火墙的概念，包括代理防火墙技术、数据包过滤网关、防火墙的选择。

天津工业大学软件学院李兰友教授对本书的编写提供了热情的指导和帮助，并提出了很多宝贵意见，特此表示感谢。

编　者

2004 年 5 月

目　录

第 1 章　网络安全的基础知识

本章要点：

- ☑ 计算机安全分级
- ☑ 信息系统安全的特点

1.1　网络安全简介

连接网络的计算机，特别是连接因特网的计算机比没有连接网络的计算机会出现更多的安全问题。如果网络安全性高可降低连接网络的风险，但就其性质而言，网络访问和计算机安全性是矛盾的：网络是一条数据高速公路，它专门用来增加对计算机系统的访问，而安全性却专门用来控制访问。因此提供网络安全性是在公开访问与控制访问之间的一种权衡举措。网络安全性一般是指对单台主机提供合适的安全性，而不是直接在网络上提供安全性。

近十年来，因特网已从一个只有数十个用户的小型网络发展到具有数百万用户的大网络。因特网的飞速发展降低了网络之间相互通信的信任度。对计算机安全性要求的增长是一个负效应，但这种发展并不是一件坏事。扩展后的网络可提供日益增加的服务，对大多数人来说，安全只是访问网络时需要考虑的一小部分。

随着网络的发展及其越来越社会化，网络的侵入也有所增加，而且容易夸大这种侵入的实际程度。对侵入的迹象反应过度会阻碍对网络的正常利用，因此一定要对症下药。有关网络安全性的最好建议是尊重常规，在 RFC1244 中很好地阐述了这一原则：“尊重常规是用来确定安全策略的最合适的准则，精心设计的安全性方案和机制，诚然是令人佩服的，也确实可以充分发挥作用，但应兼顾控制的简单性，即实施其方案时，在经济和时间上的投资也必须予以充分考虑。”

例如，防止和检测计算机通信线被渗透的技术，这种技术允许根据授权电话号码表来进行安全检查，也可提供追踪未被授权而企图存取的记录。这种识别已存在于目前一些计算机化的业务通信系统中，但只限于在那些由这种系统服务的公司的通信线中。

“信用卡终端”可提供防止篡改的方式，对于识别用户比通用的口令具有更高程度的可靠性。这种简单的硬件可产生软件不能伪造的信号，提高网络地址的安全程度。然而，计算机安全最重要的基础还是人为因素。要努力提高人们对于计算机安全的认识，特别要提高人们的道德品质，此外，也需要经常考核计算机人员，他们首先要提高安全意识，因为他们比普通用户更容易成为非法者。同时有必要澄清涉及计算机安全的责任问题，避免有人声称不知道如何防备危害计算机安全的行为而推卸责任。

1.2　计算机安全的正式分级

美国政府根据安全风险给计算机系统进行分级。几年前，美国国防部为计算机安全的不同级别制订了四个准则。橘皮书（正式名为“可信任计算机标准评估准则”）根据这四个准则

为计算机安全级别由低到高分为 D1、C1、C2、B1、B2、B3、A 七个级。

这些分类在商业软件中很少见，但认识这些分类有助于了解在一些系统中固有的安全风险，从而采取措施减少或排除这些风险。

1. D1 级

D1 级是计算机安全的最低级，整个计算机系统是不可信任的，硬件和操作系统很容易被入侵。D1 级计算机系统标准系统不要求用户进行登记（提供用户名）或使用密码（要求用户提供惟一的字符串来进行访问），即任何人都可以自由地使用该计算机系统。D1 级的计算机系统有 DOS，Windows 3.x 及 Windows 95（不在工作组方式中）和 Apple 的 System 7.x o。

2. C1 级

C1 级，即无条件安全防护（discretionary security protection）系统，要求硬件有一定的安全保护（如硬件有带锁装置，需要钥匙才能使用计算机）。用户在使用计算机系统前必须先登录。作为 C1 级保护的一部分程序或数据设立访问许可权限。常见的 C1 级兼容计算机系统有：UNIX 系统，XENIX，Novell 3.x 或更高版本和 Windows NT。

C1 级不能控制进入系统的用户的访问级别，所以用户可以将系统中的数据任意移动，可以控制系统配置，获取比系统管理员允许的更高权限，比如改变和控制用户名。

3. C2 级

C2 级对上述的 C1 级的不足之处做了补充，引进了受控访问环境（用户权限级别）的增强特性。这一特性以用户权限为基础，进一步限制用户执行某些系统指令。用户权限以个人为单位授权用户对某一程序所在目录的访问，如果其他程序和数据也在同一目录下，那么用户也将自动得到访问这些信息的权限。授权分组使系统管理员能够给用户分组，授予他们访问某些程序或访问分级目录的权限。

C2 级系统还采用了系统审计。审计特性跟踪所有的“安全事件”，如登录（成功的和失败的）和系统管理员的工作，例如改变用户访问权限和密码。需要注意的是： 通过区分安全事件接口管理员责任，审计特性提供一个附加保护级。例如，假设一个黑客成功地登录系统，审计可能不记录这一事件，但如果黑客接着进行改变密码或用户访问权限的操作，审计跟踪就将记录这一事件。如果它只是被作为一个安全事件而记录在案，则允许真正的管理员来识别这次未被发现自己离开的进攻（有些系统事件允许审计日志写成隐藏文件，使黑客更难销毁踪迹）。能够达到 C2 级的常见操作系统有：UNIX 系统，XENIX 和 Novell 3.x 或更高版本。

4. B1 级

B1 级又称符号安全防护（label security protection），支持多级安全。“符号”指网上的一个对象，该对象在安全防护计划中是可识别且受保护的。“多级”是指这一安全防护安装在不同级别（如网络、应用程序和工作站等），对敏感信息提供更高级的保护。安全级别分为保密和绝密级别。在计算机中有“搞特务活动的”成员，如国防部和国家安全局系统，在这一级，对象（如磁盘和文件服务器目录）必须在访问控制之下，不允许拥有者修改他们的权限。

B1 级安全措施的计算机系统随操作系统而定。政府机构和防御承担商们是 B1 级计算机系统的主要拥有者。

试读结束，需要全本PDF请购买 www.ertongbook.com

5. B2 级

B2 级又称为结构防护（structured protection），要求给计算机系统中所有对象加标签，而且给设备（如工作站、终端和磁盘驱动器）分配安全级别。如允许用户访问一台工作站，但不允许访问含有职员工资资料的磁盘子系统。

6. B3 级

B3 级又称为安全域（security domain），要求用户工作站或终端通过可信任途径连接网络系统，而且这一级采用硬件来保护安全系统的存储区。

7. A 级

这是橘皮书中的最高安全级。与前面提到的各级别一样，A 级包括了其下各级的所有特性，并且还附加一个安全系统受监视的设计要求，合格的安全个体必须分析并通过这个设计要求。A 级要求构成系统的所有部件来源必须有安全保证，以此保障系统的完善与安全。还必须担保在销售过程中系统部件不受损害，例如在 A 级设置中，一个磁盘驱动器从生产厂房直至销售到计算机房的过程中都被严密跟踪。

1.3　信息系统安全的脆弱性

黑客攻击网络已有十几年的历史。

网络黑客之所以能够得逞，是因为信息系统本身存在一些安全方面的脆弱性。

1. 操作系统安全的脆弱性

这种脆弱性表现在：操作系统的体系结构造成操作系统本身的不安全，这是计算机系统不安全的根本原因。操作系统的程序包括 I/O 的驱动程序与系统服务都可以用打补丁的方式进行动态链接。例如，UNIX 操作系统的许多版本升级开发都是采用打补丁的方式进行的。这种方法厂商可以使用，黑客同样也可以使用。这种动态链接是计算机病毒产生的好环境。一个靠渗透与打补丁开发的操作系统不可能从根本上解决安全问题，但操作系统支持程序动态链接与数据动态交换又是现代系统集成和系统扩展必备的功能，因此这是相互矛盾的。

操作系统不安全的另一个原因在于它可以创建进程，甚至支持在网络的结点上创建和激活远程进程，更重要的是，被创建的进程可以继承创建进程的权限，这一点与在网络上加载程序结合起来就构成了可以在远端服务器上安装“间谍”软件的条件。若再加上把这种间谍软件以补丁的方式“打”在一个合法的用户上，甚至是“打”在一个特权用户上，就可以使系统进程与作业的监视程序都监测不到间谍软件的存在。操作系统通常都提供守护进程，它们总在等待一些条件的出现，一旦有满足要求的条件出现，程序便继续运行下去。这样的软件都是黑客可以利用的。这里应该说明的是：关键不在于有没有守护进程，而在于这种守护进程在 UNIX 或 Windows NT 操作系统上是否具有与操作系统核心层软件同等的权力。

操作系统提供 RPC（Remote Procedure Call，远程过程调用），Debug 与 Wizard 服务，但这些服务本身也存在一些可以被非法用户利用的漏洞。许多研制系统软件的人员，他们的基本技能就是开发补丁程序和系统调试器。掌握了这两种技术，他们就有条件从事黑客可以从事的事情。

操作系统安排的无口令入口是为系统开发人员提供的便捷入口，但它也是黑客的通道。另外，操作系统还有隐蔽通道。

2. 计算机网络安全的脆弱性

Internet 和 Intranet 使用的 TCP/IP 协议及 FTP，E-mail，RPC 和 NFS（Network File System，网络文件系统）等都包含许多不安全的因素，存在许多漏洞。黑客通常采用源端口、源路由、Socks、TCP 序列预测或者使 RPC 进行直接扫描等方法对防火墙进行攻击。数据库管理系统的安全必须与操作系统的安全相匹配，例如 DBMS（Data Base Management System，数据库管理系统）的安全级别是 B2 级，那么操作系统的安全级别也应当是 B2 级。由于数据库的安全管理同样是建立在分级管理的基础之上的，因此 DBMS 的安全也是脆弱的。

世界上现有的信息系统绝大多数都缺少安全管理员、信息系统安全管理的技术规范，定期的安全测试与检查，更缺少安全监控。

我国许多企业的信息系统已经使用了许多年，但计算机的系统管理员与用户的注册还处于默认配置的状态。从某种意义上讲，缺少安全管理是造成系统不安全的最直接因素。因此，如果要提高系统的安全性，首要的任务就是找一位专门管理系统的人员维护和监督系统安全。

习题

1. 计算机安全级别由低到高分为 D1、C1、_____B2、B3、A 七个级。
2. C1 级又被称为_____，它兼容的系统包括_____。
3. 计算机系统不安全的根本原因是_____。
4. 黑客通常采用_____、_____、_____、_____或者使用远程过程调用（RPC）进行直接扫描等方法对防火墙进行攻击。
5. _____以用户权限为基础，进一步限制了用户执行某些系统指令。

第2章　操作系统安全

本章要点：

- ☑ 漏洞的概念
- ☑ Windows 操作系统中的漏洞及其解决方法
- ☑ UNIX 操作系统中的漏洞及其解决方法

2.1　漏洞的概念

在计算机网络安全领域中，“漏洞”是指硬件、软件或策略上的缺陷，这种缺陷导致非法用户未经授权而获得访问系统的权限或提高其访问权限。有了这种访问权限，非法用户就可以为所欲为，从而造成对网络安全的威胁。其实，每个平台无论是硬件还是软件都存在漏洞。

漏洞与后门是不同的，漏洞是难以预知的，后门则是人为故意设置的。后门是软硬件制造者为了进行非授权访问而在程序中故意设置的万能访问口令，这些口令无论是被攻破，还是只掌握在制造者手中，都对使用者的系统安全构成严重的威胁。

2.1.1　漏洞的类型

安全漏洞存在不同的类型，包括：允许拒绝服务的漏洞、允许有限权限的本地用户未经授权提高其权限的漏洞和允许外来团体（在远程主机上）未经授权访问网络的漏洞。

1. 允许拒绝服务的漏洞

允许拒绝服务的漏洞可能导致拒绝服务发生。“拒绝服务”是一种常见的恶作剧式的攻击方式，它使服务器忙于处理一些繁杂的任务，消耗大量的处理时间，而无暇顾及用户的合法请求。

允许拒绝访问的漏洞属于 C 类，是不太严重的漏洞。对于规模大的网络或站点，拒绝服务及其攻击造成的影响是有限的。然而对于规模小的站点，可能会遭到拒绝服务的重创。特别对于站点只是一台单独的计算机更是如此。这类漏洞存在于操作系统网络传送本身，是操作系统软件本身存在的漏洞。当存在这种漏洞时，必须通过软件开发者或销售商的弥补予以纠正。

拒绝服务攻击是一个人或多个人利用 Internet 协议组的某些方面拒绝其他用户对系统或信息进行合法访问的攻击。在 TCP SYN 攻击中，大量连接请求传给服务器，导致其请求信息被淹没。致使服务器反应很慢或信息不可到达，从而使用户无法正常工作。

另外还有其他形式的拒绝服务的攻击，例如某些拒绝服务攻击的实现可以针对个人而不是针对网络用户的。这种类型的攻击不涉及任何漏洞，而是利用了 Web 的基本设计。

并非每个拒绝服务攻击都需要在 Internet 发起，有许多在本地机甚至在没有网络环境的情况下发生的拒绝服务攻击。

2. 允许有限权限的本地用户未经授权提高其权限的漏洞

这是一种允许本地用户非法访问的漏洞，属 B 类。这类漏洞危险性很大。允许本地用户非法访问的漏洞所产生的影响是很大的。例如 Sendmail 这类程序中的漏洞特别值得重视，因为网络上所有的用户都有使用这个程序的基本权限，否则用户将无法发送邮件。因此 Sendmail 中的任何漏洞都是十分危险的。

允许本地用户非法访问的漏洞一般在多种平台的应用程序中发现，由应用程序中的一些缺陷引起。有些常见的编程错误导致这种漏洞的产生。

例如 Sendmail 问题。Sendmail 可能是世界上发送电子邮件最盛行的方法，是 Internet 上 E-mail 系统的中心。这个程序一般在启动时初始化，并且只要机器可用，它便可用。在其处于活动状态下，Sendmail（在端口 25）侦听网络空间上的发送和请求。

因为只有 root 有权启动和维护 Sendmail 程序，所以当其他有相同权限的用户要启动 Sendmail 的时侯，一般要求检验用户的身份。然而由于一个代码错误，Sendmail 在例程模式下可以以一种绕过潜入的方式激活。当绕过检查后，任何本地用户都可以在例程下启动 Sendmail。另外，在 8.7 版本中，Sendmail 收到一个 Signup 信号时会重启。此时调用 exec (2) 使Sendmail 重新开始操作（非 root 启动的 Sendmail）；这次重新操作被系统认为是由 root 引发的，即这次调用使 Sendmail 具有超级权限，因此入侵者利用这个漏洞非法获得超级用户权限，继而对系统实施攻击。

管理员可以利用允许本地用户非法访问的漏洞来检查出入侵者，特别是在入侵者没有经验的情况下更是如此。系统管理员通过运行强有力的登录工具，可使入侵者很难逃避检查，除非入侵者有较多的专业知识。

权限有限的本地用户在未经授权的情况下，通过各种手段提高其访问权限。这种攻击对系统安全威胁很大。

3. 允许未经授权远程主机访问网络的漏洞

这种允许远程用户未经授权访问的漏洞，属于 A 类，是威胁性最大的一种漏洞。这类漏洞从外界对系统造成严重的威胁。在许多情况下，如果系统管理员只运行了很少的日志，这些攻击可能不会被记录下来，使捉获更为困难。采用搜索器便可以检查这些漏洞。因此，尽管安全性程序员把这些漏洞包含进他们的搜索器程序中作为检查的选择，这些规则总是在漏洞出现一段时间后才被制定出来。

大多数的 A 类漏洞是由于较差的系统管理或设置有误造成的。典型的设置错误是在驱动器上任意存放的脚本例程。这些脚本有时会为网络入侵者提供一些访问权限，有时甚至提供超级用户访问权限。如 Test.cgi 文件的缺陷是允许网络入侵者读取 CGI 目录下的文件。

要补救该类漏洞，建议删掉这些脚本。例如，Novell 平台的一种 HTTP 服务器含有一个称为 Convert.bas 的例子脚本。这个用 BASIC 语言编写的脚本，允许远程用户读取系统上的任何文件。删除该脚本，即可避免远程用户读取系统上的任何文件。

入侵者利用脚本获取访问权，例如，Microsoft 的 IIS（Internet Information Server，因特网信息服务器）包含一个允许任何远程用户执行任意命令的漏洞。因为 IIS 中的 HTTP 将所有 .bat 或 .cmd 后缀的文件与 CMD 和 EXE 程序联系起来，入侵者如果能够执行 CMD 和 EXE 文件，那么就可以执行任何命令，读取任意分区的任意文件。

Netscape 通信和 Netscape 商业服务器也都有类似的漏洞。对于 Netscape 服务使用 BAT 或

CMD 文件作为 CGI 脚本则会发生类似的事情。

2.1.2　漏洞对网络安全的影响

随着网络经济时代的到来，网络将会成为一个无处不在、无所不用的工具。经济、文化、军事和社会活动将会强烈地依赖于网络。网络的安全和可靠性成为世界各国共同关注的焦点。而 Internet 的无主管性、跨国界性、不设防性、缺少法律约束性的特点，在为各国带来发展机遇的同时，也带来了巨大的风险。目前，Internet 和 Web 站点风险的无数事例已使一些用户坐立不安了，似乎到处都有漏洞，到处都是黑客的行迹。事实正是如此，各种系统漏洞正严重地影响着 Internet 的安全。

1. 漏洞影响 Internet 的可靠性和可用性

Internet 网络的脆弱性也是一种漏洞。Internet 是逐步发展和演变而来的，其可靠性和可用性存在很多弱点，特别是在网络规模迅速扩大，用户数目猛增，业务类型多样化的情况下，系统资源的不足成为一个瓶颈，而系统和应用工具可靠性的弱点也逐渐暴露出来。随着经济和管理活动对网络依赖程度的加深，网络的故障和瘫痪将会给国家、组织和企业造成巨大的损失。

2. 漏洞导致 Internet 上黑客入侵和计算机犯罪

黑客攻击早在主机终端时代就已经出现，随着 Internet 的发展，现代黑客则从以系统为主的攻击转变到以网络为主的攻击。形形色色的黑客和攻击者利用网络上的任何漏洞和缺陷进行攻击。例如，通过网络监听获取网上用户的账号和密码；监听密钥分配过程，攻击密钥管理服务器，得到密钥或认证码，从而取得合法资格；利用 UNIX 操作系统提供的守护进程的默认账户进行攻击，如 Telnet Daemon，FTP Daemon 和 RPC Daemon 等；利用 Finger 等命令收集信息，提高自己的攻击能力；利用 SendMail，采用 Debug，Wizard 和 Pipe 等进行攻击；利用 FTP，采用匿名用户访问进行攻击；利用 NFS 进行攻击；通过隐蔽通道进行非法活动；突破防火墙等。显然黑客入侵和计算机犯罪给 Internet 的安全造成了严重的威胁。

3. 漏洞致使 Internet 遭受网络病毒和其他软件的攻击

计算机病毒被发现以来，其种类以几何级数增长，而且病毒的机理和变种不断演变为检测和消除带来了更大的难度，成为计算机和网络发展的一大公害。计算机病毒破坏计算机的正常工作及信息的正常存储。严重时，可以使计算机系统陷于瘫痪。

总之，漏洞对于 Internet 安全性的影响是非常严重的。不采取措施对漏洞进行补救，将严重地制约 Internet 的发展。

2.2　Windows 2000

2.2.1　Windows 2000 漏洞集锦

Windows 2000 的强大的功能和全新的构架使它成为新一代服务器操作系统的主流，同

时也成为黑客攻击的对象。由于新的 Windows 2000 的全新构架很大程度都依赖于 AD（Active Directory，活动目录），这使得管理员急于适应新的操作系统和对原来的资料进行系统的迁移，而没有足够重视对 Windows 2000 的安全性问题。

Windows 2000 系统存在的漏洞要求管理员制定具体应对策略，以便在维护网络系统时尽量做到有的放矢。

1. 登录输入法漏洞

登录错误，即是常说的输入法漏洞。当启动 Windows 2000 进入登录验证的提示界面时，任何用户都可以打开各种输入法的帮助栏，并且可以利用其中具有的一些功能访问文件系统，这就可以绕过 Windows 2000 的用户登录验证机制，并且能以最高管理员权限访问整个系统。所以，这个漏洞的危害性是很大的。Windows 2000 系统自带的输入法中有这个漏洞的是：智能 ABC、微软拼音、内码、全拼、双拼、郑码。这个漏洞是首先要修补的漏洞，具体操作方法如下。

（1）把不需要的输入法删除掉，例如郑码等。

（2）毕竟不能把所有的自带输入法都删除，如果要使用有漏洞的输入法也可以把该输入法的帮助文件删除掉。这些帮助文件通常在 Windows 2000 的安装目录（如:C:\WINNT）的\help 目录下，对应的帮助文件是：

- WINIME.CHM 输入法操作指南；
- WINSP.CHM 双拼输入法帮助；
- WINZM.CHM 郑码输入法帮助；
- WINPY.CHM 全拼输入法帮助；
- WINGB.CHM 内码输入法帮助。

（3）微软公司针对这一问题发布了 MS00-069 安全公告，并在互联网上给出了简体中文 Windows 2000 和英文版 Windows 2000 的补丁。

2. NetBIOS 的信息泄漏

NetBIOS 的共享入侵是 NT 系统构架最常见的入侵手段。特别值得一提的就是 IPC$ Null session（空会话）在 NT 系统里是已知的安全隐患，虽然打上相应的补丁程序后，可以通过修改注册表来对其进行限制，但是入侵者可以使用如下命令来利用这个空会话，进而得到大量有用信息：

```
net use \\server\IPC$ "" /user:"" //此命令用来建立一个空会话
net view \\server                 //此命令用来查看远程服务器的共享资源
服务器名称            注释
命令成功完成。
net time \\server //此命令用来得到一个远程服务器的当前时间
nbtstat -A server //此命令用来得到远程服务器的 NetBIOS 用户名字表
NetBIOS Remote Machine Name Table
Name Type Status
NULL <00> UNIQUE Registered
NULL <20> UNIQUE Registered
INTERNET <00> GROUP Registered
```

试读结束，需要全本PDF请购买 www.ertongbook.com