巧学活用系列

巧学活用
网络安全与维护

丁文彦　主　编
张伟剑　纪文平　副主编

取材精巧　简单易学　选读灵活　技巧实用

★ 本书以实际应用为出发点
★ 介绍网络安全与防护基础知识及病毒/反病毒技术
★ 适合网络安全与维护人员阅读

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

巧学活用系列

巧学活用
网络安全与维护

丁文彦　主　编
张伟剑　纪文平　副主编

取材精巧　简单易学　选读灵活　技巧实用

★ 本书以实际应用为出发点
★ 介绍网络安全与防护基础知识及病毒/反病毒技术
★ 适合网络安全与维护人员阅读

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

网络安全是指网络系统中的硬件、软件及其数据受到保护，不因偶然或恶意的原因而遭受破坏、更改、泄露，使系统连续、可靠、正常地运行，网络服务不被中断。从其本质上来讲，网络安全就是网络上的信息安全。本书系统介绍了网络安全基础知识，TCP/IP 基础知识，网络攻击、检测与防范技术，操作系统的安全漏洞，计算机病毒与反病毒技术，防火墙技术，Web 服务的安全性，以及常见网络安全故障处理。

本书适合企事业单位从事网络安全与维护的技术、管理人员阅读，也可作为相关岗位职业培训的教学用书。

图书在版编目（CIP）数据

巧学活用网络安全与维护 / 丁文彦主编. —北京：电子工业出版社，2013.2
（巧学活用系列）
ISBN 978-7-121-19375-0

Ⅰ. ①巧… Ⅱ. ①丁… Ⅲ. ①计算机网络-安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2012）第 311961 号

责任编辑：张　剑（zhang@phei.com.cn）
印　　刷：北京中新伟业印刷有限公司
装　　订：北京中新伟业印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：880×1230　1/32　印张：4.25　字数：118 千字
印　　次：2013 年 2 月第 1 次印刷
印　　数：6000 册　　定价：18.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。
质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。
服务热线：（010）88258888。

巧学活用系列丛书编委会

丛书序

随着信息技术的飞速发展和计算机系统的广泛应用，办公自动化、电子商务、电子政务、ERP 等新的信息化技术层出不穷，信息化在各行业中扮演着日益重要的角色。为了适应信息化发展的需要，提高信息化技术的应用水平，我们组织编写了“巧学活用系列”丛书，内容涉及 Word、Excel、PPT、WPS、Windows、Linux、AutoCAD、Photoshop、多媒体处理、电脑维护、打印机维护、网络安全与防护、网管工具和 CISCO 网络典型配置。与传统的 IT 丛书相比较，“巧学活用系列”丛书突出的特点是“精巧、易学、灵活、实用”。

【精巧】本丛书并不追求大而全，只是精心挑选了与日常工作密切相关的方面加以介绍，以满足读者的实际需求，取材巧妙，篇幅适当。

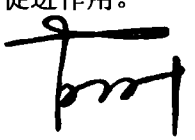
【易学】本丛书较少涉及理论知识，而是以通俗易懂的讲解方式来介绍解决实际问题的方法和技巧，简单易学。

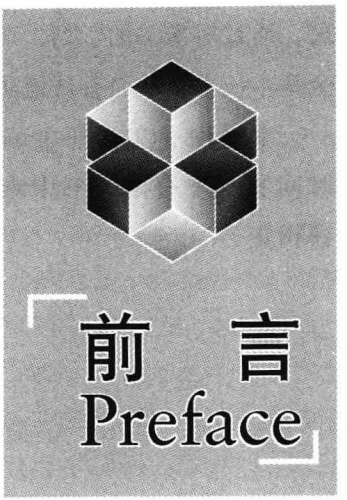
【灵活】本丛书涉及信息技术的多个方面，每个方面单独成册，没有先后次序。读者完全可以根据自己的实际需要，灵活选读自己感兴趣的内容，从而节省宝贵的时间。

【实用】本丛书旨在帮助读者解决日常工作中遇到的常见问题，所介绍的方法和技巧都是实践经验的归纳和总结，完全可以做到即学即用，实用性强。

从上述特点可以看出，“巧学活用系列”丛书不仅有助于职场人士提高工作效率和业绩，也对电脑爱好者提高自身技能大有裨益。

希望“巧学活用系列”丛书的出版，能对普及信息化技术的应用，提高广大读者的计算机使用水平，起到积极的促进作用。





近年来，伴随着科学技术及经济快速发展，互联网技术已经迅速覆盖了全球。目前，计算机、网络设备等的普及程度越来越高，为人们提供了极大的方便同时，我们也正受到日益严重的来自网络的安全威胁。网络和现实中充斥着众多的数据窃贼、网络黑客、病毒发布者，甚至系统内部的泄密者，他们为了各种利益，不惜手段地窃取可以为他们创造利益的数据信息。

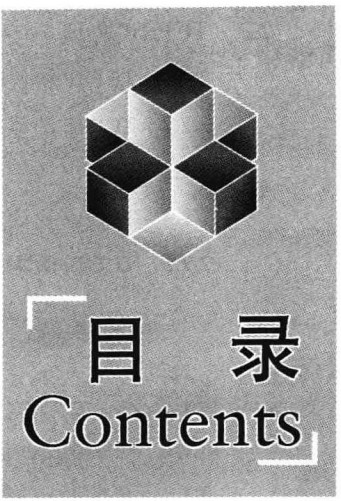
尽管我们正在广泛使用各种复杂的软件技术，如防火墙、代理服务器、侵袭探测器、通道控制机制，但是全球的黑客活动越来越猖獗，他们无孔不入，对社会造成了严重的危害。针对各种来自网上的安全威胁，如何才能确保网络信息的安全性，尤其是网络上重要的数据的安全性，已变得越来越重要。

本书系统介绍了网络安全基础知识，TCP/IP 基础知识，网络攻击、检测与防范技术，操作系统的安全漏洞，计算机病毒与反病毒技

术，防火墙技术，Web 服务的安全性，以及常见网络安全故障处理。通过对本书的学习，可以使读者提高网络安全意识，掌握网络安全基本技术，从而有效地防范网络黑客、病毒的入侵。

本书由丁文彦任主编，张伟剑和纪文平任副主编。由于编写时间和水平有限，书中难免有错误和不足之处，恳请广大读者批评指正。

编　者



第 1 章 网络安全基础知识

第 2 章 TCP/IP 基础知识

第 3 章 网络攻击、检测与防范技术

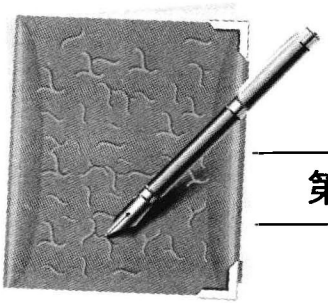
第 4 章 操作系统的安全漏洞

第5章 计算机病毒与反病毒技术

第6章 防火墙技术

第7章 Web服务的安全性

第8章 常见网络安全故障处理



第 1 章　网络安全基础知识

1.1　网络安全的重要性

安全性是互联网技术中很关键的问题，也是很容易被忽视的问题。许多公司或个人因为在使用网络的过程中没有意识到网络安全性的问题，直到受到了信息安全的威胁或直接造成重大损失，才开始重视和采取相应的安全措施。

例如，现在许多公司和个人使用网上银行系统，许多用户都认为网上银行系统是安全的，没有必要再去注意各种保障安全的措施。诚然，各个银行把自己的网上银行系统设计的相对比较安全，但是真正的威胁并不是网上银行系统的安全性问题，而是存在其他不安全因素，如本地计算机操作系统漏洞、各种软件漏洞、杀毒软件性能低、操作系统安全策略存在缺陷、使用者缺乏安全意识、系统内部存在不怀好意者、系统外部存在窃密者等，在网络上也存在计算机木马、病

毒、网络欺骗者、网络入侵者、钓鱼网站、恶意软件、灰色软件等不安全因素。这些不安全因素都有可能给用户造成惨重损失。

现在，网络上时刻都存在安全威胁，用户的信息安全没有出问题，并不是防护措施完善，而是用户的信息的价值不够高。因此，在网络广泛使用的今天，用户更应该了解网络安全，做好防范措施，尽可能保证不损失或减少损失。

1.2 安全事件

1983 年，凯文·米特尼克（Kevin David Mitnic）因被发现使用一台大学里的计算机擅自进入今日互联网的前身——ARPA 网，并通过该网络进入了美国五角大楼的计算机系统，而被判管教 6 个月。1988 年，凯文·米特尼克再次被执法当局逮捕，原因是 DEC 指控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，这次他被判处一年徒刑。

1995 年，来自俄罗斯的黑客 Vladimir Levin 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计算机系统来获利的黑客。1995 年，他侵入美国花旗银行并盗走 1000 万美元，然后他把账户里的钱转移至美国、芬兰、荷兰、德国、爱尔兰等地。

1999 年，梅利莎病毒使世界上 300 多家公司的计算机系统崩溃，该病毒造成的损失接近 4 亿美元，它是首个具有全球破坏力的病毒，该病毒的编写者戴维·史密斯（David Smith）在编写此病毒时年仅 30 岁。

2000 年，年仅 15 岁的绰号“黑手党男孩”的黑客在 2 月 6 日至 14 日成功侵入包括雅虎、eBay 和亚马逊在内的大型网站服务器，他成功阻止服务器向用户提供服务。

2001 年，中美撞机事件发生后，中美黑客之间发生的网络大战越演越烈。自 4 月 4 日以来，美国黑客组织 PoizonBox 不断袭击中国

网站。对此，我国的网络安全人员积极防御美方黑客的攻击。

2002年，英国著名黑客Gary McKinnon被指控侵入美国军方90多个计算机系统，造成约140万美元的损失，美方称此案为史上“最大规模入侵军方网络事件”。2005年7月14日，McKinnon表示，安全性差是他能够入侵美国国防部网站的主要原因。他面临“与计算机有关的欺诈”的指控，控方称，他的活动涉及美国陆军、海军、空军及美国航空航天局。由此可以看出，一方面，尽管这位黑客的主动入侵没有恶意，但是事实上对美国国防部的网络信息安全造成威胁，假如这位黑客出于某种目的，那么后果将无法估量；另一方面，即使网络技术很高的国家和部门也会被黑客成功入侵。

2005年6月17日，万事达信用卡公司称，大约4000万名信用卡用户的账户被一名黑客利用计算机病毒侵入，遭到入侵的数据包括信用卡用户的姓名、银行和账号，这都能够被用于盗用资金。如果该黑客真的用这些信息来盗用资金，不仅将给这些信用卡用户带来巨大的损失，而且侵犯了这些信用卡用户的个人隐私。

2007年，俄罗斯黑客成功劫持Windows Update下载服务器。

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。最关键的是，目前FBI还没破案，甚至据说连一个嫌疑人也没找到。

2009年，Heartland Breach信用卡失窃，有人称之为新版本TJX信用卡失窃案。这是迄今为止历史上最大一笔信用卡盗窃案。Heartland Payment Systems中的大量数据被泄露，涉及1.3亿信用卡和相关交易数据。Heartland因为接到Visa及MasterCard信用卡公司的通知，警告有可疑的信用卡交易活动而揭发事件，估计黑客在2008年已入侵该系统。Heartland Breach信用卡失窃案再一次警示人们安全威胁带来的风险——无论系统多么强大，都不能完全避免遭到恶意攻击。

1.3 黑客及其扮演的角色

- 充当工具：黑客非法入侵到国防、政府等一些机密信息系统，盗取国家的军事和政治情报，危害国家安全。
- 用于战争：通过网络，利用黑客手段侵入敌方信息系统，获取军事信息，发布假信息或病毒，扰乱对方系统等。
- 非法入侵商业系统，盗取商业信息，在商务、金融证券系统中进行诈骗、盗窃等违法犯罪活动，破坏正常的经济秩序。证券系统接二连三地发生盗用他人密码进行诈骗的案件，已经引起了网民的不安。
- 非法侵入他人的系统，获取个人隐私，以便利用这些信息进行敲诈、勒索或损害他人的名誉，阻塞电子邮箱，使系统瘫痪等。

1.4 计算机网络存在的安全问题

导致计算机网络信息安全受到威胁的根本原因在于网络存在安全问题。

1. 固有的安全漏洞

现在，新的操作系统或应用软件刚一上市，漏洞就会很快被找出来。没有任何一个系统可以排除漏洞的存在，想要修补所有的漏洞简直是不可能的。从 CERT（CarnegieMellon 大学计算机紧急事件响应队）那里可以找到相当全面的程序错误列表。另一个消息来源就是诸如 BugNet 或 NTBug traq 一类的新闻组。

- 缓冲区溢出：这是攻击中最容易被利用的系统漏洞。很多系统在不检查程序与缓冲区间变化的情况下，就接收任何长度的数据输入，把溢出部分放在堆栈内，系统还照常执行命令。这样破坏者便有机可乘，他只要发送超出缓冲区所能处理的长度的指令，系统便进入不稳定状态。假如破坏者特别

配置一串准备用做攻击的字符，他甚至可以进入系统的根目录，进而获得管理权限。

- 拒绝服务：拒绝服务攻击的原理是搅乱 TCP/IP 链接的次序。典型的 DOS 攻击会耗尽或损坏一个或多个系统的资源（CPU 周期、内存和磁盘空间），直至系统无法处理合法的程序。这类攻击的例子是 Synflood 攻击。发动 Synflood 攻击的破坏者发送大量的不合法请求要求链接，目的是使系统不胜负荷。其结果是系统拒绝所有合法的请求，直至等待回答的请求超时。

2. 合法工具的滥用

大部分系统都配备了用于改进系统管理及服务质量的工具软件，但遗憾的是，这些工具同时也会被破坏者利用，以收集非法信息及加强攻击力度。

例如，NBTSTAT 命令是用于给系统管理员提供远程节点信息的。但是，破坏者也用这一命令收集对系统有威胁性的信息，如区域控制软件的身份信息、NetBIOS 的名字、IIS 名甚至是用户名。这些信息足以被黑客用于破译口令。

另一个经常被利用的工具是网包嗅探器（PacketSniffer）。系统管理员用此工具来监控及分发网包，以便找出网络的潜在问题。若黑客要攻击网络，则先把网卡变成功能混杂的设备，截取经过网络的包（包括所有未加密的口令和其他敏感信息），然后短时间运行网包嗅探器，就可以有足够的信息去攻击网络。

3. 不正确的系统维护措施

系统固有的漏洞及一大堆随处可见的破坏工具大大方便了黑客的攻击，但无效的安全管理也是造成安全隐患的一个重要因素。当发现新的漏洞时，管理人员应仔细分析危险程度，并马上采取补救措施。

有时，虽然已经对系统进行了维护，对软件进行了更新或升级，但由于路由器及防火墙的过滤规则过于复杂，系统又可能会出现新的漏洞。所以，及时、有效地改变管理措施，可以大大降低系统所承担的风险。

4．低效的系统设计和检测能力

在不重视信息保护的情况下设计出来的安全系统会非常不安全，而且不能抵御复杂的攻击。建立安全的架构一定要从底层着手。这个架构应能提供实效性的安全服务，并且需要妥善地管理。

服务器的代码设计及执行也要进行有效管理。正如很多公开的漏洞报告指出，在输入检查不完全时，CGI BIN 是非常脆弱的。黑客可以利用这一漏洞发动拒绝服务攻击，非法获取敏感信息或篡改 Web 服务器的内容。低效的设计最后会产生漏洞百出的入侵检测系统，这样的系统非常危险，它不能提供足够的信息，就连已提供的信息都可能是不真实、不准确的。

5．人为的疏忽

人为的疏忽包括失误、失职、误操作等。这些可能是工作人员安全意识不到位，对安全的配置不当，不注意保密工作，密码选择不慎重，保密资料丢失等造成的。

6．人为的恶意攻击

这是网络安全的最大威胁，敌意的攻击和计算机犯罪就是这个类别。这种行为破坏性最强，可能造成极大的危害，导致机密数据的泄露。如果涉及金融机构，则很可能导致破产，也给社会带了震荡。

人为的恶意攻击有两种，即主动攻击和被动攻击。主动攻击有选择性地破坏信息的有效性和完整性。被动攻击是在不影响网络正常工作的情况下截获、窃取、破译重要机密信息。能够进行这些攻击行为的大多是具有很高的专业技能和智商的人员，一般需要相当的专业知识才能破解。