21世纪网络工程丛书——安全防卫系列

附CD

黑客防范技术揭秘

刘宝旭　许榕生等　编著

机械工业出版社
China Machine Press

21世纪网络工程丛书——安全防卫系列

黑客防范技术揭秘

刘宝旭　许榕生　等编著

机械工业出版社

本书针对网络攻击行为，系统介绍了网络信息安全的防护策略，提出了建立网络安全防护体系的具体思路，在对黑客防范技术与安全防护工具进行分析的同时，给出了切实有效的防范措施、安全服务介绍及安全建议，书中实例的讲解，可帮助读者提高应对黑客攻击的能力，并可从中获取所需的安全解决方案。全书共分 8 章，包括：网络安全策略、网络安全标准与体系、防范技术、安全防护工具、系统防护技术、防范措施、安全服务、安全建议。

本书适用于关心我国网络信息安全发展的各界人士，特别对广泛应用网络进行工作与交流的人员有很好的参考价值。针对本书的读者对象，书中讲述力求深入浅出，通俗易懂，注重科学性与实用性，并配有精选实例，供读者参考。

本书对网络信息安全领域的专业技术人员及信息时代的创业者都不失为一本实用的工具书。

图书在版编目（CIP）数据

黑客防范技术揭秘/刘宝旭等编著. —北京：机械工业出版社，2002.2
(21 世纪网络工程丛书——安全防卫系列)
ISBN 7-111-09806-4
Ⅰ. 黑… Ⅱ. 刘… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08
中国版本图书馆 CIP 数据核字（2002）第 000247 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：边 萌 王琼先
责任印制：路 琳
中国建筑工业出版社密云印刷厂印刷·新华书店北京发行所发行
2002 年 2 月第 1 版第 1 次印刷
1000mm×1400mm B5 · 8.375 印张 · 322 千字
0 001—5 000 册
定价：29.00 元 (含 1CD)
凡购本书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话（010）68993821、68326677-2527

序　言

国庆与中秋双节前夕，作者将其姊妹篇《黑客防范技术揭秘》和《黑客攻击技术揭秘》书稿交给了我，委托我为这两本新作作序。月圆长假本想处理些其他任务的我，只好遵托响应了这个优先中断。端坐屏前逐章拜读，书中的描述和现实的世界不时显现心头。

攻与防自古为兵家研习的方略，信息化发展的今天却依然困扰着原本欣喜的世人。信息革命带给人们的遐想，像一轮中天的明月如歌如赋。但“911”纽约世贸双子星在暴力和恐怖面前的消失使人们从遐想中清醒。世界未到大同时，太平难自空中降。我们必须为信息革命付出代价，认真对付阻碍信息化健康发展的“无知”、“恐怖”与“暴力”。

为什么像书中提到的那样，我们的信息系统存在那么多的漏洞？看来本质上还是我们的“无知”。人类认识真理和正确地进行社会实践的过程是一个求极限的趋近过程。在这个规律的“惩罚”下，再能干的人编写的程序，设计的电路，免不了依然存在错误。记得在一次国际会议上 IBM 的一位专家说，平均一千行源程序中就可能存在一处错误（bug），而在这个国际会议的另一次年会上，应用密码学的作者布鲁斯·斯奈尔声称还要多，平均达到 5 到 15 个之多。今天操作系统和应用程序的规模动辄上百万行，上千万行。出错的可能性实在太大了，难怪我们用计算机时常莫名其妙地“死掉”。

无知不仅仅伴随着设计和制造者，它更是使用者的隐患。初为电子公民，对许多知识、技能、道德、规则了解不多或没认真遵循，不仅常会坑害自己，还会波及他人。

除了以上内因外，造成信息安全事件层出不穷的外因是因为世界上存在犯罪、竞争、斗争、战争。这些因素驱使一些人和组织，甚至国家，花费大力去发掘信息系统客观存在的漏洞，千方百计钻进未被授权的系统去窥视他人，欺骗、偷窃、破坏，制造信息世界的恐怖和暴力。他们不但利用系统的漏洞，还会有意设置一些后门、木马，以便长期控制他人，达到其利己的目的。

人类追求的真善美，伴随了这些不协调的假恶丑，使数字化的信息空间如一轮明月被乌云遮盖。

为了和这些假恶丑斗争，必须加强对信息安全保障的研究。这几年来国内出版了不少有关信息安全的译著。也出现了一批我国科学技术工作者自己撰写的书籍。这个姊妹篇就是这批书籍中的两本。两本书从攻和防两个角度介绍论述了同一个问题的两个侧面，使人们读起来更有味道。这套书的特点是：不但论述了技术，而且论述了管理；不但论述了原则，而且论述了实践技巧；同时还给出了许

多实例，从宏观和微观两个方面给人以启示。其中不乏作者们自己的亲身实践经验与体会，确可使人开篇有益。

愿更多的人们投身于对假恶丑的斗争，愿信息化社会的发展持续健康，让我们用自己的双手送别明月，迎接信息革命成功的一轮朝阳。

中国科学院研究生院
信息安全国家重点实验室
赵战生

2001 年国庆节于北京

前 言

目前国内业界人士已普遍达成共识：我们的世界正在演变为一个电子化的世界（E-World），所有的信息正在全面数字化，电子世界中四通八达的网络把人们联系在一起。在网络上，天涯变为咫尺，物理上的距离几乎都消弭于无形，人们可以运筹帷幄，决胜于千里之外。统计显示，因特网发展的速度超过了它以前的所有其他技术。无线电广播问世 38 年后拥有 5000 万听众，电视诞生 13 年后拥有同样数量的观众，而因特网从 1993 年对公众开放到拥有 5000 万用户只花了四年时间。目前，全世界因特网使用者超过 2 亿，预计到 2001 年年底因特网使用者将达 10 亿。然而，伴随着网络的迅猛发展，一系列的问题也随之而来，如何建设和发展网络？在我国有没有条件推广使用？其制约因素是什么……

我国的信息化进程，经历了单机、专用局域网、广域网到 Internet 的发展阶段。“金”系列工程许多都是利用物理的公用网络条件实施逻辑的专业和行业应用，以 Internet 为代表的信息网络正在成为未来全球信息系统的最重要的基础设施。这一发展变化使我们的信息安全观念必须有所拓展。

网络由智能设备构成，而智能设备将按照制造者或设计者的意图执行使用者或拥有者的指令。当制造者与所有者的利益发生冲突时，智能设备会站在哪一边是由制造者在制造时确定的。不能保证制造者的意图全部向使用者或拥有者公开，这包括个别设计雇员未经允许偷偷留下的后门和生产测试需要的附件。比如，一个保密的 CPU 使外界无法存储芯片内的某保密字，然而，设计者不公开的测试端口保留了对此保密字的存取。

网络拥有较为复杂的设备和协议，保证复杂的系统没有缺陷和漏洞是不可能的。如 Windows NT 系统，没有任何人能全部地了解其每一细节，随着用户的增加，其 BUG 也不断被发现。Intel 的 MMX 芯片经过无数专家审核仍存在设计上的错误。系统设计的后门随着系统的复杂越来越难于发现。系统和软件工程学也告诉我们，大型系统将永远有令用户不满意的地方，直到此系统被停止使用，即生命终止。

网络的地域分布使得安全管理难于顾及网络联接的每个角落。

随着工业化进程，任何网络拥有者或用户都不能单靠自己完全研制、开发、设计和制造网络的所有设备，组织大规模的开发和研制也无法保证每个人都忠于职守。网络是一个社会，社会大了，各种人都会有，有守法的、也有表面守法背后违法的。

没有人能证明网络是安全的。网络安全问题变为了一个风险管理问题，安全性成为概率意义上无法准确定义的指标。合理地增加安全投资，增加正确的安全

设备，改善安全管理无疑可以提高网络的安全性能。

从攻击者的角度看，由于网络的复杂性与协议的多样性，攻击的投入越大，找到攻击入口和网络弱点的可能性也越大，攻击成功的机会也越大。如果攻击成功后的收益很大，攻击者一般会投入较大力量的。

网络安全没有保障。使用网络带来效益也带来风险，正确增加安全投入就减少了风险，而错误的投入就如同投资迷信和神汉一样，不能减少风险。但在某阶段侥幸没有损失的可能性也是存在的。

网络安全的威胁同时来自于内外两个方面。有一段时间，人们把初期的防火墙保障安全的功能强调到了不适当的地位，给人一个错觉，好像安全威胁全部来自于诸如 Internet 这些公众环境，这其实是一种误解。

对我国而言，自 1994 年因特网发展至今，已发生多次规模性的因黑客攻击造成的网络安全事件，第一次发生于 1997 年印尼排华反华事件后；第二次发生于 1999 年 5 月，北约轰炸中国驻南联盟大使馆后；第三次发生在 1999 年 7 月李登辉公然抛出“两国论”之后；第四次发生在 2000 年初日本右翼公然为南京大屠杀翻案后；第五次发生在 2001 年 2、3 月间，由于日本三菱事件、日航事件、松下事件、教科书事件、《台湾论》等引起；第六次发生在中美“撞机事件”后，美国电脑黑客组织——POIZONBOX 的挑衅行为激怒了许多中国的电脑黑客引起，这次攻击事件在 2001 年 5 月 4 日左右达到高潮。在这次世界范围大规模的攻击事件过程中，我国共有千余个站点受到攻击和破坏，美国也有数百个网站被攻击破坏，这是近年来中国网络安全受到的最大挑战。

面对这些频频发生的安全挑战，人们不禁要问：我们的网络安全吗？中国的网络安全之路究竟应该怎样走？这需要安全法规、法律、策略、技术、工具、措施、服务等各方面的配合，在未来的信息社会，要掌握自己的命运，就必须在网络安全防护技术、网络安全人才和相关法律政策上构建自己的网上长城，建筑自己的安全体系，只有这样，才能保证国家信息系统处于安全状态，“信息化”才能真正为中国腾飞带来希望。

编者的话

本书取名《黑客防范技术揭秘》，其宗旨是注重知识性和实用性。作者在回顾网络信息安全发展和参与网络安全防范技术具体研究与实践的基础上，针对网络攻击行为，系统介绍了网络信息安全的防护策略，提出了建立网络安全防护体系的具体思路，在对黑客防范技术与安全防护工具进行分析的同时，给出了切实有效的防范措施、安全服务介绍及安全建议，在文字的表述上力求深入浅出、不落俗套。本书第 1 章在结合实际工作经验的基础上，总结了黑客防范技术的核心环节——网络安全策略，并给出几个实例说明。第 2 章系统地论述了网络安全标准与体系，以使读者对网络安全标准和黑客防范体系有一个整体认识。第 3～8 章，针对具体防范技术、安全防护工具、系统防护技术、防范措施、安全服务、安全建议几个方面，分别进行介绍和说明，叙述尽量浅显易懂，具有教科书性质，使读者能够循序渐进地了解黑客入侵防范的关键技术与方法，提高安全防护意识，应用于实际工作中。该书对于网络信息安全专业技术人员、网络安全管理人员、网络使用者及信息时代的创业者都不失为一本实用的工具书，并将引导广大读者登堂入室、步入佳境。本书内容翔实，颇具启发性。对于读者和网络信息安全相关从业人员来说，应学会充实、修正原有的知识和材料，这样才能保证每个人都可以共享他人的经验。我们在本书中也尝试着这样做。

本书由刘宝旭主笔，许榕生、曾勇、杨泽明、吴海燕、郭立生、孙笑庆、冉敏、任金强、雷乃旺、崔石、毕学尧、洪立强、安德海、吴春珍、丁宇征、胡季敏、钱桂琼、李雪莹、梁志广等参加了部分内容的编写。全书由许榕生统稿。

感谢中科院高能所计算中心网络安全课题组、国家计算机网络入侵防范中心、北京金元龙脉信息科技有限公司、北京中科网威信息技术有限公司、福建省海峡信息技术有限公司的各位同仁在提供资料、论文和录入编排方面所做的工作。同时感谢边萌、王琼先两位责任编辑在成书过程中给予我们的指导和建议。

在本书写作过程中还得到了各方面专家和技术人员的支持和帮助，特别是参考引用了《中国计算机报》、《计算机世界》和许多互联网站上有关作者、编者、读者发表的观点和素材，恕不一一列举，在此一并表示感谢。

本书的创意要求坚持特色，集思广益。但由于时间仓促，错误与不妥之处在所难免，敬请广大读者谅解，并欢迎批评指正。

编者

目 录

网络安全策略

- 网络安全目标
- 制定网络安全策略的原则
- 安全策略举例
- 安全应急处理对策

第1章 网络安全策略

要制定一个好的网络安全策略，需要有一个明确的网络安全目标，下面先对网络安全目标做一描述。

1.1 网络安全目标

通俗地说，网络信息安全与保密主要是指保护网络信息系统，使其没有危险、不受威胁、不出事故。从技术角度来说，网络信息安全与保密的目标主要表现在系统的保密性、完整性、真实性、可靠性、可用性、不可抵赖性等方面。

1.1.1 可靠性

可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定功能的特性。可靠性是系统安全的最基本要求之一，是所有网络信息系统建设和运行的目标。网络信息系统的可靠性测度主要有三种：抗毁性、生存性和有效性。

抗毁性是指系统在人为破坏下的可靠性。比如，部分线路或节点失效后，系统是否仍然能够提供一定程度的服务。增强抗毁性可以有效地避免因各种灾害（战争、地震等）造成的大面积瘫痪事件。

生存性是指系统在随机破坏下的可靠性。生存性主要反映随机性破坏和网络拓扑结构对系统可靠性的影响。这里，随机性破坏是指系统部件因为自然老化等造成的自然失效。

有效性是一种基于业务性能的可靠性。有效性主要反映在网络信息系统部件失效的情况下，满足业务性能要求的程度。比如，网络部件失效虽然没有引起连接性故障，但是却造成质量指标下降、平均延时增加、线路阻塞等现象。

可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见。软件可靠性是指在规定的时间内，程序成功运行的概率。人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演重要角色，因为系统失效的大部分原因是人为差错造成的。人的行为要受到生理和心理的影响，受到其技术熟练程度、责任心和品德等素质方面的影响。因此，人员的教育、培养、训练和管理以及合理的人机界面，是提高可靠性的重要方面。环境可靠性是指在规定的环境内，保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

1.1.2 可用性

可用性是网络信息可被授权实体访问并按需求使用的特性。即网络信息服务在需要时，允许授权用户或实体使用的特性；或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的

安全性能。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。

可用性还应该满足以下要求：身份识别与确认、访问控制（对用户的权限进行控制，只能访问相应权限的资源，防止或限制经隐蔽通道的非法访问。包括自主访问控制和强制访问控制）、业务流控制（利用均分负荷方法，防止业务流量过度集中而引起网络阻塞）、路由选择控制（选择那些稳定可靠的子网、中继线或链路等）、审计跟踪（把网络信息系统中发生的所有安全事件信息存储在安全审计跟踪之中，以便分析原因，分清责任，及时采取相应的措施。审计跟踪的信息主要包括：事件类型、被管客体等级、事件时间、事件信息、事件回答以及事件统计等方面的信息）。

1.1.3 保密性

保密性是网络信息不泄露给非授权的用户、实体或过程，或供其利用的特性。即，防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

常用的保密技术包括：防侦收（使对手侦收不到有用的信息）、防辐射（防止有用信息以各种途径辐射出去）、信息加密（在密钥的控制下，用加密算法对信息进行加密处理。即使对手得到了加密后的信息，也会因为没有密钥而无法读懂有效信息）、物理保密（利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露）。

1.1.4 完整性

完整性是网络信息未经授权不能进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成和正确存储与传输。

完整性与保密性不同，保密性要求信息不泄露给未授权人，而完整性则要求信息不致受到各种原因的破坏。影响网络信息完整性的主要因素有：设备故障、误码（传输、处理和存储过程中产生的误码，定时的稳定度和精度降低造成的误码，各种干扰源造成的误码）、人为攻击、计算机病毒等。

保障网络信息完整性的主要方法如下。

协议：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段。

纠错编码方法：由此完成检错和纠错功能。最简单和常用的纠错编码方法是奇偶校验法。

密码校验方法：它是抗篡改和传输失败的重要手段。

数字签名：保障信息的真实性。

公证：请求网络管理或中介机构证明信息的真实性。

1.1.5 不可抵赖性

不可抵赖性也称作不可否认性，在网络信息系统的信息交互过程中，确信参与者的真实同一性。即，所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送的信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

1.1.6 可控性

可控性是对网络信息的传播及内容具有控制能力的特性。

概括地说，网络信息安全与保密的核心，是通过计算机、网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储的消息的保密性、完整性、真实性、可靠性、可用性、不可抵赖性等。

1.2 制定网络安全策略的原则

网络安全策略是指为了保护网络不受来自网络内外的各种危害而采取的防范措施的总和，是针对网络的实际情况(被保护信息价值、被攻击危险性、可投入的资金)，在网络管理的整个过程中，具体地对各种网络安全措施进行取舍。网络的安全策略可以说是在一定条件下的成本和效率的平衡。虽然网络的具体应用环境不同，但在制定安全策略时应遵循一些总的原则，主要包括如下内容。

1.2.1 适应性原则

安全策略是在一定条件下采取的安全措施，其必须和网络的实际应用环境相结合。通常，在一种情况下实施的安全策略到另一环境下未必适合，例如：校园网环境一般情况下允许匿名登录，而企业网络的安全策略是不允许匿名登录的。

1.2.2 动态性原则

安全策略又是在一定时期采取的安全措施。由于用户在不断增加，网络规模在不断扩大，网络技术本身的发展变化也很快，各种漏洞和隐患不断被发现，而安全措施又是防范性的、持续不断的，所以，制定的安全措施必须不断适应网络发展和环境的变化。

1.2.3 简单性原则

网络用户越多，网络管理人员越多，网络拓扑结构越复杂，采用的网络设备种类和软件种类越多，网络提供的服务和捆绑的协议越多，出现安全漏洞的可能

性就越大，出现安全问题后找出问题原因和责任者的难度就越大。安全的网络是相对简单的网络。所以，可以这样说，世界上最不安全的网络应该是 Internet。

1.2.4 系统性原则

网络安全管理是一个系统化的工作，必须考虑到整个网络的方方面面。也就是在制定安全策略时，应全面考虑网络上各类用户、各种设备、各种情况，有计划、有准备地采取相应的策略。任何一点疏漏都会造成整个网络安全性的降低。

1.2.5 最小授权原则

从网络安全的角度考虑问题，打开的服务越多，可能出现的安全漏洞就会越多。“最小授权”原则指的是网络中账号设置、服务配置、主机间信任关系配置等应该设为网络正常运行所需的最小限度。关闭网络安全策略中没有定义的网络服务并将用户的权限配置为策略定义的最小限度、及时删除不必要的账号等措施可以将系统的危险性大大降低。在没有明确的安全策略的网络环境中，网络安全管理员通过简单关闭不必要或者不了解的网络服务、删除主机信任关系、及时删除不必要的账号等手段，也可以将入侵危险降低一半以上。

当前最为简单、流行的攻击手段包括主机扫描、端口扫描、用户扫描、猜口令、缓冲区溢出等一系列手段，所以应注意如下几点。

关闭“finger”服务可以减少暴露账号和登录情况的威胁，也就是减少了攻击者猜口令成功的可能性。

关闭“r”系列可以减少远程攻击和由主机信任关系引起的连锁反应以及电子欺骗等的威胁。

关闭“sunrpc”服务可以减少远程攻击（包括远程的缓冲区溢出，例如 rpc.ttdbserver）的威胁。

关闭“snmpd”可以减少因为 SNMP V1 协议本身安全性引起的安全漏洞。

关闭 UNIX 的路由功能可以减少由路由协议和转发数据包引起的安全漏洞等。

通过编辑相关的文件（如/etc/inetd.conf、/etc/rc2.d 目录下“S”打头的相应文件等）可以关闭相应服务；通过创建空文件/etc/notrouter 来关闭 IP 转发功能（或者在 SUN 系统中使用命令 ndd 来改变系统内核的各种参数设置，包括对缓冲区溢出类的攻击的对抗、/dev/ip、/dev/tcp、/dev/udp 等设备的参数）等。

但是普通版本 UNIX 的标准配置中，却缺少限制特定地址访问和特定服务的功能。例如根据网络安全策略，可能只允许某个 IP 地址使用 TELNET 服务，另一个子网用户可以使用 FTP 服务。这可以用软件 tcp wrapper 来实现，该软件在当前网络上有多处可信站点可以免费下载，安装配置都非常简洁明了，并且这样做对网络安全策略的细化有重要意义。因此，该软件也成为网络安全中最受欢迎