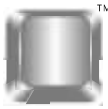

张 涛 主编
阴东锋 谢 魏 叶振建 编著

网络安全管理技术

专 家 门 诊

清华大学出版社

内容简介

本书重点介绍各种常见的网络安全方面的问题，包括了对黑客的认识、网络安全基础、网络工具的使用、计算机病毒、特洛伊木马、日常上网安全防护、Windows 2000 系统安全、应用程序安全、缓冲区溢出等方面的内容。本书强调理论与实践相结合，注重技术的可操作性，采用面向问题的讲述方式，列举了大量典型的实例。

本书的最大特点是从问题出发，在简单的基础理论之上以实际应用为主，体现了“以防为主、攻防兼备”的写作特色。本书所给出的问题在论坛中也经常出现，都是网络爱好者比较关心的问题，可以提供很强的参考作用。

本书内容丰富，语言通俗易懂，实用性非常强，是一本很适合入门及初级读者的网络安全教程。

图书在版编目（CIP）数据

网络安全管理技术专家门诊 / 张涛主编；阴东锋，谢魏，叶振建编著. —北京：清华大学出版社，2005.2
（黑魔方丛书）
ISBN 7-302-10295-3

Ⅰ.网…　Ⅱ.①张…②阴…③谢…④叶…　Ⅲ.计算机网络-安全技术-问答　Ⅳ.TP393.08-44

中国版本图书馆 CIP 数据核字（2005）第 000673 号

出 版 者：清华大学出版社　　印 刷 者：北京市鑫丰华彩印有限公司
地　　址：北京清华大学学研大厦　　装 订 者：三河市金元装订厂
　　http://www.tup.com.cn　　发 行 者：新华书店总店北京发行所
邮　　编：100084　　开　　本：185×230　印张：23.75　插页：2　字数：497 千字
社 总 机：010-62770175　　版　　次：2005 年 2 月第 1 版　　2005 年 2 月第 1 次印刷
客户服务：010-62776969　　书　　号：ISBN 7-302-10295-3/TP·1140
责任编辑：魏江江　　印　　数：1～3000
装帧设计：吴文越　　定　　价：32.00 元

导读

首先，非常感谢您阅读本书，希望本书不同于其他同类的书籍，能确确实实地给您带来一些收获。当您仔细阅读完本书后，您就已经进入了一扇通往网络安全的大门。为了能更好地帮助您学习本书的知识，请仔细阅读下面的内容。

本书的读者对象

本书是一本面向大众的网络安全基础类书籍，风格简洁明了，文字通俗易懂，采用一问一答的形式，对常见的各种网络安全事项进行了详细的剖析，并通过实际例子手把手地教您学习网络安全的基础知识。

本书适合广大在校大学生、网络管理员、家庭用户、宽带用户，以及广大网络安全爱好者阅读，是一本很实用的入门级读物。

如果您要阅读并掌握本书的内容，您需要对 Windows 操作系统和网络基础知识有一定的认识，并有一定的实际操作能力。

本书的写作环境

本书除第 4、5、6 章在 Windows XP 环境下完成写作外，其他所有内容都在 Windows 2000 环境下完成，如在书中未进行特别说明，则技术和方法可以在其他 Windows 环境下使用。

本书中介绍的所有软件，其版本均以软件抓图或文章描写为准。

本书的学习方法

网络安全重在预防，学习并领会这种思想才是本书的精神所在，而这种思想的实践基础就是本书介绍的各种技术和方法。

要更好地学习本书的内容，建议您先快速浏览整本书，在看第二遍时做好这两方面：仔细阅读，认真领会，最好能作笔记；多做实验，胆大心细，不要怕失败。如果您对其中的一些术语或简单知识不了解，建议您到搜索引擎先查找并掌握相关基础知识。

在本书出版的同时，www.54master.com 将同时开设相应的读者交流版块，在您阅读本书过程中，您的任何建议、要求、疑问等，都可以到此版块发表。同时您还可以通过电子邮件方式同作者取得联系，联系方式：security@54master.com。

作者介绍

本书所有内容由“我是网管”论坛的三位管理员所写。

原攻防技术版版主“SimpleLove”（阴东锋），熟悉 Windows、FreeBSD 和 Linux 安全，精通各种协议，有一定的网络攻防能力，编写了第 1、2、3、8、9 章。

坛主“红色代码”（张涛），熟悉各种 Windows 系统的安全配置，精通各类计算机病毒

的原理和查杀办法，多次在各种杂志发表文章，编写了第 4、5、6 章。

总版主“xieweinick”（谢魏），精通服务器、网络攻防、SQL，可熟练配置各种网络环境下的 ISA Server 和 Exchange Server，编写了第 7 章。

特别感谢

“我是网管”论坛：http://www.54master.com

微软中国：http://www.microsoft.com/china

安全焦点：http://www.xfocus.net

绿盟科技：http://www.nsfocus.net

CVC 电脑病毒论坛：http://www.retcvc.com/

另外，还要感谢广大网友和兄弟论坛提出的意见和建议，感谢很多前辈的指点和教导，感谢李婷婷、刘飞倩及孟宪芳三位同志在整个写作过程中的大力支持。

目录

第 1 章

认识黑客

计算机网络技术是当今世界上最为激动人心的高新技术之一，它的出现和快速发展，特别是因特网（Internet）的迅猛发展正在使世界成为一个整体。不可否认，黑客的出现和网络有着十分密切的联系。也可以这么说，正是因为有了计算机网络，才产生了黑客。

1.1 黑客的概念

1.1.1 人们心目中的黑客

“我的电子信箱怎么登录不进去了？”，“QQ 密码又被盗了”，“哎，昨天在一个聊天室里被人炸了”，“计算机怎么又中病毒了？防火墙还打开着啊”……整天听着这些人无奈和抱怨的话，心里冒出了一个词——黑客。目前在很多人心目中的黑客就是以这个形象出现的。

网络就像一个潘多拉魔盒，它在给我们的生活带来无穷乐趣的同时，在一般人不留意的网络深处，还存在着一个神秘的群体——黑客。他们经常隐蔽在网络的深处，他们的智力和所掌握的计算机技术超乎寻常，他们可以分析一个系统的漏洞并编写一些工具来利用这些漏洞进入一台计算机。

当然，上面所出现的情况只是黑客行为中的一小部分，如果把范围再放大一点，可以包括计算机里的文件被删除、硬盘被格式化、网络游戏的账号被盗、信用卡被盗、主页被修改等。总之一句话，目前很多人心目中的黑客就是一个在网络上为所欲为，到处破坏，可以随便入侵一台计算机并在上面搞恶作剧的神秘高手和网络罪犯。

如果按照上面的行为标准来对黑客下定义，那么懂一点网络安全知识甚至计算机知识的人都可以成为黑客了。但事实并不是这样，他们中的很多人并不能被称为黑客，于是人们送给他们另外一个名字——“骇客（Cracker）”或者“入侵者”，他们这类人破解商业软件、入侵网络站点、修改主页、非法进入计算机系统、删除文件、盗取各类密码、窃取他人隐私和机密文件资料，对网络安全构成很大的威胁。

如果说黑客是创造新东西、研究探索软件程序和网络中的漏洞、检查网络和系统完整性和安全性的人，那么入侵者只不过就是那些利用真正的黑客们已经发现的漏洞和编写出来的工具而到处破坏的人。他们往往做一些重复性的工作，例如用暴力法破解密码，利用黑客工具进行大范围的扫描。他们也具备广泛的计算机知识，但与黑客不同的是他们以利用和破坏为目的。

还有一种人介于黑客与入侵者之间，他们自称为一名网络安全爱好者。他们可以随心所欲地编写一些程序实现自己的目的和意图，他们也能发现一些漏洞并加以利用，或者通知管理员或者软件开发者对漏洞进行修复，但他们很少对计算机系统进行破坏。

1.1.2 真正的黑客含义

“黑客”大多数是程序员，他们对于操作系统和编程语言有着深刻的认识，乐于探索其中的奥秘，并且善于通过探索了解系统中的漏洞，他们有着自己的道德和行为准则。他们近乎疯狂地钻研更深入的计算机系统知识，并乐于与他人共享成果，他们中有一部分曾经是计算机发展史上的英雄，为推动计算机的发展起了重要的作用。

“黑客”一词原来并没有丝毫的贬义成份，甚至在早期的美国计算机界是带有褒义的。直到后来，少数怀着不良企图，利用非法手段或者利用前辈们的方法和工具，获得了对系统的访问权去闯入远程机器，破坏重要数据；或为了自己的私利而制造麻烦的具有恶意行为特征的人的出现，玷污了“黑客”的名声，改变了人们对黑客的认识和看法。从此，“黑客”才逐渐衍变成入侵者、破坏者的代名词。

虽然现在媒体和书刊杂志对黑客的准确定义仍然持有不同的意见，但是，从网络和信息安全角度来说，“黑客”一词的普遍含义是指具有一定的软件和硬件方面知识，对计算机和网络系统的安全构成威胁的人。

1.2 黑客的产生和发展

在上一节里主要讲述了黑客的基本概念，让大家对黑客有一个最初的认识和基本的了解。本节主要来讨论黑客的起源和黑客的产生，让大家明白最早的黑客是在什么时间，在什么环境下产生的，他们为什么要选择去做一名黑客。

1.2.1 黑客的起源

最早的黑客行为应该从电话入侵技术开始。在电话普及的初期，昂贵的电话费用不是一般人所能承受得了的，于是，一群聪明人发明了一些电子装置，得以免费打电话。人们把他们称之为“电话飞客”。

一般认为最早的黑客始于 20 世纪 50 年代。1946 年世界上第一台计算机问世，麻省理工学院（MIT）率先研制出“分时系统”，学生们第一次拥有了自己的计算机终端。一些才华出众的学生结成小组，经常通宵达旦地在实验室里操作机器，他们认为任何信息都是应该公开的，任何人都可以平等地获取，于是他们便闯入了限制使用的某个计算机系统。

他们在工作中已经积累了相当多的方法和技巧，但这些方法不是严密的理论。他们当然不会教条地套用这些方法，否则他们就不会是黑客了。MIT 的这些人，应该属于第一代黑客，他们精力充沛，热衷于解决难题，对计算机全身心投入，为计算机技术的发展做出了巨大贡献。

1.2.2 黑客的发展

20 世纪 60 年代中期，起源于 MIT 的“黑客文化”开始扩散到美国其他校园，并逐渐向商业渗透，黑客们进入或自己建立电脑公司。他们中最著名的有贝尔实验室的邓尼斯·里奇和肯·汤姆森，1969 年他俩在小型计算机 PDP—11/20 上用 C 语言编写出 Unix 操作系统，推动了工作站和网络的成长。MIT 的理查德·斯德尔曼后来发起成立了自由软件基金会，成为国际自由软件运动的精神领袖。他们是第二代“黑客”的代表人物。

1969 年，因特网的前身 ARPANET 出现。这样，以 ARPANET 为网络，以 DEC－PDP 系列小型机分时系统为硬件基础，以 Unix 的出现为软件基础，整个黑客文化开始迅速繁荣。以 MIT 的人工智能实验室为中心，蔓延到斯坦福大学人工智能实验室（SAIL）与稍后的卡内基梅隆大学（CMU）。三个都是大型的计算机研究中心及人工智能的权威，聚集着世界各地的精英，不论在技术上或精神层次上，对黑客文化都有极高的贡献。

20 世纪 70 年代，黑客倡导了一场个人计算机革命，他们发明并生产了个人计算机，打破了以往计算机技术只掌握在少数人手里的局面，并提出了计算机为人民所用的观点，这一代黑客是计算机史上的英雄。其领头人是史蒂夫·乔布斯和比尔·盖茨，他们分别创办了苹果和微软公司。

从 20 世纪 70 年代起，新一代黑客已经逐渐走向自己的反面。1970 年，约翰·达帕尔发现“嘎吱船长”牌麦片圈盒里的口哨玩具吹出的哨音可以开启电话系统，从而借此进行免费的长途通话。他在黑客圈子里被叫做“嘎吱船长”，因盗用电话线路而多次被捕。苹果公司乔布斯和沃兹奈克也制作过一种“蓝盒子”，成功侵入了电话系统。

20 世纪 80 年代初，计算机地下组织开始形成，出现了早期的计算机窃贼。1984 年，德国汉堡出现了一个名叫“混沌”计算机俱乐部（CCC），其成员竟然通过网络将 10 万美元从汉堡储蓄银行转到 CCC 账号上。1987 年，CCC 的成员攻入了美国宇航局的 SPAN 网络。

1982 年，年仅 15 岁的凯文·米特尼克（Kevin Mitnick）闯入了“北美空中防务指挥系统”，这是首次发现的从外部侵袭的网络事件。他后来连续进入到美国多家大公司（Sun、Motorola 和 AT&A）的计算机网络，把一些重要合同涂改得面目全非。1994 年，他向圣迭戈超级计算机中心发动攻击，将整个因特网置于危险的境地。米特尼克曾多次入狱，被指控偷窃了数以千计的文件以及非法使用 2 万多个信用卡。他是著名的“世界头号黑客”。

1984 年，美国黑客戈德斯坦创办著名的黑客杂志 2600：The Hacker Quarterly；10 年后，这份杂志已有可观的发行量，1995 年达到了 2 万册。

1988 年 11 月 2 日，美国康奈尔大学 23 岁学生罗伯特·莫里斯，向因特网释放了“蠕虫病毒”，美国军用和民用计算机系统同时出现了故障，至少有 6200 台受到波及，约占当时因特网中计算机总数的 10%以上，用户直接经济损失接近 1 亿美元，造成了美国高技术史上空前规模的灾难事件。

1995 年，俄罗斯黑客列文在英国被捕。他被指控用笔记本电脑从纽约花旗银行非法转移至少 370 万美元到世界各地由他和他的同党控制的账户。

1999 年 3 月，美国黑客戴维·史密斯制造了“梅利莎(Melissa)”病毒，通过因特网在全球传染数百万台计算机和数万台服务器。该病毒是有史以来传播最快的宏病毒之一，它的变种病毒可以修改文件，并将受害者的机密信息发送出去。

2000 年 2 月，全世界黑客们联手发动了一场“黑客战争”，把整个网络搅了个天翻地覆。神通广大的黑客，接连袭击了因特网最热门的几大网站，让亚马逊（Amazon）、雅虎（Yahoo）和微软（Microsoft）这些网站瘫痪长达数小时，估计造成了高达 17 亿美元的损失。

2000 年 5 月，菲律宾学生奥内尔·古兹曼炮制出“爱虫”病毒，因计算机瘫痪所造成的损失高达 100 亿美元。全世界反黑客、反病毒的斗争呈现出越来越激烈的趋势。

1.3 黑客的行为特征

从行为方面来分类，黑客通常可以分为以下几种类型。

- 好奇型：他们没有反社会色彩，只是为了追求技术上的精进，在好奇心驱使下进行一些并无恶意的攻击，以不正当侵入为手段找出网络漏洞，他们在发现了某些内部网络漏洞后，会主动向网络管理员指出或者干脆帮助修补网络错误以防止损失扩大。他们能使更多的网络趋于完善和安全。
- 恶作剧型：闯入他人网站，篡改、更换网站信息或者删除该网站的全部内容，并在被攻击的网站上公布自己的绰号，以便在技术上寻求刺激，炫耀自己的网络攻击能力。
- 隐密型：喜欢先通过种种手段把自己深深地隐藏起来，然后再以匿名身份从暗处实施主动网络攻击；有时干脆冒充网络合法用户，通过正常渠道侵入网络后再进行攻击。此类黑客大都技术高超、行踪无定，攻击性比较强。
- 定时炸弹型：极具破坏性的一种类型。为了达到个人目的，通过在网络上设置陷阱或事先在生产线或网络维护软件内置入逻辑炸弹或后门程序，在特定的时间或特定条件下，根据需要干扰网络正常运行或致使生产线或者网络完全陷入瘫痪状态。
- 重磅炸弹型：这种黑客凭借高超的黑客技术，利用高技术手段干扰竞争对手的正常商业行为。或者非法闯入军事情报机关的内部网络，干扰军事指挥系统的正常工作，窃取、调阅和篡改有关军事资料，使高度敏感信息泄密，意图制造军事混乱或政治动荡。

从特征方面来分类，黑客一般具有以下几个特征。