网上冲浪实用技术

FANHEIKE
JIAOCHENG

反黑客教程

高志国 龙文辉 ❖ 编著

黑客行径分析

特洛伊木馬

黑客软件

计算机病毒

黑客常用攻击手段

黑客实例

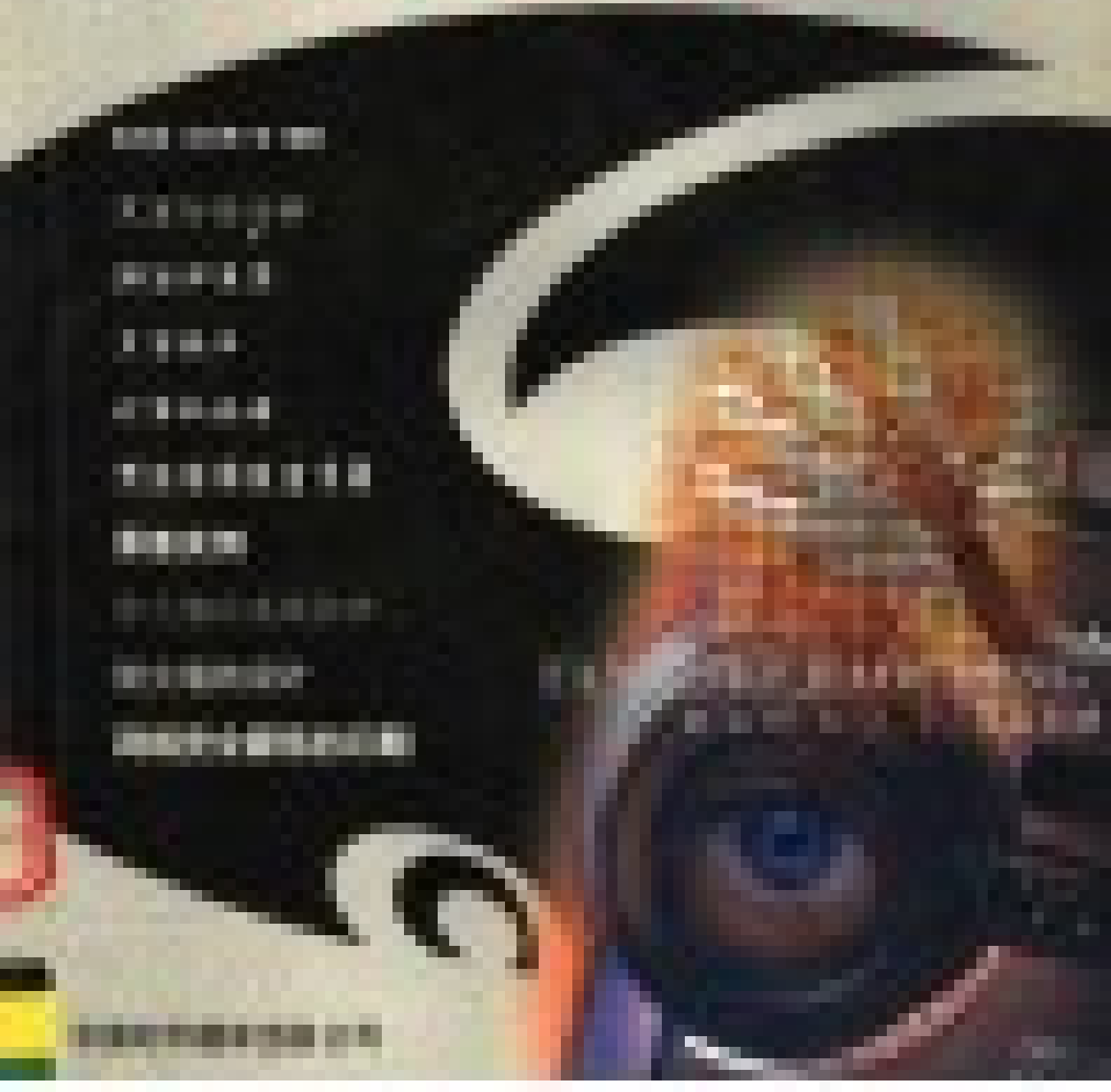
防火墙的高级知识

防火墙的设计

网络安全服务的问题

中国对外翻译出版公司

黑客教程



反黑客教程

高志国　龙文辉　编著

中国对外翻译出版公司

图书在版编目(CIP)数据

反黑客教程/高志国，龙文辉编著. -北京：中国对外翻译出版公司，2000.1
ISBN 7-5001-0719-6

Ⅰ.反… Ⅱ.①高…②龙… Ⅲ.计算机网络-安全技术-教材 Ⅳ.TP393.08-43

中国版本图书馆 CIP 数据核字(1999)第 57161 号

出版发行/中国对外翻译出版公司
地　　址/北京市西城区太平桥大街 4 号
电　　话/66168195
邮　　编/100810
责任编辑/赵英伟
责任校对/苏　醒
封面设计/老　乡
印　　刷/北方工业大学印刷厂
经　　销/全国新华书店
规　　格/787×1092 毫米　1/16
印　　张/23
版　　次/2000 年 1 月第一版
印　　次/2000 年 1 月第一次印刷
字　　数/550 千字

ISBN7－5001－0719－6-/G・176　定价：29.80 元

前　言

信息网络国际化、社会化、开放化、个人化的特点使国家的“信息边疆”不断延伸，甚至到了每一个上网者个人。国际上围绕信息的获取、使用和控制的斗争愈演愈烈，信息安全成为维护国家安全和社会稳定的一个焦点，各国都给予了极大的关注与投入。

信息安全的概念在２０世纪经历了一个漫长的历史阶段，90 年代以来得到了深化。从信息的保密性（保证信息不泄漏给未经授权的人）拓展到信息的完整性（防止信息被未经授权的篡改，保证真实的信息从真实的信源无失真地到达真实的信宿）、信息的可用性（保证信息及信息系统确实为授权使用者所用，防止由于计算机病毒或其他人为因素造成的系统拒绝管理）、信息的不可否认性（保证信息行为人不能否认自己的行为）等。信息安全需要“攻、防、测、控、管、评”等多方面的基础理论和实施技术。

由于在广泛应用的国际互联网上，黑客入侵事件不断发生，不良信息大量传播，网络安全监控管理理论和机制的研究受到重视，黑客入侵手段的研究分析，系统脆弱性检测技术，报警技术，信息内容分级标识机制，智能化信息内容分析等研究成果已经成为众多安全工具软件的基础研究，它揭示出系统中存在许多设计缺陷，并存在情报机构有意埋伏的安全陷阱的可能。例如在 CPU 芯片中，在发达国家现有技术条件下，可以植入无线发射接收功能，在操作系统、数据库管理系统或应用程序中能够预先安置从事情报收集、受控激发破坏程序。通过这些功能，可以接收特殊病毒；接收来自网络或空间的指令来触发 CPU 的自杀功能，搜集和发送敏感信息；通过特殊指令在加密操作中将部分明文隐藏在网络协议层中传输等。而且，通过惟一识别 CPU 个体的序列号，可以主动、准确地识别、跟踪或攻击一个使用该芯片的计算机系统，根据预先设定收集敏感信息或进行定向破坏。

计算机的安全性历来都是人们讨论的主要话题之一。而计算机安全主要研究的是计算机病毒的防治和系统的安全。在计算机网络日益扩展和普及的今天，计算机安全的要求更高，涉及面更广。不但要求防治病毒，还要提高系统抵抗外来非法黑客入侵的能力，还要提高对远程数据传输的保密性，避免在传输途中遭受非法窃取。

随着计算机网络技术的发展和局域网、因特网的广泛应用，网络系统的管理责任越来越重大。

网络被攻击是不可避免的事情，只有加强预防措施，及时地堵住漏洞才能把损失降低到最小。这就需要我们不但了解黑客攻击的方法，还要了解计算机网络安全的有关知识，提高网络安全意识。

编　者

1999 年 12 月

内 容 提 要

本书由浅入深，共分为三个部分：基础知识、黑客篇和反击黑客篇。

在基础知识中，读者可以了解到计算机网络与操作系统的基础知识。包括各种协议的工作原理、计算机网络安全的基本常识，以及一些 UNIX 基本的命令。

在黑客篇中，介绍了黑客常用的攻击手段以及黑客的常用工具、计算机病毒的知识。这一篇中包括了大量的病毒源代码和部分的特洛伊木马、邮件炸弹的源代码，可以供读者研究。这一部分还有大量的攻击实例和拆解软件的实例。

在反击黑客篇中，着重介绍了防火墙的有关知识，还有口令安全和数据加密的有关内容。防火墙部分图文并茂，并且配合有防火墙的实例，可以给读者一个直观的印象。有利于读者更好地理解此部分的内容。

这本书无论是对黑客，还是网络管理员都有极大的参考价值。在本书中还列出了部分的网址，有兴趣的读者可以作为相关查看的对象。

由于编者水平有限，在某些方面有所不足，望读者给予指正。

目 录

第一部分　网络安全基础知识

第二部分 黑客篇

第三部分 反击黑客篇

第一部分 网络安全基础知识

这一部分将详细介绍计算机网络的各种基本知识。网络安全对多数网络管理员来说是很大的难题。要创建既提供多数用户要求的灵活性又要保证网络的安全是十分困难的。增加灵活性就意味着打开一个安全漏洞。网络管理员必须仔细权衡，同时也必须认识到任何安全系统都可能被其他人攻破。因此，真正的目标是设置合理的安全限制。

要实现攻击他人的网络或是防止他人的攻击，就必须了解网络的体系结构和网络的各层协议之间是如何工作的，以及一些网络安全的基本概念。

第一章 引 论

国际互联网的发展可谓是一日千里，一两年前还不知“Internet”为何物的人，可能现在已经开始埋怨网络速度太慢。随着计算机网络的普及，“黑客”这个名字也越来越引起世人的关注。这一章将解释什么是黑客，并且介绍黑客的常用攻击手段。

第一节 “黑客”引起公众的注意

提起黑客，总是那么神秘莫测。在人们眼中，黑客是一群聪明绝顶，精力旺盛的年轻人，一门心思地破译各种密码，以便偷偷地、未经允许地闯入政府、企业或他人计算机系统，窥视他人的隐私。

其实，黑客成为人们眼中“电脑捣乱分子”的代名词，只是近几年的事。黑客的产生与变迁，有极其复杂的背景，并且与计算机技术的发展紧密相关。一部“黑客史”其实就是一部计算机发展的历史。

1988 年 12 月，凯文·米尼克被捕，它的故事立即成为媒体的大餐。米尼克 17 岁时就破坏了太平洋贝尔电话公司的电脑，还从旧金山一家公司偷出了价值 20 万美元的数据。他曾经在一所青年监狱坐牢 6 个月，然后出狱服缓刑，一天，他的缓刑警官突然发现他的电话被切断，而电话公司却没有任何纪录。米尼克曾经是一家通信社发布的一条假新闻的炮制者，新闻声称平安太平洋银行在 1988 年第一季度亏损 4 亿美元。他还多次侵入过国家安全局的电脑。

1988 年 12 月 27 日，《洛杉矶每日新闻》报道说，“为了保护国家的电脑系统，有关机构计划仔细研究米尼克案件。一个像米尼克这样的人可以在 10 分钟内颠覆全世界。”因为米尼克的所作所为不是为了金钱，所以他更加危险。一个具有像米尼克能力的人可能使用电脑犯下任何罪行。

米尼克 10 年的黑客生涯并不是为了钱。他对电脑怀有特殊的感情，在他的眼里电脑绝