

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

特洛伊木马

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

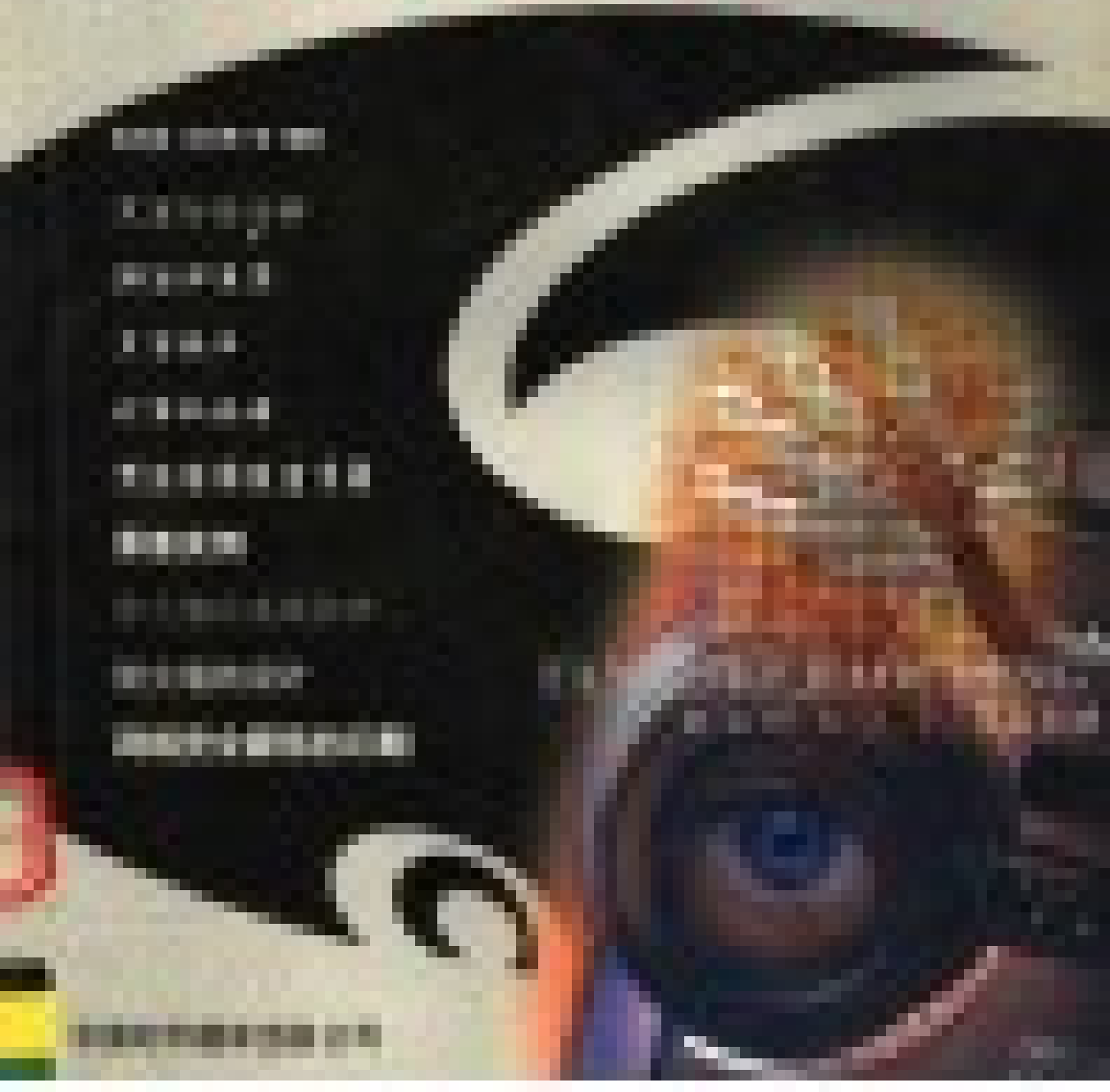
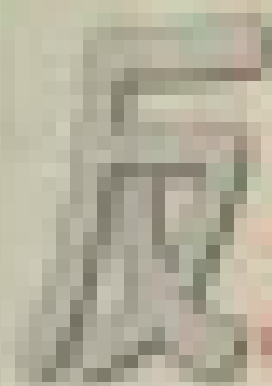
防火墙的设计

网络安全服务的问题

FANHEIKEJIAOCHENG

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… I.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 and 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相关知识，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

第一章 引论.....	1
第一节 “黑客”引起公众的注意.....	1
第二节 黑客和入侵者	3
第三节 计算机安全基础	4
一、网络安全问题的提出.....	5
二、网络安全的关键技术.....	6
三、计算机安全的组成.....	7
四、计算机安全的目标.....	8
五、计算机网络安全评估.....	8
第四节 黑客常用攻击手段	10
第五节 基本黑客技术	11
第六节 优秀网络安全站点集锦	12
一、系统安全.....	13
二、加密技术.....	13
三、黑客防范.....	13
四、计算机安全组织、厂商.....	13
五、计算机安全产品.....	15
六、计算机网络安全知识.....	16
七、安全漏洞及补丁程序.....	16
第二章 操作系统.....	18
第一节 操作系统的基本概念	18
一、操作系统的历史.....	18
二、操作系统的功能.....	19
三、操作系统的类型.....	20
第二节 UNIX 简介	20
一、UNIX 的历史与发展.....	20
二、UNIX 的特点.....	21
三、UNIX 的结构.....	21
四、UNIX 基本操作.....	22
五、UNIX 的文件系统.....	23

六、UNIX 的基本命令.....	24
七、UNIX 系统的 Shell	27
第三节 Windows X 系列	27
一、Windows NT 的特性.....	27
二、Service Pack 的新增功能.....	29
第四节 操作系统与安全	33
一、Windows NT 的漏洞.....	34
二、N T 服务器和工作站的安全漏洞.....	34
第三章 网络的发展.....	36
第一节 计算机网络的发展	36
第二节 网络的拓扑结构	36
一、总线型网络.....	37
二、环型总线.....	38
第三节 网络的 OSI 模型.....	38
一、OSI 模型的基本结构	39
二、OSI 的数据传输	40
第四节 NetWare 协议.....	41
一、OSI 模型与 NetWare 协议、TCP/IP 的关系.....	41
二、NetWare 的核心协议(NCP).....	42
三、网际分组交换协议(IPX).....	43
四、顺序组交换协议(SPX).....	43
第五节 TCP/IP 协议	44
一、IP 地址	44
二、网际协议 (IP)	45
三、传输控制协议 (TCP)	46
第六节 APPLE TALK	47
第四章 基本安全.....	50
第一节 安全形式	50
一、虚假的安全.....	50
二、物理安全.....	50
第二节 基本安全措施	50
一、硬件的安全.....	50
二、备份(Backups).....	50
三、清除措施.....	51
第三节 用户的安全	51
一、口令安全.....	52
二、文件许可权.....	52

三、目录许可.....	53
四、umask 命令.....	53
五、设置用户 ID 和同组用户 ID 许可.....	53
六、cpmvln 和 cpio 命令.....	53
七、su 和 newgrp 命令.....	54
八、文件加密.....	55
九、其他安全问题.....	55
第四节 程序员安全	55
一、系统子程序.....	56
二、标准 C 库.....	60
第五节 系统管理员安全	61
一、安全管理.....	62
二、超级用户.....	62
三、文件系统安全.....	62

第二部分 黑客篇

第五章 黑客行径分析	66
第一节 攻击事件	66
第二节 攻击的目的	67
一、进程的执行.....	67
二、获取文件和传输中的数据.....	68
三、获取超级用户的权限.....	68
四、对系统的非法访问.....	68
五、进行不许可的操作.....	68
六、拒绝服务.....	69
七、涂改信息.....	69
八、暴露信息.....	69
第三节 实施攻击的人员	69
一、计算机黑客.....	69
二、不满或被解雇的雇员.....	69
三、极端危险的罪犯和工业间谍.....	70
第四节 工具	70
第五节 攻击的三个阶段	71
一、寻找目标，收集信息.....	71
二、获得初始的访问权和特权.....	72
三、攻击其他系统.....	73
第六节 攻击的时间	73
第七节 攻击示例一	73

第八节 攻击实例二	75
第六章 特洛伊木马	77
第一节 特洛伊木马简介	77
第二节 木马的克星 The Cleaner2.1	79
第三节 一个特洛伊木马的源程序	81
第七章 计算机病毒	85
第一节 计算机病毒简介	85
一、计算机病毒的各种传染途径及其防治对策	85
二、计算机网络病毒及防治方法	87
三、病毒与特洛伊木马的程序的比较	89
第二节 计算机病毒的监测方法	90
一、比较法	90
二、搜索法	91
三、计算机病毒特征字的识别法	93
四、分析法	94
五、手工扫描病毒的方法	95
第三节 计算机病毒的编制	96
一、可执行文件型病毒	96
二、编写主引导记录 and BOOT 区病毒的方法	98
三、一个主引导记录病毒例子	100
四、病毒的传播	106
第四节 其他病毒的源代码	122
一、台湾 NO.1 WORD 宏病毒源码	123
二、SetMode 宏病毒源码	125
三、UNIX 下的电脑病毒	127
四、Pascal 写的伴随型病毒	134
第八章 黑客软件	138
第一节 扫描工具	138
一、扫描器的基础知识	138
二、扫描工具回顾	139
三、端口扫描工具	143
四、其他扫描工具	146
五、一个简单的端口扫描程序	148
第二节 网络监听工具	150
一、什么是网络监听	151
二、网络监听的目的	154

三、常用监听工具.....	158
四、其他网络监听软件.....	165
五、网络监听的检测.....	166
第三节 炸弹	168
一、E-mail 炸弹.....	168
二、浏览器炸弹.....	172
三、Back Orifice.....	175
第九章 黑客常用攻击手段	177
第一节 利用程序处理错误的攻击	177
一、攻击的现象和后果.....	177
二、泪滴 (TearDrop) 攻击工具.....	178
三、Land 攻击工具.....	180
四、OOB 攻击工具.....	181
第二节 WWW 简介	183
一、WWW 概况.....	183
二、WEB 服务器.....	184
三、基于网关的分布式 WWW 系统构建.....	186
四、WEB 安全技术与防火墙.....	189
第三节 WEB 欺骗的攻击和对策	192
一、WEB 面临的安全威胁.....	193
二、WEB 攻击的行为和特点.....	193
三、攻击的原理和过程.....	194
四、保护方法.....	197
五、WEB 服务器的一些安全措施.....	197
第四节 IP 欺骗以及防范对策	198
一、关于盗用 IP 地址.....	198
二、IP 欺骗及欺骗的对象.....	200
三、IP 欺骗的实施.....	202
四、防备 IP 欺骗的攻击.....	204
五、其他形式的 IP 欺骗.....	205
第五节 缓冲区溢出	205
一、缓冲区溢出的危害.....	206
二、使用缓冲区溢出程序取得特权.....	207
三、缓冲区溢出的原理.....	208
四、缓冲区溢出程序的原理及要素.....	210
五、缓冲区溢出的其他危害.....	214
六、缓冲区溢出攻击 Windows 系.....	216
七、关于缓冲区溢出的一些讨论.....	218

八、再论 SUID	219
第六节 远程攻击	221
一、什么是远程攻击	221
第七节 危险的程序	225
第十章 黑客实例	227
第一节 攻击聊天室	227
一、基于 JavaScript 的炸弹	227
二、使用工具	228
第二节 拆解 ACDSee'95	228
一、Soft-Ice 的使用	228
二、拆解 ACDSee'95	231
第三节 拆解 WINZIP6.2	235
第四节 拆解 SNAP32	236

第三部分 反击黑客篇

第十一章 防火墙的基本知识	241
第一节 防火墙概况	241
一、Internet 防火墙（主要的防火墙）	242
二、数据包的过滤	245
三、代理服务	246
第十二章 防火墙的高级知识	249
第一节 防火墙的体系结构	249
一、双重宿主主机体系结构	249
二、屏蔽主机体系结构	251
三、屏蔽子网体系结构	252
第二节 防火墙的组成方式	255
一、使用多堡垒主机	256
二、合并内部路由器与外部路由器	258
三、合并堡垒主机和外部路由器	258
四、合并堡垒主机和内部路由器	259
五、使用多台内部路由器	260
六、使用多台外部路由器	262
七、使用多个周边网络	263
八、使用双重宿主主机与屏蔽子网	263
第三节 内部防火墙	264
一、试验网络	264

二、低保密度网络.....	265
三、高保密度网.....	265
四、联合防火墙.....	266
五、共享参数网络.....	267
六、内部防火墙的堡垒主机选择.....	267
第十三章 防火墙的设计.....	268
第一节 设计防火墙的准备.....	268
一、信息收集.....	268
二、安全弱点的探测系统.....	268
三、访问受保护系统.....	269
第二节 互联网防火墙技术的回顾与展望.....	269
一、对防火墙技术与产品发展的回顾.....	269
二、第四代防火墙的主要技术与功能.....	271
三、第四代防火墙的技术实现方法.....	273
四、第四代防火墙的抗攻击能力.....	274
五、对防火墙技术的展望.....	275
第三节 基本的防火墙设计.....	276
一、防火墙的姿态.....	276
二、机构的安全策略.....	276
三、防火墙系统的组成.....	277
第四节 防火墙实例.....	282
一、防火墙实例 1: 包过滤路由器.....	282
二、防火墙实例 2: 屏蔽主机防火墙.....	283
三、防火墙实例 3: DMZ 或屏蔽子网防火墙.....	284
第五节 防火墙的选择.....	285
一、代理型与状态检测型的比较.....	285
二、7 种防火墙性能介绍.....	285
第十四章 网络安全服务的问题.....	287
第一节 网络文件系统 (NFS) 的安全.....	287
一、网络文件系统的安全问题.....	288
二、攻击实例.....	289
三、NFS 的 RPC 认证.....	292
四、从服务端调出文件系统.....	292
五、showmount 命令.....	294
六、不安全的 NFS 对系统的危害.....	294
七、NFS 服务器的攻击.....	295
八、安全措施.....	295

九、安全的 NFS	296
第二节 网络信息系统 (NIS)	297
一、NIS 与分布环境的管理	297
二、NIS 如何解决分布环境的问题	298
三、NIS 对/etc/passwd 文件的集中控制	298
四、NIS 的组成	299
五、NIS 的安全性问题	299
六、欺骗服务器	300
第三节 远程登录/远程 Shell 作为作案工具	301
第四节 文件传输协议服务作为作案工具	305
第五节 Sun OS 系统的网络安全	306
一、NFS 的安全	306
二、NFS 安全性方面的缺陷	306
三、远程过程调用 (RPC) 鉴别	307
四、UNIX 鉴别机制	307
五、DES 鉴别系统	308
六、公共关键字的编码	309
第十五章 平台的安全性	310
第一节 漏洞	310
一、漏洞的概念	310
二、脆弱性等级	310
三、其他漏洞	311
四、漏洞对于 Internet 安全性的影响	312
第二节 UNIX 平台的安全	312
一、控制台安全	312
二、机器应放在何处	312
三、保护你的安装介质	312
四、本地缺陷	313
五、重要环节: 口令安全	313
六、隐藏安全口令	313
七、安装一个主动口令检查程序	313
八、下一步: 检查服务	314
九、其他远程服务: Telnet	314
十、FTP: 匿名 FTP	314
十一、Gopher	314
十二、网络文件系统	315
十三、HTTP	315
十四、关于 X	316

十五、修订程序.....	316
第三节 Microsoft 的平台.....	317
一、一个过分友好的平台.....	317
二、DOS.....	317
三、Windows 和 Windows for Workgroups	317
四、Windows 95	317
五、Microsoft Internet 安全框架	319
六、Microsoft Windows NT	319
第四节 细说 Windows 的安全性.....	320
一、安全性的基本框架.....	321
二、Windows 的安全性介绍	321
三、Windows 2000 的安全性设计	322
第五节 NOVELL	324
一、NetWare 安全性概论	324
二、缺省口令.....	324
三、欺骗 (Spoofing)	324
四、Sniffers 和 Novell	324
五、攻击工具.....	325
六、拒绝服务.....	325
七、工具.....	326
第十六章 口令安全	327
第一节 口令与安全	327
第二节 口令破解和其他的认证方式	328
一、口令破解.....	328
二、认证方式.....	328
第三节 好的口令——一个紧锁的门	329
一、不安全口令.....	329
二、保持口令的安全.....	330
第四节 一次性口令	330
第五节 UNIX 系统的口令	330
一、/etc/password 文件.....	331
二、口令时效.....	331
三、网络数据库.....	332
第六节 UNIX 口令加密与破译	333
一、crypt()函数.....	333
二、crypt16()和其他算法.....	334
三、破译口令.....	334
第十七章 反攻击的小技巧	336

第一节 入侵者的追踪(Intruder Tracing)	336
一、通信过程的纪录设定	336
二、查找记录	338
三、地理位置的追踪	339
四、来话者电话侦测(CallerID)	339
五、靠 IPAddress 或 DomainName 找出入侵者位置	340
第二节 IRC 的有关情况	342
第十八章 UUCP 简介	346
第一节 UUCP 系统概述	346
一、UUCP 命令	346
二、uucico 程序	346
三、uuxqt 程序	347
第二节 UUCP 的安全问题	347
一、USERFILE 文件	347
二、L.cmds 文件	348
三、uucp 登录	348
四、uucp 使用的文件和目录	348
第三节 HONEYDANBER UUCP	349
一、HONEYDANBER UUCP 与老 UUCP 的差别	349
二、登录名规则	350
三、MACHINE 规则	351
四、组合 MACHINE 和 LOGNAME 规则	352
五、uuccheck 命令	353
六、网关(gateway)	353
七、登录文件检查	353

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