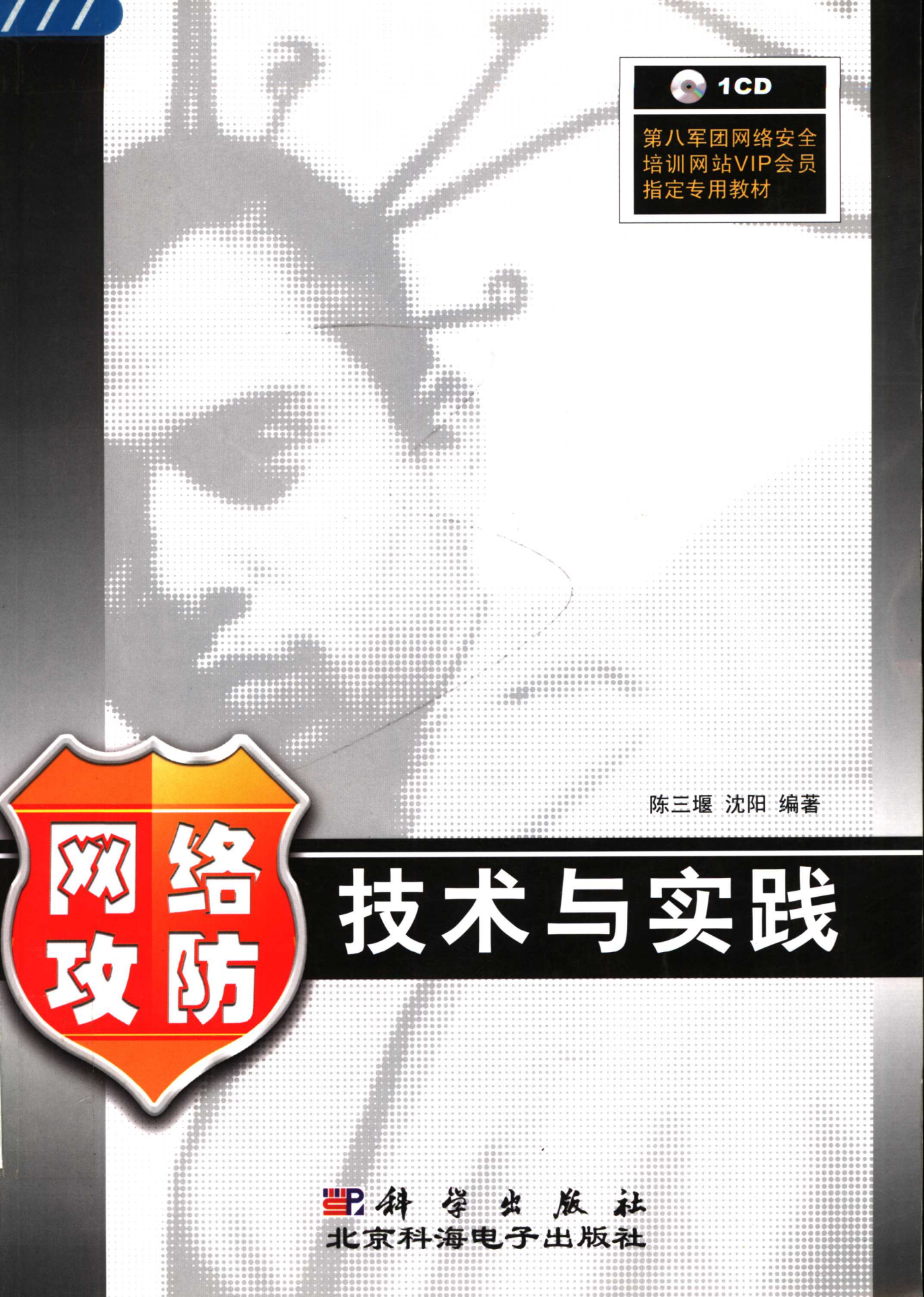
1CD
第八军团网络安全
培训网站VIP会员
指定专用教材
网络攻防
技术与实践
陈三堰 沈阳 编著
科学出版社
北京科海电子出版社

网络攻防技术与实践

陈三堰　沈　阳　编著

科学出版社
北京科海电子出版社

内 容 简 介

本书从计算机网络安全知识入手，结合实际攻防案例，由浅入深、循序渐进地介绍网络攻击与防御的方法，叙述各个知识要点，向读者揭开“黑客”的神秘面纱。本书共分 17 章，主要讲述计算机系统、网络与服务器方面的基础知识，与网络安全知识相关的编程、病毒、Windows Sockets 规范、特络伊木马和后门知识，常用扫描器、嗅探器等，包括使用技巧，密码破解技术，各种入侵技术、攻击方法及检测技术和防御方法等。

本书附送的光盘是第八军团网络安全人才培训所用的录像教程，使你在购买本书的时候还能额外获得专业网络安全培训机构的培训教程，物超所值。

本书内容全面，讲解细致，可作为高等院校网络安全相关专业教学用书，也适合用作培训机构进行网络安全人才培训的教材。

图书在版编目（CIP）数据

网络攻防技术与实践/陈三堰，沈阳编著.
—北京：科学出版社，2006
ISBN 7-03-017077-6

Ⅰ. 网… Ⅱ. 陈… 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（2006）第 026807 号

责任编辑：俞凌娣 / 责任校对：科 海
责任印刷：科 海 / 封面设计：林 陶

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京科普瑞印刷有限责任公司印刷
科学出版社发行 各地新华书店经销

*

2006 年 5 月第一版 开本：16 开
2006 年 5 月第一次印刷 印张：24.75
印数：0001-4000 字数：602 千字

定价：37.00 元

（如有印装质量问题，我社负责调换）

序　言

近年来“黑客”一词充斥着各类媒体，某政府网站被一高中生黑掉，国内第一个黑客盗卖 QQ 案开庭，甘肃第一例黑客攻击案开庭，等等。当看到这些新闻的时候，你或许感觉“黑客”离我们很远，似乎不关己事。可是“网络攻击”并不因为你不了解和不知道它而不存在，实际上我们的生活也是越来越需要互联网络，如手机、电子信箱、网上银行等。当你在享受这些互联网带来的方便的同时，你是否有考虑过有双偷窥的眼睛在盯着你？稍不留意你将受到严重的损失。这些网络安全事件的频繁出现证明了信息网络防御的脆弱。缘于此，产生了本书，并向广大读者隆重推荐。

本书通过实际案例介绍网络攻击与防御的方法，向读者揭开“黑客”的神秘面纱。读完本书，你将会对网络的应用、系统等各个层次了解更多，也知道如何加强你的网络以及 Web 应用、数据库等安全性。知己知彼，方能百战百胜，本书的价值也在于此。

网络攻防技术是实践性和理论性覆盖面比较广的综合性技术，实际上它并非人们想像的那样枯涩难懂，本书从计算机网络安全知识入手，结合实际案例来叙述各个知识要点，而这一点也是市场上各类黑客书籍所无法比拟的。

书中所描述的内容为当前比较流行的安全攻击技术，并且提供了相应的防御方式。

本书作者陈三堰（网名：陈三公子）是国内著名黑客站点第八军团网站负责人，更是一位深谙网络攻击与防御、密码破解、代码优化、操作系统漏洞分析与反病毒技术等许多领域的专家，并具备多年的安全培训经验。正是由于具备多方面的技术功底和经验才能将原本深奥的技术难题通过一些实例浅显易懂地描述出来。

本书是难得一见的基础性安全培训范本，可以作为高等院校网络安全相关专业的教学用书，也可作为初、中级安全人才教育与学习的教材。

李成峰

天融信公司技术总监

前 言

本书编写的初衷是作为第八军团（http://www.juntuan.net）VIP 培训课程的教材，但在编写的过程中越来越有种把本书印刷成册的强烈愿望，由此促使了本书最终的面世。

随着网络安全知识的普及，越来越多的安全技术站点以及安全机构开始进行网络安全培训，但是在市场上一直很少见到一本实用、全面的网络安全培训教材，尤其是国内大中专院校所使用的网络安全技术培训教材过于理论化，知识过于落后，因此本书可以算是填补了这个空白。本书可以作为网络安全培训机构的教材使用，也可用作高等院校的网络安全相关专业的教材和参考资料。

由于我国互联网和 IT 行业起步较晚，一直以来，国内的网络安全技术都远远落后于国外，在一年一度的世界安全论坛上很少能看到华人的影子，国内更是没有一名安全专家出席。虽然国内的网络安全事业在压力中蹒跚起步，但是已经欣喜地看到越来越多的朋友正投身于或准备投身于网络安全事业，越来越多的朋友开始对网络安全技术有了渴望和热情，这所有的一切都得益于网络安全在国内的不断普及。相信所有从事于这个领域的仁人志士都是秉承着“传播网络安全知识，提高网络安全意识，推动网络安全发展”的理念。

网络安全本身博大精深，包罗万象，本书所概括的内容仅仅只是冰山一角，本书并没有针对某某漏洞讲解详细利用过程，而且出于本书的性质，对某些技术方面也并未深入探究。如果读者有需要，可以登录 http://www.juntuan.net 网站，和专业人士进行更加深入的探讨。

由于时间仓促，书中难免有错，望广大读者批评指正。如果对本书有什么意见和建议，欢迎大家批评指证。感谢所有给予我帮助的朋友，因为有了他们，本书才得以最终完稿，同时感谢出版社编辑所作出的辛苦劳动。

陈三堰

2006 年 3 月

于广州 • 天河

目　录

第1章　黑客历史与黑客文化概述 1

1.1　黑客的定义与起源 2

1.1.1　什么是黑客 2

1.1.2　什么是骇客 2

1.1.3　什么是红客 2

1.1.4　怎样才算一名黑客 3

1.2　黑客文化 3

1.2.1　黑客行为 3

1.2.2　黑客精神 3

1.2.3　黑客准则 4

1.3　如何成为一名黑客 4

1.3.1　黑客必备的基本技能 4

1.3.2　如何学习黑客技术 5

1.4　中国黑客发展史 5

1.4.1　中国黑客的起源（1994年~1996年） 6

1.4.2　中国黑客的成长（1997年~1999年） 7

1.4.3　走向2003，浮躁的欲望（2000年~2002年） 8

第2章　基础知识之系统部分 11

2.1　常用DOS命令 12

2.2　文件系统 21

2.2.1　批处理文件 22

2.2.2　VBS、VBE文件 26

2.3　端口、服务、进程知识 38

2.3.1　端口 38

2.3.2　进程 43

2.3.3　服务 44

2.4　系统其他知识 49

2.4.1　回收站与系统安全 49

2.4.2　注册表与系统安全 50

2.4.3　访问控制概述 63

第3章 基础知识之网络部分 65
3.1 基本概念解析 66
3.1.1 万维网（WWW） 66
3.1.2 TCP/IP协议 67
3.1.3 超文本传输协议（HTTP） 68
3.1.4 简单邮件传输协议（SMTP） 68
3.1.5 文件传输协议（FTP） 69
3.1.6 远程登录标准telnet 70
3.1.7 域名服务（DNS） 70
3.2 关于TCP/IP 71
3.2.1 TCP/IP中的基本概念 71
3.2.2 IP协议 75
3.2.3 TCP协议 77
3.2.4 UDP协议 78
3.3 局域网基础知识 80
3.3.1 局域网定义和特性 80
3.3.2 简单局域网拓扑结构 81
3.3.3 局域网常见设备 85
3.4 HTML基础知识 93
3.4.1 基础 93
3.4.2 字体 94
3.4.3 表格 94
3.4.4 区段标记 95
第4章 基础知识之网络应用 97
4.1 Web服务器的搭建 98
4.1.1 利用IIS搭建ASP环境 98
4.1.2 利用IIS搭建PHP环境 99
4.1.3 利用IIS搭建CGI环境 99
4.1.4 搭建JSP环境 100
4.2 其他应用服务器的搭建 102
4.2.1 FTP服务器的搭建 102
4.2.2 mail服务器的搭建 107
4.2.3 DNS服务器的搭建 109
4.2.4 VPN服务器的搭建 111
第5章 基础知识之网络安全 113
5.1 网络安全概述 114

5.1.1 网络安全的定义 114
5.1.2 Internet的安全隐患 114
5.2 安全技术综述 116
5.2.1 杀毒软件技术 116
5.2.2 防火墙技术 116
5.2.3 文件加密和数字签名技术 117
5.2.4 加密技术在智能卡上的应用 118
5.2.5 虚拟专用网技术 119
5.2.6 安全隔离 119
5.3 病毒 120
5.3.1 计算机病毒 120
5.3.2 计算机病毒的发展 120
5.3.3 计算机病毒的特征 121
5.3.4 计算机病毒的分类 122
5.3.5 病毒的作用机理 123
5.3.6 计算机病毒的预防 123
5.3.7 病毒的检测和清除 124
第6章 基础知识之编程技术 127
6.1 Windows Sockets简介 128
6.1.1 Windows Sockets规范 128
6.1.2 Bekeley套接口 129
6.1.3 针对Windows的扩展 129
6.1.4 规范的地位 129
6.2 使用Windows Sockets 1.1编程 129
6.2.1 套接口基本概念 130
6.2.2 客户机/服务器模型 130
6.2.3 带外数据 131
6.2.4 广播 131
6.2.5 字节顺序 131
6.2.6 套接口属性选项 132
6.2.7 数据库文件 133
6.2.8 与Bekeley套接口的不同 133
6.2.9 指针 134
6.2.10 重命名的函数 134
6.2.11 阻塞例程和EINPROGRESS宏 135
6.2.12 Windows Sockets支持的最大套接口数目 135
6.2.13 头文件 135

6.2.14 API调用失败时的返回值 135
6.2.15 原始套接口 136
6.2.16 多线程Windows版本中的Windows Sockets 136
6.3 Windows Sockets 1.1应用实例 137
6.3.1 套接口网络编程原理 137
6.3.2 Windows Sockets编程扩充 138
6.3.3 最简单的C/S编程实例 139
6.3.4 Windows Sockets与UNIX套接口编程实例 141
6.3.5 应用程序实例——wshout 143

第7章 特洛伊木马和后门 145

7.1 特洛伊木马概述 146
7.1.1 特洛伊木马的概念 146
7.1.2 特洛伊木马的特点 146
7.1.3 未来木马的发展方向 147
7.1.4 木马的分类 148
7.2 特洛伊木马深入解析 149
7.2.1 特洛伊木马原理 149
7.2.2 特洛伊木马的攻击步骤 151
7.3 木马的编写方法 155
7.3.1 隐藏进程技术 155
7.3.2 自动启动技术 155
7.3.3 发送数据的方法 157
7.3.4 目标机器情况的获取 163
7.3.5 其他方面的问题 166
7.4 后门 167
7.4.1 后门的概念 167
7.4.2 后门产生的条件及其特点 167
7.4.3 后门的分类 168
7.4.4 后门的编写 171

第8章 扫描器 175

8.1 扫描器的相关知识 176
8.1.1 什么是扫描器 176
8.1.2 扫描器的分类 176
8.1.3 端口扫描原理 177
8.1.4 端口扫描技术 178
8.2 常用扫描器介绍 180
8.2.1 NMAP 180

8.2.2 SSS 183
8.2.3 Nessus 184
8.2.4 X-Scan 185
8.2.5 流光 185
第9章 嗅探器 189
9.1 Sniffer 190
9.1.1 Sniffer基础 190
9.1.2 Sniffer的工作原理 190
9.1.3 Sniffer的实现 193
9.1.4 检测和防范Sniffer 196
9.2 Sniffer的使用 197
9.2.1 Sniffer的选择 197
9.2.2 数据分析 201
9.2.3 实例分析 206
9.2.4 Sniffer的编写 209
第10章 密码破解 211
10.1 选择安全的密码 212
10.1.1 密码的安全性 212
10.1.2 常见的获取密码的方法 212
10.2 常用密码破解工具介绍 213
10.2.1 John the Ripper 213
10.2.2 LOpht Crack 214
第11章 远程攻击的一般步骤 217
11.1 攻击的准备阶段 218
11.1.1 确定攻击的目的 218
11.1.2 信息收集 218
11.2 攻击的实施阶段 221
11.2.1 获得权限 221
11.2.2 权限提升 222
11.3 攻击的善后工作 222
11.3.1 日志系统简介 222
11.3.2 隐藏踪迹 223
11.3.3 留下后门 223
第12章 拒绝服务攻击 225
12.1 概述 226

12.1.1 DoS攻击的定义 226
12.1.2 使用DoS攻击的目的 226
12.1.3 谁容易受DoS攻击 226
12.1.4 DoS攻击模式 227
12.2 常见的DoS攻击 228
12.2.1 Tear Drop 228
12.2.2 SYNFlooding和Land攻击 228
12.2.3 SMURF攻击 229
12.2.4 UDPFlood攻击 230
12.3 分布式DoS攻击 231
12.3.1 分布式DoS攻击介绍 231
12.3.2 分布式DoS攻击防范 231

第13章 Web攻击 237

13.1 常见Web安全问题 238
13.1.1 用户输入没有过滤 238
13.1.2 远程提交问题 243
13.1.3 表单提交时间间隔问题 243
13.1.4 Cookie欺骗问题 243
13.1.5 跨站攻击 247
13.1.6 上传漏洞 249
13.2 CGI的安全性 252
13.2.1 CGI的常见安全问题 252
13.2.2 CGI安全性实例 257
13.3 ASP程序的安全性 262
13.3.1 SQL注入 262
13.3.2 暴库并下载数据库 280
13.3.3 将.MDB改为.asp的灾难 283
13.3.4 备份/恢复数据库 284
13.4 PHP程序的安全性 284
13.4.1 包含文件漏洞 284
13.4.2 脚本命令执行漏洞 285
13.4.3 文件泄露漏洞 285
13.4.4 变量未初始化漏洞 285
13.4.5 SQL注入漏洞 287

第14章 高级攻击手法 307

14.1 IP欺骗攻击 308
14.1.1 IP欺骗攻击的概念 308

14.1.2 IP欺骗原理 308
14.1.3 IP欺骗攻击过程解析 309
14.1.4 IP欺骗攻击实例 310
14.1.5 IP欺骗攻击工具 312
14.2 DNS欺骗 313
14.2.1 DNS欺骗概念 313
14.2.2 DNS欺骗原理 313
14.2.3 DNS欺骗的现实过程 317
14.3 会话劫持攻击 318
14.3.1 会话劫持攻击概念 318
14.3.2 注射式攻击 318
14.3.3 中间人攻击 325
14.4 钓鱼式攻击和Google Hack 332
14.4.1 钓鱼式攻击 332
14.4.2 Google Hack 334
14.5 缓冲区溢出 338
14.5.1 缓冲区溢出概念 338
14.5.2 缓冲区溢出的危害 338
14.5.3 缓冲溢出漏洞攻击 338
14.6 攻击网络设备 340

第15章 主机安全防护 341

15.1 通用主机安全防护 342
15.1.1 安装前的准备 342
15.1.2 安装后的安全设置 342
15.2 特定环境的安全设置 345
15.2.1 IIS的安全设置 345
15.2.2 SQLServer的安全配置 345
15.2.3 PHP安全设置 347

第16章 防火墙技术 349

16.1 防火墙的定义 350
16.2 防火墙的优点和弱点 350
16.2.1 防火墙的优点 350
16.2.2 防火墙的弱点 351
16.3 防火墙技术工作原理 351
16.3.1 包过滤技术 351
16.3.2 包过滤技术的过程 351
16.3.3 包过滤技术的优点和缺点 352

16.4 应用级网关技术 353
16.5 电路级网关技术 354
16.5.1 电路级网关的工作过程 354
16.5.2 电路级网关技术的缺点 354
16.6 状态检测技术 354
16.7 防火墙的分类和体系结构 355
16.7.1 防火墙的分类 355
16.7.2 防火墙的体系结构 357
16.8 防火墙技术发展趋势 358

第17章 入侵检测系统 361

17.1 入侵检测系统介绍 362
17.1.1 入侵检测系统概述 362
17.1.2 入侵检测系统的功能 362
17.1.3 入侵检测系统的分类 363
17.1.4 入侵检测技术的分类 364
17.2 入侵检测系统的安装与配置 365
17.2.1 入侵检测系统的安装 365
17.2.2 IDS系统配置 367

附录 详细端口功能对照表 374

参考文献 380

第1章

黑客历史与黑客文化概述

黑客一词来源于英文单词Hacker的翻译，它从诞生至今已有50多年的历史。在历史的长河中，一代又一代的黑客曾为计算机技术的发展做出了巨大的贡献，他们对计算机技术的革新作出了不可磨灭的贡献。

1.1 黑客的定义与起源

1.1.1 什么是黑客

一般认为，黑客起源于20世纪50年代麻省理工学院的实验室中，他们精力充沛，热衷于解决难题。在那个年代，计算机系统是非常昂贵的，只存在于各大院校与科研机构，技术人员使用一次计算机，需要很复杂的手续，而且计算机的效率也不是很高，为了绕过一些限制，最大限度地利用这些昂贵的计算机，最初的程序员们就写出了一些简洁高效的捷径程序，这些程序往往较原有的程序系统更完善，而这种行为便被称为Hack。Hacker一词源于此，指从事Hack行为的人。20世纪60、70年代，“黑客”一词极富褒义，用于指代那些独立思考、奉公守法的计算机迷，他们智力超群，对计算机全身心投入，从事黑客活动意味着对计算机的最大潜力进行智力上的自由探索，为计算机技术的发展做出了巨大贡献。正是这些黑客，倡导了一场个人计算机革命，倡导了现行计算机的开放式体系结构，打破了以往计算机技术只掌握在少数人手里的局面，开了个人计算机的先河，提出了“计算机为人民所用”的观点，他们是计算机发展史上的英雄。

从传统意义上来说，黑客是指那些具有超常编程水平或计算机系统知识的人，这些人能够以设计者始料未及的方式对某个系统或编程语言进行操纵。曾几何时，被人称为黑客是一件非常光荣的事情。

然而，当现今人们听到“黑客”一词时，大多数人联想到的是那些以恶意方式侵入计算机系统的人。这是由于媒体对黑客一词的误用使得该词几乎失去了其原本的含义。真正的黑客从不恶意入侵他人计算机，他们只是为了进一步提高安全性技术研究水平，乐于研究各种各样的安全漏洞，悄悄地进入他人系统并给系统打上安全补丁后悄然离去。黑客群体发展到后来其中不乏一些怀有恶意的人，他们入侵他人系统，偷窃系统内的资料，非法控制他人计算机，传播蠕虫病毒等，给社会带来了巨大损失，同时也使“黑客”一词蒙羞。通常把这些具有恶意的黑客称为“黑帽子黑客”（Black hat Hacker），那些闯入系统只为了进行安全研究的黑客则称为“白帽子黑客”（White hat Hacker），而那些时好时坏的黑客则称为“灰帽子黑客”（Gray hat Hacker）。

1.1.2 什么是骇客

骇客是“Cracker”的音译。从某种意义上来说，它是Hacker的一个分支，他们同样具有超强的计算机知识，只不过他们倾向于软件破解、加密解密技术方面。在很多时候，Hacker与Cracker在技术上是紧密结合的。Cracker一词发展到今天，也有黑帽子黑客之意。

1.1.3 什么是红客

相信很多人都听说过“红客”一词，红客是中国特有的一个称谓，指那些具有强烈爱国主义的黑客。1999年4月~5月，以美国为首的北约对南斯拉夫发动了战争，在随后的日子里，

中国人民通过各种媒体发表了对正义的声援，网络上更是掀起了对美国霸权主义的批判浪潮。就在当年的5月份，美国的轰炸机悍然轰炸了我驻南联盟大使馆。消息一经传出，中国的黑客以他们自己的方式在网络上开始了一场反击战。就在中国大使馆被炸后的第二天，第一个中国红客网站——中国红客之祖国团结阵线诞生了，以宣扬爱国主义红客精神为主导，网站宣言中铿锵激扬的爱国词语，同时也创造出了一个中国特有的黑客分支——红客。

1.1.4 怎样才算一名黑客

一个黑客首先需要在技术上得到大家的认可，在某项安全技术上拥有出众的能力，才能算是个黑客。此外，还需要具备自由、共享的黑客精神与正义的黑客行为。总的来说，要成为一个黑客，必须是技术上的行家，并且热衷于解决问题，能无偿地帮助其他人。

1.2 黑客文化

1.2.1 黑客行为

真正的黑客拥有自己的职业道德，恪守自己的行为规范，他们有着自己圈内的游戏准则，总结起来有如下几条。

1. 不随便进行攻击行为

真正的黑客很少从事攻击行为，他们在找到系统漏洞并入侵时，会很小心地避免造成损失，并尽量善意地提醒管理者或帮系统打好安全补丁。他们不会随便攻击个人用户和站点。

2. 公开自己的作品

一般黑客们所编写的软件等作品都是免费的，并且公开源代码，黑客们的作品不带任何商业性质，真正地做到了开源共享。

3. 帮助其他黑客

网络安全包含的内容广泛，没有哪个人能做到每一方面都精通，真正的黑客会很热心地在技术上帮助其他黑客。

4. 义务地做一些力所能及的事情

黑客都以探索漏洞与编写程序为乐，但在圈内，除此之外还有很多其他的杂事，如维护和管理相关的黑客论坛、讨论组和邮件列表，维持大的软件供应站点等，这些事情都需要人做，但并非有趣。所以，那些花费大量精力，义务地为网友们整理FAQ、写教程的黑客，以及各大黑客站点的站长，他们都付出了大量的时间和精力，是值得尊敬的。

1.2.2 黑客精神

1. 自由共享的精神

这是黑客文化的精髓，是黑客精神最值得称赞的地方，自由共享是黑客应具备的最基

本品质。黑客诞生并成长于开放的互联网，他们解决问题并创造新的东西，他们相信自由并自愿的相互帮助。最明显的表现是黑客们在互联网上所编写的各种黑客软件都是完全免费共享包括源代码都是公开的。自由共享是黑客的传统精神，也是现代黑客所尽力保持的。

2. 探索与创新的精神

黑客探索着程序与系统的漏洞，并能够从中学到很多知识，在发现问题的同时，他们都会提出解决问题的创新方法。他们努力打破传统的计算机技术，努力探索新的知识，在他们身上有着很强的“反传统”精神。

3. 合作的精神

个人的力量是有限的，何况不可能精通任何网络安全方面的技术，黑客很明白这一点，因此他们乐于与他人交流技术，在技术上保守的人是不可能成为黑客的。

需要说明的是，所谓的黑客精神不应该是想成为黑客的人所刻意追求的，而是每一个黑客以及每一个即将成为黑客的人身上自发地表现出来的。

1.2.3 黑客准则

黑客有着他们自己的游戏规则，他们崇尚自由，有组织（大部分是松散的单纯技术讨论的组织）。事实上，他们是一群最崇尚自由的人，最不喜欢的就是规则，所以并没有绝对的黑客准则。但大多数黑客意识里都有着一种行为规范，比较典型的有如下几条：

（1）不恶意破坏任何的系统，不破坏他人的软件或偷窥他人资料，不清除或更改已侵入计算机的账号。

（2）不修改任何系统文件，如果是因为进入系统的需要而修改，在达到目的后将其改回原状。可以为隐藏自己的入侵行为而作一些修改，但尽量保持原有系统的安全性，不得因得到系统的控制权而将门户大开。

（3）不轻易地将要黑的或黑过的站点告诉他人，不向他人炫耀自己的技术。

（4）不入侵或破坏政府机关的主机，不做无聊、单调且愚蠢的重复性工作，不从事传播蠕虫病毒等会对互联网带来巨大损失的行为。

（5）做真正的黑客，努力钻研技术，研究各种漏洞。

1.3 如何成为一名黑客

1.3.1 黑客必备的基本技能

作为一名黑客，需要有高超的技术水准，计算机技术的发展日新月异，每天都有大量新的知识不断涌现，黑客们需要不断地学习、尝试新的技术，才能走在时代的前面。作为一个黑客，必须掌握一些基本的技能。