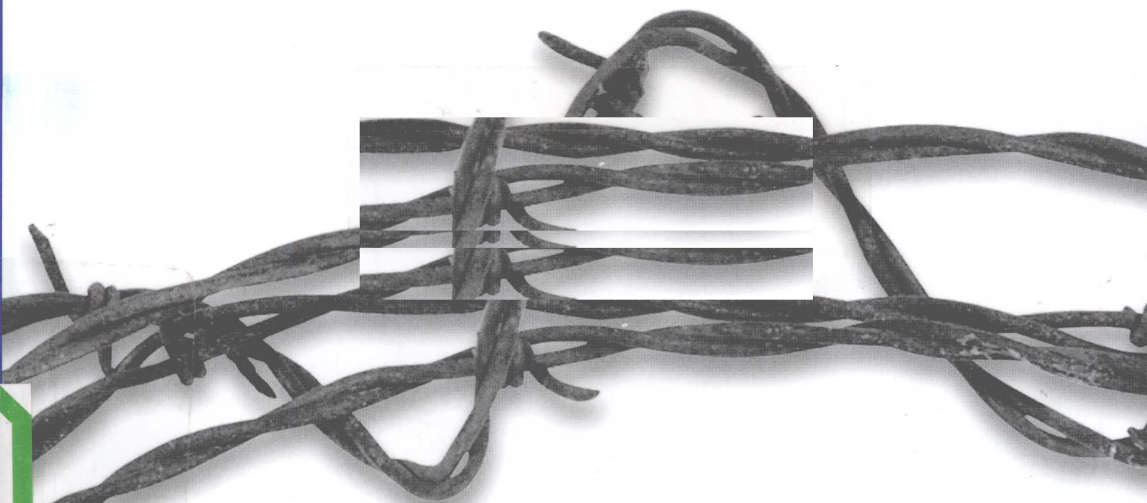


网络安全 HACKS™

第二版

保护隐私的技巧与工具

NETWORK SECURITY HACKS



O'REILLY®

中国电力出版社

HACKS
SERIES™

Andrew Lockhart 著

陈新 译

网络安全 HACKSTM

第二版

—— 保护隐私的技巧与工具

Andrew Lockhart 著

陈新 译

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Sebastopol • Taipei • Tokyo

O'Reilly Media, Inc. 授权中国电力出版社出版

中国电力出版社

图书在版编目 (CIP) 数据

网络安全 HACKS: 第二版 / (美) 洛克哈特 (Lockhart, A.) 著; 陈新译.
—北京: 中国电力出版社, 2009

书名原文: Network Security Hacks™, Second Edition

ISBN 978-7-5083-9279-0

I. 网… II. ①洛… ②陈… III. ①计算机网络—安全技术 ②关系数据库—数据库
管理系统—程序设计 IV. TP393.08 TP311.138

中国版本图书馆 CIP 数据核字 (2009) 第 138371 号

北京市版权局著作权合同登记

图字: 01-2009-7870 号

©2006 by O'Reilly Media, Inc.

Simplified Chinese Edition, jointly published by O'Reilly Media, Inc. and China Electric Power Press, 2008. Authorized translation of the English edition, 2006 O'Reilly Media, Inc., the owner of all rights to publish and sell the same.

All rights reserved including the rights of reproduction in whole or in part in any form.

英文原版由 O'Reilly Media, Inc. 出版 2006。

简体中文版由中国电力出版社出版 2008。英文原版的翻译得到 O'Reilly Media, Inc. 的授权。此简体中文版的出版和销售得到出版权和销售权的所有者——O'Reilly Media, Inc. 的许可。

版权所有, 未得书面许可, 本书的任何部分和全部不得以任何形式重制。

书 名 / 网络安全 HACKS (第二版)

书 号 / ISBN 978-7-5083-9279-0

责任编辑 / 胡顺增

封面设计 / Karen Montgomery, 张健

出版发行 / 中国电力出版社 (www.infopower.com.cn)

地 址 / 北京三里河路 6 号 (邮政编码 100044)

经 销 / 全国新华书店

印 刷 / 汇鑫印务有限公司

开 本 / 787 毫米 × 1092 毫米 18 开本 26 印张 480 千字

版 次 / 2010 年 3 月第 1 版 2010 年 3 月第 1 次印刷

印 数 / 0001 — 4000 册

定 价 / 48.00 元 (册)

敬告读者

本书封面贴有防伪标签, 加热后中心图案消失。

本书如有印装质量问题, 我社发行部负责退换。

版权所有 翻印必究

O'Reilly Media, Inc. 介绍

为了满足读者对网络和软件技术知识的迫切需求,世界著名计算机图书出版机构 O'Reilly Media, Inc. 授权中国电力出版社, 翻译出版一批该公司久负盛名的英文经典技术专著。

O'Reilly Media, Inc. 是世界上在 UNIX、X、Internet 和其他开放系统图书领域具有领导地位的出版公司, 同时也是联机出版的先锋。

从最畅销的 *The Whole Internet User's Guide & Catalog* (被纽约公共图书馆评为 20 世纪最重要的 50 本书之一) 到 GNN (最早的 Internet 门户和商业网站), 再到 WebSite (第一个桌面 PC 的 Web 服务器软件), O'Reilly Media, Inc. 一直处于 Internet 发展的最前沿。

许多书店的反馈表明, O'Reilly Media, Inc. 是最稳定的计算机图书出版商 —— 每一本书都一版再版。与大多数计算机图书出版商相比, O'Reilly Media, Inc. 具有深厚的计算机专业背景, 这使得 O'Reilly Media, Inc. 形成了一个非常不同于其他出版商的出版方针。O'Reilly Media, Inc. 所有的编辑人员以前都是程序员, 或者是顶尖级的技术专家。O'Reilly Media, Inc. 还有许多固定的作者群体 —— 他们本身是相关领域的技术专家、咨询专家, 而现在则编写著作, O'Reilly Media, Inc. 依靠他们及时地推出图书。因为 O'Reilly Media, Inc. 紧密地与计算机业界联系着, 所以 O'Reilly Media, Inc. 知道市场上真正需要什么图书。

目录

荣誉	1
前言	7
第 1 章 Unix 系统主机安全	13
1 保障 Mount 点安全 (初级难度)	13
2 扫描 SUID 及 SGID 程序 (初级难度)	15
3 扫描具有全局可写和组可写权限的目录 (初级难度)	17
4 使用 POSIX 的 ACL (Access Control List, 访问控制表) 来创建灵活的权限层次 (中级难度)	17
5 保护日志不被篡改 (初级难度)	21
6 授权管理员角色 (初级难度)	23
7 自动验证加密签名 (中级难度)	25
8 检查监听的服务 (初级难度)	27
9 阻止服务绑定某个接口 (中级难度)	30
10 采用沙盒 (sandbox) 环境来限制服务 (高级难度)	32
11 使用具有 MySQL 验证源的 proftpd 工具 (中级难度)	36
12 防止堆栈粉碎攻击 (高级难度)	39
13 使用 grsecurity 锁定内核 (高级难度)	41

14	使用 grsecurity 工具限制应用程序 (高级难度)	46
15	使用 Systrace 工具限制系统调用 (高级难度)	48
16	自动创建 systrace 工具的策略 (高级难度)	52
17	使用 PAM 控制登录访问 (中级难度)	54
18	限制用户对 SCP 和 SFTP 的访问 (高级难度)	59
19	为身份认证使用一次性使用的密码 (高级难度)	63
20	限制 Shell 环境 (中级难度)	66
21	加强对用户和组的资源的限制 (中级难度)	67
22	自动更新系统 (初级难度)	69
 第 2 章 Windows 系统主机安全		72
23	检查服务器所应用的补丁 (中级难度)	73
24	使用组策略来配置自动更新 (初级难度)	77
25	获得当前打开的文件及其进程的列表 (初级难度)	80
26	列出正在运行的服务和开放的端口 (初级难度)	82
27	启用系统审核功能 (初级难度)	84
28	枚举自动运行程序 (中级难度)	84
29	保障事件日志的安全 (初级难度)	87
30	修改日志文件大小的最大值 (初级难度)	88
31	备份和清除事件日志 (中级难度)	89
32	禁用默认共享 (初级难度)	92
33	加密临时文件夹 (初级难度)	94
34	备份 EFS (中级难度)	95
35	在关机时清除页面文件 (中级难度)	101
36	检查永不过期的密码 (中级难度)	103
 第 3 章 隐私与匿名		106
37	躲避流量分析 (中级难度)	106
38	通过 Tor 挖掘隧道 SSH (初级难度)	110
39	无缝加密文件系统 (初级难度)	111
40	预防网络钓鱼 (中级难度)	116

41 采用更少的密码来使用 Web (初级难度)	120
42 使用 Thunderbird 加密电子邮件 (初级难度)	122
43 在 Mac OS X 系统下加密电子邮件 (初级难度)	127
第 4 章 防火墙	132
44 使用 Netfilter 防火墙 (初级难度)	132
45 使用 OpenBSD 的防火墙 PacketFilter (初级难度)	137
46 使用 Windows 防火墙保护计算机 (初级难度)	144
47 关闭开放的端口和阻止协议 (初级难度)	153
48 替换 Windows 防火墙 (高级难度)	154
49 建立身份认证网关 (中级难度)	162
50 使得网络自治化 (中级难度)	165
51 测试防火墙 (中级难度)	167
52 使用 Netfilter 过滤物理地址 (中级难度)	170
53 阻止 Tor (高级难度)	171
第 5 章 加密与安全服务	174
54 使用 SSL 加密 IMAP 和 POP (高级难度)	174
55 采用 Sendmail 使用支持 TLS 的 SMTP (高级难度)	177
56 采用 Qmail 使用支持 TLS 的 SMTP (高级难度)	179
57 使用 SSL 和 suEXEC 来安装 Apache 服务器 (高级难度)	181
58 保障 BIND 服务器的安全 (高级难度)	186
59 安装小巧并安全的 DNS 服务器 (高级难度)	189
60 保障 MySQL 服务器的安全 (高级难度)	193
61 在 Unix 系统下安全地共享文件 (高级难度)	196
第 6 章 网络安全	200
62 检测 ARP 欺骗攻击 (初级难度)	201
63 建立静态 ARP 表 (中级难度)	203
64 保护 SSH 不受暴力攻击 (高级难度)	205
65 欺骗远程操作系统检测软件 (高级难度)	207

66	维持网络的产品清单 (初级难度)	211
67	扫描网络漏洞 (中级难度)	214
68	保持服务器时钟同步 (初级难度)	225
69	创建自己的 CA (初级难度)	227
70	向客户端发布您的 CA 证书 (中级难度)	230
71	使用证书服务备份与恢复 CA (中级难度)	232
72	远程检测以太网嗅探器 (高级难度)	239
73	帮助追踪攻击者 (初级难度)	244
74	在 Unix 服务器上扫描病毒 (中级难度)	246
75	追踪漏洞 (初级难度)	251
第 7 章 无线安全		253
76	使您的便利无线路由器变成一个智能安全平台 (高级难度)	253
77	为无线网络使用良好粒度的身份认证 (高级难度)	257
78	配置 Captive Portal (高级难度)	261
第 8 章 日志		267
79	运行集中式 Syslog 服务器 (中级难度)	268
80	操纵 syslog 工具 (初级难度)	269
81	将 Windows 系统整合到 syslog 基础设置中 (中级难度)	271
82	自动归纳总结日志 (中级难度)	279
83	自动监视日志 (中级难度)	281
84	聚合来自远程站点的日志 (高级难度)	284
85	使用进程记账技术来记录用户活动 (中级难度)	290
86	集中监控服务器的安全形势 (高级难度)	291
第 9 章 监视和趋势		300
87	监视可用性 (中级难度)	301
88	趋势图 (高级难度)	309
89	实时监控网络状况 (初级难度)	312

90 使用防火墙规则收集统计信息 (高级难度)	314
91 远程嗅探以太网 (中级难度)	316

第 10 章 安全隧道 320

92 在 Linux 系统下配置 IPsec (中级难度)	320
93 在 FreeBSD 系统下配置 IPsec (中级难度)	325
94 在 OpenBSD 系统下配置 IPsec (中级难度)	329
95 使用 Openswan 进行随机加密 (高级难度)	333
96 通过 SSH 转发并加密流量 (初级难度)	335
97 使用 SSH 客户密钥自动登录 (初级难度)	337
98 通过 SSH 使用 Squid 代理 (中级难度)	340
99 将 SSH 用作 SOCKS 代理 (初级难度)	342
100 使用 SSL 加密流量, 并为流量建立隧道 (初级难度)	345
101 使用 HTTP 内部的隧道连接 (初级难度)	348
102 使用 VTun 和 SSH 建立隧道 (中级难度)	350
103 自动生成 Vtun 配置 (中级难度)	355
104 创建跨平台的 VPN (高级难度)	359
105 使用 PPP 隧道 (中级难度)	366

第 11 章 网络入侵检测 369

106 使用 Snort 进行入侵检测 (中级难度)	370
107 持续关注报警 (中级难度)	375
108 实时监视 IDS (高级难度)	378
109 管理探测器网络 (高级难度)	385
110 编写您自己的 Snort 规则 (中级难度)	392
111 使用 Snort_inline 来防御入侵和容侵 (高级难度)	398
112 使用 SnortSam 实现自动化的动态防火墙 (高级难度)	402
113 检测异常行为 (中级难度)	406
114 自动升级 Snort 的规则库 (中级难度)	408
115 创建一个分布式 Stealth 探测代理网络 (高级难度)	410
116 利用 Barnyard 在高性能环境中使用 Snort (高级难度)	412

117 检测和阻止对 Web 应用程序的入侵 (中级难度)	415
118 扫描网络流量, 发现病毒 (高级难度)	420
119 模拟一个包含多个有漏洞主机的网络 (高级难度)	424
120 记录 Honeypot 活动 (高级难度)	430
 第 12 章 恢复与响应	437
121 镜像挂载的文件系统 (中级难度)	437
122 检验文件完整性, 寻找遭受破坏的文件 (中级难度)	439
123 使用 RPM 寻找遭受破坏的程序包 (初级难度)	444
124 查找系统中的 Rootkit (中级难度)	447
125 寻找网络的所有者 (初级难度)	449

荣誉

关于作者

Andrew Lockhart 原来居住在美国南卡罗莱纳州, 现在居住于美国科罗拉多州北部。Andrew 在那里学习了如何审计反汇编后的二进文件, 并努力防止由于天气寒冷而被冻死。他拥有科罗拉多州立大学计算机系的理学学士学位, 并担任该州某些小型公司的安全顾问。现在当不写作的时候, 他在 Network Chemistry 公司担当资深安全分析员, 该公司是无线安全解决方案最主要的提供商。Andrew 还是无线漏洞及其应用项目 (<http://www.wirelessve.org>) 的编辑委员会成员之一, 并经常为他们刊登在 Network-World 上的无线安全专栏 (<http://www.networkworld.com/topics/wireless-security.html>) 出力。在业余时间里, 他为一个名为 Snort-Wireless (<http://snort-wireless.org>) 的项目组工作。该项目组主要研究如何为流行的开源 IDS Snort 增加无线入侵检测功能。

贡献者

下面人员对本书贡献了他们的技术和灵感:

- Oktay Altunergil 是 Free Linux CD 项目组 (<http://www.freelinuxcd.org>) 的创始人和 Turk-PHP.com (一个土耳其 PHP 门户网站) 的维护人员之一。另外, 他的专职工作是担任 Unix 系统管理员和 PHP 程序员。
- Michael D. (Mick) Bauer (<http://mick.wiremonkeys.org>) 是 Linux

Journal “Paranoid Penguin” 安全栏目的专栏作者。此外，他白天主要的工作是研究如何防止陌生人对银行计算机网络的攻击。

- Schuyler Erle (<http://nocat.net>) 是一个自由软件开发者和激进主义分子。他对绘图学、无线网络、社会与政治对软件的影响和语义网感兴趣。同时，Schuyler 还是 NoCatAuth 的主要开发人员，NoCatAuth 是一个具有领导地位的开源无线门户网站。
- Bob Fleck (<http://www.securesoftware.com>) 是 Secure Software 公司安全服务的主管。他从事于安全的开发环境和无线网络安全领域的研究，并且他也是《802.11 安全手册》（由 O'Reilly 出版）的合著者。可以在 <http://bluetooth.shmoo.com> 找到他最近在蓝牙安全方面的研究。
- Rob Flickenger (<http://nocat.net>) 是 O'Reilly 的 Hacks 系列图书的作者和编辑之一。他现在从事于多个项目并推动无线网络社区的建设。
- Preston Gralla 是 30 多本计算机与因特网著作的作者，这些书被翻译成 15 种语言，其中包括《Windows XP Hack》（由 O'Reilly 出版）、《Internet Annoyances》（由 O'Reilly 出版）、《Windows XP Power Hound》（由 Pogue 出版社出版）等。他从 PC 时代开始就撰写技术文章，Preston 曾经是多个全国性的报纸、杂志和网站的编辑，他是《PC Week》的初创编辑之一，在《PC/Computing》杂志先后担当过初创编辑、编辑和编辑部主任，并且担当过 ZDNet/CNet 的执行编辑。Preston 为大量杂志撰写过文章，其中包括 *PC Magazine*、*Computerworld*、*CIO Magazine*、*Computer Shopper*、*Los Angeles Times*、*USA Today* 和 *Dallas Morning News*（担任技术专栏作家）等。他曾经是 ZDNet/CNet 的技术专栏作家，现在是 TechTarget.com 网站的技术专栏作家。他关于技术的评论被国家公共电台评为“All Things Considered”，并获得计算机出版协会授予的计算机出版物最佳奖。在他的校订下，《PC/Computing》入围了全国杂志大奖 General Excellence 类的决赛。Preston 还是 O'Reilly 公司的 WindowsDevCenter.com 网站编辑。他和他的妻子及两个孩子住在马萨诸塞州 Cambridge 市——尽管他的女儿刚刚离开这个家去上大学去了。除了写书、文章和专栏以外，他还经常游泳、打网球、去看歌剧，有时还沉思于挂在他办公室墙上的公羊的头骨。
- Michael Lucas (<http://www.blackhelicopters.org/~mwlucas/>) 和他的妻子 Liz 及很多啮齿动物、鱼住在密歇根州底特律市的一个神出鬼没的

地方。他是一个宠物争论者，同时也是图书馆管理员和安全顾问。他现在在Great Lakes科技集团担任网络工程师和系统管理员。他是《Absolute BSD》、《Absolute OpenBSD》和《Cisco Routers》三本书的作者。现在准备写一本关于NetBSD方面的书。

- Matt Messier (<http://www.securesoftware.com>) 是 Secure Software 公司的工程主管，并且是一个拥有近 20 年编程经验的安全权威。他还是 O'Reilly 出版的《Secure Programming Cookbook for C》和《C++ and Network Security with OpenSSL》这两本书的合著者。Matt 还合著编写了《Safe C String Library (SafeStr), XXL, RATS, and EGADS》。
- Ivan Ristic (<http://www.modsecurity.org>) 是 Web 安全专家，他还是 mod_security 的作者，这是一种用于 Web 应用的开源入侵检测和预防的引擎。他是 OASIS 网页应用程序安全技术委员会的成员，他在那里从事于网页应用程序保护的标准制定。
- Hans Schefske 是 myITforum.com (<http://www.myitforum.com>) 网站的专栏作家。他有 8 年多工程与设计微软的基于 client/server 网络解决方案的架构与实现的经验。他在 IT 工业担当了很多项目的顾问和领导，他为例如 Nabisco、Prudential、AIG、Simpson、Thatcher and Bartlett、Novartis 和 Hoffman LaRoche Pharmaceuticals 这样的大型企业级公司提供在设计与实现其基础设施领域的专家技术经验。在 2003 年，由于 Hans 杰出的技术技能和主动地与大家分享知识，Hans 获得了微软存储管理服务 (SMS) 方面最有价值专家 (MVP) 奖。作为 myITforum.com 网站的技术作家，他为 IT 职业人员和管理员提供了技术信息、工具、脚本和实用工具，以便帮助他们更好地管理基于微软的解决方案。Hans 现在在佐治亚州亚特兰大市的一家大型电信公司担当资深 Active Directory 和 SMS 的顾问。
- Rod Trent 是 myITforum.com (<http://www.myitforum.com>) 网站的经理，他是微软 SMS 方面的首席专家。他有超过 18 年的从事 IT 业方面经验，其中 8 年他专注于研究 SMS。他是《Microsoft SMS Installer》、《Admin911:SMS》和《Windows 2000 IIS 5.0: A Beginner's Guide》(都是由 McGraw-Hill 出版社出版) 三本书的作者，另外还撰写了上千篇技术专题文章。myITforum.com 是第三方 SMS 支持的中心单元，同时也是一个 IT 职业人士和社区众所周知的在线聚集地。Rod 每年至少要在各

种会议上发表三次演讲，并且担当 NetImpress 有限公司 (<http://www.netimpress.com>) 的负责人。

- Mitch Tulloch (<http://www.mitit.com>) 是 MTIT 公司 (该公司位于加拿大的 Winnipeg 州，是一个 IT 内容开发公司) 的董事长。在 1998 年创建自己的公司之前，Mitch 在 Productivity Point International 公司担当微软认证训练员。在 Windows 管理、网络及安全方面，Mitch 是一个广泛公认的专家。他在配置 Windows 平台、产品和解决方案方面还获得了微软最有价值专家 (MVP) 奖。Mitch 现在还是 Jones 国际大学 (JIU) 的教授，在那里他教授信息安全管理方面的研究生课程，该课程是他和他的妻子 Ingrid Tulloch 一起为 JIU 大学的 MBA 开发的。Mitch 是 14 本书的作者，其中包括《Windows Server Hacks》(由 O'Reilly 出版)、《Windows Server 2003 in a Nutshell》(由 O'Reilly 出版)、《the Microsoft Encyclopedia of Networking》(由微软出版社出版)、《the Microsoft Encyclopedia of Security》(由微软出版社出版)、《IIS 6 Administration》(由 Osborne/McGraw-Hill 公司出版) 等。Mitch 还为例如《NetworkWorld》、《Microsoft Certified Professional Magazine》等业内杂志撰写特稿，并经常为 O'Reilly 的一些网站 (WindowsDevCenter.com、ITWorld.com 和 WindowsNetworking.com) 贡献文章。Mitch 的文章也被广泛地在其他 IT 网站 (例如 Computerworld.com、Smallbusiness.com，甚至是 CNN.com) 联合发表。
- John Viega (<http://www.securesoftware.com>) 是 Secure Software 公司的首席技术官和创始人。他也是许多软件安全书籍的合著者，其中包括《Secure Programming Cookbook for C and C++》(由 O'Reilly 出版) 和《Building Secure Software》(由 Addison-Wesley 出版)。此外，John 还负责大量软件安全工具，他还是 Mailman (一个 GNU 邮件列表管理器) 的发明者。

致谢

我再一次必须感谢 Karen (a.k.a. DJ Jackalope for Defcon attendees)，感谢她一直以来的支持和鼓励，感谢她忍受长期以来的辛劳。

我还要感谢 Brian Sawyer，感谢他在本书编写的整个过程中的耐心帮助。同时也要感谢 O'Reilly 公司的所有其他优秀的工作者，是他们的努力使得这本书变为切实可能。感谢 John Hoopes，他为这个版本在技术上进行了复查，John 的建议有助于使得本书变得更好。

最后要感谢的是我的父母，感谢他们持续不断地给我鼓励。

前言

在网络安全领域，人们常常会误解黑客这个词的意思。这是可以理解的，因为网络安全专家会使用工具来探测自身网络的稳健性，然而攻击者也可以用这些工具实施对因特网上主机的攻击。系统管理员合法地测试自己的机器，而系统破坏者则试图获得未授权的访问权限。他们在技术上和使用工具方面并没有什么不同，但是他们的意图却完全不同。毕竟，和任何强大的技术一样，没有一个安全工具天生是正义的或恶意的——这完全取决于如何使用该工具。同一个锤头可以用来建造城墙，也可以用来推倒城墙。

“白帽子”黑客和“黑帽子”黑客的区别并不在于他们所使用的工具或技术（甚至是他们帽子的颜色），而是在于他们的意图。这样的区别很微妙，但是却十分重要。白帽子黑客将构建安全的系统作为一项有趣的挑战，并且希望构建的系统的安全性可以彻底通过真实环境下的测试（假定该环境下攻击者拥有所有破坏系统的技术和工具）。黑帽子黑客（更合适的称呼是骇客）学习和白帽子黑客相同的技术，但是对构建系统的人员及他们攻击的服务器并不关心。黑帽子黑客使用自己的技术来破坏这些系统，从而获得自己个人的收益，他们经常破坏被他们渗透的系统。

当然，国际上有一些大胆的依靠技术“抢劫”的人以及一袭黑衣、叼着香烟、挥舞着笔记本的邪恶的计算机天才，他们的故事往往比单纯构建一个健壮网络的工程师的故事受人们欢迎，因此，“hacking”这个词在媒体中享有的声誉比较差。媒体通常将黑客看做是那些闯入系统或用计算机作为武器来发起破坏行为的人。然而那些解决计算机实际问题的人们通常将“hack”这个词看做是快速解决某个问题，或者是一个完成某件事情的巧妙的方法。而黑客