Broadview
www.broadview.com.cn

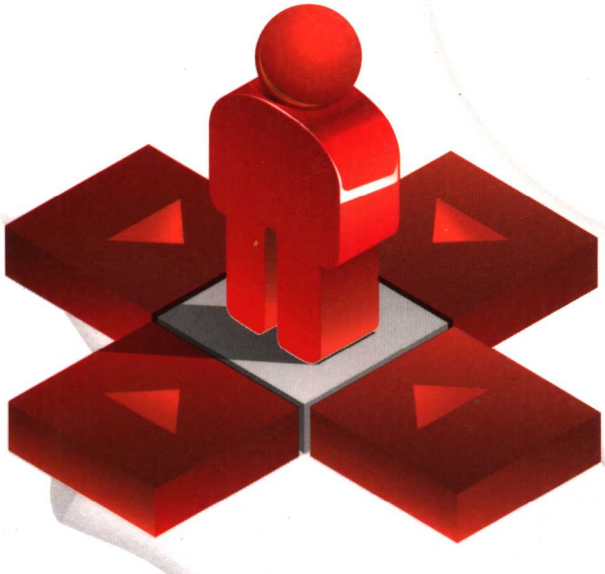
SYNGRESS®

安全技术大系

Stealing the Network : How to Own the Box

网络盗窃——10个黑客入侵的故事

[美] Ryan Russell Tim Mullen(Thor) FX Dan "Effugas" Kaminsky
Joe Grand Ken Pfeil Ido Dubrawsky 著
Mark Burnett Paul Craig
包春霞 冷发光 陈明慧 译



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

网络盗窃

——10个黑客入侵的故事

Stealing the Network: How to Own the Box

[美] Ryan Russell　Tim Mullen (Thor)　FX
Dan "Effugas" Kaminsky　Joe Grand
Ken Pfeil　Ido Durbrawsky
Mark Burnett　Paul Craig
著

包春霞　冷发光　陈明慧　译

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书是一本描写黑客进行网络盗窃的小说体裁的书，书中包含 10 个虚构的故事，但故事中黑客采用的技术却是真实的。本书的主要目的是揭示黑客攻击网络所用的武器和策略，对人们增强系统防范、确保网络安全起到警世作用。

本书适合于计算机程序员、系统管理员、网管和信息安全工作人员阅读，也适合于大中学生、研究生、教师、影视剧编导人员，以及各种职业和所有年龄段的电脑爱好者阅读。

版权贸易合同登记号　图字：01-2003-6399

图书在版编目（CIP）数据

网络盗窃——10 个黑客入侵的故事 /（美）拉塞尔（Russell, R.）等著；包春霞，冷发光，陈明慧译. 北京：电子工业出版社，2005. 3
（安全技术大系）
书名原文：Stealing the Network: How to Own the Box
ISBN 7-121-00886-6

Ⅰ. 网…　Ⅱ. ①拉…　②包…　③冷…　④陈…　Ⅲ. 长篇小说－美国－现代　Ⅳ. I712.45

中国版本图书馆 CIP 数据核字（2005）第 005337 号

责任编辑：顾慧芳
印　　刷：北京智力达印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×980　1/16　印张：16.5　字数：317 千字
印　　次：2005 年 3 月第 1 次印刷
印　　数：4000 册　　定价：32.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

译者序

内容简介

这不是一本关于安装、配置、更新、排错和防御的计算机书籍，也不是相互竞争的无数黑客书籍中的一本，而是用第一手素材编写的、文笔犀利的、具有煽动性的描写黑客攻击的系列短篇小说集，全书共由10个虚构的故事组成，每个故事都是从攻击者的视角来写的。他们采用攻击网络和系统的巷战战术，以获得对未授权网络系统和资源信息的访问，或者禁止有权访问的人访问他们要访问的系统和资源。

本书谈到了三种类型的攻击技术：靠软件、协议或系统探索获得配置缺陷的纯技术攻击；利用系统周围环境的弱点的物理攻击；通过信任的社会工程（SE）进行攻击。这三种攻击相结合，即综合利用系统的弱点、周围环境的弱点和人性的弱点，形成强大的攻击力量，并引起人们的恐慌。

有人说这给黑客攻击提供了指南，但是如果系统管理员和普通用户都有了黑客攻击的基本常识，就能从以上三个方面增强防范，从而保障系统安全。

尽管本书的人物刻画形象生动、栩栩如生，但这些人物并不是作者想突出的主题。本书的主题是黑帽子黑客们在攻击中所使用的工具，是无援的管理员所用的总是失效的防御方法。另外，书中对攻击的细节和人物心理所做的大量描述，还可以作为编制影视作品的参考。

阅读指导

尽管本书的故事是虚构的，但是所涉及到的技术却是真实的。人们可以将本书纯粹作为茶余饭后放松的消遣，体会故事中的冒险情节；技术人员也可从中看到技术的价值。

本书明显涉及到Cisco路由器，OpenSSH，Windows 2000的攻击技术，而且有许多命令行的图示。这些细节会让读者清楚地了解自己系统的弱点，并保持清醒，也能让安全工作者在巡视网络时引起注意。

本书采用虚构故事与真实的黑客相结合的手法，每章自成独立的一篇，读者可

以从头至尾阅读，也可以挑选某一章阅读。全书适当采用表格和图形来说明问题和举例，从而让读者对书中所阐述的方法能够有更深刻和更容易的理解。

本书通篇文笔犀利、幽默，对黑客的攻击过程的心路历程描绘真实深刻，读来回味无穷。

建议的读者

本书适合大中学生、研究生、教师及研究人员等各种职业和所有年龄段的人阅读。计算机程序员、对计算机安全感兴趣的人员，阅读本书更能了解本书中与黑客攻击有关的技术细节。系统管理员、网络管理员、信息安全方面的专家，阅读本书更能够透视黑客攻击的有可能发生的各个方面，对做好职责范围内的网络安全工作起到警世作用。电影、电视剧本编写人员，可以参考本书中的黑客攻击情节。

近年来出版发行的类似论及黑客的书籍很多，但像这样寓教于乐的计算机书籍还是第一本。尤其是本书既能完全满足电脑爱好者的阅读需求，又能给计算机安全人员提供指导。

本书虽然是一本虚构的小说集，但还是值得反复阅读、研究。

本书由包春霞负责翻译，参加翻译的有冷发光、陈明慧。由于译者水平有限，译稿尚不能完全展现作者的神来之笔和阐述艺术，敬请读者批评指正。

译　者

2005 年 1 月于北京

致　谢

感谢以下人员的热心支持，才使本书得以出版：

感谢 Group West 出版社的 Karen Cross，Lance Tilford，Meaghan Cunningham，Kim Wylie，Harry Kirchner，Kevin Votel，Kent Anderson，Frida Yara，Jon Mayes，John Mejak，Peg O'Donnell，Sandra Patterson，Betty Redmond，Roy Remer，Ron Shapiro，Patricial Kelly，Kristin Keith，Jennifer Pascal，Doug Reil，David Dahl，Janis Carpenter 和 Susan Fryer，感谢他们贡献了丰富的市场经验和专业技术。

感谢 Elseiver Science 非常努力的工作团队，包括 Jonathan Bunkell，AnnHelen Lindeholm，Duncan Enright，David Burton，Rosanna Ramacciotti，Robert Fairbrother，Miguel Sanchez，Klaus Beran 和 Rosie Moss，他们让我们有了十分宏观的概念。

感谢 STP 发行社的 David Buckland，Wendi Wong，Daniel Loh，Marie Chieng，Lucy Chong，Leslie Lim，Audrey Gan 和 Joseph Chan，感谢他们热情地接受了本书。

感谢 Acorn 出版社大名鼎鼎的 Sung June 给予了大力支持。

感谢 Jackie Gross & Associates 的 Jackie Gross，Gayle Voycey，Alexia Penny，Anik Robitaille，Craig Siddall，Darlene Morrow，Iolanda Miller，Jane Mackay 和 Marie Skelly，感谢他们在加拿大代理我们产品所给予的帮助和热情。

感谢 Lois Fraser，Connie McMenemy，Shannon Russell 以及 Jaguar 图书小组的许许多多其他的人，感谢他们帮助在加拿大批量发行了 Syngress 出版社的书。

感谢 Woodslane 的 David Scott，Tricia Wilden，Marilla Burgess，Annette Scott，Geoff Ebbs，Hedley Partis，Bec Lowe 和 Mark Langley 在澳大利亚、新西兰、巴布亚新几内亚、斐济、所罗门岛和库克岛发行了本书。

全球出版社的 Winston Lim 帮助和支持了 Syngress 出版社的书在菲律宾发行。

感谢黑帽子的 Ping Look 和 Jeff Moss 在计算机安全领域的无价探索及他们对 Syngress 出版工作的支持。还要特别感谢 Jeff 为本书写了前言，Ping 为本书的封面提供了专业设计。

Syngress 出版社要特别向 Ryan Russel 表示感谢。Ryan 多年来一直是我们出版工作的一个重要成员——他是一个很有天才的作家和技术编辑，是一个全才——谢谢你，Ryan。

贡献者

Dan Kaminsky，即著名的 **Effugas**，是 Avaya 的企业安全实践的资深顾问，他在那儿从事大规模安全体系结构方面的工作。Dan 曾在 Cisco 公司工作两年，有为跨组织的网络监视系统设计安全体系结构的经验，他因在极快速端口巡视器 Scanrand（它是“paketto keiretsu”的一部分，操纵 TCP/IP 网络用的一个新型和不同寻常战略的工具集）方面的工作而出名。他写了《黑客检验你的网络》（第二版）（Syngress 出版社，ISBN：1-928994-70-9）的“检验和通道”一章，并已经在几个主要的专业会议上提交了介绍：例如 LinuxWorld，DefCon 和过去的黑帽子简报。Dan 负责动态发布 OpenSSH 的补丁，将 VPN 样式的主要功能集成到广泛部署的密码工具箱中。他从 1997 年开始发起了跨学科的 DoxPara 研究，寻求将心理和技术理论相结合，为现场中并非理想而是非常实际的环境创造更有效的系统。Dan 现住在加州的硅谷。

过去的几年中，Phenoelit 的 **FX** 在 Internet 基础设施所面临的安全问题上花了不少时间，包括 Cisco 路由器的基于协议的攻击和探测。他在几个专业会议上提出了研究结果，例如 DefCon 会议、黑帽子简报和无序通讯大会。FX 现在被 N.runs Gmbh 聘任为安全解决方案顾问，为欧洲的主要客户做各种安全审计。他专门研究客户应用和黑盒子设备的安全评估与测试。FX 喜欢黑客，并常跟 Phenoelit 的朋友在一起，但他不会做他的母亲、朋友，尤其是给了他持久的关心和爱的年轻妻子 Bine 所不能理解的事情。

Mark Burnett 是一个独立安全顾问、自由撰稿人，Windows 的 IISWeb 服务器安全专家。Mark 是《最大化 Windows 安全》和 Tom Shinder 博士的《ISA 服务器及拓展：Microsoft 企业网络现实安全解决方案》（Syngress 出版社，ISBN：1-931836-66-3）的合作者。他是 Syngress 出版社《Microfot，UNIX，Oracle 的主机和网络安全》（ISBN：1-931836-69-8）的参与者和技术编辑。Mark 在多个安全会议上发过言，在《Windows &. NET 信息安全》、《Windows Web 解决方案》、《安全管理员》杂志上发表了多篇文章，是 SecurityFouce.com 的长期贡献者。Mark 也在他自己的 Web 站点 IISSecurity.info 上发表文章。

Joe Grand 是 Grand Idea Studio 公司的总裁兼 CEO，这是一家产品设计和开发公司，它通过知识产权许可将独一无二的发明带入市场。作为电子工程师，Joe Grand 的许多发明，包括消费者设备、医疗产品、视频游戏和玩具，已销售到世界各地。他是计算机

安全界的名人，还是传奇黑客智囊团的前成员，Joe 有关产品设计和分析、移动设备和数字法庭的前导研究 L0pht，已在多个行业杂志上发表。他参与编写了《穿透你网络的黑客》（第二版）（Syngress 出版社，ISBN1-928994-70-9）。Joe 在美国参议院政府事务委员会面前证实了关于州政府和本国的计算机安全。他参与了美国海事研究生院 INFOSEC 的学习和研究，美国空军部门的特别调查，USENIX 安全讨论会和 IBM Thomas J.Watson 研究中心的工作。Joe 是一个个人探索者，他在多个大学和研究论坛发言。

Ido Dubrawsky（CCNA，CCDA，SCSA）是 Cisco 系统公司 SAFE 体系结构小组的网络安全体系架构师。其职责包括研究网络安全设计及其实施。Ido 曾经是美国得克萨斯州奥斯汀的 Cisco 安全顾问服务的成员，他在那儿为客户做安全状况评估和入侵测试，并为安全设计评审提供技术咨询。Ido 还是安全咨询服务无线网络评估工具集的合作开发者之一。他的特长是 Cisco 路由器和交换机、PIX 防火墙、Cisco 入侵检测系统和 Solaries 操作系统。他对免费的入侵检测系统软件特别感兴趣。Ido 拥有位于奥斯汀的 Texas 大学的航空工程的学士和硕士学位，是 USENIX 和 SAGE 的长期成员。他给 Sysadmin 以及 SecurityFocus 在线写了许多关于 Solaris 安全和网络安全的文章。他是《黑客穿透 Sun Solaris8》（Syngress 出版社，ISBN：1-928994-44-X）和《穿透你网络的黑客》（第二版）（Syngress，ISBN：1-928994-70-9）的贡献者之一。现在他跟家人一起住在美国 MD 的 Silver Spring。

Paul Craig 是新西兰一家大型广播公司的网络管理员。他有各种网络和操作系统安全的经验，在数字权限管理（DRM）和拷贝保护系统方面也做过大量的研究和开发。

Ken Pfeil 是纽约的一位有着 Avaya 企业安全咨询实践的高级安全顾问。Ken 有在微软、Dell、Identix 和 Merrill Lynch 等公司 18 年的丰富的 IT 和安全经验，担任的职位从系统技术体系架构师到首席安全官。在微软时，Ken 与人合作撰写了《微软的最佳企业安全实践》白皮书系列，他是 MCSE 考试、《Windows 2000 安全设计》及同等正式课程的技术贡献者之一，Ken 合作和参与编写的其他书籍还有《穿透你网络的黑客》（第二版）（Syngress 出版社，ISBN：1-928994-70-9），《网络防火墙和 VPN 权威指南》、《Web 服务安全》，《安全规划和灾难恢复》及《CISSP 学习指南》。Ken 拥有许多行业认证，他还是 Comp TIA+安全认证的主要顾问。1998 年 Ken 创建了 NT 工具箱 Web 站点，在那里他预见到了 GFI 软件要到 2002 年才能获得全面的推广。Ken 是 ISSA 国际私人顾问委员会、纽约电子犯罪特遣队、IEEE、IETF 和 CSI 的成员。

Timothy Mullen 是 AnchorIS.com 公司的 CIO 和首席软件架构师，企业财务解决方案的安全开发人员。Mullen 还是安全中心微软部分的专栏作家，是 InFocus 技术文章的长期撰稿人。作为著名作家，他又是“Hammer Of God”安全 COOP 小组的发起人。

技术编辑

Ryan Russell 已在 IT 领域工作了 13 年，最近的 7 年侧重于信息安全。他是《穿透你网络的黑客：Internet 间谍》的主要作者（Syngress 出版社，ISBN：1-928994-15-6），也是穿透网络的黑客系列书籍的长期技术编辑。他还是 Syngress 出版社的《Snort 2.0 入侵检测》（ISBN：1-931836-74-4）的技术顾问。Ryan 建立了 Vuln-dev 邮件列表，曾经有 3 年一直以“蓝色野猪”为别名。他常常是安全会议上的演讲者，也经常参加安全邮件列表和 Web 站点讨论。Ryan 是 AnchorlS 公司的软件工程主管，在那里他一直在开发反蠕虫产品，Enforcer。解剖蠕虫是他的爱好之一。

前　言

《网络盗窃——10 个黑客入侵的故事》是一本别具一格的虚幻小说。我收集了一些技术真实的虚构的故事。尽管这些特定的事情没有发生过，但也没理由说他们就不能这样做。你可能提出异议说，它为网络犯罪提供了指南，但是我要说本书还提供了一些其他的东西：它让我们看见一些当代有创造性思想的最好的黑客，甚至这些黑客称这是一种智力游戏。由 K0resh 创造并印在 DEFCON 牌衬衫上的俗语“精神状态是根本”总结得很好：即使你有这种技能，但如果精神不够坚韧，也决不能到达顶峰。这就是黑客精英与想要做黑客两者之间区别的标志。

说起黑客，我的意思并不指犯罪。自从大量媒体开始报道计算机入侵以来，有关这个词就有许多混淆。最初，这是对技术熟练的计算机程序员和系统管理员的称赞。如果你的系统有问题需要快速修复，就可以让最好的黑客来做。他们会找到源代码来修复，因为他们知道整体的蓝图。其他人可能知道系统的不同部分如何工作，而黑客即使是在最小的细节上工作时他们心中也有一幅整体蓝图。这种洞察力让他们在解决问题时有更大的灵活性，因为他们并不把希望寄托在他们正在努力做的第一件事情上。

《黑客：计算机革命的英雄》，Steven levy 著（1984），一书真实地记录了早期的黑客精英，并为以后发生的事情做了铺垫。其后，“黑客”一词被媒体和市场运作大肆宣传为某种邪恶的东西。它现已成为流行的方便用语，所以媒体不是简单地说某人是一个“黑客罪犯”，而只是叫他“黑客”。通常你不会简单地将一台犯罪用的电动机描述为机器，同样对于黑客也不会如此。

在 1955 年的电影《黑客》中，当第一个 Web 站点磨灭的时候，竞争就开始了。Web 毁灭团伙晚上出来活动。几个小组在攻击 Web 站点的数量和速度上比赛看谁能胜出。没有人是安全的，包括纽约时报和白宫。自此，大多数在线的犯罪黑客都表现为“脚本—戏弄—出局”——这些人虽没有很多的知识却持有很好的工具。这一大群人产生的背景噪声，安全专家在防御他们的网络时是必须要加以处理的。你怎么知道对你的攻击是简单的脚本，还是真正老练的攻击战役的开始呢？许多时候你无从知道。我的日志记录了大量入侵企图，但是我不知道哪一个是比较严重的企图，哪一个只是大量弱点的自动巡视。不光我没有时间或资源来决定哪一个威胁是真的，其他人也决定不了。许多攻击者就指望这个事实。

攻击者是如何做的呢？通常，有三种类型的攻击。纯技术攻击依靠软件、协议或系统暴露出的配置缺陷，利用这些以获得访问。这些攻击可以来自这颗行星上的许多位置，他们一般通过许多系统链接使最终源代码模糊。现在世界上大多数的攻击者都属于这种类型，因为他们很易于自动化，也最容易防御。

物理攻击依靠系统周围的弱点。可以采用寻求废弃密码和配置信息或秘密使用计算机系统上的按键登录设备等形式。过去，人们物理地接进传真电话线来记录文档，进入电话系统去窃听呼叫信号，蹑手蹑脚通过电话公司的中心办公室。这些攻击绕过信息安全防御系统直捣目标。他们之所以得逞，是因为人们认为物理安全与信息安全是分开的。为了执行物理攻击，你必须要在信息所在的地方；有些事会极大地减少我的风险，因为许多印度黑客不大可能跳上一架喷气式飞机来攻击我在西雅图的网络。这些攻击虽然很难防御但却很少可能发生。

社会工程（SE）攻击依靠信任。通过说服某人让他信任你，在电话上或私下里，你可以了解各种秘密。通过给一个公司的客服打电话并假装成一个新雇员，就有可能获得通过 MODEM 拨号到银行的电话号码，应该如何配置你的软件，是否认为防御系统的技术人员有能力让你出去。这些攻击一般在对目标做了实质性研究之后通过电话执行。在大公司里很难防御，因为通常每个人都想相互帮助以解决问题，右边的人往往不知道左边的人的职责是什么。因为这些攻击是面向语音的，他们可以从世界的任何能使用电话线的地方执行。正像技术攻击一样，为隐藏其位置，有技能的 SE 攻击者会通过许多次跳跃来链接他们的语音呼叫。

当罪犯综合使用这些攻击时，他们就真能引起恐慌了。只有极端偏执狂者才能够防御他们，但是成为偏执狂的代价常常连最大的公司也是要禁止的。例如，在 1989 年，当 Kevin Poulson 想知道 Pac Bell 是否在他的电话上盗用线路，他决定查明真相。还有什么比扮演成电话公司的职员四处查看更好的办法呢？他能完全用电话公司的行话侃侃而谈，他能穿着工作服四处走动。他恰巧走到位于旧金山的安全部门的办公室，在公司的文件柜中阅读了关于他自己的信息，他知道他们在监视他。

在为 Ernst&Young 工作期间，有人雇我闯入一家地区银行的公司总部。我们躲在银行的楼里，直到清洁工来了，我们就能跟着其他两个穿着套装的人走进贷款部。我们假装知道要干什么。当那个部门的最后一位职员问我们的时候，我们说是跟审计员一起的。这就足以使那个雇员让我们单独留下了；毕竟，银行总是要有人审计的。此时，就该执行我们的任务了。在秘书的计算机上有键盘记录器，银行行长的办公室上了锁不让我们进去，我们有机会便在银行系统中建立一个立足之处。一旦从内部开始攻击网络，游戏差不多就要结束了。

现实世界中很少有这么酷的攻击。让我们现在来理解它。为了执行这些攻击，你必须要有极端“内在的坚韧”并面对它，只有最被激发的攻击者才会冒这个险。在这种情况下，门卫真的有枪，只是不会像 Kevin 那样：我有银行行长签署的“通行卡”。

在现实世界中，黑客总是追逐最容易得手的东西。他们冒最小的风险却要获得最大的回报。他们常常单独行动或者结成团伙，没有政府基金，也不属于世界犯罪组织。他们有的只是业余时间和非常大的好奇心。我向你保证：攻击是很花时间的。一些最好的黑客在一次探索上就花了数月。所有那样的探索结束后，结果可能会证明是不可靠或根本不起作用！攻入一个站点也是同样的方式。黑客在一个站点上可能要花数周侦察，只要发现没有可行的进入路径，就得重头再来。

在电影里，好莱坞倾向于掩盖有关涉及攻击时间的事实。谁想看几个星期黑客做研究和测试 Bug？例如银行抢劫者的行动未必是一个可看的活动，也不是观众有体验或与他们有关的事情。在电影《黑客》中，导演试图用视觉上的蒙太奇和一些时间流逝效果来表达。在 Swordfish 中，黑客被描绘为通过喝酒被鼓舞，在视觉上一夜之间构造一个病毒。一部最老的黑客电影《战争游戏》是在大屏幕上最接近现实的一部。在那部电影中，主角花了相当长的时间来研究目标，试图采用不同的方法进行攻击，但最后被人发现并被追捕。

但是，假如……如果攻击者被高度激励并有高超的技能，会怎么样？假如他们有勇气和技能来执行老练的攻击呢？你正在看的本书作者喝了一些酒后，很快就会推测出哪些是可能的。如今，他们花了时间和努力编著了这 10 个探讨黑客如何盗窃网络的故事。

于 1983 年播出的电影《战争游戏》给我们这一代人充了电，并让我开始进入黑客行列。就像虚构的向公众介绍黑客的电影那样，我希望本书能激发并鼓舞新一代的人们能挑战常规的感知能力并总是问问自己，“假如……”

——Jeff Moss
Black Hat 公司
www.blackhat.com
西雅图，2003 年

目　录

亡要好许多。我以为自己成功了——只要攻入不安全的系统就可以挣到免税的美元，接着就是最终的抢劫：闯入一个敏感的实验室窃取美国一直在开发的最重要武器的资料。现在一切都过去了。我现在在一个陌生的国家以一种新的身份，为一个刚从学校出来的人做着愚蠢的工作。每天都必须面对毫无意义的公司策略，监视着不能为自己考虑而只是盲目地听从命令的雇员，而现在我就是其中的一员。我认为这只是办公室里的又一天。

h3X 是黑客，或者更准确地说是个女黑客（hexe 一词来自德语女巫）。现在 h3X 正在寻找一些打印机。打印机是隐藏文件并与一些匿名的家伙们共享文件的最好的地方。因为没有太多人知道这个，h3X 喜欢在打印机上保存探索代码和其他古怪的东西，使她的密友注意实际上在这些打印机上运行的 Web 服务器。她在……之前就这样做了。

我的眼睛慢慢睁开，看着发出尖叫声的电话和液晶显示屏在昏暗的房间里闪烁。我接了电话。

“Hmm……，喂？”

“Yo Dex，我是 Silver Surfer。看，我有一个题目需要你帮忙。干点工作好吗？”

Silver Surfer 和我交往有些年头了。他是第一个让我开始以黑客赚钱的人。我为他工作已将近两年。尽管我信任他，但我们并不知道彼此的真实姓名。我的思想慢慢活跃起来。我早上 5 点才睡，现在刚上午 10 点。还有点迷迷糊糊的。

“好的，但是目标是什么？最后期限是什么时候？”

“Denizeit 的 Digital Designer V3，据称今天最后完成，本周末就会上市，周先生自己要这个题目。如果你能在它上市之前给我们搞到就能挣一大笔钱。市场上已经有相当大的需求了。”

“好吧，我一喝完咖啡就看看我能做什么。”

“谢谢伙计。拜托你。”有一声挂断电话的响声。

我不仅连接到私有无线网上，也能访问 Internet。我一旦在网上，底层的无线协议就是透明的了，并且我就能像在标准有线网上一样操作。从一个黑客的观点来看这太好了。有人只是进入星型主干，再跳到他们的无线网，并攻击 Internet 上的其它

系统，被发现的可能性很小。公用无线网络对保持你的匿名是完美的。

30 分钟后，我用安全 Web 邮件客户端检查完 E-mail，阅读了新闻，在 eBay 上为我一直在寻找的一对罕见的 20 世纪 50 年代的棒球卡出了价。我又困了，还有半小时才开始登机。

我最喜欢的娱乐之一就是让无猜疑的人为我做肮脏的事。其关键是能通过所谓的社会反向工程获得知识，无非是对人的分析。你能用社会反向工程做什么呢？通过观察人们如何对待计算机技术，你就能很快认识到实际上人们是多么的一致。你将看到能用作人类行为路线图的模式。

人们是难以置信地可预言的。作为一个十几岁的少年，我习惯于看晚间著名的智力型电视节目。当他老是猜测观众成员的社会安全号时我就会留心。起初我并没有什么太深的印象——对他来说，将自己置于大庭广众之下有多困难？他接着做的引起了我的兴趣：他获得了电视观众的参与。他让在家的每个人想起一种蔬菜。我自己想起的是胡萝卜。令我惊讶的是，“胡萝卜”的单词突然出现在电视屏幕上。这只是一次幸运的猜测。

一般情况下，我并不是一个爱报复的人，我认为只是什么事情冒犯了我。当这些发生时，我回击了——只是有点难。当他们告诉我我将要被解雇时，我非常生气。是谁以为自己能为所欲为？我为这些愚蠢的家伙们卖了 7 年的命，每个周末加班，工作到第二天凌晨 3 点，为什么？可恶的几周就对我做了了断？我创建了这个 IT 组织，他们回过头来就说不再需要我了。他们说已经决定将所有的 IT 业务外包给 ICBM 全球服务公司了。

解雇的收据就要过期了，花了将近一年的时间来试图另辟经济途径，我以为该是回报的时间了。也许在过去的几年中我技术上有些落后了，但我还是有足够的能力打击这些杂种们的。我相信能获得一些值得卖给竞争对手的信息，或者用这些信息获得这些公司的聘用。你能想像出当他们知道自己的网络被黑了时脸上的表情吗？如果我是墙上的一只苍蝇就好了。

黑帽子防御：你要比敌人能够更多地了解你的网络……

SMB——服务器消息块（Server Message Block）的缩写，是 NBT（TCP/IP 之上

的 NetBios 协议）之后最后的协议，是老式的 IBM 局域网管理者和它的现代第 n 代克隆，Windows 文件共享。当像 ECFDEECACACACACACACACACACACACA 那样的大块文字从屏幕上喷涌出来时，Elena 笑了。从前，一个相当有办法的 IBM 工程师曾裁决："第一级编码"可能是写名为"BSD"的一种关系方式。可读吗？除非你是幸运的 Kenneth Casson Leighton，他能够从十六进制导出文件中完全体验原始的 SMB，一个后现代的吞剑者的化身。

黑客怎么思考是很奇怪的。你会认为白帽子的黑客在频谱的一端，而黑帽子的黑客在另外一端。恰恰相反，他们都在频谱的同一端。其余的世界在另一端。实际上，在责任攻击和罪恶攻击之间没有什么区别。任何一种攻击都是攻击。惟一的区别是内容。也许这就是为什么黑帽子合法行事如此自然，为什么白帽子变黑帽子也是如此容易。两者之间的界限是明显的，大多由伦理和法律来定义。对于黑客来说，伦理和法律正像其他别的任何事情一样都有漏洞。

许多安全公司喜欢雇用改邪归正的黑客。事实上黑客没有改邪归正这样的事情。他们可能改变攻击的重点和改变报酬，但是他们决不会从良。给黑客支付报酬并不能使他们更少像一个黑客。

黑客有点像艺术家。一个艺术家要学会画他们想画的东西。他们能画高山、动物，或许画裸体。他们能用他们想用的任何媒体、任何曲线和任何颜色。如果有一天艺术家有一份做艺术的工作，他就变成了商业艺术家。惟一的区别是现在他要画的是别人让他画的东西。

本书包含一系列虚构的短篇小说，以说明日常用来犯罪的黑客技术。虽然这些故事是虚构的，但危险却显然是真实的。同样，我们编写了本附录，它对如何减轻本书详细陈述的这些攻击的影响进行了探讨。虽然这些安全规则并不是一个全面的参考，但也能给读者提供阻止黑客盗窃你网络的一些基本知识。

Chapter 1

第1章 隐藏和盗窃

——Ido Dubrawsky 著

这并不是很困难。几乎没有我想像的那么困难。事实上，真的相当容易。你只是得考虑一下，仅此而已。似乎许多安全人士都以为把路由器和防火墙及入侵检测系统（IDSs）放在适当的位置就能让网络安全。但事实上未必是这种情况。只要是网络或服务器上某个位置的一点微小的配置错误，就能给某个人的进入提供足够的缝隙。