黑客大曝光

计算机信息安全旷世之作·全球销量第一

网络安全机密与解决方案

Hacking Exposed Network Security Secrets & Solutions

第6版

现在，摆在你面前的是有史以来写得最为成功的一本信息安全旷世之作，书中介绍的黑客防范技术和方法都是无价之宝，完全可以协助个人、企业、国家打赢 Cyber 空间的犯罪阻击战！

Dave DeWalt
迈克菲（McAfee）公司总裁兼CEO

Stuart McClure (CISSP, CNE, CCSE)
Joel Scambray (CISSP)
George Kurtz (CISSP, CISA, CPA)
著

钟向群
郑　林
译
审校

McGraw Hill

清华大学出版社

黑客大曝光

网络安全机密与解决方案

第6版

Stuart McClure (CISSP, CNE, CCSE)
Joel Scambray (CISSP)
George Kurtz (CISSP, CISA, CPA) 著
钟向群 译
郑 林 审校

清华大学出版社
北 京

本书版权登记号：图字：01-2009-4892

内 容 简 介

《黑客大曝光》是全球销量第一的计算机信息安全图书，被信息安全界奉为圣经。作者独创“黑客大曝光方法学”，从攻防两方面系统阐述了最常见的黑客入侵手段及对应的防御策略。

本书在前5版的基础上对内容进行全面扩充和更新。开篇仍以“踩点”→“扫描”→“查点”三部曲，拉开黑客入侵的序幕。之后从“系统”、“基础设施”、“应用程序和数据”三个方面对黑客攻击惯用手段进行剖析：“系统攻击”篇针对Windows、UNIX系统攻击给出精辟分析；“基础设施攻击”篇展示4类基础设施的攻击手段和防范策略——远程连接和VoIP攻击、网络设备攻击、无线攻击和硬件攻击；“应用程序和数据攻击”篇则引入全新概念——应用程序代码攻击，详细解释源代码泄露、Web应用程序攻击、攻击因特网用户等最新黑客技术手段。

本书面向各行各业、政府机关、大专院校关注信息安全的从业人员，是信息系统安全专业人士的权威指南，也可作为信息安全相关专业的教材教辅用书。

图书在版编目（CIP）数据

黑客大曝光：网络安全机密与解决方案：第6版 /（美）麦克卢尔（McClure,S.），（美）斯卡姆布赖（Scambray,J.），（美）库尔茨（Kurtz,G.）著；钟向群译. —北京：清华大学出版社，2010.1
书名原文：Hacking Exposed: Network Security Secrets & Solutions
ISBN 978-7-302-21822-7
I. ①黑… II. ①麦… ②斯… ③库… ④钟… III.①计算机网络—安全技术 IV. ①TP393.08
中国版本图书馆CIP数据核字（2009）第233678号

责任编辑：夏非彼　卢　亮
责任校对：闫秀华
责任印制：何芊
出版发行：清华大学出版社　　**地　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　编**：100084
社 总 机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×230　　**印　张**：42.75　　**字　数**：958千字
版　　次：2010年1月第1版　　**印　次**：2010年1月第1次印刷
印　　数：1~4000
定　　价：89.00元

本书如存在文字不清、漏印以及缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。
联系电话：（010）62770177转3103　产品编号：033796-01

作者简介

Stuart McClure, CISSP, CNE, CCSE

Stuart McClure 对各种安全产品有着全面深入的了解，是当今信息安全领域公认的权威之一。作为一名在安全方面有很多著作并且广受欢迎的卓有远见者，McClure 在技术、实际操作和财务管理方面都有着超过 20 多年的深厚的技术积累和领导艺术。

Stuart McClure 是 McAfee 公司高级副总裁兼风险与法规遵从业务部门总经理，主要负责制定风险管理及法规遵从产品的发展以及服务解决方案。2008 年，Stuart McClure 担任世界上最大的卫生保健组织 Kaiser Permanente 公司安全服务部的执行董事，他管理着 140 名安全专家，并且负责安全法规遵从、监察、咨询、架构和运营工作。2005 年，McClure 成为 McAfee 公司全球威胁部的资深副总裁，作为最高领导管理 AVERT 部门。AVERT 是 McAfee 公司负责病毒、恶意软件、攻击检测特征和启发式响应的部门，拥有来自全世界的超过 140 名顶尖的程序员、工程师和安全专家。他的部门监控着全球的安全威胁并且提供不间断的特征发布服务。McClure 在担负公司战略层面的很多责任之外，还负责为部门提供战略视野和营销策略，以便以消费者和公众的眼光对公司的安全产品做出客观的评价。同时，他还创办了一本致力于监控和披露全球安全威胁的半年刊杂志 *Sage Magazine*。

在掌管 AVERT 部门之前，Stuart McClure 是 McAfee 公司负责风险管理产品研发的资深副总裁，主要负责制定 McAfee Foundstone 系列风险化解和管理解决方案的产品研发和市场营销战略。在加盟 McAfee 公司之前，McClure 是 Foundstone 公司的创始人、总裁和首席技术执行官，该公司于 2004 年 10 月被 McAfee 公司以 8600 万美元收购。在 Foundstone 公司，McClure 既是产品规划和发展策略方面的领路人，也是所有技术开发、技术支持以及项目实施工作的具体领导者。在 McClure 的带领下，Foundstone 公司自 1999 年成立以来每年的业绩增长率都超过了 100%。同时，McClure 也是该公司最主要的专利 No.7152105 的作者。

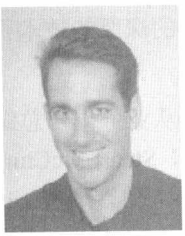
在 1999 年，他牵头编写了有史以来最畅销的计算机信息安全类书籍——*Hacking Exposed: Network Security Secrets and Solutions*，该书迄今已销售了 50 万册，被翻译成 26 种语言以上，在计算机类书籍中排名第四，并且成为历史上最畅销的计算机安全类书籍之一。此外，Stuart 还是 *Hacking Exposed: Windows 2000*（McGraw-Hill 出版公司）和 *Web Hacking: Attacks and Defense*（Addison-Wesley 出版公司）的作者之一。

在加入 Foundstone 公司之前，Stuart 曾在 Ernst & Young 咨询公司的 National Security Profiling Team 担任过多种与信息安全和 IT 有关的领导职务，他还在 InfoWorld 杂志的测试中心担任过两年的行业分析师，在加利福尼亚州政府和地方政府担任过五年的 IT 部门主管，有两年

自营一家 IT 咨询公司，还有两年在科罗拉多州立大学负责 IT 事务。

Stuart 拥有科罗拉多州立大学的心理学和哲学学士学位，同时他还学习了大量的计算机科学与应用专业的课程，后来又陆续获得了包括 ISC2 机构的 CISSP、Novell 公司的 CNE 以及 Check Point 公司的 CCSE 在内的多个证书。

Joel Scambray, CISSP



Joel Scambray 是提供战略安全咨询服务的 Consciere 公司的创始人和 CEO。他的服务对象包括刚刚创建的小公司到财富 50 强成员公司，在应对信息安全挑战与机遇领域具有超过 12 年的经验。

Scambray 的个人经历包括执行官、技术咨询专家以及企业家。他曾是微软公司的高级总监，在接手 Windows 平台服务部专注于安全技术架构之前，他从事微软在线服务安全工作超过 3 年。Joel 也是提供安全软件和服务的新公司 Foundstone 的创始人之一，并且成功地使公司被 McAfee 公司以 8600 万美元收购。他还担任过 Ernst & Young 咨询公司的经理、Microsoft TechNet 网站的安全专栏作家、InfoWorld 杂志的主编以及一家大型商业房地产公司的 IT 总监。

自从 1999 年 *Hacking Exposed: Network Security Secrets and Solutions* 一书出版以来，Joel Scambray 一直是该书的作者之一。他同时也是 *Windows Hacking Exposed* 和 *Web Applications Hacking Exposed* 系列书籍（McGraw-Hill 出版公司）的主要作者。

不论是对于小的创新型企业还是著名的跨国公司，Scambray 在技术开发、IT 运营安全和客户咨询方面都拥有大量的实际经验。Joel 还在很多场合作过信息安全方面的演讲，包括 Black Hat、I-4、ASEM（The Asia Europe Meeting，亚欧会议）等著名的论坛峰会，CERT、The Computer Security Institute（CSI，计算机安全技术学院）、ISSA、ISACA、SANS、各种私营企业以及 KISA（Korean Information Security Agency）、FBI 和 RCMP 等政府机构。

Scambray 还拥有加州大学戴维斯分校的学士学位，加州大学洛杉矶分校的硕士学位以及 CISSP 证书。

George Kurtz, CISSP, CISA, CPA

在担任 McAfee 公司的风险及法规遵从部的资深副总裁和总经理之前，George Kurtz 是 Foundstone 公司的 CEO。Kurtz 在安全领域有超过 16 年的工作经验并且帮助数以百计的组织和政府机构解决了无数高难度的安全问题。作为一名国际公认的信息安全专家、专著作者和企业家，George 经常在该领域的各年会上发表演讲，他的言论经常出现在众多顶级刊物和公共媒体上，其中包括 CNN 电视台、Fox News（福克斯新闻）、ABC World News（ABC

世界新闻）、Wall Street Journal（华尔街邮报）、Time（时代杂志）、USA Today（今日美国杂志）、Associated Press、ComputerWorld、eWeek、CNET 等。

George Kurtz 目前主要负责 McAfee 公司风险法规遵从部全球业务的增长，他成功地帮助 McAfee 公司从单一产品供应商变成安全风险管理和法规遵从优化解决方案的集成供应商。在他的任期内，McAfee 公司的企业总体平均售价（ASP，average selling price）及业界的竞争地位得到了显著提升。在此之前，Kurtz 担任 McAfee 公司 SVP 部门的主管，负责全球范围内公司产品组合的销量增长。

在加盟 McAfee 公司之前，Kurtz 是 Foundstone 公司的 CEO，该公司于 2004 年 10 月被 McAfee 公司收购。Kurtz 利用自己的商业远见和技术天份为 Foundstone 公司制定了发展战略，使该公司在众多的信息安全解决方案提供商中脱颖而出。在 1999 年与其他人合伙创办 Foundstone 公司之后，Kurtz 以自己的远见和企业家精神吸引了一大批世界一流的人才加入该公司的管理团队，并把 Foundstone 经营成一家最成功和最主要的私营信息安全公司。在成功地募集到了超过 2000 万美元的风险投资后，Kurtz 带领公司快速发展，在四年内扩张到雇员超过 135 名。Kurtz 的企业家精神是把 Foundstone 公司定位于业内顶尖的安全解决方案供应商。

在合伙创办 Foundstone 公司之前，Kurtz 是 Ernst & Young 咨询公司信息安全服务部门的全美总经理。在其任期内，Kurtz 主要负责管理和展示大量的电子商务方面的安全解决方案，客户覆盖金融服务、制造业、零售业、制药行业和高科技产业等各个领域。在加入 Ernst & Young 公司之前，Kurtz 是 Price Waterhouse Coopers 公司负责全球因特网信息安全测试项目研发工作的经理。

在 George Kurtz 的领导下，他本人和 Foundstone 公司获得了无数的殊荣：Inc 的“全球 500 强公司”，南加州软件协会颁发的“2003 年度、2005 年度南加州著名软件企业”、Fast 公司颁布的“进步最快 50 强”、美国电子协会的“杰出企业家”、Deloitte 的“进步最快 50 强”、Ernst & Young 公司的“年度优秀企业家”和 Orange 县的“热门人物 25 强”等等。

George 拥有信息安全行业的多项证书，包括 CISSP（Certified Information Systems Security Professional）、CISA（Certified Information Systems Auditor）和 CPA（Certified Public Accountant）证书。George 毕业于塞顿霍尔大学，在那里获得了财务专业的学士学位。他最近还获得了专利 No.7152105“用于检测和报告网络弱点的系统和方法”，其他的专利还在申请之中。

其他作者简介

Nathan Sportsman 是一名信息安全咨询专家，具有 McAfee 旗下 Foundstone 分公司、赛门铁克、Sun 微系统以及戴尔等多家公司供职经验。最近几年，Sportsman 有机会服务于各大主要行业，他的客户大多来自华尔街、硅谷、政府情报机构以及知名教育机构。虽然其工作跨越多

个领域，但他专注于各行业的软件和网络安全。Sportsman 也是公众演讲的常客，最近刚刚在美国国家安全局就最新的黑客技术作过报告。他还是黑帽（Black Hat）组织终极黑客系列（Ultimate Hacking Series）的讲师，并且是包括 ISSA、Infragard 和 OWASP 在内的各种安全组织的固定报告人。Sportsman 开发了许多安全工具并且是 Solaris Software Security Toolkit（SST）软件的开发者。Sportsman 拥有信息安全行业的多项证书，包括 CISSP（Certified Information Systems Security Professional）和 GCIH（GIAC Certified Incident Handler）。Sportsman 在德州大学奥斯汀分校获得电气及计算机工程专业学士学位。

Brad Antoniewicz 是 Foundstone 公司网络弱点和评估渗透服务产品线的负责人。他是资深安全咨询专家，主要负责内外部的弱点评估、Web 应用渗透、防火墙及路由器配置研究、安全网络架构以及无线黑客攻击。Antoniewicz 开创了 Foundstone 公司的终极黑客无线攻击课程，并且负责教授终极黑客无线攻击课程以及传统的终极黑客课程。Antoniewicz 也在很多场合作过演讲，发表过大量的文章和白皮书，并且开发了许多 Foundstone 公司内部的评估工具。

Jon McClintock 是西北太平洋地区资深信息安全咨询专家，专门从事应用安全设计、实施及配置的研究。他具有十年以上的软件开发经验，覆盖了信息安全、企业及面向服务的软件开发以及嵌入式系统开发各个领域。McClintock 目前在亚马逊公司的信息安全团队担任资深软件工程师，负责定义安全需求、评估应用安全级别及传授新员工最好的安全软件开发经验。在加入亚马逊公司之前，Jon 曾给移动终端、low-level 操作系统及设备编写过驱动程序。他在加州大学 Chico 分校获得计算机科学学士学位。

Adam Cecchetti 作为一名安全领域工程师和研究员，具有七年以上的工作经验，他是位于西北太平洋地区的 Leviathan Security Group 的资深安全咨询专家。Cecchetti 主要从事硬件研发以及应用渗透测试。他曾对各个领域的财富 500 强企业进行过安全评估。在从事咨询行业之前，他是亚马逊公司的首席安全工程师。Cecchetti 在卡内基梅隆大学的电气与计算机工程专业获得硕士学位。

技术审校简介

Michael Price 作为 McAfee 旗下 Foundstone 公司的研发经理，主要负责 McAfee Foundstone 企业安全弱点管理产品的内容开发工作。他管理着一支由全球安全研究专家组成的团队，负责对进行远程计算机系统弱点侦测的软件实施质量检查。他在信息安全领域具有丰富的经验，曾经在弱点分析及安全软件开发领域工作过九年以上。

前　言

最近十几年来，“信息安全”这一名词的使用范围越来越广泛，其概念已经不仅是保护大公司和企业的商业机密，而且包括保护大众消费者的网络隐私。我们大量的敏感信息都保存在网络上，不法分子使用各种工具去窃取他人的保密数据的动机是如此强烈，以致于我们无法置之不理。而且，目前颁布的法律对网络犯罪起到的震慑作用似乎还不够有效。

本书中涵盖了最新的各种对信息安全构成威胁的案例，其目标是教育，这是抵御网络犯罪最基础的方法。本书致力于使读者掌握相关技能，从而保护我们的国家、教育机构、银行、零售商、公共事业、基础设施和我们的家庭不受侵害。最近两年，全球范围的网络威胁翻了一倍。为了应付这些攻击，我们的安全人员在能力上相对于犯罪分子需要两倍的提升才能胜任。

通过本书，我们希望扩展目前安全人员的知识范围，并且鼓励新一代的 IT 安全专家能够勇敢的站出来对抗目前大量出现的、经验丰富、技能高超的黑客罪犯。随着网络犯罪交流论坛的大量发展，黑客在网上自由交流着他们的黑客技术及犯罪手段，因此我们也必须就我们弱点和面临的威胁互通有无。只有我们用知识武装好自己和盟友之后，才能更好的与掌握大量技巧和策略的黑客作斗争。

在过去，对于信息泄露的担心我们只是在电影中见到过，那种犯罪分子潜入密室使用一台 PC 侵入主机系统的场景曾经是一种遥远的、传奇式的概念，很难让人们广泛理解在生活中这也是一种实实在在的威胁。但最近几年的数以亿计的私人信息被泄露的现实告诉我们，数据泄露正在疯狂的侵犯着哪怕是日常生活中最普通的部分。

与老一辈黑客希望出名和好奇心使然的动机不同，新一代黑客的动力完全来自于对利益的追逐。因此数据窃取的目标也从严密防范的安全场所转移到无数的毫无保护措施可言的信用卡信息上来。我们不但要教育安全人员，而且要让那些负责保管他人资料的工作人员注意保护我

们最重要的财产——广大民众的个人数据。

随着网络用户创建的公共内容越来越多，网络的未来发展越来越依靠于网络用户们自己的贡献。通过保证 Internet 的安全，我们也能够保证其本身的活力，并防止由于恐惧而束缚了我们的手脚，这种恐惧会扼杀新通信技术给我们带来的便利和进步。通过执法机构、政府、国际组织、持续的对尖端科技的研究和教育等各个方面的联合，我们就可以去引导对抗网络犯罪的潮流。现在你手中拿的就是迄今为止最成功的安全书籍。与其在一边观望，倒不如利用本书所提供的宝贵见解来帮助你自己、你的公司和你的国家与网络犯罪进行战斗！

Dave DeWalt

McAfee 公司总裁兼 CEO

推荐序

——曝光黑客 护卫信息

《黑客大曝光》一书面世以来，以其全面、深入和实用等特点，被业界赋予众多封号——“信息安全界的圣经”、“信息安全第一书”、“旷世之作”等等溢美之称。如今，《黑客大曝光》中文第6版又送到我手中，并嘱我作序。面对这本被称为全球最畅销的计算机安全书籍，我以能为中文版作序而深感荣幸，尤其是第6版的推出恰逢该书出版十周年，我也深感此次修订再版意义更重大。

《黑客大曝光》的三位作者都是目前信息安全领域的巨子，其中Stuart McClure和George Kurtz是迈克菲公司的“大员”，不但理论基础雄厚，更有在迈克菲与广大IT产业和信息安全领域携手合作进行“曝光”与“反制”黑客的前沿战斗中积累起的丰富实践经验。

正因如此，《黑客大曝光》新版在令专业人士“可以把其他信息安全图书从书架上拿掉”（Lawrence M. Walsh,《Information Security》杂志主编语）的第5版基础上，三位作者进一步深化和灵活运用独创的“黑客大曝光方法学”，针对目前和未来全球广泛互联与信息技术对人类发展推动作用日渐强大的新形势，以及知识经济发展中面临日趋严峻的黑客新挑战，遵从久经考验的“攻击对策哲学”，对内容进行了革命性的“大修”，为信息安全捍卫者提供了抵御、抗击黑客的制胜武器。

在遭受了百年一遇的金融危机之后，国际社会普遍认识到IT技术与知识经济在推动人类社会平衡、恒久发展中的重大作用。中国作为全球经济发展中的新型核心力量，不仅通过坚定的政府投资政策取得了经济的持续发展，而且及时将未来方略从“保增长”转向了“促转变”，这就是预示着信息对社会经济发展的推动作用将更加重大，而其中，防范黑客入侵、保障信息安全的任务也将日重。

如今，信息安全早已突破保障一个组织、一个机构数据安全、系统安全等狭隘理解，而提升到关系国家安全、经济安全、社会安全等的战略水平，当然更随着互联网在家庭应用和个人应用方面的普及，而渗入每个人的工作、生活、娱乐等每个领域和时时刻刻。

另外，随着犯罪的高科技化，黑客入侵事件在近年不仅数量激增——据 CERT 统计，全球平均每 20 秒钟就会发生一起 Internet 计算机侵入事件，而且更令人警觉的是，犯罪类型也从原来黑客彰显高超技术的“出名型”转向直接的经济目的——通过各种手段攫取钱财。迈克菲今年进行了全球范围内首次关于知识产权和敏感信息中存在漏洞的调查，研究显示，受访的上千家公司中平均每家公司在 2008 年损失的知识产权价值高达 460 万美元。据日前中国国家计算机病毒应急处理中心透露，目前网络犯罪的趋利性更是呈现出明显上升趋势，通过木马盗取银行账号和密码，偷取客户资金已经成为网上银行的更大挑战。

关注中国知识经济发展的巨大潜力和无限机会，迈克菲作为全球最大的专注于提供网络与信息安全产品和解决方案的厂商，倾力支持和推动《黑客大曝光》修订出版，并且认为，其第 6 版推出恰逢迈克菲加快实施在华发展战略之年颇具特殊意义——不仅能够从理论层面推动中国信息安全研究和教育发展，而且对迈克菲与中国广大的合作伙伴分享经验，共同促进中国信息技术进一步安全应用，从而推动经济发展模式的转变发挥积极作用。

文振邦

迈克菲大中华区总裁

致　谢

“《黑客大曝光》”（第 6 版）的作者在此向包括 Jane Brownlow 和 Carly Stapleton 在内为第 6 版辛勤工作的杰出的 McGraw-Hill 出版社的编辑和职工表示诚挚的感谢。没有他们为本书各个版本的无私奉献，我们很难将如此完美的书籍提供给读者，我们也很欣慰有一支实力如此雄厚的团队致力于告诉全世界网民黑客们的想法和手段。

同时也感谢我的同事们，他们是：Kevin Rich, Jon Espenschied, Blake Frantz, Caleb Sima, Vinnie Liu, Patrick Heim, Kip Boyle 及 PMIC 团队, Chris Peterson, the Live Security gang, Dave Cullinane, Bronwen Matthews, Jeff Lowder, Jim Maloney, Paul Doyle, Brian Dezell, Pete Narmita, Ellen McDermott, Elad Yoran，Jim Reavis；感谢他们经常与我们进行颇具启发意义的讨论，在各个方面给我们灵感使我们能够坚持写完本书（同时向由于我们的疏忽没有列在这里的更多的同事们表示歉意）。尤其要感谢第 6 版的其他作者：Jon McClintock，Adam Cecchetti，Nathan Sportsman，以及 Brad Anthoiewicz，他们也提供了许多创意性观点和引人入胜的内容。

最后万分感谢我们广大的忠实读者们，是您们使得这本书能取得巨大的全球范围的成功，我们对您的谢意无以言表！

序　言

CISO 的观点

如今的信息安全是以风险为核心的业务

当十年之前 Hacking Exposed 第 1 版上架之时，安全风险管理还只是一个孩子，不会走路、说话、照顾自己，更不用说搞清楚自己想干什么了。很长一段时间，我们都认为“风险”一词只与保险业有关而与安全工作无关。而在今天，如果不去认真思考并且将风险分析纳入你的安全工作之中，你都不知道如何开始安全工作。欢迎进入安全工作的新时代：风险管理。

今天的安全风险管理是一个主流概念，贯穿各大公司的法律、财务以及运营等各个环节。诸如 Sarbanes Oxley（SOX）、Payment Card Industry（PCI）、Health Information Portability and Accountability Act（HIPAA），以及加利福尼亚州的 SB1386 在内的很多法规遵从法案都将信息安全关注的焦点从不惜一切代价必需实现的后端 IT 服务功能层面转移到同公司运作各个环节、各种类型的安全风险紧密关联的综合的和共享的企业级责任上来。

如今，很多新的黑客工具、技术、方法、脚本以及自动运行的黑客软件越来越放肆的攻击着我们的世界，快速演变的安全威胁给我们原来用来保护企业的流程和优先级处理带来了挑战。我们几乎无法跟上安全威胁发展的步伐。然而，不论安全威胁怎样千变万化，有两点是不变的。第一是一条永恒的真理：好和坏的界限往往模糊不清，因此“要想抓贼，就必须先像贼一样思考”。但针对目前的安全威胁，我觉得仅仅“像贼一样思考”是不够的，我们需要“像魔鬼一样思考”。第二是安全人员必须拥有饱满的工作激情和信息安全领域深入实际的工作技能。如果没有上述两点亘古不变的真理做保证，安全工作的失败是不可避免的。

“像魔鬼一样思考”是安全心态体系的核心，它已经在安全领域的相关著作中被多次提到。

简而言之，要想成为一名成功的信息安全工作者，就必须能够像一名优秀的黑客一样思考问题。如果没有这种先发制人进行防范的威胁预见能力，安全工作就变成了一种按照过去发生的问题清单机械的进行防御的徒劳之举。并且你注定会重复过去的失败。成功的信息安全工作还包括一系列的综合性技能要求，诸如政策制定、程序管理、法律执行及认证等，这些都是必需的。然而最终，拥有丰富的、最新的计算机技能则是至关重要的。对于在信息安全的战壕里战斗并且成功生存下来的信息安全工作人员来说，具备丰富的经验和专业技能这一前提是无可替代的。拥有明确的安全政策和标准以及强大的法规遵从流程是必需的，但这些都无法解决开放的端口带来的危险，网络本身的弱点就是获得隐私数据的入口。只有不断地提高那些有激情去保护网络安全的工作人员的技术实力，我们才能保障在任何环境下都拥有可靠的安全性。

《黑客大曝光》一书是实现上述这些成功准则的知识源泉。不论你在安全工作生命周期中处于哪个环节，也不论你目前的技术实力如何，我强烈推荐你读一读本书，哪怕你从事的是非技术性的安全工作，只有这样你才能够学着像黑客们一样思考，或者至少能够了解你的敌人的技术水平是如此的高超和完备。一旦你读了、理解了并且真正掌握了书中的内容从而建立起了安全观念，你才能在任何环境下都可以进行有效的基于风险的安全管理。没有本书中提供的这些工具和技巧，你将在安全管理的道路上漫无目的地挣扎前行并且总是疑惑不解："为什么安全管理如此困难啊？"

Patrick Heim

凯泽永久医疗集团 首席信息安全官

绪　论

名叫“自满”的敌人无处不在

随着信息安全行业发展进入第二个十年，遇到了一个强大的敌人。这个敌人无声无形，甚至没有名字，我们找不到它的任何档案记录。我们唯一能确定他存在的方法就是通过衡量我们自己是否缺乏进步。这个敌人就是“自满”。

在第 5 版中，我们讲过要警惕敌人，但是自满恰恰是我们缺乏警惕的根源所在。就像我们在 2001 年“911”之前一样，我们变得自鸣得意。如 Spock 所说：“人类是很奇特的”。我们只会条件反射，而不会提前作出预防。直到事情发生了，我们才想到去阻止。这不是有点晚，而是太迟了。

信息安全行业以及安全人员都已经行动起来与“门口的”及身后的敌人作战了，而我们的企业大佬们还不明白由于他们对于安全防范的松懈正导致他们的企业面临着什么样的安全风险。因此我们必须尽快解决掉这种“身处险境却茫然不知”的自满情绪。记住，最好的安全防范就是保证什么威胁都不发生。而当威胁没有发生时，我们的心态发生了什么变化呢？我们相信我们是不可战胜的，威胁不会发生在我们身上，我们忘记了自身的弱点，我们忘记了坏事迟早会发生……直到下一次灾难出现，我们才如梦方醒。

那么如何从上述泥潭中脱身呢？在我们与黑客不懈斗争的道路上，唯一能使我们保持必要的安全状态的方法就是时刻保持警惕，争取在第一时间发现安全的隐患。这也是我们编写本书的原因。将本书作为你的向导，作为帮助你时刻保持警惕的药方，并且把它推荐给每个身边的人，演示给他们看当危险分子企图进行黑客攻击时会发生些什么，从而帮助他们回到和你一样的正确道路上来，避免再次跌入泥潭。让我们时刻警钟长鸣吧！

第 6 版新增内容

如今，每年因特网和公司局域网的各种新技术和解决方案不断涌现，而这些技术和解决方案在推出之前都没有进行任何的安全考虑。我们继续编写《黑客大曝光》第 6 版的目的就是针对当今网络、服务器、应用及数据库方面的新技术继续提供安全分析的知识更新，从而保护我们的网络安全。

新增内容

下面是《黑客大曝光》第 6 版新增部分内容：

- 新增章节：第 9 章“硬件攻击”，对物理锁、门禁卡、RFID、笔记本安全、U3 USB 设备、蓝牙设备、固件以及其他方面的攻击手段及应对策略进行了探讨。
- 新增了 Windows 黑客攻击的部分内容，包括终端服务、Kerberos 嗅探、中间人攻击、缓存溢出、设备驱动篡改、新口令破解工具、Windows 防火墙、Bitlocker 驱动加密功能和加密文件系统（EFS）等。
- 新增 UNIX 黑客攻击内容，包括 THC-Hydra、Solaris 输入验证攻击、悬摆（dangling）指针攻击、DNS 缓存毒化（Kaminsky 2008 年所发布的）、UNIX Trojan、内核 rootkit，以及新的口令字破解技术。
- 补充了新的无线黑客攻击内容，使第 8 章的内容更为全面。
- 在网络设备攻击部分新增了思科设备在对付新的 VPN 和 VoIP 黑客攻击时的弱点等内容，包括利用 Google 进行 VPN 配置的黑客攻击、攻击 IPSec VPN 服务器、攻击 IKE 主动模式、SIP 扫描和查点、SIP 泛洪攻击，以及利用 TFTP 技巧攻击 VoIP 等。
- 增加了用户完全无法察觉的踩点、扫描、查点新技术。
- 精简了拒绝服务（Denial of Service）的内容，只保留必要的部分，并作为附录。
- 更新了“攻击因特网用户”和“攻击应用程序代码”两章的前言。
- 提供了全新的“案例研究”，可以让大家及时了解现实生活中最近出现的黑客技术，当然我们隐匿了相关的个人信息。

本书内容的基本结构

本书沿用了《黑客大曝光》以往的一贯设计风格。

这个图标代表攻击手段

这个图标可以帮助读者快速查找到特定的渗透工具和具体操作步骤。在介绍完每一种攻击手段之后，我们会立刻给出针对这种攻击手段的防范措施并用下面这个图标加以突出。

这个图标代表防范措施

这个图标可以帮助读者快速查找到修补安防漏洞和挫败攻击者的具体措施和操作步骤。

在查阅书中代码清单时，请特别注意我们用黑体字强调的用户输入内容。

我们对书中介绍的每一种攻击手段都从三个方面进行了风险评级：

流行度	*利用这种手段对实际目标进行攻击的频率：1 代表最少见，10 代表最常见*
简单度	*使用这种攻击手段所需的技能：10 代表需要的技能最少，1 则代表只有资深安全人员才能实施*
影响力	*攻击得手时可能造成的损失大小：1 代表目标系统上的信息损失程度最小，10 代表黑客能攻破超级用户帐户或造成与此种情况相当的损失*
风险率	*前三个数字的平均值（舍入为与之最接近的整数），这个数值给出了这种攻击手段的总体危害程度*

致读者

《黑客大曝》第 6 版光同之前的几版一样，都需要读者去认真阅读，汲取书中丰富的内容并学以致用，重复本书中的所有实验；因为没有比亲自动手更好的学习方法了。要想弄懂本书中的各个案例及相关信息，你需要一遍又一遍地研习本书。换句话说，即使你觉得你完全懂了，你也应该回过头来再温习一下。我们保证每次重复你都会有新的发现，而这些新知识都能够救你于水火之中。

我们希望今后也能够不断的更新本书的内容，努力把最新的网络安全信息提供给各位读者。而本书的成功很大程度上也归因于内容自身的可读性很强，我们只是尽可能将其以最容易消化的方式展现给大家。《黑客大曝光》在 1999 年的成功大大超出了我们当初的预想，但我们能够保证：只要您觉得我们的写作是有意义的，我们就会持之以恒的把关于黑客技术、工具和相关对策的最新信息及时、准确、原汁原味地提供给您。祝您阅读愉快！