HACKING EXPOSED

黑客大曝光

网络安全机密与解决方案

第7版

Stuart McClure (CISSP, CNE, CCSE)
Joel Scambray (CISSP)
George Kurtz (CISSP, CISA, CPA) 著
赵 军 张云春 陈红松 等译
郑 林 审校

McGraw Hill
清华大学出版社

黑客大曝光 第7版

网络安全机密与解决方案

Stuart McClure (CISSP, CNE, CCSE)
Joel Scambray (CISSP)
George Kurtz (CISSP, CISA, CPA) 著
赵 军 张云春 陈红松 等译

清华大学出版社
北 京

本书版权登记号：图字：01-2012-8051

内 容 简 介

《黑客大曝光》是全球销量第一的网络和计算机信息安全图书，也是有史以来写得最为成功的信息安全旷世之作，被信息安全界奉为“武林秘笈”。作者以独创的知己知彼视角揭示了“黑客攻击的方法学”，从攻防两方面系统阐述了最常见和最隐秘的黑客入侵手段以及针锋相对的防范对策。

本书在前6版的基础上对内容进行全面更新和扩充，以便涵盖黑客攻击伎俩的最新动态，如增加了有关针对特定目标的持续性攻击、硬件攻击以及智能手机攻击（Android系统和iOS系统）的新章节；第7版开篇仍以黑客攻击技术的“踩点”→“扫描”→“查点”三部曲，拉开黑客入侵的序幕；之后从黑客攻击的主要目标：“系统”、“基础设施”、“应用程序和数据”3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和对症下药的防范对策；“基础设施攻击”篇揭示了3类基础设施的攻击手段和行之有效的防范对策——远程连接和VoIP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——网页和数据库攻击、移动设备攻击，并给出了针对上述黑客最新攻击的防范对策手册。

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甚至是信息安全“发烧友”的权威指南和必备工具书；也可作为信息安全相关专业的教材教辅用书，以及IT专业培训的教材。

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7版/（美）麦克克鲁尔（Mcclure,S.），（美）斯坎布雷（Scambray,J.），（美）克茨（Kurtz,G.）著，赵军等译. -北京：清华大学出版社，2013

书名原文: Hacking exposed 7:network security secrets & solutions

ISBN 978-7-302-33159-9

I. ①黑… II. ①麦… ②斯… ③克… ④张… 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(2013)第159622号

责任编辑：夏非彼
封面设计：王　翔
责任校对：闫秀华
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**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：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　张**：44.75　　**字　数**：1002千字
版　　次：2013年10月第1版　　**印　次**：2013年10月第1次印刷
印　　数：1～5000
定　　价：129.00元

产品编号：049545-01

作者简介

Stuart McClure

Stuart McClure（CNE、CCSE）是一家全球优秀的安全服务和产品公司Cylance的CEO兼董事长，该公司致力于为全球重要的公司解决大多数最困难的安全问题。在就职于Cylance之前，Stuart是McAfee/Intel的全球CTO，主要负责大约30亿美元的消费者和企业安全产品业务。在McAfee任职期间，Stuart McClure同时兼任McAfee/Intel安全管理业务的总经理，促使所有McAfee企业的安全产品都实现了可操作、可管理和可度量。与此同时，Stuart McClure在McAfee内管理着一支名为TRACE的精英团队，该团队由优秀的黑客构成，负责发现新的漏洞和出现的攻击。在就职于McAfee之前，Stuart效力于美国最大的卫生保健组织Kaiser Permanente公司安全服务部。1999年，Stuart还是Foundstone公司的最初创始人之一，该公司是一家全球咨询和产品公司并于2004年被McAfee公司收购。

Stuart是《黑客大曝光》系列书籍的编写者、主要作者和原始创办者，他拥有长达25年的道德黑客经验。Stuart如今被认为是信息安全风险方面的权威，其声名远播，经常被邀请介绍其有关黑客和探索技术的渊博知识。作为获得大家公认的著名安全专家，McClure在技术方面知识渊博，在和领导方面经验丰富，在书中他和大家分享如何广泛而深入地了解信息安全威胁领域，以及运营和财务风险，这些知识和经验都是个人和企业取得业务成功的必备条件。

Joel Scambray

Joel是Cigital公司的管理人，Cigital成立于1992年，是一家国际领先的软件安全公司。该公司服务的对象包括刚刚创建的小公司到世界500强公司，在应对信息安全挑战与机遇领域具有超过15年的经验。

Joel的个人经历包括执行官、技术咨询专家以及企业家。他是信息安全咨询公司Consciere的创始人之一，该公司于2011年6月被Cigital公司收购。他曾是微软公司的高级主管，为微软的在线服务和Windows部门提供安全方面的指导。Joel也是提供安全软件和服务的Foundstone公司的创始人之一，并且成功地使公司于2004年被McAfee公司收购。此前还担任Ernst & Young咨询公司的经理、微软TechNet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。

Joel是信息安全领域一位广获赞誉的作家和演讲家。他是十多本有关IT和软件安全方面书籍的合著者之一，这些书多数是畅销书。他在很多场合发表过演讲，包括Black Hat等论坛峰会，IANS、CERT、CSI、ISSA、ISACA、SANS等组织，各种私营企业以及FBI和RCMP等政府组织。

Joel 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

George Kurtz（CISSP、CISA、CPA）是 CrowdStrike 公司的创始人之一同时兼任 CEO，该公司是一家前沿的大数据安全技术公司，致力于帮助企业和政府保护其大多数敏感知识产权和国家安全信息。George 也是国际公认的安全专家、作家、企业家和发言人。他在安全领域拥有超过 20 年的工作经验并且帮助全世界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。他作为企业家的背景以及将新生技术商业化的能力，赋予了他识别市场趋势并将其同顾客反馈相关联的能力，从而使其自己经营的事业飞速发展。

2011 年，George 辞去 McAfee 全球 CTO 一职并成为合著作家，同时募集了 2600 万美元的风险投资并创建了 CrowdStrike 公司。在其担任 McAfee 的 CTO 期间，Kurtz 负责整合整个 McAfee 产品的安全架构和平台。Kurtz 还致力于推动兼并战略，从而使得 McAfee 的营业额从 2007 年的 10 亿美元增长到 2011 年的超过 25 亿美元。2011 年，Intel（INTC）以接近 80 亿美元的价格收购了 McAfee，这也是该年度技术界最大的兼并收购案例之一。在加盟 McAfee 之前，Kurtz 是 Foundstone 公司的 CEO 和创始人之一，该公司于 2004 年被 McAfee 公司收购。可以关注 George 的 Twitter @george_kurtz 或他的博客 http://securitybattlefield.com。

其他作者简介

Christopher Abad 是 McAfee 的一名安全专家，致力于研究嵌入式的威胁。他拥有 13 年的计算机安全研究及软件和硬件开发经验，并毕业于 UCLA 大学数学专业。他对许多安全产品都有所贡献，在过去的数年里频繁在各种安全会议上演讲。

Brad Antoniewicz 在 Foundstone 的安全研究部门工作，致力于揭示流行技术中的缺陷。他对《黑客大曝光》和《无线黑客大曝光》系列书籍都有所贡献，并且是多种内部和外部 Foundstone 工具、白皮书和方法论的作者。

Christiaan Beek 是 McAfee Foundstone 服务团队的首席架构师。他也是 EMEA（欧洲、中东和非洲）地区的事故响应和取证调查服务小组的组长。从系统攻击、窃取、儿童色情、恶意软件感染、高级持续攻击（Advanced Persistent Threats，APT，或者称为针对特定目标的持续攻击）到移动设备，他都进行过大量的取证调查。

Carlos Castillo 是 Intel 旗下 McAfee 公司的一名移动恶意软件研究者，在该公司内，他对可疑应用程序进行静态和动态分析，为 Android（安卓）产品提供 McAfee 的移动安全解决方案。Carlos 现在的研究包括剖析 Android Market 恶意软件 DroidDream，他是 McAfee 发表的一份名

为《Android 恶意软件的过去、现在和将来》白皮书的作者。Carlos 还是 McAfee 博客中心的一名活跃分子。在 McAfee 之前，Carlos 在哥伦比亚 Cuperintendencia Financiera 进行安全合规审计工作。在此之前，Carlos 任职于一家新成立的安全公司 Easy Solutions，他对网页应用程序进行渗透测试，帮助关闭钓鱼网站和恶意网站，支持安全和网络设备，执行软件的功能性测试，以及支持与防电子诈骗有关的研究和开发。Carlos 赢得 ESET 拉美地区的“最佳防病毒研究”比赛之后，就加入了恶意病毒研究的领域。其获奖文章名为 Sexy View: The Beginning of Mobile Botnets。Carlos 从哥伦比亚波哥大的 Universidad Javeriana 大学获得系统工程师学位。

Carric Dooley 从 1997 年便致力于信息安全研究。在 ISS 专业服务小组工作了 5 年之后，他于 2005 年 3 月加入 Foundstone 服务团队。目前他在 EMEA 致力于构建 Foundstone 服务团队，和其可爱的妻子 Michelle 以及 3 个孩子居住在英国。他主持了在不同领域进行的数以百计的多种类型的评估活动，其客户包括全球知名的银行、石油化工、公共事业以及位于欧洲和中东的消费者电子产品公司。你也许在 Black Hat 峰会（Vegas/Barcelona/Abu Dhabi）或 Defcon 会议上见过 Carric，除了在 Defcon 16 上做报告之外，他也常在会务小组里工作。

Max Klim 是 Cigital 公司的一名安全顾问。Cigital 公司是一家成立于 1992 年的软件安全领军公司。在加入 Cigital 之前，Max 是 Consciere 公司的一名安全顾问。Max 拥有超过 9 年以上的 IT 和安全经验，曾效力于财富 500 强企业和新生公司。他精通渗透测试、数字取证、事件响应、合规以及网络和安全工程。Max 从华盛顿中央大学获得信息技术管理应用科学学士学位，获得 EnCE（Encase Certificated Examiner）、CISSP 证书，并拥有多项 GIAC 证书。

Tony Lee 拥有超过 8 年的专业经验，他把热情投入到信息安全的所有领域。他目前是 Foundstone 专业服务（McAfee 的一个部门）的首席安全顾问，负责多数网络渗透服务热线的推进。他最近的兴趣是对 Citrix 和 kiosk 的入侵、post 漏洞（从本地管理员到域管理员的权限提升）的利用以及 SCADA 漏洞的利用。作为一名热心的教育者，Tony 在全球许多地方培养了上千名学生，包括政府机构、大学、企业和 Black Hat 之类的会议。他不失时机地通过课程与大家分享他的经验，这些课程包括 Foundstone 的 Ultimate Hacking（UH）、UH：Windows、UH：Wireless 以及 UH：Web。他拥有 Virginia Tech 的计算机工程科学学士学位，Johns Hopkins 大学的安全信息学硕士学位。

Slavik Markovich 在基础设施、安全和软件开发方面拥有超过 20 年的经验。Slavik 是 Sentrigo 公司的创始人之一，该公司专注于数据库安全，最近被 McAfee 收购。在创建 Sentrigo 之前，Slavik 是 db@net 的研发副总裁和首席架构师，该公司是一家 IT 架构咨询公司。Slavik 致力于开源项目，且是业界各种会议上发言的常客。

Hernan Ochoa 作为一名安全顾问和研究者，已经拥有超过 15 年的专业经验。Hernan 是 Amplia Security 公司的创始人之一，该公司是一家信息安全服务商，提供的服务包括网络、无线、网页应用程序渗透测试、独立/客户端-服务器应用程序黑盒评估、源代码审计、逆向工程

以及漏洞分析。Hernan 在 1996 年创建了 Virus Sentinel，开启了专业生涯，Virus Sentinel 是一个基于签名的文件/内存/mbr/boot 扇区检测/删除病毒的防病毒应用程序，它能启发式地检测多形态病毒。Hernan 还开发了一个详细的技术病毒信息数据库和相应的简报。他于 1999 年加入了 Core Security 科技公司，在此工作的 10 年中担任了多种角色，包括安全顾问、为多类安全评估编写漏洞利用代码、制定方法、编写 shellcode（恶意代码）和安全工具以及添加新的攻击向量。他还为 multi-OS 安全系统设计和开发了多种底层/内核部件，该系统最终部署在一个金融机构里并成为了开发和支持 multi-OS 的“技术领头羊”。Hernan 已经发布了大量安全工具并在多个国际安全会议上发表其成果，包括 Black Hat、Hack in the Box、Ekoparty 和 RootedCon。

Dr. （Shane） Shook 是一名高级信息安全专家和 SME，他设计、建造并优化信息安全执行方案。他还开展信息安全审计和漏洞评估、业务持续性规划、灾难恢复测试以及安全事件响应，包括计算机取证分析和恶意软件评估。他还为犯罪共同起诉、IRS、SEC、EPA 和 ITC 案例，以及州和联邦行政事务方面的技术问题提供权威证据。

Nathan Sportsman 是 Praetorian 公司的创始人和 CEO，该公司是一家私营的资产数百万美元的安全咨询、研究和产品公司。Nathan 在信息安全方面拥有广泛丰富的经验，其中涵盖了从 NASDAQ 证交所到美国国家安全局等各行各业不同的客户进行咨询的经验。在成立 Praetorian 公司之前，Nathan 在 Sun Microsystems、Symantec 和 McAfee 公司担任软件开发和咨询职务。Nathan 是一名出版作者、美国专利持有者、NIST 个人贡献者、以及 DoD 顾问。Nathan 在德克萨斯大学获得电气及计算机工程专业学士学位。

技术审校简介

Ryan Permeh 是 McAfee 的首席科学家。他在 CTO 办公室工作，致力于构想如何避免现在和将来出现的威胁。他是一名拥有 15 年业内经验的漏洞研究者、逆向工程师以及漏洞发现者。Ryan 在多个安全和技术会议上就高级安全主题发表过演讲，发布了许多博文和文章，并对这类专题的书贡献良多。

Mike Price 目前在 Appthority 公司担任 iOS 首席架构师。Mike 全职从事与 iOS 操作系统和应用程序安全有关的研究和开发工作。Mike 曾是 McAfee 在智利首都圣地亚哥实验室的高级运营主管，在此期间，他主要负责实验室的正常运作、与位于智利和拉美等地的外部企业进行合作、推进团队和区域的技术发展和创新。Mike 作为 Foundstone 研究小组的成员长达 9 年。最近，他负责 McAfee Foundstone 企业漏洞管理产品的内容开发，在此期间，Mike 带领一个全球安全研究者小组工作，主要负责执行软件检查，以便远程检测操作系统和应用程序中的漏洞。他在信息安全领域拥有全面丰富的经验，在漏洞分析和信息安全研发方面工作了近 13 年。Mike 同时是 8.8 计算机安全会议的创始人之一，该会议每年定期在智利首都圣地亚哥举行。Mike 还为本书第 11 章做出了贡献。

序 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。

术语网络安全和一张以“网络”作为前缀的无穷的单词表每天都冲击着我们的感官。计算机和信息技术是让我们这个世界相互关联和依存的关键因素，虽然人们广泛讨论到计算机和信息技术领域的多种术语，但是对这些术语的理解往往不到位。政府、私营和合资企业以及个人都逐渐意识到我们日常生活中的在线活动所面临的挑战和威胁。在近几年内，世界范围内依赖于计算机进行存储、访问和交换信息的速度呈现指数级增长，这涵盖几乎全球依仗计算机操作或计算机辅助基础设施和工业机制，由此可见，网络对我们生活的重要性是显而易见的。

安全问题所导致的影响范围小到因其所带来的不便，大到严重的商业损失，乃至国家的安全隐患。黑客攻击是网络不安全的罪魁祸首，其所造成的危害包括令人不快却相对无害的年轻人的爱开玩笑活动，到由政府发起的以及由专业黑客发起的危害巨大的、复杂的且有目标的网络攻击活动。

上一版的《黑客大曝光》被公认为是网络安全的基础文档，是 IT 专家、技术领袖以及其他人员有兴趣了解黑客及其方法的重要文献。但是作者意识到，要想在快速变化的 IT 安全领域保有一席之地，需要机敏、洞察力以及对最新黑客攻击活动和技术的深入理解。借用《罗宾汉》电影中的台词，“不断进步……”，以此勉励我们应对网络黑客无休止入侵而需要付出不懈的安全努力。

本书第 7 版对由来已久的那些安全问题做了内容更新，并增加了有关针对特定目标的持续

性攻击（Advanced Persistent Threats, APTs）、硬件以及嵌入式系统的新章节。书中解释了黑客入侵如何发生、渗透者在干什么以及如何抵御他们，作者涵盖了计算机安全的所有方面。鉴于移动设备和社交媒体的流行，今天的网民也可以在本书中找到在此类常见平台的漏洞和隐患的精彩内容。

处理 IT 和计算机安全问题的前提条件是知识。首先，我们必须了解所使用的系统的架构及其软硬件的优点和缺点。其次，我们必须了解敌手：他们是谁以及他们要试图做什么。简而言之，在我们能够采取有效的应对措施之前，需要通过侦查和分析以洞悉有关的威胁和敌手。本书提供了必需的基础知识，武装那些真正关心网络安全的人们。

如果我们变得聪明并了解自己，了解我们的设备、网络和敌手，我们将能够成功地找到一种可以保护网络的方法。不变的是改变的现实：新技术和方法的出现，不断演变的威胁。因此，我们必须“不断进步”以保持同新发展齐头并进，更新知识并获得对黑客攻击全面而深入的了解。

新版本的《黑客大曝光》将帮助你变得聪明，并采取有效的措施。小绵羊终将成为网络安全界的狮子。

William J. Fallon
美国海军上将（退役）
CounterTack 公司主席

海军上将 William J. Fallon 在经历了 40 年的辉煌战事和战略生涯之后从美国海军退役。他领导美国和盟军的 8 个独立纵队，在美国政府最高级别的战事和外交事务中扮演了领导角色。作为美国中央司令部的首脑，海军上将 Fallon 指挥了美国在中东、中亚和非洲之角的军事行动，主要有对伊拉克和阿富汗的联合行动。Fallon 上将是网络安全领域新兴公司 CounterTack 公司的理事会主席，他同时还是 Tilwell Petroleum 有限责任公司的合伙人、多家商业公司的顾问以及 Naval Analyses 中心的杰出成员。他还是美国国防科学局秘书组和美国安全项目组的成员。

致　谢

《黑客大曝光》(第 7 版)的作者在此向包括 Amy Jollymore、Ryan Willard 和 LeeAnn Pickrell 在内所有为第 7 版辛勤工作的 McGraw-Hill 出版社的编辑和员工表示诚挚的感谢。没有他们为本书的无私奉献，您将很难见到此刻在您手上（iPad 或 Kindle 上）的这本完美的书籍。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有关黑客们的想法和手段。

感谢本书中文翻译版的所有参与者，由于大家的认真和辛勤劳动才使本书能惠及对计算机信息安全感兴趣的读者。同时感谢除署名译者、审校者外，参与本书译校工作的郑智捷、张晓彤、朱阔成、王国春、施妍然、王川、郎亚妹、王金柱、卞诚君、王翔、孟宗斌、李竹、李征、周成、李丽等同志的共同努力。

同时特别感谢所有对此版本有所贡献的人员和技术审校。万分感谢广大的忠实读者们，是你们使得这本书能取得全球范围的巨大成功，对你们的谢意无以言表！

绪　论

“不断进步，直到羔羊变成雄狮。”

来自 Russell Crowe 于 2010 年拍摄的电影《罗宾汉》中的台词，为第 7 版的《黑客大曝光》提供的不仅仅是一句口号。无疑，今天的我们就是一只羔羊，每一分每一秒都等待着被宰割。但是这种情况不会再继续发生了，我们不能允许它再发生，反击的后果是如此的严重，黑客们将以悲剧作为结局。

我们希望您能阅读每一页上的每一个字，并时刻铭记这一忠告。我们必须理解那些坏家伙是如何工作的，然后运用书中所写的防范对策，否则，我们将继续被宰割，并将继续蒙受损失。

本书的内容包括

当修改并扩充此书中的所有内容时，我们必须强调一些全新且十分重要的内容。首先，我们对持续增长的 APT（针对特定目标的持续攻击）攻击进行了深入分析，并提供了现实的例子予以说明此类攻击成功的原因，以及侦测和阻止此类攻击的方法。其次，我们新增了一个章节介绍嵌入式攻击，包括那些坏家伙把电路板同其上所有芯片分离的技术，对其进行逆向工程，然后在让人眼花缭乱的 1 和 0 数字世界中找到要攻击的要害。再次，我们增加了有关数据库入侵的章节，讨论其目标和用于窃取敏感数据的技术。然后，我们花了一整章介绍移动设备，揭示平板电脑、智能手机和移动计算的嵌入式世界，以及那些坏家伙如何开始攻击这迅猛增长的新领域。最后新增了一章介绍防范对策，我们从本书 1999 年的第 1 版就应该包含这部分。在这一章节中，我们详尽深入地解释了作为管理员或最终用户的你能够做些什么，以便阻止那些坏家伙入侵你的系统。

如何使用本书

本书的目的是让你了解黑客的世界，他们是怎么思考以及如何行动的。但是同时也让你学会阻止黑客的方法。可将本书作为实现这两个目的的权威资料。

本书的基本结构

在第 1 部分“收集情报”中，我们讨论了黑客如何获取其目标的情报，他们通常采用审慎的步骤去完整地理解和穷举目标，我们揭露了此类伎俩的真相。在第 2 部分“终端和服务器攻击”中，我们单刀直入地揭露了黑客老手的最终目标，即终端桌面或服务器，这一部分也包括有关 APT 的新增章节。第 3 部分“基础设施攻击”讨论了那些坏家伙攻击我们系统所接入的高速网络的方法，这一部分还包括了入侵嵌入式系统的新章节。第 4 部分“应用程序和数据攻击”不仅讨论了网页/数据库领域，还讨论了移动攻击。此部分我们也探讨了各个方面都能使用的防范对策。

导读

我们为第 7 版使用了《黑客大曝光》一贯的设计风格，每一项攻击技术都采用下面的图标突出显示。

攻击图标

使得能够轻易地识别出特定渗透工具和方法。每一种攻击都使用了实用的、确切的、经实地测试的解决方法。解决方法使用特定的防范对策图标。

防范对策图标

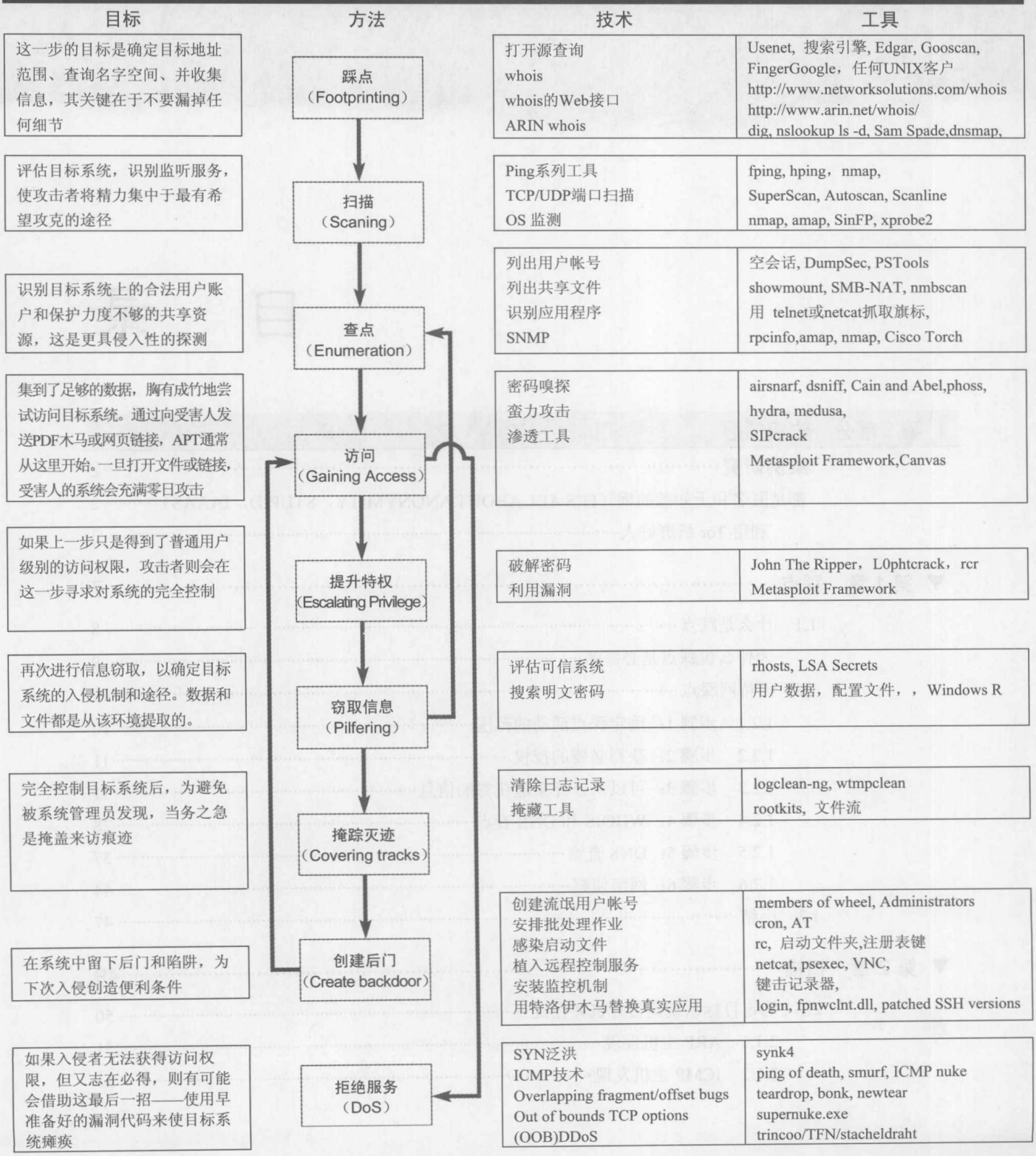
正确执行以修复问题并阻止攻击者。

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 3 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要的技能。1 代表只有资深安全人员才能实践这种攻击，10 代表需要的技能很少或者不需要什么技能*
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账户或造成与此种情况相当的损失*
风险评级：	***前 3 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***

黑客剖析图


目标
方法
技术
工具
这一步的目标是确定目标地址范围、查询名字空间、并收集信息，其关键在于不要漏掉任何细节
踩点 (Footprinting)
打开源查询
whois
whois的Web接口
ARIN whois
Usenet，搜索引擎, Edgar, Gooscan, FingerGoogle，任何UNIX客户
http://www.networksolutions.com/whois
http://www.arin.net/whois/
dig, nslookup ls -d, Sam Spade,dnsmap,
评估目标系统，识别监听服务，使攻击者将精力集中于最有希望攻克的途径
扫描 (Scaning)
Ping系列工具
TCP/UDP端口扫描
OS 监测
fping, hping，nmap,
SuperScan, Autoscan, Scanline
nmap, amap, SinFP, xprobe2
识别目标系统上的合法用户账户和保护力度不够的共享资源，这是更具侵入性的探测
查点 (Enumeration)
列出用户帐号
列出共享文件
识别应用程序
SNMP
空会话, DumpSec, PSTools
showmount, SMB-NAT, nmbscan
用 telnet或netcat抓取旗标,
rpcinfo,amap, nmap, Cisco Torch
集到了足够的数据，胸有成竹地尝试访问目标系统。通过向受害人发送PDF木马或网页链接，APT通常从这里开始。一旦打开文件或链接，受害人的系统会充满零日攻击
访问 (Gaining Access)
密码嗅探
蛮力攻击
渗透工具
airsnarf, dsniff, Cain and Abel,phoss,
hydra, medusa,
SIPcrack
Metasploit Framework,Canvas
如果上一步只是得到了普通用户级别的访问权限，攻击者则会在这一步寻求对系统的完全控制
提升特权 (Escalating Privilege)
破解密码
利用漏洞
John The Ripper，L0phtcrack，rcr
Metasploit Framework
再次进行信息窃取，以确定目标系统的入侵机制和途径。数据和文件都是从该环境提取的。
窃取信息 (Pilfering)
评估可信系统
搜索明文密码
rhosts, LSA Secrets
用户数据，配置文件，，Windows R
完全控制目标系统后，为避免被系统管理员发现，当务之急是掩盖来访痕迹
掩踪灭迹 (Covering tracks)
清除日志记录
掩藏工具
logclean-ng, wtmpclean
rootkits，文件流
在系统中留下后门和陷阱，为下次入侵创造便利条件
创建后门 (Create backdoor)
创建流氓用户帐号
安排批处理作业
感染启动文件
植入远程控制服务
安装监控机制
用特洛伊木马替换真实应用
members of wheel, Administrators
cron, AT
rc，启动文件夹,注册表键
netcat, psexec, VNC,
键击记录器,
login, fpnwclnt.dll, patched SSH versions
如果入侵者无法获得访问权限，但又志在必得，则有可能会借助这最后一招——使用早准备好的漏洞代码来使目标系统瘫痪
拒绝服务 (DoS)
SYN泛洪
ICMP技术
Overlapping fragment/offset bugs
Out of bounds TCP options
(OOB)DDoS
synk4
ping of death, smurf, ICMP nuke
teardrop, bonk, newtear
supernuke.exe
trincoo/TFN/stacheldraht

内容预览

第 1 部分　收集情报

▼ 第 1 章　踩点 ……7
▼ 第 2 章　扫描 ……49
▼ 第 3 章　查点 ……85

第 2 部分　终端和服务器攻击

▼ 第 4 章　攻击 Windows ……161
▼ 第 5 章　攻击 Unix ……235
▼ 第 6 章　网络犯罪和高级持续威胁 ……317

第 3 部分　基础设施攻击

▼ 第 7 章　远程连接和 VoIP 攻击 ……375
▼ 第 8 章　无线攻击 ……463
▼ 第 9 章　硬件攻击 ……493

第 4 部分　应用程序和数据攻击

▼ 第 10 章　攻击网页和数据库 ……523
▼ 第 11 章　攻击移动设备 ……583
▼ 第 12 章　防范对策手册 ……659

第 5 部分　附录

▼ 附录 A　端　口 ……681
▼ 附录 B　十大安全漏洞 ……689
▼ 附录 C　拒绝服务（DOS）与分布式拒绝服务（DDOS）攻击 ……691

目　录

第 1 部分　收集情报

案例研究 …… 2

都是匿名和无知惹的祸（IT'S ALL ABOUT ANONYMITY，STUPID，IAAAS） …… 2

利用 Tor 折磨好人 …… 3

▼ 第 1 章　踩点 …… 7

1.1　什么是踩点 …… 8

为什么说踩点是必需的 …… 9

1.2　因特网踩点 …… 10

1.2.1　步骤 1：确定踩点活动的范围 …… 10

1.2.2　步骤 2：获得必要的授权 …… 11

1.2.3　步骤 3：可以从公开渠道获得的信息 …… 11

1.2.4　步骤 4：WHOIS 和 DNS 查点 …… 28

1.2.5　步骤 5：DNS 查询 …… 37

1.2.6　步骤 6：网络侦察 …… 44

1.3　小结 …… 47

▼ 第 2 章　扫描 …… 49

2.1　确定目标系统是否开机并在线 …… 50

2.1.1　ARP 主机发现 …… 51

2.1.2　ICMP 主机发现 …… 53

2.1.3 TCP/UDP 主机发现 …… 58
2.2 确定目标系统上哪些服务正在运行或监听 …… 63
2.2.1 扫描类型 …… 64
2.2.2 确定 TCP 和 UDP 服务正在运行 …… 66
2.3 侦测操作系统 …… 74
2.3.1 从现有的端口进行猜测 …… 75
2.3.2 主动式协议栈指纹分析技术 …… 76
2.3.3 被动式协议栈指纹分析技术 …… 80
2.4 处理并存储扫描数据 …… 82
用 Metasploit 管理扫描数据 …… 82
2.5 小结 …… 84

▼ 第 3 章 查点 …… 85

3.1 服务指纹分析技术 …… 87
3.2 漏洞扫描器 …… 88
3.3 最基本的标语抓取技术 …… 92
3.4 对常用网络服务进行查点 …… 94
3.5 小结 …… 157

第 2 部分 终端和服务器攻击

案例研究：国际阴谋 …… 160

▼ 第 4 章 攻击 Windows …… 161

4.1 概述 …… 163
4.2 取得合法身份前的攻击手段 …… 164
4.2.1 认证欺骗攻击 …… 164
4.2.2 远程非授权漏洞发掘 …… 180
4.3 取得合法身份后的攻击手段 …… 188
4.3.1 权限提升 …… 188
4.3.2 获取并破解口令 …… 189
4.3.3 远程控制和后门 …… 204
4.3.4 端口重定向 …… 208
4.3.5 掩盖入侵痕迹 …… 210

4.3.6 通用防御措施：攻击者已经可以“合法地”登录到你的系统时该怎么办 213
4.4 Windows 安全功能 217
4.4.1 Windows 防火墙 217
4.4.2 自动更新 218
4.4.3 安全中心 219
4.4.4 安全策略与群组策略 219
4.4.5 微软安全软件 MSE（Microsoft Security Esstentials） 221
4.4.6 加强减灾经验工具包 222
4.4.7 Bitlocker 和 EFS 222
4.4.8 Windows 资源保护（WRP） 224
4.4.9 完整性级别（Integrity Level）、UAC 和 PMIE 225
4.4.10 数据执行保护：DEP 226
4.4.11 Windows 服务安全加固 227
4.4.12 基于编译器的功能加强 231
4.4.13 反思：Windows 的安全负担 232
4.5 小结 232

▼ 第 5 章 攻击 Unix 235

5.1 获取 root 权限 236
5.1.1 简短回顾 236
5.1.2 弱点映射 237
5.1.3 远程访问与本地访问 238
5.2 远程访问 238
5.2.1 数据驱动攻击 243
5.2.2 我想有个 shell 259
5.2.3 常见的远程攻击 263
5.3 本地访问 282
5.4 获取 root 特权之后 299
rootkit 恢复 314
5.5 小结 315

▼ 第 6 章 网络犯罪和高级持续威胁 317

6.1 APT 是什么？ 319