<<黑客大曝光（第6版）>>

图书基本信息

书名：<<黑客大曝光（第6版）>>

13位ISBN编号：9787302218227

10位ISBN编号：7302218226

出版时间：2010-1

出版时间：清华大学出版社

作者：[美] Stuart McClure,Joel Scambray,George Kurtz

页数：658

译者：钟向群

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！

内容概要

本书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。

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。

<<黑客大曝光（第6版）>>

书籍目录

章节摘录

插图：正如你们将在下面章节中看到的，踩点、扫描及查点是情报收集中至关重要的概念。
正如一个银行抢劫者在实施最后致命一击之前会搜集银行的相关情报一样，你的网络敌人也会做同样的事情。
他们有计划地进行探查，直到找出你在网络中最易受攻击的软肋。
而且，这并不需要多长的时间。
指望这些坏家伙还是在打开所有选项使用网络扫描工具，比如nmap，已经是]999年（碰巧那一年我们写了第一版的《黑客大曝光》的古老想法了。
现在，这些家伙变得更加狡猾，他们知道藏匿行踪对于一个成功的黑客的重要性。
也许我们需要稍微深入讨论一下。
随着因特网的发展，保护隐私已成为一种独特的需求。
很多开发出来的系统具有实用价值的同时也提供强有力的匿名保护。
相比于洋葱路由器（TheOnionRouter，或简称Tof）系统，大多数系统做得显然不够的。
Tor系统基于洋葱路由器，是第二代低延迟匿名系统，用户可通过它在因特网上进行匿名交互。
Tor系统最初由美国海军研究实验室赞助，随后于2004年成为电子前沿基金会（ElectronicFron.tierFoundation，FFF）的项目。
洋葱路由可能听起和“铁人料理”之类的电视节目有些关系，但实际上它是提供网络匿名交互的相当复杂的一门技术。
洋葱路由志愿者在系统上提供一个洋葱代理服务器，客户通过这个代理以TCP协议在Tor网络上对外进行匿名交互。
Tor网的使用者必须在他们的系统上运行一个洋葱代理，这个代理允许他们在Tor网络上进行通信，并协商一个虚拟链路。
Tor之所以名为洋葱路由，是因为其采用了基于层次的高级别加密操作。
在所有的匿名网络中，Tor最重要的优势在于其独立于应用，在TCP数据流层工作。
它可以支持SOCKS代理，一般能够用于即时通信、互联网中继聊天系统（IntemetRelayChat，IRC）及web浏览器。
尽管目前还达不到100%的安全和稳定，Tot已经是一个实现在因特网的匿名交互的惊人的进步。

媒体关注与评论

“在任何公司里，如果想把安全做好，必须像黑客那样思考，并且紧跟真正的风险所在……黑客大曝光对这两方面者随行了完美注解”。

——Patrick Heim，CISO，Kaiser Permanent“从第1版开始，黑客大曝光系列就已经成为安全专业人员的权威指南，直到第6版它依然会在我的书架上拥有一席之地”。

——Jeff Moss，著名的BlackHat安全论坛的创始人“理解黑客思路以及防范方法的权威资源”。

——Vince Rossi，St．Bernard软件公司CEO兼总裁“每年由于身份窃取而导致的损失达数十亿元计。
除非你充分了解这类威胁，否则你很可能成为下一个受害者。
黑客大曝光第6版为你提供了避免成为受害者的工具”。

——Bill Loesch，Guard ID Systems公司CTO“这本书紧跟时代、全面、深入、源于实践，并且没有厂商的偏见——所有的这些都是任何安全从业人员珍视的特点”。

——Kip Boyle，PEMCO Mutual保险公司CISO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

<<黑客大曝光（第6版）>>

编辑推荐

《黑客大曝光:网络安全机密与解决方案(第6版)》：利用全球闻名的黑客大曝光团队提供的专家建议，您可以在当今高度互联的世界中克服难以应对的安全挑战。
依据经过时间检验的“攻击及对策”的思想，这本10周年纪念版已经进行了全面更新，涵盖了黑客世界中最新的秘密武器。
新增和更新的内容：新增了攻击硬件的章节，包括撞锁、门禁卡克隆、RFID攻击、USBU3攻击以及蓝牙设备劫持等更新了Windows攻击和对策，包括新的WindowsVista和SerVer2008操作系统漏洞，以及Metasploit漏洞利用最新的UNIX木马和rootkit技术，以及悬摆指针、输入验证漏洞利用方法新的无线和RFID安全工具，包括多层加密和网关全新的针对网络硬件和Cisco设备的路由跟踪和窃听技术涵盖了更新的拒绝服务攻击、中间人攻击、DNS毒化，以及缓冲区溢出攻击VPN和VolP漏洞利用，包括Google和TFTP技巧，SIP泛洪攻击，以及IPSec攻击对因特网用户攻击、Web攻击以及安全编码等章节进行了全面更新全球销量50万册，被翻译成26种语言计算机信息安全旷世之作·全球销量第一一本最为成功的信息安全旷世之作！
内容全面扩充升级，安全专业人员的权威指南

版权说明