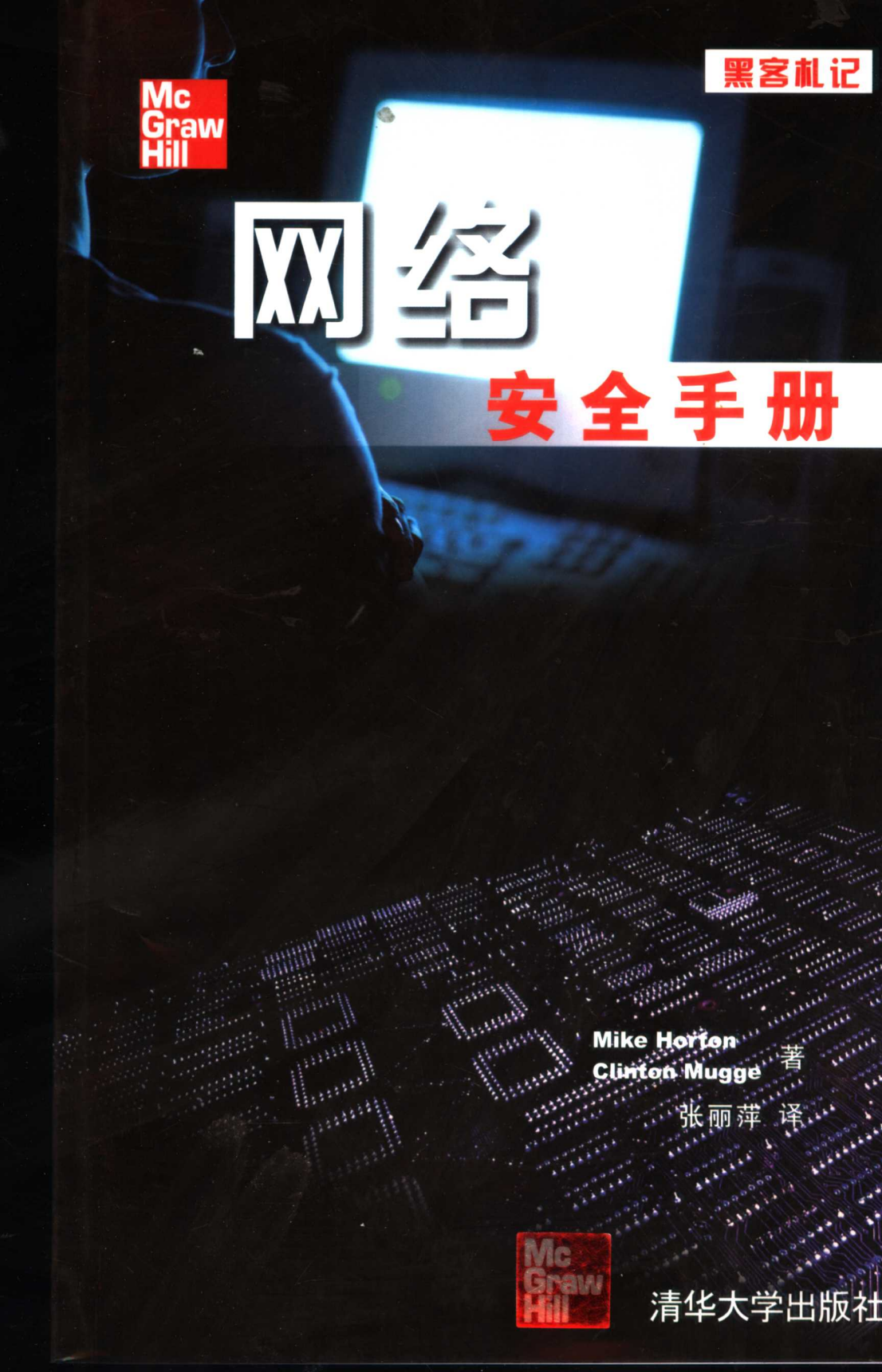
黑客札记
Mc Graw Hill
网络
安全手册
Mike Horton
Clinton Mugge 著
张丽萍 译
Mc Graw Hill
清华大学出版社

Mike Horton & Clinton Mugge
HackNotes: Network Security Portable Reference
EISBN: 0-07-222783-4

图书在版编目(CIP)数据

黑客札记:网络安全手册/哈顿(Horton,M.),穆格(Mugge,C.)著;张丽萍译.
—北京:清华大学出版社,2005.6
ISBN 7-302-10877-3

Ⅰ.黑… Ⅱ.①哈… ②穆… ③张… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2005)第 037989 号

出 版 者:清华大学出版社 地 址:北京清华大学学研大厦
http://www.tup.com.cn 邮 编:100084
社 总 机:010-62770175 客户服务:010-62776969
责任编辑:常晓波
封面设计:立日新
印 刷 者:北京密云胶印厂
装 订 者:三河市李旗庄少明装订厂
发 行 者:新华书店总店北京发行所
开 本:150×230 印张:17.75 字数:285 千字
版 次:2005 年 6 月第 1 版 2005 年 6 月第 1 次印刷
书 号:ISBN 7-302-10877-3/TP·7235
印 数:1~3000
定 价:32.50 元

作者简介

Mike Horton

Mike Horton 是 Foundstone 公司的首席顾问，从事安全网络结构设计、网络渗透评估、操作安全程序分析和物理安全评估。他是《黑客札记》系列书籍的主创人，也是 Enigma Sever 安全研究的缔造者（详见网站 www. enigmasever. com）。他有超过 10 年的公司和行业安全工作经验，为财富 500 强企业做过安全评估并且参与过军方的反间谍行动。

在加入 Foundstone 公司前，Mike 是防火墙和访问控制系统的安全集成顾问、Ernst & Young 公司的电子安全服务部的高级顾问，负责执行网络渗透评估，并且是某个安全的实时通信软件启动工作的首席技术员、美国军方反间谍密探。

Mike 获得位于华盛顿州西雅图市的城市大学的学士学位，同时也获得了军方的 Top Secret/SCI 证书。

Clinton Mugge

Clinton Mugge 是 Foundstone 公司在西海岸运作的咨询主管，提出并监督提供战略服务的问题，其范围从网络评估到综合的企业级风险管理。Clinton 的职业生涯是从作为军方信息战争部下属的特别计划组的反间谍密探开始的。他在研究过程中直接接触过物理、操作以及 IT 安全措施。离开军方后，他在 Ernst & Young 公司的电子安全解决方案小组工作，管理和实施网络安全评估。

Clinton 在 Blackhat、USENIX、CSI 以及 ISACA 做过演讲，写过《黑客大曝光》丛书、*Windows XP Professional Security*（2002 年，McGraw-Hill/Osborne 出版社），另外还是《应急响应》（2001 年，McGraw-Hill/ Osborne 出版社）的技术编辑。

Clinton 获得了南伊利诺伊大学的学士学位和马里兰大学硕士学位，并通过了 CISSP 认证。

撰稿人简介

Vijay Akasapu

Vijay Akasapu 是 Foundstone 公司信息安全顾问，通过了 CISSP 认证，从事产品评估、Web 应用程序评估以及安全架构设计。Vijay 先前为国际电信供应商设计安全架构，同时也做过侧重密码技术的安全应用程序开发，并从事过 Internet 安全方面的工作。他获取了密歇根州立大学的硕士学位，获得了马德拉斯印第安纳技术学院的学士学位。

Nishchal Bhalla

Nishchal Bhalla 是 Foundstone 公司信息安全顾问，从事产品测试、IDS 架构建立和设计、Web 应用程序测试等工作。Nish 为众多的著名软件公司、银行、保险公司以及其他的《财富》500 强企业做过无数的安全评估。他也是 *Windows XP Professional Security*（2002 年，McGraw-Hill/Osborne 出版社）的撰稿人，并且是 Foundstone 公司的“终极 Web 黑客行动”及“终极黑客行动”课程的主讲。

Nish 有 7 年的系统和网络管理经验，从事过包括 Solaris、AIX、Linux 和 Windows NT 在内的多种系统的安全工作。他先前的工作经验包括网络攻击和渗透测试、主机操作系统强化、基于主机和网络的入侵检测系统的实现、访问控制系统设计和部署、策略和程序开发。在加入 Foundstone 公司前，Nish 为 Sun Microsystems、Lucent Technologies、TD Waterhouse、The Axa Group 等公司提供工程以及安全咨询。

Nish 获得了谢菲尔德大学并行处理专业的硕士学位，获得了斯特拉思克莱德大学金融专业的硕士学位，本科毕业于班加罗尔大学的商学专业。他通过了 GSEC（SANS）和 AIX 认证。

Stephan Barnes

Stephan Barnes 是 Foundstone 公司现任西部地区销售部副经理，

是公司的元老级人物。Ste/phen 的专业技术包括渗透测试和顾问经历，曾为金融、电信、保险、制造业、公益事业和高新技术公司做过渗透方面的工作。Stephan 曾在 Big X 和 Northrop 公司从事多个“Black World”项目。Stephen 获得加利福尼亚 Pomona 的加州理工学院的计算机信息系统学士学位。

Stephan 是许多安全会议和地方组织的活跃分子。由于二十多年的“Black World”及 Big X 安全顾问经历，他在安全领域名声显赫。他还是《黑客大曝光》(McGraw-Hill/Osborne 出版社)的第二、第三及第四版的撰稿人，撰写了有关“战争拨号”、PBX 和语音电子邮件攻击等章节。Stephan 使用“M4phrlk”这个 White-Hat 昵称有二十多年了(他是真正意义的黑客，为系统厂商报告漏洞)，他的个人主页 www.m4phrk.com 概述和讨论了战争拨号、PBX、语音邮件安全背后的概念以及其他相关的安全技术。

Rohyt Belani

Rohyt Belani 是 Foundstone 公司信息安全顾问，从事渗透测试和 Web 应用程序评估，具有深厚的网络和无线技术背景。Rohyt 完成了多个产品的安全审查，涉及到架构和设计审查、渗透测试，以及对产品的审查。他还是 Foundstone 公司的“终极黑客行动”和“终极 Web 黑客行动”课程的主讲。

Rohyt 在去 Foundstone 公司的 CERT(计算机应急响应小组)做研究助理前获得了卡内基梅隆大学信息网络专业的硕士学位。

Rohyt 发表了大量计算机安全、网络仿真、无线网络及容错分布式系统相关主题的文章和研究报告

Robert Clugston

Robert Clugston 是 Foundstone 公司信息安全顾问，已经有 6 年的系统管理、网络安全及 Web 产品工程的经验。他最初加入 Foundstone 公司是设计和保护公司的网站，现在为客户提供这些服务。在加入 Foundstone 公司前他是一个 Internet 服务提供商的系统管理员，主要职责是部署、维护、保护重要业务系统，包括 Web 服务器、路由器、DNS 服务器、电子邮件服务器以及附加的 Internet 传输设备和系统。Robert 曾短时间做过 Perl/PHP Web 开发的独立承包商，他通过了 Windows NT 的 MSCE 认证。

Nitesh Dhanjani

Nitesh Dhanjani 是 Foundstone 公司的信息安全顾问，参与过《财富》500 强公司的许多项目，包括网络、应用程序、主机渗透、安全评估及安全构架设计服务。Nitesh 是安全类畅销书籍《黑客大曝光》(2003 年，McGraw-Hill/Osborne 出版社)的撰稿人，并且在许多技术出版物上发表文章，例如 *Linux Journal*。另外他也讲授 Foundstone 公司的"终极黑客行动：专家"和"终极黑客行动"安全课程。

在加入 Foundstone 公司前，Nitesh 是 Ernst & Young LLP 公司的信息安全服务部门的顾问，在那里，他完成了许多 IT 领域重大公司的攻击和渗透审查，同时也开发出了在 Ernst & Young LLP 公司的电子安全服务部门内使用的专用网络扫描工具。

Nitesh 获得了 Purdue 大学计算机科学专业的学士和硕士学位，在校期间他参与了大量的 CERIAS(信息维护与安全教研中心)项目组的研究项目。

Jeff Dorsz

Jeff Dorsz 是 Foundstone 公司现任高级安全和系统管理员，在他 11 年职业生涯中，在几个私营公司从事网络、系统及数据库管理方面的工作。另外，他还是企业级安全架构和基础设施部署的高级安全顾问。Jeff 撰写了关于安全的白皮书，包括 *Securing Windows NT*、*Securing Solaris*、*Securing Sendmail*。他在业余时间里担任南加利福尼亚州的大学和学院的讲师并对课程发展提出建议。

Matthew Ploessel

Matthew Ploessel 为 Foundstone 公司提供信息安全服务。他在过去的 5 年里从事着信息安全和电信领域的工作，主要研究 BGP 工程和第 2 层网络安全。他也是多本著作的撰稿人，包括全球畅销的《黑客大曝光》(2003 年，McGraw-Hill/Osborne 出版社)。Matthew 是聘用讲师、IEEE 会员，并且是位于洛杉矶的一家 ISP——Niuhi 公司的 CTO。

致谢

安全行业是个令人着迷的行业，里面充满着富有想像力的人，致力于安全事业。通过每个人的协作努力、研究、分析、建议，我们在不断地建设着一个无穷的安全相关主题的库。没有你们的支持，作为安全行业顾问的我们将一无所成，正是由于你们不断的支持，我们才能够创作这样一本书。我们感谢你们，感谢你们的努力，感谢你们的热情，我们希望能够竭尽全力献身于这个事业。

我们还要感谢 McGraw-Hill/ Osborne Publishing 的工作人员，正是在他们的指导和耐心校订下，这本书及这套丛书才得以出版。我们知道出书是一件棘手的事情，但我们很快发现“棘手”仅仅是表面现象，一本书带给那些在职人员繁重的工作，还有义务和责任。Scott Rogers、Jane Brownlow、Athena Honore、Katie Conley、Judith Brown、Monika Faltiss 以及其他的工作人员，跟你们一起工作是很愉快的。我们感谢你们的帮助和努力，我们期待你们继续努力。

当然，没有其他默默贡献的人群，这本书同样不可能成为现实。许多人坚持不懈地工作使得我们的文字更加生动，更加有信息量，他们是 Nitesh Dhanjani、Stephen Barnes、Jeff Dorsz、Nish Bhalla、John Bock、Rob Clugston、Vijay Akasapu、Rohyt Belani 和 Matt Ploessel。在日常工作中他们证明了一点：他们理解他们的工作，他们能够把他们拥有的渊博的知识和经验变成文字。我们也要感谢 Foundstone、Chris Prosise、George Kurtz 和 Stuart McClure，没有他们的努力，支持和帮助，这本书可能不会诞生。

技术评论简介

John Bock

John Bock 是 Foundstone 公司研发工程师，通过了 CISSP 认证，主要研究网络评估技术及无线安全。他负责 Foundstone 企业风险解决方案产品系列的新评估特性设计。他在网络安全方面有着作为顾问和某企业安全团队领导的深厚背景。在加入 Foundstone 公司前，他从事渗透测试和安全评估工作，做过 Internet 安全系统(ISS)的无线安全顾问。在到 ISS 前是 marchFIRST 的网络安全分析师，在那里负责维护一个拥有七千多用户的全球性网络。John 也是《黑客大曝光》(McGraw-Hill/Osborne 出版社)和 *Special Ops: Host and Network Security for Microsoft, UNIX, and Oracle Special Ops: Internet Network Securtiy*(2003 年，Syngress 出版社)的撰稿人。

《黑客札记》丛书

McGraw-Hill/Osborne 为安全专业人士策划了一套全新的便携手册。这套速成书籍对页数进行了控制，使之成为真正的便携手册。

《黑客札记》丛书的目标是：

- 提供易懂易用、精简的安全参考资讯。
- 教导大家如何保护网络或系统，展现黑客与犯罪分子如何利用知名手段闯入系统，阐述防御黑客攻击的最佳方式。
- 本套丛书能让那些新接触安全主题的人很快地上手，并且能提供精练、直接的知识源泉。为此大家会发现自己会不时地要参考本书。

这套丛书设计得易于携带，或者放在书包里也不会增加太多份量，并且使用时也不会引起不必要的注意。这套丛书尽可能地利用图表、表格与项目列表，只有在理解重点必须用到屏幕截图时，才会使用图例。更为重要的是，这套便携且轻巧的参考书不会用无关的空话烦人，也就不会让大家在繁忙工作之余还要费劲啃它们。我们保持了书写的清楚、精练与中肯。

不管是信息安全领域的新手(希望不用翻查 400 余页资料就能得到有用的基础知识与基本事实)，还是了解手册使用价值(手册相当于另一个大脑，它含有丰富的有用清单、表格及快速确认时所需的特定细节，或者说手册相当于一部安全话题的便携参考)的老练的专业人士，《黑客札记》丛书都能对你有所帮助。

丛书中的关键元素及图标

我们尽可能有条理地组织、展现本书。本书使用紧凑的形式，另外还放入页标签来标记主题。本书最后的“参考中心”包含了大家

希望快速、容易访问到的信息及表格。

图标说明

本书中用到的图标使得导航非常容易。每种黑客技术或攻击都用一个特殊的利剑图标突出标示。

这种图标代表一种黑客技术或攻击

获得黑客用以闯入脆弱系统的各种技术/谋略的详细信息。

只要可能，每种黑客技术或攻击也会有一种防御手段：防御手段同样也有自己的特殊图标——盾牌。

这种图标代表对抗黑客技术/攻击的防御手段

获得如何防御所展现黑客技术或攻击的精练细节。

《黑客札记》丛书设计时还用到了其他特殊元素，其中有一些脱离于正文的信息小块，这是为了引起注意。

"i"图标代表一种信息提示，表明阅读该具体小节内容时应该记住这一点。

这种火焰图标代表一种热门事物或一个重要问题，要避免花样繁多的缺陷，就不应该忽视它们。

命令与代码清单

本书通篇都用黑体字显示用户命令输入以表强调，比如：

```
[bash] # whoami
root
```

另外，Linux 和 Unix 命令及参数使用 monospaced 字体来和正文区分开来。如 whoami。

让我们听听你的意见

我们真诚地感谢你对本丛书的兴趣，希望你能觉得本丛书既有知识性又有趣味性。我们欢迎任何关于将来怎么改进的反馈意见。《黑客札记》丛书的初衷是迎合你的需求。欢迎到网站 http://www.hacknotes.com 上获得关于该丛书进一步的信息，你可以把意见和看法发送到信箱 feedback@hacknotes.com。

简介

安全领域里有这样一个简单的事实：如果不知道防范什么就不可能防范得非常好。即使知道在防范什么，理解黑客或罪犯们的心理和行事方法将能更好地保护自己。安全知识是把双刃剑：了解方法和战术所需的信息同样会教导攻击者。知识的传播只会变慢而不会停止，我们知道黑客在暗中潜伏，帮助防范者缩短学习过程是我们的责任。

本书的组织形式

本书分为四个主要部分：

- 第一部分：网络安全原理和方法
- 第二部分：黑客技术与防范
- 第三部分：专题
- 参考中心

第一部分：网络安全原理和方法论

第一部分对信息安全和黑客攻击的操作原理做了一个全面的概括和定义。同时也介绍性地提及了管理风险和评估风险。

- 第 1 章讲述了信息安全的组成部分，并讨论了它们之间的联系。本章通过搭建起一个框架为后面的章节打下基石。
- 第 2 章延伸了第 1 章介绍的原理，并集中阐述了风险管理和曾令人费解的风险评估的概念。

第二部分：黑客技术与防范

第二部分在第一部分介绍的安全概念基础之上详细讨论了计算机系统和网络内部的进程和方法，并阐述了危及系统安全的策略和技术以及相对应于这些攻击的防范措施。

- 第3章详细讨论了黑客行动模型，以及危及计算机系统和网络安全的几种过程。
- 第4章开始阐述黑客行动模型的实际技术，从信息搜集开始入手，读者将学会怎样了解、探测网络和系统。
- 第5章继续阐述黑客行动模型，讨论关于不同系统和网络的身份鉴定及威胁。

第三部分：专题

第三部分讨论了读者应该熟悉的一些有关更为重要的安全和攻击概念的专题。这些专题通常以高层次技术术语来描述，所表达的信息足够使你不仅仅能理解问题所在，而且能够很容易地继续学习你所选择的定向研究方面的知识。

- 第6章介绍了无线网络原理。本章讨论了其弱点及可能的攻防方法。
- 第7章给读者介绍了Web程序攻击原理，讨论其可能的攻防方法。
- 第8章对不同系统不同形势下的最常见的攻击方法做了一个集中的概述。本章从技术角度讲述了一些精选的主题，比如网络嗅探、社会工程学、漏洞利用代码和战争拨号。
- 第9章介绍了检测和响应，讨论了威胁检测的概念和方法，以及怎样处理系统威胁。
- 第10章概述了安全措施的最佳惯例和保护不同技术及系统的考虑因素。本章涉及了包括Windows、UNIX、Web、FTP、DNS、电子邮件、路由器、有线/无线网络和物理环境。
- 附录给出了Internet上一些安全方面的最佳资料的URL。所给出的URL涉及的主题有安全新闻和信息、漏洞利用程序

和攻击、密码破解和暴力破解字典、特洛伊木马信息、安全教育和认证、安全出版物、安全电子邮件列表和安全会议等。

参考中心

为了便于阅读，参考中心放在本书的最后。内容包括常用命令、常用端口、特定的在线资源、IP 编址和子网划分、ASCII 码表和顶级安全/攻击工具资源。

致读者

正如前面所述，本书提供的信息是双刃剑。我们希望读者选择“好”的方面。如果没有得到“测试”一个网络或环境的许可，请不要尝试用本书中的方法。这是违法的，会受牢狱之灾——一个非常了无生趣的地方。至少，这么做的代价很大。

总之一句话：向前迈进，披荆斩棘，学会事物是怎样运作的，应该干什么，在法律上不应该干什么。哪里是突破点？哪里是薄弱点？设计者和用户常常会在什么地方出纰漏或犯错误？综上所述，享受乐趣，坚持学习。还有许多信息安全知识方面的好书和资源等着你进一步学习。

目录

第一部分　网络安全原理和方法

第二部分 黑客技术与防范

第三部分 专题