Broadview
www.broadview.com.cn

安全技术大系

网络攻防技术与实践

诸葛建伟 编著

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

网络攻防技术与实践

诸葛建伟　编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书是一本面向网络安全技术初学者和相关专业学生的基础书籍，全面介绍了网络攻防的基本理论知识、技术方法和工具软件。在介绍每一部分网络攻防技术之后，通过一些自主设计和从社区借鉴的实践作业，来引导读者在具体实战答题过程中，更加深入地去理解所讲解的攻防理论知识与技术原理，并培养核心的安全攻防实践技能。

本书共分为四个部分 12 章，系统地介绍了网络攻防技术的基础知识体系、核心技术方法，并在每章中结合实际案例讲解、hands-on 动手实践、实践作业，来引导读者学习和掌握网络攻防的实践技能。

本书附带的 DVD 光盘中包含了各个章节的演示案例、hands-on 实践作业与部分实践的视频演示或示范解答。本书支持网站 netsec.ccert.edu.cn/hacking 上提供了搭建本书设计的网络攻防实验环境所需的定制虚拟机镜像，可供读者下载使用。在某种程度上，本书也是一本网络攻防技术的参考手册。

本书适合于网络和系统安全技术的爱好者、信息安全专业学生、网络与系统安全方向的研究生、网络与系统管理员，以及网络安全从业人员。

图书在版编目（CIP）数据

网络攻防技术与实践 / 诸葛建伟编著. —北京：电子工业出版社，2011.6
（安全技术大系）
ISBN 978-7-121-13802-7

Ⅰ. ①网… Ⅱ. ①诸… 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（2011）第 108279 号

策划编辑：毕　宁　　bn@phei.com.cn
责任编辑：许　艳
特约编辑：顾慧芳
印　　刷：三河市鑫金马印装有限公司
装　　订：
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
开　　本：787×980　1/16　印张：33　字数：707 千字
印　　次：2011 年 6 月第 1 次印刷
印　　数：4000 册　　定价：65.00 元（含 DVD 光盘 1 张）

前　言

“什么都略懂一点，生活更多彩一些。”

——金城武版“诸葛亮”于《赤壁》电影

笔者于2008年秋季开始以本书主要内容在北大讲授课程时，正是《赤壁》电影热映时期。《赤壁》中的大量雷人对白让很多人认为它并非预想中的史诗大片，而是搞笑片，但导演吴宇森却坚持称《赤壁》是部励志片，他表示赤壁之战体现了团结的力量，体现了勇气和智慧，与奥运精神还很相符。笔者在北大的大讲堂电影院观看影片时，与观众一样被“强烈地雷到”，刚从网上看到吴导对影片的定位时，也与网民一起对这种说法“嗤之以鼻”，但在哈哈大笑和轻蔑冷笑之后，仔细回味影片中塑造的一些个性鲜明的人物对白和形象，还是很能受到影片启迪的。作为诸葛氏族的后裔，笔者当然比较关注氏族的标志性人物——诸葛亮，金城武版“诸葛亮”的“略懂”成了他的口头禅，前后四次分别“略懂”阵法、音律，以及给马接生和制造军械，并以一句富有哲理的“什么都略懂一点，生活更多彩一些”收场“略懂篇”，为我们塑造了一位初出茅庐、聪明帅气但又谦和幽默的“真实版”诸葛亮。

尽管笔者复姓诸葛，故里浙江贾岙诸葛村与兰溪诸葛村的族谱中能找出从诸葛孔明至笔者的血脉传承，族人也多以诸葛亮传人而自居；但笔者在公开场合却不敢妄称诸葛亮后人，因族谱中从孔明次孙诸葛京至五胡乱华之后隋唐年间的传承关系经不起推敲，而南北朝时期仍流传的诸葛家族谱牒——《诸葛氏谱》在陈隋时代的亡佚，已经让笔者是否是诸葛亮后人成为了一个千古之迷：P。这种无法证伪的状况也让笔者在私底下可以“有恃无恐”地宣称自诸葛孔明到笔者的传承关系，好歹也多少借点氏族先贤的光啊。

一本“非淡泊无以明志，非宁静无以致远”的诸葛亮《诫子书》，在诸葛氏族繁衍生息中代代相传，也在激励着笔者在专业技术修养与教书育人的道路走得更加静心、更加踏实。“什么都略懂一点，生活更多彩一些”，这句金城武“假借”诸葛亮之口而出的名言，也被笔者用来鼓励自己，以及实验室与课堂上和笔者亦生亦友共同成长的学生们，一起去学习网络攻防专业知识、修炼实践技能，并探索创新的技术方法。

本书诞生过程

笔者自2008年开始在北大信息学院为研究生开设《网络攻防技术与实践》课程时，也曾翻阅了大量国内出版的相关教材与技术书籍，但这些书要么过于偏重理论，难以直接指导技术实践和应用；要么局限于网络安全技术和工具软件的基础性讲解，容易让读者上手，

但却无法让读者建立其对网络攻防技术的全局视图轮廓，并积累起完整的基础原理知识与实践技能体系；国外的一些经典信息安全书籍如《黑客大曝光》对初学者而言又过于纷扰繁杂，中文版的翻译质量也难如人意。因此笔者开始萌生编写本书的想法，期望将基础理论与实践技能进行很好的融合，既能让读者对网络攻防技术建立起比较清晰和完整的基础知识系统轮廓，又能引导读者通过动手实践掌握核心的网络攻防实践技能，提高解决实际问题的技术能力，从而更加适合于国内对网络攻防感兴趣的技术爱好者与相关专业的学生。然而由于当时笔者科研与授课任务的繁重，以及自认为当时还并未有足够的经验来驾驭完成这样的一本书稿，因此将编写本书的想法暂时搁置一边。

至2010年完成两轮课程授课、在学生反馈意见基础上进行不断地完善课程内容和实践材料之后，笔者在参加电子工业出版社博文视点组织的一次沙龙活动中，和毕宁编辑提起编写本书的想法，便很快收到了博文视点的书约。然而本书的写作过程并没有预期的那么轻松和顺利，虽然在2010年暑假中带着几位非常优秀的北大本科生组织了一个网络攻防技术Seminar，为本书的框架内容设计、实践选题、素材整理打下了坚实的基础，但在开始编写章节内容时，才真正体验到了书籍写作的艰辛。在编写本书的近十个月时间里，单位的科研和授课任务仍然繁重，并多次有项目申请、修改论文等紧急事务完全打断写作过程，期间笔者还经历了一次流程颇为漫长手续繁杂的调职，离开了学习和工作十三年之久的北大，“跳槽”到了隔壁清华，因此编写本书只能充分利用晚上与假期的时间，而笔者也成为了一个标准的“宅男”，除了上班之外“大门不出二门不迈”，埋头写书到深夜，在寒假春节期间甚至创造了近一个月没出一步房门的个人“宅男”记录。在历经“十月怀胎”之后，本书终于在2011年春暖花开之际完了稿。

本书特色

作为一本面向网络安全技术初学者和相关专业学生的基础书籍，本书内容上更多的是在笔者个人教学、科研和实践经验的基础之上，对网络攻防的基本理论知识、技术方法、工具软件进行的系统性整理与组织，同时结合了笔者在北大开设的相关课程授课经验，在介绍每一部分网络攻防技术之后，通过一些自主设计和从社区借鉴的实践挑战，来引导读者在具体实践解决挑战过程中，更加深入地去理解所讲解的网络攻防理论知识与技术原理，并培养起核心的安全攻防实战技能。

与网络安全技术同类书籍和教材相比，本书拥有如下的特色。

1）**注重网络攻防技术的系统性与基础性**，按照笔者在网络攻防技术多年的科研与授课经验，以攻防实验环境构建、网络攻防技术、系统攻防技术、Web攻防技术四大部分12章内容，尝试建立起网络攻防技术的基础框架；并在每个部分章节中提炼出网络攻防中最为

核心的基础技术，从原理知识开始，到技术方法、软件工具、实际实践、防范策略与技巧，期望让读者对网络攻防技术建立起比较清晰的知识与技能轮廓。

2）**突出实践能力的培养**，本书通过向读者提供一整套完整的网络攻防实验环境（基于虚拟机与蜜网技术，在支持网站提供下载），并在具体技术章节中结合实际网络攻防案例讲解、知名软件工具介绍、hands-on 实践、实践挑战与攻防对抗等多种形式，引导读者在掌握网络攻防技术原理的基础上，通过实际动手实战，熟悉和了解实现这些攻防技术最著名的一些开源与免费软件工具，并掌握相关的网络攻防实践能力，最终能够在实际环境中进行应用。

本书适合读者

- 网络和系统安全技术的爱好者。本书将帮助这些朋友建立起网络攻防技术的系统性基础知识轮廓，并培养锻炼攻防实践技能。
- 信息安全专业学生，网络与系统安全方向的研究生。本书可以作为本科生或研究生网络攻防技术方向课程的教材，并为选用本书的教师提供开课指导、教学课件、演示材料和课外实践作业的参考解答。
- 网络与系统管理员。知己知彼，百战不殆，作为防御和应对网络和系统攻击的一线技术群体，通过本书了解各种网络与系统攻击技术的基本原理、具体方法和相关工具，以及相应的安全防范技术措施，可以帮助他们更加安全地运营网络与信息系统，减少由于网络攻击遭受损失的风险。
- 网络安全从业人员。本书可以作为这些朋友的网络攻防技术参考手册。

本书属于全面系统性讲解网络攻防技术和实践的书籍，由于定位不同和篇幅限制，具体章节内容的技术深度与广度无法与专题技术类书籍相比，故本书在每个章节的参考与进一步阅读中列出了推荐的专题技术类书籍，为读者深入学习感兴趣的专题技术提供指引。

内容导读

本书共分为四个部分 12 章，系统性地介绍了网络攻防技术的基础知识体系、核心技术方法，并在每章中结合实际案例讲解、hands-on 动手实践、实践挑战作业，来引导读者学习和掌握网络攻防的实践技能。

第一部分　概述

第 1 章　网络攻防技术概述

笔者通过亲身经历的黛蛇蠕虫应急响应事件这个典型案例，让读者建立起对网络攻防技术的初始印象；然后回顾网络攻防技术领域的掌控者——黑客道的发展史，来共同体会黑客先驱们创道的激情与艰辛；作为技术概述，还将给出网络攻防技术框架体系，并以此

作为本书结构，来展开对各种类型攻防技术的介绍与讲解；本章还将向读者介绍攻防技术中不可忽视的物理攻击与社会工程学。

第 2 章　网络攻防实验环境

作为实践技能锻炼与培养的基础平台，本章介绍的网络攻防实验环境在整本书中的地位至关重要。为了更好地发挥本书培养实战技能的作用，建议读者在了解实验环境的基础技术原理、组成结构与详细的组件配置情况后，能够按照本书附带的详细操作文档，在自己的计算机中尝试搭建起一套完全属于自己的“网络攻防实验室”，并充分利用这套环境来进行后继章节的实践能力培养。

第二部分　网络安全攻防技术与实践

第 3 章　网络信息收集技术

信息是决定网络攻防博弈的胜负关键，本章主要讨论攻击者可能采用的各种网络信息收集技术，以及防御者相应的防范和应对措施。在本章中，读者将看到一个结合各种信息收集技术追溯攻击者的案例，也将面对使用各种在线工具进行 DNS 和 IP 信息查询追踪、Nmap 系统配置扫描和 Nessus 漏洞扫描的动手实践，并完成个人互联网足迹搜索等实践挑战。

第 4 章　网络嗅探与协议分析技术

网络嗅探与协议分析无论是对于网络攻击者、还是防御者，或安全研发人员，都是一个基础技术，本章将对嗅探与协议分析技术原理、实现机制和软件工具进行细致介绍，并提供使用 tcpdump 和 Wireshark 工具解决基本嗅探和解码任务的动手实践挑战。

第 5 章　TCP/IP 网络协议攻击

TCP/IP 协议是 Internet 得以成功的基础，本章讨论了 TCP/IP 网络基础协议所面临的安全问题和攻击技术，包括网络层上的 IP 源地址欺骗、ARP 欺骗与 ICMP 路由重定向攻击，以及传输层上的 TCP RST 攻击、TCP 会话劫持、TCP SYN Flood 与 UDP Flood 拒绝服务攻击，并介绍了如何应用最新的安全协议来加固基础网络。在本章中，读者也可以利用开源的 Netwox 工具来亲身体验基础网络协议攻击的过程。

第 6 章　网络安全防范技术

本章是本书中唯一的完全从防御者角度来介绍安全模型体系、技术和软件工具的章节，分别详细介绍了防火墙、入侵检测与安全响应技术，并期望读者能够通过具体动手实践来掌握开源社区中非常优秀和传统的安全解决技术方案——netfilter/iptables 防火墙以及 Snort 入侵检测系统。

第三部分　系统安全攻防技术与实践

第 7 章　Windows 操作系统攻防

本章可能是一些读者最感兴趣的，因为目前 Windows 操作系统在国内的台式机和服务

器市场上均占据了优势地位，所以针对 Windows 系统的攻击也是最为常见和流行的。本章首先对 Windows 操作系统的安全体系结构和核心机制进行了简要介绍，然后按照从远程到本地的网络攻击基本流程，讨论了包括传统远程口令猜测和破解攻击、网络服务远程渗透攻击、本地特权提升攻击、敏感信息窃取、掩踪灭迹和远程控制在内的各类主流 Windows 攻击技术。本章还包括了对著名的 Metasploit 渗透测试开源软件，以及 Meterpreter 强力木马工具的演示与实践挑战，让读者更加深入地认知 Windows 系统渗透攻击技术。最后，本章简要介绍了针对这些主流攻击技术的安全控制机制和策略，来指导防御者更好地加固他们的 Windows 操作系统。

第 8 章　Linux 操作系统安全攻防

本章可以视为第 7 章的姊妹篇，采用了同样的内容结构和介绍流程，来讨论 Linux 操作系统上的远程和本地安全攻防技术。另外，本章还通过 Metasploit 软件进行 Linux 系统的远程渗透攻击挑战以及攻防对抗实践，来帮助读者掌握针对 Linux 系统的渗透攻击与安全监控防御实践技能。

第 9 章　恶意代码安全攻防

恶意代码作为网络攻击威胁自动化实施的利器，一直以来都是网络安全领域的主角。本章从恶意代码的基础知识、基本分类入手，来帮助读者理清目前恶意代码形态的“千头万绪”，然后由浅入深地介绍了恶意代码分析环境、静态恶意代码分析技术和动态恶意代码分析技术，并通过从简单的静态分析实践与 Crackme 分析实践，到难度较大的完整分析一个自制恶意代码样本、僵尸网络取证分析实践挑战，让读者能够循序渐进地通过实际动手分析恶意代码样本和场景数据，来建立起恶意代码分析的基本技术能力。

第 10 章　软件安全攻防——缓冲区溢出和 Shellcode

所有安全攻防问题归根结底都离不开底层软件代码的安全漏洞与破解，而缓冲区溢出是一种最为基础的软件安全漏洞与利用技术，本章以缓冲区溢出，特别是栈溢出作为重点，介绍了软件安全漏洞的基本概念、基础机理和渗透利用技术，并对 Windows 和 Linux 两种主流平台上的缓冲区溢出利用技术和 Shellcode 撰写与提取原理进行了实例分析。本章还包含了两个基础的实践训练挑战题目，为对程序代码安全感兴趣的读者提供了编写和调试渗透利用与 Shellcode 入门代码的机会。

第四部分　Web 安全攻防技术与实践

第 11 章　Web 应用程序安全攻防

Web 从诞生以来一直是互联网上的“杀手级”应用，而 Web 攻防也是近年来网络攻防技术最炙手可热的领域。本章概述了 Web 应用体系结构各个层面上所面对的安全威胁，以及针对 Web 应用的多样化攻击渠道，然后结合具体实例，介绍了目前最流行的 Web 应用程

序攻击技术——SQL 注入与 XSS 跨站脚本。本章针对 SQL 注入、XSS 分别提供了实践挑战作业，让读者能够体验挖掘漏洞、利用漏洞攻击以及防御攻击的具体过程和技巧。

第 12 章　Web 浏览器安全攻防

Web 浏览器攻击技术（如网页木马、网络钓鱼等），是近年来针对网民用户最为流行的安全威胁形态，本章结合笔者近三年来在网页木马检测与分析方面的研究和开发经验，深入分析了网页木马威胁在国内流行的经济驱动力、技术基础和发展历程，结合具体实际案例细致地讲解了网页木马的技术机理，并和读者分享了网页木马检测分析技术方法和具体防范措施。本章也对网站钓鱼攻击幕后过程进行了揭示。作为实践挑战，本章将引导读者了解使用 Metasploit 渗透软件针对 Web 浏览器漏洞实施攻击的具体过程，并通过两个实际的网页木马案例，来提升读者应对网页木马攻击的技术能力。

本书附带资料、相关资源和建议使用方法

本书附带的 DVD 光盘中包含了各个章节的演示案例、hands-on 实践作业与部分实践挑战的视频演示或示范解答，另外也提供了一些笔者撰写的相关讲义资料。本书支持网站 netsec.ccert.edu.cn/hacking 上提供了搭建本书设计的网络攻防实验环境所需的定制虚拟机镜像，可供读者自由下载使用。

本书的撰写目标是能够为读者提供一套将网络攻防理论知识讲解和实践技能培养进行较好结合的参考书籍，在使用本书时，建议读者在阅读各个章节内容之后，能够按照提示从支持站点上下载相关软件与虚拟机镜像，建立起专属的网络攻防实验环境，并在环境中尝试各个章节中提供的 hands-on 实践和实践作业，对于所涉及的网络攻防工具，可以在参阅本书简要介绍内容基础上，通过搜索引擎了解更多工具使用的方法和技巧，并使用这些工具来完成挑战，相信通过这样的流程，读者能够充分发掘出本书的价值，并在网络攻防技术积累和实践技能方面得到提升。

技术支持

读者在阅读本书有任何问题或看法，请到 netsec.ccert.edu.cn/hacking 网站论坛上进行交流，同时读者也可以在该网站上找到本书中所涉及的软件、虚拟机镜像和其他有用工具。本书的答疑修订、再版内容也将在该网站上进行发布。笔者也非常欢迎读者将自己对本书中实践挑战的解答、建议发表在该论坛中，一起来探讨技术问题与实践技能。

致谢

本书全书均由笔者独立编写完成，但在编写过程中得到了笔者指导的几位学生——鲍由之、陈霖、彭立群、叶树雄、郑聪和余超旻的协助，他们在笔者组织的攻防技术 Seminar 中，投入了非常多的时间来制作相关实践的演示视频、解答样例，以及相关的文档图表，为丰富本书的实践技术内容及附带 DVD 光盘中配套材料作出了很大的贡献，谢谢你们！笔者课程自 2008 年以来的助教宋程昱、钟金辉和张慧琳在整理内容、实践答疑、协助改进授课质量等方面对笔者也帮助颇多，在此一并致谢。

感谢 SEED Project 为社区提供了大量的网络安全实践材料，本书中也采纳了部分 SEED Lab 作为实践挑战；感谢笔者所在的 The Honeynet Project 开源信息安全团队，参与团队中的研究讨论、开源开发让我在技术方面能够保持着热情，而每次参加 Annual Honeynet Workshop 总是让我受益匪浅，The Honeynet Project 对公众提供的取证分析挑战为本书也提供了部分实践素材；感谢宋程昱、陈志杰、韩心慧等中国蜜网项目组的成员，虽然我们的水平与 THP 核心的一些成员还有很大的距离，但我们一直都在努力，也相信团队能够发展得越来越好。

特别感谢电子工业出版社和博文视点公司提供本书出版的机会，感谢策划编辑毕宁一直以来的包容和督促，他总是在关键时刻注入本书撰写的推动力。感谢本书特约编辑顾慧芳和封面设计侯士卿所做的工作，你们的辛苦工作让本书避免了一些错误，并添色不少。

笔者在本书相关的研究内容上得到了国家自然科学基金项目（61003127）和教育部博士点新教师基金（200800011019）的资助，在此对资助方致以谢意。

最后，要感谢在背后默默支持我工作的家人，在我撰写本书的日子里，他们给予了我最大程度的包容、照顾、支持和鼓励。出于寒假中集中精力写书的需要，我没有按照惯例回到老家过年团圆，未能向进入花甲之年的父亲拜年祝寿；岳父岳母在本书撰写的大部分时间中来到北京，和我们生活在一起，承担了几乎所有的家务，照顾了我们的饮食与生活起居，让我的工作与撰书没有了后顾之忧；我的爱人帮我承担了家庭的琐事，并忍受了我在这段时间经常工作到深夜，并打搅了她原本就不好的睡眠；由于工作等原因，我们也一直在敷衍着来自父母、岳父岳母的唠叨，拖延着宝宝的出世时间。回想起这段时期内的一个个情景，只想对他们说："谢谢！我会更加努力，也会承担起作为儿子、作为丈夫，以及未来的父亲对家庭的责任，让我们的家庭拥有更加美好的未来！"

诸葛建伟

2011 年 4 月于清华园

目　录

第一部分　概述

第二部分　网络安全攻防技术与实践

第三部分 系统安全攻防技术与实践

1

第一部分　概述

CHAPTER

1

第 1 章　网络攻防技术概述

“道可道，非常道。名可名，非常名。无名天地之始，有名万物之母。故常无欲以观其妙；常有欲以观其徼。此两者同出而异名，同谓之玄，玄之又玄，众妙之门。”

——春秋·老子《道德经》

尘世间，万物发展皆有其“道”，网络攻防技术之“道”则由真正意义上的黑客们所掌控，谓之黑客道。在黑客道的起源和发展过程中，最早的黑客先驱和前辈们创造了计算机与网络，让我们的社会拥有了丰富多彩的网络世界；那些自称为黑客的网络“骇客”们出于经济、政治、心理等各种不同类型的动机，在这个原本平和的网络世界中兴风作浪，对人们能够安全和自由地使用计算机网络构成威胁；而真正的黑客们，则在利用他们的智慧、经验和技能，永不停歇地探索着新的攻防技术，帮助人们建设一个更加安全、开放和自由的网络世界。本章将对网络攻防技术基本轮廓，以及网络攻防领域的掌控者——黑客道进行概述。

1.1　网络攻防实际案例——黛蛇蠕虫

黛蛇（Dasher）蠕虫是互联网上爆发的一个著名蠕虫案例，对该蠕虫的应急响应处置是笔者在学生阶段与狩猎女神团队（中国蜜网项目组）一起在网络攻防技术领域的“开山之作”。我们在第一时间监测到了黛蛇蠕虫的活动，并截获了传播样本，在深入分析样本行为机理的基础上，协助国家计算机网络应急技术处理协调中心（CNCERT/CC）对该蠕虫实施了有效控制，从而避免了它的进一步爆发性传播。本节将通过回顾黛蛇蠕虫事件全过程，以及重现蠕虫传播场景，希望给读者留下对网络攻防领域的一个初始印象。

1.1.1　黛蛇蠕虫事件过程

从 1988 年莫里斯（Morris）蠕虫造成互联网前身阿帕网（ARPANET）瘫痪开始，蠕