21世纪高等学校信息安全专业规划教材

网络攻防原理及应用

◎ 文伟平 编著

清華大學出版社

网络攻防原理及应用

◎ 文伟平 编著

清华大学出版社
北京

内 容 简 介

本书涵盖网络攻防中的常用方法，通过对网络攻击和网络防范两方面技术的介绍（特别针对缓冲区溢出导致的漏洞和缓冲区溢出的内存保护机制做了详细介绍），帮助读者较为全面地认识网络攻防的本质。

本书适合作为高等院校信息安全、网络空间安全及计算机相关专业的教材，也可作为安全行业入门者、安全领域研究人员及软件开发工程师的相关培训和自学教材。

图书在版编目(CIP)数据

网络攻防原理及应用/文伟平编著. —北京：清华大学出版社，2017
(21世纪高等学校信息安全专业规划教材)
ISBN 978-7-302-46692-5

Ⅰ. ①网… Ⅱ. ①文… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2017)第038742号

责任编辑：付弘宇　王冰飞
封面设计：刘　键
责任校对：梁　毅
责任印制：李红英

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
课 件 下 载：http://www.tup.com.cn，010-62795954
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：21　　**字　　数**：512千字
版　　次：2017年10月第1版　　**印　　次**：2017年10月第1次印刷
印　　数：1～2000
定　　价：49.00元

产品编号：054766-01

INTRODUCTION

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取、甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到了整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革，适应社会对信息安全人才的培养需求，教材内容坚持基本理论的扎实和清晰，反映基本理论和原理的综合应用，在其基础上强调工程实践环节，并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要，促进教学发展。教材要适应多样化的教学需要，正确把握教学内容和课程体系的改革方向，在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略，突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上；特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本，合理配套。专业核心课和相关基础课的教材要配套，同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化，基本教材与辅助教材、教学参考书，文字教材与软件教材的关系，实现教材系列资源的配套。

(5) 依靠专家，择优落实。在制定教材规划时依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

21 世纪高等学校信息安全专业规划教材

联系人：魏江江 weijj@tup.tsinghua.edu.cn

FOREWORD

前言

近年来，随着互联网络技术的飞速发展，互联网使用者不约而同地将注意力转向网络安全领域。用户在选择互联网服务时将商家是否能提供稳定安全的服务纳入考虑范畴，商家通过向客户提供安全的服务来吸引用户。从政府角度而言，网络空间安全已上升到国家安全层面，政府通过立法的手段来保障网络空间安全。为提升国内网络空间安全，需要大量从业人员加入到安全行业中。

如今市场上有大量关于网络攻防方面的书籍，其中不乏经典之作，笔者在阅读这些书籍的过程中收获良多。本书以介绍网络攻防技术为主，涵盖了网络攻防中常用的方法，通过介绍网络攻击和网络防范两个角度的技术，帮助读者较为全面地认知网络攻防的本质。笔者结合自身研究内容和教学经历，整理编写此书，希望能为读者提供不同的角度来认识网络攻防的世界。本书对缓冲区溢出导致的漏洞和针对缓冲区溢出的内存保护机制进行了详细的介绍，希望能为漏洞分析、漏洞挖掘、恶意代码研究方向的读者提供具有参考价值的实例。

内容及特色

第一部分　网络攻防基础

这一部分帮助读者建立良好的理论基础，以便读者阅读后文内容。在实际的攻防场景中，对网络安全现状、攻击原理、漏洞标准的了解并不是必需的，但这些理论知识有助于提升读者对于网络攻防的整体认知，帮助读者在后续的学习过程中从根本上理解技术点的应用范围和适用场景。

第 1 章分析了当代网络安全现状，介绍了信息安全领域的问题和发展趋势。读者通过阅读本章可对信息安全领域的网络攻防方向有整体的认知。

第 2 章详细介绍了网络攻击过程以及网络攻防模型。深入理解本部分内容有助于读者建立学习网络攻防技术的知识框架，帮助读者在阅读后文的过程中将细节知识点纳入整体知识框架中，加深读者对知识点的记忆和理解。

第3章介绍了漏洞标准以及漏洞分析方法。漏洞是攻击者和防护者在较量过程中关注的焦点。本部分除了介绍通用的漏洞标准，还详细介绍了漏洞分析技术、漏洞挖掘技术、漏洞利用技术。希望有意愿深入学习网络攻防知识的读者对本章进行深入学习，并按照本章介绍动手实践。

第二部分　网络攻击技术原理与防范

这一部分介绍在网络攻防世界中攻击者常使用的攻击技术。网络上已存在许多功能完备、可供读者使用的攻击工具，直接使用攻击工具有助于读者快速入门网络攻防领域，因此在本部分的每个章节中都会介绍相应的攻击工具。为防止读者陷入“通过使用工具就可以实施网络攻击”的误区，在每一章节中还会对实施攻击行为的原理进行深入的分析，可以让读者了解到实现攻击工具的内部底层原理。本部分的内容建立在读者对于计算机网络技术有一定认知的基础上。本部分中每个章节的内容相对独立，读者可选择感兴趣的章节阅读。

第4章介绍了网络攻击扫描技术，在网络攻击场景中，搜集攻击目标信息是实施攻击行为的重要环节之一。读者通过阅读本章节可以掌握攻击者搜集信息的方法、过程以及途径。

第5章详细介绍了恶意代码的原理、传播、实现，恶意代码的关键性技术以及分析恶意代码技术的方法体系。本章部分涉及对各类恶意代码实现技术细节的分析，仅适合于对计算机体系有一定理解的读者阅读。

第6章主要介绍了攻击者针对用户口令的攻击方式，并以实际场景中的服务和软件为例列举了几种常见的口令破解工具。口令攻击的实现原理相对容易被读者理解，没有计算机基础的读者也可以阅读本章内容。

第7章阐述了各类网络欺骗攻击，欺骗攻击的实施难度不高，但产生的负面影响大。理解本章内容需要读者对计算机网络有一定的了解，通过本章的学习读者可以采取技术手段绕过攻击者的欺骗攻击。

第8章主要介绍了缓冲区溢出攻击的原理，列举出针对不同操作系统的典型缓冲区溢出攻击实例，并向读者推荐了几类防范缓冲区溢出攻击的方法。读者可以在阅读过程中实践构造相应的缓冲区溢出代码，这有助于读者深入理解缓冲区溢出的原理，加强读者对于程序运行时系统底层实现的理解。

第9章介绍了几类典型的拒绝服务攻击，并分析了其实现原理。拒绝服务攻击是攻击者常使用的网络攻击手段之一，本章内容适合对网络协议有一定了解的读者学习。

第10章介绍了SQL注入攻击的原理、注入策略、防范方法等。本章适合对SQL语言有一定了解的读者学习，也适合于服务器端的开发人员阅读，用于增强服务器端的数据安全。建议在阅读过程中配合实践，以便在实际环境中了解如何实施SQL注入攻击。

第三部分　网络攻击防范技术及应用

这一部分介绍对抗网络攻击技术的防范技术。信息安全领域中攻击和防范的联系是矛与盾的关系，通过不断的攻防对抗来提升攻防技术。在本书的第二部分介绍了大量的网络攻击技术，而本部分则着重介绍对抗网络攻击的防范措施，帮助读者了解安全从业人员通过哪些具体的策略实现对系统的保护，进而对抗外界的攻击。

第11章主要介绍了Windows操作系统安全。相较于Linux操作系统，Windows操作系统的安全增强功能封装性更强，加之Windows不是开源的操作系统，用户基于Windows进行自主开发的空间较小，因此本章主要介绍了Windows系统已经提供的安全防范功能，普

通的 Windows 用户也可通过本章的阅读对自己所使用的 Windows 系统进行安全增强。

第 12 章介绍了 Linux 操作系统的安全防护体系。以操作系统对于文件权限管理、用户认证、恶意代码查杀、协议安全等几个方面的安全加强措施作为切入点，帮助读者了解在对系统进行防范功能增强时，应当从哪些方面实施。本章适合对于 Linux 操作系统有一定了解的读者进行阅读。

第 13 章主要介绍了防火墙的原理及应用。随着硬件设备互联度的增强，设备间边界逐渐模糊，通过划分区域对设备进行安全隔离的技术已逐渐退出大众视野，但防火墙技术作为一种高级的访问控制设备对区域内设备和网络的保护起到了不容忽视的作用。读者通过阅读本章可以了解防火墙技术的实现部署细节，可以将其设计思路延续到其他场景的安全防护中。

第 14 章主要介绍了入侵检测的原理及应用。通过本章的学习，读者可以了解到攻击者在绕过防火墙的防范后，如何通过检测系统内动态的信息来发现攻击行为。入侵检测技术的实现原理在当今互联的设备中依旧可以延续使用，达到保护系统整体安全的目的。

第 15 章主要介绍了数据安全及应用。数据安全是系统防护的最后保障，保证用户在受到攻击后可以快速恢复，继续提供服务。为帮助读者理解数据安全实现的本质，本章还介绍几类不同的文件系统结构和数据恢复的基本原理。

第四部分　新型网络攻击防范技术探索

这一部分介绍了新型的漏洞分析技术，对新型操作系统的安全机制进行分析。本部分内容翔实，涉及计算机底层知识，需要读者在对计算机技术有较为深入理解的基础上再进行阅读。本部分需要实践操作的内容较多，所以在阅读本部分内容时，建议读者根据书中的指导进行手动调试，更有助于增强理解。

第 16 章介绍了新型的漏洞分析技术，为了方便读者理解，对应不同漏洞分析方法配合了相关的实例分析。本章的漏洞分析以 MS11－010 漏洞为例，建议读者在了解 MS11－010 漏洞原理的基础上进行学习。

第 17 章介绍了对于 Windows 7、Windows 8 以及 Windows 10 系统的内存保护机制。需要读者对系统底层有充分的了解之后再学习内存保护机制的内容，对本章内容理解困难时建议读者结合第 8 章缓冲区溢出的知识进行理解。

适合的读者

信息安全、网络空间安全专业学生及安全行业入门者

本书囊括许多攻防工具的实际操作和系统底层知识的介绍，有助于初学者了解安全领域涉及的各类知识，帮助初学者快速入门。

安全领域研究人员

本书介绍了一些安全领域的研究方法，可以为安全从业人员进行漏洞分析、漏洞挖掘、恶意代码分析等方面的研究提供一定的帮助。

软件开发人员

安全作为软件开发的质量属性之一，是开发人员在设计实现软件时必须考虑的重要因素之一。通过阅读本书可以帮助开发者了解如何通过编码加强软件的安全性。

配套资源与支持

在本书交稿之后，笔者依然担心会因自身语言表达和理解不足误导读者对于知识的领悟。由于笔者的写作水平和写作时间有限，书中存在许多不足之处，因此特开通读者邮箱 weipingwen@ss.pku.edu.cn 与大家共同交流，如有任何建议和意见欢迎随时与笔者联系。

本书的配套 PPT 课件等资源可以从 www.tup.com.cn 下载，关于本书的使用及课件下载中的问题，欢迎联系 fuhy@tup.tsinghua.edu.cn。

本书的勘误将不定期发布在 www.pku-exploit.com(北京大学软件安全小组)网站，该网站持续发布关于漏洞评测等专业文章，欢迎读者访问。

致谢

感谢本书编辑付弘宇老师。在编写本书期间，她提出了许多建议，由于她细心付出才使得本书得以顺利出版。感谢我的家人对我一直以来的支持和理解，是他们给了我继续学习的动力。感谢北京大学软件安全小组所有成员为本书初期工作付出的努力。感谢我的师兄蒋建春老师对我的支持，希望我们能继续保持在专业领域的切磋和交流。感谢那些不断在安全领域进行探索的组织和个人，没有他们的奉献，笔者无法在安全领域进行深入的研究。

作　者

2017 年 5 月

CONTENTS

目录

第一部分　网络攻防基础

第三部分 网络攻击防范技术及应用