高等院校信息安全专业规划教材

网络攻防原理

- 密码技术、网络侦察技术、网络扫描技术、拒绝服务攻击
- 计算机病毒、木马的基本概念、工作原理及防御方法
- 网络监听技术、缓冲区溢出攻击、Web网站攻击技术
- 信息认证技术、访问控制技术、网络防火墙技术、入侵检测技术

提供电子教案

吴礼发　洪 征　李华波　编著

机械工业出版社
CHINA MACHINE PRESS

高等院校信息安全专业规划教材

网络攻防原理

吴礼发　洪征　李华波　编著

机械工业出版社

面对严峻的网络安全形势，了解和掌握网络攻防知识具有重要的现实意义。本书着重阐述攻防技术原理及应用，内容包括网络攻防概论、密码技术、网络侦察技术、网络扫描技术、拒绝服务攻击、计算机病毒、特洛伊木马、网络监听技术、缓冲区溢出攻击、Web 网站攻击技术、信息认证技术、访问控制技术、网络防火墙技术和入侵检测技术。

本书可作为网络工程、信息安全、计算机等专业的教材，也可作为相关领域的研究人员和工程技术人员的参考书。

图书在版编目（CIP）数据

网络攻防原理/吴礼发，洪征，李华波编著. —北京：机械工业出版社，2012.2
高等院校信息安全专业规划教材
ISBN 978-7-111-37234-9

Ⅰ. ①网… Ⅱ. ①吴… ②洪… ③李… 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（2012）第 012431 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：郝建伟 牟桂玲
责任印制：杨 曦
北京鑫海金澳胶印有限公司印刷

2012 年 4 月第 1 版·第 1 次印刷
184mm×260mm·17.5 印张·434 千字
0001—3000 册
标准书号：ISBN 978-7-111-37234-9
定价：35.00 元

凡购本书，如有缺页、倒页、脱页、由本社发行部调换

电话服务
社服务中心：(010)88361066
销售一部：(010)68326294
销售二部：(010)88379649
读者购书热线：(010)88379203

网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com

封面无防伪标均为盗版

出版说明

信息技术的发展和推广，为人类开辟了一个新的生活空间，它正对世界范围内的经济、政治、科教及社会发展各方面产生重大的影响。如何建设安全的网络空间，已成为一个迫切需要人们研究、解决的问题。目前，与此相关的新技术、新方法不断涌现，社会也更加需要这类专门人才。为了适应社会对信息安全人才的需求，我国许多高等院校已相继开设了信息安全专业。为了配合相关的教材建设，机械工业出版社邀请了解放军信息工程大学、解放军理工大学通信工程学院、上海交通大学、西安电子科技大学、湖南大学、中山大学、南京邮电大学等高校的专家和学者，成立了教材编委会，共同策划了这套面向高校信息安全专业的教材。

本套教材的特色：

1. 作者队伍强。本套教材的作者都是全国各院校从事一线教学的知名教师和学术带头人，具有很高的知名度和权威性，保证了本套教材的水平和质量。

2. 系列性强。整套教材根据信息安全专业的课程设置规划，内容尽量涉及该领域的方方面面。

3. 系统性强。能够满足专业教学需要，内容涵盖该课程的知识体系。

4. 注重理论性和实践性。按照教材的编写模式编写，在注重理论教学的同时，注意理论与实践的结合，使学生能在更大范围内、更高层面上掌握技术，学以致用。

5. 内容新。能反映出信息安全领域的最新技术和发展方向。

本套教材可作为信息安全、计算机等专业的教学用书，同时也可以供从事信息安全工作的科技人员以及相关专业的研究生参考。

机械工业出版社

前　言

近年来，新型网络服务的发展、通信量的上升以及计算机技术和通信技术的进步，一直推动着计算机网络不断向前发展。网络技术的发展进一步促进了网络在世界范围内的广泛应用，网络就像水电一样，已成为生活中不可缺少的部分。人们在享受网络带来的种种便利时，也不得不承受它所带来的问题。网络上每天都有成千上万的网络安全事件发生，影响对象小到普通民众、商业公司，大到军队、国家。国家政治、经济、文化、军事等受网络的影响日益增强，网络在国家安全中的地位越来越重要。因此，了解和掌握网络攻防知识，具有重要的现实意义。

全书共分14章，系统地阐述网络攻防技术的基本原理及应用。第1章介绍网络安全形势、网络安全威胁、网络安全防护体系与发展。第2章介绍密码技术，包括密码学的基本概念、古典密码系统、现代密码系统和典型的现代密码算法。第3章介绍网络侦察技术，包括网络侦察的方法、网络侦查工具及网络侦察防御。第4章介绍网络扫描技术，包括主机扫描技术、端口扫描技术、操作系统扫描技术和漏洞扫描技术。第5章介绍拒绝服务攻击，包括拒绝服务攻击的分类、剧毒包型拒绝服务攻击、风暴型拒绝服务攻击、拒绝服务攻击的应用、拒绝服务攻击的检测及响应技术。第6章、第7章分别介绍计算机病毒和木马的基本概念、工作原理及防御方法。第8章介绍网络监听技术，包括监听技术的基本原理，共享网络和交换网络的监听方法以及网络监听的防范方法。第9章介绍缓冲区溢出攻击，包括缓冲区溢出攻击的原理、分类及防御方法。第10章介绍Web网站攻击技术，包括SQL注入攻击、跨站脚本攻击和Cookie攻击。第11章介绍信息认证技术，包括身份认证、数字签名、报文认证和数字证书认证中心。第12章介绍访问控制技术，包括访问控制的基本概念，自主访问控制、强制控制和基于角色的访问控制技术的原理和实现，以及常见的访问控制模型与实现等。第13章介绍网络防火墙技术，包括防火墙的基本概念、工作原理、体系结构、评价标准和使用方法等。第14章介绍入侵检测技术，包括入侵检测的基本概念，入侵检测系统的信息源和分析方法，以及典型的入侵检测系统。

本书可作为网络工程、信息安全、计算机等专业的教材，参考理论学时数为40～50学时（本书附带的电子课件是按理论学时数为40学时来组织的），实验学时数为20～30学时。学习本门课程之前，读者最好对计算机网络、操作系统、C语言程序设计等课程的内容已有所了解或掌握。因此，建议在大学四年级或研究生阶段开设本课程。本书也可作为相关领域的研究人员和工程技术人员、广大网络攻防技术爱好者的参考书。

从2000年起，编者一直主讲本科生的网络攻防原理课程。在授课过程中，深感以网络攻击技术为主，着重阐述攻防技术原理及应用的可作为教材的书籍较少。虽然介绍攻击的参考书众多，各种宝典、攻略、秘籍随处可见，但大多是介绍具体攻击工具的使用方法；大量介绍网络安全原理的教材仅适合以防护技术为主的网络安全类课程。基于此，编者所在的课程建设小组经过多年的教学实践，确定了网络攻防课程的教学内容，自编了课程讲义。本书的主体内容就是在课程讲义的基础上修改而成的。经过10多年的教学实践，深受学生的好评。

本书的第1章、第5章、第9章、第10章由吴礼发编写，第2章、第4章、第6章、第7章、第8章、第11～14章由洪征编写，第3章由李华波编写，全书由吴礼发统稿、审定。编者邮箱 wulifa@ vip. 163. com。

本书在编写过程中得到了编者所在课程建设小组其他成员（胡谷雨教授、赖海光副教授、潘志松副教授、郑成辉讲师、曾晓光讲师）的大力支持，博士研究生周振吉也为本书部分内容提供了很好的建议，在这里表示诚挚的感谢。

由于网络攻防技术涉及内容广，更新速度快，加之编者水平有限，书中的错误和不妥之处在所难免，敬请读者批评指正。

编　者

高等院校信息安全专业规划教材

编委会成员名单

目　录

第1章 绪 论

1.1 网络安全形势

近年来，三股来自不同方向的力量一直推动着计算机网络不断向前发展，这三股力量是：新服务的发展、通信量的上升和信息技术的进步。不断增长的网络应用需求催生了各种各样的新型网络服务，而新型网络服务的实现对网络技术提出了新的要求。为了应对日益增长的网络流量，特别是多媒体流量，各种新的网络传输技术相继出现，进一步促进了网络技术的发展。而信息技术的发展，特别是计算机技术和通信技术的发展，更是对网络技术的发展起到了非常大的促进作用。网络技术的发展进一步促进了网络在世界范围内的广泛应用，网络已深入到人们的日常生活当中，就像水电一样，是生活中不可缺少的部分。

人们在享受网络带来的种种好处时，也不得不承受它所带来的问题。每天都有成千上万的网络安全事件发生，影响对象小到普通民众、商业公司，大到军队、国家。国家政治、经济、文化、军事等受网络的影响也日益增强，网络在国家安全中的地位越来越重要。

下面来看几起比较著名的网络安全事件。

1）1995 年 8 月 21 日，设防严密的花旗银行系统网络（Citi Bank）被俄罗斯黑客 Vladimir Levin 通过 Internet 侵入，损失现金高达 1000 万美元。

2）1996 年 8 月 17 日，黑客入侵美国司法部的网络服务器，将“美国司法部”的主页改成了“美国不公正部”，将司法部部长的照片换成了阿道夫·希特勒，将司法部的徽章换成了纳粹党的党徽，并加上一张色情女郎的图片作为司法部长的助手。同年 9 月 18 日，黑客们又将美国“中央情报局”主页改成了“中央愚蠢局”。

3）1997 年由于黑客入侵美国空军防务系统，五角大楼被迫把防务网络关闭 24 小时。

4）1999 年 4 月 26 日，由台湾学生陈盈豪制造的“CIH”病毒发作，震撼了全球，据保守的估计至少有 6000 万台计算机受害。

5）2000 年 2 月发生的黑客攻击事件，使雅虎、亚马逊、微软等世界著名大公司的网络几近瘫痪，直接或间接经济损失高达上亿美元。

6）中美撞机事件导致中美黑客大战，从 2001 年 4 月 30 开始，两天内已有超过 700 家中美政府及民间网站相继被“攻陷”。

7）2001 年，“红色代码”（Code Red）、“红色代码Ⅱ”病毒大规模爆发，导致全球网络大范围的访问速度下降甚至阻断。

8）2003 年的“熊猫烧香”病毒，造成了巨大的经济损失。

9）2009 年 5 月 19 日发生的网络攻击事件，导致我国江苏、安徽、广西、海南、甘肃、浙江六省区电信互联网络瘫痪。

以上这些事件只是每天都在上演的网络安全事件中的几朵比较大的浪花而已。根据国家互联网应急中心（CNCERT）发布的《2009 年中国互联网网络安全报告》中指出，2009

年 CNCERT 共接收到 21927 件网络安全事件报告，而实际的网络安全事件要远远超过这个数量。

由此可见，网络安全问题日益严重，研究网络安全问题、了解和掌握网络安全知识具有重要的现实意义。

1.2 网络战

随着信息时代的到来，战争的形式也在发生着深刻的变化，现代战争已成为信息的战争。信息是战略资源、决策资源，可以毫不夸张地说，它是战场的灵魂和武器系统的核心。而网络是敌对双方借以获取信息优势的制高点，网络攻击与防护已成为军队作战的新模式，即网络战。

网络战是为干扰、破坏敌方网络信息系统，并保证己方网络信息系统的正常运行而采取的一系列网络攻防行动。它正在成为高技术战争的一种日益重要的作战样式，通过破坏敌方的指挥控制、情报信息和防空等军用网络系统，可以悄无声息地破坏、控制敌方的商务、政务等民用网络系统，不战而屈人之兵。

美国于 2003 年 2 月 14 日正式将网络安全提升至国家安全的战略高度，并发布了《国家网络安全战略》，从国家战略的全局谋划网络的正常运行并确保国家和社会生活的安全稳定。

2005 年 3 月，美国国防部公布的《国防战略报告》中明确将网络空间和陆、海、空以及太空定义为同等重要的、需要美国维持决定性优势的五大空间。

2009 年 6 月，美国国防部长盖茨宣布正式创建网络战司令部，对目前分散在美国各军种中的网络战指挥机构进行力量整合，协调当前美军的各种网络战武器，并制定关于如何运用这些武器的策略，明确美军的网络战战略，使得网络战科学、有序地长期进行。按照计划，美国网络战司令部将于 2030 年左右完成网络战部队的全面组建。该部队将担负网络攻防任务，确保美国在未来战争中拥有绝对的信息优势。

美军成立网络战司令部其实是美国网络空间国家安全战略的一部分，其主要意图在于：

（1）由攻击代替防御，实现网络威慑战略。

首先，美国具备了网络威慑的条件，主要表现在互联网的核心基础设施大部分由美国控制，例如，互联网 13 台根域名服务器中，有 10 台在美国；微软操作系统在个人计算机操作系统领域的市场占有率在 85% 以上；思科核心交换机、路由器遍布全球网络节点；英特尔的 CPU 占据全球计算机 90% 以上的市场份额。其次，美军还具备网络攻击的经历，在科索沃战争和伊拉克战争中美军都曾经通过网络攻击对手的信息系统，达到使对手的信息系统瘫痪的目的。可以说，网络威慑要甚于核威慑。

（2）全面发展“先发制人”的网络攻击能力。

美国是世界上第一个引入网络战概念的国家，也是第一个将其应用于战争的国家。2008 年年初，美国总统布什赋予国防部更大的网络战反制权，允许美军主动发起网络攻击，要求美军具备进入任何远距离公开或封闭的计算机网络的能力，然后潜伏在那里，保持“完全隐蔽”，并“悄悄窃取信息”，最终瓦解对方系统，兵不血刃地破坏敌方的指挥控制、情报信息和防空等军用网络系统。

2011 年年初，美国国防部引入一项新网络战略。该战略将网络入侵行为分门别类，其中

最严重一类是由一个国家对美国发起的网络攻击行为，这类攻击被视为“战争行为”，美国可对对方发起传统方式的军事回击。假想中的这一类攻击可能是，利用计算机网络破坏美国的供电系统导致大面积停电，利用网络系统攻击美国的城市交通等。

（3）频繁的网络攻防演习显示威慑力量。

美国在2006年、2008年和2010年先后进行了代号为“网络风暴Ⅰ”、“网络风暴Ⅱ”、“网络风暴Ⅲ”的网络攻防对抗演习。网络防御体系也已经被纳入北约的战略规划之中。

美国网络战司令部的最终目标是打造世界上最强大的黑客部队。这支黑客部队在平时以及战争爆发时，能渗透、监控、摧毁敌方网络系统并承担窃取情报的任务。经过多年的经验积累与实践，美国军方的一些高级黑客已经完全掌握了当今最先进的网络攻防技术，能够轻松渗入敌国军事和民用信息网络，并向系统中注入病毒或予以摧毁。

除了美国之外，俄罗斯、英国、日本、韩国、以色列和中国都提出了自己的互联网安全战略，同时，都已组建或正在积极组建、发展自己的网络战部队。

因此，了解和掌握网络对抗技术及网络战理论，对于保障国家安全具有重要的意义。

1.3 网络安全威胁

我们将所有影响网络正常运行的因素称为网络安全威胁，从这个角度讲，网络安全威胁既包括环境因素和灾害因素，也包括人为因素和系统自身因素。

1. 环境因素和灾害因素

网络设备所处环境的温度、湿度、供电、静电、灰尘、强电磁场、电磁脉冲等，自然灾害中的火灾、水灾、地震、雷电等，均会影响和破坏网络系统的正常工作。针对这些非人为的环境因素和灾害因素目前已有比较好的应对策略。

2. 人为因素

多数网络安全事件是由于人员的疏忽或黑客的主动攻击造成的，也就是人为因素，主要包括：

（1）有意：人为的恶意攻击、违纪、违法和犯罪等。

（2）无意：工作疏忽造成失误（配置不当等），对网络系统造成不良后果。

网络安全技术主要针对此类网络安全威胁进行防护。

3. 系统自身因素

系统自身因素是指网络中的计算机系统或网络设备因自身的原因导致网络不安全，主要包括：

1）计算机硬件系统的故障。

2）各类计算机软件故障或安全缺陷，包括系统软件（如操作系统）、支撑软件（各种中间件、数据库管理系统等）和应用软件。

3）网络和通信协议自身的缺陷也会导致网络安全问题，1.4节将详细分析互联网协议的安全问题。

系统自身的脆弱和不足（或称为安全漏洞）是造成信息系统安全问题的内部根源，攻击者正是利用系统的脆弱性使各种威胁变成现实。

一般来说，在系统的设计、开发过程中有很多因素会导致系统漏洞，主要包括：

1）系统基础设计错误导致漏洞，例如互联网在设计时没有认证机制，使假冒 IP 地址很容易。

2）编码错误导致漏洞，例如缓冲区溢出、格式化字符串漏洞、脚本漏洞等都是在编程实现时没有实施严格的安全检查而产生的漏洞。

3）安全策略实施错误导致漏洞，例如在设计访问控制策略时，没有对每一处访问都进行访问控制检查。

4）实施安全策略对象歧义导致漏洞，即实施安全策略时，处理的对象和最终操作处理的对象不一致，如 IE 浏览器的解码漏洞。

5）系统开发人员刻意留下的后门。一些后门是开发人员为了调试用的，而另一些则是开发人员为了以后非法控制用的，这些后门一旦被攻击者获悉，则将严重威胁系统的安全。

除了上述在设计实现过程中产生的系统安全漏洞外，很多安全事故是因为不正确的安全配置造成的，例如短口令、开放 Guest 用户、安全策略配置不当等。

尽管人们逐渐意识到安全漏洞对网络安全所造成的严重威胁，并采取很多措施来避免在系统中留下安全漏洞，但互联网上每天都在发布新的安全漏洞公告，漏洞不仅存在，而且层出不穷，为什么会这样呢？原因主要在于：

1）方案的设计可能存在缺陷。

2）从理论上证明一个程序的正确性是非常困难的。

3）一些产品测试不足就匆匆投入市场。

4）为了缩短研制时间，厂商常常将安全性置于次要地位。

5）系统中运行的应用程序越来越多，相应的漏洞也就不可避免地越来越多。

为了降低安全漏洞对网络安全造成的威胁，目前一般的处理措施就是打补丁，消除安全漏洞。但是，打补丁也不是万能的，主要原因是：

1）由于漏洞太多，相应的补丁也太多，补不胜补。

2）有的补丁会使某些已有的功能不能使用，导致拒绝服务。

3）有时补丁并非厂商们所宣称的那样解决问题。

4）很多补丁一经打上，就不能卸载。如果发现补丁因为这样或那样的原因不合适，就只好把整个软件卸载，然后重新安装软件，非常麻烦。

5）漏洞的发现到补丁的发布有一段时间差，此外，漏洞也可能被某些人发现而未被公开，这样就没有相应的补丁可用。

6）网络和网站增长太快，没有足够的合格的补丁管理员。

7）有时候打补丁需要离线操作，这就意味着关闭该计算机上的服务，这对很多关键的服务来说也许是致命的。

8）有时补丁并非总是可以获得的，特别是对于那些应用范围不广的系统而言，生产厂商可能没有足够的时间、精力和动力去开发补丁程序。

9）厂商可能在补丁中除解决已有问题之外添加很多的其他功能，这些额外的功能可能导致新的漏洞出现，系统性能下降，服务中断，或者出现集成问题和安全功能的暂时中断等。

10）补丁的成熟也需要一个过程，仓促而就的补丁常常会有这样或那样的问题，甚至还会带来新的安全漏洞。

11）自动安装补丁也有它的问题，很多自动安装程序不能正常运行。