HZ BOOKS
华章教育

高等院校信息安全专业规划教材

网络攻防技术

Network Security: Attack and Defense

吴 灏 ◎ 等编著

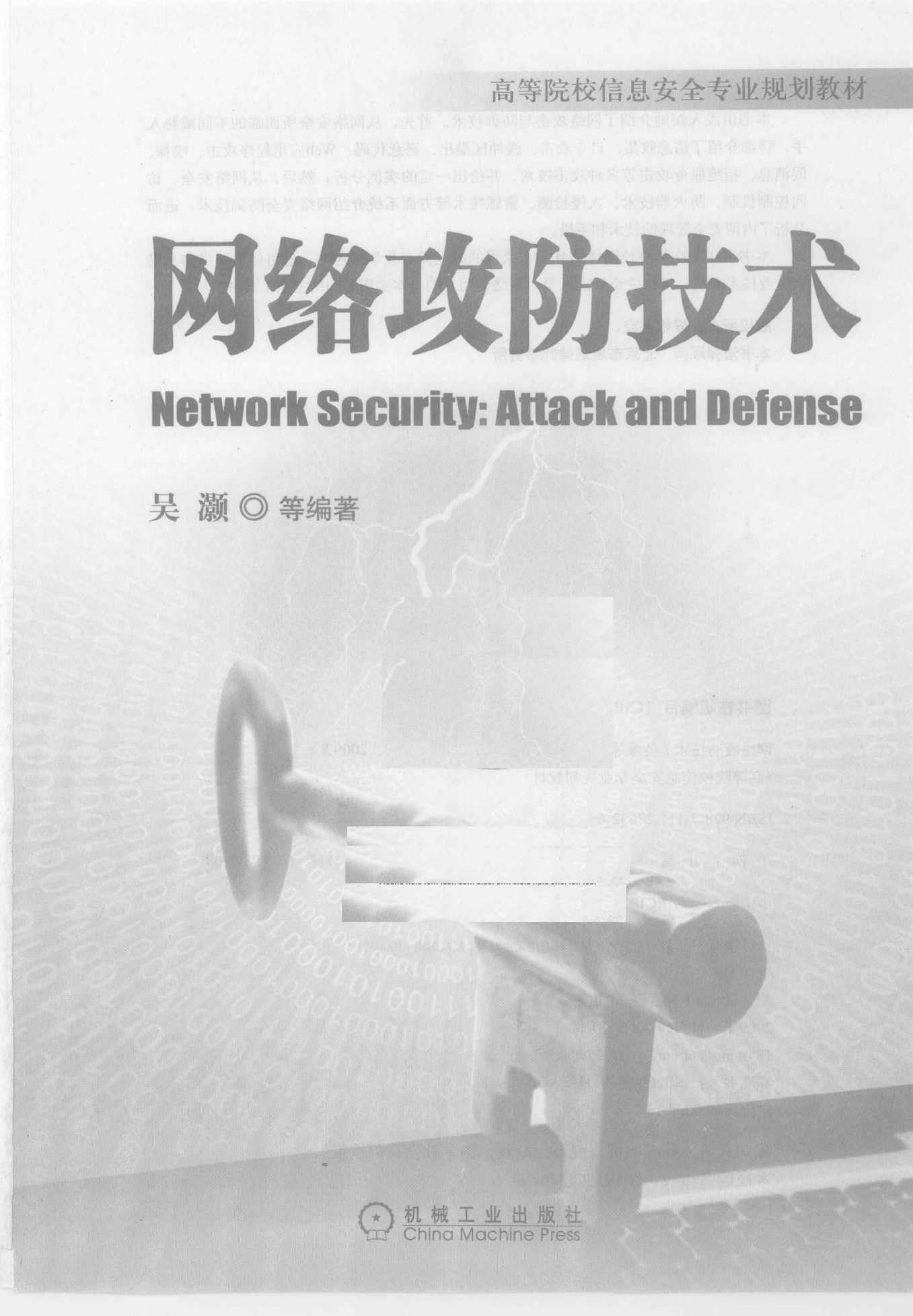
机械工业出版社
China Machine Press

高等院校信息安全专业规划教材

网络攻防技术

Network Security: Attack and Defense

吴 灏 ◎ 等编著



机械工业出版社
China Machine Press

本书由浅入深地介绍了网络攻击与防御技术。首先，从网络安全所面临的不同威胁入手，详细介绍了信息收集、口令攻击、缓冲区溢出、恶意代码、Web应用程序攻击、嗅探、假消息、拒绝服务攻击等多种攻击技术，并给出一定的实例分析；然后，从网络安全、访问控制机制、防火墙技术、入侵检测、蜜罐技术等方面系统介绍网络安全防御技术，进而分析了内网安全管理的技术和手段。

本书可作为高等院校网络信息安全课程的教材或者教学参考书，也可作为网络信息安全专业技术人员、网络安全管理人员、网络使用者的一本实用的网络安全工具书。

图书在版编目（CIP）数据

网络攻防技术 / 吴灏等编著. —北京：机械工业出版社，2009.8
（高等院校信息安全专业规划教材）

ISBN 978-7-111-27632-6

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

中国版本图书馆CIP数据核字（2009）第118881号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）
责任编辑：迟振春
北京京北印刷有限公司印刷
2009年8月第1版第1次印刷
184mm × 260mm · 15.25印张
标准书号：ISBN 978-7-111-27632-6
定价：29.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换
本社购书热线：（010）68326294

编委会

丛书序

经过数年的筹划与努力，信息安全系列丛书终于和广大读者见面了。

众所周知，进入21世纪以来，信息化对社会发展的影响日益深刻。全球信息化正在引发当今世界的深刻变革，重塑世界政治、经济、社会、文化和军事发展的新格局。

人们在享受信息化所带来的便利的同时，也不得不面对各种信息安全问题。信息安全是信息化的关键，各种天灾（如地震、洪水、飓风）和“人祸”（如网络故障、黑客入侵、病毒等）都会影响信息化进程。因此，在发展信息化的同时要重视信息安全，要在安全中发展，在发展中确保安全。

目前，世界各国都将信息安全视为国家安全的重要组成部分。党的十六届四中全会在《中共中央关于加强党的执政能力建设的决定》中明确提出：“坚决防范和打击各种敌对势力的渗透、颠覆和分裂活动，有效防范和应对来自国际经济领域的各种风险，确保国家的政治安全、经济安全、文化安全和信息安全”。党中央把信息安全和政治安全、经济安全、文化安全并列，作为我们国家四大安全内容之一，可见信息安全之重要，绝不能掉以轻心。近年来，我国在信息安全保障方面的工作逐步加强，制定并实施了国家信息安全战略，建立了信息安全管理体制和工作机制。基础信息网络和重要信息系统的安全防护水平明显提高，互联网信息安全管理进一步加强。

信息安全问题的解决，既要依靠技术的发展，更要重视人的作用。随着科技的进步，信息安全的概念和内涵不断发生变化，今天我们所说的信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等领域的交叉学科，各种保障信息安全的技术也不断推陈出新。我们应大力培养信息安全的专业人才，对从业人员进行技术、职业道德、法律等全方位的教育。同时，要普及信息安全教育，增强国民的信息安全意识，提高全民的信息化知识水平和防范意识。

面对社会对信息安全人才的迫切需求，国内已有几十所高校设立了信息安全专业，还有众多高校开设了信息安全相关的必修与选修课。为了有力地支持信息安全相关课程的教学，促进信息安全的科学研究，在机械工业出版社华章分社的精心策划与组织下，国内高校从事信息安全领域研究、教学的专家和教师共同编写了这套“高等院校信息安全专业规划教材”。这套丛书是各位作者多年教学、科研成果的结晶，其特点是理论与实践紧密结合、深入浅出、实例丰富，既包括基础知识，也反映最新科研成果与发展趋势。我深信，丛书的出版必将对信息安全知识的普及和推广、信息安全人才的培养、教学与科研产生积极影响并作出重要的贡献。

最后，作为本丛书的编委会主任，我对各位编委的努力工作、各位作者的辛勤劳动、机械工业出版社华章分社的大力支持表示衷心的感谢。

丛书编委会主任　卿斯汉

2009年6月

前言

在信息化高度发展的今天，计算机网络已经把国家的政治、军事、经济、文化教育等行业和部门紧密地联系在一起，成为社会基础设施的重要组成部分。

随着网络技术的发展，网络安全问题日趋严重。黑客利用网络漏洞对网络进行攻击、传播病毒和木马、控制他人的计算机和网络、篡改网页、破坏网络的正常运行、窃取和破坏计算机上的重要信息，严重影响了网络的健康发展。网络信息安全已成为事关国家安全、经济发展、社会稳定和军事战争成败的重大战略性课题，在维护国家利益、保障国民经济稳定有序发展、打赢未来战争中占有重要地位。

目前国内已有一批专门从事信息安全基础研究、技术开发与技术服务的研究机构与高科技企业，形成了我国信息安全产业的雏形。但由于国内信息安全技术人才相对不足，阻碍了我国信息安全事业的发展，为此，国内很多高校开设了信息安全专业，并将“网络攻防技术”作为该专业的一门主要课程。

作为一本专门针对本科生网络安全课程的教材，本书比较详细地介绍了现有的主要攻击手段和方法，剖析了系统存在的缺陷和漏洞，让网络安全防护更有针对性。在此基础上，对网络防御中常用的技术和方法进行了较为系统的分析和介绍。通过本课程的学习，学生可以了解和掌握网络攻击的手段和方法，系统掌握网络防御的基本原理和技术，熟悉网络安全管理的相关知识，为将来从事网络安全的研究、安全技术的开发和网络安全管理打下坚实的基础。

本书涉猎面广，不仅突出实用性，而且强调对技术原理的掌握。限于篇幅，书中没有涉及信息安全的重要支撑技术——密码学，如读者有兴趣，请参阅有关书籍。

本书共分15章，各章的内容既独立又有联系，主要内容如下：

第1章介绍网络安全威胁、网络攻击的分类、攻击的五个步骤，并且列出了网络攻击导致的后果，展望了网络攻击技术的主要发展趋势。

第2章从网络信息挖掘、网络扫描技术、网络拓扑探测、系统类型探测四个方面对信息收集技术进行详细的介绍。

第3章从口令的强度、存储和传输三个方面对常见的口令攻击技术和防范方法进行介绍。

第4章介绍了缓冲区溢出的相关概念、类型，详细讨论了溢出利用的基本原理及如何编写Shellcode代码。

第5章介绍恶意代码的现状、危害和发展历程，介绍几种主要的恶意代码类型，并归纳出恶意代码的攻击模型。在此基础上分析了恶意代码所使用的关键技术，详细阐述了基于主机的恶意代码防范技术和基于网络的恶意代码防范技术。

第6章介绍了Web应用的基本模型和相关概念，详细讨论了对Web应用程序的两种常见的攻击方法，并给出了相应的防范策略。

第7章介绍了嗅探器的原理及嗅探器的实现过程，并列出了一些编写方法，最后介绍了嗅探器的检测与防范方法。

第8章按照TCP/IP协议的层次，对假消息攻击进行分类，并详细介绍每一层对应的攻击技术。

第9章详细地介绍了拒绝服务攻击的概念、成因和原理。

第10章主要探讨了网络安全模型、网络安全的评估标准、安全策略、网络的纵深防御、安全检测、安全响应、灾难恢复和网络安全管理等方面。

第11章介绍了访问控制的原理、模型及实现，详细介绍了操作系统访问控制机制和网络访问控制机制。

第12章重点介绍了目前广泛采用的防火墙技术，包括它们所能提供的安全特性与优缺点。

第13章介绍了与防火墙完全不同的一种网络安全技术——入侵检测，讨论了入侵检测系统的模型、技术，并介绍了几种开源的网络入侵检测软件。

第14章介绍了蜜罐技术的基本概念和技术原理，并详细讨论了两种典型的蜜罐应用实例。

第15章介绍了内网安全管理的内容及目标，并讨论了终端的接入控制、非法外联监控、移动存储介质等安全管理内容。

本书由解放军信息工程大学信息工程学院网络工程系组织编写，具体分工如下：第1、10章由吴灏编写；第2、3章由曹宇、胡雪丽编写；第4章由魏强编写；第5章由王亚琪编写；第6章由奚琪编写；第7、8章由彭建山编写；第9章由耿俊燕编写；第11章由尹中旭编写；第12、13章由朱俊虎编写；第14章由曾勇军、徐长征编写；第15章由吴灏、邵峥嵘编写。全书由吴灏教授统稿，胡雪丽协助。此外，王高尚、曹琰、崔颖、任栋、刘国栋、朱磊、李正也参与了本书的编写工作。

由于网络攻防技术的快速发展，再加之作者水平有限，疏漏和错误之处在所难免，恳请读者和有关专家不吝赐教。

编　者

2009年6月

教学和阅读建议

本课程的先修课程为“操作系统”、“计算机网络”、“程序设计”、“网络协议分析”。本课程建议学时数为40（38学时授课，2学时复习考试），各章的教学内容可作如下安排。

第1章　网络攻击技术概述（2学时）

教学内容：

- 网络安全的起因。
- 网络面临的主要威胁。
- 网络攻击的分类。
- 网络攻击的一般步骤。
- 网络攻击的后果及网络攻击技术发展趋势。

考核要求：

- 通过课堂讲解，学生应能比较全面地了解网络面临的威胁和网络安全现状，了解产生网络安全问题的深层次原因、网络攻击的分类，掌握网络攻击的一般步骤，通过网络安全事件实例讲解，激发学生对本课程的学习兴趣。

第2章　信息收集技术（4学时）

教学内容：

- 信息收集概述。
- 信息收集的方法和技术。

考核要求：

- 通过课堂讲解，学生应能理解信息收集的作用，掌握利用公开服务收集信息的主要方法。

第3章　口令攻击（2学时）

教学内容：

- 身份认证与口令。
- 口令的安全性分析。
- 口令攻击的方法与种类。
- 口令攻击的防范。

考核要求：

- 通过课堂讲解，学生应了解口令攻击的方法与类别，掌握Windows系统的口令验证机制，熟悉常用的口令破解工具和口令攻击方法，掌握口令攻击的防范技术和方法。

第4章　缓冲区溢出攻击（4学时）

教学内容：

- 缓冲区溢出概述。
- 缓冲区溢出分类与原理。
- Shellcode的编写。

考核要求：

- 通过课堂讲解，学生应能掌握缓冲区溢出的相关概念，了解缓冲区溢出的危害，掌握Windows系统的堆栈结构，掌握栈溢出、堆溢出、整型溢出、格式化字符串溢出及文件流溢出的主要原因，了解通过缓冲区溢出实施攻击的主要机理。

第5章　恶意代码（4学时）

教学内容：

- 恶意代码概述。
- 恶意代码的关键技术。
- 恶意代码的防范技术。

考核要求：

- 通过课堂讲解，学生应能了解恶意代码的定义，了解恶意代码的关键技术，掌握一定的防范技术和手段。

第6章　Web应用程序攻击（2学时）

教学内容：

- Web应用程序攻击概述。
- 不同种类Web应用程序的攻击。
- Web应用程序攻击的安全防范。

考核要求：

- 通过课堂讲解，学生应能了解Web应用程序所面临的威胁，掌握脚本注入攻击、跨站攻击等攻击方法，掌握Web应用程序攻击的主要防范技术。

第7章　网络嗅探（2学时）

教学内容：

- 嗅探技术概述。
- 嗅探的原理与实现。
- 嗅探的检测与防范。

考核要求：

- 通过课堂讲解，学生应能掌握嗅探的基本原理及Windows下嗅探器的实现方法，掌握嗅探的检测与防范技术。

第8章　假消息攻击（2学时）

教学内容：

- 假消息攻击概述。
- 假消息攻击的分类。
- 假消息攻击的原理。

考核要求：

- 通过课堂讲解，学生应能了解协议的设计缺陷，掌握假消息攻击手段的原理。

第9章　拒绝服务攻击（2学时）

教学内容：

- 拒绝服务攻击概述。
- 拒绝服务攻击的成因与分类。
- 分布式拒绝服务攻击技术原理与防范技术。

考核要求：

- 通过课堂讲解，学生应能了解拒绝服务攻击的成因，掌握拒绝服务攻击的危害，掌握分布式拒绝服务攻击技术的原理与防范技术。

第10章　网络防御概述（2学时）

教学内容：

- 网络安全模型。
- 网络安全评估标准和安全策略。
- 网络安全检测技术。

考核要求：

- 通过课堂讲解，学生应能掌握网络安全模型，掌握安全策略及评估标准，掌握网络安全的主要检测技术。

第11章　访问控制机制（2学时）

教学内容：

- 访问控制机制概述。
- 操作系统访问控制相关机制。
- 网络访问控制相关机制。

考核要求：

- 通过课堂讲解，学生应能掌握访问控制的概念、访问控制模型及网络访问控制的机制和方法。

第12章　防火墙（4学时）

教学内容：

- 防火墙概述。
- 常用防火墙技术。

考核要求：

- 通过课堂讲解和讨论，学生应能掌握防火墙的相关概念，掌握常用防火墙技术和体系结构。

第13章　入侵检测（2学时）

教学内容：

- 入侵检测系统概述。
- 入侵检测技术。
- Snort入侵检测软件分析。

考核要求：

- 通过课堂讲解，学生应能了解入侵检测的作用和意义，掌握入侵检测的主要技术，了解入侵检测的发展趋势。

第14章　蜜罐技术（2学时）

教学内容：

- 蜜罐技术概述。
- 蜜罐技术原理。

考核要求：

- 通过课堂讲解，学生应能了解蜜罐技术概念，掌握蜜罐技术的原理及分类。

第15章　内网安全管理（2学时）

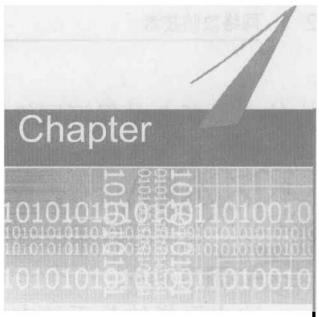
教学内容：

- 内网安全管理目标。
- 内网安全管理的内容。
- 移动介质安全管理。

考核要求：

- 通过课堂讲解和讨论，学生应能了解安全管理的目标和管理内容，掌握终端安全检测、物理隔离监控、移动介质安全管理等技术。

目录



第1章 网络攻击技术概述

网络攻击也称为网络入侵（network intrusion），指的是网络系统内部发生的任何违反安全策略的事件，这些事件可能来自系统外部，也可能来自系统内部；可能是故意的，也可能是无意偶发的。

1.1 网络面临的安全威胁

网络安全威胁是网络系统所面临的已发生过的安全事件或潜在的安全事件的负面影响。网络安全威胁的种类很多，对计算机网络的影响各不相同，产生的原因也各不相同。

网络安全威胁主要来自以下几个方面：

1. 协议缺陷

TCP/IP作为Internet使用的标准协议集，是攻击者实施网络攻击的重点目标。TCP/IP协议簇是目前使用最为广泛的网络互连协议，但TCP/IP协议簇本身存在着一些安全问题。TCP/IP协议设计时面向的是封闭、专用的网络环境，首要解决的是网络互连、缺乏认证等基本的安全特性，否则会带来许多安全威胁。例如，中间人攻击所利用的就是通信双方、网络设备之间没有认证的缺点，即使有中间人插入，通信双方也不会察觉。TCP/IP协议的缺陷主要表现在：缺乏有效的身份鉴别机制，通信双方无法可靠识别身份；缺乏有效的信息加密机制，通信内容容易被第三方窃取。

2. 软件漏洞

在操作系统和应用系统中，由于系统越来越复杂，代码的规模越来越庞大，加之软件开发者开发软件时的疏忽，或者是编程者安全知识的局限，几乎可以肯定地说所有的软件都存在实现的缺陷和漏洞。

几乎所有引起身份被盗、网络中断、数据丢失与网站崩溃的安全破坏都有一个根本的原因，即软件代码本身编写粗糙。

3. 策略弱点

网络系统的安全策略能够极大地提高系统的安全性。例如，访问控制是网络安全防范和保护的主要策略，

它的主要任务是保证网络资源不被非法使用和非法访问。它也是维护网络系统安全、保护网络资源的重要手段，可以说是保证网络安全的核心策略之一。

网络系统的安全程度应该与安全策略一致。如果安全策略设计时考虑不周，或实现时选择不当，就会造成系统存在安全漏洞，从而遭受攻击。

4. 恶意利用

这主要指的是系统内部别有用心的人利用网络系统中的合法身份，进行违规操作或恶意破坏。堡垒最容易从内部被攻破，来自于内部的攻击可谓防不胜防，危害性当然也最大。

5. 硬件漏洞

虽然硬件漏洞比较少，但BIOS中的漏洞、CPU中的缺陷也可能造成更为严重的安全问题，修复的难度比软件漏洞要大得多。

6. 管理不当

指因管理制度不到位、技术手段使用不当也会带来各种安全隐患。

1.2　网络攻击的分类

网络攻击的方法非常灵活。从攻击的目的来看，有拒绝服务攻击（DoS/DDoS）、获取系统权限的攻击、获取敏感信息的攻击；从攻击的切入点来看，有缓冲区溢出攻击、系统设置漏洞的攻击等；从攻击的纵向实施过程来看，有获取初级权限攻击、提升最高权限的攻击、后门攻击、跳板攻击等；从攻击的实施对象来看，有对各种操作系统的攻击、对网络设备的攻击、对特定应用系统的攻击等。因此，很难用一种统一的模式对各种攻击手段进行分类。

本书按照攻击者与被攻击者的物理位置关系进行分类，以便读者明晰攻击的思路。按照这种分类方法，可以将攻击分为物理攻击（local attack）、主动攻击（server-side attack）、被动攻击（client-side attack）和中间人攻击（man-in-middle attack）。

1. 物理攻击

物理攻击指的是攻击者通过实际接触被攻击的主机而发起的一类攻击。

攻击者通过接触被攻击的计算机，既可以直接窃取或破坏被攻击者的账号、密码和硬盘内的各类信息，也可以在被攻击主机内植入特定的程序，如植入木马程序，以便于远程控制该机器。图1-1是物理攻击的示意图。

图1-1　物理攻击示意图

物理攻击比较难以防范，因为攻击者往往是来自能够接触到物理设备的用户，并且对于目标网络的防护也非常熟悉。

2. 主动攻击

主动攻击指的是攻击者对被攻击主机所运行的开放网络服务（Web、FTP、Telnet等）实施攻击。攻击者通过网络将虚假信息、垃圾数据、计算机病毒或木马程序等置入系统内部，破坏信息的真实性和完整性，或者窃取被攻击主机中的信息，如图1-2所示。

主动攻击的方法主要有漏洞扫描、远程口令猜解、远程控制、信息窃取、信息篡改、拒绝服务攻击、资源利用、欺骗等。

3. 被动攻击

被动攻击指的是攻击者对被攻击主机的客户程序实施攻击，如攻击浏览器、邮件接收程序、文字处理程序等。在被动攻击中，部分攻击行为需要被攻击者的“配合”才能完成，比如阅读夹带有木马的邮件，浏览挂有木马的网站等。被动攻击如图1-3所示。

图1-2 主动攻击示意图

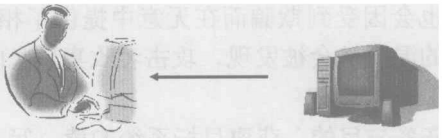


图1-3 被动攻击示意图

需要说明的是，主动攻击和被动攻击的界定一直存在争议，主要体现在邮件攻击和网站“挂马”攻击上。有人认为这两种攻击都属于主动攻击，有人则认为这两种攻击均属于被动攻击。本书倾向于后者，主要是因为这两种攻击过程的完成需要被攻击者的操作（被攻击者查看邮件或网页）才能完成整个攻击过程。

4. 中间人攻击

中间人攻击指的是攻击者处于被攻击主机的某个网络会话的中间人位置，进行数据窃取、破坏或篡改。

这种攻击模式是通过各种技术手段将受入侵者控制的一台计算机虚拟地放置在网络连接中的两台通信计算机之间，这台计算机称为“中间人”，如图1-4所示。入侵者使用这台计算机模拟原始通信的一方或双方，使“中间人”能够与原始计算机建立活动连接并能够读取或修改传递的信息，并且使两台原始计算机用户误认为他们是在互相通信。通常，这种“拦截数据－修改数据－发送数据”的过程被称为“会话劫持”。

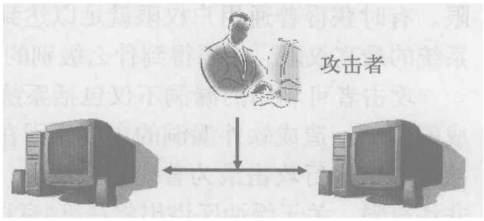


图1-4 中间人攻击示意图

1.3 网络攻击的步骤

通常，一个完整的、有预谋的攻击涉及信息收集、权限获取、安装后门、扩大影响和消除痕迹5个阶段。下面就各个阶段攻击者的目的、主要方法、技术手段进行简要介绍。

1. 信息收集

任务与目的：尽可能多地收集目标的相关信息，为后续的“精确”攻击打下基础。

这一阶段收集的信息包括：网络信息（域名、IP地址、网络拓扑）、系统信息（操作系统版本、开放的各种网络服务版本）、用户信息（用户标识、组标识、共享资源、邮件账号、即时通信软件账号）等。

主要方法：利用公开信息服务，主机扫描与端口扫描，操作系统探测与应用程序类型识别等。

信息收集是耗时最长的阶段，有时可能会持续几个星期甚至几个月。除了上述对目标网络的非入侵性扫描探测之外，攻击者还会利用各种渠道尽可能多地了解攻击目标的类型和工作模式，包括：

- 互联网搜索。
- 社会工程学。
- 垃圾数据搜寻。
- 域名管理/搜索服务。

由于这些活动处于搜索阶段，因此很难防范。由于很多公司的信息很容易在网络上找到，

员工也会因受到欺骗而在无意中提供了相应的信息，随着时间的推移，公司的组织结构以及潜在的漏洞就会被发现，攻击者收集信息的目的就达到了。

2. 权限获取

任务与目的：获取目标系统的读、写、执行等权限。

与超级用户相比，普通用户账号的安全防范可能会弱一些。得到普通用户账号会得到对目标中某些资源的访问权限，比如对特定目录的读写；得到普通用户权限为进一步得到超级用户权限提供了更多可用的技术手段。

得到超级用户权限是攻击者在单个系统中的终极目标，因为得到超级用户权限就意味着对目标系统的完全控制，包括对所有资源的使用以及所有文件的读、写和执行等权限。

主要方法：综合使用信息收集阶段得到的各种信息，利用口令猜测、系统漏洞或者特洛伊木马对目标实施攻击。

入侵性攻击往往要利用收集到的信息，找到其系统漏洞，然后利用该漏洞获取一定的权限。有时获得普通用户权限就足以达到修改主页等目的，但要更进行深入的攻击则需要获得系统的最高权限。需要得到什么级别的权限取决于攻击者的目的。

攻击者可利用的漏洞不仅包括系统软件设计上的安全漏洞，还包括因管理配置不当而造成的漏洞。造成软件漏洞的主要原因在于编写该软件的程序员缺乏安全编程的知识。利用缓冲区溢出进行攻击最为普遍，据统计，80%以上成功的攻击都是利用缓冲区溢出漏洞来获得非法权限。关于缓冲区溢出将在第4章进行详细讨论。

无论是作为一名攻击者还是一名网络管理员，都需要掌握尽可能多的系统漏洞。攻击者需要用它来完成攻击，而管理员则需要根据不同的漏洞采取不同的防御措施。可以到诸如Securityfocus（www.securityfocus.com）、Rootshell（www.rootshell.com）、Packetstorm（www.packetstorm.securify.com）等网站上了解最新、最多的漏洞信息。

3. 安装后门

一般攻击者都会在攻入系统后反复地进入该系统。为了下次能够方便地进入系统，攻击者常会留下一个后门。

任务与目的：在目标系统中安装后门程序，以更加方便、更加隐蔽的方式对目标系统进行操控。

主要方法：利用各种后门程序以及特洛伊木马。

4. 扩大影响

任务与目的：以目标系统为“跳板”，对目标所属网络的其他主机进行攻击，最大程度地扩大攻击的影响。

如果所攻击的主机处于某个局域网，则攻击者就能很容易地利用内部网络环境和各种手段在局域网内扩大其影响。由于内部网的攻击避开了防火墙、NAT等网络安全工具的防范，因而更容易实施，也更容易得手。

扩大影响是指攻击者将网络内部的一台机器作为中转点而进一步攻击网络上其他机器的过程。它使用的技术手段涵盖了远程攻击的所有攻击方式，而且由于是在局域网内部，因此其攻击手段也更为丰富、有效。嗅探技术和假消息攻击均为有效的扩大影响的攻击方法。

5. 消除痕迹

任务与目的：清除攻击的痕迹，以尽可能长久地对目标进行控制，并防止被识别、追踪。

这一阶段是攻击者打扫战场的阶段，其目的是消除一切攻击的痕迹，尽量做到使管理员无法察觉系统已被入侵，否则至少也要做到使管理员无法找到攻击的发源地。