HZ BOOKS
华章教育

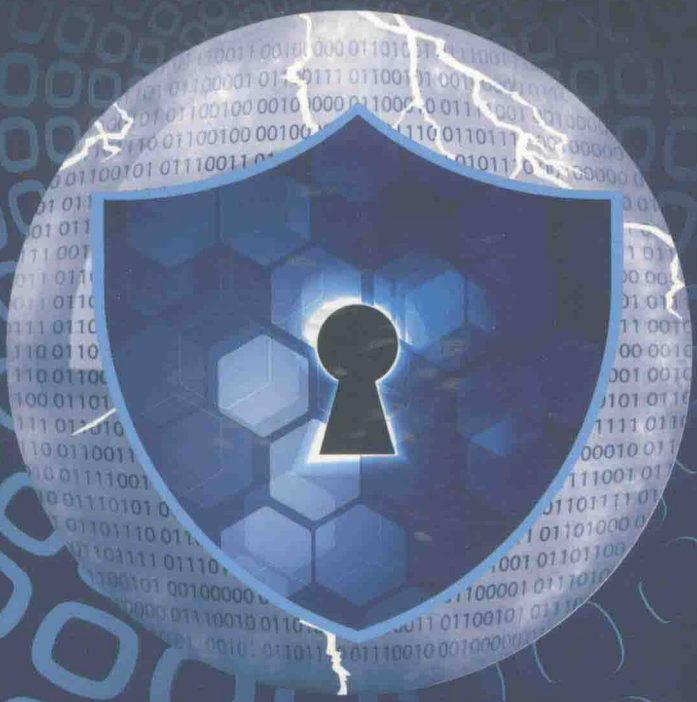
网络空间安全学科规划教材

第2版

网络攻防技术

Network Security: Attack and Defense

朱俊虎◎主编　　王清贤◎主审



机械工业出版社
China Machine Press

网络空间安全学科规划教材

第2版

网络攻防技术

Network Security: Attack and Defense

朱俊虎◎主编　王清贤◎主审

奚　琪 张连成 周天阳 曹　琰 颜学雄
彭建山 邱　菡 胡雪丽 尹中旭 秦艳锋 ◎参编

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

网络攻防技术 / 朱俊虎主编 . —2 版 . —北京：机械工业出版社，2019.1
（网络空间安全学科规划教材）

ISBN 978-7-111-61936-9

I. 网… II. 朱… III. 网络安全 - 教材 IV. TN915.08

中国版本图书馆 CIP 数据核字（2019）第 030496 号

本书系统地介绍了网络攻击与防御技术。全书从内容上分为两大部分：第一部分从网络安全面临的不同威胁入手，详细介绍信息收集、口令攻击、软件漏洞、Web 应用攻击、恶意代码、假消息攻击、拒绝服务攻击等多种攻击技术，并结合实例进行深入的分析；第二部分从网络防御的模型入手，详细介绍访问控制机制、防火墙、网络安全监控、攻击追踪与溯源等安全防御的技术与方法，并从实际应用角度分析它们的优势与不足。

本书体系合理，概念清晰，内容详尽实用，结合丰富的实例剖析了技术的细节与实质。本书既注重讨论当前广泛应用的成熟理论与技术，也注重介绍领域最新的研究进展与趋势。书中各章均附有习题，方便讲授和开展自学。

本书可作为高等学校网络空间安全、信息安全等专业相关课程的教材，也可作为计算机科学与技术、网络工程、通信工程等专业相关课程的教学参考书，还可作为信息技术人员、网络安全技术人员的参考用书。

出版发行：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：朱　劼　　责任校对：李秋荣
印　　刷：北京诚信伟业印刷有限公司　　版　　次：2019 年 3 月第 2 版第 1 次印刷
开　　本：185mm × 260mm　1/16　　印　　张：17.75
书　　号：ISBN 978-7-111-61936-9　　定　　价：49.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

第 2 版前言

随着信息技术的高速发展，以互联网为代表的计算机网络已经成为全球化的信息共享与交互平台，深刻地影响着各国政治、经济、军事以及人们日常工作和生活的各个方面。虽然网络安全已经得到普遍重视，但新的网络威胁依然层出不穷。2010 年，震网病毒广为传播并使伊朗核设施遭到攻击；2013 年披露的“棱镜”计划揭开了“网络监听窃密”的冰山一角；2016 年，黑客组织“影子经纪人”（The Shadow Brokers）公开拍卖盗取的“网络攻击工具集”；2017 年，勒索病毒 Wannacry 在全球范围内广泛传播，感染了 150 多个国家的近 20 万台计算机。这些案例使大众深刻感受到网络威胁造成的影响。

增强网络安全意识、掌握网络安全技能是应对网络威胁的必然要求。网络攻击与网络防御本质上是攻防双方围绕对网络脆弱性的认知而进行的博弈。网络攻击技术既是网络防御技术发展的动因，也是网络防御技术的防范对象。因此，要掌握网络安全技能，就应当系统全面地学习网络攻击与网络防御技术。

全书共分 13 章，按照先介绍“攻击技术”后介绍“防御技术”的顺序进行组织，第 1 章至第 8 章讨论攻击技术，第 9 章至第 13 章讨论防御技术。“攻击技术”部分在介绍各种攻击的危害和原理的基础上，进一步分析该攻击的成因以及针对该攻击技术的防御方法；“防御技术”部分则在介绍防御原理、功能的基础上，进一步分析每种防御技术的优势与不足。全书各章的具体内容如下：

- 第 1 章介绍网络安全威胁、网络攻击的类型，分析攻击的主要步骤及各步骤所应用的攻击技术，并对网络攻击技术的发展趋势进行展望。
- 第 2 章从公开信息收集、网络扫描、漏洞扫描、网络拓扑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 章介绍软件漏洞的相关概念、主要类型及触发原理，以溢出类漏洞为例讨论漏洞利用的一般方法，并介绍当前广为应用的四种漏洞利用保护机制。
- 第 5 章介绍 Web 应用的基本模型和相关概念，详细讨论 XSS 攻击、SQL 注入攻击和 HTTP 会话攻击三类典型的 Web 应用攻击技术及其防范方法。
- 第 6 章介绍恶意代码的发展历程、基本分类和攻击模型，分析恶意代码使用的关键技术，讨论主机恶意代码防范技术和网络恶意代码防范技术。
- 第 7 章介绍假消息攻击的基本概念，在介绍网络嗅探技术的基础上，按照由低至高的协议层顺序，详细讨论各协议层假消息攻击的方法以及相应的防范措施。
- 第 8 章介绍拒绝服务攻击的概念、危害，重点讨论各种拒绝服务攻击破坏服务的基

本原理和攻击效能放大的主要方法，并介绍当前检测与防范此类攻击的主要思路与方法。

- 第 9 章主要从网络安全模型、网络安全管理和网络防御新技术三个方面探讨网络安全防御的主要内容与技术发展趋势。
- 第 10 章介绍访问控制的原理、模型及实现，重点讨论 Windows 操作系统的访问控制机制。
- 第 11 章介绍防火墙的基本概念和主要功能，重点讨论目前广泛采用的各种防火墙技术，包括它们所能提供的安全特性与优缺点。
- 第 12 章介绍网络安全监控的概念与原理，在统一的网络安全监控的概念框架下，重点介绍入侵检测、蜜罐、沙箱等常见的网络安全监控技术。
- 第 13 章介绍网络攻击追踪溯源的基本概念及作用，重点分析追踪的溯源典型技术。

战略支援部队信息工程大学网络空间安全学院组织了全书的编写工作，朱俊虎担任主编，奚琪、张连成、周天阳、曹琰、颜学雄、彭建山、邱菡、胡雪丽、尹中旭、秦艳锋等参与编写。本书的第 1、8 章由朱俊虎、秦艳锋编写，第 2、6 章由奚琪编写，第 3 章由胡雪丽编写，第 4 章由曹琰编写，第 5 章由颜学雄编写，第 7 章由彭建山编写，第 9、13 章由张连成编写，第 10 章由尹中旭编写，第 11 章由邱菡编写，第 12 章由周天阳编写。全书由朱俊虎进行统稿，秦艳锋、奚琪、颜学雄同时参与了部分审校工作。王清贤教授作为本书的主审，对全书内容进行了审定。

本书第 1 版是由吴灏教授组织编写的，第 2 版延续了第 1 版的撰写思路和主体结构，在此对第 1 版所有编写人员表示诚挚的谢意。在本书的统稿过程中，葛潇月、李静轩、刘自勉、胡泰然等为提高本书的质量进行了内容与文字的校对，衷心感谢他们为本书做出的贡献。机械工业出版社朱劼编辑为本书付梓做了大量专业细致的工作，在此一并表示感谢。

网络攻防技术发展迅猛，限于作者水平，书中错误和不足之处在所难免，恳请读者批评指正。

作　者

2018 年 9 月

第 1 版前言

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，涵盖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 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

目录

第 2 版前言
第 1 版前言

第 1 章　网络攻击概述 …… 1
1.1　网络安全威胁 …… 1
1.1.1　网络安全威胁事件 …… 1
1.1.2　网络安全威胁的成因 …… 2
1.2　网络攻击技术 …… 4
1.2.1　网络攻击的分类 …… 4
1.2.2　网络攻击的步骤与方法 …… 6
1.3　网络攻击的发展趋势 …… 8
1.4　本章小结 …… 9
1.5　习题 …… 9
第 2 章　信息收集技术 …… 10
2.1　信息收集概述 …… 10
2.1.1　信息收集的内容 …… 10
2.1.2　信息收集的方法 …… 11
2.2　公开信息收集 …… 11
2.2.1　利用 Web 服务 …… 11
2.2.2　利用搜索引擎服务 …… 12
2.2.3　利用 WhoIs 服务 …… 14
2.2.4　利用 DNS 域名服务 …… 14
2.2.5　公开信息收集方法的应用 …… 15
2.3　网络扫描 …… 17
2.3.1　主机扫描 …… 18
2.3.2　端口扫描 …… 20
2.3.3　系统类型扫描 …… 24
2.4　漏洞扫描 …… 27
2.4.1　漏洞扫描的概念 …… 27
2.4.2　漏洞扫描的分类 …… 27
2.4.3　漏洞扫描器的组成 …… 28
2.5　网络拓扑探测 …… 29
2.5.1　拓扑探测 …… 29
2.5.2　网络设备识别 …… 31
2.5.3　网络实体 IP 地理位置定位 …… 33
2.6　本章小结 …… 34
2.7　习题 …… 34
第 3 章　口令攻击 …… 35
3.1　概述 …… 35
3.1.1　口令和身份认证 …… 35
3.1.2　口令攻击的分类 …… 36
3.2　针对口令强度的攻击 …… 37
3.2.1　强口令与弱口令 …… 37
3.2.2　针对口令强度的攻击方法 …… 38
3.2.3　Windows 系统远程口令猜解 …… 41
3.3　针对口令存储的攻击 …… 44
3.3.1　针对口令存储的攻击方法 …… 44
3.3.2　Windows 系统账号口令攻击 …… 45
3.4　针对口令传输的攻击 …… 48
3.4.1　口令嗅探 …… 48
3.4.2　键盘记录 …… 48
3.4.3　网络钓鱼 …… 49
3.4.4　重放攻击 …… 50
3.5　口令攻击的防范 …… 52
3.6　本章小结 …… 52
3.7　习题 …… 53
第 4 章　软件漏洞 …… 54
4.1　概述 …… 54
4.1.1　漏洞的概念 …… 54
4.1.2　漏洞的标准化研究 …… 55
4.2　典型的漏洞类型 …… 55

4.2.1 栈溢出 …… 55
4.2.2 堆溢出 …… 59
4.2.3 格式化串漏洞 …… 64
4.2.4 整型溢出 …… 66
4.2.5 释放再使用（UAF） …… 68
4.3 溢出漏洞利用的原理 …… 69
4.3.1 溢出攻击的基本流程 …… 69
4.3.2 溢出利用的关键技术 …… 70
4.4 漏洞利用保护机制 …… 74
4.4.1 GS 编译保护机制 …… 74
4.4.2 SafeSEH 机制 …… 75
4.4.3 DEP 机制 …… 75
4.4.4 ASLR 机制 …… 76
4.5 本章小结 …… 76
4.6 习题 …… 77
第 5 章 Web 应用攻击 …… 78
5.1 概述 …… 78
5.1.1 Web 应用的基本原理 …… 78
5.1.2 Web 应用攻击的类型 …… 84
5.2 XSS 攻击 …… 85
5.2.1 XSS 攻击的基本原理 …… 85
5.2.2 XSS 攻击的主要类型 …… 87
5.2.3 XSS 漏洞的利用方式分析 …… 87
5.2.4 XSS 攻击的防范措施 …… 88
5.3 SQL 注入攻击 …… 89
5.3.1 SQL 注入攻击的基本原理 …… 89
5.3.2 SQL 注入的利用方式分析 …… 91
5.3.3 SQL 注入攻击的类型 …… 92
5.3.4 防范措施 …… 94
5.4 HTTP 会话攻击及防御 …… 95
5.4.1 HTTP 会话的基本原理 …… 95
5.4.2 HTTP 会话的示例 …… 96
5.4.3 HTTP 会话攻击 …… 98
5.4.4 CSRF 攻击 …… 98
5.4.5 防范措施 …… 100
5.5 本章小结 …… 100
5.6 习题 …… 100
第 6 章 恶意代码 …… 101
6.1 恶意代码概述 …… 101
6.1.1 恶意代码的发展历程 …… 102
6.1.2 恶意代码的定义与分类 …… 104
6.1.3 恶意代码的攻击模型 …… 106
6.2 恶意代码的关键技术 …… 107
6.2.1 恶意代码入侵技术 …… 107
6.2.2 恶意代码隐蔽技术 …… 109
6.2.3 恶意代码生存技术 …… 119
6.3 恶意代码的防范技术 …… 121
6.3.1 基于主机的恶意代码防范技术 …… 121
6.3.2 基于网络的恶意代码防范技术 …… 123
6.4 本章小结 …… 124
6.5 习题 …… 124
第 7 章 假消息攻击 …… 125
7.1 概述 …… 125
7.1.1 TCP/IP 的脆弱性 …… 125
7.1.2 假消息攻击的模式和危害 …… 126
7.2 网络嗅探 …… 127
7.2.1 网络嗅探的原理与实现 …… 127
7.2.2 网络嗅探与协议还原 …… 130
7.2.3 嗅探器的检测与防范 …… 134
7.3 ARP 欺骗攻击 …… 136
7.3.1 ARP 欺骗的原理与应用 …… 136
7.3.2 ARP 欺骗的防范 …… 138
7.4 ICMP 路由重定向攻击 …… 139
7.4.1 ICMP 路由重定向的原理 …… 139
7.4.2 ICMP 路由重定向的防范 …… 140
7.5 IP 欺骗攻击 …… 140
7.5.1 IP 欺骗与 TCP 序列号猜测 …… 140
7.5.2 IP 欺骗防范 …… 142
7.6 DNS 欺骗攻击 …… 142
7.6.1 DNS 欺骗的原理与实现 …… 142
7.6.2 DNS 欺骗的防范 …… 144
7.7 SSL 中间人攻击 …… 144
7.7.1 SSL 中间人攻击的原理与实现 …… 144
7.7.2 SSL 中间人攻击的防范 …… 145
7.8 本章小结 …… 145
7.9 习题 …… 145

第 8 章 拒绝服务攻击 …… 146
8.1 概述 …… 146
8.1.1 基本概念 …… 147
8.1.2 拒绝服务攻击的分类 …… 147
8.2 典型拒绝服务攻击技术 …… 148
8.2.1 传统的拒绝服务攻击 …… 149
8.2.2 洪泛攻击 …… 151
8.2.3 低速率拒绝服务攻击 …… 153
8.3 分布式拒绝服务攻击 …… 155
8.3.1 基于僵尸网络的分布式拒绝服务攻击 …… 155
8.3.2 分布式反射拒绝服务攻击 …… 161
8.4 拒绝服务攻击的防御 …… 163
8.4.1 拒绝服务攻击预防 …… 164
8.4.2 拒绝服务攻击检测 …… 164
8.4.3 拒绝服务攻击响应 …… 165
8.4.4 拒绝服务攻击容忍 …… 166
8.5 本章小结 …… 167
8.6 习题 …… 167
第 9 章 网络防御概述 …… 169
9.1 网络安全模型 …… 169
9.1.1 风险评估 …… 170
9.1.2 安全策略 …… 172
9.1.3 系统防护 …… 173
9.1.4 安全检测 …… 175
9.1.5 安全响应 …… 176
9.1.6 灾难恢复 …… 177
9.2 网络安全管理 …… 177
9.3 网络防御技术的发展趋势 …… 178
9.3.1 主动防御 …… 179
9.3.2 动态防御 …… 181
9.3.3 软件定义安全 …… 183
9.4 本章小结 …… 185
9.5 习题 …… 185
第 10 章 访问控制机制 …… 186
10.1 访问控制概述 …… 186
10.1.1 访问控制原理 …… 186
10.1.2 访问控制模型 …… 187
10.1.3 访问控制机制的实现 …… 190
10.2 操作系统访问控制的相关机制 …… 191
10.2.1 身份认证和授权机制 …… 191
10.2.2 访问检查机制 …… 192
10.2.3 可信通路机制 …… 194
10.2.4 对象重用机制 …… 195
10.2.5 审计机制 …… 195
10.3 UAC 机制分析 …… 196
10.3.1 权限提升提示机制 …… 196
10.3.2 强制完整性控制机制 …… 197
10.3.3 会话隔离机制 …… 198
10.3.4 UAC 机制的弱点分析 …… 198
10.4 本章小结 …… 200
10.5 习题 …… 200
第 11 章 防火墙 …… 201
11.1 防火墙概述 …… 201
11.1.1 防火墙的定义 …… 201
11.1.2 防火墙的安全策略 …… 202
11.1.3 防火墙的功能 …… 202
11.1.4 防火墙的不足 …… 203
11.1.5 防火墙技术和产品的发展历程 …… 204
11.2 常用的防火墙技术 …… 206
11.2.1 包过滤 …… 206
11.2.2 状态检测 …… 209
11.2.3 应用代理 …… 211
11.2.4 NAT 代理 …… 212
11.2.5 流量识别技术 …… 213
11.3 常用的防火墙类型 …… 214
11.3.1 主机防火墙 …… 214
11.3.2 网络防火墙 …… 216
11.3.3 Web 应用防火墙 …… 218
11.4 本章小结 …… 219
11.5 习题 …… 219
第 12 章 网络安全监控 …… 221
12.1 网络安全监控概述 …… 221
12.1.1 网络安全监控概念的内涵 …… 221
12.1.2 网络安全监控原理的特征 …… 222
12.1.3 网络安全监控技术的原理 …… 224
12.1.4 网络安全监控系统的部署 …… 229
12.2 入侵检测 …… 230
12.2.1 入侵检测的定义 …… 230

12.2.2 入侵检测系统的分类 …… 231
12.2.3 入侵检测系统模型 …… 232
12.2.4 开源入侵检测系统 Snort …… 233
12.3 蜜罐 …… 234
12.3.1 蜜罐的定义 …… 234
12.3.2 蜜罐的分类 …… 235
12.3.3 蜜罐技术的原理 …… 237
12.3.4 蜜罐实例 …… 238
12.4 沙箱 …… 241
12.4.1 沙箱的定义 …… 241
12.4.2 沙箱的分类 …… 242
12.4.3 沙箱的关键技术 …… 243
12.4.4 开源沙箱系统 Cuckoo …… 245
12.5 本章小结 …… 247
12.6 习题 …… 247
第 13 章 追踪溯源 …… 248
13.1 追踪溯源概述 …… 248
13.1.1 网络攻击追踪溯源的基本概念 …… 248
13.1.2 网络攻击追踪溯源的目标层次 …… 249
13.1.3 网络攻击追踪溯源的典型场景 …… 251
13.2 追踪溯源面临的挑战 …… 252
13.2.1 跳板对追踪溯源的挑战 …… 252
13.2.2 匿名通信系统对追踪溯源的挑战 …… 253
13.2.3 追踪溯源面临的其他挑战 …… 255
13.3 追踪溯源的典型技术 …… 256
13.3.1 定位伪造地址的 IP 追踪技术 …… 256
13.3.2 跳板攻击溯源技术 …… 259
13.3.3 针对匿名通信系统的追踪溯源技术 …… 264
13.4 追踪溯源技术的发展趋势 …… 264
13.5 本章小结 …… 266
13.6 习题 …… 266
缩略语表 …… 267
参考文献 …… 270

Chapter 1

第1章 网络攻击概述

网络攻击技术与网络防御技术的对抗是网络安全的永恒主题。网络攻击与网络防御本质上是攻防双方围绕对网络脆弱性的认知而进行的博弈：攻击方发掘网络和信息系统的脆弱性，不断发展攻击技术来实施攻击；防御方分析攻击的工作原理和作用机制，不断构筑新的安全防御体系。网络攻击技术既是网络防御技术发展的动因，也是网络防御技术的防范对象。要掌握网络防御技术与方法，应对网络攻击，应当从了解网络攻击开始。

本章将对网络攻击进行初步介绍。首先，介绍当前网络安全威胁的现状，并从客观和主观两个方面分析网络安全威胁的成因；接下来，介绍网络攻击技术的分类，并分析、归纳网络攻击各阶段所运用的网络攻击技术；最后，对网络攻击技术的发展进行综述。

1.1 网络安全威胁

网络安全威胁的内涵可从广义网络安全威胁以及狭义网络安全威胁来描述。广义的网络安全威胁泛指任何潜在的对网络安全造成不良影响的事件，包括自然灾害、非恶意的人为损害以及网络攻击等。狭义的网络安全威胁则指各类网络攻击行为。

1.1.1 网络安全威胁事件

自网络诞生以来，各类安全威胁事件就层出不穷。下面列举几个影响较大的网络安全威胁事件：20 世纪 80 年代，凯文·米特尼克（Kevin Mitnick）入侵多家公司的内部网络，窃取了大量信息资产和源代码，造成数百万美元的损失，网络安全由此开始引起广泛关注；1988 年，Morris 蠕虫病毒（莫里斯蠕虫）在互联网上传播，感染了约 6000 台计算机，造成数千万美元的损失；1995 年，俄罗斯黑客弗拉季米尔·列宁（Vladimir Levin）通过入侵美国花旗银行获利，成为第一个入侵金融信息系统而获利的黑客；1996 年，纽约市互联网服务提供商成为首个分布式拒绝服务攻击的受害者，造成至少 6000 名用户无法正常收取邮件；1998 年，以

SQL 注入为代表的 Web 脚本攻击方式开始出现，并迅速成为互联网安全的最大威胁之一；1999 年起，基于 IRC（Internet Relay Chat，互联网中继聊天）的僵尸网络开始大量出现，为分布式拒绝服务攻击提供了前沿阵地；1999 年，梅丽莎病毒破坏了世界上 300 多家公司的计算机系统，造成近 4 亿美元的损失，成为首个具有全球破坏力的病毒；2000 年，包括雅虎、eBay 和亚马逊在内的大型网站遭受分布式拒绝服务攻击；2002 年，全球根域名服务器遭受分布式拒绝服务攻击，导致 13 台根域名服务器中的 9 台瘫痪；2006 年，美国空军提出 APT（Advanced Persistent Threat，高级持续性威胁）的概念，专指针对政府、军队、公司、组织的长期而复杂的网络攻击，其后大量 APT 攻击事件报告被发布；2007 年，俄罗斯黑客成功劫持 Windows Update 服务器；2010 年，针对伊朗核设施的震网病毒（Stuxnet）被检测并曝光，成为首个被公开披露的武器级网络攻击病毒，此后，火焰（Flame）、Duqu 等一批设计精巧、功能复杂的武器级恶意代码也陆续被曝光；2013 年，前美国中央情报局职员爱德华·斯诺登（Edward Snowden）披露了美国国家安全局的“棱镜”监听项目，公开了大量针对实时通信和网络存储的监听窃密技术与计划；2016 年 9 月，俄罗斯黑客组织“奇幻熊”（Fancy Bear）入侵了世界反兴奋剂组织数据库，公布了近百名因不同原因长期服用兴奋剂的运动员名单；自 2016 年 8 月开始，黑客组织“影子经纪人”（The Shadow Broker）陆续以多种形式在互联网公开拍卖据称来自美国国家安全局的网络攻击工具集，公开的部分资料显示这些工具集包含了大量针对路由设备、安全设备、Windows 操作系统等多个平台的零日工具（Zero-day Exploits）、攻击辅助工具和恶意代码；2017 年 5 月，勒索病毒 Wannacry 在全球范围内广泛传播，感染了 150 多个国家的近 20 万台计算机。

对比网络安全威胁发展的历史和互联网发展的历史，可以发现网络安全问题伴随着互联网的出现而出现，并且随互联网的发展而发展。在互联网日益壮大并深刻影响普通人日常生活的时候，网络安全威胁的程度也越发严重，影响范围日趋扩大。

1.1.2　网络安全威胁的成因

造成目前网络安全威胁现状的原因非常复杂，这些原因大致可归结为技术因素和人为因素两个方面。

（1）技术因素

网络安全技术的发展速度与网络技术的发展速度不相适应是导致网络安全问题层出不穷的主要原因之一。网络通信技术在发展之初就定义了清晰明确的 OSI 参考模型，但该模型并未考虑网络通信和网络设备的安全性。随着网络攻击形态的不断演变，学术界和产业界不断对现有网络技术进行安全性修补，设计开发了大量的网络安全协议、技术与设备。总体上，网络安全仍缺乏一个定义良好的通用设计过程，网络协议、软硬件系统均缺乏有效安全保证。具体来看，造成当前网络安全威胁现状的技术因素主要来自以下几个方面。

- **协议缺陷**

以 TCP（Transmission Control Protocol，传输控制协议）和 IP（Internet Protocol，网际协议）为核心的 TCP/IP 协议簇是互联网使用的标准协议集，也是攻击者开发攻击方法时的重点研究对象。TCP/IP 设计时面向的是封闭专用的网络环境，重点解决网络互联的问题，缺乏认证、加密等基本的安全特性。因此，TCP/IP 的弱点带来诸多安全威胁，如 IP 欺骗攻击就是由于通信的双方没有认证，导致攻击者可以较容易地假冒合法用户的身份而造成的。总结来说，TCP/IP 的安全缺陷主要有：①缺乏有效的身份鉴别机制，通信双方无法可靠地识别身份；②缺乏有效的信息加密机制，通信内容容易被第三方窃取。

尽管已经对 TCP/IP 的安全缺陷有了较清晰的认识，研究者也开发出更为安全的 IPv6 协议，但由于兼容性、商业投入等多种原因，IPv6 协议仍很难完全取代现有的 IPv4 协议。目前，在应用领域中多采用 SSH（Secure Shell，安全外壳协议）、HTTPS（Hypertext Transfer Protocol Secure，安全超文本传输协议）等安全应用协议来增强运行在 TCP/IP 之上的应用的安全性。但需要注意的是，即便是安全协议也并不能保证没有安全缺陷。安全协议只是在协议中提供了安全性设计，并不能保证这种设计本身没有安全缺陷，也不能保证这种设计的所有实现没有安全缺陷。

- **软件漏洞**

在信息系统中，几乎所有的设计都是依赖软件来实现的。上面所说的协议实现的安全缺陷实质上就是一种软件漏洞。不仅是协议实现，在操作系统和应用系统中，所有软件都可能存在漏洞。特别是随着信息应用系统越来越复杂，代码的规模越来越庞大，不管是由于软件开发者开发软件时的疏忽，还是由于编程者安全知识的局限，均可能导致软件漏洞问题。

从技术的角度分析，形成软件漏洞的深层原因有很多。现代计算机采用的冯·诺依曼体系架构中，程序指令和程序处理的数据以混合方式存储。这会导致一旦发生缓冲区溢出问题，程序逻辑就有可能被攻击者篡改。为提高效率，软件程序采用多线程并行处理的方式。如果未合理限制多线程对同一内存区域的访问，就有可能导致机密信息的泄露。应用程序（如 Web、文字处理程序等）功能越来越丰富，结构也越来复杂，复杂的结构加之庞大的第三方代码，使得开发者很难驾驭这些应用的安全性。

- **策略弱点**

安全策略（Security Policy）是根据安全需求，对组织、系统、设备等所做的各种安全约束。常见的安全策略有公司的保密规定、主机系统的访问控制策略和安全设备的访问控制策略等。针对组织机构而言，安全策略是具体的、有针对性的。由于组织架构、安全需求等的不同，一个组织机构的安全策略通常不会与另一个组织机构的安全策略完全相同。

安全策略是安全需求的体现。通常，组织机构一旦具备一定规模，其安全需求必然会趋于复杂。如果安全策略在设计时考虑不周，或实现时对**安全机制**（Security Mechanism）选择不当，就会造成安全问题。另一方面，安全需求往往和应用需求相矛盾。很多情况下，在安全策略影响应用时，用户更愿意选择在安全策略方面做出妥协，这也更容易使安全策略出现弱点。

- **硬件漏洞**

虽然目前在 CPU、BIOS 和外围设备中发现的漏洞比较少，但其中一旦发现漏洞，其危害程度可能比一般的软件漏洞更为严重，修复的难度也更大。2018 年 1 月，谷歌公司的安全团队 Project Zero 披露了重大处理器漏洞 Meltdown（熔毁）和 Spectre（幽灵）。相关漏洞利用了芯片硬件层面执行加速机制的实现缺陷，通过侧信道攻击，可以间接地从 CPU 缓存中读取系统内存数据。漏洞存在于英特尔（Intel）x86-64 的硬件中，同时 AMD、Qualcomm 和 ARM 处理器也受到影响。对于已得到广泛应用的云计算环境来说，该漏洞的发现意味着某个虚拟机的“合法”租户或者成功入侵某个虚拟机的攻击者，都可以通过相关攻击机制获取完整的物理机的 CPU 缓存数据。该漏洞对于桌面节点同样有巨大的攻击力，攻击者可以将此漏洞与其他普通用户权限漏洞相结合，获取用户设备上的密码、登录密钥等关键敏感数据。

1965 年，Intel 创始人之一戈登·摩尔（Gordon Moore）提出了摩尔定律，对人类计算之路的快速进步做出了预言。摩尔定律指出：在价格不变的情况下，大约每隔 18 ～ 24 个月，

集成电路上可容纳的元器件的数目便会增加一倍，性能也会提升一倍。虽然摩尔定律并没有理论上的依据，但数十年硬件发展的实际数据几乎完美地与之吻合。在这个过程中，人们对硬件速度的追求在一定程度上影响了对硬件安全的关注，硬件漏洞成为安全威胁存在与发展的一个重要因素。

（2）人为因素

形成网络安全问题的另一个重要原因是攻防双方的人为因素。传统观点认为，对网络安全造成威胁的人主要是黑客（或者说是骇客，即那些躲在角落里，以破坏为乐事的人）。但这种认识显然已不符合实际网络威胁现状。通过1.1.1节所列举的重大网络安全威胁事件可以看出，对网络安全造成威胁的主体人群很多，既有传统意义上的黑客，又有恐怖分子、商业间谍、犯罪分子，甚至包括敌对国家的信息战士、间谍机构。这些主体人群各有目的，持续不断地在网络空间对个人、组织、地区乃至一个国家构成新的威胁（如表1-1所示）。事实上，随着信息和网络技术对社会各方面发展影响的日益深化，原来在真实世界的各种利益争夺必然体现到这一新的虚拟空间。只要存在利益冲突，网络空间就不会太平，网络安全问题就会持续。

与攻击方相比，网络的防御方长期处于被动状态，且往往缺乏专门的安全队伍，网络安全人才缺口非常大。以我国为例，近年来各高校培养的网络安全专业人才仅3万余人，而网络安全人才总需求量则超过70万人，缺口高达95%。此外，多数普通用户安全意识淡薄，在面对攻击时无论防护能力还是检测能力均非常薄弱。这也是攻击者，特别是近年异常活跃的各个APT攻击组织总是能够达成令人惊讶的攻击效果的一个重要原因。在攻防两方的博弈中，防御方还难以很快取得优势地位。

表1-1　主要网络安全威胁制造者

威胁类别	威胁主体	从事网络攻击的主要目的
国家安全威胁	信息战士	制造混乱，破坏目标
	恐怖分子	收集情报
共同安全威胁	恐怖分子	破坏公共秩序，制造混乱
	工业间谍	商业情报
	犯罪团伙	报复，实现经济目的
局部威胁	黑客	喜欢挑战，证明自己

1.2　网络攻击技术

网络攻击是指利用安全缺陷或不当配置对网络信息系统的硬件、软件或通信协议进行攻击，损害网络信息系统的完整性、可用性、机密性和抗抵赖性，导致被攻击信息系统敏感信息泄露、非授权访问、服务质量下降等后果的攻击行为。

1.2.1　网络攻击的分类

网络攻击的分类维度非常多，从不同角度区分可以得到不同的分类结果。从攻击的目的来看，可以分为**拒绝服务**（Denial-of-Service，DoS）**攻击**、获取系统权限的攻击、获取敏感信息的攻击等；从攻击的机理来看，有缓冲区溢出攻击、SQL注入攻击等；从攻击的实施过程来看，有获取初级权限的攻击、提升最高权限的攻击、后门控制攻击等；从攻击的实施对象来看，包括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。所以，很难以一个统一的模式对各种攻击手段进行分类。

按照攻击发生时攻击者与被攻击者之间的交互关系进行分类，可以将网络攻击分为**本地攻击**（Local Attack）、**主动攻击**（Server-side Attack，亦称服务端攻击）、**被动攻击**（Client-side Attack，亦称客户端攻击）、**中间人攻击**（Man-in-Middle Attack）四种。这种分类方法能够帮助我们较好地理解攻击的原理和攻击的发起方式，在此基础上，可较好地归纳对应的防御策略与方法。下面分别讨论这四类攻击的基本概念与特点。

（1）本地攻击

本地攻击指攻击者通过实际接触被攻击的主机而实施的攻击。

攻击者通过实际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，又可以在被攻击主机内植入特定的程序，如木马程序，以便将来能够远程控制该机器。

本地攻击比较难以防御，因为攻击者往往是能够接触到物理设备的用户，并且对目标网络的防护手段非常熟悉。防御本地攻击主要依靠严格的安全管理制度。

（2）主动攻击

主动攻击指攻击者对被攻击主机所运行的 Web、FTP（File Transfer Protocol，文件传输协议）、Telnet 等开放网络服务实施攻击。

利用目标网络服务程序中存在的安全缺陷或者不当配置，攻击者可获取目标主机权限，并进一步将虚假信息、垃圾数据、计算机病毒或木马程序等植入系统内部，从而破坏信息系统的机密性和完整性。主动攻击包括漏洞扫描、远程口令猜解、远程控制、信息窃取、信息篡改、拒绝服务攻击等攻击方法。

防御主动攻击的主要思路是：通过技术手段或安全策略加固系统所开放的网络服务。

（3）被动攻击

被动攻击指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。

在发动被动攻击时，攻击者常常先通过电子邮件或即时通信软件等向目标用户发送“诱骗”信息。如果用户被蒙骗而打开邮件中的恶意附件或者访问恶意网站，恶意附件或恶意网站就会利用用户系统中的安全缺陷与不当配置取得目标主机的合法权限。被动攻击包括钓鱼攻击、跨站脚本攻击、网站挂马攻击等攻击方法。

由于被动攻击通常从“诱骗”开始，因此社会工程学在被动攻击中应用广泛且作用关键。社会工程学是“一种操纵他人采取特定行动的行为，该行动不一定符合目标人的最佳利益，其结果包括获取信息、取得访问权限或让目标采取特定的行动”。本书以攻防技术为主要内容，对社会工程学感兴趣的读者可自行查阅有关资料与书籍。

要防御被动攻击，一方面是对系统以及网络应用中的客户程序进行安全加固，另一方面需要加强安全意识以辨识并应对网络攻击中的社会工程学手段。

（4）中间人攻击

中间人攻击指攻击者处于被攻击主机的某个网络应用的中间人位置，实施数据窃听、破坏或篡改等攻击。

这种攻击方法是通过各种技术手段将一台受攻击者控制的计算机置于客户程序和服务器的服务通信之间，这台计算机即所谓的“中间人”。攻击者使用“中间人”冒充客户身份与服务器通信，同时冒充服务器的身份与客户程序通信，并在此过程中读取或修改传递的信息。在整个攻击过程中，“中间人”对于客户程序和服务器而言是透明的，客户程序和服务器均难以觉察到“中间人”的存在。这种“拦截数据—修改数据—发送数据”的攻击方法有

时也称为劫持攻击。

防御中间人攻击的主要思路是为网络通信提供可靠的认证与加密机制，以确保通信双方身份的合法性和通信内容的机密与完整性。

1.2.2 网络攻击的步骤与方法

蓄意的网络攻击是防御者面临的主要网络安全威胁。学会从攻击者的角度思考，有助于更好地认识攻击，理解攻击技术的实质，进而实施有效的防御。一个完整的、有预谋的攻击往往可以分为信息收集、权限获取、安装后门、扩大影响、消除痕迹五个阶段。下面简要介绍攻击者在五个阶段的任务目标和内容方法，对应的具体攻击技术原理和相应防范措施将在后续各章详细探讨。本书前半部分关于网络攻击的内容也基本按照攻击步骤的顺序进行组织。

（1）信息收集

攻击者在信息收集阶段的主要目的是尽可能多地收集目标的相关信息，为后续的“精确”攻击奠定基础。

为更好地开展后续攻击，攻击者重点收集的信息包括：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。

攻击者可以直接对目标网络进行扫描探测，通过技术手段分析判断目标网络中主机的存活情况、端口开放情况、操作系统和应用软件的类型与版本信息等。除了对目标网络进行扫描探测，攻击者还会利用各种渠道尽可能地了解攻击目标的类型和工作模式，可能会借助以下方式：

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

攻击者所开展的信息收集活动通常没有直接危害，有些甚至不需要与目标网络交互，所以很难防范。随着越来越多的信息被数字化、网络化，很多安全相关的信息也越来越容易在网络上通过搜索得到；依托社会工程学，内部人员往往在无意中就向攻击者泄露了关键的安全信息。信息收集是耗费时间最长的阶段，有时可能会持续几个星期甚至几个月。随着信息收集活动的深入，公司的组织结构、潜在的信息系统漏洞就会逐步被攻击者发现，信息收集阶段的目的也就达到了。

本书第 2 章将详细探讨信息收集阶段攻击者常用的技术、方法和工具。

（2）权限获取

攻击者在权限获取阶段的主要目的是获取目标系统的读、写、执行等权限。

现代操作系统将用户划分为超级用户、普通用户等若干类别，并按类别赋予用户不同的权限，以进行细粒度的安全管理。

得到超级用户的权限是一个攻击者在单个系统中的终极目标，因为得到超级用户的权限就意味着对目标有了完全控制权，包括对所有资源的使用以及对所有文件的读、写和执行权限。

相对超级用户来说，普通用户权限的安全防范可能会弱一些。得到普通用户权限可以对目标中某些资源进行访问，比如对特定目录进行读写；同时，得到普通用户权限将为进一步得到超级用户权限提供更多的可能。

攻击者在这一阶段会使用信息收集阶段得到的各种信息，通过猜测用户账号口令、利用