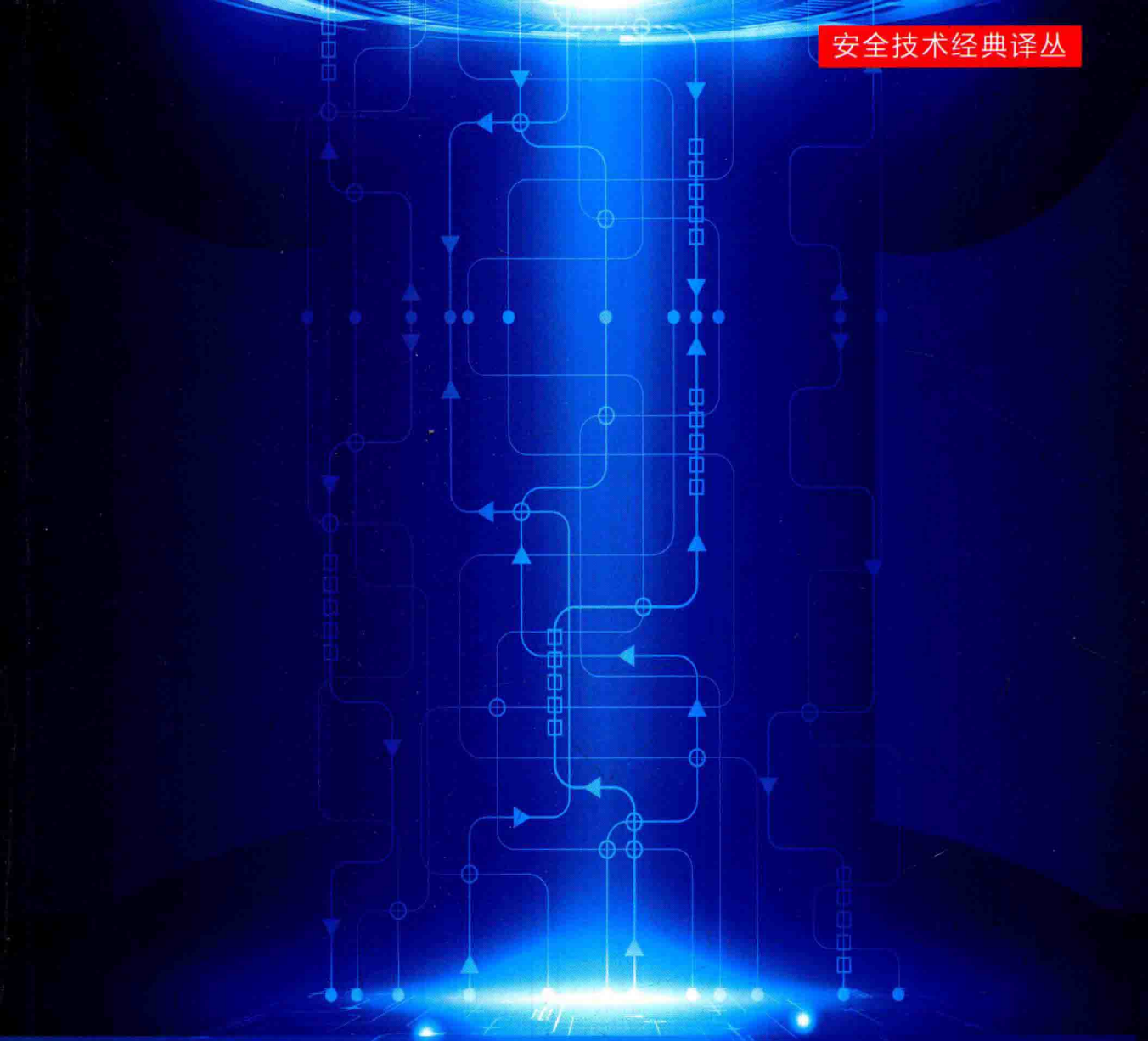
安全技术经典译丛



Penetration Testing Essentials

渗透测试入门实战

ean-Philip Oriyano 著
博 杜静 李海莉 译

清华大学出版社

安全技术经典译丛

渗透测试入门实战

[美] Sean-Philip Oriyano 著

李博 杜静 李海莉 译

清华大学出版社

北 京

Sean-Philip Oriyano
Penetration Testing Essentials
EISBN：978-1-119-23530-9

北京市版权局著作权合同登记号 图字：01-2017-3863

图书在版编目(CIP)数据

渗透测试入门实战 / (美)肖恩•飞利浦•奥瑞雅诺(Sean-Philip Oriyano) 著；李博，杜静，李海莉 译. —北京：清华大学出版社，2018
(安全技术经典译丛)
书名原文：Penetration Testing Essentials
ISBN 978-7-302-48693-0

Ⅰ. ①渗… Ⅱ. ①肖… ②李… ③杜… ④李… 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(2017)第 270947 号

责任编辑：王 军 于 平
封面设计：牛艳敏
版式设计：孔祥峰
责任校对：曹 阳
责任印制：杨 艳

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
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经 销：全国新华书店
开 本：185mm×260mm 印 张：18 字 数：404 千字
版 次：2018 年 1 月第 1 版 印 次：2018 年 1 月第 1 次印刷
印 数：1~3000
定 价：59.80 元

产品编号：074947-01

译 者 序

随着计算机网络技术的飞速发展并深入到经济和社会的方方面面，盗用身份、窃取信息和钱财，甚至进行网络恐怖攻击等种种网络犯罪也随之粉墨登场、愈演愈烈，从而催生了日益强烈的安全防护需求，而渗透测试正是查找、分析、展现潜在的安全问题并帮助制定策略以降低安全风险的最佳手段之一。

渗透测试，又称“白帽黑客”测试，是出于增强安全性的目的，在得到授权的前提下，通过利用与恶意攻击者相同的思路、技术、策略和手段，对给定组织机构的安全问题进行检测和评估的过程。通过渗透测试，能够由“知彼”做到“知己”，发现使用传统检测方法无法发现的攻击路径、攻击方法和技术弱点，从而在安全问题被攻击者利用之前，对其未雨绸缪地进行修复。

本书作者Sean-Philip Oriyano是一位专注于安全领域25年的资深专家，同时还是一名美军准尉，指挥一支专门从事网络安全训练、开发和策略制定的网络战分队，经验十分丰富。本书是一本关于渗透测试的入门书籍，适用于具有一定计算机技术基础、希望更深入学习渗透测试、在网络安全领域有所建树的读者。本书首先从攻击者的视角，介绍了渗透测试的基本概念和方法论，以及情报收集、漏洞扫描、密码破解、维持访问、对抗防御措施、无线网络与移动设备攻击、社会工程攻击等种种渗透测试手段；然后从防御方的角度阐述了如何加固主机和网络的防护；最后给出了如何规划职业发展，建立渗透测试实验室，进一步锻炼渗透测试技能的指南。书中介绍深入浅出，提供了丰富的操作实例和章后思考题，便于读者实践和提高。

本书主要内容由李博、杜静、李海莉翻译，参与本书翻译的还有程若思、韩哲、秦富童、庞训龙、孔德强、黄赫东、刘宇、袁学军、岁赛等。为了完美地翻译本书，做到“信、达、雅”，译者们在翻译过程中查阅、参考了大量的中英文资料。当然，限于水平和精力有限，翻译中的错误和不当之处在所难免，我们非常希望得到读者的积极反馈以利于更正和改进。

感谢本书的作者们，于字里行间感受到你们的职业精神和专业素养总是那么令人愉悦；感谢清华大学出版社给予我们从事本书翻译工作和学习的机会；感谢清华大学出版社的编辑们，他们为本书的翻译、校对投入了巨大的热情并付出了很多心血，没有他们的帮助和鼓励，本书不可能顺利付梓。

最后，希望读者通过阅读本书能够早日掌握渗透测试的技术精髓，成为一名“行黑客手段，显白帽风范”的安全高手！

译 者

献　辞

本书献给我的父母，他们赋予我成长过程中尤为宝贵的核心价值观。虽然父亲已经离开了我们，但我仍然能时时处处感受到他的影响，事实上，我有时会感觉自己自豪地开怀大笑的样子和从前的他完全一样。我的母亲仍在人世(愿她健康长寿)，我要感谢她支持和推动我钻研科学技术，并赋予我对科幻、冷笑话的热爱以及对正确行事的追求。我爱你们两人，这本书首先献给你们。

我也想把这本书献给军队的战友，是他们慷慨地给予我就读候补军官学校(Officer Candidate School，OCS)的机会，尽管我并不成熟并且以自我为中心。虽然学校里经历的磨难当时令我难以忍受，但它帮助我的生活走上正轨，并认识到自己的能力。它也帮助我意识到重要的并不是自己，而是那些生活受自己影响的人。我希望阅读这本书的读者都能思考这些问题。K上校、A中校、M上尉、 D上尉、J上尉和A上尉，我永远感谢你们对我耐心、真诚、直接、坦率的评价。 我希望我已经成为一名令你们自豪的准尉。这本书也是献给你们的。

我最后还要将这本书献给我的团队，你们展示了化腐朽为神奇的能力。在过去的一年里，你们一直不断地给我惊喜。你们让我光鲜亮丽，但我不能自居功劳。我没有承担那些繁重的工作，是你们承担的；我缺乏即兴发挥的能力和创造力，是你们提供的。E上士、L上士、S上士和N准尉，请继续出类拔萃，赢得荣誉。我还要感谢我的指挥官L中校，他信赖我的能力，给予我完成这一切的支持。

致　谢

重复一次，需要感谢的人太多，我真心希望没有漏掉任何人。

首先，感谢Jim Minatel给予我创作这本书的机会，我期待今后的其他机会。

接下来，我要感谢Kim Wimpsett。你无疑是我没有因语言和辞不达意的段落显得愚蠢的主要原因。我不知道如何表达你在团队中的价值，我希望未来我的每一个项目都有你加入。

然后，我希望向美国军队的所有人致以谢意，不论你们是谁。虽然可能你们不一定所有人都能安全回家(当然我真诚地希望都能)，任何人都永远不会被遗忘。而当我穿上制服时，不仅是为了工作，也是为了纪念你们的牺牲。

作者简介

Sean-Philip Oriyano是一位资深安全专业人士和企业家。在过去的25年中，他将时间分别投入到安全研究、咨询和提供IT以及网络安全领域的培训。此外，他还是一位在数字和印刷媒体出版方面均有多年经验的畅销书作家。在过去十年中，Sean出版了几本书，并通过参与电视和广播节目进一步扩大了他的影响力。到目前为止，Sean已经参加了十几个电视节目和广播节目，讨论不同的网络安全主题和技术。在摄像机前，Sean因其平易近人的风度而著称，并因深入浅出地解释复杂话题的能力广受好评。

除了从事自己的商业活动，他还是一名准尉，指挥一支专门从事网络安全训练、开发和战略的分队。此外，作为一名准尉，他被公认为是其领域的主题专家，经常在需要时被要求提供专业知识、培训和指导。

在不工作时，Sean是一位狂热的障碍赛跑运动员，已经完成了多项赛事，其中包括一项世界冠军锦标赛，四次斯巴达三项大满贯。他还喜欢旅游、健身、MMA格斗、玩游戏“银河战士”和“塞尔达传说”。

前　言

安全是当今世界受到高度重视的主题之一。由于人们越来越依赖不同形式的技术、随身数字产品以及许多其他类型的系统和设备，对这些设备和系统实际安全性究竟如何的关注与日俱增。为了应对诸如身份盗用、信息窃取、服务中断、黑客运动甚至恐怖主义等网络犯罪的增加，许多公共和私人组织面临着必须在自己成为网络犯罪的受害者以及发生诉讼之前对这些潜在安全性问题进行测试、评估和修复的挑战。正是为了应对过去、现在和未来的此类情况，许多组织正在仓促实施或寻求各种安全解决方案。

因此，渗透测试者应运而生，他们背后代表的是查找、分析、呈现和推荐策略以降低安全事件引起的潜在风险的最佳和最有效手段之一。渗透测试者是那些利用他们对技术及其漏洞和优势的深刻理解，应客户的要求抢在对组织不怀好意者之前定位和评估安全问题的人。

本书读者对象

本书的目标受众包括那些已经拥有一定技术背景并希望进入渗透测试领域的人。与许多涵盖渗透测试主题的其他书籍不同，本书力图以简单易懂的方式介绍该主题。本书的目标是帮助读者更好地了解渗透测试过程，并通过学习各种渗透测试基础理论和实践练习获得经验和知识。

在完成本书之后，你应该能对成为渗透测试者的意义以及成功所需的技能、工具和通用知识有一个更好的了解。在完成本书并且练习了所学内容后，就掌握了寻求更先进技术、测试方法和技能所需的工具。

本书使用条件

要充分利用本书的价值，需要有一些便利条件。在开始之前，你应该有一台至少具有8GB RAM的能够运行最新版本微软Windows或Kali Linux的计算机。此外，你应该有能够使用的虚拟化软件，如Oracle的VirtualBox或VMware的产品；选择使用何种虚拟化软件取决于个人喜好和经济能力。

在你阅读本书的过程中，将向你介绍用于完成任务的基于硬件和软件的工具。在章节和习题中，将给出所选工具的下载链接或通过其他方式获取的方法。

各章内容提要

本书涵盖了广泛的渗透测试入门主题。下面列出了各章及其关注重点的简介。

第1章“渗透测试简介” 该章重点介绍渗透测试的一般原理，以及成功所需的技能和知识。

第2章“操作系统与网络简介” 对操作系统及其所连接网络的结构有着扎实了解是渗透测试者所必需的。该章探讨两者的基本原理，以奠定学习的基础。

第3章“密码学简介” 如果没有加密技术，很多用于防止无意泄露信息的手段将无法正常工作。另外，如果不了解密码学，满足各种法律法规的要求将非常困难。该章介绍密码学功能和机制以及如何应用的基础知识。

第4章“渗透测试方法学综述” 为了可靠地获得最完整和最有效的结果，渗透测试有一套必须遵循的流程和方法。在该章中，将介绍最流行的执行渗透测试的方法。

第5章“情报收集” 渗透测试过程的第一步是收集有关目标的信息。在该章中，将探讨收集信息的各种手段，以及如何将它们集成到整个渗透过程中。

第6章“扫描和枚举” 一旦收集到关于目标的足够的情报，即可开始探测并找出可以提取哪些信息。该章包括如何获取用户名、组、安全策略等信息。

第7章“实施漏洞扫描” 想采取一种不同的方法了解目标？那么，可以使用手动或自动漏洞扫描的过程，定位环境中的弱点，以供以后利用。

第8章“破解密码” 由于密码是许多环境和应用程序的第一线防御，因此必须在获取这些有价值信息的过程中投入一定时间。在枚举中已经获得了用户名，所以可以专注于收集这些用户名的密码。

第9章“使用后门和恶意软件保持访问权” 通过调查、探索、突破，现在你已进入系统。但是，在获得访问权并建立这个滩头阵地后，如何才能保住它？该章要探讨的正是相关内容。

第10章“报告” 记住，你是在根据合同为客户工作，目标是查找问题并报告你的发现。在该章中，将介绍报告的一般格式和谋篇布局。

第11章“应对安防和检测系统” 当然并非所有的系统都是门户大开，等待渗透的。事实上，许多系统中会有几层不同形式的防御，严阵以待。在这种情况下，入侵检测和预防系统是渗透测试者的死敌，而在该章中将学习如何应对它们。

第12章“隐藏踪迹与规避检测” 在犯罪现场留下线索极易导致被抓住和挫败。在该章中，将学习如何在事后进行清理，以使除了最坚定的人都无法发现你。

第13章“探测和攻击无线网络” 无线网络普遍存在，因此几乎在任何你所探索的环境中都需要应对它。如果这些环境中包括移动设备，就必然会遇到此类网络，然后即可将之作为目标。

第14章“移动设备安全” 无论你如何看待移动设备，移动设备都不会就此停下发展

的脚步，而是不断推出新的形式、功能、外形，并且已成为我们日常生活中的一部分。由于它们已被整合到商业环境中，并且商业和个人使用之间的界限已经模糊，因此你必须学习如何应对移动设备。

第15章“进行社会工程攻击” 在每个系统中都有一个最弱的环节，在许多情况下，最弱的环节是人类。作为一名渗透测试人员，可以利用你的伶牙俐齿、心理学和巧妙的措辞，将谈话引向那些能够提供有用信息的话题。

第16章“加固主机系统” 有着各种可用于迟滞或阻止攻击的对策。最外层防线之一是经常锁定或者加固系统，以减少其被破坏的机会。

第17章“加固你的网络” 与加固主机一样，具有可用于迟滞或阻止对网络的攻击的对策。删除非必要协议，应用防火墙和其他机制可以迟滞并挫败攻击者。

第18章“规划职业成功之路” 在该章中，将自己视为一名毕业生。现在你正在寻求未来在渗透测试领域的发展。该章将提供下一步应如何继续培养技能的指南。

第19章“建立一个渗透测试实验室” 一名好的渗透测试者需要在实践中练习所拥有的装备。在该章中，我们将探讨如何建立一个可用于实践和实验的基础实验室。

目　录

第1章　渗透测试简介……1

1.1　渗透测试的定义……1

1.1.1　渗透测试者的工作内容……2

1.1.2　识别对手……2

1.2　保护机密性、完整性与可用性……3

1.3　黑客进化史漫谈……4

1.3.1　Internet的角色……5

1.3.2　黑客名人堂(或耻辱柱)……6

1.3.3　法律如何分类黑客行为……7

1.4　本章小结……9

1.5　习题……10

第2章　操作系统与网络简介……11

2.1　常见操作系统对比……11

2.1.1　微软Windows……12

2.1.2　Mac OS……13

2.1.3　Linux……14

2.1.4　Unix……15

2.2　网络概念初探……16

2.2.1　OSI模型……17

2.2.2　TCP/IP 协议族……19

2.2.3　IP地址……20

2.2.4　IP地址的格式……22

2.2.5　网络设备……25

2.3　本章小结……27

2.4　习题……27

第3章　密码学简介……29

3.1　认识密码学的4个目标……29

3.2 加密的历史……30
3.3 密码学常用语……31
3.4 比较对称和非对称加密技术……32
3.4.1 对称加密技术……32
3.4.2 非对称(公钥)加密技术……34
3.5 通过哈希算法变换数据……36
3.6 一种混合系统：使用数字签名……37
3.7 使用PKI……38
3.7.1 认证证书……39
3.7.2 构建公钥基础设施(PKI)结构……40
3.8 本章小结……40
3.9 习题……40

第4章 渗透测试方法学综述……43

4.1 确定工作的目标和范围……43
4.2 选择要执行的测试类型……45
4.3 通过签订合同获取许可……46
4.3.1 收集情报……47
4.3.2 扫描与枚举……48
4.3.3 渗透目标……49
4.3.4 维持访问……50
4.3.5 隐藏痕迹……50
4.3.6 记录测试结果……50
4.3.7 了解EC-Council流程……51
4.4 依法测试……52
4.5 本章小结……53
4.6 习题……54

第5章 情报收集……55

5.1 情报收集简介……55
5.1.1 信息分类……56
5.1.2 收集方法分类……56
5.2 检查公司网站……57
5.2.1 离线查看网站……58
5.2.2 寻找子域……59
5.3 找到不复存在的网站……60

5.4 用搜索引擎收集信息 60
5.4.1 利用谷歌进行黑客活动 61
5.4.2 获取搜索引擎告警 61
5.5 使用搜人网站定位员工 62
5.6 发现位置信息 63
5.7 应用社交网络 64
5.8 通过金融服务查找信息 67
5.9 调查职位招聘公告栏 67
5.10 搜索电子邮件 68
5.11 提取技术信息 68
5.12 本章小结 69
5.13 习题 69

第6章 扫描和枚举 71

6.1 扫描简介 71
6.2 检查存活系统 72
6.3 执行端口扫描 76
6.3.1 全开扫描(端口扫描) 78
6.3.2 隐蔽扫描(半开扫描) 79
6.3.3 圣诞树扫描 80
6.3.4 FIN扫描 80
6.3.5 NULL扫描 81
6.3.6 ACK扫描 81
6.3.7 分段扫描 82
6.3.8 UDP扫描 84
6.4 识别操作系统 84
6.5 漏洞扫描 86
6.6 使用代理服务器(即保持低调) 87
6.7 进行枚举 88
6.7.1 有价值的端口 88
6.7.2 利用电子邮件ID 89
6.7.3 SMTP枚举 89
6.7.4 常被利用的服务 91
6.7.5 NetBIOS 91
6.7.6 空会话 93
6.8 本章小结 93

6.9 习题……94

第7章 实施漏洞扫描……95

7.1 漏洞扫描简介……95
7.2 认识漏洞扫描的局限……96
7.3 漏洞扫描流程概述……97
7.3.1 对现有设备进行定期评估……97
7.3.2 评估新的系统……98
7.3.3 理解扫描目标……98
7.3.4 缓解风险……98
7.4 可执行的扫描类型……99
7.5 本章小结……100
7.6 习题……100

第8章 破解密码……101

8.1 识别强密码……101
8.2 选择一种密码破解技术……102
8.3 实施被动在线攻击……103
8.3.1 网络嗅探和数据包分析……103
8.3.2 中间人攻击……104
8.4 实施主动在线攻击……104
8.4.1 密码猜测……104
8.4.2 恶意软件……105
8.5 实施离线攻击……105
8.6 使用非技术性方法……107
8.6.1 默认密码……107
8.6.2 猜测……108
8.6.3 使用闪存驱动器窃取密码……108
8.7 提升权限……109
8.8 本章小结……110
8.9 习题……111

第9章 使用后门和恶意软件保持访问权……113

9.1 决定如何攻击……113
9.2 使用PsTools安装后门……114

9.3 使用LAN Turtle开启一个shell……115
9.4 识别各种恶意软件……116
9.5 启动病毒……117
9.5.1 病毒的生命周期……117
9.5.2 病毒的类型……119
9.6 启动蠕虫……121
9.7 启动间谍软件……122
9.8 植入木马……123
9.8.1 使用netcat工作……124
9.8.2 与netcat通信……126
9.8.3 使用netcat发送文件……126
9.9 安装rootkit……127
9.10 本章小结……127
9.11 习题……128

第10章 报告……129

10.1 报告测试参数……129
10.2 收集信息……130
10.3 突出重要信息……131
10.4 添加支持文档……134
10.5 实施质量保证……135
10.6 本章小结……136
10.7 习题……136

第11章 应对安防和检测系统……137

11.1 检测入侵……137
11.1.1 基于网络的入侵检测……137
11.1.2 网络检测引擎的分类……139
11.1.3 基于主机的入侵检测……140
11.1.4 入侵防御系统……140
11.2 识别入侵痕迹……141
11.2.1 主机系统入侵……141
11.2.2 统一威胁管理……142
11.2.3 网络入侵的指标……142
11.2.4 入侵的模糊迹象……143

11.3 规避IDS ……143
11.3.1 以IDS为目标 ……144
11.3.2 混淆 ……144
11.3.3 利用隐蔽通道 ……145
11.3.4 “狼来了” ……145
11.3.5 通过加密进行规避 ……146
11.4 攻破防火墙 ……146
11.4.1 防火墙配置 ……147
11.4.2 防火墙的类型 ……148
11.4.3 了解目标 ……148
11.4.4 防火墙上“蹈火” ……149
11.5 使用蜜罐：披着羊皮的狼 ……151
11.5.1 检测蜜罐 ……152
11.5.2 蜜罐的问题 ……152
11.6 本章小结 ……153
11.7 习题 ……153

第12章 隐藏踪迹与规避检测 …… 155

12.1 认识规避动机 ……155
12.2 清除日志文件 ……156
12.2.1 禁用Windows中的日志记录过程 ……157
12.2.2 删除日志文件中的事件 ……158
12.2.3 清除Linux计算机上的事件日志 ……160
12.2.4 擦除命令历史 ……160
12.3 隐藏文件 ……161
12.3.1 使用备用数据流(NTFS)隐藏文件 ……161
12.3.2 用隐写术隐藏文件 ……163
12.4 规避防病毒软件检测 ……166
12.5 通过后门规避防御 ……168
12.6 使用rootkit进行规避 ……169
12.7 本章小结 ……170
12.8 习题 ……170

第13章 探测和攻击无线网络 …… 171

13.1 无线网络简介 ……171

13.1.1 认识无线网络标准 172
13.1.2 比较5GHz和2.4GHz无线网络 173
13.1.3 识别无线网络的组件 174
13.1.4 Wi-Fi认证模式 177
13.2 攻破无线加密技术 178
13.2.1 破解WEP 178
13.2.2 从WEP转换到WPA 179
13.2.3 破解WPA和WPA2 180
13.2.4 了解无线部署选项 181
13.2.5 防护WEP和WPA攻击 183
13.3 进行Wardriving 攻击 183
13.4 进行其他类型的攻击 185
13.5 选择攻击无线网络的工具 186
13.5.1 选择实用程序 187
13.5.2 选择合适的无线网卡 187
13.6 破解蓝牙 189
13.6.1 蓝牙攻击的类型 190
13.6.2 关于蓝牙的注意事项 191
13.7 物联网黑客技术 192
13.8 本章小结 192
13.9 习题 193

第14章 移动设备安全 195

14.1 认识当今的移动设备 195
14.1.1 移动操作系统的版本和类型 196
14.1.2 移动设备面临的威胁 197
14.1.3 移动安全的目标 197
14.2 使用Android操作系统 199
14.2.1 Android系统的root操作 200
14.2.2 在沙箱中操作 200
14.2.3 搭建定制的Android系统 202
14.3 使用苹果iOS 203
14.4 查找移动设备中的安全漏洞 204
14.4.1 破解移动密码 204
14.4.2 寻找不受保护的网络 205
14.5 有关自带设备 205