

安全技术经典译丛

# 灰帽黑客

正义黑客的道德规范、渗透测试、攻击方法和漏洞分析技术

(第3版)

Gray Hat Hacking:  
The Ethical Hacker's Handbook, Third Edition

[美] Allen Harper, Shon Harris 等著

杨明军 韩智文 程文俊 译

专家级的系统攻击方法

最先进的渗透测试技术

最新安全漏洞和补救措施

恶意软件和rootkit的分析与捕获

缓冲区溢出、SQL注入、逆向工程

Mc  
Graw  
Hill Education

清华大学出版社



Allen Harper, Shon Harris, et al.

Gray Hat Hacking: The Ethical Hacker's Handbook, Third Edition

EISBN: 978-0-07-174255-9

Copyright © 2011 by The McGraw-Hill Companies, Inc.

All Rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including without limitation photocopying, recording, taping, or any database, information or retrieval system, without the prior written permission of the publisher.

This authorized Chinese translation is jointly published by McGraw-Hill Education (Asia) and Tsinghua University Press. This edition is authorized for sale in the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan.

Copyright © 2012 by McGraw-Hill Education (Asia), a division of the Singapore Branch of The McGraw-Hill Companies, Inc. and Tsinghua University Press.

版权所有。未经出版人事先书面许可，对本出版物的任何部分不得以任何方式或途径复制或传播，包括但不限于复印、录制、录音，或通过任何数据库、信息或可检索的系统。

本授权中文简体字翻译版由麦格劳-希尔(亚洲)教育出版公司和清华大学出版社合作出版。此版本经授权仅限在中华人民共和国境内(不包括香港特别行政区、澳门特别行政区和台湾)销售。

版权©2012 由麦格劳-希尔(亚洲)教育出版公司与清华大学出版社所有。

北京市版权局著作权合同登记号 图字：01-2011-3514

本书封面贴有 McGraw-Hill 公司防伪标签，无标签者不得销售。

版权所有，侵权必究。侵权举报电话：010-62782989 13701121933

#### 图书在版编目(CIP)数据

灰帽黑客：正义黑客的道德规范、渗透测试、攻击方法和漏洞分析技术(第3版)/(美)哈珀(Harper, A.)，(美)哈里斯(Harris, S.)等著；杨明军，韩智文，程文俊译。—北京：清华大学出版社，2012.11  
(安全技术经典译丛)

ISBN 978-7-302-30150-9

书名原文：Gray Hat Hacking: The Ethical Hacker's Handbook, Third Edition

I. ①灰… II. ①哈… ②哈… ③杨… ④韩… ⑤程… 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(2012)第 222891 号

责任编辑：王 军 韩宏志

装帧设计：康 博

责任校对：蔡 娟

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：清华大学印刷厂

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：37.75 字 数：895 千字

版 次：2012 年 11 月第 1 版 印 次：2012 年 11 月第 1 次印刷

印 数：1~3000

定 价：79.80 元

# 译者序

当人类跨入网络信息时代，人们在享受信息技术带来的高效率的同时，也面临着更大的挑战：小到个人隐私信息，大到企业信息资产，再到国家信息安全，现代社会的方方面面都受到越来越多的网络威胁和攻击。2010年伊朗核设施遭受 Stuxnet 蠕虫攻击，分析显示这次攻击针对的是该设施使用的西门子 SCADA 系统，最终导致浓缩铀离心机被病毒破坏。2011年底 CSDN 用户数据库泄露事件导致众多中国互联网用户人人自危，因为泄露的用户数据中包含部分以明文方式保存的用户密码，而其中的相当一部分人在其他网站上也使用了同样的用户名和密码，从而可能导致泄露更多的数据。

不断出现的各类网络安全事件使得人们越来越重视网络信息安全的重要性。孙子说：“知己知彼，百战不殆”。虽然没有绝对的安全，但如果能够做到知己知彼，了解敌方的攻击手段，包括如何利用漏洞(物理、信息系统)进入系统、如何展开攻击以及如何规避探测，那么对于防御战而言，即使不能百战百胜，也能做到及时发现漏洞，使损失最小化。

本书从渗透测试的角度来讨论网络攻防技术，在研究黑客攻击的策略、技能、工具和动机的同时，还探讨如何进行有效的防御。本书出自安全领域富有实战经验的专家之手，既包含广泛的、透彻的理论分析，又包括大量可操作性极高的实用范例。“魔高一尺，道高一丈”，安全领域的攻防技术日新月异。本书的作者来自安全一线战场，他们在本书中介绍了最新的黑客攻击技术和相应的防御手段，其中的大部分内容都是研究网络安全的不可多得的宝贵资料。

如果您是一位希望从事网络安全工作的新手，那么本书讨论的广泛主题能够让您对安全领域有一个综合性认识。而如果您是一名具有丰富实践经验的老兵，那么本书提供的最新攻防技术将会让您开阔视野，耳目一新。

本书主要由杨明军、韩智文、程文俊翻译。对于本书的翻译，我们力求做到语言平实无华、技术方面准确无误，希望能给读者带来轻松愉悦的阅读体验。

# 作者简介

**Allen Harper**, CISSP、PCI QSA, 北卡罗莱纳州 N2NetSecurity, Inc. 公司总裁和所有者。他曾在美国海军陆战队服役 20 年并在伊拉克“旅游”之后退役。此外,他还曾经担任美国财政部、国税局计算机安全应急响应中心(IRS CSIRC)的安全分析师。他经常在 Black Hat 和 Technot 等会议上发表演讲和授课。

**Shon Harris**, CISSP, Logical Security 总裁, 作家、教育工作者和安全咨询师。曾经担任过美国空军信息战部队的工程师, 并且出版过一些有关信息安全领域的不同学科的著作和论文。信息安全杂志(Information Security Magazine)曾经将她评为信息安全领域的 25 位最杰出的女性精英之一。

**Jonathan Ness**, CHFI, 微软安全响应中心(MSRC)首席软件安全工程师。他和他的同事致力于确保微软的安全更新能够全面地修复已报告的漏洞。他还负责微软的应急响应流程的技术响应, 致力于解决公开披露的针对微软软件的漏洞和攻击。他每月中有一个周末要担任预备役部队的安全工程师。

**Chris Eagle** 是位于美国加州蒙特利尔的海军研究生院计算机科学系的高级讲师。作为一位具有超过 25 年经验的计算机工程师和科学家, 他的研究兴趣包括计算机网络攻防、计算机取证以及逆向工程和反逆向工程技术。他经常在 Black Hat 会议上发表演讲, 并且特别钟爱 Defcon 的夺旗(capture the flag)比赛。

**Gideon Lenkey**, CISSP, Ra Security Systems, Inc. 公司总裁和联合创始人, 这是一家总部位于新泽西州的托管服务公司, 他在那里专门负责测试企业 IT 基础设施的信息安全状况。他曾为 FBI 提供过高级培训, 而且担任过 FBI 在新泽西州的 InfraGard 项目的负责人。他在多个场合中的杰出贡献得到了 FBI 主管 Robert Muller 的认可, 而且经常为国内外政府机构提供咨询。他经常为 Internet Evolution 网站供稿, 而且是东西方研究所网络安全计划的参与者。

**Terron Williams**, NSA IAM-IEM、CEH、CSSLP, Elster Electricity 资深测试工程师, 主要关注智能网络安全。他曾经在 Nortel 担任安全测试工程师和 VoIP 系统集成工程师。还曾经在 Hakin9 IT Security Magazine 杂志编辑部工作, 并在该杂志发表过多篇文章。他主要关注的是 VoIP、漏洞攻击研究、SCADA 安全以及新兴的智能网格技术。

免责声明: 本书中发表的内容均属本书作者的个人观点, 并不代表政府或微软公司的观点。

# 技术编辑简介

Michael Baucom 是北卡罗莱纳州 N2NetSecurity, Inc. 公司的研发副总裁。他的软件工程师职业生涯长达 15 年，曾经编写过各种软件，既包括采用汇编语言编写的路由转发代码，也包括 Windows 应用程序和服务。除编写软件外，他还从事过安全咨询工作，包括培训、源代码审查以及渗透测试。

# 致 谢

本书所有作者都非常感谢麦格劳希尔出版社的编辑们。尤其想要感谢 Joya Anthony，正是您让我们步入正轨，而且在整个过程中给予了我们巨大的帮助。您对这个项目所做的贡献非常显著。非常感谢。

**Allen Harper:** 感谢爱妻 Corann 和女儿 Haley 与 Madison，感谢她们在本书写作期间所给予的支持和理解。我每天都深深地爱着你们。此外，我还想感谢教会成员给予的爱和支持。尤其是 Rob Martin 和 Ronnie Jones 已经成为真正的兄弟和知己。此外，我还想感谢在写作过程中提供帮助的其他黑客：Alex Sotirov、Mark Dowd、Alexey Sintsov、Shuichiro Suzuki、Peter Van Eeckhoutte、Stéfan Le Berre 和 Damien Cauquil。

**Shon Harris:** 感谢其他作者和团队成员对这个项目所做的持续努力以及对整个行业所做的持续不断的贡献。我还想感谢狂热的 Fairbairn 姐妹 Kathy Conlon、Diane Marshall 和 Kristy Gorenz 对我和我的工作所给予的毕生支持。

**Jonathan Ness:** 感谢爱妻 Jessica 忍受我花费大量时间写作本书以及从事其他工作。还要感谢 Didier Stevens 为第 15 章所提供的慷慨帮助(以及在 <http://blog.didierstevens.com/programs/pdf-tools> 提供免费的 PDF 分析工具)。还要十分感谢 Terry McCorkle 提供的专家指导和建议，这帮助我完成了现在的第 16 章的内容，Terry 真是一位救命的大好人！最后，我想向在职业生涯中曾经指导过自己的导师、老师、同事、牧师、家庭和朋友们表示感谢，他们为我的成功提供了莫大的帮助。

**Chris Eagle:** 感谢 DDTEK 团队的所有核心成员。他们所做的艰苦卓绝的工作和所提供的技能令我惊叹不已。

**Gideon Lenkey:** 感谢亲爱的家庭和朋友们对我的工作的支持。还想感谢所有 FBI 特工，包括在职的和退休的，他们让我不再感到无聊！

**Terron Williams:** 感谢亲爱的妻子 Mekka 和继子 Christian Morris。你们是我生活的中心，感激我们一起分享的每分每秒。此外，还想感谢我的母亲 Christina Williams 和妹妹 Sharon Williams-Scott。我无时无刻不感激你们一直给予我的爱和支持。

# 前 言

我已经受够了一场战争，更别提再来一场了。

——托马斯·杰弗逊

我不知道第三次世界大战的武器会是什么样子。但我知道第四次世界大战战场上用的肯定是棍棒与石头。

——阿尔伯特·爱因斯坦

兵法非常简单。找出敌人在哪里，尽快到达那里，尽可能凶狠地打击他，而且要挺住。

——尤利西斯·S·格兰特

本书的目标是帮助培养更多技术精湛的、专注于抵御恶意黑客攻击的安全专家。事实一再证明，对敌方的了解是非常重要的，包括他们的策略、技能、工具和动机。企业和国家所面临的敌手非常专注，而且技艺超群。我们必须携起手来才能理解敌方的行动过程和流程，以确保我们能够正确地挫败敌方具有破坏性的恶意攻击。

本书的作者希望为读者提供他们认为这个行业所需的信息，即对负责的而且在意图和物质方面真正合乎道德标准的正义黑客技术的整体性讨论。这也是为什么本书一开始就给出正义黑客的定义的原因所在，社会上对正义黑客的理解是非常模糊的。

本书对前两版中的材料进行了更新，并尝试将最全面、最新的技术、流程和材料汇集起来。因此增加了9章全新的内容，同时对其他章的内容进行了更新。

本书第I部分制定了灰帽黑客必要的伦理和期望基础。该部分内容包括：

- 理清人们对白帽、黑帽和灰帽黑客的定义和特征的混淆认识
- 讨论在实施任何类型的正义黑客行动前应该了解的一些棘手的道德问题
- 讨论漏洞发现报告的难点以及可用于解决这些难题的一些模型
- 调查黑客攻击以及许多其他类型的恶意行为所涉及的法律问题
- 概览适当的漏洞发现流程以及当前提供指导方向的模型

第II部分介绍了现如今其他书籍中没有讲到的更高级的渗透测试方法和工具。现在的许多书籍讲的都是些相同的、被无数次反复翻新的旧的的工具和方法，而本书决定更加深入地讲解真正的灰帽黑客正在使用的高级机制。该部分将讨论如下内容：

- 用来实施渗透测试的自动化渗透测试方法和高级工具
- 最新的渗透测试工具
- 潜入攻击、社会工程以及内部攻击

第III部分将深入底层代码，向读者讲解各种操作系统和应用程序的特定部件的工作原理以及如何对它们加以利用。该部分将讨论如下内容：

- 介绍一些基本的编程知识，这些是理解本书剩余内容所需要掌握的概念
- 如何利用栈操作漏洞以及如何识别和编写缓冲区溢出攻击代码



- 如何识别高级的 Linux 和 Windows 漏洞以及如何对它们加以利用
- 如何创建不同类型的 shellcode 来开发自己的概念验证漏洞攻击程序和必要的软件，以测试和识别漏洞
- 最新的攻击类型，包括客户端、Web 服务器、VoIP 以及 SCADA 攻击

第IV部分将更深入地研究正义黑客技术的最高级主题，甚至当今的许多安全专家都没有理解这些主题。该部分将讨论如下内容：

- 被动和主动分析工具和方法
- 如何识别源代码和二进制文件中的漏洞
- 如何进行软件的逆向工程和组件的反汇编
- 模糊处理和调试技术
- 如何为二进制和源代码打补丁

第V部分将讲解恶意软件分析。有时候正义黑客会遇到恶意软件，而且可能需要进行一些基本的分析。该部分将讨论如下内容：

- 收集恶意软件样本
- 分析恶意软件，包括对反模糊处理技术进行讨论。

如果您希望进一步提高和加深对正义黑客技术的了解，那么本书非常适合您。

如果您有任何想法和评论，均可与我们联系，我们的反馈信箱是 [wkservice@vip.163.com](mailto:wkservice@vip.163.com)，投稿信箱是 [bookservice@vip.263.net](mailto:bookservice@vip.263.net)。此外，如果希望了解与本书有关的额外技术信息和资源，请浏览 [www.grayhathackingbook.com](http://www.grayhathackingbook.com) 或 [www.mhprofessional.com/product.php?cat=112&isbn=0071742557](http://www.mhprofessional.com/product.php?cat=112&isbn=0071742557)。

# 目 录

## 第 I 部分 “合乎道德的揭秘行为” 简介

<b>第 1 章 正义黑客的道德规范</b> .....	3
1.1 理解敌方策略的意义 .....	3
1.2 认识安全领域的灰色区域 .....	7
1.3 本书与正义黑客类图书 的关系 .....	8
1.3.1 漏洞评估 .....	8
1.3.2 渗透测试 .....	9
1.4 关于黑客类图书和课程的 争议 .....	12
1.4.1 工具的双重性 .....	13
1.4.2 识别攻击 .....	14
1.4.3 模拟攻击 .....	15
1.5 攻击者最喜欢利用的漏洞 .....	15
<b>第 2 章 合乎道德的正当揭秘行为</b> .....	19
2.1 各方看待问题的不同角度 .....	20
2.2 CERT 目前采取的工作流程 .....	21
2.3 完全揭秘策略—— RainForest Puppy Policy .....	23
2.4 Internet 安全组织 .....	24
2.4.1 发现 .....	25
2.4.2 通知 .....	25
2.4.3 验证 .....	27
2.4.4 解决 .....	29
2.4.5 发布 .....	30
2.5 争议仍将存在 .....	30
2.6 案例分析 .....	34
2.6.1 正当揭秘过程的优缺点 .....	35
2.6.2 供应商更加关注 .....	38
2.7 接下来应该处理的事项 .....	38

## 第 II 部分 渗透测试及工具

<b>第 3 章 社会工程攻击</b> .....	43
3.1 社会工程攻击原理 .....	43
3.2 实施社会工程攻击 .....	44
3.3 渗透测试中常用到的 攻击手段 .....	46
3.3.1 好心人 .....	47
3.3.2 会议室 .....	51
3.3.3 加入公司 .....	53
3.4 准备好进行面对面的攻击 .....	54
3.5 防御社会工程攻击 .....	56
<b>第 4 章 潜入攻击</b> .....	57
4.1 潜入攻击如此重要的原因 .....	57
4.2 实施潜入攻击 .....	58
4.2.1 侦察 .....	58
4.2.2 思想准备 .....	60
4.3 进入目标建筑物的常用方法 .....	60
4.3.1 吸烟区入口 .....	61
4.3.2 人工检查点 .....	62
4.3.3 锁住的门 .....	64
4.3.4 物理方式开锁 .....	66
4.3.5 进入目标之后 .....	69
4.4 防御潜入攻击 .....	69
<b>第 5 章 内部攻击</b> .....	71
5.1 模拟内部攻击的重要性 .....	71
5.2 实施内部攻击 .....	72
5.2.1 工具和准备工作 .....	72
5.2.2 了解情况 .....	72
5.2.3 获得本地管理员权限 .....	73
5.2.4 禁用防病毒软件 .....	76
5.2.5 使用 Cain .....	77

5.3	防御内部攻击	83
<b>第6章 使用 BackTrack Linux</b>		
	分发版本	85
6.1	BackTrack 简介	85
6.2	将 BackTrack 安装到 DVD 或 U 盘	86
6.3	直接在虚拟机中使用 BackTrack ISO 映像文件	87
6.3.1	使用 VirtualBox 创建 BackTrack 虚拟机	88
6.3.2	引导 BackTrack LiveDVD 系统	88
6.3.3	探索 BackTrack X 窗口环境	89
6.3.4	启动网络服务	90
6.4	永久性更改 BackTrack	90
6.4.1	将 BackTrack 完整地安装在硬盘或者 U 盘中	91
6.4.2	新建一个包含永久性更改信息的 ISO 文件	92
6.4.3	使用自定义文件自动保存和恢复更改	94
6.5	研究 BackTrack 引导菜单	95
6.6	更新 BackTrack	97
<b>第7章 使用 Metasploit</b>		
7.1	Metasploit 简介	99
7.2	获取 Metasploit	99
7.3	使用 Metasploit 控制台加载攻击工具	100
7.4	使用 Metasploit 攻击客户端漏洞	105
7.5	使用 Metasploit Meterpreter 进行渗透测试	107
7.6	Metasploit 的自动化与脚本化	113
7.7	更进一步探讨 Metasploit	115
<b>第8章 渗透测试管理</b>		
8.1	制定渗透测试计划	117

8.1.1	渗透测试的类型	117
8.1.2	渗透测试的范围	118
8.1.3	渗透测试的位置	118
8.1.4	渗透测试小组成员构成	118
8.1.5	方法和标准	118
8.1.6	渗透测试的各个阶段	119
8.1.7	渗透测试计划	120
8.2	签署渗透测试协议	121
8.2.1	工作声明	121
8.2.2	“保释信”	121
8.3	实施渗透测试	122
8.3.1	测试启动会议	122
8.3.2	渗透测试中的资源访问	122
8.3.3	测试预期值管理	123
8.3.4	测试问题管理	123
8.3.5	欲速则不达	123
8.3.6	外部和内部协同	123
8.4	在渗透测试中进行信息共享	124
8.5	生成渗透测试结果报告	128
8.5.1	报告格式	128
8.5.2	报告摘要	128

### 第III部分 漏洞攻击

<b>第9章 编程技能</b>		
9.1	C 编程语言	131
9.1.1	C 语言基本结构	131
9.1.2	程序范例	135
9.1.3	使用 gcc 进行编译	136
9.2	计算机内存	137
9.2.1	随机存取存储器(RAM)	137
9.2.2	字节序	137
9.2.3	内存分段	138
9.2.4	内存中的程序	138
9.2.5	缓冲区	139
9.2.6	内存中的字符串	139
9.2.7	指针	139
9.2.8	内存知识小结	140
9.3	Intel 处理器	141

9.4	汇编语言基础	142	10.4.5	测试漏洞攻击	177
9.4.1	机器指令、汇编语言与C语言	142	<b>第 11 章</b>	<b>高级 Linux 漏洞攻击</b>	<b>179</b>
9.4.2	AT&T 与 NASM	142	11.1	格式化字符串漏洞攻击	179
9.4.3	寻址模式	144	11.1.1	问题描述	179
9.4.4	汇编文件结构	145	11.1.2	从任意内存读取	183
9.4.5	汇编过程	146	11.1.3	写入任意内存	184
9.5	使用 gdb 进行调试	146	11.1.4	利用 .dtors 获得根 特权级	186
9.5.1	gdb 基础	146	11.2	内存保护机制	189
9.5.2	使用 gdb 进行反汇编	148	11.2.1	编译器改进	190
9.6	Python 编程技能	149	11.2.2	内核补丁和脚本	193
9.6.1	获取 Python	149	11.2.3	“返回到 libc”漏洞 攻击	194
9.6.2	Python 中的 Hello World 程序	149	11.2.4	综合比较	202
9.6.3	Python 对象	150	<b>第 12 章</b>	<b>shellcode 策略</b>	<b>203</b>
9.6.4	字符串	150	12.1	用户空间 shellcode	203
9.6.5	数字	151	12.1.1	系统调用	203
9.6.6	列表	152	12.1.2	基本 shellcode	204
9.6.7	字典	153	12.1.3	端口绑定 shellcode	205
9.6.8	Python 文件操作	154	12.1.4	反向 shellcode	206
9.6.9	Python 套接字编程	155	12.1.5	查找套接字 shellcode	207
<b>第 10 章</b>	<b>基本的 Linux 漏洞攻击</b>	<b>157</b>	12.1.6	命令执行代码	208
10.1	栈操作	157	12.1.7	文件传输代码	208
10.2	缓冲区溢出	159	12.1.8	多级 shellcode	209
10.2.1	meet.c 溢出	160	12.1.9	系统调用代理 shellcode	209
10.2.2	缓冲区溢出的后果	163	12.1.10	进程注入 shellcode	210
10.3	本地缓冲区溢出漏洞攻击	164	12.2	其他 shellcode 考虑因素	211
10.3.1	漏洞攻击组成部分	164	12.2.1	shellcode 编码	211
10.3.2	在命令行上进行栈溢出 漏洞攻击	167	12.2.2	自我破坏 shellcode	212
10.3.3	使用通用漏洞攻击代码 进行栈溢出漏洞攻击	168	12.2.3	反汇编 shellcode	213
10.3.4	对小缓冲区进行 漏洞攻击	170	12.3	内核空间 shellcode	214
10.4	漏洞攻击开发过程	173	<b>第 13 章</b>	<b>编写 Linux shellcode</b>	<b>217</b>
10.4.1	控制 eip	173	13.1	基本的 Linux shellcode	217
10.4.2	确定偏移	173	13.1.1	系统调用	217
10.4.3	确定攻击途径	176	13.1.2	使用 C 进行系统调用	218
10.4.4	构建漏洞攻击三明治	176	13.1.3	使用汇编语言进行 系统调用	219

13.1.4	系统调用 exit	219	14.2.4	确定偏移	257
13.1.5	系统调用 setreuid	221	14.2.5	确定攻击途径	258
13.1.6	利用 execve 实现创建 shell 的 shellcode	222	14.2.6	构建攻击三明治	261
13.2	实现端口绑定 shellcode	226	14.2.7	根据需要调试漏洞攻击程序	262
13.2.1	Linux 套接字编程	226	14.3	理解 SEH	264
13.2.2	采用汇编语言编程建立一个套接字	228	14.4	理解 Windows 内存保护 (XP SP3、Vista、7 和 Server 2008)	266
13.2.3	测试 shellcode	231	14.4.1	基于栈的缓冲区溢出检测(/GS)	266
13.3	实现反向连接 shellcode	234	14.4.2	SafeSEH	268
13.3.1	反向连接 C 语言编程	234	14.4.3	SEHOP	268
13.3.2	反向连接汇编程序	235	14.4.4	堆保护	268
13.4	shellcode 编码	237	14.4.5	DEP	268
13.4.1	简单的 XOR 编码	237	14.4.6	ASLR	269
13.4.2	编码后 shellcode 的结构	238	14.5	绕过 Windows 内存保护	270
13.4.3	JMP/CALL XOR 解码器示例	238	14.5.1	绕过/GS	270
13.4.4	FNSTENV XOR 示例	239	14.5.2	绕过 SafeSEH	271
13.4.5	将代码组合起来	241	14.5.3	绕过 ASLR	272
13.5	利用 Metasploit 自动生成 shellcode	244	14.5.4	绕过 DEP	272
13.5.1	利用 Metasploit 生成 shellcode	244	14.5.5	绕过 SEHOP	278
13.5.2	利用 Metasploit 对 shellcode 进行编码	245	14.5.6	内存保护绕过方法小结	285
<b>第 14 章</b>	<b>Windows 漏洞攻击</b>	<b>247</b>	<b>第 15 章</b>	<b>Content-Type 攻击原理与检测</b>	<b>287</b>
14.1	Windows 程序编译与调试	247	15.1	Content-Type 攻击原理	287
14.1.1	在 Windows 上进行编译	247	15.2	现今可被攻击的文件格式	289
14.1.2	在 Windows 上用 OllyDbg 进行调试	249	15.3	PDF 文件格式简介	290
14.2	编写 Windows 漏洞攻击程序	253	15.4	恶意 PDF 漏洞攻击分析	293
14.2.1	漏洞攻击程序开发过程回顾	254	15.5	恶意 PDF 文件检测工具	296
14.2.2	ProSSHD 服务器	254	15.5.1	PDFiD	296
14.2.3	控制 eip	255	15.5.2	Pdf-parser.py	300
			15.6	Content-Type 攻击防御测试工具	303
			15.7	Content-Type 攻击防御方法	304
			15.7.1	安装所有的安全更新	304
			15.7.2	在 Adobe Reader 中禁用 JavaScript	305

15.7.3	针对微软 Office 应用程序和 Adobe Reader 启用 DEP .....	305
<b>第 16 章</b>	<b>Web 应用程序安全漏洞 .....</b>	<b>307</b>
16.1	最流行的 Web 应用程序 安全漏洞概述 .....	307
16.1.1	注入漏洞 .....	307
16.1.2	跨站脚本漏洞 .....	308
16.1.3	OWASP 十大隐患中 的其他内容 .....	308
16.2	SQL 注入漏洞攻击 .....	308
16.2.1	SQL 数据库与语句 .....	310
16.2.2	测试 Web 应用程序并 搜寻 SQL 注入漏洞 .....	312
16.3	跨站脚本漏洞攻击 .....	317
16.3.1	“脚本”的含义 .....	317
16.3.2	跨站脚本的含义 .....	318
<b>第 17 章</b>	<b>VoIP 攻击 .....</b>	<b>323</b>
17.1	VoIP 的含义 .....	323
17.2	VoIP 使用的协议 .....	324
17.2.1	SIP .....	324
17.2.2	Megaco H.248 .....	325
17.2.3	H.323 .....	325
17.2.4	TLS 和 DTLS .....	326
17.2.5	SRTP .....	327
17.2.6	ZRTP .....	327
17.3	VoIP 攻击类型 .....	327
17.3.1	枚举 .....	328
17.3.2	SIP 口令破解 .....	328
17.3.3	窃听与分组捕获 .....	329
17.3.4	拒绝服务 .....	329
17.4	如何防范 VoIP 攻击 .....	335
<b>第 18 章</b>	<b>SCADA 攻击 .....</b>	<b>337</b>
18.1	SCADA 的含义 .....	337
18.2	SCADA 使用的协议 .....	338
18.2.1	OPC .....	338
18.2.2	ICCP .....	338
18.2.3	Modbus .....	338
18.2.4	DNP3 .....	339
<b>18.3</b>	<b>SCADA fuzzing 测试 .....</b>	<b>340</b>
18.3.1	使用 Autodafé 进行 SCADA fuzzing 测试 .....	340
18.3.2	使用 TFTP Daemon Fuzzer 进行 SCADA fuzzing 测试 .....	346
<b>18.4</b>	<b>Stuxnet 恶意软件(网络恐怖 主义新浪潮) .....</b>	<b>349</b>
<b>18.5</b>	<b>防范 SCADA 攻击 .....</b>	<b>349</b>
<b>第IV部分 漏洞分析</b>		
<b>第 19 章</b>	<b>被动分析 .....</b>	<b>353</b>
19.1	道德的逆向工程 .....	353
19.2	使用逆向工程的原因 .....	354
19.3	源代码分析 .....	355
19.3.1	源代码审计工具 .....	355
19.3.2	源代码审计工具的 实用性 .....	357
19.3.3	手工源代码审计 .....	359
19.3.4	自动化源代码分析 .....	363
19.4	二进制分析 .....	365
19.4.1	二进制代码的手工审计 .....	365
19.4.2	自动化的二进制 分析工具 .....	376
<b>第 20 章</b>	<b>使用 IDA Pro 进行高级 静态分析 .....</b>	<b>381</b>
20.1	静态分析难点 .....	381
20.1.1	剥离的二进制文件 .....	381
20.1.2	静态链接程序和 FLAIR .....	383
20.1.3	数据结构分析 .....	389
20.1.4	已编译的 C++ 代码 的怪异之处 .....	393
20.2	扩展 IDA Pro .....	396
20.2.1	IDC 脚本编程 .....	396
20.2.2	IDA Pro 插件模块 及 IDA Pro SDK .....	398
20.2.3	构建 IDA Pro 插件 .....	400

20.2.4	IDA Pro 加载器及 处理器模块	402	22.3.2	历史上针对客户端 攻击的著名漏洞	431
<b>第 21 章</b>	<b>高级逆向工程技术</b>	<b>405</b>	<b>22.4</b>	<b>挖掘基于浏览器的新漏洞</b>	<b>437</b>
21.1	软件攻击的目的	405	22.4.1	mangleme	437
21.2	软件开发过程概述	406	22.4.2	Mozilla 安全团队的 模糊测试工具	440
21.3	检测工具	407	22.4.3	AxEnum	441
21.3.1	调试器	407	22.4.4	AxFuzz	446
21.3.2	代码覆盖分析工具	409	22.4.5	AxMan	446
21.3.3	统计分析工具	410	<b>22.5</b>	<b>可利用的堆喷射技术</b>	<b>451</b>
21.3.4	流程分析工具	410	<b>22.6</b>	<b>防范客户端漏洞攻击</b>	<b>452</b>
21.3.5	内存使用监视工具	412	22.6.1	同步更新安全补丁	452
21.4	模糊测试	416	22.6.2	获取最新信息	453
21.5	定制的模糊测试工具 和技术	417	22.6.3	在缩减权限下运行 Internet 应用	453
21.5.1	一个简单的 URL 模糊 测试工具	417	<b>第 23 章</b>	<b>攻击 Windows 访问控制 模型</b>	<b>455</b>
21.5.2	对未知协议进行模糊 测试	420	23.1	攻击访问控制机制的 理由	455
21.5.3	SPIKE	421	23.1.1	多数人不理解访问 控制机制	455
21.5.4	SPIKE 静态内容原语	421	23.1.2	访问控制漏洞易于攻击	456
21.5.5	SPIKE Proxy	424	23.1.3	访问控制漏洞数量巨大	456
21.5.6	Sharefuzz	424	<b>23.2</b>	<b>Windows 访问控制的 工作机制</b>	<b>456</b>
<b>第 22 章</b>	<b>客户端浏览器的漏洞攻击</b>	<b>427</b>	23.2.1	安全标识符	456
22.1	客户端软件漏洞的重要性	427	23.2.2	访问令牌	457
22.1.1	客户端漏洞可以规避 防火墙保护	427	23.2.3	安全描述符	460
22.1.2	客户端应用程序经常 在管理权限下运行	428	23.2.4	访问检查	463
22.1.3	客户端漏洞易于针对 特定人群或机构目标	428	<b>23.3</b>	<b>访问控制配置分析工具</b>	<b>465</b>
22.2	Internet Explorer 的安全 概念	429	23.3.1	转储进程令牌	466
22.2.1	ActiveX 控件	429	23.3.2	转储安全描述符	468
22.2.2	Internet Explorer 安全区域	430	<b>23.4</b>	<b>特殊 SID、特殊访问权限和 “禁止访问”问题</b>	<b>469</b>
22.3	客户端漏洞攻击的历史 与发展趋势	431	23.4.1	特殊的 SID	469
22.3.1	客户端漏洞的流行	431	23.4.2	特殊访问权限	471
			23.4.3	“禁止访问”的原理	472
			<b>23.5</b>	<b>访问控制引起的提权漏洞</b>	<b>477</b>

23.6	各种对象类型的攻击模式	478	25.3.2	缓冲区的方向	534
23.6.1	服务攻击	478	25.3.3	自毁式 shellcode	534
23.6.2	Windows 注册表 DACL 攻击	484	25.4	对问题进行归档	535
23.6.3	目录 DACL 攻击	488	25.4.1	背景知识	535
23.6.4	文件 DACL 攻击	493	25.4.2	环境	536
23.7	其他对象类型的枚举方法	497	25.4.3	研究结果	536
23.7.1	共享内存段	497	<b>第 26 章</b>	<b>关闭漏洞：缓解问题</b>	<b>537</b>
23.7.2	命名管道	498	26.1	各种缓解方案	537
23.7.3	进程	499	26.1.1	端口碰撞技术	537
23.7.4	其他已命名的内核对象 (信号量、互斥锁、事件、 设备)	500	26.1.2	迁移	538
<b>第 24 章</b>	<b>智能模糊测试框架 Sulley</b>	<b>503</b>	26.2	打补丁	539
24.1	协议分析	503	26.2.1	对源代码打补丁的 注意事项	539
24.2	Sulley 模糊测试框架	504	26.2.2	给二进制程序打补丁 的注意事项	541
24.2.1	安装 Sulley	505	26.2.3	二进制变异	545
24.2.2	强大的模糊测试工具	505	26.2.4	第三方打补丁方案	549
24.2.3	块结构	507			
24.2.4	监视进程中的错误	511	<b>第 V 部分 恶意软件分析</b>		
24.2.5	监视网络流量	512	<b>第 27 章</b>	<b>收集恶意软件和初步分析</b>	<b>553</b>
24.2.6	控制 VMware	512	27.1	恶意软件	553
24.2.7	综述	513	27.1.1	恶意软件类型	553
24.2.8	崩溃事件的事后分析	515	27.1.2	恶意软件的防护技术	554
24.2.9	网络使用分析	516	27.2	蜜网技术的最新发展趋势	555
24.2.10	进一步研究	517	27.2.1	蜜罐	555
<b>第 25 章</b>	<b>漏洞的可利用性和漏洞 攻击程序</b>	<b>519</b>	27.2.2	蜜网	555
25.1	漏洞的可利用性	519	27.2.3	为什么要使用蜜罐	555
25.1.1	通过调试分析可利用性	520	27.2.4	蜜罐的局限性	556
25.1.2	初始分析	520	27.2.5	低交互性蜜罐	556
25.2	理解漏洞攻击问题	524	27.2.6	高交互性蜜罐	557
25.2.1	先决条件和后置条件	524	27.2.7	蜜网的类型	557
25.2.2	可重复性	525	27.2.8	规避 VMware 检测 技术	559
25.3	构造漏洞攻击程序有效 载荷的相关考虑事项	533	27.3	捕捉恶意软件：设置陷阱	561
25.3.1	漏洞攻击程序有效 载荷的协议元素	533	27.3.1	VMware 宿主机设置	561
			27.3.2	VMware 客户机设置	561
			27.3.3	使用 Nepenthes 进行 捕获	562



27.4	恶意软件的初步分析.....	563	28.2	对恶意软件进行去混淆处理.....	575
27.4.1	静态分析.....	563	28.2.1	加壳程序基础.....	576
27.4.2	动态分析.....	565	28.2.2	对二进制文件进行脱壳处理.....	577
27.4.3	Norman SandBox 技术.....	569	28.3	对恶意软件进行逆向工程.....	584
<b>第 28 章</b>	<b>破解恶意软件.....</b>	<b>573</b>	28.3.1	恶意软件的设置阶段.....	584
28.1	恶意软件的发展趋势.....	573	28.3.2	恶意软件的运行阶段.....	584
28.1.1	嵌入的组件.....	573	28.3.3	自动化的恶意软件分析.....	585
28.1.2	加密的使用.....	574			
28.1.3	用户空间隐藏技术.....	574			
28.1.4	rootkit 技术的应用.....	574			
28.1.5	持久化措施.....	575			