- 剖析黑客攻击原理
- 编写攻击代码
- 通过假设创建攻击
- 分析漏洞及修补方法

# 灰帽攻击安全手册

Gray Hat Hacking: the Ethical Hacker's Handbook

## 渗透测试与漏洞分析技术

关键内容：
渗透测试及自动化渗透测试
漏洞分析及修补

（美） Shon Harris Allen Harper Chris Eagle
Jonathan Ness Michael Lester 著

郭 旭 译

Osborne
McGraw Hill

McGraw Hill

清华大学出版社

# 灰帽攻击安全手册——渗透测试与漏洞分析技术


[美] Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Michael Lester 著

郭 旭 译



清 华 大 学 出 版 社

北 京

Shon Harris Allen Harper Chris Eagle Jonathan Ness Michael Lester
Gray Hat Hacking : The Ethical Hacker's Handbook
EISBN 0-07-225709-1


北京市版权局著作权合同登记号 图字 01-2006-0344 号

**图书在版编目（CIP）数据**

灰帽攻击安全手册：渗透测试与漏洞分析技术/（美）哈里斯（Harris,S.），（美）哈珀（Harper,A.）等著；郭旭译. —北京：清华大学出版社，2007
书名原文：Gray Hat Hacking:The Ethical Hacker's Handbook

ISBN 978-7-302-14615-5

Ⅰ.灰… Ⅱ. ①哈…②哈…③郭… Ⅲ. 电子计算机－安全技术－手册 Ⅳ. TP309-62

中国版本图书馆 CIP 数据核字（2007）第 014520 号

**责任编辑**：刘秀青
**责任校对**：刘雪莲
**责任印制**：科 海
**出版发行**：清华大学出版社 **地 址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn **邮 编**：100084
c - service@tup.tsinghua.edu.cn
**社 总 机**：010-62770175 **邮购热线**：010-62786544
**投稿咨询**：010-62772015 **客户服务**：010-62776969
**印 装 者**：北京市鑫山源印刷有限公司
**经 销**：全国新华书店
**开 本**：185×230 **印 张**：26.5 **字 数**：579 千字
**版 次**：2007 年 4 月第 1 版 **印 次**：2007 年 4 月第 1 次印刷
**印 数**：1~4 000
**定 价**：49.00 元

# 内 容 简 介

灰帽黑客在网络安全中代表发现漏洞但不利用漏洞进行攻击，而是与软件厂商协作寻找解决方案的人。

本书由多位安全领域的著名专家编写，按部就班地描述了灰帽黑客适用的道德、法律、操作过程、使用的工具和方法，旨在使你成为一个合格、全面的正义黑客。

全书分为 4 大部分共 15 章。第 1 部分从道德规范和法律的角度介绍正义黑客，包括相关制度、工作步骤以及正确的漏洞发现过程，这些内容在同类书中极少涉及；第 2 部分介绍了渗透测试的过程与工具，包括建立测试团队和实验室、在工作中合法地保护自己、嗅探工具和渗透测试工具的合理使用；第 3 部分讲解各种攻击方法，有使用编程技巧对 Linux 系统的缓冲区、格式串和堆进行攻击，创建 shellcode 攻击，编写对 Windows 漏洞的攻击，并对代码逐行分析、点睛技巧，也是同类书难以寻觅；第 4 部分主要介绍各种漏洞分析方法和工具，包括被动分析，在源代码和二进制文件中识别漏洞并打补丁，对软件进行逆向工程、杂凑等。

本书涵盖了 Linux 和 Windows 系统，原理和技术并重，涉及面广，是信息安全管理人员、程序员以及对黑客技术感兴趣读者的必备工具书。

# 作者简介

Shon Harris：MCSE、CISSP、Logical Security 的总裁，教育工作者和安全顾问。她曾是美国空军信息战部队（the U.S. Air Force Information Warfare Unit）的工程师，并在与信息安全相关的不同领域出版过一些书和文章。信息安全杂志（Information Security Magazine）认为 Shon 是信息安全领域最顶尖的 25 位女士之一。

Allen Harper：CISSP，曾在美国海军陆战队服役过 17 年，目前是美国国防部的安全工程师。此前，他是美国海军海空战争系统司令部（the Navy Space and Naval Warfare Systems Command，SPAWAR）的讲师，讲授渗透测试技术。此外，他还是美国财政部、美国国税局、计算机安全事件响应中心的安全分析师。现住在北弗吉尼亚。

Chris Eagle：美国海军研究生院（the Naval Postgraduate School，NPS，位于加州的蒙特利尔）计算机科学系的副主席。作为一位有 18 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击和防御、计算机相关的法律以及逆向和反逆向工程。在黑客大会 Defcon 的夺旗（capture the flag）比赛中，经常可以看到他。

Jonathan Ness：微软公司的软件安全工程师，为微软公司增强下一代产品的安全性，并修复由安全社区报告的漏洞。作为空军国家防卫局（Air National Guard）的信息战攻击中队（Information Warfare Aggressor Squadron）的成员，他也领导了针对全美范围内空军设施的网络渗透测试。

Michael J Lester：CISSP、MCSE（Messaging and Security）、MCSE+I、MCSA、MCT、CCNP、CCDP、CCSE+、CCI、CCEA、CTT+、Linux+、Security+、Network+、I-net+、A+，信息技术理学士学位，Logical Security（www.LogicalSecurity.com）公司的 Ethical Hacking and Forensics 项目的项目经理。他讲授并编写过各种课程，包括 Microsoft 和 Cisco 认证，以及 Check Point、Citrix 和 IT Security 等课程。可以通过 Mike@MichaelJLester.com 与他联系。

# 关于技术编辑

Dave Odom（CISSP）是一位网络安全工程师，他对于设计并实现信息安全保障以支持安全方面的需求有丰富的经验，为无数商业和政府组织提供过服务，包括美国国防部、能源部、美国国税局等。他曾在美国海军服役十年，是美国国防部 Computer Network Operations 战术专家之一。在美国国家安全局工作时，他参与了海军和 Joint Red Teams 对 Defensive Information Operations 演习的规划和执行，并帮助开发和评估安全、防御策略。Dave 是个自由职业者，其工作包括：对 IRS 和 CSIRC 提供的安全分析支持、一家第二层 ISP 的网络工程师以及 Titan Corporation 和 Logical Security 的技术课程开发者。他在美国海军研究生院对无线网络协议的安全性进行了广泛的研究，拥有诺福克州立大学的计算机科学本科和海军研究生院的硕士学位。他是 ISC2 和 Infragard 宾夕法尼亚匹兹堡分会的成员。

# 献　辞

Shon Harris 要感谢其他作者和团队成员，感谢他们对本项目的支持。

Allen Harper 要感谢他了不起的妻子 Corann，女儿 Haley 和 Madison，感谢她们在本书漫长编写过程中的支持与理解。尽管并没有用言语表达出来，她们是他生活中最重要的部分。他还要感谢他的朋友和业务上的合作者，从他们那里，他获得了鼓励和忠告。

Chris Eagle 要感谢他的孩子 Jasmine、Daniel 和 Tessa，对他们在编写本书期间的耐心表示感谢。他还希望，如果他母亲看到他已经能够连贯地写出两个以上的句子时，不至于激动得昏倒。

Jonathan Ness 要感谢他迷人的妻子 Jessica，没有她，他就无法完成本项目。他还要感谢他的家庭、指导者、教师、合作者和朋友，他们指导了他的方向，对他的成功贡献良多。

Mike Lester 要感谢他父母为他提供了良好的基因，感谢 Shon Harris 和其他作者，感谢 McGraw Hill/Osborne 的所有工作人员的指导，感谢他女朋友的爱和耐心。

# 前　言

本书的作者都是安全界的专业人士，他们致力于以正义、负责的工作方式，来改进个人、公司、国家的整体安全态势；本书的目标读者也是这样的人。

# 简　介

“创造和平的最佳手段是，准备好迎敌。”

——乔治·华盛顿

“一千个朋友不见得能使你忙碌，一个敌人就足以让你处处碰壁。”

——拉尔夫·瓦尔多·爱默生

本书的目标是帮助提高安全人士的技术，使之能够更有效地防御恶意的攻击行为。事实一次又一次地证明，理解敌人的策略、技巧、工具和动机是多么重要。公司和国家都有很多非常执著而有才华的敌人。我们必须通力协作，理解敌人的方法和步骤，以确保我们能够真正地挫败其破坏性的恶意行为。

本书的作者打算向读者传授一些他们认为业界需要的知识：对正义黑客的整体评估是，负责任的、无论行为和意图都是正义的。笔者之所以在本书开始就明确定义正义黑客，是因为目前社会对这个概念的认识极其模糊。

在本书的第 1 部分，笔者拟定了灰帽黑客的基本道德规范，以及对灰帽黑客的期望。本部分的内容有：

- 介绍白帽、黑帽、灰帽黑客的定义和特征。
- 列出正义黑客在工作时所遵循的步骤。
- 纵览与黑客和许多其他类型恶意活动相关的法律问题。
- 概述正确的漏洞发现过程（具体的模型将在后文介绍）。

在第 2 部分，笔者将介绍更先进的渗透方法和工具，在其他书中都没有完全涵盖；许多书籍只讲述了一些比较老旧的工具和方法，而这些都已经改头换面许多次了。笔者打算深入到真实的灰帽黑客工作中，讲述一些高级的机制。在本节中，笔者将讨论下列主题：

- 如何建立测试团队和实验室。
- 如何在所进行的工作中，合法地保护自己。
- 高级的嗅探工具、rootkit 和认证工具，包括工具的使用方法、缺点，如何改进功能等。
- 自动渗透试验方法和工具。

在第 3 部分，笔者将深入到代码中，向读者讲授操作系统和应用程序的特定组件的工作方式，以及如何对其进行攻击。在本部分中，笔者将讨论下述主题：

- 理解本部分其他内容所需的基础知识和概念。
- 如何对栈操作，如何识别缓冲区溢出，如何溢出缓冲区。
- 如何识别高级的 Linux 和 Windows 漏洞，如何攻击漏洞。
- 如何创建不同类型的 shellcode 来实施攻击，如何开发必要的软件来测试并识别漏洞。

在第 4 部分，笔者将更深入地讨论正义黑客相关的最高级的主题，其中有许多安全从业者目前尚不了解这些内容。在本部分中，笔者将讨论下述主题：

- 被动分析和主动分析工具和方法。
- 如何在源代码和二进制文件中识别漏洞。
- 如何对软件进行逆向工程，如何反汇编。
- 杂凑和调试技术。
- 对二进制代码和源代码打补丁，缓解漏洞造成的问题。

如果读者打算深入了解正义黑客，本书就是为你而准备的。

笔者对读者的任何想法和评论，都非常欢迎，请通过电子邮件告知我们，笔者的邮箱是 GrayHat@logicalsecurity.com。此外，与本书和正义黑客相关的附加技术信息和资源，可以浏览 www.logicalsecurity.com。

# 目　录

## 第 1 部分　泄密的道德

# 第 2 部分 渗透测试与工具

# 第3部分 攻击101

# 第 4 部分 漏洞分析

# 第 1 部分

# 泄密的道德

- **第 1 章**　正义黑客的道德规范
- **第 2 章**　正义黑客与法制
- **第 3 章**　完全而道德的揭密

CHAPTER

# 正义黑客的道德规范

**信息安全领域的专业人员需要了解：正义黑客在信息安全中所处的位置，如何对黑客工具适度利用，不同类型的黑客技术，和围绕所有这些问题的道德规范。本章将涵盖以下内容：**

- **正义黑客在当今世界的作用**
- **漏洞评估 vs 渗透测试**
- **安全专业人员如何使用黑客工具**
- **黑客和安全专业人员使用黑客工具的一般步骤**
- **白帽黑客和黑帽黑客之间的道德问题**

本书写作的目的，不是给心怀恶意者提供破坏工具，本书提供给希望拓展或熟练技巧的人，以抵御此类攻击或破坏行为。

我们先来看一下这方面常见的问题，并以此作为出发点。

本书写作的目的，是为了使当今的黑客能够更有效地进行破坏吗？

**回答**：否。下一个问题。

那么笔者究竟为什么要讲授如何进行破坏呢？

**回答**：如果你不了解所面临的威胁，就无法适当地保护你自己。此目的在于识别并阻止破坏和犯罪，而非引发。

我不相信你。恐怕写这本书，只是为了利润和版税吧？

**回答**：本书写作的目的，实际上是向信息安全从业者讲授坏家伙们已经了解的知识和正在进行的行为。版税当然是多多益善，因此请务必买两本。

仍然觉得没有说服力？为什么全世界的军队都研究敌人的兵法、武器、战略、技术呢？因为对敌人的了解越深入，就越了解应该采用何种保护机制来防御自身。

大部分国家的军队都会以许多形式进行战斗演习。例如，空军将他们的队伍分为“好

人”和“坏人”，坏人会使用敌方的某一特定战术、技巧和战斗方法。这些演习的目标在于使飞行员能够理解敌方的攻击方式，能够识别出特定的进攻行为并准备应对，再以正确的防御方式作出反应。

从飞行员的实战演习，到公司通过实际演练来保证信息安全，对读者而言思维跳跃可能较大，但二者涉及的都是相应的团队需要保护的东西和相关的风险。

军队试图保护其国家和所属财产。在全世界范围内，一些政府已经明白，它们花费了数百万到数十亿美金来保护的财产，现在仍然受到不同的威胁。坦克、飞机和武器仍然需要保护，以避免被炸毁。这些保护，现在都依赖于软件来实现，但这些软件可能随时被黑客侵入而遭受攻击或者破坏，例如，投弹的坐标可以被修改。各个军事基地仍然需要通过空中侦察和秘密警察保护，这是所谓的物理安全性。空中侦察是使用卫星和飞机监视远处发生的可疑的活动，而秘密警察则监控进出基地的入口。类似于当今的每一个组织，军事基地的保护在相当程度上依赖于软件，而现在又有如此多的通信方式可用（互联网、外部网、无线网络、租用线路、共享广域网线路等等），因此需要有另一种不同类型的“秘密警察”，来监控基地所有此类入口。

当然，读者的公司并不会保存有关阿富汗驻军的行动计划之类的顶级秘密信息，也不会有本·拉登的藏身位置，更不需要保护原子弹的发射密码。但这是否意味着读者不需要关注安全问题，不需要了解对策呢？不。军队需要保护其资产，读者同样也需要。

保护军事基地的例子看起来是极端了一点，让我们来看一下由于在信息安全方面准备不足，许多公司和个人所经历的大量黑客挑战吧。

表 1.1 引自 USA Today，给出了全世界范围内的公司和组织，为度过目前为止最恶劣的一些恶性软件所造成的危机并清除其影响所耗费的代价。

| 年份 | 病毒/蠕虫 | 估计损失 |
|---|---|---|
| 1999 | Melissa 病毒 | 8 千万美元 |
| 2000 | Love Bug 病毒 | 100 亿美元 |
| 2001 | Code Red 蠕虫 I 和 II 型 | 26 亿美元 |
| 2001 | Nimda 病毒 | 5.9~20 亿美元 |
| 2002 | Klez 蠕虫 | 90 亿美元 |
| 2003 | Slammer 蠕虫 | 10 亿美元 |

**表 1.1　恶性软件损害估计（来源：USA Today）**

有关恶性软件一个有意思的现象是，许多人认为它与黑客入侵不同。但事实上，恶性软件已经衍变为黑客行为的一种最复杂、最自动化的形式。攻击者只需用一些前期努力来