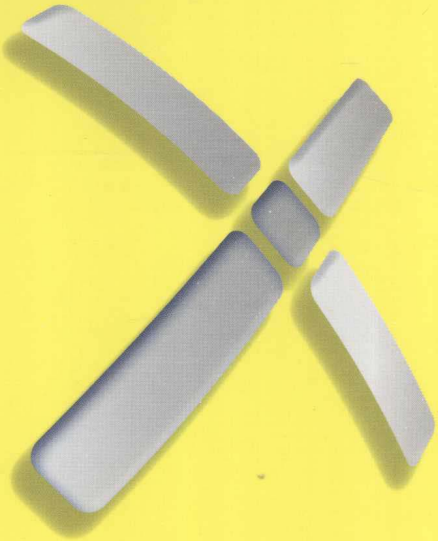
HZ BOOKS
华章科技

ELSEVIER

Amazon五星级超级畅销书，美国国家安全局主管Keith B. Alexander将军（向奥巴马汇报）鼎力推荐！
以独创性的ZEH方法，结合前沿、实用的开源工具，采用科学、有序的四步模型，高级渗透测试专家为你呈现渗透测试和黑客活动的领域全景！
以“大道至简”的思维方式，配以代表性极强的完整案例，系统讲解渗透测试必知必会的工具和方法。

安全技术大系
SECURITY



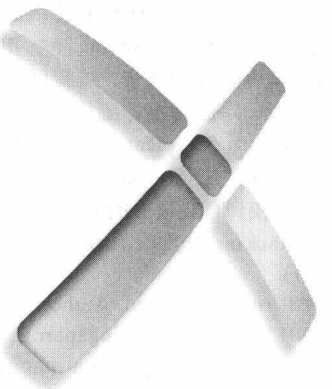
The Basics of Hacking and Penetration Testing
Ethical Hacking and Penetration Testing Made Easy

# 渗透测试实践指南
## 必知必会的工具与方法

（美）Patrick Engebretson 著
缪纶 只莹莹 蔡金栋 译

机械工业出版社
China Machine Press

安全技術大系
SECURITY



The Basics of Hacking and Penetration Testing
Ethical Hacking and Penetration Testing Made Easy

# 渗透测试实践指南

## 必知必会的工具与方法

（美）Patrick Engebretson 著
缪纶 只莹莹 蔡金栋 译

机械工业出版社
China Machine Press

这是一本权威而实用的渗透测试实践指南，Amazon 超五星畅销书，美国国家安全局主管鼎力推荐，被誉为学习渗透测试必读的书之一。以独创性的 ZEH 方法，结合前沿、实用的开源工具，采用科学、有序的四步模型，全面讲解了渗透测试的技术、工具和方法，同时结合大量的演示实例，配以详细的操作步骤和图文解说，适合作为系统学习渗透测试的参考书。

全书共分 7 章：第 1 章介绍了渗透测试的概念、常用工具（Backtrack 等）、测试环境的搭建，以及四步模型法；第 2 章讲解了 HTTrack、Google 搜索指令、The Harvester（邮箱地址侦察）、DNS 和电子邮件服务器信息提取、MetaGooFil、筛选信息技巧等侦察工具和手段；第 3 章讲解了 ping 命令、ping 扫描、端口扫描涉及的切实可用的工具及参数设置，如 Nmap、Nessus 等；第 4 ～ 5 章解读了漏洞利用的过程、工具和技巧，包括获得远程服务访问权限、密码重置和破解、嗅探网络流量、自动化漏洞攻击和 Web 漏洞扫描、Web 服务器扫描、拦截请求、代码注入、跨站脚本等流行的黑客技术及工具；第 6 章介绍了使用后门和 rootkit 的方法及注意事项，侧重讲解 Netcat、Cryptcat、Netbus 工具和常用 rootkit 的使用、检测和防御技术；第 7 章着重介绍了如何编写渗透测试报告。每一章的结尾都有扩展阅读，包括对一些工具的介绍和相关深入主题的讲解，使有兴趣的读者可以找到自我提升的方向。



**本书版权登记号：图字：01-2012-5190**

**图书在版编目（CIP）数据**

渗透测试实践指南：必知必会的工具与方法 /（美）恩格布雷森（Engebretson, P.）著；缪纶，只莹莹，蔡金栋译 . —北京：机械工业出版社，2012.11

书名原文：The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy

ISBN 978-7-111-40141-4

Ⅰ . 渗… Ⅱ . ① 恩… ② 缪… ③ 只… ④ 蔡… Ⅲ . 计算机网络 – 安全技术 Ⅳ . TP393.08

中国版本图书馆 CIP 数据核字（2012）第 248190 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：高婧雅

北京京师印务有限公司印刷

2013 年 1 月第 1 版第 1 次印刷

186mm×240mm • 11.5 印张

标准书号：ISBN 978-7-111-40141-4

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

购书热线：（010）68326294；88379649；68995259

投稿热线：（010）88379604

读者信箱：hzjsj@hzbook.com

# 译 者 序

本书是软件安全领域的“思想方法学”。所谓“大道至简”就是以简单化的思维去思考复杂的事物。对于普通人来说，“黑客”、“渗透测试”是如此深不可测。本书即以“大道至简”的方式，剥去“黑客”的神秘外衣，挥动奥卡姆剃刀，去粗取精，用“少而精”的论述，描绘了“多而广”的“黑客”理论。

本书提出了一个体系化的概念，系统介绍了“道德黑客”以及“渗透测试”应该掌握的知识，从最初的搜集信息到漏洞扫描，再到漏洞利用以及维持访问，本书用一个四步模型方法论体系直观地阐述了完成一个完整的渗透测试所需要的所有工作内容。书中不仅阐述了基本概念，还包含了大量的演示实例，有很强的实际指导意义，而且每一个实例都给出了详细的操作步骤及图文解说，方便读者快速掌握渗透测试的原理和技术。书中的内容基于实践，但却高于实践，从更高的理论层次指导读者怎样学习黑客知识和渗透测试。

本书的读者群主要是网络与信息安全领域的爱好者，以及从事渗透测试与黑客活动研究的安全从业人员。作者将看上去艰深的渗透测试话题，用生动易懂的语言娓娓道来，深入浅出，带领读者迅速跨入渗透测试的门槛。一个合格的渗透测试者不能逾越“道德”的范畴，需要在合法的授权范围内进行恰当的行为操作。真诚期待读者以本书为起点，不断发散和完善自己的知识链，并一次次勇敢地把已经掌握的知识抛到脑后，去迎接新的挑战。

本书的翻译组织工作由我全面负责。第 1 章、第 3 章、第 6 章、第 7 章由我和只莹莹翻译并审校，作者简介、前言、第 2 章、第 4 章、第 5 章由我和蔡金栋翻译并审核。

翻译本书的过程有快乐，也有痛苦。虽然我一直关注国内外信息安全领域的相关动态，但是这却是我第一次翻译英文专业书籍，就像教师第一次走向讲台，我很激动，也有些担忧。鉴于原著在 Amazon 排行榜上的影响力，

我担心自己把握不好原著恰到好处的笔锋，担心自己翻译不出原著将初学者吸引到渗透测试领域中的魅力。因此，我对这次翻译非常用心，与两位合作者一起查阅了大量相关资料，力求做到专业词汇准确权威，内容正确，意译部分既不失原著意境又无偏差。

现在，我怀着期盼和忐忑的心情，将这本译著呈献给大家，渴望得到您的认可，更渴望和您成为朋友，如果您有任何问题和建议，请与我联系（lunmiao@tom.com），让我们一起探讨，共同进步！

感谢机械工业出版社对我的信任，感谢我的领导王冠华、阎继军给予的指导和大力支持，以及我的同事王志璋、叶茂、段媛媛对我的帮助，特别要感谢家人的支持和理解。

缪　纶

# 前　言

当你打算阅读本书时，我想会有几个问题萦绕在你的脑海中：本书读者对象是谁？这本书与其他书（在这里插入你最喜爱的书名）有什么不同？我为什么要买这本书？这些都是很平常的问题，而且我正在让读者为其支付他们辛辛苦苦赚来的现金，所以为这些问题提供一些答案是很重要的。

对于有兴趣学习黑客技能和渗透测试的人来说，进入一个琳琅满目的书店就如同在 amazon.com 搜索关于“黑客”的书籍那样让人迷惑。最初，似乎是有无尽的选择让人从中挑选。最大的书店都会为计算机安全书籍设立几个书架，包括编程安全、Web 应用安全、rootkit 和恶意软件、渗透测试方面，当然，还有黑客方面的书籍。然而，即使是关于黑客的书籍，它们在内容和题材上似乎也各不相同。有的书侧重于使用工具，但不讨论如何将这些工具结合在一起。其他书籍侧重于黑客领域中的某个特定主题，却缺乏对大局的论述。

本书旨在解决上述问题，它是任何对黑客活动或渗透测试知识感兴趣的人的起点。本书会涉及具体的工具和知识点，并且还将研究如何将这些工具结合在一起，探讨如何利用这些工具成功地完成任务。

## 本书读者对象

本书是关于黑客活动和渗透测试的一个非常易懂但却很彻底的指南。它特别注重帮助读者掌握完成一次黑客攻击或渗透测试所需的基本步骤，而且不会让你感到不知所措。当你阅读本书后，将会对渗透测试过程有一个扎实的理解，并且能自如地运用所需要的基本工具来完成工作。

需要强调的是，本书面向从事黑客活动和渗透测试的新手和那些很少或根本没有经验的人们，也面向那些因无法顾全大局（各种工具和各个阶段是如何结合在一起的）而感到沮丧的人们，或那些希望学习到更多有关威慑安全相关知识的人们。

总之，本书是为所有对计算机安全、黑客活动或渗透测试感兴趣，但没有经验、不知道从哪里开始的人们撰写的。我和一位同事称这个概念为“黑客入门”（Zero Entry Hacking，ZEH），就像现在的游泳池，入门级游泳池由浅到深逐渐倾斜，初学者涉水时不会有被淹没的感觉，也不用担心溺水。“入门”这一概念允许每个人都能够使用这个“游泳池”，不论年龄或能力。本书采用了类似的技术。ZEH 旨在揭示基本概念而不会令人感到不知所措。掌握 ZEH 将为你将来学习更高级的课程和阅读更深入的书籍打下坚实的基础。

## 本书与其他书有什么不同

当不与我的家人共度时光时，我喜欢做两件事情：阅读和从事与黑客相关的活动。大部分时间，我通过阅读有关黑客方面的书籍来将这两个爱好结合起来。可以想象，作为一名教授和渗透测试者，我书架上排列着许多有关黑客、安全和渗透测试方面的书籍。如同生活中大多数事情一样，每本书的质量和价值是不一样的。有些书是非常优秀的资源，书读百遍以至于这些书籍的封面差不多都破碎了。另外一些书籍提供的帮助则比较少，一直崭新如一。一本能够很好地解释细节且没有失去读者的书，如同金子般珍贵。遗憾的是，大多数我喜爱的书籍都已经磨损和破碎，它们要么特别厚（500 页），要么内容针对性强（单一主题的深入指南）。这并不是什么坏事，事实上，正好相反，它们内容详尽且清晰，因此它们都是非常棒的书籍。但同时，侧重详细安全性主题的大型巨著似乎会使新手不知所措。

遗憾的是，对于进入安全领域的初学者和想学习道德黑客的人来说，那些向他们介绍黑客知识基本原理的书籍，既令人望而却步又使人困惑。本书在两个方面与其他书籍有所不同。首先，它适合初学者（运用“入门”的概念）。如果你从来没有执行过任何类型的黑客活动，或已经使用了一些工具但不是很确定下一步要做什么（或不知道如何解释工具的输出结果），那么本书是为你准备的。我们的目标不是让你迷失在细节中，而是为你呈现整个领域的全景。

当然，本书仍然会介绍每一个用于完成渗透测试步骤所需要的主要工具，它不仅会深入地探究每一个工具，并且还会详细讲解它们的附加功能。从这个观点来看，这样的讲解有助于本书将重点集中到基本知识介绍上，而且在

很大程度上，可以使我们避免陷入由工具版本的高级功能或细微差别所带来的困惑中。

例如，3.3 节将介绍如何使用常用的端口扫描器 Nmap 来运行基本扫描。因为本书侧重于基础知识，所以到底运行哪个版本的 Nmap 就变得不那么重要了。不管你使用的是 Nmap 版本 2 或版本 5，执行 SYN 扫描是完全一样的，没有什么不同。我们将尽可能地采用这个技巧，这样读者可以在学习 Nmap（或任何工具）过程中不必担心功能的变化，因为往往由于版本的改变，会随之带来一些高级特性。

本书旨在介绍通用的知识，这有助于读者将来理解更前沿的主题。请记住，一旦扎实地掌握了基础知识，就可以随时回过头来学习具体的细节并掌握工具的高级功能。此外，每章结尾都会建议性地介绍一些工具和深入的主题，这些工具和主题超出了本书的范围，但你可以做进一步研究从而增进知识层次。

本书不仅仅是为初学者编写的，实际上它以一种非常独特的方式呈现信息。我们在书中使用的所有工具和技术将会以少量的机器作为目标，并以一种特定的顺序进行实践。（所有目标机器将属于同一子网，读者将能够轻松地重建这个“目标”网络。）读者将会了解如何解释工具的输出，以及如何利用输出继续后续的攻击。

本书使用了一个贯穿全书且有先后次序的例子来帮助读者了解渗透测试的全景，而且这个例子可以使读者更好地理解各种工具和各个阶段是如何结合在一起的。这与如今市场上的许多其他书籍不同，这些书籍通常会讨论各种工具和不同的攻击手段，但未能解释如何有效地将这些工具衔接在一起。本书为读者清楚地解释了渗透测试的某个阶段是如何向另一个阶段过渡的。以这种方式呈现信息，可以为读者提供宝贵的经验，并可让他们通过简单地模仿书中的例子完成整个渗透测试过程。这种方法可以帮助读者清楚地理解基础知识，同时了解各种工具和各个阶段是如何相互关联的。

## 为什么要购买本书

对于这个问题，我们在前面已经给出了直接的回答，下面我们将这一问题的答案以列表的形式呈现出来：

- 你想了解更多有关黑客活动和渗透测试方面的知识，但不确定从哪里开始。
- 你已涉足黑客活动和渗透测试，但不知道如何将各部分结合在一起。
- 你想了解更多有关黑客和渗透测试者为获得网络和系统的访问控制权限所使用的工具以及实现的过程。
- 你在寻找学习威慑安全知识的理想入手点。
- 你喜欢挑战。

# 致　谢

像多数人一样，我也有我的人生理想，其中既包含了我的人生目标，也囊括了我渴求有一天能够实现的梦想。在我所有的人生理想中，有目标宏大的，也有微不足道的，有目标明确、稳定而具体的，同时也有短暂、模糊不清、瞬间万变的——就像清晨卢森（Lutsen）山脉上的迷雾，不断变化和移动，时隐时现。显然，我的理想并不是磐石一块，在我生命的历程中，它在不断变化和更新。但是，有一些事情一直停留在那里，它们如同拉什莫尔（Rushmore）山一样矗立在我的生命中。它们就像数百英尺高、雕刻坚实的花岗岩一样，从未改变。无论生活经历多少风暴和沧桑，它们一直优雅地站在那里，静静地等待着我有一天去完成。它们有些是高尚的，有些是自私的，有些甚至是异想天开的。我有幸在我生命中能够完成许多项目，甚至是大的项目。本书代表我完成了一个“拉什莫尔”项目。它肯定是一个总统级的项目。（虽然我不确定它实际代表的是哪一位总统！）

如同生活中大多数事情一样，本书，你看到的最终产品，是许多人心血和精力的结晶。所以，当我完成它并且我的名字出现在封面上的时候，请不要认为本书是我个人的创作。如果没有所有参与者的奉献、支持、帮助和意见，毫无疑问，现在，你不会阅读到这些文字。书写一段适当的“致谢”，如果要列出相关的每个人，将会填满许多许多页纸，因此，在下面，你将会看到一个简单的致谢。如果忘了提到任何人，我提前道歉。

## 我的妻子

用什么语言或用什么方式才能表达你对我的重要性呢？毫无疑问，你为本书所付出的努力与我一样多。你给予我鼓励的翅膀，让我飞翔，在我工作时，你默默支持我，日日夜夜做出奉献。当我需要你更多的帮助时，你从不抱怨，从不拒绝，并且一直笑脸相迎。不是每个男人都是这么幸运的。因为有了你才成就了今天的我，谢谢。

## 我的女儿们

我的小宝贝，你们是我生命的荣耀！我道歉，为所有的清晨、深夜和长长的周末，使你们错过了在日光室上演的小人们、Mary 和 Joseph、公主们、芭比娃娃和海盗船！爸爸爱你们超过生活本身。

## 我的家庭

感谢我的父亲、母亲给予我的礼物——教育，他们让我明白辛勤工作对项目奉献的价值。也感谢我的另外一位母亲，她花费无数个小时阅读和修改我的草稿。

## 致出版社团队

感谢这次机会，感谢编辑团队。我感谢你们为这个项目的所有辛勤工作和奉献。特别感谢 Angelina Ward，她最终获得了该项目许可；感谢我的编辑 Heather Scherer 为这本书付出了无数的时间和协助；感谢 James Broad 在整个技术审校过程中的慧眼和好建议。想了解更多新闻和有关本书所发生的事情，或其他与安全相关的内容，请随时在 Twitter 上关注 pengebretson 或访问我的主页 http://homepages.dsu.edu/pengebretson。

# 目　录

# 第 1 章

# 渗 透 测 试

**本章知识点**

- Backtrack Linux 介绍
- 使用 Backtrack：启动引擎
- 黑客实验环境的搭建与使用
- 渗透测试的步骤

## 1.1 内容简介

渗透测试是一种合法且授权定位计算机系统，并对其成功实施漏洞攻击的方法，其目的是为了使这些受测系统更加安全。测试过程包括漏洞探测和提供概念证明（Proof of Concept，POC）攻击，以证明系统漏洞确实存在。一个恰当的渗透测试会在完成之后，标明发现的系统漏洞并给出明确的修补意见。总之，渗透测试用于加强计算机和网络系统的安全性，让它们在未来的使用中免遭攻击。

渗透测试（Penetration Testing 或者 Pen Testing，PT）也称为：

- 黑客活动（Hacking）
- 道德黑客（Ethical Hacking）
- 白帽黑客（White Hat Hacking）

我们有必要花些时间讨论一下渗透测试和漏洞评估（vulnerability assessment）之间的区别。许多安全领域中的人士（还有厂商）在使用时都会混淆这两个术语。所谓漏洞评估是检查系统和服务是否存在潜在安全问题的过程，而渗透测试则是通过执行漏洞利用和概念证明（POC）攻击来证明系统确实存在安全隐患。渗透测试能够模拟黑客行为并提供攻击载荷

（payload），它比漏洞评估更进一步。本书将把漏洞评估的全过程作为完成渗透测试众多步骤之一进行介绍。

## 搭建平台

掌握黑客活动和渗透测试的核心就是要理解其中的所有不同角色以及它们的作用。我们先对其进行粗线条描述。请注意，虽然下述内容是概要描述，但是可以帮助读者理解这些密切相关的不同角色之间的差别。

我们借用电影《星球大战》为例进行理解。在影片中，宇宙中存在着两种“原力”：绝地（Jedis）和西斯（Siths），分别代表正义和邪恶。双方都拥有不可估量的能力。一方将自己的能力用在保卫和服务上，而另一方则用在私利和掠夺上。

学习黑客技术与学习如何使用原力非常相似（我是这么认为的！）。你学到得越多，你的能力就越强。到了最后，你必须决定如何使用你的能力，是用来做好事还是做坏事。《星球大战》前传 I 有一张经典的海报，海报上是孩提时代的阿纳金（Anakin）。如果你仔细观察海报上阿纳金的影子，你会发现这个影子其实是达斯·维德（Darth Vade）的轮廓。你可以上网搜索一下“阿纳金·达斯·维德的影子”去亲自验证一下。知道这张海报为什么如此有吸引力是很关键的——作为一个孩子，阿纳金并不打算成为达斯·维德，但是结果却不可避免。

如果掌握黑客技能的人都不会变成超级恶棍，那么我们所处的环境可能是安全的，问题是人性走向邪恶的过程是不知不觉的。所以，如果你想成为精英，被同行们尊重，并且能够就职于安全行业以及拥有高薪，那么你就必须将能力用在从事正当的安全保障和服务工作上。你一旦有了犯罪记录，也就没有机会再从事其他的职业了。事实上，当前合格的安全专家非常匮乏，即使如此，也不会有老板愿意冒险雇有犯罪前科的人做他的雇员，特别是对那些涉及计算机犯罪的人更是如此。

在渗透测试领域里，人们通常使用“白帽”和“黑帽”这两个术语来描述绝地和西斯。本书中，我们会交替地使用“白帽”，“道德黑客”或“渗透测试者”这些术语来代表绝地。用“黑帽”、“破解者”或“恶意攻击者”来表示西斯。

值得注意的是，道德黑客与恶意攻击者采用一样的工具完成相同的活动。在任何情况下，道德黑客都应当力求以真正的黑帽黑客的方式来做事和思考。渗透测试模拟现实环境中的攻击，其仿真程度越高，能给购买渗透测试服务的客户带来的价值就越多。

请注意前一段提到的“在任何情况下”。即使白帽使用与真正的黑客攻击完全相同的工具完成相同的任务，他们也完全是两回事。本质上，他们的差异可归纳为三个主要方面：授权、动机和意图。需要强调的是，这三点并不能完全涵盖他们之间的不同之处，但是可以用它们来判断某一行为是道德的还是恶意的。

区分白帽和黑帽最直接、最简单的方式就是看其是否是授权的。所谓授权就是在进行任何测试和攻击前要先获得许可。获得授权后，渗透测试人员和被审计公司必须协商测试范围。该范围要包括一些明确信息，诸如对哪些资源和系统进行测试。在该范围中，要对渗透测试者有权进行测试的目标给出明确的限定。充分理解渗透测试的授权目标和范围对双方来讲都是很重要的。白帽必须始终遵守授权，并限制其行为在上述范围之内。黑帽则不会遵从此约束。

区分道德黑客和恶意攻击者的第二种方法是审查他们的动机。如果攻击者被一己私利所诱惑和驱使，通过敲诈、欺骗、报复等卑鄙手段来获得财富或名利，那么他（或她）就应认定为黑帽。反之，如果攻击者获得了预先授权，他（或她）的目的是帮助机构提高安全性，那么他（或她）就应认定为白帽。

最后，如果其意图是为机构提供一次真实的攻击模拟，以期该机构可以对漏洞进行早期发现和缓解，那么这样的攻击者应该被认为是白帽攻击者。白帽与黑帽另一个重要的本质区别是白帽会对渗透测试结果保密。道德黑客永远不会向除客户之外的任何人提供渗透测试中获取的敏感信息。但是，如果是为了个人的利益或目的去攫取信息，那就是黑帽黑客的行为了。

## 1.2 Backtrack Linux 介绍

几年前，公开讨论和教授黑客技术是不允许的。幸运的是，随着社会的

发展人们开始逐渐认识到威慑安全（offensive security）的重要性。目前，威慑安全正被不同规模不同行业的机构所接受。许多政府已经公开声明他们正积极地建设和发展威慑安全能力。

从根本上说，渗透测试应当在企业的整体安全方面发挥重要作用。就像政策规划、风险评估、业务持续性计划和灾难恢复已经成为维护企业安全不可或缺的组成部分一样，渗透测试也需要成为企业整体安全规划中的一部分。渗透测试会让你用敌对的眼光审视自己的企业。这会带给你许多意外的发现，让你在遭受真正的黑客攻击之前进行系统漏洞的修补。

令人高兴的是，当前存在大量非常有用的工具可以帮助我们掌握黑客知识。这些工具不仅易用，而且经过多年的发展，很多已经非常成熟了。更重要的是，大多数工具都是免费的。本书介绍的**每一个**工具都是免费的。

完成一次基本的渗透测试，不仅要知道所需工具是否免费，还要懂得如何查找、编译和安装工具。虽然这一过程在现今的 Linux 操作系统上已经变得非常简单，但对于新手来说还是会有些畏惧。大多数人开始的时候会对学习如何使用工具更感兴趣，却忽略了通过 Internet 搜索来全面了解如何安装和配置工具。

说句公道话，你真的应该知道如何在 Linux 系统上手动编译和安装软件，或者最起码，你应该能够熟悉 apt-get 指令（或类似其他指令）。

**拓展知识**

APT（Advanced Package Tool，高级软件包工具）是一个打包管理系统。APT 允许使用命令行的方式，快速便捷地安装、更新、删除软件。除了简单以外，APT 最大的优势是它可以自动解析软件之间的依赖关系。也就是说，如果安装的软件包还需要其他软件，APT 会自动地定位并安装这个软件。这种自动解析软件依赖关系的方法是对过去“依赖地狱”（dependency hell）的重大改进。

通过 APT 来安装软件非常直观。举例来说，假如你想安装网络映射工具 Cheops。只要你知道了想要安装的软件包的名字，在命令行输入 apt-get install 加软件的名字即可。安装软件之前最好先运行 apt-get update，这样可以确保获得安装软件的最新版本。安装 Cheops 时，需输