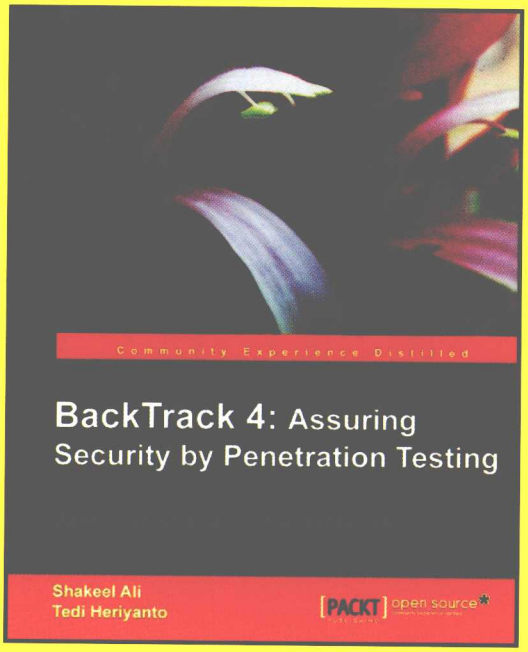
HZ BOOKS
华章科技

全面剖析BackTrack平台，分类介绍各种网络渗透测试工具
一整套针对BackTrack平台的渗透测试流程，其中各个环节分工明确、层层递进，并涵盖了所有主流的测试类型

安全技术大系
SECURITY

[PACKT]
PUBLISHING



BackTrack 4

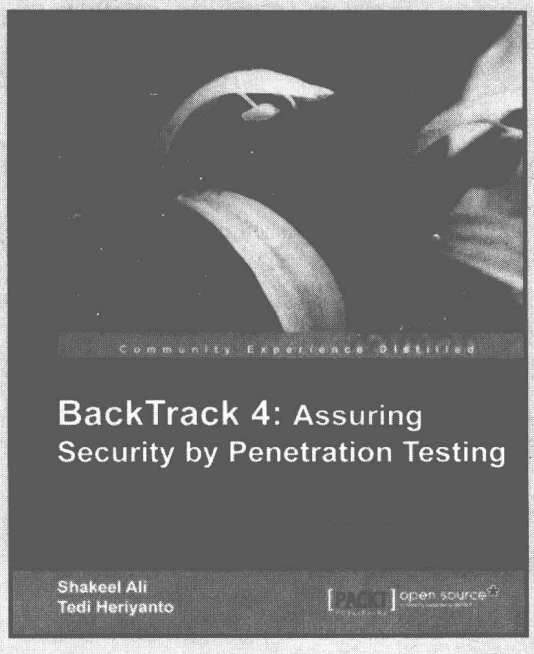
利用渗透测试保证系统安全

BACKTRACK 4: ASSURING SECURITY BY PENETRATION TESTING

（英）Shakeel Ali　Tedi Heriyanto　著
陈雪斌　赵见星　莫凡　译

机械工业出版社
China Machine Press

安全技術大系
SECURITY



BackTrack 4

利用渗透测试保证系统安全

BACKTRACK 4: ASSURING SECURITY BY PENETRATION TESTING

（英）Shakeel Ali　Tedi Heriyanto　著
陈雪斌　赵见星　莫凡　译

机械工业出版社
China Machine Press

本书系统介绍 BackTrack 操作平台以及利用渗透测试保证系统安全的方法。从环境准备和测试流程开始，演示了最基本的安装和配置过程，介绍了渗透测试的分类（白盒测试和黑盒测试），揭示了开放式安全测试的方法，并提出了一套针对 BackTrack 平台的渗透测试流程。本书把这个功能强大的渗透测试平台的工具分成几大类别：目标范围划定、信息收集、目标发现、目标枚举、漏洞映射、社会工程学、目标利用、提权、持续控制目标、报告，并介绍了这些工具的正确使用方法。对每一款工具的介绍都配以实际案例来突出其用途和典型配置。除此之外，还提供了一些珍贵的私房工具，以及重要资源的链接。

本书适合网络安全技术人员以及安全技术爱好者参考。

Shakeel Ali，Tedi Heriyanto: *BackTrack 4:Assuring Security by Penetration Testing* (ISBN: 978-1-849513-94-4).

本书版权登记号：图字：01-2011-6859

图书在版编目（CIP）数据

BackTrack 4：利用渗透测试保证系统安全 /（英）阿里（Ali, S.），（英）赫里扬托（Heriyanto, T.）著；陈雪斌，赵见星，莫凡译 . —北京：机械工业出版社，2011.12

书名原文：BackTrack 4：Assuring Security by Penetration Testing

ISBN 978-7-111-36643-0

I. B… II. ①阿… ②赫… ③陈… ④赵… ⑤莫… III. 互联网络－安全技术－应用软件，BackTrack 4 IV. TP393.408

中国版本图书馆 CIP 数据核字（2011）第 243544 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：吴　怡

北京市荣盛彩色印刷有限公司印刷

2012 年 1 月第 1 版第 1 次印刷

186mm×240mm • 17.5 印张

标准书号：ISBN 978-7-111-36643-0

定价：59.00 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

“千丈之堤，以蝼蚁之穴溃；百尺之室，以突隙之烟焚。”——《韩非子·喻老》

在当今互联网时代，网络攻击和犯罪行为时刻都在发生，仅2011年下半年，就已相继爆出好几家知名跨国公司遭黑客入侵，丢失用户资料的事件。根据木桶原理，一个木桶的最大容量取决于组成该木桶最短的那块木板的长度；同样，一个组织的安全防御系统也往往是从最薄弱的环节被攻破，然后逐步蔓延到内部核心网络。因此，作为一名安全保障人员，有义务在系统遭受外部恶意攻击之前，提前找出所有可能被利用的薄弱环节，并予以修补和加固，从而提高组织的整体信息安全水平。

渗透测试作为一项专业的安全服务，在不破坏组织正常业务的前提下，模拟黑客可能的攻击行为，并从中发现当前系统架构中的薄弱环节和潜在安全隐患。如今已经有越来越多的企业开始认同这种测试方式，并积极地利用渗透测试来发现潜在问题，提高自身安全强度。渗透测试的实施者是整个测试的决定性因素，可以说直接影响到测试的成败。要想成为一名出色的渗透测试人员，必须具备丰富的理论知识和实践经验，以及良好的职业道德。本书以介绍当前最流行的渗透测试平台——BackTrack中的各种先进工具为主线，中间穿插各类安全测试相关的理论知识和最佳实践，来帮助读者深刻理解渗透测试流程，熟练掌握操作技巧。

本书最大的特点是理论与实践相结合。作者并不是简单地对渗透测试工具进行堆砌和罗列，而是加入了自己的思考，提出了一个使用BackTrack进行渗透测试的方法论。这一点非常重要。我见过一些刚接触安全测试的朋友，他们往往缺乏对渗透测试流程的整体认识，不知应该如何开始一次测试、测试应该分几个步骤、涵盖哪些方面、测试的期望输出是什么。最后在没有明确指导方针的情况下随意地使用几个工具进行测试，效果自然也不会很好。正所谓没有规矩，不成方圆，像渗透测试这样复杂多样、重复性较强的工作，有一个科学的方法论进行指导是非常有必要的。本书的作者们在其丰富的安全工作经验的基础上，提出了BackTrack测试方法论，其中各个环节分工明确、层层递进，并涵盖了所有主流的测试类型。即使是没有太多经验的新人，也能够在该方法论的指导下，使用书中介绍的各种工具，完成一次系统、规范而又全面的渗透测试。

本书由陈雪斌、赵见星、莫凡共同翻译，其中，陈雪斌负责第1～4章，赵见星负责第5～8章，莫凡负责第9～12章以及附录。在翻译过程中，我们对于一些有多种译名的术语进行了讨论，参考了网上和其他书籍，达成共识。由于时间紧迫，加之译者水平有限，译文难免有疏漏之处，恳请广大读者朋友批评指正。

陈雪斌

2011年11月7日

于南京

前　言

BackTrack 是一个渗透测试和安全审计平台，它包含了一系列先进的工具用于发现、检测和利用目标网络环境中的已知漏洞。通过定义明确的业务目标和测试流程，并采用合理的测试方法，BackTrack 能够帮助您完成对自身网络进行高质量的渗透测试。

本书是一部结构清晰、重点明确的专业书籍，通过对当前最前沿的黑客工具和技术进行详尽而有条理的演示，使读者能够掌握高实用性的渗透测试技术。本书从业务角度出发，提供了所有必需的环境搭建和测试步骤，从而模拟出现实世界中存在的真实攻击场景。

本书的作者们具有丰富的专业技术实践，向读者展示出当前产业环境下渗透测试的最佳实践。

本书是当前市面上第一本也是唯一的一本关于 BackTrack 操作平台的书籍，从环境准备和测试流程开始，演示了最基本的安装和配置过程，介绍了渗透测试的分类（包括白盒测试和黑盒测试），揭示了开放式安全测试的方法，并提出了一整套针对 BackTrack 平台的渗透测试流程。本书介绍了实际渗透测试中需要用到的数量众多的安全评估工具，将它们分成不同的类别（目标范围划定、信息收集、目标发现、目标枚举、漏洞映射、社会工程学、目标利用、提权、持续控制目标、报告），并介绍了这些工具的正确使用方法。对每一款工具的介绍都会配以实际案例来突出其用途和典型配置。除此之外，还提供了一些珍贵的私房工具，以及重要资源的链接。对于所有专业的渗透测试人员来说，这些资料能起到很大的帮助作用。

本书是一本具有很强专业性和实用性的指导书，旨在帮助读者从零开始掌握坚实的渗透测试技术。通过本书你将学会如何充分有效地在商业环境或实验平台下运用 BackTrack 系统。

本书将通过一个个精心组织的实例，教会你如何熟练掌握并使用 BackTrack 来发现、检测和利用漏洞。

本书涵盖的内容

第 1 章　初识 BackTrack　概要介绍 BackTrack，一个经过特殊定制开发以满足渗透测试需求的 Linux DVD 发行版。该章首先简要介绍了 BackTrack 的历史和它的各种功能，然后介绍如何获取、安装、配置、更新 BackTrack，以及如何在你的 BackTrack 环境中添加额外的工具。在本章最后，你可以学到如何根据自己的需求定制 BackTrack。

第 2 章　渗透测试方法论　介绍渗透测试的基本概念、规则、操作、方法，以及渗透测试的流程。你将学到如何清晰地区分两种流行的渗透测试方法：白盒测试和黑盒测试，以及漏洞评估和渗透测试的区别。该章还将介绍几种不同的安全测试方法论，包括它们各自的业务功能、性质和优点。这些方法论包括开源安全测试方法（OSSTMM）、信息系统安全评估框架

（ISSAF）、开放式 Web 应用程序安全项目（OWASP）和 Web 应用安全联合威胁分类（WASC-TC）。然后，介绍在遵守基本法律和道德伦理的基础上，使用 BackTrack 进行渗透测试的流程，该流程由 10 个相互连贯的步骤所构成。

第 3 章　目标范围划定　该章将介绍一套用于划定测试目标范围的流程，以规范化测试需求。该流程中定义和描述的各种要素，对于测试的实际实施将起到重要的指导作用。我们将介绍这个流程中包含的一些关键元素，诸如采集用户需求、准备测试计划、界定测试边界、定义业务目标，以及项目的管理和进度规划。还介绍获取、管理目标测试环境的相关信息。

第 4 章　信息收集　介绍渗透测试流程中的信息收集阶段。该章介绍一些相关工具和技术，它们的用途包括：从各种不同的文档类型中收集元数据（metadata），提取域名解析服务（DNS）信息，收集路由信息，此外还包括主动或被动的智能化的信息收集。还介绍一款实用小工具，用来对收集到的目标信息进行归档和组织。

第 5 章　目标发现　介绍如何发掘和识别测试目标。首先解释在渗透测试流程中，目标发掘阶段存在的理由，接着介绍一系列用于扫描并发现目标计算机的工具。该章最后会介绍几款可以区分目标计算机上操作系统的工具。

第 6 章　目标枚举　介绍目标信息枚举的整个流程及其作用，包括什么是端口扫描，不同类型的端口扫描方式，以及完成端口扫描所需要的一系列工具。还介绍如何根据开放的端口号来判断目标机上运行了什么服务。

第 7 章　漏洞映射　介绍两种最基本的漏洞类型：本地漏洞和远程漏洞。包括漏洞的分类方法，业界的漏洞分类标准和不同种类漏洞的特征，以及如何将任意的漏洞进行归类。该章包括一系列可以用来挖掘和分析目标环境中安全漏洞的工具，这些工具包括开放式漏洞评估系统（OpenVAS）、思科公司的设备分析工具、模糊测试（Fuzzing）工具、服务器信息块协议（SMB）分析工具、简单网络管理协议（SNMP）分析工具以及 Web 应用分析工具。

第 8 章　社会工程学　介绍了社会工程学专家们在诱使目标泄露自己的信息或采取特定行动时，所遵循的核心原则。包括一些基本的心理学知识，这些都是一个社会工程学专家能够取得成功的关键所在。讲解运用社会工程学进行攻击的步骤和方法，以及一个现实生活中使用社会工程学的案例。该章最后，提供了两款社会工程学工具，可以用来发掘被测试目标组织中的人员组成信息。

第 9 章　漏洞利用　重点介绍了一系列可以用于实战的漏洞利用工具和方法。包括漏洞研究领域的一些关键技术，从而帮助你理解、评估和利用漏洞。该章还将介绍一些公开的漏洞信息数据库和利用工具数据库，这样你就能查看到所有公开的漏洞信息和利用工具，并知道何时使用它们。你还将学到如何从安全评估者的角度出发来使用一款知名的漏洞利用工具。最后，你将掌握如何向 Metasploit 框架中添加一个新的漏洞利用模块。

第 10 章　提权　介绍一系列用于权限提升、网络嗅探和网络欺骗的工具和技术。包括使用通过攻击密码保护从而提升权限的工具，以及使用嗅探网络数据的工具。该章最后介绍几款可以用来发起网络数据欺骗攻击的工具。

第 11 章　持续控制目标　介绍几款用于隧道协议、代理和端对端通信的重要工具。这些工具可以用来在受害者计算机和攻击者使用的计算机之间建立通信管道。

第 12 章　编写文档和报告　对渗透测试文档的生成、测试报告的准备和报告的陈述提供指导。这些指导提供了一个系统化、结构化和持续化的方法来生成渗透测试报告。讲解如何验证测试结果、测试报告的种类、测试报告的陈述，以及如何进行渗透测试的收尾工作。

附录 A　补充工具　介绍了一些正文没有提到的渗透测试工具。

附录 B　关键资源　提供重要资源的链接。

阅读本书所需的准备

您仅需要安装、配置并运行 BackTrack，所有相关内容在本书第 1 章都有介绍。

本书的读者对象

IT 安全技术人员、了解 Unix/Linux 操作系统基础知识和信息安全基本概念的网络管理员，并且想要使用 BackTrack 进行渗透测试的技术人员。

本书所使用的一些格式约定

这些内容包括警告和重要注解内容。

提供小建议和小技巧。

读者反馈

随时欢迎读者朋友向我们提供宝贵意见。请不吝告知您对本书的看法、您喜欢这本书的哪些地方、您觉得哪些地方做得不好。您的反馈能帮助我们在将来提供更多符合广大读者需求的书籍。

如果您有任何关于本书的意见，只需发送邮件到 feedback@packtpub.com，并在邮件标题中注明相关书籍名称即可。

关于作者

Shakeel Ali 是英国 Cipher Storm 有限公司的首席技术官和主要创始人。他从事过大量的安全评估、审计、规则制定、管理和取证工作，并从中积累了出色的安全领域专业知识。他还是 CSS-Providers S.A.L 的首席安全官。作为一名资深安全人员，在无数个不眠之夜里，他为许多商业公司、教育机构、政府研究所提供了持续性的安全支持。同时作为一名活跃的独立研究者，他还著有很多文章和论文，并在 Ethical-Hacker.net 网站上开设了博客。他长期出席在墨西哥举办的 BugCon 安全会议，在会议上报告最前沿的网络安全威胁，并提出相关的实用解决方案。

我想感谢我的朋友们、审稿人员以及所有在本书出版过程中帮助过我的人。特别感谢 Packt 公司的出版小组、技术编辑和审稿编辑，他们为本书的成功出版提供了宝贵的意见、建议和反馈。还要感谢 Tedi Heriyanto（本书的另一位作者），正是因为有了他持续不断的贡献、精彩的想法和技术上的讨论，才能诞生这样一本有用的书籍。最后，我要感谢我的好搭档们，在和他们一起共事的过程中，灵感总是能够不断降临，正是他们时刻警惕的守护，才将 IT 产业带入一个更加安全和稳定的环境中。

Tedi Heriyanto 目前是印度尼西亚的一家信息安全公司的资深技术咨询人员。他曾经和许多知名研究机构合作，工作内容包括设计安全的网络架构，部署和管理企业级的安全系统，设计信息安全制度和流程，进行信息安全审计和评估，以及进行信息安全意识的培训。在工作之余，他会从事一些研究工作，撰写各种文章，并在 http://theriyanto.wordpress. com 网站上拥有个人博客。他还通过撰写一些信息安全和计算机编程方面的书籍，来分享他在信息安全领域的专业知识。

我想感谢我的家人，他们在我写作本书的过程中给予了极大支持。我还要感谢我的朋友们，他们在信息安全领域给我指导，并随时乐意和我讨论相关问题，他们是 Gildas Deograt、Mada Perdhana、Pamadi Gesang 和 Tom Gregory。感谢本书的技术评审：Arif Jatmoko、Muhammad Rasyid Sahputra 和 Peter“corelanc0d3r” Van Eeckhoutte，他们分别在自己擅长的领域提供了最宝贵的意见。还要感谢尊敬的 Packt 出版社工作人员（Kartikey Pandey、Kavita Iyer、Tarun Singh 和 Sneha Harkut），他们的宝贵评论、反馈和迅速的支持使本书得以顺利出版。最后，我要向本书的合著者 Shakeel Ali 致以最高的谢意，他的专业知识、热情、想法和建议将本书的写作过程变成了一趟美妙的经历。

审校者简介

Peter “corelanc0d3r” Van Eeckhoutte 是 Corelan 小组（http://www.corelan.be）的创始人，该组织聚集了一批具有相同兴趣爱好的人，他们从事 IT 安全 / 漏洞研究、分享知识、撰写并出版教程、发布安全公告并开发相关工具。他撰写了 Win32 Exploit 开发教程系列，开发了 Immunity Debugger 的 pvefindaddr 插件，而这些只是他对安全社区中所贡献的一小部分。Peter 从 20 世纪 90 年代后期开始从事 IT 安全工作，从 2006 年开始，他主要关注于漏洞利用程序的开发。

我想感谢我的爱人和女儿一直以来对我的支持，还要感谢 Corelan 小组的伙伴们，这是一个伟大的组织。

Arif Jatmoko （MCom，CISSP，CISA，CCSP，CEH）是一名 IT 安全审计人员，在印度尼西亚最大的银行——Mandiri tbk 银行工作。Arif 作为一名安全专家，有超过 15 年的工作经验。从 1999 年开始，他作为 IT 安全官员加入了一家财富 500 强企业，在政府和军事研究所实施了多个项目，并为四大审计公司和一些主流金融机构提供渗透测试服务。

从学生时代开始，Arif 就热爱编程、调试和其他逆向工程相关技术。这些爱好使他拥有了能够分析安全事件的技术。之后（在他最近的工作中），Arif 最感兴趣的是安全事件分析和计算机取证。特别是作为一名审计人员，他经常对安全犯罪事件以及公司内部的欺诈事件进行调查分析。

Muhammad Rasyid Sahputra 目前是一名安全顾问，就职于 Xynexis 国际公司。他的研究兴趣包括分析开源和商业软件 / 产品中的各种漏洞，并对电信基础设施进行渗透测试。

目　录

第 1 章

初识 BackTrack

本章将初步介绍 BackTrack，它是一个专门用于渗透测试的 Linux DVD 发行版。本章所涉及的内容包括：

- 简要介绍 BackTrack 的背景知识
- BackTrack 的一些常见用法
- 获取并安装 BackTrack
- BackTrack 的配置和更新

本章最后，我们将介绍如何在 BackTrack 上安装额外的测试工具，以及如何对 BackTrack 进行定制。

1.1 BackTrack 的历史

BackTrack 是一个经过特殊定制开发以满足渗透测试需求的、可启动的 Linux DVD 发行版。BackTrack 以可启动的 DVD 格式发布，因此可以直接使用 DVD 光盘启动而不必事先将其安装在硬盘上。你也可以选择将 BackTrack 安装到计算机硬盘上，像使用其他普通的操作系统一样方便地使用它。

BackTrack 混合了三个用于渗透测试的 Linux 发行版的功能，它们是 IWHAX、WHOPPIX 和 Auditor。BackTrack 的当前版本（4.0 版）是在 Ubuntu Linux 8.10 版本的基础上开发的。

截止到 2010 年 7 月 19 日，已经有超过 150 万的用户下载使用 BackTrack 4。

1.2 BackTrack 的用途

BackTrack 包含一系列可以在渗透测试过程中使用的工具。BackTrack 中的渗透测试工具可以分成以下几类：

- **信息收集工具**：该类别包含一系列用于收集目标信息的工具，这些信息包括目标的域名服务信息、路由信息、电子邮件地址、网站信息、邮件服务器信息等。这些信息都可以在不触及目标系统的情况下通过互联网获取。

- **网络映射工具**：该类别中的工具用于：探测在线主机、检测目标操作系统类型、枚举目标系统上运行的应用、端口扫描等。
- **漏洞定位工具**：该类别包括一系列用于扫描常用系统和思科设备中的漏洞的工具，还包含了可以对服务器消息块（SMB）、简单网络管理协议（SNMP）进行模糊测试和分析的工具。
- **Web 应用分析工具**：该类别包含了一系列 Web 应用审计工具。
- **无线网络分析工具**：当需要对测试目标的无线网络、蓝牙、无线射频识别（Radio Frequency Identifier，RFID）进行审计时，将会用到该类别中的许多工具。
- **Web 应用分析工具**：该类别包含一系列用于攻击目标系统中的漏洞的工具。
- **提权工具**：当成功攻击了目标系统中存在的漏洞，并取得了对目标系统的访问权限之后，可以使用提权工具来获得目标系统的最高权限。
- **持续控制目标**：该类工具可以用于维持对目标系统的控制权。在安装使用该类别工具之前，可能需要先通过提权工具来获得目标系统的最高权限。
- **互联网语音协议**（Voice over Internet Protocol，VOIP）**工具**：该类别中的工具可以用来分析目标环境中的互联网语音协议。

BackTrack 4 中还包含如下用途的工具：

- **数字取证工具**：包含一系列可以用于数字取证的工具，包括硬盘数据提取、文件内容搜索和提取、硬盘数据分析等。要使用这类工具，可以在 BackTrack 的开始菜单中选择 Start BackTrack Forensics（开始 BackTrack 取证）。在实际操作中，最好以只读（read-only）方式挂载硬盘和交换文件以避免硬盘数据遭到破坏。
- **逆向工程工具**：这类工具可以用于调试程序或者反汇编可执行文件。

1.3 获取 BackTrack

在安装和使用 BackTrack 之前，需要先获取它。你可以通过种子文件来下载 BackTrack 4.0，也可以从 BackTrack 的官方网站上下载（http：//www. backtrack-linux.org/downloads/）。

在 BackTrack 的官方网站上，存在两种格式的 BackTrack 4.0。其中之一是 ISO 光盘镜像格式，如果想要将 BackTrack 刻录到 DVD 上，或者安装到硬盘上，你可以选择下载此版本。另一个版本是 VMWare 虚拟机的映像文件格式。如果想要在虚拟机上使用 BackTrack，那么使用该版本将可以省去在虚拟机平台上安装和配置 BackTrack 所花的时间。

在作者撰写本书时，BackTrack 的最新版本是 BackTrack 4 最终版，因此建议选择 BackTrack 4 最终版（BackTrack 4 Final Release）。

当下载完 BackTrack 后，请比对所下载文件的 MD5 散列值和官方网站提供的 MD5 散列值并确认它们是相同的，这样做可以保证您下载的文件没有被恶意篡改。

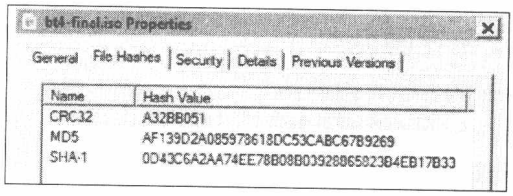
在 UNIX/Linux/BSD 操作系统上，可以使用如下命令来得到所下载的镜像文件的 MD5 值，整个计算过程可能需要花费一点时间：

```
md5sum bt4-final.iso
af139d2a085978618dc53cabc67b9269  bt4-final.iso
```

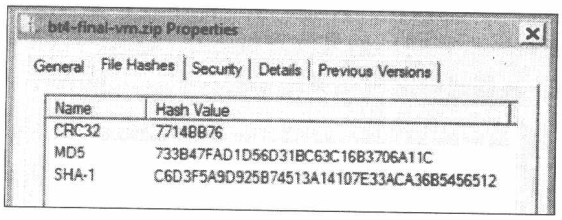
在 Windows 平台上，有很多计算 MD5 散列值的工具，其中一个就是 HashTab。可以从 http：//beeblebrox.org/ 上下载 HashTab，该工具支持 MD5、SHA1、SHA2、RIPEMD、HAVAL 以及 Whirlpool 散列算法。

在安装完 HashTab 以后，要得到某个文件的 MD5 散列值，只需要选择该文件，右击并选择 Properties（属性），可以看到一系列选项卡：General、File Hashes、Security、Details、Previous Version，选择其中的 File Hashes（文件散列值），就可以看到相应的 MD5 值。

使用 HashTab 计算出的 BackTrack 4 ISO 镜像文件的 MD5 散列值如下图所示：



同样使用 HashTab 计算 BackTrack 4 的 VMWare 虚拟机镜像文件（以 ZIP 格式压缩压缩）的 MD5 散列值，结果如下图所示：



请对比计算得到的 MD5 散列值和官方提供的 MD5 散列值是否一致。官方 MD5 散列值记录在一个文件中，只需比较该文件的内容和你通过 `md5sum` 或者 `HashTab` 计算出来的 MD5 散列值是否相同。如果两者是相同的，那么可以进入下一步，否则你可能需要重新下载 BackTrack。

1.4　使用 BackTrack

你可以通过下面几种方法来使用 BackTrack：

- 直接使用 BackTrack DVD 光盘。
- 将 BackTrack 安装在硬盘上。
- 将 BackTrack 安装在 USB 闪存盘上（便携式的 BackTrack）。

下面我们会详细介绍每一种方法。

1.4.1 通过 DVD 光盘使用 BackTrack

如果你想使用 BackTrack 但又不想将它安装在计算机硬盘上，那么可以将 BackTrack 的 ISO 镜像文件刻录到一张 DVD 光盘上，然后通过 DVD 光盘启动计算机。BackTrack 将会直接从 DVD 光盘中运行。

使用 DVD 方式运行 BackTrack 的好处在于：方式简单，不受现有计算机上的配置的影响。

然而，这种方式也存在着一些缺点。首先，为了使用计算机上的一些硬件资源，可能需要对 BackTrack 进行额外的配置。如果以 DVD 形式使用 BackTrack，那么这些配置上的更改在重启之后无法保存。其次，由于需要从 DVD 光盘上读取要运行的程序，速度也会比较慢。

因此，如果你希望自己的 BackTrack 具备较好的扩展性，那么建议将其安装在硬盘上。

1.4.2 将 BackTrack 安装在硬盘上

在硬盘上安装 BackTrack 的方式有两种：

- 在物理机上安装 BackTrack（常规安装）
- 在虚拟机上安装 BackTrack

请选择适合自己的安装方式。下面分别介绍这两种方法。

在物理机上安装 BackTrack

在物理机上安装 BackTrack 之前，请确保硬盘上没有任何重要数据。为了方便安装，我们建议在安装时使用所有的磁盘空间。如果物理机上已经安装了别的操作系统，那么需要先为 BackTrack 创建一个分区。在创建分区时请务必小心行事，以免破坏了原有操作系统。

网上有一篇讲述如何在已经安装了其他操作系统（例如 Windows XP）的情况下，安装 BackTrack 的文章，可以通过如下链接访问：http：//www. backtrack-linux. org/tutorials/dual-boot-install/。

我们建议使用专用的分区工具来进行磁盘分区，有许多开源的 Linux 启动光盘可以完成这项工作，比如 SystemRescueCD（http：//www. sysresccd.org/）和 gparted（http：//gparted. sourceforge.net/）。通过启动光盘启动系统，然后就可以开始进行分区了。在实际使用分区工具之前，请先备份你的数据。尽管从我们的经验来看，使用这些分区工具是相对安全的，但是，小心驶得万年船。

当完成了对磁盘的分区工作之后（或者一开始就准备使用整个磁盘空间），就可以通过 BackTrack 4 的 DVD 光盘启动系统了。稍等片刻，待启动过程完成之后，就可以看到如下图所示的登录界面：

```
BackTrack 4 PunSauce bt tty1

bt login: root
Password:
Last login: Fri Jul  2 14:22:41 WIT 2010 on tty1

BackTrack 4 (PunSauce) Penetration Testing and Auditing Distribution
```

如果系统要求输入用户名和密码，可以使用如下默认值：

- Username：root
- Password：toor

如果想要进入 BackTack 4 的图形界面模式，可以在 root 提示符下输入：

```
startx
```

进入系统后，如果桌面上存在一个名为 install.sh 的文件，那么可以点击运行该文件来将 BackTrack 安装到硬盘上。如果找不到对应文件，可以使用 ubiquity 命令来安装。

要使用 ubiquity 命令，首先通过点击状态栏上左起第五个图标来启动 Konsole 终端程序。然后在 Konsole 窗口下输入：

```
ubiquity
```

之后就能看到一个窗口显示正在安装。安装程序会要求你回答如下问题：

- 你所在的城市：请使用地图或者下拉框来选择你所在的城市。
- 键盘布局：如果没有特殊情况，可以使用默认键盘布局——USA-USA。
- 磁盘分区：安装程序会指导你完成磁盘分区。如果事先已经分好区了，那么可以选择“Guided-use the entire disk”来使用整个分区。
- 安装程序会显示你之前所选择的所有安装选项以供确认。确认没有问题之后，可以点击 Install 按钮进行安装。

等待一段时间后，安装程序运行完毕，BackTrack 4 就已经成功安装到硬盘上了。

在虚拟机上安装 BackTrack

我们也可以将 BackTrack 安装在一台虚拟机上。使用这种安装方式的优点在于：不再需要为安装 BackTrack 而准备新的磁盘分区，从而可以保证系统中已有的操作系统不受影响。而在虚拟机中使用 BackTrack 的主要问题是：它的运行速度要比在物理机上直接运行慢很多。并且如果想要使用无线网络，必须配备 USB 无线网卡。这是因为虚拟机软件禁止了从虚拟机中访问除 USB 设备以外的其他硬件资源。

要在虚拟机上安装 BackTrack，有两种选择。第一种选择是直接使用 BackTrack 官方提供的 VMWare 镜像。这种安装方式的优点是既简单又快速，而它的缺点在于我们无法更改虚拟机的相关配置（磁盘大小）。

BackTrack 官方提供的 VMWare 镜像的配置如下：

- 内存：768 MB
- 磁盘大小：30GB（分成好几个独立的映像文件，每个文件的大小为 2GB）
- 网络连接：网络地址转换（Network Address Translation，NAT）

我们在使用 NAT 作为 BackTrack 虚拟机的网络连接类型时，曾经碰到过这样一个问题。当时我们试图追踪网络数据包所经过的路由，但是追踪结果只显示了两个节点，一个是本机，另一个是目标计算机。而在本机和目标计算机之间的那些路由节点都变得不可见了。但是当我们在物理机上做相同的追踪时，显示的结果却是正确的。最后我们通过将网络连接类型设成桥接（Bridge）才解决了这个问题。