



华章科技



Amazon五星级超级畅销书，奥巴马政府国家安全局局长、美军网络司令部司令Keith B. Alexander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。

S 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

渗透测试实践指南： 必知必会的工具与方法

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

(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。

Patrick Engebretson: The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (ISBN: 9781597496551).

Copyright © 2011 by Elsevier Inc. All rights reserved. Authorized Simplified Chinese translation edition published by the Proprietor. Copyright © 2013 by Elsevier (Singapore) Pte Ltd. All rights reserved.

Published in China by China Machine Press under special arrangement with Elsevier (Singapore) Pte Ltd. This edition is authorized for sale in China only, excluding Hong Kong SAR and Taiwan. Unauthorized export of this edition is a violation of the Copyright Act. Violation of this Law is subject to Civil and Criminal Penalties.

本书简体中文版由机械工业出版社与Elsevier (Singapore) Pte Ltd.在中国大陆境内合作出版。本版仅限在中国境内（不包括中国香港特别行政区及中国台湾地区）出版及标价销售。未经许可之出口，视为违反著作权法，将受法律之制裁。

封底无防伪标均为盗版

版权所有，侵权必究

本书法律顾问 北京市展达律师事务所

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

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>。

华章图书

目 录

译者序	
前言	
致谢	
第 1 章 渗透测试	1
1.1 内容简介.....	1
1.2 Backtrack Linux 介绍.....	3
1.3 使用 Backtrack：启动引擎	7
1.4 黑客实验环境的搭建与使用	10
1.5 渗透测试的步骤	11
1.6 本章回顾.....	15
1.7 小结	15
第 2 章 偷察	17
2.1 内容简介.....	17
2.2 HTTrack：网站复制机	21
2.3 Google 指令——Google 搜索 实践	24
2.4 The Harvester：挖掘并利用 邮箱地址	29
2.5 Whois	31
2.6 Netcraft.....	34
2.7 host 工具.....	35
2.8 从 DNS 中提取信息.....	36
2.8.1 NS Lookup	37
2.8.2 Dig	39
2.9 从电子邮件服务器提取信息	39
2.10 MetaGooFil	40
2.11 社会工程学.....	42
2.12 筛选信息以寻找可攻击的 目标	43
2.13 如何实践	44
2.14 接下来该做什么	44
2.15 小结	45
第 3 章 扫描	47
3.1 内容简介.....	47
3.2 ping 和 ping 扫描	50
3.3 端口扫描	52
3.3.1 三次握手	53
3.3.2 使用 Nmap 进行 TCP 连接 扫描	54
3.3.3 使用 Nmap 进行 SYN 扫描	55
3.3.4 使用 Nmap 进行 UDP 扫描	57
3.3.5 使用 Nmap 执行 Xmas 扫描	60
3.3.6 使用 Nmap 执行 Null 扫描	61
3.3.7 端口扫描总结	62
3.4 漏洞扫描	63
3.5 如何实践	66
3.6 接下来该做什么	68

3.7 小结	68	5.8 如何实践	133
第 4 章 漏洞利用	69	5.9 接下来该做什么	134
4.1 内容简介	69	5.10 小结	135
4.2 利用 Medusa 获得远程服务 的访问权限	71	第 6 章 使用后门和 rootkit 维持 访问	137
4.3 Metasploit	74	6.1 内容简介	137
4.4 John the Ripper: 密码破解 之王	87	6.2 Netcat: 瑞士军刀	138
4.5 密码重置: 破墙而入	96	6.3 Netcat 神秘的家族成员: Cryptcat	144
4.6 嗅探网络流量	99	6.4 Netbus: 一款经典的工具	145
4.7 macof: 泛洪攻击交换机	100	6.5 rootkit	146
4.8 Fast-Track Autopwn: 自动化 漏洞攻击	104	6.6 rootkit 的检测与防御	152
4.9 如何实践	108	6.7 如何实践	154
4.10 接下来该做什么	110	6.8 接下来该做什么	155
4.11 小结	112	6.9 小结	156
第 5 章 基于 Web 的漏洞利用	115	第 7 章 渗透测试总结	157
5.1 内容简介	115	7.1 内容简介	157
5.2 扫描 Web 服务器: Nikto	116	7.2 编写渗透测试报告	158
5.3 Websecurify: 自动化的 Web 漏洞扫描	117	7.2.1 综合报告	159
5.4 网络爬虫: 抓取目标网站	119	7.2.2 详细报告	159
5.5 使用 WebScarab 拦截请求	122	7.2.3 原始输出	161
5.6 代码注入攻击	125	7.3 继续前行	164
5.7 跨站脚本: 轻信网站的 浏览器	129	7.4 接下来该做什么	166
		7.5 结束语	168
		7.6 学无止境	169
		7.7 小结	169

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 Vader）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。在该范围内，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

入以下命令：

```
apt-get update  
apt-get install cheops
```

软件安装之前，你会看到还有多少磁盘空间可用，并询问你是否继续。你可以输入“Y”并按回车键来进行新软件的安装。

如果你不喜欢使用命令行，有几个 GUI 可用于与 API 交互。当前最流行的图形交互前端软件是 Aptitude。其他软件包管理器的讨论超出了本书的范围。

对 Linux 系统有个基本了解是很有帮助的，从长远来看，这也会给你带来许多益处。本书不要求你必须有使用 Linux 的经验，但是不管是通过系统学习的方式，还是通过读书，或者自己钻研的方式，将来你一定要努力让自己成为一名 Linux 大师。相信我，你以后一定会感谢我。如果你对渗透测试或黑客感兴趣，就必须掌握 Linux，别无他法。

幸运的是，安全社区拥有一个非常活跃、热心的群体。已经有好几个机构坚持不懈地致力于各种面向安全应用的 Linux 发布版的研发。每一个版本，或短期的“发行版”(distro)，都是基于 Linux 的风格、类型以及品牌。

用于渗透测试的最常用的发行版之一是“Backtrack”。Backtrack Linux 是学习黑客知识和执行渗透测试最便捷的工具。Backtrack Linux 让我想起了《黑客帝国》第一部中的一个场景，当时探克 (Tank) 问尼奥 (Neo)：“除了奇迹你还需要什么？”尼奥回答说：“枪。许多枪。”这时，一排又一排的枪涌现在电影画面中。这里有各种能够想到的供尼奥和崔妮蒂 (Trinity) 使用的枪：手枪、步枪、猎枪，半自动的、全自动的、大小不同的手枪，从发射到爆破不一而同，各种武器源源不断地供他们选择。对于大多数新手来说，当他们第一次使用 Backtrack 时，会有同样的感受，那就是他们面对着“工具。许多工具”。

Backtrack Linux 让黑客爱好者梦想成真。Backtrack Linux 完整版是专为渗透测试人员定制的。它预先加载了成百上千种安装并配置好的安全工具，以方便用户使用。尤其是，Backtrack 是免费的！你可以从 <http://www.Backtrack-linux.org/downloads/> 上下载。

Backtrack 网站提供了 .iso 或 VMware 映像两种下载格式。如果选择下载 .iso 格式的文件，需要将该文件刻录到 DVD 中。如果你不知道如何刻录 DVD，请在 Google 上搜索“刻录 iso 格式文件”(burning an iso)。一旦你完成了刻录，你就拥有了一张启动盘。大多数情况下，使用这张启动盘启动 Backtrack 是非常简单的，只需要将光盘放入光驱并重启机器即可。但有些时候，你可能需要在 BIOS 中将光驱设置为优先启动。

如果你下载的是 VMware 映像格式的文件，你还需要能够打开、部署或者能直接运行该映像文件的软件。幸运的是，有几个很好的工具能完成这项工作。你可以根据自己的喜好选择 VMware 公司的 VMware Player，Sun 公司 Microsystem 的 VirtualBox，或微软公司的 Virtual PC。如果你不喜欢上面提到的三款软件，还有很多其他的选择。你只需要选择一款适合自己的就行了。

上面列出的三个虚拟化软件都是免费的，都能运行 VM 映像文件。你需要决定哪个版本最适合自己的。本书会着重介绍 Backtrack VMware 映像和 VMware Player 的使用。在本书编写时，VMware Player 的下载地址是：<http://www.vmware.com/products/player/>。你需要先注册一个账号才能下载该软件，注册过程非常简单而且是免费的。

如果你不知道该选择哪个软件，建议你使用 VMware。它不仅是一种值得称道的技术，而且可以让你在单机上搭建一个完整的渗透测试实验环境。如果你使用笔记本电脑，你就拥有了一个“可移动的”渗透测试实验环境，可以随时随地练习你的技能。

若你使用 DVD 启动盘来运行 Backtrack，系统启动之后，你会马上看到一个菜单列表。你必须仔细阅读菜单列表，它包含几个不同的选项，最开始的两个选项用来设置屏幕分辨率的一些基本信息。如果你无法正常启动 Backtrack，请选择“图形界面安全模式启动 Backtrack”。菜单中的其他选项本书就不再讨论了。要选择所需的引导方式，只需移动箭头来高亮显示相应的选项，按回车键确认即可。图 1-1 就是 Backtrack 启动时的一个截图。

使用 Backtrack 不需要完全照搬本书的内容，也不需要什么黑客知识。Backtrack 可以在 Linux 的任何版本上运行。Backtrack 的最大优势是它已经为你预加载了所有的工具。如果你使用与本书不同版本的 Linux，就需要在阅读相关章节之前安装必要的工具。请记住，本书侧重于基础知识，任

任何版本的 Backtrack 都是可行的。本书研究和使用的所有工具在任何版本的 Backtrack 中都有。

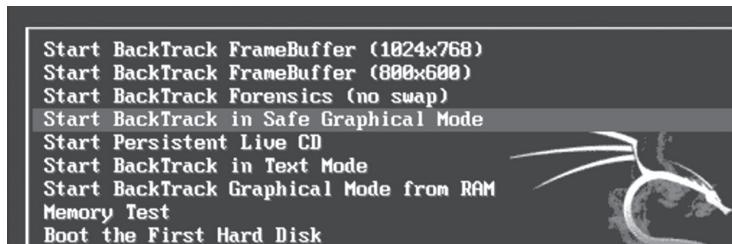


图 1-1 Live DVD 启动选项截图

1.3 使用 Backtrack：启动引擎

不管选择 VM 来运行 Backtrack 还是选择 Live DVD 启动 Backtrack，系统加载后就会看到一个登录提示符，默认的用户名是 root，默认密码是 toor。

请注意，默认的密码只是反过来拼写的“root”。这种默认用户名和密码的组合方法从 Backtrack 1 开始沿用至今，很可能会在以后的版本中继续使用。当输入默认的用户名和密码之后，就可以登录系统了，登录后会看到系统提示符：“root@bt:~#”。虽然本书讨论的很多工具直接通过命令行就能运行，但对于初学者而言，使用图形化的 X Window System 会更加容易。启动 GUI 需要在“root@bt:~#”提示符后边输入命令：

```
startx
```

输入这条命令后按回车键，X 将开始加载。对于它的环境，大多数计算机用户都非常熟悉。一旦完成加载，就会看到桌面、图标、任务栏和系统托盘。这个界面与微软的 Windows 操作系统类似，可以通过移动鼠标并单击所需对象与系统进行交互。

本书用到的大多数程序都是在终端中运行的。如图 1-2 所示，可以通过单击任务栏左下角的黑色方框来启动一个终端会话，也可以在启动器中输入下面的命令：

```
konsole
```

默认情况下，Backtrack 并不启用网络功能，这与微软的 Windows 系统

以及大多数当今流行的 Linux 操作系统不同。这种设置是故意的，因为作为渗透测试人员，我们通常会设法隐藏自己来避免被人发现。计算机一旦接入网络，启动之后就会马上通过广播的方式向整个网络申请 DHCP 服务器和 IP 地址，好似无声的呐喊：“快看！！快看！！我在这里！！”为了避免这种情况，Backtrack 机器的网络接口默认是关闭的。

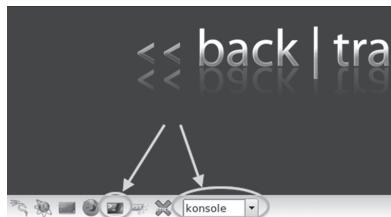


图 1-2 两种启动 Konsole（终端）的方式

启用网络最简单的方法就是通过终端。单击最左边箭头形状的终端图标可以打开一个终端窗口，如图 1-2 所示。终端打开后，输入如下指令：

```
ifconfig -a
```

这条命令会把计算机上所有可用的接口以列表的形式罗列出来。大多数计算机至少都会有一个 eth0 网卡和一个 lo 接口。“lo”接口是计算机的环回接口。“eth0”是计算机上的第一张以太网卡。根据计算机的硬件配置，可能会有其他的接口或接口设备清单。如果通过 VM 来运行 Backtrack，主接口一般就是 eth0。

要打开网卡，需要在终端窗口中输入如下命令：

```
ifconfig eth0 up
```

我们详细解析一下这条命令，“ifconfig”是一条 Linux 命令，其含义是“我想要配置一个网络接口”。众所周知，“eth0”是计算机系统的第一个网络设备（记住计算机的计数是从 0 开始而不是 1），关键字“up”用于激活接口。因此我们大致可以将这条命令翻译为“我想将第一个接口配置成打开状态”。

现在，接口打开了，需要配置一个 IP 地址。配置 IP 地址有两种基本方法。第一种方法是手动分配 IP 地址，在上述命令（ifconfig eth0 up）的后边添加要配置的 IP 地址即可。例如，如果我们想给网卡分配一个 IP 地址 192.168.1.23，应该输入：

```
ifconfig eth0 up 192.168.1.23
```

现在 IP 地址配好了，还需要配置网关和域名系统（DNS）服务器。在 Google 上搜索“设置 linux 网络接口卡”（setting up nic linux），我们就会了解到相关知识。通过在终端窗口执行如下命令来验证输入是否有效：

```
ifconfig
```

运行该命令后，你就会看到网络接口的所有当前配置信息。因为本书面向的是初学者，为了简单起见，这里不考虑网络隐身。在这种情况下，获取地址最简单的方法是使用 DHCP。通过 DHCP 分配地址，只需执行命令：

```
dhclient eth0
```

请注意，使用上述命令的前提是已经运行相关命令，并成功地打开了网络接口（本例中为 eth0）。

现在，我们已经成功地分配了 IP 地址，最后要解决的问题是如何关闭 Backtrack。和大多数 Linux 系统一样，有很多方法可以关闭 Backtrack。其中最简单的一个方法是在终端窗口中输入命令：

```
poweroff
```

如果你想重启系统而不是关闭系统，那么也可以使用 reboot 命令来代替 poweroff。

在继续下面的内容之前，你应该花些时间来复习和实践一下之前所强调的步骤，它们包括：

- 启动 Backtrack；
- 使用默认的用户名和密码登录；
- 启动 X (Windows GUI)；
- 查看机器上所有的网络接口；
- 开启所需网络接口；
- 手动分配 IP 地址；
- 检查手动分配的 IP 地址是否正确；
- 使用 DHCP 指定 IP 地址；
- 检查动态分配 IP 地址是否正确；
- 使用命令行界面重启机器；
- 使用命令行界面关闭机器。

1.4 黑客实验环境的搭建与使用

每个道德黑客都需要一个能够进行实践和探测的环境。学习使用黑客工具怎样才能不违法，或者怎样才能确保不侵犯未授权的目标，这让大多数新手都感到迷惑。通常搭建一个个人“黑客实验环境”就可以解决上述问题。黑客实验环境是一个沙箱环境，在这里的流量和攻击被隔离起来，或者不会触及未授权和未经同意的目标。在这个环境中，你可以任意利用所有的工具和技术，不用担心某些流量或者攻击脱离了你的网络。搭建实验环境至少需要两台计算机：一台模拟攻击机器，另一台模拟受攻击机器。还可以有其他的配置方法，同时部署多个受攻击机器能够模拟更真实的网络环境。

合理的使用和搭建黑客实验环境是至关重要的，因为这是最有效的学习手段之一。学习和掌握渗透测试的基本知识也需如此。

对黑客实验环境而言，至关重要的一点是要保证网络的隔离。你必须通过配置实验室的网络环境以确保通信流量不会逃逸或流出本网络之外。错误总会发生，即使最谨慎的人也有可能输错 IP 地址。即使是输错 IP 地址中的一个数字这样简单的错误，都有可能给你带来非常严重的后果。如果在黑客实验环境中本打算设置的目标地址是 172.16.1.1，并对其进行了一系列的扫描和攻击，后来却发现实际上录入的 IP 地址是 122.16.1.1，这会令你感到惭愧，而且更重要的是，这样的错误有可能会违法。

搭建沙箱或隔离的环境，最简单、最有效的方式就是从物理上断开网络或将你的网络与互联网断开连接。如果你使用的是物理设备，那么通过调整以太网线缆和交换机来改变路由流量是最好的方法。另外要再三检查你的无线 NIC 是不是关闭了。继续下一步工作之前要经常地检查你的网络是否存在潜在的流量泄露。

虽然用物理机器搭建黑客实验环境是一个不错的解决方案，但是，使用虚拟机来做这件事有几个明显的好处。首先，基于当前处理器的处理能力，在单个台式机或笔记本电脑上搭建一个“迷你”的黑客实验环境是很容易的。大多数情况下，我们会使用最少的资源来建立攻击目标，因此一台普通的计算机能同时运行两台或三台虚拟机。即使是在笔记本电脑上，也能同时运行两台虚拟机。使用笔记本电脑的另一个好处是实验环境是可移动的。现在外

部存储器成本非常便宜，将几百台虚拟机器装入一个外置硬盘驱动器上很容易，携带起来也方便，安装也就几分钟的事情。每次你想实践的时候，或者想研究一下新工具的时候，只要打开 Backtrace 并将虚拟机部署为目标对象就可以了。搭建一个这样的实验环境可以让你拥有快速的、以即插即用的方式安装和配置不同操作系统的能力。

在渗透测试实验环境中使用虚拟机的另一个好处是，它可以很轻松地使整个系统沙箱化。只需要关闭无线网卡并拔出网线，这时物理机和虚拟机仍可互相通信，并且确保了没有攻击流量能流出你的物理机器。

一般而言，渗透测试是一个破坏性的过程。我们使用的许多工具和漏洞利用方法都有可能导致系统损坏或掉线。有些时候，重装操作系统或应用程序比修复更容易。这也是虚拟机的另一个优势。虚拟机可以快速地重置或恢复到它的初始配置，既不需要重新安装像 SQL Server 这样的程序，也不需要重新安装整个操作系统。

1.5 渗透测试的步骤

与大多数工作一样，渗透测试的整个过程可以分解为一系列的步骤或阶段。各个步骤放到一起，就形成了一个完成渗透测试的全面方法论。如果对未涉密事件的响应报告或已泄密公开的文件进行仔细分析，那么就能发现大部分黑帽黑客在进行目标攻击时也会遵循一定的流程。规范的测试流程很重要，这不仅能让渗透测试人员集中注意力并不断推进工作，而且每一步的测试结果或输出也能在接下来的测试阶段得到使用。

运用一套已成体系的方法论，可以将一个复杂的过程分解为一系列小的、易操作的任务。理解并遵循某个方法论对于掌握黑客基础知识十分重要。不同的方法论其步骤也不尽相同，但一般都包括 4 ~ 7 个步骤或阶段。虽然每套方法论拥有不同的名称和步骤数，但重要的是，这些方法论都提供了一个与渗透测试过程相关的完整概述。

例如，有的方法论使用术语“信息收集”，而其他的方法论则把这个同样的过程叫做“侦察”（Reconnaissance）。本书侧重于不同阶段的活动内容而不是它们的名称。当你掌握了基本知识以后，就可以从众多的渗透测试方法

论中选择最适合自己的那一个了。

为了简单起见，我们用一个包括四个步骤的方法论来学习和探讨渗透测试。如果你搜索和研究其他的方法论（这样做很重要），你会发现它们采用的步骤与我们使用的不同，也许多一些，也许少一些，并且每个步骤的名称也不相同。重要的是要了解，虽然每个渗透测试方法论使用的术语不同，但大多数所涵盖的主题是一样的。

上述规则中有一个例外：许多黑客方法论的最后一步称为“隐藏”、“掩藏痕迹”或者“销毁证据”。因为本书侧重于基本概念的理解，所以我们使用的方法论不包含这一步。一旦你掌握了扎实的基础知识，你就可以继续研究和学习关于这一步骤的更多知识了。

本书其余的内容将着重讨论和介绍以下步骤：侦察、扫描、漏洞利用、维持访问（*maintaining access*）。有时候，用倒三角的方式来表示这些步骤会更加直观，如图 1-3 所示。使用倒三角表示这些步骤是因为初始阶段获得的成果非常多。当讨论其他的阶段时，我们会更加关注某些特定的细节。



图 1-3 黑客渗透测试入门方法论

倒三角方法论很好地契合了本书由广泛到具体的讨论方法。例如，侦查阶段，我们要尽可能多地搜集网络上的信息。关于目标的每一个细节和每一条信息都要搜集并保存。在渗透测试领域里有很多经典的例子，那些在渗透测试初始阶段收集到的看似微不足道的信息，后来被证明是成功完成漏洞攻击并获取系统权限的重要组成部分。在后续的阶段，我们就可以关注目标更加具体的细节问题了。目标在哪里？它的 IP 地址是多少？它运行的是什么操

作系统？它开启了哪些服务和哪些版本的软件？正如你所看到的，每一个问题都变得越来越细化了。

理解每个步骤的次序也是很重要的。这些步骤执行的先后顺序非常关键，因为某一步的输出或者结果就是后续步骤的输入。你不仅需要了解如何简单地运行本书介绍的安全工具，更要知道，以正确的顺序运行这些工具对执行一个全面且真实的渗透测试来说至关重要。

例如，很多初学者跳过了侦查阶段直接开始对目标进行漏洞攻击。跳过了第一步和第二步，结果只能是在每个目标上搜集到少量的目标列表和攻击向量（attack vector）。换句话说，这是在投机取巧。虽然知道如何使用一套工具能够引起他人的关注，但这并不是安全从业者和专业人士所采用的严谨的工作方法。

对于初学者而言，将介绍的这些步骤想象成一个环是很有帮助的。当前，重要系统都不会将自己直接暴露在互联网上。大多数情况下，在渗透测试人员找到一条到达预定目标的路径之前，他们必须先对一系列相关的目标进行访问和渗透。在这种情况下，每一个步骤常常会重复出现。图 1-4 用环形过程介绍了这一方法论。

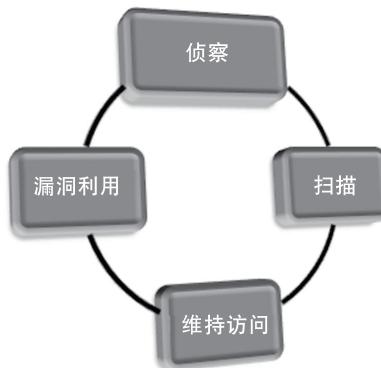


图 1-4 入门方法论的环形表示法

黑客入门：四步模型法

我们粗略地讨论一下四步模型法涉及的内容，以便你对它有一个直观的

认识。任何渗透测试方法的第一步都是“侦查”。这个阶段负责收集目标的信息。如前所述，你从目标上搜集到的信息越多，你就越有可能在后续阶段取得成功。第2章将详细地讨论侦查。

不管你有什么样的初始信息，在完成深入侦查之后，你都应该获得了目标的IP地址列表。该方法论的第二步可以分解为两个截然不同的活动。一个是执行端口扫描。一旦完成了端口扫描，就拥有了目标的开放端口和可能已开启服务的列表。第二个活动是漏洞扫描。漏洞扫描用于定位和识别在目标计算机上运行的软件和服务所存在的缺陷。

依据步骤2得到的相关结果，继续“漏洞利用”阶段。一旦我们确切地知道了目标计算机上开启了哪些端口，端口上都运行了哪些服务以及这些服务存在着什么样的漏洞，就可以开始进行目标攻击了。大多数新手都认为这一步才是“真正”的黑客行为。漏洞利用包含许多不同的技巧、工具和代码。第4章会讨论一些最常用的工具。漏洞利用的最终目标是在目标计算机上获得管理员权限（即完全控制权）。

要掌握的最后一个步骤是“维持访问”。通常，在漏洞利用阶段提供的攻击载荷只能提供开启系统的临时访问权限。因为大多数攻击载荷都是临时的，所以需要创建一个可以永久控制目标系统的后门进程。这个后门进程可以让我们以管理员的权限重新开启已经关闭的程序，甚至是重新启动目标计算机。作为一名道德黑客，对于这一阶段的使用和实现我们必须非常小心谨慎。我们将讨论如何完成这一步骤，以及使用后门或远程控制软件所涉及的道德问题。

每一个渗透测试最后的工作就是编写报告（这无疑是最重要的），但是它并不作为渗透测试方法论中的一个正式步骤。不管你花了多少时间和心血来实施渗透测试，客户通常只会根据报告的质量来评判你的工作效果。渗透测试的最终报告应当包含测试过程中发现的所有相关信息，还要说明测试实施的细节和测试内容。报告应当尽可能地针对发现的安全问题给出缓解和解决的方案。最后，每一个渗透测试报告都要包括一个总结。总结的目的是对你的成果进行一个简短的（大约1~2页纸）、非技术性的概述。报告应对你发现的最关键的安全问题进行强调并做简要总结。一定要注意，报告对技术人员和非技术人员来说都要通俗易懂。这才是详细报告的真正目的，千万别在报告中涉及太多的技术细节。

1.6 本章回顾

本章从系统安全的角度介绍了渗透测试和有关黑客的基本概念。也讨论了执行黑客攻击时涉及的不同角色及其特点。本章介绍了 Backtrack Linux 的基本使用方法，包括如何启动、登录、启动 X、获取 IP 地址以及如何关闭。还讨论了如何搭建你自己的隔离渗透测试实验环境，以便你进行实践时不用担心触犯法律，最后介绍了渗透测试的各个步骤。

需要注意的是 Backtrack 有好几个版本。有些时候，你可能需要查找和摸索其他的发行版本。Matriux 与 Backtrack 非常相似，区别仅仅在于它包含一个可被 Windows 直接访问并使用的 Windows 二进制目录。Fedora Security Spin 是一个安全工具集，适用于 Fedora 发行版的 Linux。KATANA 是一个可多重引导的系统，它将许多不同的工具和发行版搜集在一张 DVD 中。最后，你可能想摸索一下经典的标准发行版（如 Pentoo 和 Blakbuntu）。还有许多其他的基于 Linux 的渗透测试发行版——在 Google 上搜索“Linux 渗透测试发行版”（Linux Penetration Testing Distributions），你就会得到很多的选择。你还应该花些时间通过搜集和安装工具来建立并定制自己的 Linux 发布版，这会成为你黑客生涯中的一大进步。

1.7 小结

本章介绍了渗透测试和道德黑客的基本概念，并讲解了一个特定的“只面向初学者”的四步方法体论，包括侦察、扫描、漏洞挖掘和维持访问。介绍了怎样搭建和使用 Backtrack Linux，包括如何配置网络连接和在终端窗口发布命令。概要介绍了如何搭建和使用渗透测试实验环境。它为你提供了一个安全的沙箱环境来练习技能。这个实验环境也能让你亲自完成本书中提到的所有例子。

第 2 章

侦察

本章知识点

- HTTrack: 网站复制机
- Google 指令——Google 搜索实践
- The Harvester: 挖掘并利用邮箱地址
- Whois
- Netcraft
- host 工具
- 从 DNS 中提取信息
- 从电子邮件服务器中提取信息
- MetaGooFil
- 社会工程学
- 筛选信息以寻找可攻击的目标

2.1 内容简介

大部分时候，参加过黑客讲座或课程的人对若干安全工具都会有基本的认识。很典型的例子是，这些学生可能曾经利用端口扫描工具对某一系统进行过检查，或曾使用 Wireshark 来查看网络流量。其中有些人可能还玩过 Metasploit 之类的漏洞利用工具。遗憾的是，如何在渗透测试过程中运用这些工具，大部分初学者其实并不了解。也正因如此，他们的知识结构是不完整的。如果能遵循一定的方法论，就等于有个方案在手，也就知道了下一步该做什么。

为了强调使用并遵循某一方法论的重要性，通常描述一种场景来加以解释，这是很有帮助的，该场景可用来强调在渗透测试过程中本步骤（侦察）的重要性以及应用一整套方法论的价值所在。

假设你是在一家安全公司工作的道德渗透测试员，你老板跑到你办公室，递给你一张纸，说：“我刚跟那家公司的 CEO 在电话里聊了聊。他要我派出最好的员工给他们公司做渗透测试——这事得靠你了。一会儿法律部会给你发封邮件，确认我们已经得到相应的授权和保障。”然后你点了点头，接下这项任务。老板转身走了，你翻了翻文件，发现纸上只写了公司的名字，Syngress。这家公司你从来没听过，手头也没有其他任何信息。

怎么办？

无论做什么工作，第一步总是调研。准备工作越彻底，成功的几率就越高。创建 Backtrack Linux 的人总喜欢引用亚伯拉罕·林肯（Abraham Lincoln）的一句话：“如果我有 6 个小时来砍一棵树，我会先花 4 个小时把斧头磨锋利。”想要学好渗透测试以及侦察阶段的知识，应该先读懂这句话的含义。

侦察（reconnaissance）也就是信息收集，有人甚至认为这是渗透测试四大步骤中最重要的一环。在收集目标信息上所花的时间越多，后续阶段的成功率就越高。具有讽刺意味的是，侦察这一步骤恰恰是当前整个渗透测试方法体系中最容易被忽略、最不被重视、最易受人误解的一环。

这一步之所以容易被忽略，可能是因为没有人好好向初学者介绍侦察工作的概念和益处，也没有告诉他们做好信息收集工作对后续步骤是多么重要。还有一种可能性，就是侦察工作太没有“技术”含量了。初学黑客技术的人经常会觉得侦察太无趣，一点挑战性也没有。事实上，根本就不是这么回事。

没错，现在的确没有多少工具能够很好地、自动地完成侦察工作，但是一旦你弄明白了其中的基础原理，就能以全新的视角来看待这一阶段。优秀的信息收集者应同时具备以下几个身份：黑客、社会工程师和私家侦探。侦察之所以与其他步骤不同，除了缺乏可用的工具之外，也没有什么定义严格的规则能够明确地区分出侦察中的不同阶段。这种现状与方法论中的其他步

骤有着天壤之别。例如，第3章讨论的扫描就有特定的顺序和清晰的步骤序列，为了顺利完成对目标的扫描，只需要遵照这些步骤进行就可以了。

对于生活在当今世界的任何人而言，学习如何执行数字侦察都是一项宝贵的技能，对渗透测试人员及黑客来说更是无价之宝。出色的侦察可以使测试人员轻易地获得某个网络或系统的控制权，这样的故事在渗透测试领域里俯拾皆是。

考虑下边这个例子：假设有两种罪犯，正准备抢银行。第一种罪犯买了一支枪，冲进他找到的第一家银行，大喊：“把手举起来！把钱都掏出来给我！”不难想象这样的场面得有多混乱，而且即使这家伙拿钱跑了，恐怕用不了多久就得让警察给发现、逮捕，然后关进监狱。对比好莱坞电影里经常出现的另一种情景：罪犯在动手之前花几个月时间做计划、定步骤、巧安排，仔细检查每一个环节。还要花时间匿名买武器、安排逃脱路线、详细研究大楼平面图。此外，他们还得去银行踩点，了解摄像头的位置和记录安保部署情况，推测银行什么时候现金最多、什么时间防备最薄弱。很明显，第二种罪犯更有可能顺利抢到钱并安全撤离。

很明显，以上两种情形的区别在于准备工作和事前做的功课。黑客活动和渗透测试也是一样的道理，不能仅仅获得了个IP就开始运行Metasploit（其实也不是不可以，但效率肯定会很低）。

再回到本章开篇的例子。老板让你完成一次渗透测试，却没提供什么信息，就只给了公司的名字。每一个雄心勃勃的黑客都会问这样的问题：“只知道公司的名字，我得怎样才能控制网络内部的系统呢？”一开始，我们对这家机构真是一无所知：公司网站、地理位置、员工数目等，一概不知。不知道公共IP地址、内部IP方案，当然也不清楚这家公司的技术部署情况以及所使用的操作系统和防御措施。

步骤1以彻底地搜索目标的公共信息作为开始。这个步骤有一点好处是，大多数情况下，不用向目标发送数据包也能收集到海量数据。虽然侦察阶段所用到的某些工具确实会直接向目标发送信息，但要分清楚哪些工具会跟目标联络，哪些不会，这一点很重要。该步骤有两个主要任务：第一，收集与目标有关的信息，越多越好；第二，分类所有收集的信息，创建可进行攻击的IP地址列表。

第1章讲过，白帽黑客和黑帽黑客的主要区别在于授权。步骤1为我们提供了能够体现这种区别的范例。两种黑客都对目标进行了详细的侦察。但是，恶意的黑客根本不受范围和授权的约束。

道德黑客展开调研的时候，他必须确保自己始终保持在测试的范围之内。在信息收集过程中，黑客完全有可能发现某个脆弱的系统，它与目标有关系，但不属于目标所有。即使通过这个相关的系统能够进入最初设定的目标机构，倘若没有事先获得授权，白帽黑客是不允许利用或借助该途径的。举个例子，假设你正针对某个公司做渗透测试，然后你发现这家公司的Web服务器（包含客户记录）已外包或托管给第三方。假如你在客户网站上发现一个严重的漏洞，但没有明确获得测试和利用该网站的授权，那么你必须忽略这个漏洞。而黑帽黑客并不受这些条条框框的约束，他们会借助一切手段入侵目标系统。大多数情况下，因为无权测试并检查这些外部系统，所以也无法提供大量细节。但在你的最终报告中，必须提供尽可能多的信息，指出你认为有可能给目标机构带来风险的系统。

若想要侦察工作能够顺利进行，必须先制定策略。几乎各种信息的收集都需要借助互联网的力量。典型的策略应该同时包含主动和被动的侦察。

主动侦察 (*active reconnaissance*) 包括与目标系统的直接交互。必须注意的是，在这个过程中，目标可能会记录下我们的IP地址及活动。

被动侦察 (*passive reconnaissance*) 则利用从网上获取的海量信息。当执行被动侦察的时候，我们不会直接与目标交互，因此目标也不可能知道或记录我们的活动。

前面提到过，侦察的目的在于尽可能多地收集与目标相关的信息。在渗透测试的这个阶段，不能忽视任何细节，哪怕是看起来无关痛痒的。收集信息的时候，应该将数据集中保存。可能的话，最好都以电子格式保存。这可以方便后期进行快速而精准的搜索。每个黑客都有自己的习惯，有的黑客更喜欢把收集到的所有信息打印出来。每张纸都认真归类并放进文件夹里。如果你也要使用这种传统的收集方式，记得要仔细整理你的记录。用纸作为介质收集材料的话，就算只是针对一个目标，也会很快就用完几百页纸。

大多数时候，首先需要定位目标的网站。在该例子中，可以在搜索引擎上直接查找名字是“Syngress”的网站。

2.2 HTTrack：网站复制机

一般情况下，步骤1首先要做的是仔细浏览目标的网站。有些时候，实际上我们可能要用一款叫做 HTTrack 的工具，将整个网站逐页复制下来。HTTrack 是一款免费的实用工具，能够创建与目标网站完全相同的脱机副本。复制的内容包含原始网站所有的网页、链接、图片和代码。不过，这些文件将储存在你的本地电脑里。利用 HTTrack 这类网站复制工具，可以在脱机状态下尽情挖掘某个网站的资源，而不用花时间在目标公司的 Web 服务器上闲逛。

补充资源

必须要懂得，你浏览和摸索目标网站所花的时间越多，你的活动就越有可能被跟踪（哪怕只是随意浏览网站）。记住，只要是属于目标的资源，任何时候与之直接交互，都有可能留下数字痕迹（digital fingerprint）。

高级渗透测试人员也会利用自动化工具，从某个网站的本地副本中提取额外或者隐藏的信息。

HTTrack 可以直接从该公司的网站 (<http://www.httrack.com>) 下载。在 Windows 系统下安装该软件就和下载这个软件一样简单，只要一直单击“下一步”按钮就可以了。如果你想在 Backtrack 上安装 HTTrack，需要像第1章里所说的，首先连接互联网，然后打开终端，输入如下语句：

```
apt-get install webhttrack
```

程序安装完毕之后，可以通过单击 K-Start → Internet（互联网）→ WebHTTrack Website Copier（见图 2-1）找到 HTTrack。K-Start 的图标是一条龙，在屏幕的左下角。单击该图标，可以发现许多内置在 Backtrack 中的工具。K-Start 和微软众多操作系统中的 Windows 或“开始”按钮一样。

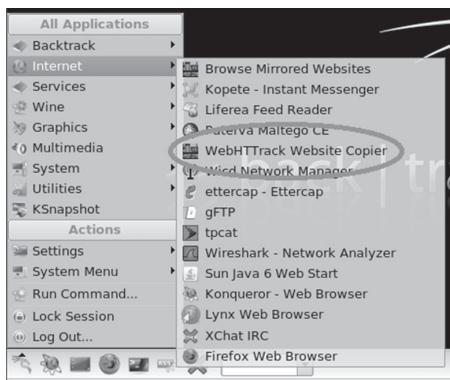


图 2-1 访问刚安装的 HTTrack

HTTrack 安装好了之后，就可以针对目标网站运行该软件。请记住，这种行为很容易被跟踪，同时也会被视为极具攻击性。没有事先获得授权的话，不要运该工具。启动 HTTrack 之后，会出现若干网页，可以对复制过程进行设置和定制。每个页面都有不同的选项，可以对程序的不同方面进行设置。例如，可以更改程序语言（默认为英语）、项目名称、网站复制后存放的位置，以及准备复制的网站地址。可以根据需要按照你自己的习惯一步一步更改设置，然后单击“Next”（下一步）按钮。最后的配置页面包含一个“Strat”（开始）按钮，如果已经做好目标网站复制的准备，就可以单击该按钮。复制过程所需的时间取决于目标网站的大小。HTTrack 完成整个网站的复制任务之后，将提供一个网页，通过它可以在浏览器里 Browse the Mirrored Website（浏览镜像网站），也可以打开保存网站的路径浏览保存的网站。

不管是把整个网站复制下来，还是实时浏览网站，都要记得关注细节。一开始就应该不断总结并记录下你在目标网站上找到的所有信息。通常情况下，不需要挖太深就能有一些重大发现，例如，物理地址和位置、电话号码、电子邮箱地址、运营时间、商业关系（伙伴关系）、员工的姓名、与社会化媒体的联系，以及其他公开的花絮趣闻。

做渗透测试时，通常需要特别关注“新闻”和“公告”这类的信息，这很重要。公司经常都会对自己的成就感到骄傲，在这类报道中就会不小心泄露有用的信息。企业兼并与收购也会产生有用的数据，在扩大渗透测试范围、

增加新的目标时就显得尤其重要。收购过程再顺利，也会对企业的组织架构带来变动和混乱。而在企业兼并过程中，总会有一段过渡期，这就为我们创造了绝佳的机会，可以充分利用这种变动和混乱。哪怕兼并事件已是旧闻，或者过程波澜不惊，这类信息总有其用武之地，可以为我们提供新的目标。被兼并或合并的企业，对它们的测试也必须获得他们的授权，并加入到最初的目标列表中，因为它们也可能会有进入母公司的入口。

最后，还要搜索并检查目标公司挂在网上招聘启事，这很重要。因为在这类启事中经常会详细地说明它们所使用的技术。很多时候，在招聘启事上就可以直接了解招聘单位的软硬件使用情况。同时，别忘了在全国人力资源中心搜索关于目标的信息。举个例子，如果你发现这么一则招聘启事：岗位是网络管理人员，要求具备使用思科 ASA 防火墙的经验，看到这样的启事，则马上就可以得到一些结论，并可以据此作一些大胆的猜测。首先可以确定的是，这家公司要么正在用，要么准备采用思科的 ASA 防火墙。然后，根据企业的规模，可以推测这家公司要么一直紧缺懂得使用并设置思科 ASA 防火墙的人员，要么就是这方面的人员即将离职。无论哪一种情况，关于这家公司所使用的技术，你都已经获得了宝贵的信息。

大多数情况下，只要彻底检查目标的网站，就能对目标有一个很全面的了解，包括这是什么样的公司、具体做什么业务、公司设在哪里。

有了这些目标的基本信息之后，就可以进入被动侦察阶段。一家公司想知道是不是有黑客或渗透测试员在做被动侦察，就算不是不可能，也是十分困难。被动侦察对黑客来说，是一项低风险、高回报的工作。我们提到过的，被动侦察不会向目标系统发送任何数据包。在被动侦察中，我们所要用到的一个武器是互联网。首先要做的是利用各个搜索引擎对目标进行地毯式的搜索。

现今是有不少还不错的搜索引擎，但因为现在我们只涉及黑客和渗透测试的基础知识，所以我们侧重介绍 Google 引擎。Google 对于做这项工作来说简直就是利器。Google 公司的股票每股高达 400 ~ 600 美元，是有一定道理的。Google 的网络爬虫遍及互联网各个角落，夜以继日、不知疲惫地搜索并索引任何抓得到的信息，然后发回 Google。该搜索引擎工作效率极高，黑客经常只需要 Google 就能完成整个渗透测试工作。

在第 13 届 Defcon 黑客大会上，Jonny Long 发表了题为“渗透测试人员应该知道的 Google 黑客技术”（Google Hacking for Penetration Testers）的演讲，震动了整个黑客社区。随后他还出版了一本书，详细介绍了 Google 黑客的艺术。

这里不会详细介绍用 Google 进行入侵的方方面面，但想要成为一名熟练的渗透测试人员，必须扎实地理解如何正确使用 Google。随便找一个人，问他：“Google 要怎么用？”他会说：“这个，很容易的……你打开浏览器，然后打开 Google 的主页，然后在搜索框里输入你想搜索的关键字。”

补充资源

如果你对渗透测试有兴趣，强烈建议你观看 Defcon 的相关视频，并购买 Jonny 写的这本书。视频可以在线免费观看（查找 Defcon 网站的视频库就能找到），该书由 Syngress 公司出版发行，随便一家书店都能买到。Jonny 的发现永久性改变了渗透测试与安全领域，他的演讲和著述都很精彩，绝对值得你花时间好好研读。

这样的回答对地球上 99% 的人来说就很好了，但对于有理想有抱负的黑客来说还远远不够。你必须学会各种使用技巧，这样才能最大化地搜取所要的结果。简而言之，你必须练好 Google 搜索这门绝世武功。学会正确使用 Google 这样的搜索引擎会让你事半功倍，并在浩瀚无垠的网页大海中捞到隐藏在深处的宝藏。

2.3 Google 指令——Google 搜索实践

幸运的是，Google 为我们准备好了“指令”（directive），它简单易学，可以最大限度帮助我们完成每一次搜索。这些指令其实就是一个个的关键字，能够让我们从 Google 的索引文件中更准确地提取信息。

举个例子：假设你在达科他州立大学（Dakota State University）的官方网站（dsu.edu）上搜索与我（作者）相关的信息，最简单的做法就是在 Google 搜索框里输入“pat engebretson dsu”（不含引号）。然后你就能看到不少的搜索结果。只是，在 Google 返回的前 50 条搜索结果中，只有 4 条直

接来自于该大学的官方网站。

如果使用 Google 指令，就能强制该搜索引擎按要求显示索引数据。回到刚才的例子，关键字和网站我们都已经知道。具体来说，我们希望 Google 只显示来自于某个目标域名（dsu.edu）的相关搜索结果。这时候，就需要用到“site:”指令。使用这条指令，Google 不但会返回与关键字相关的网页，而且只显示来自于某个具体网站的搜索结果。

正确使用 Google 指令，需要输入三项内容：

- 1) 你想要用的指令；
- 2) 半角冒号（:）；
- 3) 指令中要用到的具体的内容。

输入这三项内容之后，接下来就和普通搜索没什么两样了。要使用“site:”指令，需要在 Google 搜索框里输入：

```
site:domain term(s) to search
```

注意指令、半角冒号和域名三者之间没有空格。在前面的例子中，我们想在达科他州立大学官方网站上搜索与 Pat Engebretson 有关的信息。要达到这个目的，只需要在 Google 搜索框里输入：

```
site:dsu.edu pat engebretson
```

这次搜索返回的结果与第一次大不相同。首先，原来的搜索结果高达 600 条以上，现在只剩下大约 50 条。很明显，50 条比 600 条记录更易于分类和收集信息。其次，可能也是更重要的，这 50 条记录全部直接来自于目标网站。使用“site:”指令可以很方便地搜索某一目标网站，找寻其他有用的信息。使用这条指令可以避免搜出一大堆不加区分的内容，可以将注意力集中到有用的搜索结果上。

注意

Google 不区分大小写，所以不管输入的是“pat”、“Pat”还是“PAT”，结果都一样。

另外，Google 的“intitle:”和“allintitle:”指令也很好用。在搜索框里加入这两条指令中任意一条的话，只有当网页标题包含所搜索的关键字时，它才会出现在搜索结果里。“intitle:”和“allintitle:”的区别很明显，

“allintitle:” 表示网页标题必须包含所有关键字才会出现在搜索结果里，而“intitle:”不用包含全部关键字，只要包含任意一个关键字即可。

使用 “allintitle:” 指令执行 Google 黑客攻击的经典例子是进行如下搜索：

```
allintitle:index of
```

执行该搜索，就能查看 Web 服务器上的所有可用的索引目录列表。这通常也是侦察信息的宝库。

如果想要搜索 URL 中包含某些特定字符的网站，可以使用 “inurl:” 指令。例如，如果执行下面这条命令，就有可能发现目标网站上许多有意思的页面：

```
inurl:admin
```

这条命令在发现目标网站的管理或设置页面方面极其有用。

搜索 Google 的网页快照可能比搜索目标网站更有价值，因为这样做不但减少你在目标服务器上留下的痕迹，你的活动不容易受到跟踪，而且能有机会浏览原网站上已移除的网页和文件。只要是 Google 爬虫抓取过的网页，都会在 Google 网页快照中保存一个精简过的副本。重要的是要理解，这些网页快照不仅包含网站创建时所用到的代码，还会有爬虫抓取过程中发现的许多文件。这些文件的格式可能是 PDF，也可能是 Word 和 Excel 等微软 Office 文档文件，或者文本文件等。

不小心把重要信息放到互联网上，这也不是什么稀奇的事情。举个例子，假设你是某家公司的网络管理员。你用微软的 Excel 软件创建了一个简单的工作簿，里面包含你管理的网络中的所有电脑的 IP 地址、计算机的名称和所在位置。你决定把这个文件放到内部网，只有公司内部的人员才能浏览，这样也避免到哪儿都要带着这个文件。遗憾的是，你本来是想把它放在内部网上，结果却不小心发布到公司互联网网站上了。在你撤下这个文件之前，可能已经被 Google 爬虫抓到手了。这么一来，就算你后来把这个文件删除，很可能在 Google 网页快照里还是可以搜索得到。所以说，搜索 Google 的网页快照是很重要的。

使用 cache: 指令就可以让 Google 只显示网页快照里的信息。使用下面这条搜索命令就会显示网页快照里的 Syngress 主页：

cache:syngress.com

要知道，单击任何网址链接都会跳转到真实的网页，而不是快照版本的网页。如果你想浏览快照里的某些网页，就需要修改搜索命令。

最后我们再来聊一聊“filetype:”指令。用这个指令可以搜索特定的文件扩展名，当你需要搜索目标网站上的特定类型的文件时，这个指令就很有用。例如，如果只想搜索 PDF 文档，则可以执行下面这条命令：

filetype:pdf

用这个指令还能查找扩展名为 .doc、xlsx、ppt、txt 等。选择几乎是无限的，可以查找任意的文件类型。

想要获得更加强大的功能的话，可以在搜索时将多个指令搭配起来使用。例如，如果我们想找出达科他州立大学网站上所有的 PowerPoint 演示文稿，可以在搜索框里输入以下命令：

site:dsu.edu filetype:ppt

这样一来，返回的搜索结果都将是 PPT 文档，而且全部直接来自 dsu.edu 这个域名。从图 2-2 的截图我们可以看到两次不同的搜索：第一次使用了 Google 指令，而第二次只是一次传统的搜索。使用 Google 指令可以大幅减少搜索结果。（足足少了 33 364 个！）

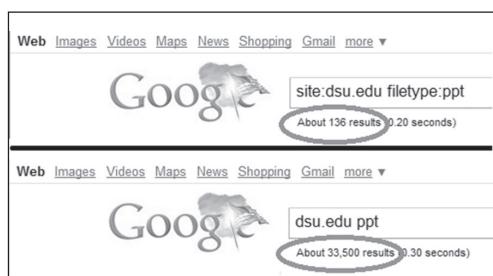


图 2-2 Google 指令的力量

还有很多其他不同类型的指令和 Google 黑客技巧，你应该尽快熟悉它们。除了 Google，还应该能够熟练使用其他搜索引擎才行。不同搜索引擎经常能够提供不同的结果，哪怕你输入了相同的关键字。身为一名渗透测试人员，做侦察工作时信息当然是越详细越好。

最后要提醒一点，我们说的是被动侦察，但也仅仅是搜索的时候才是被

动的。一旦你单击搜索结果的任何一条链接，就会建立起与目标系统的联系，也就回到了主动侦察模式。记住，如果没有事先获得授权，那么主动侦察很可能是非法活动。

当你彻底浏览了目标网页，并借助 Google 和其他搜索引擎开展了地毯式的搜索之后，别忘了，还要检查互联网的其他各个角落，这也是很重要的。像 UseNet 和 Google Groups 这种新闻组和 BBS，对收集目标信息也是相当有用的。人们会在这些讨论网站上就技术问题提问，经常也会得到其他人的帮助。员工经常会在提问题的时候写得很详细，甚至包含敏感和涉密的信息，这种情况说起来既不幸，又很幸运，就像是每个硬币都有两面一样。例如，也许某个网络管理员在配置防火墙的时候出了点问题，他在公开的论坛上把整个配置文件都贴出来讨论，这种现象并不少见。更糟糕的是，有些人甚至用公司的邮箱发表帖子。对攻击者而言，这些信息简直就是金矿。

聪明的网管也许不会把详细的配置文件贴出来，但是想要获得社区同仁的帮助，一点儿信息不泄露几乎是不可能的。就算发布之前帖子里的敏感信息都清除干净了，仔细阅读的话，经常还是能发现软件的版本、硬件型号、当前的配置信息以及与内部系统相关的诸如此类信息。这些信息应该都收集起来，以备未来不时之需。

公共论坛是分享信息、寻求技术支持的好去处。但在利用这些资源的时候，应该尽可能使用像 Gmail 或 Hotmail 等可以匿名的公共电子邮箱地址，避免使用公司邮箱。

近年来 Facebook、MySpace、Twitter 等社交媒体呈爆炸式发展的同时，也为我们挖掘数据提供了新的途径。执行侦察时，应该好好利用这些网站。想象一下这样一个虚构的场景：你正针对一家小公司进行渗透测试。你正做着侦察工作，然后发现这家公司的网络管理员同时拥有 Twitter 和 Facebook 的账号。稍微利用一下社会工程学的技巧，在 Facebook 和 Twitter 上加这位不知情的网管为好友，关注他的动态。也许几个星期下来，你所看到的全是一些无聊的微博。然后突然有一天，“猛料”来了。他在 Facebook 上发表了这段文字：“这下好了，今天防火墙突然坏掉，连点告警都没有。新的明天才能送来。看来想要一切恢复正常，明晚要通宵了。”

再举个例子，某计算机技术人员可能会发微博，说：“微软新补丁出了问

题，只好卸载。明早给微软打电话吧。”

甚至还可能有这样的微博：“年度预算尘埃落定，看来明年还得接着用Server 2000 啊。”

这三个例子也许读起来有点夸张，但只要稍稍关注一下员工在线发布的言论，你会惊奇地发现，网上能收集到大量有用的信息。

2.4 The Harvester：挖掘并利用邮箱地址

The Harvester 是一款可用于侦察的优秀工具。它简单却十分有效，是 Edge Security 安全公司的 Christian Martorella 用高效的 Python 脚本语言编写的，可以快速准确地给电子邮件及其子域名建立目录，这两项内容与目标系统直接相关。

尽量使用最新版本的 The Harvester 很重要，因为许多搜索引擎会定期升级并修改系统。搜索引擎行为的变化，哪怕再细微，都可能导致自动化工具效率低下。在一些情况下，搜索引擎会将结果事先过滤，然后再将结果返回给你。许多搜索引擎甚至还会采用限制技术，阻止使用自动化搜索工具。

The Harvester 可用于搜索 Google、Bing 和 PGP 服务器的电子邮件、主机以及子域名。还能搜索 LinkedIn 的用户名。大多数人都以为他们的电子邮件地址不会有危害性。前面我们已经提到过使用公司电子邮件地址在公共论坛上发布帖子的风险。其实还有其他的风险，必须要引起注意。假设你在侦察过程中发现目标公司某个员工的电子邮箱，只要对邮箱中“@”符号前面的字符加以修改和操作，就能得到一大串可能是准确无误的网络账号。企业经常拿员工的名字作为账号和邮箱用户名（即“@”符号前面的那一串字符），这种做法相当普遍。只要知道了几个可能准确的用户名，我们就可以强行登录到 SSH、VPN 或 FTP 等任何一个服务中。接下来的步骤 3（扫描），我们将详细讨论这个话题。

补充资源

如果你用的操作系统不是 Backtrack，可以登录 www.edge-security.com 直接从 Edge Security 公司的网站：<http://www.edge-security.com> 上

下载这个工具。下载完毕之后，在终端中输入如下命令，将下载的 .tar 文件进行解压：

```
tar xf theHarvester
```

请注意，解压时，命令行中的“H”是大写的。Linux 区分大小写，所以“theHarvester”和“theharvester”在 Linux 中是不一样的。你得留心这个可执行文件，才能确定到底是大写还是小写的“h”。如果没有正确输入大小写字母，终端通常会给出提示消息：“没有这样的文件或目录”。这句话就是在提醒你，文件名拼错了。

Backtrack 本身已内置了 The Harvester。要使用这个工具，可按照以下步骤进行：

- 1) 单击位于屏幕左下角的 K-Start 龙图标。
- 2) 将鼠标指向菜单顶端的 Backtrack。
- 3) 进入 Information Gathering（信息收集）。
- 4) 进入 All（所有）。
- 5) 单击 The Harvester（注意，所有工具按字母顺序排列）。

也可以直接打开终端窗口，然后用下面的命令进入 The Harvester 的目录：

```
cd /pentest/enumeration/google/theharvester
```

无论你使用的是下载的 The Harvester、还是使用安装在 Backtrack 上的 The Harvester 版本，它都可以用来收集与目标相关的额外信息。确信你已进入 The Harvester 的目录，然后运行以下命令：

```
./theHarvester.py -d syngress.com -l 10 -b google
```

这条命令将搜索属于 syngress.com 的电子邮箱、子域名和主机。搜索结果如图 2-3 所示。

在进一步分析这个工具的搜索结果之前，我们先来仔细看一看上面这行命令。“./theHarvester.py”用来调用这个工具，小写的“-d”用来指定目标的域名。小写的“-l”（是小写的 L 字母，不是数字 1）用来限定返回的搜索结果的数目。在本例中，我们要求这个工具只返回 10 个结果。“-b”用来指定将要搜索的公共知识库，可以选择 Google、Bing、PGP 或者 LinkedIn。在本例中，我们选择的是 Google。

现在你已经充分理解这行命令的含义了，那我们再来看一看搜索结果。

```

root@bt:/pentest/enumeration/google/theharvester# ./theHarvester.py -d syngress.com -b google
=====
*TheHarvester Ver. 1.6 *
*Coded by Christian Martorella *
*Edge-Security Research *
*cmartorella@edge-security.com *
=====

Searching for syngress.com in google :

Accounts found:
=====
solutions@syngress.com
www.solutions@syngress.com
sales@syngress.com
[REDACTED]@syngress.com
Solutions@syngress.com
[REDACTED]@syngress.com
=====

Total results: 6

Hosts found:
=====
www.syngress.com
booksite.syngress.com
.syngress.com
ebook_www.syngress.com
root@bt:/pentest/enumeration/google/theharvester#

```

图 2-3 The Harvester 的搜索结果

从图 2-3 中可以发现，The Harvester 至少搜索到 2 个电子邮箱地址，这些邮箱地址对我们可能会有用处。请注意，截图中的电子邮箱被圈了出来并打上了马赛克。此外，The Harvester 还至少搜索到 2 个额外的子域名。需要对“booksite.syngress.com”和“ebook_www.syngress.com”这两个子域名进行彻底侦察。我们直接把这两个新的域名添加到目标列表之中，然后重启侦察进程。

侦察工作的第一步经常是反反复复的，因为每次深入侦察经常会挖出一些新的目标，这样一来就又需要开始新的侦察过程。也正因如此，这个阶段所需花费的时间就很不好说了，几个小时或几个星期都有可能。记住，一个有决心的恶意黑客不但很清楚良好侦察的力量，也深知所需花费的时间难以估计。作为一名有抱负的渗透测试者，你更应该尽可能抽时间多加练习，并动手实践一下信息收集工作。

2.5 Whois

收集与目标相关的额外信息，其实还有一个简单却有效的工具，那就是 Whois。利用 Whois 服务，可以获取与目标相关的具体信息，包括 IP 地址或

公司 DNS 主机名以及地址和电话号码等联系信息。

Linux 操作系统已内置了 Whois。要使用这项服务，最简单的办法是打开终端，输入如下命令：

```
whois target_domain
```

例如，要查询与 Syngress 相关的信息，可以输入如下命令：whois syngress.com。图 2-4 显示了使用这个工具所得到的部分结果。

```
root@bt:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:~# whois syngress.com
Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.
for detailed information.

Domain Name: SYNGRESS.COM
Registrar: SAFENAMES LTD
Whois Server: whois.safenames.net
Referral URL: http://www.safenames.net
Name Server: NS1.DREAMHOST.COM
Name Server: NS2.DREAMHOST.COM
Name Server: NS3.DREAMHOST.COM
Status: ok
Updated Date: 23-sep-2009
Creation Date: 10-sep-1997
Expiration Date: 09-sep-2015
>>> Last update of whois database: Sun, 14 Nov 2010 19:20:36 UTC <<<
```

图 2-4 Whois 查询所返回的部分结果

记录下所有信息，特别留意 DNS 服务器，这一点很重要。如果返回的 DNS 服务器像图 2-4 所示的那样只列出名字，我们可以利用 host 命令将名字翻译成 IP 地址。下一节我们将详细讨论 host 命令的使用。也可以在网页浏览器里搜索 Whois。打开 <http://www.whois.net> 网站，就可以在 WHOIS Lookup（WHOIS 查询）框里进行搜索了，如图 2-5 所示。



图 2-5 Whois.net——基于网页的查询工具

再次提醒，应细致检查你所查询到的信息。有时候搜索结果并没有太多

细节。这时我们可以查询原先 Whois 搜索出来的具体服务器列表，以获取额外的细节。图 2-6 即是一个例子。



```

WHOIS information for syngress.com :

[Querying whois.verisign-grs.com]
[whois.verisign-grs.com]

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: SYNGRESS.COM
Registrar: SafeNames Ltd
Whois Server: whois.safenames.net
Referral URL: http://www.safenames.net
Name Server: NS1.DREAMHOST.COM
Name Server: NS2.DREAMHOST.COM
Name Server: NS3.DREAMHOST.COM
Status: ok
Updated Date: 23-sep-2009
Creation Date: 10-sep-1997
Expiration Date: 09-sep-2015

```

图 2-6 Whois 的搜索结果显示出哪些地方可以找到额外的信息

我们可以使用 Whois 对“引用 URL：(Referral URL:)”字段提供的链接地址做进一步的搜索。可能需要搜索这个网页，以找到这个网页的 Whois 服务链接。利用 Safename 的 Whois 服务，我们可以提取出大量的信息，如下所示：

```

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.[whois.safenames.net]
Safenames Whois Server Version 2.0

Domain Name: SYNGRESS.COM

[REGISTRANT]
Organisation Name: Elsevier Ltd
Contact Name: Domain Manager
Address Line 1: The Boulevard
Address Line 2: Langford Lane, Kidlington
City/Town: Oxfordshire
State/Province:
Zip/Postcode: OX5 1GB
Country: UK
Telephone: +44 (18658) 43830
Fax: +44 (18658) 53333
Email: domainsupport@elsevier.com

[ADMIN]
Organisation Name: Safenames Ltd
Contact Name: International Domain Administrator
Address Line 1: PO Box 5085
Address Line 2:
City/Town: Milton Keynes MK6 3ZE
State/Province: Bucks
Zip/Postcode: MK6 3ZE
Country: UK
Telephone: +44 (19082) 00022

```

Fax:	+44 (19083) 25192
Email:	hostmaster@safenames.net
[TECHNICAL]	
Organisation Name:	International Domain Tech
Contact Name:	International Domain Tech
Address Line 1:	PO Box 5085
Address Line 2:	
City/Town:	Milton Keynes MLO
State/Province:	Bucks
Zip/Postcode:	MK6 3ZE
Country:	UK
Telephone:	+44 (19082) 00022
Fax:	+44 (19083) 25192
Email:	tec@safenames.net

2.6 Netcraft

另外一个搜索信息的好去处是 Netcraft，可以登录 <http://news.netcraft.com> 访问他们的网站。在 What's that site Running?（那是什么网站？）下面的文本框中输入目标网站即可开始搜索，如图 2-7 所示。

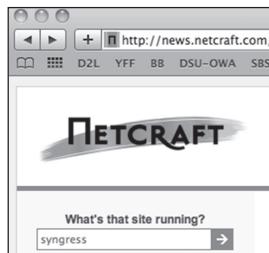


图 2-7 Netcraft 搜索选项

Netcraft 将显示所有它能找到的、包含搜索关键字的相关网站。在本例中，将返回三个网站：syngress.com、www.syngress.com 以及 booksite.syngress.com。如果之前我们的搜索漏掉了哪个网站，要将其加入目标列表之中。搜索结果页面上还可以单击查看 Site Report（网站报告）。如图 2-8 所示，浏览网站报告应该可以发现一些有用的信息。

从图中可以发现，网站报告里有一些十分有用的信息，例如目标网站的 IP 地址、Web 服务器的操作系统以及 DNS 服务器。所有这些信息也需要编目并记录。

Site report for syngress.com				
Site	http://syngress.com	Last reboot	unknown	Uptime graph
Domain	Syngress.com	Netblock owner	New Dream Network, LLC	
IP address	69.163.177.2	Site rank	20511	
Country	US	Nameserver	ns1.dreamhost.com	
Date first seen	March 2000	DNS admin	hostmaster@dreamhost.com	
Domain Registrar	enom.com	Reverse DNS	ps14872.dreamhost.com	
Organisation	Syngress Publishing	Nameserver Organisation	unknown	
Check another site:	<input type="text"/>	Netcraft Site Report Gadget	[More Netcraft Gadgets]	
Hosting History				
Netblock Owner	IP address	OS	Web Server	Last changed
New Dream Network, LLC 417 Associated Rd. PMB 257 Brea CA US 92821	69.163.177.2	Linux	Apache	13-Sep-2010
New Dream Network, LLC 417 Associated Rd. PMB 257 Brea CA US 92821	69.163.177.2	Linux	Apache	24-Feb-2010
New Dream Network, LLC 417 Associated Rd. PMB 257 Brea CA US 92821	69.163.177.2	Linux	Apache	23-Feb-2010

图 2-8 Syngress.com 的网站报告

2.7 host 工具

做侦察时经常会收集到主机名，而不是 IP 地址。出现这种情况的时候，就需要使用“host”工具来将 IP 地址翻译出来。Backtrack 内置了这个 host 工具，直接打开终端，输入以下命令就可以使用：

```
root@bt~# host target_hostname
```

此前搜索时，我们发现了一个 DNS 服务器，主机名为“ns1.dreamhost.com”。为了把它翻译成 IP 地址，可以在终端中输入如下命令：

```
host ns1.dreamhost.com
```

图 2-9 显示了这个 host 命令的结果。

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt: # host ns1.dreamhost.com
ns1.dreamhost.com has address 66.33.206.206
```

图 2-9 host 命令的结果

host 命令也可以反过来应用。它可以将 IP 地址翻译成主机名。直接输入以下命令即可：

```
root@bt~# host IP_address
```

使用“-a”参数可以显示详尽的输出，有可能从中发现与目标相关的额外信息。host 手册和帮助文件值得你花时间好好阅读，可以直接在终端窗口中输入“man host”命令查看这些信息。host 帮助文件可以帮助你了解各种各样的选项，好好使用的话，将能够充分利用 host 工具的各种功能。

2.8 从 DNS 中提取信息

DNS 服务器是黑客和渗透测试人员的极佳目标。它上面经常包含对黑客来说十分有用的信息。DNS 是本地网络和互联网的核心组件。它的一个用途就是负责将域名翻译成 IP 地址。对于我们而言，“google.com”要比“http://74.125.95.105”好记得多。但对计算机而言，情况却恰好相反。DNS 就在两者之间充当翻译。

渗透测试人员必须集中精力，研究目标的 DNS 服务器。原因很简单。DNS 要想正常工作，必须首先掌握网络中每一台电脑的 IP 地址及对应的域名。在侦察阶段，如果能够获得一家公司 DNS 服务器的完整权限，那就和“天上掉馅饼”一样幸运。或者，更准确地说，就跟拿到企业蓝图一样幸运，只不过在这种情况下，蓝图中有目标内部 IP 地址的完整列表。别忘了，信息收集的主要目标之一是收集目标的 IP 地址。

除了运气，选择 DNS 作为攻击目标是因为它有一个很有趣的特点，就是这些服务器的运行原则经常是“没到坏掉时就别去管它”。

经验不够丰富的网络管理员在看待自己公司的 DNS 服务器时经常会带着怀疑和不信任的眼光。他们经常会彻底无视这个设备，因为他们还没有充分了解这台服务器。也正因如此，他们不会优先考虑做与 DNS 服务器相关的工作，例如打补丁、升级或更改配置。再加上大部分 DNS 服务器都相当稳定（只要网络管理员不去折腾它的话），而且网管手上也握着各种安全问题的解决办法。这些网管在他们职业生涯的初级阶段就错误地了解到，越少去摆弄他们的 DNS 服务器，出问题的机会就会越少。

对于渗透测试人员来说，考虑到当前未能正确配置或没有打上安全补丁的 DNS 服务器比比皆是，认定现在的网管们通常会以相同的原则运行 DNS 服务器，也就显得顺理成章了。

哪怕上面说的情况只出现在少数几个公司里，我们也非常有可能找到几个没好好打补丁或也没好好升级的目标。因此，逻辑上讲，接下来的问题，当然是如何控制这个“大馅饼”。在开始检查 DNS 服务器进程之前，我们需要一个 IP 地址。在侦察阶段的早期，我们遇到过几个对 DNS 的引用。这些引用中有些是通过主机名实现的，有些则是通过 IP 地址实现的。利用 host 命令，我们可以将任何主机名翻译成 IP 地址，然后将它们加入到潜在的目标列表之中。再次提醒，继续下一步之前，必须再三确保你收集到的 IP 地址是在被授权范围之内。

现在我们手上已经握有了 DNS 的 IP 地址列表，这些地址列表或者是属于目标的，或者服务于目标，现在我们可以开始查询 DNS 以获取更准确的信息了。在和目标 DNS 进行互动之时，首先我们需要试着进行区域传输（zone transfer），虽然这么做现在越来越少见了。

记住，DNS 服务器包含了一系列它所知道的 IP 地址和对应域名相匹配的记录信息。许多网络部署了多台 DNS 服务器，以保证冗余或负载平衡。因此，多台 DNS 服务器之间需要进行信息共享。这个“共享”过程正是通过区域传输实现的。区域传输通常也叫 AXFR，在这个过程中，一台 DNS 服务器将其所有域名与 IP 映射发送到另一台 DNS 服务器。这一过程允许多台 DNS 服务器保持信息同步。

即使我们无法进行区域传输，仍然有必要花时间好好考察一下被授权范围内所有 DNS 服务器。

2.8.1 NS Lookup

NS Lookup 是检查 DSN 的首选工具。这个工具能查询 DNS 服务器，并可能获得 DNS 服务器知道的各种主机的记录。包括 Backtrack 在内的众多 Linux 版本都内置了 NS Lookup，甚至在 Windows 下通过命令行也能使用该工具。NS Lookup 的使用方法在各个不同操作系统下都是相似的，但你还是必须好好研究一下与你所用系统相关的说明。在 Linux 中，可以直接浏览 NS Lookup 的使用帮助文档。打开终端并输入以下命令就可以打开使用帮助：

```
root@bt~# man nslookup
```

NS Lookup 这个工具可以在交互模式下运行。也就是说，先启动这个程

序，然后再输入特定的参数使其运行特定的功能。在终端输入如下命令并回车就可开始使用 NS Lookup 了：

```
root@bt-# nslookup
```

执行 nslookup 命令之后，就可以使用操作系统提供的 NS Lookup 工具了。输入“nslookup”并按回车键之后，通常的“#”提示符就会变成“>”提示符，这时候就可以输入 NS Lookup 执行查找功能所需的各种额外信息了。

我们首先输入关键字“server”，然后输入我们想查询的 DNS 服务器的 IP 地址，以此给 NS Lookup 下达命令。举例如下：

```
server 8.8.8.8
```

NS Lookup 将简单地接受这行命令，然后显示“>”提示符。接着我们要指明所要查询的记录类型。侦察阶段你可能已经发现了许多感兴趣的记录类型。想获得各种 DNS 记录类型的列表及描述信息的话，就需要用到你刚学会的 Google 技巧！如果你只是想查找一般性信息，可以使用“any”关键字，指定记录类型为“任何”类型。

```
set type = any
```

而如果你想查看 DNS 服务器的某些特殊信息，例如目标公司处理电子邮件的邮件服务器的 IP 地址，就可以输入“set type 5 mx”。

我们在接下来的“>”提示符后面输入目标的域名，以此来完成用 NS Lookup 进行的初始 DNS 查询。

假设你想知道 Syngress 处理电子邮件时使用的邮件服务器。前面我们已经发现，Syngress 的其中一个命名服务器是“ns1.dreamhost.com”，所以我们可以用 host 工具迅速查出 ns1.dreamhost.com 对应的 IP 地址。有了这些信息，我们就可以利用 NS Lookup 查询 DNS，并找出 Syngress 的邮件服务器。图 2-10 所显示的就是这个过程的一个例子，邮件服务器的名字已高亮显示，就在屏幕的右下角，我们需要将它加入到我们的潜在目标列表中。

2.8.2 Dig

“dig”也是从 DNS 提取信息的利器。要使用这个工具，只需打开终端，输入以下命令：

```
dig @target_ip
```

```
root@bt: ~ $ dig @target_ip
root@bt: ~ $ host ns1.dreamhost.com
ns1.dreamhost.com has address 66.33.206.206
ns1.dreamhost.com is an alias for ns1.dreamhost.com.
ns1.dreamhost.com has address 66.33.206.206
ns1.dreamhost.com is an alias for ns1.dreamhost.com.
ns1.dreamhost.com has address 66.33.206.206
root@bt: ~ $ nslookup
> server 66.33.206.206
Default server: 66.33.206.206
Address: 66.33.206.206#53
> set type=mx
> syngress.com
Server:       66.33.206.206
Address:      66.33.206.206#53
syngress.com  mail exchanger = 0 elsevier.com.s200a1.psmtp.com
> 
```

图 2-10 使用 host 和 NS Lookup 确定目标公司的电子邮件服务器

显然，你需要把“target_ip”替换成真实的目标 IP 地址。除此之外，用 dig 命令还能轻松进行区域传输。前面已经提到，区域传输就是从 DNS 服务器提取大量记录的过程。在一些情况下，区域传输可能会导致目标 DNS 服务器将它所包含的所有记录发送出去。进行区域传输时，如果你的目标不区分内外网 IP 的话，那么这样的区域传输是非常有利用价值的。用 dig 命令进行区域传输时，可以使用“-t AXFR”参数。

如果我们想将区域传输给 IP 地址为 192.168.1.23 以及域名为“example.com”这样的伪造的 DNS 服务器的话，就可以在终端窗口中输入以下命令：

```
dig @192.168.1.23 example.com -t AXFR
```

如果区域传输获得允许并且不受限制，目标 DNS 服务器就会返回与目标域名相关的主机和 IP 地址列表。

Backtrack 还有许多其他的工具，可用于与 DNS 进行互动。在对 DNS 工作机制有了扎实的理解之后，你还应该积极探索和使用这些工具。进行渗透测试时可能会用到与 DNS 相关的其他工具，请关注本章末尾的一个简短的介绍。

2.9 从电子邮件服务器提取信息

电子邮件服务器可以为黑客和渗透测试人员提供大量的信息。从各方面来讲，电子邮件就像是个通往目标公司的旋转门。如果目标公司拥有自己的电子邮件服务器，那么它经常会成为攻击的热门对象。有一条原则必须牢记：

“你必须放进来的，你就无法进行阻拦。”换句话说，想要正常使用电子邮件的话，外部流量就一定会通过你的路由器、防火墙等边界设备，进入到内部计算机中，进而进入受保护网络的某个地方。

正因如此，通过直接与电子邮件服务器进行交互，我们通常能够获得大量的信息。对电子邮件服务器进行侦察的时候，首先可以向目标公司发送一封附件内容为空的批处理文件或是像 calc.exe 之类的非恶意可执行文件的电子邮件。向目标的电子邮件服务器发送这样的邮件，其目的是让这个公司的邮件服务器对邮件进行检查，然后发送退信。

收到退信消息之后，我们就可以开始尝试提取目标电子邮件服务器的信息。在很多情况下，退信正文会有一段预先准备好的文字，解释说，“如果附件的扩展名带有潜在威胁，服务器将不予接受”。这条信息通常还会指明用来扫描这封邮件的杀毒软件是什么公司的产品，哪个版本号。对于攻击者而言，这是相当有用的信息。

收到电子邮件服务器的退信之后，我们还应该好好检查一下邮件头信息。检查邮件的 Internet 头可以提取出许多与邮件服务器相关的基础信息，例如 IP 地址、具体的软件版本，或者是所运行的电子邮件服务器的品牌。等到我们进入漏洞利用环节，知道 IP 地址和软件版本信息是非常重要的（步骤 3）。

2.10 MetaGooFil

“MetaGooFil”也是信息收集过程中可以利用的优秀软件，由开发 The Harvester 的团队编写而成，可用来提取元数据（metadata）。元数据经常被定义为是关于数据的数据。在我们创建文档时，例如 Word 或 PowerPoint 演示文稿，额外的数据也会被同时创建，并储存在文档里。这些数据通常是对该文档的描述信息，包括文件名、文件大小、作者或创建者的用户名，以及文件保存的位置或路径。这个过程全自动进行，无需用户输入或干预。

攻击者若能读取到这些信息，就能对目标公司的用户名、系统名、文件共享以及其他诸多好东西有独特的见解。MetaGooFil 就是这么一个工具，能在互联网上搜索属于目标的文档。一旦有所发现，MetaGooFil 就会把这些文档下载下来，并尝试提取有用的元数据。

Backtrack 本身已内置 MetaGooFil，在 All Programs（所有程序）菜单里选择 Backtrack option（选项），然后进入 Information Gathering（信息收集）就能找到。同样，也可以直接打开终端，输入如下命令：

```
cd /pentest/enumeration/google/metagoofil
```

进入 MetaGooFil 的目录之后，最好新建一个名为 files 的文件夹，专门用来存放下载的文档，以保持原来目录的结构。输入如下命令新建文件夹：

```
mkdir files
```

目录创建之后，就可以执行如下命令运行 MetaGooFil：

```
./metagoofil.py -d syngress.com -f all -o results -t files
```

我们来详细分析一下上面这行命令。“./metagoofil.py”是用来触发 MetaGooFil 的 Python 脚本。命令行前面的“./”千万别漏掉了。“-d”参数用来指定搜索的目标域。“-f”参数用来指定 MetaGooFil 查找哪一种或哪些类型的文件。“all”参数则是告诉 MetaGooFil 要将所有其能处理的文件格式全都下载下来，包括 ppt、pdf、xls、odp、docx 等。也可以指定唯一的文件类型来限定搜索的结果。用“-o”参数指定 MetaGooFil 生成报告的名称。最后还要指定一个文件夹，以存放 MetaGooFil 发现并下载下来的文件。前面我们已经事先创建了“files”文件夹，因此这时候只要在命令行里输入“-f files”就可以把所有找到的文档保存到这个文件夹里了。

虽然 MetaGooFil 的输出并没有显示与 Syngress 有关的任何信息，但在输出文件的下面有一个最近使用该工具进行渗透测试所产生的输出的一个样本，该样本很明确地给出了一些有额外价值的信息，应该将它们加入侦察数据的宝库中。

```
C:\Documents and Settings\dennis1\My Documents\
```

这个例子给我们带来了不少信息。首先是一个有效的网络用户名“dennis1”。另外，这条信息也清楚地告诉我们，Dennis 用的机器上安装的是 Windows 操作系统。

2.11 社会工程学

不谈社会工程学的话，侦察是不完整的。许多人甚至认为社会工程学是信息收集最简单、最有效的方法之一。

社会工程学是攻击“人性”弱点的过程，而这种弱点是每个公司天然固有的。当使用社会工程学的时候，攻击者的目标是找到一个员工，并从他口中撬出本应是保密的信息。

假设你正在针对某家公司进行渗透测试。前期侦察阶段你已经发现这家公司某个销售人员的电子邮箱。你很清楚，销售人员非常有可能对产品问询邮件进行回复。所以用匿名邮箱对他发送邮件，假装对某个产品很感兴趣。实际上，你对该产品并不关心。发这封邮件的真正目的是希望能够得到该销售人员的回复，这样你就可以分析回复邮件的邮件头。该过程可以使你收集到这家公司内部电子邮件服务器的相关信息。

接下来我们把这个社会工程学案例再往前推一步。假设这个销售人员的名字叫 Ben Owned。（这个名字是根据对公司网站的侦察结果以及他回复邮件里的落款了解到的。）假设在这个案例中，你发出产品问询邮件之后，结果收到一封自动回复的邮件，告诉你 Ben Owned “目前正在海外旅游，不在公司”，以及“接下来这两周只能通过有限的途径查收邮件”。

最经典的社会工程学的做法是冒充 Ben Owned 的身份给目标公司的网络支持人员打电话，要求协助重置密码，因为你人在海外，无法以 Web 方式登录邮箱。运气好的话，技术人员会相信你的话，帮你重置密码。如果他们使用相同的密码，你就不但能够登录 Ben Owned 的电子邮箱，而且能通过 VPN 之类的网络资源进行远程访问，或通过 FTP 上传销售数据和客户订单。

社会工程学跟一般的侦察工作一样，都需要花费时间进行钻研。不是所有人都适合当社会工程学攻击者的。想要获得成功，你首先得足够自信、对情况的把握要到位，然后还得灵活多变，随时准备“开溜”。如果是在电话里进行社会工程学攻击，最好是手头备好各种详尽、清楚易辨的信息小抄，以免被问到一些不好回答的细节。

另外一种社会工程学攻击方法是把优盘或光盘落在目标公司里。优盘需要扔到目标公司内部或附近多个地方，例如停车场、大厅、厕所或员工办公

桌等，都是“遗落”的好地方。大部分人出于本性，在捡到优盘或光盘之后，会将其插入电脑或放进光驱，查看里面是什么内容。而这种情况下，优盘和光盘里都预先装载了自执行后门程序，当优盘或光盘放入电脑的时候，就会自动运行。后门程序能够绕过防火墙，并拨号至攻击者的电脑，此时目标暴露无遗，攻击者也因此获得一条进入公司内部的通道。第6章我们还会专门讨论后门程序。

2.12 筛选信息以寻找可攻击的目标

完成以上步骤之后，你得安排好时间认真整理收集到的侦察信息。大部分情况下，就算是小规模的侦察工作也能收获海量数据。侦察过程结束之时，你对目标应该就有了十分清楚的认识，包括公司组织构架，甚至内部部署的技术。

整理信息的时候，建议创建一个简易的列表，用来集中记录收集到的IP地址。同样的，对于电子邮件地址，主机名称和URL地址等，还应分别为它们维护各自独立的列表。

不幸的是，你收集到的大部分信息都无法帮助你直接发起攻击。整理资料的时候，记得把所有相关的、不是基于IP地址的信息转换为IP地址。利用Google和host命令可以提取与目标相关的额外的IP地址。把这些IP地址添加进IP列表中。

仔细整理过收集来的侦察信息并把这些数据转换之后，我们应该能得到一个可攻击目标的IP地址列表，其中的IP地址就算不属于目标，至少也是相关的。无论什么情况下，都必须牢记我们被授权的范围，因为我们收集到的IP地址不一定是在这个范围之内。因此，侦察阶段的最后一个步骤是检查你所创建的IP地址列表，然后联系这家公司看能否扩大测试范围，或将授权外的IP地址从列表中删除。

到这一步的时候，你手上就有一个IP地址列表，且都是在可攻击的授权范围之内。不要忽视或低估那些收集的不可直接用于攻击的信息。接下来的每一个步骤里，我们都会重新整理并提取步骤1所获得的信息。

2.13 如何实践

现在你对侦察工作所使用到的基础工具和技术已经有了清楚的认识，接下来就应该把学到的知识应用到实践中去。实践的途径有很多，一个简单而有效的方法就是买份报纸，然后把上面的公司都记录下来。如果一时买不到报纸，也可以上新闻网站，www.cnn.com 或 www.msnbc.com 之类的都可以。

把可以将进行侦察的潜在目标做成一个列表，尽量找一些你没听说过的公司。任何一份优秀的报纸，或是优秀的网站，都会出现一大堆你不熟悉的公司。**警告：** 千万不要进行主动侦察！很明显，你手上没有任何授权，自然也不能使用本章讨论的主动技术。当然，你还可以利用我们讨论过的被动侦察技术进行信息收集。做这项工作可以锻炼和提升你的技术，并可借此建立起你自己的系统，用于对收集到的数据进行目录建立、组织和整理。记住，这一步虽然看似最没有技术含量，但经常能获得最好的回报。

2.14 接下来该做什么

经过练习，如果你已经掌握侦察的基础知识，你就拥有了足够的信息和技能，可以开展高级的信息收集工作了。下面列出几种工具和技术，可以使你的信息收集水平更上一层楼：

- Google 以外其他搜索引擎的指令。

即使你的 Google 功夫已经炉火纯青了，你仍需要掌握其他搜索引擎的搜索指令。大部分现代搜索引擎都支持利用指令或其他方式进行高级搜索。记住，不要只依靠一家搜索引擎就想出色地完成全部侦察工作。哪怕是相同的关键字，用不同的搜索引擎搜索出的结果通常是截然不同的，甚至是令人惊喜的结果。

- 搜索引擎评估工具（SEAT）。

SEAT 是一个非常棒的工具，它一次搜索即可同时快速查询出多家不同的搜索引擎。做侦察工作时，经常需要在不同搜索引擎之间来回查询，而这个工具可以自动完成这部分的手工活。Backtrack 已内置这款工具，在它的官方网站 (www.midnightresearch.com) 上也能下载。网站上甚至还提供“如

何使用”的视频教程。

- Johnny Long 的 Google 黑客数据库 (GHDB)。

这只是一个知识库，却包含了迄今为止最有用、最有威慑力的几种 Google 黑客技术！我们一而再、再而三地强调过，**千万不要针对未获授权的目标运行这些查询！**可以登录 www.hackersforcharity.org/ghdb 获取这个知识库。登录网站之后，花几分钟了解一下“慈善黑客协会”(Hackers for Charity) 以及 Johnny 对“以工换粮计划”(food for work) 所做的努力。

- 《渗透测试人员应该懂的 Google 黑客技术》，第 2 版，Syngress 出版。

所有渗透测试人员都必须阅读 Johnny 这本关于 Google 黑客技术的书。

- Paterva 公司出品的 Maltego 社区版。

Maltego 这款软件十分强大，能够聚合公共数据库的信息，然后提供目标公司的详细信息，准确度高到惊人。在它所提供的细节中，有的是技术信息，包括防火墙的位置或 IP 地址，有的则是个人信息，例如某个（正在出差的）销售人员此时的物理位置。掌握这款工具需要费点力气，但绝对值得。Backtrack 内置了一个免费版本。

2.15 小结

对于任何渗透测试或黑客活动，信息收集都是第一步。虽然这个步骤与其他大多数步骤相比，技术含量较少，它的的重要性却不容忽视。收集到的信息越多，渗透测试后续步骤的成功率就越高。一开始你收集到的关于目标的信息可能看起来有点多，但只要好好整理，善用工具并多加练习，很快你就能掌握侦察的艺术。

渗透测试实践指南

必知必会的工具与方法



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

“你是否听说过渗透测试但不知道它包含哪些内容？本书就是你步入渗透测试领域的良好开端，它简单易读，也不需要什么先验知识，而且其内容也是当前最流行的。我诚挚向你推荐Pat的最新力作。”

—Jared Demott, Crucial Security股份有限公司首席安全研究员

本书以“大道至简”的方式阐述了高深的“道德黑客”和“渗透测试”的知识，通过讲解操作案例和技术细节（涵盖四个阶段，其间穿插多种实用、前沿的热点工具和技巧），让你了解通用知识和真正的渗透测试工作；令人期待的是，部分案例为你真实再现好莱坞大片中的神秘“黑客”情景。

本书结合大量可操作性极强的实例和步骤图解，通过输出结果将渗透测试四个阶段和所用工具巧妙关联，使你不再为只知其一而踌躇不前，从而真正掌握渗透测试精髓，余下的提升问题也迎刃而解。

本书主要内容：

- 搭建渗透测试环境技巧及注意事项；
- 侦察阶段的各种可利用工具及其参数设置，包括HTTTrack、Google搜索指令、The Harvester、DNS和电子邮件服务器信息提取、MetaGoos等；
- 扫描系统和网络漏洞的切实可用工具和方法，ping命令和ping扫描、端口扫描（如Nmap、Nessus等）；
- 漏洞利用过程涉及的常用黑客工具和技巧，如密码重置和破解、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；
- 后门和rootkit的利用方法及rootkit的检测和防御，涵盖Netcat、Cryptcat、Netbus等实用工具；
- 如何编写渗透测试报告为你赢得回头客。



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

华章网站 <http://www.hzbook.com>

网上购书：www.china-pub.com

上架指导：计算机/信息安全

ISBN 978-7-111-40141-4



9 787111 401414

定价：49.00元