信息安全技术丛书

The quieter you become,
the more you are able to hear.

PACKT PUBLISHING

Kali Linux :
Assuring Security By Penetration Testing

Kali Linux

渗透测试的艺术

[英] Lee Allen
[印尼] Tedi Heriyanto 著
[英]Shakeel Ali
Archer 译

人民邮电出版社
POSTS & TELECOM PRESS

Kali Linux 渗透测试的艺术

[英] Lee Allen
[印尼] Tedi Heriyanto 著
[英] Shakeel Ali
Archer 译

人 民 邮 电 出 版 社
北 京

版 权 声 明

◆ 著　[英] Lee Allen　[印尼] Tedi Heriyanto
[英] Shakeel Ali
译　Archer
责任编辑　傅道坤
责任印制　张佳莹

◆ 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　印刷

◆ 开本：800×1000　1/16
印张：24.75
字数：505 千字　2015 年 2 月第 1 版
印数：1– 000 册　2015 年 2 月北京第 1 次印刷

著作权合同登记号　图字：01-2014-5790 号

定价：　元

读者服务热线：(010)81055410　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

内容提要

Kali Linux 是一个渗透测试兼安全审计平台，集成了多款漏洞检测、目标识别和漏洞利用工具，在信息安全业界有着广泛的用途。

本书从业务角度出发，通过真实攻击案例并辅之以各种实用的黑客工具，探讨了进行渗透测试所需的各种准备工序和操作流程。本书共分为 12 章，其内容涵盖了 Kali Linux 的使用、渗透测试方法论、收集评估项目需求的标准流程、信息收集阶段的工作流程、在目标环境中探测终端设备的方法、服务枚举及用途、漏洞映射、社会工程学、漏洞利用、提升权限、操作系统后门和 Web 后文的相关技术、渗透测试文档报告的撰写等。

本书适合讲解步骤清晰易懂、示例丰富，无论是经验丰富的渗透测试老手，还是刚入门的新手，都会在本书中找到需要的知识。

关于作者

Lee Allen 是在顶尖大学里任职的安全架构师。多年以来，他持续关注信息安全行业和安全界内的新近发展。他有 15 年以上的 IT 行业经验，并且持有 OSWP 等多项业内的资格认证。

Lee Allen 还是 *Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide*（由 Packt Publishing 出版，人民邮电出版社出版了其中文版）一书的作者。

在此向我的爱人 Kellie 和我们的孩子表示感谢；他们为了本书的创作对我多有照顾。同时，我要向祖父母 Raymond 和 Ruth Johnson，以及岳父母 George 和 Helen Slocum 表示谢意；感谢他们这些年对我的支持和鼓励。

Tedi Heriyanto 是印尼一家信息安全公司的首席顾问。他一直在与（印尼）国内外的多家知名机构进行信息安全渗透测试方面的合作。他擅长设计安全网络架构、部署与管理企业级的信息安全系统、规范信息安全制度和流程、执行信息安全审计和评估，以及提供信息安全意识培训。在闲暇之余，他在印尼安全界的各种活动中不停地研究和学习。他还通过写作各种安全图书与大家分享界内知识。有兴趣的读者可以访问他的博客 `http://theriyanto.wordpress.com`。

感谢我的家人，谢谢他们在本书创作过程中给我的支持。感谢我的老板，谢谢他在本书的创作过程中给予我的信任、帮助和支持。感谢各位同事和客户，你们是我的良师益友。此外，感谢为本书提供宝贵意见和建议的 Packt Publishing 的各位同仁——Rubal Kaur、SwenySukumaran、Joel Goveya、Usha Iyer 和 Abhijit Suvarna。与此同时，感谢为本书投入大量时间和精力并分享了个人经验的技术审稿人 Alex Gkiouros 和 Neil Jones。最后要感谢本书的另外两名作者——Lee Allen 和 Shakeel Ali，他们通过这本书分享了各自的技术知识、热情、想法、挑战和建议，使我陶醉于这本书的创作过程。

最终要感谢的是您——本书的读者，感谢您购买了此书，希望您能喜欢它。祝您在信息安全的工作中一帆风顺。

Shakeel Ali 在世界 500 强公司里担任安全和风险管理顾问。在此之前，他是英国 Cipher Storm Ltd.的核心创始人。他从事过安全评估、系统审计、合规部门顾问、IT 管理和法证调查工作，积累了信息安全领域的各种知识。他还是 CSS Providers SAL 的首席安全员。他以废寝忘食的工作态度，为全球各类商业公司、教育机构和政府部门提供了不间断的安全支持服务。作为一名活跃的业内独立研究人员，他发表了大量的文章和白皮书。有兴趣的读者可以访问他的个人博客 `Ethical-Hacker.net`。此外，他还长期参与墨西哥举办的 BugCon Security Conferences 活动，定期报告最前沿的网络安全威胁，并分享相应的应对方案。

我向参与本书创作的各位朋友、审稿人和同事表示感谢。特别感谢 Packt Publishing 的团队和它们的技术编辑、审稿人，他们分享了无价的意见和建议，是这本书的幕后英雄。在此感谢本书的其他两位作者 Lee Allen 和 Tedi Heriyanto，本书的成功离不开他们不断的奉献、贡献、理念和技术讨论。最后，感谢我迄今为止遇到的各位搭档。他们总是能够在毫不松懈的安防工作中迸发出各种灵感。我相信，没有诸位的共同努力就没有安全稳定的信息安全环境。

关于审稿人

Alex Gkiouros 当前是一名独立的 IT 专业人士，参与过希腊的各种项目。他在 2006 年步入 IT 行业，已经持有 2 个 ISACA 的资格认证，目前在学习 CCNP。他热爱网络安全，并花费大量时间研究 Kali Linux 或 Backtrack。有兴趣的读者可以访问他的个人博客 `http://www.voovode.net/`。

Neil Jones 在一家总部在英国的全球安全公司任职安全顾问。他过去就希望在年轻的时候就进入安全行业，如今他不仅达成这一心愿，而且获取了业内认可的多项资格认证。

他是一名不折不扣的安全研究人员。他从吃饭、睡觉，甚至在呼吸之间都挤出时间进行研究，还为业内开发过多款开放源代码的安全工具。

前言

Kali Linux 是一个渗透测试平台兼安全审计平台，它集成了多款漏洞检测、目标识别和漏洞利用工具。在明确业务目标的情况下，测试人员采取适当的渗透测试方法论，结合详细的测试计划即可进行富有成效的渗透测试。

本书循序渐进地演示了多款尖端的黑客工具，连贯地介绍了各种实用的黑客技术，是一本系统化地讲解渗透测试技巧的图书。它从业务的角度出发，以时下数字时代的真实攻击案例入手，探讨了所需的各种必要的准备工序和测试流程。

本书揭示了渗透测试的最优逻辑思路和业内最佳的测试方法。

本书最先讲解了实验室的制备方法，依次说明了基本的安装和配置方法，讨论了渗透测试的不同类型，介绍了开放的安全测试方法，并提出了 Kali Linux 特有的测试过程。在此之后，本书将遵循正式的测试方法论，依据渗透测试各个阶段（范围界定、信息收集、目标发现、服务枚举、漏洞映射、社会工程学、提升权限、访问维护和文档报告）的需要介绍相应的测试工具。我们会通过真实的渗透案例来演示这些工具的使用和配置方法。本书最后一部分还简要介绍了额外的渗透工具以及渗透测试人员通常会参考的重要资源。

本书从零起步介绍了渗透测试的必备技能，可作为读者专业且实用的专家指导。在学习本书的内容之后，读者可以在现实环境中或者在实验测试平台中使用 Kali Linux 进行渗透测试。

本书内容

第 1 章，Kali Linux 入门。简要介绍 Kali Linux 的 Live DVD 的使用方法。本章首先介绍 Kali Linux 的研发简史和各类工具，然后介绍获取、使用、配置、更新 Kali Linux 的方法，以及多个重要网络服务（HTTP、MySQL、SSH）的配置方法。最后，本章还演示了使用镜像文件安装并配置一台漏洞百出的问题虚拟机，以及安装额外工具包的方法。

第 2 章，渗透测试方法论。探讨了标准渗透测试的基本概念、规则、管理、方法和流程。本章将介绍两种著名的类型渗透测试，即黑盒测试和白盒测试之间的明显区别。另外，它还分析了脆弱性评估和渗透测试之间的区别。本章重点讲解了各种渗透测试方法论的业务特性、功能和优点，分别讨论了 OSSTMM、ISSAF、OWASP 和 WASC-TC。最后，介绍了由 10 个连贯的测试阶段组成的 Kali Linux 的通用渗透测试流程。

第 3 章，范围界定。阐述收集评估项目需求的标准流程。本章将阐述制定渗透测试项目工作路线图所需的各个要素。这个阶段的工作可分为多个关键步骤，即收集需求、筹划工作、边界分析、明确业务指标、项目管理和统筹调度。本章讲解获取测试环境具体信息的方法。

第 4 章，信息收集。介绍信息收集阶段的工作流程。本章首先演示了通过公共资源获取目标环境有关信息的方法，然后介绍了分析 DNS 信息和收集网络路由信息的手段，最后讲解了利用搜索引擎获取目标域名、E-mail 地址和文件元数据的技术。

第 5 章，目标识别。讲解了在被测环境中探索终端设备的方法。本章介绍了目标识别阶段的任务以及相应的工具，以及对目标主机进行操作系统指纹识别的各种工具。

第 6 章，服务枚举。探讨了服务枚举及其用途。本章介绍了端口扫描的概念和相关工具。本章重点介绍 Nmap 的各种可用选项，以及在被测网络中搜索 SMB、SNMP 和 VPN 服务的各种工具。

第 7 章，漏洞映射。讨论了漏洞的两种类型：本地漏洞和远程漏洞。您将在本章了解漏洞区分依据和分类方法，及各种行业标准。此外，本章讲解了 OpenVAS、Cisco、Fuzzing、SMB、SNMP 和 Web 应用程序分析工具，这些工具可以用来查找、分析目标网络种存在的安全漏洞。

第 8 章，社会工程学攻击。介绍了社会工程学专业人员操纵他人，使后者泄露信息或进行某种行为的核心原则和业内认可的做法。本章将阐述社工涉及的基本心理学原理。社会工程学专业人士制定的社工目标和具体方法都是基于这些心理学原理。本章还通过实际案例讲解了社工的攻击流程和攻击方法。本章最后介绍了 Kali Linux 的社会工程学工具集，并演示了利用这些工具攻击人力资源部门的社工方法。

第 9 章，漏洞利用。重点介绍了可切实利用漏洞的实践方法和各种工具。本章讲解了漏洞研究领域的各个方面，以及理解、检验和测试目标环境脆弱性的关键手段。本章还列举了一些知名的漏洞资料库和使用方法。同时，本章还从安全评估的角度讲解了恶名昭彰的开发工具包，并演示了使用 Metasploit 的 exploit 模块编写简单的漏洞利用程序的方法。

第 10 章，提升权限。介绍了提升权限、网络监听及网络欺骗的概念。本章不仅介绍了

通过本地漏洞提升权限的方法，而且介绍了分别以离线和在线的方式碰撞用户密码的工具。本章最后还讲解了可用于网络欺骗和网络监听的多款工具。

第 11 章，访问维护。演示了操作系统后门和 Web 后门的有关技术。本章介绍了各种不同的后门及其使用方法。此外，本章还讲解了多款网络隧道工具，这些工具可以在攻击者和受害者之间建立秘密通信。

第 12 章，文档报告。涵盖了渗透测试文档、汇报文件和现场演示的有关内容。本章内容旨在指导读者以撰写系统化的、结构化的、一致的工程文档。此外，本章还介绍了验证测试结果、报告的不同种类、现场演示及测试的后期流程工作。

附录 A，辅助工具。介绍了渗透测试工作可能会用到的几款额外工具。

附录 B，关键资源。列举了多个可帮助您提高渗透测试技术的参考资源。

阅读群体

本书适合大体了解 UNIX/Linux 操作系统，并了解信息安全各项构成因素的 IT 安全专业人士或网络管理员，以及想要使用 Kali Linux 进行渗透测试的读者。

目录

第 1 部分　系统的搭建与测试

第 3 部分 额外资源

第 1 部分

系统的搭建与测试

第 1 章　Kali Linux 入门

第 2 章　渗透测试方法论

第 1 章

Kali Linux 入门

本章将带领读者初步了解渗透测试专用的独立 Linux 操作系统——Kali Linux。本章涵盖下述主题：

- Kali 的发展简史；
- Kali 的一般用途；
- Kali 的下载与安装；
- Kali 的配置与更新。

在本章的结尾部分，我们还会介绍 Kali Linux 附加功能包和配置工具。

1.1 Kali 的发展简史

Kali Linux（Kali）是专门用于渗透测试的 Linux 操作系统，它由 BackTrack 发展而来。在整合了 IWHAX、WHOPPIX 和 Auditor 这 3 种渗透测试专用 Live Linux 之后，BackTrack 正式改名为 Kali Linux。

BackTrack 是相当著名的 Linux 发行版本。在 BackTrack 发布 4.0 预览版的时候，它的下载次数已经超过了 400 万次。

Kali Linux 1.0 版于 2013 年 3 月 12 日问世。在 5 天之后，官方为修复 USB 键盘的支持问题而发布了 1.0.1 版。在这短短的 5 天之内，Kali 的下载次数就超过了 9 万次。

根据官网的介绍（`http://docs.kali.org/introduction/what-is-kali-linux`），Kali 的主要特色有：

- 它是基于 Debian 的 Linux 发行版；
- 它集成 300 多个渗透测试程序；
- 它支持绝大多数的无线网卡；

- 它修改了内核以支持（无线）数据包注入；
- 所有的软件包都有研发团队的 PGP 签名；
- 用户可以自制满足各自需求的 Kali Linux 发行版；
- 支持基于 ARM 的硬件系统。

1.2 Kali Linux 工具包

Kali Linux 含有可用于渗透测试的各种工具。这些工具程序大体可以分为以下几类。

- **信息收集**：这类工具可用来收集目标的 DNS、IDS/IPS、网络扫描、操作系统、路由、SSL、SMB、VPN、VoIP、SNMP 信息和 E-mail 地址。
- **漏洞评估**：这类工具都可以扫描目标系统上的漏洞。部分工具可以检测 Cisco 网络系统缺陷，有些还可以评估各种数据库系统的安全问题。很多模糊测试软件都属于漏洞评估工具。
- **Web 应用**：即与 Web 应用有关的工具。它包括 CMS（内容管理系统）扫描器、数据库漏洞利用程序、Web 应用模糊测试、Web 应用代理、Web 爬虫及 Web 漏洞扫描器。
- **密码攻击**：无论是在线攻击还是离线破解，只要是能够实施密码攻击的工具都属于密码攻击类工具。
- **漏洞利用**：这类工具可以利用在目标系统中发现的漏洞。攻击网络、Web 和数据库漏洞的软件，都属于漏洞利用（exploitation）工具。Kali 中的某些软件可以针对漏洞情况进行社会工程学攻击。
- **网络监听**：这类工具用于监听网络和 Web 流量。网络监听需要进行网络欺骗，所以 Ettercap 和 Yersinia 这类软件也归于这类软件。
- **访问维护**：这类工具帮助渗透人员维持他们对目标主机的访问权。某些情况下，渗透人员必须先获取主机的最高权限才能安装这类软件。这类软件包括用于在 Web 应用和操作系统安装后门的程序，以及隧道类工具。
- **报告工具**：如果您需要撰写渗透测试的报告文件，您应该用得上这些软件。
- **系统服务**：这是渗透人员在渗透测试时可能用到的常见服务类软件，它包括 Apache 服务、MySQL 服务、SSH 服务和 Metasploit 服务。

为了降低渗透测试人员筛选工具的难度，Kali Linux 单独划分了一类软件 —— **Top 10 Security Tools**，即 10 大首选安全工具。这 10 大工具分别是 `aircrack-ng`、`burp-suite`、

hydra、john、maltego、metasploit、nmap、sqlmap、wireshark 和 zaproxy。

除了可用于渗透测试的各种工具以外，Kali Linux 还整合了以下几类工具。

- **无线攻击**：可攻击蓝牙、RFID / NFC 和其他无线设备的工具。
- **逆向工程**：可用于调试程序或反汇编的工具。
- **压力测试**：用于各类压力测试的工具集。它们可测试网络、无线、Web 和 VoIP 系统的负载能力。
- **硬件破解**：用于调试 Android 和 Arduino 程序的工具。
- **法证调查**：即电子取证的工具。它的各种工具可以用于制作硬盘磁盘镜像、文件分析、硬盘镜像分析。如需使用这类程序，首先要在启动菜单里选择 **Kali Linux Forensics | No Drives or Swap Mount**。在开启这个选项以后，Kali Linux 不会自动加载硬盘驱动器，以保护硬盘数据的完整性。

本书仅介绍 Kali Linux 的渗透测试工具。

1.3　下载 Kali Linux

要安装使用 Kali Linux，首先需要下载它。下载 Kali Linux 的官方网站是 http://www.kali.org/downloads/。

在下载页面中（见图 1.1），您可以通过下列项目选择适用的 Kali Linux 镜像。

图 1.1

- **主机架构**：i386、amd64、armel 或 armhf。
- **镜像类型**：ISO 或 VMware 镜像。

如果您想要把镜像烧录为 DVD 光盘，或者在主机上安装 Kali Linux，就需要下载 ISO 镜像。但是如需在 VMware 里使用 Kali Linux，直接下载 VMware 镜像，然后再在虚拟机环境里安装和配置 Kali 系统更为方便。

在下载镜像文件之后，您需要校验镜像文件的 SHA1 哈希值是否和下载网站上提示的哈希值一致。检查 SHA1 哈希值主要为了确保下载镜像文件的完整性。这步工作可以使您免受文件下载不完整而带来的灾难，也可验证文件是否用被他人蓄意篡改。

在 UNIX/Linux/BSD 操作系统中，您可以直接使用 `sha1sum` 命令检查下载文件的哈希值。因为镜像文件很大，所以计算哈希值的时间可能较长。例如，您可以使用下述指令检查 `kali-linux-1.0.1-i386.iso` 文件的哈希值：

```
sha1sum kali-linux-1.0.1-i386.iso
41e5050f8709e6cd6a7d1baaa3ee2e89f8dfae83 kali-linux-1.0.1-i386.iso
```

很多 Windows 程序都可以生成 SHA1 的哈希值。我们推荐读者使用 `sha1sum`，它可在下述网址下载：`http://www.ring.gr.jp/pub/net/gnupg/binary/sha1sum.exe`。

`sha1sum` 短小实用。如果您想要尝试其他程序，可考虑 `HashMyFiles`（`http://www.nirsoft.net/utils/hash_my_files.html`）。`HashMyFiles` 能够计算 MD5、SHA1、CRC32、SHA-256、SHA-384 和 SHA-512 算法的哈希值。

下载 `HashMyFiles` 之后，打开这个程序，在菜单里选择 **File | Add Files** 或直接按快捷键 F2，则可添加需要计算哈希值的文件。

使用 `HashMyFiles` 计算 Kali Linux i386 ISO 镜像的哈希值，情况会如图 1.2 所示。

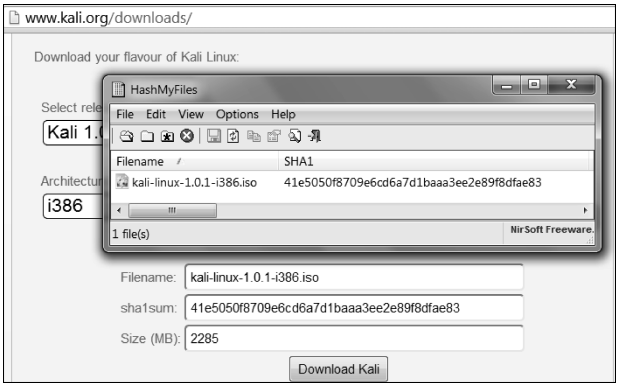

图 1.2

在使用 sha1sum、HashMyFile 这类工具计算下载文件的哈希值之后，您需要将其与网页所示的哈希值进行比较，检查它们是否相同。

如果两个值相同，那您可直接进入下节的操作。如果两个值不相同，那么就说明您下载的文件有问题，您可能需要在官方的镜像下载网站重新下载有关文件。

1.4　使用 Kali Linux

Kali Linux 有以下几种使用方式：

- 可以直接通过 Live DVD 运行 Kali Linux；
- 可以在硬盘上安装并运行 Kali Linux；
- 可以在 USB 磁盘上安装 Kali Linux（即 portable Kali Linux）。

后续几个小节将简要介绍这几种安装方式。

1.4.1　Live DVD 方式

如果您想要跳过安装过程直接使用 Kali Linux，您可以把 ISO 镜像录制在 DVD 光盘上。制备好光盘以后，就可以直接通过 DVD 光盘启动 Kali。当然，您需要事先设置好 BIOS，使其从光驱启动操作系统，

通过 Live DVD 的方式启动 Kali Linux，最大的优点就是安装速度快且易用性较好。

不幸的是，Live DVD 的方式有几个不可避免的局限。例如，在重新启动系统之后，设置好的文件和配置都会丢失。另外，因为 DVD 光盘的读写速度比硬盘的速度慢很多，以 DVD 光盘的方式运行 Kali Linux 系统，其运行速度远远不如在硬盘上安装的 Kali Linux 系统。

我们推荐仅在测试的情况下以 Live DVD 的运行方式运行 Kali Linux。如果您需要在日常工作里使用 Kali Linux，我们推荐您首先安装 Kali Linux，然后再使用它。

1.4.2　硬盘安装

硬盘安装 Kali Linux 的方式分为以下两种：

- 安装在物理机 / 真实主机上（常规安装）；
- 安装在虚拟机上。

通常我们会把 Kali Linux 安装在虚拟机上。

1. 安装在物理主机上

在物理（真实）主机上安装 Kali Linux 之前，请务必确认整个硬盘是空磁盘。即使您的硬盘上有数据，在以硬盘方式安装 Kali 系统时，安装程序（默认选项）将会把整个硬盘格式化。要想轻松安装这个系统，最好把整个硬盘都分配给 Kali 使用。如果您的主机已经装有其他操作系统，则需要划分出一个单独的分区给 Kali Linux。总之，在有数据的硬盘上安装 Kali Linux 时应当格外小心，以免破坏原有数据。

Kali Linux 官方网站介绍了在 Windows 操作系统的主机上安装 Kali Linux 的具体方法。如需查询，请访问下述网址：`http://docs.kali.org/installation/dual- boot-kali-with-windows`。

硬盘分区工具有很多。就开源工具而言，可选择的 Linux Live CD 有：

- SystemRescueCD（`http://www.sysresccd.org/`）；
- GParted Live（`http://gparted.sourceforge.net/livecd.php`）；
- Kali Linux（`http://www.kali.org`）。

上述 Linux Live CD 的使用方法很简单，从光盘启动操作系统就可以管理磁盘分区。在使用 Linux Live CD 的磁盘分区工具之前，建议您事先备份好硬盘上的重要数据。虽然我们认为上述工具都安全可靠，没遇到过事故，但是小心驶得万年船，如果硬盘上有重要数据最好还是事先备份一下。

在您划分好相应分区，或者决定使用整个硬盘安装系统时，就可以从 Kali Linux Live DVD 启动，然后从启动菜单中选择 **Install** 或者 **Graphical install**。

从光盘系统之后，您就会看到安装界面（见图 1.3）。在安装过程中，需要设置的几个地方如下所示。

1. 需要在安装过程中设置系统语言。默认系统语言是英文。
2. 通过下拉选项设置国别。
3. 设置区域选项（locale setting）。默认情况下，地区为 **United States**，编码集是 **en_US.UTF-8**。
4. 您需要设置键盘布局（keymap）。通常情况下，设置美式键盘（**American English**）就可以了。

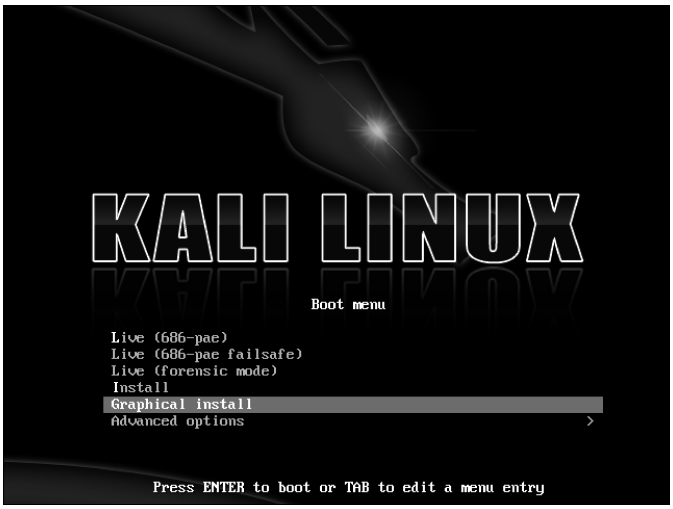

图 1.3

5．安装程序会询问您主机名称、域名等网络配置。

6．安装程序会在下一步提示您设置 root 密码。

7．安装程序接下来帮您设置时区。

8．在硬盘分区阶段，安装程序会进行磁盘分区。如果您使用的硬盘没有数据，则可选用默认的 **Guided - use entire disk** 选项。如果您的主机安装有其他操作系统，您可能首先分配分区给 Kali Linux 使用，这就需要选择菜单中的 **Manual** 选项手动管理磁盘分区。安装程序会根据您的选择创建相应的分区。

9．安装程序会询问您采取何种分区方案。默认情况下，Kali 会推荐 **All files in one partition**，即把所有文件写在一个分区里。考虑到日后可能重新安装系统，通常需要保留 `home` 文件夹里的文件，选择 **Separate/home partition** 会更好。之后，您要根据自己的需要设置`/home` 分区的大小。如果要把所有文件都放在`/home` 目录（分区）里，您可能需要把分区大小设置得大一些（大于 50GB）。一般而言，把这个分区的大小设置为 10GB 到 20GB 就可以了。

10．安装程序会总结您的分区设置，如图 1.4 所示。在您确认之后，它才会真正地进行分区管理操作。

11．接下来，安装程序开始安装 Kali Linux 系统。这个过程可能会比较长，不过此后您就把 Kali Linux 安装在硬盘上了。在我们的测试环境下，整个安装过程耗时 20 分钟左右。

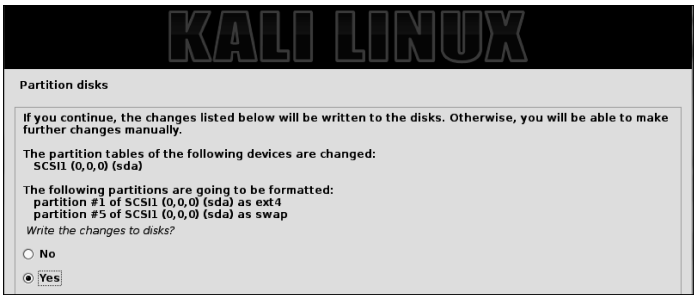

图 1.4

12. 完成上述安装过程之后，安装程序会提示您配置软件包，然后询问您是否把 GRUB（启动管理程序）安装到主引导记录 MBR 里。在设置两个选项时，采用默认的设置不会有什么问题。请注意，如果您的主机上安装有其他操作系统，您可能不应当在 MBR 上安装 GRUB。

13. 如果您看到如图 1.5 所示的信息，那么您的主机已经成功安装了 Kali 系统。

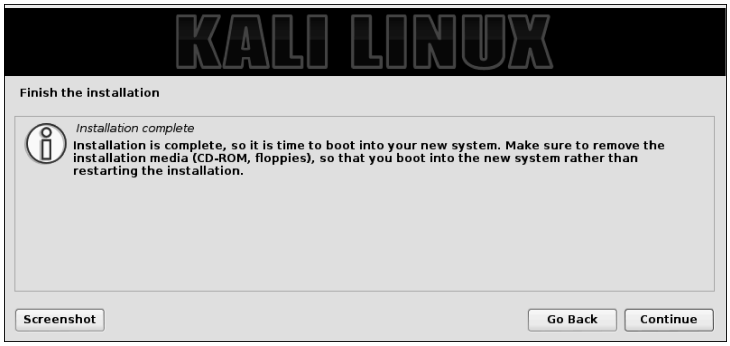

图 1.5

14. 选择 **Continue** 就会重新启动计算机，测试刚刚安装好的 Kali 系统。在重新启动计算机之后，您将看到 Kali 的登录界面（见图 1.6）。

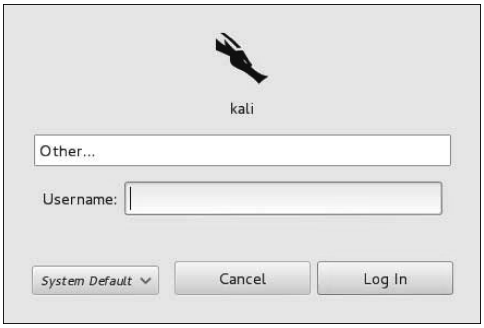

图 1.6

15．现在，输入您在安装过程中指定的用户名和密码就可以使用 Kali 系统了。

2．安装在虚拟机上

您也可以在虚拟机系统里安装 Kali Linux。采用这种方式安装 Kali Linux 系统，无须单独准备物理硬盘（或分区），也不会影响主机上已有的操作系统。

本文使用 **VirtualBox**（`http://www.virtualbox.org`）虚拟机系统。VirtualBox 是开放源代码的虚拟化软件，支持 Windows、Linux、OS X 和 Solaris 操作系统。

在虚拟机里运行 Kali Linux，比在物理机上运行的 Kali Linux 系统的性能差。

我们既可以通过 ISO 镜像在虚拟机里安装 Kali Linux 系统，也可以直接下载 VMware 磁盘镜像直接加载 Kali Linux 系统。采用前面一种方法的安装时间较长，但是可以更为详细地调整 Kali 的设置。

在虚拟机里使用 ISO 镜像安装 Kali

在虚拟机里通过 ISO 镜像安装 Kali Linux 的详细步骤如下。

1．在 VirtualBox 的工具栏里选择 **New**，创建一个新的虚拟机。

2．设置虚拟机的名称和操作系统类型。本例中，我们设置 VM 的名称为 `Kali Linux`，并选择操作系统为 **Linux－Debian**（见图 1.7）。

3．分配虚拟机的内存。内存分配的越多，虚拟机的性能也就越好。本例中，我们分配给 Kali Linux 的虚拟机 2048MB 内存（见图 1.8）。请注意，您不可能把主机所有内存都分配给虚拟机使用，因为您主机的操作系统也要使用内存。

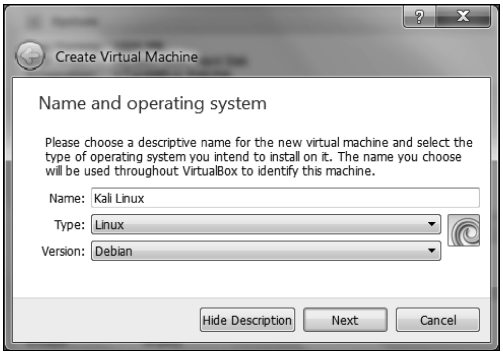

图 1.7

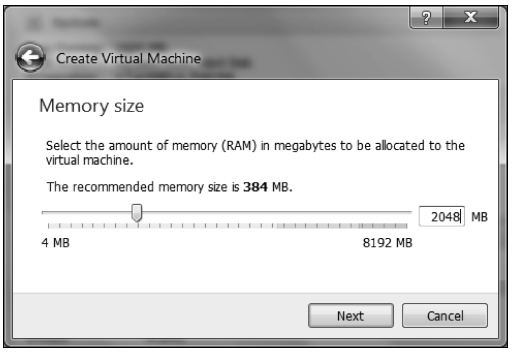

图 1.8

4. 设置虚拟机的硬盘。您可以设置虚拟硬盘文件的类型为 VDI。这种格式的虚拟硬盘文件可以动态调整文件大小。我们推荐您分配给虚拟机 32GB 以上的虚拟硬盘（见图 1.9）。如果您日后需要安装软件，就需要把虚拟硬盘设置得更大一些。

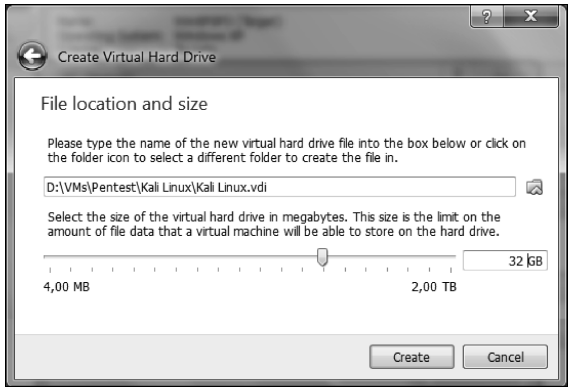

图 1.9

5. 完成上述步骤之后，虚拟机清单里会列出刚才新建的虚拟机。

6. 如需通过 Kali Linux 的 ISO 镜像安装系统，要在 VirtualBox 菜单里选中那个虚拟机，然后点击 **Storage** 菜单进行配置（见图 1.10）。

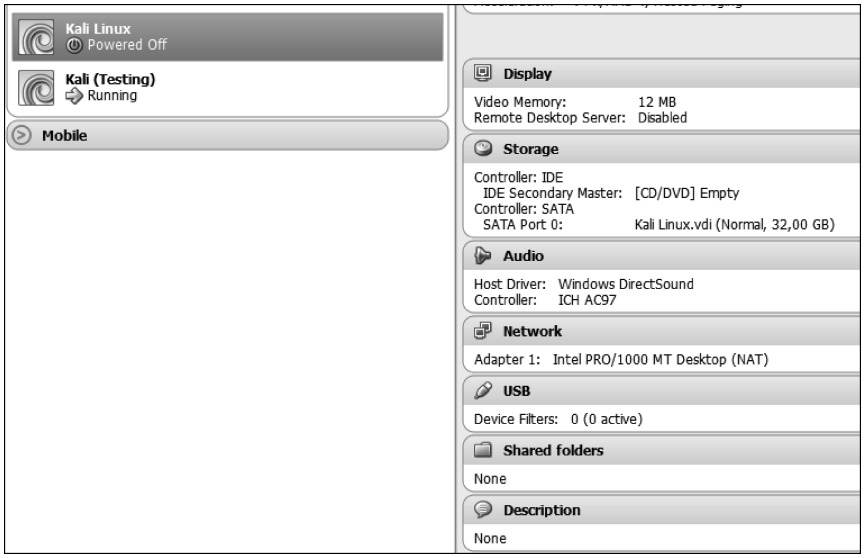

图 1.10

7. 在 **Storage Tree** 里选择 **IDE Controller-Attributes**，然后选中 Kali Linux 的 ISO 镜像

文件。本例中，这个文件应该是 kali-linux-1.0.1-i386.iso。如果设置成功，将会在 **Controller：IDE** 字段中看到这个镜像的文件名（见图 1.11）。

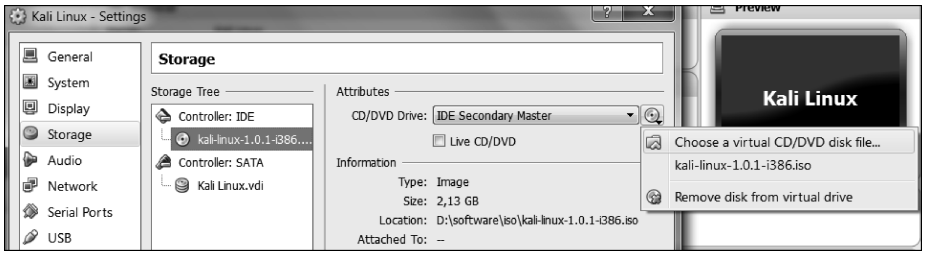

图 1.11

8．只要启动虚拟机，就可以从 ISO 镜像启动并安装 Kali Linux。接下来的设置过程，请参见前文的“安装在物理主机上”的相关内容。

在虚拟机里使用 VM 镜像安装 Kali Linux

我们同样可以使用官方提供的 VMware 磁盘镜像，直接安装 Kali Linux。

在 Kali Linux 团队提供的 VMware 磁盘镜像中，适用于 i386 平台的 Kali Linux 镜像只有 GNOME GUI 版本。

这种安装方法相当简单。

在下载 Kali Linux VMware 硬盘镜像文件（kali-linux-1.0-i386-gnome-vm.tar.gz）之后，您需要验证下载文件的 SHA1 哈希值是否与网站公布的值一致。只有在它们相同的情况下，您才能从文件中解压缩出正确的镜像文件。

官方提供的 VMware 镜像文件是 GZ 格式的压缩文件。如果您使用的是 Windows 系统，您就需要 gzip 或 7-Zip 这类工具将其解压缩。这个 GZ 格式的压缩包包含 21 个文件。在解压缩之后，您将看到 21 个文件（见图 1.12）。

在 VirtualBox 的工具栏中，选择 **New** 新建 VM 虚拟机。接下来在程序的向导窗口中进行如下设置，使这个 VM 加载刚才解压出来的虚拟机镜像文件。

1．我们设置虚拟机名称为 kali-gnome-vm-32，并设置操作系统为 **Linux—Debian**。

2．分配 2048MB 内存给 Kali Linux 虚拟机。

3．设置虚拟机硬盘类型为 **Use an existing virtual hard drive file**，然后指定其硬盘使用镜像文件 kali - linux - i386-gnome-vm.vmdk。接下来，点击 **Create** 创建虚拟机，如图 1.13 所示。

kali-linux-i386-gnome-vm	nvram	8.684	11/03/2013 23:25 -a-
kali-linux-i386-gnome-vm	vmdk	1.358	11/03/2013 23:19 -a-
kali-linux-i386-gnome-vm	vmsd	0	09/03/2013 02:59 -a-
kali-linux-i386-gnome-vm	vmx	2.736	11/03/2013 23:25 -a-
kali-linux-i386-gnome-vm	vmxf	382	09/03/2013 03:26 -a-
kali-linux-i386-gnome-vm-s001	vmdk	1.936.130.048	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s002	vmdk	953.548.800	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s003	vmdk	100.007.936	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s004	vmdk	1.101.004.800	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s005	vmdk	586.285.056	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s006	vmdk	337.772.544	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s007	vmdk	830.144.512	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s008	vmdk	565.968.896	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s009	vmdk	390.529.024	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s010	vmdk	299.565.056	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s011	vmdk	196.411.392	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s012	vmdk	364.773.376	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s013	vmdk	203.292.672	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s014	vmdk	294.191.104	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s015	vmdk	1.441.792	11/03/2013 23:36 -a-
kali-linux-i386-gnome-vm-s016	vmdk	65.536	11/03/2013 23:36 -a-

图 1.12

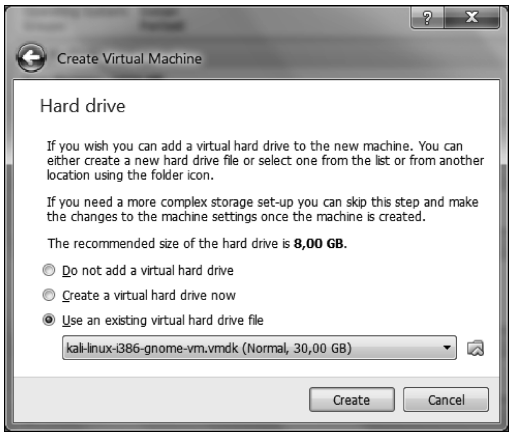

图 1.13

使用硬盘镜像方式安装 Kali Linux 之后，系统的默认设置值如下所示。

- 硬盘容量：30 GB。
- 联网方式：NAT。
- 用户名：root。
- 密码：toor。

如果要把 Kali 当做渗透测试平台使用，应当避免以 NAT 方式接入网络。本文推荐您以桥接（bridged）方式联网。

在配置 Kali VM 的时候，应当尽快更改默认密码。

如果操作成功，虚拟机管理列表应能列出刚才新建的虚拟机（见图 1.14）。

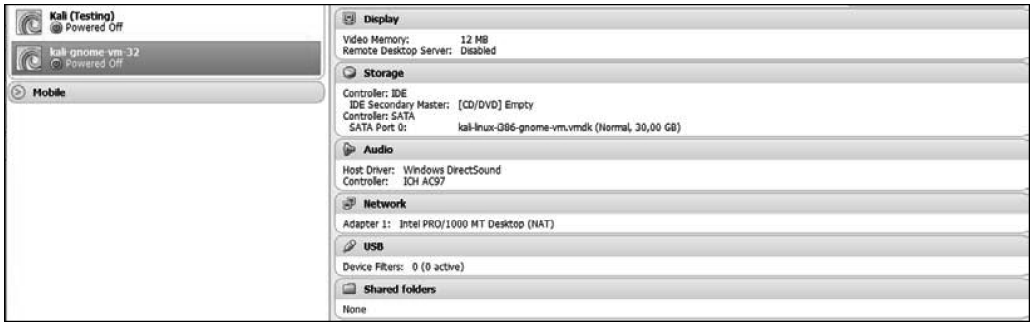

图 1.14

在虚拟机菜单条中点击 Start 图标，即可运行 Kali Linux 虚拟机。完成启动过程之后，Kali Linux 应当会进入登录界面。

如果您遇到了图 1.15 所示的问题，那么就需要安装 **VirtualBox Extension Pack**（功能增强包）。您可在 `http://www.virtualbox.org/wiki/Downloads` 下载这个工具。

请注意，您应当下载版本号和 VirtualBox 完全相同的功能增强包。也就是说，如果您使用的是 4.3.0 版的 VirtualBox，就应当下载 4.3.0 版的 Extension Pack。

在 VirtualBox 管理程序安装功能增强包的步骤如下。

1. 通过菜单 **File | Preferences**，进入 **Settings** 设置界面。随后，选择左侧的 **Extensions**（见图 1.16）。

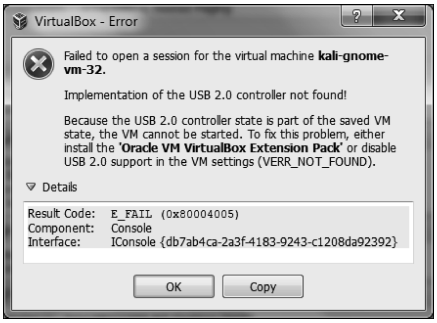

图 1.15

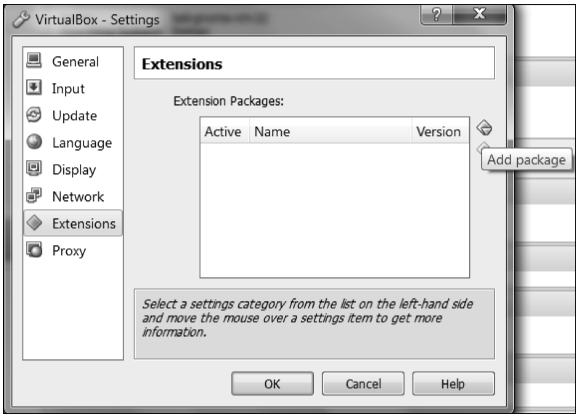

图 1.16

2. 点击 **Add package** 按钮，选中刚才下载的 VirtualBox Extension Pack。这时，VirtualBox 会在弹出窗口里列出扩展功能包的信息，并请您确认是否继续安装（见图 1.17）。

3. 选择 **Install** 按照屏幕上的提示安装扩展功能包。如果安装过程顺利，您将在 Extension 列表里看到扩展功能包的相关信息（见图 1.18）。

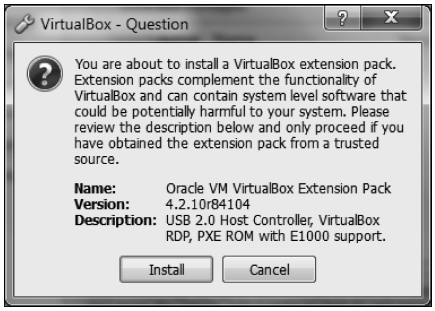

图 1.17

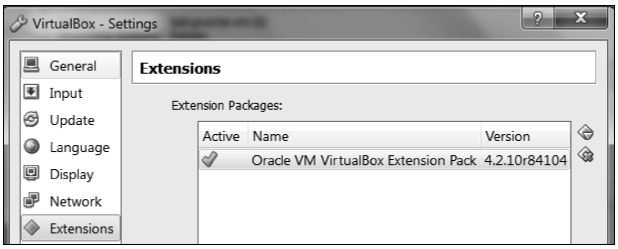

图 1.18

4. 现在，您可以使用默认的用户名和密码登录 Kali Linux。

1.4.3 安装在 USB 闪存上

安装 Kali Linux 的第三种方法，就是把它安装到 USB 闪存里。通常，人们把安装在闪存上的 Kali Linux 叫做 **portable（便携）Kali Linux**。按照 Kali 官方文件的说法，这种安装方式的启动和安装速度最快，是 Kali 研发人员最喜欢的安装方式。相比在硬盘上安装，只能在一台机器上启动 Kali 系统而言，装有 Kali Linux 的闪存盘可以在所有支持 USB 启动的主机上使用 Kali 系统。

这种安装方法同样适合在内存卡（SSD、SDHC、SDXC 等）上安装 Kali Linux。

很多工具都可以制作 portable Kali Linux。其中，**Rufus**（`http:// rufus.akeo.ie`）就不错。这个工具只能在 Windows 操作系统下运行。

其他可从 ISO 镜像文件制作可启动 USB 的工具如下所示：

- **Win32DiskImager**（`https://launchpad.net/win32-image-writer`）；
- **Universal USB Installer**（`http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/`）；

- **Linux Live USB Creator**（`http://www.linuxliveusb.com`）。

在制作 portable Kali Linux 之前，您需要准备好几样素材。

- **Kali Linux 的 ISO 镜像文件**：虽然您可以使用启动磁盘创建工具直接下载镜像文件，但是我们仍然认为提前下载好 ISO 镜像文件，再用 Rufus 使用镜像文件比较稳妥。
- **USB 闪存盘**：您需要一个容量足够大的 USB 闪存盘。我们推荐您使用 16GB 以上的闪存盘。

在下载 Rufus 之后，在 Windows 里双击 `rufus.exe` 文件就可以运行它。它会显示出程序界面。

如果您使用的是基于 UNIX 的操作系统，您可以直接使用 `dd` 指令创建可启动闪存盘。例如：

```
dd if=kali-linux-1.0.1-i386.iso of=/dev/sdb bs=512k
```

此处的`/dev/sdb` 应当是您 USB 闪存盘的设备名称。

使用 Rufus 创建可启动的 Kali USB 闪存盘的设置如下（见图 1.19）。

- **Device**：选择 USB 闪存驱动器。本例中，它是 Windows 系统的 E 盘。
- **Partition scheme and target system type**：设置为 **MBR partition scheme for BIOS or UEFI computers**。
- **Create a bootable disk using**：设置为 **ISO Image** 并使用右侧磁盘图标选取 ISO 镜像文件。

然后点击 **Start** 创建可启动闪存盘（见图 1.20）。

在完成这些步骤之后，如果您想要立即测试 USB 闪存盘，则应在保存好所有文件的情况下重启计算机。您可能需要配置计算机的 BIOS，使其从 USB 磁盘启动计算机。如果没有问题的话，您应该可以通过 USB 闪存盘启动 Kali Linux 系统。

在 USB 闪存盘上安装系统之后，如果您想要让系统能够保存您所更改的文件（即 persistence capabilities），您可参照 Kali 官方文档进行设置。请参见 **Adding Persistence to Your Kali Live USB**，地址为 `http://docs.kali.org/installation/kali-linux-live-usb-install`。

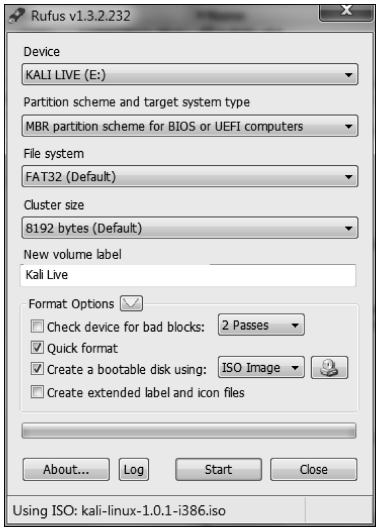

图 1.19

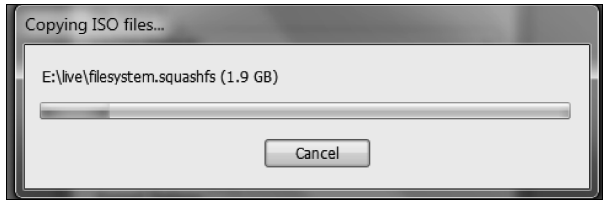

图 1.20

1.5 配置虚拟机

在登录 Kali Linux 虚拟机之后，需要进行几项配置。对执行渗透测试来说，这几项配置相当重要。

1.5.1 安装客户端功能增强包

在 VirtualBox 里配置好 Kali Linux 所用的虚拟机之后，我们建议您安装客户端功能增强包（**VirtualBox guest additions**）。这个功能增强包的作用有很多。

- 它支持以全屏模式查看虚拟机的桌面。
- 它显著改善鼠标操作方面的用户体验。
- 它支持物理主机到虚拟主机之间的文本复制功能。
- 它支持物理主机和虚拟主机之间的文件夹共享。

安装客户端功能增强包的具体步骤如下。

1. 在 VirtualBox 的菜单里，选择 **Devices | Install Guest Additions**。此后，被虚拟机会以光盘的形式加载 VirutualBox guest additions（见图 1.21）。

图 1.21

2．在图 1.22 所示的 Virutalbox 窗口里，点击 **Cancel**。

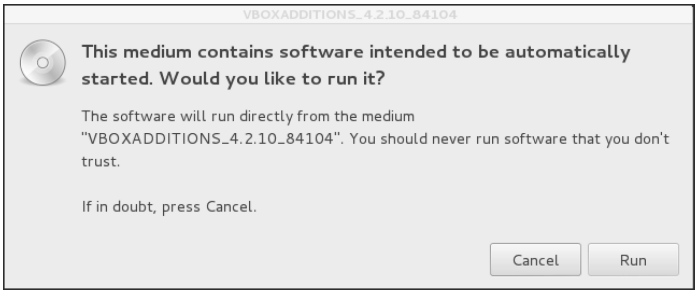

图 1.22

3．打开终端程序 terminal，进入 VirtualBox guest additions 所在的 CDROM 目录。一般情况下，这个目录的路径是`/media/cdrom0`（见图 1.23）。

```
root@kali:~# cd /media/cdrom0/
root@kali:/media/cdrom0# ls
32Bit         cert                    VBoxSolarisAdditions.pkg
64Bit         OS2                     VBoxWindowsAdditions-amd64.exe
AUTORUN.INF   runasroot.sh            VBoxWindowsAdditions.exe
autorun.sh    VBoxLinuxAdditions.run  VBoxWindowsAdditions-x86.exe
root@kali:/media/cdrom0#
```

图 1.23

4．执行`VBoxLinuxAdditions.run`，以启动它的安装程序。

```
sh./VBoxLinuxAdditions.run
```

5．等待数分钟之后，安装程序会编译并安装好客户端功能增强包的各种模块（见图 1.24）。

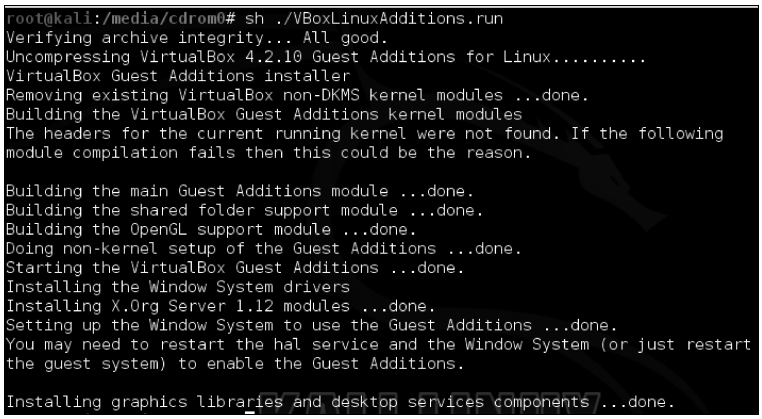

图 1.24

6．进入 root 的主目录。

7．在 VirtualBox 的菜单里，使用右键点击 VBoxAdditions 的 CD 镜像文件，然后选中 **Eject**，弹出这个虚拟光驱。如果操作成功，VBoxAdditions 的光盘图标将从虚拟机的桌面上消失。

8．在终端窗口里使用 `reboot` 指令重新启动虚拟机。

9．待重启之后，您可以在菜单栏选择 **View | Switch to fullscreen** 进入全屏模式。

1.5.2 网络设置

本节将介绍在 Kali Linux 里设置有线网络和无线网络的方法。

1．配置有线网络

无论是通过 VMware 磁盘镜像还是通过 ISO 镜像安装 Kali Linux，默认情况下 Kali Linux 接入网络的方式都是 NAT（网络地址转换）。在 NAT 方式下，Kali Linux 的虚拟机可以通过物理主机联入外部网络，而外部网络甚至是物理主机自身都无法直接访问安装有 Kali Linux 的虚拟机。

进行实地的渗透测试时，您可能需要把网络结构变更为 **Bridged Adapter**。具体的设置步骤如下。

1．首先请确定您已经关闭（power off）虚拟机。

2．在 VirtualBox 管理程序里，选中相应的虚拟机，即安装 Kali Linux 的虚拟机，然后点击窗口右侧的 **Network**，通过下拉选项把 **Attached to** 从 **NAT** 变更为 **Bridged Adapter**（桥接适配器）。如图 1.25 所示，其中的 **Name** 选项可设置为您需要测试的网卡接口。

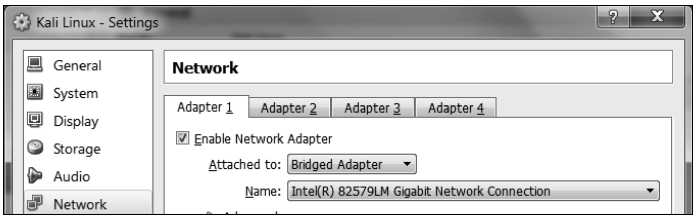

图 1.25

如需使用桥接连接，首先要使物理主机与网络设备连接，例如路由器或交换机。同时，接入的网络里应当有 DHCP 服务，以分配 IP 地址给虚拟机。

您可能已经注意到了，通过 DHCP 获取的 IP 地址并不是固定的 IP 地址，这种 IP 地址在一定时间后可能会发生变化。如果 Kali Linux 通过 DHCP 获取 IP 地址，在超过固定周期（DHCP 的租赁时间）之后，DHCP 会重新给虚拟机分配一次 IP 地址。重新分配的 IP 地址可能和上次分配的 IP 地址相同，也可能不同。

如果虚拟机需要使用固定的 IP 地址，应该修改虚拟机的网络设置文件`/etc/network/interfaces`。

默认情况下，Kali Linux 的网络设置文件如下。

```
auto lo
iface lo inet loopback
```

这个配置文件指定所有网卡都通过 DHCP 获取 IP 地址。如需为虚拟机绑定固定 IP 地址，就不得不对这个文件进行相应修改。

```
auto eth0
iface eth0 inet static
address 10.0.2.15
netmask 255.255.255.0
network 10.0.2.0
broadcast 10.0.2.255
gateway 10.0.2.2
```

上述文件令第一个有线网卡`eth0`绑定了 IP 地址`10.0.2.15`。您可能需要根据实际情况修改上述设置。

2．配置无线网络

在虚拟机里安装的 Kali Linux 无法使用笔记本上集成的无线网卡。好在您可以使用 USB 接口的无线网卡。

在 Kali 虚拟机上使用 USB 接口的无线网卡时，要把 USB 无线网卡插在主机 USB 接口上，在 VirtualBox 的菜单里选 **Devices | USB Devices**，再选中所要使用的 USB 无线网卡。

如图 1.26 所示，我们选择了 Realtek 芯片的 USB 无线网卡。

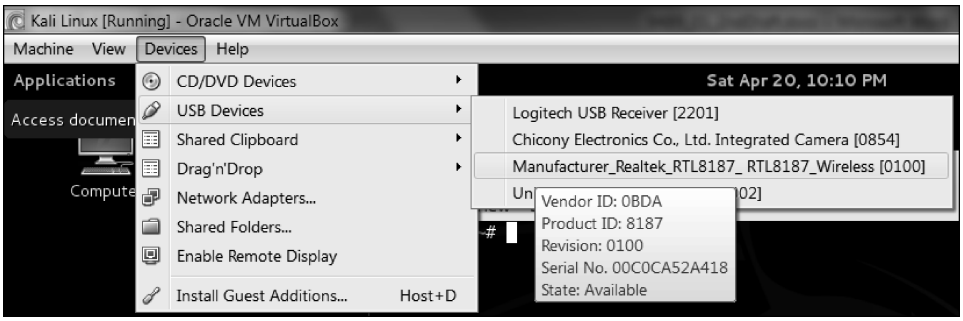

图 1.26

如果您的无线网卡可以被 Kali 识别，可以在 `dmesg` 指令的输出中看到无线网卡的硬件信息。

在 Kali 桌面的右上角可以找到 Network Connection（网络连接）的图标。点击这个图标后，将能看到网络信息。

此时可以看到您的机器可用的有线网络和无线网络的名称（见图 1.27）。

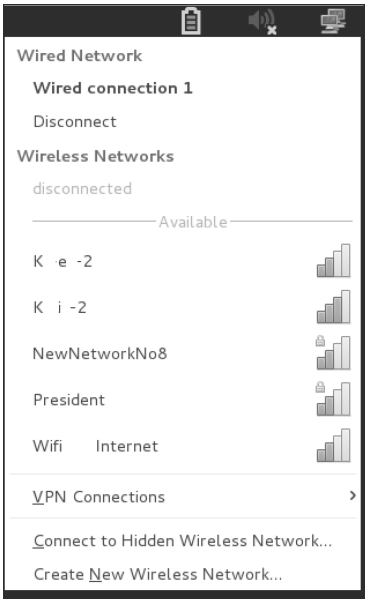

图 1.27

要想连接无线网络，就要双击该网络的 SSID。如果选定的网络要求您进行身份验证，程序会提示您输入密码。在输入正确的无线网络密码后，您就被授权使用该无线网络。

3．启用网络

我们通过 **service** 指令来启动和关闭网络。

如需启用网络，可以使用下述指令：

```
service networking start
```

如需关闭网络，可以使用下述指令：

```
service networking stop
```

您需要有 root 权限才能运行上述两条指令。

接下来，您可以通过 ARP ping 请求（`arping` 指令）连接同网段的其他主机，来测试网络配置是否正确。

默认情况下，您需要在计算机每次重启后手动启动网络连接服务。您可通过下述指令，让（虚拟）计算机在每次启动的时候都自动启动网络连接服务：

```
update-rc.d networking defaults
```

上述指令会在`/etc/rc*.d` 目录里创建必要的连接，以在 Kali 启动的时候自动执行网络配置的脚本程序。

1.5.3　文件夹共享

在进行渗透测试的工作时，我们经常需要在物理主机和虚拟机之间交换文件，例如把渗透测试的文档复制到物理主机上。VirtualBox 的文件夹共享（**Shared Folders**）功能可以满足这一需求。

您要先关闭虚拟机，再在 VirtualBox 里配置文件夹共享。关闭虚拟机之后，选中相应的虚拟机名称（右键点击 Settings），然后在窗口左侧菜单里点击 **Shared Folders**，如图 1.28 所示。

点击右侧的加号“+”图标，即可添加要物理主机共享给虚拟机的文件夹。在此之后，**Folder Path** 里会显示共享文件夹的信息。

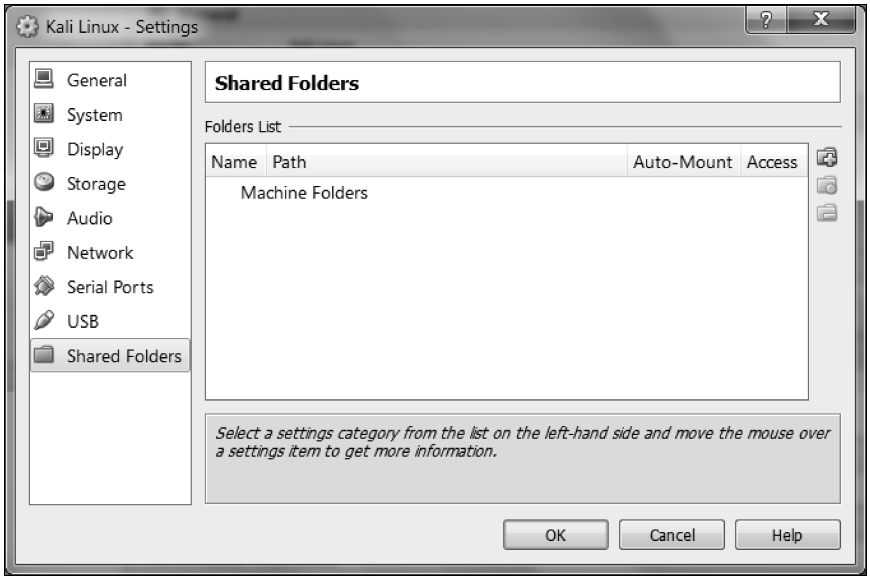

图 1.28

您还可以调整 **Folder Name** 选项，设置共享文件夹的共享名称。此后，虚拟机（Guest OS）就可以通过这个共享名称访问物理主机的文件夹。

如果不希望虚拟机更改共享文件夹的内容，可设置 **Read-only** 选项设置，把该文件夹设置为只读。如果选中 **Auto-mount** 选项，虚拟机在每次启动后都会连接这个文件夹。这些设置如图 1.29 所示。

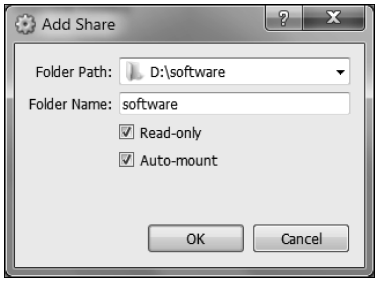

图 1.29

在图 1.29 所示的设置里，我们共享了主机上的 **D:\software** 文件夹给虚拟机，并且设置其文件夹权限为只读。

虚拟机可以通过目录`/media/sf_software`目录访问物理主机共享的文件夹。

1.5.4　快照备份

一旦您把虚拟机配置到理想的可工作状态，我们建议您立刻对虚拟机进行快照备份。万一日后出现配置故障，可利用快照备份把虚拟机迅速恢复到正常工作状态。

VirtualBoxti 提供了方便的快照备份功能。您可通过菜单 **Machine-Take Snapshot** 进行快照备份（见图 1.30）。只有在启动虚拟机的情况下才能进行快照。

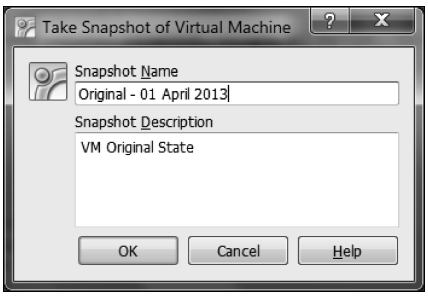

图 1.30

Snapshot Name 就是您给此次备份起的名字，我们建议您在里面标注上备份日期。您还可以在 **Snapshot Description** 里对此次备份进行详细备注。填写完全部信息并点击 OK 后，VirtualBox 就开始进行备份。备份时间的长短取决于保存信息的信息量大小。

1.5.5　导出虚拟机

人们时常需要以文件形式备份虚拟机，或通过这种方法把虚拟机分享给他人使用。VirtualBox 的虚拟机导出功能简化了这种操作。在关闭需要导出的虚拟机之后，在菜单栏选中 **File | Export Appliance** 就可导出所选的虚拟机。

导出虚拟机的操作步骤如下。

1．选中 **Export Appliance** 选项，调出 **Appliance Export Wizard**。

2．选择需要导出的虚拟机。

3．设置导出文件的目录和文件名。默认情况下，文件将保存在主目录下，文件将保存为 **ova**（**Open Virtualization Format Archive**）格式。如果您不清楚应该以何种格式保存这个文件，就应当使用默认的文件存储格式。

4．您可以在图 1.31 所示的界面里设置虚拟机的各种属性。如果不需要进行特定设置，可以不填写任何选项。

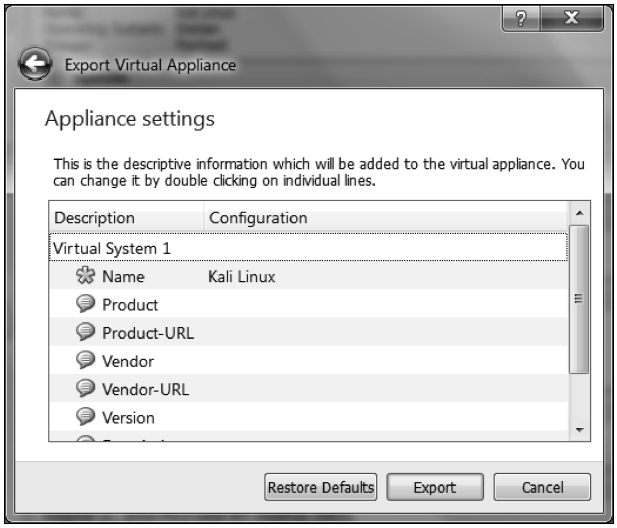

图 1.31

5．点击 **Export** 之后，VirtualBox 将把虚拟机导出到文件。导出时间的长短取决于虚拟机硬盘容量的大小。它的硬盘文件越多，导出的时间也就越长。在我们的测试环境下，导出 Kali Linux 虚拟机的操作耗时大约 20 分钟。

1.6 系统更新

Kali Linux 由操作系统内核和数百个软件构成。如果需要使用软件的最新功能，您就需要将其更新到最新的版本。

我们建议您仅从 Kali Linux 官方的软件仓库（repository）进行更新。

在您安装和配置好 Kali Linux 之后，就应当立即进行系统更新。因为 Kali 是基于 Debian 的操作系统，您需要使用 Debian 的指令（`apt-get`）进行系统更新。

更新指令 `apt-get` 会查询`/etc/apt/sources.list` 文件，从中获取更新服务器的信息。您需要确定这个文件指定了正确的升级服务器。

默认情况下，Kali Linux 的 `sources.list` 文件包含下述信息。

```
# deb cdrom:[Debian GNU/Linux 7.0 _Kali_ - Official Snapshot i386
LIVE/INSTALL Binary 20130315-11:39]/ kali contrib main non-free
```

```
#deb cdrom:[Debian GNU/Linux 7.0 _Kali_ - Official Snapshot i386 LIVE/
INSTALL Binary 20130315-11:39]/ kali contrib main non-free

deb http://http.kali.org/kali kali main non-free contrib
deb-src http://http.kali.org/kali kali main non-free contrib

## Security updates
deb http://security.kali.org/kali-security kali/updates main contrib  non-free
```

在进行系统更新之前，要使主机上软件包的索引信息与/etc/apt/sources.list上的服务器进行同步。同步索引的指令是：

```
apt-get update
```

在为 Kali 安装软件或安装系统更新之前，每次都要执行 apt-get update 指令。

待同步软件包的索引信息之后，就可以进行软件更新。

系统更新的指令有两种。

- apt-get upgrade：升级系统上安装的所有软件包。如果在升级软件包时出现什么意外，所涉及的软件包会原封未动地保持在更新之前的状态。
- apt-get dist-upgrade：升级整个 Kali Linux 系统。如需从 Kali Linux 1.0.1 升级到 Kali Linux 1.0.2，就应当使用这条指令。它不仅能够升级所有已安装的软件包，而且会处理升级过程中可能出现的软件冲突。某些情况下，它的部分升级过程需要人工参与。

在输入升级 Kali Linux 所需的适当指令之后，apt-get 程序会详细列出将要安装、升级或删除的软件包信息，然后等待您的确认。

在您进行确认之后，apt-get 程序将开始进行系统更新。系统更新的时间长短，主要取决于带宽和网速的情况。

1.7　Kali Linux 的网络服务

Kali Linux 系统可安装多种网络服务。在这一节，我们仅讨论其中三种服务的安装和配置方法：HTTP、MySQL 和 SSH 服务。您可以通过菜单 **Kali Linux | System Services**，查看可以安装的其他服务。

1.7.1 HTTP

从事渗透测试的工作人员，可能会经常用到 Web 服务器。例如，当需要测试 Web 程序的恶意脚本时，就需要自己搭建个 Web 服务器。其实 Kali Linux 已经集成了 Apache，只要将之启动就可以开始使用了。

激活 Kali Linux 的 HTTP 服务的步骤如下。

1. 如果要通过桌面菜单启动 **Apache HTTP** 服务，可在桌面菜单中依次选中 **Kali Linux | System Service | HTTPD | apache2 start**。如果要通过命令行启动它，可在终端窗口里输入下述指令：

```
service apache2 start
```

2. 如果配置文件没有问题，系统会返回下述响应信息。

```
[....] Starting web server: apache2 ok
```

3. 在此之后，您可以使用浏览器浏览网页。正常情况下它会显示 **It works!**的默认页面（见图 1.32）。

图 1.32

停止 Apache HTTP 服务的操作步骤如下。

1. 如果要通过桌面菜单停止 Apache HTTP 服务，可在桌面菜单中依次选中 **Kali Linux | System Service | HTTPD | apache2 stop**。如果要通过命令行停止它，可在终端窗口里输入下述指令：

```
service apache2 stop
```

2. 系统会返回下述响应信息。

```
[....] Stopping web server: apache2 [ ok waiting .
```

请注意，在计算机启动的时候，系统并不会自动启动上述服务。在下次启动 Kali Linux 系统的时候，您都需要再次执行这个命令。好在我们可以通过下述指令，指定计算机在启动时自动启动 Apache HTTP 服务：

```
update-rc.d apache2 defaults
```

这条指令将把 apache2 服务添加到自动启动的程序组里。

1.7.2　MySQL

下面将要介绍 **MySQL** 服务。MySQL 属于标准的关系数据库（RDBMS）。人们通常会使用 Apache 服务器执行 PHP 程序，并通过 PHP 程序调用 MySQL；以这种配置组合来创建动态的 Web 应用服务程序。就渗透测试的工作而言，您可以把渗透测试的测试结果存储到 MySQL 服务器里。例如，可以用 MySQL 数据保存漏洞信息和网络映射的分析结果。当然，这需要您首先启用这个程序。

启动 Kali Linux 自带的 MySQL 服务的操作步骤如下。

1. 如果要从桌面菜单启动 MySQL 服务，可在桌面菜单中依次选中 **Kali Linux | System Service | MySQL | mysql start**。如果要通过命令行启动它，可在终端窗口里输入下述指令：

```
service mysql start
```

2. 系统会返回下述响应信息。

```
[ ok ] Starting MySQL database server: mysqld . . ..
[info] Checking for tables which need an upgrade, are corrupt or were not closed
cleanly..
```

3. 如需测试 MySQL 的工作状态是否正常，可使用 MySQL 客户端登录到服务器。我们使用用户名（root）和密码登录 MySQL 服务器。

```
mysql -u root -p
```

4. 系统会返回下述响应信息。

```
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 42
Server version: 5.5.30-1 (Debian)
Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights
reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type ''help;'' or ''\h'' for help. Type ''\c'' to clear the
current input statement.
mysql>
```

5. 您可以在 MySQL 的提示符下直接使用 SQL 命令。如需退出 MySQL 客户端程序，请使用 `quit` 命令。

出于安全性的考虑，默认情况下，只能从本机访问 Kali Linux 系统里的 MySQL 服务。如需调整这个设置，请修改配置文件 `/etc/mysql/my.cnf` 里的 `bind-address` 语句。除非需要从其他主机访问 MySQL 服务，否则我们建议您不要修改它。

停止 MySQL 服务的操作步骤如下。

1. 如果要通过桌面菜单停止 MySQL 服务，可在桌面菜单中依次选中 **Kali Linux | System Service | MySQL | mysql stop**。如果要通过命令行停止它，可在终端窗口里输入下述指令。

```
service mysql stop
```

2. 系统会返回下述响应信息。

```
[ ok ] Stopping MySQL database server: mysqld.
```

下述指令可使 Kali Linux 系统在启动过程中自动启动 MySQL 服务。

```
update-rc.d mysql defaults
```

这条指令将把 MySQL 服务添加到自动启动的程序组里。

1.7.3　SSH

SSH 的全称是 **Secure Shell**。它是目前较为可靠的专为远程登录会话和其他网络服务提供安全性的协议。除了远程登录的服务功能以外，它还有很多功能：它支持在主机间安全地传递文件、在远程主机上执行命令，以及 X11（Linux 的桌面）会话转发等。

管理 SSH 服务的操作步骤如下。

1. 如果要从桌面菜单启动 SSH 服务，可在桌面菜单中依次选中 **Kali Linux | System Service | SSH | sshd start**。如果要通过命令行启动它，可在终端窗口里输入下述指令。

```
service ssh start
```

2. 系统会返回下述响应信息。

```
[ ok ] Starting OpenBSD Secure Shell server: sshd.
```

3. 如需测试 SSHD 的工作状态是否正常，可以在其他主机上使用 SSH 客户端登录到服务器。如果您使用的是 Microsoft Windows 系统，可以使用 putty 进行测试。下载 putty 的官方网站是 `http://www.chiark.greenend.org.uk/~sgtatham/putty/`。
4. 如果要通过桌面菜单停止 SSHD 服务，可在桌面菜单中依次选中 **Kali Linux | System Service | SSH | sshd stop**。如果要通过命令行停止它，可在终端窗口里输入下述指令。

```
service ssh stop
```

5. 系统会返回下述响应信息。

```
[ ok ] Stopping OpenBSD Secure Shell server: sshd.
```

6. 下述指令可使 Kali Linux 系统在启动过程中自动启动 SSH 服务。

```
update-rc.d ssh defaults
```

这条指令将把 SSH 服务添加到自动启动的程序组里。

1.8 安装脆弱系统

我们在本节安装渗透和测试的目标——一台存在很多漏洞的虚拟主机。本书很多章节里的特定主题都涉及这台脆弱系统（vulnerable server）。在法律许可的范围之内，我们不可以攻击任何在 Internet 上的存在漏洞的真实主机，所以我们必须使用自己安装的脆弱系统。我们在此强调，除非有对方的书面许可，否则决不可以渗透或测试他人的主机。此外，我们希望您能够在自己搭建的环境中提高渗透技能。当攻击没有达到预期成效时，只要渗透环境完全可控，您就可以轻易地检查目标主机的情况，从而找到失败的原因。

在很多国家，只要目标主机不是您自己的，哪怕您对其进行端口扫描都会被认为是犯罪。而且，只要使用虚拟机作为目标主机，即使它发生了故障，我们也能很快将其修复。

我们将在虚拟机里安装 **Metasploitable 2**，用它作为我们的脆弱系统。Metasploitable 的研发团队是 Rapid7 旗下著名的 HD Moore。

除了 Metasploitable 2 之外，还有很多可用于搭建渗透测试环境的脆弱系统。详情请参见：`http://www.felipemartins.info/2011/05/pentesting-vulnerable-study-frameworks-complete-list/`。

无论是操作系统、网络，还是 Web 应用服务方面，Metasploitable 2 都有非常多的漏洞和问题。

有关这些漏洞的详细情况，请参见 Rapid 7 的官方网站：`https://community.rapid7.com/docs/DOC-1875`。

在 VirtualBox 里安装 Metasploitable 2 的操作步骤如下。

1. 从网络上下载 Metasploitable 2 的虚拟机镜像文件。该网站网址是 `http://sourceforge.net/projects/metasploitable/files/Metasploitable2/`。
2. 解压缩下载的 ZIP 文件。待解压缩 Metasploitable 2 的 ZIP 文件之后，您将看到 5 个文件。
   - `Metasploitable.nvram`

- Metasploitable.vmdk
- Metasploitable.vmsd
- Metasploitable.vmx
- Metasploitable.vmxf

3．在 VirtualBox 里创建一个虚拟机。本例设置这个虚拟主机的名称（**Name**）为 Metasploitable 2，并设置操作系统为 **Linux—Ubuntu**。

4．给这个虚拟主机分配 1024MB 内存。

5．在 **Virtual Hard Disk** 设置里，选择 **Use existing hard disk**，然后选中我们先前解压缩出来的 Metasploitable 文件（见图 1.33）。

图 1.33

6．修改联网类型为 **Host-only adapter**，以保证这台虚拟主机服务器同时可被物理主机和 Kali Linux 主机访问。我们还要修改 Kali Linux 的虚拟主机，把它的联网类型也改为 **Host-only adapter**。

7．启动虚拟主机 Metasploitable 2。待完成启动过程之后，您可使用下述信息登录 Metasploitable 2 的终端。

- 用户名：msfadmin
- 密码：msfadmin

8．登录成功之后，Metasploitable 2 的终端窗口如图 1.34 所示。

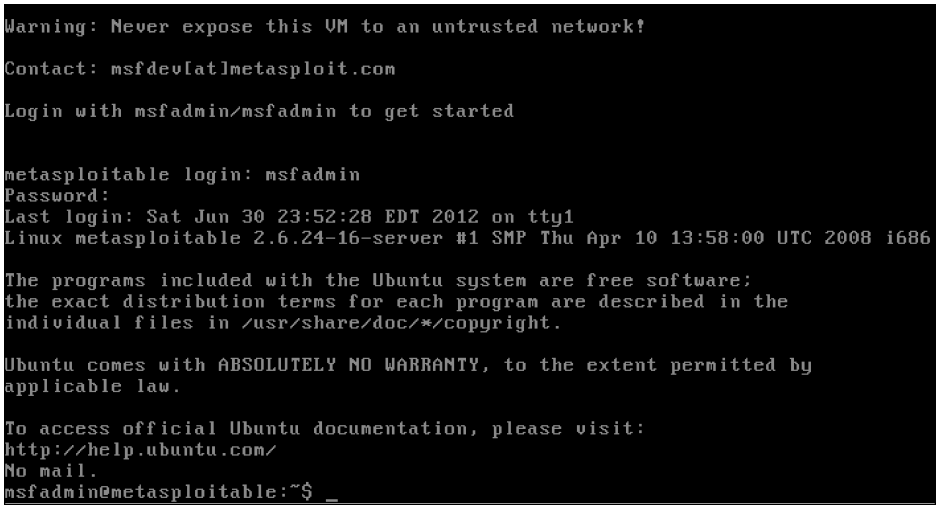

图 1.34

1.9 安装额外工具包

虽然最新版本的 Kali Linux 带有大量的安全工具，但是由于以下原因，您可能还会需要从软件仓库之外安装程序：

- Kali Linux 所采纳的版本，可能不是该软件的最新版；
- Kali Linux 的软件仓库（repository）可能没有收录您所需要的软件。

我们的建议是首先在软件仓库里搜索软件。如果软件仓库里有您所需要的软件，就通过软件仓库安装该软件。如果在软件仓库里找不到该软件，您可能就不得不从软件作者的网站下载并安装它。

我们的经验表明，您应当尽量通过软件仓库安装软件。这样一来，您就不必关注软件管理（主要是更新）的那些繁琐事项。

Debian 系统有很多可助您管理软件包的程序，例如 `dpkg`、`apt` 和 `aptitude` 程序。按照默认方式安装的 Kali Linux 会带有 `dpkg` 和 `apt` 程序。

如需了解 `apt` 和 `dpkg` 命令的详细信息，请参见：`https://help.ubuntu.com/community/AptGet/Howto/`和 `http://www.debian.org/doc/manuals/debian-reference/ch02.en.html`。

本节将通过几个与安装软件包有关的实例来介绍 apt 命令。

如需在软件仓库中查找某个软件包的名称，可使用指令：

```
apt-cache search <软件包名称>
```

上述指令将列出含有“软件包名称”的全部软件包。例如，我们可以使用下述指令搜索一个叫做 nessus 的软件包。

```
apt-cache search nessus
```

如需查看软件包的详细信息（描述信息、软件包大小和版本等信息），可使用命令：

```
apt-cache show <软件包名称>
```

如果决定安装或更新某个软件，那么就可用 apt-get 命令安装该软件包。apt-get 指令的基本用法是：

```
apt-get install <软件包名称>
```

如果您未能在 Kali Linux 的软件仓库里找到您所需要的软件，并且您能够确定它日后不会对系统造成不良影响，那么您可以手动安装软件包。

务必从可信的软件源下载软件，尽量从软件研发团队的网站下载。如果研发团队提供.deb 安装包（后缀名为.deb 的文件是 Debian 的安装包文件），您可以使用 dpkg 命令安装该软件包。如果他们没有提供.deb 安装包，您可以通过源代码安装该软件。虽然实际情况各有不同，但是通过源代码安装软件的方法大体都可归纳为下述几个步骤。

1．使用压缩包管理软件（例如 Tar 和 7-Zip）解压缩软件包。

2．进入到解压缩文件所在的目录。

3．执行指令：

```
./configure
make
make install
```

本节后续的篇幅将介绍如何安装没有被 Kali 软件仓库收录的软件工具。我们将演示以下两种软件安装软件机制：

- 通过 Debian 安装包安装应用程序；
- 通过源代码安装应用程序。

1.9.1 安装 Nessus 漏洞扫描程序

本小节将通过第一种安装机制安装最新的 Nessus 漏洞扫描程序（第 5 版）。我们在 Kali Linux 的软件仓库进行过相关搜索，并没有找到这个程序。

与上一版本的程序相比，第 5 版的 Nessus 的程序具有更多功能。新版程序能够通过更为详细的过滤规则整理扫描结果，创建创建更为灵活的扫描报告，而且简化了扫描策略的设置过程。因此我们不再使用第 4 版的 Nessus。

如需了解新版 Nessus 的改进之处，请参见：`http://www.tenable.com/products/ nessus/ nessus-product- overview/why-upgrade-to-nessus-5`。

我们可以访问 Nessus 的官方网站（`http://www.nessus.org/products/nessus/nessus-download- agreement`），并下载其针对 Debian 6 的安装包。然后，通过 `dpkg` 指令安装这个软件包：

```
dpkg -i Nessus-x.y.z-debian6_i386.deb
```

在这个指令里，`x.y.z` 代表 Nessus 的版本号。请根据下载文件的文件名进行相应替换。

接下来，根据 Nessus 安装程序在屏幕上的提示进行相应配置。

1. 您可通过下述指令启动 Nessus 的服务端程序。

   ```
   /etc/init.d/nessusd start
   ```

2. 使用浏览器访问网址 `https://localhost:8834`。浏览器会提示 Nessus 所用的 SSL 证书无效。您需要检查 SSL 证书并为这个网站设置例外规则。处理过 SSL 证书问题之后，您将看到 Nessus 的页面内容，如图 1.35 所示。
3. 上图 1.35 所示的界面会引导您设置 Nessus 的管理员账号。而后，它要求您输入 Nessus 扫描程序的激活码。您可在官方网站（`http://www.nessus.org/register/`）进行注册，从而获取启动程序所需的激活码（见图 1.36）。

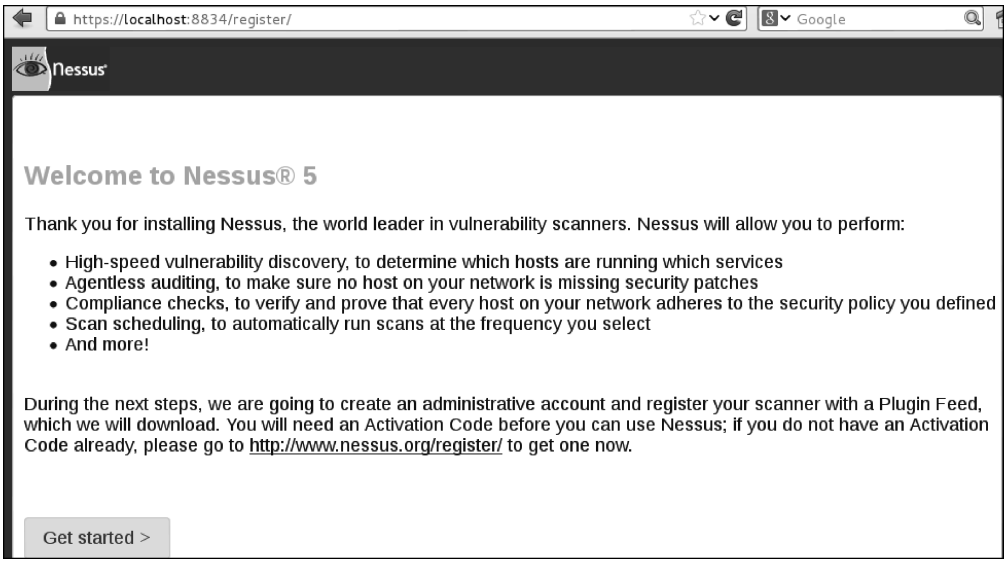

图 1.35

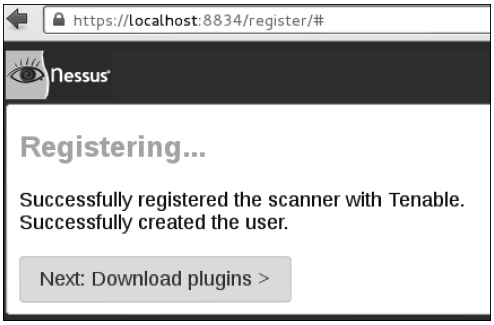

图 1.36

4．您只有在成功注册之后才能下载并使用最新的 Nessus 组件。下载程序组件的时间会比较长，您可以充分利用这个时间做些其他事情。

1.9.2　安装 Cisco 密码破解工具

在第二个实例里，我们将安装一个名为 `cisco_crack` 的密码破解工具。它主要用来破解 Cisco 配置文件中的 type 7 类型密码。我们可以在官方网站下载它的源代码，该网站网址是 `http:// insecure.org/sploits/cisco.passwords.html`。

Cisco 配置文件中的 type 7 类型密码，其加密强度相当弱，所以应当避免使用这种类型的密码。虽然此类密码已经很少见了，但是还是有些设备在使用这种密码。在这种情况下，Cisco Crack 这类工具将会派得上用场。

下载了源代码之后，下一个步骤就是编译源代码。在开始编译它之前，您需要在原文件里添加两条 include 语句：

```
#include <string.h>
#include <stdlib.h>
```

现在，这个源代码文件应该有 4 条 include 语句。

我们使用下述命令编译程序的源代码。

```
gcc cisco_crack.c -o cisco_crack
```

如果编译成功，将会产生一个名为 cisco_crack 的可执行文件。我们可以通过下述指令查看它的帮助信息。

```
# ./cisco_crack  -h
Usage: ./cisco_crack -p <encrypted password>
       ./cisco_crack <router config file> <output file>
```

1.10 本章总结

本章带您步入 Kali Linux 的奇妙世界。您可以在实地的渗透测试工作中直接使用其独到的 Live DVD 系统。Kali 的前身是 BackTrack——一个非常著名的主攻渗透测试的 Linux 发行版。

本章首先介绍了 Kali Linux 的简史，然后介绍了它的主要功能。最新版本的 Kali Linux 自带有很多可用于渗透测试的软件工具。除了渗透功能之外，Kali Linux 还可用于电子取证、无线安全研究、逆向工程和硬件破解。

在此基础上，本章介绍了安装 Kali Linux 的多种方法。虽然无需安装 Kali Linux 系统就可以把它直接当作 Live DVD 使用，但是我们也可以把它安装到硬盘上，甚至是 USB 闪存里。当我们把它安装到 USB 闪存的时候，它就成为了 portable Kali Linux。

在使用 Kali Linux 开始做渗透测试之前，您还需要设置好或有线或无线的网络连接。我们还介绍了 VirtualBox 虚拟机系统的一些特性，包括安装虚拟机客户端功能增强包，设置文件夹共享，导出虚拟机和快照备份。

因为 Kali Linux 整合了操作系统以外的一些软件，所以在必要的时候需要进行系统更新。我们可以单独更新应用程序，也可以连同 Linux 内核一并更新。

您可能需要进行一些渗透测试方面的练习。但是在多数国家里，未经许可就渗透他人的服务器是违法行为。为了满足教学的需要，人们刻意单独研发出了多种脆弱系统——一种含有很多漏洞的虚拟主机。您可以在虚拟机里安装脆弱系统，以进行渗透测试的练习。本文推荐的脆弱系统是 Rapid7 推出的 Metasploitable 2。

Kali Linux 系统自带有多种网络应用服务，我们选取了 HTTP、MySQL 和 SSH 进行介绍。具体来讲，相关内容都由简介和管理服务（例如启动和停止服务的方法）的篇幅组成。

在本章的最后，我们演示了安装 Nessus 网络扫描程序和 Cisco 密码破解工具的过程，介绍了如何安装没有被 Kali Linux 收录的信息安全工具。

在下一章，我们将探讨渗透测试的方法学理论。

第 2 章

渗透测试方法论

渗透测试（penetration testing，pentest）是实施安全评估（即审计）的具体手段。方法论是在制定、实施信息安全审计方案时，需要遵循的规则、惯例和过程。人们在评估网络、应用、系统或三者组合的安全状况时，不断摸索各种务实的理念和成熟的做法，并总结出了一套理论——测试方法论。本章简要介绍了渗透测试方法论的各关键要点，涉及的主题包括：

- 两种广为认知的渗透测试类型——黑盒测试和白盒测试；
- 漏洞评估和渗透测试的区别；
- 业界普遍采纳的安全测试方法论，以及其核心功能、特征和优势；
- 典型的渗透测试所涉及的 10 个阶段；
- 安全测试的道德准则。

渗透测试可能是单独进行的一项工作，也可能是常规研发生命周期（例如，Microsoft SDLC）里 IT 安全风险管理的一个组成部分。产品的安全性并不完全取决于 IT 方面的技术因素，还会受到与该产品有关的最佳安全实践的影响。具体而言，增强产品安全性的工作涉及安全需求分析、风险分析、威胁建模、代码审查和运营安全。

通常认为，渗透测试是安全评估最终的也是最具侵犯性的形式，它必须由符合资质的专业人士实施。在进行评估之前，有关人员可能了解也可能不了解目标的具体情况。渗透测试可用于评估所有的 IT 基础设施，包括应用程序、网络设备、操作系统、通信设备、物理安全和人类心理学。渗透测试的工作成果就是一份渗透测试报告。这种报告分为多个部分阐述在当前的目标系统里找到的安全弱点，并且会讨论可行的对抗措施和其他改进建议。充分应用渗透测试方法论，有助于测试人员在渗透测试的各个阶段深入理解并透彻分析当前存在的防御措施。

2.1 渗透测试的种类

虽然渗透测试各种各样，但是业内普遍将其划分为两类：白盒测试和黑盒测试。

2.1.1 黑盒测试

在进行黑盒测试时，安全审计员在不清楚被被测单位的内部技术构造的情况下，从外部评估网络基础设施的安全性。在渗透测试的各个阶段，黑盒测试借助真实世界的黑客技术，暴露出目标的安全问题，甚至可以揭露尚未被他人利用的安全弱点。渗透测试人员应能理解安全弱点，将之分类并按照风险级别（高、中、低）对其排序。通常来说，风险级别取决于相关弱点可能形成的危害的大小。老练的渗透测试专家应能确定可引发安全事故的所有攻击模式。当测试人员完成黑盒测试的所有测试工作之后，他们会把与测试对象安全状况有关的必要信息进行整理，并使用业务的语言描述这些被识别出来的风险，继而将之汇总为书面报告。黑盒测试的市场报价通常会高于白盒测试。

2.1.2 白盒测试

白盒测试的审计员可以获取被测单位的各种内部资料甚至不公开资料，所以渗透测试人员的视野更为开阔。若以白盒测试的方法评估安全漏洞，测试人员可以以最小的工作量达到最高的评估精确度。白盒测试从被测系统环境自身出发，全面消除内部安全问题，从而增加了从单位外部渗透系统的难度。黑盒测试起不到这样的作用。白盒测试所需的步骤数目与黑盒测试不相上下。另外，若能将白盒测试与常规的研发生命周期相结合，就可以在入侵者发现甚至利用安全弱点之前，尽可能最早地消除全部安全隐患。这使得白盒测试的时间、成本，以及发现、解决安全弱点的技术门槛都全面低于黑盒测试。

2.2 脆弱性评估与渗透测试

正确地理解和使用安全评估领域的技术术语十分必要。在您的职业生涯中，您可能时常会遇到那些不了解行业术语，却需要从这些专用名词里选一个进行采购的人。其实商业公司和非商业机构里大有这样的人在。至少您应该明白这些类型的测试各是什么。

脆弱性评估通过分析企业资产面临威胁的情况和程度，评估内部和外部的安全控制的安全性。这种技术上的信息系统评估，不仅要揭露现有防范措施里存在的风险，而且要提出多重备选的补救策略，并将这些策略进行比较。内部的脆弱性评估可保证内部系统的安全性，而外部的脆弱性评估则用于验证边界防护（perimeter defenses）的有效性。无论进行内部脆弱性评估还是进行外部脆弱性评估，评估人员都会采用各种攻击模式严格测试网络资产的安全性，从而验证信息系统处理安全威胁的能力，进而确定应对措施的有效性。不同类型的脆弱性评估需要的测试流程、测试工具和自动化测试技术也不相同。这可以通过

一体化的安全弱点管控（vulnerability management）平台来实现。现在的安全弱点管控平台带有可自动更新的漏洞数据库，能够测试不同类型的网络设备，而且不会影响配置管理和变更管理的完整性。

脆弱性评估和渗透测试两者最大的区别就是：渗透测试不仅要识别目标的弱点，它还涉及在目标系统上进行漏洞利用、权限提升和访问维护。换句话说，脆弱性评估虽然可以充分发现系统里的缺陷，但是不会考虑去衡量这些缺陷对系统造成的危害。另外，相比脆弱性评估，渗透测试更倾向于入侵，会刻意使用各种技术手段利用安全漏洞；所以渗透测试可能对生产环境带来实际的破坏性影响。而脆弱性评估则是以非入侵性的方式，定性、定量地识别已知安全弱点。

为何需要渗透测试？

如果不能确定防火墙、IDS、文件完整性监控等风险减缓控制的实际效果，那么就应当进行渗透测试。虽然漏洞扫描（脆弱性评估）能够发现各个漏洞，但是渗透测试则会验证这些漏洞在实际环境里被利用的可能性。

有些观点认为，这两种类型的安全评估重复性很高，只是同义词而已。这种观点绝对有误。合格的安全顾问会根据客户的商务需求，选择一种最合适的安全评估向顾客推荐，绝对不会把不同类型的安全评估混为一谈。然而，仔细核实安全评估项目的内容和做出最终决定确实是顾客的责任。

渗透测试的价格比脆弱性评估的价格要高。

2.3　安全测试方法论

为满足安全评估的相应需求，人们已经总结出了多种开源方法论。无论被评估目标的规模有多大，复杂性有多高，只要应用这些安全评估的方法论，就可以策略性地完成各种时间要求苛刻、富有挑战性的安全评估任务。某些方法论专注于安全测试的技术方面，有些则关注管理领域。只有极少数的方法论能够同时兼顾技术因素和管理因素。在评估工作中实践这些方法论，基本上都是按部就班地执行各种测试，以精确地判断被测试系统的安全状况。

本书再次向您推荐几种著名的安全评估方法论。本章将重点突出这些方法论的关键特征和优势，希望它们能够帮助您拓宽网络安全和应用安全评估的视野。

- 开源安全测试方法论
- 信息系统安全评估框架
- 开放式 Web 应用安全项目
- Web 应用安全联合威胁分类
- 渗透测试执行标准

上述这些测试框架和方法论，都能够指导安全人士针对客户需求制定最得当的策略。其中，前两个方法论所提供的通用原则和方法，几乎可以指导面向任何类型资产的安全测试。由 **OWASP（Open Web Application Security Project）**推出的测试框架主要面向应用安全的安全评估。**PTES（Penetration Testing Execution Standard）**能够指导所有类型的渗透测试工作。然而需要注意的是，安全状态本身是一个持续变化的过程，而渗透测试只能够获取目标系统在被测试的那一时刻的安全状态。在测试的过程中，哪怕被测的信息系统发生了细微的变化，都可能影响安全测试的全局工作，从而导致最终的测试结果不正确。此外，单一的测试方法论并不一定能够涵盖风险评估工作的所有方面。而拟定适合目标网络和应用环境的最佳测试策略，确实是安全审计人员的职责。

安全测试的方法论有很多。要选取最佳的指导理论，就需要综合考虑成本和效果的因素。所以，评估策略的筛选工作受到多种因素的制约。这些因素包括与目标系统有关的技术细节和各种资源、渗透人员的知识结构、业务目标以及法规问题。以业务的角度看，效果和成本控制至关重要。本文介绍的这几种方法论，在官方网站上都有非常正规的详细说明文件。在此，我们对它们进行简要总结。如需了解详细的工作流程，您需要亲自访问相关网站，仔细研究各种文件和实施细则。

2.3.1 开源安全测试方法论（OSSTMM）

开源安全测试方法论（Open Source Security Testing Methodology Manual，OSSTMM）（官方网站是 `http://www.isecom.org/research/osstmm.html`）是由 Pete Herzog 创建，继而由 ISECOM 发展的测试方法论。它是国际公认的安全测试和安全分析标准。很多企业正在他们的日常评估工作中应用这一标准。以技术的角度看，这一方法论把安全评估工作划分为 4 组：范围（scope）、信道（channel）、索引（index）和矢量（vector）。“范围”指代评估人员收集被测单位全部资产相关信息的工作。“信道”则是这些资产之间的通信方式和互动类型；包括物理方式、光学方式和其他方式的通信。每个信道都构成了一套独特的安

全组件，都要在评估阶段进行测试和验证。这些组件包括物理安全、人类心理学、数据网络、无线通信介质和电信设施。所谓“索引”，泛指特定资产和相应 ID 的对应关系。例如，审计人员常常要明确 MAC 地址和 IP 地址的对应关系，就是为了整理一种索引。而“矢量”指的是审计人员访问和分析功能性资产的方式。以上几个部分，组成了全面评估被测 IT 运营环境的整个技术流程，被称为审计范畴（**audit scope**）。

OSSTMM 的方法论总结了多种形式的安全测试，并将它们划分为 6 个标准种类。

- **盲测（blind）**：事先不了解目标系统的任何情况的测试就是盲测。然而，在评估过程开始之前，被测单位会知道何时开始安全测试。道德黑客（Ethical hacking）和对抗竞赛（War Gaming）就是典型的盲测。因为盲测遵循了道德规范，事先通知被测单位，所以这种测试方法也被广泛接受。
- **双盲测试（double blind）**：在双盲测试中，审计人员事先不清楚目标系统的情况，被测单位事先也不会知道将有安全测试。黑盒审计和渗透测试都属于双盲测试。当前绝大多数的安全审计采用双盲测试方法。对于审计人员来说，选择能够胜任的最佳工具和最佳技术已经是一种考验了。
- **灰盒测试（grey box）**：在灰盒测试中，审计师仅了解被测系统有限的情况，被测单位也会知道审计开始和结束的时间。脆弱性评估就属于灰盒测试。
- **双灰盒测试（double grey box）**：双灰盒测试工作的方式类似于灰盒测试。只不过在双灰盒测试中，会给审计人员定义一个时限，而且这种测试不涉及信道测试和渗透矢量。白盒审计就属于双灰盒测试。
- **串联测试（tandem）**：在串联测试中，审计人员对目标系统只有最低限度的了解，而在测试开始前他们会通告被测单位。需要注意的是，串联测试会测试得比较彻底。水晶盒测试和内部审计都是串联测试的例子。
- **逆向测试（reversal）**：在逆向测试中，审计员充分了解目标系统；而被测单位将永远不会知道测试的时间或方式。

OSSTMM 推广的技术评估框架十分灵活。即使某个项目在逻辑上可分为 3 个连续的信道和 5 个安全组件，我们照样可以使用 OSSTMM 的框架评估其安全性。OSSTMM 体系的测试方法，通过检查访问控制安全、流程安全、数据控制、物理位置、周界防护、安全意识水平、信任关系、反欺诈控制等诸多过程，全面评估被测单位的安全性。总体而言，这一理论强调测试目标和测试方法，注重在测试前、测试中、测试后应当采用的相应策略，而且介绍了解读和综合分析测试结果的方法。确切掌握目标系统当前的防护水平至关重要，有关数据十分珍贵。OSSTMM 引入了 **RAV**（**Risk Assessment Value**，**风险评估值**）的概念，

并通过它阐述了这一理论的很多理念。RAV 的基本功能是分析测试结果，进而基于三个因素（运营安全、损耗控制、局限程度）的标称值来计算安全的标称值。最后求得的这个标称值称为 RAV 得分。在引入 RAV 得分的概念之后，审计人员可以量化评估当前的安全状态，并可为企业安全的下一步目标设定里程碑。从商业的角度来看，RAV 有助于优化安全投资，并可助您选择更为有效的安全解决方案。

主要特性与优势

OSSTMM 的主要特性与优势如下。

- OSSTMM 的方法可从本质上降低假阴性和假阳性的发生率。它推出的测量方法具有普遍的应用价值。
- 该架构适用于多种类型的安全测试，可用于渗透测试、白盒测试审计、漏洞评估等其他测试。
- 它能够确保每次评估应进行得全面彻底，还能保证评估过程的一致性、可测性、可靠性。
- 该方法本身可分为 4 个相对独立的阶段，即定义阶段、信息阶段、调节阶段和控制测试阶段。每一个阶段都会获取、评估和验证目标环境中的相关信息。
- RAV 的计算方法综合衡量了运营安全、损耗控制、局限程度的情况。它的计算结果即 RAV 得分，可代表目标系统当前的安全状况。
- 这种方法的评估报告均采用**安全测试审计报告（STAR，Security Test Audit Report）**模板。以这种格式书写的报告同时适合被测单位的管理层和技术层阅读，有助于他们共同理解测试目标、风险评估值（RAV）和每个阶段的测试结果。
- 该方法定期更新。OSSTMM 会符合安全测试、法规和法规问题的新变化。
- OSSTMM 与行业法规、企业政策，以及政府法规兼容。此外，官方认可的审计员都是直接从 **ISECOM（安全与开放式方法论研究协会）**获取的资格认证。

2.3.2 信息系统安全评估框架

信息系统安全评估框架（Information Systems Security Assessment Framework，ISSAF）（www.oissg. org/issaf）是另外一种开放源代码的安全性测试和安全分析框架。为了解决安全评估工作的逻辑顺序问题，该框架已分为若干个领域（domain）。不同领域评估目标系统的不同部分，而且可以根据实际情况对每个领域进行相应调整。把这一架构

与日常业务的生命周期相结合，可以充分满足企业安全测试的准确性、完整性、高效性的需求。ISSAF 兼顾了安全测试的技术方面和管理方面。在技术方面，它有一整套关键的规则和程序，形成了一套完备的评估程序。在管理方面，它明确了在整个测试过程中应当遵循的管理要则和最佳实践。应当注意，ISSAF 主张安全评估是一个过程，而不是一次审计。审计框架应当分为计划、评估、修复、评审以及维护阶段，应当有更为完善的标准。然而 ISSAF 具有灵活和高效的特点，是审计工作各个阶段的通用准则，可适用于所有企业结构。

这一框架的交付报告分为业务活动、安全措施、目标系统中可能存在的安全弱点的完整清单。其评估过程注重分析被测单位最容易被利用的关键漏洞，侧重于以通过最短路径尽快完成测试任务。

ISSAF 的技术评估基准十分全面，可用于测试各种技术和不同流程。不过，丰富的内容带来了一大副作用，即要跟上评估领域的技术变化速度，这一框架就需要频繁更新。相对而言，OSSTMM 受技术更新影响的幅度略小。即使审计人员使用不同的工具和全新的技术，他们遵循的方法论却基本不变。虽然如此，但是 ISSAF 仍然号称是由最新的安全工具、最佳实践，以及补充安全评估计划的管理理念所组成的广泛框架。它也可以和 OSSTMM 或其他测试方法论一起使用，从而能够兼有各种方法的优点。

主要特性与优势

ISSAF 的主要特性与优势如下。

- ISSAF 主要测试当前安全控制措施中的严重漏洞，所以它在保障系统安全方面的意义重大。
- 它关注信息安全范畴内的各个关键领域，涵盖了风险评估、业务结构和管理、控制评估、服务管理、安全策略的开发和常规的最佳实践。
- ISSAF 渗透测试方法论评估网络、系统或应用程序的安全性。应用该框架可以无阻碍地把精力重点放在特定技术上，如路由器、交换机、防火墙、入侵检测和防御系统、存储区域网络、虚拟专用网络、各种操作系统、Web 应用服务器、数据库等。
- 通过必要的控制和处理，它可以统一技术层和管理层这两方面人员对安全测试的理解。
- 它可帮助管理人员理解当前边界防御体系的现有风险，并可指出可能影响业务完整性的安全弱点，从而帮助人们主动地减少风险。

可同时结合OSSTMM和ISSAF两种理论评估企业环境的安全状况。

2.3.3 开放式 Web 应用程序安全项目

开放式 Web 应用程序安全项目（**Open Web Application Security Project，OWASP**）定期推出其 **top 10 project**（ 排名前十位的安全隐患防护守则）以提高公共对应用安全的认知意识。这个项目公开了编写安全程序所需遵循的各种原则和惯例。OWASP 的测试项目（https://www.owasp.org/index.php/owasp- Testing_Project）公布了一套非常实用的安全测试指南。您应当仔细阅读这部分内容，因为这个测试框架往往可以指导您的工作。

OWASP 的 Top 10 Project 总结了各种攻击矢量，按照各种隐患可能在技术上和业务上造成的危害，对影响应用安全的风险进行分类和排名。在评估应用程序安全时，这些排名前十的安全风险揭露了普遍存在于各种技术和平台的通用攻击方法。它还阐述了测试、验证和修补应用程序安全弱点的具体方法。尽管 Top 10 Project 揭示了安全领域的高风险问题，但是这 10 种风险也只是 Web 应用程序安全性问题的一部分而已。尽管如此，OWASP 社区的很多指南仍然可以指导开发人员和安全审计人员有效地管理 Web 应用程序的安全。

- **测试指南**：https://www.owasp.org/index.php/OWASP_Testing-Guide_v3_Table_of_Content。
- **开发人员指南**：https://www.owasp.org/index.php/Guide。
- **代码审查指南**：https://www.owasp.org/index.php/Category: OWASP_Code_Review_ Project。

OWASP 的 Top 10 Project 每年都会更新。如需获取详细信息，请访问这个项目的官方网站 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project。

主要特性与优势

OWASP 的主要特性与优势如下。

- OWASP 推出了 Web 应用程序的十大安全风险的测试方法。应用这些方法，可使应用程序避免出现常见的安全缺陷，免受常见攻击的危害，进而巩固了应用程序的保密性、完整性和可用性。
- OWASP 社区研发出大量安全工具，这些工具可辅助进行自动或手动的 Web 应用程

序测试。Kali Linux 收录了其中较为著名的程序，如 WebScarab、Wapiti、JBroFuzz 和 SQLiX 等。

- 在网络基础设施的安全评估方面，OWASP 测试指南为您提供了特定技术的评估细则。举例来说，它的甲骨文（Oracle）的测试方法与 MySQL 的测试方法就各有针对性。该指南采用多种相互关联的方法评估各种技术，有助于审计人员因地制宜地制定测试方法。
- 它鼓励研发人员在研发周期的每个阶段进行有计划的安全测试。这能提高应用程序的健全性、安全性，并能减少程序中的错误。
- 它在业内的认可度和知名度屈指可数。若把排名前十位的安全隐患防护守则与其他 Web 应用程序安全评估标准结合使用，您可同时满足一个以上的安全标准。

2.3.4　Web 应用安全联合威胁分类

只有彻底、严格的测试流程，才能发现应用程序的安全隐患，而这些测试流程完全可以纳入软件的开发生命周期。Web 应用安全联合威胁分类（Web Application Security Consortium Threat Classification，WASC-TC）是这样的一个评估 Web 应用程序安全性的开放标准。与 OWASP 标准相似，它也从攻击和弱点两方面讨论安全问题，但这一标准以更为深入的方式解决安全隐患。要识别、验证应用程序所面临的各种威胁，就要遵循标准化的工作流程。WASC-TC 可以迅速适用于各种技术环境，有着显著的易用性。整体上说，它能够帮助开发人员和安全审计人员以不同的视图了解 Web 应用程序面临的安全威胁。

- **枚举视图**：枚举视图是分析 Web 应用程序攻击手段和相应安全弱点的基础。它从定义、类型和多种编程平台的实例这几个角度，详细讨论了每种攻击手段和每个安全弱点。另外，所涉及的安全弱点和攻击手段都被分配了唯一的识别编号，以便于人们引用。目前，这个视图里总共有 49 个 WASC-ID 号码（1～49）。这些编号并不代表相应条目的危害程度，仅仅是为了方便引用而分配的编号。
- **开发视图**：开发视图关联分析外部的攻击和程序内部的安全弱点，将开发人员的视野转向程序自身的漏洞。这一分析适用于开发周期的三个阶段，即设计、实现（编程）、部署阶段。如果在明确应用程序的需求时没有充分考虑安全方面要求，就会在研发周期的初期阶段引发漏洞，形成设计阶段的安全弱点。不安全的编程规则或不当的惯例产生会造成实现阶段的安全弱点。无论在应用程序、Web 服务器或是其他外部系统的配置过程中哪个部分出现差错，最终都会导致部属阶段的安全弱点。可见，这个视图以最佳安全实践为蓝本，提出了将安全保障措施融入到日常的研发生命周期的具体方法。

- **交叉引用视图**：这个视图关联地分析了多种 Web 应用安全标准。通过对该视图的引用，审计人员和开发团队能够把当前所使用的标准中的术语（标准条款）与其他标准的相应内容进行对照分析。如此一来，只需要较少的开销，就可以让一个项目同时符合多种不同的安全标准。因为不同的应用程序安全标准会从不同的角度评估应用程序的安全性，所以它们衡量同一的风险的评估指标也不尽相同。因此，要对不同安全标准进行差异性分析，才能够正确地计算安全风险及其严重程度。当前 WASC-TC 中的攻击方法和薄弱环节，可以映射到 OWASP 的 Top 10 Project、Mitre **通用缺陷列表（Common Weakness Enumeration，CWE）**、Mitre **通用攻击模式列表和分类（Common Attack Pattern Enumeration and Classification，CAPEC）**、SANS-CWE 排名前 25 的软件高危错误列表（SANS-CWE Top 25 list）。

Mitre's CWE 的官方网站是 `https://cwe.mitre.org/`。

Mitre's CAPEC 的官方网站是 `http://capec.mitre.org/`。

SANS-CWE 的排名前 25 的软件高危错误列表的发布网站是 `http://www.sans.org/top25-software-errors/`。

如需详细了解 WASC-TC 及其评论，请访问官方网站：`http://projects.webappsec.org/Threat-Classification`。

主要特性与优势

WASC－TC 的主要特性与优势如下。

- WASC－TC 围绕常见攻击和常规弱点这一中心，深入讨论了 Web 应用程序运营系统的安全评估方法。
- 无论何种 Web 应用程序平台，都可使用 Kali Linux 的工具集验证、测试 WASC－TC 提出的常见攻击和常规弱点。
- 它提出了三种不同视图，即枚举视图、开发视图和交叉引用视图。枚举视图起到了基础数据库的作用，它列举了在 Web 应用中所有可能被发现的攻击方法和安全弱点。开发视图将这些攻击方法和安全弱点进行关联分析，整理成一系列漏洞，并根据它们在开发过程中的出现阶段进行分类。而开发阶段又可分为设计阶段、实现阶段和部署阶段。WASC-TC 标准的交叉引用视图用于对照、引用其他的应用程序安全标准。
- WASC-TC 标准已经得到了业界的广泛认可。在许多开源和商业解决方案里，特别

是漏洞评估和管控产品中，都能看到 WASC-TC 的身影。

- WASC-TC 也可以和其他著名的应用安全标准兼容，例如 OWASP 和 SANS-CWE。

2.4　渗透测试执行标准

渗透测试执行标准（Penetration Testing Execution Standard，PTES）的先驱都是渗透测试行业的精英。这个标准由渗透测试 7 个阶段的标准组成，可在任意环境中进行富有成果的渗透测试。它的官方网站详细介绍了具体测试方法，有兴趣的读者可访问 `http://www.pentest-standard.org/index.php/Main_Page`。

根据这一标准，标准的渗透测试可以分为下述 7 个阶段：

- 事前互动；
- 情报收集；
- 威胁建模；
- 漏洞分析；
- 漏洞利用；
- 深度利用；
- 书面报告。

PTES 的官方网站详细介绍了每个阶段的思维导图（mind maps）和组成步骤。这些内容有助于审计人员根据被测环境的测试要求，对 PTES 标准进行相应调整。只要在其官方网站上点击思维导图的构成节点，就可详细查看该节点的各个组成步骤。

主要特性与优势

PTES 的主要特性与优势如下。

- 它是非常全面的渗透测试框架，涵盖了渗透测试的技术方面和其他重要的方面，如范围蔓延（scope creep）、报告，以及渗透测试人员保护自身的方法。
- 它介绍了多数测试任务的具体方法，可指导您准确测试目标系统的安全状态。
- 它汇聚了多名日行一“渗”的渗透测试专家的丰富经验。
- 它包含了最常用的以及很罕见的相关技术。
- 它浅显易懂，您可根据测试工作的需要对相应测试步骤进行调整。

2.5 通用渗透测试框架

Kali Linux 属于通用型操作系统，它配备有多种安全评估工具和渗透测试工具。在没有合适的测试理论指导的情况下冒然使用这些工具，可能会导致测试失败，测试结果可能无法让人满意。因此，从技术管理的角度来看，遵循正规的测试框架对安全测试极为重要。

这一小节将通过黑盒测试的具体方法和白盒测试的通用测试方法介绍通用测试框架。它涵盖了典型的审计测试工作和渗透测试工作会涉及到的各个阶段。评估人员可以根据被测目标的具体情况对上述测试方法进行相应调整。这一方法论由一系列相关步骤所组成。要想成功完成安全评估项目，必须在测试的初始化阶段、测试进行阶段以及测试结束阶段全面遵循这些步骤。这些步骤包括：

- 范围界定；
- 信息收集；
- 目标识别；
- 服务枚举；
- 漏洞映射；
- 社会工程学；
- 漏洞利用；
- 提升权限；
- 访问维护；
- 文档报告。

无论是进行白盒测试还是黑盒测试，选择和使用测试步骤都是测试人员的责任。在测试开始前，测试人员需要根据目标系统的实际环境和已掌握的关于目标系统的情况，制定最佳的测试策略。下文将会介绍每一个测试阶段，包括它们的简要描述、定义和可能适用的应用程序。虽然这种通用测试方法论可以配合其他的方法论同时使用，但是它只是一种指导建议，而不是全能的渗透测试解决方案。

2.5.1 范围界定

在开始技术性安全评估之前，务必要观察、研究目标环境的被测范围。同时还要了解，

这个范围牵扯到多少个单位，是单个单位还是多个单位会参与到安全评估的工作中来。在范围界定阶段，需要考虑的典型因素如下。

- 测试对象是什么？
- 应当采取何种测试方法？
- 有哪些在测试过程中需要满足的条件？
- 哪些因素可能会限制测试执行的过程？
- 需要多久才能完成测试？
- 此次测试应当达成什么任务目标？

审计人员只有确切理解被评估系统所使用的技术，理解其基本功能，以及相关技术与网络之间的相互影响，才能成功达成渗透测试的目标。因此，无论是进行什么类型的安全评估项目，审计人员的知识结构都将起着至关重要的作用。

2.5.2　信息收集

在划定了测试范围之后，就需要进入信息收集阶段。在这个阶段，渗透测试人员需要使用各种公开资源尽可能地获取测试目标的相关信息。他们从互联网上搜集信息的互联网渠道主要有：

- 论坛；
- 公告板；
- 新闻组；
- 媒体文章；
- 博客；
- 社交网络；
- 其他商业或非商业性的网站。

此外，他们也可借助各种搜索引擎中获取相关数据，例如谷歌、雅虎、MSN 必应、百度等。进一步说，审计人员可以使用 Kali Linux 收录的各种工具在测试目标的网络系统里挖掘信息。这些运用漏洞数据挖掘技术的工具能够收集可观信息，包括 DNS 服务器、路由关系、whois 数据库、电子邮件地址、电话号码、个人信息以及用户账户。收集到的信息越多，渗透测试成功的概率就越高。

2.5.3 目标识别

这个阶段的主要任务是识别目标的网络状态、操作系统和网络架构。该阶段工作旨在完整地展现目标网络里各种联网设备或技术的完整关系，以帮助测试人员在接下来的工作里枚举目标网络的各种服务。Kali Linux 提供的一系列先进的网络工具，可以轻松探测到联网主机，识别这些主机运行的操作系统，并根据每个设备在网络系统中的不同角色对它们进行归类。这些工具通常采用了基于上层网络协议的主动和被动的检测技术。它们能够通过不同的方式巧妙地利用各种协议获取许多有用的信息，比如操作系统指纹等。

2.5.4 服务枚举

这一阶段会根据前面各个阶段的成果，进一步找出目标系统中所有开放的端口。一旦找到了所有开放的端口，就可以通过这些端口来列出目标系统上运行的服务。有很多扫描端口的技术，如全开（full-open）扫描、半开（half-open）扫描、隐蔽式（stealth）扫描等。这些技术都可用来检测端口的开放情况，甚至可以扫描处于防火墙或者入侵检测系统保护下的主机。主机上开放的端口都有相应的服务程序，对这些信息进行深度分析之后，可进一步发掘目标网络基础设施中可能存在的漏洞。因此，这个阶段为其后的测试工作打下了基础，有助于测试人员继而发现各种网络设备上可能会造成严重危害的安全漏洞。Kali Linux 收录的部分自动化工具可以辅助审计人员完成这一阶段的目标。

2.5.5 漏洞映射

至此为止，我们已经充分收集了目标网络的各种信息。接下来，我们就可以根据已经发现的开放端口和服务程序，查找、分析目标系统中存在的漏洞。Kali Linux 系统中提供的一系列自动化的网络和应用漏洞评估工具可以担任完成这个阶段的任务。当然，人工（手动）完成这些任务未尝不可，只是人工操作极为耗时，而且需要有关人员拥有专家级的知识。但是，如果能够将自动和手动这两种不同的测试方法结合起来，审计人员对目标系统的认知就会更为清晰、透彻，并能够仔细地检查任何已知和未知的漏洞。否则，被遗漏的漏洞将会一直残留在目标网络系统里。

2.5.6 社会工程学

如果目标网络没有直接的入口，欺骗的艺术将起到抛砖引玉的重要作用。对目标组织中的人员进行定向攻击，很有可能帮助我们找到渗透目标系统的入口。例如，诱使用户运

行会安装后门的恶意程序，就可能为审计人员的渗透工作形成突破。社会工程学渗透分为多种不同实现形式。伪装成网络管理员，通过电话要求用户提供自己的账户信息；发送钓鱼邮件来劫持用户的银行账户；甚至是诱使某人出现在某个地点——这些都属于社会工程学攻击。在社会工程学中，达成同一既定目标的实现方式应有尽有。需要注意的是，在对目标实施欺骗以达成渗透目标之前，多数情况下需要长时间研究目标人员的心理。另外，在开展这个阶段的工作之前，您需要事先研究国内的法律是否有关于社会工程学的相关条款。

2.5.7　漏洞利用

在仔细检查和发现目标系统中的漏洞之后，就可以使用已有的漏洞利用程序对目标系统进行渗透。某些情况下不得不对漏洞利用程序（exploit）进行额外的研究和修改，否则它可能就无法正常工作。虽然这听起来就很麻烦，但是先进的漏洞利用（修改）工具可使这项工作容易得多，而且 Kali Linux 已经收录了这种工具。此外，审计人员可以把客户端漏洞利用程序和社会工程学进行结合，进而控制目标系统。这个阶段的主要任务是控制目标系统。整个流程可以分为 3 步，涉及攻击前、攻击、攻击后的相关行动。

2.5.8　提升权限

获取目标系统的控制权是渗透成功的标志。接下来，审计人员就可以依据其所拥有的访问权限，在被测系统中自由发挥。审计人员也可以使用适用于目标系统的本地漏洞来提升自己的权限。只要他们能够在目标系统上运行提权漏洞利用程序，就可以获得主机上的超级用户权限或者系统级权限。审计人员还可以以该主机为跳板，进一步攻击局域网络。根据之前对渗透范围的界定，审计人员接下来会开展的攻击可能是受限制的，也可能是不受限的。而后，他们很有可能以各种方式获得与被控制系统有关的更多信息。具体的说，他们可能使用嗅探手段截获网络数据包，破解各种服务的密码，在局域网络中使用网络欺骗手段。所以说，提升权限的最终目的是获得目标系统的最高访问权限。

2.5.9　访问维护

多数情况下，审计人员需要在一段时间内维护他们对目标系统的访问权限。例如，在演示越权访问目标系统的时候，安装后门将节省重新渗透目标系统所耗费的大量时间。这些情况下，访问维护将节约获取目标系统访问权限所需要的时间、花费和资源。审计人员可以通过一些秘密的通信隧道，在既定时间内维持对目标的访问权限。这些隧道往往基于特定协议、代理或者点对点通信方法的后门程序。这种对系统的访问方法可以清楚地展示，

入侵人员在目标系统实施攻击时隐匿行踪的具体方法。

2.5.10 文档报告

在渗透测试的最后一个环节里，审计人员要记录、报告并现场演示那些已经识别、验证和利用了的安全漏洞。被测单位的管理和技术团队会检查渗透时使用的方法，并会根据这些文档修补所有存在的安全漏洞。所以从道德角度来看，文档报告的工作十分重要。为了帮助惯例人员和技术人员共同理解、分析当前 IT 基础架构中的薄弱环节，可能需要给不同的部门撰写不同措辞的书面报告。此外，这些报告还可以用来获取和比较渗透测试前后目标系统的完整性。

2.6 道德准则

专业的、道德的、经过授权的安全测试服务，离不开由事先约定的规则所组成的安全测试道德准则。这些准则约定了安全测试服务的服务方式、安全实施的测试方法、合同和谈判所约定的法律条款、测试的范围、测试的准备、测试的流程，以及报告结构的一致性。要顾全上述因素，就要仔细地考察、设计在整个测试过程中都要遵循的正规的操作方法和相关流程。下面将介绍一些常见的到的准则。

- 审计人员不得在和客户达成正式协议之前对目标系统进行任何形式的渗透测试。这种不道德的营销方法有可能破坏客户的正常业务。在某些国家或地区，这种行为甚至可能是违法行为。
- 在测试过程中，在没有得到客户明确许可的情况下，测试人员不得进行超出测试范围越过已约定范畴的安全测试。
- 具有法律效力的正式合同可帮助测试人员避免承担不必要的法律责任。正式合同将会约定哪些渗透行为属于免责范围。这份合同必须清楚地说明测试的条款和条件、紧急联系信息、工作任务声明以及任何明显的利益冲突。
- 测试人员应当遵守测试计划所明确的安全评估的时间期限。渗透测试的时间应当避开正常生产业务的时间段，以避免造成相互影响。
- 测试人员应当遵循在测试流程里约定的必要步骤。这些规则以技术和管理不同角度，通过内部环境和相关人员来制约测试的流程。
- 在范围界定阶段，应当在合同书里明确说明安全评估业务涉及到的所有实体，以及他们在安全评估的过程中受到哪些制约。

- 测试结果和书面报告必须清晰，其顺序必须一致。报告中提及的所有已知的和未知的漏洞，必须以安全保密的方式递交给有权查看报告的相关责任人。

2.7　本章总结

本章详细介绍了多种渗透测试方法论，以及渗透测试的基本术语、相关类型，还有这些术语和业内其他术语之间的区别。本章的重点内容如下。

- 渗透测试可分为黑盒测试和白盒测试。黑盒测试也称为外部测试，在黑盒测试中，审计人员事先不了解目标系统的内部结构或任何技术。白盒测试也叫内部测试，在白盒测试中，审计人员了解目标系统的全部细节。结合黑盒测试和白盒测试的测试类型，称做灰盒测试。
- 脆弱性评估和渗透测试最基本的不同点在于：脆弱性评估旨在找出目标系统中存在的安全漏洞，并不会去衡量这些漏洞可能造成的相应危害；而渗透测试会进一步利用这些漏洞，发起实质性攻击以评估它们可能造成的安全问题。
- 虽然业内有很多安全测试方面的方法论，但是在评测网络系统或应用程序安全性方面，只有极少数的方法论才能够具有阶段性的循序渐进的指导意义。本章介绍了 5 个非常有名的开源安全评估方法论，突出了它们的技术功能、主要特征和优势。这 5 个方法论分别是开源安全测试方法论（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），渗透测试执行标准（PTES）以及 Web 应用安全联合威胁分类 （WASC-TC）。
- 本章还介绍了一个简单的结构化的通用测试方法论。它由安全测试行业标准方法归纳而来，分为多个标准化测试阶段。这些阶段分为：范围界定、信息收集、目标识别、服务枚举、漏洞映射、社会工程学、漏洞利用、提升权限、访问维护、文档报告。
- 最后，本章讨论了在整个安全评估过程中必须遵守的渗透测试道德准则。在安全评估的各个阶段落实有关道德准则，可以切实保障审计人员和商业实体双方的各自利益。

在接到一个渗透测试任务时，如何从客户那里获取相关信息，又如何对信息进行管理？请参见下一章。