HZ BOOKS 华章科技
[PACKT] PUBLISHING

信息安全技术丛书

Metasploit 渗透测试与开发实践指南

[美] Aditya Balapure 著 缪纶 魏大威 王鹏 刘盈斐 译

Learning Metasploit Exploitation and Development

- 分阶段深入探讨真实网络环境下的黑客攻击，全方位展示漏洞利用的最佳技巧
- 从实际的安装到漏洞评估，再到最后的漏洞利用，详细讲解渗透测试的基础知识和最佳实践，包括最新的漏洞利用方法，以及真实黑客的实践经验

机械工业出版社
China Machine Press

信息安全
技术丛书

Metasploit
渗透测试与开发实践指南

Learning Metasploit Exploitation and Development

[美] Aditya Balapure 著 缪纶 魏大威 王鹏 刘盈斐 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Metasploit渗透测试与开发实践指南 /（美）巴拉飘（Balapure，A.）著；缪纶等译 . —北京：机械工业出版社，2014.11
（信息安全技术丛书）
书名原文：Learning Metasploit Exploitation and Development

ISBN 978-7-111-48387-8

I. M… II. ①巴… ②缪… III. 计算机网络－安全技术－应用软件－指南 IV. TP393.08-62

中国版本图书馆 CIP 数据核字（2014）第 250038 号

本书版权登记号：图字：01-2013-6794

Metasploit 渗透测试与开发实践指南

出版发行：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：谢晓芳　　责任校对：董纪丽
印　　刷：三河市宏图印务有限公司　　版　　次：2014 年 11 月第 1 版第 1 次印刷
开　　本：186mm×240mm　1/16　　印　　张：12.75
书　　号：ISBN 978-7-111-48387-8　　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　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

The Translator's Words 译者序

本书是一本关于Metasploit——近年来最强大、最流行、最活跃的开源渗透测试平台软件——的使用手册。Metasploit自2004年问世时，就立即引起了整个安全社区的高度关注，并很快成为最流行的渗透测试软件。Metasploit不仅为渗透测试的初学者提供了一款功能强大、简单易用的软件，其漏洞利用代码库还是安全技术人员进行漏洞分析与研究的重要资源。甚至，当前Metasploit已经成为安全社区进行软件安全漏洞分析研究与开发的通用平台。随着Metasploit的流行，以Metasploit模块发布的漏洞利用程序成为漏洞发布的主流，同时相关书籍、资料也如泉涌般涌入市面。毋庸置疑，Meatsploit已经成为安全社区一颗璀璨的明珠，是安全技术人员“出门在外，有备无患”的渗透测试软件。

本书不是第一本介绍Metasploit软件的书籍，我们相信，它也绝对不会是最后一本。但是本书特点鲜明，不同于那些“僵硬且冰冷”的技术使用手册，书中对几乎每一个使用Metasploit的步骤都进行了实例化和图形化的演示，读者阅读本书时，会有一种阅读卡通画报般的轻松感觉，它将Metasploit强大的能力化于无形，点滴间渗入到每一个操作步骤演示实例中，让读者身临其境。同时，本书又不失深入和全面，对利用Metasploit实施网络渗透测试的各个流程环节进行了细致流畅的描述和案例讲解，并且涉及了Metasploit兵器库的每一个兵刃，真正做到了“深入浅出”，从而使读者能够理解和掌握渗透测试的基本原理、流程方法与实践技能，而且也为“资深”的技术人员提供Metasploit的实用参考手册。

本书面向网络与系统安全领域的技术爱好者与学生，以及渗透测试与漏洞分析研究方面的安全从业人员，由于Metasploit在国外安全社区中已经成为事实上的渗透测试与漏洞分析平台，相信国内也会有很多对此书感兴趣的读者。本书的翻译过程，也是我自己学习、提高和完善的过程。书中涉及的每一条指令，每一个操作我们都力求付诸实践，以深刻体会作者的意图和思想。这里也希望读者能够亲自动手实践，这样才能够更快地掌握Metasploit强大的功能和使用方法。

本书的翻译组织工作由缪纶、魏大威全面负责。第 1、2、3、4、5 章由魏大威译校，前言、第 6、7、8、9 章由王鹏译校，第 10、11、12、13 章由刘盈斐译校。

我们在翻译本书的过程中力求行文流畅，但纰漏之处在所难免，还请广大读者能够批评指正。关于本书的任何意见和建议，欢迎发送邮件至 lunmiao@tom.com，让我们共同讨论。

缪纶

2014 年 10 月于北京

Preface 前 言

本书是一本关于真实网络攻击的指南，它展示了漏洞利用这一艺术领域的最佳技巧。

为帮助读者提高学习效率，在组织结构上，作者将本书设计成定义明确的不同阶段，分阶段讲解。从实际的安装到漏洞评估，再到最后的漏洞利用，本书深入讲解了渗透测试的知识内容。本书采用了某些业界常用的工具和报告生成技巧来进行漏洞评估实践。其涵盖的内容包括客户端漏洞利用（client exploitation）、后门（backdoors）、后漏洞利用（post-exploitation），以及使用 Metasploit 开发漏洞利用代码。

本书开发了一套便于记忆的实际动手方法，方便读者对书中讲解的内容进行实践。我们相信，本书可为攻击型渗透测试人员的开发技能提供有效的帮助。

本书内容

第 1 章讲解如何搭建本书所需要的实验环境。

第 2 章介绍 Metasploit 框架的组织结构，包括 Metesploit 框架的各种接口以及体系结构。

第 3 章介绍了漏洞（vulnerability）、攻击载荷（payload）以及漏洞利用等概念。在这一章，我们也会学习如何借助于 Metasploit，使用不同的漏洞利用技术攻陷脆弱系统。

第 4 章介绍如何使用 Meterpreter 攻陷系统，并讲解在漏洞利用实施之后，借助 Meterpreter 提供的功能，我们能够收集到的信息。

第 5 章介绍 Metasploit 模块中提供的不同信息收集技术。

第 6 章介绍 Metasploit 提供的几种应用于客户端的漏洞利用技术。

第 7 章涵盖后漏洞利用的第一阶段，并讨论使用 meterpreter 对被攻陷系统进行信息收集的几种技术。

第 8 章介绍系统攻陷之后的几种提升权限技术。我们会使用几种不同的脚本和后漏洞利用模块来实现权限提升。

第 9 章介绍攻陷系统之后用于清理痕迹，以防止被系统管理员发现的几种技术。

第 10 章介绍为建立一个持久性连接，如何将一个可执行的后门程序部署到已被攻陷的系统之内。

第 11 章介绍几种不同的技术手段，通过这些技术手段，可以对外部网络上我们可触及的服务器或系统进行利用，利用这些服务器或系统攻击另外网络中的其他系统。

第 12 章介绍如何应用 Metasploit 进行漏洞攻击开发的基础知识，包括利用 Metasploit 编制漏洞攻击模块以及编制应用于这些漏洞攻击模块的不同攻击载荷。

第 13 章介绍如何使用 Metasploit 框架中的附加工具来进一步提高我们的漏洞利用技能。

开始阅读之前请了解以下内容

阅读本书，你需要事先准备好可以随手练习的软件，包括：BackTrack R2/R3、Windows XP SP2 以及 Virtual Box。

本书读者对象

本书的读者是那些对网络漏洞利用和攻击感兴趣的安全专业人员。本指南的章节安排可以帮助业内的渗透测试人员，提高他们对业界网络进行测试的技术能力。

约定

警告或重要的说明会显示在一个方框中。

提示和小技巧会以这种方式显示。

读者反馈

欢迎读者对本书内容给予反馈。这样我们就能了解你对本书的看法——喜欢还是不喜欢。读者的反馈对我们来说是非常重要的，可以帮助我们了解到读者真正从本书收获了什么。

要反馈信息，可以给我们发送邮件，邮箱是 feedback@packtpub.com，请在邮件中将本书的书名作为邮件主题（subject）。

如果你对某项主题内容非常擅长，并且也有兴趣编著或合著书籍，请关注作者指南，网址是 www.packtpub.com/authors。

客户支持

现在，你已经成为 Packt 的尊贵用户，我们会尽最大可能为你提供帮助。

勘误

虽然我们尽力保证书中内容的准确性，但错误还是难免会出现。如果你找到了书中的一处错误——可能是正文中的，也可能是代码中的——请告知我们，我们表示由衷的感谢。这样做，不仅可以帮助其他读者免受困惑之苦，还能够促使我们在本书的后续版本中进行改进。如果你发现了任何错误，请通过访问网站 http://www.packtpub.com/submit-errata 通知我们，选择书籍，单击该页面上的 errata submission（错误提交）连接，然后输入错误的详细内容即可。验证之后，你提交的内容将被接受，勘误信息就会上传到我们网站上，或者添加到对应书名已有的勘误列表中。你可以在 http://www.packtpub.com/support 上，通过选择你关心的勘误标题来查看勘误信息。

盗版

任何一种介质的出版物在互联网上的盗版问题都将一直存在下去。Packt 非常重视对版权和授权的保护。如果你在互联网上，获取了我们作品的非法副本，不管任何形式的，请你立刻将其地址或网站名称提供给我们，以便我们采取相关措施。

请将涉嫌盗版材料的链接地址发送至 copyright@packtpub.com。

你的行为，保护了作者，我们表示感谢，并尽我们所能为你提供有价值的内容。

疑问

关于本书的任何内容，如果有什么问题，你可以通过邮箱 questions@packtpub.com 联系我们，我们将竭尽所能为你解答。

技术审校者简介 *About the Reviewers*

Kubilay Onur Gungor 在 IT 安全领域有 7 年以上的工作经验，最初他从事基于无序逻辑加密图的图像 – 图像加密（images-images encrypted）方法的密码分析工作。在伊希克（Isik）大学的数据处理中心（当时他是信息安全与研究社团的会长）工作期间，他在网络安全领域获取了宝贵的经验。他曾是 Netsparker Web 应用程序安全扫描项目组的 QA 测试员。之后，他就职于土耳其一家具有领先地位的安全公司，主要从事渗透测试工作。在此期间，他为一些大客户，如银行、政府机构以及电信公司等，提供过许多基于 IT 基础架构的渗透测试和咨询服务。

目前（自 2012 年 9 月以来），作为索尼欧洲事故管理小组（Sony Europe Incident Management team）成员之一，Kubilay 致力于制定事故管理和全球网络安全策略。

同时，Kubilay 也一直在从多学科领域探究网络安全解决方法，包括犯罪、冲突管理、知觉管理、非常规战争理论、国际关系以及社会学等。他是 Arquanum 多学科网络安全和情报机构的创办人，该机构是一个国际研究学会，致力于研究不同学科卷入网络斗争中之后所造成的影响。

Kubilay 曾多次参加安全会议并经常发表演讲。

除了安全证书以外，Kubilay 还拥有外交政策、市场营销、品牌管理以及生存领域的证书。

Kubilay 还是 Freedom Riders Motorcycle Club（自由骑士摩托车俱乐部）的高级会员。

Contents 目 录

第 1 章 Chapter 1

实验环境搭建

本章将描述一个实用的实验环境的完整搭建过程。在此基础上，我们可以动手实践本书中讲述的内容。建立实验环境，需要以下三套软件：Oracle VM VirtualBox、Microsoft Windows XP SP2 以及 BackTrack5 R2。

Oracle VM VirtualBox 是 Sun 的一款产品，用于软件虚拟化，同时用于实现在一台计算机上运行多个操作系统。Oracle VM VirtualBox 支持包括 Linux、Macintosh、Sun Solaris、BSD 以及 OS/2 在内的很多操作系统。每一台虚拟机都可以独立于宿主操作系统，运行其自己的操作系统。该款软件在虚拟机中也支持网络适配器（网卡）、USB 以及物理磁盘驱动器等设备。

Microsoft Windows XP 是微软公司的一个操作系统，主要用于个人计算机和笔记本电脑。

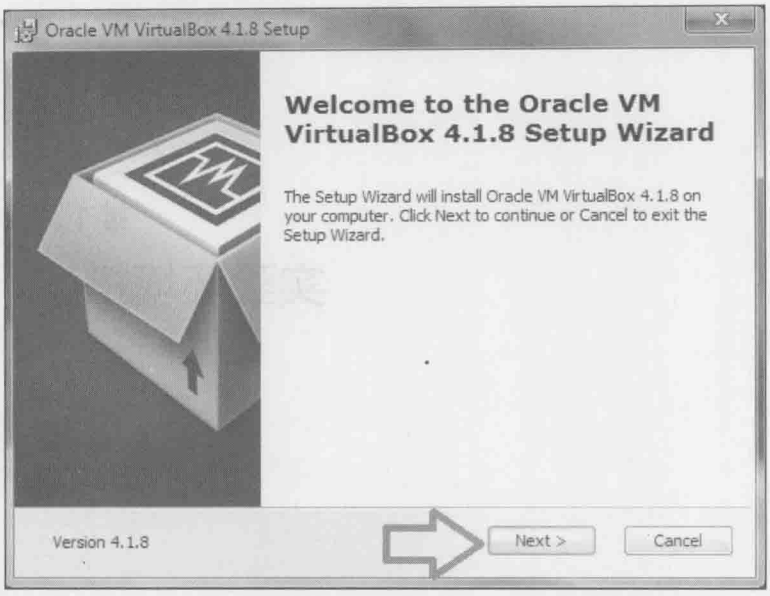
BackTrack 是一个基于 Linux 的免费操作系统，其最广大的用户是安全专业人员和渗透测试人员。该操作系统包含很多用于渗透测试和数字取证的开源工具。

现在，我们使用 Oracle VM VirtualBox 安装两个操作系统，其中 BackTrack 作为实施攻击的主机，而 Windows XP 作为受攻击主机。

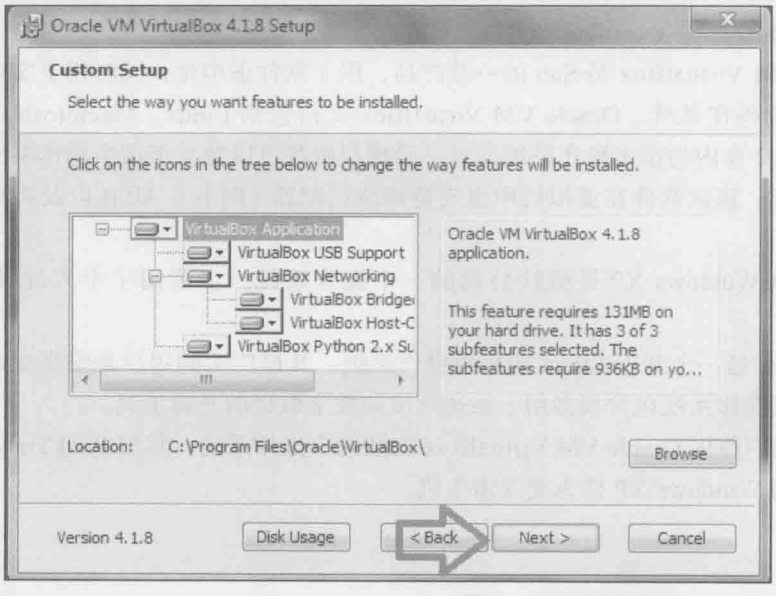
1.1 安装 Oracle VM VirtualBox

安装 Oracle VM VirtualBox 的步骤如下。

1）首先，运行安装文件开始安装，单击 Next 按钮进入下一步。

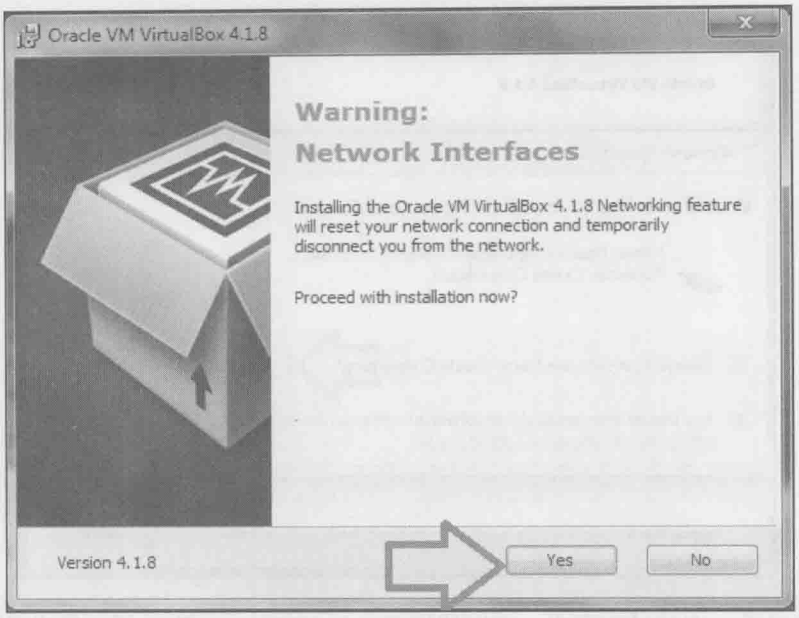


2）现在，选择安装目录并单击 Next 按钮。

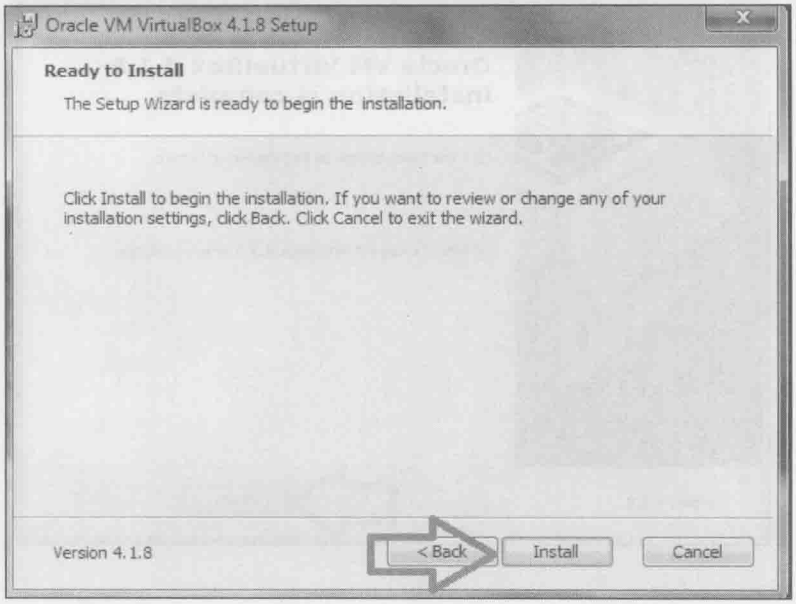


3）如果想在桌面或者开始菜单中创建快捷方式，就选择 shortcut 选项（快捷方式），然后单击 Next 按钮。

4）接下来，安装过程会重置网络连接并显示一个警告提示信息，单击 Yes 按钮，继续执行安装向导。

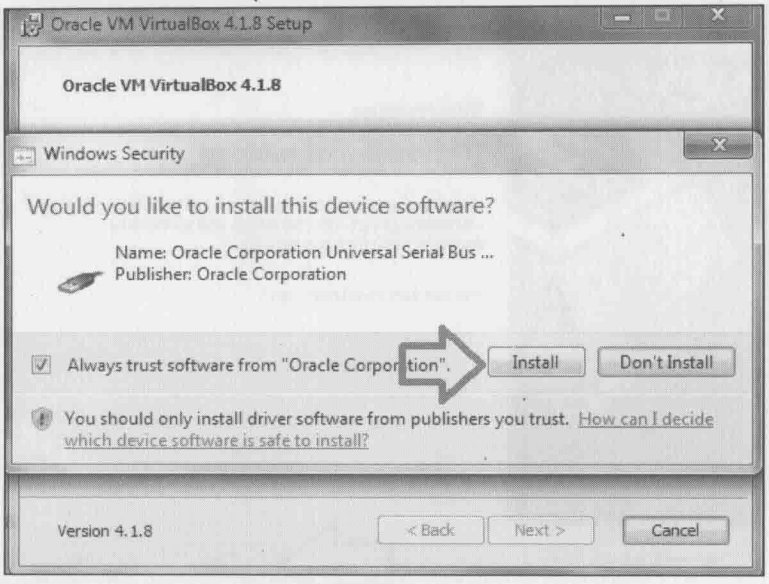


5）到这一步，安装向导已经做好安装准备，单击 Install 按钮，继续执行安装过程。

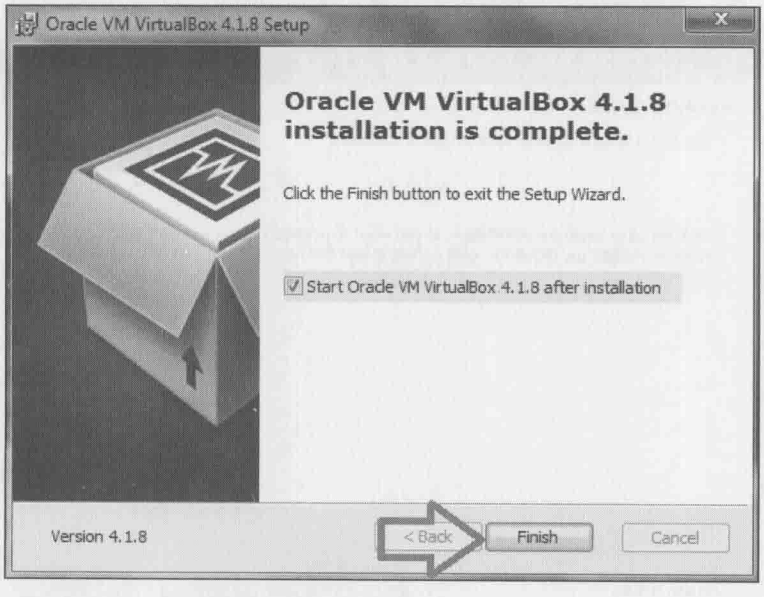


6）现在，开始安装了，这个安装过程可能需要几分钟才能完成。

7）随后，安装向导会询问是否安装 USB 设备驱动，单击 Install 按钮，同意安装 USB 设备驱动程序。



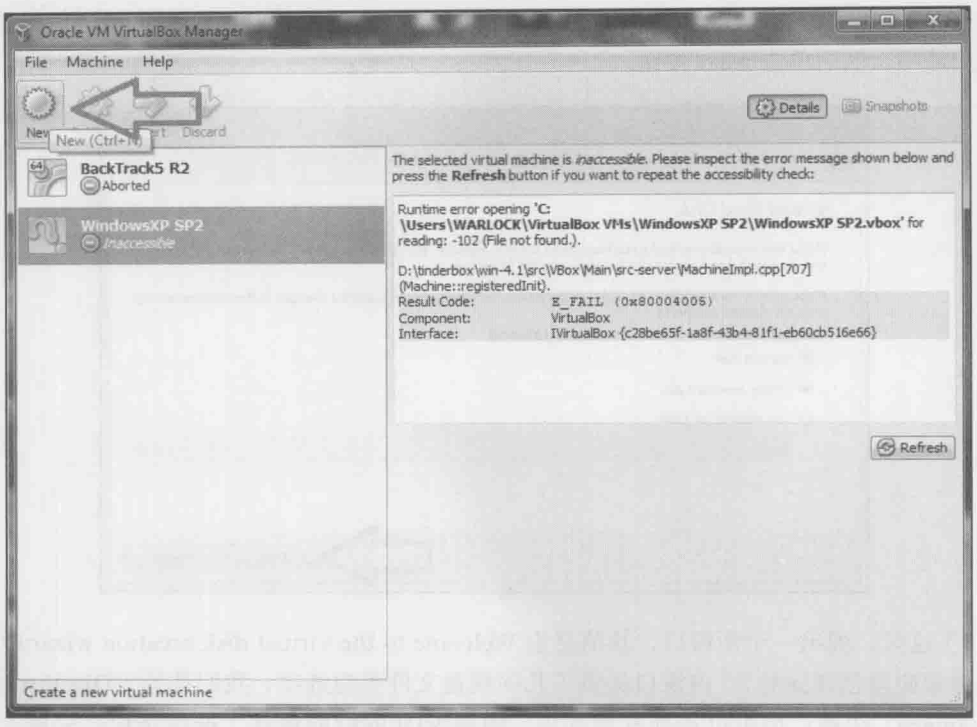
8）几分钟后，安装过程完成，可以使用 Oracle VM VirtualBox 了。单击 Finish 按钮。



1.2 在 Oracle VM VirtualBox 上安装 Windows XP

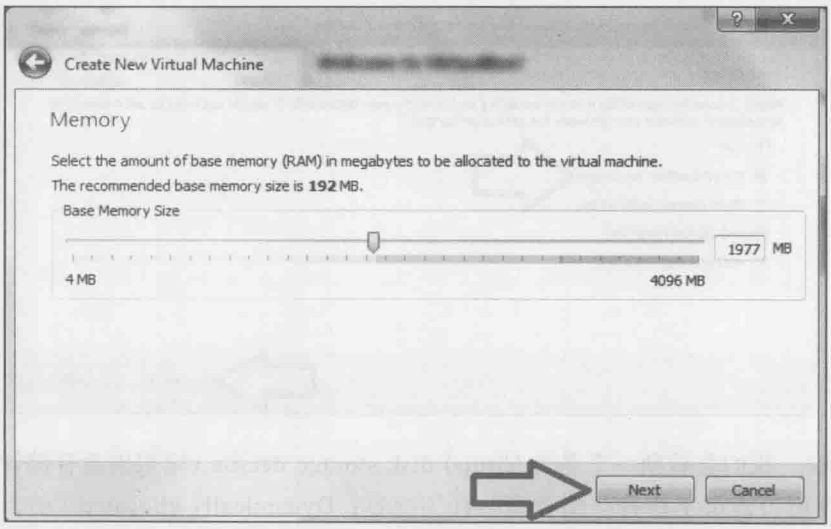
现在，开始在 VirtualBox 上安装 Windows XP SP2。执行步骤如下。

1）首先，启动 VirtualBox，单击 New 按钮。

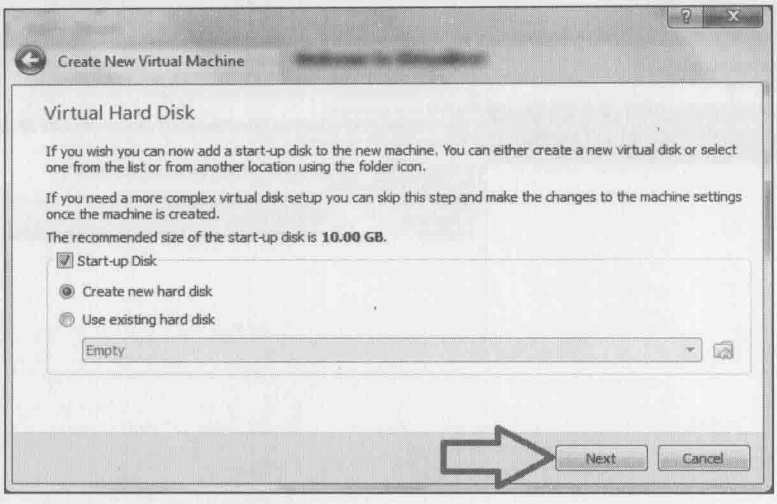


2）这时，弹出一个带有 Welcome to the New Virtual Machine Wizard（欢迎使用新建虚拟机向导）消息的窗口，单击该窗口中的 Next 按钮。

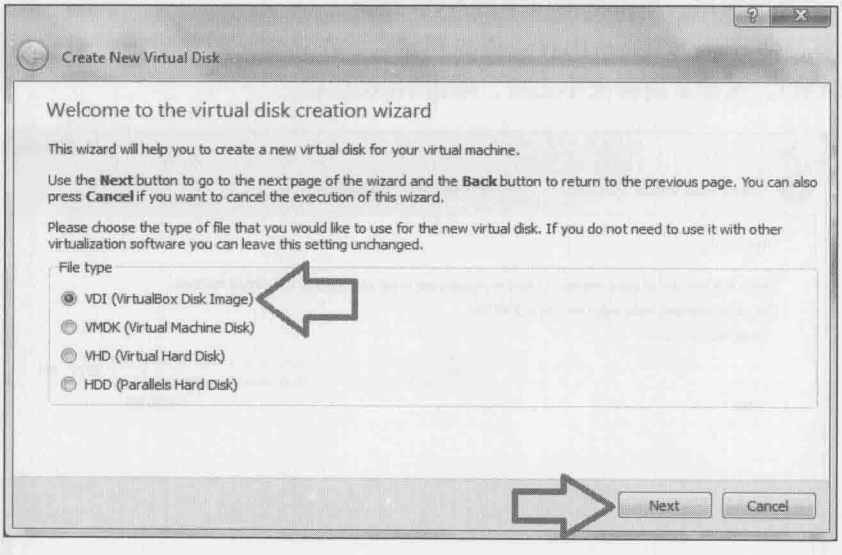
3）接着，会打开一个显示内存选项的新窗口，在这里，要指定虚拟机使用的基本的内存大小（RAM）。选择了内存大小之后，单击 Next 按钮。



4）接下来，弹出一个新窗口，用于创建虚拟磁盘。选择 Create new hard disk（创建新硬盘）选项，然后单击 Next 按钮。



5）这时，弹出一个新窗口，其消息为 Welcome to the virtual disk creation wizard（欢迎使用虚拟磁盘创建向导）。该窗口提供了几项硬盘文件类型选项，我们选择 VDI（VirtualBox Disk Image）选项；也可以选择其他选项，但是 VDI 的性能最佳，推荐选用。完成文件类型选择之后，单击 Next 按钮。



6）这时，我们会看到一个名为 Virtual disk storage details（虚拟磁盘存储详细信息）的新窗口。该窗口提供了两种存储类型的详细内容：Dynamically allocated（动态分配）以及