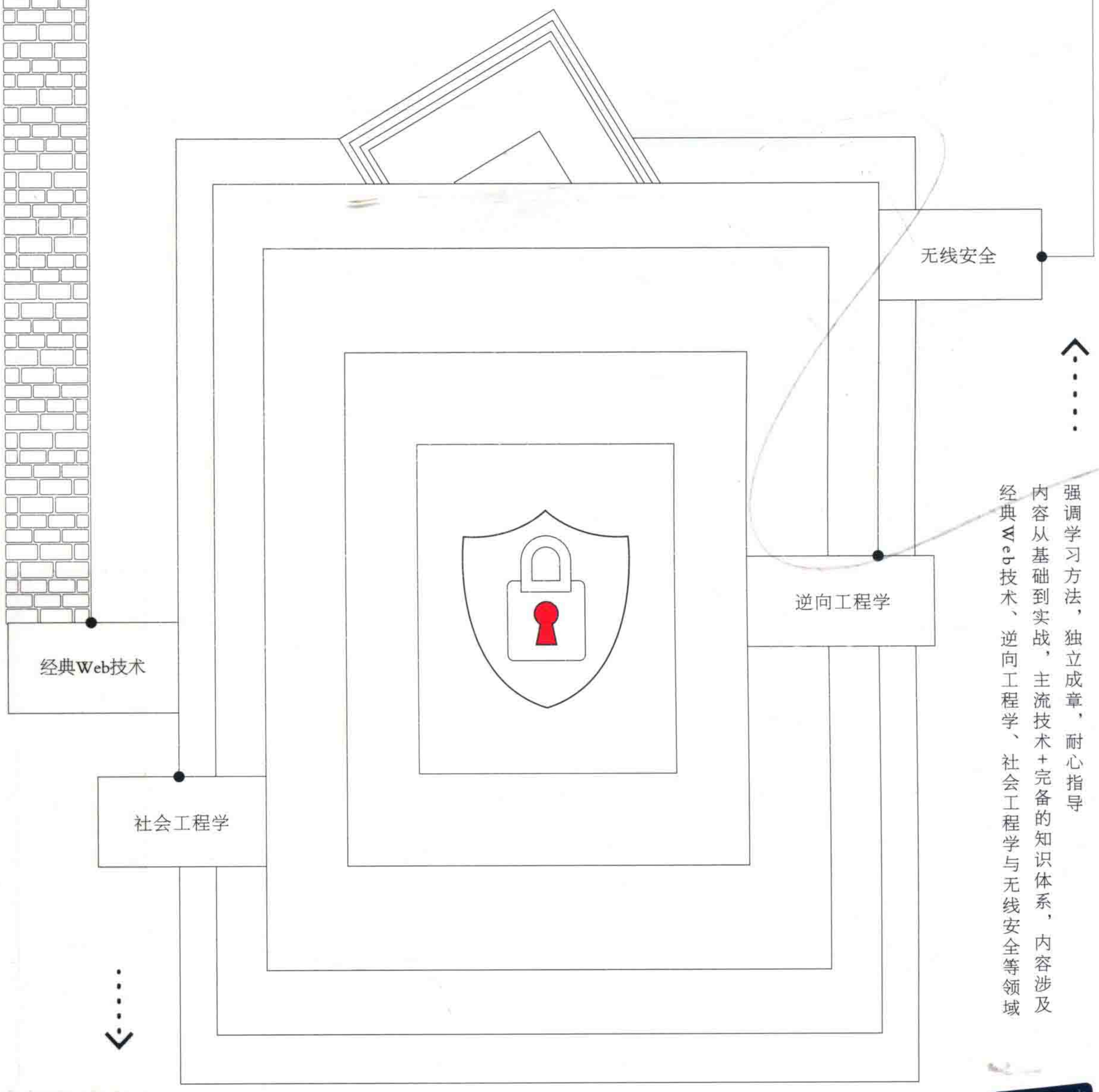
信息安全围绕攻防展开，解读黑客技术，梳理知识脉络，
助力读者成为有技术能力的安全人员

黑客与安全技术指南

王 成 编著

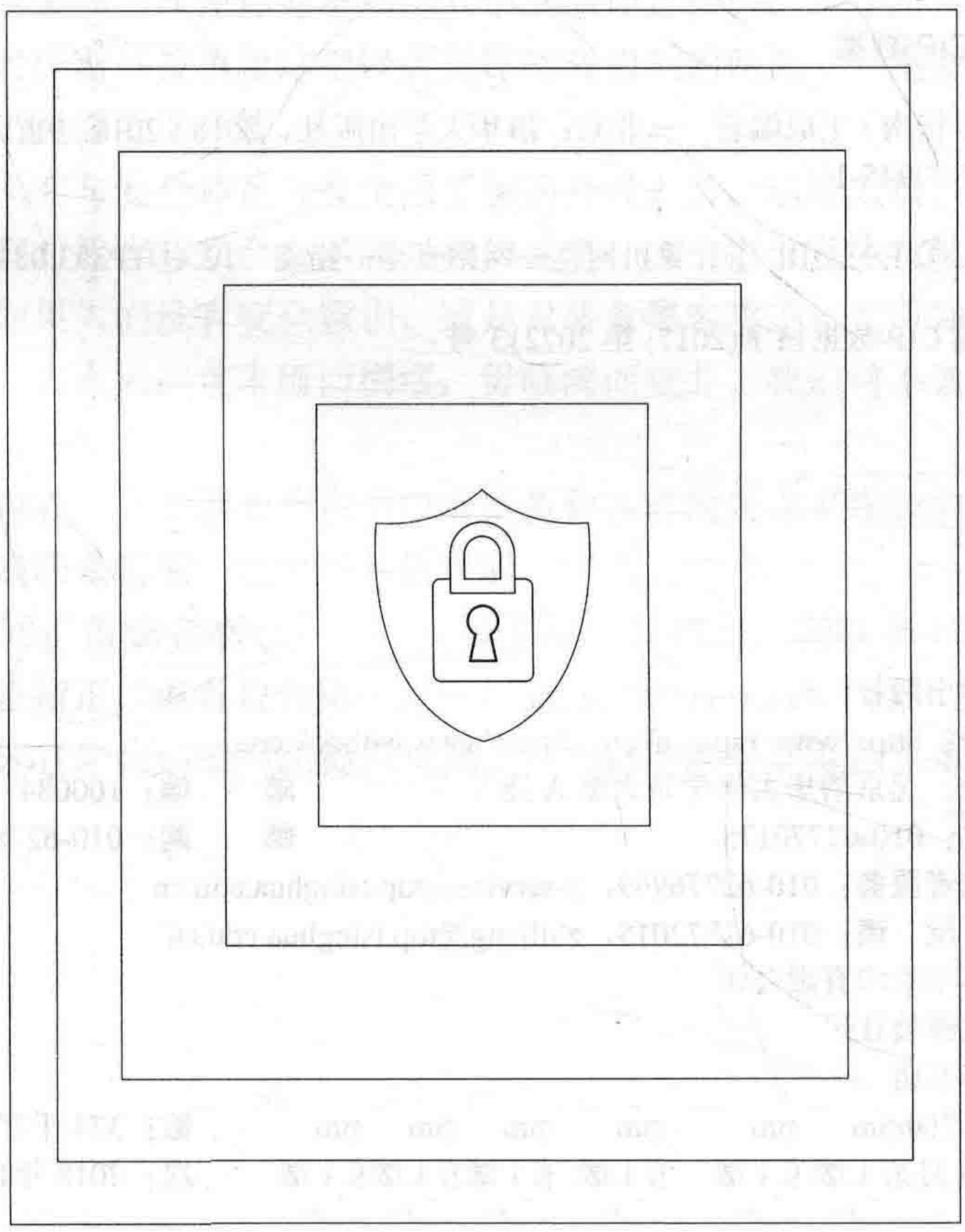


强调学习方法，独立成章，耐心指导
内容从基础到实战，主流技术+完备的知识体系，内容涉及
经典Web技术、逆向工程学、社会工程学与无线安全等领域

清華大學出版社

黑客与安全技术指南

王 成 编著



清華大學出版社
北 京

内 容 简 介

这是一本专门介绍并分享黑客与安全技术的入门书，内容从基础知识出发，通过相关实例为读者剖析计算机安全领域的各种技巧。

全书由 10 章组成，第 1 章主要介绍了一些经典、高效的学习方法与基本技能；第 2 章浅析了当今相关技术的现状与基本概念；第 3 章讲解通过 Web 渗透测试来模拟恶意黑客的攻击行为，借此讲解评估计算机网络系统的安全性的方法；第 4 章讲解比一般的黑盒渗透测试更直观、全面的代码审计的方法与相关知识；第 5 章从基础原理开始，详细介绍了无线安全的各种应用；第 6 章从 HTML 基础开始，详细分析了 XSS 等前端漏洞的成因、危害以及防御措施；第 7 章深入浅出地探讨了社会工程学这朵黑客与安全技术中的“奇葩”；第 8 章通过对多种相关调试工具的使用和实例分析，讲解逆向技术与软件安全的相关知识；第 9 章通过对各种病毒的调试分析，帮助读者了解并掌握病毒攻防技术及相关知识；第 10 章介绍了安全领域的一项竞赛——CTF。本书各章都有相应的练习环节，读者可以亲自动手，以便更好地理解相关知识及掌握相关技能。

本书适用于想了解黑客与安全技术的开发人员、运维人员以及对相关技术感兴趣的读者。

图书在版编目(CIP)数据

黑客与安全技术指南 / 王成编著. — 北京：清华大学出版社，2018（2018.10重印）
ISBN 978-7-302-47945-1

Ⅰ. ①黑… Ⅱ. ①王… Ⅲ. ①计算机网络—网络安全—指南 Ⅳ. ①TP393.08-62

中国版本图书馆 CIP 数据核字(2017) 第 207213 号

责任编辑： 杨如林
封面设计： 杨玉兰
责任校对： 徐俊伟
责任印制： 宋 林

出版发行： 清华大学出版社
网 址： http://www.tup.com.cn，http://www.wqbook.com
地 址： 北京清华大学学研大厦 A 座 **邮 编：** 100084
社 总 机： 010-62770175 **邮 购：** 010-62786544
投稿与读者服务： 010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈： 010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者： 北京鑫丰华彩印有限公司
装 订 者： 三河市溧源装订厂
经 销： 全国新华书店
开 本： 185mm×260mm **印 张：** 16.5 **字 数：** 374 千字
版 次： 2018 年 8 月第 1 版 **印 次：** 2018 年10月第 2 次印刷
定 价： 49.00 元

产品编号：065791-01

编 者 序

由于科技不断发展，科技黑箱（一种特殊的存储、传播和交流知识的设施）的出现也给计算机发展带来了巨大的进步，人们无须掌握全部知识，只须按照步骤去学习和操作，便可得到预期的结果——即便你并不知道其中的原理是什么。这在黑客与安全方面的体现主要有两点，正对应着科技黑箱这把锋利无比的双刃剑的两面：一是安全技术进步迅速；二是恶意黑客攻击变得更加频繁。

本书面向对黑客与安全体系没有全面了解的开发人员、运维人员、计算机相关专业在校学生，以及所有对黑客与安全技术感兴趣的读者。安全事件发生在转瞬之间，可能与每个人息息相关。如果人们没有安全意识，或是对恶意黑客攻击一无所知，那么面对攻击，只剩下不知所措。古人云：宜未雨而绸缪，毋临渴而掘井。我们何不通过研究黑客攻击的手段寻找防御的方法呢？

本书的重点内容，在于读者将在书中看到各种各样的攻击手段和防御措施，编者尽可能地将理论和实践联系起来，以便于各位理解。

由于成书时间正值编者高三复习，受限于阅历和精力，所以书中难免出现不严谨之处，还请读者不吝指正，编者也会第一时间在https:// mapers.net/上进行勘误。

同时也欢迎读者来我们的网站提问交流，我们将不断更新原创文章，与你一起讨论安全热点。

前　言

“时维九月，序属三秋”。傍晚，夜色如酒，天气微凉，阴雨和乌云笼罩的天空，没有雷鸣轰动、一扫阴霾的气势，仿佛静静地诉说着积蓄已久的孤独。

这份神秘的气息，大概如同多数人对于黑客的认识—— 暗淡的灯光下，一个背影，一袭黑衣，盯着屏幕上闪烁的数据流，嘴角挂着玩世不恭的微笑，轻描淡写地入侵着一个个网站，在网络世界中肆无忌惮地破坏着。

但实际上，黑客真的如同电影中描绘的与人们想象中的那样吗？

这里我要给出否定的答案。黑客无处不在，黑客之所以如此神秘，最大的原因是人们给“黑客”这个词语，以及一切与黑客相关的事物，蒙上了一层神秘的面纱。

那么，到底什么才是黑客？

“黑客”这个词，其实最初曾指热衷于计算机技术、水平高超的计算机专家，尤其是程序设计人员。现在，黑客们活跃在安全领域的一线，依靠着敏锐的感知，发掘、研究并修复各种漏洞。甚至可以这样说：没有黑客，计算机安全将无法进步。黑客其实并不神秘，也并不可怕。你想了解黑客吗？想通过学习黑客与安全知识，去化解来自计算机的恶意攻击吗？那么，本书值得一读。在这条路上你也许会遇到很多在电影中才遇到过的场景和人物，可无论走得多远，也请务必记住：心存敬畏，莫生邪念。引用谷歌公司一句不成文的口号就是：Don’t be Evil。

黑客与安全的世界广阔无边，本书涵盖的内容只是沧海一粟，我们试图用最典型的技术和最精炼的语言，向读者朋友们呈现一个精彩的、属于黑客的神秘技术世界。

我们不会把“以提高计算机领域安全水平为目标”这样空洞的口号挂在嘴边，学习也并不是靠嘴说说就行。我们要做的，就是影响正在认真阅读本书的读者，传达正确的观念、知识以及学习方法，让读者更深刻地了解黑客，学习安全技术，通过钻研黑客与安全技术，从而在计算机世界中更好地保护自己。

本书共10章，各个章节独立却又相互关联，知识点之间也有相互影响的地方，虽然每章之间的关联性不是那么强，不过在内容安排上是按照由浅入深设计。作为一本黑客与安全技术的启蒙书，我们尽量照顾初学者，但仍然有很多基础知识需要新手朋友们自己去钻研，毕竟，自己“折腾”的过程也是相当重要的，不是吗?

由于信息技术的更新迭代速度十分惊人，时效性较强，所以我们拟建mapers.net社区以供读者朋友们交流，希望可以在计算机安全的道路上助读者一臂之力。

■ 本书适合的人：

- 认真的人；
- 愿意花时间钻研知识而不是沉迷于游戏的人；
- 善于遇到问题先独立寻找答案的人。

■ 与本书无缘的人：

- 浮躁的人；
- 希望速成的人；
- 仅仅是觉得黑客很酷而决定学习黑客技术的人；
- 抱着不良目的的人。

■ 致谢

首先感谢在计算机黑客与安全领域不断钻研的前辈们，给我们留下了丰富的学习资源，让我们得以站在巨人的肩膀上，向更远的未来眺望。

感谢清华大学出版社编辑老师们对本书做出的贡献，他们认真地审读和修改，保证了本书的质量，也感谢他们对我的耐心指导。

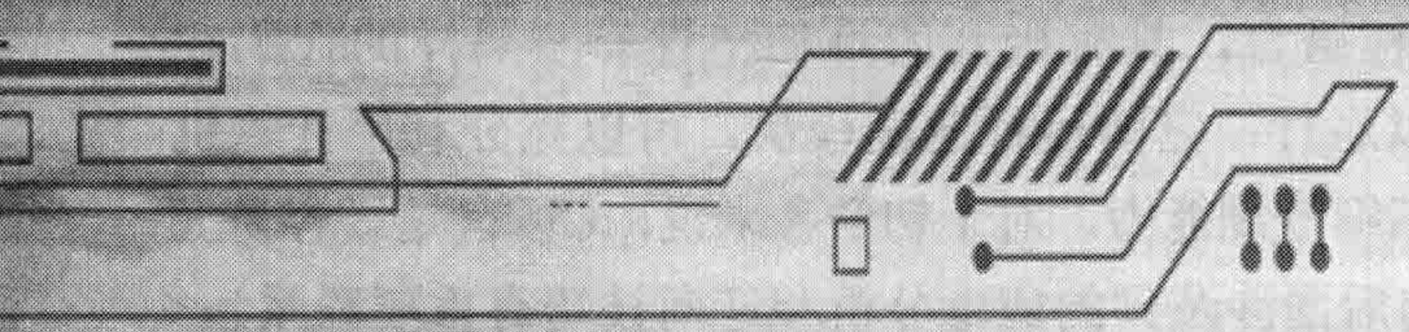
感谢参与本书编写和为本书出谋划策的朋友们，他们是陈梓涵、田健、周慧娴、孟爻、K0sh1、白三、Ricky。

感谢 D3AdCa7 在CTF知识方面给予笔者的建议，让笔者这个CTF新手也能“装模作样”地写出一点东西；感谢病毒吧@王And木提供“病毒不神秘”章节中几例病毒样本及分析过来，使得本书在病毒方面的知识更加详尽。

最后要感谢我的亲人和老师，可能我不是一个传统意义上的好孩子，为了自己的梦想而忽视了你们的感受，特别是我的父母，实在很抱歉，希望你们能慢慢理解儿子的执着，期待着你们支持我的那一天，我爱你们。

王　成

目　录



第 1 章

高效学习之道——方法态度经验总结

本章作为全书第1章，将会介绍一些基础知识和经典的学习方法。方法与技能有无数种，希望读者朋友们能增强独立思考能力，自己总结规律，在互联网上寻找书中没有提到的知识，这样才能更好地掌握知识技能。

1.1 基本技能

1.1.1 编程基础

编程在计算机领域称得上是必备技能了，在此我们不再探讨各种语言的优缺点，也不介绍类似“‘面向对象’和‘面向过程’之间区别”的问题，更不会空谈编译原理等问题，这里将简单介绍一些适合新手入门学习的编程语言以及书中涉及的各种技术所需的编程语言。

1. Python

Python是一种解释性脚本语言，它拥有众多的“库”。Python功能强大而且简洁，还可以将其他语言的模块轻松联结起来，故又被称为“胶水语言”。由于Python需要的代码量极少且易于学习，其程序源代码对于使用者完全开放，在开源软件工作者和编程初学者中具有极好的声誉。学习Python对人们日后的网络编程学习，以及Web渗透中部分工具的使用具有重要意义。

目前Python主要分为2.x与3.x两个版本，两者在语法上略有差异，且各有优缺点，大家可以根据自己的需求学习不同的版本。

2. C语言

C语言是一种极其重要和流行的编程语言，具有极高的可移植性——同样的代码在Linux、Windows、Mac OS系统上都可以运行；它的运行速度极快，可以充分利用计算机的优点，表现出只有汇编语言才具有的精细控制能力。对于初学者来说，C语言是最容易上手的一门“大型”编程语言，C语言也与后面涉及到的病毒分析和逆向技巧有重要联系。

3. 汇编语言

汇编语言是计算机的底层语言，大部分计算机的汇编语言基于X86指令集，计算机可通过汇编程序将汇编代码转化为机器码——计算机可以直接执行的代码。汇编可以使人们更清晰地了解计算机的运行原理，同时也对在接下来的章节中要中学习的软件漏洞分析、逆向分析以及病毒机制的理解具有重要意义。

4. JavaScript

JavaScript是一种脚本语言，在Web前端中担任着重要的角色，但它也是造成XSS（跨

站脚本攻击）、CSRF等漏洞的罪魁祸首之一，所以说JavaScript是学习渗透测试和前端安全的一门必修课。

1.1.2　命令提示符

命令提示符在许多人印象里就是一个“黑洞洞的窗口”（其实cmd窗口也是可以美化的，例如图1-1被笔者设置成透明色，毕竟如果长时间使用终端工作，一个赏心悦目的界面还是很有必要的）。在Windows系统中，按Win＋R键，输入cmd并回车，就可以调出cmd窗口。

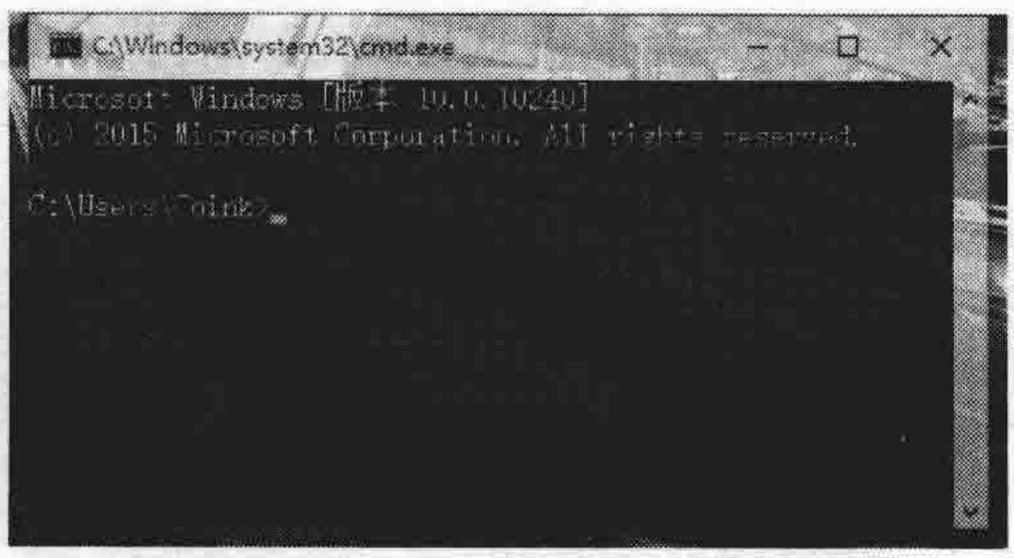


图1-1　笔者的cmd命令提示符界面

许多应用在命令提示符窗口进行操作会更加简洁，比如输入Python可以启动Python解释器（前提是已搭建了Python环境），学会命令提示符的常用用法和语法后，可以写出批处理（*.bat）文件，来进行许多原始而又简单的操作。

类似地，Linux系统的Shell则是Linux的命令提示符，称为命令行，一般以终端方式打开。俗话说尺有所短，寸有所长，Linux的图形化界面虽然没有Windows易用，但是它在命令行方面比Windows更加成熟，读者可以尝试Linux的一些发行版，例如Ubuntu、Debian等，熟悉Linux系统对于提升工作效率是大有裨益的。

1.1.3　虚拟专用网络

虚拟专用网络，这个名词可能令部分读者感到些许陌生，但它的英文名称读者一定听过，Virtual Private Network，即VPN。VPN能够让其他人连接到企业网络或内部网络，通过一个公用网络建立一个临时的、安全的连接，这是一条穿过混乱的公用网络的安全、稳定的隧道。同时VPN能提供高水平的安全性，使用高级的加密和身份识别协议保护数据，阻止没有被授权的用户接触数据。而在渗透测试中，使用VPN则可以进入一些无法正常访问的网络环境，从而进一步开展渗透测试。

1.1.4　虚拟机

虚拟机（Virtual Machine）指通过软件模拟具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。

简单来说，虚拟机就是操作系统中的一个沙盒，在沙盒之中执行操作的时候主系统是不会干扰到外部系统的，可以说是安全测试中必不可少的工具。

从20世纪五六十年代IBM提出虚拟机技术开始，虚拟机技术随着互联网的发展，日益成熟。目前，比较流行的虚拟机软件有VMware、VirtualBox和Virtual PC，它们都能在Windows系统中虚拟出多个计算机系统。当需要在其他系统环境测试软件或以另一个系统作靶机来测试某漏洞时，则可以在自己的同一台计算机上安装两个或多个操作系统，例如可以同时安装Linux与Windows操作系统，并且在虚拟机与物理机之间共享文件、应用程序及网络资源等，这将极大地提高工作效率。

接下来，我们以VirtualBox软件为例来介绍一下虚拟机的安装方法。

VirtualBox是一款常用的开源的虚拟机软件，它具有操作简便、界面简洁等很多优点。图1-2是在Windows 环境下运行VirtualBox的界面。

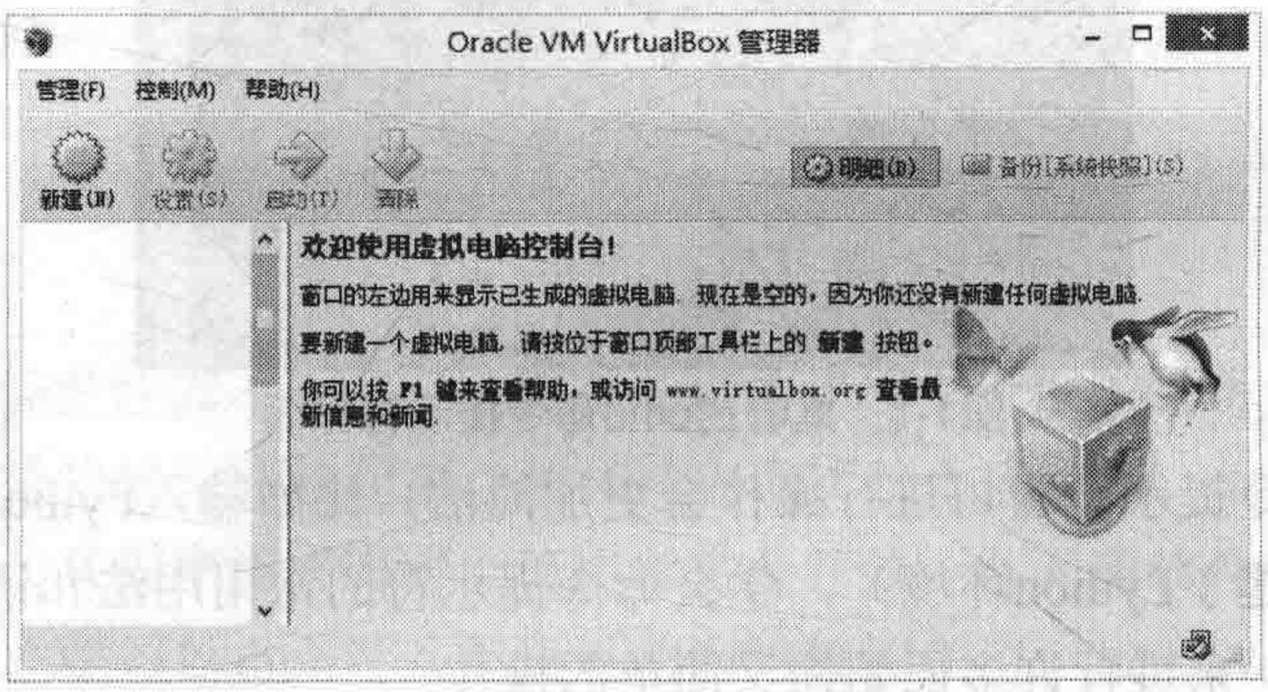


图1-2　VirtualBox主界面

单击“新建”按钮，会弹出如图1-3所示的界面，这里需要键入虚拟机的名称以及选择所安装系统的类型和版本。

之后，单击“下一步”按钮进入内存分配界面，如图1-4所示。在安装每一个虚拟系统的时候，都要为其分配相应大小的内存，这些内存用以支持虚拟系统的运行及虚拟系统中程序的运行。

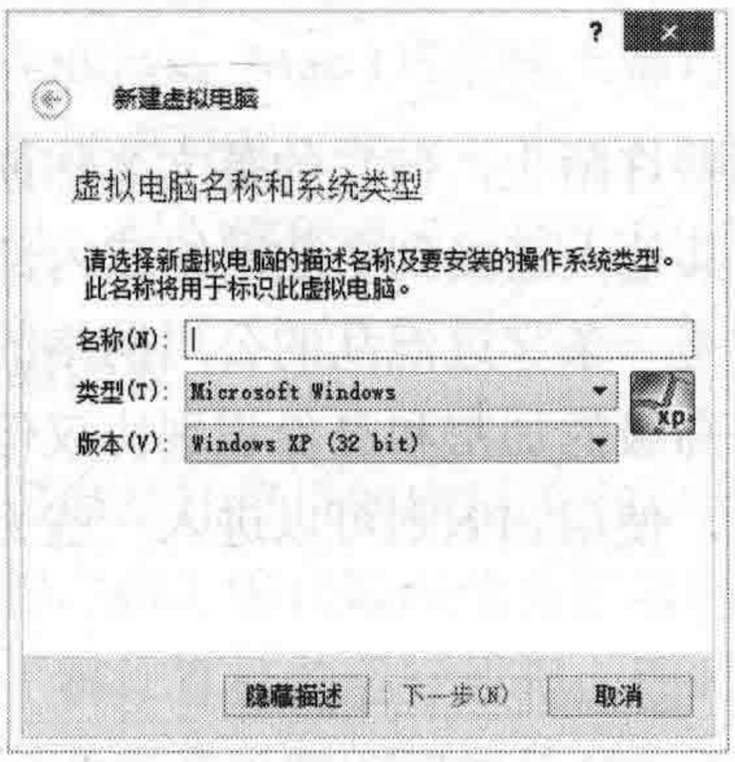


图1-3　为虚拟机命名并选择镜像的系统类型与版本

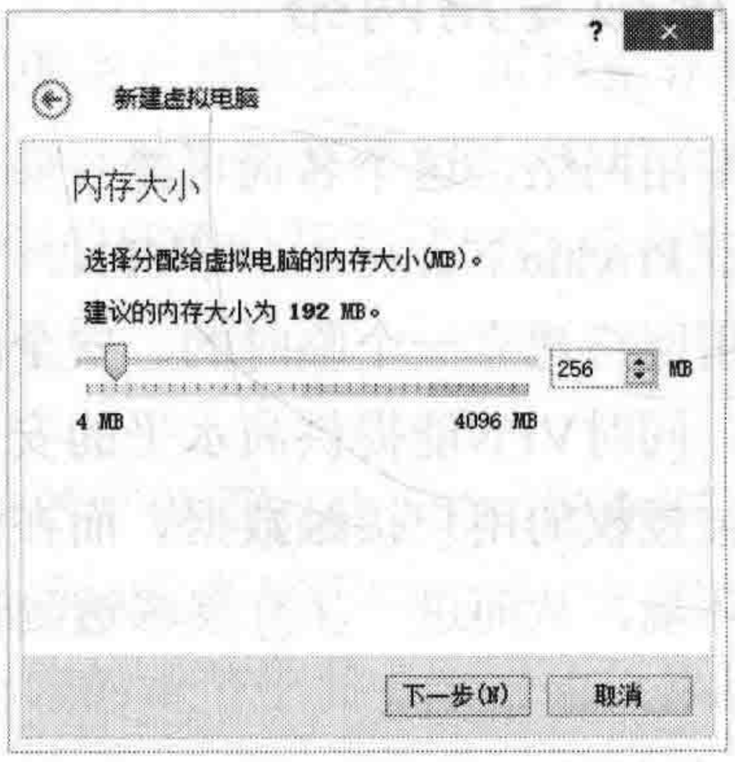


图1-4　为虚拟机分配内存

虚拟机系统为Windows XP时，为其分配256M的运行内存足够支持虚拟机中的常用操作。当然，所能分配的最大内存不能超过物理机内存的剩余部分，毕竟虚拟机内存是无法凭空虚拟的。

除了分配内存，还要给虚拟系统分配硬盘。硬盘是一个载体，如同主系统安装在主机的硬盘上一样，我们要给所安装的虚拟系统分配一块虚拟硬盘。分配硬盘有两种方式，一种是固定大小，另一种是动态分配，如图1-5所示。

顾名思义，动态分布模式下，给虚拟系统分配的硬盘空间会随着虚拟系统的增大而增大，在该模式下，新建硬盘很快，而且不需要消耗太大空间，分配给虚拟系统的硬盘大小会随着逐渐使用而增加。

而固定大小模式，则是为虚拟系统分配固定的空间，在空间足够时，虚拟系统可以流畅地运行，如果虚拟系统所占的空间大于或等于所分配的硬盘内存，则会出现错误。如图1-6所示，VirtualBox软件会根据所选择的系统类型默认一个硬盘大小，可供参考。

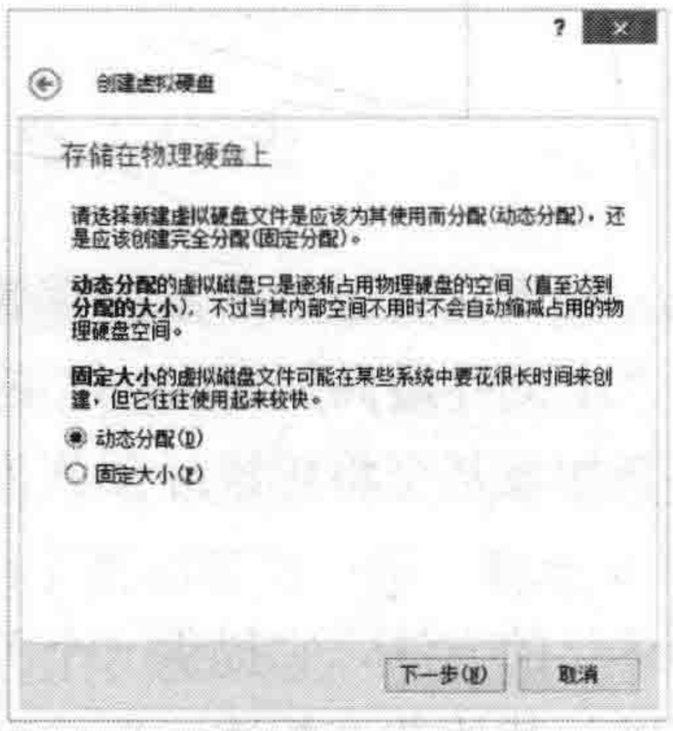


图1-5　为虚拟机设置虚拟硬盘类型

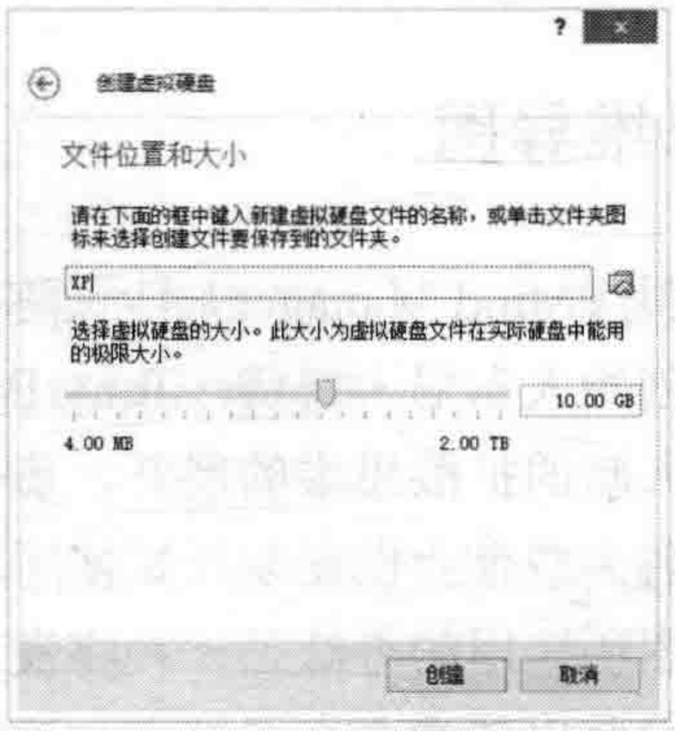


图1-6　为虚拟硬盘命名并分配大小

单击“创建”按钮，我们可以看到创建过程，如图1-7所示。

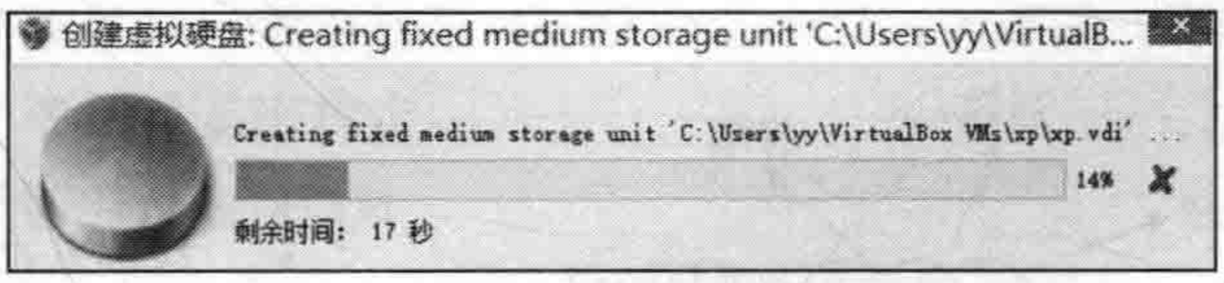


图1-7　创建虚拟硬盘

至此，我们的虚拟硬盘就建立完毕了。之后在VirtualBox的主界面可以看到左侧的管理列表出现了刚刚创建的虚拟系统。单击选中左侧的系统，单击启动栏上的“启动”按钮，便可以进入创建的虚拟系统中，如图1-8所示。

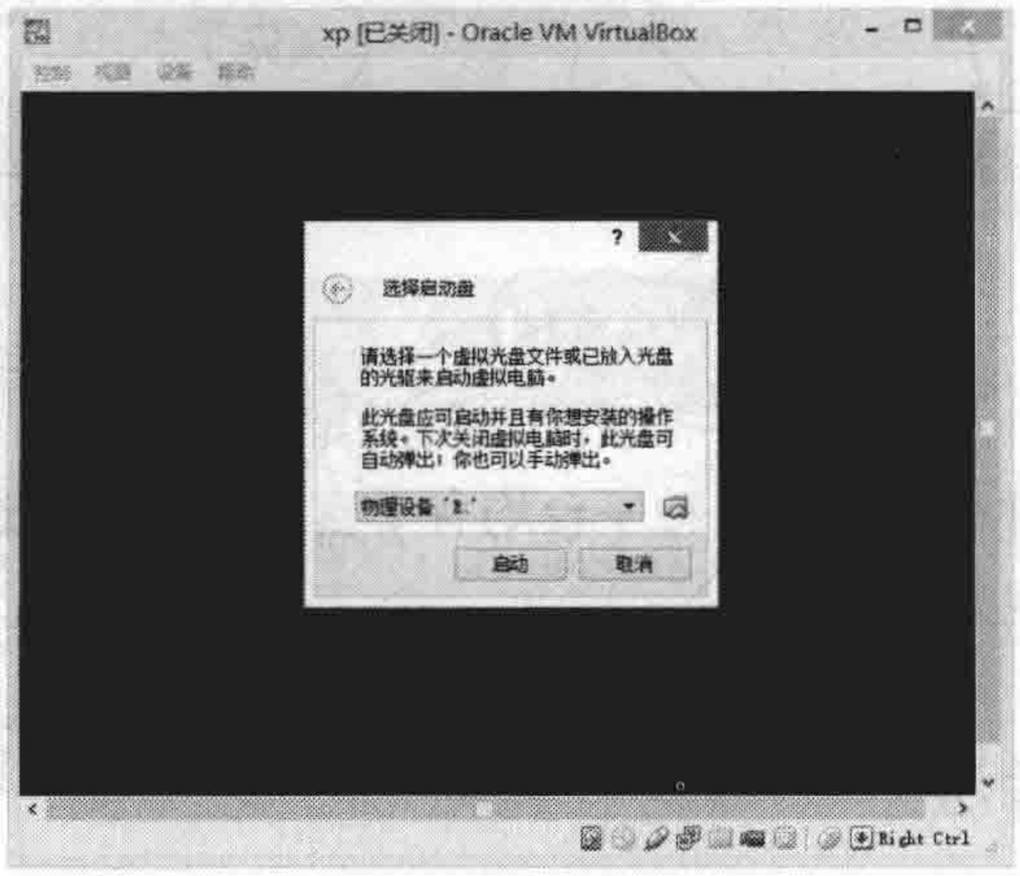


图1-8　开启虚拟机