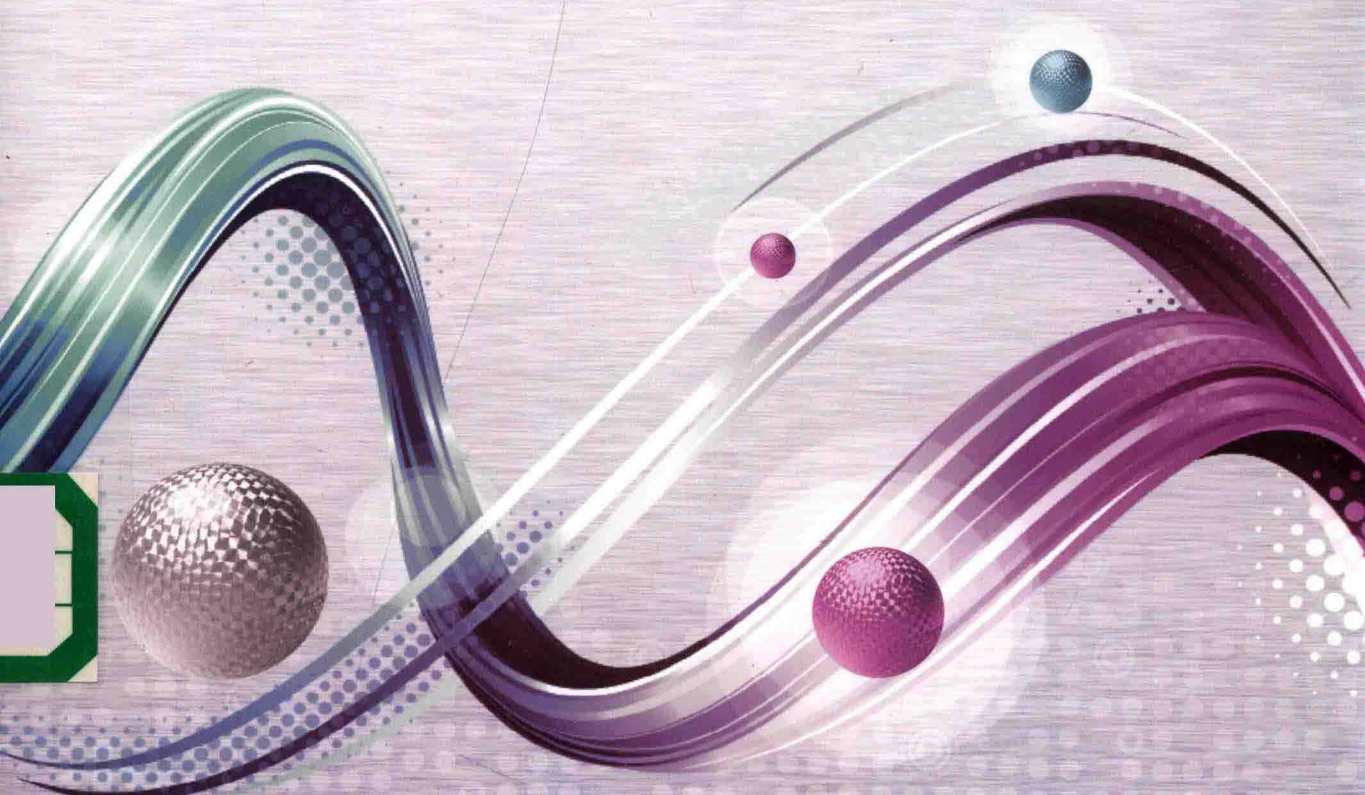
信息类“十三五”规划教材

信息安全工程技术人才培养系列教材

计算机网络安全防护技术

秦 燊　劳翠金　程 钢　编著



西安电子科技大学出版社
http://www.xduph.com

高等学校电子信息类“十三五”规划教材

应用型网络与信息安全工程技术人才培养系列教材

计算机网络安全防护技术

秦 燊　劳翠金　程 钢　编著

西安电子科技大学出版社

内 容 简 介

本书主要介绍计算机网络安全防护技术，涉及丰富的计算机网络安全软、硬件知识。全书共 7 章，主要内容包括网络安全简介、VMware Workstation 和 EVE-NG 实验环境的搭建与应用，以及防火墙技术、数据加密技术、虚拟专用网技术、局域网安全技术、网络安全渗透测试技术、Web 安全技术等。本书涉及面广，技术新，实用性强，所有知识点均配有实验支持环节，使读者能理论结合实践，获得知识的同时掌握技能。本书的案例设计均采用 EVE-NG 技术构建的实验环境，使全书的实验能在一台电脑上仿真出来。

本书可作为应用型本科和高职高专计算机及相关专业的教材，也可作为广大网络安全爱好者的参考书或培训教材。

图书在版编目(CIP)数据

计算机网络安全防护护技术 / 秦燊，劳翠金，程钢编著. —西安：西安电子科技大学出版社，2019.3

ISBN 978-7-5606-5298-6

Ⅰ. ① 计… Ⅱ. ① 秦… ② 劳… ③ 程… Ⅲ. ① 计算机网络—安全技术 Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字(2019)第 060105 号

策划编辑　李惠萍

责任编辑　李惠萍

出版发行　西安电子科技大学出版社(西安市太白南路 2 号)

电　　话　(029)88242885　88201467　　邮　　编　710071

网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com

经　　销　新华书店

印刷单位　陕西日报社

版　　次　2019 年 4 月第 1 版　　2019 年 4 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　印　张　18.5

字　　数　438 千字

印　　数　1～3000 册

定　　价　43.00 元

ISBN 978-7-5606-5298-6/TP

XDUP 5600001-1

前　言

计算机网络安全防护涉及计算机网络的硬件安全、软件安全、局域网安全、广域网安全等方方面面。要学习计算机网络安全防护的相关知识、实施相关实验，就需要架设出小型局域网、大型广域网的硬件环境，并配备 Windows 服务器靶机、Linux 服务器靶机、Web 服务器靶机等被攻击对象的软件环境，以及对这些靶机实施网络安全渗透测试攻击的 Kali Linux 系统软件环境。在一台个人电脑上构造出这样规模的环境，在过去是不太现实的，作者运用最新的虚拟化技术，在本书第 1 章及后续章节，通过整合 VMware Workstation、EVE-NG、Kali Linux 网络安全渗透测试系统、Metasploit 网络安全渗透测试工具、Windows 服务器靶机、Linux 服务器靶机、DVWA 网站靶机，使读者在一台个人电脑上就能仿真出各种规模的计算机网络安全防护实验的实施环境。

本书的实验环境 EVE-NG 支持厂商的虚拟化产品，这些安全设备、网络设备等是由厂商采用虚拟化技术设计实现并在现实中销售与应用的虚拟化产品，并非模拟设备。将它们免费用于实验时，仅有速度上的限制，并无功能上的限制，这些虚拟化产品与真实应用能实现零差距对接。

本书基于项目导向、任务驱动的模式设计，使读者不仅能学习计算机网络安全的理论知识，更能通过动手实施，在完成任务的过程中，掌握各种网络安全防护的知识和技能，最终能综合运用和实施网络安全技术。

本书各章内容安排如下：

本书第 1 章介绍了 VMware Workstation、EVE-NG、Kali Linux 网络安全渗透测试系统，Windows 服务器的安装、克隆及使用技巧，并为读者分别设计了一个软件和一个硬件的网络安全任务。通过软件安全任务的实施，可指导读者架设网站，使用灰鸽子木马实现网页挂马，当上网者浏览该挂马网站时，电脑就毫不知情地被网站主人控制，即使上网者重启电脑，电脑仍然被控制。通过硬件安全任务的实施，可指导读者架设一个拥有路由器和交换机的硬件环境，配置路由器实现 telnet 远程网管功能，掌握抓包软件 Wireshark 的使用方法和技巧，以及利用抓包软件捕获 telnet 密码的方法。

本书第 2、3、4 章主要介绍了广域网安全的知识和安全防护技能。涉及的硬件有防火墙、路由器，软件有加密技术、公钥基础架构 PKI、虚拟专用网技术等。通过防火墙保护公司内网和 DMZ 区域的安全；通过路由器、防火墙的虚拟专用网技术实现公司总部与分部之间、出差员工和在家办公员工与公司内网之间网络的安全。

其中，第 2 章防火墙技术主要介绍了如何配置防火墙接口，为防火墙配置路由，如何通过字符界面 telnet、SSH 以及图形界面 ASDM 远程管理防火墙，如何控制内网用户对 DMZ 区域和外网的访问，如何运用防火墙防御泪滴攻击、防御 IP 分片攻击、防御死亡之 ping 攻击等，如何通过 policy-map 控制穿越防火墙的流量，指导读者完成穿越防火墙的灰

鸽子木马实验。

第 3 章是第 4 章的基础，第 3 章数据加密技术主要介绍了古典加密技术、DES 加密技术和三重 DES 加密技术、非对称加密技术 RSA、Hash 算法、HMAC 算法、数字签名、PGP 加密软件的使用、PKI 技术、SSL 应用等。第 4 章虚拟专用网技术主要介绍了通过路由器实现 IPSec、GRE Over IPSec、SVTI 等虚拟专用网，通过防火墙实现 SSL 虚拟专用网的方法，实现了总部与分部之间、出差员工和在家办公员工与公司内网之间网络的安全。

本书第 5 章介绍了局域网安全技术，主要涉及的硬件是交换机。本章介绍了 VMware Workstation 与 EVE-NG 配合使用的方法，VMware Workstation 的 NAT 使用技巧，路由器 MAC 地址、Windows 服务器 MAC 地址、Linux 服务器 MAC 地址的配置方法，MAC 地址泛洪攻击、DHCP 攻击、ARP 欺骗攻击的实施，以及通过配置交换机的 port-security 属性、使用交换机的 DHCP Snooping 技术、启用交换机的 DAI 检查实现对这些攻击的防御等。

本书第 6 章介绍了网络安全渗透测试技术，主要涉及操作系统、数据库、应用软件等软件安全。通过信息收集，了解目标相关信息；通过扫描，获取开放的主机、端口、漏洞等信息；通过 Kali Linux 网络安全渗透测试系统、Metasploit 网络安全渗透测试工具对 Windows 服务器靶机、Linux 服务器靶机进行渗透测试攻击，获取控制权、种植木马、远程操控目标，最终生成评估报告，给出技术解决方案，帮助被评估者修补和提升系统的安全性。

本书第 7 章介绍了 Web 安全技术，指导读者安装与搭建 phpStudy 实验环境、搭建和配置 Web 服务器靶机 DVWA。本章通过 php 动态网站的搭建与 MySQL 数据库的基本操作，指导读者实施 XSS 跨站脚本攻击、窃取网站用户 Cookie、篡改网站页面、SQL 注入、绕过用户名和密码认证、CSRF 漏洞攻击、篡改用户密码及防御措施等。

本书由柳州城市职业学院秦燊负责第 2 章至第 7 章的编写，劳翠金负责第 1 章的编写，长春工业大学程钢编写了书中部分程序，最后，由秦燊和劳翠金共同完成全书的审稿、定稿工作。

由于编写水平有限，书中难免有不妥之处，恳请广大读者批评指正。

作　者

2019 年 2 月

目　录

第 1 章　初识计算机网络安全

小张是计算机网络专业的毕业班学生，在校期间学习成绩优异，目前在 A 公司实习。最近，A 公司为实现企业的信息化，决定采购一批路由器、交换机和服务器，让员工可以随时进行异地访问，提高办公效率。公司让小张向售后工程师好好学习，并测试一下这些设备的性能。小张建议公司在实现企业信息化的同时，要加强网络安全建设。为了说服公司领导，小张决定用在学校学习到的知识架设一个测试网站，并在网页上挂马，证明木马的危害性；另外，再通过抓包软件抓取网络上传输的密码，证明网络安全建设的必要性。

为避免木马和病毒在现实环境中扩散，网络安全防护实验一般要在封闭的环境中进行。为此，我们采用 VMware Workstation 来仿真 Windows、Linux 等服务器和主机；采用 EVE-NG 来仿真路由器、交换机和防火墙等网络设备；将 Kali Linux 作为渗透测试的主要环境；将 phpStudy 作为 Web 网页安全的网站和数据库环境。本章主要介绍 VMware Workstation、Kali Linux 及 EVE-NG 的安装和使用方法，phpStudy 的安装和使用方法将在后继章节中介绍。

1.1　网络安全简介

计算机网络发展迅速，据中国互联网络信息中心(CNNIC)发布的中国互联网络发展状况统计报告，截至 2018 年 6 月 30 日，我国网民规模达 8.02 亿人，互联网普及率为 57.7%(如图 1-1-1 所示)。其中，手机网民规模达 7.88 亿人，网民通过手机接入互联网的比例高达 98.3%。交通、环保、金融、医疗、家电等行业与互联网融合程度加深，互联网服务呈现智慧化和精细化特点。

图 1-1-1　我国网民规模和互联网普及率

计算机网络给人们带来资源共享等便利的同时，也带来了计算机网络安全的问题。图1-1-2是从国家信息安全漏洞共享平台CNDV查询到的数据，2018年CNDV收录的漏洞达13 952个，其中高危漏洞4760个。

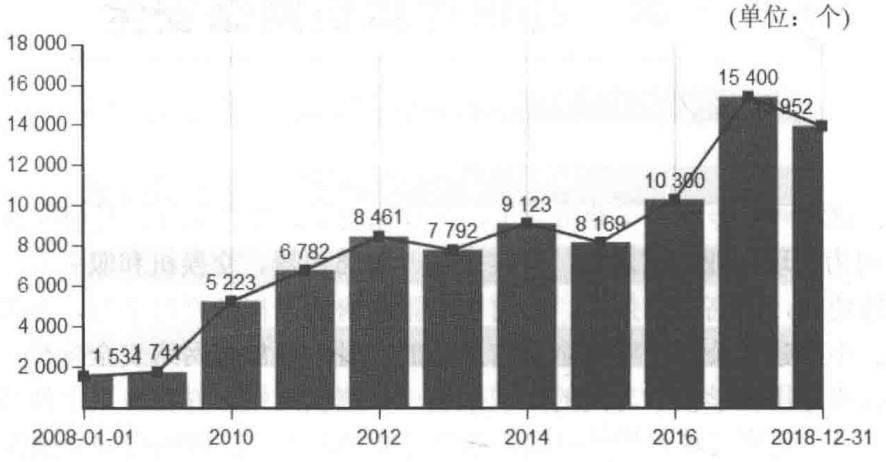


图1-1-2　国家信息安全漏洞趋势图

漏洞的存在，使计算机网络安全受到了严重威胁。2018年1月，英特尔处理器被曝出存在“Meltdown”(熔断)和“Spectre”(幽灵)两大新型漏洞，类似的，AMD和ARM处理器也存在同样的风险。漏洞是Google旗下的Project Zero团队发现的，所有1995年后发布的处理器都会受到漏洞的影响，影响面涉及手机、电脑、服务器及云计算等产品。这两大新型漏洞允许恶意程序从其他程序的内存空间中窃取信息，导致包括用户名、密码在内的一切可存储在内存中的信息都可因这两个漏洞而被窃取。

2018年3月末的清明小长假期间，黑客利用思科高危漏洞CVE-2018-0171发动的攻击，导致国内多家机构的配置文件被清洗一空，安全设备形同虚设。思科于3月28日发布安全公告指出，思科IOS和IOS-XE软件Smart Install Client存在远程代码执行漏洞CVE-2018-0171，攻击者可远程向TCP 4786端口发送恶意数据包，触发目标设备的堆栈缓冲区溢出，使攻击者无需身份验证就能远程执行任意代码，从而完全控制设备。由于该漏洞影响到底层网络设备，若被利用，将构成重大威胁。

1.2　VMware Workstation实验环境的搭建与应用

1.2.1　安装VMware Workstation

为完成网络安全的相关实验，需要多台电脑和服务器，以及不同类型的操作系统。VMware Workstation能让用户在一台真机上安装多个虚拟的操作系统，这些虚拟的操作系统与真机性能并无区别。下面以VMware Workstation 12.5.5 Pro为例，介绍软件的安装与使用方法。

1. 进入VMware Workstation Pro安装包所在位置，双击VMware Workstation Pro安装

包。如图 1-2-1 所示，点击“下一步”按钮。

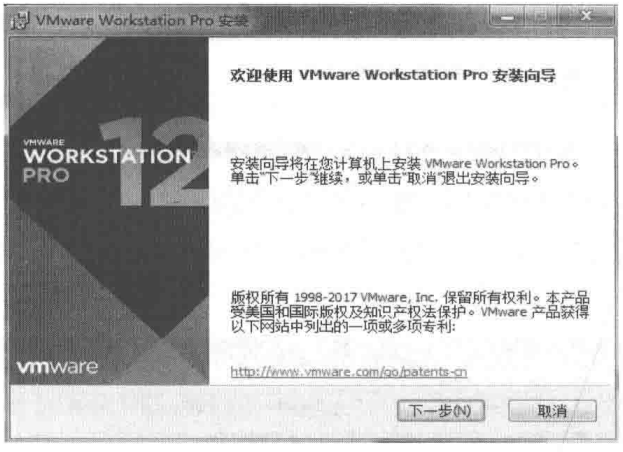


图 1-2-1　安装向导

2. 如图 1-2-2 所示，勾选“我接受许可协议中的条款”，然后一直点击“下一步”按钮。

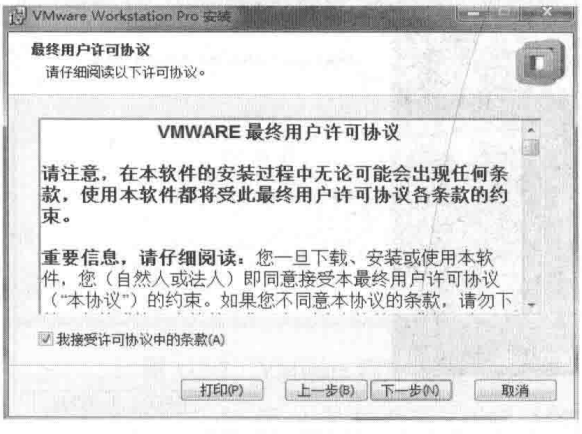


图 1-2-2　接受许可协议中的条款

3. 如图 1-2-3 所示，出现“启动时检查产品更新”选项时，取消该选项的选择(以免每次启动软件时都会联网检查更新，拖慢速度)，然后一直点击“下一步”按钮。

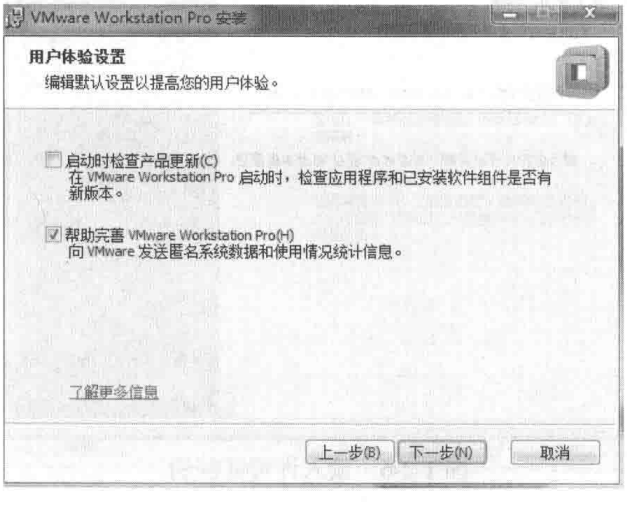


图 1-2-3　取消启动时检查产品更新

4. 如图 1-2-4 所示，出现“安装”按钮后，点击“安装”按钮。

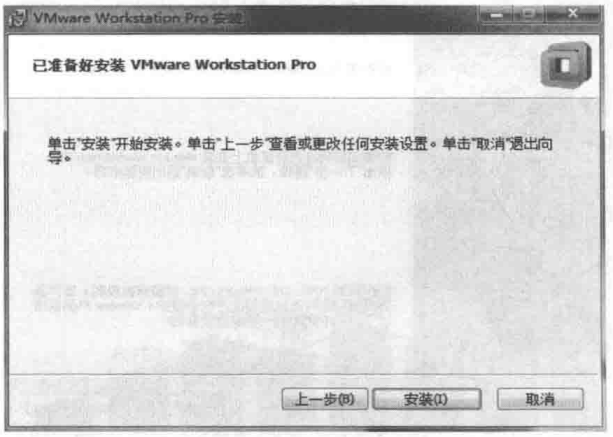


图 1-2-4　开始安装

5. 如图 1-2-5 所示，出现“许可证”按钮后，点击“许可证”按钮。

图 1-2-5　安装向导完成

6. 如图 1-2-6 所示，输入购买软件时获得的产品许可证密钥，点击“完成”按钮。

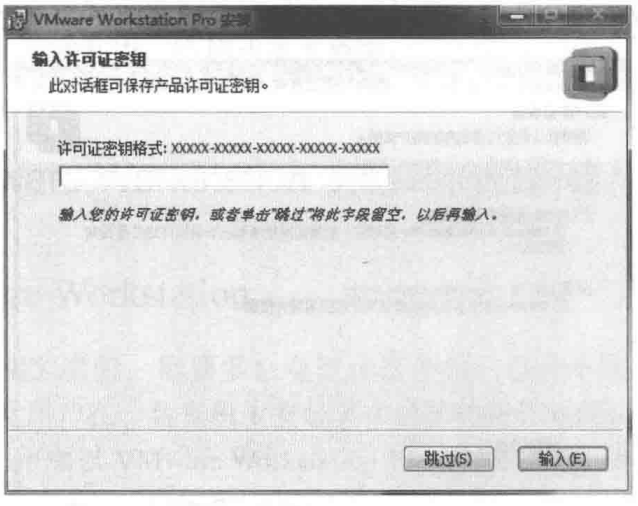


图 1-2-6　输入许可证密钥

7. 安装完成后，可以看到桌面上多了一个“VMware Workstation Pro”图标。

1.2.2　创建 Windows Server 虚拟机

VMware Workstation 安装完成后，就可以它为平台，在它的基础上安装、创建各类操作系统了。

一、使用 VMware Workstation 软件创建第一台 Windows Server 2008 虚拟机

1. 双击桌面上的“VMware Workstation Pro”图标，启动该软件。如图 1-2-7 所示，点击“创建新的虚拟机”按钮。

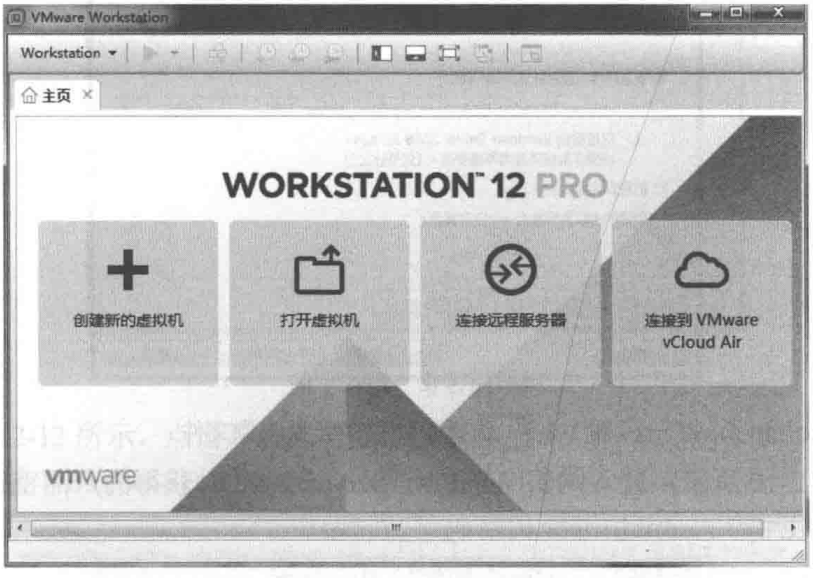


图 1-2-7　VMware 程序主页

2. 如图 1-2-8 所示，选择“典型”选项，点击“下一步”按钮。

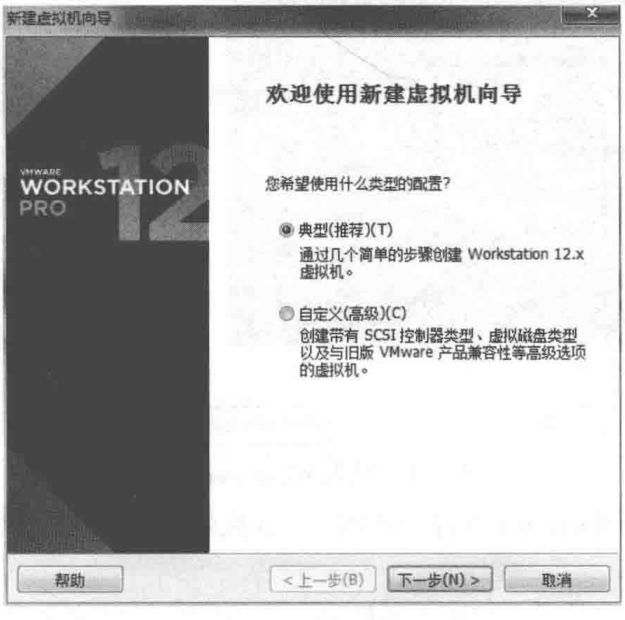


图 1-2-8　新建虚拟机向导

3. 如图 1-2-9 所示，在安装来源选项中，选择“安装程序光盘映像文件(iso)(M)”选项，并点击其后的“浏览”按钮，找到 Windows Server 2008 安装程序光盘映像文件所在位置并选中它，然后点击“下一步”按钮。

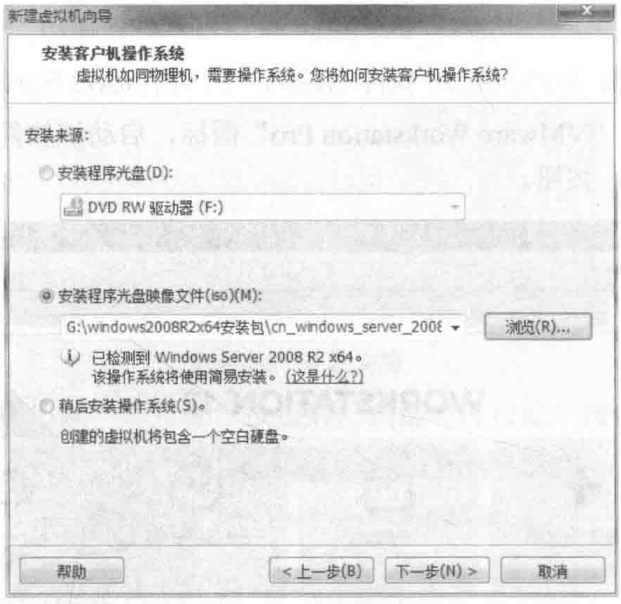


图 1-2-9　选择安装程序光盘映像文件

4. 如图 1-2-10 所示，输入购买 Windows Server 2008 时获得的产品密钥，点击“下一步”按钮。超级用户 Administrator 的密码可暂时留空。

图 1-2-10　输入 Windows 产品密钥

5. 切换到真机的 Windows 资源管理器，在真机的 D:盘新建文件夹 Win2008-1，用于存储新建的虚拟机。

6. 切换回 VMware 软件，如图 1-2-11 所示，将虚拟机名称更改为“Win2008-1”，将位置更改为“D:\win2008-1”。点击“下一步”按钮，出现指定磁盘容量，保留默认值 40 G，

点击“下一步”按钮，再点击“完成”按钮。

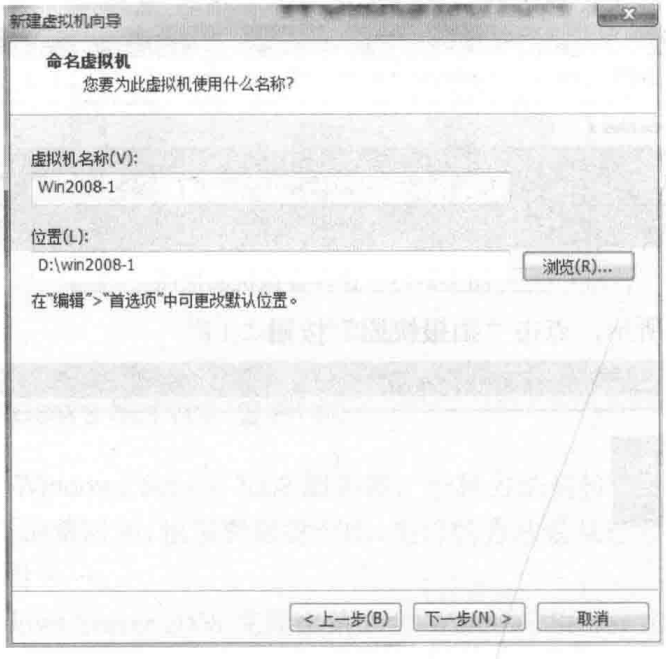


图 1-2-11　命名虚拟机

7. 如图 1-2-12 所示，点击开启此虚拟机按钮 ▶。VMware Workstation 将按刚才的配置开始自动安装 Windows Server 2008。等待一段时间后即安装成功。

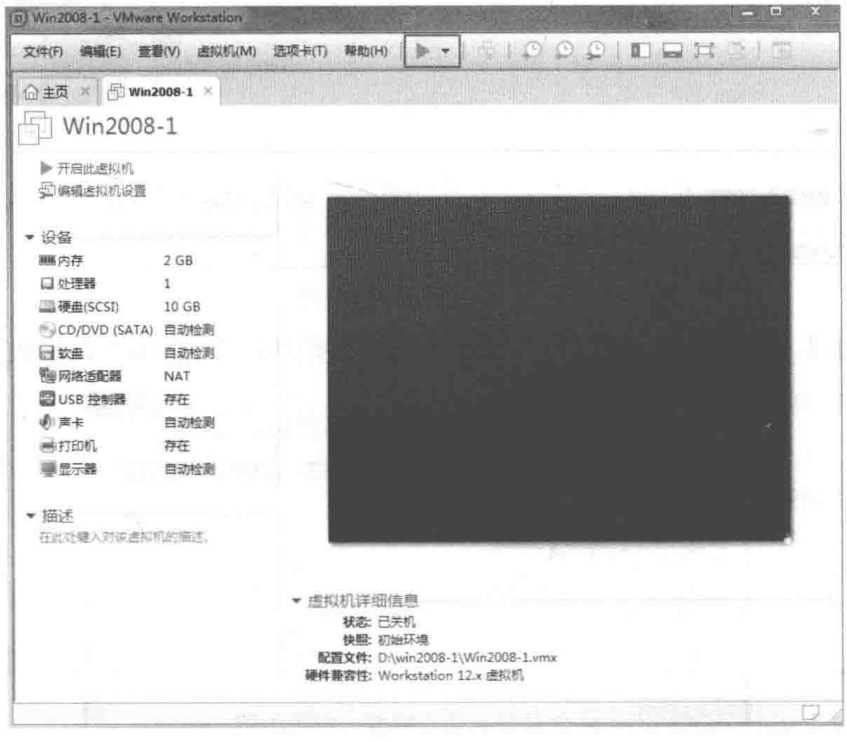


图 1-2-12　准备开始自动安装虚拟机

二、为新安装好的 Windows Server 2008 创建快照

快照很重要，因为做过某些实验后，虚拟机服务器的环境会发生变化，通过虚拟机的

快照恢复功能，可以使虚拟机服务器恢复到原始环境，避免旧实验对新实验产生不良影响。

1. 如图 1-2-13 所示，点击管理此虚拟机的快照按钮 。

图 1-2-13　管理虚拟机的快照

2. 如图 1-2-14 所示，点击“拍摄快照”按钮。

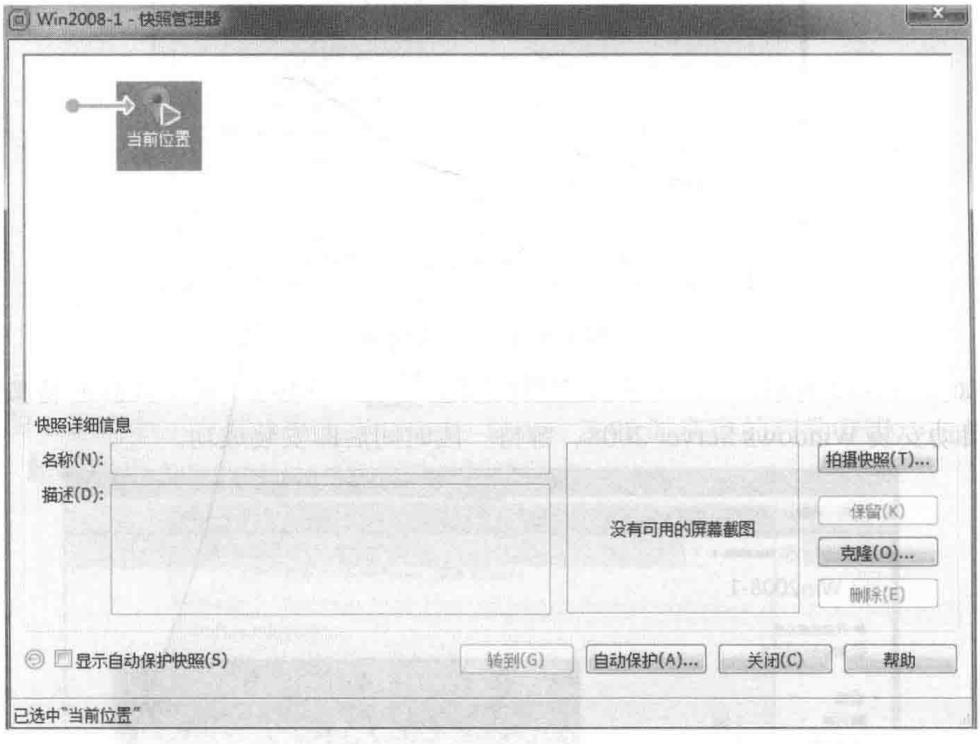


图 1-2-14　拍摄快照

3. 如图 1-2-15 所示，将快照名称重命名为“初始环境”，点击“拍摄快照”按钮。

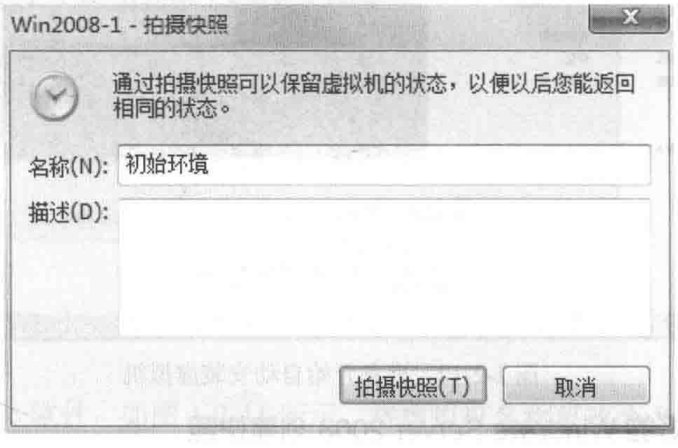


图 1-2-15　给快照命名

4. 如图 1-2-16 所示，快照拍摄成功。

图 1-2-16　快照拍摄成功

1.2.3　克隆 Windows Server 虚拟机

若要用到第二台 Windows Server 2008 服务器，一种方法是按照 1.2.2 节中的步骤再安装一次，但这种方法既浪费时间，也浪费磁盘空间。更好的方法是从已经安装好的 Win2008-1 克隆出第二台、第三台……。

用安装好的 Windows Server 2008 克隆出第二台 Windows Server 2008 的步骤如下：

1. 选择克隆的起始状态。如图 1-2-13 所示，先点击管理此虚拟机的快照按钮，然后如图 1-2-17 所示，选中“初始环境”，点击“转到”按钮。

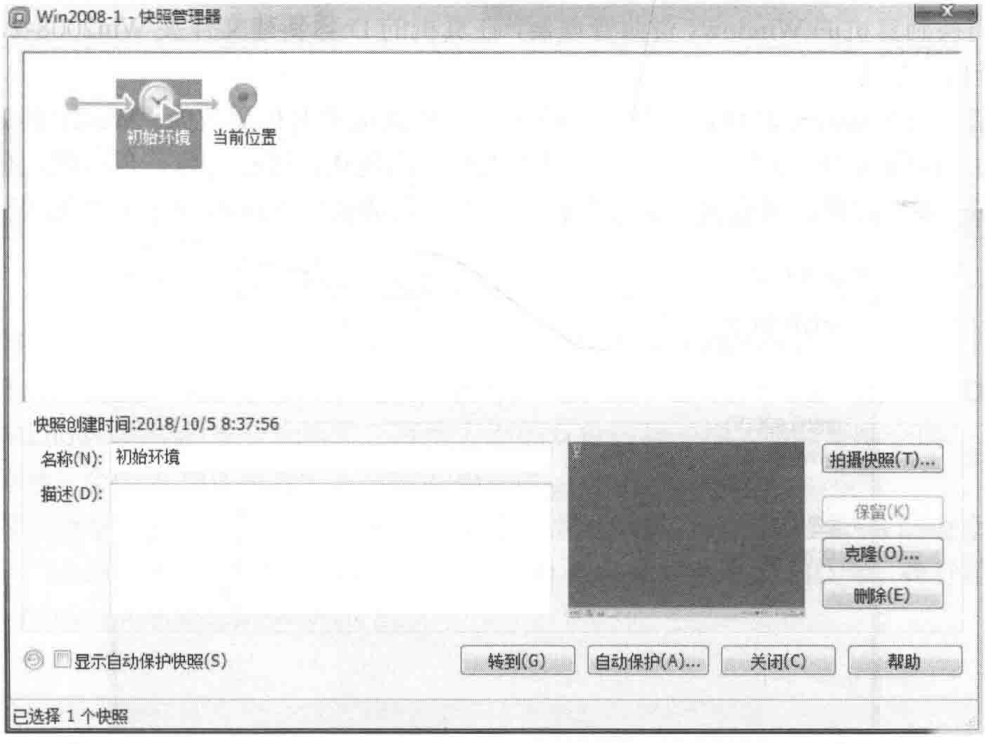


图 1-2-17　选择克隆的起始状态

2. 确保转到的状态是关机状态，如果是开机状态，则将其关机。

3. 如图 1-2-13 所示，先点击管理此虚拟机的快照按钮，然后如图 1-2-17 所示，点击“克隆”按钮，克隆源选择默认的“虚拟机中的当前状态(C)”，再点击“下一步”按钮。