第 1 章　计算机安全概述

本章学习目标

- 认识到计算机安全的重要性；
- 了解计算机系统面临的威胁；
- 了解计算机安全基本概念；
- 了解计算机安全技术体系结构。

计算机安全行业属于国家鼓励发展的高技术产业和战略性新兴产业，受到国家政策的大力扶持。国家网络安全工作要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益。要坚持网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态。没有计算机安全就没有国家安全。2011 年 5 月 25 日，解放军建立了网络蓝军。这标志着网络战已经开启并将长期持续。网络战（信息战）是为干扰、破坏敌方网络信息系统并保证己方网络信息系统正常运行而采取的一系列网络攻防行动。网络战正在成为高技术战争的一种日益重要的作战样式，它可秘密地破坏敌方的指挥控制、情报信息和防空等军用网络系统，甚至可以悄无声息地破坏、瘫痪、控制敌方的商务、政务等民用网络系统。网络战分为战略网络战和战场网络战：①战略网络战包括平时和战时两种。战略平时网络战是在双方不发生火力杀伤破坏的战争情况下，一方对另一方的金融、交通、电力等民用网络信息系统和设施，以计算机病毒和黑客等手段实施的攻击。战略战时网络战是在战争状态下，一方对另一方战略级军用和民用网络信息系统的攻击。②战场网络战旨在攻击、破坏、干扰敌军战场信息网络系统和保护己方信息网络系统。网络战是一种革命性的新型作战方式，既可实施单域作战，也可穿插于陆、海、空、天作战之中，在现代战争中的战略地位和独特作用愈加凸显。

网络攻击有可能使现代社会的机能陷入瘫痪，在现代战争中计算机安全技术已变得不可或缺。因此，美国把网络防御定位为国家安全保障上的重大课题。美国是世界上第一个提出网络战概念的国家，也是第一个将其应用于实战的国家，但美军尚未形成统一的网络战指挥体系。舆论认为，组建网络司令部，意味着美国准备加强争夺网络空间霸权的行动。网络战作为一种全新的战争样式正在走上战争舞台。组建网络司令部表明，美军研制多年的网络战手段已基本成熟，并做好了打网络战的准备。目前美军已经拥有大批网络战武器：在软件方面，已研制出 2000 多件“逻辑炸弹”等计算机病毒；在硬件方面，则研发了电磁脉冲弹、次声波武器、高功率微波武器，可对敌方网络进行物理攻击。尤其值得注意的是，美国利用其握有核心信息技术的优势，在芯片、操作系统等硬软件上预留“后门”，植入木马病毒，一旦需要即可进入对方网络系统或激活沉睡的病毒。

早在 1991 年海湾战争中，美军就对伊拉克使用了一些网络战手段。开战前，美国中

央情报局派特工秘密打入伊拉克内部，将伊军购买自法国的防空系统使用的打印机芯片，换成染有病毒的芯片，在空袭前用遥控手段激活病毒，致使伊军防空指挥中心主计算机系统程序错乱，防空计算机控制系统失灵。

2019 年 6 月 20 日，伊朗使用霍尔达特 -3 地对空导弹击落美国“全球鹰”无人机后，美国对伊朗发动了网络攻击，这次网络攻击旨在摧毁伊朗的雷达及火控系统，使伊朗的神经系统和侦察观测系统瘫痪，使伊朗没有还手之力。事实上，这不是美国对伊朗第一次进行网络攻击，早在几年前，美国就利用“震网”病毒，对伊朗的浓缩铀离心机系统进行了网络攻击，据说是瘫痪了整个的离心机加工系统，尽管效果不得而知，但是美国这些年来一直对此乐此不疲，而最新一次对伊朗雷达等设施的网络攻击，恰恰是美国对伊朗进行网络战的一个组成部分。

2020 年 12 月发生的 SolarWinds 供应链攻击渗透了包括五角大楼、美国财政部、白宫、国家核安全局在内的几乎所有关键部门，包括电力、石油、制造业等十多个关键基础设施中招，是美国关键基础设施迄今面临的最严峻的网络安全危机。

除美国外，世界其他主要大国也纷纷组建网络战部队，英国、日本、俄罗斯、法国、德国、印度和朝鲜等国家都已建立成编制的网络战部队。各种网络战手段已经在局部战争中得到多次运用。今后，国家间的网络战会向纵深发展，个人的网络行为也会更加活跃。因此，随着计算机及网络技术应用的不断发展，伴随而来的信息系统安全问题更加引起人们的关注。计算机系统一旦遭受破坏，将给使用单位造成重大经济损失，并严重影响正常工作的顺利开展。计算机安全是一个涉及多知识领域的综合学科，只有全面掌握相关的基础理论和技术原理，才能准确把握和应用各种安全技术和产品。

1.1　计算机安全基本概念

在计算机系统中，所有的文件，包括各类程序文件、数据文件、资料文件、数据库文件，甚至硬件系统的品牌、结构、指令系统等都属于信息。

信息已渗入社会的方方面面，信息的特殊性在于：无限的可重复性和易修改性。

计算机安全是指秘密信息在产生、传输、使用和存储过程中不被泄露或破坏。计算机安全涉及信息的保密性、完整性、可用性和不可否认性。综合来说，就是要保障信息的有效性，使信息避免遭受一系列威胁，保证业务的持续性，最大限度减少损失。

1. 计算机安全的 4 个方面

1）保密性

保密性是指对抗对手的被动攻击，确保信息不泄露给非授权的个人和实体。采取的措施包括：信息的加密和解密；划分信息的密级，为用户分配不同权限，对不同权限用户访问的对象进行访问控制；防止硬件辐射泄露、网络截获和窃听等。

2）完整性

完整性是指对抗对手的主动攻击，防止信息被未经授权的篡改，即保证信息在存储或传输的过程中不被修改、破坏及不丢失。完整性可通过对信息完整性进行检验，对信息交换真实性和有效性进行鉴别以及对系统功能正确性进行确认来实现。该过程可通过密码技

术来完成。

3）可用性

可用性是保证信息及信息系统确为授权使用者所使用，确保合法用户可访问并按要求的特性使用信息及信息系统，即当需要时能存取所需信息，防止由于计算机病毒或其他人为因素而造成系统拒绝服务。维护或恢复信息可用性的方法有很多，如对计算机和指定数据文件的存取进行严格控制，进行系统备份和可信恢复及应急处理等。

4）不可否认性

不可否认性是保证信息的发送者无法否认已发出的信息，信息的接收者无法否认已经接收的信息。例如，保证曾经发出过数据或信号的发送方事后不能否认。可通过数字签名技术来确保信息提供者无法否认自己的行为。

2. 计算机安全的组成

一般来说，计算机安全主要包括系统安全和数据安全两个方面。

系统安全：一般采用防火墙、防病毒及其他安全防范技术等措施，是属于被动型的安全措施。

数据安全：则主要采用现代密码技术对数据进行主动的安全保护，如数据保密、数据完整性、数据不可否认与抵赖、双向身份认证等技术。

1.2　计算机安全面临的威胁

由于信息系统的复杂性、开放性以及系统软硬件和网络协议的缺陷，导致了信息系统的安全威胁是多方面的：网络协议的弱点、网络操作系统的漏洞、应用系统设计的漏洞、网络系统设计的缺陷、恶意攻击、病毒、黑客的攻击、合法用户的攻击等。另外，非技术的社会工程攻击也是计算机安全面临的威胁，通常把基于非计算机的欺骗技术称为社会工程。在社会工程中，攻击者设法伪装自己的身份，让人相信他就是某个人，从而去获得密码和其他敏感的信息。

1.3　计算机安全技术体系结构

计算机安全技术是一门综合的学科，它涉及信息论、计算机科学和密码学等多方面知识，它的主要任务是研究计算机系统和通信网络内信息的保护方法，以实现系统内信息的安全、保密、真实和完整。一个完整的计算机安全技术体系结构由物理安全技术、基础安全技术、系统安全技术、网络安全技术以及应用安全技术组成。

1.3.1　物理安全技术

物理安全在整个计算机网络信息系统安全体系中占有重要地位。计算机信息系统物理安全的内涵是保护计算机信息系统设备、设施以及其他媒体免遭地震、水灾、火灾等环境

事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏。包含的主要内容为环境安全、设备安全、电源系统安全和通信线路安全。

1. 环境安全

计算机网络通信系统的运行环境应按照国家有关标准设计实施，应具备消防报警、安全照明、不间断供电、温湿度控制和防盗报警功能，以保护系统免受水、火、有害气体、地震和静电的危害。

2. 设备安全

要保证硬件设备随时处于良好的工作状态，建立健全使用管理规章制度，建立设备运行日志。同时要注意保护存储介质的安全性，包括存储介质自身和数据的安全。存储介质自身的安全主要是安全保管、防盗、防毁和防霉；数据安全是指防止数据被非法复制和非法销毁，关于存储与数据安全这一问题将在第 2 章具体介绍和解决。

3. 电源系统安全

电源是所有电子设备正常工作的能量源，在信息系统中占有重要地位。电源系统安全主要包括电力能源供应、输电线路安全和保持电源的稳定性等。

4. 通信线路安全

通信设备和通信线路的装置安装要稳固牢靠，具有一定对抗自然因素和人为因素破坏的能力。包括防止电磁信息的泄露、线路截获以及抗电磁干扰。

1.3.2 基础安全技术

随着计算机网络不断渗透到各个领域，密码学的应用范围也随之扩大。数字签名、身份鉴别等都是由密码学派生出来的新技术和应用。

密码技术（基础安全技术）是保障计算机安全的核心技术。密码技术在古代就已经得到应用，但仅限于外交和军事等重要领域。随着现代计算机技术的飞速发展，密码技术正在不断向更多其他领域渗透。它是结合数学、计算机科学、电子与通信等诸多学科于一身的交叉学科，不仅具有保证信息机密性的信息加密功能，而且具有数字签名、身份验证、秘密分存、系统安全等功能。所以，使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和确定性，防止信息被篡改、伪造和假冒。

密码学包括密码编码学和密码分析学，密码体制的设计是密码编码学的主要内容，密码体制的破译是密码分析学的主要内容，密码编码技术和密码分析技术是相互依存、互相支持、密不可分的两个方面。

从密码体制方面而言，密码体制有对称密钥密码技术和非对称密钥密码技术：对称密钥密码技术要求加密和解密双方拥有相同的密钥；非对称密钥密码技术要求加密和解密双方拥有不相同的密钥。

密码学不仅包含编码与破译，而且包括安全管理、安全协议设计、散列函数等内容。不仅如此，随着密码学的进一步发展，涌现了大量的新技术和新概念，如零知识证明技术、盲签名、比特承诺、遗忘传递、数字化现金、量子密码技术、混沌密码等。

我国明确规定严格禁止直接使用国外的密码算法和安全产品，这主要有两个原因：一

是国外禁止出口密码算法和产品，所谓出口的安全密码算法国外都有破译手段；二是担心国外的算法和产品中存在“后门”，关键时刻危害我国安全。

1.3.3　系统安全技术

随着社会信息化的发展，计算机安全问题日益严重，建立安全防范体系的需求越来越强烈。操作系统是整个计算机信息系统的核心，操作系统安全是整个安全防范体系的基础，同时也是计算机安全的重要内容。

操作系统的安全功能主要包括：标识与鉴别、自主访问控制（DAC）、强制访问控制（MAC）、安全审计、客体重用、最小特权管理、可信路径、隐蔽通道分析、加密卡支持等。

另外，随着计算机技术的飞速发展，数据库的应用十分广泛，深入各个领域，但随之而来产生了数据的安全问题。各种应用系统的数据库中大量数据的安全问题、敏感数据的防窃取和防篡改问题，越来越引起人们的高度重视。数据库系统作为信息的聚集体，是计算机信息系统的核心部件，其安全性至关重要，关系到企业兴衰和成败。因此，如何有效地保证数据库系统的安全，实现数据的保密性、完整性和可用性，已经成为业界人士探索研究的重要课题之一。

数据库安全性问题一直是数据库用户非常关心的问题。数据库往往保存着生产和工作需要的重要数据和资料，数据库数据的丢失以及数据库被非法用户侵入往往会造成无法估量的损失，因此，数据库的安全保密成为一个网络安全防护中非常需要重视的环节，要维护数据信息的完整性、保密性、可用性。

数据库系统的安全除依赖自身内部的安全机制外，还与外部网络环境、应用环境、从业人员素质等因素有关，因此，从广义上讲，数据库系统的安全框架可以划分为 3 个层次：

- 网络系统层次；
- 宿主操作系统层次；
- 数据库管理系统层次。

这 3 个层次构筑成数据库系统的安全体系，与数据安全的关系是逐步紧密的，防范的重要性也逐层加强，从外到内、由表及里保证数据的安全。

1.3.4　网络安全技术

一个最常见的网络安全模型是 PDRR 模型。PDRR 是指 protection（防护）、detection（检测）、response（响应）、recovery（恢复）。这 4 个部分构成了一个动态的计算机安全周期，如图 1-1 所示。

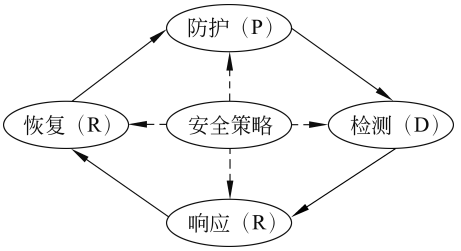

图 1-1　PDRR 网络安全模型

安全策略的每一部分包括一组相应的安全措施来实施一定的安全功能。安全策略的第一部分是防护，根据系统已知的所有安全问题做出防护措施，如打补丁、访问控制和数据加密等。安全策略的第二部分是检测，攻击者如果突破了防护系统，检测系统就会检测出入侵者的相关信息，一旦检测出入侵，响应系统就开始采取相应的措施，即第三部分——响应。安全策略的第四部分是系统恢复，在入侵事件发生后，把系统恢复到原来的状态。每次发生入侵事件，防护系统都要更新，保证相同类型的入侵事件不能再次发生。

1. 防护

PDRR 模型的最重要的部分就是防护。防护是预先阻止攻击可以发生条件的产生，让攻击者无法顺利入侵，防护可以减少大多数的入侵事件。

2. 检测

PDRR 模型的第二个环节就是检测。防护系统可以阻止大多数的入侵事件的发生，但是不能阻止所有的入侵。特别是那些利用新的系统缺陷、新的攻击手段的入侵。因此安全策略的第二个安全屏障就是检测，如果入侵发生就会被相应工具检测出来，这个工具是入侵检测系统（intrusion detection system，IDS）。

3. 响应

PDRR 模型中的第三个环节是响应。响应就是已知一个攻击（入侵）事件发生之后，进行相应的处理。在一个大规模的网络中，响应这个工作都由一个特殊部门负责，此部门称为计算机响应小组。世界上第一个计算机响应小组 CERT 于 1989 年建立，位于美国 CMU 大学的软件研究所（SEI）。从 CERT 建立之后，世界各国以及各机构也纷纷建立自己的计算机响应小组。我国第一个计算机紧急响应小组 CCERT 于 1999 年建立，主要服务于中国教育和科研网。

入侵事件的报警可以是入侵检测系统的报警，也可以是通过其他方式的汇报。响应的主要工作也可以分为两种：一种是紧急响应；另一种是其他事件处理。紧急响应就是当安全事件发生时采取应对措施；其他事件处理主要包括咨询、培训和技术支持。

4. 恢复

恢复是 PDRR 模型中的最后一个环节。恢复是事件发生后，把系统恢复到原来的状态，或者比原来更安全的状态。恢复也可以分为两个方面：系统恢复和信息恢复。

1）系统恢复

系统恢复是指修补该事件所利用的系统缺陷，不让黑客再次利用这样的缺陷入侵。一般系统恢复包括系统升级、软件升级和打补丁等。系统恢复的另一个重要工作是除去“后门”。一般来说，黑客在第一次入侵的时候都是利用系统的缺陷。在第一次入侵成功之后，黑客就在系统打开一些“后门”，如安装一个特洛伊木马。所以，尽管系统缺陷已经打了补丁，黑客下一次还是可以通过“后门”进入系统。

2）信息恢复

信息恢复是指恢复丢失的数据。数据丢失的原因可能是由于黑客入侵造成的，也可以是由于系统故障、自然灾害等原因造成的。信息恢复就是从备份和归档的数据恢复原来数据。信息恢复过程与数据备份过程有很大的关系。数据备份做得是否充分对信息恢复有很大的影响。信息恢复过程的一个特点是有优先级别。直接影响日常生活和工作的信息必须

先恢复，这样可以提高信息恢复的效率。

1.3.5　应用安全技术

目前，全球互联网用户已突破 30 亿，截至 2021 年 12 月中国网民已突破 10.3 亿。大部分用户会利用网络进行购物、银行转账支付、网络聊天和各种软件下载等。人们在享受便捷网络的同时，网络环境也变得越来越危险，如网上钓鱼、垃圾邮件以及网站被黑、企业上网账户密码被窃取、QQ 号码被盗和个人隐私数据被窃取等。因此，对每一个使用网络的人来说，掌握一些应用安全技术是很必要的。

1.4　计算机安全发展趋势

随着计算机技术的快速发展与应用，计算机安全的内涵在不断地延伸，从最初的信息保密性发展到信息的完整性、可用性、保密性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）和评（评估）”等多方面的基础理论和实施技术。计算机安全的核心问题是密码理论及其应用。目前，在计算机安全领域人们关注的焦点主要有：密码理论与技术、安全协议理论与技术、安全体系结构理论与技术、信息对抗理论与技术、网络安全与安全产品。

1.5　安全系统设计原则

安全防范体系在整体设计过程中应遵循以下 12 项原则。

1. 木桶原则

木桶原则是指对信息进行均衡、全面的保护。木桶的最大容积取决于最短的一块木板。

2. 整体性原则

要求在发生网络被攻击、破坏事件的情况下，必须尽可能地快速恢复网络信息中心的服务，减少损失。因此，计算机安全系统应该包括安全防护机制、安全检测机制和安全恢复机制。

3. 有效性与实用性原则

不能影响系统的正常运行和合法用户的操作活动。网络中的计算机安全和信息共享存在一个矛盾：一方面，为健全和弥补系统缺陷或漏洞，会采取多种技术手段和管理措施；另一方面，势必给系统的运行和用户的使用造成负担和麻烦，尤其在网络环境下，实时性要求很高的业务不能容忍安全连接和安全处理造成的时延和数据扩张。如何在确保安全性的基础上，把安全处理的运算量减小或分摊，减少用户记忆、存储工作和安全服务器的存储量、计算量，应该是一个计算机安全设计者主要解决的问题。

4. 安全性评价与平衡原则

对任何网络，绝对安全难以达到，也不一定是必要的，所以需要建立合理的实用安全

性和用户需求评价与平衡体系。安全体系设计要正确处理需求、风险与代价的关系，做到安全性与可用性相容，做到组织上可执行。对于信息是否安全，没有绝对的评判标准和衡量指标，只能取决于系统的用户需求和具体的应用环境，具体取决于系统的规模和范围以及系统的性质和信息的重要程度。

5. 标准化与一致性原则

系统是一个庞大的系统工程，其安全体系的设计必须遵循一系列的标准，这样才能确保各个分系统的一致性，使整个系统安全地互联互通、信息共享。

6. 技术与管理相结合原则

安全体系是一个复杂的系统工程，涉及人、技术、操作等要素，单靠技术或单靠管理都不可能实现。因此，必须将各种安全技术与运行管理机制、人员思想教育和技术培训以及安全规章制度建设相结合。

7. 统筹规划、分步实施原则

由于政策规定、服务需求的不明朗，环境、条件、时间的变化，攻击手段的进步，安全防护不可能一步到位，可在一个比较全面的安全规划下，根据网络的实际需要，先建立基本的安全体系，保证基本的、必须的安全性。今后随着网络规模的扩大及应用的增加，网络应用和复杂程度的变化，网络脆弱性也会不断增加，需要调整或增强安全防护力度，保证整个网络最根本的安全需求。

8. 等级性原则

等级性原则是指安全层次和安全级别。良好的计算机安全系统必然是分为不同等级的，包括对信息保密程度分级，对用户操作权限分级，对网络安全程度分级（安全子网和安全区域），对系统实现结构的分级（应用层、网络层、链路层等），从而针对不同级别的安全对象，提供全面、可选的安全算法和安全体制，以满足网络中不同层次的各种实际需求。

9. 动态发展原则

要根据网络安全的变化不断调整安全措施，适应新的网络环境，满足新的网络安全需求。

10. 易操作性原则

首先，安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

11. 自主和可控性原则

网络安全与保密问题关系着一个国家的主权和安全，所以网络安全产品不可能依赖从国外进口，必须解决网络安全产品的自主权和自控权问题，建立我国自主的网络安全产品和产业。同时为了防止安全技术被不正当的用户使用，必须采取相应的措施对其进行控制，如密钥托管技术等。

12. 权限分割、互相制约、最小化原则

在很多系统中都有一个系统超级用户或系统管理员，拥有对系统全部资源的存取和分配权，所以它的安全至关重要，如果不加以限制，有可能由于超级用户的恶意行为、口令泄密、偶然破坏等对系统造成不可估量的损失和破坏。因此有必要对系统超级用户的权限

加以限制，实现权限最小化原则。管理权限交叉，有几个管理用户来动态地控制系统的管理，实现互相制约。对于普通用户，则实现权限最小化原则，不允许其进行非授权以外的操作。

计算机系统安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化最大限度地影响着整个计算机网络系统的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上减少其他层次的安全漏洞。

1.6　本书实验环境 —— VirtualBox

VirtualBox 是一款最早由德国 InnoTek 公司开发的开源虚拟机软件，以 GNU General Public License（GPL）释出，后来被 Sun 公司收购，改名为 Sun VirtualBox，性能得到很大的提高。在 Sun 公司被 Oracle 公司收购后更名为 Oracle VM VirtualBox。可以在 VirtualBox 上安装并运行的操作系统有 Windows、Linux、Mac OS、Android-x86、OS/2、Solaris、BSD、DOS 等。

1.6.1　安装 VirtualBox

安装 VirtualBox 的要求如下。

操作系统：Windows 7/10/11，64 位。

内存：8GB 以上。

本书使用的 VirtualBox 版本为 VirtualBox-6.1.4-136177-Win.exe 和 VirtualBox 扩展包 Oracle_VM_VirtualBox_Extension_Pack-6.1.4-136177.vbox-extpack。

双击 VirtualBox-6.1.4-136177-Win.exe，进入安装向导，开始 VirtualBox 的安装，单击“下一步”按钮，进入自定义安装界面，如图 1-2 所示，可以选择安装位置和功能。连续单

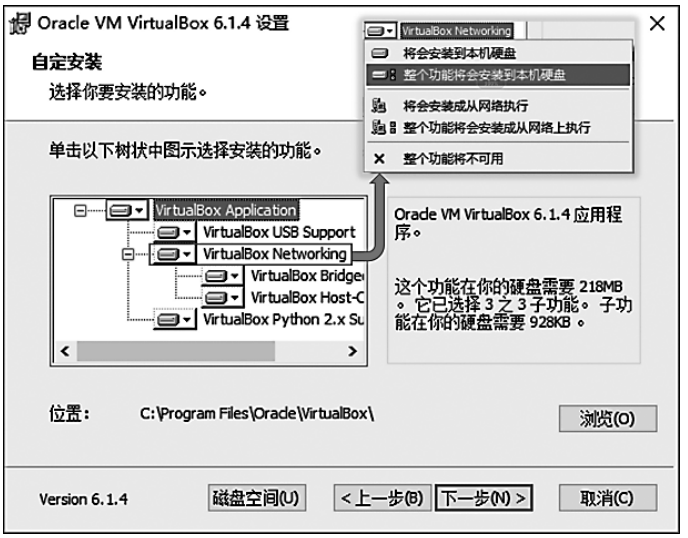

图 1-2　选择安装位置和功能

击“下一步”按钮，即可完成 VirtualBox 的安装。

注意：VirtualBox Networking 默认选择将整个功能安装到本机硬盘。

运行 VirtualBox，进入 VirtualBox 主界面，如图 1-3 所示。单击“全局设定”按钮，如图 1-4 所示。单击左侧栏“扩展”选项，然后单击右侧“”按钮，安装 VirtualBox 扩展包：Oracle_VM_VirtualBox_Extension_Pack-6.1.4-136177.vbox-extpack。

图 1-3　VirtualBox 主界面

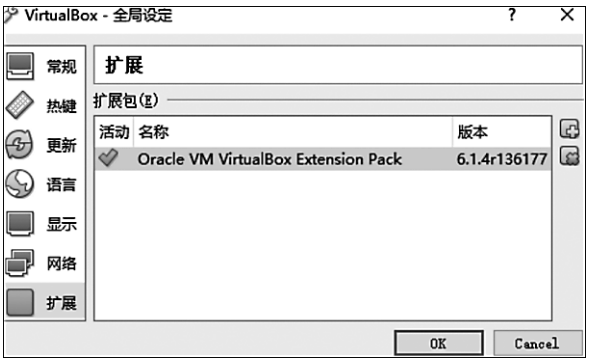

图 1-4　安装 VirtualBox 扩展包

1.6.2　在 VirtualBox 中安装操作系统

1. 在 VirtualBox 中安装 KaliLinux

在 KaliLinux 官方网站（https://www.kali.org/downloads/）或清华大学开源软件镜像站（https://mirror.tuna.tsinghua.edu.cn/kali-images/）下载 KaliLinux 的安装镜像文件，本书使用 kali-linux-2020.1b-installer-amd64.iso。

打开 VirtualBox，在主界面单击“新建”按钮，打开“新建虚拟电脑”对话框，相关设置如图 1-5 所示。

注意：可能有的计算机没有 Debian（64bit）选项，这是因为 CPU 没有开启虚拟化。解决办法是重启计算机进入 BIOS，选择 Virtualization Technology。