巍巍交大　百年书香
www.jiaodapress.com.cn
bookinfo@sjtu.edu.cn

丛书策划　张荣昌
责任编辑　王　清　孟海江
封面设计　唐漪設計

新时代计算机人才培养系列教材

大数据

大数据基础
大数据采集与预处理技术
数据结构与算法
大数据集群搭建维护与数据存储
大数据采集与数据处理
Hadoop应用与开发
数据可视化技术与应用
大数据分析技术与应用
数据挖掘技术与应用

云计算

云计算基础
私有云基础架构与运维
公有云服务架构与运维
云平台配置与管理
云安全技术应用
云网络技术应用
云计算运维开发
云计算应用开发

人工智能

人工智能应用基础
人工智能数学基础
人工智能数据服务
计算机视觉应用开发
深度学习应用开发
机器学习应用开发
自然语言处理及应用开发
智能语音处理及应用开发
人工智能系统部署与运维
人工智能综合项目开发

区块链

区块链应用基础
区块链核心技术
区块链部署与运维
区块链应用设计与开发
区块链项目综合实践
智能合约开发

物联网

物联网基础
物联网工程导论
物联网嵌入式技术
物联网设备装调与维护
物联网系统部署与运维
物联网工程设计与管理
物联网终端智能应用开发基础案例教程（基于HAL/LL库）

信息安全

信息安全技术
信息安全基础
信息安全标准与法规
信息安全工程与管理
信息安全风险评估
密码产品部署与应用
电子商务安全技术
无线网络安全技术
大数据安全技术
电子数据取证技术
终端数据安全及防泄密
数据存储与容灾
Web应用安全与防护
渗透测试

专业基础

数据库应用技术（基于达梦数据库）
MySQL数据库应用技术项目教程
计算机组装与维护
计算机网络基础
Linux系统管理与服务器配置
Linux服务器安全高级运维
Windows Server操作系统基础
现代通信原理
无线传输技术
自动识别应用技术
智能传感与检测技术
路由交换技术项目实战教程
虚拟化技术基础

本书提供教学资源包
网址：https://www.sjhtbook.com

扫描二维码
关注上海交通大学出版社
官方微信

ISBN 978-7-313-31864-0
9 787313 318640 >
定价：49.80元

新时代计算机人才培养系列教材
信息安全技术
主编◎赵志俊　徐永冰　廖大强

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

广东省课程思政示范课程“信息安全技术”配套教材
新时代计算机人才培养系列教材

信息安全技术

主编◎赵志俊　徐永冰　廖大强

上海交通大学出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

广东省课程思政示范课程“信息安全技术”配套教材
新时代计算机人才培养系列教材

信息安全技术

主编◎赵志俊　徐永冰　廖大强

扫一扫
学习资源库

上海交通大學出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

内容提要

本书采用项目驱动方式，全面地介绍了信息安全领域各个方面的基础知识，能够为信息安全专业人员提供全景蓝图。全书共分 14 个项目，项目 1 为导论，介绍信息安全基础知识和相关法律法规，项目 2 至项目 14 介绍环境搭建、信息收集、漏洞扫描、中间人攻击、暴力攻击、木马控制、Web 渗透、计算机病毒、数据加密、防火墙等内容。同时，本书在每个项目中都提供多个实操任务，让读者在学习知识的同时，能够理论联系实际，做到学以致用。本书可作为高等院校计算机专业信息安全、网络安全等课程的教材，也可作为相关专业人员自学及培训的参考用书。

图书在版编目（CIP）数据

信息安全技术 / 赵志俊，徐永冰，廖大强主编.
上海 : 上海交通大学出版社，2024. 12 -- ISBN 978-7-313-31864-0

Ⅰ. TP309

中国国家版本馆 CIP 数据核字第 2024YS5078 号

信息安全技术
XINXI ANQUAN JISHU

主　　编：赵志俊　徐永冰　廖大强
出版发行：上海交通大学出版社
邮政编码：200030
印　　制：北京荣玉印刷有限公司
开　　本：889 mm × 1194 mm　1/16
字　　数：536 千字
版　　次：2024 年 12 月第 1 版
书　　号：ISBN 978-7-313-31864-0
定　　价：49.80 元

地　　址：上海市番禺路 951 号
电　　话：021-6407 1208
经　　销：全国新华书店
印　　张：17
印　　次：2024 年 12 月第 1 次印刷
电子书号：ISBN 978-7-89424-960-9

在线课程学习指南

本书配有在线开放课程“信息安全技术”，读者可在学银在线平台进行学习。

一、搜索课程

进入学银在线平台（https://www.xueyinonline.com），在页面上方输入框中输入“信息安全技术”，单击搜索按钮后在搜索结果中选择对应课程（主讲教师：廖大强）。

二、在线学习

选择对应课程后进入课程界面，单击“加入课程”，登录后即可在线学习该课程。

前言

近年来，随着科技的快速发展，互联网产品和服务在多个领域展现出其重要性。无论是在紧急应对各类突发情况方面，还是在支持远程工作、教育、医疗和智能化生产等日常活动方面，创新的解决方案不断涌现，加快了社会向数字化转型的步伐。在这一过程中，信息安全问题也日益受到关注。安全漏洞、数据泄露、网络诈骗、恶意软件等问题逐渐增多，有组织的网络攻击行为变得更加明显，这为网络信息安全防护工作带来了新的挑战。

本教材采用“项目化教学 + 任务驱动”的教学方法，为培养高端应用型人才提供合适的教学与训练内容。本教材以实际项目转化的案例为主线，结合“岗课赛证”一体化培养体制，突出课程思政教育，在完成技术讲解的同时，对读者提出相应的自学要求并给予指导。本教材实践“用劳模精神感召人、用劳动精神培养人、用工匠精神铸造人”的特色育人理念，读者在学习本教材的过程中，不仅能深入理解信息安全的知识和技能，还能够培养自己的道德情操，了解中国信息安全方面最新的发展成就，树立“没有网络安全就没有国家安全”的理念。

本教材作者有着多年的实际项目开发经验和丰富的一线教育教学经验，有的作者还参与了多轮次、多类型的教育教学改革与研究工作。教材在编写过程中，得到了中兴通讯股份有限公司电子制造学院院长、广东省职业院校产业导师、深圳市五一劳动奖章获得者孙磊高级工程师和全国五一劳动奖章获得者、中国移动通信集团广东有限公司清远分公司工程师、广东省技术能手李冬梅高级工程师的大力支持。奇安信安全技术（广东）有限公司副总经理李双喜工程师也对本教材的编写提出了宝贵意见。

本教材主要特点如下。

1. 校企双元开发，实际项目开发与理论教学紧密结合

本教材在编写过程中联合中兴通讯股份有限公司、奇安信安全技术（广东）有限公司、中国移动通信集团广东有限公司清远分公司，导入企业项目资源。同时，为了使读者能快速地掌握并按实际项目开发要求熟练运用相关技术，本教材在各个项目重要知识点后面都根据实际项目设计了相关实验和企业案例。

2. 深入挖掘思政元素，将课程思政和信息技术有机融合

本教材将习近平新时代中国特色社会主义思想、党的二十大精神融入书中项目和任务，为读者全面展示党对社会和科学技术的巨大推动力和指引效能，做到全面、全程的思政教育和道德熏陶。

3. 开发配套数字资源，构建“课 + 书 + 空间”体系

本教材吸取先进经验，开发数字教学资源，做到“一课一书一空间”。“一课”即省级课程思政示范课，“一书”就是配套教材，“一空间”是“学银在线”开放课学习空间。

本教材由赵志俊、徐永冰、廖大强任主编，杨帆、郑海清、李冬梅任副主编，其中项目 1 由李冬梅编写，项目 2、6、7 由赵志俊编写，项目 3、4、5 由杨帆编写，项目 8 由郑海清编写，项目 9、10、11 由廖大强编写，项目 12、13 由徐永冰编写，项目 14 由杨帆和徐永冰联合编写。

由于编者水平有限，书中若存在不妥或疏漏之处，殷切希望广大读者给予批评和指正。

编　者

2024 年 2 月

目录

项目 1 认识信息安全

项目目标

知识目标

（1）了解信息安全的概念。
（2）了解信息安全的发展历程。
（3）了解信息安全的重要性。
（4）了解我国信息安全相关的法律法规。

能力目标

（1）能够把握信息安全的发展趋势。
（2）能够利用 IT 工具搜索信息安全前沿知识。

素质目标

（1）树立爱国主义情怀，持续关注我国信息安全事业的发展。
（2）培养信息安全意识和防范习惯。

思政聚焦

2024 年 9 月 9 日至 15 日，以“网络安全为人民，网络安全靠人民”和“市民身边的网络安全”为主题的国家网络安全宣传周在全国范围内统一开展，体现了党和国家领导人全面深化改革、加强顶层设计的意志，显示出保障网络安全、维护国家利益、推动信息化发展的决心。信息网络技术对国家经济、政治、外交、国防等关键领域都具有深远的影响，在国际竞争和网络攻防中亦发挥重要作用，这都突显了国家信息安全的重要性。

党的二十大报告进一步强调了提升公共安全治理水平的必要性，提出“坚持安全第一、预防为主”的原则。报告中提到构建全面的大安全大应急框架，完善公共安全体系，推动治理模式向事前预防转型。这包括深化安全生产风险的专项整治，加强重点行业和领域的安全监管，提高防灾减灾救灾和应对重大突发公共事件处置保障能力。同时，报告也强调了加强食品药品安全监管，完善生物安全监管预警防控体系，以及加强个人信息保护的重要性。

这些措施体现了国家对维护公共安全和国家安全的坚定决心，旨在通过预防和准备，提高国家对各类风险的应对能力，确保人民的生命财产安全和社会稳定。

【项目导入】

网络技术和信息技术的频繁更迭推动了社会的整体发展，它们在经济、生产、文化、科学技术等多个方面都发挥着不可替代的作用。网络在生活中的应用已经十分广泛，为日常生活提供了巨大便捷。与此同时，网络信息的开放性和全球性也带来了一定的挑战和危险。如今，网络资源共享化趋势明显，在快速获取信息的同时，信息安全问题也逐渐显露。伴随网络规模的迅速扩张，网络黑客、病毒等大量出现，严重威胁着我们的信息安全。因此，维护信息安全是每一个信息安全相关人员的责任与义务，也是每一个身处信息时代的个体应积极关注和配合的事情。

1.1 知识储备

1.1.1 信息安全的概念和内容

信息安全的实质就是要保护信息资源免受各种类型的威胁、干扰和破坏，防止信息资源被故意或偶然地非授权泄露、更改、破坏，或使信息被非法系统辨识、控制，即保证信息的完整性、可用性、保密性和可靠性。

信息安全是国家安全的关键组成部分，它不仅关乎国家机密的守护，确保战略利益不外泄，还可延伸至商业领域，关系到企业秘密和知识产权的保护。同时，信息安全在青少年保护方面扮演着重要角色，如通过过滤不良信息，为年轻一代营造健康网络环境。此外，个人信息的安全同样重要，防止私人数据泄露和隐私侵犯、保障民众的网络权益刻不容缓。

过去几年，信息技术（Information Technology，IT）发展迅猛，诸如云计算、远程工作、在家办公、自带设备办公（BYOD）计划，以及智能门铃、智能网联汽车等各种联网设备，均带来了巨大的商业优势和科技进步，但也为网络罪犯创造了成倍增加的攻击机会。根据 IBM 公司发布的《2023 年数据泄露成本报告》，2023 年数据泄露的平均成本为 445 万美元，比过去几年增长了 15%；2023 年与勒索软件相关的数据泄露平均成本甚至更高，达到 513 万美元，这还不包括赎金支付的费用，赎金支付的费用平均额外增加了 154 万美元，比上一年增长了 89%。据估计，到 2025 年，网络犯罪每年可能给世界经济造成 10.5 万亿美元的损失。

1.1.2 信息安全发展历程

信息安全的发展是一段不断演进的历程，从古罗马的凯撒密码到现代的加密技术，信息保密传递始终是人类追求的目标。随着信息技术的发展，信息的电子化带来了获取、携带与传输的便利，也使得信息安全保障技术变得尤为重要。

20 世纪初期，信息安全主要表现在通信安全上，侧重于信息的保密性。然而，随着半导体、集成电路技术的发展，计算机软硬件得到广泛应用，信息安全的关注点扩展到了保密性、完整性和可用性。1969 年，美国兰德公司首次提出“计算机安全”概念，起初主要关注计算机的物理安全问题。

进入 20 世纪 70 年代和 80 年代，计算机管理系统和各种应用的增多使得“计算机安全”逐步演化为“计算机信息系统安全”，安全概念扩展到了软件与信息内容等的安全。到了 20 世纪 80 年代后期，“网络安全”和“信息安全”开始被广泛采用，信息安全管理变得越来越重要。

中国的信息安全事业起步于 1986 年，这一时间点标志着中国计算机安全事业的开端。1986 年中国计算机学会计算机安全专业委员会正式开始活动，1987 年国家信息中心信息安全处建立，这两个事件共同反映了中国计算机安全事业的进步。尽管当时法规建设尚处于初步发展阶段，但随着对信息安全重要性认识的提升，法规建设、安全管理和技术创新等方面都在不断加强。

1994 年，《中华人民共和国计算机信息系统安全保护条例》颁布，该条例是我国计算机安全方面的首个法律，全面阐述了计算机信息系统安全的法规要求。该条例的出台促使企事业单位开始重视信息安全，建立专门安全部门，学校和研究机构也开始培养信息安全人才。

进入 21 世纪，中国安全产业进入快速发展阶段，国家重视信息安全工作，出台了一系列重要政策和措施。信息安全市场销售额从 1998 年的 4.5 亿元（人民币，后同）增长至 2012 年的近 300 亿元，中国自主研发的安全设备品种逐步健全。

国际上，美国国土安全部成立国家网络安全司，全球首次认识到信息安全具有国家甚至全球意义。21 世纪 00 年代初期，随着虚拟专用网络（VPN）的出现，安全工具开始呈现多样化趋势。2007 年，基于“云”的安全解决方案发布，信息安全工具得到更广泛应用。

随着智能手机和社交媒体的普及，信息安全产品的可访问性不断提高，这也使得大众更容易受到黑客的攻击。21 世纪 10 年代，新型网络战手段的演变开始加速，个人数据和企业数据泄露的风险均呈现日益严重的态势。某国核项目的计算机感染恶意软件事件更预示着网络攻击可能被武器化，对全球关键基础设施构成严重威胁。

与此同时，数据收集的重要性被大众所认知。Facebook 和 Google 等公司收集大量用户信息，数据泄露可能导致这些信息在暗网上出售，被用于网络钓鱼攻击或身份盗窃。2019 年 Facebook 用户数据泄露事件就是一个典型例子。

近年来，随着远程工作成为常态，关键基础设施的信息安全得到显著加强，国际合作在信息安全领域也达到新的高度。这些进步提高了信息安全的整体水平，为未来的技术发展和政策制定提供了宝贵经验。

信息安全技术的发展是一条不断适应科技进步和应对新挑战的道路。从古至今，信息安全的核心始终是保证信息的保密性、完整性和可用性，随着科技的演进，信息安全技术将继续发展，以应对不断变化的网络环境和安全威胁。

1.1.3 信息安全的发展现状

信息安全的历史正被不断书写，随着风险和应对策略的演变，被动应对信息安全事件的时代已经结束。

5G 技术的崛起为数字化转型带来了新的机遇和挑战。它在远程医疗、智能制造、增强现实培训等领域的应用前景广阔，但同时也增加了网络威胁的攻击面。因此，从设计之初就嵌入信息安全对 5G 技术的发展至关重要，尽管这将会增加一定的技术复杂性。

数字经济的发展推动了人工智能、大数据、区块链等新兴技术在数据安全领域的应用。这些技术通过深度学习和大数据分析等方法，能够实时检测异常，智能化识别和阻断数据泄露，识别潜在的安全漏洞。同时，它们还优化了数据标识和匿名方法，这也体现了安全产品与服务的不断创新和升级。

人工智能生成内容（Artificial Intelligence Generated Content，AIGC）的快速发展引起了全球对数据安全和隐私保护的极大关注。AIGC 模型训练过程中可能涉及敏感信息，存在隐私泄露和恶意攻击的风险。因此，需要采取针对性措施应对 AIGC 带来的新挑战。

量子计算的兴起对传统加密算法构成威胁，如 Shor 算法能破解 RSA（非对称加密算法）和椭圆曲线公钥密码算法等，Grover 算法对对称加密算法和数字签名构成挑战，这都加速了对量子安全加密算法的需求。

信息安全策略必须考虑量子计算的崛起，采用量子安全技术以确保信息的保密性、完整性和可用性。

总之，信息安全不仅仅是技术问题，更是战略问题。随着新兴技术的发展，我们必须前瞻性地构建安全策略，以确保在数字化转型的道路上稳步前行。

1.2 任务实施

1.2.1 系统安全检查

系统是否安全是没有标准定义的，不同的需求也有不同的安全标准。对于个人用户来说，可以检查以下几个方面。

（1）程序运行是否正常。在日常使用过程中，如果发现某些程序运行异常、无法运行或运行时报错，须及时杀毒。

（2）是否存在文件丢失或损坏情况。如果计算机在启动、运行过程中经常出现文件丢失或损坏情况，那么很有可能是因为系统被病毒感染，处于非安全状态。

（3）网络是否通畅。现在相当多的软件都需要使用网络，如果软件不能正常联网就需要检查是否有中毒的风险。

1.2.2 了解我国信息安全法律法规

随着网络信息技术的迅猛发展，信息安全形势日益严峻。法治化是确保网络空间安全的关键，有法可依则是依法治网的基石，中国在网络空间法治化建设上不断深化改革，通过制定和完善一系列法律法规，逐步构建起一个较为完整的信息安全法律法规体系。

自 1994 年全功能接入国际互联网以来，中国的互联网治理和网络立法经历了从技术工具到社会基础设施的转变。早期，如《中华人民共和国计算机信息系统安全保护条例》等法规，主要关注信息技术本身安全和应用发展。进入 21 世纪，随着互联网媒体属性和商业价值的显现，《中华人民共和国电信条例》和《互联网信息服务管理办法》等规定相继出台，体现了我国各部门对网络信息治理的重视。

2014 年 2 月 27 日，中央网络安全和信息化领导小组成立，这标志着中国互联网治理进入了统筹协调、顶层设计的新时代。随后，我国颁布了《中华人民共和国网络安全法》，确立了网络空间主权原则，建立了关键信息基础设施安全保护制度，明确了各方在信息安全保护领域的权利与义务，成为网络空间法治化建设道路上的重要里程碑。

2021 年，中国网络空间法治化建设再上新台阶，《关键信息基础设施安全保护条例》和《中华人民共和国数据安全法》的通过，进一步强化了对关键信息基础设施和数据安全的保护。同年，《中华人民共和国个人信息保护法》的通过，更是标志着个人信息保护立法体系进入新的发展阶段，为个人信息权益提供了更为坚实的法律保障。

此外，中国还出台了《网络安全审查办法》《云计算服务安全评估办法》等政策文件，建立了网络安全审查、云计算服务安全评估、数据安全管理、个人信息保护等重要制度，并制定发布了 300 余项信息安全领域的国家标准，为信息安全法律法规体系的构建提供了坚实的基础。

中国的信息安全法律法规体系，不仅保障了网络空间的国家主权，也维护了公民的个人信息权利与信息

安全，促进了网络空间的良性和可持续发展。通过依法管理，中国正逐步探索出一条符合自身国情的网络空间法治之道，并为全球网络治理贡献了中国智慧和中国方案。

1.2.3 了解人工智能对信息安全的影响

1. 了解人工智能

人工智能（Artificial Intelligence，AI）是致力于解决与人类智能相关联的认知性问题的计算机科学领域，这些问题包括学习、创造和图像识别等。人工智能从各种来源（如智能传感器、人工生成的内容、监控工具、系统日志等）收集大量数据，创建从数据中获取意义的自我学习系统，然后应用所学知识以类似人类的方式解决新问题。例如，人工智能技术可以对人类对话做出有意义的响应，创建原始图像和文本，并根据实时数据输入做出决策。

在 Alan Mathison Turing（艾伦·麦席森·图灵）1950 年发表的开创性论文《计算机器与智能》中，他首次提出了“人工智能”这一概念，将其作为一种理论和哲学概念，深刻探讨了其本质，并提出了著名的“图灵测试”，这是评估机器是否具有智能的标准。然而，值得注意的是，“人工智能”一词本身是由 John McCarthy（约翰·麦卡锡）在 1956 年的达特茅斯会议上首次正式提出的。因此，虽然图灵在 1950 年提出了人工智能的概念和相关理论，但“人工智能”这一术语的正式使用是在 1956 年。

在 1957 年至 1974 年之间，计算机的发展使计算机能够存储更多数据并更快地进行处理。在此期间，科学家进一步开发了机器学习（Machine Learning，ML）算法。该领域的进展促使美国国防部高级研究计划局（DARPA）等机构设立了人工智能研究基金。起初，该基金的主要用途是研究计算机是否可以转录和翻译口语。

20 世纪 80 年代，可用资金的增加和科学家在人工智能开发中使用的算法工具包的不断扩展简化了开发。David Rumelhart（大卫·鲁梅尔哈特）和 John Hopfield（约翰·霍普菲尔德）发表了关于深度学习技术的论文，这些论文表明计算机可以从经验中学习。

从 1990 年到 21 世纪初，科学家实现了人工智能的许多核心目标，比如击败世界象棋冠军。与前几十年相比，当前人工智能的数据计算和处理能力更强，人工智能研究也变得更加普遍，更容易获得。人工智能正在逐渐演变为通用人工智能，软件可以执行复杂的任务，可以自己创造、决策和学习，而这些以前只限于人类。

2. 人工智能前沿知识

2018 年以来，大模型首先在自然语言处理领域取得突破，以 ChatGPT 为代表的现象级产品拉开了通用人工智能的序幕，引发了新一轮人工智能发展浪潮。当前人工智能发展已由小模型时代迈向大模型时代。

大模型是大数据、大算力、强算法结合的产物，至少具有三个特点：一是规模大，神经网络参数规模要达到百亿以上；二是涌现性，要产生预料之外的新能力，这是人工智能发展近 70 年来最具里程碑意义的新特性；三是通用性，能够解决各类问题。

美国 OpenAI 公司的 GPT（生成型预训练 Transformer 模型）系列大模型是当前国际大模型领域的领先代表。2022 年 11 月，OpenAI 发布的人工智能对话大模型 ChatGPT 表现出了惊人的智能水平，能够长时间进行自然流畅的对话，同时还能够高质量撰写各种类型的书面材料，可以完成很多需要创造性思考的任务，一经发布就受到全球用户的广泛关注，成为历史上增长最快的消费应用。

除语言能力以外，大模型也在迅速扩展视觉、听觉、具身（有身体的智能，能与环境进行交互）、行动等其他通用智能能力，在向多模态方向发展的同时，也将逐渐进入现实世界，发展实体智能，引发下一波人工智能发展浪潮。

3. 人工智能在信息安全中的应用

随着技术的飞速发展，人工智能已经在各个领域展现出巨大的潜力，信息安全领域也不例外。人工智能正在成为保护信息资源免受各种威胁的关键手段。

1）威胁检测与预测

人工智能可以通过对大量历史数据的分析，识别出潜在的网络威胁和攻击模式。利用机器学习算法，人工智能可以从过去的攻击中汲取经验，从而预测未来可能的威胁。这种预测性的防御可以帮助系统提前采取措施，从而降低潜在损失。

2）异常检测与行为分析

人工智能可以监测网络和系统的正常行为，检测出异常活动。通过对用户和实体的行为进行建模，人工智能可以迅速识别出异常情况，如未经授权的访问、数据泄露等。这种基于行为的检测方法可以帮助系统在攻击发生之前就采取行动。

3）自动化威胁响应

当发现潜在的安全事件时，人工智能可以自动采取措施来阻止攻击的进一步扩散。这种自动化响应可以节省时间和资源，并且在攻击发生时能够更快地采取行动，从而减少损失。

4）威胁情报分析

人工智能可以处理大量的威胁情报数据，从各种来源收集信息，并分析其与系统的关联。这可以帮助相关人员更好地了解当前的威胁环境，并做出更明智的决策来保护系统和数据。

5）智能防火墙和入侵防御

智能防火墙可以根据实时的网络流量和威胁情报自动调整其策略，以封锁潜在的攻击。入侵防御系统可以通过学习攻击模式，自动识别并阻止新型的攻击行为。

6）恶意软件检测与清除

人工智能可以识别出恶意软件的特征，并快速检测出系统中的潜在威胁。在检测到恶意软件时，人工智能会自动隔离、清除恶意软件，从而阻止其进一步传播。

【项目小结】

信息安全已经成为世界各国关注的焦点和热点问题，也成为急需专业人才的新领域。本项目介绍了信息安全的相关概念和发展态势，并对信息安全的法律法规进行了概述。本项目中所涉及的一些概念和技术的技术细节和实现方法将在本书随后的项目中进行详细的介绍和分析。

信息安全的最终目标和关键是保护系统的信息资源安全，做好预防是确保信息安全的最好举措。世界上并没有绝对的安全，信息安全也是个系统工程，需要多方面密切配合、综合防范才能收到实效。

【拓展阅读】

拓展阅读 1

巩固练习

1. 选择题

（1）网络安全的实质和关键是保护网络的（　　）安全。

A. 系统　　B. 软件　　C. 信息　　D. 网站

（2）在短时间内向网络中的某台服务器发送大量无效连接请求，导致合法用户暂时无法访问服务器的攻击行为是破坏了（　　）。

A. 保密性　　B. 完整性　　C. 可用性　　D. 可控性

（3）大模型的特点不包括（　　）。

A. 规模大　　B. 涌现性　　C. 通用性　　D. 可控性

（4）下列说法不正确的是（　　）。

A. 黑客多数利用计算机进行犯罪活动，如窃取国家机密

B. 计算机黑客是指那些制造计算机病毒的人

C. 安装防火墙是预防计算机病毒的措施之一

D. 黑客攻击网络的主要手段之一是寻找系统漏洞

（5）如果访问者有意避开系统的访问控制机制，则该访问者对网络设备及资源进行非正常使用属于（　　）。

A. 破坏数据完整性　　B. 非授权访问　　C. 信息泄露　　D. 拒绝服务攻击

2. 简答题

（1）根据自己的理解，简述信息安全事件频发的原因。

（2）简述信息安全发展的历程。

（3）根据自己的理解，分析人工智能对信息安全的影响是利大还是弊大。

项目 2 环境搭建

【项目目标】

知识目标

（1）了解渗透测试及其分类。

（2）熟悉标准渗透测试流程。

（3）掌握渗透测试平台搭建。

能力目标

（1）能够搭建 Kali Linux 渗透测试平台。

（2）能够搭建 OWASP 靶机平台。

素质目标

（1）关注国产操作系统发展现状，培养创新精神。

（2）了解我国在操作系统领域取得的成就，培养爱国精神。

【思政聚焦】

党的二十大报告中将信息安全和国产操作系统定位为国家信息化发展的核心领域，赋予其推进国家安全体系现代化建设和维护社会稳定的重大使命。国产操作系统，作为科技自立自强的体现，对保障网络安全和激发国家创新活力至关重要。

尽管国产操作系统整体国产化率尚不足 5%，但其在金融和电信行业的应用正迅速增长，预计 2024 年市场规模将达到人民币 34.1 亿元，该数据显示出市场的强劲增长势头。国产操作系统厂商正通过技术创新和生态建设等措施，努力提升产品竞争力，如中科方德的“融合生态新平台”和统信软件的开源社区。

目前，国产操作系统已在多个关键行业实现规模化应用，充分展示了其在国家信息化建设中的重要作用。面对与国际主流操作系统的差距，国产操作系统将继续强化生态建设和提升用户体验，以满足市场需求。

展望未来，国产操作系统凭借快速发展的势头，有望在全球市场取得显著成就，为国家信息化建设和信息安全做出更大贡献。

【项目导入】

党的二十大胜利召开，宣示了我国向第二个百年奋斗目标进军。在新发展格局的构建和高质量发展的推动中，信息安全被提升至前所未有的战略高度，为行业发展注入了强劲动力与信心。信息安全是国家安全的关键一环，它不仅关乎个人生活与工作的方方面面，更是国家发展的重要组成部分。

渗透测试作为保障信息安全的关键措施，能够及时发现并修复潜在的安全漏洞，提升企业的安全防护意识，增强系统的安全性与稳定性，预防业务损失。它不仅是技术实践，也是一项合规要求，企业和组织应积极履行，确保业务的合法合规性。

本项目通过虚拟化技术，结合主流渗透测试系统和靶机，搭建起合法合规的渗透测试环境，旨在深化对渗透测试工作原理的理解，为项目实施奠定坚实基础。

2.1 知识储备

2.1.1 了解渗透测试

渗透测试是一种通过模拟黑客攻击手段，来评估计算机网络系统安全性的评估方法。它主动分析系统的弱点、技术缺陷和漏洞，旨在通过攻击者视角发现并挫败安全控制措施，揭露可能影响业务的安全隐患。

渗透测试不仅对系统安全进行测试，更从攻防双方角度深入分析目标系统的脆弱性，以确保安全为最终目标。它涉及对目标系统的主动探测分析，识别不当配置、软硬件漏洞及安全计划中的操作性弱点。这一过程要求测试者站在攻击者的角度，进行深入的分析和攻击尝试。渗透测试的结果，包括安全问题带来的业务影响后果评估和解决方案，将在报告中详细呈现，助力系统所有者修补漏洞，提升系统安全性。

渗透测试已成为系统安全评估中不可或缺的一部分，银行和支付行业的数据安全标准（PCI DSS）等都将之列为必须执行的安全测试。随着经济和信息化的快速发展，渗透测试也演变为安全公司提供的专业服务，为各行业信息安全保驾护航。

2.1.2 渗透测试的分类

渗透测试是信息安全评估的关键环节，主要分为三种方法：黑盒测试、白盒测试和灰盒测试。

1. 黑盒测试

黑盒测试（Black-box Testing），亦称外部测试，是模拟外部攻击者对目标网络基础设施进行评估的过程。测试团队在缺乏内部信息的情况下，使用流行的攻击技术和工具，逐步渗透目标组织，揭示安全漏洞并评估其潜在影响。此方法还能评估目标组织内部安全团队的检测与响应能力。黑盒测试虽耗时耗力，且要求测试者具备高超技术，但因其能逼真模拟真实攻击过程而受到推崇。

2. 白盒测试

白盒测试（White-box Testing），又称内部测试，允许测试团队全面了解目标环境的内部结构和底层信息。这种方法使测试者能以较低成本发现和验证系统严重漏洞，为组织带来更大价值。白盒测试流程与黑盒类似，但省去了目标定位和情报搜集步骤。它便于集成于一次常规开发周期中，早期发现并解决安全问题，避免被攻击者利用。相较于黑盒测试，白盒测试在发现和修复漏洞上更为高效，但无法有效地测试目

标组织应急响应程序和安全防护计划的效率。

3. 灰盒测试

灰盒测试（Grey-box Testing）结合了黑盒和白盒测试的优势，要求测试者在对目标系统所掌握的有限知识的基础上，选择最佳途径评估系统安全性。在外部渗透场景中，测试者虽从外部开始，但对目标网络底层结构的了解有助于更精准地选择攻击途径和方法，提高测试效果。

这三种测试方法各有特点，组织应根据具体需求和资源选择最合适的渗透测试策略，以确保信息资源无懈可击。

2.1.3 标准渗透测试流程

PTES（Penetration Testing Execution Standard，渗透测试执行标准）是由安全行业的多家领军企业技术专家共同发起的，旨在为企业组织和安全服务提供商设计并制定一套通用的渗透测试实施准则。

1. 前期交互阶段

在前期交互（Pre-Engagement Interaction）阶段，渗透测试团队与客户组织进行深入讨论，明确渗透测试的范围、目标、限制条件及服务合同细节。此阶段的关键是确保客户组织对测试目标有清晰的了解，并选择现实可行的测试目标进行实施。

2. 情报搜集阶段

在情报搜集（Information Gathering）阶段，团队利用各种信息来源和技术方法，收集目标组织网络拓扑、系统配置和安全防御措施的信息。情报搜集的方法包括公开来源查询、Google Hacking、社会工程学、网络侦查、扫描探测、被动监听和端口服务查点等。情报搜集的全面性直接影响渗透测试的成效。

3. 威胁建模阶段

威胁建模（Threat Modeling）阶段会利用情报搜集阶段的信息，识别目标系统可能存在的安全漏洞和弱点。在这一阶段，渗透测试团队需要确定最有效的攻击方法、进一步需要的信息和攻击的切入点。

4. 漏洞分析阶段

在漏洞分析（Vulnerability Analysis）阶段，渗透测试者综合分析前几个阶段获取并汇总的情报信息，特别是安全漏洞扫描结果和服务查点信息，通过搜索渗透代码资源，找出可实施攻击的点，并在实验环境中验证。高水平的团队还会探测和挖掘关键系统与服务的未知漏洞。

5. 渗透攻击阶段

在渗透攻击（Exploitation）阶段，测试者利用发现的安全漏洞侵入系统，获取访问控制权。这可能涉及使用公开的渗透代码，或根据目标系统特性定制攻击方法，以挫败系统的安全防御措施。

6. 后渗透攻击阶段

后渗透攻击（Post Exploitation）阶段最能体现团队的创造力和技术能力。团队需根据目标组织的业务模式和安全防御计划，设计攻击目标，识别关键基础设施，寻找客户组织最具价值的信息和资产，实现对客户组织业务影响最大的攻击。

7. 报告阶段

渗透测试的最终成果是一份渗透测试报告（Reporting），它汇总了所有阶段的关键情报、发现的安全漏洞、渗透攻击过程和业务影响分析。报告旨在帮助客户组织从防御者角度分析安全防御体系中的薄弱环节，并提供修补和升级的技术方案。报告通常包括摘要、过程展示和技术发现等部分，其中，技术发现部

分对客户组织修补安全漏洞至关重要。

PTES 标准为渗透测试提供了一个结构化和标准化的框架，确保测试过程的专业性和有效性，帮助组织更好地评估和提升其信息安全状况。

2.1.4 认识渗透测试平台

渗透测试平台主要由渗透测试系统和渗透测试靶机构成。

1. 渗透测试系统

目前流行的渗透测试系统众多，各有特色。其中，Kali Linux、Parrot Security OS 和 BlackArch Linux 因其卓越性能而广受推崇，而 Kali Linux 以其高市场占有率和易学易用性脱颖而出，成为渗透测试领域的佼佼者。

Kali Linux，曾用名 BackTrack Linux，是基于 Debian 的开源 Linux 发行版，专为渗透测试和安全审计设计。它预装了 600 余款渗透测试工具，如 Nmap 端口扫描器、Wireshark 数据包分析器、John the Ripper 密码破解器、Aircrack-ng 无线网络渗透工具等，为安全专业人士和爱好者提供了强大的支持。

Kali Linux 不仅适合安全行业的新手使用，也深受资深技术专家的青睐。它能帮助用户发现并利用系统漏洞，收集分析网络信息，模拟攻击场景，提升安全技能。Kali Linux 提供 32 位和 64 位镜像文件，支持多种硬件设备，包括 ARM 架构，适用于树莓派（一种小型、低成本的单板计算机）和 ARM Chromebook（一款笔记本计算机）等。用户可通过硬盘、Live CD、Live USB 等多种方式运行 Kali Linux。

Kali Linux 主要的优点如下。

（1）完全可定制：用户可根据需求定制 ISO 镜像、软件和配置。

（2）多平台支持：Kali Linux 可在移动设备、ARM 设备、云平台、容器（与容器化技术相关）、Windows 系统、虚拟机等多种设备和平台上运行。

（3）多语言支持：Kali Linux 提供包括中文、英文、法文、德文在内的多语言安装和使用选项。

（4）无线设备渗透测试：Kali Linux 预装了 Reaver、Aircrack-ng、Wifite 等多个支持无线网卡的工具，这些工具可帮助实现数据包捕获、网络侦查、密码破解等功能。

2. 渗透测试靶机

渗透测试靶机是一种用于渗透测试训练和实验的虚拟或物理机器，它故意设置了一些漏洞或弱点，让渗透测试人员或学习者可以尝试攻击和利用它们。渗透测试靶机可以帮助测试人员学习和练习渗透测试的技能，增强其安全意识。靶机可以有不同的难度级别（从简单到困难）、不同的操作系统（从 Windows 到 Linux）和不同的使用场景（从 Web 应用到网络服务）。渗透测试靶机可以自己搭建，也可以从网上下载或在线访问。当前常用的渗透测试靶机有如下两类。

1）Web 漏洞实验平台 OWASP

OWASP 是开放式 Web 应用程序安全项目（Open Web Application Security Project）的简写，它是一个开源的、非营利的全球性安全组织，致力于推动安全标准、安全测试工具、安全指导手册等应用安全技术的发展。OWASP 还提供了一组易受攻击的 Web 应用程序安全项目，这些项目采用虚拟机集成了 SQL 注入、XSS 攻击等类型漏洞，几乎包含了当前全部类型的漏洞。OWASP 由一家非营利性组织——OWASP 基金会提供持续性支持，可在官网上免费下载与使用。

2）渗透靶机平台 Metasploitable

Metasploitable（简称 MSF）的设计目的是为安全工具测试和演示常见漏洞攻击提供一个环境。其中最重要的是它可以作为攻击用的靶机。Metasploitable 开放了很多的高危端口，如 21、23、445 等，而且具有很多未打补丁的高危漏洞，如 Samba MS-RPC Shell 命令注入漏洞等，还对外开放了很多服务，且数据库允

许外联，其系统中的用户口令均为弱口令，同时搭载了 DVWA、Mutillidae 等 Web 漏洞演练平台。

2.2 任务实施

2.2.1 安装攻击机

1. Kali Linux 下载

（1）访问 Kali Linux 的官网进行下载，其界面如图 2-1 所示。

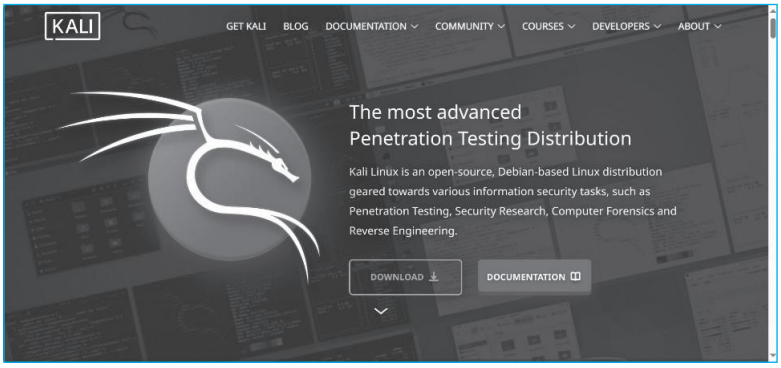

图 2-1 Kali Linux 官网界面

（2）单击“DOWNLOAD”按钮，跳转到 Kali Linux 安装方式选择界面，如图 2-2 所示。

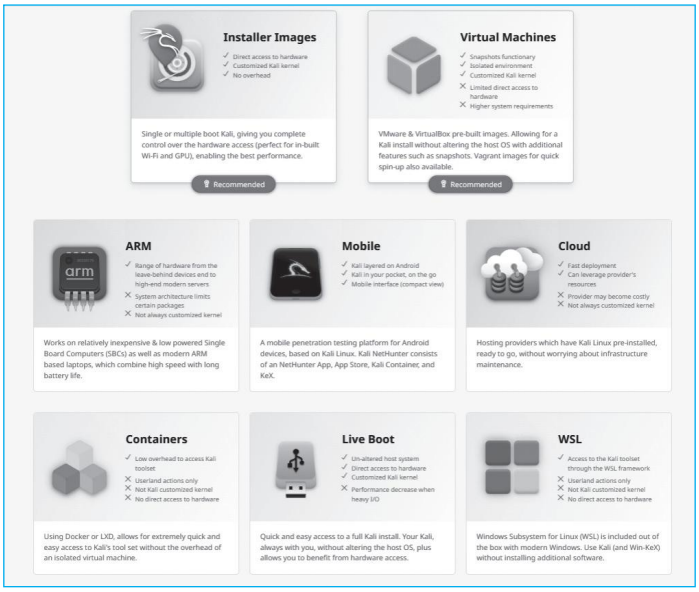

图 2-2 Kali Linux 安装方式选择界面

（3）在 Kali Linux 的安装方式选择界面中，官方根据用户安装方式和运行平台提供了 8 种下载模式，同时官方网站提供了 32 位和 64 位的 ISO 镜像文件。本书以 64 位为例，讲解 Kali Linux 的安装和使用。这里选择以镜像文件的方式安装 Kali Linux 系统。单击 Kali Linux 安装方式选择页面中的“Installer Images”选项，

跳转到 Kali Linux 下载界面，如图 2-3 所示。

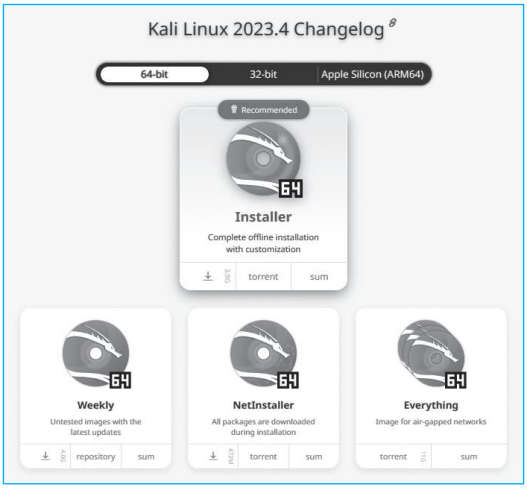

图 2-3 Kali Linux 下载界面

在 Kali Linux 的下载界面中，可以看到另外三个镜像文件旁边带有“Weekly”“NetInstaller”“Everyt hing”等字样，“Weekly”表示使用最新更新的未测试镜像，“NetInstaller”表示安装期间下载所有软件包，“Everyting”则表示包含所有可能的工具。当然，Kali Linux 也自带了配置好的虚拟机文件，单击第一行带“Installer”字样的图标，下载 64 位的 Kali Linux 镜像文件。

2. 创建 Kali Linux 虚拟机

虚拟机（Virtual Machine）是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。虚拟机通过生成现有操作系统的全新虚拟镜像，具有与真实操作系统（包括 Windows 和 Linux）完全一样的功能。当用户进入虚拟系统后，所有操作都是在这个全新的、独立的虚拟系统里面进行的，用户可以独立安装运行软件、保存数据、拥有自己的独立桌面，并且不会对真正系统产生任何影响，而且能够在现有虚拟镜像和真实系统之间灵活切换。

目前最流行的虚拟机软件是 VMware Workstation 和 VirtualBox。下面将以 VMware Workstation 虚拟机软件为例，介绍安装 Kali Linux 的方法。

（1）打开 VMware Workstation 虚拟机软件，在“主页”中单击“创建新的虚拟机”按钮，即可新建虚拟机，如图 2-4 所示。

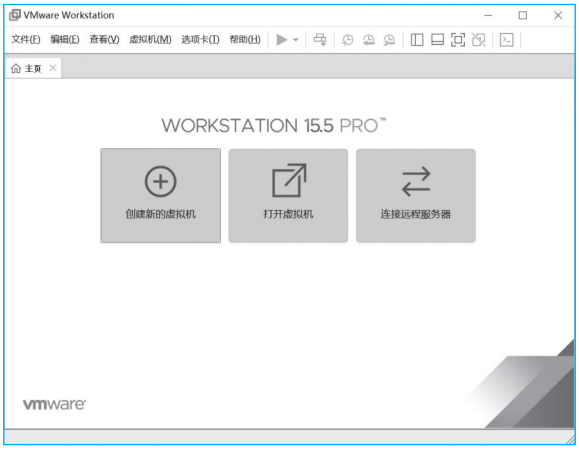

图 2-4 新建虚拟机

（2）在弹出的“欢迎使用新建虚拟机向导”界面中有“典型”和“自定义”两种选项。选“自定义”的方式，单击“下一步”按钮，如图 2-5 所示。

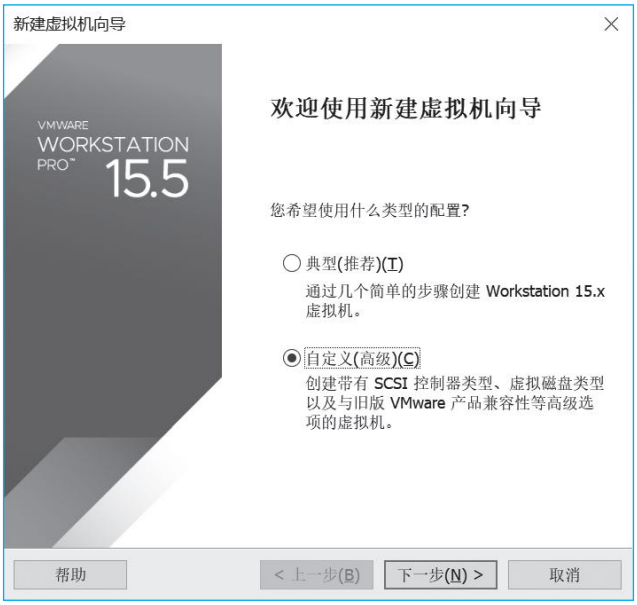

图 2-5　选择虚拟机配置类型

（3）在弹出的“选择虚拟机硬件兼容性”界面中保持默认配置，单击“下一步”按钮，如图 2-6 所示。

图 2-6　选择虚拟机硬件兼容性

（4）在弹出的“安装客户机操作系统”界面中可以选择以哪种安装方式进行安装。选择“稍后安装操作系统”，然后单击“下一步”按钮，如图 2-7 所示。

（5）在弹出的“选择客户机操作系统”界面中，选择“客户机操作系统”选项中的“Linux”选项，因为 Kali Linux 是以 Linux 为基础的发行版；在“版本”下拉选项中选择“其他 Linux 3.x 内核 64 位”选项，然后单击“下一步”按钮，如图 2-8 所示。

图 2-7 选择安装来源

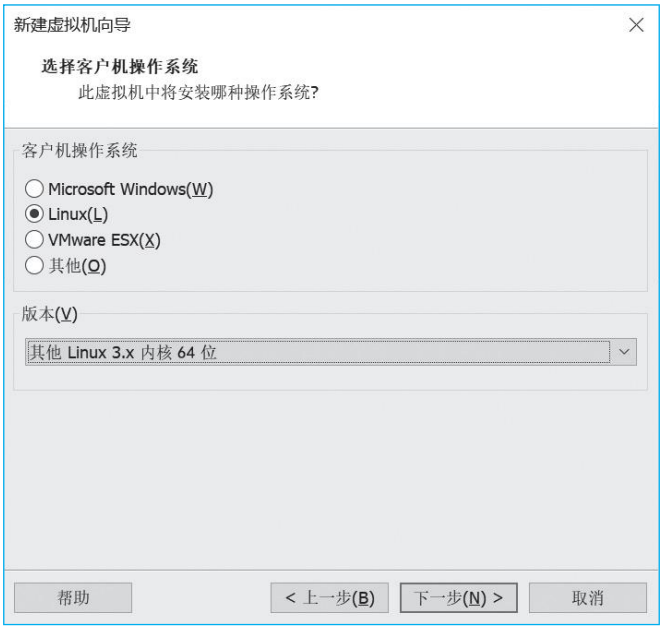

图 2-8 选择客户机操作系统

（6）在弹出的“命名虚拟机”界面的“虚拟机名称”输入框中输入“kali”，把本虚拟机命名为 kali，单击“位置”输入框右边的“浏览”按钮，选择保存虚拟机的位置，这里选择“D:\kali”目录，然后单击“下一步”按钮，如图 2-9 所示。

（7）在弹出的“处理器配置”界面中的“处理器数量”输入框中输入“2”，“每个处理器的内核数量”输入框中输入“2”，这时“处理器内核总数”会显示“4”，表示当前虚拟机 CPU 共有 4 核。可以根据实际需求和物理机（即宿主机）的 CPU 内核数量进行选择，注意虚拟机 CPU 内核数不能超过物理机 CPU 的内核数，否则就会报错。然后单击“下一步”按钮，如图 2-10 所示。

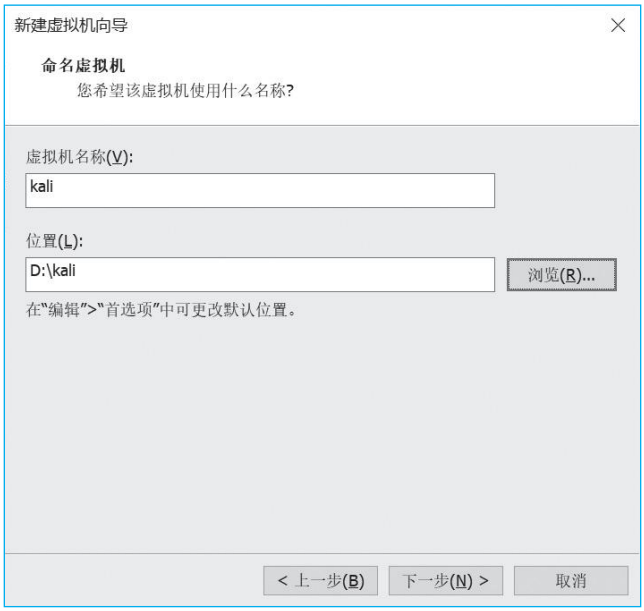

图 2-9　命名虚拟机

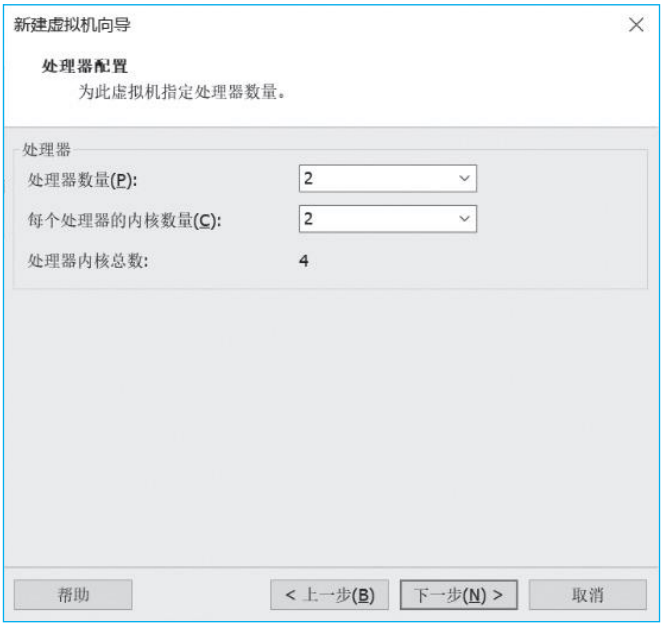

图 2-10　处理器配置

（8）在弹出的“此虚拟机的内存”界面中，把内存设置为 2048MB（2GB），然后单击“下一步”按钮，如图 2-11 所示。

注意

在设置虚拟机的内存时，尽量不要超出宿主机内存的 3/4。

（9）在弹出的“网络类型”界面中，选择“使用网络地址转换”选项，然后单击“下一步”按钮，如图 2-12 所示。

图 2-11 设置虚拟机的内存

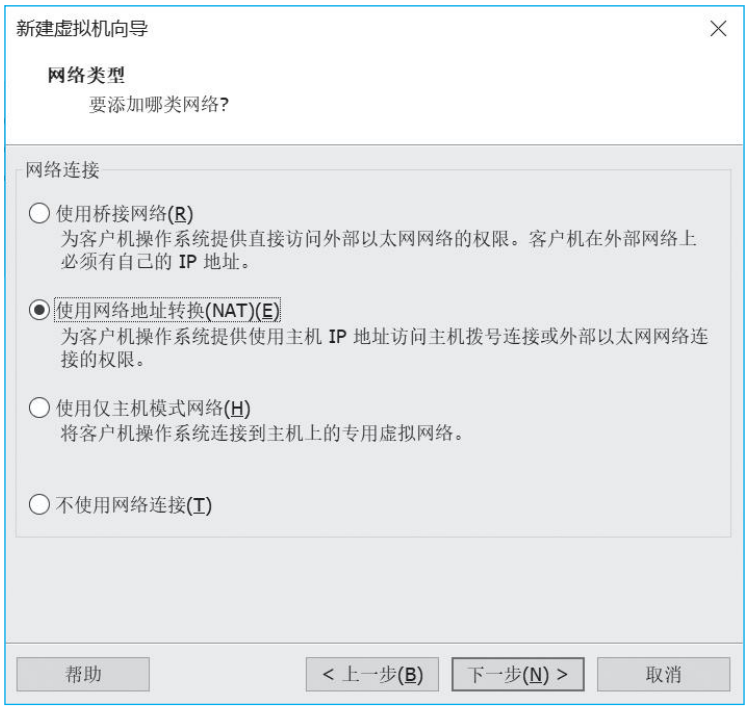

图 2-12 选择网络类型

（10）在弹出的“选择 I/O 控制器类型”界面中，选择“LSI Logic”选项，然后单击“下一步”按钮，如图 2-13 所示。

（11）在弹出的“选择磁盘类型”界面中，选择“SCSI”选项，然后单击“下一步”按钮，如图 2-14 所示。

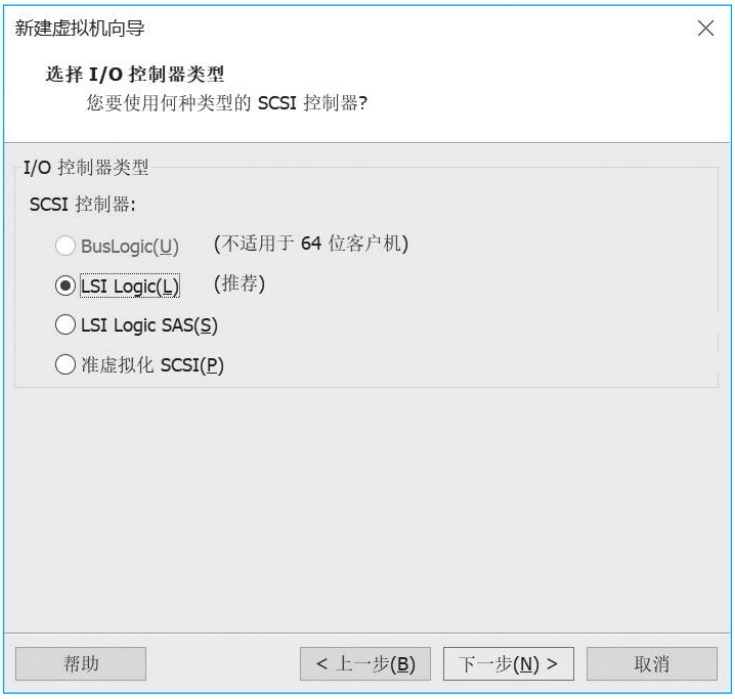

图 2-13 选择 I/O 控制器类型

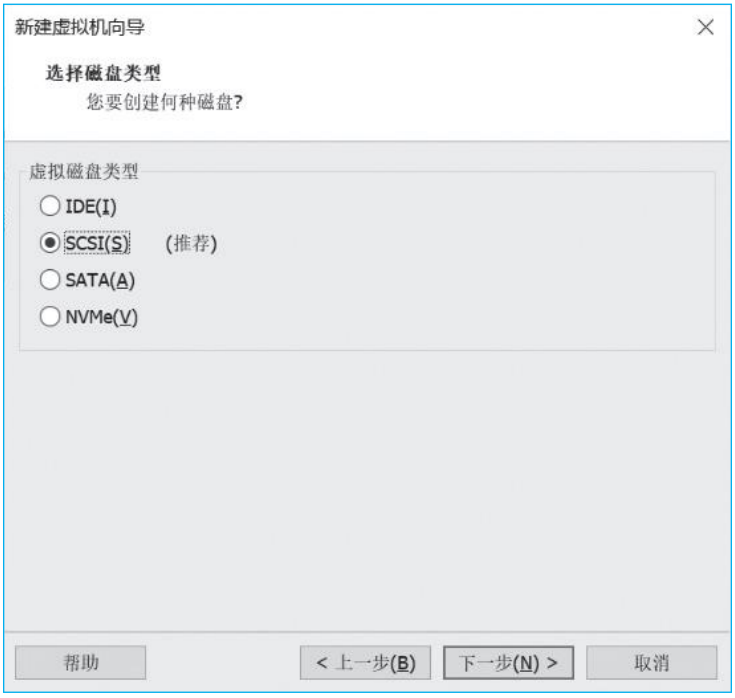

图 2-14 选择磁盘类型

（12）在弹出的“选择磁盘”界面中，选择“创建新虚拟磁盘”选项，然后单击“下一步”按钮，如图 2-15 所示。

（13）在弹出的“指定磁盘容量”界面的“最大磁盘大小”输入框中输入“60”，把虚拟机硬盘大小设置为 60GB，并选择“将虚拟磁盘拆分成多个文件”选项，然后单击“下一步”按钮，如图 2-16 所示。

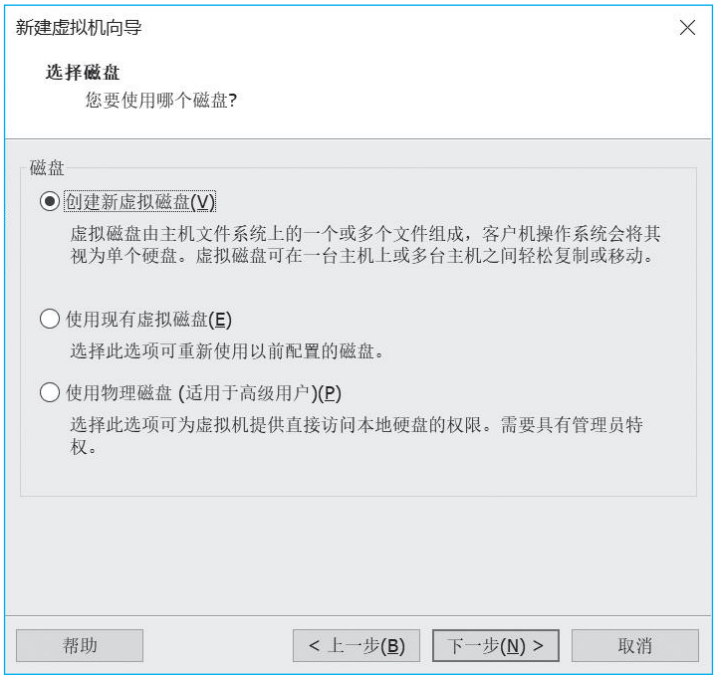

图 2-15 选择磁盘

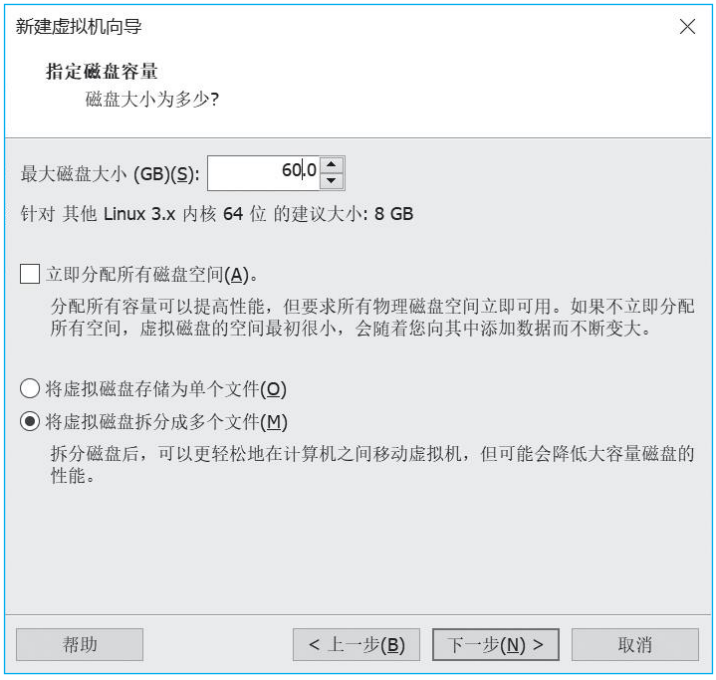

图 2-16 指定磁盘容量

（14）在弹出的“指定磁盘文件”界面的“磁盘文件”输入框中，输入“kali.vmdk”（系统自动输入），然后单击“下一步”按钮，如图 2-17 所示。

（15）在弹出的“已准备好创建虚拟机”界面中，可以看到虚拟机的详细配置，如图 2-18 所示。如果需要对虚拟机的内存、CPU、网络资源进行调整，可以单击“自定义硬件”按钮进入调整窗口。最后，单击“完成”按钮，Kali Linux 虚拟机创建完成。

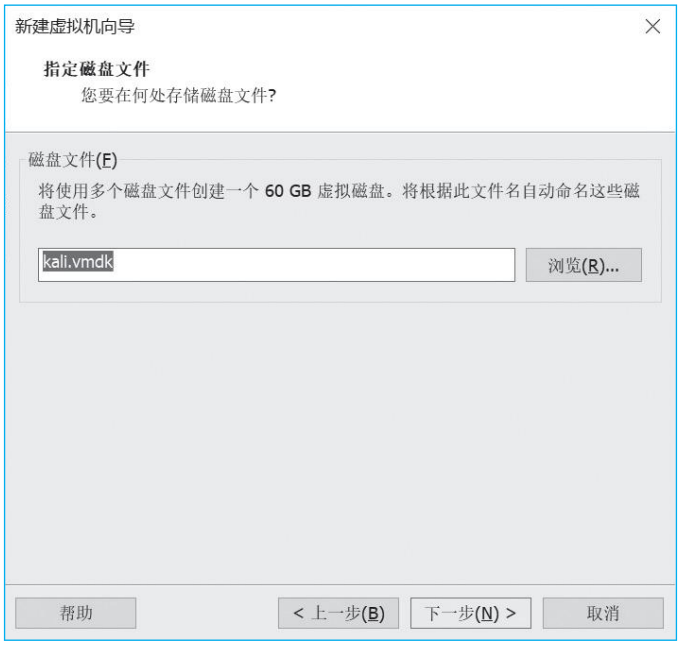

图 2-17　指定磁盘文件

图 2-18　虚拟机的详细配置

此时，一台有 4 个 CPU 内核、2024MB 内存、60GB 硬盘的 Kali Linux 虚拟机便创建成功了。

3. 安装 Kali Linux

（1）Kali Linux 虚拟机创建成功后就要开始安装 Kali Linux 了。在如图 2-18 所示的“已准备好创建虚拟机”的界面上单击“完成”按钮就会进到“虚拟机设置”界面。此时单击“硬件”选项卡中的“CD/DVD”选项，选择页面右侧的“使用 ISO 映像文件”选项，并单击“浏览”按钮，在浏览窗口中选中从官网上下载的 Kali Linux 的 ISO 镜像文件，然后单击“确定”按钮，如图 2-19 所示。

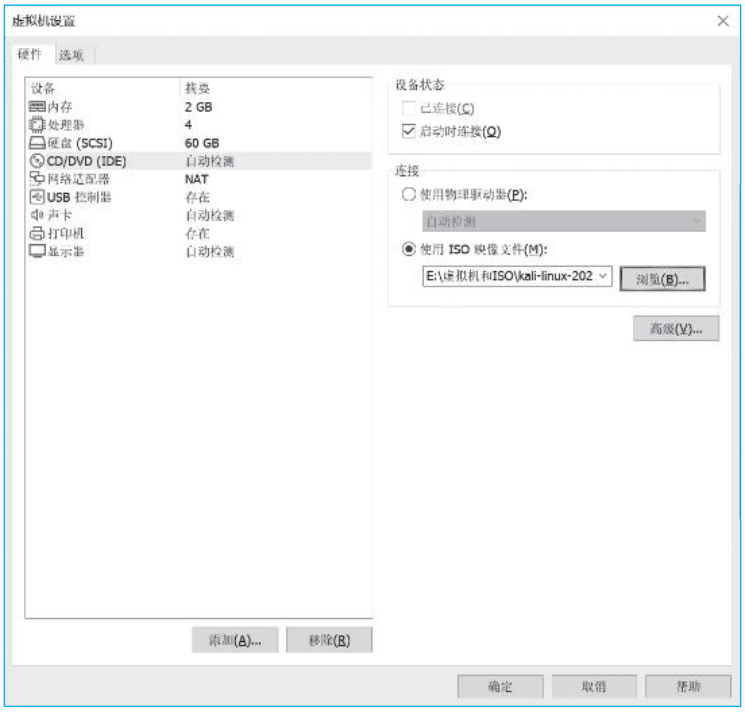

图 2-19 虚拟机设置

（2）经过上述操作，虚拟机会加电启动，进到选择 Kali Linux 安装方式界面。Kali Linux 提供了 5 种安装方式，在这里选择最上面的“Graphical install”（图形界面安装）方式，然后按下回车键开始安装，如图 2-20 所示。

注意

Kali Linux 设计有 25 秒的倒计时，在 25 秒后系统会自动安装。

图 2-20 选择 Kali Linux 安装方式

（3）系统很快就会进到“Select a language”（选择安装语言）界面，选择“Chinese(Simplified)- 中文（简体）”，然后单击“Continue”（继续）按钮，如图 2-21 所示。

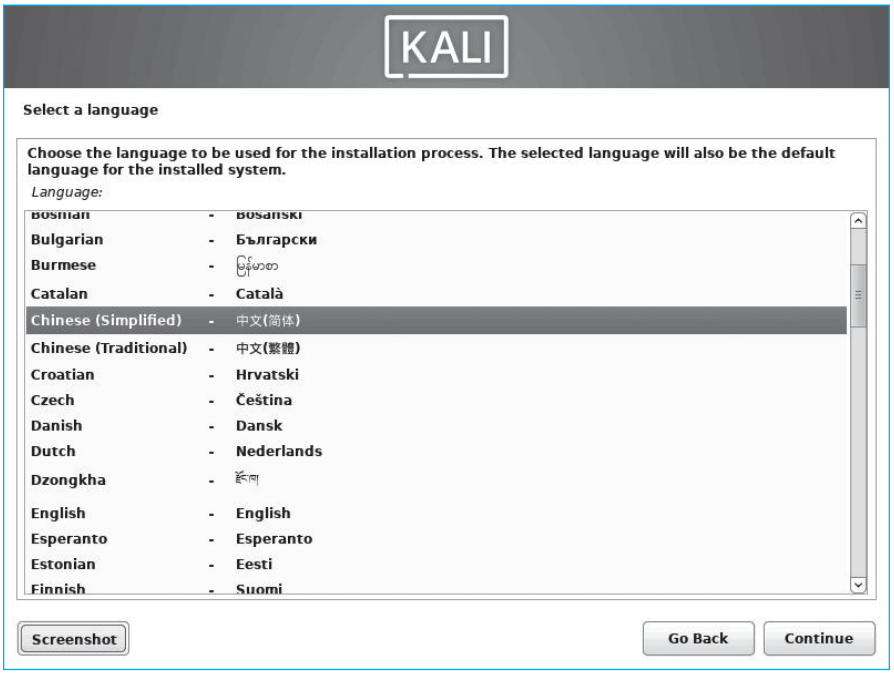

图 2-21　选择安装语言

（4）在选择安装语言为“中文（简体）”后，安装界面的文字就会以简体中文显示。在“请选择您的位置”界面中，选择“中国”，然后单击“继续”按钮，如图 2-22 所示。

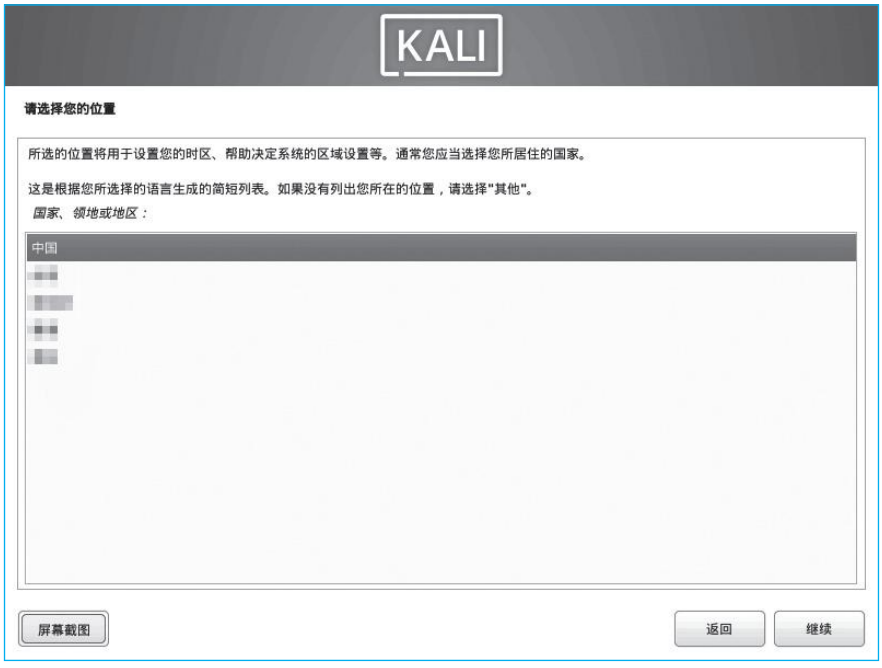

图 2-22　选择所在区域

（5）系统进入“配置键盘”界面，选择“汉语”，然后单击“继续”按钮，如图 2-23 所示。

图 2-23 配置键盘

（6）进入“配置网络”界面，在“主机名”输入框中输入“kali”，也可以输入其他名字，然后单击“继续”按钮，如图 2-24 所示。

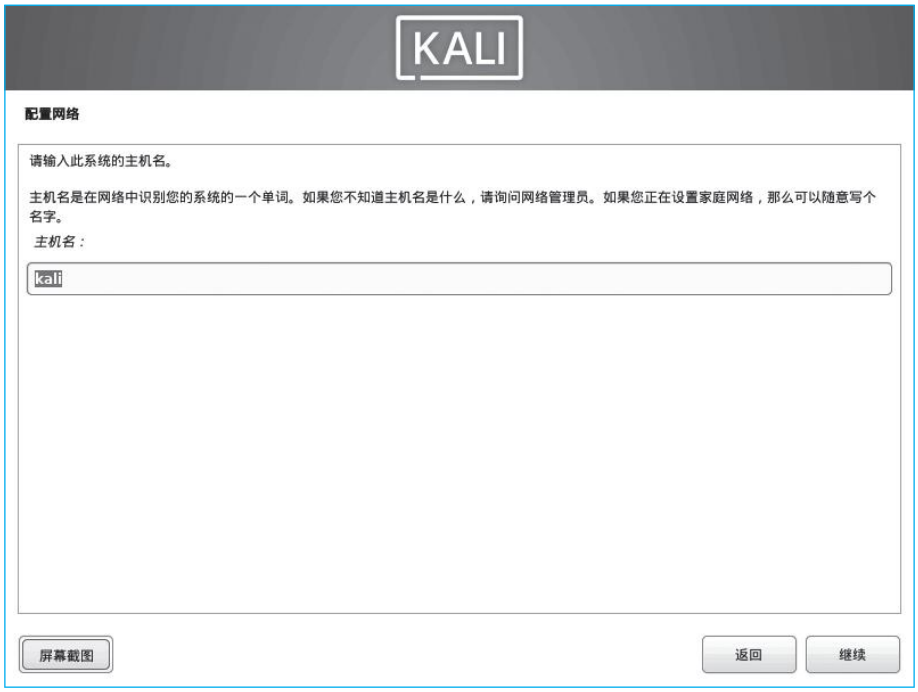

图 2-24 配置网络主机名

（7）进入配置网络域名界面，这里可以不使用域名，也可以输入自己喜欢的域名，然后单击“继续”按钮，如图 2-25 所示。

图 2-25　配置网络域名

（8）进入“设置用户和密码”界面，输入新用户的全名，这是给计算机创建一个用来取代 root 用户执行非管理任务的普通用户账号，可以创建“student”账号，也可以输入自己喜欢的账号，然后单击“继续”按钮，如图 2-26 所示。

图 2-26　输入新用户的全名

（9）进入输入账户的用户名界面，这里同样用“student”创建用户名，也可以输入自己喜欢的用户名，然后单击“继续”按钮，如图 2-27 所示。

图 2-27 输入账户的用户名

（10）进入设置用户密码界面，在密码输入框中输入简单的密码“123456”，给创建的用户设置一个密码，然后单击“继续”按钮，如图 2-28 所示。

图 2-28 设置用户密码

（11）进入“对磁盘进行分区”中的“分区方法”界面，选择默认方式“使用整个磁盘”，然后单击“继续”按钮，如图 2-29 所示。

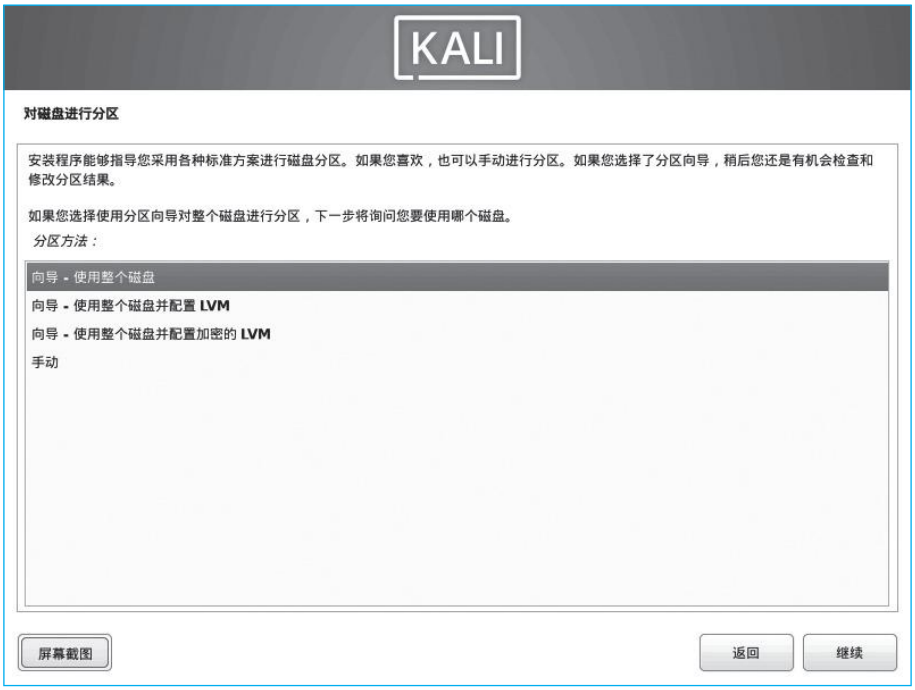

图 2-29　选择磁盘分区方法

（12）进入“对磁盘进行分区”中的“请选择要分区的磁盘”界面，本系统只有 1 块磁盘，所以这里使用默认磁盘就可以了，然后单击“继续”按钮，如图 2-30 所示。

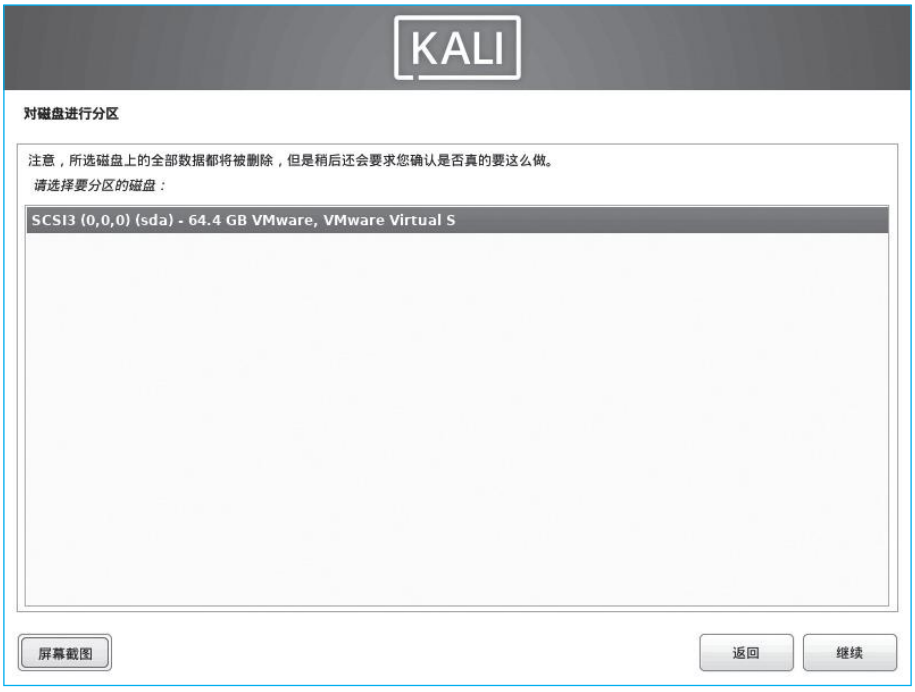

图 2-30　选择要分区的磁盘

（13）进入“对磁盘进行分区”中的“分区方案”界面，选择分区方案。系统提供了 3 种分区方案，这里选择“将所有文件放在同一个分区中”，然后单击“继续”按钮，如图 2-31 所示。

图 2-31 选择磁盘分区方案

（14）进入“对磁盘进行分区”中的“初始化分区表”界面，选择“完成分区操作并将修改写入磁盘”，然后单击“继续”按钮，如图 2-32 所示。如果想要撤销修改分区，可以在该界面选择“撤销对磁盘分区的修改”。

图 2-32 磁盘初始化分区表

（15）进入“对磁盘进行分区”中的“将改动写入磁盘”界面，选择“是”，执行分区操作，把调整后的

分区信息写入磁盘，然后单击“继续”按钮（如果选择“否”，将不执行分区操作），如图 2-33 所示。

图 2-33　把分区信息写入磁盘

（16）进入“软件选择”界面，这里保持默认选项就可以，然后单击“继续”按钮，如图 2-34 所示。

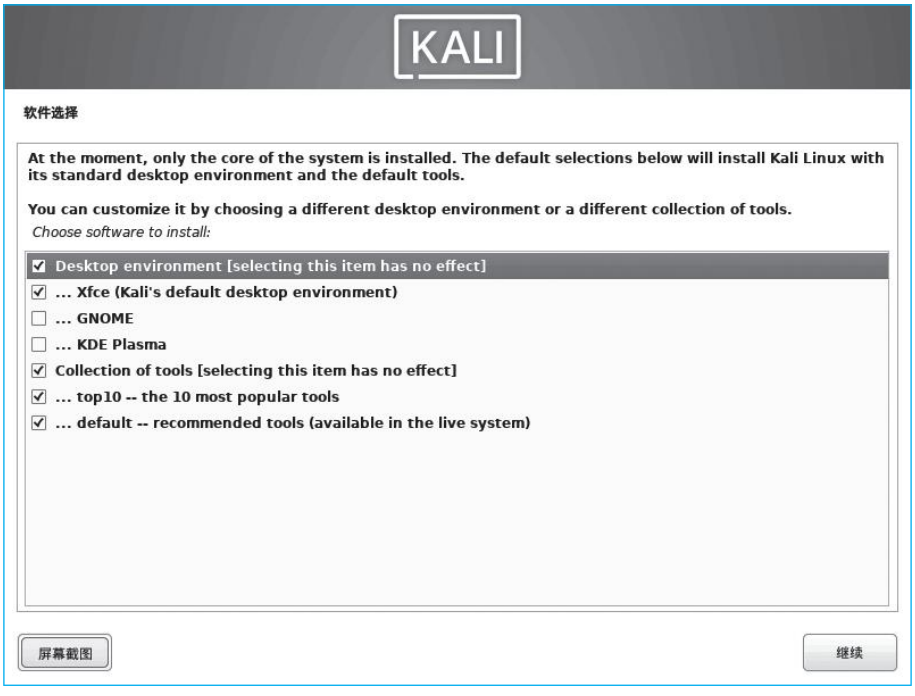

图 2-34　软件选择

（17）进入“安装 GRUB 启动引导器”界面，在该界面中选择“是”，将 GRUB 启动引导器安装到主驱动器上，然后单击“继续”按钮，如图 2-35 所示。

图 2-35 安装 GRUB 启动引导器

（18）进入“安装 GRUB 启动引导器”的“安装启动引导器的设备”界面，选择“/dev/sda”，也就是系统的磁盘，然后单击“继续”按钮，如图 2-36 所示。

图 2-36 选择安装启动引导器的设备

（19）接下来，系统会自动完成所有软件安装，之后进入“结束安装进程”界面，这说明 Kali Linux 系

统及其相关系统安装完毕，重新启动后就可以使用了，单击“继续”按钮后将进入系统，如图 2-37 所示。

图 2-37　结束安装进程

（20）系统重新启动后，进入 Kali Linux 系统登录界面，在这里输入之前设置的用户名“student”和密码“123456”，就可以登录使用了，如图 2-38 所示。

图 2-38　Kali Linux 系统登录界面

至此，Kali Linux 系统就安装成功了。

2.2.2 配置 Kali Linux 系统

1. 启用 root 账号

Kali Linux 中的很多工具都需要使用 root 用户权限（root 是 Linux 中权限最高的用户）才能执行成功，而前面创建的 student 属于普通用户，在每次使用某些工具及功能时，只能在其命令前面加上“sudo”并输入相应的密码才能执行。这个过程比较烦琐，要是切换到 root 用户登录就好了。

Kali Linux 系统默认没有给 root 账号设置密码，因此不能使用 root 账号直接登录。但可以采用如下命令启用 root 账号：

```
$ sudo passwd root
[sudo] password for student:
New password:
Retype new password:
```

具体操作如图 2-39 所示。

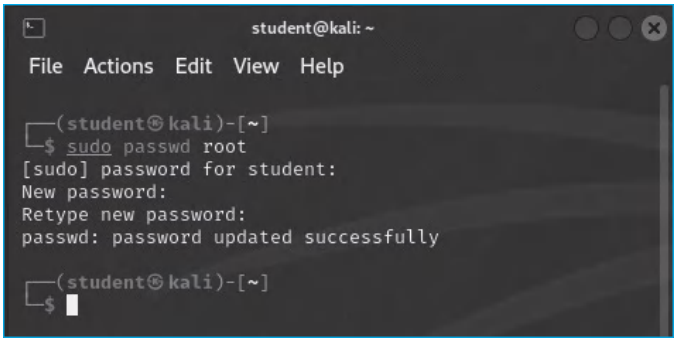

图 2-39 设置 root 用户密码

当屏幕上出现“passwd: password updated successfully”时，表示 root 用户密码设置成功，采用如下命令重启系统：

```
$ sudo reboot
```

重启完成后，打开一个终端，如图 2-40 所示。

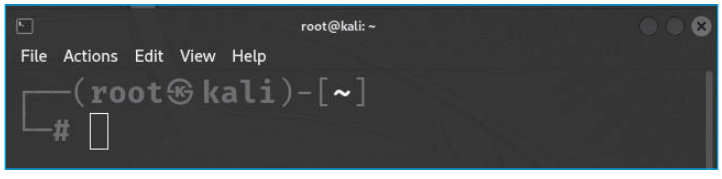

图 2-40 root 用户终端

2. 配置网络

在给 Kali Linux 系统设置网络 IP 地址之前，需要对应用 NAT 模式的 VMnet8 网络地址进行设置，具体操作如下。

打开虚拟机，单击菜单“编辑”选项卡，在弹出来的选项中单击“虚拟网络编辑器”，在弹出的“虚

拟网络编辑器”界面里选中“VMnet8”，然后在“子网 IP”输入框中输入网络地址“10.10.10.0”，在“子网掩码”输入框中输入“255.255.255.0”，然后单击“确定”按钮，完成 VMnet8 网络的网络地址设置，如图 2-41 所示。

图 2-41　VMnet8 网络地址设置

使用 ifconfig 命令可以查看到如下 Kali Linux 虚拟主机网络情况：

```
#ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.128  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::20c:29ff:fe6d:6770  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:6d:67:70  txqueuelen 1000  (Ethernet)
        RX packets 15  bytes 1954 (1.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 4072 (3.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

可以看到主机的网卡名称是 eth0，已经通过 VMware 的 DHCP 功能设置的 IP 地址为 10.10.10.128，子网掩码是 255.255.255.0，但该 IP 地址并不是我们拓扑上指定的 IP 地址 10.10.10.127/24，用命令 vi /etc/network/interfaces 可以编辑该网卡的配置文件。

在编辑界面上输入如下代码：

```
auto eth0
iface eth0 inet static                    // 配置 eth0 使用默认的静态地址
address 10.10.10.127                      // 设置 eth0 的 IP 地址
```

```
netmask 255.255.255.0          // 配置 eth0 的子网掩码
gateway 10.10.10.2             // 配置当前主机的默认网关
```

保存并退出 vi 编辑器（:wq 命令），然后输入如下重启网络命令：

```
# systemctl restart networking.service
```

重启网络后，可以用 ifconfig 命令查看 IP 地址是否是 10.10.10.127。

3. 配置更新源

Kali Linux 中的工具种类繁多，其中包含很多需要及时更新的工具，而且 Kali Linux 系统的环境也需要更新。

Kali Linux 采用了滚动更新的方式。所谓滚动更新是指在软件开发中，将更新内容发送到软件而不需要重新安装。Kali Linux 的更新需要用到 apt 安装包管理工具，当使用其他软件更新的源地址时，需要先修改更新源地址。

所谓的 Kali Linux 系统的更新源，可以将它理解为软件仓库，系统通过它安装和更新软件。更新源的服务器地址写在 /etc/apt/sources.list 文件中。

由于 Kali Linux 系统默认配置的是国外更新源，在国内使用国外的更新源通常会比较慢，甚至无法使用，这时就需要更换成国内的更新源。国内著名的 Kali Linux 更新源有中科大 Kali 镜像源和阿里云 Kali 镜像源。

用命令 vi /etc/apt/sources.list 打开 Kali Linux 更新源文件。将原有 Kali 更新源内容删除或使用“#”对原有第二行内容进行注释，代码如下：

```
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
# deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
# Additional line for source packages
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware
```

然后将国内源写入文件并保存。本教材以阿里云 Kali 镜像源为例进行演示，代码如下：

```
deb http://mirrors.aliyun.com/kali kali-rolling main non-free contrib
deb-src http://mirrors.aliyun.com/kali kali-rolling main non-free contrib
```

保存退出后，尝试对系统进行更新，观察系统是否采用阿里云 Kali 镜像源对系统进行更新，部分代码如下：

```
# apt-get update
Get:1 http://mirrors.aliyun.com/kali kali-rolling InRelease [41.5 kB]
Get:2 http://mirrors.aliyun.com/kali kali-rolling/main Sources [16.0 MB]
Get:3 http://mirrors.aliyun.com/kali kali-rolling/contrib Sources [83.5 kB]
```

在软件包更新完成后，可以继续更新系统包。输入命令 apt-get dist-upgrade -y 更新系统，部分代码如下：

```
# apt-get dist-upgrade -y
Reading package lists... Done
```

```
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
```

在更新完系统后，重启 Kali Linux 即可。

2.2.3 搭建 OWASP 靶机

1. 认识 OWASP

OWASP（开放式 Web 应用程序安全项目）是一个享有盛誉的国际非营利组织，在 Web 应用程序安全领域以其权威性和丰富的专业知识而著称。它专注于开源的软件安全研究，并为全球安全社区提供技术支持和资源。OWASP 的使命是推动软件安全研究，并提供实用的测试程序和代码审查指南，以帮助开发人员增强软件的安全性，同时帮助企业和组织识别和决策应用安全风险。

随着信息安全意识的提高，OWASP 在中国的影响力也在迅速增长，吸引了大量中国安全专家和工程师的参与，这不仅加强了本地社区建设，而且促进了国际知识交流与合作。

2. 配置 OWASP 靶机

下载好相关资源文件后，解压 OWASP 靶机文件。因为 OWASP 靶机文件是虚拟机文件，所以直接用虚拟机软件 VMware Workstation 打开即可。

注意

需将 OWASP 靶机的网络适配器改成与 Kali Linux 一样。本教材的 Kali Linux 网络适配器是 NAT 模式的，所以 OWASP 靶机也要是 NAT 模式的。

配置完毕后，启动 OWASP 靶机，即可进入如图 2-42 所示的系统界面。

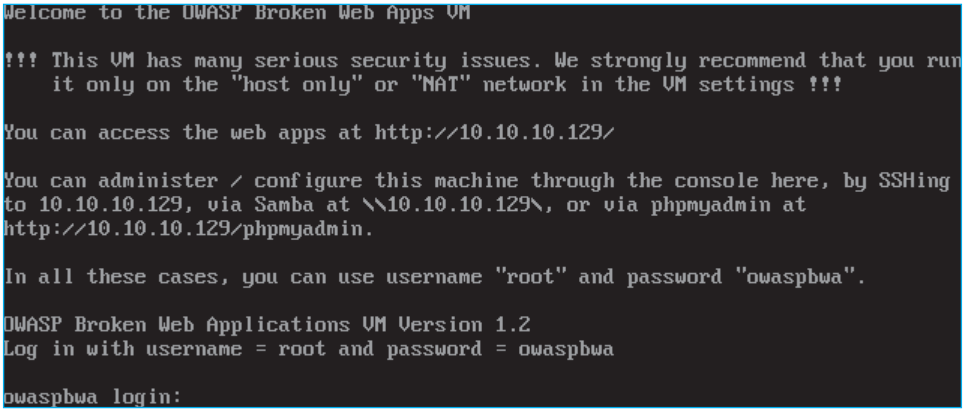

图 2-42　OWASP 靶机的系统界面

此时，系统要求输入用户名和密码。OWASP 靶机的默认用户名为 root，默认密码为 owaspbwa，输入后即可登录成功，如图 2-43 所示。

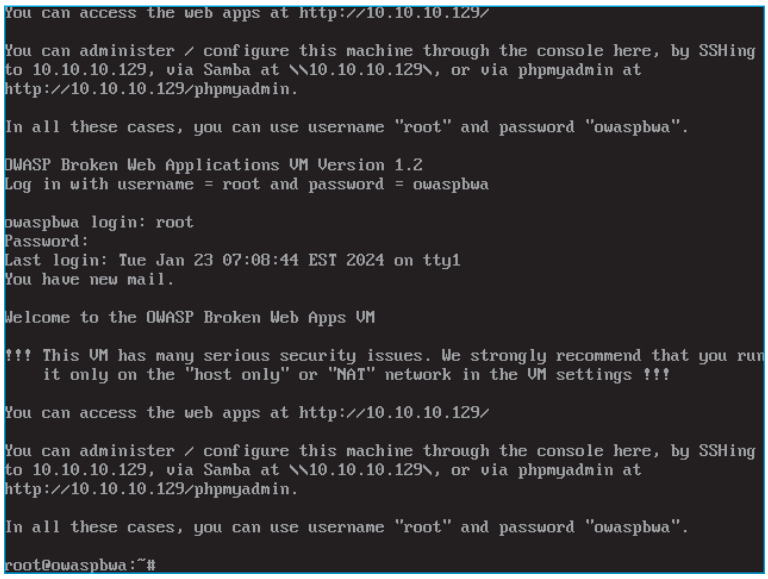

图 2-43 成功登录 OWASP 靶机系统

用命令 vi /etc/network/interfaces 可以编辑网卡的配置。在网卡配置的编辑界面上输入如下代码：

```
auto eth0
iface eth0 inet static          // 配置 eth0 使用默认的静态地址
address 10.10.10.129            // 设置 eth0 的 IP 地址
netmask 255.255.255.0           // 配置 eth0 的子网掩码
gateway 10.10.10.2              // 配置当前主机的默认网关
```

编辑完成后，按下 Esc 键退出编辑模式，使用 :wq 命令，保存退出 vi 编辑器。

用命令 ifconfig eth0 10.10.10.129 netmask 255.255.255.0 也可以修改 OWASP 靶机的 IP 地址。

在浏览器中，输入靶机系统的地址“10.10.10.129”，即可进入 OWASP 靶机系统的 Web 界面，如图 2-44 所示。

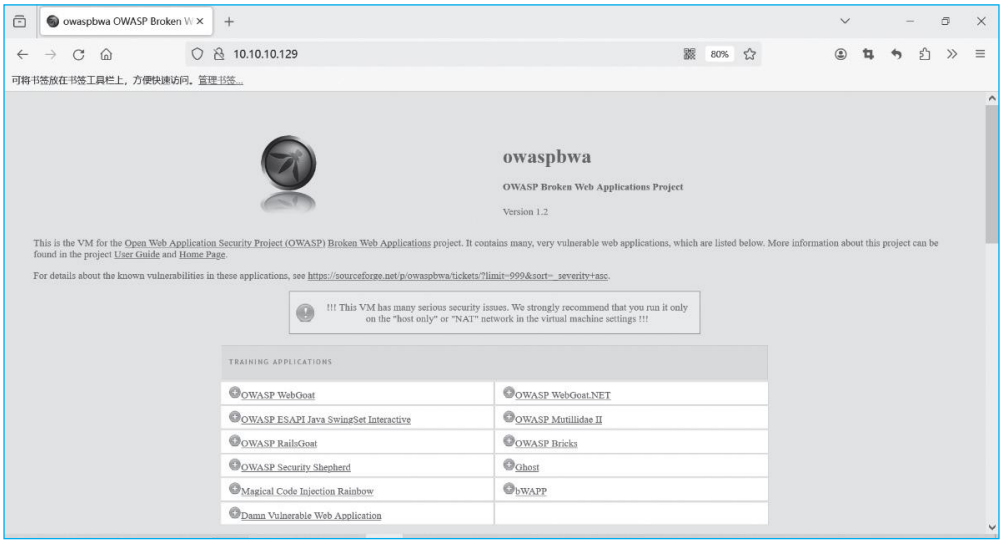

图 2-44 OWASP 靶机系统的 Web 界面

至此，OWASP 靶机环境已经全部部署好，可以直接使用了。

项目小结

在本项目中，介绍了什么是渗透测试，Kali Linux 的下载、安装和基本配置方法，以及如何搭建 OWASP 靶机进行实验。这些内容可以帮助我们更好地理解渗透测试的流程和攻击流量。

拓展阅读

拓展阅读 2

巩固练习

1. 选择题

（1）渗透测试有（　　）、白盒和灰盒三种测试方法。

A. 黄盒　　B. 黑盒　　C. 绿盒　　D. 盲盒

（2）渗透测试是一种通过模拟恶意（　　）的攻击方法，来评估计算机网络系统安全的评估方法。

A. 红客　　B. 黑客　　C. 客户　　D. 技术员

（3）Kali Linux 系统在提示符 $ 后面输入下面哪条命令可以给 root 用户设置密码？（　　）

A. sudo passwd root　　B. passwd root

C. sudo passwd root 1234　　D. passwd root 1234

（4）在 Kali Linux 系统中，哪条命令能查看 IP 地址？（　　）

A. ifconfig　　B. ipconfig　　C. address　　D. arp

（5）OWASP 靶机默认登录用户的用户名是 root，那默认登录密码是（　　）。

A. password　　B. owasp　　C. admin　　D. owaspbwa

2. 简答题

（1）什么是渗透测试？渗透测试平台有哪些？请写出 3 个。

（2）什么是渗透测试靶机？

（3）标准渗透测试流程有几个阶段，分别是什么？

3. 操作题

请根据所学的知识，按照表 2-1 和测试平台网络拓扑图（图 2-45）提供的信息，将网络拓扑图重画一遍，并完成所有主机的安装和配置。

表 2-1　虚拟机配置

序号	角色	平台	IP 地址	网络
1	攻击机	Kali Linux	10.10.10.127/24	NAT
2	靶机	Linux	10.10.10.128/24	NAT

续表

序号	角色	平台	IP 地址	网络
3	靶机	OWASP	10.10.10.129/24	NAT
4	靶机	Win 7	10.10.10.130/24	NAT
5	靶机	Win 10	10.10.10.131/24	NAT
6	网关、DNS	—	10.10.10.2/24	NAT

在物理机上安装 VMware Workstation 虚拟机软件，并用 VMware Workstation 安装其他相应的平台，其网络连接如图 2-45 所示。

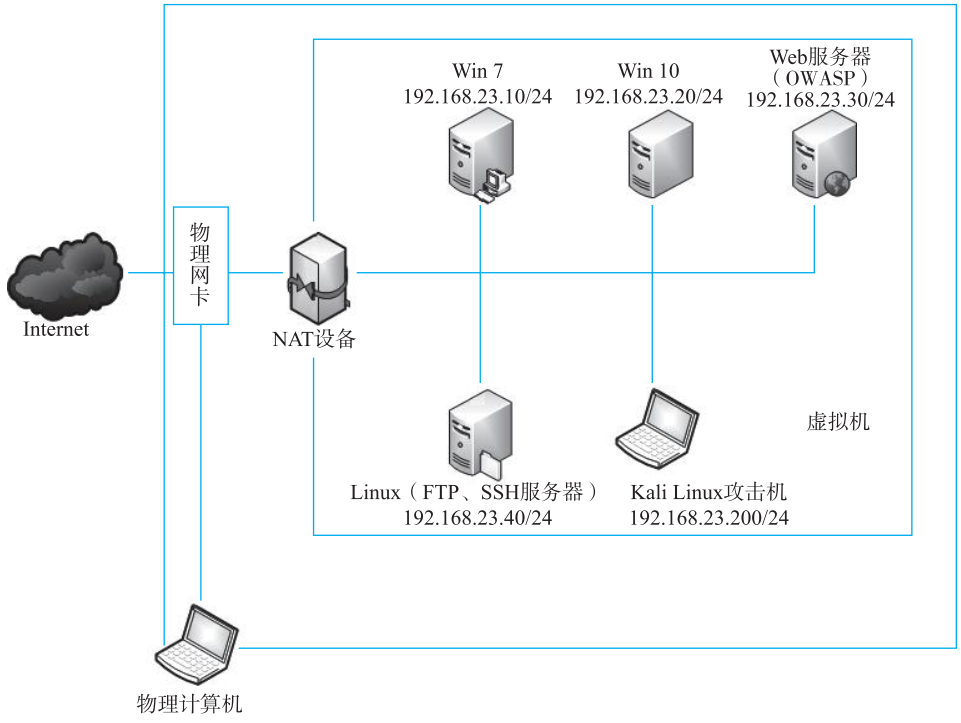

图 2-45 测试平台网络拓扑图