教育部师资实践基地系列教材——信息与网络安全

DCN | 神州数码 Digital China

网络安全项目实践

徐雪鹏　主编

全国职业技能大赛推荐参考书
神州数码网络认证指定教材
校企合作新课改教材

机械工业出版社
CHINA MACHINE PRESS

网络安全项目实践

主　编　徐雪鹏
副主编　岳大安　孙雨春
参　编　赵　飞　包　楠　张　鹏　李晓隆

机械工业出版社

本书是神州数码技能教室项目的配套指导教材，也是信息安全实践基地的指定训练教材。本书共4章，分别为网络安全基本理论、局域网安全、防火墙和虚拟专用网络安全。

本书可作为各类职业院校信息安全专业的教材，也可作为信息安全从业人员的参考用书。

如果选用本书的教师需要配套电子课件，可以从机械工业出版社教育服务网（www.cmpedu.com）免费注册下载或联系编辑（010-88379194）咨询。

图书在版编目（CIP）数据

网络安全项目实践/徐雪鹏主编. —北京：机械工业出版社，2017.4

教育部师资实践基地系列教材. 信息与网络安全

ISBN 978-7-111-56396-9

Ⅰ. ①网… Ⅱ. ①徐… Ⅲ. ①计算机网络—网络安全—教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2017）第059669号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）

策划编辑：梁 伟 责任编辑：李绍坤 范成欣

责任校对：马立婷 封面设计：鞠 杨

责任印制：李 飞

北京机工印刷厂印刷（三河市南杨庄国丰装订厂装订）

2017年5月第1版第1次印刷

184mm×260mm · 10.25印张 · 231千字

0 001—2000册

标准书号：ISBN 978-7-111-56396-9

定价：29.80元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务 网络服务

服务咨询热线：（010）88379833 机 工 官 网：www.cmpbook.com

读者购书热线：（010）88379649 机 工 官 博：weibo.com/cmp1952

教育服务网：www.cmpedu.com

封面无防伪标均为盗版 金 书 网：www.golden-book.com

前　言

当前，信息技术产业欣欣向荣，处于空前繁荣的阶段，但是危害信息安全的事件也在不断发生，信息安全的形势非常严峻，黑客入侵、利用计算机实施犯罪、恶意软件侵扰、隐私泄露等，是我国信息网络空间面临的主要威胁和挑战。我国已经成为世界信息产业大国，但是还不是信息产业强国，在信息产业的基础性产品研制、生产方面还比较薄弱，例如，现在我国计算机操作系统等基础软件和 CPU 等关键性集成电路还部分依赖国外的产品，这就使得我国的信息安全基础不够牢固。

随着计算机和网络在军事、政治、金融、工业、商业等行业部门的广泛应用，社会对计算机和网络的依赖越来越大，如果计算机和网络系统的安全受到破坏，不仅会带来巨大的经济损失，还会引起社会的混乱。因此，确保以计算机和网络为主要基础设施的信息系统的安全已成为世人关注的社会问题和信息科学技术领域的研究热点。当前，我国正处在全面建成小康社会的决定性阶段，实现我国社会信息化并确保信息安全是我国全面建成小康社会的必要条件之一。而要实现我国社会信息化并确保信息安全的关键是人才，这就需要我们培养规模宏大，素质优良的信息化和信息安全人才队伍。

2014 年，习近平主席在中央网络安全与信息化领导小组会议上指出：没有网络安全就没有国家安全，没有信息化就没有现代化。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建成网络强国。

“十三五”时期，我国要积极推动网络强国建设。网络强国涉及技术、应用、文化、安全、立法、监管等诸多方面，不仅要突出抓好核心技术突破，还要提供更加安全可靠的软硬件支撑，加快建设高速、移动、安全、泛在的新一代信息基础设施，在不断推进新技术新业务应用，繁荣发展互联网经济的同时，要强化网络和信息安全，而培育高素质人才队伍是实施网络强国战略的重要措施。2015 年，国务院学位委员会和教育部增设“网络空间安全”一级学科。我国信息安全学科建设和人才培养，迎来了全面高速发展的新阶段。

本书以培养学生的职业能力为核心，以工作实践为主线，以项目为导向，采用任务驱动、场景教学的方式，面向企业信息安全工程师人力资源岗位设置教材内容，建立以实际工作过程为框架的职业教育课程结构。本书共有 4 章，分别为网络安全基本理论、局域网安全、防火墙、虚拟专用网络安全。

第 1 章：网络安全基本理论，主要介绍了网络安全模型、网络攻击的分类、黑客的分类以及黑客入侵思路。

第 2 章：局域网安全，主要介绍了 MAC 攻击及其解决方案、DHCP 攻击及其解决方案、ARP 攻击及其解决方案、生成树攻击及其解决方案、VLAN 攻击及其解决方案、Routing Protocol 攻击及其解决方案、LAN 非授权访问攻击及其解决方案。

第 3 章：防火墙，主要介绍了 IP 应用非授权访问攻击及其解决方案、DoS/DDoS 攻击及其解决方案。

第 4 章：虚拟专用网络安全，主要介绍了网络被动监听攻击及其解决方案、IPSec VPN、IKE、SSL VPN。

本书由徐雪鹏担任主编，岳大安和孙雨春任副主编，参加本书编写的还有赵飞、包楠、张鹏和李晓隆。

由于编者水平有限，书中难免存在不当和疏漏之处，敬请读者批评指正。联系方式 ceo@knowskill.com。

编者

登场人物介绍：

小李（姓名李子涛）：小李从小就对数字不敏感，小学时数学简单，他凭着一点小聪明还可以混个不错的分数，上了中学他还被不明真相的数学老师选中参加市里的华罗庚数学金杯赛。然而当小李沉着地看完试卷之后，才发现原来自己只知道“考生姓名”和“考生学校”这两个问题的答案。自此之后，小李终于彻头彻尾地明白了自己的终极归宿。高中毕业之后，小李的第一志愿不幸落空，他满腹悲愤地进入了一所理工大学的计算机系。小李一心向文，结果却要去学技术含量很高的计算机。更加让人想不到的是，命运对他眷顾良多，小李大学毕业后竟然被 TaoJin（韬金）电子商务公司录取。从业几年之后，小李居然也对计算机有了一点自己的心得，这也算是他人生中一段“东隅桑榆”的际遇。

Yueda（岳总，姓名岳大安）：Yueda 是 TaoJin（韬金）电子商务公司的 CSO（Chief Security Officer，首席安全官），主要负责监控、协调公司内部的信息安全工作，还负责制定公司安全措施和安全标准。此外，Yueda 还需要经常举办或参加相关领域的活动，如参与业务连续性、预防损失、诈骗预防和保护隐私等议题的相关活动。

Mr.White（白先生）：黑客并非都是黑的，那些用自己的黑客技术来做好事的黑客们叫“白帽黑客”。Mr.White（白先生）在某安全公司工作，负责检测计算机系统的安全性。Mr.White（白先生）被 TaoJin（韬金）电子商务公司首席安全官 Yueda 聘请来测试 TaoJin（韬金）电子商务公司的系统，以便进行安全审查。

故事梗概：

Yueda 为对 TaoJin（韬金）电子商务公司的系统进行全面的安全审查，聘请了某安全公司的白帽黑客 Mr.White 对系统进行了全面的渗透测试。渗透测试就是为了证明网络防御按照预期计划正常运行而提供的一种机制。不妨假设，公司定期更新安全策略和程序，时时给系统安装补丁程序，并采用了漏洞扫描器等工具，以确保所有补丁程序都已安装好。如果早已做到了这些，那么为什么还要请外方进行审查或渗透测试呢？因为渗透测试能够独立地检查网络策略，也就是给系统安了一双“眼睛”，保障公司对抗黑客对系统攻击的网络防御策略是有效的。通过 Mr.White 对系统进行了一系列的渗透测试，Yueda 指导员工小李实施了一系列安全有效的网络防御策略。

目　录

第1章　网络安全基本理论

场景

TaoJin（韬金）电子商务公司首席安全官 Yueda 要面向社会招聘若干网络安全工程师，负责公司内部的信息安全工作。Yueda 将招聘需求提交至 TaoJin（韬金）公司人力资源部，招聘需求如下。

岗位职责：

1．负责对客户网络、系统进行安全评估和安全加固。

2．在出现网络攻击或安全事件时，提供紧急响应服务，帮助用户恢复系统及调查取证。

3．针对客户网络架构，提出合理的网络安全解决方案。

4．能够解决客户日常安全问题。

5．负责完成领导交办的其他工作。

任职条件：

1．精通网络通信 TCP/IP、Windows 操作系统、Linux 操作系统。

2．至少懂得一种 Web 开发语言（PHP、Java、ASP.NET）。

3．精通网络安全技术，深入了解基础网络安全、防火墙、VPN（Virtual Private Network，虚拟专用网络）、WAF（Web Application Firewall，网站应用级入侵防御系统）、IPS（Intrusion Prevention System，入侵防御系统）、FS、系统加固等安全技术。

4．具备较强的撰写技术文档、技术分析报告及提供解决方案、评审技术方案的能力。

5．具有责任感、团队合作精神及沟通能力，具有较强的学习能力及自我管理能力。

小李在前程无忧网站看到了招聘需求，便投了简历。TaoJin（韬金）人力资源部专员看到了小李的简历，便电话通知小李前来公司面试。

面试前几天，小李认真地阅读了任职条件中的每一条要求，他想起任职条件中的每一条在学校上学时都学过相应的知识，便将当初上课时候用过的书和笔记统统翻了出来，对照着每条要求，进行了认真复习和准备。

1.1　网络安全的重要性

场景

小李到 TaoJin（韬金）公司面试的那天，面试小李的面试官为 Yueda。Yueda 问小李的第一个问题是：“请你说一说我们公司为什么需要信息安全，换句话说，你觉得我们公司为什么聘用你？”

小李想起来当时在学校上网络安全课时，老师曾经讲过的关于网络安全基本理论的几

张 PPT，他的回答如下：

第一，从网络结构上来说，过去的网络是封闭的，没有 Internet 的入口点；而现在的网络有很多互联网的入口点，自然有风险，所以需要网络安全。

第二，从黑客技术上来说，过去要实施一些简单的网络攻击，需要很多的知识，如网络编程。现在我们能够很轻松地获取各种攻击软件、渗透测试套件，有些软件只需要知道怎么用就行了，无须知道原理，这样就可以很轻松发起网络攻击。

第三，从资产价值来看，过去计算机上的数据并没有太多的价值。例如，我上学时计算机里的游戏、MP3、图片等，就算丢失也无所谓。现在不一样了，尤其是电子商务出现以后，对于电子商务公司来说，数据对于公司而言至关重要，需要保障持续地为客户服务。

Yueda：不错，现在我们公司就是这样一家电子商务公司，恰恰需要网络安全方面的人才帮助我们解决一系列的问题。

理论：网络安全的重要性

信息是信息论中的一个术语，常常把消息中有意义的内容称为信息。1948 年，美国数学家、信息论的创始人仙农在题为“通讯的数学理论”的论文中指出：“信息是用来消除随机不定性的东西”。1948 年，美国著名数学家、控制论的创始人维纳在《控制论》一书中，指出：“信息就是信息，既非物质，也非能量。”

安全是指不受威胁，没有危险、危害、损失，人类的整体与生存环境资源的和谐相处，互相不伤害，不存在危险的危害的隐患，是免除了不可接受的损害风险的状态。安全是在人类生产过程中，将系统的运行状态对人类的生命、财产、环境可能产生的损害控制在人类能接受水平以下的状态。

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。信息安全主要包括以下 5 个方面的内容，即需保证信息的保密性、真实性、完整性、未授权复制和所寄生系统的安全性。

信息安全的根本目的就是使内部信息不受外部威胁，因此信息通常要加密。为保障信息安全，要求有信息源认证、访问控制，不能有非法软件驻留，不能有非法操作。

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。根据国际标准化组织的定义，信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。信息安全是任何国家、政府、部门、行业都必须十分重视的问题。但是，对于不同的部门和行业来说，其对信息安全的要求和重点却是有区别的。

随着科技的发展各方面信息量的急剧增加，并要求大容量、高效率地传输这些信息。为了适应这一形势，通信技术发生了前所未有的“爆炸性”发展。目前，除有线通信外，短波、超短波、微波、卫星等无线电通信也正在越来越广泛地应用。

日益繁多的事情托付给计算机来完成，敏感信息正经过脆弱的通信线路在计算机系统之间传送，专用信息在计算机内存储或在计算机之间传送，电子银行业务使财务账目可以通过通信线路查阅，执法部门从计算机中了解罪犯的前科，医生们用计算机管理病历，所有这一切，最重要的问题是不能在非法（非授权）获取（访问）不加防范的条件下传输信息。

传输信息的方式有很多，有局域网、互联网和分布式数据库，有蜂窝式无线、分组交换式无线、卫星电视会议、电子邮件及其他各种传输技术。信息在存储、处理和交换过程中，都存在泄密或被截收、窃听、篡改和伪造的可能性。不难看出，单一的保密措施已很难保证通信和信息的安全，必须综合应用各种保密措施，即通过技术的、管理的、行政的手段，实现信源、信号、信息3个环节的保护，藉以达到信息安全的目的。

信息安全本身包括的范围很大。大到国家军事政治等机密安全，小到如防范商业企业机密泄露、防范青少年对不良信息的浏览、防范个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、信息认证、数据加密等），直至安全系统，其中任何一个安全漏洞便可以威胁全局安全。信息安全服务至少应该包括支持信息网络安全服务的基本理论以及基于新一代信息网络体系结构的网络安全服务体系结构。

在计算机领域中，网络就是用物理链路将各个孤立的工作站或主机连在一起，组成数据链路，从而达到资源共享和通信的目的。凡是将地理位置不同并具有独立功能的多个计算机系统通过通信设备和线路而连接起来，且以功能完善的网络软件（网络协议、信息交换方式及网络操作系统等）实现网络资源共享的系统，都可以称为计算机网络。

网络的安全是指通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。网络安全的具体含义会随着“角度”的变化而变化。例如，从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护。

网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

随着计算机技术的迅速发展，在计算机上处理的业务也由基于单机的数学运算、文件处理以及基于简单连接的内部网络的内部业务处理、办公自动化等发展到基于复杂的内部网（Intranet）、企业外部网（Extranet）、全球互联网（Internet）的企业级计算机处理系统和世界范围内的信息共享和业务处理。在系统处理能力提高的同时，系统的连接能力也在不断提高。但在连接能力、流通能力提高的同时，基于网络连接的安全问题也日益突出，整体的网络安全主要表现在以下几个方面：网络的物理安全、网络拓扑结构安全、网络的系统安全、应用系统安全和网络管理的安全等。

通常，系统安全与性能和功能是一对矛盾的关系。如果某个系统不向外界提供任何服务（断开），则外界对其是不可能构成安全威胁的。但是，企业接入国际互联网络，提供网上商店和电子商务等服务，等于将一个内部封闭的网络建成了一个开放的网络环境，各种安全包括系统级的安全问题也随之产生。

构建网络安全系统，一方面由于要进行认证、加密、监听、分析、记录等工作，因此会影响网络效率，并且降低客户应用的灵活性；另一方面也增加了管理费用。

但是，来自网络的安全威胁是实际存在的，特别是在网络上运行关键业务时，网络安全是首先要解决的问题。

采用适当的安全体系设计和管理计划，能够有效降低网络安全对网络性能的影响并降低管理费用。

选择适当的技术和产品，制订灵活的网络安全策略，在保证网络安全的情况下，提供灵活的网络服务通道。

网络安全产品有以下几大特点：①网络安全来源于安全策略与技术的多样化，如果采用一种统一的技术和策略也就不安全了；②网络的安全机制与技术要不断地变化；③随着网络在社会各方面的延伸，进入网络的手段也越来越多，因此网络安全技术是一个十分复杂的系统工程。为此建立有中国特色的网络安全体系，需要国家法规和政策的保障支持及集团联合研究开发。安全与反安全就像矛盾的两个方面，总是不断地向上攀升，所以安全产业将来也是一个随着新技术发展而不断发展的产业。

1.2 网络安全 CIA 模型

场景

Yueda：现在请回答我的第 2 个问题，你觉得需要怎样做，公司的系统才是安全的？

小李想起在上课时老师曾讲过信息安全 CIA 模型图（见图 1-1）。

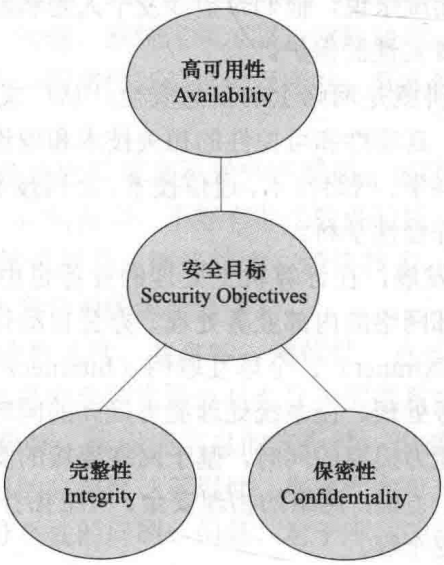

图 1-1　信息安全目标 CIA

他向 Yueda 回答了信息安全目标 CIA 模型的概要。

首先，保密性是为了通过物理或逻辑的访问控制方式限制用户对系统的访问。

其次，完整性是为了保障系统中的数据是没有被修改过的。

再次，可用性是为了保障系统是时时可以被访问的。

Yueda：很好！简单明了。

理论：网络安全 CIA 模型

（1）保密性（Confidentiality）

保密性又称机密性，是指个人或团体的信息不为其他不应获得者获得。在计算机中，许多软件（包括邮件软件、网络浏览器等）都有保密性相关的设定，用以维护用户资讯的保密性。

（2）完整性（Integrity）

数据完整性是指在传输、存储信息或数据的过程中，确保信息或数据不被未授权的篡改或在篡改后能够被迅速发现。

（3）可用性（Availability）

数据可用性是一种以使用者为中心的设计概念。易用性设计的重点在于让产品的设计能够符合使用者的习惯与需求。以互联网网站的设计为例，希望让使用者在浏览的过程中不会产生压力或感到挫折，并能让使用者在使用网站功能时，用最少的努力发挥最大的效能。基于这个原因，任何有违信息的“可用性”都算是违反信息安全的规定。

对信息安全的认识经历了数据安全阶段（强调保密通信）、网络信息安全时代（强调网络环境）和信息保障时代（强调不能被动地保护，需要有保护——检测——反应——恢复 4 个环节）。

1.3　网络攻击的分类

场景

Yueda：很好！现在请回答我的第 3 个问题，作为网络安全工程师，一般需要防御黑客对公司的系统做出哪些攻击？

小李想起在学校时，教网络安全的老师把网络攻击分为 2 种，他的回答如下。

Passive：为被动攻击，指黑客不进行主动发包，只对网络流量做出监听，获取数据信息。

Active：为主动攻击，是指黑客向系统注入代码获取系统权限的攻击方式。

理论：网络攻击的分类

1．主动攻击

主动攻击会导致某些数据流的篡改和虚假数据流的产生。这类攻击可分为篡改、伪造消息数据和终端（拒绝服务）。

（1）篡改消息

篡改消息是指一个合法消息的某些部分被改变、删除，消息被延迟或改变顺序，通常用以产生一个未授权的效果。例如，修改传输消息中的数据，将“允许甲执行操作”改为“允许乙执行操作”。

（2）伪造

伪造是指某个实体（人或系统）发出含有其他实体身份信息的数据信息，假扮成其他实体，从而以欺骗方式获取一些合法用户的权利和特权。

（3）拒绝服务

拒绝服务即通常说的 DoS（Deny of Service），会导致对通信设备的正常使用或管理被无条件地终端，通常是对整个网络实施破坏，以达到降低性能、终端服务的目的。

2. 被动攻击

被动攻击中攻击者不对数据信息做任何修改。截取 / 窃听是指在未经用户同意和认可的情况下，攻击者获得了信息或相关数据。被动攻击通常包括窃听、流量分析、破解弱加密的数据流等攻击方式。

（1）流量分析

流量分析攻击方式适用于一些特殊场合，如敏感信息都是保密的，攻击者虽然从截获的消息中无法得到消息的真实内容，但攻击者还能通过观察这些数据报的模式，分析确定出通信双方的位置、通信的次数及消息的长度，获知相关的敏感信息。

（2）窃听

窃听是最常用的手段。目前应用最广泛的局域网上的数据传送是基于广播方式进行的，这就使一台主机有可能收到本子网上传送的所有信息。当计算机的网卡工作在杂收模式时，它就可以将网络上传送的所有信息传送到上层，以供进一步分析。如果没有采取加密措施，则通过协议分析，就可以完全掌握通信的全部内容。窃听还可以用无线截获方式得到信息，通过高灵敏接收装置接收网络站点辐射的电磁波或网络连接设备辐射的电磁波，通过对电磁信号的分析恢复原数据信号从而获得网络信息。虽然有时数据信息不能通过电磁信号全部恢复，但是肯定能够得到极有价值的情报。

由于被动攻击不会对被攻击的信息做任何修改，留下痕迹的很少，或者根本不留下痕迹，因此非常难以检测。所以抗击这类攻击的重点在于预防，具体措施包括采用虚拟专用网 VPN，采用加密技术保护信息以及使用交换式网络设备等。被动攻击不易被发现，因此常常是主动攻击的前奏。

1.4 黑客的分类

场景

Yueda：很好！你了解对系统进行攻击的黑客都分为哪些种类吗？

小李立刻做出了回答：

白帽黑客，攻击他们自己的系统，或被聘请来攻击客户的系统以便进行安全审查。

黑帽黑客，与白帽黑客相反，黑帽黑客（Black Hat Hacker）就是人们常说的“黑客”或“骇客”了。他们往往利用自身技术，在网络上窃取别人的资源或破解收费的软件，以达到获利。

这种破坏了整个市场的秩序，或者泄露了别人的隐私，属于违法行为，应当加以制止。

灰帽黑客是指使用计算机或某种产品系统中的安全漏洞，而其目的是引起其拥有者对系统漏洞的注意。

小　李：按照我的理解，灰帽黑客可能会变成白帽黑客，也可能会变成黑帽黑客，这就是矛盾的两方面吧！

Yueda：聪明！可以这么理解。实际上，黑客还有更详细的分类，如图 1-2 所示。

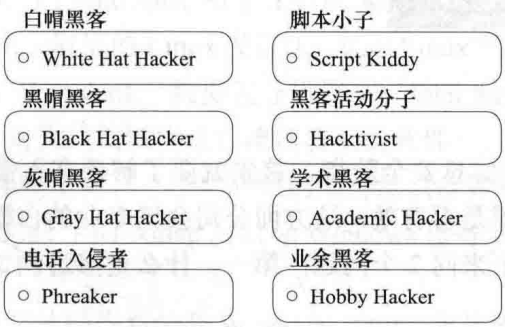

图 1-2　黑客的分类

理论：黑客的分类

“黑客”大体上应该分为“正”“邪”两类，正派黑客依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并加以完善，而“邪”派黑客则是通过各种黑客技能对系统进行攻击、入侵或者做其他一些有害于网络的事情。因为“邪”派黑客所从事的事情违背了《黑客守则》，所以他们真正的名字叫“骇客”（Cracker）而非“黑客”（Hacker）。

黑客的行为主要有以下几种：

（1）学习技术

互联网上的新技术一旦出现，黑客就必须立刻学习，并用最短的时间掌握这项技术，这里所说的掌握并不是一般的了解，而是阅读有关的“协议”、深入了解该技术的原理。

（2）伪装自己

黑客的一举一动都会被服务器记录下来，所以黑客必须伪装自己，使得对方无法辨别其真实身份，这需要有熟练的技巧，用来伪装自己的 IP 地址、使用“跳板”逃避跟踪、清理记录扰乱对方线索、巧妙躲开防火墙等。

如果有朝一日你成为了真正的黑客，千万别对网络进行攻击，毕竟黑客的成长是一种学习，应当把技术用在安全防范上，而不是用来违法犯罪。

（3）发现漏洞

漏洞对黑客来说是最重要的信息，黑客要经常学习别人发现的漏洞，努力自己寻找未知漏洞，并从海量的漏洞中寻找有价值的、可被利用的漏洞进行试验，当然他们最终的目的是来修补上这个漏洞。

（4）利用漏洞

对于正派黑客来说，漏洞要被修补。黑客利用漏洞可以做下面的事情。

1）获得系统信息：有些漏洞可以泄露系统信息，暴露敏感资料，从而进一步入侵系统。

2）入侵系统：通过漏洞进入系统内部或取得服务器上的内部资料，或完全掌管服务器。

3）寻找下一个目标：一个胜利意味着下一个目标的出现，黑客应该充分利用自己已经掌管的服务器作为工具，寻找并检测下一个系统。

4）做一些好事：正派黑客在完成上面的工作后，就会修复漏洞或者通知系统管理员，做出一些维护网络安全的事情。

1.5 黑客入侵思路

场景

Yueda：要想真正进行信息安全防御，首先就要了解黑客入侵的思路。一般地，为了验证公司的信息安全工作做得是否有效，这方面公司会请专业的白帽黑客通过渗透测试的方法来测试系统是否安全。接下来问 2 个问题；第一，什么是渗透测试？第二，能谈一谈你对黑客入侵思路的理解吗？

小 李：渗透测试是为了证明网络防御按照预期计划正常运行而提供的一种机制。不妨假设，你的公司定期更新安全策略和程序，及时给系统安装补丁程序，并采用了漏洞扫描器等工具，以确保所有补丁程序都已安装好。如果早已做到了这些，为什么还要请外方进行审查或渗透测试呢？因为渗透测试能够独立地检查网络策略，换句话说，就是给系统安了一双“眼睛”。而且，进行这类测试的都是寻找网络系统安全漏洞的专业人士。

Yueda：很好！接下来能谈一谈你对黑客入侵思路的理解吗？

小李想起了在学校网络安全课上，老师当时做的演示，如图 1-3 所示。

Step1：实施探测（Perform Reconnaisance）

Step2：识别操作系统、应用程序（Identify Operating System&Applications）

Step3：获取对系统的访问（Gain Access To The System）

Step4：提权（Login With User Credentials，Escalate Privileges）（可选）

Step5：创建其他用户名、密码（Setup Additional Username&Password）

Step6：创建后门（Setup “Back Door”）

Step7：使用系统（Use The System）

图 1-3 黑客的思路

Yueda：很好！不过你只是说出了操作步骤，那么具体的渗透测试操作你实践过吗？

小 李：在学校的宿舍，曾经用自己的笔记本式计算机安装虚拟机做过一些测试。

Yueda：很好！我的问题基本就是这些了，接下来请公司信息安全部门的同事为你搭建测试环境，你来实际演示实践过的渗透测试操作的过程，你觉得如何？

小 李：我尽力而为吧，这个方面之前实践的也不是很多。

Yueda：没关系，我觉得你之前对我的提问回答得已经很不错了，接下来想了解你是否具备一些网络安全实践能力。你先休息一下，我安排同事为你搭建安全测试环境。

半个小时后，TaoJin（韬金）电子商务公司信息安全部门工程师为小李搭建好了渗透测试环境，使用的是 Vmware 中的两台虚拟机，其中一台是 Kali Linux，另一台是 Windows 服务器，两台虚拟机之间做了桥接，也就是设置为同一个子网内。注：Kali Linux 是基于 Debian 的 Linux 发行版，设计用于数字取证和渗透测试，由 Offensive Security Ltd. 维护和资助，最先由 Offensive Security 的 Mati Aharoni 和 Devon Kearns 通过重写 BackTrack 来完成，BackTrack 是他们之前写的用于取证的 Linux 发行版。Kali Linux 预装了许多渗透测试软件，包括 nmap（端口扫描器）、Wireshark（数据包分析器）、John the Ripper（密码破解器）以及 Aircrack-ng（一个应用于对无线局域网进行渗透测试的软件）。

Yueda：现在你在这个环境上对自己刚才介绍的渗透测试步骤简单实践一下吧。

小李首先使用了 Kali Linux 下的 Nmap 对目标 Windows 服务器做了一下扫描，如图 1-4 和图 1-5 所示。

屏幕显示这台计算机安装的操作系统是 Windows 2000，而且还开放了 80 端口。

小　李：你们这个 Kali Linux 下有没有安装漏洞扫描程序，我想看一看目标系统是否存在漏洞。

Yueda：可以，不过这个 Kali Linux 下目前没有安装，这样，我再给你加上一台带有漏洞扫描程序的虚拟机吧。

信息安全部门的工程师又在小李的测试环境上加上了一台带有漏洞扫描程序 Nessus 的虚拟机。

```
root@bt:~# nmap -v -n -A 202.100.1.10

Starting Nmap 6.01 ( http://nmap.org ) at 2015-04-05 10:20 CST
NSE: Loaded 93 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 10:20
Scanning 202.100.1.10 [1 port]
Completed ARP Ping Scan at 10:20, 0.01s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:20
Scanning 202.100.1.10 [1000 ports]
Discovered open port 1025/tcp on 202.100.1.10
Discovered open port 445/tcp on 202.100.1.10
Discovered open port 21/tcp on 202.100.1.10
Discovered open port 135/tcp on 202.100.1.10
Discovered open port 80/tcp on 202.100.1.10
Discovered open port 139/tcp on 202.100.1.10
Discovered open port 443/tcp on 202.100.1.10
Discovered open port 1026/tcp on 202.100.1.10
Completed SYN Stealth Scan at 10:20, 0.09s elapsed (1000 total ports)
Initiating Service scan at 10:20
Scanning 8 services on 202.100.1.10
Completed Service scan at 10:20, 48.59s elapsed (8 services on 1 host)
Initiating OS detection (try #1) against 202.100.1.10
NSE: Script scanning 202.100.1.10.
Initiating NSE at 10:20
```

图 1-4　使用 Nmap 扫描 1