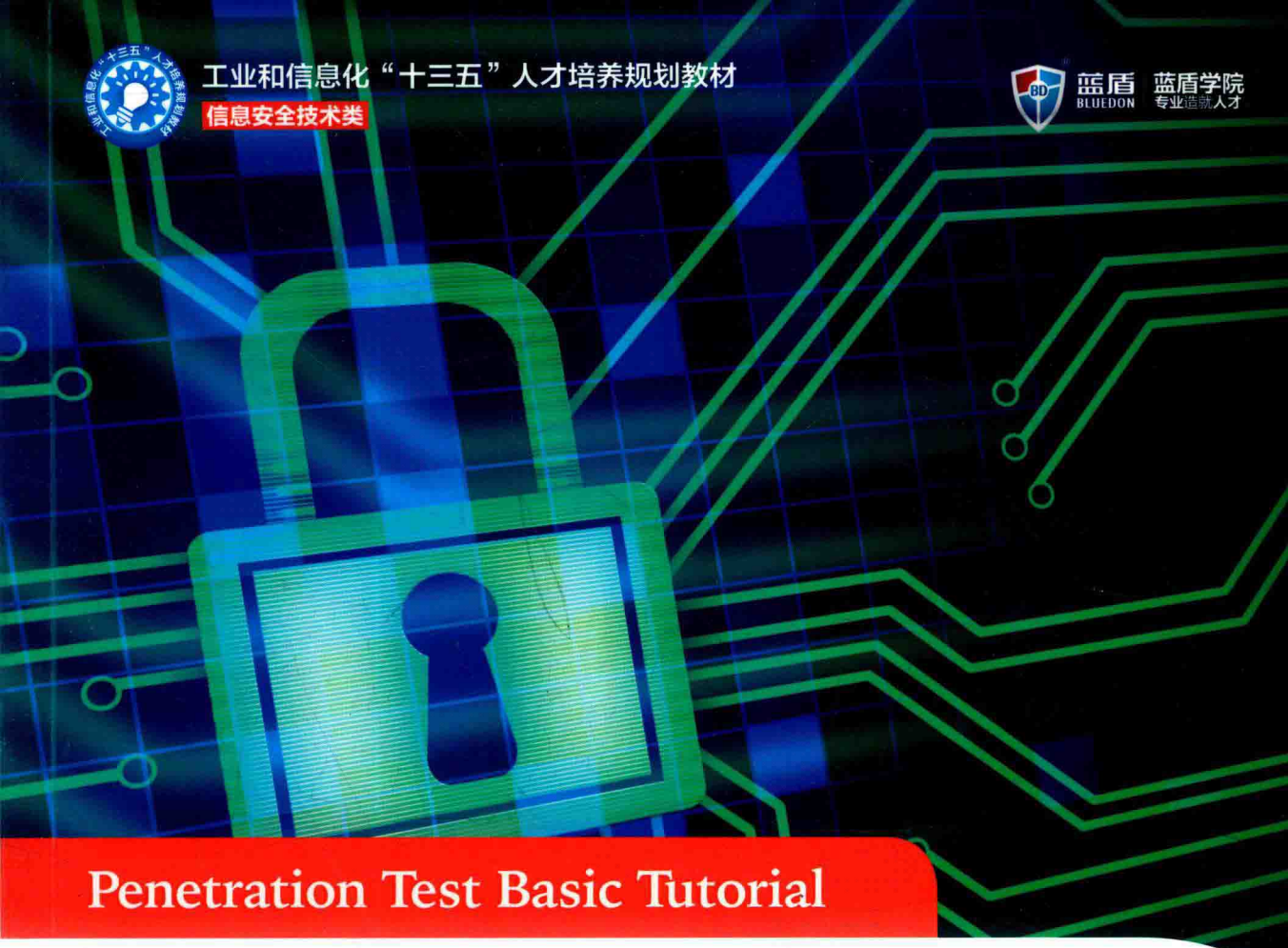

工业和信息化“十三五”人才培养规划教材

信息安全技术类

蓝盾 BLUEDON 蓝盾学院 专业造就人才

Penetration Test Basic Tutorial

渗透测试基础教程

◎ 黄洪 尚旭光 王子钰 编著

- 全书分为四篇，共 8 章，全面系统地讲解了**渗透测试**的基础知识和应用
- 本书编写人员都有信息安全的**一线攻防经验**
- 本书通过**理论与实践**相结合的方式，让读者在完成每个**生动实验**的过程中，逐步掌握**渗透测试**的方法，从而逐步
  测试的工作中去

工信出版集团 人民邮电出版社 POSTS & TELECOM PRESS

工业和信息化“十三五”人才培养规划教材
信息安全技术类

Penetration Test Basic Tutorial

渗透测试基础教程

◎ 黄洪 尚旭光 王子钰 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

渗透测试基础教程 / 黄洪，尚旭光，王子钰编著
. -- 北京 : 人民邮电出版社，2018.6
工业和信息化“十三五”人才培养规划教材. 信息安全技术类
ISBN 978-7-115-47608-1

Ⅰ. ①渗… Ⅱ. ①黄… ②尚… ③王… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2017)第319420号

内 容 提 要

渗透测试是一种通过模拟恶意黑客的攻击行为，来评估计算机网络系统安全的方法。本书采用理论与案例相结合的方式，向读者介绍渗透测试的基本思路、方法，以及常用工具的用法。读者通过学习本书，并动手操作本书提供的案例之后，即可对渗透测试的工作内容有一个基本的了解。

本书共分为 8 章，内容涵盖渗透测试概述、Web 渗透测试基础、SQL 注入漏洞利用与防御、跨站脚本漏洞利用与防御、其他常见 Web 漏洞利用与防御、常见的端口扫描与利用、操作系统典型漏洞利用，以及典型案例分析。在内容编排上，本书穿插了大量案例，希望通过案例的讲解，让读者基本掌握渗透测试常用工具的安装配置、漏洞发现和漏洞利用等内容。

本书适合信息安全专业的本科、专科学生及从业者学习使用，是一本较好的渗透测试工作入门教材。

◆ 编　　著　黄　洪　尚旭光　王子钰
责任编辑　范博涛
责任印制　马振武

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京隆昌伟业印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：11.5　　2018 年 6 月第 1 版
字数：286 千字　　2018 年 6 月北京第 1 次印刷

定价：39.80 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

前言 FOREWORD

当今社会，随着信息技术的迅猛发展，我们面临着越来越严峻的信息安全问题，从国家安全、社会稳定到个人隐私保护，无处不见信息安全的重要性。特别是“棱镜门”事件之后，各国对信息安全问题更加重视，这一问题已经成为全社会关注的焦点，社会对信息安全人才的需求也越来越大。

渗透测试作为检验信息系统安全保障体系有效性的重要手段之一，已经越来越受到业界的重视。然而，渗透测试的学习相对困难，它涉及操作系统、数据库、常用中间件和网络协议等众多对象，不仅要求渗透测试人员掌握渗透测试的基本方法、流程和工具，而且要求渗透测试人员具有安全问题分析的独立视角，因此让很多人望而却步。本书通过理论与实践相结合的方式，让读者在完成一个个生动实验的过程中，逐步掌握渗透测试的方法，从而逐步参与到渗透测试的工作中去。

本书的编写团队由公安部信息安全等级保护评估中心、成都安信共创检测技术有限公司、成都市锐信安信息安全技术有限公司、西南科技大学等的一线科技人员组成，他们长期在渗透测试领域从事研究与实践工作，具有丰富的经验。其中，黄洪博士（西南科技大学引进博士，曾任公安部信息安全等级保护评估中心测评部门的负责人）为主创作人，尚旭光（公安部信息安全等级保护评估中心渗透测试部门的负责人）对全书进行修订，并参与编写第 1 章至第 5 章，钱志祁（成都市锐信安信息安全技术有限公司渗透测试资深工程师）参与编写第 6 章和第 7 章，王子钰（公安部信息安全等级保护评估中心渗透测试工程师）参与编写第 8 章，西南科技大学的卢泽中、陶琦、胡家新、王鹏诚、章楠、吴毅等参与材料收集、实验验证等工作，成都安信共创检测技术有限公司资深测评工程师邓跃良，西南科技大学周绍华、韦勇和廖晓鹃等教师参与了本书的审校工作。

感谢公安部信息安全等级保护评估中心的张宇翔主任、李明主任助理、朱建平研究员，西南科技大学计算机科学与技术学院的范勇院长、左旭辉书记、吴亚东副院长，成都市锐信安信息安全技术有限公司负责人陈伟、祁志敏，国防大学信息作战与指挥训练教研部的刘增良教授对本书的大力支持。

最后要感谢在本书成稿过程中给予我们支持的同事、朋友，以及在我们忙碌工作时给予我们理解和支持的家人。

由于信息技术发展迅速、测评技术本身的时效性也很强，且作者的水平和经验有限，本书的缺点和疏漏之处在所难免，望有关专家和读者批评指正，以利于再版时修正，交流邮箱 hong.huang@139.com。

作者

2018年3月于成都

目录 CONTENTS

第一篇 基础篇

第二篇 Web 渗透测试篇

第三篇 系统渗透测试篇

第四篇 实战案例篇

第一篇

基础篇

渗透测试工程师是很多信息安全领域从业者向往的职业，特别是年轻的信息安全专业的大学生们。在他们眼中，这个行业神秘而神圣，能将理想与职业很好地合二为一。每当他们找出那些防范严密的系统中存在的安全问题的时候，他们内心深处都会产生极大的成就感。本篇将从一些基本概念讲起，逐步带你进入渗透测试的神秘王国。

PENETRATION TEST

Chapter 1

第 1 章
渗透测试概述

随着互联网的快速发展，信息安全变得越来越重要，渗透测试作为保障信息安全的一种重要手段，正在引起人们的广泛关注。本章通过对网络安全的发展简史、渗透测试的定义及主要特点、渗透测试的主要测试方法和流程等内容的介绍，使读者对渗透测试有一个基本的认识。

1.1 网络安全概述

1.1.1 网络安全定义

自 20 世纪 60 年代计算机网络诞生起，网络迅速发展，如今网络已渗透进每个人生活的方方面面，手机、平板电脑和个人计算机都处在网络中。然而，网络的迅速发展也导致了一系列安全问题的产生，对我们的日常生活甚至国家安全都产生了极大的影响。因此，网络安全成了一个亟待解决的问题。

那么，什么是网络安全呢？网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露；系统连续可靠正常地运行，网络服务不中断。网络安全的主要特性为：保密性、完整性、可用性、可控性和可审查性。

- 保密性——指信息不泄露给非授权用户、实体或过程，或供其利用的特性。
- 完整性——指数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。
- 可用性——指可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息，例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。
- 可控性——指对信息的传播及内容具有控制能力。
- 可审查性——指出现安全问题时可提供依据与手段的特性。

1.1.2 网络安全发展简史

从 20 世纪 80 年代开始，互联网技术迅速发展，计算机网络安全开始被人们关注。特别是，自 1987 年发现了全世界首例计算机病毒以来，计算机病毒的数量和种类迅速增加，计算机网络安全逐步成为热点问题之一。国外计算机病毒专家开始研究反病毒程序，我国一部分有安全意识的计算机学者对网络安全的实际工作也开始进行摸索，但并没有形成规模。在网络保护方面大都也只是在物理安全及保密通信等环节上有些规定，企业和大多部门还没有意识到网络安全的重要性。

20 世纪 90 年代，随着计算机病毒问题愈加严重，网络安全成了一个不可忽视的问题。我国也逐步加强了对计算机安全的监管，1994 年颁布了《中华人民共和国计算机信息系统安全保护条例》，较全面地从法规角度阐述了关于计算机信息系统安全的概念、内涵、管理、监督和责任。很多企业及事业单位也意识到网络安全的重要性，将网络安全作为系统建设的重要内容。随后的 10 多年里，我国的网络安全产业进入了快速发展时期，政府出台了一系列重要政策措施，网络安全设备和品种也逐渐健全，标志着我国的网络安全正式走向快速发展时期。

与此同时，网络成为各国继陆地、海洋、天空和太空之后争夺的“第五区域”。各国的网络攻防便是一场没有硝烟的战争，2010 年 5 月，美国国防部组建的网络司令部正式启动，于 2010 年 10 月全面运作。日本也在 2009 年年底决定，在 2011 年建立一支专门的“网络空间防卫队”。

2016 年 11 月 7 日，第十二届全国人民代表大会常务委员会第二十四次会议表决通过《中华人民共和国网络安全法》，并于 2017 年 6 月 1 日正式实施。

1.2 渗透测试的定义和分类

1.2.1 渗透测试的定义

渗透测试（Penetration Test）并没有一个标准的定义，国外一些安全组织的通用说法是：渗透测试是测试人员通过模拟恶意攻击者的技术与方法，来评估计算机网络系统安全的一种评估方法。整个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析及利用。

换句话来说，渗透测试是指测试人员在不同的位置（如内网、外网等）利用各种手段对某个特定网络进行测试，以期发现和挖掘系统中存在的漏洞，然后形成渗透测试报告，并提交给网络所有者。网络所有者根据渗透人员提供的渗透测试报告，可以清晰知晓系统中存在的安全隐患和问题。

自 20 世纪 90 年代后期以来，渗透测试逐步从军队与情报部门拓展到安全业界，一些对安全性需求很高的企业也开始采纳这种方法来对自己的业务网络与系统进行测试。于是，渗透测试逐渐发展为一种由安全公司提供的专业化安全评估服务，成为系统整体安全评估的一个重要组成部分。通过渗透测试，对业务系统进行系统性评估，可以达到以下目的。

- 知晓技术、管理与运维方面的实际水平，使管理者清楚目前的防御体系可以抵御什么级别的入侵攻击。
- 发现安全管理与系统防护体系中的漏洞，可以有针对性地进行加固与整改。
- 可以使管理人员保持警觉性，增强防范意识。

渗透测试有以下两个显著特点。

- 渗透测试是一个渐进的、持续的、兼具深度和广度的漏洞发现过程。
- 渗透测试是在获取到被测系统授权并且尽可能不影响业务系统正常运行的前提下，模拟攻击者使用的攻击方法进行的测试。

注意

渗透测试并非黑客攻击，必须在具有书面授权的条件下进行。

1.2.2 渗透测试的分类

从渗透测试发起角度，可将渗透测试分为内部测试、外部测试和灰盒测试。

1. 内部测试

进行内部测试的团队可以了解到关于目标环境的所有内部与底层知识，因此渗透测试者可以以最小的代价发现和验证系统中最严重的安全漏洞。所以，内部测试可以比外部测试消除更多的目标基础设施环境中的安全漏洞与弱点，从而给客户组织带来更大的价值。

内部测试无须进行目标定位与情报搜集，此外，内部测试能够更加方便地在一次常规的开发与部署计划周期中集成，故能够在早期消除掉一些可能存在的安全隐患，从而避免被入侵者发现和利用。

内部测试中发现和解决安全漏洞所需花费的时间和代价要比外部测试少得多。而内部测试的最大问题在于无法有效地测试客户组织的应急响应程序，也无法判断出他们的安全防护计划

对防御特定攻击的效率。如果时间有限或是特定的渗透测试环节（如情报搜集）并不在范围之内，那么内部测试可能是最好的选择。

2. 外部测试

采用外部测试方式进行测试时，渗透测试团队将从一个远程网络位置来评估目标网络基础设施，并且没有任何目标网络内部拓扑等相关信息，他们完全模拟真实网络环境中的外部攻击者，采用流行的攻击技术与工具，有组织、有步骤地对目标系统进行逐步渗透与利用，寻找目标网络中一些已知或未知的安全漏洞，并评估这些漏洞能否被利用。

外部测试还可以对目标系统内部安全团队的检测与响应能力做出评估。在测试结束之后，外部测试会对发现的目标系统安全漏洞、所识别的安全风险及其业务影响评估等信息进行总结和报告。

外部测试是比较费时费力的，同时需要渗透测试者具备较高的技术能力。在安全业界的渗透测试者眼中，外部测试通常是更受推崇的，因为它能更逼真地模拟一次真正的攻击过程。

3. 灰盒测试

以上两种渗透测试基本类型的组合可以提供对目标系统更加深入和全面的安全审查，这就是灰盒测试（Grey Box Testing）。组合之后的好处就是能够同时发挥两种基本类型渗透测试方法的各自优势。灰盒测试需要渗透测试者能够根据对目标系统所掌握的有限知识与信息来选择评估整体安全性的最佳途径。在采用灰盒测试方法的外部渗透场景中，渗透测试者也需要从外部逐步渗透进入目标网络，但其所拥有的目标网络底层拓扑与架构将有助于更好地决策攻击途径与方法，从而达到更好的渗透测试效果。

1.3 渗透测试的流程

渗透测试执行标准（Penetration Testing Execution Standard，PTES）所定义的渗透测试过程环节基本上反映了安全业界的普遍认同，主要包括以下几个阶段，如图 1-1 所示。

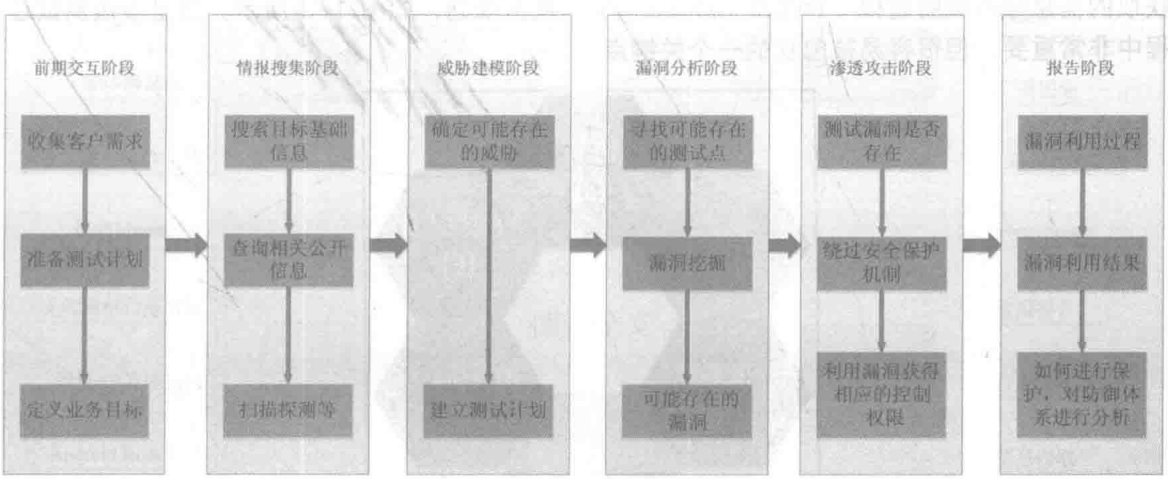

图 1-1　渗透测试的流程

1.3.1 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进行交互讨论，最重要的是确定渗透测试的范围、目标、限制条件及服务合同的细节。

该阶段通常涉及收集客户需求、准备测试计划、定义测试范围与边界、定义业务目标、项目管理与规划等活动。

1.3.2 情报搜集阶段

在目标范围确定之后，将进入情报搜集（Information Gathering）阶段，如图 1-2 所示。渗透测试团队可以利用各种信息来源与技术，尝试获取更多关于目标组织网络拓扑、系统配置与安全防御措施的信息。

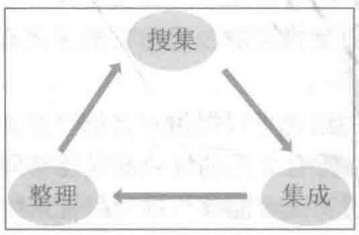

图 1-2 情报收集阶段

渗透测试者可以使用的情报搜集方法包括公开来源信息查询、Google Hacking、社会工程学、网络踩点、扫描探测、被动监听等。对目标系统的情报探查能力是渗透测试者一项非常重要的技能，情报搜集是否充分在很大程度上决定了渗透测试的成败，因为如果渗透测试者遗漏关键的情报信息，那么他们将可能在后面的阶段里一无所获。

1.3.3 威胁建模阶段

在搜集到充分的情报信息之后，渗透测试团队的成员们停下敲击键盘，大家聚到一起针对获取的信息进行威胁建模（Threat Modeling）与攻击规划，如图 1-3 所示。这是渗透测试过程中非常重要，但很容易被忽视的一个关键点。

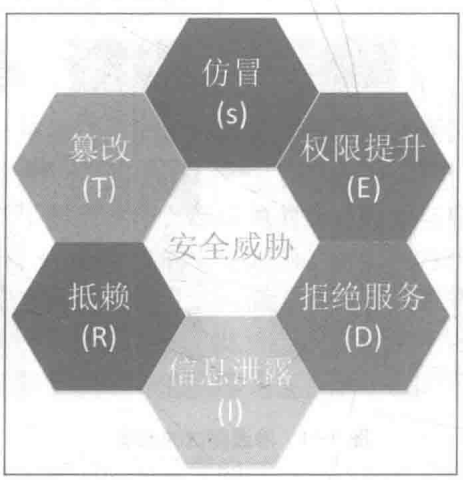

图 1-3 威胁建模与攻击规划

通过团队全体人员共同的缜密情报分析与攻击思路头脑风暴，可以从大量的情报信息中理出头绪，确定好最可行的攻击通道。

注意

渗透测试不是黑客攻击，不能破坏目标系统。

1.3.4 漏洞分析阶段

确定了可行的攻击通道之后，接下来需要考虑应该如何取得目标系统的访问控制权，即漏洞分析（Vulnerability Analysis）阶段。

在该阶段，渗透测试者需要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、服务站点信息等，通过搜索可获取的渗透代码资源，找出可以实施渗透攻击的攻击点，并在实验环境中进行验证。在该阶段，高水平的渗透测试团队还会针对攻击通道上的一些关键系统与服务进行安全漏洞探测与挖掘，以期找出可被利用的未知安全漏洞，并开发出渗透代码，从而打开攻击通道上的关键路径。

1.3.5 渗透攻击阶段

渗透攻击（Exploitation）是渗透测试过程中颇具魅力的一个环节。在此环节中，渗透测试团队需要利用他们所找出的目标系统安全漏洞进入系统，获得访问控制权。

渗透攻击可以利用公开渠道获取渗透代码，但一般在实际应用场景中，渗透测试者还需要充分地考虑目标系统特性来定制渗透攻击，并需要绕过目标系统中实施的安全防御措施，才能成功达到渗透目的。在黑盒测试中，渗透测试者还需要考虑对目标系统检测机制的逃逸，从而避免被目标系统安全响应团队发现，常见的渗透方式如图 1-4 所示。

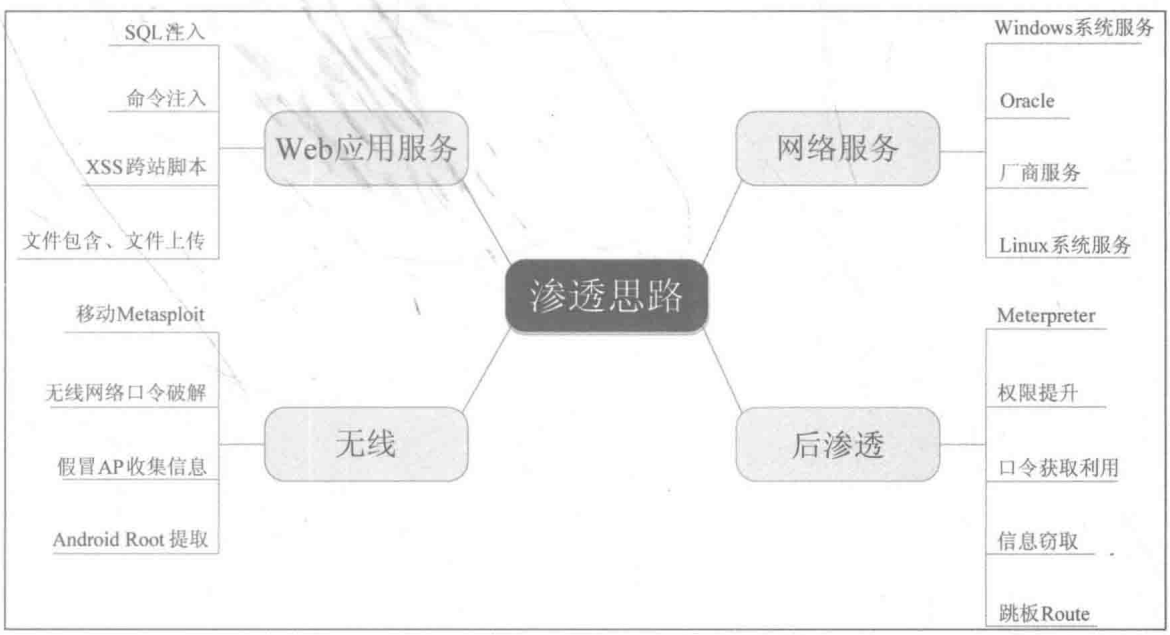

图 1-4 常见的渗透方式

1.3.6 报告阶段

渗透测试过程结束后，最终向客户提交一份渗透测试报告（Reporting）。这份报告凝聚了之前所有阶段中渗透测试团队所获取的关键情报信息、探测和发掘出的系统安全漏洞、成功渗透攻击的过程，以及造成业务影响后果的攻击途径，同时，还要站在防御者的角度，帮助客户分析安全防御体系中的薄弱环节、存在的问题，以及修补与升级技术方案。

1.4 小结

渗透测试技术发展迅速，面对不同的环境，方法众多，在了解了渗透测试的分类和操作流程之后，接下来，将对渗透测试的具体方法进行分析，从 Web 渗透测试开始，对测试思路和相关漏洞的原理、利用及防御进行探索。

课后习题

1. 什么是网络安全？什么是渗透测试？
2. 渗透测试的特点有哪些？
3. 简述渗透测试的分类，以及它们的区别。
4. 渗透测试的流程是什么？尝试画出流程图。
5. 试列出你能想到的搜集信息的几种方法。

第二篇

Web 渗透测试篇

随着 Web 技术的广泛应用，人们的生活已经发生了根本转变，同时，Web 安全也面临着前所未有的挑战，Web 渗透测试技术已成为保障 Web 安全的一种重要手段。本篇对 Web 渗透测试的思路和方法进行介绍，对 Web 渗透测试中的典型漏洞（SQL 注入、XSS 等）、渗透工具和防御方式进行剖析，并对典型漏洞配以实例进行漏洞利用演示，使读者对 Web 渗透测试的方法和防御方法有基本的认识，并逐步了解渗透测试的思路，掌握常用工具的用法。

PENETRATION TEST

Chapter 2

第 2 章
Web 渗透测试基础

在渗透测试过程中，渗透测试人员通常只能访问到目标对象的外网系统，这时通常需要针对企业部署的 Web 应用（如网站、OA、邮箱等）进行渗透，在攻陷这些目标后，进一步利用这些目标和内网之间的关联进入内网环境，为内网渗透做好准备。

2.1 Web 渗透测试常用术语

1. WebShell

WebShell 就是以 ASP、PHP、JSP 或 CGI 等网页文件形式存在的一种命令执行环境，也可以称为一种网页后门，测试人员可通过这个程序对目标服务器进行一些操作，如文件管理、上传下载、链接数据库、执行命令等。

2. 弱口令

容易被恶意攻击者猜测到或被破解工具破解的口令均称为弱口令，这些口令通常是简单数字和字母的组合，如“123456”“admin”等。

3. SQL 注入

在输入的字符串中注入 SQL 语句，设计不当的程序忽略了对 SQL 语句的检查，这些语句会被数据库误认为是正常的 SQL 指令而被执行。

4. 注入点

注入点是可以进行注入的漏洞链接，通过在此链接输入恶意语句，可对 Web 应用程序进行攻击。

5. XSS

XSS（Cross Site Scripting，跨站脚本）是一种网站应用程序的安全漏洞，是代码注入的一种。它允许恶意用户将代码注入网页，其他用户在查看网页时会受到影响。

6. 命令执行

由于 Web 系统对用户输入检查过滤不严，因此攻击者可以在输入的字符串中添加恶意语句，从而执行系统命令。

7. C 段嗅探

每个 IP 由 ABCD 四段数字组成。例如，192.168.0.1，A 段就是 192，B 段是 168，C 段是 0，D 段是 1，而 C 段嗅探就是窃听同一 C 段中的一台服务器，也就是 D 段 1～255 中的一台服务器，然后利用工具嗅探窃听该服务器。

2.2 搭建 Web 服务器环境

由于在未授权的条件下对真实环境进行渗透测试属于违法行为，因此需要搭建实验环境，模拟真实情景，学习相关知识，训练渗透技能。

1. 新建虚拟机

下面以 VMware 为例，介绍虚拟机的使用方法。打开 VMware Workstation 10，选择“创建新的虚拟机”（见图 2-1），选择默认的“典型（推荐）(T)”类型，单击“下一步”按钮，如图 2-2 所示。

选择“稍后安装操作系统（S）”（稍后会安装映像文件），单击“下一步”按钮，如图 2-3 所示，操作系统选择“Microsoft Windows（W）”，版本选择“Windows XP Professional”，选择好后单击“下一步”按钮。