HZ BOOKS 华章IT
Pearson

· 网络空间安全技术丛书 ·

PENETRATION TESTING FUNDAMENTALS

A Hands-On Guide to Reliable Security Audits

渗透测试基础

可靠性安全审计实践指南

[美] 查克 · 伊斯特姆 著　张刚 译
(Chuck Easttom)

- 清晰阐述渗透测试的关键概念、术语、挑战、工具和技能
- 涵盖来自 NSA、PCI 和 NIST 的新渗透测试标准

机械工业出版社
China Machine Press

渗透测试基础

可靠性安全审计实践指南

PENETRATION TESTING FUNDAMENTALS

A Hands-On Guide to
Reliable Security Audits

[美] 查克·伊斯特姆 著 张刚 译
(Chuck Easttom)

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

渗透测试基础：可靠性安全审计实践指南 /（美）查克·伊斯特姆（Chuck Easttom）著；张刚译 . —北京：机械工业出版社，2019.10
（网络空间安全技术丛书）
书名原文：Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits

ISBN 978-7-111-63741-7

I. 渗… II. ①查… ②张… III. 计算机网络－网络安全－指南 IV. TP393.08-62

中国版本图书馆 CIP 数据核字（2019）第 212141 号

本书版权登记号：图字 01-2018-8482

渗透测试基础：可靠性安全审计实践指南

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：冯秀泳　　责任校对：李秋荣
印　　刷：大厂回族自治县益利印刷有限公司　　版　　次：2019 年 10 月第 1 版第 1 次印刷
开　　本：186mm×240mm 1/16　　印　　张：19.75
书　　号：ISBN 978-7-111-63741-7　　定　　价：99.00 元

客服电话：（010）88361066 88379833 68326294　　投稿热线：（010）88379604
华章网站：www.hzbook.com　　读者信箱：hzit@hzbook.com

译 者 序

随着 IT 技术的快速发展和广泛应用，在促进经济发展和社会进步的同时，企业 IT 环境也越来越受到重视。应用系统的复杂性、基础设施的多样化，导致在企业 IT 环境中可能存在多种安全隐患。这些隐患可能对企业最核心的数据资产造成致命打击，后果不堪设想。VFEmail 是美国一家经营近 20 年的邮件服务商，因黑客删除其近 20 年的数据和全部备份而宣布倒闭。Cryptopia Limited 是新西兰一家经营加密货币交易的公司，拥有来自全球各地的 30 多万个账户，因黑客成功窃取价值 1 600 多万美元的加密货币而申请美国破产保护。因此，信息安全已成为企业至关重要、不容忽视的一部分。

在国内，银行、证券等金融机构对信息安全建设极其重视，一直在不断增强企业信息的安全性。但也有很多中小型企业，对信息安全建设甚至没有明确概念，忽视建设的重要性，从而导致出现问题后需要用更高的代价去维护。由于信息安全具有极高的专业性，近年来逐渐涌现出一大批信息安全团队和创业公司。在这个垂直的细分领域存在大量的市场需求，因此也充满商业机会。

近年来，随着云计算的蓬勃发展，企业基础设施得到了长足发展，更多的应用系统可以更快、更方便地运行在公有云之上。这给企业信息安全带来了更大的挑战。企业需要储备自己的专业人才，个人需要发展自己的专业技能。不同于传统 IT 领域，无论大学教育、职业培训，还是技术生态圈，个人都可以获得体系化的知识、系统性的教育。但在安全领域，一方面专业性的图书相对较少，另一方面系统性介绍某个专题的图书相对较少。在安全领域存在“脚本小子”的戏谑，其中一个原因就是有些人在学习知识时没有好的参考资料。本书就是渗透测试入门的一本好书。

本书对渗透测试领域的基础知识进行了详细讲述，系统地涵盖了渗透测试的全生命周期。针对每个主题，都提供了大量的实用工具，并结合实例进行讲解，具有理论联系实际的特点。虽然不可能对每个主题进行特别深入的讲解（比如，单就 Metasploit 这个主题就可以写成一本书），但是各种基础知识涵盖很全。在读完本书后，读者对渗透测试将有一个清晰视图，从而建立完整的知识体系，有利于快速入门和后续的技能精进。如有必要，在工作和学习的过程中可以就某个主题进行深入研究。

我认为技术类图书的翻译工作是一个学习再创造的过程。在充分理解作者意图的同时，译文需要极大限度地保持作者原意，“信达雅”是译者追求的理想目标。在翻译图书的过程中，得到了关敏等编辑的大力帮助，他们为本书的出版付出了艰辛的劳动，做出了卓越的贡献。没有他们的努力，就没有本书的出版。同时，感谢家人对我的理解和支持。正是他们在背后的默默支持，才让我能够全力以赴翻译本书。

为者常成，行者常至。每一份辛勤付出，都终有收获。与诸位共勉。

张刚

2019 年 8 月

前　言

本书对渗透测试行业进行了概述，包括需要遵循的标准、特定的黑客技术，甚至如何进行渗透测试和编写报告。它不仅仅是一本关于黑客的图书，也是一本适用于专业渗透测试人员的图书。书中包括许多实践练习，可帮助读者掌握进行专业渗透测试所需的技能。

读者对象

本书专为专业渗透测试人员设计，包括新手和经验丰富的专业人员。新手可以对这个领域有一个全面的认识；经验丰富的专业人员可以弥补自己的知识空缺，最可能的是在测试标准和方法论方面。作为一本专门为渗透测试课程而设计的教科书，本书非常适用于大学课程或行业培训。

致谢

我要感谢为本书出版而努力的 Pearson 出版社的每位成员。技术评审者和编辑都是一流的。我曾与很多出版商和编辑 / 评论家合作过，但没有比 Pearson 更优秀的出版商了。

作者、技术评审者、译者简介

作者简介

Chuck Easttom 从事 IT 行业已超过 25 年，从事网络安全已超过 15 年。他拥有 40 多个行业认证，并撰写了 25 本图书。他还是一位拥有 13 项专利的发明家。Chuck 经常在各种安全会议（包括 DEF CON、ISC2 安全大会、Secure World 等）上发表演讲。他还撰写了大量与安全主题相关的论文，内容涉及恶意软件研发、渗透测试和黑客技术。他拥有丰富的网络安全问题咨询和渗透测试的实践经验。

技术评审者简介

Steve Kalman 既是一名律师，也是一名专业的安全专家。他持有 $(ISC)^2$ 的以下证书并担任授权讲师：CISSP、CCFP-US、CSSLP、ISSMP、ISSAP、HCISPP、SSCP。Steve 是超过 20 本图书的作者或技术编辑，这些书均由 Pearson 或 Cisco 出版社出版。

Everett Stiles 拥有田纳西大学计算机工程硕士学位，目前是思科公司安全研究方面的一名高级工程师。

译者简介

张刚，金融行业从业十多年，长期从事基础系统领域的研究，先后从事非结构化数据、前端技术、云计算、数据库、中间件等多个领域的技术预研、平台研发、技术管控和支持等工作。由于网络安全关乎研究的每个领域，因此，一直保持对安全领域的关注和学习。

目　录

第1章

渗透测试概览

本章目标

阅读本章并完成练习后，你将能够：

- ❑ 理解什么是渗透测试
- ❑ 理解渗透测试方法论
- ❑ 理解各种渗透测试方法
- ❑ 深入理解渗透测试的道德规范
- ❑ 理解与渗透测试相关的法律问题

计算机和网络安全或许是当今这个年代谈及最多的一个话题。随着计算设备不断渗入人们生活，这些设备和网络的安全备受关注。如何有效地进行安全测试成为一个非常重要的话题。一种测试网络安全的方法是执行渗透测试。渗透测试是实际利用恶意攻击者所使用的技术的过程，但它不是试图破坏目标系统，而是利用这些技术测试目标系统的安全性。

人们可能经常听说某些系统遭受某种程度的破坏。当然，即使没有经常关注这类新闻，系统遭受破坏的事情每天都会发生。网络和计算机安全有多种方法。有人专注于合适的安全策略和程序，有人专注于用作攻击对策的设备，还有人专注于安全编程并将此作为缓解日益增长的网络攻击的一种手段。所有这些安全视角都有自己的优点，可视作任何组织安全策略的一部分。

如果未经充分测试，所有个人能够实现的这些安全措施都不可靠。在严格测试任何系统或设备时，最有效的一种方法就是实际使用攻击者所采用的技术。只有这样才能真正对系统的安全充满信心。本书将会讲述如何执行有效的、系统性的渗透测试。

1.1 什么是渗透测试

人们已经看到，渗透测试包含实际使用的攻击技术。但渗透测试不是安全测试的唯一形式。所以，区分渗透测试和其他形式的测试十分重要。正如后文所示，网络安全测试有三种主要方法：

- ❑ 审计
- ❑ 漏洞扫描

❑ 渗透测试

1.1.1　审计

审计通常是对文档的审查，主要指审查事件响应计划、灾难恢复计划和安全策略。审计还包含对过去的事件响应报告的审查，以确保遵守已制定的计划和策略。事实上，审计的关键就是对合规性的审查。

审计有时也包含对系统日志的审查。这可能包含防火墙日志、入侵检测系统日志和任何有助于了解安全策略合规性是否得到遵从的系统日志。审计最重要的关注点是评估目标网络是否遵从适当的应用策略和法规，以及在某些情况下是否符合适用于该组织的法律。

审计是网络安全的一个重要方面，也可以看作是与渗透测试相对的另一方面。审计是一个非常被动的过程。没有系统会真正受到审计影响，或与之产生交互。审计是一个历史过程，因为审查的是截止到审计时间那一刻所发生的事情。政策是否被遵守？这些可应用的法律和标准是否得到遵守？这些都是被动性的历史问题。正如本章和后续章节所言，渗透测试是检查当前时刻所发生的事情，它在不断变化。

1.1.2　漏洞扫描

漏洞扫描的目的是发现目标网络或者系统的已知漏洞。第一个问题是明确什么是已知漏洞。漏洞是任意系统中可能导致安全性被破坏的缺陷。

当任何计算机系统的一个漏洞被确认后，就会被分配一个 CVE（Common Vulnerabilities and Exposure）编号。详情参考 https://cve.mitre.org/ 的“常见漏洞和披露：信息安全漏洞名称标准”。

Mitre 公司这样描述 CVE 系统：

“ CVE 是公共网络安全漏洞的常见标识符列表。世界各地 CVE 编号机构分配 CVE 标识符（或者 CEV ID），确保各方在讨论或分享一个软件或固件漏洞信息时，可以提供工具评估的基准，实现网络安全自动化的数据交换。”

漏洞扫描与渗透测试相关联，但二者却不等同。这或许是网络安全中最常见的误解之一。笔者经常通过一个或多个漏洞扫描来开始自己的渗透测试。但是，这仅仅用于辅助选择渗透测试的目标，漏洞扫描本身并不是渗透测试。

当然，漏洞扫描是安全测试的一个关键部分。正如后续章节所言，多数情况下漏洞扫描是一个自动化的过程。因此，强烈建议任何网络都要定期进行漏洞扫描。

1.1.3　渗透测试

如前面所提及的，渗透测试是为测试目标系统的安全性而真正使用黑客技术。但是，渗透测试不等同于黑客攻击。

首先从明确黑客攻击开始。不同于从媒体描述中所看到的信息，黑客攻击并非都是犯罪行为。黑客攻击是通过发现和利用系统缺陷来尝试理解系统的过程。当然，这些技术也可以用于犯罪活动。但黑客社区的多数人不会成为罪犯，也不会触犯法律。他们是试图理

解系统的研究人员。多数情况下，这些都是非正式的、个人的或者学术环境之外的研究，但仍然只是研究。简而言之，黑客攻击就是学习。

现在看一下什么是渗透测试。渗透测试是一个使用标准项目管理方法论的正式过程。渗透测试的目标是尝试利用目标系统中的漏洞。在本质上，渗透测试是渗透到系统中，因此得名“渗透测试”。

渗透测试与黑客攻击究竟有何区别？第一个也是最明显的区别就是方法。黑客攻击是一种临时性的非结构化的过程。黑客仅仅简单满足自己的好奇心。这就是说，当黑客攻击系统时，仅仅出于自己的好奇心和兴趣来探索系统的细微差异。渗透测试人员只有一个目标：测试系统安全性。对于渗透测试人员，漫无目的的好奇心是一种奢侈品，他们必须完成既定的测试目标。

第二个区别是黑客攻击和渗透测试的范围。黑客可能关注系统的某个方面，但渗透测试人员只关注事前已经确定的范围。

第三个区别是合法性。正如前面所言，黑客攻击未必是犯罪行为。很多黑客都是守法公民。当然，部分黑客也参与了犯罪活动。渗透测试人员从不参与网络犯罪。渗透测试人员通常拥有系统所有者的权限。如本章后续的讨论，实际上，无犯罪背景和完美无瑕的道德规范是渗透测试人员必须具备的品质。

1.1.4 混合测试

大型组织会分别进行审计、漏洞扫描和渗透测试。这些测试有时甚至由不同的团队实施；但对于小型组织，这种方法可能不具有成本效益。如前面所言，笔者经常通过一些漏洞扫描开始渗透测试。在混合测试中，可以扩大开始时的漏洞扫描，并将这些扫描写入最终的渗透测试报告。

在测试之前简要地回顾策略的合规性和过去的事件报告可能非常有用。这些步骤的最终产物就是进行渗透测试，其中包含漏洞评估和简要的审计。对于小型组织而言，这通常是一种经济有效的解决方案。

1.2 术语

在进一步研究之前，理解黑客和渗透测试社区中使用的基本术语非常重要。有些术语已广泛使用，可能之前就已听说过；有些术语不经常使用，可能就会有些陌生。

- **随机测试**：没有系统方法或方法论的测试。希望本书可以让读者远离这种测试。
- **黑帽黑客**：违反法律的黑客。这个术语和骇客（cracker）是同义词，但是黑帽黑客应用更广。不同于媒体描述，黑帽黑客不必具备娴熟的技能。有些触犯法律的人只掌握很少的技能。
- **骇客**：为恶意、非法或者有害的事情而侵入系统的人，是黑帽黑客的同义词。
- **道德黑客**：为合法和道德的事情而使用黑客技术的人。
- **踩点**：为了解目标而对其进行扫描。
- **灰帽黑客**：通常情况下遵守法律但某些情况下会跨越红线的黑客。

- **黑客**：试图通过逆向工程或探测系统来详细了解系统的人。这个定义非常重要。黑客不一定是罪犯。一个人可以成为黑客，永远不违法，也永远不做不道德的事情。
- **脚本小子**：对自称黑客但是技术不娴熟的人员的一种戏称。有些人下载一两个工具，学会了如何使用它们，就自我感觉是一个了不起的黑客，但事实上并非如此。
- **白帽黑客**：不触犯法律的黑客，是道德黑客的同义词。本质上，他们以合法和道德的方式运用黑客技术。

这些都是基本术语。随着本书内容的深入，会介绍更多术语。必须和术语一起讲清楚的另一个问题是黑客文化。笔者再次强调，虽然渗透测试和黑客攻击密切关联，但二者并不相同。这可能引起人们的好奇，为什么需要关注黑客文化。事实上，可以从黑客那里学到很多知识。所以，了解黑客文化非常有用。

黑客文化通常是一种探索。黑客社区中的确有人犯罪，但这不是黑客社区的全部或者大多数。事实上，不存在一个组织化和统一化的黑客社区，社区有着令人难以置信的多样化和无组织化。维系黑客社区并使之成为社区的正是对知识的渴求。这正是黑客世界的关键因素。知识才是王道。在黑客社区中，学位和认证用途不大，能够证明自己所知和所做才重要。选择参加一个重大的黑客会议（如 DEF CON）才是关键。参会者只关注学习。参会者可能对演讲者和主持人进行尖锐的批评，因此他们希望所有的演讲者和主持人可以演示一些新的可应用的知识。

黑客文化的这一特性，正是人们需要与黑客社区保持联系的重要原因。这是一个可以学习知识的地方，这些知识并不总是来自出版的图书期刊。再次重申，黑客攻击和渗透测试不是同一件事情。但渗透测试的确需要了解黑客技术。因此，尽可能多地学习各种多样化的黑客技术十分重要（本书稍后将会探索更多的黑客技术）。

虽然已经强调（并将继续强调）黑客攻击和渗透测试是互相独立并且密切相关的活动，渗透测试人员应当从热爱学习的黑客社区中汲取更多知识。渗透测试、漏洞和系统安全一直在变化。可能今天学到的渗透测试的所有知识在 24 个月后就会过时，从而需要更多新知识。有人认为这个职业特征令人敬畏，但笔者认为它令人振奋。作为一名黑客或专业渗透测试人员，将一直处于不断的终身学习中。永恒不变的是没人（即使笔者）掌握足够多的知识。渴望获取更多知识才是黑客社区的决定性特征。

1.3　方法论

方法论是区分渗透测试和黑客攻击的一个关键因素。使用什么方法进行渗透测试呢？首先研究各种通用方法，然后再深入了解更多具体的方法论。方法论有别于渗透测试标准，第 2 章将讨论标准。

1.3.1　测试本质

渗透测试包含三种主要类型，分别是黑盒测试、白盒测试和灰盒测试。名字本身就描述了在测试之前渗透测试人员所掌握的信息量。