开发者成长丛书

Python黑客渗透之道

刘晓阳 黄雪丹 ◎编著

清華大學出版社
北 京

内 容 简 介

本书以 Python 3 语言环境为基础，全面阐述黑客编程技术。从本质原理出发，融合实践项目，深入阐释用 Python 语言开发渗透工具的相关内容。

全书共 10 章。第 1 章详尽讲述实现主机和端口状态扫描的相关内容；第 2 章着重介绍如何离线破解哈希值和 PDF 文件密码，以及如何在线破解 FTP、SSH 服务认证；第 3 章阐述中间人测试技术，包括 ARP 欺骗、DNS 欺骗、嗅探数据等技术的原理与实现；第 4 章讲解实现反向连接后门的原理与实现，包括系统管理、文件管理、键盘记录等功能；第 5 章讲述勒索软件的原理和实现；第 6 章讲解窃取数据的方法，包括浏览器、粘贴板等中的数据；第 7 章和第 8 章详细介绍僵尸网络和网络蠕虫的原理与实现方法；第 9 章主要说明 SQL 注入漏洞的原理与利用；第 10 章重点讲述栈溢出漏洞原理，以及挖掘并利用该漏洞的方法。

本书示例代码丰富，实践性与系统性兼备，对每个案例都进行了详细阐述，助力读者透彻地理解书中的重点与难点。本书不仅适合初学者入门学习，工作多年的渗透测试工程师也可参考，还可作为高等院校和培训机构相关专业的教学参考书。

图书在版编目（CIP）数据

Python 黑客渗透之道 / 刘晓阳, 黄雪丹编著. 北京：清华大学出版社, 2026. 4. --（开发者成长丛书）. -- ISBN 978-7-302-71502-3

Ⅰ. TP393.081

中国国家版本馆 CIP 数据核字第 20268VK558 号

责任编辑：赵佳霓
封面设计：刘 键
责任校对：郝美丽
责任印制：刘海龙

出版发行：清华大学出版社
网 址：https://www.tup.com.cn，https://www.wqxuetang.com
地 址：北京清华大学学研大厦 A 座 邮 编：100084
社 总 机：010-83470000 邮 购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
配套资源下载：https://www.tup.com.cn，010-83470236

印 装 者：北京同文印刷有限责任公司
经 销：全国新华书店
开 本：186mm×240mm 印 张：20 字 数：440 千字
版 次：2026 年 6 月第 1 版 印 次：2026 年 6 月第 1 次印刷
印 数：1～1500
定 价：89.00 元

产品编号：111303-01

前言
PREFACE

当前，信息技术飞速发展，网络安全问题已经成为全球范围内关注的核心议题。从个人隐私数据泄露到企业核心机密被窃取，再到国家级别的网络攻击，网络威胁层出不穷，并且其形式与手段愈发复杂多样。这些威胁不仅对个人生活产生了深远影响，还对企业的运营安全、国家的公共利益与社会稳定构成了严重威胁，因此为了有效地应对这些日益严峻的挑战，掌握渗透测试技术的重要性愈加凸显。通过模拟真实攻击手段识别系统中的安全漏洞，并基于发现的问题制定针对性的防御策略，已成为保护网络安全的核心方法之一。

然而，网络攻击技术正在以极快的速度演变和升级，其复杂性和多样性对渗透测试工程师提出了更高的要求。传统的安全工具往往因功能单一、缺乏灵活性而难以满足现阶段多变的网络安全需求。在这种背景下，渗透测试工程师不仅需要熟练使用已有工具，还必须掌握开发自定义工具的能力，以便在面对复杂多变的攻击场景时，能够快速地响应并灵活应对。

在众多编程语言中，Python 凭借其简洁易学、功能强大、扩展灵活等特点，成为网络安全领域不可或缺的技术利器。Python 的语法结构直观明了，极大地降低了开发者的学习门槛；同时，其丰富的第三方模块库为安全工具的开发提供了全面支持，使渗透测试工程师能够高效地开发各种安全工具。

基于这一技术优势，本书旨在提供一条全面、系统的学习路径，帮助读者掌握如何使用 Python 开发和应用渗透测试工具，以应对实际网络安全场景中的各种挑战。本书内容兼具理论性与实用性，由浅入深，逐步引导读者深入了解 Python 在网络安全中的强大应用能力。

笔者希望，通过阅读本书，读者能够在网络安全学习的过程中少走弯路，更加系统地掌握用 Python 语言开发渗透测试工具的核心技术与方法。不论是刚接触网络安全的初学者，还是希望在职业生涯中更进一步的网络安全从业者都能通过本书提升自身的技术能力，真正实现理论与实践相结合。

同时，笔者在撰写本书的过程中，从总结实际案例到深入分析技术细节，收获了诸多新的启迪，对网络安全技术的理解更加深刻。希望本书不仅能为读者提供技术支持，更能为网络安全领域的从业者拓展视野，共同推动行业发展。

本书主要内容

第 1 章主要介绍文件操作、多线程编程和命令行参数处理等核心技术。随后，讲解了 socket 模块实现端口扫描，利用 ARP 协议结合 Scapy 模块发现活跃主机的案例。

第 2 章主要介绍暴力破解中的常用手段，包括离线破解密码哈希值与 PDF 文件密码，以及在线破解 FTP 和 SSH 服务认证。

第 3 章主要介绍 ARP 欺骗和 DNS 欺骗解析中间人攻击的原理与实现。通过嗅探 HTTP 请求等实践案例，展示如何利用 Python 构建和检测中间人攻击工具。

第 4 章主要介绍后门的设计与实现，包括反向连接、文件管理、系统命令执行及键盘记录等功能，同时讲解持久化控制技术。

第 5 章主要介绍勒索软件的运行机制，结合 Python 模块与核心加密算法，逐步实现文件加密、解密与提示信息设置等功能。

第 6 章主要介绍如何窃取浏览器凭证、粘贴板数据和操作系统信息，以获取目标系统中可能存在的敏感信息。

第 7 章主要介绍基于 SSH 和 TCP 协议构建僵尸网络的方法，涵盖主机管理、命令执行及 DDoS 攻击测试等功能。

第 8 章主要介绍网络蠕虫的工作原理，通过案例实现网络扫描、漏洞利用和载荷传播等功能。

第 9 章主要介绍 SQL 注入漏洞的原理，讲解各种注入类型及其利用技术，并结合 sqlmap 工具展示漏洞检测方法，同时提供绕过技巧与修复方案。

第 10 章主要介绍栈溢出漏洞的工作原理与利用方法，逐步讲解从定位偏移字符到剔除坏字节、查找可用模块，再到获取目标系统权限的完整过程，最后，说明生成可执行文件的方法。

本书涵盖多个领域的内容，适用于渗透测试、数字取证、恶意软件分析等领域的从业人员。通过深入浅出的理论讲解和丰富的实践案例，本书帮助读者快速提升技术能力，并能在实际工作中高效应对网络安全挑战。

资源下载提示

扫描目录上方的二维码可下载本书源码。

致谢

特别感谢清华大学出版社赵佳霓编辑及其他相关老师在写作过程中给予的支持与帮助，使本书得以顺利出版。

由于时间仓促，书中难免存在不妥之处，请读者见谅，并提宝贵意见。

刘晓阳

2026 年 2 月

本书源码

目 录

CONTENTS