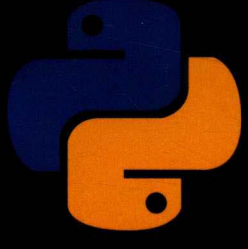
一线网络安全教师撰写，凝聚自己多年教学与实践开发经验，系统且深入阐释Python在网络安全编程方面的方法与应用

由浅入深剖析使用Python进行网络安全管理的相关技术，涉及渗透测试常见库、漏洞渗透、网络嗅探与监听、拒绝服务攻击、身份认证攻击、远程控制、无线网络渗透及Web渗透测试等

Python渗透测试编程技术

方法与实践

李华峰◎著



PYTHON PENETRATION TEST TECHNOLOGY

METHODS & PRACTICES

清华大学出版社

Python渗透测试编程技术

方法与实践

李华峰◎ 著

PYTHON PENETRATION TEST TECHNOLOGY

METHODS & PRACTICES

清华大学出版社
北京

内 容 简 介

本书由资深网络安全教师撰写，书中系统并深入地将 Python 应用实例与网络安全相结合进行讲解，不仅讲述了 Python 的实际应用方法，而且从网络安全原理的角度分析了 Python 实现网络安全编程的技术，真正做到理论与实践相结合。

全书共分为 15 章。第 1 章介绍网络安全渗透测试的相关理论。第 2 章介绍 Kali Linux 2 使用基础。第 3 章介绍 Python 语言基础。第 4 章介绍安全渗透测试中的常见模块。第 5 章介绍使用 Python 实现信息收集。第 6 章和第 7 章介绍使用 Python 对漏洞进行渗透。第 8 章介绍使用 Python 实现网络的嗅探与监听。第 9 章介绍使用 Python 实现拒绝服务攻击。第 10 章介绍使用 Python 实现身份认证攻击。第 11 章介绍使用 Python 编写远程控制工具。第 12 章和第 13 章介绍使用 Python 完成无线网络渗透。第 14 章介绍使用 Python 对 Web 应用进行渗透测试。第 15 章介绍使用 Python 生成渗透测试报告。

本书适合网络安全渗透测试人员、运维工程师、网络管理人员、网络安全设备设计人员、网络安全软件开发人员、安全课程培训学员、高校网络安全专业方向的学生阅读。

图书在版编目 (CIP) 数据

Python 渗透测试编程技术：方法与实践 / 李华峰著. —北京：清华大学出版社，2019

ISBN 978-7-302-51450-3

Ⅰ. ① P… Ⅱ. ①李… Ⅲ. ①软件工具—程序设计 Ⅳ. ① TP311.561

中国版本图书馆 CIP 数据核字（2018）第 243451 号

责任编辑： 秦 健 薛 阳
封面设计： 李召霞
责任校对： 徐俊伟
责任印制： 沈 露

出版发行： 清华大学出版社
网 址：http://www.tup.com.cn，http://www.wqbook.com
地 址：北京清华大学学研大厦 A 座　　邮 编：100084
社 总 机：010-62770175　　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
印 装 者： 北京嘉实印刷有限公司
经 销： 全国新华书店
开 本： 186mm × 240mm　　**印 张：** 18.5　　**字 数：** 390 千字
版 次： 2019 年 1 月第 1 版　　**印 次：** 2019 年 1 月第 1 次印刷
印 数： 1 ~ 2000
定 价： 69.00 元

产品编号：077507-01

Preface 前　言

为什么要写这本书

“人生苦短，我用 Python。”短短的几年时间中，Python 在国内迅速成为最热门的编程语言之一。为什么 Python 会取得如此大的成功呢？原因很简单，功能强大、简单易学就是它最大的优势。

而 Python 的到来对于国内的网络安全从业人员来说，更是一个好消息。虽然目前市面上已经有了很多功能强大的网络安全工具，但是复杂的网络环境往往是事先无法预知的，因此这些工具经常会有无法胜任的时候。如果网络安全从业人员具备编程能力，就可以弥补这些工具的不足之处。

对于网络安全从业人员来说，最重要的应该是掌握各种网络安全的缺陷。因此，目前的网络安全培训和书籍大都以工具的使用为主，而忽视了编程能力的培养。编程能力的欠缺直接造成了网络安全从业人员工作效率的低下。但是要网络安全从业人员花费大量的时间和精力去精通一门传统的编程语言，实际上也并不现实。因此，一门简单而又强大的语言才是网络安全从业人员所需要的。近年来，Python 在编程界异军突起，几乎成为最热门的编程语言无所不能，因此受到了广大网络安全行业从业人员的喜爱。假以时日，Python 语言必会成为最流行的网络安全编程语言。

在本书的编写过程中，作者一直在学校从事网络安全方面的教学。在实践中，作者发现这个专业的学生面对的最大困难就是无法将网络安全中各种分散的知识联系起来。这些年作者也一直在寻求这个难题的解决方法，在此期间参阅了大量的国外优秀图书。而最终作者发现解决这个问题的方法就是掌握一门编程语言，编程实现所有的知识点，而这门编程语言的最好选择正是 Python。本书在出版之前已经作为讲义在课堂上使用了多年，作者也根据学生的反映对其进行了增删。这些同学也成为本书最初的读者，希望这本书在给他们带来知识的同时，也能为各位读者带来一些帮助。

本书特色

本书由资深的网络安全教师撰写，内容围绕如何使用目前最受瞩目的 Python 语言进行网络安全编程展开。本书从 Python 的基础讲起，系统讲述了网络安全的作用、方法论，Python 在网络安全管理上的应用，以及 Python 在实现这些应用时相关的网络原理和技术。结合实例讲解了使用 Python 进行网络安全编程的方法，以及在实际渗透中的各种应用，包括安全工具的开发、自动化报表的生成、自定义模块的开发等，将 Python 变成读者手中的编程利器。

阅读本书的建议

（1）没有 Python 基础的读者，建议从第 1 章开始按顺序阅读并演练每一个实例。

（2）有一定 Python 基础的读者，可以根据实际情况有重点地选择阅读部分技术要点。

（3）对于每一个知识点和项目案例，先通读一遍以便有一个大概印象，然后将每个知识点的示例代码都在开发环境中操作以便加深对知识点的理解。

读者对象

本书的读者群主要是网络安全渗透测试人员、运维工程师、网络管理人员、网络安全设备设计人员、网络安全软件开发人员、安全课程培训学员、高校网络安全专业方向的学生，还包括各种非专业但却热衷于网络安全研究的人员。

目前，黑客文化的盛行，以及网络安全爱好者的日益增多，也为本书聚集了大量的潜在读者。

如何阅读本书

全书一共包括 15 章。

第 1 章主要介绍了网络安全渗透测试的相关理论。

第 2 章主要介绍了 Kali Linux 2 使用基础。

第 3 章主要介绍了 Python 语言基础。

第 4 章主要介绍了安全渗透测试中的常见模块。

第 5 章主要介绍了使用 Python 实现信息收集。

第 6 章主要介绍了使用 Python 对漏洞进行渗透的基础部分。

第 7 章主要介绍了使用 Python 对漏洞进行渗透的高级部分。

第 8 章主要介绍了使用 Python 实现网络的嗅探与监听。

第 9 章主要介绍了使用 Python 实现拒绝服务攻击。

第 10 章主要介绍了使用 Python 实现身份认证攻击。

第 11 章主要介绍了使用 Python 来编写远程控制工具。

第 12 章主要介绍了使用 Python 完成无线网络渗透基础部分。

第 13 章主要介绍了使用 Python 完成无线网络渗透高级部分。

第 14 章主要介绍了使用 Python 对 Web 应用进行渗透测试。

第 15 章主要介绍了使用 Python 生成渗透测试报告。

关于勘误

虽然作者花了很多时间和精力去核对书中的文字、代码和图片，但因为时间仓促和水平有限，书中仍难免会有一些不足和纰漏，如果读者发现问题，恳请反馈给作者，相关信息可发到邮箱 lihuafeng1999@163.com。作者会努力回答疑问或者指出一个正确的方向。

致谢

感谢所有的读者，是你们的支持促成了本书的面世。感谢作者所在单位提供了自由的科研工作环境，正是这种完全自由的氛围才使得作者多年的心血能够以文字的形式展示出来。

感谢清华大学出版社在本书的编写过程中对作者的支持。

最后感谢身边的每一位亲人、朋友以及学生，感谢你们在作者编写此书时给予的支持与理解。

Contents 目　录

CHAPTER 01

第 1 章 网络安全渗透测试

程序和网络设计者的目的是创造，而黑客的目标却是破坏和窃取。随着信息数据越来越重要，现在每一个程序都好像一家拥有大量现金的银行一样，吸引着无数心怀不轨的盗贼。遗憾的是，这些行走在二进制世界里的盗贼们恰恰是现实世界中比较聪明的人。

有什么办法能阻止这些本来只应该生活在传说中的人呢？这其实是一个困扰了人们很多年的问题。不过现在这个问题有了答案，“最了解你的人其实正是你的敌人”。既然迟早要面对黑客的入侵，那么为何不在他们下手前找出自身的弱点呢？显然设计者本身很难胜任这样的工作。那么经验丰富的黑客呢？由他们来负责检验系统的安全性是不是会更合适一些？答案是肯定的。不过此时这些进行检验的人充当的角色不再是黑客，而是网络安全渗透测试专家，他们所从事的工作也不再是破坏和窃取，而是保障系统安全。

如果你是第一次接触网络安全渗透测试这个问题，可能会对此充满好奇和期待。那么在这一章中将从以下三个主题来展开对网络安全渗透测试的学习。

（1）什么是网络安全渗透测试？

（2）如何开展网络安全渗透测试？

（3）进行网络安全渗透测试都需要掌握哪些技能？

1.1 网络安全渗透测试简介

在学习这个主题之前，先来了解一下网络安全渗透测试是什么。长期以来，在人们的心

目中常常会有如下一些错误的观点。

（1）网络安全渗透测试就是漏洞扫描，所以只需要用工具对目标进行扫描操作就可以了。一款功能强大的扫描工具的确可以比人工更快地检测出一个系统的漏洞问题，因此渗透测试者也都会使用一些工具。但是漏洞扫描仅仅是网络安全渗透测试的一个步骤，除此之外，例如目标系统设备的部署问题、使用者的安全意识等都无法通过扫描工具获得。而且单单使用工具进行扫描也无法展示出一个漏洞可能产生的后果。

（2）网络安全渗透测试就是破解。破解还有一个专业的名称，那就是逆向工程。同样，破解也是网络安全渗透测试的一个部分，破解的目的就是发掘系统的漏洞，许多优秀黑客都是以发掘了重大的漏洞而著名。但这一点和前面的漏洞扫描一样，只能作为全部渗透测试的一个环节。

（3）网络安全渗透测试就是黑客入侵。这是一个十分普遍的错误观点，黑客入侵是为了实现某种目的，例如窃取信息或者破坏系统，因此只需要找到能实现该目的的一种方法，而渗透测试则需要找出黑客实现目的的所有途径，并且给出可能产生的效果和修复的方案。

可是网络安全渗透测试是什么呢？

实际上，网络安全渗透测试严格的定义应该是一种针对目标网络进行安全检测的评估。通常这种测试由专业的网络安全渗透测试专家完成，目的是发现目标网络存在的漏洞以及安全机制方面的隐患并提出改善方法。从事渗透测试的专业人员会采用和黑客相同的方式对目标进行入侵，这样就可以检测网络现有的安全机制是否足以抵挡恶意的攻击。

根据事先对目标信息的了解程度，网络安全渗透测试的方法有黑盒测试、白盒测试和灰盒测试三种。

黑盒测试也称为外部测试。在进行黑盒测试时，事先假定渗透测试人员先期对目标网络的内部结构和所使用的程序完全不了解，从网络外部对其网络安全进行评估。黑盒测试中需要耗费大量的时间来完成对目标信息的收集。除此之外，黑盒测试对渗透测试人员的要求也是最高的。

白盒测试也称为内部测试。在进行白盒测试时，渗透测试人员必须事先清楚地知道被测试环境的内部结构和技术细节。相比黑盒测试，白盒渗透测试的目标是明确定义好的，因此白盒测试无须进行目标范围定义、信息收集等操作。这种测试的目标网络都是某个特定业务对象，因此相比黑盒测试，白盒测试能够给目标带来更大的价值。

将白盒测试和黑盒测试组合使用，就是灰盒测试。在进行灰盒测试时，渗透测试人员只能了解部分目标网络的信息，但不会掌握网络内部工作原理和限制信息。

网络安全渗透测试的目标包括一切和网络相关的基础设施，其中包括：

（1）网络设备，主要包含连接到网络的各种物理实体，如路由器、交换机、防火墙、无线接入点、服务器、个人计算机等。

（2）操作系统，是指管理和控制计算机硬件与软件资源的计算机程序。例如，个人计算机经常使用的 Windows 7、Windows 10 等，服务器上经常使用的 Windows 2012 和各种 Linux。

（3）物理安全，主要是指机房环境、通信线路等。

（4）应用程序，主要是为针对某种应用目的所使用的程序。

（5）管理制度，这部分其实是全部目标中最为重要的，指的是为保证网络安全对使用者提出的要求和做出的限制。

网络安全渗透测试的成果通常是一份报告。这个报告中应当给出目标网络中存在的威胁，以及威胁的影响程度，并给出对这些威胁的改进建议和修复方案。

另外需要注意的一点是，网络安全渗透测试并不能等同于黑客行为。相比黑客行为，网络安全渗透测试具有以下几个特点。

（1）网络安全渗透测试是商业行为，要由客户主动提出，并给予授权许可才可以进行。

（2）网络安全渗透测试必须对目标进行整体性评估，进行尽可能全面的分析。

（3）网络安全渗透测试的目的是改善用户的网络安全机制。

1.2　开展网络安全渗透测试

作为一次网络安全渗透测试的执行者，首先要明确在整个渗透测试过程中需要进行的工作。当接收到客户的渗透测试任务时，往往对于所要进行测试的目标知之甚少甚至一无所知。而在渗透测试结束的时候，对目标的了解程度已经远远超过客户。在此期间，要从事大量的研究工作，根据 pentest-standard.org 给出的渗透测试执行标准，整个渗透测试过程中的工作可以分成如下 7 个阶段。

（1）前期与客户的交流阶段。

（2）情报的收集阶段。

（3）威胁建模阶段。

（4）漏洞分析阶段。

（5）漏洞利用阶段。

（6）后渗透攻击阶段。

（7）报告阶段。

接下来分别介绍这 7 个阶段中所需要完成的工作。

1.2.1　前期与客户的交流阶段

在这个阶段中，渗透测试者需要得到客户的配合来确定整个渗透测试的范围。也就是说，

要确定对目标的哪些设备和哪些问题进行测试。而这些内容是在与客户进行了商讨之后得出的。在整个商讨的过程中，重点要考虑的因素主要如下。

1. 渗透测试的目标

通常这个目标会是一个包含很多主机的网络。这时需要确定的是渗透测试所涉及的 IP 地址范围和域名范围。但是客户所使用的 Web 应用程序和无线网络，甚至安保设备和管理制度，也可能会是渗透测试的目标。同样需要明确的还有，客户需要的是全面评估还是只针对其中某一方面或部分评估。

2. 进行渗透测试过程所使用的方法

这个阶段可以采用的方法主要有黑盒测试、白盒测试和灰盒测试三种。

3. 进行渗透测试所需要的条件

如果采用的是白盒测试，就需要客户提供测试所必需的信息和权限，客户最好可以接受问卷调查。确定可以进行渗透的时间，例如，只能在周末进行还是随时都可以进行。如果在渗透测试过程中导致目标受到了破坏，应该如何补救等。

4. 渗透测试过程中的限制条件

在整个渗透测试过程中，必须与客户明确哪些设备不能进行渗透测试，以及哪些技术不能应用。另外，也需要明确在哪些时间点不能进行渗透测试。

5. 渗透测试过程的工期

根据客户的需求，给出整个渗透测试的进度表。客户可以了解渗透测试的开始时间与结束时间，以及在每个时间段所进行的工作。

6. 渗透测试的费用

这个话题其实很少出现在一本教科书中，但是这在实践中恰恰是一个很复杂的问题，需要考虑的因素很多。例如，在对一个拥有 100 台计算机的网络进行渗透测试的时候，收取的费用为 10 万元，那么平均每一台计算机的费用就是 1000 元。但这并不是一种线性的关系，如果某个客户只要求对 1 台计算机进行渗透测试，那么费用就不能只是 1000 元，因为工作量明显不同。在计算费用的时候要充分考虑到各种成本。

7. 渗透测试过程的预期目标

作为渗透测试者必须牢记的一点是，我们并非黑客。发现目标存在的漏洞、获取目标的控制权限或者得到目标的管理密码只完成了一部分任务，还需要明确客户期望在渗透测试结束时应该达到什么目标，最终的渗透报告应该包含哪些内容。

1.2.2　情报的收集阶段

这里的“情报”指的是目标网络、服务器、应用程序的所有信息。渗透测试人员需要使用各种资源尽可能地获取要测试目标的相关信息。

如果现在采用黑盒测试的方式，那么这个阶段可以说是整个渗透测试过程中最为重要的一个阶段。所谓“知己知彼，百战不殆”也正说明了情报收集的重要性。这个阶段所使用的技术也可以分成以下两种。

1. 被动扫描

这种扫描方式通常不会被对方所发现，打一个比方，如果希望了解某一个人的信息，那么可以向他身边的人询问，如他的邻居、他的同事甚至他所在社区的工作人员。那么收集到信息又有什么呢？可能是他的名字、年龄、职业、籍贯、兴趣、学历等。

同样对于一个目标网络来说，也可以获得很多信息，例如，现在仅仅知道客户的一个域名——www.testfire.net（这是美国 IBM 公司提供的一个专门用来进行渗透测试训练的目标，所以对该目标进行扫描无须担心法律问题），通过这个域名就可以使用 Whois 查询到这个域名所有者的联系方式（包括电话号码、电子邮箱、传真、公司所在地等信息），以及域名的注册和到期时间，通过搜索引擎还可以查找与该域名相关的电子邮箱地址、博客、文件等。

2. 主动扫描

这种扫描方式的技术性比较强，通常会使用专业的扫描工具来对目标进行扫描。扫描之后将会获得的信息包括目标网络的结构、目标网络所使用设备的类型、目标主机上运行的操作系统、目标主机上所开放的端口、目标主机上所提供的服务、目标主机上所运行的应用程序等。

1.2.3　威胁建模阶段

如果将开展一次渗透测试看作指挥一场战争，那么威胁建模阶段就像是在制定战争的策略。在这个阶段有两个关键性的要素——资产和攻击者（攻击群体）。对客户的资产进行评估，可找出其中重要的资产。例如，客户是一家商业机构，那么这家机构的客户信息就是重要资产。

在这个阶段主要考虑如下问题。

（1）哪些资产是目标中的重要资产？

（2）攻击时采用什么技术和手段？

（3）哪些群体可能会对目标系统造成破坏？

（4）这些群体会使用哪些方法进行破坏？

分析以上不同群体发起攻击的可能性，可以更好地帮助确定渗透测试时所使用的技术和

工具。通常这些攻击群体可能是：

（1）有组织的犯罪机构。

（2）黑客。

（3）脚本小子。

（4）内部员工。

1.2.4 漏洞分析阶段

这个阶段是从目标中发现漏洞的过程。漏洞可能位于目标的任何一个位置。从服务器到交换机，从所使用的操作系统到 Web 应用程序，都是要检查的对象。在这个阶段会根据之前情报收集时发现的目标的操作系统、开放端口和服务程序，查找和分析目标系统中存在的漏洞。这个阶段如果单纯依靠手动分析来完成，是十分耗时耗力的，不过在 Kali Linux 2 系统中提供了大量的网络和应用漏洞评估工具，利用这些工具可以自动化地完成这些任务。另外一点需要提到的是，对目标的漏洞分析不仅限于软件和硬件，还需要考虑人的因素，也就是长时间地研究目标人员的心理，从而对其实施欺骗以便达到渗透目标。

1.2.5 漏洞利用阶段

找到目标上存在的漏洞之后，就可以利用漏洞渗透程序对目标系统进行测试了。

这个阶段中关注的重点是，如何绕过目标的安全机制来控制目标系统或访问目标资源。如果在上一阶段中顺利完成任务，那么这个阶段就可以准确顺利地进行。这个阶段的渗透测试应该具有精准的范围。漏洞利用的主要目标是获取之前评估的重要资产。最后进行渗透时还应该考虑成功的概率和对目标可能造成破坏的最大影响。

目前最为流行的漏洞渗透程序框架是 Metasploit。通常这个阶段也是最为激动人心的时刻，因为渗透测试者可以针对目标系统使用对应的入侵模块获得控制权限。

1.2.6 后渗透攻击阶段

这个阶段和上一个阶段连接十分紧密，作为一个渗透测试者，必须尽可能地将目标被渗透后所可能产生的后果模拟出来。在这个阶段可能要完成的任务包括：

（1）控制权限的提升。

（2）登录凭证的窃取。

（3）重要信息的获取。

（4）利用目标作为跳板。

（5）建立长期的控制通道。

这个阶段的主要目的是向客户展示当前网络存在的问题会带来的风险。

1.2.7　报告阶段

这个阶段是整个渗透测试阶段的最后一个阶段，同时也是最能体现工作成果的一个阶段，要将之前的所有发现以书面的形式提交给客户。实际上，这个报告也是客户唯一的需求。必须以简单、直接且尽量避免大量专业术语的形式向客户汇报测试目标中存在的问题，以及可能产生的风险。这份报告中应该指出：目标系统最重要的威胁，使用渗透数据生成的表格和图标，对目标系统存在问题的修复方案，以及对当前安全机制的改进建议等。

1.3　网络安全渗透测试需要掌握的技能

在《诸神之眼——Nmap 网络安全审计技术提秘》出版之后，作者收到了很多读者的邮件，其中大部分都问到了这个问题：如何才能成为一个合格的网络安全渗透测试者？在作者看来，如下几点是必不可少的。

（1）网络方面的知识。这方面的知识其实十分庞大，其中包括计算机体系结构，局域网技术，广域网技术，各种常见网络设备，TCP/IP 协议族中的各种技术，应用层常见的协议和软件等。

（2）渗透测试工具的使用。目前世界上存在大量的安全工具，黑客可能会利用这些工具来实现入侵。而安全渗透测试人员也可以利用这些工具提前对目标进行检查，从而提前发现目标的漏洞和缺陷等。现在这些工具的数量极为众多，而且仍然在不断增加。对于一个初学者来说，最为困难的两个问题就是在面对某个问题时如何选择正确的工具，以及如何使用这种工具。

这些问题如果放在以前的确是很难解决的，那时候作者一直有编写一本《黑客词典》的想法，按照最初的想法，就是按照功能的不同将各种工具分类，然后分别介绍该工具的功能和用法。不过很快作者就发现这几乎是一个不可能完成的任务，因为世界上的各种工具的数量实在是太多了，而且增加的速度也太快了。

不过现在因为 Kali Linux 操作系统的出现，这个问题已经得到了解决，在这个系统中集成了大量优秀的安全工具，而且 Kali Linux 中也对这些工具进行了分类，节省了用户大量的精力和时间。所以本书的实验都采用 Kali Linux 操作系统作为环境。

（3）程序的编写。既然已经有了那么多优秀的安全工具，为什么还要学习编写程序呢？很多所谓的黑客，甚至上了新闻宣传的黑客，并不会编程，他们通常使用别人开发的程序恶意破坏系统，这些人也被称为“脚本小子”。这可不是一个褒义词，在计算机的世界中不会编程就如同在现实世界中无法讲话。

程序的编写也正是本书的内容，作为一个合格的安全渗透测试人员，最好熟练掌握一门