TURING 图灵程序设计丛书

FREELEC

Python

Python Hacking Exercises

黑客攻防入门

【韩】赵诚文 郑暎勋 著 武传海 译

中国工信出版集团 人民邮电出版社 POSTS & TELECOM PRESS

TURING 图灵程序设计丛书

Python 黑客攻防入门

【韩】赵诚文 郑暎勋 著 武传海 译

Python Hacking Exercises

人民邮电出版社
北京

图书在版编目（CIP）数据

Python黑客攻防入门 /（韩）赵诚文，（韩）郑暎勋著；武传海译. -- 北京：人民邮电出版社，2018.1
（图灵程序设计丛书）
ISBN 978-7-115-47300-4

Ⅰ. ①P… Ⅱ. ①赵… ②郑… ③武… Ⅲ. ①黑客－网络防御 Ⅳ. ①TP393.081

中国版本图书馆CIP数据核字（2017）第284377号

内 容 提 要

全书内容划分为基础知识、各种黑客攻击技术、黑客攻击学习方法三部分。基础知识部分主要介绍各种黑客攻击技术、计算机基础知识以及Python基本语法；第二部分讲解各种黑客攻击技术时，具体划分为应用程序黑客攻击、Web黑客攻击、网络黑客攻击、系统黑客攻击等；最后一部分给出学习建议，告诉大家如何才能成为顶尖黑客。

◆ 著　　[韩] 赵诚文　郑暎勋
译　　武传海
审　　校　OWASP子明
责任编辑　陈　曦
责任印制　彭志环
◆ 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
北京圣夫亚美印刷有限公司印刷
◆ 开本：800×1000　1/16
印张：15.75
字数：350千字　　2018年1月第1版
印数：1-3 000册　　2018年1月北京第1次印刷
著作权合同登记号　图字：01-2015-1717号

定价：59.00元

读者服务热线：(010)51095186转600　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

站在巨人的肩上

Standing on Shoulders of Giants

iTuring.cn

推荐序

以前的 Python 书籍都以编程、网络爬虫等内容居多，针对如何用 Python 编写网络攻防相关的书籍较少，而本书就是关于这部分内容的好书。

本书第一部分先介绍了黑客与白帽黑客的区别，让大家清楚地理解“什么是黑客”，第二部分介绍了 Web 攻击手段（OWASP Top 10 等）、主流系统攻击手段（缓冲区溢出等）、网络攻击手段（拒绝服务攻击等），第三部分介绍具备前两部分的综合能力之后，如何利用自身的编程功底编写攻防工具。

作为 OWASP 中国北京区的负责人，我个人推荐相关的计算机专业以及信息安全专业的专科和本科学生通过本书进行学习，从事信息安全相关社会工作的人员也可以阅读本书提高自身水平。

感谢图灵公司能将此书引入国内，同时也感谢译者的辛苦劳动。作为本书的校验者我感到非常荣幸，但由于自身基础还相对欠缺，校验过程中多少还是会有些问题，请各位读者见谅。

OWASP 子明

OWASP 中国负责人

作者序

赵诚文（iaman1016@gmail.com）

在本书写作过程中，我遇到了很多困难，感谢所有帮助过我的人。

我平时经常在公司加班，没有时间写作，所以只好周末去图书馆写书。感谢妻子与两个儿子，谢谢你们对我的支持与理解。本书历时一年才得以付梓，谨以此书献给我的家人，以表歉意。

在人生道路上，我曾一度迷失，感谢郑暎勋先生将我带入 Python 黑客攻击世界。他是本书的共同作者，也是我的好老师，是他教会我如何将自己掌握的知识写入本书。

还要感谢李相韩、具光民、郑尚美、朴宰根等几位，他们丰富的经验让我受益良多。

最后，感谢身边的所有朋友，谢谢你们的支持与鼓励。

郑暎勋

与发达国家不同，韩国大部分人对黑客攻击仍然抱有否定看法。由于缺少“白帽黑客”成长的土壤，人们也很少有机会能够接受到良好的相关领域教育。这也造成很多韩国人道德意识淡薄，滥用网上的各种黑客攻击工具与资料实施恶意攻击，产生了恶劣的负面影响。本书写作初衷是向对黑客攻击感兴趣的朋友讲解计算机有关基础知识及工作原理，介绍各种黑客攻击技术，督促人们提高网络安全意识。本书讲解黑客攻击技术原理时，采用 Python 语言。它易学易用，非常适合用于编写黑客攻击程序。

书中大量实操与练习示例都经过了赵诚文先生的测试，感谢他夜以继日的努力付出。本书写作也得到了李相韩先生和朋友奎达的大力支持与帮助，在此表示感谢。

最后，感谢妻子秀美、大女儿雅茵、二女儿诗雨，谢谢你们一直以来的关心与支持，我爱你们。

前　言

“数学定理”般的黑客攻击基础用书

近年来，信息安全需求激增，大学纷纷开设信息安全专业，各地也举办各种形式的黑客攻防大赛。各企业开始构建安全系统，接受安全咨询，以合乎法律法规要求。

黑客攻击是安全之“花”。足球比赛中，前锋最引人注目；安全领域中，黑客则最受人关注。只要是IT领域的从业人员，应该都曾经梦想过成为一名黑客。很多人都对黑客攻击感兴趣，但讲解有关黑客攻击技术的图书并不多。并且现有的图书就像拼图中的一小块，只深入讲解了黑客攻击的某个方面。接触一个新概念时，最好先把握其整体轮廓，然后再选择自己感兴趣的部分深入学习。

我们从初中升入高中后，会感觉数学课突然变难。学习中最常见的是“数学定理”，它们能够将复杂概念阐述清楚，再辅以示例，帮助我们比较容易地理解其内容。

我写作本书的初衷就是将其打造为黑客攻击领域中的“数学定理”。事实上，黑客攻击涉及的知识领域庞大，仅凭一本书很难成为一名合格的黑客。通过阅读本书，各位会对黑客攻击形成基本的认识，知道成为一名黑客要学习哪些内容。这样，本书才能称得上是黑客攻击领域的“数学定理”。

搭建成本低廉、易学易用的测试环境

本书特色之一就是使用虚拟机搭建黑客攻击学习环境，使学习更快速、更容易，且成本低廉。

只需一台物理PC机即可测试书中所有示例代码。也就是说，学习书中的黑客攻击知识时，并不需要另外购买实际物理设备。读者可以直接查看所有示例代码的运行结果，不会产生似是而非的模糊认识。关于测试环境的搭建，书中进行了详细说明，即使是初学者也能轻松完成。讲解相关内容时，我们针对每个关键步骤都给出了截图，各位不必忧虑，只要跟着书中讲解逐步进行即可。与文字相比，使用图示能够更容易地传递多种知识。因此，本书讲解相关概念时，插入了许多进行辅助说明的示意图，并且为每个操作步骤编号，按顺序进行讲解。

最后，希望本书能够让各位感受到黑客攻击的真正乐趣。

本书结构

为了使各位对整个黑客攻击领域有总体认识，全书内容划分为基础知识、各种黑客攻击技术、黑客攻击学习方法三部分。基础知识部分主要介绍各种黑客攻击技术、计算机基础知识以及Python 基本语法；第二部分讲解各种黑客攻击技术时，具体划分为应用程序黑客攻击、Web 黑客攻击、网络黑客攻击、系统黑客攻击等；最后一部分给出学习建议，告诉大家如何才能成为顶尖黑客。

讲解每种黑客攻击技术时，将分别从概念、黑客攻击代码、工作原理、运行结果等方面进行详细说明。通过介绍概念，大家可以掌握相关基础知识；编写黑客攻击代码，让各位熟悉实操感觉。逐一讲解黑客攻击代码的工作原理，并通过运行结果检查代码编写是否正确。

本书分为如下三部分。

第一部分　黑客攻击基础知识（第 1~4 章）

要想成为一名合格的黑客，不仅要掌握相关攻击技术，还要学习计算机有关的各种知识。这部分讲解了黑客是什么样的人，并介绍了多种黑客攻击技术以及进行黑客攻击必备的基础知识。第 4 章简单介绍了 Python 基本语法，这些是编写黑客攻击程序必需的知识。

第二部分　各种黑客攻击技术（第 5~8 章）

这部分详细介绍使用 VirtualBox 搭建测试环境的过程，只要遵循书中介绍的搭建步骤，任何人都能轻松完成。书中所用示例都比较简单，学习过程中，大家可以亲自动手编写应用程序、Web、网络、系统的黑客攻击代码，并观察代码执行结果。掌握书中介绍的所有示例代码后，即可上网自己学习新的黑客攻击技术。

第三部分　高级黑客修炼之路（第 9 章）

本书旨在向各位介绍黑客攻击的基本概念。如果认真学习了前 8 章，就会想学习更高级的黑客攻击技术。本书最后一部分将告诉各位成为顶尖黑客需要学习哪些内容。

测试环境

黑客攻击受测试环境影响较大。如果示例代码无法正常运行，请对照下表，检查测试环境是否搭建正确。必须安装 32 位版本 Windows 和 2.7.6 版本 Python。

程序	版本	网址
Windows	7 professional 32 bits	http://www.microsoft.com/ko-kr/default.aspx
Python	2.7.6	http://www.python.org/download
PaiMei	1.1 REV122	http://www.openrce.org/downloads/details/208/PaiMei
VirtualBox	4.3.10 r93012	https://www.virtualbox.org/wiki/Downloads
APM	APMSETUP 7 Apache 2.2.14 (openssl 0.9.8k) PHP 5.2.12 MySQL 5.1.39 phpMyAdmin 3.2.3	http://www.apmsetup.com/download.php http://httpd.apache.org http://windows.php.net http://www.mysql.com http://www.phpmyadmin.net
WordPress	3.8.1	http://ko.wordpress.org/releases/#older
HTTP Analyzer	Stand-alone V7.1.1.445	http://www.ieinspector.com/download.html
NMap	6.46	http://nmap.org/download.html
Python-nmap	0.3.3	http://xael.org/norman/python/python-nmap/
Wireshark	1.10.7	https://www.wireshark.org/download.html
Linux	Ubuntu 12.04.4 LTS Pricise Pangolin	http://releases.ubuntu.com/precise/
pyloris	3.2	http://sourceforge.net/projects/pyloris/
py2exe	py2exe-0.6.9.win32-py2.7.exe	http://www.py2exe.org/
BlazeDVD	5.2.0.1	http://www.exploit-db.com/exploits/26889
adrenalin	2.2.5.3	http://www.exploit-db.com/exploits/26525/

目 录

第 1 章 概要

第 2 章 黑客攻击技术

第 3 章 基础知识

第 5 章 应用程序黑客攻击

第 6 章 Web 黑客攻击