

# 《python绝技：运用python》

## 图书基本信息

书名：《python绝技：运用python成为顶级黑客》

13位ISBN编号：9787121277131

出版时间：2016-1

作者：[美] TJ O'Connor

页数：264

译者：崔孝晨,武晓音

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu111.com](http://www.tushu111.com)

# 《python绝技：运用python》

## 内容概要

Python 是一门常用的编程语言，它不仅上手容易，而且还拥有丰富的支持库。对经常需要针对自己所处的特定场景编写专用工具的黑客、计算机犯罪调查人员、渗透测试师和安全工程师来说，Python 的这些特点可以帮助他们又快又好地完成这一任务，以极少的代码量实现所需的功能。《Python绝技：运用Python成为顶级黑客》结合具体的场景和真实的案例，详述了 Python 在渗透测试、电子取证、网络流量分析、无线安全、网站中信息的自动抓取、病毒免杀等领域内所发挥的巨大作用。

《Python绝技：运用Python成为顶级黑客》适合计算机安全管理人员、计算机犯罪调查和电子取证人员、渗透测试人员，以及所有对计算机安全感兴趣的爱好者阅读。同时也可供计算机、信息安全及相关专业的本/专科院校师生学习参考。

## 作者简介

参编作者——Robert Frost

2011年 Robert Frost 毕业于美国军事学院，随后成为一名陆军通信兵。他以优异的成绩获得了计算机科学的理学学士学位，其毕业论文主要关注于开源信息的收集。在 2011 年度电子防御练习赛中，由于他规避规则的能力，Rob 个人被公认为国家锦标赛团队中最优秀的两名成员之一。Rob 也参加并赢得了多次电子安全竞赛。

技术编辑——Mark Baggett

Mark Baggett 是 SANS 的认证讲师，担任了 SANS 的渗透测试课程体系中多门课程的授课任务。Mark 是提供应急响应和渗透测试服务的深度防御公司的首席顾问和创始人。目前他是 SANS 防御部门的技术指导教师，专注于把 SANS 的资源实际应用于提升军事能力的方向。Mark 在跨国公司和财富 1000 强企业中拥有多个信息安全职位。他曾经是一名软件开发者、网络和系统工程师、安全管理员和 CISO（首席信息安全官）。作为一名首席信息安全官，Mark 对信息安全策略的制定、遵守情况、应急事件的响应，以及其他信息安全操作负责。Mark 掌握当前在销售、实现和支持信息安全时，信息安全专家所面临挑战的第一手资料。Mark 也是信息安全社区中的一名活跃成员，是 Greater Augusta ISSA 的创始人兼总裁。他拥有包括 SANS 声誉卓著的 GSE 在内的多张认证证书。Mark 的个人博客中对多个安全主题均有涉猎，其地址为：<http://www.pauldotcom.com>。

# 《python绝技：运用python》

## 书籍目录

序一	
III	
序二	
V	
译者序	
VII	
致谢	
IX	
参编作者——Robert Frost	
X	
技术编辑——Mark Baggett	
XI	
前言——Mark Baggett	
XII	
第1章 入门	
1	
引言：使用Python进行渗透测试	
1	
准备开发环境	
2	
安装第三方库	
2	
Python解释与Python交互	
5	
Python语言	
6	
变量	
6	
字符串	
7	
List ( 列表 )	
7	
词典	
8	
网络	
9	
条件选择语句	
9	
异常处理	
10	
函数	
11	
迭代	
13	
文件输入/输出	
15	
sys模块	

16	
OS模块	
17	
第一个Python程序	
19	
第一个程序的背景材料：布谷蛋	
19	
第一个程序：UNIX口令破解机	
20	
第二个程序的背景材料：度恶为善	
22	
第二个程序：一个Zip文件口令破解机	
23	
本章小结	
27	
参考文献	
28	
第2章 用Python进行渗透测试	
29	
引言：Morris蠕虫现在还有用吗	
29	
编写一个端口扫描器	
30	
TCP全连接扫描	
30	
抓取应用的Banner	
32	
线程扫描	
34	
使用NMAP端口扫描代码	
36	
用Python构建一个SSH僵尸网络	
38	
用Pexpect与SSH交互	
39	
用Pxssh暴力破解SSH密码	
42	
利用SSH中的弱私钥	
45	
构建SSH僵尸网络	
49	
利用FTP与Web批量抓“肉机”	
52	
用Python构建匿名FTP扫描器	
53	
使用Ftplib暴力破解FTP用户口令	
54	
在FTP服务器上搜索网页	
55	

在网页中加入恶意注入代码

56

整合全部的攻击

58

Conficker，为什么努力做就够了

62

使用Metasploit攻击Windows SMB服务

64

编写Python脚本与Metasploit交互

65

暴力破解口令，远程执行一个进程

67

把所有的代码放在一起，构成我们自己的Conficker

67

编写你自己的0day概念验证代码

70

基于栈的缓冲区溢出攻击

70

添加攻击的关键元素

71

发送漏洞利用代码

72

汇总得到完整的漏洞利用脚本

73

本章小结

75

参考文献

75

第3章 用Python进行取证调查

77

引言：如何通过电子取证解决BTK凶杀案

77

你曾经去过哪里？——在注册表中分析无线访问热点

78

使用WinReg读取Windows注册表中的内容

79

使用Mechanize把MAC地址传给Wigle

81

用Python恢复被删入回收站中的内容

85

使用OS模块寻找被删除的文件/文件夹

85

用Python把SID和用户名关联起来

86

元数据

88

使用PyPDF解析PDF文件中的元数据

88

理解Exif元数据

90	
用BeautifulSoup下载图片	
91	
用Python的图像处理库读取图片中的Exif元数据	
92	
用Python分析应用程序的使用记录	
95	
理解Skype中的SQLite3数据库	
95	
使用Python和SQLite3自动查询Skype的数据库	
97	
用Python解析火狐浏览器的SQLite3数据库	
103	
用Python调查iTunes的手机备份	
111	
本章小结	
116	
参考文献	
116	
第4章 用Python分析网络流量	
119	
引言：“极光”行动以及为什么明显的迹象会被忽视	
119	
IP流量将何去何从？——用Python回答	
120	
使用PyGeolIP关联IP地址和物理位置	
121	
使用Dpkt解析包	
121	
使用Python画谷歌地图	
125	
“匿名者”真能匿名吗？分析LOIC流量	
128	
使用Dpkt发现下载LOIC的行为	
128	
解析Hive服务器上的IRC命令	
130	
实时检测DDoS攻击	
131	
H.D.Moore是如何解决五角大楼的麻烦的	
136	
理解TTL字段	
136	
用Scapy解析TTL字段的值	
138	
“风暴”（Storm）的fast-flux和Conficker的domain-flux	
141	
你的DNS知道一些不为你所知的吗？	
142	

使用Scapy解析DNS流量	143
用Scapy找出fast-flux流量	144
用Scapy找出Domain Flux流量	145
Kevin Mitnick和TCP序列号预测	146
预测你自己的TCP序列号	147
使用Scapy制造SYN泛洪攻击	148
计算TCP序列号	148
伪造TCP连接	150
使用Scapy愚弄入侵检测系统	153
本章小结	159
参考文献	159
第5章 用Python进行无线网络攻击	161
引言：无线网络的（不）安全性和冰人	161
搭建无线网络攻击环境	162
用Scapy测试无线网卡的嗅探功能	162
安装Python蓝牙包	163
绵羊墙——被动窃听无线网络中传输的秘密	165
使用Python正则表达式嗅探信用卡信息	165
嗅探宾馆住客	168
编写谷歌键盘记录器	171
嗅探FTP登录口令	174
你带着笔记本电脑去过哪里？Python告诉你	176
侦听802.11 Probe请求	176
寻找隐藏网络的802.11信标	177
找出隐藏的802.11网络的网络名	

178	
用Python截取和监视无人机	
179	
截取数据包，解析协议	
179	
用Scapy制作802.11数据帧	
181	
完成攻击，使无人机紧急迫降	
184	
探测火绵羊	
186	
理解Wordpress的会话cookies	
187	
牧羊人——找出Wordpress Cookie重放攻击	
188	
用Python搜寻蓝牙	
190	
截取无线流量，查找（隐藏的）蓝牙设备地址	
192	
扫描蓝牙RFCOMM信道	
195	
使用蓝牙服务发现协议	
196	
用Python ObexFTP控制打印机	
197	
用Python利用手机中的BlueBug漏洞	
197	
本章小结	
199	
参考文献	
199	
第6章 用Python刺探网络	
201	
引言：当今的社会工程	
201	
攻击前的侦察行动	
202	
使用Mechanize库上网	
202	
匿名性——使用代理服务器、User-Agent及cookie	
203	
把代码集成在Python类的AnonBrowser中	
206	
用anonBrowser抓取更多的Web页面	
208	
用Beautiful Soup解析Href链接	
209	
用Beautiful Soup映射图像	
211	

研究、调查、发现

213

用Python与谷歌API交互

213

用Python解析Tweets个人主页

216

从推文中提取地理位置信息

218

用正则表达式解析Twitter用户的兴趣爱好

220

匿名电子邮件

225

批量社工

226

使用Smtplib给目标对象发邮件

226

用smtplib进行网络钓鱼

227

本章小结

230

参考文献

231

第7章 用Python实现免杀

233

引言：火焰腾起！

233

免杀的过程

234

免杀验证

237

本章小结

243

参考文献

243

# 《python绝技：运用python》

## 精彩短评

- 1、科普了几个常用库
- 2、略坑。
- 3、有点虚...
- 4、全书最精彩的地方就是序言！
- 5、Violent Python中文版，都是介绍python能做什么什么的，还不如直接去看代码呢
- 6、之前大概看了看，以后再接着读吧。
- 7、感觉买坑了...以为是砖头书。。。
- 8、和python黑帽子有点相似，看了下电子版便放弃了纸质版的念头，介绍了几个库的用法和一些攻击思路，有些还不太实用。
- 9、有点儿看不懂啊
- 10、还是叫做python进阶更好，而且这书抢钱啊，这么贵

# 《python绝技：运用python》

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:[www.tushu111.com](http://www.tushu111.com)