BLACK HAT PYTHON

2nd Edition

Python Programming for Hackers and Pentesters

by Justin Seitz and Tim Arnold

no starch
press

San Francisco

BLACK HAT PYTHON, 2ND EDITION. Copyright © 2021 by Justin Seitz and Tim Arnold.

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

ISBN-13: 978-1-7185-0112-6 (print)
ISBN-13: 978-1-7185-0113-3 (ebook)

Publisher: William Pollock
Executive Editor: Barbara Yien
Production Editor: Dapinder Dosanjh
Developmental Editor: Frances Saux
Cover Illustration: Garry Booth
Interior Design: Octopod Studios
Technical Reviewer: Cliff Janzen
Copyeditor: Bart Reed
Compositor: Jeff Lytle, Happenstance Type-O-Rama
Proofreader: Sharon Wilkey

For information on book distributors or translations, please contact No Starch Press, Inc. directly:
No Starch Press, Inc.
245 8th Street, San Francisco, CA 94103
phone: 1-415-863-9900; info@nostarch.com
www.nostarch.com

Library of Congress Control Number: 2014953241

No Starch Press and the No Starch Press logo are registered trademarks of No Starch Press, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, we are using the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The information in this book is distributed on an “As Is” basis, without warranty. While every precaution has been taken in the preparation of this work, neither the authors nor No Starch Press, Inc. shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in it.

[S]

To my beautiful wife, Clare. I love you.
—Justin

About the Authors

Justin Seitz is a renowned cybersecurity and open source intelligence practitioner and the co-founder of Dark River Systems Inc., a Canadian security and intelligence company. His work has been featured in *Popular Science*, *Motherboard*, and *Forbes*. Justin has authored two books on developing hacking tools. He created the AutomatingOSINT.com training platform and Hunchly, an open source intelligence collection tool for investigators. Justin is also a contributor to the citizen journalism site Bellingcat, a member of the International Criminal Court's Technical Advisory Board, and a Fellow at the Center for Advanced Defense Studies in Washington, DC.

Tim Arnold is currently a professional Python programmer and statistician. He spent much of his early career at North Carolina State University as a respected international speaker and educator. Among his accomplishments, he has ensured that educational tools are accessible to underserved communities worldwide, including making mathematical documentation accessible to the blind.

For the past many years, Tim has worked at SAS Institute as a principal software developer, designing and implementing a publishing system for technical and mathematical documentation. He has served on the board of the Raleigh ISSA and as a consultant to board of the International Statistical Institute. He enjoys working as an independent educator, making infosec and Python concepts available to new users and elevating those with more advanced skills. Tim lives in North Carolina with his wife, Treva, and a villainous cockatiel named Sidney. You can find him on Twitter at @jtimarnold.

About the Technical Reviewer

Since the early days of Commodore PET and VIC-20, technology has been a constant companion to **Cliff Janzen**—and sometimes an obsession! Cliff spends a majority of his workday managing and mentoring a great team of security professionals, striving to stay technically relevant by tackling everything from security policy reviews and penetration testing to incident response. He feels lucky to have a career that is also his favorite hobby and a wife who supports him. He is grateful to Justin for including him on the first edition of this wonderful book and to Tim for leading him to finally make the move to Python 3. And special thanks to the fine people at No Starch Press.

BRIEF CONTENTS

Foreword xv

Preface xvii

Acknowledgments xix

Chapter 1: Setting Up Your Python Environment 1

Chapter 2: Basic Networking Tools 9

Chapter 3: Writing a Sniffer 35

Chapter 4: Owning the Network with Scapy 53

Chapter 5: Web Hackery 71

Chapter 6: Extending Burp Proxy 93

Chapter 7: GitHub Command and Control 117

Chapter 8: Common Trojaning Tasks on Windows 127

Chapter 9: Fun with Exfiltration 139

Chapter 10: Windows Privilege Escalation 153

Chapter 11: Offensive Forensics 169

Index 185

CONTENTS IN DETAIL

FOREWORD XV

PREFACE XVII

ACKNOWLEDGMENTS XIX

1
SETTING UP YOUR PYTHON ENVIRONMENT 1

Installing Kali Linux . . . 2
Setting Up Python 3 . . . 3
Installing an IDE . . . 5
Code Hygiene . . . 5

2
BASIC NETWORKING TOOLS 9

Python Networking in a Paragraph . . . 10
TCP Client . . . 10
UDP Client . . . 11
TCP Server . . . 12
Replacing Netcat . . . 13
    Kicking the Tires . . . 17
Building a TCP Proxy . . . 19
    Kicking the Tires . . . 24
SSH with Paramiko . . . 26
    Kicking the Tires . . . 30
SSH Tunneling . . . 30
    Kicking the Tires . . . 34

3
WRITING A SNIFFER 35

Building a UDP Host Discovery Tool . . . 36
Packet Sniffing on Windows and Linux . . . 36
    Kicking the Tires . . . 38
Decoding the IP Layer . . . 38
    The ctypes Module . . . 39
    The struct Module . . . 41
    Writing the IP Decoder . . . 43
    Kicking the Tires . . . 45
Decoding ICMP . . . 46
    Kicking the Tires . . . 50

4
OWNING THE NETWORK WITH SCAPY 53

Stealing Email Credentials 54
    Kicking the Tires 57
ARP Cache Poisoning with Scapy 57
    Kicking the Tires 62
pcap Processing 63
    Kicking the Tires 69

5
WEB HACKERY 71

Using Web Libraries 72
    The urllib2 Library for Python 2.x 72
    The urllib Library for Python 3.x 73
    The requests Library 74
    The lxml and BeautifulSoup Packages 74
Mapping Open Source Web App Installations 76
    Mapping the WordPress Framework 76
    Testing the Live Target 80
    Kicking the Tires 81
Brute-Forcing Directories and File Locations 82
    Kicking the Tires 85
Brute-Forcing HTML Form Authentication 85
    Kicking the Tires 90

6
EXTENDING BURP PROXY 93

Setting Up 94
Burp Fuzzing 95
    Kicking the Tires 101
Using Bing for Burp 104
    Kicking the Tires 108
Turning Website Content into Password Gold 110
    Kicking the Tires 113

7
GITHUB COMMAND AND CONTROL 117

Setting Up a GitHub Account 118
Creating Modules 119
Configuring the Trojan 120
Building a GitHub-Aware Trojan 121
    Hacking Python's import Functionality 123
    Kicking the Tires 124

8
COMMON TROJANING TASKS ON WINDOWS 127

Keylogging for Fun and Keystrokes. 128
Kicking the Tires 130
Taking Screenshots 131
Pythonic Shellcode Execution 132
Kicking the Tires 134
Sandbox Detection 135

9
FUN WITH EXFILTRATION 139

Encrypting and Decrypting Files. 140
Email Exfiltration 142
File Transfer Exfiltration 144
Exfiltration via a Web Server 145
Putting It All Together 148
Kicking the Tires 150

10
WINDOWS PRIVILEGE ESCALATION 153

Installing the Prerequisites 154
Creating the Vulnerable BlackHat Service 154
Creating a Process Monitor 156
Process Monitoring with WMI. 157
Kicking the Tires 158
Windows Token Privileges 159
Winning the Race 161
Kicking the Tires 164
Code Injection 164
Kicking the Tires 166

11
OFFENSIVE FORENSICS 169

Installation. 170
General Reconnaissance. 171
User Reconnaissance 173
Vulnerability Reconnaissance. 176
The volshell Interface 177
Custom Volatility Plug-Ins 177
Kicking the Tires 182
Onward!. 184

INDEX 185