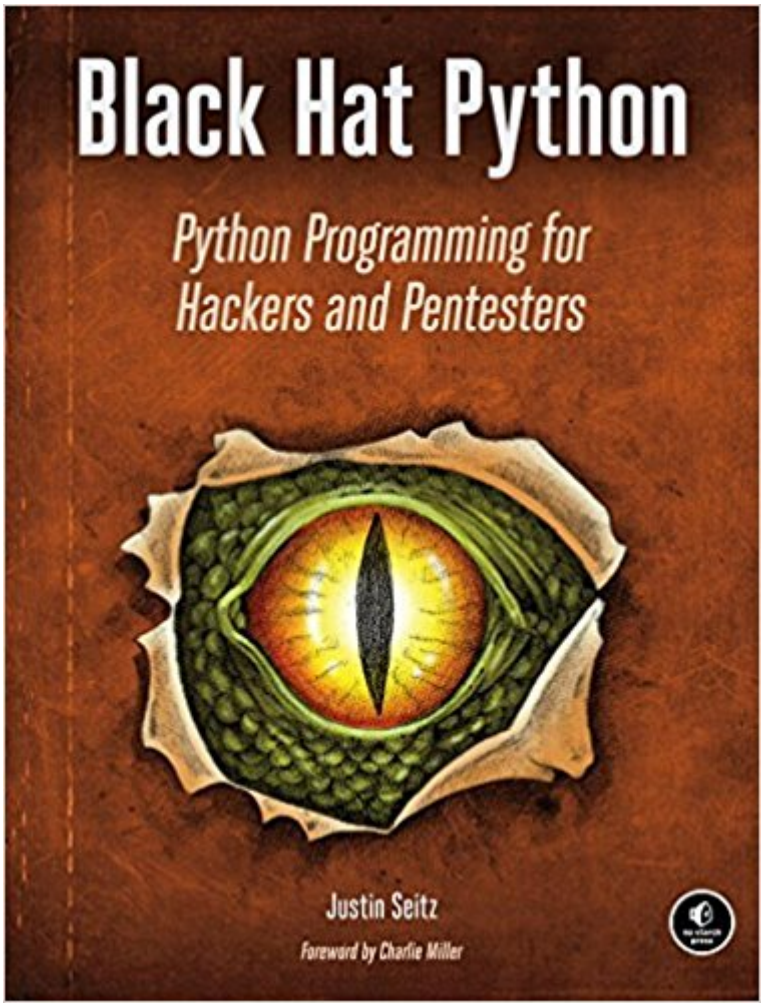
Black Hat Python: Python Programming For Hackers And Pentesters



Synopsis

When it comes to creating powerful and effective hacking tools, Python is the language of choice for most security analysts. But just how does the magic happen?In Black Hat Python, the latest from Justin Seitz (author of the best-selling Gray Hat Python), youÃ¢â ¬â„¢ll explore the darker side of PythonÃ¢â ¬â„¢s capabilitiesÃ¢â ¬â •writing network sniffers, manipulating packets, infecting virtual machines, creating stealthy trojans, and more.YouÃ¢â ¬â„¢ll learn how to:Ã¢â ¬â œCreate a trojan command-and-control using GitHubÃ¢â ¬â œDetect sandboxing and automate comÃ Â- mon malware tasks, like keylogging and screenshottingÃ¢â ¬â œEscalate Windows privileges with creative process controlÃ¢â ¬â œUse offensive memory forensics tricks to retrieve password hashes and inject shellcode into a virtual machineÃ¢â ¬â œExtend the popular Burp Suite web-hacking toolÃ¢â ¬â œAbuse Windows COM automation to perform a man-in-the-browser attackÃ¢â ¬â œExfiltrate data from a network most sneakilyInsider techniques and creative challenges throughout show you how to extend the hacks and how to write your own exploits.When it comes to offensive security, your ability to create powerful tools on the fly is indispensable. Learn how in Black Hat Python.Uses Python 2

Book Information

Paperback: 192 pages

Publisher: No Starch Press; 1 edition (December 21, 2014)

Language: English

ISBN-10: 1593275900

ISBN-13: 978-1593275907

Product Dimensions: 7.1 x 0.6 x 9.2 inches

Shipping Weight: 15.2 ounces (View shipping rates and policies)

Average Customer Review: 4.2 out of 5 stars 82 customer reviews

Best Sellers Rank: #36,293 in Books (See Top 100 in Books) #11 inÃ Â Books > Computers & Technology > Security & Encryption > Viruses #20 inÃ Â Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #30 inÃ Â Books > Computers & Technology > Internet & Social Media > Hacking

Customer Reviews

"Whether you’re interested in becoming a serious hacker/penetration tester or just want to know how they work, this book is one you need to read. Intense, technically sound, and eye-opening."

Justin Seitz is a senior security researcher for Immunity, Inc., where he spends his time bug hunting, reverse engineering, writing exploits, and coding Python. He is the author of Gray Hat Python (No Starch Press), the first book to cover Python for security analysis.

You will love this book, especially if you already have some programming knowledge. You'll have some fun to play with and fully functioning tools written by you by the end of chapter 2.

Great book with some good techniques. Would absolutely recommend to any security researching looking to build their own tools in python

Has some great examples and tools in the book. Haven't used them all but am enjoying the book so far.

Very good book and maybe not for beginners. Did not finish yet but very looking forward to.

I just got this book in the mail earlier today and couldn't help but sit down and read through the entire thing. Starting from chapter two, author Justin Seitz walks you through the creation of classic networking tools in the popular Python programming language (Chapter 1 focuses on setting up your environment). From netcat to proxies to SSH tunnels, the amount of information packed in is amazing. He then delves deeper into the world of network analysis and shows you how to write your own sniffers leading to a pared-down nmap implementation. The best part is that you learn all of this while staying essentially crippled- Seitz doesn't just introduce one of Python's many libraries and just say "Play", he walks your though all the nitty gritty details along the way. It's great.He then pulls you from the dark undergrounds of low(ish) level socket programming to show you what Python can do against application-layer targets. You begin with learning to bruteforce directories and image locations before quickly moving to extending Burp Suite to fit whatever your needs may be. From there, you get into some of the heavier materials by taking another step further from networks to create command and control points for a trojan that you eventually get around to writing. Keylogging, surreptitious screenshots, and even rooting techniques become your new playground.There's more, naturally, but I feel as though you can get the point clearly enough looking through the table of contents. Besides, I wouldn't want to spoil all the fun. Suffice it to say, by the end of this book you'll be leaps and bounds closer to understanding not only how the "bad guys" get into you computer, exfiltrate your data, and maintain access over time, but you may even be able to

create software of your own to detect and avoid them.All this being said, I can’t help but remain a little bit disappointed in the overall amount of material presented. The book tops off at a measly 161 pages (pretty much the same as Gray Hat Python), but with the vast majority being code samples and screenshots I feel almost a little bit let down. Print is a fantastic medium for many things, but presenting a few code snippets that can be found through some (albeit extensive) Googling with matching explanations may not be one of them. It also would have been nice if the author pointed us towards online resources for more information regarding the tools we ultimately create. Don’t let this turn you away, though. If you’re interested in a one-stop-shop for your lessons in using Python for hacking and penetration testing, look no further because this book rocks.

Going to give this book 5 stars because the author does an excellent job of explaining Python in an informal way. Easily taking someone from a beginner level to a more advanced level. However I must add that in Chapter 1, it was nowhere near as easy to set up WingIDE as he explained. Now to be fair I was installing on Kali 2.0, but I downloaded the newest versions as well as the exact versions that were in the book. Still with no success. Yes I also tried the dependency command that was given as well as hours of Linux "dependency" posts. The program looks great so I still try to correct the dependency issue from time to time but initially I just gave up and continued with the book. Do not let this deter you. If you are interested in Python development or learning it for pen-testing purposes, then this book should be on your bookshelf.

this book was awesome! Great intro into scapy and sockets

Interresting book. For me, a web developper and a layman user of security.

SHEET)(PYTHON FOR BEGINNERS, PYTHON FOR DUMMIES, PYTHON PROGRAMMING) PYTHON: LEARN PYTHON in A Day and MASTER IT WELL. The Only Essential Book You Need To Start Programming in Python Now. Hands On Challenges INCLUDED! (Programming for Beginners, Python) Python Programming: An In-Depth Guide Into The Essentials Of Python Programming (Included: 30+ Exercises To Master Python in No Time!) C++ and Python Programming: 2 Manuscript Bundle: Introductory Beginners Guide to Learn C++ Programming and Python Programming C++ and Python Programming 2 Bundle Manuscript. Introductory Beginners Guide to Learn C++ Programming and Python Programming Python Programming: The Complete Step By Step Guide to Master Python Programming and Start Coding Today! (Computer Programming Book 4) Python: Learn Python in a Day and Master It Well: The Only Essential Book You Need to Start Programming in Python Now Python: The Fundamentals Of Python Programming: A Complete Beginners Guide To Python Mastery. Data Analytics and Python Programming: 2 Bundle Manuscript: Beginners Guide to Learn Data Analytics, Predictive Analytics and Data Science with Python Programming Python Programming Advanced: A Complete Guide on Python Programming for Advanced Users Python Programming Guide + SQL Guide - Learn to be an EXPERT in a DAY!: Box Set Guide (Python Programming, SQL) Python Programming for Beginners: A Comprehensive Guide to Learning the Basics of Python Programming Oh, the Places on Earth! A Cat in the Hat's Learning Library Collection (Cat in the Hat Knows a Lot About That!: Cat in the Hat's Learning Library) C++: The Ultimate Crash Course to Learning the Basics of C++ (C programming, C++ in easy steps, C++ programming, Start coding today) (CSS,C Programming, ... Programming,PHP, Coding, Java Book 1) Maya Python for Games and Film: A Complete Reference for Maya Python and the Maya Python API