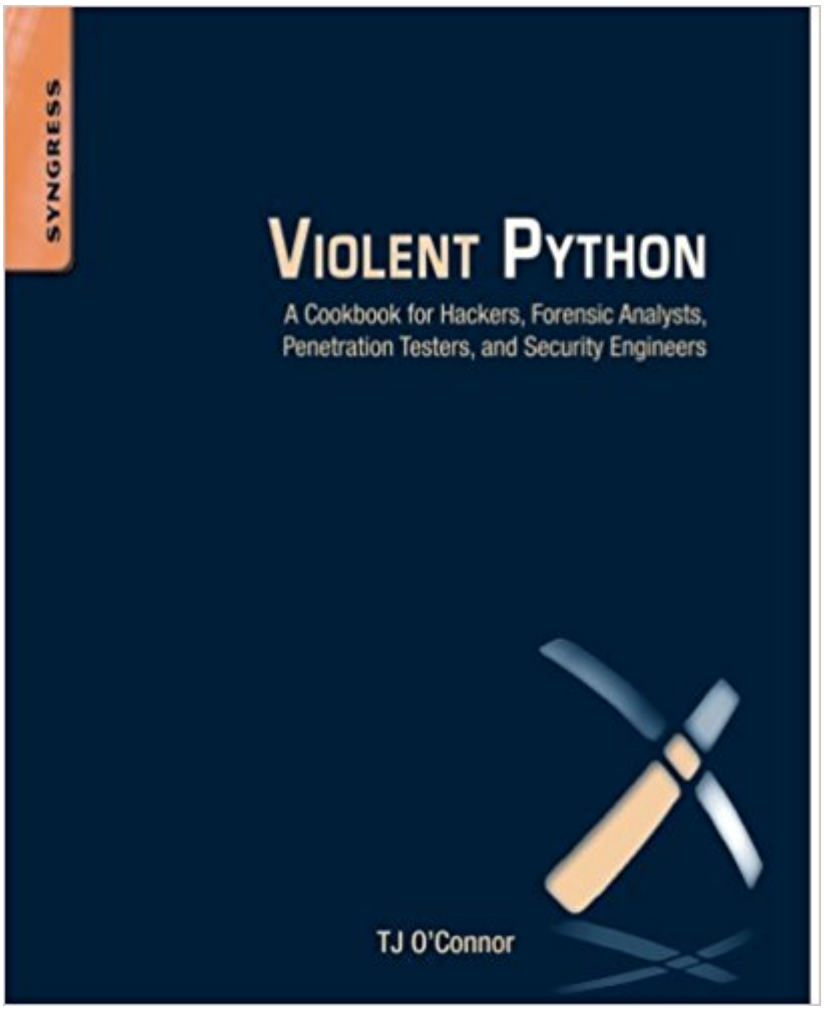
Violent Python: A Cookbook For Hackers, Forensic Analysts, Penetration Testers And Security Engineers



Synopsis

Violent Python shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attackerâ ™s tools, this book will teach you to forge your own weapons using the Python programming language. This book demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts. It also shows how to write code to intercept and analyze network traffic using Python, craft and spoof wireless frames to attack wireless and Bluetooth devices, and how to data-mine popular social media websites and evade modern anti-virus. Demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifactsWrite code to intercept and analyze network traffic using Python. Craft and spoof wireless frames to attack wireless and Bluetooth devicesData-mine popular social media websites and evade modern anti-virus

Book Information

Paperback: 288 pages

Publisher: Syngress; 1 edition (November 22, 2012)

Language: English

ISBN-10: 1597499579

ISBN-13: 978-1597499576

Product Dimensions: 7.5 x 0.6 x 9.2 inches

Shipping Weight: 14.4 ounces (View shipping rates and policies)

Average Customer Review: 4.3 out of 5 stars 95 customer reviews

Best Sellers Rank: #37,831 in Books (See Top 100 in Books) #31 inÂ Books > Computers & Technology > Internet & Social Media > Hacking #39 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security #56 inÂ Books > Textbooks > Computer Science > Networking

Customer Reviews

"An information security specialist with the US Army, O'Connor introduces the hacker's programming language Python to new users, and describes some advanced features to those who already know it." --Reference and Research Book News, August 2013 "A quick glance at [the authors] collective credentials and experience undoubtedly creates high expectations for this titleâ | The end result is that the book demonstrates how powerful just a few dozen lines of Python code can beâ | useful tips and tricks will surely be acquired simply by working through the exercises."

--The Ethical Hacker Network, February 2013 "Violent Python is an excellent resource that develops and enhances a diverse set of security-related Python skills. The book also serves as a great reference, where recipes could be quickly implemented to address specific issues as they arise. Readers who are actively working in an InfoSec position will likely be able to put their newly acquired skills to use immediately, and those looking to break into the field will acquire skills that differentiate themselves from others who are dependent on prebuilt tools. This title is highly recommended for anyone who wants to improve his or her Python skills within the InfoSec realm." --The Ethical Hacker Network, February 2013 "When it comes to Python and penetration testing, TJ O'Connor is the grand Python master. This is the book that keeps on giving. From building penetration testing Python scripts, to antivirus-evading penetration testing malware, to interrogating the Windows Registry and investigating other forensic artifacts...O'Connor masterfully walks the reader from basic to advanced penetration testing techniques with sample code throughout." --Ove Carroll, SANS Certified Instructor, Co-Author of SANS Forensics 408 - Windows In Depth "Violent Python is chalked full of practical examples and is for all security professionals. It covers the spectrum - knowledge for pen testers to forensic analysts, beginner to advanced and offensive to defensive tasks. If you are involved in information security and are looking for a Python book, this is an excellent source." --James Shewmaker, Security Analyst, Bluenotch Corporation "The best hackers know when to write their own tools. Violent Python is a very relevant collection of examples to seed your personal hacking toolbox. From offensive actions to digital forensics, this book has useful bits for everyone." --Raphael Mudge, Creator of Armitage

TJ Oâ ™Connor is a Department of Defense expert on information security and a US Army paratrooper. While assigned as an assistant professor at the US Military Academy, TJ taught undergraduate courses on forensics, exploitation and information assurance. He twice co-coached the winning team at the National Security Agencyâ ™s annual Cyber Defense Exercise and won the National Defense Universityâ ™s first annual Cyber Challenge. He has served on multiple red teams, including twice on the Northeast Regional Team for the National Collegiate Cyber Defense Competition.TJ holds a Master of Science degree in Computer Science from North Carolina State, a Master of Science degree in Information Security Engineering from the SANS Technical Institute, and a Bachelor of Science degree in Computer Science from the US Military Academy. He has published technical research at USENIX workshops, ACM conferences, security conferences, the SANS Reading Room, the Internet Storm Center, the Army Magazine, and the Armed Forces Journal. He holds expert cyber security credentials, including the prestigious GIAC Security Expert

(GSE) and Offensive Security Certified Expert (OSCE). TJ is a member of the elite SANS Red and Blue Team Cyber Guardians.TJ O'Connor is an active duty Army Major and former faculty member at the United States Military Academy, where he taught courses on forensics, exploitation, and information assurance. He has published research at USENIX workshops, ACM Conferences, and spoken at various security conferences, including ShmooCon. He has participated in numerous cyber defense exercises, including winning the National Defense University Cyber Challenge, coaching the winning team at the National Security Agency's Cyber Defense Exercise and working as a red team member of the Northeast Regional Collegiate Cyber Defense Competition. He has earned the SANS Certifications GIAC Gold certifications in GCFA, GCIH, GSEC, GCIA, and holds other GIAC certifications.

Really fun book to extend your python abilities why creating some handy tools.

Okay

Great book. A great cover to cover reading

I just got it recently and jumped right into Forensics Investigations with Python. Learning many great things, exited to be adding new skills and ideas into my craft. Thumbs up on this one.

As a cookbook, this has a lot of good ideas. I am looking for a good beginning-Python book, and this isn't that. But if you know a bit about programming, and a bit about Digital Forensics, this book will bring things together beautifully.Pros: engrossing, and functioning, examples. Range of ideas.Cons: Editing is kind of weak. The code examples don't translate well into digital-MOBI format --- unidentified wordwrapping and compression of leading whitespace are deadly flaws in a Python listing --- and there's the occasional not-quite-a-sentence. A couple of the links are also obsolete/dead.

This was a great introduction into using python as a security too. I would recommend it to anyone who wants to learn python to use in pen testing or web security testing.

Provides walkthrough-ish examples for using python to develop security and analysis tools. Good place to start for beginners with python.

This was an optional read for a Python class I attended to obtain my Masters Degree in digital forensics. At first I was skeptical of how useful it would be in class (it wasn't) but I was able to find a use for it in my day-to-day work as a digital forensic examiner. This would like useful because it provides (and explains) code for projects for creating a port scanner, SSH BotNets, as well as an extensive coverage on how TCPIP spoofing works. For the forensic analyst there are recipes for investigating iTunes backups, Sqlite databases, and application artifacts. Everything is brilliantly explained, real-world stories and several code examples are given enhance the readers knowledge. This is not a Python tutorial but a book on how to apply your Python knowledge in the security world. If you are a practitioner or security student then this is highly recommended.

No Time!) Python: The Fundamentals Of Python Programming: A Complete Beginners Guide To Python Mastery. Rapid Penetration into Granular Media: Visualizing the Fundamental Physics of Rapid Earth Penetration Hacking: Computer Hacking, Security Testing, Penetration Testing, and Basic Security Social Security & Medicare Facts 2016: Social Security Coverage, Maximization Strategies for Social Security Benefits, Medicare/Medicaid, Social Security Taxes, Retirement & Disability, Ser Easy Asian Cookbook Box Set: Easy Korean Cookbook, Easy Filipino Cookbook, Easy Thai Cookbook, Easy Indonesian Cookbook, Easy Vietnamese Cookbook (Korean ... Recipes, Asian Recipes, Asian Cookbook 1) Agile Testing: A Practical Guide for Testers and Agile Teams