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

Learning Penetration Testing with PythonPython for Data AnalysisPython 3 Object Oriented ProgrammingPython in a NutshellAttacking Network ProtocolsThe Browser Hacker's HandbookBlack Hat PythonBeginning Ethical Hacking with PythonViolent PythonMetasploitGray Hat PythonViolent PythonPython for Offensive PenTestHacking With PythonPython ProgrammingInside Cyber WarfarePython ForensicsPython ProgrammingPractical Reverse EngineeringLearning Python for ForensicsKingpinMastering Machine Learning with Python in Six StepsFoundations of Python Network ProgrammingFoundations for Analytics with PythonA Cognitive Theory of MagicPython CookbookPython Penetration Testing CookbookWeb Security Testing CookbookDesign for HackersThe Basics of Hacking and Penetration TestingInformation Assurance Handbook: Effective Computer Security and Risk Management StrategiesThe Car Hacker's HandbookHands-On Penetration Testing with PythonDying to KnowGoogle Hacking for Penetration TestersEffective PythonHands-On Penetration Testing with PythonViolent PythonMastering Python NetworkingPython Programming in Context

Learning Penetration Testing with Python

Discover the techniques behind beautiful design by deconstructing designs to understand them The term 'hacker' has been redefined to consist of anyone who has an insatiable curiosity as to how things work—and how they can try to make them better. This book is aimed at hackers of all skill levels and explains the classical principles and techniques behind beautiful designs by deconstructing those designs in order to understand what makes them so remarkable. Author and designer David Kadavy provides you with the framework for understanding good design and places a special emphasis on interactive mediums. You'll explore color theory, the role of proportion and geometry in design, and the relationship between medium and form. Packed with unique reverse engineering design examples, this book inspires and encourages you to discover and create new beauty in a variety of formats. Breaks down and studies the classical principles and techniques behind the creation of beautiful design Illustrates cultural and contextual considerations in communicating to a specific audience Discusses why design is important, the purpose of design, the various constraints of design, and how today's fonts are designed with the screen in mind Dissects the elements of color, size, scale, proportion, medium, and form Features a unique range of examples, including the graffiti in the ancient city of Pompeii, the lack of the color black in Monet's art, the style and sleekness of the iPhone, and more By the end of this book, you'll be able to apply the featured design principles to your own web designs, mobile apps, or other digital work.

Python for Data Analysis

Python Forensics provides many never-before-published proven forensic modules, libraries, and solutions that can be used right out of the box. In addition, detailed

instruction and documentation provided with the code samples will allow even novice Python programmers to add their own unique twists or use the models presented to build new solutions. Rapid development of new cybercrime investigation tools is an essential ingredient in virtually every case and environment. Whether you are performing post-mortem investigation, executing live triage, extracting evidence from mobile devices or cloud services, or you are collecting and processing evidence from a network, Python forensic implementations can fill in the gaps. Drawing upon years of practical experience and using numerous examples and illustrative code samples, author Chet Hosmer discusses how to: Develop new forensic solutions independent of large vendor software release schedules Participate in an open-source workbench that facilitates direct involvement in the design and implementation of new methods that augment or replace existing tools Advance your career by creating new solutions along with the construction of cutting-edge automation solutions to solve old problems Provides hands-on tools, code samples, and detailed instruction and documentation that can be put to use immediately Discusses how to create a Python forensics workbench Covers effective forensic searching and indexing using Python Shows how to use Python to examine mobile device operating systems: iOS, Android, and Windows 8 Presents complete coverage of how to use Python scripts for network investigation

Python 3 Object Oriented Programming

"The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, documentation is lacking and the tool can be hard to grasp for first-time users. Metasploit: A Penetration Tester's Guide fills this gap by teaching you how to harness the Framework, use its many features, and interact with the vibrant community of Metasploit contributors. The authors begin by building a foundation for penetration testing and establishing a fundamental methodology. From there, they explain the Framework's conventions, interfaces, and module system, as they show you how to assess networks with Metasploit by launching simulated attacks. Having mastered the essentials, you'll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, devastating wireless attacks, and targeted social engineering attacks. Metasploit: A Penetration Tester's Guide willteach you how to: Find and exploit unmaintained, misconfigured, and unpatched systems Perform reconnaissance and find valuable information about your target Bypass anti-virus technologies and circumvent security controls Integrate Nmap, NeXpose, and Nessus with Metasploit to automate discovery Use the Meterpreter shell to launch further attacks from inside the network Harness standalone Metasploit utilities, third-party tools, and plug-ins Learn how to write your own Meterpreter post exploitation modules and scripts You'll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework, and learn how to cover your tracks. Whether your goal is to make your own networks more secure or to put someone else's to the test, Metasploit: A Penetration Tester's Guide will take you there and beyond"--

Python in a Nutshell

Your one-stop guide to using Python, creating your own hacking tools, and making the most out of resources available for this programming language Key Features Comprehensive information on building a web application penetration testing framework using Python Master web application penetration testing using the multi-paradigm programming language Python Detect vulnerabilities in a system or application by writing your own Python scripts Book Description Python is an easy-to-learn and cross-platform programming language that has unlimited third-party libraries. Plenty of open source hacking tools are written in Python, which can be easily integrated within your script. This book is packed with step-by-step instructions and working examples to make you a skilled penetration tester. It is divided into clear bite-sized chunks, so you can learn at your own pace and focus on the areas of most interest to you. This book will teach you how to code a reverse shell and build an anonymous shell. You will also learn how to hack passwords and perform a privilege escalation on Windows with practical examples. You will set up your own virtual hacking environment in VirtualBox, which will help you run multiple operating systems for your testing environment. By the end of this book, you will have learned how to code your own scripts and mastered ethical hacking from scratch. What you will learn Code your own reverse shell (TCP and HTTP) Create your own anonymous shell by interacting with Twitter, Google Forms, and SourceForge Replicate Metasploit features and build an advanced shell Hack passwords using multiple techniques (API hooking, keyloggers, and clipboard hijacking) Exfiltrate data from your target Add encryption (AES, RSA, and XOR) to your shell to learn how cryptography is being abused by malware Discover privilege escalation on Windows with practical examples Countermeasures against most attacks Who this book is for This book is for ethical hackers; penetration testers; students preparing for OSCP, OSCE, GPEN, GXPN, and CEH; information security professionals; cybersecurity consultants; system and network security administrators; and programmers who are keen on learning all about penetration testing.

Attacking Network Protocols

Become an expert in implementing advanced, network-related tasks with Python. About This Book Build the skills to perform all networking tasks using Python with ease Use Python for network device automation, DevOps, and software-defined networking Get practical guidance to networking with Python Who This Book Is For If you are a network engineer or a programmer who wants to use Python for networking, then this book is for you. A basic familiarity with networking-related concepts such as TCP/IP and a familiarity with Python programming will be useful. What You Will Learn Review all the fundamentals of Python and the TCP/IP suite Use Python to execute commands when the device does not support the API or programmatic interaction with the device Implement automation techniques by integrating Python with Cisco, Juniper, and Arista eAPI Integrate Ansible using Python to control Cisco, Juniper, and Arista networks Achieve network security with Python Build Flask-based web-service APIs with Python Construct a Python-based migration plan from a legacy to scalable SDN-based network. In Detail This book begins with a review of the TCP/ IP protocol suite and a refresher of the core elements of the Python language. Next, you will start using Python and supported libraries to automate network tasks from the current major network vendors. We will look at automating traditional network devices based on the command-line

interface, as well as newer devices with API support, with hands-on labs. We will then learn the concepts and practical use cases of the Ansible framework in order to achieve your network goals. We will then move on to using Python for DevOps, starting with using open source tools to test, secure, and analyze your network. Then, we will focus on network monitoring and visualization. We will learn how to retrieve network information using a polling mechanism, ?ow-based monitoring, and visualizing the data programmatically. Next, we will learn how to use the Python framework to build your own customized network web services. In the last module, you will use Python for SDN, where you will use a Python-based controller with OpenFlow in a hands-on lab to learn its concepts and applications. We will compare and contrast OpenFlow, OpenStack, OpenDaylight, and NFV. Finally, you will use everything you've learned in the book to construct a migration plan to go from a legacy to a scalable SDN-based network. Style and approach An easy-to-follow guide packed with hands-on examples of using Python for network device automation, DevOps, and SDN.

The Browser Hacker's Handbook

Violent Python shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attacker'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 artifacts Write code to intercept and analyze network traffic using Python. Craft and spoof wireless frames to attack wireless and Bluetooth devices Data-mine popular social media websites and evade modern anti-virus

Black Hat Python

Attacking Network Protocols is a deep dive into network protocol security from James Forshaw, one of the world's leading bug hunters. This comprehensive guide looks at networking from an attacker's perspective to help you discover, exploit, and ultimately protect vulnerabilities. You'll start with a rundown of networking basics and protocol traffic capture before moving on to static and dynamic protocol analysis, common protocol structures, cryptography, and protocol security. Then you'll turn your focus to finding and exploiting vulnerabilities, with an overview of common bug classes, fuzzing, debugging, and exhaustion attacks. Learn how to: - Capture, manipulate, and replay packets - Develop tools to dissect traffic and reverse engineer code to understand the inner workings of a network protocol - Discover and exploit vulnerabilities such as memory corruptions, authentication bypasses, and denials of service - Use capture and analysis tools like Wireshark and develop your own custom network proxies to manipulate network traffic Attacking Network Protocols is a must-have for any penetration tester, bug hunter, or developer looking to understand and discover network vulnerabilities.

Beginning Ethical Hacking with Python

In Black Hat Python, the latest from Justin Seitz (author of the best-selling Gray Hat Python), you'll explore the darker side of Python's capabilities—writing network sniffers, manipulating packets, infecting virtual machines, creating stealthy trojans, and more. You'll learn how to: Create a trojan command-and-control using GitHubDetect sandboxing and automate common malware tasks, like keylogging and screenshottingEscalate Windows privileges with creative process controlUse offensive memory forensics tricks to retrieve password hashes and inject shellcode into a virtual machineExtend the popular Burp Suite web-hacking toolAbuse Windows COM automation to perform a man-in-the-browser attackExfiltrate data from a network most sneakily Insider 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.

Violent Python

If you're like many of Excel's 750 million users, you want to do more with your data—like repeating similar analyses over hundreds of files, or combining data in many files for analysis at one time. This practical guide shows ambitious non-programmers how to automate and scale the processing and analysis of data in different formats—by using Python. After author Clinton Brownley takes you through Python basics, you'll be able to write simple scripts for processing data in spreadsheets as well as databases. You'll also learn how to use several Python modules for parsing files, grouping data, and producing statistics. No programming experience is necessary. Create and run your own Python scripts by learning basic syntax Use Python's csv module to read and parse CSV files Read multiple Excel worksheets and workbooks with the xlrd module Perform database operations in MySQL or with the mysqlclient module Create Python applications to find specific records, group data, and parse text files Build statistical graphs and plots with matplotlib, pandas, ggplot, and seaborn Produce summary statistics, and estimate regression and classification models Schedule your scripts to run automatically in both Windows and Mac environments

Metasploit

Gray Hat Python

Dying is overrated. Murder is not. Detective Oliver Tucker prefers to be the guy investigating shootings, not the guy getting shot. So when he returns as a ghost after being murdered in his home, it's only natural for Tuck to investigate the most important case of his life—his own. Detective, solve thyself! Piecing together cold cases, foggy memories, and eerie premonitions, Tuck fears that if he doesn't figure out who pulled the trigger, his wife may be the next victim. Surprised to discover many earth-bound spirits chasing the same killer, Tuck's unique perspective from the other side leads him to a chilling conclusion—it's the living, not the dead, who are most terrifying. Praise: "TJ O'Connor has a smash hit with his debut novel

Dying to Know . . . I couldn't stop reading."—Stephen Frey, New York Times bestselling author

Violent Python

* Covers low-level networking in Python —essential for writing a new networked application protocol. * Many working examples demonstrate concepts in action -- and can be used as starting points for new projects. * Networked application security is demystified. * Exhibits and explains multitasking network servers using several models, including forking, threading, and non-blocking sockets. * Features extensive coverage of Web and E-mail. Describes Python's database APIs.

Python for Offensive PenTest

This book helps people find sensitive information on the Web. Google is one of the 5 most popular sites on the internet with more than 380 million unique users per month (Nielsen/NetRatings 8/05). But, Google's search capabilities are so powerful, they sometimes discover content that no one ever intended to be publicly available on the Web including: social security numbers, credit card numbers, trade secrets, and federally classified documents. Google Hacking for Penetration Testers Volume 2 shows the art of manipulating Google used by security professionals and system administrators to find this sensitive information and "self-police their own organizations. Readers will learn how Google Maps and Google Earth provide pinpoint military accuracy, see how bad guys can manipulate Google to create super worms, and see how they can "mash up" Google with MySpace, LinkedIn, and more for passive reconaissance. • Learn Google Searching Basics Explore Google's Web-based Interface, build Google queries, and work with Google URLs. • Use Advanced Operators to Perform Advanced Queries Combine advanced operators and learn about colliding operators and bad search-fu. • Learn the Ways of the Google Hacker See how to use caches for anonymity and review directory listings and traversal techniques. • Review Document Grinding and Database Digging See the ways to use Google to locate documents and then search within the documents to locate information. • Understand Google's Part in an Information Collection Framework Learn the principles of automating searches and the applications of data mining. • Locate Exploits and Finding Targets Locate exploit code and then vulnerable targets. • See Ten Simple Security Searches Learn a few searches that give good results just about every time and are good for a security assessment. • Track Down Web Servers Locate and profile web servers, login portals, network hardware and utilities. • See How Bad Guys Troll for Data Find ways to search for usernames, passwords, credit card numbers, social security numbers, and other juicy information. • Hack Google Services Learn more about the AJAX Search API, Calendar, Blogger, Blog Search, and more.

Hacking With Python

Learn the art of designing, developing, and deploying innovative forensic solutions through Python About This Book This practical guide will help you solve forensic dilemmas through the development of Python scripts Analyze Python scripts to extract metadata and investigate forensic artifacts Master the skills of parsing

complex data structures by taking advantage of Python libraries Who This Book Is For If you are a forensics student, hobbyist, or professional that is seeking to increase your understanding in forensics through the use of a programming language, then this book is for you. You are not required to have previous experience in programming to learn and master the content within this book. This material, created by forensic professionals, was written with a unique perspective and understanding of examiners who wish to learn programming What You Will Learn Discover how to perform Python script development Update yourself by learning the best practices in forensic programming Build scripts through an iterative design Explore the rapid development of specialized scripts Understand how to leverage forensic libraries developed by the community Design flexibly to accommodate present and future hurdles Conduct effective and efficient investigations through programmatic pre-analysis Discover how to transform raw data into customized reports and visualizations In Detail This book will illustrate how and why you should learn Python to strengthen your analysis skills and efficiency as you creatively solve real-world problems through instruction-based tutorials. The tutorials use an interactive design, giving you experience of the development process so you gain a better understanding of what it means to be a forensic developer. Each chapter walks you through a forensic artifact and one or more methods to analyze the evidence. It also provides reasons why one method may be advantageous over another. We cover common digital forensics and incident response scenarios, with scripts that can be used to tackle case work in the field. Using built-in and community-sourced libraries, you will improve your problem solving skills with the addition of the Python scripting language. In addition, we provide resources for further exploration of each script so you can understand what further purposes Python can serve. With this knowledge, you can rapidly develop and deploy solutions to identify critical information and fine-tune your skill set as an examiner. Style and approach The book begins by instructing you on the basics of Python, followed by chapters that include scripts targeted for forensic casework. Each script is described step by step at an introductory level, providing gradual growth to demonstrate the available functionalities of Python.

Python Programming

"It's easy to start writing code with Python: that's why the language is so immensely popular. However, Python has unique strengths, charms, and expressivity that can be hard to grasp at first -- as well as hidden pitfalls that can easily trip you up if you aren't aware of them. Effective Python will help you harness the full power of Python to write exceptionally robust, efficient, maintainable, and well-performing code. Utilizing the concise, scenario-driven style pioneered in Scott Meyers's best-selling Effective C++, Brett Slatkin brings together 53 Python best practices, tips, shortcuts, and realistic code examples from expert programmers. Through realistic examples, Slatkin uncovers little-known Python quirks, intricacies, and idioms that powerfully impact code behavior and performance. You'll learn how to choose the most efficient and effective way to accomplish key tasks when multiple options exist, and how to write code that's easier to understand, maintain, and improve. Drawing on his deep understanding of Python's capabilities, Slatkin offers practical advice for each major area of development with both Python 3.x and Python 2.x. Coverage includes: * Algorithms * Objects * Concurrency * Collaboration * Built-in modules * Production techniques

* And more Each section contains specific, actionable guidelines organized into items, each with carefully worded advice supported by detailed technical arguments and illuminating examples. Using Effective Python, you can systematically improve all the Python code you write: not by blindly following rules or mimicking incomprehensible idioms, but by gaining a deep understanding of the technical reasons why they make sense."--[Source inconnue].

Inside Cyber Warfare

Implement defensive techniques in your ecosystem successfully with Python Key Features Identify and expose vulnerabilities in your infrastructure with Python Learn custom exploit development . Make robust and powerful cybersecurity tools with Python Book Description With the current technological and infrastructural shift, penetration testing is no longer a process-oriented activity. Modern-day penetration testing demands lots of automation and innovation; the only language that dominates all its peers is Python. Given the huge number of tools written in Python, and its popularity in the penetration testing space, this language has always been the first choice for penetration testers. Hands-On Penetration Testing with Python walks you through advanced Python programming constructs. Once you are familiar with the core concepts, you'll explore the advanced uses of Python in the domain of penetration testing and optimization. You'll then move on to understanding how Python, data science, and the cybersecurity ecosystem communicate with one another. In the concluding chapters, you'll study exploit development, reverse engineering, and cybersecurity use cases that can be automated with Python. By the end of this book, you'll have acquired adequate skills to leverage Python as a helpful tool to pentest and secure infrastructure, while also creating your own custom exploits. What you will learn Get to grips with Custom vulnerability scanner development Familiarize yourself with web application scanning automation and exploit development Walk through day-to-day cybersecurity scenarios that can be automated with Python Discover enterprise-or organization-specific use cases and threat-hunting automation Understand reverse engineering, fuzzing, buffer overflows , key-logger development, and exploit development for buffer overflows. Understand web scraping in Python and use it for processing web responses Explore Security Operations Centre (SOC) use cases Get to understand Data Science, Python, and cybersecurity all under one hood Who this book is for If you are a security consultant , developer or a cyber security enthusiast with little or no knowledge of Python and want in-depth insight into how the pen-testing ecosystem and python combine to create offensive tools , exploits , automate cyber security use-cases and much more then this book is for you. Hands-On Penetration Testing with Python guides you through the advanced uses of Python for cybersecurity and pen-testing, helping you to better understand security loopholes within your infrastructure .

Python Forensics

What people are saying about Inside Cyber Warfare "The necessary handbook for the 21st century." --Lewis Shepherd, Chief Tech Officer and Senior Fellow, Microsoft Institute for Advanced Technology in Governments "A must-read for policy makers and leaders who need to understand the big-picture landscape of cyber war." --Jim Stogdill, CTO, Mission Services Accenture You may have heard

about "cyber warfare" in the news, but do you really know what it is? This book provides fascinating and disturbing details on how nations, groups, and individuals throughout the world are using the Internet as an attack platform to gain military, political, and economic advantages over their adversaries. You'll learn how sophisticated hackers working on behalf of states or organized crime patiently play a high-stakes game that could target anyone, regardless of affiliation or nationality. Inside Cyber Warfare goes beyond the headlines of attention-grabbing DDoS attacks and takes a deep look inside multiple cyber-conflicts that occurred from 2002 through summer 2009. Learn how cyber attacks are waged in open conflicts, including recent hostilities between Russia and Georgia, and Israel and Palestine Discover why Twitter, Facebook, LiveJournal, Vkontakte, and other sites on the social web are mined by the intelligence services of many nations Read about China's commitment to penetrate the networks of its technologically superior adversaries as a matter of national survival Find out why many attacks originate from servers in the United States, and who's responsible Learn how hackers are "weaponizing" malware to attack vulnerabilities at the application level

Python Programming

Analyzing how hacks are done, so as to stop them in thefuture Reverse engineering is the process of analyzing hardware orsoftware and understanding it, without having access to the sourcecode or design documents. Hackers are able to reverse engineersystems and exploit what they find with scary results. Now the goodguys can use the same tools to thwart these threats. PracticalReverse Engineering goes under the hood of reverse engineeringfor security analysts, security engineers, and system programmers,so they can learn how to use these same processes to stop hackersin their tracks. The book covers x86, x64, and ARM (the first book to cover allthree); Windows kernel-mode code rootkits and drivers; virtualmachine protection techniques; and much more. Best of all, itoffers a systematic approach to the material, with plenty ofhands-on exercises and real-world examples. Offers a systematic approach to understanding reverseengineering, with hands-on exercises and real-world examples Covers x86, x64, and advanced RISC machine (ARM) architecturesas well as deobfuscation and virtual machine protectiontechniques Provides special coverage of Windows kernel-mode code(rootkits/drivers), a topic not often covered elsewhere, andexplains how to analyze drivers step by step Demystifies topics that have a steep learning curve Includes a bonus chapter on reverse engineering tools Practical Reverse Engineering: Using x86, x64, ARM, WindowsKernel, and Reversing Tools provides crucial, up-to-dateguidance for a broad range of IT professionals.

Practical Reverse Engineering

Utilize Python scripting to execute effective and efficient penetration tests About This Book Understand how and where Python scripts meet the need for penetration testing Familiarise yourself with the process of highlighting a specific methodology to exploit an environment to fetch critical data Develop your Python and penetration testing skills with real-world examples Who This Book Is For If you are a security professional or researcher, with knowledge of different operating systems and a conceptual idea of penetration testing, and you would like to grow your knowledge in Python, then this book is ideal for you. What You Will Learn

Familiarise yourself with the generation of Metasploit resource files Use the Metasploit Remote Procedure Call (MSFRPC) to automate exploit generation and execution Use Python's Scapy, network, socket, office, Nmap libraries, and custom modules Parse Microsoft Office spreadsheets and eXtensible Markup Language (XML) data files Write buffer overflows and reverse Metasploit modules to expand capabilities Exploit Remote File Inclusion (RFI) to gain administrative access to systems with Python and other scripting languages Crack an organization's Internet perimeter Chain exploits to gain deeper access to an organization's resources Interact with web services with Python In Detail Python is a powerful new-age scripting platform that allows you to build exploits, evaluate services, automate, and link solutions with ease. Python is a multi-paradigm programming language well suited to both object-oriented application development as well as functional design patterns. Because of the power and flexibility offered by it, Python has become one of the most popular languages used for penetration testing. This book highlights how you can evaluate an organization methodically and realistically. Specific tradecraft and techniques are covered that show you exactly when and where industry tools can and should be used and when Python fits a need that proprietary and open source solutions do not. Initial methodology, and Python fundamentals are established and then built on. Specific examples are created with vulnerable system images, which are available to the community to test scripts, techniques, and exploits. This book walks you through real-world penetration testing challenges and how Python can help. From start to finish, the book takes you through how to create Python scripts that meet relative needs that can be adapted to particular situations. As chapters progress, the script examples explain new concepts to enhance your foundational knowledge, culminating with you being able to build multi-threaded security tools, link security tools together, automate reports, create custom exploits, and expand Metasploit modules. Style and approach This book is a practical guide that will help you become better penetration testers and/or Python security tool developers. Each chapter builds on concepts and tradecraft using detailed examples in test environments that you can simulate.

Learning Python for Forensics

Harness the power of Python 3 objects.

Kingpin

Python is fast becoming the programming language of choice for hackers, reverse engineers, and software testers because it's easy to write quickly, and it has the low-level support and libraries that make hackers happy. But until now, there has been no real manual on how to use Python for a variety of hacking tasks. You had to dig through forum posts and man pages, endlessly tweaking your own code to get everything working. Not anymore. Gray Hat Python explains the concepts behind hacking tools and techniques like debuggers, trojans, fuzzers, and emulators. But author Justin Seitz goes beyond theory, showing you how to harness existing Python-based security tools—and how to build your own when the pre-built ones won't cut it. You'll learn how to: –Automate tedious reversing and security tasks –Design and program your own debugger –Learn how to fuzz Windows drivers and create powerful fuzzers from scratch –Have fun with code and

library injection, soft and hard hooking techniques, and other software trickery –Sniff secure traffic out of an encrypted web browser session –Use PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU, and more The world's best hackers are using Python to do their handiwork. Shouldn't you?

Mastering Machine Learning with Python in Six Steps

Demonstrates the programming language's strength as a Web development tool, covering syntax, data types, built-ins, the Python standard module library, and real world examples.

Foundations of Python Network Programming

Modern cars are more computerized than ever. Infotainment and navigation systems, Wi-Fi, automatic software updates, and other innovations aim to make driving more convenient. But vehicle technologies haven't kept pace with today's more hostile security environment, leaving millions vulnerable to attack. The Car Hacker's Handbook will give you a deeper understanding of the computer systems and embedded software in modern vehicles. It begins by examining vulnerabilities and providing detailed explanations of communications over the CAN bus and between devices and systems. Then, once you have an understanding of a vehicle's communication network, you'll learn how to intercept data and perform specific hacks to track vehicles, unlock doors, glitch engines, flood communication, and more. With a focus on low-cost, open source hacking tools such as Metasploit, Wireshark, Kayak, can-utils, and ChipWhisperer, The Car Hacker's Handbook will show you how to: –Build an accurate threat model for your vehicle –Reverse engineer the CAN bus to fake engine signals –Exploit vulnerabilities in diagnostic and data-logging systems –Hack the ECU and other firmware and embedded systems –Feed exploits through infotainment and vehicle-to-vehicle communication systems –Override factory settings with performance-tuning techniques –Build physical and virtual test benches to try out exploits safely If you're curious about automotive security and have the urge to hack a two-ton computer, make The Car Hacker's Handbook your first stop.

Foundations for Analytics with Python

Explore fundamental to advanced Python 3 topics in six steps, all designed to make you a worthy practitioner. This updated version's approach is based on the "six degrees of separation" theory, which states that everyone and everything is a maximum of six steps away and presents each topic in two parts: theoretical concepts and practical implementation using suitable Python 3 packages. You'll start with the fundamentals of Python 3 programming language, machine learning history, evolution, and the system development frameworks. Key data mining/analysis concepts, such as exploratory analysis, feature dimension reduction, regressions, time series forecasting and their efficient implementation in Scikit-learn are covered as well. You'll also learn commonly used model diagnostic and tuning techniques. These include optimal probability cutoff point for class creation, variance, bias, bagging, boosting, ensemble voting, grid search, random search, Bayesian optimization, and the noise reduction technique for IoT data.

Finally, you'll review advanced text mining techniques, recommender systems, neural networks, deep learning, reinforcement learning techniques and their implementation. All the code presented in the book will be available in the form of iPython notebooks to enable you to try out these examples and extend them to your advantage. What You'll Learn Understand machine learning development and frameworks Assess model diagnosis and tuning in machine learning Examine text mining, natuarl language processing (NLP), and recommender systems Review reinforcement learning and CNN Who This Book Is For Python developers, data engineers, and machine learning engineers looking to expand their knowledge or career into machine learning area.

A Cognitive Theory of Magic

Best practices for protecting critical data and systems Information Assurance Handbook: Effective Computer Security and Risk Management Strategies discusses the tools and techniques required to prevent, detect, contain, correct, and recover from security breaches and other information assurance failures. This practical resource explains how to integrate information assurance into your enterprise planning in a non-technical manner. It leads you through building an IT strategy and offers an organizational approach to identifying, implementing, and controlling information assurance initiatives for small businesses and global enterprises alike. Common threats and vulnerabilities are described and applicable controls based on risk profiles are provided. Practical information assurance application examples are presented for select industries, including healthcare, retail, and industrial control systems. Chapter-ending critical thinking exercises reinforce the material covered. An extensive list of scholarly works and international government standards is also provided in this detailed guide. Comprehensive coverage includes: Basic information assurance principles and concepts Information assurance management system Current practices, regulations, and plans Impact of organizational structure Asset management Risk management and mitigation Human resource assurance Advantages of certification, accreditation, and assurance Information assurance in system development and acquisition Physical and environmental security controls Information assurance awareness, training, and education Access control Information security monitoring tools and methods Information assurance measurements and metrics Incident handling and computer forensics Business continuity management Backup and restoration Cloud computing and outsourcing strategies Information assurance big data concerns

Python Cookbook

The author presents a new theory of magical actions based on a wide array of recent findings in the cognitive sciences. Analysing classical ethnographic cases, he argues that paying close attention to the underlying cognitive processes will not only explain why magical rituals look the way they do, it will also supply new insights into the role of magic in the formation of institutionalised religion.

Python Penetration Testing Cookbook

Implement defensive techniques in your ecosystem successfully with Python Key

Features Identify and expose vulnerabilities in your infrastructure with Python Learn custom exploit development . Make robust and powerful cybersecurity tools with Python Book Description With the current technological and infrastructural shift, penetration testing is no longer a process-oriented activity. Modern-day penetration testing demands lots of automation and innovation; the only language that dominates all its peers is Python. Given the huge number of tools written in Python, and its popularity in the penetration testing space, this language has always been the first choice for penetration testers. Hands-On Penetration Testing with Python walks you through advanced Python programming constructs. Once you are familiar with the core concepts, you'll explore the advanced uses of Python in the domain of penetration testing and optimization. You'll then move on to understanding how Python, data science, and the cybersecurity ecosystem communicate with one another. In the concluding chapters, you'll study exploit development, reverse engineering, and cybersecurity use cases that can be automated with Python. By the end of this book, you'll have acquired adequate skills to leverage Python as a helpful tool to pentest and secure infrastructure, while also creating your own custom exploits. What you will learn Get to grips with Custom vulnerability scanner development Familiarize yourself with web application scanning automation and exploit development Walk through day-to-day cybersecurity scenarios that can be automated with Python Discover enterprise-or organization-specific use cases and threat-hunting automation Understand reverse engineering, fuzzing, buffer overflows , key-logger development, and exploit development for buffer overflows. Understand web scraping in Python and use it for processing web responses Explore Security Operations Centre (SOC) use cases Get to understand Data Science, Python, and cybersecurity all under one hood Who this book is for If you are a security consultant , developer or a cyber security enthusiast with little or no knowledge of Python and want in-depth insight into how the pen-testing ecosystem and python combine to create offensive tools , exploits , automate cyber security use-cases and much more then this book is for you. Hands-On Penetration Testing with Python guides you through the advanced uses of Python for cybersecurity and pen-testing, helping you to better understand security loopholes within your infrastructure .

Web Security Testing Cookbook

This book is suitable for use in a university-level first course in computing (CS1), as well as the increasingly popular course known as CS0. It is difficult for many students to master basic concepts in computer science and programming. A large portion of the confusion can be blamed on the complexity of the tools and materials that are traditionally used to teach CS1 and CS2. This textbook was written with a single overarching goal: to present the core concepts of computer science as simply as possible without being simplistic.

Design for Hackers

The user-friendly, object-oriented programming language Python is quickly becoming the most popular introductory programming language for both students and instructors. This updated Second Edition of Python Programming in Context provides a comprehensive, accessible introduction to Python fundamentals. An ideal first language for learners entering the rapidly expanding field of computer

science, Python gives students a solid platform of key problem-solving skills that translate easily across programming languages. Building on essential concepts of computer science, and offering a plenitude of real-world examples, Python Programming in Context, Second Edition offers a thorough overview of multiple applied areas, including image processing, cryptography, astronomy, the Internet, and bioinformatics. The text's emphasis on problem-solving, extrapolation, and development of independent exploration and solution-building provides students with a unique and innovative approach to learning programming. Python Programming in Context, Second Edition is the ideal introductory text for those delving into computer programming. Key Features - Utilizes Python 3 - Provides a clear, accessible, and skill-focused approach to programming with Python - Contains problem sets based on real-world examples and problem-solving rather than language features - Offers a variety of exercises that develop independent skill-building and exploration - Every new copy of the text is packaged with full student access to Turing's Craft Custom CodeLab. Customized to match the organization of the text, CodeLab offers students hands-on Python programming experience with immediate feedback. - Accompanied by a full suite of instructor support material, including solutions to the exercises in the text, downloadable source code, PowerPoint Lecture Outlines, and a complete Test Bank.

The Basics of Hacking and Penetration Testing

Violent Python shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attacker'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 artifacts Write code to intercept and analyze network traffic using Python. Craft and spoof wireless frames to attack wireless and Bluetooth devices Data-mine popular social media websites and evade modern anti-virus

Information Assurance Handbook: Effective Computer Security and Risk Management Strategies

Over 50+ hands-on recipes to help you pen test networks using Python, discover vulnerabilities, and find a recovery path About This Book Learn to detect and avoid various types of attack that put system privacy at risk Enhance your knowledge of wireless application concepts and information gathering through practical recipes Learn a pragmatic way to penetration-test using Python, build efficient code, and save time Who This Book Is For If you are a developer with prior knowledge of using Python for penetration testing and if you want an overview of scripting tasks to consider while penetration testing, this book will give you a lot of useful code for your toolkit. What You Will Learn Learn to configure Python in different environment setups. Find an IP address from a web page using BeautifulSoup and

Scrapy Discover different types of packet sniffing script to sniff network packets Master layer-2 and TCP/ IP attacks Master techniques for exploit development for Windows and Linux Incorporate various network- and packet-sniffing techniques using Raw sockets and Scrapy In Detail Penetration testing is the use of tools and code to attack a system in order to assess its vulnerabilities to external threats. Python allows pen testers to create their own tools. Since Python is a highly valued pen-testing language, there are many native libraries and Python bindings available specifically for pen-testing tasks. Python Penetration Testing Cookbook begins by teaching you how to extract information from web pages. You will learn how to build an intrusion detection system using network sniffing techniques. Next, you will find out how to scan your networks to ensure performance and quality, and how to carry out wireless pen testing on your network to avoid cyber attacks. After that, we'll discuss the different kinds of network attack. Next, you'll get to grips with designing your own torrent detection program. We'll take you through common vulnerability scenarios and then cover buffer overflow exploitation so you can detect insecure coding. Finally, you'll master PE code injection methods to safeguard your network. Style and approach This book takes a recipe-based approach to solving real-world problems in pen testing. It is structured in stages from the initial assessment of a system through exploitation to post-exploitation tests, and provides scripts that can be used or modified for in-depth penetration testing.

The Car Hacker's Handbook

If you need help writing programs in Python 3, or want to update older Python 2 code, this book is just the ticket. Packed with practical recipes written and tested with Python 3.3, this unique cookbook is for experienced Python programmers who want to focus on modern tools and idioms. Inside, you'll find complete recipes for more than a dozen topics, covering the core Python language as well as tasks common to a wide variety of application domains. Each recipe contains code samples you can use in your projects right away, along with a discussion about how and why the solution works. Topics include: Data Structures and Algorithms Strings and Text Numbers, Dates, and Times Iterators and Generators Files and I/O Data Encoding and Processing Functions Classes and Objects Metaprogramming Modules and Packages Network and Web Programming Concurrency Utility Scripting and System Administration Testing, Debugging, and Exceptions C Extensions

Hands-On Penetration Testing with Python

Python Programming Complete Crash Course Python Programming For Beginners, Python Programming For Intertmediates, Python Programming For Advanced This Python Programming Bundle includes all 3 books Python Programming For Beginners Python Programming For Intermediates Python Programming For Advanced

Dying to Know

The Basics of Hacking and Penetration Testing, Second Edition, serves as an

introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. The book teaches students how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. It provides a simple and clean explanation of how to effectively utilize these tools, along with a four-step methodology for conducting a penetration test or hack, thus equipping students with the know-how required to jump start their careers and gain a better understanding of offensive security. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and utilize those results in later phases. Tool coverage includes: Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. This is complemented by PowerPoint slides for use in class. This book is an ideal resource for security consultants, beginning InfoSec professionals, and students. Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. Written by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. Utilizes the Kali Linux distribution and focuses on the seminal tools required to complete a penetration test.

Google Hacking for Penetration Testers

Hackers exploit browser vulnerabilities to attack deep withinnetworks The Browser Hacker's Handbook gives a practicalunderstanding of hacking the everyday web browser and using it as abeachhead to launch further attacks deep into corporate networks.Written by a team of highly experienced computer security experts,the handbook provides hands-on tutorials exploring a range ofcurrent attack methods. The web browser has become the most popular and widely usedcomputer "program" in the world. As the gateway to the Internet, itis part of the storefront to any business that operates online, butit is also one of the most vulnerable entry points of any system.With attacks on the rise, companies are increasingly employingbrowser-hardening techniques to protect the unique vulnerabilitiesinherent in all currently used browsers. The Browser Hacker'sHandbook thoroughly covers complex security issues and exploresrelevant topics such as: Bypassing the Same Origin Policy ARP spoofing, social engineering, and phishing to accessbrowsers DNS tunneling, attacking web applications, andproxying—all from the browser Exploiting the browser and its ecosystem (plugins andextensions) Cross-origin attacks, including Inter-protocol Communicationand Exploitation The Browser Hacker's Handbook is written with aprofessional security engagement in mind. Leveraging browsers aspivot points into a target's network should form an integralcomponent into any social engineering or red-team securityassessment. This handbook provides a complete methodology tounderstand and structure your next browser penetration test.

Effective Python

Offering developers an inexpensive way to include testing as part of the development cycle, this cookbook features scores of recipes for testing Web applications, from relatively simple solutions to complex ones that combine several solutions.

Hands-On Penetration Testing with Python

Get complete instructions for manipulating, processing, cleaning, and crunching datasets in Python. Updated for Python 3.6, the second edition of this hands-on guide is packed with practical case studies that show you how to solve a broad set of data analysis problems effectively. You'll learn the latest versions of pandas, NumPy, IPython, and Jupyter in the process. Written by Wes McKinney, the creator of the Python pandas project, this book is a practical, modern introduction to data science tools in Python. It's ideal for analysts new to Python and for Python programmers new to data science and scientific computing. Data files and related material are available on GitHub. Use the IPython shell and Jupyter notebook for exploratory computing Learn basic and advanced features in NumPy (Numerical Python) Get started with data analysis tools in the pandas library Use flexible tools to load, clean, transform, merge, and reshape data Create informative visualizations with matplotlib Apply the pandas groupby facility to slice, dice, and summarize datasets Analyze and manipulate regular and irregular time series data Learn how to solve real-world data analysis problems with thorough, detailed examples

Violent Python

Documents how a troubled young computer hacker seized control of a massive international computer fraud network in 2006, tracing the efforts of FBI and Secret Service agents as well as an undercover operator to locate and arrest him. Reprint.

Mastering Python Networking

Hacking with Python: The Ultimate Beginners Guide This book will show you how to use Python, create your own hacking tools, and make the most out of available resources that are made using this programming language. If you do not have experience in programming, don't worry - this book will show guide you through understanding the basic concepts of programming and navigating Python codes. This book will also serve as your guide in understanding common hacking methodologies and in learning how different hackers use them for exploiting vulnerabilities or improving security. You will also be able to create your own hacking scripts using Python, use modules and libraries that are available from third-party sources, and learn how to tweak existing hacking scripts to address your own computing needs. Order your copy now!

Python Programming in Context

Learn the basics of ethical hacking and gain insights into the logic, algorithms, and syntax of Python. This book will set you up with a foundation that will help you understand the advanced concepts of hacking in the future. Learn Ethical Hacking with Python 3 touches the core issues of cyber security: in the modern world of interconnected computers and the Internet, security is increasingly becoming one of the most important features of programming. Ethical hacking is closely related to Python. For this reason this book is organized in three parts. The first part deals with the basics of ethical hacking; the second part deals with Python 3; and the

third part deals with more advanced features of ethical hacking. What You Will Learn Discover the legal constraints of ethical hacking Work with virtual machines and virtualization Develop skills in Python 3 See the importance of networking in ethical hacking Gain knowledge of the dark web, hidden Wikipedia, proxy chains, virtual private networks, MAC addresses, and more Who This Book Is For Beginners wanting to learn ethical hacking alongside a modular object oriented programming language.

ROMANCE ACTION & ADVENTURE MYSTERY & THRILLER BIOGRAPHIES & HISTORY CHILDREN'S YOUNG ADULT FANTASY HISTORICAL FICTION HORROR LITERARY FICTION NON-FICTION SCIENCE FICTION