Pwntools

Mastering MetasploitReverse Engineering Code with IDA ProInformation SecurityBlack Hat GoPython One-LinersBut how Do it Know?□□□□□□□□□□□□□□□□□□□The Web Application Hacker's Handbook□□□□□□□□□□□□The Hitchhiker's Guide to PythonThe Art of Debugging with GDB, DDD, and EclipseViolent PythonPractical Binary AnalysisDive Into PythonSlackermediaAnsible for DevOpsCracking Codes with PythonThe IoT Hacker's HandbookDeep Learning with PyTorchShell Programming in Unix, Linux and OS XPoC or GTFOThe IDA Pro Book, 2nd EditionSQL Injection Attacks and DefenseComposing SoftwarePenetration TestingSoftware Similarity and ClassificationYahtzee Score BookProgramming from the Ground Up□□pwnable □□□□□□□□□□□□□□□□□□Penetration Testing with ShellcodeSecurity Power ToolsCoffee Break Python WorkbookPractices of the Python Pro21st Century CComplete Guide to Modern JavaScriptThink Data Structures□□□ □□#6(Square CTF RR)Information Security ApplicationsData Structures and Algorithms in PythonThe Shellcoder's Handbook

Mastering Metasploit

□□□□□□□□□□□□□□□CTF□□□□□□□□pwnable□□□□□□□pwnable□□CTF□□□□□□□□□□□□□□□□□□□□pwnable□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Docker□□ □□□□ □1□ □□ □2□ login1□□□□□□□□□□□□□□□□1□ □3□ login2□□□□□□□□□□□□□□□□2□ □4□

login3□□□□□□□□□□□□□□□□□□3□ □5□ rot13□□□□□□□□□□ □6□ birdcage□□□□□□□□□□□□□□□□□□□□ □7□ strstr□double free□□□□□□□□ □8□ strstrstr□□□□□□□□□□□□□□□□□□ □9□ freefree□House of Orange□ □10□ freefree++□file stream oriented programming□ □11□ writefree□House of Corrosion□ □12□ shellsort□□□□□□□□□

Reverse Engineering Code with IDA Pro

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 Security

A comprehensive and detailed, step by step tutorial guide that takes you through important aspects of the Metasploit framework. If you are a penetration tester, security engineer, or someone who is looking to extend their penetration testing skills with Metasploit, then this book is ideal for you. The readers ofthis book must have a basic knowledge of using Metasploit. They are also expected to have knowledge of exploitation and an indepth understanding of object-oriented programming languages.

Black Hat Go

Shell Programming in Unix, Linux and OS X is a thoroughly updated revision of Kochan and Wood's classic Unix Shell Programming tutorial. Following the methodology of the original text, the book focuses on the POSIX standard shell, and teaches you how to develop programs in this useful programming environment, taking full advantage of the underlying power of Unix and Unix-like operating systems. After a quick review of Unix utilities, the book's authors take you step-by-step through the process of building shell scripts, debugging them, and understanding how they work within the shell's environment. All major features of the shell are covered, and the large number of practical examples make it easy for you to build shell scripts for your particular applications. The book also describes the major features of the Korn and Bash shells. Learn how to… Take advantage of the many utilities provided in the Unix system Write powerful shell scripts Use the shell's built-in decision-making and looping constructs Use the shell's powerful quoting mechanisms Make the most of the shell’s built-in history and command editing capabilities Use regular expressions with Unix commands Take advantage of the special features of the Korn and Bash shells Identify the major differences between versions of the shell language Customize the way your Unix system responds to you Set up your shell environment Make use of functions Debug scripts Contents at a Glance 1 A Quick Review of the Basics 2 What Is the Shell? 3 Tools of the Trade 4 And Away We Go 5 Can I Quote You on That? 6 Passing Arguments 7 Decisions, Decisions 8 ‘Round and ‘Round She Goes 9 Reading and Printing Data 10 Your Environment 11 More on Parameters 12 Loose Ends 13 Rolo Revisited 14 Interactive and Nonstandard Shell Features A Shell Summary B For More Information

Python One-Liners

What if you could sit down with some of the most talented security engineers in the world and ask any network security question you wanted? Security Power Tools lets you do exactly that! Members of Juniper Networks' Security Engineering team and a few guest experts reveal how to use, tweak, and push the most popular network security applications, utilities, and tools available using Windows, Linux, Mac OS X, and Unix platforms. Designed to be browsed, Security Power Tools offers you multiple approaches to network security via 23 cross-referenced chapters that review the best security tools on the planet for both black hat techniques and white hat defense tactics. It's a must-have reference for network administrators, engineers and consultants with tips, tricks, and how-to advice for an assortment of freeware and commercial tools, ranging from intermediate level command-line operations to advanced programming of self-hiding exploits. Security Power Tools details best practices for: Reconnaissance -- including tools for network scanning such as nmap; vulnerability scanning tools for Windows and Linux; LAN reconnaissance; tools to help with wireless reconnaissance; and custom packet generation Penetration -- such as the Metasploit framework for automated penetration of remote computers; tools to find wireless networks; exploitation framework applications; and tricks and tools to manipulate shellcodes Control -- including the configuration of several tools for use as backdoors; and a review of known rootkits for Windows and Linux Defense -- including host-based firewalls; host hardening for Windows and Linux networks; communication security with ssh; email security and anti-malware; and device security testing Monitoring -- such as tools to capture, and analyze packets; network monitoring with Honeyd and snort; and host monitoring of production servers for file changes Discovery -- including The Forensic Toolkit, SysInternals and other popular forensic tools; application fuzzer and fuzzing techniques; and the art of binary reverse engineering using tools like Interactive Disassembler and Ollydbg A practical and timely network security ethics chapter written by a Stanford University professor of law completes the suite of topics and makes this book a goldmine of security information. Save yourself a ton of headaches and be prepared for any network security dilemma with Security Power Tools.

But how Do it Know?

Like the best-selling Black Hat Python, Black Hat Go explores the darker side of the popular Go programming language. This collection of short scripts will help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset. Black Hat Go explores the darker side of Go, the popular programming language revered by hackers for its simplicity, efficiency, and reliability. It provides an arsenal of practical tactics from the perspective of security practitioners and hackers to help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset, all using the power of Go. You'll begin your journey with a basic overview of Go's syntax and philosophy and then start to explore examples that you can leverage for tool development, including common network protocols like HTTP, DNS, and SMB. You'll then dig into various tactics and problems that penetration testers encounter, addressing things like data pilfering, packet sniffing, and exploit development. You'll create dynamic, pluggable tools before diving into cryptography, attacking Microsoft Windows, and implementing steganography. You'll learn how to: • Make performant tools that can be used for your own security projects • Create usable tools that interact with remote APIs • Scrape arbitrary HTML data • Use Go's standard package, net/http, for building HTTP servers • Write your own DNS server and proxy • Use DNS tunneling to establish a C2 channel out of a restrictive network • Create a vulnerability fuzzer to discover an application's security weaknesses • Use plug-ins and extensions to future-proof productsBuild an RC2 symmetric-key brute-forcer • Implant data within a Portable Network Graphics (PNG) image. Are you ready to add to your arsenal of security tools? Then let's Go!

□□□□□□□□□□□□□□□□□□□

This book is a practical guide to discovering and exploiting security flaws in web applications. The authors explain each category of vulnerability using real-world examples, screen shots and code extracts. The book is extremely practical in focus, and describes in detail the steps involved in detecting and exploiting each kind of security weakness found within a variety of applications such as online banking, e-commerce and other web applications. The topics covered include bypassing login mechanisms, injecting code, exploiting logic flaws and compromising other users. Because every web application is different, attacking them entails bringing to bear various general principles, techniques and experience in an imaginative way. The most successful hackers go beyond this, and find ways to automate their bespoke attacks. This handbook describes a proven methodology that combines the virtues of human intelligence and computerized brute force, often with devastating results. The authors are professional penetration testers who have been involved in web application security for nearly a decade. They have presented training courses at the Black Hat security conferences throughout the world. Under the alias "PortSwigger", Dafydd developed the popular Burp Suite of web application hack tools.

The Web Application Hacker's Handbook

Ansible is a simple, but powerful, server and configuration management tool. Learn to use Ansible effectively, whether you manage one server--or thousands.

□□□□□□□□□□□□□

□□ □□1□2□□□ □□ □□ □□□□ □□□□ 0□ □□□□□□ 0-1 □□□□□□□□□□□□□0-2 Windows□□□□□□□□ □□ 1□ □□□□□□□□□□□□□□ 1-1 □□□□□□□□□□1-2 □□□□□ □□ 2□ □□□□□□□□□□□□□□□□□□□ 2-1 □□□□□2-2 CPU□□□□ □□ 3□ ASCII□□□□□□□□□□ 3-1 □□□□□□□□16□□□3-2 ASCII□□□ □□ 4□ □□□□□□ 4-1 □□□□□□□□□□□4-2 □□□□ □□ 5□ □□□□□□□ 5-1 □□□□□□□□□5-2 □□□□□□gdb-peda □□□□□□□□□□□ □□

6□ □□□□□□□□□ 6-1 □□□□□□□□□□□□□6-2 □□□□□□□□□□ □□ 7□ gdb-peda□□□□□□□□□□□□ 7-1 4□□□□□7-2 □□□□□□gdb-peda□□□□□□□□□□ □□ 8□ □□□□□□□□□□□□□ 8-1 □□□□□□□□8-2 □□□□□□□□□ □□ 9□ Return to libc 9-1 sh□□□□□system□□□9-2 □□□□□□□□□ □□ 10□ □□□□□□□□□ 10-1 □□□□□□□10-2 □□□□□□□□□□□□ □□ 11□ □□□□□□□□□□□□□□□□□□□ 11-1 Stack Smash Protection - canary□□□□□□□□□□11-2 □□□□ - Executable Space Protection□NX Bit □□

The Hitchhiker's Guide to Python

This book thoroughly explains how computers work. It starts by fully examining a NAND gate, then goes on to build every piece and part of a small, fully operational computer. The necessity and use of codes is presented in parallel with the apprioriate pieces of hardware. The book can be easily understood by anyone whether they have a technical background or not. It could be used as a textbook.

The Art of Debugging with GDB, DDD, and Eclipse

Learn how to build your own multimedia workstation, and how to use it! Slackermedia is a multimedia guidebook for people looking to get away from operating systems that tell them what they can or can't do in their art. But it doesn't stop there! In this volume, you'll find detailed guides on the most important multimedia applications on Linux today: the Kdenlive video editor and the Qtractor digital audio workstation. You'll also get tips and resources on other great multimedia applications of Linux, like Blender, Audacity, Jamin, CALF, LADSPA, GIMP, Inkscape, ffmpeg, sox, Qsynth, fluidsynth, soundfonts, Xsynth, whySynth, QJack Control, Font Matrix, and many many more. By the end of your journey with Slackermedia, you'll know everything you need to know to create original multimedia content and any kind of digital art on the powerful, free operating system of GNU Linux. So put your nerd glasses on, roll up your sleeves, and prepare yourself for creativity like you've never experienced.

Violent Python

This highly anticipated print collection gathers articles published in the much-loved International Journal of Proof-of-Concept or Get The Fuck Out. PoC||GTFO follows in the tradition of Phrack and Uninformed by publishing on the subjects of offensive security research, reverse engineering, and file format internals. Until now, the journal has only been available online or printed and distributed for free at hacker conferences worldwide. Consistent with the journal's quirky, biblical style, this book comes with all the trimmings: a leatherette cover, ribbon bookmark, bible paper, and gilt-edged pages. The book features more than 80 technical essays from numerous famous hackers, authors of classics like "Reliable Code Execution on a Tamagotchi," "ELFs are Dorky, Elves are Cool," "Burning a Phone," "Forget Not the Humble Timing Attack," and "A Sermon on Hacker Privilege." Twenty-four full-color pages by Ange Albertini illustrate many of the clever tricks described in the text.

Practical Binary Analysis

Whether you are a complete beginner or you have some knowledge in JavaScript, this book will guide you from the basics of the language to all the new features introduced until 2020. At the end of each chapter test your knowledge with quizzes. After reading this book, Let Const, generators, promises, and async won't be a problem anymore. If you want to experience something new, this book also includes an introduction to the basics of TypeScript, a must-know for any JavaScript develop in 2020.

Dive Into Python

□□□□ SquareCTF(2017)□ □□ □□□ □□□□ □□□□□. □□□□ □□□ □□ □□□□ □□□□ □□□□□. * Square: □□□□ □□□. □□□ CEO□ □□□□ □□. - □□□□ □□□ □□□ □□□ □□□□ □□ □□□□□ □□□ □□(□□□)□□□. - □□ □□□□ □□□□ □□ □□□□ □□□□□ □□□□□. - □□□□ □□□□ □□□□ □□□□ □□□□□. - □□□ □□ □□□ □□□ □□ □□□ □□□□ □□□□□. - □□ □□□ □□□□ □ □ □ □ □□□□□. - □□□ □□□□ □□ □□ □□□ □□□□ □□□ □□□ □□ □□□ □□□□□. * □□□ □□□ □□□ □□□□ □□□□ □□□□ □□ □□ □□□□ □□□□□.

Slackermedia

Programming from the Ground Up uses Linux assembly language to teach new programmers the most important concepts in programming. It takes you a step at a time through these concepts: * How the processor views memory * How the processor operates * How programs interact with the operating system * How computers represent data internally * How to do low-level and high-level optimization Most beginning-level programming books attempt to shield the reader from how their computer really works. Programming from the Ground Up starts by teaching how the computer works under the hood, so that the programmer will have a sufficient background to be successful in all areas of programming. This book is being used by Princeton University in their COS 217 "Introduction to Programming Systems" course.

Ansible for DevOps

[illegible]CTF[illegible]
CTF[illegible]Capture The Flag[illegible]
[illegible] [illegible]
[illegible]
[illegible]
[illegible]Web[illegible]
[illegible]
[illegible]CTF[illegible]
CTF[illegible]
[illegible]
※2015/12/28[illegible]
[illegible]

Cracking Codes with Python

Debugging is crucial to successful software development, but even many experienced programmers find it challenging. Sophisticated debugging tools are available, yet it may be difficult to determine which features are useful in which situations. The Art of Debugging is your guide to making the debugging process more efficient and effective. The Art of Debugging illustrates the use three of the most popular debugging tools on Linux/Unix platforms: GDB, DDD, and Eclipse. The text-command based GDB (the GNU Project Debugger) is included with most distributions. DDD is a popular GUI front end for GDB, while Eclipse provides a complete integrated development environment. In addition to offering specific advice for debugging with each tool, authors Norm Matloff and Pete Salzman cover general strategies for improving the process of finding and fixing coding errors, including how to: –Inspect variables and data structures –Understand segmentation faults and core dumps –Know why your program crashes or throws exceptions –Use features like catchpoints, convenience variables, and artificial arrays –Avoid common debugging pitfalls Real world examples of coding errors help to clarify the authors' guiding principles, and coverage of complex topics like thread, client-server, GUI, and parallel programming debugging will make you even more proficient. You'll also learn how to prevent errors in the first place with text editors, compilers, error reporting, and static code checkers. Whether you dread the thought of debugging your programs or simply want to improve your current debugging efforts, you'll find a valuable ally in The Art of Debugging.

The IoT Hacker's Handbook

Cracking Secret Codes with Python is a hands-on introduction to Python that teaches readers how to make and hack cipher programs, which are used to encrypt secret messages. It covers ciphers like the Caesar cipher, transposition cipher, and the RSA cipher, and teaches readers how to test and hack them. For every program, Sweigart provides the full source code and then walks readers through it, explaining how every line works. Along the way, readers will learn Python fundamentals - and by the book's end, they'll have a solid foundation in Python and some fun programs under their belt.

Deep Learning with PyTorch

"The IDA Pro Book" provides a comprehensive, top-down overview of IDA Pro and its use for reverse engineering software. This edition has been updated to cover the new features and cross-platform interface of IDA Pro 6.0.

Shell Programming in Unix, Linux and OS X

If you’re a student studying computer science or a software developer preparing for technical interviews, this practical book will help you learn and review some of the most important ideas in software engineering—data structures and algorithms—in a way that’s clearer, more concise, and more engaging than other materials. By emphasizing practical knowledge and skills over theory, author Allen Downey shows you how to use data structures to implement efficient algorithms, and then analyze and measure their performance. You’ll explore the important classes in the Java collections framework (JCF), how they’re implemented, and how they’re expected to perform. Each chapter presents hands-on exercises supported by test code online. Use data structures such as lists and maps, and understand how they work Build an application that reads Wikipedia pages, parses the contents, and navigates the resulting data tree Analyze code to predict how fast it will run and how much memory it will require Write classes that implement the Map interface, using a hash table and binary search tree Build a simple web search engine with a crawler, an indexer that stores web page contents, and a retriever that returns user query results Other books by Allen Downey include Think Java, Think Python, Think Stats, and Think Bayes.

PoC or GTFO

Practical Binary Analysis is the first book of its kind to present advanced binary analysis topics in an accessible way. After an introduction on the basics of binary formats, disassembly, and code injection, you'll dive into more complex topics such as binary instrumentation, dynamic taint analysis, and symbolic execution. By the end of the book, you'll be able to build your own binary analysis tools on Linux by following hands-on and practical examples.

The IDA Pro Book, 2nd Edition

* Quick start to learning python—very example oriented approach * Book has its own Web site established by the author: http://diveintopython.org/ Author is well known in the Open Source community and the book has a unique quick approach to learning an object oriented language.

SQL Injection Attacks and Defense

Your expert guide to information security As businesses and consumers become more dependent on complexmultinational information systems, the need to understand anddevise sound information security systems has never been greater.This title takes a practical approach to information security byfocusing on real-world examples. While not sidestepping the theory,the emphasis is on developing the skills and knowledge thatsecurity and information technology students and professionals needto face their challenges. The book is organized around four majorthemes: * Cryptography: classic cryptosystems, symmetric key cryptography,public key cryptography, hash functions, random numbers,information hiding, and cryptanalysis * Access control: authentication and authorization, password-basedsecurity, ACLs and capabilities, multilevel and multilateralsecurity, covert channels and inference control, BLP and Biba'smodels, firewalls, and intrusion detection systems * Protocols: simple authentication protocols, session keys, perfectforward secrecy, timestamps, SSL, IPSec, Kerberos, and GSM * Software: flaws and malware, buffer overflows, viruses and worms,software reverse engineering, digital rights management, securesoftware development, and operating systems security Additional features include numerous figures and tables toillustrate and clarify complex topics, as well as problems-rangingfrom basic to challenging-to help readers apply their newlydeveloped skills. A solutions manual and a set of classroom-testedPowerPoint(r) slides will assist instructors in their coursedevelopment. Students and professors in information technology,computer science, and engineering, and professionals working in thefield will find this reference most useful to solve theirinformation security issues. An Instructor's Manual presenting detailed solutions to all theproblems in the book is available from the Wiley editorialdepartment. An Instructor Support FTP site is also available.

Composing Software

What is SQL injection? -- Testing for SQL injection -- Reviewing code for SQL injection -- Exploiting SQL injection -- Blind SQL injection exploitation -- Exploiting the operating system -- Advanced topics -- Code-level defenses -- Platform level defenses -- Confirming and recovering from SQL injection attacks -- References.

Penetration Testing

If you want to master the art and science of reverse engineering code with IDA Pro for security R&D or software debugging, this is the book for you. Highly organized and sophisticated criminal entities are constantly developing more complex, obfuscated, and armored viruses, worms, Trojans, and botnets. IDA Pro's interactive interface and programmable development language provide you with complete control over code disassembly and debugging. This is the only book which focuses exclusively on the world's most powerful and popular took for reverse engineering code. *Reverse Engineer REAL Hostile Code To follow along with this chapter, you must download a file called !DANGER!INFECTEDMALWARE!DANGER! 'nuff said. *Portable Executable (PE) and Executable and Linking Formats (ELF) Understand the physical layout of PE and ELF files, and analyze the components that are essential to reverse engineering. *Break Hostile Code Armor and Write your own Exploits Understand execution flow, trace functions, recover hard coded passwords, find vulnerable functions, backtrace execution, and craft a buffer overflow. *Master Debugging Debug in IDA Pro, use a debugger while reverse engineering, perform heap and stack access modification, and use other debuggers. *Stop Anti-Reversing Anti-reversing, like reverse engineering or coding in assembly, is an art form. The trick of course is to try to stop the person reversing the application. Find out how! *Track a Protocol through a Binary and Recover its Message Structure Trace execution flow from a read event, determine the structure of a protocol, determine if the protocol has any undocumented messages, and use IDA Pro to determine the functions that process a particular message. *Develop IDA Scripts and Plug-ins Learn the basics of IDA scripting and syntax, and write IDC scripts and plug-ins to automate even the most complex tasks.

Software Similarity and Classification

Python programmers will improve their computer science skills with these useful one-liners. Python One-Liners will teach you how to read and write "one-liners": concise statements of useful functionality packed into a single line of code. You'll learn how to systematically unpack and understand any line of Python code, and write eloquent, powerfully compressed Python like an expert. The book's five chapters cover tips and tricks, regular expressions, machine learning, core data science topics, and useful algorithms. Detailed explanations of one-liners introduce key computer science concepts and boost your coding and analytical skills. You'll learn about advanced Python features such as list comprehension, slicing, lambda functions, regular expressions, map and reduce functions, and slice assignments. You'll also learn how to: • Leverage data structures to solve real-world problems, like using Boolean indexing to find cities with above-average pollution • Use NumPy basics such as array, shape, axis, type, broadcasting, advanced indexing, slicing, sorting, searching, aggregating, and statistics • Calculate basic statistics of multidimensional data arrays and the K-Means algorithms for unsupervised learning • Create more advanced regular expressions using grouping and named groups, negative lookaheads, escaped characters, whitespaces, character sets (and negative characters sets), and greedy/nongreedy operators •

Understand a wide range of computer science topics, including anagrams, palindromes, supersets, permutations, factorials, prime numbers, Fibonacci numbers, obfuscation, searching, and algorithmic sorting By the end of the book, you'll know how to write Python at its most refined, and create concise, beautiful pieces of "Python art" in merely a single line.

Yahtzee Score Book

Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine–based lab that includes Kali Linux and vulnerable operating systems, you’ll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you’ll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: * Crack passwords and wireless network keys with brute-forcing and wordlists * Test web applications for vulnerabilities * Use the Metasploit Framework to launch exploits and write your own Metasploit modules * Automate social-engineering attacks * Bypass antivirus software * Turn access to one machine into total control of the enterprise in the post exploitation phase You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.

Programming from the Ground Up

Summary Professional developers know the many benefits of writing application code that's clean, well-organized, and easy to maintain. By learning and following established patterns and best practices, you can take your code and your career to a new level. With Practices of the Python Pro, you'll learn to design professional-level, clean, easily maintainable software at scale using the incredibly popular programming language, Python. You'll find easy-to-grok examples that use pseudocode and Python to introduce software development best practices, along with dozens of instantly useful techniques that will help you code like a pro. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Professional-quality code does more than just run without bugs. It's clean, readable, and easy to maintain. To step up from a capable Python coder to a professional developer, you need to learn industry standards for coding style, application design, and development process. That's where this book is indispensable. About the book Practices of the Python Pro teaches you to design and write professional-quality software that’s understandable, maintainable, and extensible. Dane Hillard is a Python pro who has helped many dozens of developers make this step, and he knows what it takes. With helpful examples and exercises, he teaches you when, why, and how to modularize your code, how to improve quality by reducing complexity, and much more. Embrace these core principles, and your code will become easier for you and others to read, maintain, and reuse. What's inside Organizing large Python projects Achieving the right levels of abstraction Writing clean, reusable code Inheritance and composition Considerations for testing and performance About the reader For readers familiar with the basics of Python, or another OO language. About the author Dane Hillard has spent the majority of his development career using Python to build web applications. Table of Contents: PART 1 WHY IT ALL MATTERS 1 ¦ The bigger picture PART 2 FOUNDATIONS OF DESIGN 2 ¦ Separation of concerns 3 ¦ Abstraction and encapsulation 4 ¦ Designing for high performance 5 ¦ Testing your software PART 3 NAILING DOWN LARGE SYSTEMS 6 ¦ Separation of concerns in practice 7 ¦ Extensibility and flexibility 8 ¦ The rules (and exceptions) of inheritance 9 ¦ Keeping things lightweight 10 ¦ Achieving loose coupling PART 4 WHAT’S NEXT? 11 ¦ Onward and upward

□□pwnable □□□□□□□□□□□□□□□□□□

The Hitchhiker's Guide to Python takes the journeyman Pythonista to true expertise. More than any other language, Python was created with the philosophy of simplicity and parsimony. Now 25 years old, Python has become the primary or secondary language (after SQL) for many business users. With popularity comes diversity—and possibly dilution. This guide, collaboratively written by over a hundred members of the Python community, describes best practices currently used by package and application developers. Unlike other books for this audience, The Hitchhiker's Guide is light on reusable code and heavier on design philosophy, directing the reader to excellent sources that already exist.

Penetration Testing with Shellcode

Every other day we hear about new ways to put deep learning to good use: improved medical imaging, accurate credit card fraud detection, long range weather forecasting, and more. PyTorch puts these superpowers in your hands, providing a comfortable Python experience that gets you started quickly and then grows with you as you—and your deep learning skills—become more sophisticated. Deep Learning with PyTorch will make that journey engaging and fun. Summary Every other day we hear about new ways to put deep learning to good use: improved medical imaging, accurate credit card fraud detection, long range weather forecasting, and more. PyTorch puts these superpowers in your hands, providing a comfortable Python experience that gets you started quickly and then grows with you as you—and your deep learning skills—become more sophisticated. Deep Learning with PyTorch will make that journey engaging and fun. Foreword by Soumith Chintala, Cocreator of PyTorch. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Although many deep learning tools use Python, the PyTorch library is truly Pythonic. Instantly familiar to anyone who knows PyData tools like NumPy and scikit-learn, PyTorch simplifies deep learning without sacrificing advanced features. It’s excellent for building quick models, and it scales smoothly from laptop to enterprise. Because companies like Apple, Facebook, and JPMorgan Chase rely on PyTorch, it’s a great skill to have as you expand your career options. It’s easy to get started with PyTorch. It minimizes cognitive overhead without sacrificing the access to advanced features, meaning you can focus on what matters the most - building and training the latest and greatest deep learning models and contribute to making a dent in the world. PyTorch is also a snap to scale and extend, and it partners well with other Python tooling. PyTorch has been adopted by hundreds of deep learning practitioners and several first-class players like FAIR, OpenAI, FastAI and Purdue. About the book Deep Learning with PyTorch teaches you to create neural networks and deep learning systems with PyTorch. This practical book quickly gets you to work building a real-world example from scratch: a tumor image classifier. Along the way, it covers best practices for the entire DL pipeline, including the PyTorch Tensor API, loading data in Python, monitoring training, and visualizing results. After covering the basics, the book will take you on a journey through larger projects. The centerpiece of the book is a neural network designed for cancer detection. You'll discover ways for training networks with limited inputs and start processing data to get some results. You'll sift through the unreliable initial results and focus on how to diagnose and fix the problems in your neural network. Finally, you'll look at ways to improve your results by training with augmented data, make improvements to the model architecture, and perform other fine tuning. What's inside Training deep neural networks Implementing modules and loss functions Utilizing pretrained models from PyTorch Hub Exploring code samples in Jupyter Notebooks About the reader For Python programmers with an interest in machine learning. About the author Eli Stevens had roles from software engineer to CTO, and is currently working on machine learning in the self-driving-car industry. Luca Antiga is cofounder of an AI engineering company and an AI tech startup, as well as a former PyTorch contributor. Thomas Viehmann is a PyTorch core developer and machine learning trainer and consultant. consultant based in Munich, Germany and a PyTorch core developer. Table of Contents PART 1 - CORE PYTORCH 1 Introducing deep learning and the PyTorch Library 2 Pretrained networks 3 It starts with a tensor 4 Real-world data representation using tensors 5 The mechanics of learning 6 Using a neural network to fit the data 7 Telling birds from airplanes: Learning from images 8 Using convolutions to generalize PART 2 - LEARNING FROM IMAGES IN THE REAL WORLD: EARLY DETECTION OF LUNG CANCER 9 Using PyTorch to fight cancer 10 Combining data sources into a unified dataset 11 Training a classification model to detect suspected tumors 12 Improving training with metrics and augmentation 13 Using segmentation to find suspected nodules 14 End-to-end nodule analysis, and where to go next PART 3 - DEPLOYMENT 15 Deploying to production

Security Power Tools

Throw out your old ideas of C, and relearn a programming language that’s substantially outgrown its origins. With 21st Century C, you’ll discover up-to-date techniques that are absent from every other C text available. C isn’t just the foundation of modern programming languages, it is a modern language, ideal for writing efficient, state-of-the-art applications. Learn to dump old habits that made sense on mainframes, and pick up the tools you need to use this evolved and aggressively simple language. No matter what programming language you currently champion, you’ll agree that C rocks. Set up a C programming environment with shell facilities, makefiles, text editors, debuggers, and memory checkers Use Autotools, C’s de facto cross-platform package manager Learn which older C concepts should be downplayed or deprecated Explore problematic C concepts that are too useful to throw out Solve C’s string-building problems with C-standard and POSIX-standard functions Use modern syntactic features for functions that take structured inputs Build high-level object-based libraries and programs Apply existing C libraries for doing advanced math, talking to Internet servers, and running databases

Coffee Break Python Workbook

This much-anticipated revision, written by the ultimate group of top security experts in the world, features 40 percent new content on how to find security holes in any operating system or application New material addresses the many new exploitation techniques that have been discovered since the first edition, including attacking "unbreakable" software packages such as McAfee's Entercept, Mac OS X, XP, Office 2003, and Vista Also features the first-ever published information on exploiting Cisco's IOS, with content that has never before been explored The companion Web site features downloadable code files

Practices of the Python Pro

Take a practioner’s approach in analyzing the Internet of Things (IoT) devices and the security issues facing an IoT architecture. You’ll review the architecture's central components, from hardware communication interfaces, such as UARTand SPI, to radio protocols, such as BLE or ZigBee. You'll also learn to assess a device physically by opening it, looking at the PCB, and identifying the chipsets and interfaces. You'll then use that information to gain entry to the device or to perform other actions, such as dumping encryption keys and firmware. As the IoT rises to one of the most popular tech trends, manufactures need to take necessary steps to secure devices and protect them from attackers. The IoT Hacker's Handbook breaks down the Internet of Things, exploits it, and reveals how these devices can be built securely. What You’ll Learn Perform a threat model of a real-world IoT device and locate all possible attacker entry points Use reverse engineering of firmware binaries to identify security issues Analyze,assess, and identify security issues in exploited ARM and MIPS based binaries Sniff, capture, and exploit radio communication protocols, such as Bluetooth Low Energy (BLE), and ZigBee Who This Book is For Those interested in learning about IoT security, such as pentesters working in different domains, embedded device developers, or IT people wanting to move to an Internet of Things security role.

21st Century C

This book is the chess grandmaster way of learning Python. It offers you 127 unique and brand-new Python puzzles. Every puzzle points to gaps in your knowledge, challenges you to guess a solution, and then explains potential solutions, in an easy-to-understand manner: ~~~ # Here's one example puzzle: my_list = [1, 1, 1, 1] my_list[1::2] = [2, 3] print(my_list) # What's the output of this code snippet? ~~~ An easy, fun, and effective way of learning Python -- day after day -- in your COFFEE BREAK PYTHON! Here's what research says about puzzle-based learning: "Students who were quizzed after studying a short text could recall significantly more information than students who were asked to reread it" -- Karpicke, 2007, Elsevier Journal of Memory and Language Practice testing is scientifically proven to generate up to 44% better learning retention and efficiency. Simply put: quizzes and puzzles work! More than 100,000 Finxters and thousands of "Coffee Break Python" book customers have already successfully improved their skills with code puzzles. Learning does not happen in a linear and orderly manner. It's a probabilistic, chaotic, and iterative process of creating knowledge gaps in your brain -- and filling them with just the right information you need. That's the premise of the "Coffee Break Python" textbook series. What will you get out of the book? Improve your level of deep Python code understanding. Surprise your peers with your newly acquired code speed reading skills. Enjoy the small daily doses of intellectual challenges. A Finxter once called it "Sudoku for coders"! ;) Improve your brain's working memory by hammering down the most important concepts. Learn all the basic Python syntax elements. Discover your own skill level by tracking your puzzle-solving performance. Compare your skill level against other coders: are you a grandmaster of code? Enjoy the fun of rushing over Python -- from "hello world" to "recursive Quicksort". Get the best of all Finxter Python cheat sheets to revive 80% of the Python features in 20% of the time. Get your dream job and rock future code interviews! And take one step forward mastering the most popular programming language ON THE PLANET!

Complete Guide to Modern JavaScript

Think Data Structures

Software similarity and classification is an emerging topic with wide applications. It is applicable to the areas of malware detection, software theft detection, plagiarism detection, and software clone detection. Extracting program features, processing those features into suitable representations, and constructing distance metrics to define similarity and dissimilarity are the key methods to identify software variants, clones, derivatives, and classes of software. Software Similarity and Classification reviews the literature of those core concepts, in addition to relevant literature in each application and demonstrates that considering these applied problems as a similarity and classification problem enables techniques to be shared between areas. Additionally, the authors present in-depth case studies using the software similarity and classification techniques developed throughout the book.

□□□ □□#6(Square CTF RR)

All software design is composition: the act of breaking complex problems down into smaller problems and composing those solutions. Most developers have a limited understanding of compositional techniques. It's time for that to change.In "Composing Software", Eric Elliott shares the fundamentals of composition, including both function composition and object composition, and explores them in the context of JavaScript. The book covers the foundations of both functional programming and object oriented programming to help the reader better understand how to build and structure complex applications using simple building blocks.You'll learn: Functional programmingObject compositionHow to work with composite data structuresClosuresHigher order functionsFunctors (e.g., array.map)Monads (e.g., promises)TransducersLensesAll of this in the context of JavaScript, the most used programming language in the world. But the learning doesn't stop at JavaScript. You'll be able to apply these lessons to any language. This book is about the timeless principles of software composition and its lessons will outlast the hot languages and frameworks of today. Unlike most programming books, this one may still be relevant 20 years from now.This book began life as a popular blog post series that attracted hundreds of thousands of readers and influenced the way software is built at many high growth tech startups and fortune 500 companies

Information Security Applications

Master Shellcode to leverage the buffer overflow concept Key Features Understand how systems can be bypassed both at the operating system and network level with shellcode, assembly, and Metasploit Learn to write and modify 64-bit shellcode along with kernel-level shellcode concepts A step-by-step guide that will take you from low-level security skills to covering loops with shellcode Book Description Security is always a major concern for your application, your system, or your environment. This book’s main goal is to build up your skills for low-level security exploits, enabling you to find vulnerabilities and cover loopholes with shellcode, assembly, and Metasploit. This book covers topics ranging from memory management and assembly to compiling and extracting shellcode and using syscalls and dynamically locating functions in memory. This book also covers how to compile 64-bit shellcode for

Linux and Windows along with Metasploit shellcode tools. Lastly, this book will also show you to how to write your own exploits with intermediate techniques, using real-world scenarios. By the end of this book, you will have become an expert in shellcode and will understand how systems are compromised both at the operating system and at the network level. What you will learn Create an isolated lab to test and inject Shellcodes (Windows and Linux) Understand both Windows and Linux behavior in overflow attacks Learn the assembly programming language Create Shellcode using assembly and Metasploit Detect buffer overflows Debug and reverse-engineer using tools such as gdb, edb, and immunity (Windows and Linux) Exploit development and Shellcode injections (Windows and Linux) Prevent and protect against buffer overflows and heap corruption Who this book is for This book is intended to be read by penetration testers, malware analysts, security researchers, forensic practitioners, exploit developers, C language programmers, software testers, and students in the security field. Readers should have a basic understanding of OS internals (Windows and Linux). Some knowledge of the C programming language is essential, and a familiarity with the Python language would be helpful.

Data Structures and Algorithms in Python

Keep score for you favorite Yahtzee game. Included in Your Yahtzee Score Book Yahtzee Score Record: Record every player's score and dice throwing. Easy

Monitoring: Strategically designed to help keep track of scores, so you'll always know when you're winning! 8.5 x 11 Inch: A perfectly sized, large paged score book to easily write and see what you need to without missing a thing. High-quality paper: Bright white paper with a clean modern design. This Yahtzee Score Book is ideal for any real Yahtzee player who wants to stay on top of their game! Kws: yahtzee score pads, yatzee score pads, yahtzee score cards, yahtzee pads, yahtzee score sheets, yathzee, yahtzee sheets, yahtzee score card

The Shellcoder's Handbook

Based on the authors market leading data structures books in Java and C++, this textbook offers a comprehensive, definitive introduction to data structures in Python by authoritative authors. Data Structures and Algorithms in Python is the first authoritative object-oriented book available for the Python data structures course. Designed to provide a comprehensive introduction to data structures and algorithms, including their design, analysis, and implementation, the text will maintain the same general structure as Data Structures and Algorithms in Java and Data Structures and Algorithms in C++.

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